

VMware Cloud on AWS Networking and Security

16 June 2022

SDDC Version 1.18

VMware Cloud on AWS

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

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2017-2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

About VMware Cloud on AWS Networking and Security 5

1 NSX-T Networking Concepts 6

Features Supported with NSX-T 12

2 Configuring VMware Cloud on AWS Networking and Security Using NSX-T 14

Assign NSX Service Roles to Organization Members 15

SDDC Network Administration with NSX-T Manager 17

Open NSX Manager 18

Configure AWS Direct Connect Between Your SDDC and On-Premises Data Center 21

Set Up an AWS Direct Connect Connection 22

Configure Direct Connect to a Private Virtual Interface for SDDC Management and Compute Network Traffic 22

Configure Direct Connect to a Public Virtual Interface for Access to AWS Services 26

Specify the Direct Connect MTU 27

Configure a VPN Connection Between Your SDDC and On-Premises Data Center 28

Create a Route-Based VPN 29

Create a Policy-Based VPN 33

Configure a Layer 2 VPN and Extended Network Segment 38

View VPN Tunnel Status and Statistics 42

IPsec VPN Settings Reference 43

Configure Management Gateway Networking and Security 45

Set vCenter Server FQDN Resolution Address 45

Set HCX FQDN Resolution Address 46

Add or Modify Management Gateway Firewall Rules 46

Configure Compute Gateway Networking and Security 51

Create or Modify a Network Segment 51

Add or Modify Compute Gateway Firewall Rules 58

Add or Modify Distributed Firewall Rules 61

Configure DNS Services 67

View Routes Learned and Advertised over VMware Transit Connect 69

View Statistics and Manage Settings for Uplinks 69

Add a Tier-1 Gateway 70

Configure a Multi-Edge SDDC With Traffic Groups 72

Enable AWS Managed Prefix List Mode for the Connected Amazon VPC 76

Working With Inventory Groups 78

Add a Management Group 78

Add or Modify a Compute Group 79

Add a Custom Service	81
View Virtual Machine Inventory	81
About Context Profiles	82
Managing Workload Connections	82
Attach a VM to or Detach a Workload VM from a Compute Network Segment	83
Request or Release a Public IP Address	84
Create or Modify NAT Rules	84
Creating Firewall Rules to Manage Traffic Between the Compute and Management Networks	88
3 Configure Monitoring and Troubleshooting Features	90
Configure IPFIX	90
Configure Port Mirroring	91
View Connected VPC Information and Troubleshoot Problems With the Connected VPC	92
4 About NSX Advanced Firewall Features	95

About VMware Cloud on AWS Networking and Security

The *VMware Cloud on AWS Networking and Security* guide provides information about configuring NSX-T networking and security for VMware Cloud on AWS.

Intended Audience

This information is intended for anyone who wants to use VMware Cloud on AWS to create an SDDC that has the networking and security infrastructure necessary to migrate workloads off premises and run them securely in the cloud. It was written for readers who have used vSphere in an on-premises environment and are familiar with the fundamentals of IP networking using NSX-T or another networking solution. In-depth knowledge of vSphere or Amazon Web Services is not required.

For a detailed discussion of how VMware Cloud on AWS uses NSX-T networking, see the VMware Press eBook [VMware Cloud on AWS: NSX Networking and Security](#).

NSX-T Networking Concepts

1

VMware Cloud on AWS uses NSX-T to create and manage SDDC networks. NSX-T provides an agile software-defined infrastructure to build cloud-native application environments

The *VMware Cloud on AWS Networking and Security* explains how to use the VMC Console **Networking & Security** tab to manage your SDDC networks. Beginning with SDDC version 1.16, you also can use the NSX Manager Web UI to manage these networks. NSX Manager supports a superset of the features found on the **Networking & Security** tab. See [NSX Manager](#) in the *NSX-T Data Center Administration Guide* for information about how to use NSX Manager. The NSX Manager in your VMware Cloud on AWS SDDC is accessible at a public IP address reachable by any browser that can connect to the Internet. You can also access it from your internal network over a VPN or AWS Direct Connect. See [Open NSX Manager](#) for details.

User interface layout and navigation in the NSX Manager Web UI is similar to that of the VMC Console **Networking & Security** tab, and you can use either tool to complete most of the procedures in this document. The **Networking & Security** tab combines NSX **Networking** features like VPN, NAT, and DHCP with NSX-T **Security** features like firewalls. When a procedure requires you to use NSX Manager, we note that in the prerequisites to the procedure.

SDDC Network Topology

When you create an SDDC, it includes a Management Network. Single-host trial SDDCs also include a small Compute Network. You specify the Management Network CIDR block when you create the SDDC. It cannot be changed after the SDDC has been created. See [Deploy an SDDC from the VMC Console](#) for details. The Management Network has two subnets:

Appliance Subnet

This subnet is used by the vCenter Server, NSX-T, and HCX appliances in the SDDC. When you add appliance-based services such as SRM to the SDDC, they also connect to this subnet.

Infrastructure Subnet

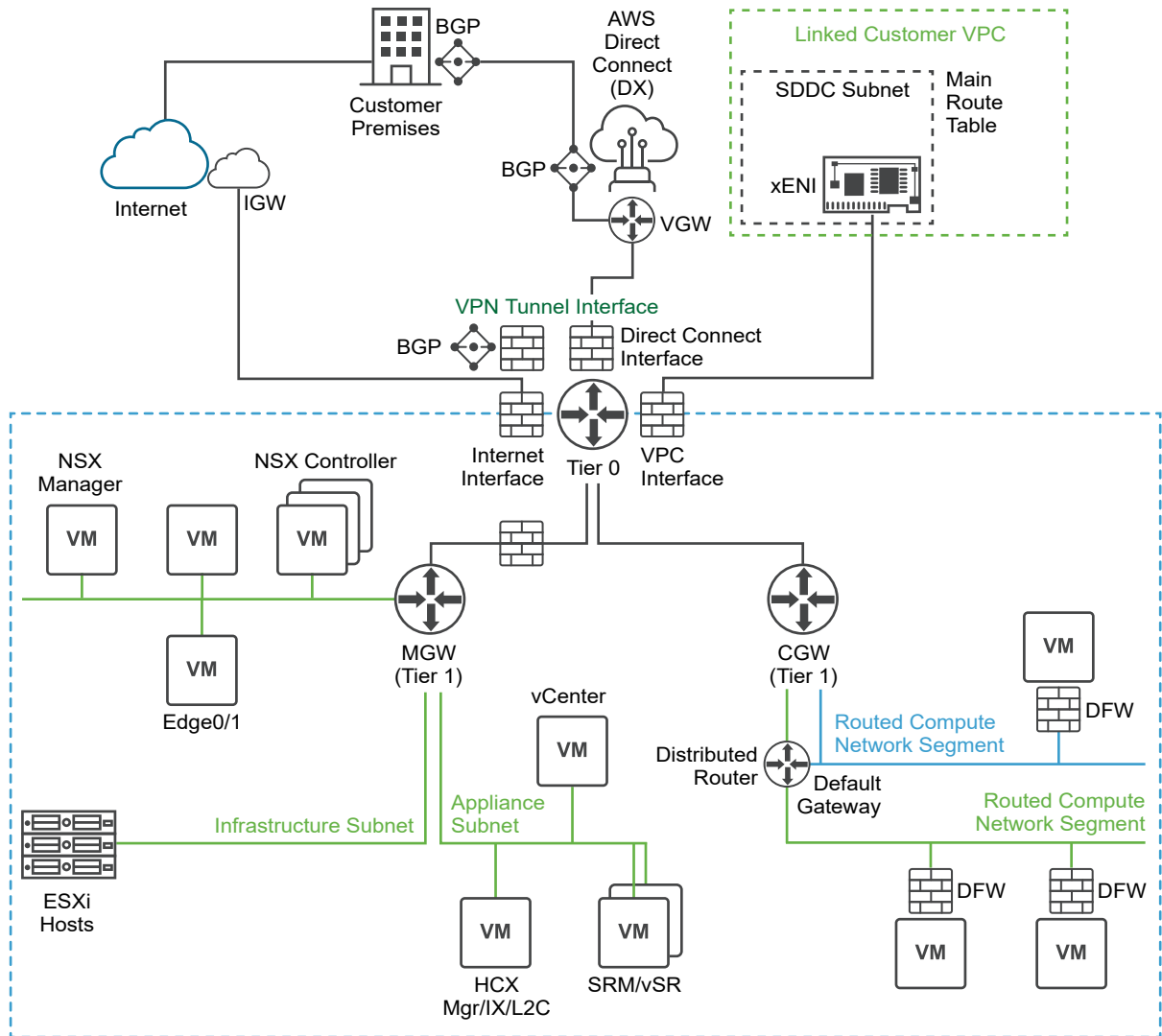
This subnet is used by the ESXi hosts in the SDDC.

The Compute Network includes an arbitrary number of logical segments for your workload VMs. See [VMware Configuration Maximums](#) for current limits on logical segments. In a Single Host SDDC starter configuration, we create a compute network with a single routed segment. In SDDC configurations that have more hosts, you'll have to create compute network segments to meet your needs. See [VMware Configuration Maximums](#) for applicable limits.

An SDDC network has two notional tiers:

- Tier 0 handles north-south traffic (traffic leaving or entering the SDDC, or between the Management and Compute gateways). In the default configuration, each SDDC has a single Tier-0 router. If an SDDC is a member of an SDDC group, you can reconfigure the SDDC to add Tier-0 routers that handle SDDC group traffic. See [Configure a Multi-Edge SDDC With Traffic Groups](#).
- Tier 1 handles east-west traffic (traffic between routed network segments within the SDDC). In the default configuration, each SDDC has a single Tier-1 router. You can create and configure additional Tier-1 gateways if you need them. See [Add a Tier-1 Gateway](#).

