

# VMware SD-WAN Administration Guide

VMware SD-WAN 6.0



You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

<https://docs.vmware.com/>

**VMware by Broadcom**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2023 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to <https://www.broadcom.com>. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

# Contents

<b>1</b>	About VMware SD-WAN Administration Guide	13
<b>2</b>	What's New	14
<b>3</b>	Enterprise-level UI Changes in the New SASE Orchestrator	17
<b>4</b>	Overview	55
	VMware SD-WAN Routing Overview	56
	Dynamic Multipath Optimization (DMPO)	71
	Solution Components	85
	SD-WAN Edge Performance and Scale Data	86
	Capabilities	96
	Tunnel Overhead and MTU	98
	Network Topologies	103
	Branch Site Topologies	106
	Roles and Privilege Levels	108
	User Role Matrix	110
	Key Concepts	113
	Supported Browsers	117
	Supported Modems	117
<b>5</b>	User Agreement	119
<b>6</b>	Log in to VMware SASE Orchestrator Using SSO for Enterprise User	120
<b>7</b>	Monitor Enterprise	124
	Monitor Network Overview	125
	Monitor Security Overview	127
	Monitor Edges	136
	Monitor Edge Overview	138
	Monitor QoE	139
	Monitor Links of an Edge	141
	Monitor Path Visibility	142
	Monitor Flow Visibility	144
	Monitor Edge Applications	148
	Monitor Edge Sources	149
	Monitor Edge Destinations	151
	Monitor Business Priorities of an Edge	153

Monitor System Information of an Edge	154
Monitoring High Availability Edges	155
Monitor Network Services	161
Monitor Non SD-WAN Destinations through Gateway	162
Monitor Non SD-WAN Destinations through Edge	165
Monitor Cloud Security Service Sites	166
Monitor Zscaler IaaS Subscription	167
Monitor Edge Clusters	167
Monitor Edge VNFs	168
Monitor Routing Details	169
Monitor Multicast Groups	169
Monitor PIM Neighbors	170
Monitor BGP Edge Neighbor State	170
Monitor BFD	171
Monitor BGP Gateway Neighbor State	172
Gateway Route Table	174
Monitor Alerts	176
Monitor Events	178
Auto Rollback to the Last Known Good Configuration	179
Platform Firmware Upgrade Progress	179
Monitor Firewall Logs	180
Enterprise Reports	185
Create a New Enterprise Report	186
Create Customized Report	187
Monitor Enterprise Reports	193
View Analytics Data	196

## **8 Configure Segments** 200

## **9 SD-WAN Edge in a vNet Connecting to a vWAN Hub** 203

## **10 Configure Network Services** 206

Configure a Non SD-WAN Destination	207
VPN Workflow	208
Configure Non SD-WAN Destinations via Gateway	210
Configure Non SD-WAN Destinations via Edge	282
Configure API Credentials	300
Configure Clusters and Hubs	303
About Edge Clustering	307
Configure Netflow Settings	322
IPFIX Templates	326

Configure DNS Services	350
Configure Private Network Names	352
Configure Prefix Delegation Tags	353
Configure Authentication Services	355
Configure TACACS Services	357
Configure Edge Services	359

## 11 Cloud Security Services 367

Configure a Cloud Security Service	367
Configure Cloud Security Services for Profiles	374
Configure Cloud Security Services for Edges	376
Configure Business Policies with Cloud Security Services	387
Monitor Cloud Security Services	389
Monitor Cloud Security Services Events	393

## 12 Azure Virtual WAN IPsec Tunnel Automation 395

Azure Virtual WAN IPsec Tunnel Automation Overview	395
Prerequisite Azure Configuration	397
Register SASE Orchestrator Application	397
Assign the SASE Orchestrator Application to Contributor Role	399
Register a Resource Provider	400
Create a Client Secret	401
Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity	402
Create a Resource Group	403
Create a Virtual WAN	405
Create a Virtual Hub	406
Create a Virtual Network	408
Create a Virtual Connection between VNet and Hub	410
Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Gateway	411
Associate a Microsoft Azure Non SD-WAN Destination to an SD-WAN Profile	412
Edit a VPN Site	413
Synchronize VPN Configuration	414
Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Edge	414
Associate a Microsoft Azure Non SD-WAN Destination to an SD-WAN Edge and Add Tunnels	415
Monitor Non SD-WAN Destinations	417

## 13 Azure Accelerated Networking Support for Virtual Edges 420

Azure Instance Support	420
Enable or Disable Azure Accelerated Networking	421

Enable Accelerated Networking	421
Disable Accelerated Networking	422
Verifying Accelerated Networking	423
Azure Host Servicing	424
<b>14 VMware SD-WAN in Azure Virtual WAN Hub Deployment</b>	<b>426</b>
About VMware SD-WAN in Azure Virtual WAN Hub Deployment	426
Deploy VMware SD-WAN in Azure Virtual WAN Hub	427
Hub Upgrade Instructions for VMware SD-WAN Edge Deployed as Azure vWAN NVA	436
<b>15 SD-WAN Edge in a vNet Connecting to a vWAN Hub</b>	<b>442</b>
<b>16 CloudHub Automated Deployment of NVA in Azure vWAN Hub</b>	<b>445</b>
About CloudHub Automated Deployment of NVA in Azure Virtual WAN Hub	445
CloudHub Deployment Prerequisites	446
CloudHub Automated Deployment of Azure vWAN NVA via VMware SASE Orchestrator	447
<b>17 Configure Amazon Web Services</b>	<b>454</b>
Configure Edge for Amazon Web Services (AWS) Transit Gateway (TGW) Connect Service	454
Obtain Amazon Web Services Configuration Details	464
Configure a Non SD-WAN Destination	465
AWS CloudWAN CNE Connect using Tunnel-less BGP	465
<b>18 Security Service Edge (SSE)</b>	<b>475</b>
Palo Alto Networks Strata Cloud Manager Configuration	484
Configure Symantec API Credentials	492
<b>19 Configure Profiles</b>	<b>496</b>
Create Profile	497
Configure Profile settings	498
Global IPv6 Settings for Profiles	499
View Profile Information	500
<b>20 Configure Device Settings for Profiles</b>	<b>503</b>
Configure a Profile Device	503
Assign Segments in Profile	508
Configure VLAN for Profiles	510
Configure Management IP Address for Profiles	514
Configure Address Resolution Protocol Timeouts for Profiles	515
Configure Interface Settings	517
IPv6 Settings	557

Configure Wi-Fi Radio Settings	566
Configure Common Criteria Firewall Settings for Profiles	566
Assign Partner Gateway Handoff	568
Assign Controllers	572
Configure Cloud VPN	575
Configure Cloud Security Services for Profiles	594
Configure Zscaler Settings for Profiles	596
Configure Secure Access Service for Profiles	598
Configure Multicast Settings for Profiles	599
Configure DNS for Profiles	601
Activate OSPF for Profiles	605
Configure BFD for Profiles	609
LAN-Side NAT Rules at Profile Level	611
Configure BGP from Edge to Underlay Neighbors for Profiles	614
Configure Visibility Mode for Profiles	622
Configure SNMP Settings for Profiles	623
Configure Syslog Settings for Profiles	626
Configure Netflow Settings for Profiles	636
Configure Authentication Settings for Profiles	638
Configure NTP Settings for Profiles	639

## **21 Configure Business Policy** 642

Configure Business Policies	642
Create Business Policy Rule	646

## **22 Firewall Overview** 673

Configure Profile Firewall	676
Configure Edge Firewall	687
Configure Firewall Rule	692
Edge Firewall Support for FTPv6	698
Enhanced Firewall Services	700
Enhanced Firewall Services Overview	700
Configure Enhanced Security Services	701
View IDS/IPS Signatures	713
Monitor Security Overview	715
Enhanced Firewall Services Alerts and Events	724
Monitor Firewall Logs	730
Troubleshooting Firewall	734

## **23 Provision a New Edge** 737

**24 Provision a New Edge with Analytics 742**

- Configure Analytics Settings on an Edge 747
- Activate Self-Healing for SD-WAN Edges 749

**25 Manage Edges 751**

- Configure Edge Settings 753
- Reset Edges to Factory Settings 755

**26 Activate SD-WAN Edges 757**

- Activate SD-WAN Edges using Edge Auto-activation 758
  - Sign-Up for Edge Auto-activation 758
  - Assign Profile and License to Edges 759
  - Assign Inventory to an Edge 761
- Activate SD-WAN Edges Using Email 762
  - Send Edge Activation Email 762
  - Activate an Edge Device 764
- Request RMA Reactivation 768
  - Request RMA Reactivation Using Edge Auto-activation 768
  - Request RMA Reactivation Using Email 769

**27 Configure User Account details 771**

- Enable Secure Edge Access for an Enterprise 777
- Secure Edge CLI Commands 778
- Sample Outputs 780

**28 View Edge Information 784****29 Configure Edge Overrides 798**

- Configure VLAN for Edges 806
- Loopback Interfaces Configuration 812
  - Loopback Interfaces—Benefits 812
  - Loopback Interfaces—Limitations 812
- Configure a Loopback Interface for an Edge 813
- Configure Management Traffic for Edges 817
- Configure Address Resolution Protocol Timeouts for Edges 818
- Configure Interface Settings for Edges 819
  - Configure DHCP Server on Routed Interfaces 835
  - Enable RADIUS on a Routed Interface 839
- Configure RADIUS Authentication for a Switched Interface 842
- MAC Address Bypass (MAB) for RADIUS-based Authentication 845
- Configure Edge LAN Overrides 850

Configure Edge WLAN Overrides	851
Configure Edge WAN Overlay Settings	853
SD-WAN Service Reachability via MPLS	870
Configure Class of Service	877
Configure Hot Standby Link	880
Configure DHCPv6 Prefix Delegation for Edges	883
Global IPv6 Settings for Edges	887
Configure Wi-Fi Radio Overrides	888
Configure Automatic SIM Switchover	890
Configure Common Criteria Firewall Settings for Edges	893
Configure Cloud VPN and Tunnel Parameters for Edges	894
Configure Cloud Security Services for Edges	897
Configure Zscaler Settings for Edges	908
Configure Secure Access Service for Edges	912
Configure Multicast Settings for Edges	913
Configure BFD for Edges	914
LAN-side NAT Rules at Edge Level	915
Configure ICMP Probes/Responders	917
Configure Static Route Settings	919
Configure DNS for Edges	921
Activate OSPF for Edges	922
Configure BGP from Edge to Underlay Neighbors for Edges	923
Configure High Availability Settings for Edges	924
Configure VRRP Settings	925
Configure Visibility Mode for Edges	928
Configure Syslog Settings for Edges	928
Configure Netflow Settings for Edges	930
Configure SNMP Settings for Edges	932
Security Virtual Network Functions	935
Configure VNF Management Service	938
Configure Security VNF without High Availability	939
Configure Security VNF with High Availability	944
Define Mapping Segments with Service VLANs	948
Configure VLAN with VNF Insertion	949
Monitor VNF for an Edge	952
Monitor VNF Events	953
Configure VNF Alerts	954
Configure Authentication Settings for Edges	955
Configure NTP Settings for Edges	956
Configure TACACS Services for Edges	958

**30 SD-WAN Gateway Migration 959**

- VMware SD-WAN Gateway Migration - Limitations 960
- Migrate Quiesced Gateways 961
- What to do When Switch Gateway Action Fails 968

**31 Object Groups 969**

- Configure Object Groups 969
- Configure Business Policies with Object Group 975
- Configure Firewall Rule with Object Group 977

**32 Site Configurations 982**

- Data Center Configurations 983
- Configure Branch and Hub 984

**33 Configure Dynamic Routing with OSPF or BGP 992**

- Activate OSPF for Profiles 992
- Route Filters 996
- Activate OSPF for Edges 996
- Configure BGP 997
  - Configure BGP from Edge to Underlay Neighbors for Profiles 997
  - Configure BGP from Edge to Underlay Neighbors for Edges 1005
  - Configure BGP Over IPsec from Edge to Non SD-WAN Neighbors 1005
  - Configure BGP Over IPsec from Gateways 1016
  - Monitor BGP Sessions 1026
  - Monitor BGP Events 1026
  - Troubleshooting BGP Settings 1027
- OSPF/BGP Redistribution 1028
- BFD Settings 1029
  - Configure BFD for Profiles 1030
  - Configure BFD for Edges 1032
  - Configure BFD for BGP for Profiles 1033
  - Configure BFD for BGP for Edges 1034
  - Configure BFD for OSPF 1034
  - Configure BFD for OSPF for Edges 1037
  - Configure BFD for Gateways 1038
  - Monitor BFD Sessions 1040
  - Monitor BFD Events 1041
  - Troubleshooting BFD 1042
- Overlay Flow Control 1042
  - Configure Global Routing Preferences 1046
  - Configure Subnets 1048

**34 Route Summarization 1051**

Route Summarization Configuration 1052

**35 Configure Alerts and Notifications 1053**

Configure Alerts 1054

Configure SNMP Traps 1058

Configure Webhooks 1059

**36 Testing and Troubleshooting 1065**

Run Remote Diagnostics 1065

Remote Actions 1067

Diagnostic Bundles for Edges 1068

Request Packet Capture Bundle 1069

Request Diagnostic Bundle 1071

**37 Edge Licensing 1074**

Example of Edge Licensing 1076

**38 Edge Software Image Management 1079**

Edge Software Image Management Overview 1079

Activate Edge Image Management 1079

Edge Image Assignment and Access 1080

Edge Management 1081

Upgrade SD-WAN Edges 1084

**39 User Management - Enterprise 1085**

**40 Enterprise Settings 1086**

**41 Configure High Availability on SD-WAN Edge 1087**

How SD-WAN Edge High Availability (HA) Works 1087

Failure Scenarios 1088

High Availability Deployment Models 1088

Standard HA 1089

Enhanced HA 1093

Mixed-Mode HA 1100

Split-Brain Condition 1101

Split-Brain Detection and Prevention 1102

Support for BGP Over HA Link 1105

High Availability Graceful Switchover with BGP Graceful Restart 1105

Selection Criteria to Determine Active and Standby Status 1110

VLAN-tagged Traffic Over HA Link	1110
Configure High Availability (HA)	1111
Deploying High Availability on VMware ESXi	1111
Prerequisites	1121
Activate High Availability	1121
Wait for SD-WAN Edge to Assume Active	1124
Connect the Standby SD-WAN Edge to the Active Edge	1124
Connect LAN and WAN Interfaces on Standby SD-WAN Edge	1125
Deactivate High Availability (HA)	1126
HA Event Details	1127

## **42 VMware Virtual Edge Deployment** 1129

Deployment Prerequisites for VMware Virtual Edge	1129
Special Considerations for VMware Virtual Edge deployment	1131
Cloud-init Creation	1132
Install VMware Virtual Edge	1134
Activate SR-IOV on KVM	1134
Install Virtual Edge on KVM	1136
Enable SR-IOV on VMware	1140
Install Virtual Edge on VMware ESXi	1142

## **43 Appendix** 1148

Enterprise-Level Orchestrator Alerts and Events	1148
Supported VMware SD-WAN Edge Events for Syslogs	1196

# About VMware SD-WAN Administration Guide

1

The VMware SD-WAN™ (*formerly known as VMware SD-WAN™ by VeloCloud®*) Administration Guide provides information about VMware SASE Orchestrator and the core VMware configuration settings, including how to configure and manage Network, Network Services, Edges, Profiles, and Customers who use the SASE Orchestrator.

## Intended Audience

This guide is intended for network administrators, network analysts, and IT administrators responsible for deploying, monitoring and managing Enterprise branch network.

Beginning with Release 4.4.0, VMware SD-WAN is offered as part of VMware SASE. To access SASE documentation for Cloud Web Security and Secure Access, along with Release Notes for version 4.4.0 and later, see [VMware SASE](#).

Here is a quick walkthrough of the user journey as an Enterprise super user:

- 1 [Install SD-WAN Orchestrator](#) (On-prem deployments only)
- 2 [Configure Enterprise Information and Authentication](#)
- 3 [Configure Alerts and Notifications](#)
- 4 [Configure Enterprise Administrator and Users](#)
- 5 [Configure Profiles](#)
- 6 [Manage Edge Licensing](#)
- 7 [Provision Edges](#)
- 8 [Configure Edges](#)
- 9 [Monitor and Troubleshoot Edges](#)

# What's New

# 2

# What's New in Version 6.0.0

Feature	Description
Enhanced Firewall Services	<p>In Release 6.0.0, the <a href="#">Enhanced Firewall Services Overview</a> functionality supports URL Category Filtering, URL Reputation Filtering, and Malicious IP Filtering in addition to Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) services on VMware SD-WAN Edges. The following enhancements are introduced for the EFS functionality:</p> <ul style="list-style-type: none"> <li>■ URL Filtering and Malicious IP Filtering - The URL Filtering and Malicious IP Filtering services are powered by VMware's award-winning Security components, empowering IT administrators to reduce their system's attack surface. Through URL Filtering, web traffic is filtered based on Category and Reputation. Integrating the capabilities of VMware Security with VMware SD-WAN Edge platforms enables clients to confidently remove legacy firewalls at branch locations without compromising security and experiencing the benefits of streamlined network and security operations. Additionally, clients leverage VMware's investment in threat intelligence. The solution also provides extensive traffic and threat visualization through improved security dashboards. To configure and manage URL Filtering and Malicious IP Filtering, see the following topics: <ul style="list-style-type: none"> <li>■ <a href="#">Configure Enhanced Security Services</a></li> <li>■ <a href="#">Configure Profile Firewall</a></li> <li>■ <a href="#">Configure Edge Firewall</a></li> <li>■ <a href="#">Configure Firewall Rule</a></li> </ul> </li> <li>■ Security Service Groups - Security Service Groups are organized collections of security service settings that are offered as part of the Enhanced Firewall Services. These settings include URL Category, URL Reputation, Malicious IP, and IDS/IPS. These groups are designed to simplify firewall policy management by enabling the creation and reuse of predefined security service configurations across multiple firewall rules. This approach eliminates the need to create and maintain multiple individual security service settings for each firewall rule, thereby streamlining the process and enhancing efficiency. To create a Security Service Group using the pre-configured security services and associate that Security Service Group with the Firewall rules, see <a href="#">Configure Enhanced Security Services</a>.</li> <li>■ Monitor Security Overview - The <a href="#">Security Overview</a> page is enhanced to display the overall impact summary of configured Security services, like IDS/IPS, URL Categories, URL Reputations, and Malicious IP for all Edges within an Enterprise, based on the metrics collected using the various EFS engines (IDS/IPS/URL Filtering/Malicious IP). For more information, see <a href="#">Monitor Security Overview</a>.</li> <li>■ Improved Firewall Logging - The Firewall logging feature presents a comprehensive pane view for each log record selection, encompassing both Firewall and Enhanced Firewall Service engine-related data. Furthermore, new intelligent filters have been integrated to facilitate the searching of logs based on</li> </ul>

Feature	Description
	<p>specific engines, including Firewall, Intrusion Detection System/Intrusion Prevention System (IDS/IPS), URL Category, URL Reputation, and Malicious IP. For more information, see <a href="#">Monitor Firewall Logs</a>.</p> <ul style="list-style-type: none"> <li>■ To support configuration and monitoring of URL Filtering and Malicious IP Filtering on Edges, new events, alerts, and troubleshooting tests are added. For more information, see <a href="#">Enhanced Firewall Services Alerts and Events</a> and <a href="#">Troubleshooting Firewall</a>.</li> </ul>
ECMP Support on Gateway	<p>To optimize the utilization of the aggregated bandwidth across the ingress interfaces of non-SDWAN sites, VMware SD-WAN solution incorporates <b>active-active</b> mode support in its gateways. <b>Active/Active</b> mode supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP. This can be achieved by enabling the establishment of multiple IPsec tunnels in active-active mode towards non-SDWAN sites. This configuration allows load balancing of network traffic across tunnels optimizing the flow of distribution. For more information, see</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure Non SD-WAN Destinations via Gateway</a></li> <li>■ <a href="#">Configure BGP Over IPsec from Gateways</a></li> </ul> <p><b>Monitor Non SD-WAN Destinations through Gateway</b></p> <p>The Non SD-WAN Destinations via Gateway tab displays the details of already configured Non SD-WAN Destination. The parameters displayed are:</p> <ol style="list-style-type: none"> <li>1 Total Bytes</li> <li>2 Bytes Received/Sent</li> <li>3 Total Packets</li> <li>4 Packets Received/Sent</li> </ol> <p>For more information, see <a href="#">Monitor Non SD-WAN Destinations through Gateway</a>.</p>
VMware Edge Intelligence	<p><b>VMware Edge Network Intelligence</b> is now renamed to VMware Edge Intelligence in the documentation.</p> <p><b>Note</b> As the rebranding of the SASE Orchestrator for the product name change is targeted for the next release, all the UI screenshots in this document still display the old product name.</p>

## Release Notes

For information on all the new/modified features for 6.0.0, see <https://docs.vmware.com/en/VMware-SASE/6.0.0/rn/vmware-sase-600-release-notes/index.html>.

## Previous VMware SD-WAN Versions

To get product documentation for previous VMware SD-WAN versions, contact your VMware SD-WAN representative.

# Enterprise-level UI Changes in the New SASE Orchestrator

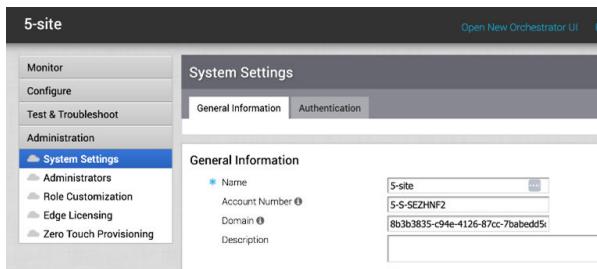
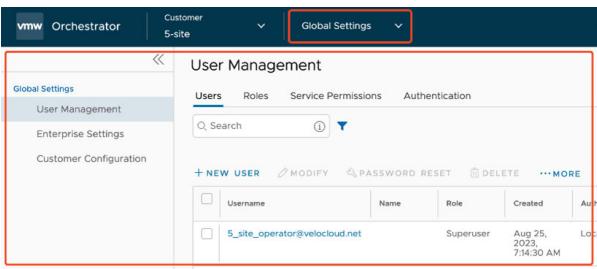
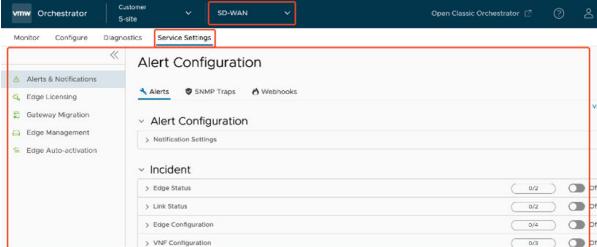
3

The VMware SASE Orchestrator (formerly the VeloCloud Orchestrator and soon to be the VMware Edge Cloud Orchestrator) has moved and redesigned some features to fit the wider scope of the product and user interface (UI). The new UI has changed from a single product portal (only for SD-WAN) to a common management system that lets customers access multiple services in one place. These services include VMware SD-WAN, VMware Edge Intelligence, VMware Secure Access, VMware Cloud Web Security, and VMware SD-Access (formerly called as VMware SD-WAN Client). Future services such as VMware Private Mobile Network and VMware Edge Compute Stack will also be added. The new UI navigation has adapted to allow access to multiple services within one shared header. The primary global header now has an **Enterprise Applications** (Services) drop-down menu that lists the various supported services. You can select and navigate to each service from this menu. Enterprise **Global Settings** is now located in the **Enterprise Applications** (Services) drop-down because it has features that are shared across services. These features include User Management, Authentication, Role Customization (now Roles and Service Permissions), Customer Configuration, and more.

This document explains the changes in the Enterprise UI for some features. It also gives the reasons for these changes.

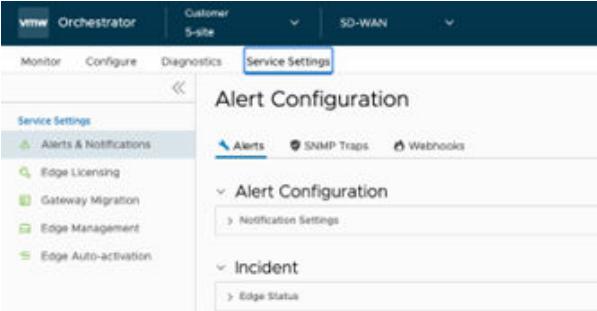
## SD-WAN Administration:Global Settings and SD-WAN Settings

Now that **SD-WAN** is one of the many services available in the Orchestrator, the original **Administration** section is split and moved under **Global Settings** and **SD-WAN Settings**. All Edge or **SD-WAN** specific settings are moved to **Service Settings** within the **SD-WAN** service, and all **Administration** related or shared settings across services are moved to the **Global Settings** service.

Classic Orchestrator Location	New Orchestrator Location
<b>Enterprise &gt; Administration</b>	<b>Enterprise &gt; Global Settings</b>
	
<b>Enterprise &gt; SD-WAN &gt; Service Settings</b>	
	

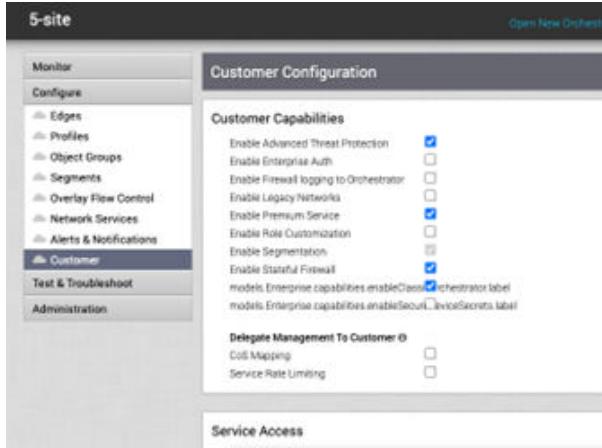
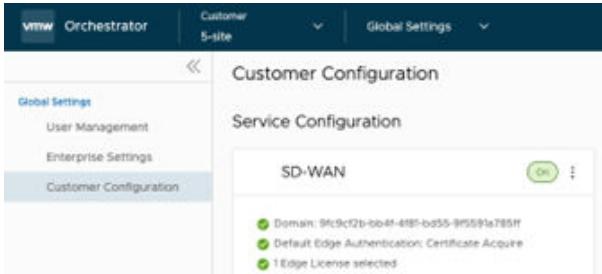
## Alert Configuration

**Alert Configuration** is moved under **Service Settings** because these settings affect the operations of the **SD-WAN** service and are not related to the **SD-WAN** network configuration.

Classic Orchestrator Location	New Orchestrator Location
<b>Enterprise &gt; Configure &gt; Alerts &amp; Notifications</b>	<b>Enterprise &gt; &gt; Service Settings &gt; Alerts &amp; Notifications &gt; SD-WAN</b>
	

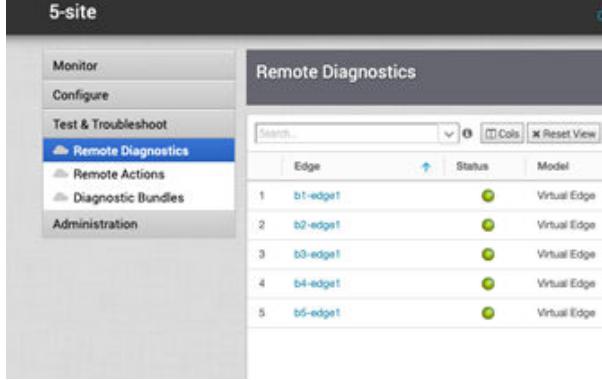
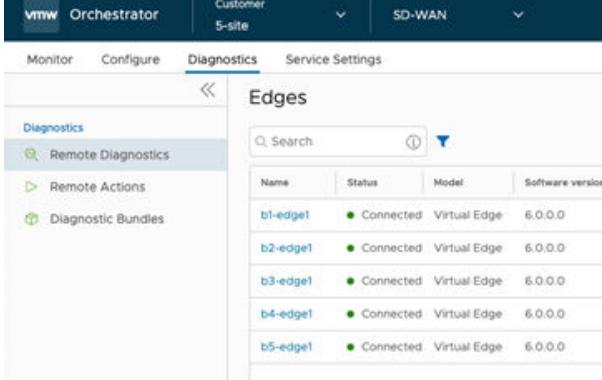
# Customer Configuration

**Customer Configuration** is moved under Enterprise **Global Settings** because this page is shared across various Orchestrator services in addition to the core **SD-WAN** service. The **Customer Configuration** page is reorganized with a section to add and modify services for the customer account, group feature access within services, and additional global settings at a high level for each service and across multiple services.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer	Enterprise > Global Settings > Customer Configuration
	

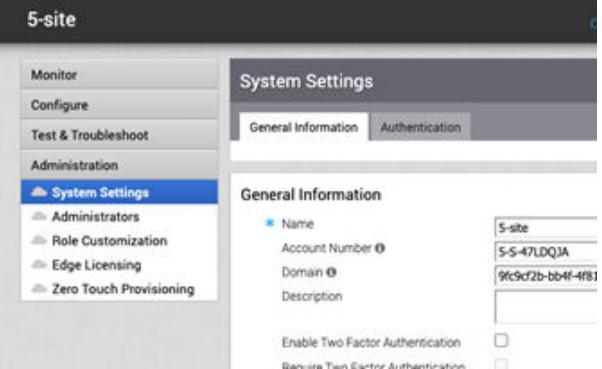
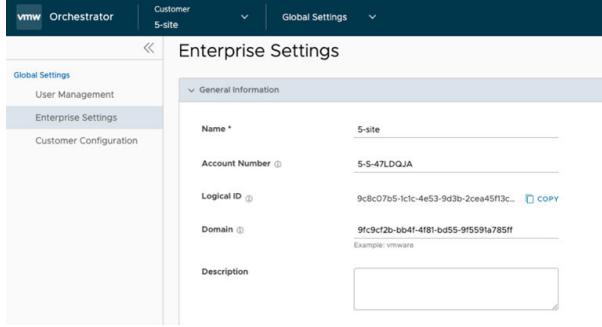
# Test & Troubleshoot

**Test & Troubleshoot** is renamed to **Diagnostics** to better align with the features nested inside it.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Test & Troubleshoot	Enterprise > SD-WAN > Diagnostics
	

## System Settings > General Information > General Information section

Most sections of **System Settings** are moved within **Global Settings** because the **Global Settings** menu provides a single location for shared settings across various Orchestrator services. The **System Settings** is renamed to **Enterprise Settings** because this page is focused on Enterprise-specific configuration settings.

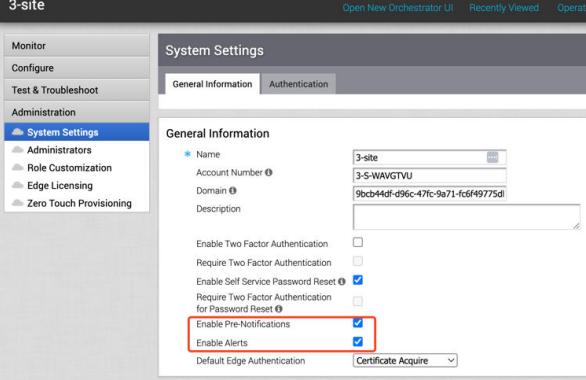
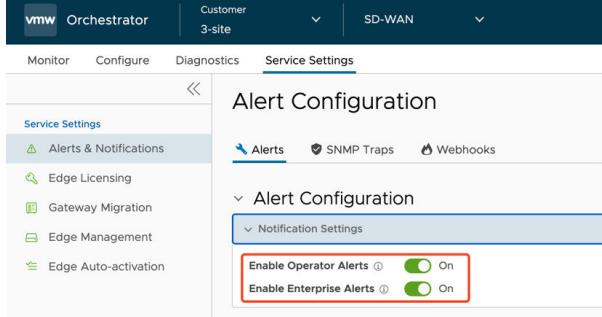
Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > General Information	Enterprise > Global Settings > Enterprise Settings
	

## System Settings > General Information > Pre-Notifications and Alerts

Alert Notification settings are moved under **Alerts & Notifications** section in the **SD-WAN > Service Settings** page. This helps in better understanding of the alerts and their corresponding services.

Also, **Enable Pre-Notifications** is renamed to **Enable Operator Alerts**, and **Enable Alerts** is renamed to **Enable Enterprise Alerts**.

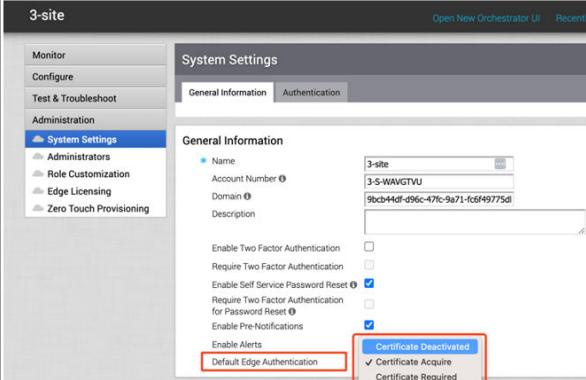
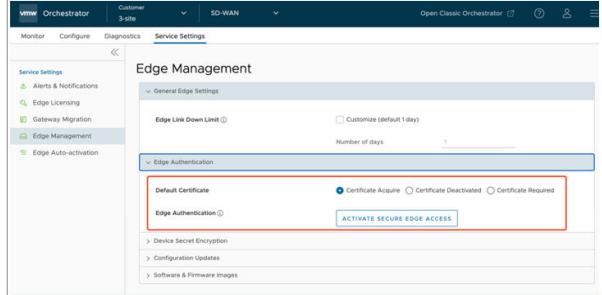
Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > General Information	Enterprise > SD-WAN > Service Settings > Alerts & Notifications > Alerts

## System Settings > General Information > Default Edge Authentication

**Default Edge Authentication** is renamed to **Default Certificate**, and is moved under **Edge Management** in the **SD-WAN > Service Settings** page. These settings are now redesigned as radio buttons.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > General Information UI label was originally <b>Default Edge Authentication</b> .	Enterprise > SD-WAN > Service Settings > Edge Management > Edge Authentication UI label <b>Default Edge Authentication</b> renamed <b>Default Certificate</b> .

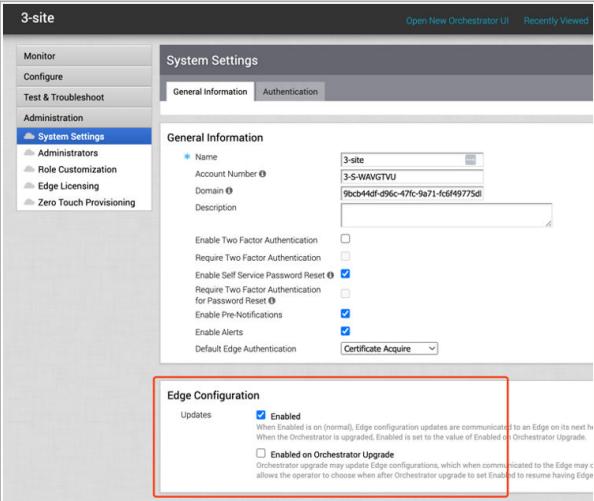



# System Settings > General Information > Edge Configuration Updates

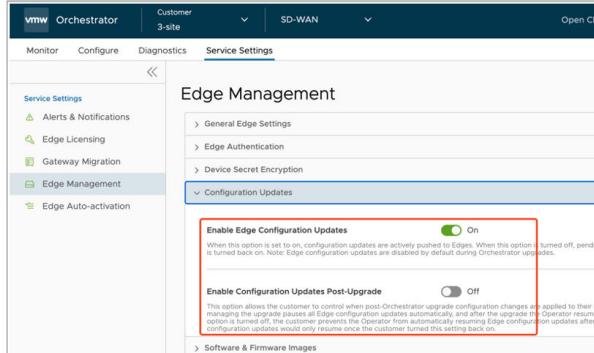
Edge Configuration is moved into the **SD-WAN Edge Management** page for better organization. The controls for updates are renamed to provide more clarity on the Edge action and result.

Classic Orchestrator Location	New Orchestrator Location
<p><b>Enterprise &gt; Administration &gt; System Settings &gt; General Information &gt; Edge Configuration</b></p> <p>UI labels were originally:</p> <ul style="list-style-type: none"> <li>■ <b>Updates - Enabled</b></li> <li>■ <b>Updates - Enabled on Orchestrator Upgrade</b></li> </ul>	<p><b>Enterprise &gt; SD-WAN &gt; Service Settings &gt; Edge Management &gt; Edge Authentication</b></p> <ul style="list-style-type: none"> <li>■ UI label <b>Updates - Enabled</b> is renamed to <b>Enable Edge Configuration Updates</b>.</li> <li>■ <b>Updates - Enabled on Orchestrator Upgrade</b> is renamed to <b>Enable Configuration Updates Post-Upgrade</b>.</li> </ul>



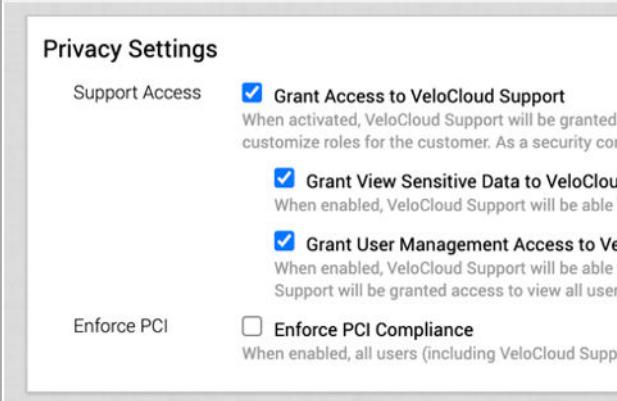
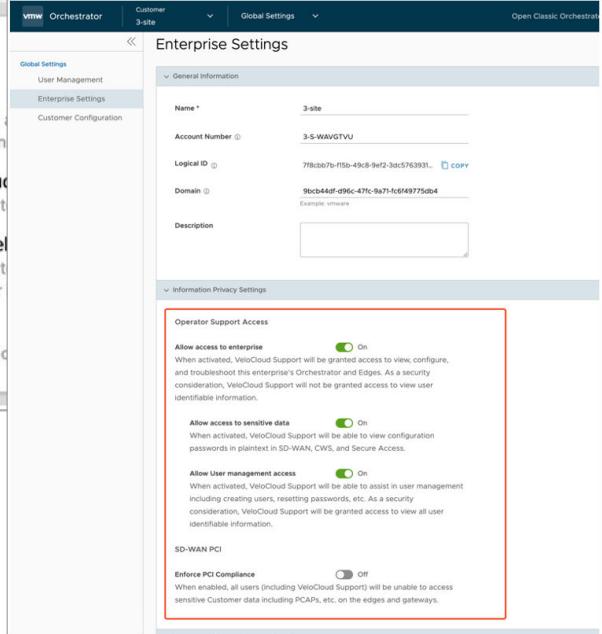
The screenshot shows the 'General Information' tab selected in the 'System Settings' section. On the left, the navigation menu includes 'System Settings' under 'Administration'. The 'Edge Configuration' section contains two main options: 'Enabled' (checkbox checked) and 'Enabled on Orchestrator Upgrade' (checkbox unchecked). A red box highlights the 'Enabled' checkbox.



The screenshot shows the 'Service Settings' tab selected in the 'SD-WAN' section. Under 'Edge Management', there are two configuration options: 'Enable Edge Configuration Updates' (checkbox checked, labeled 'On') and 'Enable Configuration Updates Post-Upgrade' (checkbox unchecked, labeled 'Off'). A red box highlights the 'On' checkbox for 'Enable Edge Configuration Updates'.

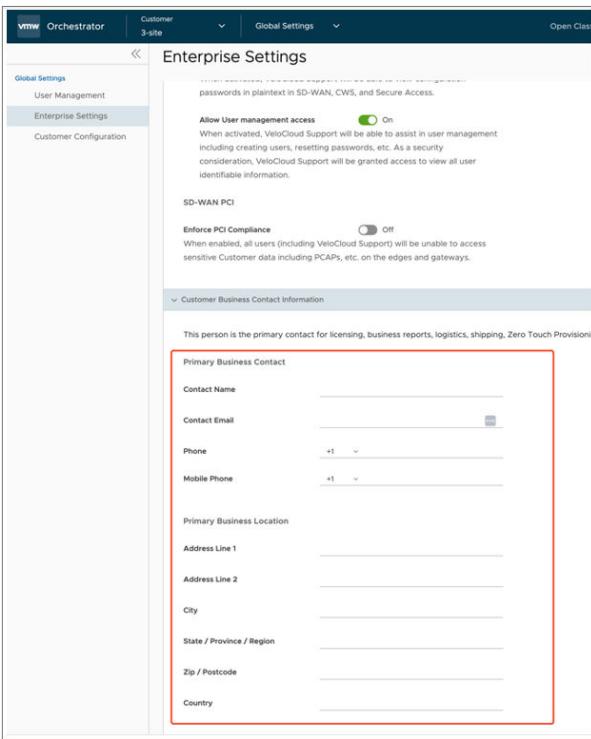
# System Settings > General Information > Privacy Settings

We have relocated the **Privacy Settings** feature to the **Global Settings** page. This is because the **Privacy Settings** feature affects various Orchestrator services, not just SD-WAN.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > General Information > Edge Configuration	Enterprise > Global Settings > Enterprise Settings > Information Privacy Settings
	

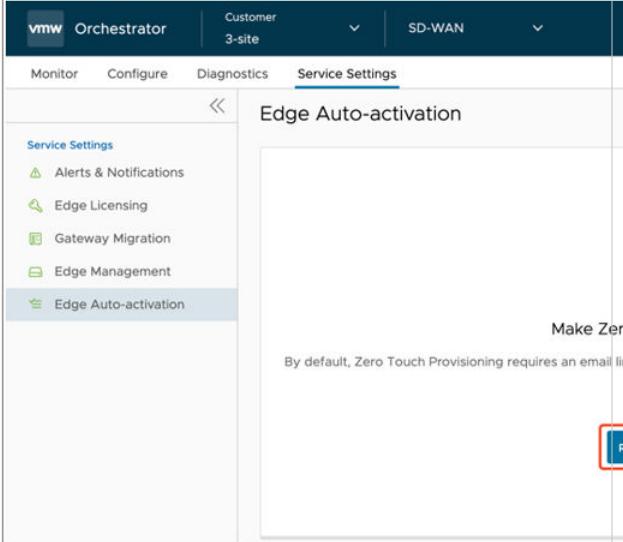
## System Settings > General Information > Contact Information

We have moved the **Contact Information** for the Enterprise feature to the **Global Settings** page. We also renamed **Contact Information** to **Customer Business Contact Information**, and together these changes make it easier to understand and use the customer information across various Orchestrator services.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > General Information > Contact Information	Enterprise > Global Settings > Enterprise Settings > Customer Business Contact Information
	

## System Settings > General Information > Zero Touch Provisioning Sign Up

We have moved all the Zero Touch Provisioning related UI sections to the new **Edge Auto-activation** section within the **SD-WAN > Service Settings** page for better clarity and organization.

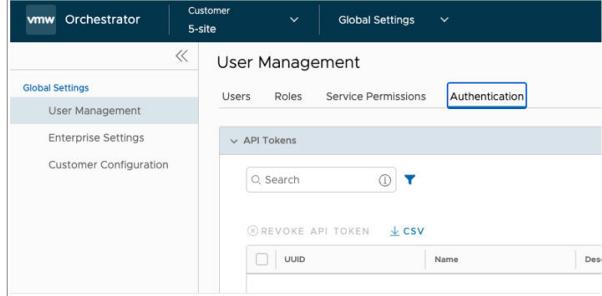
Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > General Information > Zero Touch Provisioning Sign Up	Enterprise > SD-WAN > Service Settings > Edge Auto-activation
	 <p>VMW Orchestrator Customer 3-site SD-WAN</p> <p>Monitor Configure Diagnostics Service Settings</p> <p>Service Settings</p> <ul style="list-style-type: none"> <li>Alerts &amp; Notifications</li> <li>Edge Licensing</li> <li>Gateway Migration</li> <li>Edge Management</li> <li>Edge Auto-activation</li> </ul> <p>Edge Auto-activation</p> <p>Make Zero Touch Provisioning</p> <p>By default, Zero Touch Provisioning requires an email link to activate Edges. To a capability below.</p> <p>REQUEST AUTO ACTIVATION</p>

<h3>Zero Touch Provisioning Sign Up</h3> <p>In order to use push fulfillment you should include the SID entered discovered with inventory please contact support with the order number inventory shipped after you sign up for Zero Touch Provisioning w</p> <p>* SID <input type="text"/></p> <p><b>Submit</b></p>	<p>Request Auto-activation</p> <p>To use the Auto-activation feature, you must enter a valid Subscription ID, received at the time of registering with VMware for the SD-WAN service. This will allow VMware to track your inventory correctly.</p> <p>Please note that only inventory shipped after you sign up for the Auto-activation capability will show up on your account.</p> <p>Subscription ID (SID)</p> <p>Required field. This is the Enterprise commercial ID used for transactions with VMware</p> <p>CANCEL REQUEST AUTO-ACTIVATION</p>
---	--

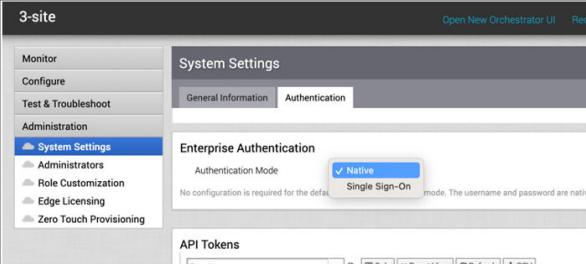
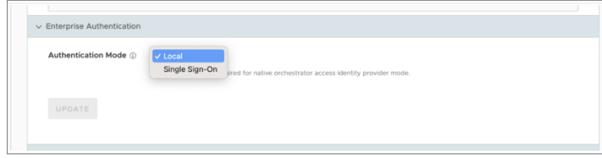
## System Settings > Authentication Tab

We have moved the Enterprise Authentication related settings from the **System Settings > Authentication** tab to the **Global Settings** page. This is because the **Global Settings** page is a single location for settings that apply to various Orchestrator services. Authentication is one of these settings, as it affects multiple services and the whole Orchestrator. The new location for the Authentication settings is under the **User Management > Authentication** page within **Global Settings**. This groups the user management related features together and makes them consistent with how other VMware products handle their user authentication organization.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > Authentication	Enterprise > Global Settings > User Management > Authentication
	

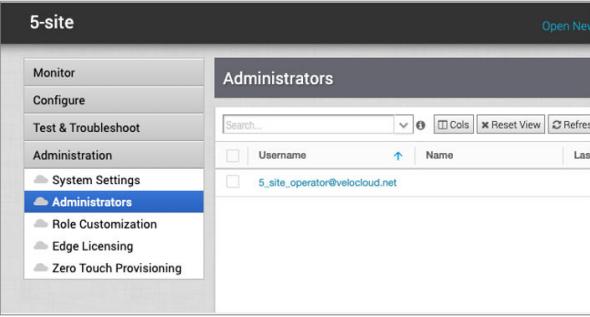
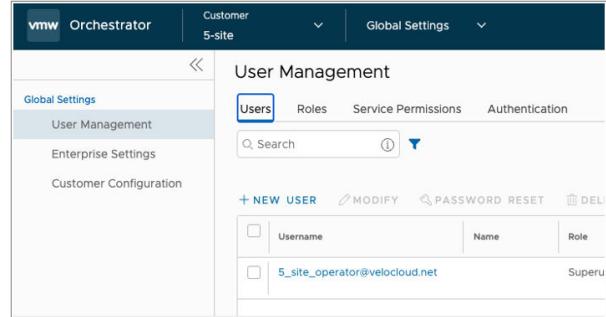
## System Settings > Authentication Tab > Enterprise Authentication

We moved **Enterprise Authentication** settings to **Global Settings** because this setting affects various Orchestrator services, not just SD-WAN. We have also changed the name of the **Native** authentication option to **Local**, with the **Single Sign-On** authentication option remaining unchanged.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > Authentication > Enterprise Authentication	Enterprise > Global Settings > User Management > Authentication
	

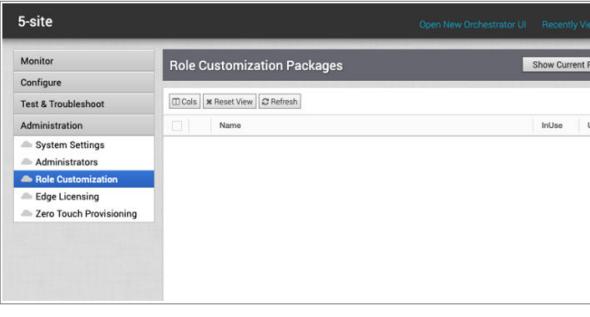
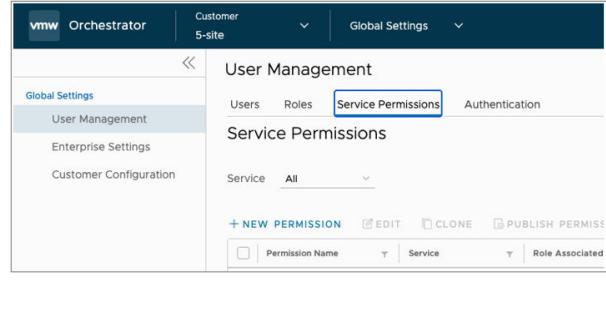
## Administrators

We have moved the **Administrators** feature from the **System Settings** tab to the **Global Settings** page. This is because the **Global Settings** page is a single location for settings that apply to various Orchestrator services. **Administrators** is one of these settings, as it allows you to manage and create users and roles for multiple services and the whole Orchestrator. We have also changed the name of the **Administrators** feature to **Users**. This is to make it consistent with other VMware product terminology and to avoid confusion with the admin role.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > Administrators	Enterprise > Global Settings > User Management > Users
	

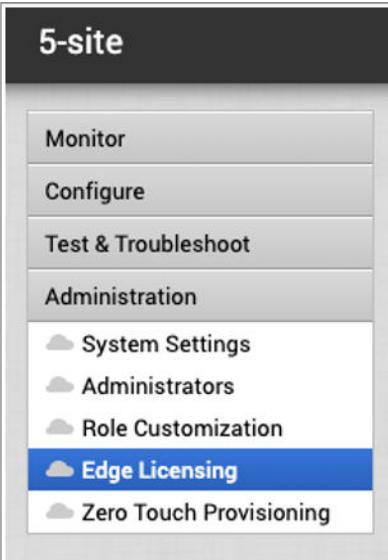
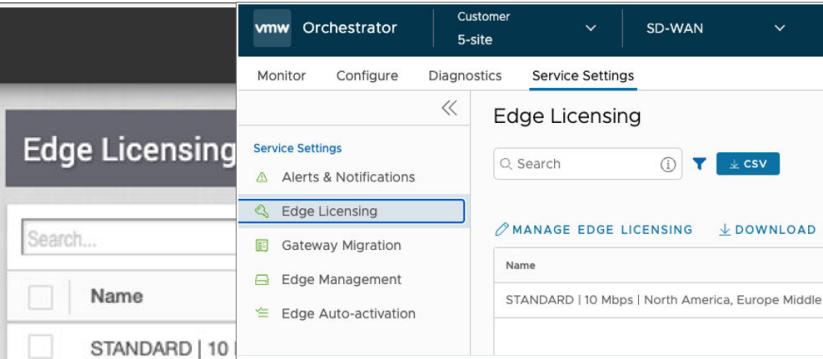
## Role Customization

We have changed the name of the **Role Customization** feature to **Service Permissions**. This is to make room for the new **Role Builder** feature that lets you create custom roles by combining different service permissions. **Service Permissions** is a more accurate name for the feature, as it allows you to adjust the access levels for each service.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > Role Customization	Enterprise > Global Settings > User Management > Service Permissions
	

## Edge Licensing

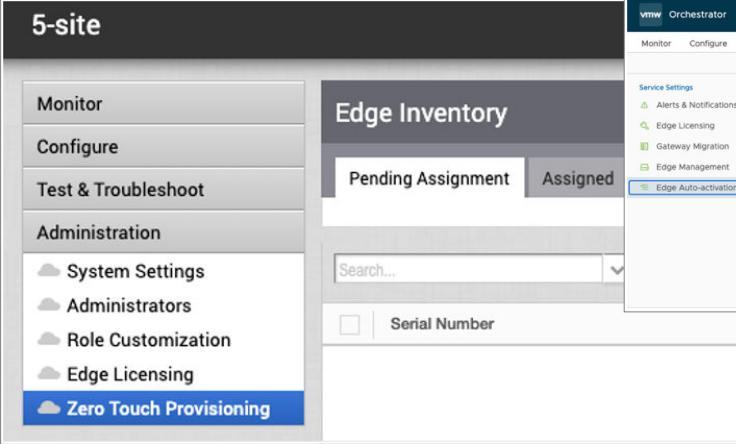
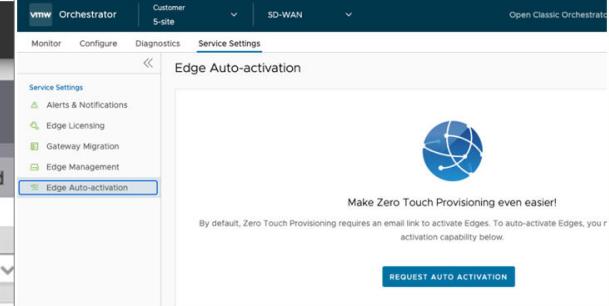
We have relocated the **Edge Licensing** feature because the Classic Orchestrator UI could not handle multiple services that need configuration at the Enterprise level. The New Orchestrator UI is a portal for many services, not just SD-WAN. Edge Licensing is a feature that only applies to SD-WAN, so we have moved it to the new **Service Settings** tab within the **SD-WAN** service.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > Edge Licensing	Enterprise > SD-WAN > Service Settings > Edge Licensing
	

## Zero Touch Provisioning (ZTP)

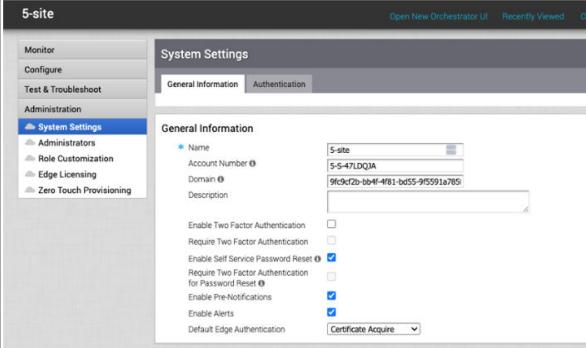
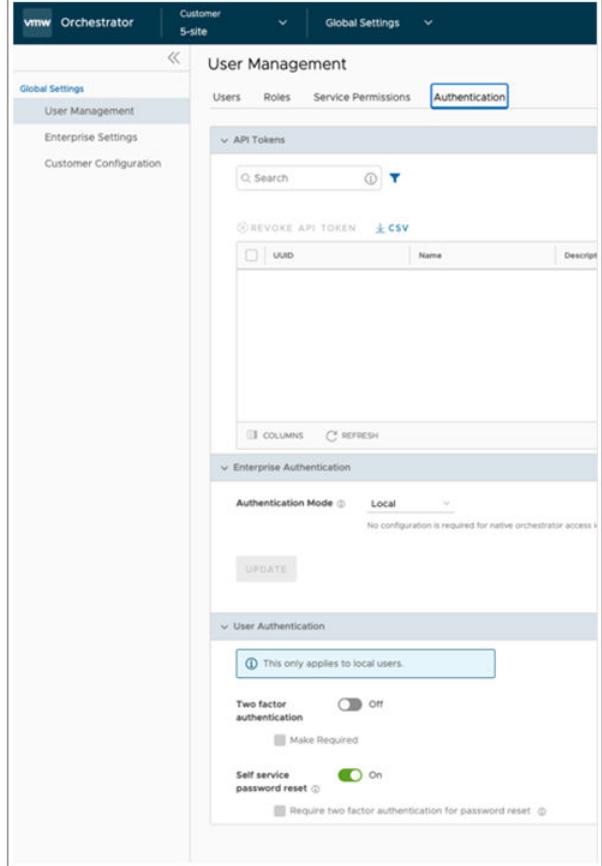
We have changed the way you activate your Edges in the New Orchestrator UI. You no longer need to enable **Zero Touch Provisioning** (ZTP) in the **System Settings**. You can access the ZTP feature directly from the **Edge Auto-Activation** page. We have also renamed the ZTP feature to **Edge Auto-Activation**, because it includes both the new automatic activation method and the original email activation method. You can choose either method from the Edge Configuration page. The **Edge Auto-Activation** feature is specific to SD-WAN, so we have moved it to the new **Service Settings** tab within the **SD-WAN** service. The **Service Settings** tab is part of the **Global Settings** page, which is a single location for settings that apply to various Orchestrator services.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > Zero Touch Provisioning	Enterprise > SD-WAN > Service Settings > Edge Auto-Activation

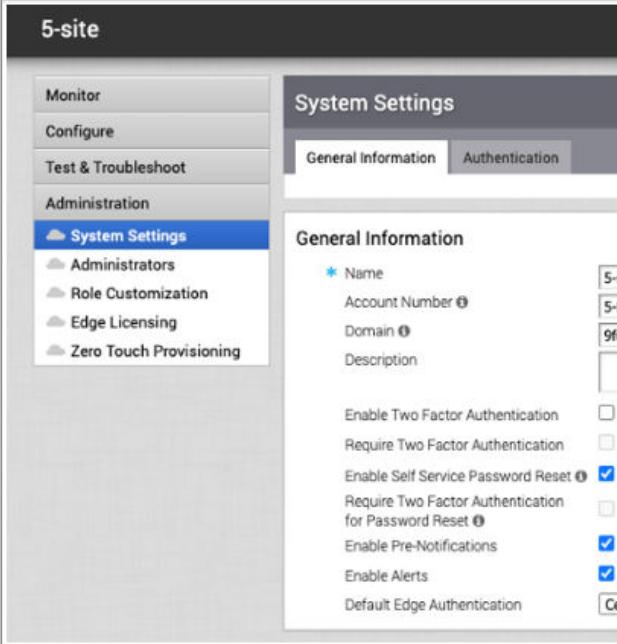
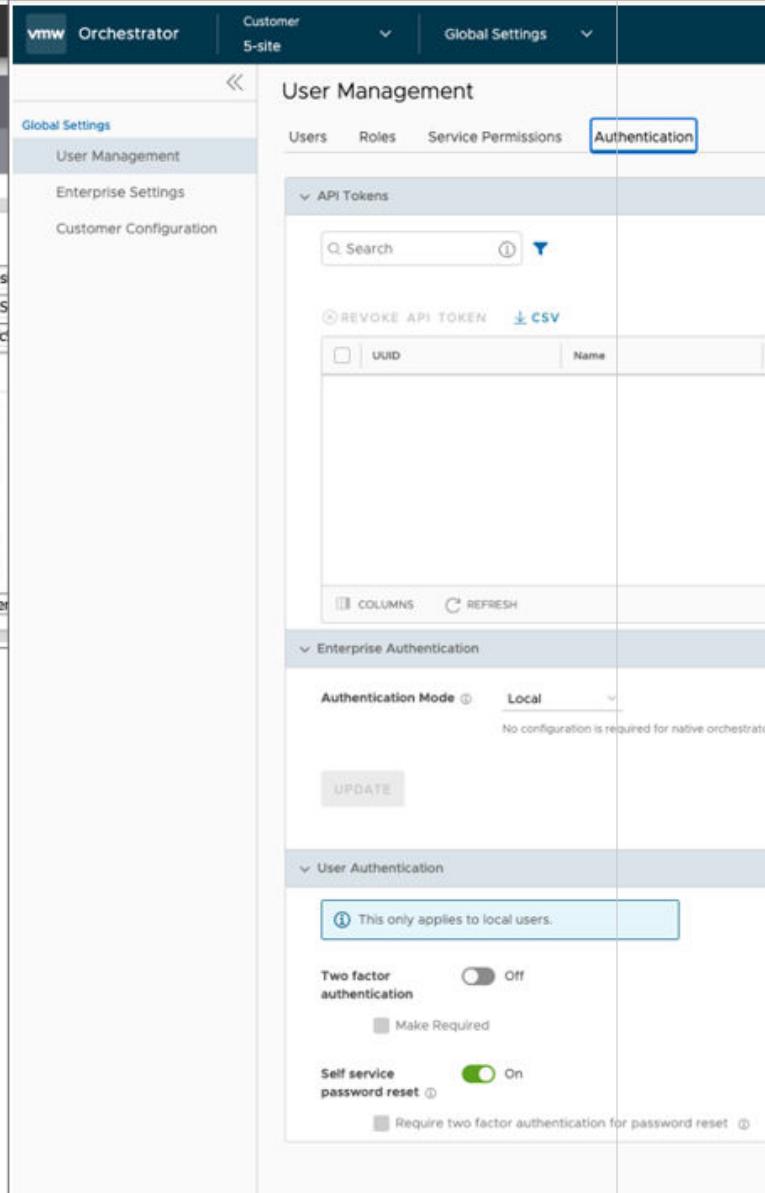
## Two Factor Authentication

We have relocated the **Two Factor Authentication** feature from the **System Settings** tab to the **Global Settings** page. This is because the Two Factor Authentication feature affects users across various Orchestrator services. The new location for the feature is under the **User Management** section within the **Global Settings** page. This makes it more consistent with other VMware products.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > General Information > Enable Two Factor Authentication	Enterprise > Global Settings > User Management > Authentication > User Authentication > Two Factor Authentication
 <p>The screenshot shows the 'System Settings' page with the 'General Information' tab selected. It displays fields for Name (5-site), Account Number (5-S-47.DQJA), Domain (9fd9c2b-bb4f-4f81-bd55-9f5591a785), and Description. Under 'Enable Two Factor Authentication', the 'Require Two Factor Authentication' checkbox is unchecked, while 'Enable Self Service Password Reset' and 'Require Two Factor Authentication for Password Reset' are checked.</p>	 <p>The screenshot shows the 'User Management' page with the 'Authentication' tab selected. It includes sections for 'API Tokens' (with a 'REVOKE API TOKEN' button and CSV export option) and 'Enterprise Authentication' (set to 'Local'). In the 'User Authentication' section, a note states 'This only applies to local users.' Below it, 'Two factor authentication' is set to 'Off' (checkbox unchecked), 'Make Required' is unchecked, and 'Self service password reset' is set to 'On' (checkbox checked). A note at the bottom says 'Require two factor authentication for password reset'.</p>

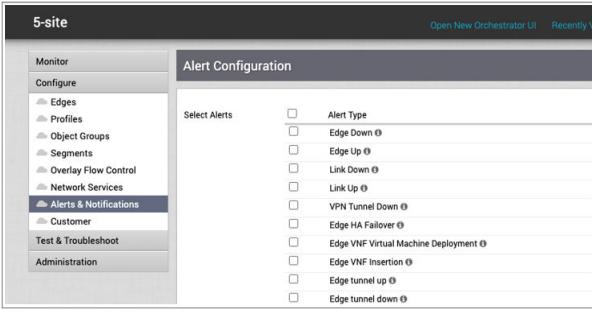
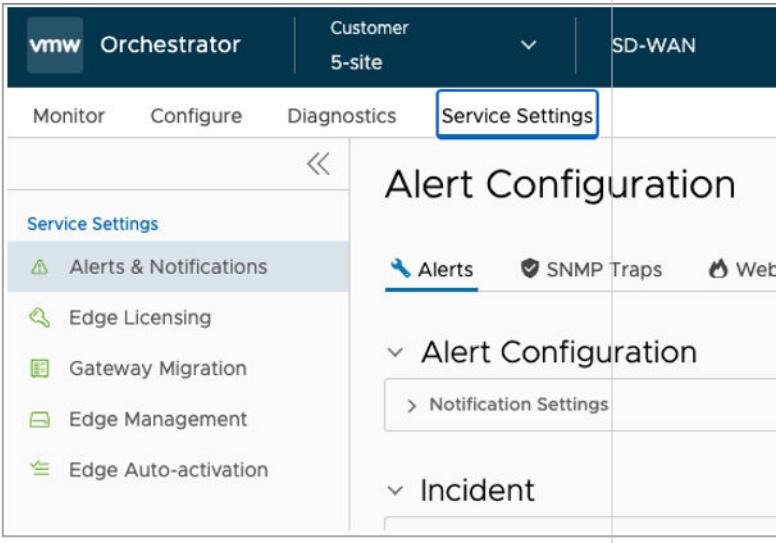
## Self-Service Password Reset

We have moved **Password Reset** to the **Authentication** tab within **Global Settings** because this setting affects the Enterprise Orchestrator as a whole and not just SD-WAN.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Administration > System Settings > General Information > Enable Self Service Password Reset	Enterprise > Global Settings > User Management > Authentication > User Authentication > Self Service Password Reset
	

## Enterprise > Configure > Alerts & Notifications

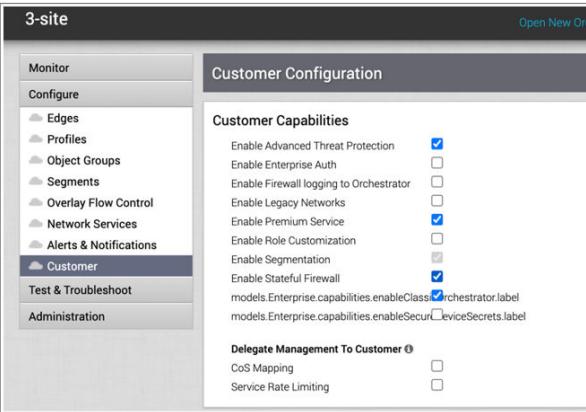
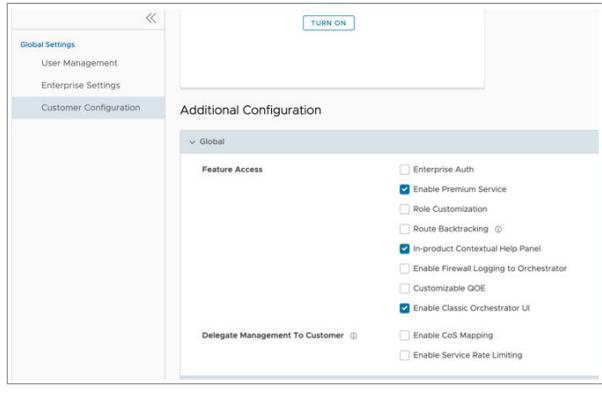
We have moved the **Alerts & Notifications** feature from the **Configure** tab to the **SD-WAN > Service Settings** page. This is because the **Configure** tab is for **Network Configurations**, such as Profiles, Business Policies, and Firewall Rules. The **Service Settings** page is for SD-WAN Orchestrator settings, such as **Edge Licensing**, **Edge Auto-Activation**, and **Alerts & Notifications**.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Alerts & Notifications	Enterprise > SD-WAN > Service Settings > Alerts & Notifications
	The Alert Configuration page is organized into three tabs: <ul style="list-style-type: none"> <li>■ Alerts</li> <li>■ SNMP Traps</li> <li>■ Webhooks</li> </ul> 

## Customer Configuration > Customer Capabilities

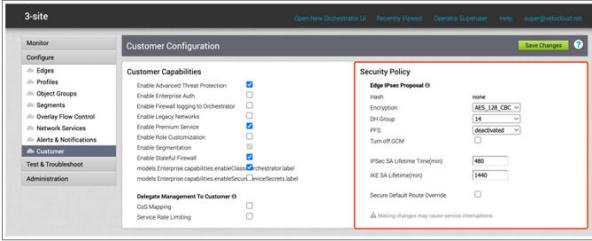
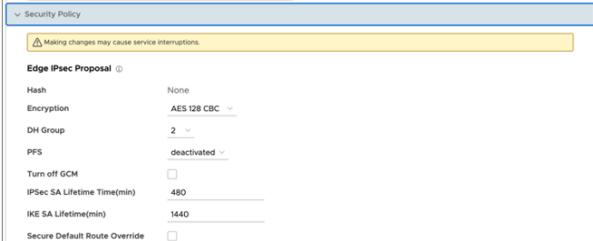
We have relocated the **Customer Capabilities** feature from the **System Settings** tab to the **Global Settings** page. This is because the **Customer Capabilities** feature affects the whole Enterprise Orchestrator, not just SD-WAN. We have also changed the name of the feature to **Feature Access**, because it allows you to activate or deactivate various features for your Enterprise. Some of these features are SD-WAN specific, such as **Edge Licensing** and **Edge Auto-Activation**. Others are common to all Orchestrator services, such as **Alerts & Notifications** and **Privacy Settings**.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > Customer Capabilities	<p>Enterprise &gt; Global Settings &gt; Customer Configuration &gt; Additional Configuration &gt; Global</p> <p>The following <b>Customer Capabilities</b> are removed from the New Orchestrator:</p> <ul style="list-style-type: none"> <li>■ Enable Advanced Threat Protection</li> <li>■ Enable Legacy Networks</li> <li>■ Enable Segmentation</li> <li>■ Enable Secure Service Secrets</li> </ul> <p>The following Customer Capabilities are <b>added</b> to the New Orchestrator</p> <ul style="list-style-type: none"> <li>■ Enable Classic Orchestrator UI</li> <li>■ Customizable QoE</li> <li>■ In-product Contextual Help Panel</li> <li>■ Route Backtracking</li> </ul> <p>The following Customer Capabilities are <b>moved</b> to Enterprise &gt; Global Settings &gt; Customer Configuration &gt; Additional Configuration &gt; SD-WAN Settings</p> <ul style="list-style-type: none"> <li>■ Enable Stateful Firewall</li> <li>■ Enhanced Firewall Services</li> </ul>

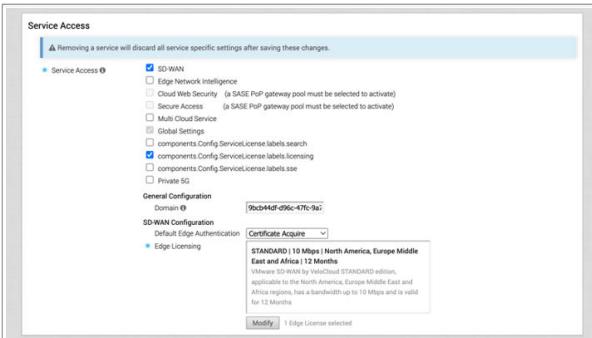
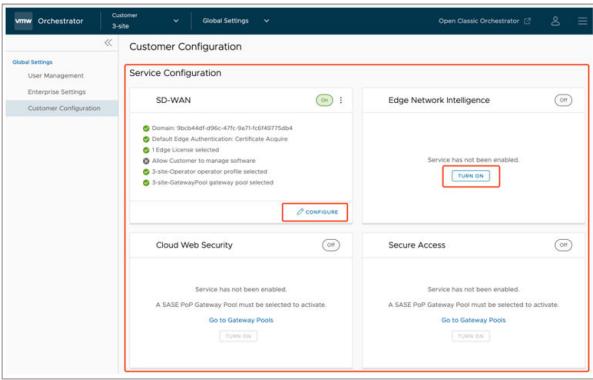
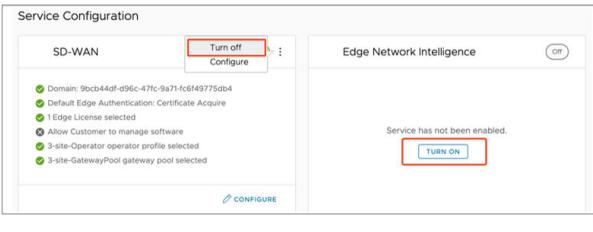
## Customer Configuration > Security Policy

We have moved **Security Policy** to the **Global Settings** tab because these settings affect the Enterprise Orchestrator as a whole and not just SD-WAN.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > Security Policy	Enterprise > Global Settings > Customer Configuration > Additional Configuration > Security Policy
	

## Customer Configuration > Service Access

We have moved the **Service Access** feature from the **System Settings** tab to the **Global Settings** page. This is because the **Service Access** feature affects the whole Enterprise Orchestrator, not just SD-WAN. The **Service Access** feature allows you to manage the additional services that you can purchase, enable, and configure for your Enterprise. You can find these services under the **Customer Configuration** section in the **Global Settings** page. Each service is displayed as a **Service Configuration** card that shows its name, description, status, and settings. You can turn on or off each service and complete high-level configuration of each service from the card.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > Service Access	Enterprise > Global Settings > Customer Configuration > Service Configuration
	
	

## Customer Configuration > Gateway Pool

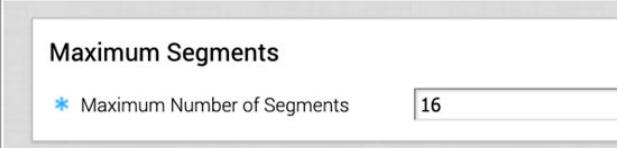
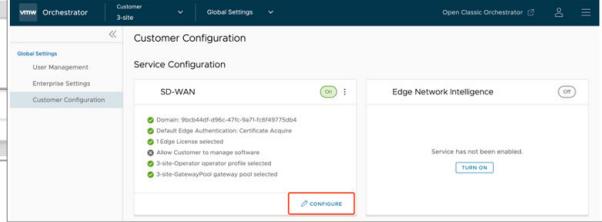
We have moved **Gateway Pool** to the **Global Settings** tab because these settings affect the Enterprise Orchestrator as a whole and not just SD-WAN.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > Gateway Pool	Enterprise > Global Settings > Customer Configuration > Gateway Pool

The screenshot shows two side-by-side interface views. The left view is from the 'Classic Orchestrator' and displays a 'Gateway Pool' configuration with two entries: 'gateway-1' (IP 20.0.1.2, MAC fd00:ff01:0:1::2) and 'gateway-2' (IP 20.0.2.2, MAC fd00:ff02:0:1::2). The right view is from the 'New Orchestrator' under 'Global Settings > Customer Configuration > Gateway Pool'. It shows a similar list of gateways and includes additional configuration options like 'Partner Hand Off' (set to 'On'), 'Configure Hand Off' (set to 'All Gateways'), and 'Customer BGP Priority'.

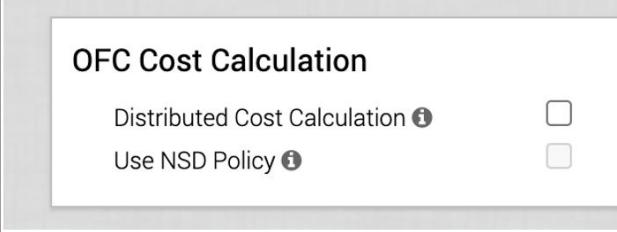
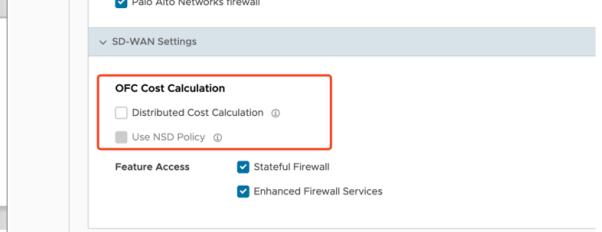
## Customer Configuration > Maximum Segments

We have relocated the **Maximum Segments** feature from the **Configure** tab to the **SD-WAN** service card in the **Global Settings** page. This is because the **Maximum Segments** feature is a high-level service configuration that applies to the whole Enterprise Orchestrator. The service configuration cards are where you can find the required configurations to enable each service. You can access the SD-WAN service card from the **Customer Configuration** section in the **Global Settings** page.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > Maximum Segments	Enterprise > Global Settings > Customer Configuration > Service Configuration > SD-WAN > Configure
	

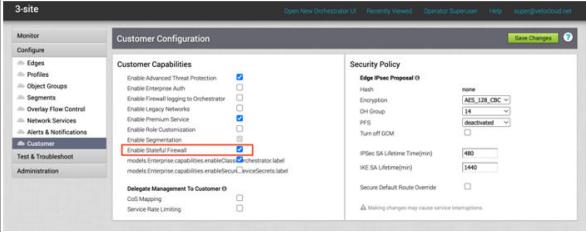
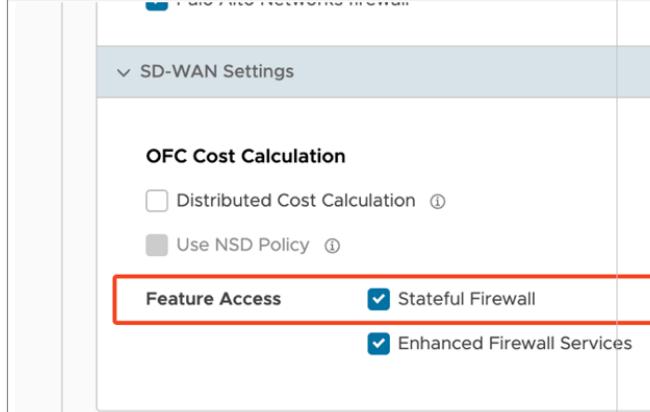
## Customer Configuration > OFC Cost Calculation

We have moved **OFC Cost Calculation** to the **Global Settings** tab because this is a high-level SD-WAN configuration.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > OFC Cost Calculation	Enterprise > Global Settings > Customer Configuration > SD-WAN Settings > OFC Cost Calculation
	

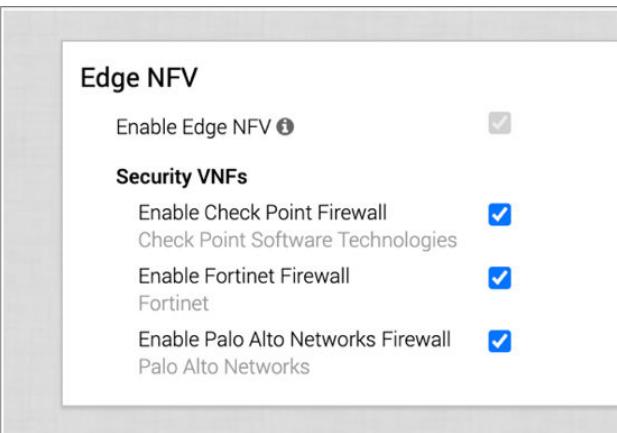
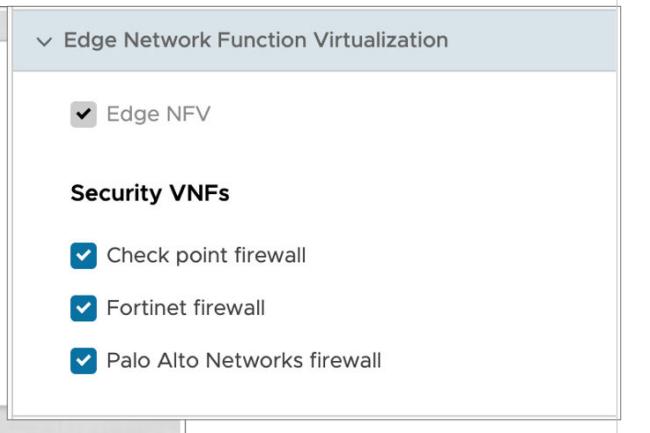
## Customer Configuration > Enable Stateful Firewall

We have moved **Enable Stateful Firewall** to the **Global Settings** tab because this is a high-level SD-WAN configuration.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > Customer Capabilities > Enable Stateful Firewall	Enterprise > Global Settings > Customer Configuration > SD-WAN Settings > Feature Access > Stateful Firewall
	

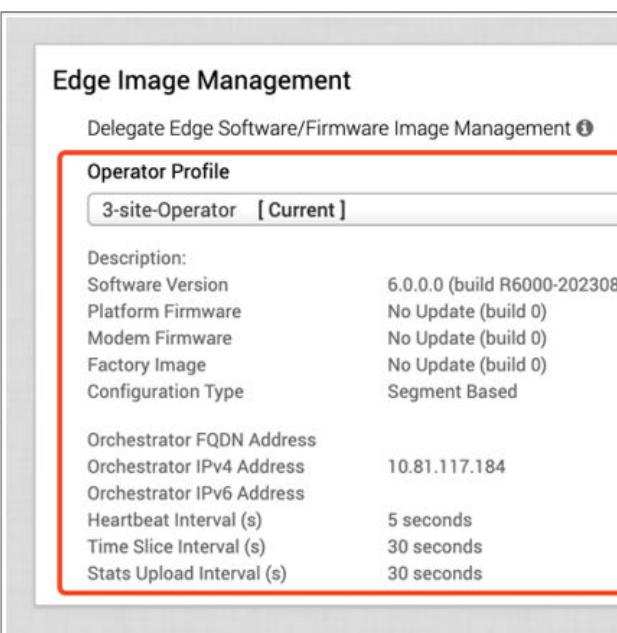
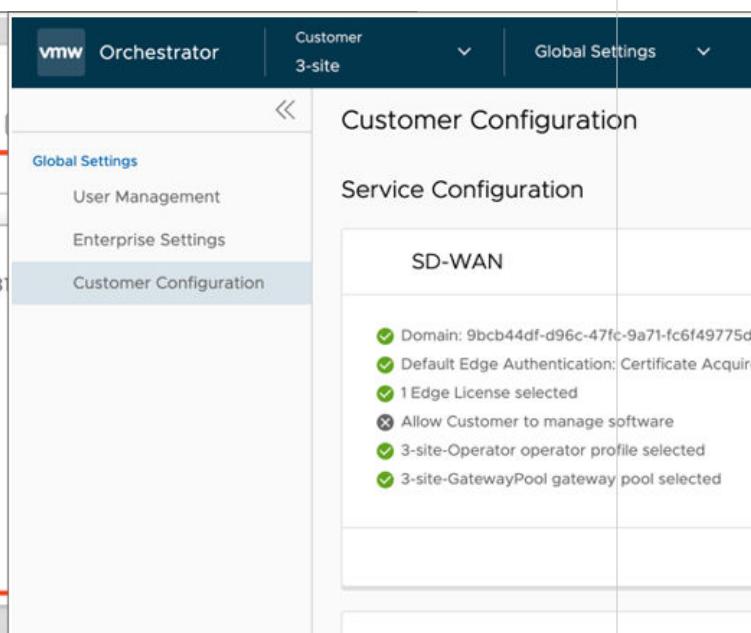
## Customer Configuration > Edge NFV ( Network Function Virtualization)

We have moved **Edge NFV** to the **Global Settings** tab because these settings affect the Enterprise Orchestrator as a whole and not just SD-WAN.

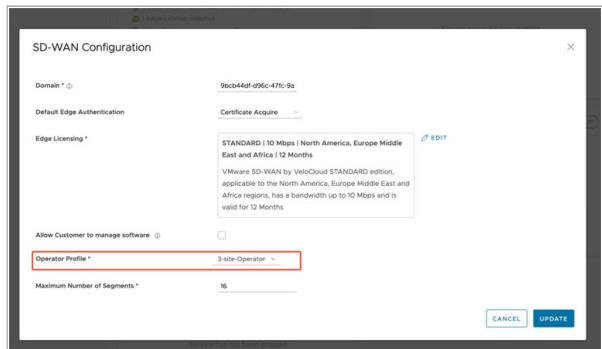
Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > Edge NFV	Enterprise > Global Settings > Customer Configuration > Edge Network Function Virtualization
	

# Customer Configuration > Edge Image Management > Operator Profile

We have moved the **Operator Profile** feature to the **SD-WAN** service card in the **Global Settings** page. This is because the Operator Profile feature is a high-level service configuration that applies to the whole Enterprise Orchestrator. The **Service Configuration** cards are where you can find the required configurations to enable each service.

Classic Orchestrator Location	New Orchestrator Location																												
Enterprise > Configure > Customer > Customer Configuration > Edge Image Management > Operator Profile	Enterprise > Global Settings > Customer Configuration > SD-WAN > Configure > Operator Profile																												
 <p>The screenshot shows the 'Edge Image Management' interface. A red box highlights the 'Operator Profile' section, which contains a table with the following data:</p> <table border="1"> <thead> <tr> <th colspan="2">Operator Profile</th> </tr> </thead> <tbody> <tr> <td>3-site-Operator</td> <td>[ Current ]</td> </tr> <tr> <td>Description:</td> <td></td> </tr> <tr> <td>Software Version</td> <td>6.0.0.0 (build R6000-202308)</td> </tr> <tr> <td>Platform Firmware</td> <td>No Update (build 0)</td> </tr> <tr> <td>Modem Firmware</td> <td>No Update (build 0)</td> </tr> <tr> <td>Factory Image</td> <td>No Update (build 0)</td> </tr> <tr> <td>Configuration Type</td> <td>Segment Based</td> </tr> <tr> <td>Orchestrator FQDN Address</td> <td></td> </tr> <tr> <td>Orchestrator IPv4 Address</td> <td>10.81.117.184</td> </tr> <tr> <td>Orchestrator IPv6 Address</td> <td></td> </tr> <tr> <td>Heartbeat Interval (s)</td> <td>5 seconds</td> </tr> <tr> <td>Time Slice Interval (s)</td> <td>30 seconds</td> </tr> <tr> <td>Stats Upload Interval (s)</td> <td>30 seconds</td> </tr> </tbody> </table>	Operator Profile		3-site-Operator	[ Current ]	Description:		Software Version	6.0.0.0 (build R6000-202308)	Platform Firmware	No Update (build 0)	Modem Firmware	No Update (build 0)	Factory Image	No Update (build 0)	Configuration Type	Segment Based	Orchestrator FQDN Address		Orchestrator IPv4 Address	10.81.117.184	Orchestrator IPv6 Address		Heartbeat Interval (s)	5 seconds	Time Slice Interval (s)	30 seconds	Stats Upload Interval (s)	30 seconds	 <p>The screenshot shows the 'Customer Configuration' interface. The 'SD-WAN' service card is selected. A red box highlights the 'Operator Profile' dropdown, which is set to '3-site-Operator'. The configuration pane on the right lists several checked options:</p> <ul style="list-style-type: none"> <li>Domain: 9bcb44df-d96c-47fc-9a71-fc6f49775db4</li> <li>Default Edge Authentication: Certificate Acquire</li> <li>1 Edge License selected</li> <li>Allow Customer to manage software</li> <li>3-site-Operator operator profile selected</li> <li>3-site-GatewayPool gateway pool selected</li> </ul>
Operator Profile																													
3-site-Operator	[ Current ]																												
Description:																													
Software Version	6.0.0.0 (build R6000-202308)																												
Platform Firmware	No Update (build 0)																												
Modem Firmware	No Update (build 0)																												
Factory Image	No Update (build 0)																												
Configuration Type	Segment Based																												
Orchestrator FQDN Address																													
Orchestrator IPv4 Address	10.81.117.184																												
Orchestrator IPv6 Address																													
Heartbeat Interval (s)	5 seconds																												
Time Slice Interval (s)	30 seconds																												
Stats Upload Interval (s)	30 seconds																												



The screenshot shows the 'SD-WAN Configuration' dialog box. A red box highlights the 'Operator Profile' dropdown, which is set to '3-site-Operator'. Other fields include 'Domain' (9bcb44df-d96c-47fc-9a71-fc6f49775db4), 'Default Edge Authentication' (Certificate Acquire), 'Edge Licensing' (STANDARD | 10 Mbps | North America, Europe Middle East and Africa | 12 Months), 'Allow Customer to manage software' (unchecked), and 'Maximum Number of Segments' (16).

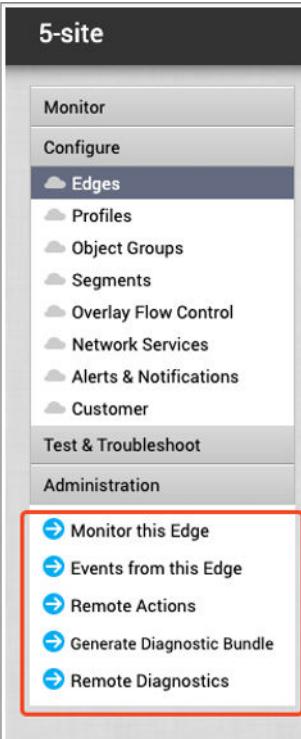
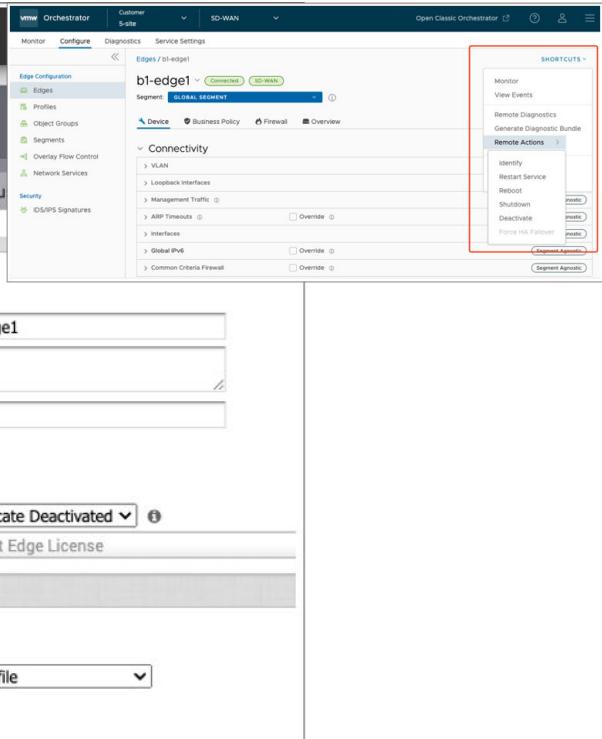
## Customer Configuration > Edge Image Management > Delegate Edge Software/Firmware Image Management

We have changed the name of the **Delegate Edge Software/Firmware Image Management** feature to **Allow Customer to Manage Software**. We have also moved this feature to the **SD-WAN** service configuration card in the **Global Settings** page. This is because the feature is a high-level service configuration that applies to the whole Enterprise Orchestrator. The service cards are where you can find the required configurations to enable each service.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Customer > Customer Configuration > Edge Image Management > Delegate Edge Software/Firmware Image Management	Enterprise > Global Settings > Customer Configuration > SD-WAN > Configure > Allow Customer to Manage Software

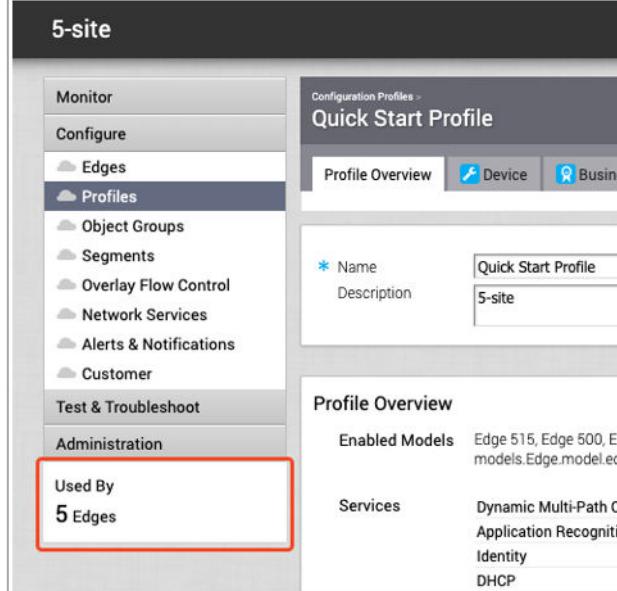
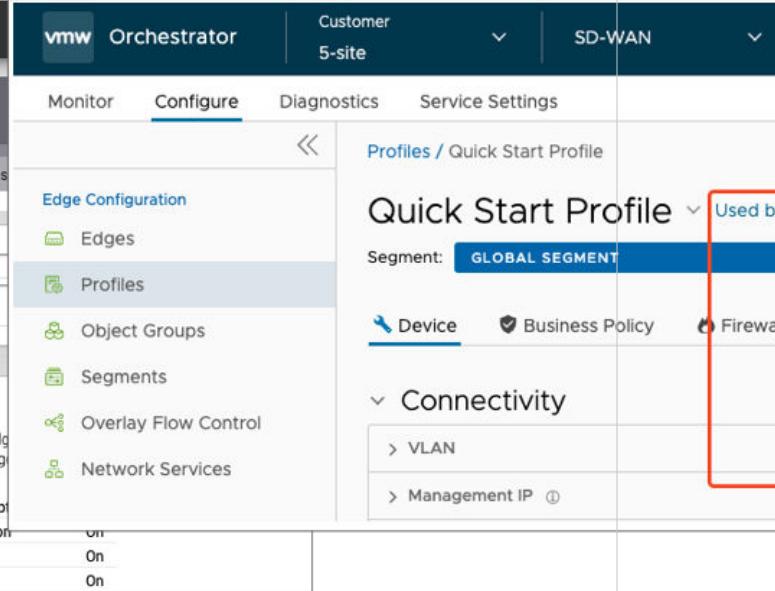
## Edge Shortcuts

We have improved the way you access the feature shortcuts in the New Orchestrator UI. You no longer need to look for them in the navigation menu, which was not very convenient. You can find the shortcuts in the upper right corner of the screen, next to the content of the page. This makes it easier to use the shortcuts that are relevant to the page you are viewing.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Edges > Select an Edge > Feature Shortcut appear at the bottom of the left-side navigation pane	Enterprise > SD-WAN > Configure > Edges > Select an Edge > Shortcuts drop-down menu appears at top right corner of each Edge page
	

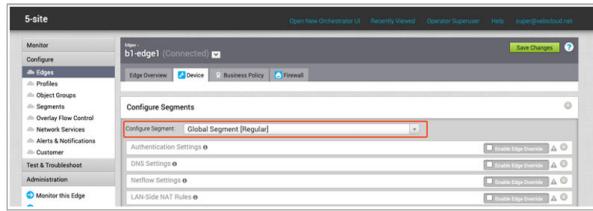
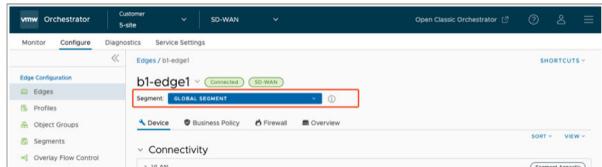
## Profile Used By

We have changed the location of the Profile information in the New Orchestrator UI. You no longer need to look for it in the navigation menu, which was not very convenient. You can find the Profile information next to the title of the Profile, on the same page. This makes it easier to see which Edges and Business Policies are using the Profile.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Profiles > Select a Profile > Profile information appears at the bottom of Left side navigation pane	Enterprise > SD-WAN > > Configure > Profiles > Select a Profile > Profile information is moved to the right of the Profile Name
	

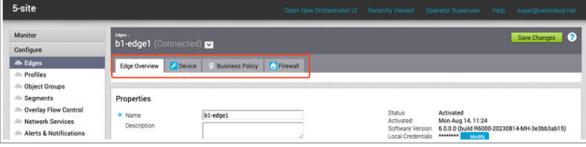
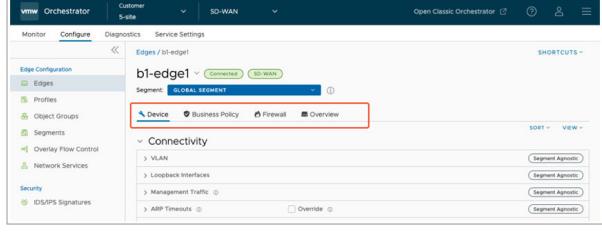
## Segment Selector

We have moved the **Segment Selector** to the top of the page in the New Orchestrator UI. This is to make it consistent with the Edge/Profiles tabs, so you can switch between them without changing the selected segment. Most of the **Device** settings depend on the segment, so having the **Segment Selector** at the top of the page is more efficient. The **Segment Selector** stays fixed as you scroll down the page, so you can easily see and change it.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Edge/Profile > Below Edge/Profile tabs > (Overview, Device, Business Policy, Firewall)	Enterprise > SD-WAN > > Configure > Edge/Profile > Above Edge/Profile tabs (Device, Business Policy, Firewall, Overview)
	

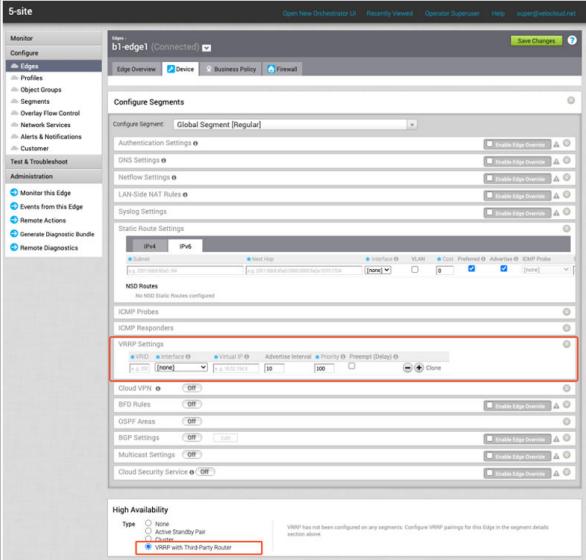
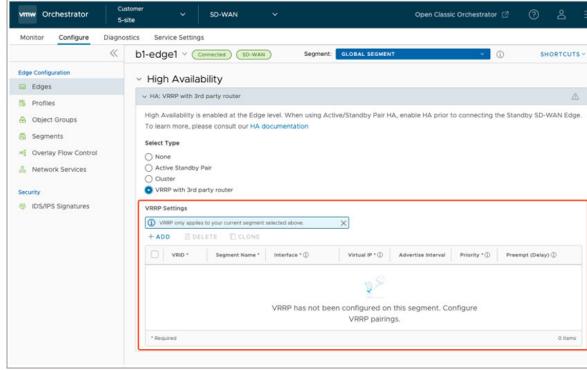
## Edge/Profile Configuration Tab Order (Overview, Device, Business Policy, and Firewall)

We have changed the default tab that appears when you click on the Edge name in the New Orchestrator UI. It is now the **Device** tab, instead of the **Overview** tab. This is because most users want to see the **Device** settings first, such as Device Name, Model, Serial Number, and Firmware Version. If you want to see the **Overview** tab, you can still access it from the navigation menu. The **Overview** tab shows you the Edge status, statistics, and events. Please note that after you provision an Edge, you will automatically see the **Overview** tab first.

Classic Orchestrator Location	New Orchestrator Location
Enterprise > Configure > Edge/Profile > The Overview tab is first	Enterprise > SD-WAN > Configure > Edge/Profile > The Device tab is now the first tab The new tab order is: <b>Device, Business Policy, Firewall, and Overview</b> .
	

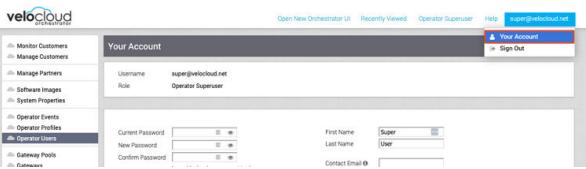
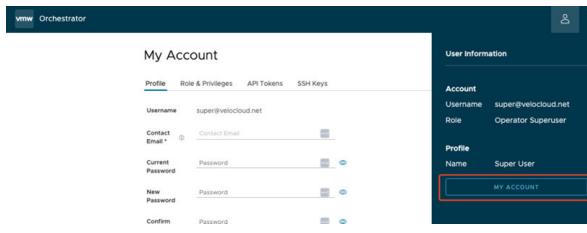
## VRRP Settings

We have relocated the **VRRP Settings** data grid from the **Device** tab to the **High Availability** section in the New Orchestrator UI. This is to make it easier for you to select and configure the VRRP options for your Edges. This change was made based on the feedback from our users, who wanted the VRRP data grid to be more visible and in context with the VRRP HA selection.

Classic Orchestrator Location	New Orchestrator Location
<p><b>Enterprise &gt; Configure &gt; Edge/Profile &gt; VRRP Settings &gt;</b>  <b>Located in its own section within Device Settings</b></p> 	<p><b>Enterprise &gt; SD-WAN &gt; Configure &gt; Edge/Profile &gt; High Availability</b></p> <p><b>VRRP Settings</b> is now under <b>High Availability</b>. If the VRRP option is selected as the HA option, then the VRRP data grid appears in the <b>High Availability</b> section.</p> 

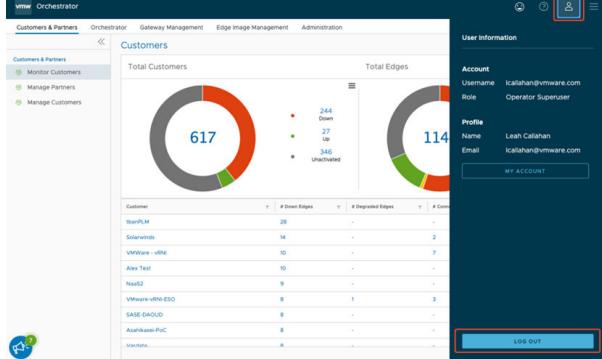
## My Account

This change is made to be consistent with the navigation of other VMware applications. All user account information is stored under the 'User' icon in the header navigation.

Classic Orchestrator Location	New Orchestrator Location
<p><b>Header Navigation &gt; User Email address &gt; Your Account</b></p> 	<p><b>Header Navigation &gt; User Icon &gt; My Account</b></p> 

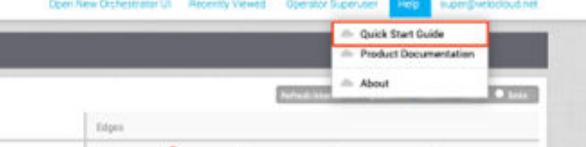
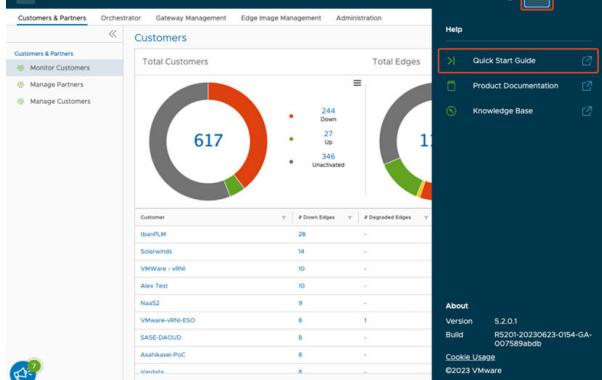
## Logout

This change is made to be consistent with the navigation of other VMware applications. All user account information is stored under the 'User' icon in the header navigation.

Classic Orchestrator Location	New Orchestrator Location
Header Navigation > User Email address > Sign Out	Header Navigation > User Icon > Log Out
	

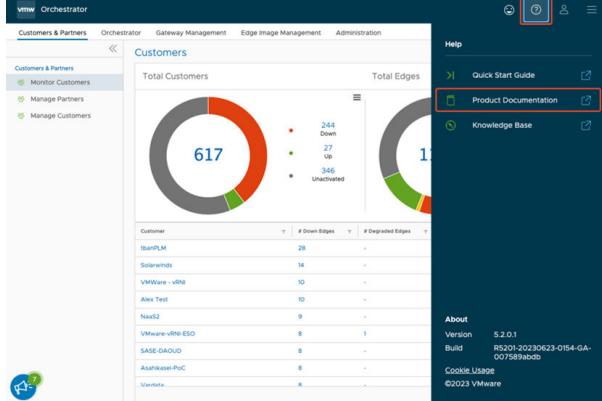
## Quick Start Guide

This change is made to be consistent with the navigation of other VMware applications. All help resources can be found under the 'Question Mark' icon in the header navigation.

Classic Orchestrator Location	New Orchestrator Location
Header Navigation > Help > Quick Start Guide	Header Navigation > Question Mark Icon > Quick Start Guide
	

## Product Documentation

This change was made to be consistent with the navigation of other VMware applications. All help resources can be found under the 'Question Mark' icon in the header navigation.

Classic Orchestrator Location	New Orchestrator Location
Header Navigation > Help > Product Documentation	Header Navigation > Question Mark Icon > Product Documentation
	

## New Features that do not exist in the Classic Orchestrator

### Enterprise > SD-WAN > Service Settings

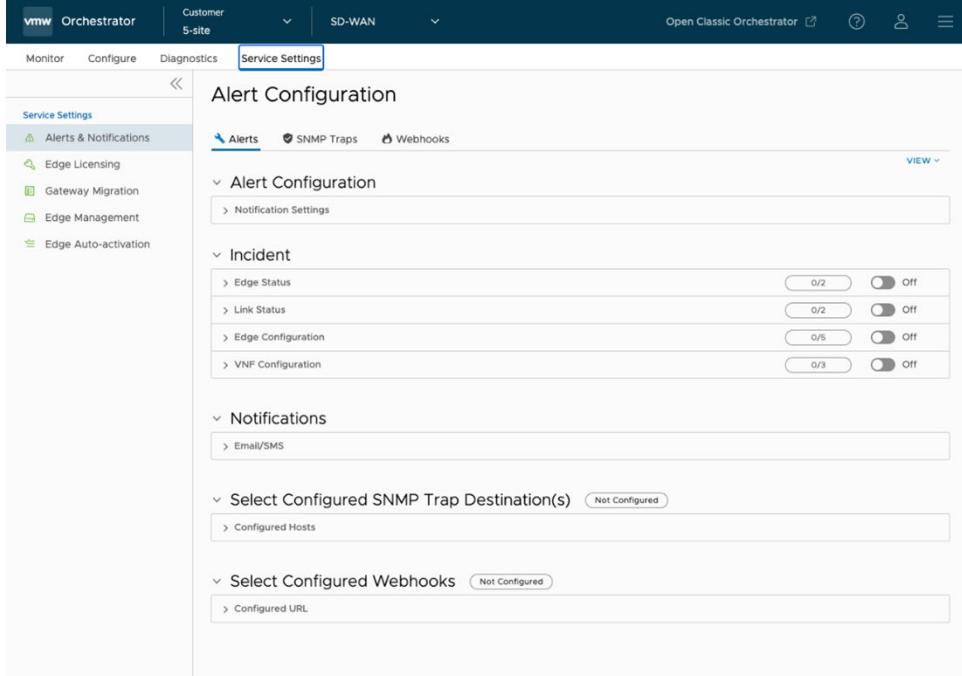
**Service Settings** is a new menu within **SD-WAN** that includes SD-WAN Orchestrator specific configurations. This provides us with a set of configurations that are separated from the SD-WAN Network configurations.

**New Orchestrator Location**

**Enterprise > SD-WAN > Service Settings**

The following are the settings that are in this section:

- **Alerts & Notifications**
- **Edge Licensing**
- **Gateway Migration**
- **Edge Management**
- **Edge Auto-activation**



## Enterprise > Global Settings

**Global Settings** is a new section that allows global Orchestrator configurations and settings that span across more than one (or all) services.

### New Orchestrator Location

**Enterprise > Global Settings**

The following are the settings that are in this section:

- **User Management > Users**
- **User Management > Roles**
- **User Management > Service Permissions (Operator Only)**
- **User Management > Authentication**
- **Enterprise Settings**
- **Customer Configuration**

Username	Name	Role	Created	Authentication	Activation State	Locked	Last Login Date Time
5_site_operator@velocloud.net	Superuser	Aug 14, 2023, 11:19:55 AM	Local	Active	Unlocked		

## Gateway Migration

**Gateway Migration** is relocated because it contains quiesced Gateways that are used by the current Enterprise and are needed for migration. Users must perform the migration per Enterprise because this feature is not available for Partner Gateways yet.

**New Orchestrator Location**

Enterprise > SD-WAN > Service Settings > Gateway Migration

## Cloud Hub

**Cloud Hub** is a new section added to the **SD-WAN** Configuration, that is separated from SD-WAN Edge and Profile Configuration.

**New Orchestrator Location**

Enterprise > SD-WAN > Configure > Cloud Hub

## Profile Shortcuts

The new **Shortcuts** drop-down menu located in the top right corner of each Profile page allows the user to efficiently choose the actions to perform.

**New Orchestrator Location**

Enterprise > SD-WAN > Configure > Profile

## Pendo Opt Out/In

Clicking the "Cookie Usage" link allows the users to either opt out or opt into the Pendo analytics tracking tool.

**New Orchestrator Location**

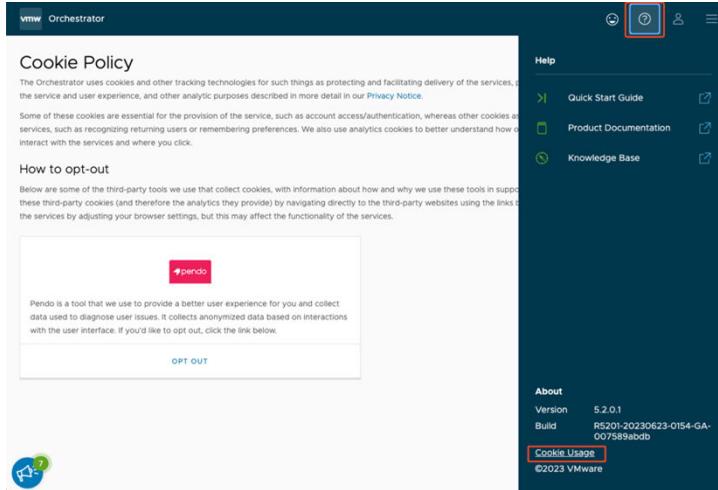
Header Navigation > Question Mark Icon > Cookie Usage Link > Opt Out or Opt In. This opens Cookie Policy page.

## Cookie Usage

All help resources can be found under the 'Question Mark' icon in the header navigation. This option is located here to be consistent with the navigation of other VMware applications.

## New Orchestrator Location

Header Navigation > Question Mark Icon > Cookie Usage Link > Opt Out or Opt In. This opens Cookie Policy page.

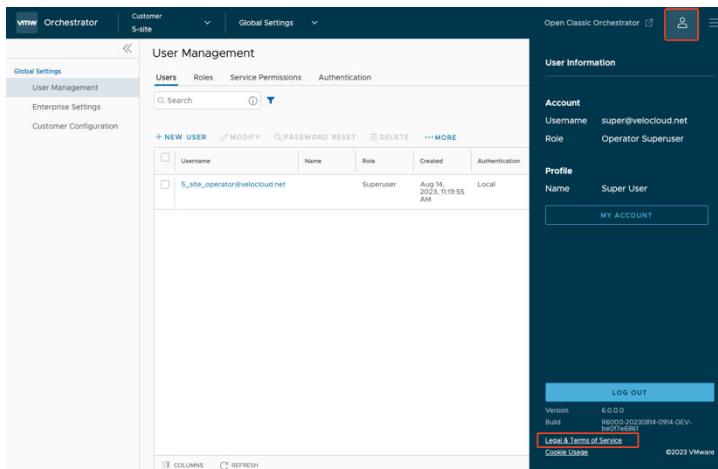


## Legal & Terms of Service

All information related to the user account is stored under the 'User' icon in the header navigation. This option is located here to be consistent with the navigation of other VMware applications.

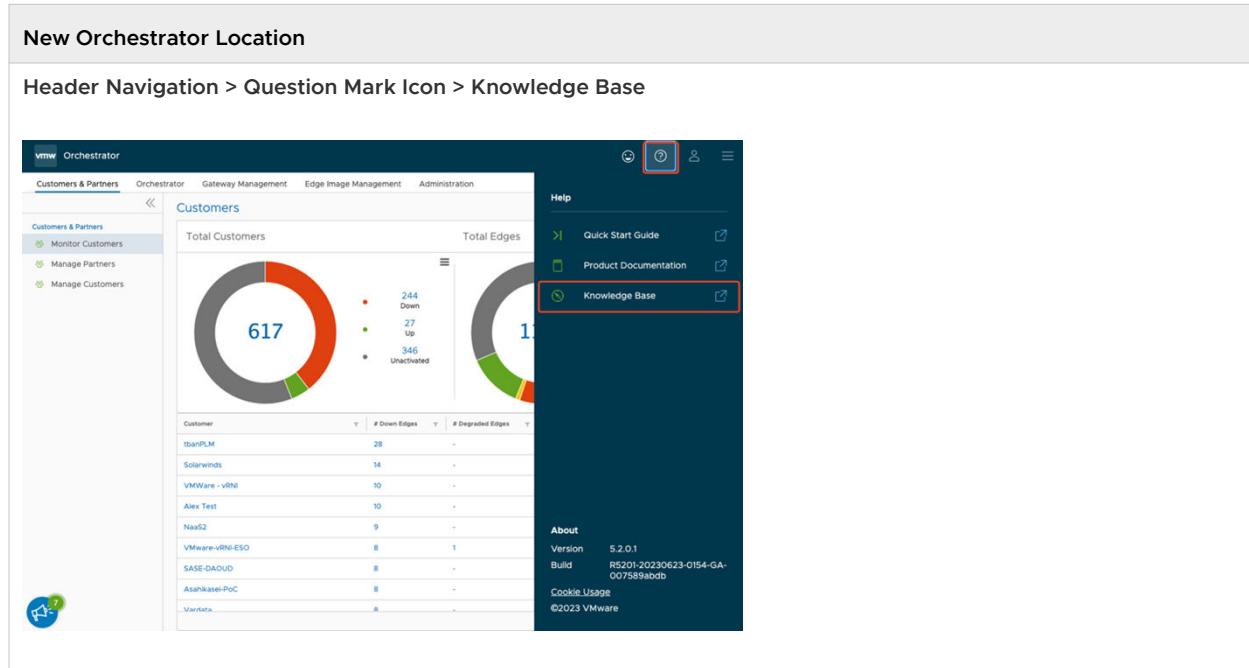
## New Orchestrator Location

Header Navigation > User Icon > Legal & Terms of Service Link > Opt Out or Opt In. This opens VMware site in a new tab.



# Knowledge Base

All help resources can be found under the 'Question Mark' icon in the header navigation. This option is located here to be consistent with the navigation of other VMware applications.



The screenshot shows the VMware Orchestrator web interface. In the top right corner, there is a 'Help' button with a question mark icon, which is highlighted with a red box. Below it, the 'Help' menu is open, and the 'Knowledge Base' option is also highlighted with a red box. The main dashboard displays various metrics and a table of customer edge connections.

## SD-WAN > Configure > Edges > Firewall > Syslog Forwarding > View Syslogs

This option is now a read only output of configured syslog within the **Firewall > Syslog Forwarding** section. This allows users to view the configured syslog settings without navigating to the **Device** tab.

**New Orchestrator Location**

Enterprise > SD-WAN > Configure > Edges > Firewall > Syslog Forwarding > View Syslogs

Configure Firewall

IP	Protocol	Port	Source Interface	Roles	Syslog Level	Tag	All Segments
1.1.1.1	TCP	514	Auto	Edge Event	Error	-	<input checked="" type="checkbox"/> Enabled

1 item

## SD-WAN > Configure > Edges > Firewall > New Rule > Read only views of selected Address Group and Service Group

This option is now a read only output of configured address groups and service groups within the **Firewall > New Firewall Rule** creation section. This allows the users to view the selected address groups and service groups configurations without navigating to the **Object Groups** section.

**New Orchestrator Location**

Enterprsie > SD-WAN > Configure > Edges > Firewall > New Rule > Select Source as Object Group > Add an Address Group and a Service Group > View the Address Group and Service Group information

Firewall / New Rule      Edge: b1-edge1      Segment: G1

### Rule-0

Duplicate Rule      Search for a previous rule...

Rule Name \*      Rule-0

Match

IP Version      IPv4 and IPv6

Source      Object Group

Address Group      test

Service Group

Destination      Any

Application      Any

Address Group

Name: test  
Description: This is my description

IP Addresses

IP Address	Prefix / Mask
1.1.1.1/32	Exact

Domains

Domains
vmware.com

Match

IP Version      IPv4 and IPv6

Source      Object Group

Address Group      test

Service Group      test-02

Destination      Any

Application      Any

Service Group

Name: test-02  
Description: my description

Service Ranges

Protocol	Ports	Type	Code
TCP	123		

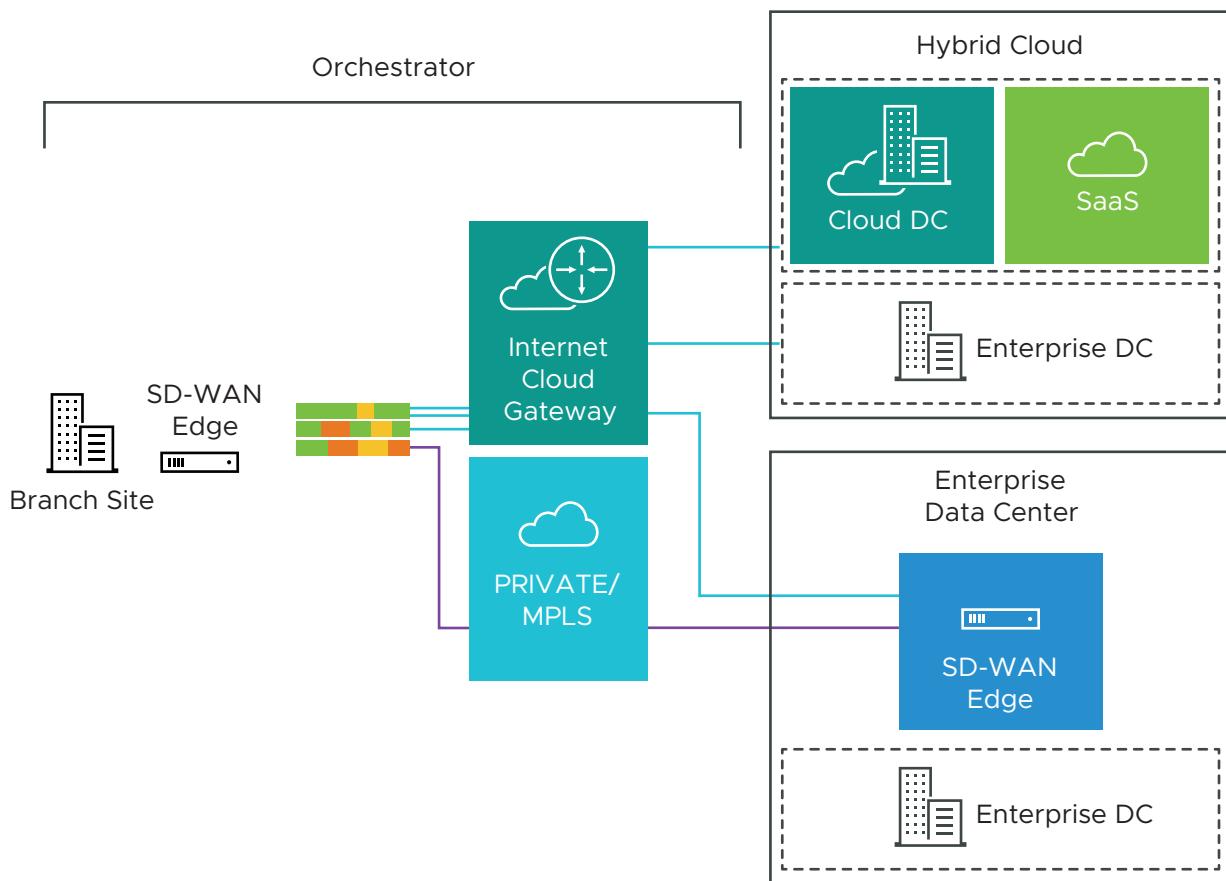
# Overview

4

VMware SD-WAN is a cloud network service solution enabling sites to quickly deploy Enterprise grade access to legacy and cloud applications over both private networks and Internet broadband.

Cloud-delivered Software-defined WAN assures enterprises the cloud application performance over Internet and hybrid WAN, while simplifying deployments and reducing costs.

The following figure shows the VMware SD-WAN solution components. The components are described in more detail in the following sections.



To become familiar with the basic configuration and Edge activation, see [Chapter 26 Activate SD-WAN Edges](#).

Read the following topics next:

- [VMware SD-WAN Routing Overview](#)
- [Dynamic Multipath Optimization \(DMPO\)](#)
- [Solution Components](#)
- [SD-WAN Edge Performance and Scale Data](#)
- [Capabilities](#)
- [Tunnel Overhead and MTU](#)
- [Network Topologies](#)
- [Branch Site Topologies](#)
- [Roles and Privilege Levels](#)
- [User Role Matrix](#)
- [Key Concepts](#)
- [Supported Browsers](#)
- [Supported Modems](#)

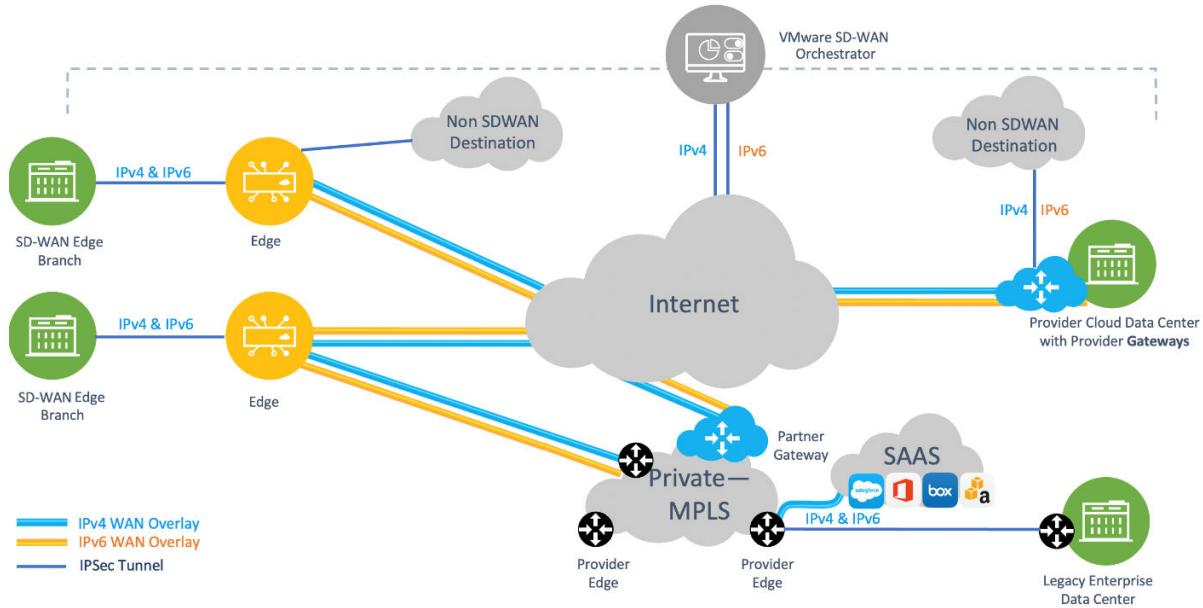
## VMware SD-WAN Routing Overview

This section provides an overview of VMware SASE routing functionality including route types, connected and static routes, and dynamic routes with tie-breaking scenarios and preference values in Overlay Flow Control (OFC) with Distributed Cost Calculation (DCC).

### Overview

VMware SASE routing is built on a proprietary protocol called **VCRP**, which is multi-path capable and secured through **VCMP** transport. The SD-WAN endpoints are connected using VCRP similar to iBGP full mesh. The SD-WAN Gateway acts as a BGP route reflector which reflects the routes from one SD-WAN Edge to another SD-WAN Edge within the customer enterprise based on the profile settings.

The following diagram illustrates a typical SD-WAN deployment with Multi-Cloud Non SD-WAN Destinations, where the Orchestrator performs the route calculation (as contrasted with the newer and preferred method using Dynamic Cost Calculation (DCC)).



## SD-WAN Components for Routing Purposes

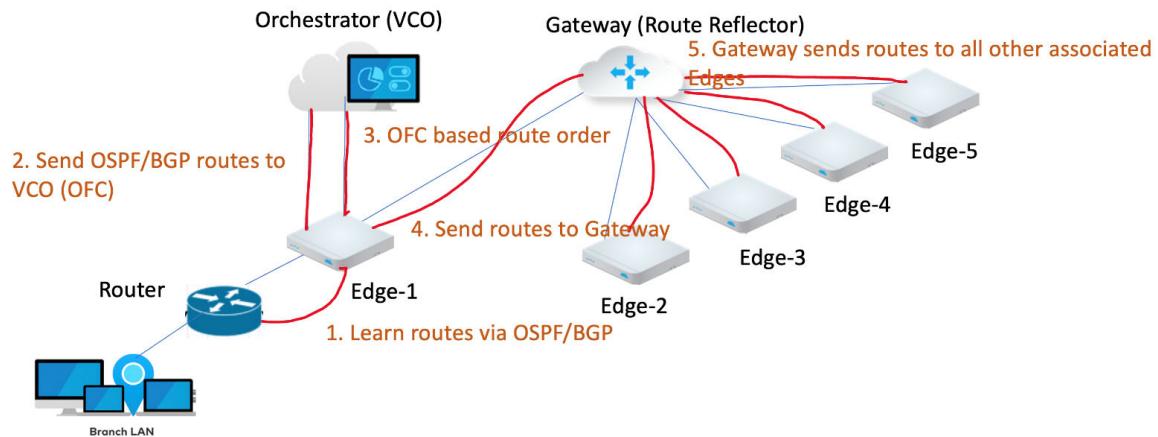
VMware SD-WAN routing uses three components: Edge, Gateway, and Orchestrator as described below.

- The **SD-WAN Edge** is an Enterprise-class device or virtualized cloud instance that provides secure and optimized connectivity to private, public and hybrid applications, and virtualized services. In SD-WAN routing, the Edge is a **Border Gateway**. An Edge can function as a regular Edge (with no Hub configuration), as a Hub by itself or as part of a cluster, or as a spoke (when Hubs are configured).
- The **SD-WAN Gateway** is autonomous, stateless, horizontally scalable, and cloud-delivered to which Edges from multiple tenants can connect. For any SD-WAN deployment, several SD-WAN Gateways are deployed as a geographically distributed (for lower latency) and horizontally scalable (for capacity) network with each Gateway acting as a **Route Reflector** for their connected Edges.

All routes that are locally learned on an Edge are sent to the Gateway based on the configuration. The Gateway then reflects these routes to other Edges in the enterprise, allowing for efficient full mesh VPN connectivity without building a full mesh of tunnels.

- The **SASE Orchestrator** is a multi-tenant cloud-based configuration and monitoring portal. In SD-WAN routing, the Orchestrator manages routes for all enterprises and can override default routing behavior.

See the image below for an illustration of the VMware SD-WAN components for routing purposes.



## Route Types

There are two general types of routes for SD-WAN:

- **Local Routes:** Any route that is learned locally on a SD-WAN Edge. This can either be a connected subnet, statically configured route, or any route that is learned via BGP or OSPF.
- **Remote Routes:** Any route that is learned from VCRP, in other words, a route that is not locally present on an Edge is a remote route. This route originated from a different Edge and is reflected by the Gateway to other Edges in the customer enterprise based on the configuration.

SD-WAN uses a strict order to route traffic for non-dynamic routes (BGP and OSPF) that cannot be altered. However, in some scenarios, you can use the **Longest Prefix Match** technique to manipulate how the routing flows.

### Route Ordering in an Edge:

- 1 Longest prefix length.
- 2 Local connected.
- 3 Local static if preferred option enabled (LAN static < WAN static).
  - If preferred option is not enabled, overlay routes would be preferred.
- 4 NSD static routes local.
  - NSD IPsec wins over NSD GRE.
- 5 Remote NSD static.
- 6 Remote Edge connected.
- 7 Remote Edge LAN/WAN static.
- 8 PG static.
  - PG secure static > PG non-secure static.

- 9 Dynamic routes (Overlay Flow Control (OFC) or Distributed Cost Calculation Driven route order).
  - Site Local (OSPF Inter/Intra, BGP non-uplink) is preferred than overly dynamic routes.
  - Local OSPF inter/intra area routes wins over Local BGP.
  - Local BGP wins over Local OSPF-external (OE1/OE2).
  - Remote routes with preferred cost wins over non-preferred local route (OE1,OE2,UPLINK BGP).
  - Within the remote dynamic routes preference is considered(lower preference wins).
  - If preference is same, BGP attributes and OSPF metrics are compared).
    - OSPF INTRA> INTER > OE1 > OE2
    - BGP
      - a Higher Local preference
      - b Lower AS\_PATH Length
      - c Smaller BGP metric
  - For more details on preference calculation, please refer to the DCC section.

## Connected and Static Routes

This section includes essential information regarding connected and static routes. A connected route is a route configured to a network that is directly attached to the interface. A static route is useful for special cases in which static routes are needed for existing network attached devices, such as printers. More information about static routes can be found at [Configure Static Route Settings](#).

### Connected Routes

- For a connected route to be visible in SD-WAN, configure the following settings on the Orchestrator:
  - **Cloud VPN** must be activated.
  - The connected route must be configured with a valid IP address.
  - The Edge interface for this route must be up at Layer 1, and functional at Layers 2 and 3.
  - VLANs associated with this Edge interface must also be up.
  - The **Advertise** flag must be set on the Edge interface under **Interface IP settings** for the configured connected route.

### Static Routes

- For a static route to be visible in SD-WAN, configure the following settings on the Orchestrator:
  - **Cloud VPN** must be activated.

- The static route configuration must have **Advertised** checked.
- Static routes can forward the traffic to the WAN underlay or LAN.
- Adding a static route bypasses the NAT on the Edge interface.
- ECMP (Equal-cost multi-path routing) with a static route is not supported, and only the first static route would be used.
- Use an ICMP Probe to avoid blackholing traffic in case of failure in next hop.

- A static route with the **Preferred** flag checked is preferred over any VPN route learned over the Overlay.

---

**Note** The difference between the **Preferred** flag, and the **Advertise** flag:

When the **Preferred** check box is selected, the static route will always be matched first, even if a VPN route with a lower cost is available.

Not selecting this option means that any available VPN route is matched over the static route, even when the VPN route has a higher cost than the static route. The static route is matched only when corresponding VPN routes are not available.

When the **Advertise** check box is selected, the static route is advertised over VPN and other SD-WAN Edges in the network will have access to the resource. This also enables static route redistribution into a routing protocol like local BGP/OSPF.

Do not select this option when a private resource like a remote worker's personal printer is configured as a static route and other users should be prevented from accessing the resource.

The OFC **Global Advertise Flags** control which routes are added to the overlay. By default, the following route types are not advertised into the overlay: External OSPF and Non SD-WAN Destination iBGP. In addition, if an Edge is acting as both Hub and Branch, the **Global Advertise Flags** configured for the Branch will be used, not the Hub.

---

**Note** There are two additional route types: **Self Routes** and **Cloud Routes**, which are installed on an Edge (depending on the Edge's configuration). Each route has a narrow application outlined below, which requires no additional treatment beyond their mention here:

A **Self Route** refers to an interface-based prefix using IP Longest prefix match (LPM) (for example: 172.16.1.10/32) which is installed locally on the Edge but is not advertised to remote Edges. Another term for Self Routes is "Interface Routes." In the Edge logs, self routes are displayed as route flag "s."

A self route differs from a connected route, as a connected route can be advertised into the overlay so that the remote Edge clients can reach back to clients belonging to the connected route on the source Edge side. Self routes are strictly local to the Edge itself.

A **Cloud Route** is indicated with a "v" flag and refers to a route installed on an Edge pointing to Primary VMware SD-WAN Gateway for multi-path traffic destined for the Internet (in other words, Internet traffic using Dynamic Multi-Path Optimization (DMPO) which leverages a Gateway prior to reaching the Internet).

The Edge also uses a cloud route via a corresponding Gateway for management traffic destined for a VMware Orchestrator, which is hosted on the public cloud.

---

## Overlay Flow Control (OFC) with Distributed Cost Calculation (DCC)

This section explains how a route order using OFC with DCC works.

---

**Important** This material is valid only for customers who have **Distributed Cost Control (DCC)** activated. DCC was first made available in SD-WAN Release 3.4.0 and is now recommended to be activated for all customers. This feature will automatically be activated for new customers in an upcoming release. For more information about DCC including best practices, see [Configure Distributed Cost Calculation](#).

---

### Distributed Cost Calculation Overview

Distributed Cost Calculation (DCC) is a feature that leverages the SD-WAN Edges and Gateways for route preference calculation instead of relying on the SASE Orchestrator. The Edge and Gateway each insert the routes instantly upon learning them and then convey these preferences to the Orchestrator.

DCC resolves an issue seen in large scale deployments where relying solely on the Orchestrator can prevent timely route preference updates either because it could not be reached by an Edge or Gateway to receive updated routing preferences, or because the Orchestrator could not deliver route updates quickly when it is calculating a large number of them at one time. Distributing the responsibilities for route preference calculation to the Edges and Gateways ensures fast and reliable route updates.

### How Distributed Cost Calculation Preference is Done

Table 1-2 includes the types of dynamic routes supported in SD-WAN while table 1-3 is a glossary of route types. A dynamic route is first categorized by whether it is learned on the Edge or the Gateway.

**Table 4-1. Dynamic Route Types**

Edge	Partner Gateway / Hosted Gateway
NSD E BGP	NSD E/I BGP
NSD I BGP	E/I BGP
NSD Uplink BGP	
OSPF O	
OSPF IA	
E BGP	
I BGP	
OSPF OE1	
OSPF OE2	
Uplink BGP	

**Table 4-2. Route Type Meanings**

O = OSPF Intra area
IA = OSPF Inter area
OE1 = OSPF External Type-1
OE2 = OSPF External Type-2
E BGP = External BGP
I BGP = Internal BGP
NSD = Non SD-WAN Destination

**Note** Non SD-WAN Destination (NSD) support with OFC is available from Release 4.3.0 and forward. For more information on NSDs, see [Configure a Non SD-WAN Destination](#).

Each route type has a preference value (consider the preference as the cost in this document), and each learned route is assigned a preference value based on the route's type. The lower the preference value, the higher the priority. Table 1-3 lists the default preference value for each route type.

**Table 4-3. Preference Values**

Device	Route Type	Default Preference
Edge/Hub	NSD E BGP	997
Edge/Hub	NSD I BGP	998
Gateway	NSD E/I BGP	999
Edge/Hub	NSD Uplink BGP	1000
Edge/Hub	OSPF O	1001
Edge/Hub	OSPF IA	1002
Edge/Hub	E BGP	1003
Edge/Hub	I BGP	1004
Partner Gateway	E/I BGP	1005
Edge/Hub	OSPF OE1	1001006
Edge/Hub	OSPF OE2	1001007
Hub/Edge	BGP Uplink	1001008

The preference values displayed in the table above are based on the default priority order in the Overlay Flow Control configuration. The values will be adjusted accordingly if the default order is changed.

## Dynamic Route Workflow

- 1 The Edge or Gateway learns a dynamic route.
- 2 SD-WAN internally identifies what type of route it is and its default preference value.
- 3 SD-WAN assigns the correct preference value and installs the route in the routing information base (RIB) and forwarding information base (FIB).
- 4 SD-WAN considers the default advertising action configured for this route. Based on the advertising action, SD-WAN either advertises the route across the customer enterprise (advertised) or takes no action apart from adding the route locally into the RIB and FIB (not advertised).
- 5 SD-WAN then synchronizes this route to the Orchestrator which displays it on the Orchestrator.

## Preferred VPN Exit Points

This section covers **Preferred VPN Exit Points**: what they are, what routes can fall into which categories, and using route pinning to override default values.

In the **SD-WAN** service of the Enterprise portal, when navigating to **Configure > Overlay Flow Control**, you can see a section titled **Preferred VPN Exits**. This section displays default priorities and marks some route categories to be preferred over others.

The screenshot shows the VMware SD-WAN Administration Guide interface. The top navigation bar includes 'Monitor', 'Configure' (which is selected and highlighted in blue), 'Diagnostics', and 'Settings'. The left sidebar under 'Edge Configuration' has the following items: 'Edges', 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control' (selected and highlighted in blue), 'Network Services', and 'Alerts & Notifications'. The main content area is titled 'Overlay Flow Control' and 'IPv4'. It shows 'VRF Global Routing Preferences' with a sub-section 'Preferred VPN Exits'. Below this is a table titled 'Default Priority' with columns 'Order' and 'Header'. The table rows are: 1. NSD, 2. Edge, 3. Partner Gateway, 4. Router, and 5. Hub. At the bottom of the main content area is a button labeled 'Global Advertise Flags'.

The **Preferred VPN Exit** categories:

- **Edge:** Any **internal route** that can be learned either on a Hub or Spoke Edge falls under this category and is marked with the highest priority. An **internal route** cannot be an OSPF OE 1 / OE 2 or BGP Uplink type route.
- **Hub:** Any external Route that is learned on an Edge/Hub falls into the Hub category and typically has a lower priority. Hub routes include OSPF OE1/2 and BGP Uplink.
- **Partner Gateway:** Any route learned on a Partner Gateway.
- **Router:** A router represents any route prefix learned by an Edge with a BGP or OSPF and determines the preference that is assigned to a dynamic route. Typically, all exit points above the **Router** in the VPN Exit are assigned a low preference value (preferred cost) and are more preferred, while all exit points below the **Router** are assigned a higher preference value and are less preferred.
  - For example: When DCC is activated, all routes that belong to **VPN Exit Points** (Edge, Partner Gateway, or Hub) that are above **Router** get a preference value of less than 1,000,000, and the routes that are below **Router** get a preference value greater than 1,000,000.

- In the example below, the **VPN Exit Points** above **Router**, which are NSD, Edge, and Partner Gateway will get a preference value less than 1,000,000 and Hub will get a preference value greater than 1,000,000.

The screenshot shows the VMware SD-WAN Administration interface. The top navigation bar includes Monitor, Configure (selected), Diagnostics, and Settings. The left sidebar under 'Edge Configuration' has options: Edges, Profiles, Object Groups, Segments, Overlay Flow Control (selected and highlighted in grey), Network Services, and Alerts & Notifications. The main content area is titled 'Overlay Flow Control' for 'IPv4'. It shows 'VRF Global Routing Preferences' with 'Preferred VPN Exits' expanded. A table lists routes by order:

Order	Header
1.	NSD
2.	Edge
3.	Partner Gateway
4.	Router
5.	Hub

A green box highlights the 'Router' entry in the table. Below the table is a link to 'Global Advertise Flags'.

### Pinning a Route to Override a Default Preference Value

SD-WAN has a route pinning feature that allows a user to override the default preference value assigned to any dynamic route. Once a dynamic route is learned and synchronized with the Orchestrator, the user can navigate to the **Overlay Flow Control** page and override the default order for that route. The workflow for this is as follows:

- A user pins a route on the **Overlay Flow Control** page by either:
  - On the **Routes List**, select one or more routes and then click the **Pin Learned Route Preference** option.
  - Modifying the order of the **Preferred VPN Exits** by clicking **Edit** under the table.
- The Orchestrator sends this routing event to the relevant Edges in the customer enterprise.
- The Edges override the previous preference value to match the pinned order.

- 4 The preference values that get assigned to pinned routes start from 1, 2, 3, and so on (the lowest values and thus the highest preferences), and this matches the order of the routes on the **Overlay Flow Control** page.

**Note** For more information on pinning a route, consult [Configure Subnets](#).

## Tie-Breaking Scenarios for All Types of Routes

What happens when an Edge receives the same prefix for two or more sources/neighbors?

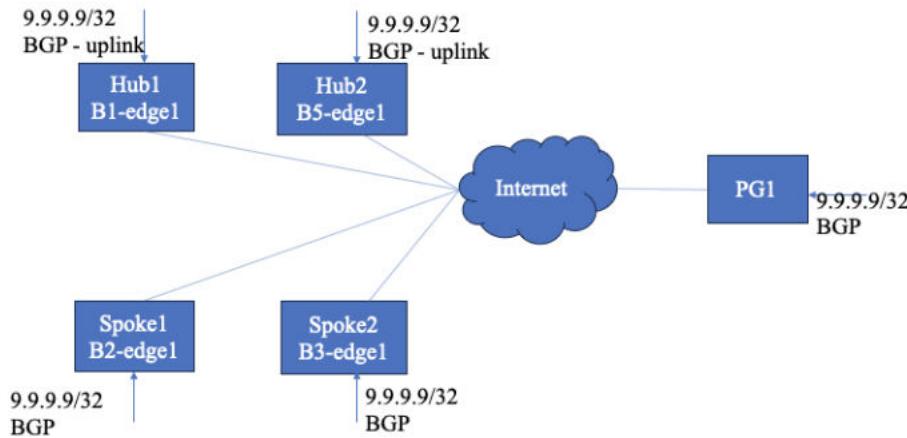
A potential scenario in SD-WAN deployments is for the same prefix to be advertised from two different Edges or Partner Gateways. With VMware SD-WAN, if the subnets are within the same category (Edge, Hub, or Partner Gateway) and have the same preference value, the BGP attributes or OSPF metrics are first considered for route sorting.

If there is still a tie, SD-WAN uses the **logical ID** (which is derived from the Edge or Gateway's **universally unique identifier (UUID)**) of the next hop device to break the tie. The next hop device can be a Gateway or a Hub Edge depending on the type of Branch to Branch VPN being used. If the customer enterprise is using Branch to Branch via Gateway, the next hop is a Gateway, while a customer using Branch to Hub would have the next hop be a Hub Edge.

There is a final tie-breaker if multiple Gateways advertise the same exact route type and preference. This final tie-breaker prefers the oldest route learned. To ensure the routing outcome you want, you can either pin certain routes or configure the BGP attributes and costs to favor some routes over others.

**Note** Customers do not have control over how a **logical ID** (LID) is generated and you cannot change its value. LID values are not directly comparable. Instead, they are compared using an internal software algorithm that breaks down a LID into four blocks and compares them one by one. For example, lid1-data1 is greater than lid1-data2, and lid1-data2 is greater than lid2-data2.

See the image below for an illustration of preference calculation and route sorting for dynamic routes.



Consider the above topology where the same route 9.9.9.9/32 is learned by two spokes.

- 1 Spoke1 and Spoke2 learn the route as BGP routes (non-uplink).
- 2 Hub1 and Hub2 learn the routes as uplink BGP routes.
- 3 PG1 also learns the same route.
- 4 Branch to branch via Hub1 and Hub2 is enabled in spoke profile.

#### **Route ordering in spokes with non-uplink routes:**

- 1 Since spoke1 and spoke2 learn the route as BGP, they pick the preferred cost value (the preference value is referred to as cost in this section) is 1003, as per the DCC preference mapping table.
- 2 Route 9.9.9.9/32 will be installed in FIB of Spoke1 and Spoke2 with a reference cost of 1000000. As always, the underlay route will be installed in FIB with a reference cost only. The derived cost/preference from the DCC preference table is for remote SD-WAN entities (Edges/Gateway) to use for route sorting.
- 3 Spoke1 and Spoke2 redistribute the route over VCRP with a derived cost of 1003 to the Gateway and remote Edges/Hubs. The below output image shows the derived cost/preference in spokes.

```
edge:b2-edge1:~# debug.py --bgp_view 9.9.9.9/32 0
Address      Netmask      Gateway      Nbr IP      Nbr ID      Metric      Type      Intf      Sync'd      Advertise      Inbound      Preference      LocalP      Aspl      Reachable      Ptr      Age      SEG      Communities
9.9.9.9      255.255.255.255  172.16.2.3  172.16.2.3  0.0.0.0      0          E          GE5        RCVD       true        learn       1003       100        4          yes        0x7fc83834efc0  175        0          186:6854
```

- 4 Similarly Hub1 and Hub2 learn the route and derive the non-preferred cost (1001008), since they learn the route as an uplink route. Hubs redistribute the route to Gateways and other Edges with this cost. The below output shows the derived cost/preference in Hubs.

```
edge:b1-edge1:~# debug.py --bgp_view 9.9.9.9/32 0
Address      Netmask      Gateway      Nbr IP      Nbr ID      Metric      Type      Intf      Sync'd      Advertise      Inbound      Preference      LocalP      Aspl      Reachable      Ptr      Age      SEG      Communities
9.9.9.9      255.255.255.255  172.16.1.11  172.16.1.11  0.0.0.0      0          EU         GE6        RCVD       true        learn       1001008     100        3          yes        0x7fe9e06c8b40  66997     0          174:2767
edge:b1-edge1:~#
```

- 5 PG1 learns the same route from BGP and uses cost 1005 and redistributes it to the Edges. The below output shows the derived cost/preference in PG.

```
root@karun1-gateway1:~# debug.py --bgp_view 9.9.9.9/32 0
Enterprise      Address      Netmask      Gateway      Nbr IP      Nbr ID      Metric      Type      Intf      Sync'd      Advertise      Inbound      Age      SEG      Pref      Communities
184014ff-7cc1-496e-a5eb-13b75933a822  9.9.9.9      255.255.255.255  101.101.101.10  101.101.101.10  100.0.0.0      0          any        RCVD       true        learn       839        0          1005
```

- 6 Spoke1 receives the route from Hub1 and Hub2 with the non-preferred cost of 1001008. Spoke1 has the preferred cost of 003. Hence, spoke1's own underlay route will be preferred and Hub routes will be installed below the underlay route (SB). Within the Hub routes, if the preference (cost) is the same, BGP attributes will be compared for route sorting. If BGP attributes are also the same, then the Hub order will be used to install the routes.

- 7 Spoke1 receives a route from Spoke2 and PG1 with costs 1003 and 1005, respectively. Since Spoke1 is having preferred cost 1003, and receives routes from Spoke2 and PG1 with a preferred cost (<100000), Spoke1 adds the reference cost 1000000 to the incoming preferred cost and install the routes in FIB. In this case, Spoke2's route will be installed with a cost of 1001003 and PG1's route will be installed with a cost of 1001005.

```
edge:b2-edge1:# debug.py --routes 9.9.9.9/32 0
Address      Netmask   Type  Gateway  Next Hop Name          Next Hop ID Destination Name          Dst LogicalId Reachable Metric Preference Flags Vlan Intf Sub IntfId MTU SEG
9.9.9.9  255.255.255.255  edge2edge    any    b1-edge1  7651bc6-414d-45e8-acdd-a2bad10e0acf  b3-edge1  fc8946eb-e2e4-4412-adea-73b16a6ef7c8  True     0  1000000  SB  0  GEB  N/A  N/A  0
9.9.9.9  255.255.255.255  edge2edge    any    b5-edge1  c91db03-0b06-4b4e-a908-334c8c704f7a  b3-edge1  fc8946eb-e2e4-4412-adea-73b16a6ef7c8  True     0  1001003  DSBR  0  any   N/A  1500  0
9.9.9.9  255.255.255.255  cloud        any    gateway-1  7f53063e-47af-44dc-a20e-9a0c7c0a8266  gateway-1  7f53063e-47af-44dc-a20e-9a0c7c0a8266  True     0  1001005  PBR   0  any   N/A  N/A  0
9.9.9.9  255.255.255.255  edge2edge    any    b1-edge1  7651bc6-414d-45e8-acdd-a2bad10e0acf  b1-edge1  7651bc6-414d-45e8-acdd-a2bad10e0acf  True     0  1001008  DSBR  0  any   N/A  1500  0
9.9.9.9  255.255.255.255  edge2edge    any    b5-edge1  c91db03-0b06-4b4e-a908-334c8c704f7a  b5-edge1  c91db03-0b06-4b4e-a908-334c8c704f7a  True     0  1001008  DSBR  0  any   N/A  1500  0
P - PG, B - BGP, D - DCE, L - LAN SR, C - Connected, O - External, W - WAN SR, S - SecureEligible, R - Remote, s - self, r - recursive, H - HA, m - Management, n - nonVeloCloud, v - ViaVeloCloud, A - RouterAdvertisement, c - CWS, a - Global PG Static, b - Blackhole, I - IPsec, G - GRE, p - Peer
```

- 8 The same route sorting logic is applied in Spoke2 or even Hubs if they learn the route as non-uplink route.
- 9 If there is no underlay route learned in any entity, there will not be any correction to the received route preference/cost. The routes will be installed as per the received preference/cost.

### Route Ordering in Hub with Uplink Routes:

- Hubs install their own underlay route (SB) with a reference cost of 1000000 in FIB.
- Hubs receive spoke routes with a preferred cost of 1003. Since cost is same between the spokes, BGP attributes will be compared and sorted based on that. If BGP attributes are also same, then spoke logical id will be used for sorting(lower destination logical ID wins the tie-breaker). The spoke's routes will be installed with received cost as it is.
- The Hub receives PG1's route with preferred cost. Therefore, it installs with that cost as is.

```
edge:b1-edge1:# debug.py --routes 9.9.9.9/32 0
Address      Netmask   Type  Gateway  Next Hop Name          Next Hop ID Destination Name          Dst LogicalId Reachable Metric Preference Flags Vlan Intf Sub IntfId MTU SEG
9.9.9.9  255.255.255.255  edge2edge    any    b3-edge1  fc8946eb-e2e4-4412-adea-73b16a6ef7c8  b3-edge1  fc8946eb-e2e4-4412-adea-73b16a6ef7c8  True     0  1003  DSBR  0  any   N/A  1500  0
9.9.9.9  255.255.255.255  edge2edge    any    b2-edge1  1c2656e5-1f7f-4a33-b471-97d8e3b01ac6  b2-edge1  1c2656e5-1f7f-4a33-b471-97d8e3b01ac6  True     0  1003  DSBR  0  any   N/A  1500  0
9.9.9.9  255.255.255.255  cloud        any    gateway-1  7f53063e-47af-44dc-a20e-9a0c7c0a8266  gateway-1  7f53063e-47af-44dc-a20e-9a0c7c0a8266  True     0  1005  PBR   0  any   N/A  N/A  0
9.9.9.9  255.255.255.255  any    172.16.1.1  N/A          N/A          N/A          N/A          N/A          True     0  1000000  SB  0  GEB  N/A  N/A  0
P - PG, B - BGP, D - DCE, L - LAN SR, C - Connected, O - External, W - WAN SR, S - SecureEligible, R - Remote, s - self, r - recursive, H - HA, m - Management, n - nonVeloCloud, v - ViaVeloCloud, A - RouterAdvertisement, c - CWS, a - Global PG Static, b - Blackhole, I - IPsec, G - GRE, p - Peer
edge:b1-edge1:#
```

### Route Ordering in PG:

- PG1 installs its own underlay route (PB) with preference 100000.
- PG1 receives spoke routes and Hub route with corresponding preference. Routes are placed in the FIB based on the preference value. If preference are same, BGP attributes are considered. If they are also same, then logical ID will be used for sorting.
- In PG, there is no preference/cost correction.

```
root@karuni-gateway-1:# debug.py --routes all 9.9.9.9/32 0
EnterpriseID          Address      Netmask   Type  Peer Name          Destination          Reachable  Metric  Preference  Flags  C-Tag  S-Tag  Handoff  Mode  Age
184014ff-7cc1-496e-05eb-13b75933a822  9.9.9.9  255.255.255.255  edge2edge    b3-edge1  fc8946eb-e2e4-4412-adea-73b16a6ef7c8  True     0  1003  SB  0  0  N/A  N/A  2
184014ff-7cc1-496e-05eb-13b75933a822  9.9.9.9  255.255.255.255  edge2edge    b2-edge1  1c2656e5-1f7f-4a33-b471-97d8e3b01ac6  True     0  1003  SB  0  0  N/A  N/A  208
184014ff-7cc1-496e-05eb-13b75933a822  9.9.9.9  255.255.255.255  cloud        N/A          0.0.0.0  True     0  1000000  PB  100  0  VLAN  802.1Q  202871
184014ff-7cc1-496e-05eb-13b75933a822  9.9.9.9  255.255.255.255  edge2edge    b1-edge1  7651bc6-414d-45e8-acdd-a2bad10e0acf  True     0  1001008  SB  0  0  N/A  N/A  269181
184014ff-7cc1-496e-05eb-13b75933a822  9.9.9.9  255.255.255.255  edge2edge    b5-edge1  c91db03-0b06-4b4e-a908-334c8c704f7a  True     0  1001008  SB  0  0  N/A  N/A  202869
P - PG, B - BGP, D - DCE, L - LAN SR, C - Connected, O - External, W - WAN SR, S - SecureEligible, R - Remote, s - self, r - recursive, H - HA, m - Management, n - nonVeloCloud, v - ViaVeloCloud, A - RouterAdvertisement, c - CWS, a - Global PG Static, b - Blackhole, I - IPsec, G - GRE, p - Peer
```

### Behavior if DCC is not enabled:

- If DCC is not enabled, the advertisement verdict and the preference calculation is performed by the Orchestrator. Each entity (Edge or Gateway) sends the learned routes to the Orchestrator and expects to receive a reply from the Orchestrator. Upon receiving the reply from the Orchestrator, Edge, or Gateway would begin redistributing the routes to other SDWAN entities if the advertise flag is "true" in the reply.

- The route ordering remains the same, as is the case of DCC being enabled, but the preference values are not fixed in this scenario of DCC being disabled.
- The reference preference/cost is 512 for the Orchestrator based preference calculation. The preference/cost < 512 is the preferred cost, whereas > 512 is given to non-preferred routes (UPLINK routes, OSPF external routes). Other route sorting logic remains the same as when DCC is enabled.
- If spoke2 learns the route first and sends it to the Orchestrator, the Orchestrator will begin assigning the preference based on the entity and route type. Since spoke2 learns as non-uplink, the Orchestrator will assign the preference value (for example, 64). Later, when spoke1 sends the same route to the Orchestrator, the Orchestrator will compare the entity, route type, and route attributes. If it is better, it will assign the preference to < 64. If it is worse, it will assign the preference to > 64.
- Hubs learn the routes as uplink routes and send them to the Orchestrator. The Orchestrator assigns a non-preferred cost (>512); in this example, it is 4096. If the preference is the same, the Hub order will be used to sort the routes in the spokes.
- When DCC is disabled, the route order in spoke1 (with a non-uplink route) will look like the following image.

```
edge:b2-edge1:# debug.py --bgp_view 9.9.9.9/32 0
Address Netmask Gateway Nbr IP Nbr ID Metric Type Intf Sync'd Advertise Inbound Preference LocalP Aspl Reachable Ptr Age SEG Communities
9.9.9.9 255.255.255.255 172.16.2.3 172.16.2.3 0.0.0.0 0 E GES RCVD true learn 184 100 4 yes 0x7fc838350f0d 120 0 186:6884
edge:b2-edge1:# debug.py --routes 9.9.9.9/32 0
Address Netmask Type Gateway Next Hop Name Next Hop ID Destination Name Dst LogicalId Reachable Metric Preference Flags Vlan Intf Sub IntfId MTU SEG
9.9.9.9 255.255.255.255 dry 172.16.2.3 N/A N/A N/A N/A 655 5B N/A N/A 0
9.9.9.9 255.255.255.255 edge2edge any b1-edge1 765c1bc6-414d-45e8-acdd-a2bad1ea0ecf b3-edge1 fc8946eb-e2e4-4412-adea-73b16def7c8 True 0 512 DSBR 0 any N/A 1500 0
9.9.9.9 255.255.255.255 edge2edge any b5-edge1 c091ab03-c0b6-4b4e-a008-334c8c70af7a b3-edge1 fc8946eb-e2e4-4412-adea-73b16def7c8 True 0 512 DSBR 0 any N/A 1500 0
9.9.9.9 255.255.255.255 cloud any gateway-1 7f53063e-47af-4d6c-a20e-9a0c7c0a8266 gateway-1 7f53063e-47af-4d6c-a20e-9a0c7c0a8266 True 0 816 PBR 0 any N/A N/A 0
9.9.9.9 255.255.255.255 edge2edge any b1-edge1 765c1bc6-414d-45e8-acdd-a2bad1ea0ecf b1-edge1 765c1bc6-414d-45e8-acdd-a2bad1ea0ecf True 0 4096 DSBR 0 any N/A 1500 0
9.9.9.9 255.255.255.255 edge2edge any b5-edge1 c091ab03-c0b6-4b4e-a008-334c8c70af7a b5-edge1 c091ab03-c0b6-4b4e-a008-334c8c70af7a True 0 4096 DSBR 0 any N/A 1500 0
P - PG, B - BGP, D - DCE, L - LAN SR, C - Connected, 0 - External, W - WAN SR, S - SecureEligible, R - Remote, s - self, r - recursive, H - HA, m - Management, n - nonVeloCloud, v - VeloCloud, A - RouterAdvertisement, c - CMS, a - Global PG Static, b - Blackhole, I - IPSec, G - GRE, p - Peer
```

- The router order in Hubs with an uplink route will look like the following image.

```
edge:b1-edge1:# debug.py --bgp_view 9.9.9.9/32 0
Address Netmask Gateway Nbr IP Nbr ID Metric Type Intf Sync'd Advertise Inbound Preference LocalP Aspl Reachable Ptr Age SEG Communities
9.9.9.9 255.255.255.255 172.16.1.11 172.16.1.11 0.0.0.0 0 EU GES RCVD true learn 4096 100 3 yes 0x7fe9e06c840 1009 0 174:2767
edge:b1-edge1:# debug.py --routes 9.9.9.9/32 0
Address Netmask Type Gateway Next Hop Name Next Hop ID Destination Name Dst LogicalId Reachable Metric Preference Flags Vlan Intf Sub IntfId MTU SEG
9.9.9.9 255.255.255.255 edge2edge any b3-edge1 fc8946eb-e2e4-4412-adea-73b16def7c8 b3-edge1 fc8946eb-e2e4-4412-adea-73b16def7c8 True 0 64 DSBR 0 any N/A 1500 0
9.9.9.9 255.255.255.255 edge2edge any b2-edge1 1c2656e5-1f7f-4a33-b471-97d8e3b01c6 b2-edge1 1c2656e5-1f7f-4a33-b471-97d8e3b01c6 True 0 184 DSBR 0 any N/A 1500 0
9.9.9.9 255.255.255.255 cloud any gateway-1 7f53063e-47af-4d6c-a20e-9a0c7c0a8266 gateway-1 7f53063e-47af-4d6c-a20e-9a0c7c0a8266 True 0 304 PBR 0 any N/A N/A 0
9.9.9.9 255.255.255.255 any 172.16.1.11 N/A N/A N/A N/A 512 SB 0 GEB N/A N/A 0
P - PG, B - BGP, D - DCE, L - LAN SR, C - Connected, 0 - External, W - WAN SR, S - SecureEligible, R - Remote, s - self, r - recursive, H - HA, m - Management, n - nonVeloCloud, v - VeloCloud, A - RouterAdvertisement, c - CMS, a - Global PG Static, b - Blackhole, I - IPSec, G - GRE, p - Peer
```

- The route order in PG will look like the following image.

```
root@arun1-gateway-1:# debug.py --bgp_view 9.9.9.9/32 0
Address Netmask Gateway Nbr IP Nbr ID Metric Type Intf Sync'd Advertise Inbound Preference LocalP Aspl Reachable Ptr Age SEG Pref Communities
Enterprise 18401aff-7c1-496e-05eb-13b75933a822 9.9.9.9 255.255.255.255 101.101.101.10 101.101.101.10 100.0.0.0 0 E GES RCVD true learn 1060 0 304
root@arun1-gateway-1:# debug.py --routes all 9.9.9.9/32 0
EnterpriseID Address Netmask Type Peer Name DestinationReachable Metric Preference Flags C-Tag S-Tag Handoff Mode Age SEG
18401aff-7c1-496e-05eb-13b75933a822 9.9.9.9 255.255.255.255 edge2edge b3-edge1 fc8946eb-e2e4-4412-adea-73b16def7c8 True 0 64 SB 0 N/A N/A 1068 0
18401aff-7c1-496e-05eb-13b75933a822 9.9.9.9 255.255.255.255 edge2edge b2-edge1 1c2656e5-1f7f-4a33-b471-97d8e3b01c6 True 0 184 SB 0 0 N/A N/A 261 0
18401aff-7c1-496e-05eb-13b75933a822 9.9.9.9 255.255.255.255 cloud N/A 0.0.0.0 True 0 512 PB 100 0 0 VLAN 802.1Q 1059 0
18401aff-7c1-496e-05eb-13b75933a822 9.9.9.9 255.255.255.255 edge2edge b1-edge1 765c1bc6-414d-45e8-acdd-a2bad1ea0ecf True 0 4096 SB 0 0 N/A N/A 1071 0
18401aff-7c1-496e-05eb-13b75933a822 9.9.9.9 255.255.255.255 edge2edge b5-edge1 c091ab03-c0b6-4b4e-a008-334c8c70af7a True 0 4096 SB 0 0 N/A N/A 1062 0
P - PG, B - BGP, D - DCE, L - LAN SR, C - Connected, 0 - External, W - WAN SR, S - SecureEligible, R - Remote, s - self, H - HA, m - Management, n - nonVeloCloud, v - VeloCloud, p - Peer, c - CMS, a - RAS, M - MTGRE, F - FRR
```

## Route Ordering in Gateway:

- Longest prefix length.
- NSD static routes local .
- Remote NSD static.
- PG secure static.
  - Enterprise level PG static route wins over Global Level PG static.

- 5 Remote connected/static.
  - a Edge logical\_id will be the tie breaker (higher logical ID wins).
- 6 Dynamic routes (Overlay Flow Control (OFC) or Distributed Cost Calculation Driven route order).
  - a Dynamic route sorting will be based on preference value. Lower preference wins.
  - b Unlike an Edge, there is no preference in auto correction in Gateway. For dynamic routes, the Gateway installs the routes with the received preference. The local route will always be installed with the reference preference of 1000000.

---

**Note** For more information about Preference Calculation, see the “Overlay Flow Control (OFC) with Distributed Cost Calculation (DCC)” section.

---

- 7 PG non-secure static.

---

**Note** In the Gateway, the route selection for the traffic forwarding depends on other conditions, e.g., Edge Profile settings, direction of the flow, etc.

---

## Dynamic Multipath Optimization (DMPO)

This section provides an in-depth overview of Dynamic Multipath Optimization (DMPO) as used by the VMware SD-WAN service.

### Overview

VMware SD-WAN™ is a solution that lets enterprise and service providers use multiple WAN transports at the same time. This way, they can increase bandwidth and ensure application performance. The solution works for both on-premise and cloud applications (SaaS/IaaS). It uses a Cloud-Delivered architecture that builds an overlay network with multiple tunnels. It monitors and adapts to the changes in the WAN transports in real time. Dynamic Multipath Optimization (DMPO) is a technology that VMware SD-WAN has developed to make the overlay network more resilient. It considers the real time performance of the WAN links. This document explains the key features and benefits of DMPO.

The following diagram depicts a typical SD-WAN deployment with Multi Cloud Non SDWAN Destinations.

### Key Functionalities

DMPO is a technology that VMware SD-WAN uses for data traffic processing and forwarding. It works between the VMware SD-WAN Edge and VMware SD-WAN Gateway devices. These devices are the DMPO endpoints.

- For enterprise locations (Branch to Branch or Branch to Hub), the Edges create DMPO tunnels with each other.
- For cloud applications, each Edge creates DMPO tunnels with one or more Gateways.

DMPO has three key features that are discussed below.

## Continuous Monitoring

**Automated Bandwidth Discovery:** Once the WAN link is detected by the VMware SD-WAN Edge, it first establishes DMPO tunnels with one or more VMware SD-WAN Gateways and runs bandwidth test with the closest Gateway. The bandwidth test is performed by sending short bursts of bi-directional traffic and measuring the received rate at each end. Since the Gateway is deployed at the Internet PoPs, it can also identify the real public IP address of the WAN link in case the Edge interface is behind a NAT or PAT device. A similar process applies for a private link. For the Edges acting as the Hub or headend, the WAN bandwidth is statically defined. However, when the branch Edge establishes a DMPO tunnel with the Hub Edges, they follow the same bandwidth test procedures similar to how it is done between an Edge and a Gateway on the public link.

**Continuous Path Monitoring:** Dynamic Multipath Optimization (DMPO) performs continuous, unidirectional measurements of performance metrics - loss, latency and jitter of every packet, on every tunnel between any two DMPO endpoints, Edge or Gateway. VMware SD-WAN's per-packet steering allows independent decisions in both uplink and downlink directions without introducing any asymmetric routing. DMPO uses both passive and active monitoring approaches. While there is user-traffic, DMPO tunnel header contains additional performance metrics, including sequence number and timestamp. This enables the DMPO endpoints to identify lost and out-of-order packets, and calculate jitter and latency in each direction. The DMPO endpoints communicate the performance metrics of the path between each other every 100 ms.

While there is no user traffic, an active probe is sent every 100 ms and, after 5 minutes of no high priority user-traffic, the probe frequency is reduced to 500 ms. This comprehensive measurement enables the DMPO to react very quickly to the change in the underlying WAN condition, resulting in the ability to deliver sub-second protection against sudden drops in bandwidth capacity and outages in the WAN.

**MPLS Class of Service (CoS):** For a private link that has CoS agreement, DMPO can be configured to take CoS into account for both monitoring and application steering decisions.

## Dynamic Application Steering

**Application-aware Per-packet Steering:** Dynamic Multipath Optimization (DMPO) identifies traffic using layer 2 to 7 attributes, e.g., VLAN, IP address, protocol, and applications. VMware SD-WAN performs application-aware per-packet steering based on business policy configuration and real-time link conditions. The business policy contains out of the box Smart Defaults that specifies the default steering behavior and priority of more than 2500 applications: Customers can immediately use dynamic packet steering and application-aware prioritization without having to define any policy.

Throughout its lifetime, any traffic flow is steered onto one or more DMPO tunnels, in the middle of the communication, with no impact to the flow. A link that is completely down is referred to as having an outage condition. A link that is unable to deliver SLA for a given application is referred to as having a brownout condition. VMware SD-WAN offers sub-second outage and

sudden drops in bandwidth capacity protection. With the continuous monitoring of all the WAN links, DMPO detects sudden loss of SLA or outage condition within 300-500 ms and immediately steers traffic flow to protect the application performance, while ensuring no impact to the active flow and user experience. There is one minute hold time from the time that the brownout or outage condition on the link is cleared before DMPO steers the traffic flow back onto the preferred link if specified in the business policy.

Intelligent learning enables application steering based on the first packet of the application by caching classification results. This is necessary for application-based redirection, e.g., redirect Netflix onto the branch Internet link, bypassing the DMPO tunnel, while backhauling Office 365 to the enterprise regional hub or data center.

**Example:** Smart Defaults specifies that Microsoft Skype for Business is High Priority and is Real-Time application. Assuming there are 2 links with latency of 50 ms and 60ms respectively. Assume all other SLAs are equal or met. DMPO will chose the link the better latency, i.e. link with 50ms latency. If the current link to which the Skype for Business traffic is steered experiences high latency of 200 ms, within less than a second the packets for the Skype for Business flow is steered on to another link which has better latency of 60 ms.

**Bandwidth Aggregation for Single Flow:** For the type of applications that can benefit from more bandwidth, e.g. file transfer, DMPO performs per-packet load balancing, utilizing all available links to deliver all packets of a single flow to the destination. DMPO takes into account the real time WAN performance and decides which paths should be used for sending the packets of the flow. It also performs resequencing at the receiving end to ensure there is no out-of-order packets introduced as a result of per-packet load balancing.

**Example:** Two 50 Mbps links deliver 100Mbps of aggregated capacity for a single traffic flow. QoS is applied at both the aggregate and individual link level.

## On-demand Remediation

**Error and Jitter Correction:** In a scenario where it may not be possible to steer the traffic flow onto the better link, e.g., single link deployment, or multiple links having issues at the same time, Dynamic Multipath Optimization (DMPO) can enable error corrections for the duration the WAN links have issues. The type of error corrections used depends on the type of applications and the type of errors.

Real-time applications such as voice and video flows can benefit from **Forward Error Correction (FEC)** when there is packet loss. DMPO automatically enables FEC on single or multiple links. When there are multiple links, DMPO will select up to two of the best links at any given time for FEC. Duplicated packets are discarded and out-of-order packets are re-ordered at the receiving end before delivering to the final destination.

DMPO enables jitter buffer for the real-time applications when the WAN links experience jitter. TCP applications such as file transfer benefit from Negative Acknowledgement (NACK). Upon the detection of a missing packet, the receiving DMPO endpoint informs the sending DMPO endpoint to retransmit the missing packet. Doing so protects the end applications from detecting packet loss and, as a result, maximizes TCP window and delivers high TCP throughput even during lossy condition.

When the packet loss surpasses a specific threshold, it prompts the initiation of **Adaptive Forward Error Correction (FEC)** through packet duplication. The error-correction applied is based on the traffic class:

- **Transactional/Bulk traffic:** In this case, we apply a NACK based retransmit algorithm, which is done at the VCMP protocol level where we attempt to correct the error condition before handing over the packet to the application.
- **Realtime traffic:** In this case, we apply adaptive FEC to replicate packets (activate/deactivate upon loss SLA violation) and/or jitter buffer correction (upon jitter SLA violation – this one can only be activated and will persist for the life of the flow).

The link SLA (loss, latency, jitter) is continually being monitored and measured on a periodic basis and FEC (packet duplication) will be activated upon threshold violation for real-time traffic (different values for voice vs. video applications).

In a single WAN link scenario, duplicate packets are transmitted on the same link adjacent to one another. Since packet drops due to congestion are random, it is statistically unlikely that two adjacent packets will be dropped, greatly increasing the likelihood that one of the packets will make it through to the destination. The replicated packets are sent on separate links in the case of two or more WAN links.

**Adaptive FEC** is triggered on a per-flow basis in real-time based on measured packet loss thresholds, and disabled in real-time once packet loss no longer exceeds the activation threshold. This ensures that available bandwidth is used as efficiently as possible, unnecessary packet duplication is avoided, and resource overhead is reduced. Another significant benefit of VMware's Adaptive FEC approach is that the effect of packet loss in the transport network on end-user devices is minimized or eliminated. When end-user devices do not see packet drops, they avoid retransmissions and TCP congestion avoidance mechanisms like slow start, which can negatively impact overall throughput, application performance, and end-user experience.

## DMPO Real World Results

**Scenario 1:** Branch-to-branch VoIP call on a single link. The results in the below figure demonstrate the benefits of on-demand remediation using FEC and jitter remediation on a single Internet link with traditional WAN and VMware SD-WAN. A mean opinion score (MOS) of less than 3.5 is unacceptable quality for a voice or video call.

## Traditional WAN

**Connection Summary**

**Test audit report:**

**Results analysis for: voip test**

Your connection's **jitter** was measured as 0.4 ms, which indicates that it can produce a constant flow of data. Voice-over-IP conversations should be of good quality.

Your connection's **packet loss** was measured at 1.9%, which indicates that it is dropping too much data along the route to the server. VoIP conversations may sound slightly broken, but should nonetheless be understandable.

Your connection's **MOS score** is estimated to be 2.1.

MOS: 2.1 @  
2% Packet loss

**Connection Summary**

**Test audit report:**

**Results analysis for: voip test**

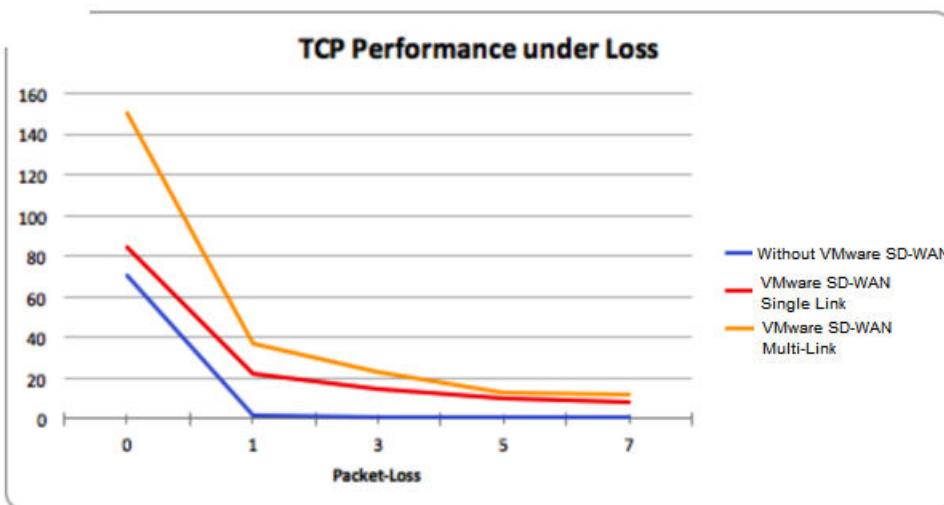
Your connection's **jitter** was measured as 33.2 ms, which indicates that it is too unpredictable to sustain a constant flow of data. As such, voice-over-IP conversations may be broken.

Your connection's **packet loss** was measured at 0.0%, which indicates that it is accurately transferring data. Voice-over-IP conversations should be of good quality.

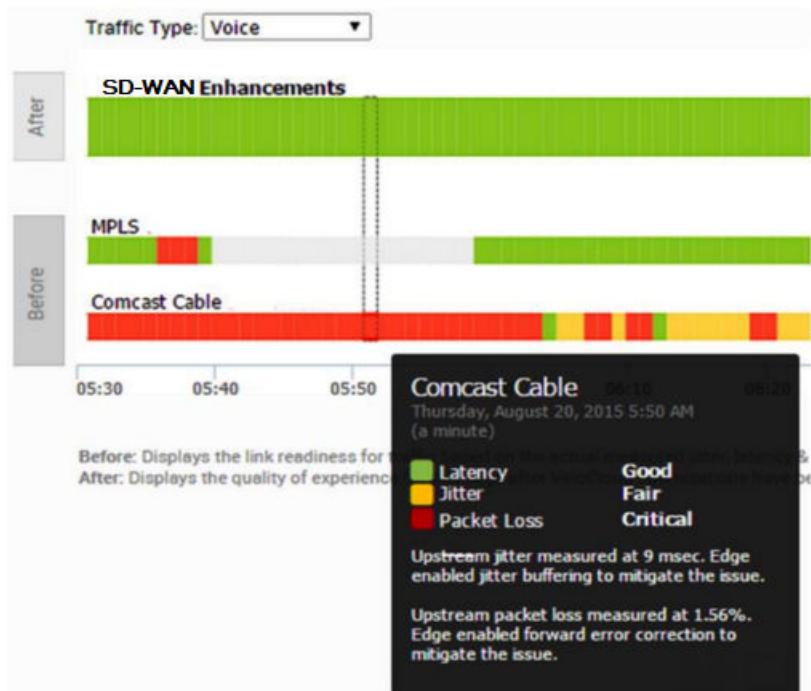
Your connection's **MOS score** is estimated to be 3.3.

MOS: 3.3 @  
33ms Jitter

**Scenario 2:** TCP Performance with and without VMware SD-WAN for Single and Multiple Links. These results show how NACK enables per-packet load balancing.



**Scenario 3:** Hybrid WAN scenario with an outage on the MPLS link and both jitter and loss on the Internet (Comcast) link. These results show how DMPO protects applications from sub-second outages by steering them to Internet links and enabling on-demand remediation on the Internet link.



## Business Policy Framework and Smart Defaults

The business policy lets the IT administrator control QoS, steering, and services for the application traffic. Smart Defaults provides a ready-made business policy that supports over 2500 applications. DMPO makes steering decisions based on the type of application, real time link condition (congestion, latency, jitter, and packet loss), and the business policy. Here is an example of a business policy.

Each application has a category. Each category has a default action, which is a combination of Business Priority, Network Service, Link Steering, and Service Class. You can also define custom applications.

### Add Rule

Rule Name \*

IP Version \*  IPv4  IPv6  IPv4 and IPv6

Match Action

Source Any

Destination Any

Application Define

Application Category

- Business Collaboration
- Real Time Audio/Video
- Authentication
- Business Application
- Business Collaboration
- Email
- File Sharing

Application Microsoft Skype for Business (formerly Microsoft Lync Online)

DSCP

Remote Desktop Multi Path

Add Rule

Rule Name \*

IP Version \*  IPv4  IPv6  IPv4 and IPv6

Match Action

Priority	<input checked="" type="radio"/> High <input type="radio"/> Normal <input type="radio"/> Low
Enable Rate Limit	<input type="checkbox"/>
Network Service	<input type="text" value="MultiPath"/>
Link Steering	<input type="text" value="Auto"/>
Inner Packet DSCP Tag	<input type="text" value="Leave as is"/>
Outer Packet DSCP Tag	<input type="text" value="0 - CS0/DF"/>
Enable NAT	<input type="checkbox"/> ⓘ
Service Class ⓘ	<input checked="" type="radio"/> Realtime <input type="radio"/> Transactional <input type="radio"/> Bulk

Each application has a Service Class: **Real Time**, **Transactional**, or **Bulk**. The Service Class determines how DMPO handles the application traffic. You cannot change the Service Class for the default applications, but you can specify it for your own custom applications.

Each application also has a Business Priority: **High**, **Normal**, or **Low**. The Business Priority determines how DMPO prioritizes and applies QoS to the application traffic. You can change the Business Priority for any application.

	High	Normal	Low	High	Normal
Real Time	Business Collaboration	Audio/Video		35	15
Transactional	Remote Desktop, Business App	Infrastructure, Auth, Mgmt, Network Services, Tunneling	IM App, Web, Proxies, Games, Media, Social	20	7
Bulk	Email	File Sharing	Storage/Backup, P2P	15	5

Default application/category and traffic class mapping

Default weight and traffic class mapping

There are three types of Network Services: **Direct**, **MultiPath**, and **Internet Backhaul**. By default, an application is assigned one of the default Network Services, which can be modified by the customers.

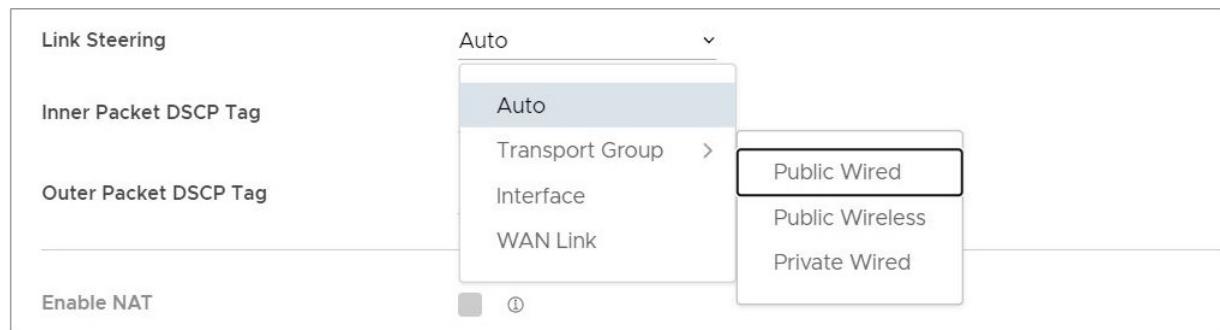
- **Direct:** This action is typically used for non-critical, trusted Internet applications that should be sent directly, bypassing DMPO tunnel. An example is Netflix. Netflix is considered a non-business, high-bandwidth application and should not be sent over the DMPO tunnels. The traffic sent directly can be load balanced at the flow level. By default, all the low priority applications are given the Direct action for Network Service.
- **MultiPath:** This action is typically given for important applications. By inserting the Multipath service, the Internet-based traffic is sent to the VMware SD-WAN Gateway. The table below shows the default link steering and on-demand remediation technique for a given Service Class. By default, high and normal priority applications are given the Multipath action for Network Service.
- **Internet Backhaul:** This action redirects the Internet applications to an enterprise location that may or may not have the VMware SD-WAN Edge. The typical use case is to force important Internet applications through a site that has security devices such as firewall, IPS, and content filtering before the traffic is allowed to exit to the Internet.

## Link Steering Abstraction With Transport Group

Across different branch and hub locations, there may be different models of the VMware SD-WAN Edge with different WAN interfaces and carriers. In order to enforce the centralized link steering policy using Profile, it is important that the interfaces and carries are abstracted. Transport Group provides the abstraction of the actual interfaces of the devices and carriers used at various locations. The business policy at the Profile level can be applied to the Transport Group instead, while the business policy at the individual Edge level can be applied to Transport Group, WAN Link (carrier), and Interfaces.

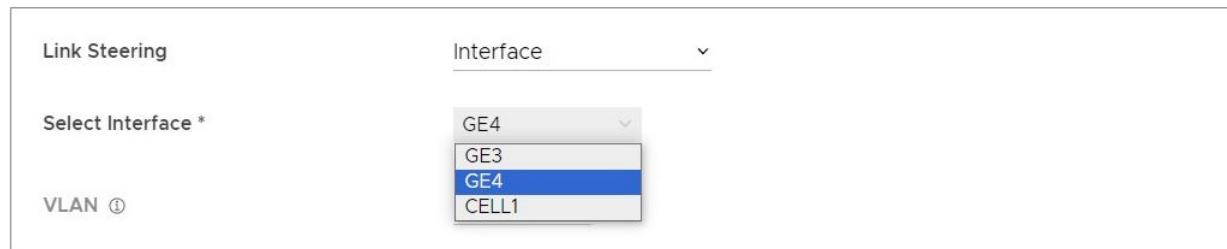
## Link Steering by Transport Group

Different locations may have different WAN transports, e.g. WAN carrier name, WAN interface name, DMPO uses the concept of transport group to abstract the underlying WAN carriers or interfaces from the business policy configuration. The business policy configuration can specify the transport group (public wired, public wireless, private wired, etc.) in the steering policy so that the same business policy configuration can be applied across different device types or locations, which may have completely different WAN carriers and WAN interfaces, etc. When the DMPO performs the WAN link discovery, it also assigns the transport group to the WAN link. This is the most desirable option for specifying the links in the business policy because it eliminates the need for IT administrators to know the physical connectivity or WAN carrier.



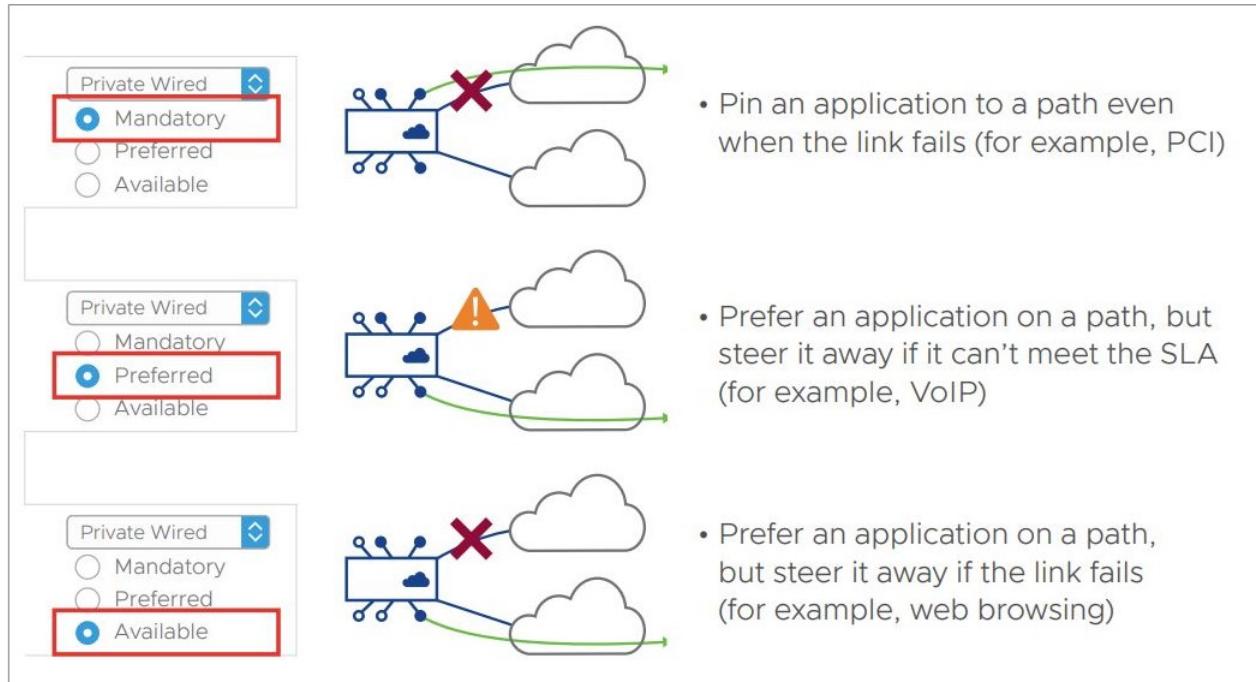
## Link Steering by Interface

The link steering policy can be applied to the interface, e.g. GE2, GE3, which will be different depending on the Edge model and the location. This is the least desirable option to use in the business policy because IT administrators have to be fully aware of how the Edge is connected to be able to specify which interface to use.



## Link Steering and On-demand Remediation

There are four possible options for Link Steering – **Auto**, **Preferred**, **Mandatory**, and **Available**.



**Link Selection: Mandatory**– Pin the traffic to the link or the transport group. The traffic is never steered away regardless of the condition of the link including outage. On-demand remediation is triggered to mitigate brownout condition such as packet loss and jitter.

**Example:** Netflix is a low priority application and is required to stay on the public wired links at all times.

**Link Selection: Preferred**– Select the link to be marked as "preferred". Depending on the type of WAN links available on the Edge, there are three possible scenarios:

- **Where the preferred Internet link has multiple public WAN link alternatives:** Application traffic stays on the preferred link as long as it meets SLA for that application, and steers to other public links once the preferred link cannot deliver the SLA needed by the application. In the situation that there is no link to steer to, meaning all public links fail to deliver the SLA needed by the application, on-demand remediation is enabled. Alternatively, instead of steering the application away as soon as the current link cannot deliver the SLA needed by the application, DMPO can enable the on-demand remediation until the degradation is too severe to be remediated, then DMPO will steer the application to the better link.
  - **Example:** Prefer the video collaboration application on the Internet link until it fails to deliver the SLA needed by video, then steer to a public link that meets this application's SLA.
- **Where the preferred Internet link has multiple public WAN link and private WAN link alternatives:** Application traffic stays on the preferred link as long as it meets SLA for that application, and steers to another public link once the preferred link cannot deliver the SLA needed by the application. The preferred link will NOT steer to a private link in the event of an SLA failure, and would only steer to that private link in the event both the preferred link and another public link were both either unstable or down completely. In the situation that

there is no link to steer to, meaning another public links failed to deliver the SLA needed by the application, on-demand remediation is enabled. Alternatively, instead of steering the application away as soon as the current link cannot deliver the SLA needed by the application, DMPO can enable the on-demand remediation until the degradation is too severe to be remediated, then DMPO will steer the application to a better link.

- **Example A:** Prefer the video collaboration application on the Internet link until it fails to deliver the SLA needed by video, then steer to a public link that meets this application's SLA.
- **Example B:** Prefer the video collaboration application on the Internet link until it goes unstable or drops completely, other public links are also unstable or have also dropped completely, then steer to an available private link.
- **Where the preferred Internet link has only private WAN link alternatives:** Application traffic stays on the preferred link regardless of the SLA status for that application, and will not steer to another private links even if the preferred link cannot deliver the SLA needed by the application. In place of steering to the private links on an SLA failure for that application, on-demand remediation is enabled. The preferred link would steer to the private link(s) would only steer to another private link(s) in the event that the preferred link was either unstable or down completely.
  - **Example:** Prefer the video collaboration application on the Internet link until the link goes unstable or drops completely, and then steer to an available private link.

---

**Note** The default manner in which a private link is treated with reference to a preferred link (in other words, that a preferred link will only steer to a private link if the preferred link is unstable or offline) is configurable through a setting on the Orchestrator UI.

---

**Link Selection: Available**– This option picks the available link as long as it is up. DMPO enables on-demand remediation if the link fails to meet the SLA. DMPO will not steer the application flows to another link unless the link is down.

**Example:** Web traffic is backhauled over the Internet link to the hub site using the Internet link as long as it is active, regardless of SLA.

**Link Selection: Auto**– This is the default option for all applications. DMPO automatically picks the best links based on the type of application and enables on-demand remediation when needed. There are four possible combinations of Link steering and On-demand Remediation for Internet applications. Traffic within the enterprise (VPN) always goes through the DMPO tunnels, so it always gets the benefits of on-demand remediation.

SERVICE CLASS		DESTINATION: INTERNET	
		Network Service: Multipath Link Steering: Auto	Network Service: Direct Link Steering: Auto
Real Time	Link selection behavior	Per-Packet Steering	Flow-Based Load Balancing
	On-demand remediation	FEC and Jitter Buffer	-
Transactional	Link selection behavior	Per-Packet Load Balancing	Flow-Based Load Balancing
	On-demand remediation	NACK	-
Bulk	Link selection behavior	Per-Packet Load Balancing	Flow-Based Load Balancing
	On-demand remediation	NACK	-

The below examples explain the default DMPO behavior for different type of applications and link conditions. Please see the appendix section for the default SLA for different application types.

**Example:** Real-Time applications.

- 1 **Scenario:** There is one link that meets the SLA for the application.

Expected DMPO behavior: It picks the best available link.

- 2 **Scenario:** There is one link with packet loss above the SLA for the application.

Expected DMPO behavior: It enables FEC for the real-time applications on this link.

- 3 **Scenario:** There are two links with loss on only one link.

Expected DMPO behavior: It enables FEC on both links.

- 4 **Scenario:** There are multiple links with loss on multiple links.

Expected DMPO behavior: It enables FEC on the two best links.

- 5 **Scenario:** There are two links but one link is unstable, i.e. it misses three consecutive heartbeats.

Expected DMPO behavior: It marks the link as unusable and steers the flow to the next best available link.

- 6 **Scenario:** There are two links with both jitter and loss.

Expected DMPO behavior: It enables FEC and jitter buffer on both links. Jitter buffer is enabled when jitter is more than 7 ms for voice and more than 5 ms for video. The sending DMPO endpoint tells the receiving DMPO endpoint to enable jitter buffer. The receiving DMPO endpoint buffers up to 10 packets or 200 ms of traffic, whichever is first. It uses the original timestamp in the DMPO header to calculate the flow rate for de-jitter buffer. If the flow is not constant, it disables jitter buffering.

**Example:** Transactional and bulk applications. Enables NACK if packet loss exceeds the threshold that is acceptable per application type (see the appendix for this value).

## Secure Traffic Transmission

DMPO encrypts both the payload and the tunnel header with IPsec transport mode end-to-end for private or internal traffic. The payload contains the user traffic. DMPO supports AES128 and AES256 for encryption. It uses the PKI and IKEv2 protocols for IPsec key management and authentication.

## Protocols and Ports Used

DMPO uses the following ports:

- **UDP/2426** – UDP/2426: This port is for overlay tunnel management and information exchange between the two DMPO endpoints (Edges and Gateways). It is also for data traffic that is already secured or not important, such as SFDC traffic from branch to the cloud between Edge and Gateway. SFDC traffic is encrypted with TLS.
- **UDP/500 and UDP/4500** – These ports are for IKEv2 negotiation and for IPsec NAT transparency.
- **IP/50** – This protocol is for IPsec over native IP protocol 50 (ESP) when there is no NAT between the two DMPO endpoints.

## Appendix: QoE threshold and Application SLA

DMPO uses the SLA threshold below for different types of applications. It will immediately take action to steer the affected application flows or perform on-demand remediation when the WAN link condition exceeds one or more thresholds. Packet loss is calculated by dividing the number of lost packets by the total packets in the last 1-minute interval. The DMPO endpoints communicate the number of lost packets every second. The QoE report also reflects this threshold.

DMPO will also take action immediately when it loses communications (no user data or probes) within 300 ms.

<b>Latency</b> One Way Delay in the Transmit Direction			
Traffic Type	Green	Yellow	Red
Realtime (small packets – voice)	<25ms	<65ms	>=65ms
Realtime (large packets – video)	<25ms	<65ms	>=65ms
Transactional	<50ms	<80ms	>=80ms

<b>Jitter</b> RFC 3550 Formula			
Traffic Type	Green	Yellow	Red
Realtime (small packets – voice)	<7ms	<30ms	>=30ms
Realtime (large packets – video)	<5ms	<15ms	>=15ms
Transactional	Not applicable		

<b>Packet Loss</b>			
Every second the Rx side reports the number of lost packets to the Tx side. The Tx side keeps a sliding window of the last 60 samples.			
Traffic Type	Green	Yellow	Red
Realtime (small packets – voice)	<0.3%	<1.0%	>=1.0%
Realtime (large packets – video)	<0.05%	<0.1%	>=0.1%
Transactional	<1.0%	<3.0%	>=3.0%

**Note** Beginning in Release 5.2.0, users have the capability to modify the threshold values for latency for video, voice, and transactional traffic types through a Customizable QoE feature. This means that customers can include high latency links as part of the selection process and the Orchestrator applies the new values to the QoE monitoring page.

## Solution Components

This section describes VMware solution components.

### VMware SD-WAN Edge

A thin “Edge” that is zero IT touch provisioned from the cloud for secured, optimized connectivity to your apps and virtualized services. The SD-WAN Edges are zero-touch, enterprise-class devices or virtual software that provide secure and optimized connectivity to private, public and hybrid applications; compute; and virtualized services. SD-WAN Edges perform deep application recognition, application and per-packet steering, on-demand remediation performance metrics and end-to-end quality of service (QoS) in addition to hosting Virtual Network Function (VNF) services. An Edge pair can be deployed to provide High Availability (HA). Edges can be deployed in branches, large sites and data centers. All other network infrastructure is provided on-demand in the cloud.

## VMware SASE Orchestrator

The VMware SASE Orchestrator provides centralized enterprise-wide configuration and real-time monitoring, as well as orchestrates the data flow into and through the SD-WAN overlay network. Additionally, it provides the one-click provisioning of virtual services across Edges, in centralized and regional enterprise service hubs and in the cloud.

## VMware SD-WAN Gateways

VMware SD-WAN network consists of gateways deployed at top tier network points-of-presence and cloud data centers around the world, providing SD-WAN services to the doorstep of SaaS, IaaS and cloud network services, as well as access to private backbones. Multi-tenant, virtual Gateways are deployed both by VMware SD-WAN transit and cloud service provider partners. The gateways provide the advantage of an on-demand, scalable and redundant cloud network for optimized paths to cloud destinations as well as zero-installation applications.

For more information about the VMware SD-WAN Gateways functionality and resiliency, see <https://knowledge.broadcom.com/external/article?legacyId=71374>.

## SD-WAN Edge Performance and Scale Data

This section covers the performance and scale architecture of the VMware SD-WAN Edge. It provides recommendations based on tests conducted on the various Edges configured with specific service combinations. It also explains performance and scale data points and how to use them.

### Introduction

The tests represent common deployment scenarios to provide recommendations that apply to most deployments. The test data herein are not all-inclusive metrics, nor are they performance or scale limits. There are implementations where the observed performance exceeds the test results and others where specific services, extremely small packet sizes, or other factors can reduce performance below the test results.

Customers are welcome to perform independent tests, and results could vary. However, recommendations based on our test results are adequate for most deployments.

### VMware SD-WAN Edge

VMware SD-WAN Edges are zero-touch, enterprise-class appliances that provide secure optimized connectivity to private, public, and hybrid applications as well as compute and virtualized services. VMware SD-WAN Edges perform deep application recognition of traffic flows, performance metrics measurements of underlay transport and apply end-to-end quality of service by applying packet-based link steering and on-demand application remediation, in addition to supporting other virtualized network services.

## Throughput Performance Test Topologies

Figure 4-1. FIGURE 1: Throughput performance test topology for devices 1 Gbps or lower

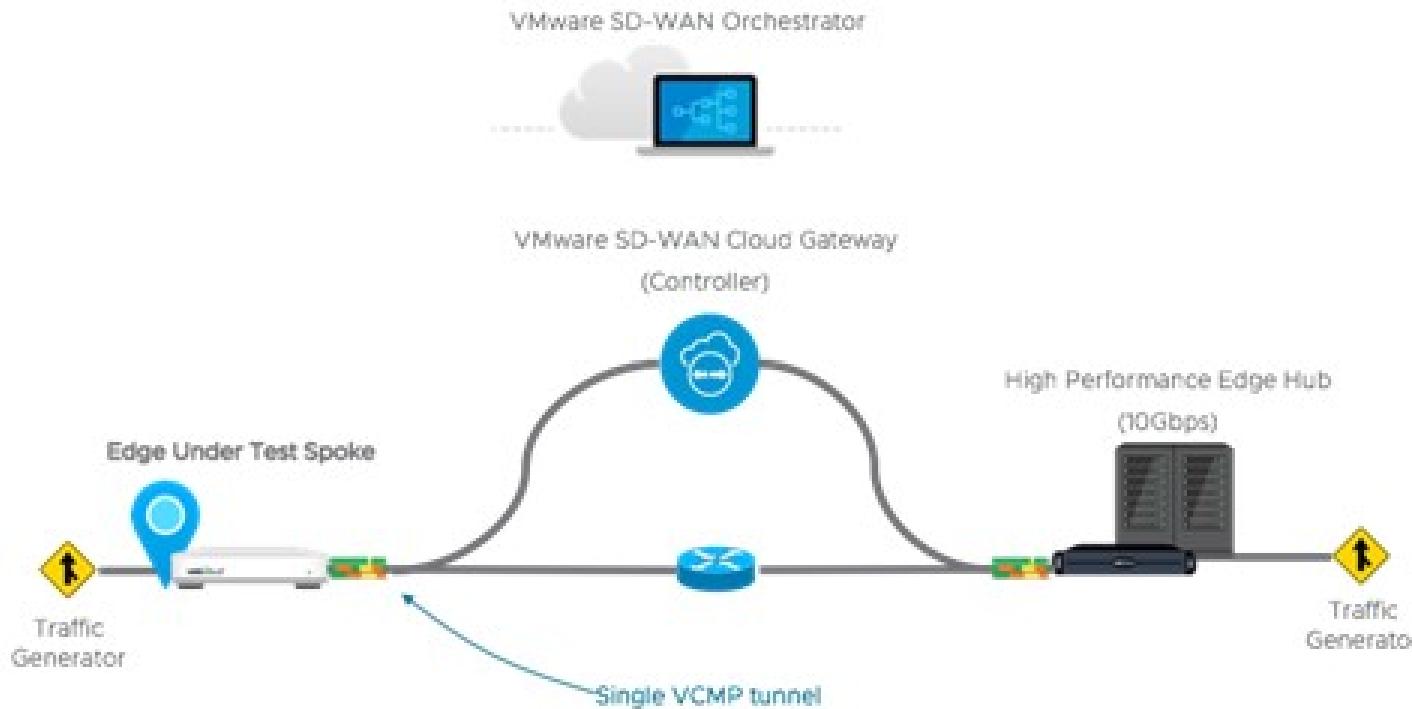
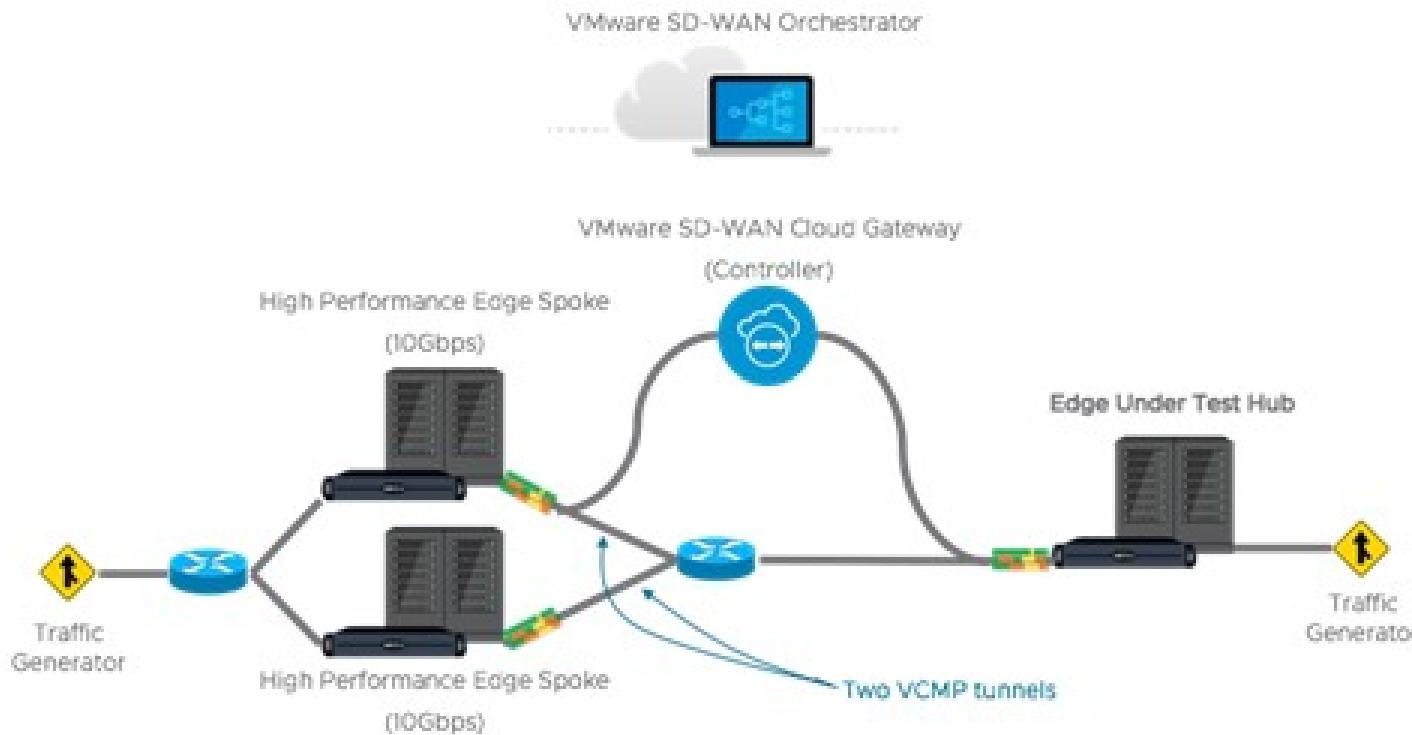


Figure 4-2. FIGURE 2: Throughput performance test topology for devices above 1 Gbps



## Test Methodology

This subsection details the performance and scale test methodology used to derive the results.

### Performance Test Methodology

The testing methodology for Edges uses the industry benchmarking standard RFC 2544 as a framework to execute throughput performance testing. There are specific changes to the type of traffic used and configurations set during testing, described below:

- 1 Performance is measured using a fully operational SD-WAN network overlay (DMPO tunnels) test topology in order to exercise the SD-WAN features and obtain results that can be used to appropriately size WAN networks. Testing is conducted using stateful traffic that establishes multiple flows (connections) and are a mix of well-known applications. The number of flows depends on the platform model being tested. Platforms are divided by expected aggregate performance of under 1 Gbps and over 1 Gbps models. Typically, hundreds of flows are needed to fully exercise and determine max throughput of platforms expected to perform under 1 Gbps, and thousands of flows are used to exercise platforms of over 1 Gbps.

The traffic profiles simulate two network traffic conditions:

- **Large Packet**, a 1300-byte condition.
- **IMIX**, a mix of packet sizes that average to a 417-byte condition.

These traffic profiles are used separately to measure maximum throughput per profile.

- 2 Performance results are recorded at a packet drop rate (PDR) of 0.01%. The PDR mark provides a more realistic performance result which accounts for normal packet drop that may occur within the SD-WAN packet pipeline in the device. A PDR of 0.01% does not impact application experience even in single link deployment scenarios.
  - The device under test is configured with the following DMPO features; IPsec encrypted using AES-128 and SHA1 for hashing, Application Recognition, link SLA measurements, per-packet forwarding. Business Policy is configured to match all traffic as bulk/low priority to prevent DMPO NACK or FEC from executing and incorrectly altering the traffic generator's packet count tracking.

## Test Results

### VMware SD-WAN Edge Performance and Scale Results

Performance metrics are based on the Test Methodology detailed above.

**Switched Port Performance:** VMware SD-WAN Edges are designed to be deployed as gateway routers between the LAN and the WAN. However, the Edges also provide the flexibility of meeting a variety of other deployment topologies. For example, SD-WAN Edges can have their interfaces configured to operate as switched ports—allowing the switching of LAN traffic between various LAN interfaces without the need for an external device.

An Edge with its interfaces configured as switched ports is ideal for small office deployments where high throughput is not required, as the additional layer of complexity required to handle traffic switching reduces the overall performance of the system. For most deployments, VMware recommends using all routed interfaces.

### Note

- The Edge device's **Maximum Throughput** is the sum of throughput across all interfaces of the Edge under test.
- Overall traffic is the “aggregate” of all traffic flows going to and from an Edge device.

**Table 4-4. Physical Edge Appliances using Edge Release 6.0.0**

VMware SD-WAN Edge	510, 510N	510-LTE	520	520V	540
<b>Maximum Throughput Large Packet (1300-byte)</b>					
Routed Mode All Ports	850 Mbps	850 Mbps	850 Mbps	850 Mbps	1.5 Gbps
<b>Maximum Throughput Internet Traffic (IMIX)</b>					
Routed Mode All Ports	300 Mbps	300 Mbps	300 Mbps	300 Mbps	650 Mbps
Routed Mode All Ports with Edge Intelligence activated.	200 Mbps	200 Mbps	200 Mbps	200 Mbps	500 Mbps
Routed Mode All Ports with IPS, Malicious IP Filtering, and Stateful Firewall activated.	150 Mbps	150 Mbps	150 Mbps	150 Mbps	350 Mbps
Routed Mode All Ports with Edge Intelligence, IPS, Malicious IP Filtering, and Stateful Firewall all activated.	150 Mbps	150 Mbps	150 Mbps	150 Mbps	350 Mbps
<b>Other Scale Vectors</b>					
Maximum Tunnel Scale	50	50	50	50	100
Flows Per Second	2,400	2,400	2,400	2,400	4,800
Flows Per Second with Edge Intelligence activated	1,200	1,200	1,200	1,200	1,200
Maximum Concurrent Flows	225K	225K	225K	225K	225K
Maximum Concurrent Flows with Edge Intelligence activated.	110K	110K	110K	110K	110K
Maximum Concurrent Flows with IPS, Malicious IP Filtering, and Stateful Firewall activated.	110K	110K	110K	110K	110K
Maximum Concurrent Flows with Edge Intelligence, IPS, Malicious IP Filtering, and Stateful Firewall activated.	110K	110K	110K	110K	110K
Maximum Number of BGP Routes	100K	100K	100K	100K	100K
Maximum Number of Segments	32	32	32	32	32
Maximum Number of NAT Entries	225K	225K	225K	225K	225K

**Table 4-5.**

VMware SD-WAN Edge	620, 620C, 620N	640, 640C, 640N	680, 680C, 680N	840	2000
<b>Maximum Throughput Large Packet (1300-byte)</b>					
Routed Mode All Ports	1.55 Gbps	5.5 Gbps	8.5 Gbps	6.5 Gbps	15.5 Gbps
<b>Maximum Throughput Internet Traffic (IMIX)</b>					
Routed Mode All Ports	950 Mbps	2.2 Gbps	3.2 Gbps	2.2 Gbps	6.2 Gbps
Routed Mode All Ports with Edge Intelligence activated.	700 Mbps	1.0 Gbps	2.0 Gbps	1.5 Gbps	5.0 Gbps
Routed Mode All Ports with IPS, Malicious IP Filtering, and Stateful Firewall activated.	600 Mbps	800 Mbps	1.5 Gbps	1.0 Gbps	4.0 Gbps
Maximum Concurrent Flows with Edge Intelligence, IPS, Malicious IP Filtering, and Stateful Firewall activated.	600 Mbps	800 Mbps	1.5 Gbps	1.0 Gbps	4.0 Gbps
<b>Other Scale Vectors</b>					
Maximum Tunnel Scale	100	400	800	400	6,000
Flows Per Second	4,800	19,200	19,200	19,200	50,000
Flows Per Second with Edge Intelligence activated	2,400	9,600	9,600	9,600	25,000
Maximum Concurrent Flows	460K	1.15M	1.9M	1.9M	1.9M
Maximum Concurrent Flows with IPS, Malicious IP Filtering, and Stateful Firewall activated.	230K	460K	960K	460K	1.9M
Maximum Concurrent Flows with Edge Intelligence activated	230K	460K	960K	460K	1.0M
Maximum Concurrent Flows with Edge Intelligence, IPS, Malicious IP Filtering, and Stateful Firewall activated.	230K	460K	960K	460K	1.0M
Maximum Number of BGP Routes	100K	100K	100K	100K	100K
Maximum Number of Segments	128	128	128	128	128
Maximum Number of NAT Entries	460K	960K	960K	960K	1.9M

**Note**

- **Large Packet** performance is based on a large packet (1300-byte) payload with AES-128 encryption and DPI turned on.
- **Internet Traffic (IMIX)** performance is based on an average packet size of 417-byte payload with AES-128 encryption and DPI turned on.
- **Edge Intelligence** performance numbers were measured with a 400-byte payload.
- **IPS and Stateful Firewall** performance numbers were measured using TREX setup with an average packet size of 400-bytes.

**Important** **Maximum Tunnel Scale** is understood as the total number of tunnels an Edge model can establish at one time with all other sites. However, the maximum number of tunnels an Edge can establish with another Edge or Gateway is 16, regardless of Edge model or type. Each public WAN link an Edge uses establishes a tunnel with each WAN link the peer Edge or Gateway has.

For example: Edge 1 with public WAN links A, B, C, and D connects to Edge 2 with public WAN links E, F, G, and H. Edge 1's WAN link A establishes a tunnel with each of Edge 2's WAN links E, F, G, and H for a total of 4 tunnels for WAN link A to Edge 2. And this follows for Edge 1's other WAN links B, C, and D. Each establishes tunnels with Edge 2's four public WAN links and so four WAN links with 4 tunnels each results in Edge 1 having 16 total tunnels to Edge 2. In this example, no additional tunnels can be established between the two Edges if an additional WAN link is added to either Edge as the maximum has been reached.

**Tip** Multiple SD-WAN Edges can be deployed in a cluster for multi-gigabit performance.

**Table 4-6. Edge Maximum Throughput When a Firewall VNF is Actively Service Chained:**

Edge Model	520V	620, 620C, 620N	640, 640C, 640N	680, 680C, 680N	840	3400, 3400C
Max. Throughput with FW VNF (1300-byte)	100 Mbps	300 Mbps	600 Mbps	1 Gbps	1 Gbps	2 Gbps

**Table 4-7. Enhanced High-Availability (HA) Link Performance**

Edge Model	510, 510N	510-LTE	520, 520v	540	610, 610C, 610N
Maximum Throughput (IMIX) Across Enhanced HA Link	220 Mbps	220 Mbps	220 Mbps	480 Mbps	220 Mbps
Edge Model	620, 620C, 620N	640, 640C, 640N	680, 680C, 680N	840	2000
Maximum Throughput (IMIX) Across Enhanced HA Link	700 Mbps	1 Gbps	2 Gbps	1 Gbps	4 Gbps

**Note** The default HA interface (GE1) is ~800 Mbps for Edge 510, 610, and 620 models. In Release 5.2 and later, any Edge interface can be used as the HA interface, including the 10G interface.

**Important** **Performance with Edge Intelligence activated:**

- There is a performance impact of up to 20% when analytics are activated.
- Flow capacity is reduced by half when analytics are activated due to the additional memory and processing required for analysis.

## Platform Independent Edge Scale Numbers

The Edge Scale numbers listed in the following table are platform independent and are valid for all Edge models, both hardware and virtual.

**Note** The listed maximum value for each feature represents the supported limits that have been tested and verified by VMware. In some cases, customers may exceed values higher than that is listed in the table. If a customer exceeds the published maximum value, the environment may work, but VMware cannot guarantee that it would.

Feature	Supported Number	
	IPv4	IPv6
Maximum number of Port Forwarding rules on a single segment	128	128
Maximum number of Port Forwarding rules across 16 segments	128	128
Maximum number of Port Forwarding rules across 128 segments	128	128
Maximum number of Outbound Firewall Rules on a single segment	2040	2040
Maximum number of Outbound Firewall Rules across 16 segments	2040	2040
Maximum number of Outbound Firewall Rules across 128 segments	2040	2040
Maximum number of 1:1 NAT rules on a single segment	128	128
Maximum number of 1:1 NAT rules across 16 segments	128	128
Maximum number of 1:1 NAT rules across 128 segments	128	128
Maximum number of LAN side NAT rules on a single segment	256	-
Maximum number of LAN side NAT rules across 16 segments	256	-
Maximum number of LAN side NAT rules across 128 segments	256	-
Maximum number of Object Groups (1000 business policies, each business policy assigned to one object group, each object group supports 255 address groups)	1000	1000

## Virtual Edge

Table 4-8. Private Cloud (Hypervisors)

Edge Device	Maximum Throughput	Maximum Number of Tunnels	Flows Second	Per	Maximum Concurrent Flows
ESXi Virtual Edge (2-core, VMXNET3)	1.5 Gbps (1300-byte) 900 Mbps (IMIX)	50	2400		240K
KVM Virtual Edge (2-core, Linux Bridge)	800 Mbps (1300-byte) 250 Mbps (IMIX)	50	2400		240K

**Table 4-8. Private Cloud (Hypervisors) (continued)**

<b>Edge Device</b>	<b>Maximum Throughput</b>	<b>Maximum Number of Tunnels</b>	<b>Flows Second Per</b>	<b>Maximum Concurrent Flows</b>
KVM Virtual Edge (2-core, SR-IOV)	1.5 Gbps (1300-byte) 900 Mbps (IMIX)	50	2400	240K
ESXi Virtual Edge (4-core, VMXNET3)	4 Gbps (1300-byte) 1.5 Gbps (IMIX)	400	4800	480K
ESXi Virtual Edge (4-core, SR-IOV)	5 Gbps (1300-byte) 1.5 Gbps (IMIX)	400	4800	480K
KVM Virtual Edge (4-core, Linux Bridge)	1 Gbps (1300-byte) 350 Mbps (IMIX)	400	4800	480K
KVM Virtual Edge (4-core, SR-IOV)	4 Gbps (1300-byte) 1.5 Gbps (IMIX)	400	4800	480K
ESXi Virtual Edge (8-core, VMXNET3)	6 Gbps (1300-byte) 2 Gbps (IMIX)	800	28800	1.9M
ESXi Virtual Edge (8-core, SR-IOV)	6 Gbps (1300-byte) 3 Gbps (IMIX)	800	28800	1.9M
KVM Virtual Edge (8-core, SR-IOV)	6.5 Gbps (1300-byte) 3.2 Gbps (IMIX)	800	28800	1.9M

	<b>2 vCPU</b>	<b>4vCPU</b>	<b>8vCPU</b>	<b>10vCPU</b>
Minimum Memory (DRAM)	8 GB	16 GB	32 GB	32 GB
Minimum Storage	8 GB	8 GB	16 GB	16 GB
Supported Hypervisors	Software version 4.0 and above: <ul style="list-style-type: none"> <li>■ ESXi 6.5U1, 6.7U1, 7.0</li> <li>■ KVM Ubuntu 16.04 and 18.04</li> </ul>			
Supported Public Cloud	AWS, Azure, GCP, and Alibaba			

	2 vCPU	4vCPU	8vCPU	10vCPU
Support Network I/O	SR-IOV, VirtIO, VMXNET3			
Recommended Host Settings	<p>CPU settings at 2.0 GHz or higher</p> <p>CPU configuration:</p> <ul style="list-style-type: none"> <li>■ AES-NI activated.</li> <li>■ Power savings deactivated</li> <li>■ CPU turbo activated</li> <li>■ Hyper-threading deactivated</li> <li>■ Minimum instructions sets: SSE3, SSE4, and RDTSC.</li> <li>■ Recommended instruction sets: AVX2 or AVX512</li> </ul> <p>VMware ESXi required settings:</p> <ul style="list-style-type: none"> <li>■ CPU reservation: Maximum</li> <li>■ CPU shares: High</li> <li>■ Memory reservation: Maximum</li> <li>■ Latency sensitivity: High</li> </ul>			

**Note** Performance metrics are based on a system using an Intel® Xeon® CPU E5-2683 v4 at 2.10 GHz (AES-NI).

## Public Cloud

Table 4-9. Amazon Web Services (AWS)

AWS Instance Type	c5.large	c5.xlarge	c5.2xlarge
Maximum Throughput	100 Mbps (1300-byte) 50 Mbps (IMIX)	200 Mbps (1300-byte) 100 Mbps (IMIX)	1.5 Gbps (1300-byte) 450 Mbps (IMIX)
Maximum Tunnels	50	400	800
Flows Per Second	1,200	2,400	4,800
Maximum Concurrent Flows	125,000	250,000	550,000
Maximum Number of Routes	35,000	35,000	35,000
Maximum Number of Segments	128	128	128

**Note** c5.2xlarge and c5.4xlarge performance and scale numbers are based on AWS Enhanced Networking (ENA SR-IOV drivers) being ‘activated’.

Table 4-10. Microsoft Azure (Without Accelerated Networking)

Azure VM Series	D2d v4	D4d v4	D8d v4
Maximum Throughput	100 Mbps (1300-byte) 50 Mbps (IMIX)	200 Mbps (1300-byte) 100 Mbps (IMIX)	1 Gbps (1300-byte) 450 Mbps (IMIX)
Maximum Tunnels	50	400	800

**Table 4-10. Microsoft Azure (Without Accelerated Networking) (continued)**

Azure VM Series	D2d v4	D4d v4	D8d v4
Flows Per Second	1,200	2,400	4,800
Maximum Concurrent Flows	125,000	250,000	550,000
Maximum Number of Routes	35,000	35,000	35,000
Maximum Number of Segments	128	128	128

**Table 4-11. Microsoft Azure (With Accelerated Networking)**

Azure VM Series	Ds3 v2	Ds4 v2	Ds5 v2
Maximum Throughput	2.5 Gbps (1300-byte) 1.5 Gbps (IMIX)	5.3 Gbps (1300-byte) 2.7 Gbps (IMIX)	6.5 Gbps (1300-byte) 3.1 Gbps (IMIX)
Maximum Tunnels	400	800	2000
Flows Per Second	2,400	4,800	4,800
Maximum Concurrent Flows	250,000	550,000	550,000
Maximum Number of Routes	35,000	35,000	35,000
Maximum Number of Segments	128	128	128

**Note**

- Azure Accelerated Networking is supported only from release 5.4.0.
- Accelerated Networking is supported only on Connect-X4 and Connect-X5 NICs.

**Table 4-12. Google Cloud Platform**

GCP Instance Type	n2-highcpu-4	n2-highcpu-8	n2-highcpu-16
Maximum Throughput	850 Mbps (1300-byte) 500 Mbps (IMIX)	4.5 Gbps (1300-byte) 1.6 Gbps (IMIX)	6.5 Gbps (1300-byte) 1.9 Gbps (IMIX)
Maximum Tunnels	50	400	800
Flows Per Second	1,200	2,400	4,800
Maximum Concurrent Flows	125,000	250,000	550,000
Maximum Number of Routes	35,000	35,000	35,000
Maximum Number of Segments	128	128	128

## Use of DPDK on VMware SD-WAN Edges

To improve packet throughput performance, VMware SD-WAN Edges take advantage of Data Plane Development Kit (DPDK) technology. DPDK is a set of data plane libraries and drivers provided by Intel for offloading TCP packet processing from the operating system kernel to processes running in user space and results in higher packet throughput. For more details, see <https://www.dpdk.org/>.

Edge hardware models 620 and higher and all virtual Edges use DPDK by default on their routed interfaces. Edges do not use DPDK on their switched interfaces. A user cannot activate or deactivate DPDK for an Edge interface.

## Capabilities

This section describes VMware SD-WAN capabilities.

### Dynamic Multi-path Optimization

VMware SD-WAN Dynamic Multi-path Optimization is comprised of automatic link monitoring, dynamic link steering and on-demand remediation.

### Link Steering and Remediation

Dynamic, application aware per-packet link steering is performed automatically based on the business priority of the application, embedded knowledge of network requirements of the application, and the real-time capacity and performance of each link. On-demand mitigation of individual link degradation through forward error correction, jitter buffering and negative acknowledgment proxy also protects the performance of priority and network sensitive applications. Both the dynamic per-packet link steering and on-demand mitigation combine to deliver robust, sub-second blocked and limited protection to improve application availability, performance and end user experience.

### Cloud VPN

Cloud VPN is a 1-click, site-to-site, VPNC-compliant, IPsec VPN to connect VMware SD-WAN and Non SD-WAN Destinations while delivering real-time status and the health of the sites. The Cloud VPN establishes dynamic edge-to-edge communication for all branches based on service level objectives and application performance. Cloud VPN also delivers secure connectivity across all branches with PKI scalable key management. New branches join the VPN network automatically with access to all resources in other branches, enterprise data centers, and 3rd party data centers, like Amazon AWS.

## Firewall

VMware SD-WAN delivers stateful and context-aware (application, user, device) integrated application aware firewall with granular control of sub-applications, support for protocol-hopping applications – such as Skype and other peer-to-peer applications (for example, turn off Skype video and chat, but allow Skype audio). The secure firewall service is user- and device OS-aware with the ability to separate voice, video, data, and compliance traffic. Policies for BYOD devices (such as Apple iOS, Android, Windows, and Mac OS) on the corporate network are easily controlled.

## Network Service Insertion

The VMware SD-WAN Solution supports a platform to host multiple virtualized network functions to eliminate single-function appliances and reduce branch IT complexity. VMware SD-WAN service-chains traffic from the branch to both cloud-based and enterprise regional hub services, with assured performance, security, and manageability. Branches leverage consolidated security and network services, including those from partners like Zscaler and Websense. Using a simple click-to-enable interface, services can be inserted in the cloud and on-premise with application specific policies.

## Activation

SD-WAN Edge appliances automatically authenticate, connect, and receive configuration instructions once they are connected to the Internet in a zero-touch deployment. They deliver a highly available deployment with SD-WAN Edge redundancy protocol and integrate with the existing network with support for OSPF and BGP routing protocols and benefit from dynamic learning and automation.

## Overlay Flow Control

The SD-WAN Edge learns routes from adjacent routers through OSPF and BGP. It sends the learned routes to the Gateway/Controller. The Gateway/Controller acts like a route reflector and sends the learned routes to other SD-WAN Edge. The Overlay Flow Control (OFC) allows enterprise-wide route visibility and control for ease of programming and for full and partial overlay.

## OSPF

VMware SD-WAN supports inbound/outbound filters to OSPF neighbors, OE1/OE2 route types, MD5 authentication. Routes learned through OSPF will be automatically redistributed to the controller hosted in the cloud or on-premise.

## BGP

VMware SD-WAN supports inbound/outbound filters that can be set to Deny, or optionally add/change the BGP attribute to influence the path selection, that is RFC 1998 community, MED, AS-Path prepend, and local preference.

## Segmentation

Network segmentation is an important feature for both enterprises and service providers. In the most basic form, segmentation provides network isolation for management and security reasons. Most common forms of segmentation are VLANs for L2 and VRFs for L3.

### Typical Use Cases for Segmentation:

- Line of Business Separation: Engineering, HR etc. for Security/Audit
- User Data Separation: Guest, PCI, Corporate traffic separation
- Enterprise uses overlapping IP addresses in different VRFs

However, the legacy approach is limited to a single box or two physically connected devices. To extend the functionality, segmentation information must be carried across the network.

VMware SD-WAN allows end-to-end segmentation. When the packet traverses through the Edge, the Segment ID is added to the packet and is forwarded to the Hub and cloud Gateway, allowing network service isolation from the Edge to the cloud and data center. This provides the ability to group prefixes into a unique routing table, making the business policy segment aware.

## Routing

In Dynamic Routing, SD-WAN Edge learns routes from adjacent routers through OSPF or BGP. The SASE Orchestrator maintains all the dynamically learned routes in a global routing table called the Overlay Flow Control (OFC). The Overlay Flow Control allows management of dynamic routes in the case of "Overlay Flow Control sync" and "change in Inbound/Outbound filtering configuration." The change in inbound filtering for a prefix from IGNORE to LEARN would fetch the prefix from the Overlay Flow Control and install into the Unified routing table.

For more information, see [Chapter 33 Configure Dynamic Routing with OSPF or BGP](#).

## Business Policy Framework

Quality of Service (QoS), resource allocations, link/path steering, and error correction are automatically applied based on business policies and application priorities. Orchestrate traffic based on transport groups defined by private and public links, policy definition, and link characteristics.

## Tunnel Overhead and MTU

VMware, like any overlay, imposes additional overhead on traffic that traverses the network. This section first describes the overhead added in a traditional IPsec network and how it compares with VMware, which is followed by an explanation of how this added overhead relates to MTU and packet fragmentation behaviors in the network.

## IPsec Tunnel Overhead

In a traditional IPsec network, traffic is usually carried in an IPsec tunnel between endpoints. A standard IPsec tunnel scenario (AES 128-bit encryption using ESP [Encapsulating Security Payload]) when encrypting traffic, results in multiple types of overhead as follows:

- **Padding**

- AES encrypts data in 16-byte blocks, referred to as "block" size.
- If the body of a packet is smaller than or indivisible by block size, it is padded to match the block size.
- Examples:
  - A 1-byte packet will become 16-bytes with 15-bytes of padding.
  - A 1400-byte packet will become 1408-bytes with 8-bytes of padding.
  - A 64-byte packet does not require any padding.

- **IPsec headers and trailers:**

- UDP header for NAT Traversal (NAT-T).
- IP header for IPsec tunnel mode.
- ESP header and trailer.

Element	Size in Bytes
IP Header	20
UDP Header	8
IPsec Sequence Number	4
IPsec SPI	4
Initialization Vector	16
Padding	0 – 15
Padding Length	1
Next Header	1
Authentication Data	12
<b>Total</b>	<b>66-81</b>

---

**Note** The examples provided assume at least one device is behind a NAT device. If no NAT is used, then IPsec overhead is 20-bytes less, as NAT-T is not required. There is no change to the behavior of VMware regardless of whether NAT is present or not (NAT-T is always activated).

---

## VMware Tunnel Overhead

To support Dynamic Multipath Optimization™ (DMPO), VMware encapsulates packets in a protocol called the VeloCloud Multipath Protocol (VCMP). VCMP adds 31-bytes of overhead for user packets to support resequencing, error correction, network analysis, and network segmentation within a single tunnel. VCMP operates on an IANA-registered port of UDP 2426. To ensure consistent behavior in all potential scenarios (unencrypted, encrypted and behind a NAT, encrypted but not behind a NAT), VCMP is encrypted using transport mode IPsec and forces NAT-T to be true with a special NAT-T port of 2426.

Packets sent to the Internet via the SD-WAN Gateway are not encrypted by default, since they will egress to the open Internet upon exiting the Gateway. As a result, the overhead for Internet Multipath traffic is less than VPN traffic.

---

**Note** Service Providers have the option of encrypting Internet traffic via the Gateway, and if they elect to use this option, the “VPN” overhead applies to Internet traffic as well.

---

### VPN Traffic

Element	Size in Bytes
IP Header	20
UDP Header	8
IPsec Sequence Number	4
IPsec SPI	4
VCMP Header	23
VCMP Data Header	8
Initialization Vector	16
Padding	0 – 15
Padding Length	1
Next Header	1
Authentication Data	12
<b>Total</b>	<b>97 – 112</b>

### Internet Multipath Traffic

Element	Size in Bytes
IP Header	20
UDP Header	8
VCMP Header	23

Element	Size in Bytes
VCMP Data Header	8
<b>Total</b>	59

## Impact of IPv6 Tunnel on MTU

VMware SD-WAN supports IPv6 addresses to configure the Edge Interfaces and Edge WAN Overlay settings.

The VCMP tunnel can be setup in the following environments: IPv4 only, IPv6 only, and dual stack. For more information, see [IPv6 Settings](#).

When a branch has at least one IPv6 tunnel, DMPO uses this tunnel seamlessly along with other IPv4 tunnels. The packets for any specific flow can take any tunnel, IPv4 or IPv6, based on the real time health of the tunnel. An example for specific flow is path selection score for load balanced traffic. In such cases, the increased size for IPv6 header (additional 20 bytes) should be taken into account and as a result, the effective path MTU will be less by 20 bytes. In addition, this reduced effective MTU will be propagated to the other remote branches through Gateway so that the incoming routes into this local branch from other remote branches reflect the reduced MTU.

## Path MTU Discovery

After it is determined how much overhead will be applied, the SD-WAN Edge must discover the maximum permissible MTU to calculate the effective MTU for customer packets. To find the maximum permissible MTU, the Edge performs Path MTU Discovery:

- For public Internet WAN links:
  - Path MTU discovery is performed to all Gateways.
  - The MTU for all tunnels will be set to the minimum MTU discovered.
- For private WAN links:
  - Path MTU discovery is performed to all other Edges in the customer network.
  - The MTU for each tunnel is set based on the results of Path MTU discovery.

The Edge will first attempt RFC 1191 Path MTU discovery, where a packet of the current known link MTU (Default: 1500 bytes) is sent to the peer with the "Don't Fragment" (DF) bit set in the IP header. If this packet is received on the remote Edge or Gateway, an acknowledgement packet of the same size is returned to the Edge. If the packet cannot reach the remote Edge or Gateway due to MTU constraints, the intermediate device is expected to send an ICMP destination unreachable (fragmentation needed) message. When the Edge receives the ICMP unreachable message, it will validate the message (to ensure the MTU value reported is sane) and once validated, adjust the MTU. The process then repeats until the MTU is discovered.

In some cases (for example, USB LTE dongles), the intermediate device will not send an ICMP unreachable message even if the packet is too large. If RFC 1191 fails (the Edge did not receive an acknowledgement or ICMP unreachable), it will fall back to RFC 4821 Packetization Layer Path MTU Discovery. The Edge will attempt to perform a binary search to discover the MTU.

When an MTU is discovered for a peer, all tunnels to this peer are set to the same MTU. That means that if an Edge has one link with an MTU of 1400 bytes and one link with an MTU of 1500 bytes, all tunnels will have an MTU of 1400 bytes. This ensures that packets can be sent on any tunnel at any time using the same MTU. We refer to this as the **Effective Edge MTU**. Based on the destination (VPN or Internet Multipath) the overhead outlined above is subtracted to compute the **Effective Packet MTU**. For Direct Internet or other underlay traffic, the overhead is 0 bytes, and because link failover is not required, the effective Packet MTU is identical to the discovered WAN Link MTU.

---

**Note** RFC 4821 Packetization Layer Path MTU Discovery will measure MTU to a minimum of 1300 bytes. If your MTU is less than 1300 bytes, you must manually configure the MTU.

---

## VPN Traffic and MTU

Now that the SD-WAN Edge has discovered the MTU and calculated the overheads, an effective MTU can be computed for client traffic. The Edge will attempt to enforce this MTU as efficiently as possible for the various potential types of traffic received.

### TCP Traffic

The Edge automatically performs TCP MSS (Maximum Segment Size) adjustment for TCP packets received. As SYN and SYN|ACK packets traverse the Edge, the MSS is rewritten based on the Effective Packet MTU.

### Non-TCP Traffic without DF bit set

If the packet is larger than the Effective Packet MTU, the Edge automatically performs IP fragmentation as per RFC 791.

### Non-TCP Traffic with DF bit set

If the packet is larger than the Effective Packet MTU:

- The first time a packet is received for this flow (IP 5-tuple), the Edge drops the packet and sends an ICMP Destination unreachable (fragmentation needed) as per RFC 791.
- If subsequent packets are received for the same flow which are still too large, these packets are fragmented into multiple VCMP packets and reassembled transparently before handoff at the remote end.

## Jumbo Frame Limitation

VMware SD-WAN does not support jumbo frames as of Release 5.0. The maximum IP MTU supported for packets sent across the overlay without fragmentation is 1500.

# Network Topologies

This section describes network topologies for branches and data centers.

## Branches to Private Third Party (VPN)

Customers with a private data center or cloud data center often want a way to include it in their network without having to define a tunnel from each individual branch office site to the data center. By defining the site as a Non SD-WAN Destination, a single tunnel will be built from the nearest SD-WAN Gateway to the customer's existing router or firewall. All the SD-WAN Edges that need to talk to the site will connect to the same SD-WAN Gateway to forward packets across the tunnel, simplifying the overall network configuration and new site bring up.

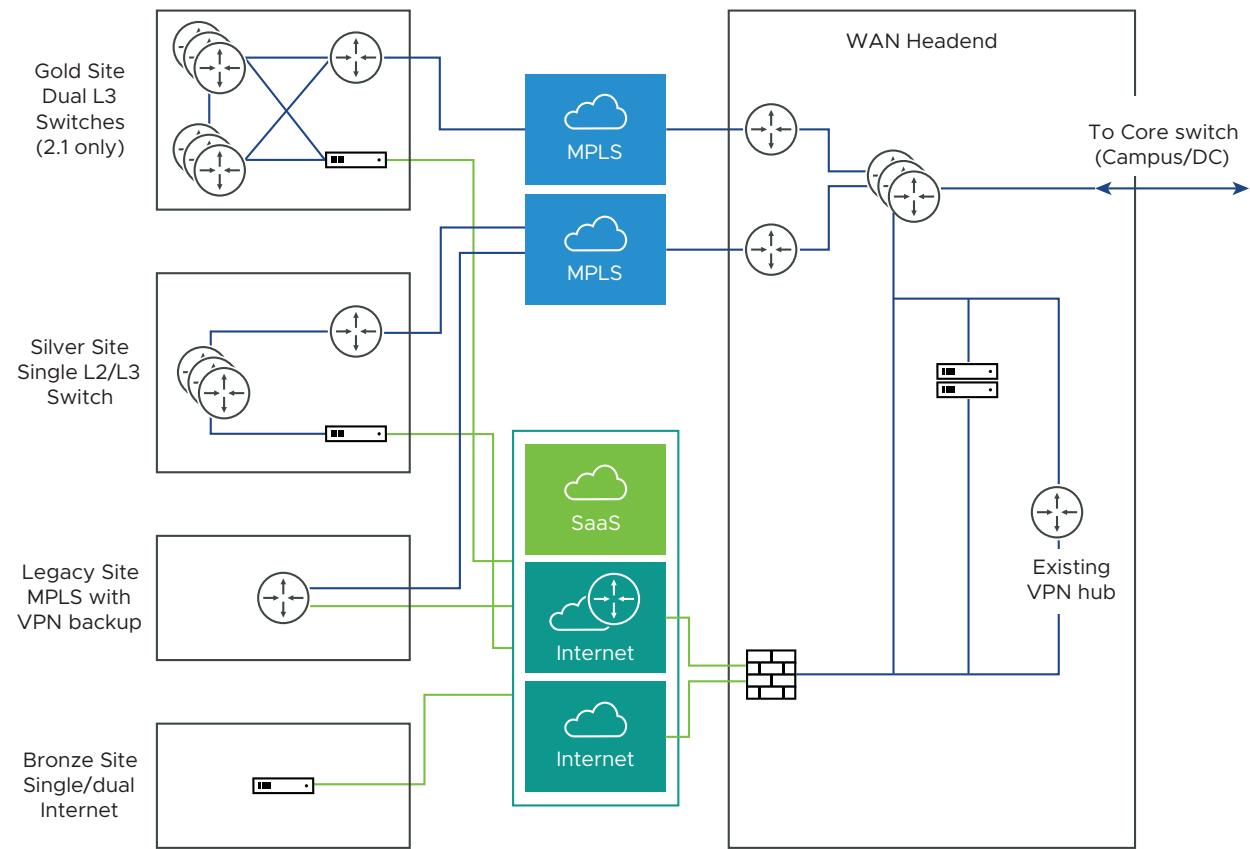


VMware simplifies the branch deployment and delivers enterprise great application performance or public/private link for cloud and/or on-premise applications.

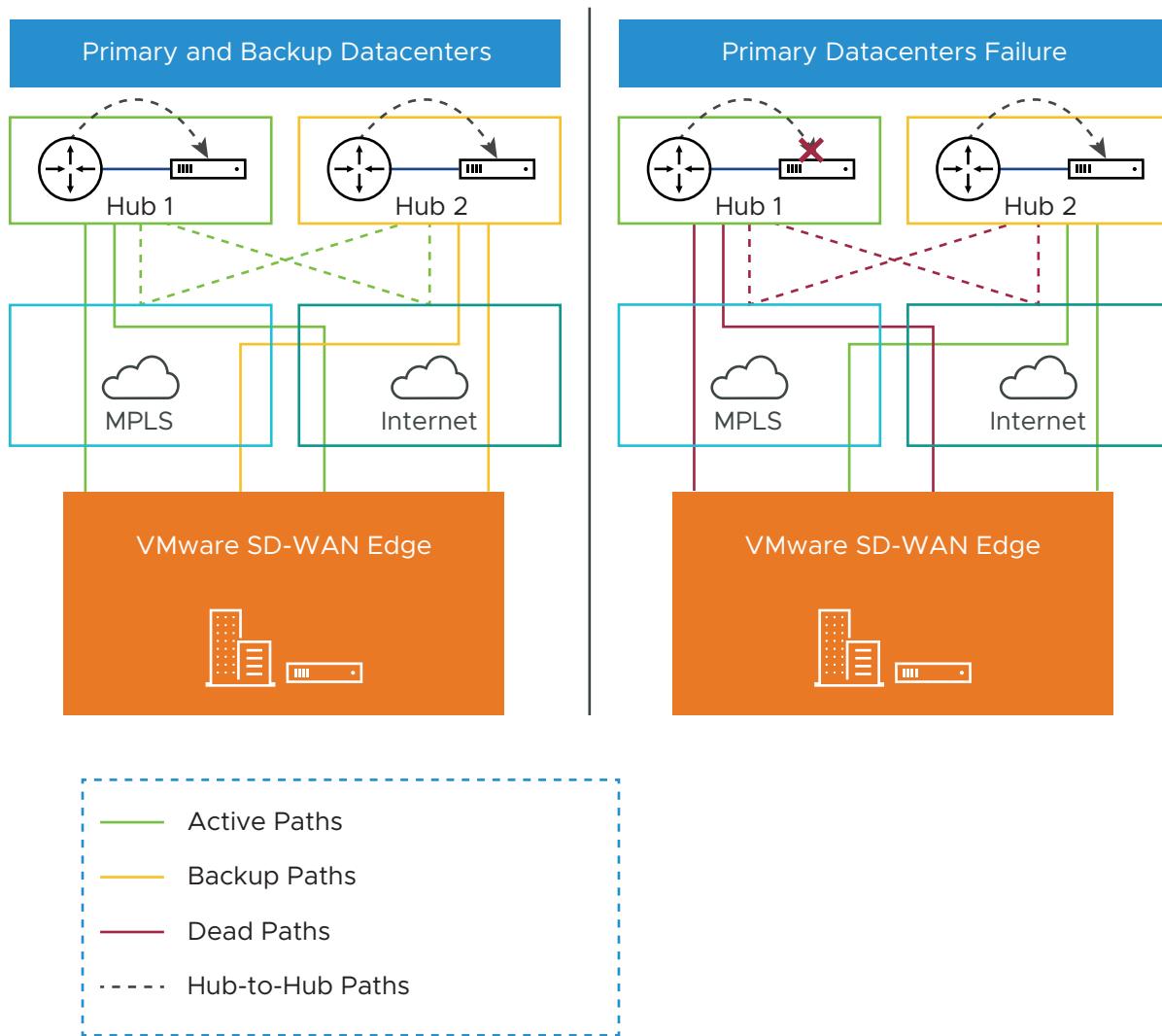
## Data Center Network Topology

The Data Center Network topology consists of two hubs and multiple branches, with or without SD-WAN Edge. Each hub has hybrid WAN connectivity. There are several branch types.

The MPLS network runs BGP and peers with all the CE routers. At Hub 1, Hub 2, and Silver 1 sites, the L3 switch runs OSPF, or BGP with the CE router and firewall (in case of hub sites).



In some cases, there may be redundant data centers which advertise the same subnets with different costs. In this scenario, both data centers can be configured as edge-to-edge VPN hubs. Since all edges connect directly to each hub, the hubs in fact also connect directly to each other. Based on route cost, traffic is steered to the preferred active data center.



In previous versions, users could create an enterprise object using Zscaler or Palo Alto Network as a generic Non SD-WAN Destination. In 4.0 version, that object will now become a first-class citizen as a Non SD-WAN Destination.

The Cloud-Delivered solution of VMware combines the economics and flexibility of the hybrid WAN with the deployment speed and low maintenance of cloud-based services. It dramatically simplifies the WAN by delivering virtualized services from the cloud to branch offices. VMware customer-premise equipment, SD-WAN Edge, aggregates multiple broadband links (e.g., Cable, DSL, 4G-LTE) at the branch office, and sends the traffic to SD-WAN Gateways. Using cloud-based orchestration, the service can connect the branch office to any type of data center: enterprise, cloud, or Software-as-a-Service.

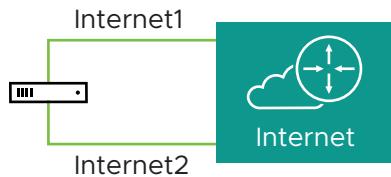
SD-WAN Edge is a compact, thin Edge device that is zero-IT-touch provisioned from the cloud for secure, optimized connectivity to applications and data. A cluster of gateways is deployed globally at top-tier cloud data centers to provide scalable and on-demand cloud network services. Working with the Edge, the cluster delivers Dynamic Multi-path Optimization so multiple, ordinary broadband links appear as a single, high bandwidth link. Orchestrator management provides centralized configuration, real-time monitoring, and one-click provisioning of virtual services.

## Branch Site Topologies

The VMware service defines two or more different branch topologies designated as Bronze, Silver, and Gold. In addition, pairs of SD-WAN Edges can be configured in a High Availability (HA) configuration at a branch location.

### Bronze Site Topology

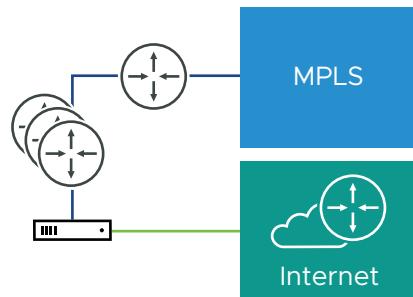
The Bronze topology represents a typical small site deployment where there are one or two WAN links connected to the public internet. In the Bronze topology, there is no MPLS connection and there is no L3 switch on the LAN-side of the SD-WAN Edge. The following figure shows an overview of the Bronze topology.



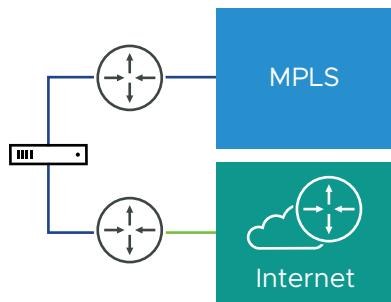
### Silver Site Topology

The Silver topology represents a site that also has an MPLS connection, in addition to one or more public Internet links. There are two variants of this topology.

The first variant is a single L3 switch with one or more public internet links and an MPLS link, which is terminated on a CE and is accessible through the L3 switch. In this case, the SD-WAN Edge goes between the L3 switch and Internet (replacing existing firewall/router).

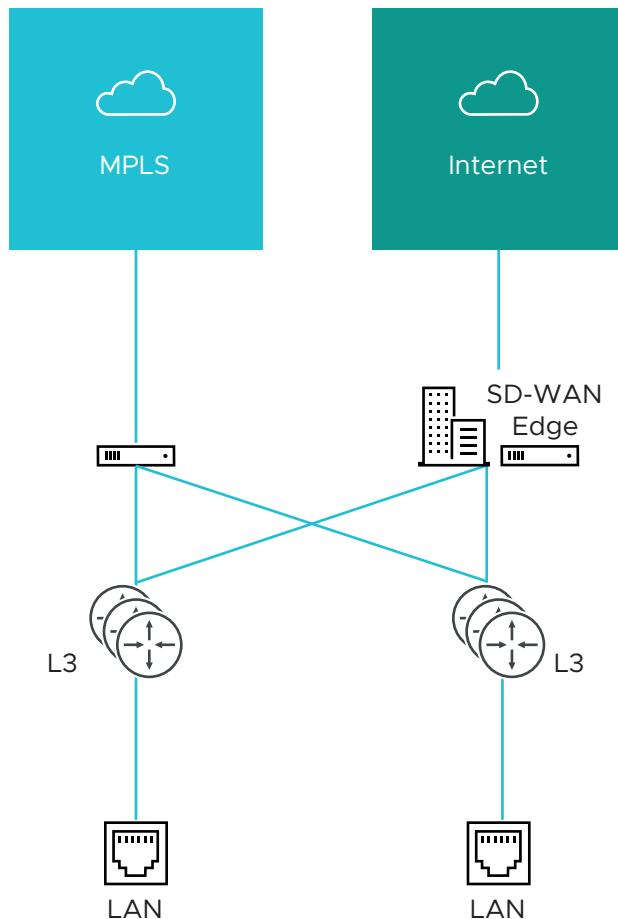


The second variant includes MPLS and Internet routers deployed using either Cisco's Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) using a different router vendor, with an L2 switch on the LAN side. In this case, the SD-WAN Edge replaces the L2 switch.

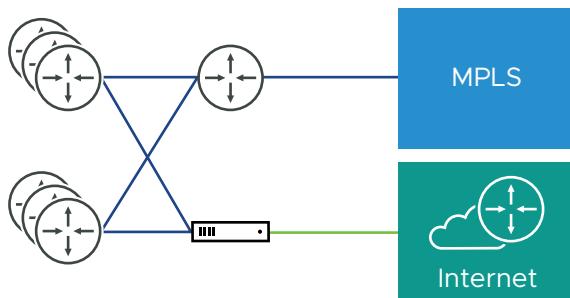


## Gold Site Topology

The Gold topology is a typical large branch site topology. The topology includes active/active L3 switches which communicate routes using OSPF or BGP, one or more public internet links and a MPLS link which is terminated on a CE router that is also talking to OSPF or BGP and is accessible through the L3 switches.



A key differentiation point here is a single WAN link is accessible via two routed interfaces. To support this, a virtual IP address is provisioned inside the edge and can be advertised over OSPF, BGP, or statically routed to the interfaces.



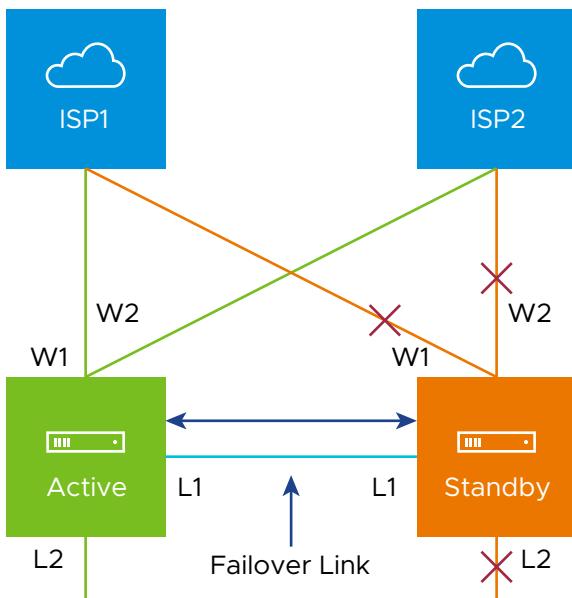

---

**Note** The Gold Site is not currently in the scope of this release and will be added at a later time.

---

## High Availability (HA) Configuration

The following figure provides a conceptual overview of the VMware High Availability configuration using two SD-WAN Edges, one active and one standby.



Connecting the L1 ports on each edge is used to establish a failover link. The standby SD-WAN Edge blocks all ports except the L1 port for the failover link.

## Roles and Privilege Levels

VMware has pre-defined roles with different set of privileges.

- IT Administrator (or Administrator)
- Site Contact at each site where an SD-WAN Edge device is deployed

- IT Operator (or Operator)
- IT Partner (or Partner)

## Administrator

The Administrator configures, monitors, and administers the VMware service operation. There are three Administrator roles:

Administrator Role	Description
Enterprise Standard Admin	Can perform all configuration and monitoring tasks.
Enterprise Superuser	Can perform the same tasks as an Enterprise Standard Admin and can also create additional users with the Enterprise Standard Admin, Enterprise MSP, and Customer Support role.
Enterprise Support	Can perform configuration review and monitoring tasks but cannot view user identifiable application statistics and can only view configuration information.

---

**Note** An Administrator should be thoroughly familiar with networking concepts, web applications, and requirements and procedures for the Enterprise.

---

## Site Contact

The **Site Contact** is responsible for SD-WAN Edge physical installation and activation with the VMware service. The Site Contact is a non-IT person who can receive an email and perform the instructions in the email for Edge activation.

## Operator

The Operator can perform all the tasks that an Administrator can perform, plus additional operator-specific tasks – such as create and manage customers, Cloud Edges, and Gateways. There are four Operator roles:

Operator Role	Description
Standard Operator	Can perform all configuration and monitoring tasks.
Superuser Operator	Can view and create additional users with the Operator roles.
Business Specialist Operator	Can create and manage customer accounts.
Customer Support Operator	Can monitor Edges and activity.

An Operator should be thoroughly familiar with networking concepts, web applications, and requirements and procedures for the Enterprise.

## Partner

The **Partner** can perform all the tasks that an Administrator can perform, along with additional Partner specific tasks – such as creating and managing customers. There are four Partner roles:

<b>Partner Role</b>	<b>Description</b>
Standard Admin	Can perform all configuration and monitoring tasks.
Superuser	Can view and create additional users with the Partner roles.
Business Specialist	Can perform configuration and monitoring tasks but cannot view user identifiable application statistics.
Customer Support	Can perform configuration review and monitoring tasks but cannot view user identifiable application statistics and can only view configuration information.

A Partner should be thoroughly familiar with networking concepts, web applications, and requirements and procedures for the Enterprise.

## User Role Matrix

This section describes feature access according to VMware user roles.

### Operator-level SASE Orchestrator Features User Role Matrix

The following table lists the Operator-level user roles that have access to the SASE Orchestrator features.

- R: Read
- W: Write (Modify/Edit)
- D: Delete
- NA: No Access

<b>SASE Orchestrator Feature</b>	<b>Partner:</b>								
	<b>Operator:</b> Superuser Operator	<b>Operator:</b> Standard Operator	<b>Partner:</b> Business Specialist	<b>Customer Support Operator</b>	<b>Super User</b>	<b>Standard Admin</b>	<b>Business Specialist</b>	<b>Customer Support</b>	
Monitor Customers	R	R	R	R	R	R	R	R	
Manage Customers	RWD	RWD	RWD	R	RWD	RWD	RWD	R	
Manage Partners	RWD	RWD	RWD	R	NA	NA	NA	NA	
(Managing Edge) Software Images	RWD	RWD	R	R	*See Note	*See Note	*See Note	*See Note	
System Properties	RWD	R	NA	R	NA	NA	NA	NA	
Operator Events	R	R	NA	R	NA	NA	NA	NA	
Operator Profiles	RWD	RWD	R	R	NA	NA	NA	NA	

SASE Orchestrator Feature	Operator: Superuser Operator	Operator: Standard Operator	Partner: Business Specialist	Partner:				
				Customer Support Operator	Super User	Standard Admin	Business Specialist	Customer Support
Operator Users	RWD	R	R	R	NA	NA	NA	NA
Gateway Pools	RWD	RW	R	R	RWD	RWD	NA	R
Gateways	RWD	RWD	R	R	RW	RW	NA	R
Gateway Diagnostic Bundle	RWD	RWD	R	R	NA	NA	NA	NA
Application Maps	RWD	RWD	R	R	NA	NA	NA	NA
CA Summary	RW	R	R	R	NA	NA	NA	NA
Orchestrator Authentication	RWD	R	NA	R	NA	NA	NA	NA
Replication	RW	R	NA	R	NA	NA	NA	NA

**Note** Operator superusers have "RWD" access to certificate related configurations and standard operators have Read-only access to certificate related configurations. These users can access the certificate related configurations at **Configure > Edges** from the navigation panel.\*

**Note** Enterprise users at all levels do not have access to the Operator-level features.

## Partner-level SASE Orchestrator Features User Role Matrix

The following table lists the Partner-level user roles that have access to the SASE Orchestrator features.

- R: Read
- W: Write (Modify/Edit)
- D: Delete
- NA: No Access

SASE Orchestrator Feature	Partner: Superuser	Partner: Standard Admin			Business Specialist	Customer Support
		Admin				
Monitor Customers	R	R			R	R
Manage Customers	RWD	RWD			RWD	R
Events	R	R			NA	R
Admins	RWD	R			NA	R
Overview	R	R			R	R

SASE Orchestrator Feature	Partner: Superuser	Partner: Standard Admin	Business Specialist	Customer Support
Settings	RW	R	R	R
Gateway Pools	RW	RWD	NA	R
Gateways	RW	RW	NA	R

## Enterprise-level SASE Orchestrator Features User Role Matrix

The following table lists the Enterprise-level user roles that have access to the SASE Orchestrator features.

- R: Read
- W: Write (Modify/Edit)
- D: Delete
- NA: No Access

SASE Orchestrator Feature	Enterprise: Super User	Enterprise: Standard Admin	Customer Support	Read Only
Monitor > Edges	R	R	R	R
Monitor > Network Services	R	R	R	R
Monitor > Routing	R	R	R	NA
Monitor > Alerts	R	R	R	NA
Monitor > Events	R	R	R	NA
Monitor > Reports	RWD	RWD	R	R
Configure > Edges	RWD	RWD	R	NA
Configure > Profiles	RWD	RWD	R	NA
Configure > Networks	RWD	RWD	R	NA
Configure > Segments	RWD	RWD	R	NA
Configure > Overlay Flow Control	RWD	RWD	R	NA
Configure > Network Services	RWD	RWD	R	NA
Configure > Alerts & Notifications	RW	RW	R	NA
Test & Troubleshoot > Remote Diagnostics	RW	RW	RW	NA
Test & Troubleshoot > Remote Actions	RW	RW	RW	NA
Test & Troubleshoot > Packet Capture	RW	RW	RW	NA

SASE Orchestrator Feature	Enterprise: Super User	Enterprise: Standard Admin	Customer Support	Read Only
Test & Troubleshoot > Diagnostic Bundles	RWD	RWD	RWD	NA
Administration > System Settings	RW	RW	RW	NA
Administration > Administrators	RW	R	R	NA

**Note** Operator users have complete access to the SASE Orchestrator features.

## Key Concepts

This section describes the key concepts and the core configurations of SASE Orchestrator.

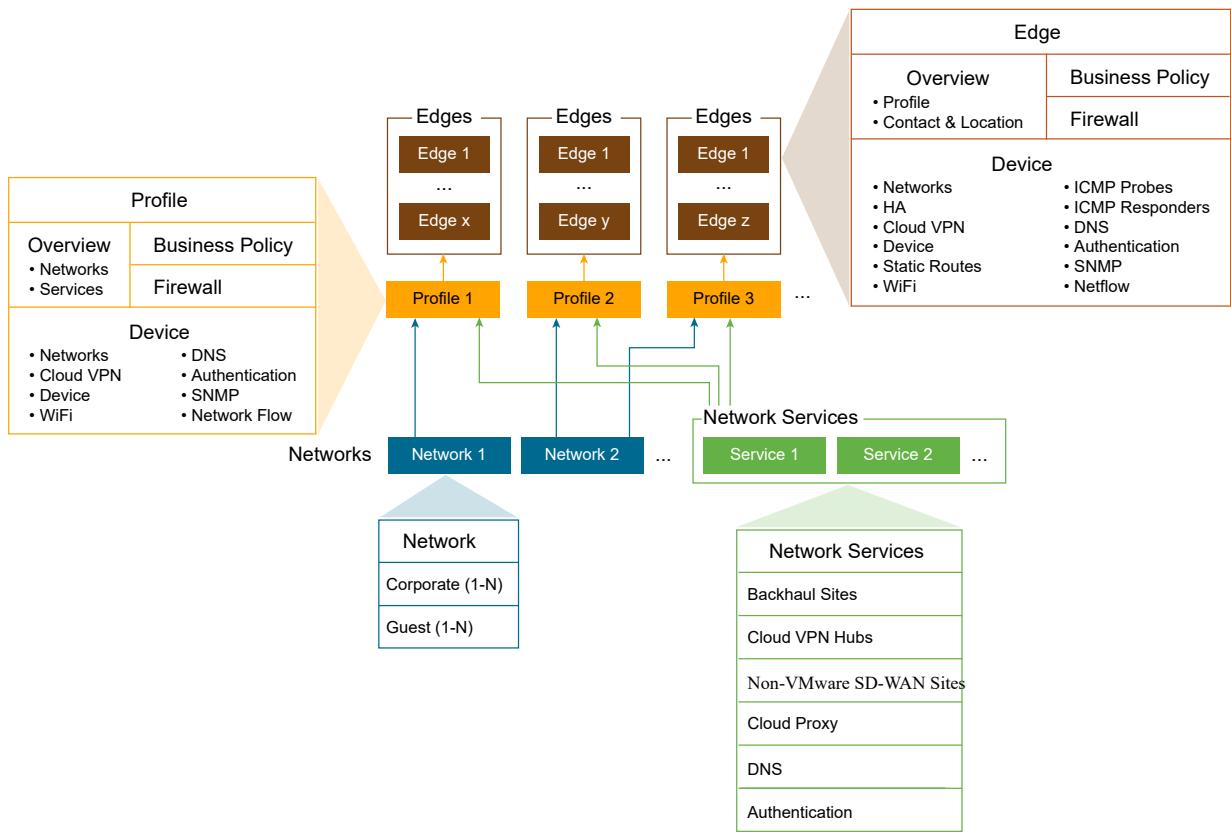
### Configurations

The VMware service has four core configurations that have a hierarchical relationship. Create these configurations in the SASE Orchestrator.

The following table provides an overview of the configurations:

Configuration	Description
Network	Defines basic network configurations, such as IP addressing and VLANs. Networks can be designated as Corporate or Guest and there can be multiple definitions for each network.
Network Services	Define several common services used by the VMware Service, such as BackHaul Sites, Cloud VPN Hubs, Non SD-WAN Destinations, Cloud Proxy Services, DNS services, and Authentication Services.
Profile	Defines a template configuration that can be applied to multiple Edges. A Profile is configured by selecting a Network and Network Services. A profile can be applied to one or more Edge models and defines the settings for the LAN, Internet, Wireless LAN, and WAN Edge Interfaces. Profiles can also provide settings for Wi-Fi Radio, SNMP, Netflow, Business Policies and Firewall configuration.
Edge	Configurations provide a complete group of settings that can be downloaded to an Edge device. The Edge configuration is a composite of settings from a selected Profile, a selected Network, and Network Services. An Edge configuration can also override settings or add ordered policies to those defined in the Profile, Network, and Network Services.

The following image shows a detailed overview of the relationships and configuration settings of multiple Edges, Profiles, Networks, and Network Services.



A single Profile can be assigned to multiple Edges. An individual Network configuration can be used in more than one Profile. Network Services configurations are used in all Profiles.

## Networks

Networks are standard configurations that define network address spaces and VLAN assignments for Edges. You can configure the following network types:

- Corporate or trusted networks, which can be configured with either overlapping addresses or non-overlapping addresses.
- Guest or untrusted networks, which always use overlapping addresses.

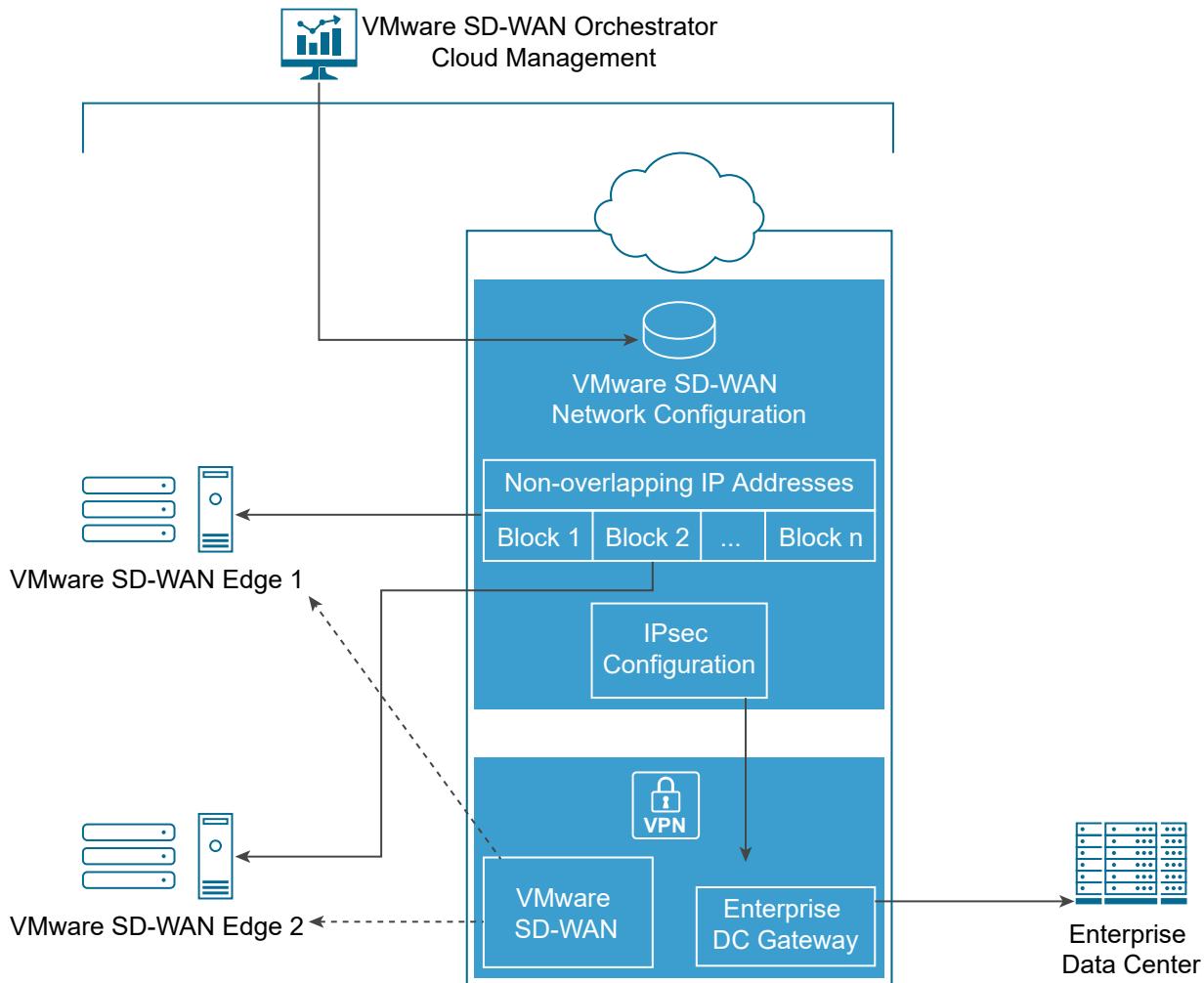
You can define multiple Corporate and Guest Networks, and assign VLANs to both the Networks.

With overlapping addresses, all Edges that use the Network have the same address space. Overlapping addresses are associated with non-VPN configurations.

With non-overlapping addresses, an address space is divided into blocks of an equal number of addresses. Non-overlapping addresses are associated with VPN configurations. The address blocks are assigned to Edges that use the Network so that each Edge has a unique set of addresses. Non-overlapping addresses are required for **Edge-to-Edge** and **Edge -to- Non SD-WAN Destination** VPN communication. The VMware configuration creates the required

information to access an Enterprise Data Center Gateway for VPN access. An administrator for the Enterprise Data Center Gateway uses the IPSec configuration information generated during Non SD-WAN Destination VPN configuration to configure the VPN tunnel to the Non SD-WAN Destination.

The following image shows unique IP address blocks from a Network configuration being assigned to SD-WAN Edge.



**Note** When using non-overlapping addresses, the SASE Orchestrator automatically allocates the blocks of addresses to the Edges. The allocation happens based on the maximum number of Edges that might use the network configuration.

## Network Services

You can define your Enterprise Network Services and use them across all the Profiles. This includes services for Authentication, Cloud Proxy, Non SD-WAN Destinations, and DNS. The defined Network Services are used only when they are assigned to a Profile.

## Profiles

A profile is a named configuration that defines a list of VLANs, Cloud VPN settings, wired and wireless Interface Settings, and Network Services such as DNS Settings, Authentication Settings, Cloud Proxy Settings, and VPN connections to Non SD-WAN Destinations. You can define a standard configuration for one or more SD-WAN Edges using the profiles.

Profiles provide Cloud VPN settings for Edges configured for VPN. The Cloud VPN Settings can activate or deactivate Edge-to-Edge and Edge-to- Non SD-WAN Destination VPN connections.

Profiles can also define rules and configuration for the Business Policies and Firewall settings.

## Edges

You can assign a profile to an Edge and the Edge derives most of the configuration from the Profile.

You can use most of the settings defined in a Profile, Network, or Network Services without modification in an Edge configuration. However, you can override the settings for the Edge configuration elements to tailor an Edge for a specific scenario. This includes settings for Interfaces, Wi-Fi Radio Settings, DNS, Authentication, Business Policy, and Firewall.

In addition, you can configure an Edge to augment settings that are not present in Profile or Network configuration. This includes Subnet Addressing, Static Route settings, and Inbound Firewall Rules for Port Forwarding and 1:1 NAT.

## Orchestrator Configuration Workflow

VMware supports multiple configuration scenarios. The following table lists some of the common scenarios:

Scenario	Description
SaaS	Used for Edges that do not require VPN connections between Edges, to a Non SD-WAN Destination, or to a VMware SD-WAN Site. The workflow assumes the addressing for the Corporate Network using overlapping addresses.
Non SD-WAN Destination via VPN	Used for Edges that require VPN connections to a Non SD-WAN Destination such as Amazon Web Services, Zscaler, Cisco ISR, or ASR 1000 Series. The workflow assumes the addressing for the Corporate Network using non-overlapping addresses and the Non SD-WAN Destinations are defined in the profile.
VMware SD-WAN Site VPN	Used for Edges that require VPN connections to a VMware SD-WAN Site such as an Edge Hub or a Cloud VPN Hub. The workflow assumes the addressing for the Corporate Network using non-overlapping addresses and the VMware SD-WAN Sites are defined in the profile.

For each scenario, perform the configurations in the SASE Orchestrator in the following order:

**Step 1:** Network

**Step 2:** Network Services

**Step 3:** Profile

## Step 4: Edge

The following table provides a high-level outline of the Quick Start configuration for each of the workflows. You can use the preconfigured Network, Network Services, and Profile configurations for Quick Start Configurations. For VPN configurations modify the existing VPN Profile and configure the VMware SD-WAN Site or Non SD-WAN Destination. The final step is to create a new Edge and activate it.

Quick Start Configuration Steps	SaaS	Non SD-WAN Destination VPN	VMware SD-WAN Site VPN
Step 1: Network	Select Quick Start Internet Network	Select Quick Start VPN Network	Select Quick Start VPN Network
Step 2: Network Service	Use pre-configured Network Services	Use pre-configured Network Services	Use pre-configured Network Services
Step 3: Profile	Select Quick Start Internet Profile	Select Quick Start VPN Profile Activate Cloud VPN and configure Non SD-WAN Destinations	Select Quick Start VPN Profile Activate Cloud VPN and configure VMware SD-WAN Sites
Step 4: Edge	Add New Edge and activate the Edge	Add New Edge and activate the Edge	Add New Edge and activate the Edge

For more information, see [Chapter 26 Activate SD-WAN Edges](#).

## Supported Browsers

The SASE Orchestrator supports the following browsers:

Browsers Qualified	Browser Version
Google Chrome	77 – 79.0.3945.130
Mozilla Firefox	69.0.2 - 72.0.2
Microsoft Edge	42.17134.1.0- 44.18362.449.0
Apple Safari	12.1.2-13.0.3

**Note** For the best experience, VMware recommends Google Chrome or Mozilla Firefox.

**Note** Starting from VMware SD-WAN version 4.0.0, the support for Internet Explorer has been deprecated.

## Supported Modems

This section describes how to get a list of supported modems.

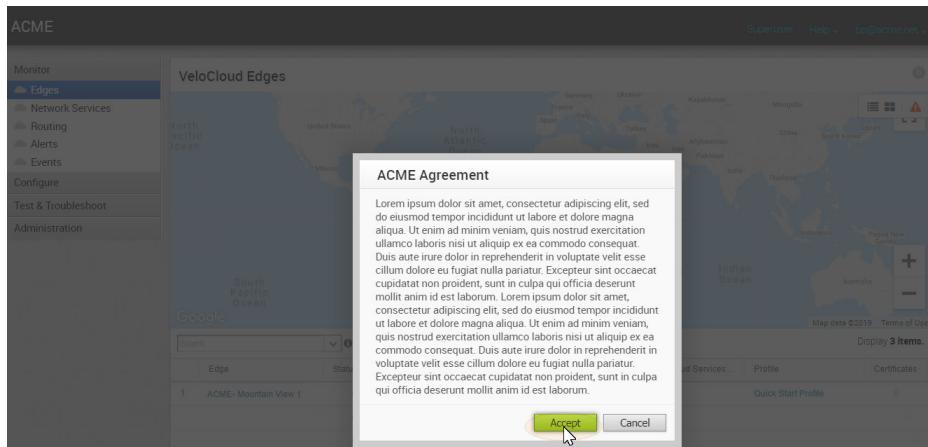
For a detailed list of supported modems, see <https://sdwan.vmware.com/get-started/supported-modems>.



# User Agreement

5

An Enterprise Superuser or Partner Superuser might see a user agreement upon logging into the SASE Orchestrator. The user must accept the agreement to get access to the SASE Orchestrator. If the users do not accept the agreement, they will be automatically logged out.



# 6

# Log in to VMware SASE Orchestrator Using SSO for Enterprise User

Describes how to log in to VMware SASE Orchestrator using Single Sign On (SSO) as an Enterprise user.

To login into SASE Orchestrator using the SSO as an Enterprise user:

## Prerequisites

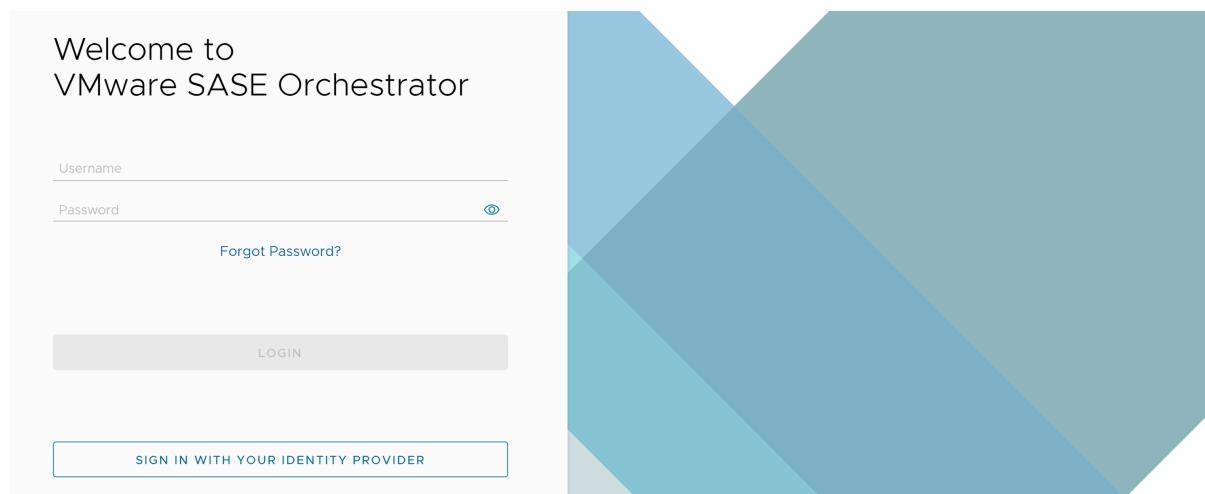
- You must configure the SSO authentication in SASE Orchestrator.
- You must set up users, roles and OIDC application for the SSO in your preferred IDPs.

For more information, see the topic *Authentication in VMware SASE Global Settings Guide*, located at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

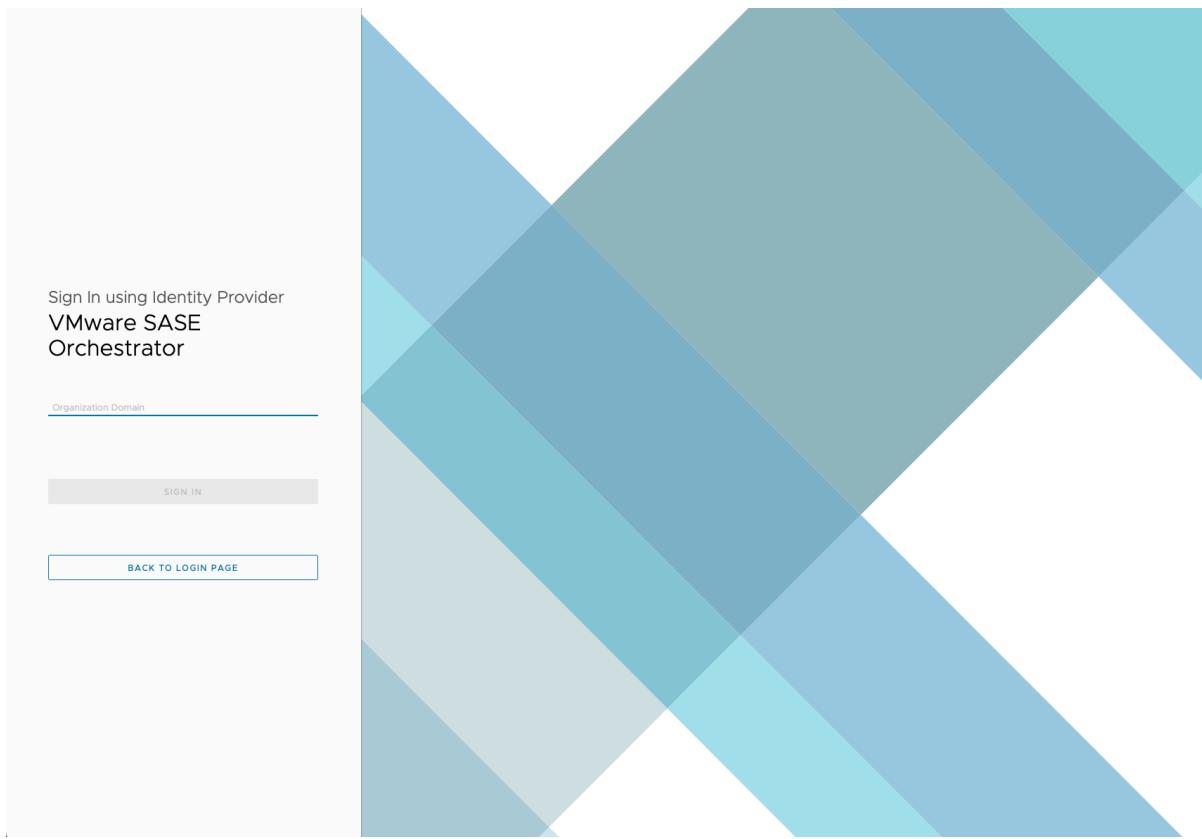
## Procedure

- 1 In a web browser, launch the SASE Orchestrator application as an Enterprise user.

The VMware SASE Operations Console screen appears.



## 2 Click Sign In With Your Identity Provider.



- 3 In the **Organization Domain** text box, enter the domain name used for the SSO configuration and click **Sign In**.

The IDP configured for the SSO authenticates the user and redirects the user to the configured SASE Orchestrator URL.

---

**Note** Once the users log in to the SASE Orchestrator using SSO, they are not allowed to login again as native users.

---

### What to do next

- Monitor Customers
- Configure Customers
- Configure Service Settings
- Test and Troubleshoot Edges

Additionally, in the SASE Orchestrator home page, you can access the following features from the Global Navigation bar:

- The user can click the **User** icon located at the top right of the screen to access the **My Account** page. The **My Account** page allows users to configure basic user information, SSH keys, and API tokens. Users can also view the current user's role, associated privileges, and additional information such as version number, build number, legal and terms information, cookie usage, and VMware trademark. For more information, see [Chapter 27 Configure User Account details](#).

The screenshot displays the VMware SD-WAN Orchestrator interface. On the left, the Global Navigation bar shows 'Customer custtest' and 'SD-WAN'. The main area is titled 'Network Overview' under 'Activated Edges'. It features two circular diagrams labeled 'Hubs' with a count of '0'. Between them are three status categories: 'Connected' (green), 'Degraded' (yellow), and 'Offline' (red). Below this is a table with columns: Edge Name, Status, Secrets Encryption, HA (Mode), Cluster Name, and Links. A message 'No edges for this network found' is centered. At the bottom are 'COLUMNS' and 'REFRESH' buttons. On the right, a sidebar titled 'User Information' shows 'Account' details: Username 'custttest@vmware.com', Role 'Enterprise Superuser', and 'Profile' Email 'custttest@vmware.com'. A 'MY ACCOUNT' button is at the bottom. At the very bottom, there is footer information: Version 5.4.0.0, Build R5400-20230914-0655-QA-998cc4c1f9, Legal & Terms of Service, Cookie Usage, and ©2023 VMware.

- Starting with the 5.4.0 release, the **In-product Contextual Help Panel** with context-sensitive user assistance is supported in the SD-WAN service of the Enterprise Orchestrator UI and as well as for the Operator and Partner levels. In the Global Navigation bar, click the **Question Mark** icon located at the top right of the screen to access the Support panel.

The Support panel allows users across all levels to access helpful and important information such as Question-Based Lists (QBLs), Knowledge base links, Ask the Community link, how to file a support ticket, and other related documentation from within the Orchestrator UI page itself. This makes it easier for the user to learn our product without having to navigate to another site for guidance or contact the Support Team.

---

**Note** By default, the Support Panel is not available to all Enterprise users. Contact your Operator or Partner Admins if you want to activate the **In-product Contextual Help Panel** feature.

---

**Activated Edges**

Edge Name	Status	Secrets Encryption	HA (Mode)	Cluster Name	Links
No edges for this network found					

**Links**

**Hubs**

**SUPPORT**

**POPULAR TOPICS**

- Help • What is SD-WAN Service Reachable and how MPLS Only SD-WAN Edge site can use SD-WAN Services?
- Help • How to change the Primary Gateway of the SD-WAN Edge?
- Help • What is Conditional Backhaul?
- Help • What is 1:1 NAT rule and Port Forwarding rule and when can you configure these rules?
- Help • How can you configure a LAN interface effectively?
- Help • How does an Edge select the Cloud Security Service (CSS) tunnel if it is having more than one link configured?
- Help • How does SD-WAN perform remediation for Dynamic Multipath Optimization?

[VIEW MORE IN VMWARE DOCS](#)

[Knowledge Base](#)

[Ask the Community](#)

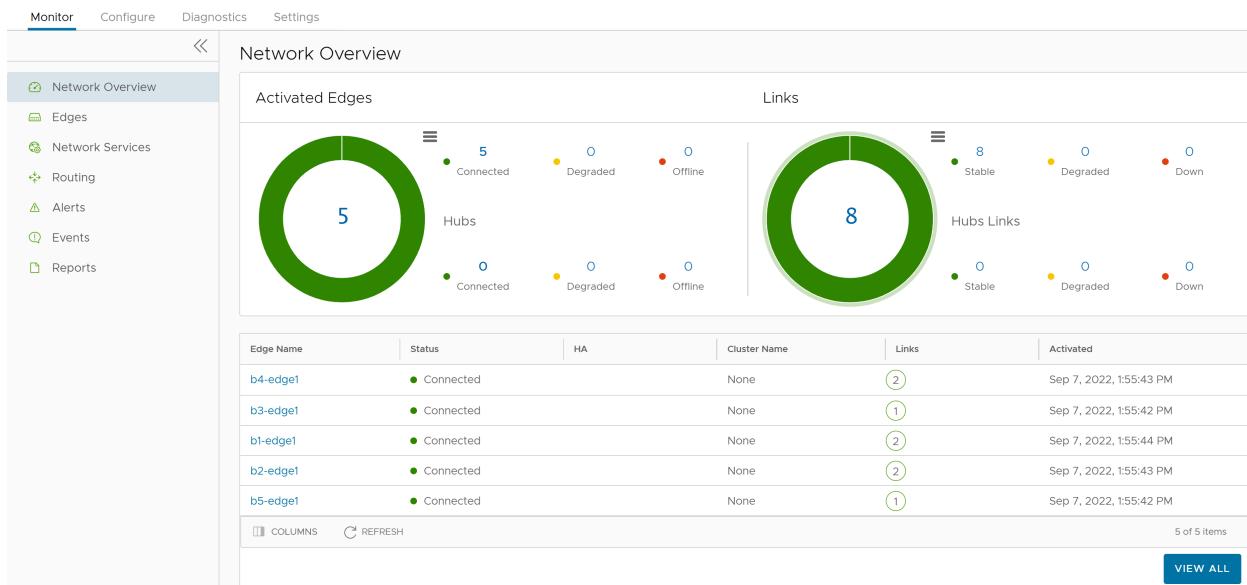
[How to file a support ticket](#)

# Monitor Enterprise

7

VMware SD-WAN allows an Enterprise user to monitor the events and services using a redesigned portal.