Figure 1-1. SDDC Network Topology



NSX Edge Appliance

The default NSX Edge Appliance is implemented as a pair of VMs that run in active/standby mode. This appliance provides the platform on which the default Tier 0 and Tier 1 routers run, along with IPsec VPN connections and their BGP routing machinery. All north-south traffic goes through the default Tier 0 router. To avoid sending east-west traffic through the appliance, a component of each Tier 1 router runs on every ESXi host that handles routing for destinations within the SDDC.

If you need additional bandwidth for the subset of this traffic routed to SDDC group members, a Direct Connect Gateway attached to an SDDC group, HCX Service Mesh, or to the Connected VPC, you can reconfigure your SDDC to be Multi-Edge by creating traffic groups, each of which creates an additional T0 router. See [Configure a Multi-Edge SDDC With Traffic Groups](#) for details.

Note VPN traffic, as well as DX traffic to a private VIF must pass through on the default T0 and cannot be routed to a non-default traffic group. In addition, because NAT rules always run on the default T0 router, additional T0 routers cannot handle traffic subject to NAT rules. This includes traffic to and from the SDDC's native Internet connection. It also includes traffic to the Amazon S3 service, which uses a NAT rule and must go through the default T0.

Management Gateway (MGW)

The MGW is a Tier 1 router that handles routing and firewalling for vCenter Server and other management appliances running in the SDDC. Management gateway firewall rules run on the MGW and control access to management VMs. In a new SDDC, the Internet connection is labelled **Not Connected** in the **Overview** tab and remains blocked until you create a Management Gateway Firewall rule allowing access from a trusted source. See [Add or Modify Management Gateway Firewall Rules](#).

Compute Gateway (CGW)

The CGW is a Tier 1 router that handles network traffic for workload VMs connected to routed compute network segments. Compute gateway firewall rules, along with NAT rules, run on the Tier 0 router. In the default configuration, these rules block all traffic to and from compute network segments (see [Configure Compute Gateway Networking and Security](#)).

Routing Between Your SDDC and the Connected VPC

Important Any VPC Subnets on which AWS services or instances communicate with the SDDC must be associated with the main route table of the Connected VPC. Use of a custom route table or replacement of the main route table is not supported.

When you create an SDDC, we pre-allocate 17 AWS Elastic Network Interfaces (ENIs) in the selected VPC owned by the AWS account you specify at SDDC creation. We assign each of these ENIs an IP address from the subnet you specify at SDDC creation, then attach each of the hosts in the SDDC cluster `cluster-1` to one of these ENIs. An additional IP address is assigned to the ENI where the active NSX Edge Appliance is running.

This configuration, known as the Connected VPC, supports network traffic between VMs in the SDDC and native AWS service endpoints. The main route table of the Connected VPC is aware of the VPC's primary subnet as well as all SDDC subnets (NSX-T network segments). When you create or delete routed network segments on the SDDC, the main route table is automatically updated. When the NSX Edge appliance in your SDDC is moved to another host, either to recover from a failure or during SDDC maintenance, the IP address allocated to the appliance is moved to the new ENI (on the new host), and the main route table is updated to reflect the change. If

you have replaced the main route table or are using a custom route table, that update fails and network traffic can no longer be routed between SDDC networks and the Connected VPC. See [View Connected VPC Information and Troubleshoot Problems With the Connected VPC](#) for more about how to use the VMC Console to see the details of your Connected VPC.

VMware Cloud on AWS provides several facilities to help you aggregate routes to the Connected VPC, other VPCs, and your VMware Managed Transit Gateways. See [Enable AWS Managed Prefix List Mode for the Connected Amazon VPC](#) and [Manage Routing to an External VPC](#).

For an in-depth discussion of SDDC network architecture and the AWS network objects that support it, read the VMware Cloud Tech Zone article [VMware Cloud on AWS: SDDC Network Architecture](#).

Reserved Network Addresses

Certain IPv4 address ranges are unavailable for use in SDDC compute networks. Several are used internally by SDDC network components. Most are reserved by convention on other networks as well.

Table 1-1. Reserved Address Ranges in SDDC Networks

<ul style="list-style-type: none"> ■ 10.0.0.0/15 ■ 172.31.0.0/16 	These ranges are reserved within the SDDC management subnet, but can be used in your on-premises networks or SDDC compute network segments.
100.64.0.0/16	Reserved for carrier-grade NAT per RFC 6598 . Avoid using addresses in this range in SDDC networks and others. They are not likely to be reachable within the SDDC or from outside it. See VMware Knowledge Base article 76022 for a detailed breakdown of how SDDC networks use this address range.
<ul style="list-style-type: none"> ■ 169.254.0.0/19 ■ 169.254.64.0/24 ■ 169.254.101.0/30 ■ 169.254.105.0/24 ■ 169.254.106.0/24 	Per RFC 3927 , all of 169.254.0.0/16 is a link-local range that cannot be routed beyond a single subnet. However, with the exception of these CIDR blocks, you can use 169.254.0.0/16 addresses for your virtual tunnel interfaces. See Create a Route-Based VPN .
192.168.1.0/24	This the default compute segment CIDR for a single-host starter SDDC and is not reserved in other configurations.

SDDC networks also observe the conventions for special Use IPv4 address ranges enumerated in [RFC 3330](#).

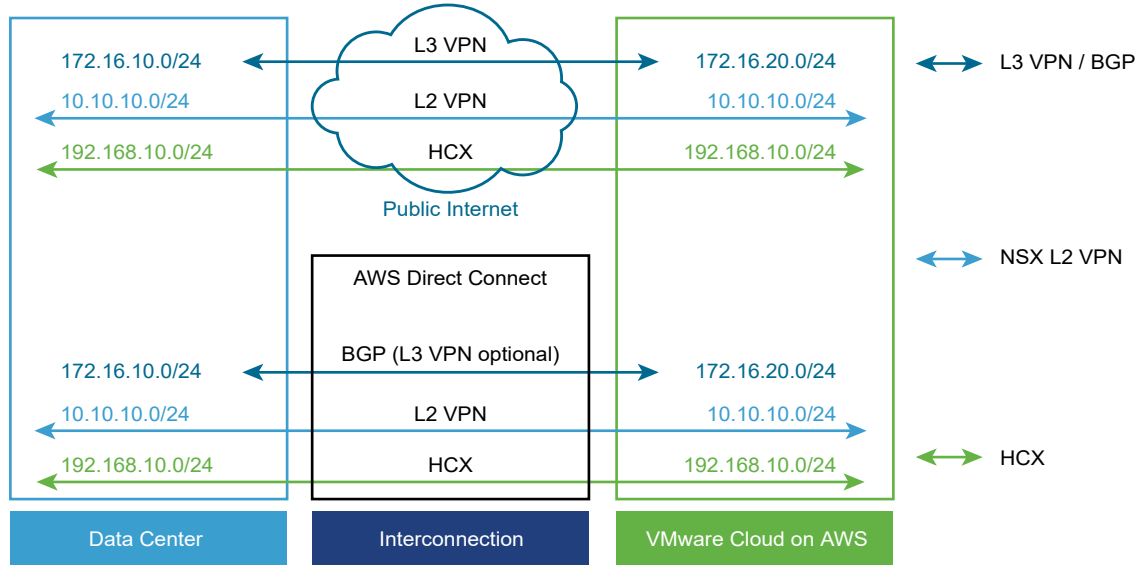
Multicast Support in SDDC Networks

In SDDC networks, layer 2 multicast traffic is treated as broadcast traffic on the network segment where the traffic originates. It is not routed beyond that segment. Layer 2 multicast traffic optimization features such as IGMP snooping are not supported. Layer 3 multicast (such as Protocol Independent Multicast) is not supported in VMware Cloud on AWS.

Connecting Your On-Premises SDDC to Your Cloud SDDC

To connect your on-premises data center to your VMware Cloud on AWS SDDC, you can create a VPN that uses the public Internet, a VPN that uses AWS Direct Connect, or just use AWS Direct Connect alone. You can also take advantage of SDDC groups to use VMware Transit Connect™ and an AWS Direct Connect Gateway to provide centralized connectivity between a group of VMware Cloud on AWS SDDCs and an on-premises SDDC. See [Creating and Managing SDDC Deployment Groups](#) in the *VMware Cloud on AWS Operations Guide*.

Figure 1-2. SDDC Connections to your On-Premises Data Center



Layer 3 (L3) VPN

A layer 3 VPN provides a secure connection between your on-premises data center and your VMware Cloud on AWS SDDC over the public Internet or AWS Direct Connect. These IPsec VPNs can be either route-based or policy-based. For the on-premises endpoint, you can use any device that supports the settings listed in the [IPsec VPN Settings Reference](#).

Layer 2 (L2) VPN

A layer 2 VPN provides an extended, or stretched, network with a single IP address space that spans your on-premises data center and your SDDC and enables hot or cold migration of on-premises workloads to the SDDC. You can create only a single L2VPN tunnel in any SDDC. The on-premises end of the tunnel requires NSX. If you are not already using NSX in your on-premises data center, you can download a standalone NSX Edge appliance to provide the required functionality. An L2 VPN can connect your on-premises data center to the SDDC over the public Internet or AWS Direct Connect.

AWS Direct Connect (DX)

AWS Direct Connect is a service provided by AWS that creates a high-speed, low latency connection between your on-premises data center and AWS services. When you configure

AWS Direct Connect, VPNs can route traffic over DX instead of the public Internet. Because DX implements Border Gateway Protocol (BGP) routing, use of an L3VPN for the management network is optional when you configure DX. DX traffic is not encrypted. If you want to encrypt that traffic, configure an IPsec VPN that uses DX and a private IP address.

VMware HCX

VMware HCX, a multi-cloud app mobility solution, is provided free to all SDDCs and facilitates migration of workload VMs to and from your on-premises data center to your SDDC. For more information about installing, configuring, and using HCX, see the [Hybrid Migration with HCX Checklist](#).

This chapter includes the following topics:

- [Features Supported with NSX-T](#)

Features Supported with NSX-T

NSX-T support a wide range of networking and security solutions.

NSX-T was designed specifically to support diverse data center environments at scale and provide robust capabilities for containers and the cloud.

Note NSX-T Configuration Maximums are now included in [VMware Configuration Maximums](#).

Networking and Connectivity Features

NSX-T provides all the networking capabilities required by workloads running in the SDDC. These capabilities allow you to:

- Deploy networks (L2, L3, and isolated) and define subnets and gateways for the workloads that will reside there.
 - L2VPNs extend your on-premises L2 domains to the SDDC, enabling workload migration without IP address changes.
 - Route-based IPsec VPNs can connect to on-premises networks, VPCs, or other SDDCs. Route-based VPNs use BGP to learn new routes as networks become available.
 - Policy-based IPsec VPNs can also be used to connect to on-premises networks, VPCs, or other SDDCs.
 - Isolated networks have no uplinks, and provide access only to those VMs connected to them.
- Use AWS Direct Connect (DX) to carry traffic between on-premises and SDDC networks over high bandwidth, low latency connectivity. You can optionally use a route-based VPN as backup for DX traffic.
- Enable native DHCP selectively for network segments or use DHCP relay to link with an on-premises IPAM solution.

- Create multiple DNS zones, allowing use of different DNS servers for network subdomains.
- Take advantage of distributed routing, managed by an NSX kernel module running on the host where the workload resides, so workloads can efficiently communicate with each other.

Security Features

NSX-T security features include network address translation (NAT) and advanced firewall capabilities.

- Source NAT (SNAT) is automatically applied to all workloads in the SDDC to enable Internet access. To provide a secure environment, Internet access is blocked at edge firewalls, but firewall policy can be changed to allow managed access. You can also request a public IP for workloads and create custom NAT policies for them.
- Edge firewalls run on the management and compute gateways. These stateful firewalls examine all traffic into and out of the SDDC.
- Distributed Firewall (DFW) is a stateful firewall that runs on all SDDC hosts. It provides protection for traffic within the SDDC and enables micro-segmentation to allow fine-grained control over traffic between workloads.

Network Operations Tools

NSX-T also provides several popular network operations management tools.

- Port mirroring can send mirrored traffic from a source to a destination appliance in the SDDC or your on-premises network.
- IPFIX supports segment-specific network traffic analysis by sending traffic flows to an IPFIX collector.

Configuring VMware Cloud on AWS Networking and Security Using NSX-T

2

Follow this workflow to configure NSX-T networking and security in your SDDC.

Procedure

1 Assign NSX Service Roles to Organization Members

Grant users in your organization an NSX service role to allow them to view or configure features on the Networking & Security tab.

2 SDDC Network Administration with NSX-T Manager

You can use either the NSX-T Web UI or the VMC Console **Networking & Security** tab to manage your SDDC networks.

3 Configure AWS Direct Connect Between Your SDDC and On-Premises Data Center

Use of AWS Direct Connect is optional. If traffic between your on-premises network and your SDDC workloads requires higher speeds and lower latency than you can achieve with a connection over the public Internet, configure VMware Cloud on AWS to use AWS Direct Connect.

4 Configure a VPN Connection Between Your SDDC and On-Premises Data Center

Configure a VPN to provide a secure connection to your SDDC over the public Internet or AWS Direct Connect. Route-based and policy-based IPsec VPNs are supported. Either type of VPN can connect to the SDDC over the Internet. A route-based VPN can also connect to the SDDC over AWS Direct Connect.

5 Configure Management Gateway Networking and Security

The management network and Management Gateway are largely preconfigured in your SDDC, but you'll still need to configure access to management network services like vCenter and HCX and create management gateway firewall rules to allow traffic between the management network and other networks, including your on-premises networks and other SDDC networks.

6 Configure Compute Gateway Networking and Security

Compute Gateway networking includes a compute network with one or more segments and the DNS, DHCP, and security (gateway firewall and distributed firewall) configurations that manage network traffic for workload VMs. It can also include a layer 2 VPN and extended network that provides a single broadcast domain that spans your on-premises network and your SDDC workload network.

7 Add a Tier-1 Gateway

Every new SDDC includes a default Tier-1 gateway named the Compute Gateway (CGW). You can create and configure additional Tier-1 gateways if you need them. Each Tier-1 gateway sits between the SDDC Tier-0 gateway and an arbitrary number of compute network segments.

8 Configure a Multi-Edge SDDC With Traffic Groups

In the default configuration, your SDDC network has a single edge (T0) router through which all North-South traffic flows. This edge supports the default traffic group, which is not configurable. If you need additional bandwidth for the subset of this traffic routed to SDDC group members, a Direct Connect Gateway attached to an SDDC group, VMware HCX Service Mesh, or to the Connected VPC, you can reconfigure your SDDC to be Multi-Edge by creating traffic groups, each of which creates an additional T0 router.

9 Enable AWS Managed Prefix List Mode for the Connected Amazon VPC

AWS Managed Prefix List Mode can simplify route table management in a Multi-Edge SDDC and enable support in any SDDC for custom route tables and route aggregation.

10 Working With Inventory Groups

VMware Cloud on AWS network administrators can use NSX-T inventory objects to define collections of services, groups, context profiles, and virtual machines to use in firewall rules.

11 Managing Workload Connections

Workload VMs on routed segments or HCX extended networks with MON enabled can connect to the Internet by default. NAT rules, Compute Gateway firewall rules, and distributed firewall rules, as well as default routes advertised by a VPN, DX, or VTGWconnection all give you fine-grained control over Internet access.

Assign NSX Service Roles to Organization Members

Grant users in your organization an NSX service role to allow them to view or configure features on the Networking & Security tab.

Organization roles specify the privileges that an organization member has over organization assets. Service roles specify the privileges that an organization member has when accessing VMware Cloud Services that the organization uses. All service roles can be assigned and changed by a user with organization owner privileges, so restrictive roles such as Administrator (Delete Restricted) or NSX Cloud Auditor should be assigned along with the role of organization member to prevent modification.

A user must log out and then log back in for a new service role to take effect.

Prerequisites

You must be an Organization Owner to assign a role to an organization member.

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click the services icon and select **Identity & Access Management**.
- 3 Select a user and click **Edit Roles**.
- 4 Select a role name from the **Assign Organization Roles** drop-down control.

The following roles are available:

Organization Owner

This role has full rights to manage organization members and assets.

Organization Member

This role has rights to access organization assets.

- 5 Select the **VMware Cloud on AWS** service name under **Assign Service Roles**.
- 6 Select an NSX service role to assign.

The following NSX service roles are available:

NSX Cloud Auditor

This role can view NSX service settings and events but cannot make any changes to the service.

NSX Cloud Admin

This role can perform all tasks related to deployment and administration of the NSX service.

Note When multiple service roles are assigned to an organization user, permissions are granted for the most permissive role. For example, an organization member who has both the NSX Cloud Admin and NSX Cloud Auditor roles is granted all the NSX Cloud Admin permissions, which include those granted to the NSX Cloud Auditor role.

- 7 Click **SAVE** to save your changes.

What to do next

Ensure that any users whose roles were changed log out and log back in for the changes to take effect.

SDDC Network Administration with NSX-T Manager

You can use either the NSX-T Web UI or the VMC Console **Networking & Security** tab to manage your SDDC networks.

NSX Manager supports a superset of the features found on the **Networking & Security** tab. See [NSX Manager](#) in the *NSX-T Data Center Administration Guide* for information about how to use NSX Manager.

Accessing NSX-T Manager

You can use Direct Connect or a VPN to can access the local NSX-T manager at its private IP address, or use any browser to access it over the Internet at its public IP address. See [Open NSX Manager](#).

Note Many NSX-T workflows start by telling you to "log in with admin privileges to an NSX Manager." If you use the **Networking & Security** tab or click **OPEN NSX MANAGER** and choose **ACCESS VIA THE INTERNET**, you can skip this step. Both options give you access to the SDDC NSX-T manager with the rights included in your VMware Cloud on AWS organization role. The **NSX Cloud Admin** role has admin access to NSX-T. The the **NSX Cloud Auditor** has read-only access to NSX-T. See [Assign NSX Service Roles to Organization Members](#) for more information on service roles and how to assign them.

If you click **OPEN NSX MANAGER** and log in to NSX-T via the internal network, your role is determined by your NSX-T credentials, not your organization role.

Workflow Navigation

The **Networking & Security** tab combines NSX-T **Networking** page features like VPN, NAT, and DHCP with **Security** page features like firewalls and features from other NSX-T pages including **Inventory**, **Plan & Troubleshoot**, and **System**. In this publication, references to NSX-T user interface items apply to both the NSX Manager Web UI and the VMC Console **Networking & Security** tab.