In the **SD-WAN** service of the Enterprise portal, click **Monitor** from the top menu. The following screen appears:



You can explore each monitoring option and click the graphs to view more detailed drill-down reports.

Each monitoring window consists of the following options:

- **Search** – Enter a term to search for specific details. Click the Filter icon to filter the view by a specific criterion.
- **Column** – Click and select the columns to be shown or hidden in the view.
- **Refresh** – Click to refresh the details displayed with the most current data.

Read the following topics next:

- [Monitor Network Overview](#)
- [Monitor Security Overview](#)

- [Monitor Edges](#)
- [Monitor Network Services](#)
- [Monitor Routing Details](#)
- [Monitor Alerts](#)
- [Monitor Events](#)
- [Monitor Firewall Logs](#)
- [Enterprise Reports](#)
- [View Analytics Data](#)

## Monitor Network Overview

The Network Overview page displays the overall summary of the network, like activated Edges, links, top applications, and other configured data.

To view the Network Overview summary:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Overview**.

The **Network Overview** page displays the summary of the network in a graphical representation. In this page, you can find details about Activated Edges, Links, Top performing Applications and Edges by data volume, Profiles used by the Edges, Activated Segements, Software version of the Edges, and so on.

Also, the **Network Overview** page displays additional information about the Edges that are connected, degraded, and down in a table format as shown in the screenshot below. For a provisioned and activated Edge, you can find additional details such as name and status of Edge, number of links and hub links that are stable, name of Cluster to which the Edge is assigned, [Activate High Availability](#) if the Edge is running 5.2.0.0 and above versions, Bastion state if Bastion Orchestrator is configured, secrets encryption, and date/time when the Edge is activated.

The screenshot shows the VMware SD-WAN Administration Guide interface. The top navigation bar includes sections for Orchestrator, Customer 5-site-cluster, SD-WAN, Monitor, Configure, Diagnostics, Service Settings, and a Help icon.

**Network Overview**

**Activated Edges**

Edge Name	Status	Secrets Encryption	HA (Mode)	Cluster Name	Links	Bastion State	Activated
b1-edge2 [cluster1]	Connected	Cluster	cluster1	(2)	Unconfigured	Apr 20, 2023, 12:23:32 PM	
b1-edge1 [cluster1]	Connected	Cluster	cluster1	(2)	Unconfigured	Apr 20, 2023, 12:23:31 PM	
b5-edge1 [cluster2]	Connected	Cluster	cluster2	(2)	Unconfigured	Apr 20, 2023, 12:23:31 PM	
b5-edge3 [cluster2]	Connected	Cluster	cluster2	(2)	Unconfigured	Apr 20, 2023, 12:23:32 PM	
b1-edge3 [cluster1]	Connected	Cluster	cluster1	(3)	Unconfigured	Apr 20, 2023, 12:23:32 PM	
b5-edge2 [cluster2]	Connected	Cluster	cluster2	(2)	Unconfigured	Apr 20, 2023, 12:23:32 PM	
b2-edge1	Connected	None		(3)	Unconfigured	Apr 20, 2023, 12:23:31 PM	
b4-edge1	Connected	None		(2)	Unconfigured	Apr 20, 2023, 12:23:31 PM	
b3-edge1	Connected	None		(2)	Unconfigured	Apr 20, 2023, 12:23:31 PM	
b1-edge4	Connected	None		(3)	Unconfigured	Apr 20, 2023, 12:23:32 PM	

**Links**

Hubs	Connected	Degraded	Offline	Hubs Links	Stable	Degraded	Down
10	0	0	0	23	0	0	0
6	0	0	0	13	0	0	0

**Top Apps by Data Volume** (Past 2 weeks)

App	Data Volume (GB)
SD-WAN Control	28 GB
SD-WAN Managem...	5.5 GB
Domain Name Se...	0.5 GB

**Top Edges by Data Volume** (Past 2 weeks)

Edge	Data Volume (GB)
b1-edge4	10.5 GB
b2-edge1	9.5 GB
b4-edge1	8.5 GB
b3-edge1	7.5 GB

**Configuration data**

**Profiles used**

Total	Used	Unused
5	4	1
80%		

**Segments Activated**

Total	Activated	Other
3	3	0
100%		

**Software Version** (Up to date)

Total	Up to date	Outdated
10	10	0
100%		

**Edges with Enabled VNF**

Error	Off	On
0	0	0

**Edges with Enabled A-S Pair**

Failed	Pending	Ready
0	0	0

**Non SD-WAN Destinations via Gateway**

Total	Connected	Offline
0	0	0

The following details are displayed:

Option	Description
Activated Edges	<p>Displays the number of Edges and Hubs that are connected, degraded, and down, along with a graphical representation. Click the link to a number and details of the corresponding Edges or Hubs are displayed in the bottom panel.</p> <p>In the following table, click the link to the Edge or the cluster name to navigate to the corresponding tabs.</p>
Links	<p>Displays the number of links and hub links that are stable, degraded, and down, along with a graphical representation. Click the link to a number and details of the corresponding links or Hub links are displayed in the bottom panel.</p> <p>In the following table, click the link to the Hub name to navigate to the corresponding tab.</p>
Top Apps by Data Volume	Displays the top 10 applications sorted by volume of data.
Top Edges by Data Volume	Displays the top 10 Edges sorted by volume of data.
Profiles Used	Displays the details of used and unused profiles.
Segments Activated	Displays the details of activated and other segments.
Software Version	Displays the details of software versions of the Edges, that are up to date and outdated.
Edges with Enabled VNF	Displays the number of Edges activated with VNF, that are with status Error, Off, and On.
Edges with Enabled A-S Pair	Displays the number of Edges activated as Active-Standby pair, that are with status Failed, Pending, and Ready.
Non SD-WAN Destinations via Gateway	Displays the number of non SD-WAN destinations that are connected and offline.

Hover the mouse on the graphs to view more details.

## Monitor Security Overview

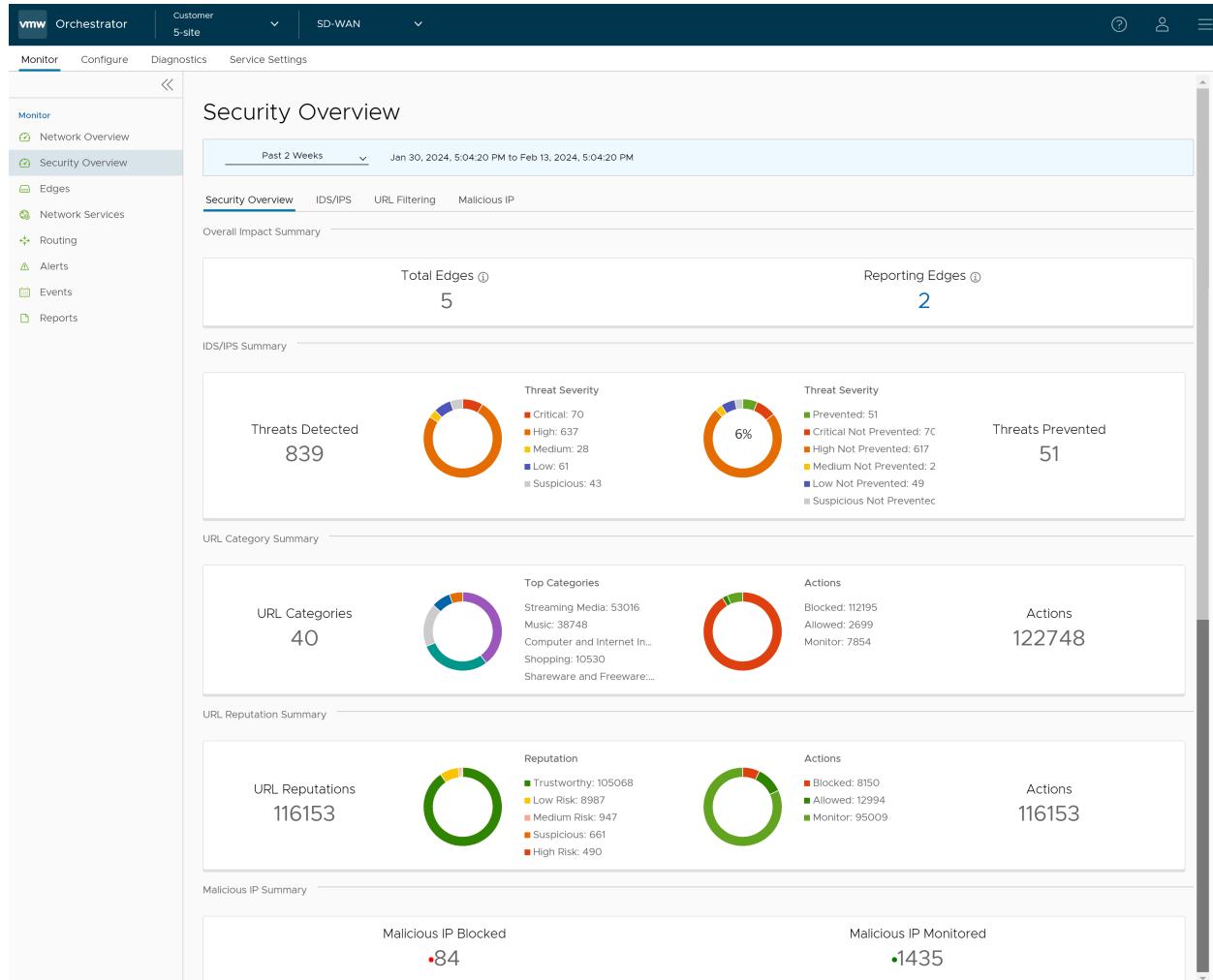
The **Security Overview** page displays the overall impact summary of configured Security services, like Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), URL Categories, URL Reputations, and Malicious IP for all Edges within an Enterprise, based on the metrics collected using the various Enhanced Firewall Services (EFS) engines (IDS/IPS/URL Filtering/Malicious IP).

---

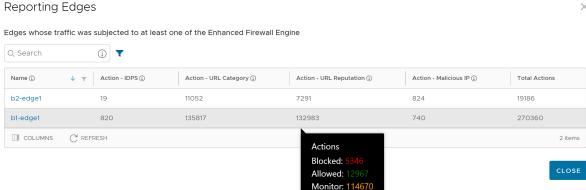
**Note** Under the **Monitor** tab, the **Security Overview** option will be visible only if the EFS feature is activated in the **Global Settings** page.

## Monitor Security Overview - Enterprise View

To view the overall impact summary of configured Security services for an Enterprise, in the **SD-WAN** service of the Enterprise portal, click **Monitor > Security Overview**. The **Security Overview** page appears.



In the **Security Overview** page, you can find the following details:

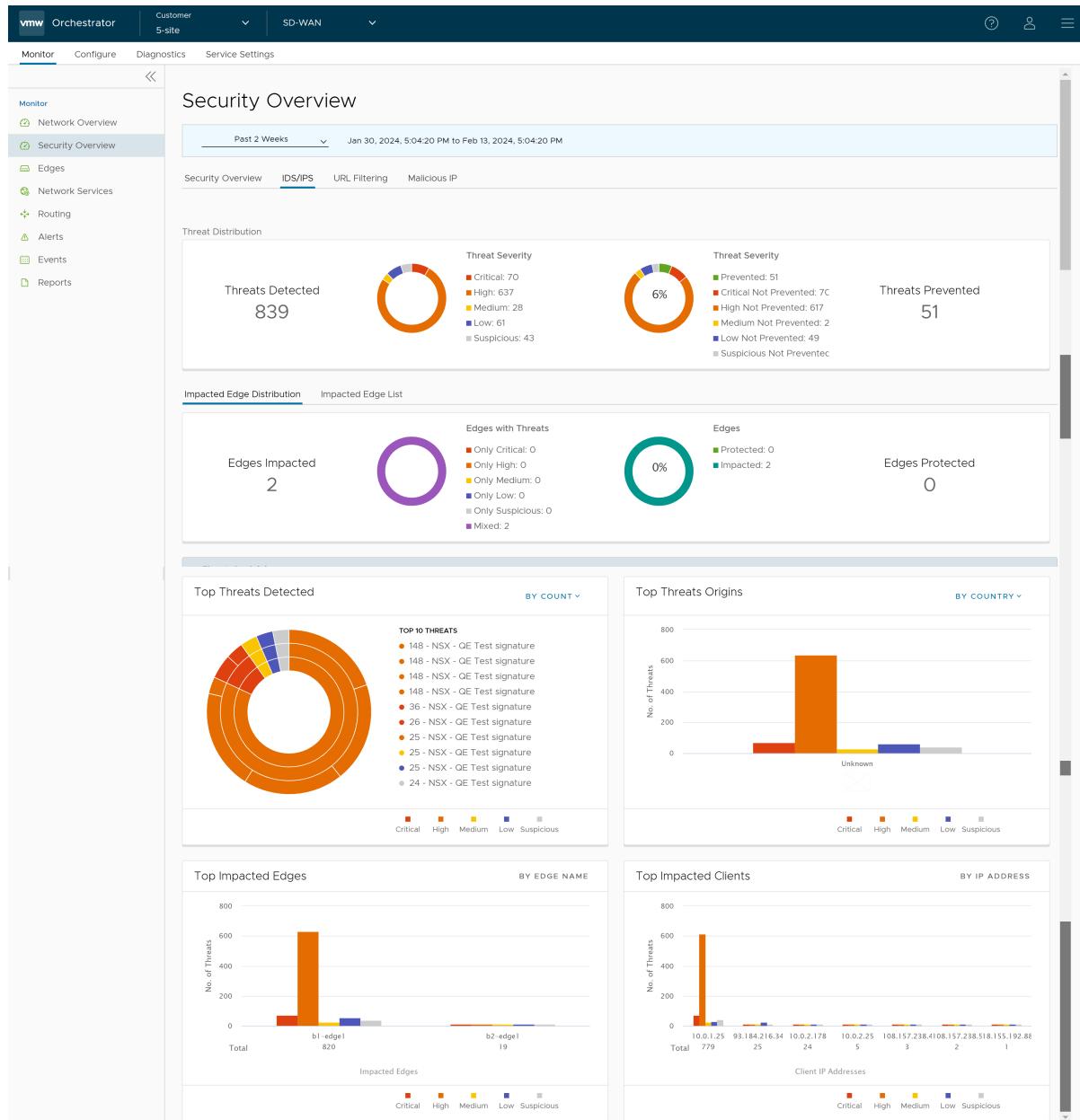
Option	Description
Overall Impact Summary	<p>Displays the total count of Edges within the Enterprise and total count of Reporting Edges whose traffic was subjected to at least one of the Enhanced Firewall Engines.</p> <p>Under <b>Reporting Edges</b>, clicking the link to the number displays a tabular view of all Edges whose traffic hit atleast one EFS engine along with the Action count details. Hover the mouse over the Action count to view the split count by supported <b>Action</b> types.</p>  <p>To view the EFS Threats details for a specific Edge, click the link to the Edge name. You will be navigated to the Edge-specific Security Overview page. See <a href="#">Monitor Security Overview - Edge View</a>.</p>
IDS/IPS Summary	<p>Displays the total count of IDS/IPS Threats Detected and Prevented for all Edges within the Enterprise, along with the Threat Severity and Action details in a graphical representation. Hover the mouse on the graphs to view specific threat details.</p> <p>For detailed information about the IDS/IPS Threat distribution, see <a href="#">Monitor IDS/IPS</a>.</p>
URL Category Summary	<p>Displays the total count of URL Categories and Action count details for all Edges within the Enterprise, along with the <b>Top 5 URL Categories</b> details in a graphical representation.</p> <p>For detailed information about the URL Category Threats distribution, see <a href="#">Monitor URL Filtering</a>.</p>
URL Reputation Summary	<p>Displays the total count of URL Reputation risks and Action count details for all Edges within the Enterprise in a graphical representation.</p> <p>For detailed information about the URL Reputation Threats distribution, see <a href="#">Monitor URL Filtering</a>.</p>
Malicious IP Summary	<p>Displays the total count of Malicious IP Blocked and Monitored.</p> <p>For detailed information about the Malicious IP Threats distribution, see <a href="#">Monitor Malicious IP</a>.</p>

## Monitor IDS/IPS

To view the IDS/IPS specific threats details for an Enterprise, click **Monitor > Security Overview > IDS/IPS**.

The **IDS/IPS** page is a graphical representation of Threat distribution (Threats Detected/Threats Prevented) based on the metrics collected using the IDS/IPS engines for all Edges within an Enterprise. You can view the Threat distribution of all the Edges using the following two views:

- **Impacted Edge Distribution** – Represents a map view of all the IDS/IPS Impacted Edges (by severity) and Protected Edges. The page graphically displays the following IDS/IPS Threat details for an Enterprise:
  - Total count of Edges Impacted
  - Total count of Edges Protected
  - Top Threats Detected filtered "By Count" (Default) or "By Impact"
  - Top Threat Origins filtered "By Country" (Default) or "By IP Address"
  - Top Impacted Edges filtered "By Edge Name"
  - Top Impacted Clients filtered "By IP Address"



- **Impacted Edge List** – Represents a tabular view of all the IDS/IPS impacted Edges along with Threat details. The page displays the following details: Name and Description of the impacted Edge, Threat Impact on Edge, and Status of impacted Edge.

**Threat Distribution**

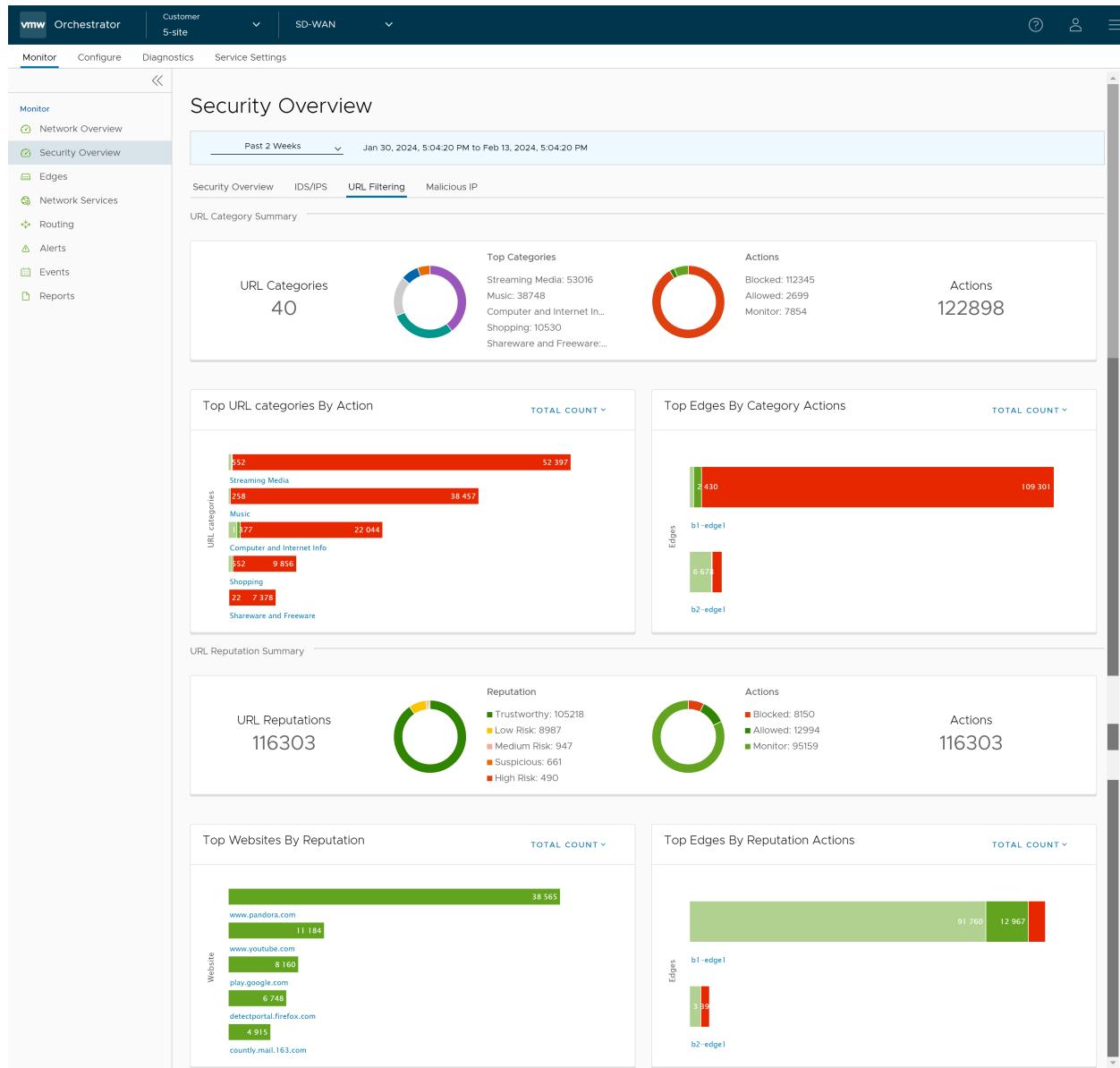
Threat Type	Count
Critical	70
High	637
Medium	28
Low	61
Suspicious	43

Edge Name	Description	Threat Impact	Status
b1-edge1	H (629) M (26) L (57) C (70) S (38)	<span style="color: purple;">Alerted</span>	
b2-edge1	H (8) M (2) L (4) C (0) S (5)	<span style="color: purple;">Alerted</span>	

## Monitor URL Filtering

To view the URL Filtering specific threats details for an Enterprise, click **Monitor > Security Overview > URL Filtering**.



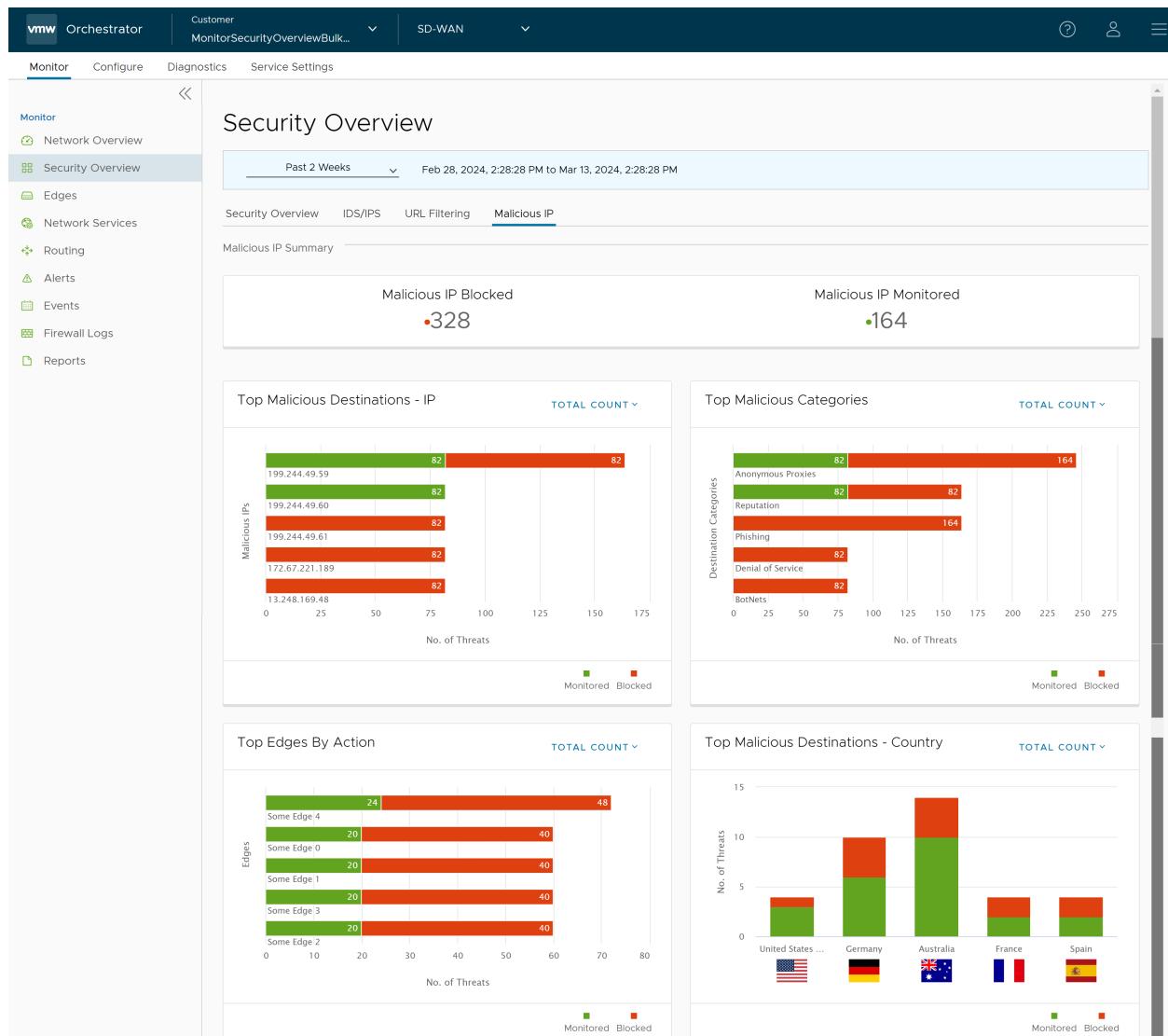
The **URL Filtering** page graphically displays the following URL Categories and URL Reputations threat details for an Enterprise:

- Total count of URL Categories
- Total count of URL Category Actions
- Top URL Categories
- Top URL categories filtered by "Action" (Blocked, Allowed, and Monitored) or "Total Count" (Default)
- Top Edges filtered by "Category Actions" (Blocked, Allowed, and Monitored) or "Total Count" (Default)
- Total count of URL Reputations

- Total count of URL Reputation Actions
- Top Websites filtered by "URL Reputation" (High Risk, Suspicious, Medium Risk, Low Risk, and Trustworthy) or "Total Count" (Default)
- Top Edges filtered by "Reputation Actions" (Blocked, Allowed, and Monitored) or "Total Count" (Default)

## Monitor Malicious IP

To view the Malicious IP specific threats details for an Enterprise, click **Monitor > Security Overview > Malicious IP**.



The **Malicious IP** page graphically displays the following Malicious IP threat details for an Enterprise:

- Total count of Blocked Malicious IP

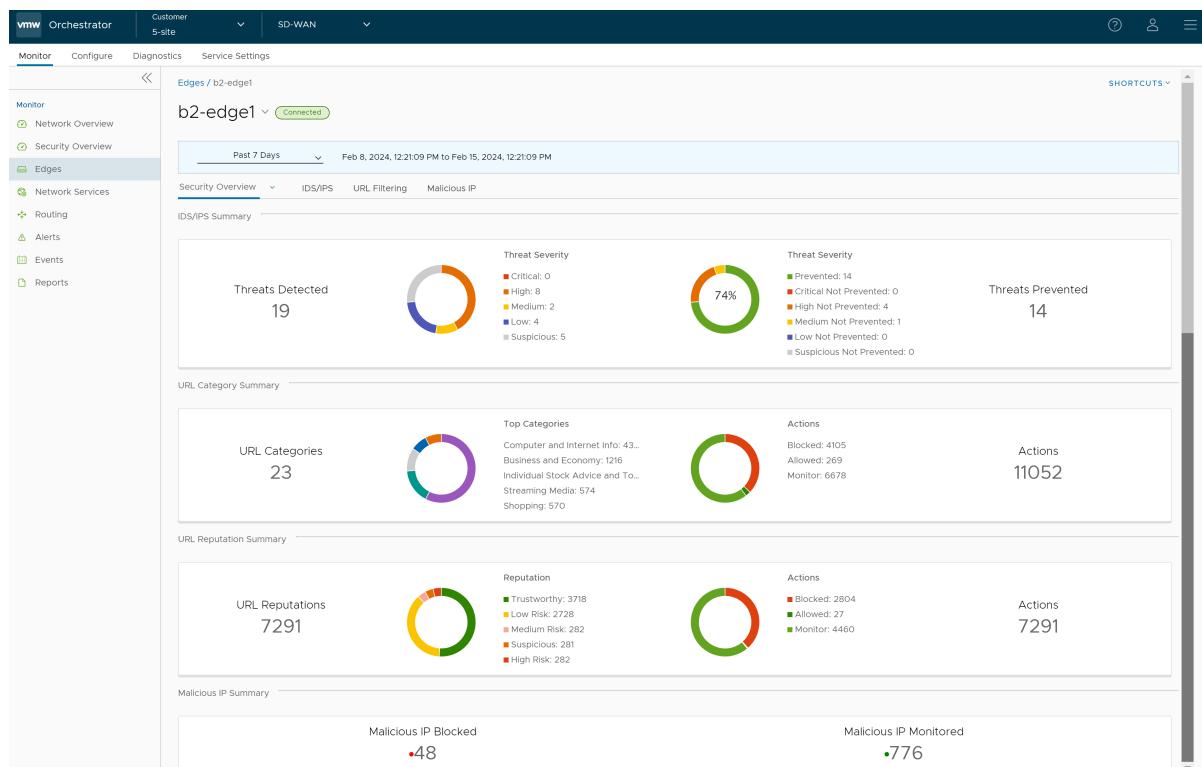
- Total count of Monitored Malicious IP
- Top Malicious Destination IPs filtered by "Action" (Blocked and Monitored) or "Total Count" (Default)
- Top Malicious Categories filtered by "Action" (Blocked and Monitored) or "Total Count" (Default)
- Top Edges filtered by "Action" (Blocked and Monitored)) or "Total Count" (Default)
- Top Malicious Destination Countries filtered by "Action" (Blocked and Monitored) or "Total Count" (Default)

## Monitor Security Overview - Edge View

To view the EFS Threat details for a specific Edge:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges**. The list of Edges associated with the Enterprise appears.
- 2 Select an Edge by clicking the link to an Edge. The **Network Overview** page (default page view) appears.
- 3 From the **Network Overview** drop-down menu, select **Security Overview**.

The **Security Overview** page displays the overall impact summary of configured Security services, like IDS/IPS, URL Categories, URL Reputations, and Malicious IP for the selected Edge.



## Monitor Edges

You can monitor the status of Edges and view the details of each Edge, like the WAN links, top applications used by the Edges, usage data through the network sources and traffic destinations, business priority of network traffic, system information, details of Gateways connected to the Edge, and so on.

To monitor the Edge details:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise. The page displays the details of the Edges, like the status, links, Gateways, and other information.

Name	Status	HA	Links	VNF VM Status	VNF Type	Gateways	Last Contact
b1-hub1 [HUB_CLUSTER1]	Connected	Cluster	(3)			View	Dec 8, 2020, 10:28:46 PM
b2-hub1 [HUB_CLUSTER2]	Connected	Cluster	(3)			View	Dec 8, 2020, 10:28:41 PM
b7-edge1	Connected	○ View Events	(2)			View	Dec 8, 2020, 10:28:41 PM
b1-hub2 [HUB_CLUSTER1]	Connected	Cluster	(3)			View	Dec 8, 2020, 10:28:46 PM
b1-hub3 [HUB_CLUSTER1]	Connected	Cluster	(3)			View	Dec 8, 2020, 10:28:39 PM
b2-hub2 [HUB_CLUSTER2]	Connected	Cluster	(2)			View	Dec 8, 2020, 10:28:39 PM
b2-hub3 [CLUSTER3]	Connected	Cluster	(2)			View	Dec 8, 2020, 10:28:42 PM
b8-edge1	Connected	= Unknown	(4)			View	Dec 8, 2020, 10:28:38 PM
b10-edge1	Connected	● Standby ready	(1)			View	Dec 8, 2020, 10:28:40 PM
spoke-1-7	Connected		(3)			View	Dec 8, 2020, 10:28:47 PM
spoke-1-2	Connected		(3)			View	Dec 8, 2020, 10:28:27 PM

Click **CSV** to download a report of the Edges in CSV format.

Click **View** in the **Gateways** column to view the details of the Gateways connected to the corresponding Edge.

Click an Edge name in the **Name** column to view the details of the selected Edge. Click the relevant tabs to view the corresponding information. Each tab displays a drop-down list at the top which allows you to select a specific time period. The tab displays the details for the selected duration.

Some of the tabs provide drop-down menu of metrics parameters. You can choose the metrics from the list to view the corresponding data. The following table lists the available metrics:

The following table describes each drop-down menu that are available in the **Links**, **Applications**, **Sources**, **Destinations**, and **Business Priority** tabs.

Metrics Option	Description
Average Throughput	Total bytes in a given direction divided by the total time. The total time is the periodicity of statistics uploaded from the Edge. By default, the periodicity in SASE Orchestrator is 5 minutes.
Total Bytes	Total number of bytes sent and received during a network session.

Metrics Option	Description
Bytes Received/Sent	Split up details of number of bytes sent and received during a network session.
Total Packets	Total number of packets sent and received during a network session.
Packets Received/Sent	Split up details of number of packets sent and received during a network session.
Bandwidth	The maximum rate of data transfer across a given path. Displays both the upstream and downstream bandwidth details.
Latency	Time taken for a packet to get across the network, from source to destination. Displays both the upstream and downstream Latency details.
Jitter	Variation in the delay of received packets caused by network congestion or route changes. Displays both the upstream and downstream Jitter details.
Packet loss	Packet loss happens when one or more packets fail to reach the intended destination. A lost packet is calculated when a path sequence number is missed and does not arrive within the re-sequencing window. A “very late” packet is counted as a lost packet.
Auto Dual-Mode SIM	Status of the Edge with respect to the <b>Automatic Switchover</b> feature configured on that Edge, and is applicable only for a <b>610-LTE</b> . For more information on the <b>Automatic Switchover</b> feature, see <a href="#">Configure Automatic SIM Switchover</a> .
Signal	Signal strength of the Edge indicated by the number of bars.

For each Edge, you can view the following details:

- [Monitor Edge Overview](#)
- [Monitor QoE](#)
- [Monitor Links of an Edge](#)
- [Monitor Path Visibility](#)
- [Monitor Flow Visibility](#)
- [Monitor Edge Applications](#)
- [Monitor Edge Sources](#)
- [Monitor Edge Destinations](#)
- [Monitor Business Priorities of an Edge](#)
- [Monitor System Information of an Edge](#)

Select an Edge and click the **Shortcuts** option at the top to perform the following activities:

- **Configure** – Navigates to the Configuration tab of the selected Edge. See [Chapter 29 Configure Edge Overrides](#).
- **View Events** – Displays the Events related to the selected Edge.
- **Remote Diagnostics** – Allows to run the Remote Diagnostics tests for the selected Edge. See [Run Remote Diagnostics](#).
- **Generate Diagnostic Bundle** – Allows to generate Diagnostic Bundle for the selected Edge. See [Diagnostic Bundles for Edges](#).
- **Remote Actions** – Allows to perform the Remote actions for the selected Edge. See [Remote Actions](#).
- **View Profile** – Navigates to the Profile page, that is associated with the selected Edge.
- **View Gateways** – Displays the Gateways connected to the selected Edge.

The following are the other options available on this page:

Option	Description
Search	Enter a search term to search for the matching text across the page. Use the advanced search option to narrow down the search results.
Columns	Click and select the columns to be displayed or hidden on the page.
Refresh	Click to refresh the page to display the most current data.

## Monitor Edge Overview

The Overview tab of an Edge in the monitoring dashboard displays the details of WAN links along with bandwidth consumption and network usage.

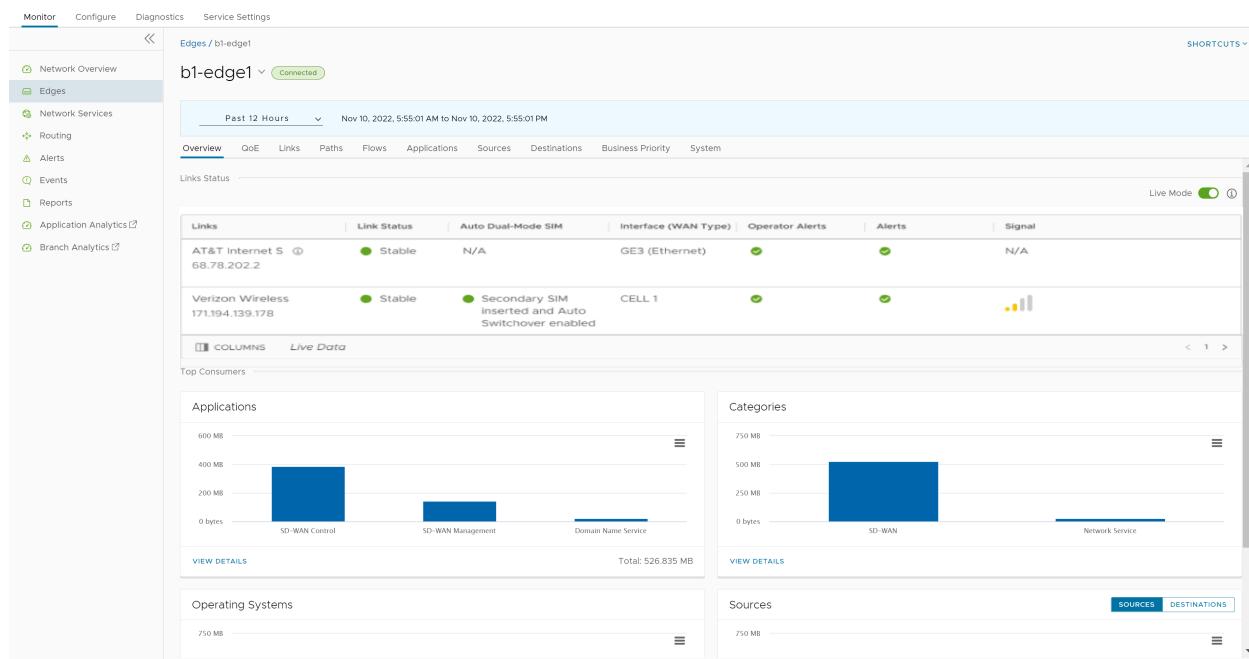
To view the information of an Edge:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- 2 Click the link to an Edge and the **Overview** tab is displayed by default.

### Results

The **Overview** tab displays the details of links with status and the bandwidth consumption.



You can choose whether to view the Edge information live using the **Live Mode** option. When this mode is ON, live monitoring of the Edge happens and the data in the page is updated whenever there is a change. The live mode is automatically moved to offline mode after a period of time to reduce the network load.

The **Links Status** section displays the details of Links, Link Status, Auto Dual-Mode SIM, WAN Interface, Throughput, Bandwidth, Signal, Latency, Jitter, and Packet Loss. For more information on these parameters, see [Monitor Edges](#).

The **Top Consumers** section displays graphical representation of bandwidth and network usage of the following: Applications, Categories, Operating Systems, Sources, and Destinations of the Edges. Click **View Details** in each panel to navigate to the corresponding tab and view more details.

Hover the mouse on the graphs to view more details.

---

**Note** The minimum amount of data consumption for SD-WAN control traffic on a link is 1.5 - 2 GB per month depending on the number of paths.

## Monitor QoE

The VMware **Quality of Experience (QoE)** tab shows the Quality Score for different applications. The Quality score rates an application's quality of experience that a network can deliver for a period of time. The QoE is calculated based on the best score comparing all the Static tunnels (Edge to Gateways and Edge to Hubs) and then displays the best performing tunnel.

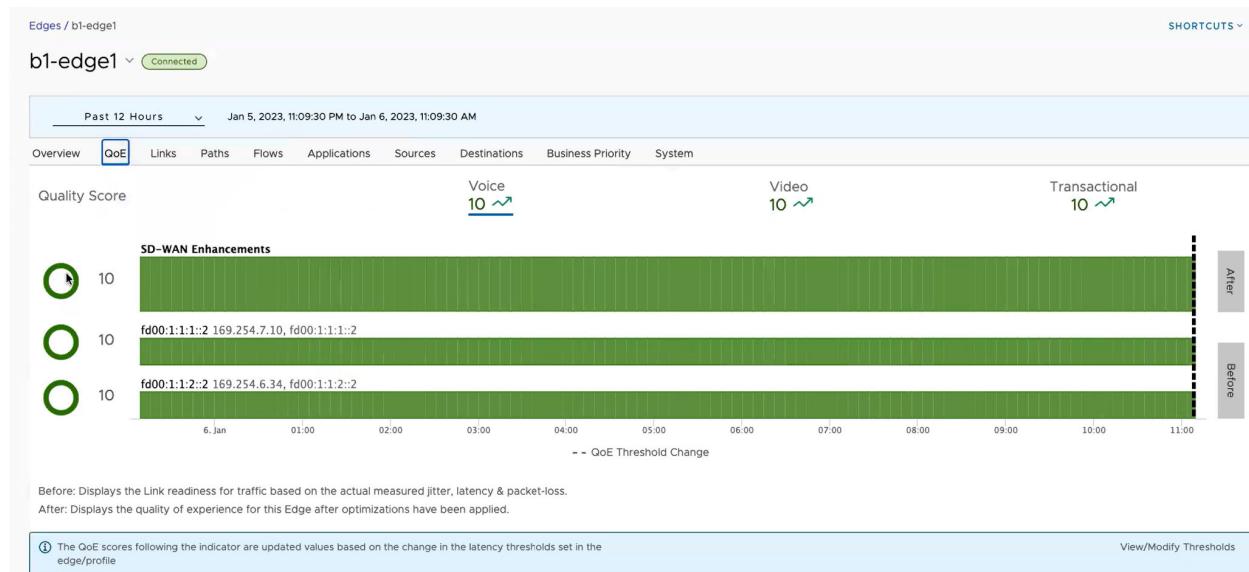
To view the QoE report of an Edge:

## Procedure

- In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- Click the link to an Edge, and then click the **QoE** tab.

## Results

The **QoE** tab displays the quality score of applications for different traffic types.



The following traffic types are supported: Voice, Video, and Transactional. Click the link to a traffic type displayed at the top, to view the corresponding data. You can hover the mouse on a WAN network link or an aggregate link to display a summary of Latency, Jitter, and Packet Loss.

The Quality Score rates an application's quality of experience that a network can deliver for a given time frame. The QoE graphs display the quality scores of the selected Edge before and after the SD-WAN optimization. A black vertical dotted line indicating an anchor, appears on the graph, whenever there is a threshold value change in a Profile or an Edge. You can hover the mouse on the anchor to see the modified latency threshold values for Voice, Video, and Transactional. Also, the of the graph varies depending on the threshold value as listed below:

color	Rating Color	Rating Option	Definition
Green	Good	All metrics are better than the objective thresholds. Application SLA is met/exceeded.	
Yellow	Fair	Some or all metrics are between the objective and maximum values. Application SLA is partially met.	
Red	Poor	Some or all metrics have reached or exceeded the maximum value. Application SLA is not met.	

To modify the threshold values, click the **View/Modify Thresholds** link located at the bottom of the screen, which directly takes you to the **Configure > Edges > Business Policy** page.

## Monitor Links of an Edge

You can monitor the WAN links connected to a specific Edge along with the status, interface details, and other metrics.

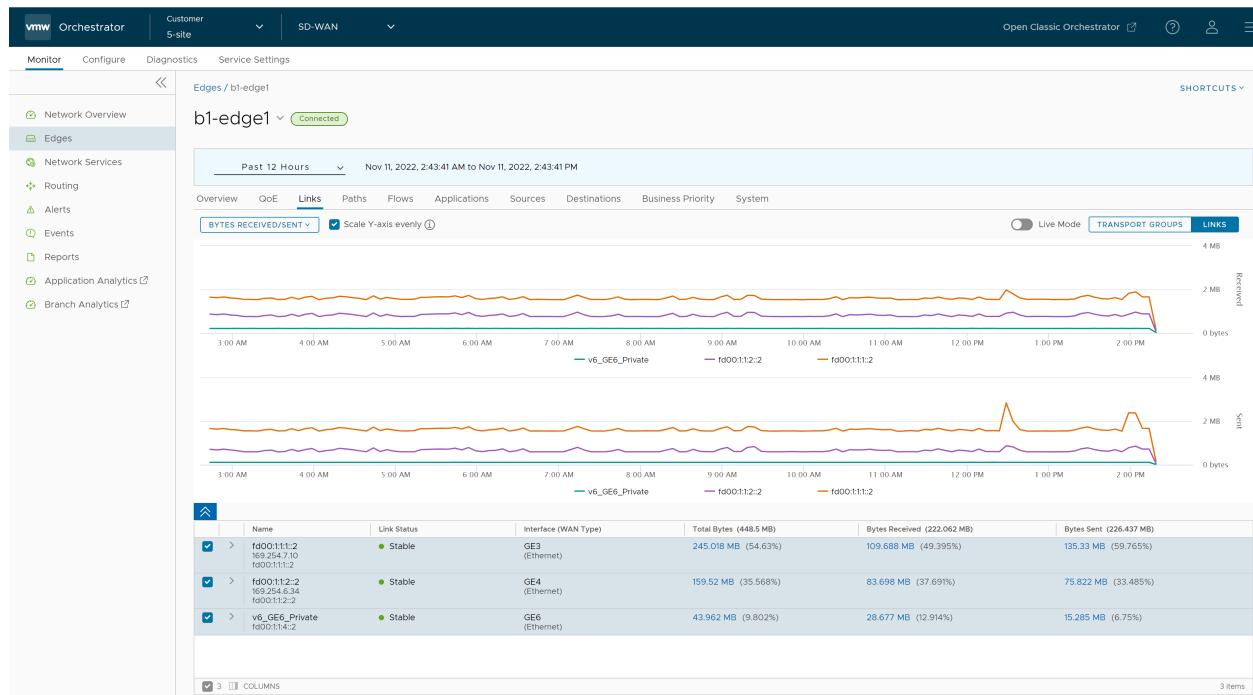
To view the details of Links and Transport groups used by the traffic:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- 2 Click the link to an Edge, and then click the **Links** tab.

### Results

The **Links** tab displays the details of WAN links connected to the selected Edge.



At the top of the page, you can choose a specific time period to view the details of the priorities for the selected duration.

By default, the **Scale Y-axis evenly** check box is selected. This option synchronizes the Y-axis between the charts. If required, you can turn off this option.

Hover the mouse on the graphs to view more details.

Click **Transport Groups** to view the links grouped into one of the following categories: Public Wired, Public Wireless, or Private Wired.

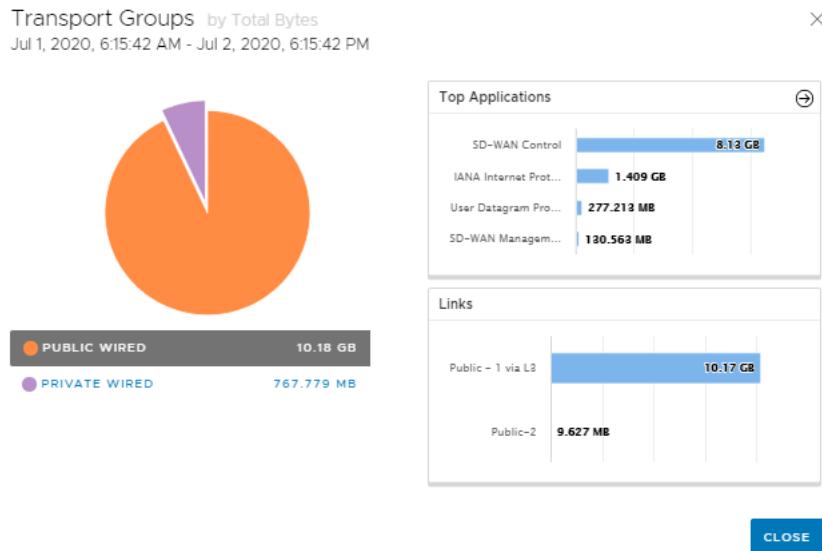
You can choose whether to view the information live using the **Live Mode** option. When this mode is ON, you can view live monitoring of the links and the transport groups.

Choose the metrics from the drop-down to view the details related to the selected parameter.

The bottom panel displays the details of the selected metrics for the links or the transport groups. You can view the details of a maximum of 4 links at a time.

Click the arrow prior to the link name or the transport group to view the break-up details. To view drill-down reports with more details, click the links displayed in the metrics column.

The following image shows a detailed report of transport groups with top applications and links.



Click the arrow next to **Top Applications** to navigate to the **Applications** tab.

## Monitor Path Visibility

Path is a tunnel between two endpoints. Path visibility is a report on utilization and quality of the paths between an Edge and its VMware SD-WAN peers. SASE Orchestrator allows an Enterprise user to monitor the Path visibility using the monitoring dashboard.

For a selected Edge, you can monitor the Path information for the VMware SD-WAN peers with traffic flow observed for a specific period.

### Procedure

- In the **SD-WAN** service of the Enterprise portal,, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- Click the link to an Edge, and then click the **Paths** tab.

### Results

For the selected Edge, the **Paths** tab displays the details of VMware SD-WAN peers with traffic flow observed for specified period.

**Note** The **Paths** tab is available only for Edges with software image version 4.0 or later.

SD-WAN Peer Name	SD-WAN Peer Type	Paths	Path QoE	SD-WAN Peer Description
b5-edge1	Branch	3	10	
gateway-2	Gateway	2	10	
b4-edge1	Branch	4	10	
b2-edge1	Branch	5	10	
gateway-1	Gateway	2	10	

At the top of the page, you can choose a specific time period to view the details of the priorities for the selected duration.

To get a report of a VMware SD-WAN peer in CSV format, select the peer and click **Export Path Statistics**.

Click the link to a VMware SD-WAN peer to view the corresponding Path details as follows:

- All the VMware SD-WAN peers that have traffic observed during the selected time period.
- The status of the paths available for a selected peer.
- Overall quality score of the paths for a selected peer for voice, video, and transactional traffic.
- Time series data for each path by metrics like: Throughput, Latency, Packet loss, Jitter, and so on. For more information on the parameters, see [Monitor Edges](#).

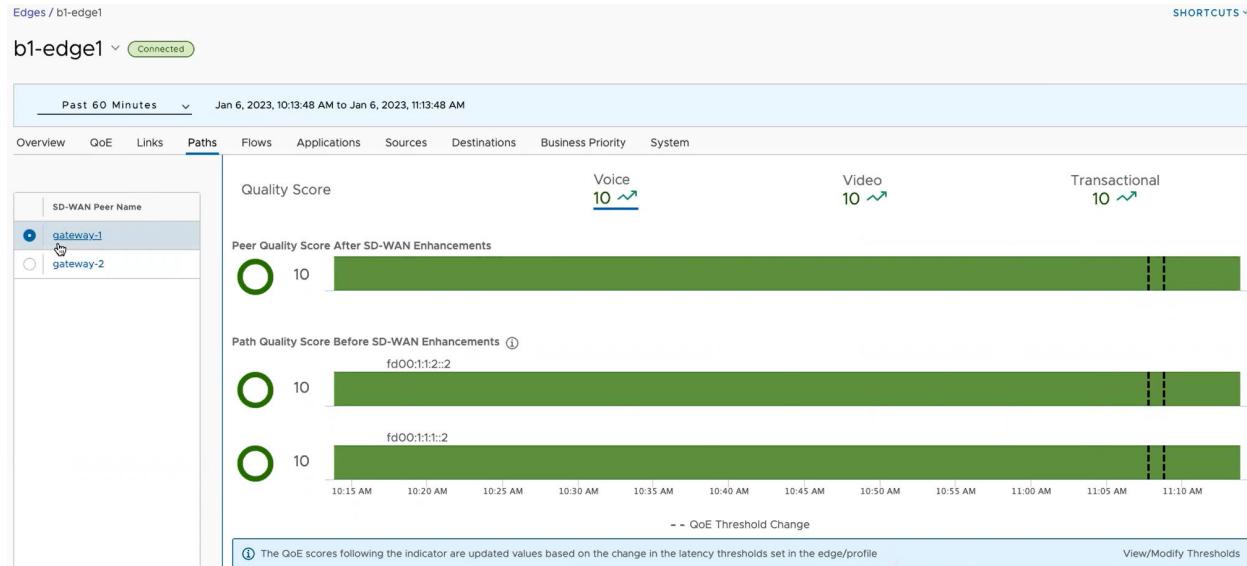
The screenshot shows the 'Paths' tab for edge b1-edge1. The top section displays a table of SD-WAN peers with their names, types, and path counts. Below this, the 'Paths' tab is selected, showing a chart of Quality Score (Voice, Video, Transactional) and a graph of Bytes Received/Sent over time for two selected paths (fd00:11:1:2 and fd00:11:2:2).

The metrics time-series data is displayed in a graphical format. You can select and view the details of a maximum of 4 paths at a time.

By default, the **Scale Y-axis evenly** check box is selected. This option synchronizes the Y-axis between the charts. If required, you can turn off this option.

Hover the mouse on the graphs to view more details.

Expand the **Quality Score** pane at the top, to view the Path score by the traffic types.



You can click a VMware SD-WAN peer displayed in the left pane, to view the corresponding Path details.

A black vertical dotted line indicating an anchor, appears on the graph, whenever there is a threshold value change in a Profile or an Edge. You can hover the mouse on the anchor to see the modified latency threshold values for Voice, Video, and Transactional. To modify the threshold values, click the **View/Modify Thresholds** link located at the bottom of the screen, which directly takes you to the **Configure > Edges > Business Policy** page.

## Monitor Flow Visibility

The Flow Visibility feature introduces a new Flows tab to the Orchestrator UI in the 5.1.0 release, which provides detailed data on each traffic flow for each Edge. The comprehensive end-to-end flow is built based on certain flow parameters, such as Source IP, Destination IP & Port, and Protocol. These parameters are displayed in a single view table format, which can assist with monitoring and troubleshooting efforts.

### Procedure

- In the **SD-WAN** service of the Enterprise portal,, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- Click the link of an Edge, and then click the **Flows** tab.

### Results

For the selected Edge, the **Flows** tab displays the details of the SD-WAN Edge for a specified period. See image below.

**Note** For the **Flows** feature, the unselected table fields are only available for Edges with software image version 5.1 or later.

The **Flows** tab displays detailed flow information about an Edge. See the table below for a description of the text fields, icons, and columns in the **Flows** tab area.

**Table 7-1. Flows Tab Description**

Field Item	Description
Specified Time text field	Provides time filter capabilities from the past 60 minutes to 1 year (from 0-14 days, high resolution data is displayed, after which low resolution data up to one year is displayed). Custom filter capabilities are also available. At the top of the page, choose a specific time period to view the details of the priorities for the selected duration.
Search	Provides Search capabilities to find a specific flow parameter. Enter a search string to find text that matches in the Source IP, Destination IP, Destination FQDN, and Destination Domain fields. Use the Advanced Search feature for more advanced filtering criteria.

**Table 7-1. Flows Tab Description (continued)**

Field Item	Description
Filter	<p>Provides Filter capabilities based on Flow parameters; such as, Source IP, Destination IP, Destination Port, Segment, Host Name, Application, Category, Destination FQDN, Destination Domain, and Next Hop.</p> <p><b>Note</b> The client device table filters hostname; however, the values are shown in accordance with what was uploaded by the flow stats that were uploaded to the flow stats table. As a result, the hostname can be null, or it might not correspond to the hostname that is being filtered. In essence, it displays the value submitted at the time the flow was uploaded.</p>
Export	<p>Provides capability to create customized reports by exporting flow data in CVS format. NOTE: A user can download the first 60K records matching the filter/quickSearch/sortBy/startTime/endTime criteria when the metrics/getEdgeFlowVisibilityMetrics request was made.</p>

**Table 7-2. Flows Parameter Description**

Field Item	Description
Source IP	Displays the IP address that owns the flow item. This information is also available on the Source tab and can be mapped to the name of the client device/operating system.
Destination IP	Displays flow data of the Destination (Domain, FQDN, and IP). This information can also be found in the Destination tab.
Destination Port	Displays the destination port number, which identifies the process that is to receive the data.
Protocol	Displays Protocols (e.g. UDP, TCP).
Segment	Routing domain. Each segment has a unique routing table.
Link	Underlying link through which the flow stats are reported.
Host Name	The hostname associated with the source device of the flow.
Application	Column that displays the application. This information can also be found in the Application tab.
Application Category	Similar applications that are used by a specific Edge can be grouped into a category.
Destination FQDN	The Fully Qualified Domain Name (FQDN) of the Destination to which the traffic flow was directed.
Next Hop	The name of Next Hop device for the flow (i.e., The name of the Gateway if the route is Cloud via Gateway). See the Route to Nexthop Mapping table in the section below.

**Table 7-2. Flows Parameter Description (continued)**

<b>Field Item</b>	<b>Description</b>
Route	The path taken to the next hop across one or more networks.
Start Time	The timestamp of when the Edge started the flow stats aggregation period.
End Time	The timestamp of when the Edge ended the flow stats aggregation period. The difference between start and end times equals the amount of time a flow stat record was aggregated for.
Total Bytes	Displays the total number of bytes sent and received during a flow.
Bytes Received	Displays details of the number of bytes received during a flow.
Bytes Sent	Displays details of the number of bytes sent during a flow.
Total Packets	Total number of packets sent and received during a flow.
Packets Received	Displays details of the number of packets received during a flow.
Packets Sent	Displays details of the number of packets sent during a flow.

**Table 7-3. Route to Nexthop Mapping Table**

<b>Route Name</b>	<b>Nexthop</b>
cloudViaGateway	The name of the Gateway that routes traffic to the cloud.
internetViaDirectBreakout	Nexthop has no name. The traffic is coming from the Internet directly.
branchToBranch (Gateway)	The name of the Gateway responsible for routing traffic to the other branch.
branchToBranch (Edge)	The name of the Edge that was used to route traffic to the other branch.
branchToNVSDirect	The name of the HUB device serving as the nexthop Edge.
branchToNVSViaGateway	The name of the Gateway that routes traffic to NVS.
branchToBackhaul	The name of the Edge or enterprise object that is used to route traffic to a non-velocloud site.
cloudViaGateway (Edge – to Partner Gateway)	The nexthop is the name of the Partner Gateway that will route the traffic.
branchRouted	Nexthop has no name. For basic routed traffic, there is no destination object, specifically, via an Edge router.
internetViaBranchCSS	Name of enterprise object used to route traffic to a non-velocloud branch.

## Monitor Edge Applications

You can monitor the network usage of applications or application categories used by a specific Edge.

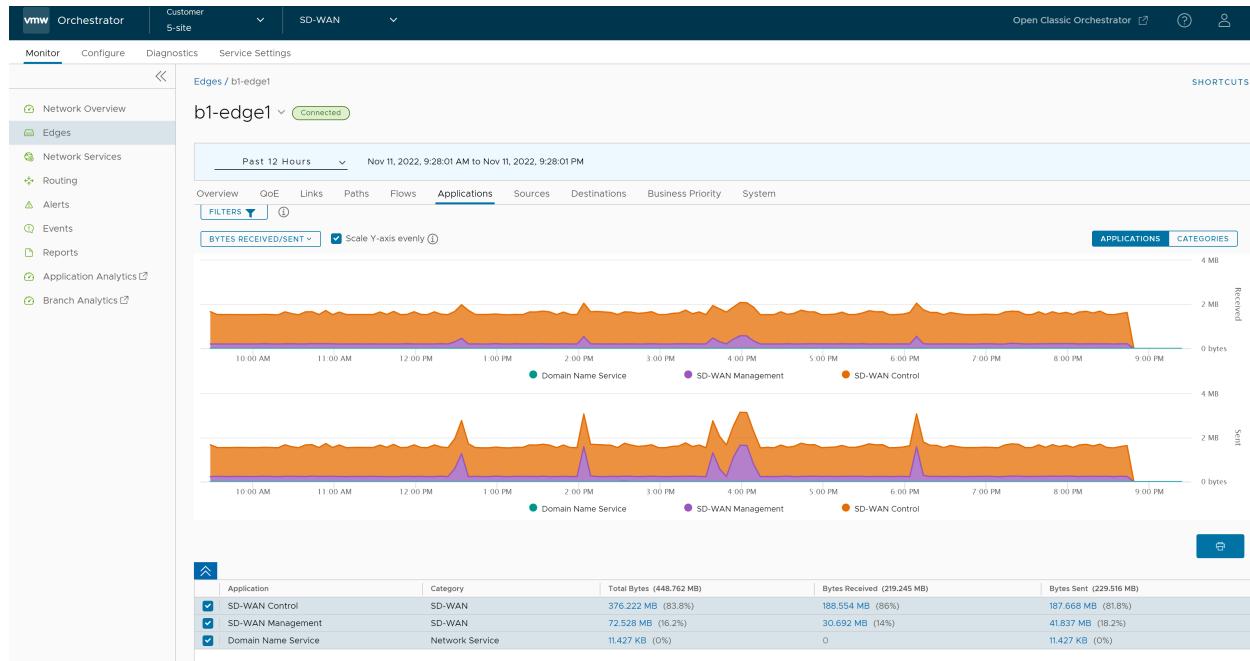
To view the details of applications or application categories:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- 2 Click the link to an Edge, and then click the **Applications** tab.

### Results

The **Applications** tab displays the details of the applications used by the selected Edge.



At the top of the page, you can choose a specific time period to view the details of the priorities for the selected duration.

Click **Filter** to define a criterion and view the application details filtered by the specified criteria.

By default, the **Scale Y-axis evenly** check box is selected. This option synchronizes the Y-axis between the charts. If required, you can turn off this option.

Click **Categories** to view similar applications grouped into categories.

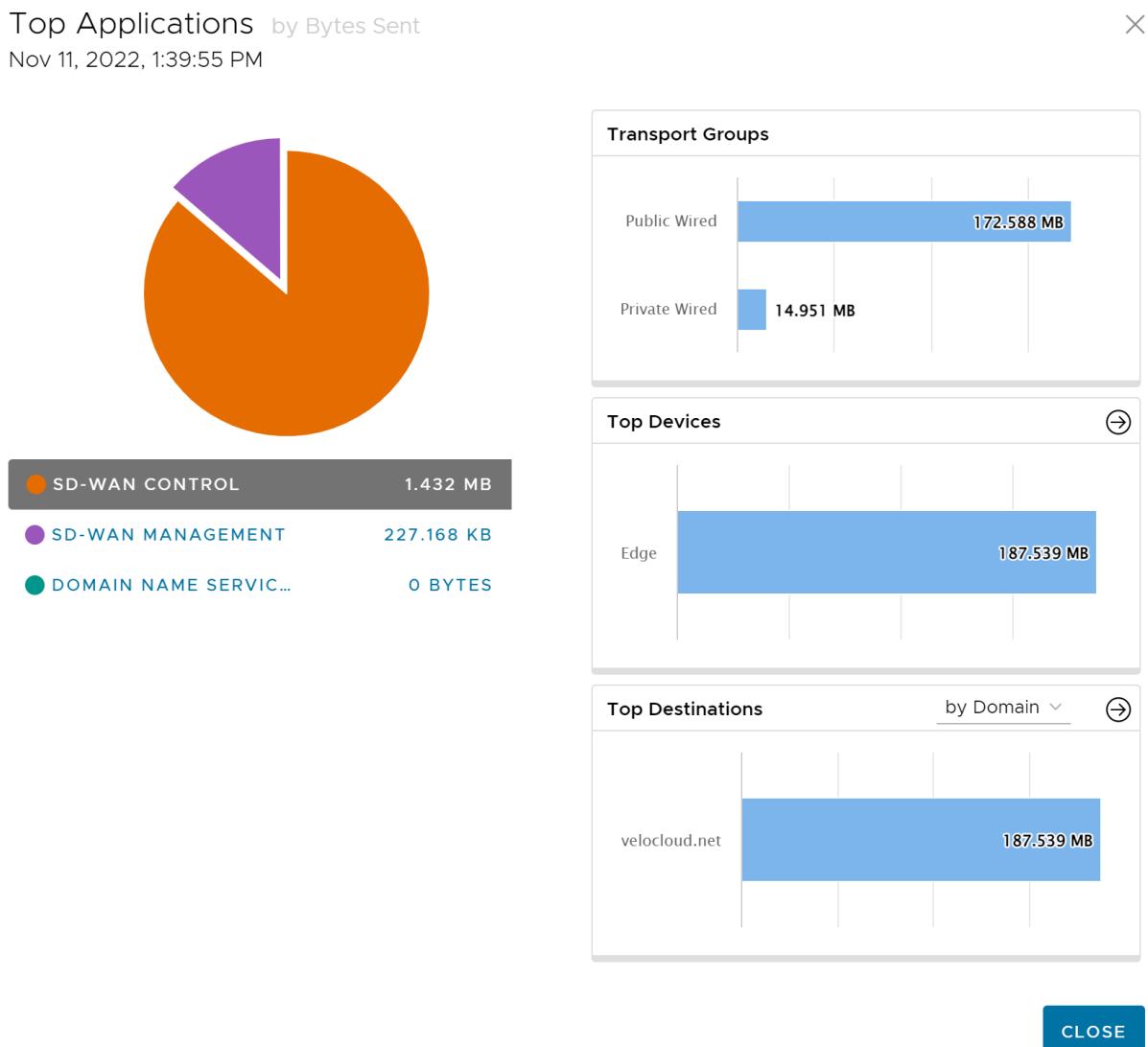
Hover the mouse on the graphs to view more details.

Choose the metrics from the drop-down to view the details related to the selected parameter.

The bottom panel displays the details of the selected metrics for the applications or categories. You can select and view the details of a maximum of 4 applications at a time. Click **Columns** to select the columns to be shown or hidden in the view.

To view drill-down reports with more details, click the links displayed in the metrics column.

The following image shows a detailed report of top applications.



Click the arrows displayed next to **Transport Groups**, **Top Devices**, or **Top Destinations** to navigate to the corresponding tabs.

## Monitor Edge Sources

You can monitor the network usage of devices and operating systems for a specific Edge.

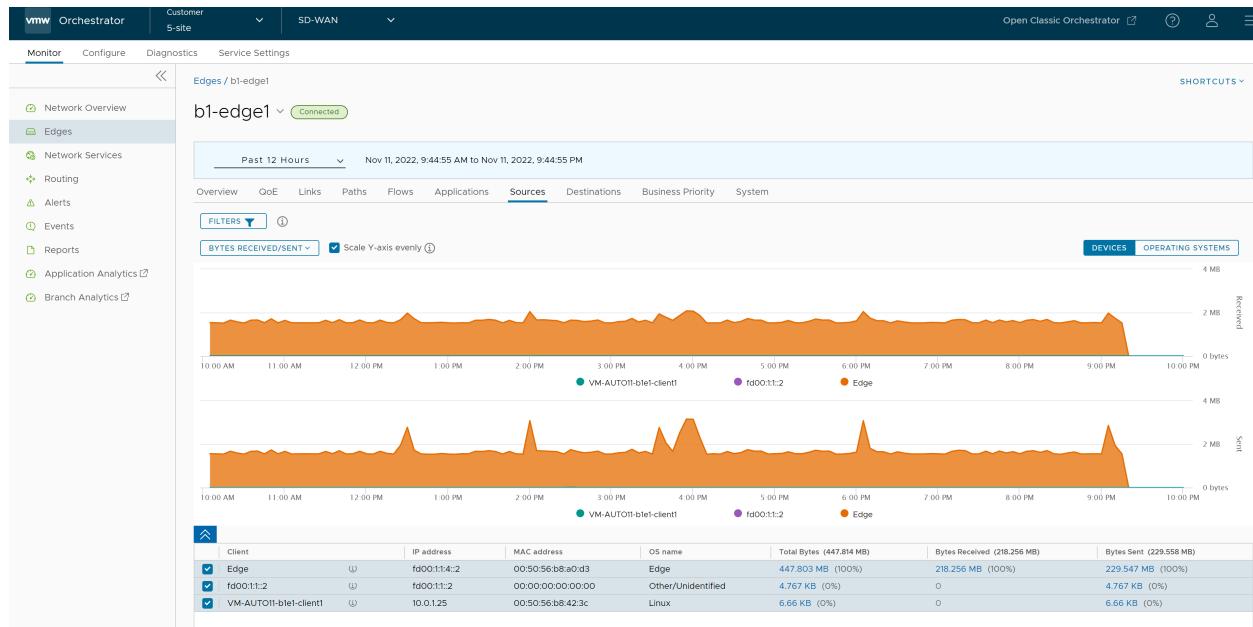
To view the details of devices and operating systems:

## Procedure

- In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- Click the link to an Edge, and then click the **Sources** tab.

## Results

The **Sources** tab displays the details of the client devices used by the selected Edge.



At the top of the page, you can choose a specific time period to view the details of the priorities for the selected duration.

By default, the **Scale Y-axis evenly** check box is selected. This option synchronizes the Y-axis between the charts. If required, you can turn off this option.

Hover the mouse on the graphs to view more details.

Click **Filter** to define a criterion and view the application details filtered by the specified criteria.

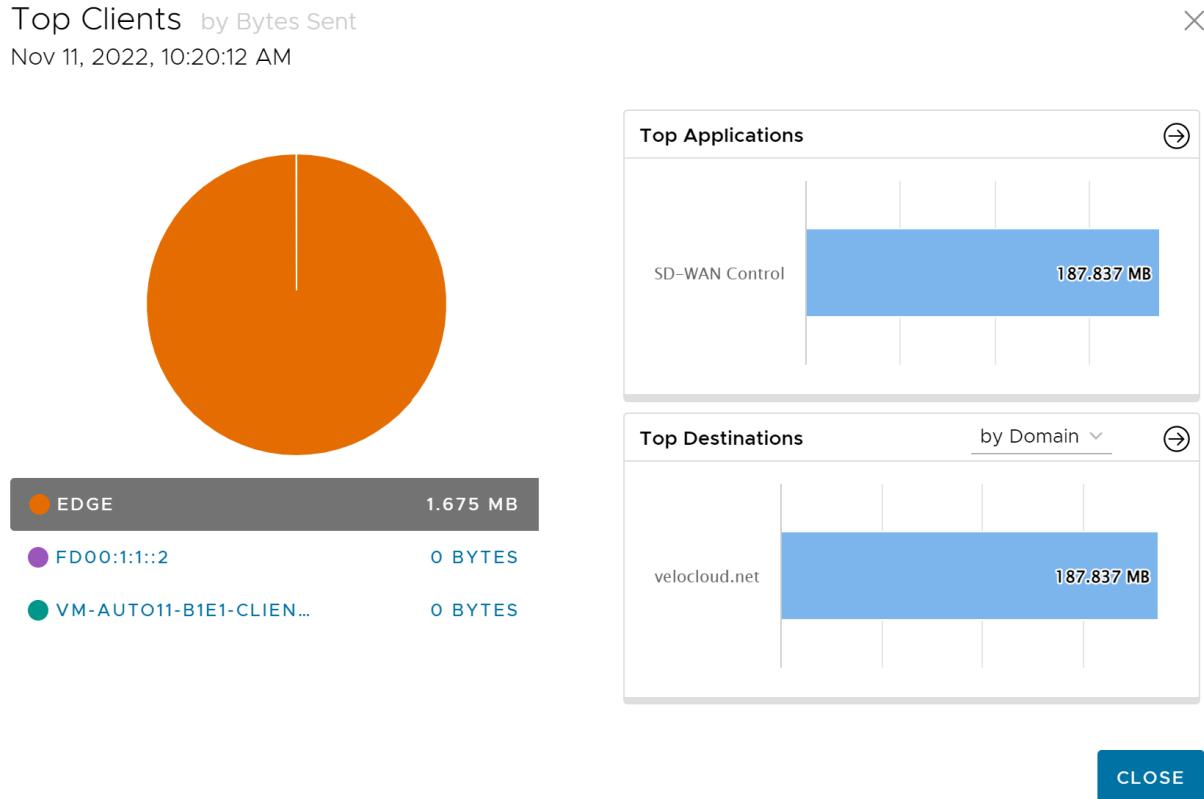
Click **Operating Systems** to view the report based on the Operating Systems used in the devices.

Choose the metrics from the drop-down to view the details related to the selected parameter.

The bottom panel displays the details of the selected metrics for the devices or operating systems. You can select and view the details of a maximum of 4 client devices at a time. Click **Columns** to select the columns to be shown or hidden in the view.

To view drill-down reports with more details, click the links displayed in the metrics column.

The following image shows a detailed report of top clients.



Click the arrows displayed next to **Top Applications** or **Top Destinations** to navigate to the corresponding tabs.

## Monitor Edge Destinations

You can monitor the network usage data of the destinations of the network traffic.

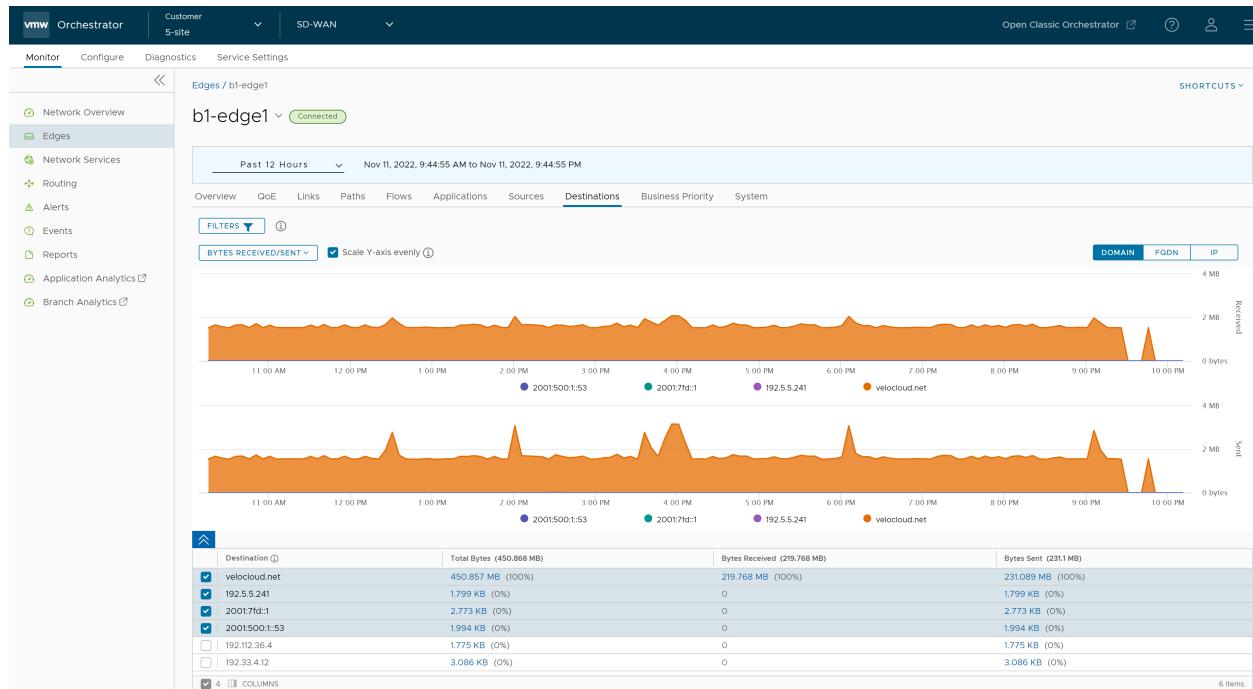
To view the details of destinations:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- 2 Click the link to an Edge, and then click the **Destinations** tab.

### Results

The **Destinations** tab displays the details of the destinations of the network traffic for the selected Edge.



At the top of the page, you can choose a specific time period to view the details of the priorities for the selected duration.

Click **Filter** to define a criterion and view the application details filtered by the specified criteria.

By default, the **Scale Y-axis evenly** check box is selected. This option synchronizes the Y-axis between the charts. If required, you can turn off this option.

You can view the report of Destinations by **Domain**, **FQDN**, or **IP** address. Click the relevant type to view the corresponding information.

Hover the mouse on the graphs to view more details.

Choose the metrics from the drop-down to view the details related to the selected parameter.

The bottom panel displays the details of the selected metrics for the destinations by the selected type. You can select and view the details of a maximum of 4 destinations at a time. Click **Columns** to select the columns to be shown or hidden in the view.

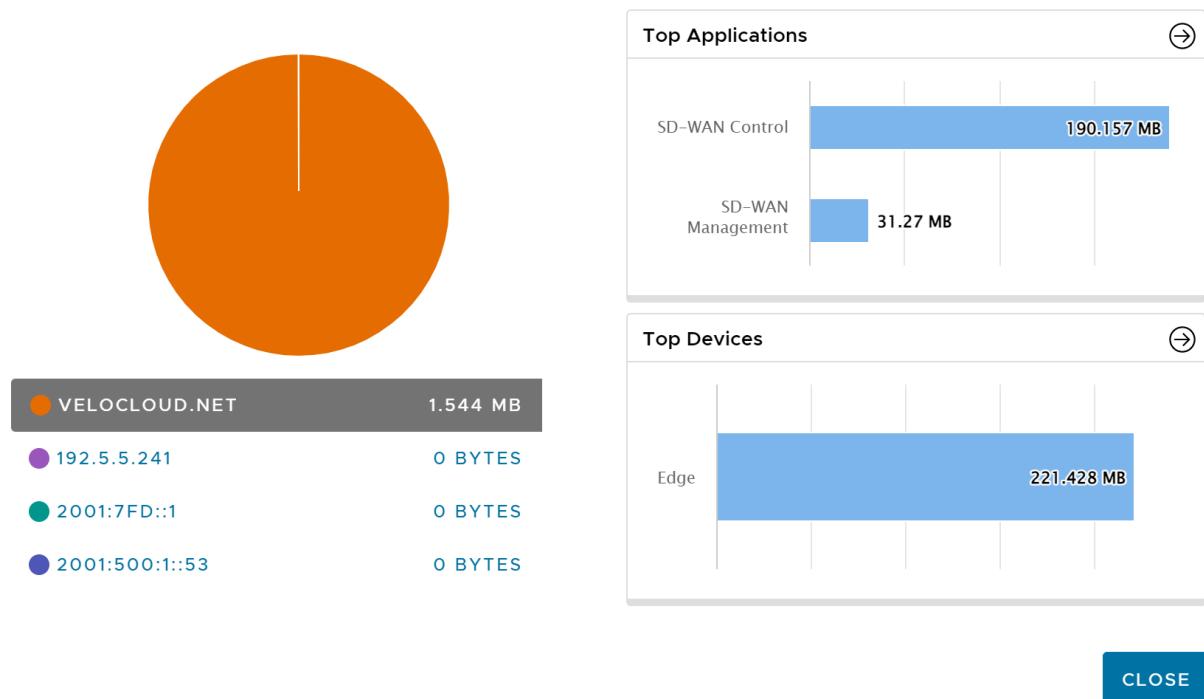
To view drill-down reports with more details, click the links displayed in the metrics column.

The following image shows a detailed report of top destinations.

X

## Top Destinations by Bytes Received

Nov 11, 2022, 12:15:48 PM



Click the arrows displayed next to **Top Applications** or **Top Devices** to navigate to the corresponding tabs.

## Monitor Business Priorities of an Edge

You can monitor the Business policy characteristics according to the priority and the associated network usage data for a specific Edge.

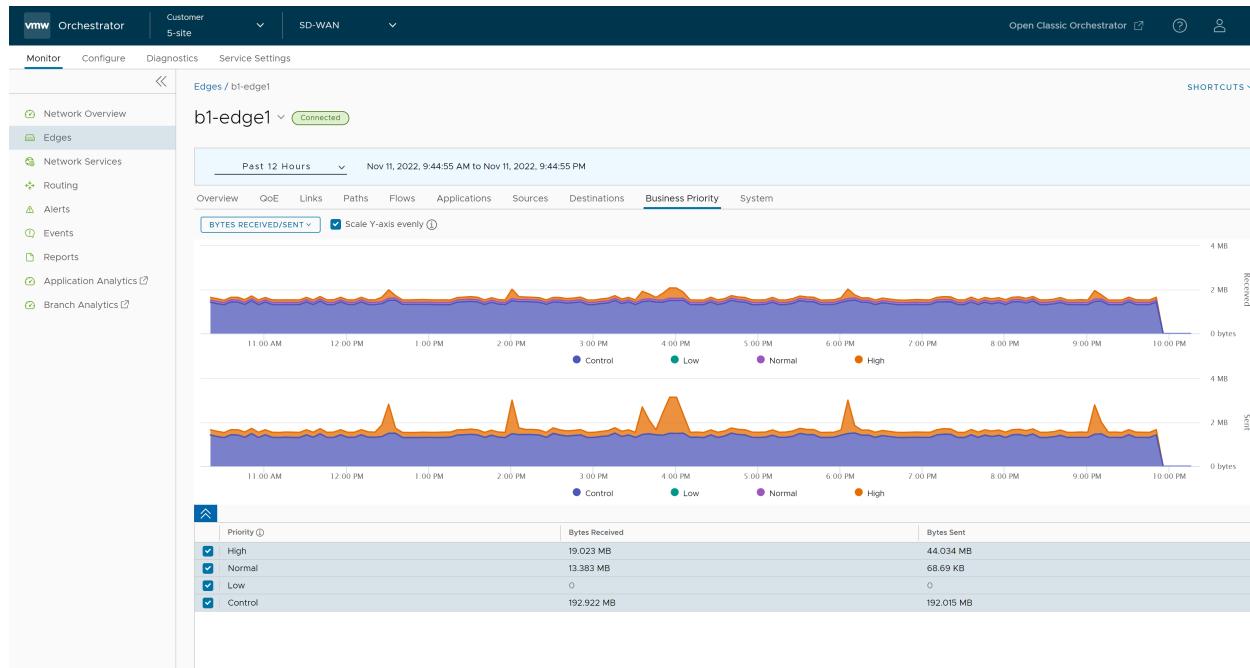
To view the details of business priorities of the network traffic:

### Procedure

- In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- Click the link to an Edge, and then click the **Business Priority** tab.

### Results

The **Business Priority** tab displays the details of the priorities of the network traffic for the selected Edge.



At the top of the page, you can choose a specific time period to view the details of the priorities for the selected duration.

Choose the metrics from the drop-down to view the details related to the selected parameter.

By default, the **Scale Y-axis evenly** check box is selected. This option synchronizes the Y-axis between the charts. If required, you can turn off this option.

Hover the mouse on the graphs to view more details.

The bottom panel displays the details of the selected metrics for the business priorities.

## Monitor System Information of an Edge

You can view the detailed network usage by the system for a specific Edge.

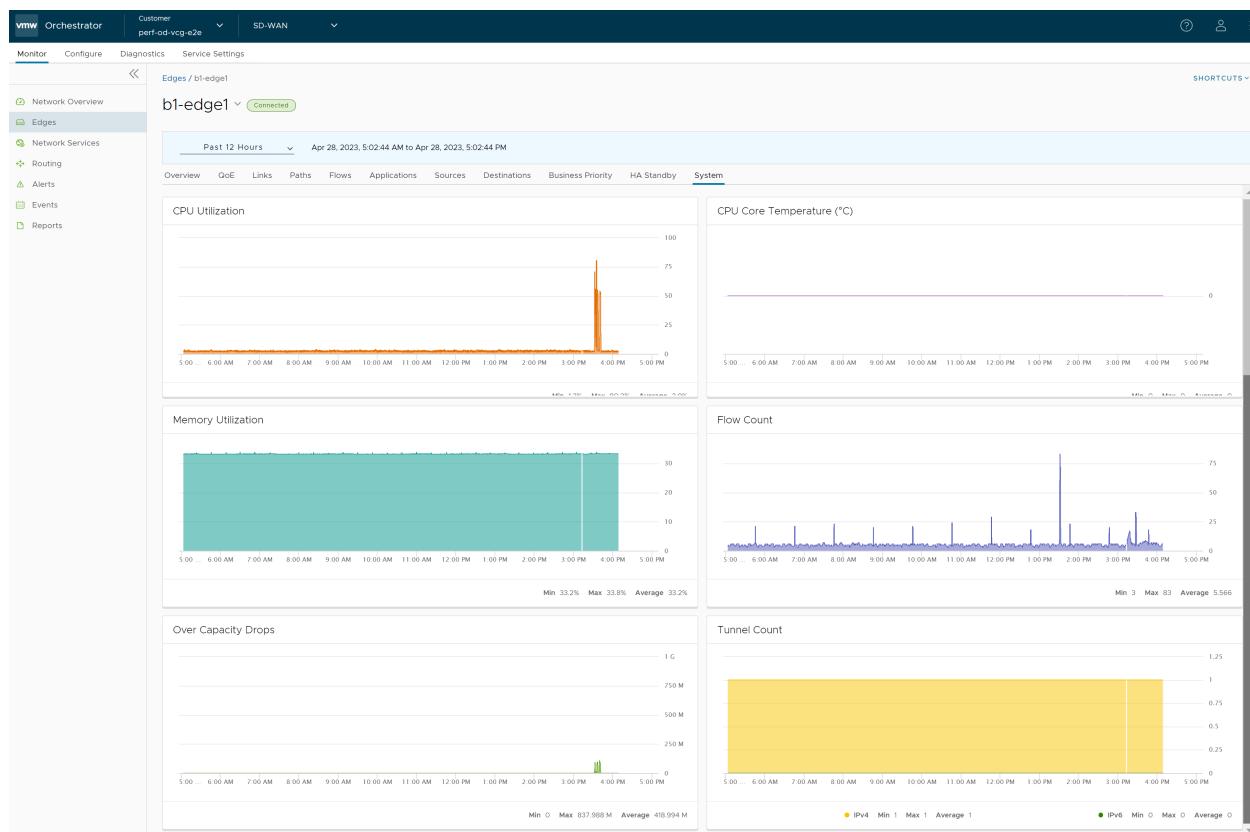
To view the details of system information:

### Procedure

- In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- Click the link to an Edge and click the **System** tab.

### Results

The **System** tab displays the details of network usage by the system for the selected Edge.



The page displays graphical representation of usage details of the following over the period of selected time duration, along with the minimum, maximum, and average values.

- **CPU Utilization** – Percentage of usage of CPU.
- **CPU Core Temperature** – The core temperature of the Edge CPU.

**Note** The "CPU Core Temperature" feature is supported only for Edges running 5.1 and later versions.

- **Memory Utilization**– Percentage of usage of memory.
- **Flow Count** – Count of traffic flow.
- **Over Capacity Drops** – Total number of packets dropped due to over capacity since the last sync interval. Occasional drops are expected, usually caused by a large burst of traffic. However, a consistent increase in drops usually indicates an Edge capacity issue.
- **Tunnel Count** – Count of tunnel sessions.

Hover the mouse on the graphs to view more details.

## Monitoring High Availability Edges

The Orchestrator includes special monitoring for a site deployed with a High Availability topology which are outlined in this section.

## Overview

Beginning in Release 5.2.0, the Orchestrator includes improved monitoring for sites deployed in a High Availability topology:

- In the **SD-WAN** service of the Enterprise portal, the **Monitor > Edge > Overview** tab now includes two HA specific improvements:
  - WAN link information includes which HA Edge the link is associated with by serial number, which is especially important with Enhanced HA deployments.
  - HA Interface Status.
- HA specific failover bars on the **Monitor > Edge > System** tab denoting where an HA Edge site failed over.
- A new **Monitor > Edge > HA Standby** tab for Standby Edge monitoring information.

### High Availability specific information on the Monitor > Edge > Overview tab

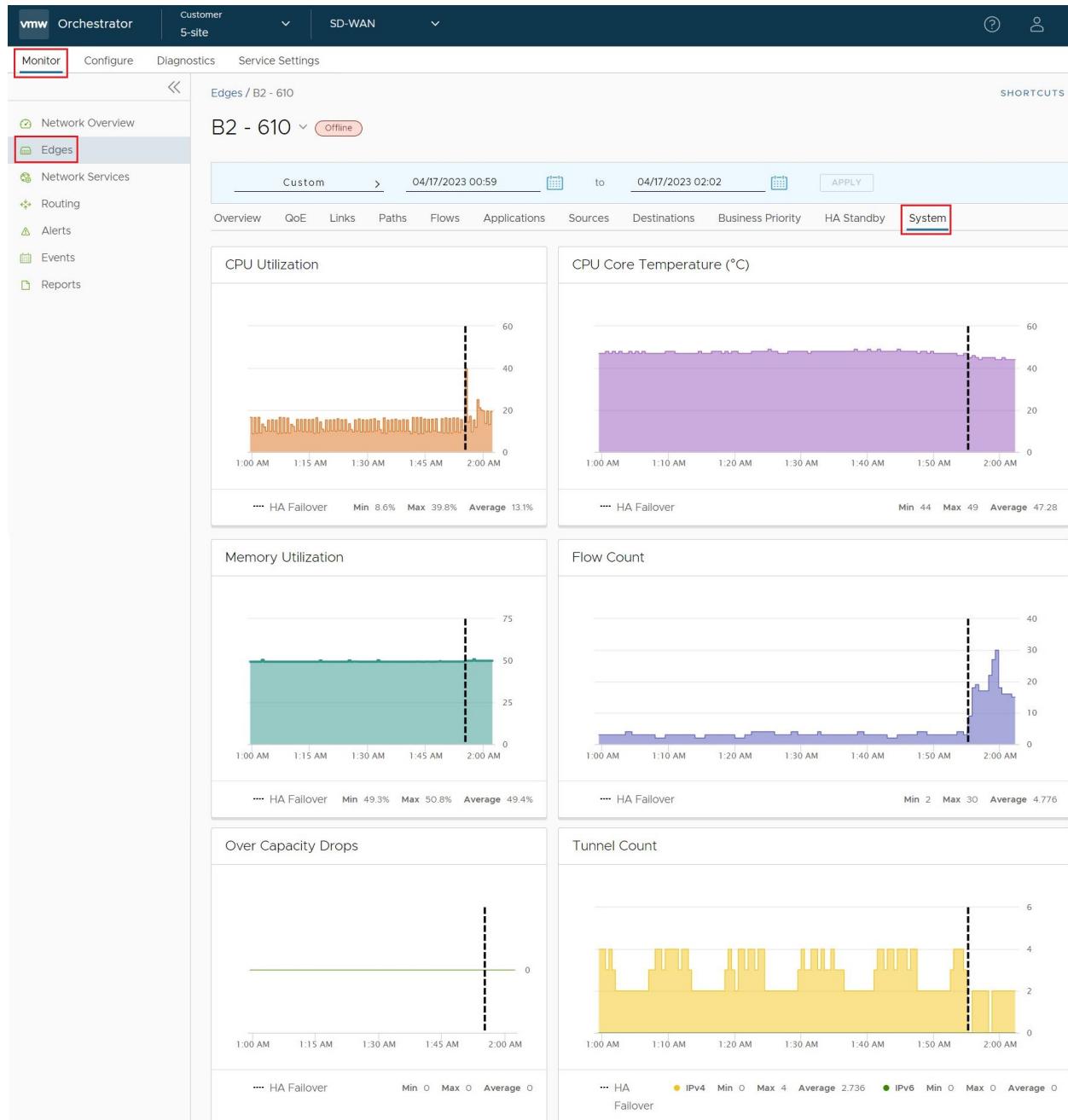
In the **SD-WAN** service of the Enterprise portal, when you navigate to the **Monitor > Edge > Overview** tab, a site deployed in High Availability has added information specific to an HA deployment:

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar shows 'vmw Orchestrator', 'Customer 5-site', 'SD-WAN', and user icons. The left sidebar has links for Network Overview, Edges, Network Services, Routing, Alerts, Events, and Reports. The main content area is titled 'Edges / B2 - 610' and shows 'B2 - 610' as offline. It has a date range selector from '04/17/2023 00:59' to '04/17/2023 02:02' with an 'APPLY' button. Below this are tabs for Overview, QoE, Links, Paths, Flows, Applications, Sources, Destinations, Business Priority, HA Standby, and System. The 'Overview' tab is selected. Under 'Overview', there is a 'Links' table with columns: Links, Auto Dual-Mode SIM, Device Serial No (Device State), Link Status, Interface (WAN Type), Throughput | Bandwidth, Pre-Notifications, Alerts, and Sign. One row is highlighted with a red box, showing '169.254.6.42' and 'GYKJIV43 (ACTIVE)'. To the right of the table is a 'Link Status' table with columns: Name, Interface Status, and Interface (HA Type). It shows '169.254.2.1' with 'Up' status and 'GE1 (standard)' type. The 'HA Interface Status' section is also highlighted with a red box.

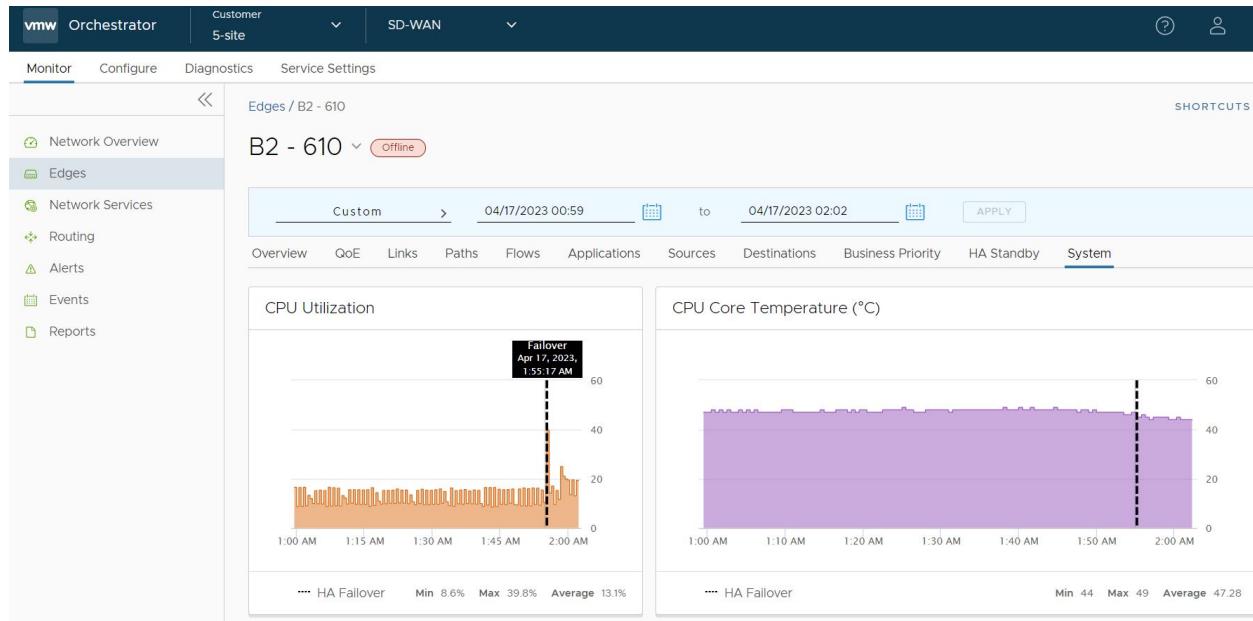
- In the **Link Status** section, each connected WAN link includes a column **Device Serial No (Device State)** that includes the Edge serial number associated with that WAN link and the HA status of that Edge (Active or Standby). This information is valuable in Enhanced HA deployments where WAN links are uniquely associated to different HA Edges and allows you to see the status of WAN links on the Standby Edge just as you see them on the Active Edge.
- The **Overview** tab adds an **HA Interface Status** section which includes the IP Address, Interface Status (Up or Down), and Interface (HA Type).

## High Availability Failover Bars on the System tab

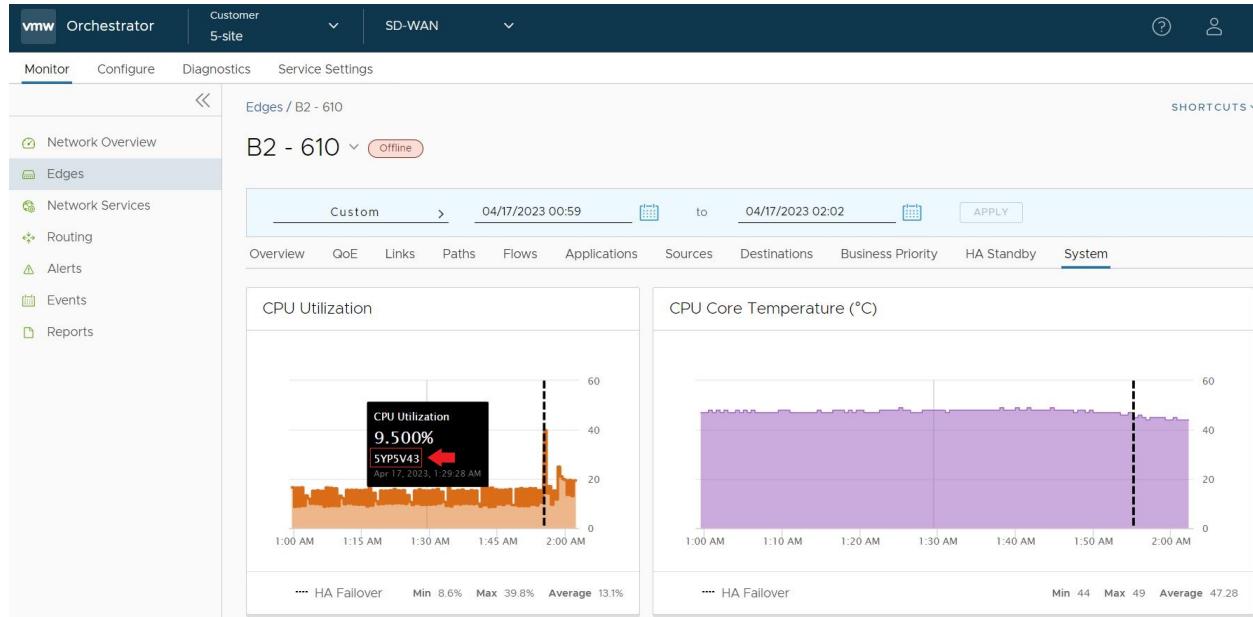
In the **SD-WAN** service of the Enterprise portal, when you navigate to the **Monitor > Edge > System** tab, a site deployed in High Availability has additional functionality which is best seen when a HA failover has occurred. When an HA failover occurs, the Orchestrator renders a vertical bar marking the point of the failover.



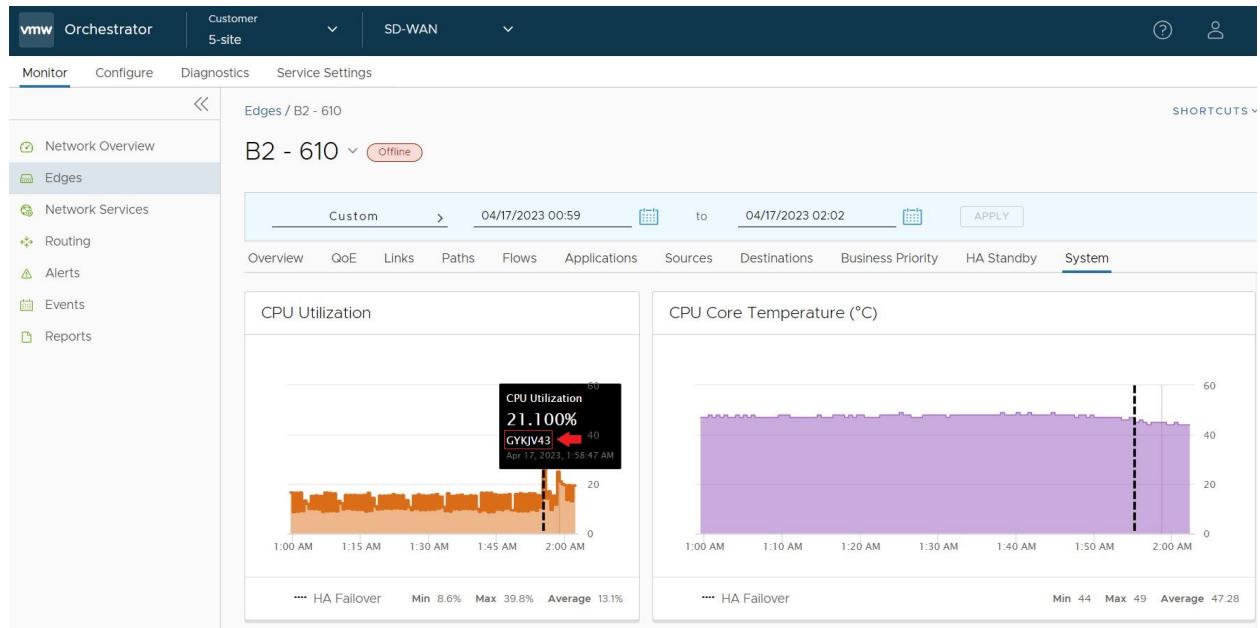
Focusing on the CPU Utilization graph, if a user hovers their mouse on the bar, the bar indicates when the failover occurred. This failover bar represents a boundary marking how the System statistics apply to each respective HA Edge when they serve as the Active Edge.



If you click on the graph to the left (earlier) side of the failover bar, the Orchestrator will indicate which Edge was Active at the time of those statistics. In this example, the Active Edge prior to the failover was Edge serial # SYP5V43.



If you click on the graph to the right (later) side of the failover bar, the Orchestrator indicates that the Active Edge for the post-failover statistics is Edge serial # GYKJV43. In this way you can always know which Edge applies to which System values.



## The Monitor > Edge > HA Standby Tab

You can now view the System Health statistics for the HA Edge when it is serving a standby role by clicking on the **Monitor > Edge > HA Standby** tab. This page also includes a failover bar indicating when an HA site has triggered a failover and there is now a different Edge in the role of Standby.

Monitor   Configure   Diagnostics   Service Settings

Edges / B2 - 610   SHORTCUTS

**B2 - 610** (offline)

Custom   04/17/2023 00:59   to   04/17/2023 02:02   APPLY

Overview   QoE   Links   Paths   Flows   Applications   Sources   Destinations   Business Priority   **HA Standby**   System

Standby Edge: 5YP5V43 ①

**CPU Utilization**

Min 8.5% Max 16.4% Average 12.3%

... HA Failover

**CPU Core Temperature (°C)**

Min 45 Max 48 Average 46.874

... HA Failover

**Memory Utilization**

Min 48.4% Max 49.5% Average 48.5%

... HA Failover

**WAN Interface**

Name	Interface Status	Interface(WAN Type)
169.254.6.42 169.254.6.42	● DOWN	GE3 (Ethernet)
0.0.0.0 0.0.0.0	● DOWN	GE4 (Ethernet)
0.0.0.0 0.0.0.0	● DOWN	GE5 (Ethernet)
0.0.0.0 0.0.0.0	● DOWN	GE6 (Ethernet)
0.0.0.0 0.0.0.0	● DOWN	SFP1 (Ethernet)
0.0.0.0 0.0.0.0	● DOWN	SFP2 (Ethernet)

6 items

The **HA Standby** tab also provides live **WAN Interface** information which is especially helpful in Enhanced HA deployments where the Standby Edge is using unique WAN links.

Click on the information button to get Standby Edge information at the same level as what a user sees on the **Monitor > Edge > Overview** tab for the Active Edge.

The screenshot shows the VMware SD-WAN Administration Guide interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnostics', and 'Service Settings'. The 'Monitor' tab is selected. The left sidebar has links for 'Network Overview', 'Edges' (which is selected), 'Network Services', 'Routing', 'Alerts', 'Events', and 'Reports'. The main pane shows 'Edges / B2 - 610' and 'B2 - 610' status as Offline. A red arrow points to the 'Standby Edge: 5YP5V43' link. The right side displays detailed device information for 5YP5V43, including Activation pending, Edge Info, High Availability, Device Hardware, Device Software, Device Firmware, Modem Version, Configuration Profile, and Quick Start Profile.

## Monitor Network Services

You can view the details of configured network services for an Enterprise.

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services**. You can view the configuration details of the following network services:

- Monitor Non SD-WAN Destinations through Gateway
- Monitor Non SD-WAN Destinations through Edge
- Monitor Cloud Security Service Sites
- Monitor Edge Clusters
- Monitor Zscaler IaaS Subscription
- Monitor Edge VNFs

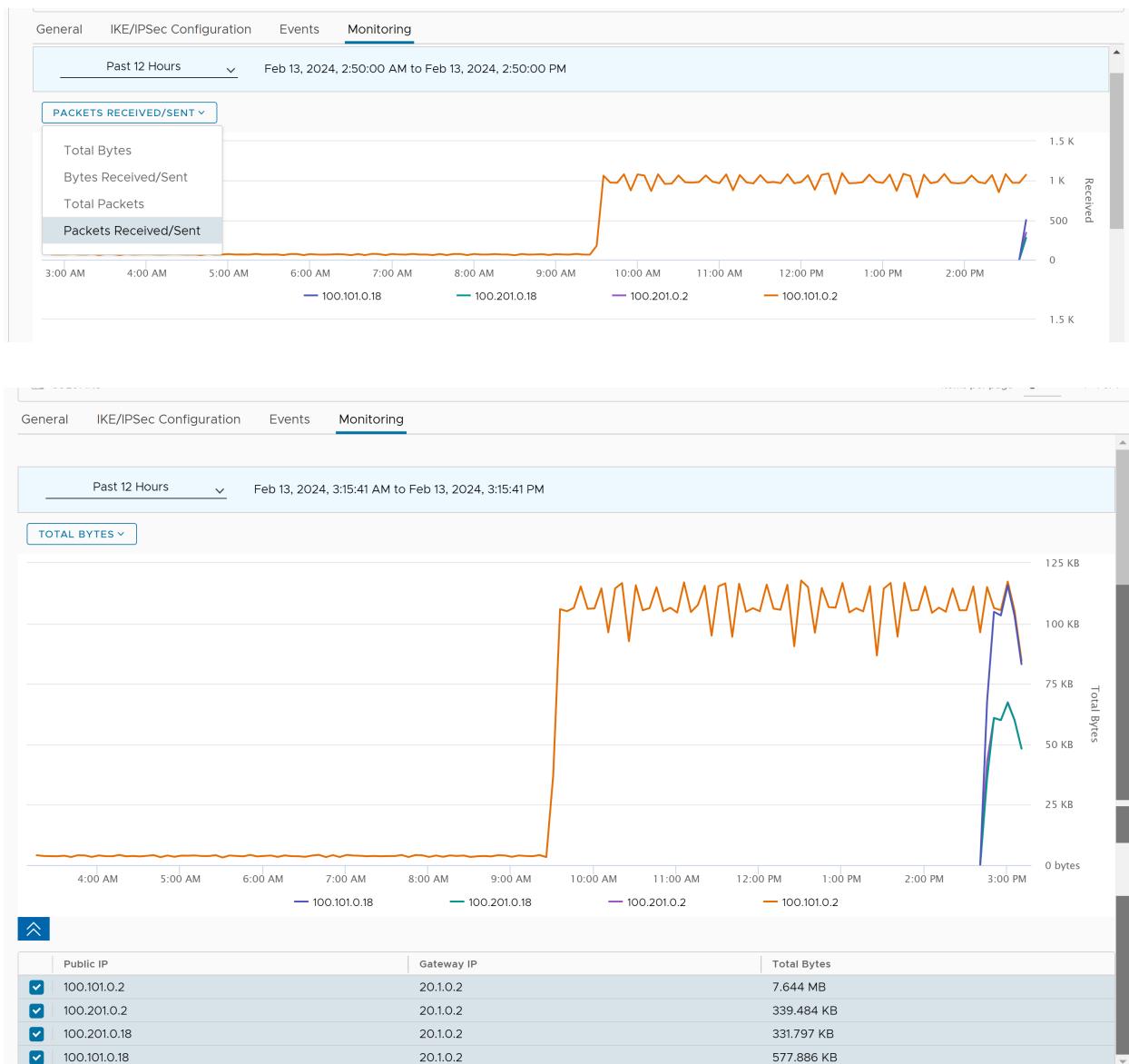
## Monitor Non SD-WAN Destinations through Gateway

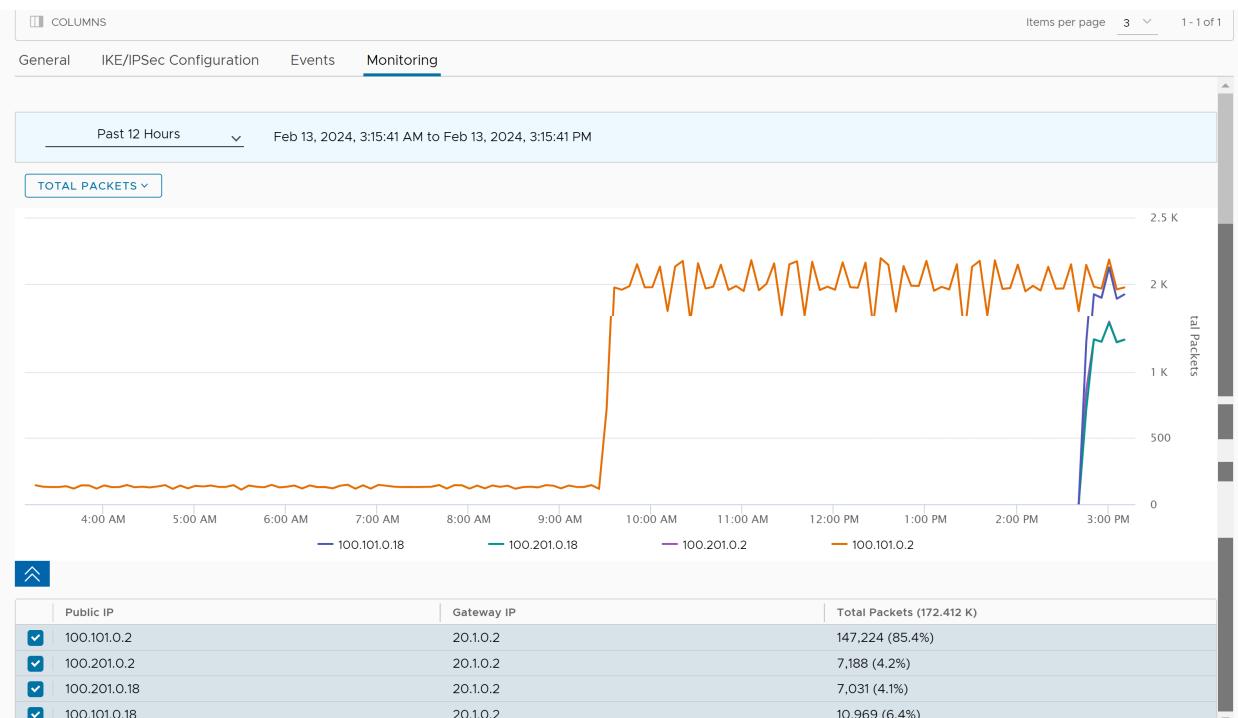
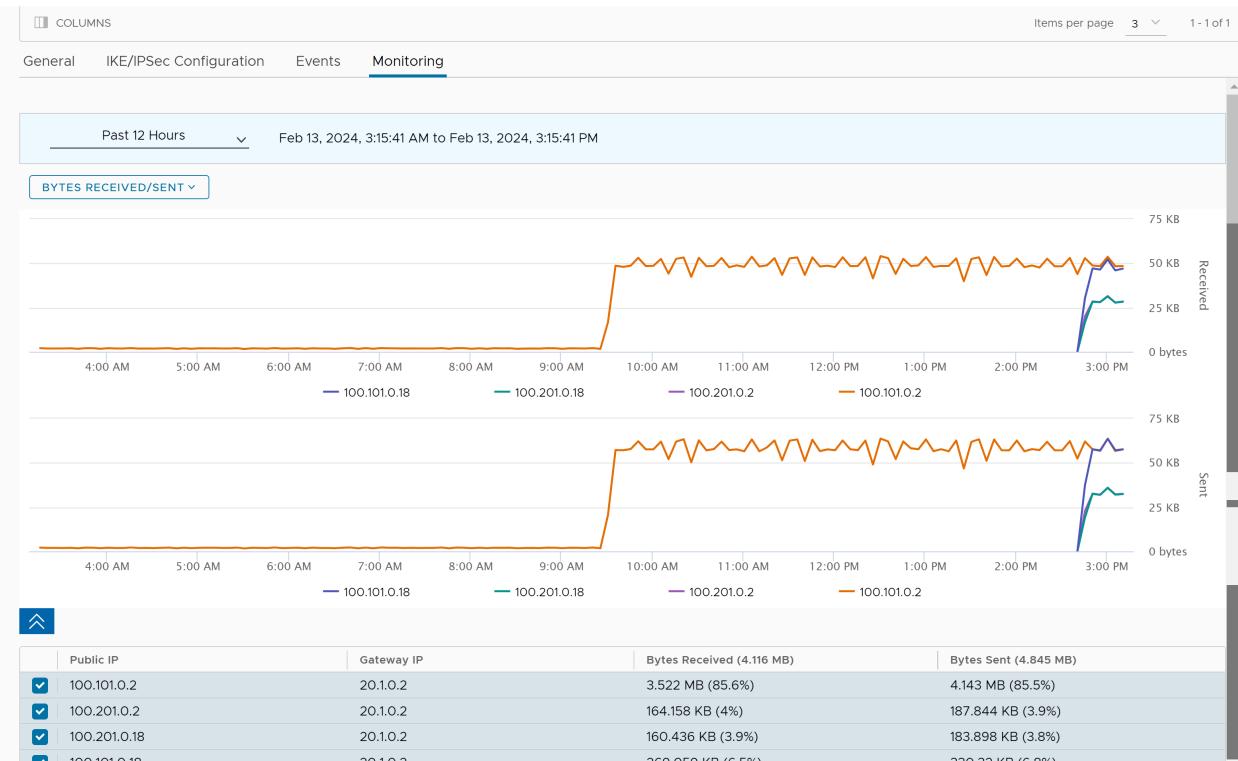
You can view the configured Non SD-WAN Destinations along with the VPN Gateways, Site Subnets, and other configuration details.

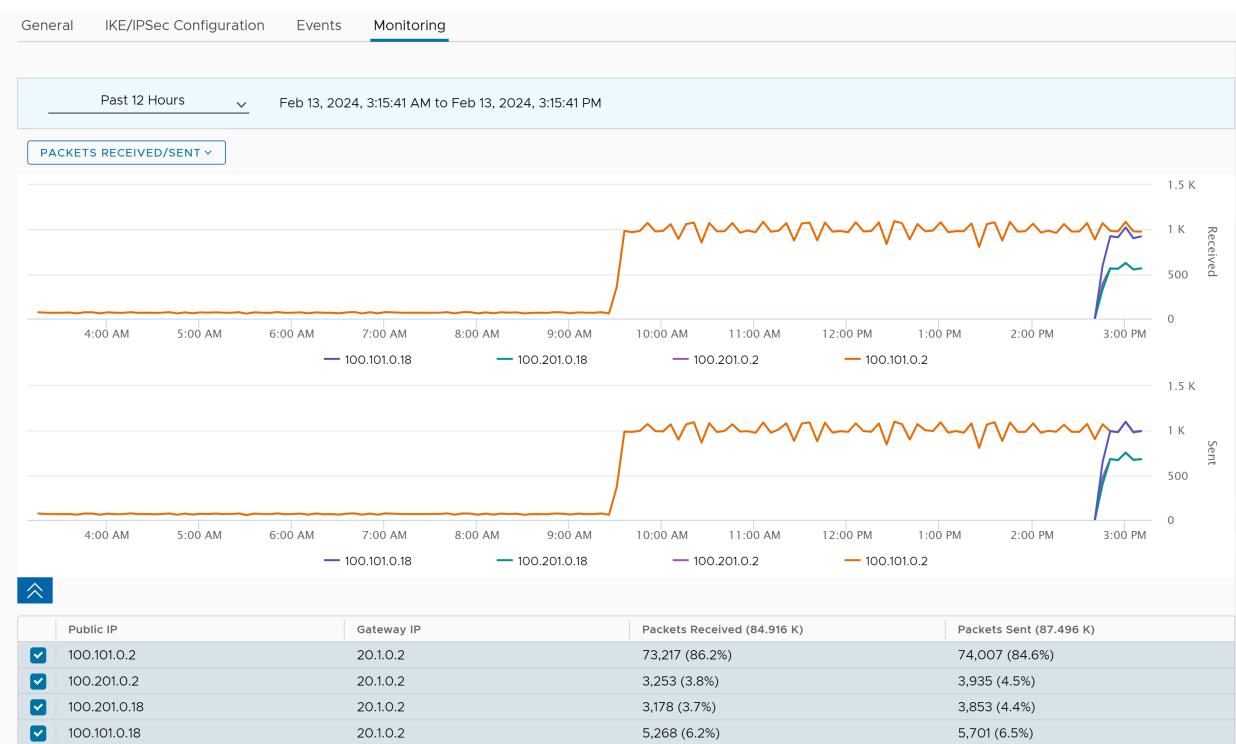
To view the configured Non SD-WAN Destinations:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services**. The **Non SD-WAN Destinations via Gateway** tab is displayed.

The **Non SD-WAN Destinations via Gateway** tab displays the details of already configured Non SD-WAN Destinations. To configure the Non SD-WAN Destinations via Gateway, see [Configure Non SD-WAN Destinations via Gateway](#).







## Graphical Monitoring Options

Options	
Total Bytes	
Bytes Received/Sent	
Total Packets	
Packets Received/Sent	

The page displays the following details: Name of the Non SD-WAN Destination, Public IP Address, Status of the Non SD-WAN Destination, Status of the tunnel, Number of profiles and Edges that use the Non SD-WAN Destination, and last contacted date and time.

You can also sort the report by clicking the header of each column. You can use the Filter icon displayed next to the header to filter the details by specific Name, IP address, or Status.

Click a Non SD-WAN Destination to view the following details in the bottom panel:

Options	Description
General	Displays the Name, Type, IP address and tunnel settings of Primary and Secondary VPN Gateways, location details, and Site subnet details.
IKE/IPSec Configuration	Click the tab to view sample configuration template for Primary and Secondary VPN Gateways. You can copy the template and customize the settings as per your requirements.

Options	Description
Events	Click the tab to view the events related to the selected Non SD-WAN Destination. Click the arrow displayed in the first column to view more details of an event.
Monitoring	Click the tab to view the NSD tunnels display statistics in both table and chart format of the Bytes, Packets sent and received.

## Monitor Non SD-WAN Destinations through Edge

You can view the configured Non SD-WAN Destinations along with the VPN Gateways, Site Subnets, and other configuration details.

To view the configured Non SD-WAN Destinations through Edge:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services > Non SD-WAN Destinations via Edge**. The **Non SD-WAN Destinations via Edge** tab appears.

The **Non SD-WAN Destinations via Edge** tab displays the details of already configured Non SD-WAN Destinations. To configure the Non SD-WAN Destinations via Edge, see [Configure Non SD-WAN Destinations via Edge](#).

Name	Public IP	Tunnel Status	Used By	Last Contact	Deployment Status
NSD_via_B3_IPv4 Generic IKEv2 Router (Route Based VPN)	14.1.1.1 14.1.1.3	1 Down 1 Up	1 Profile 0	N/A	

The page displays the following details: Name of the Non SD-WAN Destination, Public IP Address, Status of the tunnel, Number of Profiles and Edges that use the Non SD-WAN Destination, last contacted date and time, and deployment status of Edge.

You can also sort the report by clicking the header of each column. You can use the Filter Icon displayed next to the header to filter the details by specific Name, IP address, or Status.

Clicking a Non SD-WAN Destination displays Name, Type, IP address and tunnel settings of Primary and Secondary VPN Gateways, location details, and Site subnet details under the **General** tab.

## Monitor Cloud Security Service Sites

You can view the details of Cloud Security Services configured for the Enterprise.

To monitor the Cloud Security Services:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services > Cloud Security Service Sites**.

The **Cloud Security Service Sites** tab displays the already configured Cloud Security Services. To configure a Cloud Security Service, see [Chapter 11 Cloud Security Services](#).

Name	Type	Public IP	Status	Tunnel Status	Service Status	State Changed Time	Deployment Status
CSS IPsec	Zscaler Cloud Security Service	199.168.148.132 104.129.194.39	All Up	2 Standby 2 Up	4 Unknown	Apr 20, 2023, 2:52:22 PM (a few seconds ago)	<a href="#">VIEW</a>

Edge	Identifier	Public IP	State	State Changed Time
b1-edge1	satheesh@velocloud.net	199.168.148.132	Up	Apr 20, 2023, 2:52:52 PM (2023-04-20T09:22:52.593Z)
b1-edge1	Link 00000003-55f7-4848-a0ba-e287b4f3b35d	104.129.194.39	Standby	Apr 20, 2023, 2:52:52 PM (2023-04-20T09:22:52.593Z)
b1-edge1	Link 00000003-55f7-4848-a0ba-e287b4f3b35d	104.129.194.39	Standby	Apr 20, 2023, 2:52:52 PM (2023-04-20T09:22:52.593Z)
b1-edge1	satheesh@velocloud.net	199.168.148.132	Up	Apr 20, 2023, 2:52:52 PM (2023-04-20T09:22:52.593Z)
b1-edge1	satheesh@velocloud.net	104.129.194.39	Up	Apr 19, 2023, 2:25:00 PM (2023-04-19T08:55:00.633Z)
b1-edge1	satheesh@velocloud.net	104.129.194.39	Up	Apr 19, 2023, 2:24:30 PM (2023-04-19T08:54:30.621Z)

The page displays the following details: Name, Type, IP address of the CSS provider, overall status of the CSS provider, status of tunnels created from the CSS provider from different Edges, status of the external service as recorded by each Edge, date and time by when the state change occurred, and the deployment status of the CSS provider.

You can also sort the report by clicking the header of each column. You can use the Filter Icon displayed next to the header to filter the details by specific Name, Type, IP address, or Status.

Click a Cloud Security Service to view the related state change events along with the IP address and State, in the bottom panel.

Click the **View** link in the **Deployment Status** column to view the deployment status of the CSS provider.

## Monitor Zscaler IaaS Subscription

You can view the configured Zscaler IaaS Subscription from the **Monitor > Network Services** page.

To view the Zscaler IaaS Subscription:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services > Zscaler IaaS Subscription**.

The **Zscaler IaaS Subscription** tab displays the details of already configured Zscaler IaaS subscriptions. To configure a new IaaS subscription, see [Configure API Credentials](#).

Name	Deployment Status
No Zscaler IaaSSubscription found	

The page displays the name of the service along with the deployment status.

## Monitor Edge Clusters

You can view the details of the configured Edge Clusters and the usage data.

To view the details of Edge clusters:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services > Edge Clusters**.

The **Edge Clusters** tab displays the details of already configured Edge clusters. To configure the clusters, see [Configure Clusters and Hubs](#).

Cluster Name	Edges	CPU Utilization	Memory Utilization	# Tunnels	Flow Count	# Over Capacity Drops
HUB_CLUSTER1	b1-hub1 b1-hub2 b1-hub3	4.00% 4.00% 5.00%	13.00% 13.00% 13.00%	251 182 214	220 2837 5062	1975 7921156 20901588
HUB_CLUSTER2	b2-hub1 b2-hub2	2.00% -	14.00% 13.00%	627 12	111 99	- -
CLUSTER3	b2-hub3	-	13.00%	12	114	-

This page displays the following details:

Option	Description
Cluster Name	Name of the Cluster as configured under <b>Configure &gt; Network Services &gt; SD-WAN Destinations &gt; Clusters and Hubs.</b>
Edges	Name of the Hub Edges that are a part of this Cluster.
CPU Utilization	Percentage value of CPU utilization of the corresponding Edge.
Memory Utilization	Percentage value of memory utilization of the corresponding Edge.
# Tunnels	Number of tunnels associated with the Hub Edge that is a part of the Cluster.
Flow Count	Number of flows associated with the Hub Edge that is a part of the Cluster.
# Over Capacity Drops	Number of packets that are dropped when they exceed over capacity of Hub Edge in the Cluster.

**Note** Starting from the 5.2.0 release, **# Handoff Queue Drops** field has been renamed to **# Over Capacity Drops**.

## Monitor Edge VNFs

You can view the details of the configured Edge VNFs and the VM status.

To view the Edge VNFs:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services > Edge VNFs**.

The **Edge VNFs** tab displays the details of already configured VNFs. To configure VNF on an Edge, see [Configure Edge Services](#).

Service	Used By	Edge VM Status
ft Fortinet Security Firewall	1 Edge	Powered On (Insertion Enabled) 1 Edge

Edge Name	Edge VM Status
b2-edge1-520v	Powered On (Insertion Enabled)

The page displays the following details: Name of the VNF Service, Number of Edges that use the VNF, and VM status.

Click a VNF to view the corresponding VNF Edge deployment details.

## Monitor Routing Details

You can view the routing services configured in the Enterprise.

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Routing**. You can view the details of following routing services:

- Monitor Multicast Groups
- Monitor PIM Neighbors
- Monitor BGP Edge Neighbor State
- Monitor BFD
- Monitor BGP Gateway Neighbor State
- Gateway Route Table

## Monitor Multicast Groups

You can view the multicast groups configured for the Enterprise.

To view the multicast groups:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Routing**. The **Multicast Groups** tab is displayed.

The **Multicast Groups** displays the details of already configured multicast group settings. To configure multicast groups, see [Configure Multicast Settings for Profiles](#).

Segment	Multicast Group	Source Address	RP	Multicast Edges	Created	Last Update
Global Segment	224.0.140	*	1.1.1.1	2 Edges	7 days ago	10 hours ago
Global Segment	224.112	*	1.1.1.1	3 Edges	10 months ago	9 months ago
Global Segment	224.111	*	1.1.1.1	9 Edges	10 months ago	10 hours ago
Global Segment	227.1.111	*	1.4.1.1	2 Edges	10 months ago	9 months ago
Global Segment	227.11.9	*	1.4.1.1	2 Edges	10 months ago	9 months ago
Global Segment	227.1110	*	1.4.1.1	2 Edges	10 months ago	9 months ago

**Multicast Group Members**

Multicast Edges	Upstream	Downstream
b1-hub2 View PIM Neighbors	GE6	b8-edge1
b8-edge1 View PIM Neighbors	b1-hub2 - 1	

The page displays the following details: multicast group address, segment that consist of the multicast group, Source IP address, RP address, number of Edges in the multicast group, created time period, and the last updated time period.

Click a multicast group to view the details of the Edges in the group, along with the upstream and downstream information. Click **View PIM Neighbors** to view the detail of the PIM neighbors connected to a specific Edge.

## Monitor PIM Neighbors

You can view the details of Edges and the PIM neighbors available in the multicast groups.

To view the PIM neighbors:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Routing > PIM Neighbors**.

The **PIM Neighbors** tab displays the Edges available in the multicast groups.

Segment	Edge Name	Interface	Address	Created	Last Update
Global Segment	b1-hub1		10.11.1	Dec 8, 2020, 10:04:17 AM	Dec 8, 2020, 4:18:31 PM
Global Segment	b4-hub-edge2000		10.4.11	Dec 8, 2020, 5:50:20 PM	Dec 8, 2020, 2:46:29 PM
Global Segment	b1-hub2		10.12.1	Dec 8, 2020, 2:46:29 PM	Dec 8, 2020, 4:17:23 PM

Select an Edge to view the PIM neighbors connected to the Edge. The **PIM Neighbors** section displays the following details: Segment of the multicast group, Edge name, Interface details, IP address of the neighbor, created and last updated date with time.

## Monitor BGP Edge Neighbor State

You can view the details BGP neighbors connected to Edges.

To view the BGP neighbors connected to Edges:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Routing > BGP Edge Neighbor State**.

The **BGP Edge Neighbor State** tab displays the Edges connected as BGP neighbors, when you have configured BGP settings on the Edges.

Edge Name	Segment	Neighbor IP	State	State Changed Time	# Msg Received	# Msg Sent	# Events	Up/Down	# Prefix Received
b2-edge1	Global Segment	10.2.1.25	● Active	May 16, 2023, 8:23:34 PM 19 hours ago	0	0	121	Never	0
b2-edge1		10.2.1.25	● Removed	Mar 3, 2022, 9:54:51 PM 1 year ago	0	0	8		0
b1-edge1	Global Segment	172.21.1.2	● Idle	May 16, 2023, 9:02:12 PM 19 hours ago	9,443	8,781	52	Never	0
b1-edge1		172.21.1.2	● Removed	Mar 3, 2022, 9:58:52 PM 1 year ago	640	285	7		0

State Changed Time	State	# Msg Received	# Msg Sent	Up/Down	# Prefix Received
Nov 19, 2020, 9:59:13 AM 2 years ago	● Active	0	0	Never	0
Nov 19, 2020, 9:58:14 AM 2 years ago	● Connect	0	0	Never	0
Nov 19, 2020, 9:42:12 AM 2 years ago	● Active	0	0	Never	0
Nov 19, 2020, 9:41:13 AM 2 years ago	● Connect	0	0	Never	0
Nov 19, 2020, 9:21:10 AM 2 years ago	● Active	0	0	Never	0

The page displays the following details: Edge name, IPv4 and IPv6 address of the neighbor, State of the neighbor, Date and time of the state change, number of messages received and sent, number of Events, duration for which the BGP neighbor is Up/Down, and number of prefixes received.

Click an Edge name to view the corresponding event details. The **Related State Change Events** section displays the change in the state and other details for the selected Edge.

### Note

- You can click the Filter Icon next to the **Search** option to filter the details by Edge Name, Neighbor IP, Neighbor IP Type, and Status.
- BGP Edge Neighbor State (API: monitoring/getEnterpriseEdgeBgpPeerStatus): At the time of calling the API, if the Edge state is "OFFLINE", then the user interface displays the neighbor state as "Unavailable" with appropriate tooltip showing the current Edge state to the user.

## Monitor BFD

You can view the BFD sessions on Edges and Gateways.

To view the BFD sessions:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Routing > BFD**.

The **BFD** tab displays the details of already configured BFD sessions. To configure BFD, see [Configure BFD for Profiles](#).

Edge	Segment	Peer Address	Local Address	State	Remote Timers	Local Timers	Events	Session Time
b1-hub3	Global Segment	1199.1	172.21.120	Down	rx: 300ms / tx: 300ms	rx: 300ms / tx: 300ms	110	<a href="#">View</a>
b1-hub2	Global Segment	1199.1	172.21.10	Down	rx: 300ms / tx: 300ms	rx: 300ms / tx: 300ms	104	<a href="#">View</a>
b1-hub1	Global Segment	1199.1	172.21.12	Down	rx: 300ms / tx: 300ms	rx: 300ms / tx: 300ms	120	<a href="#">View</a>
b4-hub-edge2000	Global Segment	14.1.1	14.1.100	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	87	<a href="#">View</a>
b4-hub-edge2000	segment1	14.1.1	14.1.100	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	33	<a href="#">View</a>
b4-hub-edge2000	segment2	14.1.2.1	14.1.102	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	120	<a href="#">View</a>
b9-edge1_E540	Global Segment	19.1.1	19.1.100	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	120	<a href="#">View</a>
b1-hub2	Global Segment	172.21.11	172.21.10	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	120	<a href="#">View</a>

Gateway	Segment	Peer Address	Local Address	State	Remote Timers	Local Timers	Events	Session Time
No BFD events available for selected enterprise								

The page displays the following details for the Edges and Gateways: Name of the Edge or Gateway, Segment name, Peer IP address, Local IP address, State of the BFD session, Remote and Local timers, number of Events, and duration of the BFD session.

Click the link to an event number to view the break-up details of the events.

## Monitor BGP Gateway Neighbor State

You can view the details of the BGP neighbors connected to Gateways.

To view the BGP neighbors connected to Gateways, follow the steps below.

### Procedure

- In the **SD-WAN** service of the Enterprise portal, click **Monitor > Routing > BGP Gateway Neighbor State**.
- Click a Gateway name to view the corresponding event details.

The **Related State Change Events** section displays the change in the state and other details for the selected Gateway.

3

The **BGP Gateway Neighbor State** tab displays the details of Gateways connected to BGP neighbors.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'Customer 7-site' and 'SD-WAN'. The left sidebar has sections: Network Overview, Edges, Network Services, **Routing** (selected), Alerts, Events, Reports, Application Analytics, and Branch Analytics. The main content area is titled 'Routing' and shows the 'BGP Gateway Neighbor State' table. The table has columns: Gateway, Segment, Neighbor IP, State, State Changed Time, # Msg Received, # Msg Sent, # Events, Up/Down, and # Prefix Received. It lists four entries: gateway-1 (Global Segment, 101.101.101.2, Established, May 17, 2023, 3:50:30 PM a few seconds ago, 0, 57, 0, Never, 0); gateway-1 (SEG1, 101.101.101.2, Established, May 17, 2023, 3:50:30 PM a few seconds ago, 6,776, 6,757, 119, 01:52:35, 40); gateway-1 (101.101.101.3, Removed, Mar 3, 2022, 6:57:01 PM 1 year ago, 0, 0, 2, 0); and gateway-4 (104.104.104.10, Removed, Mar 3, 2022, 6:57:19 PM 1 year ago, 348,994, 348,738, 3, 36). Below the table are tabs for 'Related State Change Events', 'BGP Received Routes', and 'BGP Advertised Routes'. The 'Related State Change Events' table shows four entries for May 17, 2023, 3:50:30 PM a few seconds ago, all in an 'Established' state with 6,776 received and sent messages, 01:52:35 up/down, and 40 prefix received.

**Note** BGP Gateway Neighbor State (API: monitoring/getEnterpriseBgpPeerStatus): At the time of calling the API, if the Gateway state is one out of "QUIESCED", "OUT\_OF\_SERVICE" or "OFFLINE", then the user interface displays the Neighbor state as "Unavailable" with appropriate tooltip showing the current Gateway state to the user.

## BGP Received Routes and BGP Advertised Routes

For the 5.2 release, the BGP Gateway Neighbor State feature is enhanced with the BGP Received Routes and BGP Advertised Routes.

The BGP Received Routes displays routes (up to 16K) that have been received from the selected BGP neighbor at the Gateway, providing valuable insight into the routing information that is available in the network. This information can be used to troubleshoot connectivity issues in Customer deployments. The BGP Advertised Routes displays all routes that are being advertised to a selected BGP neighbor, providing visibility into the routes that are being used to reach destinations in the network (as shown in the image above the previous paragraphs).

See the table below for a detailed description of the fields in the BGP Received and Advertise Routes table.

**Table 7-4. BGP Received Routes and BGP Advertise Routes**

Status Code	Displays the status code of the BGP route, as follows: ■ * valid ■ > best ■ = multipath ■ i-internal
Network Prefix/Mask	Displays the prefix carried by the BGP route.
Next Hop	Displays the Next-hop IP address that is used by BGP to reach the BGP prefix.
Metric	Displays the MED (multi-exit discriminator) value associated with a route.
Local Preference	Displays the local preference value assigned by a BGP router to a route.
Weight	Displays the weight value assigned by the BGP router to a route.
AS Path	Displays the list of AS Path numbers that are carried by the BGP route.
Community	Displays the community attribute carried by the BGP route.
CSV	Click the CSV button to export the data to an Excel sheet.

## Gateway Route Table

The Gateway Route Table is a new feature for the 5.2 release that provides a comprehensive view of the routing information on an SD-WAN Gateway, displaying the routes (up to 16k) that are known to a Gateway, including both learned routes and statically configured routes.

The 5.2 release introduces the Gateway Route Table, which displays important information about each route, such as the Network Prefix and Mask Preference, Flags, and Metric, to name a few. The Gateway Route Table is updated in real-time, providing an up-to-date view of the routing information on a Gateway. It can be used to diagnose routing issues and to optimize routing policies.

To access the Gateway Route Table:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Routing > Gateway Route Table**, as shown in the image below.

The screenshot shows the VMware SD-WAN Orchestrator web interface. The top navigation bar includes 'vmw Orchestrator', 'Customer 5-site-csr', 'SD-WAN', and icons for help, user, and settings. Below the navigation is a menu bar with 'Monitor' (selected), 'Configure', 'Diagnostics', and 'Service Settings'. On the left, a sidebar lists 'Network Overview', 'Edges', 'Network Services', 'Routing' (selected), 'Alerts', 'Events', and 'Reports'. The main content area is titled 'Routing' and shows the 'Gateway Route Table'. It has tabs for 'Multicast Groups', 'PIM Neighbors', 'BGP Edge Neighbor State', 'BFD', 'BGP Gateway Neighbor State', and 'Gateway Route Table' (selected). Below the tabs are filters for 'Gateway' (set to 'GATEWAY-5'), 'Segment' (set to 'GLOBAL SEGMENT'), and 'Prefix' (with an input field 'Enter Prefix' and example '192.2.3.11/27 or 192.2.3.11'). There is also an 'APPLY' button and a 'CSV' download link. A search bar with placeholder 'Q, Search' and a help icon is at the top of the table. The table itself has columns: Network Prefix, Network Mask, Type, Peer Name, Reachable, Metric, Preference, Flags, Age, and C Tag. Two rows of data are shown:

Network Prefix	Network Mask	Type	Peer Name	Reachable	Metric	Preference	Flags	Age	C Tag
1.1.100.1	255.255.255.255	edge2edge	b1-edge1	true	0	0	CS	1239019	0
1.1.100.1	255.255.255.255	cloud	N/A	true	0	512	PSB	1240253	101

**Note** The WebSocket connection will be terminated and will ask to reconnect when the Gateway WebSocket connections are opened in two tabs for the same session, or if idle time for five minutes.

See the table below for a description of the fields in the Gateway Route Table.

**Table 7-5. Gateway Route Table Description**

Field	Description
Network Prefix	The destination address of the route. It specifies the network to which the route applies.
Network Mask	Displays the prefix carried by the BGP route.
Type	Indicates the type of routes: <ul style="list-style-type: none"> <li>■ edge2edge: remote routes received from Edges.</li> <li>■ datacenter: NSD BGP routes.</li> <li>■ cloud: PG BGP routes.</li> </ul>
Peer Name	Indicates the name of the BGP peer that learned the route.
Reachable	Indicates whether the route is reachable or not. If the route is reachable, it can be used for forwarding packets.
Metric	A value that represents the cost of using a particular route. Lower values indicate a lower cost.
Preference	A value that is used to influence the preferred path for outbound traffic. A lower value indicates a more preferred route.

**Table 7-5. Gateway Route Table Description (continued)**

Field	Description
Flags	Flags are listed below: <ul style="list-style-type: none"> <li>■ B BGP</li> <li>■ D DCE</li> <li>■ L LAN SR</li> <li>■ C Connected</li> <li>■ O External</li> <li>■ W WAN SR</li> <li>■ S SecureEligible</li> <li>■ s self</li> <li>■ r recursive</li> <li>■ H HA</li> <li>■ m Management</li> <li>■ n nonVeloCloud</li> <li>■ v ViaVeloCloud</li> <li>■ A RouterAdvertisement</li> <li>■ c CWS</li> <li>■ a RAS</li> <li>■ M MTGRE</li> <li>■ I IPSec</li> </ul>
Age	Indicates the amount of time that has elapsed since the route was last updated.
C Tag	Used to identify the customer that the route belongs to in a multi-tenant environment.
CSV	Click the <b>CSV</b> button to export the data to an Excel sheet.

## Monitor Alerts

SASE Orchestrator allows to configure alerts that notify the Enterprise Administrators or other support users, whenever an event occurs.

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Alerts**.

The **Alerts** window displays the alerts received for different type of events:

Trigger Time	Notification Time	Category	Type	Description	Status
> Dec 8, 2020, 5:51:26 PM	Dec 8, 2020, 5:53:33 PM	Customer	Edge CSS Tunnel Down	II.4.2.1 Edge CSS Tunnel Down on Edge b4-hub-edge2000	Closed
> Dec 8, 2020, 5:50:15 PM	Dec 8, 2020, 5:51:23 PM	Customer	Edge HA Failover	Edge b4-hub-edge2000	Closed
> Dec 8, 2020, 5:11:59 PM	Dec 8, 2020, 5:14:03 PM	Customer	Edge CSS Tunnel Down	II.4.2.1 Edge CSS Tunnel Down on Edge b4-hub-edge2000	Closed
> Dec 8, 2020, 5:11:00 PM	Dec 8, 2020, 5:12:03 PM	Customer	Link Up	Private (SPP) Link Up on Edge b3-hub-E840	Closed
> Dec 8, 2020, 5:10:45 PM	Pending	Customer	Link Down	II.4.2.1 (GE4) Link Down on Edge b4-hub-edge2000	Closed
> Dec 8, 2020, 5:10:15 PM	Dec 8, 2020, 5:11:23 PM	Customer	Edge HA Failover	Edge b4-hub-edge2000	Closed
> Dec 8, 2020, 5:09:39 PM	Dec 8, 2020, 5:11:43 PM	Customer	Edge CSS Tunnel Down	II.3.11 Edge CSS Tunnel Down on Edge b3-hub-E840	Closed
> Dec 8, 2020, 5:08:40 PM	Dec 8, 2020, 5:10:43 PM	Customer	Edge CSS Tunnel Down	II.4.2.1 Edge CSS Tunnel Down on Edge b4-hub-edge2000	Closed
> Dec 8, 2020, 5:07:30 PM	Dec 8, 2020, 5:09:33 PM	Customer	Link Down	Private (SPP) Link Down on Edge b3-hub-E840	Closed
> Dec 8, 2020, 5:07:15 PM	Pending	Customer	Link Down	II.4.2.1 (GE4) Link Down on Edge b3-hub-edge2000	Closed
> Dec 8, 2020, 5:06:41 PM	Dec 8, 2020, 5:08:43 PM	Customer	Edge CSS Tunnel Down	II.3.11 Edge CSS Tunnel Down on Edge b3-hub-E840	Closed
> Dec 8, 2020, 5:05:33 PM	Dec 8, 2020, 5:07:33 PM	Customer	Edge CSS Tunnel Down	II.4.2.1 Edge CSS Tunnel Down on Edge b4-hub-edge2000	Closed
> Dec 8, 2020, 5:05:05 PM	Pending	Customer	Edge CSS Tunnel Down	II.3.11 Edge CSS Tunnel Down on Edge b3-hub-E840	Closed
> Dec 8, 2020, 4:42:55 PM	Dec 8, 2020, 4:45:03 PM	Customer	Edge CSS Tunnel Up	II.4.2.1 Edge CSS Tunnel Up on Edge b4-hub-edge2000	Closed
> Dec 8, 2020, 4:37:55 PM	Pending	Customer	Edge CSS Tunnel Down	II.4.2.1 Edge CSS Tunnel Down on Edge b4-hub-edge2000	Closed

You can choose a specific time period from the drop-down menu, to view the alerts for the selected duration.

To view details of specific alerts, you can use the filter option. Click the Filter icon in the Search option to define the criteria.

Click the **CSV** option to download a report of the Alerts in CSV format. You can also choose to include the Operator alerts.

The Alerts window displays the following details:

Option	Description
Trigger Time	Time at which the alert got triggered.
Notification Time	Time at which the operator or customer received the alert. The notification time depends on the delay time configured in the <b>Alerts &amp; Notifications</b> page.
Category	Indicates whether the alert is received by the Operator or the Customer.
Type	Displays the alert type.
Description	Displays the details of Edge or link related to the alert. Click the link displayed in this column to view the details of the Edge or link.
Status	Status of the alert as Active, Closed, or Pending.

## Prerequisites

Ensure that you have configured the relevant alerts, along with the notification delay, in **Service Settings > Alerts & Notifications**. See [Chapter 35 Configure Alerts and Notifications](#).

# Monitor Events

The Events page displays the events generated by the SASE Orchestrator. These events help to determine the operational status of the system.

To view the Events page:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Events**.

The **Events** page displays the list of events.

Event	User	Segment	Edge	Severity	Time	Message
Edge Non SD-WAN Destination tunnel up	Global Segment	b1-edge1	● Info	Apr 19, 2023, 1:55:27 PM		IPsec tunnel up for edge [b1-edge1] for provider: [CSS IPsec]
VPN Tunnel state change			● Notice	Apr 19, 2023, 1:55:04 PM		Tunnel to [NSD via GW ZScaler] - Tunnel established (1/1) to 199.168.148.132
Edge Non SD-WAN Destination tunnel up	Seg1	b1-edge1	● Info	Apr 19, 2023, 1:54:58 PM		IPsec tunnel up for edge [b1-edge1] for provider: [CSS IPsec]
Edge Non SD-WAN Destination tunnel up	Seg1	b1-edge1	● Info	Apr 19, 2023, 1:51:26 PM		IPsec tunnel up for edge [b1-edge1] for provider: [CSS IPsec]
Edge Non SD-WAN Destination tunnel up	Global Segment	b1-edge1	● Info	Apr 19, 2023, 1:51:26 PM		IPsec tunnel up for edge [b1-edge1] for provider: [CSS IPsec]
Edge Non SD-WAN Destination tunnel down	Seg1	b1-edge1	● Info	Apr 19, 2023, 1:51:26 PM		IPsec tunnel down for edge [b1-edge1] for provider: [CSS IPsec]
Edge Non SD-WAN Destination tunnel down	Global Segment	b1-edge1	● Info	Apr 19, 2023, 1:51:25 PM		IPsec tunnel down for edge [b1-edge1] for provider: [CSS IPsec]
CSS tunnels are up		b1-edge1	● Alert	Apr 19, 2023, 1:51:05 PM		CSS paths are UP. Traffic will be routed through CSS based on Business Policy rules.
All CSS tunnels down		b1-edge1	● Alert	Apr 19, 2023, 1:51:00 PM		CSS paths are DOWN. If Conditional Backhauler (CBH) is enabled, all Business Policy rules are subject to failover traffic through CBH.

You can choose a specific time period from the drop-down list, to view the events for the selected duration. Click the link to an event name to view more details.

To view details related to specific events, you can use the filter option. Click the Filter Icon in the **Search** option to define the criteria.

Click the CSV option to download a report of the events in CSV format.

The **Events** window displays the following details:

Option	Description
Event	Name of the event
User	Name of the user for events that involve the user.
Segment	Name of the segment for segment related events.
Edge	Name of the Edge for Edge related events.

Option	Description
Severity	Severity of the event. The available options are: Alert, Critical, Debug, Emergency, Error, Info, Notice, and Warning.
Time	Date and time of the event.
Message	A brief description of the event.

## Auto Rollback to the Last Known Good Configuration

If an Administrator changes device configuration that cause the Edge to disconnect from the Orchestrator, the Administrator will get an **Edge Down** alert. Once the Edge detects that it cannot reach the SASE Orchestrator, it will rollback to the last known configuration and generate an event on the Orchestrator titled, “bad configuration.”

The rollback time, which is the time necessary to detect a bad configuration and apply the previous known “good” configuration for a standalone Edge, is between 5-6 minutes. For HA Edges, the rollback time is between 10-12 minutes.

---

**Note** This feature rolls back only Edge-level device settings. If the configuration is pushed from the Profile that causes multiple Edges to go offline from the Orchestrator, the Edges will log “Bad Configuration” events and roll back to the last known good configuration individually. **IMPORTANT:** The Administrator is responsible for fixing the Profile accordingly. The Profile configuration will not roll back automatically.

---

## Platform Firmware Upgrade Progress

You can view the progress of the Platform Firmware upgrade on the SASE Orchestrator UI, as described in the sections below.

To view the progress for the Platform Firmware upgrade on the Orchestrator UI, go to **Monitor > Events**. The **Events** page displays a list of events and shows the status of the Platform Firmware upgrade (In Progress or Installed).

**Events**

Event	Edge	Severity	Time	Message
Configuration applied	610lte_local	Info	Dec 16, 2022, 12:20:56 PM	Applied new configuration for imageUpdate version 1671221754378
Platform Firmware update installed	610lte_local	Info	Dec 16, 2022, 12:20:51 PM	Completed: Success: pfw applied bios(), cpfd(), pic(no need to update), bundle:version 1.3.1 build R131-20221216-GA
Platform Firmware upgrade is in progress	610lte_local	Info	Dec 16, 2022, 12:20:46 PM	Inprogress: pfw update (final) version(1.3.1;R131-20221216-GA) path(/root/pfw6x0/VEP1400) at Fri Dec 16 20:20:45 UTC 2022, bundle:version 1.3.1 build R131-20221216-GA
Platform Firmware upgrade is in progress	610lte_local	Info	Dec 16, 2022, 12:19:05 PM	Inprogress: pic will be updated from to v20N, this will take more than 5 minutes, bundle:version 1.3.1 build R131-20221216-GA
Platform Firmware upgrade is in progress	610lte_local	Info	Dec 16, 2022, 12:18:56 PM	Inprogress: Updating pfw components, be patient, bundle:version 1.3.1 build R131-20221216-GA
Platform Firmware upgrade is in progress	610lte_local	Info	Dec 16, 2022, 12:18:52 PM	Inprogress: Update status bios[] cpfd[] pic[from to v20N], bundle:version 1.3.1 build R131-20221216-GA

**Note** On the Orchestrator UI, you can use the **Filter** feature to see only specific events, which is especially helpful when upgrading multiple SD-WAN Edges.

## Monitor Firewall Logs

The **Firewall Logs** page displays the details of firewall log originating from VMware SD-WAN Edges. Previously the only way a customer could store and view firewall logs was by forwarding them to a Syslog server. With Release 5.2.0 the customer has the option to store firewall logs on the Orchestrator where they can be viewed, sorted, and searched on the Orchestrator UI. By default, Edges cannot send their Firewalls logs to Orchestrator. For an Edge to send the Firewall logs to Orchestrator, ensure that the “**Enable Firewall Logging to Orchestrator**” customer capability is activated at the Customer level under “Global Settings” UI page. By default, Orchestrator retains the Firewall logs until it reaches the maximum retention time of 7 days or a maximum log size of 15 GB per customer tenant on a rotation basis.

Firewall Logs are generated:

- When a flow is created (on the condition that the flow is accepted)
- When the flow is closed
- When a new flow is denied
- When an existing flow is updated (due to a firewall configuration change)

EFS Alerts are generated whenever the flow traffic matches any URL Categories and/or URL Reputation, or Malicious IP, or any IDS/IPS suricata signatures configured in the EFS engine:

- If a firewall rule has URL Categories filtering service activated, the URL Category engine looks up the categories of destination URLs and detects if that matches the Blocked or Monitor categories configured. If the URL matches the Blocked categories, the URL Categories engine generates an alert and blocks the Edge traffic. If the URL matches the Monitor categories, the engine allows the Edge traffic and captures the firewall logs.
- If a firewall rule has URL Reputation filtering service activated, the URL Reputation engine looks up the reputation score of the URL and takes action (Allow/Block) based on the minimum reputation configured. If the reputation score of the URL is less than the minimum reputation configured, the Edge blocks the traffic and generates EFS alerts and logs, otherwise allows the traffic. The URL Reputation engine generates EFS logs for the allowed traffic based on the **Capture Logs** configuration.
- If a firewall rule has Malicious IP filtering service activated, the Malicious IP engine checks if the destination IP is present in the Malicious IP Database (Network Query DB and Local DB). If the engine detects the destination IP in the Malicious IP database, then the engine generates EFS alerts and logs and takes Edge traffic decisions based on the configured action (Block/ Monitor).
- If a firewall rule has only the Intrusion Detection System (IDS) activated, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If an attack is detected, the EFS engine generates an alert and sends the alert message to SASE Orchestrator/Syslog Server if Firewall logging is activated in Orchestrator and will not drop any packets.
- If a firewall rule has Intrusion Prevention System (IPS) activated, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If an attack is detected, the EFS engine generates an alert and blocks the traffic flow to the client only if the signature rule has action as "Reject", matched by the malicious traffic. If the action in the signature rule is "Alert", the engine allows the traffic without dropping any packets even if you configure IPS.

To view the Edge Firewall logs in Orchestrator:

- 1 In the **SD-WAN** service of the Enterprise portal, navigate to **Monitor > Firewall Logs**. The **Firewall Logs** page appears.

With the Stateful Firewall and Enhanced Firewall Services (EFS) features activated, more information can be reported in the firewall logs. The following table describes all the parameters reported in the firewall logs.

Field	Description
Time	The timestamp of the traffic flow session on which the alert was triggered.
Segment	The name of the segment to which the session belongs.
Edge	The name of the Edge to which the session belongs.
Action	Any of the following actions that were triggered against the event/alert: <ul style="list-style-type: none"> <li>■ Allow</li> <li>■ Close</li> <li>■ Deny</li> <li>■ Open</li> <li>■ Update</li> </ul>
Interface	The name of the interface on which the first packet of the session was received. In the case of overlay received packets, this field will contain VPN. For any other packets (received through underlay), this field will display the name of the interface in the Edge.
Protocol	The type of IP protocol used by the session. The possible values are TCP, UDP, GRE, ESP, and ICMP.
Source IP	The source IP address of the traffic flow session on which the alert was triggered.
Source Port	The source port number of the traffic flow session on which the alert was triggered.

Field	Description
Destination IP	The destination IP address of the traffic flow session on which the alert was triggered.
Destination Port	The destination port of the traffic flow session on which the alert was triggered.
Extension Headers	The extension headers of the traffic flow packet.
Rule	The Rule to which the Signature belongs.
Reason	The reason for closure or denial of the session. This field is available for Close and Deny log messages.
Bytes Sent	The amount of data sent in bytes in the session. This field is available only for Close log messages.
Bytes Received	The amount of data received in bytes in the session. This field is available only for Close log messages.
Duration	The duration for which the session has been active. This field is available only for Close log messages.
Application	The Application name to which the session was classified by DPI Engine. This field is available only for Close log messages.
Destination Domain	The destination domain of the traffic flow session.
Destination Name	The name of the destination device of the traffic flow session.
Session ID	The Session ID of the traffic flow on which the alert was triggered.
Signature ID	A unique ID of the signature rule.
Signature	The Signature installed on the Edge.
Attack Source	The Source of the attack.
Attack Target	The Target of the attack.
Severity	The severity of the intrusion.
Category	The category type to which the intrusion belongs.
IDS Alert	Displays "Yes" if the alert notification is received from the IDS engine, or else displays "No".
IPS Alert	Displays "Yes" if the alert notification is received from the IPS engine, or else displays "No".
URL	The URL of the destination to which the traffic flow was directed.
Engine Types	Total count of Engine types that match the flow. Click the link in this column to view the Engine types that match the flow.
URL Categories	Total count of URL category types that matches the flow. Click the link in this column to view the URL categories that matches the flow.

Field	Description
URL Category Filter Action	The URL Category Engine-specific filtering action: ■ Block ■ Monitor
URL Reputation	The URL Reputation type defined in the policy rule.
URL Reputation Action	The URL Reputation Engine-specific filtering action: ■ Block ■ Monitor
IP Categories	Total count of threat types that match the flow. Click the link in this column to view the IP categories that match the flow.
Malicious IP Action	The Malicious IP Engine-specific filtering action: ■ Block ■ Monitor

**Note** Not all fields will be populated for all firewall logs. For example, Reason, Bytes Received/Sent and Duration are fields included in logs when sessions are closed. Signature ID, Signature, Attack Source, Attack Target, Severity, Category, IDS Alert, IPS Alert, URL, Engine Types, URL Categories, URL Category Filter Action, URL Reputation, URL Reputation Action, IP Categories, and Malicious IP Action are populated only for EFS alerts, not for firewall logs.

- 2 You can use the **Filter** options and select a filter from the drop-down menu to query the Firewall logs.
- 3 To view more detailed information about a specific Firewall log, select the Firewall log entry. Under the **Firewall Log Details** section, you can view the detailed **Log Overview** and **Engine** information for the selected log entry.

**Note** If the selected Firewall log entry is generated by Engines other than Enhanced Security Services, the **Engine** tab will not be available.

Firewall Log Details					
Log Overview		Engine			
Log Time	Dec 15, 2023, 10:10:41 AM	Engine	URL Reputaion Filtering,URL Category Filtering	Extension headers	--
Segment	Global Segment	Source IP	10.0.1.233	Reason	--
Edge	b1-edge1	Source Port	41020	Bytes Sent	--
Rule	Rule-0	Destination IP	34.107.221.82	Bytes Received	--
Interface	--	Destination Port	80	Duration	00:00:00
Protocol	TCP	Destination Domain	detectportal.firefox.com	Application	--
Action	DENY	Destination Name	--	Session ID	9519

- 4 In the **Log Overview** tab, click the link next to **Engine** to view detailed information about the specific Engine that matched the flow along with the Engine-specific filtering action.

The screenshot shows the 'Firewall Log Details' page with the 'Engine' tab selected. Under 'URL Reputation Filtering', 'URL Reputation Action' is set to 'ALLOW' and 'URL Reputation' is set to 'Trustworthy'. Under 'URL Category Filtering', 'URL' is set to 'detectportal.firefox.com/success.txt', 'URL Category Filter Action' is set to 'DENY', and 'URL Categories' include 'Computer and Internet Info, Shareware and Freeware'.

- To create customized reports by exporting Edge Firewall Logs data in CVS format, in the **Firewall Logs** page, click the **CSV** option.

## Enterprise Reports

VMware SD-WAN allows you to generate Enterprise reports for the analysis of your network.

You can generate reports including all the data or configure them to include customized data. You can also create a recurring schedule to generate the reports during specified time period.

**Note** By default, the SASE Orchestrator stores 50 reports at a time for an Enterprise. An Operator can modify the number of reports using the system property, **vco.reporting.maxReportsPerEnterprise**.

A report has 60 days of age out period after which it will be deleted automatically. When a customer exceeds the maximum report value (i.e., default is 50), the oldest report will be deleted first.

To access the Enterprise reports:

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Reports**.

In the **Reports** page, you can create a new quick report (a consolidated Enterprise report with default selection of the data for all Edges over the last month), customize the report, and schedule report generation for a recurring period.

The screenshot shows the 'Reports' page in the VMware SD-WAN interface. The left sidebar menu is visible with 'Reports' selected. The main area displays a search bar, a 'Deleted no' button, and a 'RECURRING REPORTS' section. Below this is a table header with columns: Name, Created By, Created Date, Report Period, and Status. A central illustration of a robot holding a magnifying glass is present, along with the message 'No reports available as per selected filter criteria'. At the bottom, there are 'COLUMNS' and 'REFRESH' buttons, and navigation icons for items, pages, and rows.

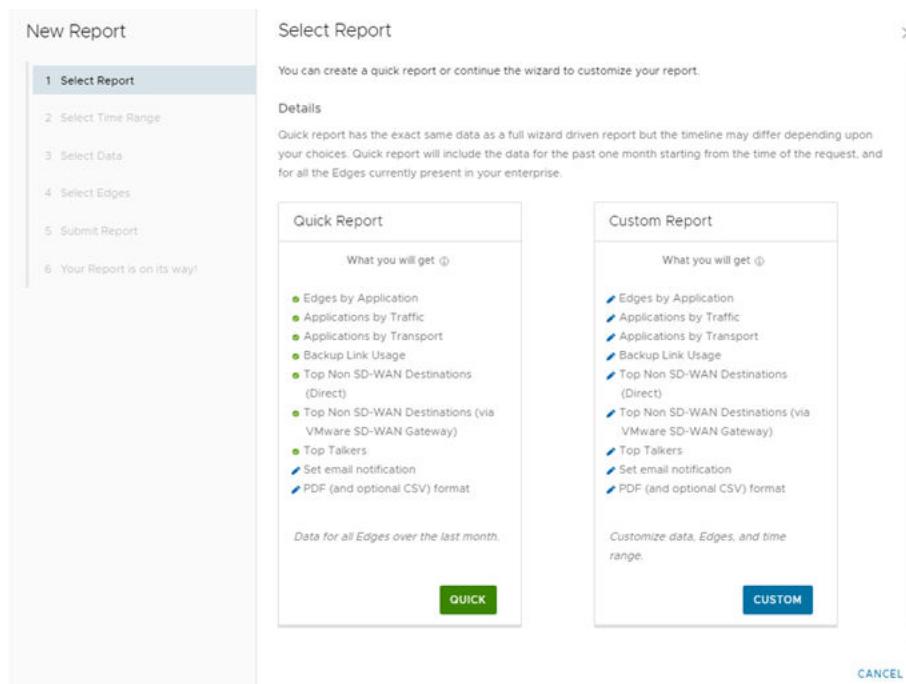
For more information, see [Create a New Enterprise Report](#).

## Create a New Enterprise Report

You can either generate a consolidated Enterprise report or configure the settings to generate a customized Enterprise report.

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Reports**.
- 2 In the **Reports** page, click **New Report**.
- 3 In the **New Report** page, you can configure to generate a consolidated report (quick report) or a customized report.

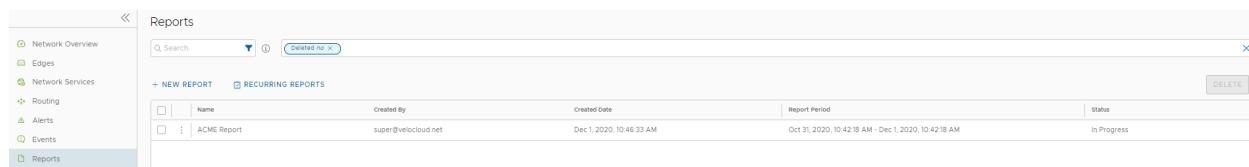


- 4 Click **Quick** to generate a consolidated report with the settings displayed in the **Quick Report** pane. By default, this report includes data for the last 30 days, with breakdown details of the following:
  - Top 10 applications and the top 10 Edges using each application.
  - SD-WAN consumption based on traffic distribution with top 10 applications for each traffic type.
  - SD-WAN consumption based on transport distribution with top 10 applications for each transport type.
  - Top backup links based on traffic with top 5 applications for each of the backup links.
  - Top Non SD-WAN destinations directly from the VMware SD-WAN Edges with top 5 Edges for each destination.

- Top Non SD-WAN destinations using VMware SD-WAN Gateways with top 5 Edges for each destination.
  - Top clients across Edges with top 5 applications for each client.
- 5 In the **Submit Report** window that appears, enter the Report Name, choose the Format to be either PDF or PDF and CSV, select the language of the Report, and choose whether to send the generated report as Email and specify the Email IDs. See [Submit Report](#).
- 6 In the window **Your Report is on its way** that appears, click **Done**.

## Results

Once you submit the report, the Report details are displayed with the status in the **Reports** window.



The screenshot shows the 'Reports' page in the VMware SD-WAN interface. On the left, there's a sidebar with navigation links: Network Overview, Edges, Network Services, Routing, Alerts, Events, and Reports (which is selected and highlighted in blue). The main area has a header with 'Reports', a search bar ('Search'), and a button ('Created no X'). Below the header are two buttons: '+ NEW REPORT' and 'RECURRING REPORTS'. A table lists the reports, with one entry shown:

Name	Created By	Created Date	Report Period	Status
ACME Report	super@velocloud.net	Dec 1, 2020, 10:46:33 AM	Oct 31, 2020, 10:42:18 AM - Dec 1, 2020, 10:42:18 AM	In Progress

## What to do next

Your report is generated and is displayed in the **Reports** page. See [Monitor Enterprise Reports](#).

To generate a customized report with specific values, see [Create Customized Report](#).

## Create Customized Report

You can create an Enterprise report with customized settings by specifying the time range, required data, and Edges.

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Reports**.
- 2 Click **New Report**.
- 3 In the **New Report** page, click **Custom**.

## What to do next

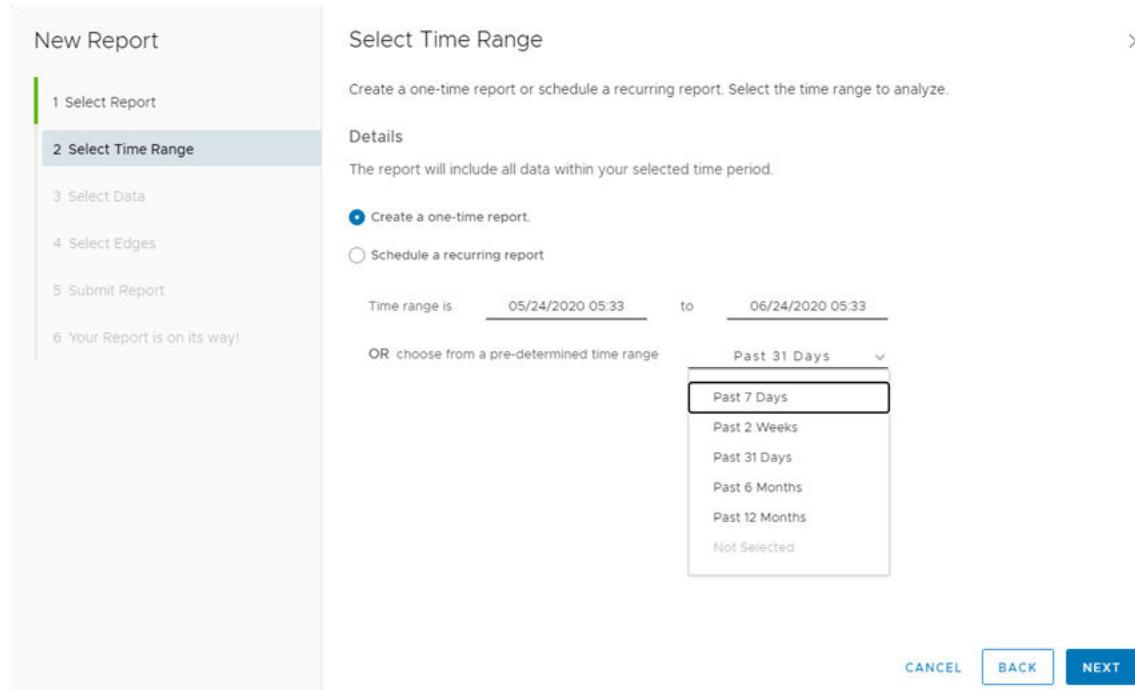
Follow the instructions on the screen to select the configuration settings for the custom report. See [Select Time Range](#).

## Select Time Range

You can customize a report for a selected time period. In addition, you can schedule a report to run on recurring basis.

## Procedure

- When you choose to customize the Enterprise report and click **Custom** in **Create Customized Report**, the **Select Time Range** window appears.



- The **Create a one-time Report** option is selected by default. You can either enter the start and end date for which the report should be generated, or choose the time range from the list.

- 3 To configure a scheduled report, choose **Schedule a recurring report** and select the schedule period and time from the list.

The screenshot shows the 'New Report' wizard at step 2, 'Select Time Range'. On the left, a vertical list of steps is shown: 1. Select Report, 2. Select Time Range (which is highlighted in blue), 3. Select Data, 4. Select Edges, 5. Submit Report, and 6. Your Report is on its way!. The main area contains instructions and configuration options. It says 'Create a one-time report or schedule a recurring report. Select the time range to analyze.' Below this is a 'Details' section stating 'The report will include all data within your selected time period.' There are two radio button options: 'Create a one-time report.' (unselected) and 'Schedule a recurring report.' (selected). Under 'Schedule a recurring report.', there are dropdown menus for 'Generate a report for the' (set to 'Last Week'), 'Repeat every week' (set to 'Monday'), 'on' (set to 'Monday'), and 'at' (set to '07:00'). At the bottom right are three buttons: 'CANCEL', 'BACK' (disabled), and 'NEXT' (highlighted in blue).

- 4 Click **Next**.

#### What to do next

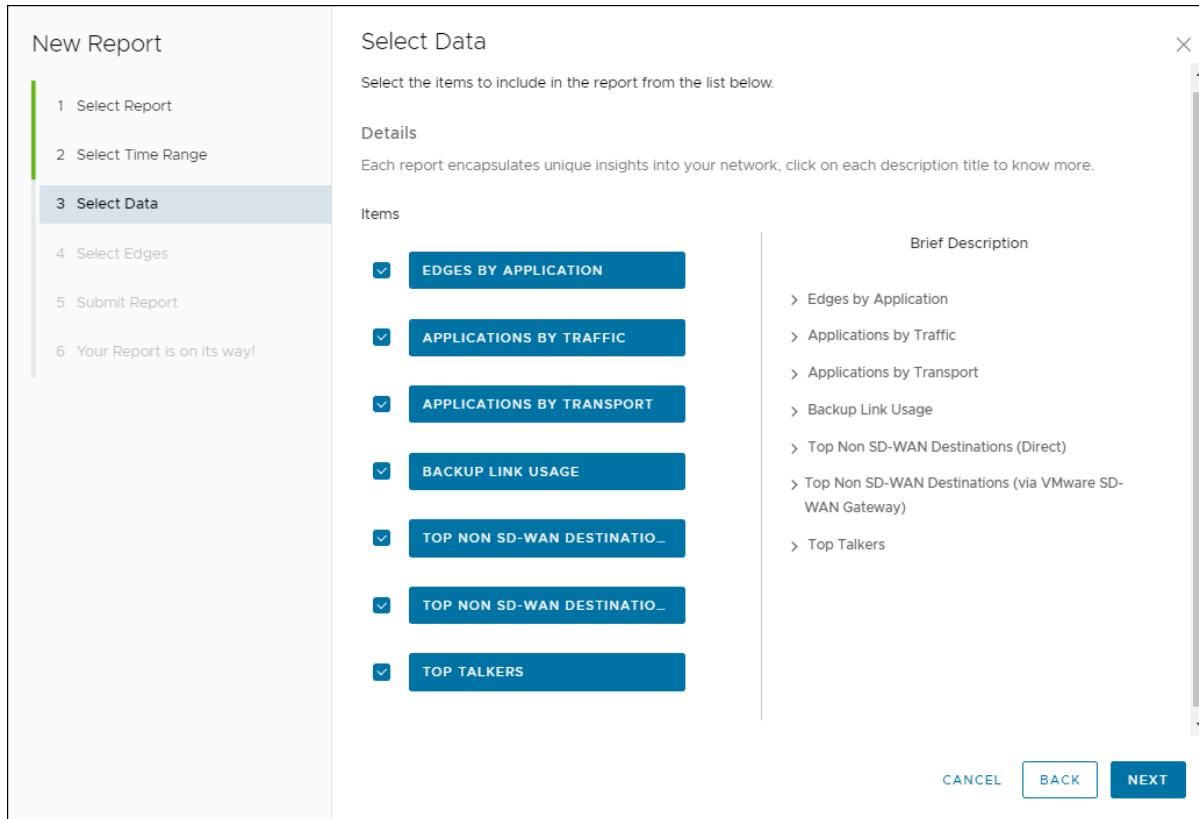
See [Select Data](#).

### Select Data

You can select the data to be included in a custom report.

## Procedure

- When you click **Next** after selecting the time range in **Select Time Range**, the **Select Data** window appears.



- Select the check boxes of the data items that you want to include in the report from the following available options:

**Note** By default, all data items are selected.

- **Edges by Application** – Breakdown details of top 10 applications and the top 10 Edges using each application.
- **Applications by Traffic** – Breakdown details of SD-WAN consumption based on traffic distribution with top 10 applications for each traffic type.
- **Applications by Transport** – Breakdown details of SD-WAN consumption based on transport distribution with top 10 applications for each transport type.
- **Backup Link Usage** – List of top backup links based on traffic with top 5 applications for each backup link.
- **Top Non SD-WAN Destinations (Direct)** – List of top Non SD-WAN destinations directly from the VMware SD-WAN Edges with top 5 Edges for each destination.
- **Top Non SD-WAN Destinations (via SD-WAN Gateway)** – List of top Non SD-WAN destinations via VMware SD-WAN Gateways with top 5 Edges for each destination.

- **Top Talkers** – List of top clients across Edges with top 5 applications for each client.

3 Click **Next**.

**What to do next**

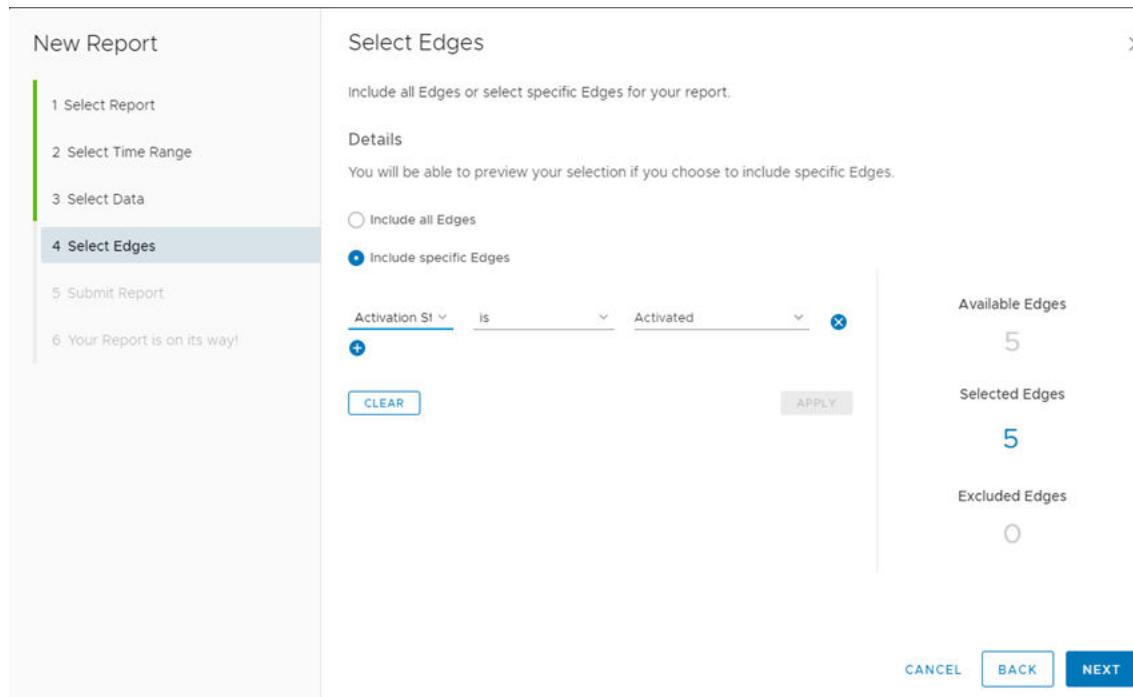
See [Select Edges](#).

## Select Edges

You can select to generate an Enterprise report including all the Edges or choose to include specific Edges.

**Procedure**

- When you click **Next** after selecting the data to be included in the report in [Select Data](#), the **Select Edges** window appears.



- By default, the **Include all edges** option is selected. This option generates the report including data from all the Edges in the Enterprise.
- You can choose **Include specific edges** to generate the report with data from specific Edges. Select the appropriate condition from the list to include the corresponding Edges. You can click the Plus (+) Icon to include more conditions. After specifying the conditions, click **Apply** and the details of Edges selected according to the conditions are displayed at the right side.
- Click **Next**.

**What to do next**

See [Submit Report](#).

## Submit Report

After configuring all the settings, you can generate the Enterprise report.

### Procedure

- When you click **Quick** to create a Quick Report in [Create a New Enterprise Report](#), or click **Next** after selecting the Edges in [Select Edges](#), the **Submit Report** window appears.

The screenshot shows the 'Submit Report' window. On the left, a sidebar lists steps: 1. Select Report, 2. Select Time Range, 3. Select Data, 4. Select Edges, 5. Submit Report (which is highlighted), and 6. Your Report is on its way!. The main area has a header 'Submit Report' with a note: 'Please name your report and review your selections'. It includes fields for 'Report Name' (ACME Report), 'Format' (PDF And C...), 'Report Language' (English), and a checked checkbox 'Send email to list' with the recipient 'admin@acme.com'. Below this is a 'Report Summary' section containing a table of selected items and their details. At the bottom are 'CANCEL', 'BACK', and a large blue 'SUBMIT' button.

Selected Name:	ACME Report
Selected Time Range:	Create a one-time report. Time range is Oct 31, 2020 to Dec 1, 2020
Selected Items:	Edges by Application Applications by Traffic Applications by Transport Backup Link Usage Top Non SD-WAN Destinations (Direct) Top Non SD-WAN Destinations (via VMware SD-WAN Gateway) Top Talkers
Selected Edge Devices:	Include all Edges
Selected Format:	PDF and export CSV data for the selected items
Selected Language:	English
Selected Notifications:	Send an email on report completion to the following destinations: admin@acme.com

- Configure the following:

- Report Name:** Enter a name for the report.
- Format:** Choose the format of the report from the list, as PDF or PDF and CSV.
- Report Language:** Choose the language in which you want to generate the report. Currently the following languages are supported: English, Simplified Chinese, Czech, Italian, French, and German.
- Send email to list:** If you want to send the generated report through Email, select the checkbox and enter the Email addresses separated by comma. The report is attached to the Email that is sent.

- In the **Report Summary** verify the settings and click **Submit**.

- In the window **Your Report is on its way** that appears, click **Done**.

## Results

Once you submit the report, the Report details are displayed with the status in the **Reports** window.

### What to do next

Your report is generated and is displayed in the **Reports** page. See [Monitor Enterprise Reports](#).

## Monitor Enterprise Reports

You can generate a Quick report using the default values or a custom report with specified values. You can also schedule a custom report to run on a recurring basis. All the reports are displayed in the **Reports** page, where you can download and view the report data. You can also view the scheduled reports in this page.

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Reports**. The page displays all the generated reports.

	Name	Created by	Created Date	Report Period	Status
<input checked="" type="checkbox"/>	Daily Report	super@velocloud.net	Dec 1, 2020, 3:00:00 PM	Nov 30, 2020, 2:30:00 PM - Dec 1, 2020, 2:30:00 PM	Completed
<input type="checkbox"/>	Weekly Report	super@velocloud.net	Dec 1, 2020, 2:00:00 PM	Nov 24, 2020, 1:30:00 PM - Dec 1, 2020, 1:30:00 PM	Completed
<input type="checkbox"/>	Monthly Report	super@velocloud.net	Dec 1, 2020, 12:30:00 PM	Nov 30, 2020, 12:30:00 PM - Dec 1, 2020, 12:30:00 PM	Completed
<input type="checkbox"/>	ACME Report	super@velocloud.net	Dec 1, 2020, 10:46:33 AM	Oct 31, 2020, 10:42:18 AM - Dec 1, 2020, 10:42:18 AM	Completed

To download a report, click the **Completed** link of the report. The report downloads as a ZIP file, which consists of the PDF format of the report. If you have configured to export the report to CSV format, the ZIP file consists of both the PDF and CSV files.

For a custom report, the data in the report may vary according to the customized settings. The report files consist of the following.

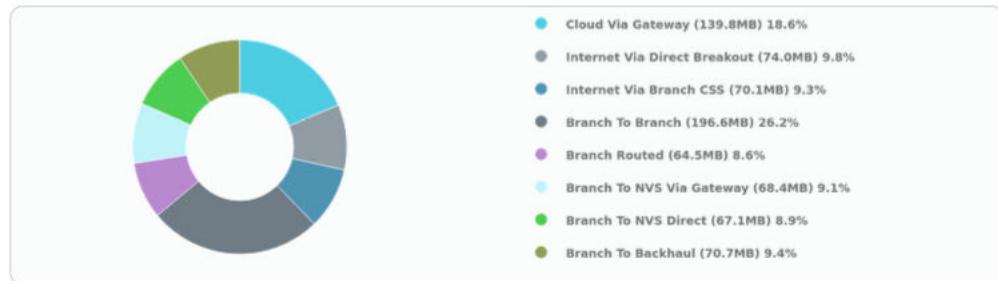
### ■ PDF:

- Graphical representation of distribution of Enterprise Traffic, Transport, and top Applications.
- Top 10 Applications by Traffic and Transport types.
- Top 10 Edges by Applications.
- Top Backup links with top Applications.
- Top Talkers with top Applications.
- Top Edges in top Non SD-WAN Destinations from Edge.
- Top Sites in top Non SD-WAN Destinations via Gateway.

The following image shows an example snippet of a PDF report:

## Traffic Distribution

### Enterprise Traffic Distribution



### Top Ten Applications by Traffic Type

	<b>Cloud Via Gateway</b> <b>140MB</b>	<b>Internet Via Direct Breakout</b> <b>74MB</b>	<b>Internet Via Branch CSS</b> <b>70.1MB</b>
1	Spotify 12.5MB	Pandora Radio 6.39MB	ShoreTel 6.14MB
2	Microsoft Skype for ... 12MB	Skype Audio 6.18MB	Microsoft Office 365... 5.94MB
3	Internet Control Mes... 11.7MB	Salesforce 6.09MB	Youtube.com 5.87MB
4	Domain Name Service 11.6MB	Microsoft Office 365... 5.99MB	Salesforce 5.81MB
5	ShoreTel 11.1MB	Youtube.com 5.7MB	Independant Computin... 5.47MB
6	Independant Computin... 10.5MB	Facebook 5.62MB	Domain Name Service 5.4MB
7	Skype Audio 10.4MB	Domain Name Service 5.55MB	Internet Control Mes... 5.22MB
8	Microsoft Office 365... 10.1MB	Microsoft Skype for ... 5.51MB	Microsoft Skype for ... 5.16MB
9	Pandora Radio 9.84MB	ShoreTel 5.1MB	Skype Chat 5.06MB
10	Skype Chat 9.55MB	Independant Computin... 4.98MB	Spotify 4.69MB
11	Other 30.4MB	Other 16.8MB	Other 15.3MB

The Enterprise Traffic distribution lists the following data:

- **Cloud Via Gateway:** Internet bound traffic that goes through the SD-WAN Gateway.
- **Internet Via Direct Breakout:** Internet bound traffic that breaks out directly from branch and does not go through VMware Tunnels.
- **Internet Via Branch CSS:** Traffic bound to Cloud Security Services directly from VMware branch.

- **Branch To Branch:** Traffic going through SD-WAN Gateway / SD-WAN Hub / dynamic SD-WAN Tunnels, directly between two VMware branches.
- **Branch Routed:** Traffic bound to local connected / static / routed (underlay) destinations.
- **Branch To NVS Via Gateway:** Traffic bound from branch to Non SD-WAN Destination through SD-WAN Gateway.
- **Branch To NVS Direct:** Traffic bound from branch to Non SD-WAN Destination over direct IPsec tunnels.
- **Branch To Backhaul:** Internet bound traffic being backhauled from branch to VMware SD-WAN Hubs.
- **CSV:** The following CSV files are downloaded.
  - **Top Sites by Applications:** Lists all the applications, Edge name, Edge description, Bytes transmitted, and Bytes received.
  - **Traffic Type:** Lists all the flow paths, applications, Edge name, Edge description, Bytes transmitted, and Bytes received.
  - **Transport Type:** Lists all the Transport types, applications, Edge name, Edge description, Bytes transmitted, and Bytes received.
  - **Backup Link Usage:** Lists the names of all the Backup links, total bytes and applications used by the links, Bytes transmitted, and Bytes received.
  - **Non SD-WAN Destinations from Edge:** Lists all the Non SD-WAN Destinations connected directly from the Edges, name and description of the connected Edges, Bytes transmitted, and Bytes received.
  - **Non SD-WAN Destinations via Gateway:** Lists all the Non SD-WAN Destinations connected through SD-WAN Gateways, name of the Gateway, Bytes transmitted, and Bytes received. This report also lists the name and description of the Edges connected to each destination along with the Bytes transmitted, and Bytes received.
  - **Top Talkers:** Lists the names of clients, source IP address, source MAC address, name and description of the Edges connected to each client, total bytes used by the client, applications, Bytes transmitted, and Bytes received.

The following image shows an example snippet of a CSV report for **Top Sites by Applications:**

A	B	C	D	E	F	G	H	I	J	K	L
1	application	edge name	edge description	bytesTx	bytesRx						
2	SD-WAN Management	b3-edge1	null	597701239	934689460						
3	SD-WAN Management	b5-edge1	null	591260533	924932150						
4	SD-WAN Management	b4-edge1	null	583855260	913713227						
5	SD-WAN Management	b1-edge1	null	580227094	907978707						
6	SD-WAN Management	b2-edge1	null	570211413	892110780						
7	SD-WAN Control	b4-edge1	null	883073607	407330289						
8	SD-WAN Control	b2-edge1	null	709745212	408807549						
9	SD-WAN Control	b1-edge1	null	689832100	409380507						
10	SD-WAN Control	b5-edge1	null	564023796	366809552						

To delete a report, select the report and click **DELETE**.

To view the scheduled reports, click **RECURRING REPORTS**.

<input type="checkbox"/>	Name	Created By	Created Date	Recurrence	Recipients
<input type="checkbox"/>	Daily Report	super@velocloud.net	Dec 1, 2020, 12:13:03 PM	Every day at 3:00 PM	
<input type="checkbox"/>	Monthly Report	super@velocloud.net	Dec 1, 2020, 12:12:26 PM	Every month on day 1 at 12:30 PM	
<input type="checkbox"/>	Weekly Report	super@velocloud.net	Dec 1, 2020, 12:06:20 PM	Every week on Tuesday at 2:00 PM	admin@acme.com

The **Recurring Reports** window displays the details of reports and the recurrence schedule.

To remove a report from the scheduled list, select the report and click **DELETE**.

## View Analytics Data

Once a SD-WAN Edge is provisioned with Analytics, the Analytics functionality collects data (application-specific Analytics or application and branch Analytics). The collected Analytics data are then sent directly from the SD-WAN Edge to the Cloud Analytics Engine. Operator Super User, Operator Standard Admin, Enterprise Super User, Enterprise Standard admin, Partner

Super User, and Partner Standard Admin can view the Analytics data for a specific customer in the Analytics portal (<https://app.nyansa.com>).

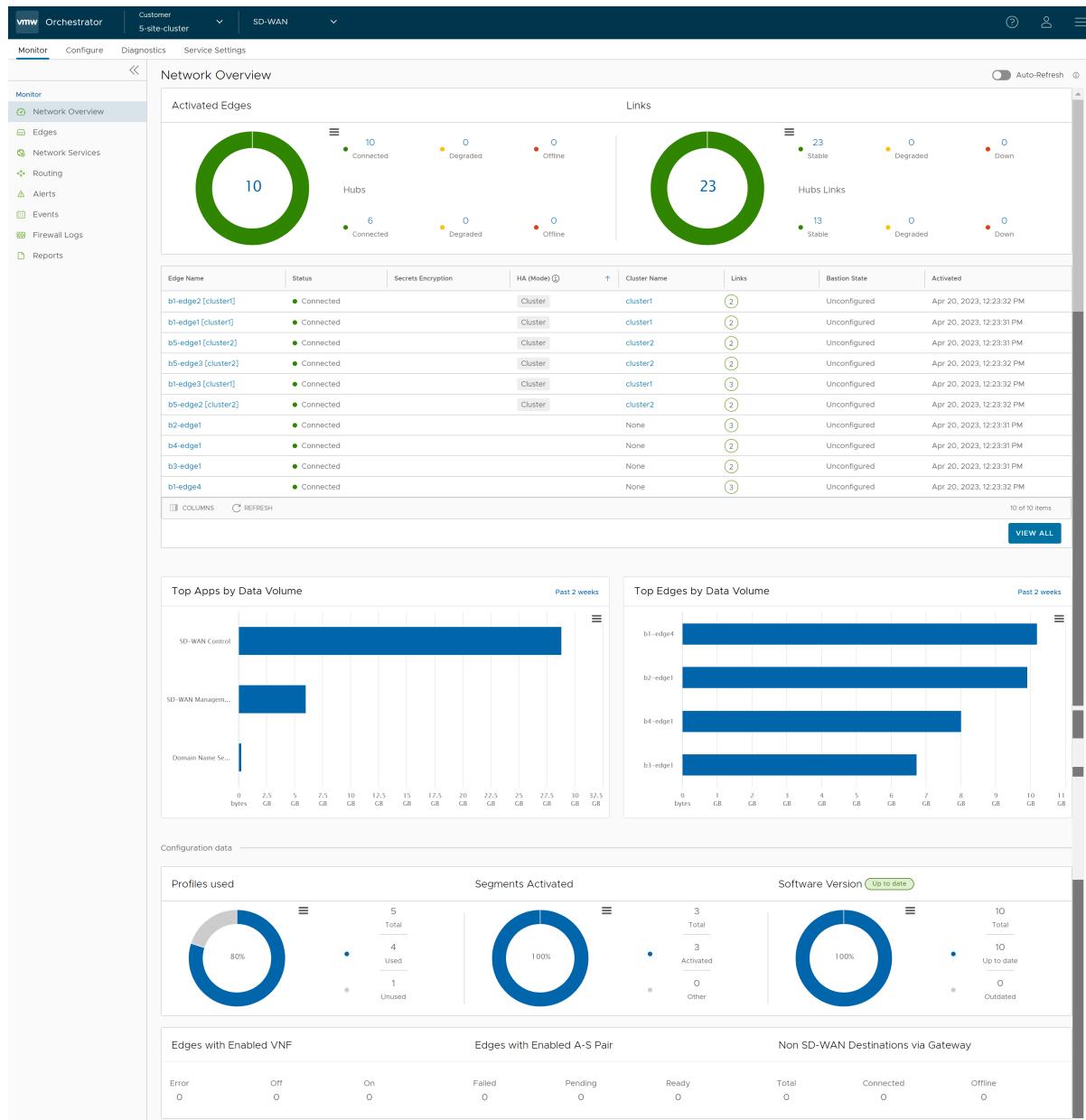
To view the Analytics data, perform the following steps.

#### Prerequisites

- Ensure that all the necessary system properties to activate Analytics are properly set in the SASE Orchestrator. For more information, contact your Operator Super User.
- Ensure that you have access to the Analytics portal to view the Analytics data.

## Procedure

- In the **SD-WAN** service of the Enterprise portal, click **Monitor > Application Analytics** to view the Application Analytics data for the selected Enterprise.



- To view Branch Analytics data, click **Monitor > Branch Analytics**.

When the Analytics menu is clicked, the Analytics portal will be opened in a new browser tab, where you can view the Analytics data (Application and Branch) of all the Edges configured for a selected customer. Note that the Browser settings may prevent this action as popups. You need to allow it when browser shows notification.

### What to do next

In the Analytics portal, you can configure additional data sources such as Wi-Fi and Wired metrics. For more information, see *VMware Edge Intelligence User Guide* available at <https://docs.vmware.com/en/VMware-Edge-Intelligence/index.html>.

# Configure Segments

8

Segmentation is the process of dividing the network into logical sub-networks called Segments by using isolation techniques on a forwarding device such as a switch, router, or firewall. Network segmentation is required when traffic from different organizations and data types must be isolated.

In the segment-aware topology, different Virtual Private Network (VPN) profiles can be activated for each segment. For example, Guest traffic can be backhauled to remote data center firewall services, Voice media can flow direct from Branch-to-Branch based on dynamic tunnels, and the PCI segment can backhaul traffic to the data center to exit out of the PCI network.

To activate the segmentation capability for an Enterprise, in the Operator portal, navigate to **System Properties**, and then set the value of the system property, `enterprise.capability.enableSegmentation` as **True**. For more information about how to configure system properties, refer to the "System Properties" section in the VMware SASE Orchestrator Deployment and Monitoring Guide.

By default, you can configure a maximum of 16 segments per Enterprise. However, you can choose to increase this default value to a maximum of 128 segments per Enterprise. Ensure that you define the maximum number of allowed segments in the `enterprise.segments.system.maximum` system property. For more information about the various system properties that you must set up for the segmentation capability, refer to the "Segmentation" table in the "List of System Properties" section in the VMware SASE Orchestrator Deployment and Monitoring Guide.

## Limitations

Keep in mind the following limitations before you increase the default value to a maximum of 128 segments per Enterprise:

- It is mandatory that you upgrade your SASE Orchestrator and your Edges to version 4.3 or above.
- After you have configured 128 segments for an Enterprise, you cannot downgrade your Edges to a version lower than 4.3. If you need to downgrade your Edges, ensure that you have only 16 segments, which is the default value for any Enterprise and delete the remaining segments before you downgrade the Edges.

# Configure a New Segment for an Enterprise

To configure the Segments:

- 1 In the **SD-WAN** service of the Enterprise Portal, click **Configure > Segments**.
- 2 The **Segments** page displays the existing Segments.

Segment Name *	Description	Type	Service VLAN	Delegate To Partner	Delegate To Customer	Number of Profiles in Use
Global Segment	Default segment f...	Regular	Enter VLAN	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	2
segment1	Enter Description	Regular	Enter VLAN	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	2
segment2	Enter Description	Regular	Enter VLAN	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	2

- 3 Click **Add** to add a new Segment and configure the following details:

Option	Description
Segment Name	Enter a name for the Segment. The maximum number of characters allowed is 256.
Description	Enter a descriptive text for the Segment. The maximum number of characters allowed is 256.
Type	<p>Choose the Segment type as one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>Regular</b> - The standard segment type.</li> <li>■ <b>Private</b> - Used for traffic flows that require limited visibility in order to address end user privacy requirements.</li> <li>■ <b>CDE</b> - VMware provides PCI certified SD-WAN service. The Cardholder Data Environment (CDE) type is used for traffic flows that require PCI and want to leverage the VMware PCI certification.</li> </ul> <p><b>Note</b> For Global Segment, you can set the type either to <b>Regular</b> or <b>Private</b>. For non-global segments, the type can be <b>Regular</b>, <b>CDE</b>, or <b>Private</b>.</p>
Service VLAN	Enter the service VLAN identifier. For more information, see <a href="#">Define Mapping Segments with Service VLANs</a> .
Delegate To Partner	By default, this checkbox is selected. If this checkbox is not selected, the Partner cannot change the configurations within the segment, including the Interface assignment.
Delegate To Customer	By default, this checkbox is selected. If this checkbox is not selected, the Customer cannot change the configurations within the segment, including the Interface assignment.

#### 4 Click **Save Changes**.

If the segment is configured as **Private**, then the segment:

- Does not upload user flow stats to Orchestrator except for VMware Control, VMware Management, and a single IP flow that counts all transmitted and received packets and bytes sent on the segment. For example, Customer flow stats like Source IP, Destination IP and so on, are not shown in the **Monitor** tab for the flows related to **Private** segment.
- Does not allow users to view flows in Remote Diagnostics.
- Does not allow traffic to be sent as **Internet Multipath** as all business policies that are set to **Internet Multipath** are automatically overridden to **Direct** by the Edge.

If the segment is configured as **CDE**, then the VMware hosted Orchestrator and Controller will be aware of the PCI segment and will be in the PCI scope. Gateways (marked as non-CDE Gateways) will not be aware or transmit PCI traffic and will be out of PCI scope.

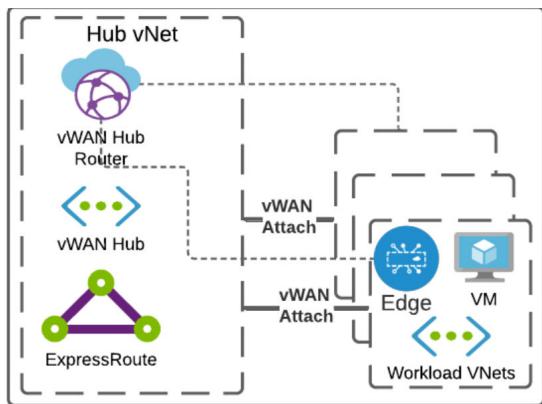
To remove a Segment, select the Segment and click **Delete**. You cannot delete a Segment used by a Profile.

## 9

# SD-WAN Edge in a vNet Connecting to a vWAN Hub

This section outlines how to integrate an SD-WAN Edge in a traditional vNet with a vWAN Hub.

Integrate an SD-WAN Edge in a traditional vNet with a vWAN Hub is an alternative design to deploying Edges as a managed NVA inside of the vWAN Hub itself, resulting in a topology similar to the image below.



It is important to adhere to the following:

- You must deploy the Virtual Edge in a vNet.
- Azure Virtual WAN Hub must be deployed, i.e., the following must be created in the desired Azure region:
  - A Resource Group must be created.
  - A Virtual WAN (vWAN) must be created.
  - A Virtual Hub (vHUB) must be created.

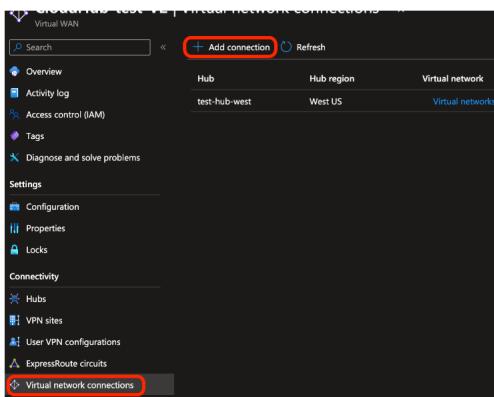
---

**Note** This section assumes that Edges, vWAN, and applicable Hub(s) have already been deployed as documented in the Azure Virtual Edge Deployment Guide and the section titled "Deploy VMware SD-WAN in Azure Virtual WAN Hub" in the Administration Guide.

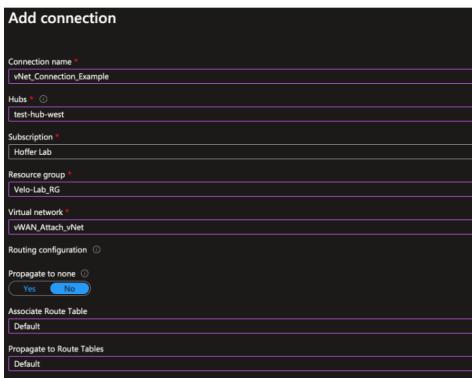
---

To integrate an SD-WAN Edge in a traditional vNet with a vWAN hub:

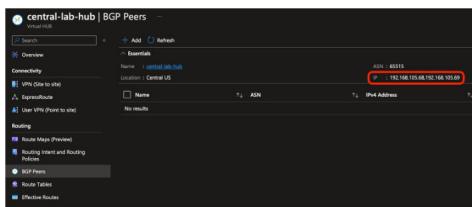
- 1 The vNET in which the Edge(s) are deployed must be attached to the vWAN Hub by navigating to the vWAN by selecting **Virtual network connections** and then selecting **Add connection**.



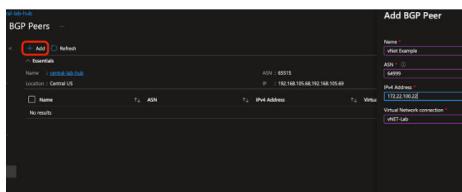
- When creating the connection, ensure that it is propagated to the default route table of the vWAN Hub you are connecting to; this ensures reachability for BGP peering.



- After the vNet attachment is complete, navigate to the vWAN hub and select **BGP Peers** from the Routing menu. Make a note of the IPs listed, as they will be the addresses that the Edge will peer with.



- Select **Add** and enter the ASN and LAN IP address of the SD-WAN Edge that the vWAN Hub router will peer with.



- The Hub router is not on the SD-WAN Edge's local subnet; therefore, a static route must be configured for the IPs recorded in Step 3 and pointed to the Gateway IP of the LAN subnet.

Subnet *	Source IP	Next Hop IP *	Interface *	VLAN	Cost *	Preferred	Advertise
192.168.105.68/31	N/A	172.22.100.17	GE2	0	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Yes	

- 6 Create BGP neighbors with each of the IP addresses recorded in Step 3 using Microsoft's ASN of 65515. As BGP multi-hop is used, the Max-Hop option must be set to "2."

Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options
192.168.105.68	65515	No Default	No Default	Max-Hop: 2 Local IP: <input type="text"/> IP Address: <input type="text"/> Source Interface: Auto Uplink: <input type="checkbox"/> Allow AS: <input type="checkbox"/> Default Route: <input type="checkbox"/>

- 7 Once the configuration is applied, the BGP neighborship should be established, Azure routes should be learned by the SD-WAN Edge, and SD-WAN overlay routes should be present in the Azure vWAN Default route table.

# Configure Network Services

10

As an Enterprise user, SASE Orchestrator allows you to configure a number of network services across multiple Edges and Profiles.

**Note** If you are logged in using a user ID that has Customer Support privileges, you can only view the SASE Orchestrator objects. You cannot create new objects or configure/update existing ones.

## Procedure

- 1 In the **SD-WAN** service of the Enterprise Portal, click **Configure > Network Services**.
- 2 The following screen is displayed:

**Figure 10-1. Network Services**

The screenshot shows the 'Network Services' configuration interface. At the top, a note states: 'Configuring Network Services are optional and can be configured in any order. Use these configurations across multiple Edges and Profiles for a more efficient workflow.' Below this, there are several sections with expandable sub-options:

- Non SD-WAN Destinations:**
  - > Non SD-WAN Destinations via Gateway ⓘ
  - > Non SD-WAN Destinations via Edge ⓘ
- Credentials:**
  - > API Credentials ⓘ
- SD-WAN Destinations:**
  - > Clusters and Hubs ⓘ
- Network Management:**
  - > Netflow
  - > DNS Services
  - > Private Network Names
  - > Prefix Delegation Tags
  - > Authentication Services
  - > TACACS Services
- Edge Services:**
  - > VNFs

3 You can configure the following network services:

- Configure Non SD-WAN Destinations via Gateway
- Configure Non SD-WAN Destinations via Edge
- Configure API Credentials
- Configure Clusters and Hubs
- Configure Netflow Settings
- Configure DNS Services
- Configure Private Network Names
- Configure Prefix Delegation Tags
- Configure Authentication Services
- Configure TACACS Services
- Configure Edge Services

---

**Note** Configuring Network Services is optional and can be configured in any order.

---

## Configure a Non SD-WAN Destination

The Non SD-WAN Destination (earlier known as Non VeloCloud Site (NVS)) functionality consists of connecting a VMware network to an external Network (for example: Zscaler, Cloud Security Service, Azure, AWS, Partner Datacenter and so on). This is achieved by creating a secure Internet Protocol Security (IPsec) tunnel between a VMware entity and a VPN Gateway at the Network Provider.

VMware allows the Enterprise users to define and configure a datacenter type of Non SD-WAN Destination instance and establish a secure tunnel directly to an External network in the following two ways: Non SD-WAN Destinations via Gateway and Non SD-WAN Destinations via Edge, as described below.

- **Non SD-WAN Destinations via Gateway** - Allows an SD-WAN Gateway to establish an IPsec tunnel directly to a Non SD-WAN Destination. VMware supports the following Non SD-WAN Destination configurations through SD-WAN Gateway:

- AWS VPN Gateway

---

**Note** The AWS VPN Gateway type is introduced in the 4.3.0 release.

---

- Check Point
- Cisco ASA
- Cisco ISR
- Generic IKEv2 Router (Route Based VPN)

- Microsoft Azure Virtual Hub
- Palo Alto
- SonicWALL
- Zscaler
- Generic IKEv1 Router (Route Based VPN)
- Generic Firewall (Policy Based VPN)

---

**Note** VMware supports both Generic Route-based and Policy-based Non SD-WAN Destination from Gateway.

For information on how to configure Non SD-WAN Destinations via Gateway, see [Configure Non SD-WAN Destinations via Gateway](#).

- **Non SD-WAN Destinations via Edge** - Allows an SD-WAN Edge to establish an IPsec tunnel directly to a Non SD-WAN Destination (AWS and Azure Datacenter). VMware supports the following Non SD-WAN Destination configurations through SD-WAN Edge:
  - Generic IKEv1 Router (Route Based VPN)
  - Generic IKEv2 Router (Route Based VPN)
  - Microsoft Azure Virtual Wan

For information on how to configure Non SD-WAN Destinations via Edge, see [Configure Non SD-WAN Destinations via Edge](#).

## Non SD-WAN Destination Configuration Workflow

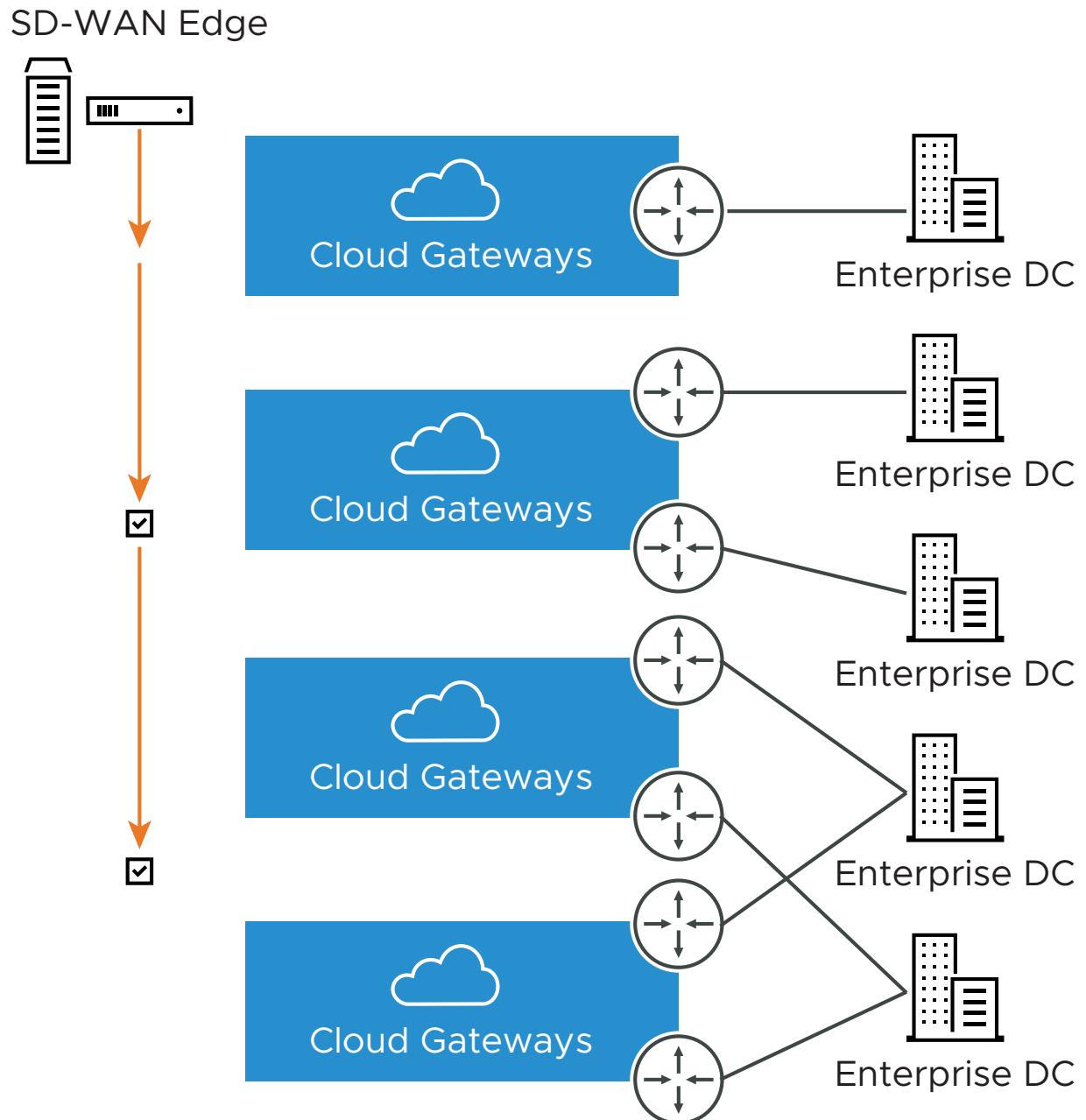
- Configure a Non SD-WAN Destination Network Service.
- Associate a Non SD-WAN Destination Network Service to a Profile or Edge.
- Configure Tunnel Parameters: WAN link selection and Per tunnel credentials.
- Configure Business Policy.

## VPN Workflow

This is an optional service that allows you to create VPN tunnel configurations to access one or more Non SD-WAN Destinations. The VMware provides the configuration required to create the tunnel(s) – including creating IKE IPsec configuration and generating a pre-shared key.

## Overview

The following figure shows an overview of the VPN tunnels that can be created between the VMware and a Non SD-WAN Destination.



---

**Note** It is required that an IP address be specified for a Primary VPN Gateway at the Non SD-WAN Destination. The IP address is used to form a Primary VPN Tunnel between a SD-WAN Gateway and the Primary VPN Gateway.

Optionally, an IP address can be specified for a Secondary VPN Gateway to form a Secondary VPN Tunnel between a SD-WAN Gateway and the Secondary VPN Gateway. Using Advanced Settings, Redundant VPN Tunnels can be specified for any VPN tunnels you create.

---

**Important** Beginning with the 4.0 release, it is required that the AES-NI instruction set be supported by the CPU on all types of Virtual Machines.

## Configure Non SD-WAN Destinations via Gateway

VMware allows the Enterprise users to define and configure a Non SD-WAN Destination instance to establish a secure IPsec tunnel to a Non SD-WAN Destination through an SD-WAN Gateway.

The Orchestrator selects the nearest Gateway for the Non SD-WAN Destination with its configured IP address, using geolocation service.

You can configure Non SD-WAN Destination via Gateway only at the Profile Level and cannot override at the SD-WAN Edge level.

### ECMP

To optimize the utilization of the aggregated bandwidth across the ingress interfaces of non-SDWAN sites, VMware SD-WAN solution incorporates active-active mode support in its gateways.

This can be achieved by enabling the establishment of multiple IPsec tunnels in active-active mode towards non-SDWAN sites. This configuration allows load balancing of network traffic across tunnels optimizing the flow of distribution.

To implement active-active mode with multiple IPsec tunnels towards non-SDWAN sites, the following three steps are required:

- 1 Set up tunnels connecting to Non-SDWAN sites with tunnel mode as Active-Active.
- 2 Choose the preferred load balancing algorithm.
- 3 Configure BGP or Static site subnet routes directing traffic to these sites.

## Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Non SD-WAN Destinations**, expand **Non SD-WAN Destinations via Gateway**.

### Non SD-WAN Destinations

	Name	Servers	SD-WAN Gateway	Tunnels	Operator Alerts ⓘ	Update Alerts ⓘ	Segment
<input type="checkbox"/>	test	Type: CheckPoint Primary: 20.0.2.2 Secondary: None	Primary: 54.183.9.192 Secondary: None	Deactivated	Activated	Activated	

1 item

- Click **New** or **New NSD via Gateway** option to create a new Non SD-WAN Destination.

**Note** The **New NSD via Gateway** option appears only when there are no items in the table.

### Non SD-WAN Destinations via Gateway

X

Name *	TEST
Type *	Required <span style="color: red;">!</span>
Tunnel Mode	Active/Hot-Standby
<b>VPN Gateways ⓘ</b>	
VPN Gateway 1 (Primary)*	54.183.9.192 Example 54.183.9.192
VPN Gateway 2 (Secondary)	54.183.9.193 Example 54.183.9.192
<span style="border: 1px solid #ccc; border-radius: 50%; padding: 5px; margin-right: 10px;"></span> <span style="border: 1px solid #0070C0; border-radius: 50%; padding: 5px; background-color: #0070C0; color: white; font-weight: bold; font-size: small;">-</span> <span style="border: 1px solid #0070C0; border-radius: 50%; padding: 5px; background-color: #0070C0; color: white; font-weight: bold; font-size: small;">+</span>	
<span style="border: 1px solid #0070C0; border-radius: 5px; padding: 5px; color: white; font-weight: bold; font-size: small; margin-right: 20px;">CANCEL</span> <span style="background-color: #0070C0; color: white; font-weight: bold; font-size: small; padding: 5px 10px; border-radius: 5px;">CREATE</span>	

## Non SD-WAN Destinations via Gateway

**Name \***

TEST

**Type \***

Required

**Tunnel Mode**

Active/Active



If Tunnel Mode is Active/Active, up to 4 tunnel endpoints/Gateways can be configured. All 'Active' Tunnels will be used to send/receive traffic aka ECMP.

## ECMP

**Load Sharing** Flow Load Based  Hash Load Based**Method**

## VPN Gateways

**VPN Gateway 1\***

54.183.9.192



Example 54.183.9.192

**VPN Gateway 2**

54.183.9.193



Example 54.183.9.192

**VPN Gateway 3**

54.183.9.194



Example 54.183.9.192

**VPN Gateway 4**

54.183.9.195

**CANCEL****CREATE**

## Non SD-WAN Destinations via Gateway

**Name \*** TEST

**Type \***

**Tunnel Mode** Active/Active

**ECMP**

**Load Sharing Method**

If Tunnel Mode is Active/Active, up to 4 tunnel endpoints/Gateways can be configured. All 'Active' Tunnels will be used to send/receive traffic aka ECMP.

**VPN Gateways**

<b>VPN Gateway 1*</b>	54.183.9.192	(-)
Example 54.183.9.192		
<b>VPN Gateway 2</b>	54.183.9.193	(-)
Example 54.183.9.192		
<b>VPN Gateway 3</b>	54.183.9.194	(-)
Example 54.183.9.192		
<b>VPN Gateway 4</b>	54.183.9.195	(-) (+)
Example 54.183.9.192		

**CANCEL** **CREATE**

Option	Description
Name	Enter a name for the Non SD-WAN Destination in the text box.
Type	<p>Select an IPsec tunnel type. The available options are:</p> <ul style="list-style-type: none"> <li>■ Configure a Non SD-WAN Destination of Type AWS VPN Gateway</li> </ul>
	<p><b>Note</b> This service is introduced in the 4.3.0 release. Customers can also use different primary Public IPs and Secondary Public IPs for NVS Gateways for AWS.</p>
	<ul style="list-style-type: none"> <li>■ Configure a Non SD-WAN Destination of Type Check Point</li> <li>■ Configure a Non SD-WAN Destination of Type Cisco ASA</li> </ul>
	<p><b>Note</b> Secondary VPN Gateway is not supported for this option.</p>
	<ul style="list-style-type: none"> <li>■ Configure a Non SD-WAN Destination of Type Cisco ISR</li> <li>■ Configure a Non SD-WAN Destination of Type Generic IKEv2 Router (Route Based VPN)</li> <li>■ Configure a Non SD-WAN Destination of Type Microsoft Azure Virtual Hub</li> </ul>
	<p><b>Note</b> Requires a valid subscription.</p>
	<ul style="list-style-type: none"> <li>■ Configure a Non SD-WAN Destination of Type Palo Alto</li> <li>■ Configure a Non SD-WAN Destination of Type SonicWALL</li> <li>■ Configure a Non SD-WAN Destination of Type Zscaler</li> <li>■ Configure a Non SD-WAN Destination of Type Generic IKEv1 Router (Route Based VPN)</li> <li>■ Configure a Non SD-WAN Destination of Type Generic Firewall (Policy Based VPN)</li> </ul>
	<p><b>Note</b> Secondary VPN Gateway is not supported for this option.</p>
Tunnel Mode	<p><b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways.</p>
	<p><b>Active/Active</b> mode supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.</p>
ECMP Load Sharing Method	<p><b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination.</p>

Option	Description
	<b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.
VPN Gateway 1	Enter a valid IP address.
VPN Gateway 2	Enter a valid IP address. This field is optional.
VPN Gateway 3	Enter a valid IP address. This field is optional.
VPN Gateway 4	Enter a valid IP address. This field is optional.

- 3 Click the **Create** button.

You are redirected to an additional configuration options page based on the selected IPsec tunnel type. Click each of the links in the table above for more information on these tunnel types.

- 4 Following are the various options available under the **Non SD-WAN Destinations via Gateway** section:

Option	Description
Delete	Select an item and click this option to delete it.
Operator Alerts	Select an item and set the Operator Alert to <b>On</b> or <b>Off</b> .
Update Alerts	Select an item and update the previously set Operator Alert.
Columns	Click and select the columns to be displayed or hidden on the page.

#### Note

- You can also access these options by clicking the vertical ellipsis next to the item name in the table.
- The **Edit** option takes you to the additional configuration settings screen.
- Click the information icon at the top of the table to view the Conceptual Destination Diagram, and then hover across the diagram for more details.

To edit or configure **BGP**, see [Configure BGP Over IPsec from Gateways](#).

To edit or configure **BFD**, see [Configure BFD for Gateways](#).

Non SD-WAN Peer Type	Number of Tunnels Allowed	
	Active/Active Mode	Active/Hot standbyMode
AWS VPN Gateway	upto 4	upto 2

Non SD-WAN Peer Type	Number of Tunnels Allowed	
Check Point	upto 4	upto 2
Cisco ASA	1 (Mode not applicable)	1 (Mode not applicable)
Cisco ISR	upto 4	upto 2
Generic IKEv2 Router (Route Based VPN)	upto 4	upto 2
Microsoft Azure Virtual Hub	upto 2	upto 2
Palo Alto	upto 4	upto 2
SonicWALL	upto 4	upto 2
Zscaler	upto 4	upto 2
Generic IKEv1 Router (Route Based VPN)	upto 4	upto 2
Generic Firewall (Policy Based VPN)	1 (Mode not applicable)	1 (Mode not applicable)

## Flow Pinning Behavior

Existing flows are pinned to the same path as long as the path/route is available. These flows are not affected during mode or algorithm change.

### What to do next

- Associate your Non SD-WAN Destination to a Profile. For more information, see:
  - [Configure a Tunnel Between a Branch and a Non SD-WAN Destinations via Gateway](#)
  - [Configure Tunnel Between Branch and Non SD-WAN Destinations via Edge](#)
  - [Configure BGP Over IPsec from Gateways](#)
- Configure a Business Policy. For more information, see [Configure Business Policies](#).

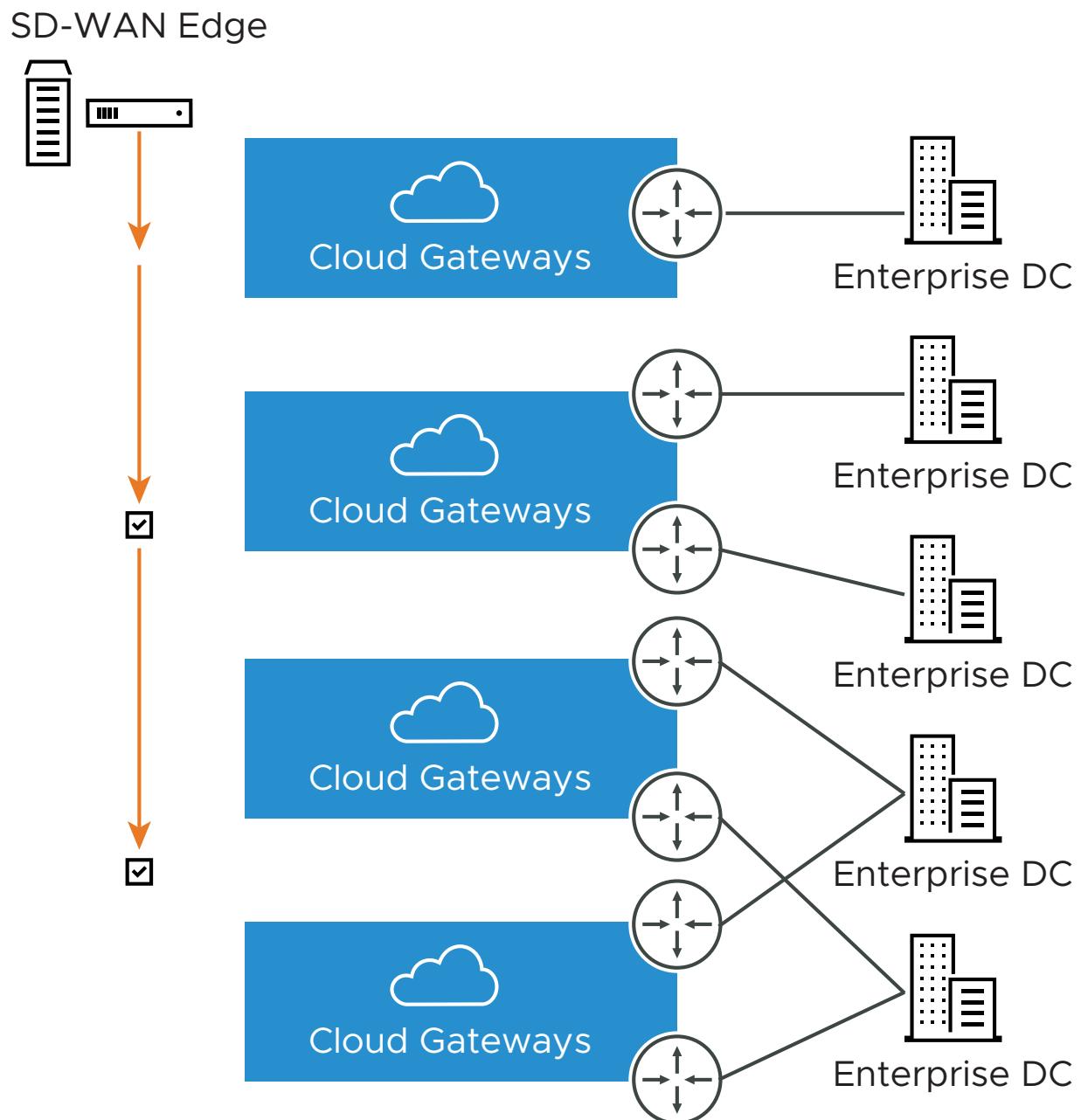
**Note** Configuring Business Policy is not mandatory for this feature.

## Configure a Non SD-WAN Destination of Type AWS VPN Gateway

This service allows you to create VPN tunnel configurations to access one or more Non SD-WAN Destinations. VMware provides the configuration required to create the tunnel(s) – including creating IKE IPsec configuration and generating a pre-shared key.

### Overview

The following figure shows an overview of the VPN tunnels that can be created between VMware and a Non SD-WAN Destination.



**Note** It is required that an IP address be specified for a Primary VPN Gateway at the Non SD-WAN Destination. The IP address is used to form a Primary VPN Tunnel between a SD-WAN Gateway and the Primary VPN Gateway.

Optionally, an IP address can be specified for a Secondary VPN Gateway to form a Secondary VPN Tunnel between an SD-WAN Gateway and the Secondary VPN Gateway. Redundant VPN Tunnels can be specified for any VPN tunnels you create.

#### Configure a Non SD-WAN Destination of type AWS VPN Gateway

Once you have created a Non SD-WAN Destination configuration of the type **AWS VPN Gateway**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST12
Type *	AWS VPN Gateway
Tunnel Mode	Active/Hot-Standby ▾
VPN Gateways ⓘ	
VPN Gateway 1 (Primary)*	54.183.9.192 <span style="float: right;">-</span>
	Example 54.183.9.192
VPN Gateway 2 (Secondary)	54.183.9.193 <span style="float: right;">- +</span>
	Example 54.183.9.192

CANCEL CREATE

Network Services / TEST12 Type: AWS VPN Gateway

## TEST12

**General**

Name \* TEST12

Type \* AWS VPN Gateway

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

⚠ If Tunnel Mode is Active/Hot-Standby, up to 2 tunnel endpoints/Gateways can be configured.

Authentication

Local Auth Id Default

Location

Location  Lat, Lng: 37.402889, -122.116859

**VPN Gateways**

VPN Gateway 1  VPN Gateway 2  Redundant VMware Cloud VPN

VPN Gateway 2  [- REMOVE](#)

Public IP\* 54.183.9.193  Example 54.183.9.192

**Advanced Settings (VPN Gateway 2)**

Tunnel settings

PSK

Encryption AES-128

DH Group 2

PFS 2

Authentication Algorithm SHA\_1

IKE SA Lifetime(min) 1440

IPsec SA Lifetime(min) 480

DPD Type onDemand

DPD Timeout(sec) 20

**Sample IKE / IPsec**

COPY

⚠ This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device.

```
==== VPN Gateway 2 config =====
==== IKE Security Association ====
  Authentication Method: Pre-Shared Key
  Pre-Shared Key: 76a519d80caa3fdb06f019272aae85bd25724eab
  Authentication Algorithm: SHA1
  Encryption Algorithm: AES-128-CBC
  Lifetime: 86,400 seconds
```

You can configure the following tunnel settings, and then click **Save Changes**.

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>AWS VPN Gateway</b> . You cannot edit this option.
Enable Tunnel(s)	Click the toggle button to initiate the tunnel(s) from the SD-WAN Gateway to the AWS VPN Gateway.
Tunnel Mode	<p><b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways.</p> <p><b>Active/Activemode</b> supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.</p>
ECMP Load Sharing Method	<p><b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination.</p> <p><b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.</p>
VPN Gateway 1	Enter a valid IP address.
VPN Gateway 2	Enter a valid IP address. This field is optional.
VPN Gateway 3	Enter a valid IP address. This field is optional.
VPN Gateway 4	Enter a valid IP address. This field is optional.
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> .
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>2</b> .

Option	Description
Authentication Algorithm	<p>Select the authentication algorithm for the VPN header. Select one of the supported Secure Hash Algorithm (SHA) functions from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ SHA1</li> <li>■ SHA256</li> <li>■ SHA384</li> <li>■ SHA512</li> </ul> <p>The default value is <b>SHA 1</b>.</p>
IKE SA Lifetime(min)	<p>Time when Internet Key Exchange (IKE) rekeying is initiated for SD-WAN Edges. The minimum IKE lifetime is 10 minutes and maximum is 1440 minutes. The default value is <b>1440</b> minutes.</p>
IPsec SA Lifetime(min)	<p>Time when Internet Security Protocol (IPsec) rekeying is initiated for Edges. The minimum IPsec lifetime is 3 minutes and maximum is 480 minutes. The default value is <b>480</b> minutes.</p>
DPD Type	<p>The Dead Peer Detection (DPD) method is used to detect if the Internet Key Exchange (IKE) peer is alive or dead. If the peer is detected as dead, the device deletes the IPsec and IKE Security Association. Select either <b>Periodic</b> or <b>onDemand</b> from the drop-down menu. The default value is <b>onDemand</b>.</p>
DPD Timeout(sec)	<p>Enter the DPD timeout value. The DPD timeout value will be added to the internal DPD timer, as described below. Wait for a response from the DPD message before considering the peer to be dead (Dead Peer Detection). Prior to the 5.1.0 release, the default value is 20 seconds. For the 5.1.0 release and later, see the list below for the default value.</p> <ul style="list-style-type: none"> <li>■ Library Name: Quicksec</li> <li>■ Probe Interval: Exponential (0.5 sec, 1 sec, 2 sec, 4 sec, 8 sec, 16 sec)</li> <li>■ Default Minimum DPD Interval: 47.5sec (Quicksec waits for 16 seconds after the last retry. Therefore, <math>0.5+1+2+4+8+16+16 = 47.5</math>).</li> <li>■ Default Minimum DPD interval + DPD Timeout(sec): 67.5 sec</li> </ul> <hr/> <p><b>Note</b> Prior to the 5.1.0 release, you can deactivate DPD by configuring the DPD timeout timer to 0 seconds. However, for the 5.1.0 release and later, you cannot deactivate DPD by configuring the DPD timeout timer to 0 seconds. The DPD timeout value in seconds will get added onto the default minimum value of 47.5 seconds).</p>

Option	Description
Secondary VPN Gateway	<p>Click the <b>Add</b> button, and then enter the IP address of the Secondary VPN Gateway. Click <b>Save Changes</b>.</p> <p>The Secondary VPN Gateway is immediately created for this site and provisions a VMware VPN tunnel to this Gateway.</p>
Redundant VMware Cloud VPN	<p>Select the check box to add redundant tunnels for each VPN Gateway. Changes made to <b>Encryption</b>, <b>DH Group</b>, or <b>PFS</b> of Primary VPN Gateway also apply to the redundant VPN tunnels, if configured.</p>
Local Auth Id	<p>Local authentication ID defines the format and identification of the local gateway. From the drop-down menu, choose from the following types and enter a value:</p> <ul style="list-style-type: none"> <li>■ <b>FQDN</b> - The Fully Qualified Domain Name or hostname. For example: vmware.com</li> <li>■ <b>User FQDN</b> - The User Fully Qualified Domain Name in the form of email address. For example: user@vmware.com</li> <li>■ <b>IPv4</b> - The IP address used to communicate with the local gateway.</li> <li>■ <b>IPv6</b> - The IP address used to communicate with the local gateway.</li> </ul> <p><b>Note</b> If you do not specify a value, <b>Default</b> is used as the local authentication ID.</p>
Sample IKE / IPsec	<p>Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).</p>
Location	<p>Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.</p>
Site Subnets	<p>Use the toggle button to activate or deactivate the <b>Site Subnets</b>. Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b>.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</li> <li>■ If there are no site subnets configured, deactivate <b>Site Subnets</b> to activate the tunnel.</li> </ul>

## Configure a Non SD-WAN Destination of Type Check Point

The SD-WAN Gateway connects to the Check Point CloudGuard service using IKEv1/IPsec. There are two steps to configure a Check Point: Configuring the Check Point CloudGuard service and configuring the Non SD-WAN Destination of type Check Point. You must perform the first step on the Check Point Infinity Portal and the second step on the SASE Orchestrator.

### Configure the Check Point CloudGuard service

- 1 Login to the Check Point's Infinity Portal using the link <https://portal.checkpoint.com/>.
- 2 Once logged in, create a site at Check Point's Infinity Portal using the link <https://sc1.checkpoint.com/documents/integrations/VeloCloud/check-point-VeloCloud-integration.html>.

### Configure a Non SD-WAN Destination of type Check Point

- 1 Once you have created a Non SD-WAN Destination configuration of the type **Check Point**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST14
Type *	Check Point
Tunnel Mode	Active/Hot-Standby
<b>VPN Gateways</b> ⓘ	
VPN Gateway 1 (Primary)*	<input type="text" value="54.183.9.197"/> <span style="margin-left: 10px;">-</span> <span style="color: blue; border: 1px solid blue; border-radius: 50%; padding: 2px;">+</span>
<small>Example 54.183.9.192</small>	
<span style="border: 1px solid #ccc; padding: 5px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 5px 10px; border-radius: 5px;">CREATE</span>	

Network Services / TEST14

Type: Check Point

## TEST14

General

Name \* TEST14

Type \* Check Point

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

⚠ If Tunnel Mode is Active/Hot-Standby, up to 2 tunnel endpoints/Gateways can be configured.

Authentication

Local Auth Id Default

Location

Location  [EDIT](#)

VPN Gateways

Redundant VMware Cloud VPN

**VPN Gateway 1** VPN Gateway 2

VPN Gateway 1 (Primary) [- REMOVE](#)

Public IP\* 54.183.9.197

Example 54.183.9.192

Advanced Settings (VPN Gateway 1 - Primary)

Tunnel settings

PSK  [@](#)

Encryption AES-128

DH Group 2

PFS 2

Sample IKE / IPSec

[COPY](#)

⚠ This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device.

```
==== VPN Gateway 1 config =====
==== IKE Security Association ====
Authentication Method: Pre-Shared Key
Primary tunnel Pre-Shared Key: 1ac3a74f0ec252f19b1de64969d99d4be847b46e
Authentication Algorithm: SHA1
Encryption Algorithm: AES-128-CBC
Lifetime: 86,400 seconds
Authentication Time: 172,800 seconds
Phase 1 Negotiation Mode: main

==== IPSec Security Association ====
Protocol: ESP
Authentication Algorithm: SHA_1
Encryption Algorithm: AES-128-CBC
Lifetime: 28,800 seconds
Mode: tunnel
```

Site Subnets

[+ ADD](#) [DELETE](#)

Subnet <a href="#">@</a>	Description	Advertise
<input type="checkbox"/> Enter IPv4 Subnet	Enter Description (optional)	<input checked="" type="checkbox"/>

1 item

Network Services / test

Type: Check Point

test

**General**

Name *	test
Type *	Check Point
Enable Tunnel(s) ⓘ	<input checked="" type="checkbox"/>
Tunnel Mode	Active/Hot-Standby

**VPN Gateways**

Primary VPN Gateway	Secondary VPN Gateway									
Public IP * 54.183.29.192 Example 54.183.9.192	+ ADD									
<b>Advanced Settings</b> <table border="1"> <tr> <td>Tunnel settings ⓘ</td> </tr> <tr> <td>PSK</td> <td>.....</td> </tr> <tr> <td>Encryption</td> <td>AES-128</td> </tr> <tr> <td>DH Group</td> <td>2</td> </tr> <tr> <td>PFS</td> <td>2</td> </tr> </table>		Tunnel settings ⓘ	PSK	.....	Encryption	AES-128	DH Group	2	PFS	2
Tunnel settings ⓘ										
PSK	.....									
Encryption	AES-128									
DH Group	2									
PFS	2									
<input type="checkbox"/> Redundant VMware Cloud VPN										

---

**Authentication**

Local Auth Id ⓘ	Default
-----------------	---------

**Sample IKE / IPSec**

**Location**

Location ⓘ	Lat, Lng: 37.402889, -122.116859	EDIT
------------	----------------------------------	------

**Site Subnets ⓘ**

+ ADD		DELETE
Subnet ⓘ	Description	Advertise
<input type="checkbox"/> Enter IPv4 Subnet	Enter Description (optional)	<input checked="" type="checkbox"/>

1 item

## 2 You can configure the following tunnel settings:

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>Check Point</b> . You cannot edit this option.

Option	Description
Enable Tunnel(s)	Click the toggle button to initiate the tunnel(s) from the SD-WAN Gateway to the Check Point VPN Gateway.
<b>ECMP Load Sharing Method</b>	<p><b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination.</p> <p><b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.</p>
VPN Gateway 1	Enter a valid IP address.
VPN Gateway 2	Enter a valid IP address. This field is optional.
VPN Gateway 3	Enter a valid IP address. This field is optional.
VPN Gateway 4	Enter a valid IP address. This field is optional.
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> .
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>2</b> .
Redundant VMware Cloud VPN	Select the check box to add redundant tunnels for each VPN Gateway. Changes made to <b>Encryption</b> , <b>DH Group</b> , or <b>PFS</b> of Primary VPN Gateway also apply to the redundant VPN tunnels, if configured.
Secondary VPN Gateway	<p>Click the <b>Add</b> button, and then enter the IP address of the Secondary VPN Gateway. Click <b>Save Changes</b>.</p> <p>The Secondary VPN Gateway is immediately created for this site and provisions a VMware VPN tunnel to this Gateway.</p>

Option	Description
Local Auth Id	<p>Local authentication ID defines the format and identification of the local gateway. From the drop-down menu, choose from the following types and enter a value:</p> <ul style="list-style-type: none"> <li>■ <b>FQDN</b> - The Fully Qualified Domain Name or hostname. For example: vmware.com</li> <li>■ <b>User FQDN</b> - The User Fully Qualified Domain Name in the form of email address. For example: user@vmware.com</li> <li>■ <b>IPv4</b> - The IP address used to communicate with the local gateway.</li> <li>■ <b>IPv6</b> - The IP address used to communicate with the local gateway.</li> </ul>
	<p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ If you do not specify a value, <b>Default</b> is used as the local authentication ID.</li> <li>■ For Checkpoint Non SD-WAN Destination, the default local authentication ID value used is SD-WAN Gateway Interface Public IP.</li> </ul>
Sample IKE / IPsec	<p>Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).</p>
Location	<p>Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.</p>
Site Subnets	<p>Use the toggle button to activate or deactivate the <b>Site Subnets</b>. Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b>.</p> <p><b>Note</b> To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</p>

### 3 Click **Save Changes**.

#### Prerequisites

You must have an active Check Point account and login credentials to access Check Point's Infinity Portal.

#### Configure a Non SD-WAN Destination of Type Cisco ASA

Follow the below steps to configure a Non SD-WAN Destination of type **Cisco ASA** in the SASE Orchestrator.

**Procedure**

- Once you have created a Non SD-WAN Destination configuration of the type **Cisco ASA**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST15
Type *	Cisco ASA
Tunnel Mode	Active/Hot-Standby ▾
<b>VPN Gateways ⓘ</b>	
VPN Gateway 1 (Primary)*	54.183.9.165 <span style="float: right;">(–)</span> Example 54.183.9.192
<div style="border: 1px solid #f0c080; padding: 10px; background-color: #fffacd;"><p><span style="color: #f0c080;">⚠</span> Secondary VPN Gateways are not supported for Cisco ASA VPN. This is a limitation of the Cisco ASA VPN.</p></div>	
<span style="border: 1px solid #0070C0; padding: 5px 10px; color: #0070C0; border-radius: 5px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 5px 10px; border-radius: 5px; margin-left: 10px;">CREATE</span>	

Network Services / TEST15 Type: Cisco ASA

## TEST15

**General**

Name \* TEST15

Type \* Cisco ASA

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

⚠ Secondary VPN Gateways are not supported for Cisco ASA VPN. This is a limitation of the Cisco ASA VPN.

Authentication

Local Auth Id Default

Location

Location  Lat, Lng: 37.402889, -122.116859 [EDIT](#)

**VPN Gateways**

**VPN Gateway 1**

VPN Gateway 1 (Primary)

Public IP\* 54.183.9.165

Example 54.183.9.192

**Advanced Settings (VPN Gateway 1 - Primary)**

Tunnel settings

PSK

Encryption AES-128

DH Group 2

PFS deactivated

**Sample IKE / IPSec**

[COPY](#)

⚠ This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device.

[ASA V8.4 OR LATER](#) [ASA V8.3 OR EARLIER](#)

```
!
! Example ASA Configuration for Cisco ASA Version 8.4 or later
!
! This is an example ASA configuration that has been pre-populated with the
! values required to interoperate with the Cloud VPN. This configuration is
! intended to serve as a guideline. Some assumptions have been made regarding
! system configuration so modifications will likely need to be made to generate
! a working configuration.
!
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 100
    encryption aes
    authentication pre-share
    group 2
    lifetime 86400
```

**Site Subnets**

[+ ADD](#) [DELETE](#)

Subnet <input type="checkbox"/>	Description	Advertise <input checked="" type="checkbox"/>
<input type="checkbox"/> Enter IPv4 Subnet	Enter Description (optional)	<input checked="" type="checkbox"/>

1 item

**Note** Secondary VPN Gateway is not supported for the Cisco ASA service type.

- 2 You can configure the following tunnel settings:

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>Cisco ASA</b> . You cannot edit this option.
Enable Tunnel(s)	Click the toggle button to initiate the tunnel(s) from the SD-WAN Gateway to the Cisco ASA VPN Gateway.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways.  <b>Active/Active</b> mode supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnel can send and receive traffic through ECMP.
VPN Gateway 1	Enter a valid IP address.
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> .
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>deactivated</b> .

Option	Description
Local Auth Id	<p>Local authentication ID defines the format and identification of the local gateway. From the drop-down menu, choose from the following types and enter a value:</p> <ul style="list-style-type: none"> <li>■ <b>FQDN</b> - The Fully Qualified Domain Name or hostname. For example: vmware.com</li> <li>■ <b>User FQDN</b> - The User Fully Qualified Domain Name in the form of email address. For example: user@vmware.com</li> <li>■ <b>IPv4</b> - The IP address used to communicate with the local gateway.</li> <li>■ <b>IPv6</b> - The IP address used to communicate with the local gateway.</li> </ul>
	<p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ If you do not specify a value, <b>Default</b> is used as the local authentication ID.</li> <li>■ For Cisco ASA Non SD-WAN Destination, the default local authentication ID value used is the Local IP address of the SD-WAN Gateway.</li> </ul>
Sample IKE / IPsec	<p>Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).</p>
Location	<p>Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.</p>
Site Subnets	<p>Use the toggle button to activate or deactivate the <b>Site Subnets</b>. Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b>.</p> <p><b>Note</b> To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</p>
Custom Site Subnets	<p>Use this section to override the source subnets routed to this VPN device. Normally, source subnets are derived from the Edge LAN subnets routed to this device.</p>

### 3 Click **Save Changes**.

## Configure a Non SD-WAN Destination of Type Cisco ISR

Follow the below steps to configure a Non SD-WAN Destination of type **Cisco ISR** in the SASE Orchestrator.

**Procedure**

- Once you have created a Non SD-WAN Destination configuration of the type **Cisco ISR**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST45
Type *	Cisco ISR
Tunnel Mode	Active/Hot-Standby
VPN Gateways ⓘ	
VPN Gateway 1 (Primary)*	54.183.9.190
	Example 54.183.9.192
VPN Gateway 2 (Secondary)	53.185.9.192
	Example 54.183.9.192
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px;">CREATE</span>	

Network Services / TEST45 Type: Cisco ISR

## TEST45

**General**

Name \* TEST45

Type \* Cisco ISR

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

⚠ If Tunnel Mode is Active/Hot-Standby, up to 2 tunnel endpoints/Gateways can be configured.

Location

Location  [EDIT](#)

**VPN Gateways**

Redundant VMware Cloud VPN

VPN Gateway 1 [VPN Gateway 2](#)

VPN Gateway 1 (Primary) [- REMOVE](#)

Public IP\* 54.183.9.190

Example 54.183.9.192

**Advanced Settings (VPN Gateway 1 - Primary)**

Tunnel settings

PSK  [\(copy\)](#)

Encryption AES-128

DH Group 2

PFS deactivated

**Sample IKE / IPSec**

[COPY](#)

⚠ This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device.

```
!!! VPN Gateway 1 config =====
! -----
! Example IOS Configuration for Cisco ISR
! -----
! This is an example ISR configuration that has been pre-populated with the
! values required to interoperate with the Cloud VPN. This configuration is
! intended to serve as a guideline. Some assumptions have been made regarding
! system configuration so modifications will likely need to be made to generate
! a working configuration.
!
crypto isakmp policy 100
  encryption aes 128
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
```

**Site Subnets**

[+ ADD](#) [DELETE](#)

<input type="checkbox"/> Subnet <a href="#">(i)</a>	Description	Advertise
<input type="checkbox"/> Enter IPv4 Subnet	Enter Description (optional)	<input checked="" type="checkbox"/>

1 item

VMware by Broadcom

[DISCARD CHANGES](#) [SAVE CHANGES](#)

**2** You can configure the following tunnel settings:

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>Cisco ISR</b> . You cannot edit this option.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways. <b>Active/Activemode</b> supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.
<b>ECMP</b> Load Sharing Method	<b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination.
	<b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.
VPN Gateway 1	Enter a valid IP address.
VPN Gateway 2	Enter a valid IP address. This field is optional.
VPN Gateway 3	Enter a valid IP address. This field is optional.
VPN Gateway 4	Enter a valid IP address. This field is optional.
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> .
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>deactivated</b> .

Option	Description
Redundant VMware Cloud VPN	Select the check box to add redundant tunnels for each VPN Gateway. Changes made to <b>Encryption</b> , <b>DH Group</b> , or <b>PFS</b> of Primary VPN Gateway also apply to the redundant VPN tunnels, if configured.
Secondary VPN Gateway	Click the <b>Add</b> button, and then enter the IP address of the Secondary VPN Gateway. Click <b>Save Changes</b> . The Secondary VPN Gateway is immediately created for this site and provisions a VMware VPN tunnel to this Gateway.
Sample IKE / IPsec	Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).
Location	Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.
Site Subnets	<p>Use the toggle button to activate or deactivate the <b>Site Subnets</b>. Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b>.</p> <p><b>Note</b> To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</p>

**Note** For Cisco ISR Non SD-WAN Destination, by default, the local authentication ID value used is SD-WAN Gateway Interface Local IP.

- 3 Click **Save Changes**.

### Configure a Non SD-WAN Destination of Type Generic IKEv2 Router (Route Based VPN)

Follow the below steps to configure a Non SD-WAN Destination of type **Generic IKEv2 Router (Route Based VPN)** in the SASE Orchestrator.

**Procedure**

- Once you have created a Non SD-WAN Destination configuration of the type **Generic IKEv2 Router (Route Based VPN)**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST51
Type *	Generic IKEv2 Router (Route Based VPN) <span style="float: right;">▼</span>
Tunnel Mode	Active/Hot-Standby <span style="float: right;">▼</span>
 VPN Gateways <span style="color: #0070C0;">(i)</span>	
VPN Gateway 1 (Primary)*	55.185.9.193 <span style="float: right;">(−) (+)</span> Example 54.183.9.192
<span style="border: 1px solid #ccc; padding: 5px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 5px 10px; border-radius: 5px;">CREATE</span>	

Network Services / TEST51      Type: Generic IKEv2 Router (Route Based VPN)

## TEST51

**General**

Name \* TEST51

Type \* Generic IKEv2 Router ( [Edit](#) )

Enable Tunnel(s) [Edit](#)

Tunnel Mode Active/Hot-Standby

**⚠️** If Tunnel Mode is Active/Hot-Standby, up to 2 tunnel endpoints/Gateways can be configured.

Authentication

Local Auth Id Default

Location

Location [Edit](#) Lat, Lng: 37.402889, -122.116859

**VPN Gateways**

Redundant VMware Cloud VPN

VPN Gateway 1 [+ Add New Gateway](#)

VPN Gateway 1 (Primary)

Public IP\* 55.185.9.193  
Example 54.183.9.192

**Advanced Settings (VPN Gateway 1 - Primary)**

Tunnel settings [Edit](#)

PSK	***** <a href="#">Edit</a>
Encryption	AES-128
DH Group	2
PFS	2
Authentication Algorithm	SHA_1
IKE SA Lifetime(min)	1440
IPSec SA Lifetime(min)	480
DPD Type	onDemand
DPD Timeout(sec)	20

**Sample IKE / IPSec**

[COPY](#)

**⚠️** This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device. [X](#)

```
== VPN Gateway 1 config =====
== IKE Security Association ==
Authentication Method: Pre-Shared Key
Primary tunnel Pre-Shared Key: 9aae21a63df545a413a0813e942ade3ac1b7d47f
Authentication Algorithm: SHA1
Encryption Algorithm: AES-128-CBC
Lifetime: 86,400 seconds
Authentication Time: 172,800 seconds
Phase 1 Negotiation Mode: main
```

**2** You can configure the following tunnel settings:

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>Generic IKEv2 Router (Route Based VPN)</b> . You cannot edit this option.
Enable Tunnel(s)	Click the toggle button to initiate the tunnel(s) from the SD-WAN Gateway to the Generic IKEv2 Router VPN Gateway.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways. <b>Active/Active</b> mode supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.
<b>ECMP</b> Load Sharing Method	<b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination. <b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.
VPN Gateway 1	Enter a valid IP address.
VPN Gateway 2	Enter a valid IP address. This field is optional.
VPN Gateway 3	Enter a valid IP address. This field is optional.
VPN Gateway 4	Enter a valid IP address. This field is optional.
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> .

Option	Description
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>2</b> .
Authentication Algorithm	<p>Select the authentication algorithm for the VPN header. Select one of the supported Secure Hash Algorithm (SHA) functions from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ SHA1</li> <li>■ SHA256</li> <li>■ SHA384</li> <li>■ SHA512</li> </ul> <p>The default value is <b>SHA 1</b>.</p>
IKE SA Lifetime(min)	Time when Internet Key Exchange (IKE) rekeying is initiated for SD-WAN Edges. The minimum IKE lifetime is 10 minutes and maximum is 1440 minutes. The default value is <b>1440</b> minutes.
IPsec SA Lifetime(min)	Time when Internet Security Protocol (IPsec) rekeying is initiated for Edges. The minimum IPsec lifetime is 3 minutes and maximum is 480 minutes. The default value is <b>480</b> minutes.
DPD Type	The Dead Peer Detection (DPD) method is used to detect if the Internet Key Exchange (IKE) peer is alive or dead. If the peer is detected as dead, the device deletes the IPsec and IKE Security Association. Select either <b>Periodic</b> or <b>onDemand</b> from the drop-down menu. The default value is <b>onDemand</b> .
DPD Timeout(sec)	<p>Enter the DPD timeout value. The DPD timeout value will be added to the internal DPD timer, as described below. Wait for a response from the DPD message before considering the peer to be dead (Dead Peer Detection).</p> <p>Prior to the 5.1.0 release, the default value is 20 seconds. For the 5.1.0 release and later, see the list below for the default value.</p> <ul style="list-style-type: none"> <li>■ Library Name: Quicksec</li> <li>■ Probe Interval: Exponential (0.5 sec, 1 sec, 2 sec, 4 sec, 8 sec, 16 sec)</li> <li>■ Default Minimum DPD Interval: 47.5sec (Quicksec waits for 16 seconds after the last retry. Therefore, <math>0.5+1+2+4+8+16+16 = 47.5</math>).</li> <li>■ Default Minimum DPD interval + DPD Timeout(sec): 67.5 sec</li> </ul>
	<p><b>Note</b> Prior to the 5.1.0 release, you can deactivate DPD by configuring the DPD timeout timer to 0 seconds. However, for the 5.1.0 release and later, you cannot deactivate DPD by configuring the DPD timeout timer to 0 seconds. The DPD timeout value in seconds will get added onto the default minimum value of 47.5 seconds).</p>

Option	Description
Redundant VMware Cloud VPN	Select the check box to add redundant tunnels for each VPN Gateway. Changes made to <b>Encryption</b> , <b>DH Group</b> , or <b>PFS</b> of Primary VPN Gateway also apply to the redundant VPN tunnels, if configured.
Secondary VPN Gateway	Click the <b>Add</b> button, and then enter the IP address of the Secondary VPN Gateway. Click <b>Save Changes</b> . The Secondary VPN Gateway is immediately created for this site and provisions a VMware VPN tunnel to this Gateway.
Local Auth Id	<p>Local authentication ID defines the format and identification of the local gateway. From the drop-down menu, choose from the following types and enter a value:</p> <ul style="list-style-type: none"> <li>■ <b>FQDN</b> - The Fully Qualified Domain Name or hostname. For example: vmware.com</li> <li>■ <b>User FQDN</b> - The User Fully Qualified Domain Name in the form of email address. For example: user@vmware.com</li> <li>■ <b>IPv4</b> - The IP address used to communicate with the local gateway.</li> <li>■ <b>IPv6</b> - The IP address used to communicate with the local gateway.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ If you do not specify a value, <b>Default</b> is used as the local authentication ID.</li> <li>■ The default local authentication ID value is the SD-WAN Gateway Interface Public IP.</li> </ul>
Sample IKE / IPsec	Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).
Location	Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.
Site Subnets	<p>Use the toggle button to activate or deactivate the <b>Site Subnets</b>. Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b>.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</li> <li>■ If there are no site subnets configured, deactivate <b>Site Subnets</b> to activate the tunnel.</li> </ul>

---

**Note** When AWS initiates the rekey tunnel with a VMware SD-WAN Gateway (in Non SD-WAN Destinations), a failure can occur and the tunnel may not be established, which can cause traffic interruption. In this case, adhere to the following:

- IPsec SA Lifetime(min) timer configurations for the SD-WAN Gateway must be less than 60 minutes (recommended value = 50 minutes), to match the AWS default IPsec configuration.
  - **DH Group** and **PFS** values must be matched.
- 

- 3 Click **Save Changes**.

## Configure a Non SD-WAN Destination of Type Microsoft Azure Virtual Hub

Follow the below steps to configure a Non SD-WAN Destination of type **Microsoft Azure Virtual Hub** in the SASE Orchestrator.

### Prerequisites

- Ensure you have configured a Cloud subscription. For steps, see [Configure API Credentials](#).
- Ensure you have created Virtual WAN and Hubs in Azure. For steps, see [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#).

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Non SD-WAN Destinations**, expand **Non SD-WAN Destinations via Gateway**.

- 2 Click **New**, and then enter the **Name** and **Type** of the Non SD-WAN Destination. Once you enter the **Type** as **Microsoft Azure Virtual Hub**, **Virtual Hub Configuration** section is displayed in the dialog:

Non SD-WAN Destinations via Gateway X

<b>Name *</b>	<input type="text" value="Enter Name"/>
<b>Type *</b>	<input type="text" value="Microsoft Azure Virtual Hub"/> <span style="float: right;">▼</span>
<b>Tunnel Mode</b>	<input type="text" value="Active/Hot-Standby"/> <span style="float: right;">▼</span>
<b>Virtual Hub Configuration</b>	
<b>Subscription *</b>	<input type="text"/> <span style="float: right;">! ▼</span> No compatible Subscriptions were found for the selected Service Type.
<b>Virtual WAN *</b>	<input type="text"/> <span style="float: right;">▼</span>
<b>Resource Group</b>	N/A
<b>Virtual Hub *</b> <span style="color: red;">!</span>	<input type="text"/> <span style="float: right;">▼</span>
<b>Azure Region</b>	N/A
<b>Enable Tunnel(s)</b> <span style="color: red;">!</span>	<input checked="" type="checkbox"/>
<span style="border: 1px solid #ccc; padding: 5px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 5px 10px; border-radius: 5px;">CREATE</span>	

**3** You can configure the following settings:

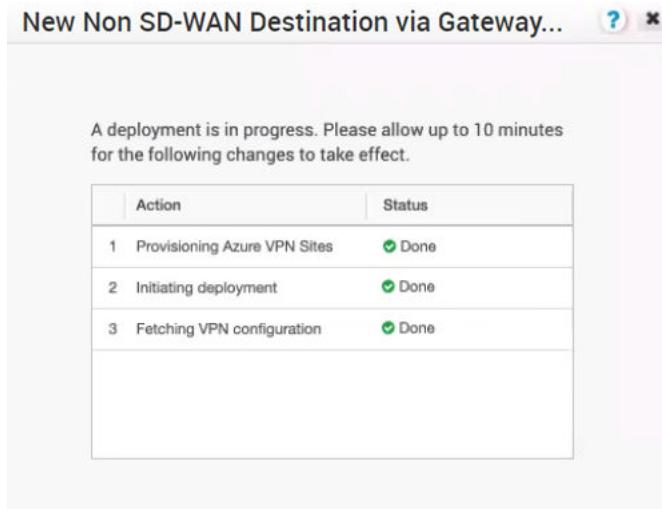
Option	Description
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>Microsoft Azure Virtual Hub</b> . You cannot edit this option.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways. <b>Active/Activemode</b> supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.
<b>ECMP</b> Load Sharing Method	<b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination. <b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.
Subscription	Select a subscription from the drop-down menu.
Virtual WAN	The application fetches all the available Virtual WANs dynamically from Azure. Select a virtual WAN from the drop-down menu.
Resource Group	The application auto-populates the resource group to which the selected <b>Virtual WAN</b> is associated.
Virtual Hub	Select a virtual Hub from the drop-down menu.
Azure Region	The application auto-populates the Azure region corresponding to the selected <b>Virtual Hub</b> .
Enable Tunnel(s)	Select the <b>Enable Tunnel(s)</b> check box to allow VMware VPN Gateways to initiate VPN connections to the target <b>Virtual Hub</b> as soon as the site is successfully provisioned.

#### Note

- VMware VPN Gateways initiate the IKE negotiation only when the Non SD-WAN Destination is configured on at least one profile.
- For Microsoft Azure Non SD-WAN Destination, the default local authentication ID value used is SD-WAN Gateway Interface Public IP.

**4 Click **Create**.**

The SASE Orchestrator automatically initiates deployment, provisions Azure VPN Sites, and downloads the VPN Site Configuration for the newly configured sites. It stores the configuration in the SASE Orchestrator's Non SD-WAN Destination configuration database.



Once the Azure VPN sites are provisioned at the SASE Orchestrator side, you can view the VPN sites (Primary and Redundant) in the Azure portal by navigating to **Virtual WAN > Virtual WAN architecture > VPN sites**.

#### What to do next

- Associate the Microsoft Azure Non SD-WAN Destination to a Profile to establish a tunnel between a branch and Azure Virtual Hub. For more information, see [Associate a Microsoft Azure Non SD-WAN Destination to an SD-WAN Profile](#).
- You must add SD-WAN routes into Azure network manually. For more information, see [Edit a VPN Site](#).
- After associating a Profile to the Microsoft Azure Non SD-WAN Destination, you can return to the **Non SD-WAN Destinations via Gateway** section by navigating to **Configure > Network Services**, and then configure the BGP settings for the Non SD-WAN Destination. Scroll to the name of your Non SD-WAN Destination, and then click the **Edit** link in the **BGP** column. For more information, see [Configure BGP Over IPsec from Gateways](#).
- In the **Non SD-WAN Destinations via Gateway** area, click the **Edit** link in the **BFD** column for a Non SD-WAN Destination, to configure the BFD settings. For more information, see [Configure BFD for Gateways](#).

For information about Azure Virtual WAN Gateway Automation, see [Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Gateway](#).

## Configure a Non SD-WAN Destination of Type Palo Alto

Follow the below steps to configure a Non SD-WAN Destination of type **Palo Alto** in the SASE Orchestrator.

### Procedure

- Once you have created a Non SD-WAN Destination configuration of the type **Palo Alto**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST55					
Type *	Palo Alto					
Tunnel Mode	Active/Hot-Standby					
VPN Gateways <span style="color: #0070C0;">(i)</span>	<table border="0"><tr><td>VPN Gateway 1 (Primary)*</td><td>55.136.10.195</td><td><span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px;">-</span> <span style="border: 1px solid #0070C0; border-radius: 50%; padding: 2px; color: #0070C0;">+</span></td></tr><tr><td colspan="2">Example 54.183.9.192</td></tr></table>	VPN Gateway 1 (Primary)*	55.136.10.195	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px;">-</span> <span style="border: 1px solid #0070C0; border-radius: 50%; padding: 2px; color: #0070C0;">+</span>	Example 54.183.9.192	
VPN Gateway 1 (Primary)*	55.136.10.195	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px;">-</span> <span style="border: 1px solid #0070C0; border-radius: 50%; padding: 2px; color: #0070C0;">+</span>				
Example 54.183.9.192						
<span style="border: 1px solid #ccc; border-radius: 5px; padding: 5px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; border-radius: 5px; padding: 5px 10px; font-weight: bold;">CREATE</span>						

Network Services / TEST55 Type: Palo Alto

## TEST55

**General**

Name \* TEST55

Type \* Palo Alto

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

⚠ If Tunnel Mode is Active/Hot-Standby, up to 2 tunnel endpoints/Gateways can be configured.

Location

Location  Lat, Lng: 37.402889, -122.116859

**VPN Gateways**

VPN Gateway 1   Redundant VMware Cloud VPN

VPN Gateway 1 (Primary)

Public IP\* 55.136.10.195  Example 54.183.9.192

**Advanced Settings (VPN Gateway 1 - Primary)**

Tunnel settings

PSK

Encryption AES-128

DH Group 2

PFS 5

**Sample IKE / IPSec**

⚠ This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device.

```
==== VPN Gateway 1 config =====
```

Tunnel Config

Step 1

Navigate to Network, Network Profiles, IKE Gateways, Add

```
==== IKE Gateway ====
Name: (Choose a name)
Interface: ethernet1/1 (or your WAN interface)
Local IP Address: None
Peer Type: Static
Peer IP Address: 20.1.0.2
Pre-Shared Key: ee30b89351c83eb16b8bbaf6983c4042e5aae91c
Confirm Pre-shared Key: ee30b89351c83eb16b8bbaf6983c4042e5aae91c
Local Identification: IP address: (Your WAN interface IP address)
Peer Identification: IP address: 20.1.0.2
Show Advanced Phase 1 Options: True
Exchange Mode: main
IKE Crypto Profile: New IKE Crypto Profile
Name: (Choose a name)
DH Group: group 2
Encryption: aes128
Authentication: sha1
Lifetime: 8 hours
Enable Passive Mode: False
Enable NAT Traversal: True
Dead Peer Detection: True
Interval: 10
```

VMware by Broadcom

**2** You can configure the following tunnel settings:

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>Palo Alto</b> . You cannot edit this option.
Enable Tunnel(s)	Click the toggle button to initiate the tunnel(s) from the SD-WAN Gateway to the Palo Alto VPN Gateway.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways. <b>Active/Activemode</b> supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.
ECMP Load Sharing Method	<b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination. <b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.
VPN Gateway 1	Enter a valid IP address.
VPN Gateway 2	Enter a valid IP address. This field is optional.
VPN Gateway 3	Enter a valid IP address. This field is optional.
VPN Gateway 4	Enter a valid IP address. This field is optional.
Primary VPN Gateway	
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> . It is recommended to use DH Group <b>14</b> .

Option	Description
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>5</b> .
Redundant VMware Cloud VPN	Select the check box to add redundant tunnels for each VPN Gateway. Changes made to <b>Encryption</b> , <b>DH Group</b> , or <b>PFS</b> of Primary VPN Gateway also apply to the redundant VPN tunnels, if configured.
Secondary VPN Gateway	Click the <b>Add</b> button, and then enter the IP address of the Secondary VPN Gateway. Click <b>Save Changes</b> . The Secondary VPN Gateway is immediately created for this site and provisions a VMware VPN tunnel to this Gateway.
Sample IKE / IPsec	Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).
Location	Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.
Site Subnets	Use the toggle button to activate or deactivate the <b>Site Subnets</b> . Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b> .
<p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</li> <li>■ If there are no site subnets configured, deactivate <b>Site Subnets</b> to activate the tunnel.</li> </ul>	

**Note** For Palo Alto Non SD-WAN Destination, the default local authentication ID value used is SD-WAN Gateway Interface Public IP.

- 3 Click **Save Changes**.

## Configure a Non SD-WAN Destination of Type SonicWALL

Follow the below steps to configure a Non SD-WAN Destination of type **SonicWALL** in the SASE Orchestrator.

**Procedure**

- Once you have created a Non SD-WAN Destination configuration of the type **SonicWALL**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST65
Type *	SonicWall
Tunnel Mode	Active/Hot-Standby
VPN Gateways ⓘ	
VPN Gateway 1 (Primary)*	65.172.2.180
	Example 54.183.9.192
	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px;">-</span> <span style="border: 1px solid #0070C0; border-radius: 50%; padding: 2px; color: #0070C0;">+</span>
<span style="border: 1px solid #ccc; padding: 5px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: none; padding: 5px; font-weight: bold;">CREATE</span>	

Network Services / TEST65

Type: SonicWall

## TEST65

**General**

Name *	TEST65
Type *	SonicWall
Enable Tunnel(s) ⓘ	<input checked="" type="checkbox"/>
Tunnel Mode	Active/Hot-Standby
<b>⚠ If Tunnel Mode is Active/Hot-Standby, up to 2 tunnel endpoints/Gateways can be configured.</b>	
<b>Location</b>	
Location ⓘ	Lat, Lng: 37.402889, -122.116859 <a href="#">EDIT</a>

**VPN Gateways**

<input type="checkbox"/> Redundant VMware Cloud VPN
<b>VPN Gateway 1</b> + Add New Gateway
VPN Gateway 1 (Primary)
Public IP* 65.172.2.180
Example 54.183.9.192
<b>Advanced Settings (VPN Gateway 1 - Primary)</b>
Tunnel settings ⓘ
PSK ..... ⓘ
Encryption AES-128
DH Group 2
PFS 2

**Sample IKE / IPsec**

<input type="button" value="COPY"/>
<b>⚠ This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device.</b>
==== VPN Gateway 1 config =====
<b>Tunnel Config</b>
Step 1
Navigate to VPN, Settings, Add...
<b>In the General Tab</b>
Policy Type: Tunnel Interface Authentication Method: IKE using Preshared Secret Name: (Choose a name) IPsec Primary Gateway Name or Address: 20.1.0.2
Shared Secret: d2e81beb381fbac30ecb6f13bc9df6e45dee272d Confirm Shared Secret: d2e81beb381fbac30ecb6f13bc9df6e45dee272d Local IKE ID: IP Address (Leave Blank) Peer IKE ID: IP Address (Leave Blank)
<b>In the Proposal Tab</b>
Exchange: Main Mode DH Group: Group 2 Encryption: AES-128 Authentication: SHA1 Life Time (seconds): 86400
Protocol: ESP Encryption: AES-128 Authentication: SHA1

**2** You can configure the following tunnel settings:

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>SonicWALL</b> . You cannot edit this option.
Enable Tunnel(s)	Click the toggle button to initiate the tunnel(s) from the SD-WAN Gateway to the SonicWALL VPN Gateway.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways. <b>Active/Activemode</b> supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.
ECMP Load Sharing Method	<b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination.
	<b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.
VPN Gateway 1	Enter a valid IP address.
VPN Gateway 2	Enter a valid IP address. This field is optional.
VPN Gateway 3	Enter a valid IP address. This field is optional.
VPN Gateway 4	Enter a valid IP address. This field is optional.
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> .
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>2</b> .

Option	Description
Redundant VMware Cloud VPN	Select the check box to add redundant tunnels for each VPN Gateway. Changes made to <b>Encryption</b> , <b>DH Group</b> , or <b>PFS</b> of Primary VPN Gateway also apply to the redundant VPN tunnels, if configured.
Secondary VPN Gateway	Click the <b>Add</b> button, and then enter the IP address of the Secondary VPN Gateway. Click <b>Save Changes</b> . The Secondary VPN Gateway is immediately created for this site and provisions a VMware VPN tunnel to this Gateway.
Sample IKE / IPsec	Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).
Location	Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.
Site Subnets	Use the toggle button to activate or deactivate the <b>Site Subnets</b> . Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b> .
<b>Note</b> <ul style="list-style-type: none"> <li>■ To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</li> <li>■ If there are no site subnets configured, deactivate <b>Site Subnets</b> to activate the tunnel.</li> </ul>	

**Note** For SonicWALL Non SD-WAN Destination, the default local authentication ID value used is SD-WAN Gateway Interface Public IP.

### 3 Click **Save Changes**.

## Zscaler and VMware SD-WAN Integration

Enterprises can take advantage of secure local Internet breakout by using VMware SD-WAN integrated with Zscaler. Using VMware SD-WAN, the network administrator can decide what traffic should be forwarded to Zscaler, using IPsec tunnels (with NULL encryption).

### Prerequisites

The prerequisites to provision a new service with Zscaler and VMware SD-WAN are:

- Zscaler Internet Access (ZIA)
  - A working instance of ZIA (any cloud)
  - Administrator login credentials

- VMware SASE Orchestrator
  - Enterprise account access to VMware SASE Orchestrator
  - Administrator login credentials
  - One or more VMware SD-WAN Edge appliances with “Online” status in VMware SASE Orchestrator

### Zscaler SD-WAN Gateway Selection and Routing Behavior

The VMware SASE Orchestrator configuration process for building tunnels to Zscaler does not require the manual selecting of specific VMware SD-WAN Gateways. Using a geo-IP lookup process, the VMware SD-WAN Gateways are dynamically chosen based on proximity to the provided Zscaler IP endpoint. Operator and Partner Administrators with sufficient permissions can manually override the SASE Orchestrator-default Gateway selections. Normally, this is not necessary, and the recommended best-practice is to accept the SD-WAN Gateways as chosen by the system. After the Zscaler configuration has been completed on the SASE Orchestrator and the tunnels are up and active, Operator and Partner Administrators (with sufficient permissions) can verify which SD-WAN Gateways were chosen. To verify which SD-WAN Gateways were selected, login to the Orchestrator and go to Operator > Gateways. Click on a specific SD-WAN Gateway and look for “Secure VPN Gateway”. Listed beside “Secure VPN Gateway” will be the name of the Zscaler setup as set during the configuration process. The primary SD-WAN Gateway will be denoted with the *Zscaler\_Name* and the redundant SD-WAN Gateway will be denoted as *Zscaler\_Name[redundant]*.

#### Primary SD-WAN Gateway

Customer Usage			
	Customer	Pool	Gateway Type
1	SEC	Production	On Premise Gateway <input checked="" type="checkbox"/> 1 Edge
2	SEC	Production	Secure VPN Gateway <input checked="" type="checkbox"/> Zscaler
3	SEC	Production	Secure VPN Gateway <input checked="" type="checkbox"/> Zscaler

#### Redundant SD-WAN Gateway

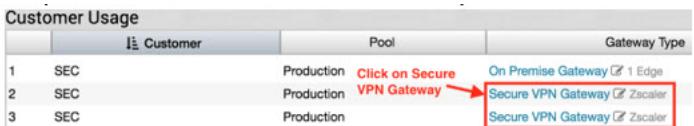
Customer Usage			
	Customer	Pool	Gateway Type
1	SEC	Production	Super Gateway <input checked="" type="checkbox"/>
2	SEC	Production	On Premise Gateway <input checked="" type="checkbox"/> 1 Edge
3	SEC	Production	Secure VPN Gateway <input checked="" type="checkbox"/> Zscaler [redundant]
4	SEC	Production	Secure VPN Gateway <input checked="" type="checkbox"/> Zscaler [redundant]

To set the Zscaler tunnel to a specific SD-WAN Gateway, you must first locate which SD-WAN Gateway has the tunnel by following the process above. From there you can click on “Secure VPN Gateway” and move/assign the tunnel to a different SD-WAN Gateway.

- 1 Locate current tunnel location.

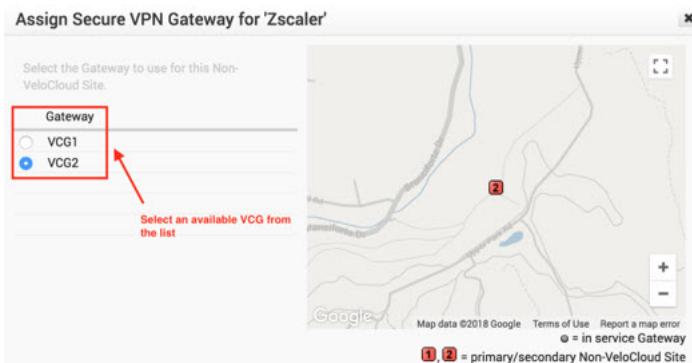
Customer Usage			
	Customer	Pool	Gateway Type
1	SEC	Production	On Premise Gateway <input checked="" type="checkbox"/> 1 Edge
2	SEC	Production	Secure VPN Gateway <input checked="" type="checkbox"/> Zscaler
3	SEC	Production	Secure VPN Gateway <input checked="" type="checkbox"/> Zscaler

2 Click on Secure VPN Gateway.



Customer Usage			
	Customer	Pool	Gateway Type
1	SEC	Production	On Premise Gateway <input checked="" type="checkbox"/> 1 Edge
2	SEC	Production	Secure VPN Gateway <input checked="" type="checkbox"/> Zscaler
3	SEC	Production	Secure VPN Gateway <input checked="" type="checkbox"/> Zscaler

3 Select a SD-WAN Gateway.



**Note** Assigning/Moving a tunnel to a different SD-WAN Gateway is service affecting. The existing tunnel connection will terminate and a new tunnel from the newly assigned SD-WAN Gateway will be established.

During the VMware SD-WAN Edge configuration/activation process, each Edge is assigned a pair of cloud SD-WAN Gateways or a set of Partner SD-WAN Gateways, in accordance with the device configuration. If the SD-WAN Gateways used by the Edge are not the same SD-WAN Gateways which contain the Zscaler tunnels, the Edge will automatically build VCMP tunnels to the SD-WAN Gateways that connect to Zscaler in addition to the SD-WAN Gateways that are selected during the activation process. This ensures the Edge has a path to reach Zscaler.

## Zscaler Setup Examples

### Example 1: Primary Zscaler tunnel to 1.1.1.1 with NO Redundant Velocloud Cloud VPN Selected

Network Services / Zscaler1

Zscaler1

Type: Zscaler

**General**

Name: Zscaler1

Type: Zscaler

Enable Tunnel(s):

Tunnel Mode: Active/Hot-Standby

**VPN Gateways**

Primary VPN Gateway

Public IP\*: 1.1.1.1  
Example 54.193.9.192

Zscaler IP Address:

Secondary VPN Gateway: [+ ADD](#)

**Advanced Settings**

Tunnel settings:  PSK:

Redundant VMware Cloud VPN: Unchecked = No Gateway Redundancy

**Authentication**

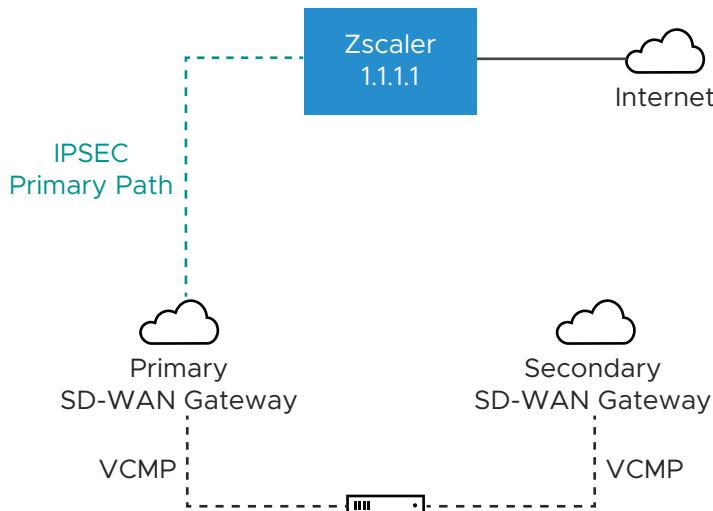
Local Auth Id: IPv4  
10.0.1.1  
Example 10.0.2.5

**Sample IKE / IPSec**

**Location**

**Zscaler Settings**

[DISCARD CHANGES](#) [SAVE CHANGES](#)

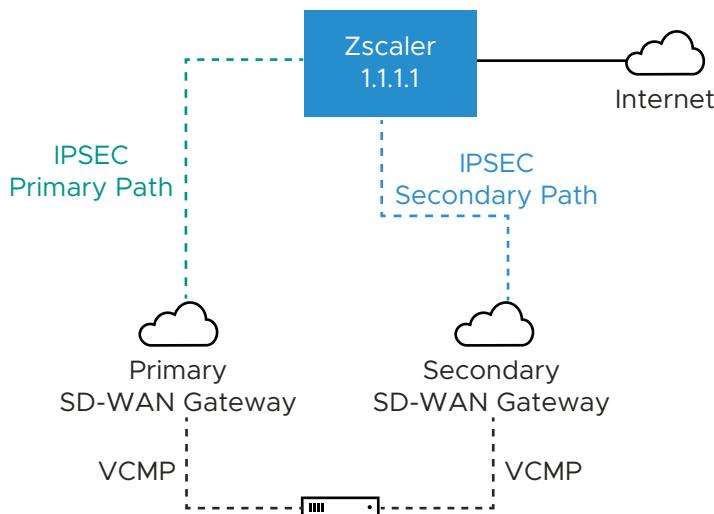


In this example, only one Zscaler VPN tunnel is created, and the Redundant Velocloud Cloud VPN checkbox is not selected. A single Gateway (Primary SD-WAN Gateway in this case) selected based on the proximity to the remote VPN Gateway (as determined via Geo-IP lookup), will create an IPsec tunnel to the Zscaler VPN endpoint. Dependent on Business Policy configuration, traffic will flow from the SD-WAN Edge, to the Primary SD-WAN Gateway and then on to Zscaler. Even though the SD-WAN Edge always has VCMP tunnels to at least two SD-WAN Gateways,

there is no redundancy in this design. Since the Redundant Velocloud Cloud VPN checkbox is not selected, there will not be a backup SD-WAN Gateway tunnel to Zscaler. If either Zscaler or the primary SD-WAN Gateway fails or if the IPsec tunnel between the two goes down for any reason traffic to Zscaler will be dropped.

### Example 2: Primary Zscaler tunnel to 1.1.1.1 with Redundant Velocloud Cloud VPN Selected

The screenshot shows the 'Network Services / Zscaler1' configuration page. Under 'General' settings, the 'Name' is set to 'Zscaler1' and the 'Type' is 'Zscaler'. The 'Enable Tunnel(s)' switch is turned off. The 'Tunnel Mode' is set to 'Active/Hot-Standby'. In the 'VPN Gateways' section, the 'Primary VPN Gateway' is configured with a 'Public IP' of '1.1.1.1' and a 'Zscaler IP Address' of '54.183.9.192'. The 'Secondary VPN Gateway' section has a '+ ADD' button. Under 'Advanced Settings', 'Tunnel settings' are shown with PSK and Redundant Tunnel PSK fields. A red box highlights the 'Redundant VMCloud Cloud VPN' checkbox, which is checked, with a callout 'Checked = Gateway Redundancy'. The 'Authentication' section shows a 'Local Auth Id' of 'IPv4' with an IP address of '10.0.1.1'. The 'Sample IKE / IPSec' section is collapsed. The 'Location' section is also collapsed. At the bottom right are 'DISCARD CHANGES' and 'SAVE CHANGES' buttons.

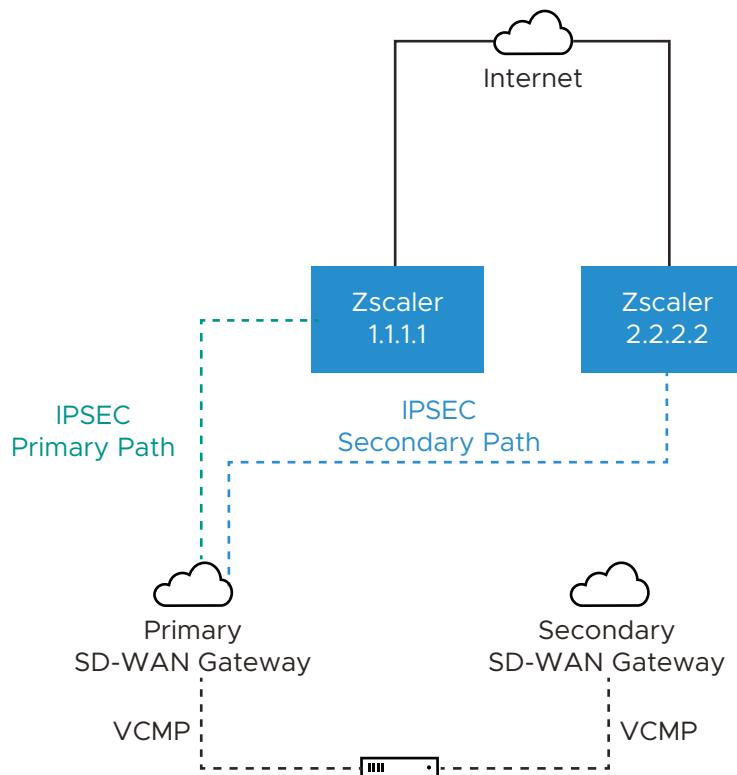


In this example, only one Zscaler VPN tunnel is created, and the Redundant Velocloud Cloud VPN checkbox is selected. Two SD-WAN Gateways selected based on the proximity to the remote VPN Gateway (as determined via Geo-IP lookup) that are the closest to the Zscaler location will build IPsec tunnels to Zscaler. Both of these tunnels are active, however all traffic to Zscaler will traverse through the Primary SD-WAN Gateway. If the Primary SD-WAN Gateway fails traffic will then shift to the Secondary SD-WAN Gateway. Since only a single Zscaler endpoint is defined if it goes down traffic to Zscaler will be dropped.

### Example 3: Primary Zscaler tunnel to 1.1.1.1, Secondary Zscaler tunnel to 2.2.2.2 with NO Redundant Velocloud Cloud VPN Selected

The screenshot shows the VMware SD-WAN Administration interface for a network service named "Zscaler1".

- General:** Name is set to "Zscaler1", Type is "Zscaler", and Tunnel Mode is "Active/Hot-Standby".
- VPN Gateways:**
  - Primary VPN Gateway:** Public IP is 1.1.1.1 (Example 54.193.9.192). A red box highlights the "Zscaler Primary IP Address" field.
  - Secondary VPN Gateway:** Public IP is 2.2.2.2 (Example 54.193.9.192). A red box highlights the "Zscaler Secondary IP Address" field.
  - Advanced Settings:** Tunnel settings (PSK) and PSK values are shown.
  - Redundant VMCloud VPN:** An unchecked checkbox labeled "Unchecked = No Gateway Redundancy".
- Authentication:** Local Auth Id is set to IPv4 (10.0.1.1, Example 10.0.2.5).
- Sample IKE / IPSec:** Shows basic configuration options.
- Buttons:** DISCARD CHANGES and SAVE CHANGES.