Use this table to map starting points for workflows in this publication to the appropriate items in the **Networking & Security** tab and NSX-T manager

Table 2-1. SDDC Network Administration Workflows

Workflow	Networking & Security Tab	NSX-T
Overview	Overview	Overview
Create or Modify a Network Segment	Network > Segments	Networking > Connectivity > Segments
Configure a VPN Connection Between Your SDDC and On-Premises Data Center	Network > VPN	Networking > Network Services > VPN
Create or Modify NAT Rules	Network > NAT	Networking > Network Services > NAT

Table 2-1. SDDC Network Administration Workflows (continued)

Workflow	Networking & Security Tab	NSX-T
Add a Tier-1 Gateway	Network > Tier-1 Gateways	Networking > Connectivity > Tier-1 Gateways
Configure a Multi-Edge SDDC With Traffic Groups	Network > Transit Connect	Networking > Cloud Services > Transit Connect
Configure AWS Direct Connect Between Your SDDC and On-Premises Data Center	System > Direct Connect	Networking > Cloud Services > Direct Connect
View Connected VPC Information and Troubleshoot Problems With the Connected VPC	System > Connected VPC	Networking > Cloud Services > Connected VPC
Request or Release a Public IP Address	System > Public IPs	Networking > Cloud Services > Public IPs
Configure DNS Services	System > DNS	Networking > IP Management > DNS
Configure Segment DHCP Properties	System > DHCP	Networking > IP Management > DHCP
Add or Modify Management Gateway Firewall Rules, Add or Modify Compute Gateway Firewall Rules	Security > Gateway Firewall	Security > Gateway Firewall
Add or Modify Distributed Firewall Rules	Security > Distributed Firewall	Security > Distributed Firewall
Chapter 4 About NSX Advanced Firewall Features	Security > Distributed IDS/IPS	Security > Distributed IDS/IPS
Working With Inventory Groups	Inventory	Inventory
Chapter 3 Configure Monitoring and Troubleshooting Features	Tools	Plan & Troubleshoot

Open NSX Manager

Beginning with SDDC version 1.16, the SDDC NSX-T Manager is accessible at a public IP address reachable by any browser that can connect to the Internet. Click **OPEN NSX MANAGER** on the SDDC **Summary** page.

The SDDC NSX-T Manager also has a private IP address on the management network, which is protected by the management gateway (MGW). By default, the MGW blocks traffic to all management network destinations, including NSX-T, from all sources. To access the local NSX-T Manager at its private IP address, you must add management gateway firewall rules that allow only secure traffic from trusted sources. You can use any of the following connection types to connect to the SDDC NSX-T Manager at a private IP address:

- [Configure AWS Direct Connect Between Your SDDC and On-Premises Data Center](#)

This option provides a dedicated connection between your enterprise and the SDDC. It can be combined with an IPsec VPN to encrypt traffic.

■ Configure a VPN Connection Between Your SDDC and On-Premises Data Center

This option provides an encrypted connection between your enterprise and the SDDC.

If you can't use Direct Connect or a VPN, you can access the local NSX-T manager over the Internet at its public IP address. All traffic to the local NSX manager public IP is encrypted and authenticated, which minimizes the risk of tampering with this connection or its traffic outside of your private network. The **Settings** tab for your SDDC provides connection and authentication details for connecting to the local NSX-T manager.

Note In an SDDC where VMware Tanzu Kubernetes Grid has been enabled, NSX Manager can display a **Load Balancers** tab. Services from this load balancer are available only to Tanzu Kubernetes Grid workloads. See VMware Knowledge Base article [86368](#) for more information.

Prerequisites

This operation is restricted to users who have an organization role of **NSX Cloud Admin** or **NSX Cloud Auditor**. See [Assign NSX Service Roles to Organization Members](#) for more information on service roles and how to assign them.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click the **OPEN NSX MANAGER** button on the SDDC card to open the local NSX-T Manager at its default public IP address.

You are logged in to NSX-T using your VMware Cloud on AWS credentials.

- 4 If your SDDC includes a VPN or DX connection and you want to access NSX-T Manager at its private IP address, create a Management Gateway firewall rule that allows HTTPS traffic from the VPN or DX to the local NSX-T Manager, then use a browser to open a connection to one of the **NSX Manager URLs** listed on the **Settings** tab.

- a Click the **OPEN NSX MANAGER** button or open the **Networking & Security** tab and create the firewall rule.

See [Add or Modify Management Gateway Firewall Rules](#) for more information about how to create a Management Gateway firewall rule. The rule must have the following parameters:

MGW Firewall Rule Property	Value
Sources	An IP address or CIDR block in your on-premises data center. Important Although you can select Any as the source address in a firewall rule, using Any as the source address in this firewall rule can enable attacks on your NSX-T Manager and may lead to compromise of your SDDC. As a best practice, configure this firewall rule to allow access only from trusted source addresses.
Destinations	The NSX Manager system-defined group.
Services	HTTPS (TCP 443)
Action	Allow

- b Use a browser to open a connection to NSX-T.

Expand the **NSX Manager URLs** on the **Settings** tab to see the URLs and accounts that you can use.

Access NSX Manager via the Internet

This URL contains the local NSX-T Manager's public IP address. We use this address when you click the **OPEN NSX MANAGER** button.

Access NSX Manager via internal network

This is the NSX-T Manager's **Private IP** address on the management subnet. A management gateway firewall rule like the one shown in [4.a](#) allows traffic to this address.

If you cannot access NSX-T Manager via the internal network even though you have created the necessary firewall rules, the problem might be caused by transient network issues. Click **TRY AGAIN** to re-try access via the internal network, or open a browser and connect to NSX-T Manager at its public URL. NSX-T private and public URLs are listed on the SDDC Console **Settings** page.

URL to access via internal network (Log in through VMware Cloud Services)

Open this URL in a browser and log in to NSX-T manager using your VMware Cloud on AWS credentials.

URL to access via internal network (Log in through NSX Manager credentials)

Open this URL in a browser and log in using the credentials of the **NSX Manager Admin User Account** (to perform all tasks related to deployment and administration of NSX) or the **NSX Manager Audit User Account** (to view NSX-T service settings and events).

- c (Optional) Change the NSX-T manager default access to use the internal network.

After you have configured access to NSX-T manager via the internal network, you can open the SDDC **Settings** tab and change the **NSX Manager button default access** from **Via the Internet (Public)** to **Via internal network (Private)**. After you make this change, clicking the **OPEN NSX MANAGER** button opens the local NSX-T Manager at its private IP address on the internal network.

Configure AWS Direct Connect Between Your SDDC and On-Premises Data Center

Use of AWS Direct Connect is optional. If traffic between your on-premises network and your SDDC workloads requires higher speeds and lower latency than you can achieve with a connection over the public Internet, configure VMware Cloud on AWS to use AWS Direct Connect.

There are a couple of ways you can configure your VMware Cloud on AWS SDDC to take advantage of AWS Direct Connect for traffic to and from your on-premises datacenter:

Configure Direct Connect to a private VIF in your VPC.

AWS Direct Connect (DX) provides a dedicated network connection between your on-premises network infrastructure and a virtual interface (VIF) in your AWS VPC. A private VIF provides direct private access to your SDDC. Configure DX over a private VIF to carry workload and management traffic, including VPN and vMotion, between your on-premises data center and your connected VPC. A DX connection over a private VIF can be used for all traffic between your on-premises data center and your SDDC. It terminates in your connected Amazon VPC, provides a private IP address space, and uses BGP to advertise routes in your SDDC and learn routes in your on-premise data center. Provisioning procedures for this VIF depend on the type of DX connection you choose.

Associate a Direct Connect Gateway with your SDDC Group's VMware Managed Transit Gateway.

If you have created an SDDC Group in your VMware Cloud on AWS organization, you can connect an on-premises SDDC to that group's Direct Connect Gateway to give it DX connectivity to all members of the SDDC group. See [Attach a Direct Connect Gateway to an SDDC Group](#) in the *VMware Cloud on AWS Operations Guide*.

Access AWS services over a public VIF

If you just want to use DX to access AWS services in a VPC you own, you can do so over a public VIF. You cannot use a public VIF to carry the same kinds of SDDC traffic (such as vMotion) that require a private VIF or Direct Connect Gateway.

Set Up an AWS Direct Connect Connection

To set up an AWS Direct Connect connection, place an order through the AWS console to create a Direct Connect connection in a region where VMware Cloud on AWS is available.

Connection Types

AWS offers three types of Direct Connect connections:

Dedicated Connection

A dedicated connection provides a physical Ethernet port dedicated to a single customer that supports multiple private or public virtual interfaces (VIF) and 1 transit VIF.

To order a dedicated connection, ask a member of the AWS Direct Connect Partner Program to provision a circuit to an AWS Direct Connect location in the same region as your SDDC. Use your (customer-managed) AWS account to make this request. After the circuit has been provisioned, create a hosted private VIF to your SDDC using the account shown in the **AWS Account ID** field of the NSX-T **Direct Connect** page. In an SDDC that is a member of an SDDC group, you can create a Direct Connect Gateway (DXGW) in your account and connect a transit VIF to it from the DXGW. See [Creating and Managing SDDC Deployment Groups with VMware Transit Connect](#).

Hosted Connection

A hosted connection is a circuit shared by multiple customers and provisioned to your AWS account by an AWS Direct Connect Partner. After the circuit has been provisioned, create a hosted private VIF to your SDDC using the account shown in the **AWS Account ID** field of the NSX-T **Direct Connect** page. If your hosted connection speed is 1Gbps or higher and the SDDC that is a member of an SDDC group, you also have the option to create a Direct Connect Gateway (DXGW) in your account, and connect a transit VIF to it from the DXGW. See [Creating and Managing SDDC Deployment Groups with VMware Transit Connect](#).