In this example, redundant IPsec tunnels to Zscaler are configured in the SASE Orchestrator by adding a secondary Zscaler IP address, however Redundant Velocloud Cloud VPN checkbox is not selected. A single SD-WAN Gateway selected based on the proximity to the remote VPN Gateway (as determined via Geo-IP lookup), will create an IPsec tunnel to both Zscaler VPN endpoints. Both of these tunnels are active, but by configuration settings the SD-WAN Gateway knows which IPsec tunnel to Zscaler is the primary path and will send traffic through that tunnel. Zscaler does not mark primary or backup IPsec tunnels. Zscaler will simply return traffic via the SD-WAN Gateway that originated the request. Should the primary Zscaler location go down, traffic from the SD-WAN Gateway will shift to the secondary Zscaler IPsec tunnel. Since the Redundant Velocloud Cloud VPN checkbox is not selected, there are no redundant SD-WAN Gateway connections to Zscaler. If the SD-WAN Gateway fails, then traffic to Zscaler will be dropped.

**Example 4: Primary Zscaler tunnel to 1.1.1.1 , Secondary Zscaler tunnel to 2.2.2.2 with Redundant Velocloud VPN Selected**

Network Services / Zscaler1

Zscaler1

Type: Zscaler

**General**

Name \* Zscaler1

Type \* Zscaler

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

**VPN Gateways**

**Primary VPN Gateway**

Public IP \* 1.1.1  
Example 54.183.9.192

Zscaler Primary IP Address

**Secondary VPN Gateway**

Public IP \* 2.2.2  
Example 54.183.9.192

- REMOVE Zscaler Secondary IP Address

**Advanced Settings**

Tunnel settings

PSK

Redundant Tunnel PSK

Redundant VMware Cloud VPN  
Checked = Gateway Redundancy

**Authentication**

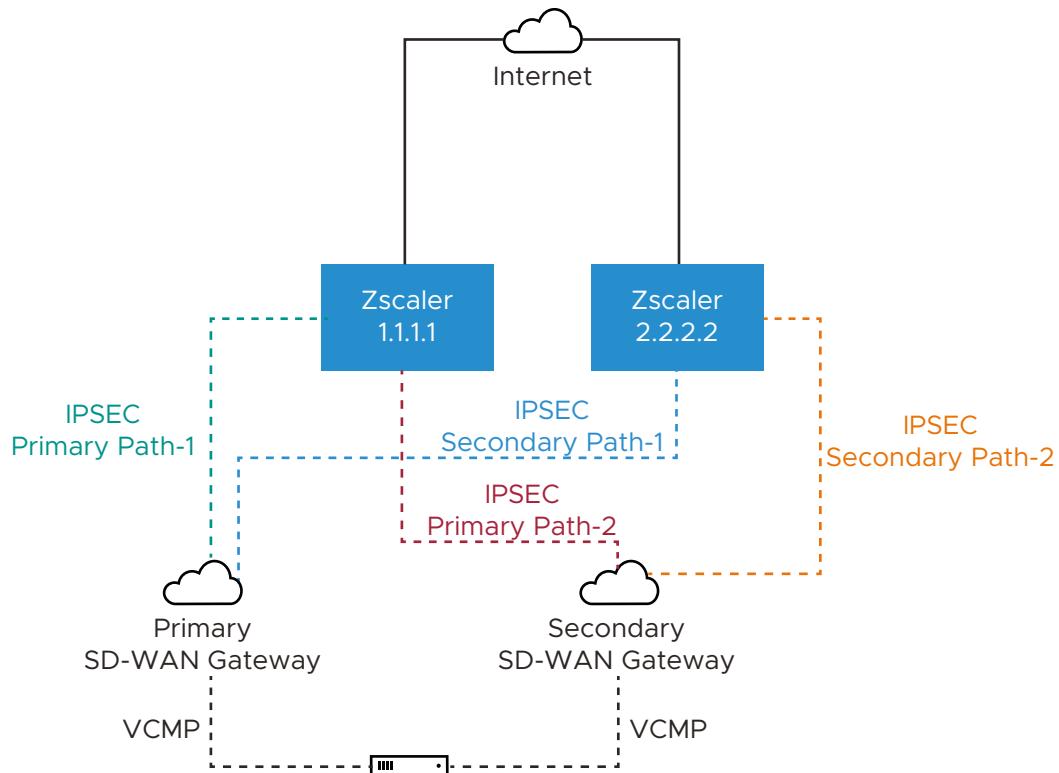
Local Auth Id  IPv4

10.0.1.1  
Example 10.0.2.5

**Sample IKE / IPsec**

**Location**

DISCARD CHANGES  SAVE CHANGES



In this example, redundant IPsec tunnels to Zscaler are configured in the SASE Orchestrator by adding a secondary Zscaler IP address and Redundant Velocloud Cloud VPN checkbox is selected. Two SD-WAN Gateways selected based on the proximity to the remote VPN Gateway (as determined via Geo-IP lookup), will create IPsec tunnels to both Zscaler VPN endpoints. All of these tunnels are active, but by configuration settings the SD-WAN Gateways knows which of the two is the primary SD-WAN Gateway and which is secondary. The SD-WAN Gateways also know which of their IPsec tunnels to Zscaler is the primary path and which is the secondary path. Zscaler does not mark primary or backup IPsec tunnels. Zscaler will simply return traffic via the SD-WAN Gateway that originated the request. Should the primary Zscaler location go down, traffic from the primary SD-WAN Gateway will shift to the secondary Zscaler IPsec tunnel. Since the Redundant Velocloud Cloud VPN checkbox is selected, if the primary SD-WAN Gateway fails traffic will shift to the secondary SD-WAN Gateway. The secondary SD-WAN Gateway will utilize the primary IPsec tunnel provided that path is available. If not, it will use the secondary IPsec tunnel to reach Zscaler.

## Layer 7 Health Checks

When you establish an IPsec/GRE tunnel to a given Zscaler datacenter for Zscaler Internet Access (ZIA), the tunnel is established between the SD-WAN Edge or SD-WAN Gateway, to a virtual IP (VIP) on a Zscaler load balancer for ZIA. When the end user traffic from the branch reaches the load balancer, the load balancer distributes traffic to ZIA Public Service Edges. Dead Peer Detection (DPD) and GRE keepalives can only detect the availability to the public VIP on the load balancer (since it is the tunnel destination). The public VIP is a highly available endpoint and does not reflect the availability of a given ZIA Public Service Edge. Layer 7 health checking allows you to monitor performance and availability of ZIA Edges based on HTTP probes and allows you to failover to an alternate tunnel based on the results. The SD-WAN Edge or SD-WAN Gateway sends probe requests periodically to the HTTP probe URL (in the following format) if probe is activated.

`http://gateway.<zscaler_cloud>.net/vpntest`

The probe URL is configurable in the SASE Orchestrator, but the probe interval and number of retries are currently not editable in the SASE Orchestrator. If the probe fails consecutively for the number of retries defined, the tunnel is marked down, and the traffic will failover to the secondary tunnel if defined. The probe failure could be either because the https response (200 OK) is not received, or the latency is greater than the defined threshold. If conditional backhaul is configured in an Edge, probe failures to both primary and secondary tunnel will trigger traffic failover to the backhaul hub configured. When the probe is UP again, traffic will fall back to the CSS tunnel. If Redundant Cloud VPN is configured for Non SD-WAN Destination (NSD) via Gateway, probe failures to both primary and secondary tunnel from primary gateway will trigger traffic failover to secondary gateway. When the probe in the primary gateway is UP again, traffic will fall back to the CSS tunnel on the primary gateway.

## Zscaler and VMware SD-WAN Deployment Configurations

Describes the configuration steps for integrating Zscaler Internet Access (ZIA) and VMware SD-WAN:

- 1 Configure Zscaler
- 2 Configure a Non SD-WAN Destination of Type Zscaler
- 3 Associate a Non SD-WAN Destination to a Configuration Profile
- 4 Configure Business Priority Rules

For more information, see <https://www.zscaler.com/resources/solution-briefs/partner-vmware-sdwan-deployment-guide.pdf>. This guide will provide GUI examples for configuring Zscaler Internet Access and VMware SASE Orchestrator.

## Layer 7 health check Events

Event	Displayed on Orchestrator UI as	Severity	Notification Configurable	Generated By	Generated When
EDGE_NVS_TUNNEL_UP	Edge Direct IPsec tunnel up	INFO	N	SASE Orchestrator	A Cloud Security Service tunnel or NSD via Edge tunnel is up.
EDGE_NVS_TUNNEL_DOWN	Edge Direct IPsec tunnel down	INFO	N	SASE Orchestrator	A Cloud Security Service tunnel or NSD via Edge tunnel is down.
VPN_DATACENTER_STATUS	VPN Tunnel state change	NOTICE	N	SD-WAN Gateway	The VPN Tunnel state is changed.

For information about events related to cloud security services, see [Monitor Cloud Security Services Events](#).

## Configure a Non SD-WAN Destination of Type Zscaler

To create and configure a Non SD-WAN Destination of type Zscaler, perform the following steps:

- 1 From the navigation panel in the SASE Orchestrator, go to **Configure > Network Services**. The **Services** screen appears.
- 2 In the **Non SD-WAN Destinations via Gateway** area, click the **+New** button. The **New Non SD-WAN Destinations via Gateway** dialog box appears.

## Non SD-WAN Destinations via Gateway

Name *	<input type="text" value="velo NSD via GW1"/>
Type *	<input type="text" value="Zscaler"/>
VPN Gateways	
Primary VPN Gateway *	<input type="text" value="10.10.10.1"/> Example 54.183.9.192
Secondary VPN Gateway	<input type="text" value="Enter Name"/> Example 54.183.9.192

- 3 In the **Name** text box, enter the name for the Non SD-WAN Destination.
- 4 From the **Type** drop-down menu, select **Zscaler**.
- 5 Enter the IP address for the Primary VPN Gateway (and the Secondary VPN Gateway if necessary) and click **Next**. A Non SD-WAN Destination of type Zscaler is created and a dialog box for your Non SD-WAN Destination appears.

## Non SD-WAN Destinations via Gateway

**Name \*** TEST68**Type \*** Zscaler**Tunnel Mode** Active/Hot-Standby

## VPN Gateways

**VPN Gateway 1  
(Primary)\*** 55.184.10.118

Example 54.183.9.192

[CANCEL](#)[CREATE](#)

Network Services / TEST68 Type: Zscaler ^

## TEST68

**General**

Name \* TEST68

Type \* Zscaler

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

⚠ If Tunnel Mode is Active/Hot-Standby, up to 2 tunnel endpoints/Gateways can be configured.

Authentication

Local Auth Id  User FQDN

test@ab.com Example user@some.domain.com

Location

Location  Lat, Lng: 37.402889, -122.116859  EDIT

**VPN Gateways**

Redundant VMware Cloud VPN

VPN Gateway 1  + Add New Gateway

VPN Gateway 1 (Primary)

Public IP\* 55.184.10.118 Example 54.183.9.192

**Advanced Settings (VPN Gateway 1 - Primary)**

Tunnel settings

PSK

**Sample IKE / IPSec**

**Zscaler Settings**

Zscaler Login URL URL for logging into Zscaler. Ex: zscaler.com

L7 Health Check  Activate

- To configure tunnel settings for the Non SD-WAN Destination's Primary VPN Gateway, click the **Advanced Settings** expand button.

- 7 In the **Primary VPN Gateway** area, under **Tunnel Settings**, you can configure the Pre-Shared Key (PSK), which is the security key for authentication across the tunnel. The Orchestrator generates a PSK by default. If you want to use your own PSK or password, then you can enter it in the textbox.

**Note** Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.

---

- 8 If you want to create a Secondary VPN Gateway for this site, then click the **+Add** button next to **VPN Gateway 1**. In the pop-up window, enter the IP address of the VPN Gateway 2 and click **Save Changes**. The **VPN Gateway 2** will be created immediately for this site and will provision a VMware VPN tunnel to this Gateway.
- 9 Select the **Redundant VMware Cloud VPN** checkbox to add redundant tunnels for each VPN Gateway. Any changes made to PSK of Primary VPN Gateway will also be applied to the redundant VPN tunnels, if configured. After modifying the tunnel settings of the VPN Gateway 1, save the changes and then click **Sample IKE/IPSec** to view the updated tunnel configuration.
- 10 Under the **Location** area, click the **Edit** link to update the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.
- 11 Local authentication ID defines the format and identification of the local gateway. From the **Local Auth Id** drop-down menu, choose from the following types and enter a value that you determine:
  - **FQDN** - The Fully Qualified Domain Name or hostname. For example, google.com.
  - **User FQDN** - The User Fully Qualified Domain Name in the form of email address. For example, user@google.com.
  - **IPv4** - The IPv4 address used to communicate with the local gateway.
  - **IPv6** - The IPv6 address used to communicate with the local gateway.

**Note** For Zscaler Non SD-WAN Destination, it is recommended to use FQDN or User FQDN as the local authentication ID.

---

- 12 When the Zscaler Cloud Security Service is selected as the Service type, to determine and monitor the health of Zscaler Server, you can configure additional settings such as Zscaler Cloud and Layer 7 (L7) Health check.
  - a Select the **L7 Health Check** checkbox to enable L7 Health check for the Zscaler Cloud Security Service provider, with default probe details (HTTP Probe interval = 5 seconds, Number of Retries = 3, RTT Threshold = 3000 milliseconds). By default, L7 Health Check is deactivated.

**Note** Configuration of health check probe details is not supported.

---

- b From the **Zscaler Cloud** drop-down menu, select a Zscaler cloud service or enter the Zscaler cloud service name in the textbox.
- 13 To login to Zscaler portal from here, enter the login URL in the **Zscaler Login URL** textbox and then click **Login to Zscaler**. This will redirect you to the Zscaler Admin portal of the selected Zscaler cloud. The **Login to Zscaler** button will be enabled if you have entered the Zscaler login URL.
- For more information, see [Configure a Cloud Security Service](#).
- 14 Check the **Enable Tunnel(s)** checkbox once you are ready to initiate the tunnel from the SD-WAN Gateway to the Zscaler VPN gateways.
- 15 Click **Save Changes**.

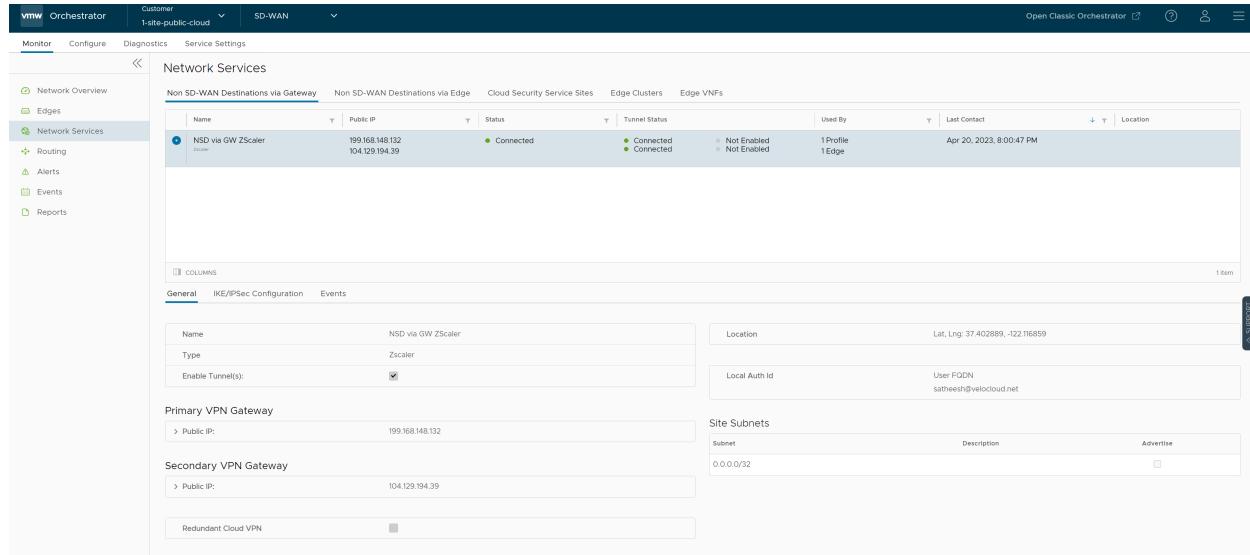
---

**Note** A Zscaler tunnel is established with IPsec Encryption Algorithm as *NULL* and Authentication Algorithm as *SHA-256* irrespective of whether Customer Export Restriction is activated or deactivated.

---

The configured network service appears under the **Non SD-WAN Destinations via Gateway** area in the **Network Services** window. You can associate the network service to a Profile. For more information, see [Associate a Non SD-WAN Destination to a Configuration Profile](#).

You can view the L7 health status along with the L7 health check RTT from **Monitor > Network Services > Non SD-WAN Destinations via Gateway > Service Status**.



The screenshot shows the VMware Orchestrator web interface. The top navigation bar includes 'Customer 1-site-public-cloud' and 'SD-WAN'. The left sidebar has sections for 'Network Overview', 'Edges', 'Network Services' (which is selected), 'Routing', 'Alerts', 'Events', and 'Reports'. The main content area is titled 'Network Services' and shows a table for 'Non SD-WAN Destinations via Gateway'. One entry is listed: 'NSD via GW Zscaler' with Public IP 199.168.148.132 and 104.129.194.39, Status 'Connected', Tunnel Status 'Connected', Used By '1 Profile 1 Edge', and Last Contact 'Apr 20, 2023, 8:00:47 PM'. Below the table are tabs for 'General', 'IKE/IPSec Configuration', and 'Events'. Under 'General', there are fields for 'Name' (NSD via GW Zscaler), 'Type' (Zscaler), 'Enable Tunnel(s)' (checkbox checked), 'Primary VPN Gateway' (Public IP 199.168.148.132), 'Secondary VPN Gateway' (Public IP 104.129.194.39), and 'Redundant Cloud VPN' (checkbox). Under 'Events', there is a section for 'Site Subnets' with a table showing 'Subnet' (0.0.0.0/32), 'Description' (User FQDN satheesh@velocloud.net), and 'Advertise' (checkbox). The bottom right corner of the interface has a 'Support' link.

### Associate a Non SD-WAN Destination to a Configuration Profile

After configuring a Non SD-WAN Destination of type **Zscaler** in SASE Orchestrator, you have to associate the Non SD-WAN Destination to the desired Profile in order to establish the tunnels between SD-WAN Gateways and Zscaler VPN Gateways. To associate a Non SD-WAN Destination to a configuration profile, perform the following steps:

- 1 Login to the SASE Orchestrator as an Enterprise user.

- 2 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Configuration Profiles** page appears.
- 3 Select a profile you want to associate your Non SD-WAN Destination of type **Zscaler** and click the **View** link under the **Device** column. The **Device Settings** page for the selected profile appears.
- 4 Under **VPN Services** category, navigate to **Cloud VPN > Edge to Non SD-WAN Sites**, select the **Enable Edge to Non SD-WAN via Gateway** checkbox.

The screenshot shows the VMware SD-WAN Configuration Profiles interface. The top navigation bar includes Monitor, Configure (selected), Diagnostics, and Service Settings. The left sidebar lists Edge Configuration (Edges, Profiles, Object Groups, Segments), Overlay Flow Control, Network Services, and Cloud Hub. The main content area shows a 'Quick Start Profile' (Used by 1 Edges) with a 'Segment: GLOBAL SEGMENT' dropdown. Under 'VPN Services', the 'Cloud VPN' section has its toggle switch set to 'On'. The 'Edge to Non SD-WAN Sites' section contains a checkbox labeled 'Enable Edge to Non SD-WAN via Gateway' which is checked. Below this are buttons for '+ ADD', '+ NEW DESTINATION', and 'DELETE'. A list of destinations shows one item: 'NSD via GW Zscaler'. A note at the bottom right indicates '1 item'.

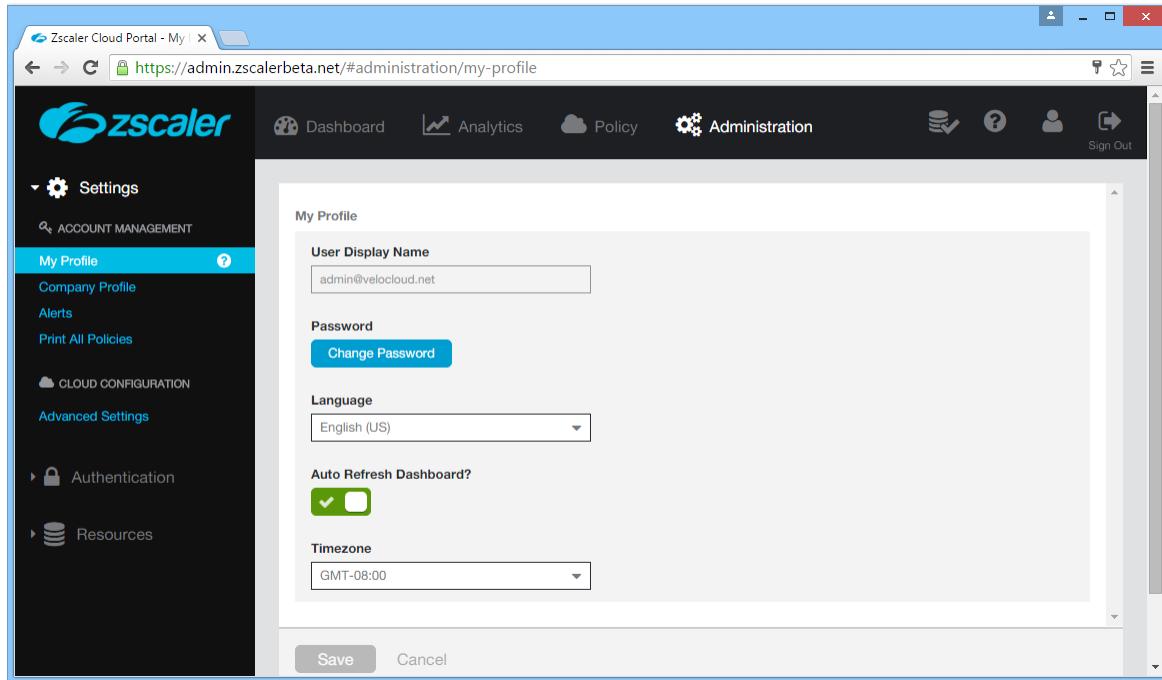
- 5 From the drop-down menu, select your Non SD-WAN Destination of type **Zscaler** to establish VPN connection between the branch and the Zscaler Non SD-WAN Destination.
- 6 Click **Save Changes**.

## Configure Zscaler

This section describes Zscaler configuration.

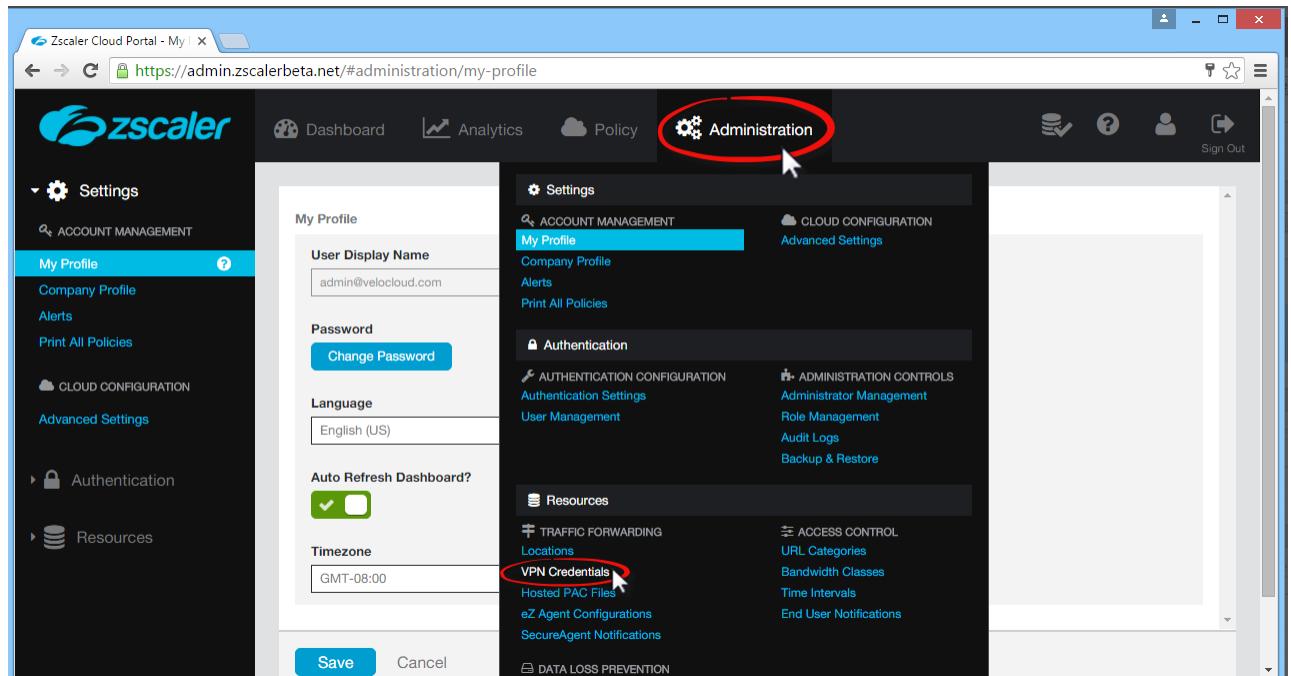
Complete the following these steps on the Zscaler website. From there, you will create a Zscaler account, add VPN credentials, and add a location.

- 1 From the Zscaler website, create a Zscaler web security account.

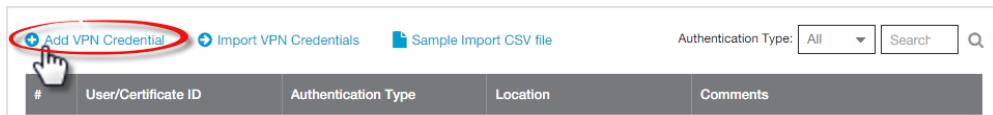


2 Set up your VPN Credentials:

- At the top of the Zscaler screen, hover over the **Administration** option to display the drop down menu. (See image below).
- Under **Resources**, click **VPN Credentials**.



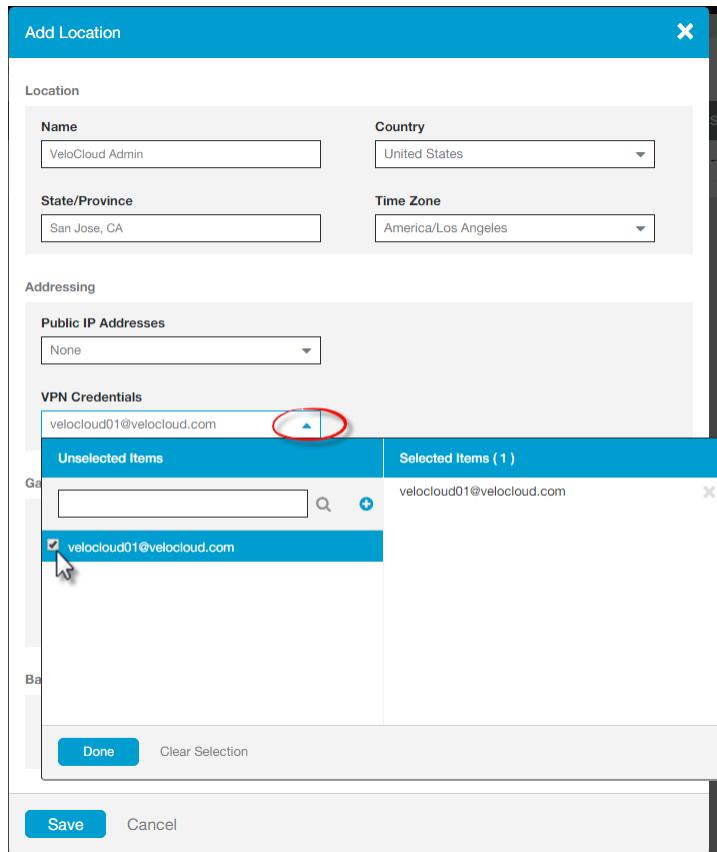
- Click **Add VPN Credentials** at the top left corner.



- d From the **Add VPN Credential** dialog box:
  - 1 Choose **FQDN** as the Authentication Type.
  - 2 Type the User ID and Pre-Shared Key (PSK). You obtained this information from your Non SD-WAN Destination's dialog box in the SASE Orchestrator.
  - 3 If necessary, type in any comments in the **Comments** section.

The 'Add VPN Credential' dialog box is shown. The 'Authentication Type' section has a radio button for 'FQDN' which is selected and highlighted with a red circle. The 'User ID' field contains 'velocloud01' and the '@' dropdown shows 'velocloud.com'. The 'New Pre-Shared Key' and 'Confirm New Pre-Shared Key' fields both contain a series of asterisks. In the 'Comments' section, there is a text area containing the text: 'The PSK and User ID FQDN was obtained from the VeloCloud portal when the Non-VeloCloud Site was created.' This entire comments section is also circled with a red oval. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

- 4 Click **Save**.
- 3 Assign a location:
  - a At the top of the Zscaler screen, hover over the **Administration** option to display the drop-down menu.
  - b Under **Resources**, click **Locations**.
  - c Click **Add Location** at the top left corner.
  - d In the **Add Location** dialog box (see image below):
    - 1 Complete the text boxes in the Location area (Name, Country, State/Province, Time Zone).
    - 2 Choose **None** from the **Public IP Addresses** drop-down menu.
    - 3 In the **VPN Credentials** drop-down menu, select the credential you just created. (See image below).
    - 4 Click **Done**.
    - 5 Click **Save**.



## Configure Business Priority Rules

Define the business policy in your SASE Orchestrator to determine web security screening. The business policy matches parameters such as IP addresses, ports, VLAN IDs, interfaces, domain names, protocols, operating system, object groups, applications, and DSCP tags. When a data packet matches the match conditions, the associated action or actions are taken. If a packet matches no parameters, then a default action is taken on the packet.

You can configure Business Policy rules using the **Business Policy** tab in the Profile Configuration page. Optionally, you can also override the Profile Business Policy rules at the Edge-level. To create a business policy at the Edge level:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge, and then click the **Business Policy** tab. Alternatively, you can click the **View** link in the **Business Policy** column of the Edge. The **Configure Business Policy** page appears.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'vmw Orchestrator', 'Customer 5-site', 'SD-WAN', and various icons for help, user, and settings. The main menu has tabs for 'Monitor', 'Configure' (which is selected), 'Diagnostics', and 'Service Settings'. On the left, a sidebar titled 'Edge Configuration' lists 'Edges', 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control', and 'Network Services'. The main content area is titled 'Edges / b1-edge1' and shows 'b1-edge1' is connected to 'SD-WAN'. A dropdown for 'Segment' is set to 'GLOBAL SEGMENT'. Below this, there are tabs for 'Device', 'Business Policy' (selected), 'Firewall', and 'Overview'. A 'Business Policy Rules' section contains a table with columns: Rule Name, IP Version, Match, Action, Network Service, Link, Priority, and Service Class. A note says 'There are no business profiles found.' Below this is a 'Rules From Profile' section with a similar table, listing rules like 'Object group policy1', 'Box', 'Speedtest', 'Skype', etc., with their respective details.

- 3 The business policy rules and other settings inherited from the associated Profile are displayed under the **Rules From Profile** section of the **Configure Business Policy** page. You can edit the existing rules or add new rules for the selected Edge, by selecting the **Override** check box. The new and overridden rules appear in the **Edge Overrides** section.
- 4 To create a new business policy rule, under **Business Policy Rules**, click **+ADD**. The **Add Rule** dialog box appears.

Add Rule

Rule Name \* zscaler Biz rule1

IP Version \*  IPv4  IPv6  IPv4 and IPv6

**Match** **Action**

Priority  High  Normal  Low

Enable Rate Limit

Network Service Internet Backhaul > Non SD-WAN Destination via Gateway

Non SD-WAN Destination via Gateway \* NSD via GW ZScaler

Link Steering Auto

Inner Packet DSCP Tag Leave as is

Outer Packet DSCP Tag 0 - CS0/DF

Enable NAT

Service Class  Realtime  Transactional  Bulk

CANCEL CREATE

- a Enter the Rule Name and select the IP version. You can configure the Source and Destination IP addresses according to the selected IP version.
- b Under the **Match** area, configure the match criteria for Source, Destination, and Application traffic.
- c In the **Action** area, configure the actions for the rule.

**Note** VMware recommends configuring a business policy rules to Backhaul web traffic, using Port 80 and 443. You can send all Internet traffic to Backhaul Zscaler.

- d After configuring the required settings, click **Create**.

For more information, see [Create Business Policy Rule](#).

## Configure a Non SD-WAN Destination of Type Generic IKEv1 Router (Route Based VPN)

Follow the below steps to configure a Non SD-WAN Destination of type **Generic IKEv1 Router (Route Based VPN)** in the SASE Orchestrator.

**Procedure**

- Once you have created a Non SD-WAN Destination configuration of the type **Generic IKEv1 Router (Route Based VPN)**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST63
Type *	Generic IKEv1 Router (Route Based VPN) <span style="float: right;">▼</span>
Tunnel Mode	Active/Hot-Standby <span style="float: right;">▼</span>
VPN Gateways <span style="color: blue; font-size: small;">(i)</span>	
VPN Gateway 1 (Primary)*	55.184.10.193 <span style="float: right;">(−) <span style="color: blue; border: 1px solid #ccc; border-radius: 50%; padding: 2px;">+</span></span>
<span style="border: 1px solid #ccc; padding: 5px; margin-right: 20px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 5px; border-radius: 5px;">CREATE</span>	

Network Services / TEST63 Type: Generic IKEv1 Router (Route Based VPN)

## TEST63

**General**

Name \* TEST63

Type \* Generic IKEv1 Router (i)

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

If Tunnel Mode is Active/Hot-Standby, up to 2 tunnel endpoints/Gateways can be configured.

Authentication

Local Auth Id Default

Location

Location Lat, Lng: 37.402889, -122.116859 [EDIT](#)

**VPN Gateways**

VPN Gateway 1 + Add New Gateway  Redundant VMware Cloud VPN

VPN Gateway 1 (Primary)

Public IP\* 55.184.10.193 Example 54.183.9.192

**Advanced Settings (VPN Gateway 1 - Primary)**

Tunnel settings

PSK

Encryption AES-128

DH Group 2

PFS 2

**Sample IKE / IPSec**

This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device. [COPY](#)

```
==== VPN Gateway 1 config =====
==== IKE Security Association ====
Authentication Method: Pre-Shared Key
Primary tunnel Pre-Shared Key: 23400d8691a29860b6d0efc05179efd8cdcae1629
Authentication Algorithm: SHA1
Encryption Algorithm: AES-128-CBC
Lifetime: 86,400 seconds
Authentication Time: 172,800 seconds
Phase 1 Negotiation Mode: main

==== IPSec Security Association ====
Protocol: ESP
Authentication Algorithm: SHA_1
Encryption Algorithm: AES-128-CBC
Lifetime: 28,800 seconds
Mode: tunnel
```

**Site Subnets**

+ ADD

Subnet	Description	Advertise
<input type="checkbox"/> Enter IPv4 Subnet	Enter Description (optional)	<input checked="" type="checkbox"/>

1 item

**2** You can configure the following tunnel settings:

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>Generic IKEv1 Router (Route Based VPN)</b> . You cannot edit this option.
Enable Tunnel(s)	Click the toggle button to initiate the tunnel(s) from the SD-WAN Gateway to the Generic IKEv1 Router VPN Gateway.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways. <b>Active/Active</b> mode supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.
<b>ECMP</b> Load Sharing Method	<b>Flow Load Based</b> (Default) Flow load based algorithm maps the new flow to the path with least number of flows mapped among the available paths to the destination. <b>Hash Load Based</b> algorithm takes input parameters from 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol). These inputs can be any or all or any subset of this tuple based on user configuration. Flow is mapped to the path based on hash value with selected inputs.
VPN Gateway 1	Enter a valid IP address.
VPN Gateway 2	Enter a valid IP address. This field is optional.
VPN Gateway 3	Enter a valid IP address. This field is optional.
VPN Gateway 4	Enter a valid IP address. This field is optional.
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.
	<b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .

Option	Description
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> .
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>2</b> .
Redundant VMware Cloud VPN	Select the check box to add redundant tunnels for each VPN Gateway. Changes made to <b>Encryption</b> , <b>DH Group</b> , or <b>PFS</b> of Primary VPN Gateway also apply to the redundant VPN tunnels, if configured.
Secondary VPN Gateway	<p>Click the <b>Add</b> button, and then enter the IP address of the Secondary VPN Gateway. Click <b>Save Changes</b>.</p> <p>The Secondary VPN Gateway is immediately created for this site and provisions a VMware VPN tunnel to this Gateway.</p>
Local Auth Id	<p>Local authentication ID defines the format and identification of the local gateway. From the drop-down menu, choose from the following types and enter a value:</p> <ul style="list-style-type: none"> <li>■ <b>FQDN</b> - The Fully Qualified Domain Name or hostname. For example: vmware.com</li> <li>■ <b>User FQDN</b> - The User Fully Qualified Domain Name in the form of email address. For example: user@vmware.com</li> <li>■ <b>IPv4</b> - The IP address used to communicate with the local gateway.</li> <li>■ <b>IPv6</b> - The IP address used to communicate with the local gateway.</li> </ul>
<b>Note</b>	<ul style="list-style-type: none"> <li>■ If you do not specify a value, <b>Default</b> is used as the local authentication ID.</li> <li>■ The default local authentication ID value is the SD-WAN Gateway Interface Public IP.</li> </ul>
Sample IKE / IPsec	Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).

Option	Description
Location	Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.
Site Subnets	<p>Use the toggle button to activate or deactivate the <b>Site Subnets</b>. Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b>.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</li> <li>■ If there are no site subnets configured, deactivate <b>Site Subnets</b> to activate the tunnel.</li> </ul>

3 Click **Save Changes**.

### Configure a Non SD-WAN Destination of Type Generic Firewall (Policy Based VPN)

Follow the below steps to configure a Non SD-WAN Destination of type **Generic Firewall (Policy Based VPN)** in the SASE Orchestrator.

**Procedure**

- Once you have created a Non SD-WAN Destination configuration of the type **Generic Firewall (Policy Based VPN)**, you are redirected to an additional configuration options page:

Non SD-WAN Destinations via Gateway X

Name *	TEST78
Type *	Generic Firewall (Policy Based VPN) <span style="float: right;">▼</span>
Tunnel Mode	Active/Hot-Standby <span style="float: right;">▼</span>
VPN Gateways <span style="color: #0070C0;">(i)</span>	
VPN Gateway 1 (Primary)*	65.175.10.232 <span style="float: right;">-</span> Example 54.183.9.192
 <div style="border: 1px solid #E6A239; padding: 10px; background-color: #FFFACD;"><span style="color: #E6A239;">⚠</span> Secondary VPN Gateways are not supported for Policy Based VPN. This is a limitation of the Policy Based VPN.</div> 	
<span style="border: 1px solid #0070C0; padding: 5px 10px; color: #0070C0; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 5px 10px; font-weight: bold;">CREATE</span>	

Network Services / TEST78      Type: Generic Firewall (Policy Based VPN)

## TEST78

**General**

Name \* TEST78

Type \* Generic Firewall (Policy Based VPN)

Enable Tunnel(s)

Tunnel Mode Active/Hot-Standby

**Warning:** Secondary VPN Gateways are not supported for Policy Based VPN. This is a limitation of the Policy Based VPN.

**Authentication**

Local Auth Id Default

**Location**

Location Lat, Lng: 37.402889, -122.116859

**VPN Gateways**

**VPN Gateway 1**

VPN Gateway 1 (Primary)

Public IP\* 65.175.10.232  
Example 54.183.9.192

**Advanced Settings (VPN Gateway 1 - Primary)**

Tunnel settings

PSK

Encryption AES-128

DH Group 2

PFS deactivated

**Sample IKE / IPSec**

**Warning:** This sample should not be used without customization. Copy the template and customize it for your environment before running these commands on your device.

```
==== VPN Gateway 1 config =====
==== IKE Security Association ====
Authentication Method: Pre-Shared Key
Primary tunnel Pre-Shared Key: b346b0d924181858eda59c985d2b46bb9f582e42
Authentication Algorithm: sha1
Encryption Algorithm: AES-128-CBC
Lifetime: 28,800 seconds
==== IPSec Security Association ====
Protocol: ESP
Authentication Algorithm: sha1
Encryption Algorithm: AES-128-CBC
Lifetime: 28,800 seconds
Perfect Forward Secrecy (PFS): disabled

==== IPSec Dead Peer Detection (DPD) Setting ====
DPD Type:
```

**Site Subnets**

+ ADD

<input type="checkbox"/>	Subnet	Description	Advertise
<input type="checkbox"/>	Subnet 1	Enter Description (optional)	<input checked="" type="checkbox"/>

1 item

**Custom Site Subnets**

**Note** Secondary VPN Gateway is not supported for the **Generic Firewall (Policy Based VPN)** service type.

- 2 You can configure the following tunnel settings:

Option	Description
General	
Name	You can edit the previously entered name for the Non SD-WAN Destination.
Type	Displays the type as <b>Generic Firewall (Policy Based VPN)</b> . You cannot edit this option.
Enable Tunnel(s)	Click the toggle button to initiate the tunnel(s) from the SD-WAN Gateway to the Generic Firewall VPN Gateway.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways.
VPN Gateway 1	Enter a valid IP address.
Public IP	Displays the IP address of the Primary VPN Gateway.
PSK	The Pre-Shared Key (PSK) is the security key for authentication across the tunnel. The SASE Orchestrator generates a PSK by default. If you want to use your own PSK or password, enter it in the text box.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Encryption	Select either <b>AES-128</b> or <b>AES-256</b> as the AES algorithm key size to encrypt data. The default value is <b>AES-128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down menu. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , and <b>14</b> . The default value is <b>2</b> .
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>deactivated</b> , <b>2</b> , and <b>5</b> . The default value is <b>deactivated</b> .

Option	Description
Local Auth Id	<p>Local authentication ID defines the format and identification of the local gateway. From the drop-down menu, choose from the following types and enter a value:</p> <ul style="list-style-type: none"> <li>■ <b>FQDN</b> - The Fully Qualified Domain Name or hostname. For example: vmware.com</li> <li>■ <b>User FQDN</b> - The User Fully Qualified Domain Name in the form of email address. For example: user@vmware.com</li> <li>■ <b>IPv4</b> - The IP address used to communicate with the local gateway.</li> <li>■ <b>IPv6</b> - The IP address used to communicate with the local gateway.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ If you do not specify a value, <b>Default</b> is used as the local authentication ID.</li> <li>■ The default local authentication ID value is the SD-WAN Gateway Interface Local IP.</li> </ul>
Sample IKE / IPsec	<p>Click to view the information needed to configure the Non SD-WAN Destination Gateway. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).</p> <p><b>Note</b> Currently, the supported IKE version is <b>IKEv1</b>.</p>
Location	<p>Click <b>Edit</b> to set the location for the configured Non SD-WAN Destination. The latitude and longitude details are used to determine the best Edge or Gateway to connect to in the network.</p>
Site Subnets	<p>Use the toggle button to activate or deactivate the <b>Site Subnets</b>. Click <b>Add</b> to add subnets for the Non SD-WAN Destination. If you do not need subnets for the site, select the subnet and click <b>Delete</b>.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.</li> <li>■ If there are no site subnets configured, deactivate <b>Site Subnets</b> to activate the tunnel.</li> </ul>
Custom Site Subnets	<p>Use this section to override the source subnets routed to this VPN device. Normally, source subnets are derived from the Edge LAN subnets routed to this device.</p>

### 3 Click **Save Changes**.

## Configure Non SD-WAN Destinations via Edge

VMware allows the Enterprise users to define and configure a Non SD-WAN Destination instance in order to establish a secure IPSec v4 and v6 tunnels directly from an SD-WAN Edge to a Non SD-WAN Destination. This section also allows you to configure Cloud Security Services.

## Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Non SD-WAN Destinations**, expand **Non SD-WAN Destinations via Edge**.

Non SD-WAN Destinations via Edge

+ NEW    DELETE

<input type="checkbox"/>	Name	Type	Used By
There are no Non SD-WAN Destinations via Edges			

+ NEW NSD VIA EDGE

COLUMNS    0 items

- In the **Non SD-WAN Destinations via Edge** area, click **New** or **New NSD via Edge** option to create a new Non SD-WAN Destination.

**Note** The **New NSD via Edge** option appears only when there are no items in the table.

- Following configuration options are available:

**Note** To support the datacenter type of Non SD-WAN Destination, besides the IKE/IPSec settings, you must configure Non SD-WAN Destination local subnets into the VMware system.

Non SD-WAN Destinations via Edge

X

General    IKE/IPSec Settings    Site Subnets

Service Name *	NSD1
Service Type *	Generic IKEv2 Router (Route Based VPN)
Tunnel mode	Active/Active

CANCEL    SAVE

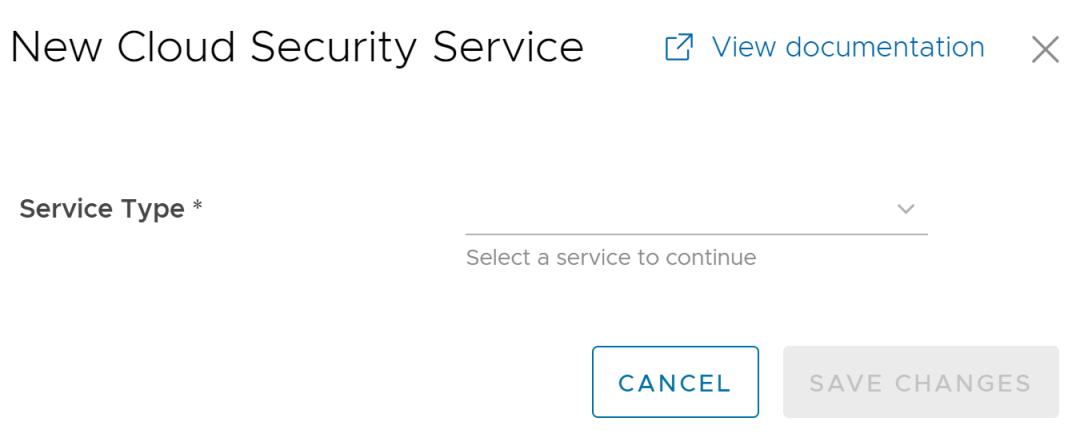
Option	Description
<b>General</b>	
Service Name	Enter a name for the Non SD-WAN Destination. This field is mandatory.
Service Type	Select the service type from the drop-down menu. The available options are <b>Generic IKEv1 Router (Route Based VPN)</b> , <b>Generic IKEv2 Router (Route Based VPN)</b> , and <b>Microsoft Azure Virtual Wan</b> . This field is mandatory.

Option	Description
Tunnel mode	Select a tunnel mode from the drop-down menu. The available options are <b>Active/Active</b> , <b>Active/Hot-Standby</b> , and <b>Active/Standby</b> .
<b>IKE/IPSec Settings</b>	
IP Version	Select an IP version (IPv4 or IPv6) of the current Non SD-WAN Destination from the drop-down menu.
Primary VPN Gateway	
Public IP	Enter a valid IPv4 or IPv6 address. This field is mandatory.
View advanced settings for IKE Proposal: Expand this option to view the following fields.	
Encryption	Select the AES algorithm key size from the drop-down list, to encrypt data. The available options are <b>AES 128</b> , <b>AES 256</b> , <b>AES 128 GCM</b> , <b>AES 256 GCM</b> , and <b>Auto</b> . The default value is <b>AES 128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down list. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , <b>14</b> , <b>15</b> , <b>16</b> , <b>19</b> , <b>20</b> , and <b>21</b> . The default value is <b>14</b> .
Hash	<p>Select one of the following supported Secure Hash Algorithm (SHA) functions from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA 256</li> <li>■ SHA 384</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan Service Type</b>.</p> <ul style="list-style-type: none"> <li>■ SHA 512</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan Service Type</b>.</p> <ul style="list-style-type: none"> <li>■ Auto</li> </ul> <p>The default value is <b>SHA 256</b>.</p>
IKE SA Lifetime(min)	<p>Enter the time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is <b>10</b> minutes and maximum is <b>1440</b> minutes. The default value is <b>1440</b> minutes.</p> <p><b>Note</b> Rekeying must be initiated before 75-80 % of lifetime expires.</p>
DPD Timeout(sec)	Enter the DPD timeout value. The DPD timeout value will be added to the internal DPD timer, as described below. Wait for a response from the DPD message before considering the peer to be dead (Dead Peer Detection).

Option	Description
	<p>Prior to the 5.1.0 release, the default value is 20 seconds. For the 5.1.0 release and later, see the list below for the default value.</p> <ul style="list-style-type: none"> <li>■ Library Name: Quicksec</li> <li>■ Probe Interval: Exponential (0.5 sec, 1 sec, 2 sec, 4 sec, 8 sec, 16 sec)</li> <li>■ Default Minimum DPD Interval: 47.5sec (Quicksec waits for 16 seconds after the last retry. Therefore, <math>0.5+1+2+4+8+16+16 = 47.5</math>).</li> <li>■ Default Minimum DPD interval + DPD Timeout(sec): 67.5 sec</li> </ul> <p><b>Note</b> For the 5.1.0 release and later, you cannot deactivate DPD by configuring the DPD timeout timer to 0 seconds. The DPD timeout value in seconds gets added into the default minimum value of 47.5 seconds.</p>
View advanced settings for IPsec Proposal: Expand this option to view the following fields.	
Encryption	<p>Select the AES algorithm key size from the drop-down list, to encrypt data. The available options are <b>None</b>, <b>AES 128</b>, and <b>AES 256</b>. The default value is <b>AES 128</b>.</p>
PFS	<p>Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>2</b>, <b>5</b>, <b>14</b>, <b>15</b>, <b>16</b>, <b>19</b>, <b>20</b>, and <b>21</b>. The default value is <b>14</b>.</p>
Hash	<p>Select one of the following supported Secure Hash Algorithm (SHA) functions from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA 256</li> <li>■ SHA 384</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan Service Type</b>.</p> <ul style="list-style-type: none"> <li>■ SHA 512</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan Service Type</b>.</p> <p>The default value is <b>SHA 256</b>.</p>
IPsec SA Lifetime(min)	<p>Enter the time when Internet Security Protocol (IPsec) rekeying is initiated for Edges. The minimum IPsec lifetime is <b>3</b> minutes and maximum is <b>480</b> minutes. The default value is <b>480</b> minutes.</p> <p><b>Note</b> Rekeying must be initiated before 75-80 % of lifetime expires.</p>
Secondary VPN Gateway	
<b>Add</b> - Click this option to add a secondary VPN Gateway. Following fields are displayed.	

Option	Description
Public IP	Enter a valid IPv4 or IPv6 address.
Remove	Deletes the Secondary VPN Gateway.
Tunnel settings are the same as Primary VPN Gateway	Select this check box if you want to use the same settings for Primary and Secondary Gateways. You can choose to enter the settings for the Secondary VPN Gateway manually.
<b>Site Subnets</b>	
Add	Click this option to add a subnet and a description for the Non SD-WAN Destination.
Delete	Click this option to delete the selected Subnet.

- c Click **Save**.
- 2 In the **Cloud Security Services** area, click **New**.



- 3 In the **New Cloud Security Service** window, select a service type from the drop-down menu. VMware SD-WAN supports the following CSS types:
- Generic Cloud Security Service
  - Symantec / Palo Alto Cloud Security Service

- Zscaler Cloud Security Service
  - a If you have selected either "Generic" or "Symantec / Palo Alto" Cloud Security Service as the **Service Type**, then configure the following fields, and then click **Save Changes**.

Option	Description
Service Name	Enter a descriptive name for the cloud security service.
Primary Point-of-Presence/Server	Enter the IP address or hostname for the Primary server.
Secondary Point-of-Presence/Server	Enter the IP address or hostname for the Secondary server. This field is optional.

- b If you have selected **Zscaler Cloud Security Service** as the **Service Type**, then configure the following fields, and then click **Save Changes**.

Option	Description
Service Name	Enter a descriptive name for the cloud security service.
Automate Cloud Service Deployment	Select the check box to choose automation deployment.
URL for logging in to Zscaler	You can choose to use the existing Zscaler URL from the drop-down list or enter a new URL.
Primary Server	Enter the IP address or hostname for the Primary server.
Secondary Server	Enter the IP address or hostname for the Secondary server. This field is optional.
L7 Health Check	Select the check box to monitor the health of Zscaler Server.  <b>Note</b> For a given Edge/Profile, a user cannot override the L7 Health Check parameters configured in the Network Services.
HTTP Probe Interval	Displays the duration of the interval between individual HTTP probes. The default probe interval is <b>5</b> seconds.
Number of Retries	Select the number of retries allowed before marking the cloud service as DOWN. The default value is <b>3</b> .
RTT Threshold	The Round Trip Time (RTT) threshold, expressed in milliseconds, is used to calculate the cloud service status. The cloud service is marked as DOWN if the measured RTT is above the configured threshold. The default value is <b>3000</b> milliseconds.
Zscaler Login URL	Enter the login URL and then click <b>Login to Zscaler</b> . This will redirect you to the Zscaler Admin portal of the selected Zscaler cloud.

Option	Description
	<b>Note</b> The <a href="#">Login to Zscaler</a> link is activated only if you enter the Zscaler login URL.

**Note** For more information, see [Chapter 11 Cloud Security Services](#).

- 4 Following are the other options available under the **Non SD-WAN Destinations via Edge** section:

Option	Description
Delete	Select an item and click this option to delete it.
Columns	Click and select the columns to be displayed or hidden on the page.

**Note** Click the information icon at the top of the table to view the Conceptual Diagram, and then hover across the diagram for more details.

#### What to do next

- Configure tunnel settings for your Non SD-WAN Destination. For more information, see:
  - [Configure a Non-VMware SD-WAN Site of Type Generic IKEv1 Router via Edge](#)
  - [Configure a Non-VMware SD-WAN Site of Type Generic IKEv2 Router via Edge](#)
- Associate your Non SD-WAN Destination to a Profile or Edge. For more information, see [Configure Tunnel Between Branch and Non SD-WAN Destinations via Edge](#).
- Configure Tunnel parameters (WAN link selection and Per tunnel credentials) at the Edge level. For more information, see [Configure Cloud VPN and Tunnel Parameters for Edges](#).
- Configure Business Policy. Configuring business policy is an optional procedure for Non SD-WAN Destinations via Edge. If there are no Non SD-WAN Destinations configured then you can redirect the Internet traffic via business policy. For more information, see [Create Business Policy Rule](#).

### Configure a Non-VMware SD-WAN Site of Type Generic IKEv1 Router via Edge

This topic describes how to configure a Non SD-WAN Destination of type **Generic IKEv1 Router (Route Based VPN)** through SD-WAN Edge in SASE Orchestrator.

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to [Configure > Network Services](#).  
The **Network Services** screen appears.

- 2 In the **Non SD-WAN Destinations via Edge** area, click the **New** button.

The **Non SD-WAN Destinations via Edge** dialog box appears.

Non SD-WAN Destinations via Edge

General    IKE/IPSec Settings    Site Subnets

Service Name \* NSD

Tunneling Protocol  IPsec  GRE

Service Type \* Generic IKEv1 Router (Route Based VPN)

Tunnel mode Active/Active

**CANCEL** **SAVE**

- 3 In the **Service Name** text box, enter a name for the Non SD-WAN Destination.
- 4 From the **Service Type** drop-down menu, select **Generic IKEv1 Router (Route Based VPN)** as the IPSec tunnel type.
- 5 Click the **IKE/IPSec Settings** tab and configure the following parameters:

Option	Description
IP Version	Select an IP version (IPv4 or IPv6) of the current Non SD-WAN Destination from the drop-down menu.
Primary VPN Gateway	
Public IP	Enter a valid IPv4 or IPv6 address. This field is mandatory.
View advanced settings for IKE Proposal: Expand this option to view the following fields.	
Encryption	Select the AES algorithm key size from the drop-down list, to encrypt data. The available options are <b>AES 128</b> , <b>AES 256</b> , <b>AES 128 GCM</b> , <b>AES 256 GCM</b> , and <b>Auto</b> . The default value is <b>AES 128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down list. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , <b>14</b> , <b>15</b> , <b>16</b> , <b>19</b> , <b>20</b> , and <b>21</b> . The default value is <b>14</b> .

Option	Description
Hash	<p>Select one of the following supported Secure Hash Algorithm (SHA) functions from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA 256</li> <li>■ SHA 384</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p> <ul style="list-style-type: none"> <li>■ SHA 512</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p> <ul style="list-style-type: none"> <li>■ Auto</li> </ul> <p>The default value is <b>SHA 256</b>.</p>
IKE SA Lifetime(min)	<p>Enter the time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is <b>10</b> minutes and maximum is <b>1440</b> minutes. The default value is <b>1440</b> minutes.</p> <p><b>Note</b> Rekeying must be initiated before 75-80 % of lifetime expires.</p>
DPD Timeout(sec)	<p>Enter the DPD timeout value. The DPD timeout value will be added to the internal DPD timer, as described below. Wait for a response from the DPD message before considering the peer to be dead (Dead Peer Detection).</p> <p>Prior to the 5.1.0 release, the default value is 20 seconds. For the 5.1.0 release and later, see the list below for the default value.</p> <ul style="list-style-type: none"> <li>■ Library Name: Quicksec</li> <li>■ Probe Interval: Exponential (0.5 sec, 1 sec, 2 sec, 4 sec, 8 sec, 16 sec)</li> <li>■ Default Minimum DPD Interval: 47.5sec (Quicksec waits for 16 seconds after the last retry. Therefore, <math>0.5+1+2+4+8+16+16 = 47.5</math>).</li> <li>■ Default Minimum DPD interval + DPD Timeout(sec): 67.5 sec</li> </ul> <p><b>Note</b> For the 5.1.0 release and later, you cannot deactivate DPD by configuring the DPD timeout timer to 0 seconds. The DPD timeout value in seconds gets added into the default minimum value of 47.5 seconds.</p>
View advanced settings for IPsec Proposal: Expand this option to view the following fields.	
Encryption	<p>Select the AES algorithm key size from the drop-down list, to encrypt data. The available options are <b>None</b>, <b>AES 128</b>, and <b>AES 256</b>. The default value is <b>AES 128</b>.</p>
PFS	<p>Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>2</b>, <b>5</b>, <b>14</b>, <b>15</b>, <b>16</b>, <b>19</b>, <b>20</b>, and <b>21</b>. The default value is <b>14</b>.</p>

Option	Description
Hash	<p>Select one of the following supported Secure Hash Algorithm (SHA) functions from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA 256</li> <li>■ SHA 384</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p>
	<ul style="list-style-type: none"> <li>■ SHA 512</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p>
	<p>The default value is <b>SHA 256</b>.</p>
IPsec SA Lifetime(min)	<p>Enter the time when Internet Security Protocol (IPsec) rekeying is initiated for Edges. The minimum IPsec lifetime is <b>3</b> minutes and maximum is <b>480</b> minutes. The default value is <b>480</b> minutes.</p> <p><b>Note</b> Rekeying must be initiated before 75-80 % of lifetime expires.</p>
Secondary VPN Gateway	
	<p><b>Add</b> - Click this option to add a secondary VPN Gateway. Following fields are displayed.</p>
Public IP	<p>Enter a valid IPv4 or IPv6 address.</p>
Remove	<p>Deletes the Secondary VPN Gateway.</p>
Keep Tunnel Active	<p>Select this check box to keep the Secondary VPN tunnel active for this site.</p>
Tunnel settings are the same as Primary VPN Gateway	<p>Select this check box if you want to apply the same advanced settings for Primary and Secondary Gateways. You can choose to enter the settings for the Secondary VPN Gateway manually.</p>

**Note** When AWS initiates the rekey tunnel with a VMware SD-WAN Gateway (in Non SD-WAN Destinations), a failure can occur and a tunnel is not established, which can cause traffic interruption. Adhere to the following:

- IPsec SA Lifetime(min) timer configurations for the SD-WAN Gateway must be less than 60 minutes (50 minutes recommended) to match the AWS default IPsec configuration.
- **DH Group** and **PFS** values must match.

The Secondary VPN Gateway is created immediately for this site and provisions a VMware VPN tunnel to this Gateway.

- Click the **Site Subnets** tab and configure the following:

Option	Description
Add	Click this option to add a subnet and a description for the Non SD-WAN Destination.
Delete	Click this option to delete the selected Subnet.

**Note** To support the datacenter type of Non SD-WAN Destination, besides the IPSec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.

- Click **Save**.

#### What to do next

- Configure Tunnel Between Branch and Non SD-WAN Destinations via Edge
- Configure Cloud VPN and Tunnel Parameters for Edges

### Configure a Non-VMware SD-WAN Site of Type Generic IKEv2 Router via Edge

This topic describes how to configure a Non SD-WAN Destination of type **Generic IKEv2 Router (Route Based VPN)** through SD-WAN Edge in SASE Orchestrator.

#### Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**.
- In the **Non SD-WAN Destinations via Edge** area, click the **New** button.

The **Non SD-WAN Destinations via Edge** dialog box appears.

General		IKE/IPSec Settings	Site Subnets
Service Name *	test1234		
Tunneling Protocol	<input checked="" type="radio"/> IPsec <input type="radio"/> GRE		
Service Type *	Generic IKEv1 Router (Route Based VPN)		
Tunnel mode	Active/Active		
<input type="button" value="CANCEL"/> <input type="button" value="SAVE"/>			

- In the **Service Name** text box, enter a name for the Non SD-WAN Destination.
- From the **Service Type** drop-down menu, select **Generic IKEv2 Router (Route Based VPN)** as the IPSec tunnel type.

5 Click the **IKE/IPSec Settings** tab and configure the following parameters:

Option	Description
IP Version	Select an IP version (IPv4 or IPv6) of the current Non SD-WAN Destination from the drop-down menu.
Primary VPN Gateway	
Public IP	Enter a valid IPv4 or IPv6 address. This field is mandatory.
View advanced settings for IKE Proposal: Expand this option to view the following fields.	
Encryption	Select the AES algorithm key size from the drop-down list, to encrypt data. The available options are <b>AES 128</b> , <b>AES 256</b> , <b>AES 128 GCM</b> , <b>AES 256 GCM</b> , and <b>Auto</b> . The default value is <b>AES 128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down list. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , <b>14</b> , <b>15</b> , <b>16</b> , <b>19</b> , <b>20</b> , and <b>21</b> . The default value is <b>14</b> .
Hash	<p>Select one of the following supported Secure Hash Algorithm (SHA) functions from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA 256</li> <li>■ SHA 384</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan Service Type</b>.</p> <ul style="list-style-type: none"> <li>■ SHA 512</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan Service Type</b>.</p> <ul style="list-style-type: none"> <li>■ Auto</li> </ul> <p>The default value is <b>SHA 256</b>.</p>
IKE SA Lifetime(min)	<p>Enter the time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is <b>10</b> minutes and maximum is <b>1440</b> minutes. The default value is <b>1440</b> minutes.</p>
	<p><b>Note</b> Rekeying must be initiated before 75-80 % of lifetime expires.</p>

Option	Description
DPD Timeout(sec)	<p>Enter the DPD timeout value. The DPD timeout value will be added to the internal DPD timer, as described below. Wait for a response from the DPD message before considering the peer to be dead (Dead Peer Detection).</p> <p>Prior to the 5.1.0 release, the default value is 20 seconds. For the 5.1.0 release and later, see the list below for the default value.</p> <ul style="list-style-type: none"> <li>■ Library Name: Quicksec</li> <li>■ Probe Interval: Exponential (0.5 sec, 1 sec, 2 sec, 4 sec, 8 sec, 16 sec)</li> <li>■ Default Minimum DPD Interval: 47.5sec (Quicksec waits for 16 seconds after the last retry. Therefore, <math>0.5+1+2+4+8+16+16 = 47.5</math>).</li> <li>■ Default Minimum DPD interval + DPD Timeout(sec): 67.5 sec</li> </ul> <p><b>Note</b> For the 5.1.0 release and later, you cannot deactivate DPD by configuring the DPD timeout timer to 0 seconds. The DPD timeout value in seconds gets added into the default minimum value of 47.5 seconds.</p>
View advanced settings for IPsec Proposal: Expand this option to view the following fields.	
Encryption	<p>Select the AES algorithm key size from the drop-down list, to encrypt data. The available options are <b>None</b>, <b>AES 128</b>, and <b>AES 256</b>. The default value is <b>AES 128</b>.</p>
PFS	<p>Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>2</b>, <b>5</b>, <b>14</b>, <b>15</b>, <b>16</b>, <b>19</b>, <b>20</b>, and <b>21</b>. The default value is <b>14</b>.</p>
Hash	<p>Select one of the following supported Secure Hash Algorithm (SHA) functions from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA 256</li> <li>■ SHA 384</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p> <ul style="list-style-type: none"> <li>■ SHA 512</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p> <p>The default value is <b>SHA 256</b>.</p>
IPsec SA Lifetime(min)	<p>Enter the time when Internet Security Protocol (IPsec) rekeying is initiated for Edges. The minimum IPsec lifetime is <b>3</b> minutes and maximum is <b>480</b> minutes. The default value is <b>480</b> minutes.</p> <p><b>Note</b> Rekeying must be initiated before 75-80 % of lifetime expires.</p>

Option	Description
Secondary VPN Gateway	
<b>Add</b> - Click this option to add a secondary VPN Gateway. Following fields are displayed.	
Public IP	Enter a valid IPv4 or IPv6 address.
Remove	Deletes the Secondary VPN Gateway.
Keep Tunnel Active	Select this check box to keep the Secondary VPN tunnel active for this site.
Tunnel settings are the same as Primary VPN Gateway	Select this check box if you want to apply the same advanced settings for Primary and Secondary Gateways. You can choose to enter the settings for the Secondary VPN Gateway manually.

**Note** When AWS initiates the rekey tunnel with a VMware SD-WAN Gateway (in Non SD-WAN Destinations), a failure can occur and a tunnel will not be established, which can cause traffic interruption. Adhere to the following:

- IPsec SA Lifetime(min) timer configurations for the SD-WAN Gateway must be less than 60 minutes (50 minutes recommended) to match the AWS default IPsec configuration.
  - DH and PFS DH groups must be matched.
- 6 The Secondary VPN Gateway is created immediately for this site and provisions a VMware VPN tunnel to this Gateway.
- 7 Click the **Site Subnets** tab and configure the following:

Option	Description
Add	Click this option to add a subnet and a description for the Non SD-WAN Destination.
Delete	Click this option to delete the selected Subnet.

**Note** To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.

- 8 Click **Save**.

#### What to do next

- Configure Tunnel Between Branch and Non SD-WAN Destinations via Edge
- Configure Cloud VPN and Tunnel Parameters for Edges

## Configure a Non-VMware SD-WAN Site of Type Microsoft Azure via Edge

This topic describes how to configure a Non SD-WAN Destination of type **Microsoft Azure Virtual Hub** via Edge in SASE Orchestrator.

To configure a Non SD-WAN Destination of type **Microsoft Azure Virtual Hub** via Edge in SASE Orchestrator:

### Prerequisites

- Ensure you have configured a Cloud subscription. For steps, see [Configure API Credentials](#).
- Ensure you have created Virtual WAN and Hubs in Azure. For steps, see [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#).

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Non SD-WAN Destinations**, expand **Non SD-WAN Destinations via Edge**.
- 2 In the **Non SD-WAN Destinations via Edge** area, click the **New** button.

The **New Non SD-WAN Destinations via Edge** dialog box appears.

## Non SD-WAN Destinations via Edge

General	IKE/IPSec Settings	Site Subnets
<b>Service Name *</b>	test12	
<b>Tunneling Protocol</b>	<input checked="" type="radio"/> IPsec <input type="radio"/> GRE	
<b>Service Type *</b>	Microsoft Azure Virtual Wan	
<b>Tunnel mode</b>	Active/Active	
<b>Virtual Hub Configuration</b>		
<b>Subscription *</b>	<div style="display: flex; align-items: center;"> <div style="flex-grow: 1;"></div> <div style="font-size: 2em; color: red;">!</div> </div>	

- 3 Enter the **Service Name** and **Service Type** of the Non SD-WAN Destination. Once you enter the **Service Type** as **Microsoft Azure Virtual Hub**, **Virtual Hub Configuration** section is displayed.

- 4 From the **Subscription** drop-down menu, select a cloud subscription. The application fetches all the available Virtual WANs dynamically from Azure.
- 5 From the **Virtual WAN** drop-down menu, select a virtual WAN. The application auto-populates the resource group to which the virtual WAN is associated.
- 6 From the **Virtual Hub** drop-down menu, select a Virtual Hub. The application auto-populates the Azure region corresponding to the Hub
- 7 Click the **IKE/IPSec Settings** tab and configure the following parameters:

Option	Description
IP Version	Select an IP version (IPv4 or IPv6) of the current Non SD-WAN Destination from the drop-down menu.
Primary VPN Gateway	
Public IP	Enter a valid IPv4 or IPv6 address. This field is mandatory.
View advanced settings for IKE Proposal: Expand this option to view the following fields.	
Encryption	Select the AES algorithm key size from the drop-down list, to encrypt data. The available options are <b>AES 128</b> , <b>AES 256</b> , <b>AES 128 GCM</b> , <b>AES 256 GCM</b> , and <b>Auto</b> . The default value is <b>AES 128</b> .
DH Group	Select the Diffie-Hellman (DH) Group algorithm from the drop-down list. This is used for generating keying material. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are <b>2</b> , <b>5</b> , <b>14</b> , <b>15</b> , <b>16</b> , <b>19</b> , <b>20</b> , and <b>21</b> . The default value is <b>14</b> .
Hash	Select one of the following supported Secure Hash Algorithm (SHA) functions from the drop-down list: <ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA 256</li> <li>■ SHA 384</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p> <ul style="list-style-type: none"> <li>■ SHA 512</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p> <ul style="list-style-type: none"> <li>■ Auto</li> </ul> <p>The default value is <b>SHA 256</b>.</p>
IKE SA Lifetime(min)	Enter the time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is <b>10</b> minutes and maximum is <b>1440</b> minutes. The default value is <b>1440</b> minutes.
	<b>Note</b> Rekeying must be initiated before 75-80 % of lifetime expires.

Option	Description
DPD Timeout(sec)	<p>Enter the DPD timeout value. The DPD timeout value will be added to the internal DPD timer, as described below. Wait for a response from the DPD message before considering the peer to be dead (Dead Peer Detection).</p> <p>Prior to the 5.1.0 release, the default value is 20 seconds. For the 5.1.0 release and later, see the list below for the default value.</p> <ul style="list-style-type: none"> <li>■ Library Name: Quicksec</li> <li>■ Probe Interval: Exponential (0.5 sec, 1 sec, 2 sec, 4 sec, 8 sec, 16 sec)</li> <li>■ Default Minimum DPD Interval: 47.5sec (Quicksec waits for 16 seconds after the last retry. Therefore, <math>0.5+1+2+4+8+16+16 = 47.5</math>).</li> <li>■ Default Minimum DPD interval + DPD Timeout(sec): 67.5 sec</li> </ul> <p><b>Note</b> For the 5.1.0 release and later, you cannot deactivate DPD by configuring the DPD timeout timer to 0 seconds. The DPD timeout value in seconds gets added into the default minimum value of 47.5 seconds.</p>
View advanced settings for IPsec Proposal: Expand this option to view the following fields.	
Encryption	<p>Select the AES algorithm key size from the drop-down list, to encrypt data. The available options are <b>None</b>, <b>AES 128</b>, and <b>AES 256</b>. The default value is <b>AES 128</b>.</p>
PFS	<p>Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are <b>2</b>, <b>5</b>, <b>14</b>, <b>15</b>, <b>16</b>, <b>19</b>, <b>20</b>, and <b>21</b>. The default value is <b>14</b>.</p>
Hash	<p>Select one of the following supported Secure Hash Algorithm (SHA) functions from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ SHA 1</li> <li>■ SHA 256</li> <li>■ SHA 384</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p> <ul style="list-style-type: none"> <li>■ SHA 512</li> </ul> <p><b>Note</b> This value is not available for the <b>Microsoft Azure Virtual Wan</b> Service Type.</p> <p>The default value is <b>SHA 256</b>.</p>
IPsec SA Lifetime(min)	<p>Enter the time when Internet Security Protocol (IPsec) rekeying is initiated for Edges. The minimum IPsec lifetime is <b>3</b> minutes and maximum is <b>480</b> minutes. The default value is <b>480</b> minutes.</p> <p><b>Note</b> Rekeying must be initiated before 75-80 % of lifetime expires.</p>

Option	Description
Secondary VPN Gateway	
<b>Add</b> - Click this option to add a secondary VPN Gateway. Following fields are displayed.	
Public IP	Enter a valid IPv4 or IPv6 address.
Remove	Deletes the Secondary VPN Gateway.
Keep Tunnel Active	Select this check box to keep the Secondary VPN tunnel active for this site.
Tunnel settings are the same as Primary VPN Gateway	Select this check box if you want to apply the same advanced settings for Primary and Secondary Gateways. You can choose to enter the settings for the Secondary VPN Gateway manually.

**Note** Non SD-WAN Destination via Edge of type Microsoft Azure Virtual WAN automation supports only IKEv2 protocol with Azure Default IPsec policies (except GCM mode), when SD-WAN Edge act as an Initiator and Azure act as a Responder during an IPsec tunnel setup.

- 8 The Secondary VPN Gateway is created immediately for this site and provisions a VMware VPN tunnel to this Gateway.
- 9 Click the **Site Subnets** tab and configure the following:

Option	Description
Add	Click this option to add a subnet and a description for the Non SD-WAN Destination.
Delete	Click this option to delete the selected Subnet.

**Note** To support the datacenter type of Non SD-WAN Destination, besides the IPsec connection, you must configure Non SD-WAN Destination local subnets into the VMware system.

- 10 Click **Save**.

The Microsoft Azure Non SD-WAN Destination is created and a dialog box for your Non SD-WAN Destination appears.

#### What to do next

- [Configure Cloud VPN for Profiles](#)
- [Associate the Microsoft Azure Non SD-WAN Destination to an Edge and configure tunnels to establish a tunnel between a branch and Azure Virtual Hub. For more information, see \[Associate a Microsoft Azure Non SD-WAN Destination to an SD-WAN Edge and Add Tunnels\]\(#\).](#)

For information about Azure Virtual WAN Edge Automation, see [Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Edge](#).

## Configure Tunnel Between Branch and Non SD-WAN Destinations via Edge

After configuring a Non SD-WAN Destination via Edge in SASE Orchestrator, you have to associate the Non SD-WAN Destination to the desired Profile in order to establish the tunnels between SD-WAN Gateways and the Non SD-WAN Destination.

To establish a VPN connection between a branch and a Non SD-WAN Destination configured via Edge, perform the following steps:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.
- 2 Click the link to the Profile or click the link under the **Device** column of the selected Profile. The **Device Settings** page for the selected profile appears.
- 3 Go to the **VPN Services** area and activate the **Cloud VPN** by turning on the toggle button.
- 4 To establish a VPN connection directly from a SD-WAN Edge to a Non SD-WAN Destination (VPN gateway of Cloud provider such as Azure, AWS), under **Non SD-WAN Destination via Edge**, select the **Enable Non SD-WAN via Edge** check box.

Service		Link					
<input type="checkbox"/>	Name	Automation for all public WAN Links	Enable Service	Enable Tunnel	Destination Primary Public IP	Destination Secondary Public IP	Action
<input type="checkbox"/>	test123	N/A	<input checked="" type="checkbox"/> Enabled		No sites added		

1 item

- 5 From the list of configured Services, select a Non SD-WAN Destination to establish VPN connection. Click **Add** to add additional Non SD-WAN Destinations.

---

**Note** Only one Non SD-WAN Destinations via Edge service is allowed to be activated in at most one segment. Two segments cannot have the same Non SD-WAN Destinations via Edge service activated.

- 6 To deactivate a particular service, deselect the respective **Enable Service** check box.
- 7 Click **Save Changes**.

---

**Note** Before associating a Non SD-WAN Destination to a Profile, ensure that the Gateway for the Enterprise Data Center is already configured by the Enterprise Data Center Administrator and the Data Center VPN Tunnel is activated.

## Configure API Credentials

This section allows you to configure both, IaaS and Cloud Subscriptions. IaaS Subscription refers to Microsoft Azure Subscription and Cloud Subscription refers to Zscaler Subscription.

## Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then expand **API Credentials** to display the **IaaS Subscriptions** and **Cloud Subscriptions** sections.
- 2 In the **IaaS Subscriptions** area, click **+New** or **Configure IaaS Subscriptions**. The **+Create IaaS Subscription** dialog appears.

**Note** The **+Configure IaaS Subscriptions** option appears only when there are no items in the table.

Create IaaS Subscription X

Subscription Type *	Microsoft Azure Subscription
Active Directory Tenant ID *	test
Client ID *	12334
Client Secret *	.....  <span style="font-size: small;">@</span>

**GET SUBSCRIPTIONS**

CANCEL SAVE CHANGES

- 3 The following configuration options are available:

Option	Description
Subscription Type	Displays <b>Microsoft Azure Subscription</b> by default. This field cannot be edited.
Active Directory Tenant ID	Enter a valid Tenant ID.
Client ID	Enter the Client ID.
Client Secret	Enter a password corresponding to your SASE Orchestrator Application Registration.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Get Subscriptions	Click this button to retrieve the list of Azure Subscriptions.

- 4 Click **Save Changes**.

- 5 To configure Zscaler Cloud subscriptions, go to the **Cloud Subscriptions** area, and then click **+New** or **+Configure Cloud Subscriptions**. The **Create Cloud Subscription** dialog appears.

**Note** The **+Configure Cloud Subscriptions** option appears only when there are no items in the table.

The screenshot shows the 'Create Cloud Subscription' dialog. At the top left is the title 'Create Cloud Subscription' and a close button 'X'. Below the title is a dropdown menu labeled 'Subscription Type \*' with 'Zscaler Subscription' selected. The main form area contains the following fields:

- Subscription Name \***: test123
- Zscaler Cloud \***: zscaler.net
- Partner Admin Username \***: abc
- Partner Admin Password \***: ..... (with an eye icon)
- API Key \***: ..... (with an eye icon)
- Domain \***: abc123

At the bottom left is a blue 'VALIDATE SUBSCRIPTION' button. At the bottom right are three buttons: 'CANCEL' (blue outline), 'SAVE CHANGES' (grey background), and another 'SAVE CHANGES' button (light grey background).

- 6 The following configuration options are available:

Option	Description
Subscription Type	Displays <b>Zscaler Subscription</b> by default. This field cannot be edited.
Subscription Name	Enter a name for the Cloud subscription.
Zscaler Cloud	From the drop-down menu, select a value from the following list: <ul style="list-style-type: none"> <li>■ newCloud</li> <li>■ zscaler.net</li> <li>■ zscalerone.net</li> <li>■ zscalertwo.net</li> <li>■ zscalerthree.net</li> <li>■ zscalerbeta.net</li> <li>■ zscloud.net</li> </ul>
Partner Admin Username	Enter the Partner Admin username.

Option	Description
Partner Admin Password	Enter the Partner Admin password.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
API Key	Enter the API Key. Minimum length must be 12 alphanumeric characters.
Domain	Enter a valid domain name.
Validate Subscription	Click this button to validate the cloud subscription details.

- 7 Click **Save Changes**.
- 8 The following are the other options available in the **IaaS Subscriptions** and **Cloud Subscriptions** areas:

Option	Description
Delete	Select an item and click this option to delete it.
Columns	Click and select the columns to be displayed or hidden on the page.

## Configure Clusters and Hubs

This section allows you to configure Edge Clusters. You can also view the existing Cloud VPN Hubs.

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **SD-WAN Destinations**, expand **Clusters and Hubs**.

**SD-WAN Destinations**

Clusters and Hubs (1)

Edge Clusters (1)

[+ NEW](#) [DELETE](#)

<input type="checkbox"/>	Name	Location	Used in Profiles
There are no Edge Clusters			
<a href="#">+ NEW CLUSTER</a>			
<a href="#">COLUMNS</a>		0 items	

Cloud VPN Hubs

SD-WAN Orchestrator does not allow you to configure Cloud VPN Hubs from the Network Services screen, but it provides a summary of all configured SD-WAN Edges. Go to Profiles to add Cloud VPN Hubs.

Hub	Type	Used in Profiles	Segment	VPN Hub <span style="color: #ccc;">(1)</span>	Backhaul Hub <span style="color: #ccc;">(1)</span>
No Cloud VPN Hubs					
<a href="#">COLUMNS</a>		0 items			

- 2 In the **Edge Clusters** area, click **New** or **New Cluster**.

---

**Note** The **New Cluster** option appears only when there are no items in the table.

---

## Edge Cluster

**Name \*** test123

**Description**

**Auto ReBalance**

### Edges in Cluster

Search

<input type="checkbox"/>	Available Edges
<input type="checkbox"/>	Su-Edg3
<input type="checkbox"/>	Su-Edge1
<input type="checkbox"/>	virtual-edge
<input type="checkbox"/>	virtual-edge-2
<input type="checkbox"/>	zsu-test

1 - 5 of 5 items

Show only selected

**IPv4** **IPv6**

### Route Summarization

ADD DELETE

<input type="checkbox"/>	Subnets	Segment	Cost
<input type="checkbox"/>	100.34.21.0/24	Global Segment	4

1 item

- 3 Following configuration options are available:

Option	Description
Name	Enter the name of the Edge Cluster.
Description	Enter the description for the Edge Cluster. This field is optional.
Auto ReBalance	Select the check box if required.  <b>Note</b> If this check box is selected, when an individual Edge in a Hub Cluster exceeds a Cluster Score of 70, Spoke Edges rebalance at the rate of one Spoke Edge per minute until the Cluster Score is reduced to below 70. When a Spoke Edge is reassigned to a different Hub, the Spoke Edge's VPN tunnels are disconnected and there may be up to 6-10 seconds of downtime. If all of the Hubs in a Cluster exceed a 70 Cluster Score, no rebalancing is performed. For more information, see <a href="#">How Edge Clustering Works</a> .
Edges in Cluster	Displays the available Edges. Select the required Edges to be moved in the Edge Cluster. For more information, see <a href="#">About Edge Clustering</a> .
Show only selected	Use this toggle button to display only the selected Edges.
Route Summarization	You can configure Route Summarization for both, <b>IPv4</b> and <b>IPv6</b> . Click <b>Add</b> , and then configure <b>Subnets</b> , <b>Segment</b> , and <b>Cost</b> . For more information, see <a href="#">Chapter 34 Route Summarization</a> .

- 4 Click **Save Changes**.

- 5 Following are the other options available in the **Edge Clusters** area:

Option	Description
Delete	Select an item and click this option to delete it.
Columns	Click and select the columns to be displayed or hidden on the page.

**Note** Click the information icon at the top of the **Edge Clusters** table to view the Conceptual Diagram.

- 6 The **Cloud VPN Hubs** area displays all the configured VMware SD-WAN Edges.

Cloud VPN Hubs

SD-WAN Orchestrator does not allow you to configure Cloud VPN Hubs from the Network Services screen, but it provides a summary of all configured SD-WAN Edges. Go to Profiles to add Cloud VPN Hubs.

Hub	Type	Used in Profiles	Segment	VPN Hub ⓘ	Backhaul Hub ⓘ
No Cloud VPN Hubs					
0 items					

- 7 To add a new Cloud VPN Hub, go to **Configure > Profiles > Device tab > VPN Services > Cloud VPN**. For more information, see [Configure Cloud VPN for Profiles](#).

For information on Hub or Cluster Interconnect, see [Hub or Cluster Interconnect](#).

## About Edge Clustering

The size of a single VMware VPN Network with a VMware SD-WAN Hub is constrained by the scale of the individual Hub. For large networks containing thousands of remote sites, it would be preferable for both scalability and risk mitigation to use multiple Hubs to handle the Edges. However, it is impractical to mandate that the customer manage individual separate Hubs to achieve this. Clustering allows multiple Hubs to be leveraged while providing the simplicity of managing those Hubs as one common entity with built-in resiliency.

SD-WAN Edge Clustering addresses the issue of SD-WAN Hub scale because it can be used to easily expand the tunnel capacity of the Hub dynamically by creating a logical cluster of Edges. Edge Clustering also provides resiliency via the Active/Active High Availability (HA) topology that a cluster of SD-WAN Edge would provide. A cluster is functionally treated as an individual Hub from the perspective of other Edges.

The Hubs in a VMware Cluster can be either physical or Virtual Edges. If they are virtual, they may exist on a single hypervisor or across multiple hypervisors.

Each Edge in a cluster periodically reports usage and load stats to the SD-WAN Gateway. The load value is calculated based on Edge CPU and memory utilization along with the number of tunnels connected to the Hub as a percentage of the Edge model's tunnel capacity. The Hubs within the cluster do not directly communicate nor exchange state information. Typically, Edge Clusters are deployed as Hubs in data centers.

---

**Note** Theoretically, Edge Clustering could be used to horizontally scale other vectors, such as throughput. However, the current Edge Clustering implementation has been specifically designed and tested to scale at tunnel capacity only.

---

For more information, see:

- [How Edge Clustering Works](#)
- [Configure Clusters and Hubs](#)
- [Troubleshooting Edge Clustering](#)

### How Edge Clustering Works

This section provides an in-depth overview of how the SD-WAN Edge Clustering functionality works.

The following are important concepts that describe the SD-WAN Edge Clustering functionality:

- Edge Clustering can be used on Hubs as follows:
  - To allow greater tunnel capacity for a Hub than an individual Edge serving as a Hub can provide.
  - To distribute the remote Spoke Edges among multiple Hubs and reduce the impact of any incident that may occur.
- Cluster Score is a mathematical calculation of the overall utilization of the system as follows:

The three measured utilization factors are CPU usage, memory usage, and tunnel capacity.

- Each measure of utilization is treated as a percentage out of a maximum of 100%.
- Tunnel capacity is based on the rated capacity for a given hardware model or Virtual Edge configuration.
- All three utilization percentages are averaged to arrive at an integer-based Cluster Score (1-100).
- While throughput is not directly considered, CPU and memory usage indirectly reflect throughput and flow volume on a given Hub.
- For example, on an Edge 2000:
  - CPU usage = 20%
  - Memory usage = 30%
  - Connected Tunnels = 600 (out of a capacity of 6000) = 10%
  - Cluster Score:  $(20 + 30 + 10)/3 = 20$
- A Cluster Score greater than 70 is considered "over capacity."
- A "logical ID" is a 128-bit UUID that uniquely identifies an element inside the VMware Network.
  - For instance, each Edge is represented by a logical ID and each Cluster is represented by a logical ID.
  - While the user is providing the Edge and Cluster names, the logical IDs are guaranteed to be unique and are used for internal identification of elements.
- By default, the load is evenly distributed among Hubs. Hence, it is necessary that all Edges that are part of a cluster must be of the same model and capacity.

Each cluster member will have its own IP addressing for the WAN and LAN Interfaces. All the VMware SD-WAN Edges in the hub cluster are required to run a dynamic routing protocol, like eBGP, with the Layer 3 devices on the LAN side with a unique Autonomous System Number (ASN) for each cluster member. Dynamic routing on the clusters LAN side ensures that traffic from the DC to a particular Spoke site is routed through the appropriate Edge Cluster member.

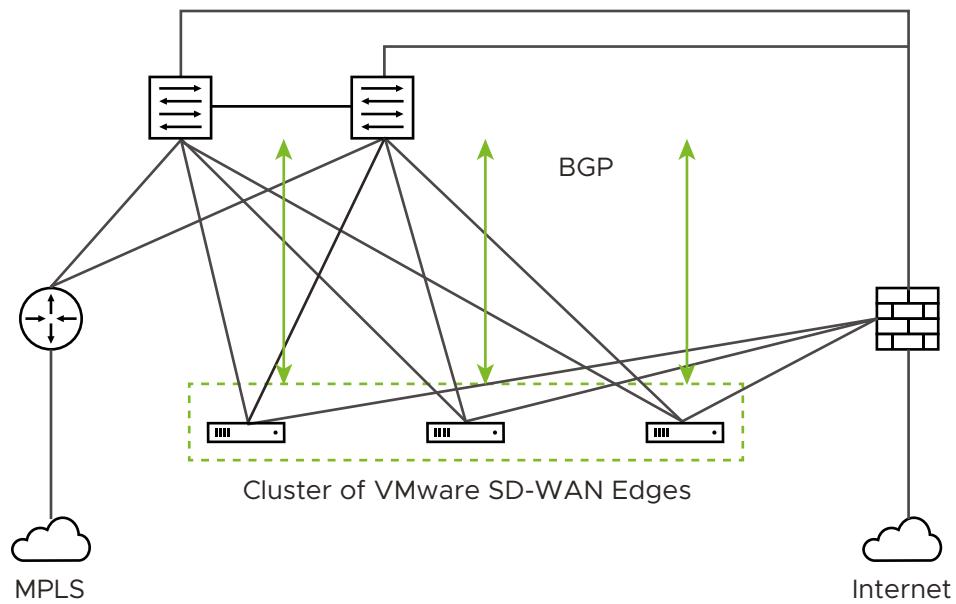
---

**Important** Hub Edges in a cluster do not connect or communicate with each other through tunnels or routing protocols. They act as independent Edges for data plane functions. They depend on the LAN-side BGP peering to the core switch to handle Branch to Branch traffic when the Branch Edges are connected to different Hub Edges in the cluster.

---

### How are Edge Clusters tracked by the VMware SD-WAN Gateway ?

Once a Hub is added to a VMware SD-WAN Cluster, the Hub will tear down and rebuild tunnels to all of its assigned Gateways and indicate to each Gateway that the Hub has been assigned to a Cluster and provide a Cluster logical ID.



For the Cluster, the SD-WAN Gateway tracks:

- The logical ID
- The name
- Whether Auto Rebalance is activated
- A list of Hub objects for members of the Cluster

For each Hub object in the Cluster, the Gateway tracks:

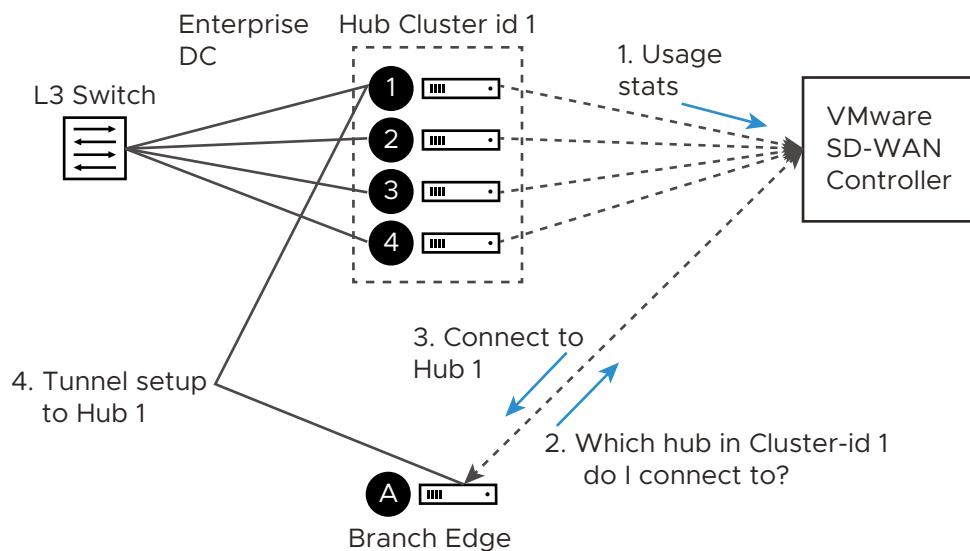
- The logical ID
- The name
- A set of statistics, updated every 30 seconds via a periodic message sent from the Hub to each assigned Gateway, including:
  - Current CPU usage of the Hub
  - Current memory usage of the Hub
  - Current tunnel count on the Hub
  - Current BGP route count on the Hub
- The current computed Cluster Score based on the formula provided above.

A Hub is removed from the list of Hub objects when the Gateway has not received any packets from the Hub Edge for more than seven seconds.

## How are Edges assigned to a specific Hub in a Cluster?

In a traditional Hub and Spoke topology, the SASE Orchestrator provides the Edge with the logical ID of the Hub to which it must be connected. The Edge asks its assigned Gateways for connectivity information for that Hub logical ID—i.e. IP addresses and ports, which the Edge will use to connect to that Hub.

From the Edge's perspective, this behavior is identical when connecting to a Cluster. The Orchestrator informs the Edge that the logical ID of the Hub it should connect to is the Cluster logical ID rather than the individual Hub logical ID. The Edge follows the same procedure of sending a Hub connection request to the Gateways and expects connectivity information in response.



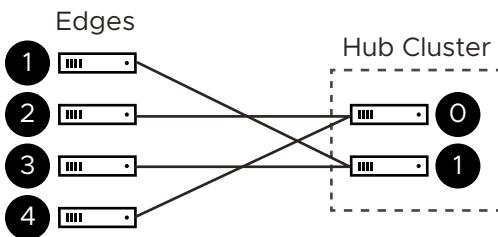
There are two divergences from basic Hub behavior at this point:

- **Divergence Number One:** The Gateway must choose which Hub to assign.
- **Divergence Number Two:** Due to Divergence Number One, the Edge may get different assignments from its different Gateways.

Divergence Number One was originally addressed by using the Cluster Score to assign the least loaded Hub in a Cluster to an Edge. While in practice this is logical, in the real world, it turned out to be a less than ideal solution because a typical reassignment event can involve hundreds or even thousands of Edges and the Cluster Score is only updated every 30 seconds. In other words, if Hub 1 has a Cluster Score of 20 and Hub 2 has a Cluster Score of 21, for 30 seconds all Edges would choose Hub 1, at which point it may be overloaded and trigger further reassessments.

Instead, the Gateway first attempts a fair mathematical distribution disregarding the Cluster Score. The Edge logical IDs, which were generated by a secure random-number generator on the Orchestrator, will (given enough Edges) have an even distribution of values. That means that using the logical ID, a fair share distribution can be calculated.

- Edge logical ID **modulo** the number of Hubs in Cluster = Assigned Hub index
- For example:
  - Four Edges that have logical IDs ending in 1, 2, 3, 4
  - Cluster with 2 Hubs
  - $1 \% 2 = 1$ ,  $2 \% 2 = 0$ ,  $3 \% 2 = 1$ ,  $4 \% 2 = 0$  (Note: "%" is used to indicate the modulo operator)
  - Edges 2 and 4 are assigned Hub Index 0
  - Edges 1 and 3 are assigned Hub Index 1



This is more consistent than a round-robin type assignment because it means that Edges will tend to be assigned the same Hub each time, which makes assignment and troubleshooting more predictive.

---

**Note** When a Hub restarts (e.g. due to maintenance or failure), it will be disconnected from the Gateway and removed from the Cluster. This means that Edges will always be evenly distributed following all Edges restarting (due to the above described logic), but will be unevenly distributed following any Hub event that causes it to lose connectivity.

#### What happens when a Hub exceeds its maximum allowed tunnel capacity?

The Edge assignment logic will attempt to evenly distribute the Edges between all available Hubs. However, after an event (like restart) on the Hub, the Edge distribution will no longer be even.

---

**Note** Generally, the Gateway tries at initial assignment to evenly distribute Edges among Hubs. An uneven distribution is not considered an invalid state. If the assignments are uneven but no individual Hub exceeds 70% tunnel capacity, the assignment is considered valid.

Due to such an event on the Hub (or adding additional Edges to the network), Clusters might reach a point where an individual Hub has exceeded 70% of its permitted tunnel capacity. If this happens, and at least one other Hub is at less than 70% tunnel capacity, then fair share redistribution is performed automatically regardless of whether rebalancing is activated on the

Orchestrator. Most Edges will retain their existing assignment due to the predictive mathematical assignment using logical IDs, and the Edges that have been assigned to other Hubs due to failovers or previous utilization rebalancing will be rebalanced to ensure the Cluster is returned to an even distribution automatically.

### **What happens when a Hub exceeds its maximum allowed Cluster Score?**

Unlike tunnel percentage (a direct measure of capacity), which can be acted upon immediately, the Cluster Score is only updated every 30 seconds and the Gateway cannot automatically calculate what the adjusted Cluster Score will be after making an Edge reassignment. In the Cluster configuration, an Auto Rebalance parameter is provided to indicate whether the Gateway should dynamically attempt to shift the Edge load for each Hub as needed.

If Auto Rebalance is deactivated and a Hub exceeds a 70 Cluster Score (but not 70% tunnel capacity), then no action is taken.

If Auto Rebalance is activated and one or more Hubs exceed a 70 Cluster Score, the Gateway will reassign one Edge per minute to the Hub with the lowest current Cluster Score until all Hubs are below 70 or there are no more reassessments possible.

---

**Note** Auto Rebalance is deactivated by default.

---

### **What happens when two VMware SD-WAN Gateways give different Hub assignments?**

As is the nature of a distributed control plane, each Gateway is making an individual determination of the Cluster assignment. In most cases, Gateways will use the same mathematical formula and thus arrive at the same assignment for all Edges. However, in cases like Cluster Score-based rebalancing this cannot be assured.

If an Edge is not currently connected to a Hub in a Cluster, it will accept the assignment from any Gateway that responds. This ensures that Edges are never left unassigned in a scenario where some Gateways are down and others are up.

If an Edge is connected to a Hub in a Cluster and it gets a message indicating it should choose an alternate Hub, this message is processed in order of “Gateway Preference.” For instance, if the Super Gateway is connected, the Edge will only accept reassessments from the Super Gateway. Conflicting assignments requested by other Gateways will be ignored. Similarly, if the Super Gateway is not connected, the Edge would only accept reassessments from the Alternate Super Gateway. For Partner Gateways (where no Super Gateways exist), the Gateway Preference is based on the order of configured Partner Gateways for that specific Edge.

---

**Note** When using Partner Gateways, the same Gateways must be assigned to both the Hubs in a Cluster and the Spoke Edges, otherwise a scenario may arise where a Spoke Edge is not able to receive Hub assignments because the Spoke Edge is connected to a Gateway that is not also connected to the Hubs in a Cluster.

---

## What happens when a VMware SD-WAN Gateway goes down?

When a SD-WAN Gateway goes down, Edges may be reassigned if the most preferred Gateway was the one that went down, and the next most preferred Gateway provided a different assignment. For instance, the Super Gateway assigned Hub A to this Edge while the Alternate Super Gateway assigned Hub B to the same Edge.

The Super Gateway going down will trigger the Edge to fail over to Hub B, since the Alternate Super Gateway is now the most preferred Gateway for connectivity information.

When the Super Gateway recovers, the Edge will again request a Hub assignment from this Gateway. In order to prevent the Edge switching back to Hub A again in the scenario above, the Hub assignment request includes the currently assigned Hub (if there is one). When the Gateway processes the assignment request, if the Edge is currently assigned a Hub in the Cluster and that Hub has a Cluster Score less than 70, the Gateway updates its local assignment to match the existing assignment without going through its assignment logic. This ensures that the Super Gateway, on recovery, will assign the currently connected Hub and prevent a gratuitous failover for its assigned Edges.

## What happens if a Hub in a Cluster loses its dynamic routes?

As noted above, the Hubs report to the SD-WAN Gateways the number of dynamic routes they have learned via BGP every 30 seconds. If routes are lost for only one Hub in a Cluster, either because they are erroneously retracted or the BGP neighborship fails, the SD-WAN Gateways will failover Spoke Edges to another Hub in the Cluster that has an intact routing table.

As the updates are sent every 30 seconds, the route count is based on the moment in time when the update is sent to the SD-WAN Gateway. The SD-WAN Gateway rebalancing logic occurs every 60 seconds, meaning that users can expect failover to take 30-60 seconds in the unlikely event of total loss of a LAN-side BGP neighbor. To ensure that all Hubs have a chance to update the Gateways again following such an event, rebalancing is limited to a maximum of once per 120 seconds. This means that users can expect failover to take 120 seconds for a second successive failure.

---

**Note** Routes received from BGP over IPsec/GRE are not accounted for LAN side failure detection. When BGP over IPsec/GRE session goes down, the issue is not detected by LAN side failure and therefore this does not trigger cluster failover.

---

## How to configure Routing on Cluster Hubs?

As the Gateway can instruct the spokes to connect to any member Hub of the Cluster, the routing configuration should be mirrored on all the Hubs. For example, if the spokes must reach a BGP prefix 192.168.2.1 behind the Hubs, all the Hubs in the cluster should advertise 192.168.2.1 with the exact same route attributes.

BGP uplink community tags should be used in the cluster deployment. Configure the cluster nodes to set the uplink community tag when redistributing routes to BGP peers.

## What happens if a Hub in a Cluster fails?

The SD-WAN Gateway will wait for tunnels to be declared dead (7 seconds) before failing over Spoke Edges. This means that users can expect failover to take 7-10 seconds (depending on RTT) when an SD-WAN Hub or all its associated WAN links fail.

## Troubleshooting Edge Clustering

This section describes the troubleshooting enhancements for Edge Clustering.

### Overview

Edge Clustering includes a troubleshooting feature to rebalance VMware SD-WAN Spoke Edges within a Cluster. The rebalancing of the Spokes can be performed on any of the Hubs within the Cluster. There are two methods to rebalance Spokes:

- Evenly rebalance Spokes across all the Hubs in the Cluster.
- Exclude one Hub and rebalance the Spokes across the remaining Hubs in the Cluster.

### Rebalancing Spokes on the Hub Using the VMware SASE Orchestrator

An administrator may rebalance Spokes in a Cluster via **Remote Diagnostics** on the VMware SASE Orchestrator. When an SD-WAN Edge is deployed as a Hub in a Cluster, a new Remote Diagnostics option will appear named **Rebalance Hub Cluster**, which offers users two choices.

#### Redistribute Spokes in Hub Cluster

- This option attempts to evenly re-distribute Spoke Edges among all Hub Edges in the Cluster.

#### Redistribute Spokes excluding this Hub

- This option attempts to evenly re-distribute Spokes among Hubs in the Cluster, excluding the Hub Edge from which a user is running the Redistribute Spokes utility.
- This option can be used for troubleshooting or maintenance to remove all Spokes from this Hub Edge.

---

**Note** Rebalancing Spokes causes a brief traffic interruption when the Spoke is moved to a different Hub in the Cluster. Therefore, it is highly recommended to use this troubleshooting mechanism during a maintenance window.

---

**Note** In case of Partner Gateway setups, the "Rebalance Hub Cluster" from Remote Diagnostics would not take effect if the Primary Gateway of the Spoke and the Hub are not common.

For such scenarios, customers are expected to reach out to VMware support for manually rebalancing the Spoke from its Primary Gateway.

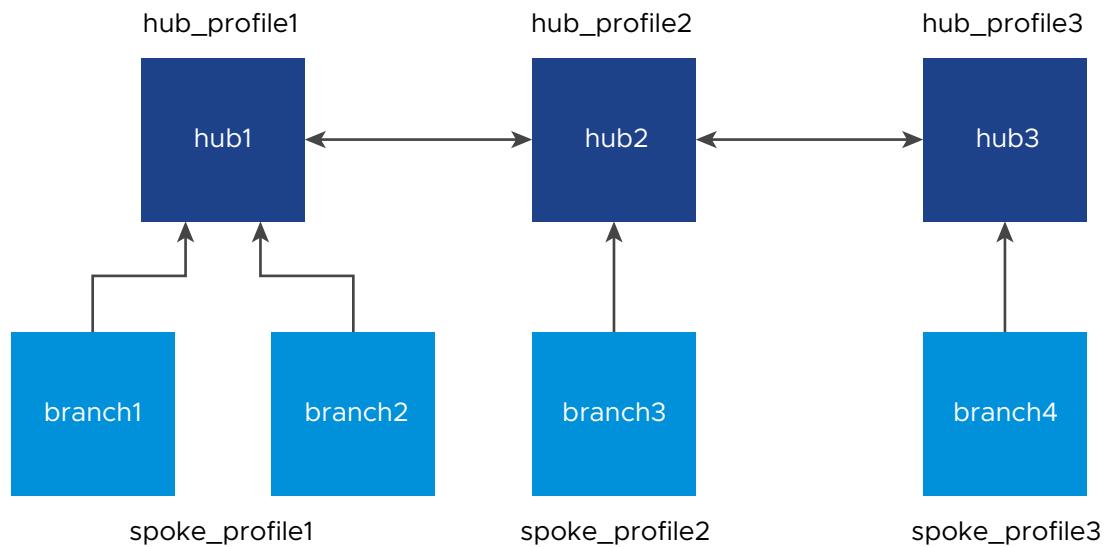
## Hub or Cluster Interconnect

VMware SASE supports interconnection of multiple Hub Edges and/or Hub Clusters to increase the range of Spoke Edges that can communicate with each other. This feature allows communication between the Spoke Edges connected to one Hub Edge/Hub Cluster and the

Spoke Edges connected to another Hub Edge/Hub Cluster, using multiple overlay and underlay connections.

When a Spoke Edge tries to connect to a Hub Cluster, one of the members from the Hub Cluster is selected as the Hub to the Spoke Edge. If this Hub goes down, another member from the same Hub Cluster is automatically selected to serve the Spoke Edge, without any user configuration. The Hub Cluster members are connected to each other via underlay (BGP), and can exchange the routes and data using this underlay connection. Spoke Edges connected to different members of the same Hub Cluster can then communicate with each other using this underlay connection. This solution provides better resiliency.

The Orchestration configuration is shown below:



In this case, for all the three profiles:

- The **Hub or Cluster Interconnect** feature must be activated.
- The **Branch to Hub Site (Permanent VPN)** check box must be selected. The two interconnected Hub nodes must be configured as Hubs to each other as explained in the below table.

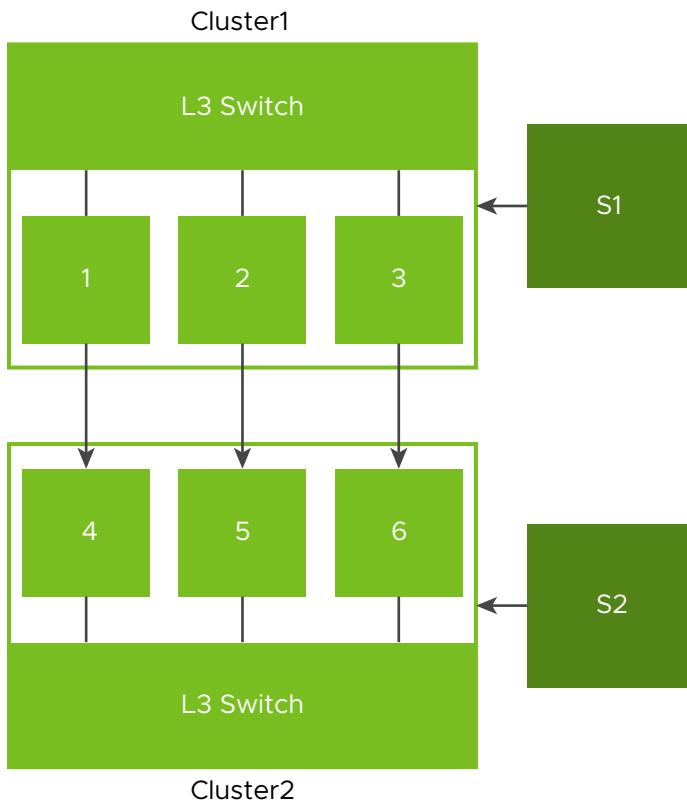
The following table explains the Profile and the corresponding Hubs Designation:

Profile	Hubs Designation
hub_profile1	hub2
hub_profile2	hub1 and hub3
hub_profile3	hub2

**Note** Activating the **Branch to Branch VPN (Transit & Dynamic)** option is not required in Hub Profiles. The branches are a part of Spoke Profile with their corresponding Hub(s) as **Branch to Branch VPN Hubs**.

When **Hub or Cluster Interconnect** feature is activated, tunnels are formed from one Cluster to another Cluster with at least one peer in other Cluster. Based on the condition, two members from one Cluster can form tunnels to same members in another Cluster. In case of individual Hub and Hub Cluster interconnect, all the Cluster members form tunnels to that individual Hub. The end Spoke Edges connected to these Hub Clusters can then communicate with each other through these two Hub Clusters and the intermediate VMware SD-WAN Routing Protocol hops.

The intra Cluster routes are advertised with special BGP extended community, wherein the last four bytes of the Cluster ID are embedded in the extended community. For example, if the Cluster ID is `fee2f589-eab6-4738-88f2-8af84b1a3d9c`, `4b1a3d9c` is reversed and used to derive the Cluster community as `9c3d1a4b00000003`. Based on this community tag, the intra Cluster routes are filtered out towards the controller. This avoids reflecting redundant routes from multiple Cluster members.



In the above example, Cluster 1 (C1) and Cluster 2 (C2) are Hub Clusters, and S1 and S2 are the set of Spoke Edges connected to C1 and C2 respectively. S1 can communicate with S2 through the following connections:

- Overlay connection between S1 and C1.
- Overlay connection between S2 and C2.
- Overlay connection between C1 and C2.
- Underlay connection within C1.
- Underlay connection within C2.

In this way, the Hub Clusters can exchange routes with each other, providing a way for the packets to flow between Spoke Edges connected to different Hub Clusters.

#### **Supported Use Cases:**

- Dynamic branch to branch is supported between Spokes connected to two different or same Clusters.
- Profile isolation in Spoke Profile is supported.
- Internet Backhaul via Cluster is supported.

#### **Limitations:**

When the **Hub or Cluster Interconnect** feature is activated:

- Hub or Cluster Interconnect through Gateway is not supported.
- Exchanging routes between Hub Cluster members using OSPF is not supported.
- Asymmetric routing can occur when two Clusters are interconnected. Enhanced Firewall Services or Stateful Firewall must not be activated as they can block the traffic due to asymmetric routing.
- When all the Overlay tunnels go down between two Cluster members, traffic drop is expected until they form a tunnel with other members in the peer Cluster.
- If there are more than one LAN/WAN routers running BGP with Cluster, **Trusted Source** check box must be selected and the value of **Reverse Path Forwarding** must be **Not enabled**, on the Cluster Edge interfaces connecting BGP routers. For more information, see [Configure Interface Settings for Edges](#).
- Without **Hub or Cluster Interconnect** feature, a Cluster Hub Profile cannot have another Cluster or Hub configured as a Hub.

## Configuring Hub or Cluster Interconnect

### Prerequisites

- Ensure to upgrade the Orchestrator, Gateways, and Hubs or Hub Clusters to version 5.4.0.0 or above.
- The **Cloud VPN** service must be activated for the Cluster Profile associated with the Edge Clusters or Hubs.
- The **Branch to Branch VPN (Transit & Dynamic)** check box must not be selected in interconnect Hub Profiles, as shown below.

**hub\_profile1** Used by 4 Edges

Segment: GLOBAL SEGMENT

VPN Services

- > Gateway Handoff Assignment
- > Controller Assignment
- < Cloud VPN  On ⓘ

To activate this check box, deactivate Hub or Cluster interconnect

Edge to SD-WAN Sites

Branch to Hub Site (Permanent VPN)

Enable Branch to Hubs

EDIT HUBS

Hubs	Hub Order ⓘ
cluster2 <span style="background-color: #009640; color: white; border-radius: 50%; padding: 2px;">Cluster</span>	1

Conditional Backhaul Enabled

Branch to Branch VPN (Transit & Dynamic)

Enable Branch to Branch VPN

Edge to Non SD-WAN Sites

Enable Edge to Non SD-WAN via Gateway

Configuring **Hubs Designation** on interconnect Profiles is sufficient for end to end communication with all nodes. You can configure the Branch to Branch via Hubs for Spoke Profiles.

- **Hub or Cluster Interconnect** feature must be activated in all the Hub Profiles involved in the interconnect process.
- Cluster members must run the BGP with LAN/L3 router, and the router must be configured to forward the BGP extended communities.
- There must be at least one common Gateway for all Edges (Spokes and Hubs) in case of Partner Gateway assignment. The order of Partner Gateways assignment should be same across all the Hub/Cluster Profiles.

---

**Note** Activating **Hub or Cluster Interconnect** feature introduces a fundamental change to the VMware SD-WAN Routing Protocol where it allows packets to traverse more than one hop in the network. Starting from the 5.4.0.0 release, the maximum supported interconnect hops are **4**. In order to connect more than 4 hops, contact VMware Support.

---

## Procedure

### 1 Create new Clusters:

- a In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services > Clusters and Hubs**.
- b Click **New** to create new Clusters. For more information, see [Configure Clusters and Hubs](#).
- c Associate the available Edges to these Clusters.
- d Click **Save Changes**.

### 2 Create a Profile for each of these Clusters:

- a Go to **Configure > Profiles**.
- b Create a separate Profile for each new Cluster. For information on how to create a Profile, see [Create Profile](#).

### 3 Designate Hub to the Cluster Profile:

- a On the **Profile Device Settings** screen, go to **VPN Services** and turn on the **Cloud VPN** service.

- b Select the **Enable Branch to Hubs** check box.
  - c Click **Edit Hubs** located under **Hub Designation**.
  - d Click **Update Hubs**.
- 4 **Activate 'Hub or Cluster Interconnect' feature:** On the **Profile Device Settings** screen, navigate to **Hub or Cluster Interconnect** located under **VPN Services**, and then select the **Enable** check box.

**Note** Hub and Cluster Interconnect configurations can be done only at Profile level.

This activates the feature and creates a tunnel between the Hub Clusters which allows their respective Spoke Edges to communicate with each other.

**Caution** Activating or deactivating the **Hub or Cluster Interconnect** feature causes all Edge devices associated with the Profile to restart. Hence, it is recommended to configure the feature only in a maintenance mode to prevent traffic disruption.

#### What to do next

- **Assign Profiles to the Edges:** Navigate to **Configure > Edges** to assign Profiles to the available Edges.

Edges															
		Q. Search		<input type="button" value="ADD EDGE"/> <input checked="" type="button" value="ASSIGN PROFILE"/> <input checked="" type="button" value="ASSIGN EDGE LICENSE"/> <input type="button" value="DOWNLOAD"/> ...MORE											
	Name	Certificates	Profile	Operator Profile	Analytics	Secrets Encryption	HA	Device	Business Policy	Firewall	Alerts	Operator Alerts			
<input checked="" type="checkbox"/>	b1-edge1 [cluster1]	0	hub_profile1	9-site-cluster-Operator	None		Cluster	View	Edit	Delete	Enabled	Enabled			
<input checked="" type="checkbox"/>	b1-edge2 [cluster1]	0	hub_profile1	9-site-cluster-Operator	None		Cluster	View	Edit	Delete	Enabled	Enabled			
<input checked="" type="checkbox"/>	b1-edge3 [cluster1]	0	Quick Start Profile	9-site-cluster-Operator	None		Cluster	View	Edit	Delete	Enabled	Enabled			
<input checked="" type="checkbox"/>	b1-edge4 [cluster1]	0	Quick Start Profile	9-site-cluster-Operator	None		Cluster	View	Edit	Delete	Enabled	Enabled			
<input type="checkbox"/>	b2-edge1	0	spoke_profile2	9-site-cluster-Operator	None			View	Edit	Delete	Enabled	Enabled			
<input type="checkbox"/>	b3-edge1	0	spoke_profile2	9-site-cluster-Operator	None			View	Edit	Delete	Enabled	Enabled			
<input type="checkbox"/>	b4-edge1	0	spoke_profile1	9-site-cluster-Operator	None			View	Edit	Delete	Enabled	Enabled			
<input type="checkbox"/>	b5-edge1 [cluster2]	0	hub_profile2	9-site-cluster-Operator	None		Cluster	View	Edit	Delete	Enabled	Enabled			
<input type="checkbox"/>	b5-edge2 [cluster2]	0	hub_profile2	9-site-cluster-Operator	None		Cluster	View	Edit	Delete	Enabled	Enabled			
<input type="checkbox"/>	b5-edge3 [cluster2]	0	hub_profile2	9-site-cluster-Operator	None		Cluster	View	Edit	Delete	Enabled	Enabled			

- You can monitor the events by navigating to **Monitor > Events**. The following table lists the new Orchestrator events added for the **Hub or Cluster Interconnect** feature:

Event	Level	Description
CLUSTER_IC_ENABLED	Info	This event is generated whenever an Edge is associated with a Cluster service.
CLUSTER_IC_DISABLED	Info	This event is generated whenever an Edge is disassociated from a Cluster service.
CLUSTER_IC_PEER_UP	Warning	This event is generated whenever the first interconnect tunnel between two Cluster Hub nodes, comes up.
CLUSTER_IC_PEER_DOWN	Warning	This event is generated whenever the last interconnect tunnel between two Cluster Hub nodes, goes down.
CLUSTER_IC_TUNNEL_UP	Warning	This event is generated whenever interconnect tunnels between the Clusters, come up.

Event	Level	Description
CLUSTER_IC_TUNNEL_DOWN	Warning	This event is generated whenever the interconnect tunnels between the Clusters, go down.
HUB_CLUSTER_REBALANCE	Warning	This event is generated whenever a Cluster rebalance action is triggered.

### Note

- 1 After **Hub or Cluster Interconnect** feature is activated, removing or adding a Cluster member under Network Services, triggers service restart on that particular Edge. It is advised to perform such actions during maintenance window.
- 2 When a Spoke is connected to primary and secondary Hub Cluster and learns same route from both of them, the route order is based on BGP attributes. If the routing attributes are same, then route sorting happens based on VPN Hub order configuration. On the other hand, the Spoke's subnets are redistributed by primary and secondary Hub or Hub Cluster to their neighbor with metric (MED) 33 and 34 respectively. You must configure "bgp always-compare-med" in the neighbor router for symmetric routing.
- 3 When Hub or Hub Clusters are connected to MPLS core through CE, you must configure UPLINK tag in those BGP neighbors.
- 4 In a network set up with a spoke, a primary hub, and a secondary hub, initiating a flow from behind the spoke creates a local flow on the spoke that is then routed through the primary hub. If the primary hub goes down, the route of the local flow is updated to the secondary hub. Since the route is checked with each packet for local flows, when the primary hub comes back up, the route is updated accordingly. However, the behavior is different when the flow is a peer flow. In this case, if the primary hub goes down, the peer flow is routed through the secondary hub, but when the primary hub comes back up, the peer route is not updated. This is because the peer flow relies on the peer's updates, which is the expected behavior. The workaround for this is to flush the affected flows.

## Configure Netflow Settings

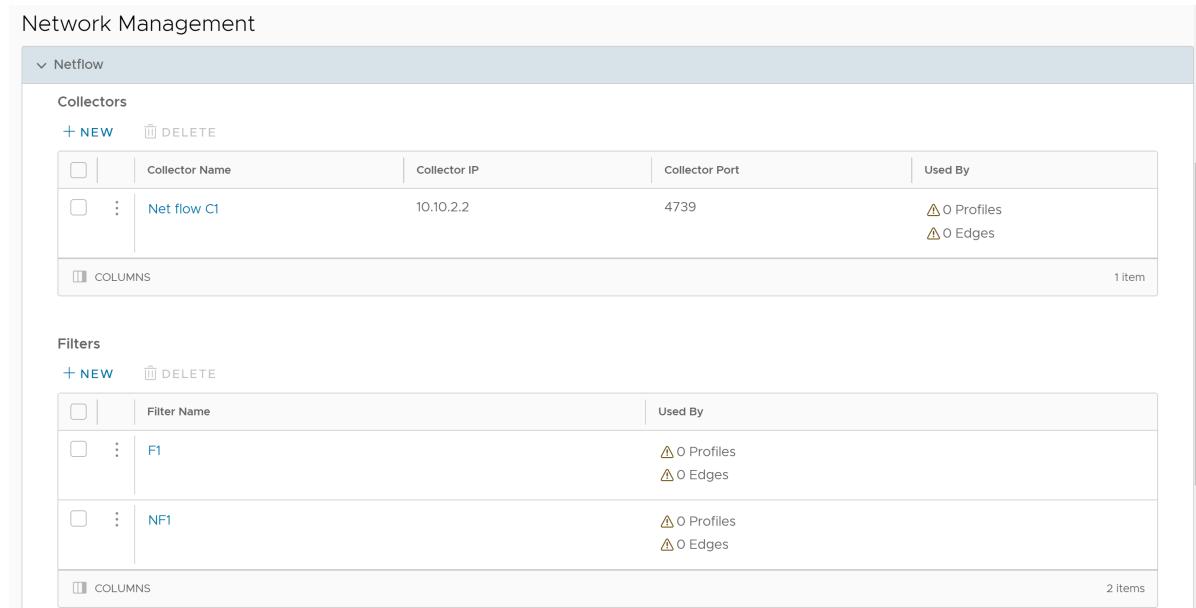
In an Enterprise network, Netflow monitors traffic flowing through SD-WAN Edge and exports Internet Protocol Flow Information Export (IPFIX) information directly from SD-WAN Edge to one or more Netflow collectors. IPFIX is an IETF protocol that defines the standard of exporting flow information from an end device to a monitoring system. VMware supports IPFIX version 10 to export IP flow information to a collector. Generally, an IP flow is identified by five tuples namely: Source IP, Destination IP, Source Port, Destination Port, and Protocol. But the Netflow records that are exported by SD-WAN Edge aggregates the source port. This means that data of different flows that have same source and destination IPs, same destination port, but different source ports will be aggregated.

The SASE Orchestrator allows you to configure Netflow collectors and filters as network services at the Profile, Edge, and Segment level. You can configure a maximum of two collectors per Segment and eight collectors per Profile and Edge. Also, you can configure a maximum of 16 filters per collector.

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**.

The **Network Services** page appears.



The screenshot shows the Network Management section of the VMware SD-WAN interface. It is divided into two main sections: **Netflow** and **Filters**.

**Netflow** section:

- Collectors:**
  - + NEW
  - DELETE

	Collector Name	Collector IP	Collector Port	Used By
<input type="checkbox"/>	Net flow C1	10.10.2.2	4739	<span style="color: orange;">⚠ 0 Profiles ⚠ 0 Edges</span>
- Filters:**
  - + NEW
  - DELETE

	Filter Name	Used By
<input type="checkbox"/>	F1	<span style="color: orange;">⚠ 0 Profiles ⚠ 0 Edges</span>
<input type="checkbox"/>	NF1	<span style="color: orange;">⚠ 0 Profiles ⚠ 0 Edges</span>

- 2 To configure a collector, scroll down to the **Network Management** category and click **Netflow**.

- 3 Under **Collectors**, click the **+ New**. The **New Collector** dialog box appears.

The screenshot shows the 'New Collector' dialog box. At the top right are 'View documentation' and a close button. The form contains three fields: 'Collector Name \*' with value 'Net flow C1', 'Collector IP \*' with value '10.10.2.2', and 'Collector Port \*' with value '4739'. At the bottom are two buttons: 'CLOSE' (in a white box) and 'SAVE CHANGES' (in a green box).

Collector Name *	Net flow C1
Collector IP *	10.10.2.2
Collector Port *	4739

**CLOSE** **SAVE CHANGES**

- In the **Collector Name** text box, enter a unique name for the collector.
- In the **Collector IP** text box, enter the IP address of the collector.
- In the **Collector Port** text box, enter the port ID of the collector.
- Click **Save Changes**.

Under **Network Services**, the newly added collector appears in the Collector table.

- 4 SASE Orchestrator allows filtering of traffic flow records by source IP, destination IP, and application ID associated with the flow.

---

**Note** Netflow filters are not applicable for the SD-WAN Control, Overflow, and Private data.

To configure a Netflow filter, under **Filters** click the **+New** button. The **Add Filter** dialog box appears.

## Add Filter

**Filter Name \*** NF1

**Match** Action

Source Define

Any  
 IP Address

IP Address  
10.0.1.0

---

Destination Any

---

Application Any

- a In the **Filter Name** text box, enter a unique name for the filter.
- b In the **Match** tab, click **Define** to define per collector filtering rules to match by source IP or destination IP or application associated with the flow, or click **Any** to use any of the source IP or destination IP or application associated with the flow as the match criteria for Netflow filtering.
- c In the **Action** tab, select either **Allow** or **Deny** as the filter action for the traffic flow, and click **OK**.

## Add Filter

**Filter Name \*** NF1

Under **Network Services**, the newly added filter appears in the Filter table.

## Results

At the Profile and Edge level, the configured collectors and filters appears as a list under the **Netflow** area in the **Device** tab.

- While configuring a Profile or Edge, you can either select a collector and filter from the available list or add a new collector and a filter. For steps, see [Configure Netflow Settings for Profiles](#).
- To override Netflow settings at the Edge level, see [Configure Netflow Settings for Edges](#).

After you enable Netflow on the SD-WAN Edge, it periodically sends messages to the configured collector. The contents of these messages are defined using IPFIX templates. For more information on templates, see [IPFIX Templates](#).

## IPFIX Templates

After you enable Netflow on the VMware SD-WAN Edge, it periodically sends messages to the configured collector. The contents of these messages are defined using templates. Internet Protocol Flow Information Export (IPFIX) templates have additional parameters that provide more information regarding the traffic flows.

### Non-NAT Template

<https://www.iana.org/assignments/ipfix/ipfix.xhtml>. This is an aggregated flow. Keys for this flow record are: sourceIPv4Address, destinationIPv4Address, destinationTransportPort, ingressVRFID, ApplicationID, protocolIdentifier. Source port is aggregated out.

#### Template ID: 256

The Non-NAT template is the common Netflow template.

Element ID	Name	Type	Description	Recommended Implementation	Applicable Edge Release
1	octetDeltaCount	unsigned64	The number of octets includes IP header(s) and IP payload.	Used to report on total bytes (aggregate of bytesTX and bytesRx) and BytesRX.	3.3.0
2	packetDeltaCount	unsigned64	The number of incoming packets since the previous report (if any) for this flow at the observation point.	Used to report on total packet (aggregate of packetTX and packetRX) and packetRX.	3.3.0

<b>Element ID</b>	<b>Name</b>	<b>Type</b>	<b>Description</b>	<b>Recommended Implementation</b>	<b>Applicable Edge Release</b>
32769	octetDeltaCount_rev	unsigned64	Biflow RFC 5103. The number of outgoing byte.	Used to report on total bytes (aggregate of bytesTX and bytesRX) and BytesTX.	3.3.0
32770	packetDeltaCount_rev	unsigned64	Biflow RFC 5103. The number of outgoing packets.	Used to report on total packet (aggregate of packetTX and packetRx) and packetTX.	3.3.0
3	deltaFlowCount	unsigned64	The conservative count of original flows contributing to this aggregated flow; may be distributed via any of the methods expressed by the valueDistribution Method Information Element.	See <a href="#">IPFIX Information Element Definitions</a> .	3.3.0
4	protocolIdentifier	unsigned8	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.	Implement as per description.	3.3.0
5	ipClassOfService	unsigned8	For IPv4 packets, this is the value of the TOS field in the IPv4 packet header.	Implement as per description.	3.3.0
8	sourcePv4Address	ipv4Address	The IPv4 source address in the IP packet header.	Implement as per description.	3.3.0

Element ID	Name	Type	Description	Recommended Implementation	Applicable Edge Release
10	ingressInterface	unsigned32	The index of the IP interface where packets of this flow are being received. The value matches the value of managed object 'ifIndex' as defined in <a href="#">RFC2863</a> .	This value maps to Interface option template 272 'ingressInterface' value where to map the flow to SD-WAN link interface number.	3.3.0
11	destinationTransportPort	unsigned16	The destination port identifier in the transport header.	Implement as per description.	3.3.0
12	destinationIPv4Address	ipv4Address	The IPv4 destination address in the IP packet header.	Implement as per description.	3.3.0
14	egressInterface	unsigned32	The index of the IP interface where packets of this flow are being sent. The value matches the value of managed object 'ifIndex' as defined in <a href="#">RFC2863</a> .	Egress interface	3.3.0
15	ipNextHopIPv4Address	ipv4Address	The IPv4 address of the next IPv4 hop. <a href="http://www.iana.org/go/rfc2863">http://www.iana.org/go/rfc2863</a>	This IP address identifies the next hop device when there is no SD-WAN overlay (underlay next hop).	3.3.0
56	sourceMacAddress	macAddress	The IEEE 802 source MAC address field.	Implement as per description.	3.3.0

Element ID	Name	Type	Description	Recommended Implementation	Applicable Edge Release
239	biflowDirection	unsigned8	<p>A description of the direction assignment method used to assign the biflow Source and destination. This Information element may be present in a flow data record or applied to all flows exported from an exporting process or observation domain using IPFIX options. If this Information element is not present in a flow record or associated with a biflow via scope, it is assumed that the configuration of the direction assignment method is done out-of-band.</p> <p><b>Note</b> When using IPFIX options to apply this Information element to all flows within an observation domain or from an exporting process, the option should be sent reliably. If reliable transport is not available (i.e., when using UDP), this Information element should appear in each flow record.</p>	<p>See <a href="#">IPFIX Information Element Definitions</a>.</p>	3.3.0

<b>Element ID</b>	<b>Name</b>	<b>Type</b>	<b>Description</b>	<b>Recommended Implementation</b>	<b>Applicable Edge Release</b>
95	applicationId	octetArray(8)	Specifies an application ID. RFC6759. For details, see <a href="#">Application Option Template</a> .	Implement to recognize L7 app signature.	3.3.0
148	flowID	unsigned64	An identifier of a flow that is unique within an observation domain. This information element can be used to distinguish between different flows if flow keys such as IP addresses and port numbers are not reported or are reported in separate records.	Unique flow ID maps to flow links stats option template 257.	3.3.0
152	flowStartMilliseconds	dateTimeMilliseconds	The absolute timestamp of the first packet of this flow.	Implement as per description.	3.3.0
153	flowEndMilliseconds	dateTimeMilliseconds	The absolute timestamp of the last packet of this flow.	Implement as per description.	3.3.0

Element ID	Name	Type	Description	Recommended Implementation	Applicable Edge Release
136	flowEndReason	unsigned8	<p>The reason for flow termination. The range of values includes the following:</p> <ul style="list-style-type: none"> <li>■ 0x01: idle timeout - The flow was terminated because it was considered to be idle.</li> <li>■ 0x02: active timeout - The flow was terminated for reporting purposes while it was still active, for example, after the maximum lifetime of unreported Flows was reached.</li> <li>■ 0x03: end of flow detected - The flow was terminated because the metering process detected signals indicating the end of the flow, for example, the TCP FIN flag.</li> <li>■ 0x04: forced end - The flow was terminated because of some external event, for</li> </ul>	Implement as per description.	3.3.0

Element ID	Name	Type	Description	Recommended Implementation	Applicable Edge Release
			<p>example, a shutdown of the metering process initiated by a network management application.</p> <ul style="list-style-type: none"> <li>■ 0x05: lack of resources - The flow was terminated because of lack of resources available to the metering process and/or the exporting process.</li> </ul>		
234	ingressVRFID	unsigned32	<p>A unique identifier of the VRFname where the packets of this flow are being received. This identifier is unique per metering process.</p>	<p>This maps to the VMware SASE Orchestrator segments. A segment should be visualized and reported as a separated L3 domain within the Edge.</p>	3.3.0

### Enterprise-Specific Fields (ID>32767)

## VMware SD-WAN IANA-PEN: 45346

Element ID (Enterprise Element ID)	Name	Type	Description	Recommended Implementation	Applicable Edge Release
45001 (12233)	destinationUUID	octetArray	Destination node UUID	This identifies the final SD-WAN endpoint in the path (same as nexthop UUID in e2e).	3.3.0
45002 (12234)	vcPriority	unsigned8	<ul style="list-style-type: none"> <li>■ 0 - Unset</li> <li>■ 1 - Control</li> <li>■ 2 - High</li> <li>■ 3 - Normal</li> <li>■ 4 - Low</li> </ul>	<p>This identifies the BizPolicy 'Priority' classification applied.</p> <p>Unset should be monitored to deduce a warning since it would only occur during overflow.</p>	3.3.0
45003 (12235)	vcRouteType	unsigned8	<ul style="list-style-type: none"> <li>■ 0 - Unset</li> <li>■ 1 - Gateway (using hosted GW svc)</li> <li>■ 2 - Direct (using direct Internet)</li> <li>■ 3 - Backhaul (using Hub to Internet)</li> </ul>	<p>This identifies the path type out to Internet the flow is taking.</p> <p>Unset should be monitored to deduce a warning since it would only occur during overflow.</p>	3.3.0
45004 (12236)	vcLinkPolicy	unsigned8	<ul style="list-style-type: none"> <li>■ 0 - NA</li> <li>■ 1 - Fixed</li> <li>■ 2 - Load balance</li> <li>■ 3 - Replicate</li> </ul>	<p>This value provides the type of link steering and remediation configured for this application under BizPolicy.</p>	3.3.0
45005 (12237)	vcTrafficType	unsigned8	<ul style="list-style-type: none"> <li>■ 0 - Realtime</li> <li>■ 1 - Transactional</li> <li>■ 2 - Bulk</li> </ul>	<p>This identifies the BizPolicy 'Service Class' classification applied.</p>	3.3.0

Element ID (Enterprise Element ID)	Name	Type	Description	Recommended Implementation	Applicable Edge Release
45007 (12239)	vcFlowPath	unsigned8	<ul style="list-style-type: none"> <li>■ 0 - Edge2CloudViaGateway (SaaS optimized)</li> <li>■ 1 - Edge2CloudDirect (SaaS not optimized)</li> <li>■ 2 - Edge2EdgeViaGateway (spoke2hub2 spoke via VCG)</li> <li>■ 3 - Edge2EdgeViaHub (spoke2hub2 spoke via PDC Hub)</li> <li>■ 4 - Edge2EdgeDirect (Edge2Edge dynamic)</li> <li>■ 5 - Edge2DataCenterDirect (Edge2PDC using underlay routing)</li> <li>■ 6 - Edge2DataCenterViaGateway (Edge2PDC using NVS)</li> <li>■ 7 - Edge2Backhaul (Edge2internal using PDC Hub)</li> <li>■ 8 - Edge2Proxy</li> </ul>	This identifies the type of 'path' the flow is taking.	3.3.0

Element ID (Enterprise Element ID)	Name	Type	Description	Recommended Implementation	Applicable Edge Release
			<ul style="list-style-type: none"> <li>■ 9 - Edge2OPG (PGW)</li> <li>■ 10 – Routed (path using underlay routing)</li> <li>■ 11 - Edge2CloudViaSecurityService (path using a CASB service to internet)</li> </ul>		
45009 (12241)	replicatedPacketsRxDeltaCount	unsigned64	Count of replicated packets received for the flow	This value provides the number of packets replicated (FEC) in the Rx path due to loss (applies to real-time protocols).	3.3.0
45010 (12242)	replicatedPacketsTxDeltaCount	unsigned64	Count of packets replicated for the flow	This value provides the number of packets replicated (FEC) in the Tx path due to loss (applies to real-time protocols).	3.3.0
45011 (12243)	lostPacketsRxDeltaCount	unsigned64	Count of packets lost for the flow at the receive	This value provides the total number of packets lost for the flow.	3.3.0
45012 (12244)	retransmittedPacketsTxDeltaCount	unsigned64	Count of packets retransmitted for the flow	This value provides the number of retransmitted packets due to loss (applies to transactional traffic).	3.3.0

<b>Element ID (Enterprise Element ID)</b>	<b>Name</b>	<b>Type</b>	<b>Description</b>	<b>Recommended Implementation</b>	<b>Applicable Edge Release</b>
45085 (12317)	tcpRttMs	unsigned16	Maximum RTT observed for a TCP flow	The maximum Roundtrip Time observed in milliseconds for the tcp packets in the flow, since the previous report (if any) for this flow at the observation point.	4.0.0
45086 (12318)	tcpRetransmits	unsigned32	Count of TCP packets retransmitted for the flow	The number of TCP packets retransmitted since the previous report (if any) for this flow at the observation point.	4.0.0
45080 (12312)	bizPolicyId	string	Business policy logical Id this flow is matching.	This value is a UUID and must be mapped to a BizPolicy via Orchestrator API.	3.3.2
45082 (12314)	nextHopUUID	octetArray	Next hop UUID for this flow. This will be populated in case of overlay traffic.	This value identifies the device that is in the path between source and destination in the SD-WAN overlay network (not underlay).	3.3.2

## NAT Template

Template ID: 259

Common + NAT template

Element ID	Name	Type	Description	Applicable Edge Release
225	postNATSourceIPv4Address	ipv4Address	The definition of this information element is identical to the definition of information element <i>sourceIPv4Address</i> , except that it reports a modified value caused by a NAT middlebox function after the packet passed the observation point.	3.4.0
226	postNATDestinationIPv4Address	ipv4Address	The definition of this information element is identical to the definition of information element <i>destinationIPv4Address</i> , except that it reports a modified value caused by a NAT middlebox function after the packet passed the observation point.	3.4.0

### Note

- Netflow exports are unidirectional flows. VMware SD-WAN needs to export flow stats as two flow records or implement RFC5103 (Bidirectional Flow Export).
- flowID will need to be constructed to be unique within the Enterprise.
- Direct NAT:
  - Consider a flow which comes from LAN client with IP 10.0.1.25 to Internet 169.254.6.18. This gets NATed due to business policy (SNAT source IP to a WAN interface IP 169.254.7.10). So, flow record for this flow will be with SIP: 10.0.1.25 and DIP: 169.254.6.18. The postNAT Source IP will be 169.254.7.10 and the postNAT Dest IP will be 169.254.6.18.

## Flow Link Stats Template

The Flow Link Stats template captures the flow stats broken down by link.

## Template ID: 257

Element ID (Enterprise Element ID)	Name	Type	Description	Applicable Edge Release
148	flowID	unsigned64	An identifier of a flow that is unique within an observation domain. This information element can be used to distinguish between different flows if flow keys such as IP addresses and port numbers are not reported or are reported in separate records.	3.3.0
1	octetDeltaCount	unsigned64	The number of octets since the previous report (if any) in incoming packets for this flow at the observation point. The number of octets includes IP header(s) and IP payload.	3.3.0
2	packetDeltaCount	unsigned64	The number of incoming packets since the previous report (if any) for this flow at the observation point.	3.3.0
32769	octetDeltaCount_rev	unsigned64	Biflow RFC 5103. The number of outgoing bytes.	3.3.0
32770	packetDeltaCount_rev	unsigned64	Biflow RFC 5103. The number of outgoing packets.	3.3.0
14	egressInterface	unsigned32	The index of the IP interface where packets of this flow are being sent. The value matches the value of managed object as defined in [RFC2863].	3.3.0
45008 (12240)	linkUUID	octetArray(16)	The VMware internal link ID.	3.3.0

Element ID (Enterprise Element ID)	Name	Type	Description	Applicable Edge Release
45009 (12241)	replicatedPacketsRxDeltaCount	unsigned64	Count of replicated packets received for the flow.	3.3.2 (This field was part of template Id 256 in 3.3.0)
45010 (12242)	replicatedPacketsTxDeltaCount	unsigned64	Count of packets replicated for the flow.	3.3.2 (This field was part of template Id 256 in 3.3.0)
45012 (12244)	retransmittedPacketsTxDeltaCount	unsigned64	Count of packets retransmitted for the flow.	3.3.2 (This field was part of template Id 256 in 3.3.0)

## Tunnel Stats Template

A tunnel is established over a link and has communication with a peer. A peer can be a Gateway (edge to Cloud traffic), Hub (edge to data center traffic) or Edge (dynamic edge-to-edge VPN traffic). The Tunnel Stats template captures the stats of a tunnel and it is sent every one minute. The linkUUID field lists the link established for the tunnel. The interface Index field says to which peer it is communicating.

### Difference between Tunnel and Path

Path is a unidirectional entity and tunnel is bi-directional. TX and RX paths make up a tunnel.

---

#### Note

- Only connected tunnels will be exported. If a tunnel goes DEAD, this tunnel's stats will not be exported from the next export interval. For example: if the tunnel stats template export interval is 300 seconds and the tunnel was exported at time t1 and tunnel goes down at t1+100. Stats between (t1 and t1+100) will be exported at t1+300. And from the next interval, this tunnel's stats will not be exported since the tunnel has gone DEAD.
  - Number of tunnels down events will be exported as part of tunnel stats template.
  - Formula for Loss computation:
    - TX Loss Percent =  $((packetsLostDeltaTxCount) / (packetsLostDeltaTxCount + packetsLostCompDeltaTxCount)) * 100$
    - RX Loss Percent =  $((packetsLostDeltaRxCount) / (packetsLostDeltaRxCount + packetsLostCompDeltaRxCount)) * 100$
-

**Template ID: 258**

<b>Element ID</b>	<b>Name</b>	<b>Type</b>	<b>Description</b>	<b>Applicable Edge Release</b>
12	destinationIPv4Address	Ipv4Address	This is destination Ipv4 address of tunnel.	3.4.0
45008 (12240)	linkUUID	octetArray(16)	This is link UUID on which tunnel is established. This value points to entry in link option template (276).	3.4.0
10	interfaceIndex	Unsigned32	This value identifies a peer. This value points to entry in interface option template (272).	3.4.0
1	octetsDeltaTxCount	Unsigned64	Total bytes transmitted on this path.	3.4.0
2	packetsDeltaTxCount	Unsigned64	Total packets transmitted out of this path.	3.4.0
45079 (12311)	packetsLostDeltaTxCount	Unsigned64	Total packets lost on this path.	3.4.0
45083 (12315)	txLossPercent	Float32	Loss percentage in this TX path.	3.4.0
45058 (12290)	jitterTxMs	Unsigned32	Tx average jitter of path in configured interval period.	3.4.0
45060 (12292)	avgLatencyTxMs	Unsigned32	Average TX latency of path in configured interval period.	3.4.0
32769	octetDeltaRxCount_rev	Unsigned64	Total bytes received on this path.	3.4.0
32770	packetsDeltaRxCount_rev	Unsigned64	Total packets received on this path.	3.4.0
45011 (12243)	packetsLostDeltaRxCount	Unsigned64	Total packets lost on this path.	3.4.0
45084 (12316)	rxLossPercent	Float32	Loss percentage in this RX path.	3.4.0

Element ID	Name	Type	Description	Applicable Edge Release
45061 (12293)	jitterRxMs	Unsigned32	RX average jitter of path in configured interval period.	3.4.0
45063 (12295)	avgLatencyRxMs	Unsigned32	Average RX latency of path in configured interval period.	3.4.0

## Application Option Template

<https://tools.ietf.org/html/rfc6759>. The Application Option template is sent every 5 minutes or when changed. Only applications that have been referenced in flows are exported.

Template ID: 271

Element ID	Name	Type	Description	Applicable Edge Release
95	applicationId	octetArray(8)	Scope field. Specifies an application ID. RFC 6759.	3.3.0
96	applicationName	string	Specifies the name of an application.	3.3.0
372	applicationCategory Name	string	An attribute that provides a first level categorization for each application ID.	3.3.0

## Application ID Format

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+-----+-----+-----+-----+-----+-----+-----+-----+			
20   enterprise ID = 45346 ...			
+-----+-----+-----+-----+-----+-----+-----+-----+			
...Ent.ID.contd  app ID			
+-----+-----+-----+-----+-----+-----+-----+-----+			

## Classification Engine ID: 20 (PANA-L7-PEN)

Proprietary layer 7 definition, including a Private Enterprise Number (PEN) [IANA-PEN] to identify that the application registry being used is not owned by the exporter manufacturer or to identify the original enterprise in the case of a mediator or third-party device. The Selector ID represents the enterprise unique global ID for the layer 7 applications. The Selector ID has a global significance for all devices from the same enterprise.

- 45346 is VMware SD-WAN PEN
- App ID is internal application ID

## Interface Option Template

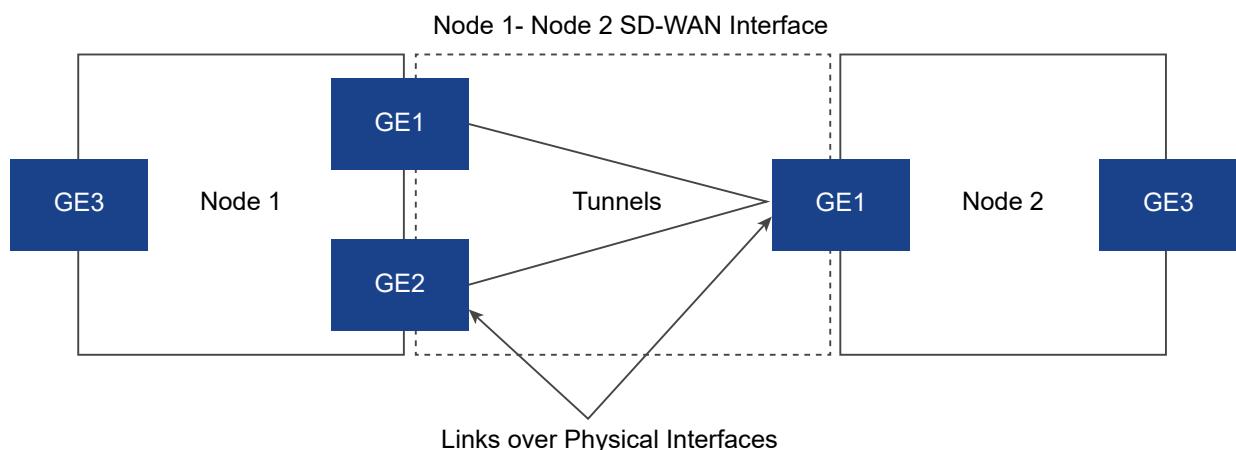
Interfaces in the VMware Netflow context can be broadly classified into two types: Physical and SD-WAN.

- Physical – These are Ethernet (e.g. GE1, GE2), VLAN (e.g. br-network1), or IP interfaces (e.g. PPPoE or some USB modem interfaces).
- SD-WAN – These are point-to-point interfaces between a pair of VMware devices. On the overlay, there may be several tunnels between a pair of VMware devices. These tunnels use a proprietary protocol called VCMP that provides several features including encryption, retransmission, and more. The tunnels between two devices may be always present or may be created on-demand depending on the configuration. The end points of these tunnels are called “links” in VMware terminology. Typically, there is a “link” for each physical WAN-facing interface on an Edge.

The diagram below depicts the relationship between physical/SD-WAN interfaces, links and tunnels. On both the nodes below, GE1, GE2 and GE3 are physical interfaces. GE1 and GE2 are WAN-side interfaces and have links defined over them. In contrast, GE3 is a LAN-side interface and thus does not have a link defined over it. Tunnels are formed between links on each node. The Node1-Node2 SD-WAN interface is the overlay interface on which traffic may be sent from Node 1 to Node 2. When traffic is sent on the Node1-Node2 SD-WAN interface, the individual packets may be either:

- Replicated on both the tunnels.
- Load-balanced between the two tunnels.
- Sent on only one tunnel.

The treatment of the packets depends on the type of traffic, configuration, and network conditions.



**Template ID: 272**

The interface option template is sent every 5 minutes by default. The timer is configurable.

Element ID (Enterprise Element ID)	Name	Type	Description	Applicable Edge Release
10	ingressInterface	unsigned32	Scope field. The index of this interface. The value matches the value of managed object as defined in [RFC2863].	3.3.0
82	interfaceName	string	A short name uniquely describing an interface, e.g. "Eth1/0".	3.3.0
83	interfaceDescription	string	The description of an interface, e.g. "FastEthernet1/0" or "ISP connection".	3.3.0
45000 (12232)	interfaceType	unsigned8	<ul style="list-style-type: none"> <li>■ 1 - Physical</li> <li>■ 2 - SDWAN E2E</li> <li>■ 3 - SDWAN E2DC</li> <li>■ 4 - SDWAN E2C</li> <li>■ 5 - Physical Sub-Interface (Supported from 3.4.0)</li> </ul>	3.3.0
45001 (12233)	destinationUUID	octetArray	Destination node UUID	3.3.0
45013 (12245)	primaryIpv4Address	ipv4Address	Primary IP address of a physical interface. For SD-WAN interfaces this is always 0.0.0.0.	3.3.0

## VMware Segment ID to Segment Mapping Template

The template is sent every 10 minutes and utilizes VRF as the nomenclature to define a segment.

**Template ID: 273**

Element ID	Name	Type	Description	Applicable Edge Release
234	ingressVRFID	unsigned32	Scope field. A unique identifier of the VRFname where the packets of this flow are being received. This identifier is unique per metering process.	3.3.0
236	VRFname	string	The name of a VPN Routing and Forwarding table (VRF).	3.3.0

## Link Option Template

The link option template provides a mapping between linkUUID and the interface index to which this link points. From the link option template, it is also possible to get the link name which is a configurable field in the .

### Template ID: 276

The Link Option template is sent every 5 minutes.

Element ID (Enterprise Element ID)	Name	Type	Description	Applicable Edge Release
45008 (12240)	linkUUID	octetArray(16)	The VMware internal link ID.	3.3.2
45078 (12310)	linkName	string	A short name uniquely describing the link. This is a configurable field in Orchestrator.	3.3.2
10	ingressInterface	unsigned32	Index of underlying interface to which this link points. The value matches the value of managed object as defined in [RFC2863].	3.3.2
58	vlanId	unsigned16	The VLAN ID of this link. There can be more than one link on an interface which is differentiated by this VLAN ID.	3.3.2

Element ID (Enterprise Element ID)	Name	Type	Description	Applicable Edge Release
8	sourcelP	unsigned32	The source IP for this link.	3.3.2
15	nextHopIP	unsigned32	The nextHop IP for this link.	3.3.2

## Netflow Source Address and Segmentation

Netflow source interface's primary IP address should come from VMware SASE Orchestrator. In absence of the optional source interface configuration, the flow records would consume one of the up and advertised LAN/Routed IP address as source IP address. It is mandatory to have at least one up and advertised LAN/Routed interface on the particular segment, for Netflow to function. The Orchestrator UI needs to be modified to reflect this.

When multiple Netflow exporting processes originate from the same IP, Netflow provides the information element to ensure the uniqueness of the export. The options are:

- Use different source interface for each segment.
- If we consider segments distinct exporting processes, then use observation DomainId to distinguish between segments.

## Interface Mappings

Interface numbering: 32-bit number (RFC2863). Ingress or egress is defined by source/destination route in flow container. Interface index is derived from route type and destination system ID or interface for direct traffic. The same mapping must be used for SNMP interface table (ifTable - RFC1213).

0..7	0..7	0..16
destination_type	reserved	destination_if_idx

destination\_type:

- E2E
- E2DC
- CLOUD
- ANY/DIRECT

destination\_if\_idx:

- E2E, E2DC, CLOUD: map(next\_hop\_id) -> if\_idx
- ANY/DIRECT: map(link\_logical\_id) -> if\_idx

## Filtering

Allow Netflow to be filtered by:

- ingressVRFID (or all segments)
- ApplicationID
- sourceIPv4Address (mask)
- destinationIPv4Address (mask)
- protocolIdentifier

## IPFIX Information Element Definitions

The following table lists the IPFIX information element definitions.

38	valueDistributionMethod	A description of the method used to distribute the counters from contributing flows into the aggregated flow records described by an associated scope, generally a template. The method is deemed to apply to all the non-key information elements in the referenced scope for which value distribution is a valid operation. If the originalFlowsInitiated and/or originalFlowsCompleted information elements appear in the template, they are not subject to this distribution method, as they each infer their own distribution method. This is intended to be a complete set of possible value distribution methods; it is encoded as follows:
----	-------------------------	--

Value	Description
0	Unspecified: The counters for an Original Flow are explicitly not distributed according to any other method defined for this Information Element; use for arbitrary distribution, or distribution algorithms not described by any other codepoint.
1	Start Interval: The counters for an Original Flow are added to the counters of the appropriate Aggregated Flow containing the start time of the Original Flow. This must be assumed the default if value distribution information is not available at a Collecting Process for an Aggregated Flow.
2	End Interval: The counters for an Original Flow are added to the counters of the appropriate Aggregated Flow containing the end time of the Original Flow.
3	Mid Interval: The counters for an Original Flow are added to the counters of a single appropriate Aggregated Flow containing some timestamp between start and end time of the Original Flow.

4	Simple Uniform Distribution: Each counter for an Original	
	Flow is divided by the number of time intervals the	
	Original Flow covers (that is, of appropriate Aggregated	
	Flows sharing the same Flow Key), and this number is	
	added to each corresponding counter in each Aggregated	
	Flow.	
	-----	
5	Proportional Uniform Distribution: Each counter for an	
	Original Flow is divided by the number of time units the	
	Original Flow covers, to derive a mean count rate. This	
	mean count rate is then multiplied by the number of times	
	units in the intersection of the duration of the Original	
	Flow and the time interval of each Aggregated Flow. This	
	is like simple uniform distribution, but accounts for the	
	fractional portions of a time interval covered by an	
	Original Flow in the first- and last-time interval.	
	-----	
6	Simulated Process: Each counter of the Original Flow is	
	distributed among the intervals of the Aggregated Flows	
	according to some function the Intermediate Aggregation	
	Process uses based upon properties of Flows presumed to	
	be like the Original Flow. This is essentially an	
	assertion that the Intermediate Aggregation Process has	
	no direct packet timing information but is nevertheless	
	not using one of the other simpler distribution methods.	
	The Intermediate Aggregation Process specifically makes	
	no assertion as to the correctness of the simulation.	
	-----	

		<table border="1"> <tr><td>  7   Direct: The Intermediate Aggregation Process has access  </td></tr> <tr><td>    to the original packet timings from the packets making up  </td></tr> <tr><td>    the Original Flow, and uses these to distribute or  </td></tr> <tr><td>    recalculate the counters.  </td></tr> <tr><td>+-----+-----+-----+</td></tr> </table>	7   Direct: The Intermediate Aggregation Process has access	to the original packet timings from the packets making up	the Original Flow, and uses these to distribute or	recalculate the counters.	+-----+-----+-----+	
7   Direct: The Intermediate Aggregation Process has access								
to the original packet timings from the packets making up								
the Original Flow, and uses these to distribute or								
recalculate the counters.								
+-----+-----+-----+								
23 9	biflowDirection	<p>A description of the direction assignment method used to assign the Biflow Source and Destination. This Information Element may be present in a Flow Data Record or applied to all flows exported from an Exporting Process or Observation Domain using IPFIX Options. If this Information Element is not present in a Flow Record or associated with a Biflow via scope, it is assumed that the configuration of the direction assignment method is done out-of-band.</p> <p><b>Note</b> when using IPFIX Options to apply this Information Element to all flows within an Observation Domain or from an Exporting Process, the Option must be sent reliably. If reliable transport is not available (that is, when using UDP), this Information Element must appear in each Flow Record.</p> <p>This field may take the following values:</p> <table border="1"> <tr><td>  Value   Name   Description  </td></tr> <tr><td>+-----+-----+-----+</td></tr> <tr><td>  0x00   arbitrary   Direction is assigned arbitrarily.  </td></tr> <tr><td>  0x01   initiator   The Biflow Source is the flow initiator, as determined by the Metering Process' best effort to detect the initiator.  </td></tr> <tr><td>  0x02   reverseInitiator   The Biflow Destination is the flow initiator, as determined by the Metering Process' best effort to detect the initiator. This value is provided for the convenience of Exporting Processes to revise an initiator estimate without re-encoding the Biflow Record.  </td></tr> <tr><td>  0x03   perimeter   The Biflow Source is the endpoint outside of a defined perimeter. The perimeter's definition is implicit in the set of Biflow Source and Biflow  </td></tr> </table>	Value   Name   Description	+-----+-----+-----+	0x00   arbitrary   Direction is assigned arbitrarily.	0x01   initiator   The Biflow Source is the flow initiator, as determined by the Metering Process' best effort to detect the initiator.	0x02   reverseInitiator   The Biflow Destination is the flow initiator, as determined by the Metering Process' best effort to detect the initiator. This value is provided for the convenience of Exporting Processes to revise an initiator estimate without re-encoding the Biflow Record.	0x03   perimeter   The Biflow Source is the endpoint outside of a defined perimeter. The perimeter's definition is implicit in the set of Biflow Source and Biflow
Value   Name   Description								
+-----+-----+-----+								
0x00   arbitrary   Direction is assigned arbitrarily.								
0x01   initiator   The Biflow Source is the flow initiator, as determined by the Metering Process' best effort to detect the initiator.								
0x02   reverseInitiator   The Biflow Destination is the flow initiator, as determined by the Metering Process' best effort to detect the initiator. This value is provided for the convenience of Exporting Processes to revise an initiator estimate without re-encoding the Biflow Record.								
0x03   perimeter   The Biflow Source is the endpoint outside of a defined perimeter. The perimeter's definition is implicit in the set of Biflow Source and Biflow								

		Destination addresses exported in the
		Biflow Records.
+-----+	+-----+	+-----+

## Configure DNS Services

This is an optional service that allows you to create a configuration for DNS.

The DNS service can be a public DNS service or a private DNS service provided by your company. It is handled by the `dnsmasq` service, which sends the request to all the servers configured at the same time. The server with the fastest response is selected. The service is preconfigured to use Google and Open DNS servers.

### Procedure

- In the **SD-WAN service** of the Enterprise portal, go to **Configure > Network Services**, and then under **Network Management** area, expand **DNS Services**.

DNS Services				
		+ NEW	EDIT	DELETE
	Name	Type	Servers	Used By
<input type="checkbox"/>	OpenDNS	Public	IPv4 Servers 208.67.222.222 208.67.220.220  IPv6 Servers 2620:119:35::35 2620:119:53::53	 
<input type="checkbox"/>	Google	Public	IPv4 Servers 8.8.8.8 8.8.4.4  IPv6 Servers 2001:4860:4860::8888 2001:4860:4860::8844	 
<input type="checkbox"/>	VMWare	Public	IPv4 Servers 10.148.20.5 10.112.16.144  IPv6 Servers None None	 

- To configure a DNS service, click **New** or **New DNS Service** option.

**Note** The **New DNS Service** option appears only when there are no items in the table.

- 3 The following screen displays the sample configuration for a Public DNS:

## New Public DNS Service

Private  
 Public

### Server Details

Service Name *	test123
IPv4 Server	<input type="text" value="208.67.221.221"/> <small>Example: 10.10.10.10</small>
IPv6 Server	<input type="text" value="2001:db8:3333:4444:5555:6666:7777:8888"/> <small>Example: 2001:db8:3333:4444:5555:6666:7777:8888</small>
	<span>-</span> <span>+</span>
	<span>-</span> <span>+</span>

CANCEL SAVE CHANGES

Option	Description
DNS Type	Choose either <b>Private</b> or <b>Public</b> as the DNS service type.
Service Name	Enter a name for the DNS Service.
IPv4 Server	Enter the IP address.
IPv6 Server	Enter the IP address. This field is optional.

#### Note

- Use the '+' and '-' buttons to add or delete the IP addresses.
- For a **Private** service, you can add one or more Private Domains.

**4 Click Save Changes.**

The newly added DNS service appears in the table.

**5 The following are the other options available in the **DNS services** area:**

Option	Description
Edit	Select an item and click this option to edit the selected DNS service.
Delete	Select an item and click this option to delete it.
Columns	Click and select the columns to be displayed or hidden on the page.

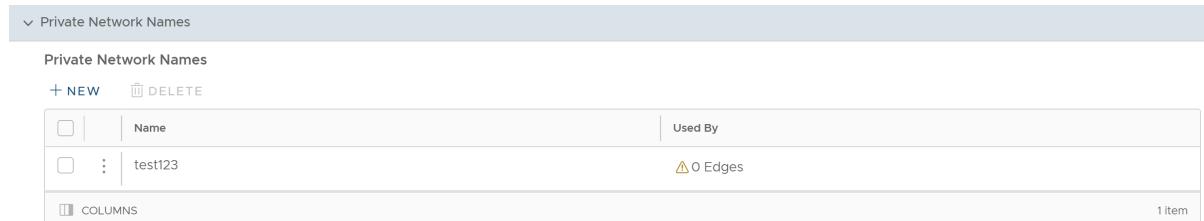
**Note** You can also access these options by clicking the vertical ellipsis next to the item name in the table.

## Configure Private Network Names

You can define multiple private networks and assign them to individual private WAN overlays.

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Network Management** area, expand **Private Network Names**.**

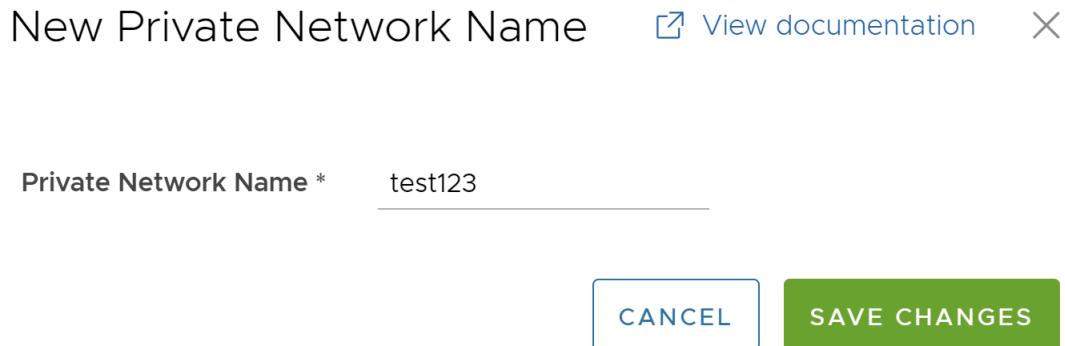


The screenshot shows a table titled "Private Network Names". At the top, there are buttons for "+ NEW" and "DELETE". The table has two columns: "Name" and "Used By". There is one row in the table with the name "test123" and a note "0 Edges". At the bottom of the table, there is a "COLUMNS" button and a note "1 item".

- 2 To configure a private network name, click **New** or **New Private Network Name** option.**

**Note** The **New Private Network Name** option appears only when there are no items in the table.

- 3 The following dialog is displayed:



- 4 Enter an appropriate name for the Private Network.

- 5 Click **Save Changes**.

The new Private Network Name appears in the table.

- 6 The following are the other options available in the **Private Network Names** area:

Option	Description
Delete	Select an item and click this option to delete it.
<b>Note</b>	
	<ul style="list-style-type: none"> <li>■ Only private network names that are not used by an Edge device can be deleted.</li> <li>■ Clicking this option opens another dialog where you must specify the number of items selected for deletion, and then click <b>Delete</b>.</li> </ul>
Columns	Click and select the columns to be displayed or hidden on the page.
<b>Note</b> You can also access the <b>New</b> and <b>Delete</b> options by clicking the vertical ellipsis next to the item name in the table.	

## Configure Prefix Delegation Tags

Prefix Delegation tags are defined to connect the LAN and WAN interfaces. The LAN interfaces can receive the prefixes from the associated WAN interface only if they share a common tag.

You can define Prefix Delegation tags by performing the following steps:

## Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Network Management** area, expand **Prefix Delegation Tags**.

Prefix Delegation Tags		
<input type="checkbox"/>	Tags	Used By
<input type="checkbox"/> :	tag_1	⚠ 0 Profiles ① 1 Edge
<input type="checkbox"/> COLUMNS		1 item

- To configure a Prefix Delegation tag, click **New** or **New Prefix Delegation Tag** option.

**Note** The **New Prefix Delegation Tag** option appears only when there are no items in the table.

- The following dialog is displayed:

New Prefix Delegation Tag ✖

Prefix Delegation Tag \*

CANCEL SAVE CHANGES

- Enter a unique name for the Prefix Delegation tag.
- Click **Save Changes**.

The new Prefix Delegation tag appears in the table.

- 6 The following are the other options available in the **Prefix Delegation Tags** area:

Option	Description
Delete	Select an item and click this option to delete it.
<b>Note</b>	
<ul style="list-style-type: none"> <li>■ Only Prefix Delegation tags that are not used by an Edge device can be deleted.</li> <li>■ Clicking this option opens another dialog where you must specify the number of items selected for deletion, and then click <b>Delete</b>.</li> </ul>	
Columns	Click and select the columns to be displayed or hidden on the page.

**Note** You can also access the **New** and **Delete** options by clicking the vertical ellipsis next to the item name in the table.

#### What to do next

Associate the Prefix Delegation tag to a Profile. For more information, see [Configure DHCPv6 Prefix Delegation for Profiles](#).

Associate the Prefix Delegation tag to an Edge. For more information, see [Configure DHCPv6 Prefix Delegation for Edges](#).

## Configure Authentication Services

If your organization uses a service for authentication or accounting, you can create a Network Service that specifies the IP address and ports for the service. This is a part of the 802.1x configuration process, which is configured in the profile.

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Network Management** area, expand **Authentication Services**.

Authentication Services		
<input type="button" value="+ NEW"/> <input type="button" value="DELETE"/>		
	Name	Servers
		Used By
There are no Authentication Services		
<input type="button" value="+ NEW AUTHENTICATION"/>		
<input type="button" value="COLUMNS"/> 0 items		

- 2 To configure an authentication service, click **New** or **New Authentication** option.

**Note** The **New Authentication** option appears only when there are no items in the table.

- 3 The following configuration options are displayed:

### New Radius Service

[View documentation](#) X

<b>Service Name *</b>	test123								
<b>Server Address *</b>	12.35.45.43								
Example 54.183.9.192									
<b>Shared Secret *</b>	.....  <span style="font-size: small;">(eye icon)</span>								
<b>Authentication Port *</b>	1812								
<b>Accounting Port</b>									
<b>Custom Attributes</b>									
<span style="color: blue; font-weight: bold;">+ ADD</span> <span style="color: grey;">■ DELETE</span>									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; padding: 5px;">□</th> <th style="text-align: center; padding: 5px;">ID ⓘ</th> <th style="text-align: center; padding: 5px;">Type</th> <th style="text-align: center; padding: 5px;">Value</th> </tr> </thead> <tbody> <tr> <td colspan="4" style="text-align: center; padding: 10px;">No Custom Attributes</td> </tr> </tbody> </table>		□	ID ⓘ	Type	Value	No Custom Attributes			
□	ID ⓘ	Type	Value						
No Custom Attributes									
<span style="border: 1px solid #ccc; padding: 5px; border-radius: 5px; color: blue;">CANCEL</span>	<span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 5px; border-radius: 5px; font-weight: bold;">ADD</span>								

Option	Description
Service Name	Enter an appropriate name for the authentication service.
Server Address	Enter the server IP address.

Option	Description
Shared Secret	Enter a password.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Authentication Port	Enter a port number. The valid range is 1 to 65535. The default value is 1812.
Accounting Port	Enter a port number if required.
Custom Attributes	Click <b>Add</b> , and enter the attribute details.

**Note** Source interfaces are configured only at Edge level. For more information, see [Chapter 29 Configure Edge Overrides](#).

- 4 Click **Add**.

The new Authentication service appears in the table.

- 5 The following are the other options available in the **Authentication Services** area:

Option	Description
Delete	Select an item and click this option to delete it.
Columns	Click and select the columns to be displayed or hidden on the page.

**Note** You can also access the **New** and **Delete** options by clicking the vertical ellipsis next to the item name in the table.

#### What to do next

To configure the Authentication settings for Profiles and Edges, see the topics [Configure Authentication Settings for Profiles](#) and [Configure Authentication Settings for Edges](#).

## Configure TACACS Services

TACACS services are used by organizations for authentication purpose to access the router or Network-attached Storage (NAS).

#### Prerequisites

You can configure the TACACS settings for an Edge from the TACACS Services section available under **Configure > Edges > Device Settings > Edge Services** category.

tab.

**Note** By default, **TACACS Services** section is not available in the **Device** page for Edges. Contact your Operator to get this feature activated.

## Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Network Management** area, expand **TACACS Services**.

TACACS Services			
	Name	Servers	Used By
<input type="checkbox"/>	test123	12.34.56.76:49	0 Edges
<input type="checkbox"/> COLUMNS			

1 item

- To configure TACACS services, click **New** or **Configure TACACS Service** option.

**Note** The **Configure TACACS Service** option appears only when there are no items in the table.

New TACACS Service
[View documentation](#)
X

**Service Name \***

**Server**

**IP Address \***

**Port \***

**Shared Secret \***

(eye icon)

CANCEL
SAVE CHANGES

- You can configure the following options:

Option	Description
Service Name	Enter an appropriate name for the authentication service.
Server Address	Enter the server IP address.

Option	Description
Port	Enter the port value.
Shared Secret	Enter a password.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.

- 4 Click **Save Changes**. The newly created TACACS service appears in the TACACS Services list.
- 5 To delete the TACACS service, Click **Delete**.

**Note** Clicking **Delete** removes the service from the TACACS Services list but the TACACS service that is used by an Edge cannot be deleted.

#### What to do next

To configure TACACS services for Edges, see [Configure TACACS Services for Edges](#).

## Configure Edge Services

This section allows you to configure VNFs and VNF Licenses. Virtual Network Functions (VNFs) are individual network services, such as routers and firewalls, running as software-only Virtual Machine (VM) instances on generic hardware.

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Network Services**, and then under **Edge Services** area, expand **VNFs**.

The screenshot shows the 'Edge Services' configuration interface. At the top, there's a header 'Edge Services'. Below it, there are two main sections:

- VNFs**: This section has a header 'VNFs' and a sub-header '+ NEW'. It contains a table with columns for 'Name', 'Type', and 'Used By'. A message 'There are no VNFs' is displayed. Below the table is a '+ CONFIGURE VNF' button. At the bottom of the table is a 'COLUMNS' button and a '0 items' count.
- VNF Licenses**: This section has a header 'VNF Licenses' and a sub-header '+ NEW'. It contains a table with columns for 'Name', 'Type', and 'Used By'. A message 'There are no VNF Licenses' is displayed. Below the table is a '+ NEW VNF LICENSE' button. At the bottom of the table is a 'COLUMNS' button and a '0 items' count.

- 2 To configure a new VNF, click **New** or **Configure VNF** option.

**Note** The **Configure VNF** option appears only when there are no items in the table.

Configure VNF X

Name \*

VNF Type \*  ▼

◀  ▶

CANCEL SAVE CHANGES

- 3 Enter a name for the VNF service and select a VNF type from the drop-down list.
- 4 Configure the settings based on the selected **VNF Type**.
- a For the VNF type **Check Point Firewall**, configure the following and click **Save Changes**.

## Configure VNF

Name \* test1

VNF Type \* Check Point Firewall

Primary Check Point Mgmt Server IP 172.2.24.23

SIC Key for Mgmt Server Access ..... (eye)

Admin Password ..... (eye)

VNF Image Location \* abc

Image Version \* R77.20.87 (8f8f, sha-1)

File Checksum Type sha-1

File Checksum 8f8f42784818f473c36b26d2ba1db1c977b7ebca

Download Type  https  s3

Access Key ID

Secret Access Key ..... (eye)

Region ca-central-1

< >

CANCEL SAVE CHANGES

Option	Description
Primary Check Point Mgmt Server IP	Enter the Check Point Smart Console IP address that must connect to the Check Point Firewall.
SIC Key for Mgmt Server Access	Enter the password used to register the VNF to the Check Point Smart Console.
Admin Password	Enter the administrator password.
VNF Image Location	Enter the image location from where the SASE Orchestrator must download the VNF image.
Image Version	Select a version of the Check Point VNF image from the drop-down list. The image version is derived from the system property <code>edge.vnf.extraImageInfos</code> .
File Checksum Type	Displays the method used to validate the VNF image and is automatically populated after you select an image version.

Option	Description
File Checksum	Displays the checksum used to validate the VNF image and is automatically populated after you select an image version. The checksum value is derived from the system property <code>edge.vnf.extraImageInfos</code> .
Download Type	Choose the type of the image. For <code>https</code> , enter the <b>Username</b> and <b>Password</b> . For <code>s3</code> , enter the <b>Access Key ID</b> , <b>Secret Access Key</b> , and choose the <b>Region</b> .

- b For the VNF type **Fortinet Firewall**, configure the following and click **Save Changes**.

## Configure VNF

Name \* test1

VNF Type \* Fortinet Firewall

Fortinet Mgmt Server IP \* 192.168.33.38

Fortimanager Serial Number \* FMG-VMTM-10055654

Registration Password \* ..... 

VNF Image Location \* zsu-p3s/forti-512

Image Version \* 6.2.0 (5a06, sha-1)

File Checksum Type \* sha-1

File Checksum \* 5a063f66a9b53a3ea1d0d8eac4596bb3c05e0946

Download Type  https  s3

Access Key ID

Secret Access Key ..... 

Region ap-south-1

Option	Description
Fortinet Mgmt Server IP	Enter the IP address of the FortiManager to connect to the FortiGate.
Fortimanager Serial Number	Enter the serial number of FortiManager.
Registration Password	Enter the password used to register the VNF to the FortiManager.
VNF Image Location	Enter the image location from where the SASE Orchestrator must download the VNF image.
Image Version	Select a version of the Fortinet VNF image from the drop-down list. The following options are available: 6.4.0, 6.2.4, 6.0.5, 6.2.0. The image version is derived from the system property <code>edge.vnf.extraImageInfos</code> .
File Checksum Type	Displays the method used to validate the VNF image and is automatically populated after you select an image version.

Option	Description
File Checksum	Displays the checksum used to validate the VNF image and is automatically populated after you select an image version. The checksum value is derived from the system property <code>edge.vnf.extraImageInfos</code> .
Download Type	Choose the type of the image. For <code>https</code> , enter the <b>Username</b> and <b>Password</b> . For <code>s3</code> , enter the <b>Access Key ID</b> , <b>Secret Access Key</b> , and choose the <b>Region</b> .

- c For the VNF type **Palo Alto Networks Firewall**, configure the following and click **Save Changes**.

Configure VNF X

Name *	test1
VNF Type *	Palo Alto Networks Firewall
Primary Panorama IP Address *	172.16.3.45
Secondary Panorama IP Address	
Panorama Auth Key *	..... <span style="border: 1px solid black; padding: 2px;">eye icon</span>
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #2e6b2e; color: white; border: 1px solid #2e6b2e; padding: 2px 10px; border-radius: 5px;">SAVE CHANGES</span>	

Option	Description
Primary Panorama IP Address	Enter the primary IP address of the Panorama server.
Secondary Panorama IP Address	Enter the secondary IP address of the Panorama server.
Panorama Auth Key	Enter the authentication key configured on the Panorama server. VNF uses the Auth Key to login and communicate with Panorama.

- 5 After configuring **Palo Alto Networks** as the **VNF Type**, define the **VNF Licenses**. These licenses are applied to one or more VNF configured Edges. To configure a VNF License, click **New** or **New VNF License** option, in the **VNF Licenses** area.

**Note** The **New VNF License** option appears only when there are no items in the table.



## VNF License Configuration

The screenshot shows the 'VNF License Configuration' window. It includes fields for 'Name' (Test123), 'VNF Type' (Palo Alto Networks Firewall), 'License Server API Key' (redacted), and 'Auth Code' (V5073094). There are buttons for 'VALIDATE LICENSE', 'CLOSE', and 'SAVE CHANGES'.

Name *	Test123
VNF Type *	Palo Alto Networks Firewall
License Server API Key *	.....
Auth Code *	V5073094
<input type="button" value="VALIDATE LICENSE"/> <input type="button" value="CLOSE"/> <input type="button" value="SAVE CHANGES"/>	

- 6 In the **VNF License Configuration** window, configure the following:

Option	Description
Name	Enter a name for the VNF license.
VNF Type	Select the VNF type from the drop-down list. Currently, <b>Palo Alto Networks Firewall</b> is the only available option.
License Server API Key	Enter the license key from your Palo Alto Networks account. The SASE Orchestrator uses this key to communicate with the Palo Alto Networks license server.
Auth Code	Enter the authorization code purchased from Palo Alto Networks.
Validate License	Click to validate the configuration.

- 7 Click **Save Changes**.

### Note

- If you want to remove the deployment of **Palo Alto Networks Firewall** configuration from a VNF type, ensure that you have deactivated the **VNF License** of Palo Alto Networks before removing the configuration.
- Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.

- 8 The following are the other options available in the **Edge Services** area:

Option	Description
Delete	Select an item and click this option to delete it.
Columns	Click and select the columns to be displayed or hidden on the page.

---

**Note** You can also access the **New** and **Delete** options by clicking the vertical ellipsis next to the item name in the table.

---

# Cloud Security Services

11

Cloud Security Service (CSS) is a cloud-hosted security that protects an Enterprise branch and/or data center. The security services include firewalls, URL filtering, and other such services.

In CSS, you can define and configure a cloud security service instance and establish a secure tunnel directly from the Edge to the CSS.

You can also configure the branch Edge to establish a tunnel directly to the cloud service pop. This option has the following advantages:

- Simplified configuration.
- Saves link bandwidth costs by offloading non-enterprise traffic to the internet.
- The branch sites are protected from malicious traffic by redirecting the Internet traffic to a cloud security service.

## Related Links:

- [Configure a Cloud Security Service](#)
- [Configure Cloud Security Services for Profiles](#)
- [Configure Cloud Security Services for Edges](#)

Read the following topics next:

- [Configure a Cloud Security Service](#)
- [Configure Cloud Security Services for Profiles](#)
- [Configure Cloud Security Services for Edges](#)
- [Configure Business Policies with Cloud Security Services](#)
- [Monitor Cloud Security Services](#)
- [Monitor Cloud Security Services Events](#)

## Configure a Cloud Security Service

The Cloud Security Service (CSS) establishes a secure tunnel from an Edge to the cloud security service sites. This ensures secured traffic flow to the cloud security services.

To configure a Cloud Security Service, perform the following steps.

## Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Network Services**.
- 2 In the Network Services page, navigate to **Non SD-WAN Destinations via Edge > Cloud Security Service**, click **New**.



- 3 In the **New Cloud Security Provider** window, select a service type from the drop-down menu. VMware SD-WAN supports the following CSS types:

- Generic Cloud Security Service
- Symantec / Palo Alto Cloud Security Service

**Note** Starting from 5.0.0 release, Palo Alto CSS are configured under the new service type template "Symantec / Palo Alto Cloud Security Service". All customers who have an existing Palo Alto CSS configured under "Generic Cloud Security Service" must move to the new template "Symantec / Palo Alto Cloud Security Service".

- Zscaler Cloud Security Service
- a If you have selected either "Generic" or "Symantec / Palo Alto" Cloud Security Service as the Service Type, then configure the following required details and click **Add**.

Option	Description
Service Name	Enter a descriptive name for the cloud security service.
Primary Point-of-Presence/Server	Enter the IP address or hostname for the Primary server.
Secondary Point-of-Presence/Server	Enter the IP address or hostname for the Secondary server. This is optional.

- b If you have selected Zscaler Cloud Security Service as the Service Type, then you can choose between manual deployment and automated deployment by selecting the **Automate Cloud Service Deployment** checkbox. Also, you can configure additional settings such as Zscaler Cloud and Layer 7 (L7) Health Check details to determine and monitor the health of the Zscaler Server.

### Configure Automatic Tunnels from SD-WAN Edge to Zscaler

This section describes how to automatically create a GRE or IPsec tunnel from SD-WAN Edge to Zscaler service provider.

## New Cloud Security Service

[View documentation](#)


<b>Service Type *</b> Zscaler Cloud Security Service	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">Select a service to continue</div>
<b>Service Name *</b> <input type="text" value="css_zscaler_gre_auto"/>	
<b>Automate Cloud Service Deployment *</b> <input checked="" type="checkbox"/> Enable	
Zscaler Cloud <input checked="" type="radio"/> Use existing Zscaler Cloud <input type="radio"/> Use new Zscaler Cloud	
<b>Existing Zscaler Cloud</b> <input type="text" value="zscalerbeta.net"/>	
<b>Tunneling Protocol</b> <input type="radio"/> IPsec <input checked="" type="radio"/> GRE	
<b>Domestic Preference</b> <input checked="" type="checkbox"/> Enable	
<b>Partner Admin Username *</b> <input type="text" value="zscaler-testing@velocloud.net"/>	
<b>Partner Admin Password *</b> <input type="password" value="....."/>	
<b>Partner Key *</b> <input type="password" value="....."/>	
<b>Domain *</b> <input type="text" value="velocloud.net"/> <small>Validate credentials after entering domain</small> <small>VALIDATE CREDENTIALS</small>	
<b>L7 Health Check</b> <input type="checkbox"/> Enable	
<b>Zscaler Login URL</b> <input type="text" value="https://admin.zscaler.net"/> <small>URL for logging into Zscaler. Example: zscaler.com</small>	
<b>Test Zscaler Login</b> <input style="background-color: #0070C0; color: white; border: none; padding: 5px; margin-right: 10px;" type="button" value="LOGIN"/> <span style="border: 1px solid #ccc; padding: 2px 10px; background-color: #fff; font-size: small;">CANCEL</span> <span style="border: 1px solid #0070C0; padding: 2px 10px; background-color: #0070C0; color: white; font-size: small;">SAVE CHANGES</span>	

- a In the **New Cloud Security Provider** window, enter a service name.
- b Select the **Automate Cloud Service Deployment** checkbox.

- c Select GRE or IPsec protocol for tunnel establishment.

**Note** The total number of CSS Zscaler GRE tunnels that can be configured per customer depends on the customer's subscription on Zscaler. The default value is 100.

- d Configure additional details such as Domestic Preference, Zscaler Cloud, Partner Admin Username, Password, Partner Key, and Domain, as described in the following table.

Option	Description
Domestic Preference	<p>Enable this option to prioritize Zscaler data centers from the country of origin of the IP address even if they are farther away from the other Zscaler data centers.</p> <p><b>Note</b> Previously, the <b>Domestic Preference</b> option was only available for GRE tunnels. Starting with the 6.0.0 release, this option is configurable for establishing IPsec tunnels as well.</p>
Zscaler Cloud	<p>You can choose to use the existing Zscaler clouds or use a new Zscaler Cloud. If you choose to use the existing cloud then select a Zscaler cloud service from the drop-down menu. For new Zscaler cloud, you must enter the Zscaler cloud service name in the textbox.</p>
Partner Admin Username	<p>Enter the provisioned username of the partner admin.</p>
Partner Admin Password	<p>Enter the provisioned password of the partner admin.</p> <p><b>Note</b> Starting from the 4.5 release, the use of the special character "&lt;" in the password is no longer supported. In cases where users have already used "&lt;" in their passwords in previous releases, they must remove it to save any changes on the page.</p>
Partner Key	<p>Enter the provisioned partner key.</p>
Domain	<p>Enter the domain name on which the cloud service would be deployed.</p>
Sub Cloud	<p>This is an optional parameter that Zscaler Internet Access (ZIA) customers use to have a custom pool of data centers for Geo-location purposes.</p> <p><b>Note</b> This option is available on CSS Zscaler automated deployment mode, if IPsec is selected for establishing tunnels.</p>

- e Click **Validate Credentials**. If the validation is successful, the **Save Changes** button will be activated.

**Note** You must validate the credentials to add a new CSS Provider.

- f Optional: Configure the following **L7 Health Check** details to monitor the health of the Zscaler Server.

**Note** The **L7 Health Check** feature tests HTTP reachability to the Zscaler backend server. Upon enabling L7 Health Check, the Edge sends HTTP L7 probes to a Zscaler destination (Example: `http://<zscaler cloud>/vpntest`) which is Zscaler's backend server for the HTTP health check. This method is an improvement over using network level keep-alive (GRE or IPsec) as that method only tests for network reachability to the frontend of a Zscaler server.

If an L7 response is not received after 3 successive retries, or if there is an HTTP error, the Primary Tunnel will be marked as 'Down' and the Edge will attempt to failover Zscaler traffic to the Standby Tunnel (if one is available). If the Edge successfully fails over Zscaler traffic to the Standby Tunnel, the Standby becomes the new Primary Tunnel.

In the unlikely event that the L7 Health Check marks both the Primary and Standby tunnels as 'Down', the Edge would route Zscaler traffic using a Conditional Backhaul policy (if such a policy has been configured).

The Edge only sends L7 probes over the Primary Tunnel towards the Primary Server, never over the Standby Tunnel.

Option	Description
L7 Health Check	<p>Select the checkbox to enable L7 Health Check for the Zscaler Cloud Security Service provider, with default probe details (HTTP Probe interval = 5 seconds, Number of Retries = 3, RTT Threshold = 3000 milliseconds). By default, L7 Health Check is not enabled.</p> <p><b>Note</b> Configuration of health check probe details is not supported.</p> <p><b>Note</b> For a given Edge/Profile, a user cannot override the L7 health check parameters configured in the Network Service.</p>
HTTP Probe Interval	The duration of the interval between individual HTTP probes. The default probe interval is 5 seconds.
Number of Retries	Specifies the number of probes retries allowed before marking the cloud service as DOWN. The default value is 3.

Option	Description
RTT Threshold	<p>The round trip time (RTT) threshold, expressed in milliseconds, used to calculate the cloud service status. The cloud service is marked as DOWN if the measured RTT is above the configured threshold. The default value is 3000 milliseconds.</p>
Zscaler Login URL	<p>Enter the login URL and then click <b>Login to Zscaler</b>. This will redirect you to the Zscaler Admin portal of the selected Zscaler cloud.</p> <p><b>Note</b> The <b>Login to Zscaler</b> button will be enabled if you have entered the Zscaler login URL.</p>

- g If you want to login to the Zscaler Admin portal from the Orchestrator, enter the Zscaler login URL and then click **Login to Zscaler**. This will redirect you to the Zscaler Admin portal of the selected Zscaler cloud.

---

**Note** The **Login to Zscaler** button will be enabled if you have entered the Zscaler login URL.

---

**Note** For more information about Zscaler CSS automated deployment, see [Zscaler and VMware SD-WAN Deployment Guide](#).

---

**Note** For specific details on how Zscaler determines the best data center Virtual IP addresses (VIPs) to use for establishing IPsec VPN tunnels, see [SD-WAN API Integration for IPsec VPN Tunnel Provisioning](#).

---

### Configure Manual Tunnels from SD-WAN Edge to Zscaler

This section describes how to manually create a GRE or IPsec tunnel from an SD-WAN Edge to a Zscaler service provider. Unlike automatic tunnels, configuring manual tunnels requires you to specify a tunnel destination to bring up the tunnels.

## New Cloud Security Service

[View documentation](#)

<b>Service Type *</b>	Zscaler Cloud Security Service	
Select a service to continue		
<b>Service Name *</b>	zscaler manual	
<b>Automate Cloud Service Deployment *</b>	<input type="checkbox"/> Enable	
<b>Zscaler Cloud *</b>	<input checked="" type="radio"/> Use existing Zscaler Cloud <input type="radio"/> Use new Zscaler Cloud	
<b>Existing Zscaler Cloud</b>	zscalerbeta.net	
<b>Primary Server *</b>	199.168.148.131	
<b>Secondary Server</b>	Enter FQDN/IP address	
<b>L7 Health Check</b>	<input checked="" type="checkbox"/> Enable	
<b>HTTP Probe Interval</b>	5	sec
<b>Number of Retries</b>	3	
	Must be a number from 0 to 5.	
<b>RTT Threshold</b>	3000	msec
	Must be a number from 0 to 5000.	
<b>Zscaler Login URL</b>	https://admin.zsclar.net	
URL for logging into Zscaler. Example: zscaler.com		
		<input type="button" value="CANCEL"/> <input type="button" value="SAVE CHANGES"/>

- a In the **New Cloud Security Provider** window, enter a service name.
- b Enter the IP address or hostname for the Primary server.
- c Optionally, you can enter the IP address or hostname for the Secondary server.
- d Select a Zscaler cloud service from the drop-down menu or enter the Zscaler cloud service name in the textbox.

- e Configure other parameters as desired, and then click **Save Changes**.

**Note** If you have selected Zscaler Cloud Security Service as the Service Type and planning to assign a GRE tunnel, it is recommended to enter only IP address in the Primary and Secondary server, and not the hostname, as GRE does not support hostnames.

## Results

The configured cloud security services are displayed under the **Cloud Security Service** area in the **Network Services** window.

Cloud Security Services			
	Name	Type	Used By
<input type="checkbox"/>		Zscaler Cloud Security Service	2 Edges
<input type="checkbox"/>		Zscaler Cloud Security Service	0 Edges
<b>COLUMNS</b>			
2 Items			

## What to do next

Associate the cloud security service with a Profile or an Edge:

- [Configure Cloud Security Services for Profiles](#)
- [Configure Cloud Security Services for Edges](#)

## Configure Cloud Security Services for Profiles

Enable Cloud Security Service (CSS) to establish a secured tunnel from an Edge to cloud security service sites. This enables the secured traffic being redirected to third-party cloud security sites. At the Profile level, VMware SD-WAN and Zscaler integration supports automation of IPsec and GRE tunnels.

**Note** Only one CSS with GRE is allowed per Profile.

Before you begin:

- Ensure that you have access permission to configure network services.
  - Ensure that your SASE Orchestrator has version 3.3.x or above.
  - You should have Cloud security service gateway endpoint IPs and FQDN credentials configured in the third party Cloud security service.
- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
  - 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. The configuration options for the selected Profile are displayed in the **Device** tab.
  - 3 Under the **VPN Services** category, click **Cloud Security Service** and activated **Cloud Security Service** by turning the toggle button to **On**.
  - 4 Configure the following settings:



Option	Description
Cloud Security Service	<p>Select a cloud security service from the drop-down menu to associate with the profile. You can also click <b>New Cloud Security Service</b> from the drop-down to create a new service type. For more information about how to create a new CSS, see <a href="#">Configure a Cloud Security Service</a>.</p> <p><b>Note</b> For cloud security services with Zscaler login URL configured, <b>Login to Zscaler</b> button appears in the <b>Cloud Security Service</b> area. Clicking the <b>Login to Zscaler</b> button will redirect you to the Zscaler Admin portal of the selected Zscaler cloud.</p>
Tunneling Protocol	<p>This option is available only for Zscaler cloud security service provider. If you select a manual Zscaler service provider then choose either IPsec or GRE as the tunneling protocol. By default, IPsec is selected.</p> <p><b>Note</b> If you select an automated Zscaler service provider then the <b>Tunneling Protocol</b> field is not configurable but displays the protocol name used by the service provider.</p>
Hash	Select the Hash function as SHA 1 or SHA 256 from the drop-down. By default, SHA 1 is selected.
Encryption	Select the Encryption algorithm as AES 128 or AES 256 from the drop-down. By default, None is selected.
Key Exchange Protocol	<p>Select the key exchange method as IKEv1 or IKEv2. By default, IKEv2 is selected.</p> <p>This option is not available for Symantec cloud security service.</p>
Login to Zscaler	Click <b>Login to Zscaler</b> to login to the Zscaler Admin portal of the selected Zscaler cloud.

## 5 Click **Save Changes**.

When you enable Cloud Security Service and configure the settings in a profile, the setting is automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge. See [Configure Cloud Security Services for Edges](#).

For the profiles created with cloud security service enabled and configured prior to 3.3.1 release, you can choose to redirect the traffic as follows:

- Redirect only web traffic to Cloud Security Service
- Redirect all Internet bound traffic to Cloud Security Service
- Redirect traffic based on Business Policy Settings – This option is available only from release 3.3.1. If you choose this option, then the other two options are no longer available.

---

**Note** For the new profiles that you create for release 3.3.1 or later, by default, the traffic is redirected as per the Business Policy settings. See [Configure Business Policies with Cloud Security Services](#).

---

## Configure Cloud Security Services for Edges

When you have assigned a profile to an Edge, the Edge automatically inherits the cloud security service (CSS) and attributes configured in the profile. You can override the settings to select a different cloud security provider or modify the attributes for each Edge.

To override the CSS configuration for a specific Edge, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Profiles.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Under the **VPN Services** category, in the **Cloud Security Service** area, the CSS parameters of the associated profile are displayed.
- 4 In the **Cloud Security Service** area, select the **Override** check box to select a different CSS or to modify the attributes inherited from the profile associated with the Edge. For more information on the attributes, see [Configure Cloud Security Services for Profiles](#).
- 5 Click **Save Changes** in the **Edges** window to save the modified settings.

---

**Note** For CSS of type Zscaler and Generic, you must create VPN credentials. For Symantec CSS type, the VPN credentials are not needed.

---

## Manual Zscaler CSS Provider Configuration for Edges

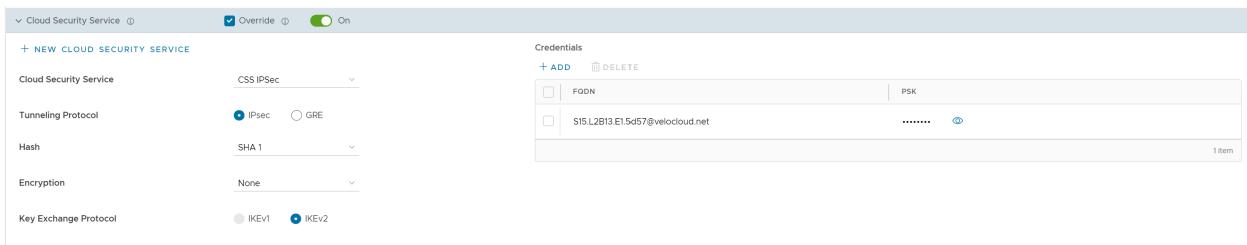
At the Edge level, for a selected manual Zscaler CSS provider, you can override the settings inherited from the profile and can configure additional parameters manually based on the tunneling protocol selected for tunnel establishment.

If you choose to configure an IPsec tunnel manually, apart from the inherited attributes, you must configure a Fully Qualified Domain Name (FQDN) and Pre-Shared Key (PSK) for the IPsec session.

---

**Note** As a prerequisite, you should have Cloud security service gateway endpoint IPs and FQDN credentials configured in the third party Cloud security service.

---



**Note** For cloud security services with Zscaler login URL configured, **Login to Zscaler** button appears in the **Cloud Security Service** area. Clicking the **Login to Zscaler** button will redirect you to the Zscaler Admin portal of the selected Zscaler cloud.

If you choose to configure a GRE tunnel manually, then you must configure GRE tunnel parameters manually for the selected WAN interface to be used as source by the GRE tunnel, by following the steps below.

- Under **GRE Tunnels**, click **+Add**.



- In the **Configure Tunnel** window appears, configure the following GRE tunnel parameters, and click **Update**.

X

## Configure Tunnel

**WAN Links** 54.69.238.136 ▾  
Select a link to continue

**Tunnel Source Public IP** Custom WAN IP ▾

**Link IP** 216.66.5.49

**Tunnel Addressing**

Tunnel Addressing	Point-of-Presence	Router IP / Mask	Internal ZEN IP / Mask
Primary Address	199.168.148.132	Enter Router IP	Enter Internal ZEN IP
Secondary Address	104.129.194.39	Enter Router IP	Enter Internal ZEN IP
2 items			

CANCEL

UPDATE

Option	Description
WAN Links	Select the WAN interface to be used as source by the GRE tunnel.
Tunnel Source Public IP	Choose the IP address to be used as a public IP address by the Tunnel. You can either choose the WAN Link IP or Custom WAN IP. If you choose Custom WAN IP, enter the IP address to be used as public IP. Source public IPs must be different for each segment when Cloud Security Service (CSS) is configured on multiple segments.
Primary Point-of-Presence	Enter the primary Public IP address of the Zscaler Datacenter.
Secondary Point-of-Presence	Enter the secondary Public IP address of the Zscaler Datacenter.
Primary Router IP/Mask	Enter the primary IP address of Router.
Secondary Router IP/Mask	Enter the secondary IP address of Router.

Option	Description
Primary Internal ZEN IP/Mask	Enter the primary IP address of Internal Zscaler Public Service Edge.
Secondary Internal ZEN IP/Mask	Enter the secondary IP address of Internal Zscaler Public Service Edge.

#### Note

- The Router IP/Mask and ZEN IP/Mask are provided by Zscaler.
- Only one Zscaler cloud and domain are supported per Enterprise.
- Only one CSS with GRE is allowed per Edge. An Edge cannot have more than one segment with Zscaler GRE automation enabled.
- Scale Limitations:
  - GRE-WAN: Edge supports maximum of 4 public WAN links for a Non SD-WAN Destination (NSD) and on each link, it can have up to 2 tunnels (primary/secondary) per NSD. So, for each NSD, you can have maximum of 8 tunnels and 8 BGP connections from one Edge.
  - GRE-LAN: Edge supports 1 link to Transit Gateway (TGW), and it can have up to 2 tunnels (primary/secondary) per TGW. So, for each TGW, you can have maximum of 2 tunnels and 4 BGP connections from one Edge (2 BGP sessions per tunnel).

## Automated Zscaler CSS Provider Configuration for Edges

At the Edge level, VMware SD-WAN and Zscaler integration supports:

- [IPsec/GRE Tunnel Automation](#)
- [Zscaler Location/Sub-Location Configuration](#)

For a selected automated Zscaler CSS provider at the Edge level, you can override the CSS settings inherited from the profile, establish automatic IPsec/GRE tunnels for each Edge Segment, create Sub-locations, and configure Gateway options and Bandwidth controls for Location and Sub-locations.

### IPsec/GRE Tunnel Automation

IPsec/GRE tunnel automation can be configured for each Edge segment. Perform the following steps to establish automatic tunnels from an Edge.

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Select an Edge you want to establish automatic tunnels.
- 3 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.

- 4 Under the **VPN Services** category, in the **Cloud Security Service** area, the CSS parameters of the associated profile are displayed.
- 5 In the **Cloud Security Service** area, select the **Override** check box to select a different CSS or to modify the attributes inherited from the profile associated with the Edge. For more information on the attributes, see [Configure Cloud Security Services for Profiles](#).
- 6 From the **Cloud Security Service** drop-down menu, select an automated CSS provider and click **Save Changes**.

The automation will create a tunnel in the segment for each Edge's public WAN link with a valid IPv4 address. In a multi-WAN link deployment, only one of the WAN Links will be utilized for sending user data packets. The Edge chooses the WAN link with the best Quality of Service (QoS) score using bandwidth, jitter, loss, and latency as criteria. Location is automatically created after a tunnel is established. You can view the details of tunnel establishment and WAN links in the **Cloud Security Service** section

---

**Note** After automatic tunnel establishment, changing to another CSS provider from an Automated Zscaler service provider is not allowed on a Segment. For the selected Edge on a segment, you must explicitly deactivate Cloud Security service and then reactivate CSS if you want to change to a new CSS provider from an Automated Zscaler service provider.

---

## Zscaler Location/Sub-Location Configuration

After you have established automatic IPsec/GRE tunnel for an Edge segment, Location is automatically created and appears under the **Zscaler** section of the Edge Device page.

---

**Note** Prior 4.5.0 release, the Sub-location configuration is located in the **Cloud Security Service** section for each segment. Currently, the Orchestrator allows you to configure the Zscaler configurations for Location and Sub-location for the entire Edge from the **Zscaler** section of the **Device Settings** page. For existing user of CSS Sub-location automation, the data will be migrated as part of Orchestrator upgrade.

---

In the **Zscaler** section, if you want to update the Location or create Sub-locations for the selected Edge, make sure:

- you check that the tunnel is established from the selected Edge and Location is automatically created. You will not be allowed to create a Sub-location if the VPN credentials or GRE options are not set up for the Edge. Before configuring Sub-locations, ensure you understand about Sub-location and their limitations. See <https://help.zscaler.com/zia/about-sub-locations>.

- you select the same Cloud Subscription that you used to create the Automatic CSS.

To update the Location or create Sub-locations for the selected Edge, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Select an Edge and click the icon under the **Device** column. The **Device Settings** page for the selected Edge appears.
- 3 Go to the **Zscaler** section and turn on the toggle button.

Name
edge_b1-edge1_f15e73

Sub-Location Name	LAN Networks	Subnets
other		

- 4 From the **Cloud Subscription** drop-down menu, select the same Cloud Subscription that you used to create the Automatic CSS. The Cloud Name associated to the selected Cloud Subscription automatically appears.

---

**Note** Cloud Subscription must have same Cloud name and Domain name as CSS.

---

**Note** If you want to change provider for "Cloud Subscription", you must first remove the "Location" by deactivating CSS and Zscaler, and then perform the creation steps with the new provider.

---

- 5 After you have established automatic IPsec/GRE tunnel for an Edge segment, Location is automatically created and appears under the **Location** table. Note that the Zscaler Location name now includes the Edge name at the beginning so it can be easily identified especially on the Zscaler portal where they can search for the Edge name to find the location.

If you want to configure the Gateway options and Bandwidth controls for the Location, click the **Edit** button. For more information, see [Configure Zscaler Gateway Options and Bandwidth Control](#).

- 6 To create a Sub-location, click **Add**.
  - In the **Sub-Location Name** textbox, enter a unique name for the Sub-location. The Sub-location name should be unique across all segments for the Edge. The name can contain alphanumeric with a maximum word length of 32 characters.

- b From the **LAN Networks** drop-down menu, select a VLAN configured for the Edge.
- c In the **Subnets** textbox, add subnets for the selected LAN network.

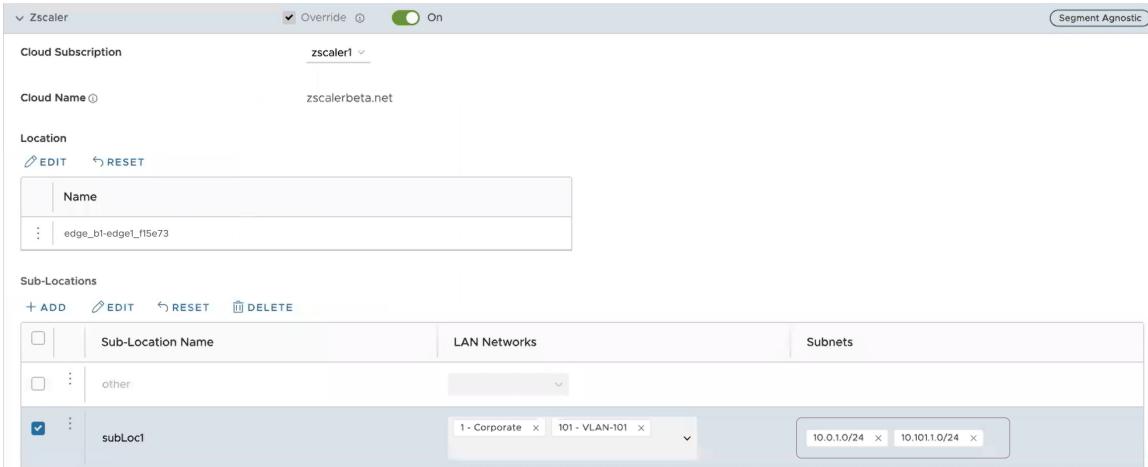
In prior Orchestrator versions, for the Zscaler sub-location configuration, the **Subnets** field that takes in subnets ignores the user input if the subnet being added is not directly connected to the Edge device, and users could not modify these subnets using the Orchestrator UI. This limitation presented a challenge for a branch offices where the LAN-side subnets were one hop away due to the presence of a layer 3 switch between the Edge and LAN devices. Release 6.0.0 allows users to add both direct and non-direct subnets.

---

**Note** For a selected Edge, Sub-locations should not have overlapping Subnet IPs.

---

- d Click **Save Changes**.



**Note** After you create at least one Sub-location in the Orchestrator, an “Other” Sub-location is automatically created in the Zscaler side, and it appears in the Orchestrator UI. You can also configure the “Other” Sub-location’s Gateway options by clicking the **Edit** button under **Gateway Options** in the **Sub-Locations** table. For more information, see [Configure Zscaler Gateway Options and Bandwidth Control](#).

---

- e After creating a Sub-location, you can update the Sub-location configurations from the same Orchestrator page. Once you click **Save Changes**, the Sub-location configurations on the Zscaler side will be updated automatically.
- f To delete a Sub-location, click **Delete**.

---

**Note** When the last Sub-location is deleted from the table, the “other” Sub-location will also be deleted automatically.

---

## Configure Zscaler Gateway Options and Bandwidth Control

To configure Gateway options and Bandwidth controls for the Location and Sub-location, click the **Edit** button under **Gateway Options**, in the respective table.

The **Zscaler Gateway Options and Bandwidth Control** window appears.

## Edit Location Gateway Options



### Location

#### Gateway Options

**Use XFF from Client Request**  Off

**Enable Caution**  Off

**Enable AUP**  Off

**Enforce Firewall Control**  Off

**Authentication**  Off

#### Bandwidth Control

**Bandwidth Control**  Off

**CANCEL**

**DONE**

Configure the Gateway options and Bandwidth controls for the Location and Sub-location, as needed, and click **Save Changes**.

**Note** The Zscaler Gateway Options and Bandwidth Control parameters that can be configured for the Locations and Sub-locations are slightly different, however; the Gateway Options and Bandwidth Control parameters for the Locations and Sub-locations are the same ones that one can configure on the Zscaler portal. For more information about Zscaler Gateway Options and Bandwidth Control parameters, see <https://help.zscaler.com/zia/configuring-locations>

Option	Description
<b>Gateway Options for Location/Sub-Location</b>	
Use XFF from Client Request	<p>Enable this option if the location uses proxy chaining to forward traffic to the Zscaler service, and you want the service to discover the client IP address from the X-Forwarded-For (XFF) headers that your on-premises proxy server inserts in outbound HTTP requests. The XFF header identifies the client IP address, which can be leveraged by the service to identify the client's sub-location. Using the XFF headers, the service can apply the appropriate sub-location policy to the transaction, and if <b>Enable IP Surrogate</b> is turned on for the location or sub-location, the appropriate user policy is applied to the transaction. When the service forwards the traffic to its destination, it will remove the original XFF header and replace it with an XFF header that contains the IP address of the client gateway (the organization's public IP address), ensuring that an organization's internal IP addresses are never exposed to externally.</p> <p><b>Note</b> This Gateway option is only configurable for Parent location.</p>
Enable Caution	<p>If you have not enabled <b>Authentication</b>, you can enable this feature to display a caution notification to unauthenticated users.</p>
Enable AUP	<p>If you have not enabled <b>Authentication</b>, you can enable this feature to display an Acceptable Use Policy (AUP) for unauthenticated traffic and require users to accept it. If you enable this feature:</p> <ul style="list-style-type: none"> <li>■ In <b>Custom AUP Frequency (Days)</b> specify, in days, how frequently the AUP is displayed to users.</li> <li>■ A <b>First Time AUP Behavior</b> section appears, with the following settings: <ul style="list-style-type: none"> <li>■ <b>Block Internet Access</b> - Enable this feature to deactivate all access to the Internet, including non-HTTP traffic, until the user accepts the AUP that is displayed to them.</li> <li>■ <b>Force SSL Inspection</b> - Enable this feature to make SSL Inspection enforce an AUP for HTTPS traffic.</li> </ul> </li> </ul>
Enforce Firewall Control	<p>Select to enable the service's firewall control.</p> <p><b>Note</b> Before enabling this option, user must ensure if its Zscaler account has subscription for "Firewall Basic".</p>
Enable IPS Control	<p>If you have enabled <b>Enforce Firewall Control</b>, select this to enable the service's IPS controls.</p> <p><b>Note</b> Before enabling this option, user must ensure if its Zscaler account has subscription for "Firewall Basic" and "Firewall Cloud IPS".</p>

Option	Description
Authentication	Enable to require users from the Location or Sub-location to authenticate to the service.
IP Surrogate	If you enabled <b>Authentication</b> , select this option if you want to map users to device IP addresses.
Idle Time for Dissociation	<p>If you enabled <b>IP Surrogate</b>, specify how long after a completed transaction, the service retains the IP address-to-user mapping. You can specify the Idle Time for Dissociation in Mins (default), or Hours, or Days.</p> <ul style="list-style-type: none"> <li>■ If the user selects the unit as Mins, the allowable range is from 1 through 43200.</li> <li>■ If the user selects the unit as Hours, the allowable range is from 1 through 720.</li> <li>■ If the user selects the unit as Days, the allowable range is from 1 through 30.</li> </ul>
Surrogate IP for Known Browsers	Enable to use the existing IP address-to-user mapping (acquired from the surrogate IP) to authenticate users sending traffic from known browsers.
Refresh Time for re-validation of Surrogacy	<p>If you enabled <b>Surrogate IP for Known Browsers</b>, specify the length of time that the Zscaler service can use IP address-to-user mapping for authenticating users sending traffic from known browsers. After the defined period of time elapses, the service will refresh and revalidate the existing IP-to-user mapping so that it can continue to use the mapping for authenticating users on browsers. You can specify the Refresh Time for re-validation of Surrogacy in minutes (default), or hours, or days.</p> <ul style="list-style-type: none"> <li>■ If the user selects the unit as Mins, the allowable range is from 1 through 43200.</li> <li>■ If the user selects the unit as Hours, the allowable range is from 1 through 720.</li> <li>■ If the user selects the unit as Days, the allowable range is from 1 through 30.</li> </ul>
<b>Bandwidth Control Options for Location</b>	
Bandwidth Control	Enable to enforce bandwidth controls for the location. If enabled, specify the maximum bandwidth limits for Download (Mbps) and Upload (Mbps). All sub-locations will share the bandwidth limits assigned to this location.
Download	If you enabled Bandwidth Control, specify the maximum bandwidth limits for Download in Mbps. The allowable range is from 0.1 through 99999.
Upload	If you enabled Bandwidth Control, specify the maximum bandwidth limits for Upload in Mbps. The allowable range is from 0.1 through 99999.

Option	Description
Bandwidth Control Options for Sub-Location (if Bandwidth Control is enabled on Parent Location)	
<h2>Edit Location Gateway Options</h2> <span style="float: right;">X</span>	
<b>Location</b> subLoc1	
<h3>Gateway Options</h3>	
<b>Enable Caution</b>	<input type="checkbox"/> Off
<b>Enable AUP</b>	<input type="checkbox"/> Off
<b>Enforce Firewall Control</b>	<input type="checkbox"/> Off
<b>Authentication</b>	<input type="checkbox"/> Off
<h3>Bandwidth Control</h3>	
<b>Bandwidth Control</b>	<input type="checkbox"/> Off
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; font-weight: bold;">DONE</span>	
<p><b>Note</b> The following bandwidth control options are configurable for sub-location only if you have bandwidth control enabled on the parent location. If the bandwidth control is not enabled on the parent location, then the bandwidth control options for sub-location are the same as location (Bandwidth Control, Download, Upload).</p>	
<b>Use Location Bandwidth</b>	If you have bandwidth control enabled on the parent location, select this option to enable bandwidth control on the sub-location and use the download and upload maximum bandwidth limits as specified for the parent location.

Option	Description
Override	Select this option to enable bandwidth control on the sub-location and then specify the maximum bandwidth limits for Download (Mbps) and Upload (Mbps). This bandwidth is dedicated to the sub-location and not shared with others.
Disabled	Select this option to exempt the traffic from any Bandwidth Management policies. Sub-location with this option can only use up to a maximum of available shared bandwidth at any given time.

## Limitations

- In 4.5.0 release, when a Sub-location is created, Orchestrator automatically saves the "Other" Sub-location. In earlier version of Orchestrator, the Zscaler "Other" Sub-location was not saved in Orchestrator. After upgrading Orchestrator to 4.5.0 release, the "Other" Sub-location will be imported automatically only after a new normal (non-Other) Sub-location is created using automation.
- Zscaler Sub-locations cannot have overlapping IP addresses (subnet IP ranges). Attempting to edit (add, update, or delete) multiple Sub-locations with conflicting IP addresses may cause the automation to fail.
- Users cannot update the bandwidth of Location and Sub-location at the same time.
- Sub-locations support **Use Location Bandwidth** option for bandwidth control when its Parent Location bandwidth control is enabled. When user turns off the Location bandwidth control on a Parent Location, the Orchestrator does not check or update the Sub-location bandwidth control option proactively.

## Related links

- [Monitor Cloud Security Services](#)
- [Monitor Cloud Security Services Events](#)
- [Monitor Network Services](#)

## Configure Business Policies with Cloud Security Services

You can create business policies to redirect the traffic to a Cloud Security Service.

For more information on business policies, see [Create Business Policy Rule](#).

### Procedure

- 1 In the SD-WAN service of the Enterprise portal, click **Configure > Profiles**.
- 2 Select a profile from the list and click the **Business Policy** tab.

- 3 Under **Configure Business Policy > Business Policy Rules**, click **+ADD**. The **Add Rule** dialog box appears.
- 4 Enter a name for the business rule and select the IP version.
- 5 Click the **Match** tab, choose the **Match** options to match the traffic.
- 6 Click the **Action** tab and from the **Network Service** drop-down menu click **Internet Backhaul** and choose a **Cloud Security Service** from the drop-down menu. You must have already associated the cloud security service to the profile.

Add Rule

Rule Name \*

IP Version \*  IPv4  IPv6  IPv4 and IPv6

**Match** **Action**

Priority  High  Normal  Low

Enable Rate Limit

Network Service

Non SD-WAN Destination via Edge / Cloud Security Service \*

Link Steering

Inner Packet DSCP Tag

Outer Packet DSCP Tag

Enable NAT  ⓘ

Service Class  Realtime  Transactional  Bulk

**CANCEL** **CREATE**

- 7 Choose the other actions as required and click **OK**.

## Results

The business policies that you create for a profile are automatically applied to all the Edges associated with the profile. If required, you can create additional business policies specific to the Edges.

- 1 Navigate to **Configure > Edges**, select an Edge, and click the **Business Policy** tab.
- 2 Under **Configure Business Policy > Business Policy Rules**, click **+ADD**. The **Add Rule** dialog box appears.
- 3 Define the rule with cloud security service associated with the Edge.

The Business Policy tab of the Edge displays the policies from the associated profile along with the policies specific to the Edge.

# Monitor Cloud Security Services

You can view the details of Cloud Security Services (CSS) configured for the Enterprise from the **Monitor > Network Services** page.

To monitor the cloud security service sites:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services**. The **Network Services** page appears.
- 2 Click the **Cloud Security Service Sites** tab to view all the CSS configured for the Enterprise along with the following configuration details.

Name	Type	Public IP	Status	Tunnel Status	Service Status	State Changed Time	Deployment Status
CSS IPSec	Zscaler Cloud Security Service	104.129.194.39 199.168.148.132	All Up	2 Standby 2 Up	4 Unknown	Apr 20, 2023, 2:55:22 PM (a few seconds ago)	

Field	Description
Name	The name of the CSS provider.
Type	The type of the CSS provider.
Public IP	The Public IP address of the CSS provider.

Field	Description
Status	<p>The overall status of the CSS provider:</p> <ul style="list-style-type: none"> <li>■ White - Specifies two possible states:           <ul style="list-style-type: none"> <li>■ ALL_STANDBY - The CSS provider is in this state if all the tunnels associated with the CSS provider are in STANDBY mode.</li> <li>■ UNKNOWN - The CSS provider is in this state if the overall status of the CSS provider is undetermined.</li> </ul> </li> <li>■ Green - The CSS provider is in ALL_UP state if all the tunnels associated with the CSS provider are UP.</li> <li>■ Red - The CSS provider is in ALL_DOWN state if all the tunnels associated with the CSS provider are DOWN.</li> <li>■ Amber - The CSS provider is in PARTIAL state if the tunnels associated with the CSS provider are partially UP, DOWN, or in STANDBY mode.</li> </ul>
Tunnel Status	<p>The status of tunnels created from the CSS provider from different Edges:</p> <ul style="list-style-type: none"> <li>■ White - Specifies two possible states:           <ul style="list-style-type: none"> <li>■ UNKNOWN - The tunnel is in this state if the tunnel is unestablished.</li> <li>■ NOT ENABLED - The tunnel is in this state if the tunnel is not enabled.</li> </ul> </li> <li>■ Gray - The tunnel associated with the CSS provider is in STANDBY mode.</li> <li>■ Green - Specifies two possible states:           <ul style="list-style-type: none"> <li>■ ALL_UP - All the tunnels associated with the CSS provider are UP.</li> <li>■ UP - A specific tunnel associated with the CSS provider is UP.</li> </ul> </li> <li>■ Red - Specifies two possible states:           <ul style="list-style-type: none"> <li>■ ALL_DOWN - All the tunnels associated with the CSS provider are DOWN.</li> <li>■ DOWN - A specific tunnel associated with the CSS provider is DOWN.</li> </ul> </li> </ul> <p><b>Note</b> The numbers that appear on the Tunnel Status and Service Status icons signify the number of Edges associated with that state for the respective CSS provider.</p>

Field	Description
Service Status	<p>The status of the external service as recorded by each Edge:</p> <ul style="list-style-type: none"> <li>■ Green - The Layer 7 (L7) Health status of external service is UP.</li> <li>■ Red - The L7 Health status of external service is DOWN.</li> <li>■ Red - The L7 Health status of external service is DOWN due to one of the following reasons:           <ul style="list-style-type: none"> <li>■ The Zen service does not respond to 'N' (Default = 3) consecutive HTTP probe messages.</li> <li>■ The HTTP response (200 OK) time exceeds the set time (Default = 300 milliseconds).</li> <li>■ The Zen server responds with 4xx HTTP error code.</li> </ul> </li> <li>■ Amber - The L7 Health status of external service is DEGRADED if the HTTP load time exceeds 'N' seconds (Default = 3 seconds).</li> <li>■ Gray - The L7 Health status of external service is UNKNOWN.</li> </ul>
State Changed Time	The date and time by when the state change occurred.
DeploymentStatus	Allows to view the deployment status of the CSS provider.

- 3 Click the Radio button before the CSS provider Name to view the related state change events.

The screenshot shows the VMware SD-WAN Administration interface. The left sidebar has tabs for Monitor, Configure, Diagnostics, and Service Settings, with Monitor selected. Under Network Services, there are links for Network Overview, Edges, Network Services (which is selected), Routing, Alerts, Events, and Reports. The main pane displays 'Network Services' with a table of Cloud Security Service Sites. One row is highlighted for 'CSS IPSec' (Zscaler Cloud Security Service). Below the table is a 'Related State Change Events' section with a table showing events for edge 'b1-edge1'.

Edge	Identifier	Public IP	State	State Changed Time
b1-edge1	satheesh@velocloud.net	199.168.148.132	Up	Apr 20, 2023, 2:59:22 PM (2023-04-20T09:29:22.698Z)
b1-edge1	Link 00000003-55f7-4848-a0ba-e287b4f3b35d	104.129.194.39	Standby	Apr 20, 2023, 2:59:22 PM (2023-04-20T09:29:22.698Z)
b1-edge1	Link 00000003-55f7-4848-a0ba-e287b4f3b35d	104.129.194.39	Standby	Apr 20, 2023, 2:59:22 PM (2023-04-20T09:29:22.698Z)
b1-edge1	satheesh@velocloud.net	199.168.148.132	Up	Apr 20, 2023, 2:59:22 PM (2023-04-20T09:29:22.698Z)
b1-edge1	satheesh@velocloud.net	104.129.194.39	Up	Apr 19, 2023, 2:25:00 PM (2023-04-19T08:55:00.633Z)
b1-edge1	satheesh@velocloud.net	104.129.194.39	Up	Apr 19, 2023, 2:24:30 PM (2023-04-19T08:54:30.621Z)

- 4 Click the **View** link in the Deployment Status column to view the deployment status of the CSS provider.

Cloud Security Service Automated Deployment Status for CSS IPSec

Edge	Segment	Action	Status	Zscaler Sub-Location Name
 No deployment statuses found.				

**DONE**

The following are the seven different states for an Edge action:

- Pending Location - The Edge action is in this state until a Zscaler location is created. This state is only applicable for Sub-location Edge actions.
- Pending - The Edge action is in this state as it waits for a backend worker process to pick it up and start working on it.
- In-Progress - The Edge action is in this state after a backend worker process picks up the Edge action and starts working on it.
- Completed - The Edge action is in this state if the Edge action task is successfully completed.
- Failed - The Edge action is in this state if an error has occurred.
- Timed Out - The Edge action is in this state if it takes more than the expected amount of time to complete the Edge action task.
- Pending Delete - The Edge action is in this state if it is pending deletion.
- **Note** Currently, the "Pending Location" and "Pending Delete" states are not used and these states will be removed from the UI in the future release.

## 5 Click **Details** to view the Event details.

You can also view the Layer 7 (L7) health check statistics for Cloud Security Service from the **Monitor > Edges** menu.

# Monitor Cloud Security Services Events

You can view the events related to cloud security services from the **Monitor > Events** page.

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Events**.

To view the events related to cloud security service sites, you can use the **Search** and **Filter** options. Click the **Filter** icon and choose to filter either by the **Event** or by the **Message** column.

Event	User	Segment	Edge	Severity	Time	Message
Edge Non SD-WAN Destination tunnel up	Global Segment	b1-edge1	● Info	Apr 19, 2023, 1:55:27 PM		IPsec tunnel up for edge [b1-edge1] for provider: [CSS IPsec]
VPN Tunnel state change			● Notice	Apr 19, 2023, 1:55:04 PM		Tunnel to [NSD via GW ZScaler] - Tunnel established (1/1) to 199.168.148.132
Edge Non SD-WAN Destination tunnel up	Seg1	b1-edge1	● Info	Apr 19, 2023, 1:54:58 PM		IPsec tunnel up for edge [b1-edge1] for provider: [CSS IPsec]
Edge Non SD-WAN Destination tunnel up	Seg1	b1-edge1	● Info	Apr 19, 2023, 1:51:26 PM		IPsec tunnel up for edge [b1-edge1] for provider: [CSS IPsec]
Edge Non SD-WAN Destination tunnel up	Global Segment	b1-edge1	● Info	Apr 19, 2023, 1:51:26 PM		IPsec tunnel up for edge [b1-edge1] for provider: [CSS IPsec]
Edge Non SD-WAN Destination tunnel down	Seg1	b1-edge1	● Info	Apr 19, 2023, 1:51:26 PM		IPsec tunnel down for edge [b1-edge1] for provider: [CSS IPsec]
Edge Non SD-WAN Destination tunnel down	Global Segment	b1-edge1	● Info	Apr 19, 2023, 1:51:25 PM		IPsec tunnel down for edge [b1-edge1] for provider: [CSS IPsec]
CSS tunnels are up		b1-edge1	● Alert	Apr 19, 2023, 1:51:05 PM		CSS paths are UP. Traffic will be routed through CSS based on Business Policy rules.
All CSS tunnels down		b1-edge1	● Alert	Apr 19, 2023, 1:51:00 PM		CSS paths are DOWN. If Conditional Backhauled (CBH) is enabled, all Business Policy rules are subject to failover traffic through CBH.

The following table includes the Enterprise events which help track various Edge actions related to CSS deployment, Location and Sub-location automation.

Events	Description
Call made to external API	An API call to some external service has been made.
CLOUD_SECURITY_PROVIDER_ADDED	A new CSS provider has been added.
CLOUD_SECURITY_PROVIDER_UPDATED	A new CSS provider has been updated.
CLOUD_SECURITY_PROVIDER_REMOVED	A CSS provider has been removed.
Cloud Security Service site creation enqueued	A CSS site creation task has been enqueued.
Cloud Security Service site update enqueued	A CSS site update task has been enqueued.
Cloud Security Service site deletion enqueued	A CSS site deletion task has been enqueued.
Network Service created	A CSS site has been created.
Network Service updated	A CSS site has been updated.
Network Service deleted	A CSS site has been deleted.
CSS tunnels are up	The CSS paths are UP. The traffic will be routed through CSS based on the Business policy rules configured.

<b>Events</b>	<b>Description</b>
All CSS tunnels are down	The CSS paths are DOWN.
Edge Non SD-WAN Destination tunnel up	The tunnel is UP for the Edge.
Edge Non SD-WAN Destination tunnel down	The tunnel is DOWN for the Edge.
Zscaler Location creation enqueued	An Edge action has been enqueued to create a location.
Zscaler Location update enqueued	An Edge action has been enqueued to update a location.
Zscaler Location deletion enqueued	An Edge action has been enqueued to delete a location.
Zscaler Location object created	A Zscaler location object is created.
Zscaler Location object updated	A Zscaler location object is updated.
Zscaler Location object deleted	A Zscaler location object is deleted.
Zscaler Sub Location creation enqueued	An Edge action has been enqueued to create a sub-location.
Zscaler Sub Location update enqueued	An Edge action has been enqueued to update a sub-location.
Zscaler Sub Location deletion enqueued	An Edge action has been enqueued to delete a sub-location.
Zscaler Sub Location object created	A Zscaler Sub-location object is created.
Zscaler Sub Location object updated	A Zscaler Sub-location object is updated.
Zscaler Sub Location object deleted	A Zscaler Sub-location object is deleted.

# Azure Virtual WAN IPsec Tunnel Automation

12

VMware SASE Orchestrator supports integration and automation of Azure Virtual WAN from VMware SD-WAN Gateway and VMware SD-WAN Edge to enable Branch-to-Azure VPN Connectivity.

Read the following topics next:

- [Azure Virtual WAN IPsec Tunnel Automation Overview](#)
- [Prerequisite Azure Configuration](#)
- [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#)
- [Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Gateway](#)
- [Synchronize VPN Configuration](#)
- [Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Edge](#)
- [Monitor Non SD-WAN Destinations](#)

## Azure Virtual WAN IPsec Tunnel Automation Overview

Azure Virtual WAN is a network service that facilitates optimized and automated Virtual Private Network (VPN) connectivity from enterprise branch locations to or through Microsoft Azure.

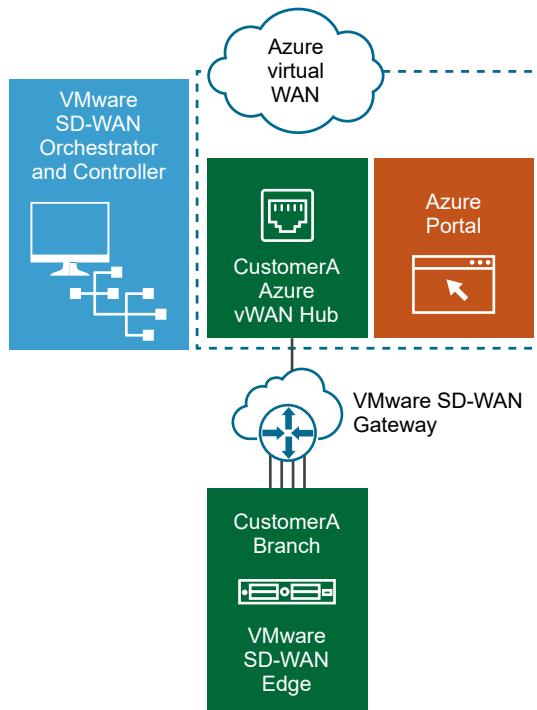
Azure subscribers provision Virtual Hubs corresponding to Azure regions and connect branches (which may or may not be SD-WAN enabled) through IP Security (IPsec) VPN connections.

To establish branch-to-Azure VPN connectivity, SASE Orchestrator supports Azure Virtual WAN and VMware SD-WAN integration and automation by leveraging the Azure backbone. Currently, the following Azure deployment options are supported from the VMware SD-WAN perspective:

- IPsec from SD-WAN Gateway to Azure virtual WAN hub with automation.
- Direct IPsec from SD-WAN Edge to Azure virtual WAN hub with automation.

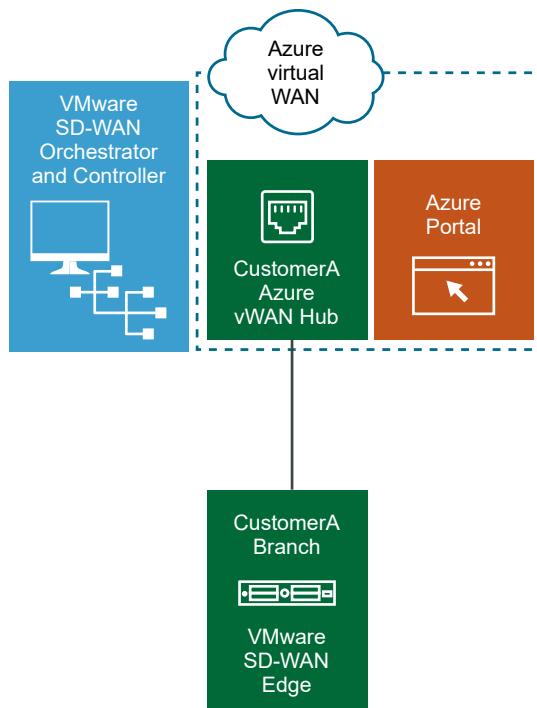
## Azure Virtual WAN SD-WAN Gateway automation

The following diagram illustrates the IPsec tunnel from SD-WAN Gateway to Azure virtual WAN hub.



## Azure Virtual WAN SD-WAN Edge automation

The following diagram illustrates the IPsec tunnel directly from SD-WAN Edge to Azure virtual WAN hub.



The following topics provide instructions for configuring the SASE Orchestrator and Azure to enable branch-to-Azure VPN connectivity through the SD-WAN Gateway and SD-WAN Edge:

- Prerequisite Azure Configuration
- Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity
- Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Gateway
- Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Edge

## Prerequisite Azure Configuration

Enterprise network administrators must complete the following prerequisite configuration tasks at the Azure portal to ensure that the SASE Orchestrator application can function as the Service Principal (identity for the application) for the purposes of Azure Virtual WAN and SD-WAN Gateway integration.

- Register SASE Orchestrator Application
- Assign the SASE Orchestrator Application to Contributor Role
- Register a Resource Provider
- Create a Client Secret

## Register SASE Orchestrator Application

Describes how to register a new application in Azure Active Directory (AD).

To register a new application in Azure AD:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Click **All Services** and search for **Azure Active Directory**.

- 3 Select **Azure Active Directory** and go to **App registrations > New registration**.

The **Register an application** screen appears.

### Register an application

#### \* Name

The user-facing display name for this application (this can be changed later).



#### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Velocloud Networks, Incit@velo)
- Accounts in any organizational directory
- Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

#### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.




By proceeding, you agree to the Microsoft Platform Policies [\[ \]](#)

**Register**

- 4 In the **Name** field, enter the name for your SASE Orchestrator application.
- 5 Select a supported account type, which determines who can use the application.
- 6 Click **Register**.

#### Results

Your SASE Orchestrator application will be registered and displayed in the **All applications** and **Owned applications** tabs.

Make sure to note down the Directory (tenant) ID and Application (client) ID to be used during the SASE Orchestrator configuration for Cloud Subscription.

#### What to do next

- [Assign the SASE Orchestrator Application to Contributor Role](#)

- Create a Client Secret

## Assign the SASE Orchestrator Application to Contributor Role

To access resources in your Azure subscription, you must assign the application to a role. You can set the scope at the level of the subscription, resource group, or resource. Permissions are inherited to lower levels of scope.

To assign a Contributor role at the subscription scope:

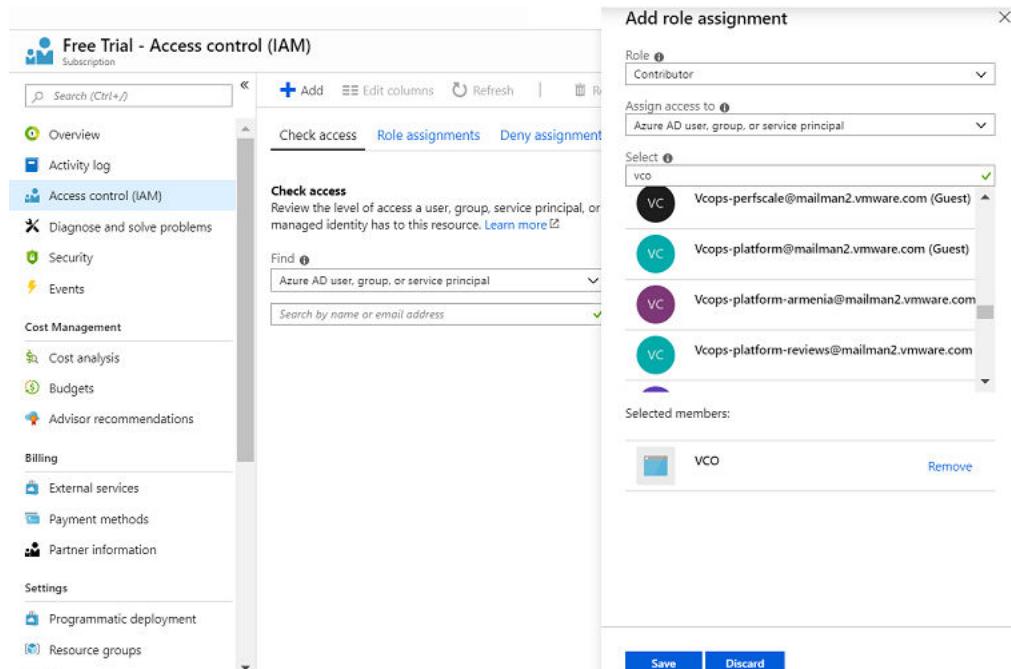
### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

### Procedure

- 1 Click **All Services** and search for **Subscriptions**.
- 2 From the list of subscriptions, select the subscription to which you want to assign your application. If you do not see the subscription that you are looking for, select **global subscriptions filter**. Make sure the subscription you want is selected for the portal.
- 3 Click **Access control (IAM)**.
- 4 Click **+Add > Add role assignment**.

The **Add role assignment** dialog box appears.



- 5 From the **Role** drop-down menu, select the **Contributor** role to assign to the application.

To allow the application to execute actions like **reboot**, **start** and **stop** instances, it is recommended that users assign the **Contributor** role to the App Registration.

- 6 From the **Assign access to** drop-down menu, select **Azure AD user, group, or service principal**.

By default, Azure AD applications are not displayed in the available options. To find your application, search for the name and select it.

- 7 Select **Save**.

#### Results

The application is assigned to the Contributor role and it appears in the list of users assigned to a role for that scope.

#### What to do next

- [Create a Client Secret](#)
- [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#)

## Register a Resource Provider

To download Virtual WAN Virtual Private Network (VPN) configurations, the SASE Orchestrator requires a Blob Storage Account that acts as an intermediary data store from where the configurations can be downloaded. The SASE Orchestrator aims to create seamless user experience by provisioning a transient storage account for each of the download task. To download VPN site configurations, you must manually register the **Microsoft.Storage** resource provider on your Azure Subscription. By default, the **Microsoft.Storage** resource provider is not registered on Azure Subscriptions.

To register a resource provider for your subscription:

#### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).
- Ensure you have the Contributor or Owner roles permission.

#### Procedure

- 1 Log in to your [Microsoft Azure](#) account.
- 2 Click **All Services** and search for **Subscriptions**.
- 3 From the list of subscriptions, select your subscription.

- 4 Under the **Settings** tab, select **Resource providers**.

PROVIDER	STATUS
Microsoft.Storage	Registering
Microsoft.StorageSync	NotRegistered

- 5 From the list of available resource providers, select **Microsoft.Storage**, and click **Register**.

#### Results

The resource provider is registered and configures your subscription to work with the resource provider.

#### What to do next

You can create the resources in Azure, for steps, see [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#).

## Create a Client Secret

Describes how to create a new client secret in Azure AD for the purpose of authentication.

To create a new client secret in Azure AD:

#### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

#### Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Select **Azure Active Directory > App registrations**.
- 3 On the **Owned applications** tab, click on your registered SASE Orchestrator application.

**4 Go to Certificates & secrets > New client secret.**

The **Add a client secret** screen appears.

**5 Provide details such as description and expiry value for the secret and click **Add**.**

### Results

The client secret is created for the registered application.

**Note** Copy and save the new client secret value to be used during the Cloud Subscription in SASE Orchestrator.

### What to do next

- Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity
- Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Gateway

## Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity

This section describes the procedures to configure Azure for integrating Azure Virtual WAN and SD-WAN Gateway to enable the branch-to-Azure VPN connectivity.

Before you begin to configure the Azure Virtual WAN and the other Azure resources:

- Verify that none of the subnets of your on-premises network overlap with the existing virtual networks that you want to connect to. Your virtual network does not require a gateway subnet and cannot have any virtual network gateways. For steps to create a virtual network, see [Create a Virtual Network](#).

- Obtain an IP address range for your Hub region and ensure that the address range that you specify for the Hub region does not overlap with any of your existing virtual networks that you connect to.
- Ensure you have an Azure subscription. If not, create a [free account](#).

For step-by-step instructions about the various procedures that need to be completed in the Azure portal side for integrating Azure Virtual WAN and SD-WAN Gateway, see:

- [Create a Resource Group](#)
- [Create a Virtual WAN](#)
- [Create a Virtual Hub](#)
- [Create a Virtual Network](#)
- [Create a Virtual Connection between VNet and Hub](#)

## Create a Resource Group

Describes how to create a resource group in Azure.

To create a resource group in Azure:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Click **All Services** and search for **Resource groups**.

- 3 Select **Resource groups** and click **+Add**.

The **Create a resource group** screen appears.

**Home** > **Resource groups** > Create a resource group

## Create a resource group

**Basics**   **Tags**   **Review + create**

**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

**Project details**

- \* Subscription [?](#) Free Trial
- \* Resource group [?](#) Sasi\_RG1

**Resource details**

- \* Region [?](#) (US) Central US

**Review + create**   < Previous   Next : Tags >

- 4 From the **Subscription** drop-down menu, select your Microsoft Azure subscription.
- 5 In the **Resource group** text box, enter a unique name for your new resource group.  
A resource group name can include alphanumeric characters, periods (.), underscores (\_), hyphens (-), and parenthesis (), but the name cannot end with a period.
- 6 From the **Region** drop-down menu, select the location for your resource group, where the majority of your resources will reside.
- 7 Click **Review+create** and then click **Create**.

## Results

A resource group is created and appears on the Azure portal dashboard.

## What to do next

Create an Azure Virtual WAN. For steps, see [Create a Virtual WAN](#).

## Create a Virtual WAN

Describes how to create a Virtual WAN in Azure.

To create a Virtual WAN in Azure:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).
- Ensure you have a resource group created to add the Virtual WAN.

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.

The **Microsoft Azure** home screen appears.

- 2 Click **All Services** and search for **Virtual WANs**.
- 3 Select **Virtual WANs** and click **+Add**.

The **Create WAN** screen appears.

## Create WAN

[Basics](#)   [Review + create](#)

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#)

### Project details

<b>Subscription *</b> 	<input type="text" value="Microsoft Azure Enterprise"/>	
<b>Resource group *</b> 		
<input type="text" value="MIL-AZAUSYD-PROD-ARG"/>		
<a href="#">Create new</a>		

### Virtual WAN details

<b>Resource group location *</b> 	<input type="text" value="Australia East"/>	
<b>Name *</b> 		
<input type="text" value="Velocloud_vWan"/>		
<b>Type</b> 		
<input type="text" value="Standard"/>		

- 4 From the **Subscription** drop-down menu, select your Microsoft Azure subscription.

- 5 From the **Resource group** drop-down menu, select your resource group to add the Virtual WAN.
- 6 From the **Resource group location** drop-down menu, select the location where the metadata associated with the Virtual WAN will reside.
- 7 In the **Name** text box, enter a unique name for your Virtual WAN.
- 8 From the **Type** drop-down menu, select **Standard** as the Virtual WAN type.
- 9 Click **Create**.

## Results

A Virtual WAN is created and appears on the Azure portal dashboard.

## What to do next

Create Virtual Hubs. For steps, see [Create a Virtual Hub](#).

# Create a Virtual Hub

Describes how to create a Virtual Hub in Azure.

To create a Virtual Hub in Azure:

## Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).
- Ensure that you have a resource group created to add the Azure resources.

## Procedure

- 1 Log in to your [Microsoft Azure](#) account.

The **Microsoft Azure** home screen appears.

- 2 Go to **All resources** and from the list of available resources, select the Virtual WAN that you have created.
- 3 Under the **Virtual WAN architecture** area, click **Hubs**.

**4 Click +New Hub.**

The **Create virtual hub** screen appears.

**Create virtual hub**

**Basics**   [Site to site](#)   [Point to site](#)   [ExpressRoute](#)   [Routing](#)   [Tags](#)   [Review + create](#)

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpngate). The hub is the core of your network in a region. There can only be one hub per Azure region. When you create a hub using Azure portal, it creates a virtual hub VNet and a virtual hub vpngateway. [Learn more](#)

**Project details**

The hub will be created under the same subscription and resource group as the vWAN.

\* Subscription: (Disabled) Free Trial  
└─ \* Resource group: Sasi\_RG

**Virtual Hub Details**

\* Region: Central US  
\* Name: Sasi\_Virtual\_Hub  
\* Hub private address space: 10.0.0.0/24

**Note:** Creating a hub with a gateway will take 30 minutes.

[Review + create](#)   [Previous](#)   [Next : Site to site >](#)

**5 In the Basics tab, enter the following Virtual Hub details.**

- From the **Region** drop-down menu, select the location where the Virtual Hub resides.
  - In the **Name** text box, enter the unique name for your Hub.
  - In the **Hub private address space** text box, enter the address range for the Hub in Classless inter-domain routing (CIDR) notation.
- 6 Click Next: Site to site >** and enable Site to site (VPN gateway) before connecting to VPN sites by selecting **Yes**.

**Note** A VPN Gateway is required for tunnel automation to work, otherwise it is not possible to create VPN connections.

### Create virtual hub

The screenshot shows the 'Create virtual hub' wizard on the 'Basics' tab. It includes fields for 'AS Number' (set to 65515) and 'Gateway scale units' (set to '1 scale unit - 500 Mbps x 2'). A note at the bottom states: 'Creating a hub with a gateway will take 30 minutes.'

- From the **Gateway scale units** drop-down menu, select a scaling value.

**7** Click **Review + Create**.

### Results

A Virtual Hub is created and appears on the Azure portal dashboard.

### What to do next

- Create Virtual Connection between Hubs and Virtual Networks (VNets). For steps, see [Create a Virtual Connection between VNet and Hub](#).
- If you do not have an existing VNet, you can create one by following the steps in [Create a Virtual Network](#).

## Create a Virtual Network

Describes how to create a Virtual Network in Azure.

To create a Virtual Network in Azure:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Click **All Services** and search for **Virtual networks**.

- 3 Select **Virtual networks** and click **+Add**.

The **Create virtual network** screen appears.

**Create virtual network**

\* Name: Sasi\_Virtual\_Network ✓

\* Address space: 10.0.0.0/24 ✓  
10.0.0.0 - 10.0.0.255 (256 addresses)

\* Subscription: Free Trial

\* Resource group: Sasi\_RG  
Create new

\* Location: (US) Central US

**Subnet**

\* Name: Sasi\_Virtual\_Subnet ✓

\* Address range: 10.0.0.0/24 ✓  
10.0.0.0 - 10.0.0.255 (256 addresses)

DDoS protection:  Basic  Standard

Service endpoints:  Disabled  Enabled

**Create**   [Automation options](#)

- 4 In the **Name** text box, enter the unique name for your virtual network.
- 5 In the **Address space** text box, enter the address range for the virtual network in Classless inter-domain routing (CIDR) notation.
- 6 From the **Subscription** drop-down menu, select your Microsoft Azure subscription.
- 7 From the **Resource group** drop-down menu, select your resource group to add the virtual network.
- 8 From the **Location** drop-down menu, select the location where the virtual network resides.
- 9 Under the **Subnet** area, enter the name and address range for the subnet.  
Do not make any changes to the other default settings of DDoS protection, Service endpoints, and Firewall.
- 10 Click **Create**.

## Results

A Virtual network is created and appears on the Azure portal dashboard.

### What to do next

Create Virtual Connection between Hubs and Virtual Networks (VNets). For steps, see [Create a Virtual Connection between VNet and Hub](#).

## Create a Virtual Connection between VNet and Hub

Describes how to create a virtual connection between Virtual Networks (VNets) and the Virtual Hub in a particular Azure region.

To create a virtual network connection between a VNet and a Virtual Hub in a particular Azure region:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).
- Ensure you have Virtual Hubs and Virtual Networks created.

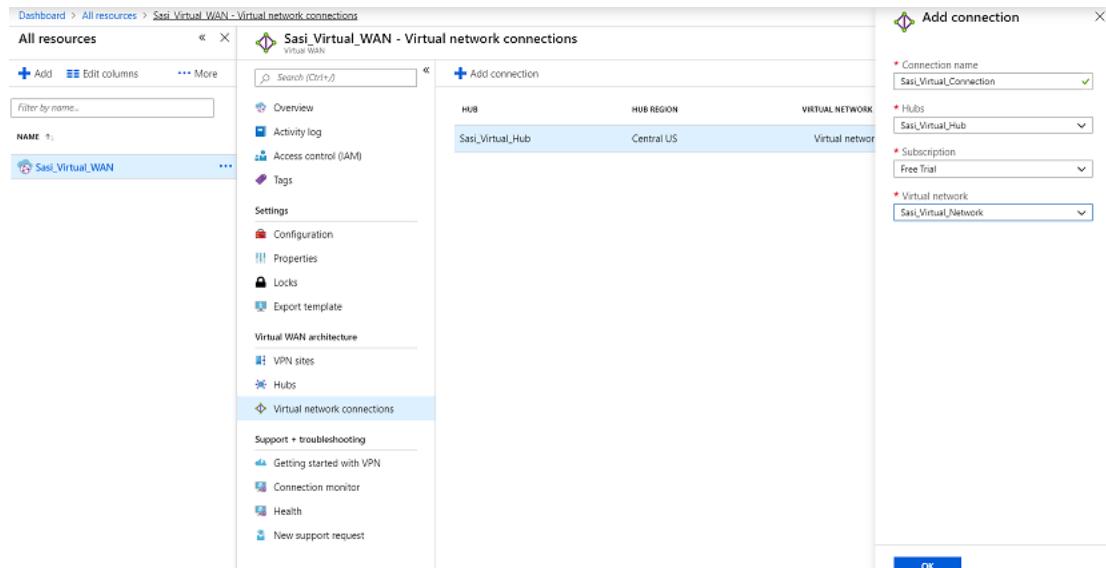
### Procedure

**1** Log in to your [Microsoft Azure](#) account.

The **Microsoft Azure** home screen appears.

- 2** Go to **All resources** and from the list of available resources, select the Virtual WAN that you have created.
- 3** Under the **Virtual WAN architecture** area, click **Virtual network connections**.
- 4** Click **+Add connection**.

The **Add connection** screen appears.



- 5 In the **Connection name** text box, enter the unique name for the virtual connection.
- 6 From the **Hubs** drop-down menu, select the Hub you want to associate with this connection.
- 7 From the **Subscription** drop-down menu, select your Microsoft Azure subscription.
- 8 From the **Virtual network** drop-down menu, select the virtual network you want to connect to this Hub.
- 9 Click **OK**.

#### Results

A peering connection is established between the selected VNet and the Hub.

#### What to do next

- [Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Gateway](#)

## Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Gateway

You can configure SASE Orchestrator for integrating Azure Virtual WAN and SD-WAN Gateway to enable the branch-to-Azure VPN connectivity.

---

**Note** By default, the Azure Virtual WAN feature is deactivated. To enable the feature, an Operator Super user must set the `session.options.enableAzureVirtualWAN` system property to true.

---

**Note** When using the Azure Virtual WAN Automation from SD-WAN Gateway feature, the Non SD-WAN Destination (NSD) tunnel only supports static routes. As a result, this feature is not currently compatible with BGP over IPsec.

---

Before you begin the SASE Orchestrator configuration for Azure Virtual WAN - SD-WAN Gateway automation, ensure you have completed all the steps explained in the [Prerequisite Azure Configuration](#) and [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#) sections.

For step-by-step instructions about the various procedures that need to be completed in the SASE Orchestrator for integrating Azure Virtual WAN and SD-WAN Gateway, see:

- [Configure API Credentials](#)
- [Configure a Non SD-WAN Destination of Type Microsoft Azure Virtual Hub](#)
- [Synchronize VPN Configuration](#)

To view the details of Non SD-WAN Destinations network services configured for an enterprise, see [Monitor Non SD-WAN Destinations](#).

## Associate a Microsoft Azure Non SD-WAN Destination to an SD-WAN Profile

After configuring a Non SD-WAN Destination of type **Microsoft Azure Virtual Hub** in SASE Orchestrator, you must associate the Non SD-WAN Destination to the desired Profile to establish the tunnels between SD-WAN Gateways and Microsoft Azure Virtual Hub.

To associate a Non SD-WAN Destination to a Profile, perform the following steps:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.  
The **Profiles** page appears.
- 2 Select a profile you want to associate your Microsoft Azure Non SD-WAN Destination with, and then click the **View** link in the **Device** column.
- 3 In the **Device** settings page, under **VPN** services, activate **Cloud VPN** by turning on the toggle button.

### Branch to Branch VPN (Transit & Dynamic)

Enable Branch to Branch VPN  
 Cloud Gateways  
 Hubs for VPN

Isolate profile  ⓘ

Enable Dynamic Branch to Branch VPN via:  
( ⓘ To activate this check box, deactivate Hub or Cluster Interconnect

### Edge to Non SD-WAN Sites

Enable Edge to Non SD-WAN via Gateway

		+ ADD	+ NEW DESTINATION	DELETE
<input type="checkbox"/>	Non SD-WAN Destinations via Gateway			
<input type="checkbox"/>	test			
1 item				

- 4 Under **Edge to Non SD-WAN Sites**, select the **Enable Edge to Non SD-WAN via Gateway** check box.
- 5 From the drop-down menu, select your Non SD-WAN Destination of type **Microsoft Azure Virtual Hub** to establish VPN connection between the branch and the Microsoft Azure Non SD-WAN Destination.
- 6 Click **Save Changes**.

## Results

A tunnel is established between the branch and the Microsoft Azure Non SD-WAN Destination.

## Edit a VPN Site

Describes how to add SD-WAN routes into the Azure network manually.

To add SD-WAN routes manually into the Azure network:

### Prerequisites

Ensure you have completed provisioning the Azure VPN sites at the SASE Orchestrator side.

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.
- The **Microsoft Azure** home screen appears.
- 2 Go to **All resources** and from the list of available resources, select the Virtual WAN that you have created.
- 3 Under the **Virtual WAN architecture** area, click **VPN sites**.
- 4 From the available list of VPN sites, select your VPN site (for example, *Non SD-WAN Destination name.primary*), that is added as a result of Non SD-WAN Destination provisioning step done using the SASE Orchestrator.
- 5 Click on the name of the selected VPN site and from the top of the next screen, select **Edit site**.

SITE	PUBLIC IP ADDRESS	STATUS	HUB	RESOU
Azure_Hub_USWEST1.primary	34.216.153.76	See hub association status	1 hubs	West
Azure_Hub_USWEST1.redund...	34.214.141.66	See hub association status	1 hubs	West
<b>Azure_India.primary</b>	35.164.28.19	<b>Updating</b>	Association needed	Centr
Azure_India.redundant	34.216.153.76	Updating	Association needed	Centr
velo2_uswest4.primary	34.216.153.76	All connected	Azure_Hub_East_US1	East
velo_uswest3.primary	34.214.141.66	See hub association status	1 hubs	East
velo_uswest3.redundant	35.164.28.19	See hub association status	1 hubs	East

- 6 In the **Private address space** text box, enter the address range for the SD-WAN routes.

**7 Click Confirm.**

Similarly, you can edit your Redundant VPN site by following the above steps.

---

**Note** Currently, Azure vWAN supports only Active/Active tunnel mode, and it does not have the provision to specify priority or primary tunnel to the VPN site (Primary and Redundant sites), and therefore load balancing will be done by Azure on equal cost multi-path routing. This may cause asymmetric traffic flow and might increase the latency for those flows. The workaround to avoid the asymmetric flow is to remove the SD-WAN Gateway redundancy on the Azure vWAN Hub NVS tunnel; however removing of redundant Gateway tunnel may not be acceptable for all deployments and needs to handle with caution.

---

## Synchronize VPN Configuration

After successful Non SD-WAN Destination provisioning, whenever there are changes in the endpoint IP address of the Azure Hub or static routes, you need to resynchronize Azure Virtual Hub and Non SD-WAN Destination configurations. Clicking the **Resync configuration** button in the **Non-VeloCloud Sites** area will automatically fetch the VPN configuration details from the Azure portal and will update the SASE Orchestrator local configuration.

## Configure SASE Orchestrator for Azure Virtual WAN IPsec Automation from SD-WAN Edge

You can configure SASE Orchestrator for integrating Azure Virtual WAN and SD-WAN Edge to enable the branch-to-Azure VPN connectivity directly from SD-WAN Edge.

---

**Note** When using the Azure Virtual WAN Automation from SD-WAN Edge feature, the Non SD-WAN Destination (NSD) tunnel only supports static routes. As a result, this feature is not currently compatible with BGP over IPsec.

---

Before you begin the SASE Orchestrator configuration for Azure Virtual WAN - SD-WAN Edge automation, ensure you have completed all the steps explained in the [Prerequisite Azure Configuration](#) and [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#) sections.

For step-by-step instructions about the various procedures that need to be completed in the SASE Orchestrator side for integrating Azure Virtual WAN and SD-WAN Edge, see:

- [Configure API Credentials](#)
- [Configure a Non-VMware SD-WAN Site of Type Microsoft Azure via Edge](#)
- [Configure Cloud VPN for Profiles](#)
- [Associate a Microsoft Azure Non SD-WAN Destination to an SD-WAN Edge and Add Tunnels](#)

## Associate a Microsoft Azure Non SD-WAN Destination to an SD-WAN Edge and Add Tunnels

After configuring a Non SD-WAN Destination of type **Microsoft Azure Virtual Hub** from SD-WAN Edge, you must associate the Non SD-WAN Destination to an Edge and configure tunnels to establish IPsec tunnels between the Edge and Microsoft Azure Virtual Hub.

At the Edge level, to associate a Non SD-WAN Destination to an SD-WAN Edge, perform the following steps:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
- 2 Select an Edge you want to associate your Microsoft Azure Non SD-WAN Destination with, and then click the **View** link in the **Device** column.
- 3 In the **Device** settings page, under **VPN** services, expand **Non SD-WAN Destinations via Edge**, and then select the **Override** check box.
- 4 Select the **Enable Non SD-WAN via Edge** check box.

Service		Link			Action		
<input type="checkbox"/>	Name	Automation for all public WAN Links	Enable Service	Enable Tunnel	Destination Primary Public IP	Destination Secondary Public IP	Action
<input type="checkbox"/>	test123	N/A	<input checked="" type="checkbox"/> Enabled		No sites added		<a href="#">+</a>

1 item

- 5 From the **Name** drop-down menu, select your **Microsoft Azure Virtual Hub** network service to establish VPN connection between the branch and the Microsoft Azure Non SD-WAN Destination.

- 6 To configure tunnels for the Edge, under **Action**, click the **+** link. The **Add Tunnel** dialog box appears.

Add Tunnel	
Public WAN Link * ⓘ	169.254.6.2
Local Identification Type	IPv4
Local Identification * ⓘ	169.254.6.2
PSK *	..... <span style="color: blue;">(eye icon)</span>
Destination Primary Public IP *	34.56.43.12
Destination Secondary Public IP	
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; font-weight: bold;">SAVE</span>	

- a From the **Public WAN Link** drop-down menu, select a WAN link to establish IPsec tunnel and click **Save**.

For the WAN links to appear in the drop-down menu, the customer needs to first configure the WAN links for the Edges from the **Configure > Edges > Device > WAN Settings** page, and wait for the Edge's WAN links to come up with the valid public IPs. The link's public IP is used as the Local Identification value of the tunnel. You can select only the WAN link with Public IP address.

A tunnel is automatically established between the Edge and the Microsoft Azure Non SD-WAN Destination via Azure APIs. After that the Orchestrator sends the tunnel configuration to the Edge to establish tunnel to the Azure service. Note that the automation for each tunnel takes about 1 to 5 minutes to complete. Once the tunnel automation is complete, you are able to view the details of configured tunnel and Public WAN link.

- b Once tunnels are created, you can perform the following actions at the Edge level:
  - Update a tunnel - When the Edge Public WAN link IP address of the tunnel changes, the Orchestrator automatically enqueues automation job to update the Azure VPN site link and the VPN tunnel configurations. Under **Action**, click the + link to view the tunnel settings such as PSK.
  - Delete a network service - Select a network service and click **Delete**.
  - Deactivate a network service - Under **Enable Service** column, deselect the check box to deactivate a specific network service.

#### 7 Click **Save Changes**.

##### What to do next

You can monitor the automated deployment status of the Microsoft Azure Non SD-WAN Destinations configured for an Enterprise from the **Monitor > Network Services > Non SD-WAN Destinations via Edge** page in the **SD-WAN** service of the Enterprise portal. See [Monitor Non SD-WAN Destinations](#).

## Monitor Non SD-WAN Destinations

You can view the details of Non SD-WAN Destinations configured for the Enterprise from the **Monitor > Network Services** page in the **SD-WAN** service of the Enterprise portal.

In the **Network Services** page, you can view:

- Non SD-WAN Destinations via Gateway - Displays the configured Non SD-WAN Destinations along with the other configuration details such as Name of the Non SD-WAN Destination, Public IP Address, Status of the Non SD-WAN Destination, Status of the tunnel, Number of profiles and Edges that use the Non SD-WAN Destination, Last contacted date and time, and Number of related state change Events.
- Non SD-WAN Destinations via Edge - Displays the configured Non SD-WAN Destinations along with the other configuration details such as Name of the Non SD-WAN Destination, Public IP Address, Status of the tunnel, Number of profiles and Edges that use the Non SD-WAN Destination, Last contacted date and time, and Deployment status.

---

**Note** Tunnel deployment status monitoring is only supported for **Non SD-WAN Destinations via Edge** network service.

To monitor the automation deployment status of Microsoft Azure Non SD-WAN Destinations via Edge:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Network Services**.  
The **Network Services** page appears.
- 2 Under **Non SD-WAN Destinations via Edge**, click the link in the **Deployment Status** column to view the deployment status of the Non SD-WAN Destinations.

The screenshot shows the VMware SD-WAN Network Services interface. At the top, there are tabs for "Non SD-WAN Destinations via Gateway" and "Non SD-WAN Destinations via Edge". The "Non SD-WAN Destinations via Edge" tab is selected, showing a table with columns: Name, Public IP, Tunnel Status, Used By, Last Contact, and Deployment Status. One entry is listed: "test123" with Public IP "54.123.4.123", Tunnel Status "0", and Deployment Status "N/A". Below this table is a "COLUMNS" section with a "1 item" count. To the right of the table is a small sidebar with columns: Subnet, Description, and Advertise.

**General**

Name	test123
Tunnel Protocol	IPSec
Type	Generic IKEv1 Router (Route Based VPN)
Tunnel Mode	Active/Active

**Primary VPN Gateway**

Public IP:	54.123.4.123
IKE Encryption	Auto
IPSEC Encryption	AES 128 CBC
DH Group	2
PFS	deactivated
IKE Hash	Auto
IPSEC Hash	SHA 256
DPD Timeout Timer(sec)	20

**Secondary VPN Gateway**

Public IP:	
Keep Tunnel Active	<input type="checkbox"/>
Tunnel settings are same as Primary VPN Gateway	<input checked="" type="checkbox"/>
IKE Encryption	Auto
IPSEC Encryption	AES 128 CBC
DH Group	2
PFS	deactivated
IKE Hash	Auto
IPSEC Hash	SHA 256
IKE SA Lifetime(min)	1440
IPsec SA Lifetime(min)	480
DPD Timeout Timer(sec)	20

The following are the seven different states for an Edge action:

- Enqueued - The Edge action is enqueued.
- Pending - The Edge action is in this state as it waits for a backend worker process to pick it up and start working on it.
- Notified - The Edge action is in this state after a backend worker process picks up the Edge action and starts working on it.
- Completed - The Edge action is in this state if the Edge action task is successfully completed.
- Errorred - The Edge action is in this state if an error has occurred.
- Timed Out - The Edge action is in this state if it takes more than the expected amount of time to complete the Edge action task.
- Pending Delete - The Edge action is in this state if it is pending deletion.

# Azure Accelerated Networking Support for Virtual Edges

13

Azure accelerated networking support is available for Virtual Edges in the 5.4 release. This document provides detailed instructions on how to enable, disable, and verify accelerated networking for Virtual Edges, as well as providing support and host servicing details.

Accelerated Networking is Azure's implementation of single root I/O virtualization (SR-IOV), a standard that allows a physical PCIE device to appear as multiple virtual devices (virtual functions). When Accelerated Networking is enabled on an interface of a VMware SD-WAN Edge on Azure, SR-IOV support for Mellanox ConnectX-4 and ConnectX-5 Network Interface Cards (NICs) is automatically enabled in the Edge Virtual Machine (VM).

---

**Note** The SR-IOV support for Mellanox ConnectX-4 and ConnectX-5 NICs is only available for the VMware SD-WAN Edge on Azure in the 5.4 release.

---

Read the following topics next:

- [Azure Instance Support](#)
- [Enable or Disable Azure Accelerated Networking](#)
- [Verifying Accelerated Networking](#)
- [Azure Host Servicing](#)

## Azure Instance Support

The following table lists instance types that support the Accelerated Networking functionality.

Table 13-1. Accelerated Networking Support for Instance Types

Software Version	Instance Types
Edge Software 5.4 or later	Standard_D3_v2
	Standard_D4_v2
	Standard_D5_v2
	Standard_D4_v5

**Table 13-1. Accelerated Networking Support for Instance Types (continued)**

Software Version	Instance Types
	Standard_D8_v5
	Standard_D16_v5

## Enable or Disable Azure Accelerated Networking

This section provides links for detailed instructions on the different ways to enable and disable Azure Accelerated Networking.

Accelerated Networking can be enabled or disabled via the following locations:

- Azure portal
- Azure CLI or Azure PowerShell

Click the following section links for instructions on how to enable and disable Accelerated Networking via the Azure portal and the Azure CLI or Azure PowerShell.

- [Enable Accelerated Networking](#)
- [Disable Accelerated Networking](#)

### Enable Accelerated Networking

Accelerated Networking can be enabled via the Azure portal or via the Azure CLI. See this section for detailed instructions.

#### Enable Accelerated Networking

Azure requires that an existing Virtual Machine (VM) be stopped/deallocated before Accelerated Networking is enabled on any Network Interface Card (NIC). For more information, see:

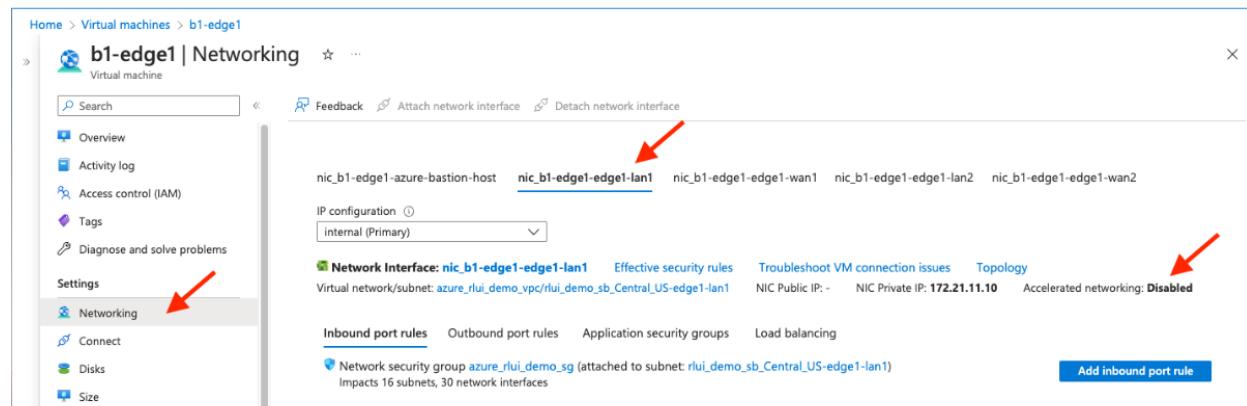
<https://learn.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli>

There are two ways to enable Accelerated Networking, via the Azure portal or via the Azure CLI. For detailed instructions for both, see the sections below.

#### Enable Accelerated Networking Via Azure Portal

To enable Accelerated Networking on an interface of an existing VM, follow the steps below, and see the image below for more information.

- 1 Stop/deallocate the VM.
- 2 Change the setting of accelerated networking to **Enabled**.
- 3 Restart the VM.



**Important** To fully benefit from the Accelerated Networking feature, enable it on all interfaces of the VM.

After the VM restarts, if the NIC model type allotted to the interface is not Mellanox ConnectX4 or ConnectX5, accelerated networking support for the interface is not activated by the Edge VM. As a troubleshooting effort, change the NIC model, stop/deallocate the VM, and then restart the VM.

**Note** You must stop the VM before you enable the Accelerated Networking support.

### Enable Accelerated Networking via Azure CLI

Follow the steps below to enable Accelerated Networking via the Azure CLI. For more information, reference the following: <https://learn.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli?tabs=windows#enable-accelerated-networking-on-individual-vms-or-vms-in-availability-sets>

1 Deallocate resources of the VM.

```
az vm deallocate --resource-group <myResourceGroup> --name <myVm>
```

2 Enable Accelerated Networking on the NIC.

```
az network nic update \
--name <myNic> \
--resource-group <myResourceGroup> \
--accelerated-networking true
```

3 Restart the VM.

```
az vm start --resource-group <myResourceGroup> --name <myVm>
```

### Disable Accelerated Networking

There are two options to disable Accelerated Networking, via the Azure portal or via the Azure CLI. See the sections below for detailed instructions.

## Disable Accelerated Networking

To disable Accelerated Networking, choose one of the two options described in the sections below.

### **Accelerated Networking Disabled Via Azure Portal**

To disable Accelerated Networking on an interface of an existing Virtual Machine (VM):

- 1 Stop/deallocate the VM.
- 2 Change the setting of accelerated networking to disabled or false.
- 3 Restart the VM.

### **Accelerated Networking disabled via Azure CLI**

- 1 Deallocate resources of the VM.

```
az vm deallocate --resource-group <myResourceGroup> --name <myVm>
```

- 2 Disable Accelerated Networking on the Network Interface Card (NIC).

```
az network nic update \
--name <myNic> \
--resource-group <myResourceGroup> \
--accelerated-networking false
```

- 3 Restart the VM.

```
az vm start --resource-group <myResourceGroup> --name <myVm>
```

## Verifying Accelerated Networking

This section describes detailed instructions on how to verify Accelerated Networking.

To verify that Accelerated Networking is enabled on the Edge, log into the Edge Virtual Machine (VM) and run "lspci" from the command line as described below.

```
edge:b1-edge1:~# lspci
0000:00:00.0 Host bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge (AGP
disabled) (rev 03)
0000:00:07.0 ISA bridge: Intel Corporation 82371AB/EB/MB PIIX4 ISA (rev 01)
0000:00:07.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
0000:00:07.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 02)
0000:00:08.0 VGA compatible controller: Microsoft Corporation Hyper-V virtual VGA
0fcf:00:02.0 Ethernet controller: Mellanox Technologies MT27710 Family [ConnectX-4 Lx Virtual
Function] (rev 80)
```

8f67:00:02.0 Ethernet controller: Mellanox Technologies MT27710 Family [ConnectX-4 Lx Virtual Function] (rev 80)

9b19:00:02.0 Ethernet controller: Mellanox Technologies MT27710 Family [ConnectX-4 Lx Virtual Function] (rev 80)

9b46:00:02.0 Ethernet controller: Mellanox Technologies MT27710 Family [ConnectX-4 Lx Virtual Function] (rev 80)

This feature does not support the Mellanox ConnectX-3 as it is not managed by the mlx5\_core driver . If the Edge VM is assigned the ConnectX-3 Network Interface Cards (NICs) by Azure, the Edge will behave as it behaves today without the Accelerated Networking support.

## Azure Host Servicing

This section describes detailed instructions for Azure Host Servicing.

The Azure Accelerated Networking support for Virtual Edges on Azure adds the DPDK failsafe/TAP/MLX PMD model. When Azure host maintenance is performed, the SR-IOV VFs might be temporarily removed and added back later.

Reference the following for more information: <https://learn.microsoft.com/en-us/azure/virtual-network/accelerated-networking-how-it-works#azure-host-servicing>

The events are logged by the kernel and can be viewed in the output of dmesg. They can also be viewed in /var/log/messages:

```
edge:b3-edge1:~# egrep 'VF registering|VF unregistering' /var/log/messages
```

```
2023-07-25T22:06:11.903 INFO kern kernel:[ 11.091250] hv_netvsc
000d3a92-2dba-000d-3a92-2dba000d3a92 eth1: VF registering: eth5
```

```
2023-07-25T22:06:12.049 INFO kern kernel:[ 11.237233] hv_netvsc
000d3a92-245f-000d-3a92-245f000d3a92 eth2: VF registering: eth6
```

```
2023-07-25T22:06:12.208 INFO kern kernel:[ 11.396127] hv_netvsc
000d3a92-2178-000d-3a92-2178000d3a92 eth3: VF registering: eth7
```

```
2023-07-25T22:06:12.362 INFO kern kernel:[ 11.549624] hv_netvsc
000d3a92-218a-000d-3a92-218a000d3a92 eth4: VF registering: eth8
```

```
2023-07-25T22:30:09.188 INFO kern kernel:[ 1448.376507] hv_netvsc
000d3a92-2178-000d-3a92-2178000d3a92 eth3-hv: VF unregistering: eth7
```

```
2023-07-25T22:30:14.390 INFO kern kernel:[ 1453.577954] hv_netvsc
000d3a92-218a-000d-3a92-218a000d3a92 eth4-hv: VF unregistering: eth8
```

```
2023-07-25T22:30:19.380 INFO kern kernel:[ 1458.568168] hv_netvsc
000d3a92-2dba-000d-3a92-2dba000d3a92 eth1-hv: VF unregistering: eth5
```

```
2023-07-25T22:30:26.555 INFO kern kernel:[ 1465.742626] hv_netvsc
000d3a92-245f-000d-3a92-245f000d3a92 eth2-hv: VF unregistering: eth6
```

The HOTPLUG OUT events are reported on the VMware SD-WAN Orchestrator, as shown in the image below.

The screenshot shows the VMware SD-WAN Orchestrator web interface. The top navigation bar includes 'Customer' (3-site-public-cloud), 'SD-WAN', and a dropdown for 'Events'. The left sidebar has sections for Monitor, Configure, Diagnostics, and Service Settings, with 'Events' currently selected. The main content area is titled 'Events' and shows a table of recent events. The table has columns for Event, User, Segment, Edge, Severity, Time, and Message. The events listed are all 'EDGE DEVICE HOTPLUG OUT' events, mostly marked as 'Alert' (red dot) and occurring on 'b3-edge1'. The messages describe SR-IOV VF hotplugging out.

Event	User	Segment	Edge	Severity	Time	Message
EDGE DEVICE HOTPLUG OUT			b3-edge1	● Alert	Jul 25, 2023, 6:30:28 PM	Device cda3:00:02.0 (SR-IOV VF for eth2) was hotplugged out
Edge Physical Link Down			b3-edge1	● Info	Jul 25, 2023, 6:30:26 PM	Edge WAN link GE7 is down
EDGE DEVICE HOTPLUG OUT			b3-edge1	● Alert	Jul 25, 2023, 6:30:20 PM	Device 2c20:00:02.0 (SR-IOV VF for eth1) was hotplugged out
Edge Physical Link Down			b3-edge1	● Info	Jul 25, 2023, 6:30:19 PM	Edge WAN link GE6 is down
EDGE DEVICE HOTPLUG OUT			b3-edge1	● Alert	Jul 25, 2023, 6:30:15 PM	Device cd79:00:02.0 (SR-IOV VF for eth4) was hotplugged out
EDGE DEVICE HOTPLUG OUT			b3-edge1	● Alert	Jul 25, 2023, 6:30:10 PM	Device fcb0:00:02.0 (SR-IOV VF for eth3) was hotplugged out

The Edge continues running during the Azure Host maintenance and the Paths stay up.

When the SR-IOV VFs are added back after Azure host maintenance is complete, the events can be viewed in the output of dmesg or in /var/log/messages.

```
edge:b3-edge1:~# egrep 'VF registering|VF unregistering' /var/log/messages
```

...

```
2023-07-25T22:31:23.137 INFO kern kernel:[ 1522.324791] hv_netvsc
000d3a92-2dba-000d-3a92-2dba000d3a92 eth1-hv: VF registering: eth5
```

```
2023-07-25T22:31:28.381 INFO kern kernel:[ 1527.568576] hv_netvsc
000d3a92-2178-000d-3a92-2178000d3a92 eth3-hv: VF registering: eth6
```

```
2023-07-25T22:31:33.416 INFO kern kernel:[ 1532.604181] hv_netvsc
000d3a92-245f-000d-3a92-245f000d3a92 eth2-hv: VF registering: eth7
```

```
2023-07-25T22:31:38.468 INFO kern kernel:[ 1537.656531] hv_netvsc
000d3a92-218a-000d-3a92-218a000d3a92 eth4-hv: VF registering: eth8
```

The HOTPLUG IN events are reported on the VMware SD-WAN Orchestrator.

The screenshot shows the VMware SD-WAN Orchestrator web interface. The top navigation bar includes 'Customer' (3-site-public-cloud), 'SD-WAN', and a dropdown for 'Events'. The left sidebar has sections for Monitor, Configure, Diagnostics, and Service Settings, with 'Events' currently selected. The main content area is titled 'Events' and shows a table of recent events. The table has columns for Event, User, Segment, Edge, Severity, Time, and Message. The events listed are all 'EDGE DEVICE HOTPLUG IN' events, mostly marked as 'Alert' (red dot) and occurring on 'b3-edge1'. The messages describe SR-IOV VF hotplugging in.

Event	User	Segment	Edge	Severity	Time	Message
EDGE DEVICE HOTPLUG IN			b3-edge1	● Alert	Jul 25, 2023, 6:31:41 PM	Device cd79:00:02.0 (SR-IOV VF for eth4) was hotplugged in
EDGE DEVICE HOTPLUG IN			b3-edge1	● Alert	Jul 25, 2023, 6:31:36 PM	Device cda3:00:02.0 (SR-IOV VF for eth2) was hotplugged in
Edge Physical Link Up			b3-edge1	● Info	Jul 25, 2023, 6:31:34 PM	Edge WAN link GEB is up
EDGE DEVICE HOTPLUG IN			b3-edge1	● Alert	Jul 25, 2023, 6:31:31 PM	Device fcb0:00:02.0 (SR-IOV VF for eth3) was hotplugged in
Edge Physical Link Up			b3-edge1	● Info	Jul 25, 2023, 6:31:29 PM	Edge WAN link GE7 is up
EDGE DEVICE HOTPLUG IN			b3-edge1	● Alert	Jul 25, 2023, 6:31:25 PM	Device 2c20:00:02.0 (SR-IOV VF for eth1) was hotplugged in

# VMware SD-WAN in Azure Virtual WAN Hub Deployment

14

Read the following topics next:

- [About VMware SD-WAN in Azure Virtual WAN Hub Deployment](#)

## About VMware SD-WAN in Azure Virtual WAN Hub Deployment

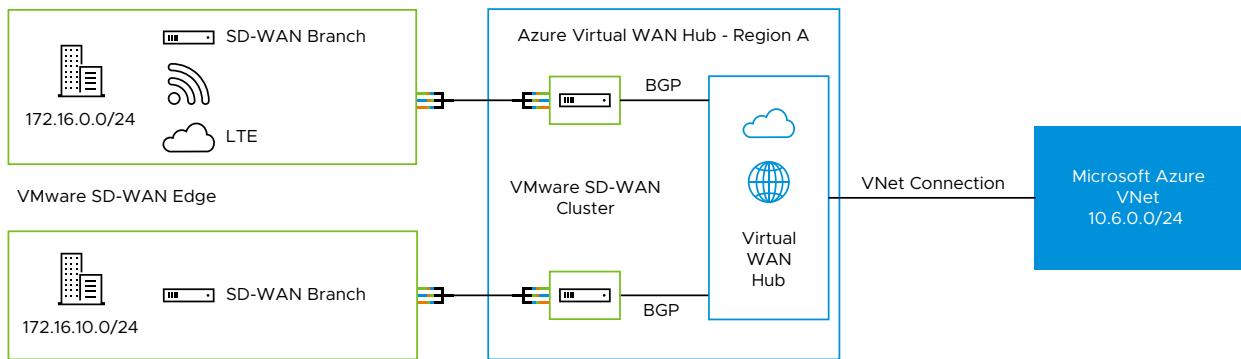
The VMware SD-WAN in Azure Virtual WAN (vWAN) Hub deployment describes the configurations that are required to manually deploy a Virtual SD-WAN Edge as a Network Virtual Appliance (NVA) in Azure vWAN Hub network.

### Overview

During cloud migration, there were lot of challenges on how to connect remote locations to Azure VNets in a simple, optimized, and secure way across myriad connectivity options. VMware SD-WAN addresses these problems by leveraging Dynamic Multipath Optimization™ (DMPO) technologies and distributed cloud gateway coverage across the globe. VMware SD-WAN transforms the unpredictable broadband transport to Enterprise-class quality connections, ensuring the application performance from remote locations to Azure Cloud.

To meet different deployment scenarios for customers who deploy Azure Virtual WAN, VMware SD-WAN have been progressively adding more capabilities to the solution. With this new integration, customers can now deploy VMware SD-WAN Edges directly inside Azure Virtual WAN hubs manually, resulting in an offering that natively integrates Azure Virtual WAN's customizable routing intelligence with VMware SD-WAN's optimized last-mile connectivity.

The following diagram illustrates the VMware SD-WAN and Azure vWAN NVA Manual Deployment scenario.



## Deploy VMware SD-WAN in Azure Virtual WAN Hub

To deploy VMware SD-WAN Edges in a Virtual Hub manually, you must have already created a Resource Group, virtual WAN (vWAN), and virtual Hub (vHUB) on the Azure side.

Configuration Steps:

### Prerequisites

Once the vWAN Hub is up and running and routing status is complete, you must meet the following prerequisites before proceeding with the Manual deployment of an Azure vWAN Network Virtual Appliance (NVA) via VMware SASE Orchestrator:

- Obtain Enterprise account access to VMware SASE Orchestrator.
- Obtain access to the Microsoft Azure portal with the appropriate IAM roles.
- Software image requirements for this deployment are as follows:
  - VMware SASE Orchestrator: 4.5.0 and above.
  - VMware SD-WAN Gateway: 4.5.0 and above.
  - VMware SD-WAN Edges: 4.2.1 and above.

### Procedure

- 1 In the Orchestrator, create a Virtual Edge by navigating to **Configure > Edges > New Edge**.
- 2 In the Orchestrator, once the Edges are created, change the interface settings for all Edges as follows:
  - Change GE1 interface to Route with Autodetect WAN overlay.
  - Change GE2 to Route with WAN overlay deactivated.

- The GE3 to GE8 interfaces are not used in this deployment.

**Note** You can configure Profiles with Virtual Edge interface settings as required by this integration so that you do not have to change interface settings after creating Virtual Edges on the Orchestrator.

**Note** If you attempt to downgrade an Edge from Release 4.2.1 to an earlier release, the Edge will become stuck in an activating loop.

- SSH access to VMware SD-WAN Azure NVAs is managed by the Azure support team. The Azure side enforces security policies that only allow the source IP address **168.63.129.16** to SSH to Azure Virtual Edges. To allow a Virtual Edge to accept SSH from this source IP, navigate to **Configure > Edges > Firewall > Edge Access > Support Access**, and add the IP address **168.63.129.16** under the **Allow the following IPs** field.



**Note** You can perform the Step 3 configuration on a Profile used by many or all of the Virtual Edges so you do not need to do it for each individual Virtual Edge.

For more details regarding this IP configuration, see <https://docs.microsoft.com/en-us/azure/virtual-network/what-is-ip-address-168-63-129-16>

- Copy the Orchestrator URL and the Activation Key of each Virtual Edge.

For example:

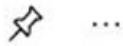
- vcoxx-usvi1.velocloud.net
- Activation Key1: XXXX:ZE8F:YYYY:67YT
- Activation Key2: XXXX:ZE8F:ZZZZ:67YT

- 5 Login to the [Azure](#) portal and search for the "VMware SD-WAN in vWAN" application in the Azure Market place. The **VMware SD-WAN in vWAN** managed application page appears. You can use this application to automate the deployment of Virtual Edges in Virtual WAN Hub.

Home >

## VMware SD-WAN in vWAN

VeloCloud



...



## VMware SD-WAN in vWAN

VeloCloud

Create

- 6 Click **Create** on the managed application and enter the following basic details:

[Home](#) > [VMware SD-WAN in vWAN \(preview\)](#) >

## Create VMware SD-WAN in vWAN

**Basics**    VMware SD-WAN in Virtual WAN    [Review + create](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="Microsoft Azure Sponsorship"/>
Resource group *	<input type="text"/> <a href="#">Create new</a>

**Instance details**

Region *	<input type="text" value="North Europe"/>
----------	---

**Managed Application Details**

Provide a name for your managed application, and its managed resource group. Your application's managed resource group holds all the resources that are required by the managed application which the consumer has limited access to.

Application Name *	<input type="text"/>
Managed Resource Group *	<input type="text" value="mrg-vmware_sdwan_in_vwan-preview-20210224133855"/>

- **Subscription:** The subscription which has the created Virtual WAN hub.
- **Resource Group:** Create a new resource group or select the existing one.
- **Region:** Select the region in which the Virtual WAN Hub is created. Virtual Edges will be deployed in that Virtual WAN Hub.
- **Application Name:** Enter a name for your managed application.
- **Managed Resource Group** - Provide the application's managed resource group. The managed resource group holds all the resources that are required by the managed application which the consumer has limited access to.

- 7 In the **VMware SD-WAN in Virtual WAN** tab, select Virtual WAN Hub in the selected region. The Virtual Edges will be deployed in this Hub.

[Home](#) > [VMware SD-WAN in vWAN \(preview\)](#) >

## Create VMware SD-WAN in vWAN

Basics	VMware SD-WAN in Virtual WAN	Review + create
Virtual WAN Hub	WestUSHub	
Scale unit *	2 Scale Units - 1.0 Gbps	
VMware SD-WAN Orchestrator *		
IgnoreCertErrors *	False	
ActivationKey for VMware SD-WAN Edge1 *		
ActivationKey for VMware SD-WAN Edge2 *		
BGP ASN *		
ClusterName *		

Once the customer selects a Virtual WAN Hub, the following information appears listing the BGP neighbor IP Addresses and the ASN of the Virtual WAN Hub. Make a note of this information as it is needed to configure BGP neighborships on the Orchestrator.

**i** BGP neighbor IPs ["10.101.32.4", "10.101.32.5"]Virtual WAN Hub BGP ASN 65515

- **Scale unit:** Select the scale as required.
- **VMware SD-WAN Orchestrator:** Paste the Orchestrator URL from Step 3.
- **IgnoreCertErrors:** Set this flag as False. Change this flag to True only if the Orchestrator URL cannot be used and the Orchestrator IP address must be provided.
- **ActivationKey for Edge1:** Paste the activation key from Step 3.
- **ActivationKey for Edge2:** Paste the activation key from Step 3.

- **BGP ASN:** The ASN that will be configured on the Virtual Edges in the VMware SASE Orchestrator. The following ASNs are reserved by Azure or IANA:
    - ASNs reserved by Azure:
      - Public ASNs: 8074, 8075, and 12076.
      - Private ASNs: 65515, 65517, 65518, 65519, and 65520.
    - ASNs [reserved by IANA](#):
      - 23456, 64496-64511, 65535-65551, and 429496729.
  - **ClusterName:** Enter a unique name for the deployment which does not include special characters such as #, @, \_, -, and so on.
- 8 After entering all the required fields, click **Review + create**.
- 9 The deployment process will start and takes approximately 10 to 15 minutes to complete. Once the deployment is complete, the Virtual Edges will connect and activate against the Orchestrator.

- 10 Once all of the Virtual Edges are connected to the Orchestrator, you need to configure static routes and BGP neighbors so that the Virtual Edges can connect to the Azure Virtual WAN Hub:

- a Configure Static Routes: Add /32 static routes sufficient that there is a unique route pointing to the respective GE2 Interface on each Virtual Edge. To add a static route, the Orchestrator requires a **next hop IP address**. Acquire the next hop IP address by running the Remote Diagnostic “Interface Status” test in the Remote Diagnostics UI page of the Orchestrator. Select the first IP address of the subnet assigned to GE2 and configure it as the next hop.

The following image shows an IP address assigned to GE2 as 10.101.112.6/25 and the first IP address of this subnet is 10.101.112.1, which is used to configure the static route on the Orchestrator.

The following is the output from **Test & Troubleshoot > Remote Diagnostics > Interface Status** diagnostic test.

Routed Interfaces										
Name	MAC Address	Link Detected	IP Address	Netmask	IPv6 Address	Speed	Autonegotiation	RX errors	TX errors	Collisions
GE1	00:22:48:06:81:2B	true	10.101.112.133	255.255.255.128		40000 Mbps, full duplex	on	0	0	0
GE2	00:22:48:06:88:45	true	10.101.112.6	255.255.255.128		40000 Mbps, full duplex	on	0	0	0

Two static routes are configured on the Edge to reach BGP neighbors as shown in the following screenshot.

The screenshot shows the 'Static Route Settings' page under the 'IPv4' tab. It lists two local routes:

Subnet	Source IP	Next Hop IP	Interface	VLAN	Cost	Preferred	Advertise	ICMP Probe	Description
10.101.32.5/32	N/A	10.101.112.1	GE2		0	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes		+ NEW Enter Descri...
10.101.32.4/32	N/A	10.101.112.1	GE2		0	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes		+ NEW Enter Descri...

2 items

- b BGP Neighbor Configuration: Configure BGP neighbors for each Virtual Edge as shown in the following diagram. Use BGP neighbor IPs and the ASN number as displayed in the information message in Step 7.

The screenshot shows the 'Neighbors' configuration page under the 'IPv4' tab. It lists two BGP neighbors:

Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options
10.101.32.5	65515	[None]	[None]	Max-Hop: 2 Local IP: <input type="text"/> Source Interface: Auto Uplink: <input type="checkbox"/> Allow AS: <input type="checkbox"/> Default Route: <input type="checkbox"/> Enable BFD: <input type="checkbox"/> Keep Alive: Example: 10 Hold Timer: Example: 10 Connect: Example: 10 MDS Auth: <input type="checkbox"/> MDS Password: <input type="password"/>
10.101.32.4	65515	[None]	[None]	Max-Hop: 2 Local IP: <input type="text"/> Source Interface: Auto Uplink: <input type="checkbox"/> Allow AS: <input type="checkbox"/> Default Route: <input type="checkbox"/> Enable BFD: <input type="checkbox"/> Keep Alive: Example: 10 Hold Timer: Example: 10 Connect: Example: 10 MDS Auth: <input type="checkbox"/> MDS Password: <input type="password"/>

Once static routes and BGP neighborships are configured, the Virtual Edges should begin learning routes from the Azure Virtual WAN Hub. BGP neighborship status can be verified under **Monitor > Network Services**.

- 11 (Optional) Add the Virtual Edges into a cluster. Go to **Configure > Network Services > Edge Cluster**, create a new cluster Hub and add the Virtual Edges into the cluster.

- 12 (Optional) To add a Virtual Network Connection with the Virtual Networks (vNETs) to the vHub, go to **Azure vWAN > Connectivity > Virtual network connections**.

Click on **Add Connection** and provide a Connection Name, Choose the Hub, Subscription, and Resource Group. Select the vNET and the associated Route table that needs to be connected to the Hub. For example, it is the ‘default’ route table in a vNET.

For the vWAN NVA Edge, the image is a 2 NIC Deployment, in other words the GE1 interface is not used as the ‘Management’ interface. This is unique to the vWAN NVA image. In the `cloud_init`, set the ‘management\_interface’ flag to ‘False’.

```
#cloud-config
password: Velocloud123
chpasswd: { expire: False }
ssh_pwauth: True
velocloud:
```

```

vce:
  management_interface: false
  vco: $vco
  activation_code: $velo2_token
  vco_ignore_cert_errors: $velo_ignore_cert_errors

```

On all other cloud Edges, the GE1 interface is allocated as a 'Management' interface and cannot be used for data traffic.

---

**Note** For Customers whose Azure vWAN Hub Routers are created with 'Cloud Services infrastructure', see [Hub Upgrade Instructions for VMware SD-WAN Edge Deployed as Azure vWAN NVA](#).

---

### Accessing the Command Line of Virtual Edges Deployed into an Azure vWAN vHub

Azure vWAN is operated as a managed service. Unlike other virtual machines deployed into Azure, vWAN does not offer the ability to associate a public key to the virtual machine (VM) when it is configured. Since Azure also does not allow password-based SSH authentication, this effectively renders the CLI of the vEdge unreachable.

To overcome these restrictions and access the vEdge's CLI for troubleshooting and operational purposes, the VMware SD-WAN's Secure Edge Access feature should be used. This will use the Orchestrator to create key-based, per-user SSH access to the vEdge's CLI.

Refer to the following documentation to enable Secure Edge Access:

[Access SD-WAN Edges Using Key-based Authentication with New Orchestrator UI](#)

---

**Note** During Secure Edge Access key creation process, specifying a password is listed as "optional." However, including a password is required to be configured to access Azure NVAs. The user will be prompted to provide the password during the SSH login process after first using key-based authentication.

---

## Hub Upgrade Instructions for VMware SD-WAN Edge Deployed as Azure vWAN NVA

This document is intended for customers who use VMware SD-WAN Edges in Azure and deploy them as Network Virtual Appliances (NVAs) in the Azure Virtual WAN (vWAN) Hub.

For more information,

see <https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#why-am-i-seeing-a-message-and-button-called-update-router-to-latest-software-version-in-portal>.

## Upgrade Instructions

Azure is deprecating its Cloud Services-based infrastructure, so the Virtual WAN team is upgrading their virtual routers from their current Cloud Services infrastructure to Virtual Machine Scale Sets based deployments. If you navigate to your Virtual WAN hub resource and see a message to upgrade your router to the latest version as shown in the following screenshot, click "**Update router to latest software version**" button to initiate router upgrade.

**Note** All newly created Virtual Hubs will be automatically deployed on the latest Virtual Machine Scale Sets-based infrastructure and do not require this upgrade.

The screenshot shows the Azure portal interface for managing a Virtual Hub named 'vhubcentral1'. The 'Overview' tab is selected. In the top right corner of the main content area, there is a red box highlighting the 'Update Router to the latest software version' button. Below this button, a warning message states: 'WARNING: Your Virtual Wan Hub router currently uses an old router version and all new Virtual WAN features will only be available on our latest version from April 30. To learn more, please visit aka.ms/vwanVMS'.

After clicking "**Upgrade Router to the latest software version**", a message will indicate that this operation must be performed during a maintenance window.

The screenshot shows the Azure portal interface with a modal dialog box titled "Update Router to the latest software version". The dialog contains a message about updating the router to support various infrastructure fixes, including support for Availability Zone (AZ), if supported in a particular region. It recommends performing the task at offline hours during a maintenance window. At the bottom of the dialog, there are two buttons: "Confirm" (highlighted with a blue box) and "Cancel".

The Hub Status would display "**Updating**" and the Routing State as "**Provisioning**". This process will take approximately 30 to 60 minutes to complete.

**vhubcentral1** Virtual HUB

**Overview**

**Essentials**

Name: vhubcentral1	Router version: Update Router to the latest software version
Resource group: vhub-testing	Routing status: Provisioning
Tags: Tags	Hub routing preference: ExpressRoute
Hub status: Updating	Metrics: View in Azure Monitor

Private address space: 172.17.0.0/16

**See more**

- Virtual network connections: vNet connections: 0
- VPN (Site to site): No gateway (Create)
- User VPN (Point to site): No gateway (Create)
- ExpressRoute: No gateway (Create)
- Azure Firewall: No firewall (Create)
- Network Virtual Appliance: No gateway (Create)

After successful completion of the router update, the Hub Status should display "**Succeeded**" and the Routing State should display "**Provisioned**" as shown in the following screenshot.

**vhubcentral1** Virtual HUB

**Overview**

**Essentials**

Name: vhubcentral1	Routing status: Provisioned
Resource group: vhub-testing	Hub routing preference: ExpressRoute
Tags: Tags	Metrics: View in Azure Monitor
Hub status: Succeeded	

Private address space: 172.16.0.0/16

**See more**

- Virtual network connections: vNet connections: 0
- VPN (Site to site): No gateway (Create)
- User VPN (Point to site): No gateway (Create)
- ExpressRoute: No gateway (Create)
- Azure Firewall: No firewall (Create)
- Network Virtual Appliance: No gateway (Create)

IP addresses are represented in the Virtual Hub's resource JSON as the `virtualRouterIps` field. Alternatively, you can find it in the **Virtual Hub > BGP Peers** menu.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a tree view with 'vhub-testing-vwan' selected, followed by 'vhubcentral1'. Under 'vhubcentral1', 'BGP Peers' is selected. The main content area shows the 'Essentials' section for 'vhubcentral1'. It lists 'Name : vhubcentral1' and 'Location : West Central US'. Below this is a table with columns 'Name', 'ASN', 'IPv4 Address', and 'Virtual Network connection'. A search bar at the top is empty. There are buttons for '+ Add' and 'Refresh'. On the right, there's a 'JSON View' link and a user profile icon.

Copy the IP Addresses. For example, in this case the IP addresses are 172.16.32.8 and 172.16.32.9. These are the IP addresses on the Virtual Hub that the BGP Peers (VMware SD-WAN NVA) will need to be configured.

On the Orchestrator, the Virtual Edge BGP connections to the Virtual Hub will be displayed as Down, either in Connect or Active state. To configure BGP neighbors for Virtual Edges, see [BGP Neighbor Configuration](#).

Before configuring BGP neighbors on the Virtual Edge, static routes must be configured to allow the Virtual Edges to connect to the Azure Virtual WAN Hub. See [Static Routes Configuration](#).

## Static Routes Configuration

To configure static routes, add sufficient /32 static routes to ensure that there is a unique route pointing to the respective GE2 interface on each Virtual Edge. To add a static route, the Orchestrator requires a next-hop IP address. The next hop IP address can be obtained by running the Remote Diagnostic “Interface Status” test in the Remote Diagnostics UI page of the Orchestrator. Select the first IP address of the subnet assigned to GE2 and configure it as the next hop.

The following image shows an IP address assigned to GE2 as 172.16.112.5/25, with the first IP address of this subnet being 172.16.112.1. This IP address is used to configure the static route on the Orchestrator.

The following is the output from **Test & Troubleshoot > Remote Diagnostics > Interface Status** diagnostic test.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'Orchestrator' (selected), 'TbanPM tbanPLM', 'SD-WAN', and icons for help, user, and menu. The main content area has tabs for 'Monitor', 'Configure', 'Diagnostics' (selected), and 'Service Settings'. A sidebar on the left shows 'Diagnostics' selected, with options for 'Remote Diagnostics', 'Remote Actions', and 'Diagnostic Bundles'. The main content area displays 'nva1-azurevwan' status as 'Connected'. Under 'Diagnostics', the 'IPv6 Route Table Dump' section contains a table of routes:

Name	MAC Address	Link Detected	IP Address	Netmask	IPv6 Address	Speed	Autonegotiation	RX errors	TX errors	Collisions
GE1	00:22:48:5E:82:84	true	172.16.112.132	255.255.255.128		50000 Mbps, full duplex	on	0	0	0
GE2	00:22:48:5E:82:8A	true	172.16.112.5	255.255.255.128		50000 Mbps, full duplex	on	0	0	0
GE3		false	N/A	N/A	N/A	N/A	N/A	-1	-1	-1
GE4		false	N/A	N/A	N/A	N/A	N/A	-1	-1	-1
GE5		false	N/A	N/A	N/A	N/A	N/A	-1	-1	-1
GE6		false	N/A	N/A	N/A	N/A	N/A	-1	-1	-1

The 'Interface Status' section shows a table of physical interfaces:

Name	MAC Address	Link Detected	IP Address	Netmask	IPv6 Address	Speed	Autonegotiation	RX errors	TX errors	Collisions
GE1	00:22:48:5E:82:84	true	172.16.112.132	255.255.255.128		50000 Mbps, full duplex	on	0	0	0
GE2	00:22:48:5E:82:8A	true	172.16.112.5	255.255.255.128		50000 Mbps, full duplex	on	0	0	0
GE3		false	N/A	N/A	N/A	N/A	N/A	-1	-1	-1
GE4		false	N/A	N/A	N/A	N/A	N/A	-1	-1	-1
GE5		false	N/A	N/A	N/A	N/A	N/A	-1	-1	-1
GE6		false	N/A	N/A	N/A	N/A	N/A	-1	-1	-1

Test Duration: 3.002 seconds

Two static routes are configured on the Edge to reach BGP neighbors, as illustrated in the following screenshot.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'Orchestrator' (selected), 'TbanPM tbanPLM', 'SD-WAN', and icons for help, user, and menu. The main content area has tabs for 'Monitor', 'Configure' (selected), 'Diagnostics', and 'Service Settings'. A sidebar on the left shows 'Edge Configuration' selected, with options for 'Edges', 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control', 'Network Services', 'Cloud Hub', and 'Security Service Edge (SS...)'. The main content area displays 'nva1-azurevwan' status as 'Connected'. Under 'Configure', the 'Static Route Settings' section shows two static routes under the 'IPv4' tab:

Subnet *	Source IP	Next Hop IP *	Interface * ⓘ	VLAN	Cost *	Preferred ⓘ	Advertise ⓘ	ICMP Probe	Description
172.16.32.8/32	N/A	172.16.112.1	GE2 ⓘ	0	0	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	[None]	+ NEW Enter Des...
172.16.32.9/32	N/A	172.16.112.1	GE2 ⓘ	0	0	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	[None]	+ NEW Enter Des...

The 'NSD Routes' section shows a table with one row, which is collapsed:

Subnet	NSD	Gateway	Cost *	Preferred ⓘ	Advertise ⓘ
No NSD Routes configured					

Below the NSD Routes table, there are sections for DNS, OSPF, and BGP:

- DNS: Override ⓘ, On
- OSPF: Override ⓘ
- BGP: Override ⓘ, On

## BGP Neighbor Configuration

Configure BGP neighbors for each Virtual Edge as shown in the following screenshot. Use the BGP neighbor IPs and the ASN number as displayed in the virtual Hub BGP Peers output. Also, make sure to configure the BGP Max-Hop to 2.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes tabs for VMW Orchestrator, TbanPM/tbanPLM, SD-WAN, Monitor, Configure (selected), Diagnostics, Service Settings, and a Help icon.

The main content area is titled "nva1-azurevwan" and shows the "Configure" tab selected. Under "Edge Configuration", the "Edges" section is active. The "Neighbors" table lists two BGP neighbors:

Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options
172.16.32.8	65515	[None]	[None]	Max-Hop: 2 Local IP: IP Address Source Interface: Auto Uplink: <input type="checkbox"/> Allow AS: <input type="checkbox"/> Default Route: <input type="checkbox"/> Enable BFD: <input type="checkbox"/> Keep Alive: Example: 10 Hold Timer: Example: 10 Connect: <input type="checkbox"/> MD5 Auth: <input type="checkbox"/> MD5 Password: Password
172.16.32.9	65515	[None]	[None]	

\*Required

VIEW LESS

VIEW ALL

2 items

Once static routes and BGP neighbors have been configured, the Virtual Edges should begin learning routes from the Azure Virtual WAN Hub. You can verify the status of the BGP neighbors under **Monitor > Network Services**.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes tabs for VMW Orchestrator, TbanPM/tbanPLM, SD-WAN, Monitor (selected), Configure, Diagnostics, Service Settings, and a Help icon.

The main content area is titled "Routing" and shows the "BGP Edge Neighbor State" tab selected. The table displays the status of BGP neighbors:

Multicast Groups	PIM Neighbors	BGP Edge Neighbor State	BFD	BGP Gateway Neighbor State	Gateway Route Table			
nva1-azurevwan	Global Segment	172.16.32.5	● Removed	Sep 27, 2023, 7:25:58 AM 12 days ago	165	149	4	0
nva2-azurevwan	Global Segment	172.16.32.8	● Established	Sep 27, 2023, 8:18:27 AM 12 days ago	20,325	17,785	0	01w5d08h 3
nva1-azurevwan	Global Segment	172.16.32.8	● Established	Sep 27, 2023, 7:25:58 AM 12 days ago	20,305	17,782	0	01w5d07h 3
nva1-azurevwan	Global Segment	172.16.32.9	● Established	Sep 27, 2023, 8:23:43 AM 12 days ago	20,309	17,779	2	01w5d07h 3
nva2-azurevwan	Global Segment	172.16.32.9	● Established	Sep 27, 2023, 8:18:27 AM 12 days ago	20,285	17,785	0	01w5d08h 3

COLUMNS REFRESH

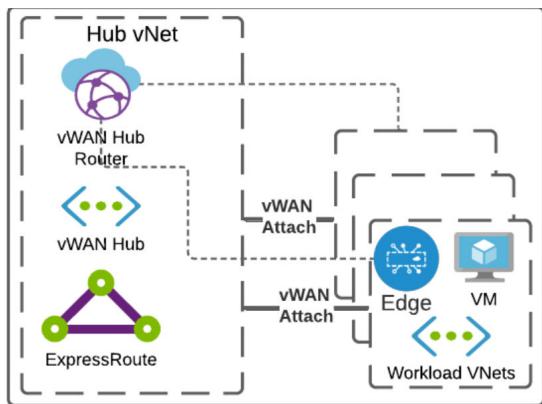
28 items

# SD-WAN Edge in a vNet Connecting to a vWAN Hub

15

This section outlines how to integrate an SD-WAN Edge in a traditional vNet with a vWAN Hub.

Integrate an SD-WAN Edge in a traditional vNet with a vWAN Hub is an alternative design to deploying Edges as a managed NVA inside of the vWAN Hub itself, resulting in a topology similar to the image below.



It is important to adhere to the following:

- You must deploy the Virtual Edge in a vNet.
- Azure Virtual WAN Hub must be deployed, i.e., the following must be created in the desired Azure region:
  - A Resource Group must be created.
  - A Virtual WAN (vWAN) must be created.
  - A Virtual Hub (vHUB) must be created.

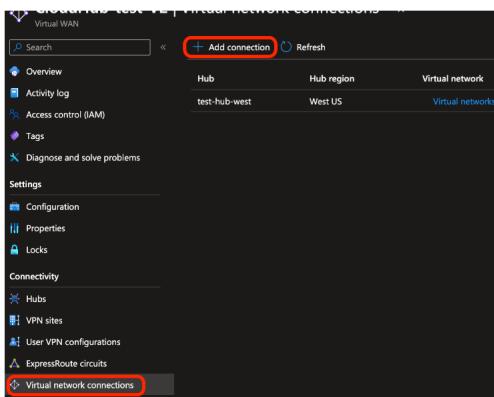
---

**Note** This section assumes that Edges, vWAN, and applicable Hub(s) have already been deployed as documented in the Azure Virtual Edge Deployment Guide and the section titled "Deploy VMware SD-WAN in Azure Virtual WAN Hub" in the Administration Guide.

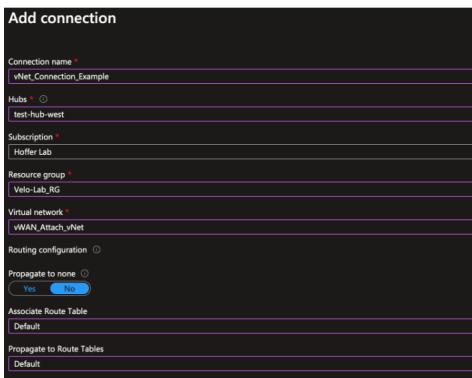
---

To integrate an SD-WAN Edge in a traditional vNet with a vWAN hub:

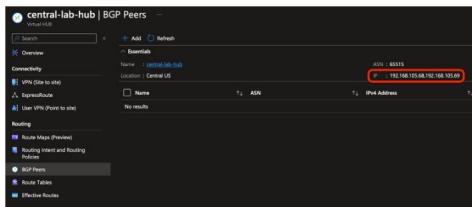
- 1 The vNET in which the Edge(s) are deployed must be attached to the vWAN Hub by navigating to the vWAN by selecting **Virtual network connections** and then selecting **Add connection**.



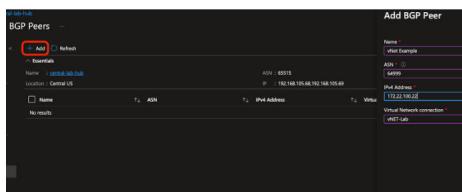
- When creating the connection, ensure that it is propagated to the default route table of the vWAN Hub you are connecting to; this ensures reachability for BGP peering.



- After the vNet attachment is complete, navigate to the vWAN hub and select **BGP Peers** from the Routing menu. Make a note of the IPs listed, as they will be the addresses that the Edge will peer with.



- Select **Add** and enter the ASN and LAN IP address of the SD-WAN Edge that the vWAN Hub router will peer with.



- The Hub router is not on the SD-WAN Edge's local subnet; therefore, a static route must be configured for the IPs recorded in Step 3 and pointed to the Gateway IP of the LAN subnet.

Subnet *	Source IP	Next Hop IP *	Interface *	VLAN	Cost *	Preferred	Advertise
192.168.105.68/31	N/A	172.22.100.17	GE2	0	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Yes	

- 6 Create BGP neighbors with each of the IP addresses recorded in Step 3 using Microsoft's ASN of 65515. As BGP multi-hop is used, the Max-Hop option must be set to "2."

Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options
192.168.105.68	65515	No Default	No Default	Max-Hop: 2 Local IP: <input type="text"/> IP Address: <input type="text"/> Source Interface: Auto Uplink: <input type="checkbox"/> Allow AS: <input type="checkbox"/> Default Route: <input type="checkbox"/>

- 7 Once the configuration is applied, the BGP neighborship should be established, Azure routes should be learned by the SD-WAN Edge, and SD-WAN overlay routes should be present in the Azure vWAN Default route table.

# CloudHub Automated Deployment of NVA in Azure vWAN Hub

16

Read the following topics next:

- [About CloudHub Automated Deployment of NVA in Azure Virtual WAN Hub](#)
- [CloudHub Deployment Prerequisites](#)
- [CloudHub Automated Deployment of Azure vWAN NVA via VMware SASE Orchestrator](#)

## About CloudHub Automated Deployment of NVA in Azure Virtual WAN Hub

The VMware SD-WAN and Azure virtual WAN (vWAN) NVA Automated Deployment guide describes the configurations that are required to automatically deploy a Virtual SD-WAN Edge as a Network Virtual Appliance (NVA) in Azure vWAN Hub network.

---

**Note** Automated Deployment of NVA in Azure Virtual WAN Hub is supported only for VMware Hosted Orchestrator.

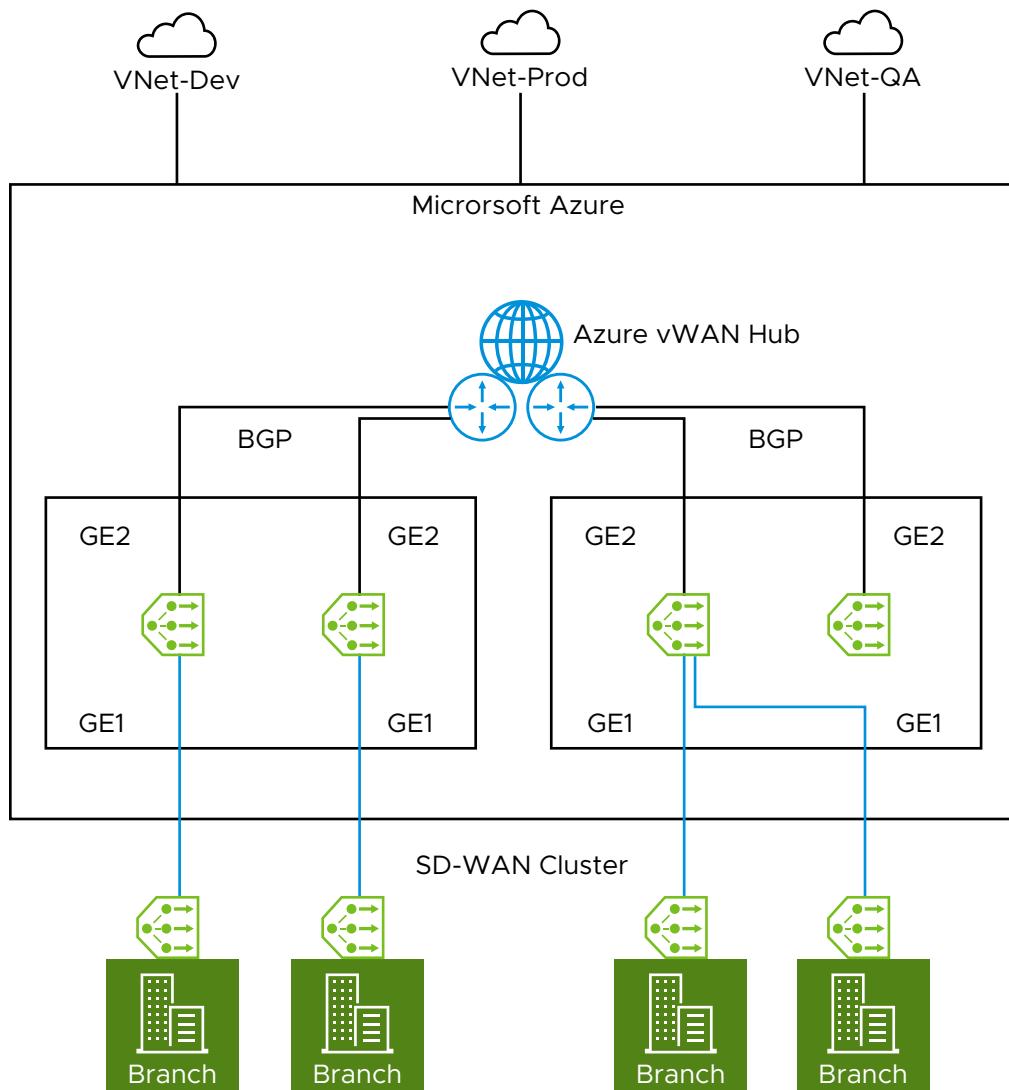
---

## Overview

During cloud migration, there were lot of challenges on how to connect remote locations to Azure VNets in a simple, optimized, and secure way across myriad connectivity options. VMware SD-WAN addresses these problems by leveraging Dynamic Multipath Optimization™ (DMPO) technologies and distributed cloud gateway coverage across the globe. VMware SD-WAN transforms the unpredictable broadband transport to Enterprise-class quality connections, ensuring the application performance from remote locations to Azure Cloud.

To meet different deployment scenarios for customers who deploy Azure Virtual WAN, VMware SD-WAN have been progressively adding more capabilities to the solution via automation. With this new integration, customers can now deploy VMware SD-WAN Edges directly inside Azure Virtual WAN hubs automatically, resulting in an offering that natively integrates Azure Virtual WAN's customizable routing intelligence with VMware SD-WAN's optimized last-mile connectivity.

The following diagram illustrates the VMware SD-WAN and Azure vWAN NVA Automated Deployment scenario.



## CloudHub Deployment Prerequisites

To use automatic deployment of VMware SD-WAN Edges as a Network Virtual Appliance (NVA) in Azure virtual WAN (vWAN) Hub, you must have already created Resource Group, vWAN, and virtual Hub (vHUB) on the Azure side. Once vWAN Hub is up and running and routing status is completed, you must ensure the following prerequisites are met before proceeding with the Automated deployment of Azure vWAN NVA via VMware SASE Orchestrator:

- Obtain Enterprise account access to VMware SASE Orchestrator.
- Obtain access to the Microsoft Azure portal with the appropriate IAM roles.
- Ensure you have already created Resource Group, vWAN and vHUB on the Azure side. For steps, see [Virtual WAN Documentation](#).
- Software image requirements for this deployment are as follows:
  - VMware SASE Orchestrator: 5.1.0.

- VMware SD-WAN Gateway: 4.2.1 and above.
- VMware SD-WAN Edges: 4.2.1 and above.

**Note** For more information about the supported regions of NVA in Virtual Hub, see <https://docs.microsoft.com/en-us/azure/virtual-wan/about-nva-hub#regions>.

## CloudHub Automated Deployment of Azure vWAN NVA via VMware SASE Orchestrator

To use Automated deployment of Azure vWAN NVA via VMware SASE Orchestrator, perform the following steps:

### Procedure

- 1 In the Orchestrator, ensure the Multi-Cloud Service (MCS) account is activated. You can verify that by checking the following system properties:
  - session.options.enableMcsServiceAccount
  - vco.system.configuration.data.mcsNginxRedirection

**Note** Contact the EdgeOps team to activate the MCS account for your Orchestrator.

Name	Value	Description	Last Modified
vco.system.configuration.data.mcsNginxRedirection	https://mcs.application-test-vmware.link	URL for Multicloud API	Oct 13, 2022, 10:22:30 AM
session.options.enableMcsServiceAccount	false		Oct 13, 2022, 9:54:14 AM

- 2 For an Enterprise user, once the MCS account is activated, you can access the MCS service by clicking **Cloud Hub** from the **Services** drop-down menu available at the top of the Orchestrator UI.

The **Cloud Hub** service page appears.

- 3 To deploy a NVA Edge in vWAN HUB network, perform the following two steps:
- Create a new credential
  - Create a new Cloud Hub
- 4 To create new credential, click **Configure > Credential > New Credential**. Provide all the required details and click **Create**.

**Add a new credential**

Name	AZDemo
Cloud Provider	AZURE
Client ID	84909115-dba6-4bf9-ad
Tenant ID	b39138ca-3cee-4b4a-a4
Client Secret	[REDACTED]
Subscription ID	a78bebe2-346c-4a95-9

Please enter the following information and click next to continue

**CANCEL** **CREATE** **VALIDATE**

Field	Description
Name	Enter a unique name for your Azure credential.
Cloud Provider	Select Azure as the Cloud Provider.
Client ID	Enter the Client ID of your Azure subscription.
Tenant ID	The ID for an Azure Active Directory (AD) tenant in the Azure portal. Enter the tenant ID to which your subscription belongs.
Client Secret	Enter the Client Secret of your Azure subscription.
Subscription ID	The ID for a subscription in the Azure portal. Enter the Azure Subscription ID which has the created Virtual WAN Hub to deploy Virtual Edges.

For more information on how to retrieve IDs for a subscription in Azure portal, see [How to create a new Azure Active Directory \(Azure AD\) application and service principal](#).

It is recommended for customers to create a custom role with the below permissions (JSON) to provide access to only the necessary resources for the CloudHub function.

```

"permissions": [
{
  "actions": [
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/deployments/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourcegroups/deployments/operationstatuses/read",
    "Microsoft.Resources/subscriptions/resourcegroups/deployments/operations/read",
    "Microsoft.Network/virtualWans/read",
    "Microsoft.Network/virtualWans/join/action",
    "Microsoft.Network/virtualWans/virtualHubs/read",
    "Microsoft.Network/virtualHubs/read",
    "Microsoft.AzureStack/linkedSubscriptions/linkedResourceGroups/linkedProviders/virtualNetworks/read",
    "Microsoft.Network/networkVirtualAppliances/delete",
    "Microsoft.Network/networkVirtualAppliances/read",
    "Microsoft.Network/networkVirtualAppliances/write",
    "Microsoft.Network/networkVirtualAppliances/getDelegatedSubnets/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/virtualNetworks/peer/action",
    "Microsoft.Network/virtualNetworks/write",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/prepareNetworkPolicies/action",
    "Microsoft.Network/virtualNetworks/subnets/unprepareNetworkPolicies/action"
  ],
  "notActions": []
}
]
  
```

```

    "dataActions": [],
    "notDataActions": []
}
]

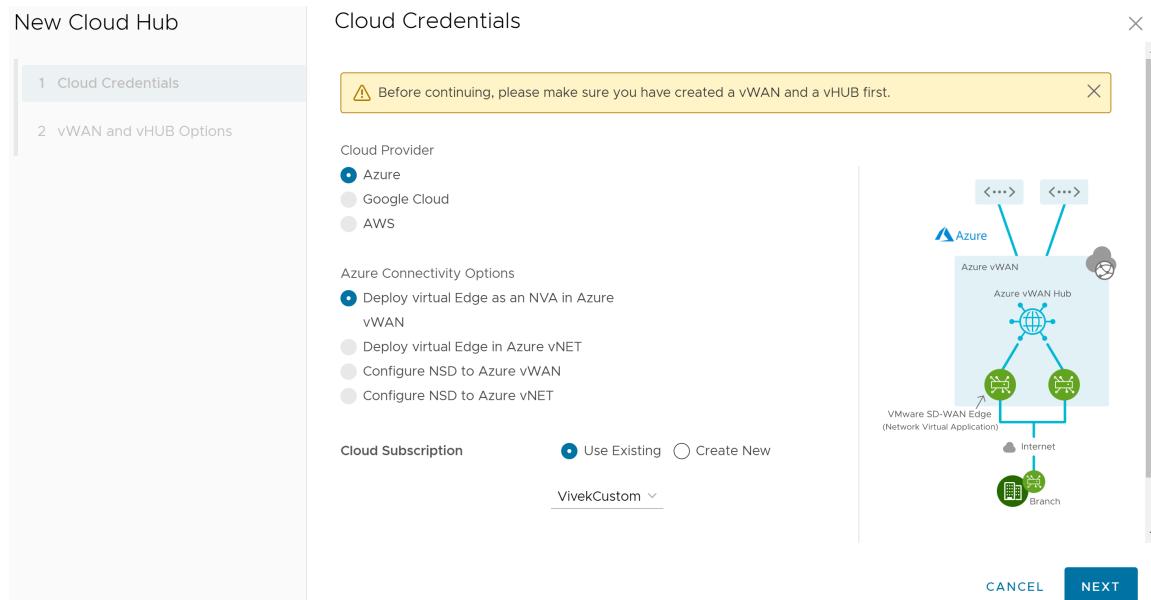
```

- 5 To create a New Cloud Hub, perform the following steps:

**Note** The Cloud Hub Workflow is tested only for the new Profile. So, it is recommended to create a new Profile before proceeding with the deployment of NVA Edge in vWAN HUB network.

- a Navigate to **Configure > Workflow** and click **New Cloud Hub**.

The **Cloud Credentials** page appears.



- b Provide all the required Cloud Credentials details and click **Next**.

Field	Description
Cloud Provider	Choose <b>Azure</b> as the Cloud Provider.
Azure Connectivity Options	Choose <b>Deploy Virtual Edge as an NVA in Azure vWAN</b> as the connectivity option between your Hub and vNet.
Cloud Subscription	You can use the existing cloud subscription or create a new subscription by clicking the <b>Create New</b> option.

The **vWAN and vHUB Options** page appears.

### New Cloud Hub

1 Cloud Credentials

2 vWAN and vHUB Options

### vWAN and vHUB Options

**vWAN and vHUB Options**

Resource Group *	vhub-testing
vWAN *	vhub-testing-vwan

---

**Choose vHUB**

Region *	eastus
vHub *	vhub-testing-vhubuseast
Address Space *	192.167.40.0/24
Workflow Name *	CloudHubtest

---

**Create Edge Networking**

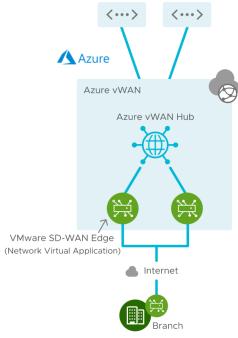
NVA Name *	vcoMcs
Select NVA Version *	Latest
Edge Cluster Name *	vcoMcsEdgeCluster
Scale Units *	2

---

**Address Assignment**

Select Profile *	Create New Profile
Edge License *	Select edge license
Contact Name *	sasi
Contact Email *	csasikala@vmware.com
BGP ASN	10000

CANCEL BACK FINISH



- c Choose vWAN, vHUB, and provision Virtual Azure NVA Edge (with unique name) by providing all the required details.

Field	Description
Resource Group	Select a resource group that you created on the Azure side.
vWAN	Select a Virtual WAN that you created on the Azure side.
Choose vHUB	
Region	Select the region in which you want to deploy the Virtual WAN Hub. Virtual Edges will be deployed in that Virtual WAN Hub.

Field	Description
vHub	Select a Virtual WAN Hub to deploy the virtual SD-WAN Edges.
Address Space	The hub's address range in CIDR notation. The minimum address space is /24 to create a hub.
Workflow Name	Enter the workflow name for the Virtual WAN Hub.
Create Edge Networking	
NVA Name	Enter a unique name for the Network Virtual Appliance (NVA) Edge device.
Select NVA Version	Select the NVA version.
Edge Cluster Name	Enter a unique name for the Edge Cluster.
Scale Units	A pair of Edges will be spun up. Scale Units can be 2, 4, or 10 which map to a Azure instance type.
Select Profile	Select a Profile to associate the Virtual Edge.  <b>Note</b> You can use the existing Profile or create a new Profile before deploying the Azure vWAN NVA Edges in Azure vWAN Hub.
Edge License	Select the Edge license associated with the Virtual Edges.
Contact Name	Enter a contact name.
Contact Email	Enter a contact email ID.
BGP ASN	Enter the ASN value that will be configured on the Virtual Edges in the VMware SASE Orchestrator.  <b>Note</b> The ASNs reserved by Azure: <ul style="list-style-type: none"><li>■ Public ASNs: 8074, 8075, and 12076.</li><li>■ Private ASNs: 65515, 65517, 65518, 65519, and 65520.</li></ul>

- d Click **Finish**. The newly created Cloud Hub appears in the **Workflow** page.
- e Under **Detail** column, click **View** to view the Event Details of the selected Cloud Hub.

**Note** Currently there is no separate Monitor page for Cloud Hub service. You can use the Monitor page of the SD-WAN service for verifying the Edge actions and states.

- 6 In the SD-WAN service portal, click **Monitor > Edges** to verify the Virtual Azure NVA Edge that you have provisioned/deployed with the Cloud Hub automation service are connected.

Name	Status	HA	Links	VNF VM Status	VNF Type	Last Contact
vcoMcsDemo1013_edge_1 [vcoMcsDemo1013...]	Connected	Cluster	0			Oct 13, 2022, 10:31:59 AM
vcoMcsDemo1013_edge_2 [vcoMcsDemo1013...]	Connected	Cluster	0			Oct 13, 2022, 10:32:01 AM
vcoMcs-1013-i-edge_1 [vcoMcs-1013-i-edge...]	Never activated	Cluster	0			
vcoMcs-1013-i-edge_2 [vcoMcs-1013-i-edge...]	Never activated	Cluster	0			

- 7 To verify if the BGP sessions are established for the deployed Virtual Azure NVA Edge, click **Monitor > Routing**.

Edge Name	Segment	Neighbor IP	State	State Changed Time	# Msg Received	# Msg Sent	# Events	Up/Down	# Prefix Received
vcoMcsDemo1013_edge_1	10.50.32.4	10.50.32.4	Established	Oct 13, 2022, 10:35:33 AM 8 minutes ago	15	13	2	00:08:47	5
vcoMcsDemo1013_edge_2	10.50.32.4	10.50.32.4	Established	Oct 13, 2022, 10:34:58 AM 9 minutes ago	14	13	2	00:08:15	5
vcoMcs-1013-i-edge_1	10.50.32.5	10.50.32.5	Established	Oct 13, 2022, 10:35:33 AM 8 minutes ago	14	13	2	00:08:47	5
vcoMcs-1013-i-edge_2	10.50.32.5	10.50.32.5	Established	Oct 13, 2022, 10:34:58 AM 9 minutes ago	13	13	2	00:08:15	5

**Important** Once the Virtual Edges are created, configure IP address for each of the Virtual Edges by navigating to **Configure > Edges > Firewall > Edge Access** and by adding the IP address "168.63.129.16" under the **Allow the following IPs** field.

**Note** You can perform this configuration on a Profile used by many or all of the Virtual Edges so you do not need to do it for each individual Virtual Edge.

For more details regarding this IP configuration, see <https://docs.microsoft.com/en-us/azure/virtual-network/what-is-ip-address-168-63-129-16>

# Configure Amazon Web Services

17

VMware supports Amazon Web Services (AWS) configuration in Non SD-WAN Destination.

Configure the Amazon Web Services (AWS) as follows:

- 1 Obtain Public IP, Inside IP, and PSK details from the Amazon Web Services website.
- 2 Enter the details you obtained from the AWS website into the Non-VMware Network Service in the SASE Orchestrator.

Read the following topics next:

- Configure Edge for Amazon Web Services (AWS) Transit Gateway (TGW) Connect Service
- Obtain Amazon Web Services Configuration Details
- Configure a Non SD-WAN Destination
- AWS CloudWAN CNE Connect using Tunnel-less BGP

## Configure Edge for Amazon Web Services (AWS) Transit Gateway (TGW) Connect Service

VMware SD-WAN Edges typically get deployed in a Transit VPC on Amazon Web Services (AWS). AWS introduced the support for AWS TGW (Transit Gateway) Connect Service for SD-WAN appliances to connect to the Transit Gateway. VMware SD-WAN Edge now has a feature (BGP over GRE support on LAN), which enables support on the VMware SD-WAN Edges to use the AWS TGW Connect Service for connectivity to the AWS Transit Gateway.

For the AWS TGW Connect Service, the Edge provisioned in the Transit VPC needs to use the LAN (routed, non-WAN) interface to set up the GRE tunnel. This effectively uses the Private IP configured on the Edge Intelligence (EI) to set up the GRE tunnel to the Transit Gateway.

## Amazon Web Services (AWS) Configuration Procedure

- 1 In the AWS portal, provision an AWS Transit Gateway in a particular region. This same region must have the Transit VPC, where the VMware SD-WAN Edge is provisioned.

The screenshot shows the VMware SD-WAN Administration interface. On the left, a sidebar lists various network components under categories like Virtual private cloud, Security, DNS firewall, and Network Firewall. The main area displays a table titled "Transit gateways (1/1) Info". The table has columns for Name, Transit gateway ID, Owner ID, and State. One row is selected, showing "Oregon-TGWConnect" with ID "tgw-06558b99ef97d8bab", Owner ID "813591333027", and State "Available". Below the table, there are tabs for Details, Flow logs, Sharing, and Tags. The Details tab is active, showing detailed configuration for the selected gateway.

Check for the Transit Gateway CIDR block to be configured, as shown in the image below.

**Note** An IP from this block is used for the GRE endpoint on the AWS TGW. The Amazon ASN is used later in the BGP configuration on the VMware SD-WAN Edge.

This screenshot shows the "Details" tab for a transit gateway. It includes fields for Transit gateway ID (tgw-06558b99ef97d8bab), ARN (arn:aws:ec2:us-west-2:813591333027:transit-gateway/tgw-06558b99ef97d8bab), Owner ID (813591333027), and Description (empty). The "Transit gateway CIDR blocks" field is highlighted with a red box and contains "1 CIDRs" followed by the value "172.43.0.0/24". Other configuration options shown include State (Available), Default association route table (Enable), Default propagation route table (Enable), Amazon ASN (64512), Association route table ID (tgw-rtb-06d1dcc255580f397), Propagation route table ID (tgw-rtb-06d1dcc255580f397), Multicast support (Disable), and various DNS and VPN settings.

- 2 Create a VPC Attachment for the Transit VPC specifying the Subnets where the LAN interface of the Edge or EI resides.

**Create transit gateway attachment** Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

**Details**

Name tag - optional  
Creates a tag with the key set to Name and the value set to the specified string.

Transit gateway ID Info

Attachment type Info

**VPC attachment**  
Select and configure your VPC attachment.

DNS support Info

IPv6 support Info

Appliance Mode support Info

VPC ID  
Select the VPC to attach to the transit gateway.

Subnet IDs Info  
Select the subnets in which to create the transit gateway VPC attachment.

<input checked="" type="checkbox"/> us-west-2a	subnet-038b9ecfec0d0571b (Oregon-VCE-VPC-A...)
<input checked="" type="checkbox"/> us-west-2b	subnet-0ea9e03f9f3339288 (Oregon-VCE-VPC-A...)
<input type="checkbox"/> us-west-2c	No subnet available
<input type="checkbox"/> us-west-2d	No subnet available

After the VPC Attachment is created, **Available** will display in the **State** column.

**Transit gateway attachments (1/4)** Info

**Actions** ▼ **Create transit gateway attachment**

**tgw-attach-0ea68bc938600d06a / Oregon-VPC-Attach**

Name	Transit gateway attachment ID	Transit gateway ID	Resource type	Resource ID	State	Association route table
App-VPC-Attach	tgw-attach-0d2fa0f67fcf296	tgw-06558b99ef97d8bab	VPC	vpc-0ddda50195949b996	<span>Available</span>	tgw-rtb-06d1dcc255
<input checked="" type="checkbox"/> Oregon-VPC-Attach	tgw-attach-0ea68bc938600d06a	tgw-06558b99ef97d8bab	VPC	vpc-096f3e4a815268daf	<span>Available</span>	tgw-rtb-06d1dcc255
dummy	tgw-attach-0813139564cba3c5d	tgw-06558b99ef97d8bab	Connect	tgw-attach-0ea68bc938...	<span>Deleted</span>	-

**Details**

Transit gateway attachment ID <input type="text" value="tgw-attach-0ea68bc938600d06a"/>	State <span>Available</span>	Resource type VPC	Association state <span>Associated</span>
Transit gateway ID <input type="text" value="tgw-06558b99ef97d8bab"/>	Resource owner ID <input type="text" value="813591333027"/>	Resource ID <input type="text" value="vpc-096f3e4a815268daf"/>	Association route table ID <input type="text" value="tgw-rtb-06d1dcc255580f397"/>
Transit gateway owner ID <input type="text" value="813591333027"/>	DNS support Enable	IPv6 support Disable	Appliance Mode support Disable
Subnet IDs <input type="text" value="subnet-038b9ecfec0d0571b"/>			

### 3 Create a Connect Attachment using the VPC Attachment.

**Create transit gateway attachment** [Info](#)

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

**Details**

**Name tag - optional**  
Creates a tag with the key set to Name and the value set to the specified string.

**Transit gateway ID** [Info](#)

**Attachment type** [Info](#)

**Connect attachment**  
A connect attachment allows you to establish connection between a transit gateway and the third-party appliances using Generic Routing Encapsulation (GRE) and Border Gateway Protocol (BGP).

**Transport attachment ID** [Info](#)

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/> <input type="button" value="X"/>	<input type="text" value="Connect-Attach"/> <input type="button" value="X"/> <input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>	

You can add 49 more tags.

After the Connect Attachment is created, **Available** will display in the **State** column.

- 4 Create a Connect peer, which will translate to a GRE Tunnel. Specify the following parameters: the Transit Gateway GRE Address, the Peer GRE Address, the BGP Inside CIDR block, and the Peer ASN.

---

**Note** The BGP Inside CIDR block and the Peer ASN must match what is configured on the VMware SD-WAN Edge.

---

**Create connect peer** [Info](#)

A connect peer is a Generic Routing Encapsulation (GRE) tunnel within which you can establish Border Gateway Protocol (BGP) peering to exchange routes.

**Details**

Name tag - optional  
Creates a tag with the key set to Name and the value set to the specified string.

Transit gateway ID  
 tgw-06558095ef97d8bab

Connect attachment ID  
 tgw-attach-0b0e87e60b353059f

**Configure tunnel options**  
Customer GRE tunnel addresses and BGP Inside CIDR blocks for your connect peer. Unspecified tunnel options will be auto-generated.

Transit gateway GRE address - optional [Info](#)  
Requires a valid IPv4 or IPv6 address.

Peer GRE address [Info](#)  
Requires a valid IPv4 or IPv6 address.

BGP Inside CIDR blocks IPv4 [Info](#)  
Requires a valid IPv4 CIDR mask.

BGP Inside CIDR blocks IPv6 - optional [Info](#)  
Requires a valid IPv6 CIDR mask.

Peer ASN - optional [Info](#)  
Requires a valid BGP ASN.

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="VCE2"/>

[Add new tag](#)  
You can add 49 more tags.

[Cancel](#) [Create connect peer](#)

In the above example:

- 172.43.0.24 is the GRE Outside IP address on the AWS TGW, this IP is allocated from the Transit Gateway CIDR block.
- 10.1.1.30 is the GRE Outside IP address on the VMware SD-WAN Edge.
- 169.254.31.0/29 is the Inside CIDR Block. The addresses from this block are used for the BGP neighbor.
- 169.254.31.1 is the IP address on the VMware SD-WAN Edge.
- 169.254.31.2 and 169.254.31.3 are addresses used for the BGP on the AWS TGW.
- 64512 is the BGP ASN configured on the AWS TGW.
- 65000 is the BGP ASN configured on the VMware SD-WAN Edge.

The VPC Resource Map for the Transit VPC lists the LAN side subnet with the Route table, as shown in the image below.

- In the Transit VPC route table, add a route for the TGW CIDR block with Target or Next Hop as the VPC Attachment.

**Note** For example, 172.43.0.0/24 is the AWS TGW CIDR block.

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
172.43.0.0/24	tgw-06558b99f97d8bab	Active	No

Add route

Cancel Preview Save changes

- In the same route table, verify that the LAN EI subnet has an explicit Subnet association.

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
Services-rtb-public	rtb-01ff288b5f6d405d2	2 subnets	-	No	vpc-0fa092870x04053e   Ser...	B13591333027
<b>Oregon-VCE-VPC-LAN</b>	<b>rtb-04170c88177159c00</b>	<b>subnet-038b0ccfec005...</b>	<b>-</b>	<b>No</b>	<b>vpc-096f3a4815268da1   Ore...</b>	<b>B13591333027</b>
-	rtb-01062d9b0940528	-	-	Yes	vpc-0fa092870d04053e   Ser...	B13591333027
app-vpc-route-table	rtb-0e950931d0fb9f9065	-	-	Yes	vpc-001ca501959489698   Ap...	B13591333027
Services-rtb-private2-us-west-2b	rtb-0e08b689303aa5f6c	subnet-017e657f66607...	-	No	vpc-0fa092870d04053e   Ser...	B13591333027
Oregon-VCE-VPC-WAN	rtb-009120e579c0096	2 subnets	-	Yes	vpc-096f3a4815268da1   Ore...	B13591333027
Services-rtb-private1-us-west-2a	rtb-09776e60013e19924	subnet-0424e09372039...	-	No	vpc-0fa092870x04053e   Ser...	B13591333027

rtb-04170c88177159c00 / Oregon-VCE-VPC-LAN

Details	Routes	Subnet associations	Edge associations	Route propagation	Tags												
<b>Explicit subnet associations (1)</b>																	
<table border="1"> <thead> <tr> <th>Name</th> <th>Subnet ID</th> <th>IPv4 CIDR</th> <th>IPv6 CIDR</th> </tr> </thead> <tbody> <tr> <td>Oregon-VCE-VPC-AZ1-Subnet1</td> <td>subnet-038b0ccfec005f71b</td> <td>10.1.1.0/24</td> <td>-</td> </tr> </tbody> </table>						Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Oregon-VCE-VPC-AZ1-Subnet1	subnet-038b0ccfec005f71b	10.1.1.0/24	-				
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR														
Oregon-VCE-VPC-AZ1-Subnet1	subnet-038b0ccfec005f71b	10.1.1.0/24	-														
<b>Subnets without explicit associations (2)</b>																	
<table border="1"> <thead> <tr> <th>Name</th> <th>Subnet ID</th> <th>IPv4 CIDR</th> <th>IPv6 CIDR</th> </tr> </thead> <tbody> <tr> <td>Oregon-VCE-VPC-AZ2-Subnet2</td> <td>subnet-0ea9e03fd3339288</td> <td>10.1.4.0/24</td> <td>-</td> </tr> <tr> <td>Oregon-VCE-VPC-AZ2-Subnet1</td> <td>subnet-005d4854718acde5e</td> <td>10.1.3.0/24</td> <td>-</td> </tr> </tbody> </table>						Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Oregon-VCE-VPC-AZ2-Subnet2	subnet-0ea9e03fd3339288	10.1.4.0/24	-	Oregon-VCE-VPC-AZ2-Subnet1	subnet-005d4854718acde5e	10.1.3.0/24	-
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR														
Oregon-VCE-VPC-AZ2-Subnet2	subnet-0ea9e03fd3339288	10.1.4.0/24	-														
Oregon-VCE-VPC-AZ2-Subnet1	subnet-005d4854718acde5e	10.1.3.0/24	-														

## VMware SASE Orchestrator Configuration Procedure

- On the VMware SASE Orchestrator, go to **Network Services > Non SD-WAN Destinations via Edge** and configure the GRE Tunnel with the AWS Transit Gateway Connect.

## Non SD-WAN Destinations via Edge

General

Service Name \* **TGW-GRE**

Tunneling Protocol  GRE  IPsec

Service Type \* AWS Transit Gateway Connect

Tunnel mode Active/Active

**CANCEL** **SAVE**

**Note** When configuring the GRE Tunnel with the AWS Transit Gateway Connect service, see the following important notes:

- The only Tunnel Mode parameter that can be configured is Active/Active.
- There are no Keepalive mechanisms for the GRE tunnel with the AWS Transit Gateway Service.
- BGP will be configured by default for the GRE tunnels. BGP Keepalive(s) are used for the BGP neighbor status.
- The Edge does not support ECMP across multiple tunnels. Therefore, only one GRE Tunnel will be used for egress Traffic.

2 Under Profile, enable CloudVPN, enable Non SD-WAN Destination via Edge, and choose NSD.

Service	Automation for all public WAN Links	Enable Service
TGW-GRE	N/A	Enabled

3 Under the Edge configuration in the Non SD-WAN Destinations via Edge, select the configured NSD.

Service		Link					
<input type="checkbox"/>	Name	Automation for all public WAN Links	Enable Service	Enable Tunnel	Destination Primary Public IP	Destination Secondary Public IP	Action
<input type="checkbox"/>	b1-edge-global-pri	N/A	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> GES	172.29.1.1	172.29.1.2	<input type="button" value="⊖ +"/>
<input type="checkbox"/>	TGW-GRE	N/A	<input checked="" type="checkbox"/> Enabled		No sites added		<input type="button" value="⊕"/>

2 items

- 4 For the specific NSD, configure the GRE tunnel parameters by selecting the + sign. Configure the following below:

- Tunnel Source as the LAN interface
- Tunnel Source IP as the IP address configured on the LAN interface, if specified dynamically use Remote Diagnostics > Interface Stats to obtain the IP address
- TGW ASN
- The Primary Tunnel parameters can be configured by providing, Destination IP, the IP address provided on the TGW Connect Peer
- The Internal Network/Mask must be the same as specified in the TGW Connect Peer Inside configuration.
- The Secondary Tunnel parameters can be configured for the Destination IP and Internal Network/Mask.

Add AWS TGW Connect Tunnel  
Destination: TGW-GRE

Tunnel Source *	GE3		
Tunnel Source IP *	10.1.1.30		
Local ASN *	65000	TGW ASN *	64512
Primary Tunnel		Secondary Tunnel	
Destination IP *	172.43.0.24	+ADD	
Internal Network/Mask *	169.254.31.0 /29	Secondary tunnel not configured yet. Click Add button to configure secondary tunnel.	
Internal IP/Mask	169.254.31.1		
Internal TGW IP/Mask	169.254.31.2, 169.254.31.3		
Internal IP/Mask and BGP Local and TGW ASN will be used to define BGP neighbors which is needed for AWS TGW Connect. Go to BGP > NSD Neighbors section for additional configuration of these BGP Neighbors.			
<a href="#">CANCEL</a> <a href="#">SAVE</a>			

**Note** BGP will be enabled by default for this feature. Local ASN field will be pre-populated.

The Non SD-WAN via Edge configuration displays, as shown in the image.

Non SD-WAN Destination via Edge						
<input checked="" type="checkbox"/> Enable Non SD-WAN via Edge <input checked="" type="checkbox"/> Override						
<a href="#">+ ADD</a> <a href="#">+ NEW NSD VIA EDGE</a> <a href="#">DELETE</a>						
Service		Link				
<input type="checkbox"/>	Name	Automation for all public WAN Links	Enable Service	Enable Tunnel	Destination Primary Public IP	Destination Secondary Public IP
<input type="checkbox"/>	TGW-GRE	N/A	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> GE3	172.43.0.24	-

1 Item

- The above configuration will automatically create the BGP configuration for the Neighbors. Each GRE Tunnel configuration towards the AWS Transit Gateway will automatically be created for two BGP Neighbors with information regarding the Link Name, Neighbor IP, Tunnel Type, and ASN.

NSD Neighbors								
<a href="#">+ ADD</a> <a href="#">DELETE</a> <a href="#">CLONE</a>								
NSD Name *	LinkName *	Tunnel Type *	Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options	
<input checked="" type="checkbox"/> TGW-GRE	GE3	Primary	169.254.31.2	64512	[None]	(-)	(+)	<a href="#">VIEW ALL</a>
<input checked="" type="checkbox"/> TGW-GRE	GE3	Primary	169.254.31.3	64512	[None]	(-)	(+)	<a href="#">VIEW ALL</a>

\*Required

2 items

In **Additional Options**, the eBGP Max Hop is configured as 2, as this is a requirement for the TGW Connect Service. The additional parameters that are populated are Keepalive and Hold Timer based off the recommendation provided by AWS. The BGP Local IP is also pre-populated. These parameters cannot be modified.

Additional Options	
<input type="button" value="-"/>	<input type="button" value="+"/>
<b>VIEW LESS</b>	
Max-Hop	2
Local IP *	169.254.31.1.1
Uplink ⓘ	<input checked="" type="checkbox"/>
Allow AS ⓘ	<input type="checkbox"/>
Default Route ⓘ	<input type="checkbox"/>
Enable BFD ⓘ	<input checked="" type="checkbox"/>
Keep Alive	10
Hold Timer	30
Connect ⓘ	120

#### Note

- Two NSD BGP Neighbors will be automatically added.
- The **Additional Options** field will be modified for Max-Hop, Local IP, Keep Alive, and Hold Timer values.

- 
- 6 For the GRE tunnel endpoint, configure a static route on the VMware SD-WAN Edge which specifies the Next-Hop to specify the Subnet Default Gateway and Interface as the LAN interface.

Static Route Settings										
IPv4		IPv6								
Local Routes										
<b>+ ADD</b>		<b>- REMOVE</b>		<b>CLONE</b>						
<input type="checkbox"/>	Subnet *	Source IP	Next Hop IP *	Interface ⓘ	VLAN	Cost *	Preferred ⓘ	Advertise ⓘ	ICMP Probe	Description
<input type="checkbox"/>	172.43.0.24/32	N/A	10.1.1.1	GE3	<input type="checkbox"/>	1	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/>	<b>+ NEW</b> Enter Des...
1 Item										

## Obtain Amazon Web Services Configuration Details

Describes how to obtain Amazon Web Services configuration details.

- 1 From Amazon's Web Services, create VPC and VPN Connections. Refer to the instructions in Amazon's documentation: <http://awsdocs.s3.amazonaws.com/VPC/latest/vpc-nag.pdf>.

- 2 Make note of the SD-WAN Gateways associated with the enterprise account in the SASE Orchestrator that might be needed to create a virtual private gateway in the Amazon Web Services.
- 3 Make a note of the Public IP, Inside IP and PSK details associated with the Virtual Private Gateway. You need to enter this information in the SASE Orchestrator when you create a Non SD-WAN Destination.

## Configure a Non SD-WAN Destination

After you obtain Public IP, Inside IP, and PSK information from the Amazon Web Services (AWS) website, you can configure a Non SD-WAN Destination.

To configure a Non SD-WAN Destination via Gateway, see:

- [Configure a Non SD-WAN Destination of Type Generic IKEv1 Router \(Route Based VPN\)](#)
- [Configure a Non SD-WAN Destination of Type Generic IKEv2 Router \(Route Based VPN\)](#)

To configure a Non SD-WAN Destination via Edge, see:

- [Configure a Non-VMware SD-WAN Site of Type Generic IKEv1 Router via Edge](#)
- [Configure a Non-VMware SD-WAN Site of Type Generic IKEv2 Router via Edge](#)

## AWS CloudWAN CNE Connect using Tunnel-less BGP

AWS has announced Tunnel-less Connect on Cloud WAN. This document describes AWS components and how to configure for AWS and VMware SD-WAN.

The new AWS CloudWAN CNE Connect using Tunnel-less BGP capability provides a simpler way to build a global SD-WAN network using AWS backbone as a middle-mile transport network. With this capability, VMware SD-WAN appliances can natively peer with AWS Cloud WAN using BGP (Border Gateway Protocol) without requiring tunneling protocols like IPSec or GRE. This simplifies the integration of customer's SD-WAN into AWS cloud and allows them to leverage the high bandwidth AWS backbone for branch-to-branch connectivity across different geographic regions. This feature also supports in-built network segmentation, enabling customers to build a secure SD-WAN at a global scale.

VMware SD-WAN Virtual Edges (vEdges) are typically deployed in what AWS calls a "Transport" VPC. This Transport VPC may then peered with other VPCs, TGWs, or in this case, a CNE (Cloud Network Edge) in the Cloud WAN backbone to achieve connectivity with resources the customer has homed into AWS.

For Cloud WAN CNE Connect, the vEdges provisioned in the Transport VPC will use the LAN-facing (routed, non-WAN) interface to establish a native L3 (i.e. unencapsulated) BGP peering with the CNE.

## AWS Components

There are 6 main components needed in AWS:

- Cloud WAN Core Network
- Policy definition
- Core Network Edge (CNE)
- Transport VPC
- VPC Attachment
- Connect Attachment

This assumes that the customer already has other resources in other AWS VPCs that use VPC peering to CNEs in Core Network. If not, the Core Network and CNEs must be defined, and attachments must be created to the customer's existing workload VPCs.

## AWS Configuration

- 1 Using the following VMware online documentation to create vEdges in an AWS VPC:
  - a Virtual Edge Deployment Guide
  - b VMware SD-WAN AWS CloudFormation Template - Green Field
  - c VMware SD-WAN AWS CloudFormation Template - Brown Field
- 2 On the AWS console, AWS Network Manager must be used to create a Global Network, if one does not already exist in the customer's AWS deployment.

The screenshot shows the 'Create global network' wizard in the AWS Network Manager. The left sidebar lists steps: Step 1 (Create global network), Step 2 (optional: Create core network), and Step 3 (Review). The main panel is titled 'Create global network' and contains the following fields:

- Name:** A name to help you identify the global network. The input field contains "My global network". A note below says: "Name must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen)."
- Description - optional:** A description to help you identify the global network. The input field contains "A global network for testing purposes." A note below says: "Description must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen)."
- Additional settings:** A button to expand additional configuration options.

At the bottom right are 'Cancel' and 'Next' buttons.

### 3 Create a Policy version.

- a A Policy version is where key details of the solution are defined and configured, as shown in the image below.

Policy version ID	Change set state	Description	Version
Policy version - 10	Execution succeeded	-	2021.12
Alias	Execution progress	Creation time	VPN ECMP support
LIVE, LATEST	-	Oct 19, 2023, 07:08:36 (UTC-05:00)	Yes

- b Enter the BGP ASN ranges used by the CNEs.

From	To
65000	65009

- c In the global "Inside CIDR blocks," the CNEs will get their respective Inside CIDR blocks defined. Enter the CIDR in the appropriate text box, as shown in the image below.

CIDR
11.0.0.0/16

- d Search for **Edge locations** in the appropriate text box, as shown in the image below. The CNE locations define the specific AWS AZ where a CNE will be instantiated.

Location	ASN	Inside CIDR blocks
Europe (Ireland)	65002	11.0.2.0/24
US West (N. California)	65001	11.0.1.0/24

**Note** The ASN and Inside CIDR Blocks for each Edge location are defined within the range defined above for the Global Network.

- e Search for **Segments** in the appropriate text box, as shown in the image below. Logical segments are defined using Tags. VPCs and Subnets may be tagged to define which segments they are a member of. In this example, the format is Key = “Segment”, Value = “SDWAN”, although the value is arbitrary.

Segments (1)							
<input type="text" value="Search segments"/> <span style="float: right;">(1)</span>							
Name	Edge locations	Description	Require attachment acceptance	Isolated attachments	Allow segment List	Deny segment List	
SDWAN	-	-	No	No	-	-	

**Note** Whatever value is used must match the value defined in the policy.

- f Attachment policies specify which Segments the VCP and Connect Attachments are a part of and what criteria are used. Search for the **Attachment Policies** in the appropriate text box, as shown in the image below. In the example below, a “tag-value” condition defines membership in the “SDWAN” segment defined above. The “Condition Values” are the key-value pair also defined above. This key-value pair must be present in VPCs and/or subnets for them to become Segment members.

Attachment policies (1)							
<input type="text" value="Search attachment policies"/> <span style="float: right;">(1)</span>							
Rule number	Description	Segment to attach	Require acceptance	Conditions	Operator	Condition values	Condition logic
100	-	Segment name - SDWAN	-	tag-value	contains	key=Segment, value=SDWAN	and

**Note** This is arguably the least intuitive and most error-prone part of the entire configuration. If you aren’t seeing routes from your remote workload VPCs, check this. Other configurations and conditions are possible, but this is what worked in lab testing.

- 4 CNE Attachments: There are two types of attachments used, VPC Attachment and Connect Attachment.
- a VPC Attachments: Each SD-WAN Transport VPC will have a VPC attachment to its respective CNE. At least one subnet within the VPC must be

specified when the VPC Attachment is created. In this example, The CNE in the us-west-1 AZ peers with the SD-WAN Transport VPC's private LAN subnet. A key-value pair defining Segment membership is also

### Create attachment

Select the type of core network attachment that you would like to create.

#### Attachment settings

**Name - optional**  
A name to help you identify the attachment.

Name must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).

**Edge location**

**Attachment type**

#### VPC attachment

Select and configure your VPC attachment. [Learn more](#)

**Appliance mode support**  
Enable Appliance mode for this attachment.

**IPv6 support**  
Enable IPv6 for this attachment.

**VPC ID**  
Select the VPC to attach to the core network.

**Subnet IDs**  
Select the subnets in which to create the core network VPC attachment. You must select at least one subnet. You can only select one subnet per Availability Zone, but all subnets in that Availability Zone can send traffic to the Global network.

<input checked="" type="checkbox"/> Availability zone	Subnet Id
<input checked="" type="checkbox"/> us-west-1b	<input type="text" value="vmware-sdwan-Public-SN"/>

#### Tags

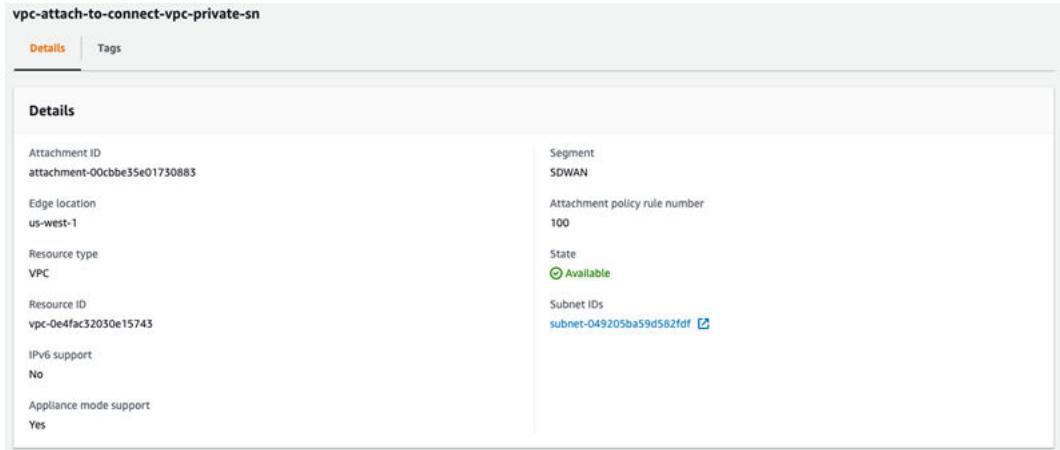
Specified tags to help identify a Network Manager resource.

Key	Value	
<input type="text" value="Segment"/>	<input type="text" value="SDWAN"/>	<input type="button" value="Remove tag"/>

You can add 49 more tags.

necessary.

If the Policy has been configured correctly, the Attachment should show that it has been made part of the “SDWAN” Segment. The Attachment policy rule number being used will display, as shown in the image



The screenshot shows a VMware SD-WAN interface for managing VPC attachments. The title bar says "vpc-attach-to-connect-vpc-private-sn". Below it, there are two tabs: "Details" (which is selected) and "Tags". The main area is titled "Details" and contains the following information:

Attachment ID	Segment
attachment-00cbbe35e01730883	SDWAN
Edge location	Attachment policy rule number
us-west-1	100
Resource type	State
VPC	<span style="color: green;">Available</span>
Resource ID	Subnet IDs
vpc-0e4fac32030e15743	<a href="#">subnet-049205ba59d582fdf</a>
IPv6 support	
No	
Appliance mode support	
Yes	

below.

- b Connect Attachments are where “Tunnel-less (No Encapsulation)” is configured. The Connect Attachment configuration must specify an existing VPC Attachment as the

Transport Attachment ID, so the VPC Attachment must be configured first. As with the VPC Attachment, tags for Segment membership must be configured.

## Create attachment

Select the type of core network attachment that you would like to create.

### Attachment settings

#### Name - optional

A name to help you identify the attachment.

example

Name must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).

#### Edge location

US West (N. California)

#### Attachment type

Connect

### Connect attachment

A Connect Attachment allows you to establish connection between a core network and the third-party appliances using Generic Routing Encapsulation (GRE) or Tunnel-less (No Encapsulation) and Border Gateway Protocol (BGP). [Learn more](#)

#### Connect protocol

Tunnel-less (No Encapsulation)

#### Transport Attachment ID

Select an existing core network Attachment to be used as transport for the Connect Attachment.

vpc-attach-to-connect-vpc-private-sn

### Tags

Specified tags to help identify a Network Manager resource.

#### Key

Segment

#### Value

SDWAN

[Remove tag](#)

[Add tag](#)

You can add 49 more tags.

If the Policy has been configured correctly, the Attachment should show that it has been made part of the “SDWAN” Segment. Note that the Attachment policy rule number being used is shown, as is “NO\_ENCAP” for the Connect protocol. See image below.

General details	
Attachment ID	attachment-077bb8fd39b9d36fa
Edge location	us-west-1
Resource type	Connect
Connect protocol	NO_ENCAP
Segment	SDWAN
Attachment policy rule number	100
State	<span style="color: green;">Available</span>
Transport Attachment ID	attachment-00cbbe35e01730883

- 5 Connect peers: Connect peers are created under the Connect Attachment. This is where the SD-WAN vEdge BGP peerings are defined in terms of the ASN and peer IP address. See image below.

Connect peer settings	
Name	A name to help you identify the connect peer. <input type="text" value="example"/>
Name must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).	
Connect peer options	
Customize Connect peer BGP IPs and ASNs. <a href="#">Learn more</a>	
Peer BGP IP address	<input type="text" value="10.0.1.155"/>
BGP IP on third-party appliance side	
Peer ASN	<input type="text" value="65010"/>
The Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your third-party appliance. You can use an ASN in the 1-429367294 range. Unspecified Peer ASN will be auto populated with the same ASN as the Core Network Edge.	
Subnet	<input type="text" value="vmware-sdwan-Private-SN"/>

below.

Once created, the AWS Console will provide two Core Network BGP peer IP addresses to use on the SD-WAN side of the BGP neighborship. These IPs will be selected randomly from the “Inside CIDR range” defined in the “Edge Locations” portion of the Policy above. See image

**Create Connect peer**

A Connect peer establishes a Border Gateway Protocol (BGP) peering to exchange routes using either a Generic Routing Encapsulation (GRE) tunnel or a Tunnel-less mechanism for connectivity. [Learn more](#)

### Connect peer settings

**Name**  
A name to help you identify the connect peer.  
**example**  
Name must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).

### Connect peer options

Customize Connect peer BGP IPs and ASNs. [Learn more](#)

**Peer BGP IP address**  
**10.0.1.155**  
BGP IP on third-party appliance side

**Peer ASN**  
**65010**  
The Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your third-party appliance. You can use an ASN in the 1-4293967294 range. Unspecified Peer ASN will be auto populated with the same ASN as the Core Network Edge.

**Subnet**  
**vmware-sdwan-Private-SN**

below.

## VMware SD-WAN Configuration

BGP neighbors must now be configured to point to the two IP addresses provided by the AWS console under **Connect Peers**. Since these BGP neighbor IPs are from the Inside CIDR range defined in the policy, static routes must be created on the Edge to point to the CNE neighbor IPs using the LAN-side routed interface (GE3).

**Note** Each Connect peer will get different BGP Core Network Peer IP addresses, so the Static Route and BGP Neighbor configurations will be different for each vEdge in an AWS hub-cluster.

- 1 Configure Static Route Settings, as shown in the image below.

Subnet *	Source IP	Next Hop IP *	Interface * ⓘ	VLAN	Cost *	Preferred ⓘ	Advertise ⓘ	ICMP Probe	Description
11.0.1.48/32	N/A	10.0.1.1	GE3		0	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Yes	[None]	+ NEW Enter De...
11.0.1.100/32	N/A	10.0.1.1	GE3		0	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Yes	[None]	+ NEW Enter De...

2 items

- 2 When creating the BGP neighbors, set “Max-Hop” to 2 or more under **Additional Options**. See image below.

Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options
11.0.1.48	65001	[None] ⓘ	[None] ⓘ	Max-Hop: 3 Local IP: IP Address Source Interface: Auto Uplink ⓘ: <input type="checkbox"/> Allow AS ⓘ: <input type="checkbox"/> Default Route ⓘ: <input type="checkbox"/> Enable BFD ⓘ: <input type="checkbox"/> Keep Alive: Example: 10 Hold Timer: Example: 10 Connect ⓘ: Example: 10 MDS Auth ⓘ: <input type="checkbox"/> MDS Password: Password ⓘ
11.0.1.100	65001	[None] ⓘ	[None] ⓘ	Max-Hop: 3 Local IP: IP Address Source Interface: Auto Uplink ⓘ: <input type="checkbox"/> Allow AS ⓘ: <input type="checkbox"/> Default Route ⓘ: <input type="checkbox"/> Enable BFD ⓘ: <input type="checkbox"/> Keep Alive: Example: 10 Hold Timer: Example: 10 Connect ⓘ: Example: 10 MDS Auth ⓘ: <input type="checkbox"/> MDS Password: Password ⓘ

\*Required

2 items

- 3 Use Monitor > Routing > BGP Edge Neighbor State to verify that the BGP peer relationship has been Established with the Neighbor IPs configured. See image below for a visual of the Routing screen.

Edge Name	Segment	Neighbor IP	State	State Changed Time	# Msg Received	# Msg Sent	# Events	Up/Down	# Prefix Received
vedge-1	Global Segment	11.0.1.100	Established	Oct 25, 2023, 8:27:18 AM 11 hours ago	127,318	63,671	3	11:10:26	4
vedge-1	Global Segment	11.0.1.48	Established	Oct 20, 2023, 3:08:15 AM 6 days ago	127,269	63,650	6	5d16h29m	4
vedge-2	Global Segment	11.0.1.53	Established	Oct 20, 2023, 3:07:51 AM 6 days ago	123,540	61,787	6	5d15h59m	4
vedge-2	Global Segment	11.0.1.57	Established	Oct 25, 2023, 8:27:05 AM 11 hours ago	123,542	61,781	5	11:10:57	4
vedge-3	Global Segment	11.0.2.56	Established	Oct 19, 2023, 7:27:24 AM 7 days ago	112,459	56,232	3	6d12h10m	4
vedge-3	Global Segment	11.0.2.79	Established	Oct 19, 2023, 7:27:24 AM 7 days ago	112,459	56,235	3	6d12h10m	4

7 items

# Security Service Edge (SSE)

18

Starting from the 5.3.0 release, VMware SD-WAN supports the Security Service Edge (SSE) feature. This feature allows VMware SD-WAN to easily integrate with a third party SSE vendor using seamless automation through the Orchestrator. You can configure multiple SSE integrations with the same vendor.

Enterprise users can now configure **Non SD-WAN Destinations via Edge** and **Cloud Subscription** through the **Security Service Edge (SSE)** feature. For manual configuration of network services, see [Chapter 10 Configure Network Services](#).

---

**Note** Currently, only **Non SD-WAN Destination via Edge** network service is supported.

The **Security Service Edge (SSE)** feature currently supports **PAN Prisma** and **Symantec** subscriptions. For an Enterprise user, the SSE feature is activated by default.

## Prerequisites:

- For the **PAN Prisma** SSE integration, the Enterprise user must first create **IKE** and **IPsec** profiles on the **Palo Alto Networks Strata Cloud Manager** portal. These profiles can then be used for the SSE integration. For more information, see [Palo Alto Networks Strata Cloud Manager Configuration](#).
- For the **Symantec** integration, the Enterprise user must first create username and password for an API credential configured in the **Symantec Cloud** portal. For more information, see [Configure Symantec API Credentials](#).

---

**Note** As tunnel establishment is an asynchronous operation, the Security Service Edge (SSE) automated configuration might take 5 - 30 minutes per WAN link tunnel, to complete. This time delay is due to **PAN Prisma**.

Before creating an **SSE Integration**, you must first create an **SSE Subscription**.

## SSE Subscriptions

To view or create an SSE subscription, follow the below steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Security Service Edge (SSE)**.

- Click the **SSE Subscriptions** tab on the **Security Service Edge (SSE)** landing page. The following screen appears:

The screenshot shows the 'SSE Subscriptions' tab selected in the top navigation bar. There are two existing subscriptions listed:

- symantec-api-cred**: Represented by a Symantec logo icon. Status: In Use. Action: [VIEW](#)
- prisma-credential**: Represented by a Prisma logo icon. Status: In Use. Action: [VIEW](#)

At the bottom right of the list area, there is a button labeled [+ NEW SSE SUBSCRIPTION](#).

- In each tile, click **View** to view the existing subscription details. Click the vertical ellipsis, and then click **Delete** to delete a subscription.
- To create a new subscription, click **+ New SSE Subscription**.
- The **Configure SSE Subscription** window appears. You must enter a **Name** for the subscription and select a **Subscription Type** from the drop-down menu. The fields displayed on the screen vary depending on the selected **Subscription Type**.

The below image and table are for the **Prisma Access** subscription type.

Configure SSE Subscription

Name *	test
Subscription Type *	Prisma Access
Tsg Id *	34
User Name *	test123
Password *	..... 
Domain *	vmware
<b>VALIDATE SUBSCRIPTION</b>	
<b>SAVE</b>	

Option	Description
Tsg Id	Enter the ID. This value must be a positive integer.
User Name	Enter the service account username.
Password	Enter the service account password.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Domain	Enter your company domain. Example: vmware.com  <b>Note</b> This field is required for IPSec FQDN creation.

**Note** The fields **Tsg Id**, **User Name**, and **Password** must match the values configured in the **Palo Alto Networks Strata Cloud Manager** portal.

The below image and table are for the **Symantec** subscription type.

## Configure SSE Subscription

X

Name *	test
Subscription Type *	Symantec
User Name *	abc
Password *	..... 
Tenant ID	
Expiry	<input checked="" type="checkbox"/> Time-Based
Expiry Date	07/30/2024 12:00 
<b>VALIDATE SUBSCRIPTION</b>	
<b>SAVE</b>	

Option	Description
User Name	Enter a username.
Password	Enter a password.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Cloud Type	Select either <b>Prod</b> or <b>Dev</b> from the drop-down menu.
Tenant ID	Enter the Tenant ID associated with the Enterprise.
Expiry	To set an expiry for the credentials, click the toggle button. The <b>Expiry Date</b> field appears. Click the calendar to set the expiry date and time.

**Note** The fields **User Name**, **Password**, **Tenant ID**, **Expiry** must match the values configured in the **Symantec Cloud** portal.

- Click **Validate Subscription** to make sure that the entered credentials are correct, and then click **Save** to save the configured subscription.

# SSE Integration

To view or create an SSE integration, follow the below steps:

- In the **SD-WAN** service of the Enterprise portal, click **Configure > Security Service Edge (SSE)**. By default, the **SSE Integrations** tab is displayed.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'Customer sse-test' and 'SD-WAN'. The left sidebar has sections like 'Edge Configuration' (Edges, Profiles, Object Groups, Segments, Overlay Flow Control, Network Services), 'Security Service Edge (SSE...)' (selected), and 'Diagnostics', 'Service Settings'. The main content area is titled 'Security Service Edge (SSE) Automated Configuration'. It contains a note: 'This is only for SSE automation configuration. For manual configuration, please go to Network Services.' Below this are two tabs: 'SSE Integrations' (selected) and 'SSE Subscriptions'. A table lists existing SSE integrations:

	Name	SSE Vendor	Used By	Tunnel Deployment Status	Created
<input type="checkbox"/>	symantec-prod-1	Broadcom - Symantec	0 Selected   0 Configured	<a href="#">View</a>	Nov 8, 2023
<input type="checkbox"/>	prisma	Palo Alto - Prisma Access	0 Selected   0 Configured	<a href="#">View</a>	Nov 8, 2023

Buttons at the bottom include '+ NEW SSE INTEGRATION', 'EDIT', and 'DELETE'. A support icon is in the bottom right corner.

- To create a new SSE integration, click **+ New SSE Integration**. The following screen is displayed:

The screenshot shows the 'Configure a New SSE Integration' wizard. The title bar says 'Security Service Edge (SSE) / Configure a New SSE Integration'. The first step is '1. Choose Cloud Subscription'. It has a 'Subscription Type' section with a dropdown labeled 'Choose Subscription Type' and a 'NEXT STEP' button. The next steps are listed below:

- 2. Create Network Service
- 3. Select Profile/Edges

- 3 Under **Choose Cloud Subscription** section, configure the following options:

Option	Description
Subscription Type	Select a subscription type for which you want to set up an SSE integration. The available options are: <ul style="list-style-type: none"><li>■ Prisma Access</li><li>■ Symantec (Tech Preview)</li></ul>
Cloud Subscription	Select a cloud subscription from the drop-down menu. Only those cloud subscriptions that are configured under the SSE vendor selected in <b>Subscription Type</b> , appear in the drop-down menu. These cloud subscriptions are populated based on the configurations under <b>Configure &gt; Security Service Edge (SSE) &gt; SSE Subscriptions</b> .

- 4 Click **Next Step** to activate the next section.
- 5 The fields displayed under **Create Network Service** section vary depending on the selected **Subscription Type**.

The below image and table are for the **Prisma Access** subscription type:

▼ 2. Create Network Service

All form fields are required.

Service Name	<input type="text"/>
Minimum Bandwidth per Tunnel (Mbps)	2 <input type="text"/>
Tunneling Protocol	<input checked="" type="radio"/> IPsec <input type="radio"/> IKEv2
IPsec Crypto Profile	<input type="text"/> Andy-Test-IPsec-Defaults <span style="float: right;">▼</span>
IKE Crypto Profile	<input type="text"/> Andy-Test-IKEv2-Defaults <span style="float: right;">▼</span>
<a href="#" style="border: 1px solid #ccc; padding: 2px 10px; color: inherit; text-decoration: none;">CREATE AND CONTINUE</a>	

Option	Description
Service Name	Enter a unique service name.
Minimum Bandwidth per Tunnel (Mbps)	Enter the required bandwidth. The default value is <b>2</b> .
Tunneling Protocol	By default, IPsec tunneling protocol is selected. You must select the <b>IPsec Crypto Profile</b> and <b>IKE Crypto Profile</b> from the respective drop-down menus. These drop-down menus are populated based on the Profiles created in the <b>Palo Alto Networks Strata Cloud Manager</b> portal.

The below image and table are for the **Symantec** subscription type:

2. Create Network Service

All form fields are required.

Service Name	test12
Tunneling Protocol	<input checked="" type="radio"/> IPsec

**CREATE AND CONTINUE**

Option	Description
Service Name	Enter a unique service name.
Tunneling Protocol	This field is set to <b>IPsec</b> , which is the only supported protocol.

- 6 Click **Create and Continue** to activate the next section.
- 7 Under **Select Profile/Edges** section, configure the following options:

Verify capacity availability at Peer Endpoints for the Edges selected based on the configured Minimum Bandwidth value under "Create Network Service"

**VALIDATE TUNNEL CONFIGURATION**

**SAVE AND FINISH**

Option	Description
Select Profile	Select an <b>SD-WAN</b> Edge Profile from the drop-down menu.
Select Segment	Select a Segment from the drop-down menu. By default, <b>Global Segment</b> is selected.  <b>Note</b> You can select only one Segment for <b>Prisma</b> subscription, whereas multiple Segments can be selected for <b>Symantec</b> subscription.

- 8 Once you select Profile and Segment, a list of Edges associated with the selected Profile gets auto-populated. Select one or more Edges for which you wish to apply the SSE integration.
- 9 If an Edge has more than two WAN links, the first two WAN links are auto-populated in the table. You can select the WAN links that you wish to use for the automation.
- 10 Click **Validate Tunnel Configuration**. A warning is displayed if any of the datacenters is over subscribed.

**Note** The **Validate Tunnel Configuration** button is available only for the **Prisma Access** subscription type. In Prisma deployment, you must buy a license to add bandwidth capacity at a datacenter. This license restricts the maximum throughput, thus displaying a warning.

- 11 Once the tunnel configuration is validated, click **Save and Finish**. The newly created SSE integration appears on the list on the **Security Service Edge (SSE)** landing page.
- 12 If you wish to edit the existing SSE integration, select the SSE integration from the list and click **Edit**. You can also click the SSE integration name link to edit it.
- 13 To delete the SSE integration, select the SSE integration from the list and click **Delete**.

**Note** You cannot delete SSE integrations that are currently used by Edges.

- 14 To monitor the automation status, click the **View** link in the **Tunnel Deployment Status** column. The following screen appears:

## Non SD-WAN Destinations Deployment Status for test

Edge	Action	Status	Created	Last Modified	API Tracking Info
» e2e_symantec_vce	createNvsFromEdgeSite	Complete	Dec 2, 2023, 5:41:15 AM	Dec 2, 2023, 5:41:32 AM	<a href="#">Details</a>
» e2e_symantec_vce	createOrUpdateEdgeConfiguration	Complete	Dec 2, 2023, 5:41:15 AM	Dec 2, 2023, 5:41:15 AM	<a href="#">Details</a>
» e2e_symantec_vce	deleteEdgeConfiguration	Complete	Dec 2, 2023, 5:40:15 AM	Dec 2, 2023, 5:40:15 AM	<a href="#">Details</a>
» e2e_symantec_vce	createOrUpdateEdgeConfiguration	Complete	Dec 1, 2023, 10:03:00 AM	Dec 1, 2023, 10:03:00 AM	<a href="#">Details</a>
» e2e_symantec_vce	createOrUpdateEdgeConfiguration	Complete	Dec 1, 2023, 10:02:15 AM	Dec 1, 2023, 10:02:15 AM	<a href="#">Details</a>
» e2e_symantec_vce	createOrUpdateEdgeConfiguration	Complete	Dec 1, 2023, 9:32:15 AM	Dec 1, 2023, 9:32:15 AM	<a href="#">Details</a>
» e2e_symantec_vce	createOrUpdateEdgeConfiguration	Complete	Dec 1, 2023, 4:29:30 AM	Dec 1, 2023, 4:29:30 AM	<a href="#">Details</a>
» e2e_symantec_vce	createOrUpdateEdgeConfiguration	Complete	Dec 1, 2023, 4:24:30 AM	Dec 1, 2023, 4:24:30 AM	<a href="#">Details</a>

[DONE](#)

The actions `createOrUpdateEdgeConfiguration` and `deleteEdgeConfiguration` indicate the SSE automation to update the Orchestrator Edge Device Settings. The other actions are for third party automations.

**Note** You can also monitor the SSE deployment status on **Monitor > Events** and **Monitor > Network Services > Non SD-WAN Destinations via Edge** screens. For more information, see [Monitor Events](#) and [Monitor Network Services](#).

- To verify whether the tunnels are up, go to **Monitor > Edges**, and hover the mouse under the **Edge Tunnels** column. You can view the details as shown below:

Name	Status	Links	Edge Tunnels	Gateways	Profile	Software version	Model	Serial number	Last Contact
Branch-Edge	Connected	1	NSD Via Edge Tunnels Symantec SSE IPsec SSE - Symantec GE1 Global Segment 34.139.172.102 • Up Draper, US GE1 Global Segment 34.83.136.59 • Up Draper, US	View	Branch Profile	5.2.0.1	Edge 520-V	VC05200055596	Nov 6, 2023, 11:26:59 AM

**What to do next:**

Associate the Security Service Edge Subscription to an Edge. For more information, see [Configure Cloud VPN and Tunnel Parameters for Edges](#).

To direct the network traffic to a specific Enterprise Cloud, navigate to **Configure > Edges > Business Policy**. Click **+ Add** to add a new rule. For more information, see [Create Business Policy Rule](#).

Read the following topics next:

- [Palo Alto Networks Strata Cloud Manager Configuration](#)
- [Configure Symantec API Credentials](#)

## Palo Alto Networks Strata Cloud Manager Configuration

Before configuring the Security Service Edge (SSE) automation, you must first configure **IKE** and **IPsec** profiles to be used by the SSE automation. This is required for initiating the tunnel from the Edge to Prisma Cloud. This is a one-time manual configuration that must be performed in the **Palo Alto Networks Strata Cloud Manager** portal.

Follow the below steps to configure **IKE** and **IPsec** profiles:

---

**Note** This procedure is for guidance purpose only.

---

### Prerequisites

There is no dedicated location in the **Palo Alto Networks Strata Cloud Manager** portal to configure the **IKE** and **IPsec** profiles. Hence, this configuration must be done in the **Remote Networks** configuration section.

You can reuse the existing profiles if they have been already configured and supported by the Edges. To create new profiles, refer to the below template:

- AES 128 CBC
- DH Group 14 (IKE Crypto Profile)
- PFS configured (same as the DH Group value)
- SHA 256
- IKE SA Lifetime 1440 min
- IPsec SA Lifetime 480 min

---

**Note** This template is just an example. You can configure a stronger encryption algorithm if needed.

---

## Procedure

- 1 Log into the Palo Alto Networks Strata Cloud Manager portal.

The following screen is displayed:

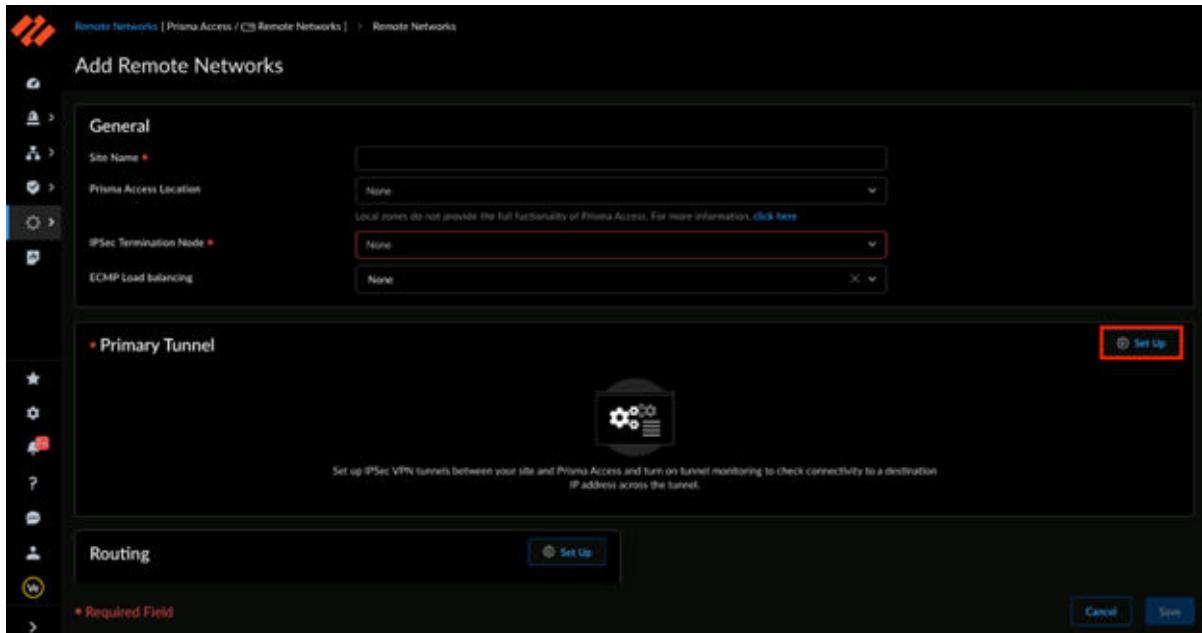
- 2 Navigate to **Workflows > Prisma Access Setup > Remote Networks** as shown in the above screenshot.

The **Remote Networks Setup** screen appears.

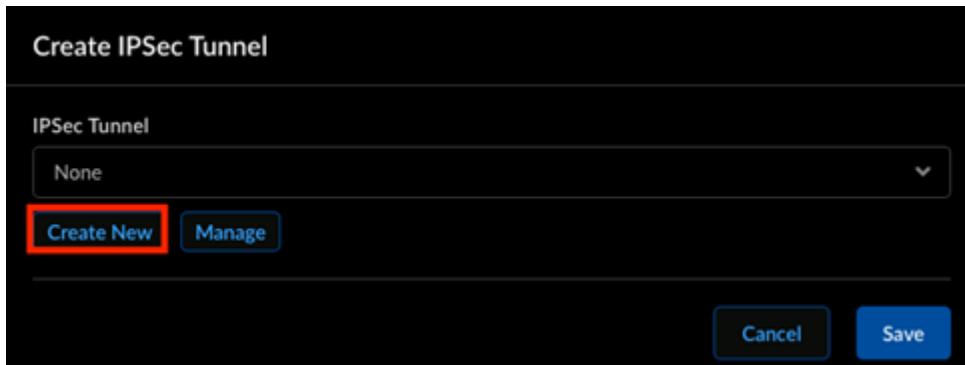
- 3 Click **Add Remote Networks** in the top right corner of the **Remote Networks Setup** screen.

Remote Networks (13)									
			Group By		Routing Information				
	Name	Subnets	Connect...	Status	Tunnel	Config	Prisma Access	Location	
<input type="checkbox"/>	London	10.2.0.0/24	Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	UK	0	192.168.25...
<input type="checkbox"/>	Tokyo	10.6.2.0/24	Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	Japan Central	0	192.168.25...
<input type="checkbox"/>	Sao Paulo	10.3.2.0/24	Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	Brazil South	0	192.168.25...
<input type="checkbox"/>	Frankfurt	10.4.2.0/24	Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	Germany Central	0	192.168.25...
<input type="checkbox"/>	Sydney	10.5.2.0/24	Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	Australia Southeast	0	192.168.25...
<input type="checkbox"/>	PN Branch-Edge		Prisma Access	<span style="color:green;">OK</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	US West	0	192.168.25...
<input type="checkbox"/>	PN-SU_11-edge1		Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	US West	0	192.168.25...
<input type="checkbox"/>	PN-SU_52-edge1		Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	US West	0	192.168.25...
<input type="checkbox"/>	PN-PaloAlto10		Prisma Access	<span style="color:green;">OK</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	US West	0	192.168.25...
<input type="checkbox"/>	PN-d199a37306ad-edg		Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	Nigeria	0	192.168.25...
<input type="checkbox"/>	PN-Home		Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	US East	0	192.168.25...
<input type="checkbox"/>	PN-d199a37306ad-edg		Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	US West	0	192.168.25...
<input type="checkbox"/>	PN-8ae0641a133-11-e		Prisma Access	<span style="color:red;">Error</span>	<span style="color:green;">OK</span>	<span style="color:green;">In sync</span>	US West	0	192.168.25...

- 4 In the **Add Remote Networks** screen, ignore the mandatory fields and directly go to the **IKE** and **IPsec** profile configurations, by clicking **Set Up** in the **Primary Tunnel** section as shown below:



- 5 In the **Create IPsec Tunnel** screen, click **Create New**.



- 6 Ignore all the mandatory fields and scroll down to the bottom of this screen. Click **IKE Advanced Options**.

**Create IPSec Tunnel**

[Create IPSec Tunnel](#)

**Static IP \***

IKE Passive Mode

Turn on Tunnel Monitoring

**Proxy ID**  
IPv4      IPv6

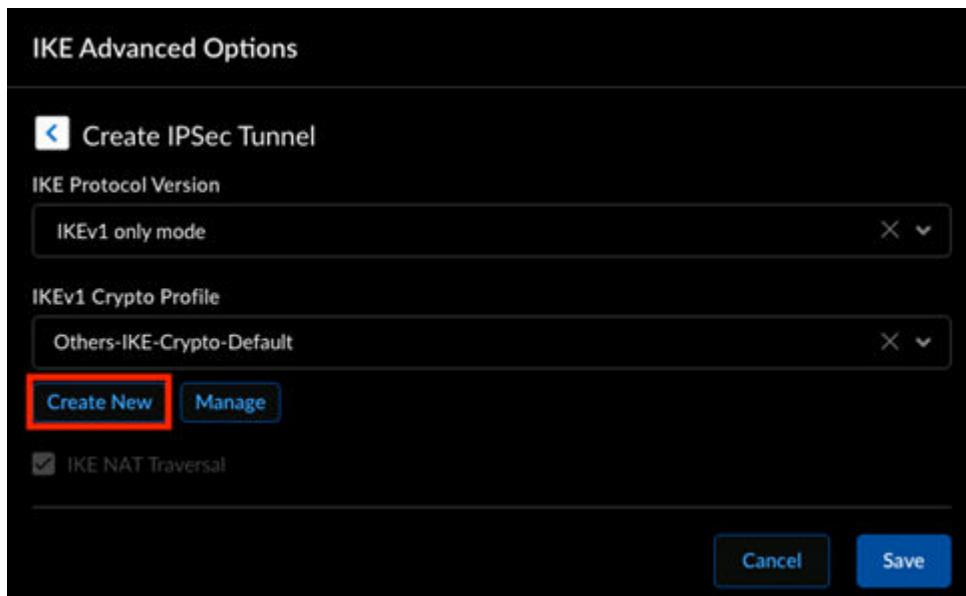
	Proxy ID	Local Proxy ID	Remote Proxy ...	Protocol
Items (0)				

**IKE Advanced Options**

**IPSec Advanced Options**

[Cancel](#) [Save](#)

- 7 Click **Create New** on the **IKE Advanced Options** screen.



**Note** Ignore all the pre-configured options. You must create a new **IKE** profile to be used for the VMware SSE automation.

- 8 Clicking **Create New** displays the following screen:

The screenshot shows the 'Create IKE Crypto Profile' dialog box. At the top left is a back arrow icon and the title 'Create IKE Crypto Profile'. Below the title is a link 'IKE Advanced Options'. The form fields include:

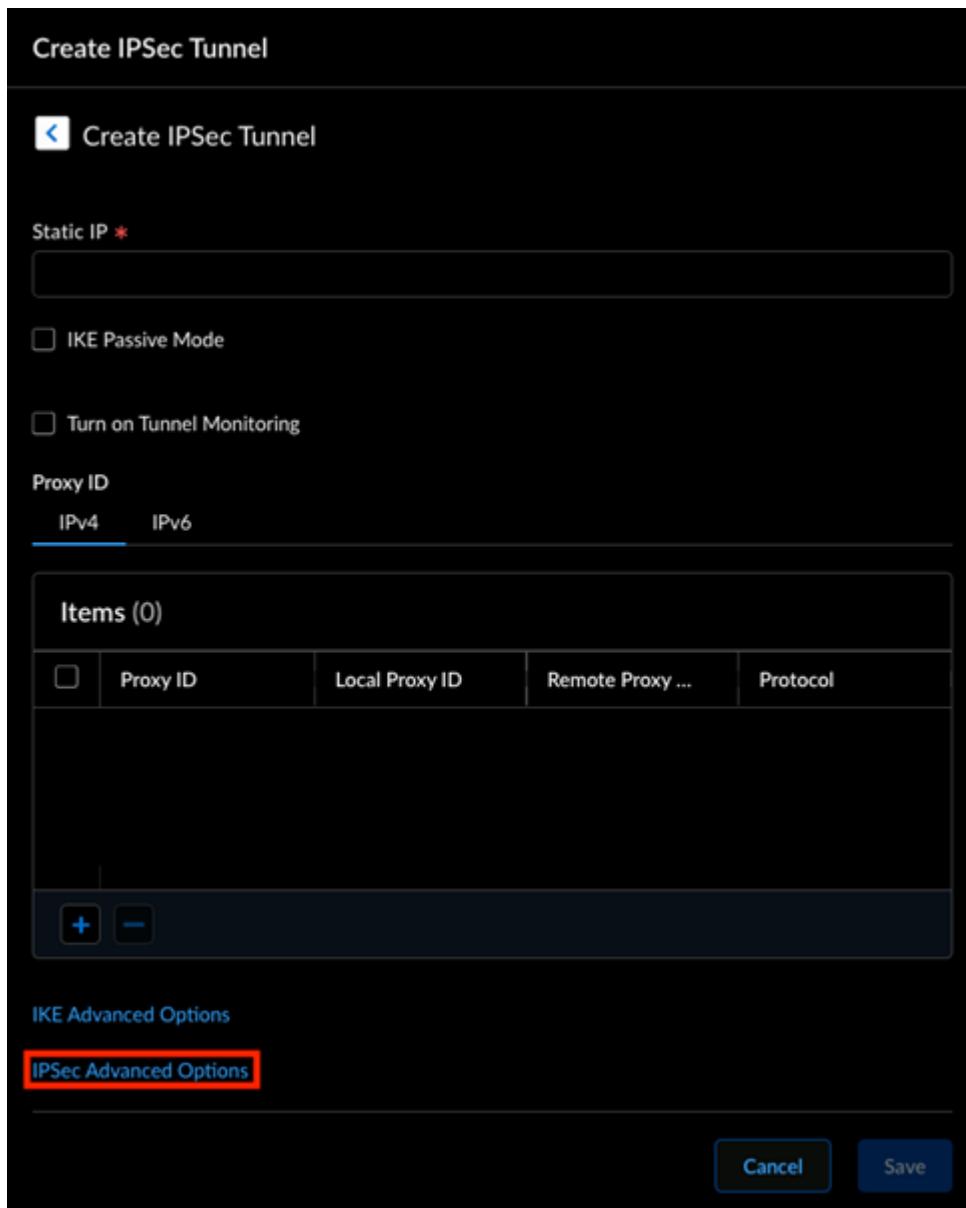
- Name \***: A text input field containing 'VMware-IKE-defaults'.
- Encryption \***: A dropdown menu showing 'aes-128-cbc ...' with a '+' button to add more options.
- Authentication \***: A dropdown menu showing 'sha256 ...' with a '+' button to add more options.
- DH Group \***: A dropdown menu showing 'group14 ...' with a '+' button to add more options.
- Lifetime**: Two input fields: '24' and 'Hours' with a dropdown arrow.
- IKEv2 Authentication Multiple**: A text input field showing '0 [false - 50]'.

At the bottom left is a red note: **\* Required Field**. At the bottom right are two buttons: 'Cancel' and 'Save'.

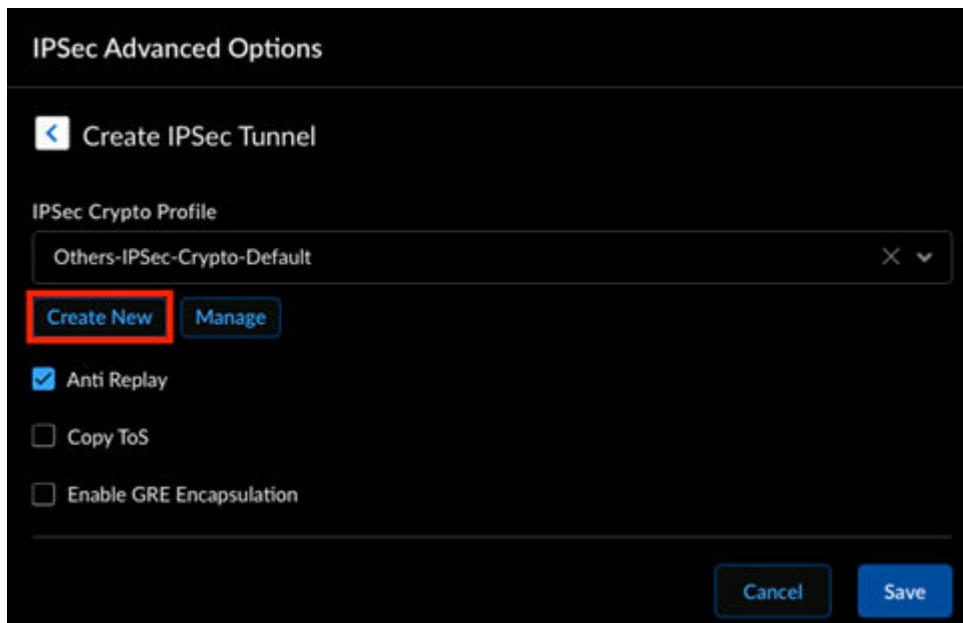
- 9 Enter the values based on the template provided in the pre-requisites section, and then click **Save**.
- 10 Click **Save** on the **IKE Advanced Options** screen to save the **IKE** profile.

This step takes you back to the **Create IPsec Tunnel** screen.

- 11 On the **Create IPsec Tunnel** screen, click **IPsec Advanced Options** as shown below:



- 12 Click **Create New** on the **IPsec Advanced Options** screen.



**Note** Ignore all the pre-configured options. You must create a new **IPsec** profile to be used for the VMware SSE automation.

- 13 Clicking **Create New** displays the following screen:

**Create IPSec Crypto Profile**

**IPSec Advanced Options**

**Name \***  
VMware-IPsec-Defaults

**IPSec Protocol**  
ESP

**Encryption \***  
aes-128-cbc ...

**Authentication \***  
sha256 ...

**DH Group**  
no-pfs

**Lifetime \***  
8 Hours

**Lifesize**  
[1 - 65535] MB

**Cancel** **Save**

- 14 Enter the values based on the template provided in the pre-requisites section, and then click **Save**.

- 15 Click **Save** on the **IPsec Advanced Options** screen to save the **IPsec** profile.

#### What to do next

You may now log into the Orchestrator to configure the Security Service Edge (SSE) and initiate the automation. For more information, see [Chapter 18 Security Service Edge \(SSE\)](#).

## Configure Symantec API Credentials

Before configuring the Security Service Edge (SSE) automation, you must first configure API credentials on the **Symantec Cloud** portal, which must be then used on the Orchestrator subscription screen.

Follow the below steps to configure Symantec API credentials:

### Procedure

- 1 Log into the **Symantec Cloud** portal, and then click **Account Configuration**.

The **Account Configuration** screen appears:

Cloud Secure Web Gateway

Account Configuration

## Account Configuration

**General**

- [Products & Licensing](#) View account information and licensed products
- [Data Retention & Privacy](#) Configure how Cloud SWG handles PII and other data

**Administrators & Access Control**

- [Administrators](#) Manage access to your account
- [Account Auditing](#) View account activity
- [API Credentials](#) Integrate external systems with Cloud SWG

**Reporting Settings**

- [Log Export](#) Download traffic logs
- [Event Streaming](#) Manage event streaming feeds
- [Reporting Alerts](#) Receive notifications when traffic matches the specified conditions
- [Cost Calculations for Reports](#)

- 2 Under the **Administrators & Access Control** section, click **API Credentials**, and then click the **Add** button.

The following window appears:

**Add**

Create API Credentials to integrate external systems with the Cloud SWG.

Username:	<input type="text"/>	<input type="button" value=""/>
Password:	<input type="text"/>	<input type="button" value=""/>
Expiry:	<input type="button" value="Time-based"/> <input type="button" value="Never"/>	
Access:	<input checked="" type="checkbox"/> Reporting Access Logs <input checked="" type="checkbox"/> Location Management <input checked="" type="checkbox"/> Audit Logs <input checked="" type="checkbox"/> Agent Config Management <input checked="" type="checkbox"/> Dedicated IPs <input checked="" type="checkbox"/> Policy List Management	
Comments:	<small>255 of 255 characters left</small>	

**Note** Once saved, the token cannot be displayed again. Ensure that you have a copy.

- 3 Configure the following:

Option	Description
Username	This field is auto-generated and cannot be edited.
Password	This field is auto-generated and cannot be edited.
Expiry	To set an expiry for the entered credentials, select <b>Time-based</b> , and then select the date and time as required.
Reporting Access Logs	Select this check box to allow the user to download or sync the Access Logs from Cloud SWG to Reporter or a third party SIEM.
<b>Note</b> Selecting this check box is mandatory.	
Location Management	Select this check box to allow the user to create or update locations. This is useful when the external IP address of a location changes.
<b>Note</b> Selecting this check box is mandatory.	
Audit Logs	Select this check box to allow the user to download the audit logs and retain the data post expiry.

Option	Description
Agent Config Management	Select this check box to allow the user to create or update agent configuration.
Dedicated IPs	Select this check box to allow dedicated IP management.
Policy List Management	Select this check box to allow access to the REST API for Policy List Management.
Comments	Enter your comments if any. This field is not mandatory.

**Note** Make sure to copy the entered **Username** and **Password**. You must use these credentials for the Symantec SSE automation.

- 4 Click **Save**.

#### What to do next

You may now log into the Orchestrator to configure the Security Service Edge (SSE) and initiate the automation.

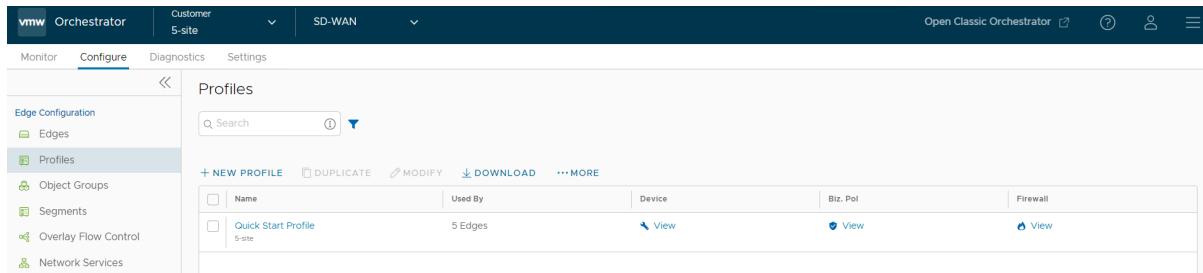
# Configure Profiles

19

Profiles define a template configuration that can be applied to multiple Edges. A default profile, named as **Quick Start Profile** is available when you install SASE Orchestrator.

You can configure the Profiles by performing the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click the **Configure** tab.
- 2 From the left menu, select **Profiles**. The **Profiles** page appears.



Name	Used By	Device	Biz. Pol	Firewall
Quick Start Profile 5-site	5 Edges	<a href="#">View</a>	<a href="#">View</a>	<a href="#">View</a>

Option	Description
Name	Displays the name of the Profile. Click the link to modify the configurations. See <a href="#">Configure Profile settings</a> .
Used By	Displays the number of Edges associated with the Profile.
Device	Click the <a href="#">View</a> link to modify the configurations. See <a href="#">Configure Profile settings</a> .
Biz. Pol	Click the <a href="#">View</a> link to modify the configurations. See <a href="#">Configure Business Policies</a> .
Firewall	Click the <a href="#">View</a> link to modify the configurations. See <a href="#">Configure Profile Firewall</a> .

You can perform the following actions:

- **New Profile** – Click this option to create a new Profile. See [Create Profile](#).
- **Duplicate** – Select a profile and click this option to create a duplicate of the selected Profile.
- **Modify** – Select a profile and click this option to edit the selected Profile. See [Configure Profile settings](#).
- **Download** – Click this option to download the details of all the Profiles into an MS Excel file.

Click **More** to perform the following:

- **Delete** – Select a profile and click this option to delete the selected Profile. You cannot delete the Profiles that are associated with Edges.

Read the following topics next:

- [Create Profile](#)
- [Configure Profile settings](#)
- [Global IPv6 Settings for Profiles](#)
- [View Profile Information](#)

## Create Profile

After installing SASE Orchestrator, a default profile is available. If required, you can create additional Profiles.

To create a Profile, perform the following steps:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click the **Configure** tab.
- 2 From the left menu, select **Profiles**. The **Profiles** page appears.
- 3 In the **Profiles** page, click **New Profile**.

The screenshot shows a modal dialog titled "New Profile". At the top right is a close button (X). The form contains two input fields: "Profile name\*" with the value "Bastion Profile" and "Description" with the placeholder "Description". At the bottom are two buttons: "CANCEL" and a blue "CREATE" button.

- 4 Enter a name and description for the new Profile and click **Create**.
- 5 The **Device** tab opens, which provides options to configure the Profile settings. For more information, see [Configure Profile settings](#).

# Configure Profile settings

Profiles provide a composite of the configurations created in Segments and Network Services.

To configure a specific Profile, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click the **Configure** tab.
- 2 From the left menu, click **Profiles**. The **Profiles** page displays the existing Profiles.
- 3 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. The configuration options are displayed in the **Device** tab.

- 4 The **View** drop-down menu at the right side of the page allows the user to select the view options. The available options are **Expand All** and **Collapse All**. By default, the settings are collapsed.
- 5 The **Sort** drop-down menu at the right side of the page allows the user to select the sort options: **Sort by category** and **Sort by segment aware**. You can view the configuration settings sorted by category or segment aware. By default, the settings are sorted by category. If you choose to sort by segmentation, the settings are grouped as segment aware and segment agnostic.
- 6 Configure the required settings and click **Save Changes**.

---

**Note** On the **Device** page, whenever you make configuration changes for the selected Profile, a footer notification appears at the left bottom corner of the screen. You can click the notification to view the recent configuration changes.

---

- 7 On the top right corner of the selected Profile page, you can click the **Shortcuts** drop-down menu to perform the following actions:
  - **Duplicate Profile** – Clicking this option opens a **Copy Profile** dialog box that allows you to create a duplicate of the selected Profile.
  - **Modify Profile** – Clicking this option navigates to the **Overview** page of the selected profile, where you can edit the properties of the selected Profile.
  - **Delete Profile** – Clicking this option opens a **Delete Profile** dialog box that allows you to delete the selected Profile. You cannot delete the Profiles that are associated with Edges.

For more details on various Profile configuration settings, see [Configure a Profile Device](#).

## Global IPv6 Settings for Profiles

For IPv6 addresses, you can activate some of the configuration settings globally.

To activate global settings for IPv6 at the Profile level:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. The configuration options for the selected Profile are displayed in the **Device** tab.
- 3 Under the **Connectivity** category, click **Global IPv6**.

The screenshot shows the VMware SD-WAN Enterprise portal interface. The left sidebar has a tree view with 'Edge Configuration' expanded, showing 'Profiles' selected. The main content area is titled 'Profiles / Quick Start Profile' and shows 'Quick Start Profile' used by 6 Edges. The 'Device' tab is selected. Under the 'Connectivity' section, the 'Global IPv6' section is expanded, showing several configuration options with toggle switches. Most options are set to 'On'. The 'Segment' dropdown is set to 'GLOBAL SEGMENT'. The bottom of the screen shows other collapsed sections: 'Wi-Fi Radio', 'VPN Services', 'Routing & NAT', and 'Telemetry'.

Category	Setting	Status
IPv6 Configuration	All IPv6 Traffic	On
	Routing Header Type 0 Packets	On
	Enforce Extension Header Validation	On
	Enforce Extension Header Order Check	On
	Drop & Log Packets for RFC Reserved Fields	On
ICMPv6 Messages		
ICMPv6 Destination Unreachable messages	On	
ICMPv6 Time Exceeded Message	On	
ICMPv6 Parameter Problem Message	On	

- 4 You can activate or deactivate the following settings, by using the toggle button. By default, all the options are deactivated.

Option	Description
All IPv6 Traffic	Allows all IPv6 traffic in the network.  <b>Note</b> By default, this option is activated.
Routing Header Type 0 Packets	Allows Routing Header type 0 packets. Deactivate this option to prevent potential DoS attack that exploits IPv6 Routing Header type 0 packets.
Enforce Extension Header Validation	Allows to check the validity of IPv6 extension headers.
Enforce Extension Header Order Check	Allows to check the order of IPv6 Extension Headers.
Drop & Log Packets for RFC Reserved Fields	Allows to reject and log network packets if the source or destination address of the network packet is defined as an IP address reserved for future definition.
ICMPv6 Destination Unreachable messages	Generates messages for packets that are not reachable to IPv6 ICMP destination.
ICMPv6 Time Exceeded Message	Generates messages when a packet sent by IPv6 ICMP has been discarded as it was out of time.
ICMPv6 Parameter Problem Message	Generates messages when the device finds problem with a parameter in ICMP IPv6 header.

By default, the configurations are applied to all the Edges associated with the Profile. If required, you can modify the settings for each Edge by clicking the **Override** option in the **Configure > Edges > {Edge Name} > Device > Connectivity > Global IPv6** page.

## View Profile Information

The Profile Overview page provides complete view of all the configurations of a specific profile. You can also modify the name, description, and the local credentials of the selected profile.

To access the Profile Overview page in the Orchestrator UI:

- In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- Click the link to a Profile and then click the **Overview** tab. You can edit the Profile Name, Description, and Local Credentials.

**Properties**

- Name: Quick Start Profile
- Description: 5-site
- Local Credentials: \*\*\*\*\* [EDIT](#)

**Profile Overview**

Enabled Models: Edge 500, Edge 5X0, Edge 510, Edge 510-LTE, Edge 515, Edge 6X0, Edge 610-LTE, Edge 840, Edge 1000, Edge 2000, Edge 3X00, Edge 3X10, Virtual Edge

**Services**

Dynamic Multi-Path Optimization	<input checked="" type="radio"/> On
Application Recognition	<input checked="" type="radio"/> On
Identity	<input checked="" type="radio"/> On
DHCP	<input checked="" type="radio"/> On
Wireless	<input checked="" type="radio"/> On
802.1x	<input type="radio"/> Off

**Segments**

Segment	Netflow	Cloud VPN	QoS	BGP	Multicast	Cloud Security	Auth	Business Policy	Firewall
Global Segment	<input type="radio"/> Off	22 rules	1 outbound rule						
segment1	<input type="radio"/> Off	<input type="radio"/> Off	N/A	<input type="radio"/> Off	<input type="radio"/> Off	<input type="radio"/> Off	<input type="radio"/> Off	22 rules	1 outbound rule
segment2	<input type="radio"/> Off	<input type="radio"/> Off	N/A	<input type="radio"/> Off	<input type="radio"/> Off	<input type="radio"/> Off	<input type="radio"/> Off	22 rules	1 outbound rule

3 items

- 3 Default Local Credentials are set to a random password by the Orchestrator. You can change the random password by clicking the **EDIT** button and then selecting the **Change Password** check box. Enter the new password and click **SUBMIT**

## Modify Local Credentials

User \* admin

Password \* \*\*\*\*

Change Password

New Password \* .....

Confirm Password \* .....

[CLOSE](#) [SUBMIT](#)

---

**Note**

- Ensure the new password meets the following password policy criteria:
    - Should be at least 8 characters
    - Should be less than 32 characters
    - Should have at least one number
    - Should have at least one lower case character
  - Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
- 

**Note** The updated credentials are applied to the Profile and all associated Edges. If you add a new Edge to a Profile without changing the default local credentials for the Profile, the local credentials for the Edge will be different from that of the Profile. You must change the local credentials at the Edge level. For details, refer to [Chapter 28 View Edge Information](#).

---

- 4 The **Profile Overview** section displays Edge models that are activated for the profile, network services configured for the profile, and the segments configuration details assigned to the profile. For more information, see [Chapter 19 Configure Profiles](#).

# Configure Device Settings for Profiles

20

This section describes how to configure a profile device.

---

**Note** If you are logged in using a user ID with Customer Support privileges, you will only be able to view SASE Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

---

In the **SD-WAN** service of the Enterprise portal, you can perform various configuration settings for a Profile by navigating to the **Configure > Profiles > Device** tab. For more information about Segmentation, see [Chapter 8 Configure Segments](#).

Read the following topics next:

- [Configure a Profile Device](#)

## Configure a Profile Device

Device configuration page allows you to assign segments to a Profile and configure various settings and interfaces to be associated with a Profile.

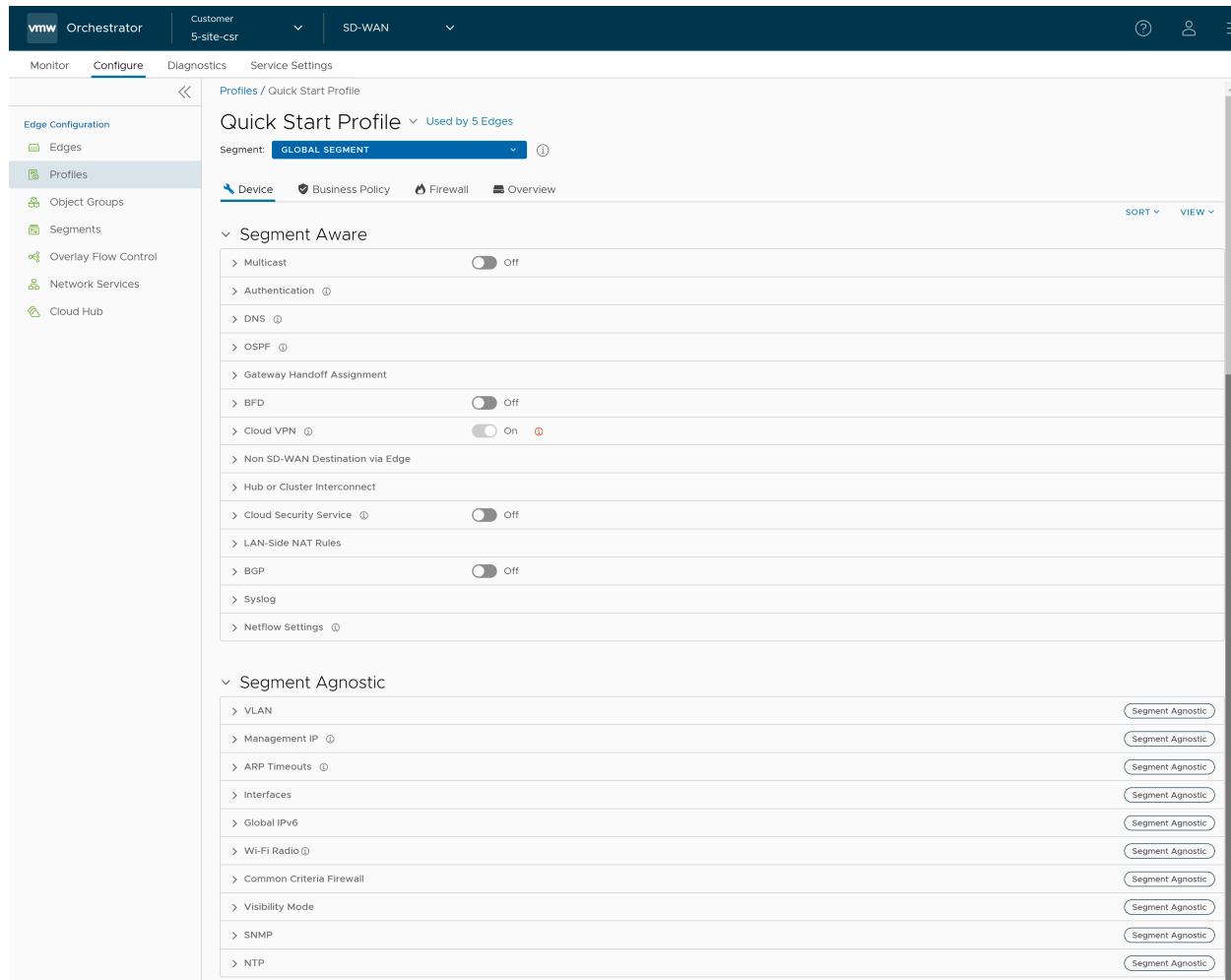
In the **SD-WAN** service of the Enterprise portal, when you click **Configure > Profiles** and select a Profile. The configuration options for the selected Profile are displayed in the **Device** tab.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'VMW Orchestrator', 'Customer 5-site-csr', 'SD-WAN', and user icons. The left sidebar has categories: Edge Configuration (Edges, Profiles, Object Groups, Segments, Overlay Flow Control, Network Services), Monitor, Configure (selected), Diagnostics, and Service Settings. The main content area is titled 'Profiles / Quick Start Profile' and shows a 'Quick Start Profile' used by 5 Edges. It has sections for Connectivity (VLAN, Management IP, ARP Timeouts, Interfaces, Global IPv6, Wi-Fi Radio, Common Criteria Firewall), VPN Services (Cloud VPN, Non SD-WAN Destination via Edge, Hub or Cluster Interconnect, Cloud Security Service), Routing & NAT (Multicast, DNS, OSPF, BFD, LAN-Side NAT Rules, BGP), Telemetry, and Edge Services. A 'Segment' dropdown at the top is set to 'GLOBAL SEGMENT'. On the right, there are 'SORT' and 'VIEW' dropdowns, and a 'SHORTCUTS' section with various icons.

The **View** drop-down menu at the left side of the page allows the user to select the view options. The available options are **Expand All** and **Collapse All**. By default, the settings are collapsed.

The **Sort** drop-down menu at the left side of the page allows the user to select the sort options: **Sort by category** and **Sort by segment aware**. You can view the configuration settings sorted by category or segment aware. By default, the settings are sorted by category. If you choose to sort by segmentation, the settings are grouped as Segment Aware and Segment Agnostic as shown in the following screenshot.

In Segment Aware configurations, configuration settings apply only to a specific segment selected from the Segment drop-down menu. In Segment Agnostic configurations, configuration settings apply to multiple segments.



**Note** On the **Device** page, whenever you make configuration changes for the selected Profile, an action bar appears at the bottom of the screen. You can click the notification to view the recent configuration changes and save the changes made to the Profile.

## Profile Device Configurations—A Roadmap

The following table provides the list of Profile-level configurations:

### Connectivity

Settings	Description
VLAN	Configure the VLANs with both IPv4 and IPv6 addresses for Profiles. Click the IPv4 or IPv6 tabs to configure the corresponding IP addresses for the VLANs. See <a href="#">Configure VLAN for Profiles</a> .
Management IP	The Management IP address is used as the source address for local services like DNS and as a destination for diagnostic tests like pinging from another Edge. See <a href="#">Configure Management IP Address for Profiles</a> .

Settings	Description
ARP Timeouts	By default, the ARP Timeout values are configured. If required, select the <b>Override default ARP Timeouts</b> checkbox, to modify the default values. See <a href="#">Configure Address Resolution Protocol Timeouts for Profiles</a> .
Interfaces	Configure the Interface Settings for each Edge model. See <a href="#">Configure Interface Settings for Profiles</a> .
Global IPv6	Activate IPv6 configurations globally. See <a href="#">Global IPv6 Settings for Profiles</a> .
Wi-Fi Radio	Turn on or turn off Wi-Fi Radio and configure the band of radio frequencies. See <a href="#">Configure Wi-Fi Radio Settings</a> .
Common Criteria Firewall	Common Criteria (CC) is an international certification accepted by many countries. Obtaining the CC certification is an endorsement that our product has been evaluated by competent and independent licensed laboratories for the fulfilment of certain security properties. This certification is recognized by all the signatories of the Common Criteria Recognition Agreement (CCRA). The CC is the driving force for the widest available mutual recognition of secure IT products. Having this certification is an assurance of security to a standard extent and can provide VMware with the much needed business parity or advantage with its competitors. Enterprise users can configure the Common Criteria Firewall settings. By default, this feature is deactivated. See <a href="#">Configure Common Criteria Firewall Settings for Profiles</a> .

## VPN Services

Settings	Description
Cloud VPN	<p>Activate Cloud VPN to initiate and respond to VPN connection requests. In the Cloud VPN, you can establish tunnels as follows:</p> <ul style="list-style-type: none"> <li>■ Branch to Hub VPN</li> <li>■ Branch to Branch VPN</li> <li>■ Edge to Non SD-WAN via Gateway</li> </ul> <p>Select the checkboxes as required and configure the parameters to establish the tunnels. See <a href="#">Configure Cloud VPN for Profiles</a>.</p>
Non SD-WAN Destination via Edge	<p>Activate to establish tunnel between a branch and Non SD-WAN destination via Edge. See <a href="#">Configure Tunnel Between Branch and Non SD-WAN Destinations via Edge</a>. Click <b>Add</b> to add Non SD-WAN Destinations. Click <b>New NSD via Edge</b> to create new Non SD-WAN Destination via Edge. See <a href="#">Configure Non SD-WAN Destinations via Edge</a>.</p>

Settings	Description
Hub or Cluster Interconnect	VMware SD-WAN supports interconnection of multiple Hub Edges or Hub Clusters to increase the range of Spoke Edges that can communicate with each other. This feature allows communication between the Spoke Edges connected to one Hub Edge or Hub Cluster and the Spoke Edges connected to another Hub Edge or Hub Cluster, using multiple overlay and underlay connections. See <a href="#">Hub or Cluster Interconnect</a> .
Cloud Security Service	Activate to establish a secured tunnel from an Edge to cloud security service sites. This allows the secured traffic being redirected to third-party cloud security sites. See <a href="#">Chapter 11 Cloud Security Services</a> .
Zscaler	Allows to establish a secured tunnel from an Edge to Zscaler sites. See <a href="#">Configure Zscaler Settings for Profiles</a> .
Gateway Handoff Assignment	Allows to assign Partner Gateways for Profiles or Edges. In order for customers to be able assign Partner Gateways, the Partner Handoff feature must be activated for the customers. See <a href="#">Assign Partner Gateway Handoff</a> .
Controller Assignment	Allows to assign Controllers for Profiles or Edges. In order for customers to be able assign Controllers, the Partner Handoff feature must be activated for the customers. See <a href="#">Assign Controllers</a> .
Secure Access Service	Allows to configure Secure Access Service for Profiles. See <a href="#">Configure Secure Access Service for Profiles</a> .

## Routing & NAT

Settings	Description
Multicast	Activate and configure Multicast to send data to only interested set of receivers. See <a href="#">Configure Multicast Settings for Profiles</a> .
DNS	Use the DNS Settings to configure conditional DNS forwarding through a private DNS service and to specify a public DNS service to be used for querying purpose. See <a href="#">Configure DNS for Profiles</a> .
OSPF	Configure OSPF areas for the selected Profile. See <a href="#">Activate OSPF for Profiles</a> .
BFD	Configure BFD settings for the selected Profile. See <a href="#">Configure BFD for Profiles</a> .
LAN-Side NAT Rules	Allows you to NAT IP addresses in an unadvertised subnet to IP addresses in an advertised subnet. See <a href="#">LAN-Side NAT Rules at Profile Level</a> .
BGP	Configure BGP for Underlay Neighbors and Non SD-WAN Neighbors. See <a href="#">Configure BGP</a> .

## Telemetry

Settings	Description
Visibility Mode	Choose the visibility mode to track the network using either MAC address or IP address. See <a href="#">Configure Visibility Mode for Profiles</a> .
Syslog	Configure Syslog collector to receive SASE Orchestrator bound events and firewall logs from the Edges configured in an Enterprise. See <a href="#">Configure Syslog Settings for Profiles</a> .
Netflow Settings	As an Enterprise Administrator, you can configure Netflow settings at the Profile level. <a href="#">Configure Netflow Settings for Profiles</a> .
SNMP	Activate the required SNMP version for monitoring the network. Ensure that you download and install all the required SNMP MIBs before enabling SNMP. See <a href="#">Configure SNMP Settings for Profiles</a> .

## Edge Services

Settings	Description
Authentication	<p>Allows to select a RADIUS server to be used for authenticating a user. See <a href="#">Configure Authentication Settings for Profiles</a>.</p> <p>Click <b>New RADIUS Service</b> to create a new RADIUS server. For more information, see <a href="#">Configure Authentication Services</a>.</p>
NTP	Activate to synchronize the system clocks of Edges and other network devices. See <a href="#">Configure NTP Settings for Profiles</a> .

## Assign Segments in Profile

After creating a Profile, you can select the Segments that you want to include in your profile from the **Segment** drop-down menu in the **Device** tab.

To assign segments to a Profile, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile for which you want to assign segments. You can also select a Profile and click **Modify** to configure the Profile. The configuration options for the selected Profile are displayed in the **Device** tab.
- 3 From the **Segment** drop-down menu, click the **Change Profile Segments** link. The **Change Profile Segments** dialog box appears.

X

## Change Profile Segments

Profile Quick Start Profile

Available segments for this Profile

<input type="checkbox"/> All Segments	VLAN IDs	Edge Models
<input checked="" type="checkbox"/> Global Segment [REGULAR]	1	Virtual Edge, Edge 2000, Edge 1000, Edge 3X00, Edge 3X10, Edge 6X0, Edge 610-LTE, Edge 840, Edge 510, Edge 510-LTE, Edge 5X0, Edge 500
<input checked="" type="checkbox"/> Segment1 [REGULAR]	100	<input checked="" type="checkbox"/> None
<input checked="" type="checkbox"/> Segment2 [REGULAR]	101	<input checked="" type="checkbox"/> None

3 1 - 3 of 3 items

Show only selected

**CANCEL** **UPDATE SEGMENTS**

- 4 In this dialog box, you can select the Segments that you want to include in your profile. Segments with a lock symbol next to them indicate that the Segment is in use within a profile, and it cannot be removed. Segments available for use will be displayed under **All Segments**.
- 5 Click **Update Segments** and then click **Save Changes**.

After you have assigned a Segment to the Profile, you can configure your Segment through the **Segment** drop-down menu. All Segments available for configuration are listed in the **Segment** drop-down menu. If a Segment is assigned to a VLAN or interface, it will display the VLAN ID and the Edge models associated with it.

When you choose a Segment to configure from the **Segment** drop-down menu, depending upon the Segment's options, the settings associated that Segment display in the **Segments** area.

## Configure VLAN for Profiles

As an Enterprise Administrator, you can configure VLANs in a Profile.

To configure VLAN settings in a Profile:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. You can also select a Profile and click **Modify** to configure the Profile.
- 3 The configuration options for the selected Profile are displayed in the **Device** tab.
- 4 Scroll down to the **Connectivity** category and click **VLAN**.

- 5 You can add a new VLAN by clicking **+ Add VLAN**. You can delete a selected VLAN by clicking the **Delete**.

**Note** A VLAN that has been already assigned to a device interface, cannot be deleted.

- 6 Click **IPv4** or **IPv6** button to display the respective list of VLANs.
- 7 Clicking **+ Add VLAN** displays the following screen:

## Add VLAN

### General Settings

**Segment \***

**VLAN Name \***

**VLAN ID \***

**Description**   
Maximum 256 characters

**LAN Interfaces** Applicable at the edge level

**SSID** Applicable at the edge level

**ICMP Echo Response**  Yes

**DNS Proxy**  Enabled

### IPv4 Settings

Active ⓘ

**Assign Overlapping Subnets**  Yes

**Edge LAN IPv4 Address**

**Cidr Prefix**

### Network

**OSPF**  OSPF is not enabled for the selected segment

**Multicast** Select a segment to configure Multicast

**VNF Insertion** Select a segment to configure VNF insertion

**Advertise**  Yes

**Fixed IPs** Applicable at the edge level

### IPv4 DHCP Server

**Type** ACTIVATED RELAY DEACTIVATED

**DHCP start**

**Num. Addresses \***

**Lease Time \***

### Options

+ ADD ||| DELETE

<input type="checkbox"/>	Option	Code	Data Type	Value
 No items found. Add a new option.				

0 items

### IPv6 Settings

Active ⓘ

**Assign Overlapping Subnets**  Yes

**Edge LAN IPv6 Address**

**Prefix Length**

### Network

**Advertise**  Yes

**Fixed IPs** Applicable at the edge level

- 8 In the **Add VLAN** window, configure the following VLAN details:

Option	Description
<b>General Settings</b>	
Segment	Select a segment from the drop-down list. The VLAN belongs to the selected segment.
VLAN Name	Enter a unique name for the VLAN.
VLAN ID	Enter the VLAN ID.
Description	Enter a description. This field is optional.
LAN Interfaces	You can configure the LAN Interfaces only at the Edge level.
SSID	You can configure the Wi-Fi SSID details for the VLAN only at the Edge level.
ICMP Echo Response	Select the check box to allow the VLAN to respond to ICMP echo messages.
DNS Proxy	This check box is selected by default. This option allows you to activate or deactivate a <b>DNS Proxy</b> , irrespective of the IPv4 or IPv6 DHCP Server settings.
<b>IPv4 and IPv6 Settings</b>	
<p><b>Note</b> You can activate either IPv4 or IPv6 or both settings.</p>	
Assign Overlapping Subnets	<p>Select the check box if you want to assign the same subnet for the VLAN to every Edge in the Profile and define the subnet in the Edge LAN IP Address. If you want to assign different subnets to every Edge, do not select the check box and configure the subnets on each Edge individually.</p> <p><b>Note</b> Overlapping subnets for the VLAN are supported only for SD-WAN to SD-WAN traffic (provided LAN side NAT is activated) and SD-WAN to Internet traffic. Overlapping subnets are not supported for SD-WAN to Cloud Web Security traffic.</p>
Edge LAN IPv4/IPv6 Address	This option is available only if <b>Assign Overlapping Subnets</b> is set to <b>Yes</b> . Enter the LAN IPv4/IPv6 address of the Edge.
Cidr Prefix / Prefix Length	This option is available only if <b>Assign Overlapping Subnets</b> is set to <b>Yes</b> . Enter the CIDR prefix for the LAN IPv4/IPv6 address.
Network	Enter the IPv4/IPv6 address of the Network.

Option	Description
OSPF	<p>This option is activated only when you have configured OSPF for the Edge. Select the check box and choose an OSPF from the drop-down list.</p> <p><b>Note</b> The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6, which is only available in the 5.2 release.</p> <p>For more information on OSPF settings and OSPFv3, see <a href="#">Activate OSPF for Profiles</a>.</p>
Multicast	<p>This option is activated only when you have configured multicast settings for the Edge. You can configure the following multicast settings for the VLAN:</p> <ul style="list-style-type: none"> <li>■ IGMP</li> <li>■ PIM</li> </ul> <p>Click <b>toggle advanced multicast settings</b> to set the following timers:</p> <ul style="list-style-type: none"> <li>■ PIM Hello Timer</li> <li>■ IGMP Host Query Interval</li> <li>■ IGMP Max Query Response Value</li> </ul> <p><b>Note</b> This option is available only under <a href="#">IPv4 Settings</a>.</p>
VNF Insertion	<p>Select the check box to insert a VNF to the VLAN, which redirects traffic from the VLAN to the VNF. To activate <b>VNF Insertion</b>, ensure that the selected segment is mapped with a service VLAN. For more information about VNF, see <a href="#">Security Virtual Network Functions</a>.</p> <p><b>Note</b> This option is available only under <a href="#">IPv4 Settings</a>.</p>
Advertise	<p>Select the check box to advertise the VLAN to other branches in the network.</p>
Fixed IPs	<p>You can configure the fixed IP only at the Edge level.</p>

#### IPv4/IPv6 DHCP Server:

- The available options for **IPv4 DHCP Server** are **Activated**, **Relay**, and **Deactivated**.
- The available options for **IPv6 DHCP Server** are **Activated** and **Deactivated**.

Option	Description
<b>Activated:</b> Activates the DHCP with the Edge as the DHCP server. Following configuration options are available for this type.	
DHCP Start	Enter a valid IPv4/IPv6 address available within the subnet.
Num. Addresses	Enter the number of IPv4/IPv6 addresses available on a subnet in the DHCP Server.

Option	Description
Lease Time	Select the period of time from the drop-down list. This is the duration the VLAN is allowed to use an IPv4/IPv6 address dynamically assigned by the DHCP Server.
Options	Click <b>Add</b> and select pre-defined or custom DHCP options from the drop-down list. The DHCP option is a network service passed to the clients from the DHCP server. For a custom option, enter the <b>Code</b> , <b>Data Type</b> , and <b>Value</b> . Click <b>Delete</b> to delete a selected option.
<b>Relay:</b> Activates the DHCP with the DHCP Relay Agent installed at a remote location. Following configuration options are available for this type.	
Source from Secondary IP(s)	When you select this check box, the DHCP discover/request packets from the client are relayed to the DHCP Relay servers sourced from the primary IP address and all the secondary IP addresses configured for the VLAN. The reply from the DHCP Relay servers is sent back to the client after rewriting the source and destination. The DHCP server receives the request from both the primary and secondary IP addresses and the DHCP client can get multiple offers from primary subnet and secondary subnets. When this option is not selected, the DHCP discover/request packets from the client are relayed to the DHCP Relay servers sourced only from the primary IP address.
Relay Agent IP(s)	Click <b>Add</b> to add IPv4 addresses. Click <b>Delete</b> to delete a selected address.
<b>Deactivated:</b> Deactivates the DHCP.	

**Note** A warning message is displayed when **DNS proxy** check box is selected in the following scenarios:

- Both IPv4 and IPv6 DHCP Servers are **Deactivated**.
- IPv4 DHCP Server is in **Relay** state and IPv6 DHCP Server is **Deactivated**.

9 Click **Done**. On the **Device** settings screen, click **Save Changes** to save the settings.

The VLAN is configured for the Profile. You can edit the VLAN settings by clicking the link under the **VLAN** column.

To configure VLANs for Edges, see [Configure VLAN for Edges](#).

## Configure Management IP Address for Profiles

The Management IP address is used as the source address for local services (for example, DNS) and as a destination for diagnostic tests (for example, pinging from another Edge). The Management IP is deprecated and is replaced with Loopback Interfaces.

You can configure loopback interfaces only for SD-WAN Edges that are running on version 4.3 and above. The **Configure Loopback Interfaces** area is not available for SD-WAN Edges that are running on version 4.2 or lower. For such Edges, you must configure Management IP address at the Profile level.



The Loopback Interface configurations can be done only at the Edge level. For more information about Loopback Interfaces and limitations, see [Loopback Interfaces Configuration](#).

## Configure Address Resolution Protocol Timeouts for Profiles

VMware SASE Orchestrator supports Address Resolution Protocol (ARP) timeout configuration to allow the user to override the default timeout values of the ARP table entries. VMware SASE Orchestrator allows configuration of three types of timeouts: Stale, Dead, and Cleanup. The default values for the various ARP timeouts are Stale: 2 minutes, Dead: 25 minutes, and Cleanup: 4 hours.

To override the default ARP timeouts at the Profile-level, perform the following steps:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.  
The **Configuration Profiles** page appears.
- 2 Click the link to a Profile for which you want to override ARP timeouts or click the **View** link in the **Device** column of the Profile.  
The **Device** tab displays the configuration options for the selected Profile.
- 3 Under the **Connectivity** category, click **ARP Timeouts**.

- 4 To override the default ARP timeouts, select the **Override default ARP Timeouts** check box.

The screenshot shows the VMware SD-WAN Administration interface. In the top navigation bar, 'Profiles / Quick Start Profile' is selected. Below it, 'Segment: GLOBAL SEGMENT' is chosen. The main content area is titled 'Connectivity' and includes sections for 'VLAN', 'Management IP', and 'ARP Timeouts'. Under 'ARP Timeouts', the 'Override default ARP Timeouts' checkbox is checked. A note below the table states: 'ARP Stale Timeout must be less than ARP Dead Timeout. ARP Dead Timeout must be less than ARP Cleanup Timeout.' The table for ARP Timeouts has three rows: ARP Stale Timeout (Hours: 0, Minutes: 2), ARP Dead Timeout (Hours: 0, Minutes: 25), and ARP Cleanup Timeout (Hours: 3, Minutes: 30).

	Hours	Minutes
ARP Stale Timeout:	0	2
ARP Dead Timeout:	0	25
ARP Cleanup Timeout:	3	30

- 5 Configure the various ARP timeouts in hours and minutes as follows:

---

**Note** ARP Stale Timeout must be less than ARP Dead Timeout. ARP Dead Timeout must be less than ARP Cleanup Timeout.

---

Field	Description
ARP Stale Timeout	<p>When an ARP's age exceeds the Stale time, its state changes from ALIVE to REFRESH. At the REFRESH state, when a new packet tries to use this ARP entry, the packet will be forwarded and also a new ARP request will be sent. If the ARP gets resolved, the ARP entry will be moved to the ALIVE state. Otherwise the entry will remain in the REFRESH state and the traffic will be forwarded in this state.</p> <p>The allowable value ranges from 1 minute to 23 hours and 58 minutes.</p>
ARP Dead Timeout	<p>When an ARP's age exceeds the Dead time, its state changes from REFRESH to DEAD. At the DEAD state, when a new packet tries to use this ARP entry, the packet will be dropped and also an ARP request will be sent. If the ARP gets resolved, the ARP entry will be moved to ALIVE state and the next data packet will be forwarded. If the ARP is not resolved, the ARP entry will remain in the DEAD state. In the DEAD state, traffic will not be forwarded to that port and will be lost.</p> <p>The allowable value ranges from 2 minutes to 23 hours and 59 minutes.</p>
ARP Cleanup Timeout	<p>When an ARP's age exceeds the Cleanup time, the entry will be completely removed from ARP table.</p> <p>The allowable value ranges from 3 minutes to 24 hours.</p>

**Note** The ARP timeout values can only be in increasing order of minutes.

## 6 Click **Save Changes**.

### What to do next

At the Edge-level, you can override the inherited ARP Timeouts for specific edges. For more information, see [Configure Address Resolution Protocol Timeouts for Edges](#).

## Configure Interface Settings

This section explains how to configure the Interface Settings for one or more Edge models in a Profile.

When you configure the Interface Settings for a Profile, the settings are automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge. See [Configure Interface Settings for Edges](#).

Depending on the Edge Model, each interface can be a Switch Port (LAN) interface or a Routed (WAN) Interface. Depending on the Branch Model, a connection port is a dedicated LAN or WAN port, or ports can be configured to be either a LAN or WAN port. Branch ports can be Ethernet or SFP ports. Some Edge models may also support wireless LAN interfaces.

It is assumed that a single public WAN link is attached to a single interface that only serves WAN traffic. If no WAN link is configured for a routed interface that is WAN capable, it is assumed that a single public WAN link should be automatically discovered. If one is discovered, it will be reported to the SASE Orchestrator. This auto-discovered WAN link can then be modified via the SASE Orchestrator and the new configuration pushed back to the branch.

---

### **Note**

- If the routed Interface is activated with the WAN overlay and attached with a WAN link, then the interface will be available for all Segments.
  - If an interface is configured as PPPoE, it will only support a single auto-discovered WAN link. Additional links cannot be assigned to the interface.
- 

If the link should not or cannot be auto-discovered, it must be explicitly configured. There are multiple supported configurations in which auto-discovery will not be possible, including:

- Private WAN links
- Multiple WAN links on a single interface. Example: A Datacenter Hub with 2 MPLS connections
- A single WAN link reachable over multiple interfaces. Example: for an active-active HA topology

Links that are auto-discovered are always public links. User-defined links can be public or private, and will have different configuration options based on which type is selected.

---

**Note** Even for auto-discovered links, overriding the parameters that are automatically detected – such as service provider and bandwidth – can be overridden by the Edge configuration.

---

## **Public WAN Links**

Public WAN links are any traditional link providing access to the public internet such as Cable, DSL, etc. No peer configuration is required for public WAN links. They will automatically connect to the SD-WAN Gateway, which will handle the dissemination of information needed for peer connectivity.

## **Private (MPLS) WAN Links**

Private WAN links belong to a private network and can only connect to other WAN links within the same private network. Because there can be multiple MPLS networks, within a single enterprise, for example, the user must identify which links belong to which network. The SD-WAN Gateway will use this information to distribute connectivity information for the WAN links.

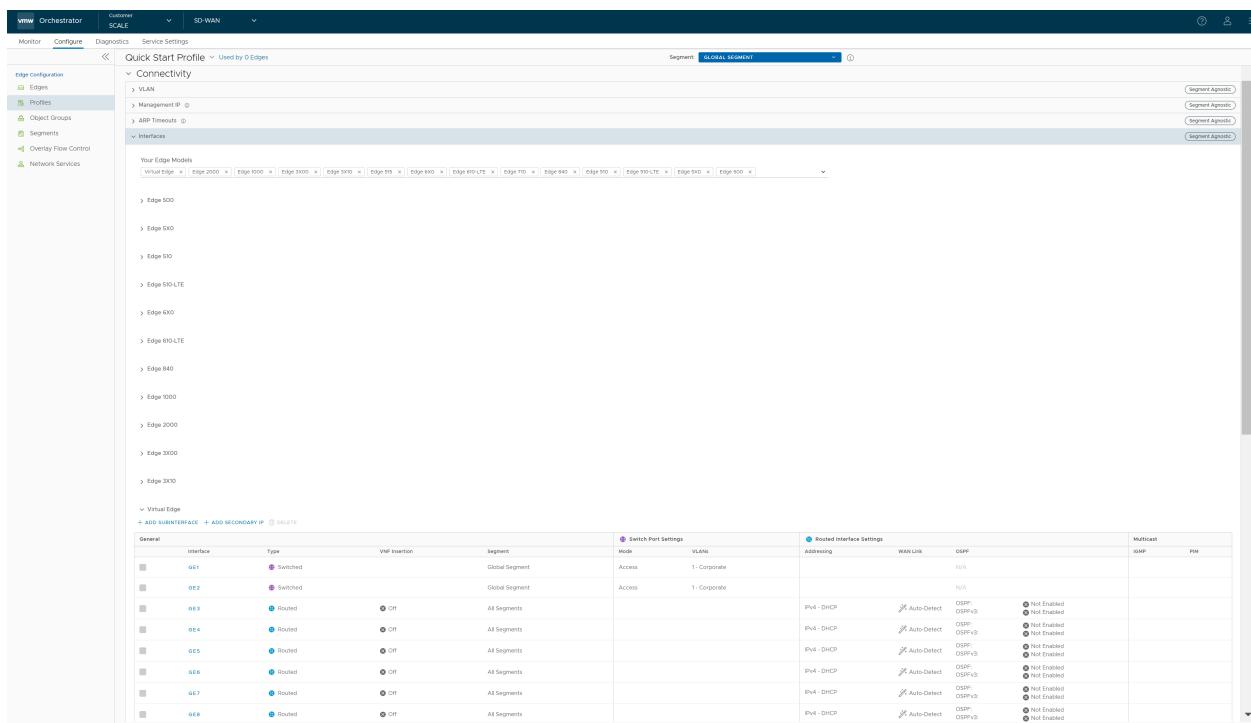
You may choose to treat MPLS links as a single link. However, to differentiate between different MPLS classes of service, multiple WAN links can be defined that map to different MPLS classes of service by assigning each WAN link a different DSCP tag.

Additionally, you may decide to define a static SLA for a private WAN link. This will eliminate the need for peers to exchange path statistics and reduce the bandwidth consumption on a link. Since probe interval influences how quickly the device can fail over, it's not clear whether a static SLA definition should reduce the probe interval automatically.

## Device Settings

You can configure the interface settings for one or more Edge models in a Profile by navigating to the **Configure > Profiles/Edges > Connectivity > Interfaces**. The following screen illustrates the various Edge models and the Interface Settings that can be configured for the supported SD-WAN Edge devices from the **Device** Settings page of the selected Profile.

Click an Edge model to view the Interfaces available in the Edge.



The following table describes the various interface settings configurable for the selected Edge model:

Your Edge Models	Select the Edge model for which you want to configure Interface settings from the drop-down menu. The selected Edge models appears in the <b>Interfaces</b> section. Click and expand the Edge model to configure the interface settings.
General	<ul style="list-style-type: none"><li>■ <b>Interface</b> - The name of the interface. This name matches the Edge port label on the Edge device or is predetermined for wireless LANs. You can click the Interface name link to modify the Interface and Layer 2 (L2) settings. For more details, see <a href="#">Configure Interface Settings for Profiles</a>.</li><li>■ <b>Type</b> - The type of interface. Either Switched or Routed.</li><li>■ <b>VNF Insertion</b> - Displays if the VNF insertion is turned on or OFF for the interface.</li><li>■ <b>Segments</b> - Displays the Segment for which the configuration settings are applicable.</li></ul>

Switch Port Settings	The list of Switch Ports with a summary of some of their settings (such as Access or Trunk mode and the VLANs for the interface). Switch Ports are highlighted with a light, yellow background.
Routed Interface Settings	The list of Routed Interfaces with a summary of their settings (such as the addressing type and if the interface was auto-detected or has an Auto Detected or User Defined WAN overlay). Routed Interfaces are highlighted with a light, blue background.
Multicast	The Multicast settings configured for the interfaces in the Profile. The following are supported Multicast settings: <ul style="list-style-type: none"><li>■ <b>IGMP</b> - Only Internet Group Management Protocol IGMP v2 is supported.</li><li>■ <b>PIM</b> – Only Protocol Independent Multicast Sparse Mode (PIM-SM) is supported.</li></ul>
Add Wi-Fi SSID	The list of Wireless Interfaces (if available on the Edge device). You can add additional wireless networks by clicking the <b>Add Wi-Fi SSID</b> button.
Add SubInterface	You can add sub interfaces by clicking the <b>Add SubInterface</b> button. Sub interfaces are displayed with "SIF" next to the interface. Sub interface for PPPoE interfaces is not supported.
Add Secondary IP	You can add secondary IPs by clicking the <b>Add Secondary IP</b> button. Secondary IPs are displayed with 'SIP' next to the interface.

## Edges Without WiFi Modules

VMware supports Edge models 510, 610, 620, 640, and 680 without WiFi modules for the following releases: 3.4.6, 4.2.2, 4.3.0, 4.3.1, 4.5.0 or newer. For specific model names, see the "*Model Names: Edges Without WiFi Modules*" table below the image. The Edge 6X0 series device and 510 Edge device are shipped with default images, but the working image is typically downloaded from the SASE Orchestrator upon activation.

General				Switch Port Settings		Routed Interface Settings			Multicast	
Interface	Type	VNF Insertion	Segment	Mode	VLANs	Addressing	WAN Link	OSPF	IGMP	PIM
GE1	Switched		Global Segment	Access	1 - Corporate			N/A		
GE2	Switched		Global Segment	Access	1 - Corporate			N/A		
GE3	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: Not Enabled OSPFv3: Not Enabled		
GE3: 10 : SIF	Routed	Off	Global Segment			IPv4 - DHCP	N/A	OSPF: Not Enabled OSPFv3: Not Enabled		
GE4	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: Not Enabled OSPFv3: Not Enabled		
GE5	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: Not Enabled OSPFv3: Not Enabled		
GE5: 12 : SIP	Routed	Off	Global Segment			IPv4 - Static	N/A	N/A		
GE6	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: Not Enabled OSPFv3: Not Enabled		
SFP1	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: Not Enabled OSPFv3: Not Enabled		
SFP2	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: Not Enabled OSPFv3: Not Enabled		
WLAN1	Switched									
WLAN2	Switched									

**Table 20-1. Model Names: Edges Without WiFi Modules**

Marketing Name	Hardware Model	Hardware Part Number
Edge 510N	Edge 510	Edge 510-NW
Edge 610N	E42W	Edge 610N
Edge 620N	E42W	Edge 620N
Edge 640N	E42W	Edge 640N
Edge 680N	E42W	Edge 680N

## Edge 710

The Edge 710 is different from all the previous WiFi models, as it has two separate radios for bands 2.4GHz and 5GHz. Dual-radio models independently use both 2.4 and 5GHz bands. However, if the 5GHz band is selected in an unsupported country, it is deactivated, and the 2.4GHz band is activated by default.

The following screen displays the interfaces for Edge 710 Wi-Fi:

General					Switch Port Settings		Routed Interface Settings			Multicast	
Interface	Interface Override	Type	VNF Insertion	Segment	Mode	VLANs	Addressing	WAN Link	OSPF	IGMP	PIM
GE1	No	Switched		Global Segment	Access	1-Corporate			N/A		
GE2	No	Switched		Global Segment	Access	1-Corporate			N/A		
GE3	No	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
GE4	No	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
SFP1	No	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
WLAN1		Switched									
WLAN2		Switched									

## Edge 710 Troubleshooting

- If the desired outcome is 5GHz Wi-Fi, but the Edge is operating in 2.4GHz:

Check the device-level location settings:

- The location country must be a country that allows 5GHz.
- The country name must be a proper ISO 3166-1 2-character country code.

- Ensure that the desired IEEE 802.11 standards (802.11n, 802.11ac, 802.11ax, etc.), are explicitly set at the device-level.

## Edge 610-LTE

The Edge 610-LTE is an extension of the Edge 610 with an integrated CAT12 EM75xx Sierra Wireless (SWI) modem. The 610-LTE device supports all the features that the 510-LTE offers, with an additional power of an CAT12 module and with a wide range of bands covering various geographical locations. The 610-LTE Edge device has two physical SIM slots. The top slot represents SIM1 and is mapped to the WAN routed interface CELL1. The bottom slot represents SIM2 and is mapped to the WAN routed interface CELL2.

---

**Note** Only one SIM will be active on the 610-LTE Edge even if both SIMs are inserted in the Edge.

---

With the Edge 610-LTE device, new routed interfaces (CELL1 and CELL 2) are configurable. For more information, see [Configure Interface Settings for Profiles](#).

General				Switch Port Settings		Routed Interface Settings			Multicast	
Interface	Type	VNF Insertion	Segment	Mode	VLANs	Addressing	WAN Link	OSPF	IGMP	PIM
GE1	Switched		Global Segment	Access	1 - Corporate			N/A		
GE2	Switched		Global Segment	Access	1 - Corporate			N/A		
GE3	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
GE4	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
GE5	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
GE6	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
SFP1	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
SFP2	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
CELL1	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
CELL2	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3:	Not Enabled Not Enabled	
WLAN1	Switched									
WLAN2	Switched									

## Edge 610-LTE Troubleshooting

- **610-LTE Modem Information Diagnostic Test:** For the 4.2.0 release, if the Edge 610-LTE device is configured, the “LTE Modem Information” diagnostic test will be available. The LTE Modern Information diagnostic test will retrieve diagnostic information, such as signal strength, connection information, etc. For information on how to run a diagnostic test, see "VMware SD-WAN Troubleshooting Guide" published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.
- If two 610-LTE SIM cards are inserted, CELL1(top slot/SIM1) will be activated by default.

- To use CELL2 (bottom slot/SIM2) do either of the following:
  - Reboot the 610-LTE Edge with the SIM2 only.
  - Perform the SIM switch from the SASE Orchestrator with both SIMs inserted.
- Hot swapping SIM cards is not supported; a reboot is required.
- If you want to remove a SIM slot, the SIM must be fully removed from the SIM cage. If some part of the SIM is still inserted in the SIM cage, the SASE Orchestrator will display the CELL instance, but the CELL Interface will not be functional. The following image shows the CELL1(SIM1 slot), where SIM1 is not fully inserted or removed.



## Edge 3810

Edge 3810 is an evolution of the Edge 3800 platform, which includes 6 GE ports and 8 SFP ports. Otherwise, the functionality is identical to the Edge 3800.

## Edge 6X0

Edge models supported are 610, 620, 640, and 680 devices.

---

**Note** For information on how to Configure DSL Settings, see [Configure DSL Settings](#).

---

## Edge 510-LTE

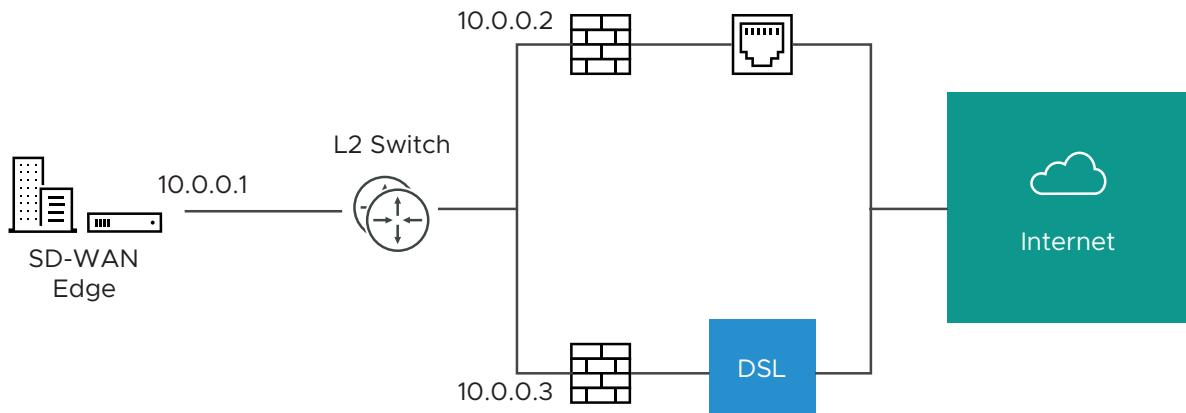
For the Edge 510-LTE model, a new routed interface (CELL1) is displayed in the **Interface Settings**. To edit the Cell Settings, see [Configure Interface Settings for Profiles](#).

**Note 510-LTE Modern Information Diagnostic Test:** When Edge 510- LTE device is configured, the **LTE Modem Information** diagnostic test is available. The LTE Modern Information diagnostic test will retrieve diagnostic information, such as signal strength, connection information, etc. For more information, see "*VMware SD-WAN Troubleshooting Guide*" published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

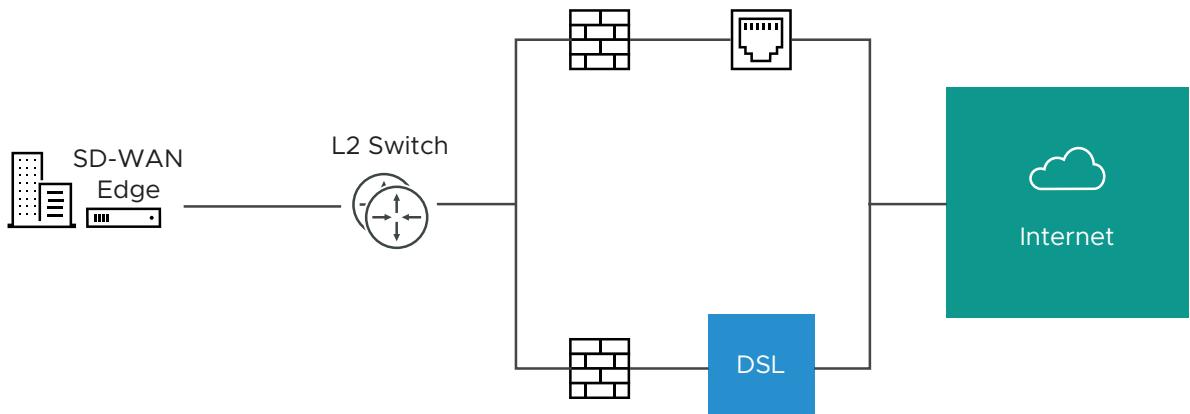
## User-defined WAN Overlay Use Cases

The scenarios wherein this configuration is useful are outlined first, followed by a specification of the configuration itself.

- 1 **Use Case 1: Two WAN links connected to an L2 Switch** – Consider the traditional data center topology where the SD-WAN Edge is connected to an L2 switch in the DMZ that is connected to multiple firewalls, each connected to a different upstream WAN link.



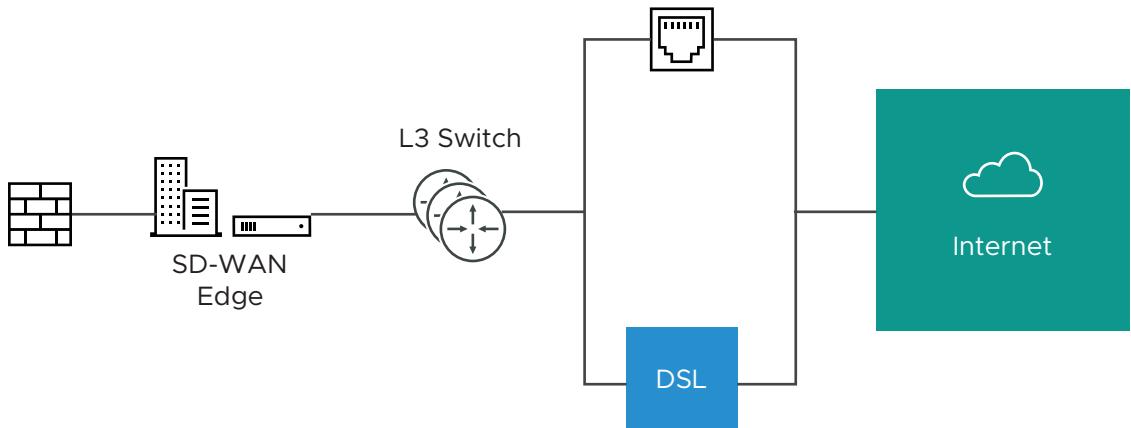
In this topology, the VMware interface has likely been configured with FW1 as the next hop. However, in order to use the DSL link, it must be provisioned with an alternate next hop to which packets should be forwarded, because FW1 cannot reach the DSL. When defining the DSL link, the user must configure a custom next hop IP address as the IP address of FW2 to ensure that packets can reach the DSL modem. Additionally, the user must configure a custom source IP address for this WAN link to allow the edge to identify return interfaces. The final configuration becomes similar to the following figure:



The following paragraph describes how the final configuration is defined.

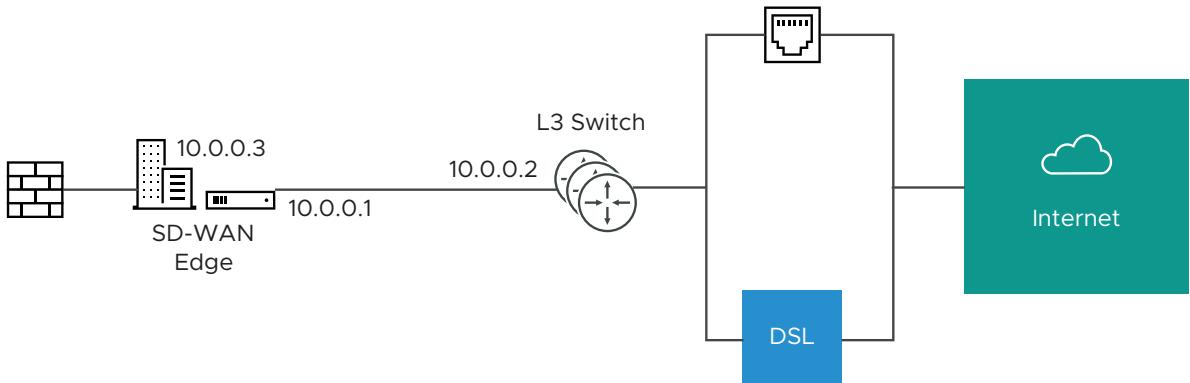
- The interface is defined with IP address 10.0.0.1 and next hop 10.0.0.2. Because more than one WAN link is attached to the interface, the links are set to “user defined.”
- The Cable link is defined and inherits the IP address of 10.0.0.1 and next hop of 10.0.0.2. No changes are required. When a packet needs to be sent out the cable link, it is sourced from 10.0.0.1 and forwarded to the device that responds to ARP for 10.0.0.2 (FW1). Return packets are destined for 10.0.0.1 and identified as having arrived on the cable link.
- The DSL link is defined, and because it is the second WAN link, the SASE Orchestrator flags the IP address and next hop as mandatory configuration items. The user specifies a custom virtual IP (e.g. 10.0.0.4) for the source IP and 10.0.0.3 for the next hop. When a packet needs to be sent out the DSL link, it is sourced from 10.0.0.4 and forwarded to the device that responds to the ARP for 10.0.0.3 (FW2). Return packets are destined for 10.0.0.4 and identified as having arrived on the DSL link.

- 2 **Case 2: Two WAN links connected to an L3 switch/router:** Alternatively, the upstream device may be an L3 switch or a router. In this case, the next hop device is the same (the switch) for both WAN links, rather than different (the firewalls) in the previous example. Often this is leveraged when the firewall sits on the LAN side of the SD-WAN Edge.



In this topology, policy-based routing will be used to steer packets to the appropriate WAN link. This steering may be performed by the IP address or by the VLAN tag, so we support both options.

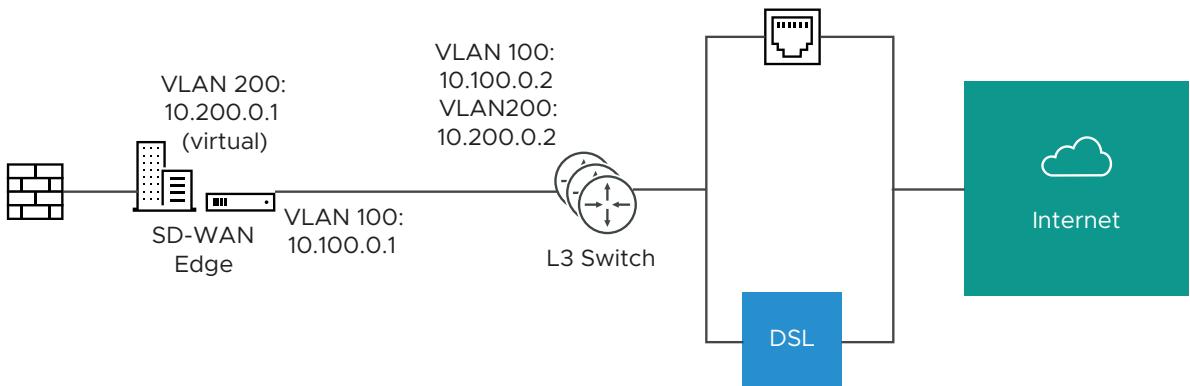
**Steering by IP:** If the L3 device is capable of policy-based routing by source IP address, then both devices may reside on the same VLAN. In this case, the only configuration required is a custom source IP to differentiate the devices.



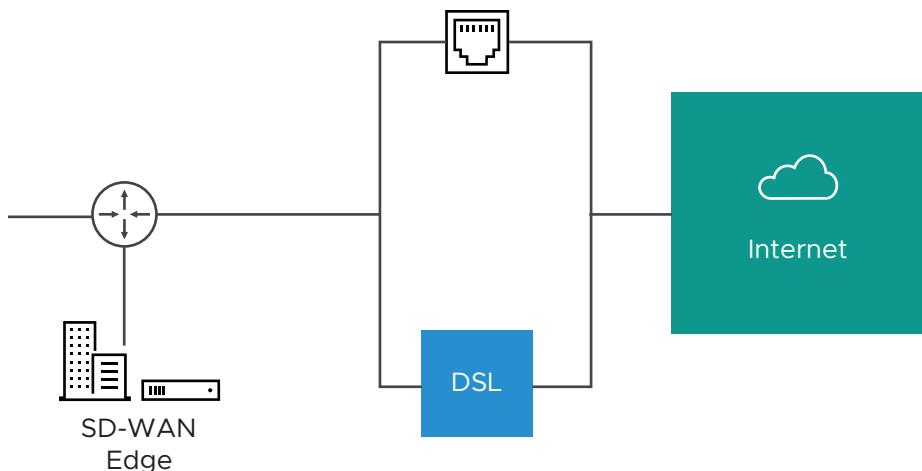
The following paragraph describes how the final configuration is defined.

- The interface is defined with IP address 10.0.0.1 and next hop 10.0.0.2. Because more than one WAN link is attached to the interface, the links are set to “user defined.”
- The Cable link is defined and inherits the IP address of 10.0.0.1 and next hop of 10.0.0.2. No changes are required. When a packet needs to be sent out the cable link, it is sourced from 10.0.0.1 and forwarded to the device that responds to ARP for 10.0.0.2 (L3 Switch). Return packets are destined for 10.0.0.1 and identified as having arrived on the cable link.
- The DSL link is defined, and because it is the second WAN link, the SASE Orchestrator flags the IP address and next hop as mandatory configuration items. The user specifies a custom virtual IP (for example, 10.0.0.3) for the source IP and the same 10.0.0.2 for the next hop. When a packet needs to be sent out the DSL link, it is sourced from 10.0.0.3 and forwarded to the device that responds to the ARP for 10.0.0.2 (L3 Switch). Return packets are destined for 10.0.0.3 and identified as having arrived on the DSL link.

**Steering by VLAN:** If the L3 device is not capable of source routing, or if for some other reason the user chooses to assign separate VLANs to the cable and DSL links, this must be configured.

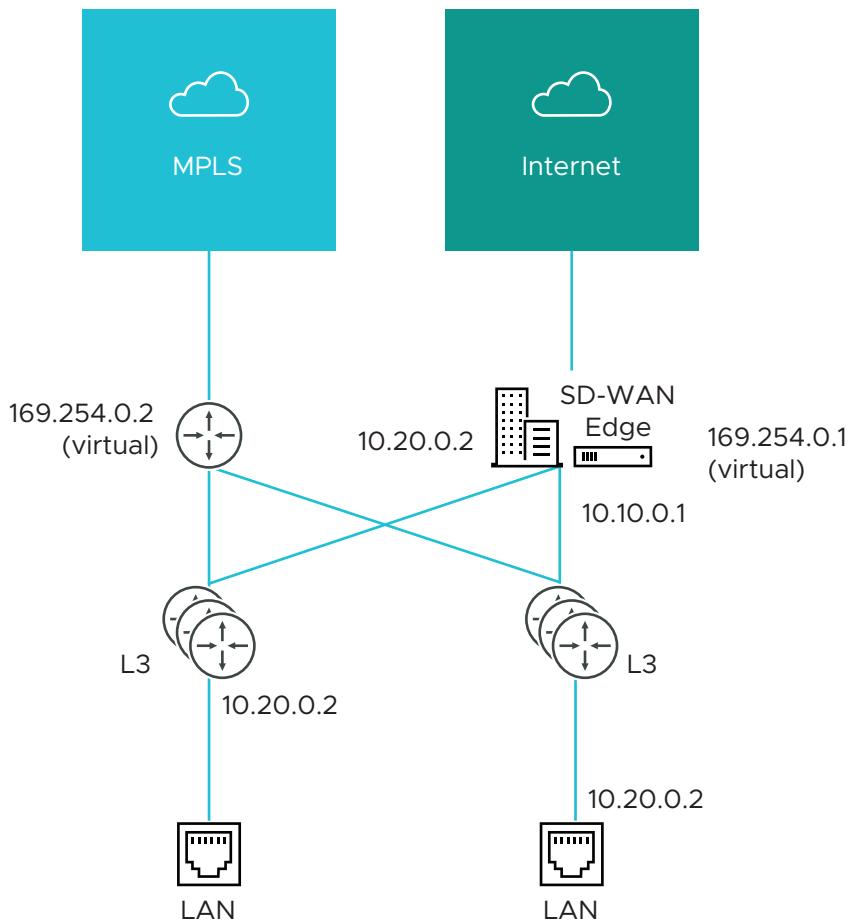


- The interface is defined with IP address 10.100.0.1 and next hop 10.100.0.2 on VLAN 100. Because more than one WAN link is attached to the interface, the links are set to “user defined.”
  - The Cable link is defined and inherits VLAN 100 as well as the IP address of 10.100.0.1 and next hop of 10.100.0.2. No changes are required. When a packet needs to be sent out the cable link, it is sourced from 10.100.0.1, tagged with VLAN 100 and forwarded to the device that responds to ARP for 10.100.0.2 on VLAN 100 (L3 Switch). Return packets are destined for 10.100.0.1/VLAN 100 and identified as having arrived on the cable link.
  - The DSL link is defined, and because it is the second WAN link the SASE Orchestrator flags the IP address and next hop as mandatory configuration items. The user specifies a custom VLAN ID (200) as well as virtual IP (e.g. 10.200.0.1) for the source IP and the 10.200.0.2 for the next hop. When a packet needs to be sent out the DSL link, it is sourced from 10.200.0.1, tagged with VLAN 200 and forwarded to the device that responds to the ARP for 10.200.0.2 on VLAN 200 (L3 Switch). Return packets are destined for 10.200.0.1/VLAN 200 and identified as having arrived on the DSL link.
- 3 **Case 3: One-arm Deployments:** One-arm deployments end up being very similar to other L3 deployments.



Again, the SD-WAN Edge shares the same next hop for both WAN links. Policy-based routing can be done to ensure that traffic is forwarded to the appropriate destination as defined above. Alternately, the source IP and VLAN for the WAN link objects in the VMware may be the same as the VLAN of the cable and DSL links to make the routing automatic.

- 4 **Case 4: One WAN link reachable over multiple interfaces:** Consider the traditional gold site topology where the MPLS is reachable via two alternate paths. In this case, we must define a custom source IP address and next hop that can be shared regardless of which interface is being used to communicate.



- GE1 is defined with IP address 10.10.0.1 and next hop 10.10.0.2
- GE2 is defined with IP address 10.20.0.1 and next hop 10.20.0.2
- The MPLS is defined and set as reachable via either interface. This makes the source IP and next hop IP address mandatory with no defaults.
- The source IP and destination are defined, which can be used for communication irrespective of the interface being used. When a packet needs to be sent out the MPLS

link, it is sourced from 169.254.0.1, tagged with the configured VLAN and forwarded to the device that responds to ARP for 169.254.0.2 on the configured VLAN (CE Router). Return packets are destined for 169.254.0.1 and identified as having arrived on the MPLS link.

**Note** If OSPF or BGP is not activated, you may need to configure a transit VLAN that is the same on both switches to allow reachability of this virtual IP.

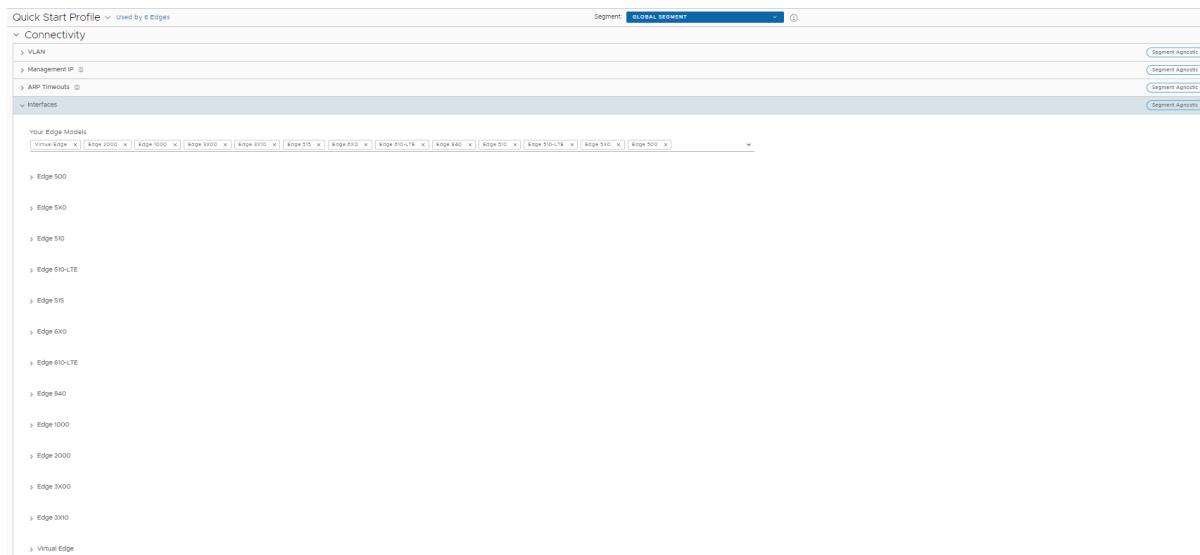
## Configure Interface Settings for Profiles

In a Profile, you can configure Interface settings for various Edge models.

You can configure the Interface settings for each Edge model. Each Interface on an Edge can be a Switch Port (LAN) or a Routed (WAN) Interface. The Interface settings vary based on the Edge model. For more information on different Edge models and deployments, see [Configure Interface Settings](#).

To configure the Interface settings for different Edge models in a Profile:

- 1 In the **SD-WAN** service of the Enterprise portal, go to [Configure > Profiles](#).
- 2 The **Profiles** page displays the existing Profiles.
- 3 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. You can also select a Profile and click **Modify** to configure the Profile.
- 4 The configuration options for the selected Profile are displayed in the **Device** tab.
- 5 In the **Connectivity** category, click **Interfaces**. The Edge models available in the selected Profile are displayed:



- 6 Click an Edge model to view the Interfaces available in the Edge.

You can edit the settings for the following types of Interfaces, based on the Edge model:

- Switch Port

- Routed Interface
- WLAN Interface

You can also add Sub Interface, Secondary IP address, and Wi-Fi SSID based on the Edge model.

General				Switch Port Settings		Routed Interface Settings			Multicast	
Interface	Type	VNF Insertion	Segment	Mode	VLANs	Addressing	WAN Overlay	OSPF	IGMP	PIM
LAN1	Switched		Global Segment	Access	1 - Corporate			N/A		
LAN2	Switched		Global Segment	Access	1 - Corporate			N/A		
LAN3	Switched		Global Segment	Access	1 - Corporate			N/A		
LAN4	Switched		Global Segment	Access	1 - Corporate			N/A		
INTERNET1	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	Off		
INTERNET2	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	Off		
INTERNET3	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	Off		
WLAN1	Switched		Global Segment	Wi-Fi	1 - Corporate			N/A		
WLAN2	Switched									

- 7 Configure the settings for a **Routed** Interface. See the table below for a description of these configuration settings.

---

**Note** The Interface settings in the table below can be overwritten at the Edge level.

---

## Edge 500

X

## Interface INTERNET1

▲

## Description

Enter Description (Optional)

Maximum 256 characters

## Interface Enabled

 Enabled

## Capability

Routed

▼

## Segments

All Segments

## Radius Authentication

✖ WAN Overlay must be disabled to configure RADIUS Authentication.

## ICMP Echo Response

 EnabledUnderlay Accounting  ⓘ Enabled

## Enable WAN Overlay

 Enabled

## DNS Proxy

 Enabled

## VLAN

## IPv4 Settings

 Enabled

## Addressing Type

DHCP

▼

IP Address N/A

Cidr Prefix N/A

Gateway: N/A

## WAN Overlay

Auto-Detect

▼

## OSPF

✖ OSPF not enabled for the selected Segment

## Multicast

✖ Multicast is not enabled for the selected segment

## Advertise

 Enabled

## NAT Direct Traffic

 EnabledTrusted Source  ⓘ Enabled

## Reverse Path Forwarding

Specific

▼

Reverse Path Forwarding options are only settable when trusted zone is checked. When trusted zone is un-checked, the value will default to Specific.

 Enabled

Option	Description
Description	Type the description. This field is optional.
Interface Enabled	This check box is selected by default. If required, you can deactivate the Interface. When deactivated, the Interface is not available for any communication.
Capability	For a Routed interface, the option <b>Routed</b> is selected by default. You can choose to convert the port to a Switch Port Interface by selecting the option <b>Switched</b> from the drop-down list.
Segments	By default, the configuration settings are applicable to all the segments. This field cannot be edited.
Radius Authentication	Deactivate the <b>Enable WAN Overlay</b> check box to configure <b>Radius Authentication</b> . Select the <b>Radius Authentication</b> check box and add the MAC addresses of pre-authenticated devices.
ICMP Echo Response	This check box is selected by default. This helps the Interface to respond to ICMP echo messages. You can deactivate this option for security purposes.
Underlay Accounting	<p>This check box is selected by default. If a private WAN overlay is defined on the Interface, all underlay traffic traversing the interface are counted against the measured rate of the WAN link to prevent over-subscription. Deactivate this option to avoid this behavior.</p> <p><b>Note</b> Underlay Accounting is supported for both, IPv4 and IPv6 addresses.</p>
Enable WAN Overlay	This check box is selected by default. This helps to activate WAN overlay for the Interface.
DNS Proxy	<p>The DNS Proxy feature provides additional support for Local DNS entries on the Edges associated with the Profile, to point certain device traffic to specific domains. You can activate or deactivate this option, irrespective of IPv4 or IPv6 DHCP Server setting.</p> <p><b>Note</b> This check box is available only for a Routed Interface and a Routed Sub Interface.</p> <p><b>Note</b> If IPv4/IPv6 DHCP Server is activated and DNS Proxy is deactivated then the DNS Proxy feature will not work as expected and may result in DNS resolution failure.</p>
VLAN	For an Access port, select an existing VLAN from the drop-down list. For a Trunk port, you can select multiple VLANs and select an untagged VLAN.
<b>IPv4 Settings</b> – Select the check box to activate IPv4 Settings.	

Option	Description
Addressing Type	<p>By default, <b>DHCP</b> is selected, which assigns an IPv4 address dynamically. If you select <b>Static</b> or <b>PPPoE</b>, you must configure the addressing details for each Edge.</p>
WAN Overlay	<p>By default, <b>Auto-Detect Overlay</b> is activated. You can choose the <b>User Defined Overlay</b> and configure the Overlay settings. For more information, see <a href="#">Configure Edge WAN Overlay Settings</a>.</p> <p><b>Note</b> If you have a CSS GRE tunnel created for an Edge and if you change the WAN Overlay settings of the WAN link associated with the CSS tunnel interface from "Auto-Detect Overlay" to "User-Defined Overlay", the WAN link and the associated CSS tunnels are also removed from the CSS configuration at the Edge level.</p>
OSPF	<p>This option is available only when you have configured OSPF for the Profile. Select the check box and choose an OSPF from the drop-down list. Click <b>toggle advance ospf settings</b> to configure the Interface settings for the selected OSPF.</p> <p><b>Note</b> OSPF is not supported on Sub Interfaces, and it is not supported on non Global Segments.</p> <p>The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6, which is only available in the 5.2 release.</p> <p><b>Note</b> OSFPv3 is only available in the 5.2 release.</p> <p>For more information on OSPF settings and OSPFv3, see <a href="#">Activate OSPF for Profiles</a>.</p>

Option	Description
Multicast	<p>This option is available only when you have configured multicast settings for the Profile. You can configure the following multicast settings for the selected Interface.</p> <ul style="list-style-type: none"> <li>■ <b>IGMP</b> - Select the check box to activate Internet Group Management Protocol (IGMP). Only IGMP v2 is supported.</li> <li>■ <b>PIM</b> - Select the check box to activate Protocol Independent Multicast. Only PIM Sparse Mode (PIM-SM) is supported.</li> </ul> <p>Click <b>toggle advanced multicast settings</b> to configure the following timers:</p> <ul style="list-style-type: none"> <li>■ <b>PIM Hello Timer</b> – The time interval at which a PIM Interface sends out <b>Hello</b> messages to discover PIM neighbors. The range is from 1 to 180 seconds and the default value is 30 seconds.</li> <li>■ <b>IGMP Host Query Interval</b> – The time interval at which the IGMP querier sends out host-query messages to discover the multicast groups with members, on the attached network. The range is from 1 to 1800 seconds and the default value is 125 seconds.</li> <li>■ <b>IGMP Max Query Response Value</b> – The maximum time that the host has to respond to an IGMP query. The range is from 10 to 250 deciseconds and the default value is 100 deciseconds.</li> </ul> <p><b>Note</b> Currently, Multicast Listener Discovery (MLD) is deactivated. Hence, Edge will not send the multicast listener report when IPv6 address is assigned to Interface. If there is a snooping switch in the network then not sending MLD report may result in Edge not receiving multicast packets which are used in Duplicate Address Detection (DAD). This would result in DAD success even with duplicate address.</p>
VNF Insertion	<p>You must deactivate <b>WAN Overlay</b> and select the <b>Trusted Source</b> check box to activate <b>VNF Insertion</b>. When you insert the VNF into Layer 3 interfaces or sub-interfaces, the system redirects traffic from the Layer 3 interfaces or sub interfaces to the VNF.</p>
Advertise	<p>Select the check box to advertise the Interface to other branches in the network.</p>

Option	Description
NAT Direct Traffic	<p>Select the check box to activate NAT Direct traffic for IPv4 on a routed interface.</p> <p><b>Caution</b> It is possible that an older version of the SASE Orchestrator inadvertently configured NAT Direct on a main interface with either a VLAN or subinterface configured. If that interface is sending direct traffic one or hops away, the customer would not observe any issues because the NAT Direct setting was not being applied. However, when an Edge is upgraded to 5.2.0 or later, the Edge build includes a fix for the issue (Ticket #92142) with NAT Direct Traffic not being properly applied, and there is a resulting change in routing behavior since this specific use case was not implemented in prior releases.</p> <p>In other words, because a 5.2.0 or later Edge now implements NAT Direct in the expected manner for all use cases, traffic that previously worked (because NAT Direct was not being applied per the defect) may now fail because the customer never realized that NAT Direct was checked for an interface with a VLAN or subinterface configured.</p> <p>As a result, a customer upgrading their Edge to Release 5.2.0 or later should first check their Profiles and Edge interface settings to ensure NAT Direct is configured only where they explicitly require it and to deactivate this setting where it is not, especially if that interface has a VLAN or subinterface configured.</p>
Trusted Source	Select the check box to set the Interface as a trusted source.

Option	Description
Reverse Path Forwarding	<p>You can choose an option for Reverse Path Forwarding (RPF) only when you have selected the <b>Trusted Source</b> check box. This option allows traffic on the interface only if return traffic can be forwarded on the same interface. This helps to prevent traffic from unknown sources like malicious traffic on an enterprise network. If the incoming source is unknown, then the packet is dropped at ingress without creating flows. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ <b>Not Enabled</b> – Allows incoming traffic even if there is no matching route in the route table.</li> <li>■ <b>Specific</b> – This option is selected by default, even when the <b>Trusted Source</b> option is deactivated. The incoming traffic should match a specific return route on the incoming interface. If a specific match is not found, then the incoming packet is dropped. This is a commonly used mode on interfaces configured with public overlays and NAT.</li> <li>■ <b>Loose</b> – The incoming traffic should match any route (Connected/Static/Routed) in the routing table. This allows asymmetrical routing and is commonly used on interfaces that are configured without next hop.</li> </ul>
<b>IPv6 Settings</b> – Select the check box to activate IPv6 Settings.	
Addressing Type	<p>Choose one of the options from the following to assign an IPv6 address dynamically.</p> <ul style="list-style-type: none"> <li>■ <b>DHCP Stateless</b> – Allows the Interface to self-configure the IPv6 address. It is not necessary to have a DHCPv6 server available at the ISP. An ICMPv6 discover message originates from the Edge and is used for auto-configuration.</li> </ul> <p><b>Note</b> In DHCP Stateless configuration, two IPv6 addresses are created at the Kernel Interface level. The Edge does not use the host address which matches the Link local address.</p> <hr/> <ul style="list-style-type: none"> <li>■ <b>DHCP Stateful</b> – This option is similar to DHCP for IPv4. The Gateway connects to the DHCPv6 server of the ISP for a leased address and the server maintains the status of the IPv6 address.</li> </ul> <p><b>Note</b> In stateful DHCP, when the valid lifetime and preferred lifetime are set with the infinite value (<b>0xffffffff(4294967295)</b>), the timer does not work properly. The maximum value that the valid and preferred timers can hold is <b>2147483647</b>.</p> <hr/> <ul style="list-style-type: none"> <li>■ <b>Static</b> – If you select this option, you should configure the addressing details for each Edge.</li> </ul> <p><b>Note</b> For Cell Interfaces, the Addressing Type would be <b>Static</b> by default.</p>

Option	Description
WAN Overlay	<p>By default, <b>Auto-Detect</b> Overlay is activated. You can choose the <b>User Defined</b> Overlay and configure the Overlay settings. For more information, see <a href="#">Configure Edge WAN Overlay Settings</a>.</p>
OSFP	<p>This option is available only when you have configured OSPF for the Profile. Select the check box and choose an OSPF from the drop-down list. Click <b>toggle advance ospf settings</b> to configure the Interface settings for the selected OSPF.</p>
	<p><b>Note</b> OSPF is not supported on Sub Interfaces, and it is not supported on non Global Segments.</p> <p>The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6.</p> <p><b>Note</b> OSPFv3 is only available in the 5.2 release.</p>
Advertise	<p>Select the check box to advertise the Interface to other branches in network.</p>
NAT Direct Traffic	<p>Select the check box to activate NAT Direct traffic for IPv6 on a routed interface.</p> <p><b>Caution</b> It is possible that an older version of the SASE Orchestrator inadvertently configured NAT Direct on a main interface with either a VLAN or subinterface configured. If that interface is sending direct traffic one or hops away, the customer would not observe any issues because the NAT Direct setting was not being applied. However, when an Edge is upgraded to 5.2.0 or later, the Edge build includes a fix for the issue (Ticket #92142) with NAT Direct Traffic not being properly applied, and there is a resulting change in routing behavior since this specific use case was not implemented in prior releases.</p> <p>In other words, because a 5.2.0 or later Edge now implements NAT Direct in the expected manner for all use cases, traffic that previously worked (because NAT Direct was not being applied per the defect) may now fail because the customer never realized that NAT Direct was checked for an interface with a VLAN or subinterface configured.</p> <p>As a result, a customer upgrading their Edge to Release 5.2.0 or later should first check their Profiles and Edge interface settings to ensure NAT Direct is configured only where they explicitly require it and to deactivate this setting where it is not, especially if that interface has a VLAN or subinterface configured.</p>
Trusted Source	<p>Select the check box to set the Interface as a trusted source.</p>

Option	Description
Reverse Path Forwarding	<p>You can choose an option for Reverse Path Forwarding (RPF) only when you have selected the <b>Trusted Source</b> check box. This option allows traffic on the interface only if return traffic can be forwarded on the same interface. This helps to prevent traffic from unknown sources like malicious traffic on an enterprise network. If the incoming source is unknown, then the packet is dropped at ingress without creating flows. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ <b>Not Enabled</b> – Allows incoming traffic even if there is no matching route in the route table.</li> <li>■ <b>Specific</b> – This option is selected by default, even when the <b>Trusted Source</b> option is deactivated. The incoming traffic should match a specific return route on the incoming interface. If a specific match is not found, then the incoming packet is dropped. This is a commonly used mode on interfaces configured with public overlays and NAT.</li> <li>■ <b>Loose</b> – The incoming traffic should match any route (Connected/Static/Routed) in the routing table. This allows asymmetrical routing and is commonly used on interfaces that are configured without next hop.</li> </ul>

**Router Advertisement Host Settings** - These settings are available only when you select the **IPv6 Settings** check box, and choose the **Addressing Type** as **DHCP Stateless** or **DHCP Stateful**. Select the check box to display the following RA parameters. These parameters are activated by default. If required, you can deactivate them.

**Note** When RA host parameters are deactivated and activated again, then the Edge waits for the next RA to be received before installing routes, MTU, and ND/NS parameters.

MTU	Accepts the MTU value received through Route Advertisement. If you deactivate this option, the MTU configuration of the Interface is considered.
Default Routes	Installs default routes when Route Advertisement is received on the Interface. If you deactivate this option, then there is no default routes available for the Interface.
Specific Routes	Installs specific routes when Route Advertisement receives route information on the Interface. If you deactivate this option, the Interface does not install the route information.
ND6 Timers	Accepts ND6 timers received through Route Advertisement. If you deactivate this option, default ND6 timers are considered. The default value for NDP retransmit timer is 1 second and NDP reachable timeout is 30 seconds.
<b>L2 Settings</b>	

Option	Description
Autonegotiate	This check box is selected by default. This allows the port to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection.
Speed	This option is available only when <b>Autonegotiate</b> is deactivated. Select the speed at which the port communicates with other links. By default, <b>100 Mbps</b> is selected.
Duplex	This option is available only when <b>Autonegotiate</b> is deactivated. Select the mode of the connection as <b>Full duplex</b> or <b>Half duplex</b> . By default, <b>Full duplex</b> is selected.
MTU	The default MTU size for frames received and sent on all routed interfaces is <b>1500</b> bytes. You can change the MTU size for an Interface.

---

**Note** A warning message is displayed when **DNS proxy** check box is selected in the following scenarios:

- Both IPv4 and IPv6 DHCP Servers are **Deactivated**.
- IPv4 DHCP Server is in **Relay** state and IPv6 DHCP Server is **Deactivated**.

If you are using USB Modem to connect to the network, to enable IPv6 addressing, configure the following manually in the Edge:

- a Add the global parameter “`usb_tun_overlay_pref_v6`”:1 to `/etc/config/edged`, to update the preference to IPv6 address.
- b Run the following command to update the IP type of the Interface to IPv6.

```
/etc/modems/modem_apn.sh [USB] [ACTION] [ACTION ARGS...]
```

Enter the parameters as follows:

- *USB* – Enter the USB Number
- Enter the APN settings as follows:
  - *apn* – Enter the Access Point Name.
  - *username* – Enter the username provided by the carrier.
  - *password* – Enter the password provided by the carrier.
  - *spnetwork* – Enter the name of the Service Provider Network.
  - *simpin* – Enter the PIN number used to unlock the SIM card.
  - *auth* – Specify the Authentication type.
  - *iptype* – Enter the type of IP address.

The following is an example command with sample parameters:

```
/etc/modems/modem_apn.sh USB3 set "vzwinternet" "VERIZON" "ipv4v6"
```

---

**Note** For a list of modems supported for use on a SD-WAN Edge, see the [Supported Modems](#) page.

- 
- 8 Configure the settings for a **Switched** Interface. See the table below for a description of these configuration settings.

Edge 510 X

Interface GE1

Interface Enabled	<input checked="" type="checkbox"/> Enabled
Capability	Switched
Mode	Access Port
VLANs	1 - Corporate

L2 Settings

Autonegotiate	<input checked="" type="checkbox"/> Enabled
MTU	1500

CANCEL
SAVE

Option	Description
Interface Enabled	This option is activated by default. If required, you can deactivate the Interface. When deactivated, the Interface is not available for any communication.
Capability	For a Switch Port, the option <b>Switched</b> is selected by default. You can choose to convert the port to a routed Interface by selecting the option <b>Routed</b> from the drop-down list.
Mode	Select the mode of the port as Access or Trunk port.
VLANs	For an Access port, select an existing VLAN from the drop-down list. For a Trunk port, you can select multiple VLANs and select an untagged VLAN.
<b>L2 Settings</b>	
Autonegotiate	This option is activated by default. When activated, Auto negotiation allows the port to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection.

Option	Description
Speed	This option is available only when <b>Autonegotiate</b> is deactivated. Select the speed that the port has to communicate with other links. By default, 100 Mbps is selected.
Duplex	This option is available only when <b>Autonegotiate</b> is deactivated. Select the mode of the connection as Full duplex or Half duplex. By default, Full duplex is selected.
MTU	The default MTU size for frames received and sent on all switch interfaces is 1500 bytes. You can change the MTU size for an Interface.

- 9 You can also add a Sub Interface, Secondary IP address, and Wi-Fi SSID based on the Edge model. Click **Delete** to remove a selected interface.
- To add Sub Interfaces to an existing Interface:
    - In the **Interface** section, click **Add SubInterface**.
    - In the **Select Interface** window, select the Interface for which you want to add a Sub Interface.
    - Enter the **Subinterface ID** and click **Next**.
    - In the **Sub Interface** window, configure the Interface settings.
  - To add Secondary IP addresses to an existing Interface:
    - In the **Interface** section, click **Add Secondary IP**.
    - In the **Select Interface** window, select the Interface for which you want to add a secondary IP address.
    - Enter the **Subinterface ID** and click **Next**.
    - In the **Secondary IP** window, configure the Interface settings.
  - Some of the Edge models support Wireless LAN. To add Wi-Fi SSID to an existing Interface:
    - In the **Interface** section, click **Add Wi-Fi SSID**. The WLAN Interface settings window appears.

Edge 500 X

WLAN1

Interface Enabled	<input checked="" type="checkbox"/> Enabled
VLAN	1 - Corporate
SSID	vc-wifi
	<input checked="" type="checkbox"/> Broadcast
Security	WPA2/Personal
Password	..... <span style="font-size: small;">(Show)</span>
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; font-weight: bold;">SAVE</span>	

- Configure the following WLAN Interface settings:

Option	Description
Interface Enabled	This option is enabled by default. If required, you can deactivate the Interface. When deactivated, the Interface is not available for any communication.
VLAN	Choose the VLAN to be used by the Interface.

Option	Description
SSID	<p>Enter the wireless network name.</p> <p>Select the <b>Broadcast</b> check box to broadcast the SSID name to the surrounding devices.</p>
Security	<p>Select the type of security for the Wi-Fi connection, from the drop-down list. The following options are available:</p> <ul style="list-style-type: none"> <li>■ <b>Open</b> – No security is enforced.</li> <li>■ <b>WPA2 / Personal</b> – A password is required for authentication. Enter the password in the <b>Passphrase</b> field.</li> </ul> <p><b>Note</b> Starting from the 4.5 release, the use of the special character "&lt;" in the password is no longer supported. In cases where users have already used "&lt;" in their passwords in previous releases, they must remove it to save any changes on the page.</p> <ul style="list-style-type: none"> <li>■ <b>WPA2 / Enterprise</b> – A RADIUS server is used for authentication. You should have already configured a RADIUS server and selected it for the Profile and Edge.</li> </ul> <p>To configure a RADIUS server, see <a href="#">Configure Authentication Services</a>.</p> <p>To select the RADIUS server for a Profile, see <a href="#">Configure Authentication Settings for Profiles</a>.</p>

#### 10 Click **Save Changes** in the **Device** window.

When you configure the Interface Settings for a Profile, the settings are automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge. See [Configure Interface Settings for Edges](#).

## Configure DSL Settings

Support is available for xDSL SFP module. It is a highly integrated SFP bridged modem, which provides a pluggable SFP compliant interface to upgrade existing DSL IAD or home Gateway devices to higher bandwidth services.

Configuring DSL includes options for configuring ADSL and VDSL Settings. See [Configure ADSL and VDSL Settings](#) for more information.

### Troubleshooting DSL Settings

**DSL Status Diagnostic Test:** The DSL diagnostic test is available only for 610 devices. In the 4.3 release, testing is also available for the 620, 640, and 680 devices. Running this test will show the DSL status, which includes information such as Mode (Standard or DSL), Profile, xDSL Mode, etc. as shown in the image below.

The screenshot shows the 'DSL Status' interface. At the top right is a 'RUN' button. Below it is a message: 'View the xDSL(ADSL2/VDSL2) modem status connected to SFP interfaces'. A note at the bottom right says 'Test Duration: 3.006 seconds'. The main area is titled 'Interfaces' and contains a table with two rows:

Name	Mode	Vendor MAC	xDSL Mode	Link Time	Status	Link Rate	Annex	Profile	TxPkts/RxPkts
SFP1	DSL	00:0E:AD:00:70:06	VDSL2	3711362	Showtime	5504-40192	AnnexB	17a	104520796138633836
SFP2	Standard	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

## Configure ADSL and VDSL Settings

The xDSL SFP module can be plugged into either the SD-WAN Edge 610 or the SD-WAN Edge 610-LTE device SFP slot and used in ADSL2+/VDSL2 mode. This module must be procured by the user.

**Note** Configuring DSL is only available for the 610, 610-LTE, 620, 640, and 680 devices.

## Configuring SFP

You can configure the SFP interfaces only for the SD-WAN Edge 610 or the SD-WAN Edge 610-LTE device by navigating to the **Configure > Profiles/Edges > Device > Connectivity > Interfaces** page in the **SD-WAN** service of the Enterprise portal.

Click the SFP interface that the specific DSL module is plugged into. When the SFP is plugged in, the slot name is displayed as **SFP1** and **SFP2** under the **Interface** column as shown in the following screenshot.

Edge 6X0										Multicast	
General				Switch Port Settings			Routed Interface Settings			Multicast	
Interface	Type	VNF Insertion	Segment	Mode	VLANs	Addressing	WAN Link	OSPF	IGMP	PIM	
GE1	Switched		Global Segment	Access	1 - Corporate			N/A			
GE2	Switched		Global Segment	Access	1 - Corporate			N/A			
GE3	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3: Not Enabled Not Enabled			
GE4	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3: Not Enabled Not Enabled			
GE5	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3: Not Enabled Not Enabled			
GE6	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3: Not Enabled Not Enabled			
SFP1	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3: Not Enabled Not Enabled			
SFP2	Routed	Off	All Segments			IPv4 - DHCP	Auto-Detect	OSPF: OSPFv3: Not Enabled Not Enabled			
WLAN1	Switched										
WLAN2	Switched										

## To Configure SFP at the Profile level:

- In the **SD-WAN** service of the Enterprise portal, navigate to the **Configure > Profiles > Device > Connectivity > Interfaces** page.
- Click and expand an Edge model (for example SD-WAN Edge 610) for which you want to configure the SFP DSL interface settings.
- Under the **Interface** column, click the SFP interface link (for example SFP1) that you want to configure.

The **Interface SFP1** dialog for the selected SD-WAN Edge device is displayed.

---

**Note** The following steps describe only the SFP configuration. For a description of the other fields in the selected SD-WAN Edge device, see section [Configure Interface Settings for Profiles](#).

---

- 4 To configure DSL settings in the **Interface SFP1** dialog, scroll down to the **SFP Settings** area.

## Edge 6X0

X

## Interface SFP1

▲

**Description**

Enter Description (Optional)



Maximum 256 characters

**Interface Enabled** Enabled**Capability**

Routed

**Segments**

All Segments

**Radius Authentication**

✖ WAN Link must be disabled to configure RADIUS Authentication.

**ICMP Echo Response** Enabled**Underlay Accounting** ⓘ Enabled**Enable WAN Link** Enabled**DNS Proxy** Enabled**VLAN**

---

**EVDSL Modem Attached** Enabled

## Edge 6X0

X

**NAT Direct Traffic** Enabled**Trusted Source** ⓘ Enabled**Reverse Path Forwarding**

Specific



Reverse Path Forwarding options are only settable when trusted zone is checked. When trusted zone is un-checked, the value will default to Specific.

**IPv6 Settings** Enabled**Addressing Type**

DHCP Stateless



IP Address	N/A
Cidr Prefix	N/A
Gateway:	N/A

**VNF Insertion**

✖ VNF insertion is disallowed when an interface is configured for WAN links

 Enabled Enabled

- 5 From the **SFP Module** drop-down menu, choose **DSL**.

The screenshot shows the configuration interface for an Edge 6X0 device. At the top, there's a header "Edge 6X0" and a close button "X". Below the header, there are two sections: "Autonegotiate" (checkbox checked, "Enabled") and "MTU" (set to 1500). A large red box highlights the "SFP Settings" section. This section contains a dropdown for "SFP Module" set to "DSL". Underneath, the "DSL Settings" section is expanded, containing fields for "Mode" (ADSL2/2+), "PVC" (0), "VPI" (0), "VCI" (35), "PVC VLAN" (1), "VLAN TX" (1), "VLAN RX" (1), "VLAN TX OP" (2), and "VLAN RX OP" (2). At the bottom right are "CANCEL" and "SAVE" buttons.

- 6 In the **DSL Settings** area, configure the following:

Option	Description
SFP Module	Three SFP modules are available: <b>Standard</b> , <b>GPON</b> , and <b>DSL</b> . By default, Standard is selected. You can select DSL as the module to use the SFP port with higher bandwidth services.
DSL Settings	The option to configure Digital Subscriber Line (DSL) settings is available when you select the SFP module as DSL.

Option	Description
DSL Mode: VDSL2	<p>This option is selected by default. Very-high-bit-rate digital subscriber line (VDSL) technology provides faster data transmission. The VDSL lines connect service provider networks and customer sites to provide high bandwidth applications over a single connection.</p> <p>When you choose VDSL2, select the <b>Profile</b> from the drop-down list. Profile is a list of pre-configured VDSL2 settings. The following profiles are supported: 17a and 30a.</p>
DSL Mode: ADSL2/2+	<p>Asymmetric digital subscriber line (ADSL) technology is part of the xDSL family and is used to transport high-bandwidth data. ADSL2 improves the data rate and reach performance, diagnostics, standby mode, and interoperability of ADSL modems. ADSL2+ doubles the possible downstream data bandwidth.</p> <p>If you choose ADSL2/2+, configure the following settings:</p> <ul style="list-style-type: none"> <li>■ <b>PVC</b> – A permanent virtual circuit (PVC) is a software-defined logical connection in a network such as a frame relay network. Choose a PVC number from the drop-down list. The range is from 0 to 7.</li> <li>■ <b>VPI</b> – Virtual Path Identifier (VPI) is used to identify the path to route the packet of information. Enter the VPI number, ranging from 0 to 255.</li> <li>■ <b>VCI</b> – Virtual Channel Identifier (VCI) defines the fixed channel on which the packet of information should be sent. Enter the VCI number, ranging from 35 to 65535.</li> <li>■ <b>PVC VLAN</b> – Set up a VLAN to run over PVCs on the ATM module. Enter the VLAN ID, ranging from 1 to 4094.</li> <li>■ <b>VLAN TX</b> – Upstream VLAN tagging ID. Supported values are 1-4094.</li> <li>■ <b>VLAN RX</b> – Downstream VLAN tagging ID, supported values are 1-4094.</li> <li>■ <b>VLAN TX OP</b> – Operation to perform the upstream PVC VLAN. Supported values are 0-2.</li> <li>■ <b>VLAN RX OP</b> – Operation to perform for the downstream PVC VLAN, supported values are 0-2.</li> </ul>

- 7 Click **Save** to save the configuration.
- 8 At the Edge level, you can override the SFP interface settings for the SD-WAN Edge 610 or the SD-WAN Edge 610-LTE device by navigating to the **Configure > Edges > Device > Connectivity > Interfaces** page.

## Configure GPON Settings

Gigabit Passive Optical Network (GPON) is a point-to-multipoint access network that uses passive splitters in a fiber distribution network, enabling one single feeding fiber from the provider to serve multiple homes and small businesses. GPON supports triple-play services, high-bandwidth, and long reach (up to 20km).

GPON has a downstream capacity of 2.488 Gb/s and an upstream capacity of 1.244 Gbps/s that is shared among users. Encryption is used to keep each user's data private and secure. There are other technologies that could provide fiber to the home; however, passive optical networks (PONs) like GPON are generally considered the strongest candidate for widespread deployments.

### GPON Support

GPON supports the following functions to meet the requirements of broadband services:

- Longer transmission distance: The transmission media of optical fibers covers up to 60 km coverage radius on the access layer, resolving transmission distance and bandwidth issues in a twisted pair transmission.
- Higher bandwidth: Each GPON port can support a maximum transmission rate of 2.5 Gbit/s in the downstream direction and 1.25 Gbit/s in the upstream direction, meeting the usage requirements of high-bandwidth services, such as high definition television (HDTV) and outside broadcast (OB).
- Better user experience on full services: Flexible QoS measures support traffic control based on users and user services, implementing differentiated service provisioning for different users.
- Higher resource usage with lower costs: GPON supports a split ratio up to 1:128. A feeder fiber from the CO equipment room can be split into up to 128 drop fibers. This economizes on fiber resources and O&M costs.

### Configuring GPON ONT from the SASE Orchestrator

You can configure the SFP GPON interface settings only for the SD-WAN Edge 610 or the SD-WAN Edge 610-LTE device by navigating to the **Configure > Profiles/Edges > Device > Connectivity > Interfaces** page in the **SD-WAN** service of the Enterprise portal.

Click the SFP interface that the specific GPON module is plugged into. When the SFP is plugged in, the slot name will display as SFP1 and SFP2 in the **Interfaces** area of the SASE Orchestrator.

General				Switch Port Settings		Routed Interface Settings			Multicast	
Interface	Type	VNF Insertion	Segment	Mode	VLANs	Addressing	WAN Link	OSPF	IGMP	PIM
GE1	Switched		Global Segment	Access	1 - Corporate			N/A		
GE2	Switched		Global Segment	Access	1 - Corporate			N/A		
GE3	Routed	<input checked="" type="checkbox"/> Off	All Segments			IPv4 - DHCP	<input checked="" type="checkbox"/> Auto-Detect	OSPF: <input checked="" type="checkbox"/> Not Enabled OSPFv3: <input checked="" type="checkbox"/> Not Enabled		
GE4	Routed	<input checked="" type="checkbox"/> Off	All Segments			IPv4 - DHCP	<input checked="" type="checkbox"/> Auto-Detect	OSPF: <input checked="" type="checkbox"/> Not Enabled OSPFv3: <input checked="" type="checkbox"/> Not Enabled		
GE5	Routed	<input checked="" type="checkbox"/> Off	All Segments			IPv4 - DHCP	<input checked="" type="checkbox"/> Auto-Detect	OSPF: <input checked="" type="checkbox"/> Not Enabled OSPFv3: <input checked="" type="checkbox"/> Not Enabled		
GE6	Routed	<input checked="" type="checkbox"/> Off	All Segments			IPv4 - DHCP	<input checked="" type="checkbox"/> Auto-Detect	OSPF: <input checked="" type="checkbox"/> Not Enabled OSPFv3: <input checked="" type="checkbox"/> Not Enabled		
SFP1	Routed	<input checked="" type="checkbox"/> Off	All Segments			IPv4 - DHCP	<input checked="" type="checkbox"/> Auto-Detect	OSPF: <input checked="" type="checkbox"/> Not Enabled OSPFv3: <input checked="" type="checkbox"/> Not Enabled		
SFP2	Routed	<input checked="" type="checkbox"/> Off	All Segments			IPv4 - DHCP	<input checked="" type="checkbox"/> Auto-Detect	OSPF: <input checked="" type="checkbox"/> Not Enabled OSPFv3: <input checked="" type="checkbox"/> Not Enabled		
WLAN1	Switched									
WLAN2	Switched									

## To Configure GPON ONT SFP at the Profile level from the SASE Orchestrator:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles > Device > Connectivity > Interfaces**
- 2 Select and expand an Edge model (for example SD-WAN Edge 610) for which you want to configure the SFP GPON interface settings.
- 3 Under the **Interface** column, click the SFP interface link (for example SFP1) that you want to configure.

The **Interface SFP1** dialog for the selected SD-WAN Edge device is displayed.

---

**Note** The following steps describe only the SFP configuration. For a description of the other fields in the selected SD-WAN Edge device, see section [Configure Interface Settings for Profiles](#).

- 4 To configure GPON settings in the **Interface SFP1** dialog, scroll down to the **SFP Settings** area.

## Edge 6X0

X

## Interface SFP1

▲

**Description**

Enter Description (Optional)



Maximum 256 characters

**Interface Enabled** Enabled**Capability**

Routed

**Segments**

All Segments

**Radius Authentication**

✖ WAN Link must be disabled to configure RADIUS Authentication.

**ICMP Echo Response** Enabled**Underlay Accounting** ⓘ Enabled**Enable WAN Link** Enabled**DNS Proxy** Enabled**VLAN**

---

**EVDSL Modem Attached** Enabled

## Edge 6X0

X

**NAT Direct Traffic** Enabled**Trusted Source** ⓘ Enabled**Reverse Path Forwarding**

Specific



Reverse Path Forwarding options are only settable when trusted zone is checked. When trusted zone is un-checked, the value will default to Specific.

**IPv6 Settings** Enabled**Addressing Type**

DHCP Stateless



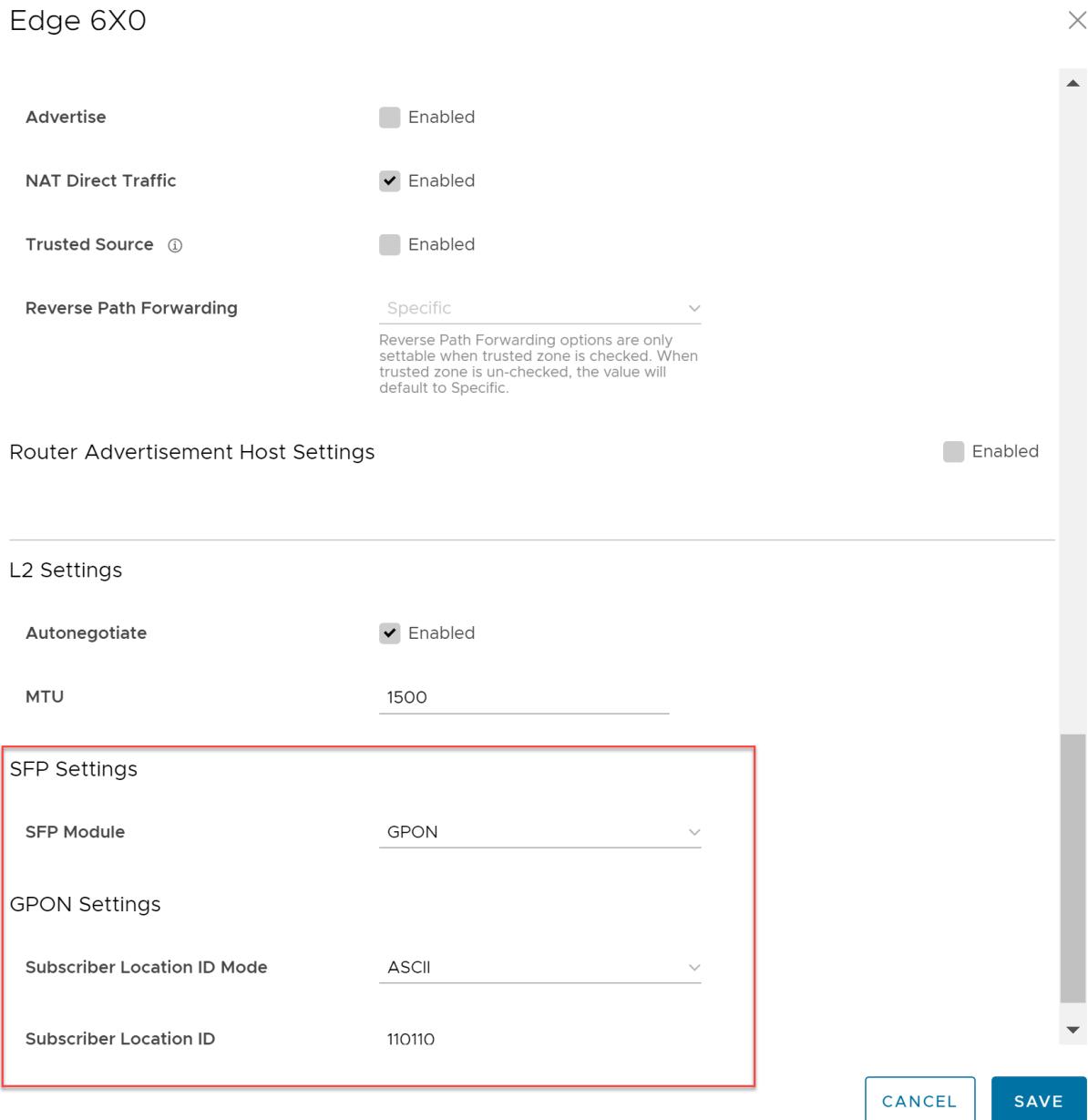
IP Address	N/A
Cidr Prefix	N/A
Gateway:	N/A

**VNF Insertion**

✖ VNF insertion is disallowed when an interface is configured for WAN links

 Enabled Enabled

- 5 From the **SFP Module** drop-down menu, choose **GPON**.



- 6 In the **GPON Settings** area, configure the following:

- **Subscriber Location ID Mode** - Enter the Subscriber Location ID Mode. The Subscriber Location ID can be up to 10 ASCII characters or up to 20 Hex Numbers. The ASCII Subscriber Location ID mode will allow up to 10 ASCII characters. The HEX Subscriber Location ID mode will allow up to 20 Hexadecimal characters.
- **Subscriber Location ID** - Enter the Subscriber Location ID.

- 7 Click **Save** to save the configuration.

- 8 At the Edge level, you can override the SFP interface settings for the SD-WAN Edge 610 or the SD-WAN Edge 610-LTE device by navigating to the **Configure > Edges > Device > Connectivity > Interfaces** page.

### Troubleshooting GPON Settings

The GPON diagnostic test is available only for 6X0 devices. For more information, see the *VMware SD-WAN Troubleshooting Guide* published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

## Configure DHCPv6 Prefix Delegation for Profiles

To configure DHCPv6 Prefix Delegation for a Profile, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**. The **Profiles** page displays the existing profiles.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. The configuration options for the selected Profile are displayed in the **Device** tab.
- 3 DHCPv6 Prefix Delegation can be configured on WAN, LAN, and VLAN interfaces. See the following sections for more details.

### DHCPv6 Prefix Delegation on a WAN interface

---

**Note** For a WAN interface, the **Enable WAN Link** option must be selected.

---

- 1 On the Profile Device settings page, go to the **Connectivity** category, and then expand **Interfaces**.
- 2 You can select an Edge model for which you wish to configure the Prefix Delegation settings.
- 3 From the list of available Edge interfaces, click the link to a Routed WAN interface.
- 4 On the Routed Interface settings screen, navigate to **IPv6 Settings**.

IPv6 Settings

Enabled

Addressing Type	DHCP Stateless
IP Address	N/A
Cidr Prefix	N/A
Gateway:	N/A

DHCPv6 Client Prefix Delegation

Enabled

Select Tag     New Tag

tag1

**⚠ Tag will not have any effect until it is associated with the corresponding LAN/VLAN.**

WAN Link

Auto-Detect

OSPF

OSPF not enabled for the selected Segment

Advertise

Enabled

**CANCEL** **SAVE**

- 5 Activate the **DHCPv6 Client Prefix Delegation** feature by selecting the **Enabled** check box.
- 6 You can either select a pre-defined tag from the drop-down menu or create a new tag by selecting the **New Tag** option. You can also define tags on the **Network Services** screen. For more information, see [Configure Prefix Delegation Tags](#).

---

**Note** Each WAN interface must have a unique tag.

---

- 7 Click **Save**.

### DHCPv6 Prefix Delegation on a LAN interface

---

**Note** For a LAN interface, ensure that the **Enable WAN Link** option is not selected.

---

- 1 On the Profile Device settings page, go to the **Connectivity** category, and then expand **Interfaces**.
- 2 You can select an Edge model for which you wish to configure the Prefix Delegation settings.
- 3 From the list of available Edge interfaces, click the link to a Routed LAN interface.
- 4 On the Routed Interface settings screen, navigate to **IPv6 Settings**.

IPv6 Settings

Enabled

Addressing Type	DHCPv6 Prefix Delegation
IP Address	N/A
Prefix Length	64
Interface Address	fd::1:2:3:1 Example: ::1:0:0:0:1
Tag	tag1
<span style="color: orange;">⚠️</span> DHCPv6 Prefix Delegation tags are effective only if they are associated with the corresponding WAN. <span style="float: right;">X</span>	
OSPF	<span style="color: red;">X</span> OSPF not enabled for the selected Segment
Advertise	<input type="checkbox"/> Enabled
NAT Direct Traffic	<input checked="" type="checkbox"/> Enabled

CANCEL SAVE

- 5 To configure Prefix Delegation for a LAN interface, you must select the **Addressing Type** as **DHCPv6 Prefix Delegation** from the drop-down menu.
- 6 The following additional options appear on the screen:

Option	Description
Prefix Length	This field is auto-populated. The value displayed is <b>64</b> . This indicates that a netmask of 64 bits is configured for this interface's address.
Interface Address	Enter a valid interface address. The new address is formed by combining the prefix provided by the server and the interface address that is configured. If 'n' bits prefix is received from the server, then the first 'n' bits of the interface address are overwritten to form a new address.
Tag	Select the tag from the drop-down menu to associate the configured interface address with the corresponding WAN interface.

**Note** Same tag can be used by multiple LAN interfaces.

- 7 Click **Save**.

**Note** For information on the other settings on this screen, see [Configure Interface Settings for Profiles](#).

### DHCPv6 Prefix Delegation on a VLAN interface

- 1 On the Profile Device settings page, go to the **Connectivity** category, and then expand **VLAN**.
- 2 Click on a VLAN interface.
- 3 In the **Edit VLAN** dialog, navigate to the **IPv6 Settings** section.

- 4 To configure Prefix Delegation for a VLAN interface, you must select the **Addressing Type** as **DHCPv6 Prefix Delegation** from the drop-down menu.
- 5 Select a tag from the drop-down menu.
- 6 Enter a valid interface address.
- 7 Click **Done**.

For more information on VLAN for Profiles, see [Configure VLAN for Profiles](#).

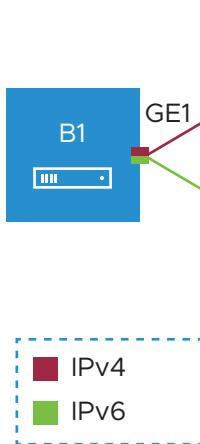
## IPv6 Settings

VMware SD-WAN supports IPv6 addresses to configure the Edge Interfaces and Edge WAN Overlay settings.

The VCMP tunnel can be setup in the following environments: IPv4 only, IPv6 only, and dual stack.

### Mixed Environment on Edge to Edge Network

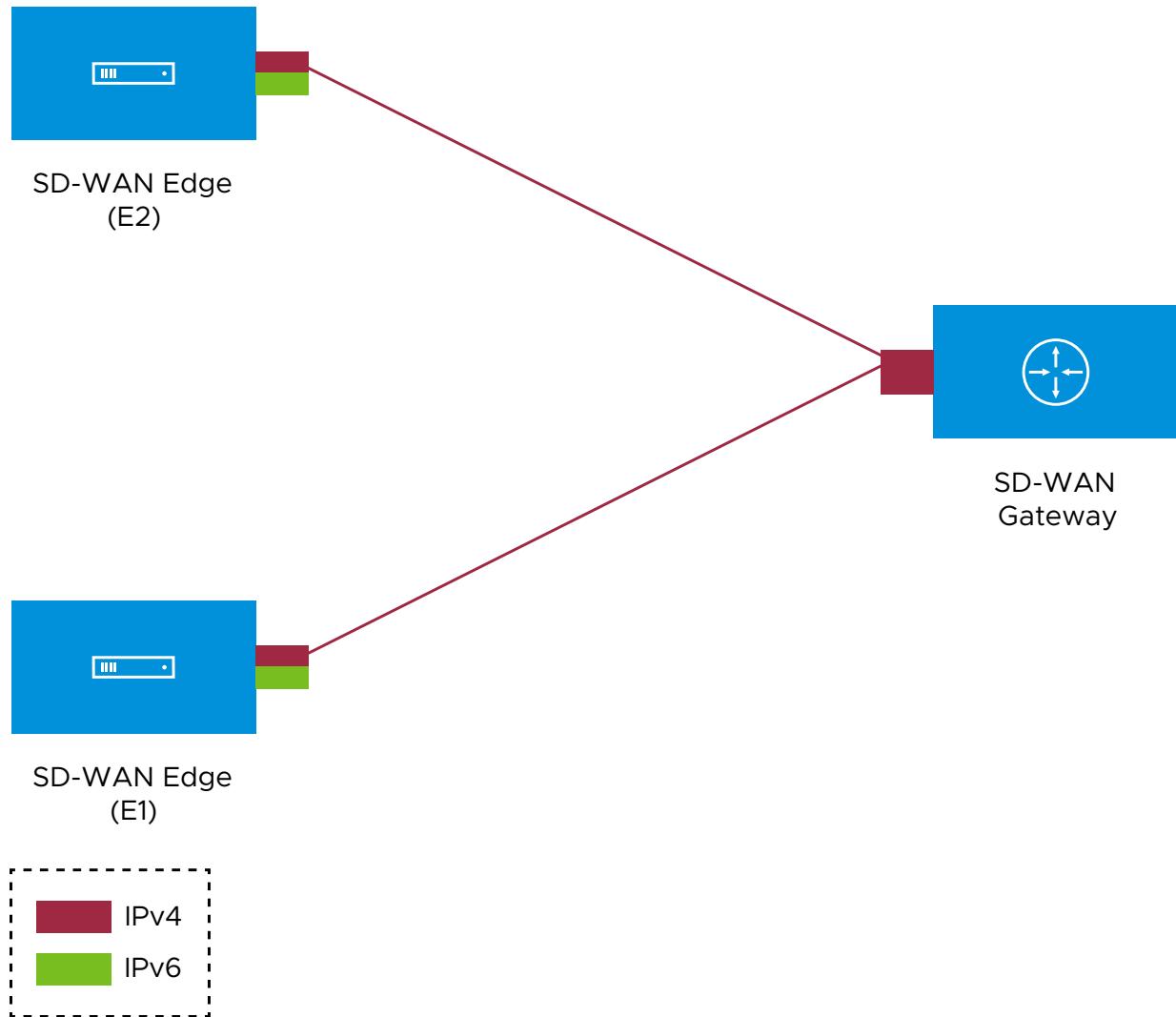
If the initiator is dual-stack and the responder is single-stack, then the tunnel preference of initiator is ignored and tunnel is formed based on IP type of the responder. In other cases, the tunnel preference of the initiator takes precedence. You cannot establish overlay between an IPv4 only and IPv6 only Interfaces.



In the above example, the Edge B1 has dual stack Interface. The Edge B1 can build IPv4 VCMP to the IPv4 only Interface on Edge B2 (unpreferred tunnel) and IPv6 VCMP to the IPv6 only Interface on Edge B3 (preferred tunnel).

#### Mixed Environment on Edge to Gateway Network

When a dual-stack (both IPv4 and IPv6 activated) Edge connects to a single-stack Gateway (IPv4 only), IPv4 tunnel is established.



In the above illustration, the IPv4-only Gateway is connected to Edges E1 and E2 that have dual stack Interfaces with preference as IPv6. An IPv4 tunnel is established between the Gateway and Edges.

In this scenario, the Edges do not learn the public IPv6 endpoints of the other Edges/Hubs from the Gateway, as the Gateway is not IPv6 capable. They only learn the IPv4 endpoints, along with the information that the overlay preference of the other Edge or Hub is IPv6. Even though both the devices negotiate and understand that their overlay preference matches (IPv6), they will not be able to form IPv6 tunnels between them due to lack of IPv6 endpoint information. In addition, the overlay preference negotiation match (both IPv6) prevents the devices from forming IPv4 tunnels with each other.

In such cases where an Edge is connected to an IPv4-only Gateway, it is recommended to set the overlay preference as IPv4 so that the Edges can establish IPv4 tunnels among themselves.

---

**Note** It is recommended not to include IPv4-only Gateway into a Gateway Pool with dual stack Gateways.

---

### Dual Stack Environment

When all the Edges and Gateways are on dual stack, the tunnel preference is selected as follows:

- **Edge to Gateway** – The initiator, Edge, always chooses the tunnel type based on the tunnel preference.
- **Edge to Hub** – The initiator, Spoke Edge, always chooses the tunnel type based on the tunnel preference.
- **Dynamic Branch to Branch** – When there is a mismatch in the tunnel preference, the connection uses IPv4 addresses to ensure consistent and predictable behavior.

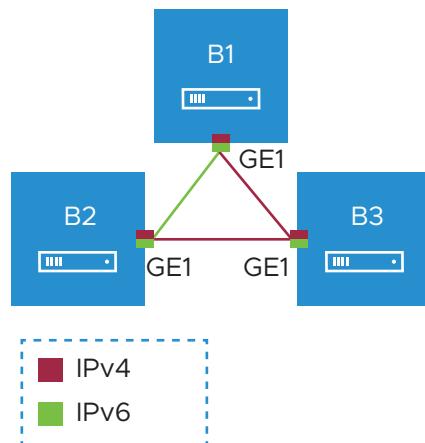
For Edge to Edge connections, the preference is chosen as follows:

- When the Interfaces of Edge peers are set with same preference, the preferred address type is used.
- When the Interfaces of Edge peers are set with different preferences, then the preference of the initiator is used.

---

**Note** When both the ends are on dual stack, with IPv4 as the preference and the overlay established with IPv4, the IPv6 overlay will not be established.

---



In the above Illustration, all the Edges are on dual stack with the following preferences:

- Edge B1: IPv6
- Edge B2: IPv6
- Edge B3: IPv4

In the above example, a dynamic Edge to Edge tunnel is built over IPv4 between the Edges B2 and B3, regardless of the site that initiates the connection.

#### **Impact of IPv6 Tunnel on MTU**

When a branch has at least one IPv6 tunnel, DMPO uses this tunnel seamlessly along with other IPv4 tunnels. The packets for any specific flow can take any tunnel, IPv4 or IPv6, based on the real time health of the tunnel. An example for specific flow is path selection score for load balanced traffic. In such cases, the increased size for IPv6 header (additional 20 bytes) should be taken into account and as a result, the effective path MTU will be less by 20 bytes. In addition, this reduced effective MTU will be propagated to the other remote branches through Gateway so that the incoming routes into this local branch from other remote branches reflect the reduced MTU.

When there are single or multiple sub Interfaces available, the Route Advertisement MTU is not updated properly in sub Interface. The sub Interfaces inherit the MTU value from the Parent Interface. The MTU values received on sub interfaces are ignored and only the parent interface MTU is honored. When an Edge has single sub Interface or multiple sub Interfaces, you must turn off the MTU option in the Route Advertisement of the peer Router. As an alternative, you can modify the MTU value of a sub Interface in a user-defined WAN overlay. For more information, see [Configure Edge WAN Overlay Settings](#).

#### **IPv6 Capability of Edge**

The IPv6 Capability of an Edge is decided based on the IPv6 admin status of any interface. The Edge should have any one of the following activated with IPv6: Switched-VLAN, Routed-Interface, Sub-Interface, Loopback-Interface. This allows to categorize the Edge as IPv6 capable node to receive the IPv6 remote routes from Gateway.

---

**Note** Hubs always receive IPv6 remote routes, irrespective of their IPv6 Capability.

---

### Limitations of IPv6 Address Configuration

- SD-WAN Edge does not support configuring private overlay on one address family and public overlay on the other address family in the same routed Interface. If configured, the SD-WAN Edge would initiate the tunnel using the preferred address family configured on the routed Interface.
- The tunnel preference change can be disruptive for the PMTU overhead. When there is a change in the configuration to setup all Interfaces with IPv4 tunnel preference, the Edge to Edge or Hub to Spoke tunnels may be torn down and re-established to use the IPv4 overhead to ensure that the tunnel bandwidth is used optimally.
- In an Interface with different IP links, the bandwidth measured by the preferred tunnel or link is inherited by other links. Whenever the tunnel preference is changed for a link from IPv6 to IPv4 or vice versa, the link bandwidth is not measured again.
- When there is a change in the tunnel address or change in the preference of the tunnel from IPv6 to IPv4 address or vice versa, the existing flows are dropped in a Hub or Spoke. You should flush the flows in the Hub or Spoke to recover the bi-directional traffic.
- While monitoring the events for a Gateway in **Operator Events** page or an Edge in the **Monitor > Events** page, when the Gateway or Edge is not able to send heartbeat, the corresponding event message displays the IPv6 address with hyphens instead of colons, in the following format: x-x-x-x-x-x-x-x. This does not have any impact on the functionality.
- Edge version running 4.x switched interface does not support IPv6 address.
- SD-WAN Edge does not use new IPv6 prefixes if it has multiple IPv6 prefixes because it might cause tunnel flaps. In this case, Edge prioritizes the old IPv6 prefix. If there is a need to use the new IPv6 prefix, it is recommended to bounce the Internet-facing WAN interface or restart the Edge for immediate recovery. Alternatively, you can wait until the old address entry ages out.

### Management Traffic and IP Addresses

When Edge goes offline with multiple combination of IP address family being used, the Edge will not be able to communicate with the Orchestrator. This happens when sending direct traffic and link selection fails.

In Dual stack Orchestrator and Edge, the Management Plane Daemon (MGD) always prefers IPv6 address for MGD to Orchestrator communication. If IPv6 fails, then it falls back to IPv4. The following matrix shows IP family chosen by MGD for Orchestrator communication.

Orchestrator				
Edge		IPv4	IPv6	Dual
	IPv4	MGD traffic is IPv4	Mis-matched family	MGD traffic is IPv4
	IPv6	Mis-matched family	MGD traffic is IPv6	MGD traffic is IPv6
	Dual	MGD traffic is IPv4	MGD traffic is IPv6	MGD traffic is IPv6

MGD traffic is always sent over overlay through cloud Gateway unless all the paths to Gateway are down. In this case MGD traffic to Orchestrator is sent directly. The following is the logic to drain packet direct.

- 1 Loop over all the Interface. In the following cases, the Edge is left with Interfaces consisting of activated WAN links only.
  - a Interface on which WAN overlay is deactivated is not considered.
  - b When Interface is single stack with IPv6 and traffic is IPv4, then it is not considered.
  - c When Interface is single stack with IPv4 and traffic is IPv6, then it is not considered.
- 2 Loop over WAN link on Interface. In the following cases, the Edge is left with a WAN link that could be used even if paths are down to cloud Gateway.
  - a If WAN link is Standby, then it is not considered.
  - b If WAN link is Private, then it is not considered.

You can configure IPv6 addresses for the following:

- [Configure Static Route Settings](#)
- [Configure Interface Settings for Edges](#)
- [Configure Edge WAN Overlay Settings](#)
- [Configure BGP](#)
- [Configure BFD for Profiles](#)
- [Configure DNS for Profiles](#)
- [Configure Firewall Rule](#)
- [Create Business Policy Rule](#)
- [Configure Object Groups](#)
- [Overlay Flow Control](#)
- [Global IPv6 Settings for Profiles](#)

## Global IPv6 Settings for Profiles

For IPv6 addresses, you can activate some of the configuration settings globally.

To activate global settings for IPv6 at the Profile level:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. The configuration options for the selected Profile are displayed in the **Device** tab.
- 3 Under the **Connectivity** category, click **Global IPv6**.

- 4 You can activate or deactivate the following settings, by using the toggle button. By default, all the options are deactivated.

Option	Description
All IPv6 Traffic	Allows all IPv6 traffic in the network.  <b>Note</b> By default, this option is activated.
Routing Header Type 0 Packets	Allows Routing Header type 0 packets. Deactivate this option to prevent potential DoS attack that exploits IPv6 Routing Header type 0 packets.
Enforce Extension Header Validation	Allows to check the validity of IPv6 extension headers.
Enforce Extension Header Order Check	Allows to check the order of IPv6 Extension Headers.
Drop & Log Packets for RFC Reserved Fields	Allows to reject and log network packets if the source or destination address of the network packet is defined as an IP address reserved for future definition.
ICMPv6 Destination Unreachable messages	Generates messages for packets that are not reachable to IPv6 ICMP destination.
ICMPv6 Time Exceeded Message	Generates messages when a packet sent by IPv6 ICMP has been discarded as it was out of time.
ICMPv6 Parameter Problem Message	Generates messages when the device finds problem with a parameter in ICMP IPv6 header.

By default, the configurations are applied to all the Edges associated with the Profile. If required, you can modify the settings for each Edge by clicking the **Override** option in the **Configure > Edges > {Edge Name} > Device > Connectivity > Global IPv6** page.

## Monitor IPv6 Events

You can view the events related to the IPv6 configuration settings.

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Events**.

To view the events related to IPv6 configuration, you can use the filter option. Click the Filter Icon next to the **Search** option and choose to filter the details by different categories.

The following image shows some of the IPv6 events.

Event	User	Segment	Edge	Severity	Time	Message
IPV6_NEW_ADDR_ADDED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Added new IPv6 Address fd00:1:3:3:2 on interface eth3:101
IPV6_NEW_ADDR_ADDED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Added new IPv6 Address fd00:1:4:2 on interface GE6
IPV6_NEW_ADDR_ADDED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Added new IPv6 Address fd00:1:2:4:2 on interface eth5:100
IPV6_NEW_ADDR_ADDED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Added new IPv6 Address fd00:1:3:4:2 on interface eth5:101
IPV6_ADDR_PREFERRED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Preferred IPv6 address fd00:1:2:2 on interface GE4
IPV6_ADDR_PREFERRED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Preferred IPv6 address fd00:1:3:2 on interface GE5
IPV6_ADDR_PREFERRED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Preferred IPv6 address fd00:1:1:4:2 on interface GE6
IPV6_ADDR_PREFERRED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Preferred IPv6 address fd00:1:1:1:2 on interface GE3
IPV6_ADDR_PREFERRED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Preferred IPv6 address fd00:1:2:3:2 on interface eth3:100
IPV6_ADDR_PREFERRED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Preferred IPv6 address fd00:1:3:3:2 on interface eth3:101
IPV6_ADDR_PREFERRED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Preferred IPv6 address fd00:1:2:4:2 on interface eth5:100
IPV6_ADDR_PREFERRED	b1-edge1			● Notice	Jul 16, 2021, 12:19:34 PM	Preferred IPv6 address fd00:1:3:4:2 on interface eth5:101
Edge Interface Up	b1-edge1			● Info	Jul 16, 2021, 10:41:45 AM	Interface GE6_101 IPv6 is up
Edge Interface Up	b1-edge1			● Info	Jul 16, 2021, 10:41:35 AM	Interface GE6_100 IPv6 is up
Edge Interface Up	b1-edge1			● Info	Jul 16, 2021, 10:41:25 AM	Interface GE6 IPv6 is up
Edge Interface Up	b1-edge1			● Info	Jul 16, 2021, 10:41:14 AM	Interface GE5_101 IPv6 is up

## Troubleshooting IPv6 Configuration

You can run Remote Diagnostics tests to view the logs of the IPv6 settings and use the log information for troubleshooting purposes.

To run the tests for IPv6 settings:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Diagnostics > Remote Diagnostics**.
- 2 The **Remote Diagnostics** page displays all the active Edges.
- 3 Select the Edge that you want to troubleshoot. The Edge enters live mode and displays all the possible Remote Diagnostics tests than you can run on the Edge.
- 4 For troubleshooting IPv6, scroll to the following sections and run the tests:
  - **IPv6 Clear ND Cache** – Run this test to clear the cache from the ND for the selected Interface.
  - **IPv6 ND Table Dump** – Run this test to view the IPv6 address details of Neighbor Discovery (ND) table.

- **IPv6 RA Table Dump** – Run this test to view the details of the IPv6 RA table.
- **IPv6 Route Table Dump** – Run this test to view the contents of the IPv6 Route Table.
- **Ping IPv6 Test** – Choose a Segment from the drop-down, enter the source Interface and the destination IPv6 address. Click **Run** to ping the specified destination from the source Interface and the results of the ping test are displayed.

For more information on Remote Diagnostics, see the "Remote Diagnostic Tests on Edges" section in the VMware SD-WAN Troubleshooting Guide published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

## Configure Wi-Fi Radio Settings

At the Profile level, you can activate or deactivate Wi-Fi Radio and configure the band of radio frequencies.

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**.  
The **Configuration Profiles** page appears.
- 2 Select a profile for which you wish to configure Wi-Fi Radio settings, and then click the **View** link in the **Device** column of the Profile.  
The **Device Settings** page for the selected profile appears.
- 3 Under the **Connectivity** category, click **Wi-Fi Radio**.



- 4 The **Wi-Fi Radio** area expands and by default, the **Radio Enabled** check box is selected and **Channel** is set to **Automatic**.
- 5 Select any one of the radio bands. In case of Edge 710, which supports dual-radio models, you can select both **2.4 GHz** and **5 GHz** radio bands.
- 6 Click **Save Changes**.

At the Edge level, you can override the Wi-Fi Radio settings specified in the Profile, by selecting the **Override** check box. For more information, see [Configure Wi-Fi Radio Overrides](#).

## Configure Common Criteria Firewall Settings for Profiles

Common Criteria (CC) is an international certification accepted by many countries. Obtaining the CC certification is an endorsement that our product has been evaluated by competent and independent licensed laboratories for the fulfilment of certain security properties. This certification is recognized by all the signatories of the Common Criteria Recognition Agreement

(CCRA). The CC is the driving force for the widest available mutual recognition of secure IT products. Having this certification is an assurance of security to a standard extent and can provide VMware with the much needed business parity or advantage with its competitors.

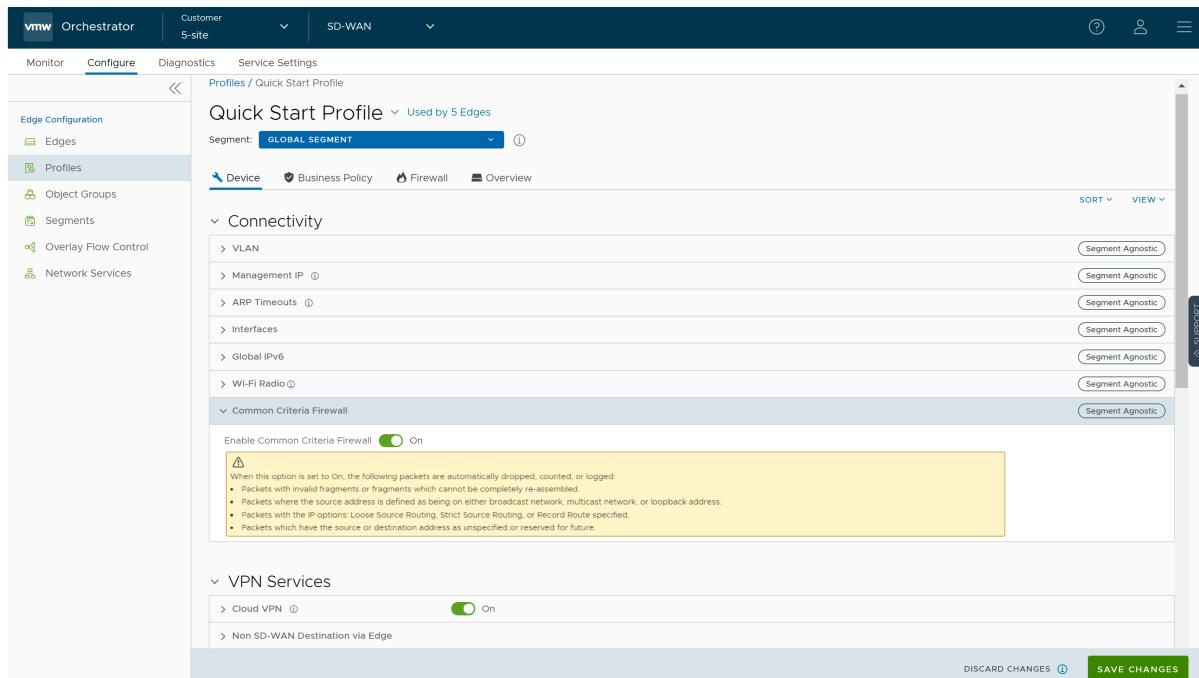
Enterprise users can configure the Common Criteria Firewall settings both at the Edge and Profile levels. By default, this feature is deactivated.

To configure Common Criteria Firewall settings for a Profile, perform the following steps:

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.

- The **Profiles** page displays the existing Profiles.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. You can also select a Profile and click **Modify** to configure the Profile.
  - 3 The **Device** tab displays the configuration options for the selected Profile.



- 4 In the **Connectivity** category, click **Common Criteria Firewall**.
- 5 Turn on **Enable Common Criteria Firewall** toggle button.

When the **Enable Common Criteria Firewall** option is set to On, the following packets are automatically dropped, counted, or logged:

- Packets with invalid fragments or fragments which cannot be completely re-assembled that are destined to the Edge.
- Packets where the source address is defined as being on either broadcast network, multicast network, or loopback address.

- Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.
- Packets which have the source or destination address as unspecified or reserved for future.
- Packets where the source address is equal to the address of the network interface where the network packet was received.
- Packets where the source address does not belong to the networks reachable via the network interface where the network packet was received.
- Packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4.
- Packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6.

The CC Firewall settings are applied to all the Edges associated with the Profile. You can choose to override the CC Firewall settings for an Edge. For steps, see [Configure Common Criteria Firewall Settings for Edges](#).

## Assign Partner Gateway Handoff

In order for customers to be able to assign Partner Gateways for Profiles or Edges, Operator must activate the **Partner Handoff** feature for the customers. If you want to activate the **Partner Handoff** feature, contact your Operator. Once you have the **Partner Handoff** feature activated, you can assign Partner Gateways from the **Configure > Profile/Edges > Device > VPN Services > Gateway Handoff Assignment** page.

### Considerations When Assigning Partner Gateways:

Consider the following notes when assigning Partner Gateways:

- Partner Gateways can be assigned at the Profile or Edge level.
- More than two Partner Gateways can be assigned to an Edge (up to 16).
- Partner Gateways can be assigned per Segment.

---

**Note** If you do not see the **Gateway Handoff Assignment** area displayed in the **Device** page, contact your Operator to activate this feature.

The **Gateway Handoff Assignment** feature has been enhanced to also support segment-based configurations. Multiple Partner Gateways can be configured on the Profile level and/or overridden on the Edge level.

To assign Partner Gateways for Profiles, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.

- 2 Select a profile you want to configure Gateway Handoff Assignment settings and click the **View** link in the **Device** column of the Profile. The **Device** page for the selected profile appears.
- 3 Scroll down to **VPN Services** section and expand **Gateway Handoff Assignment**.

The screenshot shows the 'VPN Services' section expanded, with 'Gateway Handoff Assignment' selected. A table lists one gateway entry:

Order	Gateways
1	gateway-5

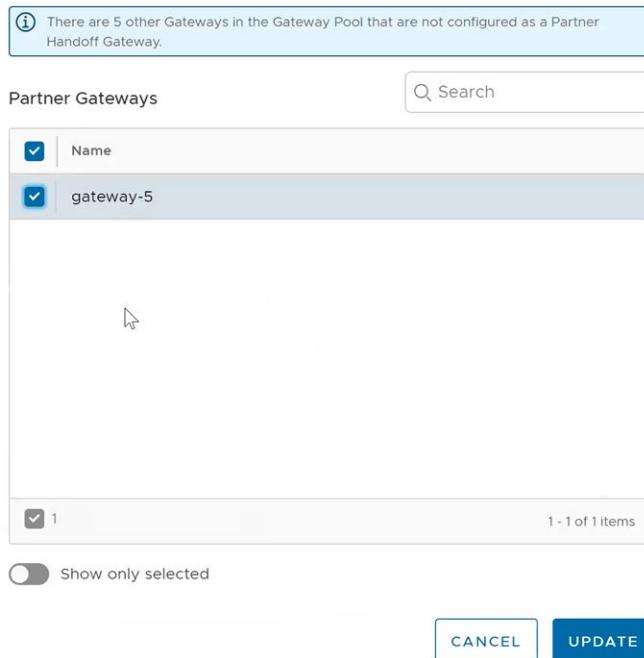
Below the table, several options are listed with their status indicated by toggle switches:

- > Cloud VPN ⓘ  On ⓘ
- > Non SD-WAN Destination via Edge
- > Hub or Cluster Interconnect
- > Cloud Security Service ⓘ  Off

- 4 Click **+ Select Gateways**, the **Select Partner Gateways for Global Segment** dialog box appears.

By default Global Segment is selected in the **Segment** drop-down. You can also choose any other segment based on your requirements.

## Select Partner Gateways for Global Segment



- 5 The **Partner Gateways** section lists the Gateways in the Gateway Pool that are configured as a Partner Handoff Gateway.

**Note** If there are other Gateways not configured as a Partner Handoff Gateway, a following sample message will appear in the dialog box: **There is one other Gateway in the Gateway Pool that is not configured as a Partner Handoff Gateway.**

**Note** If you want to see only the list of selected Partner Gateways then click **Show only selected**.

- 6 Select the Partner Gateways from the list that you want to assign to the Profile and click **Update**.
- 7 The Partner Gateway assignments configured at the Profile level will be applied to all the Edges within the Profile. You can override the settings at the Edge level by clicking the **Override** check box.

Order	Gateways
1	gateway-5

1 item

## Select CDE Gateways

In normal scenarios, the PCI traffic runs between the customer branch and Data Center where the PCI traffic is handoff to the PCI network and the Gateways are out of PCI scope. (The Operator can configure the Gateway to exclude PCI Segment by unchecking the CDE role).

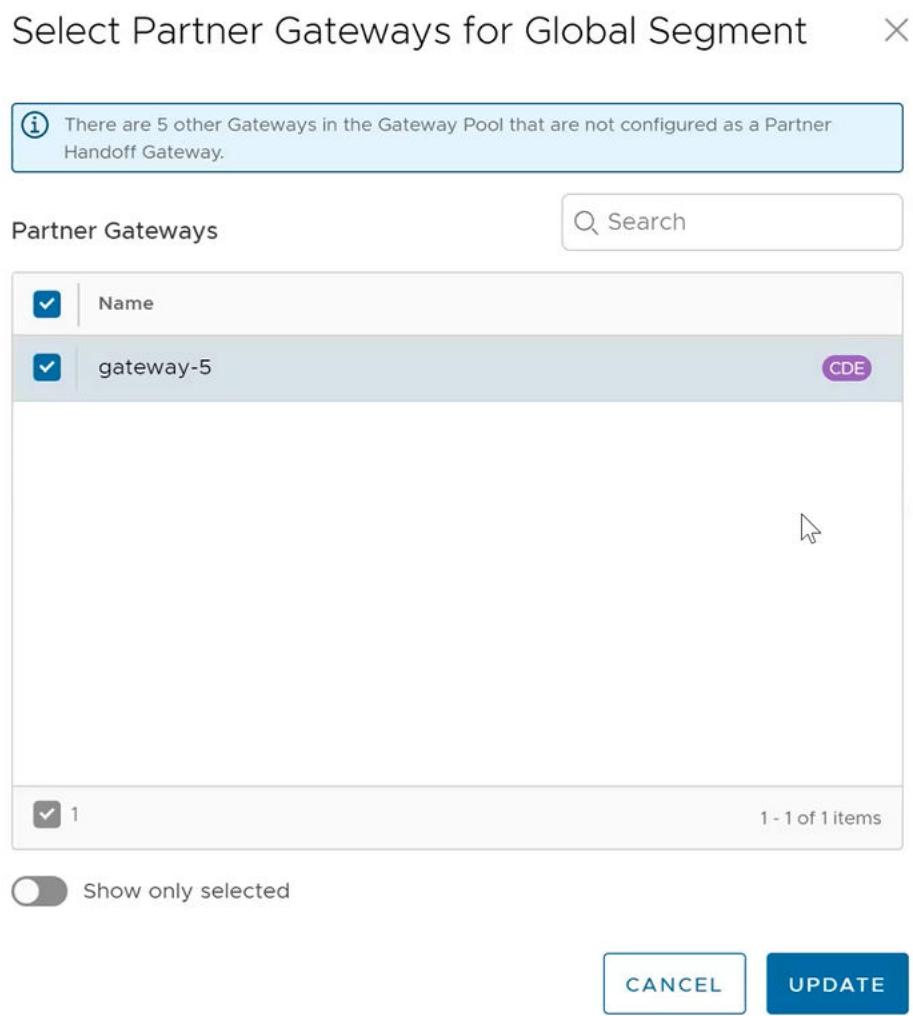
In certain scenarios where Gateways can have a handoff to the PCI network and in the PCI scope, the Operator can activate CDE role for the Partner Gateways and these Gateways (CDE Gateways) will be available for the user to assign in the PCI Segments (CDE Type).

## Assign a CDE Gateway

To assign a CDE Gateway:

By default global segment is selected in the **Segment** drop-down. You can also choose any other segment (CDE Type) based on your requirements.

- 1 a In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.
  - b Select a profile you want to configure Gateway Handoff Assignment settings and click the **View** link in the **Device** column of the Profile. The **Device** page for the selected profile appears.
  - c Scroll down to **VPN Services** section and expand **Gateway Handoff Assignment**.
  - d Click **+ Select Gateways**, the **Select Partner Gateways for Global Segment** dialog box appears.



- e In the **Select Partner Gateways for Global Segment** dialog box, in the **Partner Gateways** section select a Partner Gateway that is marked as CDE that you want to assign to the Profile and click **Update**.

## Assign Controllers

The SD-WAN Gateway is activated for supporting both the data and control plane. In the 3.2 release, VMware introduces a Controller-only feature (Controller Gateway Assignment).

There are multiple use cases which require the SD-WAN Gateway to operate as a Controller only (that is, to remove the data plane capabilities). Additionally, this will activate the Gateway to scale differently, as resources typically dedicated for packet processing can be shifted to support control plane processing. This will activate, for instance, a higher number of concurrent tunnels to be supported on a Controller than on a traditional Gateway. See the following section for a typical use case.

## Use Case: Dynamic Branch-to-Branch via Different Partner Gateways

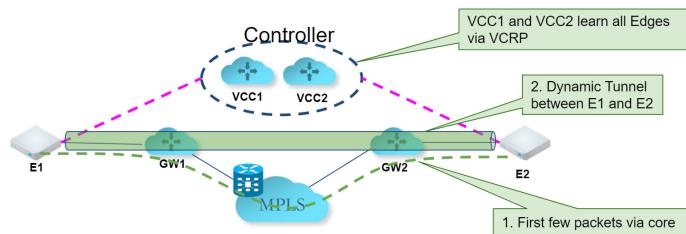
In this scenario, Edge 1 (E1) and Edge 2 (E2) as shown in the image belong to the same enterprise in the Orchestrator. However, they connect to different Partner Gateways (typically due to being in different regions). Therefore, Dynamic Branch-to-Branch is not possible between E1 and E2, but by leveraging the Controller, this is possible.

### Initial Traffic Flow

As shown in the image below, when E1 and E2 attempt to communicate directly, the traffic flow begins by traversing the private network as it would in previous versions of the code. Simultaneously, the Edges will also notify the Controller that they are communicating and request a direct connection.

### Dynamic Tunnel

The Controller signals to the Edges to create the dynamic tunnel by providing E1 connectivity information to E2 and vice versa. The traffic flow moves seamlessly to the new dynamic tunnel if and when it is established.



### Configuring a Gateway as a Controller

In order for customers to be able to assign Controllers for Profiles or Edges, Operator must activate the **Partner Handoff** feature for the customers. If you want to activate the **Partner Handoff** feature, contact your Operator. Once you have the **Partner Handoff** feature activated, you can assign a Partner Gateway as a Controller by navigating to the **Configure > Profile/Edges > Device > VPN Services > Controller Assignment** page.

---

**Note** At least one Gateway in the Gateway Pool should be a "Controller Only" Gateway.

---

- 1 To assign Controllers for Profiles, perform the following steps:
  - a In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.
  - b Select a profile you want to configure Gateway Handoff Assignment settings and click the **View** link in the **Device** column of the Profile. The **Device** page for the selected profile appears.

The screenshot shows the 'VPN Services' section of the VMware SD-WAN Administration Guide. Under 'Controller Assignment', there is a table listing two gateways:

Order	Gateways
1	gateway-4
2	gateway-3

Below the table is a button labeled '+ SELECT GATEWAYS'.

- c Scroll down to **VPN Services** section and expand **Controller Assignment**.
- d Click **+ Select Gateways**, the **Select Partner Gateways for Global Segment** dialog box appears.

## Select Partner Gateways for Global Segment X

**Controllers**

Search

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	gateway-4
<input checked="" type="checkbox"/>	gateway-3

2      1 - 2 of 2 items

Show only selected

CANCEL UPDATE

- e From the **Controllers** section, select the Controllers to assign to the Profile and click **Update**.
- f The Controller assignments configured at the Profile level will be applied to all the Edges within the Profile. You can override the settings at the Edge level by clicking the **Override** check box in the navigation path **Configure > Edges > <Edge name> > VPN Services > Controller Assignment**.

## Configure Cloud VPN

This section covers the following topics:

- [Cloud VPN Overview](#)
- [Configure Cloud VPN for Profiles](#)

- Configure Cloud VPN and Tunnel Parameters for Edges

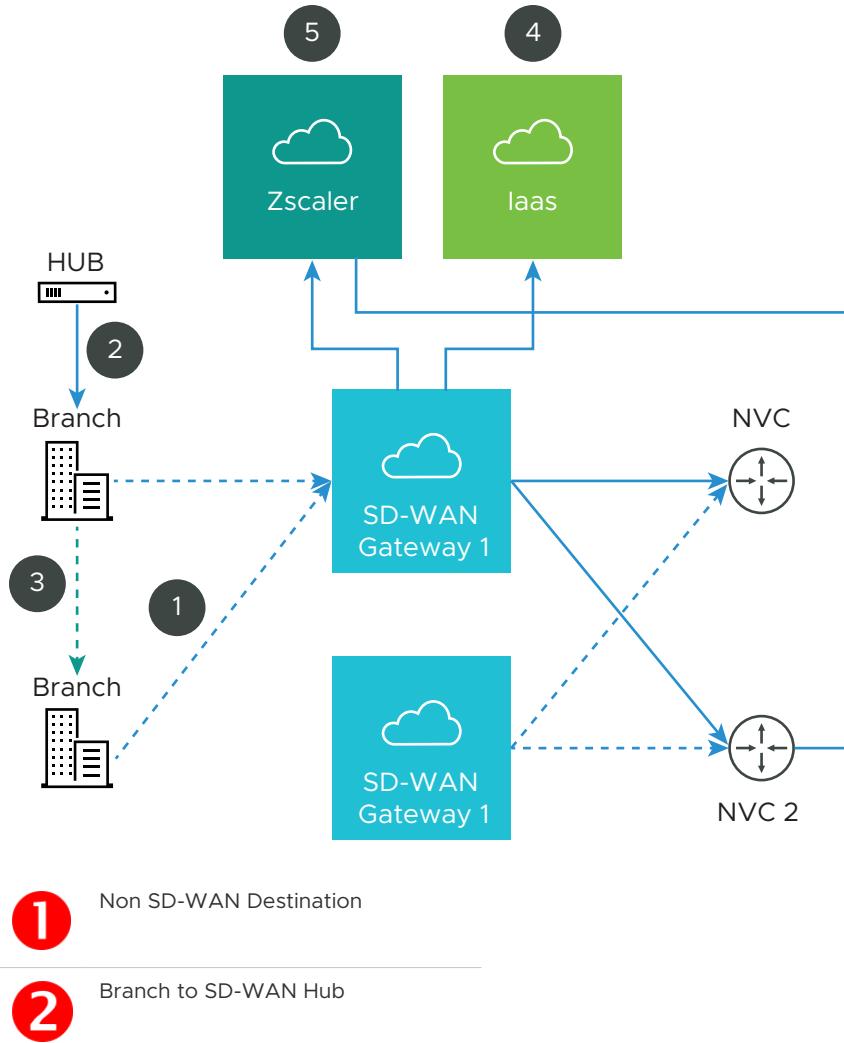
## Cloud VPN Overview

The Cloud Virtual Private Network (VPN) allows a VPNC-compliant IPSec VPN connection that connects VMware and Non SD-WAN Destinations. It also indicates the health of the sites (up or down status) and delivers real-time status of the sites.

Cloud VPN supports the following traffic flows:

- Branch to Non SD-WAN Destination via Gateway
- Branch to SD-WAN Hub
- Branch to Branch VPN
- Branch to Non SD-WAN Destination via Edge

The following figure represents all three branches of the Cloud VPN. The numbers in the image represent each branch and correspond to the descriptions in the table that follows.



- 3** Branch to Branch VPN

---

- 4** Branch to Non SD-WAN Destination

---

- 5** Branch to Non SD-WAN Destination

### Branch to Non SD-WAN Destination via Gateway

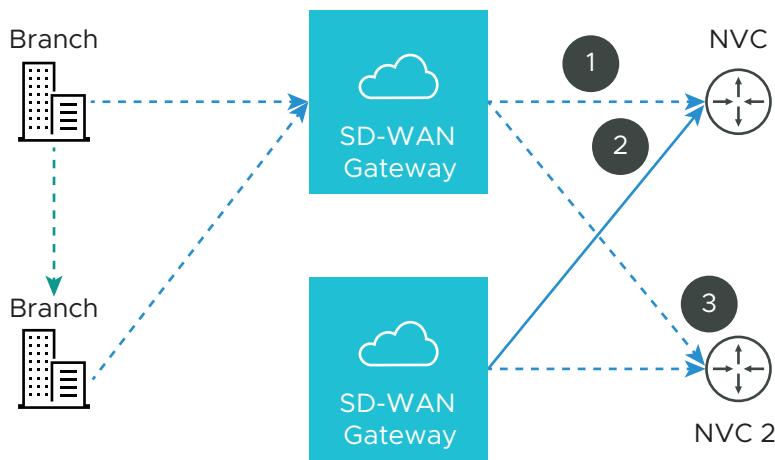
Branch to **Non SD-WAN Destination via Gateway** supports the following configurations:

- Connect to Customer Data Center with Existing Firewall VPN Router
- IaaS
- Connect to CWS (Zscaler)

### Connect to Customer Data Center with Existing Firewall VPN Router

A VPN connection between the VMware Gateway and the data center firewall (any VPN router) provides connectivity between branches (with SD-WAN Edges installed) and Non SD-WAN Destinations, resulting in ease of insertion, in other words, no customer Data Center installation is required.

The following figure shows a VPN configuration:



- 1** Primary tunnel

---

- 2** Redundant tunnel

---

- 3** Secondary VPN Gateway

VMware supports the following Non SD-WAN Destination configurations through SD-WAN Gateway:

- Check Point
- Cisco ASA
- Cisco ISR
- Generic IKEv2 Router (Route Based VPN)
- Microsoft Azure Virtual Hub
- Palo Alto
- SonicWALL
- Zscaler
- Generic IKEv1 Router (Route Based VPN)
- Generic Firewall (Policy Based VPN)

---

**Note** VMware supports both Generic Route-based and Policy-based Non SD-WAN Destination from Gateway.

---

For information on how to configure a Branch to Non SD-WAN Destination through SD-WAN Gateway see [Configure Non SD-WAN Destinations via Gateway](#).

## IaaS

When configuring with Amazon Web Services (AWS), use the Generic Firewall (Policy Based VPN) option in the Non SD-WAN Destination dialog box.

Configuring with a third party can benefit you in the following ways:

- Eliminates mesh
- Cost
- Performance

VMware Cloud VPN is simple to set up (global networks of SD-WAN Gateways eliminates mesh tunnel requirement to VPCs), has a centralized policy to control branch VPC access, assures performance, and secures connectivity as compared to traditional WAN to VPC.

For information about how to configure using Amazon Web Services (AWS), see the [Chapter 17 Configure Amazon Web Services](#) section.

## Connect to CWS (Zscaler)

Zscaler Web Security provides security, visibility, and control. Delivered in the cloud, Zscaler provides web security with features that include threat protection, real-time analytics, and forensics.

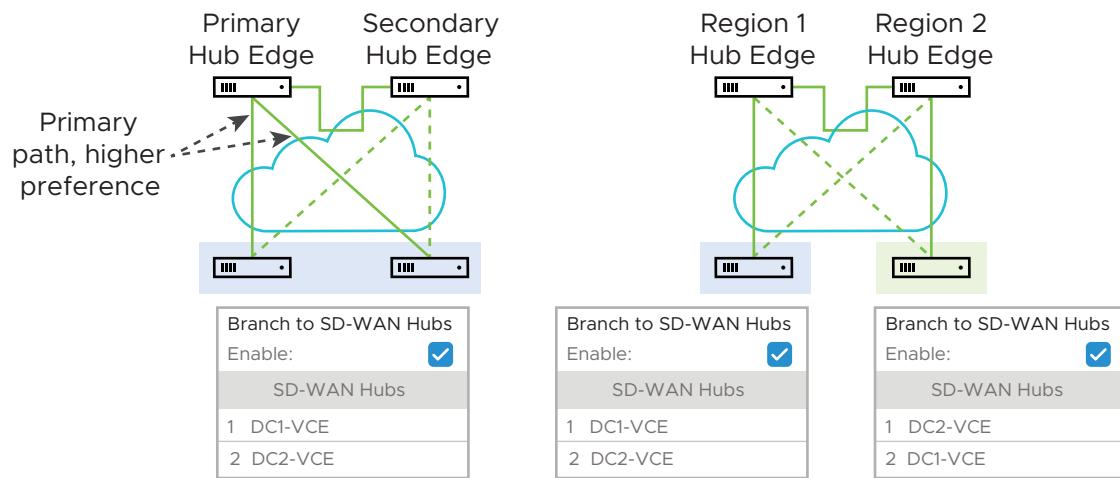
Configuring using Zscaler provides the following benefits:

- Performance: Direct to Zscaler (Zscaler via Gateway)
- Managing proxy is complex: Allows simple click policy aware Zscaler

### Branch to SD-WAN Hub

The SD-WAN Hub is an Edge deployed in Data Centers for branches to access Data Center resources. You must set up your SD-WAN Hub in the SASE Orchestrator. The SASE Orchestrator notifies all the SD-WAN Edges about the Hubs, and the SD-WAN Edges build secure overlay multi-path tunnel to the Hubs.

The following figure shows how both Active-Standby and Active-Active are supported.



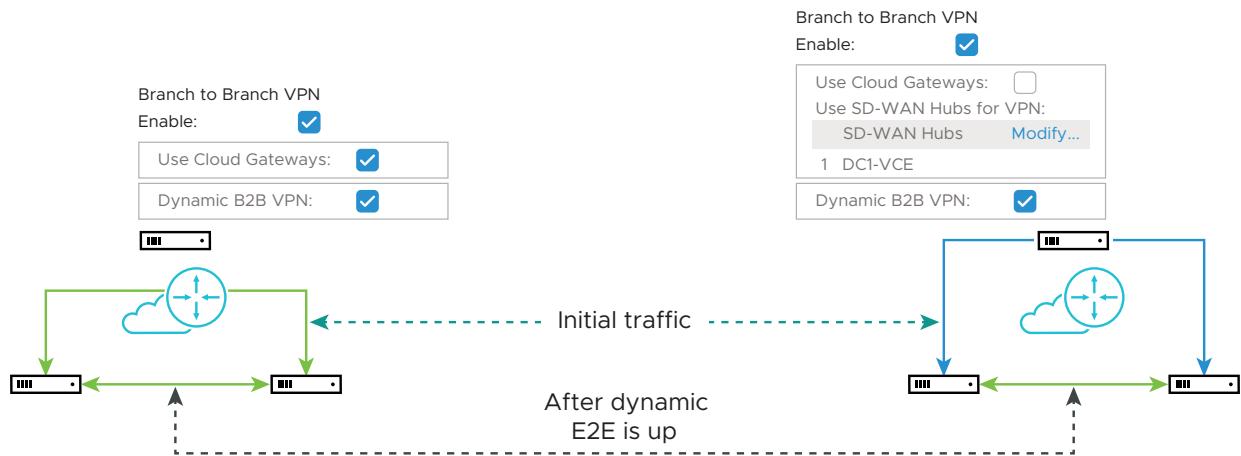
### Branch to Branch VPN

Branch to Branch VPN supports configurations for establishing a VPN connection between branches for improved performance and scalability.

Branch to Branch VPN supports two configurations:

- Cloud Gateways
- SD-WAN Hubs for VPN

The following figure shows Branch to Branch traffic flows for both Cloud Gateway and a SD-WAN Hub.



You can also activate **Dynamic Branch to Branch VPN** for both Cloud Gateways and Hubs.

You can access the 1-click Cloud VPN feature in the SASE Orchestrator from **Configure > Profiles > Device Tab** in the **Cloud VPN** area.

---

**Note** For step-by-step instructions to configure Cloud VPN, see [Configure Cloud VPN for Profiles](#).

---

### Branch to Non SD-WAN Destination via Edge

Branch to **Non SD-WAN Destination via Edge** supports the following Route-based VPN configurations:

- Generic IKEv2 Router (Route Based VPN)
- Generic IKEv1 Router (Route Based VPN)

---

**Note** VMware supports only Route-based Non SD-WAN Destination configurations through Edge.

---

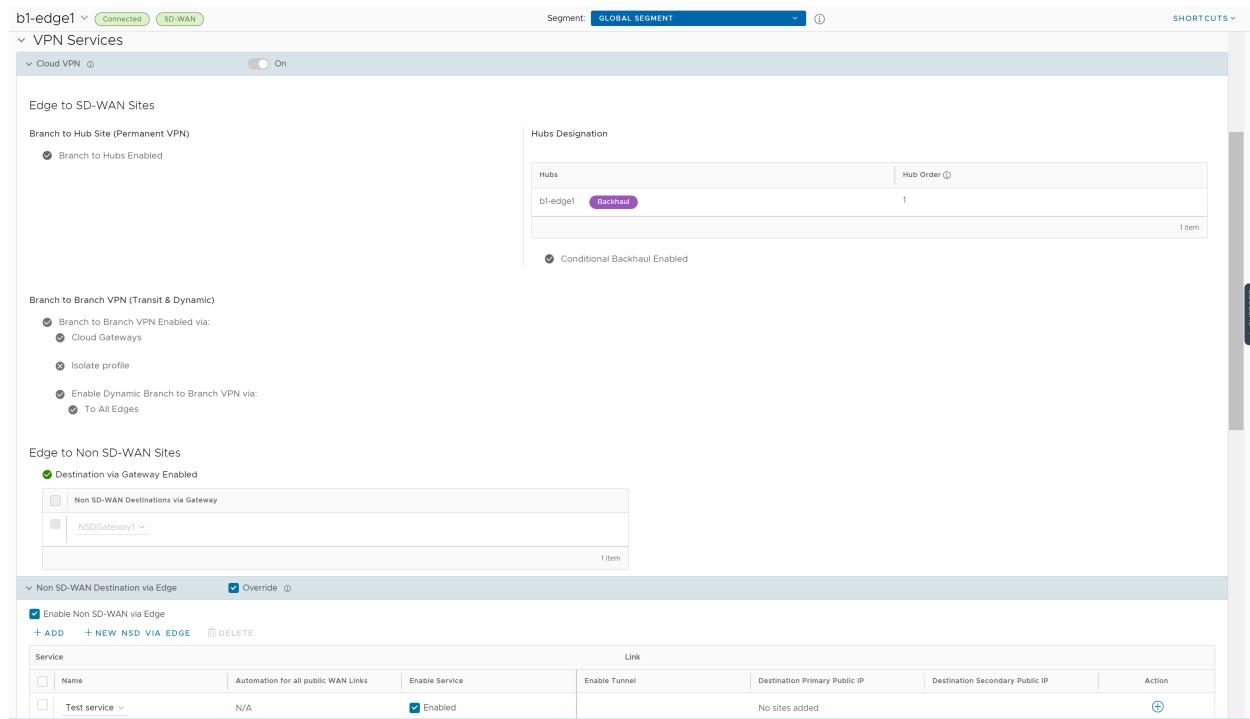
For more information, see [Configure Non SD-WAN Destinations via Edge](#).

### Configure Cloud VPN for Profiles

At the Profile level, SASE Orchestrator allows you to configure Cloud Virtual Private Network (VPN). To initiate and respond to VPN connection requests, you must activate **Cloud VPN**.

To configure **Cloud VPN** for a Profile, follow the below steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles > Device tab**.
- 2 Go to **VPN Services** area and activate **Cloud VPN** by turning the toggle button to **On**.



On activating Cloud VPN for a Profile, you can configure the following Cloud VPN types:

- Configure a Tunnel Between a Branch and SD-WAN Hubs VPN
- Configure a Tunnel Between a Branch and a Branch VPN
- Configure a Tunnel Between a Branch and a Non SD-WAN Destinations via Gateway
- Configure a Tunnel Between a Branch and a Non SD-WAN Destinations via Edge

To override these settings and to configure Cloud VPN for Edges, see [Configure Cloud VPN and Tunnel Parameters for Edges](#).