Hosted VIF

A hosted VIF is similar to a hosted connection but only provides the ability to create a single VIF managed by a partner. The hosted private VIF must be created by the AWS Partner using the account number shown in the **AWS Account ID** field of the NSX-T **Direct Connect** page, rather than provisioned to your own AWS account.

For more information about using Direct Connect with VMware Cloud on AWS, see the VMware Designlet [VMware Cloud on AWS SDDC Connectivity With Direct Connect Private VIF](#). For more information about connection types and how to set them up, see [AWS Direct Connect Partners, Getting Started with AWS Direct Connect](#).

Configure Direct Connect to a Private Virtual Interface for SDDC Management and Compute Network Traffic

Your DX connection requires a private virtual interface to enable vMotion, ESXi Management, Management Appliance, and workload traffic to use it.

Create one private virtual interface (VIF) for each Direct Connect link you want to make to your SDDC. For example, if you want to create two Direct Connect links for redundancy, create two private VIFs in the AWS account linked to your SDDC. See [VMware Configuration Maximums](#) for limits on the number of segments supported by each private VIF.

When you create a private VIF in the **AWS Account ID** shown on the **Direct Connect** page of the **Networking & Security** tab, it can be attached to any of your Organization's SDDCs in the region where you created the VIF. After you attach it to an SDDC, the VIF cannot be detached or reassigned to another SDDC. Instead, it must be deleted and a new VIF created. Deleting an SDDC deletes any attached VIFs.

Important When you connect a DX private virtual interface or a VTGW to an SDDC, all outbound traffic from ESXi hosts to destinations outside the SDDC network is routed over that interface, regardless of other routing configurations in the SDDC. This includes vMotion and vSphere replication traffic. You must ensure that inbound traffic to ESXi hosts is also routed over the DX interface so that the inbound and outbound traffic paths are symmetrical. See [Creating and Managing SDDC Deployment Groups with VMware Transit Connect](#) in the *VMware Cloud on AWS Operations Guide* for more about VMware Transit Connect and the VMware Managed Transit Gateway (VTGW).

Although routes learned from a route-based VPN are advertised over BGP to other route-based VPNs, an SDDC advertises only its own networks over DX, not any learned from VPNs. See [AWS Direct Connect quotas](#) in the *AWS Direct Connect User Guide* for detailed information about limits imposed by AWS on Direct Connect, including limits on routes advertised and learned over BGP.

Prerequisites

- Ensure that you meet the prerequisites for virtual interfaces as described in [Prerequisites for Virtual Interfaces](#).
- If you want to use route-based VPN as the backup to Direct Connect, you'll need a route-based VPN to use. See [Create a Route-Based VPN](#).

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Log in to the AWS Console and complete the *Creating a Hosted Private Virtual Interface* procedure under [Create a Hosted Virtual Interface](#).

If you're using a hosted VIF, work with your AWS Direct Connect Partner to create the VIF in the account shown in the **AWS Account ID** field of the **Direct Connect** page, then skip to [Step 5](#) of this procedure. If you are using a dedicated or hosted connection, take these steps first.

- a For **Virtual interface type**, choose **Private** and make up a **Virtual interface name**.
- b For the **Virtual interface Owner** field, select **Another AWS account** and use the **AWS Account ID** from the NSX-T **Direct Connect** page.
- c For **VLAN**, use the value provided by your AWS Direct Connect Partner.
- d For **BGP ASN**, use the ASN of the on-premises router where this connection terminates.

This value must not be the same as the **BGP Local ASN** shown on the NSX-T **Direct Connect** page.

- e Expand **Additional Settings** and make the following choices:

Address family	Select IPv4
Your router peer ip	Specify the IP address of the on-premises end of this connection (your router), or leave blank to have AWS automatically assign an address that you'll need to configure in your router.
Amazon router peer ip	Specify the IP address of the AWS end of this connection, or leave blank to have AWS automatically assign an address that you'll need to configure in your router.
BGP authentication key	Specify a value or leave blank to have AWS generate a key, which you'll need to configure in your router.
Jumbo MTU (MTU size 9001)	The default MTU for all SDDC networks is 1500 bytes. To enable DX traffic to this private VIF to use a larger MTU, select Enable under Jumbo MTU (MTU size 9001) . After the VIF has been created, you'll also need to open the NSX-T Global Configuration page and set a higher MTU value under Intranet Uplink , as described in Specify the Direct Connect MTU . Enabling this in the connection properties, even if you don't intend to use it right away, makes it easier to take advantage of jumbo frames in SDDC networks when you need them.

When the interface has been created, the AWS console reports that it is ready for acceptance.

- 5 Open **NSX Manager** or the VMC Console **Networking & Security** tab. Click **Direct Connect** and accept the virtual interface by clicking **ATTACH**.

Before it has been accepted, a new VIF is visible in all SDDCs in your organization. After you accept the VIF, it is no longer visible in any other SDDC.

It can take up to 10 minutes for the BGP session to become active. When the connection is ready, the **State** shows as **Attached** and the **BGP Status** as **Up**.

6 (Optional) Configure a route-based VPN as the backup to Direct Connect.


In the default configuration, traffic on any route advertised over BGP by both DX and a route-based VPN uses the VPN by default. To have a route advertised by both DX and VPN use DX by default and failover to the VPN when DX is unavailable click **Direct Connect** and set the **Use VPN as backup to Direct Connect** switch to **Enabled**.

Note This configuration requires a route-based VPN. You cannot use a policy-based VPN as a backup to Direct Connect. In an SDDC that is a member of an SDDC group, traffic over a route that is advertised by both the DX private VIF and the group's VMware Managed Transit Gateway (VTGW) will be routed over the VTGW.

The system requires a minute or so to update your routing preference. When the operation completes, routes advertised by both DX and VPN default to the DX connection, using the VPN only when DX is unavailable. Equivalent routes advertised by both DX and VPN prioritize the VPN connection.

Results

A list of **Advertised BGP Routes** and **Learned BGP Routes** is displayed as the routes are learned

and advertised. Click the refresh icon  to refresh these lists. All routed subnets in the SDDC are advertised as BGP routes, along with this subset of management network subnets:

- Subnet 1 includes routes used by ESXi host vmks and router interfaces.
- Subnet 2 includes routes used for Multi-AZ support and AWS integration.
- Subnet 3 includes management VMs.

Disconnected and extended networks are not advertised.

The actual CIDR blocks advertised depend on your management subnet CIDR block. The following table shows the CIDR blocks for these routes in an SDDC that uses the default management network CIDR of 10.2.0.0 in block sizes /16, /20, and /22.

Table 2-2. Advertised Routes for 10.2.0.0 Default MGW CIDR

MGW CIDR	Subnet 1	Subnet 2	Subnet 3
10.2.0.0/23	10.2.0.0/24	10.2.1.0/26	10.2.1.128/25
10.2.0.0/20	10.2.0.0/21	10.2.8.0/23	10.2.12.0/22
10.2.0.0/16	10.2.0.0/17	10.2.128.0/19	10.2.192.0/18

What to do next

Ensure the vMotion interfaces are configured to use Direct Connect. See [Configure vMotion Interfaces for Use with Direct Connect](#).

Configure vMotion Interfaces for Use with Direct Connect

If you are using a Direct Connect connection between your on-premises data center and your cloud SDDC, you must configure the vMotion interfaces for your on-premises hosts to route vMotion traffic over the Direct Connect connection.

Prerequisites

Configure Direct Connect and create a private virtual interface.

Procedure

- 1 Select one of the following methods to configure the vMotion interface on each host in your on-premises environment.

Option	Description
Override the default gateway (works for vSphere 7.0 hosts only)	For each host, edit the VMkernel adapter used for vMotion traffic, and select the option to override the default gateway. Enter an IP address in your on-premises vMotion subnet that is capable of routing traffic to the on-premises side of the Direct Connect connection. See Edit a VMkernel Adapter Configuration .
Configure the vMotion TCP/IP stack	For each host: <ol style="list-style-type: none"> a Remove any existing vMotion VMkernel adapters. b Create a new VMkernel adapter and select the vMotion TCP/IP stack. See Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host. c Edit the host vMotion TCP/IP stack to change the routing to use an IP address in your on-premises vMotion subnet that is capable of routing traffic to the on-premises side of the Direct Connect connection. See Change the Configuration of a TCP/IP Stack on a Host.

- 2 (Optional) Test connectivity between an on-premises host and a cloud SDDC host using `vmkping`.

See <https://kb.vmware.com/s/article/1003728> for more information.

Configure Direct Connect to a Public Virtual Interface for Access to AWS Services

If your on-premises workloads need access to AWS EC2 instances and services such as S3 over a DX connection, configure a public virtual interface for that traffic in your VPC.

Although SDDC management and workload traffic over DX must use a private VIF or DX Gateway, you can create a DX connection from your on-premises datacenter to a public VIF if you just want to access AWS services from your on-premises workloads or for any purpose that requires a connection to the global AWS backbone.

Prerequisites

- Ensure that you meet the prerequisites for virtual interfaces as described in [Prerequisites for Virtual Interfaces](#).

Procedure

- 1 Log in to the AWS Console, and complete the steps for creating a hosted public virtual interface under [Create a Hosted Virtual Interface](#).
 - a In the **Interface Owner** field, select **My AWS Account**.
 - b Specify **Your router peer IP** and **Amazon router peer IP**.
 - c Select **Auto-generate BGP key** and list any on-premises routes that you want advertised on the AWS backbone in **Prefixes you want to advertise**.

When the interface has been created, the AWS Console reports that it is ready for acceptance.

- 2 Open **NSX Manager** or the VMC Console **Networking & Security** tab. Click **Direct Connect** and accept the virtual interface by clicking **ATTACH**.

Before it has been accepted, a new VIF is visible in all SDDCs in your organization. After you accept the VIF, it is no longer visible in any other SDDC.

It can take up to 10 minutes for the BGP session to become active. When the connection is ready, the **State** shows as **Attached** and the **BGP Status** as **Up**.

Specify the Direct Connect MTU

The default Maximum Transmissible Unit (MTU) for all SDDC networks is 1500 bytes. When you use Direct Connect, you can specify a larger MTU for the traffic it carries.


You can enable DX to use a larger MTU when you create the VIF. If you do this, you'll also need to open the NSX-T **Global Configuration** page and set a higher **Intranet MTU Value**.

This larger (or Jumbo) MTU value applies only to DX connections over a private VIF. Any VPN, whether or not it connects over DX, uses an MTU of 1500, regardless of other settings. You should also verify that the interface MTU of workload VMs that use the DX connection is set to a value that matches the **Intranet MTU Value**. Otherwise, workload VMs won't be able to take advantage of the larger MTU.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 On the **Global Configuration** page, click the pencil icon () , set a higher **MTU** value in the **Intranet Uplink** field, then click **SAVE**.

The value you set must be less than or equal to the smallest MTU value for all your DX virtual interfaces. In practice this means that you should set all your VIFs to the same MTU value (the default, at 1500 or Jumbo, at 9001), since having any VIF that does not support a Jumbo MTU effectively limits all DX connections to an MTU of 1500. Mixing MTU sizes within a network can lead to packet fragmentation and other problems that result in poor network performance.

Note To leave room for Geneve (Generic Network Virtualization Encapsulation) headers, the SDDC intranet MTU is capped at 8900 bytes to avoid packet fragmentation at the VIF.

Configure a VPN Connection Between Your SDDC and On-Premises Data Center

Configure a VPN to provide a secure connection to your SDDC over the public Internet or AWS Direct Connect. Route-based and policy-based IPsec VPNs are supported. Either type of VPN can connect to the SDDC over the Internet. A route-based VPN can also connect to the SDDC over AWS Direct Connect.

You can also configure a Layer 2 VPN, which can be especially useful for workload migration.

For more information about IPsec VPNs, see the VMware Designlet [VMware Cloud on AWS SDDC Connectivity With IPsec VPN](#).

- [Create a Route-Based VPN](#)

A route-based VPN creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created.

- [Create a Policy-Based VPN](#)

A policy-based VPN creates an IPsec tunnel and a policy that specifies how traffic uses it. When you use a policy-based VPN, you must update the routing tables on both ends of the network when new routes are added.

- [Configure a Layer 2 VPN and Extended Network Segment](#)

You can use a VMware Cloud on AWS layer 2 Virtual Private Network (L2VPN) to extend your on-premises network to one or more VLAN-based networks in your SDDC. This extended network is a single subnet with a single broadcast domain. You can use it to migrate VMs to and from your cloud SDDC without having to change their IP addresses.

- [View VPN Tunnel Status and Statistics](#)

Your SDDC NSX-T Manager provides status and statistics for IPsec VPNs and L2VPN segments.

■ IPsec VPN Settings Reference

The on-premises end of any IPsec VPN must be configured to match the settings you specified for the SDDC end of that VPN.

Create a Route-Based VPN

A route-based VPN creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created.

Note This topic explains how to create a route-based VPN that connects to the SDDC's default public or private IP. If you have an SDDC with additional Tier-1 gateways (see [Add a Tier-1 Gateway](#)) you can click **OPEN NSX MANAGER** and add VPN services that terminate on those gateways. See [Adding VPN Services](#) in the *NSX-T Data Center Administration Guide*.

In VMware Cloud on AWS, VPN services to a Tier-1 gateway do not support BGP or Certificate-based authentication.

Route based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic and the Border Gateway Protocol (BGP) to discover and propagate routes as networks are added and removed. To create a route-based VPN, you configure BGP information for the local (SDDC) and remote (on-premises) endpoints, then specify tunnel security parameters for the SDDC end of the tunnel.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 (Optional) Change the default local Autonomous System Number (ASN).

All route-based VPNs in the SDDC default to ASN 65000. The local ASN must be different from the remote ASN. (iBGP, which requires the local and remote ASNs to be the same, is not supported in SDDC networks.) To change the default local ASN, click **EDIT LOCAL ASN**, enter a new value in the range 64521 to 65534 (or 4200000000 to 4294967294) and click **APPLY**.

Note Any change in this value affects all route-based VPNs in this SDDC.

- 5 Click **VPN > Route Based > ADD VPN** and give the new VPN a **Name** and optional **Description**.

6 Select a **Local IP Address** from the drop-down menu.

- If this SDDC is member of an SDDC group or has been configured to use AWS Direct Connect, select the private IP address to have the VPN use that connection rather than a connection over the Internet. Note that VPN traffic over Direct Connect or VMware Managed Transit Gateway (VTGW) is limited to the default MTU of 1500 bytes even if the link supports a higher MTU. See [Configure Direct Connect to a Private Virtual Interface for SDDC Management and Compute Network Traffic](#).
- Select the public IP address if you want the VPN to connect over the Internet.

7 For **Remote Public IP**, enter the address of your on-premises VPN endpoint.

This is the address of the device that initiates or responds to IPsec requests for this VPN. This address must meet the following requirements:

- It must not already be in use for another VPN. VMware Cloud on AWS uses the same public IP for all VPN connections, so only a single VPN connection (Route-based, Policy-based, or L2VPN) can be created to a given remote public IP.
- It must be reachable over the Internet if you specified a public IP in [Step 6](#).
- It must be reachable over VTGW or Direct Connect to a private VIF if you specified a private IP in [Step 6](#).

Default gateway firewall rules allow inbound and outbound traffic over the VPN connection, but you must create firewall rules to manage traffic over the VPN tunnel.

8 For **BGP Local IP/Prefix Length**, enter a network address from a CIDR block of size of /30 within the 169.254.0.0/16 subnet.

Some blocks in this range are reserved, as noted in [Reserved Network Addresses](#). If you can't use a network from the 169.254.0.0/16 subnet (due to a conflict with an existing network), you must create a firewall rule that allows traffic from the BGP service to the subnet you choose here. See [Add or Modify Compute Gateway Firewall Rules](#).

The **BGP Local IP/Prefix Length** specifies both a local subnet and an IP address in it, so the value you enter must be the second or third address in a /30 range and include the /30 suffix. For example, a **BGP Local IP/Prefix Length** of 169.254.32.1/30 creates network 169.254.32.0 and assigns 169.254.32.1 as the local BGP IP (also known as the Virtual Tunnel Interface, or VTI).

9 For **BGP Remote IP**, enter the remaining IP address from the range you specified in [Step 8](#).

For example, if you specified a **BGP Local IP/Prefix Length** of 169.254.32.1/30, use 169.254.32.2 for **BGP Remote IP**. When configuring the on-premises end of this VPN, use the IP address you specify for **BGP Remote IP** as its local BGP IP or VTI address.

10 For **BGP Neighbor ASN**, enter the ASN of your on-premises VPN gateway.

11 Enter the **Preshared Key** string.

The maximum key length is 128 characters. This key must be identical for both ends of the VPN tunnel.

12 Specify the **Remote Private IP**.

Leave this blank to use the **Remote Public IP** as the remote ID for IKE negotiation. If your on-premises VPN gateway is behind a NAT device and/or uses a different IP for its local ID, you need to enter that IP here.

13 Configure the **Advanced Tunnel Parameters**.

Parameter	Value
IKE Profile > IKE Encryption	Select a Phase 1 (IKE) cipher that is supported by your on-premises VPN gateway.
IKE Profile > IKE Digest Algorithm	<p>Select a Phase 1 digest algorithm that is supported by your on-premises VPN gateway. The best practice is to use the same algorithm for both the IKE Digest Algorithm and the Tunnel Digest Algorithm.</p> <p>Note If you specify a GCM-based cipher for IKE Encryption, set IKE Digest Algorithm to None. The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher .</p>
IKE Profile > IKE Version	<ul style="list-style-type: none"> ■ Specify IKE V1 to initiate and accept the IKEv1 protocol. ■ Specify IKE V2 to initiate and accept the IKEv2 protocol. You must use IKEv2 if you have specified a GCM-based IKE Digest Algorithm. ■ Specify IKE FLEX to accept either IKEv1 or IKEv2 and then initiate using IKEv2. If IKEv2 initiation fails, IKE FLEX will not fall back to IKEv1.
IKE Profile > Diffie Hellman	Select a Diffie Hellman group that is supported by your on-premises VPN gateway. This value must be identical for both ends of the VPN tunnel. Higher group numbers offer better protection. The best practice is to select group 14 or higher.
IPSec Profile > Tunnel Encryption	Select a Phase 2 security association (SA) cipher that is supported by your on-premises VPN gateway.
IPSec Profile Tunnel Digest Algorithm	<p>Select a Phase 2 digest algorithm that is supported by your on-premises VPN gateway.</p> <p>Note If you specify a GCM-based cipher for Tunnel Encryption, set Tunnel Digest Algorithm to None. The digest function is integral to the GCM cipher.</p>
IPSec Profile > Perfect Forward Secrecy	Enable or Disable to match the setting of your on-premises VPN gateway. Enabling Perfect Forward Secrecy prevents recorded (past) sessions from being decrypted if the private key is ever compromised.
IPSec Profile > Diffie Hellman	Select a Diffie Hellman group that is supported by your on-premises VPN gateway. This value must be identical for both ends of the VPN tunnel. Higher group numbers offer better protection. The best practice is to select group 14 or higher.