---

**Note** **Cloud VPN** must be configured per Segment.

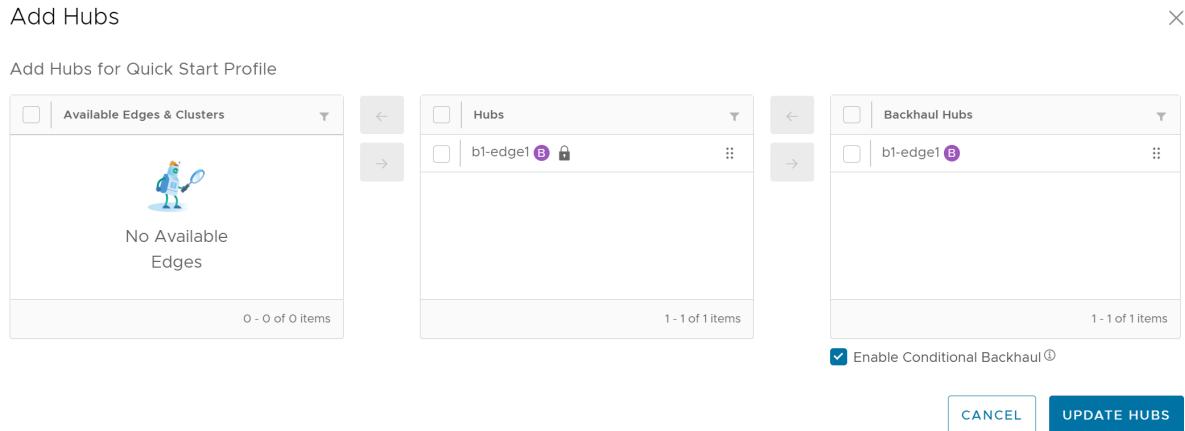
---

For topology and use cases, see [Cloud VPN Overview](#).

### Configure a Tunnel Between a Branch and SD-WAN Hubs VPN

To establish a VPN connection between Branch and Hubs, follow the below steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to [Configure > Profiles](#).
- 2 Select a profile or click the **View** link in the **Device** column. The **Device** settings page for the selected profile appears.
- 3 Go to **VPN Services** area and activate **Cloud VPN** by turning the toggle button to **On**.
- 4 Select the **Enable Branch to Hubs** check box under **Branch to Hub Site (Permanent VPN)**. The **Hubs Designation** section appears on the screen.
- 5 Click **Edit Hubs**. The following window is displayed:



- 6 From **Available Edges & Clusters** section, you can select and configure the Edges to act as SD-WAN Hubs, or Backhaul Hubs.

**Note** An Edge cluster and an individual Edge can be simultaneously configured as Hubs in a Branch Profile. Once Edges are assigned to a Cluster, they cannot be assigned as individual Hubs.

- 7 Select the **Enable Conditional BackHaul** check box to activate Conditional Backhaul.

With **Conditional Backhaul** activated, the Edge can failover Internet-bound traffic (Direct Internet traffic, Internet via SD-WAN Gateway (IPv4 and IPv6) and Cloud Security Traffic via IPsec) to MPLS links whenever there are no Public Internet links available. When Conditional Backhaul is activated, by default all Business Policy rules at the Branch level are subject to failover traffic through Conditional Backhaul. You can exclude traffic from Conditional Backhaul based on certain requirements for selected policies by deactivating this feature at the selected Business Policy level. For more information, see [Conditional Backhaul](#).

- 8 Click **Update Hubs**.

#### Conditional Backhaul

Conditional Backhaul (CBH) is a feature designed for Hybrid SD-WAN branch deployments that have at least one Public and one Private link.

#### Use case 1: Public Internet Link Failure

Whenever there is a Public Internet link failure on a VMware SD-WAN Edge, tunnels to VMware SD-WAN Gateway, Cloud Security Service (CSS), and Direct breakout to Internet are not established. In this scenario, the Conditional Backhaul feature, if activated, makes use of the connectivity through Private links to designated Backhaul Hubs, giving the SD-WAN Edge the ability to failover Internet-bound traffic over Private overlays to the Hub and provides reachability to Internet destinations.

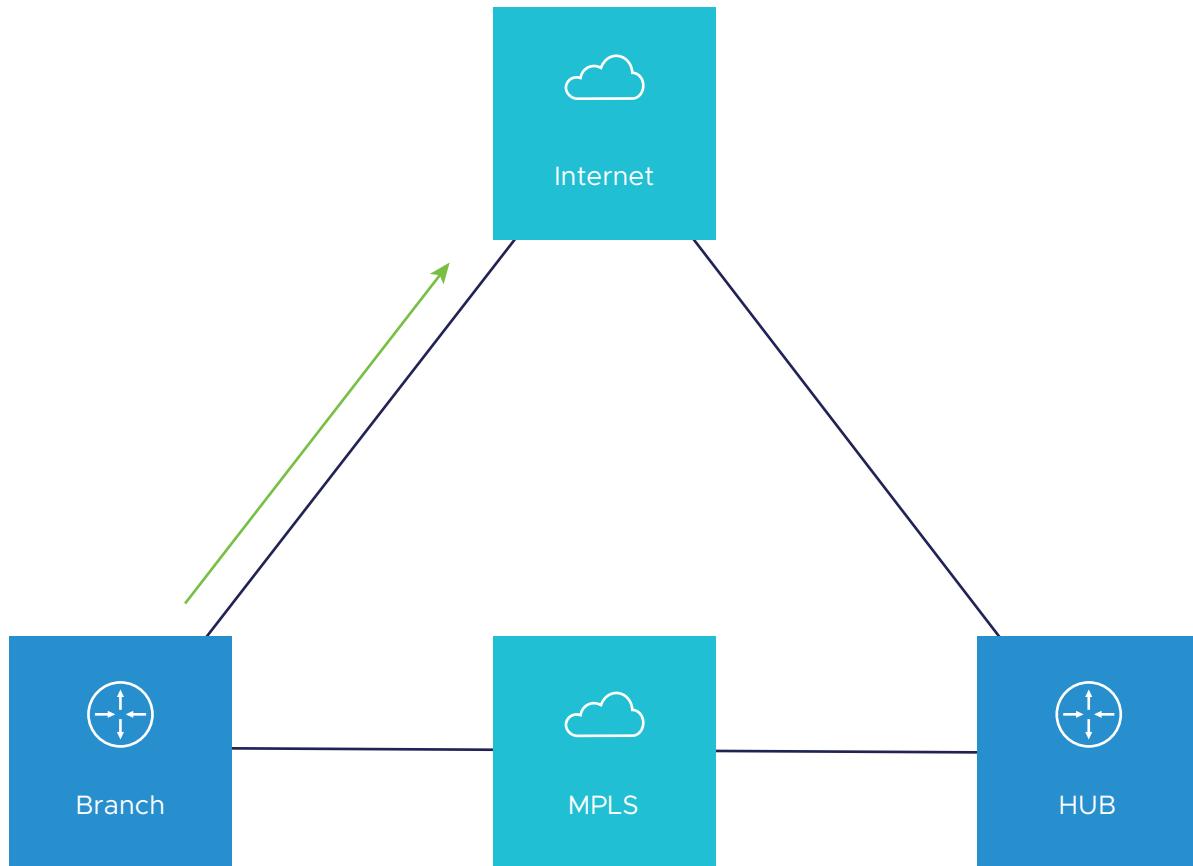
Whenever Public Internet link fails and Conditional Backhaul is activated, the Edge can failover the following Internet-bound traffic types:

- 1 Direct to Internet

2 Internet via SD-WAN Gateway

3 Cloud Security Service traffic

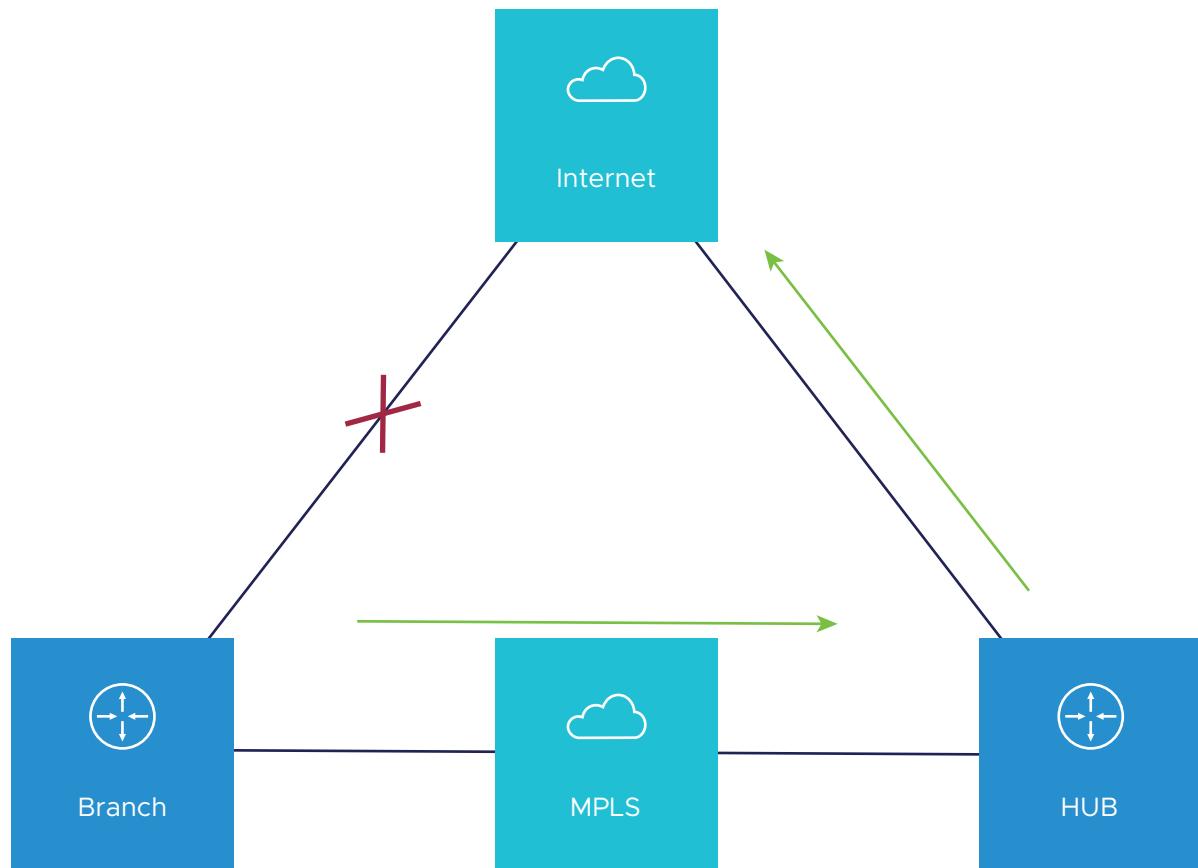
Under normal operations, the Public link is UP and Internet-bound traffic will flow normally either Direct or via SD-WAN Gateway as per the Business Policies configured.



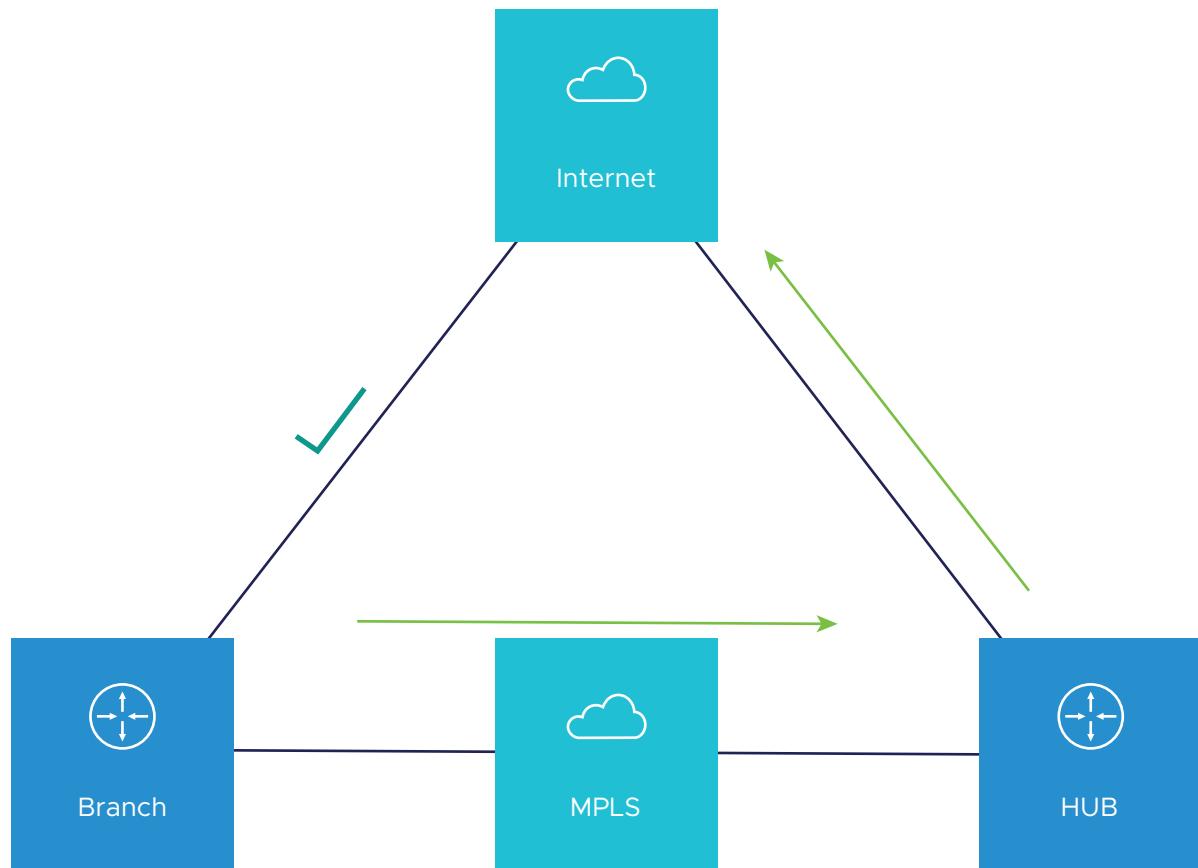
When the Public Internet link goes DOWN, or the SD-WAN Overlay path goes to QUIET state (no packets received from Gateway after 7 heartbeats), the Internet-bound traffic is dynamically backhauled to the Hub.

The Business Policy configured on the Hub will determine how this traffic is forwarded once it reaches the hub. The options are:

- Direct from Hub
- Hub to Gateway and then breakout from the Gateway



When the Public Internet link comes back, CBH will attempt to move the traffic flows back to the Public link. To avoid an unstable link causing traffic to flap between the Public and Private links, CBH has a default 30 seconds holdoff timer. After the holdoff timer is reached, flows will be failed back to the Public Internet link.



#### Use case 2: Cloud Security Service (CSS) Link Failure

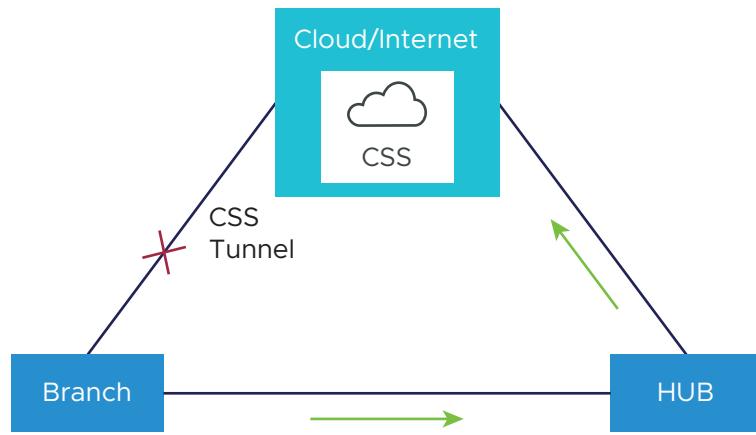
Whenever there is a CSS (Zscaler) link failure on an SD-WAN Edge, while the Public Internet is still up, tunnels to CSS are not established and it causes traffic to get black-holed. In this scenario, the Conditional Backhaul feature, if activated, will allow the business policy to perform conditional backhaul and route the traffic to the Hub.

The Policy-based Conditional Backhaul provides the SD-WAN Edge the ability to failover Internet-bound traffic that use CSS link based on the status of CSS tunnel, irrespective of the status of the public links.

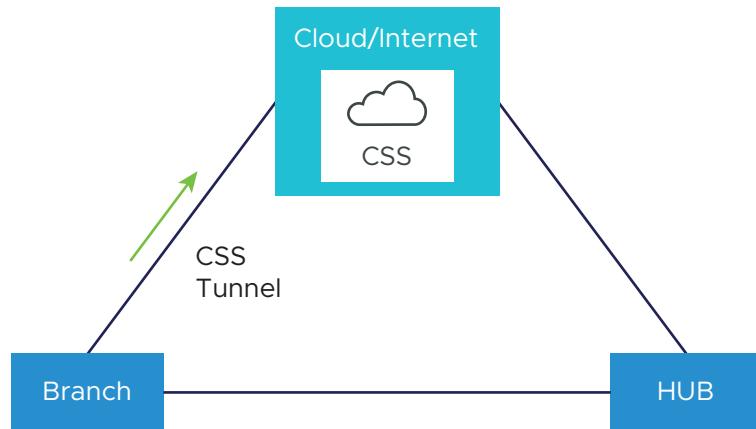
CBH will be effective only if:

- CSS tunnels on all the segment goes down in the VPN profile.
- While primary CSS tunnel goes down and if secondary CSS tunnel is configured then Internet traffic will not be conditional backhauled, instead traffic will go through the secondary CSS tunnel.

When the CSS link goes DOWN and Public Internet link is UP, the Internet-bound traffic that use CSS link is dynamically backhauled to the Hub, irrespective of the status of the public link.



When the tunnels to CSS link come back, CBH will attempt to move the traffic flows back to the CSS and the traffic will not be Conditionally Backhauled.



#### Behavioral Characteristics of Conditional Backhaul

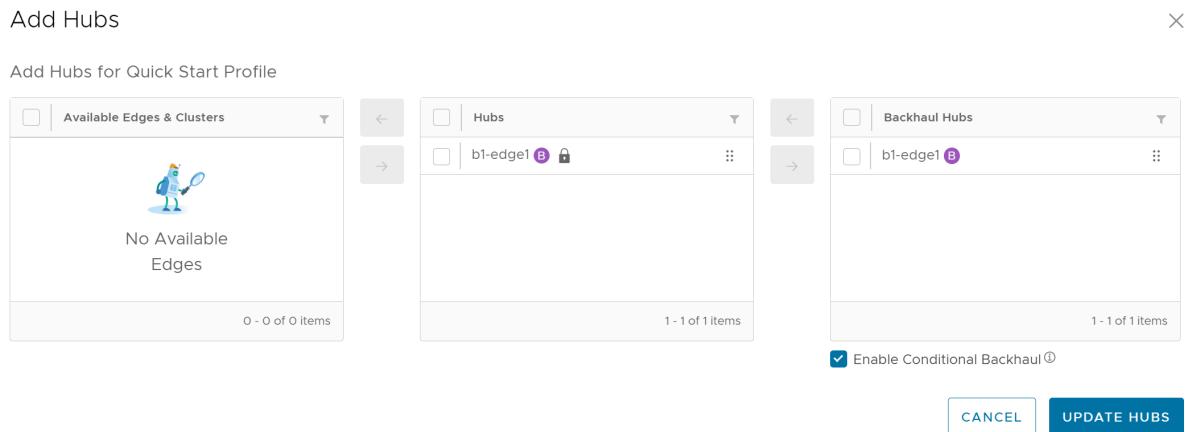
- When Conditional Backhaul is activated, by default all Business Policy rules at the branch level are subject to failover traffic through CBH. You can exclude traffic from Conditional Backhaul based on certain requirements for selected policies by deactivating this feature at the selected business policy level.
- Conditional Backhaul will not affect existing flows that are being backhauled to a Hub already if the Public link(s) goes down. The existing flows will still forward data using the same Hub.
- If a branch location has backup Public links, the backup Public link will take precedence over CBH. Only if the primary and backup links are all inoperable then the CBH gets triggered and uses the Private link.
- If a Private link is acting as backup, traffic will fail over to Private link using CBH feature when active Public link fails and Private backup link becomes Active.

- In order for the feature to work, both Branches and Conditional Backhaul Hubs need to have the same Private Network name assigned to their Private links. (The Private tunnel will not come up otherwise.)

### Configuring Conditional Backhaul

At the Profile level, in order to configure Conditional Backhaul, you should activate **Cloud VPN**, and then establish VPN connection between Branch and SD-WAN Hubs by performing the following steps:

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.
- Select a profile or click the **View** link in the **Device** column. The **Device** settings page for the selected profile appears.
- From the **Segment** drop-down menu, select a profile segment to configure Conditional Backhaul. By default, **Global Segment [Regular]** is selected.
- Go to **VPN Services** area and activate **Cloud VPN** by turning the toggle button to **On**.
- Select the **Enable Branch to Hubs** check box.
- Click the **Edit Hubs** link. The **Add Hubs** window for the selected profile appears.



From **Hubs** area, select the Hubs to act as Backhaul Hubs and move them to **Backhaul Hubs** area by using the arrows.

- To activate Conditional Backhaul, select the **Enable Conditional BackHaul** check box.

With Conditional Backhaul activated, the SD-WAN Edge can failover:

- Internet-bound traffic (Direct Internet traffic, Internet via SD-WAN Gateway and Cloud Security Traffic via IPsec) to MPLS links whenever there is no Public Internet links available.

- Internet-bound CSS traffic to the Hub whenever there is a CSS (Zscaler) link failure on the SD-WAN Edge, while the Public Internet link is still up.

Conditional Backhaul, when activated will apply for all Business Policies by default. If you want to exclude traffic from Conditional Backhaul based on certain requirements, you can deactivate Conditional Backhaul for selected policies to exclude selected traffic (Direct, Multi-Path, and CSS) from this behavior by selecting the **Turn off Conditional Backhaul** check box in the **Action** area of the **Configure Rule** screen for the selected business policy. For more information, see [Configure Network Service for Business Policy Rule](#).

Add Rule X

Rule Name *	NS Rule1
IP Version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> IPv4 and IPv6
<b>Match</b> <b>Action</b>	
Priority	<input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low
Enable Rate Limit	<input type="checkbox"/>
Network Service	Internet Backhaul > Non SD-WAN Destination via Edge / Cloud Security Service <span style="float: right;">▼</span>
Non SD-WAN Destination via Edge / Cloud Security Service	* <input type="text" value="GCS service1"/> <span style="float: right;">▼</span>
Link Steering <span style="float: right;">①</span>	<input type="text" value="Auto"/> <span style="float: right;">▼</span>
Inner Packet DSCP Tag	<input type="text" value="Leave as is"/> <span style="float: right;">▼</span>
Outer Packet DSCP Tag	<input type="text" value="0 - CS0/DF"/> <span style="float: right;">▼</span>
Enable NAT	<input type="checkbox"/> <span style="float: right;">①</span>
Service Class	<input type="radio"/> Realtime <input checked="" type="radio"/> Transactional <input type="radio"/> Bulk
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; font-weight: bold;">CREATE</span>	

### Note

- Conditional Backhaul and SD-WAN Reachability can work together in the same Edge. Both Conditional Backhaul and SD-WAN reachability support failover of Cloud-bound Gateway traffic to MPLS when Public Internet is down on the Edge. If Conditional Backhaul is activated and there is no path to Gateway and there is a path to hub via MPLS then both direct and Gateway bound traffic apply Conditional Backhaul. For more information about SD-WAN reachability, see [SD-WAN Service Reachability via MPLS](#).
- When there are multiple candidate hubs, Conditional Backhaul uses the first hub in the list unless the Hub has lost connectivity to Gateway.

## 8 Click **Save Changes**.

### Troubleshooting Conditional Backhaul

Consider a user with Business Policy rules created at the Branch level. You can check if the constant pings to each of these destination IP addresses are active for the Branch by running the **List Active Flows** command from the **Remote Diagnostics** section.

For more information, see the *Remote Diagnostic Tests on Edges* section in the *VMware SD-WAN Troubleshooting Guide* published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

If extreme packet loss occurs in the Public link of the Branch and the link is down then the same flows toggle to Internet Backhaul at the Branch.

---

**Note** The Business Policy on the Hub determines how the Hub forwards the traffic. As the Hub has no specific rule for these flows, they are categorized as default traffic. For this scenario, a Business Policy rule can be created at the Hub level to match the desired IPs or Subnet ranges to define how flows from a specific Branch are handled in the event when Conditional Backhaul becomes operational.

---

### Configure a Tunnel Between a Branch and a Branch VPN

Configure Branch to Branch VPN to establish a VPN connection between Branches.

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles > Device tab**.
- 2 Go to **VPN Services** area and activate **Cloud VPN** by turning the toggle button to **On**.
- 3 To configure a Branch to Branch VPN, select the **Enable Branch to Branch VPN** check box under **Branch to Branch VPN (Transit & Dynamic)**.

## VPN Services

### Cloud VPN (i)

On

#### Edge to SD-WAN Sites

##### Branch to Hub Site (Permanent VPN)

Enable Branch to Hubs

##### Branch to Branch VPN (Transit & Dynamic)

Enable Branch to Branch VPN

Cloud Gateways

Hubs for VPN

Isolate profile (i)

Enable Dynamic Branch to Branch VPN via:

To All Edges

To Edges Within Profile

#### Edge to Non SD-WAN Sites

Enable Edge to Non SD-WAN via Gateway

- 4 **Branch to Branch VPN** supports following two configurations for establishing a VPN connection between branches:

Configuration	Description
Cloud Gateways	In this option, Edges establish VPN tunnel with the closest Gateway and connections between Edges go through this Gateway. The SD-WAN Gateway may have traffic from other Customers.
Hubs for VPN	In this option, one or more Edges are selected to act as Hubs that can establish VPN connections with Branches. Connections between Branch Edges go through the Hub. The Hub is your only asset which has your corporate data on it, improving overall security.

- 5 To activate profile isolation, select the **Isolate Profile** check box. If selected, the Edges within the Profile do not learn routes from other Edges outside the Profile via the SD-WAN Overlay.
- 6 You can activate **Dynamic Branch To Branch VPN** to all Edges or to Edges within a Profile. By default, it is configured for all Edges.

When you activate **Dynamic Branch to Branch VPN**, the first packet goes through the Cloud Gateway (or the Hub). If the initiating Edge determines that traffic can be routed through a secure overlay multi-path tunnel, and if Dynamic Branch to Branch VPN is activated, then a direct tunnel is created between the Branches.

Once the tunnel is established, traffic begins to flow over the secure overlay multi-path tunnel between the Branches. After 180 seconds of traffic silence (forward or reverse from either side of the Branches), the initiating Edge tears down the tunnel.

---

**Note** To configure **Dynamic Branch To Branch VPN** by Profile, make sure the **Isolate Profile** check box is unselected.

---

- 7 Click **Save Changes**.

### Configure a Tunnel Between a Branch and a Non SD-WAN Destinations via Gateway

You can establish a VPN connection between a branch and a Non SD-WAN Destination through SD-WAN Gateway by activating **Cloud VPN**.

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.
- 2 Select a profile or click the **View** link in the **Device** column.  
The **Device** settings page for the selected profile appears.
- 3 Go to **VPN Services** area and activate **Cloud VPN** by turning the toggle button to **On**.

- 4 To establish a VPN connection between a Branch and Non SD-WAN Destination through SD-WAN Gateway, select the **Enable Edge to Non SD-WAN via Gateway** check box under **Edge to Non SD-WAN Sites**.

VPN Services

Cloud VPN (i)

On (i)

Edge to SD-WAN Sites

Branch to Hub Site (Permanent VPN)

Enable Branch to Hubs

Branch to Branch VPN (Transit & Dynamic)

Enable Branch to Branch VPN

Edge to Non SD-WAN Sites

Enable Edge to Non SD-WAN via Gateway

+ ADD    + NEW DESTINATION    DELETE

<input type="checkbox"/>	Non SD-WAN Destinations via Gateway
<input type="checkbox"/>	test <span style="color: blue;">▼</span>

1 item

- 5 From the drop-down menu, select a Non SD-WAN Destination to establish VPN connection. Click the **Add** button to add additional Non SD-WAN Destinations.
- 6 You can also create VPN connections by clicking the **New Destination** button. The **New Non SD-WAN Destinations via Gateway** dialog appears.

For more information about configuring a Non SD-WAN Destination Network Service through Gateway, see [Configure Non SD-WAN Destinations via Gateway](#).

- 7 Click **Save Changes**.

**Note** Before associating a Non SD-WAN Destination to a Profile, ensure that the Gateway for the Enterprise Data Center is already configured by the Enterprise Data Center Administrator and the Data Center VPN Tunnel is activated.

### Configure a Tunnel Between a Branch and a Non SD-WAN Destinations via Edge

After configuring a Non SD-WAN Destination via Edge in SASE Orchestrator, you have to associate the Non SD-WAN Destination to the desired Profile in order to establish the tunnels between SD-WAN Gateways and the Non SD-WAN Destination.

To establish a VPN connection between a Branch and a Non SD-WAN Destination configured via Edge, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles > Device tab**.
- 2 Go to **VPN Services** area and activate **Cloud VPN** by turning the toggle button to **On**.
- 3 To establish a VPN connection directly from an SD-WAN Edge to a Non SD-WAN Destination (VPN gateway of Cloud provider such as Azure, AWS), select the **Enable Non SD-WAN via Edge** check box under **Non SD-WAN Destinations via Edge** section.

Service		
<input type="checkbox"/>	Name	Automation for all public WAN Links
<input type="checkbox"/>	test123	N/A
<input checked="" type="checkbox"/> Enabled		
1 item		

- 4 From the configured Services drop-down menu, select a Non SD-WAN Destination to establish VPN connection.
- 5 Click the **Add** button to add additional Non SD-WAN Destinations.

**Note** Only one Non SD-WAN Destinations via Edge service is allowed to be activated in at most one Segment. Two Segments cannot have the same Non SD-WAN Destinations via Edge service activated.

For more information about configuring a Non SD-WAN Destination Network Service through Edge, see [Configure Non SD-WAN Destinations via Edge](#).

- 6 To deactivate a particular service, deselect the respective **Enable Service** check box.
- 7 Click **Save Changes**.

**Note** Before associating a Non SD-WAN Destination to a Profile, ensure that the Gateway for the Enterprise Data Center is already configured by the Enterprise Data Center Administrator and the Data Center VPN Tunnel is activated.

## Configure Cloud Security Services for Profiles

Enable Cloud Security Service (CSS) to establish a secured tunnel from an Edge to cloud security service sites. This enables the secured traffic being redirected to third-party cloud security sites. At the Profile level, VMware SD-WAN and Zscaler integration supports automation of IPsec and GRE tunnels.

---

**Note** Only one CSS with GRE is allowed per Profile.

---

Before you begin:

- Ensure that you have access permission to configure network services.
  - Ensure that your SASE Orchestrator has version 3.3.x or above.
  - You should have Cloud security service gateway endpoint IPs and FQDN credentials configured in the third party Cloud security service.
- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
  - 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. The configuration options for the selected Profile are displayed in the **Device** tab.
  - 3 Under the **VPN Services** category, click **Cloud Security Service** and activated **Cloud Security Service** by turning the toggle button to **On**.
  - 4 Configure the following settings:



Option	Description
Cloud Security Service	<p>Select a cloud security service from the drop-down menu to associate with the profile. You can also click <b>New Cloud Security Service</b> from the drop-down to create a new service type. For more information about how to create a new CSS, see <a href="#">Configure a Cloud Security Service</a>.</p> <p><b>Note</b> For cloud security services with Zscaler login URL configured, <b>Login to Zscaler</b> button appears in the <b>Cloud Security Service</b> area. Clicking the <b>Login to Zscaler</b> button will redirect you to the Zscaler Admin portal of the selected Zscaler cloud.</p>
Tunneling Protocol	<p>This option is available only for Zscaler cloud security service provider. If you select a manual Zscaler service provider then choose either IPsec or GRE as the tunneling protocol. By default, IPsec is selected.</p> <p><b>Note</b> If you select an automated Zscaler service provider then the <b>Tunneling Protocol</b> field is not configurable but displays the protocol name used by the service provider.</p>
Hash	Select the Hash function as SHA 1 or SHA 256 from the drop-down. By default, SHA 1 is selected.
Encryption	Select the Encryption algorithm as AES 128 or AES 256 from the drop-down. By default, None is selected.
Key Exchange Protocol	<p>Select the key exchange method as IKEv1 or IKEv2. By default, IKEv2 is selected.</p> <p>This option is not available for Symantec cloud security service.</p>
Login to Zscaler	Click <b>Login to Zscaler</b> to login to the Zscaler Admin portal of the selected Zscaler cloud.

## 5 Click **Save Changes**.

When you enable Cloud Security Service and configure the settings in a profile, the setting is automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge. See [Configure Cloud Security Services for Edges](#).

For the profiles created with cloud security service enabled and configured prior to 3.3.1 release, you can choose to redirect the traffic as follows:

- Redirect only web traffic to Cloud Security Service
- Redirect all Internet bound traffic to Cloud Security Service
- Redirect traffic based on Business Policy Settings – This option is available only from release 3.3.1. If you choose this option, then the other two options are no longer available.

---

**Note** For the new profiles that you create for release 3.3.1 or later, by default, the traffic is redirected as per the Business Policy settings. See [Configure Business Policies with Cloud Security Services](#).

---

## Configure Zscaler Settings for Profiles

Describes how to configure Zscaler for Profiles. You can configure the Zscaler settings for a Profile from the **Zscaler** section available under the **VPN Services** category in the **Device** tab.

Before you configure Zscaler, you must have Zscaler cloud subscription. For steps on how to create cloud subscription of type Zscaler, [Configure API Credentials](#).

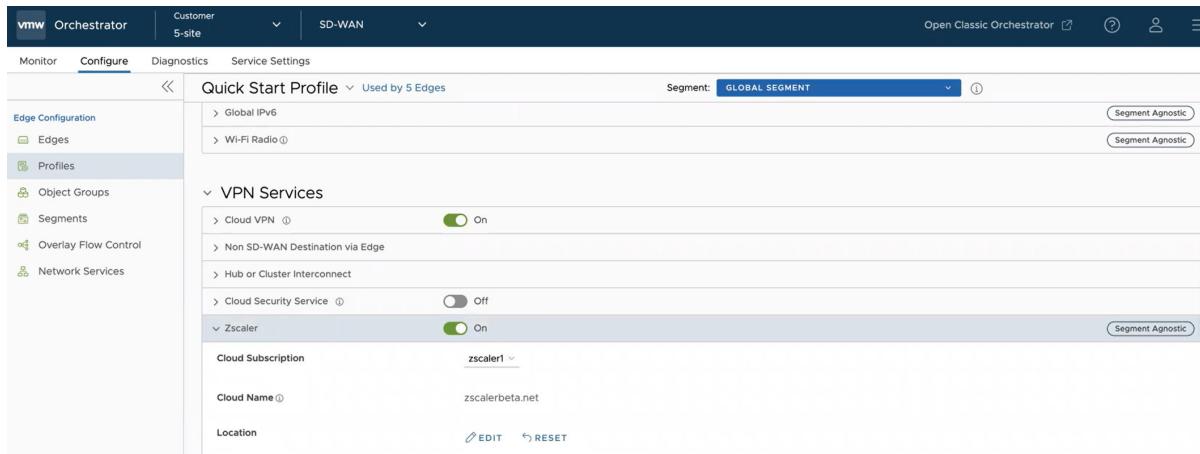
---

**Note** By default, **Zscaler** section is not available in the **Device** page for Profiles. Contact your Operator to get this feature activated at the Profile level.

---

To configure Zscaler at the Profile level, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. The configuration options for the selected Profile are displayed in the **Device** tab.



- 3 Under the **VPN Services** category, click **Zscaler** and activate Zscaler by turning the toggle button to **On**.
- 4 From the **Cloud Subscription** drop-down menu, select your Zscaler subscription.

- 5 The Zscaler Cloud associated with the selected subscription automatically appears in the **Cloud Name** Field.
- 6 To edit location Gateway options, click the **Edit** button. The **Edit Location Gateway Options** dialog box appears.

## Edit Location Gateway Options

### Location

#### Gateway Options

**Use XFF from Client Request**  Off

**Enable Caution**  Off

**Enable AUP**  Off

**Enforce Firewall Control**  Off

**Authentication**  Off

#### Bandwidth Control

**Bandwidth Control**  Off

- 7 Configure the Gateway options and Bandwidth control settings for Location and click **Done**. For more information about Zscaler Gateway Options and Bandwidth Control parameters, see <https://help.zscaler.com/zia/configuring-locations>.
- 8 Click **Reset** to reset Zscaler Location gateway options to default.
- 9 After updating the required settings, click **Save Changes** in the **Device** page.

## Related Topics

- Configure Cloud Security Services for Profiles
- Configure Cloud Security Services for Edges

## Configure Secure Access Service for Profiles

VMware provides an advanced feature called Secure Access Service. SASE Orchestrator allows you to configure the Secure Access Service on the Device Settings page for a Profile. Different services can be applied for different Segments.

### Configure Secure Access Service for a Profile

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 Click the link to a Profile. Alternatively, you can click the **View** link in the **Device** column of the Profile.
- 3 Go to the **VPN Services** section, and then turn on **Secure Access Service**.



- 4 Select a pre-defined service from the drop-down list.
- 5 Click **Save Changes**.

### Prerequisites

To turn on the **Secure Access** feature, an Operator user must navigate to the **Global Settings** service of the Enterprise portal. From the left menu, click **Customer Configuration**, and then on the **Secure Access** card, click **Turn On**. If the **Secure Access** service is deactivated, follow the below steps to activate it before turning it on:

- 1 Click **Go to Gateway Pools** link on the **Secure Access** card. Select a Gateway pool, and then select a Gateway.
- 2 In the **Properties** section, select the **Cloud Web Security** check box.

**Properties**

Name *	gateway-1
Description	Enter Description
Gateway Roles	<input checked="" type="checkbox"/> Data Plane <input checked="" type="checkbox"/> Control Plane <input checked="" type="checkbox"/> Secure VPN Gateway <input type="checkbox"/> Partner Gateway ⓘ <input type="checkbox"/> CDE <input checked="" type="checkbox"/> Cloud Web Security

- 3 In the **Cloud Web Security** section of the screen, enter appropriate details for **Geneve Endpoint IP Address** and **Pop name**.

**Cloud Web Security**

Geneve Endpoint IP Address	67.23.34.54
Pop name	1234

- 4 Click **Save Changes**.  
 5 Go back to the **Global Settings > Customer Configuration** screen, and then turn on the **Secure Access** service.

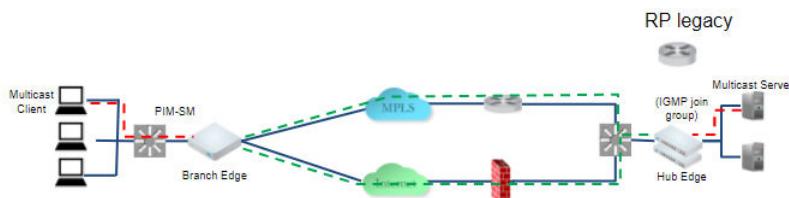
#### What to do next

To configure the Secure Access Service for an Edge, see [Configure Secure Access Service for Edges](#).

## Configure Multicast Settings for Profiles

Multicast provides an efficient way to send data to an interested set of receivers to only one copy of data from the source, by letting the intermediate multicast-routers in the network replicate packets to reach multiple receivers based on a group subscription.

Multicast clients use the Internet Group Management Protocol (IGMP) to propagate membership information from hosts to Multicast activated routers and PIM to propagate group membership information to Multicast servers via Multicast routers.



Multicast support includes:

- Multicast support on both overlay and underlay
- Protocol-Independent Multicast - Sparse Mode (PIM-SM) on SD-WAN Edge
- Internet Group Management Protocol (IGMP) version 2 on SD-WAN Edge
- Static Rendezvous Point (RP) configuration, where RP is activated on a 3rd party router.

You can activate and configure Multicast globally and at the interface-level. If required, you can override the Multicast configurations at the Edge-level.

## Configure Multicast for Profiles

To configure Multicast globally:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. You can also select a Profile and click **Modify** to configure the Profile. The configuration options for the selected Profile are displayed in the **Device** tab.
- 3 Scroll down to the **Routing & NAT** category and expand the **Multicast** area.
- 4 Turn on the toggle button to activate the Multicast feature.

---

**Note** There must be at least one RP group when Multicast is turned on.

---

The RP Selection is set to **Static** by default.

RP Address *	Multicast Group ⓘ	S.No
10.0.3.39	224.0.0.0/8	1

5 Configure the following Multicast settings:

Multicast Setting	Description
RP Selection	<b>Static</b> is the default and supported mechanism.
RP Address	Enter the IP address of the device, which is the route processor for a multicast group.
Multicast Group	Enter a range of IP addresses and port numbers that define a Multicast group. Once the host device has membership to the Multicast group, it can receive any data packets that are sent to the group defined by the IP address and port number.
Enable PIM on Overlay	Activate PIM peering on SD-WAN Overlay. For example when activated on both branch SD-WAN Edge and hub SD-WAN Edge, they form a PIM peer. By default, the source IP address for the overlays is derived from any Switched interfaces (if present), or a Routed interface of type Static with a deactivated WAN Overlay. You can choose to change the source IP by specifying <b>Source IP Address</b> , which will be a virtual address and will be advertised over the overlay automatically.
PIM Timers	<p>Under <b>Advanced Settings</b>, configure the PIM timers details, if needed:</p> <ul style="list-style-type: none"> <li>■ <b>Join Prune Send Interval</b> - The Join Prune Interval Timer. Default value is 60 seconds. The allowable range is 60 through 600.</li> <li>■ <b>Keep Alive Timer</b> - PIM keep alive timer. Default value is 60 seconds. The allowable range is 31 through 60000.</li> </ul>

To configure the multicast settings at the Interface level, see: [Configure Interface Settings for Profiles](#).

## Configure DNS for Profiles

Domain Name System (DNS) is used to configure conditional DNS forwarding through a private DNS service and to specify a public DNS service to be used for querying purpose.

The DNS Service can be used for a public DNS service or a private DNS service provided by your company. A Primary Server and Backup Server can be specified. The public DNS service is preconfigured to use Google and Open DNS servers.

To configure the DNS settings for a Profile:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.
- 2 The **Profiles** page displays the existing Profiles.
- 3 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. You can also select a Profile and click **Modify** to configure the Profile.
- 4 The configuration options for the selected Profile are displayed in the **Device** tab.
- 5 Scroll down to the **Routing & NAT** category and click **DNS**.

**Conditional DNS Forwarding (Private DNS)**

- + NEW PRIVATE DNS
- + ADD
- DELETE

<input type="checkbox"/> Private DNS	
<input type="checkbox"/> acme1	▼
1 item	

**Public DNS**

- + NEW PUBLIC DNS

Public DNS	
ACME	▼
1 item	

**Local DNS Entries**

- + NEW LOCAL DNS ENTRY
- EDIT
- DELETE

Domain Name	IP Addresses
velo.com	10.0.0.1
1 item	

- In the **Conditional DNS Forwarding (Private DNS)** section, select **Private DNS** to forward the DNS requests related to the domain name. Click **Add** to add existing private DNS servers to the drop-down menu. Click **Delete** to remove the selected private DNS server from the list.
- To add a new private DNS, click **New Private DNS**.

## New Private DNS Service

X

DNS Type  Private  Public

Service Name \* acme1

IPv4 Server ⓘ

IPv4 Address 10.10.1.1 (−) (+)  
Example: 10.10.10.10

IPv6 Server ⓘ

IPv6 Address (−) (+)  
Example: 2001:db8:3333:4444:5555:6666:7777:8888

Private Domains

+ ADD DELETE

<input type="checkbox"/> Private Domain	Description
<input type="checkbox"/> www.abc.com	Description

1 item

CANCEL SAVE CHANGES

- Following are the available options:

Option	Description
DNS Type	Displays <b>Private</b> by default. You cannot edit this option.
Service Name	Type the name of the DNS service.
IPv4 Server	Type the IPv4 address for IPv4 Server. Click the plus (+) icon to add more addresses.
IPv6 Server	Type the IPv6 address for IPv6 Server. Click the plus (+) icon to add more addresses.
Private Domains	Click <b>Add</b> , and then type the Private Domain name and description.

- Click **Save Changes**.
- In the **Public DNS** section, select a public DNS service from the drop-down menu to be used for querying the domain names. By default, **Google** and **OpenDNS** servers are pre-configured as public DNS.

- To add a new public DNS, click **New Public DNS**.

**Note** The **Public DNS** service is activated on a VLAN or a routed interface, if **DNS Proxy** is activated on the same VLAN or routed interface.

New Public DNS Service X

DNS Type  Private  Public

Service Name \* ACME

IPv4 Server ⓘ

IPv4 Address 10.10.0.1 (−) (+)  
Example: 10.10.10.10

IPv6 Server ⓘ

IPv6 Address 2001:db8:3333:4444:5555:6666:7777:8888 (−) (+)  
Example: 2001:db8:3333:4444:5555:6666:7777:8888

CANCEL SAVE CHANGES

- Following are the available options:

Option	Description
DNS Type	Displays <b>Public</b> by default. You cannot edit this option.
Service Name	Enter the name of the DNS service.
IPv4 Server	Enter the IPv4 address for IPv4 Server. Click the plus (+) icon to add more addresses.
IPv6 Server	Enter the IPv6 address for IPv6 Server. Click the plus (+) icon to add more addresses.

- Click **Save Changes**.
- In the **Local DNS Entries** section, click **Edit** to edit an existing local DNS entry. Click **Delete** to remove the selected local DNS entry from the list.
- To add a new local DNS entry, click **New Local DNS Entry**.



## New Local DNS Entry

### Server Details

**Domain Name \***      velo.com

### IP Addresses

**+ ADD**

**DELETE**

<input type="checkbox"/>	IP Address
<input type="checkbox"/>	10.0.0.1
1 item	

**CANCEL**

**SAVE CHANGES**

- Following are the available options:

Option	Description
Domain Name	Enter the device domain name.
IP Addresses	Enter either an IPv4 or an IPv6 address.
Add	Click to add multiple IP addresses.  <b>Note</b> A maximum of 10 IP addresses can be added for each domain name.
Delete	Click to delete the selected IP addresses.

- Click **Save Changes**.

- After configuring the **Private DNS**, **Public DNS**, and **Local DNS Entries**, click **Save Changes** in the **Device** page.

## Activate OSPF for Profiles

Open Shortest Path First (OSPF) can be enabled only on a LAN interface as an active or passive interface. The Edge will only advertise the prefix associated with that LAN switch port. To get full OSPF functionality, you must use it in routed interfaces.

OSPF (Open Shortest Path First) is an interior gateway protocol (IGP) that operates within a single autonomous system (AS).

**Note** OSPF is configurable only on the Global Segment.

OSPFv3 is introduced in the 5.2 release and provides support for the following:

- Support for OSPFv3 is introduced in the SD-WAN Edge for IPv6 underlay routing in addition to existing BGPv6 support. The following is supported:
  - Underlay IPv6 route learning.
  - Redistribution of OSPFv3 routes into overlay/BGP and vice-versa.
  - Support for Overlay Flow Control (OFC).
- OSPFv3 is implemented with feature parity to OSPFv2 with the following exceptions:
  - Point to Point (P2P) is not supported.
  - BFDv6 with OSPFv3 is not supported.
  - md5 authentication is not available, as OSPFv3 header does not support it.

This section describes how to configure dynamic routing with OSPFv2 and OSPFv3 along with Route Summarization.

**Note** OSPFv2 supports only IPv4. OSPFv3 supports only IPv6 and is available starting with the 5.2 release.

**Note** Route Summarization is available starting with the 5.2 release.

To activate OSPF, perform the steps in the procedure below:

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise Portal, click the **Configure**.

**Note** Depending upon your login permissions, you might need to select a Customer or Partner first, then click the **Configure** tab as indicated in next step.

- 2 From the left menu, select **Profiles**.

The **Profile** page displays.

- 3 Click a Profile from the list of available Profiles (or Add a Profile if necessary).
- 4 Go to the **Routing & NAT** section in the UI and click the arrow next to OSPF.

- 5 In the **OSPF Areas** section, configure the Redistribution Settings for OSPFv2/v3, BGP Settings, and if applicable, Route Summarization as shown in the image below. See the table below for a description of the options and fields in the below image.

**Note** OSPFv2 supports only IPv4. OSPFv3 supports only IPv6 and is only available in the 5.2 release.

Option	Description
Redistribution Settings	
Default Route	Choose an OSPF route type (O1 or O2) to be used for default route. Default selection for this configuration is "None".
Advertise	Choose either Always or Conditional. (Choosing Always means to Advertise the default route always. Choosing Conditional means to redistribute default route only when Edge learns via overlay or underlay). The "Overlay Prefixes" option must be checked to use the Conditional default route.
Overlay Prefixes	
Overlay Prefixes	If applicable, check the <b>Overlay Prefixes</b> check box.
BGP Settings	
BGP	To enable injection of BGP routes into OSPF, select the BGP check box. BGP routes can be redistributed into OSPF, so if this is applicable, enter or choose the configuration options as follows:
Set Metric	In the Set Metric text box, enter the metric. (This is the metric that OSPF would put in its external LSAs that it generates from the redistributed routes). The default metric is 20.
Set Metric Type	From the Set Metric Type drop-down menu, choose a metric type. (This is either type E1 or E2 (OSPF External-LSA type)); the default type is E2.

- 6 In **OSPF Areas**, click **+Add** and configure the options, as described in the table below. Add additional areas, if necessary, by clicking **+Add**. The fields in the table below cannot be overridden at the Edge level.

Option	Description
Area ID	Click inside the <b>Area ID</b> text box, enter an OSPF area ID.
Name	Click inside the <b>Name</b> text box, enter a descriptive name for your area.
Type	By default, the Normal type is selected. Only Normal type is supported at this time.

- 7 Next, configure the Interface Settings for OSPF. For configuration details, see either [Configure Interface Settings for Profiles](#) or [Configure Interface Settings for Edges](#).

**Note** OSPF has to be activated at the Profile level first before you can configure it on Edge interfaces.

- 8 If applicable, configure Route Summarization.

**Note** The Route Summarization feature is available starting with the 5.2 release, for an overview and use case for this feature, see [Chapter 34 Route Summarization](#). For configuration details, follow the steps below in Step #10.

- 9 Scroll down to the **Route Summarization** area.

- 10 Click **+Add** in the **Route Summarization** area. A new row is added to the **Route Summarization** area.

Configure route summarization, as described in the table below. See image below.

**Route Summarization**

<b>Route Summarization</b>					
<b>+ ADD</b>		<b>DELETE</b>	<b>CLONE</b>		
<input type="checkbox"/>	<b>Subnet *</b>	<b>No Advertise</b>	<b>Tag</b>	<b>Metric Type</b>	<b>Metric</b>
<input type="checkbox"/>	3.5.0.0/16	<input checked="" type="checkbox"/> Yes	1000	E1	20
<input type="checkbox"/>	Enter Subnet	<input type="checkbox"/> Yes	Enter Tag (Optio...)	E1	Enter Metric (Op...
2 items					

Option	Description
Subnet	Enter the IP subnet.
No Advertise	When <b>No Advertise</b> is set, all the external routes (Type-5) that are under this supernet are summarized and have chosen not to advertise it. This means it effectively blocks the whole supernet from advertising to its peer.
Tag	Enter the router Tag value (1-4294967295).

Option	Description
Metric Type	Enter the Metric Type (E1 or E2).
Metric	Enter the advertised metric for this route ((0-16777215)).

- 11 Add additional routes, if necessary, by clicking **+Add**. To Clone or Delete a route summarization, use the appropriate buttons, located next to **+Add**.
- 12 Click **Save Changes**.

## Route Filters

There are two different types of routing: inbound and outbound.

- Inbound routing includes preferences that can be learned or ignored from OSPF and installed into the Overlay Flow Control.
- Outbound Routing indicates what prefixes can be redistributed into the OSPF.

## Configure BFD for Profiles

VMware SD-WAN allows to configure BFD sessions to detect route failures between two connected entities.

To configure a BFD session for Profiles:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**.
- 2 Click the **Device** icon for a profile, or select a profile and click the **Device** tab.

---

**Note** The **Device** tab is normally the default tab.

- 3 In the **Device** tab, scroll down to the **Routing & NAT** section and click the arrow next to the **BDF** area to open it.
- 4 Click the **BDF** slider to **ON** position.

- 5 Configure the following settings, as described in the table below. See image below for example.

Field	Description
Peer Address	Enter the IPv4 address of the remote peer to initiate a BFD session.
Local Address	<p>Enter a locally configured IPv4 address for the peer listener. This address is used to send the packets.</p> <p><b>Note</b> You can click the <b>IPv6</b> tab to configure IPv6 addresses for the remote peer and the peer listener.</p> <p>For IPv6, the local and peer addresses support only the following format:</p> <ul style="list-style-type: none"> <li>■ IPv6 global unicast address (2001:CAFE:0:2::1)</li> <li>■ IPv6 unique local address (FD00::1234:BEFF:ACE:EOA4)</li> </ul>
Multihop	Select the check box to enable multi-hop for the BFD session. While BFD on Edge and Gateway supports directly connected BFD Sessions, you need to configure BFD peers in conjunction with multi-hop BGP neighbors. The multi-hop BFD option supports this requirement.  Multihop must be enabled for the BFD sessions for NSD-BGP-Neighbors.
Detect Multiplier	Enter the detection time multiplier. The remote transmission interval is multiplied by this value to determine the detection timer for connection loss. The range is from 3 to 50 and the default value is 3.
Receive Interval	Enter the minimum time interval, in milliseconds, at which the system can receive the control packets from the BFD peer. The range is from 300 to 60000 milliseconds and the default value is 300 milliseconds.
Transmit Interval	Enter the minimum time interval, in milliseconds, at which the local system can send the BFD control packets. The range is from 300 to 60000 milliseconds and the default value is 300 milliseconds.

- 6 Click the Plus (+) icon to add details of more peers.

**7 Click **Save Changes**.**

	Peer Address	Local Address	Multihop	Timers	Order
<input type="checkbox"/>	172.21.1.1	127.21.1.20	<input checked="" type="checkbox"/> Enabled	Detect Multiplier 3 Receive Interval 300 Transmit Interval 300	1
<input type="checkbox"/>	172.21.4.1	172.21.4.20	<input type="checkbox"/> Enabled	Detect Multiplier 3 Receive Interval 300 Transmit Interval 300	2

## Results

When you configure BFD rules for a profile, the rules are automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge. See [Configure BFD for Edges](#) for more information.

### What to do next

VMware SD-WAN supports configuring BFD for BGP and OSPF.

- To enable BFD for BGP, see [Configure BFD for BGP for Profiles](#).
- To enable BFD for OSPF, see [Configure BFD for OSPF](#).
- To view the BFD sessions, see [Monitor BFD Sessions](#).
- To view the BFD events, see [Monitor BFD Events](#).
- For troubleshooting and debugging BFD, see [Troubleshooting BFD](#).

## LAN-Side NAT Rules at Profile Level

LAN-Side NAT (Network Address Translation) Rules allow you to NAT IP addresses in an unadvertised subnet to IP addresses in an advertised subnet. For both the Profile and Edge levels, within the Device Settings configuration, LAN-side NAT Rules has been introduced for the 3.3.2 release and as an extension, LAN side NAT based on source and destination, same packet source and destination NAT support have been introduced for the 3.4 release.

From the 3.3.2 release, VMware introduced a new LAN-side NAT module to NAT VPN routes on the Edge. The primary use cases are as follows:

- Branch overlapping IP due to M&A (Merger and Acquisitions)

- Hiding the private IP of a branch or data center for security reasons

In the 3.4 release, additional configuration fields are introduced to address additional use cases.

Below is a high-level breakdown of LAN-side NAT support in different releases:

- Source or Destination NAT for all matched subnets, both 1:1 and Many:1 are supported (3.3.2 release)
- Source NAT based on Destination subnet or Destination NAT based on Source subnet, both 1:1 and Many:1 are supported (3.4 release)
- Source NAT and Destination 1:1 NAT on the same packet (3.4 release)

---

#### Note

- LAN-side NAT supports traffic over VCMP tunnel. It does not support underlay traffic.
  - Support for "Many:1" and "1:1" (e.g. /24 to /24) Source and Destination NAT.
  - If multiple rules are configured, only the first matched rule is executed.
  - LAN-side NAT is done before route or flow lookup. To match traffic in the business profile, users must use the NATed IP.
  - By default, NATed IP are not advertised from the Edge. Therefore, make sure to add the Static Route for the NATed IP and advertise to the Overlay.
  - Configurations in 3.3.2 will be carried over, no need to reconfigure upon 3.4 upgrade.
- 

## Procedure

**Note:** If the users want to configure the default rule, “any” they must specify the IP address must be all zeros and the prefix must be zero as well: 0.0.0.0/0.

### To apply LAN-Side NAT Rules at the Profile Level:

- 1 In the **SD-WAN** Service of the Enterprise Portal, go to **Configure > Profiles**.
- 2 Select the appropriate Profile by clicking the check box next to the Profile **Name**.
- 3 If not already selected, click the **Device** tab link.
- 4 Scroll down to the **Routing & NAT**.
- 5 Open the **LAN-Side NAT Rules** area.
- 6 Click **+ADD** to add a NAT Source or Destination.
- 7 In the **LAN-Side NAT Rules** area, complete the following for the NAT Source or Destination section: (See the table below for a description of the fields in the steps below).
  - a Enter an address for the **Inside Address** text box.
  - b Enter an address for the **Outside Address** text box.
  - c Enter the Source Route in the appropriate text box.
  - d Enter the Destination Route in the appropriate text box.

- e Type a description for the rule in the **Description** textbox (optional).

The screenshot shows a table titled "NAT Source or Destination" under the heading "LAN-Side NAT Rules". The table has columns: Type \*, Inside Address \*, Outside Address \*, Source Route, Destination Route, and Description. A single row is present, showing "Source" as the type, "10.0.0.0/24" as the Inside Address, "192.168.0.0/24" as the Outside Address, "N/A" as the Source Route, "192.169.0.0..." as the Destination Route, and "Enter Description (O...)" in the Description field. There are buttons for "+ ADD", "- REMOVE", and "CLONE" at the top of the table.

- 8 In the **LAN-side NAT Rules** area, complete the following for NAT Source and Destination: (See the table below for a description of the fields in the steps below).
- For the **Source** type, enter the **Inside Address** and the **Outside Address** in the appropriate text boxes.
  - For the **Destination** type, enter the **Inside Address** and the **Outside Address** in the appropriate text boxes.
  - Type a description for the rule in the **Description** textbox (optional).

This screenshot shows the same LAN-Side NAT Rules interface as above, but with the columns "Type", "Inside Address \*", "Outside Address \*", "Type", "Inside Address \*", "Outside Address \*", and "Description" explicitly labeled. The single rule entry remains the same: "Source" type, "10.0.0.0/24" Inside, "192.168.0.0/24" Outside, "Destination" Type, "10.0.0.0/23" Inside, "192.169.0.0/24" Outside, and "Enter Descript..." in the Description field.

LAN-side NAT Rule	Type	Description
Type drop-down menu	Select either Source or Destination	Determine whether this NAT rule should be applied on the source or destination IP address of user traffic.
Inside Address text box	IPv4 address/prefix, Prefix must be 1-32	The "inside" or "before NAT" IP address (if prefix is 32) or subnet (if prefix is less than 32).
Outside Address text box	IPv4 address/prefix, Prefix must be 1-32	The "outside" or "after NAT" IP address (if prefix is 32) or subnet (if prefix is less than 32).
Source Route text box	- Optional - IPv4 address/prefix - Prefix must be 1-32 - Default: any	For destination NAT, specify source IP/subnet as match criteria. Only valid if the type is "Destination."

LAN-side NAT Rule	Type	Description
Destination Route text box	<ul style="list-style-type: none"> <li>- Optional</li> <li>- IPv4 address/prefix</li> <li>- Prefix must be 1-32</li> <li>- Default: any</li> </ul>	For source NAT, specify destination IP/subnet as match criteria. Only valid if the type is “Source.”
Description text box	Text	Custom text box to describe the NAT rule.

**Note Important:** If the Inside Prefix is less than the Outside Prefix, support Many:1 NAT in the LAN to WAN direction and 1:1 NAT in the WAN to LAN direction. For example, if the Inside Address = 10.0.5.0/24, Outside Address = 192.168.1.25/32 and type = source, for sessions from LAN to WAN with source IP matching ‘Inside Address,’ 10.0.5.1 will be translated to 192.168.1.25. For sessions from WAN to LAN with destination IP matching ‘Outside Address,’ 192.168.1.25 will be translated to 10.0.5.25. Similarly, if the Inside Prefix is greater than Outside Prefix, support Many:1 NAT in the WAN to LAN direction and 1:1 NAT in the LAN to WAN direction. The NAT'ed IP are not automatically advertised, make sure a static route for the NAT'ed IP should be configured and the next hop should be the LAN next hop IP of the source subnet.

## Configure BGP from Edge to Underlay Neighbors for Profiles

You can configure the BGP per segment at the Profile level as well as at the Edge level. This section provides steps on how to configure BGP with Underlay Neighbors.

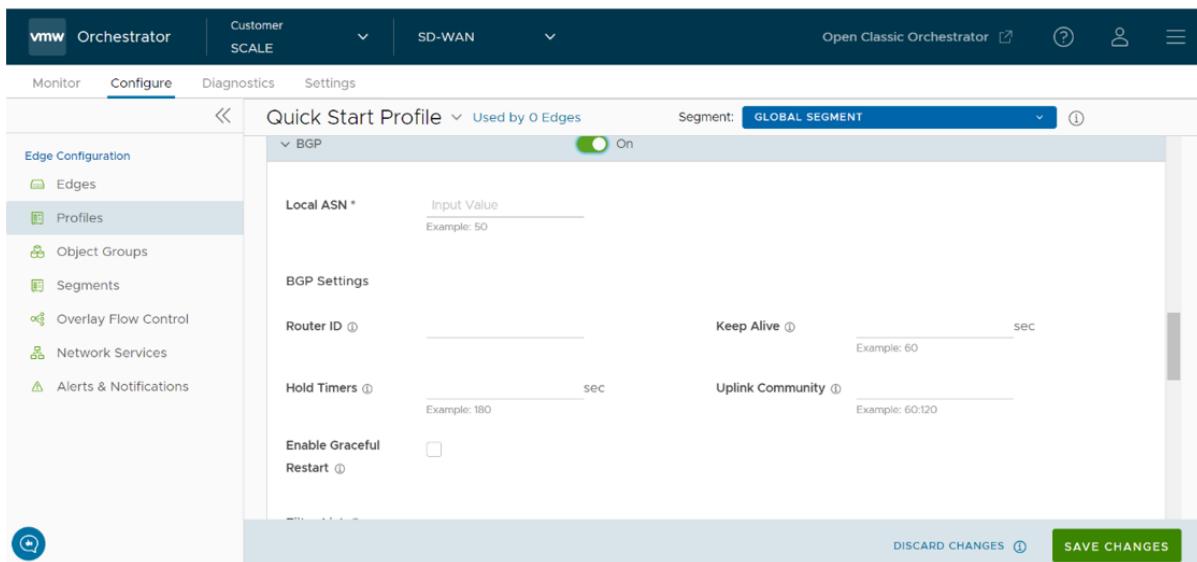
### About this task

VMware supports 4-Byte ASN BGP. See [Configure BGP](#), for more information.

**Note** Route Summarization is new for the 5.2 release. For an overview, use case, and black hole routing details for Route Summarization, see section titled, [Chapter 34 Route Summarization](#). For configuration details, see the steps below.

To configure BGP:

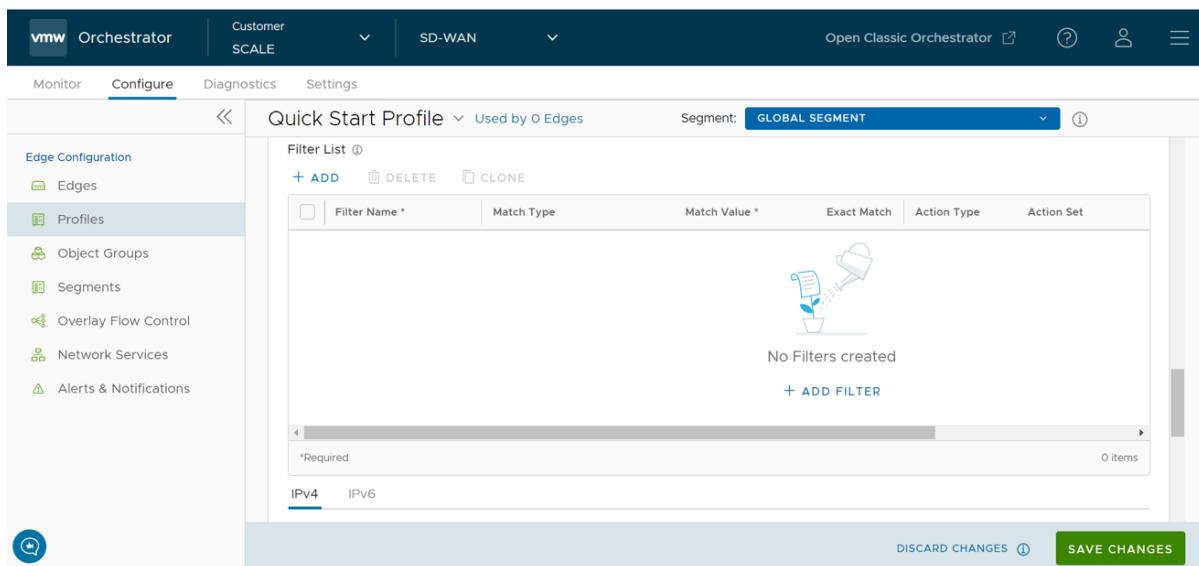
- 1 In the **SD-WAN** service of the Enterprise Portal, click the **Configure** tab.
- 2 From the left menu, select Profiles. The **Profile** page displays.
- 3 Click a Profile from the list of available Profiles (or Add a Profile if necessary).
- 4 Go to the **Routing & NAT** section and click the arrow next to **BGP** to expand.
- 5 In the **BGP** area, toggle the radio button from **Off** to **On**.



- 6 In the **BGP** area, enter the local Autonomous System Number (ASN) number in the appropriate text field.
- 7 Configure the BGP Settings, as described in the table below.

Option	Description
Router ID	Enter the global BGP router ID. If you do not specify any value, the ID is automatically assigned. If you have configured a loopback Interface for the Edge, the IP address of the loopback Interface will be assigned as the router ID.
Keep Alive	Enter the keep alive timer in seconds, which is the duration between the keep alive messages that are sent to the peer. The range is from 0 to 65535 seconds. The default value is 60 seconds.
Hold Timer	Enter the hold timer in seconds. When the keep alive message is not received for the specified time, the peer is considered as down. The range is from 0 to 65535 seconds. The default value is 180 seconds.
Uplink Community	<p>Enter the community string to be treated as uplink routes.</p> <p>Uplink refers to link connected to the Provider Edge(PE). Inbound routes towards the Edge matching the specified community value will be treated as Uplink routes. The Hub/Edge is not considered as the owner for these routes.</p> <p>Enter the value in number format ranging from 1 to 4294967295 or in AA:NN format.</p>
Enable Graceful Restart check box	<p>Please note when selecting this check box:</p> <p>The local router does not support forwarding during the routing plane restart. This feature supports preserving forwarding and routing in case of peer restart.</p>

- 8 Click **+Add** in the **Filter List** area to create one or more filters. These filters are applied to the neighbor to deny or change the attributes of the route. The same filter can be used for multiple neighbors.



- 9 In the appropriate text fields, set the rules for the filter, as described in the table below.

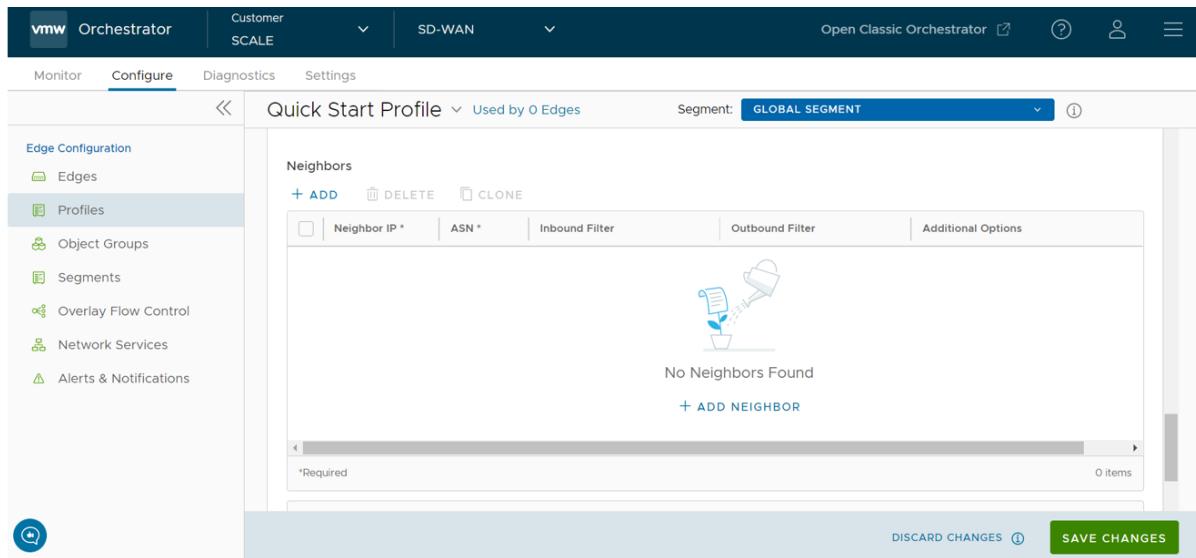
Option	Description
Filter Name	Enter a descriptive name for the BGP filter.
Match Type and Value	Choose the type of the routes to be matched with the filter: <ul style="list-style-type: none"> <li>■ Prefix for IPv4 or IPv6: Choose to match with a prefix for IPv4 or IPv6 address and enter the corresponding prefix IP address in the <b>Value</b> field.</li> <li>■ <b>Community:</b> Choose to match with a community and enter the community string in the <b>Value</b> field.</li> </ul>
Exact Match	The filter action is performed only when the routes match exactly with the specified prefix or community string. By default, this option is enabled.
Action Type	Choose the action to be performed when the routes match with the specified prefix or the community string. You can either permit or deny the traffic.
Action Set	When the BGP routes match the specified criteria, you can set to route the traffic to a network based on the attributes of the path. Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>None:</b> The attributes of the matching routes remain the same.</li> <li>■ <b>Local Preference:</b> The matching traffic is routed to the path with the specified local preference.</li> <li>■ <b>Community:</b> The matching routes are filtered by the specified community string. You can also select the <b>Community Additive</b> check box to enable the additive option, which appends the community value to existing communities.</li> <li>■ <b>Metric:</b> The matching traffic is routed to the path with the specified metric value.</li> </ul>

- 10 Click the plus (+) icon to add more matching rules for the filter. Repeat the procedure to create more BGP filters.

The configured filters are displayed in the **Filter List** area.

**Note** The maximum number of supported BGPv4 Match/Set rules is 512 (256 inbound, 256 outbound). Exceeding 512 total Match/Set rules is not supported and may cause performance issues, resulting in disruptions to the enterprise network.

11 Scroll down to the **Neighbors** area and click **+Add**.



12 Configure the following settings for the IPv4 addressing type, as described in the table below.

Option	Description
Neighbor IP	Enter the IPv4 address of the BGP neighbor
ASN	Enter the ASN of the neighbor
Inbound Filter	Select an Inbound filer from the drop-down list
Outbound Filter	Select an Outbound filer from the drop-down list

Additional Options – Click the view all button to configure the following additional settings:

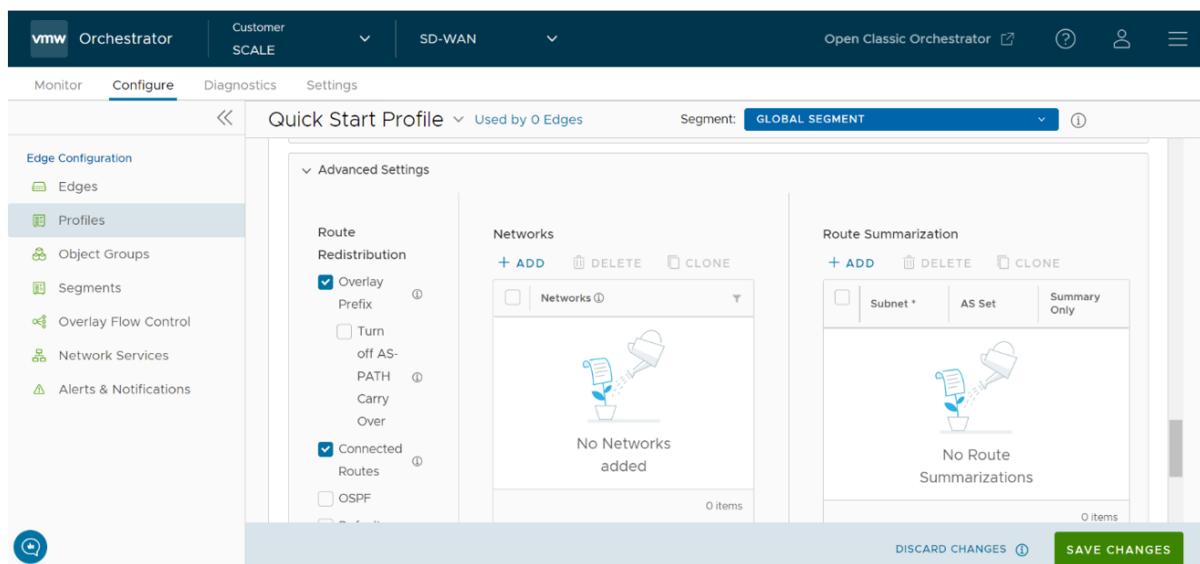
Option	Description
Max-hop	Enter the number of maximum hops to enable multi-hop for the BGP peers. The range is from 1 to 255 and the default value is 1.  <b>Note</b> This field is available only for eBGP neighbors, when the local ASN and the neighboring ASN are different. With iBGP, when both ASNs are the same, multi-hop is inherent by default and this field is not configurable.
Local IP	Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address forth outgoing packets. If you do not enter any value, the IP address of the physical Interface is used as the source IP address.  <b>Note</b> For eBGP, this field is available only when <b>Max- hop</b> count is more than 1. For iBGP, it is always available as iBGP is inherently multi-hop.
Uplink	Used to flag the neighbor type to Uplink. Select this flag option if it is used as the WAN overlay towards MPLS. It will be used as the flag to determine whether the site will become a transit site (e.g. SD-WAN Hub), by propagating routes learnt over a SD-WAN overlay to a WAN link toward MPLS. If you need to make it a transit site, also check "Overlay Prefix Over Uplink" in the Advanced Settings area.

Allow AS	Select the check box to allow the BGP routes to be received and processed even if the Edge detects its own ASN in the AS-Path.
Default Route	The Default Route adds a network statement in the BGP configuration to advertise the default route to the neighbor.
Enable BFD	Enables subscription to existing BFD session for the BGP neighbor.
Keep Alive	Enter the keep alive timer in seconds, which is the duration between the keep alive messages that are sent to the peer. The range is from 0 to 65535 seconds. The default value is 60 seconds.
Hold Timer	Enter the hold timer in seconds. When the keep alive message is not received for the specified time, the peer is considered as down. The range is from 0 to 65535 seconds. The default value is 180 seconds.
Connect	Enter the time interval to try a new TCP connection with the peer if it detects the TCP session is not passive. The default value is 120 seconds.
MD5 Auth	Select the check box to enable BGP MD5 authentication. This option is used in a legacy network or federal network, and it is common that BGP MD5 is used as a security guard for BGP peering.
MD5 Password	<p>Enter a password for MD5 authentication.</p> <p><b>Note</b> Starting from the 4.5 release, the use of the special character "&lt;" in the password is no longer supported. In cases where users have already used "&lt;" in their passwords in previous releases, they must remove it to save any changes on the page.</p>

- 13 Click the Plus (+) icon to add more BGP neighbors.

**Note** Over Multi-hop BGP, the system might learn routes that require recursive lookup. These routes have a next-hop IP which is not in a connected subnet, and do not have a valid exit Interface. In this case, the routes must have the next-hop IP resolved using another route in the routing table that has an exit Interface. When there is traffic for destination that needs these routes to be looked up, routes requiring recursive lookup will get resolved to a connected Next Hop IP address and Interface. Until the recursive resolution happens, the recursive routes point to an intermediate Interface. For more information about Multi-hop BGP Routes, see the "Remote Diagnostic Tests on Edges" section in the *VMware SD-WAN Troubleshooting Guide* published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

- 14 Scroll down to Advanced Settings and click the down arrow to open the Advanced Settings section.



- 15 Configure the following advanced settings, as indicated in the following table, which are globally applied to all the BGP neighbors with IPv4 addresses.

Option	Description
Overlay Prefix	Select the check box to redistribute the prefixes learned from the overlay. For example, when a Spoke is connected to primary and secondary Hub or Hub Cluster, the Spoke's subnets are redistributed by primary and secondary Hub or Hub Cluster to their neighbor with metric (MED) 33 and 34 respectively. You must configure "bgp always-compare-med" in the neighbor router for symmetric routing.  <b>Note</b> Prior to 5.1, the advertised MED values were starting from eight. From release 5.1 and later, the MED values advertised by HUB starts from 33.
Turn off AS-Path carry over	By default, this should be left unchecked. Select the check box to deactivate AS-PATH Carry Over. In certain topologies, deactivating AS-PATH Carry Over will influence the outbound AS-PATH to make the L3 routers prefer a path towards an Edge or a Hub.  <b>Warning:</b> When the AS-PATH Carry Over is deactivated, tune your network to avoid routing loops.
Connected Routes	Select the check box to redistribute all the connected Interface subnets.
OSPF	Select the check box to enable OSPF redistribute into BGP.
Set Metric	When you enable OSPF, enter the BGP metric for the redistributed OSPF routes. The default value is 20.
Default Route	Select the check box to redistribute the default route only when Edge learns the BGP routes through overlay or underlay. When you select the <b>Default Route</b> option, the <b>Advertise</b> option is available as <b>Conditional</b> .
Overlay Prefixes over Uplink	Select the check box to propagate routes learned from overlay to the neighbor with uplink flag.
Networks	Enter the network address in IPv4 format that BGP will be advertising to the peers. Click the plus + icon to add more network addresses.

When you enable the **Default Route** option, the BGP routes are advertised based on the Default Route selection globally and per BGP neighbor, as shown in the following table:

Default Route Selection		
Global	Per BGP Neighbor	Advertising Options
Yes	Yes	The per BGP neighbor configuration overrides the global configuration and hence default route is always advertised to the BGP peer.
Yes	No	BGP redistributes the default route to its neighbor only when the Edge learns an explicit default route through the overlay or underlay network.
No	Yes	Default route is always advertised to the BGP peer.
No	No	The default route is not advertised to the BGP peer.

- 16 Click the **IPv6** tab to configure the BGP settings for IPv6 addresses. Enter a valid IPv6 address of the BGP neighbor in the **Neighbor IP** field. The BGP peer for IPv6 supports the following address format:
  - Global unicast address (2001:CAFE:0:2::1)
  - Unique Local address (FD00::1234:BEFF:ACE:EOA4)
- 17 Configure the other settings as required.

**Note** The Local IP address configuration is not available for IPv6 address type.

- 18 Click **Advanced** to configure the following advanced settings, which are globally applied to all the BGP neighbors with IPv6 addresses.

Option	Description
Connected Routes	Select the check box to redistribute all the connected Interface subnets.
Default Route	Select the check box to redistribute the default route only when Edge learns the BGP routes through overlay or underlay. When you select the <b>Default Route</b> option, the <b>Advertise</b> option is available as <b>Conditional</b> .
Networks	Enter the network address in IPv6 format that BGP will be advertising to the peers. Click the Plus (+) icon to add more network addresses.

## Route Summarization

The Route Summarization feature is available in the 5.2 release, for an overview and use case of this functionality, see [Chapter 34 Route Summarization](#). For configuration details, follow the steps below.

- 19 Click **+Add** in the **Route Summarization** area. A new row is added to the Route Summarization area. See image below.

	Subnet *	AS Set	Summary Only
<input type="checkbox"/>	10.0.0...	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/>
1 item			

**DISCARD CHANGES** ⓘ   **SAVE CHANGES**

- 20 Under the **Subnet** column, enter the network range that you want to summarize in the A.B.C.D/M format and the IP subnet.
  - 21 Under the **AS Set** column, click the **Yes** check box if applicable.
  - 22 Under the **Summary Only** column, click the **Yes** check box to allow only the summarized route to be sent.
  - 23 Add additional routes, if necessary, by clicking **+Add**. To Clone or Delete a route summarization, use the appropriate buttons, located next to **+Add**.
- The BGP Settings section displays the BGP configuration settings.
- 24 Click **Save Changes** when complete to save the configuration.

---

**Note** When you configure BGP settings for a profile, the configuration settings are automatically applied to the SD-WAN Edges that are associated with the profile.

---

You can also configure BGP for Non SD-WAN Destination Neighbors in an Edge. For more information, see [Configure BGP Over IPsec from Edge to Non SD-WAN Neighbors](#).

## Configure Visibility Mode for Profiles

This section describes how to configure Visibility mode at the Profile level.

### About Visibility Mode

Even though tracking by MAC Address is ideal (providing a global unique identifier), there's a lack of visibility when an L3 switch is located between the client and the Edge because the switch MAC is known to the Edge, not the device MAC. Therefore, two tracking modes (MAC Address and now IP Address) are available. When tracking by MAC address is not possible, IP address will be used instead.

- 1 To choose a **Visibility Mode** in the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**. The **Profiles** page displays the existing Profiles., go to **Configure > Profiles**.
- 2 Click the link to the Profile or click the **View** link in the **Device** column of the Profile. The configuration options are displayed in the **Device** tab.



- 3 Under **Telemetry**, go to the **Visibility Mode** area and select one of the following:
  - **Visibility by MAC address**
  - **Visibility by IP address**
- 4 Click **Save Changes**.

### Considerations for Using Visibility Mode

Note the following when choosing a Visibility mode:

- If **Visibility by MAC address** is selected:
  - Clients are behind L2 SW
  - Client MAC, IP and Hostname (if applicable) will appear
  - Stats are collected based on MAC
- If **Visibility by IP address** is selected:
  - Clients are behind L3 SW
  - SW MAC, Client IP and Hostname (if applicable) will appear
  - Stats are collected based on IP

---

**Note** Changes to Visibility mode are non-disruptive.

---

## Configure SNMP Settings for Profiles

Simple Network Management Protocol (SNMP) is a commonly used protocol for network monitoring and Management Information Base (MIB) is a database associated with SNMP to manage entities. In the SASE Orchestrator, you can activate SNMP by selecting the desired SNMP version.

### Prerequisites

Follow the below steps to download the SD-WAN Edge MIB:

- In the **SD-WAN** service of the Enterprise portal, go to **Diagnostics > Remote Diagnostics**.
- Click the link to the required Edge, and then go to the **MIBs for Edge** area. Select **VELOCLOUD-EDGE-MIB** from the drop-down menu, and then click **Run**.
- Copy and paste the results onto your local machine.
- Install all MIBs required by VELOCLOUD-EDGE-MIB on the client host, including SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, IF-MIB, UUID-TC-MIB, and VELOCLOUD-MIB. All these MIBs are available on the **Remote Diagnostics** page.

### Supported MIBs

- SNMP MIB-2 System
- SNMP MIB-2 Interfaces
- VELOCLOUD-EDGE-MIB

### Procedure to Configure SNMP Settings at Profile Level:

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.
- 2 Select a profile for which you want to configure the SNMP settings, and then click the **View** link under the **Device** column.
- 3 Scroll down to the **Telemetry** area, and then expand **SNMP**.

- 4 You can select either **Enable Version 2c** or **Enable Version 3**, or both SNMP version check boxes.

The screenshot shows the SNMP configuration interface. At the top, there's a header with a dropdown for 'SNMP', a checked 'Override' checkbox, and a 'Segment Agnostic' button. Below the header, the 'SNMP Versions' section has a 'Port \*' field set to '161' and a checked 'Enable Version 2c' checkbox. The 'Community' section contains a table with two entries: 'test' and 'velocloud'. A note below says '2 \* Required' and '2 items'. Below the community table are two checkboxes: 'Allow Any IPs' (checked) and 'Enable Version 3' (checked). Further down is another table for 'Authentication' with one entry 'admin'. A note at the bottom right says '1 item'.

- 5 Select **Enable Version 2c** check box to configure the following fields:

Option	Description
Port	Type the port number in the textbox. The default value is <b>161</b> .
Community	Click <b>Add</b> to add any number of communities. Type a word or sequence of numbers as a password, to allow you to access the SNMP agent. The password may include alphabet A-Z, a-z, numbers 0-9, and special characters (e.g. &, \$, #, %).  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Allow Any IPs	You can delete or clone a selected community.  Select this check box to allow any IP address to access the SNMP agent. To restrict access to the SNMP agent, deselect the check box, and then add the IP address(es) that must have access to the SNMP agent. You can delete or clone a selected IP address.

- 6 Selecting the **Enable Version 3** check box provides additional security. Click **Add** to configure the following fields:

Option	Description
Name	Type an appropriate username.
Enable Authentication	Select this check box to add extra security to the packet transfer.
Authentication Algorithm	Select an algorithm from the drop-down menu: <ul style="list-style-type: none"> <li>■ MD5</li> <li>■ SHA1</li> <li>■ SHA2</li> </ul> <p><b>Note</b> This option is available only for the SNMP version 5.8 or above.</p>
	<b>Note</b> This field is available only when the <b>Enable Authentication</b> check box is selected.
Password	Type an appropriate password. Ensure that the Privacy Password is same as the Authentication Password configured on the Edge.
	<b>Note</b> <ul style="list-style-type: none"> <li>■ This field is available only when the <b>Enable Authentication</b> check box is selected.</li> <li>■ Starting from the 4.5 release, the use of the special character "&lt;" in the password is no longer supported. In cases where users have already used "&lt;" in their passwords in previous releases, they must remove it to save any changes on the page.</li> </ul>
Enable Privacy	Select this check box to encrypt the packet transfer.
Algorithm	Choose a privacy algorithm from the drop-down menu: <ul style="list-style-type: none"> <li>■ DES</li> <li>■ AES</li> </ul> <p><b>Note</b> Algorithm <b>AES</b> indicates <b>AES-128</b>.</p>
	<b>Note</b> This field is available only when the <b>Enable Privacy</b> check box is selected.

**Note** You can delete or clone the selected entry.

#### What to do next

Configure **Firewall** settings by following the below steps:

- 1 Navigate to **Configure > Profiles**, and then select a Profile.
- 2 Click the **View** link in the **Firewall** column.
- 3 Go to **Edge Access** located under the **Edge Security** area.

- 4 Configure **SNMP Access** and click **Save Changes**.

**Note** SNMP interface monitoring is supported on DPDK enabled interfaces for 3.3.0 and later releases.

## Configure Syslog Settings for Profiles

In an Enterprise network, SASE Orchestrator supports collection of SASE Orchestrator bound events and firewall logs originating from enterprise SD-WAN Edge to one or more centralized remote Syslog collectors (Servers), in the native Syslog format. For the Syslog collector to receive SASE Orchestrator bound events and firewall logs from the configured edges in an Enterprise, at the profile level, configure Syslog collector details per segment in the SASE Orchestrator by performing the steps on this procedure.

### Prerequisites

- Ensure that Cloud Virtual Private Network (branch-to-branch VPN settings) is configured for the SD-WAN Edge (from where the SASE Orchestrator bound events are originating) to establish a path between the SD-WAN Edge and the Syslog collectors. For more information, see [Configure Cloud VPN for Profiles](#).

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 To configure a Profile, click the link to the Profile or click the **View** link in the **Device** column of the Profile. The configuration options are displayed in the **Device** tab.
- 3 From the **Configure Segment** drop-down menu, select a profile segment to configure Syslog settings. By default, **Global Segment [Regular]** is selected.

**4** Under **Telemetry**, go to the **Syslog** area and configure the following details.

IP *	Protocol *	Port *	Source Interface *	Roles *	Syslog Level *	Tag	All Segments
10.0.0.5	TCP	514	Auto	Edge and Firewall Event	Error	Enter tag (Optional)	<input type="checkbox"/> Yes
10.0.0.0	TCP	514	Auto	Edge Event	Error	Enter tag (Optional)	<input checked="" type="checkbox"/> Yes

Facility: local0

Enable Syslog:

Note: Firewall logs are forwarded at Info level by default

- a From the **Facility** drop-down menu, select a Syslog standard value that maps to how your Syslog server uses the facility field to manage messages for all the events from SD-WAN Edge. The allowed values are from **local0** through **local7**.

**Note** The **Facility** field is configurable only for the **Global Segment**, irrespective of the Syslog settings for the profile. The other segments will inherit the facility code value from the Global segment.

- b Select the **Enable Syslog** checkbox.
- c Click the **+ ADD** button and configure the following details:

Field	Description
IP	Enter the destination IP address of the Syslog collector.
Protocol	Select either <b>TCP</b> or <b>UDP</b> as the Syslog protocol from the drop-down menu.
Port	Enter the port number of the Syslog collector. The default value is 514.
Source Interface	As Edge interfaces are not available at the Profile level, the <b>Source Interface</b> field is set to <b>Auto</b> . The Edge automatically selects an interface with 'Advertise' field set as the source interface.
Roles	Select one of the following: <ul style="list-style-type: none"> <li>■ <b>EDGE EVENT</b></li> <li>■ <b>FIREWALL EVENT</b></li> <li>■ <b>EDGE AND FIREWALL EVENT</b></li> </ul>
Syslog Level	Select the Syslog severity level that need to be configured. For example, If <b>CRITICAL</b> is configured, the SD-WAN Edge will send all the events which are set as either critical or alert or emergency. <p><b>Note</b> By default, firewall event logs are forwarded with Syslog severity level <b>INFO</b>.</p> <p>The allowed Syslog severity levels are:</p> <ul style="list-style-type: none"> <li>■ <b>EMERGENCY</b></li> <li>■ <b>ALERT</b></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ CRITICAL</li> <li>■ ERROR</li> <li>■ WARNING</li> <li>■ NOTICE</li> <li>■ INFO</li> <li>■ DEBUG</li> </ul>
Tag	Optionally, enter a tag for the syslog. The Syslog tag can be used to differentiate the various types of events at the Syslog Collector. The maximum allowed character length is 32, delimited by period.
All Segments	<p>When configuring a Syslog collector with <b>FIREWALL EVENT</b> or <b>EDGE AND FIREWALL EVENT</b> role, select the <b>All Segments</b> checkbox if want the Syslog collector to receive firewall logs from all the segments. If the checkbox is not selected, the Syslog collector will receive firewall logs only from that particular Segment in which the collector is configured.</p> <p><b>Note</b> When the role is <b>EDGE EVENT</b>, the Syslog collector configured in any segment will receive Edge event logs by default.</p>

- 5 Click the **+ ADD** button to add another Syslog collector or else click **Save Changes**. The remote syslog collector is configured in SASE Orchestrator.

**Note** You can configure a maximum of two Syslog collectors per segment and 10 Syslog collectors per Edge. When the number of configured collectors reaches the maximum allowable limit, the **+** button will be deactivated.

**Note** Based on the selected role, the edge will export the corresponding logs in the specified severity level to the remote syslog collector. If you want the SASE Orchestrator auto-generated local events to be received at the Syslog collector, you must configure Syslog at the SASE Orchestrator level by using the `log.syslog.backend` and `log.syslog.upload` system properties.

To understand the format of a Syslog message for Firewall logs, see [Syslog Message Format for Firewall Logs](#).

#### What to do next

SASE Orchestrator allows you to activate Syslog Forwarding feature at the profile and the Edge level. On the **Firewall** page of the Profile configuration, activate the **Syslog Forwarding** button if you want to forward firewall logs originating from enterprise SD-WAN Edge to configured Syslog collectors.

**Note** By default, the **Syslog Forwarding** button is available on the **Firewall** page of the Profile or Edge configuration, and is deactivated.

For more information about Firewall settings at the profile level, see [Configure Profile Firewall](#).

#### Secure Syslog Forwarding Support

The 5.0 release supports secure syslog forwarding capability. Ensuring security of syslog forwarding is required for federal certifications and is necessary to meet the Edge hardening requirements of large enterprises. The secure syslog forwarding process begins with having a TLS capable syslog server. Currently, the SASE Orchestrator allows forwarding logs to a syslog server that has TLS support. The 5.0 release allows the SASE Orchestrator to control the syslog forwarding and conducts default security checking such as hierarchical PKI verification, CRL validation, etc. Moreover, it also allows customizing the security of forwarding by defining supported cipher suites, not allowing self-signed certificates, etc.

Another aspect of secure syslog forwarding is how revocation information is collected or integrated. The SASE Orchestrator can now allow revocation information input from an Operator that can be fetched manually or via an external process. The SASE Orchestrator will pick up that CRL information and will use it to verify the security of forwarding before all connections are established. In addition, the SASE Orchestrator fetches that CRL information regularly and uses it when validating the connection.

## System Properties

Secure syslog forwarding begins with configuring the SASE Orchestrator syslog forwarding parameters to allow it to connect with a syslog server. To do so, the SASE Orchestrator accepts a JSON formatted string to accomplish the following configuration parameters, which is configured in System Properties.

The following system properties can be configured, as shown in the list below and the image below:

- log.syslog.backend: Backend service syslog integration configuration
- log.syslog.portal: Portal service syslog integration configuration
- log.syslog.upload: Upload service syslog integration configuration

Name	Value	Description	Last Modified
log.syslog.portal	{"enable":false,"options":["appNa..."]}	portal service syslog integration c...	
log.syslog.upload	{"enable":false,"options":["appNa..."]}	upload service syslog integration c...	
log.syslog.backend	{"enable":false,"options":["appNa..."]}	backend service syslog integration...	

When configuring system properties, the following Secure Syslog Configuration JSON string can be used.

- config <Object>
  - enable: <true> <false> Activate or Deactivate Syslog forwarding. Please note that this parameter controls overall syslog forwarding even if secure forwarding is activated.
  - options <Object>
    - host: <string> The host running syslog, defaults to localhost.

- port: <number> The port on the host that syslog is running on, defaults to syslogd's default port.
- protocol: <string> tcp4, udp4, tls4. Note: (tls4 allows secure syslog forwarding with default settings. To configure it please see the following secure Options object)
- pid: <number> PID of the process that log messages are coming from (Default: process.pid).
- localhost: <string> Host to indicate that log messages are coming from (Default: localhost).
- app\_name: <string> The name of the application (node-portal, node-backend, etc) (Default: process.title).
- secureOptions <Object>
  - disableServerIdentityCheck: <boolean> Optionally skipping SAN check while validating, i.e. can be used if the server's certification does not have a SAN for self-signed certificates. Default `false`.
  - fetchCRLEnabled: <boolean> If not `false`, SASE Orchestrator fetches CRL information which is embedded into provided CAs. Default: `true`
  - rejectUnauthorized: <boolean> If not `false`, the SASE Orchestrator applies hierarchical PKI validation against the list of supplied CAs. Default: `true`. (This is mostly required for testing purposes. Please do not use it in production.)
  - caCertificate: <string> SASE Orchestrator can accept a string that contain PEM formatted certificates to optionally override the trusted CA certificates (can contain multiple CRLs in openssl friendly concatenated form). Default is to trust the well-known CAs curated by Mozilla. This option can be used for allowing to accept a local CA that is governed by the entity. For instance, for On-prem customers who have their own CAs and PKIs.
  - crlPem:<string> SASE Orchestrator can accept a string that contain PEM formatted CRLs (can contain multiple CRLs in openssl friendly concatenated form). This option can be used for allowing to accept a local kept CRLs. If `fetchCRLEnabled` is set true, the SASE Orchestrator combines this information with fetched CRLs. This is mostly required for a specific scenario where certificates do not have CRLDistribution point information in it.
  - crlDistributionPoints: <Array> The SASE Orchestrator can optionally accept an array CRL distribution points URI in "http" protocol. The SASE Orchestrator does not accept any "https" URI
  - crlPollIntervalMinutes: <number> if `fetchCRLEnabled` is not set false, the SASE Orchestrator polls CRLs every 12 hours. However, this parameter can optionally override this default behavior and update CRL according to provided number.

## Configuring Secure Syslog Forwarding Example

The SASE Orchestrator has the following system property options to arrange described parameters to allow secure syslog forwarding.

---

**Note** The example below should be modified according the trust of chain structure.

---

```
{"enable": true,"options": {"appName": "node-portal","protocol": "tls","port": 8000,"host": "host.docker.internal","localhost": "localhost"},"secureOptions": {"caCertificate": "-----BEGIN CERTIFICATE-----MIID6TCCAtGgAwIBAgIUaauyk0AJ1ZK/U1OOXI0GPGXxahQwDQYJKoZIhvcNAQELBQAwYDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMQ8wDQYDVQQHDAZ2bXdhcmUxDzANBgNVBAoMBnZtd2FyZTEPMA0GA1UECwwGdm13YXJIMREwDwYDVQQDDAhyb290Q2VydDAgFwOyMTA5MjgxOTMzMjVaGA8yMDczMTAwNTE5MzMyNVowYDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMQ8wDQYDVQQHDAZ2bXdhcmUxDzANBgNVBAoMBnZtd2FyZTEPMA0GA1UECwwGdm13YXJIMREwDwYDVQQDDAhyb290Q2VydCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMwG+Xyp5wnoTDxpRRUmE63DUnaJcAIMVABm0xKoBEbOKoW0rn13nFu3l0u6FZzfq+HBjwnOtrBO0lf/sge2/QeUduCeBC/bqs5VzIRQdNaFXVtundWU+7Tn0ZDKXv4aRC0vsvejUOH7DCXLg4yGF4KbM6f0gVBgj4iFyljcy4+aMsVYufDV518RRB3M1HuLdyQXle253fVSBHA5NCn9NGEF1e6Nxt3hbzy3Xe4TwGDQfpXx7sRt9tNbnxemJ8A2ou8XzxHPc44G4O0eN/DGIwkP1GZpKcihFFMMxMlzAvotNqE25gxN/O04/JP7jfQDhqKrLKwmnAmgH9SqvV0F8CAwEAAaOBmDCBITAdBgNVHQ4EFgQUSpavxf80w/I3bdLzubsFZnwzpcMwHwYDVROjBBgwFoAUSpavxf80w/I3bdLzubsFZnwzpcMwDwYDVROTAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYwMgYDVROfBCswKTAnoCWgl4YhaHR0cDovL2xvY2FsaG9zdDo1NDgzL2NybfJvb3QuCVtMAOGCSqGSIb3DQEBCwUAA4IBAQBrYkmg+4x2FrC4W8eU0S62DVrsCtA26wKTVDtor8QAvi2sPGKNlv1nu3F2AOTBXIY+9QV/Zvg9oKunRy917BEVx8sBuwrHW9lvbThVk+NtT/5fxFQwCjO9I7/DiEkCRTsrY4WEy8AW1CcABwEscFXXgliwWLYMpkFxsNBTrUIUfpIRoWiogdtc+ccYWDSSPomWZHUmhumWlikLue9/sOvV9eWy56fZnQNBrOf5wUs0suJyLhi0hhFOAMdEJuL4WnYthX5d+ifNon8yIXGO6cOzXoAODlvSmAS+NOEekFo6R1Arrws0/nk6otGH/Be5+/WXFmpOnzT5cwnspbpA1seO----ENDCERTIFICATE----","disableServerIdentityCheck": true,"fetchCRLEnabled":true,"rejectUnauthorized": true,"crlDistributionPoints": "http://cacerts.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crt
```

To configure syslog forwarding, see the following JSON object as an example (image below).

## Modify System Property

**Name \*** log.syslog.portal

**Data Type** JSON

**Value**

```
{
  "enable": false,
  "options": {
    "appName": "node-portal",
    "protocol": "udp4",
    "port": 514,
    "host": "localhost",
    "localhost": "localhost"
  }
}
```

**Value is Password**  Yes  No

**Value is Read-only**  Yes  No

**Description**

portal service syslog integration configuration

If the configuration is successful, the SASE Orchestrator produces the following log and begins forwarding.

[portal:watch] 2021-10-19T20:08:47.150Z - info: [process.logger.163467409.0] [660] Remote Log has been successfully configured for the following options {"appName":"node-portal","protocol":"tls","port":8000,"host":"host.docker.internal","localhost":"localhost"}

### Secure Syslog Forwarding in FIPS Mode

When FIPS mode is activated for secure syslog forwarding, the connection will be rejected if the syslog server does not offer the following cipher suites: "TLS\_AES\_256\_GCM\_SHA384:TLS\_AES\_128\_GCM\_SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256." Also, independent from FIPS mode, if the syslog server certificate does not have an extended key usage field that sets "ServerAuth" attribute, the connection will be rejected.

### Constant CRL Information Fetching

If `fetchCRLEnabled` is not set to false, the SASE Orchestrator regularly updates the CRL information every 12 hours via the backend job mechanism. The fetched CRL information is stored in the corresponding system property titled, `log.syslog.lastFetchedCRL.{serverName}`. This CRL information is going to be checked in every connection attempt to the syslog server. If an error occurs during the fetching, the SASE Orchestrator generates an Operator event.

If the `fetchCRLEnabled` is set to true, there will be three additional system properties to follow the status of the CRL, as follows: `log.syslog.lastFetchedCRL.backend`, `log.syslog.lastFetchedCRL.portal`, `log.syslog.lastFetchedCRL.upload`, as shown in the image below. This information will display the last update time of the CRL and CRL information.

System Properties			
<input type="text" value="lastfetched"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">X</span> <span style="border: 1px solid #ccc; border-radius: 50%; width: 1em; height: 1em; display: inline-block;"></span> <span style="font-size: small;">▼</span>			
	<a href="#">+ NEW</a>	<a href="#"></a> EDIT	<a href="#"></a> DELETE
<input type="checkbox"/>	Name	Value	Description
<input type="checkbox"/>	<code>log.syslog.lastFetchedCRL.portal</code>	{""}	keeps the last updated CRL as PE...
<input type="checkbox"/>	<code>log.syslog.lastFetchedCRL.upload</code>	{""}	keeps the last updated CRL as PE...
<input type="checkbox"/>	<code>log.syslog.lastFetchedCRL.backend</code>	{""}	keeps the last updated CRL as PE...

## Logging

If the option "fetchCRLEnabled" is set true, the SASE Orchestrator will try to fetch CRLs. If an error occurs, the SASE Orchestrator raises an event and displays in the Operator Events page.

## Syslog Message Format for Firewall Logs

Describes the Syslog message format for Firewall logs with an example.

### Example: IETF Syslog Message Format (RFC 3164)

```
<%PRI%>%timegenerated% %HOSTNAME% %syslogtag%%msg
```

The following is a sample syslog message.

```
<158>Dec 17 07:21:16 b1-edge1 velocloud.sdwan: ACTION=VCF Deny SEGMENT=0 IN="IFNAME"
PROTO=ICMP SRC=x.x.x.x DST=x.x.x.x TYPE=8 FW_POLICY_NAME=test SEGMENT_NAME=Global Segment
```

The message has the following parts:

- Priority - Facility \* 8 + Severity (local3 & info) - 158
- Date - Dec 17
- Time - 07:21:16
- Host Name - b1-edge1
- Syslog Tag - velocloud.sdwan

- Message - ACTION=VCF Deny SEGMENT=0 IN="IFNAME" PROTO=ICMP SRC=x.x.x.x DST=x.x.x.x TYPE=8 FW\_POLICY\_NAME=test SEGMENT\_NAME=Global Segment

VMware supports the following Firewall log messages:

- With Stateful Firewall enabled:
  - Open - The traffic flow session has started.
  - Close - The traffic flow session has ended due to session timeout or the session is flushed through the Orchestrator.
  - Deny - If the session matches the Deny rule, the Deny log message will appear and the packet will be dropped. In the case TCP, Reset will be sent to the Source.
  - Update - For all the ongoing sessions, the Update log message will appear if the firewall rule is either added or modified through Orchestrator.
- With Stateful Firewall deactivated:
  - Allow
  - Deny

**Table 20-2. Firewall Log Message Fields**

Field	Description
SID	The unique identification number applied to each session.
SVLAN	The VLAN ID of the Source device.
DVLAN	The VLAN ID of the Destination device.
IN	The name of the interface on which the first packet of the session was received. In the case of overlay received packets, this field will contain <b>VPN</b> . For any other packets (received through underlay), this field will display the name of the interface in the edge.
PROTO	The type of IP protocol used by the session. The possible values are TCP, UDP, GRE, ESP, and ICMP.
SRC	The source IP address of the session in dotted decimal notation.
DST	The destination IP address of the session in dotted decimal notation.

**Table 20-2. Firewall Log Message Fields (continued)**

Field	Description
Type	<p>The type of ICMP message.</p> <p><b>Note</b> The <code>Type</code> parameter appears in logs only for ICMP packets.</p>
	<p>Some important ICMP types which are widely used include:</p> <ul style="list-style-type: none"> <li>■ Echo Reply (0)</li> <li>■ Echo Request (8)</li> <li>■ Redirect (5)</li> <li>■ Destination Unreachable (3)</li> <li>■ Traceroute (30)</li> <li>■ Time Exceeded (11)</li> </ul> <p>For complete list of ICMP message types, see <a href="#">ICMP Parameters Types</a>.</p>
SPT	The source port number of the session. This field is applicable only if the underlaying transport is UDP/TCP.
DPT	The destination port number of the session. This field is applicable only if the underlaying transport is UDP/TCP.
FW_POLICY_NAME	The name of the firewall policy applied to the session.
SEGMENT_NAME	The name of the segment to which the session belongs to.
DEST_NAME	<p>The name of the remote-end device of the session. The possible values are:</p> <ul style="list-style-type: none"> <li>■ CSS-Backhaul - For traffic which is destined to Cloud Security Service from edge.</li> <li>■ Internet-via-&lt;egress-iface-name&gt; - For Cloud traffic going directly from edge using business policy.</li> <li>■ Internet-BH-via-&lt;backhaul hub name&gt; - For Cloud-bound traffic going to Internet through Backhaul hub using business policy.</li> <li>■ &lt;Remote edge name&gt;-via-Hub - For VPN traffic flowing through Hub.</li> <li>■ &lt;Remote edge name&gt;-via-DE2E - For VPN traffic flowing between the edges through direct VCMP tunnel.</li> <li>■ &lt;Remote edge name&gt;-via-Gateway - For VPN traffic flowing through Cloud gateway.</li> <li>■ NVS-via-&lt;gateway name&gt; - For Non SD-WAN Destination traffic flowing through Cloud gateway.</li> <li>■ Internet-via-&lt;gateway name&gt; - For Internet traffic flowing through Cloud gateway.</li> </ul>
NAT_SRC	The source IP address used for source netting the direct Internet traffic.
NAT_SPT	The source port used for patting the direct Internet traffic.

**Table 20-2. Firewall Log Message Fields (continued)**

Field	Description
APPLICATION	The Application name to which the session was classified by DPI Engine. This field is available only for Close log messages.
BYTES_SENT	The amount of data sent in bytes in the session. This field is available only for Close log messages.
BYTES RECEIVED	The amount of data received in bytes in the session. This field is available only for Close log messages.
DURATION_SECS	The duration for which the session has been active. This field is available only for Close log messages.
REASON	<p>The reason for closure or denial of the session. The possible values are:</p> <ul style="list-style-type: none"> <li>■ State Violation</li> <li>■ Reset</li> <li>■ Purged</li> <li>■ Aged-out</li> <li>■ Fin-Received</li> <li>■ RST-Received</li> <li>■ Error</li> </ul> <p>This field is available for Close and Deny log messages.</p>

## Configure Netflow Settings for Profiles

As an Enterprise Administrator, you can configure Netflow settings at the Profile level.

To configure the Netflow settings for a Profile:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.  
The **Profiles** page displays the existing Profiles.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile that you want to configure Netflow. You can also select a Profile and click **Modify** to configure the Profile.  
The **Device** page for the selected profile appears.
- 3 From the **Segment** drop-down menu, select a profile segment to configure Netflow settings.

- 4 Scroll down to the **Telemetry** category and click the **Netflow Settings** area to configure Netflow details.

Collector*	Collector IP	Collector Port	Filter	Allow All
Net flow C1	10.10.2.2	4739	NFI	<input checked="" type="checkbox"/> Yes

Version v10

Intervals

Flow Stats *	60
FlowLink Stats *	60
Segment Table *	300
Application Table *	300
Interface Table *	300
Link Table *	300
Tunnel Stats *	60

- a Select the **Activate Netflow** check box.

SASE Orchestrator supports IP Flow Information Export (IPFIX) protocol version 10.

- b From the **Collector** drop-down menu, select an existing Netflow collector to export IPFIX information directly from SD-WAN Edge, or click **+ New Collector** to configure a new Netflow collector.

For more information about how to add a new collector, see [Configure Netflow Settings](#).

---

**Note** You can configure a maximum of two collectors per segment and eight collectors per profile by clicking the **+ ADD** button. When the number of configured collectors reaches the maximum allowable limit, the **+ ADD** button will be deactivated.

---

**Note** Netflow version 10 is the only supported version.

- c From the **Filter** drop-down menu, select an existing Netflow filter for the traffic flows from SD-WAN Edge, or click **+ New Filter** to configure a new Netflow filter.

For more information about how to add a new filter, see [Configure Netflow Settings](#).

---

**Note** You can configure a maximum of 16 filters per collector by clicking the **+** button. However, the '**Allow All**' filtering rule is added implicitly at the end of the defined filter list, per collector.

---

- d Select the **Allow All** check box corresponding to a collector to allow all segment flows to that collector.
- e Under **Intervals**, configure the following Netflow export intervals:
  - **Flow Stats** - Export interval for flow stats template, which exports flow statistics to the collector. By default, netflow records of this template are exported every 60 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **FlowLink Stats** - Export interval for flow link stats template, which exports flow statistics per link to the collector. By default, netflow records of this template are exported every 60 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **Segment Table** - Export interval for Segment option template, which exports segment related information to collector. The default export interval is 300 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **Application Table** - Export interval for Application option template, which exports application information to the collector. The default export interval is 300 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **Interface Table** - Export interval for Interface option template, which exports interface information to collector. The default export interval is 300 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **Link Table** - Export interval for Link option template, which exports link information to the collector. The default export interval is 300 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **Tunnel Stats** - Export interval for tunnel stats template. By default, the statistics of the active tunnels in the edge are exported every 60 seconds. The allowable export interval range is from 60 seconds to 300 seconds.

---

**Note** In an Enterprise, you can configure the Netflow intervals for each template only on the Global segment. The configured Netflow export interval is applicable for all collectors of all segments on an edge.

For more information on various Netflow templates, see IPFIX Templates.

## 5 Click **Save Changes**.

## Configure Authentication Settings for Profiles

The **Device Authentication Settings** allows you to select a Radius server to authenticate a user.

To configure the Authentication settings for a Profile:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.

- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile for which you want to configure the Authentication Settings. The configuration options for the selected Profile are displayed in the **Device** tab.
- 3 Scroll down to the **Edge Services** category and click **Authentication**.

The screenshot shows a user interface for managing authentication services. At the top, there's a navigation bar with 'Edge Services' and 'Authentication'. Below this, a dropdown menu labeled 'RADIUS Server' is open, showing 'RADSER1' as the current selection. To the right of the dropdown is a blue button labeled '+ NEW RADIUS SERVICE'.

- 4 From the **RADIUS Server** drop-down menu, select the Radius server that you want to use for authentication.

**Note** All the Radius servers that are already configured using the **Authentication Services** feature in the **Network Services** page appears in the **RADIUS Server** drop-down menu. Alternatively, you can configure a new authentication service by selecting the **New Radius Service** button. For instructions about how to configure Authentication Services, see [Configure Authentication Services](#).

- 5 Click **Save Changes**.

## Configure NTP Settings for Profiles

The Network Time Protocol (NTP) provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse network. VMware recommends using NTP to synchronize the system clocks of Edges and other network devices.

As an Enterprise user, you can configure a time source for the SD-WAN Edge to set its own time accurately by configuring a set of upstream NTP Servers to get its time. The Edge attempts to set its time from a default set of public NTP Servers, but the time set is not reliable in most secure networks. In order to ensure that the time is set correctly on an Edge, you must activate the Private NTP Servers feature and then configure a set of NTP Servers. Once the Edge's own time source is properly configured, you can configure the SD-WAN Edge to act as an NTP Server to its own clients.

### Prerequisites

NTP has the following prerequisites:

- To configure an SD-WAN Edge to act as an NTP Server for its clients, you must first configure the Edge's own NTP time sources by defining Private NTP Servers.

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**.

The **Configuration Profiles** page appears.

- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile for which you want to configure the NTP settings. The configuration options for the selected Profile are displayed in the **Device** tab.
- 3 Configure the Edge's own time sources by defining Private NTP Servers. These servers could be either known time sources within your own network, or well-known time servers on the Public Internet, if they are reachable from the Edge. To define Private NTP Servers:
  - a Scroll down to the **Edge Services** category and go to the **NTP** area.

The screenshot shows the NTP configuration interface. In the Client section, 'Source Interface' is set to 'Auto' and 'Private NTP Servers' is checked. In the Server section, 'Edge as NTP Server' is checked and 'Authentication' is set to 'MD5'. The Servers table contains two entries: '10.0.1.0' and '10.0.2.0'. The Keys table contains one entry: '123' with '1213' as the key value.

Servers	
<input type="checkbox"/>	IP Address or DNS Name *
<input type="checkbox"/>	10.0.1.0
<input type="checkbox"/>	10.0.2.0
2 items	

Keys	
<input type="checkbox"/>	Trusted Key # *
<input type="checkbox"/>	123
Key Value *	
1213	
1 item	

- b Select the **Private NTP Servers** check box.
- c In the **Servers** area, click **+Add** and enter the IP address of your Private NTP Server. If DNS is configured, you can use a domain name instead of an IP address. To configure another NTP Server, click the **+Add** button again.

It is strongly recommended to add two or three servers to increase availability and accuracy of time setting. If you do not set Private NTP Servers, the Edge attempts to set its time from a default set of public NTP Servers, but that is not guaranteed to work, especially if the Edge cannot communicate to servers on the public Internet.

---

**Note** SASE Orchestrator allows you to activate the Edge to act as an NTP Server to its clients, only if you have defined Private NTP Servers.

As Edge interfaces are not available at the Profile level, the **Source Interface** field is set to **Auto**. The Edge automatically selects an interface with 'Advertise' field set as the source interface.

- 4 Once you have defined Private NTP Servers, Orchestrator allows you to configure the SD-WAN Edge to act as an NTP Server for its clients:
  - a Select the **Edge as NTP Server** check box. You can select the check box only if you have activated at least one Private NTP Server.
  - b Choose the type of NTP Authentication as either **None** or **MD5**.
  - c If you choose **MD5**, then you must configure the NTP authentication key value pair details by clicking the **+Add** button under the **Keys** area.
- 5 Click **Save Changes**. The NTP configuration settings are applied to the selected profile.

#### What to do next

At the Edge-level, you can override the NTP settings for specific Edges. For more information, see [Configure NTP Settings for Edges](#).

# Configure Business Policy

21

VMware provides an enhanced Quality of Service feature called Business Policy. SASE Orchestrator allows you to configure business policy rules at the Profile and Edge levels. The business policy uses the parameters such as source IP address/port, destination IP address/port, domain name, address and port group, applications, application categories, and DSCP tags to create business policy rules. Operators, Partners, and Admins of all levels can create a business policy.

Read the following topics next:

- [Configure Business Policies](#)

## Configure Business Policies

You can configure Business Policy rules using the **Business Policy** tab in the Profile Configuration page. Optionally, you can also override the Profile Business Policy rules at the Edge-level.

Business Policy Rules are now Segment aware. All Segments available for configuration are listed in the **Segment** drop-down menu, located at the top of the screen. By default, **Global Segment [Regular]** Segment is selected. When you choose a Segment to configure from the **Segment** drop-down menu, the settings and options associated with that Segment appear in the **Configure Business Policy** area. For more information. see [Chapter 8 Configure Segments](#).

### Configure Business Policy for a Profile

---

**Note** If you are logged in using a user ID that has Customer Support privileges, you can only view the SASE Orchestrator objects. You cannot create new objects or configure/update existing ones.

---

Based on the business policy configuration, VMware examines the traffic being used, identifies the Application behavior, the business service objective required for a given app (High, Medium, or Low), and the Edge WAN Link conditions. Based on this, the Business Policy optimizes Application behavior driving queuing, bandwidth utilization, link steering, and the mitigation of network errors.

### Prerequisites

- Ensure that you have the details of IP addresses configured in the network devices.

- For an Enterprise user to configure the **Customizable QoE** settings, an Operator Super user must select the **Customizable QoE** check box, by navigating to **Global Settings > Customer Configuration > Additional Configuration > Global > Feature Access**.

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 Click the link to a Profile, and then click the **Business Policy** tab. Alternatively, you can click the **View** link in the **Biz. Pol** column of the Profile.

- 3 The existing pre-defined business policy rules are displayed as shown in the following screenshot. The **Configure Business Policy** section displays the business policy rules listed in order of highest precedence. Network traffic is managed by identifying its characteristics then matching the characteristics to the rule with the highest precedence. A number of rules are predefined and you can add your own rules to customize your network operation by clicking the **+ADD** button.

Rule Name	IP Version	Source	Destination	Action	Network Service	Link	Priority	Service Class
1 Object group policy1	IPv4 and IPv6	Address Group: AddressGPT	Any	Any	Multi-Path	Auto	Normal	Transactional
2 Box	IPv4 and IPv6	Any	Any	Box (File Sharing)	Multi-Path	Auto	High	Bulk
3 Speedtest	IPv4 and IPv6	Any	Any	Speedtest (File Sharing)	Multi-Path	Auto	High	Bulk
4 Skype	IPv4 and IPv6	Any	Any	Skype and Teams (Business Collaboration)	Direct	Auto	Low	Transactional
5 Business Application	IPv4 and IPv6	Any	Any	All Business Application	Multi-Path	Auto	High	Transactional
6 Remote Desktop	IPv4 and IPv6	Any	Any	All Remote Desktop	Multi-Path	Auto	High	Transactional
7 Business Collaboration	IPv4 and IPv6	Any	Any	All Business Collaboration	Multi-Path	Auto	High	Realtime
8 Email bulk/DATA	IPv4 and IPv6	Any	Any	All Email	Multi-Path	Auto	High	Bulk
9 Infrastructure	IPv4 and IPv6	Any	Any	All Infrastructure	Multi-Path	Auto	Normal	Transactional
10 Web	IPv4 and IPv6	Any	Any	All Web	Direct	Auto	Normal	Transactional
11 Authentication	IPv4 and IPv6	Any	Any	All Authentication	Multi-Path	Auto	Normal	Transactional
12 Management	IPv4 and IPv6	Any	Any	All Management	Multi-Path	Auto	Normal	Transactional
13 Network Service	IPv4 and IPv6	Any	Any	All Network Service	Multi-Path	Auto	Normal	Transactional
14 Tunneling and VPN	IPv4 and IPv6	Any	Any	All Tunneling and VPN	Multi-Path	Auto	Normal	Transactional
15 Audio/Video	IPv4 and IPv6	Any	Any	All Real Time Audio/Video	Multi-Path	Auto	High	Realtime
16 File Sharing	IPv4 and IPv6	Any	Any	All File Sharing	Multi-Path	Auto	Normal	Bulk
17 Internet Instant Messaging	IPv4 and IPv6	Any	Any	All Internet Instant Messaging	Direct	Auto	Low	Transactional

- 4 You can configure the following options:

Option	Description
<b>Business Policy Rules</b>	
Add	Click to create a new business policy. For more information, see <a href="#">Create Business Policy Rule</a> .

Option	Description
Delete	Click to delete the selected business policies.
Clone	Click to duplicate the selected business policy.
SD-WAN Traffic Class and Weight Mapping	Allows to define traffic class with priority and service class, along with mapping of scheduler weight. For more information, see <a href="#">Overlay QoS CoS Mapping</a> .
<b>Additional Settings</b>	
SD-WAN Overlay Rate Limit	Allows you to configure rate limit for tunnel traffic. For more information, see <a href="#">Tunnel Shaper for Service Providers with Partner Gateway</a> .
Customizable QoE	Allows you to configure the minimum and maximum latency threshold values, in the range 1ms to 1000ms, for <b>Voice</b> , <b>Video</b> , and <b>Transactional</b> application categories. Clicking <b>Reset All To Default</b> , resets all the values to the default values. The default values are listed in the note below the table.
Sort	You can sort the business policy rules using the following options: <ul style="list-style-type: none"> <li>■ Sort by category</li> <li>■ Sort by segment aware</li> </ul>
View	From the <b>View</b> drop-down menu, choose: <ul style="list-style-type: none"> <li>■ Expand All - Expands and shows all the business policy related details and settings.</li> <li>■ Collapse All - Collapses all the business policy related details and settings.</li> </ul>

### Note

- The default latency threshold values are:

Application Category	Good to Fair	Fair to Bad
Voice	25	65
Video	30	65
Transactional	50	80

The **Good to Fair** value must always be less than the **Fair to Bad** value.

- Whenever the **Customizable QoE** values are modified for a Profile or an Edge, an event is created on the **Monitor > Events** page.
- The **Customizable QoE** configuration settings are applied only to the Edge versions 5.2.0 and above.
- Whenever the threshold values are changed for an Edge, all the tunnels to the corresponding Gateway inherit the same threshold values.

- 5 By default, Profile configurations are applied to all the Edges associated with the Profile. If required, you can add or modify business policy rules and override other configurations for a specific Edge.

### Configure Business Policy for an Edge

- In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- Click the link to an Edge, and then click the **Business Policy** tab. Alternatively, you can click the **View** link in the **Business Policy** column of the Edge. The **Configure Business Policy** page appears.

Rule Name	IP Version	Source	Destination	Action	Network Service	Link	Priority	Service Class
Object group policy1	IPv4 and IPv6	Address Group: AddressGP1 Port Group: ServiceGP1	Any	Any	Multi-Path	Auto	Normal	Transactional
Box	IPv4 and IPv6	Any	Any	Box (File Sharing)	Multi-Path	Auto	High	Bulk
Speedtest	IPv4 and IPv6	Any	Any	Speedtest (File Sharing)	Multi-Path	Auto	High	Bulk
Skype	IPv4 and IPv6	Any	Any	Skype and Teams (Business Collaboration)	Direct	Auto	Low	Transactional
Business Application	IPv4 and IPv6	Any	Any	All Business Application	Multi-Path	Auto	High	Transactional
Remote Desktop	IPv4 and IPv6	Any	Any	All Remote Desktop	Multi-Path	Auto	High	Transactional
Business Collaboration	IPv4 and IPv6	Any	Any	All Business Collaboration	Multi-Path	Auto	High	Realtime
Email bulk/DATA	IPv4 and IPv6	Any	Any	All Email	Multi-Path	Auto	High	Bulk
Infrastructure	IPv4 and IPv6	Any	Any	All Infrastructure	Multi-Path	Auto	Normal	Transactional

- The business policy rules and other settings inherited from the associated Profile are displayed under the **Rules From Profile** section of the **Configure Business Policy** page. You can edit the existing rules or add new rules for the selected Edge, by selecting the **Override** check box. The new and overridden rules appear in the **Edge Overrides** section.

## Create Business Policy Rule

Business Policy rules are configured to steer the traffic, bandwidth management and ensure quality of service based on criterions like application, source and destination etc. Operators, Partners, and Admins of all levels can create a business policy. The business policy matches parameters such as IP addresses, ports, VLAN IDs, interfaces, domain names, protocols, operating system, object groups, applications, and DSCP tags. When a data packet matches the match conditions, the associated action or actions are taken. If a packet matches no parameters, then a default action is taken on the packet. You can create business policies for a Profile and Edge.

## Prerequisites

Ensure that you have the details of IP addresses of your network.

## Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 Click the link to a Profile or click the **View** link in the **Device** column of the Profile. The configuration options are displayed in the **Device** tab.
- 3 Click the **Business Policy** tab.

From the **Profiles** page, you can navigate to the **Business Policy** page directly by clicking the **View** link in the **Biz. Pol** column of the Profile.

- 4 In the **Business Policy** page, click **+ ADD**. The **Add Rule** window is displayed.

The screenshot shows the 'Add Rule' window with the following configuration:

- Rule Name \***: VLAN\_Rule
- IP Version \***: IPv4 and IPv6 (selected)
- Match** tab selected.
- Source**: Define > VLAN
- VLAN \***: Corporate
- Ports**: Enter Port or Port Range (Example: 8080-8090 or 443)
- Operating System**: None
- Destination**: Define
- Domain name**: www.vmware.com
- Protocol**: None
- Ports**: Enter Port or Port Range (Example: 8080-8090 or 443)
- Application**: Define
- Application Category**: Any Application
- Application**: Any Application
- DSCP**: None

At the bottom right are two buttons: **CANCEL** and **CREATE**.

- 5 Enter the Rule Name and select the IP version. You can configure the Source and Destination IP addresses according to the selected IP version, as follows:
  - **IPv4 and IPv6** – Allows to configure both IPv4 and IPv6 addresses in the matching criteria. If you choose this mode, you can choose the IP addresses from Object Groups containing Address Groups with both type of Address Groups. By default, this address type is selected.
  - **IPv4** – Applies to traffic with only IPv4 address as source and destination.
  - **IPv6** – Applies to traffic with only IPv6 address as source and destination.

**Note** When you upgrade, the Business policy rules from previous versions are moved to IPv4 mode.

---

**6** In the **Match** tab, configure the match criteria for Source, Destination, and Application traffic.

Field	Description
Source	<p>Allows to specify the source for packets. Select any of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Any</b> - Allows all source addresses by default.</li> <li>■ <b>Object Group</b> - Allows you to select a combination of address group and service group.</li> </ul> <p>If address type is IPv4, then only IPv4 address from Address Groups are considered to match the traffic source.</p> <p>If address type is IPv6, then only IPv6 address from Address Groups are considered to match the traffic source.</p> <p>If address type is both IPv4 and IPv6, then IPv4 and IPv6 both addresses from Address Groups are considered to match the traffic source.</p> <p>For more information, see <a href="#">Chapter 31 Object Groups</a> and <a href="#">Configure Business Policies with Object Group</a>.</p> <hr/> <p><b>Note</b> If the selected address group contains any domain names, then they would be ignored when matching for the source.</p> <ul style="list-style-type: none"> <li>■ <b>Define</b> - Allows you to define the source traffic from a specific VLAN, Interface, IP Address, Port, or Operating System. Select one of the following options:           <ul style="list-style-type: none"> <li>■ <b>VLAN</b> - Matches traffic from the specified VLAN, selected from the drop-down menu.</li> <li>■ <b>Interface</b> - Matches traffic from the specified interface selected from the drop-down menu.</li> </ul> <hr/> <p><b>Note</b> If an interface cannot be selected, then the interface is either not activated or not assigned to this segment.</p> <li>■ <b>IP Address</b> - Matches traffic from the specified IP address (IPv4 or IPv6).</li> </li></ul> <hr/> <p><b>Note</b> This option is not available if you select <b>IPv4 and IPv6 (Mixed mode)</b> as the IP version. In the Mixed mode, the traffic is matched based on either the specified VLAN or interface.</p> <p>Along with the IP address, you can specify one of the following address types to match the source traffic:</p> <ul style="list-style-type: none"> <li>■ <b>CIDR prefix</b> - Choose this option if you want the network defined as a CIDR value (for example: 172.10.0.0 /16).</li> <li>■ <b>Subnet mask</b> - Choose this option if you want the network defined based on a Subnet mask (for example, 172.10.0.0 255.255.0.0).</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Wildcard mask</b> - Choose this option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP, or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a '1' within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values, and the last octet is a variable value. This option is available only for IPv4 address.</li> <li>■ <b>Ports</b> - Matches traffic from the specified source port or port range.</li> <li>■ <b>Operating System</b> - Matches traffic from the specified operating system, selected from the drop-down menu.</li> </ul>
Destination	<p>Allows to specify the destination for packets. Select any of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Any</b> - Allows all destination addresses by default.</li> <li>■ <b>Object Group</b> - Allows you to select a combination of address group and service group. For more information, see <a href="#">Chapter 31 Object Groups and Configure Business Policies with Object Group</a>.</li> <li>■ <b>Define</b> - Allows you to define the matching criteria for the destination traffic to a specific IP Address, Domain Name, Protocol, or Port. Select one of the following options, by default, <b>Any</b> is selected: <ul style="list-style-type: none"> <li>■ <b>Any</b> - Matches all destination traffic.</li> <li>■ <b>Internet</b> - Matches all Internet traffic (traffic that does not match an SD-WAN Route) to the destination.</li> <li>■ <b>Edge</b> - Matches all traffic to an Edge.</li> <li>■ <b>Non SD-WAN Destination via Gateway</b> - Matches all traffic to the specified Non SD-WAN Destination through Gateway, associated with a Profile. Ensure that you have associated your Non SD-WAN sites via Gateway at the Profile level.</li> <li>■ <b>Non SD-WAN Destination via Edge</b> - Matches all traffic to the specified Non SD-WAN Destination through Edge, associated with an Edge or Profile. Ensure that you have associated your Non SD-WAN sites via Edge at the Profile or Edge level.</li> </ul> </li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Domain name</b> - Matches traffic for the entire domain name or a portion of the domain name specified in the <b>Domain Name</b> field. For example, \salesforce\ will match traffic to \www.salesforce.com\.</li> <li>■ <b>Protocol</b> - Matches traffic for the specified protocol, selected from the drop-down menu. The supported protocols are: GRE, ICMP, TCP, and UDP.</li> </ul> <p><b>Note</b> ICMP is not supported in <b>Mixed</b> mode.</p> <ul style="list-style-type: none"> <li>■ <b>Ports</b> - Matches traffic from the specified source port or port range.</li> </ul>
Application	<p>Select any one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Any</b> - Applies the business policy rule to any application by default.</li> <li>■ <b>Define</b> - Allows to select a specific application to apply the business policy rule. In addition, a DSCP value can be specified to match the traffic coming in with a preset DSCP/TOS tag.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ When creating a business policy rule matching an application only, to apply the Network Service Action for such application, the Edge might need to use DPI (Deep Packet Inspection) Engine. Generally, the DPI does not determine the application based on the first packet. The DPI Engine usually needs the first 5-10 packets in the flow to identify the application. For the first few packets received, traffic is unclassified and matches a less specific business policy, which might cause the traffic to take a different path, i.e. 'Direct' instead of 'Multipath', depending on the policy it matches. Once DPI determines the traffic type, it matches a more specific policy configured for this type of traffic. However, that flow continues to take the path from the original policy it matched, because steering to a new path would break the flow. This can cause the first flow to a specific Destination IP and port to take one path. Once the app cache is populated, the subsequent flows to the same Destination IP and port take another path as configured in a more specific policy for this type of traffic.</li> <li>■ Once the DPI classifies the traffic, it adds the Destination IP and port to the app cache, and immediately classifies any subsequent flows to that same Destination IP and port. The app cache entry expires after 10 minutes of no traffic going to that Destination IP and port. The next flow to that Destination IP and port must go through the DPI again and may take an unexpected path based on the policy it matches before the DPI identifies the application.</li> </ul>

- 7 In the **Action** tab, configure the actions to be performed when the traffic matches the defined criteria.

**Note** Depending on your **Match** choices, some Actions may not be available.

Add Rule

Rule Name *	VLAN_Rule
IP Version *	<input type="radio"/> IPv4 <input checked="" type="radio"/> IPv6 <input type="radio"/> IPv4 and IPv6
Match	Action
Priority	<input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low
Enable Rate Limit	<input checked="" type="checkbox"/>
Outbound Limit:	% Link bandwidth
Inbound Limit:	% Link bandwidth
Network Service	MultiPath
Link Steering ⓘ	Auto
Inner Packet DSCP Tag	46 - EF
Outer Packet DSCP Tag	0 - CS0/DF
Enable NAT	<input checked="" type="checkbox"/>
Source NAT IPv6	Example: 2001:db8:3333:4444:5555:6666:7777:8888
Destination NAT IPv6	Example: 2001:db8:3333:4444:5555:6666:7777:8888
Service Class	<input type="radio"/> Realtime <input checked="" type="radio"/> Transactional <input type="radio"/> Bulk
<input type="button" value="CANCEL"/> <input type="button" value="CREATE"/>	

Field	Description
Priority	Designate the priority of the rule as one of the following: <ul style="list-style-type: none"> <li>■ <b>High</b></li> <li>■ <b>Normal</b></li> <li>■ <b>Low</b></li> </ul>

Field	Description
Enable Rate Limit	<p>Select the <b>Enable Rate Limit</b> check box to set limits for inbound and outbound traffic directions.</p> <p><b>Note</b> Rate limiting is performed per flow. Rate limiting for upstream traffic only works when you specify a link or Edge interface in the Business Policy. If you set the Steering option to Auto, Transport, or Group, the rate limit will apply to the total bandwidth of all the corresponding links. This may not enforce a strict rate limit as you expect. If you want to enforce a strict rate limit, you should steer traffic to a single link or Edge interface in the Business Policy.</p>

Field	Description
Network Service	<p>Set the <b>Network Service</b> to one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Direct</b> - Sends the traffic out of the WAN circuit directly to the destination, bypassing the SD-WAN Gateway.</li> </ul> <p><b>Note</b> The Edge by default prefers a secure route over a business policy. In practice this means the Edge will forward traffic via Multipath (Branch to Branch or Cloud via Gateway, depending on the route) even if a business policy is configured to send that traffic via the Direct path if the Edge has received either secure default routes or more specific secure routes from the Partner Gateway or another Edge.</p> <p>This behavior can be overridden for Partner Gateway secure routes by activating the "Secure Default Route Override" feature for a customer. A Partner Super User or an Operator can activate this feature which overrides all Partner Gateway secure routes that also match a business policy. "Secure Default Route Override" does not override Hub secure routes.</p> <ul style="list-style-type: none"> <li>■ <b>Multi-Path</b> - Sends the traffic from one SD-WAN Edge to another SD-WAN Edge.</li> <li>■ <b>Internet Backhaul</b> - This network service is activated only if the <b>Destination</b> is set as <b>Internet</b>.</li> </ul> <p><b>Note</b> The <b>Internet Backhaul</b> Network Service will only apply to Internet traffic (WAN traffic destined to network prefixes that do not match a known local route or VPN route).</p> <p>For information about these options, see <a href="#">Configure Network Service for Business Policy Rule</a>.</p> <p>If Conditional Backhaul is activated at the profile level, by default it will apply for all Business Policies configured for that profile. You can turn off conditional backhaul for selected policies to exclude selected traffic (Direct, Multi-Path, and CSS) from this behavior by selecting the <b>Turn off Conditional Backhaul</b> check box.</p> <p>For more information about how to activate and troubleshoot the Conditional Backhaul feature, see <a href="#">Conditional Backhaul</a>.</p>

Field	Description
Link Steering	<p>Select one of the following link steering modes:</p> <ul style="list-style-type: none"> <li>■ <b>Auto</b> - By default, all applications are set to automatic Link Steering mode. When an application is in the automatic Link Steering mode, the DMPO automatically chooses the best links based on the application type and automatically activates on-demand remediation when necessary.</li> <li>■ <b>Transport Group</b> - Specify any one of the following transport group options in the steering policy so that the same Business Policy configuration can be applied across different device types or locations, which may have completely different WAN carriers and WAN interfaces: <ul style="list-style-type: none"> <li>■ <b>Public Wired</b></li> <li>■ <b>Public Wireless</b></li> <li>■ <b>Private Wired</b></li> </ul> </li> <li>■ <b>Interface</b> - Link steering is tied to a physical interface and will be used primarily for routing purposes. <p><b>Note</b> This option is only allowed at the Edge override level.</p> </li> <li>■ <b>WAN Link</b> - Allows to define policy rules based on specific private links. For this option, the interface configuration is separate and distinct from the WAN link configuration. You will be able to select a WAN link that was either manually configured or auto-discovered. <p><b>Note</b> This option is only allowed at the Edge override level.</p> </li> <li>■ <b>Inner Packet DSCP Tag</b> - Select an Inner Packet DSCP Tag from the drop-down menu.</li> <li>■ <b>Outer Packet DSCP Tag</b> - Select an Outer Packet DSCP Tag from the drop-down menu.</li> </ul> <p><b>Note</b> When the Network Service is configured as <b>Direct</b>, the IPv6 only Interfaces and IPv6 only WAN links are not supported in Link Steering mode.</p> <p>For more information about the link steering modes and DSCP, DSCP marking for both Underlay and Overlay traffic, see <a href="#">Configure Link Steering Modes</a>.</p>

Field	Description
Enable NAT	Activate or deactivate NAT. This option is not available for <b>IPv4 and IPv6</b> mode. For more information, see <a href="#">Configure Policy-based NAT</a> .
Service Class	Select one of the following Service Class options: <ul style="list-style-type: none"> <li>■ Real-time</li> <li>■ Transactional</li> <li>■ Bulk</li> </ul> <p><b>Note</b> This option is only for a custom application.</p> <p>VMware Apps/Categories fall in one of these categories.</p>

- 8 After configuring the required settings, click **Create**.

A business policy rule is created for the selected Profile, and it appears under the **Business Policy Rules** area of the **Profile Business Policy** page.

**Note** The rules created at the Profile level cannot be updated at the Edge level. To override the rule, user needs to create the same rule at the Edge level with new parameters to override the Profile level rule.

For the **IPv6** and **IPv4 and IPv6** modes, you can only Create Business policy rules from the Orchestrator. You can perform the rest of the operations like Update and Delete only through API.

Related Information: [Overlay QoS CoS Mapping](#)

## Configure Network Service for Business Policy Rule

While creating or updating a Business Policy rule and action, you can set the **Network Service** to **Direct**, **Multi-Path**, and **Internet Backhaul**.

### Direct

Sends the traffic out of the WAN circuit directly to the destination, bypassing the SD-WAN Gateway. NAT is applied to the traffic if the **NAT Direct Traffic** checkbox is enabled on the **Interface Settings** under the **Device** tab. When you configure NAT Direct, consider the following limitations.

- NAT must hit traffic in edge routing table with Next Hop as either Cloud VPN or Cloud Gateway.
- NAT works for traffic to public IP addresses only, even if Business Policy allows to configure private IP addresses as destination.

### Multi-Path

Sends the traffic from one SD-WAN Edge to another SD-WAN Edge, and from a SD-WAN Edge to a SD-WAN Gateway.

## Internet Backhaul

While configuring the business policy rule match criteria, if you define the **Destination** as **Internet**, then the **Internet Backhaul** network service will be enabled.

---

**Note** The **Internet Backhaul** Network Service will only apply to Internet traffic (WAN traffic destined to network prefixes that do not match a known local route or VPN route).

---

When the **Internet Backhaul** is selected, you can select one of the following options and configure endpoints to backhaul the following Internet-bound traffic types (Direct Internet traffic, Internet via SD-WAN Gateway, CSS traffic, and Cloud Web Security (CWS) Gateway traffic):

- Backhaul Hubs
- Non SD-WAN Destinations via Gateway
- Non SD-WAN Destinations via Edge/Cloud Security Service

---

**Note** Mixed IP mode (IPv4 and IPv6) is not supported for NSD via Edge and CSS.

---

- VMware Cloud Web Security Gateway

---

**Note** The VMware Cloud Web Security Gateway option is available only if a user has subscribed to use the VMware Cloud Web Security service.

For more information, see VMware SD-WAN Cloud Web Security Configuration Guide published at <https://docs.vmware.com/en/VMware-Cloud-Web-Security/index.html>.

- VMware Cloud To Cloud Interconnect - VMware SD-WAN supports interconnection of multiple Hub Edges or Hub Clusters to increase the range of Spoke Edges that can communicate with each other. This feature "Hub or Cluster Interconnect" allows communication between the Spoke Edges connected to one Hub Edge or Hub Cluster and the Spoke Edges connected to another Hub Edge or Hub Cluster, using multiple overlay and underlay connections. For more information, see [Hub or Cluster Interconnect](#).

You should be able to configure multiple VMware SD-WAN Sites for backhaul to support the redundancy that is inherently built into the Non SD-WAN Destination connection, but keep a consistent behavior of service unavailability leading to traffic being dropped.

Add Rule X

Rule Name *	NS Rule1		
IP Version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> IPv4 and IPv6		
Match	Action		
Priority	<input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low		
Enable Rate Limit	<input type="checkbox"/>		
Network Service	Internet Backhaul > Non SD-WAN Destination via Edge / Cloud Security Service ▾		
Non SD-WAN Destination via Edge / Cloud Security Service	<input type="text" value="GCS service1"/>		
Link Steering ⓘ	<input type="text" value="Auto"/>		
Inner Packet DSCP Tag	<input type="text" value="Leave as is"/>		
Outer Packet DSCP Tag	<input type="text" value="0 - CS0/DF"/>		
Enable NAT	<input type="checkbox"/> ⓘ		
Service Class	<input type="radio"/> Realtime <input checked="" type="radio"/> Transactional <input type="radio"/> Bulk		
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; font-weight: bold;">CREATE</span>			

If Conditional Backhaul is enabled at the profile level, by default it will apply for all Business Policies configured for that profile. You can deactivate conditional backhaul for selected policies to exclude selected traffic (Direct, Multi-Path, and CSS) from this behavior by selecting the **Turn off Conditional Backhaul** checkbox in the **Action** area of the **Configure Rule** screen for the selected business policy.

For more information about how to enable and troubleshoot the Conditional Backhaul feature, see [Conditional Backhaul](#).

## Configure Link Steering Modes

In the Business Policy, you can configure link steering with different modes.

To create or configure a Business Policy, see [Create Business Policy Rule](#).

### Link Selection: Auto

By default, all applications are given the automatic Link steering mode. This means the DMPO automatically picks the best links based on the application type and automatically enables on-demand remediation when necessary. There are four possible combinations of Link Steering and On-demand Remediation for Internet applications. Traffic within the Enterprise (VPN) always goes through the DMPO tunnels, hence it always receives the benefits of on-demand remediation.

## Add Rule

Rule Name \* LS Rule1

IP Version \*  IPv4  IPv6  IPv4 and IPv6

Match	Action
Priority	<input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low
Enable Rate Limit	<input type="checkbox"/>
Network Service	MultiPath <input type="button" value="▼"/>
Link Steering <small> ⓘ</small>	Auto <input type="button" value="▼"/>
Inner Packet DSCP Tag	Auto
Outer Packet DSCP Tag	Transport Group <input type="button" value="&gt;"/> Interface <small> ⓘ</small> WAN Link <small> ⓘ</small>
Enable NAT	<input type="checkbox"/> <small> ⓘ</small>
Service Class	<input type="radio"/> Realtime <input checked="" type="radio"/> Transactional <input type="radio"/> Bulk

Scenario	Expected DMPO Behavior
At least one link satisfies the SLA for the application.	Choose the best available link.
Single link with packet loss exceeding the SLA for the application.	Enable FEC for the real-time applications sent on this link.
Two links with loss on only one link.	Enable FEC on both links.
Multiple links with loss on multiple links.	Enable FEC on two best links.

Scenario	Expected DMPO Behavior
Two links but one link appears unstable, i.e. missing three consecutive heartbeats.	Mark link un-useable and steer the flow to the next best available link.
Both Jitter and Loss on both links.	<p>Enable FEC on both links and enable Jitter buffer on the receiving side. Jitter buffer is enabled when Jitter is greater than 7 ms for voice and greater than 5 ms for video.</p> <p>The sending DMPO endpoint notifies the receiving DMPO endpoint to enable Jitter buffer. The receiving DMPO endpoint will buffer up to 10 packets or 200 ms of traffic, whichever happens first. The receiving DMPO endpoint uses the original time stamp embedded in the DMPO header to calculate the flow rate to use in de-jitter buffer. If the flow is not sent at a constant rate, the Jitter buffering is not enabled.</p>

## Link Steering by Transport Group

A Transport Group represents WAN links bundled together based on similar characteristics and functionality. Defining a Transport Group allows business abstraction so that a similar policy can apply across different Hardware types.

Different locations may have different WAN transports (e.g. WAN carrier name, WAN interface name); DMPO uses the concept of Transport Group to abstract the underlying WAN carriers and interfaces from the Business Policy configuration. The Business Policy configuration can specify the transport group (**Public Wired**, **Public Wireless** or **Private Wired**) in the steering policy so that the same Business Policy configuration can be applied across different device types or locations, which may have completely different WAN carriers and WAN interfaces. When the DMPO performs the WAN link discovery, it also assigns the transport group to the WAN link. This is the most desirable option for specifying the links in the Business Policy because it eliminates the need for IT administrators to know the type of physical connectivity or the WAN carrier.

If you choose the **Preferred** option, the **Error Correct Before Steering** checkbox displays.

If you select the **Error Correct Before Steering** checkbox, the Loss% variable textbox displays. When you define a loss percentage (4% for example), the Edge will continue to use the selected link or transport group and apply error correction until loss reaches 4%, which is when it will steer traffic to another path. When the **Error Correct Before Steering** checkbox is unchecked, the Edge will start steering traffic away if the loss for the link exceed the application SLA - i.e. Real-time application SLA is 0.3% by default. If you do not select this checkbox, the application will steer before Error Correction occurs.

## Add Rule

X

Rule Name \* LS Rule1

IP Version \*  IPv4  IPv6  IPv4 and IPv6

**Action**

Priority  High  Normal  Low

Enable Rate Limit

Network Service MultiPath

**Link Steering** Transport Group > Public Wired

Link Policy  Mandatory  Preferred  Available

Error Correct Before Steering

Loss (%) 4.00

Inner Packet DSCP Tag Leave as is

Outer Packet DSCP Tag 0 - CSO/DF

Enable NAT

Service Class  Realtime  Transactional  Bulk

**CANCEL** **CREATE**

**Note** This option is allowed at both the Edge Override level and Profile level.

### Link Steering by Interface

For this option, the link steering is tied to a physical interface. Link steering by interface will be used primarily for routing purposes. However, even though it logically should only be used for routing traffic directly from the VMware SD-WAN Site, if the rule specified has a Network Service requiring Internet Multi-path benefits, it will pick a single WAN link connected to the interface.

If you choose the **Preferred** option, the **Error Correct Before Steering** checkbox displays. If you select the checkbox, an additional Loss% variable is available. When the option is not enabled, the Edge will start steering traffic away if the loss for the link exceeds the application SLA - i.e. Real-Time application SLA is 0.3% by default. When “Error Correct Before Steering” is applied and Loss percentage defined, let’s say if it’s 4% in this example, the Edge will continue to use the selected link or transport group and apply error correction until loss reaches 4%, which is when it will steer traffic to another path. If you do not select this checkbox, the application will steer before Error Correction occurs.

**Note** This option is only allowed at the Edge override level. This will ensure that the link options provided always match the SD-WAN Edge hardware model.

## Add Rule

IP Version \*

IPv4  IPv6  IPv4 and IPv6

Match	Action
Priority	<input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low
Enable Rate Limit	<input type="checkbox"/>
Network Service	MultiPath
Link Steering	Interface
Select Interface *	GE4
VLAN ⓘ	Corporate
ICMP Probe ⓘ	None
Link Policy	<input type="radio"/> Mandatory <input checked="" type="radio"/> Preferred <input type="radio"/> Available
Error Correct Before Steering	<input checked="" type="checkbox"/>
Loss (%)	4.00
Inner Packet DSCP Tag	46 - EF
Outer Packet DSCP Tag	0 - CS0/DF
Enable NAT	<input type="checkbox"/> ⓘ

## WAN Link

For this option, the interface configuration is separate and distinct from the WAN link configuration. You will be able to select a WAN link that was either manually configured or auto-discovered.

## WAN Link Drop Down Menu

You can define policy rules based on specific private links. If you have created private network names and assigned them to individual private WAN overlays, these private link names will display in the **WAN Link** drop-down menu.

For information on how to define multiple private network names and assign them to individual private WAN overlays, see [Configure Private Network Names](#) and [Selecting a Private Name Link](#).

If you choose the **Preferred** option, the **Error Correct Before Steering** checkbox displays. If you do not select this checkbox, the application will steer before Error Correction occurs.

---

**Note** This option is only allowed at the Edge override level.

---

## Add Rule

Rule Name \* LS2 Rule

IP Version \*  IPv4  IPv6  IPv4 and IPv6

Match	Action
Priority	<input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low
Enable Rate Limit	<input type="checkbox"/>
Network Service	MultiPath
Link Steering	WAN Link
WAN Link *	GE6_Private
Link Policy	<input type="radio"/> Mandatory <input checked="" type="radio"/> Preferred <input type="radio"/> Available
Error Correct Before Steering	<input checked="" type="checkbox"/>
	Loss (%) 4.00
Inner Packet DSCP Tag	46 - EF
Outer Packet DSCP Tag	0 - CS0/DF

Enable NAT  ⓘ

Service Class  Realtime  Transactional  Bulk

For the **Interface** and **WAN Link** choices, you must select one of the following options:

Option	Description
Mandatory	Indicates that traffic will be sent over the WAN link or link Service-group specified. If the link specified (or all links within the chosen service group) is inactive <b>or</b> if a Multi-path gateway route is unavailable, the corresponding packet will be dropped.
Preferred	Indicates that traffic should preferably be sent over the WAN link or link Service-group specified. If the link specified (or all links within the chosen service group) is inactive, or if the Multi-path gateway route chosen is unstable, or if the link Service Level Objective (SLO) is not being met, the corresponding packet will be steered on the next best available link. If the preferred link becomes available again, traffic will be steered back to the preferred link.
Available	Indicates that traffic should preferably be sent over the WAN link or link Service-group specified as long as it is available (irrespective of link SLO). If the link specified (or all links within chosen service group) are not available, or if the selected Multi-path gateway route is unavailable, the corresponding packet will be steered to the next best available link. If the preferred link becomes available again, traffic will be steered back to the available link.

## Link Steering: DSCP Marking for Underlay and Overlay Traffic Overview

VMware SD-WAN supports DSCP remarking of packets forwarded by the Edge to the Underlay. The SD-WAN Edge can re-mark underlay traffic forwarded on a WAN link as long as **Underlay Accounting** is enabled on the interface. DSCP re-marking is enabled in the Business Policy configuration in the Link Steering area. See [Create Business Policy Rule](#). In the example image shown below (assuming the Edge is connected to MPLS with both underlay and overlay traffic forwarded MPLS), if the traffic matches the network prefix 172.16.0.0/12, the Edge will re-mark the underlay packets with a DSCP value of 16 or CS2 and ignore the **Outer Packet DSCP Tag** field. For overlay traffic sent toward MPLS matching the same business policy, the DSCP value for the outer header will be set to the **Outer Packet DSCP tag**.

Match	Action
Priority	<input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low
Enable Rate Limit	<input type="checkbox"/>
Network Service	MultiPath
Link Steering	Auto
Inner Packet DSCP Tag	16 - CS2
Outer Packet DSCP Tag	0 - CS0/DF
Enable NAT	<input type="checkbox"/> ⓘ
Service Class	<input type="radio"/> Realtime <input checked="" type="radio"/> Transactional <input type="radio"/> Bulk

## Link Steering: DSCP Marking for Underlay Traffic Use Case

Edges that are connected to MPLS normally mark DSCP on the packet before sending to the PE for the SP to treat the packet according to the SLA. **Underlay Accounting** must be enabled on the WAN interface for DSCP marking on Underlay traffic via Business Policy to take effect.

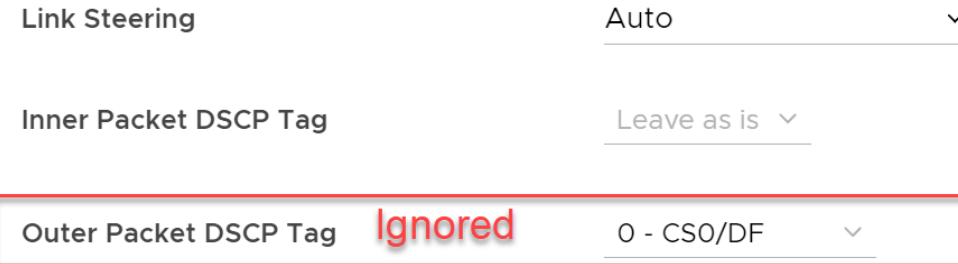
### Linking Steering: Underlay DSCP Configuration

- Verify that **Underlay Accounting** is activated for WAN Overlay by default in the SASE Orchestrator by navigating to **Configure > Edge Devices > Device > Interfaces** and select a SD-WAN Edge model.

The screenshot shows the VMware SD-WAN Edge configuration interface for a Virtual Edge. The interface is titled "Virtual Edge" and shows details for "Interface GE4". A red box highlights the "Underlay Accounting" section, which is set to "Enabled". Other settings shown include "Description" (empty), "Interface Enabled" (Enabled), "Capability" (Routed), "Segments" (All Segments), "Radius Authentication" (disabled), "ICMP Echo Response" (Enabled), "Enable WAN Link" (Enabled), "DNS Proxy" (disabled), "VLAN" (disabled), "IP Preference" (IPv6 selected), and "EVDSL Modem Attached" (disabled). At the bottom, there are "IPv4 Settings" (Enabled) and buttons for "CANCEL" and "SAVE".

- From the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges > Business Policy**.

- 3 From the **Business Policy** screen, click an existing rule or click the **+ADD** button to create a new rule.
- 4 In the **Action** section, go to the **Link Steering** area.
- 5 Click one of the following as applicable: **Auto**, **Transport Group**, **Interface**, or **WAN Link**.
- 6 Configure **Action** criteria for the underlay traffic and configure **Inner Packet DSCP Tag**.



#### Linking Steering: Overlay DSCP Configuration

- 1 Verify that **Underlay Accounting** is activated for WAN Overlay by default in the SASE Orchestrator by navigating to **Configure > Edge Devices > Device > Interfaces** and select a SD-WAN Edge model.
- 2 From the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges > Business Policy**.
- 3 From the **Business Policy** screen, click an existing rule or click the **+ADD** button to create a new rule.
- 4 In the **Action** section, go to the **Link Steering** area.
- 5 Click one of the following as applicable: **Auto**, **Transport Group**, **Interface**, or **WAN Link**.
- 6 Configure **Action** criteria for the Overlay traffic and configure **Inner Packet DSCP Tag** and **Outer Packet DSCP Tag**.



#### Configure Policy-based NAT

You can configure Policy-based NAT for both Source and Destination. The NAT can be applied to either Non SD-WAN Destination traffic or Partner Gateway Handoff traffic using Multi-path. When configuring NAT, you must define which traffic to NAT and the action you want to perform. There are two types of NAT configuration: Many to One and One-to-One.

## Accessing NAT

You can access the NAT feature from **Configure > Profiles > Business Policy tab**, then click the **+ADD** button. The NAT feature is located under the **Action** tab.

**Note** NATing is allowed for rules to an Non SD-WAN Destination via Gateway, and for Internet rules using Multipath.

### Many-to-One NAT Configuration

In this configuration, you can NAT the traffic's source or destination IP originated from the hosts behind the Edge to a different unique source or destination IP address. For example, the user can source NAT all the flows destined to a host or server in the Data Center, which is behind the Partner Gateway with a unique IP address, even though they are originated from different hosts behind an Edge.

The following figure shows an example of the Many to One configuration. In this example, all the traffic originating from the hosts that are connected to VLAN **Corporate** (behind the Edge) destined to an Internet host or a host behind the DC will get source NAT with the IP address 72.4.3.1.

## Add Rule

Rule Name \*

IP Version \*  IPv4  IPv6  IPv4 and IPv6

Match	Action
Priority	<input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low
Enable Rate Limit	<input type="checkbox"/>
Network Service	MultiPath <input type="button" value="▼"/>
Link Steering <small>ⓘ</small>	Auto <input type="button" value="▼"/>
Inner Packet DSCP Tag	Leave as is <input type="button" value="▼"/>
Outer Packet DSCP Tag	0 - CSO/DF <input type="button" value="▼"/>
<b>Enable NAT</b> <input checked="" type="checkbox"/> <b>Source NAT IP</b> <input type="text" value="72.4.3.1"/> <small>Example: 10.10.10.10</small> <b>Destination NAT IP</b> <input type="text"/> <small>Example: 10.10.10.10</small>	
Service Class	<input type="radio"/> Realtime <input checked="" type="radio"/> Transactional <input type="radio"/> Bulk

### One-to-One NAT Configuration

In this configuration, the Branch Edge will NAT a single local IP address of a host or server to another global IP address. If the host in the Non SD-WAN Destination or Data Center sends traffic to the global IP address (configured as the Source NAT IP address in the One-to-One NAT configuration), the SD-WAN Gateway will forward that traffic to the local IP address of the host or server in the Branch.

### Overlay QoS CoS Mapping

A Traffic Class is defined with a combination of Priority (High, Normal, or Low) and Service Class (Real-Time, Transactional, or Bulk) resulting into a 3x3 matrix with nine Traffic Classes. You can map Application/Category and scheduler weight onto these Traffic Classes. All applications

within a Traffic Class will be applied with the aggregate Quality of Service (QoS) treatment, including Scheduling and Policing.

All applications in a given Traffic Class have a guaranteed minimum aggregate bandwidth during congestion based on scheduler weight (or percentage of bandwidth). When there is no congestion, the applications are allowed into the maximum aggregated bandwidth. A Policier can be applied to cap the bandwidth for all the applications in a given Traffic Class. See the image below for a default of the Application/Category and Traffic Class Mapping.

---

**Note** You can match the DSCP value of the incoming traffic to a particular service class in the Business policy of an Edge. For more information, see [Configure Class of Service](#).

---



The Business Policy contains the out-of-the-box Smart Defaults functionality that maps more than 2,500 applications to Traffic Classes. You can use application-aware QoS without having to define policy. Each Traffic Class is assigned a default weight in the Scheduler, and these parameters can be changed in the Business Policy. Below are the default values for the 3x3 matrix with nine Traffic Classes. See the image below for default of the Weight and Traffic Class Mapping.



#### Example:

In this example, a customer has 90 Mbps Internet link and 10 Mbps MPLS on the Edge and the aggregate Bandwidth is 100 Mbps. Based on the default weight and Traffic Class mapping above, all applications that map to Business Collaboration will have a guaranteed bandwidth of 35 Mbps, and all applications that map to Email will have a guaranteed bandwidth of 15 Mbps. Note that business policies can be defined for an entire category like Business Collaborations, applications (e.g. Skype for Business), and more granular sub-applications (e.g. Skype File Transfer, Skype Audio, and Skype Video).

## Configure Overlay QoS CoS Mapping

**Note** The SD-WAN Traffic Class and Weight Mapping feature is editable only if it is activated by your Operator. To gain access to this feature, contact your Operator for more information.

### To activate Overlay QoS CoS Mapping:

- 1 Go to **Configure > Profiles**.
- 2 Click the link of the appropriate configuration Profile.
- 3 Click the **Business Policy** tab.
- 4 In the **SD-WAN Traffic Class and Weight Mapping** area, type in numerical values for **Real Time**, **Transactional**, and/or **Bulk** as necessary.
- 5 Check the **Policing** checkbox for a Service Class, if necessary.

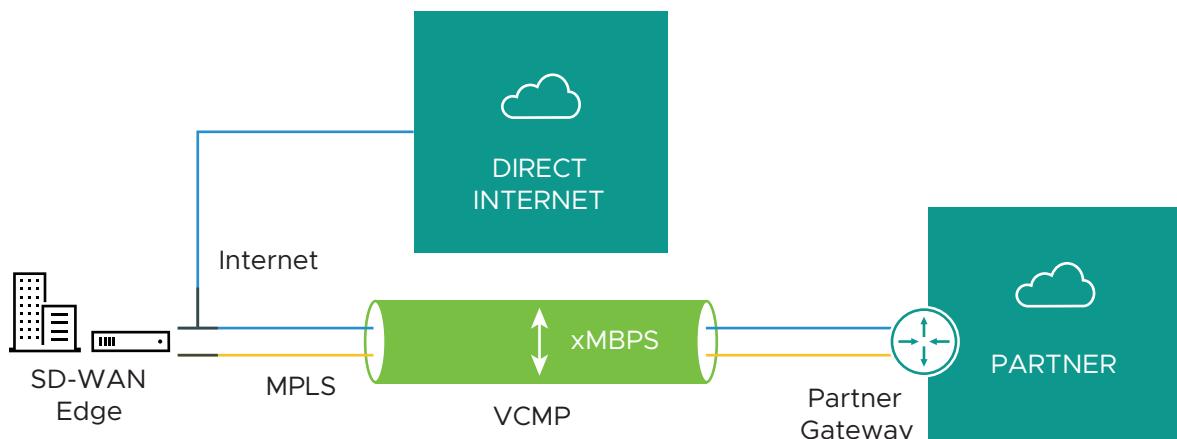
SD-WAN Traffic Class and Weight Mapping						
Service Class / Priority	High	Policing	Normal	Policing	Low	Policing
Real Time	35	<input type="checkbox"/> Off	15	<input type="checkbox"/> Off	1	<input type="checkbox"/> Off
Transactional	20	<input type="checkbox"/> Off	7	<input type="checkbox"/> Off	1	<input type="checkbox"/> Off
Bulk	15	<input type="checkbox"/> Off	5	<input type="checkbox"/> Off	1	<input type="checkbox"/> Off

## Tunnel Shaper for Service Providers with Partner Gateway

This section describes the Tunnel Shaper for Service Providers with the Partner Gateway.

Service Providers may offer SD-WAN services at a lower capacity compared to the aggregated capacity of WAN links at the local branch. For example, customers may have purchased a broadband link from another vendor and SP offering SD-WAN services, and hosting VMware Partner Gateway has no control over the underlay broadband link. In such situations, in order to ensure that the SD-WAN service capacity is being honored and to avoid congestion towards Partner Gateway, a Service Provider can enable the DMPO Tunnel Shaper between the tunnel and the Partner Gateway.

### Tunnel Shaper Example



Consider a SD-WAN Edge with two WAN links, 20 Mbps Internet and 20 Mbps MPLS, using a 35 Mbps SD-WAN service offered from a Service Provider (SP). In this case, the bandwidth of SD-WAN service (35 Mbps) is lower than the aggregated bandwidth of the WAN links (40 Mbps). To ensure that the traffic towards the Partner Gateway does not exceed 35 Mbps (displayed as "X" in the image above), the Service Provider can place a Tunnel Shaper on the DMPO tunnel.

## Configure Rate-Limit Tunnel Traffic

**Note** The Rate-Limit Tunnel Traffic feature is editable only if it is activated by your Operator. To gain access to this feature, see your Operator for more information.

### To activate Rate-Limit Tunnel Traffic:

- 1 Go to **Configure > Profiles** from the navigation panel.
- 2 Click the link of the appropriate configuration Profile.
- 3 Click the **Business Policy** tab and go to **Additional Settings**.
- 4 In the **SD-WAN Overlay Rate Limit** area, check the **Rate-Limit Tunnel Traffic** check box.
- 5 Select either the **Percent** or **Rate (Mbps)** radial buttons. By default, **None** is selected.
- 6 In the **Limit** text box, type in a numerical limit to the Tunnel Traffic.
- 7 Click **Save Changes**.



# Firewall Overview

22

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. SASE Orchestrator supports configuration of Stateless, Stateful, and Enhanced Firewall Services (EFS) rules for Profiles and Edges.

## Stateful Firewall

A Stateful firewall monitors and tracks the operating state and characteristics of every network connection coming through the firewall and uses this information to determine which network packets to allow through the firewall. The Stateful firewalls build a state table and use this table to allow only returning traffic from connections currently listed in the state table. After a connection is removed from the state table, no traffic from the external device of this connection is permitted.

The Stateful firewall feature provides the following benefits:

- Prevent attacks such as denial of service (DoS) and spoofing
- More robust logging
- Improved network security

The main differences between a Stateful firewall and a Stateless firewall are:

- Matching is directional. For example, you can allow hosts on VLAN 1 to initiate a TCP session with hosts on VLAN 2 but deny the reverse. Stateless firewalls translate into simple ACLs (Access lists) which do not allow for this kind of granular control.
- A stateful firewall is session aware. Using TCP's 3-way handshake as an example, a stateful firewall will not allow a SYN-ACK or an ACK to initiate a new session. It must start with a SYN, and all other packets in the TCP session must also follow the protocol correctly or the firewall will drop them. A stateless firewall has no concept of a session and instead filters packets based purely on a packet-by-packet, individual basis.
- A stateful firewall enforces symmetric routing. For instance, it is quite common for asymmetric routing to happen in a VMware network where traffic enters the network through one Hub but exits through another. Leveraging third-party routing, the packet is still able to reach its destination. With a stateful firewall, such traffic would be dropped.

- Stateful firewall rules get rechecked against existing flows after a configuration change. So, if an existing flow has already been accepted, and you configure the stateful firewall to now drop those packets, the firewall will recheck the flow against the new rule set and then drop it. For those scenarios where an "allow" is changed to "drop" or "reject", the pre-existing flows will time out and a firewall log will be generated for the session close.

The requirements to use the Stateful Firewall are:

- The VMware SD-WAN Edge must be using Release 3.4.0 or later.
- By default, the **Stateful Firewall** feature is a customer capability activated for new customers on an SASE Orchestrator using 3.4.0 or later releases. Customers created on a 3.x Orchestrator will need assistance from a Partner or VMware SD-WAN Support to activate this feature.
- The SASE Orchestrator allows the enterprise user to activate or deactivate the Stateful Firewall feature at the Profile and Edge level from the respective **Firewall** page. To deactivate the Stateful Firewall feature for an enterprise, contact an Operator with Super User permission.

---

**Note** Asymmetric routing is not supported in Stateful Firewall activated Edges.

---

## Enhanced Firewall Services

Enhanced Firewall Services (EFS) provide additional EFS security functionalities on VMware SD-WAN Edges. The VMware Security-powered EFS functionality supports URL Category filtering, URL Reputation filtering, Malicious IP filtering, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS) services on VMware SD-WAN Edges. The Enhanced Firewall Services (EFS) protect Edge traffic from intrusions across Branch-to-Branch, Branch-to-Hub, or Branch-to-Internet traffic patterns.

Currently, the SD-WAN Edge Firewall provides stateful inspection along with application identification without additional EFS. While the stateful Firewall SD-WAN Edge provides security, it is not adequate and creates a gap in providing EFS security integrated natively with VMware SD-WAN. Edge EFS addresses these security gaps and offers enhanced threat protection natively on the SD-WAN Edge in conjunction with VMware SD-WAN.

Customers can configure and manage the Stateful Firewall and EFS using the Firewall functionality in VMware SASE Orchestrator. Customers can configure Firewall Rules to block web traffic based on IDS/IPS Signature matching, category, and/or reputation of the URL or IP. To configure firewall settings at the Profile and Edge level, see:

- [Configure Profile Firewall](#)
- [Configure Edge Firewall](#)

## Firewall Logs

Firewall logs are generated:

- When a flow is created (on the condition that the flow is accepted)
- When the flow is closed
- When a new flow is denied
- When an existing flow is updated (due to a firewall configuration change)

With the Stateful Firewall and Enhanced Firewall Services (EFS) features activated, more information can be reported in the firewall logs. The firewall logs will contain the following fields: Time, Segment, Edge, Action, Interface, Protocol, Source IP, Source Port, Destination IP, Destination Port, Extension Headers, Rule, Reason, Bytes Sent, Bytes Received, Duration, Application, Destination Domain, Destination Name, Session ID, Signature ID, Signature, Attack Source, Attack Target, Severity, Category, IDS Alert, IPS Alert, URL, Engine Types, URL Categories, URL Category Filter Action, URL Reputation, URL Reputation Action, IP Categories, and Malicious IP Action.

---

**Note** Not all fields will be populated for all firewall logs. For example, Reason, Bytes Received/Sent, and Duration are fields included in logs when sessions are closed. Signature ID, Signature, Attack Source, Attack Target, Severity, Category, IDS Alert, IPS Alert, URL, Engine Types, URL Categories, URL Category Filter Action, URL Reputation, URL Reputation Action, IP Categories, and Malicious IP Action are populated only for EFS alerts, not for firewall logs.

You can view the firewall logs by using the following firewall features:

- **Hosted Firewall Logging** - Allows you to turn ON or OFF the Firewall Logging feature at the Enterprise Edge level to send Firewall logs to the Orchestrator.

---

**Note** Starting with the 5.4.0 release, for Hosted Orchestrators, the **Enable Firewall Logging to Orchestrator** capability is activated by default for new and existing Enterprises. At the Edge level, customers must activate **Hosted Firewall Logging** to send Firewall logs from the Edge to the Orchestrator. For On-Prem Orchestrators, customers must contact their Operators to activate the **Enable Firewall Logging to Orchestrator** capability.

You can view the Edge Firewall logs in Orchestrator from the **Monitor > Firewall Logs** page. For more information, see [Monitor Firewall Logs](#).

- **Syslog Forwarding** - Allows you to view the logs by sending the logs originating from Enterprise SD-WAN Edge to one or more configured remote servers. By default, the **Syslog Forwarding** feature is deactivated for an Enterprise. To forward the logs to remote Syslog collectors, you must:
  - a Activate the **Syslog Forwarding** feature under **Configure > Edges/Profile > Firewall** tab.

- b Configure a Syslog collector under **Configure > Edges/Profile > Device > Syslog Settings**.  
For steps on how to configure Syslog collector details per segment in the SASE Orchestrator, see [Configure Syslog Settings for Profiles](#).

**Note** For Edge versions 5.2.0 and above, Hosted Firewall Logging is not dependent on Syslog Forwarding configuration.

Read the following topics next:

- [Configure Profile Firewall](#)
- [Configure Edge Firewall](#)
- [Configure Firewall Rule](#)
- [Enhanced Firewall Services](#)
- [Monitor Firewall Logs](#)
- [Troubleshooting Firewall](#)

## Configure Profile Firewall

A Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. SASE Orchestrator supports configuration of stateless and stateful Firewalls for Profiles and Edges.

For more information on Firewall, see [Chapter 22 Firewall Overview](#).

### Configure Profile Firewall

To configure Profile Firewall:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 To configure a Profile Firewall, click the link to the Profile and click the **Firewall** tab.  
Alternatively, you can click the **View** link in the **Firewall** column of the Profile.
- 3 The **Firewall** page appears.

- 4 From the **Firewall** tab, you can configure the following Edge Security and Firewall capabilities:

Field	Description
<b>Edge Access</b>	<p>Allows you to configure a Profile for Edge access. You must make sure to select the appropriate option for Support access, Console access, USB port access, SNMP access, and Local Web UI access under Firewall settings to make the Edge more secure. This will prevent any malicious user from accessing the Edge. By default, Support access, Console access, SNMP access, and Local Web UI access are deactivated for security reasons. For more information, see <a href="#">Configure Edge Access</a>.</p>
<b>Firewall Status</b>	<p>Allows you to turn ON or OFF the Firewall rules, configure Firewall settings, and in-bound ACLs for all Edges associated with the Profile.</p> <p><b>Note</b> By default, this feature is activated. You can deactivate the Firewall function for Profiles by turning the <b>Firewall Status</b> to OFF.</p> <p><b>Attention</b> At the Edge level, once you override the inherited <b>Firewall Status</b> settings, the Edge will stop inheriting any further <b>Firewall Status</b> setting changes from the associated Profile even when the setting is changed at the associated Profile level or when assigned to a different Profile. However, if the <b>Firewall Status</b> setting is turned off in the Profile, this setting will be inherited by the Edge, and it will be deactivated even if the <b>Firewall Status</b> is enabled on the Edge.</p>

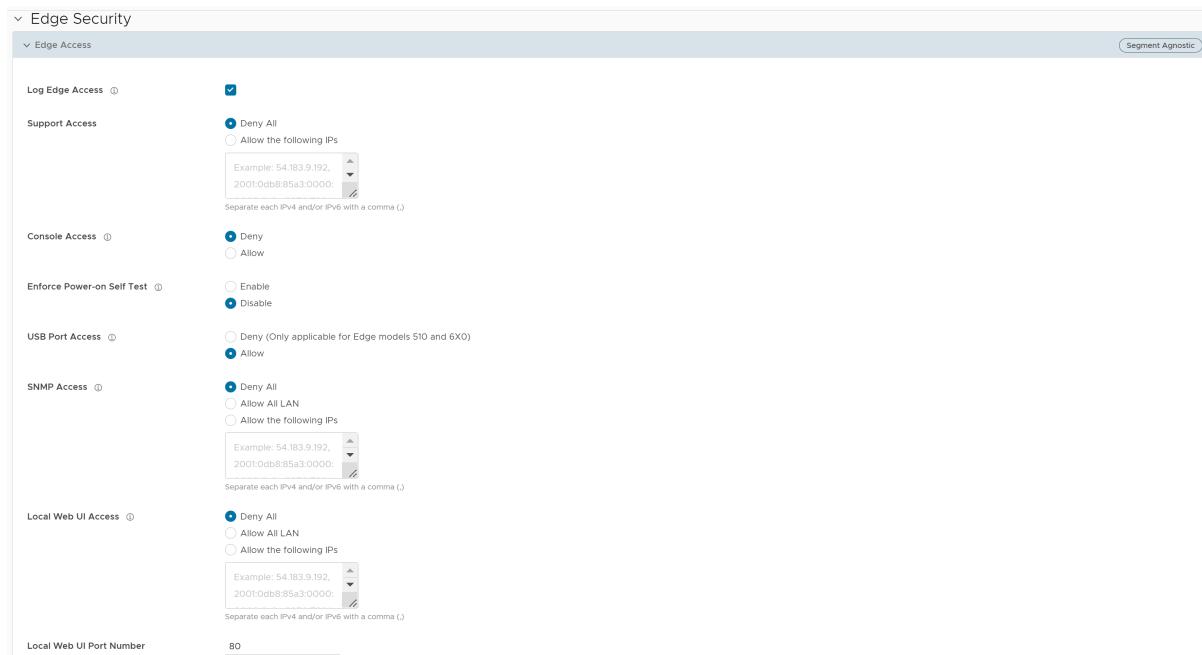
Field	Description
<b>Enhanced Security</b>	<p>Allows you to turn ON or OFF the following security services for all Edges associated with the Profile:</p> <ul style="list-style-type: none"> <li>■ Intrusion Detection/Prevention</li> <li>■ URL Filtering</li> <li>■ Malicious IP Filtering</li> </ul> <p>By default, the Enhanced Security functionality is not activated. If you activate this feature, ensure to activate at least one of the supported security services.</p> <p><b>Note</b> Enhanced Security services are not supported for routed LAN interfaces with dynamic addressing (DHCP Client, DHCPv6 Client, DHCPv6 PD, and SLAAC).</p> <p>For more information, see <a href="#">Configure Enhanced Security Services</a>.</p>
<b>Hosted Firewall Logging</b>	<p>Allows you to turn ON or OFF the Firewall Logging feature at the Enterprise Edge level to send Firewall logs to the Orchestrator.</p> <p><b>Note</b> Starting with the 5.4.0 release, for Hosted Orchestrators, the <b>Enable Firewall Logging to Orchestrator</b> capability is activated by default for new and existing Enterprises. At the Edge level, customers must activate <b>Hosted Firewall Logging</b> to send Firewall logs from the Edge to Orchestrator.</p> <p>You can view the Edge Firewall logs in Orchestrator from the <b>Monitor &gt; Firewall Logs</b> page. For more information, see <a href="#">Monitor Firewall Logs</a>.</p>
<b>Syslog Forwarding</b>	<p>By default, the Syslog Forwarding feature is deactivated for an Enterprise. To collect SASE Orchestrator bound events and Firewall logs originating from Enterprise SD-WAN Edge to one or more centralized remote Syslog collectors (Servers), an Enterprise user must activate this feature at the Edge/Profile level. To configure Syslog collector details per segment in the SASE Orchestrator, see <a href="#">Configure Syslog Settings for Profiles</a>.</p> <p><b>Note</b> You can view both IPv4 and IPv6 Firewall logging details in a IPv4-based Syslog Server.</p>

Field	Description
<b>Firewall Rules</b>	<p>The existing pre-defined Firewall rules are displayed. You can click <b>+ NEW RULE</b> to create a new Firewall rule. For more information, see <a href="#">Configure Firewall Rule</a>. To delete an existing Firewall rule, select the rule and click <b>DELETE</b>.</p> <p>To duplicate a Firewall rule, select the rule and click <b>CLONE</b>.</p> <p>To view all comments added while creating or updating a rule, select the rule and click <b>COMMENT HISTORY</b>.</p> <p>Click <b>Search for Rule</b> if you want to search for a specific rule. You can search the rule by Rule name, IP address, Port/Port range, and Address group and Service group names.</p>
<b>Stateful Firewall</b>	<p>By default, the Stateful Firewall feature is deactivated for an Enterprise. SASE Orchestrator allows you to set session timeout for established and non-established TCP flows, UDP flows, and other flows at the Profile level. Optionally, you can also override the Stateful firewall settings at the Edge level. For more information, see <a href="#">Configure Stateful Firewall Settings</a>.</p>
<b>Network &amp; Flood Protection</b>	<p>To secure all connection attempts in an Enterprise network, VMware SASE Orchestrator allows you to configure Network and Flood Protection settings at the Profile and Edge levels, to protect against the various types of attacks. For more information, see <a href="#">Configure Network &amp; Flood Protection Settings</a>.</p>

## Configure Edge Access

To configure Edge access for Profiles, perform the following steps:

- 1 In the SD-WAN service of the Enterprise portal, go to **Configure > Profiles > Firewall**.
- 2 Under **Edge Security**, click the **Edge Access** expand icon.



- 3 You can configure one or more of the following Edge Access options, and click **Save Changes**:

Field	Description
Log Edge Access	When activated, all access to the Edge is logged, including successful and failed attempts.
Support Access	Select <b>Allow the following IPs</b> if you want to explicitly specify the IP addresses from where you can SSH into this Edge. You can enter both IPv4 and IPv6 addresses separated by comma (,). By default, <b>Deny All</b> is selected.
Console Access	Select <b>Allow</b> to activate Edge access through Physical Console (Serial Port or Video Graphics Array (VGA) Port). By default, <b>Deny</b> is selected and Console login is deactivated after Edge activation.  <b>Note</b> Whenever the console access setting is changed from <b>Allow</b> to <b>Deny</b> or vice-versa, the Edge must be rebooted manually.
Enforce Power-on Self Test	When activated, a failed Power-on Self Test will deactivate the Edge. You can recover the Edge by running factory reset and then reactivate the Edge.

Field	Description
USB Port Access	<p>Select <b>Allow</b> to activate and select <b>Deny</b> to deactivate the USB port access on Edges.</p> <p>This option is available only for Edge models 510 and 6x0.</p> <p><b>Note</b> Whenever the USB port access setting is changed from <b>Allow</b> to <b>Deny</b> or vice-versa, you must reboot the Edge manually if you have access to the Edge and if the Edge is in a remote site, restart the Edge using SASE Orchestrator. For instructions, refer to <a href="#">Remote Actions</a>.</p>
SNMP Access	<p>Allows Edge access from routed interfaces/WAN through SNMP. Select one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Deny All</b> - By default, SNMP access is deactivated for all devices connected to an Edge.</li> <li>■ <b>Allow All LAN</b> - Allows SNMP access for all devices connected to the Edge through a LAN network.</li> <li>■ <b>Allow the following IPs</b> - Allows you to explicitly specify the IP addresses from where you can access the Edge through SNMP. Separate each IPv4 or IPv6 address with a comma (,).</li> </ul>
Local Web UI Access	<p>Allows Edge access from routed interfaces/WAN through a Local Web UI. Select one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Deny All</b> - By default, Local Web UI access is deactivated for all devices connected to an Edge.</li> <li>■ <b>Allow All LAN</b> - Allows Local Web UI access for all devices connected to the Edge through a LAN network.</li> <li>■ <b>Allow the following IPs</b> - Allows you to explicitly specify the IP addresses from where you can access the Edge through Local Web UI. Separate each IPv4 or IPv6 address with a comma (,).</li> </ul>
Local Web UI Port Number	<p>Enter the port number of the local Web UI from where you can access the Edge. The default value is 80.</p>

If you want to override the Edge access settings for a specific Edge, use the **Enable Edge Override** option available on the **Edge Firewall** page.

## Configure Stateful Firewall Settings

To configure Stateful Firewall Settings for Profiles, perform the following steps:

- 1 In the SD-WAN service of the Enterprise portal, go to **Configure > Profiles > Firewall**.
- 2 Under **Configure Firewall**, turn on the **Stateful Firewall** toggle button and then click the expand icon. By default, the timeout sessions are applied for IPv4 addresses.



- 3 You can configure the following Stateful Firewall settings, and click **Save Changes**:

Field	Description
Established TCP Flow Timeout (seconds)	Sets the inactivity timeout period (in seconds) for established TCP flows, after which they are no longer valid. The allowable value ranges from 60 seconds to 15999999 seconds. The default value is 7440 seconds.
Non Established TCP Flow Timeout (seconds)	Sets the inactivity timeout period (in seconds) for non-established TCP flows, after which they are no longer valid. The allowable value ranges from 60 seconds to 604800 seconds. The default value is 240 seconds.
UDP Flow Timeout (seconds)	Sets the inactivity timeout period (in seconds) for UDP flows, after which they are no longer valid. The allowable value ranges from 60 seconds to 15999999 seconds. The default value is 300 seconds.
Other Flow Timeout (seconds)	Sets the inactivity timeout period (in seconds) for other flows such as ICMP, after which they are no longer valid. The allowable value ranges from 60 seconds to 15999999 seconds. The default value is 60 seconds.

**Note** The configured timeout values apply only when the memory usage is below the soft limit. Soft limit corresponds to anything below 60 percent of the concurrent flows supported by the platform in terms of memory usage.

## Configure Network & Flood Protection Settings

VMware SD-WAN provides detection and protection against the following types of attacks to combat exploits at all stages of their execution:

- Denial-of-Service (DoS) attack
- TCP-based attacks - Invalid TCP Flags, TCP Land, and TCP SYN Fragment
- ICMP-based attacks - ICMP Ping of Death and ICMP Fragment
- IP-based attacks - IP Unknown Protocol, IP Options, IPv6 Unknown Protocol, and IPv6 Extension Header.

Attack Type	Description
Denial-of-Service (DoS) attack	<p>A denial-of-service (DoS) attack is a type of network security attack that overwhelms the targeted device with a tremendous amount of bogus traffic so that the target becomes so preoccupied with processing the bogus traffic that legitimate traffic cannot be processed. The target can be a firewall, the network resources to which the firewall controls access, or a specific hardware platform or operating system of an individual host. The DoS attack attempts to exhaust the target device's resources, making the target device unavailable to legitimate users.</p> <p>There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system.</p>
Invalid TCP Flags	<p>Invalid TCP flags attack occurs when a TCP packet has a bad or invalid flag combination. A vulnerable target device will crash due to invalid TCP flag combinations and therefore it is recommended to filter them out. Invalid TCP flags guards against:</p> <ul style="list-style-type: none"> <li>■ A packet that has no flags set in its TCP header such as SYN, FIN, ACK, and so on.</li> <li>■ TCP header that has SYN and FIN flags combined, which are mutually exclusive in reality</li> </ul>
TCP Land	<p>A Land attack is a Layer 4 DoS attack in which a TCP SYN packet is created such that the source IP address and port are set to be the same as the destination IP address and port, which in turn is set to point to an open port on a target device. A vulnerable target device would receive such a message and reply to the destination address effectively sending the packet for reprocessing in an infinite loop. Thus, the device CPU is consumed indefinitely causing the vulnerable target device to crash or freeze.</p>
TCP SYN Fragment	<p>The Internet Protocol (IP) encapsulates a Transmission Control Protocol (TCP) SYN segment in the IP packet to initiate a TCP connection and invoke a SYN/ACK segment in response. Because the IP packet is small, there is no legitimate reason for it to be fragmented. A fragmented SYN packet is anomalous and as such suspect. In a TCP SYN fragment attack, a target server or host is flooded with TCP SYN packet fragments. The host catches the fragments and waits for the remaining packets to arrive so it can reassemble them. By flooding a server or host with connections that cannot be completed, the host's memory buffer overflows, and therefore no further legitimate connections are possible, causing damage to the target host's operating system.</p>

<b>Attack Type</b>	<b>Description</b>
ICMP Ping of Death	<p>An Internet Control Message Protocol (ICMP) Ping of Death attack involves the attacker sending multiple malformed or malicious pings to a target device. While ping packets are small and used for checking the reachability of network hosts, they could be crafted larger than the maximum size of 65535 bytes by attackers.</p> <p>When a maliciously large packet is transmitted from the malicious host, the packet gets fragmented in transit and when the target device attempts to reassemble the IP fragments into the complete packet, the total exceeds the maximum size limit. This could overflow memory buffers initially allocated for the packet, causing a system crash, or freeze, or reboot, as they cannot manage such huge packets.</p>
ICMP Fragment	<p>An ICMP Fragmentation attack is a common DoS attack that involves the flooding of fraudulent ICMP fragments that cannot be defragmented on the target server. As defragmentation can only take place when all fragments are received, temporary storage of such fake fragments takes up memory and may exhaust the available memory resources of the vulnerable target server, resulting in server unavailability.</p>
IP Unknown Protocol	<p>IP Unknown Protocols refers to any protocol not listed in IANA: <a href="https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml">https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml</a>.</p> <p>Enabling IP Unknown Protocol protection blocks IP packets with the protocol field containing a protocol ID number of 143 or greater, as it could lead to a crash if not managed properly on the end device. A cautious stance would be to block such IP packets from entering the protected network.</p>
IP Options	<p>Attackers sometimes configure IP option fields within an IP packet incorrectly, producing either incomplete or malformed fields. Attackers use these malformed packets to compromise vulnerable hosts on the network. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing a packet containing a specific crafted IP option in the packet's IP header. Enabling IP Insecure Options protection blocks transit IP packets with incorrectly formatted IP option fields in the IP packet header.</p>

Attack Type	Description
IPv6 Unknown Protocol	Enabling IPv6 Unknown Protocol protection blocks IPv6 packets with the protocol field containing a protocol ID number of 143 or greater, as it could lead to a crash if not managed properly on the end device. A cautious stance would be to block such IPv6 packets from entering the protected network.
IPv6 Extension Header	An IPv6 Extension Header attack is a DoS attack that occurs due to mishandling of extension headers in an IPv6 packet. The mishandling of IPv6 extension headers creates new attack vectors that could lead to DoS, and which can be exploited for different purposes, such as creating covert channels and routing header O attacks. Enabling this option would drop an IPv6 packet with any extension header except fragmentation headers.

To configure Network and Flood Protection Settings for Profiles, perform the following steps:

- 1 In the SD-WAN service of the Enterprise portal, go to **Configure > Profiles > Firewall**.
- 2 Under **Configure Firewall**, ensure to turn on the **Stateful Firewall** feature.
- 3 Click the **Network & Flood Protection** expand icon.

The screenshot shows the 'Network & Flood Protection' configuration page for the IPv6 tab. It includes the following settings:

- New Connection Threshold: 25 % Connections per second
- Detect Duration: 10 seconds
- Denylist Duration: 10 seconds
- TCP Based Attacks:
  - Invalid TCP Flags:
  - TCP Land:
  - TCP SYN Fragment:
- ICMP Based Attacks:
  - ICMP Ping of Death:
  - ICMP Fragment:
- IP Based Attacks:
  - IPv6 Unknown Protocol:
  - IPv6 Extension Header:

- 4 You can configure the following Network and Flood Protection settings, and click **Save Changes**:

**Note** By default, the network and flood protection settings are applied for IPv4 addresses.

Field	Description
New Connection Threshold (connections per second)	The maximum number of new connections that is allowed from a single source IP per second. The allowable value ranges from 10 percent to 100 percent. The default value is 25 percent.
Denylist	Select the checkbox to block a source IP address, which is violating the new connection threshold by sending flood traffic either due to misconfiguration of the network or malicious user attacks.
	<b>Note</b> The <b>New Connection Threshold (connections per second)</b> settings will not work unless <b>Denylist</b> is selected.
Detect Duration (seconds)	<p>Before blocking a Source IP address, it is the grace time duration for which the violating source IP is allowed to send traffic flows.</p> <p>If a host sends flood traffic of new connection requests (port scan, TCP SYN flood, and so on) exceeding the maximum allowed connection per second (CPS) for this duration, it will be considered as eligible for denylisting instead of immediately denylisting it as soon as it exceeds the CPS per source once. For example, consider that the maximum allowed CPS is 10 with detect duration of 10 seconds, if the host floods new connection requests greater than 100 requests for 10 seconds, then the host will be denylisted.</p> <p>The allowable value ranges from 10 seconds to 100 seconds. The default value is 10 seconds.</p>
Denylist Duration (seconds)	The time duration for which the violated source IP is blocked from sending any packets. The allowable value ranges from 10 seconds to 86400 seconds. The default value is 10 seconds.
TCP Half-Open Threshold Per Destination	The maximum number of half-open TCP connections that is allowed per destination. The allowable value ranges from 1 percent to 100 percent.
TCP Based Attacks	<p>Supports protection from the following TCP-based attacks by enabling the respective checkboxes:</p> <ul style="list-style-type: none"> <li>■ Invalid TCP Flags</li> <li>■ TCP Land</li> <li>■ TCP SYN Fragment</li> </ul>

Field	Description
ICMP Based Attacks	Supports protection from the following ICMP-based attacks by enabling the respective checkboxes: <ul style="list-style-type: none"><li>■ ICMP Ping of Death</li><li>■ ICMP Fragment</li></ul>
IP Based Attacks	Supports protection from the following IP-based attacks by enabling the respective checkboxes: <ul style="list-style-type: none"><li>■ IP Unknown Protocol</li><li>■ IP Options</li><li>■ IPv6 Unknown Protocol</li><li>■ IPv6 Extension Header</li></ul>

## Configure Edge Firewall

By default, all the Edges inherit the Firewall rules, Security Features settings, Stateful Firewall settings, Network and Flood Protection settings, Firewall Logging, Syslog Forwarding, and Edge access configurations from the associated Profile.

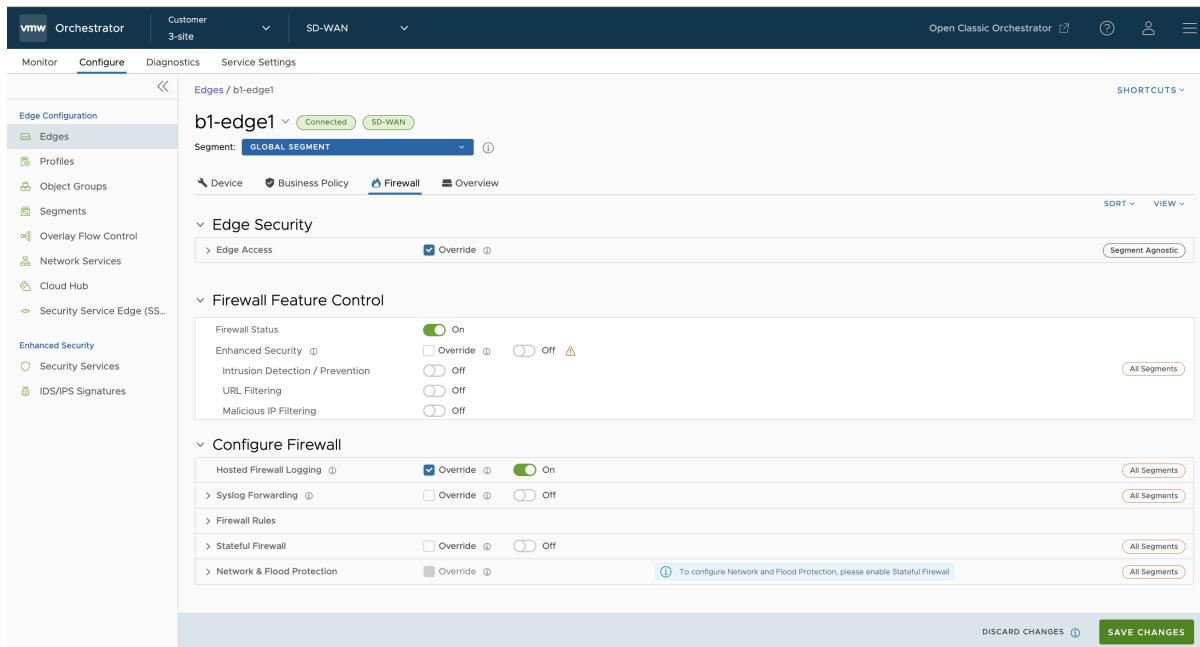
Under the **Firewall** tab of the **Edge Configuration** dialog, you can view all the inherited Firewall rules in the **Rule From Profile** area. Optionally, at the Edge-level, you can also override the inherited Firewall rules and various Firewall settings.

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
- 2 Select an Edge for which you want to override the inherited Firewall settings and click on the **Firewall** tab.
- 3 Select the **Override** checkbox against the various Firewall settings if you want to modify the inherited Firewall rules and settings for the selected Edge.

---

**Note** The Edge override rules will take priority over the inherited Profile rules for the Edge. Any Firewall override match value that is the same as any Profile Firewall rule will override that Profile rule.

---



- At the Edge level, you can configure Port Forwarding and 1:1 NAT IPv4 or IPv6 rules individually by navigating to **Additional Settings > Inbound ACLs**. For detailed information, see [Port Forwarding Rules](#) and [1:1 NAT Settings](#).

**Note** By default, all inbound traffic will be blocked unless the Port Forwarding and 1:1 NAT Firewall Rules are configured. The outside IP will always be that of WAN IP or IP address from WAN IP subnet.

**Note** When configuring IPv6 Port Forwarding and 1:1 NAT rules, you can enter only Global or Unicast IP addresses and cannot enter Link Local Address.

## Port Forwarding and 1:1 NAT Firewall Rules

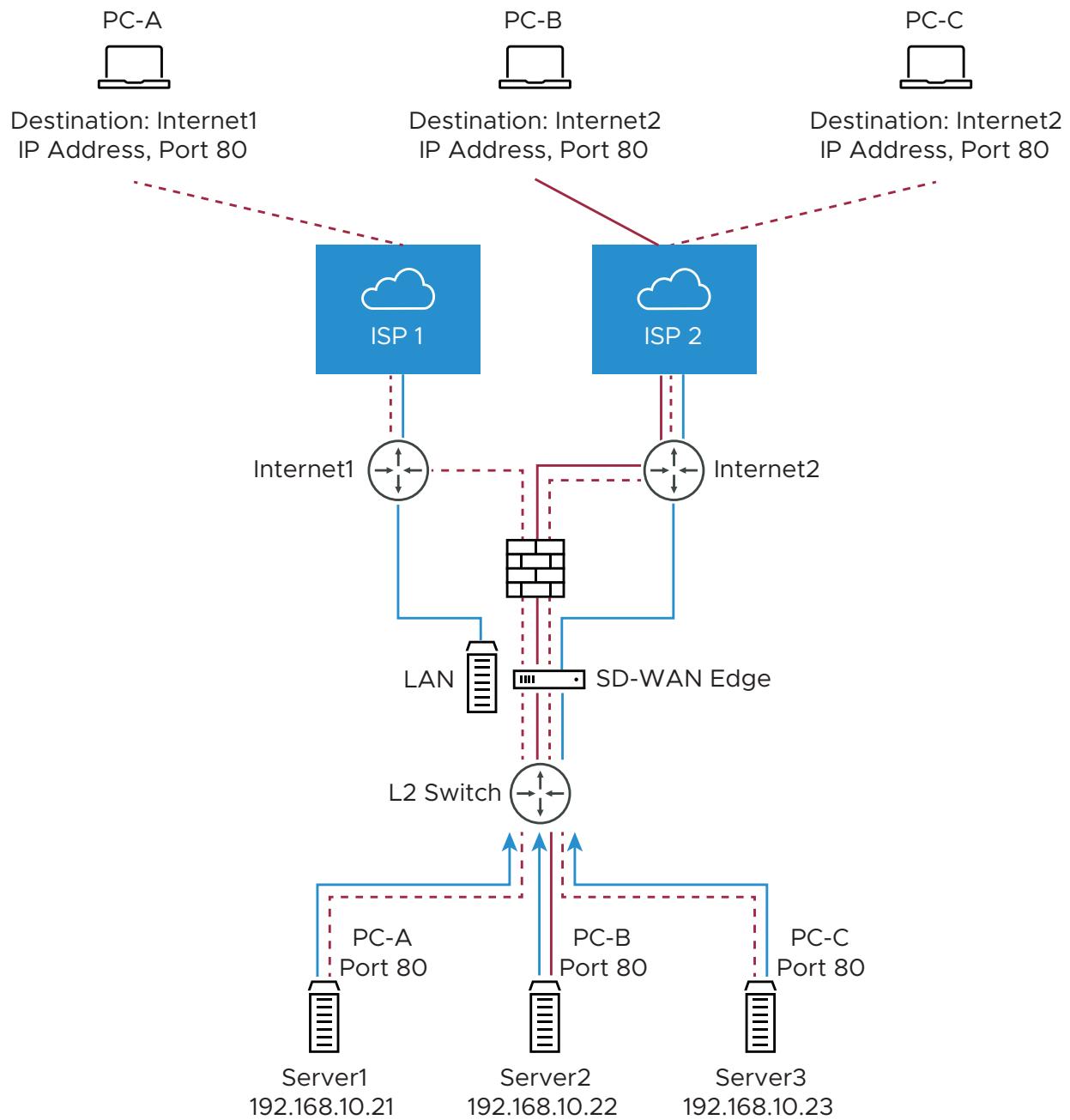
**Note** You can configure Port Forwarding and 1:1 NAT rules individually only at the Edge level.

Port Forwarding and 1:1 NAT firewall rules give Internet clients access to servers connected to an Edge LAN interface. Access can be made available through either Port Forwarding Rules or 1:1 NAT (Network Address Translation) rules.

### Port Forwarding Rules

Port forwarding rules allow you to configure rules to redirect traffic from a specific WAN port to a device (LAN IP/ LAN Port) within the local subnet. Optionally, you can also restrict the inbound traffic by an IP or a subnet. Port forwarding rules can be configured with the Outside IP which is on the same subnet of the WAN IP. It can also translate outside IP addresses in different subnets than the WAN interface address if the ISP routes traffic for the subnet towards the SD-WAN Edge.

The following figure illustrates the port forwarding configuration.



In the **Port Forwarding Rules** section, you can configure port forwarding rules with IPv4 or IPv6 address by clicking the **+Add** button and then entering the following details.

Name	Protocol	Interface	Outside IP	WAN Port(s)	LAN IP	LAN Port	Segment	Remote IP/Subnet	Log
Server1	TCP	GE3	10.1.1.0	80	192.168.10.21	80	Global Segment	Enter IPv4	<input checked="" type="checkbox"/> Enable

\* Required

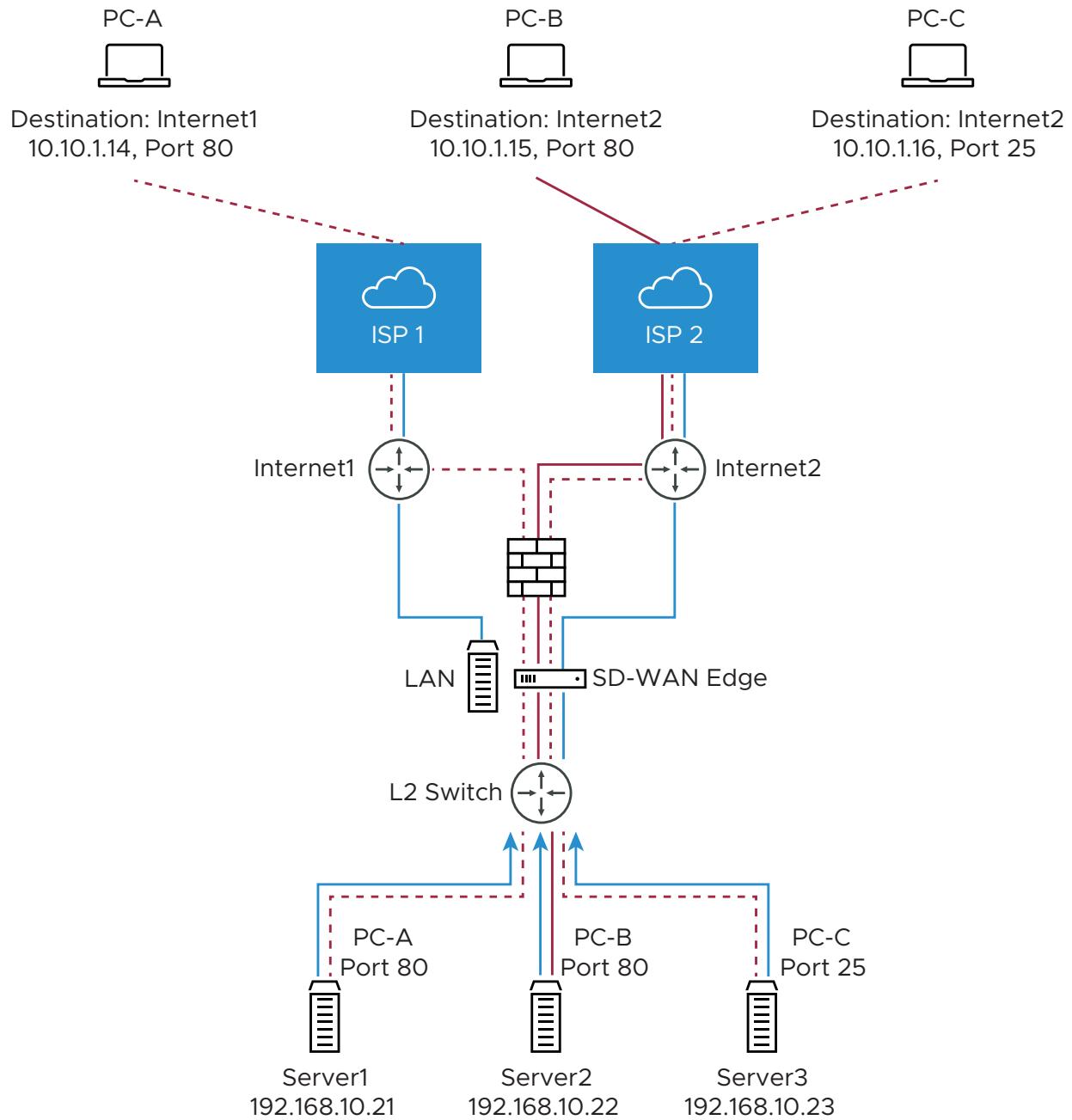
1 item

- 1 In the **Name** text box, enter a name (optional) for the rule.
- 2 From the **Protocol** drop-down menu, select either TCP or UDP as the protocol for port forwarding.
- 3 From the **Interface** drop-down menu, select the interface for the inbound traffic.
- 4 In the **Outside IP** text box, enter the IPv4 or IPv6 address using which the host (application) can be accessed from the outside network.
- 5 In the **WAN Ports** text box, enter a WAN port or a range of ports separated with a dash (-), for example 20-25.
- 6 In the **LAN IP** and **LAN Port** text boxes, enter the IPv4 or IPv6 address and port number of the LAN, where the request will be forwarded.
- 7 From the **Segment** drop-down menu, select a segment the LAN IP will belong to.
- 8 In the **Remote IP/subnet** text box, specify an IP address of an inbound traffic that you want to be forwarded to an internal server. If you do not specify any IP address, then it will allow any traffic.
- 9 Select the **Log** check box to activate logging for this rule.
- 10 Click **Save Changes**.

## 1:1 NAT Settings

These are used to map an Outside IP address supported by the SD-WAN Edge to a server connected to an Edge LAN interface (for example, a web server or a mail server). It can also translate outside IP addresses in different subnets than the WAN interface address if the ISP routes traffic for the subnet towards the SD-WAN Edge. Each mapping is between one IP address outside the firewall for a specific WAN interface and one LAN IP address inside the firewall. Within each mapping, you can specify which ports will be forwarded to the inside IP address. The '+' icon on the right can be used to add additional 1:1 NAT settings.

The following figure illustrates the 1:1 NAT configuration.



In the **1:1 NAT Rules** section, you can configure 1:1 NAT rules with IPv4 address or IPv6 address by clicking the **+Add** button and then entering the following details.

The screenshot shows a table-based configuration interface for 1:1 NAT Rules. At the top, there are buttons for '+ ADD', 'DELETE', and 'CLONE'. The table has two columns: '1:1 NAT Rules' and 'Allowed Traffic Source'. The '1:1 NAT Rules' column contains fields for 'Name' (Server2), 'Outside IP' (10.10.1.2), 'Interface' (GE3), 'Inside (LAN) IP' (192.168.10.24), 'Segment' (Global Segment), and 'Outbound Traffic' (checkbox 'Enable' checked). The 'Allowed Traffic Source' column contains fields for 'Protocol' (All), 'Port(s)' (Enter port), 'Remote IP/Subnet' (Enter IPv4), and 'Log' (checkbox 'Enable' checked). A note at the bottom left says '\* Required' and a note at the bottom right says '1 item'.

1:1 NAT Rules						Allowed Traffic Source				
		Protocol	Port(s)	Remote IP/Subnet	Log					
<input type="checkbox"/>	Name	Outside IP *	Interface *	Inside (LAN) IP *	Segment * ⓘ	Outbound Traffic ⓘ	All	Enter port	Enter IPv4	<input checked="" type="checkbox"/> Enable
<input type="checkbox"/>	Server2	10.10.1.2	GE3 ⓘ	192.168.10.24	Global Segment ⓘ	<input type="checkbox"/> Enable				

\* Required  
1 item

- 1 In the **Name** text box, enter a name for the rule.
- 2 In the **Outside IP** text box, enter the IPv4 or IPv6 address with which the host can be accessed from an outside network.
- 3 From the **Interface** drop-down menu, select the WAN interface where the Outside IP address will be bound.
- 4 In the **Inside (LAN) IP** text box, enter the actual IPv4 or IPv6 (LAN) address of the host.
- 5 From the **Segment** drop-down menu, select a segment the LAN IP will belong to.
- 6 Select the **Outbound Traffic** check box, if you want to allow traffic from LAN Client to Internet being NATed to Outside IP address.
- 7 Enter the Allowed Traffic Source (Protocol, Ports, Remote IP/Subnet) details for mapping in the respective fields.
- 8 Select the **Log** check box to activate logging for this rule.
- 9 Click **Save Changes**.

## Configure Firewall Rule

You can configure Firewall rules at the Profile and Edge levels to allow, drop, reject, or skip inbound and outbound traffic. If the stateful firewall feature is activated, the firewall rule will be validated to filter both inbound and outbound traffic. With a stateless firewall, you can only filter outbound traffic. The firewall rule matches parameters such as IP addresses, ports, VLAN IDs, Interfaces, MAC addresses, domain names, protocols, object groups, applications, DSCP tags, URL categories, URL reputation score, and Security Service groups. When a data packet matches the match conditions, the associated action or actions are taken. If a packet matches no parameters, then a default action is taken on the packet.

To configure a firewall rule at the Profile level, perform the following steps.

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.

- 2 Select a Profile to configure a firewall rule, and click the **Firewall** tab.

From the **Profiles** page, you can navigate to the **Firewall** page directly by clicking the **View** link in the **Firewall** column of the Profile.

- 3 Go to the **Configure Firewall** section and under the **Firewall Rules** area, click **+ NEW RULE**. The **New Rule** page appears.

- 4 In the **Rule Name** text box, enter a unique name for the Rule. To create a firewall rule from an existing rule, select the rule to be duplicated from the **Duplicate Rule** drop-down menu.

5 In the **Match** section, configure the match conditions for the rule:

Field	Description
IP Version	<p>By default, the <b>IPv4 and IPv6</b> address type is selected. You can configure the Source and Destination IP addresses according to the selected Address Type, as follows:</p> <ul style="list-style-type: none"> <li>■ <b>IPv4</b> – Allows to configure only IPv4 addresses as Source and Destination.</li> <li>■ <b>IPv6</b> – Allows to configure only IPv6 addresses as Source and Destination.</li> <li>■ <b>IPv4 and IPv6</b> – Allows to configure both IPv4 and IPv6 addresses in the matching criteria. If you choose this mode, you cannot configure the Source or Destination IP address.</li> </ul> <p><b>Note</b> When you upgrade, the firewall rules from previous versions are moved to IPv4 mode.</p>
Source	<p>Allows to specify the source for packets. Select any of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Any</b> - Allows all source addresses by default.</li> <li>■ <b>Object Group</b> - Allows you to select a combination of address group and service group. For more information, see <a href="#">Chapter 31 Object Groups</a> and <a href="#">Configure Firewall Rule with Object Group</a>.</li> </ul> <p><b>Note</b> In a Firewall policy, when using an Object Group to match the Source traffic, domain-based address group is not supported.</p> <ul style="list-style-type: none"> <li>■ <b>Define</b> - Allows you to define the source traffic to a specific VLAN, Interface, IPv4 or IPv6 Address, MAC Address, or Transport Port. Select one of the following options:           <ul style="list-style-type: none"> <li>■ <b>VLAN</b> - Matches traffic from the specified VLAN, selected from the drop-down menu.</li> </ul> <p><b>Note</b> When using a VLAN to match source or destination traffic in a firewall policy, it takes into account both local and remote VLANs.</p> <ul style="list-style-type: none"> <li>■ <b>Interface and IP Address</b> - Matches traffic from the specified interface and IPv4 or IPv6 address, selected from the drop-down menu.</li> </ul> <p><b>Note</b> If an interface cannot be selected, then the interface is either not activated or not assigned to this segment.</p> <p><b>Note</b> If you select <b>IPv4 and IPv6</b> (Mixed mode) as the Address Type, then the traffic is matched based on only the specified interface.</p> </li> </ul>

Field	Description
	<p>Along with the IP address, you can specify one of the following address types to match the source traffic:</p> <ul style="list-style-type: none"> <li>■ <b>CIDR prefix</b> - Choose this option if you want the network defined as a CIDR value (for example: 172.10.0.0 /16).</li> <li>■ <b>Subnet mask</b> - Choose this option if you want the network defined based on a Subnet mask (for example, 172.10.0.0 255.255.0.0).</li> <li>■ <b>Wildcard mask</b> - Choose this option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP, or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a '1' within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values, and the last octet is a variable value. This option is available only for IPv4 addresses.</li> <li>■ <b>Mac Address</b> - Matches traffic based on the specified MAC address.</li> <li>■ <b>Transport Port</b> - Matches traffic from the specified source port or port range.</li> </ul>

Field	Description
Destination	<p>Allows to specify the destination for packets. Select any of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Any</b> - Allows all destination addresses by default.</li> <li>■ <b>Object Group</b> - Allows you to select a combination of address group and service group. For more information, see <a href="#">Chapter 31 Object Groups</a> and <a href="#">Configure Firewall Rule with Object Group</a>.</li> <li>■ <b>Define</b> - Allows you to define the destination traffic to a specific VLAN, Interface, IPv4 or IPv6 Address, Domain Name, Protocol, or Port. Select one of the following options: <ul style="list-style-type: none"> <li>■ <b>VLAN</b> - Matches traffic from the specified VLAN, selected from the drop-down menu.</li> </ul> <p><b>Note</b> When using a VLAN to match source or destination traffic in a firewall policy, it takes into account both local and remote VLANs.</p> <hr/> <li>■ <b>Interface</b> - Matches traffic from the specified interface, selected from the drop-down menu.</li> </li></ul> <p><b>Note</b> If an interface cannot be selected, then the interface is either not activated or not assigned to this segment.</p> <hr/> <ul style="list-style-type: none"> <li>■ <b>IP Address</b> - Matches traffic for the specified IPv4 or IPv6 address and Domain name.</li> </ul> <p><b>Note</b> If you select <b>IPv4 and IPv6 (Mixed mode)</b> as the Address Type, then you cannot specify the IP address as the destination.</p> <p>Along with the IP address, you can specify one of the following address types to match the source traffic: <b>CIDR prefix</b>, <b>Subnet mask</b>, or <b>Wildcard mask</b>.</p> <p>Use the <b>Domain Name</b> field to match the entire domain name or a portion of the domain name. For example, <code>\salesforce\</code> will match traffic to <code>\mix\</code>.</p> <ul style="list-style-type: none"> <li>■ <b>Transport</b> - Matches traffic from the specified source port or port range.</li> </ul> <p><b>Protocol</b> - Matches traffic for the specified protocol, selected from the drop-down menu. The supported protocols are GRE, ICMP, TCP, and UDP.</p> <p><b>Note</b> ICMP is not supported in Mixed mode (IPv4 and IPv6).</p>
Application	<p>Select any of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Any</b> - Applies the firewall rule to any application by default.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>■ <b>Define</b> - Allows to select an application and Differentiated Services Code Point (DSCP) flag to apply a specific firewall rule.</li> </ul> <p><b>Note</b> When creating firewall rules matching an application, the firewall depends on the DPI (Deep Packet Inspection) Engine to identify the application to which a particular flow belongs. The DPI will not be able to determine the application based on the first packet. The DPI Engine usually needs the first 5-10 packets in the flow to identify the application, but the firewall needs to classify and forward the flow from the very first packet. This may cause the first flow to match a more generalized rule in the firewall list. Once the application has been correctly identified, any future flows matching the same tuples will be reclassified automatically and hit the correct rule.</p> <p>For more information on specific use cases matching FTPv6 Firewall/Business policy rule, see <a href="#">Edge Firewall Support for FTPv6</a>.</p>

- 6 In the **Firewall Action** section, configure the actions to be performed when the traffic matches the defined criteria.

Field	Description
Firewall	<p>Select any of the following actions the firewall should perform on packets when the conditions of the rule are met:</p> <ul style="list-style-type: none"> <li>■ <b>Allow</b> - Allows the data packets by default.</li> <li>■ <b>Drop</b> - Drops the data packets silently without sending any notification to the source.</li> <li>■ <b>Reject</b> - Drops the packets and notifies the source by sending an explicit reset message.</li> <li>■ <b>Skip</b> - Skips the rule during lookups and processes the next rule. However, this rule will be used at the time of deploying <b>SD-WAN</b>.</li> </ul> <p><b>Note</b> You will be able to configure the <b>Reject</b> and <b>Skip</b> actions only if the <b>Stateful Firewall</b> feature is activated for Profiles and Edges.</p>
Log	<p>Select this checkbox if you want a log entry to be created when this rule is triggered.</p>

- 7 While creating or updating a Firewall rule, you can add comments about the rule in the **New Comment** field in the **Comment** section. A maximum of 50 characters is allowed and you can add any number of comments for the same rule.

- 8 In the **Security Services** section, configure the security service for the rule by selecting a Security Service Group from the drop-down menu. A summary of all the security services configured within the Security Service Group will be displayed. You can click the **View** button against each of the security services to view the configuration details.

From the **Firewall** page, you can create a new Security Service Group, by clicking the **+ Create New** link on the right side of the **Security Services** section.

---

**Note** Security services can be activated in the rule only if the Firewall action is **Allow**. If the Firewall action is anything other than **Allow**, Security services will be deactivated.

---

- 9 After configuring all the required settings, click **Create**.

A firewall rule is created for the selected Profile, and it appears under the **Firewall Rules** area of the **Profile Firewall** page.

---

**Note** The rules created at the Profile level cannot be updated at the Edge level. To override the rule, user needs to create the same rule at the Edge level with new parameters to override the Profile level rule.

---

In the **Firewall Rules** area of the **Profile Firewall** page, you can perform the following actions:

- **DELETE** - To delete existing Firewall rules, select the checkboxes prior to the rules and click **DELETE**.
- **CLONE** - To duplicate a Firewall rule, select the rule and click **CLONE**.
- **COMMENT HISTORY** - To view all comments added while creating or updating a rule, select the rule and click **COMMENT HISTORY**.
- **Search for Rule** - Allows to search the rule by Rule name, IP address, Port/Port range, and Address group and Service group names.

## Edge Firewall Support for FTPv6

File Transfer Protocol version 6 (FTPv6) is an updated version of the classic FTP protocol that enables the transfer of files between a client and a server over an Internet Protocol version 6 (IPv6) network. It builds upon the principles of FTPv4 while adding support for IPv6, which provides a larger address space and improved network routing capabilities.

The following are some of the high-level use cases with FTPv6 Firewall/Business policy:

- Allowing FTPv6 traffic from specific/random hosts
- Blocking FTPv6 traffic from specific/random hosts
- Allowing FTPv6 traffic on specific/random ports
- Blocking FTPv6 traffic on specific/random ports

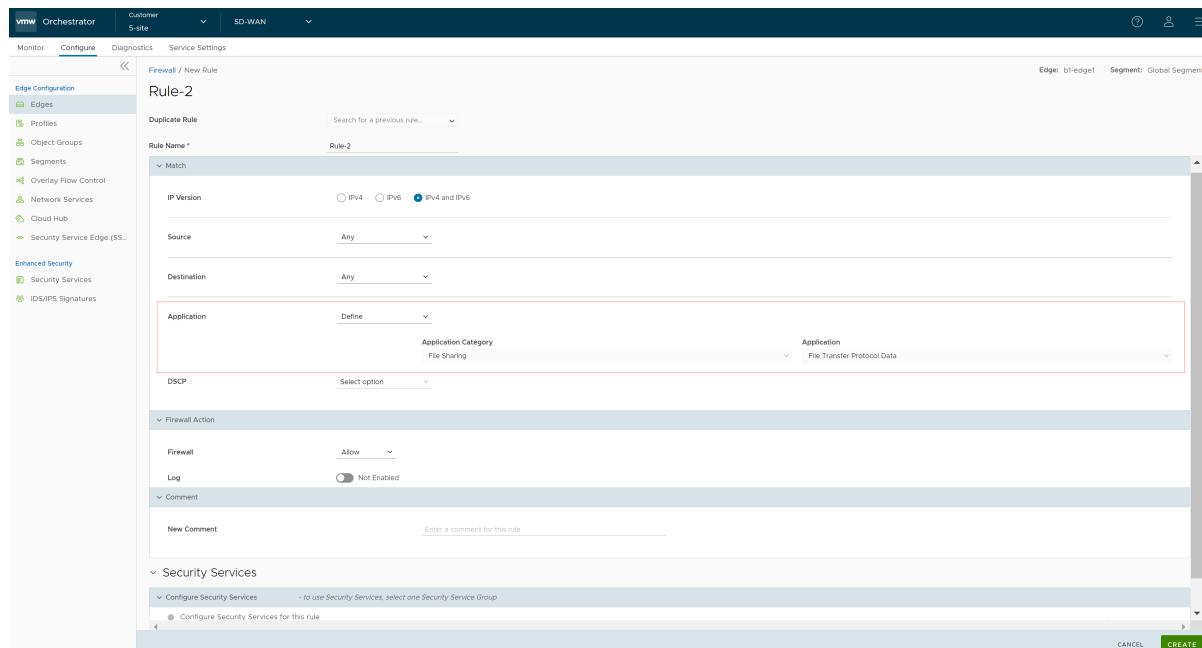
## Use Case: Identifying Passive FTPv6 Traffic and Applying FTP Firewall Rules

In this scenario, Passive FTPv6 mode uses random port numbers for data transfer, making it challenging to identify FTP traffic as it does not use standard ports 20 and 21. An efficient Deep Packet Inspection (DPI) solution is required to detect passive FTPv6 traffic and apply appropriate firewall rules for allowing or denying access.

The release 5.4 supports application identification for both FTPv4/FTPv6 Active and Passive modes when using VMware SD-WAN service. This enables customers to easily identify and permit passive FTPv6 traffic using a generic FTP firewall rule. This streamlined process benefits the customer by simplifying the management of FTPv6 traffic while ensuring secure and controlled access.

Steps to configure a firewall rule matching the FTP application at the Edge level:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Select an Edge to configure a firewall rule matching the FTP application, and click the **Firewall** tab.
- 3 Go to the **Configure Firewall** section and under **Firewall Rules** area, click **+ NEW RULE**. The **Configure Rule** dialog box appears.
- 4 In the **Rule Name** text box, enter a unique name for the Rule.
- 5 In the **Match** section, from the **Applications** drop-down menu select **Define**. This allows you to select the Application Category and Application to apply a specific firewall rule.



- 6 From the **Application Category** menu, select **File Sharing**, and from the **Application** drop-down menu select either **File Transfer Protocol** (for Control connection) or **File Transfer Protocol Data** (for Data connection).

- 7 Click **Create**. A firewall rule matching the FTP application is created at the Edge level and it appears in the **Firewall Rules** area as shown in the following screenshot.

**Note** Similarly, you can configure a Business Policy rule matching the FTP application at the Edge level by following the same steps from the **Business Policy** tab

## Enhanced Firewall Services

This section provides details about how to configure and monitor Enhanced Firewall Services (EFS).

### Enhanced Firewall Services Overview

Enhanced Firewall Services (EFS) provide additional EFS security functionalities on VMware SD-WAN Edges. The VMware Security powered EFS functionality supports URL Category filtering, URL Reputation filtering, Malicious IP filtering, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) services on VMware SD-WAN Edges. The Edge Enhanced Firewall Services (EFS) protect Edge traffic from intrusions across Branch-to-Branch, Branch-to-Hub, or Branch-to-Internet traffic patterns.

Currently, SD-WAN Edge Firewall provides stateful inspection along with application identification without additional EFS security features. While the stateful Firewall SD-WAN Edge provides security, it is not adequate and creates a gap in providing EFS security integrated natively with VMware SD-WAN. Edge EFS addresses these security gaps and offers enhanced threat protection natively on the SD-WAN Edge in conjunction with VMware SD-WAN.

Customers can configure and manage the EFS features using the Firewall functionality in VMware SASE Orchestrator. Customers can configure Firewall Rules to block web traffic based on IDS/IPS Signature matching, category, and/or reputation of the URL or IP.

## Limitations

- When EFS is activated and IDS/IPS is configured, only static addressing is supported. Do not use the Dynamic address on LAN networks such as DHCPv4 Client, DHCPv6 Client, DHCPv6 PD, and IPv6 SLAAC.

If the dynamic addressing is used and the address range is outside the private address range in the case of IPv4 and the ULA address range in the case of IPv6 described in RFC1918, rule matching might not happen due to the address not being part of HOME\_NETWORK setting in suricata.yaml.

## Configure Enhanced Security Services

A customer with the Enhanced Firewall Services (EFS) functionality activated at the Global Settings level in VMware SASE Orchestrator can now individually configure and manage Security services such as URL Filtering (URL Category filtering, URL Reputation filtering), Malicious IP filtering, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). To block user traffic based on IDS/IPS Signature matching, category, and/or reputation of the URL or IP, the customer must create a Security Service Group using the pre-configured security services and associate that Security Service Group with the Firewall rules.

### Before You Begin

For the EFS feature to work:

- Ensure the Edge version is 6.0.0 for the URL Filtering (URL Category and URL Reputation) and Malicious IP filtering to work as expected. For the IDS and IPS service configuration, ensure the Edge version is 5.2.0 and later.
- Ensure the EFS feature is activated at the Enterprise level. Contact your Operator if you would want the EFS feature to be activated. An Operator can activate the EFS feature from the **SD-WAN > Global Settings > Customer Configuration > SD-WAN Settings > Feature Access** UI page.

In the **SD-WAN** service of the Enterprise portal, to configure Security Services, click **Configure > Enhanced Security > Security Services**. The **Security Services** page appears.

Customers can configure the following Security Services:

- Configure URL Categories Service
- Configure URL Reputation Service
- Configure Malicious IP Service
- Configure IDS/IPS Security Service
- Configure Security Service Group

## Configure URL Categories Service

URL Categories service consists of assigning one or more categories to URLs/Domains. As there are hundreds of millions of websites and URLs, it is very tedious to configure the policy for individual URLs, so these URLs are already mapped to a specific category, and then filtering policy is applied over the categories.

---

**Note** An URL is classified as having an "Unknown" category when there is no categorization information available from the URL Filtering service.

---

Currently, there are more than 80 URL categories including Social Networking, Financial Services, Phishing, and so on.

To configure URL Categories, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Enhanced Security > Security Services**. The **Security Services** page appears.
- 2 Click the **URL Categories** tab and click **+ADD RULE**. The **Configure URL Category Service** pop-up window appears.

## Configure URL Category Service

Name \*

Description   
Maximum 256 characters

Select Categories

Show only selected

	Blocked Categories
<input type="checkbox"/>	Abused Drugs
<input type="checkbox"/>	Nudity

Show only selected

	Allow Categories
<input type="checkbox"/>	Uncategorized
<input type="checkbox"/>	Real Estate
<input type="checkbox"/>	Financial Services
<input type="checkbox"/>	Business and Economy
<input type="checkbox"/>	Computer and Internet Info
<input type="checkbox"/>	Auctions

Show only selected

	Monitor Categories
<input type="checkbox"/>	Computer and Internet Security
<input type="checkbox"/>	Military

Logs are automatically captured for Blocked categories rule match.

Logs are not captured for Allowed categories rule match.

By default, "Unknown" categories will be "Blocked". Uncheck to "Allow" Unknown categories.

**CANCEL** **SAVE CHANGES**

- 3 Enter a unique name for the URL Categories service and provide a description as needed.
- 4 From the **Allow Categories** list, you can select the categories that you want to block and move it to the **Blocked Categories** list by using the Left arrow button. Similarly, you can select the categories that you want to allow and log and move it to the **Monitor Categories** list by using the Right arrow button.

**Note** Logs are captured automatically for firewall rules that match the Blocked and Monitor Categories. For Allow Categories, traffic is allowed but not logged.

- 5 To allow URLs with **Unknown** categories, unselect the checkbox at the bottom.

**Note** By default, **Unknown** categories will be blocked.

- 6 Click **Save Changes**. A URL Category service rule is created, and it appears in the table in the **URL Categories** page.

Name	Description	Blocked Categories	Monitor Categories	Used By - Security Group	Last Modified
URLCat1		2	2	2	Feb 1, 2024, 4:36:13 PM

- 7 Click the link to the Security Service to modify the settings. To delete a Security Service, select the checkbox before the group and click **Delete**.

**Note** Security Services in use cannot be deleted. If you want to delete a Security Service, it must first be removed from the associated Security Service Group and firewall rules.

To view the list of blocked categories, monitor categories, and security groups associated with the security service, click the respective links under the **Blocked Categories**, **Monitor Categories**, and **Used By - Security Group** columns.

## Configure URL Reputation Service

URL reputation provides the trustworthiness of the Website. The reputation score classification for URL(s) and IP addresses is as given below:

- 81-100: Trustworthy
  - 61-80: Low risk
  - 41-60: Medium risk
  - 21-40: Suspicious
  - 01-20: High risk
- 
- Note** Trustworthy is the safest Reputation and has the least amount of risk.

URL Reputation service looks up the score of destination URLs and blocks the Edge traffic if their scores indicate a threat.

To configure URL Reputation, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Enhanced Security > Security Services**. The **Security Services** page appears.
- 2 Click the **URL Reputation** tab and click **+ADD RULE**. The **Configure URL Reputation Service** pop-up window appears.

X

## Configure URL Reputation Service

Name *	<input type="text" value="URL Rep1"/>
Description	<input type="text" value="Enter Description (Optional)"/> Maximum 256 characters
<b>Select a minimum acceptable Reputation to allow traffic to/from a URL</b>	
Minimum Acceptable Reputation	<input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;" type="button" value="Trustworthy"/> <span style="font-size: small;">▼</span> <span style="font-size: small;"> ⓘ</span>
Blocked Reputation(s)	<input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;" type="button" value="Low Risk"/> <input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;" type="button" value="Moderate Risk"/> <input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;" type="button" value="Suspicious"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="High Risk"/> <span style="font-size: small;">▼</span>
Capture Logs	<input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;" type="button" value="Trustworthy"/> <span style="font-size: small;">▼</span>
<input checked="" type="checkbox"/> "Unknown" Reputations will be "Blocked". Uncheck to "Allow" URLs with Unknown Reputations.	
<input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;" type="button" value="CANCEL"/> <input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px;" type="button" value="SAVE CHANGES"/>	

- 3 Enter a unique name for the URL Reputation service and provide a description as needed.
- 4 From the **Minimum Acceptable Reputation** drop-down menu, select an acceptable reputation to allow traffic to/from a URL. Once you configure the minimum acceptable reputation, all the other Reputations that need to be blocked are automatically listed in the **Blocked Reputation(s)** box. Traffic to/from any URL below the selected URL reputation level will be blocked and logged automatically, and traffic above the selected URL reputation level will be allowed but not logged automatically. You can specify the reputations to log using the **Capture Logs** drop-down menu.
- 5 To allow URLs with **Unknown** Reputations, unselect the checkbox at the bottom. An URL is classified as having an "Unknown" reputation when there is no reputation information available from the **URL Filtering** service.

**Note** By default, **Unknown** Reputations will be blocked.

- 6 Click **Save Changes**. A URL Reputation service rule is created, and it appears in the table in the **URL Reputation** page.

Name	Description	Minimum Acceptable Reputation	Capture Logs	Used By - Security Group	Last Modified
URL.Repl	Trustworthy	Trustworthy	2		2024-02-01T10:08:10.000Z

- Click the link to the Security Service to modify the settings. To delete a Security Service, select the checkbox before the group and click **Delete**.

## Configure Malicious IP Service

Blocking IP addresses can be useful for protecting a network or website from malicious activity. IP reputation score assigned by Webroot provides the trustworthiness of IP. Malicious IP service looks up the IP reputation score of destination IPs and blocks the Edge traffic if their scores indicate a malicious activity.

To configure Malicious IPs, perform the following steps:

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Enhanced Security > Security Services**. The **Security Services** page appears.
- Click the **Malicious IP** tab and click **+ADD RULE**. The **Configure Malicious IP Filtering Service** pop-up window appears.

Configure Malicious IP Filtering Service

Name \* MaliIP

Description Enter Description (Optional)

Select action to be taken when IPv4 traffic to malicious IP is detected

Action Block

**SAVE CHANGES**

- Enter a unique name for the Malicious IP service and provide a description as needed.
- From the **Action** drop-down menu, select an action to be taken when IPv4 traffic to/from malicious IP is detected. You can select any one of the following options:
  - Monitor - Allows and logs the IPv4 traffic automatically from the Malicious IP service.
  - Block - Blocks and logs the IPv4 traffic automatically from the Malicious IP service.

**Note** If the IP is not malicious, IPv4 traffic is allowed but not logged.

- 5 Click **Save Changes**. A Malicious IP service rule is created, and it appears in the table in the **Malicious IP** page.

Name	Description	Action	Used By - Security Group	Last Modified
MailIP1		Block	2	2024-02-01T11:09:33.000Z

- 6 Click the link to the Security Service to modify the settings. To delete a Security Service, select the checkbox before the group and click **Delete**.

## Configure IDS/IPS Security Service

To configure the Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) services, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Enhanced Security > Security Services**. The **Security Services** page appears.
- 2 Click the **IDS/IPS** tab and click **+ADD RULE**. The **Configure IDS/IPS Security Service** pop-up window appears.

# Configure IDS/IPS Security Service

X

**Name \*** IDPS1

**Description**

Enter Description (Optional)

Maximum 256 characters

## Intrusion Detection and Prevention

Intrusion Detection  On

Intrusion Prevention  On

Log Yes ▼

Enable IDS/IPS to Log

**CANCEL**

**SAVE CHANGES**

- 3 Enter a unique name for the IDS/IPS service and provide a description as needed.
- 4 Under the **Intrusion Detection and Prevention** section, activate Intrusion Detection (IDS) and/or Intrusion Prevention (IPS) toggle. When a user activates only IPS, IDS will be automatically activated. EFS engine inspects traffic sent/received through the Edges and matches content against signatures configured in the EFS engine. IDS/IPS Signatures are updated on a continuous basis with a valid EFS license. For more information about EFS, see [Enhanced Firewall Services Overview](#).
  - **Intrusion Detection** - When IDS is activated on Edges, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If an attack is detected, the EFS engine generates an alert and sends the alert message to SASE Orchestrator/Syslog Server if Firewall logging is activated in Orchestrator and will not drop any packets.

- **Intrusion Prevention** - When IPS is activated on Edges, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If an attack is detected, the EFS engine generates an alert and blocks the traffic flow to the client if the action in the signature rule is "Reject". If the action in the signature rule is "Alert", the traffic will be allowed without dropping any packets even if you configure IPS.

**Note** VMware recommends customers to not activate VNF when IDS/IPS is activated on Edges.

- From the **Log** drop-down menu, select **Yes** if you want to send the IDS/IPS logs to Orchestrator.
- Click **Save Changes**. An IDS/IPS service rule is created, and it appears in the table in the **IDS/IPS** page.

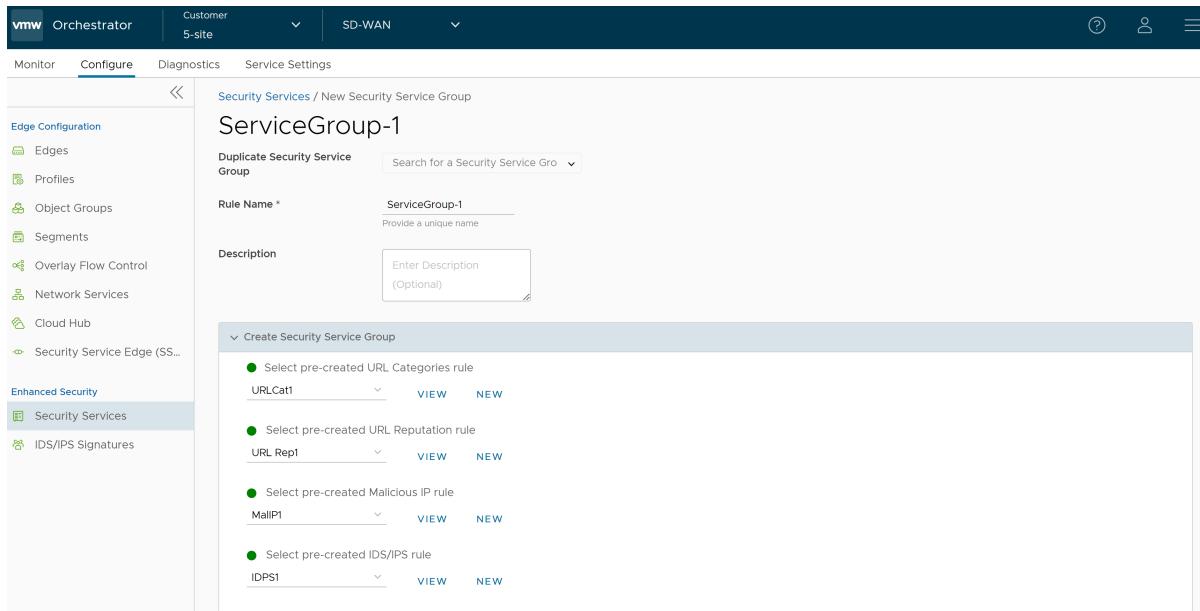
Name	Description	IDS	IPS	Log	Used By - Security Group	Last Modified
IDS_ONLY		Yes	No	Yes	1	2024-02-02T05:52:55.000Z
IDPSI		Yes	Yes	Yes	1	2024-02-01T09:00:45.000Z

- Click the link to the Security Service to modify the settings. To delete a Security Service, select the checkbox before the group and click **Delete**.

## Configure Security Service Group

A Security Service Group is used to group together individual security services namely URL filtering (URL Categories, URL Reputation), Malicious IP detection, IDS/IPS. To create a Security Service Group, perform the following steps:

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Enhanced Security > Security Services**. The **Security Services** page appears.
- Click the **Security Service Group** tab and click **+ CREATE GROUP**. The **New Security Service Group** page appears.



- 3 If you want to create a new Service Group from an existing one, choose an option from the **Duplicate Security Service Group** drop-down menu and rename the rule name alone. All the other configurations will be automatically applied from the selected Security Service Group.
- 4 To create a new Service Group, enter a unique name for the Security Service Group and provide a description as needed.
- 5 From the **Create Security Service Group** section, you can select the pre-created security services for URL Categories, URL Reputation, Malicious IP, and IDS/IPS and group them together to create a Security Group. If you do not want to use the pre-created services, you can click the **New** button and create a new security service to associate it to the Security Group. Click the **View** button to view the configuration details of the selected security service.
- 6 Click **Save Changes**. A Security Service Group is created, and it appears in the table in the **Security Service Group** page.

Name	Description	URL Categories	URL Reputation	Malicious IP	IDS/IPS	Used By	Last Modified
ServiceGroup-2		URLCat1	URL Rep1	MalIP1	IDS_ONLY	0 Profiles 1 Edge	Feb 2, 2024, 11:30:05 AM
ServiceGroup-1		URLCat1	URL Rep1	MalIP1	IDPS1	1 Profile 6 Edges	Feb 1, 2024, 4:41:02 PM

- Click the link to the Security Service Group to modify the settings. To delete a Security Service Group, select the checkbox before the group and click **Delete**.

**Note** Security Service Group in use cannot be deleted. If you want to delete a Security Service group, it must first be removed from the associated firewall rules.

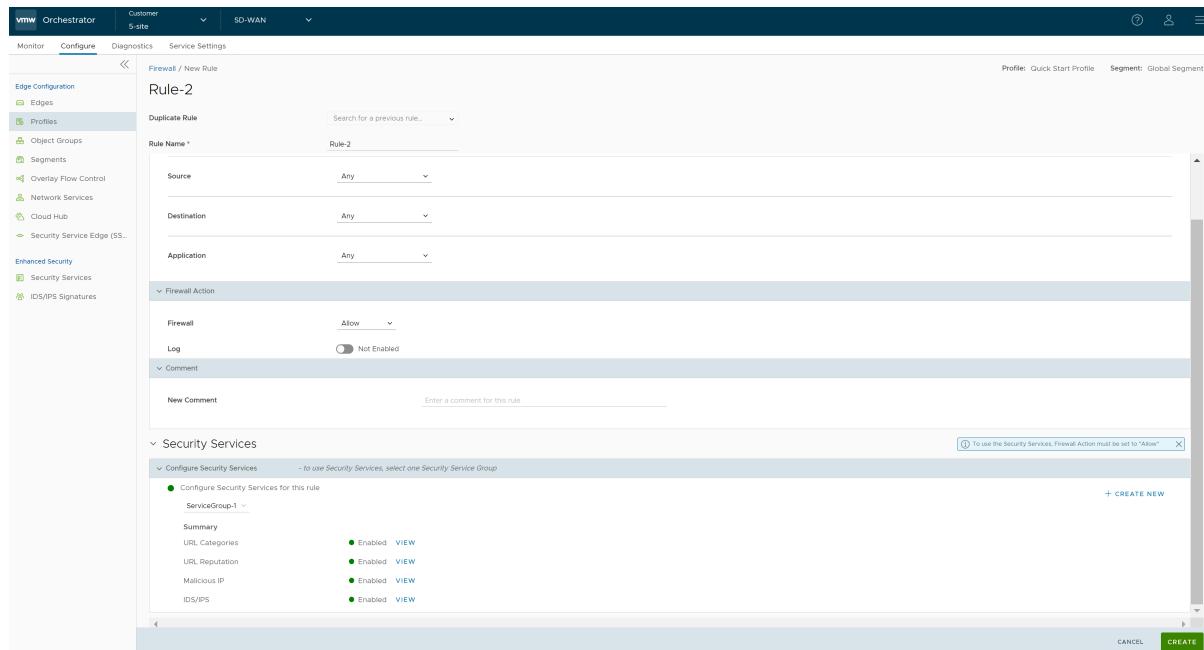
**Note** You can associate a security service group with multiple firewall rules. For steps, see [Associate a Security Service Group to a Firewall Rule at the Profile level](#).

**Note** You cannot associate more than one security service group with a firewall rule.

## Associate a Security Service Group to a Firewall Rule at the Profile level

To associate a Security Service Group to a new Firewall rule at the Profile level, perform the following steps:

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- Select a Profile to configure a firewall rule, and click the **Firewall** tab.
- Go to the **Configure Firewall** section and under the **Firewall Rules** area, click **+ NEW RULE**. The **New Rule** page appears.



- In the **Rule Name** text box, enter a unique name for the Rule. To create a firewall rule from an existing rule, select the rule to be duplicated from the **Duplicate Rule** drop-down menu.
- In the **Match** and **Firewall Action** sections, configure the match conditions for the rule and the actions to be performed when the traffic matches the defined criteria, respectively. For more information, see [Configure Firewall Rule](#).

- 6 In the **Security Services** section, configure the security service for the rule by selecting a Security Service Group from the drop-down menu. A summary of all the security services configured within the Security Service Group will be displayed. You can click the **View** button against each of the security services to view the configuration details.

**Note** Security services can be activated in the rule only if the Firewall action is **Allow**. If the Firewall action is anything other than **Allow**, Security services will be deactivated.

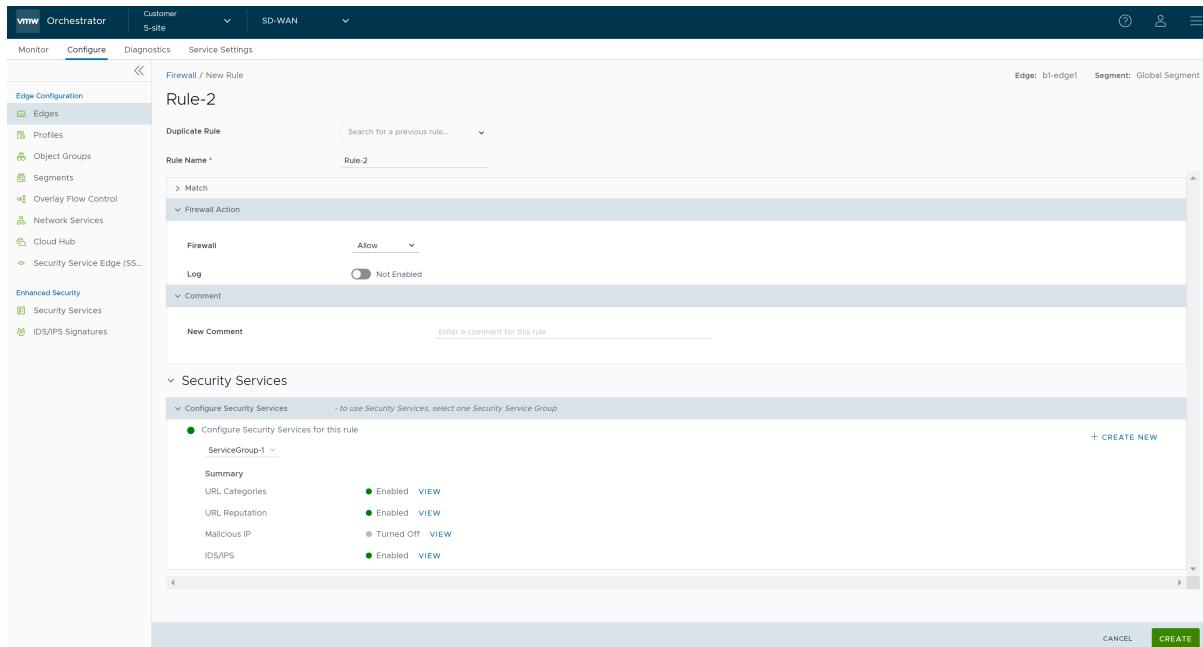
- 7 After configuring all the required settings, click **Create**. A firewall rule is created for the selected Profile, and it appears under the **Firewall Rules** area of the **Profile Firewall** page.
- 8 Click **Save Changes**.

To associate a Security Service Group to an existing Firewall rule at the Profile level, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 Select a Profile to configure a firewall rule, and click the **Firewall** tab.
- 3 Go to the **Configure Firewall** section and under **Firewall Rules** area, select the rule name for which you want to change the Security service configuration.
- 4 Under the **Security Services** section, select a different Service Group to associate to the rule and click **Edit**.
- 5 Click **Save Changes**.

## Associate a Security Service Group to a Firewall Rule at the Edge level

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 To configure an Edge, click the link to the Edge or click the **View** link in the **Firewall** column of the Edge.
- 3 Click the **Firewall** tab.
- 4 Go to the **Configure Firewall** section and from the **Firewall Rules** area, you can create a new rule with Security Service configurations or modify the existing rule's Security Service settings. Follow the procedure as described in Step 6 of [Associate a Security Service Group to a Firewall Rule at the Profile level](#) section.



**Note** The rules created at the Profile level cannot be updated at the Edge level. To override the rule, user needs to create the same rule at the Edge level with new parameters to override the Profile level rule.

- 5 After configuring all the required settings, click **Create**. A firewall rule is created for the selected Edge, and it appears under the **Firewall Rules** area of the **Edge Firewall** page.
- 6 Click **Save Changes**.

## View IDS/IPS Signatures

Once you have the Enhanced Firewall Services (EFS) feature activated at the Enterprise level, now you can view the details of the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Signatures that an Edge is using to filter the traffic from the VMware SASE Orchestrator.

You can view the IDS/IPS Signatures at the Enterprise level by logging into the **SD-WAN** service of the Enterprise portal and navigating to the **Configure > Security > IDS/IPS Signatures** page.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'vmw Orchestrator', 'Customer 5-site' (with a dropdown arrow), 'SD-WAN' (with a dropdown arrow), and icons for Help, User, and More. Below the navigation is a secondary menu with tabs: 'Monitor', 'Configure' (which is selected and underlined in blue), 'Diagnostics', and 'Service Settings'. On the left, a sidebar menu is open under 'IDS/IPS Signatures', listing 'Edges', 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control', 'Network Services', 'Cloud Hub', 'Security Service Edge (SSE)', 'Security Services', and 'IDS/IPS Signatures'. The main content area is titled 'IDS/IPS Signatures' and displays a table with one row for the 'Default' signature. The table columns are 'Name', 'Description', 'Total Intrusion Signatures', and 'Date Uploaded'. The 'Default' row shows 'IDPS Signature File version 1706847062577test' in the Description column, '11863' in the Total Intrusion Signatures column, and 'Feb 2, 2024, 9:42:08 AM' in the Date Uploaded column.

The **IDS/IPS Signatures** page displays the **Default** signature details such as name and file version of the signature, total number of intrusion signatures present in the downloaded bundle, and the date and time when the signature data is uploaded.

You can click the link under the **Total Intrusion Signatures** column to view the following additional details about the signatures present in the downloaded bundle. You can use the Search and Filter options in the UI to search and find any specific signatures within the bundle.

The screenshot shows the same VMware SD-WAN Orchestrator interface as above, but the main content area has changed. It now displays the 'IDS/IPS Signature / Default' page. The title is 'IDS/IPS Signature / Default'. Below it is a section titled 'Intrusion Signatures' with a search bar labeled 'Q. Search' and a refresh icon. A table lists 11 intrusion signatures. The columns are 'SignatureId', 'IDS Severity', 'Product Affected', 'Attack Target', 'Attack Type', 'CVSS', and 'CVE(s)'. Each row contains a 'View' link preceded by a greater-than symbol (>). The table shows various severity levels (Critical, High, Minor) and attack types (trojan-activity, attempted-user). At the bottom of the table are buttons for 'COLUMNS' and 'REFRESH', and pagination information: 'Objects per page 50' and '1 - 50 of 11863 items'.

Field	Description
SignatureId	A unique ID of the IDS signature.
IDS Severity	Signature severity of the intrusion. The following are the Severity rating: <ul style="list-style-type: none"> <li>■ Critical</li> <li>■ High</li> <li>■ Medium</li> <li>■ Minor</li> <li>■ Low</li> <li>■ Suspicious</li> </ul>
Product Affected	Illustrates what product is vulnerable to the exploit.
Attack Target	Target of the attack.
Attack Type	Type of attack, such as trojan horse, or denial of service (DoS).
CVSS	Common Vulnerability Score of the vulnerability targeted by the exploit.
CVE(s)	CVE reference of the vulnerability targeted by the exploit.

## Monitor Security Overview

The **Security Overview** page displays the overall impact summary of configured Security services, like Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), URL Categories, URL Reputations, and Malicious IP for all Edges within an Enterprise, based on the metrics collected using the various Enhanced Firewall Services (EFS) engines (IDS/IPS/URL Filtering/Malicious IP).

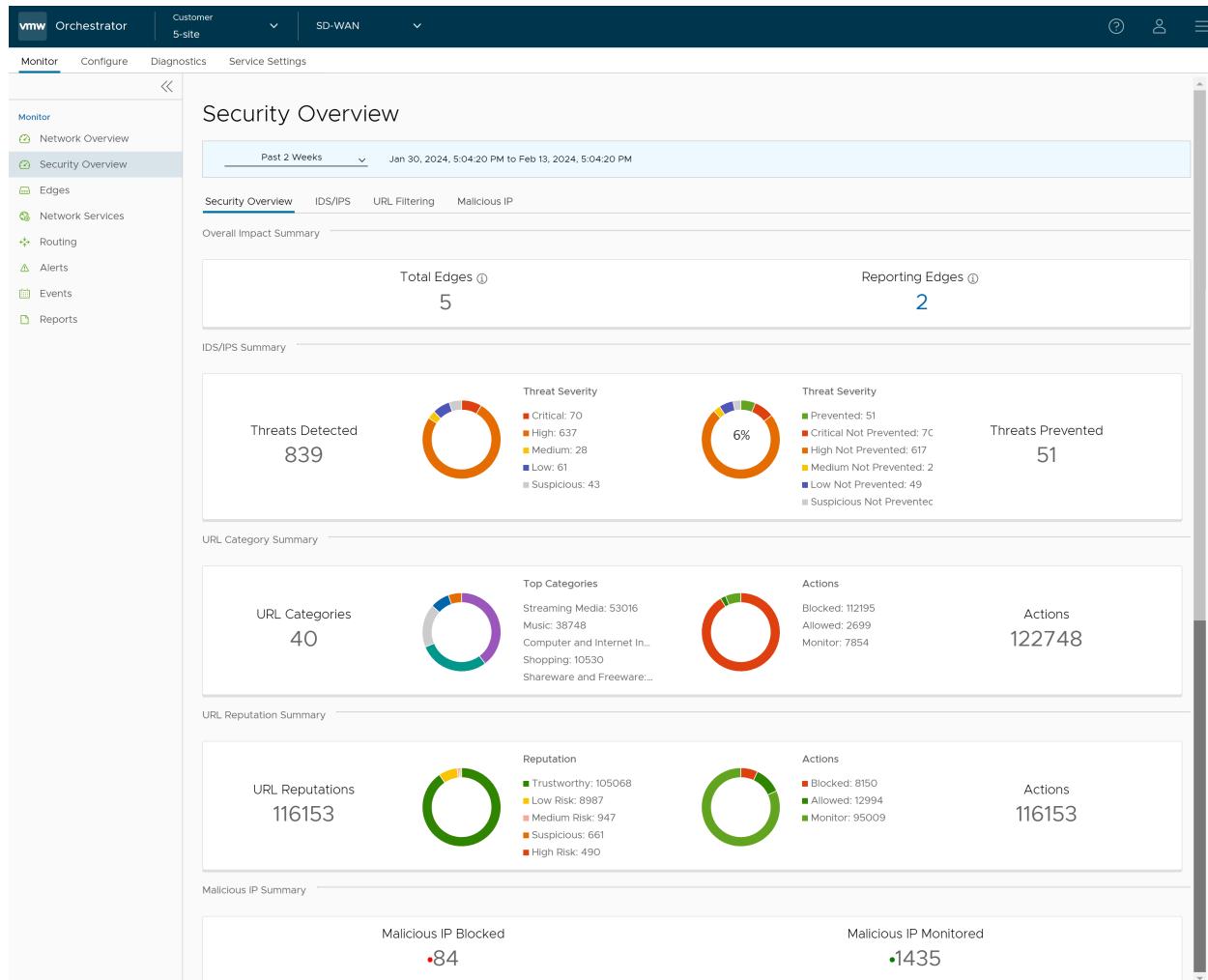
---

**Note** Under the **Monitor** tab, the **Security Overview** option will be visible only if the EFS feature is activated in the **Global Settings** page.

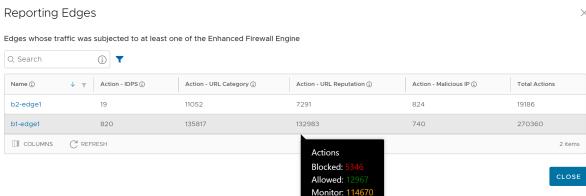
---

### Monitor Security Overview - Enterprise View

To view the overall impact summary of configured Security services for an Enterprise, in the **SD-WAN** service of the Enterprise portal, click **Monitor > Security Overview**. The **Security Overview** page appears.



In the **Security Overview** page, you can find the following details:

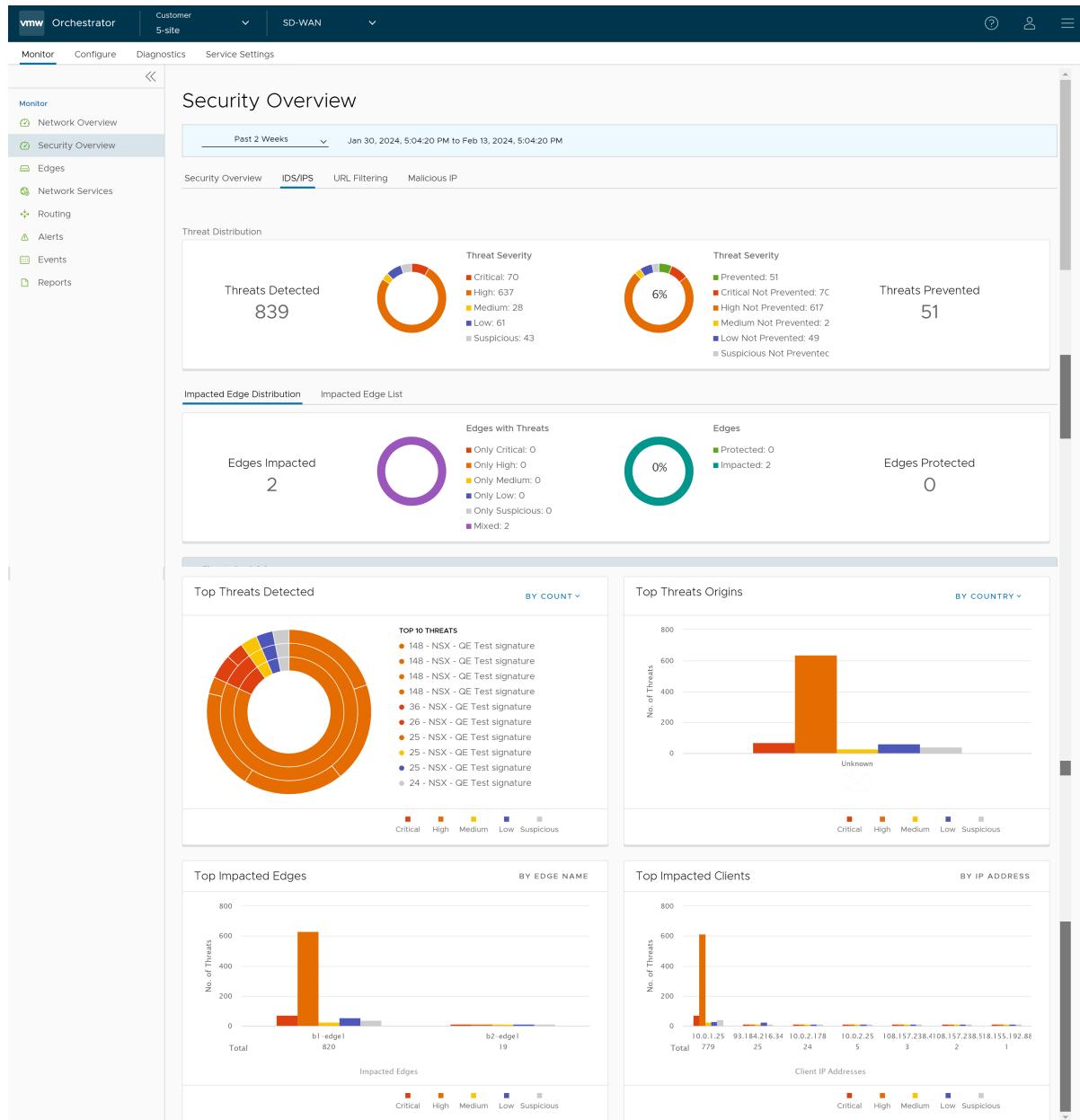
Option	Description
Overall Impact Summary	<p>Displays the total count of Edges within the Enterprise and total count of Reporting Edges whose traffic was subjected to at least one of the Enhanced Firewall Engines.</p> <p>Under <b>Reporting Edges</b>, clicking the link to the number displays a tabular view of all Edges whose traffic hit atleast one EFS engine along with the Action count details. Hover the mouse over the Action count to view the split count by supported <b>Action</b> types.</p>  <p>To view the EFS Threats details for a specific Edge, click the link to the Edge name. You will be navigated to the Edge-specific Security Overview page. See <a href="#">Monitor Security Overview - Edge View</a>.</p>
IDS/IPS Summary	<p>Displays the total count of IDS/IPS Threats Detected and Prevented for all Edges within the Enterprise, along with the Threat Severity and Action details in a graphical representation. Hover the mouse on the graphs to view specific threat details.</p> <p>For detailed information about the IDS/IPS Threat distribution, see <a href="#">Monitor IDS/IPS</a>.</p>
URL Category Summary	<p>Displays the total count of URL Categories and Action count details for all Edges within the Enterprise, along with the <b>Top 5 URL Categories</b> details in a graphical representation.</p> <p>For detailed information about the URL Category Threats distribution, see <a href="#">Monitor URL Filtering</a>.</p>
URL Reputation Summary	<p>Displays the total count of URL Reputation risks and Action count details for all Edges within the Enterprise in a graphical representation.</p> <p>For detailed information about the URL Reputation Threats distribution, see <a href="#">Monitor URL Filtering</a>.</p>
Malicious IP Summary	<p>Displays the total count of Malicious IP Blocked and Monitored.</p> <p>For detailed information about the Malicious IP Threats distribution, see <a href="#">Monitor Malicious IP</a>.</p>

## Monitor IDS/IPS

To view the IDS/IPS specific threats details for an Enterprise, click **Monitor > Security Overview > IDS/IPS**.

The **IDS/IPS** page is a graphical representation of Threat distribution (Threats Detected/Threats Prevented) based on the metrics collected using the IDS/IPS engines for all Edges within an Enterprise. You can view the Threat distribution of all the Edges using the following two views:

- **Impacted Edge Distribution** – Represents a map view of all the IDS/IPS Impacted Edges (by severity) and Protected Edges. The page graphically displays the following IDS/IPS Threat details for an Enterprise:
  - Total count of Edges Impacted
  - Total count of Edges Protected
  - Top Threats Detected filtered "By Count" (Default) or "By Impact"
  - Top Threat Origins filtered "By Country" (Default) or "By IP Address"
  - Top Impacted Edges filtered "By Edge Name"
  - Top Impacted Clients filtered "By IP Address"



- **Impacted Edge List** – Represents a tabular view of all the IDS/IPS impacted Edges along with Threat details. The page displays the following details: Name and Description of the impacted Edge, Threat Impact on Edge, and Status of impacted Edge.

The screenshot shows the VMware SD-WAN Orchestrator interface with the following details:

- Header:** VMW Orchestrator, Customer 5-site, SD-WAN.
- Navigation:** Monitor (selected), Configure, Diagnostics, Service Settings.
- Left Sidebar:** Network Overview, Security Overview (selected), Edges, Network Services, Routing, Alerts, Events, Reports.
- Section: Security Overview**
  - Time Range: Past 2 Weeks (Feb 1, 2024, 2:23:36 PM to Feb 15, 2024, 2:23:36 PM).
  - IDS/IPS tab is selected.
  - Threat Distribution:
    - Threats Detected: 839
    - Threat Severity Donut Chart (6%):
 

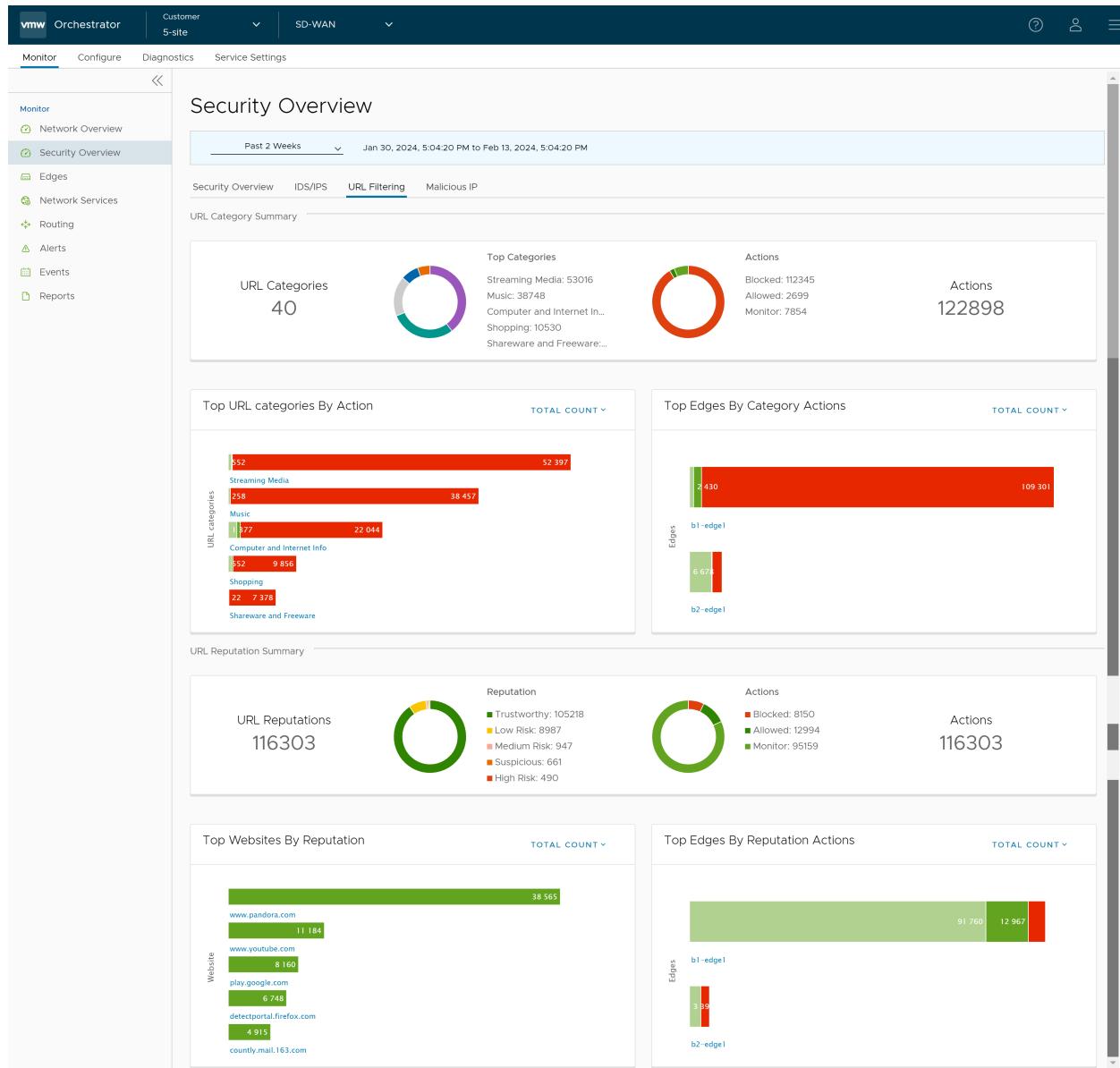
Critical: 70
High: 637
Medium: 28
Low: 61
Suspicious: 43
    - Threats Prevented: 51
    - Threat Severity Donut Chart (6%):
 

Prevented: 51
Critical Not Prevented: 7C
High Not Prevented: 617
Medium Not Prevented: 2
Low Not Prevented: 49
Suspicious Not Prevented
  - Impacted Edge Distribution:
    - Impacted Edge List Table:
 

Edge Name	Description	Threat Impact	Status
b1-edge1		H (629) M (26) L (57) C (70) S (38)	Alerted
b2-edge1		H (8) M (2) L (4) C (0) S (5)	Alerted

## Monitor URL Filtering

To view the URL Filtering specific threats details for an Enterprise, click **Monitor > Security Overview > URL Filtering**.



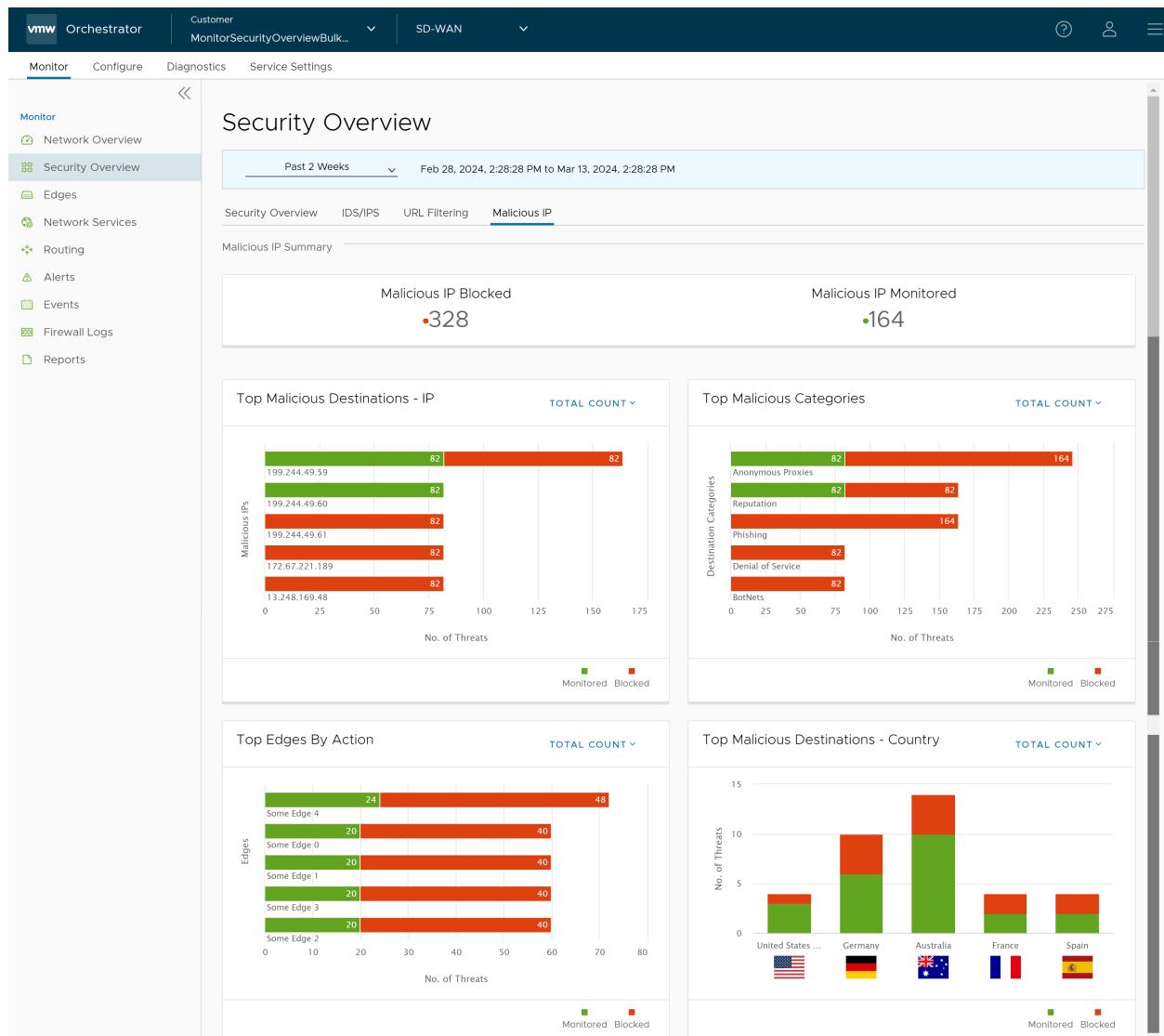
The **URL Filtering** page graphically displays the following URL Categories and URL Reputations threat details for an Enterprise:

- Total count of URL Categories
- Total count of URL Category Actions
- Top URL Categories
- Top URL categories filtered by "Action" (Blocked, Allowed, and Monitored) or "Total Count" (Default)
- Top Edges filtered by "Category Actions" (Blocked, Allowed, and Monitored) or "Total Count" (Default)
- Total count of URL Reputations

- Total count of URL Reputation Actions
- Top Websites filtered by "URL Reputation" (High Risk, Suspicious, Medium Risk, Low Risk, and Trustworthy) or "Total Count" (Default)
- Top Edges filtered by "Reputation Actions" (Blocked, Allowed, and Monitored) or "Total Count" (Default)

## Monitor Malicious IP

To view the Malicious IP specific threats details for an Enterprise, click **Monitor > Security Overview > Malicious IP**.



The **Malicious IP** page graphically displays the following Malicious IP threat details for an Enterprise:

- Total count of Blocked Malicious IP

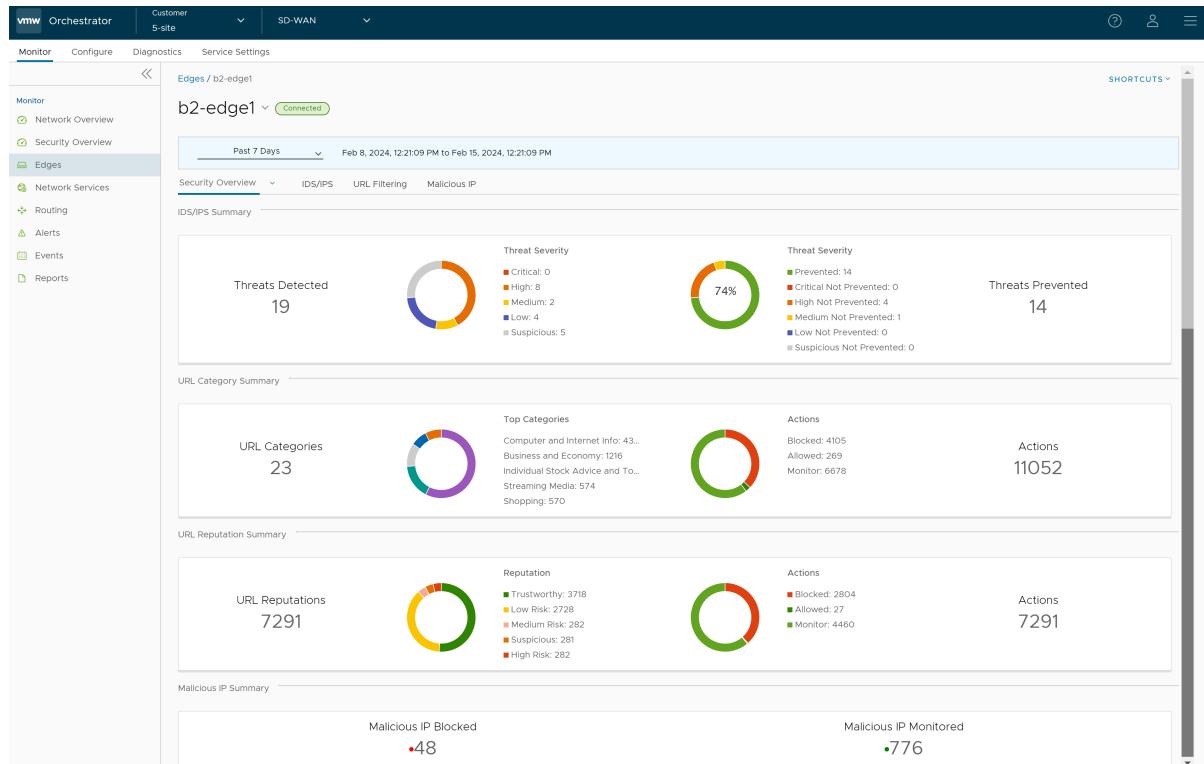
- Total count of Monitored Malicious IP
- Top Malicious Destination IPs filtered by "Action" (Blocked and Monitored) or "Total Count" (Default)
- Top Malicious Categories filtered by "Action" (Blocked and Monitored) or "Total Count" (Default)
- Top Edges filtered by "Action" (Blocked and Monitored)) or "Total Count" (Default)
- Top Malicious Destination Countries filtered by "Action" (Blocked and Monitored) or "Total Count" (Default)

## Monitor Security Overview - Edge View

To view the EFS Threat details for a specific Edge:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Monitor > Edges**. The list of Edges associated with the Enterprise appears.
- 2 Select an Edge by clicking the link to an Edge. The **Network Overview** page (default page view) appears.
- 3 From the **Network Overview** drop-down menu, select **Security Overview**.

The **Security Overview** page displays the overall impact summary of configured Security services, like IDS/IPS, URL Categories, URL Reputations, and Malicious IP for the selected Edge.



## Enhanced Firewall Services Alerts and Events

Describes details about Enhanced Firewall Services (EFS) related Enterprise and Operator Orchestrator events.

### Enterprise-level EFS Events

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATE
MGD_ATPU_P_INVALID_IDPS_SIGNATURE	Invalid IDPS Signature	ERROR	SD-WAN Edge (MGD)	Generated when there is an invalid suricata package.	5.2.0	
MGD_ATPU_P_DOWNLOAD_IDPS_SIGNATURE_FAILED	Download IDPS Signature failed	ERROR	SD-WAN Edge (MGD)	Generated when downloading of suricata package fails.	5.2.0	
MGD_ATPU_P_DECRYPT_IDPS_SIGNATURE_FAILED	Decrypt IDPS Signature failed	ERROR	SD-WAN Edge (MGD)	Generated when unpacking of suricata package fails.	5.2.0	
MGD_ATPU_P_APPLY_IDPS_SIGNATURE_FAILED	Failed to apply IDPS Signature	ERROR	SD-WAN Edge (MGD)	Generated due to error in applying Suricata files.	5.2.0	
MGD_ATPU_P_APPLY_IDPS_SIGNATURE_SUCCEEDED	Successfully applied IDPS Signature	INFO	SD-WAN Edge (MGD)	Generated when suricata files are successfully applied.	5.2.0	
MGD_ATPU_P_STANDBY_UPDATE_START	Standby device IDPS Signature update started	INFO	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDPS Signature version is started.	5.2.0	
MGD_ATPU_P_STANDBY_UPDATE_FAILED	Standby device IDPS Signature update failed	ERROR	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDP Signature version fails.	5.2.0	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_ATPU_P_STANDBY_UPDATED	Standby device IDPS Signature update completed	INFO	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDPS Signature version is successfully applied.	5.2.0	
EFS_IDPS_NOT_READY	EFS_IDPS_NOT_READY	ALERT	SD-WAN Edge (MGD)	Generated when packets are dropped while on-prem Orchestrator is not connected to GSM and so IDPS signatures are not ready.	6.0.0	
EFS_IP_DB_VERSION_UPDATE	EFS_IP_DB_VERSION_UPDATE	INFO	SD-WAN Edge (MGD)	Generated when loading of IP database succeeds or fails.	6.0.0	
EFS_IP_RTU_DB_VERSION_UPDATE	EFS_IP_RTU_DB_VERSION_UPDATE	INFO	SD-WAN Edge (MGD)	Generated when loading of IP RTU database succeeds or fails.	6.0.0	
EFS_URL_DB_VERSION_UPDATE	EFS_URL_DB_VERSION_UPDATE	INFO	SD-WAN Edge (MGD)	Generated when loading of URL database succeeds or fails.	6.0.0	
EFS_URLF_MAL_IP_NOT_READY	EFS_URLF_MAL_IP_NOT_READY	ALERT	SD-WAN Edge (MGD)	Generated when packets are dropped while EFS is activated but URLF/MAL-IP filtering is not ready.	6.0.0	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EFS_URL_RTU_DB_VERSION_UPDATE	EFS_URL_RTU_DB_VERSION_UPDATE	INFO	SD-WAN Edge (MGD)	Generated when loading of URL RTU database succeeds or fails.	6.0.0	
MGD_EFS_NTICS_REGISTRATION_SUCCEEDED	MGD_EFS_NTICS_REGISTRATION_SUCCEEDED	INFO	SD-WAN Edge (MGD)	Generated when VMware Threat Intelligent Cloud Service (NTICS) registration with Client ID succeeds.	6.0.0	
MGD_EFS_NTICS_REGISTRATION_FAILED	MGD_EFS_NTICS_REGISTRATION_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when NTICS registration fails with retry count.	6.0.0	
MGD_EFS_NTICS_AUTHENTICATION_SUCCEEDED	MGD_EFS_NTICS_AUTHENTICATION_SUCCEEDED	INFO	SD-WAN Edge (MGD)	Generated when NTICS authentication succeeds.	6.0.0	
MGD_EFS_NTICS_AUTHENTICATION_FAILED	MGD_EFS_NTICS_AUTHENTICATION_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when NTICS authentication fails.	6.0.0	

## Operator-level EFS Events

Event	Displayed On Orchestrator UI As	Severity	Generated By	Generated When	Released In	Added In	Deprecated
IDPS_SIGNATURE_VCO_VERSION_CHECK_FAIL	Querying existing signature version from local DB failed	ERROR	SASE Orchestrator	Generated when SASE Orchestrator backend poll job has failed to retrieve existing suricata signature version from Orchestrator's local database.	5.2.0		
IDPS_SIGNATURE_GSM_VERSION_CHECK_FAIL	Querying signature metadata from GSM failed	ERROR	SASE Orchestrator	Generated when SASE Orchestrator backend poll job has failed to retrieve existing suricata signature metadata (that includes signature version) from GSM.	5.2.0		
IDPS_SIGNATURE_SKIP_DOWNLOAD_NO_UPDATE	Skipping signature download due to no change in signature version	INFO	SASE Orchestrator	Generated when SASE Orchestrator backend poll job skips downloading suricata signature file due to no change in suricata signature file version.	5.2.0		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
IDPS_SIGNATURE_STORE_FAILURE_NO_PATH	Filestore path not set to store signature file	ERROR	SASE Orchestrator	Generated when SASE Orchestrator backend poll job fails to store suricata signature file due to filestore path not being set.	5.2.0	
IDPS_SIGNATURE_DOWNLOAD_SUCCESS	Successfully downloaded signature file from GSM	INFO	SASE Orchestrator	Generated when SASE Orchestrator backend poll job successfully downloads suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE_DOWNLOAD_FAILURE	Failed to download signature file from GSM	ERROR	SASE Orchestrator	Generated when SASE Orchestrator backend poll job fails to download suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE_STORE_SUCCESS	Successfully stored the signature file in filestore	INFO	SASE Orchestrator	Generated when SASE Orchestrator backend poll job successfully stores the suricata signature file in local file store.	5.2.0	
IDPS_SIGNATURE_STORE_SIGNATURE_FAILURE	Failed to store the signature file in filestore	ERROR	SASE Orchestrator	Generated when SASE Orchestrator backend poll job fails to store the suricata signature file in local file store.	5.2.0	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
IDPS_SIGNATURE_META_DATA_INSERT_SUCCESS	Successfully added metadata of the signature file to local DB	INFO	SASE Orchestrator	Generated when SASE Orchestrator backend poll job successfully adds metadata of the suricata signature file to local DB.	5.2.0	
IDPS_SIGNATURE_META_DATA_INSERT_FAILURE	Failure to add metadata of the signature file to local DB	ERROR	SASE Orchestrator	Generated when SASE Orchestrator backend poll job fails to add metadata of the suricata signature file to local DB.	5.2.0	
POLL_URL_CATEGORIES_FAIL	POLL_URL_CATEGORIES_FAIL	ERROR	SASE Orchestrator	Generated when SASE Orchestrator URL categories poll job fails.	6.0.0	
URL_CATEGORIES_STORE_SUCCESS	URL_CATEGORIES_STORE_SUCCESS	INFO	SASE Orchestrator	Generated when SASE Orchestrator URL categories are stored successfully.	6.0.0	
URL_CATEGORIES_STORE_FAILURE	URL_CATEGORIES_STORE_FAILURE	ERROR	SASE Orchestrator	Generated when SASE Orchestrator URL categories storage job fails.	6.0.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATED
VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_FAILED	VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_FAILED	ERROR	SASE Orchestrator	Generated when SASE Orchestrator Enterprise NTICS license request fails.	6.0.0	
VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_SUCCEEDED	NTICS License request succeeded	INFO	SASE Orchestrator	Generated when SASE Orchestrator Enterprise NTICS license request succeeds.	6.0.0	

## Monitor Firewall Logs

The **Firewall Logs** page displays the details of firewall log originating from VMware SD-WAN Edges. Previously the only way a customer could store and view firewall logs was by forwarding them to a Syslog server. With Release 5.2.0 the customer has the option to store firewall logs on the Orchestrator where they can be viewed, sorted, and searched on the Orchestrator UI. By default, Edges cannot send their Firewalls logs to Orchestrator. For an Edge to send the Firewall logs to Orchestrator, ensure that the “**Enable Firewall Logging to Orchestrator**” customer capability is activated at the Customer level under “Global Settings” UI page. By default, Orchestrator retains the Firewall logs until it reaches the maximum retention time of 7 days or a maximum log size of 15 GB per customer tenant on a rotation basis.

Firewall Logs are generated:

- When a flow is created (on the condition that the flow is accepted)
- When the flow is closed
- When a new flow is denied
- When an existing flow is updated (due to a firewall configuration change)

EFS Alerts are generated whenever the flow traffic matches any URL Categories and/or URL Reputation, or Malicious IP, or any IDS/IPS suricata signatures configured in the EFS engine:

- If a firewall rule has URL Categories filtering service activated, the URL Category engine looks up the categories of destination URLs and detects if that matches the Blocked or Monitor categories configured. If the URL matches the Blocked categories, the URL Categories engine generates an alert and blocks the Edge traffic. If the URL matches the Monitor categories, the engine allows the Edge traffic and captures the firewall logs.

- If a firewall rule has URL Reputation filtering service activated, the URL Reputation engine looks up the reputation score of the URL and takes action (Allow/Block) based on the minimum reputation configured. If the reputation score of the URL is less than the minimum reputation configured, the Edge blocks the traffic and generates EFS alerts and logs, otherwise allows the traffic. The URL Reputation engine generates EFS logs for the allowed traffic based on the **Capture Logs** configuration.
  - If a firewall rule has Malicious IP filtering service activated, the Malicious IP engine checks if the destination IP is present in the Malicious IP Database (Network Query DB and Local DB). If the engine detects the destination IP in the Malicious IP database, then the engine generates EFS alerts and logs and takes Edge traffic decisions based on the configured action (Block/Monitor).
  - If a firewall rule has only the Intrusion Detection System (IDS) activated, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If an attack is detected, the EFS engine generates an alert and sends the alert message to SASE Orchestrator/Syslog Server if Firewall logging is activated in Orchestrator and will not drop any packets.
  - If a firewall rule has Intrusion Prevention System (IPS) activated, the Edges detect if the traffic flow is malicious or not based on certain signatures configured in the engine. If an attack is detected, the EFS engine generates an alert and blocks the traffic flow to the client only if the signature rule has action as "Reject", matched by the malicious traffic. If the action in the signature rule is "Alert", the engine allows the traffic without dropping any packets even if you configure IPS.

To view the Edge Firewall logs in Orchestrator:

- 1 In the **SD-WAN** service of the Enterprise portal, navigate to **Monitor > Firewall Logs**. The **Firewall Logs** page appears.

VMW Orchestrator Customer 5-site SD-WAN

Monitor Configure Diagnostics Service Settings

Firewall Logs

Past 12 Hours Dec 14, 2023, 11:26:04 PM to Dec 15, 2023, 11:26:04 AM

FILTERS CSV

gret	Severity	Category	IDS Alert	IPS Alert	URL	Engine Types	URL Categories	URL Category Filter Action	URL Reputation	URL Reputation Action	IP Categories	Malicious IP Action
No	No	detectportal.firefox.com/success.txt	2	2	DENY	Trustworthy	ALLOW	0	--			
No	No	--	1	0	--	--	--	4	DENY			
No	No	--	1	0	--	--	--	4	DENY			
No	No	--	1	0	--	--	--	4	DENY			
No	No	detectportal.firefox.com/success.txt	2	2	DENY	Trustworthy	ALLOW	0	--			
No	No	snippets.cdn.mozilla.net	2	1	DENY	Trustworthy	ALLOW	0	--			
No	No	snippets.cdn.mozilla.net	2	1	DENY	Trustworthy	ALLOW	0	--			
No	No	img-getpocket.cdn.mozilla.net	2	1	DENY	Trustworthy	ALLOW	0	--			

COLUMNS REFRESH 1 - 50 of 477 items < < >

Firewall Log Details

Log Overview Engine

Log Time	Dec 15, 2023, 10:10:41 AM	Engine	URL Reputation Filtering, URL Category Filtering	Extension headers
Segment	Global Segment	Source IP	10.0.1.233	Reason
Edge	b1-edge1	Source Port	41020	Bytes Sent

With the Stateful Firewall and Enhanced Firewall Services (EFS) features activated, more information can be reported in the firewall logs. The following table describes all the parameters reported in the firewall logs.

Field	Description
Time	The timestamp of the traffic flow session on which the alert was triggered.
Segment	The name of the segment to which the session belongs.
Edge	The name of the Edge to which the session belongs.
Action	<p>Any of the following actions that were triggered against the event/alert:</p> <ul style="list-style-type: none"> <li>■ Allow</li> <li>■ Close</li> <li>■ Deny</li> <li>■ Open</li> <li>■ Update</li> </ul>
Interface	The name of the interface on which the first packet of the session was received. In the case of overlay received packets, this field will contain VPN. For any other packets (received through underlay), this field will display the name of the interface in the Edge.
Protocol	The type of IP protocol used by the session. The possible values are TCP, UDP, GRE, ESP, and ICMP.
Source IP	The source IP address of the traffic flow session on which the alert was triggered.
Source Port	The source port number of the traffic flow session on which the alert was triggered.
Destination IP	The destination IP address of the traffic flow session on which the alert was triggered.
Destination Port	The destination port of the traffic flow session on which the alert was triggered.
Extension Headers	The extension headers of the traffic flow packet.
Rule	The Rule to which the Signature belongs.
Reason	The reason for closure or denial of the session. This field is available for Close and Deny log messages.
Bytes Sent	The amount of data sent in bytes in the session. This field is available only for Close log messages.
Bytes Received	The amount of data received in bytes in the session. This field is available only for Close log messages.
Duration	The duration for which the session has been active. This field is available only for Close log messages.
Application	The Application name to which the session was classified by DPI Engine. This field is available only for Close log messages.

Field	Description
Destination Domain	The destination domain of the traffic flow session.
Destination Name	The name of the destination device of the traffic flow session.
Session ID	The Session ID of the traffic flow on which the alert was triggered.
Signature ID	A unique ID of the signature rule.
Signature	The Signature installed on the Edge.
Attack Source	The Source of the attack.
Attack Target	The Target of the attack.
Severity	The severity of the intrusion.
Category	The category type to which the intrusion belongs.
IDS Alert	Displays "Yes" if the alert notification is received from the IDS engine, or else displays "No".
IPS Alert	Displays "Yes" if the alert notification is received from the IPS engine, or else displays "No".
URL	The URL of the destination to which the traffic flow was directed.
Engine Types	Total count of Engine types that match the flow. Click the link in this column to view the Engine types that match the flow.
URL Categories	Total count of URL category types that matches the flow. Click the link in this column to view the URL categories that matches the flow.
URL Category Filter Action	The URL Category Engine-specific filtering action: <ul style="list-style-type: none"><li>■ Block</li><li>■ Monitor</li></ul>
URL Reputation	The URL Reputation type defined in the policy rule.
URL Reputation Action	The URL Reputation Engine-specific filtering action: <ul style="list-style-type: none"><li>■ Block</li><li>■ Monitor</li></ul>
IP Categories	Total count of threat types that match the flow. Click the link in this column to view the IP categories that match the flow.
Malicious IP Action	The Malicious IP Engine-specific filtering action: <ul style="list-style-type: none"><li>■ Block</li><li>■ Monitor</li></ul>

**Note** Not all fields will be populated for all firewall logs. For example, Reason, Bytes Received/Sent and Duration are fields included in logs when sessions are closed. Signature ID, Signature, Attack Source, Attack Target, Severity, Category, IDS Alert, IPS Alert, URL, Engine Types, URL Categories, URL Category Filter Action, URL Reputation, URL Reputation Action, IP Categories, and Malicious IP Action are populated only for EFS alerts, not for firewall logs.

- 2 You can use the **Filter** options and select a filter from the drop-down menu to query the Firewall logs.
- 3 To view more detailed information about a specific Firewall log, select the Firewall log entry. Under the **Firewall Log Details** section, you can view the detailed **Log Overview** and **Engine** information for the selected log entry.

**Note** If the selected Firewall log entry is generated by Engines other than Enhanced Security Services, the **Engine** tab will not be available.

Firewall Log Details					
Log Overview		Engine			
Log Time	Dec 15, 2023, 10:10:41 AM	Engine	URL Reputaion Filtering,URL Category Filtering	Extension headers	--
Segment	Global Segment	Source IP	10.0.1.233	Reason	--
Edge	b1-edge1	Source Port	41020	Bytes Sent	--
Rule	Rule-0	Destination IP	34.107.221.82	Bytes Received	--
Interface	--	Destination Port	80	Duration	00:00:00
Protocol	TCP	Destination Domain	detectportal.firefox.com	Application	--
Action	DENY	Destination Name	--	Session ID	9519

- 4 In the **Log Overview** tab, click the link next to **Engine** to view detailed information about the specific Engine that matched the flow along with the Engine-specific filtering action.

Firewall Log Details					
Log Overview		Engine			
URL Reputaion Filtering					URL Category Filtering
URL Reputation Action	● ALLOW	URL	detectportal.firefox.com/success.txt		
URL Reputation	Trustworthy	URL Category Filter Action	DENY		
		URL Categories	Computer and Internet Info,Shareware and Freeware		

- 5 To create customized reports by exporting Edge Firewall Logs data in CVS format, in the **Firewall Logs** page, click the **CSV** option.

## Troubleshooting Firewall

You can collect the firewall diagnostic logs by running the remote diagnostic tests on an Edge.

For Edges running Release 3.4.0 or later which also have Stateful Firewall activated, you can use the following remote diagnostic tests to obtain firewall diagnostic information:

- **Flush Firewall Sessions** - Run this test on the required Edge by providing the Source and Destination IP addresses to flush the active firewalls session which needs to be reset. This is specifically for the Stateful Firewall. Running this test on an Edge not only flushes the firewall sessions, but actively send a TCP RST for the TCP-based sessions.
- **List Active Firewall Sessions** - Run this test to view the current state of the active firewall sessions (up to a maximum of 1000 sessions). You can filter by Source and Destination IP and Port as well as Segment to limit the number of sessions returned.

Segment	Src IP	Dst IP	Protocol	Src Port	Dst Port	Application	Firewall Policy	TCP State	Bytes Sent	Bytes Rcvd	Duration (secs)
Global Segment	10.0.1.25	10.0.1.1	TCP	35760	179	bgp	AllowAny	CLOSED	258	164	0
Global Segment	10.0.1.25	10.0.1.1	UDP	49152	3784	udp	AllowAny	N/A	3796	5120	63

**Note** You cannot see sessions that were denied as they are not active sessions. To troubleshoot those sessions, you will need to check the firewall logs.

You can use the following remote diagnostic tests to obtain the category and reputation score of a given URL, and threat category of a given IP:

- **Get IP Threat Reputation** - Run this test on the required Edge by providing the IP address to view the threat category of the given IP.

IP: 13.248.169.48	Status: Retrieved value from Local DB	Threat Type: Windows Exploits, BotNets, Phishing, Proxy
-------------------	---------------------------------------	---

- **Get URL Category/Reputation** - Run this test on the required Edge by providing the URL to view the category and reputation score of a given URL.

Get URL Category/Reputation

View the category and reputation score of the URL.

URL  
www.google.com

Test Duration: 2.007 seconds

URL: www.google.com  
Status: Retrieved value from Local DB  
Category: Search Engines  
Reputation: 81

For more information about how and when to run these remote diagnostics on an Edge, see VMware SD-WAN Troubleshooting guide available at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

# Provision a New Edge

23

Enterprise Administrators can provision a single Edge or multiple Edges for Enterprise Customers.

To create a new Edge, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 In the **Edges** screen, click **Add Edge**. The **Provision an Edge** screen appears.

Edges / Provision an Edge

### Provision an Edge SD-WAN

1. Edge Requirements Name / Model / Profile / License / Authentication / HA / Contact / Analytics Mode

Mode * ①	<input checked="" type="radio"/> SD-WAN Edge <input type="checkbox"/> Enable Analytics <input type="radio"/> Analytics Only Edge
Name *	test
Model *	Edge 5X0
Profile * ②	Quick Start Profile
Edge License *	STANDARD   10 Mbps   North America, Europe Mic
Authentication ③	Certificate Acquire
Encrypt Device Secrets ④	<input checked="" type="checkbox"/> Enable
④ For Edge versions 5.2.0 and above, before you deactivate this option, you must first deactivate the Edge using remote actions. This action causes restart of this Edge.	
High Availability	<input type="checkbox"/> Enable
Contact	
Local Contact Name *	Super User
Local Contact Email *	super@velocloud.net
<b>NEXT</b>	
2. Additional	Serial Number / Description / Location
<b>ADD EDGE</b> <b>CANCEL</b>	

3 You can configure the following options:

Option	Description
Mode	<p>By default, <b>SD-WAN Edge</b> mode is selected.</p> <p>For Enterprise Customers with Analytics enabled, you can provision an Analytics Edge by following the steps in the topic <a href="#">Chapter 24 Provision a New Edge with Analytics</a>.</p>
Name	Enter a unique name for the Edge.
Model	Select an Edge model from the drop-down menu.
Profile	<p>Select a Profile to be assigned to the Edge, from the drop-down menu.</p> <p>For information on how to create a new Profile, see <a href="#">Create Profile</a>.</p>
Edge License	<p>Select an Edge license from the drop-down menu. The list displays the licenses assigned to the Enterprise, by the Operator.</p>

Option	Description
Authentication	<p>Choose the mode of authentication from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Deactivated:</b> Edge uses a pre-shared key mode of authentication.</li> </ul> <p><b>Warning</b> This mode is not recommended for any customer deployments.</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Acquire:</b> This mode is selected by default and is recommended for all customer deployments. With <b>Certificate Acquire</b> mode, certificates are issued at the time of Edge activation and renewed automatically. The Orchestrator instructs the Edge to acquire a certificate from the certificate authority of the SASE Orchestrator by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the SASE Orchestrator and for establishment of VCMP tunnels.</li> </ul> <p><b>Note</b> After acquiring the certificate, the option can be updated to <b>Certificate Required</b>, if needed.</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Required:</b> This mode is only appropriate for customer enterprises that are "static". A static enterprise is defined as one where no more than a few new Edges are likely to be deployed and no new PKI oriented changes are anticipated.</li> </ul> <p><b>Important</b> <b>Certificate Required</b> has no security advantages over <b>Certificate Acquire</b>. Both modes are equally secure and a customer using <b>Certificate Required</b> should do so only for the reasons outlined in this section.</p> <p><b>Certificate Required</b> mode means that no Edge heartbeats are accepted without a valid certificate.</p> <p><b>Caution</b> Using this mode can cause Edge failures in cases where a customer is unaware of this strict enforcement.</p>

Option	Description
	<p>With this mode, the Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges by editing the Orchestrator's System Properties. For more information, contact your Operator.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ With the Bastion Orchestrator feature enabled, the Edges that are to be staged to Bastion Orchestrator should have the authentication mode set to either <b>Certificate Acquire</b> or <b>Certificate Required</b>.</li> <li>■ When an Edge certificate is revoked, the Edge is deactivated and needs to go through the activation process. The current QuickSec design checks certificate revocation list (CRL) time validity. The CRL time validity must match the current time of Edges for the CRL to have impact on new established connection. To implement this, ensure the Orchestrator time is updated properly to match with the date and time of the Edges.</li> </ul>
Encrypt Device Secrets	<p>Select the <b>Enable</b> check box to allow the Edge to encrypt the sensitive data across all platforms. This option is also available on the Edge <b>Overview</b> page. For more information, see <a href="#">Chapter 28 View Edge Information</a>.</p> <p><b>Note</b> For Edge versions 5.2.0 and above, before you deactivate this option, you must first deactivate the Edge using remote actions. This causes restart of the Edge.</p>
High Availability	<p>Select the <b>Enable</b> check box to apply High Availability (HA). Edges can be installed as a single standalone device or paired with another Edge to provide High Availability (HA) support.</p> <p>For more information about HA, see the <a href="#">High Availability Deployment Models</a> section.</p>
Local Contact Name	Enter the name of the site contact for the Edge.
Local Contact Email	Enter the email address of the site contact for the Edge.

- 4 Enter all the required details and click **Next** to configure the following additional options:

**Note** The **Next** button is activated only when you enter all the required details.

Option	Description
Serial Number	Enter the serial number of the Edge. If specified, the Edge must display this serial number on activation.  <b>Note</b> When deploying virtual VMware SD-WAN Edges on AWS Edges, make sure to use the instance ID as the serial number for the Edge.
Description	Enter an appropriate description.
Location	Click the <b>Set Location</b> link to set the location of the Edge. If not specified, the location is auto-detected from the IP address when the Edge is activated.

- 5 Click **Add Edge**. The Edge gets provisioned with an activation key.

**Note** The activation key expires in one month if the Edge device is not activated against it. For information on how to activate an Edge, see the *Configure Edge Activation* section in the *Edge Activation Quick Start Guide*.

- 6 After you have provisioned an Edge, the Edge appears in the **Edges** screen.

If you have configured the Edge 510-LTE device or the 610-LTE device (version 4.2.0 release), you can run the **LTE Modem Information** diagnostic test. This test will retrieves diagnostic information, such as signal strength, connection information, and so on. For information on how to run a diagnostic test, see [Chapter 36 Testing and Troubleshooting](#).

To manage the provisioned Edges, see [Chapter 25 Manage Edges](#).

To view Edge details or to make any changes to the Edge, see [Chapter 28 View Edge Information](#).

To configure an Edge, see [Chapter 29 Configure Edge Overrides](#).

# Provision a New Edge with Analytics

24

Analytics functionality is built natively into the VMware SD-WAN Edge for collecting data inline. However, by default, Analytics is deactivated for Edges. Enterprise Administrators can create Analytics Edges only when the Analytics functionality is activated.

To create a new SD-WAN Edge with Analytics, perform the following steps.

## Prerequisites

- Ensure that all the necessary system properties to activate Analytics are properly set in the SASE Orchestrator. For more information, see *Activate VMware Edge Intelligence on a VMware SASE Orchestrator* in the *VMware SD-WAN Operator Guide*, or contact your Operator Superuser.
- Ensure that the Analytics functionality is activated for the Customer before provisioning an Analytics Edge.

---

**Note** For more information, see *VMware Edge Intelligence Configuration Guide* available at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

---

- The SASE Orchestrator must be on 5.0.1.0 and the SD-WAN Edges must be running a minimum of 4.3.1 code. You can review the software image installed on each Edge in the **SD-WAN** service of the Enterprise portal, by navigating to **Configure > Edges**. The table on the **Edges** page consists of a column that displays Software version of Edge per Customer.
- If the Edge is using the 4.2 release, ensure the Edge has a LAN interface that is up and advertised or use the special MGMT-IP software build, otherwise the Edge will not be able to send metrics to the EI backend.

## Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.

**2** In the **Edges** screen, click **Add Edge**.

The **Provision an Edge** screen appears.

Provision an Edge SD-WAN + Analytics

Edge Requirements Name / Model / Profile / License / Authentication / HA / Contact / Analytics Mode

Mode \* ⓘ  SD-WAN Edge  Enable Analytics  Analytics Only Edge

Name \* test

Model \* Virtual Edge

Profile \* ⓘ Quick Start Profile

Edge License \* ENTERPRISE | 10 Mbps | North America, Europe M

Authentication ⓘ Certificate Acquire

Encrypt Device Secrets  Enable

ⓘ For Edge versions 5.2.0 and above, before you deactivate this option, you must first deactivate the Edge using remote actions. This action causes restart of this Edge.

High Availability  Enable

Contact

Local Contact Name \* Super User

Local Contact Email \* super@velocloud.net

**NEXT**

2. Additional Serial Number / Description / Location

Serial Number ⓘ  Example: VC00000490

Description

Location ⓘ

**ADD EDGE** **CANCEL**

**3** You can configure the following options:

Option	Description
Mode	<p>Select a mode:</p> <ul style="list-style-type: none"> <li>■ <b>SD-WAN Edge:</b> Allows monitoring, diagnostics, and configuration capabilities, including fault isolation and application specific analytics that can alert you when an incident occurs on your Edge.</li> <li>■ <b>SD-WAN Edge with Analytics Enabled:</b> Allows access to all the analytics for the Edge as well as full suite of branch analytic features.</li> <li>■ <b>Analytics Only Edge:</b> Allows monitoring the health, performance, and security of your LAN along with troubleshooting the problems.</li> </ul> <p><b>Note</b> You must delete the Edge and reconfigure it in order to change it back to an <b>SD-WAN Edge</b>.</p>
Name	Enter a unique name for the Edge.
Model	Select an Edge model from the drop-down menu.
Profile	<p>Select a Profile to be assigned to the Edge, from the drop-down menu. For information on how to create a new Profile, see <a href="#">Create Profile</a>.</p> <p><b>Note</b> If an <b>Edge Staging Profile</b> is displayed as an option due to Edge Auto-activation, it indicates that this Profile is used by a newly assigned Edge, but has not been configured with a production Profile.</p>
Edge License	Select an Edge license from the drop-down menu. The list displays the licenses assigned to the Enterprise, by the Operator.

Option	Description
Authentication	<p>Choose the mode of authentication from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Deactivated:</b> Edge uses a pre-shared key mode of authentication.</li> </ul> <p><b>Warning</b> This mode is not recommended for any customer deployments.</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Acquire:</b> This mode is selected by default and is recommended for all customer deployments. With <b>Certificate Acquire</b> mode, certificates are issued at the time of Edge activation and renewed automatically. The Orchestrator instructs the Edge to acquire a certificate from the certificate authority of the SASE Orchestrator by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the SASE Orchestrator and for establishment of VCMP tunnels.</li> </ul> <p><b>Note</b> After acquiring the certificate, the option can be updated to <b>Certificate Required</b>, if needed.</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Required:</b> This mode is only appropriate for customer enterprises that are "static". A static enterprise is defined as one where no more than a few new Edges are likely to be deployed and no new PKI oriented changes are anticipated.</li> </ul> <p><b>Important</b> <b>Certificate Required</b> has no security advantages over <b>Certificate Acquire</b>. Both modes are equally secure and a customer using <b>Certificate Required</b> should do so only for the reasons outlined in this section.</p> <p><b>Certificate Required</b> mode means that no Edge heartbeats are accepted without a valid certificate.</p> <p><b>Caution</b> Using this mode can cause Edge failures in cases where a customer is unaware of this strict enforcement.</p>

Option	Description
	<p>With this mode, the Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges by editing the Orchestrator's System Properties. For more information, contact your Operator.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ With the Bastion Orchestrator feature enabled, the Edges that are to be staged to Bastion Orchestrator should have the authentication mode set to either <b>Certificate Acquire</b> or <b>Certificate Required</b>.</li> <li>■ When an Edge certificate is revoked, the Edge is deactivated and needs to go through the activation process. The current QuickSec design checks certificate revocation list (CRL) time validity. The CRL time validity must match the current time of Edges for the CRL to have impact on new established connection. To implement this, ensure the Orchestrator time is updated properly to match with the date and time of the Edges.</li> </ul>
Encrypt Device Secrets	<p>Select the <b>Enable</b> check box to allow the Edge to encrypt the sensitive data across all platforms. This option is also available on the Edge <b>Overview</b> page. For more information, see <a href="#">Chapter 28 View Edge Information</a>.</p> <p><b>Note</b> For Edge versions 5.2.0 and above, before you deactivate this option, you must first deactivate the Edge using remote actions. This causes restart of the Edge.</p>
High Availability	<p>Select the <b>Enable</b> check box to apply High Availability (HA). Edges can be installed as a single standalone device or paired with another Edge to provide High Availability (HA) support. For more information about HA, see the <a href="#">High Availability Deployment Models</a> section.</p>
Local Contact Name	Enter the name of the site contact for the Edge.
Local Contact Email	Enter the email address of the site contact for the Edge.

- 4 Enter all the required details and click **Next** to configure the following additional options:

---

**Note** The **Next** button is activated only when you enter all the required details.

---

Option	Description
Serial Number	Enter the serial number of the Edge. If specified, the Edge must display this serial number on activation. <b>Note</b> When deploying virtual VMware SD-WAN Edges on AWS Edges, make sure to use the instance ID as the serial number for the Edge.
Description	Enter an appropriate description.
Location	Click the <b>Set Location</b> link to set the location of the Edge. If not specified, the location is auto-detected from the IP address when the Edge is activated.

## 5 Click **Add Edge**.

An Analytic Edge is provisioned for the selected Customer. Once the Edge is provisioned, the Analytics functionality collects data, performs deep packet inspection of all traffic, identifies network application and correlates traffic with user information.

### What to do next

To send the collected analytics data to the Cloud Analytics Engine, you must configure an Analytics interface on which the Edge transmits Analytics data. For more information, see [Configure Analytics Settings on an Edge](#).

## Configure Analytics Settings on an Edge

Analytics Interface specifies the interface and interface IP that an Edge uses for SNMP polling, receiving AMON, traps, and so on. Once you have provisioned an Analytics Edge, you can override the default Analytics settings on the Global segment for the Edge on the **Device** settings page.

To configure Analytics settings on an existing SD-WAN Edge, perform the following steps:

### Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
  - Select an Edge for which you want to configure Analytics settings, and then click the **View** link in the **Device** column.
- The **Device** settings page for the selected Edge appears.
- From the **Segment** drop-down menu, select **Global Segment** to configure an Analytics interface.

---

**Note** Currently, source interface and Analytics flag are only supported for the **Global Segment**. Settings for non-global segments are ignored even if set.

- 4 Under **Connectivity** area, go to the **Analytics** section, and then turn on the toggle button if you want to override the default Analytics settings on the Global segment for the Edge.

The screenshot shows the VMware SD-WAN Edge configuration interface. At the top, it displays '1729-Edge' and 'Offline'. The 'SD-WAN + Analytics' tab is selected. A 'Segment' dropdown is set to 'GLOBAL SEGMENT'. On the right, there's a 'SHORTCUTS' section with several 'Segment Agnostic' buttons. Below the segment dropdown, there are several sections with 'Override' checkboxes: 'VLAN', 'Loopback Interfaces', 'Management Traffic', 'ARP Timeouts', 'Interfaces', 'Global IPv6' (which is checked), 'Wi-Fi Radio', 'Common Criteria Firewall', and 'Analytics' (which is also checked). In the 'Analytics Management Interface' section, the 'Analytics Management Interface' dropdown is set to 'Auto'. A note below it states: 'The interface only needs to be set if the Edge is going to send/receive SNMP or Telemetry from local systems like wireless controllers.' Under 'Self Healing', the toggle switch is off. In the 'Advanced settings' section, there's a 'Override Default Destination' checkbox with a note: 'Not recommended unless instructed to override by support'. Below it, there are 'Destination' options: 'Dynamic IP' (selected) and 'Static IP'.

- 5 You can configure the following options:

Option	Description
<b>Analytics Management Interface</b>	Select an Analytics interface for the Edge to ingest data. By default, <b>Auto</b> is selected.  <b>Note</b> The Edge automatically selects an interface with 'Advertise' field set as the Analytics interface, if the <b>Analytics</b> button is not turned ON or the <b>Analytics</b> button is ON and the Analytics Interface is set to <b>None</b> .
<b>Self-Healing</b>	Turn on this option to activate the Self-Healing feature for the selected Edge. For more information, see <a href="#">Activate Self-Healing for SD-WAN Edges</a> .
<b>Override Default Destination</b>	A destination IP address is required to allow communication between an Analytics Edge and Cloud Analytics Engine. Select this check box to override the default destination.
<b>Destination</b>	The default destination is <b>Dynamic IP</b> . You can change it to <b>Static IP</b> only if you select <b>Override Default Destination</b> check box.

- 6 Click **Save Changes**.

#### What to do next

- To view the Analytics data, see [View Analytics Data](#).

# Activate Self-Healing for SD-WAN Edges

Self-Healing feature enables VMware SD-WAN Enterprise and Managed Service Provider (MSP) users to activate and configure Self-Healing capabilities at the Customer, Profile, and Edge level.

Once the Operator user activates the Self-Healing feature for an Enterprise in SASE Orchestrator, VMware Edge Intelligence (EI) monitors and tracks the VMware SD-WAN network for systemic and application performance issues across Edges. EI then gathers data regarding Self-Healing actions and triggers remediation recommendations to the users on the SD-WAN side directly through the incident alert email. For more information about Self-Healing feature, see the *Self-Healing Overview* section in the *VMware Edge Intelligence User Guide* published at <https://docs.vmware.com/en/VMware-Edge-Intelligence/index.html>.

**Note** Currently, only Manual remediation is supported by EI. Automatic remediation support is planned in future releases.

To activate Self-Healing for all Edges, perform the following steps:

- 1 Log in to the SASE Orchestrator as an Enterprise user.
- 2 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
- 3 To activate Self-Healing for all Edges, select all Edges by clicking the check boxes before the **Name** Column and then select **Analytics Settings** from the **More** menu.

Name	Certificates	Profile	Analytics
b1-edge1	0	Quick Start Profile	Application and Branch Analytics
b2-edge1	0	Quick Start Profile	Application and Branch Analytics
b3-edge1	0	edge-3-profile	Application and Branch Analytics
b4-edge1	0	edge-4-profile	Application and Branch Analytics
Hub-10 (b6-e)	0	Hubs	None
hub-20 (b7-e)	0	Hubs	None
hub-30 (b8-e)	0	Hubs	None

- 4 In the **Change Analytics Settings** dialog box that appears, turn on the **Analytics Mode** and **Self Healing** functionality, and then click the **Update** button.

The Self-Healing feature is activated for all Edges.

## Activate Self-Healing for a Specific Edge

To activate Self-Healing for a specific Edge, perform the following steps:

- 1 Log in to the SASE Orchestrator as an Enterprise user.
- 2 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.

- 3 To activate Self-Healing for a specific Edge, click the link to an Edge or click the **View** link in the Device column. The **Device** page appears.
- 4 Under **Connectivity**, navigate to the **Analytics** section and turn on the **Analytics Mode** and **Self Healing** functionality and click the **Update** button.

The Self-Healing feature is activated for the selected Edge.

# Manage Edges

25

Edges inherit the configurations from the associated profile. You can choose to override the settings for a specified Edge.

You can provision a new Edge or manage the existing Edges using the Orchestrator UI. To provision a new Edge, see [Provision a New Edge with New Orchestrator UI](#).

## To manage the existing Edges:

- 1 In the **SD-WAN** service of the Enterprise portal, click the **Configure** tab.
- 2 From the left menu, click **Edges**.
- 3 The **Edges** page displays the existing Edges with their details.

Option	Description
Name	Displays the name of the Edge. Click the link to the Edge to modify the Edge configurations. See <a href="#">Chapter 29 Configure Edge Overrides</a> .
Certificates	Displays the current and expired certificates of the Edge. Click <b>View</b> to display Certificate details of the corresponding Edge. The pop-up window allows you to download, revoke, or renew a certificate.
Profile	Displays the Profile assigned to the Edge. Click the link to the Profile to modify the Profile configurations. See <a href="#">Configure Profile settings</a> .

Option	Description
Operator Profile	Displays the name of the Operator profile associated with the Edge. This column is available only for an Operator user. The Operator Profile is the template assigned to the customer, which includes the software image, application maps, Gateway selection, and the management settings of the Edge.
Analytics	Displays the analytics details of the Edge if the Edge Intelligence service is activated.
Secrets Encryption	Displays secret key encryption details for the Edge.
HA	Displays whether High Availability is activated for the Edge.
Device	Click <b>View</b> to modify the configurations of the Edge. See <a href="#">Chapter 29 Configure Edge Overrides</a> .
Business Policy	Click <b>View</b> to configure the Business Policy Rules of an Edge.
Firewall	Click <b>View</b> to configure the Firewall Rules of an Edge.
Alerts	Displays whether Customer alerts are activated or deactivated for the Edge.
Operator Alerts	Displays whether Operator alerts are activated or deactivated for the Edge.
Software Version	Displays the software version of the Edge.
Build Number	Displays the build number of the Edge, when the Edge is activated.
Model	Displays the model type of the Edge.

4 Select one or more Edges to perform the following activities:

Option	Description
Assign Profile	Allows to change the profile for the selected Edges. This operation affects the existing configurations of the Edges.
Assign Edge License	Allows to modify the Edge license for the selected licenses.
Download	Downloads the details of Edges into an MS Excel file.

Click **More** to configure the following:

Option	Description
Update Alerts	Allows to turn on or turn off the alerts sent to the Customer. To configure the alerts, see <a href="#">Configure Alerts</a> . You can view the alerts in the <b>Monitor &gt; Alerts</b> tab.
Update Operator Alerts	Allows to turn on or turn off the alerts sent to the Operator. To configure the alerts, see <a href="#">Configure Alerts</a> . You can view the alerts in the <b>Monitor &gt; Alerts</b> tab.
	<b>Note</b> This option is available only for an Operator user.
Local Credentials	Allows to modify the local credentials. By default, the local credentials include a default username as <b>admin</b> and a randomly generated password.
Assign Operator Profile	This option is available only for an Operator user. By default, all the Edges inherit the Operator profile assigned to the Enterprise customer. If required, an Operator can assign another Operator profile for specific Edges.
Rebalance Gateways	A Gateway rebalance can be triggered to move SD-WAN Edges to a different Gateway. When triggering a Gateway rebalance, the Orchestrator will attempt to equally distribute the load within Gateways in a pool. Though rebalancing is not impactful, these rebalancing events typically take place during regularly scheduled maintenance windows out of an abundance of caution.
	<b>Note</b> Refer to the <i>SD-WAN Gateway Migration FAQs</i> , <i>Important Caveats</i> , and <i>Allow List Limitation</i> sections in the <a href="#">KB article</a> for complete details.
	<b>Note</b> The <b>Rebalance Gateways</b> option is available only for Operator users.
Delete Edge	Deletes the selected Edges. You cannot delete the Edges that are connected to the Enterprise. You need to shutdown the Edge to delete it.

Read the following topics next:

- [Configure Edge Settings](#)
- [Reset Edges to Factory Settings](#)

## Configure Edge Settings

Configuration overrides can be made to some settings that were assigned to an Edge. In most cases, an override must first be enabled, and then changes can be made. Edge overrides enable Edge specific edits to the displayed settings, and discontinue further automatic updates from the configuration Profile.

To override configuration settings for a specific Edge:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.

- 3 The **View** drop-down menu at the left side of the page allows the user to select the view options. The available options are **Expand All** and **Collapse All**. By default, the settings are collapsed.

- 4 The **Sort** drop-down menu at the left side of the page allows the user to select the sort options: **Sort by category** and **Sort by segment aware**. You can view the configuration settings sorted by category or segment aware. By default, the settings are sorted by category. If you choose to sort by segmentation, the settings are grouped as segment aware and segment agnostic.
- 5 For some of the settings, the configuration is inherited from the associated Profile. To edit inherited configuration for the Edge, select the **Override** check box.
- 6 After modifying the required settings, click **Save Changes**.

---

**Note** On the **Device** page, whenever you make configuration changes for the selected Edge, a footer notification appears at the left bottom corner of the screen. You can click the notification to view the recent configuration changes.

- 7 Click the **Shortcuts** option to perform the following activities:
  - **Monitor** – Navigates to the Monitoring tab of the selected Edge. See [Monitor Edges](#).
  - **View Events** – Displays the Events related to the selected Edge.
  - **Remote Diagnostics** – Enables to run the Remote Diagnostics tests for the selected Edge. See [Run Remote Diagnostics](#).
  - **Generate Diagnostic Bundle** – Allows to generate Diagnostic Bundle for the selected Edge. See [Diagnostic Bundles for Edges](#).
  - **Remote Actions** – Allows to perform the Remote actions for the selected Edge. See [Remote Actions](#).
  - **View Profile** – Navigates to the Profile page, that is associated with the selected Edge.
  - **View Gateways** – Displays the Gateways connected to the selected Edge.

For more details on various Edge configuration settings, see [Chapter 29 Configure Edge Overrides](#).

## Reset Edges to Factory Settings

SD-WAN Edges are required to be reset to factory settings for several reasons, some of which are as follows:

- When you repurpose the Edge for another site, you must clear the existing configuration so that the Edge can be activated to the new site.
- Your site is encountering an issue for which VMware SD-WAN Support recommends that you perform a hard reset to revert the Edge to factory settings and reactivate the Edge to the site to see if that resolves the issue.
- The Edge is inaccessible or non-responsive and multiple power cycles are not resolving the issue. It is recommended that you perform a hard reset to revert the Edge to factory settings and see if that resolves the issue.

You can reset an Edge to factory settings using one of the following methods:

- Soft Reset or Deactivation—The Edge is deactivated and all the existing configuration that the Edge is using is completely removed. The Edge now uses the original factory configuration. However, the Edge software is not affected and it retains the software version it had prior to the soft reset. A soft reset Edge can be reactivated to another site or to the same site.
- Hard Reset—The Edge is fully reset to factory settings, that is the Edge is not only deactivated and uses the factory configuration, but the Edge software is also changed to the factory software version. The Edge is effectively as it was when it was shipped from the factory.

If you reset an Edge that is actively used at a site, you will completely lose the client device connectivity at the site until you either reactivate the same Edge at the site or activate another Edge at the site.

For instructions on how to reset an Edge to factory settings, see [How to Factory Reset a VMware SD-WAN Edge](#).

# Activate SD-WAN Edges

26

You can deploy and activate SD-WAN Edges using the following two methods:

- Edge Auto-activation (formerly known as Zero Touch Provisioning) — In this method, you must power-on the Edges and connect them to the internet. This causes the Edges to automatically start working as configured. For more information, refer to [Activate SD-WAN Edges using Edge Auto-activation](#).
- Email — In this method, the Edges are shipped to the Customer site with a factory-default configuration. Prior to activation, the Edges contain no configuration or credentials to connect to the Enterprise network. The administrator initiates an email with instructions to activate the Edges to the person who will install the Edges at the site. The individual to whom the email is sent follows the instructions to activate the Edges. For more information, refer to [Activate SD-WAN Edges Using Email](#).

Following table shows a comparison of activities that are allowed in each of the activation methods:

Activity	Edge Auto-activation (Central NOC Activates)	Email (Office Admin Activates)
No IT Visit Required	✓	✓
No Pre-staging Required	✓	✓
No Security Risk if Box Is Lost	✓	✓
No Site-by-site Link Profile Needed	✓	✓
No Device Tracking Needed		✓
Requires Email to Office Admin		✓
Requires Knowledge of Device to Site		✓

Read the following topics next:

- [Activate SD-WAN Edges using Edge Auto-activation](#)
- [Activate SD-WAN Edges Using Email](#)
- [Request RMA Reactivation](#)

## Activate SD-WAN Edges using Edge Auto-activation

Edge Auto-activation allows you to activate Edges by powering on the Edges and connecting them to the Internet.

---

**Note** Starting from the 5.1.0 release, **Zero Touch Provisioning** is renamed as **Edge Auto-activation**.

---

This method eliminates the need of an activation link. Using this feature, the Service Provider can preconfigure the Edges and have them shipped to the Customers. The Customers just need to power-on the Edges and connect the cables to the internet to activate the Edges.

This method of Edge activation is also useful when the person at the remote site is unable to connect a laptop/tablet/phone to the SD-WAN Edge, and therefore cannot use an email or cannot click an activation code/URL.

---

**Note**

- Edge Auto-activation supports Edge models: 510, 510 LTE, 6x0, and 3xx0.
  - For Edge Auto-activation to work, use the Orchestrator software version 4.3.0 or later.
- 

As an Enterprise user, complete the following tasks to activate Edges using Edge Auto-activation:

- [Sign-Up for Edge Auto-activation](#)
- [Assign Profile and License to Edges](#)
- [Assign Inventory to an Edge](#)

### Sign-Up for Edge Auto-activation

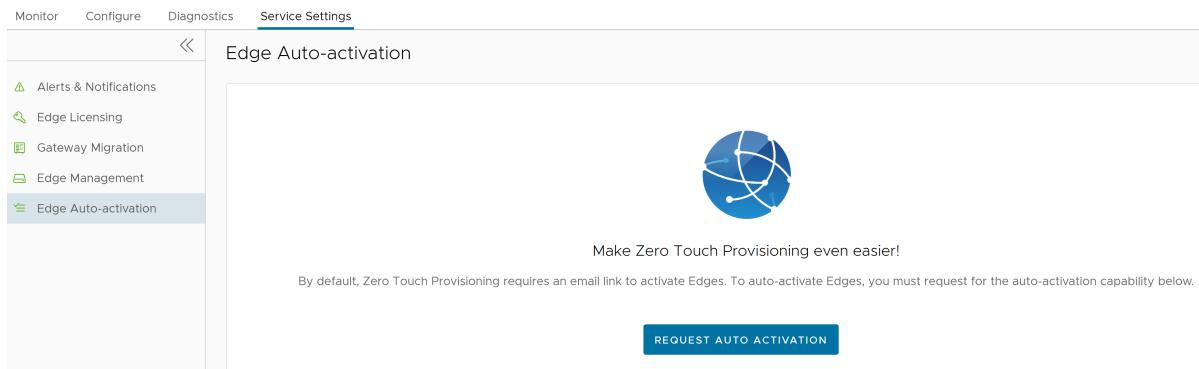
Starting from the 5.1.0 release, the procedure to sign-up for Edge Auto-activation has completely changed. You need not activate it from **System Settings** anymore. To sign-up for Edge Auto-activation, follow the below steps:

#### Prerequisites

- As an Enterprise Super User, ensure that you have a valid Subscription Identifier (SID) that was received on booking Secure Access Service Edge (SASE) orders. If you do not have a valid SID, contact [VMware Customer Support](#).
- Outbound internet connectivity via DHCP is required to complete the push activation successfully.

## Procedure

- In the **SD-WAN** service of the Enterprise portal, click **Service Settings > Edge Auto-activation**.



- Click **Request Auto Activation**. Enter the **Subscription ID (SID)**, and then click the **Request Auto-Activation** button at the bottom of the pop-up window.

**Note** You are required to enter the **Subscription ID (SID)** only when you login for the first time. You can access **Edge Auto-activation** only after the successful validation of SID. The validation process may take up to 3 to 5 days. If you enter an incorrect SID, you must contact the customer support team to get it changed.

### What to do next

You must assign a profile and a license to the Edges. For instructions, see [Assign Profile and License to Edges](#).

## Assign Profile and License to Edges

To assign profile and license to the Edges:

### Prerequisites

Ensure that you have signed-up for Edge Auto-activation so that you can view the list of Edges in the **Available Inventory** page. For instructions, refer to [Sign-Up for Edge Auto-activation](#).

## Procedure

- In the **SD-WAN** service of the Enterprise portal, click **Settings**, and then from the left menu, click **Edge Auto-activation**.

The **Edge Auto-activation** page is displayed.

The screenshot shows the 'Edge Auto-activation' interface. At the top, there are two tabs: 'Available Inventory' (which is selected) and 'Assigned Inventory'. Below the tabs is a search bar and a refresh button. Underneath is a table with columns for 'Serial Number' and 'Model'. The table contains 10 rows, each representing an unassigned Edge. The data is as follows:

Serial Number	Model
VC2	Edge 5X0
VC3	Edge 6X0
VC4	Edge 6X0
VC5	Edge 6X0
VC6	Edge 6X0
VC7	Edge 6X0
VC8	Edge 6X0
VC9	Edge 6X0
VC10	Edge 510-LTE
VC11	Edge 510

At the bottom of the table are buttons for 'COLUMNS' and 'REFRESH', and a note indicating '10 items'.

- The **Available Inventory** tab displays the list of unassigned Edges with Serial Number and Model.

**Note** Only the Edges that were shipped to you after the successful completion of the sign-up process appear in the **Available Inventory** tab. Ensure that the SID assigned to you is used in all your future orders so that the inventory is reflected correctly.

- Select the required Edges and click **Assign**. The **Edge Assignment** window appears:

The screenshot shows the 'Edge Assignment' dialog box. At the top, it says 'Select a Profile and Edge License to be assigned to all the Edges.' Below are two dropdown menus: 'Profile \*' set to 'Quick Start Profile' and 'Edge License \*' set to 'ENTERPRISE | 1 Gbps | A:'. The main area is a table with columns for 'Serial Number', 'Model', 'Profile', and 'Edge License'. It contains two rows for 'VC4' and 'VC5', both assigned to 'Quick Start Profile' and 'ENTERPRISE | 1 Gbps | A:'. At the bottom are 'CANCEL' and 'ASSIGN' buttons.

Serial Number	Model	Profile	Edge License
VC4	Edge 6X0	Quick Start Profile	ENTERPRISE   1 Gbps   A:
VC5	Edge 6X0	Quick Start Profile	ENTERPRISE   1 Gbps   A:

At the bottom right are 'CANCEL' and 'ASSIGN' buttons.

- 4 From the **Profile** and **Edge License** drop-down lists, select the required profile and license that you wish to assign to all the Edges in the inventory. You can choose to override these settings for a specific Edge, by selecting the appropriate profile and license in the table.

- 5 Click the **Assign** button.

The Edges for which you have assigned a profile and license appear in the **Assigned Inventory** tab. The **Inventory State** for the assigned Edges is displayed as **Assigned to Customer** and the **Edge State** is displayed as **Pending**.

- 6 Following are the additional options available on the **Edge Auto-activation** page:

Option	Description
Search	Enter a search term to search for the matching text across the page. Use the advanced search option to narrow down the search results.
Download CSV	Click to download the list of Edges in an excel format.
Columns	Click and select the columns to be displayed or hidden on the page.
Refresh	Click to refresh the page to display the most current data.

#### What to do next

Power-on the assigned physical Edges and connect them to the internet so that they are redirected to the SASE Orchestrator where they are automatically activated. After an Edge is activated, the **Edge State** in the **Assigned Inventory** tab changes from **Pending** to **Activated**.

## Assign Inventory to an Edge

After you assign the profile and license to an Edge and till the time you power-on the Edge to activate it, SASE Orchestrator allows you to delete the Edge. If you have accidentally deleted an Edge, you can choose to provision a new logical Edge and reassign the inventory to the logical Edge so that when you power-on the physical Edge, the Edge Auto-activation feature works and the physical Edge is activated.

To assign inventory to a logical Edge:

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
- 2 Click **Add Edge**. The **Provision an Edge** page appears.
- 3 Enter a name for the Edge, and then select the required model, profile, and license.
- 4 Click **Add Edge**. The newly added logical Edge appears in the **Available Inventory** page of the **Edge Auto-activation** window.
- 5 Select the logical Edge entry that you just created, and then click **Assign**.

- Select the Profile and Edge License in the **Edge Assignment** window, and then click **Assign**.

## Activate SD-WAN Edges Using Email

In this method, the SD-WAN Edge is shipped to the Customer site with a factory-default configuration. Prior to activation, the SD-WAN Edge contains no configuration or credentials to connect to the Enterprise network.

Complete the following steps to activate Edges using the Email method:

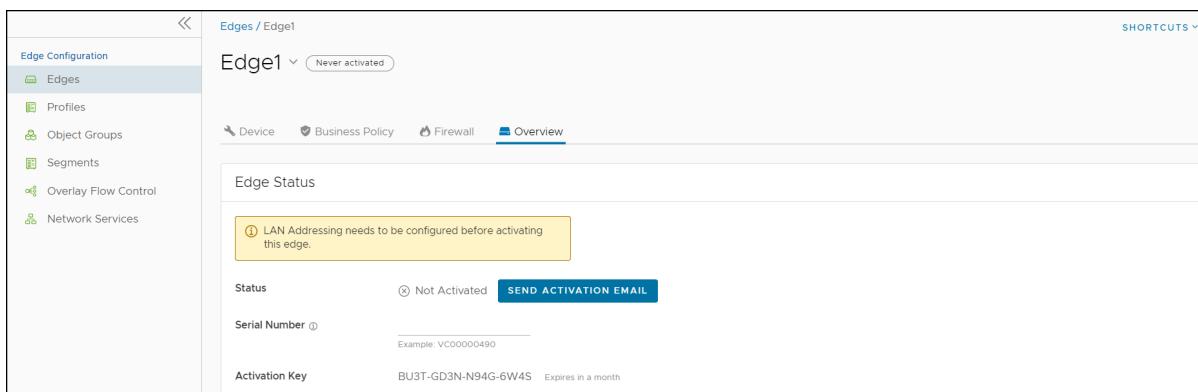
- Send an Activation Email. The administrator initiates the activation process by sending an activation procedure email to the person that will install the Edge, typically a Site Contact. For more information, see [Send Edge Activation Email](#).
- Activate the Edge Device. The instructions in the activation procedure email activates the Edge device. For more information, refer to [Activate an Edge Device](#).

### Send Edge Activation Email

The administrator initiates the activation process of an Edge by sending an activation procedure Email to the person installing the Edge, typically a Site Contact.

To send the Edge Activation Email:

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
- The **Edges** page displays the existing Profiles.
- Click the link to the Edge to be activated or click the **View** link in the **Device** column of the Edge.
- Click the **Overview** tab. For an Edge that is not activated, the **Edge Status** section displays the option to send an activation Email:



- Click **Send Activation Email**.

Send Activation Email

Once the edge has been provisioned, an activation key will be generated and the activation email will be sent.

Edge	Edge1
From	
To *	jdoe@acme.com
CC	
Subject *	Edge Activation

Dear customer,  
To activate your Edge, please follow these steps:  
1. Connect your device to power and any Internet cables or USB modems.  
2. Find and connect to the Wi-Fi network that looks like "velocloud-" followed by 3 more letters/numbers (e.g. "velocloud-01c") and use "vcsecret" as the password. If your device does not have Wi-Fi, connect to it using an Ethernet cable.  
**Note:** Wi-Fi supports only for IPv4. For IPv6, please use the Ethernet cable.  
3. Click the following link to activate your edge

If you experience any difficulty, please contact your IT admin.

IP Version ⓘ  Send IPv4 address link  Send IPv6 address link

**CANCEL** **SEND**

- 6 Enter the details like Email address of the recipient, the Site contact, and Subject line. A default Email message is available. If required, you can add the contact details of IT admin in the message. Select the IP version of the activation link to be sent. You can select the link to contain either IPv4 address or IPv6 address, or both.
- 7 Click **Send** and the activation Email is sent to the Site contact.

Once the Site contact receives the activation Email, the person can activate the Edge. For more information, see [Activate an Edge Device](#).

#### Note

- For the Edge 510 LTE device, the Activation Email consists of Cellular Settings like SIM PIN, Network, APN, and Username. A supported factory default image is required.
- For the 610, 620, 640, 680, and 610 LTE devices with SFP that are configured with ADSL2/VDSL2, the activation email consists of configuration settings like Profile, PVC, VPC, and so on. A supported factory default image is required.

#### Remote Diagnostics for 510 LTE and 6XO Devices:

- If you configure the SD-WAN Edge 510 LTE device, you can run the "LTE Modem Information" diagnostic test for troubleshooting purposes. The **LTE Modem Information** diagnostic test will retrieve diagnostic information, such as signal strength, connection information, etc..

- The **DSL Status** diagnostic test is available only for the 610, 620, 640, and 680 devices. Running this test will show the DSL status, which includes information such as Mode (Standard or DSL), Profile, xDSL Mode, and so on.

For information on how to run a diagnostic test, see the *VMware SD-WAN Troubleshooting Guide* published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

## Activate an Edge Device

The Site Contact performs the steps outlined in the Edge activation procedure email.

In general, the Site Contact completes the following steps:

- 1 Connect the Edge to a power source and insert any WAN link cables or USB modems for Internet connectivity.
- 2 Connect a personal computer or mobile device (with access to the activation email) to your Edge by one of two methods:

---

**Note** The connected personal computer or mobile device cannot directly access the public internet through the Edge device until it is activated.

---

- a Find and connect to the Wi-Fi network that looks like `velocloud-` followed by three more letters/numbers (for example, `velocloud-01c`) with the password `vcsecret`.

---

**Note** Refer to the Wi-Fi SSID from the Edge device. The default Wi-Fi is `vc-wifi`. The Edge activation email provides instructions for using one or more Wi-Fi connections.

---

- b If the Edge is not Wi-Fi capable (for example, a 6xON model or a 3x00 model), use an Ethernet cable to connect to either an Ethernet-equipped computer or a mobile device with an Ethernet adapter to one of the Edge's LAN ports.

---

**Note** For more information about using either an iOS or Android mobile device with an Ethernet adapter to activate an Edge, refer to the below sections:

- [Edge Activation using an iOS Device and an Ethernet Cable](#)
  - [Edge Activation using an Android Device and an Ethernet Cable](#)
- 

- 3 Click the hyperlink in the email to activate the Edge.

During the Edge activation, the activation status screen appears on your connected device.

The Edge downloads the configuration and software from the SASE Orchestrator and reboots multiple times to apply the software update (If the Edge has a front LED status light, that light would blink and change colors multiple times during the activation process).

Once the Edge activation process successfully completes, the Edge is ready for service (if the Edge has a front LED status light, the light would show as solid green). Once an Edge is activated, it is “useable” for routing network traffic. In addition, more advanced functions such as monitoring, testing, and troubleshooting are also available.

## Edge Activation using an iOS Device and an Ethernet Cable

There are multiple ways to activate a VMware SD-WAN Edge. It is recommended to use the Edge Auto-activation push activation whenever possible. Alternatively, you can use the email activation (pull activation) method using an iOS device and an Ethernet cable.

### Prerequisites

The components required for this procedure are:

- iPhone/iPad with email access
- Ethernet adapter suitable for phone or tablet

---

**Note** The example used here is an Edge 540 and an iPhone 12 Pro Max. You can use other Edge and iPhone/iPad models too.

---

### Procedure

- 1 Complete the Edge configuration on the Orchestrator software. For details, refer to the *Configure Edge Device* section in the *VMware SD-WAN Administration Guide*.
- 2 Navigate to **Configure > Edges > Edge Overview tab**, and then click the **Send Activation Email** button.
- 3 Enter the email address of the person activating the Edge, and then click **Send**.
- 4 Power up the Edge, and then connect it to an available internet connection using an Ethernet cable.

---

**Note** Refer to [Edge Activation Guides](#) to check details of the model you are installing to determine the correct port.

---

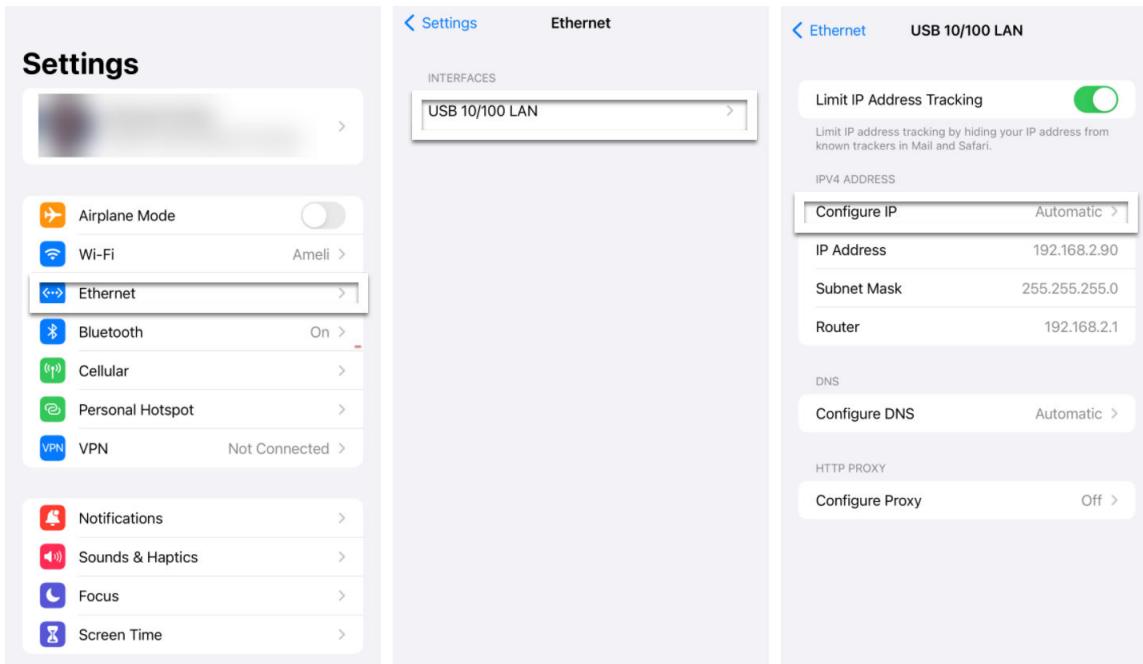
- 5 Connect an Ethernet adapter to your phone, and then connect the Edge's LAN port to the Ethernet adapter.

---

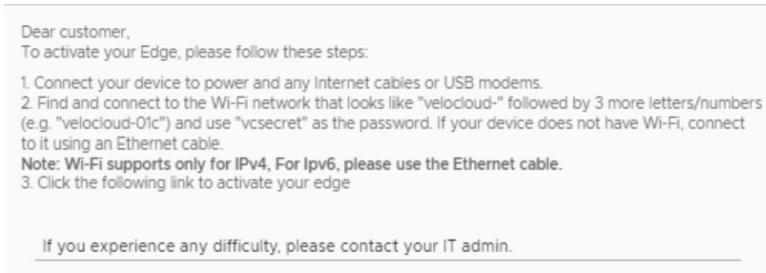
**Note** The Edge is configured by default to acquire a DHCP IP address from the ISP on the WAN (uplink). The Edge also assigns a DHCP address to the phone connected to the LAN port. When the WAN connection is fully operational, the cloud LED on the front of the Edge turns green.

---

- 6 In your iOS device, go to **Settings > Ethernet**. Select the appropriate interface. Under the IPv4 Address, select **Configure IP** as **Automatic**.



- 7 Open the activation email from your phone, and then click the activation link displayed at the bottom of the screen to activate your Edge. The following screenshot is an example.



- 8 You can see the activation progress on your phone screen. Once complete, **Activation successful** message is displayed.

## Results

Your Edge device is now activated.

## Edge Activation using an Android Device and an Ethernet Cable

The procedure below describes the Edge email activation (pull activation) using an Android device and an Ethernet cable.

## Prerequisites

The components required for this procedure are:

- Android phone with email access
- Ethernet adapter suitable for the phone

---

**Note** The example used here is an Edge 610 and a Samsung Galaxy S10+ smartphone. You can use other Edge and Android phone models too.

## Procedure

- 1 Complete the Edge configuration on the Orchestrator software. For details, refer to the *Configure Edge Device* section in the *VMware SD-WAN Administration Guide*.
- 2 Navigate to **Configure > Edges > Edge Overview tab**, and then click the **Send Activation Email** button.
- 3 Enter the email address of the person activating the Edge, and then click **Send**.
- 4 Power up the Edge, and then connect it to an available internet connection using an Ethernet cable.

---

**Note** Refer to [Edge Activation Guides](#) to check details of the model you are installing to determine the correct port.

- 5 Connect an Ethernet adapter to your phone, and then connect the Edge's LAN port to the Ethernet adapter.

---

**Note** The Edge is configured by default to acquire a DHCP IP address from the ISP on the WAN (uplink). The Edge also assigns a DHCP address to the phone connected to the LAN port. When the WAN connection is fully operational, the cloud LED on the front of the Edge turns green.

- 6 Open the activation email from your phone, and then click the activation link displayed at the bottom of the screen to activate your Edge. The following screenshot is an example.

Dear customer,  
To activate your Edge, please follow these steps:

1. Connect your device to power and any Internet cables or USB modems.
2. Find and connect to the Wi-Fi network that looks like "velocloud-" followed by 3 more letters/numbers (e.g. "velocloud-01c") and use "vcsecret" as the password. If your device does not have Wi-Fi, connect to it using an Ethernet cable.
3. Click the following link to activate your edge

**Note:** Wi-Fi supports only for IPv4. For Ipv6, please use the Ethernet cable.

If you experience any difficulty, please contact your IT admin.

- 7 You can see the activation progress on your phone screen. Once complete, **Activation successful** message is displayed.

## Results

Your Edge device is now activated.

## Request RMA Reactivation

Initiate a Return Merchandise Authorization (RMA) request either to return the existing Edge or to replace an Edge.

There are several scenarios that require an Edge RMA reactivation. Following are the two most common scenarios:

- Replace an Edge due to a malfunction—A typical scenario that requires an Edge RMA reactivation occurs when a malfunctioned Edge of the same model needs replacement. For example, a customer needs to replace a 520 Edge model with another 520 Edge model.
- Upgrade an Edge hardware model—Another common scenario that requires an Edge RMA reactivation is when you want to replace an Edge with a different model. Usually this is due to a scaling issue in which you have outgrown the capacity of the current Edge.

---

**Note** RMA reactivation request is allowed only for activated Edges.

You can initiate the RMA reactivation request using one of the following methods:

- [Request RMA Reactivation Using Edge Auto-activation](#)
- [Request RMA Reactivation Using Email](#)

## Request RMA Reactivation Using Edge Auto-activation

To request RMA reactivation using Zero Touch Provisioning:

### Procedure

- 1 Log in to SASE Orchestrator, and in the **SD-WAN** service of the Enterprise portal go to **Configure > Edges**.
- 2 Click the Edge that you want to replace. The **Edge Overview** page appears.
- 3 Scroll down to the **RMA Reactivation** area, and then click **Request Reactivation** to generate a new activation key. The status of the Edge changes to **Reactivation Pending** mode.

---

**Note** The reactivation key is valid for one month only. When the key expires, a warning message is displayed. To generate a new key, click **Generate New Activation Key**. For details, refer to *RMA Reactivation* section in the [Chapter 28 View Edge Information](#) topic.

- 4 In the **RMA Serial Number** field, enter the serial number of the new Edge that is to be activated.

- 5 From the **RMA Model** drop-down list, select the hardware model of the new Edge that is to be activated.

---

**Note** If the Serial Number and the hardware model do not match the new Edge that is to be activated, the activation fails.

- 6 Click **Update**.

The status of the new Edge changes to **Reactivation Pending** and the status of the old Edge changes to **RMA Requested**. To view the Edge State, go to **Service Settings > Edge Auto-activation**.

- 7 Complete the following tasks to activate the new Edge:
  - a Disconnect the old Edge from the power and network.
  - b Connect the new Edge to the power and network. Ensure that the Edge is connected to the Internet.

## Results

The new Edge is redirected to the SASE Orchestrator where it is automatically activated. The status of the new Edge changes to **Activated**.

## What to do next

Return the old Edge to VMware so that the logical entry for the old Edge with the state **RMA Requested** gets removed from the **Service Settings > Edge Auto-activation** page.

## Request RMA Reactivation Using Email

To request RMA reactivation using email:

### Prerequisites

### Procedure

- 1 Log in to SASE Orchestrator, and then go to **Configure > Edges**.
- 2 Click the Edge that you want to replace. The **Edge Overview** page appears.
- 3 Scroll down to the **RMA Reactivation** area, and then click **Request Reactivation** to generate a new activation key. The status of the Edge changes to **Reactivation Pending** mode.

---

**Note** The reactivation key is valid for one month only. When the key expires, a warning message is displayed. To generate a new key, click **Generate New Activation Key**. For details, refer to *RMA Reactivation* section in the [Chapter 28 View Edge Information](#) topic.

- 4 Click **Send Activation Email** to initiate the Edge activation Email with instructions. The Email consists of the instructions along with the activation URL. The URL displays the Activation key and the IP address of the SASE Orchestrator.

- 5 Complete the following tasks to activate the new Edge:
  - a Disconnect the old Edge from the power and network.
  - b Connect the new Edge to the power and network. Ensure that the Edge is connected to the Internet.
  - c Follow the activation instructions in the email. Click the activation link in the email to activate the Edge.

## Results

The Edge downloads the configuration and software from the SASE Orchestrator and gets activated.

# Configure User Account details

27

The **My Account** page allows you to configure basic user information, SSH keys, and API tokens. You can also view the current user's role and the associated privileges.

Ensure to configure privileges for a user to access Edges in a secure manner. You must choose **Basic** access level for the user. You can configure the access level when you create a new user (under User Management), and choose to modify it at a later point in time. Ensure that you have Superuser role to modify the access level for a user.

To access the **My Account** page, follow the below steps:

- 1 Click the **User** icon in the Global Navigation located at the top right of the screen.
- 2 The **User Information** panel is displayed as shown below:

The screenshot shows the VMware Orchestrator interface. On the left, the Global Navigation bar includes the VMW Orchestrator logo, Customer cust1test, SD-WAN, and a user icon. Below the navigation are tabs: Monitor (selected), Configure, Diagnostics, and Service Settings. The left sidebar under Monitor has sections: Network Overview (selected), Edges, Network Services, Routing, Alerts, Events, and Reports. The main content area displays 'Network Overview' with two circular diagrams: 'Activated Edges' and 'Links'. Both diagrams show 0 nodes and 0 connections. Below these is a table with columns: Edge Name, Status, Secrets Encryption, HA (Mode), Cluster Name, and Links. A message indicates 'No edges for this network found' with a watering can icon. At the bottom are 'COLUMNS' and 'REFRESH' buttons. On the right, the 'User Information' panel is open, showing the 'Account' section with Username: cust1test@vmware.com and Role: Enterprise Superuser, and the 'Profile' section with Email: cust1test@vmware.com. A 'MY ACCOUNT' button is highlighted. At the bottom of the interface are links for LOG OUT, Version 5.4.0.0, Build RS400-20230914-0655-QA-998c4c1f19, Legal & Terms of Service, Cookie Usage, and ©2023 VMware.

- 3 Click the **My Account** button. The following screen appears:



## My Account

Profile    Role & Privileges    API Tokens    SSH Keys

Username	super@velocloud.net
Contact Email * ⓘ	test@vmware.com
Current Password *	.....
New Password	.....
Confirm Password *	.....
First Name	Super
Last Name	User
Phone	
Mobile Phone	+1

**UPDATE**

- 4 The **Profile** tab is displayed by default. You can update the following basic user details:

Option	Description
Username	Displays the username and it is a read-only field.
Contact Email	Enter the primary contact email address of the user.
Current Password	Enter the current password.
New Password	Enter the new password.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Confirm Password	Re-enter the new password.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Phone	Enter the primary phone number of the user.
Mobile Phone	Enter the mobile number of the user along with the country code.

- 5 Click the **Role** tab to view the existing user role and description. It also displays the privileges associated with the user role.

## My Account

Profile    **Role & Privileges**    API Tokens    SSH Keys

Role

Operator Superuser

### Description

Can view, edit and create additional operators, global settings, and has full access across all services

### Privileges associated to role

> Global Settings & Administration	<input checked="" type="checkbox"/> Global Settings Operator Superuser
> SD-WAN	<input checked="" type="checkbox"/> SD-WAN Operator Superuser
> Cloud Web Security	<input checked="" type="checkbox"/> Cloud Web Security Operator Superuser
> Secure Access	<input checked="" type="checkbox"/> Secure Access Operator Superuser
> Multi Cloud	<input checked="" type="checkbox"/> MCS Operator Superuser
> App Catalog	<input checked="" type="checkbox"/> App Catalog Operator Superuser

### Privileges

Edge Access

Basic

- 6 Click the **API Tokens** tab. The following screen is displayed.

# My Account

Profile    Role & Privileges    **API Tokens**    SSH Keys

## New Token

Name *	test	
Description	test123	
Lifetime *	12	Months
<input style="background-color: #0070C0; color: white; padding: 5px; margin-right: 10px; border-radius: 5px; font-weight: bold; font-size: 10pt; border: none;" type="button" value="GENERATE KEY"/> <input style="border: 1px solid #0070C0; color: #0070C0; padding: 5px; border-radius: 5px; font-weight: bold; font-size: 10pt; border: none;" type="button" value="CANCEL"/>		

7 Enter a **Name** and **Description** for the token, and then choose the **Lifetime** from the drop-down menu.

8 Click **Generate Key**.

9 Click the **SSH Keys** tab to configure a Secure Shell (SSH) key-based authentication.

The SSH key-based authentication is a secure and robust authentication method to access VMware SD-WAN Edges. It provides a strong, encrypted verification and communication process between users and Edges. The use of SSH keys bypasses the need to manually enter login credentials and automates the secure access to Edges.

### Note

- Both the Edge and the Orchestrator must be using Release 5.0.0 or later for this feature to be available.
- Users with Operator Business or Business Specialist account roles cannot access Edges using key-based authentication.

When using key-based authentication to access Edges, a pair of SSH keys are generated - Public and Private.

The public key is stored in the database and is shared with the Edges. The private key is downloaded to your computer, and you can use this key along with the SSH username to access Edges. You can generate only one pair of SSH keys at a time. If you need to add a new pair of SSH keys, you must delete the existing pair and then generate a new pair. If a previously generated private key is lost, you cannot recover it from the Orchestrator. You must delete the key and then add a new key to gain access.

Based on their roles, users can perform the following actions:

- All users, except users with Operator Business or Business Specialist account roles, can create and revoke SSH keys for themselves.
- Operator Super users can manage SSH keys of other Operator users, Partner users, and Enterprise users, if the Partner user and Enterprise user have delegated user permissions to the Operator.
- Partner Super users can manage SSH keys of other Partner users and Enterprise users, if the Enterprise user has delegated user permissions to the Partner.
- Enterprise Super users can manage the SSH keys of all the users within that Enterprise.
- Super users can only view and revoke the SSH keys for other users.

---

**Note** Enterprise and Partners Customers without SD-WAN service access are not able to configure or view SSH keys related details.

Click the **SSH Keys** tab, and then click the **Generate Key** button. The following screen appears:

X

## My Account

[Profile](#)   [Role & Privileges](#)   [API Tokens](#)   [SSH Keys](#)

### Generate SSH Key

User Name \*  
o2super\_velocloud\_net

Actions \*  
 Generate Key    Enter Key

#### Enter Key

test11234@

Duration \* ⓘ  
30 Days

**ⓘ** The default file format is .pem (for use with OpenSSH). If you are using a Windows OS, ensure that you convert the file format from .pem to .ppk.

**GENERATE KEY**

**CANCEL**

Option	Description
User Name	Displays the username and it is a read-only field.
Actions	Select either one of the following options: <ul style="list-style-type: none"> <li>■ <b>Generate key:</b> Use this option to generate a new pair of public and private SSH keys.   <b>Note</b> The generated key gets downloaded automatically. The default file format in which the SSH key is generated is .pem. If you are using a Windows operating system, ensure that you convert the file format from .pem to .ppk, and then import the key. For instructions to convert .pem to .ppk, see <a href="#">Convert Pem to Ppk File Using PuTTYgen</a>.</li> <li>■ <b>Enter key:</b> Use this option to paste or enter the public key if you already have a pair of SSH keys.</li> </ul>
PassPhrase	If <b>Generate key</b> option is selected, then you have to enter a unique passphrase to further safeguard the private key stored on your computer.  <b>Note</b> This is an optional field and is available only if you select the <b>Generate Key</b> action.
Duration	Select the number of days by when the SSH key must expire.

10 Click **Generate Key**.

---

**Note** Only one SSH Key can be created per user.

11 To deactivate an SSH token, click the **Revoke** button. A pop-up window appears, to confirm the revoke operation. Select the check box, and then click **Revoke** to permanently revoke the key.

The SSH keys for a user are automatically deleted when:

- You change the user role to Operator Business or Business Specialist because these roles cannot access Edges using key-based authentication.
- You delete a user from the Orchestrator.

**Note** When a user is deleted or deactivated from the external SSO providers, the user can no longer access the Orchestrator. But the user's Secure Edge Access keys remain active until the user is explicitly deleted from the Orchestrator as well. Therefore, you must first delete the user from the IdP, before deleting from the Orchestrator.

---

**What to do next:**

Ensure that you enable secure Edge access for the Enterprise and switch the authentication mode from Password-based to Key-based. See [Enable Secure Edge Access for an Enterprise](#).

Read the following topics next:

- [Enable Secure Edge Access for an Enterprise](#)
- [Secure Edge CLI Commands](#)

## Enable Secure Edge Access for an Enterprise

After adding the SSH key, you must switch the authentication mode from Password-based, which is the default mode to Key-based to access Edges using the SSH username and SSH key. The SSH username is automatically created when you create a new user.

To enable secure Edge access:

**Procedure**

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Service Settings > Edge Management**.
- 2 Select the **Enable Secure Edge Access** check box to allow the user to access Edges using Key-based authentication. Once you have activated Secure Edge Access, you cannot deactivate it.

**Note** Only Operator users can enable secure Edge access for an Enterprise.

- 3 Click **Switch to Key-Based Authentication** and confirm your selection.

**Note** Ensure that you have Super User role to switch the authentication mode.

---

## What to do next

Use the SSH keys to securely login to the Edge's CLI and run the required commands. See [Secure Edge CLI Commands](#).

# Secure Edge CLI Commands

Based on the Access Level configured, you can run the following CLI commands:

**Note** Run the `help <command name>` to view a brief description of the command.

Commands	Description	Access Level = Basic	Access Level = Privileged
<b>Interaction Commands</b>			
help	Displays a list of available commands.	Yes	Yes
pagination	Paginates the output.	Yes	Yes
clear	Clears the screen.	Yes	Yes
EOF	Exits the secure Edge CLI.	Yes	Yes
<b>Debug Commands</b>			
edgeinfo	Displays the Edge's hardware and firmware information. For a sample output of the command, see <a href="#">edgeinfo</a> .	Yes	Yes
seainfo	Displays details about the secure Edge access of the user. For a sample output of the command, see <a href="#">seainfo</a> .	Yes	Yes
ping, ping6	Pings a URL or an IP address.	Yes	Yes
tcpdump	Displays TCP/IP and other packets being transmitted or received over a network to which the Edge is attached. For a sample output of the command, see <a href="#">tcpdump</a> .	Yes	Yes
pcap	Captures the packet data pulled from the network traffic and prints the data to a file. For a sample output of the command, see <a href="#">pcap</a> .	Yes	Yes

<b>Commands</b>	<b>Description</b>	<b>Access Level = Basic</b>	<b>Access Level = Privileged</b>
debug	Runs the debug commands for Edges. Run <code>debug -h</code> to view a list of available commands and options. For a sample output of one of the debug commands, see <a href="#">debug</a> .	Yes	Yes
diag	Runs the remote diagnostics commands. Run <code>diag -h</code> to view a list of available commands and options. For a sample output of one of the diag commands, see <a href="#">diag</a> .	Yes	Yes
ifstatus	Fetches the status of all interfaces. For a sample output of the command, see <a href="#">ifstatus</a> .	Yes	Yes
getwanconfig	Fetches the configuration details of all WAN interfaces. Use the logical names such as "GE3" or "GE4" as arguments to fetch the configuration details of that interface. Do not use the physical names such as "ge3" or "ge4" of the WAN interfaces. For example, run <code>getwanconfig GE3</code> to view the configuration details of the GE3 WAN interface. Run the <code>ifstatus</code> command to know the interface name mappings. For a sample output of the command, see <a href="#">getwanconfig</a> .	Yes	Yes
<b>Configuration Command</b>			
setwancfg	Configures WAN interfaces (wired interfaces only). Run <code>setwancfg -h</code> to view configuration options.	Yes	Yes
<b>Edge Actions Commands</b>			
deactivate	Deactivates the Edges and reapplies the initial default configuration.	No	Yes

<b>Commands</b>	<b>Description</b>	<b>Access Level = Basic</b>	<b>Access Level = Privileged</b>
restart	Restarts the SD-WAN service.	No	Yes
reboot	Reboots the Edge.	No	Yes
shutdown	Powers off the Edge.	No	Yes
hardreset	Deactivates the Edges, restores the Edge's default configuration, and restores original software version.	No	Yes
edged	Activates or deactivates the Edge processes.	No	Yes
restartdhcpserver	Restarts the DHCP server.	No	Yes
<b>Linux Shell Command</b>			
shell	Takes you into the Linux shell. Type <code>exit</code> to return to the secure Edge CLI.	No	Yes

## Sample Outputs

This section provides the sample outputs of some of the commands that can be run in a secure Edge CLI.

### edgeinfo

```
o10test_velocloud_net:velocli> edgeinfo
Model:      vmware
Serial:     VMware-420efa0d2a6ccb35-9b9bee2f04f74b32
Build Version: 5.0.0
Build Date: 2021-12-07_20-17-40
Build rev:  R500-20211207-MN-8f5954619c
Build Hash:  8f5954619c643360455d8ada8e49def34faa688d
```

### seainfo

```
o10test_velocloud_net:velocli> seainfo
{
  "rootlocked": false,
  "seauserinfo": {
    "o2super_velocloud_net": {
      "expiry": 1641600000000,
      "privilege": "BASIC"
    }
  }
}
```

## tcpdump

```
o10test_velocloud_net:veloccli> tcpdump -nnpi eth0 -c 10
reading from file -, link-type EN10MB (Ethernet)
09:45:12.297381 IP6 fd00:1:1:2::2.2426 > fd00:ff01:0:1::2.2426: UDP, length 21
09:45:12.300520 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 21
09:45:12.399077 IP6 fd00:1:1:2::2.2426 > fd00:ff01:0:1::2.2426: UDP, length 21
09:45:12.401382 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 21
09:45:12.442927 IP6 fd00:1:1:2::2.2426 > fd00:ff01:0:1::2.2426: UDP, length 83
09:45:12.444745 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 83
09:45:12.476765 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 64
09:45:12.515696 IP6 fd00:ff02:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 21
```

## pcap

```
o10test_velocloud_net:veloccli> pcap -nnpi eth4 -c 10
The capture will be saved to file o10test_velocloud_net_2021-12-09_09-57-50.pcap
o10test_velocloud_net:veloccli> tcpdump: listening on eth4, link-type EN10MB (Ethernet),
capture size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

## debug

```
o10test_velocloud_net:veloccli> debug --dpdk_ports_dump
name      port   link  ignore  strip   speed   duplex  autoneg  driver
ge3        0       1      0       1      1000     1        1        igb
ge6        4       0      2       1      0        0        1        ixgbe
ge5        5       0      2       1      0        0        1        ixgbe
ge4        1       0      2       1      0        0        0        igb
sfp2       2       0      2       1      0        0        1        ixgbe
sfp1       3       0      2       1      0        0        1        ixgbe
net_vhost0 6       0      0       1      10000    1        0
net_vhost1 7       0      0       1      10000    1        0
```

## diag

```
o10test_velocloud_net:veloccli> diag ARP_DUMP --count 10
Stale Timeout: 2min | Dead Timeout: 25min | Cleanup Timeout: 240min
GE3
192.168.1.254      7c:12:61:70:2f:d0      ALIVE          1s

LAN-VLAN1
10.10.1.137        b2:84:f7:c1:d3:a5      ALIVE          34s
```

## ifstatus

```
o10test:veloccli> ifstatus
{
  "deviceBoardName": "EDGE620-CPU",
  "deviceInfo": [],
```

```

"edgeActivated": true,
"edgeSerial": "HRPGPK2",
"edgeSoftware": {
    "buildNumber": "R500-20210821-DEV-301514018f\n",
    "version": "5.0.0\n"
},
"edgedDisabled": false,
"interfaceStatus": {
    "GE1": {
        "autonegotiation": true,
        "duplex": "Unknown! (255)",
        "haActiveSerialNumber": "",
        "haEnabled": false,
        "haStandbySerialNumber": "",
        "ifindex": 4,
        "internet": false,
        "ip": "",
        "is_sfp": false,
        "isp": "",
        "linkDetected": false,
        "logical_id": "",
        "mac": "18:5a:58:1e:f9:22",
        "netmask": "",
        "physicalName": "ge1",
        "reachabilityIp": "8.8.8.8",
        "service": false,
        "speed": "Unkn",
        "state": "DEAD",
        "stats": {
            "bpsOfBestPathRx": 0,
            "bpsOfBestPathTx": 0
        },
        "type": "LAN"
    },
    "GE2": {
        "autonegotiation": true,
        "duplex": "Unknown! (255)",
        "haActiveSerialNumber": "",
        "haEnabled": false,
        ...
        ...
    }
}
]
}

```

## getwanconfig

```

o10test_velocloud_net:veloccli> getwanconfig GE3
{
    "details": {
        "autonegotiation": "on",
        "driver": "dpdk",
        "duplex": "",
        "gateway": "169.254.7.9",
        ...
    }
}

```

```
"ip": "169.254.7.10",
"is_sfp": false,
"linkDetected": true,
"mac": "00:50:56:8e:46:de",
"netmask": "255.255.255.248",
"password": "",
"proto": "static",
"speed": "",
"username": "",
"v4Disable": false,
"v6Disable": false,
"v6Gateway": "fd00:1:1:1::1",
"v6Ip": "fd00:1:1:1::2",
"v6Prefixlen": 64,
"v6Proto": "static",
"vlanId": ""
},
"status": "OK"
}
```

# View Edge Information

28

The Edge Overview tab displays Edge-specific information. You can update the information like name, description, contact information, associated Profile, and other details. In addition, you can perform other activities like sending Email to activate the Edge, requesting RMA Reactivation, and so on.

To access the Edge Overview page , perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
- 2 The **Edges** page displays the existing Edges.
- 3 Click the link to an Edge or click the **View** link in the **Device** column of the Edge.
- 4 Click the **Overview** tab to view and modify properties of the selected Edge.

The existing details of the selected Edge are displayed. If required, you can modify the information.

[Edges / b2-edge1](#)

b2-edge1 [Connected](#) [SD-WAN](#)

[Device](#) [Business Policy](#) [Firewall](#) [Overview](#)

### Edge Status

Status	Activated
Activated	Mar 30, 2024, 12:52:29 AM
Software Version	6.1.0.0 (build R6100-20240328-MN-f125915d03)
Local Credentials	***** <a href="#">VIEW</a>

### Properties

Name *	b2-edge1
Description	(empty text area)
Custom Info	(empty text area)
Enable Pre-Notifications	<input checked="" type="checkbox"/> Enable
Enable Alerts	<input checked="" type="checkbox"/> Enable
Authentication Mode	Certificate Acquire
Encrypt Device Secrets	<input type="checkbox"/> Enable
<small>① For Edge versions 5.2.0 and above, before you deactivate this option, you must first deactivate the Edge using remote actions. This action causes restart of this Edge.</small>	
License *	<a href="#">EDIT LICENSE SELECTION</a>
Certificate	<a href="#">VIEW</a>

### Profile

Profile	Quick Start Profile																																																
Services	Interface <input checked="" type="checkbox"/> On High Availability <input type="checkbox"/> Off Security VNF <input type="checkbox"/> Off SNMP <input type="checkbox"/> Off Wireless <input type="checkbox"/> Off																																																
Segments	<table border="1"> <thead> <tr> <th>Segment</th> <th>Netflow</th> <th>Static Routes</th> <th>ICMP Probes</th> <th>ICMP Responders</th> <th>Cloud VPN</th> <th>OSPF</th> <th>BGP</th> <th>Multicast</th> <th>Cloud Security</th> <th>Auth</th> <th>Business Policy</th> </tr> </thead> <tbody> <tr> <td>Global Segment</td> <td>-</td> </tr> <tr> <td>segment1</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>N/A</td> <td>-</td> <td>N/A</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>segment2</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>N/A</td> <td>-</td> <td>N/A</td> <td>-</td> <td>-</td> <td>-</td> </tr> </tbody> </table> <p>3 items</p>	Segment	Netflow	Static Routes	ICMP Probes	ICMP Responders	Cloud VPN	OSPF	BGP	Multicast	Cloud Security	Auth	Business Policy	Global Segment	-	-	-	-	-	-	-	-	-	-	-	segment1	-	-	-	-	-	N/A	-	N/A	-	-	-	segment2	-	-	-	-	-	N/A	-	N/A	-	-	-
Segment	Netflow	Static Routes	ICMP Probes	ICMP Responders	Cloud VPN	OSPF	BGP	Multicast	Cloud Security	Auth	Business Policy																																						
Global Segment	-	-	-	-	-	-	-	-	-	-	-																																						
segment1	-	-	-	-	-	N/A	-	N/A	-	-	-																																						
segment2	-	-	-	-	-	N/A	-	N/A	-	-	-																																						

### Contact & Location

VMware by Broadcom	785
Local Contact Name	Super User
Local Contact Email	super@velocloud.net



**Note** The following details are displayed for an already activated Edge. If the Edge has not been activated yet, the **Properties** section displays an option to send Edge Activation Email. For more information, see [Send Edge Activation Email](#).

The Edge Overview tab allows you to view and modify the following fields:

**Table 28-1. Edge Overview tab**

Option	Description
Edge Status	
Status	<p>Displays the status of the Edge:</p> <ul style="list-style-type: none"> <li>■ <b>Pending:</b> The Edge has not been activated.</li> <li>■ <b>Activated:</b> The Edge has been activated.</li> <li>■ <b>Reactivation Pending:</b> A new or replaced Edge can be activated with the existing configuration. This status does not affect the functionality of the Edge.</li> </ul>
Activated	Displays the date and time of Edge activation.
Software Version	Displays the software version and build number of the Edge.
Local Credentials	<p>Displays the credentials for the local UI. These credentials are used to browse the Edge locally in a web-based session to access one of its active LAN interfaces. The local credentials include a default username, 'admin' and a randomly generated password.</p> <p>Click <b>Modify</b> to update the credentials at the Edge level. The local credential is the username/randomly generated password that is required to browse the Edge locally in a web-based session to one of its active LAN interfaces.</p>
Properties	
Name	Displays the name of the Edge.
Description	Displays the description of the Edge.
Custom Info	Displays the custom information associated with the Edge.
Enable Pre-Notifications	<p>By default, this option is enabled. This allows sending alert notifications for the Edge to the Operators. Operators can receive the alerts through Email, SMS, or SNMP traps. To configure the alerts, see <a href="#">Configure Alerts</a>. You can also view the alerts by clicking <b>Monitor &gt; Alerts</b>.</p>

**Table 28-1. Edge Overview tab (continued)**

Option	Description
Enable Alerts	By default, this option is enabled. This allows sending alert notifications for the Edge to the Customers. Customers can receive the alerts through Email, SMS, or SNMP traps. To configure the alerts, see <a href="#">Configure Alerts</a> . You can also view the alerts by clicking <b>Monitor &gt; Alerts</b> .

**Table 28-1. Edge Overview tab (continued)**

Option	Description
Authentication Mode	<p>Choose the mode of authentication from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Deactivated:</b> Edge uses a pre-shared key mode of authentication.</li> </ul> <p><b>Warning</b> This mode is not recommended for any customer deployments.</p> <hr/> <ul style="list-style-type: none"> <li>■ <b>Certificate Acquire:</b> This mode is selected by default and is recommended for all customer deployments. With <b>Certificate Acquire</b> mode, certificates are issued at the time of Edge activation and renewed automatically. The Orchestrator instructs the Edge to acquire a certificate from the certificate authority of the SASE Orchestrator by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the SASE Orchestrator and for establishment of VCMP tunnels.</li> </ul> <p><b>Note</b> After acquiring the certificate, the option can be updated to <b>Certificate Required</b>, if needed.</p> <hr/> <ul style="list-style-type: none"> <li>■ <b>Certificate Required:</b> This mode is only appropriate for customer enterprises that are "static". A static enterprise is defined as one where no more than a few new Edges are likely to be deployed and no new PKI oriented changes are anticipated.</li> </ul> <p><b>Important</b> <b>Certificate Required</b> has no security advantages over <b>Certificate Acquire</b>. Both modes are equally secure and a customer using <b>Certificate Required</b> should do so only for the reasons outlined in this section.</p> <hr/> <p><b>Certificate Required</b> mode means that no Edge heartbeats are accepted without a valid certificate.</p> <hr/> <p><b>Caution</b> Using this mode can cause Edge failures in cases where a customer is unaware of this strict enforcement.</p>

**Table 28-1. Edge Overview tab (continued)**

Option	Description
	<p>With this mode, the Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges by editing the Orchestrator's System Properties. For more information, contact your Operator.</p>
	<p><b>Note</b> When an Edge certificate is revoked, the Edge is deactivated and needs to go through the activation process. The current QuickSec design checks certificate revocation list (CRL) time validity. The CRL time validity must match the current time of Edges for the CRL to have impact on new established connection. To implement this, ensure the Orchestrator time is updated properly to match with the date and time of the Edges.</p>
Encrypt Device Secrets	<p>Select the <b>Enable</b> check box to allow the Edge to encrypt the sensitive data across all platforms.</p> <p><b>Note</b> For Edge versions 5.2.0 and above, before you deactivate this option, you must first deactivate the Edge using remote actions. This causes restart of the Edge.</p>
License	<p>Choose an Edge License from the available list. The list displays the licenses assigned to the Enterprise, by the Operator.</p>
Certificates	<p>Click <b>View</b> to display the certificate details. A pop-up window appears. You can also access this window from the <b>Configure &gt; Edges</b> screen. For more information, see <a href="#">Certificates</a>.</p>
Profile	
Profile	<p>Displays the Profile assigned to the Edge, along with the <b>Services</b> and <b>Segments</b> configuration details. You can modify the assigned profile by selecting a profile from the drop-down menu.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ When switching to a different Profile, the Edge override configurations are not modified.</li> <li>■ Due to push activation, an Edge staging Profile might be displayed. This is a new Edge which is not configured by a production Profile. In such cases, the Enterprise Admin must manually assign a profile from the drop-down menu.</li> </ul>
Contact & Location	<p>While switching the Profiles, check the compatibility between a Customer-assigned Operator Profile and an Edge-assigned Enterprise Profile. For more details, see <a href="#">Compatibility Matrix</a>.</p>

**Table 28-1. Edge Overview tab (continued)**

Option	Description
Local Contact Name	Displays the local contact's name associated with the Edge.
Local Contact Email	Displays the local contact's email address associated with the Edge.
Local Contact Phone	Displays the local contact's phone number associated with the Edge.
Location	Displays the existing location of the Edge. To update the location details, click <b>Edit Location</b> . A pop-up window appears. Enter the new location details and click <b>Update</b> .
Shipping Address	Select the check box <b>Same as above</b> if your shipping address is same as your Edge location. Otherwise, type the shipping contact name and set a location.
RMA Reactivation You can initiate an RMA reactivation request to: <ul style="list-style-type: none"><li>■ Replace an Edge due to a malfunction</li><li>■ Upgrade an Edge hardware model</li></ul>	<p><b>Note</b> This option is only for activated Edges.</p>
Request Reactivation	Click <b>Send Request</b> to generate a new activation key. The status of the Edge changes to <b>Reactivation Pending</b> mode.
<b>Note</b> The reactivation key is valid for one month only.	
Cancel Request	Click to cancel the RMA reactivation request. When you cancel the request, the status of the Edge changes to <b>Activated</b> mode.
Send Activation Email	Click to send an email with activation instructions to the Site Contact. This option does not activate the Edge, but initiates the activation process. A pop-up window appears with the Email details. You can modify the instructions and send the Email.
RMA Serial Number	Displays the serial number of the Edge to be activated. Optionally, you can enter the serial number of the Edge to be activated. This Edge replaces your current Edge for which you have requested the RMA reactivation.
<b>Note</b> If the Serial Number and the Edge model do not match the Edge to be activated, then the activation fails.	

**Table 28-1. Edge Overview tab (continued)**

Option	Description
RMA Model	<p>Displays the model number of the Edge to be activated. This Edge replaces your current Edge for which you have requested the RMA reactivation.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ In an event when the RMA reactivation request contains the serial number of the replacement device (optional), then this serial number must match to the current Edge, otherwise the activation fails.</li> <li>■ If the Serial Number and the Edge model do not match the Edge to be activated, then the activation fails.</li> <li>■ A warning message is displayed if the selected RMA model is not the same as the current Edge model. The Edge specific configuration settings and Profile overrides are removed on reactivation, but the statistics are still retained. It is advised to take a note of the Edge specific configuration settings, and then re-add those to the newly replaced Edge, once it is re-activated.</li> </ul>
Update	<p>Click to update the RMA Edge Attributes details.</p> <p><b>Note</b> For detailed instruction on how to initiate a RMA Reactivation request to the Site Contact, see <a href="#">Send Edge Activation Email</a>.</p>

## Certificates

Clicking **View** displays a pop-up window as shown below:

## Certificate Detail

The screenshot shows a pop-up window titled "Certificate Detail". At the top, there are four buttons: "DOWNLOAD", "COPY CERTIFICATE", "REVOKE", and "RENEW". Below these buttons is a table with the following data:

	Issued On	Expires On
Download	Apr 18, 2024, 12:03:38 PM	Jul 18, 2024, 12:03:38 PM
Copy Certificate		
Revoke		
<b>Issued To</b>	Common Name (CN): 20be822c-210b-4a84-bd2f-f2f1034b7220 Organization (O): 41d5a7dc-f095-4508-8fec-a02d92eae985 Organization Unit (OU):	
<b>Issued By</b>	Common Name (CN): vco Organization (O): VeloCloud Organization Unit (OU): OPS	
<b>Validity Period</b>	Issued On: Apr 18, 2024, 12:03:38 PM Expires On: Jul 18, 2024, 12:03:38 PM	
<b>Details</b>	Subject Key ID: 8ac5d2e2c5d0c40365add64d25831c2ff518ab8 Authority Key ID: 1b84b08c50ed12bec76ee43c264ff39ae40c81d3	

At the bottom left, there is a "REFRESH" button. On the right side, there is a "CLOSE" button.

You can expand the certificate to view more details. The following options are available on the screen:

Option	Description
Download	Click to download the certificate in a CSV format.
Copy Certificate	Select and click this option to copy the certificate details on a clipboard for later use.
Revoke	Click to revoke the selected certificate. The Edge is deactivated when its certificate is revoked.
Renew	Click to renew the expired certificate. The Edge may experience some disruption when its certificate is renewed.  <b>Note</b> For an HA pair, this action renews both active and standby Edge certificates.
Refresh	Click to reload the screen.
Close	Click to close the pop-up window.

**Note** You can also access the **Download**, **Copy Certificate**, and **Revoke** options by clicking the verticle ellipsis next to the certificate check box.

- After modifying the required settings, click **Save Changes**.

- 6 Click the **Shortcuts** option, available at the top right corner, to perform the following activities:

Option	Description
Monitor	Navigates to the Monitoring tab of the selected Edge. For more information, see <a href="#">Monitor Edges</a> .
View Events	Displays the Events related to the selected Edge.
Remote Diagnostics	Enables to run the Remote Diagnostics tests for the selected Edge. For more information, see <a href="#">Run Remote Diagnostics</a> .
Generate Diagnostic Bundle	Allows to generate Diagnostic Bundle for the selected Edge. For more information, see <a href="#">Diagnostic Bundles for Edges</a> .
Remote Actions	Allows to perform remote actions for the selected Edge. For more information, see <a href="#">Remote Actions</a> .
View Profile	Navigates to the Profile page, that is associated with the selected Edge.
View Gateways	Displays the Gateways connected to the selected Edge.  <b>Note</b> Only Operator users can view the Gateways. Enterprise Admin users cannot view the Gateways when they click this option.

## Identifying a Device Model

To identify a device model, click the down arrow next to the device name. A pop-up window displays, which shows Edge and device model information.

**Note** The 5.1.0 release supports functionality to update Firmware as follows:

- Firmware Platform images for 6X0 Edge device models and 3X00 Edge device models (3400/3800/3810)
- Firmware Modem images for 510-LTE (Edge 510LTE-AE, Edge 510LTE-AP) and 610-LTE (Edge 610LTE-AM, Edge 610LTE-RW)
- Factory images for all physical VMware SD-WAN Edge devices
- If Platform and/or Modem Firmware was updated, it will show in the Edge Info details screen as shown below. To access the **Edge Info** details screen, select an Edge. The screen for the selected Edge is displayed. Then click the down arrow icon next to the Edge's name.

X

**Edge Info**

Activation	<b>Activated</b>
Act. Key	JHPY-YG85-RLP3-FANH
Activated	Fri Oct 29, 20:09:42
Last Contact	Fri Oct 29, 21:26:27
System Up Since	Fri Oct 29, 21:24:31
Service Up Since	Fri Oct 29, 21:25:06
Pre-Notifications	<input checked="" type="checkbox"/>
Authentication	<b>Certificate Deactivated</b>

---

**Device Hardware**

Model	<b>Edge 680</b>
Serial Number	CXQ6PK2

---

**Device Software**

Current Version	<b>5.0.0 [R500-20211028-DEV-90fa5a2909]</b>
Factory Version	<b>5.0.0 [R500-20211028-DEV-90fa5a2909]</b>
Analytics	

---

**Device Firmware**

Platform Version	<b>1.1.0 [R110-20210926-QA-6f5f190f93(BIOS_3.50.0.9-12_CPLD_0x29_PIC_v20J), Upgradable]</b>
Modem Version	

---

**Configuration Profile**

Profile	<b>Quick Start Profile</b>
---------	----------------------------

---

**Actions**

<b><input checked="" type="checkbox"/> Configure</b>	<b><input checked="" type="checkbox"/> Remote Actions</b>
<b><input checked="" type="checkbox"/> Events</b>	<b><input checked="" type="checkbox"/> Remote Diagnostics</b>
<b><input checked="" type="checkbox"/> View Profile</b>	<b><input checked="" type="checkbox"/> Generate Diagnostic Bundle</b>

For the 5.2 release, updating the Factory image and Platform Firmware on HA (High-availability) SD-WAN Edges is supported. If the Factory image and/or Platform Firmware on VMware SD-WAN Edge was updated, it will show in the Edge Info details screen as shown below. To access the Edge Info details screen, click the down arrow icon next to the Edge's name.<sup>795</sup>

**Note** A non-WiFi Edge model will contain a "-n" at the end of the model name. See image below.

## Edge Info

Activation  
Act. Key  
Activated  
Last Contact  
System Up Since  
Service Up Since  
Pre-Notifications  
Authentication

### Reactivation Pending

Mon Aug 09, 16:48:28  
Mon Aug 09, 16:48:28  
Mon Aug 09, 16:48:28



### Certificate Acquire

## Device Hardware

Model	edge620-n
Serial Number	

## Device Software

Current Version <b>MN-5d80c45f9e]</b>	4.5.0 [R450-20210808-
Factory Version	
Analytics	<b>None</b>

You can modify the assigned profile by selecting a profile from the drop-down menu. For additional information, see the notes below.

**Note** Edge overrides are the changes to the inherited profile configurations at the Edge level. Edge additions are configurations that are not included in the profile, but are added to the selected Edge.

**Note** When switching to a different profile, the Edge override configurations are not modified.

**Note** Due to push activation, an Edge staging profile might be displayed. This is a new Edge which is not configured by a production profile. In such cases, the Enterprise admin must manually assign a profile from the drop-down menu.

**Note** For more information, see [Configure a Profile Device](#) and [Chapter 29 Configure Edge Overrides](#).

While switching the profiles, check the compatibility between a customer-assigned Operator Profile and an Edge-assigned Enterprise Profile. See the table in the section below for the compatibility matrix.

## Compatibility Matrix

<b>Customer Operator Profile Type</b>	<b>Current Edge Enterprise Profile</b>	<b>Selected Edge Enterprise Profile</b>	<b>Result</b>
Segment-based	Segment-based	Segment-based	No Change
Network-based	Network-based	Network-based	No Change
Segment-based	Network-based	Segment-based	The Edge configuration is converted to a Segment-based configuration. However, it is not delivered to the Edge until the Edge software image is updated to version 3.0 or later.
Network-based	Network-based	Segment-based	The Edge configuration is converted to a Segment-based configuration. However, it is not delivered to the Edge until the Edge software image is updated to version 3.0 or later.
Segment-based	Network-based	Network-based	The Edge does not receive the image update.
Network-based	Segment-based	Segment-based	The Edge does not receive the image update.

# Configure Edge Overrides

29

Configuration overrides can be made to some settings that were assigned to an Edge. In most cases, an override must first be activated, and then changes can be made.

Override rules can be added to existing Business Policy and Firewall rules. Override rules have precedence over all other rules defined for Business Policy or Firewall. For more information, see [Create Business Policy Rule](#) and [Configure Firewall Rule](#).

---

**Note** Edge overrides enable Edge specific edits to the displayed settings, and discontinue further automatic updates from the configuration Profile. You can simply turn off the override and go back to automatic updates any time.

---

To override configuration settings for a specific Edge:

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.

The screenshot shows the VMware SD-WAN Orchestrator interface. At the top, there's a navigation bar with tabs for 'Monitor', 'Configure' (which is selected), 'Diagnostics', and 'Service Settings'. Below the navigation bar, the main content area is titled 'Edges / b1-edge1'. It shows the device is 'Connected' to a 'GLOBAL SEGMENT'. The left sidebar has a tree view under 'Edge Configuration' with nodes like 'Edges', 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control', and 'Network Services'. The right side of the screen displays various configuration sections for the edge device, each with expand/collapse arrows. These sections include:

- Connectivity**: Includes VLAN, Loopback Interfaces, Management Traffic, ARP Timeouts, Interfaces, Global IPv6, and Analytics. The 'Analytics' setting is currently 'On'.
- VPN Services**: Includes Cloud VPN, Non SD-WAN Destination via Edge, Hub or Cluster Interconnect, and Cloud Security Service. The 'Cloud Security Service' setting is currently 'Off'.
- Routing & NAT**: Includes Multicast, BFD, LAN-Side NAT Rules, ICMP Probes, ICMP Responders, Static Route Settings, DNS, OSPF, and BGP. The 'BGP' setting is currently 'Off'.
- High Availability**: Shows 'HA: None'.
- Telemetry**: Includes Visibility Mode, Syslog, Netflow Settings, and SNMP. The 'Netflow Settings' setting is currently 'Off'.
- Security VNF**: Shows 'Security VNF'.
- Edge Services**: Includes Authentication and NTP. The 'NTP' setting is currently 'Off'.

At the bottom right of the configuration table, there are 'SORT' and 'VIEW' dropdown menus. The 'VIEW' menu is currently set to 'VIEW' (the default). The 'SORT' menu is set to 'Category'.

- 3 The **View** drop-down menu at the left side of the page allows the user to select the view options. The available options are **Expand All** and **Collapse All**. By default, the settings are collapsed.
- 4 The **Sort** drop-down menu at the left side of the page allows the user to select the sort options: **Sort by category** and **Sort by segment aware**. You can view the configuration settings sorted by category or segment aware. By default, the settings are sorted by category. If you choose to sort by segmentation, the settings are grouped as segment aware and segment agnostic.
- 5 For some of the settings, the configuration is inherited from the associated Profile. To edit inherited configuration for the Edge, select the **Override** check box.

- 6 After modifying the required settings, click **Save Changes**.

---

**Note** On the **Device** page, whenever you make configuration changes for the selected Edge, an action bar appears at the bottom of the screen. You can click the notification to view the recent configuration changes and save the changes made to the Edge.

---

- 7 Click the **Shortcuts** option to perform the following activities:

- **Monitor** – Navigates to the Monitoring tab of the selected Edge. See [Monitor Edges](#).
- **View Events** – Displays the Events related to the selected Edge.
- **Remote Diagnostics** – Enables to run the Remote Diagnostics tests for the selected Edge. See [Run Remote Diagnostics](#).
- **Generate Diagnostic Bundle** – Allows to generate Diagnostic Bundle for the selected Edge. See [Diagnostic Bundles for Edges](#).
- **Remote Actions** – Allows to perform the Remote actions for the selected Edge. See [Remote Actions](#).
- **View Profile** – Navigates to the Profile page, that is associated with the selected Edge.
- **View Gateways** – Displays the Gateways connected to the selected Edge.

## Edge Device Configurations—A Roadmap

At the Edge-level, some configurations are Segment Aware, that is the configurations must be enabled for each segment where they are intended to work. Whereas, other configurations are Segment Agnostic across multiple segments.

The following table provides the list of Edge-level configurations:

### Connectivity

Settings	Description
VLAN	Configure the VLANs with both IPv4 and IPv6 addresses for Edges. Click the IPv4 or IPv6 tabs to configure the corresponding IP addresses for the VLANs. For more information, see <a href="#">Configure VLAN for Edges</a> .
Loopback Interfaces	Configure a logical interface that allows you to assign an IP address, which is used to identify an Edge. For more information, see <a href="#">Configure a Loopback Interface for an Edge</a> .
Management Traffic	Configure the management traffic by selecting a source IP for the Edge to transmit the traffic to SASE Orchestrator. For more information, see <a href="#">Configure Management Traffic for Edges</a> .

Settings	Description
ARP Timeouts	By default, the Edge inherits the ARP settings from the associated Profile. Select the <b>Override</b> and <b>Override default ARP Timeouts</b> checkboxes to modify the values. For more information, see <a href="#">Configure Address Resolution Protocol Timeouts for Edges</a> .
Interfaces	<p>Configure the following settings for the Edge Interfaces:</p> <ul style="list-style-type: none"> <li>■ <b>Interface Settings</b> – Configure the settings for a Switch Port (LAN) or a Routed (WAN) Interface of the selected Edge. See <a href="#">Configure Interface Settings for Edges</a>.</li> <li>■ <b>WAN Overlay Settings</b> – Enables to add or modify a User-Defined WAN Overlay and modify or delete an existing auto-detected WAN Overlay. See <a href="#">Configure Edge WAN Overlay Settings</a>.</li> </ul>
Global IPv6	Activate IPv6 configurations globally. See <a href="#">Global IPv6 Settings for Edges</a> .
Wi-Fi Radio	<p>Activate or deactivate Wi-Fi Radio and configure the band of radio frequencies. For more information, see <a href="#">Configure Wi-Fi Radio Overrides</a>.</p> <p><b>Note</b> The <b>Wi-Fi Radio</b> option is available only for the following Edge models: 500, 5X0, Edge 510, Edge 510-LTE, Edge 6X0, and Edge 610-LTE.</p>
Common Criteria Firewall	<p>Common Criteria (CC) is an international certification accepted by many countries. Obtaining the CC certification is an endorsement that our product has been evaluated by competent and independent licensed laboratories for the fulfilment of certain security properties. This certification is recognized by all the signatories of the Common Criteria Recognition Agreement (CCRA). The CC is the driving force for the widest available mutual recognition of secure IT products. Having this certification is an assurance of security to a standard extent and can provide VMware with the much needed business parity or advantage with its competitors. Enterprise users can configure the Common Criteria Firewall settings. By default, this feature is deactivated. See <a href="#">Configure Common Criteria Firewall Settings for Edges</a>.</p>

## VPN Services

Settings	Description
Cloud VPN	<p>Allows Cloud VPN to initiate and respond to VPN connection requests. In the Cloud VPN, you can establish tunnels as follows:</p> <ul style="list-style-type: none"> <li>■ Branch to Hub VPN</li> <li>■ Branch to Branch VPN</li> <li>■ Edge to Non SD-WAN via Gateway</li> </ul> <p>Select the check boxes as required and configure the parameters to establish the tunnels. See <a href="#">Configure Cloud VPN and Tunnel Parameters for Edges</a>.</p>
Non SD-WAN Destination via Edge	<p>Allows to establish tunnel between a branch and Non SD-WAN destination via Edge. See <a href="#">Configure Tunnel Between Branch and Non SD-WAN Destinations via Edge</a>. Click <b>Add</b> to add Non SD-WAN Destinations. Click <b>New NSD via Edge</b> to create new Non SD-WAN Destination via Edge. See <a href="#">Configure Non SD-WAN Destinations via Edge</a>.</p>
Hub or Cluster Interconnect	<p>VMware SD-WAN supports interconnection of multiple Hub Edges or Hub Clusters to increase the range of Spoke Edges that can communicate with each other. This feature allows communication between the Spoke Edges connected to one Hub Edge or Hub Cluster and the Spoke Edges connected to another Hub Edge or Hub Cluster, using multiple overlay and underlay connections. See <a href="#">Hub or Cluster Interconnect</a>.</p>
Cloud Security Service	<p>Allows to establish a secured tunnel from an Edge to cloud security service sites. This enables the secured traffic being redirected to third-party cloud security sites. See <a href="#">Chapter 11 Cloud Security Services</a>.</p>
Zscaler	<p>Allows to establish a secured tunnel from an Edge to Zscaler sites. See <a href="#">Configure Zscaler Settings for Edges</a>.</p>
Gateway Handoff Assignment	<p>Allows to assign Partner Gateways for Profiles or Edges. In order for customers to be able assign Partner Gateways, the Partner Handoff feature must be activated for the customers. See <a href="#">Assign Partner Gateway Handoff</a>.</p>
Controller Assignment	<p>Allows to assign Controllers for Profiles or Edges. In order for customers to be able assign Controllers, the Partner Handoff feature must be activated for the customers. See <a href="#">Assign Controllers</a>.</p>
Secure Access Service	<p>Allows to configure Secure Access Service at Edge level. See <a href="#">Configure Secure Access Service for Edges</a>.</p>

## Routing & NAT

<b>Settings</b>	<b>Description</b>
Multicast	Configure Multicast to send data to only interested set of receivers. See <a href="#">Configure Multicast Settings for Edges</a> .
BFD	By default, the Edge inherits the BFD configuration settings from the associated Profile. If required, you can select the <b>Override</b> checkbox to modify the settings. For more information, see <a href="#">Configure BFD for Edges</a> .
LAN-Side NAT Rules	Allows you to NAT IP addresses in an unadvertised subnet to IP addresses in an advertised subnet. See <a href="#">LAN-side NAT Rules at Edge Level</a> .
ICMP Probes	Configure ICMP probes that check for the network continuity by pinging specified IP address at frequent intervals. See <a href="#">Configure ICMP Probes/Responders</a> .
ICMP Responders	Configure ICMP Responders that respond to ICMP probes from a specified IP address. See <a href="#">Configure ICMP Probes/Responders</a> .
Static Route Settings	Configure Static Route Settings for special cases in which static routes are needed for existing network attached devices, such as printers. See <a href="#">Configure Static Route Settings</a> .
DNS	Use the DNS Settings to configure conditional DNS forwarding through a private DNS service and to specify a public DNS service to be used for querying purpose. See <a href="#">Configure DNS for Edges</a> .
OSPF	The OSPF settings configured in the associated Profile are displayed. You can configure OSPF areas only for a Profile and only for a Global Segment. For Edges, you can configure additional OSPF settings for routed Interfaces. For more information, see <a href="#">Activate OSPF for Profiles</a> .
BGP	Configure BGP settings for Underlay Neighbors and Non SD-WAN Neighbors. See <a href="#">Configure BGP</a> .

## High Availability

Settings	Description
High Availability	<p>Activate High Availability for the selected Edge. Choose one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>None</b> – This is the default option where High Availability is not enabled.</li> <li>■ <b>Active Standby Pair</b> – Select this option to enable HA on the selected Edge. For more information, see <a href="#">Activate High Availability</a>.</li> <li>■ <b>Cluster</b> – If you choose this option, select an existing Edge cluster from the drop-down list to enable High Availability on the Edge cluster. To configure Edge clusters, see <a href="#">Configure Clusters and Hubs</a>.</li> <li>■ <b>VRRP with 3rd party router</b> – Select this option to configure Virtual Router Redundancy Protocol (VRRP) on the selected Edge to enable next-hop redundancy in the SASE Orchestrator network by peering with third-party CE router. To configure VRRP, see <a href="#">Configure VRRP Settings</a>.</li> </ul> <p>For more information, see <a href="#">Configure High Availability Settings for Edges</a>.</p>

## Telemetry

Settings	Description
Visibility Mode	Choose the visibility mode to track the network using either MAC address or IP address. See <a href="#">Configure Visibility Mode for Edges</a> .
Syslog	Configure Syslog collector to receive SASE Orchestrator bound events and firewall logs from the Edges configured in an Enterprise. See <a href="#">Configure Syslog Settings for Edges</a> .
Netflow Settings	As an Enterprise Administrator, at the Edge level, you can override the Netflow settings specified in the Profile. See <a href="#">Configure Netflow Settings for Edges</a> .
SNMP	Enable the required SNMP version for monitoring the network. Ensure that you download and install all the required SNMP MIBs before enabling SNMP. See <a href="#">Configure SNMP Settings for Edges</a> .

## Security VNF

Settings	Description
Security VNF	Configure security VNF to run the functions of a network service in a software-only form. For more information, see <a href="#">Security Virtual Network Functions</a> .

## Edge Services

Settings	Description
Authentication	<p>Allows to select a RADIUS server to be used for authenticating a user. For more information, see <a href="#">Configure Authentication Settings for Edges</a>. Click <b>New RADIUS Service</b> to create a new RADIUS server. For more information, see <a href="#">Configure Authentication Services</a>.</p>
NTP	<p>Allows to synchronize the system clocks of Edges and other network devices. See <a href="#">Configure NTP Settings for Edges</a>.</p>

Read the following topics next:

- [Configure VLAN for Edges](#)
- [Loopback Interfaces Configuration](#)
- [Configure Management Traffic for Edges](#)
- [Configure Address Resolution Protocol Timeouts for Edges](#)
- [Configure Interface Settings for Edges](#)
- [Global IPv6 Settings for Edges](#)
- [Configure Wi-Fi Radio Overrides](#)
- [Configure Automatic SIM Switchover](#)
- [Configure Common Criteria Firewall Settings for Edges](#)
- [Configure Cloud VPN and Tunnel Parameters for Edges](#)
- [Configure Cloud Security Services for Edges](#)
- [Configure Zscaler Settings for Edges](#)
- [Configure Secure Access Service for Edges](#)
- [Configure Multicast Settings for Edges](#)
- [Configure BFD for Edges](#)
- [LAN-side NAT Rules at Edge Level](#)
- [Configure ICMP Probes/Responders](#)
- [Configure Static Route Settings](#)
- [Configure DNS for Edges](#)
- [Activate OSPF for Edges](#)
- [Configure BGP from Edge to Underlay Neighbors for Edges](#)
- [Configure High Availability Settings for Edges](#)
- [Configure Visibility Mode for Edges](#)

- Configure Syslog Settings for Edges
- Configure Netflow Settings for Edges
- Configure SNMP Settings for Edges
- Security Virtual Network Functions
- Configure Authentication Settings for Edges
- Configure NTP Settings for Edges
- Configure TACACS Services for Edges

## Configure VLAN for Edges

At Edge level, you can add a new VLAN or update the existing VLAN settings inherited from the associated Profile. While configuring a new VLAN at the Edge level, SASE Orchestrator allows you to configure additional Edge-specific VLAN settings such as Fixed IP addresses, LAN interfaces, and Service Set Identifier (SSID) of Wi-Fi interfaces.

**Note** You can configure a maximum of 32 VLANs across 16 Segments on an Edge.

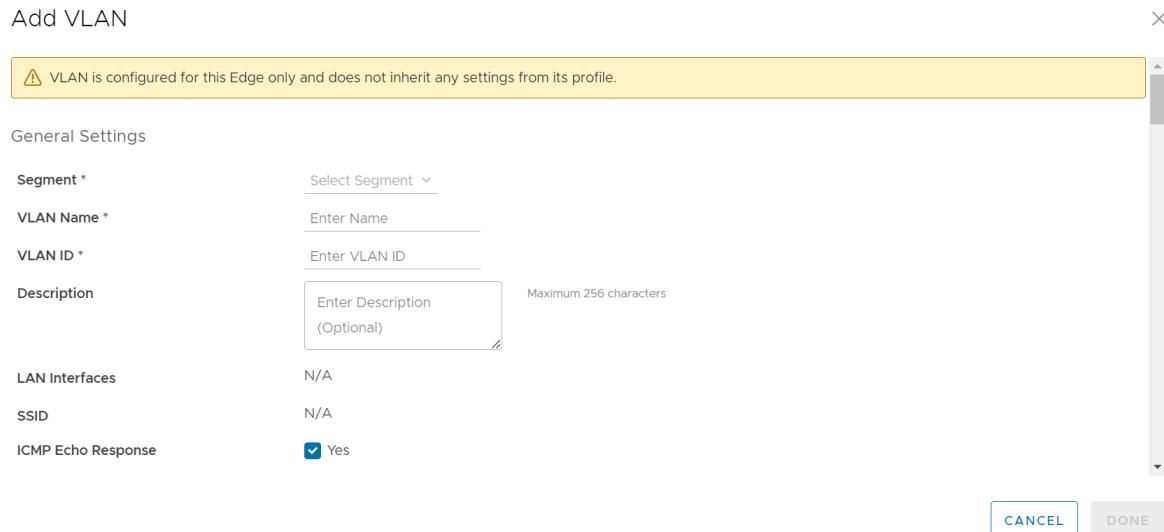
To configure VLAN settings for an Edge:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge.
- 3 In the **Device** tab, under **Connectivity**, expand the **VLAN** section.

	VLAN Override	VLAN	Network	IP Address	Interfaces	DHCP	OSPF
<input type="radio"/>	<span>ⓘ</span> Yes	1 - Corporate	10.0.1.0/24	10.0.1.1	GE1 GE2	<input checked="" type="checkbox"/> Enabled (242)	<input type="checkbox"/> Not Enabled
<input type="radio"/>	<span>ⓘ</span> N/A	100 - VLAN-100	10.100.1.0/24	10.100.1.1	GE2	<input checked="" type="checkbox"/> Enabled (242)	<span>ⓘ</span> Not Enabled
<input type="radio"/>	<span>ⓘ</span> N/A	101 - VLAN-101	10.101.1.0/24	10.101.1.1	GE2	<input checked="" type="checkbox"/> Enabled (242)	<span>ⓘ</span> Not Enabled

You can add or edit VLANs, or add secondary IP addresses. You can also delete the selected VLAN.

- 4 Click **IPv4** or **IPv6** button to display the respective list of VLANs.
- 5 To add a VLAN, click **+ Add VLAN**.



## 6 Configure the Add VLAN settings from the table below.

Option	Description
Segment	Select a segment from the drop-down menu. This assigns the VLAN to the selected segment.
VLAN Name	Enter a unique name for the VLAN.
VLAN Id	Enter the VLAN ID.
Assign Overlapping Subnets	LAN IP Addressing can be managed from the assigned Profile of the Edge. When this check box is selected, the values for <b>Edge LAN IP Address</b> , <b>Cidr Prefix</b> , and <b>DHCP</b> are inherited from the associated Profile and are read-only. The <b>Network</b> address is automatically set based on the subnet mask and CIDR value.  <b>Note</b> Overlapping subnets for the VLAN are supported only for SD-WAN to SD-WAN traffic and SD-WAN to Internet traffic. Overlapping subnets are not supported for SD-WAN to Cloud Web Security traffic.
Edge LAN IP Address	Enter the LAN IP address of the Edge.
Cidr Prefix	Enter the CIDR prefix for the LAN IP address.
Network	Enter the IP address of the Network.
Advertise	Select the check box to advertise the VLAN to other branches in the network.
ICMP Echo Response	Select the check box to enable the VLAN to respond to ICMP echo messages.
VNF Insertion	Select the check box to insert a VNF to the VLAN, which redirects traffic from the VLAN to the VNF. To enable VNF Insertion, ensure that the selected segment is mapped with a service VLAN.

Option	Description
Multicast	<p>This option is enabled only when you have configured multicast settings for the Edge. You can configure the following multicast settings for the VLAN.</p> <ul style="list-style-type: none"> <li>■ IGMP</li> <li>■ PIM</li> </ul> <p>Click <b>toggle advanced multicast settings</b> to set the timers:</p> <ul style="list-style-type: none"> <li>■ PIM Hello Timer</li> <li>■ IGMP Host Query Interval</li> <li>■ IGMP Max Query Response Value</li> </ul>
Fixed IPs	Enter the IP addresses tied to specific MAC Addresses for the VLAN.
LAN Interfaces	Configure VLAN LAN Interfaces.
SSID	Configure VLAN Wi-Fi SSIDs.

Option	Description
DHCP Type	<p>Choose one of the following DHCP settings:</p> <p><b>Enabled</b> – Enables DHCP with the Edge as the DHCP server. Configure the following details:</p> <ul style="list-style-type: none"> <li>■ <b>DHCP Start</b> – Enter a valid IP address available within the subnet.</li> <li>■ <b>Num. Addresses</b> – Enter the number of IP addresses available on a subnet in the DHCP Server.</li> <li>■ <b>Lease Time</b> – Select the period of time from the drop-down list. This is the duration the VLAN is allowed to use an IP address dynamically assigned by the DHCP Server.</li> <li>■ <b>Options</b> – Add pre-defined or custom DHCP options from the drop-down list. The DHCP option is a network service passed to the clients from the DHCP server. For a custom option, enter the code, data type, and value.</li> </ul> <p><b>Relay</b> – Enables DHCP with the DHCP Relay Agent installed at a remote location. If you choose this option, configure the following:</p> <ul style="list-style-type: none"> <li>■ <b>Source from Secondary IP(s)</b> – When you select this check box, the DHCP discover/Request packets from the client will be relayed to the DHCP Relay servers sourced from the primary IP address and all the secondary IP addresses configured for the VLAN. The reply from the DHCP Relay servers will be sent back to the client after rewriting the source and destination. The DHCP server will receive the request from both the primary and secondary IP addresses and the DHCP client can get multiple offers from primary subnet and secondary subnets.</li> </ul> <p>When this option is not selected, the DHCP discover/Request packets from the client will be relayed to the DHCP Relay servers sourced only from the primary IP address.</p> <ul style="list-style-type: none"> <li>■ <b>Relay Agent IP(s)</b> – Specify the IP address of Relay Agent. Click the Plus(+) Icon to add more IP addresses.</li> </ul> <p><b>Not Enabled</b> – Deactivates DHCP.</p>
OSPF	<p>This option is enabled only when you have configured OSPF for the Edge. Select the check box and choose an OSPF from the drop-down list.</p> <hr/> <p><b>Note</b> The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6, which is only available in the 5.2 release..</p> <hr/> <p>For more information on OSPF settings and OSPFv3, see <a href="#">Activate OSPF for Edges</a>.</p>

7 After configuring the required parameters, click the **Add VLAN** button.

## Edit VLANs

To edit the VLAN, complete the steps below.

- 1 To edit the existing VLAN settings inherited from the Profile, click the **Edit** link corresponding to the VLAN.
- 2 Click the **Override** check boxes to override the VLAN settings inherited from the Profile.

The screenshot shows the 'Edit VLAN' dialog box. At the top right is a close button (X) and an 'Override' checkbox with a help icon. The 'General Settings' tab is active, displaying fields for Segment (Global Segment), VLAN Name (Corporate), VLAN ID (1), Description (Enter Description (Optional)), LAN Interfaces (GE1, GE2), SSID (no Wi-Fi SSIDs), ICMP Echo Response (Yes checked), and DNS Proxy (Enabled checked). Below this is the 'IPv4 Settings' tab, which includes fields for Assign Overlapping Subnets (Yes checked), Edge LAN IPv4 Address (10.0.1.1), Cidr Prefix (24), Network (10.0.1.0), OSPF (Enabled checked), Area (1-1), and Passive interface (checked). At the bottom are 'CANCEL' and 'DONE' buttons.

**Note** You cannot override the Profile VLAN name and ID.

- 3 After modifying the required parameters, click **Done VLAN**.

For Configuring VLANs at the Profile level, see [Configure VLAN for Profiles](#).

## Secondary IP Addresses

The VLAN is configured with a primary IP address. You can add secondary IP addresses to the VLAN, to increase the number of host addresses for a network segment. To add secondary IP addresses to the VLAN, click **Add Secondary IP**.

X

## Configure Secondary IP

VLAN 1 - Corporate

Secondary IPs

Addressing Type Static

	IP Address *	Cidr Prefix *	Network	<input checked="" type="checkbox"/> Advertise	<input checked="" type="checkbox"/> ICMP Echo Response
<input type="checkbox"/>	1 Enter IP Address	24		<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled

1 item

**+ ADD** **+ DELETE**

**CANCEL** **DONE**

---

A row to configure a secondary IP displays, as shown in the image above. Configure the Secondary IP VLAN settings from the table below.

Option	Description
Addressing Type	By default, the addressing type is <b>Static</b> and you cannot modify the type.
IP Address	Enter the secondary IP address for the selected VLAN.
Cidr Prefix	Enter the CIDR prefix for the IP address.
Network	Displays the IP address of the Network, which is auto-generated from the secondary IP address and CIDR prefix.
Advertise	Select the check box to advertise the secondary IP address network of the VLAN to other branches in the network.
ICMP Echo Response	Select the check box to enable the VLAN with the secondary IP address to respond to ICMP echo messages.

Click (**+ ADD**) to add more IP addresses to the VLAN.

**Note** You can add up to 16 secondary IP addresses to a VLAN.

Click **Done** when complete. On the **Device** settings screen, click **Save Changes** to save the settings.

# Loopback Interfaces Configuration

A loopback interface is a logical interface that allows you to assign an IP address, which is used to identify a VMware SD-WAN Edge.

You can configure loopback interfaces only for SD-WAN Edges that are running on version 4.3 and above. The **Configure Loopback Interfaces** area is not available for SD-WAN Edges that are running on version 4.2 or lower. For such Edges, you must configure Management IP address. For details, refer to [Configure Management IP Address for Profiles](#).

## Loopback Interfaces—Benefits

Following are the benefits of configuring loopback interfaces for an Edge:

- As loopback interfaces are logical interfaces that are always up and reachable, you can use these interfaces for diagnostic purposes as long as there is layer 3 reachability to at least one physical interface.
- Loopback interfaces can be used as source interface for BGP. This ensures that when the BGP's interface state flaps, the BGP membership does not flap if there is at least one layer 3 connection available.
- Loopback interface IP address can be used as the source IP address for the various services such as Orchestrator Management Traffic, Authentication, DNS, NetFlow, Syslog, TACACS, BGP, and NTP. As loopback interfaces are always up and reachable, these services can receive the reply packets, if at least one physical interface configured for the Edge has layer 3 reachability.

## Loopback Interfaces—Limitations

Keep in mind the following limitations before you configure loopback interfaces for your Edges:

- Only IPv4 addresses can be assigned for loopback interfaces.
- Loopback interfaces can be configured only for Edges. They cannot be configured for Profiles.
- Loopback interfaces must be configured only after the Edge activation is successful.
- For any Edge that is not activated, the version of the customer operator profile is validated based on which either the Management IP Address section or the Loopback Interfaces section is visible. For example, if the version of the customer operator profile is 4.3 or above, the Loopback Interfaces section is visible at the Edge-level. Whereas, if the version of the customer operator profile is 4.2 or lower and the Edge is not activated, the Management IP Address section is visible at the Edge-level and Profile-level.
- Loopback interface IDs must be unique across all segments within an Edge and must start from 1, as Zero (0) is not supported.

- If you choose to configure loopback interfaces and Orchestrator management traffic through API, the default configuration keys for these two properties are not available. You must modify the updateConfigurationModule API to configure the loopback interface and management traffic source interface selection.
- You can access loopback interfaces only through SSH. Loopback interface access through local Web UI is not supported.
- Consider the following when you upgrade or downgrade your Edges:
  - If the Management IP address that is configured either at the Profile-level or at the Edge-level is not the default IP address (192.168.1.1) and when the Edge is upgraded to version 4.3 or above, the loopback interface is automatically created at the Edge-level with the configured Management IP address as the IP address of the loopback interface.
  - Consider that you have upgraded your SASE Orchestrator to version 4.3 or above, whereas the Edge still runs on version 4.2 or lower. If you update the Management IP address configuration either at the Profile-level or at the Edge-level, and then upgrade your Edge to version 4.3 or above, all changes that you made to the Management IP address configuration will be lost.
  - When the Edge is downgraded to a version lower than 4.3, the Management IP address that was configured before the upgrade will be retained at the Profile-level and at the Edge-level.
  - Any changes made to the loopback interface configuration will be lost after the Edge downgrade.
  - For example, consider that you had the Management IP address as 1.1.1.1. When you upgrade your Edge to version 4.3 or above, the same IP address, 1.1.1.1 will be the IP address of the loopback interface at the Edge-level. Then, you change the loopback interface IP address to 2.2.2.2. When you downgrade your Edge to a version lower than 4.3, you will notice that the Management IP address at the Edge-level will still be 1.1.1.1 and the Management IP address at the Profile-level will be empty.

## Configure a Loopback Interface for an Edge

To configure a loopback interface for an Edge:

### Prerequisites

For information about the rules and notes that you must consider before you configure a loopback interface, see [Loopback Interfaces—Limitations](#).

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
- 2 Click the link to an Edge for which you want to configure the loopback interface or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.

**3** Scroll down to the **Connectivity** category and click **Loopback Interfaces**.

The screenshot shows the VMware SD-WAN Administration interface. The top navigation bar includes 'Edges / APISIM-1-1-SCALE' and tabs for 'Connected' and 'SD-WAN'. Below this, a 'Segment' dropdown is set to 'GLOBAL SEGMENT'. The main content area has a 'Device' tab selected, followed by 'Business Policy', 'Firewall', and 'Overview'. A 'Connectivity' section is expanded, showing 'VLAN' and 'Loopback Interfaces'. Under 'Loopback Interfaces', there is a table with the following data:

+ ADD		DELETE		Addressing	Segment	OSPF
<input type="checkbox"/>	Interface	<input type="checkbox"/>	DELETE	1.0.0.1/32	Global Segment	OSPF: <input checked="" type="checkbox"/> Not Enabled OSPFv3: <input checked="" type="checkbox"/> Not Enabled
<input type="checkbox"/>	LO1	<input type="checkbox"/>	DELETE	10.0.0.1/32	Global Segment	OSPF: <input checked="" type="checkbox"/> Not Enabled OSPFv3: <input checked="" type="checkbox"/> Not Enabled
<input type="checkbox"/>	LO2	<input type="checkbox"/>	DELETE			

- 4 Click **+ Add** and in the **Add Loopback** pop-up window, configure the required loopback settings as described in the following table.

### Add Loopback

**Interface ID \***  "LO" already included

**Description**

**Segment**

**ICMP Echo Response**

---

**Enable IPv4 Settings**

**Addressing Type** Static

**IPv4 Address \***

**Advertise**

**OSPF**  OSPF not enabled.

---

**Enable IPv6 Settings**

**Addressing Type** Static

**IPv6 Address**

**Advertise**

**OSPF**  OSPF not enabled.

Field	Description
Interface ID	Enter a unique ID for the loopback interface. The ID must be unique across all segments within an Edge and must start from 1, as Zero (0) is not supported.
Segment	Select a segment from the drop-down list. The loopback interface belongs to the selected segment.
ICMP Echo Response	Select the check box to enable the loopback interface to respond to ICMP echo messages.

Field	Description
<b>IPv4 Settings</b>	
Addressing Type	By default, the addressing type is <b>Static</b> and you cannot modify the type.
IP Address	Enter the IPv4 address for the loopback interface.
CIDR Prefix	The CIDR prefix for the loopback interface IPv4 address. The default value is /32. You cannot modify the default value.
Advertise	Select the check box to advertise the loopback interface to other branches in the network.
OSPF	<p>Select the check box and choose an OSPF Area from the drop-down list. The loopback interface IP address is advertised in the selected OSPF area.</p> <p><b>Note</b> The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6, which is only available in the 5.2 release.</p> <p><b>Note</b> This option is enabled only when you have configured OSPF for the segment that you have selected for the loopback interface. OSPF is not supported on Sub Interfaces, and it is not supported on non Global Segments.</p> <p>For more information on OSPF settings and OSPFv3, see <a href="#">Activate OSPF for Profiles</a>.</p>
<b>IPv6 Settings</b>	
Addressing Type	By default, the addressing type is <b>Static</b> and you cannot modify the type.
IP Address	Enter the IPv6 address for the loopback interface.
CIDR Prefix	The CIDR prefix for the loopback interface IP address. The default value is /128. You cannot modify the default value.

**Note** You can select the **Active** check boxes for the IPv4 and IPv6 settings, to enable the corresponding addressing type for the Interface. By default, the option is enabled for IPv4 settings.

- 5 Click **Add**.
- 6 Click **Save Changes**.

## Results

The loopback interface is listed in the **Loopback Interfaces** area.

At any point in time, you can choose to edit the loopback interface settings by clicking the Address link, except **CIDR Prefix** and **Interface ID**.

If you delete a loopback interface, the **Source Interface** field for all the services for which you have selected the loopback interface, is reset to **Auto**.

In addition, following are two more scenarios based on which the **Source Interface** for the various services is reset to **Auto**:

- If the loopback interface ID is not found in the Edge.

- If you use older versions of APIs to configure the Edge, sometimes the Edge may not receive the key for source IP address for the services.

When the **Source Interface** field for any service is set to **Auto**, the Edge selects the source interface based on the following criteria:

- Any non-WAN interface that is advertised is prioritized.
- Among the non-WAN interfaces that are advertised, the source interface selection is based on the following order of priority—Loopback interfaces, VLAN interfaces, or any routed interfaces.
- If there are more than one interfaces of the same type configured and advertised, the interface with the lowest interface ID is selected.

For example, if you have two loopback interfaces (LO3 and LO4), one VLAN interface (VLAN2), and two routed interfaces (GE1 and GE2) configured and advertised, and if the **Source Interface** field for any service is set to **Auto**, the Edge selects LO3 as the source interface.

#### What to do next

Once you configure the loopback interface for an Edge, you can select the interface as the source interface for the following services:

Services/Settings	For details, refer to ...
Orchestrator Management Traffic	<a href="#">Configure Management Traffic for Edges</a>
Authentication Settings	<a href="#">Configure Authentication Settings for Profiles</a>
DNS Settings	<a href="#">Configure DNS for Profiles</a>
Netflow Settings	<a href="#">Configure Netflow Settings for Edges</a>
Syslog Settings	<a href="#">Configure Syslog Settings for Edges</a>
BGP Settings	<a href="#">Configure BGP from Edge to Underlay Neighbors for Profiles</a>
NTP Settings	<a href="#">Configure NTP Settings for Edges</a>

**Note** When the Edge transmits the traffic, the packet header will have the IP address of the selected source interface, whereas the packets can be sent through any interface based on the destination route.

## Configure Management Traffic for Edges

You can configure the Management Traffic for the Edge to transmit the traffic to VMware SASE Orchestrator.

To configure the Management Traffic at the Edge level:

#### Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.

- 2 Click the link to an Edge for which you want to configure the Orchestrator Management Traffic or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Scroll down to the **Connectivity** category and click and expand the **Management Traffic** area.

The screenshot shows the VMware SD-WAN Enterprise portal interface. At the top, it displays 'Edges / APISIM-1-1-SCALE' with status 'Connected' and 'SD-WAN'. Below this, the 'Segment' dropdown is set to 'GLOBAL SEGMENT'. The navigation bar includes 'Device' (which is selected), 'Business Policy', 'Firewall', and 'Overview'. On the left, a sidebar menu is open under 'Connectivity', showing 'VLAN', 'Loopback Interfaces', and 'Management Traffic' (which is also expanded). Under 'Management Traffic', there is a 'Source Interface' dropdown currently set to 'GE1'. The main content area has 'SORT' and 'VIEW' buttons at the top right.

- 4 From the **Source Interface** drop-down menu, select an Edge interface that is configured for the segment. This interface will be the source IP for the Edge to transmit the traffic to VMware SASE Orchestrator. By default, **Auto** is selected.

#### Results

When the Edge transmits the traffic, the packet header will have the IP address of the selected source interface, whereas the packets can be sent through any interface based on the destination route.

## Configure Address Resolution Protocol Timeouts for Edges

At the Edge level, you can override the Address Resolution Protocol (ARP) Timeout settings inherited from a Profile by selecting the **Override** check box.

To override the ARP timeouts values at the Edge-level, perform the following steps:

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge you want to override L2 settings or click the **View** link in the **Device** column of the Edge.

The **Device** tab displays the configuration options for the selected Edge.

- 3 Under the **Connectivity** category, click **ARP Timeouts** and select the **Override** check box.

- 4 Select the **Override default ARP Timeouts** check box and then override the various ARP timeouts inherited from the Profile as follows:

Field	Description
ARP Stale Timeout	The allowable value ranges from 1 minute to 23 hours and 58 minutes.
ARP Dead Timeout	The allowable value ranges from 2 minutes to 23 hours and 59 minutes.
ARP Cleanup Timeout	The allowable value ranges from 3 minutes to 24 hours.

**Note** The ARP timeout values can only be in increasing order of minutes. For detailed descriptions for Stale, Dead, and Cleanup timeouts, see [Configure Address Resolution Protocol Timeouts for Profiles](#).

**Note** To set the default ARP timeout values at the Edge level, unselect the **Override default ARP Timeouts** checkbox.

- 5 Click **Save Changes**.

## Configure Interface Settings for Edges

An Edge has different types of Interfaces. By default, the Interface configuration settings of an Edge are inherited from the associated Profile. You can modify and configure more settings for each Edge.

The Interface Settings options vary based on the Edge model. For more information on different Edge models and deployments, see [Configure Interface Settings](#).

To configure Interface settings for a specific Edge, perform the following steps:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, expand **Interfaces**.
- 4 The different types of Interfaces available for the selected Edge are displayed. Click the link to an Interface to edit the settings. The Interface settings screen as shown below appears.

X

## Virtual Edge

**⚠** If IPv4/IPv6 DHCP Server is activated and if DNS proxy is deactivated then the DNS resolution will not work as expected and may result in DNS resolution failure.

Interface GE5

 Override

## Description

Enter Description (Optional)

Maximum 256 characters

## Interface Enabled

 Enabled

## Capability

Routed

## Segments

Global Segment

## Radius Authentication

Enabled **⚠** Intra-VLAN traffic will not be filtered on hardware switching platforms (Edge 500, 520, 540, and 610)

## ICMP Echo Response

 EnabledUnderlay Accounting ① Enabled

## Enable WAN Overlay

 Enabled

## DNS Proxy

 Enabled

## VLAN

## EVDSL Modem Attached

 Enabled Enabled

## IPv4 Settings

## Addressing Type

Static

IP Address \* 172.16.1.2

CIDR Prefix \* 29

Gateway 172.16.1.3

## OSPF

**✗** OSPF not enabled for the selected Segment

## Multicast

**✗** Multicast is not enabled for the selected segment

## VNF Insertion

**✗** Trusted Source must be enabled to configure VNF insertion

## Advertise

 Enabled

## NAT Direct Traffic

 Enabled

You can edit the settings for the following types of Interfaces, based on the Edge model:

- Switch Port
- Routed Interface
- WLAN Interface

You can also add Sub Interface, Secondary IP address, and Wi-Fi SSID based on the Edge model.

5 You can configure the following settings for a Routed Interface of an Edge.

Option	Description
Description	Enter a description. This field is optional.
Interface Enabled	This option is activated by default. If required, you can deactivate the Interface. When deactivated, the Interface is not available for any communication.
Capability	For a Switch Port, the option <b>Switched</b> is selected by default. You can choose to convert the port to a routed Interface by selecting the option <b>Routed</b> from the drop-down menu.
Segments	By default, the configuration settings are applicable to all the segments.
Radius Authentication	Deactivate the <b>Enable WAN Overlay</b> check box to configure <b>Radius Authentication</b> . Select the <b>Radius Authentication</b> check box and add the MAC addresses of pre-authenticated devices.
ICMP Echo Response	This check box is selected by default. This helps the Interface to respond to ICMP echo messages. You can deactivate this option for security purposes.
Underlay Accounting	This check box is selected by default. If a private WAN overlay is defined on the Interface, all underlay traffic traversing the interface are counted against the measured rate of the WAN link to prevent over-subscription. Deactivate this option to avoid this behavior.  <b>Note</b> Underlay Accounting is supported for both, IPv4 and IPv6 addresses.
Enable WAN Overlay	Select the check box to activate WAN overlay for the Interface.
DNS Proxy	The <b>DNS Proxy</b> feature provides additional support for Local DNS entries on the Edge, to point certain device traffic to specific domains. You can activate or deactivate this option, irrespective of IPv4 or IPv6 DHCP Server setting.  <b>Note</b> This check box is available only for a Routed Interface and a Routed Sub Interface.

Option	Description
VLAN	For an Access port, select an existing VLAN from the drop-down menu. For a Trunk port, you can select multiple VLANs and select an untagged VLAN.
EVDSL Modem Attached	Select this check box to activate an EVDSL Modem which is connected to one of the ethernet ports on the Edge.
IPv4 Settings	Select the <b>Enable</b> check box and configure the IPv4 settings. For more information, see <a href="#">IPv4 Settings</a> section below.
IPv6 Settings	Select the <b>Enable</b> check box and configure the IPv6 settings. For more information, see <a href="#">IPv6 Settings</a> section below.
L2 Settings	
Autonegotiate	This option is selected by default. When selected, Auto negotiation allows the port to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection.
Speed	This option is available only when <b>Autonegotiate</b> is not selected. Select the speed that the port has to communicate with other links. By default, <b>100 Mbps</b> is selected.  <b>Note</b> Edge 720 and Edge 740 GE ports support an additional speed of 2500 Mbps.
Duplex	This option is available only when <b>Autonegotiate</b> is not selected. Select the mode of the connection as <b>Full duplex</b> or <b>Half duplex</b> . By default, <b>Full duplex</b> is selected.
MTU	The default MTU size for frames received and sent on all routed interfaces is <b>1500</b> bytes. You can change the MTU size for an Interface.
LOS Detection	This option is available only for a routed Interface of an Edge. Select the check box to activate Loss of Signal (LoS) detection by using ARP monitoring. For more information, see <a href="#">HA LoS Detection on Routed Interfaces</a> .  <b>Note</b> You can select the check box only when you have activated High Availability on the Edge.

## IPv4 Settings

Select the **Enabled** check box to configure the following **IPv4 Settings**:

Option	Description
Addressing Type	<p>Select an addressing type:</p> <ul style="list-style-type: none"> <li>■ <b>DHCP</b>: Assigns an IPv4 address dynamically.</li> <li>■ <b>PPPoE</b>: You must configure the authentication details for each Edge. PPPoE requires authentication to get a dynamically assigned IP address.</li> <li>■ <b>Static</b>: You must enter the <b>IP address</b>, <b>CIDR Prefix</b>, and <b>Gateway</b> for the selected routed Interface.</li> </ul> <p><b>Note</b> 31-bit prefixes are supported for IPv4 as per RFC 3021.</p>
OSPF	<p>This option is available only when you have configured OSPF for the selected <b>Segment</b>. Select the check box and choose an OSPF from the drop-down menu. Click <b>toggle advance ospf settings</b> to configure the Interface settings for the selected OSPF.</p> <p><b>Note</b> OSPF is not supported on Sub Interfaces, and it is not supported on non Global Segments.</p> <p>The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6.</p> <p><b>Note</b> OSPFv3 is only available in the 5.2 release.</p> <p>For more information on OSPF settings and OSPFv3, see <a href="#">Activate OSPF for Profiles</a>.</p>

Option	Description
Multicast	<p>This option is available only when you have configured multicast settings for the selected <b>Segment</b>. You can configure the following multicast settings for the selected Interface.</p> <ul style="list-style-type: none"> <li>■ <b>IGMP</b> - Select the check box to activate Internet Group Management Protocol (IGMP). Only IGMP v2 is supported.</li> <li>■ <b>PIM</b> – Select the check box to activate Protocol Independent Multicast. Only PIM Sparse Mode (PIM-SM) is supported.</li> </ul> <p>Click <b>toggle advanced multicast settings</b> to configure the following timers:</p> <ul style="list-style-type: none"> <li>■ <b>PIM Hello Timer</b> – The time interval at which a PIM Interface sends out <b>Hello</b> messages to discover PIM neighbors. The range is from 1 to 180 seconds and the default value is 30 seconds.</li> <li>■ <b>IGMP Host Query Interval</b> – The time interval at which the IGMP querier sends out host-query messages to discover the multicast groups with members, on the attached network. The range is from 1 to 1800 seconds and the default value is 125 seconds.</li> <li>■ <b>IGMP Max Query Response Value</b> – The maximum time that the host has to respond to an IGMP query. The range is from 10 to 250 deciseconds and the default value is 100 deciseconds.</li> </ul> <p><b>Note</b> Currently, Multicast Listener Discovery (MLD) is deactivated. Hence, Edge does not send the multicast listener report when IPv6 address is assigned to Interface. If there is a snooping switch in the network then not sending MLD report may result in Edge not receiving multicast packets which are used in Duplicate Address Detection (DAD). This results in DAD success even with duplicate address.</p>
VNF Insertion	<p>You must deactivate <b>WAN Overlay</b> and select the <b>Trusted Source</b> check box to activate <b>VNF Insertion</b>. When you insert the VNF into Layer 3 interfaces or sub-interfaces, the system redirects traffic from the Layer 3 interfaces or sub interfaces to the VNF.</p>
Advertise	<p>Select the check box to advertise the Interface to other branches in the network.</p>

Option	Description
NAT Direct Traffic	<p>Select the check box to apply NAT for IPv4 to network traffic sent from the Interface.</p> <p><b>Caution</b> It is possible that an older version of the SASE Orchestrator inadvertently configured NAT Direct on a main interface with either a VLAN or subinterface configured. If that interface is sending direct traffic one or hops away, the customer would not observe any issues because the NAT Direct setting was not being applied. However, when an Edge is upgraded to 5.2.0 or later, the Edge build includes a fix for the issue (Ticket #92142) with NAT Direct Traffic not being properly applied, and there is a resulting change in routing behavior since this specific use case was not implemented in prior releases.</p> <p>In other words, because a 5.2.0 or later Edge now implements NAT Direct in the expected manner for all use cases, traffic that previously worked (because NAT Direct was not being applied per the defect) may now fail because the customer never realized that NAT Direct was checked for an interface with a VLAN or subinterface configured.</p> <p>As a result, a customer upgrading their Edge to Release 5.2.0 or later should first check their Profiles and Edge interface settings to ensure NAT Direct is configured only where they explicitly require it and to deactivate this setting where it is not, especially if that interface has a VLAN or subinterface configured.</p>

Option	Description
Trusted Source	Select the check box to set the Interface as a trusted source.
Reverse Path Forwarding	<p>You can choose an option for Reverse Path Forwarding (RPF) only when you have selected the <b>Trusted Source</b> check box. This option allows traffic on the interface only if return traffic can be forwarded on the same interface. This helps to prevent traffic from unknown sources like malicious traffic on an Enterprise network. If the incoming source is unknown, then the packet is dropped at ingress without creating flows. Select one of the following options from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ <b>Not Enabled</b> – Allows incoming traffic even if there is no matching route in the route table.</li> <li>■ <b>Specific</b> – This option is selected by default, even when the <b>Trusted Source</b> option is deactivated. The incoming traffic should match a specific return route on the incoming interface. If a specific match is not found, then the incoming packet is dropped. This is a commonly used mode on interfaces configured with public overlays and NAT.</li> <li>■ <b>Loose</b> – The incoming traffic should match any route (Connected/Static/Routed) in the routing table. This allows asymmetrical routing and is commonly used on interfaces that are configured without next hop.</li> </ul>

For IPv4 address, configure the **IPv4 DHCP Server** as follows:

**Note** This option appears only when you select the **Addressing Type** as **Static**.

- **Activated**: Activates DHCP with the Edge as the DHCP server. If you choose this option, configure the following details:
  - **DHCP Start**: Enter a valid IP address available within the subnet.
  - **Num. Addresses**: Enter the number of IP addresses available on a subnet in the DHCP Server.
  - **Lease Time** : Select the period of time from the drop-down menu. This is the duration the VLAN is allowed to use an IP address dynamically assigned by the DHCP server.
  - **Options**: Click **Add** to add pre-defined or custom DHCP options from the drop-down menu. The DHCP option is a network service passed to the clients from the DHCP server. Choose a custom option and enter the code, data type, and value.
- **Relay** – Allows exchange of DHCPv4 messages between client and server. If you choose this option, configure the following:
  - **Relay Agent IP(s)**: Specify the IP address of Relay Agent. Click **Add** to add more IP addresses.
- **Deactivated** – Deactivates the DHCP server.

## IPv6 Settings

Select the **Enabled** check box to configure the following **IPv6 Settings**:

Option	Description
Addressing Type	<p>Select an addressing type:</p> <ul style="list-style-type: none"> <li>■ <b>DHCP Stateless:</b></li> <li>■ <b>DHCP Stateful:</b></li> <li>■ <b>Static:</b> You must enter the <b>IP address</b>, <b>CIDR Prefix</b>, and <b>Gateway</b> for the selected routed Interface.</li> </ul>
OSPF	<p>This option is available only when you have configured OSPF for the selected <b>Segment</b>. Select the check box and choose an OSPF from the drop-down menu. Click <b>toggle advance ospf settings</b> to configure the Interface settings for the selected OSPF.</p>
	<p><b>Note</b> OSPF is not supported on Sub Interfaces, and it is not supported on non Global Segments.</p>
	<p>The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6, which is only available in the 5.2 release.</p>
	<p><b>Note</b> OSPFv3 is only available in the 5.2 release.</p>
	<p>For more information on OSPF settings and OSPFv3, see <a href="#">Activate OSPF for Profiles</a>.</p>
Advertise	<p>Select the check box to advertise the Interface to other branches in the network.</p>

Option	Description
NAT Direct Traffic	<p>Select the check box to apply NAT for IPv6 to network traffic sent from the Interface.</p> <p><b>Caution</b> It is possible that an older version of the SASE Orchestrator inadvertently configured NAT Direct on a main interface with either a VLAN or subinterface configured. If that interface is sending direct traffic one or hops away, the customer would not observe any issues because the NAT Direct setting was not being applied. However, when an Edge is upgraded to 5.2.0 or later, the Edge build includes a fix for the issue (Ticket #92142) with NAT Direct Traffic not being properly applied, and there is a resulting change in routing behavior since this specific use case was not implemented in prior releases.</p> <p>In other words, because a 5.2.0 or later Edge now implements NAT Direct in the expected manner for all use cases, traffic that previously worked (because NAT Direct was not being applied per the defect) may now fail because the customer never realized that NAT Direct was checked for an interface with a VLAN or subinterface configured.</p> <p>As a result, a customer upgrading their Edge to Release 5.2.0 or later should first check their Profiles and Edge interface settings to ensure NAT Direct is configured only where they explicitly require it and to deactivate this setting where it is not, especially if that interface has a VLAN or subinterface configured.</p>

Option	Description
Trusted Source	Select the check box to set the Interface as a trusted source.
Reverse Path Forwarding	<p>You can choose an option for Reverse Path Forwarding (RPF) only when you have selected the <b>Trusted Source</b> check box. This option allows traffic on the interface only if return traffic can be forwarded on the same interface. This helps to prevent traffic from unknown sources like malicious traffic on an Enterprise network. If the incoming source is unknown, then the packet is dropped at ingress without creating flows. Select one of the following options from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ <b>Not Enabled</b> – Allows incoming traffic even if there is no matching route in the route table.</li> <li>■ <b>Specific</b> – This option is selected by default, even when the <b>Trusted Source</b> option is deactivated. The incoming traffic should match a specific return route on the incoming interface. If a specific match is not found, then the incoming packet is dropped. This is a commonly used mode on interfaces configured with public overlays and NAT.</li> <li>■ <b>Loose</b> – The incoming traffic should match any route (Connected/Static/Routed) in the routing table. This allows asymmetrical routing and is commonly used on interfaces that are configured without next hop.</li> </ul>

For IPv6 address, configure the **IPv6 DHCP Server** as follows:

**Note** This option appears only when you select the **Addressing Type as Static**.

- **Activated**: Activates DHCPv6 with the Edge as the DHCPv6 server. If you choose this option, configure the following details:
  - **DHCP Start**: Enter a valid IPv6 address available within the subnet.
  - **Num. Addresses**: Enter the number of IP addresses available on a subnet in the DHCPv6 Server.
  - **Lease Time** : Select the period of time from the drop-down list. This is the duration the VLAN is allowed to use an IPv6 address dynamically assigned by the DHCPv6 Server.
  - **DHCPv6 Prefix Delegation**: Click **Add** to assign prefixes chosen from a global pool to DHCP clients. Enter the prefix pool name along with the prefix start and end details.
  - **Options** – Click **Add** to add pre-defined or custom DHCP options from the drop-down menu. The DHCP option is a network service passed to the clients from the DHCP server. Choose a custom option and enter the code, data type, and value.

- **Relay** – Allows exchange of DHCPv6 messages between client and server. If you choose this option, configure the following:

- **Relay Agent IP(s)**: Specify the IP address of Relay Agent. Click **Add** to add more IP addresses.

Starting from the 5.2.0 release, VMware SD-WAN Edge supports the **DHCPv6 Relay** feature. This allows the DHCPv6 clients to communicate with a remote DHCPv6 server. It is mostly similar to the **DHCPv4 Relay** feature, except that DHCPv6 uses separate message types to allow the Relay agents to insert their own options or to identify the outgoing interface for the reply packet. To activate this feature on an Edge, you must activate IPv6 on the LAN interface of that Edge.

---

#### Note

- You must provide the Server IP address as the **Relay Agent IP** address on the customer-facing Interface.
- If this Interface belongs to a non-global segment, the Server must be reached through the same non-global segment.

- **Deactivated**: Deactivates the DHCP server.

**Router Advertisement Host Settings**: The Router Advertisement (RA) parameters are available only when you activate **IPv6 Settings**, and then choose the **Addressing Type** as **DHCP Stateless** or **DHCP Stateful**.

**Virtual Edge**

---

<b>IPv6 Settings</b>		<input checked="" type="checkbox"/> Enabled
<b>Addressing Type</b>	DHCP Stateless	
	IP Address	N/A
	Cidr Prefix	N/A
	Gateway:	N/A
<b>WAN Overlay</b>	Auto-Detect	
<b>Advertise</b>	<input type="checkbox"/> Enabled	
<b>NAT Direct Traffic</b>	<input checked="" type="checkbox"/> Enabled	
<b>Trusted Source</b> ⓘ	<input type="checkbox"/> Enabled	
<b>Reverse Path Forwarding</b>	Specific	
	Reverse Path Forwarding options are only settable when trusted zone is checked. When trusted zone is un-checked, the value will default to Specific.	
<b>Router Advertisement Host Settings</b>		
<b>MTU</b> ⓘ	<input checked="" type="checkbox"/> Enabled	
<b>Default Routes</b> ⓘ	<input checked="" type="checkbox"/> Enabled	
<b>Specific Routes</b> ⓘ	<input checked="" type="checkbox"/> Enabled	
<b>ND6 Timers</b> ⓘ	<input checked="" type="checkbox"/> Enabled	

The following RA parameters are selected by default. If required, you can turn them off.

Option	Description
MTU	Accepts the MTU value received through Route Advertisement. If you turn off this option, the MTU configuration of the Interface is considered.
Default Routes	Installs default routes when Route Advertisement is received on the Interface. If you turn off this option, then there are no default routes available for the Interface.
Specific Routes	Installs specific routes when Route Advertisement receives route information on the Interface. If you turn off this option, the Interface does not install the route information.
ND6 Timers	Accepts ND6 timers received through Route Advertisement. If you turn off this option, default ND6 timers are considered. The default value for NDP retransmit timer is 1 second and NDP reachable timeout is 30 seconds.

**Note** When RA host parameters are deactivated and activated again, then Edge waits for the next RA to be received before installing routes, MTU, and ND/NS parameters.

## Wi-Fi Access Control based on MAC Address

Wi-Fi Access Control can be used as an additional layer of security for wireless networks. When activated, only known and approved MAC addresses are permitted to associate with the base station.

## Edge 500

### WLAN1

 Override

Interface Enabled	<input checked="" type="checkbox"/> Enabled												
VLAN	1 - Corporate												
SSID	vc-wifi												
	<input checked="" type="checkbox"/> Broadcast												
Security	WPA2/Personal												
Password	.....												
Static MAC Allow List	<input checked="" type="checkbox"/> Enabled												
<div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span>+ ADD</span> <span> DELETE</span> </div> <table border="1" style="width: 100%; border-collapse: collapse; text-align: left;"> <thead> <tr> <th style="width: 10px;"></th> <th style="width: 40px;">MAC Address</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>00:16:3e:00: ...</td> <td>Enter De...</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Enter MAC A...</td> <td>Enter De...</td> </tr> <tr> <td colspan="3" style="text-align: right;">2 items</td> </tr> </tbody> </table> </div>			MAC Address	Description	<input type="checkbox"/>	00:16:3e:00: ...	Enter De...	<input type="checkbox"/>	Enter MAC A...	Enter De...	2 items		
	MAC Address	Description											
<input type="checkbox"/>	00:16:3e:00: ...	Enter De...											
<input type="checkbox"/>	Enter MAC A...	Enter De...											
2 items													
MAC filtering for AP probes	<input checked="" type="checkbox"/> Enabled												

CANCEL
**SAVE**

- In the SD-WAN Service of the Enterprise portal, click **Configure > Edges** and choose an existing WLAN interface to configure the following parameters.

Option	Description
Interface Enabled	Select the check box to activate the interface.
VLAN	Choose the <b>VLAN</b> ID from the drop-down menu.

Option	Description
SSID	Enter the SSID.
Security	Select either <b>WPA2/Enterprise</b> or <b>WPA2/Personal</b> as the Security option.
Static MAC Allow List	Select the check box to permit only the listed MACs to associate with the access point.  When <b>Static MAC Allow List</b> is configured, only the Mac addresses specified in the list are permitted to associate with the access point.
Radius ACL Check	Select the check box to associate the MAC address with a RADIUS server. If an access-accept is received, the MAC is allowed to associate with the access point.  <b>Note</b> RADIUS ACL checks are limited to <b>WPA2/Enterprise</b> security mode.
Add	Click to enter a new MAC address.
Delete	Click to remove an existing MAC address.
MAC filtering for AP Probes	Enabling MAC Filtering for AP probes prevents probes from unapproved MAC Addresses from actively discovering AP parameters. When the SSID is not broadcast, this can assist in preventing unknown stations from connecting to the network. Some devices are known to use random MAC addresses for probing regardless of AP settings and probe filtering may cause these devices to fail to discover or connect to the network even if their device MAC has been approved.

**Note**

- Both, **MAC filtering for AP Probes** and **RADIUS ACL Check** cannot happen at the same time.
- VMware SD-WAN Edge does not support **Link Layer Discovery Protocol** (LLDP).

## Configure DHCP Server on Routed Interfaces

You can configure DHCP server on a Routed Interface in an SD-WAN Edge.

To configure DHCP Server settings:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, click and expand **Interfaces**.
- 4 The **Interfaces** section displays the different types of Interfaces available for the selected Edge.
- 5 Click the link to the Routed interface that you want to configure DHCP settings.

## Edge 5X0

X

## Interface GE2

 Override

## Description

Enter Description (Optional)

Maximum 256 characters

## Interface Enabled

 Enabled

## Capability

Routed

▼

## Segments

All Segments

## Radius Authentication

✖ WAN Link must be disabled to configure RADIUS Authentication.

## ICMP Echo Response

 Enabled

## Underlay Accounting ⓘ

 Enabled

## Enable WAN Link

 Enabled

## DNS Proxy

 Enabled

## VLAN

## IP Preference ⓘ

 IPv4 IPv6

## FVDSL Modem Attached

 Enabled

## Edge 5X0

X

## IPv6 Settings

 Enabled

## Addressing Type

Static

▼

## IP Address \*

## CIDR Prefix \*

## Gateway

## WAN Link

Auto-Detect

▼

## OSPF

✖ OSPF not enabled for the selected Segment

## Advertise

 Enabled

- 6 To configure DHCP Server (IPv4/IPv6), click the **Enabled** check box in the respective **IPv4 Settings** or **IPv6 Settings** sections, and select the **Addressing Type** as **Static** and enter the IP addresses and CIDR prefix for the Edge Interface and the Gateway.
- 7 In the **DHCP Server** section for IPv4/IPv6, choose one of the following DHCP settings:
  - **Activated** – Allows DHCP with the Edge as the DHCP server. Configure the following details:
    - **DHCP Start**: Enter a valid IP address available within the subnet.
    - **Num. Addresses**: Enter the number of IP addresses available on a subnet in the DHCP Server.
    - **Lease Time** : Select the period of time from the drop-down menu. This is the duration the VLAN is allowed to use an IP address dynamically assigned by the DHCP Server.
    - **DHCPv6 Prefix Delegation**: Click **Add** to add DHCPv6 prefixes by entering the Prefix pool name, IPv6 prefix address, prefix start, and end values.
    - **Options**: Click **Add** to add pre-defined or custom DHCP options from the drop-down menu. The DHCP option is a network service passed to the clients from the DHCP server. Choose a custom option and enter the code, data type, and value. The table below lists the DHCP options for IPv4 and IPv6:

**Table 29-1. DHCP Options for IPv4**

Option	Code	Description
Time Offset	2	Specifies the offset of the client's subnet in seconds, from Coordinated Universal Time (UTC).
DNS Server	6	<p>Lists Domain Name System (RFC 1035) servers available to the client. Servers are listed in order of preference.</p> <p><b>Note</b> This value must be entered as a single entry. In case where both primary and secondary servers are needed, enter the values separated by a comma (Example: 8.8.8.8,8.8.4.4). If two separate values are entered without a comma, the client is configured with only one value.</p>
Domain Name	15	Specifies the domain name that the client must use when resolving host names using the Domain Name System.

**Table 29-1. DHCP Options for IPv4 (continued)**

<b>Option</b>	<b>Code</b>	<b>Description</b>
NTP Servers	42	Lists the NTP servers in order of preference, used for time synchronization of the client.
TFTP Server	66	Configures the address or name of the TFTP server available to the client.
Boot File Name	67	Specifies a boot image to be used by the client.
Domain Search	119	Specifies the DNS domain search list that is used to perform DNS requests, based on short name using the suffixes provided in this list.
Custom	-	Clients may need specific custom options.

**Table 29-2. DHCP Options for IPv6**

<b>DHCP Option Name</b>	<b>Code</b>	<b>Description</b>
SIP Server Names	21	Lists the domain names of the SIP outbound proxy servers that the client can use.
SIP Server Addresses	22	Lists the IPv6 addresses of the SIP outbound proxy servers that the client can use.
DNS Recursive Name Servers	23	Lists IPv6 addresses of DNS recursive name servers to which DNS queries may be sent by the client resolver in order of preference.
Domain Search List	24	Provides a domain search list for the client, to be used when resolving hostnames through DNS.
NIS Servers List	27	Provides an ordered list of NIS servers with IPv6 addresses available to the client.
NIS Domain Name	29	Provides the NIS domain name to be used by the client.
SNTP Servers	31	Provides an ordered list of SNTP servers with IPv6 addresses available to the client.

**Table 29-2. DHCP Options for IPv6 (continued)**

DHCP Option Name	Code	Description
Information Refresh Time	32	Specifies the upper bound of the number of seconds from the current time that a client should wait before refreshing information received from the DHCPv6 server, particularly for stateless DHCPv6 scenarios.
Client FQDN	39	Indicates whether the client or the DHCP server should update DNS with the AAAA record corresponding to the assigned IPv6 address and the FQDN provided in this option. The DHCP server always updates the PTR record.
Custom	-	Clients may need specific custom options.

- **Relay** – Allows DHCP with the DHCP Relay Agent installed at a remote location. If you choose this option, configure the following:
  - **Relay Agent IP(s)**: Specify the IP address of Relay Agent. Click **Add** to add more IP addresses.
  - **Deactivated** – Deactivates the DHCP server.

8 Click **Save**.

For more information on other options in the **Interface Settings** window, see [Configure Interface Settings for Edges](#).

---

**Note** See also [Tunnel Overhead and MTU](#) for more information.

---

## Enable RADIUS on a Routed Interface

RADIUS can be enabled on any interface that is configured as a routed interface. The SD-WAN Edge supports both username/password (EAP-MD5) and certificate (EAP-TLS) based 802.1x Authentication methods.

### Requirements

- A RADIUS server must be configured and added to the Edge. See [Configure Authentication Services](#).
- RADIUS may be enabled on any routed interface. This includes the interfaces for any Edge model, except for the LAN 1-8 ports on Edge models 500/520/540.

---

**Note** RADIUS enabled interfaces do not use DPDK.

---

## Enabling RADIUS on a Routed Interface

**Note** These steps can be followed at either the Profile or Edge level. If done at the Profile level every Edge associated with that Profile would be configured for RADIUS authentication on the specified switched interface.

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, click and expand **Interfaces**.
- 4 The **Interfaces** section displays the different types of Interfaces available for the selected Edge.
- 5 Click the link to the routed interface that you want to configure RADIUS authentication.

## Edge 5X0



**Radius Authentication**  Enabled ⚠ Intra-VLAN traffic will not be filtered on hardware switching platforms (Edge 500, 520, 540, and 610)

⚠ Edge "edge5X0" has radius authentication enabled on a routed interface but no authentication server was set on the global segment

Add mac-addresses of devices that are pre-authenticated (allowlist) that should not be forwarded to RADIUS for re-authentication.

[+ ADD](#) [DELETE](#)

<input type="checkbox"/>	Mac Address or OUI	Description
 Mac Address or OUI is not set. Please add new one		
0 items		

**Enable RADIUS based MAB(Mac Authentication Bypass)**  Enabled

**ICMP Echo Response**  Enabled

**Underlay Accounting**  ⓘ  Enabled

**Enable WAN Link**  Enabled

[CANCEL](#) [SAVE](#)

- 6 Deactivate the **Enable WAN Link** check box to configure RADIUS authentication.
- 7 Select the **RADIUS Authentication** check box.
- 8 Click **+Add** and configure the allowed list of devices that are pre-authenticated and should not be forwarded to RADIUS for re-authentication. You can add devices by using individual MAC addresses (e.g. 8c:ae:4c:fd:67:d5) or by using OUI (Organizationally Unique Identifier [e.g. 8c:ae:4c:00:00:00]).

**Note** The interface will use the server that has already been assigned to the Edge. In an Edge, two interfaces cannot use two different RADIUS servers.

For more information on other options in the **Interface Settings** window, see [Configure Interface Settings for Edges](#).

## Configure RADIUS Authentication for a Switched Interface

This section covers configuring user authentication with a RADIUS server using the 802.1x protocol on an Edge's switched interface through the use of a VLAN associated with that switched interface.

Beginning with SD-WAN Release 5.1.0, a user can configure RADIUS authentication to use an Edge's switched interface as they already had been able to do for a routed interface.

The SD-WAN Edge supports both username/password (EAP-MD5) and certificate (EAP-TLS) based 802.1x Authentication methods.

### Prerequisites

- A RADIUS server must be configured and added to the Edge. See [Configure Authentication Services](#).
- RADIUS may be configured on any switched interface.

### Configuring RADIUS Authentication on a Switched Interface

Adding RADIUS authentication on a switched interface is a two part process where first a VLAN is associated with the targeted switched interface, and then the VLAN is configured to use RADIUS authentication.

---

**Note** These steps can be followed at either the Profile or Edge level. If done at the Profile level every Edge associated with that Profile would be configured for RADIUS authentication on the specified switched interface.

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, click and expand **Interfaces**.
- 4 The **Interfaces** section displays the different types of Interfaces available for the selected Edge.
- 5 Click the link to the switched interface (for example GE2 as shown in the following screenshot) that you want to configure RADIUS authentication.

VLAN Override	VLAN	Network	IP Address	Interfaces	DHCP	Segment
<input checked="" type="checkbox"/> Yes	1 - Corporate	10.1.0/24	10.1.1.1	GE1, GE2	Enabled (242)	Global Segment
	Secondary IP	10.2.0/24 10.3.0/24	10.2.1.1 10.3.1.1			
<input checked="" type="checkbox"/> N/A	2 - VLAN-2	10.11.0/24	10.11.1.1	GE7, GE2	Enabled (242)	Global Segment
	Secondary IP	10.12.0/24 10.13.0/24	10.12.1.1 10.13.1.1			
<input checked="" type="checkbox"/> N/A	100 - VLAN-100	10.101.0/24	10.101.1.1	GE2	Enabled (242)	segment1

General					Switch Port Settings	Routed Interface Sett	
Interface	Interface Override	Type	VNF Insertion	Segment	Mode	VLANs	Addressing
GE1	<input checked="" type="checkbox"/> Yes	Switched		Global Segment	Access	1 - Corporate	
GE2	<input checked="" type="checkbox"/> Yes	Switched		Global Segment segment1 segment2 segment1 segment2	Trunk	1 - Corporate 100 - VLAN-100 101 - VLAN-101 200 - VLAN-200 201 - VLAN-201	

- 6 The Interface settings dialog appears. Add the VLAN where RADIUS authentication will be used to the switched interfaces list of VLANs and click **Save**.

### Virtual Edge

Interface GE2  Override

Interface Enabled	<input checked="" type="checkbox"/> Enabled
Capability	Switched
Mode	Trunk Port
VLANs	1 - Corporate <input type="button" value="X"/> 2 - VLAN-2 <input type="button" value="X"/> 100 - VLAN-100 <input type="button" value="X"/> 101 - VLAN-101 <input type="button" value="X"/> 200 - VLAN-200 <input type="button" value="X"/> 201 - VLAN-201 <input type="button" value="X"/>
Untagged VLAN	1 - Corporate
<b>L2 Settings</b>	
Autonegotiate	<input checked="" type="checkbox"/> Enabled
MTU	1500

**CANCEL** **SAVE**

- 7 In the **Device** page, under the **Connectivity** category click the **VLAN** section and click on the VLAN you want to use for RADIUS authentication.
- 8 On the **Edit VLAN** screen, select the **RADIUS Authentication** check box.

Edit VLAN

**⚠️ VLAN is configured for this Edge only and does not inherit any settings from its profile.**

**General Settings**

Segment *	Global Segment
VLAN Name *	VLAN-2
VLAN ID ⓘ	2
Description	Enter Description (Optional) Maximum 256 characters

**LAN Interfaces**  
GE7 GE2

**SSID**  
There are no Wi-Fi SSIDs configured on this VLAN

**ICMP Echo Response**  
 Yes

**DNS Proxy**  
 Enabled

**Radius Authentication**  
 Enabled **⚠️** Intra-VLAN traffic will not be filtered on hardware switching platforms (Edge 500, 520, 540, and 610)

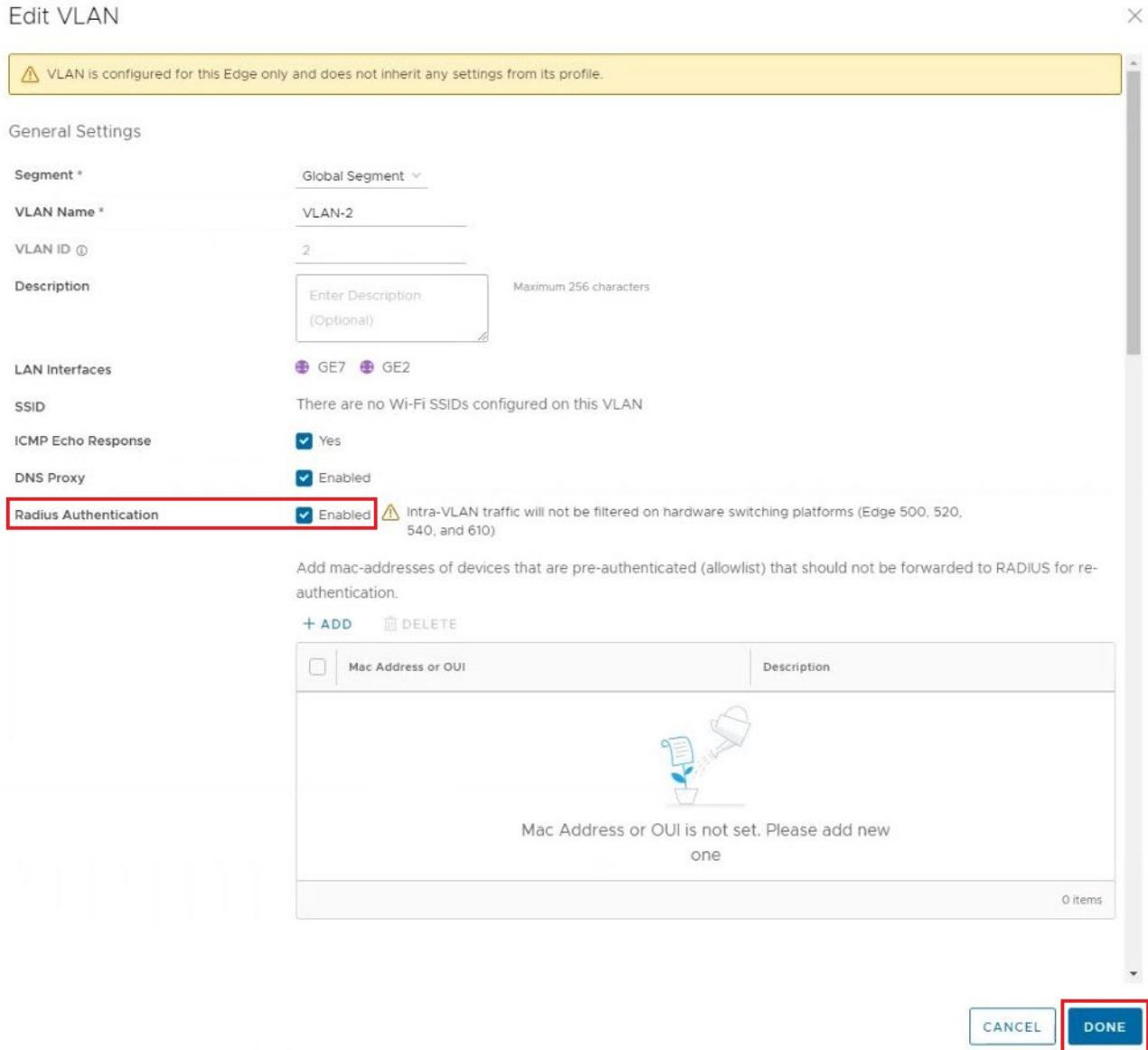
Add mac-addresses of devices that are pre-authenticated (allowlist) that should not be forwarded to RADIUS for re-authentication.

+ ADD    DELETE

<input type="checkbox"/>	Mac Address or OUI	Description
<input type="checkbox"/>		 Mac Address or OUI is not set. Please add new one

0 items

**CANCEL** **DONE**



- 9 Configure the allowed list of devices that are pre-authenticated and should not be forwarded to RADIUS for re-authentication. You can add devices by using individual MAC addresses (e.g. 8c:ae:4c:fd:67:d5) or by using OUI (Organizationally Unique Identifier [e.g. 8c:ae:4c:00:00:00]).
- 10 Select **Done**.
- 11 Finally, click on **Save Changes** in the bottom right corner to apply your configurations.

**Note** The switched interface will use the server that has already been assigned to the Edge. In an Edge, two interfaces cannot use two different RADIUS servers.

## MAC Address Bypass (MAB) for RADIUS-based Authentication

On routed interfaces customers can check MAC addresses against a RADIUS server to bypass 802.1x for LAN devices that do not support 802.1x authentication. MAB simplifies IT operations, saves time, and enhances scalability by no longer requiring customers to manually configure every MAC address that may need authentication.

### Prerequisites

- A RADIUS server must be configured and added to the Edge. See [Configure Authentication Services](#).
- The RADIUS server must have a list of MAC addresses to be bypassed to take advantage of the MAB feature.
- RADIUS authentication must be configured on an Edge's routed interface or switched interface via a VLAN either at the Profile or Edge level.

---

**Note** Beginning with Release 5.2.0, RADIUS-based MAB is also supported for VLANs for use on switched ports. The feature has the following limitation when used with a VLAN for a switched port:

- L2 traffic will not trigger RADIUS MAB.
- L2 traffic will not be forwarded on Linux-based switches until routed traffic is seen. Hardware switches already do not filter pure L2 traffic, and this limitation remains unchanged.
- If no routed traffic is observed and RADIUS MAB times out (default is 30 minutes), L2 traffic will again be blocked.
- Additional hooks to check 802.1x status for self-destined packets may cause performance degradation when 802.1x is enabled.
- Traffic destined to self and managed entirely by Linux will no longer be filtered prior to 802.1x authentication (DHCP, DNS, ssh, and so forth).

---

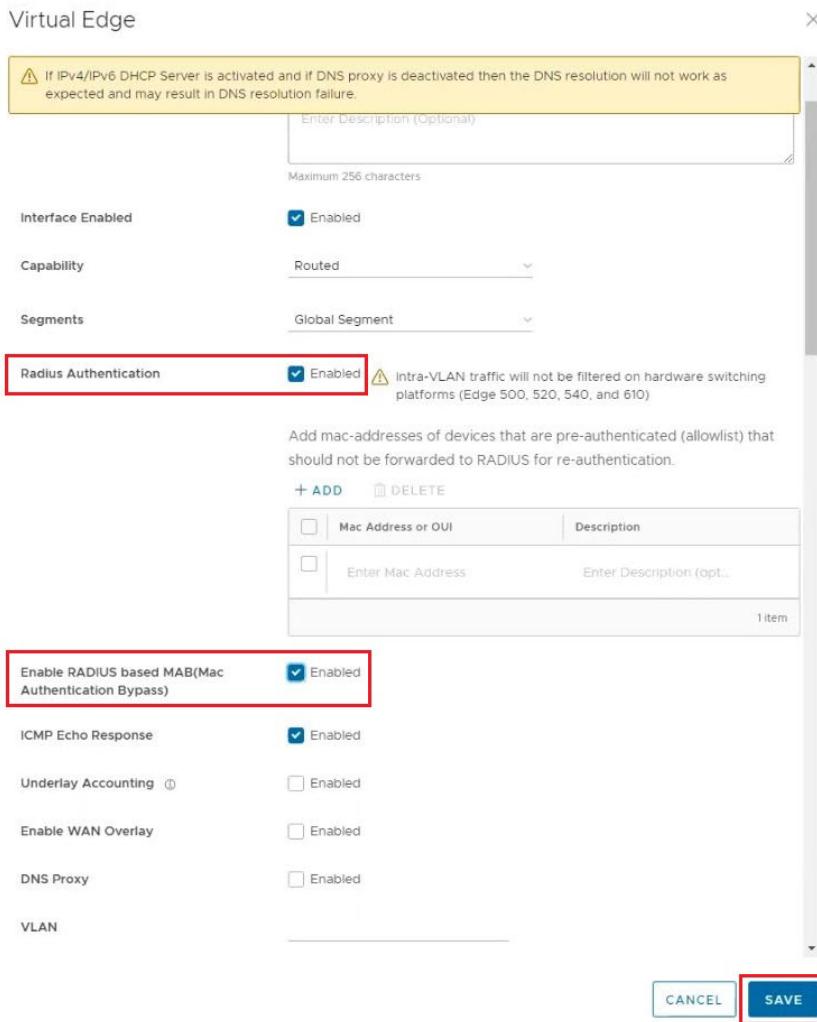
### Activating MAB for Routed Interface

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, click and expand **Interfaces**.
- 4 The **Interfaces** section displays the different types of Interfaces available for the selected Edge.

The screenshot shows the VMware Orchestrator interface for SD-WAN configuration. The top navigation bar includes 'Customer 5-site-ipv6', 'SD-WAN', 'Monitor', 'Configure' (which is highlighted with a red box), 'Diagnostics', and 'Service Settings'. Below this, the 'Edge Configuration' sidebar lists 'Edges' (selected), 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control', and 'Network Services'. The main content area shows a virtual edge named 'b5-edge1' which is 'Connected' to the 'SD-WAN' network. The 'Interfaces' section is expanded, showing a table of interfaces:

Interface	Interface Override	Type	VNF insertion	Segment	Mode
GE1	<input checked="" type="checkbox"/> Yes	Routed	<input checked="" type="checkbox"/> Off	Global Segment	
GE2	<input checked="" type="checkbox"/> Yes	Routed	<input checked="" type="checkbox"/> Off	Global Segment	
GE2: 100 : SIF	<input checked="" type="checkbox"/> Yes	Routed	<input checked="" type="checkbox"/> Off	segment1	
GE2: 101 : SIF	<input checked="" type="checkbox"/> Yes	Routed	<input checked="" type="checkbox"/> Off	segment2	
GE3	<input checked="" type="checkbox"/> Yes	Routed	<input checked="" type="checkbox"/> Off	All Segments	

- Click the **Interface** to edit the Routed interface that is configured for RADIUS authentication.



- 6 On the Interfaces Edit screen confirm that **RADIUS Authentication** is configured and then select the check box for **Enable RADIUS based MAB (MAC Address Authentication Bypass)**.
- 7 Click **Save** and return to the **Device** page.
- 8 Click **Save Changes** in the bottom right corner to apply your configuration.

## Activating MAB for Switched Port using a VLAN

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, click and expand **VLAN**.
- 4 The **VLAN** section displays the VLAN's configured for the selected Edge.

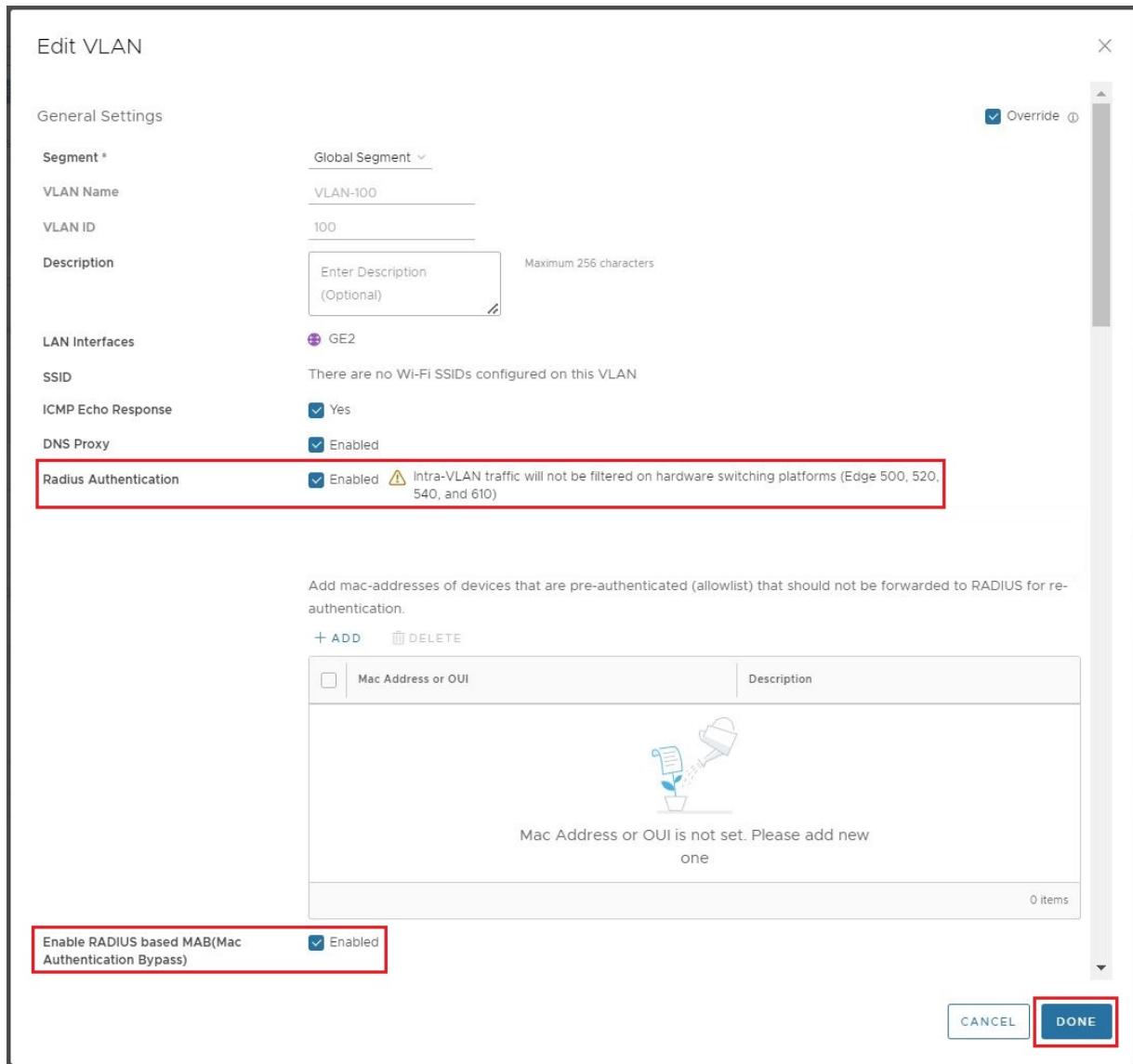
The screenshot shows the VMware Orchestrator interface for a Customer 5-site environment. The top navigation bar includes 'Customer 5-site', 'SD-WAN', and 'Configure'. The left sidebar shows 'Edge Configuration' with 'Edges' selected. The main pane displays 'b4-edge1' with a 'GLOBAL SEGMENT' assigned. Under 'Connectivity', the 'VLAN' section is expanded, showing a table with three rows:

	VLAN Override	VLAN	Network	IP Address	Interfaces	DHCP	Segment	IGMP	PIM	VNF Insertion
<input type="radio"/>	<input checked="" type="checkbox"/> Yes	1 - Corporate	10.0.4.0/24	10.0.4.1	GE1 GE2	Enabled (242)	Global Segment	<input checked="" type="checkbox"/>	No	
<input type="radio"/>	<input checked="" type="checkbox"/> Yes	100 - VLAN-100	10.100.4.0/24	10.100.4.1	GE2	Enabled (242)	Global Segment	<input checked="" type="checkbox"/>	No	
<input type="radio"/>	<input checked="" type="checkbox"/> Yes	101 - VLAN-101	10.101.4.0/24	10.101.4.1	GE2	Enabled (242)	segment2	<input checked="" type="checkbox"/>	No	

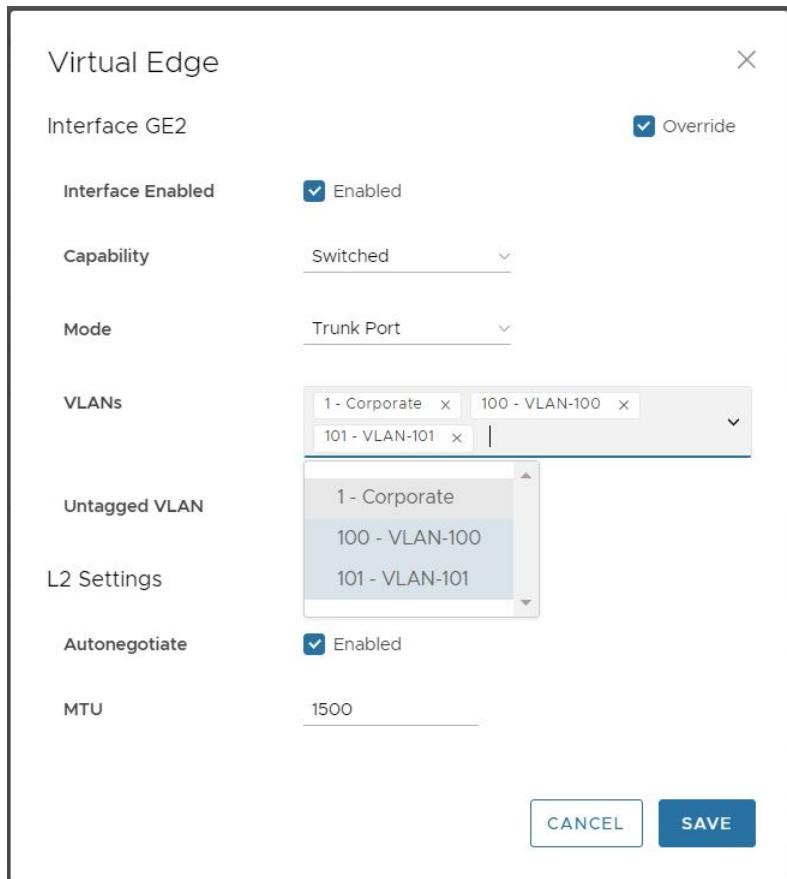
Below the VLAN table, there are sections for 'Loopback Interfaces', 'Management Traffic', 'ARP Timeouts', and 'Interfaces'. The 'Interfaces' section is expanded, showing a table with two rows:

General					Switch Port Settings		Routed Interface Settings			Multicast
Interface	Interface Override	Type	VNF Insertion	Segment	Mode	VLANs	Addressing	WAN Link	OSPF	IGMP PIM
GE1	<input checked="" type="checkbox"/> Yes	Switched		Global Segment	Access	1 - Corporate				N/A
GE2	<input checked="" type="checkbox"/> Yes	Switched		Global Segment Global Segment segment2	Trunk	1 - Corporate 100 - VLAN-100 101 - VLAN-101				N/A

- 5 Click the **VLAN** to edit the VLAN and configure it for RADIUS authentication.



- 6 On the Interfaces Edit screen confirm that **RADIUS Authentication** is configured and then select the check box for **Enable RADIUS based MAB (MAC Address Authentication Bypass)**.
- 7 Click **DONE** and return to the **Device** page.
- 8 Back on the **Connectivity** category, click and expand **Interfaces**.
- 9 The **Interfaces** section displays the different types of interfaces available for the selected Edge.
- 10 Click the **Interface** to edit the Switched interface so that you can assign the VLAN configured for RADIUS.



- 11 Once you have added the VLAN, click **SAVE** and return to the **Device** page.
- 12 Click **Save Changes** in the bottom right corner to apply your configuration.

## Configure Edge LAN Overrides

An Edge has different types of Interfaces. By default, the Interface configuration settings of an Edge are inherited from the associated Profile. At the Edge level, you can override the LAN settings inherited from the Profile.

To override the LAN settings for an Edge:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, expand **Interfaces**.
- 4 The different types of Interfaces available for the selected Edge are displayed. Click the link to a LAN Interface to edit the settings. The LAN Interface settings screen as shown below appears.

Edge 5X0 X

Interface LAN1  Override

Interface Enabled	<input checked="" type="checkbox"/> Enabled
Capability	Switched
Mode	Trunk Port
VLANs	<div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <div style="display: flex; justify-content: space-around; align-items: center;"> <span>1 - Corporate</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>2 - VLAN-2</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>3 - VLAN-3</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>4 - VLAN-4</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>5 - VLAN-5</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>6 - VLAN-6</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>7 - VLAN-7</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>8 - VLAN-8</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>9 - VLAN-9</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>10 - VLAN-10</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>11 - VLAN-11</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>12 - VLAN-12</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>13 - VLAN-13</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>14 - VLAN-14</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>15 - VLAN-15</span> <span>X</span> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 5px;"> <span>16 - VLAN-16</span> <span>X</span> </div> </div>

Untagged VLAN 1 - Corporate

L2 Settings

Autonegotiate	<input checked="" type="checkbox"/> Enabled
MTU	1500

CANCEL SAVE

- 5 To override the LAN settings inherited from the Profile, select the Override check box and modify the LAN settings for the Edge and click **Save**.

For more information about the LAN interface configuration parameters, see [Configure Interface Settings for Profiles](#).

## Configure Edge WLAN Overrides

An Edge has different types of Interfaces. By default, the Interface configuration settings of an Edge are inherited from the associated Profile. At the Edge level, you can override the WLAN settings inherited from the Profile.

To override the WLAN settings for an Edge:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, expand **Interfaces**.
- 4 The different types of Interfaces available for the selected Edge are displayed. Click the link to a WLAN Interface to edit the settings. The WLAN Interface settings screen as shown below appears.

Edge 5X0 X

WLAN1  Override

Interface Enabled	<input checked="" type="checkbox"/> Enabled
VLAN	1 - Corporate
SSID	vc-wifi
<input checked="" type="checkbox"/> Broadcast	
Security	WPA2/Personal
Password	..... <span style="font-size: small;">(eye icon)</span>
Static MAC Allow List	<input type="checkbox"/> Enabled

CANCEL
SAVE

- 5 To override the WLAN settings inherited from the Profile, select the **Override** check box and modify the WLAN settings for the Edge and click **Save**.

For more information about the WLAN interface configuration parameters, see [Configure Interface Settings for Profiles](#).

## Configure Edge WAN Overlay Settings

The WAN Overlay settings enables you to add or modify a User-Defined WAN Overlay.

---

**Note** If you have a CSS GRE tunnel created for an Edge and if you change the WAN Overlay settings of the WAN link associated with the CSS tunnel interface from "Auto-Detect Overlay" to "User-Defined Overlay", the WAN link and the associated CSS tunnels will also be removed from the CSS configuration at the Edge level.

---

A user-defined overlay needs to be attached to an interface that has been configured ahead of time for WAN overlay. You can configure any one of the following Overlays:

- **Private Overlay:** This is required on a private network where you want to have the Edge build overlay VCMP tunnels directly between private IP addresses assigned to each Edge on the private network.

---

**Note** In a Partner Gateway setup with handoff Interface configured, when an Edge with private Interface has both IPv4 and IPv6 user-defined overlays, the Edge tries to establish IP tunnels towards the public IP address of the Gateway based on the tunnel preference.

---

- **Public Overlay:** This is useful when you want to set a custom VLAN or source IP address and Gateway address for the VCMP tunnels, to reach VMware SD-WAN Gateways over the Internet, as determined by the SASE Orchestrator.

You can also modify or delete an existing auto-detected WAN Overlay that has been detected on a routed interface. An auto-detected overlay is available only when the Edge has successfully made a VCMP tunnel over a routed interface configured with WAN Overlay to Gateways designated by the SASE Orchestrator.

---

**Note** The WAN overlays listed under WAN Settings will persist even after an interface is down or not in use and can be deleted when they are no longer required.

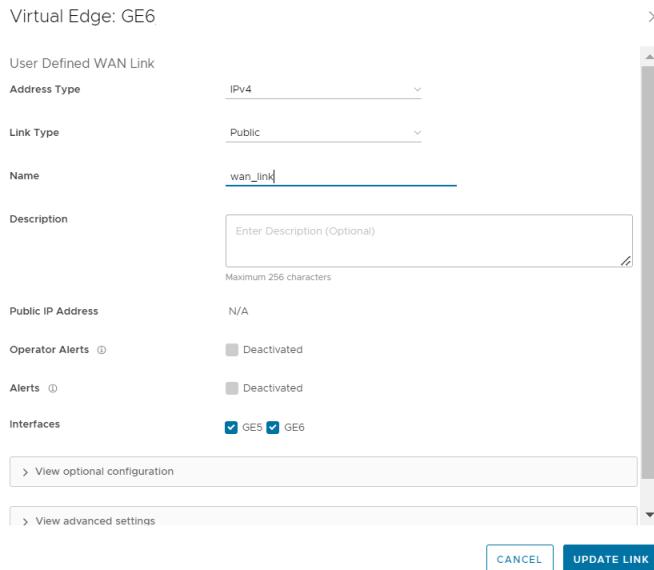
---

To configure WAN Overlay settings for a specific Edge, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, click **Interfaces**.
- 4 The **WAN Link Configuration** section displays the existing Overlays.

The screenshot shows the VMware SD-WAN Orchestrator interface under the 'Configure' tab. On the left, the 'Edge Configuration' sidebar is open, showing 'Edges' selected. The main pane displays the configuration for 'b1-edge1'. Under the 'Connectivity' section, there are several tabs: VLAN, Loopback Interfaces, Management Traffic, ARP Timouts, and Interfaces. The 'Interfaces' tab is selected, listing eight interfaces: GE1, GE2, GE3, GE4, GE5, GE6, GE7, and GE8. Each interface has settings for Type (Switched or Routed), VLANs, and various network protocols like IPv4 and OSPF. The 'WAN Link Configuration' section at the bottom is highlighted with a red border, showing three entries: GE6 (User Defined), 169.254.7.10 (Auto Detect), and 169.254.6.34 (Auto Detect).

- 5 You can click the Name of the Overlay to modify the settings. To create a new Public or Private WAN overlay, click **Add User Defined WAN Link**. The **Virtual Edge: new link** window appears.



- 6 In the **User Defined WAN Overlay** section, choose the **Link Type** from the following available options:

- **Public** overlay is used over the Internet where SD-WAN cloud Gateways, that are on the Internet, are reachable. The user-defined overlay must be attached to an Interface. The public overlay instructs the Edge to assign primary and secondary gateways over the interface it is attached, to help determine the outside global NAT address. This outside global address is reported to the Orchestrator so that all the other Edges use this outside global address, if configured to build VCMP tunnels to the currently selected Edge.

---

**Note** By default, all routed interfaces will attempt to **Auto Detect**, that is build VCMP tunnels to, pre-assigned cloud Gateways over the Internet. If the attempt is successful, an Auto Detect Public overlay is created. A User Defined Public overlay is only needed if your Internet service requires a VLAN tag or you want to use a different public IP address from the one that the Edge has learned through DHCP on the public facing interface.

- **Private** overlay is used on private networks such as an MPLS network or point-to-point link. A private overlay is attached to an interface like any user defined overlay and assumes that the IP address on the interface it is attached is routable for all other Edges on the same private network. This means that there is no NAT on the WAN side of the interface. When you attach a private overlay to an interface, the Edge advises the Orchestrator that the IP address on the interface should be used for any remote Edges configured to build tunnels to it.

The following tables describe the Overlay settings:

**Table 29-3. Settings common for Public and Private Overlay**

Option	Description
Address Type	<p>Choose the WAN overlay link to use either IPv4 or IPv6 address. You can also select IPv4 and IPv6, which enables to configure both IPv4 and IPv6 user-defined overlay towards the same ISP as a single link. This option helps preventing oversubscription of a link towards an ISP.</p> <p><b>Note</b> When you choose IPv6 address, the Duplicate Address Detection (DAD) is not supported for IP steered overlay. The overlay network is steered when you configure the source IP address in the <b>Optional Configuration</b>.</p>
Name	<p>Enter a descriptive WAN overlay name for the public or private link.</p> <p><b>Note</b> WAN overlay name should only consist of ASCII characters. Non-ASCII characters are not supported.</p> <p>You can reference this name while choosing a WAN link in a Business Policy. See <a href="#">Configure Link Steering Modes</a>.</p>
Operator Alerts	<p>Sends alerts related to the Overlay network to the Operator. Ensure that you have enabled the Link alerts in the <b>Configure &gt; Alerts &amp; Notifications</b> page to receive the alerts.</p>
Alerts	<p>Sends alerts related to the Overlay network to the Customer. Ensure that you have enabled the Link alerts in the <b>Configure &gt; Alerts &amp; Notifications</b> page to receive the alerts.</p>
Select Interfaces	<p>The Routed Interfaces enabled with IPv4 WAN Overlay or IPv6 WAN Overlay and set to <b>User Defined Overlay</b> are displayed as check boxes. The Interfaces displayed are based on the selected <b>Address Type</b>.</p> <p><b>Note</b> If the WAN Overlay link uses a static IPv4 address then you can select one or more routed interfaces and the current user-defined overlay is attached to the selected interface. If a static IPv6 address is configured then you cannot select one or more routed interfaces.</p> <p><b>Note</b> For the 610-LTE, you can add User Defined WAN overlay on CELL1 or CELL2. The SASE Orchestrator will display both CELL1 and CELL2, irrespective of SIM presence. Therefore, you must be aware of which SIM slot is enabled (Active) and choose that SIM.</p>

**Table 29-4. Public Overlay Settings**

Option	Description
Public IP Address	Displays the discovered public IP address for a public Overlay. This field is populated once the outside global NAT address is discovered using the Gateway method.

The following image shows an example of Settings for Public Overlay:

**Virtual Edge: new link**

User Defined WAN Link

Address Type	IPv4 and IPv6
Link Type	Public
Name	Enter Provider or ISP Name
Public IP Address	N/A
Operator Alerts ⓘ	<input type="checkbox"/> Deactivated
Alerts ⓘ	<input type="checkbox"/> Deactivated

Interfaces

▼ View optional configuration

IPv4 Source Address ⓘ	Enter IP Address
IPv4 Next-Hop Address ⓘ	Enter IP Address
IPv6 Source Address ⓘ	Enter IP Address
IPv6 Next-Hop Address ⓘ	Enter IP Address
Custom VLAN	<input checked="" type="checkbox"/> Activated
Custom VLAN Id	0
Enable Per Link DSCP ⓘ	<input checked="" type="checkbox"/> Activated
DSCP tag	▼

▼ View advanced settings

Bandwidth Measurement ⓘ	Measure Bandwidth (Slow Start) ▼
Dynamic Bandwidth Adjustment ⓘ	<input type="checkbox"/> Deactivated
Link Mode ⓘ	Active ▾ ▲
MTU	1500
Overhead Bytes	0
Path MTU Discovery	<input checked="" type="checkbox"/> Activated

Public Link Configuration

UDP Hole Punching	<input type="checkbox"/> Deactivated
Type	Wired ▾

Configure Class of Service ⊗To enable Class of Service, Per Link DSCP must be disabled.

**CANCEL** **ADD LINK**

**Table 29-5. Private Overlay Settings**

Option	Description
SD-WAN Service Reachable	<p>When creating a private overlay and attaching it to a private WAN like MPLS network, you may also be able to reach the internet over the same WAN, usually through a firewall in the data center. In this case, it is recommended to enable SD-WAN Service Reachable as it provides the following:</p> <ul style="list-style-type: none"> <li>■ A secondary path to the internet for access to internet hosted SD-WAN Gateways. This is used if all the direct links to the internet from this Edge fail.</li> <li>■ A secondary path to the Orchestrator, when all the direct links to the internet from this Edge fail. The management IP address the Edge uses to communicate must be routable within MPLS, otherwise NAT Direct would need to be checked on the private interface for the Orchestrator traffic to come back properly.</li> </ul> <p><b>Note</b> The SD-WAN Edge always prefers the VCMP tunnel created over a local internet link (short path), compared to the VCMP tunnel created over the private network using a remote firewall to the internet (long path).</p> <p><b>Note</b> Per-packet or round-robin load balancing will not be performed between the short and long paths.</p> <p>In a site with no direct public internet access, the SD-WAN Service Reachable option allows the private WAN to be used for private site-to-site VCMP tunnels and as a path to communicate with an internet hosted VMware SD-WAN service.</p>
Public SD-WAN Addresses	<p>When you select the <b>SD-WAN Service Reachable</b> check box, a list of public IPv4 and IPv6 addresses of SD-WAN Gateways and SASE Orchestrator is displayed, which may need to be advertised across the private network, if a default route has not been already advertised across the same private network from the firewall.</p> <p><b>Note</b> Some IP addresses in the list, such as Gateways, may change over time.</p>

The following image shows an example of Settings for Private Overlay:

## Virtual Edge: GE6

X

## User Defined WAN Link

Address Type	IPv4
Link Type	Private
Name	GE6_Private
Description	<input type="text" value="Enter Description (Optional)"/> <small>Maximum 256 characters</small>
SD-WAN Service Reachable <small> ⓘ</small>	<input type="checkbox"/> Deactivated
Public IP Address	N/A
Operator Alerts <small> ⓘ</small>	<input type="checkbox"/> Deactivated
Alerts <small> ⓘ</small>	<input type="checkbox"/> Deactivated
Interfaces	<input checked="" type="checkbox"/> GE5 <input checked="" type="checkbox"/> GE6

&gt; View optional configuration

[CANCEL](#)[UPDATE LINK](#)

Table 29-6. Optional Configuration

Option	Description
Source IP Address	<p>This is the raw socket source IP address used for VCMP tunnel packets that originate from the interface to which the current overlay is attached.</p> <p>Source IP address does not have to be pre-configured anywhere but must be routable to and from the selected interface.</p> <p>You can enter IPv4 or IPv6 address in the respective fields to establish WAN overlay with the peer.</p>
Next-Hop IP Address	<p>Enter the next hop IP address to which the packets, which come from the raw socket source IP address specified in the <b>Source IP Address</b> field, are to be routed.</p> <p>You can enter IPv4 or IPv6 address in the respective fields.</p>

**Table 29-6. Optional Configuration (continued)**

Option	Description
Custom VLAN	<p>Select this check box to enable custom VLAN and enter the VLAN ID. The range is 2 to 4094.</p> <p>This option applies the VLAN tag to the packets originated from the Source IP Address of a VCMP tunnel from the interface to which the current overlay is attached.</p>
Enable Per Link DSCP	<p>Select this check box to add a DSCP tag to a specific overlay link. The DSCP tag will be applied at the outer header of the VCMP packet going over this overlay link. This will provide the ability to leverage the private network underlay DSCP tag mechanism to treat each overlay uniquely via QoS setting defined at the upstream router. See the use case for this check box in the section below titled, "<a href="#">Use Case: DSCP Value Per User Defined Overlay</a>."</p>
802.1P Setting	<p>Select this check box to set 802.1p PCP bits on frames leaving the interface to which the current overlay is attached. This setting is only available for a specific VLAN. PCP priority values are a 3-digit binary number. The range is from 000 to 111 and default is 000.</p> <p>This check box is available only when the system property <code>session.options.enable8021PConfiguration</code> must be set to True. By default, this value is False.</p> <p>If this option is not available for you, contact the VMware support of your operations team to enable the setting.</p>

- 7 Click **View advanced settings** to configure the following settings:

**Table 29-7. Advanced Settings common for Public and Private Overlay**

Option	Description
Bandwidth Measurement	<p>Choose a method to measure the bandwidth from the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Measure Bandwidth (Slow Start):</b> When measuring the default bandwidth reports incorrect results, it may be due to ISP throttling. To overcome this behavior, choose this option for a sustained slow burst of UDP traffic followed by a larger burst.</li> <li>■ <b>Measure Bandwidth (Burst Mode):</b> Choose this option to perform short bursts of UDP traffic to an SD-WAN Gateway for public links or to the peer for private links, to assess the bandwidth of the link.</li> <li>■ <b>Do Not Measure (define manually):</b> Choose this option to configure the bandwidth manually. This is recommended for the Hub sites because: <ul style="list-style-type: none"> <li>a Hub sites can usually only measure against remote branches which have slower links than the hub.</li> <li>b If a hub Edge fails and is using a dynamic bandwidth measurement mode, it may add delay in the hub Edge coming back online while it re-measures the available bandwidth.</li> </ul> </li> </ul>
Upstream Bandwidth	<p>Enter the upstream bandwidth in Mbps. This option is available only when you choose Do Not Measure (define manually).</p>
Downstream Bandwidth	<p>Enter the downstream bandwidth in Mbps. This option is available only when you choose Do Not Measure (define manually).</p>
Dynamic Bandwidth Adjustment	<p>Dynamic Bandwidth Adjustment attempts to dynamically adjust the available link bandwidth based on packet loss and intended for use with Wireless broadband services where bandwidth can suddenly decrease.</p> <hr/> <p><b>Note</b> This configuration is not recommended for Edges with software release 3.3.x or earlier. You can configure this option for Edges with release 3.4 or later.</p> <hr/> <p><b>Note</b> This configuration is not supported with public link CoS.</p>

**Table 29-7. Advanced Settings common for Public and Private Overlay (continued)**

Option	Description
Link Mode	<p>Select the mode of the WAN link from the drop-down. The following options are available:</p> <ul style="list-style-type: none"> <li>■ <b>Active:</b> This option is selected by default. The interface is used as a primary mode to send traffic.</li> <li>■ <b>Backup:</b> This option puts the interface that this WAN Overlay is attached to into Backup Mode. This means that the management tunnels are torn down for this interface, and the attached WAN link receives no data traffic. The Backup link would only be used if all paths from a number of Active links go down, which also drops the number of Active links below the number of <b>Minimum Active Links</b> configured. When this condition is met, management tunnels would be rebuilt for the interface and the Backup Link would become Active and pass traffic.</li> </ul> <p>Only one interface on an Edge can be put into backup mode. When enabled, the interface will be displayed in <b>Monitor &gt; Edges</b> page as <b>Cloud Status: Standby</b>.</p> <hr/> <p><b>Note</b> Use this option to reduce user data and SD-WAN performance measurement bandwidth consumption on a 4G or LTE service. However, failover times will be slower when compared to a link that is configured as either Hot Standby or as Active and uses a business policy to regulate bandwidth consumption. Do not use this feature if the Edge is configured as a Hub or is part of a Cluster.</p> <ul style="list-style-type: none"> <li>■ <b>Hot Standby:</b> When you configure the WAN link for Hot Standby mode, the management tunnels are built, which enables a rapid switchover in case of a failure. The Hot Standby link receives no data traffic except for heartbeats, which are sent every 5 seconds.</li> </ul> <p>When all paths from a number of Active links go down, which also drops the number of Active links below the number of <b>Minimum Active Links</b> configured, the Hot Standby link would come up. The traffic is sent through the Hot Standby path.</p> <p>When the path to the Primary Gateway comes up on Active links such that the number of Active links exceeds the number of <b>Minimum Active Links</b> configured, the Hot Standby link returns to Standby mode and the traffic flow switches over to the Active link(s).</p> <p>For more information, see <a href="#">Configure Hot Standby Link</a>.</p>

**Table 29-7. Advanced Settings common for Public and Private Overlay (continued)**

Option	Description
	Once you activate the Backup or Hot Standby link option on an Interface, you cannot configure additional Interfaces of that Edge as either a Backup or Hot Standby Link, as an Edge can have only one WAN link as a Backup or Hot Standby at a time.
Minimum Active Links	This option is available only when you choose Backup or Hot Standby as Link Mode. Select the number of active links that can be present in the network at a time, from the drop-down list. When the number of current active links that are UP goes below the selected number, then the Backup or the Hot Standby link comes up. The range is 1 to 3, with the default being 1.
MTU	<p>The SD-WAN Edge performs path MTU discovery and the discovered MTU value is updated in this field. Most wired networks support 1500 Bytes while 4G networks supporting VoLTE typically only allow up to 1358 Bytes. It is not recommended to set the MTU below 1300 Bytes as it may introduce framing overhead. There is no need to set MTU unless path MTU discovery has failed.</p> <p>You can find if the MTU is large from the <b>Remote Diagnostics &gt; List Paths</b> page, as the VCMP tunnels (paths) for the interface never become stable and repeatedly reach an UNUSABLE state with greater than 25% packet loss.</p> <p>As the MTU slowly increases during bandwidth testing on each path, if the configured MTU is greater than the network MTU, all packets greater than the network MTU are dropped, causing severe packet loss on the path.</p> <p>For more information, see <a href="#">Tunnel Overhead and MTU</a>.</p>
Overhead Bytes	<p>Enter a value for the Overhead bandwidth in bytes. This is an option to indicate the additional L2 framing overhead that exists in the WAN path.</p> <p>When you configure the Overhead Bytes, the bytes are additionally accounted for by the QoS scheduler for each packet, in addition to the actual packet length. This ensures that the link bandwidth is not oversubscribed due to any upstream L2-framing overhead.</p>
Path MTU Discovery	<p>Select this check box to enable the discovery of Path MTU. After determining the Overhead bandwidth to be applied, the Edge performs Path MTU Discovery to find the maximum permissible MTU to calculate the effective MTU for customer packets. For more information, see <a href="#">Tunnel Overhead and MTU</a>.</p>

**Table 29-7. Advanced Settings common for Public and Private Overlay (continued)**

Option	Description
Configure Class of Service	<p>SD-WAN Edges can prioritize traffic and provide a 3x3 QoS class matrix over both Internet and Private networks alike. However, some public or private (MPLS) networks include their own quality of service (QoS) classes, each with specific characteristics such as rate guarantees, rate limits, packet loss probability etc.</p> <p>This option allows the Edge to understand the public or private network QoS bandwidth available and policing for the public or private Overlay on a specific interface.</p> <p><b>Note</b> Outer DSCP tags must be set in business policy per application/rule and in this feature, each Class of Service line is matching on those DSCP tags set in the business policy.</p> <p>After you select this check box, configure the following:</p> <ul style="list-style-type: none"> <li>■ <b>Class of Service:</b> Enter a descriptive name for the class of service. You can reference this name while choosing a WAN link in a Business Policy. See <a href="#">Configure Link Steering Modes</a>.</li> <li>■ <b>DSCP Tags:</b> Class of service will match on the DSCP tags defined here. DSCP tags are assigned to each application using business policy.</li> <li>■ <b>Bandwidth:</b> Percentage of interface transmit/upload bandwidth available for this class as determined by the public or private network QoS class bandwidth guaranteed.</li> <li>■ <b>Policing:</b> This option monitors the bandwidth used by the traffic flow in the class of service and when the traffic exceeds the bandwidth, it rate-limits the traffic.</li> <li>■ <b>Default Class:</b> If the traffic does not fall under any of the defined classes, the traffic is associated with the default CoS.</li> </ul> <p><b>Note</b> The Dynamic Bandwidth Adjustment configuration is not supported with public link CoS.</p> <p>For more information about how to configure CoS, see <a href="#">Configure Class of Service</a>.</p>
Strict IP precedence	<p>This check box is available when you select the <a href="#">Configure Class of Service</a> check box.</p> <p>When you enable this option, 8 VCMP sub-paths corresponding to the 8 IP precedence bits are created. Use this option when you want to combine the Classes of Service into less number of classes in the network of your Service Provider.</p>

**Table 29-7. Advanced Settings common for Public and Private Overlay (continued)**

Option	Description
	By default, this option is deactivated and the VCMP sub-paths are created for the exact number of classes of service that are configured. The grouping is not applied.

**Table 29-8. Advanced Settings for Public Overlay**

Option	Description
UDP Hole Punching	<p>If a Branch to Branch SD-WAN overlay is required and branch Edges are deployed behind NAT devices, that is NAT device is WAN side of the Edge, the direct VCMP tunnel on UDP/2426 will not likely come up if the NAT devices have not been configured to allow incoming VCMP tunnels on UDP port 2426 from other Edges.</p> <p>Use <b>Branch to Branch VPN</b> to enable branch to branch tunnels. See <a href="#">Configure a Tunnel Between a Branch and a Branch VPN</a> and <a href="#">Configure Cloud VPN and Tunnel Parameters for Edges</a>.</p> <p>Use <b>Remote Diagnostics &gt; List Paths</b> to check that one Edge has built a tunnel to another Edge.</p> <p>UDP hole punching attempts to work around NAT devices blocking incoming connections. However, this technique is not applicable in all scenarios or with all types of NATs, as NAT operating characteristics are not standardized.</p> <p>Enabling UDP hole punching on an Edge overlay interface, instructs all remote Edges to use the discovered NAT public IP and NAT dynamic source port discovered through SD-WAN Gateway as destination IP and destination port for creating a VCMP tunnel to this Edge overlay interface.</p> <hr/> <p><b>Note</b> Before enabling UDP hole punching, configure the branch NAT device to allow UDP/2426 inbound with port forwarding to the Edge private IP address or put the NAT device, which is usually a router or modem, into bridge mode. Use UDP hole punching only as a last resort as it will not work with firewalls, symmetric NAT devices, 4G/LTE networks due to CGNAT, and most modern NAT devices.</p> <hr/> <p>UDP hole punching may introduce additional connectivity issues as remote sites try to use the new UDP dynamic port for VCMP tunnels.</p>
Type	When configuring a business policy for an Edge, you can choose the <b>Link Steering</b> to prefer a <b>Transport Group</b> as: Public Wired, Public Wireless or Private Wired. See <a href="#">Configure Link Steering Modes</a> .

**Table 29-8. Advanced Settings for Public Overlay (continued)**

Option	Description
	Choose <b>Wired</b> or <b>Wireless</b> , to put the overlay into a public wired or wireless transport group.

The following image shows Advanced settings for a Public Overlay:

View advanced settings

**Bandwidth Measurement** ⓘ Measure Bandwidth (Slow Start) ▾

**Dynamic Bandwidth Adjustment** ⓘ  Deactivated

**Link Mode** ⓘ Active ▾ ⚠

**MTU** 1500

**Overhead Bytes** 0

**Path MTU Discovery**  Activated

**Public Link Configuration**

**UDP Hole Punching**  Deactivated

**Type** Wired

**Configure Class of Service**  Deactivated

**CANCEL** **ADD LINK**

**Table 29-9. Advanced Settings for Private Overlay**

Option	Description
Private Network Name	<p>If you have more than one private network and want to differentiate between them to ensure that the Edges try to tunnel only to Edges on the same private network then define a Private Network Name and attach the Overlay to it. This prevents tunneling to Edges on a different private network they cannot reach. In addition, configure the Edges in other locations on this private network to use the same private network name.</p> <p>For example:</p> <p>Edge1 GE1 is attached to <i>private network A</i>. Use <i>private network A</i> for the private overlay attached to GE1.</p> <p>Edge1 GE2 is attached to <i>private network B</i>. Use <i>private network B</i> for the private overlay attached to GE2.</p> <p>Repeat the same attachment and naming for Edge2.</p> <p>When you enable branch to branch or when Edge2 is a hub site:</p> <ul style="list-style-type: none"> <li>■ Edge1 GE1 attempts to connect to Edge2 GE1 and not GE2.</li> <li>■ Edge1 GE2 attempts to connect to Edge2 GE2 and not GE1.</li> </ul>
Configure Static SLA	<p>Forces the overlay to assume that the SLA parameters being set are the actual SLA values for the path. No dynamic measurement of packet loss, latency or jitter will be done on this overlay. The QoE report uses these values for its Green/Yellow/Red coloring against thresholds.</p> <p><b>Note</b> Static SLA configuration is not supported from release 3.4. It is recommended not to use this option, as dynamic measurement of packet loss, latency and jitter will provide a better outcome.</p>

The following image shows Advanced settings for a Private Overlay:

**View advanced settings**

Bandwidth Measurement ⓘ	Measure Bandwidth (Slow Start) ▾
Dynamic Bandwidth Adjustment ⓘ	<input type="checkbox"/> Deactivated
Link Mode ⓘ	Active ▾ <span style="color: red;">⚠</span>
MTU	1500
Overhead Bytes	0
Path MTU Discovery	<input checked="" type="checkbox"/> Activated
Private Network Name	<input checked="" type="radio"/> Use existing Private Network Name <input type="radio"/> Create new Private Network Name
Existing Private Network Name	None ▾
<b>Public Link Configuration</b>	
Configure Static SLA	<input type="checkbox"/> Deactivated
Configure Class of Service	<input type="checkbox"/> Deactivated

CANCEL
ADD LINK

8 Click **Add Link** to save the configuration.

## Support for DSCP Value Tag Per User Defined Overlay

With the 5.0.0 release, network administrators will have the ability to add a DSCP tag to a specific overlay link. The DSCP tag would be applied at the outer header of the VCMP packet going over the overlay link, and will leverage the private network underlay DSCP tag to treat each overlay uniquely via the QoS setting defined on the WAN underlay network.

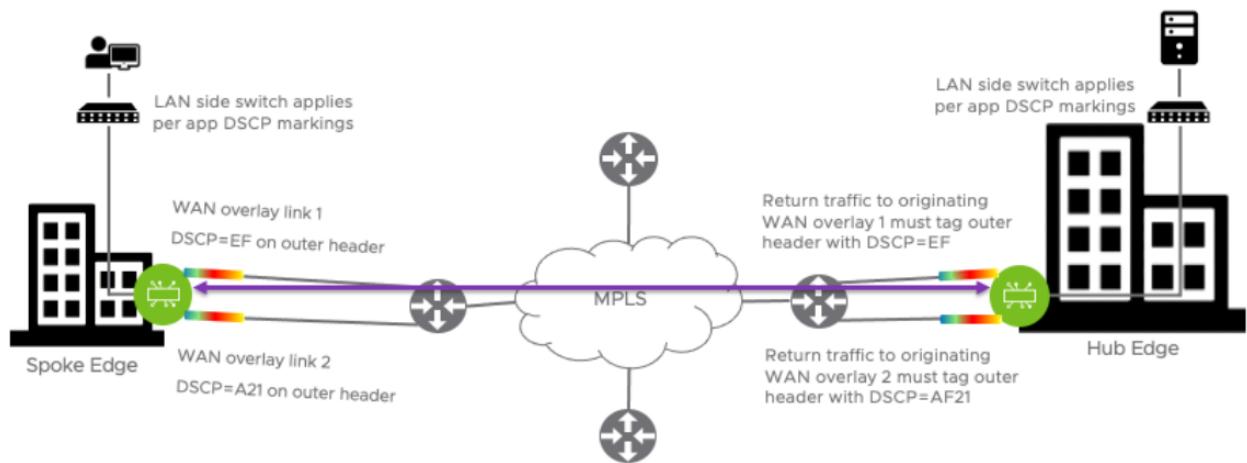
### Enable Per link DSCP Check box

Select this check box to add a DSCP tag to a specific overlay link. The DSCP tag will be applied at the outer header of the VCMP packet going over this overlay link. This will provide the ability to leverage the private network underlay DSCP tag mechanism to treat each overlay uniquely via QoS setting defined at the upstream router.

## Use Case: DSCP Value Per User Defined Overlay

In this use case, the requirement is to apply the WAN overlay DSCP tag value configured on the WAN link to all traffic egressing from this link, for the tunnel originating Edge. The configured DSCP value should apply to the VCMP outer header so that the MPLS network can read the DSCP value and apply differentiated services to the VCMP encapsulated packet. The inner DSCP tag value, coming from the LAN side of the edge network, should be kept unmodified. Requirements on the tunnel destination side: The hub or peer edge that is receiving the tunnel creation request must respond with the same DSCP overlay tag value sent by the tunnel originator on the VCMP outer header. The hub or peer edge terminating the overlay tunnel should not modify the inner DSCP tag destined for the LAN.

In the image below, the Enterprise is using DSCP values on their underlay network to provide differentiated services based on source WAN overlay link/tunnel.



## SD-WAN Service Reachability via MPLS

An Edge with only Private MPLS links can reach the Orchestrator and Gateways located in public cloud, by using the SD-WAN Service Reachable option.

In a site with no direct public internet access, the SD-WAN Service Reachable option allows the private WAN to be used for private site-to-site VCMP tunnels and as a path to communicate with an internet hosted VMware service.

For hybrid environments that have MPLS-only links or require failover to MPLS links, you can enable the SD-WAN Service Reachable option.

---

**Caution** You should be careful when you turn on SD-WAN Reachable. This feature means that the Edge can connect to both the Orchestrator and Gateways over that link. But if you use it on a private WAN link that does not have this connection, it can cause two problems:

- 1 If the Edge is a Hub, and Spoke Edges are using that Hub Edge as the internet breakout, their tunnels to the Gateway may not come up because the Hub Edge may forward those flows back out the private link.
  - 2 An Edge with this incorrect setting may appear offline in the Orchestrator. This is because it may try to use the private link to contact the Orchestrator.
- 

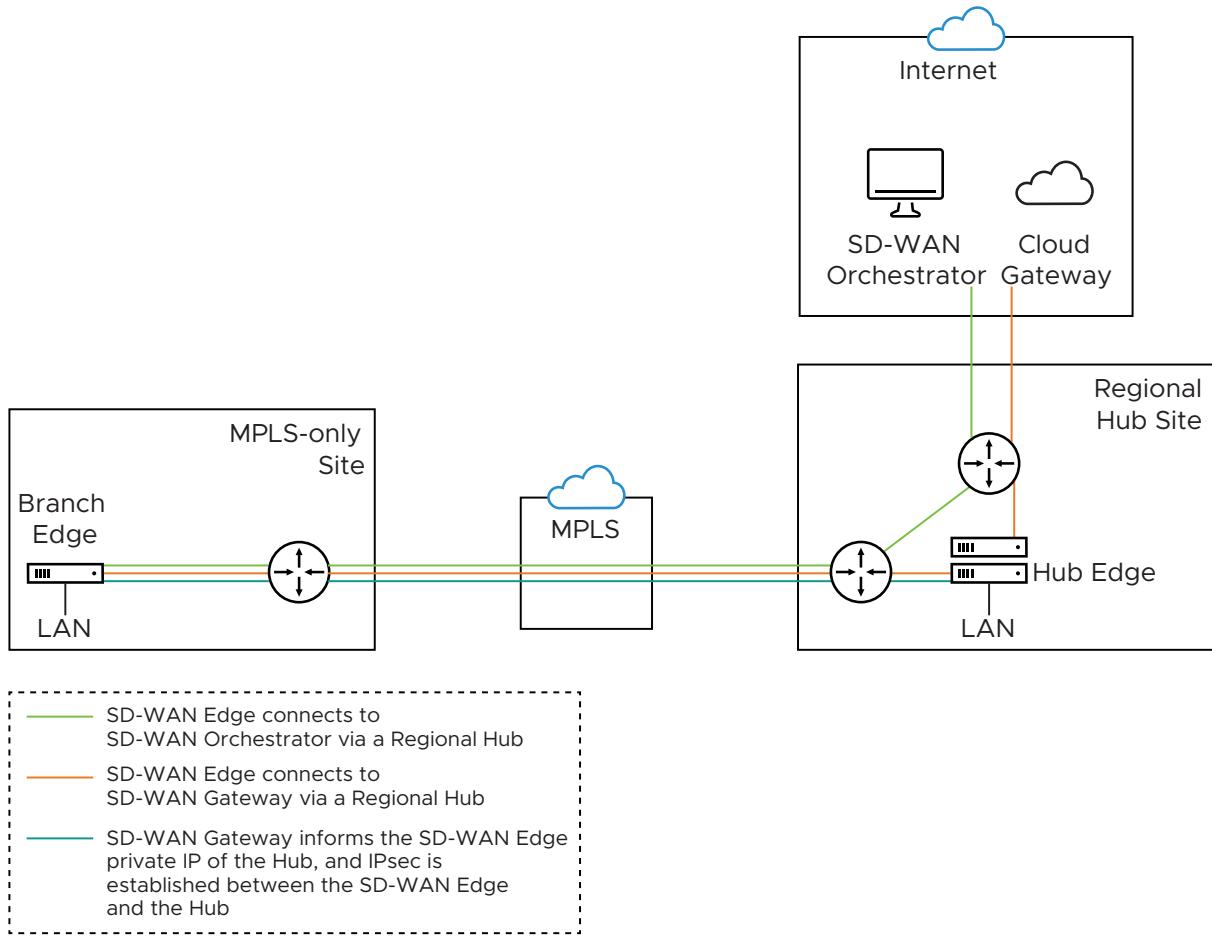
## MPLS-only Sites

VMware supports private WAN deployments with a hosted VMware service for customers with hybrid environments who deploy in sites with only a private WAN link.

In a site with no public overlays, the private WAN can be used as the primary means of communication with the VMware service, including the following:

- Enabled SD-WAN service reachability through private link
- Enabled NTP override using private NTP servers

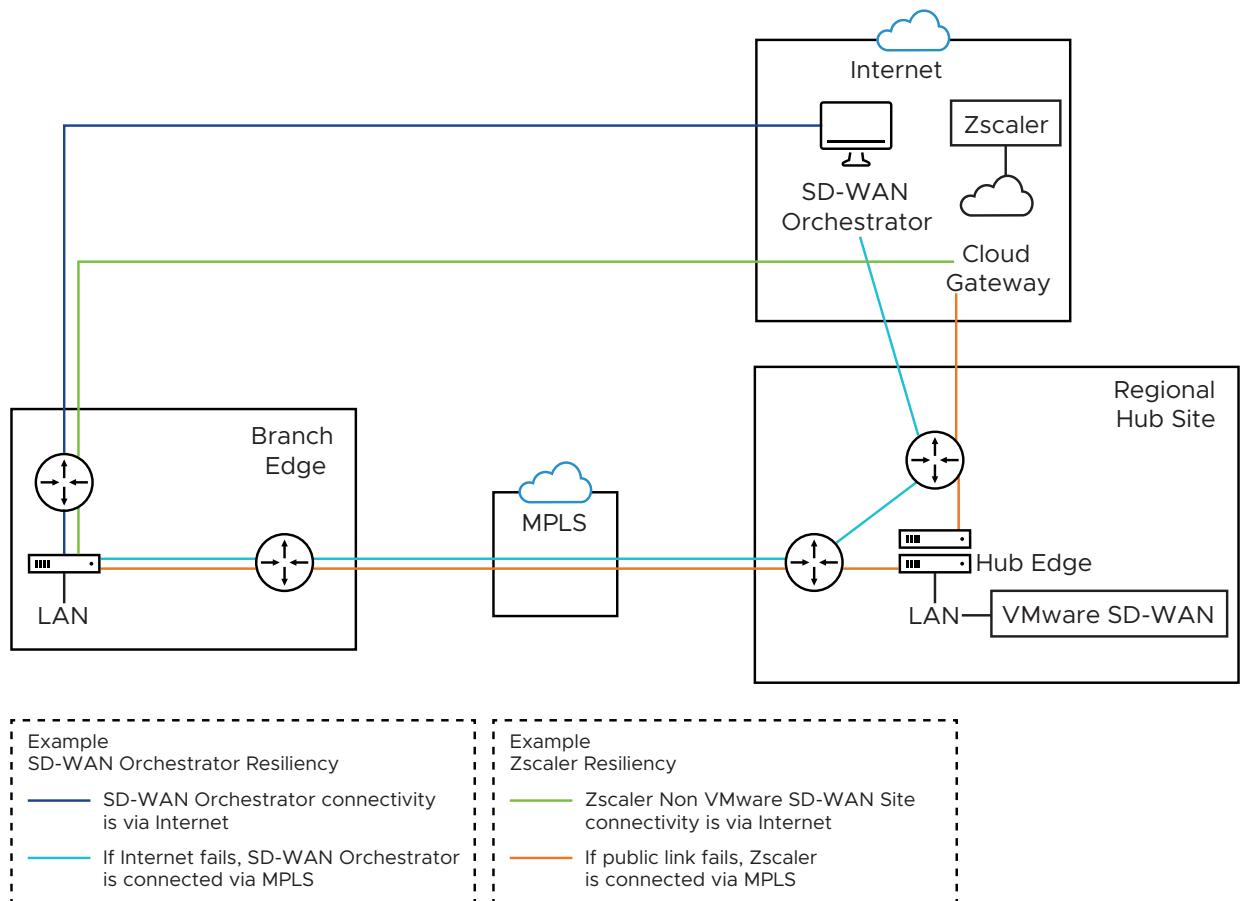
The following image shows a Regional Hub with Internet connection and SD-WAN Edge with only MPLS connection.



The traffic from the SD-WAN Edge with MPLS-only links is routed to the Orchestrator and Gateway through a Regional Hub, which is able to break out to the public cloud. SD-WAN Service Reachable option allows the Edge to remain online and manageable from the Orchestrator, and allows public internet connectivity through the Gateway irrespective of whether or not there is public link connectivity.

## Dynamic Failover via MPLS

If all the public Internet links fail, you can failover critical Internet traffic to a private WAN link. The following image illustrates Resiliency of SASE Orchestrator and Non SD-WAN Destination, Zscaler.



- **Orchestrator Resiliency** – The Orchestrator connects to the Internet. If the Internet fails, the Orchestrator will connect through MPLS. The Orchestrator connection is established using the IP Address which is advertised over MPLS. The connectivity leverages the public Internet link in the Regional Hub.
- **Zscaler Resiliency** – The Zscaler connectivity is established through Internet. If the public link fails, then Zscaler connects through MPLS.

## Configure SD-WAN Service Reachable

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, expand **Interfaces**.
- 4 The different types of Interfaces available for the selected Edge are displayed. Click the link to an Interface connected to the MPLS link.
- 5 In the **Interface** window, select the **Override** check box and from the **WAN Link** drop-down menu, select **User Defined** and click **Save**.

## Virtual Edge

Enabled

---

**IPv4 Settings**

Addressing Type	Static
IP Address *	172.16.1.10
CIDR Prefix *	29
Gateway	172.16.1.11

**WAN Link** User Defined

**OSPF**  OSPF not enabled for the selected Segment

**Multicast**  Multicast is not enabled for the selected segment

**VNF Insertion**  VNF insertion is disallowed when an interface is configured for WAN links

**Advertise**  Enabled

**NAT Direct Traffic**  Enabled

**Trusted Source**  Enabled

**CANCEL** **SAVE**

**Note** The **SD-WAN Service Reachable** is available only for a **User Defined** network.

- In the **WAN Link Configuration** section, click the Interface activated with **User Defined** WAN link. The **User Defined WAN Link** window appears.

## Virtual Edge: GE6\_Private

X

## User Defined WAN Link

Address Type IPv4

Link Type Private

Name GE6\_Private

## Description

Enter Description (Optional)

Maximum 256 characters

SD-WAN Service Reachable ⓘ  ActivatedSD-WAN Service Reachable  
Backup ⓘ  Activated

## Public SD-WAN Addresses

Address
169.254.8.2
20.1.0.2
fd00:ff01:0:1::2
20.2.0.2
100.101.0.2

Public IP Address N/A

Operator Alerts ⓘ  DeactivatedAlerts ⓘ  DeactivatedInterfaces  GE6

&gt; View optional configuration

&gt; View advanced settings

CANCEL

UPDATE LINK

- In the **User Defined WAN Link** window, select the **SD-WAN Service Reachable** check box to deploy sites which only have a private WAN link and/or activate the capability to failover critical Internet traffic to a private WAN link.

When you select the **SD-WAN Service Reachable** checkbox, a list of public IP addresses of SD-WAN Gateways and SASE Orchestrator is displayed, which may need to be advertised across the private network, if a default route has not been already advertised across the same private network from the firewall.

When you select the **SD-WAN Service Reachable Backup** check box, the Private SD-WAN reachable link is used as the backup link for Internet and as an active link for Enterprise destinations, if Public WAN overlays are present. When this option is deactivated, the Private link is used as an active link.

- Configure other options as required, and then click **Update Link** to save the settings.

For more information on other options in the **WAN Overlay** window, see [Configure Edge WAN Overlay Settings](#).

## Configure Class of Service

You can manage traffic by defining Class of Service (CoS) in a public or private WAN link. You can group similar types of traffic as a class. The CoS treats each class with its level of service priority.

For each Edge consisting of public or private WAN links, you can define the CoS.

- In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- In the **Connectivity** category, click and expand **Interfaces**.
- The **Interfaces** section displays the different types of Interfaces available for the selected Edge.
- In the **WAN Link Configuration** section, click **Add User Defined WAN Link**.

WAN Link Configuration						
<a href="#">+ ADD USER DEFINED WAN LINK</a>		<a href="#">DELETE</a>				
Type	Name	IP Version	Interfaces	Link Type	Public IP	Operator Alert
<input checked="" type="radio"/> User Defined	GE6_Private	IPv4	GE6	Private Wired		
<input type="radio"/> Auto Detect	169.254.7.10	IPv4	GE3	Public Wired	169.254.7.10	
<input type="radio"/> Auto Detect	169.254.6.34	IPv4	GE4	Public Wired	169.254.6.34	

- In the **User Defined WAN Link** window, enter the name for the new WAN link and choose the Link Type as required, that is **Public** or **Private**.
- To configure CoS for the new link, scroll down and click **View advanced settings**.

## Virtual Edge: new link

## User Defined WAN Link

Address Type

IPv4

Link Type

Public

Name

User\_defined\_Link1

Description

Enter Description (Optional)

Maximum 256 characters

Public IP Address

N/A

Operator Alerts

 Deactivated

Alerts

 Deactivated

Interfaces

 GE6

## Public Link Configuration

UDP Hole Punching

 Deactivated

Type

Wired

## Configure Class of Service

 Activated

Strict IP Precedence

 Activated

## Class Of Service

ADD

DELETE

<input type="checkbox"/>	Class Of Service	DSCP Tags	Bandwidth (%)	Policing	Default Class
<input type="checkbox"/>	costeat	AF11	100	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Default

CANCEL

ADD LINK

8 Select the **Configure Class of Service** check box and configure the following settings:

- **Strict IP precedence:** Select this check box to enforce strict IP precedence.

When you enable this option, 8 VCMP sub-paths corresponding to the 8 IP precedence bits are created. Use this option when you want to combine the Classes of Service into less number of classes in the network of your Service Provider.

By default, this option is deactivated and the VCMP sub-paths are created for the exact number of classes of service that are configured. The grouping is not applied.

- **Class of Service:** You can add multiple class of services. Click **+Add** and enter a descriptive name for the class of service. The name can be a combination of alphanumeric and special characters.
- **DSCP Tags:** You can assign multiple DSCP tags to the class of service by selecting DSCP tags from the available list.

---

**Note** You should map DSCP tags of same IP precedence to the same class of service. A CoS queue can be an aggregate of many classes but DSCP values of same class cannot be part of multiple class queues.

For example, the following set of DSCP tags cannot be spread across multiple queues:

- CS1 and AF11 to AF14
  - CS2 and AF21 to AF24
  - CS3 and AF31 to AF34
  - CS4 and AF41 to AF44
- 
- **Bandwidth:** Enter a value in percentage for the traffic designated to the CoS. This value allocates a weight to the class. The incoming traffic is processed based on the associated weight. If you have multiple class of services, the total value of the bandwidth should add up to 100.
  - **Policing:** Select the checkbox to enable the class-based policing. This option monitors the bandwidth used by the traffic flow in the class of service and when the traffic exceeds the bandwidth, it polices the traffic.
  - **Default Class:** Click to set the corresponding class of service as default. If the incoming traffic does not fall under any of the defined classes, the traffic is associated with the default CoS.

- 9 Click **Add Link** to save the settings.
- 10 Click **Save Changes** in the **Device** page.
- 11 You can also define the CoS for an existing link by clicking the existing WAN links and performing the step 9.

For more information on the Edge WAN Overlay Settings, see [Configure Edge WAN Overlay Settings](#).

## Configure Hot Standby Link

Hot Standby link an enhanced backup link, for the WAN links of an Edge, with pre-established VCMP tunnels. When the active links are down, Hot Standby link enables immediate switchover by using the pre-established VCMP tunnels.

### Prerequisites

To configure a Hot Standby link on an Edge, ensure that the Edge is upgraded to software image version 4.0.0 or later.

### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, expand **Interfaces**. The **Interfaces** section displays the different types of Interfaces available for the selected Edge.
- 4 In the **WAN Link Configuration** section, you can configure Hot Standby link mode for existing auto-detected or user-defined WAN links or you can create a new WAN link by clicking the **Add User Define WAN Link** and configure Hot Standby link mode. For steps on how to add a new user defined WAN link, see [Configure Edge WAN Overlay Settings](#).

WAN Link Configuration

WAN Link Configuration							
Type		Name	IP Version	Interfaces	Link Type	Public IP	Operator Alert
<input checked="" type="radio"/>	User Defined	GE6_Private	IPv4	GE6	Private Wired		
<input type="radio"/>	Auto Detect	169.254.7.10	IPv4	GE3	Public Wired	169.254.7.10	
<input type="radio"/>	Auto Detect	169.254.6.34	IPv4	GE4	Public Wired	169.254.6.34	

- 5 To configure Hot Standby link mode for an existing link, click the existing WAN link and modify the settings.

### Virtual Edge: GE6\_Private

#### User Defined WAN Link

Address Type	IPv4
Link Type	Private
Name	GE6_Private
Description	<input type="text" value="Enter Description (Optional)"/> <small>Maximum 256 characters</small>
SD-WAN Service Reachable <small>①</small>	<input type="checkbox"/> Deactivated
Public IP Address	N/A
Alerts <small>①</small>	<input checked="" type="checkbox"/> Deactivated
Interfaces	<input checked="" type="checkbox"/> GE6

> View optional configuration

#### View advanced settings

Bandwidth Measurement <small>①</small>	Measure Bandwidth (Slow Start)
Dynamic Bandwidth Adjustment <small>①</small>	<input type="checkbox"/> Deactivated
Link Mode <small>①</small>	Hot Standby
Minimum Active Links	1
MTU	1500
Overhead Bytes	0
Path MTU Discovery	<input checked="" type="checkbox"/> Activated
Private Network Name	<input checked="" type="radio"/> Use existing Private Network Name <input type="radio"/> Create new Private Network Name
Existing Private Network Name	None
<b>Private Link Configuration</b>	
Configure Static SLA	<input type="checkbox"/> Deactivated

- 6 In the **User Defined WAN Link** window, scroll down and click **View advanced settings**.
- 7 From the **Link Mode** drop-down menu, select **Hot Standby**.
- 8 From the **Minimum Active Links** from the drop-down menu, select the number of active links that can be present in the network at a time. When the number of current active links that are UP goes below the selected number, then the Hot Standby link comes up. The range is 1 to 3, with the default value being 1.
- 9 Configure other options as required and click **Update Link** to save the settings. For more information on other options in the **WAN Overlay** window, see [Configure Edge WAN Overlay Settings](#).

## Results

Once you configure the Hot Standby link, the tunnels are setup, which enables a quick switchover in case of a failure. The Hot Standby link receives no data traffic except the heartbeats, which are sent every 5 seconds.

When the path from Edge to Primary Gateway on Active links goes down and when the number of Active links that are UP is below the number of **Minimum Active Links** configured, the Hot Standby link will come up. The traffic is sent through the Hot Standby path.

When the path to Primary Gateway comes up on Active links and the number of Active links exceeds the number of **Minimum Active Links** configured, the Hot Standby link goes to the STANDBY mode. The traffic flow switches over to the Active links.

## What to do next

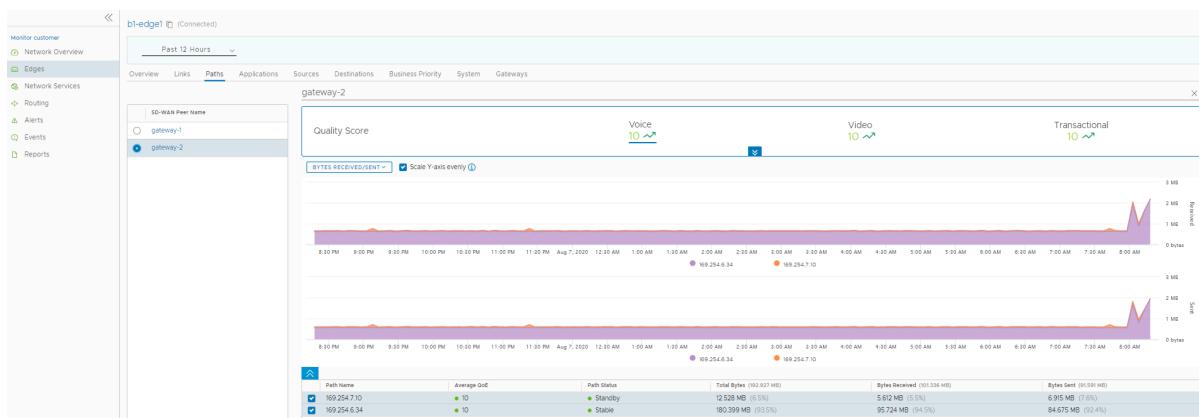
You can monitor the Hot Standby links in the monitoring dashboard. See [Monitor Hot Standby Links](#).

## Monitor Hot Standby Links

You can monitor the Hot standby links and the corresponding status using the monitoring dashboard.

To view the status of Hot Standby links:

- 1 In the SD-WAN service of the Enterprise portal, click **Monitor > Edges** to view the Edges associated with the Enterprise.
- 2 Click the link to an Edge configured with Hot standby link. The **Overview** tab displays the links with status.
- 3 Click the **Links** tab to view more details with graphs.
- 4 Click the **Paths** tab and select an SD-WAN peer to view the status of the paths from the selected Edge.



## Configure DHCPv6 Prefix Delegation for Edges

DHCPv6 Prefix Delegation feature allows packet exchange between a DHCP Client and a DHCP Server. The Edge requests the server to provide prefixes over the WAN interfaces to delegate to clients on the LAN side. The server provides a prefix to the Edge in response. The Edge then configures an IP address on the LAN interface using this delegated prefix. The Edge starts sending out router advertisements with this prefix.

You can override the Prefix Delegation settings configured on a Profile. For information on how to configure the DHCPv6 Prefix Delegation for Profiles, see [Configure DHCPv6 Prefix Delegation for Profiles](#).

To configure DHCPv6 Prefix Delegation on an Edge, ensure that the Edge is upgraded to a version that supports this feature, and then perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 DHCPv6 Prefix Delegation can be configured on WAN, LAN, and VLAN interfaces. See the following sections for more details.

### DHCPv6 Prefix Delegation on a WAN interface

**Note** For a WAN interface, the **Enable WAN Link** option must be selected.

- 1 On the Edge Device settings page, go to the **Connectivity** category, and then expand **Interfaces**.
- 2 The **Interfaces** section displays the different types of Interfaces available for the selected Edge. Click the link to a Routed WAN interface.
- 3 On the Routed Interface settings screen, navigate to **IPv6 Settings**.

IPv6 Settings

Enabled

Addressing Type: DHCP Stateless

IP Address	N/A
Cidr Prefix	N/A
Gateway:	N/A

DHCPv6 Client Prefix Delegation:  Enabled

Select Tag     New Tag

tag1

**⚠** Tag will not have any effect until it is associated with the corresponding LAN/VLAN.

WAN Link: Auto-Detect

OSPF:  OSPF not enabled for the selected Segment

Advertise:  Enabled

**CANCEL** **SAVE**

- 4 Activate the **DHCPv6 Client Prefix Delegation** feature by selecting the **Enabled** check box.
- 5 You can either select a pre-defined tag from the drop-down menu or create a new tag by selecting the **New Tag** option. You can also define tags on the **Network Services** screen. For more information, see [Configure Prefix Delegation Tags](#).
- 6 Click **Save**.

## DHCPv6 Prefix Delegation on a LAN interface

**Note** For a LAN interface, ensure that the **Enable WAN Link** option is not selected.

- 1 On the Edge Device settings page, go to the **Connectivity** category, and then expand **Interfaces**.
- 2 The **Interfaces** section displays the different types of Interfaces available for the selected Edge. Click the link to a Routed LAN interface.
- 3 On the Routed Interface settings screen, navigate to **IPv6 Settings**.

**IPv6 Settings**

Enabled

Addressing Type	DHCPv6 Prefix Delegation
IP Address	N/A
Prefix Length	64
Interface Address	fd::1:2:3:1 Example: ::1:0:0:0:1
Tag	tag1
<span style="color: orange;">⚠️</span> DHCPv6 Prefix Delegation tags are effective only if they are associated with the corresponding WAN. <span style="float: right;">X</span>	
OSPF	<span style="color: red;">✖️</span> OSPF not enabled for the selected Segment
Advertise	<input type="checkbox"/> Enabled
NAT Direct Traffic	<input checked="" type="checkbox"/> Enabled

CANCEL SAVE

- 4 To configure Prefix Delegation for a LAN interface, you must select the **Addressing Type** as **DHCPv6 Prefix Delegation** from the drop-down menu.

- 5 The following additional options appear on the screen:

Option	Description
Prefix Length	This field is auto-populated. The value displayed is <b>64</b> . This indicates that a netmask of 64 bits is configured for this interface's address.
Interface Address	Enter a valid interface address. The new address is formed by combining the prefix provided by the server and the interface address that is configured. If 'n' bits prefix is received from the server, then the first 'n' bits of the interface address are overwritten to form a new address.
Tag	Select the tag from the drop-down menu to associate the configured interface address with the corresponding WAN interface.  <b>Note</b> Same tag can be used by multiple LAN interfaces.

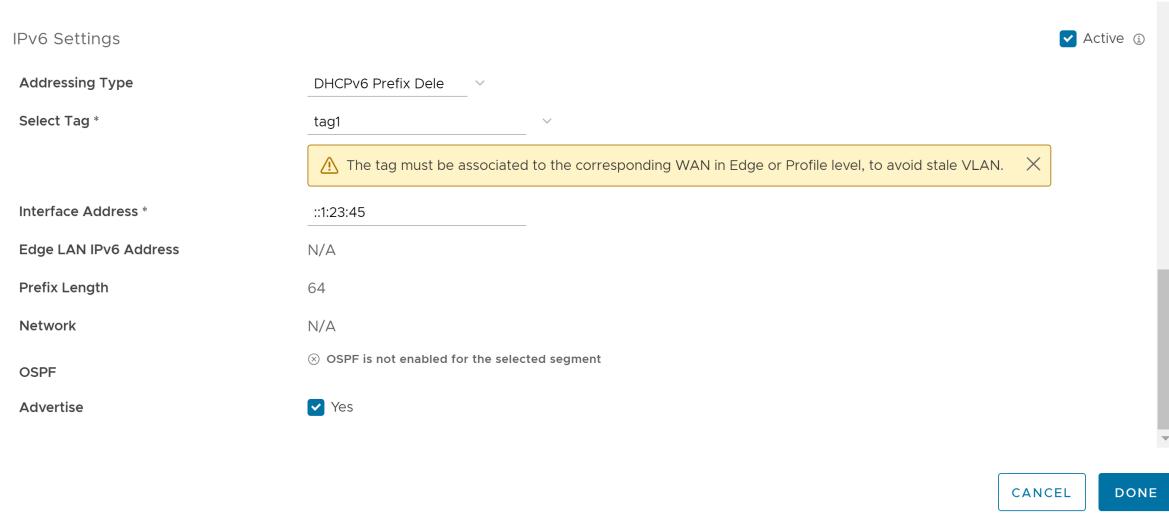
**Warning** Ensure that the same combination of **Interface Address** and **Tag** is not used on any two LAN/VLAN interfaces on the same Edge. This could lead to duplicate addresses getting assigned on those interfaces.

- 6 Click **Save**.

**Note** For information on the other settings on this screen, see [Configure Interface Settings for Edges](#).

## DHCPv6 Prefix Delegation on a VLAN interface

- 1 On the Edge Device settings page, go to the **Connectivity** category, and then expand **VLAN**.
- 2 Click on a VLAN interface.
- 3 In the **Edit VLAN** dialog, navigate to the **IPv6 Settings** section.



- 4 To configure Prefix Delegation for a VLAN interface, you must select the **Addressing Type** as **DHCPv6 Prefix Delegation** from the drop-down menu.
- 5 Select a tag from the drop-down menu.
- 6 Enter a valid interface address.
- 7 Click **Done**.

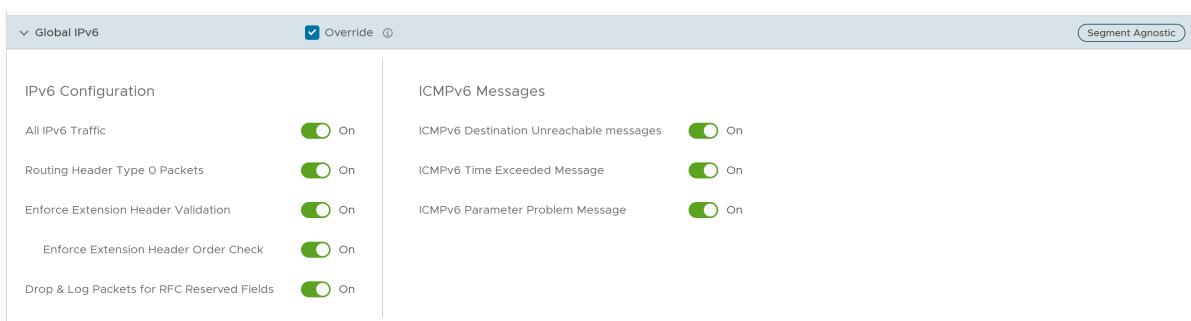
For more information on VLAN for Edges, see [Configure VLAN for Edges](#).

## Global IPv6 Settings for Edges

For IPv6 addresses, you can activate some of the configuration settings globally.

To activate global settings for IPv6 at the Edge level:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the link to a Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Under the **Connectivity** category, click **Global IPv6** and select the **Override** check box.



- 4 You can override the following settings inherited from the Profile, by using the toggle button.

Option	Description
All IPv6 Traffic	Allows all IPv6 traffic in the network
Routing Header Type 0 Packets	Allows Routing Header type 0 packets. Deactivate this option to prevent potential DoS attack that exploits IPv6 Routing Header type 0 packets.
Enforce Extension Header Validation	Allows to check the validity of IPv6 extension headers.
Enforce Extension Header Order Check	Allows to check the order of IPv6 Extension Headers.
Drop & Log Packets for RFC Reserved Fields	Allows to reject and log network packets if the source or destination address of the network packet is defined as an IP address reserved for future definition.
ICMPv6 Destination Unreachable messages	Generates messages for packets that are not reachable to IPv6 ICMP destination.
ICMPv6 Time Exceeded Message	Generates messages when a packet sent by IPv6 ICMP has been discarded as it was out of time.
ICMPv6 Parameter Problem Message	Generates messages when the device finds problem with a parameter in ICMP IPv6 header.

## Configure Wi-Fi Radio Overrides

At the Edge level, you can override the Wi-Fi Radio settings specified in the Profile, by selecting the **Override** check box. Based on the Edge model and the country configured for the Edge, Wi-Fi Radio settings allow you to select a radio band and channel supported for the Edge.

To override the Wi-Fi Radio settings at the Edge level, perform the following steps:

### Prerequisites

Before configuring the Wi-Fi radio band and channel for the Edge, it is important to set the correct country of operation for the Wi-Fi radio, to conform to local requirements for Wi-Fi transmission. The address is populated automatically after the Edge is activated; however, you can override the address manually, if needed. If you want to change the location of the Edge, go to the **Contact & Location** section of the **Edge Overview** configuration page and click **Edit Location** to set the Edge location, and then click **Save Changes**.

---

**Note** The country should be specified using the 2-character ISO 3166-1-alpha-2 notation (for example, US, DE, IN, and so on.)

---

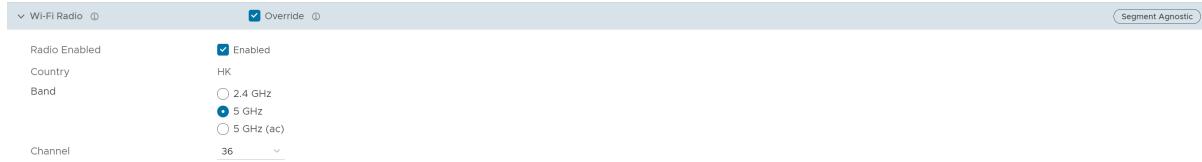
### Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.

- 2 Select an Edge for which you want to override Wi-Fi Radio settings, and then click the **View** link in the **Device** column of the Edge.

The **Device Setting** page for the selected Edge appears.

- 3 In the **Configure Segment** drop-down menu, by default, **Global Segment** is selected. If needed, you can select a different Profile segment from the drop-down menu.
- 4 Under the **Connectivity** category, go to the **Wi-Fi Radio** area and select the **Override** check box.



- 5 Select a radio band from the **Band** of radio frequencies supported for the Edge.
- 6 From the **Channel** drop-down menu, select a radio channel supported for the Edge.

---

**Note** The **Band** and **Channel** selectors display only the supported radio bands and channels for the configured location of the Edge. If a country is not set for the Edge or the country is unsupported, then the **Band** is set to **2.4 GHz** and **Channel** is set to **Automatic**.

- 7 Edge 710 supports dual-radio models. In this case, the settings from the common Profile Radio are automatically inherited, so that only one radio is activated. But if these settings are overridden, you have an option to activate both radios to simultaneously transmit on 2.4 and 5 GHz.

Radio Enabled	Band	Channel
Radio 1 <input checked="" type="checkbox"/> Enabled	<input checked="" type="radio"/> 2.4 GHz	Automatic
Radio 2 <input checked="" type="checkbox"/> Enabled	<input type="radio"/> 5 GHz <input type="radio"/> 5 GHz (ac) <input type="radio"/> 5 GHz (ax)	Automatic

#### Note

- Edge 710 has a Wi-Fi 6 card (802.11ax) that has 2 radios; one that can transmit only in the 2.4 GHz band, and one that can transmit only in 5 GHz band. Each band is independently capable of being set up as 802.11n, ac or ax. Typically, you must activate ac and ax on the 5GHz band.
- Dual-radio models independently use both, 2.4 GHz and 5 GHz bands. However, if the 5 GHz band is selected in an unsupported country, it is deactivated, and the 2.4 GHz band is activated by default.
- Single-radio models default to either 2.4 GHz or 5GHz. In case where both bands are selected, the radio transmits in the 5 GHz band, if it is in a supported country, else it is forced to use the 2.4 GHz band, irrespective of the Profile settings.

- 8 Click **Save Changes**. The Wi-Fi Radio settings are overridden for the selected Edge.

## Configure Automatic SIM Switchover

This feature allows you to automate the process of LTE SIM switching in case of primary LTE connection failure. You can configure the Edge to automatically detect the primary LTE link failure and thereby initiate the process of establishing the secondary LTE link. When the **Automatic Switchover** feature is activated, and for some reason, the secondary LTE link is also down, the Edge tries to establish the connection with the primary link again. This process continues until the Edge detects an active LTE link. Also, if automatic switchover is in progress, manual switchover cannot be performed on the Edge.

#### Prerequisites

- You must insert SIM cards in both the SIM slots on the Edge.
- This feature can be activated only on a standalone Edge where **High Availability** is deactivated. An error is displayed on the Orchestrator if you try to activate both, **High Availability** and **Automatic Switchover** features.

- Navigate to **Configure > Edges > Device tab > Interface Settings**, and make sure that the **IP Type**, **L2 Settings**, and **WAN Overlay** settings are same for both Cell1 and Cell2. Other parameters like **SIM PIN**, **Network**, and **APN** need not be same.
- Both Cell1 and Cell2 interfaces must be activated before activating the **Automatic Switchover** feature. For more information, see [Configure Interface Settings for Edges](#).

To access this feature, follow the below steps:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Connectivity** category, expand **Automatic Switchover**. The following screen appears:

The screenshot shows the 'Device' tab for the '610-LTE' edge. The 'Segment' dropdown is set to 'GLOBAL SEGMENT'. Under the 'Connectivity' category, the 'Automatic Switchover' section is expanded. It shows the 'Automatic Switchover' checkbox is checked (Enabled) and the 'Switchover Time' is set to 60. Other connectivity settings like VLAN, Loopback Interfaces, Management Traffic, ARP Timeouts, and Global IPv6 are listed with 'Segment Agnostic' status.

- 4 You can configure the following settings, and then click **Save Changes**:

Option	Description
Automatic Switchover	Select the <b>Enabled</b> check box to activate this feature.
Switchover Time	Select the time after which the Edge must switchover to the secondary LTE link. The Edge detects the connection failure and waits till the specified <b>Switchover Time</b> to initiate the switchover process. This helps in avoiding any unnecessary switchovers happening due to link flaps. Once initiated, the switchover happens in 4 to 5 minutes. The available values are <b>30</b> , <b>60</b> , and <b>90</b> seconds. By default, <b>60</b> is selected.

To monitor the Edge Switchover status, go to **Monitor > Edges**, and then click the link to your Edge. The **Overview** tab is displayed by default.

The screenshot shows the VMware SD-WAN Administration Guide interface. The left sidebar has a tree view with 'Edges' selected. The main content area is titled 'Edges / b1-edge1' and shows 'Connected'. It includes tabs for Overview, QoE, Links, Paths, Flows, Applications, Sources, Destinations, Business Priority, and System. The 'Links Status' section lists two links: 'AT&T Internet S' (68.78.202.2) and 'Verizon Wireless' (171.194.139.178). The 'Top Consumers' section shows applications like SD-WAN Control, SD-WAN Management, and Domain Name Service. The 'Operating Systems' section shows Network Service. A 'Categories' section is also visible.

- The **Auto Dual-Mode SIM** column displays the status of the Edge with respect to the **Automatic Switchover** feature configured on that Edge, and is applicable only for a **610-LTE**. See the table below for the color code details:

Color	Status
Green	Indicates that the Secondary SIM is inserted and the <b>Automatic Switchover</b> feature is activated.
Amber / Orange	Indicates that the Secondary SIM is inserted and the <b>Automatic Switchover</b> feature is deactivated.
Purple	Indicates that the Secondary SIM is not inserted and the <b>Automatic Switchover</b> feature is activated.
Red	Indicates that the Secondary SIM is not inserted and the <b>Automatic Switchover</b> feature is deactivated.

- The **Signal** column displays the signal strength of the Edge. This is indicated by the number of bars, which vary depending on the signal strength. Below are the details:

Signal Strength (dB)	Number of Bars
-10 to -85	4
-86 to -102	3
-103 to -110	2
-111 to -120	1
-121 to -999	0

For more information, see [Monitor Edges](#).

The Switchover status can also be viewed on the **Monitor > Events** page. The following two events are displayed on the screen when the **Automatic Switchover** feature is activated.

Event	Description
EDGE_AUTO_SIM_SWITCH	This event is triggered in the following scenarios when the <b>Automatic Switchover</b> feature is activated or deactivated: <ul style="list-style-type: none"> <li>■ The <b>Automatic Switchover</b> feature fails to get activated after the Orchestrator sends the configuration to the Edge.</li> <li>■ During the switchover process, when there is at least one active WAN link on the Edge.</li> </ul>
EDGE_CELL_SWITCHOVER	This event is triggered after the cell switchover process, irrespective of whether the process was successful or not.

For more information, see [Monitor Events](#).

## Configure Common Criteria Firewall Settings for Edges

The Common Criteria (CC) Firewall settings are inherited from the Profile associated with the Edge and can be reviewed in the Edge Device tab. At the Edge level, you can choose to override the CC Firewall settings for an Edge.

To configure the CC Firewall settings at the Edge level, perform the following steps:

### Procedure

1 In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**.

The **Edges** page displays the existing Edges.

2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. You can also select an Edge and click **Modify** to configure the Edge.

- The **Device** tab displays the configuration options for the selected Edge.

The screenshot shows the VMware Orchestrator interface with the SD-WAN service selected. The left sidebar shows 'Edge Configuration' with 'Edges' selected. The main area shows 'b3-edge1' connected to 'GLOBAL SEGMENT'. The 'Device' tab is active. Under 'Connectivity', the 'Common Criteria Firewall' section has an 'Override' checkbox checked. A yellow warning box is overlaid on this section with the following text:

⚠ When this option is set to On, the following packets are automatically dropped, counted, or logged:  
 • Packets with invalid fragments or fragments which cannot be completely re-assembled.  
 • Packets where the source address is defined as being on either broadcast network, multicast network, or loopback address.  
 • Packets with the IP-options: Loose Source Routing, Strict Source Routing, or Record Route specified.  
 • Packets which have the source or destination address as unspecified or reserved for future.

At the bottom right, there are 'DISCARD CHANGES' and 'SAVE CHANGES' buttons.

- In the **Connectivity** category, click **Common Criteria Firewall**.
- Select the **Override** check box to override the CC Firewall settings inherited from the associated Profile.
- After updating the required settings for the selected Edge, click **Save Changes**.

## Configure Cloud VPN and Tunnel Parameters for Edges

The Edge Cloud VPN settings are inherited from the Profile associated with the Edge and can be reviewed in the Edge **Device** tab. At the Edge level, you can override these settings inherited from a Profile and configure tunnel parameters.

- In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.
- Select an Edge you want to override Non SD-WAN Destination settings for, and then click the **View** link under the **Device** column. The **Device** settings page for the selected Edge appears.
- Go to the **VPN Services** area, and expand **Non SD-WAN Destination via Edge**.
- Select the **Override** check box to override the Non SD-WAN Destination settings inherited from the Profile as needed.

---

**Note** Any configuration changes to **Branch to Non SD-WAN Destination via Gateway** settings can be made only in the associated Profile level.

Non SD-WAN Destination via Edge						<input checked="" type="checkbox"/> Override 
<input checked="" type="checkbox"/> Enable Non SD-WAN via Edge						
 ADD		 NEW NSD VIA EDGE		 DELETE		
Service	Link					Action
<input type="checkbox"/> Name	Automation for all public WAN Links	Enable Service	Enable Tunnel	Destination Primary Public IP	Destination Secondary Public IP	Action
<input type="checkbox"/> NSD1 	N/A	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>	fd00:bbbb:1:1::1	-	 
<input type="checkbox"/> NSD2 	N/A	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>	169.254.6.18	-	 

2 items

5 Under the **Action** column, click + to add tunnels. The **Add Tunnel** pop-up window appears.

## Add Tunnel



Public WAN Link \* 

169.254.6.2



Local Identification Type

IPv4



Local Identification \* 

169.254.6.2

PSK \*

.....



Destination Primary Public IP \*

34.56.43.12

Destination Secondary Public IP

CANCEL

SAVE

6 Enter the following details for configuring a tunnel to the Non SD-WAN Destination:

Option	Description
Authentication Method	<p>Select either <b>PSK</b> or <b>Certificate</b> as the authentication method.</p> <p><b>Note</b> The <b>Certificate</b> Authentication mode is available only when the system property <code>session.options.enableNsdPkIIPv6Config</code> is set to <b>True</b>.</p>
Public WAN Link	Select a WAN link from the drop-down list.
Local Identification Type	<p>Select any one of the Local authentication types from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ <b>FQDN</b> - The Fully Qualified Domain Name or hostname. For example, vmware.com.</li> <li>■ <b>User FQDN</b> - The User Fully Qualified Domain Name in the form of email address. For example, user@vmware.com.</li> <li>■ <b>IPv4</b> - The IP address used to communicate with the local gateway.</li> <li>■ <b>IPv6</b> - The IP address used to communicate with the local gateway.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ These values are available only when you select the <b>Authentication Mode</b> as <b>PSK</b>.</li> <li>■ The <b>IPv6</b> Local Identification Type displays the value <b>DER ASN1 DN</b> when the <b>Authentication Mode</b> is <b>Certificate</b>. Also, the <b>IPv6</b> is available only when the system property <code>session.options.enableNsdPkIIPv6Config</code> is set to <b>True</b>.</li> </ul>
Local Identification	<p>Local authentication ID defines the format and identification of the local gateway. For the selected <b>Local Identification Type</b>, enter a valid value. The accepted values are IP address, User FQDN (email address), and FQDN (hostname or domain name). The default value is local IPv4 or IPv6 address.</p> <p><b>Note</b> Configuring <b>Local Identification</b> in Strongswan is optional. If not configured, Strongswan uses the value from the certificate.</p>
PSK	Enter the Pre-Shared Key (PSK), which is the security key for authentication across the tunnel in the text box.
Remote Identification Type	This field is displayed only when the <b>Authentication Method</b> is selected as <b>Certificate</b> . Currently, only <b>DER ASN1 DN</b> type is supported.

Option	Description
Remote Identification	<p>This field is displayed only when the <b>Authentication Method</b> is selected as <b>Certificate</b>. Remote authentication ID defines the format and identification of the remote gateway. For the selected <b>Remote Identification Type</b>, enter a valid value. The accepted values are IP address, User FQDN (email address), and FQDN (hostname or domain name). The default value is local IPv4 or IPv6 address.</p>
	<p><b>Note</b> Configuring <b>Remote Identification</b> in Strongswan is optional. If not configured, Strongswan uses the value from the certificate.</p>
Destination Primary Public IP	<p>Enter the Public IP address of the destination Primary VPN Gateway.</p>
Destination Secondary Public IP	<p>Enter the Public IP address of the destination Secondary VPN Gateway.</p>

#### Note

- When you choose the **Authentication Method** as **Certificate**, the **Local Identification Type** and **Remote Identification Type** display the value **DER\_ASN1\_DN** by default.
- The **Local Identification** and **Remote Identification** fields must be configured in **DER\_ASN1\_DN** format. The values **FQDN**, **User FQDN**, **IPv4**, and **IPv6** are reserved for future use.

- 7 Click **Save** to save the changes.

## Configure Cloud Security Services for Edges

When you have assigned a profile to an Edge, the Edge automatically inherits the cloud security service (CSS) and attributes configured in the profile. You can override the settings to select a different cloud security provider or modify the attributes for each Edge.

To override the CSS configuration for a specific Edge, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Profiles.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Under the **VPN Services** category, in the **Cloud Security Service** area, the CSS parameters of the associated profile are displayed.
- 4 In the **Cloud Security Service** area, select the **Override** check box to select a different CSS or to modify the attributes inherited from the profile associated with the Edge. For more information on the attributes, see [Configure Cloud Security Services for Profiles](#).

- Click **Save Changes** in the **Edges** window to save the modified settings.

**Note** For CSS of type Zscaler and Generic, you must create VPN credentials. For Symantec CSS type, the VPN credentials are not needed.

## Manual Zscaler CSS Provider Configuration for Edges

At the Edge level, for a selected manual Zscaler CSS provider, you can override the settings inherited from the profile and can configure additional parameters manually based on the tunneling protocol selected for tunnel establishment.

If you choose to configure an IPsec tunnel manually, apart from the inherited attributes, you must configure a Fully Qualified Domain Name (FQDN) and Pre-Shared Key (PSK) for the IPsec session.

**Note** As a prerequisite, you should have Cloud security service gateway endpoint IPs and FQDN credentials configured in the third party Cloud security service.

FQDN	PSK
S15.L2B13.E15d57@velocloud.net	.....

**Note** For cloud security services with Zscaler login URL configured, **Login to Zscaler** button appears in the **Cloud Security Service** area. Clicking the **Login to Zscaler** button will redirect you to the Zscaler Admin portal of the selected Zscaler cloud.

If you choose to configure a GRE tunnel manually, then you must configure GRE tunnel parameters manually for the selected WAN interface to be used as source by the GRE tunnel, by following the steps below.

- Under **GRE Tunnels**, click **+Add**.

WAN Links
WAN Links

- In the **Configure Tunnel** window appears, configure the following GRE tunnel parameters, and click **Update**.

X

## Configure Tunnel

**WAN Links** 54.69.238.136 ▾  
Select a link to continue

**Tunnel Source Public IP** Custom WAN IP ▾

**Link IP** 216.66.5.49

**Tunnel Addressing**

Tunnel Addressing	Point-of-Presence	Router IP / Mask	Internal ZEN IP / Mask
Primary Address	199.168.148.132	Enter Router IP	Enter Internal ZEN IP
Secondary Address	104.129.194.39	Enter Router IP	Enter Internal ZEN IP
2 items			

CANCEL

UPDATE

Option	Description
WAN Links	Select the WAN interface to be used as source by the GRE tunnel.
Tunnel Source Public IP	Choose the IP address to be used as a public IP address by the Tunnel. You can either choose the WAN Link IP or Custom WAN IP. If you choose Custom WAN IP, enter the IP address to be used as public IP. Source public IPs must be different for each segment when Cloud Security Service (CSS) is configured on multiple segments.
Primary Point-of-Presence	Enter the primary Public IP address of the Zscaler Datacenter.
Secondary Point-of-Presence	Enter the secondary Public IP address of the Zscaler Datacenter.
Primary Router IP/Mask	Enter the primary IP address of Router.
Secondary Router IP/Mask	Enter the secondary IP address of Router.

Option	Description
Primary Internal ZEN IP/Mask	Enter the primary IP address of Internal Zscaler Public Service Edge.
Secondary Internal ZEN IP/Mask	Enter the secondary IP address of Internal Zscaler Public Service Edge.

**Note**

- The Router IP/Mask and ZEN IP/Mask are provided by Zscaler.
- Only one Zscaler cloud and domain are supported per Enterprise.
- Only one CSS with GRE is allowed per Edge. An Edge cannot have more than one segment with Zscaler GRE automation enabled.
- Scale Limitations:
  - GRE-WAN: Edge supports maximum of 4 public WAN links for a Non SD-WAN Destination (NSD) and on each link, it can have up to 2 tunnels (primary/secondary) per NSD. So, for each NSD, you can have maximum of 8 tunnels and 8 BGP connections from one Edge.
  - GRE-LAN: Edge supports 1 link to Transit Gateway (TGW), and it can have up to 2 tunnels (primary/secondary) per TGW. So, for each TGW, you can have maximum of 2 tunnels and 4 BGP connections from one Edge (2 BGP sessions per tunnel).

## Automated Zscaler CSS Provider Configuration for Edges

At the Edge level, VMware SD-WAN and Zscaler integration supports:

- [IPsec/GRE Tunnel Automation](#)
- [Zscaler Location/Sub-Location Configuration](#)

For a selected automated Zscaler CSS provider at the Edge level, you can override the CSS settings inherited from the profile, establish automatic IPsec/GRE tunnels for each Edge Segment, create Sub-locations, and configure Gateway options and Bandwidth controls for Location and Sub-locations.

### IPsec/GRE Tunnel Automation

IPsec/GRE tunnel automation can be configured for each Edge segment. Perform the following steps to establish automatic tunnels from an Edge.

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Select an Edge you want to establish automatic tunnels.
- 3 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.

- 4 Under the **VPN Services** category, in the **Cloud Security Service** area, the CSS parameters of the associated profile are displayed.
- 5 In the **Cloud Security Service** area, select the **Override** check box to select a different CSS or to modify the attributes inherited from the profile associated with the Edge. For more information on the attributes, see [Configure Cloud Security Services for Profiles](#).
- 6 From the **Cloud Security Service** drop-down menu, select an automated CSS provider and click **Save Changes**.



The automation will create a tunnel in the segment for each Edge's public WAN link with a valid IPv4 address. In a multi-WAN link deployment, only one of the WAN Links will be utilized for sending user data packets. The Edge chooses the WAN link with the best Quality of Service (QoS) score using bandwidth, jitter, loss, and latency as criteria. Location is automatically created after a tunnel is established. You can view the details of tunnel establishment and WAN links in the **Cloud Security Service** section

---

**Note** After automatic tunnel establishment, changing to another CSS provider from an Automated Zscaler service provider is not allowed on a Segment. For the selected Edge on a segment, you must explicitly deactivate Cloud Security service and then reactivate CSS if you want to change to a new CSS provider from an Automated Zscaler service provider.

---

## Zscaler Location/Sub-Location Configuration

After you have established automatic IPsec/GRE tunnel for an Edge segment, Location is automatically created and appears under the **Zscaler** section of the Edge Device page.

---

**Note** Prior 4.5.0 release, the Sub-location configuration is located in the **Cloud Security Service** section for each segment. Currently, the Orchestrator allows you to configure the Zscaler configurations for Location and Sub-location for the entire Edge from the **Zscaler** section of the **Device Settings** page. For existing user of CSS Sub-location automation, the data will be migrated as part of Orchestrator upgrade.

---

In the **Zscaler** section, if you want to update the Location or create Sub-locations for the selected Edge, make sure:

- you check that the tunnel is established from the selected Edge and Location is automatically created. You will not be allowed to create a Sub-location if the VPN credentials or GRE options are not set up for the Edge. Before configuring Sub-locations, ensure you understand about Sub-location and their limitations. See <https://help.zscaler.com/zia/about-sub-locations>.

- you select the same Cloud Subscription that you used to create the Automatic CSS.

To update the Location or create Sub-locations for the selected Edge, perform the following steps:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Select an Edge and click the icon under the **Device** column. The **Device Settings** page for the selected Edge appears.
- 3 Go to the **Zscaler** section and turn on the toggle button.

Name	Sub-Location Name	LAN Networks	Subnets
<input type="checkbox"/> other			

- 4 From the **Cloud Subscription** drop-down menu, select the same Cloud Subscription that you used to create the Automatic CSS. The Cloud Name associated to the selected Cloud Subscription automatically appears.

---

**Note** Cloud Subscription must have same Cloud name and Domain name as CSS.

---

**Note** If you want to change provider for "Cloud Subscription", you must first remove the "Location" by deactivating CSS and Zscaler, and then perform the creation steps with the new provider.

---

- 5 After you have established automatic IPsec/GRE tunnel for an Edge segment, Location is automatically created and appears under the **Location** table. Note that the Zscaler Location name now includes the Edge name at the beginning so it can be easily identified especially on the Zscaler portal where they can search for the Edge name to find the location.

If you want to configure the Gateway options and Bandwidth controls for the Location, click the **Edit** button. For more information, see [Configure Zscaler Gateway Options and Bandwidth Control](#).

- 6 To create a Sub-location, click **Add**.
  - In the **Sub-Location Name** textbox, enter a unique name for the Sub-location. The Sub-location name should be unique across all segments for the Edge. The name can contain alphanumeric with a maximum word length of 32 characters.

- b From the **LAN Networks** drop-down menu, select a VLAN configured for the Edge.
- c In the **Subnets** textbox, add subnets for the selected LAN network.

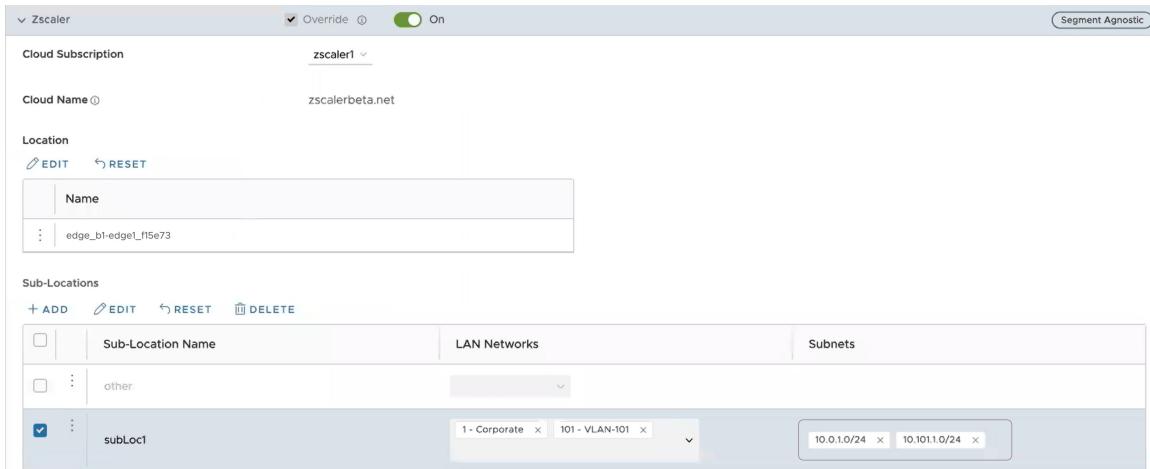
In prior Orchestrator versions, for the Zscaler sub-location configuration, the **Subnets** field that takes in subnets ignores the user input if the subnet being added is not directly connected to the Edge device, and users could not modify these subnets using the Orchestrator UI. This limitation presented a challenge for a branch offices where the LAN-side subnets were one hop away due to the presence of a layer 3 switch between the Edge and LAN devices. Release 6.0.0 allows users to add both direct and non-direct subnets.

---

**Note** For a selected Edge, Sub-locations should not have overlapping Subnet IPs.

---

- d Click **Save Changes**.



**Note** After you create at least one Sub-location in the Orchestrator, an “Other” Sub-location is automatically created in the Zscaler side, and it appears in the Orchestrator UI. You can also configure the “Other” Sub-location’s Gateway options by clicking the **Edit** button under **Gateway Options** in the **Sub-Locations** table. For more information, see [Configure Zscaler Gateway Options and Bandwidth Control](#).

---

- e After creating a Sub-location, you can update the Sub-location configurations from the same Orchestrator page. Once you click **Save Changes**, the Sub-location configurations on the Zscaler side will be updated automatically.
- f To delete a Sub-location, click **Delete**.

---

**Note** When the last Sub-location is deleted from the table, the “other” Sub-location will also be deleted automatically.

---

## Configure Zscaler Gateway Options and Bandwidth Control

To configure Gateway options and Bandwidth controls for the Location and Sub-location, click the **Edit** button under **Gateway Options**, in the respective table.

The **Zscaler Gateway Options and Bandwidth Control** window appears.

## Edit Location Gateway Options



### Location

#### Gateway Options

**Use XFF from Client Request**  Off

**Enable Caution**  Off

**Enable AUP**  Off

**Enforce Firewall Control**  Off

**Authentication**  Off

#### Bandwidth Control

**Bandwidth Control**  Off

**CANCEL**

**DONE**

Configure the Gateway options and Bandwidth controls for the Location and Sub-location, as needed, and click **Save Changes**.

**Note** The Zscaler Gateway Options and Bandwidth Control parameters that can be configured for the Locations and Sub-locations are slightly different, however; the Gateway Options and Bandwidth Control parameters for the Locations and Sub-locations are the same ones that one can configure on the Zscaler portal. For more information about Zscaler Gateway Options and Bandwidth Control parameters, see <https://help.zscaler.com/zia/configuring-locations>

Option	Description
<b>Gateway Options for Location/Sub-Location</b>	
Use XFF from Client Request	<p>Enable this option if the location uses proxy chaining to forward traffic to the Zscaler service, and you want the service to discover the client IP address from the X-Forwarded-For (XFF) headers that your on-premises proxy server inserts in outbound HTTP requests. The XFF header identifies the client IP address, which can be leveraged by the service to identify the client's sub-location. Using the XFF headers, the service can apply the appropriate sub-location policy to the transaction, and if <b>Enable IP Surrogate</b> is turned on for the location or sub-location, the appropriate user policy is applied to the transaction. When the service forwards the traffic to its destination, it will remove the original XFF header and replace it with an XFF header that contains the IP address of the client gateway (the organization's public IP address), ensuring that an organization's internal IP addresses are never exposed to externally.</p> <p><b>Note</b> This Gateway option is only configurable for Parent location.</p>
Enable Caution	<p>If you have not enabled <b>Authentication</b>, you can enable this feature to display a caution notification to unauthenticated users.</p>
Enable AUP	<p>If you have not enabled <b>Authentication</b>, you can enable this feature to display an Acceptable Use Policy (AUP) for unauthenticated traffic and require users to accept it. If you enable this feature:</p> <ul style="list-style-type: none"> <li>■ In <b>Custom AUP Frequency (Days)</b> specify, in days, how frequently the AUP is displayed to users.</li> <li>■ A <b>First Time AUP Behavior</b> section appears, with the following settings: <ul style="list-style-type: none"> <li>■ <b>Block Internet Access</b> - Enable this feature to deactivate all access to the Internet, including non-HTTP traffic, until the user accepts the AUP that is displayed to them.</li> <li>■ <b>Force SSL Inspection</b> - Enable this feature to make SSL Inspection enforce an AUP for HTTPS traffic.</li> </ul> </li> </ul>
Enforce Firewall Control	<p>Select to enable the service's firewall control.</p> <p><b>Note</b> Before enabling this option, user must ensure if its Zscaler account has subscription for "Firewall Basic".</p>
Enable IPS Control	<p>If you have enabled <b>Enforce Firewall Control</b>, select this to enable the service's IPS controls.</p> <p><b>Note</b> Before enabling this option, user must ensure if its Zscaler account has subscription for "Firewall Basic" and "Firewall Cloud IPS".</p>

Option	Description
Authentication	Enable to require users from the Location or Sub-location to authenticate to the service.
IP Surrogate	If you enabled <b>Authentication</b> , select this option if you want to map users to device IP addresses.
Idle Time for Dissociation	<p>If you enabled <b>IP Surrogate</b>, specify how long after a completed transaction, the service retains the IP address-to-user mapping. You can specify the Idle Time for Dissociation in Mins (default), or Hours, or Days.</p> <ul style="list-style-type: none"> <li>■ If the user selects the unit as Mins, the allowable range is from 1 through 43200.</li> <li>■ If the user selects the unit as Hours, the allowable range is from 1 through 720.</li> <li>■ If the user selects the unit as Days, the allowable range is from 1 through 30.</li> </ul>
Surrogate IP for Known Browsers	Enable to use the existing IP address-to-user mapping (acquired from the surrogate IP) to authenticate users sending traffic from known browsers.
Refresh Time for re-validation of Surrogacy	<p>If you enabled <b>Surrogate IP for Known Browsers</b>, specify the length of time that the Zscaler service can use IP address-to-user mapping for authenticating users sending traffic from known browsers. After the defined period of time elapses, the service will refresh and revalidate the existing IP-to-user mapping so that it can continue to use the mapping for authenticating users on browsers. You can specify the Refresh Time for re-validation of Surrogacy in minutes (default), or hours, or days.</p> <ul style="list-style-type: none"> <li>■ If the user selects the unit as Mins, the allowable range is from 1 through 43200.</li> <li>■ If the user selects the unit as Hours, the allowable range is from 1 through 720.</li> <li>■ If the user selects the unit as Days, the allowable range is from 1 through 30.</li> </ul>
<b>Bandwidth Control Options for Location</b>	
Bandwidth Control	Enable to enforce bandwidth controls for the location. If enabled, specify the maximum bandwidth limits for Download (Mbps) and Upload (Mbps). All sub-locations will share the bandwidth limits assigned to this location.
Download	If you enabled Bandwidth Control, specify the maximum bandwidth limits for Download in Mbps. The allowable range is from 0.1 through 99999.
Upload	If you enabled Bandwidth Control, specify the maximum bandwidth limits for Upload in Mbps. The allowable range is from 0.1 through 99999.

Option	Description
Bandwidth Control Options for Sub-Location (if Bandwidth Control is enabled on Parent Location)	
<h2>Edit Location Gateway Options</h2> <span style="float: right;">X</span>	
<b>Location</b> subLoc1	
<h3>Gateway Options</h3>	
<b>Enable Caution</b>	<input type="checkbox"/> Off
<b>Enable AUP</b>	<input type="checkbox"/> Off
<b>Enforce Firewall Control</b>	<input type="checkbox"/> Off
<b>Authentication</b>	<input type="checkbox"/> Off
<h3>Bandwidth Control</h3>	
<b>Bandwidth Control</b>	<input type="checkbox"/> Off
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; font-weight: bold;">DONE</span>	
<p><b>Note</b> The following bandwidth control options are configurable for sub-location only if you have bandwidth control enabled on the parent location. If the bandwidth control is not enabled on the parent location, then the bandwidth control options for sub-location are the same as location (Bandwidth Control, Download, Upload).</p>	
<b>Use Location Bandwidth</b>	If you have bandwidth control enabled on the parent location, select this option to enable bandwidth control on the sub-location and use the download and upload maximum bandwidth limits as specified for the parent location.

Option	Description
Override	Select this option to enable bandwidth control on the sub-location and then specify the maximum bandwidth limits for Download (Mbps) and Upload (Mbps). This bandwidth is dedicated to the sub-location and not shared with others.
Disabled	Select this option to exempt the traffic from any Bandwidth Management policies. Sub-location with this option can only use up to a maximum of available shared bandwidth at any given time.

## Limitations

- In 4.5.0 release, when a Sub-location is created, Orchestrator automatically saves the "Other" Sub-location. In earlier version of Orchestrator, the Zscaler "Other" Sub-location was not saved in Orchestrator. After upgrading Orchestrator to 4.5.0 release, the "Other" Sub-location will be imported automatically only after a new normal (non-Other) Sub-location is created using automation.
- Zscaler Sub-locations cannot have overlapping IP addresses (subnet IP ranges). Attempting to edit (add, update, or delete) multiple Sub-locations with conflicting IP addresses may cause the automation to fail.
- Users cannot update the bandwidth of Location and Sub-location at the same time.
- Sub-locations support **Use Location Bandwidth** option for bandwidth control when its Parent Location bandwidth control is enabled. When user turns off the Location bandwidth control on a Parent Location, the Orchestrator does not check or update the Sub-location bandwidth control option proactively.

## Related links

- [Monitor Cloud Security Services](#)
- [Monitor Cloud Security Services Events](#)
- [Monitor Network Services](#)

## Configure Zscaler Settings for Edges

Describes how to configure Zscaler at the Edge level. You can configure the Zscaler settings for an Edge from the **Zscaler** section available under the **VPN Services** category in the **Device** tab.

Before you configure Zscaler, you must have Zscaler cloud subscription. For steps on how to create cloud subscription of type Zscaler, [Configure API Credentials](#).

To configure Zscaler at the Edge level, perform the following steps:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- 2 The **Edges** page displays the existing Edges.

- 3 Click the link to an Edge or click the **View** link in the **Device** column of the Edge.
- 4 The configuration options for the selected Edge are displayed in the **Device** tab.

The screenshot shows the VMware Orchestrator interface for configuring an Edge device. The top navigation bar includes 'Customer 5-site', 'SD-WAN', and 'Open Classic Orchestrator'. The left sidebar has tabs for 'Monitor', 'Configure' (which is selected), 'Diagnostics', and 'Service Settings'. Under 'Configure', there's a tree view with 'Edges' expanded, showing 'b1-edge1' which is 'Connected' and part of 'SD-WAN'. The main content area shows 'Edge Configuration' settings. Under 'Cloud Subscription', 'Cloud Name' is set to 'zscalerbeta.net'. In the 'Location' section, there is a table with one row: 'Name' (edge\_b1-edge1\_f15e73). Below it, the 'Sub-Locations' table has one row: 'Sub-Location Name' (other). A 'Segment' dropdown is set to 'GLOBAL SEGMENT'. A 'Segment Agnostic' button is also present.

- 5 Under the **VPN Services** category, click **Zscaler**.
- 6 The Zscaler settings configured for the associated Profile are displayed. If required, you can select the **Override** check box and modify the Zscaler settings by adding new sub-locations, editing Gateway options for configured location and sub-locations.
- 7 After you have established automatic IPsec/GRE tunnel for an Edge segment, Location is automatically created and appears under the **Location** table. Note that the Zscaler Location name now includes the Edge name at the beginning so it can be easily identified especially on the Zscaler portal where they can search for the Edge name to find the location.
- 8 To edit location Gateway options, click the **Edit** button under the **Location** section. The **Edit Location Gateway Options** dialog box appears.

X

## Edit Location Gateway Options

### Location

#### Gateway Options

Use XFF from Client Request  Off

Enable Caution  Off

Enable AUP  Off

Enforce Firewall Control  Off

Authentication  Off

#### Bandwidth Control

Bandwidth Control  Off

CANCEL

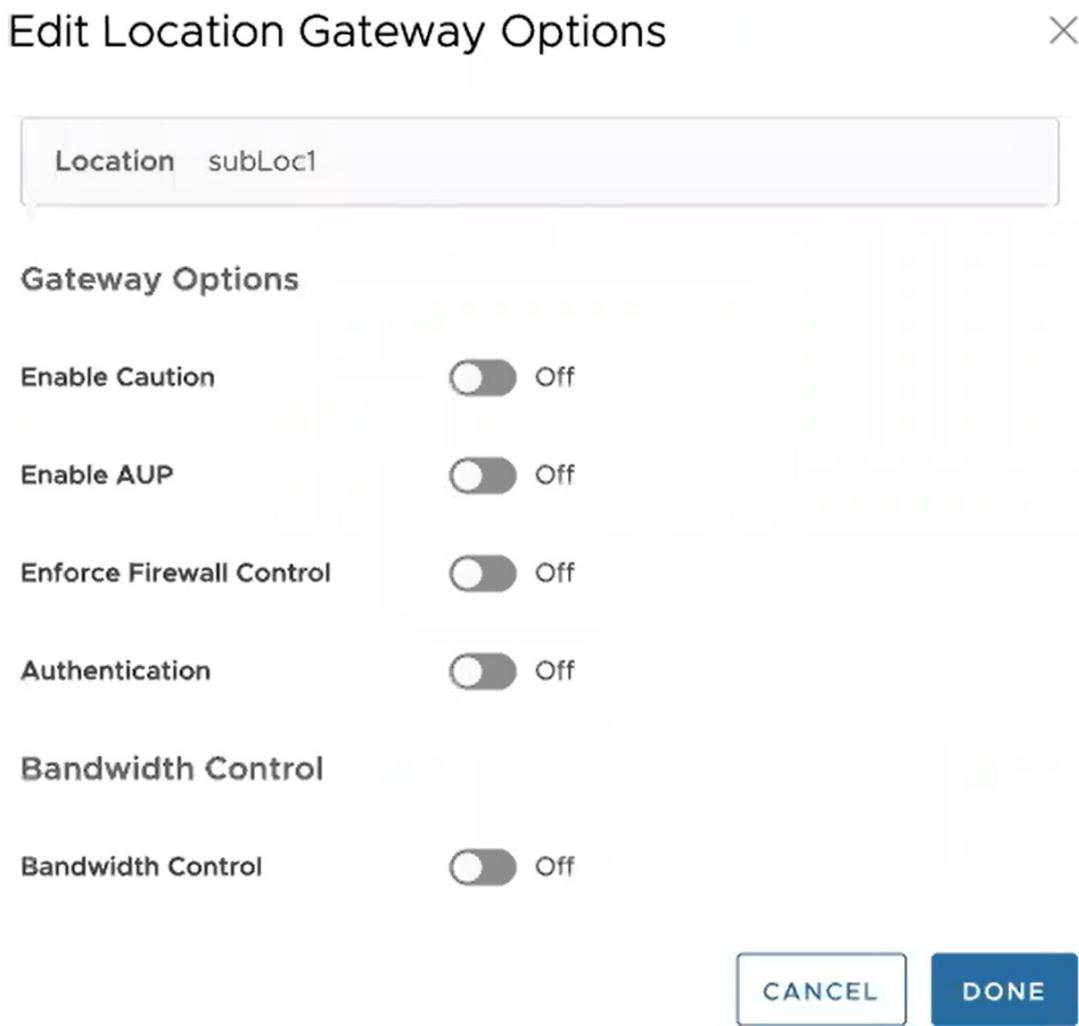
DONE

- 9 Configure the Gateway options and Bandwidth control settings for Location and click **Done**. For more information about Zscaler Gateway Options and Bandwidth Control parameters, see <https://help.zscaler.com/zia/configuring-locations>.
- 10 To reset Zscaler Location gateway options to default, click **Reset** in the **Location** section.
- 11 In the **Sub-Locations** section, you can perform the following:
  - To add sub-locations, click the **+ADD** button and specify sub-location name, LAN networks, and Subnets.

In prior Orchestrator versions, for the Zscaler sub-location configuration, the **Subnets** field that takes in subnets ignores the user input if the subnet being added is not directly connected to the Edge device, and users could not modify these subnets using the Orchestrator UI. This limitation presented a challenge for a branch offices where the LAN-side subnets were one hop away due to the presence of a layer 3 switch between the Edge and LAN devices. Release 6.0.0 allows users to add both direct and non-direct subnets.

Sub-Location Name	LAN Networks	Subnets
other		
subLoc1	1 - Corporate 101 - VLAN-101	10.0.1.0/24 10.101.1.0/24

- To edit Gateway options and Bandwidth control settings for selected Sub-Locations, click the **Edit** button.



- To reset Zscaler Sub-Location gateway options to default, click **Reset**.
  - To delete sub-locations, select the sub-locations that you want to delete and click the **Delete** button.
- 12 After updating the required settings, click **Save Changes** in the Device page.

## Related Topics

- [Configure Cloud Security Services for Profiles](#)
- [Configure Cloud Security Services for Edges](#)

## Configure Secure Access Service for Edges

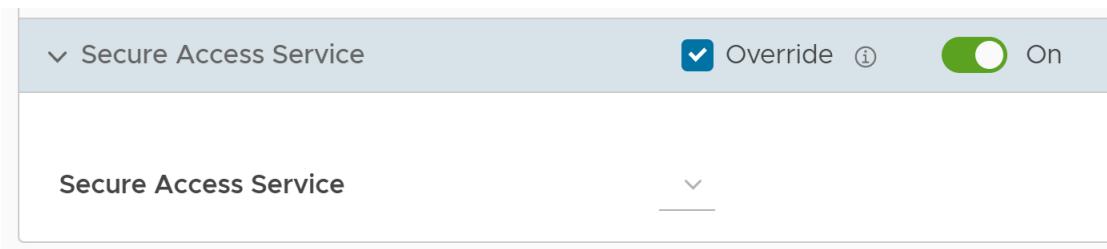
SASE Orchestrator allows you to configure the Secure Access Service at Edge level.

By default, Profile configurations are applied to all the Edges associated with the Profile. If required, you can override the configurations for a specific Edge. For more information, see [Configure Secure Access Service for Profiles](#).

To configure the Secure Access Service for an Edge, follow the below steps:

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.  
The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge. Alternatively, you can click the **View** link in the **Device** column of the Edge.
- 3 Go to the **VPN Services** section, and then expand **Secure Access Service**.



- 4 The configuration settings inherited from the associated Profile are displayed. You can edit the existing settings for the selected Edge, by selecting the **Override** check box.
- 5 Turn on the toggle button, and then select a Secure Access Service from the drop-down menu.
- 6 Click **Save Changes**.

## Configure Multicast Settings for Edges

Multicast provides an efficient way to send data to an interested set of receivers to only one copy of data from the source, by letting the intermediate multicast-routers in the network replicate packets to reach multiple receivers based on a group subscription.

The Multicast settings are applied to all the Edges associated with the Profile. You can choose to override the Multicast settings for an Edge:

- 1 In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Scroll down to the **Routing & NAT** category and expand the **Multicast** area.

The screenshot shows the 'Multicast' configuration page under the 'Routing & NAT' section. The 'Multicast' tab is active, indicated by a blue bar at the top. The 'Override' checkbox is checked, and the 'On' button is enabled. The 'RP Selection' section shows a static entry for RP Address 10.0.0.31 and Multicast Group 226.0.0.0/8. Below this, there's an 'Advanced Settings' section for PIM Timers, with 'Join Prune Send Interval' set to 90 and 'Keep Alive Timer' set to 60.

- 4 The Multicast settings configured for the associated Profile are displayed. If required, you can select the **Override** check box and modify the Multicast settings.

## Configure BFD for Edges

VMware SD-WAN allows to configure BFD sessions to detect route failures between two connected entities. Once you have configured BFD rules for a Profile, the rules are automatically applied to the Edges that are associated with the profile. Optionally, you can override the inherited settings at the Edge level.

### What to do next

To override the configuration for a specific Edge:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the Device Icon next to an Edge, or click the link to an Edge and then click the **Device** tab.
- 3 In the **Device** tab, scroll down to the **BFD Rules** section.
- 4 Select the **Override** check box to modify the BFD configuration settings for the selected Edge.

	Peer Address	Local Address	Multihop	Timers			Order
<input type="checkbox"/>	172.21.1.1	172.21.1.20	<input checked="" type="checkbox"/> Enabled	Detect Multiplier	3		1
				Receive Interval	300		
				Transmit Interval	300		
<input type="checkbox"/>	172.21.4.1	172.21.4.20	<input type="checkbox"/> Enabled	Detect Multiplier	3		2
				Receive Interval	300		
				Transmit Interval	300		

## 5 Click **Save Changes**.

VMware SD-WAN supports configuring BFD for BGP and OSPF.

- To enable BFD for BGP, see [Configure BFD for BGP for Profiles](#).
- To enable BFD for OSPF, see [Configure BFD for OSPF](#).
- To view the BFD sessions, see [Monitor BFD Sessions](#).
- To view the BFD events, see [Monitor BFD Events](#).
- For troubleshooting and debugging BFD, see [Troubleshooting BFD](#).

## LAN-side NAT Rules at Edge Level

LAN-Side NAT (Network Address Translation) Rules allow you to NAT IP addresses in an unadvertised subnet to IP addresses in an advertised subnet. For both the Profile and Edge levels, within the Device Settings configuration, LAN-side NAT Rules has been introduced for the 3.3.2 release and as an extension, LAN side NAT based on source and destination, same packet source and destination NAT support have been introduced for the 3.4 release.

By default, the LAN-Side NAT Rules are inherited by the Edges associated with the Profile. To override the NAT-Side NAT Rules at the Edge level, perform the steps below.

For more information, see [LAN-Side NAT Rules at Profile Level](#)

---

**Note** If the users want to configure the default rule, “any” they must specify the IP address must be all zeros and the prefix must be zero as well: 0.0.0.0/0.

- 1 In the **SD-WAN** Service of the Enterprise Portal, go to [Configure > Edges](#).
- 2 Select the appropriate Edge by clicking the check box next to the Edge **Name**.
- 3 If not already selected, click the **Device** tab link.

- 4 Scroll down to the **Routing & NAT**.
- 5 Open the **LAN-Side NAT Rules** area.
- 6 Click the **Override** check box to make changes to the LAN-Side NAT Rules.
- 7 In the **LAN-Side NAT Rules** area, complete the following for the NAT Source or Destination section: (See the table below for a description of the fields in the steps below).
  - a Enter an address for the **Inside Address** text box.
  - b Enter an address for the **Outside Address** text box.
  - c Enter the Source Route in the appropriate text box.
  - d Enter the Destination Route in the appropriate text box.
  - e Type a description for the rule in the **Description** textbox (optional).

LAN-side NAT Rule	Type	Description
Type drop-down menu	Select either Source or Destination	Determine whether this NAT rule should be applied on the source or destination IP address of user traffic.
Inside Address text box	IPv4 address/prefix, Prefix must be 1-32	The "inside" or "before NAT" IP address (if prefix is 32) or subnet (if prefix is less than 32).
Outside Address text box	IPv4 address/prefix, Prefix must be 1-32	The "outside" or "after NAT" IP address (if prefix is 32) or subnet (if prefix is less than 32).
Source Route text box	<ul style="list-style-type: none"> <li>- Optional</li> <li>- IPv4 address/prefix</li> <li>- Prefix must be 1-32</li> <li>- Default: any</li> </ul>	For destination NAT, specify source IP/subnet as match criteria. Only valid if the type is "Destination."
Destination Route text box	<ul style="list-style-type: none"> <li>- Optional</li> <li>- IPv4 address/prefix</li> <li>- Prefix must be 1-32</li> <li>- Default: any</li> </ul>	For source NAT, specify destination IP/subnet as match criteria. Only valid if the type is "Source."
Description text box	Text	Custom text box to describe the NAT rule.

- 8 In the **LAN-side NAT Rules** area, complete the following for NAT Source and Destination: (See the table below for a description of the fields in the steps below).
  - a For the **Source** type, enter the **Inside Address** and the **Outside Address** in the appropriate text boxes.

- b For the **Destination** type, enter the **Inside Address** and the **Outside Address** in the appropriate text boxes.
- c Type a description for the rule in the **Description** textbox (optional).

NAT Source and Destination

Type	Inside Address *	Outside Address *	Type	Inside Address *	Outside Address *	Description
<input type="checkbox"/>			<input type="checkbox"/>			

## Configure ICMP Probes/Responders

ICMP handlers may be needed to enable integration with an external router that is performing dynamic routing functionality and needs stateful information about route reachability through VMware. You can configure the ICMP Probes and Responders by navigating to the **Configure > Edges > Device** page.

### Configure ICMP Probes

To configure ICMP Probes, perform the following steps:

- 1 In the **SD-WAN** Service of Enterprise Portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge you want to configure ICMP Probes or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Scroll down to the **Routing & NAT** category, click and expand the **ICMP Probes** section.

Name*	VLAN	Source IP	Destination IP*	Next Hop IP	Frequency*	Threshold*
ICMPProb1	10	10.0.0.2	10.0.3.2	10.0.1.32	10	3

1 item

- 4 To create ICMP Probes, click **+Add** and enter the following details:

Field	Description
Name	An unique name for the ICMP Probe.
VLAN	Select the check box to activate VLAN and enter the VLAN ID.
Source IP	The IP address of the Source.
Destination IP	The Destination IP address to ping.
Next Hop IP	The Next Hop IP address.

Field	Description
Frequency	The frequency in seconds to send ping requests. The allowable range is 1 through 60.
Threshold	The number of missed ping replies that will cause the routes to be marked unreachable. The allowable range is 1 through 10.

- 5 Click **Save Changes**.
- 6 To clone an ICMP Probe, select an item and click **Clone**.
- 7 To delete an ICMP Probe, click **Delete**.

## Configure ICMP Responders

To configure ICMP Responders, perform the following steps:

- 1 In the **SD-WAN** Service of Enterprise Portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge you want to configure ICMP Responders or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Scroll down to the **Routing & NAT** category, click and expand the **ICMP Responders** section.



- 4 To create ICMP Responders, click **+Add** and enter the following details:

Field	Description
Name	An unique name for the ICMP Responder.
IP Address	An IP address (virtual IP) that will respond to Ping requests.
Mode	Determines whether to respond to pings Always or Conditional. Select any one of the following: <ul style="list-style-type: none"> <li>■ <b>Always:</b> Edge always responds to ICMP pings.</li> <li>■ <b>Conditional:</b> Edge responds to ICMP pings only when the VPN tunnels are connected.</li> </ul>

- 5 Click **Save Changes**.
- 6 To clone an ICMP Responder, select an item and click **Clone**.
- 7 To delete an ICMP Responder, click **Delete**.

# Configure Static Route Settings

**Static Route Settings** are useful for special cases in which static routes are needed for existing network attached devices, such as printers. You can add or delete Static Route Settings for an Edge. You can configure multiple static routes with different metrics, for the same network, on an Edge. However, only one static route is advertised to overlay for the network.

To configure the Static Route settings:

- 1 In the **SD-WAN** Service of Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Scroll down to the **Routing & NAT** category, click the **Static Route Settings** section.
- 4 In the **IPv4** tab, you can configure the static routes for IPv4 addresses.

Subnet *	Source IP	Next Hop IP *	Interface * ⓘ	VLAN	Cost *	Preferred ⓘ	Advertise ⓘ	ICMP Probe	Description
10.1.0.0/31	10.2.1.0	10.2.1.5	GE2	98	0	Yes	Yes	ICMPv1	Static route

Local Routes  
1 item

Subnet	NSD	Gateway	Cost *	Preferred ⓘ	Advertise ⓘ
 No NSD Routes configured					

NSD Routes  
0 items

You can click the **IPv6** tab to configure static routes for IPv6 addresses.

Subnet *	Next Hop IP *	Interface * ⓘ	VLAN	Cost *	Preferred ⓘ	Advertise ⓘ	ICMP Probe	Description
::/0	fd00::1234:beff:ac..	GE2	0	0	Yes	Yes	ICMPv6	Enter Description (Opt...)

Local Routes  
1 item

Subnet	NSD	Gateway	Cost *	Preferred ⓘ	Advertise ⓘ
 No NSD Routes configured					

NSD Routes  
0 items

Configure the settings as follows:

Option	Description
Subnet	<p>Enter the IPv4 or IPv6 address of the Static Route Subnet that should be advertised.</p> <p>The IPv6 Subnet supports the following address format:</p> <ul style="list-style-type: none"> <li>■ IPv6 global unicast address (2001:CAFE:0:2::1)</li> <li>■ IPv6 unique local address (FD00::1234:BEFF:ACE:EOA4)</li> <li>■ IPv6 Default (::/0)</li> </ul>
Source IP	<p>Enter the corresponding IPv4 or IPv6 address of the selected VLAN. This option is available only when you select the <b>VLAN</b> check box.</p>
Next Hop IP	<p>Enter the next hop IPv4 or IPv6 address for the static route.</p> <p>The IPv6 next hop supports the following address format:</p> <ul style="list-style-type: none"> <li>■ IPv6 global unicast address (2001:CAFE:0:2::1)</li> <li>■ IPv6 unique local address (FD00::1234:BEFF:ACE:EOA4)</li> <li>■ IPv6 link-local address (FE80::1234:BEFF:ACE:EOA4)</li> </ul>
Interface	<p>Choose the WAN Interface to which the static route would be bounded.</p> <p><b>Note</b> This option is displayed as <b>N/A</b>, if the next hop IP address is a part of the Edge's VLAN configuration. In this case, the interface is defined by the VLAN configuration.</p>
VLAN	Select the check box and enter the VLAN ID.
Cost	Enter the cost to apply weightage on the routes. The range is from 0 to 255.
Preferred	<p>Select the check box to match the static route first, even if a VPN route with lower cost is available. If you do not select this option, then any available VPN route is matched, even when the VPN route has higher cost than the static route.</p> <p>The static route will be matched only when the corresponding VPN routes are not available.</p> <p><b>Note</b> This option is not available for IPv6 address type.</p>
Advertise	<p>Select the check box to advertise the route over VPN. Other Edges in the network will have access to the resource. Do not select this option when a private resource like a tele-worker's personal printer is configured as a static route and other users should be prevented from accessing the resource.</p> <p><b>Note</b> This option is not available for IPv6 address type.</p>

Option	Description
ICMP Probe	<p>Choose an ICMP probe from the drop-down menu or click the <b>+New</b> button to create a new ICMP probe. The SD-WAN Edge uses ICMP probe to check for the reachability of a particular IP address and notifies to failover if the IP address is not reachable.</p> <p><b>Note</b> This option is not supported for IPv6 address type.</p>
Description	Enter an optional description for the static route.

In addition, you can configure the NSD Static Routes. The NSD Static Routes that are configured in the **Network Services** gets listed in the **Static Route Settings** section for IPv4 addresses. You can edit the additional flags like the Cost, Preferred, and Advertise options. The **Gateway** column is updated only for NSD Static Routes via Gateway. You cannot edit the **Advertise** option for NSD Static Routes from Gateway.

- Click **Save Changes** in the **Device** tab.

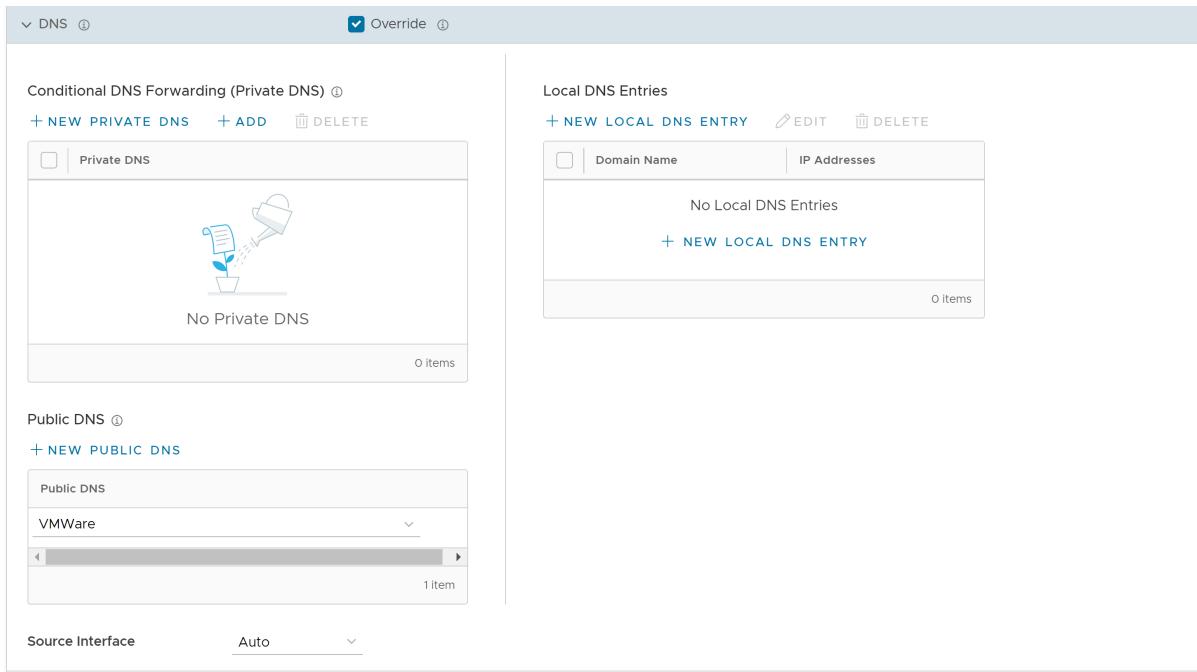
## Configure DNS for Edges

Domain Name System (DNS) is used to configure conditional DNS forwarding through a private DNS service and to specify a public DNS service to be used for querying purpose.

The DNS Service can be used for a public DNS service or a private DNS service provided by your company. A Primary Server and Backup Server can be specified. The public DNS service is preconfigured to use Google and Open DNS servers.

The DNS settings are applied to all the Edges associated with the Profile. You can choose to override the DNS settings for an Edge.

- In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- Click the link to an Edge or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- In the **Routing & NAT** category, click **DNS**. The DNS settings configured for the associated Profile are displayed. If required, you can select the **Override** check box and modify the DNS settings.



- 4 From the **Source Interface** drop-down menu, select an Edge interface that is configured for the segment. This interface will be the source IP for the DNS service.

---

**Note** When the Edge transmits the traffic, the packet header has the IP address of the selected source interface, whereas the packets can be sent through any interface based on the destination route.

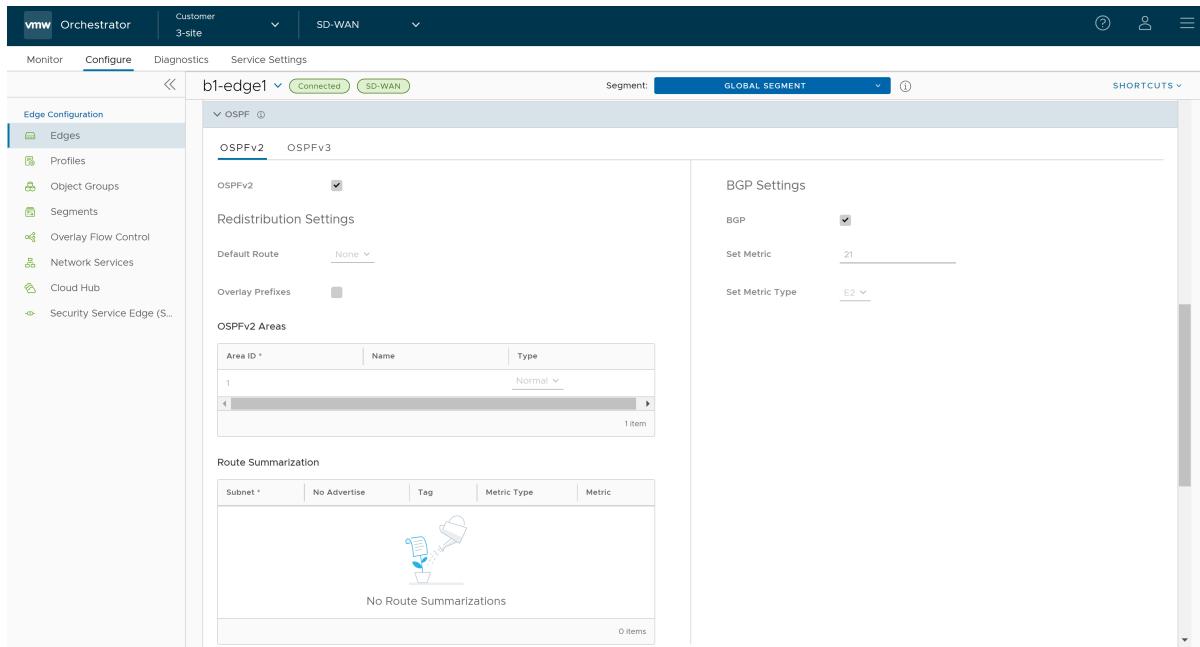
- 5 After updating the required settings, click **Save Changes** in the **Device** page.

## Activate OSPF for Edges

Open Shortest Path First (OSPF) can be enabled only on a LAN interface as an active or passive interface. The Edge will only advertise the prefix associated with that LAN switch port. To get full OSPF functionality, you must use it in routed interfaces. After you configure the OSPF settings at the Profile level, all the Edges associated with the Profile will inherit the OSPF configuration from the Profile. However, you cannot override the OSPF configuration settings at the Edge level.

If needed, you can view the OSPF configuration for a specific Edge as follows:

- In the **SD-WAN** service of the Enterprise Portal, click **Configure > Edges**.
- Click the Device Icon next to an Edge, or click the link to an Edge and then click the **Device** tab.
- Go to the **Routing & NAT** section and click the arrow next to OSPF.
- In the **OSPF** section, you can view all the inherited OSPF configuration such as OSPF areas, Redistribution settings for OSPFv2/v3, BGP settings, and Route Summarization.



## Configure BGP from Edge to Underlay Neighbors for Edges

You can override the inherited Profile settings at the Edge level when configuring BGP from the Edge to Underlay Neighbors.

If required, you can override the configuration for a specific Edge as follows:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge.
- 3 Go to the **Routing & NAT** section and click the arrow next to **BGP** to expand.
- 4 The BGP settings configured for the associated Profile are displayed. If required, you can select the **Override** check box and modify the BGP Settings.
- 5 In addition to the BGP settings configured for a Profile, you can select an Edge Interface configured in the segment as the source Interface for BGP. For the IPv4 address type, you can select only the Loopback Interface as Source Interface and for the IPv6 address type, you can select any Edge Interface as the Source Interface.

This field is available:

- Only when you choose to override the BGP Settings at the Edge level.

- For eBGP, only when **Max-hop** count is more than 1. For iBGP, it is always available as iBGP is inherently multi-hop.

### Important

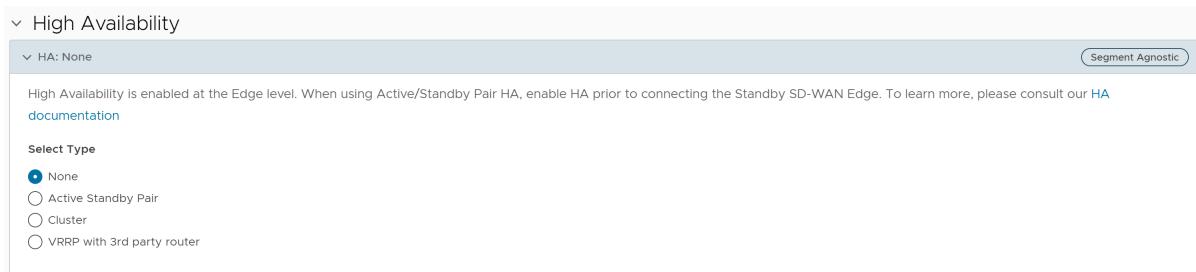
- You cannot select an Edge Interface if you have already configured a local IP address in the **Local IP** field.
- You cannot configure a local IP address if you have selected an Edge Interface in the **Source Interface** drop-down list.

- 6 Click **Save Changes** in the **Device** screen to save the modified configuration.

## Configure High Availability Settings for Edges

To configure High Availability (HA) settings for a specific Edge:

- 1 In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge you want to configure HA settings or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Scroll down to the **High Availability** section and click and expand **HA**.

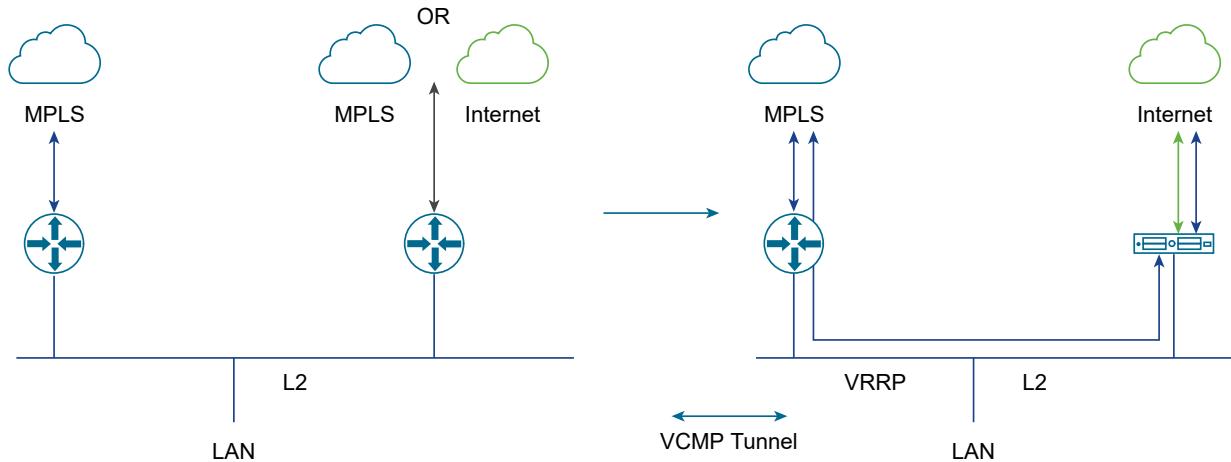


- 4 From the **Select Type** options, select any of the following:
  - None - Deactivates HA site and makes it work as a Standalone site with a single Edge. See [Deactivate High Availability \(HA\)](#).
  - Active Standby Pair - Activates HA on a pair of Edges to ensure redundancy. See [Activate High Availability](#).
  - Cluster - Activates HA on the selected Edge cluster. You can either select a cluster from the drop-down menu to activate HA or click **+ New Cluster** to create a new cluster. See [Configure Clusters and Hubs](#).
  - VRRP with 3rd Party router - Configures a Virtual Router Redundancy Protocol (VRRP) on an Edge to activate next-hop redundancy in the Orchestrator network by peering with third-party CE router. See [Configure VRRP Settings](#).
- 5 Click **Save Changes**.

## Configure VRRP Settings

You can configure Virtual Router Redundancy Protocol (VRRP) on an Edge to enable next-hop redundancy in the SASE Orchestrator network by peering with third-party CE router. You can configure an Edge to be a primary VRRP device and pair the device with a third-party router.

The following illustration shows a network configured with VRRP:



### Prerequisites

Consider the following guidelines before configuring VRRP:

- You can enable VRRP only between the SD-WAN Edge and third party router connected to the same subnet through an L2 switch.
- You can add only one SD-WAN Edge to the VRRP HA group in a branch.
- You cannot enable both Active-Standby HA and VRRP HA at the same time.
- VRRP is supported on primary routed port, sub-interface, and VLAN interfaces.
- SD-WAN Edge must be configured as the primary VRRP device, by setting higher priority, in order to steer the traffic through SD-WAN.
- If the SD-WAN Edge is configured as the DHCP server, then virtual IP addresses are set as the default Gateway address for the clients. When you use a separate DHCP server relay for the LAN, then the admin must configure the VRRP virtual IP address as the default Gateway address.
- When DHCP server is enabled in both the SD-WAN Edge and third-party router, then split the DHCP pool between the Edge and third party router, to avoid the overlapping of IP addresses.
- VRRP is not supported on an interface enabled with WAN Overlay, that is on the WAN link. If you want to use the same link for LAN, then create a sub-interface and configure VRRP on the sub-interface.

- You can configure only one VRRP group in a broadcast domain in a VLAN. You cannot add additional VRRP group for the secondary IP addresses.
- Do not add WI-FI link to the VRRP enabled VLAN. As the link failure would never happen, the SD-WAN Edge always remains as the primary device.

### Procedure

- 1 In the **SD-WAN** Service of Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge you want to configure VRRP settings or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Scroll down to the **High Availability** category, and from the **Select Type** options choose **VRRP with 3rd Party Router**.
- 4 In the **VRRP Settings**, click **+Add** and configure the following:

VRRP Settings						
		Segment Name *		Interface * ⓘ	Virtual IP * ⓘ	Advertise Interval
+ ADD		DELETE		CLONE		Priority * ⓘ
<input type="checkbox"/>	VRID *	Segment Name *	Interface * ⓘ	Virtual IP * ⓘ	Advertise Interval	Priority * ⓘ
<input type="checkbox"/>	5	Global Segment	1 - Corporate	10.0.3.20	5	100
* Required						

Field	Description
VRID	Enter the VRRP group ID. The range is from 1 to 255.
Segment Name	Displays the current Segment selected for Edge configuration.  <b>Note</b> The VRRP settings apply only to the current Segment that is selected.
Interface	Select a physical or VLAN Interface from the list. The VRRP is configured on the selected Interface.
Virtual IP	Enter a virtual IP address to identify the VRRP pair. Ensure that the virtual IP address is not the same as the IP address of the Edge Interface or the third-party router.
Advertise Interval	Enter the time interval with which the primary VRRP device sends VRRP advertisement packets to other members in the VRRP group.

Field	Description
Priority	To configure the Edge as primary VRRP device, enter a value that exceeds the priority value of the third-party router. The default is 100.
Preempt Delay	Select the check box and enter the preempt delay value so that SD-WAN Edge can preempt the third-party router which is currently the primary device, after the specified preempt delay.

5 Click **Save Changes**.

### Results

In a branch network VLAN, if the Edge goes down, then the clients behind the VLAN are redirected through the backup router.

The SD-WAN Edge that acts as a primary VRRP device becomes the default Gateway for the subnet.

If the SD-WAN Edge loses connectivity with all the SD-WAN Edge/Controllers, then the VRRP priority gets reduced to 10 and the SD-WAN Edge withdraws the routes learned from the SD-WAN Edge and routes in the remote Edges as well. This results in the third-party router to become the primary device and take over the traffic.

SD-WAN Edge automatically tracks overlay failure to the SD-WAN Edge. When all the overlay paths to the SD-WAN Edge are lost, the VRRP priority of the SD-WAN Edge is reduced to 10.

When the Edge gets into the VRRP backup mode, the Edge drops any packets that go through the virtual MAC. When the path is UP, the Edge becomes the primary VRRP device again, provided the preemption mode is enabled.

When VRRP is configured on a routed interface, the interface is used for local LAN access and can failover to the backup router.

VRRP is not supported on a routed interface enabled with WAN Overlay. In such cases, a subinterface, sharing the same physical interface, must be configured for local LAN access to support VRRP.

When LAN interface is down, VRRP instance would go to INIT state, and then the SD-WAN Edge sends the route withdrawal request to the SD-WAN Edge/Controller and all the remote SD-WAN Edge remove those routes. This behavior is applicable for the static routes added to the VRRP enabled interface as well.

If the private overlay is present with the SD-WAN Edge peer Hub, then the route is not removed from the Hub, and can cause asymmetric routing. For example, when SD-WAN spoke Edge loses connectivity with public gateway, the third-party router forwards the packets from the LAN to the SD-WAN Hub Edge. The Hub sends the return packets to the SD-WAN spoke Edge instead of the third-party router. As a workaround, enable the **SD-WAN Reachable** functionality, so that the SD-WAN Edge is reachable on private overlay and remains as the primary VRRP device. As the Internet traffic is also steered through the private link over the overlay through the SD-WAN Edge, there might be some limitation on the performance or throughput.

The conditional backhaul option is used to steer the Internet traffic through the Hub. However, in VRRP-enabled SD-WAN Edge, when public overlay goes down the Edge becomes Backup. So the conditional backhaul feature cannot be utilized on a VRRP-enabled Edge.

## Monitor VRRP Events

You can monitor the events related to changes in VRRP status.

In the **SD-WAN** service of Enterprise portal, click **Monitor > Events**.

To view the events related to VRRP, you can use the **Filter** options and select a filter from the drop-down menu to query the VRRP events. Click the **CSV** option to download a report of the Edge VRRP events in CSV format. The following events are available for VRRP:

- VRRP HA updated to primary
- VRRP HA updated out of primary
- VRRP Failed

## Configure Visibility Mode for Edges

This section describes how to configure Visibility mode at the Edge level.

By default, the Visibility mode is inherited by the Edges associated with the Profile. To configure the visibility mode for an Edge:

- 1 In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge that you want to override.
- 3 Scroll down to the **Telemetry** category and go to the **Visibility Mode** area and select the **Override** check box.



- 4 Override the inherited settings and click **Save Changes**.

---

**Note** Changes to Visibility mode are non-disruptive.

---

## Configure Syslog Settings for Edges

In an Enterprise network, SASE Orchestrator supports collection of SASE Orchestrator bound events and firewall logs originating from enterprise SD-WAN Edge to one or more centralized remote syslog collectors (Servers), in native syslog format. At the Edge level, you can override the syslog settings specified in the Profile by selecting the **Enable Edge Override** checkbox.

To override the Syslog settings at the Edge level, perform the following steps.

## Prerequisites

- Ensure that Cloud VPN (branch-to-branch VPN settings) is configured for the SD-WAN Edge (from where the SASE Orchestrator bound events are originating) to establish a path between the SD-WAN Edge and the Syslog collectors. For more information, see [Configure Cloud VPN for Profiles](#).

## Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge that you want to override.  
The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 From the **Segment** drop-down menu, select a profile segment to configure syslog settings. By default, **Global Segment** is selected.
- 4 Scroll down to the **Telemetry** category and go to the **Syslog** area and select the **Override** check box.

IP *	Protocol *	Port *	Source Interface *	Roles *	Syslog Level *	Tag	All Segments
10.0.0.1	TCP	514	LO1	Edge Event	Error	Enter tag (Optional)	<input checked="" type="checkbox"/> Yes
10.0.1.24	TCP	514	Auto	Firewall Event	Info	VMware.SDWN.Edge	<input type="checkbox"/> Yes

- 5 From the **Source Interface** drop-down menu, select one of the Edge interface configured in the segment as the source interface.

**Note** When the Edge transmits the traffic, the packet header will have the IP address of the selected source interface, whereas the packets can be sent through any interface based on the destination route.

- 6 Override the other syslog settings specified in the Profile associated with the Edge by following the Step 4 in [Configure Syslog Settings for Profiles](#).

- 7 Click the **+ ADD** button to add another Syslog collector or else click **Save Changes**. The syslog settings for the edge will be overridden.

**Note** You can configure a maximum of two Syslog collectors per segment and 10 Syslog collectors per Edge. When the number of configured collectors reaches the maximum allowable limit, the **+ button** will be deactivated.

**Note** Based on the selected role, the edge exports the corresponding logs in the specified severity level to the remote syslog collector. If you want the SASE Orchestrator auto-generated local events to be received at the Syslog collector, you must configure Syslog at the SASE Orchestrator level by using the `log.syslog.backend` and `log.syslog.upload` system properties.

To understand the format of a Syslog message for Firewall logs, see [Syslog Message Format for Firewall Logs](#).

#### What to do next

On the **Firewall** page of the Edge configuration, enable the **Syslog Forwarding** button if you want to forward firewall logs originating from enterprise SD-WAN Edge to configured Syslog collectors.

**Note** By default, the **Syslog Forwarding** button is available on the **Firewall** page of the Profile or Edge configuration, and is deactivated.

For more information about Firewall settings at the Edge level, see [Configure Edge Firewall](#).

## Configure Netflow Settings for Edges

As an Enterprise Administrator, at the Edge level, you can override the Netflow settings specified in the Profile by selecting the **Override** check box.

To override the Netflow settings at the Edge level, perform the following steps:

#### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge that you want to override.  
The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 From the **Segment** drop-down menu, select a profile segment to configure Netflow settings. By default, **Global Segment** is selected.

- 4 Scroll down to the **Telemetry** category and go to the **Netflow Settings** area and select the **Override** check box.

- 5 Select the **Activate Netflow** check box.

At the edge level, the **Observation ID** field is auto-populated with 8 bits segment ID and 24 bits edge ID and it cannot be edited. The Observation ID is unique to an Exporting Process per segment per enterprise.

- 6 Override the collector, filter, and Netflow export interval information specified in the Profile by referring to the Step 4 in [Configure Netflow Settings for Profiles](#).
- 7 From the **Source Interface** drop-down menu, select an Edge interface configured in the segment as the source interface, to choose the source IP for the NetFlow packets.

Make sure you manually select the Edge's non-WAN interface (Loopback Interfaces/ VLAN/ Routed/Sub-Interface) with 'Advertise' flag enabled as the source interface. If **none** is selected, the Edge automatically selects a LAN interface, which is 'UP' and 'Advertise' enabled from the corresponding segment as the source interface for that collector. If the Edge doesn't have interfaces which is 'UP' and 'Advertise' enabled, then the source interface will not be chosen and the Netflow packets will not be generated.

---

**Note** When the Edge transmits the traffic, the packet header will have the IP address of the selected source interface, whereas the packets can be sent through any interface based on the destination route.

- 8 Click **Save Changes**.

## Results

After you enable Netflow on the VMware SD-WAN Edge, it periodically sends messages to the configured collector. The contents of these messages are defined using IPFIX templates. For more information on templates, see [IPFIX Templates](#).

# Configure SNMP Settings for Edges

Simple Network Management Protocol (SNMP) is a commonly used protocol for network monitoring, and Management Information Base (MIB) is a database associated with SNMP to manage entities. In the SASE Orchestrator, you can activate SNMP by selecting the desired SNMP version. At the Edge Level, you can override the SNMP settings specified in the Profile.

## Prerequisites

---

**Note** SD-WAN Edges do not generate SNMP traps. If there is a failure at the Edge level, the Edge reports the failure in the form of events to SASE Orchestrator, which in turn generates traps based on the alerts configured for the received events.

---

Follow the below steps to download the SD-WAN Edge MIB:

- In the **SD-WAN** service of the Enterprise portal, go to **Diagnostics > Remote Diagnostics**.
- Click the link to the required Edge, and then go to the **MIBs for Edge** area. Select **VELOCLOUD-EDGE-MIB** from the drop-down menu, and then click **Run**.
- Copy and paste the results onto your local machine.
- Install all MIBs required by VELOCLOUD-EDGE-MIB on the SNMP manager, including SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, IF-MIB, UUID-TC-MIB, and VELOCLOUD-MIB. All these MIBs are available on the **Remote Diagnostics** page.

## Supported MIBs

- SNMP MIB-2 System
- SNMP MIB-2 Interfaces
- VELOCLOUD-EDGE-MIB

**About this task:** At the Edge level, you can override the SNMP settings specified in the Profile, by selecting the **Override** check box. The Edge Override option enables Edge specific edits to the displayed settings, and discontinues further automatic updates from the configuration Profile for this module. For ongoing consistency and ease of updates, it is recommended to set configurations at the Profile level rather than Edge level.

## Procedure to Configure SNMP Settings at Edge Level:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Edges**.

- 2 Select an Edge for which you want to configure the SNMP settings, and then click the **View** link under the **Device** column.
- 3 Scroll down to the **Telemetry** area, and then expand **SNMP**.
- 4 Select the **Override** check box to allow editing.
- 5 You can select either **Enable Version 2c** or **Enable Version 3**, or both SNMP version check boxes.

The screenshot shows the SNMP configuration interface. At the top, there's a header with a back arrow, the title 'SNMP', a checked 'Override' checkbox, and a 'Segment Agnostic' button. Below the header, the 'SNMP Versions' section is expanded, showing a table with one row for 'Port \*' set to '161'. Under the 'Community' section, there are two tables. The first table lists 'Community' entries: 'test' and 'velocloud', both with checked checkboxes. A note at the bottom says '2 \* Required'. The second table lists 'Name \*' entries: 'admin', with a checked checkbox. To the right of this table are columns for 'Enable Authentication', 'Authentication Algorithm', 'Password', 'Enable Privacy', and 'Algorithm'. A note below the second table says '1 item'.

Name *	Enable Authentication	Authentication Algorithm	Password	Enable Privacy	Algorithm
admin	<input type="checkbox"/> Enable Authentication			<input type="checkbox"/> Enable Privacy	

- 6 Select **Enable Version 2c** check box to configure the following fields:

Option	Description
Port	Type the port number in the textbox. The default value is <b>161</b> .
Community	Click <b>Add</b> to add any number of communities. Type a word or sequence of numbers as a password, to allow you to access the SNMP agent. The password may include alphabet A-Z, a-z, numbers 0-9, and special characters (e.g. &, \$, #, %).  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.  You can also delete or clone a selected community.
Allow Any IPs	Select this check box to allow any IP address to access the SNMP agent. To restrict access to the SNMP agent, deselect the check box, and then add the IP address(es) that must have access to the SNMP agent.  You can delete or clone a selected IP address.

- 7 Selecting the **Enable Version 3** check box provides additional security. Click **Add** to configure the following fields:

Option	Description
Name	Type an appropriate username.
Enable Authentication	Select this check box to add extra security to the packet transfer.
Authentication Algorithm	Select an algorithm from the drop-down menu: <ul style="list-style-type: none"> <li>■ MD5</li> <li>■ SHA1</li> <li>■ SHA2</li> </ul> <b>Note</b> This option is available only for the SNMP version 5.8 or above.  <b>Note</b> This field is available only when the <b>Enable Authentication</b> check box is selected.

Option	Description
Password	<p>Type an appropriate password. Ensure that the Privacy Password is same as the Authentication Password configured on the Edge.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>■ This field is available only when the <b>Enable Authentication</b> check box is selected.</li> <li>■ Starting from the 4.5 release, the use of the special character "&lt;" in the password is no longer supported. In cases where users have already used "&lt;" in their passwords in previous releases, they must remove it to save any changes on the page.</li> </ul>
Enable Privacy	<p>Select this check box to encrypt the packet transfer.</p>
Algorithm	<p>Choose a privacy algorithm from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ DES</li> <li>■ AES</li> <li>■ <b>Note</b> Algorithm <b>AES</b> indicates <b>AES-128</b>.</li> </ul> <p><b>Note</b> This field is available only when the <b>Enable Privacy</b> check box is selected.</p>

**Note** You can delete or clone the selected entry.

#### What to do next

Configure **Firewall** settings by following the below steps:

- 1 Navigate to **Configure > Profiles**, and then select a Profile.
- 2 Click the **View** link in the **Firewall** column.
- 3 Go to **Edge Access** located under the **Edge Security** area.
- 4 Configure **SNMP Access** and click **Save Changes**.

**Note** SNMP interface monitoring is supported on DPDK enabled interfaces for 3.3.0 and later releases.

## Security Virtual Network Functions

Virtual Network Functions (VNFs) are individual network services, such as routers and firewalls, running as software-only virtual machine (VM) instances on generic hardware. For example, a routing VNF implements all the functions of a router but runs in a software-only form, alone or along with other VNFs, on generic hardware. VNFs are administered and orchestrated within the NFV architecture.

The virtualization of both NFV and VNF denotes that network functions are implemented in a generalized manner independent of the underlying hardware. VNFs can run in any VM environment in the branch office, cloud, or data center. This architecture allows you to:

- Insert network services in an optimal location to provide appropriate security. For example, insert a VNF firewall in an Internet-connected branch office rather than incur the inefficiency of an MPLS link to hairpin traffic through a distant data center to be firewalled.
- Optimize application performance. Traffic can follow the most direct route between the user and the cloud application using a VNF for security or traffic prioritization. In a VM environment, several VNFs may run simultaneously, isolated from each other, and can be independently changed or upgraded.

The following tables list the third-party firewalls supported by VMware along with the support matrix:

**Table 29-10. Palo Alto Networks Firewall – Support Matrix**

VMware SD-WAN Edge Platform	Edge 520v	Edge 840	Edge 620	Edge 640	Edge 680
Recommended VM Series Firewall Models	VM-50 Lite	VM-100	VM-50 Lite	VM-100	VM-100
Number of vCPUs available for VM-Series Firewall	2	2	2	2	2
Memory available for VNF	4.5 GB	6.5 GB	4.5 GB	6.5 GB	6.5 GB
Storage space available on Edge for VNF	64 GB	120 GB	64 GB	120 GB	120 GB
VMware software version	Release 3.2.0 or later	Release 3.2.0 or later	Release 3.4.3 or later	Release 3.4.3 or later	Release 3.4.3 or later
Panorama version	Release 8.0.5 or later				

**Table 29-11. Check Point Firewall – Support Matrix**

VMware SD-WAN Edge Platform	Edge 520v	Edge 840	Edge 620	Edge 640	Edge 680
Memory available for VNF	2 GB	4 GB	2 GB	4 GB	4 GB
Number of vCPUs available for VNF	2	2	2	2	2
Storage available on Edge for VNF	64 GB	100 GB	120 GB	120 GB	120 GB

**Table 29-11. Check Point Firewall – Support Matrix (continued)**

<b>VMware SD-WAN Edge Platform</b>	<b>Edge 520v</b>	<b>Edge 840</b>	<b>Edge 620</b>	<b>Edge 640</b>	<b>Edge 680</b>
Maximum Throughput of SD-WAN and Checkpoint VNF	100 Mbps	1 Mbps	300 Mbps	600 Mbps	1 Gbps
VMware software version	Release 3.3.2 or later	Release 3.3.2 or later	Release 3.4.3 or later	Release 3.4.3 or later	Release 3.4.3 or later
Checkpoint VNF OS version	Release R77.20 or later				
Checkpoint manager software version	Release 80.30 or later				

**Table 29-12. Fortinet Firewall – Support Matrix**

<b>VMware SD-WAN Edge Platform</b>	<b>Edge 520v</b>	<b>Edge 840</b>	<b>Edge 620</b>	<b>Edge 640</b>	<b>Edge 680</b>
Recommended VM Series Firewall Models	VM00, VM01, VM01v	VM00, VM01, VM01v, VM02, VM02v	VM00, VM01, VM01v	VM00, VM01, VM01v, VM02, VM02v	VM00, VM01, VM01v, VM02, VM02v
Memory available for VNF	2 GB	4 GB	2 GB	4 GB	4 GB
Number of vCPUs available for VNF	2	2	2	2	2
Storage available on Edge for VNF	64 GB	100 GB	64 GB	100 GB	100 GB
Maximum Throughput of SD-WAN and FortiGate VNF	100 Mbps	1 Mbps	300 Mbps	600 Mbps	1 Gbps
VMware software version	Release 3.3.1 or later	Release 3.3.1 or later	Release 4.0.0 or later	Release 4.0.0 or later	Release 4.0.0 or later
FortiOS version	Release 6.0 and 6.2.0 Starting from VMware release 4.0.0, FortiOS version 6.4.0 and 6.2.4 are supported.	Release 6.0 and 6.2.0 Starting from VMware release 4.0.0, FortiOS version 6.4.0 and 6.2.4 are supported.	Release 6.4.0 and 6.2.4	Release 6.4.0 and 6.2.4	Release 6.4.0 and 6.2.4

You can deploy and forward traffic through VNF on an SD-WAN Edge.

## Configure VNF Management Service

VMware supports third-party firewalls that can be used as VNF to pass traffic through Edges.

Choose the third-party firewall and configure the settings accordingly. You may need to configure additional settings in the third-party firewall as well. Refer to the deployment guides of the corresponding third-party firewall for the additional configurations.

For the VNF Types **Check Point Firewall** and **Fortinet Firewall** configure the VNF image by using the System Property `edge.vnf.extraImageInfos`. You must be an Operator user to configure the system property. If you do not have the Operator role access, contact your Operator to configure the VNF Image.

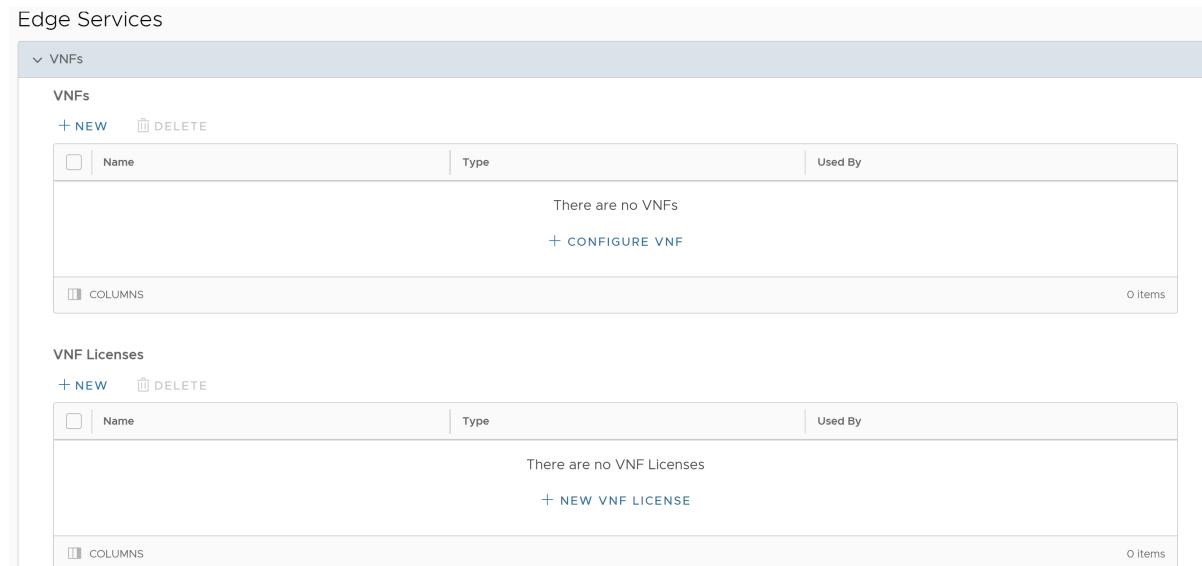
---

**Note** You must provide the correct checksum value in the system property. The Edge computes the checksum of the downloaded VNF image and compares the value with the one available in the system property. The Edge deploys the VNF only when both the checksum values are the same.

---

### Procedure

- In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Network Services**, and then under **Edge Services** area, expand **VNFs**.



The screenshot shows the VMware SD-WAN Enterprise portal interface. On the left, there's a sidebar with 'Edge Services' selected. Under 'Edge Services', 'VNFs' is expanded, showing a table with columns for Name, Type, and Used By. A message says 'There are no VNFs' and there's a '+ CONFIGURE VNF' button. Below the table are 'COLUMNS' and '0 items' buttons. Underneath this section is another for 'VNF Licenses', which also has a table with similar columns, a 'There are no VNF Licenses' message, a '+ NEW VNF LICENSE' button, and 'COLUMNS' and '0 items' buttons.

- To configure a new VNF, click **+ New** or **+ Configure VNF** option.

---

**Note** The **Configure VNF** option appears only when there are no items in the table.

---

- 3 In the **Configure VNF** window, enter a descriptive name for the security VNF service and select a VNF Type from the drop-down menu.

The screenshot shows a 'Configure VNF' dialog box. At the top right is a close button (X). Below it are two input fields: 'Name \*' with a placeholder and 'VNF Type \*' with a dropdown menu. A horizontal scroll bar is visible under the dropdown menu. At the bottom are two buttons: 'CANCEL' (in a blue box) and 'SAVE CHANGES'.

- 4 Configure the required settings based on the selected VNF Type. For more information on configuration settings for VNF types , see [Configure Edge Services](#).
- 5 Click **Save Changes**. The **VNFs** section displays the created VNF services.

#### What to do next

You can configure security VNF for an Edge to direct the traffic through the VNF management services. See:

- [Configure Security VNF without High Availability](#)
- [Configure Security VNF with High Availability](#)

## Configure Security VNF without High Availability

You can deploy and forward traffic through VNF on the SD-WAN Edge, using third-party firewalls.

Only an Operator can activate the Security VNF configuration. If the Security VNF option is not available for you, contact your Operator.

#### Prerequisites

Ensure that you have the following:

- SASE Orchestrator and activated SD-WAN Edge running software versions that support deploying a specific security VNF. For more information on the supported software versions and Edge platforms, refer to the Support Matrix in [Security Virtual Network Functions](#).
- Configured VNF Management service. For more information, see [Configure VNF Management Service](#).

#### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- 2 In the **Edges** page, click either the link to an Edge you want to configure or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.

- 3 In the **Device** tab, scroll down to the **Security VNF** section and click **+ Configure Security VNF**. The **Configure Security VNF** window appears.

Configure Security VNF

Deploy  Enable

VM Configuration

VLAN \* Select

VM-1 IP \*

VM-1 Hostname \*

Deployment State ⓘ

Image Downloaded and Powered On

Image Downloaded and Powered Off

---

Security VNF

Security VNF \* None

+ ADD

To create new VNF, go to Network Services

CANCEL UPDATE

- 4 In the **Configure Security VNF** window, select the **Deploy** check box.
- 5 Under **VM Configuration**, configure the following settings:
- VLAN** – Choose a VLAN, to be used for the VNF management, from the drop-down list.
  - VM-1 IP** – Enter the IP address of the VM and ensure that the IP address is in the subnet range of the chosen VLAN.
  - VM-1 Hostname** – Enter a name for the VM host.
  - Deployment State** – Choose one of the following options:
    - **Image Downloaded and Powered On** – This option powers up the VM after building the firewall VNF on the Edge. The traffic transits the VNF only when this option is chosen, which requires at least one VLAN or routed interface be configured for VNF insertion.
    - **Image Downloaded and Powered Off** – This option keeps the VM powered down after building the firewall VNF on the Edge. Do not select this option if you intend to send traffic through the VNF.

- 6 Under **Security VNF**, Choose a pre-defined VNF management service from the drop-down menu. You can also click **+ Add** to create a new VNF management service. For more information, see [Configure VNF Management Service](#).

- a The following image shows an example of **Fortinet Firewall** as the Security VNF type. If you choose **Fortinet Firewall**, configure the following additional settings:

Configure Security VNF

[View documentation](#)

Deploy  Enable

VM Configuration

VLAN \*

VM-1 IP \*

VM-1 Hostname \*

Deployment State   
 Image Downloaded and Powered On  
 Image Downloaded and Powered Off

---

Security VNF

Security VNF \*  [+ ADD](#)   
 To create new VNF, go to Network Services

VM Cores \*

Inspection Mode   
 proxy  
 flow

Drop your license file or paste your license file's content

Drag & drop a file here

or