Parameter	Value
DPD Profile > DPD Probe Mode	<p>One of Periodic or On Demand.</p> <p>For a periodic DPD probe mode, a DPD probe is sent every time the specified DPD probe interval time is reached.</p> <p>For an on-demand DPD probe mode, a DPD probe is sent if no IPSec packet is received from the peer site after an idle period. The value in DPD Probe Interval determines the idle period used.</p>
DPD Profile > Retry Count	<p>Integer number of retries allowed. Values in the range 1 - 100 are valid. The default retry count is 10.</p>
DPD Profile > DPD Probe Interval	<p>The number of seconds you want the NSX-T IKE daemon to wait between sending the DPD probes.</p> <p>For a periodic DPD probe mode, the valid values are between 3 and 360 seconds. The default value is 60 seconds.</p> <p>For an on-demand probe mode, the valid values are between 1 and 10 seconds. The default value is 3 seconds.</p> <p>When the periodic DPD probe mode is set, the IKE daemon sends a DPD probe periodically. If the peer site responds within half a second, the next DPD probe is sent after the configured DPD probe interval time has been reached. If the peer site does not respond, then the DPD probe is sent again after waiting for half a second. If the remote peer site continues not to respond, the IKE daemon resends the DPD probe again, until a response is received or the retry count has been reached. Before the peer site is declared to be dead, the IKE daemon resends the DPD probe up to a maximum of times specified in the Retry Count property. After the peer site is declared dead, NSX-T then tears down the security association (SA) on the dead peer's link.</p> <p>When the on-demand DPD mode is set, the DPD probe is sent only if no IPSec traffic is received from the peer site after the configured DPD probe interval time has been reached.</p>
DPD Profile > Admin Status	<p>To enable or disable the DPD profile, click the Admin Status toggle. By default, the value is set to Enabled.</p> <p>When the DPD profile is enabled, the DPD profile is used for all IPSec sessions in the IPSec VPN service that uses the DPD profile.</p>
TCP MSS Clamping	<p>To reduce the maximum segment size (MSS) payload of the TCP session during the IPsec connection, enable TCP MSS Clamping, select the TCP MSS direction value, and optionally set the TCP MSS Value. See Understanding TCP MSS Clamping in the <i>NSX-T Data Center Administration Guide</i>.</p>

- 14 (Optional) Under **Advanced BGP Parameters**, enter a BGP **Secret** that matches the one used by the on-premises gateway.

15 (Optional) Tag the VPN.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

16 Click **SAVE**.**Results**

The VPN creation process might take a few minutes. When the route-based VPN becomes available, the tunnel status and BGP session state are displayed. The following actions are available to help you with troubleshooting and configuring the on-premises end of the VPN:

- Click **DOWNLOAD CONFIG** to download a file that contains VPN configuration details. You can use these details to configure the on-premises end of this VPN.
- Click **VIEW STATISTICS** to view packet traffic statistics for this VPN. See [View VPN Tunnel Status and Statistics](#).
- Click **VIEW ROUTES** to open a display of routes advertised and learned by this VPN.
- Click **DOWNLOAD ROUTES** to download a list of **Advertised Routes** or **Learned Routes** in CSV format.

What to do next

Create or update firewall rules as needed. To allow traffic through the route-based VPN, specify **VPN Tunnel Interface** in the **Applied to** field. The **All Uplinks** option does not include the routed VPN tunnel.

Create a Policy-Based VPN

A policy-based VPN creates an IPsec tunnel and a policy that specifies how traffic uses it. When you use a policy-based VPN, you must update the routing tables on both ends of the network when new routes are added.

Note This topic explains how to create a policy-based VPN that connects to the SDDC's default public or private IP. If you have an SDDC with additional Tier-1 gateways (see [Add a Tier-1 Gateway](#)) you can click **OPEN NSX MANAGER** and add VPN services that terminate on those gateways. See [Adding VPN Services](#) in the *NSX-T Data Center Administration Guide*.

In VMware Cloud on AWS, VPN services to a Tier-1 gateway do not support BGP or Certificate-based authentication.

Policy-based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic. To create a policy-based VPN, you configure the local (SDDC) endpoint, then configure a matching remote (on-premises) endpoint. Because each policy-based VPN must create a new IPsec security association for each network, an administrator must update routing information on premises and in the SDDC whenever a new policy-based VPN is created. A policy-based VPN can be an appropriate choice when you have only a few networks on either end of the VPN, or if your on-premises network hardware does not support BGP (which is required for route-based VPNs).

Important If your SDDC includes both a policy-based VPN and another connection such as a route-based VPN, DX, or VTGW connectivity over the policy-based VPN will fail if any of those other connections advertises the default route (0.0.0.0/0) to the SDDC.

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Click **VPN > Policy Based > ADD VPN** and give the new VPN a **Name** and optional **Description**.
- 5 Select a **Local IP Address** from the drop-down menu.
 - If this SDDC is member of an SDDC group or has been configured to use AWS Direct Connect, select the private IP address to have the VPN use that connection rather than a connection over the Internet. Note that VPN traffic over Direct Connect or VMware Managed Transit Gateway (VTGW) is limited to the default MTU of 1500 bytes even if the link supports a higher MTU. See [Configure Direct Connect to a Private Virtual Interface for SDDC Management and Compute Network Traffic](#).
 - Select the public IP address if you want the VPN to connect over the Internet.
- 6 Enter the **Remote Public IP** address of your on-premises gateway.

The address must not already be in use for another VPN. VMware Cloud on AWS uses the same public IP for all VPN connections, so only a single VPN connection (Route-based, Policy-based, or L2VPN) can be created to a given remote public IP. This address must be reachable over the Internet if you specified a public IP in [Step 5](#). If you specified a private IP, it must be reachable over Direct Connect to a private VIF. Default gateway firewall rules allow inbound and outbound traffic over the VPN connection, but you must create firewall rules to manage traffic over the VPN tunnel.

- 7 Specify the **Remote Networks** that this VPN can connect to.

This list must include all networks defined as local by the on-premises VPN gateway. Enter each network in CIDR format, separating multiple CIDR blocks with commas.

8 Specify the **Local Networks** that this VPN can connect to.

This list includes all routed compute networks in the SDDC, as well as the entire Management network and the appliance subnet (a subset of the Management network that includes vCenter and other management appliances, but not the ESXi hosts). It also includes the CGW DNS Network, a single IP address used to source requests forwarded by the CGW DNS service.

9 Enter the **Preshared Key** string.

The maximum key length is 128 characters. This key must be identical for both ends of the VPN tunnel.

10 (Optional) If your on-premises gateway is behind a NAT device, enter the gateway address as the **Remote Private IP**.

This IP address must match the local identity (IKE ID) sent by the on-premises VPN gateway. If this field is empty, the **Remote Public IP** field is used to match the local identity of the on-premises VPN gateway.

11 Configure the **Advanced Tunnel Parameters**.

Parameter	Value
IKE Profile > IKE Encryption	Select a Phase 1 (IKE) cipher that is supported by your on-premises VPN gateway.
IKE Profile > IKE Digest Algorithm	<p>Select a Phase 1 digest algorithm that is supported by your on-premises VPN gateway. The best practice is to use the same algorithm for both the IKE Digest Algorithm and the Tunnel Digest Algorithm.</p> <p>Note If you specify a GCM-based cipher for IKE Encryption, set IKE Digest Algorithm to None. The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher .</p>
IKE Profile > IKE Version	<ul style="list-style-type: none"> ■ Specify IKE V1 to initiate and accept the IKEv1 protocol. ■ Specify IKE V2 to initiate and accept the IKEv2 protocol. You must use IKEv2 if you have specified a GCM-based IKE Digest Algorithm. ■ Specify IKE FLEX to accept either IKEv1 or IKEv2 and then initiate using IKEv2. If IKEv2 initiation fails, IKE FLEX will not fall back to IKEv1.
IKE Profile > Diffie Hellman	Select a Diffie Hellman group that is supported by your on-premises VPN gateway. This value must be identical for both ends of the VPN tunnel. Higher group numbers offer better protection. The best practice is to select group 14 or higher.
IPSec Profile > Tunnel Encryption	Select a Phase 2 security association (SA) cipher that is supported by your on-premises VPN gateway.