```
-----BEGIN FGT VM LICENSE-----
QAAAAMJkk+tOICJbnb7ThoHAQMOXq1AM5CssQxd7hh/d86w/j7FEe1jUXLTw9H2
44LvFMfY9K6nQ1BVikXdd+ZcydXQGQAAP4ijzNLiGfPXNf8ljQrSPjn/w5tZVlk
```

[CANCEL](#) [UPDATE](#)

- **VM Cores** – Select the number of cores from the drop-down list. The VM License is based on the VM cores. Ensure that your VM License is compatible with the number of cores selected.

- **Inspection Mode** – Choose one of the following modes:
  - **Proxy** – This option is selected by default. Proxy-based inspection involves buffering traffic and examining the data as a whole for analysis.
  - **Flow** – Flow-based inspection examines the traffic data as it passes through the FortiGate unit without any buffering.

- **License** – Drag and drop the VM License or paste your license content in the text box.
- b The following image shows an example of **Check Point Firewall** as the Security VNF type.

### Configure Security VNF

[View documentation](#)



Enable

#### VM Configuration

VLAN \* 1 - Corporate

VM-1 IP \* 10.0.1.0

VM-1 Hostname \* cpf1

#### Deployment State ⓘ

- Image Downloaded and Powered On
- Image Downloaded and Powered Off

#### Security VNF

Security VNF \* cpfvnf

+ ADD

To create new VNF, go to Network Services

CANCEL

UPDATE

- c If you choose **Palo Alto Networks Firewall** as Security VNF, configure the following additional settings:

### Configure Security VNF

[View documentation](#)



Enable

#### VM Configuration

VLAN \* 1 - Corporate

VM-1 IP \* 10.0.1.0

VM-1 Hostname \* panvlan1

#### Deployment State ⓘ

- Powered On
- Powered Off

#### Security VNF

Security VNF \* PAN VNF1

+ ADD

To create new VNF, go to Network Services

- **Device Group Name** – Enter the device group name pre-configured on the Panorama Server.
- **Config Template Name** – Enter the configuration template name pre-configured on the Panorama Server.

---

**Note** If you want to remove the deployment of **Palo Alto Networks Firewall** configuration from a VNF type, ensure that you have deactivated the **VNF License of Palo Alto Networks** before removing the configuration.

---

## 7 Click **Update**.

### Results

The configuration details are displayed in the **Security VNF** section.

### What to do next

If you want to redirect multiple traffic segments to the VNF, define mapping between Segments and service VLANs. See [Define Mapping Segments with Service VLANs](#)

You can insert the security VNF into both the VLAN as well as routed interface to redirect the traffic from the VLAN or the routed interface to the VNF. See [Configure VLAN with VNF Insertion](#).

## Configure Security VNF with High Availability

You can configure security VNF on Edges configured with High Availability to provide redundancy.

You can configure VNF with HA on Edges in the following scenarios:

- In a standalone Edge, enable HA and VNF.
- In Edges configured with HA mode, enable VNF.

The following interfaces are enabled and used between the Edge and VNF instance:

- LAN interface to VNF
- WAN interface to VNF
- Management Interface – VNF communicates with its manager

- VNF Sync Interface – Synchronizes information between VNFs deployed on Active and Standby Edges

The Edges have the HA roles as Active and Standby. The VNFs on each Edge run with Active-Active mode. The Active and Standby Edges learn the state of the VNF through SNMP. The SNMP poll is done periodically for every 1 second by the VNF daemon on the edges.

VNF is used in the Active-Active mode with user traffic forwarded to a VNF only from the associated Edge in Active mode. On the standby VM, where the Edge in the VM is standby, the VNF will have only traffic to the VNF Manager and data sync with the other VNF instance.

The following example shows configuring HA and VNF on a standalone Edge.

#### Prerequisites

Ensure that you have the following:

- SASE Orchestrator and activated SD-WAN Edge running software version 4.0.0 or later. For more information on the supported Edge platforms, refer to the Support Matrix in [Security Virtual Network Functions](#).
- Configured Check Point Firewall VNF Management service. For more information, see [Configure VNF Management Service](#).

---

**Note** VMware supports only **Check Point Firewall VNF** on Edges with HA.

---

#### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- 2 In the **Edges** page, click either the link to an Edge you want to configure or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.

- 3 Scroll down to the **High Availability** section and from the **Select Type** options, choose the **Active Standby Pair**.

High Availability is enabled at the Edge level. When using Active/Standby Pair HA, enable HA prior to connecting the Standby SD-WAN Edge. To learn more, please consult our [HA documentation](#).

**Select Type**

- None
- Active Standby Pair
- Cluster
- VRRP with 3rd party router

**HA Interface** ⓘ GE1 ⓘ

**⚠** The VLAN value configured for the switched access port is reset to the value derived from the associated profile before moving to an HA Interface

Deploy with Unique LAN MAC Address ⓘ  Enable Graceful Switchover (require Graceful Restart in routing protocol)

ⓘ Advanced Settings

- 4 Navigate to the **Security VNF** section and click **+ Configure Security VNF**. The **Configure Security VNF** window appears.

### Configure Security VNF

Deploy  Enable

VM Configuration

VLAN *	Select
VM-1 IP *	_____
VM-1 Hostname *	_____

Deployment State ⓘ

- Image Downloaded and Powered On
- Image Downloaded and Powered Off

---

Security VNF

Security VNF *	None
----------------	------

To create new VNF, go to Network Services **+ ADD**

**CANCEL** **UPDATE**

- 5 In the **Configure Security VNF** window, select the **Deploy** check box.
- 6 Under **VM Configuration**, configure the following settings:
  - a **VLAN** – Choose a VLAN, to be used for the VNF management, from the drop-down list.
  - b **VM-1 IP** – Enter the IP address of the VM and ensure that the IP address is in the subnet range of the chosen VLAN.
  - c **VM-1 Hostname** – Enter a name for the VM host.
  - d **Deployment State** – Choose one of the following options:
    - **Image Downloaded and Powered On** – This option powers up the VM after building the firewall VNF on the Edge. The traffic transits the VNF only when this option is chosen, which requires at least one VLAN or routed interface be configured for VNF insertion.
    - **Image Downloaded and Powered Off** – This option keeps the VM powered down after building the firewall VNF on the Edge. Do not select this option if you intend to send traffic through the VNF.
- 7 Under **Security VNF**, choose a pre-defined **Check Point Firewall** VNF Management service from the drop-down list. You can also click **New VNF Service** to create a new VNF management service. For more information, see [Configure VNF Management Service](#).

Configure Security VNF [View documentation](#)

Deploy  Enable

VM Configuration

VLAN *	1 - Corporate
VM-1 IP *	10.0.1.0
VM-1 Hostname *	cpf1

Deployment State

Image Downloaded and Powered On  
 Image Downloaded and Powered Off

---

Security VNF

Security VNF *	cpfvnf	ADD
----------------	--------	-----

To create new VNF, go to Network Services

CANCEL UPDATE

## 8 Click **Update**.

### Results

The **Security VNF** section displays the configured details for the Check Point Firewall Security VNF.

Wait till the Edge assumes the Active role and then connect the Standby Edge to the same interface of the Active Edge. The Standby Edge receives all the configuration details, including the VNF settings, from the Active Edge. For more information on HA configuration, see [Activate High Availability](#).

When the VNF is down or not responding in the Active Edge, the VNF in the Standby Edge takes over the active role.

---

**Note** When you want to turn off the HA in an Edge configured with VNF, turn off the VNF first and then turn off the HA.

---

### What to do next

If you want to redirect multiple traffic segments to the VNF, define mapping between Segments and service VLANs. See [Define Mapping Segments with Service VLANs](#)

You can insert the security VNF into both the VLAN as well as routed interface to redirect the traffic from the VLAN or the routed interface to the VNF. See [Configure VLAN with VNF Insertion](#).

## Define Mapping Segments with Service VLANs

When you want to redirect multiple traffic segments to the security VNF, define mapping between Segments and service VLANs.

To map the segments with the service VLANs:

### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Segments**. The **Segments** page displays the configured segments.

- 2** Define mapping between the segments and service VLANs by entering an unique Service VLAN ID for each segment.

Segment Name *	Description	Type	Service VLAN	Delegate To Partner	Delegate To Customer	Number of Profiles in Use
Global Segment	Default segment	Regular	1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	3
GUEST	Enter Description	Regular	100	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	3
SEG1	Enter Description	Regular	101	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	3
CDE	cde segment	CDE	102	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	2
PRIVATE	Private segment	Private	103	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	2

- 3** Click **Save Changes**.

## Results

The segment in which the VNF is inserted is assigned with a unique VLAN ID. The Firewall policy on the VNF is defined using these VLAN IDs. The traffic from VLANs and interfaces within these segments is tagged with the VLAN ID allocated for the specified segment.

## What to do next

Insert the security VNF into a service VLAN or routed interface to redirect the traffic from the VLAN or the routed interface to the VNF. See [Configure VLAN with VNF Insertion](#).

## Configure VLAN with VNF Insertion

You can insert the security VNF into both the VLAN as well as routed interface.

### Prerequisites

Ensure that you have created a security VNF and configured the settings. See [Configure Security VNF without High Availability](#) and [Configure Security VNF with High Availability](#).

Map the segments with service VLANs to enable VNF insertion into the VLANs. See [Define Mapping Segments with Service VLANs](#).

### Procedure

- 1** In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.

- 2 In the **Edges** page, click either the link to an Edge you want to configure or click the **View** link in the **Device** column of the Edge. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 In the **Device** tab, under **Connectivity**, expand the **VLAN** section.

	VLAN Override	VLAN	Network	IP Address	Interfaces	DHCP	OSPF
<input type="radio"/>	<span>ⓘ</span> <input checked="" type="checkbox"/> Yes	1 - Corporate	10.0.1.0/24	10.0.1.1	GE1 GE2	<input checked="" type="checkbox"/> Enabled (242)	<input type="checkbox"/> Not Enabled
<input type="radio"/>	<span>ⓘ</span> <input checked="" type="checkbox"/> N/A	100 - VLAN-100	10.100.1.0/24	10.100.1.1	GE2	<input checked="" type="checkbox"/> Enabled (242) <span> ⓘ</span>	<input type="checkbox"/> Not Enabled
<input type="radio"/>	<span>ⓘ</span> <input checked="" type="checkbox"/> N/A	101 - VLAN-101	10.101.1.0/24	10.101.1.1	GE2	<input checked="" type="checkbox"/> Enabled (242) <span> ⓘ</span>	<input type="checkbox"/> Not Enabled

- 4 Select the VLAN to which you want to insert the VNF and click the link under the **VLAN** column.

- 5 In the **Edit VLAN** window, select the **VNF Insertion** check box to insert the VNF into VLAN. This option redirects traffic from a specific VLAN to the VNF.

**Edit VLAN**

General Settings

Segment \* Global Segment ▾  
VLAN Name Corporate  
VLAN ID 1  
Description Enter Description (Optional) Maximum 256 characters

LAN Interfaces LAN1 LAN2 LAN3 LAN4 LAN5 LAN6 LAN7 LAN8

SSID There are no Wi-Fi SSIDs configured on this VLAN

ICMP Echo Response Yes

DNS Proxy Enabled

Radius Authentication Enabled Intra-VLAN traffic will not be filtered on hardware switching platforms (Edge 500, 520, 540, and 610)

---

IPv4 Settings

Assign Overlapping Subnets Yes  
Edge LAN IPv4 Address \* 10.0.2.1  
Cidr Prefix \* 24  
Network 10.0.2.0  
OSPF OSPF is not enabled for the selected segment  
Multicast Multicast is not enabled for the selected segment  
VNF Insertion  Yes  
Advertise Yes  
Fixed IPs + ADD DELETE

	MAC Address	IP Address	Description
<input type="checkbox"/>	00:50:56:a3:4a:91	10.0.2.25	Enter description

1 item

- 6 Click **Done**.

## Results

The **VLAN** section displays the status of the VNF insertion.

	VLAN Override	VLAN	Network	IP Address	Interfaces	DHCP	Segment	IGMP	PIM	VNF Insertion
1 - Corporate	Yes	1 - Corporate	10.0.0.0/24	10.0.0.1	LAN1, LAN2, LAN3, LAN4, LAN5, LAN6, LAN7, LAN8	Enabled (242)	Global Segment			<input checked="" type="checkbox"/> Yes
402 - VLAN-402	N/A	402 - VLAN-402	10.100.2.0/24	10.100.2.1	LAN2	Enabled (242)	segment1			<input checked="" type="checkbox"/> Yes

You can also insert the VNF into Layer 3 interfaces or sub-interfaces. This insertion redirects traffic from the Layer 3 interfaces or subinterfaces to the VNF.

If you choose to use the routed interface, ensure that the trusted source is checked and WAN overlay is turned off on that interface. For more information, see [Configure Interface Settings for Edges](#).

## Monitor VNF for an Edge

You can monitor the status of VNFs and the VMs for an Edge, and also view the VNF network services configured for the Enterprise.

To monitor the status of VNFs and VMs of an Edge:

- In the **SD-WAN** Service of the Enterprise portal, click **Monitor > Edges**. The list of Edges along with the details of configured VNFs appears as shown in the following screenshot.

Name	Status	Secrets Encryption	HA (Mode)	Links	VNF VM Status	VNF Type	Gateways	Last Contact
b1-edge1	Connected			(3)				View May 17, 2023, 8:47:17 PM
b2-edge1-520v	Connected			(2)	Powered On Pending receipt from Edge	Fortinet Security Firewall		View May 17, 2023, 8:47:17 PM
b3-edge1	Connected			(3)				View May 17, 2023, 8:47:19 PM

- With mouse pointer, hover-over the VNF type (for example CheckPoint) in the **VNF** column to view additional details of the VNF type.
- With mouse pointer, hover-over the link in the **VNF VM Status** column to view VNF Virtual Machine Status for the Edge. Clicking the link in the **VNF VM Status** column opens the **VNF Virtual Machine Status** window, where you can view the deployment status for the Edge.

For the VNFs configured on Edge with HA, the **VNF Virtual Machine Status** window consists of an additional column that displays the **Serial Number** of the Edges, as shown in the following screenshot.

## VNF Virtual Machine Status

Edge: b2-edge1-520v

Time	VNF VM Status	CPU %	Memory Used (MB)	Storage Used (GB)	Serial Number
May 17, 2023, 8:57:05 PM	Powered On	0.75	2,048.0	10.0	VC05200087456
May 17, 2023, 8:52:05 PM	Powered On	0.75	2,048.0	10.0	VC05200087456
May 17, 2023, 8:47:05 PM	Powered On	0.75	2,048.0	10.0	VC05200087456
May 17, 2023, 8:42:04 PM	Powered On	0.75	2,048.0	10.0	VC05200087456
May 17, 2023, 8:37:05 PM	Powered On	0.75	2,048.0	10.0	VC05200087456
May 17, 2023, 8:32:05 PM	Powered On	0.75	2,048.0	10.0	VC05200087456
May 17, 2023, 8:27:05 PM	Powered On	0.75	2,048.0	10.0	VC05200087456
May 17, 2023, 8:22:04 PM	Powered On	0.75	2,048.0	10.0	VC05200087456
150 items					

To monitor the status of VNFs and VMs:

- In the **SD-WAN** Service of the Enterprise portal, click **Monitor > Network Services > Edge VNFs**. The list of Edges along with the details of configured VNFs is displayed.

Services	Used By	Edge VM Status
ft Fortinet Security Firewall	1 Edge	Powered On (Insertion Enabled) 1 Edge

Edge Name	Edge VM Status
b2-edge1-520v	Powered On (Insertion Enabled)

## Monitor VNF Events

You can view the events when the VNF VM is deployed, when there is a change in the VNF VM configuration, and when a VNF insertion is enabled in a VLAN.

In the **SD-WAN** Service of the Enterprise portal, click **Monitor > Events**.

To view the events related to VNF, you can use the filter option. Click the drop-down arrow next to the **Search** option and choose to filter either by the Event or by the Message column.

The Event name is displayed as **VNF VM config changed** when there is a change in the configuration. The **Message** column displays the corresponding change as follows:

- VNF deployed

- VNF deleted
- VNF turned off
- VNF error
- VNF is DOWN
- VNF is UP
- VNF power off
- VNF power on

The Event name is displayed as **VNF insertion event** when VNF insertion is turned on or off in a VLAN or routed Interface. The **Message** column displays the corresponding change as follows:

- VNF insertion turned off
- VNF insertion turned on

Event	User	Segment	Edge	Severity	Time	Message
VNF VM config changed			b6-edge1-E840	Info	Jul 19, 2021, 3:28:52 PM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 19, 2021, 3:31:42 PM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 20, 2021, 1:39:27 PM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 20, 2021, 1:42:05 PM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 25, 2021, 2:50:22 AM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 25, 2021, 2:55:55 AM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 25, 2021, 2:57:13 AM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 25, 2021, 3:00:31 AM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 27, 2021, 12:55:33 PM	VNF power on
VNF VM config changed			b6-edge1-E840	Info	Jul 27, 2021, 12:58:15 PM	VNF power on

## Configure VNF Alerts

You can configure to receive alerts and notifications related to the VNF events.

---

**Note** If you are logged in as a user with Customer support privileges, you can view the Alerts and other objects, but cannot configure them.

---

To configure alerts and notifications related to the VNF events:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Service Settings > Alerts & Notifications**. The **Alert Configuration** screen appears.

- 2 Under **Incidents**, click and expand **VNF Configuration** and turn on the toggle button.

- 3 You can configure to send notification for the following VNF events:

- **VNF VM Event** – Receive an alert when there is a change in the Edge VNF virtual machine deployment state.
- **Edge VNF Insertion** – Receive an alert when there is a change in the Edge VNF deployment state.
- **Edge VNF Image Download Event** – Receive an alert when there is a change in the Edge VNF image download state.

- 4 Click **Save Changes**.

In the Orchestrator UI, you can view the alert notifications in the **Monitor > Alerts** page.

## Configure Authentication Settings for Edges

The **Device Authentication Settings** allows you to select a Radius server to authenticate a user.

At the Edge-level, you can choose to override the Authentication Settings configured for the Profile.

- 1 In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**.

- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge for which you want to configure the Authentication settings. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Click to expand the **Authentication** area and select the **Override** check box.

The screenshot shows the VMware SD-WAN Edge Services configuration interface. The top navigation bar has 'Edge Services' expanded. Under 'Authentication', the 'Override' checkbox is checked. Below this, there are two dropdown menus: 'RADIUS Server' set to 'RADSER1' and 'Source Interface' set to '1 - Corporate'. There is also a button labeled '+ NEW RADIUS SERVICE'.

- 4 From the **RADIUS Server** drop-down menu, select the Radius server that you want to use for authentication. Alternatively, you can configure a new authentication service by selecting the **New Radius Service** button.
- 5 From the **Source Interface** drop-down menu, select an Edge interface that is configured for the segment. This interface is the source IP for the Authentication Service.

#### Note

- The default value is **Auto**, which allows the Edge to automatically select the available interfaces on the global segment, in a specific order.
- When the Edge transmits the traffic, the packet header contains the IP address of the selected source interface, whereas the packets can be sent through any interface based on the destination route.

- 6 Click **Save Changes**.

## Configure NTP Settings for Edges

As an Enterprise Administrator, at the Edge level, you can override the Network Time Protocol (NTP) settings specified in the Profile by selecting the **Override** checkbox. By default, at the Edge level, the NTP Servers are deactivated.

To override NTP settings at the Edge-level, perform the following steps.

#### Prerequisites

NTP has the following prerequisites:

- To configure an SD-WAN Edge to act as an NTP Server for its Clients, you must first configure the Edge's own NTP time sources by defining **Private NTP Servers** under **Configure > Profiles**.

The SD-WAN Edge NTP Server configuration has the following limitations:

- NTP Clients can synchronize to LAN/loopback IP address of the SD-WAN Edge as NTP server but cannot synchronize to WAN IP address.

- NTP synchronization from another segment to LAN interface is not supported.

### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, go to **Configure > Edges**.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge for which you want to configure the NTP settings. The configuration options for the selected Edge are displayed in the **Device** tab.
- 3 Click to expand the **NTP** area and select the **Override** check box.

The screenshot shows the NTP configuration page for an Edge. The 'Override' checkbox is checked. The 'Client' section has '1 - Corporate' selected and 'Enable' checked. The 'Server' section has 'Edge as NTP Server' selected and 'Enable' checked. Under 'Authentication', 'MD5' is selected. The 'Servers' section contains three entries: 10.0.1.0, 10.0.2.0, and 10.0.2.0. The 'Keys' section contains one entry: Trusted Key # 123 with Key Value 1213.

- 4 Under **Client**, from the drop-down menu, select one of the Edge interface configured in the segment as the source interface.

**Note** When the Edge transmits the traffic, the packet header will have the IP address of the selected source interface, whereas the packets can be sent through any interface based on the destination route.

- 5 Override the other NTP settings specified in the Profile associated with the Edge by following the Step 3 and 4 in [Configure NTP Settings for Profiles](#).
- 6 Click **Save Changes**. The NTP settings for the Edge will be overridden.

### What to do next

Debugging and troubleshooting are much easier when the timestamps in the log files of all the Edges are synchronized. You can collect NTP diagnostic logs by running the **NTP Dump** remote diagnostic tests on an Edge. For more information about how to run remote diagnostic tests on an Edge, see *VMware SD-WAN Troubleshooting Guide* published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

# Configure TACACS Services for Edges

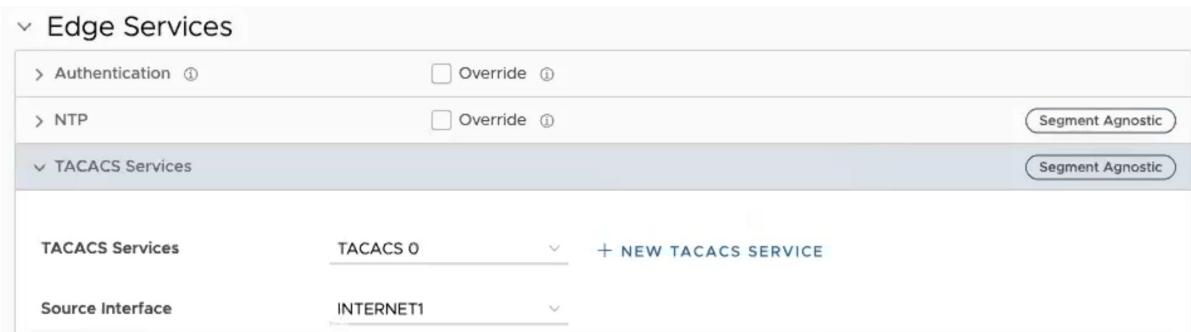
Describes how to configure TACACS Services for Edges.

## Prerequisites

Provision an Edge by following the steps at [Chapter 23 Provision a New Edge](#).

## Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges > Device**.
- 2 Under **Edge Services** expand **TACACS Services**.



- 3 From the **TACACS Services** drop-down menu, select the TACACS service from the available list, that you want to configure for the Edge or click **+New TACACS Service** to configure a new service. For more information, see [Configure TACACS Services](#).
- 4 From the **Source Interface** drop-down menu, select the required source interface.
- 5 Click **Save Changes**.

# SD-WAN Gateway Migration

30

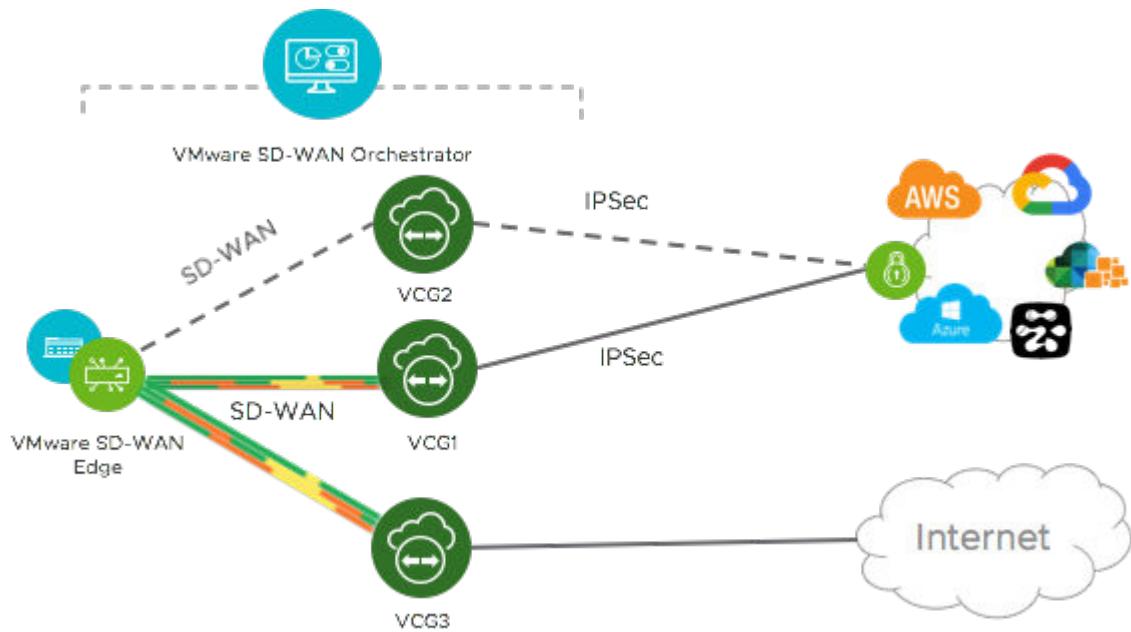
VMware SASE Orchestrator provides a self-service migration functionality that allows you to migrate from your existing Gateway to a new Gateway without your Operator's support.

Gateway migration may be required in the following scenarios:

- Achieve operational efficiency.
- Decommission old Gateways.

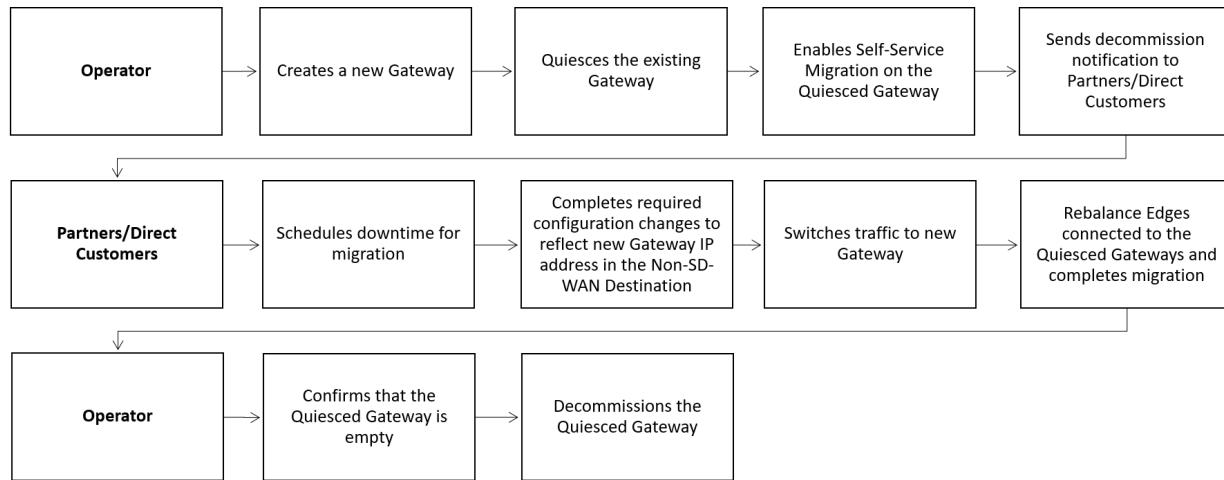
Gateways are configured with specific roles. For example, a Gateway with data plane role is used to forward data plane traffic from source to destination. Similarly, a Gateway with Control Plane role is called a Super Gateway and is assigned to an Enterprise. Edges within the Enterprise are connected to the Super Gateway. Also, there is a Gateway with Secure VPN role that is used to establish an IPSec tunnel to a Non SD-WAN destination (NSD). The migration steps may vary based on the role configured for the Gateway. For more information about the Gateway roles, see the “Configure Gateways” section in the VMware SD-WAN Operator Guide available at [VMware SD-WAN Documentation](#).

The following figure illustrates the migration process of the Secure VPN Gateway:



In this example, an SD-WAN Edge is connected to an NSD through a Secure VPN Gateway, VCG1. The VCG1 Gateway is planned to be decommissioned. Before decommissioning, a new Gateway, VCG2 is created. It is assigned with the same role and attached to the same Gateway pool as VCG1 so that VCG2 can be considered as a replacement to VCG1. The service state of VCG1 is changed to Quiesced. No new tunnels or NSDs can be added to VCG1. However, the existing assignments remain in VCG1. Configuration changes with respect to the IP address of VCG2 are made in the NSD, an IPSec tunnel is established between VCG2 and NSD, and the traffic is switched from VCG1 to VCG2. After confirming that VCG1 is empty, it is decommissioned.

Following is the high-level workflow of Secure VPN Gateway migration based on the User roles:



Read the following topics next:

- [VMware SD-WAN Gateway Migration - Limitations](#)
- [Migrate Quiesced Gateways](#)
- [What to do When Switch Gateway Action Fails](#)

## VMware SD-WAN Gateway Migration - Limitations

Keep in mind the following limitations when you migrate your Gateways:

- Self-service migration is not supported on Partner Gateways.
- There will be a minimum service disruption based on the time taken to switch Non SD-WAN Destinations (NSDs) from the quiesced Gateway to the new Gateway and to rebalance the Edges connected to the quiesced Gateway.
- If the NSD is configured with redundant Gateways and one of the Gateways is quiesced, the redundant Gateway cannot be the replacement Gateway for the quiesced Gateway.

- During self-service migration of a quiesced Gateway, the replacement Gateway must have the same Gateway Authentication mode as the quiesced Gateway.
- For a customer deploying a NSD via Gateway where BGP is configured on the NSD, if the customer migrates the NSD to a different Gateway using the Self-Service Gateway Migration feature on the Orchestrator, the BGP configurations are not migrated and all BGP sessions are dropped post-migration.

In this scenario, the existing Gateway assigned to the NSD is in a quiesced state and requires migration to another Gateway. The customer then navigates to **Service Settings > Gateway Migration** on the Orchestrator and initiates the **Gateway Migration** process to move their NSD to another Gateway. Post-migration, the BGP Local ASN & Router ID information is not populated on the new Gateway and results in NSD BGP sessions not coming up with all routes being lost and traffic using those routes is disrupted until the user manually recreates all BGP settings.

This is a Day 1 issue and while the **Gateway Migration** feature accounts for many critical NSD settings, the NSD's BGP settings that are not accounted for, and their loss post-migration is an expected behavior.

**Workaround:** The migration of a Gateway should be done in a maintenance window only. Prior to the migration, the user should document all BGP settings and be prepared to manually reconfigure these settings post-migration to minimize impact to customer users.

## Migrate Quiesced Gateways

Operators send notification emails about Gateway migration to Administrators with Super User privileges. Plan your migration based on the notification email that you receive from your Operator.

To avoid any service disruption, ensure that you migrate to the new Gateway within the Migration Deadline mentioned in the notification email.

To migrate from a quiesced Gateway to a new Gateway, perform the following steps:

### Prerequisites

Before you migrate the Edges and NSDs (if configured) from the quiesced Gateway to the new Gateway, ensure that you schedule a maintenance window as traffic may be disrupted during migration.

## Procedure

- In the **SD-WAN** service of the Enterprise portal, go to **Service Settings > Gateway Migration**.  
The list of quiesced Gateways appears.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'vmw Orchestrator', 'Customer 5-site-mpg', 'SD-WAN', and user icons. Below the navigation is a menu bar with 'Monitor', 'Configure', 'Diagnostics', and 'Service Settings' (which is underlined). On the left, a sidebar lists 'Alerts & Notifications', 'Edge Licensing', 'Gateway Migration' (selected), 'Edge Management', and 'Edge Auto-activation'. The main content area is titled 'Gateway Migration' and contains a yellow banner with the text 'Action required on this page.' Below the banner, a note states: 'The Gateways listed below are in the Quiesced service state, that is VMware SD-WAN has paused these Gateways for migration. Ensure that you complete the migration from these quiesced Gateways to new Gateways prior to the migration deadline assigned. After the migration of each quiesced Gateway, VMware SD-WAN will decommission the quiesced Gateway.' A table titled 'Quiesced Gateways' shows one entry: 'gateway-1'. To the right of the table are buttons for 'Migration Deadline 4/10/2024', 'Incomplete', 'VIEW EVENTS', and a blue 'START' button.

- Click **Start** for the quiesced Gateway from which you want to migrate to the new Gateway.

**Note** Step 3 and 4 are only applicable if you have the NSDs configured from the quiesced Gateway. If there are no NSDs configured, go to [Step 5](#) to rebalance cloud Gateways and Edges that are connected to the quiesced Gateway.

- 3 Make the required configuration to all the NSDs that are configured through the quiesced Gateway.

The screenshot shows the VMware Orchestrator interface with the 'Customer 3-site' selected. The 'SD-WAN' tab is active. On the left, the navigation menu includes 'Monitor', 'Configure', 'Diagnostics', and 'Service Settings'. Under 'Configure', 'Gateway Migration' is selected. The main pane displays 'gateway-1 (Super / Super Alt Gateway)'. A sub-section titled '1. Configure NSD Site(s)' provides instructions to add the IP address of the SD-WAN Gateway (new Gateway) to each NSD site. It includes a note: 'Do not remove the existing IP address from the configuration until after the Gateways have been switched. Removing the existing IP Address could disrupt the service to the tunnels.' Below this is a table titled 'NSD Sites for the quiesced Gateway' showing one entry: NSD1 with Action 'View IKE IPsec', SD-WAN Gateway 'gateway-2', SD-WAN Gateway IP Address '20.0.2.2', Quiesced Gateway 'gateway-1', and Quiesced Gateway IP Address '20.0.1.2'. There is also a 'REFRESH' button and pagination information 'NSD Sites per page: 10 | 1 - 1 of 1 NSD Sites'. At the bottom of this section is a checkbox 'The listed NSD site(s) have been configured' and a 'NEXT' button. Another sub-section titled '2. Switch Gateways' with the instruction 'For each NSD, switch the traffic from the quiesced Gateway to the new Gateway' is partially visible.

- Click the **View IKE IPsec** link to view a sample configuration for the NSD. Copy the template and customize it to suit your deployment.
- Add the IP address of the SD-WAN Gateway (new Gateway IP) to each NSD configured for the quiesced Gateway.

For example, if you have configured an NSD for AWS, you must add the IP address of the new Gateway in the NSD configuration in the AWS instance.

- After making the configuration changes to all the NSDs, select the **The listed NSD site(s) have been configured** check box, and then click **Next**.

---

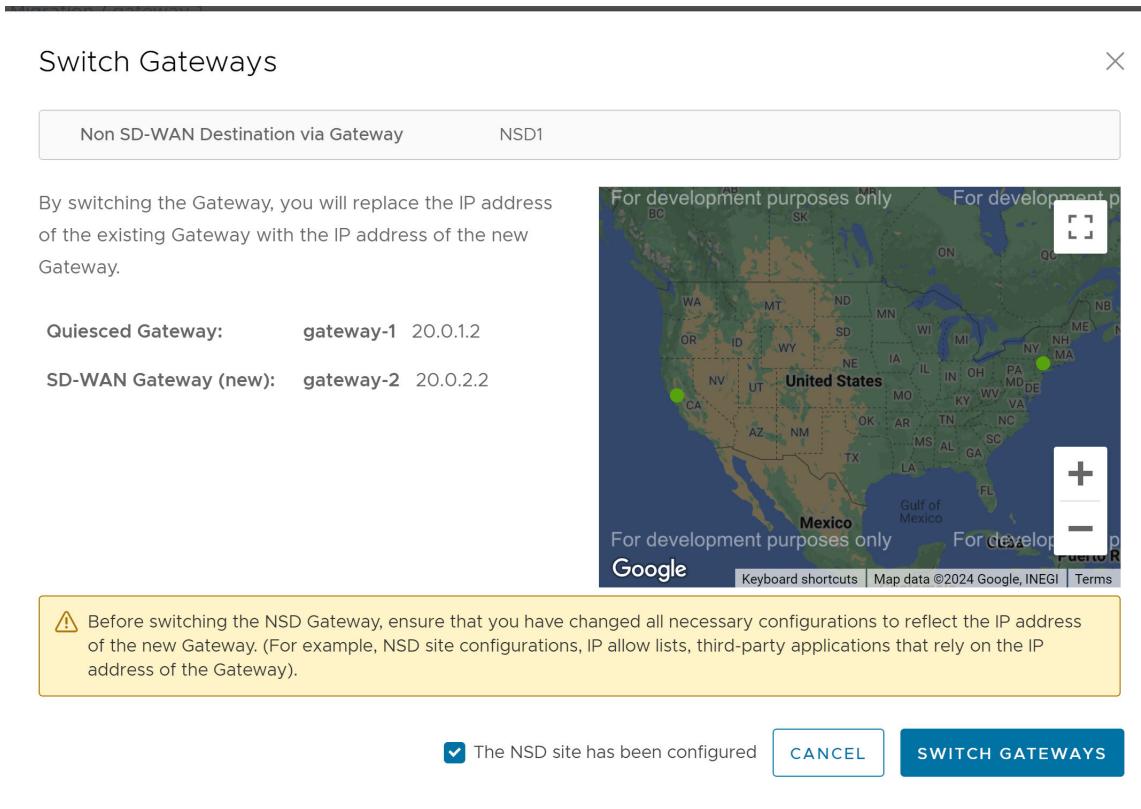
**Note** The Configure NSD Site(s) option is not available for NSDs configured automatically as well as for Gateways with Data Plane role that are not attached to any NSDs.

---

- 4 Select each NSD and click **Switch Gateway** to switch the traffic from the quiesced Gateway to the new Gateway.

The screenshot shows the VMware Orchestrator interface with the 'Customer 3-site' and 'SD-WAN' dropdown menus. The 'Configure' tab is selected. On the left, the 'Gateway Migration' option is highlighted under the 'Edge Management' section. The main pane displays the 'gateway-1' migration progress, specifically the 'Switch Gateways' step. A table lists NSD sites, their current SD-WAN gateway (Primary: 20.0.2.2, gateway-2), and their new Cloud VPN gateway (Primary: 199.168.148.132). The status for all sites is 'Not started'. Navigation buttons 'NEXT' and 'PREVIOUS' are visible at the bottom of the table.

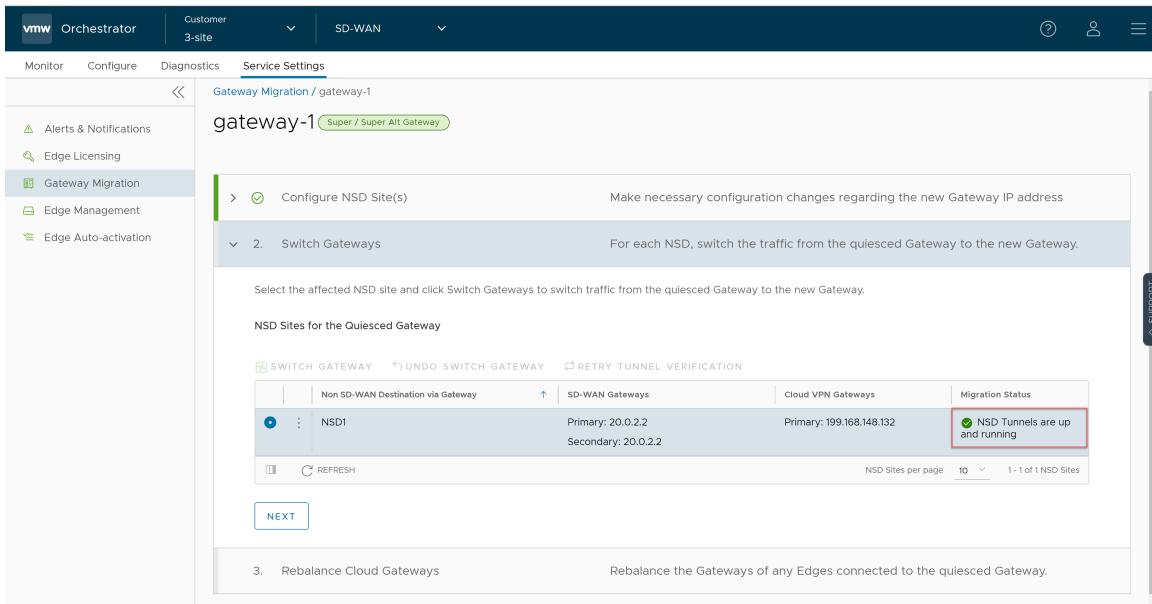
- a In the **Switch Gateway** pop-up window, select the **The NSD site has been configured** check box to confirm that you have made the required changes to the remote-end NSD configuration.



**Note** This confirmation is not applicable for NSDs configured automatically.

b Click **Switch Gateway**.

It may take few minutes to verify the tunnel status. The IP address of the quiesced Gateway is replaced with the IP address of the new Gateway so that the traffic switches to the new Gateway. The **Migration Status** changes to "NSD Tunnels are up and running" as shown in the following screenshot. If the Switch Gateway action fails, see [What to do When Switch Gateway Action Fails](#).

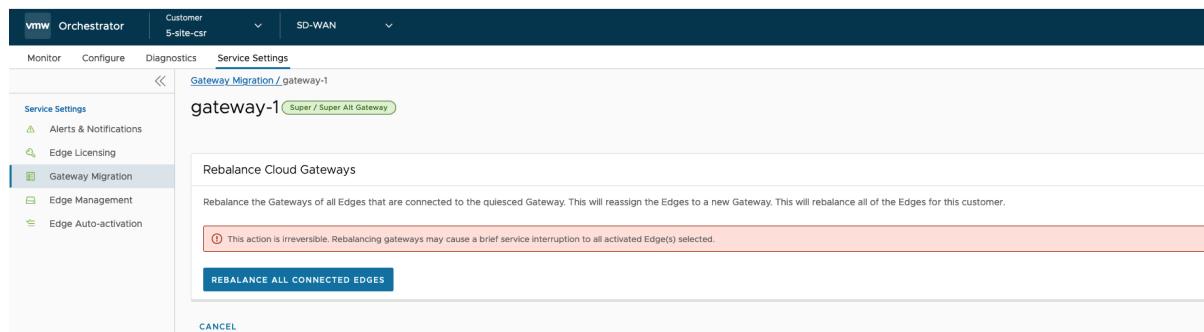


c Click **Next**.

**Note** The Switch Gateway option is not available for Gateways with Data Plane role that are not attached to any NSDs.

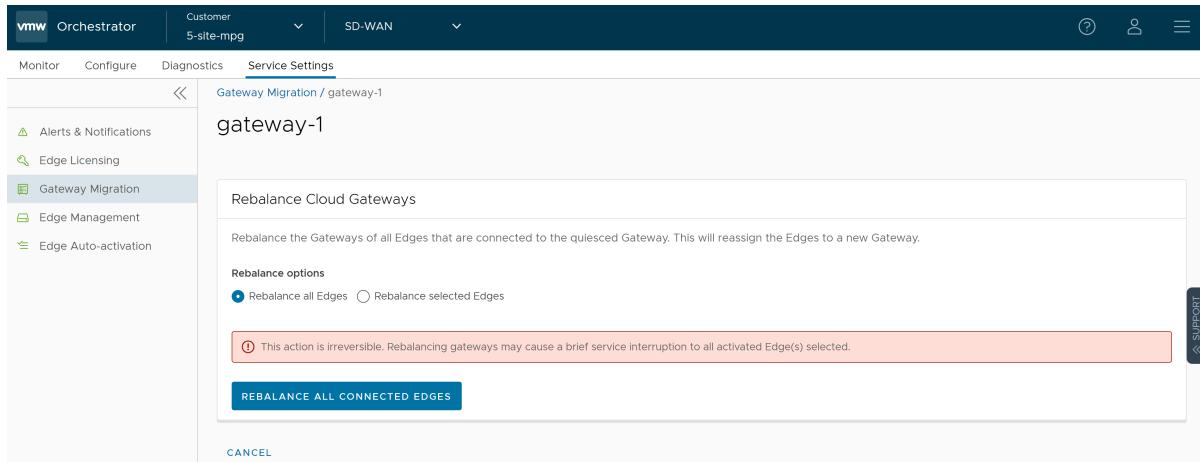
- 5 Rebalance Cloud Gateways (Primary or Secondary or Super Gateways) of all Edges or the required Edges that are connected to the quiesced Gateway so that the Edges get reassigned to the new Gateway. You can rebalance Gateways from the **Configure > Edges** page as well.

**Figure 30-1. Rebalance All Connected Edges - Super Gateway**

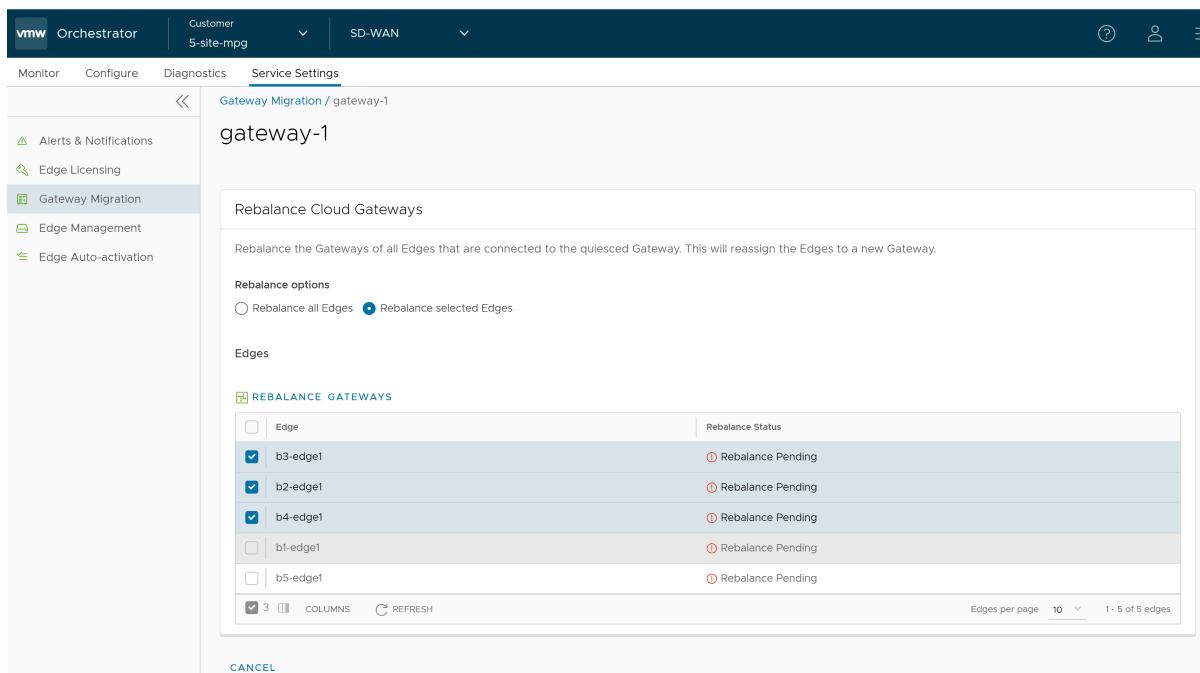


When rebalancing Super Gateways, all the Edges connected to the quiesced Gateway will be rebalanced. Rebalancing of selected Edges is not allowed.

**Figure 30-2. Rebalance All Connected Edges - Primary or Secondary Gateway**



**Figure 30-3. Rebalance Selected Edges - Primary or Secondary Gateway**



Select the Edges that are connected to the quiesced Gateway and click **Rebalance Gateways** to reassign Edges to the new Gateway.

## Rebalance Gateways

X

5 Selected Edge(s) - b5-edge1,b3-edge1,b2-edge1,b4-edge1,b1-edge1

**!** This action is irreversible. Rebalancing gateways may cause a brief service interruption to all activated Edge(s) selected.

CANCEL

REBALANCE GATEWAY

- Click **Rebalance Gateway** to complete the Gateway migration. The Edges connected to the quiesced Gateway are migrated to the new Gateway.

The screenshot shows the VMware Orchestrator interface with the 'Service Settings' tab selected. In the left sidebar, 'Gateway Migration' is highlighted. The main area displays a step-by-step process for rebalancing gateways:

- Configure NSD Site(s): Make necessary configuration changes regarding the new Gateway IP address.
- Switch Gateways: For each NSD, switch the traffic from the quiesced Gateway to the new Gateway.
- Rebalance Cloud Gateways: Rebalance the Gateways of any Edges connected to the quiesced Gateway.

A note below the steps states: "Rebalance the Gateways of all Edges that are connected to the quiesced Gateway. This will reassign the Edges to a new Gateway. This will rebalance all of the Edges for this customer." A green checkmark indicates "Gateways of all edges have been rebalanced".

At the bottom of the dialog, there is a "REBALANCE ALL CONNECTED EDGES" button, a note stating "The Gateways have been switched and it is now safe to remove the quiesced Gateway IP addresses from the configuration.", a checked checkbox for "All Quiesced Gateway IP Addresses have been removed from the original NSD configuration.", and a "FINISH" button.

- Click **Finish**.

## Results

Go to the **Gateway Migration** page and click **Review** to review the migration steps, if required.

The screenshot shows the 'Gateway Migration' page in the VMware Orchestrator interface. The left sidebar has 'Gateway Migration' selected. The main area displays a list of quiesced gateways:

Quiesced Gateways	Migration Deadline	Status	Actions
gateway-1	Migration Deadline 4/10/2024	Completed	VIEW EVENTS   REVIEW

The Gateways that have been migrated remain in this page until the Migration Deadline assigned for the quiesced Gateway. After the Migration Deadline, you can view the history of migration events in the **Monitor > Events** page.

Event	User	Segment	Edge	Severity	Time	Message
Gateway Migration State Changed	super@velocloud.net			Info	Apr 9, 2024, 9:50:58 AM	Gateway Migration - [gateway-1]: Edge(s) state changed from GATEWAY_MIGRATION_REBALANCE_PENDING to GATEWAY_MIGRATION_REBALANCE_COMPLETE

## What to do When Switch Gateway Action Fails

During the Gateway migration, when the Switch Gateway action for an Non SD-WAN Destination (NSD) fails, perform the following steps to troubleshoot the issue:

### Procedure

- In the **SD-WAN** service of the Enterprise portal, go to the **Gateway Migration** page. For instruction to navigate to this page, see [Migrate Quiesced Gateways](#).
- Under the **Switch Gateways** step of the Migration Wizard, select the NSD for which the Switch Gateway action failed, and then click **Retry Tunnel Verification**.

The tunnel status is verified again to see if the **Migration Status** changes to "NSD Tunnels are up and running".

If the **Migration Status** does not change and the Switch Gateway action fails again for the NSD, select the NSD, and then click **Undo Switch Gateway**.

All configuration changes to the NSD are reverted to the original settings.

- Click **Switch Gateway** again to replace the IP address of the quiesced Gateway with that of the new Gateway and thereby switch the traffic to the new Gateway.
- Rebalance the Gateway and complete the migration.

### What to do next

Click **View Events** in the **Gateway Migration** page to view the history of migration events in the **Monitor > Events** page.

# Object Groups

31

An Object Group is a group of Address groups and Service groups. Address groups are a collection of IP addresses, range of IP addresses and domain names. Service groups are a collection of ports, range of ports, service types, and codes. When you create business policies and firewall rules, you can define the rules for a range of IP addresses or a range of TCP/UDP/ICMPv4/ICMPv6 ports, by including the object groups in the rule definitions.

You can create Address groups to save the range of valid IP addresses and Service groups for the range of port numbers or service type and range of codes. You can simplify the policy management by creating object groups of specific types and reusing them in policies and rules.

Using Object Groups, you can:

- Manage policies easily
- Modularize and reuse the policy components
- Update all referenced business and firewall policies easily
- Reduce the number of policies
- Improve the policy debugging and readability

---

**Note** You can create, update, or delete object groups if you have Create, Update, and Delete permissions on the NETWORK\_SERVICE object. You can only view the object groups if you have Read permission on NETWORK\_SERVICE and ENTERPRISE\_PROFILE objects.

---

Read the following topics next:

- [Configure Object Groups](#)
- [Configure Business Policies with Object Group](#)
- [Configure Firewall Rule with Object Group](#)

## Configure Object Groups

This section describes how to configure Object Groups and Service Groups (formerly known as Port Groups).

For more information on Object Groups, see [Chapter 31 Object Groups](#).

In the **SD-WAN** service of the Enterprise portal, to configure Object Groups, click **Configure > Object Groups**.

The **Object Groups** screen appears. You can configure Address Group and Service Group from this screen.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes the VMware logo, 'Orchestrator', 'Customer 5-site' (with a dropdown arrow), 'SD-WAN' (with a dropdown arrow), and tabs for 'Monitor', 'Configure' (which is selected), 'Diagnostics', and 'Service Settings'. A left sidebar under 'Edge Configuration' lists 'Edges', 'Profiles', 'Object Groups' (which is selected and highlighted in grey), 'Segments', 'Overlay Flow Control', and 'Network Services'. The main content area is titled 'Object Groups' and contains tabs for 'Address Groups' (selected) and 'Service Groups'. It features a search bar, a help icon, a filter icon, and a 'CSV' download button. Below these are 'ADD' and 'DELETE' buttons. A table displays a single row with a checkbox, the name 'test\_vleng', and a description column. At the bottom are 'COLUMNS' and 'REFRESH' buttons.

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	test_vleng	

## Address Groups

To create and configure Address Groups, perform the following steps:

- 1 In the **Address Groups** tab, click **Add**. The **Configure Address Group** window appears.

Configure Address Group
X

**Name \***

**Description**

Address Group for Servers

**IP Address Ranges**

	+ ADD	DELETE	
<input type="checkbox"/>	IP Address * ⓘ	Prefix/Mask	Prefix/Mask Value
<input type="checkbox"/>	10.10.1.1	None	▼
<input type="checkbox"/>	10.0.2.0	Cidr Prefix	▼ 24
2 items			

**Domains**

	+ ADD	DELETE
<input type="checkbox"/>	Domain *	
<input type="checkbox"/>	vmware.com	
1 item		

CANCEL
SAVE CHANGES

- 2 Enter a Name and Description for the Address Group.
- 3 Under **IP Address Ranges**, click **+ADD** and enter the range of IPv4 or IPv6 Addresses by selecting the Prefix or Mask options as: **CIDR prefix**, **Subnet mask**, or **Wildcard Mask**, as required.

- 4 Under **Domains**, click **+ADD** and enter the domain names or FQDNs for the Address Group. The domain names defined in the Address Group can be used as a matching criteria for Business policies or Firewall rules.

---

**Note** When configuring domains as match criteria for an **Address Group**, the SD-WAN service first checks for an IP address match. If a match is found, then the service skips domain name matching. However, if no match is found for an IP address, then the service performs a domain name match in the **Address Group**.

---

**Important** The matching criteria may match basic wildcard patterns. For example, if you configure a domain in an **Address Group** as **google.com**, then **mail.google.com** and/or **www.google.com** may also match this criteria. However, if you configure **www.google.com** as the domain in an **Address Group**, then **mail.google.com** will not match this policy.

---

- 5 Click **Save Changes**.

## Service Groups (Formerly known as Port Groups)

To create and configure Service Groups (formerly known as Port Groups), perform the following steps:

- 1 In the **Service Groups** tab, click **Add**. The **Configure Service Group** window appears.

## Configure Service Group

X

**Name \***  
Service Group servers

**Description**

### Service Ranges

+ ADD
DELETE

<input type="checkbox"/>	Protocol *	Port ⓘ	Type	Code ⓘ
<input type="checkbox"/>	TCP ▾	443	N/A	N/A
<input type="checkbox"/>	UDP ▾	2226	N/A	N/A
<input type="checkbox"/>	ICMP ▾	N/A	2	222
<input type="checkbox"/>	ICMPv6 ▾	N/A	3	32

4 items

CANCEL
SAVE CHANGES

- 2 Enter a Name and Description for the Service Group.
- 3 Under **Service Ranges**, click **+ADD** and add Service ranges with the protocol as TCP or UDP or ICMPv4 and ICMPv6, as required.

**Note** For TCP and UDP, you must enter a single port number or port range from 0 through 65535. For ICMP and ICMPv6, you can optionally enter the **Type** and **Code**. The Type and Code value ranges from 0 through 254. The Code can be a single value or range.

- 4 Click **Save Changes**.

You can define a business policy or a firewall rule with the Object Group, to include the range of IP addresses and port numbers. For more information, see:

- [Configure Business Policies with Object Group](#)
- [Configure Firewall Rule with Object Group](#)

Click the link to the Address or Service Group to modify the settings. To delete an Address or Service Group, select the checkbox before the group and click **Delete**.

**Note** Object Groups in use cannot be deleted. If you want to delete an Object Group, it must first be removed from business policies or firewall rules.

## Configure Business Policies with Object Group

While configuring business policies at Profile and Edge level, you can select the existing object groups to match the source or destination. You can define the rules for a range of IPv4 and IPv6 addresses or port numbers available in the object groups.

At the Profile level, to configure a business policy with Object Group, perform the following steps:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.
- 2 Select a Profile to configure a business policy, and click the **Business Policy** tab.  
From the **Profiles** page, you can navigate to the **Business Policy** page directly by clicking the **View** link in the **Biz.Pol** column of the Profile.
- 3 In the **Configure Business Policy** section and under **Business Policy Rules**, click **+ ADD**. The **Add Rule** dialog box appears.

The screenshot shows the 'Add Rule' dialog box. It has a header 'Add Rule' and a close button 'X'. The 'Match' tab is selected. Under 'Match', there are three dropdown menus: 'Source' (set to 'Object Groups'), 'Address Group' (set to 'AddressGP1'), and 'Service Group' (set to 'ServiceGP1'). Under 'Destination', there is a dropdown menu for 'Application' (set to 'Any'). At the bottom right, there are two buttons: 'CANCEL' and 'CREATE'.

- 4 In the **Rule Name** text box, enter a unique name for the Rule.

5 In the **Match** area, configure the match conditions for the rule:

- a Choose the IP version type for the rule. By default, IPv4 and IPv6 address type is selected. You can configure the Source and Destination IP addresses according to the selected Address Type.

Based on the IP version selected, the behavior will be as follows:

- IPv4 Type Rule matches only the IPv4 addresses available in the selected Address Group.
- IPv6 Type Rule matches only the IPv6 addresses available in the selected Address Group.
- Mixed Type Rule matches both the IPv4 and IPv6 addresses in the selected Address Group.

- b From the **Source** drop-down menu, select **Object Groups**.
- c Select the relevant Address Group and Service Group from the drop-down menu. If the selected address group contains any domain names, they would be ignored when matching for the source.

---

**Note** When configuring domains as match criteria for an **Address Group**, the SD-WAN service first checks for an IP address match. If a match is found, then the service skips domain name matching. However, if no match is found for an IP address, then the service performs a domain name match in the **Address Group**.

---

**Important** The matching criteria may match basic wildcard patterns. For example, if you configure a domain in an **Address Group** as **google.com**, then **mail.google.com** and/or **www.google.com** may also match this criteria. However, if you configure **www.google.com** as the domain in an **Address Group**, then **mail.google.com** will not match this policy.

- d If required, you can select the Address and Service Groups for the destination as well.
- e Choose business policy actions as required and click **Create**.

For more information on the match and action parameters, see [Create Business Policy Rule](#).

- f Click **Save Changes**.

## Results

The business policy rules that you create for a profile are automatically applied to all the Edges associated with the profile. If required, you can create additional rules specific to the Edges or modify the inherited rule by navigating to **Configure > Edges**, select an Edge, and click the **Business Policy** tab.

The **Rules From Profile** section displays the rules inherited from profile and they are read only. If you want to override any Profile-level rule, then add a new rule. The added rule appears in the **Edge Overrides** section and it can be manipulated by modifying or deleting, if needed.

**Note** By default, the business policy rules are assigned to the global segment. If required, you can choose a segment from the **Segment** drop-down and create business policy rules specific to the selected segment.

You can modify the object groups with additional IP addresses, port numbers, service types and codes. The changes are automatically included in the business policy rules that use the object groups.

**Note** When an object group is associated with a business policy rule, the ICMP type and code based configuration in service groups will not be applied. Though the Orchestrator allows this type of configuration, the Edge ignores ICMP type and code based configuration when matching business policy.

## Configure Firewall Rule with Object Group

While configuring firewall rules at Profile and Edge level, you can select the existing object groups to match the source or destination. You can define the rules for a range of IP addresses or a range of TCP/UDP/ICMPv4/ICMPv6 ports, by including the object groups in the rule definitions.

At the Profile level, to configure Firewall Rule with Object Group, perform the following steps:

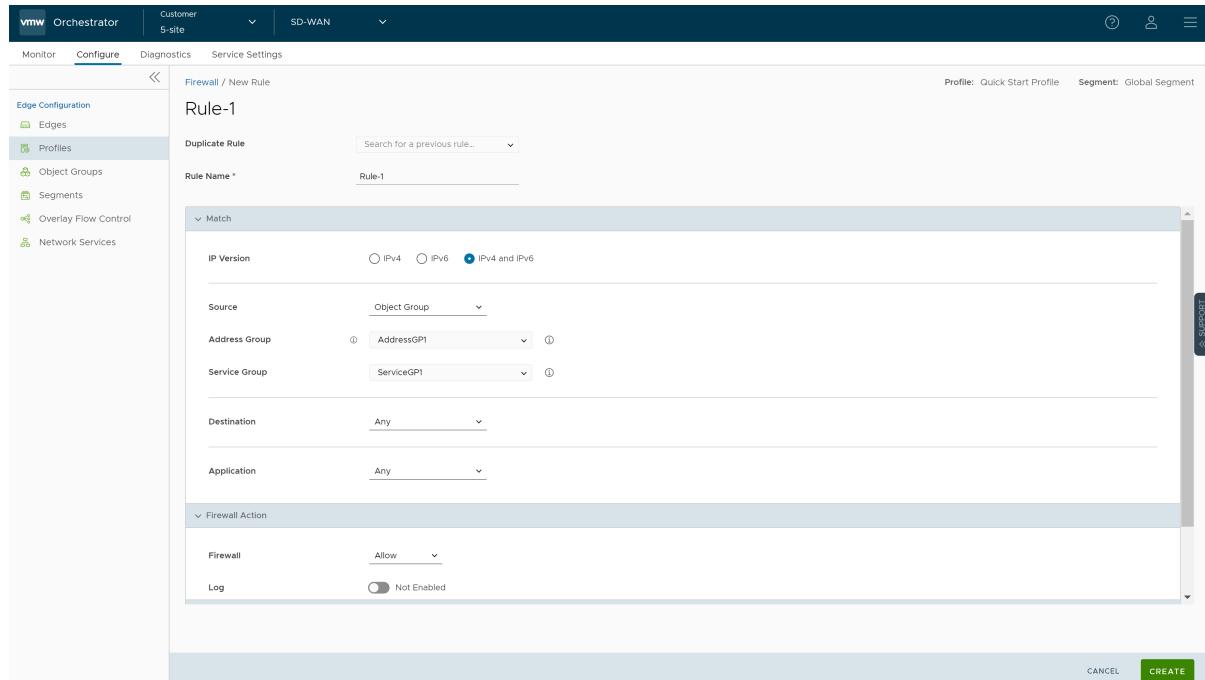
## Procedure

1 In the **SD-WAN** service of the Enterprise portal, go to **Configure > Profiles**. The **Profiles** page displays the existing Profiles.

2 Select a Profile to configure a firewall rule, and click the **Firewall** tab.

From the **Profiles** page, you can navigate to the **Firewall** page directly by clicking the **View** link in the **Firewall** column of the Profile.

3 Go to the **Configure Firewall** section and under **Firewall Rules**, click **+ NEW RULE**. The **Configure Rule** dialog box appears.



4 In the **Rule Name** text box, enter a unique name for the Rule. To create a firewall rule from an existing rule, select the rule to be duplicated from the **Duplicate Rule** drop-down menu.

5 In the **Match** area, configure the match conditions for the rule:

- Choose the IP address type for the rule. By default, IPv4 and IPv6 address type is selected. You can configure the Source and Destination IP addresses according to the selected Address Type.
- From the **Source** drop-down menu, select **Object Groups**.

- c Select the relevant Address Group and Service Group from the drop-down menu. If the selected address group contains any domain names, they would be ignored when matching for the source.

You can click the Info icon next to the Address Group and Service Group drop-down to view the configuration details of the respective Address Group and Service Group.

The screenshot shows the 'Firewall / New Rule' interface with 'Rule-4' selected. The 'Match' section is expanded, showing the following configuration:

- IP Version:** IPv4 and IPv6 (selected)
- Source:** Object Group
- Address Group:** adg1
- Service Group:** sg1
- Destination:** Any
- Application:** Any

A modal window titled 'Address Group 1' is open, displaying the contents of the selected Address Group:

Description	Address Group 1
<b>IP Addresses</b>	
IP Address	Prefix / Mask
55.45.6.7/255.25...	Subnet Mask
10.2.3.4/32	Exact
56.7.8.9/32	Exact
3 items	
<b>Domains</b>	
Domains	
velocloud.net	
1 item	

- d If required, you can select the Address and Service Groups for the destination as well.

Based on Address Type selected, the behavior will be as follows:

- IPv4 Type Rule matches only the IPv4 addresses available in the selected Address Group.
- IPv6 Type Rule matches only the IPv6 addresses available in the selected Address Group.
- Mixed Type Rule matches both the IPv4 and IPv6 addresses in the selected Address Group.

- e Choose Firewall actions as required and click **Create**.

For more information on the match and action parameters, see [Configure Firewall Rule](#).

- f Click **Save Changes**.

A firewall rule is created for the selected Profile, and it appears under the **Firewall Rules** area of the **Profile Firewall** page.

**Note** The rules created at the Profile level cannot be updated at the Edge level.

To override the rule, user needs to create the same rule at the Edge level with new parameters to override the Profile level rule.

In the **Firewall Rules** area of the **Profile Firewall** page, you can perform the following actions:

- **DELETE** - To delete existing Firewall rules, select the checkboxes prior to the rules and click **DELETE**.
- **CLONE** - To duplicate a Firewall rule, select the rule and click **CLONE**.
- **COMMENT HISTORY** - To view all comments added while creating or updating a rule, select the rule and click **COMMENT HISTORY**.
- **Search for Rule** - Allows to search the rule by Rule name, IP address, Port/Port range, and Address group and Service group names.

## Results

The Firewall rules that you create for a profile are automatically applied to all the Edges associated with the profile. If required, you can create additional rules specific to the Edges by navigating to **Configure > Edges**, select an Edge, and click the **Firewall** tab.

Rules	Match	Firewall Action	Enhanced Firewall Services
1 Rule-4	IPv4 and IPv6, Address Group: adg1, Any, Any	Allow, Enabled	Not Enabled, Not Enabled
2 Rule-3	IPv4, Address Group: adg1, IP: 5.6.7.8, Any	Allow, Not Enabled	Not Enabled, Not Enabled
3 Rule-2	IPv6, Interface: GE3, Protocol: TCP, Any	Allow, Not Enabled	Not Enabled, Not Enabled
4 Rule-1	IPv4 and IPv6, MAC: 05:45:67:89:45:56, Service Group: sg1, Any	Allow, Not Enabled	Not Enabled, Not Enabled
5 Rule-0	IPv4 and IPv6, VLAN: 1 - Corporate, Any, Any	Allow, Not Enabled	Not Enabled, Not Enabled

Rules	Match	Firewall Action	Enhanced Firewall Services
6 Rule45	IPv4, Address Group: adg1, IP: 4.5.6.7, Any	Allow, Not Enabled	Not Enabled, Not Enabled
7 Rule-4	IPv4, Ports: 32345, IP: 10.2.3.4, Any	Allow, Not Enabled	Not Enabled, Not Enabled
8 Rule-1	IPv4, Interface: GE6, IP: 10.2.3.5, Any	Allow, Enabled	Enabled, Not Enabled

The **Rules From Profile** section displays the rules inherited from profile and they are read only. If you want to override any Profile-level rule, then add a new rule. The added rule appears in the table above the **Rules From Profile** section and it can be manipulated by modifying or deleting, if needed.

---

**Note** By default, the firewall rules are assigned to the global segment. If required, you can choose a segment from the **Segment** drop-down and create firewall rules specific to the selected segment.

You can modify the object groups with additional IP addresses, port numbers, service types and codes. The changes are automatically included in the Firewall rules that use the object groups.

---

**Note** Before modifying the object groups, you can view the configuration details of the Address Group and Service Group from the same UI screen by clicking the Info icon next to the Address Group and Service name. A pop-up appears displaying the configuration details of the respective Address Group and Service Group.

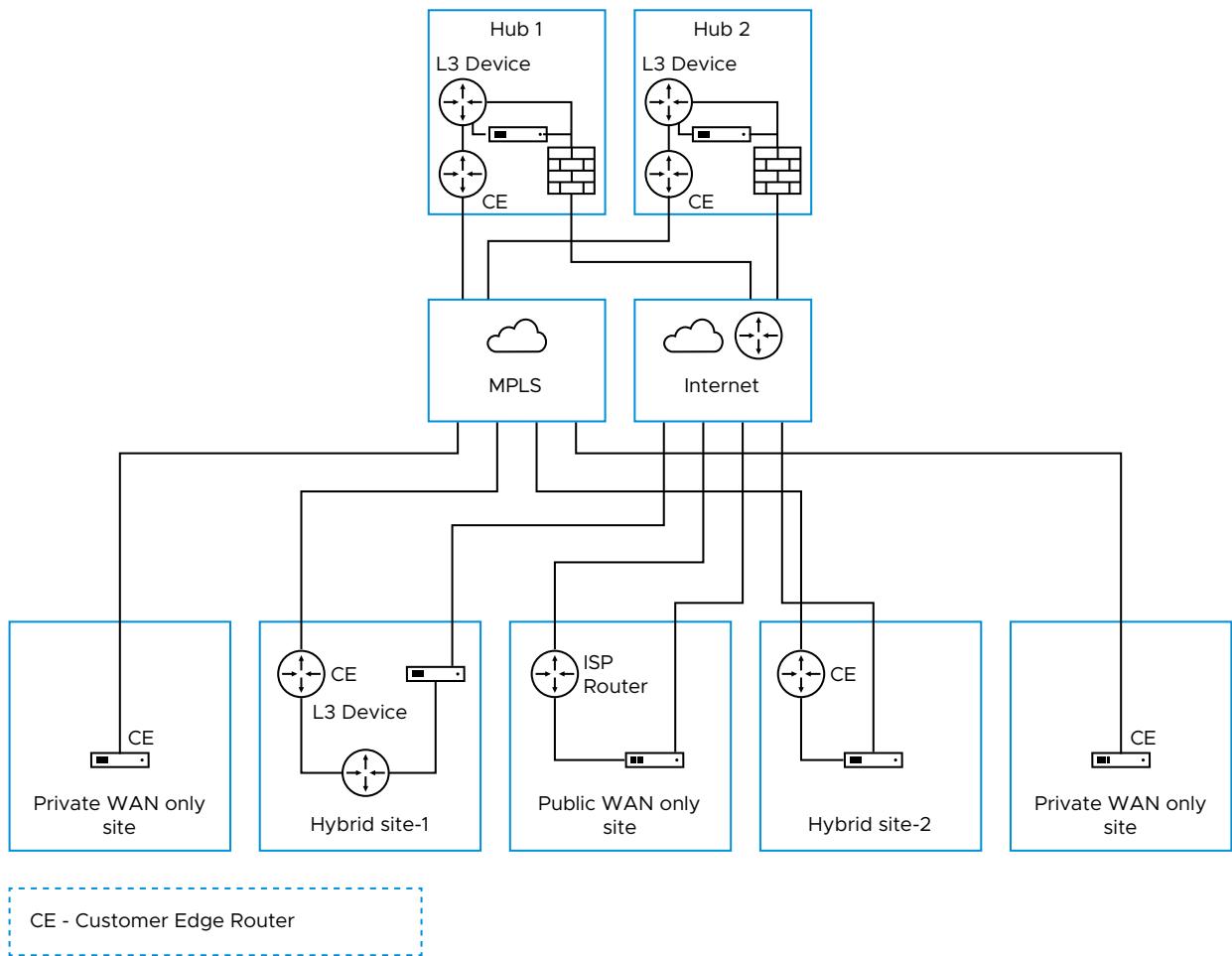
# Site Configurations

32

Topologies for data centers that include an SD-WAN Hub and VMware branch configurations that are configured using both MPLS and Internet connections. Legacy branch configurations (those without a SD-WAN Edge) are included, and hub and branch configurations are modified given the presence of the legacy branches.

The diagram below shows an example topology that includes two data center Hubs and different variations of branch topologies interconnected using MPLS and the Internet. This example will be used to describe the individual tasks required for data center and branch configurations. It is assumed that you are familiar with concepts and configuration details in earlier sections of this documentation. This section will primarily focus on configuring Networks, Profile Device Settings, and Edge configuration required for each topology.

Additional configuration steps for traffic redirection, control routing (such as for backhaul traffic and VPNs), and for Edge failover are also included.



This section primarily focuses on the configuration required for a topology that includes different types of data center and branch locations, and explains the Network, Profile/Edge Device Settings, and Profile/Edge Business Policies required to complete the configurations. Some ancillary configuration steps that may be necessary for a complete configuration – such as for Network Services, Device Wi-Fi Radio, Authentication, SNMP, and Netflow settings – are not described.

Read the following topics next:

- [Data Center Configurations](#)
- [Configure Branch and Hub](#)

## Data Center Configurations

An SD-WAN Edge in a data center can act as a Hub to direct traffic to/from branches. The SD-WAN Edge can be used to manage both MPLS and Internet traffic. The Hub in a data center can be configured in a one-arm or two-arm configuration. In addition, a data center can be used as a backup. Datacenter Edge capacity planning must be thoroughly done to enable the datacenter Hubs to handle the number of tunnels, flows and traffic load from branches. Also, the

Edge model must be selected accordingly. For more information, consult the VMware Support or Solution Architect team.

The following table describes the various designs with different options, about how SD-WAN Edge can be inserted into the topology:

Option	Description
Hub 1	Data Center or regional Hub site with SD-WAN Edge deployed in two-arm topology.
Hub 2	Data Center or regional Hub site with SD-WAN Edge deployed in one-arm topology (same interface carries multiple WAN links).
Private WAN link(s) only Site	Classic MPLS sites.
Hybrid Site-1	SD-WAN Edge is deployed off-path. SD-WAN Edge creates overlay across both MPLS and Internet paths. Traffic is first diverted to the SD-WAN Edge.
Hybrid Site-2	SD-WAN Edge is deployed in-path as the default gateway. It is always the default gateway. This topology is simpler but makes SD-WAN Edge a single point of failure and may require HA.
Public WAN link(s) only Site	Dual-Internet site (one of the links is behind a NAT router).

**Note** These are some common deployment methods used to explain the concept. The Customer topology may not be limited to these methods.

## Configure Branch and Hub

This section provides an overview of configuring SD-WAN Edge in a two-arm configuration.

### Overview

To configure the SD-WAN Edge in a two-arm configuration:

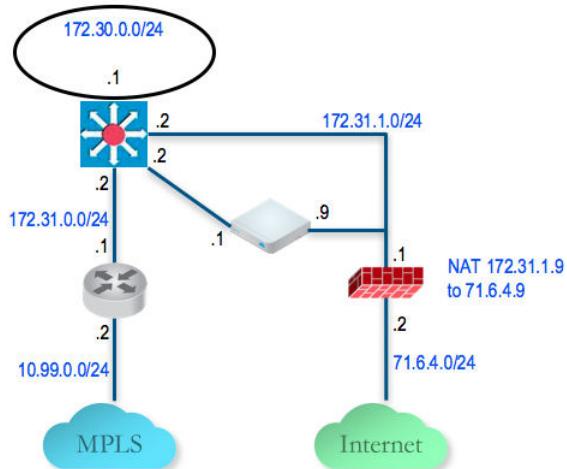
- 1 Configure and activate Hub 1
- 2 Configure and activate the Hybrid Site-1
- 3 Activate branch-to-Hub tunnel (Hybrid Site-1 to Hub 1)
- 4 Configure and activate Public WAN only Site
- 5 Configure and activate Hub 2
- 6 Configure and activate Hybrid Site-2

The following sections describe the steps in more detail.

### Configure and Activate Hub 1

This step helps you understand the typical workflow of how to bring up SD-WAN Edge at the Hub location. SD-WAN Edge is deployed with two interfaces (one interface for each WAN link).

Below is an example of the wiring and IP address information.



## Activate the SD-WAN Edge in Default Profile

- 1 Login to the SASE Orchestrator.
- 2 The default VPN profile allows the activation of the SD-WAN Edge.

## Activate Hub 1 SD-WAN Edge

- 1 Go to **Configure > Edges** and add a new SD-WAN Edge. Specify the correct model and the profile (we use the Branch VPN Profile).
- 2 Go to the Hub SD-WAN Edge (DC1-VCE) and follow the normal activation process. If you already have the email feature set up, an activation email will be sent to that email address. Otherwise, you can go to the device setting page to get the activation URL.
- 3 Copy the activation URL and paste that to the browser on the PC connected to the SD-WAN Edge or just click on the activation URL from the PC browser.
- 4 Click on **Activate** button.
- 5 Now the DC1-VCE data center Hub should be up. Go to **Monitor > Edges**. Click the **Edge Overview** tab. The public WAN link capacity is detected along with the correct public IP **238.162.42.202** and ISP.

Links	Link Status	Interface (WAN Type)	Throughput   Bandwidth	Pre-Notifications	Alerts
Bell Canada ① 238.162.42.202	● Stable	GE4 (Ethernet)	43.002 kbps ↑ 233.011 Mbps 51.983 kbps ↓ 983.442 Mbps	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/>

- 6 Go to **Configure > Edges** and select **DC1-VCE**. Go to the **Device** tab and scroll down to the **Interface Settings**.

You will see that the registration process notifies the SASE Orchestrator of the static WAN IP address and gateway that was configured through the local UI. The configuration on the SASE Orchestrator will be updated accordingly.

- 7 Scroll down to the **WAN Settings** section. The Link Type should be automatically identified as **Public Wired**.

## Configure the Private WAN Link on Hub 1 SD-WAN Edge

- 1 Configure the private MPLS Edge WAN interface directly from the SASE Orchestrator. Go to **Configure -> Edges** and choose **DC1-VCE**. Go to the **Device** tab and scroll down to the **Interface Settings** section. Configure static IP on GE3 as **172.31.2.1/24** and default gateway of **172.31.2.2**. Under **WAN Overlay**, select **User Defined Overlay**. This will allow us to define a WAN link manually in the next step.
- 2 Under **WAN Settings**, click the **Add User Defined WAN Overlay** button (see the following screen capture).
- 3 Define the WAN overlay for the MPLS path. Select the **Link Type as Private** and specify the next-hop IP (172.31.2.2) of the WAN link in the IP Address field. Choose the GE3 as the interface. Click the **Advanced** button.

**Tip:** The Hub site normally has more bandwidth than the branches. If we choose the bandwidth to be auto-discovered, the Hub site will run a bandwidth test with its first peer, e.g. the first branch that comes up, and will end up discovering an incorrect WAN bandwidth. For the Hub site, you should always define the WAN bandwidth manually, and that is done in the advanced settings.

- 4 The private WAN bandwidth is specified in advanced settings. The screen shot below shows an example of 5 Mbps upstream and downstream bandwidth for a symmetric MPLS link at the Hub.
- 5 Validate that the WAN link is configured and save the changes.

You are done with configuring the SD-WAN Edge on the Hub. You will not see the User Defined MPLS overlay that you just added until you activate a branch SD-WAN Edge.

For more information, see:

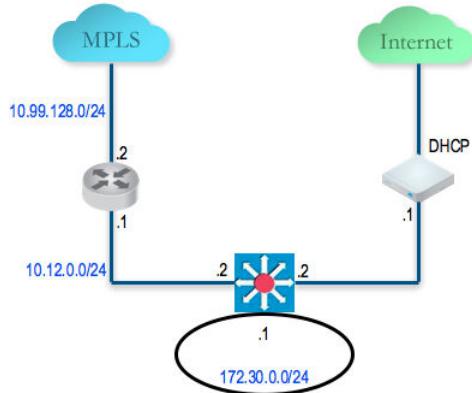
- [Configure Interface Settings for Edges](#)
- [Configure Edge WAN Overlay Settings](#)

## Configure Static Route to LAN Network Behind L3 Switch

Add a static route to the **172.30.0.0/24** subnet through the L3 switch. You need to specify the interface GE3 to use for routing to the next hop. Make sure you select the **Advertise** check box so other SD-WAN Edge can learn about this subnet behind L3 switch. For more information, see [Configure Static Route Settings](#).

## Configure and Activate Hybrid Site-1

This step helps you understand the typical workflow of how to insert the SD-WAN Edge at a Hybrid Site-1. The SD-WAN Edge is inserted off-path and relies on the L3 switch to redirect traffic to it. Below is an example of the wiring and IP address information:



## Configure the Private WAN Link on the Hybrid Site-1 SD-WAN Edge

At this point, we need to build the IP connectivity from the SD-WAN Edge towards the L3 switch.

- 1 Go to **Configure > Edges**, select the **Hybrid Site-1-VCE** and go to the **Device** tab and scroll down to the **Interface Settings** section. Configure static IP on GE3 as **10.12.1.1/24** and default gateway of **10.12.1.2**. Under **WAN Overlay**, select **User Defined Overlay**. This allows to define a WAN link manually.
- 2 Under the **WAN Settings** section, click **Add User Defined WAN Overlay**.

- 3 Define the WAN overlay for the MPLS path. Select the **Link Type** as **Private**. Specify the next-hop IP (10.12.1.2) of the WAN link in the IP Address field. Choose the GE3 as the Interface. Click the **Advanced** button. **Tip:** Since the Hub has already been set up, it is OK to auto-discover the bandwidth. This branch will run a bandwidth test with the Hub to discover its link bandwidth.
- 4 Set the Bandwidth Measurement to **Measure Bandwidth**. This will cause the branch SD-WAN Edge to run a bandwidth test with the Hub SD-WAN Edge just like what happens when it connects to the SD-WAN Gateway.
- 5 Validate that the WAN link is configured and save the changes.

## Configure Static Route to LAN Network Behind L3 Switch

Add a static route to **192.168.128.0/24** through the L3 switch. You need to specify the Interface GE3. Make sure you select the **Advertise** check box so other SD-WAN Edge learn about this subnet behind L3 switch.

## Activate Branch to Hub Tunnel (Hybrid Site-1 to Hub 1)

This step helps you build the overlay tunnel from the branch into Hub. Note that at this point, you may see that the link is up but this is the tunnel to the SD-WAN Gateway over the Internet path and not the tunnel to the Hub. We must activate Cloud VPN to enable the tunnel from the branch to the Hub to be established.

You are now ready to build the tunnel from the branch into the Hub.

## Activate Cloud VPN and Edge to SD-WAN Hub tunnel

- 1 Go to the **Configure > Profiles**, select **Branch VPN Profile** and go to the **Device** tab. Under **VPN Service**, activate the Cloud VPN and perform the following:
  - Under **Branch to Hub Site (Permanent VPN)**, check the **Enable** check box.
  - Under **Branch to Branch VPN (Transit & Dynamic)**, check the **Enable** check box.
  - Under **Branch to Branch VPN (Transit & Dynamic)**, check the **Hubs for VPN** check box. Doing this will deactivate the data plane through the SD-WAN Gateway for Branch to Branch VPN. The Branch to Branch traffic will first go through one of the Hubs (in the ordered list which you will specify next) while the direct Branch to Branch tunnel is being established.

Click the button **Hubs Designation > Edit Hubs**. Next, move the **DC1-VCE** to the right. This will designate the **DC1-VCE** to be a SD-WAN Hub. Click the **DC1-VCE** in the Hubs, and click both **Enable Backhaul Hubs** and **Enable Branch to Branch VPN Hubs** buttons. We will use the same **DC1-VCE** for both Branch to Branch traffic and to Backhaul Internet traffic to the Hub. Under the Cloud VPN section, **DC1-VCE** now shows as both SD-WAN Hubs and used for Branch to Branch VPN Hubs.

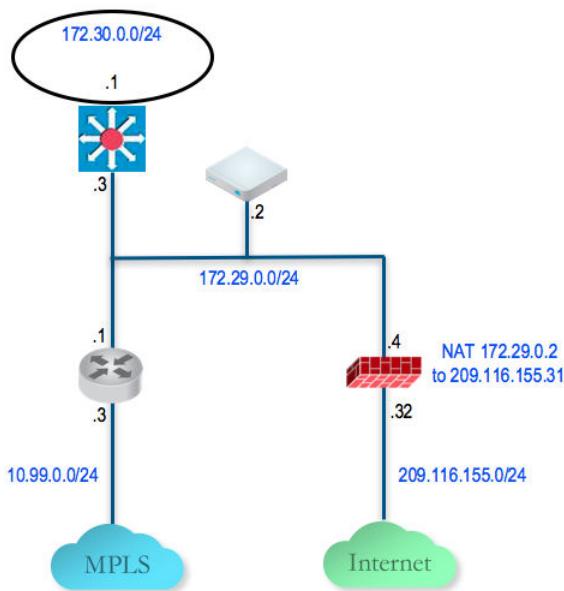
- 2 At this point, the direct tunnel between the branch and the Hub SD-WAN Edge should come up. The debug command now also shows the direct tunnel between the branch and the Hub.

## Configure and Activate Public WAN only Site

This step helps create a Public WAN only Site – a dual Internet site with one DIA and one broadband. Configure the **Public WAN only Site-VCE** SD-WAN Edge LAN and activate the SD-WAN Edge. There is no configuration required on the WAN because it uses DHCP for both WAN interfaces.

## Configure and Activate Hub 2

This step helps you to configure the "Steer by IP address" commonly used in one-arm Hub deployments. Below is an example of the wiring and IP address information. With one-arm deployment, the same tunnel source IP can be used to create overlay over different paths.



## Configure the Hub 2 SD-WAN Edge to Reach the Internet

- 1 Connect a PC to the SD-WAN Edge and use the browser to point to <http://192.168.2.1>.
- 2 Configure the Hub SD-WAN Edge to reach the Internet by configuring the first WAN interface, GE2.

<b>Status</b>	
Link Detected:	Yes
ISP:	Comcast Cable
Speed:	1000 Mbps, full duplex
Autonegotiation:	On
MAC Address:	f0:8e:db:00:03:af
<b>Configuration</b>	
Changes may require the link to briefly go offline.	
<b>IPv4 Settings</b>	
(Fields marked with * are required.)	
* Enabled:	<input checked="" type="checkbox"/>
* Addressing:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static <input type="radio"/> PPPoE
* IP Address:	172.29.0.2
* Subnet Mask:	255.255.255.0
* Gateway:	172.29.0.4
<b>IPv6 Settings</b>	
(Fields marked with * are required.)	
* Enabled:	<input type="checkbox"/>
* Addressing:	<input checked="" type="radio"/> DHCP Stateless <input type="radio"/> DHCP Stateful <input type="radio"/> Static
* IP Address:	
* CIDR Prefix:	0
* Gateway:	
<b>L2 Settings</b>	
(Fields marked with * are required.)	
* Autonegotiation:	<input checked="" type="radio"/> On <input type="radio"/> Off
* EVDSL Modem Attached:	<input type="radio"/> Yes <input type="radio"/> No

## Add the Hub 2 SD-WAN Edge to the SASE Orchestrator and Activate

In this step, you will create the second Hub SD-WAN Edge, called **DC2.VCE**.

- 1 On the SASE Orchestrator, go to **Configure > Edges**, select **New Edge** to add a new SD-WAN Edge.
- 2 Go to **Configure > Edges**, select the SD-WAN Edge that you just created, then go to the **Device** tab to configure the same Interface and IP you configured in previous step.

---

**Important** Since we are deploying the SD-WAN Edge in one-arm mode (same physical interface but there will be multiple over tunnels from this interface), it is important to specify the WAN Overlay to be User Defined.

---

- 3 At this point, you need to create the overlay. Under **WAN Settings**, click **Add User Defined WAN Overlay**.

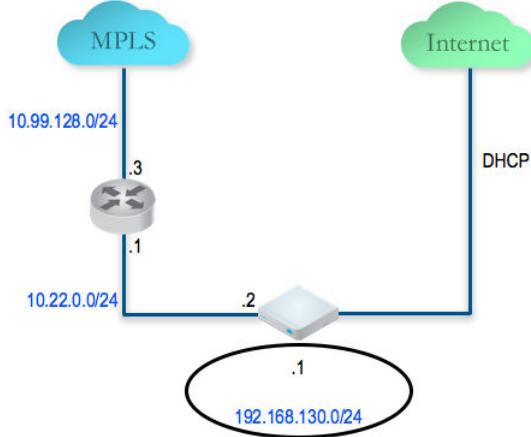
- 4 Create an overlay across the public link. In our example, we will use the next-hop IP of **172.29.0.4** to reach the Internet through the firewall. The firewall is already configured to NAT the traffic to **209.116.155.31**.
- 5 Add the second overlay across the private network. In this example, we specify the next-hop router **172.29.0.1** and also specify the bandwidth since this is the MPLS leg and **DC2-VCE** is a Hub. Add a static route to the LAN side subnet, **172.30.128.0/24** through GE2.
- 6 Activate the SD-WAN Edge. After the activation is successful, come back to the **Device** tab under the edge level configuration. Note the Public IP field is now populated. You should now see the links in the **Monitor > Edges**, under the **Overview** tab.

## Add the Hub 2 SD-WAN Edge to the Hub List in the Branch VPN Profile

- 1 Go to **Configure > Profiles** and select the profile **Quick Start VPN**.
- 2 Go to the **Device** tab and add this new SD-WAN Edge to a list of Hubs.

## Configure and Activate Hybrid Site-2

This step helps you create a Hybrid Site-1 – a hybrid site, which has the SD-WAN Edge behind CE router as well as SD-WAN Edge being the default router for the LAN. Below is an example of the wiring and IP address information for each hardware.



Connect a PC to the SD-WAN Edge LAN or Wi-Fi and use the browser to point to <http://192.168.2.1>.

For more information on activation of Edges, see [Chapter 26 Activate SD-WAN Edges](#).

# Configure Dynamic Routing with OSPF or BGP

33

This section describes how to configure dynamic routing with OSPF or BGP.

SD-WAN Edge learns routes from adjacent routers through OSPF and BGP. It sends the learned routes to the Gateway/Controller. The Gateway/Controller acts like a route reflector and sends the learned routes to other SD-WAN Edge. The Overlay Flow Control (OFC) enables enterprise-wide route visibility and control for ease of programming and for full and partial overlay.

VMware supports Inbound/Outbound filters to OSPF neighbors, OE1/OE2 route types, MD5 authentication. Routes learned through OSPF will be automatically redistributed to the controller hosted in the cloud or on-premise. Support for BGP Inbound/Outbound filters and the filter can be set to Deny, or optionally you can Add/Change the BGP attribute to influence the path selection, i.e. RFC 1998 community, MED, and local preference.

---

**Note** For information about OSPF and BGP Redistribution, see the section titled [OSPF/BGP Redistribution](#).

---

Read the following topics next:

- [Activate OSPF for Profiles](#)
- [Activate OSPF for Edges](#)
- [Configure BGP](#)
- [OSPF/BGP Redistribution](#)
- [BFD Settings](#)
- [Overlay Flow Control](#)

## Activate OSPF for Profiles

Open Shortest Path First (OSPF) can be enabled only on a LAN interface as an active or passive interface. The Edge will only advertise the prefix associated with that LAN switch port. To get full OSPF functionality, you must use it in routed interfaces.

OSPF (Open Shortest Path First) is an interior gateway protocol (IGP) that operates within a single autonomous system (AS).

---

**Note** OSPF is configurable only on the Global Segment.

---

OSPFv3 is introduced in the 5.2 release and provides support for the following:

- Support for OSPFv3 is introduced in the SD-WAN Edge for IPv6 underlay routing in addition to existing BGPv6 support. The following is supported:
  - Underlay IPv6 route learning.
  - Redistribution of OSPFv3 routes into overlay/BGP and vice-versa.
  - Support for Overlay Flow Control (OFC).
- OSPFv3 is implemented with feature parity to OSPFv2 with the following exceptions:
  - Point to Point (P2P) is not supported.
  - BFDv6 with OSPFv3 is not supported.
  - md5 authentication is not available, as OSPFv3 header does not support it.

This section describes how to configure dynamic routing with OSPFv2 and OSPFv3 along with Route Summarization.

---

**Note** OSPFv2 supports only IPv4. OSPFv3 supports only IPv6 and is available starting with the 5.2 release.

---

**Note** Route Summarization is available starting with the 5.2 release.

---

To activate OSPF, perform the steps in the procedure below:

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise Portal, click the **Configure**.

---

**Note** Depending upon your login permissions, you might need to select a Customer or Partner first, then click the **Configure** tab as indicated in next step.

---

- 2 From the left menu, select **Profiles**.

The **Profile** page displays.

- 3 Click a Profile from the list of available Profiles (or Add a Profile if necessary).
- 4 Go to the **Routing & NAT** section in the UI and click the arrow next to OSPF.
- 5 In the **OSPF Areas** section, configure the Redistribution Settings for OSPFv2/v3, BGP Settings, and if applicable, Route Summarization as shown in the image below. See the table below for a description of the options and fields in the below image.

---

**Note** OSPFv2 supports only IPv4. OSPFv3 supports only IPv6 and is only available in the 5.2 release.

---

The screenshot shows the configuration for a Spoke profile. The OSPFv2 tab is selected. Under Redistribution Settings, the Default Route is set to None. The Overlay Prefixes checkbox is unchecked. In the OSPFv2 Areas section, there is a table with columns for Area ID, Name, and Type. The BGP Settings section shows BGP checked, Set Metric set to 20, and Set Metric Type set to E2.

Option	Description
Redistribution Settings	
Default Route	Choose an OSPF route type (O1 or O2) to be used for default route. Default selection for this configuration is "None".
Advertise	Choose either Always or Conditional. (Choosing Always means to Advertise the default route always. Choosing Conditional means to redistribute default route only when Edge learns via overlay or underlay). The "Overlay Prefixes" option must be checked to use the Conditional default route.
Overlay Prefixes	If applicable, check the <b>Overlay Prefixes</b> check box.
BGP Settings	
BGP	To enable injection of BGP routes into OSPF, select the BGP check box. BGP routes can be redistributed into OSPF, so if this is applicable, enter or choose the configuration options as follows:
Set Metric	In the Set Metric text box, enter the metric. (This is the metric that OSPF would put in its external LSAs that it generates from the redistributed routes). The default metric is 20.
Set Metric Type	From the Set Metric Type drop-down menu, choose a metric type. (This is either type E1 or E2 (OSPF External-LSA type)); the default type is E2.

- 6 In **OSPF Areas**, click **+Add** and configure the options, as described in the table below. Add additional areas, if necessary, by clicking **+Add**. The fields in the table below cannot be overridden at the Edge level.

Option	Description
Area ID	Click inside the <b>Area ID</b> text box, enter an OSPF area ID.
Name	Click inside the <b>Name</b> text box, enter a descriptive name for your area.
Type	By default, the Normal type is selected. Only Normal type is supported at this time.

- 7 Next, configure the Interface Settings for OSPF. For configuration details, see either [Configure Interface Settings for Profiles](#) or [Configure Interface Settings for Edges](#).

**Note** OSPF has to be activated at the Profile level first before you can configure it on Edge interfaces.

- 8 If applicable, configure Route Summarization.

**Note** The Route Summarization feature is available starting with the 5.2 release, for an overview and use case for this feature, see [Chapter 34 Route Summarization](#). For configuration details, follow the steps below in Step #10.

- 9 Scroll down to the **Route Summarization** area.
- 10 Click **+Add** in the **Route Summarization** area. A new row is added to the **Route Summarization** area.

Configure route summarization, as described in the table below. See image below.

Route Summarization					
	<b>+ ADD</b>	<b>DELETE</b>	<b>CLONE</b>		
	Subnet *	No Advertise	Tag	Metric Type	Metric
<input type="checkbox"/>	3.5.0.0/16	<input checked="" type="checkbox"/> Yes	1000	E1	20
<input type="checkbox"/>	Enter Subnet	<input type="checkbox"/> Yes	Enter Tag (Optio...)	E1	Enter Metric (Op...

2 items

Option	Description
Subnet	Enter the IP subnet.
No Advertise	When <b>No Advertise</b> is set, all the external routes (Type-5) that are under this supernet are summarized and have chosen not to advertise it. This means it effectively blocks the whole supernet from advertising to its peer.
Tag	Enter the router Tag value (1-4294967295).
Metric Type	Enter the Metric Type (E1 or E2).
Metric	Enter the advertised metric for this route ((0-16777215).

- 11 Add additional routes, if necessary, by clicking **+Add**. To Clone or Delete a route summarization, use the appropriate buttons, located next to **+Add**.
- 12 Click **Save Changes**.

## Route Filters

There are two different types of routing: inbound and outbound.

- Inbound routing includes preferences that can be learned or ignored from OSPF and installed into the Overlay Flow Control.
- Outbound Routing indicates what prefixes can be redistributed into the OSPF.

## Activate OSPF for Edges

Open Shortest Path First (OSPF) can be enabled only on a LAN interface as an active or passive interface. The Edge will only advertise the prefix associated with that LAN switch port. To get full OSPF functionality, you must use it in routed interfaces. After you configure the OSPF settings at the Profile level, all the Edges associated with the Profile will inherit the OSPF configuration from the Profile. However, you cannot override the OSPF configuration settings at the Edge level.

If needed, you can view the OSPF configuration for a specific Edge as follows:

- 1 In the **SD-WAN** service of the Enterprise Portal, click **Configure > Edges**.
- 2 Click the Device Icon next to an Edge, or click the link to an Edge and then click the **Device** tab.
- 3 Go to the **Routing & NAT** section and click the arrow next to OSPF.
- 4 In the **OSPF** section, you can view all the inherited OSPF configuration such as OSPF areas, Redistribution settings for OSPFv2/v3, BGP settings, and Route Summarization.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'vmw Orchestrator', 'Customer 3-site', 'SD-WAN', and tabs for 'Monitor', 'Configure', 'Diagnostics', and 'Service Settings'. The main content area is titled 'b1-edge1' with 'Connected' and 'SD-WAN' status indicators. On the left, a sidebar under 'Edge Configuration' lists 'Edges', 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control', 'Network Services', 'Cloud Hub', and 'Security Service Edge (S...)'. The 'Edges' item is selected. The central panel is divided into sections: 'OSPF' (with 'OSPFv2' selected), 'Redistribution Settings' (Default Route: None), 'OSPFv2 Areas' (Area ID 1, Type: Normal), 'BGP Settings' (BGP: checked, Set Metric: 21, Set Metric Type: E2), and 'Route Summarization' (No Route Summarizations). A 'Segment' dropdown is set to 'GLOBAL SEGMENT'.

## Configure BGP

You can configure the BGP per segment for a Profile or an Edge. Configuring BGP is available for Underlay Neighbors and Non SD-WAN Neighbors.

VMware supports 4-Byte ASN BGP as follows:

- As the ASN of SD-WAN Edges.
- Peer to a neighbor with 4-Byte ASN.
- Accept 4-Byte ASNs in route advertisements.

See the following sections for configuring BGP for Underlay Neighbors and Non SD-WAN Neighbors:

- [Configure BGP from Edge to Underlay Neighbors for Profiles](#)
- [Configure BGP Over IPsec from Edge to Non SD-WAN Neighbors](#)
- [Configure BGP Over IPsec from Gateways](#)

### Configure BGP from Edge to Underlay Neighbors for Profiles

You can configure the BGP per segment at the Profile level as well as at the Edge level. This section provides steps on how to configure BGP with Underlay Neighbors.

#### About this task

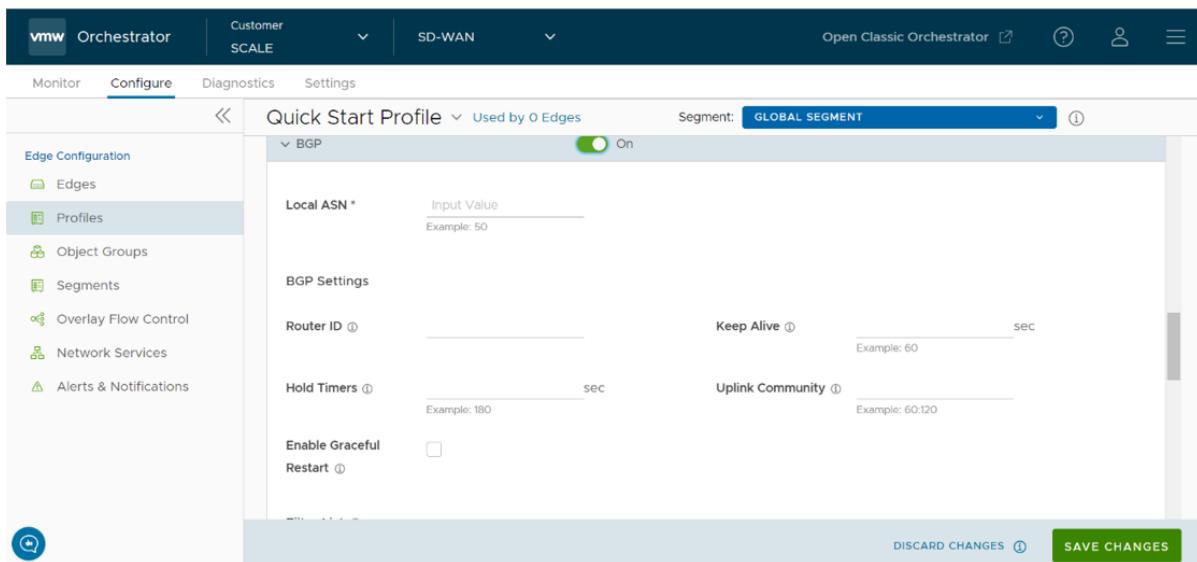
VMware supports 4-Byte ASN BGP. See [Configure BGP](#), for more information.

---

**Note** Route Summarization is new for the 5.2 release. For an overview, use case, and black hole routing details for Route Summarization, see section titled, [Chapter 34 Route Summarization](#). For configuration details, see the steps below.

To configure BGP:

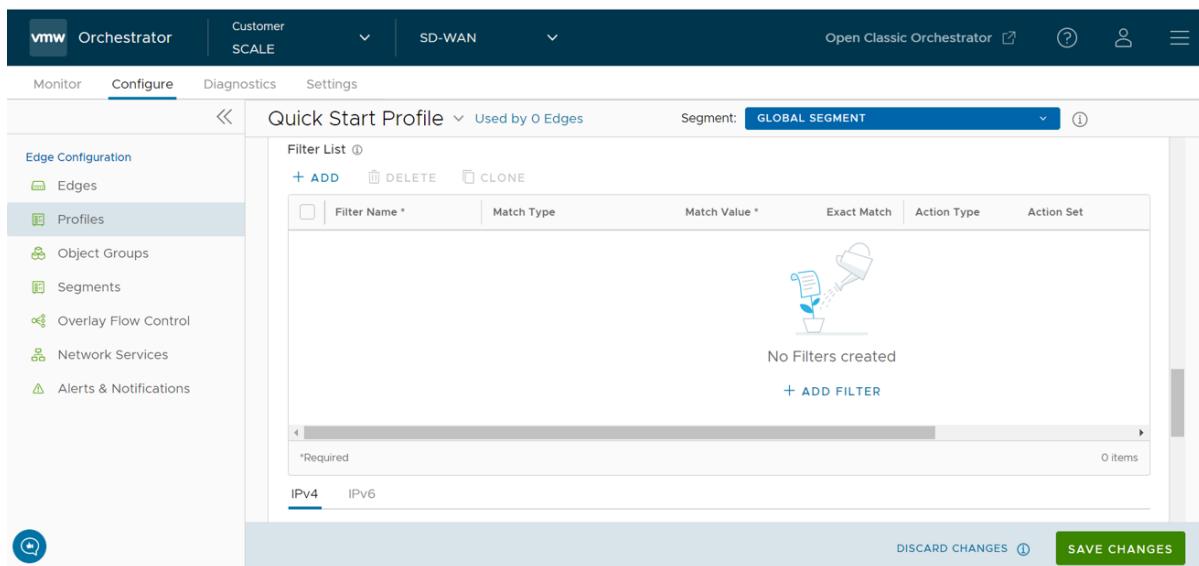
- 1 In the **SD-WAN** service of the Enterprise Portal, click the **Configure** tab.
- 2 From the left menu, select Profiles. The **Profile** page displays.
- 3 Click a Profile from the list of available Profiles (or Add a Profile if necessary).
- 4 Go to the **Routing & NAT** section and click the arrow next to **BGP** to expand.
- 5 In the **BGP** area, toggle the radio button from **Off** to **On**.



- 6 In the **BGP** area, enter the local Autonomous System Number (ASN) number in the appropriate text field.
- 7 Configure the BGP Settings, as described in the table below.

Option	Description
Router ID	Enter the global BGP router ID. If you do not specify any value, the ID is automatically assigned. If you have configured a loopback Interface for the Edge, the IP address of the loopback Interface will be assigned as the router ID.
Keep Alive	Enter the keep alive timer in seconds, which is the duration between the keep alive messages that are sent to the peer. The range is from 0 to 65535 seconds. The default value is 60 seconds.
Hold Timer	Enter the hold timer in seconds. When the keep alive message is not received for the specified time, the peer is considered as down. The range is from 0 to 65535 seconds. The default value is 180 seconds.
Uplink Community	<p>Enter the community string to be treated as uplink routes.</p> <p>Uplink refers to link connected to the Provider Edge(PE). Inbound routes towards the Edge matching the specified community value will be treated as Uplink routes. The Hub/Edge is not considered as the owner for these routes.</p> <p>Enter the value in number format ranging from 1 to 4294967295 or in AA:NN format.</p>
Enable Graceful Restart check box	<p>Please note when selecting this check box:</p> <p>The local router does not support forwarding during the routing plane restart. This feature supports preserving forwarding and routing in case of peer restart.</p>

- 8 Click **+Add** in the **Filter List** area to create one or more filters. These filters are applied to the neighbor to deny or change the attributes of the route. The same filter can be used for multiple neighbors.



- 9 In the appropriate text fields, set the rules for the filter, as described in the table below.

Option	Description
Filter Name	Enter a descriptive name for the BGP filter.
Match Type and Value	Choose the type of the routes to be matched with the filter: <ul style="list-style-type: none"> <li>■ Prefix for IPv4 or IPv6: Choose to match with a prefix for IPv4 or IPv6 address and enter the corresponding prefix IP address in the <b>Value</b> field.</li> <li>■ <b>Community:</b> Choose to match with a community and enter the community string in the <b>Value</b> field.</li> </ul>
Exact Match	The filter action is performed only when the routes match exactly with the specified prefix or community string. By default, this option is enabled.
Action Type	Choose the action to be performed when the routes match with the specified prefix or the community string. You can either permit or deny the traffic.
Action Set	When the BGP routes match the specified criteria, you can set to route the traffic to a network based on the attributes of the path. Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>None:</b> The attributes of the matching routes remain the same.</li> <li>■ <b>Local Preference:</b> The matching traffic is routed to the path with the specified local preference.</li> <li>■ <b>Community:</b> The matching routes are filtered by the specified community string. You can also select the <b>Community Additive</b> check box to enable the additive option, which appends the community value to existing communities.</li> <li>■ <b>Metric:</b> The matching traffic is routed to the path with the specified metric value.</li> </ul>

- 10 Click the plus (+) icon to add more matching rules for the filter. Repeat the procedure to create more BGP filters.

The configured filters are displayed in the **Filter List** area.

**Note** The maximum number of supported BGPv4 Match/Set rules is 512 (256 inbound, 256 outbound). Exceeding 512 total Match/Set rules is not supported and may cause performance issues, resulting in disruptions to the enterprise network.

11 Scroll down to the **Neighbors** area and click **+Add**.

12 Configure the following settings for the IPv4 addressing type, as described in the table below.

Option	Description
Neighbor IP	Enter the IPv4 address of the BGP neighbor
ASN	Enter the ASN of the neighbor
Inbound Filter	Select an Inbound filer from the drop-down list
Outbound Filter	Select an Outbound filer from the drop-down list

Additional Options – Click the view all button to configure the following additional settings:

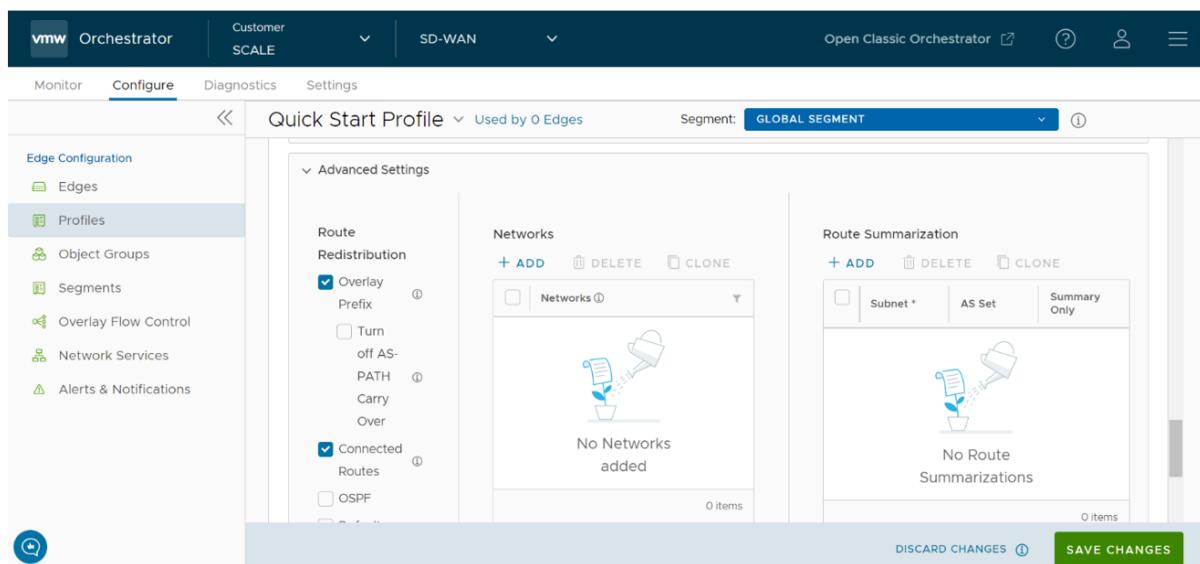
Option	Description
Max-hop	Enter the number of maximum hops to enable multi-hop for the BGP peers. The range is from 1 to 255 and the default value is 1.  <b>Note</b> This field is available only for eBGP neighbors, when the local ASN and the neighboring ASN are different. With iBGP, when both ASNs are the same, multi-hop is inherent by default and this field is not configurable.
Local IP	Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address forth outgoing packets. If you do not enter any value, the IP address of the physical Interface is used as the source IP address.  <b>Note</b> For eBGP, this field is available only when <b>Max- hop</b> count is more than 1. For iBGP, it is always available as iBGP is inherently multi-hop.
Uplink	Used to flag the neighbor type to Uplink. Select this flag option if it is used as the WAN overlay towards MPLS. It will be used as the flag to determine whether the site will become a transit site (e.g. SD-WAN Hub), by propagating routes learnt over a SD-WAN overlay to a WAN link toward MPLS. If you need to make it a transit site, also check "Overlay Prefix Over Uplink" in the Advanced Settings area.

Allow AS	Select the check box to allow the BGP routes to be received and processed even if the Edge detects its own ASN in the AS-Path.
Default Route	The Default Route adds a network statement in the BGP configuration to advertise the default route to the neighbor.
Enable BFD	Enables subscription to existing BFD session for the BGP neighbor.
Keep Alive	Enter the keep alive timer in seconds, which is the duration between the keep alive messages that are sent to the peer. The range is from 0 to 65535 seconds. The default value is 60 seconds.
Hold Timer	Enter the hold timer in seconds. When the keep alive message is not received for the specified time, the peer is considered as down. The range is from 0 to 65535 seconds. The default value is 180 seconds.
Connect	Enter the time interval to try a new TCP connection with the peer if it detects the TCP session is not passive. The default value is 120 seconds.
MD5 Auth	Select the check box to enable BGP MD5 authentication. This option is used in a legacy network or federal network, and it is common that BGP MD5 is used as a security guard for BGP peering.
MD5 Password	<p>Enter a password for MD5 authentication.</p> <p><b>Note</b> Starting from the 4.5 release, the use of the special character "&lt;" in the password is no longer supported. In cases where users have already used "&lt;" in their passwords in previous releases, they must remove it to save any changes on the page.</p>

- 13 Click the Plus (+) icon to add more BGP neighbors.

**Note** Over Multi-hop BGP, the system might learn routes that require recursive lookup. These routes have a next-hop IP which is not in a connected subnet, and do not have a valid exit Interface. In this case, the routes must have the next-hop IP resolved using another route in the routing table that has an exit Interface. When there is traffic for destination that needs these routes to be looked up, routes requiring recursive lookup will get resolved to a connected Next Hop IP address and Interface. Until the recursive resolution happens, the recursive routes point to an intermediate Interface. For more information about Multi-hop BGP Routes, see the "Remote Diagnostic Tests on Edges" section in the *VMware SD-WAN Troubleshooting Guide* published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

- 14 Scroll down to Advanced Settings and click the down arrow to open the Advanced Settings section.



- 15 Configure the following advanced settings, as indicated in the following table, which are globally applied to all the BGP neighbors with IPv4 addresses.

Option	Description
Overlay Prefix	<p>Select the check box to redistribute the prefixes learned from the overlay. For example, when a Spoke is connected to primary and secondary Hub or Hub Cluster, the Spoke's subnets are redistributed by primary and secondary Hub or Hub Cluster to their neighbor with metric (MED) 33 and 34 respectively. You must configure "bgp always-compare-med" in the neighbor router for symmetric routing.</p> <p><b>Note</b> Prior to 5.1, the advertised MED values were starting from eight. From release 5.1 and later, the MED values advertised by HUB starts from 33.</p>
Turn off AS-Path carry over	<p>By default, this should be left unchecked. Select the check box to deactivate AS-PATH Carry Over. In certain topologies, deactivating AS-PATH Carry Over will influence the outbound AS-PATH to make the L3 routers prefer a path towards an Edge or a Hub.</p> <p><b>Warning:</b> When the AS-PATH Carry Over is deactivated, tune your network to avoid routing loops.</p>
Connected Routes	Select the check box to redistribute all the connected Interface subnets.
OSPF	Select the check box to enable OSPF redistribute into BGP.
Set Metric	When you enable OSPF, enter the BGP metric for the redistributed OSPF routes. The default value is 20.
Default Route	<p>Select the check box to redistribute the default route only when Edge learns the BGP routes through overlay or underlay.</p> <p>When you select the <b>Default Route</b> option, the <b>Advertise</b> option is available as <b>Conditional</b>.</p>
Overlay Prefixes over Uplink	Select the check box to propagate routes learned from overlay to the neighbor with uplink flag.
Networks	Enter the network address in IPv4 format that BGP will be advertising to the peers. Click the plus + icon to add more network addresses.

When you enable the **Default Route** option, the BGP routes are advertised based on the Default Route selection globally and per BGP neighbor, as shown in the following table:

Default Route Selection		
Global	Per BGP Neighbor	Advertising Options
Yes	Yes	The per BGP neighbor configuration overrides the global configuration and hence default route is always advertised to the BGP peer.
Yes	No	BGP redistributes the default route to its neighbor only when the Edge learns an explicit default route through the overlay or underlay network.
No	Yes	Default route is always advertised to the BGP peer.
No	No	The default route is not advertised to the BGP peer.

- 16 Click the **IPv6** tab to configure the BGP settings for IPv6 addresses. Enter a valid IPv6 address of the BGP neighbor in the **Neighbor IP** field. The BGP peer for IPv6 supports the following address format:
  - Global unicast address (2001:CAFE:0:2::1)
  - Unique Local address (FD00::1234:BEFF:ACE:EOA4)
- 17 Configure the other settings as required.

**Note** The Local IP address configuration is not available for IPv6 address type.

- 18 Click **Advanced** to configure the following advanced settings, which are globally applied to all the BGP neighbors with IPv6 addresses.

Option	Description
Connected Routes	Select the check box to redistribute all the connected Interface subnets.
Default Route	Select the check box to redistribute the default route only when Edge learns the BGP routes through overlay or underlay. When you select the <b>Default Route</b> option, the <b>Advertise</b> option is available as <b>Conditional</b> .
Networks	Enter the network address in IPv6 format that BGP will be advertising to the peers. Click the Plus (+) icon to add more network addresses.

## Route Summarization

The Route Summarization feature is available in the 5.2 release, for an overview and use case of this functionality, see [Chapter 34 Route Summarization](#). For configuration details, follow the steps below.

- 19 Click **+Add** in the **Route Summarization** area. A new row is added to the Route Summarization area. See image below.

	Subnet *	AS Set	Summary Only
<input type="checkbox"/>	10.0.0...	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable

1 item

DISCARD CHANGES i **SAVE CHANGES**

- 20 Under the **Subnet** column, enter the network range that you want to summarize in the A.B.C.D/M format and the IP subnet.
  - 21 Under the **AS Set** column, click the **Yes** check box if applicable.
  - 22 Under the **Summary Only** column, click the **Yes** check box to allow only the summarized route to be sent.
  - 23 Add additional routes, if necessary, by clicking **+Add**. To Clone or Delete a route summarization, use the appropriate buttons, located next to **+Add**.
- The BGP Settings section displays the BGP configuration settings.
- 24 Click **Save Changes** when complete to save the configuration.

---

**Note** When you configure BGP settings for a profile, the configuration settings are automatically applied to the SD-WAN Edges that are associated with the profile.

---

You can also configure BGP for Non SD-WAN Destination Neighbors in an Edge. For more information, see [Configure BGP Over IPsec from Edge to Non SD-WAN Neighbors](#).

## Configure BGP from Edge to Underlay Neighbors for Edges

You can override the inherited Profile settings at the Edge level when configuring BGP from the Edge to Underlay Neighbors.

If required, you can override the configuration for a specific Edge as follows:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**. The **Edges** page displays the existing Edges.
- 2 Click the link to an Edge or click the **View** link in the **Device** column of the Edge.
- 3 Go to the **Routing & NAT** section and click the arrow next to **BGP** to expand.
- 4 The BGP settings configured for the associated Profile are displayed. If required, you can select the **Override** check box and modify the BGP Settings.
- 5 In addition to the BGP settings configured for a Profile, you can select an Edge Interface configured in the segment as the source Interface for BGP. For the IPv4 address type, you can select only the Loopback Interface as Source Interface and for the IPv6 address type, you can select any Edge Interface as the Source Interface.

This field is available:

- Only when you choose to override the BGP Settings at the Edge level.
- For eBGP, only when **Max-hop** count is more than 1. For iBGP, it is always available as iBGP is inherently multi-hop.

---

### Important

- You cannot select an Edge Interface if you have already configured a local IP address in the **Local IP** field.
  - You cannot configure a local IP address if you have selected an Edge Interface in the **Source Interface** drop-down list.
- 

- 6 Click **Save Changes** in the **Device** screen to save the modified configuration.

## Configure BGP Over IPsec from Edge to Non SD-WAN Neighbors

The Non SD-WAN BGP Neighbors configuration is not applicable at Profile level. You can configure the NSD Neighbors only at the Edge level.

### About this task:

BGP is used to establish the BGP neighborship over the IPSec tunnels to the Non SD-WAN Sites. Direct IPSec tunnels are used for establishing a secure communication between the SD-WAN Edge and the Non SD-WAN Destination (NSD). In previous releases, VMware supported NSD tunnels from the SD-WAN Edge with the ability to add NVS static routes. In the 4.3 release, this functionality is extended to support BGP over IPsec to the NSD endpoint for a route-based VPN.

VMware SD-WAN supports 4-Byte ASN BGP. See [Configure BGP](#), for more information.

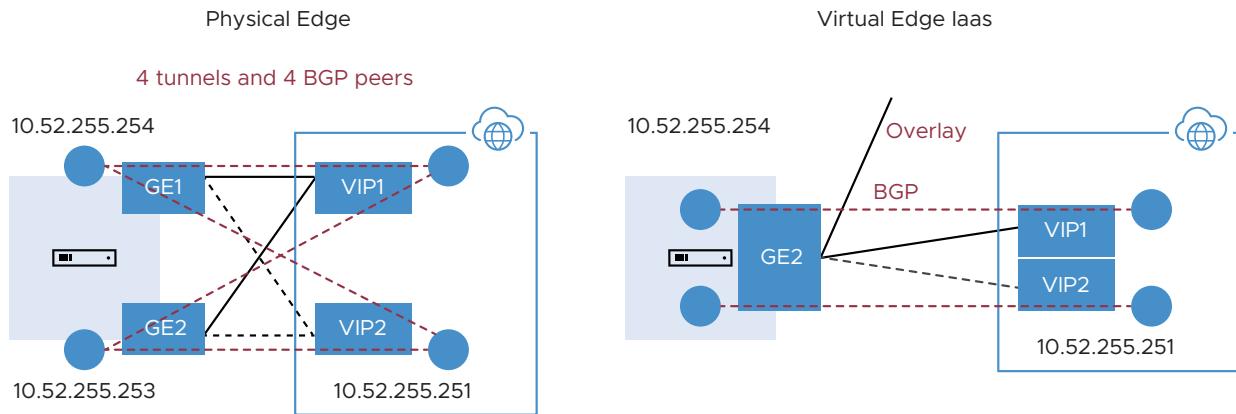
**Note** The Azure vWAN Automation from Edge feature is not compatible with BGP over IPSec. This is because only static routes are supported when automating connectivity from an Edge to an Azure vWAN.

## Use Cases

### Use Case 1: BGP Over IPSec from an Edge to an Azure VPN

Each Azure VPN gateway allocates one set of public Virtual Public IPs (VIP) for a branch Edge to form IPSec tunnels. Similarly, Azure also allocates one internal private subnet and assigns one internal IP per VIP. This internal tunnel-ip (peer tunnel-ip) will be used for creating BGP peering with the Azure Gateway.

Azure has a restriction that the BGP peer IP (Edge's local tunnel-ip) shouldn't be in the same connected subnet or 169.x.x.x subnet, and therefore we need to support multi-hop BGP on the Edge. In BGP terminology, the local tunnel-ip maps to BGP source address and peer tunnel-ip maps to neighbor/peer address. We need to form a mesh of BGP connections - one per NSD tunnel so that the return traffic from the NVS could be load-balanced (flow-based) - design on the Azure Gateway side. In the below diagram for the physical Edge, we have two public WAN links and so four tunnels to an Azure Gateway. Each tunnel is associated with one BGP connection uniquely identified by the local tunnel\_ip and remote peer tunnel\_ip. On the Virtual Edge, the only difference is that we have one public WAN link and a maximum of two tunnels and two BGP sessions to the Azure Gateway.

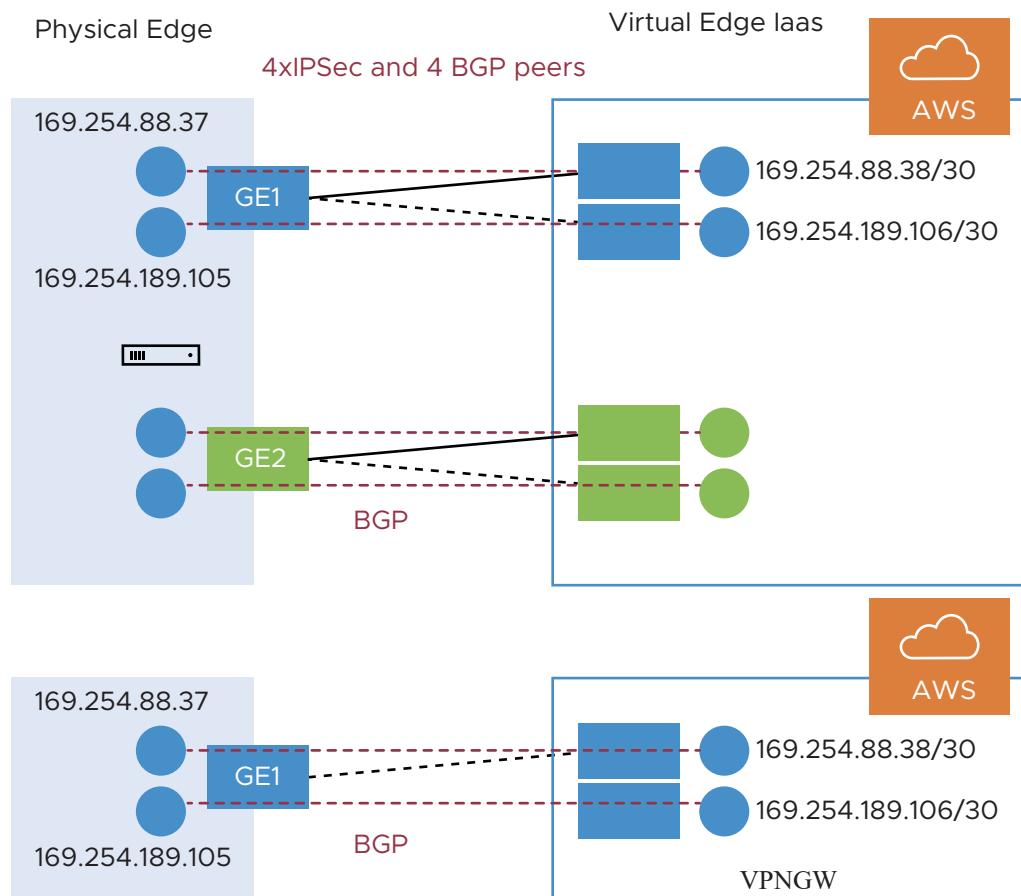


**Note** When an SD-WAN Edge is connected to the same Azure end-point using multiple WAN links, there is a maximum of two NSD-BGP neighbors that could be configured (since remote end has only two public\_ips and two NSD-BGP peer\_ips). Both NSD-BGP neighbors can be configured on the same link (primary/secondary tunnel), or tunnels on different links. If a customer attempts to configure more than two NSD-BGP neighbors and configure the same NSD-BGP peer\_ip on more than one tunnel, the last configured BGP nbr\_ip + local\_ip would be on the SD-WAN Edge and Free Range Routing (FRR).

### Use Case 2: BGP Over IPSec from Edge to AWS VPN/Transit Gateway

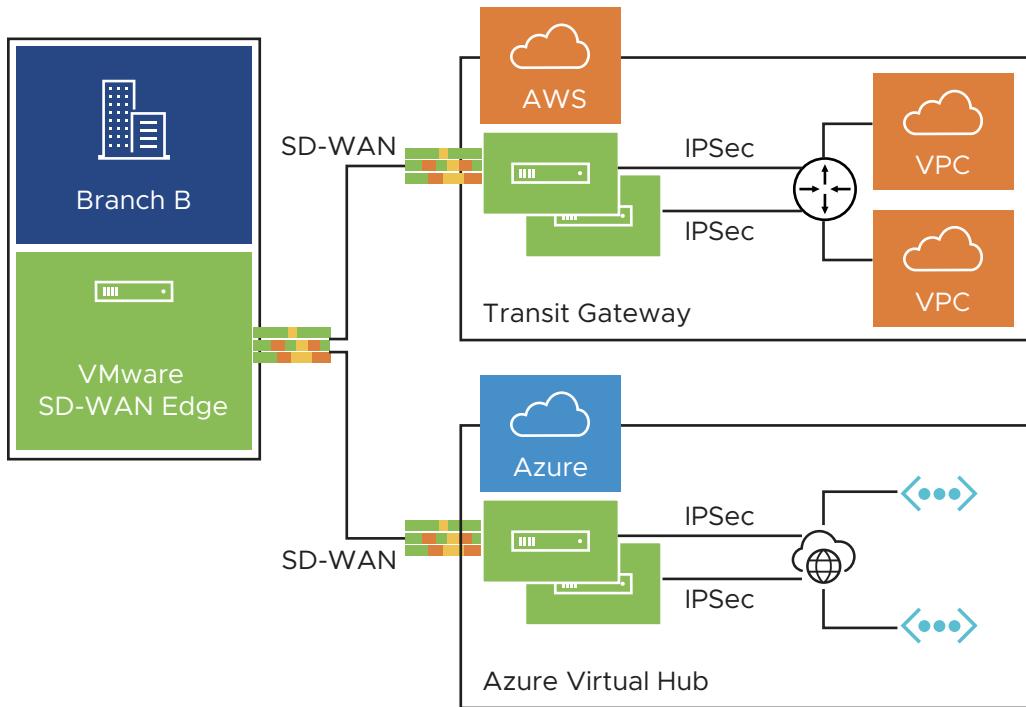
Unlike Azure, AWS VPN Gateway allocates one set of public VIPs per link to a branch Edge. The total sets of public IPs allocated to a branch Edge from an AWS Gateway will be equal to the number of Edge public WAN links that will connect to the AWS VPN Gateway. Similarly, a /30 internal/private subnet would be allocated per tunnel, which are used for BGP peering on that tunnel. These IPs could be manually overridden in AWS Gateway configuration to ensure they are unique across different availability zones.

Similar to the Azure use-case, the Edge will form a mesh of BGP connections - one per tunnel to the AWS gateway. This will allow load-balancing of the return traffic from the AWS VPN Gateway - design on the AWS side. In the diagram below, for the physical Edge, the AWS Gateway allocates one set of public IPs and one set of tunnel-ips (/30) for each Edge WAN link. There are a total of four tunnels, but terminate in different public IPs on the AWS Gateway and four BGP connections.



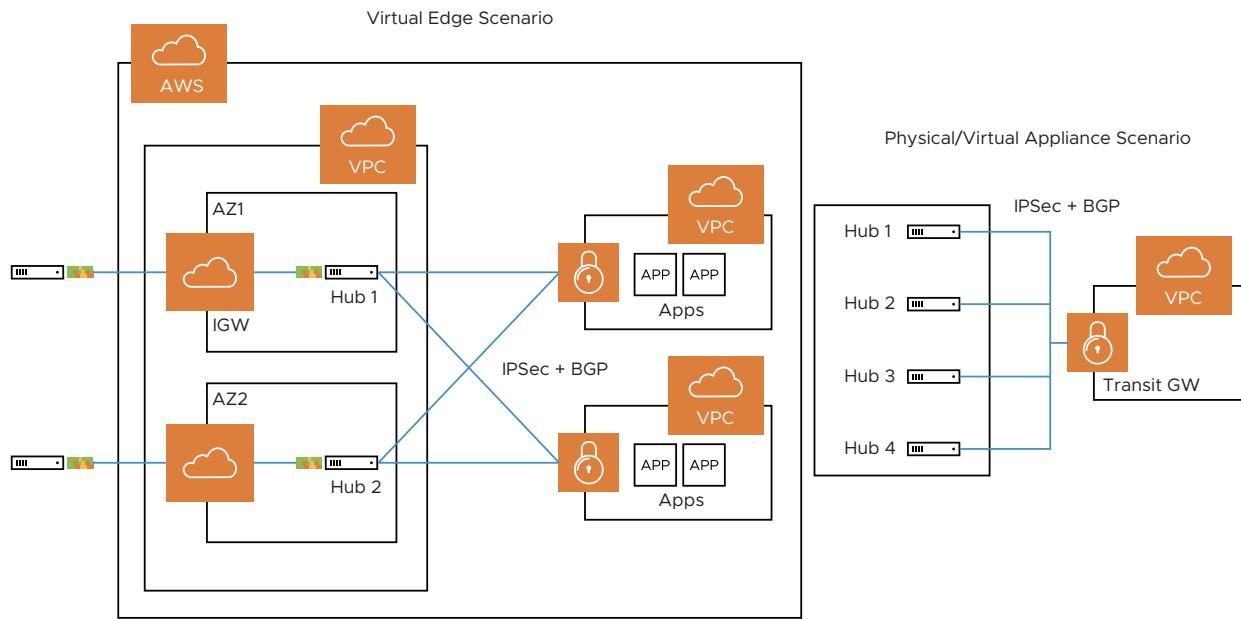
#### Use Case 3: Edge Connecting to Both AWS and Azure VPN Gateways (Hybrid Cloud)

One branch Edge could be connected to both Azure Gateway and AWS Gateway for redundancy purposes or some workloads/apps hosted in one cloud provider while other workloads/apps hosted in a different cloud provider. Regardless of the use-case, the Edge always establishes one BGP session per tunnel and propagates the routes between SD-WAN and IaaS. The diagram below is an example of one branch Edge connected to both Azure and AWS clouds.



#### Use Case 4: Hub Cluster Connecting to Azure/AWS Transit Gateways

The Hub cluster members can form IPsec tunnels to the Azure/AWS transit Gateways and leverage the transit Gateways as Layer 3 for routing traffic between different VPCs. Without the native BGP over IPsec functionality on Hub, the Hub needs to connect to an L3 router (Cisco CSR widely used here) using native BGP and the L3 router forming a mesh of BGP over IPsec tunnels with different VPCs. L3 router serves as a transit end-point between different VPCs. Usecase-1 (left diagram below): Use Hub as a transit node between different VPCs in different Availability Zones (AZ) so that one VPC can talk to another VPC. Usecase-2 (right diagram below): Connect all Hubs in the cluster directly to a cloud transit gateway and can use the cloud gateway as a PE(L3) router for routes distribution between cluster members. In both use-cases, without the support for BGP over IPsec on Hub, hub connects to an L3 router like CSR using native BGP and CSR peers with transit/VPC gateway using BGP over IPsec.



### Use Case 5: Support Transit Functionality in Cloud Providers without Native Support

Some cloud providers like Google Cloud and AliCloud do not have native support for transit functionality (no transit Gateways), and with the support for BGP over IPSec, can rely on SD-WAN Edge/Hub deployed in the cloud to achieve the transit functionality between different VPCs/VNETs. Without the BGP over IPSec support, you must use an L3 router like CSR (solution (2)) to achieve the transit functionality.

---

**Note** Prior to the 4.3 release, for customers who have reachability to the same NVS-Static destination via NVS-From-Gateway and NVS-From-Edge, the traffic from other branch SD-WAN Edges will prefer the path via NVS-Gateway. When customers upgrade their network to the 4.3 release or later, this traffic path from other branch- SD-WAN Edges will prefer the path via the NVS-Edge. Therefore, customers must update the NVS-Static-Destination's metric of the NSD-Edge and the NSD-Gateway as per their traffic path preference.

---

#### Prerequisites:

- Ensure that you have configured [Configure Tunnel Between Branch and Non SD-WAN Destinations via Edge](#) to configure BGP with NSD Neighbors.
- The Local IP address from the Edge is required to configure BGP with NSD Neighbors.

#### Procedure

To enable BGP with Non SD-WAN neighbors:

- 1 In the **SD-WAN** service of the Enterprise Portal, click **Configure**.
- 2 From the left menu, select **Edges**. The **Edges** page displays.
- 3 Click an Edge from the list of available Edges.
- 4 Go to the **Routing & NAT** section in the UI and click the arrow next to BGP.

- 5 In the **BGP** area, check the **Override** check box and toggle the radio button from Off to On.

The screenshot shows the BGP configuration page. At the top, there is a header with a dropdown arrow pointing down, the text "BGP", a checked checkbox labeled "Override", and a radio button labeled "On". Below this, there is a section titled "BGP Settings" containing the following fields:

- Local ASN \***: Input field with value "100", with a note "Example: 50" below it.
- Router ID**: Input field.
- Keep Alive**: Input field with value "60", with a note "Example: 60" below it.
- Hold Timers**: Input field with value "180", with a note "Example: 180" below it.
- Uplink Community**: Input field with value "60:120", with a note "Example: 60:120" below it.
- Enable Graceful Restart**: A checked checkbox with a blue checkmark.

In the **BGP Editor** window, configure the following settings:

- Enter the local Autonomous System Number (ASN) and then configure the following in the **BGP Settings** section.
- Configure the BGP Settings, as described in the table below.

Option	Description
Router ID	Enter the global BGP router ID. If you do not specify any value, the ID is automatically assigned. If you have configured a loopback Interface for the Edge, the IP address of the loopback Interface will be assigned as the router ID.
Keep Alive	Enter the keep alive timer in seconds, which is the duration between the keep alive messages that are sent to the peer. The range is from 0 to 65535 seconds. The default value is 60 seconds.
Hold Timer	Enter the hold timer in seconds. When the keep alive message is not received for the specified time, the peer is considered as down. The range is from 0 to 65535 seconds. The default value is 180 seconds.
Uplink Community	<p>Enter the community string to be treated as uplink routes. Uplink refers to link connected to the Provider Edge(PE). Inbound routes towards the Edge matching the specified community value will be treated as Uplink routes. The Hub/Edge is not considered as the owner for these routes.</p> <p>Enter the value in number format ranging from 1 to 4294967295 or in AA:NN format.</p>
Enable Graceful Restart check box	<p>Please note when selecting this check box: The local router does not support forwarding during the routing plane restart. This feature supports preserving forwarding and routing in case of peer restart.</p>

- Click **+Add** in the **Filter List** area to create one or more filters. These filters are applied to the neighbor to deny or change the attributes of the route. The same filter can be used for multiple neighbors.

The screenshot shows a 'Filter List' interface with the following details:

- Filter Name \***: Filter 1
- Match Type**: Prefix for IPv4
- Match Value \***: Subnet
- Exact Match**: Yes (checked)
- Action Type**: Permit
- Action Set**: None
- \*Required**: A note indicating a required field.
- 1 item**: A count of the current filters.

- 9 In the appropriate text fields, set the rules for the filter, as described in the table below.

Option	Description
Filter Name	Enter a descriptive name for the BGP filter.
Match Type and Value	<p>Choose the type of the routes to be matched with the filter:</p> <ul style="list-style-type: none"> <li><b>Prefix for IPv4 or IPv6</b>: Choose to match with a prefix for IPv4 or IPv6 address and enter the corresponding prefix IP address in the <b>Value</b> field.</li> <li><b>Community</b>: Choose to match with a community and enter the community string in the <b>Value</b> field.</li> </ul>
Exact Match	The filter action is performed only when the BGP routes match exactly with the specified prefix or community string. By default, this option is enabled.
Action Type	Choose the action to be performed when the BGP routes match with the specified prefix or the community string. You can either permit or deny the traffic.
Action Set	<p>When the BGP routes match the specified criteria, you can set to route the traffic to a network based on the attributes of the path. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li><b>None</b>: The attributes of the matching routes remain the same.</li> <li><b>Local Preference</b>: The matching traffic is routed to the path with the specified local preference.</li> <li><b>Community</b>: The matching routes are filtered by the specified community string. You can also select the <b>Community Additive</b> check box to enable the additive option, which appends the community value to existing communities.</li> <li><b>Metric</b>: The matching traffic is routed to the path with the specified metric value.</li> <li><b>AS-Path-Prepend</b>: Allows pre-pending multiple entries of Autonomous System (AS) to a BGP route.</li> </ul>

- 10 To add more matching rules to the filter, click the Plus (+) icon.

- 11 Click **OK** to create the filter.

- The configured filters are displayed in the **BGP Editor** window.
- 12 Configure Underlay Neighbors for IPv4 and IPv6 addresses, as required. For more information, see [Configure BGP from Edge to Underlay Neighbors for Profiles](#).
- 
- Note** The maximum number of supported BGPv4 Match/Set rules is 512 (256 inbound, 256 outbound). Exceeding 512 total Match/Set rules is not supported and may cause performance issues, resulting in disruptions to the enterprise network.
- 13 In the NSD Neighbors section, configure the following settings, as described in the table below.
- | Option  | Description   |
|---|---|
| NSD Name  | Select the NSD Name from the drop-down list. The NSDs already configured in the <b>Branch to Non SD-WAN Destination via Edge</b> area of the SASE Orchestrator are displayed in the drop-down list.   |
| Link Name   | Choose the name of the WAN link associated with the NSD neighbor.   |
| Tunnel Type   | Choose the tunnel type of the Peer as Primary or Secondary.   |
| Neighbor IP   | Enter the IP address of the NSD neighbor.   |
| ASN   | Enter the ASN for the NSD neighbor.   |
| Inbound Filter  | Select an Inbound filer from the drop-down list.  |
| Outbound Filter   | Select an Outbound filer from the drop-down list.   |
| <b>Additional Options – Click the <a href="#">view all</a> link to configure the following additional settings:</b> |   |
| Uplink  | Used to flag the neighbor type to Uplink. Select this flag option if it is used as the WAN overlay towards MPLS. It will be used as the flag to determine whether the site will become a transit site (e.g. SD-WAN Hub), by propagating routes learnt over a SD-WAN overlay to a WAN link toward MPLS. If you need to make it a transit site, select the <b>Overlay Prefix Over Uplink</b> check box in the <b>Advanced</b> Settings. |
| Local IP  | Local IP is mandatory for configuring Non SD-WAN Neighbors.<br>Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address for the outgoing packets.   |

Option	Description
Max-hop	<p>Enter the number of maximum hops to enable multi-hop for the BGP peers. For the 5.1 release and later, the range is from 2 to 255 and the default value is 2.</p> <p><b>Note</b> When upgrading to the 5.1 release, any max-hop value of 1 will automatically be updated to a max-hop value of 2.</p> <p><b>Note</b> This field is available only for eBGP neighbors, when the local ASN and the neighboring ASN are different. With iBGP, when both ASNs are the same, multi-hop is deactivated by default and this field is not configurable.</p>
Allow AS	<p>Select the check box to allow the BGP routes to be received and processed even if the Edge detects its own ASN in the AS-Path.</p>
Default Route	<p>The Default Route adds a network statement in the BGP configuration to advertise the default route to the neighbor.</p>
Enable BFD	<p>Enables subscription to existing BFD session for the BGP neighbor.</p> <p><b>Note</b> Single-hop BFD session is not supported for BGP over IPsec with NSD Neighbors. However, multi-hop BFD is supported. Local IP is mandatory for NSD-BGP sessions on the SD-WAN Edge. The SD-WAN Edge handles only the connected Interface IPs as a single-hop BFD.</p>
Keep Alive	<p>Enter the keep alive timer in seconds, which is the duration between the keep alive messages that are sent to the peer. The range is from 0 to 65535 seconds. The default value is 60 seconds.</p>
Hold Timer	<p>Enter the hold timer in seconds. When the keep alive message is not received for the specified time, the peer is considered as down. The range is from 0 to 65535 seconds. The default value is 180 seconds.</p>
Connect	<p>Enter the time interval to try a new TCP connection with the peer if it detects the TCP session is not passive. The default value is 120 seconds.</p>

Option	Description
MD5 Auth	Select the check box to enable BGP MD5 authentication. This option is used in a legacy network or federal network, and it is common that BGP MD5 is used as a security guard for BGP peering.
MD5 Password	Enter a password for MD5 authentication. <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.

**Note** Over Multi-hop BGP, the system might learn routes that require recursive lookup. These routes have a next-hop IP which is not in a connected subnet, and do not have a valid exit interface. In this case, the routes must have the next-hop IP resolved using another route in the routing table that has an exit interface. When there is traffic for a destination that needs these routes to be looked up, routes requiring recursive lookup will get resolved to a connected Next Hop IP address and interface. Until the recursive resolution happens, the recursive routes point to an intermediate interface. For more information about Multi-hop BGP Routes, see the "Remote Diagnostic Tests on Edges" section in the *VMware SD-WAN Troubleshooting Guide* published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

- 14 Click **Advanced** to configure the following settings, as described in the table below.

**Note** Advanced Settings are shared across both the underlay BGP neighbors and NSD BGP neighbors.

Option	Description
Overlay Prefix	Select the check box to redistribute the prefixes learned from the overlay.
Turn off AS-Path carry over	By default, this should be left unchecked. Select the check box to turn off AS-PATH Carry Over. In certain topologies, turning off AS-PATH Carry Over will influence the outbound AS-PATH to make the L3 routers prefer a path towards an Edge or a Hub. <b>Warning</b> When the AS-PATH Carry Over is turned off, tune your network to avoid routing loops.
Connected Routes	Select the check box to redistribute all the connected Interface subnets.
OSPF	Select the check box to enable OSPF redistribute into BGP.
Set Metric	When you enable OSPF, enter the BGP metric for the redistributed OSPF routes. The default value is 20.

Option	Description
Default Route	<p>Select the check box to redistribute the default route only when Edge learns the BGP routes through overlay or underlay.</p> <p>When you select the <b>Default Route</b> option, the <b>Advertise</b> option is available as <b>Conditional</b>.</p>
Overlay Prefixes over Uplink	Select the check box to propagate routes learned from overlay to the neighbor with uplink flag.
Networks	Enter the network address that BGP will be advertising to the peers. Click the Plus (+) icon to add more network addresses.

When you enable the **Default Route** option, the BGP routes are advertised based on the Default Route selection globally and per BGP neighbor, as shown in the following table.

Default Route Selection		
Global	Per BGP Neighbor	Advertising Options
Yes	Yes	The per BGP neighbor configuration overrides the global configuration and hence default route is always advertised to the BGP peer.
Yes	No	BGP redistributes the default route to its neighbor only when the Edge learns an explicit default route through the overlay or underlay network.
No	Yes	Default route is always advertised to the BGP peer.
No	No	The default route is not advertised to the BGP peer.

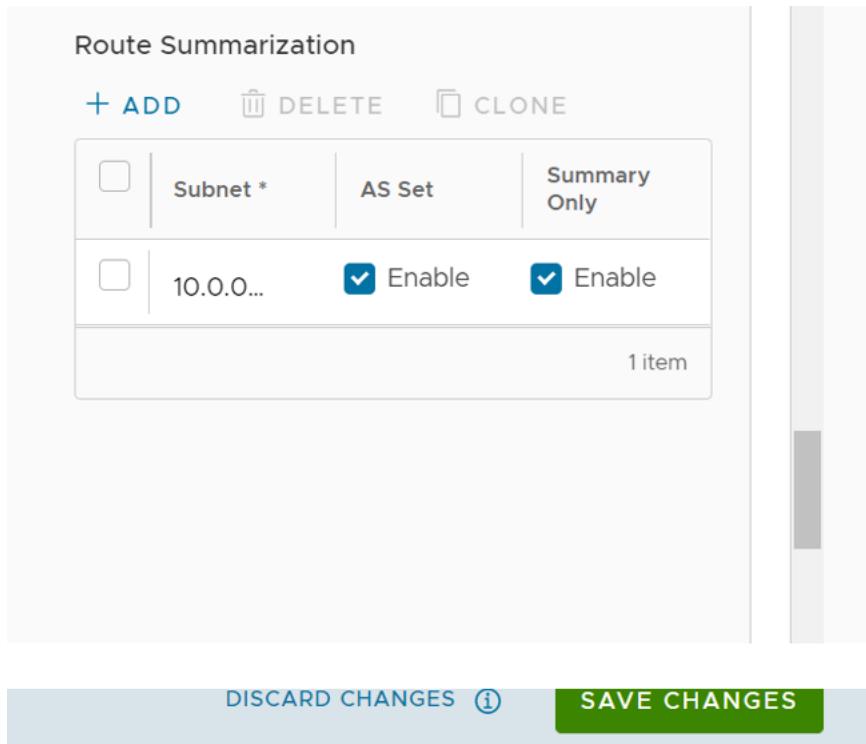
- 15 Click **OK** to save the configured filters and NSD Neighbors.

The **BGP Settings** section displays the configured settings.

### Route Summarization

The Route Summarization feature is available in the 5.2 release, for an overview and use case of this functionality, see [Chapter 34 Route Summarization](#). For configuration details, follow the steps below.

- 16 Click **+Add** in the **Route Summarization** area. A new row is added to the Route Summarization area. See image below.



- 17 Under the **Subnet** column, enter the network range that you want to summarize in the A.B.C.D/M format and the IP subnet.
  - 18 Under the **AS Set** column, click the **Yes** check box if applicable.
  - 19 Under the **Summary Only** column, click the **Yes** check box to allow only the summarized route to be sent.
  - 20 Add additional routes, if necessary, by clicking **+Add**. To Clone or Delete a route summarization, use the appropriate buttons, located next to **+Add**.
- The BGP Settings section displays the BGP configuration settings.
- 21 Click **Save Changes** when complete to save the configuration.

You can also configure BGP from Edge to underlay neighbors. For more information, see [Configure BGP from Edge to Underlay Neighbors for Profiles](#).

## Configure BGP Over IPsec from Gateways

You can configure BGP Settings for SD-WAN Gateways over IPsec tunnels.

### About this task:

Only eBGP is supported with BGP over IPsec.

---

**Note** It is recommended to use eBGP between SDWAN Gateway and NSD sites. If iBGP is used, applying local preference does not work with outbound filter. In that case, customer must choose metric or AS path prepend options to achieve desirable routing.

VMware allows Enterprise users to define and configure a Non SD-WAN Destination instance in order to establish a secure IPsec tunnel to a Non SD-WAN Destination through an SD-WAN Gateway.

---

**Note** For the 5.2 release, when multiple NSDs are configured for the same segment, the same set of summary route configurations must be present across all NSDs.

---

#### Before you begin:

---

**Note** The Azure vWAN Automation from Gateway feature is not compatible with BGP over IPsec. This is because only static routes are supported when automating connectivity from a Gateway to an Azure vWAN.

---

**Important** DCC is mandatory for ECMP to work properly.

---

Ensure that you have configured the following:

- Create a Non SD-WAN Destination via Gateway for one of the following sites:
  - Configure a Non SD-WAN Destination of Type AWS VPN Gateway
  - Configure a Non SD-WAN Destination of Type Check Point
  - Configure a Non SD-WAN Destination of Type Cisco ASA
  - Configure a Non SD-WAN Destination of Type Cisco ISR
  - Configure a Non SD-WAN Destination of Type Generic IKEv2 Router (Route Based VPN)
  - Configure a Non SD-WAN Destination of Type Microsoft Azure Virtual Hub
  - Configure a Non SD-WAN Destination of Type Palo Alto
  - Configure a Non SD-WAN Destination of Type SonicWALL
  - Configure a Non SD-WAN Destination of Type Zscaler
  - Configure a Non SD-WAN Destination of Type Generic IKEv1 Router (Route Based VPN)
  - Configure a Non SD-WAN Destination of Type Generic Firewall (Policy Based VPN)
- Associate the Non SD-WAN Destination to a Profile See [Configure a Tunnel Between a Branch and a Non SD-WAN Destinations via Gateway](#).

---

**Note** It is recommended to turn on **Distributed Cost Calculation** for best performance and scaling when using BGP over IPsec via Gateway. The **Distributed Cost Calculation** is supported starting from Release 3.4.0.

For more information on **Distributed Cost Calculation**, refer to the **Configure Distributed Cost Calculation** section in the *VMware SD-WAN Operator Guide* available at: <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

---

## Procedure

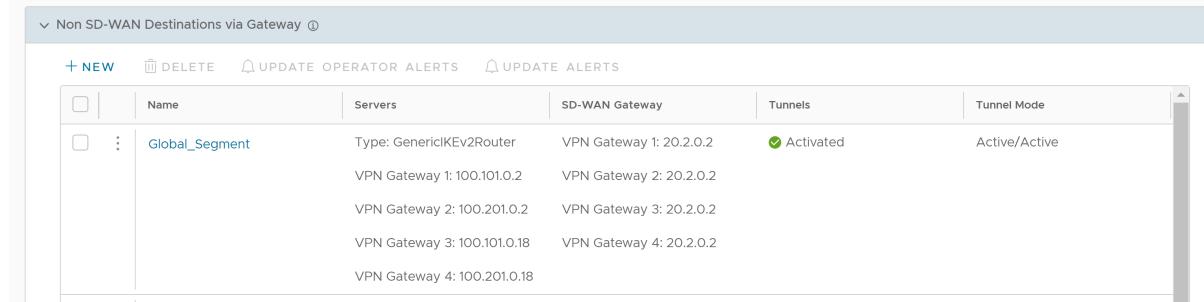
- 1 Go to **Configure > Network Services**, and then under Non SD-WAN Destinations, expand Non SD-WAN Destinations via Gateway.

**Note** If there are no new The New NSD via Gateway option appears only when there are no items in the table. Follow Steps 2 and 3 to create a new Non SD-WAN Destination.

### Network Services

Configuring Network Services are optional and can be configured in any order. Use these configurations across multiple Edges and Profiles for a more efficient workflow. [Learn more about Network Services](#).

#### Non SD-WAN Destinations



	Name	Servers	SD-WAN Gateway	Tunnels	Tunnel Mode
<input type="checkbox"/>	Global_Segment	Type: GenericIKEv2Router VPN Gateway 1: 100.101.0.2 VPN Gateway 2: 100.201.0.2 VPN Gateway 3: 100.101.0.18 VPN Gateway 4: 100.201.0.18	VPN Gateway 1: 20.2.0.2 VPN Gateway 2: 20.2.0.2 VPN Gateway 3: 20.2.0.2 VPN Gateway 4: 20.2.0.2	<input checked="" type="checkbox"/> Activated	Active/Active

- 2 Click **+New** to create a new Non SD-WAN Destination.

The **Non SD-WAN Destinations via Gateway** dialog displays, as show in the image below.

## Non SD-WAN Destinations via Gateway

**Name \***

**Type \***

**Tunnel Mode**

**VPN Gateways ⓘ**

<b>VPN Gateway 1 (Primary)*</b>	<input type="text" value="Example 54.183.9.192"/> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px;">-</span>
<b>VPN Gateway 2 (Secondary)</b>	<input type="text" value="Example 54.183.9.192"/> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px;">-</span> <span style="border: 1px solid #0070C0; border-radius: 50%; padding: 2px;">+</span>

CANCEL CREATE

- 3 In the **Non SD-WAN Destinations via Gateway** area (see image above), configure the following fields as described in the table below.

Option	Description
Name	Enter a name for the Non SD-WAN Destination in the text box.
Type	Select an IPsec tunnel type from the drop-down menu.
Tunnel Mode	<b>Active/ Hot-Standby</b> mode supports to set up a maximum of 2 tunnel endpoints or Gateways. <b>Active/Activemode</b> supports to set up a maximum of 4 tunnel endpoints or Gateways. All Active tunnels can send and receive traffic through ECMP.
VPN Gateway 1	Enter a valid IP address
VPN Gateway 2	Enter a valid IP address. This field is optional

The Non SD-WAN Destinations via Gateway is created, as shown in the image below.

## Non SD-WAN Destinations

	Name	Servers	SD-WAN Gateway	Tunnels	Operator Alerts
<input type="checkbox"/>	ACME	Type: GenericIKEv2Router Primary: 16.0.9.1 Primary: 54.183.9.192 Secondary: None	Secondary: None	<input checked="" type="checkbox"/> Activated	<input checked="" type="checkbox"/> Activated

- 4 In the **Non SD-WAN Destination via Gateway** area, slide the grey bar to the far right to the BGP column.

Click the **Edit** link under the BGP column.

If the **Edit** link does not display under the BGP column, see the section titled, "Configure a Tunnel Between a Branch and a Non SD-WAN Destinations via Edge" to enable an Edge to Non SD-WAN via Gateway.

After clicking the **Edit** link under the **BGP** column, the **Edit BGP** dialog displays.

- 5 Toggle the **BGP Activated** radio button to the right to turn it green.
- 6 Click **+Add** to create one or more filters. These filters are applied to the neighbor to deny or change the attributes of the route. The same filter can be used for multiple neighbors.
- 7 Configure the options In the **Filter List** area, as described in the table below.

Option	Description
Filter Name	Enter a descriptive name for the BGP filter.
Match Type and Value	<p>Choose the type of the routes to be matched with the filter:</p> <ul style="list-style-type: none"> <li>■ <b>Prefix for IPv4 or IPv6:</b> Choose to match with a prefix for IPv4 or IPv6 address and enter the corresponding prefix IP address in the <b>Value</b> field.</li> <li>■ <b>Community:</b> Choose to match with a community and enter the community string in the <b>Value</b> field.</li> </ul>
Exact Match	The filter action is performed only when the BGP routes match exactly with the specified prefix or community string. By default, this option is enabled.

Option	Description
Action Type	Choose the action to be performed when the BGP routes match with the specified prefix or the community string. You can either permit or deny the traffic.
Action Set	When the BGP routes match the specified criteria, you can set to route the traffic to a network based on the attributes of the path. Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>None:</b> The attributes of the matching routes remain the same.</li> <li>■ <b>Local Preference:</b> The matching traffic is routed to the path with the specified local preference.</li> <li>■ <b>Community:</b> The matching routes are filtered by the specified community string. You can also select the <b>Community Additive</b> check box to enable the additive option, which appends the community value to existing communities.</li> <li>■ <b>Metric:</b> The matching traffic is routed to the path with the specified metric value.</li> <li>■ <b>AS-Path-Prepend:</b> Allows pre-pending multiple entries of Autonomous System (AS) to a BGP route.</li> </ul>

- 8 Click the **plus (+)** icon to add more matching rules for the filter. Repeat the procedure to create more filters.

The configured filters are displayed in the **Filter List** area.

The screenshot shows the 'Edit BGP' configuration interface. At the top, there is a toggle switch labeled 'BGP Activated' which is turned on. Below it is a section titled 'Filter List' with three buttons: '+ ADD', 'DELETE', and 'CLONE'. The main area displays a table with two rows, each representing a filter rule:

Filter Name *	Match Type	Match Value *	Exact Match	Action Type	Action Set	
Inbound_Corp	Community	(-) (+) 100:101	<input checked="" type="checkbox"/> Yes	Permit	Community	12345.11 Community Additive <input checked="" type="checkbox"/> Activated
Outbound_Corp	Community	(-) (+) 125:201	<input checked="" type="checkbox"/> Yes	Permit	Community	123465.12 Community Additive <input checked="" type="checkbox"/> Activated

At the bottom of the table, there is a note: '\*Required' and a message: '2 items'. Below the table are two buttons: 'CANCEL' and 'SAVE CHANGES'.

Edit BGP

*Required		O items																														
Primary Cloud Gateway gateway-2																																
Local ASN *	501	Router ID																														
<b>Neighbors</b> <span>+ ADD</span> <span>DELETE</span> <table border="1"> <thead> <tr> <th>Tunnel *</th> <th>Neighbor IP *</th> <th>ASN *</th> <th>Inbound Filter</th> <th>Outbound Filter</th> <th>Additional Options</th> </tr> </thead> <tbody> <tr> <td>VPN Gateway 1</td> <td>169.254.0.2</td> <td>600</td> <td>[None] </td> <td>[None] </td> <td> <span>VIEW ALL</span></td> </tr> <tr> <td>VPN Gateway 2</td> <td>169.254.0.6</td> <td>601</td> <td>[None] </td> <td>[None] </td> <td> <span>VIEW ALL</span></td> </tr> <tr> <td>VPN Gateway 3</td> <td>169.254.0.10</td> <td>602</td> <td>[None] </td> <td>[None] </td> <td> <span>VIEW ALL</span></td> </tr> <tr> <td>VPN Gateway 4</td> <td>169.254.0.14</td> <td>603</td> <td>[None] </td> <td>[None] </td> <td> <span>VIEW ALL</span></td> </tr> </tbody> </table>			Tunnel *	Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options	VPN Gateway 1	169.254.0.2	600	[None]	[None]	<span>VIEW ALL</span>	VPN Gateway 2	169.254.0.6	601	[None]	[None]	<span>VIEW ALL</span>	VPN Gateway 3	169.254.0.10	602	[None]	[None]	<span>VIEW ALL</span>	VPN Gateway 4	169.254.0.14	603	[None]	[None]	<span>VIEW ALL</span>
Tunnel *	Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options																											
VPN Gateway 1	169.254.0.2	600	[None]	[None]	<span>VIEW ALL</span>																											
VPN Gateway 2	169.254.0.6	601	[None]	[None]	<span>VIEW ALL</span>																											
VPN Gateway 3	169.254.0.10	602	[None]	[None]	<span>VIEW ALL</span>																											
VPN Gateway 4	169.254.0.14	603	[None]	[None]	<span>VIEW ALL</span>																											
*Required		4 items																														
<b>Route Summarization</b> <span>+ ADD</span> <span>DELETE</span> <span>CLONE</span> <table border="1"> <tr> <td>Subnet *</td> <td>AS Set</td> <td>Summary Only</td> </tr> </table>			Subnet *	AS Set	Summary Only																											
Subnet *	AS Set	Summary Only																														
		<span>CANCEL</span> <span>SAVE CHANGES</span>																														

**Note** These BGP neighbors are assigned to their respective tunnels exclusively for neighborship establishment and subsequent control exchanges, ensuring these communication occurs solely over the designated tunnels.

- 9 In the BGP Editor window, configure the BGP settings for the Primary and Secondary Gateways.

**Note** The Secondary Gateway option is available only if you have configured a secondary Gateway for the corresponding Non SD-WAN Destination.

**Note** For a customer deployment where a Non VMware SD-WAN Destination (NSD) via Gateway is configured to use redundant tunnels, if the Primary and Secondary Gateways advertise a prefix with an equal AS path to the Primary and Secondary NSD tunnels, the Primary NSD tunnel will prefer a redundant Gateway path over the Primary Gateway. The impact of the Primary NSD over Gateway tunnel preferring the redundant Gateway path over the Primary Gateway is experienced only for return traffic to the Gateway from the NSD.

If you do not want your BGP router to prefer the redundant Gateway, the workaround is to configure AS-PATH prepend and set the metric filter to a higher (3 or more) metric for the advertised prefix in the redundant Gateway. Doing this ensures the NSD's primary tunnel chooses the Primary Gateway for return traffic.

- 10 In the **Primary Cloud Gateway** section, enter the local ASN and the Router ID.

- 11 Scroll down to the Neighbors area and click **+Add**.
- 12 Configure the following settings in the **Neighbors** area, as described in the table below.

Option	Description
Local ASN	Enter the local Autonomous System Number (ASN)
Router ID	Enter the BGP Router ID
Neighbor IP	Enter the IP address of the BGP neighbor
ASN	Enter the ASN of the neighbor
Inbound Filter	Select an Inbound filer from the drop-down list
Outbound Filter	Select an Outbound filer from the drop-down list
<b>Additional Options – Click the <a href="#">view all</a> link to configure the following additional settings:</b>	
Local IP	Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address for the outgoing packets.
Max-hop	Enter the number of maximum hops to enable multi-hop for the BGP peers. For the 5.1 release and later, the range is from 2 to 255 and the default value is 2.  <b>Note</b> When upgrading to the 5.1 release, any max-hop value of 1 will automatically be updated to a max-hop value of 2.
	<b>Note</b> This field is available only for eBGP neighbors, when the local ASN and the neighboring ASN are different.
Allow AS	Select the check box to allow the BGP routes to be received and processed even if the Gateway detects its own ASN in the AS-Path.
Default Route	The Default Route adds a network statement in the BGP configuration to advertise the default route to the neighbor.
Enable BFD	Enables subscription to the existing BFD session for the BGP neighbor.
Keep Alive	Enter the keep alive timer in seconds, which is the duration between the keep alive messages that are sent to the peer. The range is from 1 to 65535 seconds. The default value is 60 seconds.
Hold Timer	Enter the hold timer in seconds. When the keep alive message is not received for the specified time, the peer is considered as down. The range is from 1 to 65535 seconds. The default value is 180 seconds.

Option	Description
Connect	Enter the time interval to try a new TCP connection with the peer if it detects that the TCP session is not passive. The default value is 120 seconds.
MD5 Auth	Select the check box to enable BGP MD5 authentication. This option is used in a legacy network or federal network, and is used as a security guard for BGP peering.
MD5 Password	Enter a password for MD5 authentication.  <b>Note</b> Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.

The configured Neighbors are displayed in the **Neighbors** area.

Click the **Save Changes** button to save all changes.

Edit BGP

Neighbors					
Tunnel Type *	Neighbor IP *	ASN *	Inbound Filter	Outbound Filter	Additional Options
Primary	10.0.0.7	1	Inbound_Corp	Outbound_Corp	<input type="checkbox"/> Max-Hop <input type="checkbox"/> Local IP <input checked="" type="checkbox"/> Allow AS <input checked="" type="checkbox"/> Default Route <input checked="" type="checkbox"/> Enable BFD <input type="checkbox"/> Keep Alive <input type="checkbox"/> Hold Timer <input type="checkbox"/> Connect <input checked="" type="checkbox"/> MD5 Auth
<input type="button" value="VIEW LESS"/> <input type="button" value="VIEW MORE"/>					

**Note** Over Multi-hop BGP, the system might learn routes that require recursive lookup. These routes have a next-hop IP which is not in a connected subnet, and do not have a valid exit Interface. In this case, the routes must have the next-hop IP resolved using another route in the routing table that has an exit Interface. When there is traffic for a destination that needs these routes to be looked up, routes requiring recursive lookup will get resolved to a connected Next Hop IP address and Interface. Until the recursive resolution happens, the recursive routes point to an intermediate Interface. For more information about Multi-hop BGP Routes, see the "Remote Diagnostic Tests on Edges" section in the *VMware SD-WAN Troubleshooting Guide* published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

## Route Summarization

The Route Summarization feature is available in the 5.2 release, for an overview and use case of this functionality, see [Chapter 34 Route Summarization](#). For configuration details, follow the steps below.

- 13 Scroll down to the **Route Summarization** area.
- 14 Click **+Add** in the **Route Summarization** area. A new row is added to the **Route Summarization** area.

Configure route summarization, as described in the table below.

Option	Description
Filter Name	Enter a descriptive name for the BGP filter.
Subnet	Enter the IP subnet.
AS Set	Generate AS set path information from the summarized routes (while advertising the summary route to the peer). Under the <b>AS Set</b> column, click the <b>Yes</b> check box if applicable.
Summary Only	Click the <b>Yes</b> check box to allow only the summarized route to be sent.

- 15 Add additional routes, if necessary, by clicking **+Add**. To Clone or Delete a route summarization, use the appropriate buttons, located next to **+Add**.

The **BGP Settings** section displays the BGP configuration settings.

Route Summarization			
<b>+ ADD</b>	<b>DELETE</b>	<b>CLONE</b>	
<input type="checkbox"/>	Subnet *	AS Set	Summary Only
<input type="checkbox"/>	10.0.0...	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
1 item			

**DISCARD CHANGES** ① **SAVE CHANGES**

16 Click **Save Changes** when complete to save the configuration.

### Note

- Only for Gateways running version 6.0 or later have an option to configure upto 4 tunnels based on VPN type. In addition, those tunnels destined to be a Non-SDWAN gateways can operate in either AA or A-HS mode to achieve load sharing/bearing preferences of the user.
- For gateways running version less than 6.0, all active-active configurations are interpreted as active-hotstandby with tunnel 1 being active and tunnel 2 being hot-standby.

## Monitor BGP Sessions

You can monitor the BGP sessions on Edges and Gateways.

Refer to the following sections to monitor the BGP sessions:

- [Monitor Network Services](#)
- [Monitor BGP Edge Neighbor State](#)
- [Monitor BGP Gateway Neighbor State](#)

## Monitor BGP Events

You can view the events related to the BGP sessions.

In the **SD-WAN** service of the Enterprise Portal, click **Monitor > Events**.

To view the events related to BGP, you can use the filter option. Click the Filter Icon next to the **Search** option and choose to filter the details by different categories.

The following image shows some of the BGP events.

Event	User	Segment	Edge	Severity	Time	Message
BGPv6 session established to edge neighbor		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:30:40 PM	BGPv6 session up for edge [b1-edge1] to neighbor IP: [fd00:1:14:1]
BGP session established to edge neighbor		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:40 PM	BGP session up for edge [b1-edge1] to neighbor IP: [172.16.1.3]
BGP session established to edge neighbor		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:40 PM	BGP session up for edge [b1-edge1] to neighbor IP: [172.16.1.1]
BGPv6 session established to edge neighbor		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:40 PM	BGPv6 session up for edge [b1-edge1] to neighbor IP: [fd00:1:13:1]
BGP session established to edge neighbor		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:40 PM	BGP session up for edge [b1-edge1] to neighbor IP: [172.17.1.3]
BGP session established to edge neighbor		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:40 PM	BGP session up for edge [b1-edge1] to neighbor IP: [172.17.1.1]
BGPv6 session established to edge neighbor		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:40 PM	BGPv6 session up for edge [b1-edge1] to neighbor IP: [fd00:1:2:3:1]
BGPv6 session established to edge neighbor		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:40 PM	BGPv6 session up for edge [b1-edge1] to neighbor IP: [fd00:1:2:4:1]
Edge BGP neighbor unavailable		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:39 PM	BGP session down for edge [b1-edge1] to neighbor IP: [172.16.1.3]
Edge BGP neighbor unavailable		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:39 PM	BGP session down for edge [b1-edge1] to neighbor IP: [172.16.1.1]
Edge BGPv6 neighbor unavailable		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:39 PM	BGPv6 session down for edge [b1-edge1] to neighbor IP: [fd00:1:1:3:1]
Edge BGPv6 neighbor unavailable		Global Segment	b1-edge1	Info	Jul 16, 2021, 12:29:39 PM	BGPv6 session down for edge [b1-edge1] to neighbor IP: [fd00:1:1:1]

The following are the events related to BGP.

- BGP session established to Gateway neighbor
- BGP session established to Edge neighbor

- BGPv6 session established to Edge neighbor
- Edge BGP neighbor unavailable
- Edge BGPv6 neighbor unavailable
- Gateway BGP neighbor unavailable

## Troubleshooting BGP Settings

You can run Remote Diagnostics tests to view the logs of the BGP sessions and use the log information for troubleshooting purposes.

To run the tests for BGP:

- 1 In the **SD-WAN** service of the Enterprise Portal, click **Diagnostics > Remote Diagnostics**.
- 2 The **Remote Diagnostics** page displays all the active Edges.
- 3 Select the Edge that you want to troubleshoot. The Edge enters live mode and displays all the possible Remote Diagnostics tests than you can run on the Edge.
- 4 For troubleshooting BGP sessions, scroll to the following sections and run the tests:
  - **Troubleshoot BGP - List BGP Redistributed Routes** – Run this test to view routes redistributed to BGP neighbors.
  - **Troubleshoot BGP - List BGP Routes** – Run this test to view the BGP routes from neighbors. You can enter IPv4 or IPv6 prefix to view specific BGP routes or leave the prefix empty to view all the BGP routes.
  - **Troubleshoot BGP - List Routes per Prefix** – Run this test to view all the Overlay and Underlay routes for a specific IPv4 or IPv6 prefix and the related details.
  - **Troubleshoot BGP - Show BGP Neighbor Advertised Routes** – Run this test to view the BGP routes advertised to a neighbor.
  - **Troubleshoot BGP - Show BGP Neighbor Learned Routes** – Run this test to view all the accepted BGP routes learned from a neighbor after filters.
  - **Troubleshoot BGP - Show BGP Neighbor Received Routes** – Run this test to view all the BGP routes learned from a neighbor before filters.
  - **Troubleshoot BGP - Show BGP Neighbor details** – Run this test to view the details of BGP neighbor.
  - **Troubleshoot BGP - Show BGP Routes per Prefix** – Run this test to view all the BGP routes and their attributes for the specified prefix.
  - **Troubleshoot BGP - Show BGP Summary** – Run this test to view the existing BGP neighbor and received routes.
  - **Troubleshoot BGP - Show BGP Table** – Run this test to view the BGP table.
  - **Troubleshoot BGPv6 - Show BGPv6 Neighbor Advertised Routes** – Run this test to view the BGPv6 routes advertised to a neighbor.

- **Troubleshoot BGPv6 - Show BGPv6 Neighbor Learned Routes** – Run this test to view all the accepted BGPv6 routes learned from a neighbor after filters.
- **Troubleshoot BGPv6 - Show BGPv6 Neighbor Received Routes** – Run this test to view all the BGPv6 routes received from a neighbor before filters.
- **Troubleshoot BGPv6 - Show BGPv6 Neighbor details** – Run this test to view the details of BGPv6 neighbor.
- **Troubleshoot BGPv6 - Show BGPv6 Routes per Prefix** – Run this test to view all the BGPv6 routes for the prefix and their attributes.
- **Troubleshoot BGPv6 - Show BGPv6 Summary** – Run this test to view the existing BGPv6 neighbor and received routes.
- **Troubleshoot BGPv6 - Show BGPv6 Table** – Run this test to view the details of BGPv6 table.

For more information about all the supported BGP related Remote Diagnostics tests, see the "Remote Diagnostic Tests on Edges" section in the VMware SD-WAN Troubleshooting Guide published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

## OSPF/BGP Redistribution

Each of routing protocols OSPF and BGP may be enabled independently and the prior model of allowing only one routing protocol to be enabled on the system has been removed with this release. This release also allows the possibility of redistributing OSPF into BGP or BGP into OSPF (or both simultaneously), along with other possible route sources like prefixes learnt over the overlay, connected routes, static routes, etc.

In addition, with release 3.2, we are standardizing the redistribution behavior along more traditional lines (similar to that in other routing vendors). For example, if there is more than one route available for the same prefix, then only the best route for that prefix in the system RIB will be redistributed to the destination protocol if the configuration in the destination protocol allows redistribution for that route type.

Consider, as an example, redistribution of the prefix 192.168.1.0/24 into BGP. Let's say routes to the prefix 192.168.1.0/24 are locally available, learned from OSPF and separately learned as an Overlay prefix. Let's further assume that between the OFC flow ordering for the prefix, and route metrics, and route preference the OSPF route ranks above (is better than) the learned overlay route for that same prefix. Then, the OSPF route will be redistributed into BGP if OSPF redistribution has been turned on in BGP. Note that since the overlay learned prefix is not the best route for that prefix in the system RIB, it will not be redistributed into BGP even if the redistribution of overlay prefixes has been turned on in BGP.

In cases like the above, in order to facilitate the redistribution of the best route for a prefix into a given destination protocol, the user can enable redistribution for the specific route type that is the best route in the system.

Alternately, if the user prefers a different route source for that prefix to be redistributed into the destination protocol, the user can control the relative precedence of the route in the system RIB using the Overlay Flow Control facility provided by the management interface, or by varying the route metric.

### **OSPF/BGP Redistribution Metric Calculation**

Starting with the 5.2 release, the route redistribution metric calculation has changed. When a route is redistributed from the Overlay to OSPF/BGP, the redistribution metric is calculated by taking the original route metric and adding the transit metric:

- The transit metric is (0) if the route is learned from a directly connected Edge.
- The transit metric is (90) if the route is learned via a Gateway.
- The transit metric is (32 + hub's order value) if the route is learned via a Hub Edge.

For OSPF External Type-1 (OE1) routes, this is the final metric. For OSPF External Type-2 (OE2) routes, it will add up the non-preferred metric constant (8388607). This is why there is a very high metric value for an OE2 route type on Edge peers.

For BGP, this implies that the BGP MED value advertised by Hub Edges, which previously started from 9, 10, 11, and so forth, now starts from 33, 34, 35, and so forth.

See [Activate OSPF for Profiles](#), [Activate OSPF for Edges](#), [Configure BGP from Edge to Underlay Neighbors for Profiles](#), and [Configure BGP from Edge to Underlay Neighbors for Edges](#) for more information.

## **BFD Settings**

Bidirectional Forwarding Detection (BFD) is a simple Hello protocol that is similar to detection components of well-known routing protocols. A pair of systems transmit BFD packets periodically over each path between the two systems, and if a system stops receiving BFD packets for long enough, the neighboring system is assumed to have failed.

A BFD session is established based on the needs of the application that would use BFD. The user has to explicitly configure the address and parameters for the BFD session and the subscribers/applications (BGP/OSPF) of the session, as there is no discovery mechanism in BFD.

Routing protocols like BGP or OSPF exchange the learned routes between Edges and Routers. These protocols exchange routes and detect route failures using their own mechanism. Generally, route failures are detected based on the keepalive mechanism where one entity echoes other entity on a frequent configured interval, that is the keepalive time. These routing protocols have higher keepalive timers which results in longer duration to detect the route failures. BFD detects route failures between two connected entities faster with low overhead on detection of failures.

The following are the advantages of implementing BFD with routing protocols.

- Fast route failure detection with low re-convergence time.
- Less overhead in route failure detection.

- Uniform rate of route failure detection across routing protocols.

BFD can be defined as a simple service. The service primitives provided by BFD are to create, destroy, and modify a session, given the destination address and other parameters. BFD in return provides a signal to the clients indicating when the BFD session goes up or down.

There are two operating modes to BFD, asynchronous mode and demand mode. VMware supports asynchronous mode. In this mode, the systems periodically send BFD control packets to other systems and if several packets in a row are not received by a system, the session is declared to be down.

---

**Note** BFD Echo mode is not supported.

---

VMware supports BFD for the following routing protocols:

- BGP on Edges and Partner Gateways
- OSPF on Edges

## Configure BFD for Profiles

VMware SD-WAN allows to configure BFD sessions to detect route failures between two connected entities.

To configure a BFD session for Profiles:

### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**.
- 2 Click the **Device** icon for a profile, or select a profile and click the **Device** tab.

---

**Note** The **Device** tab is normally the default tab.

---

- 3 In the **Device** tab, scroll down to the **Routing & NAT** section and click the arrow next to the **BDF** area to open it.
- 4 Click the **BDF** slider to **ON** position.
- 5 Configure the following settings, as described in the table below. See image below for example.

Field	Description
Peer Address	Enter the IPv4 address of the remote peer to initiate a BFD session.
Local Address	<p>Enter a locally configured IPv4 address for the peer listener. This address is used to send the packets.</p> <p><b>Note</b> You can click the <b>IPv6</b> tab to configure IPv6 addresses for the remote peer and the peer listener.</p> <p>For IPv6, the local and peer addresses support only the following format:</p> <ul style="list-style-type: none"> <li>■ IPv6 global unicast address (2001:CAFE:0:2::1)</li> <li>■ IPv6 unique local address (FD00::1234:BEFF:ACE:EOA4)</li> </ul>

Field	Description
<b>Multihop</b>	Select the check box to enable multi-hop for the BFD session. While BFD on Edge and Gateway supports directly connected BFD Sessions, you need to configure BFD peers in conjunction with multi-hop BGP neighbors. The multi-hop BFD option supports this requirement. Multihop must be enabled for the BFD sessions for NSD-BGP-Neighbors.
<b>Detect Multiplier</b>	Enter the detection time multiplier. The remote transmission interval is multiplied by this value to determine the detection timer for connection loss. The range is from 3 to 50 and the default value is 3.
<b>Receive Interval</b>	Enter the minimum time interval, in milliseconds, at which the system can receive the control packets from the BFD peer. The range is from 300 to 60000 milliseconds and the default value is 300 milliseconds.
<b>Transmit Interval</b>	Enter the minimum time interval, in milliseconds, at which the local system can send the BFD control packets. The range is from 300 to 60000 milliseconds and the default value is 300 milliseconds.

6 Click the Plus (+) Icon to add details of more peers.

7 Click **Save Changes**.

Peer Address	Local Address	Multihop	Timers	Order
172.21.1.1	127.21.1.20	<input checked="" type="checkbox"/> Enabled	Detect Multiplier: 3 Receive Interval: 300 Transmit Interval: 300	1
172.21.4.1	172.21.4.20	<input type="checkbox"/> Enabled	Detect Multiplier: 3 Receive Interval: 300 Transmit Interval: 300	2

## Results

When you configure BFD rules for a profile, the rules are automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge. See [Configure BFD for Edges](#) for more information.

## What to do next

VMware SD-WAN supports configuring BFD for BGP and OSPF.

- To enable BFD for BGP, see [Configure BFD for BGP for Profiles](#).
- To enable BFD for OSPF, see [Configure BFD for OSPF](#).

- To view the BFD sessions, see [Monitor BFD Sessions](#).
- To view the BFD events, see [Monitor BFD Events](#).
- For troubleshooting and debugging BFD, see [Troubleshooting BFD](#).

## Configure BFD for Edges

VMware SD-WAN allows to configure BFD sessions to detect route failures between two connected entities. Once you have configured BFD rules for a Profile, the rules are automatically applied to the Edges that are associated with the profile. Optionally, you can override the inherited settings at the Edge level.

### What to do next

To override the configuration for a specific Edge:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- 2 Click the Device Icon next to an Edge, or click the link to an Edge and then click the **Device** tab.
- 3 In the **Device** tab, scroll down to the **BFD Rules** section.
- 4 Select the **Override** check box to modify the BFD configuration settings for the selected Edge.

	Peer Address	Local Address	Multihop	Timers	Order
<input type="checkbox"/>	172.21.1.1	172.21.1.20	<input checked="" type="checkbox"/> Enabled	Detect Multiplier: 3 Receive Interval: 300 Transmit Interval: 300	1
<input type="checkbox"/>	172.21.4.1	172.21.4.20	<input type="checkbox"/> Enabled	Detect Multiplier: 3 Receive Interval: 300 Transmit Interval: 300	2

- 5 Click **Save Changes**.

VMware SD-WAN supports configuring BFD for BGP and OSPF.

- To enable BFD for BGP, see [Configure BFD for BGP for Profiles](#).
- To enable BFD for OSPF, see [Configure BFD for OSPF](#).
- To view the BFD sessions, see [Monitor BFD Sessions](#).

- To view the BFD events, see [Monitor BFD Events](#).
- For troubleshooting and debugging BFD, see [Troubleshooting BFD](#).

## Configure BFD for BGP for Profiles

You can configure BFD for BGP on SD-WAN Profiles.

By default, BFD is deactivated in BGP neighbor. You can enable BFD for a BGP session to subscribe to BFD session updates.

Enabling BFD for a BGP neighbor does not create a BFD session. You must explicitly configure a BFD session. See [Configure BFD for Profiles](#).

The following procedure describes how to enable BFD for an already configured BGP session on an Edge. To configure BGP settings, see [Configure BGP from Edge to Underlay Neighbors for Profiles](#).

To enable BFD for BGP on partner Gateways, you must be an Operator super user. For more information, see the [Configure Partner Handoff](#) section in the *VMware SD-WAN Operator Guide*.

### Procedure:

#### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Profiles**.
- 2 Click the **Device** Icon for a profile, or select a profile and click the **Device** tab.
- 3 In the **Device** tab, scroll down to the **Routing & NAT** section and click the arrow next to **BGP** to open the BGP section.
- 4 Click the slider to **ON** position.
- 5 In the **BGP Editor** window, click **view all** in the **Additional Options** column for a BGP neighbor and select the **Enable BFD** check box. You can enable a BFD subscription for multiple BGP neighbors, including NSD Neighbors in the 4.3 release. NOTE: Multihop must be configured as Multihop BFD for NSD BGP Neighbors in the 4.3 release. For more information about NSD Neighbors, see section titled, [Configure BGP Over IPsec from Edge to Non SD-WAN Neighbors](#).

	ASN *	Inbound Filter	Outbound Filter	Additional Options
<input type="checkbox"/>	200	[None] <input type="button" value="▼"/>	[None] <input type="button" value="▼"/>	<input type="checkbox"/> Max-Hop <input type="checkbox"/> Local IP <input type="checkbox"/> Uplink <input type="button" value=" ⓘ"/> <input type="checkbox"/> Allow AS <input type="button" value=" ⓘ"/> <input type="checkbox"/> Default Route <input type="button" value=" ⓘ"/> <input checked="" type="checkbox"/> Enable BFD <input type="button" value=" ⓘ"/>

**Note** A single-hop BFD session is not supported for BGP over IPsec from the SD-WAN Edge.

- Configure the other settings as required and click **OK**.

## Results

When you enable BFD for BGP settings in a profile, the setting is automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge. See [Configure BFD for BGP for Edges](#) for more information.

When a BGP neighbor receives an update that BFD session is down, the corresponding BGP session immediately goes down and the routes learnt through the BGP peer are flushed without waiting for the expiry of keepalive timer.

## Configure BFD for BGP for Edges

You can override the inherited settings at the Edge level for BFD for BGP.

To override the configuration for a specific Edge:

- In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- Click the **Device** icon next to an Edge, or click the link to an Edge and then click the **Device** tab.
- In the **Device** tab, scroll down to the **Routing & NAT** section, and then scroll down and click **BGP** arrow to open the **BGP** section.
- Click the **Override** check box and move the slider to the **ON** position to modify the BGP settings for the selected Edge.

Neighbors					
	+ ADD	DELETE	CLONE		
	ASN *	Inbound Filter	Outbound Filter	Additional Options	
<input type="checkbox"/>	200	[None] <input type="button" value="▼"/>	<input type="button" value="-"/> <input type="button" value="+"/> [None] <input type="button" value="▼"/>	<input type="button" value="-"/> <input type="button" value="+"/>	<input type="button" value="VIEW LESS"/>
Max-Hop 1 Local IP IP Address Uplink <input type="checkbox"/> Allow AS <input type="checkbox"/> Default Route <input type="checkbox"/> Enable BFD <input checked="" type="checkbox"/>					

## Configure BFD for OSPF

You can configure BFD for OSPF for Profiles.

By default, BFD is deactivated in OSPF. You can enable BFD for OSPF to subscribe to BFD session updates.

Enabling BFD for an OSPF neighbor does not create a BFD session. You must explicitly configure a BFD session. See [Configure BFD for Profiles](#).

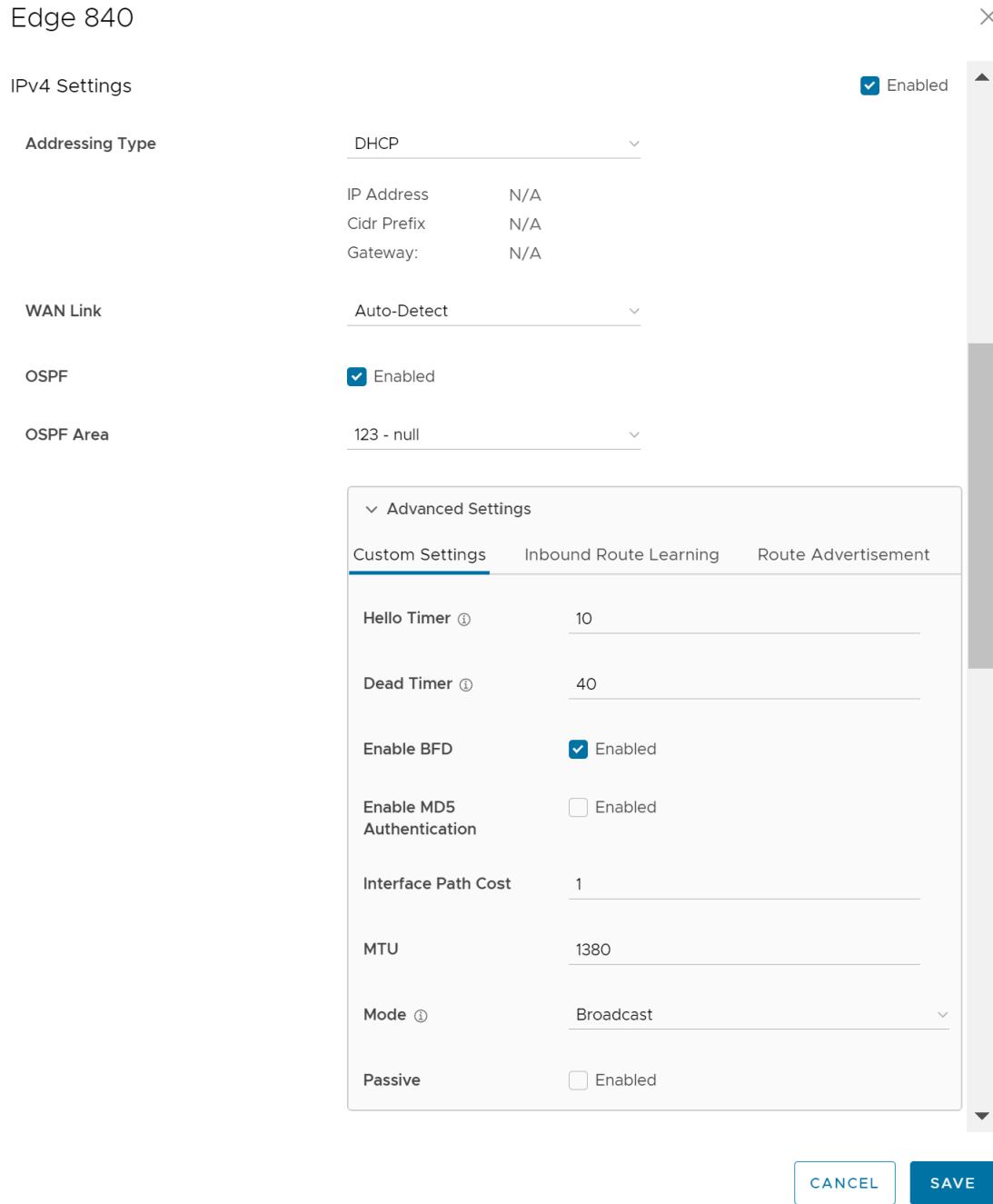
The following procedure describes how to enable BFD for an already configured OSPF session on an Edge Interface. To configure OSPF settings, see [Activate OSPF for Profiles](#).

To configure the Interface settings, see [Configure Interface Settings for Profiles](#).

#### Procedure

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Profiles**.
- 2 Select a profile you want to configure BFD for OSPF settings and click the **View** link in the **Device** column of the Profile. The **Device** page for the selected Profile appears.
- 3 In the **Device** tab, scroll down to the **Connectivity** section and click **Interfaces**. The Edge models available in the selected Profile are displayed.
- 4 In the **Interfaces** section, click an Edge model to view the interfaces available in the Edge and select an interface to edit the settings.

- 5 In the **Interface** edit window, you can configure OSPF settings under **IPv4/IPv6 Settings**. Select the **OSPF** check box and choose the **OSPF Area** from the drop-down list.



- 6 Expand **Advanced Settings** and in the **Custom Settings** tab, select the **Enable BFD** check box.  
 7 Configure the other settings as required and click **Save**.

## Results

When you enable BFD for an OSPF area in a profile, the setting is automatically applied to the corresponding Edges that are associated with the profile. If required, you can override the configuration for a specific Edge . See [Configure BFD for OSPF for Edges](#) for more information.

When an OSPF neighbor receives an update that BFD session is down, the corresponding OSPF session immediately goes down and the routes are flushed without waiting for the expiry of keepalive timer.

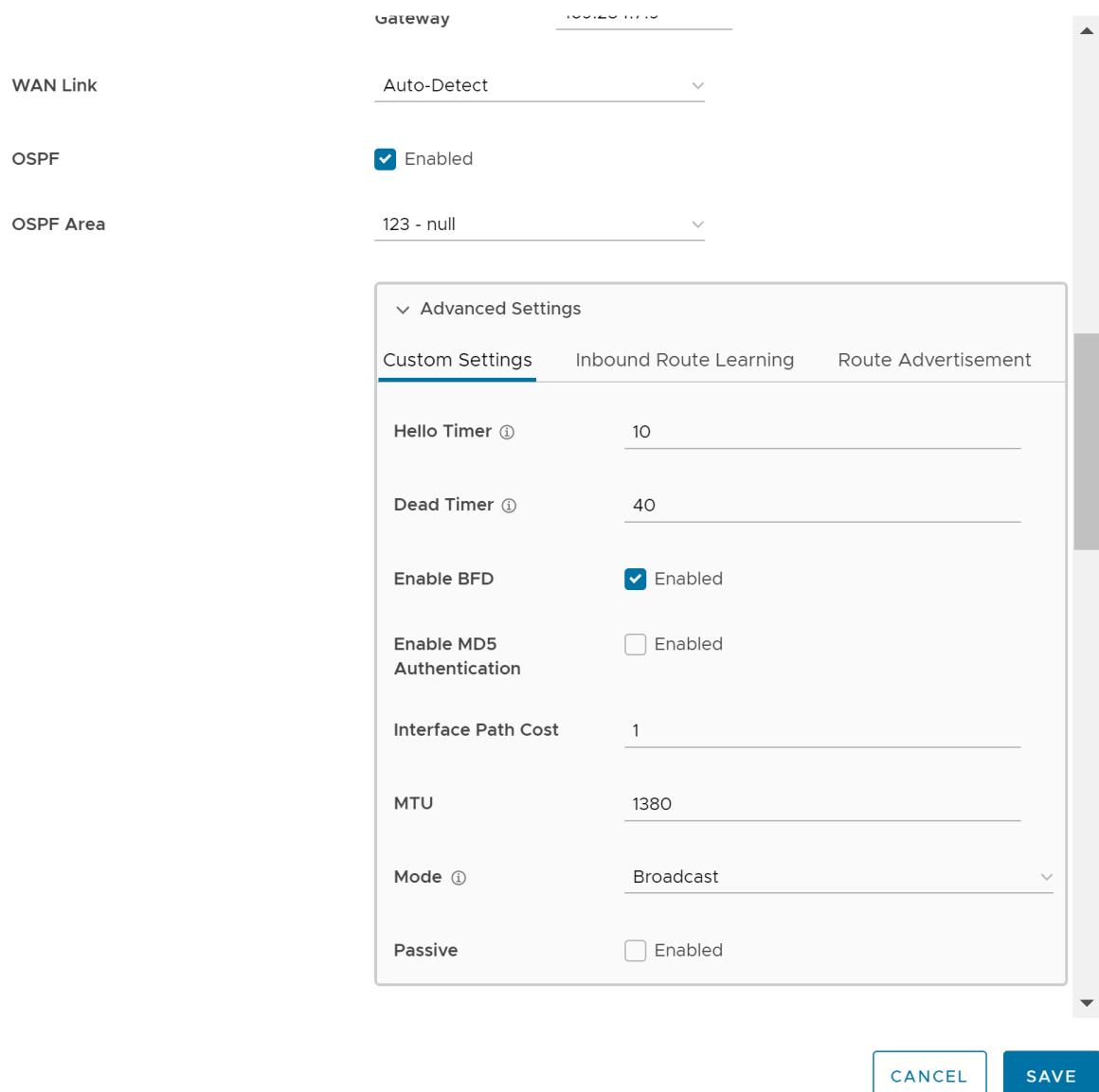
## Configure BFD for OSPF for Edges

You can modify the inherited Profile settings at the Edge level for BFD for OSPF.

If required, you can override the configuration for a specific Edge as follows:

- 1 In the **SD-WAN** service of the Enterprise portal, click **Configure > Edges**.
- 2 Select an Edge you want to configure BFD for OSPF settings and click the **View** link in the **Device** column of the Edge. The **Device** page for the selected Edge appears.
- 3 In the **Device** tab, scroll down to the **Connectivity** section and click **Interfaces**.
- 4 In the **Interfaces** section, click an interface to edit the settings.
- 5 In the **Interface** edit window, you can configure BFD for OSPF settings for the selected Edge under **IPv4/IPv6 Settings** as shown in the following screenshot.

## Virtual Edge



- 6 Expand **Advanced Settings** and in the **Custom Settings** tab, select the **Enable BFD** check box.
- 7 Configure the required settings for the Edge as required and click **Save**.

## Configure BFD for Gateways

You can configure BFD Settings for SD-WAN Gateways over IPsec tunnels.

To configure BFD settings for a Gateway:

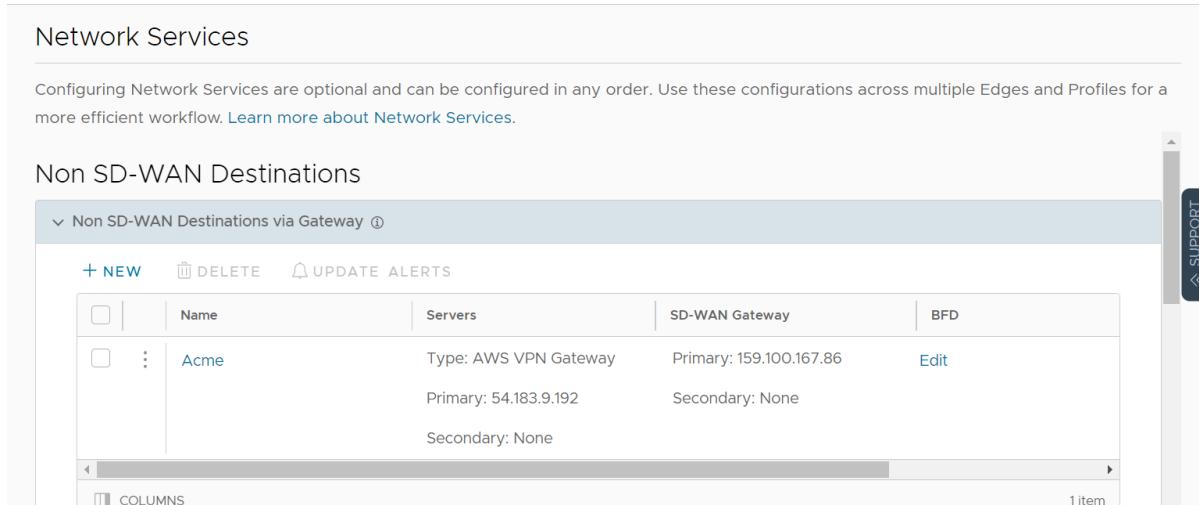
## Prerequisites

Ensure that you have configured the following:

- Create a Non SD-WAN Destination via Gateway for one of the following sites:
  - Configure a Non SD-WAN Destination of Type AWS VPN Gateway
  - Configure a Non SD-WAN Destination of Type Cisco ISR
  - Configure a Non SD-WAN Destination of Type Generic IKEv1 Router (Route Based VPN)
  - Configure a Non SD-WAN Destination of Type Generic IKEv2 Router (Route Based VPN)
  - Configure a Non SD-WAN Destination of Type Microsoft Azure Virtual Hub
- Associate the Non SD-WAN Destination to a Profile See [Configure a Tunnel Between a Branch and a Non SD-WAN Destinations via Gateway](#).

## Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Network Services**.
- 2 In the **Non SD-WAN Destinations via Gateway** area, click the **Edit** link in the **BFD** column that corresponds to the Non SD-WAN Destination.



The screenshot shows the 'Network Services' section of the VMware SD-WAN Administration Guide. Under 'Non SD-WAN Destinations', there is a table with one item named 'Acme'. The table columns are: Name, Servers, SD-WAN Gateway, and BFD. The 'BFD' column for 'Acme' contains an 'Edit' link. A tooltip for 'Non SD-WAN Destinations via Gateway' is visible above the table. The right side of the interface has a vertical support bar with icons for help, search, and refresh.

	Name	Servers	SD-WAN Gateway	BFD
<input type="checkbox"/>	Acme	Type: AWS VPN Gateway Primary: 54.183.9.192 Secondary: None	Primary: 159.100.167.86 Secondary: None	<a href="#">Edit</a>

- 3 In the **BFD Editor** window, move the **BFD Activated** slider to the right to turn it on to configure the BFD settings for the Primary and Secondary Gateways.
- 4 Configure the BFD settings, as described in the table below.

**Note** The Secondary Gateway option is available only if you have configured a secondary Gateway for the corresponding Non SD-WAN Destination.

## Edit BFD

	Tunnel Type	Peer Address	Local Address	Multihop	Timers	Order
<input type="checkbox"/>	Primary	10.0.0.12	10.0.100.12	<input checked="" type="checkbox"/> Enabled	Detect Multiplier 3 Receive Interval 300 Transmit Interval 300	1

1 item

Field	Description
Peer Address	Enter the IP address of the remote peer to initiate a BFD session.
Local Address	Enter a locally configured IP address for the peer listener. This address is used to send the packets.
Multihop	This option is not supported for the Gateways.
Detect Multiplier	Enter the detection time multiplier. The remote transmission interval is multiplied by this value to determine the detection timer for connection loss. The range is from 3 to 50 and the default value is 3.
Receive Interval	Enter the minimum time interval, in milliseconds, at which the system can receive the control packets from the BFD peer. The range is from 300 to 60000 milliseconds and the default value is 300 milliseconds.
Transmit Interval	Enter the minimum time interval, in milliseconds, at which the local system can send the BFD control packets. The range is from 300 to 60000 milliseconds and the default value is 300 milliseconds.

**Note** BFD is supported only on VTP Tunnels.

## Monitor BFD Sessions

You can monitor the BFD sessions on Edges and Gateways.

To view the BFD sessions:

- In the **SD-WAN** Service of the Enterprise portal, go to **Monitor > Routing**.
- In the **Routing** screen, click the **BFD** tab.

**Note** You can click the Filter Icon next to the **Search** option and choose to filter the details by different categories.

The **Edge BFD Sessions** screen displays the BFD sessions on Edge and Gateway.

Edge	Segment	Peer Address	Local Address	State	Remote Timers	Local Timers	Events	Session Time
bl-hub3	Global Segment	11991	172.21.1.20	Down	rx: 300ms / tx: 300ms	rx: 300ms / tx: 300ms	10 View	
bl-hub2	Global Segment	11991	172.21.1.10	Down	rx: 300ms / tx: 300ms	rx: 300ms / tx: 300ms	104 View	
bl-hub1	Global Segment	11991	172.21.1.2	Down	rx: 300ms / tx: 300ms	rx: 300ms / tx: 300ms	120 View	12 minute(s), 29 second(s)
b4-hub-edge2000	Global Segment	14.1.1	14.1.1.100	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	87 View	22 second(s)
b4-hub-edge2000	segment1	14.1.1	14.1.1.100	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	33 View	15 minute(s), 10 second(s)
b4-hub-edge2000	segment2	14.1.2.1	14.1.1.102	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	120 View	21 hour(s), 56 minute(s), 55 second(s)
b9-edge1_E540	Global Segment	19.1.1	19.1.1.100	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	120 View	1 day(s), 14 hours(s), 44 minute(s), 33 second(s)
bl-hub2	Global Segment	172.21.1.11	172.21.1.10	Down	rx: 1000ms / tx: 1000ms	rx: 300ms / tx: 300ms	120 View	

Gateway	Segment	Peer Address	Local Address	State	Remote Timers	Local Timers	Events	Session Time
No BFD events available for selected enterprise								

The BFD sessions include the following details for the Edges and Gateways:

- Name of the Edge or Gateway
- Segment name
- Peer IPv4 or IPv6 address
- Local IPv4 or IPv6 address
- State of the BFD session
- Remote and Local timers
- Number of Events
- Duration of the BFD session

Click the link to an event number to view the break-up details of the events.

## Monitor BFD Events

You can view the events related to the BFD sessions.

In the **SD-WAN** service of the Enterprise portal, click **Monitor > Events**.

To view the events related to BFD, you can use the filter option. Click the **Filter** icon next to the **Search** option and choose to filter the details by different categories.

The following image shows some of the BFD events.

Event	User	Segment	Edge	Severity	Time	Message
Edge BFDv6 neighbor unavailable		Global Segment	bl-hub1	Info	Jul 14, 2021, 4:41:29 PM	BFDv6 session down for edge [bl-hub1] to peer: [1600.172.211.1]
BFDv6 session established to edge neighbor		Global Segment	bl-hub1	Info	Jul 14, 2021, 3:19:26 PM	BFDv6 session up for edge [bl-hub1] to peer: [1600.172.211.1]
Edge BFDv6 neighbor unavailable		Global Segment	bl-hub1	Info	Jul 14, 2021, 3:18:52 PM	BFDv6 session down for edge [bl-hub1] to peer: [1600.172.211.1]
BFDv6 session established to edge neighbor		Global Segment	bl-hub1	Info	Jul 14, 2021, 9:45:59 AM	BFDv6 session up for edge [bl-hub1] to peer: [1600.172.211.1]
Edge BFDv6 neighbor unavailable		Global Segment	bl-hub1	Info	Jul 14, 2021, 9:44:59 AM	BFDv6 session down for edge [bl-hub1] to peer: [1600.172.211.1]
BFDv6 session established to edge neighbor		Global Segment	bl-hub1	Info	Jul 14, 2021, 9:12:55 AM	BFDv6 session up for edge [bl-hub1] to peer: [1600.172.211.1]
Edge BFDv6 neighbor unavailable		Global Segment	bl-hub1	Info	Jul 14, 2021, 9:00:39 AM	BFDv6 session down for edge [bl-hub1] to peer: [1600.172.211.1]
BFDv6 session established to edge neighbor		Global Segment	bl-hub1	Info	Jul 14, 2021, 1:38:31 AM	BFDv6 session up for edge [bl-hub1] to peer: [1600.172.211.1]
Edge BFDv6 neighbor unavailable		Global Segment	bl-hub1	Info	Jul 14, 2021, 1:36:35 AM	BFDv6 session down for edge [bl-hub1] to peer: [1600.172.211.1]
BFDv6 session established to edge neighbor		Global Segment	bl-hub1	Info	Jul 14, 2021, 1:06:26 AM	BFDv6 session up for edge [bl-hub1] to peer: [1600.172.211.1]
Edge BFDv6 neighbor unavailable		Global Segment	bl-hub1	Info	Jul 14, 2021, 1:05:57 AM	BFDv6 session down for edge [bl-hub1] to peer: [1600.172.211.1]
BFDv6 session established to edge neighbor		Global Segment	bl-hub1	Info	Jul 14, 2021, 12:52:51 AM	BFDv6 session up for edge [bl-hub1] to peer: [1600.172.211.1]
Edge BFDv6 neighbor unavailable		Global Segment	bl-hub1	Info	Jul 14, 2021, 10:39:11 PM	BFDv6 session down for edge [bl-hub1] to peer: [1600.172.211.1]
BFDv6 session established to edge neighbor		Global Segment	bl-hub1	Info	Jul 13, 2021, 10:27:45 PM	BFDv6 session up for edge [bl-hub1] to peer: [1600.172.211.1]

The following are the events related to BFD sessions.

- BFD session established to Gateway neighbor
- BFD session established to edge neighbor
- BFDv6 session established to edge neighbor
- Edge BFD Configuration
- Edge BFD IPv6 Configuration
- Edge BFD neighbor unavailable
- Edge BFDv6 neighbor unavailable
- Gateway BFD neighbor unavailable

## Troubleshooting BFD

You can run Remote Diagnostics tests to view the logs of the BFD sessions and use the log information for troubleshooting purposes.

To run the tests for BFD:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Diagnostics > Remote Diagnostics**.
- 2 The **Edges** page displays all the active Edges.
- 3 Select the Edge that you want to troubleshoot. The Edge enters live mode and displays all the possible Remote Diagnostics tests than you can run on the Edge.
- 4 For troubleshooting BFD, scroll to the following sections and run the tests:
  - **Troubleshoot BFD - Show BFD Peer Status** – Choose the Segment from the drop-down list. Enter the Peer and Local IP addresses of an already configured BFD session. Click **Run** to view the details of the BFD peers.
  - **Troubleshoot BFD - Show BFD Peer counters** – Choose the Segment from the drop-down list. Enter the Peer and Local IP addresses of an already configured BFD session. Click **Run** to view the details of counters of the BFD peers.
  - **Troubleshoot BFD - Show BFD Setting** – Click **Run** to view the details of BFDv4 settings and status of neighbors.
  - **Troubleshoot BFD6 - Show BFD6 Setting** – Click **Run** to view the details of BFDv6 settings and status of neighbors.

For more information about all the supported BFP related Remote Diagnostics tests, see the "Remote Diagnostic Tests on Edges" section in the VMware SD-WAN Troubleshooting Guide published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

## Overlay Flow Control

The **Overlay Flow Control** page displays a summarized view of all the routes in your network.

For the 4.3 release, a new NSD bucket has been introduced for the classification of NSD Routes. The new NSD bucket preference logic will be applicable only when the **Use NSD policy** is enabled along with the **Distributed Cost Calculation**. The **Use NSD policy** can only be enabled after you enable the **Distributed Cost Calculation**.

You can view and edit the global routing preferences and the advertise actions for the Edges, Hubs, Partner Gateways, and Non SD-WAN Destinations via Edge and Gateway.

In the **SD-WAN** Service of the Enterprise portal, click **Configure > Overlay Flow Control**.

To configure the Overlay Flow Control settings, perform the following steps:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Overlay Flow Control**.

The screenshot shows the 'Overlay Flow Control' page under the 'Edge Configuration' section. It includes tabs for 'IPv4' and 'IPv6'. A 'Refresh Routes' section allows for recalculating preferences, with a 'YES' input field and a 'REFRESH ROUTES' button. Below this are sections for 'VRF Global Routing Preferences' (listing 'Preferred VPN Exits' and 'Global Advertise Flags') and 'Routes List'. The 'Routes List' section features a search bar, CSV export, and buttons for 'EDIT SUBNET', 'PIN LEARNED ROUTE PREFERENCE', and 'RESET LEARNED ROUTE PREFERENCE'. A table lists 15 routes with columns for IP Subnet, Preferred VPN Exits, Route Type, Segment, Last Update, and Created On. Most routes are connected to 'b1-edge1' or 'b5-edge1' and are categorized as 'Global Segment'.

	IPv4 Subnet	Preferred VPN Exits	Route Type	Segment	Last Update	Created On
<input type="checkbox"/>	10.0.1.0/24	b1-edge1	Connected	Global Segment		
<input type="checkbox"/>	172.16.1.0/29	none	Connected (b1-edge1)	Global Segment		
<input type="checkbox"/>	1.1.0.1/32	b1-edge1	Connected	Global Segment		
<input type="checkbox"/>	1.1.0.2/32	b1-edge1	Connected	Global Segment		
<input type="checkbox"/>	10.0.2.0/24	b2-edge1	Connected	Global Segment		
<input type="checkbox"/>	1.2.0.1/32	b2-edge1	Connected	Global Segment		
<input type="checkbox"/>	10.0.3.0/24	b3-edge1	Connected	Global Segment		
<input type="checkbox"/>	1.3.0.1/32	b3-edge1	Connected	Global Segment		
<input type="checkbox"/>	10.0.4.0/24	b4-edge1	Connected	Global Segment		
<input type="checkbox"/>	1.4.0.1/32	b4-edge1	Connected	Global Segment		
<input type="checkbox"/>	10.0.5.0/24	b5-edge1	Connected	Global Segment		
<input type="checkbox"/>	172.16.5.0/29	none	Connected (b5-edge1)	Global Segment		
<input type="checkbox"/>	1.5.0.1/32	b5-edge1	Connected	Global Segment		

The Overlay Flow Control page displays the following details:

Option	Description
Preferred VPN Exits	Displays the priority of the destinations to where the traffic should be routed.
Global Advertise Flags	Displays the advertise actions of static, connected, internal, external, and uplink routes.
Routes List	Displays all routes. You can change the Preferred VPN Exits order for a particular subnet by clicking <b>Edge Subnet</b> in the <b>Overlay Flow Control</b> page.

- 2 In the **Overlay Flow Control** page, you can configure the following settings:

- **Edit** – Click to update the priorities and the advertise actions. See [Configure Global Routing Preferences](#).
- **Refresh Routes** – This option is available only when the **Distributed Cost Calculation** feature is enabled by the Operator. By default, the Orchestrator is actively involved in learning the dynamic routes. Edges and Gateways rely on the Orchestrator to calculate initial route preferences and return them to the Edge and Gateway. The **Distributed Cost Calculation** feature enables to distribute the route cost calculation to the Edges and Gateways. For IPv4, this option is available only when the **Distributed Cost Calculation** feature is enabled by Operator. For IPv6, **Distributed Cost Calculation** is enabled by default. The Operator cannot turn off this feature for IPv6.

For more information on **Distributed Cost Calculation**, refer to the **Configure Distributed Cost Calculation** section in the *VMware SD-WAN Operator Guide* available at: <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

---

**Note** To enable the **Distributed Cost Calculation** feature, check with your supporting partner. If you are directly supported by VMware, [contact the support team](#).

---

- Type **YES** and then click **Refresh Routes** to make the Edges and Gateways recalculate learned route costs and send them to the Orchestrator. In addition, the changes in the Overlay Flow Control are applied immediately on the new and existing learned routes.

When you refresh the routes, the Customer Enterprise has the following impact on the network:

- All the local dynamic routes are refreshed, and the preference and advertise action of these routes are updated. This updated information is advertised to the Gateway, Orchestrator, and eventually across the Enterprise. As this leads to an update in the routing table, there is a brief impact on the traffic for all the sites.
- Any existing flow using these routes can potentially be affected due to the change in the routing entries.

---

**Note** It is recommended to use **Refresh Routes** in a maintenance window to minimize the impact on the Customer Enterprise.

---

- **VRF Global Routing Preferences** – This option enables you to edit the global routing preferences, advertise actions, and modify the priorities of the destinations to where the traffic should be

The screenshot shows the 'VRF Global Routing Preferences' configuration page. It includes a 'Preferred VPN Exits' section with a priority table and a 'Global Advertise Flags' section for various protocols.

### Default Priority

Order	Header
1.	NSD
2.	Edge
3.	Partner Gateway
4.	Router
5.	Hub

### Global Advertise Flags

Protocol	Flags	Flags	Flags	Flags
Edge	Assigned	Assigned	Assigned	NSD via Edge Assigned
BGP	Advertise External	Advertise External	Advertise External & Internal	BGP Advertise External
OSPF	Advertise External	Advertise External	Advertise Internal	NSD via Gateway Assigned
			Advertise Uplink Routes	Static Routes
			Advertise Uplink Routes	Advertise Internal
			Advertise Internal	Advertise External
			Advertise IntraArea	Advertise Internal
			Advertise InterArea	Advertise External

- Click **Preferred VPN Exits** to prioritize the VPN Exits.

Click **Edit** and use the **UP** and **DOWN** arrows to modify the priorities.

The screenshot shows the 'Edit Preferred VPN' dialog. It has two lists: 'Eligible' and 'Preferred'. The 'Eligible' list contains 'Eligible VPN Exits' and 'NSD'. The 'Preferred' list contains 'Preferred VPN Exits' with items: Edge (Priority 1), Partner Gateway (Priority 2), Router (Priority 3), and Hub (Priority 4). Navigation arrows between the lists are shown.

Eligible	Preferred
<input type="checkbox"/> Eligible VPN Exits	<input type="checkbox"/> Preferred VPN Exits
<input type="checkbox"/> NSD	<input type="checkbox"/> Edge (1)
	<input type="checkbox"/> Partner Gateway (2)
	<input type="checkbox"/> Router (3)
	<input type="checkbox"/> Hub (4)

- In the **Global Advertise Flags** section, select the relevant check boxes to modify the advertise actions for the routes.
- **Routes List** – This section displays the learned routes in the subnets. You can click the IPv4 or IPv6 tab to view the corresponding subnets. The following image shows IPv6 subnets. For more information, see [Configure Subnets](#).

The screenshot shows the VMware SD-WAN Administration Guide interface for Overlay Flow Control. The left sidebar has 'Edge Configuration' selected, with 'Edges', 'Profiles', 'Segments', and 'Overlay Flow Control' listed. The main area is titled 'Overlay Flow Control' with tabs for 'IPv4' and 'IPv6' (selected). A 'Refresh Routes' section contains a note about recalculating preferences and a 'Type "YES"' input field. Below are sections for 'VRF Global Routing Preferences' (with 'Preferred VPN Exits' and 'Global Advertise Flags' subsections) and 'Routes List'. The 'Routes List' section has a search bar and CSV export button. It displays a table of learned routes:

	IPv6 Subnet	Preferred VPN Exits	Route Type	Segment	Last Update	Created On
<input type="checkbox"/>	fd00:0001:0001:0000:0000:0000:0000/64	b1-edge1	Connected	Global Segment		
<input type="checkbox"/>	fd00:ffff:ffff:0001:0000:0000:0000:0000/128	none	Connected (b1-edge1)	Global Segment		
<input type="checkbox"/>	fd00:ffff:ffff:0002:0000:0000:0000:0000/128	none	Connected (b1-edge1)	Global Segment		
<input type="checkbox"/>	fd00:0002:0001:0000:0000:0000:0000:0000/64	b2-edge1	Connected	Global Segment		
<input type="checkbox"/>	fd00:ffff:ffff:0003:0000:0000:0000:0000/128	none	Connected (b2-edge1)	Global Segment		
<input type="checkbox"/>	fd00:0003:0001:0000:0000:0000:0000:0000/64	b3-edge1	Connected	Global Segment		
<input type="checkbox"/>	fd00:ffff:ffff:0004:0000:0000:0000:0000/128	none	Connected (b3-edge1)	Global Segment		
<input type="checkbox"/>	fd00:0004:0001:0000:0000:0000:0000:0000/64	b4-edge1	Connected	Global Segment		
<input type="checkbox"/>	fd00:ffff:ffff:0005:0000:0000:0000:0000/128	none	Connected (b4-edge1)	Global Segment		
<input type="checkbox"/>	fd00:ffff:ffff:0006:0000:0000:0000:0000/128	none	Connected (b5-edge1)	Global Segment		

The bottom panel of the **Overlay Flow Control** window displays the subnets. You can prioritize the preferred destinations for the subnets and pin or unpin learned route preferences. For more information, see [For more information on the subnets, see Configure Subnets](#).

## Configure Global Routing Preferences

In the **Overlay Flow Control** window, you can edit the global routing preferences, advertise actions, and modify the priorities of the destinations to where the traffic should be routed.

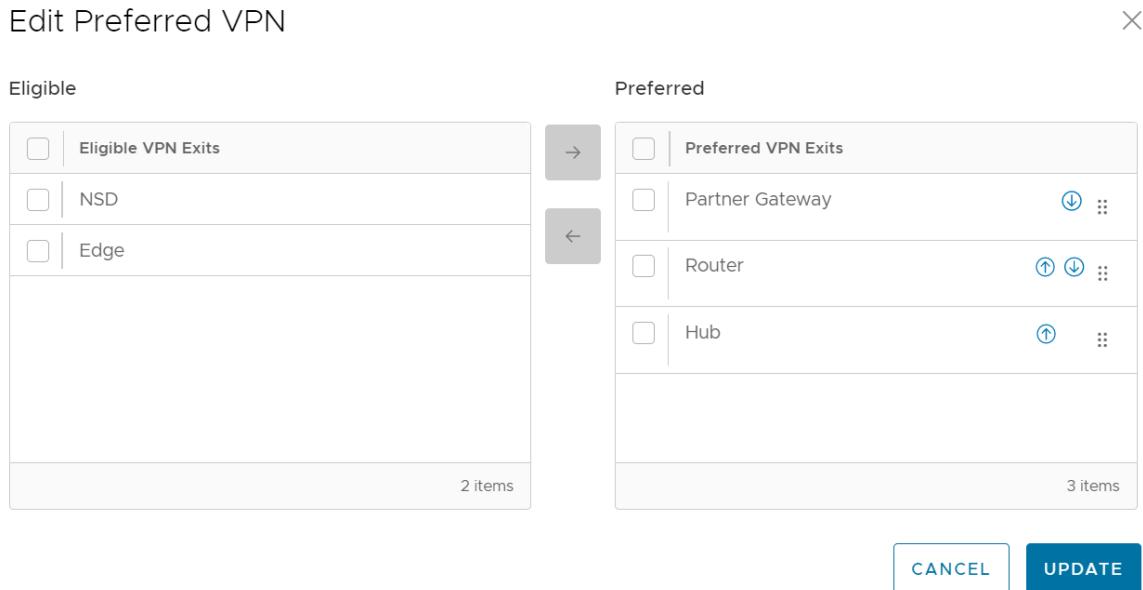
The VRF Global Routing Preferences section displays the **Preferred VPN Exits** and the **Global Advertise Flags** areas. See the Procedure section below for steps to edit these areas.

### Procedure

#### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Overlay Flow Control**.

- 2 In the **Overlay Flow Control** page, click **Preferred VPN Exits** and then click the **Edit** link to open the **Edit Preferred VPN** screen. (See image below).



- 3 You can update the **Preferred VPN Exits** area and click the **UP** and **DOWN** arrows to modify the priorities.
  - 4 In the **Overlay Flow Control** page, click **Global Advertise Flags** to open the **Edit Preferred VPN** screen. (See image below).

Overlay Flow Control					
IPv4		IPv6			
<span>▼ VRF Global Routing Preferences</span> <ul style="list-style-type: none"> <li>&gt; Preferred VPN Exits ⓘ</li> </ul>					
<span>▼ Global Advertise Flags ⓘ</span>					
Edge	Hubs	Partner Gateways	NSD via Edge		
Assigned	Assigned	Assigned	Assigned		
<input checked="" type="checkbox"/> Connected Routes	<input checked="" type="checkbox"/> Connected Routes	<input checked="" type="checkbox"/> Static Routes	<input checked="" type="checkbox"/> Static Routes		
<input checked="" type="checkbox"/> Static Routes	<input checked="" type="checkbox"/> Static Routes	BGP	BGP		
BGP	BGP	<input checked="" type="checkbox"/> Advertise External & Internal	<input checked="" type="checkbox"/> Advertise External		
			<input type="checkbox"/> Advertise Internal		

- a In the **Global Advertise Flags** area, select the relevant check boxes to modify the advertise actions for the routes.
  - b Click **Update** to save the changes.

## Results

The updated settings are displayed in the **Overlay Flow Control** page.

## Configure Subnets

In the **Overlay Flow Control** window, you can update the priorities of the destinations for the learned routes in the subnets.

### Procedure

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Overlay Flow Control**.
- 2 The **Routes List** section of the **Overlay Flow Control** window displays the subnets with the following details, as show in the image and table below.

Segment	Subnet	Preferred VPN Exits	Route Type	Last Update	Created On
	149.174.162.0/...	none	Global Segme...		
	152.122.112.0/24	none	Global Segme...		
>	71.136.165.0/26	APISIM-2-385-SCALE adjacencies	Learned (BGP-E) metrics	Global Segme... May 11, 2023, ...	May 11, 2023, 10:35:38 AM
>	49.116.171.0/26	APISIM-2-986-SCALE adjacencies	Learned (BGP-I) metrics	Global Segme... May 11, 2023, ...	May 11, 2023, 11:08:49 AM

Option	Description
Segment	Segment name.
Subnet	The network that the route corresponds to along with a list of Edges that learned the route.
Preferred VPN Exits	The route through which another branch can access the subnet.
Route Type	Displays the type of the route, which can be one of the following: Static, Connected, or Learned.
Last Update	The last updated date and time of the preferred VPN exit.
Created On	Date and time when the route was created.

Option	Description
IPv4 Subnet	
Eligible VPN Exits	

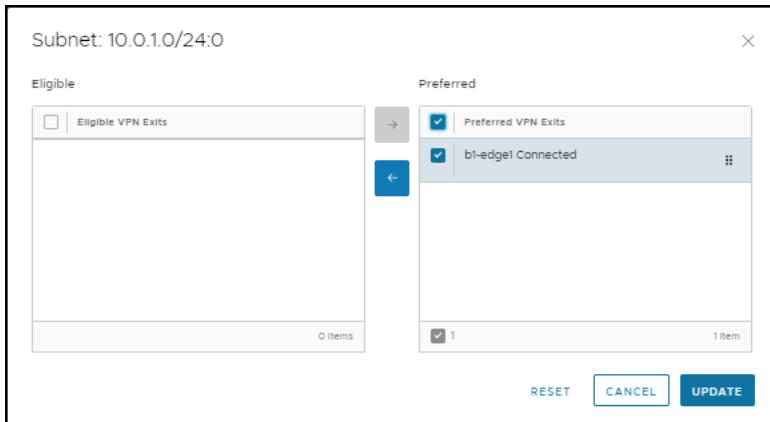
**Note** You can configure the subnets for both IPv4 and IPv6 addresses.

Currently, you can view up to 256 subnet prefixes in the API call request. You can use the Filter option to search for the specific subnet prefix. The following information message appears if the results are more than the server could return. *"There are more results that the server could return. Please narrow your search criteria."*

Select one or more subnets and click **MORE** to perform the following activities:

- **Pin Learned Route Preference** – Pins the preferences of the selected learned route.
- **Unpin Learned Route Preference** – Unpins the preference of the selected learned route to default settings.
- **Delete Learned Routes** – Deletes the learned routes. This option does not delete the connected routes, static routes, routes from Overlay Flow Control, and routes from Edge Route table. The option is available only when **Configure Distributed Cost Calculation** is turned off.

- 3 Click the **Edit Subnet** option for a subnet to modify the priorities of the preferred destination.
  - a In the **Subnet** window, you can move the destinations from the **Eligible VPN Exits** to **Preferred VPN Exits** and vice versa.



- b In the **Preferred VPN Exits** panel, click the **UP** and **DOWN** arrows to change the priorities and click **Update**.
- c You can reset the cost calculation for the subnets when there are pinned routes available. Click **Reset**, which enables the Orchestrator to clear the pinned routes, recalculate the cost for the selected subnet based on the policy, and send the results to the Edges and Gateways.

---

**Note** For IPv4 Routes, the **Reset** option is available only when **Distributed Cost Calculation** is enabled.

---

**Note** The **Reset** option is available only when Distributed Cost Calculation is enabled.

---

For more information on Distributed Cost Calculation, refer to the **Configure Distributed Cost Calculation** section in the *VMware SD-WAN Operator Guide* available at: <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

# Route Summarization

34

Route Summarization or route aggregation is a method to minimize the number of routes that a router advertises to its neighbor. It consolidates selected route prefixes into a single route advertisement. This differentiates it from regular routing, in which every unique route prefix in a route table is advertised to the neighbor.

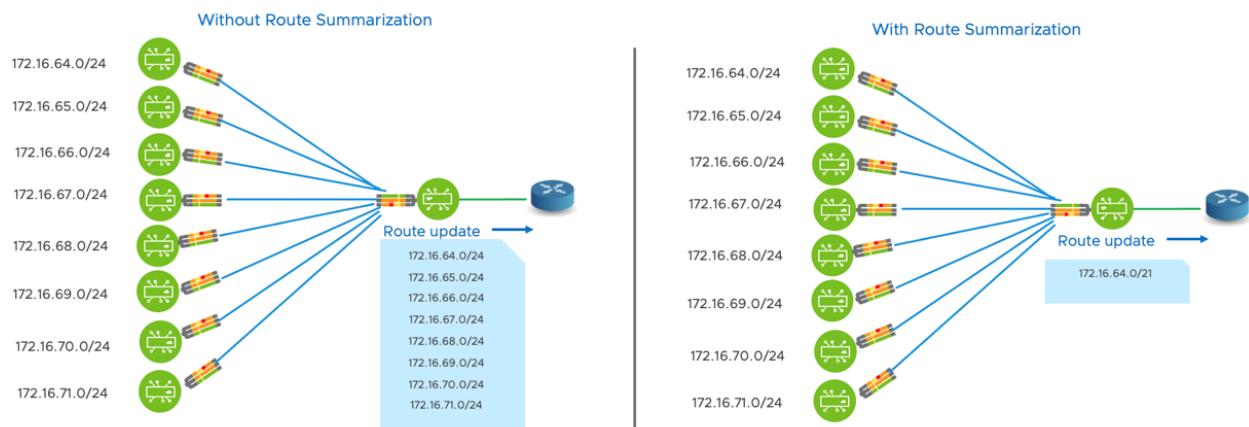
## Overview

Route Summarization or supernetting advertises a single route prefix instead of sending a bunch of contiguous route prefixes. However, with route summarization, there is a need to design the networks with summarization in mind, else, there is a possibility for introducing suboptimal routing and forwarding traffic for unused networks. Similarly, if the router does not find a matching destination route prefix in its routing table for which it advertised the summary prefix, it would drop traffic.

When using the Route Summarization feature, the network administrator must take into consideration the network design before he or she specifies the summarized prefix, which needs to be advertised to its neighbor.

## Route Summarization Use Case

In the below topology a router is learning route prefixes from multiple sources. When the router advertises route prefixes to its neighbor via BGP, it advertises the unique route prefixes. In the example below, it is advertising eight unique route prefixes. Instead, with route summarization, the router can advertise a single summary prefix to its neighbor via BGP. See image below.



Route summarization is a functionality introduced on the VMware SD-WAN Edge and the Gateway.

- In the case of the VMware SD-WAN Edge:
  - Summary prefix via BGP to a neighbor setup over Routed (LAN) interface
  - Summary prefix via BGP to a neighbor setup over NSD (IPsec/BGP) tunnel
  - Summary prefix via OSPF to a neighbor setup over Routed (LAN) interface
- In the case of the VMware SD-WAN Gateway:
  - Summary prefix via BGP to a neighbor setup over NSD (IPsec/BGP) tunnel
  - Summary prefix via BGP to a Partner Hand off router over the Partner Hand off Interface

### **Black Hole Routing**

A black hole route, also known as a null route, is a network route where traffic gets discarded. In reference to Route Summarization, black hole routing is used to drop traffic to a destination that is a part of a summary route, but not a part of the prefixes that are learned locally. From the 5.2 release, this process is required because when a summary route is advertised to the peer, all of the traffic is destined to the whole supernet summary route, including the destination prefix that is not present in the Edge/Gateway. Whenever a summary route is configured, a black hole route for summary prefix is automatically installed in the route table, and it remains until it's unconfigured.

Read the following topics next:

- [Route Summarization Configuration](#)

## **Route Summarization Configuration**

In the 5.2 release, the Route Summarization feature can be configured in the Orchestrator UI for the following topics below.

---

**Note** For an overview, use case, and information about black hole routing for Route Summarization see the following topic, [Chapter 34 Route Summarization](#) Route Summarization.

---

### **Route Summarization Configuration**

- [Configure BGP from Edge to Underlay Neighbors for Profiles](#)
- [Configure BGP Over IPsec from Edge to Non SD-WAN Neighbors](#)
- [Activate OSPF for Profiles](#)
- [Configure BGP Over IPsec from Gateways](#)
- Configure Hand Off, see the *VMware SD-WAN Operator Guide*

# Configure Alerts and Notifications

35

SASE Orchestrator allows you to configure alerts that notify the Operators, Enterprise Administrators or other support users, whenever an event occurs.

**Note** If you are logged in as a user with Customer support privileges, you can view the Alerts and other objects, but cannot configure them.

In the **SD-WAN** service of the Enterprise portal, click **Service Settings > Alerts & Notifications**. The **Alert Configuration** screen appears.

The screenshot shows the 'Alert Configuration' screen under the 'Service Settings' tab. The left sidebar includes 'Monitor', 'Configure', 'Diagnostics', and 'Service Settings'. Under 'Service Settings', 'Alerts & Notifications' is selected. The main area has tabs for 'Alerts' (selected), 'SNMP Traps', and 'Webhooks'. A 'VIEW' button is in the top right. The 'Alerts' section contains sections for 'Alert Configuration', 'Incident' (with sub-options for Edge Status, Link Status, Edge Configuration, and VNF Configuration), 'Notifications' (with sub-option for Email/SMS), and 'Select Configured SNMP Trap Destination(s)' (status: Not Configured). Below that is 'Select Configured Webhooks' (status: Not Configured).

For information on how to configure Alerts, see [Configure Alerts](#).

For information on how to configure SNMP Traps, see [Configure SNMP Traps](#).

For information on how to configure Webhooks, see [Configure Webhooks](#).

Read the following topics next:

- [Configure Alerts](#)
- [Configure SNMP Traps](#)

- Configure Webhooks

## Configure Alerts

The **Alerts** page in the **Alert Configuration** window allows you to select the events for which the alerts need to be sent. You can also add and edit the contact details of existing admin users.

The alerts can be sent to both, the Operators managing the SASE Orchestrator and the Customers. Alerts sent to the Operators are called **Operator Alerts** (formerly known as Pre-Notifications), and are sent as soon as the event occurs. Alerts sent to the Customers are called **Enterprise Alerts** and are activated only when a Customer turns on the **Enable Enterprise Alerts** option under **Alert Configuration**. **Enterprise Alerts** can be subject to delays as configured by the Enterprise Admin(s).

For example, consider that a Customer has configured the **Link Down** alert delay for 2 minutes. If a WAN link loses communication with the Edge, **Operator Alerts** are sent immediately. **Enterprise Alerts** are sent after a delay of 2 minutes.

## Procedure

- In the **Alert Configuration** window, the **Alerts** tab is displayed by default.

The screenshot shows the VMware SD-WAN Orchestrator interface with the following details:

- Top Navigation:** vmw Orchestrator, Customer derekt-corp, SD-WAN, and a Help icon.
- Left Sidebar:** Service Settings (Alerts & Notifications, Edge Licensing, Gateway Migration, Edge Management, Edge Auto-activation).
- Current Tab:** Service Settings - Service Settings tab is selected.
- Alert Configuration Tab:** Alerts tab is selected (indicated by a blue underline).
- Alert Configuration Section:** Contains a tree view with "Alert Configuration" expanded, showing "Notification Settings".
- Incident Section:** Contains a tree view with "Edge Status" expanded, showing notification settings for "Edge Down" and "Edge Up".
- Link Status Section:** Contains a tree view with "Link Status" expanded, showing notification settings for "Link Down" and "Link Up".
- Edge Configuration Section:** Contains a tree view with "Edge Configuration" expanded, showing notification settings for various edge events: "VPN Tunnel Down", "Edge HA Failover", "Edge CSS Tunnel Up", "Edge CSS Tunnel Down", and "Edge HA Failed".
- VNF Configuration Section:** Contains a tree view with "VNF Configuration" expanded, showing notification settings for "VNF VM Event", "VNF Insertion Event", and "VNF Image Download".
- Bottom Right:** A status bar showing "1055".

- 2 Configure the **Notification Settings** as required.
- 3 Under the **Incident** section, select the check boxes as required, and enter the corresponding **Anti-Flap Delay** time in minutes.

The state change often happens in pairs; for example, it occurs with an edge-down event followed by an edge-up event within a few seconds, and this phenomenon is called flapping. This flapping is caused by management plane network interruptions rather than data plane issues. To prevent the delivery of alert notifications during a quick flap, a delay time has to be configured. If an edge or link returns to its original state within the anti-flap period, an alert is created but is automatically closed without a notification being sent.

The intention of **Anti-Flap Delay** is to cancel paired alerts that happened within the configured delay time period to avoid noises.

#### Note

- The **On/Off** toggle button is automatically set to **On** if all the events are selected.
- Hover over the information icon next to each event for more information.
- You can use the event `ALERT_CONFIGURATION_UPDATED` to filter the events triggered by changes to the Enterprise Alert configurations.

- 4 Expand **Email/SMS** in the **Notifications** section to display the contact details of existing admin users.

NOTIFICATION RECEIVERS						
<a href="#">+ ADD RECEIVER</a>		<a href="#">ADD MULTIPLE EMAILS</a>	<a href="#">DELETE</a>			
<input type="checkbox"/>	Name	Role	Email Address	Phone No	Email <small>(i)</small>	SMS <small>(i)</small>
<input checked="" type="checkbox"/>	5_site_operator@velocloud.net <small>(i)</small>	Superuser	5_site_operator@velocloud.net		<input checked="" type="checkbox"/>	<input type="checkbox"/>
<small>1 item</small>						

- 5 Following contact details are displayed:

Option	Description
Name	This field is auto-populated based on the configured administrators.
Role	Displays the role of the corresponding admin user.
Email Address	Displays the email address of the corresponding admin user.
Phone No	Displays the phone number of the corresponding admin user.
Email	Activate the toggle switch to send email notification to the admin user's email address.

Option	Description
SMS	Activate the toggle switch to send SMS notification to the admin user's mobile number.  <b>Note</b> This option is available only if the admin user has a valid phone number.
Verify	Click to validate the email address and/or phone number of the user.

- 6 Following additional options are available:

Option	Description
Add Receiver	Clicking this option creates a new row for the admin user. Enter the name and phone number.
Add Multiple Emails	Click this option to add multiple email addresses for the admin user. The email addresses must be added in a comma separated list.
Delete	Click this option to delete all the contact details of the selected admin user.

- 7 Expand **Configured Hosts** under **Select Configured SNMP Trap Destination(s)** to display the configured SNMP Traps. You can select one or multiple traps using the dropdown menu.

▼ Select Configured SNMP Trap Destination(s) 1 selected

▼ Configured Hosts

Select one or multiple

2c - 23.14.35.67 X

**Note** If no SNMP Trap is configured, this section displays a link to the **SNMP Traps** page.

- 8 Expand **Configured URL** under **Select Configured Webhooks** to display the configured webhooks. You can select one or multiple webhooks using the dropdown menu.

The screenshot shows a user interface for selecting webhooks. At the top, there is a section titled "Select Configured Webhooks" with a green button labeled "1 selected". Below this, a dropdown menu is open, showing the option "https://www.abc.com" with an "X" icon to its right. A downward arrow icon is located to the right of the dropdown menu.

**Note** If no webhook is configured, this section displays a link to the **Webhooks** page.

- 9 Click **Save Changes**.

## Configure SNMP Traps

Simple Network Management Protocol (SNMP) Traps are notifications sent to an SNMP Agent to indicate that an event has occurred. SASE Orchestrator sends SNMP Traps corresponding to the existing alerts like **Edge Down** and **Edge Up**.

- The **SNMP Traps** page in the **Alert Configuration** window, allows you to configure v2c and v3 SNMP Trap Destinations.

**Note** Currently, only SHA-1 and AES-128 algorithms are supported for SNMP v3 Trap.

The screenshot shows the "SNMP Traps" configuration page. At the top, there are three tabs: "Alerts", "SNMP Traps" (which is selected), and "Webhooks".

**v2c SNMP Trap Destinations:**

<input type="checkbox"/>	Hostname / IP Address *	Port *	Community *	Verify
<input type="checkbox"/>	12.23.34.45	162	public	Verify

1 item

**v3 SNMP Trap Destinations:**

<input type="checkbox"/>	Hostname / IP Address *	Port *	Username *	Authentication	Encryption	Verify
<input type="checkbox"/>	12.22.22.34	162	Username	Disabled	Disabled	Verify

1 item

- Following fields are available under **v2c SNMP Trap Destinations**:

Option	Description
Hostname/IP Address	Enter the IP address.
Port	Enter the port number.
Community	Enter the community. Community can be private or public.
Verify	Click this option to validate the IP address.
Add Destination	Click this option to add a new v2c SNMP Trap Destination.
Delete	Click this option to remove the selected entry from the table.

- Following fields are available under **v3 SNMP Trap Destinations**:

Option	Description
Hostname/IP Address	Enter the IP address.
Port	Enter the port number.
Username	Enter the username.
Authentication	Select one of the following: <input type="checkbox"/> MD5 <input type="checkbox"/> SHA Displays <b>Disabled</b> by default.
Encryption	Select one of the following: <input type="checkbox"/> DES <input type="checkbox"/> AES Displays <b>Disabled</b> by default.
Verify	Click this option to validate the IP address.

- Click **Save Changes** to save the configured SNMP Trap Destinations.

## Configure Webhooks

Webhooks deliver data to other applications, triggered by certain alerts using HTTP POST. Whenever an alert occurs, the source sends an HTTP request to the target application configured for the webhook. SASE Orchestrator supports Webhooks that automatically send messages through HTTP POST to target apps when an event occurs. You can set the target URL in the Enterprise portal and automate actions in response to the alerts triggered by SASE Orchestrator. The webhook recipients must support HTTPS and must have valid certificates, to ensure the privacy of potentially sensitive alert payloads. This also prevents the tampering

of payloads. Any application that supports incoming webhooks with HTTPs can integrate with VMware SD-WAN.

The **Webhooks** page in the **Alert Configuration** window, allows you to configure the following details:

Configure Webhooks					
<a href="#">+ ADD WEBHOOK</a>		<a href="#">DELETE</a>			
	URL *	Code * ⓘ	Secret	JSON Payload Template ⓘ	Verify
<input type="checkbox"/> >	https://www.abc.com	200	secret	<a href="#">Configure Payload Template</a>	<a href="#">Verify</a>
1 item					

Option	Description
URL	Enter a valid HTTPS URL. This serves as the target application for the webhooks.
Code	<p>Enter an expected HTTP response status code for each webhook recipient. By default, the SASE Orchestrator expects webhook recipients to respond to HTTP POST requests with a status code as <b>HTTP 200</b>.</p> <p>When SASE Orchestrator receives an unexpected status code from a recipient server or a proxy server, it considers that the alert delivery has failed, and generates an <code>ALERT_DELIVERY_FAILED</code> customer event. This event helps to identify when a webhook recipient server may fail to function as expected.</p>

Option	Description
Secret	<p>This field is optional. Specify a secret token for each configured webhook recipient, which is used to compute an HMAC for each webhook request sent to the corresponding recipient. The HMAC is embedded in a <code>X-Webhook-Signature</code> HTTP header, along with a version parameter, which identifies the signature algorithm and a timestamp.</p> <pre data-bbox="820 481 1264 530"><code>X-Webhook-Signature: v=&lt;signature-version&gt;&amp;t=&lt;timestamp&gt;&amp;s=&lt;hmac&gt;</code></pre> <p>The recipient interprets the components as follows:</p> <ul style="list-style-type: none"> <li>■ v: Version of the algorithm used to produce the signature. The only supported value is <b>1</b>.</li> <li>■ t: Millisecond-precision epoch timestamp corresponding to the time at which the request is issued.</li> <li>■ s: HMAC computed by SASE Orchestrator. The HMAC is computed as follows: <code>HMAC-SHA256(request-body + '.' + timestamp, secret)</code>.</li> </ul> <p>The message used to compute the HMAC is formed by concatenating the request body, a single period, and the value of the timestamp parameter that appears in the signature header. The specific HMAC algorithm used to produce the code is HMAC-SHA256.</p> <p>After receiving a Webhook request, the listening server can verify the authenticity of the request by computing its own HMAC-SHA256 signature according to the same algorithm and compare the newly-computed signature with the one generated by the SASE Orchestrator.</p>
JSON Payload Template	<p>This is a required field. SASE Orchestrator delivers alert notifications to each webhook recipient, through a JSON payload contained within the body of an outgoing HTTP POST request. SASE Orchestrator generates payload content dynamically, as notifications are sent by performing variable interpolation. The supported placeholder variables in the user-configured payload template are replaced with alert-specific values.</p>
Verify	<p>Click this option to validate the entered details.</p>

Click **Configure Payload Template** link under the **JSON Payload Template** option to configure the following:

## Configure Payload Template

X

<b>Alert Time</b>	mm/dd/yyyy hh:mm	
<b>Alert Type</b>	N/A	
<b>Customer Logical ID</b>	Customer Logical ID	
<b>Customer</b>	Customer	
<b>Device Logical ID</b>	Device Logical ID	
<b>Device Description</b>	Device Description	
<b>Device Serial Number</b>	Device Serial Number	
<b>Device Name</b>	Device Name	
<b>Last Contact</b>	mm/dd/yyyy hh:mm	
<b>VCO</b>	VCO	
<b>Message</b>	Message	
<b>Entity Affected</b>	Entity Affected	

 CANCEL SAVE

Option	Description
Alert Time	Enter the date and time at which the alert must be triggered.
Alert Type	Select the type of alert from the dropdown menu. By default, it is displayed as <b>N/A</b> .
Customer Logical ID	Enter the logical ID of the customer to whom the notification must be sent.
Customer	Enter the name of the customer to whom the notification must be sent.
Device Logical ID	Enter the logical ID of the Edge to which the alert must be applied.
Device Description	Enter a brief message describing the Edge to which the alert must be applied.
Device Serial Number	Enter the serial number of the Edge to which the alert must be applied.
Device Name	Enter the name of the Edge to which the alert must be applied.
Last Contact	Enter the date and time at which the affected Edge most recently communicated with the SASE Orchestrator. This is applicable only for the Edge alerts.
VCO	Enter the Hostname or public IP of the SASE Orchestrator from which the notification must be sent.
Message	Enter a brief message describing the event that must trigger the alert.
Entity Affected	Enter the name of the entity: Edge or link or VNF, to which the alert must be applied.

The following example shows a sample JSON payload template:

```
{
  "alertTime": "alertTime",
  "alertType": "alertType",
  "customer": "customer",
  "customerLogicalId": "customerLogicalId",
  "entityAffected": "entityAffected",
  "deviceLogicalId": "deviceLogicalId",
  "lastContact": "lastContact",
  "message": "message",
  "vco": "vco",
  "deviceName": "deviceName",
  "deviceDescription": "deviceDescription",
  "deviceSerialNumber": "deviceSerialNumber"
}
```

Click **Save**, and then click **Save Changes** on the **Webhooks** page to save the webhook configurations.

Whenever an alert is triggered, an alert message along with relevant information is sent to the target URL.

# Testing and Troubleshooting

36

The SASE Orchestrator Test & Troubleshoot functionality provides tools to test the status of the VMware services, perform remote Edge actions, and gather debugging information for an Edge.

In the **SD-WAN** Service of the Enterprise portal, click the **Diagnostics** tab to access and perform the testing and troubleshooting options.

---

**Note** Starting with the 5.1.0 release, all the Troubleshooting and Diagnostics related information for Edges and Gateways is documented and published as a standalone guide titled "*VMware SD-WAN Troubleshooting Guide*" at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

Read the following topics next:

- [Run Remote Diagnostics](#)
- [Remote Actions](#)
- [Diagnostic Bundles for Edges](#)

## Run Remote Diagnostics

VMware SD-WAN supports bi-directional communication with the VMware SD-WAN Edge by using WebSockets. WebSocket is a full-duplex communication protocol over a single TCP connection. WebSockets easily enable communication between a Web browser (or other client applications) and a Web server with much lower overhead than HTTP polling. Remote Diagnostics uses a bi-directional WebSocket connection instead of the live-mode heartbeat mechanism to improve the responsiveness of the Remote Diagnostics in the VMware SASE Orchestrator.

The WebSocket communication involves the following two WebSocket connections for passing WebSocket messages from a Web browser to a VMware SD-WAN Edge and vice versa:

- A WebSocket connection between a Web browser (Orchestrator UI portal) and an Orchestrator. This connection is responsible for all communications with the Web browser and for setting up the system properties needed for establishing a WebSocket connection.
- Another WebSocket connection between an Orchestrator and an Edge. This connection is persistent and setup on Edge activation for processing heartbeats from the Edge and sending back responses to the Orchestrator.

While establishing WebSocket connections between a Web browser and an Edge, in order to ensure Web security against Distributed Denial-of-Service (DDoS) and Cross site request forgery (CSRF) attacks, the browser origin address that is used to access the Orchestrator UI is validated for incoming requests.

In most Orchestrators, the browser origin address/DNS hostname is the same as the value of the `network.public.address` system property. To support scenarios where the address used to access the Orchestrator UI from the browser is different from the value of the `network.public.address` system property, the following system properties are added newly for WebSocket connections:

- `network.portal.websocket.address` - Allows to set an alternate address/DNS hostname to access the UI from a browser if the browser address is not the same as the value of `network.public.address` system property. By default, the `network.portal.websocket.address` system property is not set.
- `session.options.websocket.portal.idle.timeout` - Allows to set the total amount of time (in seconds) the browser WebSocket connection is active in an idle state. By default, the browser WebSocket connection is active for 300 seconds in an idle state.

VMware SASE Orchestrator enables you to run various Remote Diagnostic tests on a selected Edge. To run Remote Diagnostics on an Edge, perform the following steps:

- 1 In the **SD-WAN** Service of the Enterprise portal, click the **Diagnostics** tab.
- 2 The **Remote Diagnostics** page displays the existing Edges.

Name	Status	Model	Software version	Build Number	Created	Software Updated
b1-edge1	Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	
b2-edge1	Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	
b3-edge1	Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	
b4-edge1	Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	
b5-edge1	Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	

- 3 Click the link to an Edge.
- 4 A connection is established to the Edge and the **Remote Diagnostics** window displays all the possible Remote Diagnostics tests than you can run on the Edge.

- Choose an appropriate Remote Diagnostics test to run on the Edge and click **Run**. The diagnostic information is fetched from the Edge and displayed in the screen.

For more information about all the supported Remote Diagnostics tests, see the "Remote Diagnostic Tests on Edges" section in the VMware SD-WAN Troubleshooting Guide published at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

## Remote Actions

You can perform actions like Restarting services, Rebooting, or deactivating an Edge remotely, from the Enterprise portal.

**Note** You can perform the remote actions only on Edge that are in **Connected** state.

- In the **SD-WAN** service of the Enterprise portal, you can perform remote actions from the **Diagnostics > Remote Actions > Edges** navigation path.

	Name	Status	Model	Software version	Build Number	Created	Software Updated
<input type="checkbox"/>	b1-edge1	● Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	
<input type="checkbox"/>	b2-edge1	● Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	
<input type="checkbox"/>	b3-edge1	● Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	
<input type="checkbox"/>	b4-edge1	● Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	
<input type="checkbox"/>	b5-edge1	● Connected	Edge VMware	5.2.0.0	R5200-20221027-MN-95de1ea022	Oct 27, 2022, 7:47:00 PM	

Select an Edge and perform any of the following remote actions:

Action	Description
Restart Service	Restarts the VMware SD-WAN services on the selected Edge.
Reboot	Reboots the selected Edge.
Identify	Randomly flashlights on the selected Edge to identify the device.
Shutdown	Powers off the selected Edge. To restore the Edge, you must remove the power cable, and then plug it back into the Edge.

Action	Description
Deactivate	Resets the device configuration to its factory default state.
Force HA Failover	Forces HA Failover. This option is available only when the Edge is configured with High Availability and the state is HA ready.

- 2 You can also perform the remote actions for an Edge using the **Shortcuts** option available in the **Configure > Edges** or **Monitor > Edges** pages.

See [Chapter 29 Configure Edge Overrides](#) and [Monitor Edges](#).

- 3 Click the **Shortcuts > Remote Actions** and perform any of the actions listed in the above table.

---

**Note** The actions may take up to a minute to run on the device.

---

## Diagnostic Bundles for Edges

Diagnostic bundles allow Operator users to collect all the configuration files and log files into a consolidated Zipped file. The data available in the diagnostic bundles can be used for debugging purposes.

To generate and download Diagnostic Bundles:

- 1 In the **SD-WAN** service of the Enterprise portal, click the **Diagnostics** tab.
- 2 Click **Diagnostic Bundles** to request the following bundles:
  - **Request PCAP Bundle** – The Packet Capture bundle is a collection of the packet data of the network. Operators, Standard Admins and Customer Support can request PCAP bundles. For more information, see [Request Packet Capture Bundle](#).
  - **Request Diagnostic Bundle** – The Diagnostic bundle is a collection of all the configuration and logs from a specific Edge. Only Operators can request Diagnostic bundles. For more information, see [Request Diagnostic Bundle](#).

---

**Note** The **Request Diagnostic Bundle** option is available only for an Operator user. If you are a Partner user or an Enterprise user, you can request for a PCAP Bundle.

---

The generated bundles are displayed in the **Diagnostic Bundles** window.

The screenshot shows the VMware SD-WAN Administration Guide interface. At the top, there are navigation tabs for 'Monitor', 'Configure', 'Diagnostics' (which is selected), and 'Service Settings'. Below the tabs, a search bar and a dropdown menu are present. The main content area is titled 'Diagnostic Bundles' and contains a table with the following data:

	Request Status	Type	Edge	Reason for Generation	User	Generated Date	Cleanup Date
<input checked="" type="checkbox"/>	Complete Download	PCAP	b1-edge1		super@velocloud.net	Nov 10, 2022, 3:34:53 PM	Jan 9, 2023
<input type="checkbox"/>	In Progress	Diagnostics	b1-edge1		super@velocloud.net	Nov 10, 2022, 3:34:35 PM	Jan 9, 2023

At the bottom of the table, there are buttons for 'REQUEST PCAP BUNDLE', 'REQUEST DIAGNOSTIC BUNDLE', 'DOWNLOAD BUNDLE', 'DELETE', and 'MORE'. Below the table, there are 'COLUMNS' and 'REFRESH' buttons, and a note indicating '2 items'.

To download the details of generated bundles, click **More > Download CSV**. The details are downloaded in a CSV file.

## Request Packet Capture Bundle

The Packet Capture bundle collects the packets data of a network. These files are used in analyzing the network characteristics. You can use the data for debugging an Edge device.

To generate a PCAP bundle :

- 1 In the **SD-WAN** Service of the Enterprise portal, click the **Diagnostics** tab.
- 2 Click **Diagnostic Bundles > Request PCAP Bundle**.
- 3 In the **Request PCAP Bundle** window that appears, configure the following:

Request PCAP Bundle

**Target**: b1-edge1

**Interface**: GE5

**Duration**: 5 seconds

**Reason for Generation**: For troubleshooting

**CLOSE**    **SUBMIT**

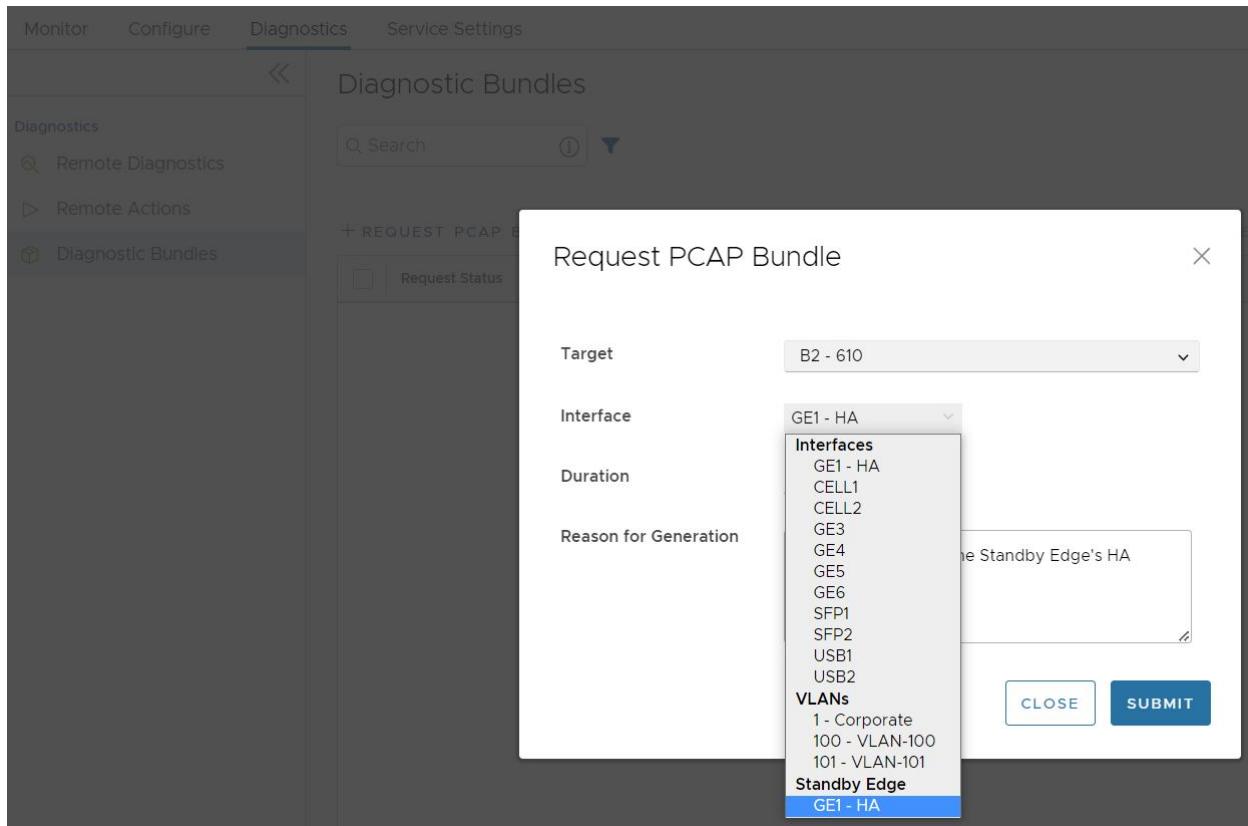
**Table 36-1.**

Option	Description
Target	Choose the target Edge from the drop-down list. The packets are collected from the selected Edge.
Interface	Choose an Interface or a VLAN from the drop-down list. The packets are collected on the selected Interface.
Duration	Choose the time in seconds. The packets are collected for the selected duration.
Reason for Generation	Optionally, you can enter your reason for generating the bundle.

The window displays the details of the bundle being generated, along with the status.

### Packet Capture for Edges configured for High Availability

In Release 5.2.0 and later, a user can request a packet capture for the Standby Edge's HA interface, the interface that connects the Standby Edge to the Active Edge. This option appears at the bottom of the menu and reads: **Standby Edge**, and then lists the HA interface.



## Request Diagnostic Bundle

A Diagnostic bundle is a collection of configuration files, logs, and related events from a specific Edge.

To generate a Diagnostic bundle:

- 1 In the **SD-WAN** Service of the Enterprise portal, click the **Diagnostics** tab.
- 2 Click **Diagnostic Bundles > Request Diagnostic Bundle**.
- 3 In the **Request Diagnostic Bundle** window, configure the following:

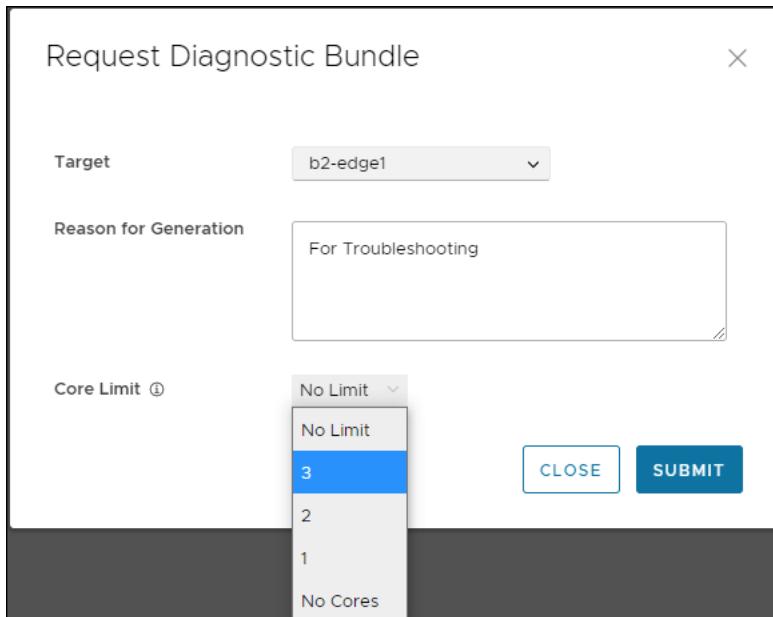


Table 36-2.

Option	Description
Target	Select the target Edge from the drop-down list. The data is collected from the selected Edge.
Reason for Generation	Optionally, you can enter your reason for generating the bundle.
Core Limit	Select a Core Limit value from the drop-down, which is used to reduce the size of the uploaded bundle when the Internet connectivity is experiencing issues.

The **Diagnostic Bundles** window displays the details of the bundle being generated, along with the status.

## Download Diagnostic Bundle

To download the generated Diagnostic bundles:

- In the **Diagnostic Bundles** window, click the **Complete** link or select the bundle and click **Download Bundle**. The bundle is downloaded as a ZIP file.
- For troubleshooting purpose, you can send the downloaded bundle to a VMware Support representative for debugging the data.

## Delete Diagnostic Bundle

The completed bundles get deleted automatically on the date displayed in the **Cleanup Date** column.

- To change the cleanup date, click the link to the cleanup date or choose the bundle and click **More > Update Cleanup Date**.

- 2 In the **Update Cleanup Date** window, choose the date on which the selected bundle should be deleted.
- 3 If you want to retain the bundle, select the **Keep Forever** option, so that the bundle does not get deleted automatically.
- 4 To delete a bundle manually, select the bundle and click **Delete**.

# Edge Licensing

37

Edge Licensing allows a customer to link a software subscription to an Edge. A software subscription is defined by bandwidth, the Edge software edition, Gateway regional geolocation, and subscription duration.

## Edge License Types

The SASE Orchestrator provides different types of licenses for deployed Edges. These license types account for POC deployments where no subscription has been purchased, and production deployments where a variety of license types are available to align with the customer's purchased subscriptions.

### POC Deployments

If an Enterprise is deployed as a proof-of-concept (POC) deployment, choose the POC license. There is only one POC license type available as follows:

**POC | 10 Gbps | North America, Europe Middle East and Africa, Asia Pacific, and Latin America | 60 Months.**

This is the only license that should be chosen for a POC enterprise and the only license used by Edges in the POC enterprise. The Orchestrator does not permit additional licenses to be selected if a POC license is chosen.

### Production Deployments

When an Edge is deployed in a production Enterprise, the license type assigned should align with the software subscription purchased. For example, if the subscription SKU **NB-VC100M-PRE-HO-HG-L34S312P-C** was purchased for use with the Edge being configured, the correct license type would be:

**PREMIUM | 100 Mbps | <Gateway Geolocation Region> | 12 Months** as per the highlighted sections of the SKU.

## Assigning an Edge License Type to a New Edge

When a new Edge is provisioned, the **Provision an Edge** configuration screen includes an **Edge License** drop-down menu. This menu provides a list of available Edge license types which may be assigned to the newly created Edge.

## Provision an Edge

▼ 1. Edge Requirements Name / Model / Profile / License / Authentication / HA / Contact

---

Name *	<input type="text"/>
Model *	Select Model <input type="button" value="▼"/>
Profile * ⓘ	Select Profile <input type="button" value="▼"/>
Edge License *	ENTERPRISE   10 Mbps   North America, Europe Middle <input type="button" value="▼"/>
Authentication ⓘ	Certificate Acquire <input type="button" value="▼"/>
High Availability	<input type="checkbox"/> Enable
<b>Contact</b>	
Local Contact Name *	<input type="text"/> Super User
Local Contact Email *	<input type="text"/> super@velocloud.net

For more information on provisioning a new Edge, see [Chapter 23 Provision a New Edge](#).

**Note** Starting from Release 4.0.0, Edge Licensing is enabled by default, and it is mandatory for a user to assign an Edge license type when creating a new Edge. This requirement helps VMware to track customer subscriptions and simplifies and standardizes the Edge activation report sent by partners.

## Assigning an Edge License Type to an Existing Edge

To assign a license to an existing Edge:

- In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- To assign a license to each Edge, click the link to the Edge, and then select the license in the **Properties** section of the **Edge Overview** page. You can also select the Edge and click **Assign Edge License** to assign the license.
- To assign a license to multiple Edges, select the appropriate Edges, click **Assign Edge License** and select the license.

If the correct license type is not shown for a subscription, contact the supporting partner to assign the license to the enterprise. If the partner is unable to locate the correct license type or if the Enterprise is managed directly by VMware, then contact VMware SD-WAN Support. Until the correct license type is available, another license type can be assigned temporarily. The correct license type should be assigned after it is made available.

If an incorrect Edge license type is chosen, the activation report for that enterprise is incorrect, and the license assignment does not align with the customer's purchases. These licensing inconsistencies are flagged during an audit.

---

**Note** For Edges enabled with High Availability, the Standby Edge gets assigned with the same license type as of the Active Edge.

---

## Edge License Reports

Standard Administrator Superusers, Standard Administrators, Business Specialists, and Customer Support users can view and generate a report of the licenses assigned to their Enterprise.

In the **SD-WAN** Service of the Enterprise portal, click **Service Settings > Edge Licensing**.

Name	Term	Bandwidth	Edition	Region	Edges Assigned
STANDARD   10 Mbps   North America, Europe Middle East and Africa   12 Months	12 Months	10 Mbps	Standard	North America, Europe, Middle East and Africa	1

Click **Download Report** to generate a report of the licenses and the associated Edges in CSV format.

Read the following topics next:

- [Example of Edge Licensing](#)

## Example of Edge Licensing

The following example describes how to assign subscription licenses to Edges as per the Order.

Assume that the Enterprise User has purchased the following:

Product	Description	Quantity
VC-510-HO-36-P	VMware SD-WAN Edge 510 Appliance, Deployment: Hosted Orchestrator for 3 years	11
VC-610-HO-36-P	VMware SD-WAN Edge 610 Appliance, Deployment: Hosted Orchestrator for 3 years	1
VC100M-STD-HO-L34S1-36P	VMware SD-WAN 100 Mbps Standard Service Subscription for 3 years, Prepaid, Hosted Orchestrator, Basic Support Backline (L3-4)	11
VC350M-STD-HO-L34S1-36P	VMware SD-WAN 350 Mbps Standard Software Subscription for 3 year, Prepaid, Hosted Orchestrator, VMware Basic Support Backline(L 3-4)	1

The purchase consists of 12 Edges and 12 Subscription Licenses. You can activate 12 Edges and assign:

- STANDARD | 100Mbps | <*Gateway Geolocation Region*> | 36 Months to **11 Edges**
- STANDARD | 350Mbps | <*Gateway Geolocation Region*> | 36 Months to **1 Edge**

Follow the below process to assign the license type to an Edge.

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- 2 In the Edges screen, click **Add Edge**.
- 3 In the **Provision an Edge** window, configure a new Edge and assign the license type.

## Provision an Edge

1. Edge Requirements Name / Model / Profile / License / Authentication / HA / Contact / Analytics Mode

<b>Mode *</b>	<input checked="" type="radio"/> SD-WAN Edge <input type="checkbox"/> Enable Analytics <input type="radio"/> Analytics Only Edge
<b>Name *</b>	Edge12
<b>Model *</b>	Edge 500
<b>Profile *</b>	Quick Start Profile
<b>Edge License *</b>	<small>STANDARD   10 Mbps   North America, Europe Mic</small>  <small>STANDARD   10 Mbps   North America, Europe Middle East and Africa   12 Months</small> 
<b>Authentication</b>	Certificate Acquire
<b>High Availability</b>	<input type="checkbox"/> Enable
<b>Contact</b>	
<b>Local Contact Name *</b>	Super User

- 4 Repeat configuring new Edges and assign the corresponding Edge licenses.

---

**Note** For Edges enabled with High Availability, the Standby Edge gets assigned with the same license type as of the Active Edge.

---

- 5 To view the list of Edge licenses and the assigned Edges, click **Service Settings > Edge Licensing**.
- 6 Click **Download Report** to download a report of the licenses and the associated Edges in CSV format.

# Edge Software Image Management

38

Read the following topics next:

- [Edge Software Image Management Overview](#)
- [Activate Edge Image Management](#)
- [Edge Image Assignment and Access](#)
- [Edge Management](#)
- [Upgrade SD-WAN Edges](#)

## Edge Software Image Management Overview

The Edge Software Image Management feature provides Enterprise Super Users the ability to upgrade SD-WAN Edge firmware without relying on VMware Support or the Partner.

Traditionally, whenever a new Edge image is published by VMware SD-WAN, the Enterprise Administrators will have to request the VMware support or the Partner to upgrade the software on their enterprise Edges. The VMware Support will then engage with the customer and upgrade all or a subset of the Edges in the customer's network. With the Edge Software Image Management feature activated, the Enterprise customers can manage the Edge software version that runs in their environment. The Edge Software Image Management feature provides Enterprise Super Users the ability to upgrade SD-WAN Edge firmware without relying on VMware Support or the Partner.

Additionally, this feature also enables tagging of a particular Edge software image as deprecated (if it was found defective or not meant to be used) after their release. Enterprises using these deprecated images will be notified so that they can migrate to a more stable release of the Edge image.

---

**Note** Only an Operator user can mark the Edge images as deprecated.

---

## Activate Edge Image Management

The Edge software image management feature is deactivated by default for customers. Only an Operator (or VMware Support) can activate this feature for a Direct Enterprise and the Partner. In turn, the Partners can activate this feature for their Partner Enterprise customers. The feature can

be activated during or after the customer creation. The Enterprises with Edge software image management deactivated must engage with VMware Support or Partner for Edge software upgrades.

## Activate Edge Image Management for SD-WAN Service

### Activate Edge Image Management for New Enterprise Customer

As an Operator User, you can manage the software images assigned to an Enterprise directly by assigning an Operator Profile to an Enterprise or allowing an Enterprise Superuser to manage the available list of software images assigned for an Enterprise by selecting the **Allow Customer to Manage Software** check box in the navigation path **Manage Customer > New Customer > Services > Global Settings**. For more information, see the *Create New Customer* section in the *VMware SD-WAN Operator Guide*.

### Activate Edge Image Management for New Partner Customer

As a Partner Administrator, in addition to managing the software images assigned to your Partner customers, you can allow a Partner Customer's Superuser to manage the available list of software images for the customer by selecting the **Allow Customer to Manage Software** check box in the navigation path **Manage Customer > New Customer > Services > Global Settings**. The list of software images that you can assign to the new customer is based on the available list of software images assigned to the particular Partner by the Orchestrator Operator. For more information, see the *Create New Customer* section in the *VMware SD-WAN Partner Guide*.

### Activate Edge Image Management for Existing Customer

As an Operator User or a Partner Administrator, you can delegate Edge image management to Enterprise or Partner Superusers. To delegate Edge image management to Enterprise Superusers, select the **Allow Customer to Manage Software** check box in the navigation path **Manage Customer > Select a customer > Global Settings > Customer Configuration > SD-WAN > Configure**. For more information, see the *Manage Customers* section in the *VMware SD-WAN Operator Guide*.

To update the Edge image management settings for an existing customer, select the **Edge Image Management** toggle button to **ON** by navigating to **Manage Customers > Select a customer > More > Update Edge Image Management**. When the feature is activated, the default software image is the only assigned software image for the customer. Once the feature is activated, you can assign additional software images post activating the feature.

For more information, see the *Manage Customers* in the *VMware SD-WAN Operator Guide*.

## Edge Image Assignment and Access

Operator and Partner Super users can assign all or subset of Edge images to their customers from the available list of images assigned to them.

Whenever VMware upgrades a hosted Orchestrator to a newer version of VMware SD-WAN, the respective Edge images are uploaded to the Orchestrator. On a hosted Orchestrator, by default, the newly uploaded Edge images are assigned to Partners automatically after successful completion of hosted Orchestrator upgrade. However, the Edge images are not made available automatically to the direct Enterprise customers. The Enterprise customer must contact the VMware support to request access to new Edge images uploaded to the hosted Orchestrator.

On an on-prem or a Partner-managed Orchestrator, the image upload or assignment of the Edge image to the Enterprise customers are largely controlled by the Partner or the service provider who manages and maintains the Orchestrator.

---

**Note** A Partner can assign Edge images to Partner customers from the available list of images assigned to them by the Operator.

---

For detailed VMware SD-WAN Edge software versions and recommended releases, refer <https://knowledge.broadcom.com/external/article?legacyId=80741>.

## Manage Edge Software Image

As an Operator Super User and Operator Standard Administrator, you can upload a new software image, modify the existing software images, deprecate a software image, and delete a software image associated with the Edges. An Edge software image can be deprecated due to one of the following reasons:

- The Edge image has a major bug or vulnerability which is fixed in the subsequent version.
- The Edge image is no longer supported by VMware or it is reaching End Of Life (EOL).

Once the image is deprecated, the image will not appear in the list of available software images or versions to be assigned to Operator Profiles, or Customers or Edges. Also, any Enterprise who has one or more of their Edges running this deprecated image will be notified about the deprecated image when they log into the Orchestrator.

For more information, see the [Edge Management](#).

## Edge Management

Edge Management feature allows you to configure general settings, authentication, and encryption for an Edge. It allows you to activate or deactivate configuration updates for an Edge. You can also select a default Software & Firmware Image.

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Service Settings > Edge Management**.
- 2 You can configure the following options and click **Save Changes**.

## Edge Management

**General Edge Settings**

**Edge Link Down Limit**  Customize (default 1 day)  
Number of days

**Edge Authentication**

**Default Certificate**  Certificate Acquire  Certificate Deactivated  Certificate Required

**Edge Authentication**

**Device Secret Encryption**

**Enable Encrypt Device Secrets**

**Configuration Updates**

**Enable Edge Configuration Updates**  On  
When this option is set to on, configuration updates are actively pushed to Edges. When this option is turned off, pending configuration changes are paused until the setting is turned back on. Note: Edge configuration updates are disabled by default during Orchestrator upgrades.

**Enable Configuration Updates Post-Upgrade**  Off  
This option allows the customer to control when post-Orchestrator upgrade configuration changes are applied to their Edges. During an Orchestrator upgrade, the Operator managing the upgrade pauses all Edge configuration updates automatically, and after the upgrade the Operator resumes these Edge configuration updates. When this option is turned off, the customer prevents the Operator from automatically resuming Edge configuration updates after the Orchestrator is upgraded, and these Edge configuration updates would only resume once the customer turned this setting back on.

**Software & Firmware Images**

Is Default?	Operator Profile	Software & Firmware Images	Description	Used by
<input checked="" type="checkbox"/>	3-site-Operator	5.2.0.0 (build R5200-20230323-MH-fe0c25d5bf)		0
<b>3-site-Operator</b> Description: Software Image: 5.2.0.0 (build R5200-20230323-MH-fe0c25d5bf) Platform Firmware: None (do not update) Modem Firmware: None (do not update) Factory Image: None (do not update) ConfigurationType: Segment Based Orchestrator FQDN Address: Orchestrator IPv4 Address: 10.81.117.120 Orchestrator IPv6 Address: Heartbeat Interval: 5 seconds Time Slice Interval: 30 seconds Stats Upload Interval: 30 seconds				

1 - 1 of 1 items

Option	Description
<b>General Edge Settings</b>	
Edge Link Down Limit	You can set this value for each Edge by selecting the <b>Customize</b> check box. This overrides the value set through the system property <code>edge.link.show.limit.sec</code> .
Number of days	Enter a value in the range <b>1</b> to <b>365</b> . The default value is <b>1</b> .
<b>Edge Authentication</b>	

Option	Description
Default Certificate	<p>Choose the default option to authenticate the Edges associated to the Customer.</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Acquire:</b> This option instructs the Edge to acquire a certificate from the certificate authority of the SASE Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the SASE Orchestrator and for the establishment of VCMP tunnels.</li> </ul> <p><b>Note</b> Only after acquiring the certificate, the option can be updated to <b>Certificate Required</b>.</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Deactivated:</b> This option instructs the Edge to use a pre-shared key mode of authentication.</li> <li>■ <b>Certificate Required:</b> This option is selected by default, and it instructs the Edge to use the PKI certificate. Operators can change the certificate renewal time window for Edges using system properties. For more information, contact your Operator.</li> </ul> <p><b>Note</b> On clicking <b>Save Changes</b>, you are asked to confirm if the selected Edge authentication setting is applicable to all the impacted Edges or only the new Edges. By default, <b>Apply to all Edges</b> check box is selected.</p>
Edge Authentication	<p>Click the <b>Activate Secure Edge Access</b> button to allow the user to access Edges using Password-based or Key-based authentication. You can activate this option only once. But you can switch to either Password-based or Key-based authentication any number of times.</p>
<b>Device Secret Encryption</b>	<p>Click the <b>Enable For All Edges</b> button to activate device secret encryption for all the Edges in the current Enterprise. This action causes restart of all the Edges. However, Edges which already have this feature activated are not affected.</p> <p><b>Note</b> You can activate this option for individual Edges at the time of creating a new Edge. For more information, see <a href="#">Chapter 23 Provision a New Edge</a>.</p>
<b>Configuration Updates</b>	
Disable Edge Configuration Updates	<p>By default, this option is activated. This option allows you to actively push the configuration updates to Edges. Slide the toggle button to turn it Off.</p>
Enable Configuration Updates Post-Upgrade	<p>By default, this option is deactivated. This option allows you to control when post-Orchestrator upgrade configuration changes are applied to their Edges. Slide the toggle button to turn it On.</p>

## Software & Firmware Images

This section is visible only when the **Edge Image Management** feature is activated. To activate this feature, an Enterprise user must navigate to **Manage Customers** and select a customer. Then click **More > Update Edge Image Management**. Turn on the toggle button, and then click **Save**.

The Enterprise user can now view the details of the images and select the default image on the **Edge Management** screen.

**Note** Only an Operator user can add, delete, or edit an image.

## Upgrade SD-WAN Edges

Enterprise users can upgrade a specific Edge or a set of Edges, or all Edges using the Edge Management feature.

### Upgrade All Edges

In the **SD-WAN** service of the Enterprise portal, click **Service Settings > > Edge Management**. Scroll down to the **Software and Firmware Images** area, and select a default image.

### Upgrade Specific Edge(s)

You can override the default software image of an Enterprise, for a selected Edge or set of Edges, and assign a different software image to upgrade to those Edges by navigating to **Manage Customers > Select a Customer**, and then click **More > Update Edge Image Management**.

For more information, see the topic [Edge Management](#).

# User Management - Enterprise

39

The User Management feature allows you to manage users, their roles, service permissions (formerly known as Role Customization), and authentication.

An Enterprise Superuser, can access the **User Management** screen by navigating to **Global Settings > User Management**.

---

**Note** Starting with the 5.4.0 release, all the User Management related information for Enterprise users is documented and published in the *VMware SASE Global Settings Guide*, which is a standalone guide located at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

# Enterprise Settings

40

The Enterprise Settings option allows you to configure the user information, privacy settings, and primary contact details for the Enterprise users.

An Enterprise Superuser, can access the **Enterprise Settings** screen by navigating to **Global Settings > Enterprise Settings**.

---

**Note** Starting with the 5.4.0 release, all the Enterprise Settings related information for Enterprise users is documented and published in the *VMware SASE Global Settings Guide*, which is a standalone guide located at <https://docs.vmware.com/en/VMware-SD-WAN/index.html>.

# Configure High Availability on SD-WAN Edge

41

This section describes the high availability deployments and configuration supported on SD-WAN Edge.

Refer to the following topics:

Read the following topics next:

- [How SD-WAN Edge High Availability \(HA\) Works](#)
- [High Availability Deployment Models](#)
- [Split-Brain Condition](#)
- [Split-Brain Detection and Prevention](#)
- [Support for BGP Over HA Link](#)
- [High Availability Graceful Switchover with BGP Graceful Restart](#)
- [Selection Criteria to Determine Active and Standby Status](#)
- [VLAN-tagged Traffic Over HA Link](#)
- [Configure High Availability \(HA\)](#)
- [HA Event Details](#)

## How SD-WAN Edge High Availability (HA) Works

The high availability solution ensures continued traffic flow in case of failures. The SD-WAN Edge is the VMware data plane component that is deployed at an end user's branch location. SD-WAN Edge configured in High Availability (HA) mode are mirror images of each other and they show up on the SASE Orchestrator as a single SD-WAN Edge.

In a high availability configuration, SD-WAN Edges are deployed at the branch site in pairs of Active and Standby roles. Configurations are mirrored across both these Edges. The Active and Standby Edges exchange heartbeats using a failover link established over a wired WAN connection. If the Standby Edge loses connectivity with the Active Edge for a defined period, the Standby Edge assumes the identity of the Active Edge and takes over the traffic load. The failover has minimal impact on the traffic flow.

The SASE Orchestrator communicates only with the Active Edge. Any changes made to the Active Edge using the Orchestrator are synchronized with the Standby Edge using the failover link.

## Failure Scenarios

The following are some common scenarios that can trigger a failover from an Active to a Standby Edge:

- WAN link failure—When a WAN link on the Active Edge fails, a failover action is triggered. The SASE Orchestrator generates the “High Availability Going Active” event. This means that another WAN link on the Standby Edge will take over as Active because the peer’s WAN interface is down.
- LAN link failure—When a LAN link on the Active Edge fails, a failover action is triggered. The SASE Orchestrator generates the “High Availability Going Active” event. This means that another LAN link on the Standby Edge will take over as Active because the peer’s LAN interface is down.
- Edge functions not responding, or Edge crash / reboot / unresponsive—When the Active Edge crashes, reboots, or is unresponsive, the Standby Edge does not receive any heartbeat messages. The SASE Orchestrator generates the “High Availability Going Active” event and the Standby Edge takes over as Active.

---

**Note** HA Edges should be deployed within an isolated broadcast domain. During failover scenarios, to ensure a seamless transition of the Active role to the Standby Edge, it is crucial that the Standby Edge does not receive any incoming packets on the HA interface.

---

## High Availability Deployment Models

The High Availability feature supports the following deployment models:

- **Standard HA**—In this model, the Active and Standby Edges have the same configurations and have symmetric connections, that is both Edges are connected to the same WAN links. All ports on the Active Edge are open for receiving and sending traffic. Whereas all ports except GE1 on the Standby Edge are blocked. The GE1 interface is used to exchange heartbeats between Active and Standby Edges. See [Standard HA](#).
- **Enhanced HA** – In this model, the Active and Standby Edges have the same configurations but have asymmetric connections, that is both Edges are connected to different WAN links. The GE1 interface is used to exchange heartbeats between Active and Standby Edges. The Active Edge can leverage the WAN link connected to the Standby Edge to send or receive traffic. It forwards the traffic through the GE1 interface to the Standby Edge, which in turn sends the traffic through the WAN link. See [Enhanced HA](#).

- **Mixed-mode HA**—This model is a combination of both Standard and Enhanced HA deployments on the same site. In this model, the Active and Standby Edges have the same configurations. The connections can be both symmetric and asymmetric. See [Mixed-Mode HA](#).

The HA options are supported on the following SD-WAN Edge platforms: 510, 510N, 520, 520v, 540, 610, 610N, 620, 620N, 640, 640N, 680, 680N, 840, 2000, 3400, 3800, 3810, and any Virtual Edge.

---

**Note** HA Edges should be deployed within an isolated broadcast domain. During failover scenarios, to ensure a seamless transition of the Active role to the Standby Edge, it is crucial that the Standby Edge does not receive any incoming packets on the HA interface.

---

**Caution** HA is supported only between identical SD-WAN Edge platform models. For more information on the Edge platform models, see <https://sdwan.vmware.com/get-started>.

---

**Important** Prior to Edge Release 5.4.0, Edge models which did not include a Wi-Fi module (510N, 610N, 620N, 640N, and 680N) could not be used with a Wi-Fi capable counterpart in an HA deployment. For example, an Edge 640 and an Edge 640N were not supported as a High Availability pair. For Release 5.4.0 and forward, this pairing is now supported.

In a scenario with mismatched Wi-Fi and Non Wi-Fi Edges, the Orchestrator detects the Edge mismatch and automatically deactivates Wi-Fi capability on the Edge that is Wi-Fi capable. The mismatch log is shown in the customer's Events:

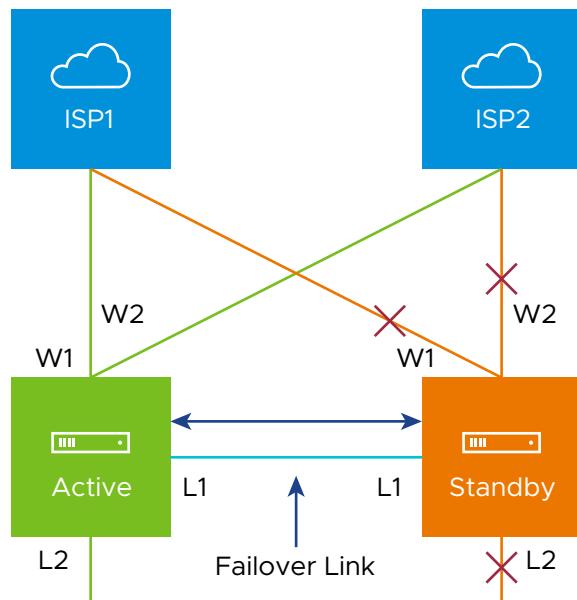
- "HA Wi-Fi capability mismatch identified, disabled Wi-Fi." (An Edge Wi-Fi mismatch is identified and Wi-Fi is deactivated on the Wi-Fi capable Edge).
  - "HA Wi-Fi capability mismatch no longer seen, reverted Wi-Fi." (Both Edges are detected as the same Wi-Fi type, and Wi-Fi functionality is restored on a Wi-Fi Edge where it was previously deactivated).
- 

## Standard HA

This section describes Standard HA.

### Topology Overview for Standard HA

The following figure shows a conceptual overview of Standard HA.



The Edges, one Active and one Standby, are connected by L1 ports to establish a failover link. The Standby SD-WAN Edge blocks all ports except the L1 port for the failover link.

## Prerequisites for Standard HA

- The LAN side switches in the following configuration descriptions must be STP capable and configured with STP.
- In addition, SD-WAN Edge LAN and WAN ports must be connected to different L2 switches. If it is necessary to connect the ports to the same switch, then the LAN and WAN ports must be isolated.
- The two SD-WAN Edges must have mirrored physical WAN and LAN connections.

## Deployment Types for Standard HA

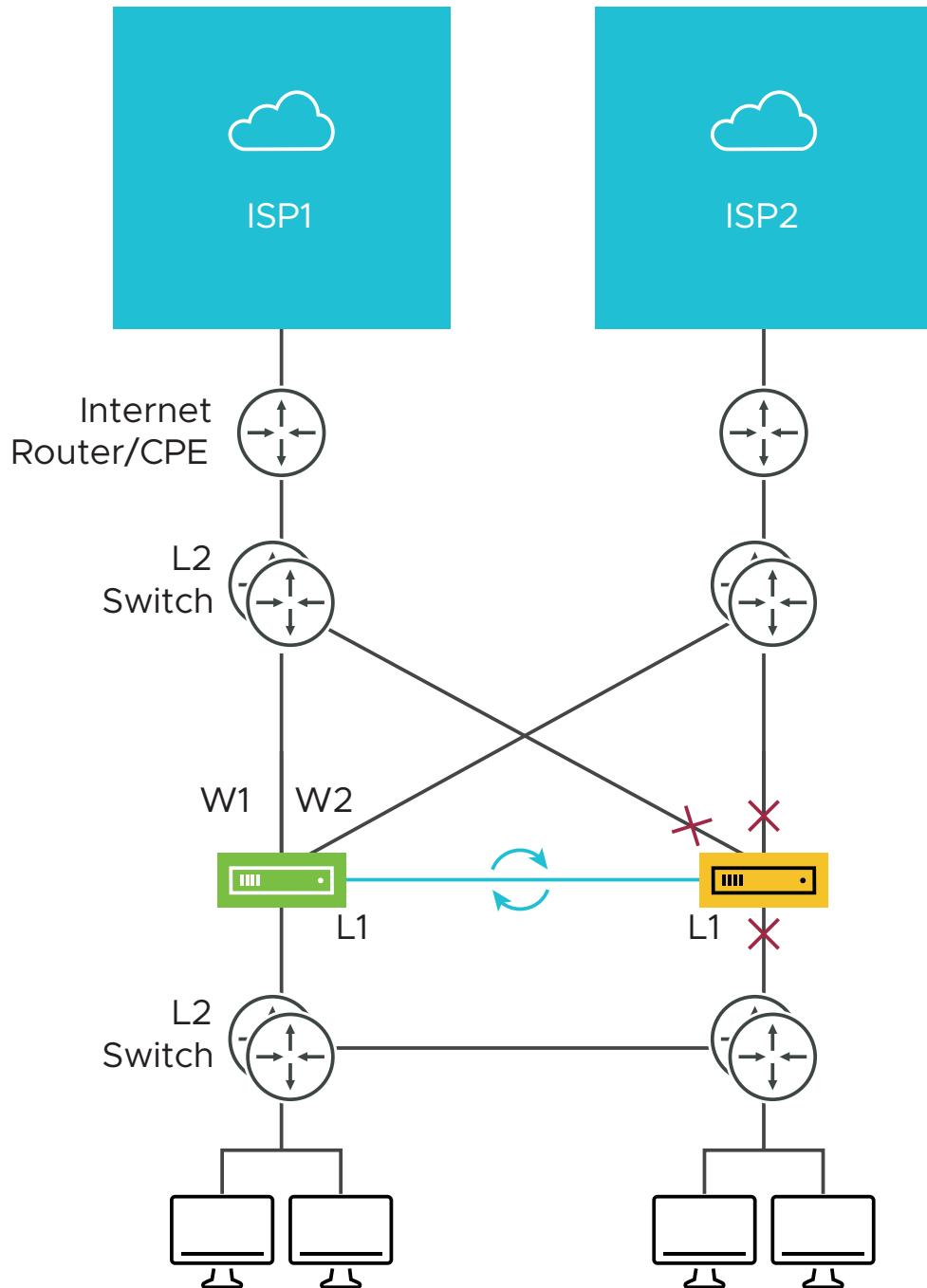
Standard HA has two possible deployment types:

- Deployment Type 1: High Availability (HA) using L2 switches
- Deployment Type 2: High Availability (HA) using L2 and L3 switches

The following sections describe these two deployment types.

### Deployment Type 1: HA using L2 switches

The following figure shows the network connections using only L2 switches.



W1 and W2 are WAN connections used to connect to the L2 switch to provide WAN connectivity to both ISPs. The L1 link connects the two SD-WAN Edges and is used for ‘keep-alive’ and communication between the SD-WAN Edges for HA support. The SD-WAN Edge’s LAN connections are used to connect to the access layer L2 switches.

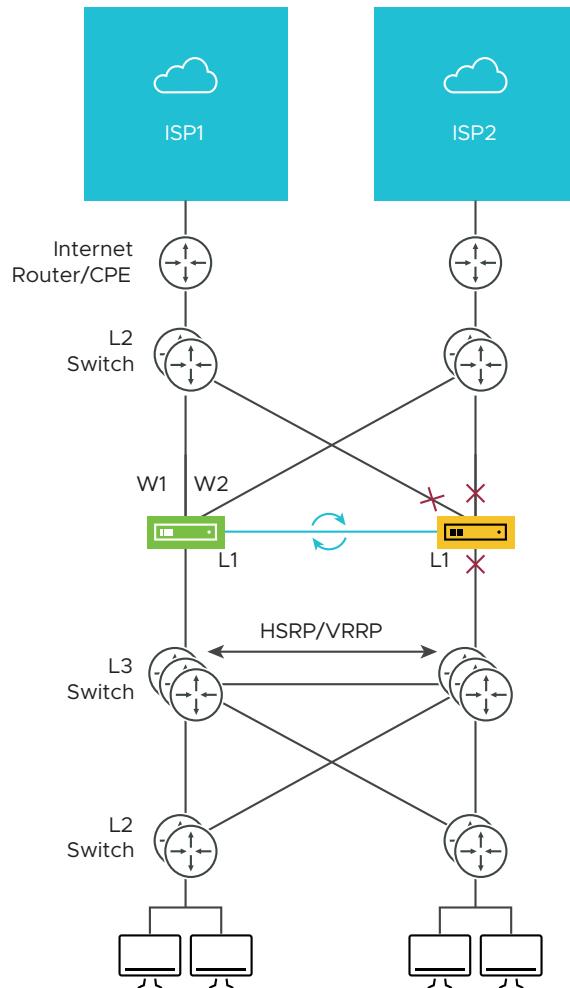
### Considerations for HA Deployment using L2 switches

- The same ISP link must be connected to the same port on both Edges.
- Use the L2 switch to make the same ISP link available to both Edges.

- The Standby SD-WAN Edge does not interfere with any traffic by blocking all its ports except the failover link (L1 port).
- Session information is synchronized between the Active and Standby SD-WAN Edges through the failover link.
- If the Active Edge detects a loss of a LAN link, it will also failover to the Standby if it has an Active LAN link.

## Deployment Type 2: HA using L2 and L3 Switches

The following figure shows the network connections using L2 and L3 switches.



The SD-WAN Edge WAN connections (W1 and W2) are used to connect to L2 switches to provide a WAN connection to ISP1 and ISP2 respectively. The L1 connections on the SD-WAN Edge are connected to provide a failover link for HA support. The VMware Edge LAN connections are used to connect L2 Switches, which have several end-user devices connected.

## Considerations for HA Deployment using L2 and L3 switches

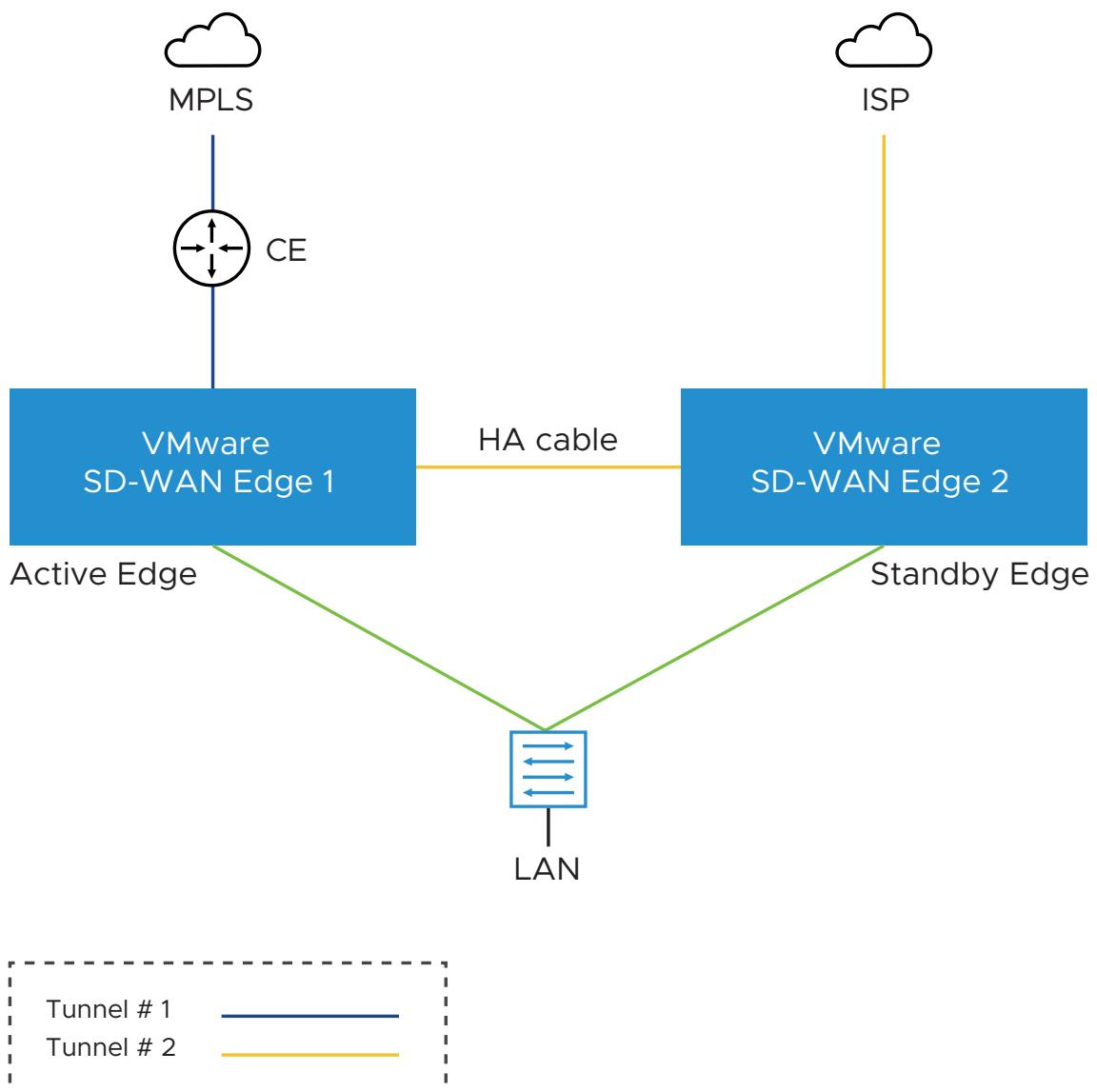
- HSRP/VRRP is required on the L3 switch pair.

- The SD-WAN Edge's static route points to the L3 switches' HSRP VIP as the next hop to reach the end stations behind L2 switches.
- The same ISP link must be connected to the same port on both SD-WAN Edges. The L2 switch must make the same ISP link available to both Edges.
- The Standby SD-WAN Edge does not interfere with any traffic by blocking all of its ports except the failover link (L1 port).
- The session information is synchronized between the Active and Standby SD-WAN Edges through the failover link.
- The HA pair also does a failover from Active to Standby on detecting the L1 loss of LAN / WAN links.
  - If Active and Standby have the same number of LAN links which are up, but Standby has more WAN links up, then a switchover to Standby will occur.
  - If the Standby Edge has more LAN links up and has at least one WAN link up, then a failover to the Standby will occur. In this situation, it is assumed that the Standby Edge has more users on the LAN side than the Active Edge, and that the Standby will allow more LAN side users to connect to the WAN, given that there is some WAN connectivity available.

## Enhanced HA

This section describes Enhanced HA. The Enhanced HA eliminates the need for L2 Switches on WAN side of the Edges. For users looking for LAN side settings, please refer to the Standard HA documentation. This option is chosen when the Active Edge detects different WAN link(s) connected to the Standby Edge when compared to the link(s) connected to itself.

The following figure shows a conceptual overview of Enhanced HA.



The Edges, one Active and one Standby, are connected by using an HA link to establish a failover link. The Active Edge establishes overlay tunnels on both WAN links (connected to itself and the Standby Edge) through the HA link.

---

**Note** The two SD-WAN Edges should not have mirrored physical WAN connections. For example, if the Active Edge has GE2 as the WAN link, then the Standby Edge cannot have GE2 as its WAN link.

---

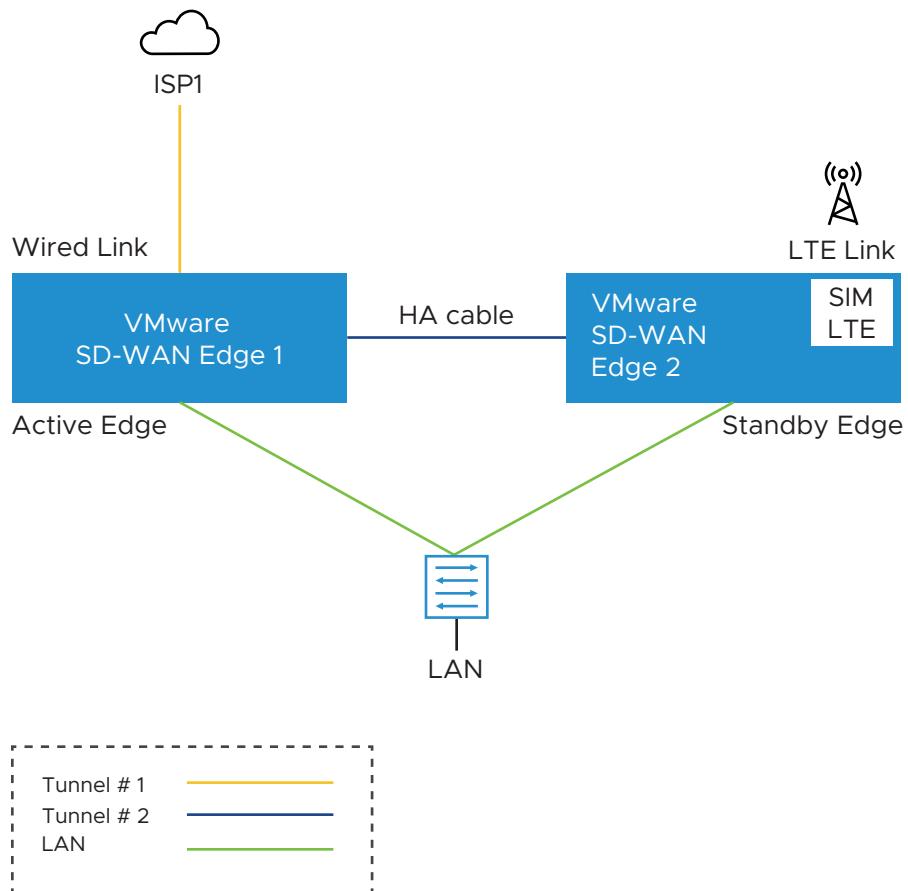
In order to leverage the WAN link connected to the Standby Edge, the Active Edge establishes the overlay tunnel through the HA link. The LAN-side traffic is forwarded to the Internet through the HA link. The business policy for the branch defines the traffic distribution across the overlay tunnels.

## Enhanced HA Support for LTE Interface

Long-Term Evolution (LTE) is a standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity and speed using a different radio interface together with core network improvements. VMware SD-WAN supports LTE in 510 and 610 Edge models which have two SIM slots.

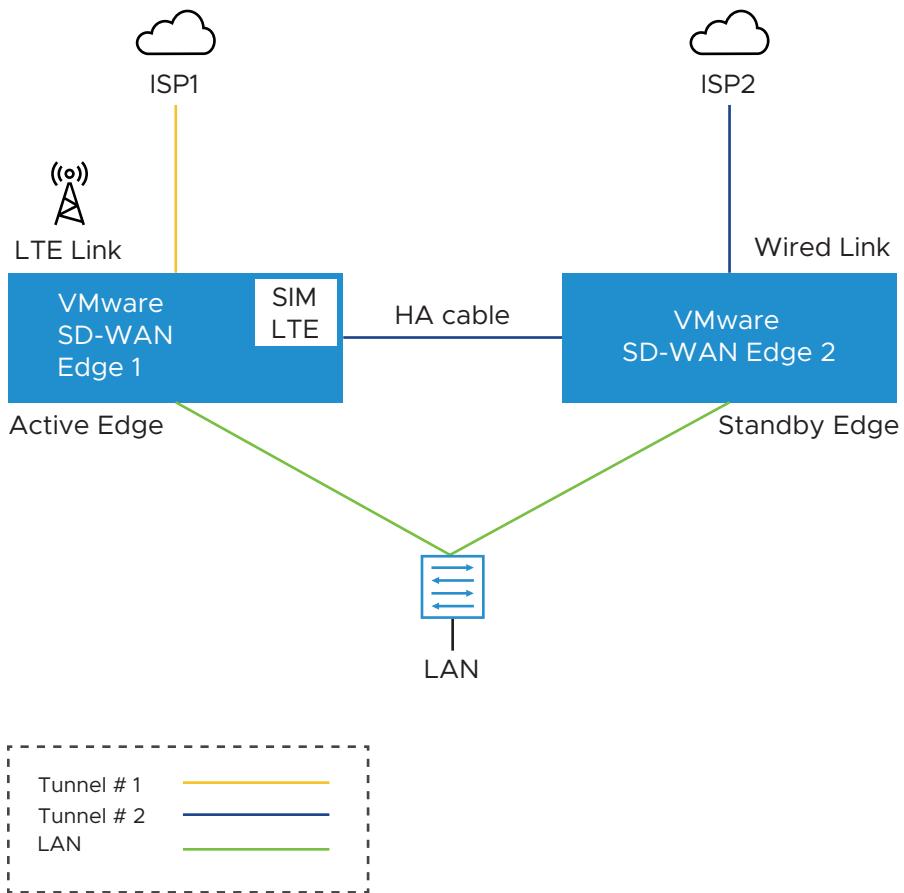
Starting with the 4.2 release, the LTE link/CELL interface is counted in the HA election. Internally, a lesser weight is provided for CELL links than wired links. So depending on the number of wired links connected to each Edge in the eHA pair, the Edge with the LTE link can either be the Active or the Standby Edge. Here are some use cases for eHA with LTE interface.

### Use case 1: 1-Wired link on Active Edge and 1-LTE link on Standby Edge



The figure illustrates the topology of Enhanced HA support for LTE Interface on a Standby Edge. In this example, there are two Edges, one Active (SD-WAN Edge 1) and one Standby (SD-WAN Edge 2), that are connected by using an HA cable to establish a failover link. The wired WAN link Edge is preferred as Active Edge. The Standby Edge uses an LTE link for tunnel establishment. The LTE link on the Standby Edge could be used as active, backup, or hot-standby link, based on the Edge configuration. The Active Edge establishes overlay tunnels on WAN link connected to itself and the LTE link on the Standby Edge through the HA link. If an Active Edge fails, the Standby Edge will continue to forward the LAN-side traffic through the LTE link.

#### Use case 2: 1-Wired and 1-LTE link on Active Edge and 1-Wired link on Standby Edge



The figure illustrates the topology of Enhanced HA support for LTE Interface on an Active Edge. In this example, the SD-WAN Edge 1 with one wired link and one LTE link acts as an Active Edge, and SD-WAN Edge 2 with one wired link acts as Standby Edge. If the wired WAN link on the Active Edge goes down, the Standby Edge would take over as Active and the LTE link would be used in eHA mode.

## Supported Topologies

The requirement for HA is to have same models connected in HA pair. The enhanced HA support for LTE supports the following topologies:

- 510 - 510 LTE HA pair
- 610 - 610 LTE HA pair
- 510 LTE - 510 LTE HA pair
- 610 LTE - 610 LTE HA pair

**Note** Inserting LTE SIM in Active Edge when Standby Edge has an LTE SIM on CELL interface is not supported for 510-LTE pairs and 610-LTE pairs topologies.

## Limitations

- LTE Dual SIM Single Standby (DSSS) is not supported with eHA LTE.
- USB modems on Standby Edge in eHA mode is not supported.

## Troubleshooting Enhanced HA support for LTE

You can troubleshoot the Enhanced HA support for LTE Interface feature, by running the following remote diagnostic tests on an Edge:

- **LTE Modem Information** - Run this test on a selected Edge interface to collect diagnostic details such as Modem information, Connection information, Location information, Signal information, and Status information for the internal LTE modem.

The below screen shows the output for an Edge's CELL1 interface where there is no SIM card attached, while exhibiting the expected fields for this diagnostic.

The screenshot shows the VMware Orchestrator interface with the following details:

- Header:** vmw Orchestrator, Customer 5-site, SD-WAN.
- Navigation:** Monitor, Configure, **Diagnostics** (selected), Service Settings.
- Device Selection:** Edges / HW-510LTE-B5, HW-510LTE-B5 (Connected).
- LTE Modem Information:**
  - Interface: CELL1
  - Test Duration: 9.021 seconds
  - Modem Information (JSON):

```
{
  "Manufacturer": "sierra Wireless, Incorporated",
  "Model": "EM7430",
  "Model identifier": "355674112041440",
  "Firmware Revision": "SWI9X30C_02.33.03.00 r8209 CARM-D-EV-FRMWR2 2019/08/28 20 59 30",
  "Hardware Revision": "1.0",
  "Supported capabilities": "gsm-umts, lte",
  "Current capabilities": "gsm-umts, lte",
  "Own number": "--",
  "State": "failed",
  "Failed reason": "sim-missing",
  "Power state": "on",
  "Current modes": "allowed any; preferred none",
  "IMEI": "--",
  "Operator code": "--",
  "Operator name": "--",
  "Registration state": "--",
  "Signal quality(%)": "0"
}
```
- Connection Information:**

```
{
  "Bearer": "Not Attached/Available",
  "Connected": "NA",
  "Suspended": "NA",
  "Interface": "NA",
  "APN": "NA",
  "IP type": "NA",
  "User": "NA",
  "Password": "NA",
  "IP method": "NA",
  "IP address": "NA",
  "Gateway": "NA",
  "DNS": "NA",
  "MTU": "NA",
  "Stats Duration": "NA",
  "Rx bytes": "NA",
  "Tx bytes": "NA"
}
```
- Location Information:**

```
{
  "STATUS": "ERROR",
  "REASON": "Location information not available"
}
```
- Signal Information:**

```
{}
```
- Status Information:**

```
response: !GSTATUS:
Current Time: 204689      Temperature: 31
Reset Counter: 1          Mode: ONLINE
System mode: LTE           PS state: Not attached
LTE band: B32              LTE bw: Unknown
LTE Rx chan: 0             LTE Tx chan: 4294967295
LTE CA status: NOT ASSIGNED
```

- **Reset USB Modem** - Run this test on a selected Edge interface to reset an malfunctioning USB modem connected to the given interface.

**Note** Not all USB modems support this type of remote reset.

### Reset USB Modem

**RUN**

This will attempt to reset an unworking USB modem connected to the given interface. Note that not all USB modems support this type of remote reset.

**Interface**

CELL1 ▾  
**CELL1**  
 CELL2  
 USB1  
 USB2

**Table Dump**

**RUN**

## Mixed-Mode HA

The Mixed-mode HA deployment model is a combination of Standard HA and Enhanced HA deployments.

In this deployment model you can have both shared interfaces and individual interfaces.

Let us consider a scenario where the private network is unable to communicate with the Orchestrator or the controller.

Diagram illustrating Mixed-Mode HA deployment:

- Active VMware SD-WAN Edge:** Connected to MPLS (GE4) and ISP1 (GE5).
- Standby VMware SD-WAN Edge:** Connected to MPLS (GE2) and ISP1 (GE3).
- Failover Link:** GE1 connects the Active Edge to the Standby Edge.
- Clouds:** MPLS and ISP1.
- Red Arrow:** Points from the MPLS cloud to the text "Unable to communicate with Orchestrator or Controller".

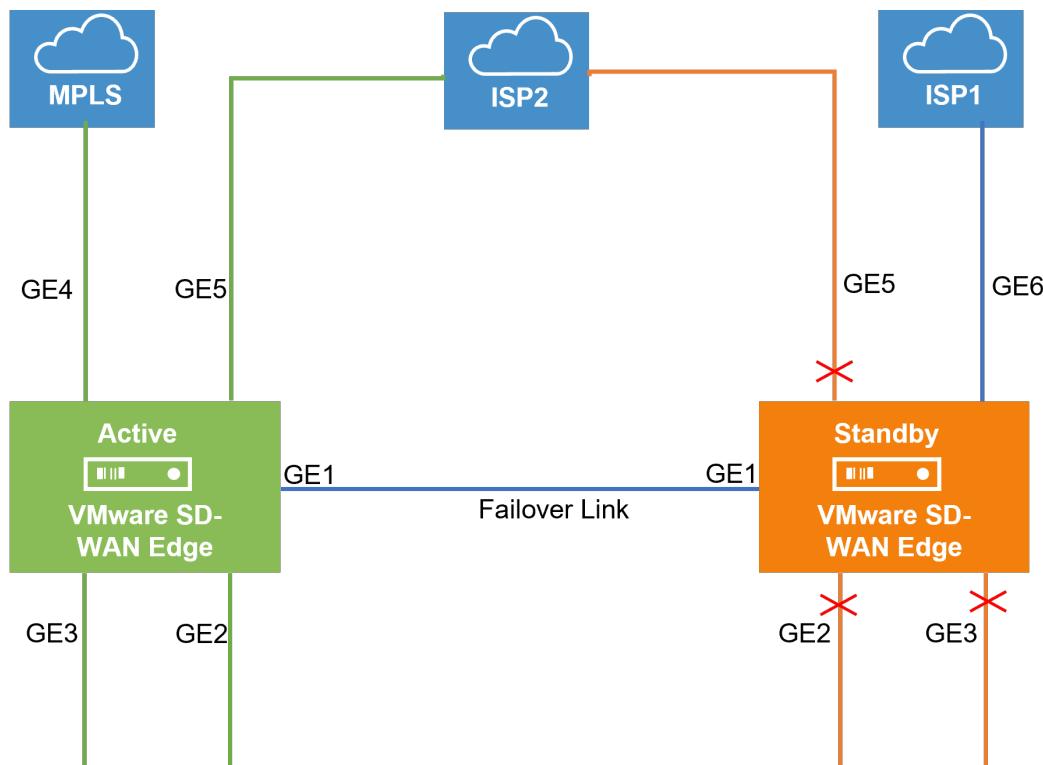
VMware by Broadcom

1100

In this topology, the Active and Standby Edges exchange heartbeat messages, synchronize configuration updates, and other information over the GE1 interface. Both SD-WAN Edges have mirrored LAN and WAN connections over the GE2, GE3, and GE5 interfaces, which is similar to the Standard HA deployment model. However, the Active Edge is connected to the private network using the GE4 WAN link. This is similar to the Enhanced HA deployment model. All ports on the Active Edge are kept open to send and receive traffic. On the Standby Edge, all ports except GE1 are blocked.

When the MPLS network is unable to communicate with the Orchestrator or the Controller, the site would still have connectivity to the Orchestrator or the Gateway and would be able to build public overlays.

Now let us consider a scenario when both private and public networks are unable to communicate with the Orchestrator or Controller.



In this topology, the ISP1 is connected only to the Standby Edge using the GE6 WAN link and ISP2 is connected to both Active and Standby Edges using the GE5 WAN link. All ports on the Active Edge are kept open to send and receive traffic. On the Standby Edge, all ports except GE1 and GE6 are blocked. The Active Edge leverages GE6 WAN link to send traffic to the public network, ISP1 through GE1.

## Split-Brain Condition

When the HA link is disconnected or when the Active and Standby Edges fail to communicate with each other, both Edges assume the Active role. As a result, both Edges start responding to

ARP requests on their LAN interfaces. This causes LAN traffic to be forwarded to both Edges, which could result in a broadcast storm on the LAN.

Typically, LAN switches connected to the HA Edge pair LAN ports run the Spanning Tree Protocol to prevent loops which trigger broadcast storms in the network. In such a condition, the switch would block traffic to one or both Edges. However, doing so would cause a total loss of traffic through the Edge pair.

---

**Important** On an Enhanced HA deployment (where there is no Layer 2 Switch connected to the Edge's WAN interfaces), connectivity to the Primary Gateway is a requirement for split-brain detection. More details on the split-brain detection functionality can be found in the section [Split-Brain Detection and Prevention](#).

---

## Split-Brain Detection and Prevention

This section covers the mechanisms used to detect and prevent a split-brain state in an Edge deployment using a high availability topology.

There are two mechanism for detecting and preventing a split-brain condition in a high availability deployment (where both HA Edges become Active).

The first mechanism involves sending layer 2 broadcast heartbeats between the two HA Edges when the HA heartbeat link between the devices is lost. A layer 2 broadcast (EtherType 0x9999) heartbeat is sent from the Active Edge on all its WAN interfaces in an effort to find the Standby Edge in that broadcast network. When the Standby Edge receives this packet, it interprets the packet as an indication to maintain its current Standby state. This mechanism is used by a Legacy High Availability deployment where both HA Edges have their WAN ports connected to the same layer 2 Switch.

The second mechanism used to detect and prevent split-brain conditions leverages the Primary Gateway used by the HA Edges. This mechanism is the sole means of detecting and preventing split-brain in an Enhanced High Availability deployment as this topology does not connect both HA Edges to an upstream layer 2 switch.

The Gateway has a pre-existing connection to the Active Edge (VCE1). In a split-brain condition, the Standby Edge (VCE2) changes state to Active and tries to establish a tunnel with the Gateway (VCG). The Gateway will send a response back to the Standby Edge (VCE2) instructing it to move to Standby state, and will not allow the tunnel to be established. The Gateway keep its tunnels only with the Active Edge. The sequence of events is as follows:

As soon as the HA link fails, the VCE2 moves to the Active state and enables the LAN/WAN ports, and tries to establish tunnels with the Primary Gateway. If the VCE1 still has tunnels, the Primary Gateway instructs the VCE2 to revert to the Standby state and thus the VCE2 blocks its LAN ports. Only the LAN interfaces remain blocked (as long as the HA cable is down). As illustrated in the following figure, the Gateway signals VCE2 to go into the Standby state. This will logically prevent the split-brain scenario from occurring.

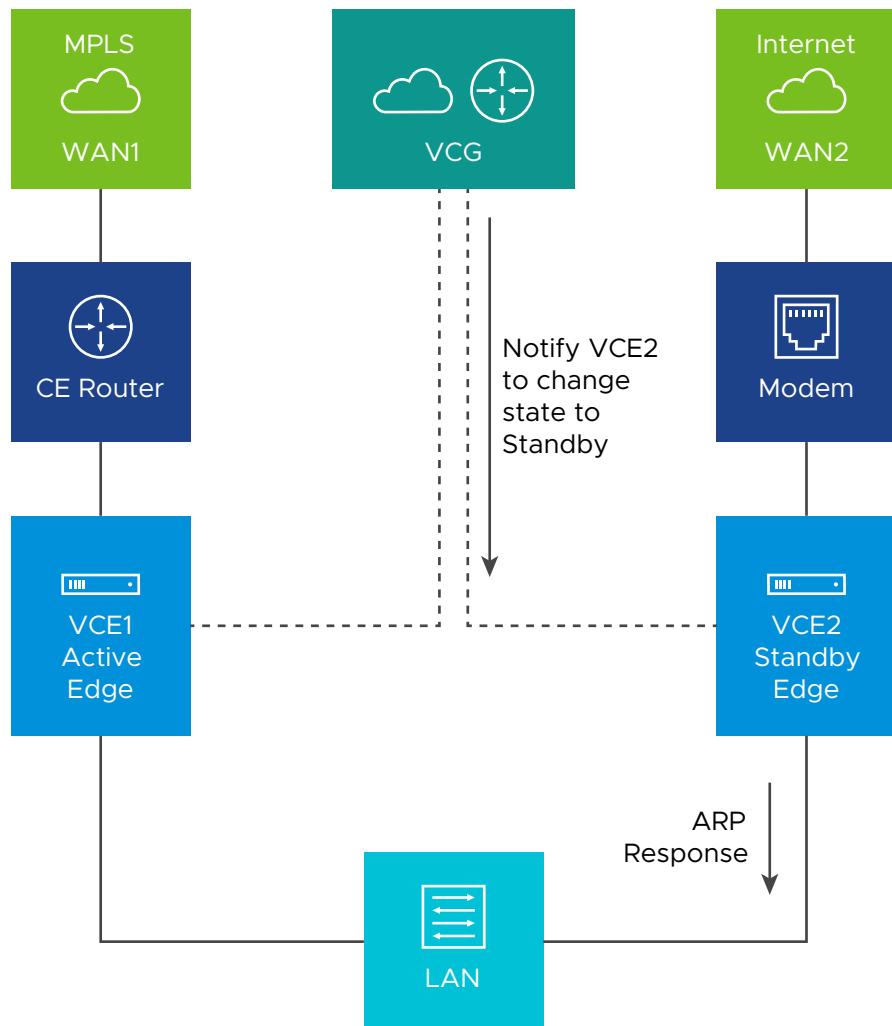
---

**Note** The normal failover from Active to Standby in a split-brain scenario is not the same as the normal failover. It could take a few extra milliseconds/seconds to converge.

---

**Note** When configuring WAN interface settings for an Edge, if you select **PPPoE** from the **Addressing Type** field, the Edge cannot send heartbeat packets by broadcast from a WAN interface so configured.

---



**Note** Beginning in Release 5.2.0, the **HA Failover Detection Time Multiplier** feature can be used to set a longer High Availability failover threshold. The timer represents how long a Standby Edge will wait for a heartbeat packet from the Active Edge before becoming active. In some instances, where a lower model Edge is under high traffic load, the Active Edge's heartbeat packet may take longer than the default threshold time to be delivered to the Standby Edge. As a result the Standby Edge triggers a failover and is promoted to Active, resulting in a Split-Brain state.

Setting the HA Failover Detection Time Multiplier to a value higher than the default can lessen the risk of a Split-Brain state in this scenario. The default value is 700 milliseconds (ms), and this value can be increased up to a value of 7000 ms. For more information, see [Activate High Availability](#).

## Support for BGP Over HA Link

When a pair of Edges are configured in a High Availability topology, the Active SD-WAN Edge will exchange BGP routes over the HA link. Where Enhanced HA is used, BGP on the Active Edge establishes neighborship with a peer connected only to the standby Edge's WAN link.

Beginning with SD-WAN Release 5.1.0 and onwards, a site deployed in High Availability with BGP configured automatically synchronizes local routes between the Active and Standby Edges and uses these routes for forwarding on the Active Edge while also ensuring that the route table is immediately available after an HA failover. This results in improved failover times as the routes are already available on the Standby Edge when it is promoted to Active.

---

**Note** To fully optimize HA failovers where BGP is used in Standard and Enhanced HA topologies, it is strongly recommended to also activate the **BGP Graceful Restart** feature. Information about this feature is found in the [High Availability Graceful Switchover with BGP Graceful Restart](#) documentation.

---

## High Availability Graceful Switchover with BGP Graceful Restart

For a site deployed in a High Availability topology where BGP is also used, an HA failover can be both slow and disruptive to customer traffic because the peer Edges have deleted all the routes on a failover. In Release 5.1.0 and later VMware adds the BGP Graceful Restart feature for HA deployments which ensures faster and less disruptive HA failovers.

### Overview

**BGP Graceful Restart** with **Graceful Switchover** ensures faster Edge restarts and HA failovers by having the neighboring BGP devices participate in the restart to ensure that no route changes occur in the network for the duration of the restart. Without BGP Graceful Restart, the peer Edge deletes all routes once the TCP session terminates between BGP peers and these routes need to be rebuilt post Edge restart or HA failover. BGP Graceful Restart changes this behavior by ensuring that peer Edges retain routes as long as a new session is established within a configurable restart timer.

---

**Note** BGP Graceful Restart is for sites deployed in High-Availability only. This feature is not yet available for sites deployed with a single, standalone Edge even if it uses the BGP routing protocol.

---

### Prerequisites

To use the BGP Graceful Restart feature, a customer site must have the following.

- A site deployed with a High Availability topology. This can be either Active/Standby or VRRP with 3rd party router. BGP Graceful Restart does not have any effect on a standalone Edge site, only on sites using HA.

- The customer enterprise must have BGP configured as the routing protocol.

**Important** To fully optimize the benefits of **BGP Graceful Restart** it is strongly recommended that **Distributed Cost Calculation (DCC)** is also activated for the customer enterprise. With DCC activated, preference and advertisement decisions are local to the Edge and the Edge synchronizes from Active to Standby as soon as it learns the routes from the routing process. DCC's value is not limited to HA sites, and for more information on this feature see [VMware SD-WAN Routing Overview](#) and [Configure Distributed Cost Calculation](#).

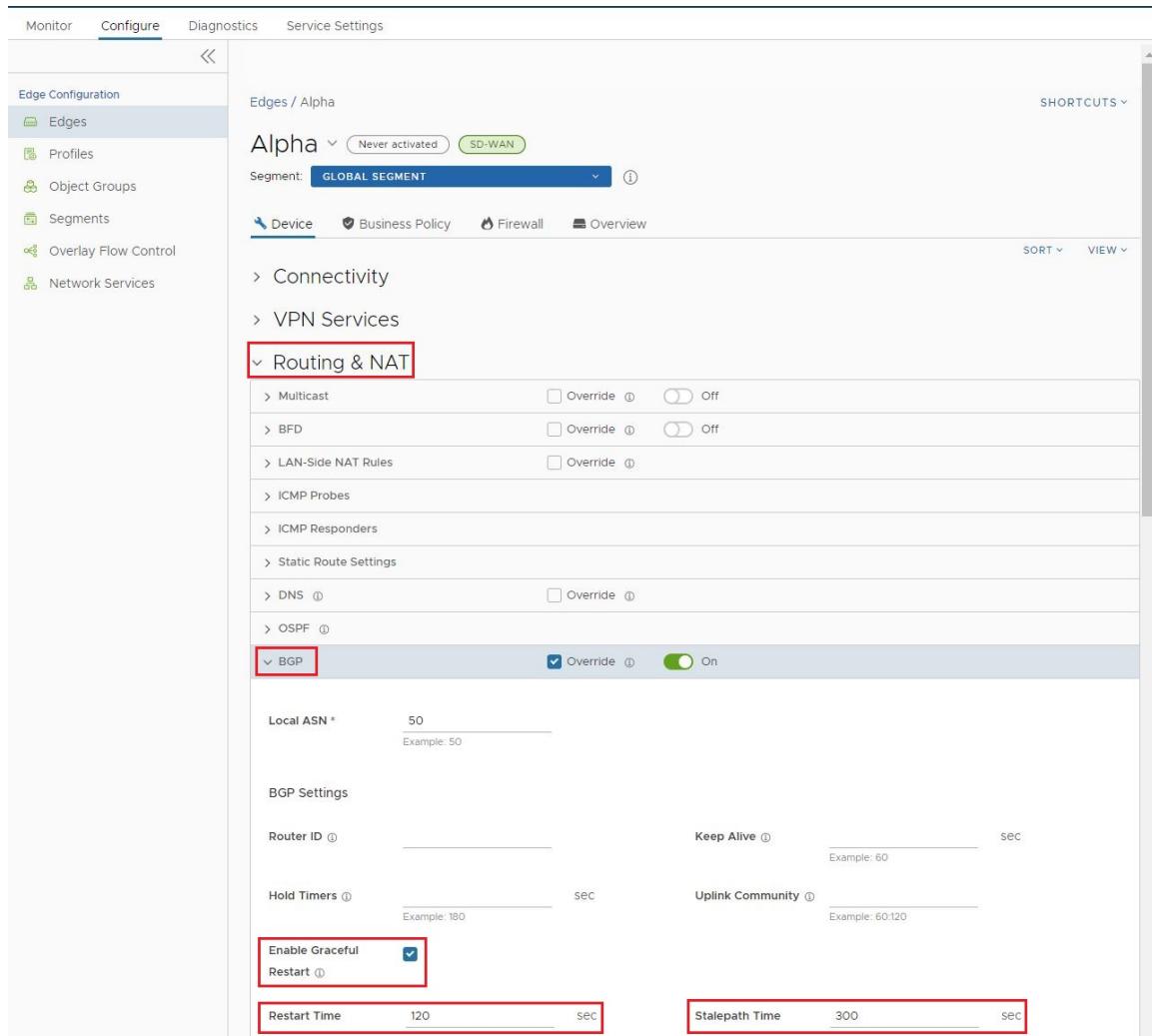
## Configuring BGP Graceful Restart

Configuring **BGP Graceful Restart** is a two part process, the first part being done on the **BGP** configuration section, and the second part in the **High Availability** configuration section. The steps are:

- 1 Activate **Graceful BGP Restart** on **Configure > Device > BGP**.
  - a In the Customer portal, click either **Configure > Profile** or **> Configure > Edges** depending on your preferences. The screenshots will show the steps for a single HA Edge.
  - b Click the **Device** icon next to an Edge, or click the link to the Edge, and then click the **Device** tab.
  - c Scroll down to the **Routing & NAT** section and open up the **BGP** section for the Edge or Profile.

The screenshot shows the VMware SD-WAN Administration Guide interface. The top navigation bar includes 'Monitor', **Configure**, 'Diagnostics', and 'Service Settings'. The left sidebar under 'Edge Configuration' lists 'Edges', 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control', and 'Network Services'. The main content area shows 'Edges / Alpha' with a 'Segment: GLOBAL SEGMENT' dropdown. Below it, the 'Device' tab is selected, showing sections for 'Connectivity', 'VPN Services', and 'Routing & NAT'. The 'Routing & NAT' section is expanded, displaying options like Multicast, BFD, LAN-Side NAT Rules, ICMP Probes, ICMP Responders, Static Route Settings, DNS, OSPF, and BGP. The 'BGP' row has an 'Override' checkbox checked and a toggle switch set to 'On'. The 'High Availability' section is also expanded, showing 'HA: Active Standby Pair' selected. It includes a 'Select Type' section with radio buttons for 'None', 'Active Standby Pair' (which is selected), 'Cluster', and 'VRRP with 3rd party router'. Below this are fields for 'HA Interface' (set to GE1) and 'Deploy with Unique LAN MAC Address'. A note states: 'The option to activate Graceful Switchover is not yet available and only becomes available after the BGP configuration is completed first.' A red box highlights the 'Enable Graceful Switchover (require Graceful Restart in routing protocol)' checkbox.

- d In the **BGP** section check the box for **Graceful Restart**.



- e Once the box is checked, two additional parameters appear related to Enable Graceful Restart: **Restart Time**, and **Stalepath Time**:
  - 1 **Restart Time** represents the maximum time the route processor (RP) waits for the RP peer to begin talking before expiring route entries. The default time for this parameter is 120 seconds and can be manually configured within a range of 1 to 600 seconds.
  - 2 **Stalepath Time** represents the maximum time routes are retained after a restart (HA failover). Updated routes from a route processor peer are expected to have been received by this time. The default time for this parameter is 300 seconds and can be manually configured within a range of 1 to 3600 seconds.
- f Once the user has activated BGP Graceful Restart and is satisfied with the two secondary settings, a user can then move to the **High Availability** section.
- 2 Activate **Graceful Switchover** on Configure > Device > **High Availability**.
  - a From the **BGP** section, scroll down to the **High Availability** section.

The screenshot shows the VMware SD-WAN Administration Guide interface. The top navigation bar includes 'Monitor', 'Configure' (which is highlighted with a red box), 'Diagnostics', and 'Service Settings'. On the left, a sidebar under 'Edge Configuration' shows 'Edges' (selected and highlighted with a red box), 'Profiles', 'Object Groups', 'Segments', 'Overlay Flow Control', and 'Network Services'. The main content area is titled 'Edges / Alpha'. It shows 'Alpha' (Never activated) and 'SD-WAN'. The 'Segment' dropdown is set to 'GLOBAL SEGMENT'. Below this, tabs include 'Device' (highlighted with a red box), 'Business Policy', 'Firewall', and 'Overview'. A 'SHORTCUTS' dropdown is in the top right. The main content area has sections for 'Connectivity', 'VPN Services', and 'Routing & NAT'. Under 'Routing & NAT', there are several options like Multicast, BFD, LAN-Side NAT Rules, ICMP Probes, ICMP Responders, Static Route Settings, DNS, OSPF, and BGP. The 'BGP' row has an 'Override' checkbox checked and a toggle switch set to 'On'. A 'High Availability' section is expanded, showing 'HA: Active Standby Pair'. It includes a 'Select Type' dropdown with 'None' (radio button), 'Active Standby Pair' (radio button, selected and highlighted with a red box), 'Cluster', and 'VRRP with 3rd party router'. Below this is an 'HA Interface' field set to 'GE1'. At the bottom of the 'High Availability' section is a checkbox for 'Deploy with Unique LAN MAC Address' and another for 'Enable Graceful Switchover (require Graceful Restart in routing protocol)', which is checked and highlighted with a red box.

- b In the **High Availability** section the option to check the box for **Graceful Switchover** is now available as a result of **BGP Graceful Restart** being activated.
  - c Check the box for **Graceful Switchover**.
  - d Nothing further is required in the **High Availability** section and there are no secondary parameters for **Graceful Switchover**.
- 3 Scroll down to the bottom of the **Configure > Device** page and click **Save Changes** in the bottom right corner. This applies the configuration changes made above.

## Limitations/Known Behaviors

- **BGP Graceful Failover** and **HA Graceful Switchover** are segment agnostic and when activated on one segment (for example, the Global Segment) these settings are applied to all other segments on a customer site. This means that the Edge will synchronize routes on other segments and hold stale routes during an HA failover.

## Selection Criteria to Determine Active and Standby Status

This section describes the selection criteria used to determine Active and Standby Status.

- Check for the Edge that has a higher number (L2 and L3) LAN interfaces. The Edge with the higher number of LAN interfaces is chosen as the Active one. Note that the interface used for the HA link is not counted as a LAN interface.
- If both Edges have the same number of LAN interfaces, the Edge with the higher number of WAN interfaces is chosen as the Active one.

---

**Note** There is no preemption if the two Edges have the same number of LAN and WAN interfaces.

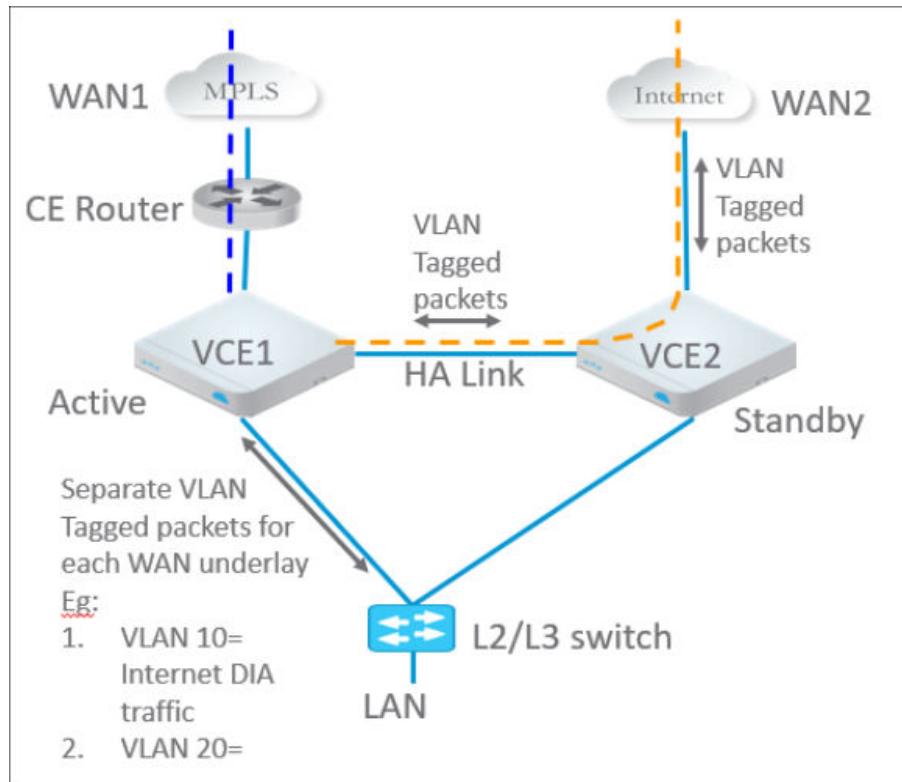
---

- Additional Support Matrix:
  - Static/DHCP/PPPoE links are supported.
  - Multiple WAN links each tagged with a separate VLAN ID on a single interface (e.g. Sub-Interfaces) are supported.
  - USB modems are not recommended on HA. The interface will not be used when present in the Standby Edge.

## VLAN-tagged Traffic Over HA Link

This section describes the VLAN-tagged Traffic over an HA Link.

- Internet traffic from ISP2 is VLAN tagged.
- Customer will have separate VLANs for Enterprise traffic versus DIA traffic.
- The WAN link on the Standby has sub-interfaces to carry Internet traffic.
- Multi segments



## Configure High Availability (HA)

To configure High Availability, configure the Active and Standby Edges.

### Deploying High Availability on VMware ESXi

You can deploy the VMware SD-WAN HA on VMware ESXi using the supported topologies.

While deploying HA on VMware ESXi, consider the following limitations:

#### ESXi vSwitch Caveats

- The upstream failures are not propagated by the vSwitch that is directly connected to a virtual SD-WAN VNF. For example, if a physical adapter goes down, the VMware Edges see the link up and do not failover.
- vSwitches do not allow the ability to configure specific VLANs on a port group. If more than one VLAN is required, then VLAN 4095 must be configured. This allows all VLANs on the port group.

---

**Note** This is not applicable to **br-HA Link**, which does not require VLANs.

---

- The virtual Edge, when working as HA, changes its original assigned MAC Address. In order to allow the virtual Edge to receive frames with a MAC Address that is different from the one originally assigned, set the **MAC address changes** option on the virtual switch to **Accept**.

- To allow the virtual Edge to receive traffic in the **br-HA Link** with multiple destination MAC Addresses, change the security settings on the port group/virtual switch to allow it to run in **Promiscuous** mode.

---

**Note** For more information on **MAC address changes** and **Promiscuous mode operation**, refer to the topic <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-3507432E-AFEA-4B6B-B404-17A020575358.html>.

---

## Limitations of VMware SD-WAN High Availability

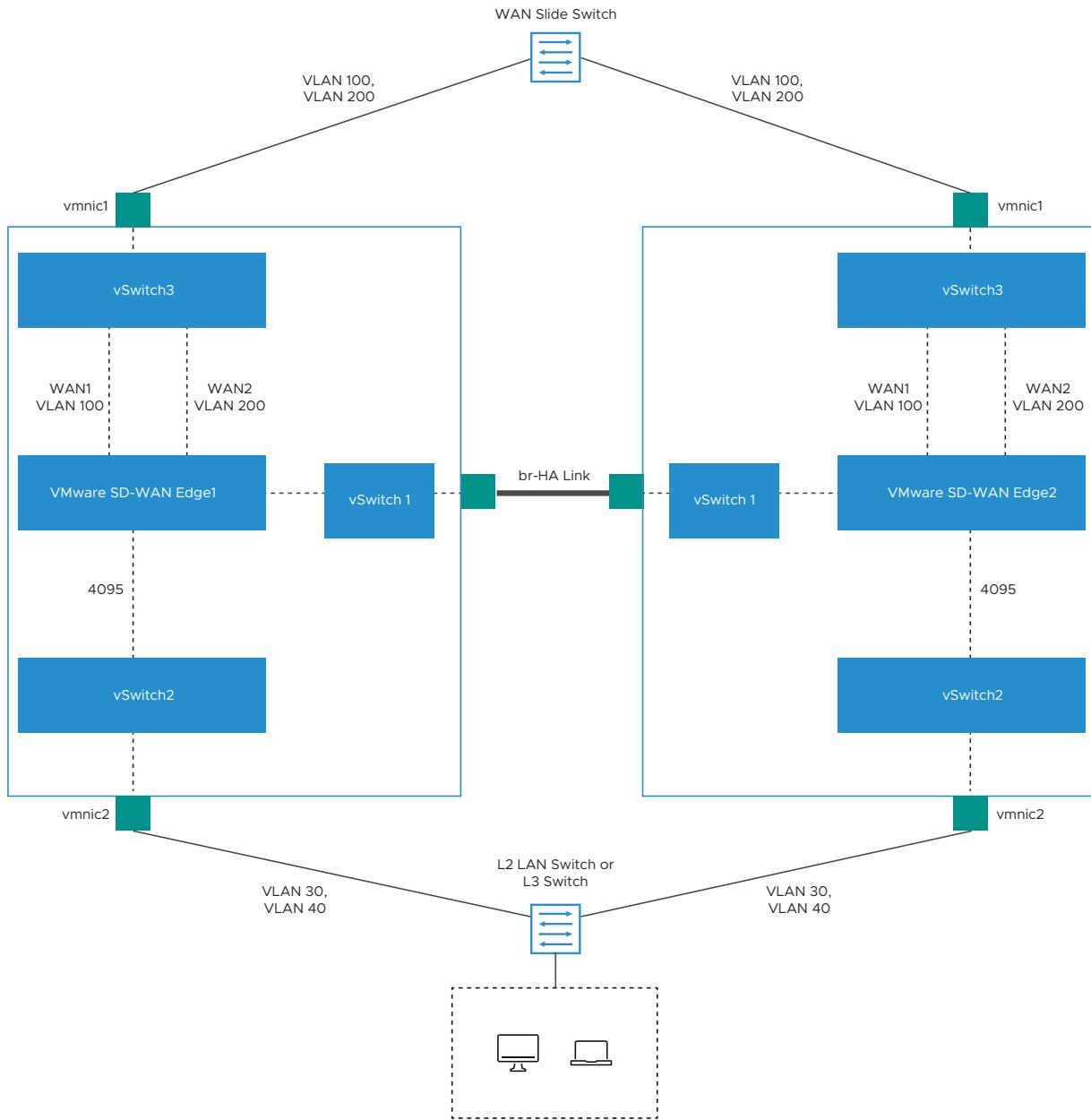
- There is no generic way of failure detection that will work on all the hardware, virtual, and uCPE platforms.

You can enable the Loss of Signal (LoS) detection to determine the HA Failover. For more information, see [HA LoS Detection on Routed Interfaces](#).

VMware SD-WAN supports the following topologies while deploying HA on VMware ESXi:

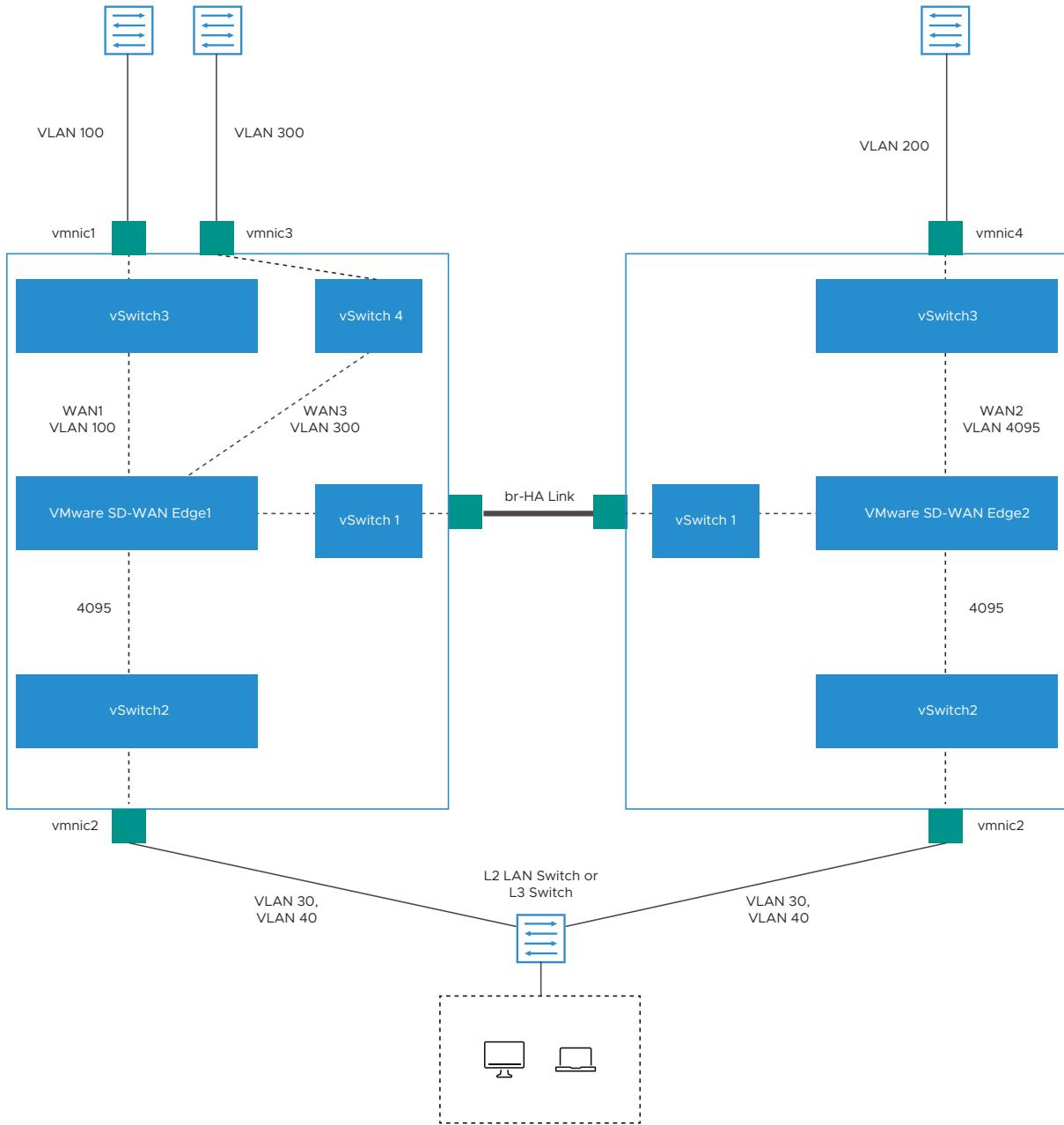
### Topology 1: Legacy HA with WAN links

The following image illustrates a topology with legacy HA along with WAN links that have been uplinked using a single physical adapter and one routed LAN or trunked LAN through single physical adapter.



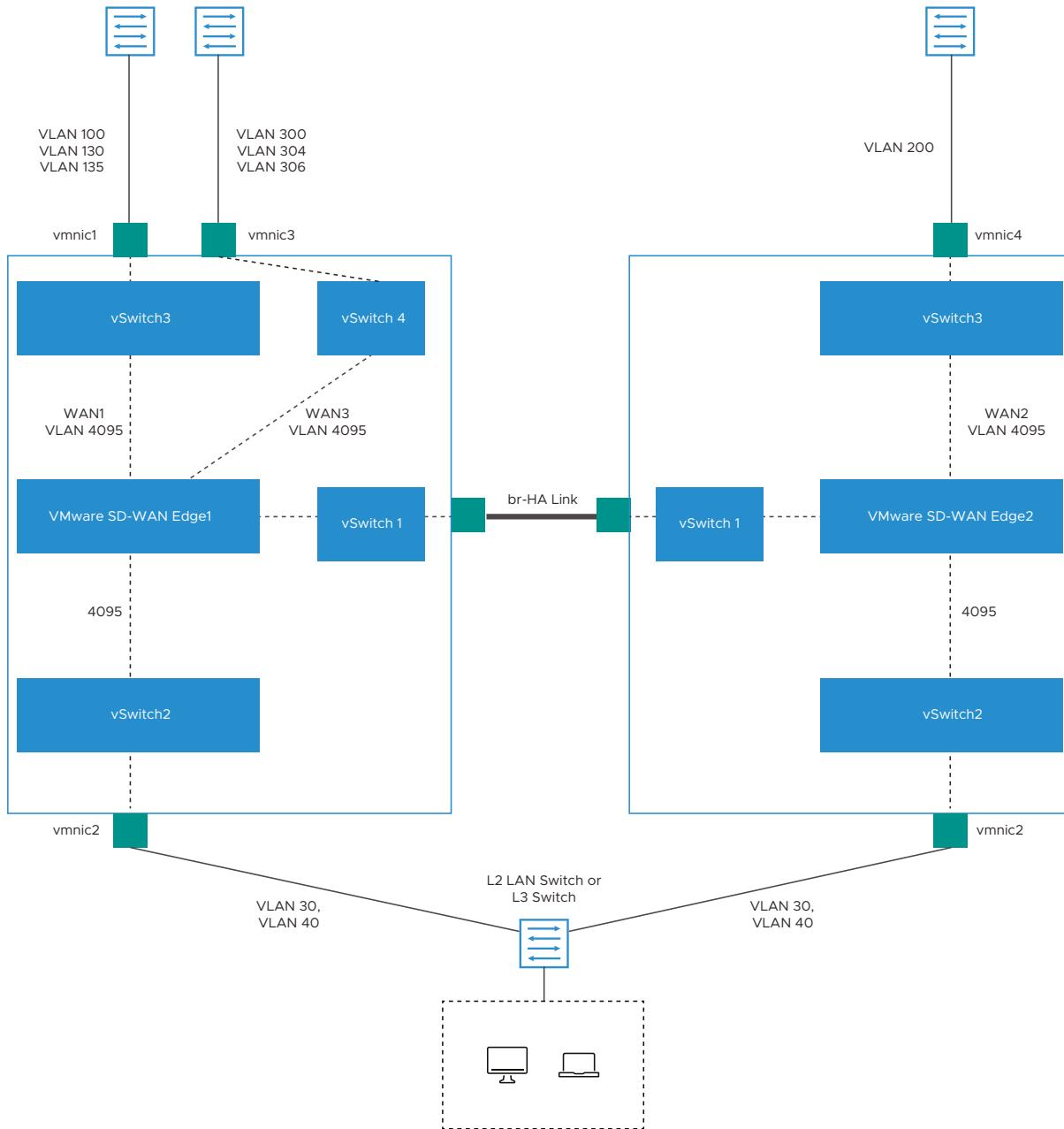
## Topology 2: Enhanced HA with WAN Links

The following topology shows enhanced HA with three WAN links.



### Topology 3: Enhanced HA with Subinterfaces

The following image shows Enhanced HA with subinterfaces on the WAN interfaces with VLAN ID as 4095 on port group.



## HA LoS Detection on Routed Interfaces

The HA Loss of Signal (LoS) detection enables an Edge to detect reachability failures in HA deployments on routed Interfaces.

When an Edge is enabled with HA, the number of LAN and WAN Interfaces connected to the Edge are detected and this count is used to take decision on performing the HA failover.

When Edges in HA mode are deployed on ESXi, the LAN and WAN vNICs of the Edge are uplinked through single or multiple physical NICs. If one of the physical NICs is down, the Interface count computed by HA will not be different from the Edge vNICs. The vSwitch connections remain intact, preventing the HA Failover.

By enabling the LoS detection on a routed Interface, it is possible to determine the Loss of Signal and Failover. The LoS detection can be done based on ARP monitoring of next hop for routed Interfaces. The LoS detection is done only on active Edge and only for Interfaces that are UP.

If an Interface is physically up but LoS is detected, then the Interface will be considered down and the relevant action, that is HA Failover, will be taken based on active and standby Interface count. LoS detection is done only on parent Interface and not on its sub Interfaces as the underlying physical link is common for both. When the Interface misses three consecutive ARP responses with the configured probe interval, it is considered to be down with LoS.

### **Limitations of LoS**

- LoS detection works only for routed Interfaces as the Edge does not know the next hop in a switched Interface. LoS detection is not supported for PPPoE Interfaces and statically configured Interfaces without default Gateway provided.
- LoS detection is not supported for Interfaces which are UP only on standby Edge
- LoS probing is not done on the Interfaces of standby Edge. Hence, any Interface connectivity change on standby Edge cannot be detected.
- In a legacy HA deployment, all the Interfaces on Standby Edge are blocked. As LoS monitoring uses ARP probing to detect liveliness of link, the connectivity state of links present on the Standby Edge cannot be ascertained because the Interfaces on Standby Edge are blocked and the ARP packets cannot go through.

### **Enable LoS Detection**

- 1 In the **SD-WAN** Settings of the Enterprise portal, click **Configure > Edges**.
- 2 Click the Device Icon next to an Edge, or click the link to an Edge and then click the **Device** tab.
- 3 In the **Device** tab, scroll down to the **Interface Settings** section, which displays the Interfaces available in the selected Edge.
- 4 Click the **Edit** option for an Interface to view and modify the settings.
- 5 Select the **Override Interface** checkbox to modify the configuration settings for the selected Interface.
- 6 In the **L2 Settings** section, select the **Enable LoS Detection** checkbox to enable Loss of Signal (LoS) detection by using ARP monitoring.
- 7 Select the **ARP Probe Interval** from the drop-down list. The available options are 1, 3, 5, 10 seconds and the default value is 3 seconds. The LoS is detected on the Interface based on the probe interval. When the Interface does not receive 3 consecutive ARP responses, then the Interface is considered to be down by LoS.

8 Configure the other settings as required and click **Update**.

## Edge 610-LTE

X

Interface GE3

 Override

## Description

Enter Description (Optional)

Maximum 256 characters

## Interface Enabled

 Enabled

## Capability

Routed



## Segments

All Segments

## Radius Authentication

WAN Link must be disabled to configure RADIUS Authentication.

## ICMP Echo Response

 Enabled

## Underlay Accounting

 Enabled

## Enable WAN Link

 Enabled

## DNS Proxy

 Enabled

## VLAN

 Enabled

## EVDSL Modem Attached

 Enabled

## IPv4 Settings

Static

IP Address \* CIDR Prefix \* Gateway 

## WAN Link

Auto-Detect



Unlock

## OSPF

OSPF not enabled for the selected Segment

## Multicast

Multicast is not enabled for the selected segment

## Advertise

 Enabled

## NAT Direct Traffic

 Enabled

## Trusted Source

 Enabled

Specific



Reverse Path Forwarding options are only settable when trusted zone is checked. When

9 Click **Save Changes** in the Devices tab.

For more information on the other settings of the Interface, see [Configure Interface Settings for Profiles](#).

To view the LoS detection events, see [Monitor Events for LoS Detection](#).

## Monitor Events for LoS Detection

You can view the events related to the LoS Detection on a routed Interface of a virtual Edge.

In the enterprise portal, click **Monitor > Events**.

To view the events related to LoS Detection, you can use the filter option. Click the drop-down arrow next to the **Search** option and choose to filter either by the Event or by the Message column.

The following events occur during LoS detection:

- LoS detected on peer's Interface <*Interface name*>
- LoS no longer seen on Interface <*Interface name*>

## Unique MAC Address

Unique MAC Address is for virtual High Availability environments that also have VNF Service Chaining, which requires a unique MAC address on the Active and Standby edges.

Instead of generating a common or shared virtual MAC address when in HA, this feature uses the physical MAC address for hardware Edges and the assigned MAC address for virtual Edges.

This feature also helps with virtual HA deployments in general, and is recommended if MAC Learning on the vSwitch isn't an option to use.

**Important** On a customer enterprise using HA Edges and VMware vSwitches: where possible, MAC learning should be configured on all vSwitches. MAC learning is available on vSphere version 6.7 and later. If MAC learning is configured on all vSwitches, **Unique MAC Address** is not required. However if the vSwitches do not have MAC learning configured, **Unique MAC Address** is required on the HA Edge.

For more information on MAC learning with vSphere Networking, see: [What is MAC Learning Policy](#).

## Configure a Unique LAN MAC Address

By default, High Availability uses a common virtual MAC address to support seamless failover between devices. If you need to use a unique MAC address in certain virtual environments, instead of generating a common or shared virtual MAC address, you can select the **Deploy with Unique LAN MAC** checkbox, which is deactivated by default. This option will use the physical MAC address for hardware Edges and the assigned MAC address for virtual Edges. The LAN and Routed LAN use physical MAC address, while the WAN links would still use virtual MAC address.

You can activate or deactivate the **Deploy with Unique LAN MAC** option only when you enable High Availability by choosing **Active Standby Pair**. Once High Availability is enabled, you cannot activate or deactivate **Deploy with Unique LAN MAC** at a later point of time.

## ✓ High Availability

### ✗ HA: Active Standby Pair

Segment Agnostic

High Availability is enabled at the Edge level. When using Active/Standby Pair HA, enable HA prior to connecting the Standby SD-WAN Edge. To learn more, please consult our HA documentation

#### Select Type

- None
- Active Standby Pair
- Cluster
- VRRP with 3rd party router

HA Interface ⓘ GE1 ▾

⚠ The VLAN value configured for the switched access port is reset to the value derived from the associated profile before moving to an HA Interface

Deploy with Unique LAN MAC Address ⓘ  Enable Graceful Switchover (require Graceful Restart in routing protocol)

✗ Advanced Settings

If you need to activate or deactivate the option, follow these steps:

- 1 Disconnect the Standby Edge's WAN and LAN links, leaving only the HA link connected to the Active Edge. If it is a Virtual Edge, disable the virtual NICs that correspond to the WAN and LAN links, leaving only the HA interface NIC connected.
- 2 In the **High Availability** section, click **None**.
- 3 Click **Save Changes** at the top of the **Device** window.
- 4 Enable High Availability again and then click the **Deploy with Unique LAN MAC** checkbox to activate or deactivate the option.
- 5 Once the HA status becomes High Availability Ready on the Orchestrator UI, reconnect the LAN and WAN cables of the Standby Edge. If using Virtual Edges, reenable the virtual NICs.

## Prerequisites

This section describes HA requirements that must be met before configuring a SD-WAN Edge as a Standby.

- The two SD-WAN Edges must be the same model.

**Note Mixing Wi-Fi Capable and Non-Wi-Fi Capable Edges in High Availability Is Supported in Release 5.4.0 and later.**

Beginning in 2021, VMware SD-WAN introduced Edge models which do not include a Wi-Fi module: the Edge models 510N, 610N, 620N, 640N, and 680N. Prior to Release 5.4.0, deploying a Wi-Fi capable Edge and a Non-Wi-Fi capable Edge of the same model (for example, an Edge 640 and an Edge 640N) as a High-Availability pair was not supported. With Release 5.4.0, this combination is supported and the customer can deploy Edges of the same model number with different Wi-Fi capabilities.

- Only one SD-WAN Edge should be provisioned on the SASE Orchestrator.
- The Standby SD-WAN Edge must not have an existing configuration on it.
- Ensure not to use 169.254.2.x for management interface.

## Activate High Availability

You can activate High Availability (HA) on a pair of Edges to ensure redundancy.

- In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- Select the SD-WAN Edge from the list and click the **Device** tab.
- Scroll down to the **High Availability** section and click **Active Standby Pair**.

- Click **Save Changes** at the bottom of the **Device** window.

By default, the HA interface to connect the pair is selected as follows:

- For Edges 520, 520v, and 540: The LAN1 port is used as HA interface and DPDK is not enabled on these platforms.
- For Edges 510, 610, 620, 640, 680, 840, 2000, 3400, and 3800: The GE1 port is used as HA interface and DPDK is enabled on these platforms.

## Configure a Non-Default High Availability Interface

The above HA interfaces are the default interfaces for their respective platforms and are selected automatically. Beginning with Release 5.2.0 you can also configure any LAN interface to be the HA interface with the **HA Interface** option.

In addition to choosing any Ethernet port configured as a LAN interface for HA traffic, beginning with Release 5.2.0, a user can configure any Edge 1G/10G SFP port to be the HA interface with the **HA Interface** option. As with an Ethernet port, the SFP port must first be configured as a LAN interface. For a list of supported SFP modules for use on SD-WAN Edges see: [VMware SD-WAN Supported SFP Module List \(79270\)](#).

Both HA Edges must be upgraded to Release 5.2.0 or later prior to using a non-default interface for HA traffic. Until both HA Edges are using Release 5.2.0, they must be configured to use the default GE1 as their HA interface. Only after both HA Edges are upgraded to Release 5.2.0 can a user configure the HA Edges to use an interface other than GE1 as the HA interface.

Configuring a non-default HA Interface can only be performed when HA is not enabled for that site. This means you can configure it prior to enabling HA for a site. However, if you want to change the HA Interface on a site where HA is already enabled, you must first disable HA, then change the HA Interface, and then re-enable HA.

### Important

In the context of a High Availability (HA) site utilizing an alternative HA Interface, the replacement of the Standby Edge with a different Edge may result in activation issues if the new Edge has a factory image earlier than version 5.2.0. To ensure a successful activation in such a scenario, it is imperative to take the following sequential steps:

- Disable HA.
- Reconfigure the HA Interface to its default value (GE1 or LAN1) on the UI, and relocate the HA Interface cable to the default HA Edge interface.
- Integrate the replacement Edge into the HA topology of the site.
- Re-enable HA and allow the replacement Edge to complete the activation process, assuming the role of the Standby Edge.
- Disable HA.
- Reconfigure the HA Interface to its alternative value on the UI, and relocate the HA Interface cable back to the alternative location on the HA Edges.
- Re-enable HA to finalize the replacement process.

## Configure a Unique LAN MAC Address

By default, High Availability uses a common virtual MAC address to support seamless failover between devices. If you need to use a unique MAC address in certain virtual environments, instead of generating a common or shared virtual MAC address, you can select the **Deploy with Unique LAN MAC** checkbox, which is deactivated by default. This option will use the physical MAC address for hardware Edges and the assigned MAC address for virtual Edges. The LAN and Routed LAN use physical MAC address, while the WAN links would still use virtual MAC address.

You can activate or deactivate the **Deploy with Unique LAN MAC** option only when you enable High Availability by choosing **Active Standby Pair**. Once High Availability is enabled, you cannot activate or deactivate **Deploy with Unique LAN MAC** at a later point of time.

If you need to activate or deactivate the option, follow these steps:

- 1 Disconnect the Standby Edge's WAN and LAN links, leaving only the HA link connected to the Active Edge. If it is a Virtual Edge, disable the virtual NICs that correspond to the WAN and LAN links, leaving only the HA interface NIC connected.
- 2 In the **High Availability** section, click **None**.
- 3 Click **Save Changes** at the top of the **Device** window.
- 4 Enable High Availability again and then click the **Deploy with Unique LAN MAC** checkbox to activate or deactivate the option.
- 5 Once the HA status becomes High Availability Ready on the Orchestrator UI, reconnect the LAN and WAN cables of the Standby Edge. If using Virtual Edges, reenable the virtual NICs.

## Advanced Options: HA Failover Detection Time Multiplier

Beginning in Release 5.2.0, a user can manually configure the time threshold before the Active Edge is marked as non-responsive which would trigger a failover to the Standby Edge. On some Edge platforms an Edge may experience a high amount of traffic sufficient to delay sending out a heartbeat response to the Standby Edge indicating that it is still functioning. This delay may exceed the default 700 millisecond threshold and trigger the Standby Edge to become active and results in an Active-Active (Split-Brain) state. With this feature, the user can increase the time threshold before the Active Edge is declared down and trigger a failover and prevent a potential split-brain state.

The value is changed under the **Advanced Options** section where a user configures the **HA Failover Detection Time Multiplier**. This multiplier is a number that is multiplied by 100 milliseconds (ms). The default value is 7 (700 ms) and be configured up to 70 (7000 ms).

High Availability

HA: None

Segment Agnostic

High Availability is enabled at the Edge level. When using Active/Standby Pair HA, enable HA prior to connecting the Standby SD-WAN Edge. To learn more, please consult our HA documentation.

Select Type

- None
- Active Standby Pair
- Cluster
- VRRP with 3rd party router

HA Interface ⓘ

Deploy with Unique LAN MAC Address ⓘ  Enable Graceful Switchover (require Graceful Restart in routing protocol)

Advanced Settings

HA Failover Detection Time Multiplier \* ⓘ 7

DISCARD CHANGES ⓘ SAVE CHANGES

## Advanced Options: HA Failover Detection Time Multiplier

### Wait for SD-WAN Edge to Assume Active

After the High Availability feature is enabled on the SASE Orchestrator, wait for the existing SD-WAN Edge to assume an Active role, and wait for the SASE Orchestrator Events to display **High Availability Going Active**.

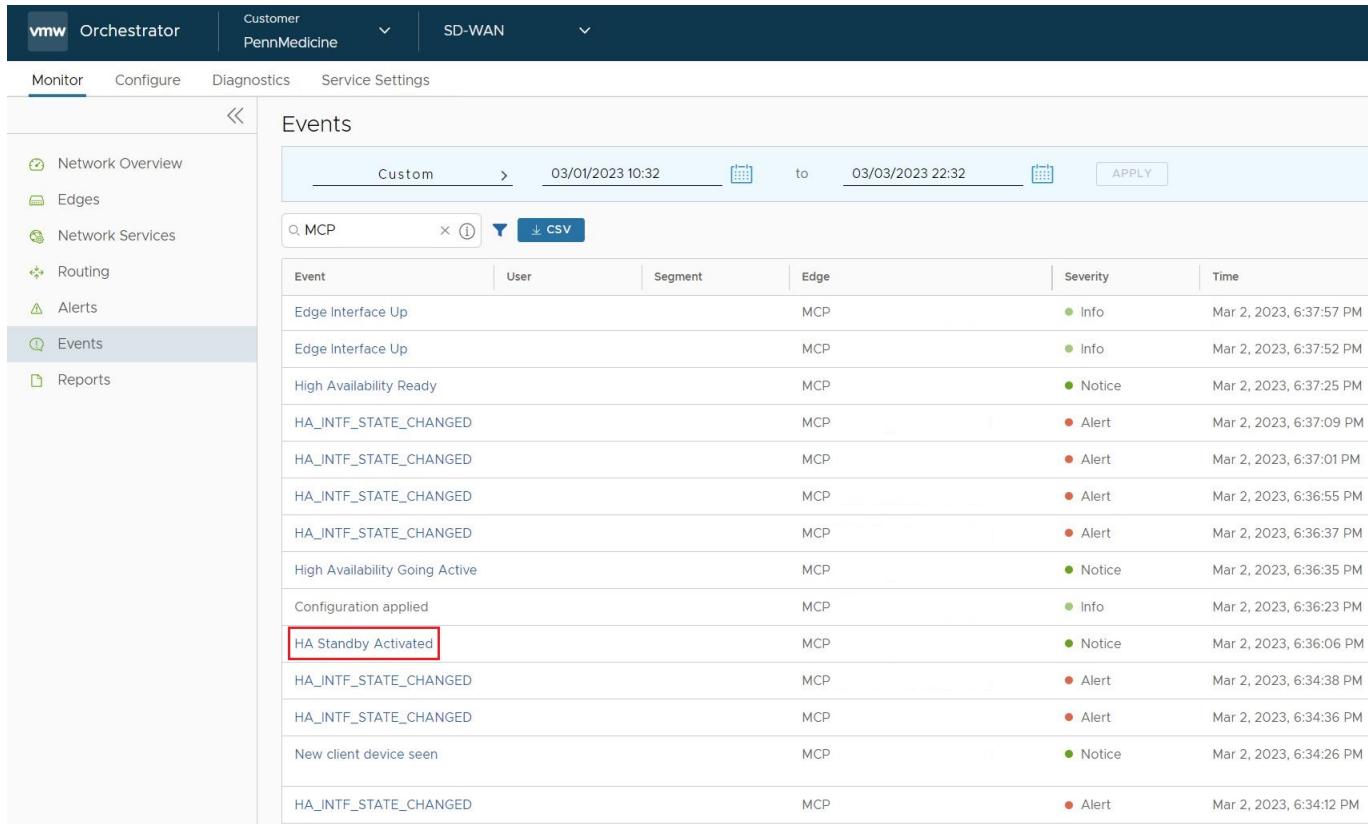
Events

Event	User	Segment	Edge	Severity	Time	Message
High Availability Ready	MCP			Notice	Mar 2, 2023, 7:17:18 PM	Standby state ready for failover
Edge Interface Up	MCP			Info	Mar 2, 2023, 7:17:18 PM	Interface GES_20 is up
Edge Interface Up	MCP			Info	Mar 2, 2023, 7:17:12 PM	Interface GES_10 is up
HA_INTF_STATE_CHANGED	MCP			Alert	Mar 2, 2023, 7:16:56 PM	HA interface Up
HA_INTF_STATE_CHANGED	MCP			Alert	Mar 2, 2023, 7:16:48 PM	HA interface Down
HA_INTF_STATE_CHANGED	MCP			Alert	Mar 2, 2023, 7:16:38 PM	HA interface Up
Edge Interface Up	MCP			Info	Mar 2, 2023, 7:13:00 PM	Interface GE4 is up
Edge Interface Up	MCP			Info	Mar 2, 2023, 7:12:55 PM	Interface GES_3568 is up
High Availability Going Active	MCP			Notice	Mar 2, 2023, 7:12:52 PM	Velocloud Edge going active, peer has not been detected

### Connect the Standby SD-WAN Edge to the Active Edge

- 1 Power on the Standby SD-WAN Edge without any network connections.
- 2 After it boots up, connect the LAN1/GE1 interface (as indicated on the **Device** tab) to the same interface on the Active SD-WAN Edge.

- 3 Wait for the Active SD-WAN Edge to detect and activate the standby SD-WAN Edge automatically. The SASE Orchestrator Events displays **HA Standby Activated** when the SASE Orchestrator successfully activates the standby SD-WAN Edge.



The screenshot shows the VMware Orchestrator interface with the 'Events' tab selected. The left sidebar includes options like Network Overview, Edges, Network Services, Routing, Alerts, Events (which is selected), and Reports. The main area shows a table of events with columns for Event, User, Segment, Edge, Severity, and Time. The 'Event' column lists various system messages, and the 'Edge' column consistently shows 'MCP'. The 'Severity' column uses colored dots to indicate the level of the event. The 'Time' column shows dates and times from March 2, 2023. The row for 'HA Standby Activated' is highlighted with a red box.

Event	User	Segment	Edge	Severity	Time
Edge Interface Up			MCP	Info	Mar 2, 2023, 6:37:57 PM
Edge Interface Up			MCP	Info	Mar 2, 2023, 6:37:52 PM
High Availability Ready			MCP	Notice	Mar 2, 2023, 6:37:25 PM
HA_INTF_STATE_CHANGED			MCP	Alert	Mar 2, 2023, 6:37:09 PM
HA_INTF_STATE_CHANGED			MCP	Alert	Mar 2, 2023, 6:37:01 PM
HA_INTF_STATE_CHANGED			MCP	Alert	Mar 2, 2023, 6:36:55 PM
HA_INTF_STATE_CHANGED			MCP	Alert	Mar 2, 2023, 6:36:37 PM
High Availability Going Active			MCP	Notice	Mar 2, 2023, 6:36:35 PM
Configuration applied			MCP	Info	Mar 2, 2023, 6:36:23 PM
HA Standby Activated			MCP	Notice	Mar 2, 2023, 6:36:06 PM
HA_INTF_STATE_CHANGED			MCP	Alert	Mar 2, 2023, 6:34:38 PM
HA_INTF_STATE_CHANGED			MCP	Alert	Mar 2, 2023, 6:34:36 PM
New client device seen			MCP	Notice	Mar 2, 2023, 6:34:26 PM
HA_INTF_STATE_CHANGED			MCP	Alert	Mar 2, 2023, 6:34:12 PM

The standby Edge will then begin to synchronize with the active SD-WAN Edge and reboot automatically during the process.

**Note** It may take up to 10 minutes for the Standby SD-WAN Edge to sync with the Active Edge and upgrade its software.

## Connect LAN and WAN Interfaces on Standby SD-WAN Edge

Connect the LAN and WAN interfaces on the standby SD-WAN Edge mirroring the network connectivity on the Active Edge.

The SASE Orchestrator Events will display **Standby device software update completed**. The **HA State** in the **Monitor > Edges** page appears green when ready.

The screenshot shows the VMware SD-WAN Orchestrator interface. The top navigation bar includes the VMware logo, 'Orchestrator', 'Customer' dropdown, 'SD-WAN' dropdown, and tabs for 'Monitor', 'Configure', 'Diagnostics', and 'Service Settings'. The 'Monitor' tab is selected. On the left, a sidebar menu lists 'Network Overview', 'Edges' (which is selected and highlighted in blue), 'Network Services', 'Routing', 'Alerts', 'Events', and 'Reports'. The main content area is titled 'Edges' and displays a table of SD-WAN edges. The table has columns for 'Name', 'Status', 'HA', 'Links', and 'VNFs'. The data in the table is as follows:

Name	Status	HA	Links	VNFs
MCP-10	Connected	Standby ready	(2)	
625	Connected	Standby ready	(3)	
10F	Connected		(3)	
102-M	Connected		(3)	

## Deactivate High Availability (HA)

This section covers deactivating a High Availability site and making it a Standalone site, one using a single Edge.

If you want a site configured with High Availability to instead work as a Standalone site with a single Edge, do the following:

- 1 In the **SD-WAN** Service of the Enterprise portal, click **Configure > Edges**.
- 2 Select the SD-WAN Edge from the list and click the **Device** tab.
- 3 Scroll down to the **High Availability** section and click **None**.

The screenshot shows the 'Device' tab for an SD-WAN Edge. Under the 'High Availability' section, the 'HA: None' option is selected. A note states: 'High Availability is enabled at the Edge level. When using Active/Standby Pair HA, enable HA prior to connecting the Standby SD-WAN Edge. To learn more, please consult our HA documentation'. Below this, a 'Select Type' section contains four radio button options: 'None' (selected), 'Active Standby Pair', 'Cluster', and 'VRRP with 3rd party router'.

- Click **Save Changes** at the top of the **Device** window.

**Note** When High Availability is deactivated on a pair of Edges, the following events are expected to occur:

- The existing **Active Edge** becomes the **Standalone Edge** for this site with no disruption in customer traffic. You can use the GE1 interface on the new **Standalone Edge** for a different purpose as it is no longer needed for HA.
- The **Standby Edge** is deactivated. This means the configuration is cleared from the Edge while retaining the existing Edge software version (the Edge is NOT factory reset). Once the Edge is completely deactivated, you can then remove all cables from the former **Standby Edge** and repurpose it to another deployment.

**Important** If the Standby Edge is removed from the HA deployment prior to deactivating HA, you would need to perform a separate Edge deactivation or factory reset for that Edge to make it usable in a different location because you cannot activate an Edge to a new location if there is an existing configuration on the Edge.

**Note** If the Standby Edge remains connected to the now Standalone Edge through the HA cable after HA is deactivated and is rebooted, the Edge may try to require certain configurations from the Standalone Edge and this would mean the former Standby Edge would need to be deactivated again or factory reset prior to being used at another location.

## HA Event Details

This section describes HA events.

HA Event	Description
HA_GOING_ACTIVE	A standby SD-WAN Edge is taking over as Active because it has not heard a heartbeat from the peer.
HA_STANDBY_ACTIVATED	When a new Standby is detected by the Active, the Active tries to activate the Edge by sending this event to the SASE Orchestrator. On a successful response, the Active will sync the configurations and sync data.
HA_FAILED	Typically happens after the HA pair has formed and the Active SD-WAN Edge no longer hears from the Standby SD-WAN Edge. For example, if the Standby SD-WAN Edge reboots, you will receive this message.
HA_READY	Means the Active SD-WAN Edge now hears from the Standby SD-WAN Edge. Once the Standby SD-WAN Edge comes back up and reestablishes the heartbeat, then you will receive this message.
HA_TERMINATED	When the HA configuration is deactivated, and it is successfully applied on the Edges, this Event is generated.
HA_ACTIVATION_FAILURE	If the SASE Orchestrator is unable to verify the HA activation, it will generate this Event. Examples include: <ul style="list-style-type: none"> <li>■ the SASE Orchestrator is unable to generate a certificate</li> <li>■ the HA has been deactivated (rare)</li> </ul>

VCO_IDENTIFIED_HA_FAILOVER	<p>Event message reads: <b>Edge HA Failover Detected</b></p> <p>The SASE Orchestrator has detected that a High Availability failover has occurred on the Edge.</p>
VCO_IDENTIFIED_HA_FAILURE	<p>Event message reads: <b>Edge HA Failure Detected</b></p> <p>The SASE Orchestrator has detected that the Standby Edge has gone down. This event will include the serial number of the Edge.</p>
HA_UPDATE_FAILOVER_TIME	<p>Event message reads: <b>Updating HA Failover time from #####ms to #####ms</b></p> <p>A user changed the failover time for when an HA Edge will failover based on how long the Edge will wait to receive a heartbeat from the Active Edge. Increasing this value can prevent an Active-Active "Split Brain" state for HA Edges under high load. This is done through the <b>HA Failover Detection Time Multiplier</b> located at <b>Configure &gt; Edge &gt; Device &gt; High Availability</b> on the Orchestrator.</p>
HA_RESET_FAILOVER_TIME	<p>Event message reads: <b>Updating HA Failover time from #####ms to #####ms</b></p> <p>When an HA Edge's system has been stable for 60 seconds, the process reduces the failover threshold time by 50%.</p>

# VMware Virtual Edge Deployment

42

The Virtual Edge is available as a virtual machine that can be installed on standard hypervisors. This section describes the prerequisites and the installation procedure for deploying a VMware Virtual Edge on KVM and VMware ESXi hypervisors.

Read the following topics next:

- [Deployment Prerequisites for VMware Virtual Edge](#)
- [Special Considerations for VMware Virtual Edge deployment](#)
- [Cloud-init Creation](#)
- [Install VMware Virtual Edge](#)

## Deployment Prerequisites for VMware Virtual Edge

Describes the requirements for VMware Virtual Edge deployment.

### Virtual Edge Requirements

Keep in mind the following requirements before you deploy a Virtual Edge:

- Supports 2, 4, 8, and 10 vCPU assignment.

	2 vCPU	4v CPU	8 vCPU	10 vCPU
Minimum Memory (DRAM)	8 GB	16 GB	32 GB	32 GB
Minimum Storage (Virtual Disk)	8 GB	8 GB	16 GB	16 GB

- AES-NI CPU capability must be passed to the Virtual Edge appliance.
- Up to 8 vNICs (default is GE1 and GE2 LAN ports, and GE3-GE8 WAN ports).

**Caution** Over-subscription of Virtual Edge resources such as CPU, memory, and storage, is not supported.

## Recommended Server Specifications

NIC Chipset	Hardware	Specification
Intel 82599/82599ES	HP DL380G9	<a href="http://www.hp.com/hpinfo/newsroom/press_kits/2014/ComputeEra/HP_ProLiantDL380_DataSheet.pdf">http://www.hp.com/hpinfo/newsroom/press_kits/2014/ComputeEra/HP_ProLiantDL380_DataSheet.pdf</a>
Intel X710/XL710	Dell PowerEdge R640	<p><a href="https://www.dell.com/en-us/work/shop/povw/poweredge-r640">https://www.dell.com/en-us/work/shop/povw/poweredge-r640</a></p> <ul style="list-style-type: none"> <li>■ CPU Model and Cores - Dual Socket Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz with 16 cores each</li> <li>■ Memory - 384 GB RAM</li> </ul>
Intel X710/XL710	Supermicro SYS-6018U-TRTP+	<p><a href="https://www.supermicro.com/en/products/system/1U/6018/SYS-6018U-TRTP_.cfm">https://www.supermicro.com/en/products/system/1U/6018/SYS-6018U-TRTP_.cfm</a></p> <ul style="list-style-type: none"> <li>■ CPU Model and Cores - Dual Socket Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz with 10 Cores each</li> <li>■ Memory - 256 GB RAM</li> </ul>

## Recommended NIC Specifications

Hardware Manufacturer	Firmware Version	Host Driver for Ubuntu 20.04.6	Host Driver for Ubuntu 22.04.2	Host Driver for ESXi 7.0U3	Host Driver for ESXi 8.0U1a
Dual Port Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+	7.10	2.20.12	2.20.12	1.11.2.5 and 1.11.3.5	1.11.2.5 and 1.11.3.5
Dual Port Intel Corporation Ethernet Controller X710 for 10GbE SFP+	7.10	2.20.12	2.20.12	1.11.2.5 and 1.11.3.5	1.11.2.5 and 1.11.3.5
Quad Port Intel Corporation Ethernet Controller X710 for 10GbE SFP+	7.10	2.20.12	2.20.12	1.11.2.5 and 1.11.3.5	1.11.2.5 and 1.11.3.5

## Supported Operating Systems

- **Ubuntu Linux Distribution**
  - Ubuntu 20.04.6 LTS
  - Ubuntu 22.04.2 LTS
- **VMware ESXi**
  - VMware ESXi 7.0U3 with VMware vSphere Web Client 7.0.
  - VMware ESXi 8.0 U1a with VMware vSphere Web Client 8.0.

## Firewall/NAT Requirements

If the VMware Virtual Edge is deployed behind the Firewall and/or a NAT device, the following requirements apply:

- The Firewall must allow outbound traffic from the VMware Virtual Edge to TCP/443 (for communication with the SASE Orchestrator).
- The Firewall must allow traffic outbound to Internet on ports UDP/2426 (VCMP).

## CPU Flags Requirements

For detailed information about CPU flags requirements to deploy Virtual Edge, see [Special Considerations for VMware Virtual Edge deployment](#).

## Special Considerations for VMware Virtual Edge deployment

Describes the special considerations for VMware Virtual Edge deployment.

- The SD-WAN Edge is a latency-sensitive application. Refer to the [VMware documentation](#) to adjust the Virtual Machine (VM) as a latency-sensitive application.
- Recommended Host settings:
  - BIOS settings to achieve highest performance:
    - CPUs at 2.0 GHz or higher
    - Enable Intel Virtualization Technology (Intel VT)
    - Deactivate Hyper-threading
    - Virtual Edge supports paravirtualized vNIC VMXNET 3 and passthrough vNIC SR-IOV:
      - When using VMXNET3, deactivate SR-IOV on host BIOS and ESXi
      - When using SR-IOV, enable SR-IOV on host BIOS and ESXi
      - To enable SR-IOV on VMware and KVM, see:
        - KVM - [Activate SR-IOV on KVM](#)
        - VMware - [Enable SR-IOV on VMware](#)
    - Deactivate power savings on CPU BIOS for maximum performance
    - Activate CPU turbo
    - CPU must support the AES-NI, SSSE3, SSE4, RDTSC, RDSEED, RDRAND instruction sets
    - Recommend reserving 2 cores for Hypervisor workloads
 

For example, for a 10-core CPU system, recommend running one 8-core virtual edge or two 4-core virtual edge and reserve 2 cores for Hypervisor processes.

- For a dual socket host system, make sure the hypervisor is assigning network adapters, memory and CPU resources that are within the same socket (NUMA) boundary as the vCPUs assigned.
- Recommended VM settings:
  - CPU should be set to '100% reserved'
  - CPU shares should be set to High
  - Memory should be set to '100% reserved'
  - Latency sensitivity should be set to High
- The default username for the SD-WAN Edge SSH console is `root`.

## Cloud-init Creation

Cloud-init is a Linux package responsible for handling early initialization of instances. If available in the distributions, it allows for configuration of many common parameters of the instance directly after installation. This creates a fully functional instance that is configured based on a series of inputs. The cloud-init config is composed of two main configuration files, the metadata file and the user-data file. The meta-data contains the network configuration for the Edge, and the user-data contains the Edge Software configuration. The cloud-init file provides information that identifies the instance of the VMware Virtual Edge being installed.

Cloud-init's behavior can be configured via user-data. User-data can be given by the user at the time of launching the instance. This is typically done by attaching a secondary disk in ISO format that cloud-init will look for at first boot time. This disk contains all early configuration data that will be applied at that time.

The VMware Virtual Edge supports cloud-init and all essential configurations packaged in an ISO image.

### Create the cloud-init metadata and user-data Files

The final installation configuration options are set with a pair of cloud-init configuration files. The first installation configuration file contains the metadata. Create this file with a text editor and name it `meta-data`. This file provides information that identifies the instance of the VMware Virtual Edge being installed. The instance-id can be any identifying name, and the local-hostname should be a host name that follows your site standards.

#### 1 Create the meta-data file that contains the instance:

```
name.instance-id: vedge1
local-hostname: vedge1
```

- 2 Add the `network-interfaces` section, shown below, to specify the WAN configuration. By default, all SD-WAN Edge WAN interfaces are configured for DHCP. Multiple interfaces can be specified.

```
root@ubuntu# cat meta-data
instance-id: Virtual-Edge
local-hostname: Virtual-Edge
network-interfaces:
  GE1:
    mac_address: 52:54:00:79:19:3d
  GE2:
    mac_address: 52:54:00:67:a2:53
  GE3:
    type: static
    ipaddr: 11.32.33.1
    mac_address: 52:54:00:e4:a4:3d
    netmask: 255.255.255.0
    gateway: 11.32.33.254
  GE4:
    type: static
    ipaddr: 11.32.34.1
    mac_address: 52:54:00:14:e5:bd
    netmask: 255.255.255.0
    gateway: 11.32.34.254
```

- 3 Create the `user-data` file. This file contains three main modules: SASE Orchestrator, Activation Code, and Ignore Certificates Errors.

Module	Description
vco	IP Address/URL of the SASE Orchestrator.
activation_code	Activation code for the Virtual Edge. The activation code is generated while creating an Edge instance on the SASE Orchestrator.
vco_ignore_cert_errors	Option to verify or ignore any certificate validity errors.

The activation code is generated while creating an Edge instance on the SASE Orchestrator.

**Important** There is no default password in SD-WAN Edge image. The password must be provided in `cloud-config`:

```
#cloud-config
password: passw0rd
chpasswd: { expire: False }
ssh_pwauth: True
velocloud:
  vce:
    vco: 10.32.0.3
    activation_code: F54F-GG4S-XGFI
    vco_ignore_cert_errors: true
```

## Create the ISO File

Once you have completed your files, they need to be packaged into an ISO image. This ISO image is used as a virtual configuration CD with the virtual machine. This ISO image (called seed.iso in the example below), is created with the following command on Linux system:

```
genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data network-data
```

Including the `network-interfaces` section is optional. If the section is not present, the DHCP option is used by default.

Once the ISO image is generated, transfer the image to a datastore on the host machine.

## Install VMware Virtual Edge

You can install VMware Virtual Edge on KVM and VMware ESXi using a cloud-init config file. The cloud-init config contains interface configurations and the activation key of the Edge.

### Prerequisites

Ensure you have created the cloud-init meta-data and user-data files and have packaged the files into an ISO image file. For steps, see [Cloud-init Creation](#).

KVM provides multiple ways to provide networking to virtual machines. VMware recommends the following options:

- SR-IOV
- Linux Bridge
- OpenVSwitch Bridge

If you decide to use SR-IOV mode, enable SR-IOV on KVM and VMware. For steps, see:

- [Activate SR-IOV on KVM](#)
- [Enable SR-IOV on VMware](#)

To install VMware Virtual Edge:

- On KVM, see [Install Virtual Edge on KVM](#).
- On VMware ESXi, see [Install Virtual Edge on VMware ESXi](#).

## Activate SR-IOV on KVM

To enable the SR-IOV mode on KVM, perform the following steps.

### Prerequisites

This requires a specific NIC card. The following chipsets are certified by VMware to work with the SD-WAN Gateway and SD-WAN Edge.

- Intel 82599/82599ES

- Intel X710/XL710

**Note** Before using the Intel X710/XL710 cards in SR-IOV mode on KVM, make sure the supported Firmware and Driver versions specified in the *Deployment Prerequisites* section are installed correctly.

**Note** SR-IOV mode is not supported if the KVM Virtual Edge is deployed with a High-Availability topology. For High-Availability deployments, ensure that SR-IOV is not enabled for that KVM Edge pair.

To enable SR-IOV on KVM:

- 1 Enable SR-IOV in BIOS. This will be dependent on your BIOS. Login to the BIOS console and look for SR-IOV Support/DMA. You can verify support on the prompt by checking that Intel has the correct CPU flag.

```
cat /proc/cpuinfo | grep vmx
```

- 2 Add the options on Bboot (in /etc/default/grub).

```
GRUB_CMDLINE_LINUX="intel_iommu=on"
```

- a Run the following commands: update-grub and update-initramfs -u.
- b Reboot
- c Make sure iommu is enabled.

```
velocloud@KVMperf3:~$ dmesg | grep -i IOMMU
[ 0.000000] Command line: BOOT_IMAGE=/vmlinuz-3.13.0-107-generic root=/dev/mapper/qa--multiboot--002--vg-root ro intel_iommu=on splash quiet vt.handoff=7
[ 0.000000] Kernel command line: BOOT_IMAGE=/vmlinuz-3.13.0-107-generic root=/dev/mapper/qa--multiboot--002--vg-root ro intel_iommu=on splash quiet vt.handoff=7
[ 0.000000] Intel-IOMMU: enabled
...
velocloud@KVMperf3:~$
```

- 3 Based on the NIC chipset used, add a driver as follows:

- For the **Intel 82599/82599ES** cards in SR-IOV mode:

- 1 Download and install **ixgbe** driver from the [Intel](#) website.
- 2 Configure ixgbe config (tar and sudo make install).

```
velocloud@KVMperf1:~$ cat /etc/modprobe.d/ixgbe.conf
```

- 3 If the ixgbe config file does not exist, you must create the file as follows.

```
options ixgbe max_vfs=32,32
options ixgbe allow_unsupported_sfp=1
options ixgbe MDD=0,0
blacklist ixgbefv
```

- 4 Run the update-initramfs -u command and reboot the Server.

- 5 Use the modinfo command to verify if the installation is successful.

```
velocloud@KVMperf1:~$ modinfo ixgbe and ip link
filename: /lib/modules/4.4.0-62-generic/updates/drivers/net/ethernet/intel/ixgbe/
ixgbe.ko
version: 5.0.4
license: GPL
description: Intel(R) 10GbE PCI Express Linux Network Driver
author: Intel Corporation, <linux.nics@intel.com>
srcversion: BA7E024DFE57A92C4F1DC93
```

- For the **Intel X710/XL710** cards in SR-IOV mode:

- 1 Download and install **i40e** driver from the [Intel](#) website.
- 2 Create the Virtual Functions (VFs).

```
echo 4 > /sys/class/net/device_name/device/sriov_numvfs
```

- 3 To make the VFs persistent after a reboot, add the command from the previous step to the "/etc/rc.d/rc.local" file.
- 4 Deactivate the VF driver.

```
echo "blacklist i40evf" >> /etc/modprobe.d/blacklist.conf
```

- 5 Run the update-initramfs -u command and reboot the Server.

## Validating SR-IOV (Optional)

You can quickly verify if your host machine has SR-IOV enabled by using the following command:

```
lspci | grep -i Ethernet
```

Verify if you have Virtual Functions:

```
01:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
```

## Install Virtual Edge on KVM

Describes how to install and activate the Virtual Edge on KVM using a cloud-init config file.

If you decide to use SR-IOV mode, enable SR-IOV on KVM. For steps, see [Activate SR-IOV on KVM](#).

---

**Note** SR-IOV mode is not supported if the KVM Virtual Edge is deployed with a High-Availability topology. For High-Availability deployments, ensure that SR-IOV is not enabled for that KVM Edge pair.

To run VMware Virtual Edge on KVM using the libvirt:

- 1 Use gunzip to extract the qcow2 file to the image location (for example, /var/lib/libvirt/images).
- 2 Create the Network pools that you are going to use for the device, using SR-IOV and OpenVswitch.

### Using SR-IOV

The following is a sample network interface template specific to Intel X710/XL710 NIC cards using SR-IOV.

```
<interface type='hostdev' managed='yes'>
    <mac address='52:54:00:79:19:3d' />
    <driver name='vfio' />
    <source>
        <address type='pci' domain='0x0000' bus='0x83' slot='0x0a' function='0x0' />
    </source>
    <model type='virtio' />
</interface>
```

### Using OpenVSwitch

```
<network>
    <name>passthrough</name>
    <model type='virtio' />
    <forward mode="bridge" />
    <bridge name="passthrough" />
    <virtualport type='openvswitch' />
    <vlan trunk='yes'>
        <tag id='33' nativeMode='untagged' />
        <tag id='200' />
        <tag id='201' />
        <tag id='202' />
    </vlan>
</network>

<network>
    <name>passthrough</name>
    <model type='virtio' />
    <forward mode="bridge" />
</network>

<domain type='kvm'>
    <name>vedge1</name>
```

```

<memory unit='KiB'>4194304</memory>
<currentMemory unit='KiB'>4194304</currentMemory>
<vcpu placement='static'>2</vcpu>
<resource>
    <partition>/machine</partition>
</resource>
<os>
    <type arch='x86_64' machine='pc-i440fx-trusty'>hvm</type>
    <boot dev='hd' />
</os>
<features>
    <acpi/>
    <apic/>
    <pae/>
</features>
<!-- Set the CPU mode to host model to leverage all the available features on the host
CPU -->
<cpu mode='host-model'>
    <model fallback='allow' />
</cpu>
<clock offset='utc' />
<on_poweroff>destroy</on_poweroff>
<on_reboot>restart</on_reboot>
<on_crash>restart</on_crash>
<devices>
    <emulator>/usr/bin/kvm-spice</emulator>
    <!-- Below is the location of the qcow2 disk image -->
    <disk type='file' device='disk'>
        <driver name='qemu' type='qcow2' />
        <source file='/var/lib/libvirt/images/edge-VC_KVM_GUEST-x86_64-2.3.0-18-R23-20161114-
GA-updatable-ext4.qcow2' />
        <target dev='sda' bus='sata' />
        <address type='drive' controller='0' bus='0' target='0' unit='0' />
    </disk>
    <!-- If using cloud-init to boot up virtual edge, attach the 2nd disk as CD-ROM -->
    <disk type='file' device='cdrom'>
        <driver name='qemu' type='raw' />
        <source file='/home/vcadmin/cloud-init/vedge1/seed.iso' />
        <target dev='sdb' bus='sata' />
        <readonly />
        <address type='drive' controller='1' bus='0' target='0' unit='0' />
    </disk>
    <controller type='usb' index='0'>
        <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2' />
    </controller>
    <controller type='pci' index='0' model='pci-root' />
    <controller type='sata' index='0'>
        <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0' />
    </controller>
    <controller type='ide' index='0'>
        <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1' />
    </controller>
    <!-- The first two interfaces are for the default L2 interfaces, NOTE VLAN support
just for SR-IOV and OpenvSwitch -->
    <interface type='network'>

```

```

<model type='virtio'/>
<source network='LAN1'/>
<vlan><tag id='#hole2_vlan#' /></vlan>
<alias name='LAN1' />
<address type='pci' domain='0x0000' bus='0x00' slot='0x12' function='0x0' />
</interface>
<interface type='network'>
<model type='virtio' />
<source network='LAN2' />
<vlan><tag id='#LAN2_VLAN#' /></vlan>
<alias name='hostdev1' />
<address type='pci' domain='0x0000' bus='0x00' slot='0x13' function='0x0' />
</interface>
<!-- The next two interfaces are for the default L3 interfaces. Note that additional 6
routed interfaces are supported for a combination of 8 interfaces total -->
<interface type='network'>
<model type='virtio' />
<source network='WAN1' />
<vlan><tag id='#hole2_vlan#' /></vlan>
<alias name='LAN1' />
<address type='pci' domain='0x0000' bus='0x00' slot='0x12' function='0x0' />
</interface>
<interface type='network'>
<model type='virtio' />
<source network='LAN2' />
<vlan><tag id='#LAN2_VLAN#' /></vlan>
<alias name='hostdev1' />
<address type='pci' domain='0x0000' bus='0x00' slot='0x13' function='0x0' />
</interface>
<serial type='pty'>
<target port='0' />
</serial>
<console type='pty'>
<target type='serial' port='0' />
</console>
<input type='mouse' bus='ps2' />
<input type='keyboard' bus='ps2' />
<graphics type='vnc' port=' -1' autoport='yes' listen='127.0.0.1'>
<listen type='address' address='127.0.0.1' />
</graphics>
<sound model='ich6'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0' />
</sound>
<video>
<model type='cirrus' vram='9216' heads='1' />
<address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0' />
</video>
<memballoon model='virtio'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0' />
</memballoon>
</devices>
</domain>

```

- 3 Save the domain XML file that defines the VM (for example, `vedge1.xml` created in step 2).

- 4 Launch the VM by performing the following steps:

- a Create VM.

```
virsh define vedge1.xml
```

- b Start VM.

```
virsh start vedge1
```

---

**Note** `vedge1` is the name of the VM defined in the `<name>` element of the domain XML file. Replace `vedge1` with the name you specify in the `<name>` element.

---

- 5 If you are using SR-IOV mode, after launching the VM, set the following on the Virtual Functions (VFs) used:

- a Set the spoofcheck off.

```
ip link set eth1 vf 0 spoofchk off
```

- b Set the Trusted mode on.

```
ip link set dev eth1 vf 0 trust on
```

- c Set the VLAN, if required.

```
ip link set eth1 vf 0 vlan 3500
```

---

**Note** The Virtual Functions configuration step is not applicable for OpenVSwitch (OVS) mode.

---

- 6 Console into the VM.

```
virsh list
Id Name State
-----
25 test_vcg running
velocloud@KVMperf2$ virsh console 25
Connected to domain test_vcg
Escape character is ^]
```

The Cloud-init already includes the activation key, which was generated while creating a new Virtual Edge on the SASE Orchestrator. The Virtual Edge is configured with the config settings from the Cloud-init file. This will configure the interfaces as the Virtual Edge is powered up. Once the Virtual Edge is online, it will activate with the SASE Orchestrator using the activation key. The SASE Orchestrator IP address and the activation key have been defined in the Cloud-init file.

## Enable SR-IOV on VMware

Enabling SR-IOV on VMware is an optional configuration.

## Prerequisites

This requires a specific NIC card. The following chipsets are certified by VMware to work with the SD-WAN Gateway.

- Intel 82599/82599ES
- Intel X710/XL710

---

**Note** Before using the Intel X710/XL710 cards in SR-IOV mode on VMware, make sure the supported Firmware and Driver versions described in the *Deployment Prerequisites* section are installed correctly.

---

To enable SR-IOV on VMware:

- 1 Make sure that your NIC card supports SR-IOV. Check the VMware Hardware Compatibility List (HCL) at <https://www.vmware.com/resources/compatibility/search.php?deviceCategory=io>

**Brand Name:** Intel

**I/O Device Type:** Network

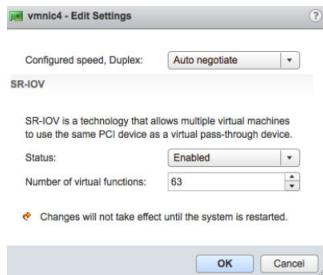
**Features:** SR-IOV

### VMware Compatibility Guide

The following VMware KB article provides details of how to enable SR-IOV on the supported NIC: <https://knowledge.broadcom.com/external/article?legacyId=2038739>.

- 2 Once you have a support NIC card, go to the specific VMware host, select the **Configure** tab, and then choose **Physical adapters**.

- 3 Select **Edit Settings**. Change **Status** to **Enabled** and specify the number of virtual functions required. This number varies by the type of NIC card.
- 4 Reboot the hypervisor.



- 5 If SR-IOV is successfully enabled, the number of Virtual Functions (VFs) will show under the particular NIC after ESXi reboots.

Physical adapters								
Device	Actual Speed	Configured Speed	Switch	MAC Address	Observed IP ranges	Wake on LAN Supported	SR-IOV Status	SR-IOV VFs
Intel(R) Ethernet Controller 10G X550T								
vmnic4	1000 Mb	Auto negotiate	-	a0:36:9f:d3:72:ba	172.16.4.4-172.16.4.4	No	Enabled	63 (61 currently...)
Intel Corporation 1350 Gigabit Network Connection								
vmnic2	1000 Mb	Auto negotiate	vSwitch0	00:25:90:fb:98:0c	0.0.1-255.255.255.25...	Yes	Disabled	-
vmnic3	Down	Auto negotiate	vSwitch1	00:25:90:fb:98:0d	No networks	No	Disabled	-
QLogic Corporation NetXtreme II BCM57810 10 Gigabit Ethernet								
vmnic0	Down	Auto negotiate	-	00:25:90:8ea:54	No networks	Yes	Not supported	-

**Note** To support VLAN tagging on SR-IOV interfaces, user must configure VLAN ID 4095 (Allow All) on the Port Group connected to the SR-IOV interface. For more information, see [VLAN Configuration](#).

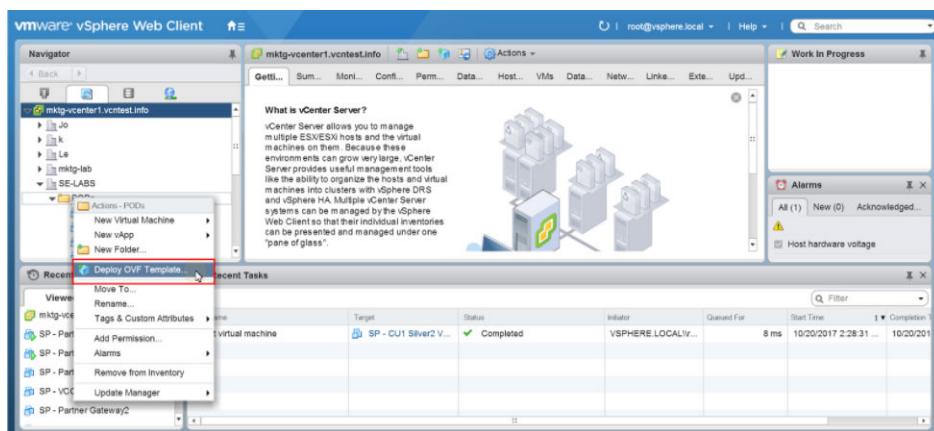
## Install Virtual Edge on VMware ESXi

Describes how to install Virtual Edge on VMware ESXi.

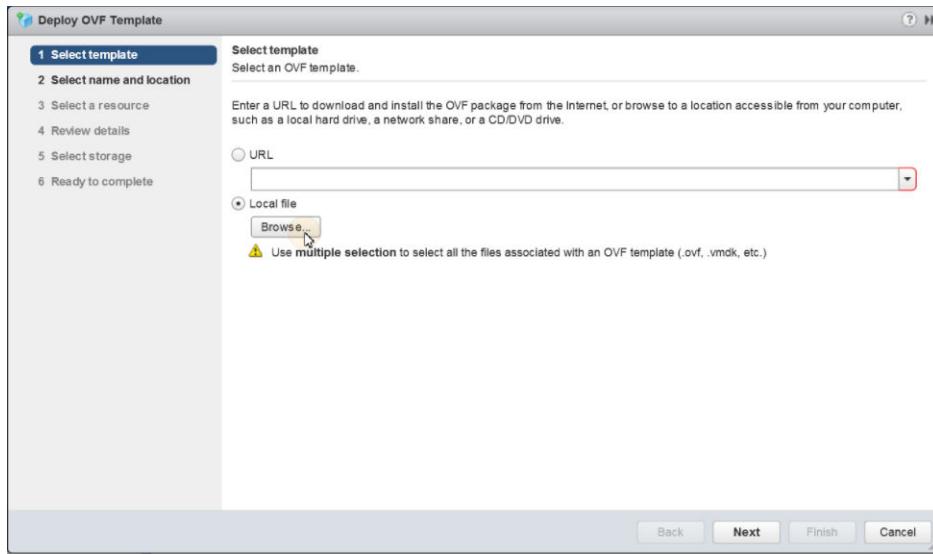
If you decide to use SR-IOV mode, enable SR-IOV on VMware. For steps, see [Enable SR-IOV on VMware](#).

To install Virtual Edge on VMware ESXi:

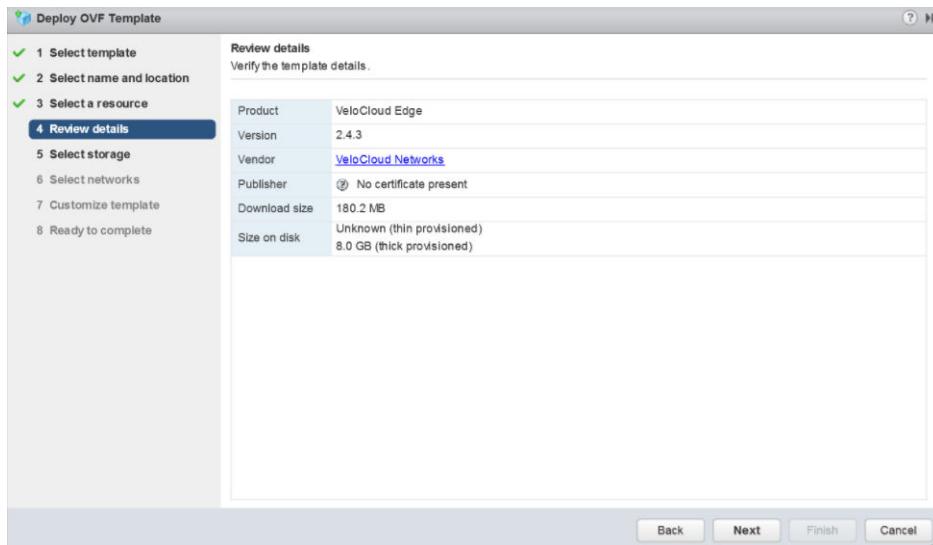
- 1 Use the vSphere client to deploy an OVF template, and then select the Edge OVA file.



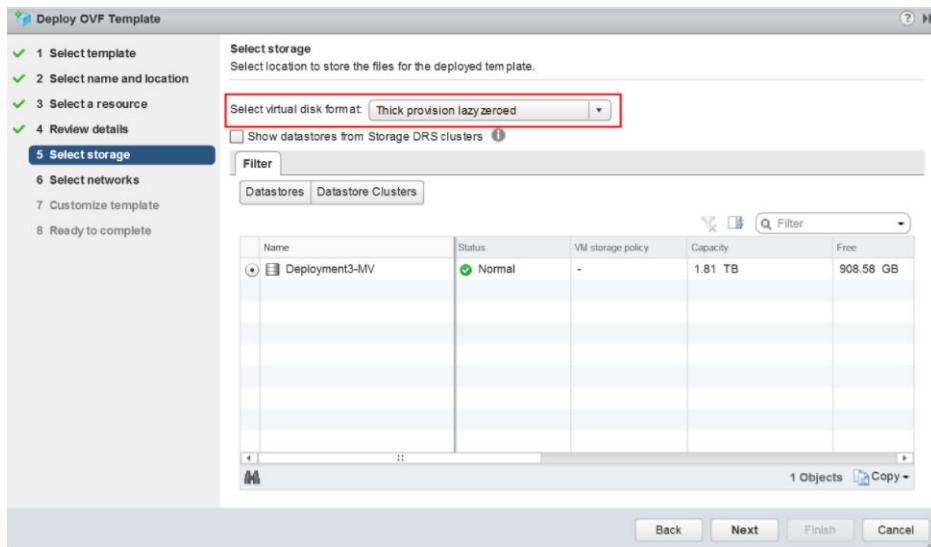
- 2 Select an OVF template from an URL or Local file.



- 3 Select a name and location of the virtual machine.
- 4 Select a resource.
- 5 Verify the template details.

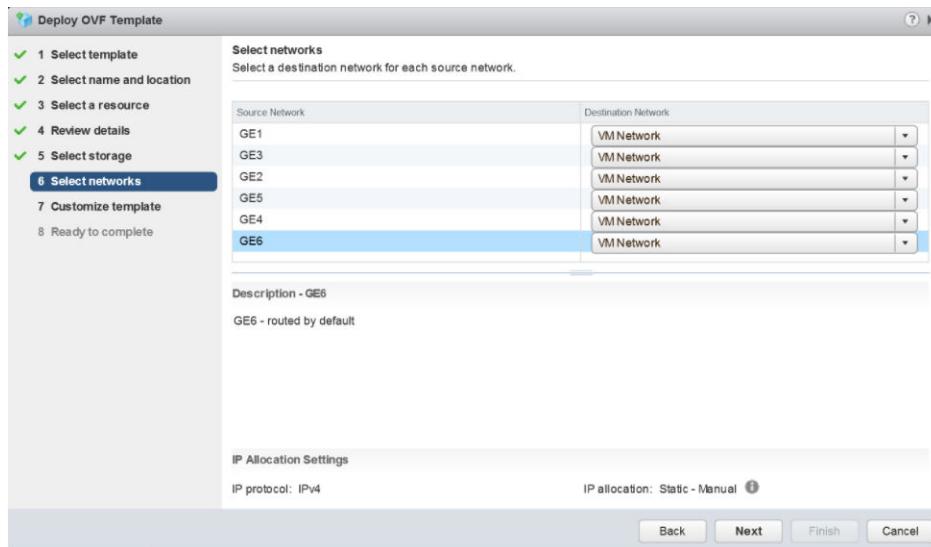


- 6 Select the storage location to store the files for the deployment template.



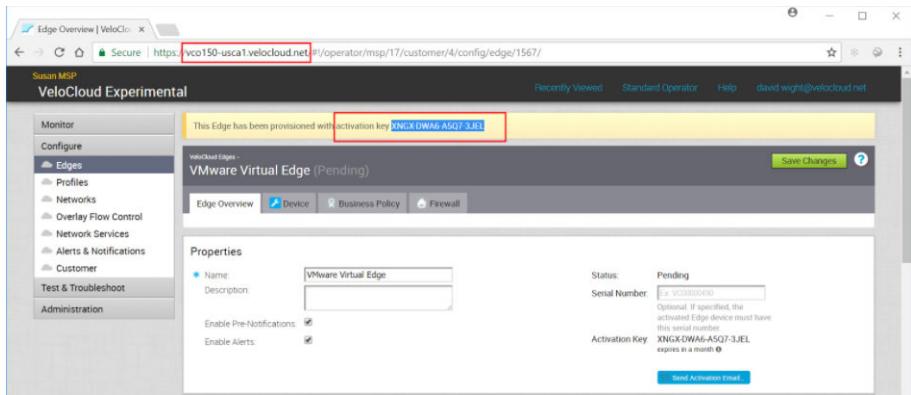
7 Configure the networks for each of the interfaces.

**Note** Skip this step if you are using a cloud-init file to provision the Virtual Edge on ESXi.

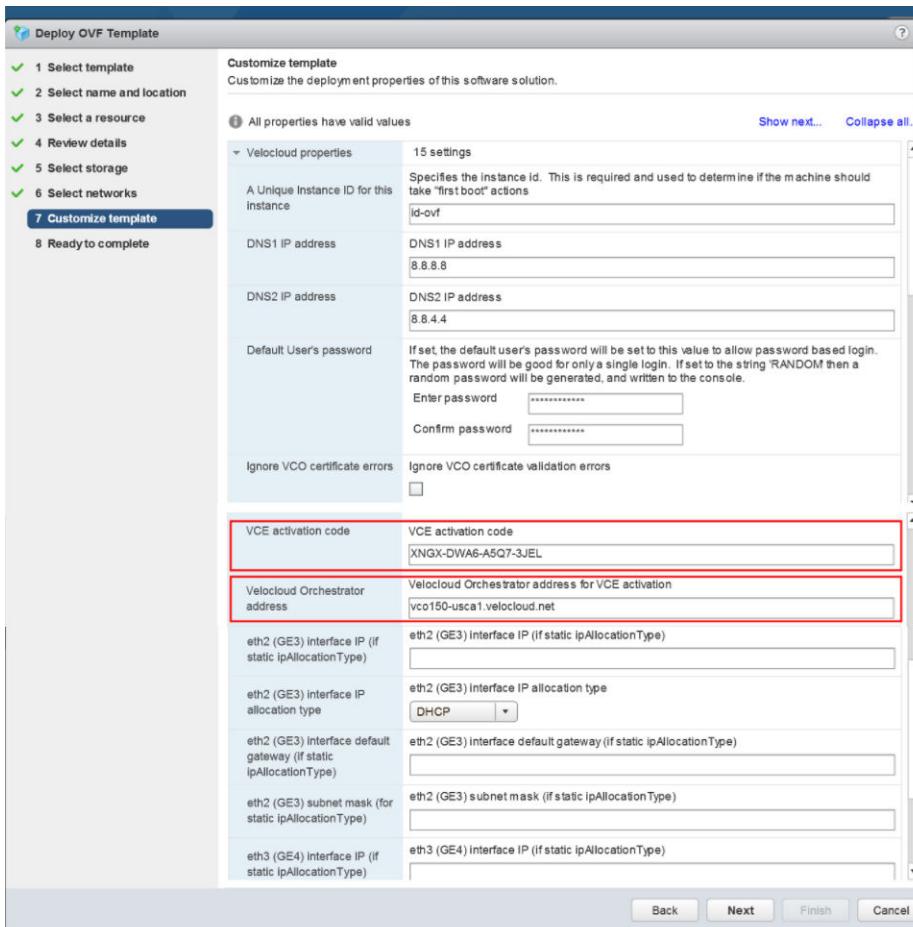


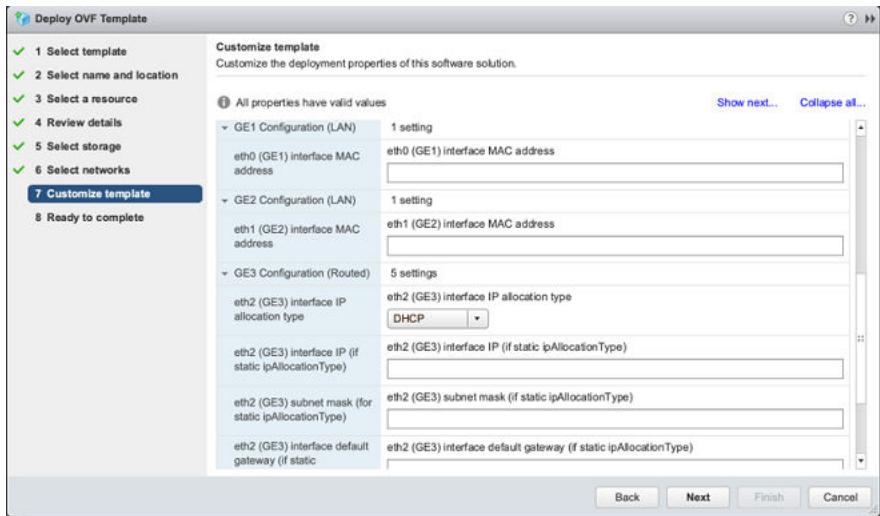
8 Customize the template by specifying the deployment properties. The following image highlights:

- From the SASE Orchestrator UI, retrieve the URL/IP Address. You will need this address for Step c below.
- Create a new Virtual Edge for the Enterprise. Once the Edge is created, copy the Activation Key. You will need the Activation Key for Step c" below.

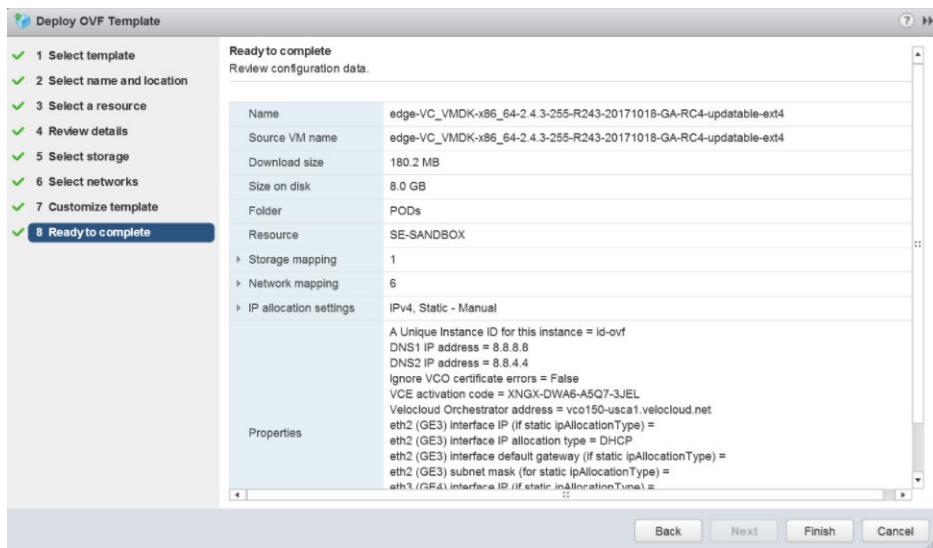


- c On the customize template page shown in the image below, type in the Activation Code that you retrieved in Step b above, and the SASE Orchestrator URL/IP Address retrieved in Step a above, into the corresponding fields.

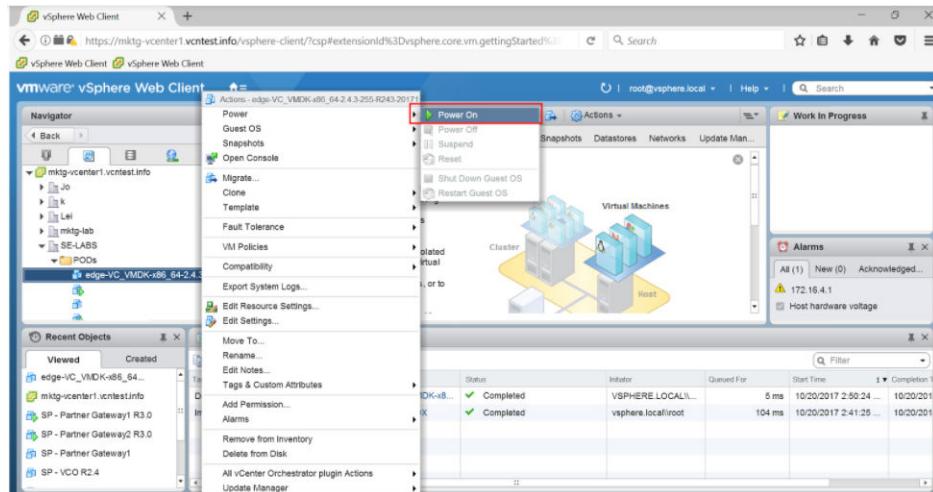




## 9 Review the configuration data.



## 10 Power on the Virtual Edge.



Once the Edge powers up, it will establish connectivity to the SASE Orchestrator.

# Appendix

43

Read the following topics next:

- [Enterprise-Level Orchestrator Alerts and Events](#)
- [Supported VMware SD-WAN Edge Events for Syslogs](#)

## Enterprise-Level Orchestrator Alerts and Events

Describes a summary of alerts and events generated within the VMware SASE Orchestrator at the Enterprise level.

The document provides details about all Enterprise-level Orchestrator events. Although these events are stored within the SASE Orchestrator and displayed on the Orchestrator UI, most of them are generated by either an SD-WAN Edge or an SD-WAN Gateway and/or one of its running components (MGD, EDGED, PROCMON, and so on) with the exception of a few which are generated by the Orchestrator itself. You can configure notifications/alerts for events in Orchestrator only.

The following table provides an explanation for each of the columns in the "Enterprise-level Orchestrator Events" table:

Column name	Details
EVENT	Unique name of the event
DISPLAYED ON ORCHESTRATOR UI AS	Specifies how the event is displayed on the Orchestrator.
SEVERITY	The severity with which this event is usually generated.
GENERATED BY	The VMware SD-WAN component generating the notification can be one of the following: <ul style="list-style-type: none"><li>■ SASE Orchestrator</li><li>■ SD-WAN Edge (MGD)</li><li>■ SD-WAN Edge (EDGED)</li><li>■ SD-WAN Edge (PROCMON)</li></ul>
GENERATED WHEN	Technical reason(s) and circumstances under which this event is generated.

Column name	Details
RELEASE ADDED IN	The release this event was first added. If not specified, this event existed prior to release 2.5.
DEPRECATED	Specifies if the event is deprecated from a specific release.

## Enterprise-level Orchestrator Events

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	ADDED IN	DEPRECATED
EDGE_UP	Edge Up	ALERT	SASE Orchestrator	Edge comes back after losing connectivity with the SASE Orchestrator through heartbeats. 2 consecutive heartbeats by an Edge causes the SASE Orchestrator to change its status to EDGE_UP. The SASE Orchestrator runs a monitor every 15 seconds that will update the status of all Edges.			
EDGE_DOWN	Edge Down	ALERT	SASE Orchestrator	Edge loses connectivity with the SASE Orchestrator and fails performing 2 or more consecutive heartbeats. The SASE Orchestrator runs a monitor every 15 seconds that will update the status of all Edges.			
LINK_UP	Link Up	ALERT	SASE Orchestrator	A WAN Link returns to a normal functioning state.			

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
LINK_DOWN	Link Down	ALERT	SASE Orchestrator	A WAN Link is disconnected from the Edge or when the Link cannot communicate with the Edge service.		
VPN_TUNNEL_DOWN	VPN Tunnel Down	ALERT	SASE Orchestrator	The IPSec tunnel configured from the Edge service to your VPN Gateway cannot be established or if the tunnel is dropped and cannot be re-established.		
EDGE_HA_FAILOVER	Edge HA Failover	ALERT	SASE Orchestrator	An HA Edge fails-over to its standby.		
EDGE_SERVICE_DOWN	Edge Service Down	ALERT	SASE Orchestrator	The Edge service running on the SD-WAN Edge may be down. This may indicate Edge device failure or failure of network connectivity.		
EDGE_CSS_TUNNEL_UP	Edge CSS Tunnel Up	ALERT	SASE Orchestrator	A Cloud Security Service tunnel from Edge is UP.		
EDGE_CSS_TUNNEL_DOWN	Edge CSS Tunnel Down	ALERT	SASE Orchestrator	A Cloud Security Service tunnel from Edge is DOWN.		
NVS_FROM_EDGE_TUNNEL_DOWN	NVS From Edge Tunnel Down	ALERT	SASE Orchestrator	A NSD via Edge tunnel is DOWN.		

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATE
NVS_FROM_EDGE_TUNNEL_UP	NVS From Edge Tunnel Up	ALERT	SASE Orchestrator	A NSD via Edge tunnel is UP.		
VNF_VM_DEPLOYED	VNF VM Deployed	ALERT	SASE Orchestrator	An Edge VNF virtual machine gets deployed on to the Edge.		
VNF_VM_POWERED_ON	VNF VM Powered ON	ALERT	SASE Orchestrator	An Edge VNF virtual machine gets deployed on to the Edge and is powered on.		
VNF_VM_POWERED_OFF	VNF VM Powered OFF	ALERT	SASE Orchestrator	An Edge VNF virtual machine is powered off.		
VNF_VM_DEPLOYED_AND_POWERED_OFF	VNF VM Deployed and Powered OFF	ALERT	SASE Orchestrator	An Edge VNF virtual machine gets deployed on to the Edge and is immediately powered on.		
VNF_VM_DELETED	VNF VM Deleted	ALERT	SASE Orchestrator	An Edge VNF virtual machine is removed from the Edge.		
VNF_VM_ERROR	VNF VM error	ALERT	SASE Orchestrator	An error occurs during deployment of an Edge VNF virtual machine.		
VNF_INSERTION_ENABLED	VNF insertion enabled	ALERT	SASE Orchestrator	Insertion of an Edge VNF virtual machine is enabled on the Edge.		
VNF_INSERTION_DISABLED	VNF insertion disabled	ALERT	SASE Orchestrator	Insertion of an Edge VNF virtual machine is deactivated on the Edge.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
VNF_IMAGE_DOWNLOAD_IN_PROGRESS	VNF Image Download In Progress	ALERT	SASE Orchestrator	An Edge VNF virtual machine image download is in progress.		
VNF_IMAGE_DOWNLOAD_COMPLETED	VNF Image Download Completed	ALERT	SASE Orchestrator	An Edge VNF virtual machine image download is completed.		
VNF_IMAGE_DOWNLOAD_FAILED	VNF Image Download Failed	ALERT	SASE Orchestrator	An Edge VNF virtual machine image failed to be downloaded on the Edge.		
EDGE_BFD_NEIGHBOR_UP	BFD session established to Edge neighbor	INFO	SASE Orchestrator	A BFD session has been established to Edge neighbor.		
EDGE_BFD_NEIGHBOR_DOWN	Edge BFD neighbor unavailable	INFO	SASE Orchestrator	A BFD session to Edge neighbor is not established.		
EDGE_BFD_V6_NEIGHBOR_UP	BFDv6 session established to Edge neighbor	INFO	SASE Orchestrator	A BFDv6 session has been established to Edge neighbor.	4.5	
EDGE_BFD_V6_NEIGHBOR_DOWN	Edge BFDv6 neighbor unavailable	INFO	SASE Orchestrator	A BFDv6 session to Edge neighbor is not established.	4.5	
EDGE_BGP_NEIGHBOR_UP	BGP session established to Edge neighbor	INFO	SD-WAN Edge	A BGP peer establishes tunnel with an SD-WAN Edge.		
EDGE_BGP_NEIGHBOR_DOWN	Edge BGP neighbor unavailable	INFO	SD-WAN Edge	The Edge's BGP peer loses tunnel with the Edge.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_BGP_V6_NEIGHBOR_UP	BGPv6 session established to Edge neighbor	INFO	SASE Orchestrator	A BGPv6 session has been established to Edge neighbor.	4.5	
EDGE_BGP_V6_NEIGHBOR_DOWN	BGPv6 session established to Edge neighbor	INFO	SASE Orchestrator	A BGPv6 session to Edge neighbor is not established.	4.5	
GATEWAY_MIGRATION_CREATE	Gateway Migration Created	INFO	SASE Orchestrator	The self-service migration is activated.	4.5.0	
GATEWAY_MIGRATION_REMOVE	Gateway Migration Removed	INFO	SASE Orchestrator	The self-service migration is deactivated.	4.5.0	
GATEWAY_MIGRATION_STATE_CHANGE	Gateway Migration State Changed	INFO	SASE Orchestrator	The Gateway migration state is changed from one state to another.	4.5.0	
PKI_PROMOTION	Endpoint PKI mode promoted	INFO	SASE Orchestrator	An Edge's PKI mode has been changed from optional to required.		
CERTIFICATE_REVOCATION	Certificate revoked	INFO	SASE Orchestrator	Edge certificate revocation occurs intentionally or due to an expired certificate (The latter should rarely happen, given Edge certificates automatically renews after 30 days into the 90 day period).		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
CERTIFICATE_RENEWAL	Certificate renewal request	INFO	SASE Orchestrator	Edge certificate automatically renews after 30 days into the 90 day period.		
UPDATE_EDGE_IMAGE_MANAGEMENT	Update Edge image management	INFO	SASE Orchestrator	Activates/deactivates management of Edge software images for a customer.		
SET_EDGE_SOFTWARE	Updated Edge software image	INFO	SASE Orchestrator	New software image is assigned to the Edge due to an Operator Profile reassignment or change in the software image within the operator profile.		
UNSET_EDGE_SOFTWARE	Unset overridden Edge software image	INFO	SASE Orchestrator	Unsetting software image overridden for the Edge and instead assign in the default software image associated with the Operator Profile.		
ADD_OPERATOR_PROFILE	Added operator profile	INFO	SASE Orchestrator	A new operator profile has been associated with this enterprise.		

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATED
REMOVE_OPERATOR_PROFILE	Removed operator profile	INFO	SASE Orchestrator	An existing operator profile has been removed from this enterprise.		
ADD_SOFTWARE_IMAGE	Added software image	INFO	SASE Orchestrator	When a new software image is associated to the operator profile for this enterprise.		
MODIFY_AS_SIGNED_OPERATOR_PROFILE_LIST	Modified the assigned operator profile list	INFO	SASE Orchestrator	List of operator profiles associated with the Enterprise has been modified.		
MODIFY_AS_SIGNED_SOFTWARE_IMAGE_LIST	Modified the assigned software image list	INFO	SASE Orchestrator	List of software images associated with the Enterprise has been modified.		
CLOUD_SECURITY_ENABLE	Cloud Security enabled	INFO	SASE Orchestrator	Cloud Security is activated in enterprise's profile or Edge-specific profile		
CLOUD_SECURITY_DISABLE	Cloud Security disabled	INFO	SASE Orchestrator	Cloud Security is deactivated in enterprise's profile		
CLOUD_SECURITY_PROVIDER_DELETED	Cloud security provider deleted	INFO	SASE Orchestrator	Cloud Security provider associated with an enterprise's profile has been deleted.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
CLOUD_SECURITY_TUNNELING_PROTOCOL_CHANGE	Cloud Security Tunneling Protocol Change	INFO	SASE Orchestrator	Cloud Security tunneling protocol changes (from IPSEC to GRE or vice versa) in an enterprise's profile		
CLOUD_SECURITY_PROVIDER_ADDED	CLOUD_SECURITY_PROVIDER_ADDED	INFO	SASE Orchestrator	Cloud Security provider associated with an Edge-specific profile has been added.		
CLOUD_SECURITY_PROVIDER_REMOVED	CLOUD_SECURITY_PROVIDER_REMOVED	INFO	SASE Orchestrator	Cloud Security provider associated with an Edge-specific profile has been removed.		
CLOUD_SECURITY_OVERRIDE_ENABLED	CLOUD_SECURITY_OVERRIDE_ENABLED	INFO	SASE Orchestrator	Cloud Security override has been activated in an Edge-specific profile.		
CLOUD_SECURITY_OVERRIDE_DISABLED	CLOUD_SECURITY_OVERRIDE_DISABLED	INFO	SASE Orchestrator	Cloud Security override has been deactivated in an Edge-specific profile.		
CREATE_CLOUD_SERVICE_SITE	Cloud Security Service site creation enqueued	INFO	SASE Orchestrator	An API automation job to create a Cloud Security Service tunnel from Edge has been enqueued.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
UPDATE_CLOUD_SERVICE_SITE	Cloud Security Service site update enqueued	INFO	SASE Orchestrator	An API automation job to update a Cloud Security Service tunnel from Edge has been enqueued.		
DELETE_CLOUD_SERVICE_SITE	Cloud Security Service site deletion enqueued	INFO	SASE Orchestrator	An API automation job to delete a Cloud Security Service tunnel from Edge has been enqueued.		
ZSCALER_SUBLOCATION_ACTION_ENQUEUED	Zscaler Sub Location Edge action enqueued	INFO	SASE Orchestrator	An API automation job for Cloud Security Service Zscaler Sub Location has been enqueued.		
EDGE_NVS_TUNNEL_UP	Edge Direct IPsec tunnel up	INFO	SASE Orchestrator	A Cloud Security Service tunnel or NSD via Edge tunnel is up.		
EDGE_NVS_TUNNEL_DOWN	Edge Direct IPsec tunnel down	INFO	SASE Orchestrator	A Cloud Security Service tunnel or NSD via Edge tunnel is down.		
DIAGNOSTIC_REQUEST	New diagnostic bundle request	INFO	SASE Orchestrator	A new Edge diagnostic bundle is requested by an enterprise or an operator user.		
EDGE_DIRECT_SITE_DELETED	Edge direct site deleted	INFO	SASE Orchestrator	A NSD via Edge tunnel has been deleted.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_DIRECT_TUNNEL_DISABLED	Edge direct tunnels disabled	INFO	SASE Orchestrator	NSD via Edge deactivated in profile device settings.		
EDGE_DIRECT_TUNNEL_ENABLED	Edge direct tunnels enabled	INFO	SASE Orchestrator	NSD via Edge enabled in profile device settings.		
EDGE_DIRECT_TUNNEL_PROVIDER_DELETED	Edge direct tunnel provider deleted	INFO	SASE Orchestrator	NSD via Edge provider associated with an enterprise's profile has been deleted.		
CREATE_NS_FROM_EDGE_SITE	NSD via Edge site creation enqueued	INFO	SASE Orchestrator	An API automation job to create a NSD via Edge tunnel has been enqueued.		
UPDATE_NS_FROM_EDGE_SITE	NSD via Edge site update enqueued	INFO	SASE Orchestrator	An API automation job to update a NSD via Edge tunnel has been enqueued.		
DELETE_NS_FROM_EDGE_SITE	NSD via Edge site deletion enqueued	INFO	SASE Orchestrator	An API automation job to delete a NSD via Edge tunnel has been enqueued.		
ENTERPRISE_ENABLE_VIEW_SENSITIVE_DATA	View sensitive data privileges granted	INFO	SASE Orchestrator	An enterprise grants privileges to its MSP or the operator to view data (keys) information.		

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATE
ENTERPRISE_ENABLE_OPERATOR_USER_MGMT	User management delegated to operator	INFO	SASE Orchestrator	An enterprise has successfully delegated access to operator to manage its users.		
ENTERPRISE_DISABLE_OPERATOR_ACCESS	User management access revoked from operator	INFO	SASE Orchestrator	An enterprise revokes access that was previously delegated to operator to manage its entities.		
ENTERPRISE_ENABLE_OPERATOR_ACCESS	Access delegated to operator	INFO	SASE Orchestrator	An enterprise has successfully delegated access to operator to manage its entities.		
ENTERPRISE_ENABLE_ROXY_ACCESS	Access revoked from operator	INFO	SASE Orchestrator	An enterprise has successfully delegated access to partner to manage its entities.		
ENTERPRISE_DISABLE_ROXY_ACCESS	Access delegated to partner	INFO	SASE Orchestrator	An enterprise revokes access that was previously delegated to partner to manage its entities.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_TO_EDGE_VPN_DISABLE	Edge to Edge VPN Disabled	INFO	SASE Orchestrator	Edge to Edge VPN associated with an Edge device or its corresponding profile has been deactivated.		
EDGE_TO_EDGE_VPN_ENABLE	Edge to Edge VPN Enabled	INFO	SASE Orchestrator	Edge to Edge VPN associated with an Edge device or its corresponding profile has been enabled.		
VPN_DISABLE	Cloud VPN disabled	INFO	SASE Orchestrator	Cloud VPN settings associated with an Edge device or its corresponding profile has been deactivated.		
VPN_ENABLE	Cloud VPN enabled	INFO	SASE Orchestrator	When cloud VPN settings associated with an Edge device or its corresponding profile has been enabled.		
VPN_UPDATE	Cloud VPN updated	INFO	SASE Orchestrator	When cloud VPN settings associated with an Edge device or its corresponding profile has been updated with new modified.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
REMOTE_ACTION	Edge remote action	INFO	SASE Orchestrator	A remote action is performed on an online Edge.		
RECURRING_REPORT_ERROR	Recurring report error	ERROR	SASE Orchestrator	When recurring report fails.		
CREATE_COMPOSITE_ROLE	Composite Role Created	INFO	SASE Orchestrator	When a composite role is created by an Enterprise, Partner, or Operator.	4.5	
UPDATE_COMPOSITE_ROLE	Composite Role Updated	INFO	SASE Orchestrator	When a composite role is updated by an Enterprise, Partner, or Operator.	4.5	
DELETE_COMPOSITE_ROLE	Composite Role Deleted	INFO	SASE Orchestrator	When a composite role is deleted by an Enterprise, Partner, or Operator.	4.5	
ENQUEUE_CREATE_ZSCALER_SUBLOCATION	Zscaler Sub Location creation enqueued	INFO	SASE Orchestrator	When sublocation configuration of Edge device settings are modified.	4.5	
ENQUEUE_UPDATE_ZSCALER_SUBLOCATION	Zscaler Sub Location update enqueued	INFO	SASE Orchestrator	When sublocation configuration of Edge device settings are modified.	4.5	
ENQUEUE_DELETE_ZSCALER_SUBLOCATION	Zscaler Sub Location deletion enqueued	INFO	SASE Orchestrator	When sublocation configuration of Edge device settings are modified.	4.5	

Event	Displayed On Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
CREATE_ZSCALER_SUBLOCATION	Zscaler Sub Location object created	INFO	SASE Orchestrator	When sublocation configuration of Edge device settings are modified.	4.5	
UPDATE_ZSCALER_SUBLOCATION	Zscaler Sub Location object updated	INFO	SASE Orchestrator	When sublocation configuration of Edge device settings are modified.	4.5	
DELETE_ZSCALER_SUBLOCATION	Zscaler Sub Location object deleted	INFO	SASE Orchestrator	When sublocation configuration of Edge device settings are modified.	4.5	
ENQUEUE_UPDATE_ZSCALER_LOCATION	Zscaler Location update enqueued	INFO	SASE Orchestrator	When location configuration of Edge device settings are modified.	4.5	
CREATE_ZSCALER_LOCATION	Zscaler Location object created	INFO	SASE Orchestrator	When location configuration of Edge device settings are modified.	4.5	
UPDATE_ZSCALER_LOCATION	Zscaler Location object updated	INFO	SASE Orchestrator	When location configuration of Edge device settings are modified.	4.5	
DELETE_ZSCALER_LOCATION	Zscaler Location Object deleted	INFO	SASE Orchestrator	When location configuration of Edge device settings are modified.	4.5	
GATEWAY_BGP_NEIGHBOR_UP	BGP session established to Gateway neighbor	INFO	SD-WAN Gateway	When a BGP peer establishes tunnel with a Gateway.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
GATEWAY_BGP_NEIGHBOR_DOWN	Gateway BGP neighbor unavailable	INFO	SD-WAN Gateway	When a Gateway's BGP peer loses tunnel with a Gateway.		
VRF_MAX_LIMIT_EXCEEDED	VMware SD-WAN Partner Gateway: Maximum rules in a route map limit hit for enterprise <enterprise-name>	WARNING	SD-WAN Gateway	Maximum inbound route map config limit reached.		
VRF_ROUTE_MAP_RULES_MAX_LIMIT_HIT	VMware SD-WAN Partner Gateway: Maximum rules in a route map limit hit for enterprise <enterprise-name>	WARNING	SD-WAN Gateway	Maximum outbound route map config limit reached.		
VRF_LIMIT_EXCEEDED	VMware SD-WAN gateway: Maximum VRF limit(1000) reached	ALERT	SD-WAN Gateway	Maximum VRF limit reached for Partner Gateway.		
GATEWAY_STARTUP	VMware SD-WAN gateway service started	INFO	SD-WAN Gateway	Gateway daemon has started.		
ZSCALER_MONITOR_DISABLED	Zscaler monitor disabled	CRITICAL	SD-WAN Edge/SD-WAN Gateway (PROCMON)	Unable to launch L7 health check daemon for CSS tunnels on Edge/Gateway. Or disabled due to too many failures.	4.4	
ZSCALER_MONITOR_FAILED	Zscaler monitor failed	ERROR	SD-WAN Edge/SD-WAN Gateway (PROCMON)	When L7 health check daemon fails with a return code.	4.4	
MGD_EMERG_REBOOT	Rebooting system to recover from stuck process(es): <process name>	CRITICAL	SD-WAN Edge/SD-WAN Gateway (PROCMON)	Edge/Gateway is rebooted to recover from stuck processes by vc_procmn.	4.4	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_SERVICES_STARTED/ GATEWAY_SERVICES_STARTED	Edge/Gateway Services Started	INFO	SD-WAN Edge/SD-WAN Gateway (PROCMON)	Generated when procmon starts the services.	4.5	
EDGE_SERVICES_STOPPED/ GATEWAY_SERVICES_STOPPED	Edge/Gateway Services Stopped	INFO	SD-WAN Edge/SD-WAN Gateway (PROCMON)	Generated when procmon stops all the services.	4.5	
EDGE_SERVICES_RESTARTED/ GATEWAY_SERVICES_RESTARTED	Edge/Gateway Services Restarted	INFO	SD-WAN Edge/SD-WAN Gateway (PROCMON)	Generated when procmon restarts all the services.	4.5	
EDGE_SERVICES_TERMINATED/ GATEWAY_SERVICES_TERMINATED	Edge/Gateway Services terminated	INFO	SD-WAN Edge/SD-WAN Gateway (PROCMON)	Generated when procmon terminates all the services.	4.5	
GATEWAY_SERVICE_DUMPED	Service gwd stopped for diagnostic memory dump	WARNING	SD-WAN Gateway (PROCMON)	Generated when gwd is stopped using SIGQUIT to generate core dump by user.	4.4	
GATEWAY_MGD_SERVICE_FAILED	service mgd failed with error ...., restarting	ERROR	SD-WAN Gateway (PROCMON)	Generated by vc_procm on Gateway when MGD gets stopped.	4.4	
GATEWAY_NAT_SERVICE_FAILED	Service natd failed with error ...., restarting	ERROR	SD-WAN Gateway (PROCMON)	Generated by vc_procm on Gateway when natd daemon gets stopped.	4.4	
EDGE_DNSMASQ_FAILED	dnsmasq FAILED to start up	ERROR	SD-WAN Edge (PROCMON)	Generated when dnsmasq daemon failed to start up.	4.4	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_SSH_LOGIN	sshd accepted connection	INFO	SD-WAN Edge (PROCMON)	Generated whenever ssh login is done for accessing the Edge.	4.4	
EDGE_SERVICEDUMPED	Service edged stopped for diagnostic memory dump	WARNING	SD-WAN Edge (PROCMON)	Generated when Edge is stopped using SIGQUIT to generate core dump by user.	4.4	
EDGE_LED_SERVICE_DISABLED	Edge front-panel LED service disabled	WARNING, CRITICAL	SD-WAN Edge (PROCMON)	LED service deactivated.		
EDGE_LED_SERVICE_FAILED	Edge front-panel LED service failed	ERROR	SD-WAN Edge (PROCMON)	LED service failed.		
EDGE_MGD_SERVICE_DISABLED	Management service disabled	CRITICAL	SD-WAN Edge (PROCMON)	Management service is unable to activate for too many failures.		
EDGE_MGD_SERVICE_FAILED	Management service failed	ERROR	SD-WAN Edge (PROCMON)	Management service failed.		
EDGE_SERVICEDISABLED	Edge data plane service disabled	WARNING/CRITICAL	SD-WAN Edge (PROCMON)	Edge Data plane service is deactivated.		
EDGE_SERVIEENABLED	Edge data plane service enabled	WARNING	SD-WAN Edge (PROCMON)	Edge Data plane service is activated by user from local UI.		
EDGE_SERVICEDIFAILED	Edge data plane service failed	ERROR	SD-WAN Edge (PROCMON)	Edge Data plane service failed.		
EDGE_VNF_D_SERVICE_DISABLED		WARNING	SD-WAN Edge (PROCMON)	Edge VNFD service deactivated.		
EDGE_VNF_D_SERVICE_FAILED		ERROR	SD-WAN Edge (PROCMON)	Edge VNFD service failed.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_DOT1_X_SERVICE_DISABLED	Edge 802.1x service disabled	WARNING, CRITICAL	SD-WAN Edge (PROCMON)	SD-WAN Edge 802.1x service is deactivated.		
EDGE_DOT1_X_SERVICE_FAILED	Edge 802.1x service failed	ERROR	SD-WAN Edge (PROCMON)	SD-WAN Edge 802.1x service failed.		
EDGE_NYA_NSA_SYSLOG_SERVICE_FAILED		ERROR	SD-WAN Edge (PROCMON)	Nyansa Syslog service failed.		
EDGE_NYA_NSA_SYSLOG_SERVICE_DISABLED		WARNING	SD-WAN Edge (PROCMON)	Nyansa Syslog service deactivated.		
EDGE_NYA_NSA_AMOND_SERVICE_FAILED		ERROR	SD-WAN Edge (PROCMON)	Nyansa Amond service failed.		
EDGE_NYA_NSA_AMOND_SERVICE_DISABLED		WARNING	SD-WAN Edge (PROCMON)	Nyansa Amond service deactivated		
EDGE_NYA_NSA_SNMP_TRAPD_SERVICE_FAILED		ERROR	SD-WAN Edge (PROCMON)	Nyansa SNMP Trapd service failed.		
EDGE_NYA_NSA_SNMP_TRAPD_SERVICE_DISABLED		WARNING	SD-WAN Edge (PROCMON)	Nyansa SNMP Trapd service deactivated.		
EDGE_NYA_NSA_SNMP_READER_SERVICE_FAILED		ERROR	SD-WAN Edge (PROCMON)	Nyansa SNMP Reader service failed.		
EDGE_NYA_NSA_SNMP_READER_SERVICE_DISABLED		WARNING	SD-WAN Edge (PROCMON)	Nyansa SNMP Reader service deactivated.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_USB_PORTS_ENA_BLED/ GATEWAY_USB_PORTS_ENABLED	Edge/Gateway USB ports Enabled	INFO	SD-WAN Edge/SD-WAN Gateway (MGD)	Generated when USB ports is activated.	4.5	
EDGE_USB_PORTS_DISABLED/ GATEWAY_USB_PORTS_DISABLED	Edge/Gateway USB ports Disabled	INFO	SD-WAN Edge/SD-WAN Gateway (MGD)	Generated when USB ports is deactivated.	4.5	
EDGE_USB_PORTS_ENA_BLE_FAILURE/ GATEWAY_USB_PORTS_ENABLE_FAILURE	Edge/Gateway USB ports Enable Failure	CRITICAL	SD-WAN Edge/SD-WAN Gateway (MGD)	Generated when procmon activates USB ports failure.	4.5	
EDGE_USB_PORTS_DISABLE_FAILURE/ GATEWAY_USB_PORTS_DISABLE_FAILURE	Edge/Gateway USB ports Disable Failure	CRITICAL	SD-WAN Edge/SD-WAN Gateway (MGD)	Generated when procmon deactivates USB ports failure.	4.5	
VNF_VM_EVENT	VNF VM Event	INFO	SD-WAN Edge (MGD)	Generated when VNF is powered on, powered off, deleted or deployed. Event detail will help distinguish the type.		
VNF_INSERTION_EVENT	VNF insertion event	ALERT	SD-WAN Edge (MGD)	VNF insertion is activated or deactivated. Event detail will help distinguish the type.		

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATE
VNF_IMAGE_DOWNLOAD_EVENT	VNF image download event	INFO	SD-WAN Edge (MGD)	VNF download is in progress, completed, or failed. Event detail will help distinguish the type.		
MGD_START	Online	INFO	SD-WAN Edge (MGD)	Management daemon on Edge has started.		
MGD_EXITING	Shutting Down	INFO	SD-WAN Edge (MGD)	Management service on a SD-WAN Edge is shutting down for a restart.		
MGD_SET_CERT_SUCCESS	Set Certificate Successful	INFO	SD-WAN Edge (MGD)	New PKI certificate for Orchestrator communication is installed successfully on a SD-WAN Edge.		
MGD_SET_CERT_FAIL	Set Certificate Failed	ERROR	SD-WAN Edge (MGD)	Installation of a new PKI certificate for Orchestrator communication on a SD-WAN Edge has failed.		
MGD_CONF_APPLIED	Configuration Applied	INFO	SD-WAN Edge (MGD)	Configuration change made on the Orchestrator has been pushed to SD-WAN Edge and is successfully applied.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_CONF_PENDING	New configuration pending	INFO	SD-WAN Edge (MGD)	New configuration is pending application (This event is currently NOT generated anywhere)		
MGD_CONF_ROLLBACK	Bad configuration rolled back	CRITICAL	SD-WAN Edge (MGD)	Configuration policy sent from the Orchestrator had to be rolled back because it destabilized the SD-WAN Edge.		
MGD_CONF_FAILED	Failed to apply configuration	ERROR	SD-WAN Edge (MGD)	Edge failed to apply a configuration change made on the Orchestrator.		
MGD_CONF_UPDATE_INVALID	Invalid software update configuration	WARNING	SD-WAN Edge (MGD)	Edge has been assigned an Operator Profile with an invalid software image that the Edge cannot use.		
MGD_DEVICE_CONFIG_WARNING		WARNING	SD-WAN Edge (MGD)	Inconsistent device settings are detected. MGD continues with warnings.		
MGD_DEVICE_CONFIG_ERROR		ERROR	SD-WAN Edge (MGD)	Invalid device settings are detected by MGD.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_SWUP_IGNORED_UPDATE	Software update ignored	INFO	SD-WAN Edge (MDG)	Software update is ignored at the activation time, because SD-WAN Edge is already running that version.		
MGD_SWUP_INVALID_SWUPDATE	Invalid software update	WARNING	SD-WAN Edge (MDG)	Software update package received from the Orchestrator is invalid.		
MGD_SWUP_DOWNLOAD_FAILED	Software download failed	ERROR	SD-WAN Edge (MDG)	Download of an Edge software update image has failed.		
MGD_SWUP_UNPACK FAILED	Software update unpack failed	ERROR	SD-WAN Edge (MDG)	Edge has failed to unpack the downloaded software update package.		
MGD_SWUP_INSTALL FAILED	Software update install failed	ERROR	SD-WAN Edge (MDG)	Edge software update installation failed.		
MGD_SWUP_INSTALLED	Software update	INFO	SD-WAN Edge (MDG)	Software update was successfully downloaded and installed.		
MGD_SWUP_REBOOT	Restart after software update	INFO	SD-WAN Edge (MDG)	Edge is being rebooted after a software update.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_SWUP_STANDBY_UPDATE_START	Standby device software update started	INFO	SD-WAN Edge (MGD)	Edge send upgrade message to standby when it detect peer software version is not same with Active Edge or Active Edge received upgrade command from SASE Orchestrator.		
MGD_SWUP_STANDBY_UPDATE_FAILED	Standby device software update failed	ERROR	SD-WAN Edge (MGD)	Active Edge report standby upgrade failed if it fail to send upgrade command to peer or standby fail to upgrade for more than 5 minutes		
MGD_SWUP_STANDBY_UPDATED	Standby device software update completed	INFO	SD-WAN Edge (MGD)	When Active Edge detects standby comes up with expected image version		
MGD_VCO_ADDR_RESOLVE FAILED	Cannot resolve Orchestrator address	WARNING	SD-WAN Edge (MGD)	DNS resolution of the Orchestrator address failed.		
MGD_DIAG_REBOOT	User-initiated restart	INFO	SD-WAN Edge (MGD)	Edge is rebooted by a Remote Action from the Orchestrator.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_DIAG_RESTART	Services restarted	INFO	SD-WAN Edge (MGD)	Data plane service on the SSD-WAN Edge is restarted by a Remote Action from the Orchestrator.		
MGD_SHUTDOWN	Powered off	INFO	SD-WAN Edge (MGD)	Edge diagnostic shutdown based on user request.		
MGD_HARD_RESET	Reset to factory defaults	INFO	SD-WAN Edge (MGD)	Edge is restored to its factory-default software and configuration.		
MGD_DEACTIVATED	Deactivated	INFO	SD-WAN Edge (MGD)	Edge is deactivated based on user request by mgd.		
MGD_NETWORK_SETTINGS_UPDATED	Network settings updated	INFO	SD-WAN Edge (MGD)	Network settings are applied to a SD-WAN Edge.		
MGD_NETWORK_MGMT_IF_BROKEN	Management Network incorrectly set up	ALERT	SD-WAN Edge (MGD)	Management network is set up incorrectly.		
MGD_NETWORK_MGMT_IF_FIXED	Network was restarted twice to fix Management Network inconsistency	WARNING	SD-WAN Edge (MGD)	Network is restarted twice to fix the Management Network inconsistency.		
MGD_INVALID_VCO_ADDRESS	Unable to heartbeat to new VCO %newprimary)s, keep talking to old VCO %oldprimary)s	WARNING	SD-WAN Edge (MGD)	Invalid address for Orchestrator was sent in a management plane policy update and was ignored.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_ACTIVATION_PARTIAL	Activation incomplete	INFO	SD-WAN Edge (MGD)	Edge is activated partially, but a software update failed.		
MGD_REBOOT_DIAG_BUNDLE	Generating diagnostic bundle before reboot	INFO	SD-WAN Edge (MGD)	When the diagnostic bundle is generated before reboot.	5.0	
MGD_ACTIVATION_SUCCESS	Activated	INFO	SD-WAN Edge (MGD)	Edge has been activated successfully.		
MGD_ACTIVATION_ERROR	Activation failed	ERROR	SD-WAN Edge (MGD)	Edge activation failed. Either the activation link was not correct, or the configuration was not successfully downloaded to the Edge.		
MGD_HA_TERMINATED	HA disabled on Edge	INFO	SD-WAN Edge (MGD)	Standby Edge send this event when HA is deactivated.		
EDGE_INTERFACE_DOWN	Edge Interface Down	INFO	SD-WAN Edge (MGD)	Generated by hotplug scripts when the interface is down.		
EDGE_INTERFACE_UP	Edge Interface Up	INFO	SD-WAN Edge (MGD)	Generated by hotplug scripts when the interface is up.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_KERN EL_PANIC		ALERT	SD-WAN Edge (MGD)	Edge operating system has encountered a critical exception and must reboot the Edge to recover. An Edge reboot is disruptive to customer traffic for 2-3 minutes while the Edge completes the reboot.		
MGD_MFRM UP_IGNORE D_UPDATE	Modem Firmware update ignored: <error message>	ALERT	SD-WAN Edge (MGD)	Generated when modem firmware update is ignored.	5.0	
MGD_MFRM UP_INVALID _MFRMUPD ATE	Invalid Modem Firmware update applied: <error message>	INFO	SD-WAN Edge (MGD)	Generated when invalid modem firmware update is applied.	5.0	
MGD_MFRM UP_INCOMP ATIBLE_UP DATE	In compatible Device or Factory Image: <error message>	WARNING	SD-WAN Edge (MGD)	Generated when the device is incompatible for modem firmware update.	5.0	
MGD_MFRM UP_DOWNL OAD_FAILE D	Error downloading MFW ver <version> <build>	WARNING	SD-WAN Edge (MGD)	Generated when error occurs downloading the modem firmware update version.	5.0	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_MFRM_UP_UNPAC_K_FAILED	Error unpacking MFW ver <version> bu <build>	ERROR	SD-WAN Edge (MDG)	Generated when the modem firmware update unpacking failed.	5.0	
MGD_MFRM_UP_INSTALL_FAILED	Error installing MFW ver <version> bu <build>	ERROR	SD-WAN Edge (MDG)	Generated when the modem firmware update installation failed.	5.0	
MGD_MFRM_UP_INSTALL_ED	Installed downloaded MFW ver <version> bu <build>	ERROR	SD-WAN Edge (MDG)	Generated when the modem firmware update version is installed.	5.0	
MGD_MFRM_UP_UPGRADE_PROGRESS	MFW update in progress ver <version> bu <build>	INFO	SD-WAN Edge (MDG)	Generated when the modem firmware upgrade is in progress.	5.0	
MGD_MFRM_UP_REBOOT	Edge is restarting into new MFW version <version> build <build>	INFO	SD-WAN Edge (MDG)	Generated when the Edge restarts with new modem firmware update version.	5.0	
MGD_MFRM_UP_STANDBY_UPDATE_START	Begin HA Standby update with new MFW	INFO	SD-WAN Edge (MDG)	Generated when the HA Standby update with new modem firmware version started.	5.0	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_MFRM_UP_STAND_BY_UPDATE_FAILED	Failed HA Standby update with new MFW	ERROR	SD-WAN Edge (MGD)	Generated when the HA Standby update with new modem firmware version failed.	5.0	
MGD_MFRM_UP_STAND_BY_UPDATE_D	Succeeded HA Standby update with new MFW	INFO	SD-WAN Edge (MGD)	Generated when the HA Standby update with new modem firmware version succeeded.	5.0	
EDGE OSPF_NSM	Edge OSPF NSM Event	INFO	SD-WAN Edge (EDGED)	Edge send this event when OSPF neighbor state changes.		
IP_SLA_PROBE	IP SLA Probe	INFO	SD-WAN Edge (EDGED)	Edge generates when IP SLA state changes.		
IP_SLA_RESPONDER	IP SLA Responder	ALERT, INFO	SD-WAN Edge (EDGED)	When IP SLA responder state changes from up to down and vice versa.		
ALL_CSS_DOWN	ALL_CSS_DOWN	ALERT	SD-WAN Edge (EDGED)	When all CSS paths go down.		
CSS_UP	CSS_UP	ALERT	SD-WAN Edge (EDGED)	When at least one CSS path is up.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
LINK_MTU	Link MTU detected	INFO	SD-WAN Edge (EDGED)	Link MTU detected. The Gateway has detected the MTU for this WAN link and all traffic sent on this link will account for that MTU reading. For Release 3.2.x and earlier, VeloCloud software uses RFC 1191 Path MTU Discovery, which relies on receiving an ICMP error (fragmentation needed) from an upstream device in order to discover the MTU. On Release 3.3.x and later, the Path MTU Discovery has been enhanced to use packet layer Path MTU Discovery (RFC 4821).		
PORT_SCAN_DETECTED	Port scan detected	INFO	SD-WAN Edge (EDGED)	If Stateful firewall detects host scanning then this event would be logged along with the IP address and port number.		
PEER_UNUSABLE	Peer unusable	ALERT	SD-WAN Edge (EDGED)	Peer is unusable.		Deprecated

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
PEER_USABLE	Peer usable	INFO	SD-WAN Edge (EDGED)	Peer is usable.		Deprecated
BW_UNMEASURABLE	Error measuring bandwidth	ALERT	SD-WAN Edge (EDGED)	Bandwidth measurement failed to the Primary Gateway. Reattempt at measurement in 30minutes. Reasons include a link suffering some quality issue like excessive loss or latency. This message should only be seen on Edge's using Release 3.1.x or lower as this was removed beginning with Edge Release 3.2.0.		
SLOW_START_CAP_MET	Bandwidth measured exceeds the slow start cap. Moving to burst mode.	NOTICE	SD-WAN Edge (EDGED)	Bandwidth measurement Slow-start limit of 175 Mbps exceeded. Link will be remeasured in Burst mode to ensure the correct measurement of a 175+ Mbps WAN link.		
EDGE_BFD_CONFIG		INFO	SD-WAN Edge (EDGED)	BFD configured with incorrect local address.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
FLOOD_ATT ACK_DETECTED		INFO	SD-WAN Edge (EDGED)	Generated when a malicious host floods the SD-WAN Edge with new connections.		
LINK_ALIVE	Link alive	INFO	SD-WAN Edge (EDGED)	When link state (link_fsm) becomes alive.		
LINK_DEAD	Link dead	ALERT	SD-WAN Edge (EDGED)	When link state (link_fsm) becomes dead.		
LINK_USABLE	Link usable	INFO	SD-WAN Edge (EDGED)	When link state (link_fsm) becomes usable.		
LINK_UNUSABLE	Link unusable	ALERT	SD-WAN Edge (EDGED)	When link state (link_fsm) becomes unusable.		
VPN_DATA_CENTER_STATUS	VPN Tunnel state change	INFO, ERROR	SD-WAN Edge (EDGED)	VPN Tunnel state change.		
INTERFACE_CONFIG_ERROR	Interface config error	ALERT	SD-WAN Edge (EDGED)			
HA_STANDBY_ACTIVATED	HA Standby Activated	INFO	SD-WAN Edge (EDGED)	When active Edge detects standby peer send this event to SASE Orchestrator to activate standby Edge.		
HA_INTF_STATE_CHANGED	HA Interface State Changed	ALERT	SD-WAN Edge (EDGED)	HA interface went down/up.		
HA_GOING_ACTIVE	High Availability Going Active	INFO	SD-WAN Edge (EDGED)	Standby Edge transition to Active Edge after detecting no heartbeat for more than 700ms.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
HA_FAILED	High Availability Peer State Unknown	INFO	SD-WAN Edge (EDGED)	Active Edge detects no heartbeat or activity from standby Edge for more than 700 milliseconds.		
HA_READY	High Availability Ready	INFO	SD-WAN Edge (EDGED)	Active Edge detects activated standby peer.		
VCO_IDENTIFIED_HA_FAILOVER	Edge HA Failover Identified	ALERT	SASE Orchestrator	Orchestrator has detected that a High Availability failover has occurred on the Edge.	5.2	
VCO_IDENTIFIED_HA_FAILURE	Edge HA Failure Identified	ALERT	SASE Orchestrator	Orchestrator has detected that the Standby Edge has gone down.	5.2	
HA_UPDATE_FAILOVER_TIME	Updating HA Failover time from #####ms to #####ms	INFO	SASE Orchestrator	User changed the failover time for when an HA Edge will failover due to a lack of heartbeat response. This time is measured in milliseconds (ms).	5.2	
HA_RESET_FAILOVER_TIME	Failover time reset from #####ms to #####ms.	INFO	SD-WAN Edge (EDGED)	When an HA Edge's system has been stable for 60 seconds, the process reduces the failover time by 50%.	5.2	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATED
HA_WAN_LINK_ACTIVE	<Edge-Name> <Active Serial Number> configured with <Standard, Enhanced, or Mixed-Mode> HA, with WAN <Link ID> is <Down or Up>	ALERT	SD-WAN Edge (EDGED)	For all HA topologies (Standard, Enhanced, and Mixed-Mode) when the WAN interface goes Up or Down on the Active Edge.	5.2	
HA_WAN_LINK_STANDBY	<Edge-Name> <Standby Serial Number> configured with <Standard, Enhanced, or Mixed-Mode> HA, with WAN <Link ID> is <Down or Up>	ALERT	SD-WAN Edge (EDGED)	For all HA topologies (Standard, Enhanced, and Mixed-Mode) when the WAN interface goes Up or Down on the Standby Edge.	5.2	
HA_LAN_LINK_ACTIVE	<Edge-Name> <Active Serial Number> configured with <Standard, Enhanced, or Mixed-Mode> HA, with LAN <Link ID> is <Down or Up>	ALERT	SD-WAN Edge (EDGED)	For all HA topologies (Standard, Enhanced, and Mixed) when the LAN interface goes Up or Down on the Active Edge.	5.2	
HA_LAN_LINK_STANDBY	<Edge-Name> <Standby Serial Number> configured with <Standard, Enhanced, or Mixed-Mode> HA, with LAN <Link ID> is <Down or Up>	ALERT	SD-WAN Edge (EDGED)	For all HA topologies (Standard, Enhanced, and Mixed) when the LAN interface goes Up or Down on the Standby Edge.	5.2	
FW_UPGRADE_PENDING_CPLD	CPLD Firmware being updated during software upgrade - edge may be offline for 3 - 5 minutes.	INFO	SASE Orchestrator	A firmware upgrade action has been initiated and sent by the Orchestrator to the Edge.	5.2	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATED
FW_UPGRADE_SUCCESSES	Note - that an edge physical reboot was required due to the edge not responding once the PENDING message was received.	INFO	SD-WAN Edge(EDGE D)	The Edge firmware upgrade was successful and required Edge reboots to complete.	5.2	
HA_SPLIT_BRAIN_DETECTED	HA split-brain detected, peer will restart	ALERT	SASE Orchestrator	The Orchestrator has detected that both HA Edges are in an Active state. This is known as an Active-Active or Split Brain state. <a href="#">Split-Brain Detection and Prevention</a> , the Orchestrator resolves this by triggering a restart of the Standby Edge (listed here as "peer") that is erroneously functioning as Active.	5.2	
HA_SPLITBRAIN_RESOLVED	HA split-brain resolved, peer will move to standby state	NOTICE	SASE Orchestrator	The Standby Edge (listed here as "peer") in an Active state has completed its restart and is demoted back to its correct Standby state. As a result, the Active-Active or Split Brain state is resolved.	5.2	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_UNREACHABLE	Management Proxy unreachable	EMERGENCY	SD-WAN Edge (EDGED)	Data plane process could not communicate to the management plane proxy.		
VRRP_INTO_MASTER_STATE	VRRP HA updated to Primary state	INFO	SD-WAN Edge (EDGED)	VRRP get into Primary state		
VRRP_OUT_OF_MASTER_STATE	VRRP HA updated out of Primary state	INFO	SD-WAN Edge (EDGED)	VRRP get out of Primary state.		
VRRP_FAIL_INFO	VRRP failed	INFO	SD-WAN Edge (EDGED)	VRRP failed.		
EDGE_HEALTH_ALERT	Edge Health Alert	EMERGENCY	SD-WAN Edge (EDGED)	Data plane is unable to allocate necessary resources for packet processing.		
EDGE_STARTUP	Edge service startup	INFO	SD-WAN Edge (EDGED)	Edge is running in mgmt-only mode.		
EDGE_DHCP_BAD_OPTION	Invalid DHCP Option	WARNING	SD-WAN Edge (EDGED)	SD-WAN Edge is configured with an invalid DHCP option.		
EDGE_NEW_USER	New client user seen	INFO	SD-WAN Edge (EDGED)	New or updated client user detected on a given MAC address.		
EDGE_NEW_DEVICE	New client device seen	INFO	SD-WAN Edge (EDGED)	A new device is detected during DHCP.		
INVALID_JSON		CRITICAL	SD-WAN Edge (EDGED)	The Edged received invalid json data from the mgd.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
QOS_OVERRIDE	QoS override	INFO	SD-WAN Edge (EDGED)	Remote diagnostics is performed to flip cloud traffic to be routed according to business policy OR sent to the Gateway OR or bypass the Gateway.		
EDGE_L2_L_OOP_DETECTED	Edge L2 loop detected	ERROR	SD-WAN Edge (EDGED)	Edge L2 loop is detected.		
EDGE_TUNNEL_CAP_WARNING	Edge Tunnel CAP warning	WARNING	SD-WAN Edge (EDGED)	Edge has reached its maximum tunnel capacity.		
Interface LoS	LoS no longer seen on interface <iface-name>/ LoS detected on interface <iface-name>	ALERT	SD-WAN Edge (EDGED)	Loss of Signal state changed on the interface in HA setup.	4.4	
EDGE_LOCAL_UI_LOGIN	Edge Local UI Login	INFO	SD-WAN Edge	LOCAL UI login is successful for a user.		

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATED
EDGE_MEMORY_USAGE_ERROR	Memory Usage Critical	ERROR	SD-WAN Edge	Resource Monitor process detects Edge memory utilization has exceeded defined thresholds and reaches 70% threshold. The Resource Monitor waits for 90 seconds to allow the Edged process to recover from a possible temporary spike in memory usage. If memory usage persists at a 70% or higher level for more than 90 seconds, the Edge will generate this error message and send this event to the Orchestrator.		

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATED
EDGE_MEMORY_USAGE_WARNING	Memory Usage Warning	WARNING	SD-WAN Edge	Resource Monitor process detects Edge memory utilization is 50% or more of the available memory. This event will be sent to the Orchestrator every 60 minutes until the memory usage drops under the 50% threshold.		
EDGE_RESTARTING	User-initiated Edge service restart	WARNING	SD-WAN Edge	User initiates an Edge service restart.		
EDGE_REBOOTING	User-initiated Edge reboot	WARNING	SD-WAN Edge	User initiates an Edge reboot.		
EDGE_HARD_RESET	User-initiated Edge hard reset	WARNING	SD-WAN Edge	Edge hard reset		
EDGE_DEACTIVATED	Edge deactivated	WARNING	SD-WAN Edge	SD-WAN Edge has all its configuration cleared and is not associated with a customer site. The software build remains unchanged.		
EDGE_CONSOLE_LOGIN	Edge console login	INFO	SD-WAN Edge	SD-WAN Edge login via console port.		

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_COMMAND	Edge Command	INFO	SD-WAN Edge	Generated by a SD-WAN Edge during remote diagnostics when executing Edge commands.		
EDGE_BIOS_UPDATED	Edge BIOS updated	INFO	SD-WAN Edge	Generated by 12-upgrade-bios.sh script when SD-WAN Edge BIOS is successfully updated.		
EDGE_BIOS_UPDATE_FAILED	Edge BIOS update failed	ERROR	SD-WAN Edge	Generated by 12-upgrade-bios.sh script when SD-WAN Edge BIOS update failed.		
IPV6_ADDR_DELETED	Deleted IPv6 address <v6addr> on interface/sub-interface <iface/subiface name>	INFO	SD-WAN Edge/SD-WAN Gateway	When IPv6 interface is deleted on interface or sub-interface.	4.4	
IPV6_NEW_ADDR_ADDED	Added new IPv6 address <v6-addr> on interface <ifacename>	INFO	SD-WAN Edge	When IPv6 address is added on interface.	4.4	
IPV6_ADDR_DEPRECATED	Deprecated IPv6 address <v6-addr> on interface <iface-name>	INFO	SD-WAN Edge	When IPv6 address gets deprecated on an interface.	4.4	
IPV6_ADDR_PREFERRED	Preferred IPv6 address <v6-addr> on interface <iface-name>	INFO	SD-WAN Edge	When IPv6 address moves from Deprecated state to Preferred state.	4.4	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
NDP_MAC_ADDR_CHANGE	Neighbor MAC address change detected in interface <iface-name>	INFO	SD-WAN Edge	When IPv6 neighbor MAC address change is detected.	4.4	
EDGE_INTC_CONFIG	DAD Failed for IPv6 Address <v6-addr> in interface <iface-name>	INFO	SD-WAN Edge	When IPv6 NDP DAD is failed.	4.4	
EDGE_SHUTTING_DOWN	Edge is shutting down - must be restarted by power-cycling	WARNING	SD-WAN Edge (LUA Backend)	When Edge is shutting down.	4.4	
BIOS_PHY_RESET_CMOS_SET	BIOS - Phy reset CMOS bit is set/ BIOS - Phy reset CMOS bit cannot be set	WARNING	SD-WAN Edge	When CMOS (BIOS) is reset to its factory default settings.	4.4	
FW_UPGRADE_PENDING	CPLD Firmware being updated during software upgrade - edge may go offline for 3-5 minutes	WARNING	SD-WAN Edge	When CPLD Firmware is being updated during software upgrade.	4.4	
EVDSL_IFACE_UP_EVENT	Contains json string with evdslModem name, status, serial number	INFO	SD-WAN Edge	Generated when EVDSL interface moves to Up state.	4.5	
EVDSL_IFACE_DOWN_EVENT	contains json string with evdslModem name, status, serial number	INFO	SD-WAN Edge	Generated when EVDSL interface moves to Down state.	4.5	
NAT_PORT_ASSIGN_FAIL	NAT Ports exhausted from <src_ip> to <dst_ip>:<dport>	WARNING	SD-WAN Edge/SD-WAN Gateway	Generated when NAT port allocation range is exhausted.	4.5	
IPV6_MAX_DAD_FAILED	IPv6 < link local / RA > stable secret address generation failed on interface <iface name> after multiple DAD failures	ALERT	SD-WAN Edge	Generated when we fail to generate stateless IPv6 address after multiple DAD failures.	4.5	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
IPV6_ADDR_GEN_FAILED	IPv6 <link local / RA> stable secret address generation failed on interface <iface name> after generating multiple invalid addresses	ALERT	SD-WAN Edge	Generated when IPv6 stable secret address generation failed on interface after generating multiple invalid addresses.	4.5	
INVALID_STATIC_ROUTE	Rejected invalid routes <route-prefix>/0 flag <route flags in hex>	ALERT	SD-WAN Edge	Generated for invalid static route.	4.5	
INVALID_OSPF_ROUTE	Rejected invalid routes <route-prefix>/0 flag <route flags in hex>	ALERT	SD-WAN Edge	Generated for invalid OSPF routes.	4.5	
INVALID_BGP_ROUTE	Rejected invalid routes <route-prefix>/0 flag <route flags in hex>	ALERT	SD-WAN Edge	Generated for invalid BGP routes.	4.5	
INVALID_REMOTE_OSPF_ROUTE	Rejected invalid routes <route-prefix>/0 flag <route flags in hex>	ALERT	SD-WAN Edge	Generated for invalid remote OSPF route.	4.5	
INVALID_REMOTE_BGP_ROUTE	Rejected invalid routes <route-prefix>/0 flag <route flags in hex>	ALERT	SD-WAN Edge	Generated for invalid remote BGP route.	4.5	
INVALID_OVERLAY_ROUTE	Rejected invalid routes <route-prefix>/0 flag <route flags in hex>	ALERT	SD-WAN Edge	Generated for invalid Overlay route.	4.5	
INVALID_ROUTE	Rejected invalid routes <route-prefix>/0 flag <route flags in hex>	ALERT	SD-WAN Edge	Generated for invalid routes.	4.5	
EDGE_BFDv6_CONFIG	Incorrect local address <IP address>. IP Address not present	INFO	SD-WAN Edge	Generated when invalid IPv6 BFD configuration is received.	4.5	
EDGE_USB_DEVICE_INSERTED	Edge USB device inserted	ALERT	SD-WAN Edge	Generated when USB device is inserted.	4.5	
EDGE_USB_DEVICE_REMOVED	Edge USB device removed	ALERT	SD-WAN Edge	Generated when USB device is removed.	4.5	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASED IN	DEPRECATE
WIFI_CARD_DEAD	Wifocard <device name> at <port> is no longer usable , reboot required to recover	EMERGENCY	SD-WAN Edge	Generated when WiFi card at a port is no longer usable.	4.5	
DNS_CACHE_LIMIT_REACHED	DNS Cache Max Limit (<cache limit of the edge>) Reached	ALERT	SD-WAN Edge	Generated when DNS cache limit is reached on the Edge.	4.5.1, 5.0	
PEER_MISMATCH	PEER_MISMATCH	ALERT	SD-WAN Edge (EDGED)	When there is a peer name mismatch between MP_INIT_REQ and MP_INIT_ACK during Edge and Gateway tunnel creation.	5.1	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_CONGESTED	Congestion alert due to either a high number of packet drops/scheduler drops	WARNING	SD-WAN Edge (EDGED)	<ul style="list-style-type: none"> <li>■ The number of packet drops (xxxx) is above the congestion threshold (1000)</li> <li>or</li> <li>■ "The number of scheduler drops (xxxx) is above the congestion threshold (1000)"</li> </ul> <p>Generated if there are either:</p> <ul style="list-style-type: none"> <li>■ Continuous packet drops above a threshold of 1000 for more than 30 seconds due to over capacity.</li> <li>■ Continuous packet drops above a threshold of 1000 for more than 30 seconds at the schedulers.</li> </ul>	5.1	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EDGE_STABLE	Congestion due to a high number of packet drops/ scheduler drops subsided	NOTICE	SD-WAN Edge (EDGED)	<ul style="list-style-type: none"> <li>■ "The number of packet drops (xxx) is within the acceptable threshold (1000)"</li> <li>or</li> <li>■ "The number of scheduler drops (xxx) is within the acceptable threshold (1000)"</li> </ul> <p>Follow up to the EDGE_CONGESTED event, indicating that the triggering criteria has subsided and the Edge is operating within acceptable parameters.</p>	5.1	
MGD_ATPUP_INVALID_IDPS_SIGNATURE	MGD_ATPUP_INVALID_IDPS_SI GNATURE	ERROR	SD-WAN Edge (MGD)	Generated when there is an invalid suricata package.	5.2	
MGD_ATPUP_DOWNLOAD_IDPS_SIGNATURE_FAILED	MGD_ATPUP_DOWNLOAD_IDPS_SIGNATURE_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when downloading of suricata package fails.	5.2	
MGD_ATPUP_DECRYPT_IDPS_SIGNATURE_FAILED	MGD_ATPUP_DECRYPT_IDPS_S IGNATURE_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when unpacking of suricata package fails.	5.2	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_ATPUP_APPLY_IDPS_SIGNATURE_FAILED	MGD_ATPUP_APPLY_IDPS_SIGNATURE_FAILED	Error	SD-WAN Edge (MGD)	Generated due to error in applying Suricata files.	5.2	
MGD_ATPUP_APPLY_IDPS_SIGNATURE_SUCCEEDED	MGD_ATPUP_APPLY_IDPS_SIGNATURE_SUCCEEDED	Info	SD-WAN Edge (MGD)	Generated when suricata files are successfully applied.	5.2	
MGD_ATPUP_STANDBY_UPDATE_START	MGD_ATPUP_STANDBY_UPDATE_START	Info	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDPS Signature version is started.	5.2	
MGD_ATPUP_STANDBY_UPDATE_FAILED	MGD_ATPUP_STANDBY_UPDATE_FAILED	Error	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDP Signature version fails.	5.2	
MGD_ATPUP_STANDBY_UPDATED	MGD_ATPUP_STANDBY_UPDATED	Info	SD-WAN Edge (MGD)	Generated when HA Standby update with new EFS IDPS Signature version is successfully applied.	5.2	
HA_SET_PEER_KEYS_SUCCESSFUL	HA_SET_PEER_KEYS_SUCCESSFUL	Notice	SD-WAN Edge (MGD)	Generated by an Edge deployed in a cluster which confirms that it has successfully saved the HA Peer keys for that cluster.	5.4	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
EFS_IDPS_NOT_READY	EFS_IDPS_NOT_READY	ALERT	SD-WAN Edge (MGD)	Generated when packets are dropped while on-prem Orchestrator is not connected to GSM and so IDPS signatures are not ready.	6.0	
EFS_IP_DB_VERSION_UPDATE	EFS_IP_DB_VERSION_UPDATE	INFO	SD-WAN Edge (MGD)	Generated when loading of IP database succeeds or fails.	6.0	
EFS_IP_RTU_DB_VERSION_UPDATE	EFS_IP_RTU_DB_VERSION_UPDATE	INFO	SD-WAN Edge (MGD)	Generated when loading of IP RTU database succeeds or fails.	6.0	
EFS_URL_DB_VERSION_UPDATE	EFS_URL_DB_VERSION_UPDATE	INFO	SD-WAN Edge (MGD)	Generated when loading of URL database succeeds or fails.	6.0	
EFS_URLF_MAL_IP_NOT_READY	EFS_URLF_MAL_IP_NOT_READY	ALERT	SD-WAN Edge (MGD)	Generated when packets are dropped while EFS is activated but URLF/MAL-IP filtering is not ready.	6.0	
EFS_URL_RTU_DB_VERSION_UPDATE	EFS_URL_RTU_DB_VERSION_UPDATE	INFO	SD-WAN Edge (MGD)	Generated when loading of URL RTU database succeeds or fails.	6.0	

Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When	Released In	Deprecated
MGD_EFS_NTICS_REGISTRATION_SUCCEEDED	MGD_EFS_NTICS_REGISTRATION_SUCCEEDED	INFO	SD-WAN Edge (MGD)	Generated when VMware Threat Intelligent Cloud Service (NTICS) registration with Client ID succeeds.	6.0	
MGD_EFS_NTICS_REGISTRATION_FAILED	MGD_EFS_NTICS_REGISTRATION_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when NTICs registration fails with retry count.	6.0	
MGD_EFS_NTICS_AUTHENTICATION_SUCCEEDED	MGD_EFS_NTICS_AUTHENTICATION_SUCCEEDED	INFO	SD-WAN Edge (MGD)	Generated when NTICS authentication succeeds.	6.0	
MGD_EFS_NTICS_AUTHENTICATION_FAILED	MGD_EFS_NTICS_AUTHENTICATION_FAILED	ERROR	SD-WAN Edge (MGD)	Generated when NTICS authentication fails.	6.0	

## Supported VMware SD-WAN Edge Events for Syslogs

The following table describes all the possible VMware SD-WAN Edge events that could be exported to syslog collectors.

Events	Severity	Description
BW_UNMEASURABLE	ALERT	Generated by a SD-WAN Edge when the path bandwidth is unmeasurable.
EDGE BIOS UPDATE FAILED	ERROR	Generated by 12-upgrade-bios.sh script when SD-WAN Edge BIOS is updated.
EDGE BIOS UPDATED	INFO	Generated by 12-upgrade-bios.sh script when SD-WAN Edge BIOS update failed.
EDGE_CONSOLE_LOGIN	INFO	Generated by a SD-WAN Edge during login via console port.
EDGE_DEACTIVATED	WARNING	Generated when a SD-WAN Edge has all its configuration cleared and is not associated with a customer site. The software build remains unchanged.

Events	Severity	Description
EDGE_DHCP_BAD_OPTION	WARNING	Generated when the SD-WAN Edge is configured with an invalid DHCP option.
EDGE_DISK_IO_ERROR	WARNING	Generated by a SD-WAN Edge when the Disk IO error has occurred during upgrade/downgrade.
EDGE_DISK_READONLY	CRITICAL	Generated by a SD-WAN Edge when a Disk turns to read-only mode.
EDGE_DNSMASQ_FAILED	ERROR	Generated when Dnsmasq service failed.
EDGE_DOT1X_SERVICE_DISABLED	WARNING, CRITICAL	Generated by vc_procmon when the SD-WAN Edge 802.1x service is deactivated.
EDGE_DOT1X_SERVICE FAILED	ERROR	Generated by vc_procmon when the SD-WAN Edge 802.1x service failed.
EDGE_HARD_RESET	WARNING	Generated when user has initiated SD-WAN Edge hard reset.
EDGE_HEALTH_ALERT	EMERGENCY	Generated by the SD-WAN Edge when the data plane is unable to allocate necessary resources for packet processing.
EDGE_INTERFACE_DOWN	INFO	Generated by hotplug scripts when the interface is down.
EDGE_INTERFACE_UP	INFO	Generated by hotplug scripts when the interface is up.
EDGE_KERNEL_PANIC	ALERT	Generated by a SD-WAN Edge when the Edge operating system has encountered a critical exception and must reboot the Edge to recover. An Edge reboot is disruptive to customer traffic for 2-3 minutes while the Edge completes the reboot.
EDGE_L2_LOOP_DETECTED	ERROR	Generated when SD-WAN EdgeL2 loop is detected.
EDGE_LED_SERVICE_DISABLED	WARNING, CRITICAL	Generated by vc_procmon when the SD-WAN Edge LED service is deactivated.
EDGE_LED_SERVICE FAILED	ERROR	Generated by vc_procmon when the SD-WAN Edge LED service failed.
EDGE_LOCALUI_LOGIN	INFO	Generated when LOCAL UI login is successful for a user.

Events	Severity	Description
EDGE_MEMORY_USAGE_ERROR	ERROR	Generated by a SD-WAN Edge when the Resource Monitor process detects Edge memory utilization has exceeded defined thresholds and reaches 70% threshold. The Resource Monitor waits for 90 seconds to allow the edged process to recover from a possible temporary spike in memory usage. If memory usage persists at a 70% or higher level for more than 90 seconds, the Edge will generate this error message and send this event to the Orchestrator.
EDGE_MEMORY_USAGE_WARNING	WARNING	Generated by a SD-WAN Edge when the Resource Monitor process detects Edge memory utilization is 50% or more of the available memory. This event will be sent to the Orchestrator every 60 minutes until the memory usage drops under the 50% threshold.
EDGE_MGD_SERVICE_DISABLED	CRITICAL, WARNING	Generated by vc_procmon when mgd is unable to start or deactivated for too many failures.
EDGE_MGD_SERVICE_FAILED	ERROR	Generated by vc_procmon when the mgd service failed.
EDGE_NEW_DEVICE	INFO	Generated when a new DHCP client is identified by processing the DHCP request.
EDGE_NEW_USER	INFO	Generated when a new client user is added.
EDGE_OSPF_NSM	INFO	Generated by the SD-WAN Edge when the OSPF Neighbor state Machine (NSM) state occurred.
EDGE_REBOOTING	WARNING	Generated when a user has initiated SD-WAN Edge reboot.
EDGE_RESTARTING	WARNING	Generated when a user has initiated SD-WAN Edge service restart.
EDGE_SERVICE_DISABLED	WARNING	Generated when the SD-WAN Edge data plane service is deactivated.
EDGE_SERVICE_ENABLED	WARNING	Generated when the SD-WAN Edge data plane service is enabled.
EDGE_SERVICE_FAILED	ERROR	Generated when the SD-WAN Edge data plane service failed.
EDGE_SHUTTING_DOWN	WARNING	Generated when a SD-WAN Edge is shutting down.

<b>Events</b>	<b>Severity</b>	<b>Description</b>
EDGE_STARTUP	INFO	Generated when a SD-WAN Edge is running in mgmt-only mode.
EDGE_SSH_LOGI	INFO	Generated by a SD-WAN Edge during login via SSH protocol.
EDGE_TUNNEL_CAP_WARNING	WARNING	Generated when a SD-WAN Edge has reached its maximum tunnel capacity.
EDGE_USB_PORTS_ENABLED	INFO	Generated when USB ports are enabled on a SD-WAN Edge.
EDGE_USB_PORTS_DISABLED	INFO	Generated when USB ports are deactivated on a SD-WAN Edge.
EDGE_USB_PORTS_ENABLE_FAILURE	CRITICAL	Generated by a SD-WAN Edge when the enable operation for its USB ports fails.
EDGE_USB_PORTS_DISABLE_FAILURE	CRITICAL	Generated by a SD-WAN Edge when the deactivate operation for its USB ports fails.
EDGE_USB_DEVICE_REMOVED	ALERT	Generated by a SD-WAN Edge when a device is removed from its USB port.
EDGE_USB_DEVICE_INSERTED	ALERT	Generated by a SD-WAN Edge when a device is inserted into its USB port.
EDGE_VNFD_SERVICE_DISABLED	WARNING, CRITICAL	Generated by vc_procmon when the Edge VNFD service is deactivated.
EDGE_VNFD_SERVICE_FAILED	ERROR	Generated by vc_procmon when the Edge VNFD service failed.
FLOOD_ATTACK_DETECTED	INFO	Generated when a malicious host floods the SD-WAN Edge with new connections.
GATEWAY_SERVICE_STATE_UPDATE		Generated when the Operator changes the Service State of a Gateway.
HA_FAILED	INFO	HA Peer State Unknown -Generated when the Standby Edge has not sent a heartbeat response and only one of the two HA Edges is communicating with the Orchestrator and Gateways.
HA_GOING_ACTIVE	INFO	An HA failover. Generated when the Active High Availability (HA) Edge has been marked as down and the Standby is brought up to be the Active.
HA_INTF_STATE_CHANGED	ALERT	Generated when the HA Interface state is changed to Active.
HA_READY	INFO	Generated when both the Active and Standby Edges are up and synchronized.

<b>Events</b>	<b>Severity</b>	<b>Description</b>
HA_STANDBY_ACTIVATED	INFO	Generated when the HA Standby Edge has accepted the activation key, downloaded its configuration, and updated its software build.
HA_TERMINATED	INFO	Generated when HA has been deactivated on a SD-WAN Edge.
INVALID_JSON	CRITICAL	Generated when a SD-WAN Edge received an invalid response from MGD.
IP_SLA_PROBE	Up = INFO, Down = ALERT	Generated when an IP ICMP Probe state change.
IP_SLA_RESPONDER	Up = INFO, Down = ALERT	Generated when an IP ICMP Responder state change.
LINK_ALIVE	INFO	Generated when a WAN link is no longer DEAD.
LINK_DEAD	ALERT	Generated when all tunnels established on the WAN link have received no packets for at least seven seconds.
LINK_MTU	INFO	Generated when WAN link MTU is discovered.
LINK_UNUSABLE	ALERT	Generated when WAN link transitions to UNUSABLE state.
LINK_USABLE	INFO	Generated when WAN link transitions to USABLE state.
MGD_ACTIVATION_ERROR	ERROR	Generated when a SD-WAN Edge activation failed. Either the activation link was not correct, or the configuration was not successfully downloaded to the Edge.
MGD_ACTIVATION_PARTIAL	INFO	Generated when a SD-WAN Edge is activated partially, but a software update failed.
MGD_ACTIVATION_SUCCESS	INFO	Generated when a SD-WAN Edge has been activated successfully.
MGD_CONF_APPLIED	INFO	Generated when a configuration change made on the Orchestrator has been pushed to SD-WAN Edge and is successfully applied.
MGD_CONF_FAILED	INFO	Generated when the SD-WAN Edge failed to apply a configuration change made on the Orchestrator.
MGD_CONF_ROLLBACK	INFO	Generated when a configuration policy sent from the Orchestrator had to be rolled back because it destabilized the SD-WAN Edge.

Events	Severity	Description
MGD_CONF_UPDATE_INVALID	INFO	Generated when a SD-WAN Edge has been assigned an Operator Profile with an invalid software image that the Edge cannot use.
MGD_DEACTIVATED	INFO	Generated when a SD-WAN Edge is deactivated based on user request by mgd.
MGD_DEVICE_CONFIG_WARNING/ERROR	WARNING, INFO	Generated when an inconsistent/invalid device setting is detected.
MGD_DIAG_REBOOT	INFO	Generated when a SD-WAN Edge is rebooted by a Remote Action from the Orchestrator.
MGD_DIAG_RESTART	INFO	Generated when the data plane service on the SD-WAN Edge is restarted by a Remote Action from the Orchestrator.
MGD_EMERG_REBOOT	CRITICAL	Generated when a SD-WAN Edge is rebooted to recover from stuck processes by vc_procmn.
MGD_ENTER_LIVE_MODE	DEBUG	Generated when the management service on a SD-WAN Edge is entering the LIVE mode.
MGD_EXIT_LIVE_MODE	DEBUG	Generated when the management service on a SD-WAN Edge is exiting the LIVE mode.
MGD_EXITING	INFO	Generated when the management service on a SD-WAN Edge is shutting down for a restart.
MGD_EXTEND_LIVE_MODE	DEBUG	Generated by a SD-WAN Edge when Live mode is extended.
MGD_FLOW_STATS_PUSH_FAILED	DEBUG	Generated by a SD-WAN Edge when Flow stats pushed to Orchestrator failed.
MGD_FLOW_STATS_PUSH_SUCCEEDED	DEBUG	Generated by a SD-WAN Edge when Flow stats pushed to Orchestrator succeeded.
MGD_FLOW_STATS_QUEUED	INFO	Generated by a SD-WAN Edge when Flow stats pushed to Orchestrator is queued.
MGD_HARD_RESET	INFO	Generated when a SD-WAN Edge is restored to its factory-default software and configuration.
MGD_HEALTH_STATS_PUSH_FAILED	DEBUG	Generated by a SD-WAN Edge when Health stats pushed to Orchestrator failed.

Events	Severity	Description
MGD_HEALTH_STATS_PUSH_SUCCEEDED	DEBUG	Generated by a SD-WAN Edge when Health stats pushed to Orchestrator succeeded.
MGD_HEALTH_STATS_QUEUED	INFO	Generated by a SD-WAN Edge when Health stats pushed to Orchestrator is queued.
MGD_HEARTBEAT	INFO	Generated by a SD-WAN Edge when Heartbeat is generated to Orchestrator.
MGD_HEARTBEAT_FAILURE	INFO	Generated by a SD-WAN Edge when generated Heartbeat to Orchestrator failed.
MGD_HEARTBEAT_SUCCESS	INFO	Generated by a SD-WAN Edge when generated Heartbeat to Orchestrator succeeded.
MGD_INVALID_VCO_ADDRESS	WARNING	Generated when an invalid address for Orchestrator was sent in a management plane policy update and was ignored.
MGD_LINK_STATS_PUSH_FAILED	DEBUG	Generated by a SD-WAN Edge when Link stats pushed to Orchestrator failed.
MGD_LINK_STATS_PUSH_SUCCEEDED	DEBUG	Generated by a SD-WAN Edge when Link stats pushed to Orchestrator succeeded.
MGD_LINK_STATS_QUEUED	INFO	Generated by a SD-WAN Edge when Link stats pushed to Orchestrator is queued.
MGD_LIVE_ACTION_FAILED	DEBUG	Generated by a SD-WAN Edge when Live Action failed.
MGD_LIVE_ACTION_REQUEST	DEBUG	Generated by a SD-WAN Edge when Live Action is requested.
MGD_LIVE_ACTION_SUCCEEDED	DEBUG	Generated by a SD-WAN Edge when Live Action is succeeded.
MGD_NETWORK_MGMT_IF_BROKEN	ALERT	Generated when the Management network is set up incorrectly.
MGD_NETWORK_MGMT_IF_FIXED	WARNING	Generated when a Network is restarted twice to fix the Management Network inconsistency.
MGD_NETWORK_SETTINGS_UPDATE_D	INFO	Generated when new network settings are applied to a SD-WAN Edge.
MGD_SET_CERT_FAIL	ERROR	Generated when the installation of a new PKI certificate for Orchestrator communication on a SD-WAN Edge has failed.

<b>Events</b>	<b>Severity</b>	<b>Description</b>
MGD_SET_CERT_SUCCESS	INFO	Generated when a new PKI certificate for Orchestrator communication is installed successfully on a SD-WAN Edge.
MGD_SHUTDOWN	INFO	Generated when the SD-WAN Edge diagnostic shutdown based on user request.
MGD_START	INFO	Generated when the management daemon on the SD-WAN Edge has started.
MGD_SWUP_DOWNLOAD_FAILED	ERROR	Generated when the download of an Edge software update image has failed.
MGD_SWUP_DOWNLOAD_SUCCEEDED	DEBUG	Generated when the download of an Edge software update image has succeeded.
MGD_SWUP_IGNORED_UPDATE	INFO	Generated when a software update is ignored at the activation time, because SD-WAN Edge is already running that version.
MGD_SWUP_INSTALL_FAILED	ERROR	Generated when a software update installation failed.
MGD_SWUP_INSTALLED	INFO	Generated when a software update was successfully downloaded and installed.
MGD_SWUP_INVALID_SWUPDATE	WARNING	Generated when a software update package received from the Orchestrator is invalid.
MGD_SWUP_REBOOT	INFO	Generated when the SD-WAN Edge is being rebooted after a software update.
MGD_SWUP_STANDBY_UPDATE FAILED	ERROR	Generated when a software update of the standby HA Edge failed.
MGD_SWUP_STANDBY_UPDATE_STARTED	INFO	Generated when the HA standby software update has started.
MGD_SWUP_STANDBY_UPDATED	INFO	Generated when a software update of the standby HA Edge has started.
MGD_SWUP_UNPACK_FAILED	ERROR	Generated when an Edge has failed to unpack the downloaded software update package.
MGD_SWUP_UNPACK_SUCCEEDED	INFO	Generated when an Edge has succeeded to unpack the downloaded software update package.

Events	Severity	Description
MGD_UNREACHABLE	EMERGENCY	Generated when the data plane process could not communicate to the management plane proxy.
MGD_VCO_ADDR_RESOLV_FAILED	WARNING	Generated when the DNS resolution of the Orchestrator address failed.
MGD_WEBSOCKET_INIT	DEBUG	Generated when a WebSocket communication is initiated with the Orchestrator.
MGD_WEBSOCKET_CLOSE	DEBUG	Generated when a WebSocket communication with the Orchestrator is closed.
NSD_MIGRATION_TASKS_QUEUED		Generated when the Enterprise customers have pending migration tasks for the Gateways that are attached to Non SD-WAN Destinations.
PEER_UNUSABLE	ALERT	Generated when overlay connectivity to a peer goes down while transmitting peer stats.
PEER_USABLE	INFO	Generated when overlay connectivity to a peer resumes after a period of unusability.
PORT_SCAN_DETECTED	INFO	Generated when port scan is detected.
QOS_OVERRIDE	INFO	Generated to flip traffic path (gateway or direct).
REBALANCE_EDGE_SUCCEEDED		Generated when the Enterprise customers have successfully rebalanced the required Edges from the quiesced Gateway to the new Gateway.
SLOW_START_CAP_MET	NOTICE	Generated when the Bandwidth measurement slow-start cap limit is exceeded. It will be done in Burst mode
SWITCH_GATEWAY_COMPLETED		Generated when the Enterprise customers have successfully switched the traffic from the quiesced Gateways to new Gateways for Non SD-WAN Destinations.
SWITCH_GATEWAY_FAILED		Generated when the Switch Gateway action for a Non SD-WAN Destination fails during the SD-WAN Gateway migration.
VPN_DATACENTER_STATUS	INFO, ERROR	Generated when a VPN Tunnel state change.
VRRP_FAIL_INFO	INFO	Generated when VRRP failed.

Events	Severity	Description
VRRP_INTO_MASTER_STATE	INFO	Generated when VRRP get into Primary state.
VRRP_OUT_OF_MASTER_STATE	INFO	Generated when VRRP get out of Primary state.