Parameter	Value
IPSec Profile Tunnel Digest Algorithm	<p>Select a Phase 2 digest algorithm that is supported by your on-premises VPN gateway.</p> <p>Note If you specify a GCM-based cipher for Tunnel Encryption, set Tunnel Digest Algorithm to None. The digest function is integral to the GCM cipher.</p>
IPSec Profile > Perfect Forward Secrecy	<p>Enable or Disable to match the setting of your on-premises VPN gateway. Enabling Perfect Forward Secrecy prevents recorded (past) sessions from being decrypted if the private key is ever compromised.</p>
IPSec Profile > Diffie Hellman	<p>Select a Diffie Hellman group that is supported by your on-premises VPN gateway. This value must be identical for both ends of the VPN tunnel. Higher group numbers offer better protection. The best practice is to select group 14 or higher.</p>
DPD Profile > DPD Probe Mode	<p>One of Periodic or On Demand.</p> <p>For a periodic DPD probe mode, a DPD probe is sent every time the specified DPD probe interval time is reached.</p> <p>For an on-demand DPD probe mode, a DPD probe is sent if no IPSec packet is received from the peer site after an idle period. The value in DPD Probe Interval determines the idle period used.</p>
DPD Profile > Retry Count	<p>Integer number of retries allowed. Values in the range 1 - 100 are valid. The default retry count is 10.</p>

Parameter	Value
DPD Profile > DPD Probe Interval	<p>The number of seconds you want the NSX-T IKE daemon to wait between sending the DPD probes.</p> <p>For a periodic DPD probe mode, the valid values are between 3 and 360 seconds. The default value is 60 seconds.</p> <p>For an on-demand probe mode, the valid values are between 1 and 10 seconds. The default value is 3 seconds.</p> <p>When the periodic DPD probe mode is set, the IKE daemon sends a DPD probe periodically. If the peer site responds within half a second, the next DPD probe is sent after the configured DPD probe interval time has been reached. If the peer site does not respond, then the DPD probe is sent again after waiting for half a second. If the remote peer site continues not to respond, the IKE daemon resends the DPD probe again, until a response is received or the retry count has been reached. Before the peer site is declared to be dead, the IKE daemon resends the DPD probe up to a maximum of times specified in the Retry Count property. After the peer site is declared dead, NSX-T then tears down the security association (SA) on the dead peer's link.</p> <p>When the on-demand DPD mode is set, the DPD probe is sent only if no IPSec traffic is received from the peer site after the configured DPD probe interval time has been reached.</p>
DPD Profile > Admin Status	<p>To enable or disable the DPD profile, click the Admin Status toggle. By default, the value is set to Enabled.</p> <p>When the DPD profile is enabled, the DPD profile is used for all IPSec sessions in the IPSec VPN service that uses the DPD profile.</p>
TCP MSS Clamping	<p>To reduce the maximum segment size (MSS) payload of the TCP session during the IPsec connection, enable TCP MSS Clamping, select the TCP MSS direction value, and optionally set the TCP MSS Value. See Understanding TCP MSS Clamping in the <i>NSX-T Data Center Administration Guide</i>.</p>

12 (Optional) Tag the VPN.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

13 Click **SAVE**.

Results

The VPN creation process might take a few minutes. When the policy-based VPN becomes available, the following actions are available to help you with troubleshooting and configuring the on-premises end of the VPN:

- Click **DOWNLOAD CONFIG** to download a file that contains VPN configuration details. You can use these details to configure the on-premises end of this VPN.
- Click **VIEW STATISTICS** to view packet traffic statistics for this VPN. See [View VPN Tunnel Status and Statistics](#).

What to do next

Create or update firewall rules as needed. To allow traffic through the policy-based VPN, specify **Internet Interface** in the **Applied to** field.

Configure a Layer 2 VPN and Extended Network Segment

You can use a VMware Cloud on AWS layer 2 Virtual Private Network (L2VPN) to extend your on-premises network to one or more VLAN-based networks in your SDDC. This extended network is a single subnet with a single broadcast domain. You can use it to migrate VMs to and from your cloud SDDC without having to change their IP addresses.

In addition to data center migration, you can use an extended L2VPN network for disaster recovery, or for dynamic access to cloud computing resources as needed (often referred to as "cloud bursting").

VMware Cloud on AWS uses NSX-T to provide the L2VPN server in your cloud SDDC. L2VPN client functions are provided by an on-premises NSX Edge. See [VMware Configuration Maximums](#) for L2VPN limits.

The VMware Cloud on AWS L2VPN feature supports extending VLAN networks. The L2VPN connection to the NSX-T server uses an IPsec tunnel. The L2VPN extended network is used to extend Virtual Machine networks and carries only workload traffic. It is independent of the VMkernel networks used for migration traffic (ESXi management or vMotion), which use either a separate IPsec VPN or a Direct Connect connection.

Important You cannot bring up an L2VPN tunnel until you have configured the L2VPN client and server and created an extended network that specifies the tunnel ID you assigned to the client.

Procedure

1 [Configure a Layer 2 VPN Tunnel in the SDDC](#)

Specify local (SDDC) and remote (on-premises) IP addresses to create the SDDC end of the Layer 2 VPN tunnel.

2 Configure an Extended Segment for the Layer 2 VPN

Extended networks require a layer 2 Virtual Private Network (L2VPN), which provides a secure communications tunnel between an on-premises network and one in your cloud SDDC.

3 Install and Configure the On-Premises NSX Edge

The on-premises end of your L2VPN must be an NSX Edge appliance. You must configure this appliance and related on-premises vSphere networking before you can create an L2VPN.

Configure a Layer 2 VPN Tunnel in the SDDC

Specify local (SDDC) and remote (on-premises) IP addresses to create the SDDC end of the Layer 2 VPN tunnel.

Note This topic explains how to create a Layer 2 VPN that connects to the SDDC's default public or private IP. If you have an SDDC with additional Tier-1 gateways (see [Add a Tier-1 Gateway](#)) you can click **OPEN NSX MANAGER** and add VPN services that terminate on those gateways. See [Adding VPN Services](#) in the *NSX-T Data Center Administration Guide*.

VMware Cloud on AWS supports a single Layer 2 VPN tunnel between your on-premises installation and your SDDC.

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Click **VPN > Layer 2**.
- 5 Click **ADD VPN TUNNEL**.

6 Configure the VPN parameters.

Option	Description
Local IP Address	<ul style="list-style-type: none"> ■ Select the private IP address if you have configured AWS Direct Connect for this SDDC and want the VPN to use it. See Configure Direct Connect to a Private Virtual Interface for SDDC Management and Compute Network Traffic. ■ Select the public IP address if you want the VPN to connect to the SDDC over Internet.
Remote Public IP	Enter the remote public IP address of your on-premise L2VPN gateway. For an L2VPN, this is always the standalone NSX Edge appliance (see Install and Configure the On-Premises NSX Edge).
Remote Private IP	Enter the remote private IP address if the on-premise gateway is configured behind NAT.

Note To reduce the maximum segment size (MSS), TCP TMSS clamping is always enabled for Layer 2 VPNs in SDDC version 1.15 and later.

7 (Optional) Tag the VPN.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

8 (Optional) Add a **Description**.

9 Click **SAVE**.

Depending on your SDDC environment, the Layer 2 VPN creation process might take a few minutes. When the Layer 2 VPN tunnel becomes available, the status changes to Up.

Configure an Extended Segment for the Layer 2 VPN

Extended networks require a layer 2 Virtual Private Network (L2VPN), which provides a secure communications tunnel between an on-premises network and one in your cloud SDDC.

Each end of this tunnel has an ID. When the tunnel ID matches on the cloud SDDC and the on-premises side of the tunnel, the two networks become part of the same broadcast domain. Extended networks use an on-premises gateway as the default gateway. Other network services such as DHCP and DNS are also provided on-premises.

You can change a logical network from routed to extended or from extended to routed. For example, you might configure a logical network as extended to allow migration of VMs from your on-premises data center to your cloud SDDC. When the migration is complete, you might then change the network to routed to allow the VMs to use VMware Cloud on AWS networking services.

Prerequisites

Verify that Layer 2 VPN tunnel is available. See [Configure a Layer 2 VPN Tunnel in the SDDC](#).

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.
 You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.
- 4 Follow the procedure in [Create or Modify a Network Segment](#) to create an Extended segment bound to the Tunnel ID of the L2VPN tunnel.
- 5 Click **SAVE**.
- 6 Click **DOWNLOAD CONFIG** to download a file containing the peer code and other information you'll need when configuring the on-premises of the remote side VPN configuration.
- 7 Configure the client side of the L2VPN.

See [Install and Configure the On-Premises NSX Edge](#).

Install and Configure the On-Premises NSX Edge

The on-premises end of your L2VPN must be an NSX Edge appliance. You must configure this appliance and related on-premises vSphere networking before you can create an L2VPN.

If you have a compatible version of NSX-T installed in your on-premises data center, you can use your existing NSX Edge appliance as the on-premises (client) side of an L2VPN that connects to your SDDC. If necessary, you can download and deploy a standalone NSX Edge to use as the L2VPN client. The following table lists compatible SDDC and on-premises versions. To determine the version of NSX-T running in your SDDC, see [Correlating VMware Cloud on AWS with Component Releases](#) in the *VMware Cloud on AWS Operations Guide*.

Table 2-3. L2VPN Interoperability

L2VPN Server Version (SDDC)	L2VPN Client Version (On-Premises Edge)
3.1.3	3.1.3, 3.1.2
3.1.2	3.1.2, 3.1.1, 2.5.3
3.1.1	3.1.1, 3.1.0, 3.0.1
3.1.0	3.1.1, 3.0.1, 3.0.0
3.0.3	3.0.3, 3.0.2, 3.0.1
3.0.2	3.0.2, 3.0.1, 2.5.2
3.0.0	3.0.0, 2.5.0, 2.5.1

Procedure

1 (Optional) Download the standalone NSX Edge.

If you do not have a compatible version of NSX-T installed in your on-premises data center, you may be able to download and configure a standalone NSX Edge appliance to use as the on-premises endpoint for your L2VPN. After you configure the server side of the L2VPN, follow the instructions on the **Remote L2 VPN Client Configuration** page to download the **NSX Edge for VMware ESXi** as an OVF file.

2 Install and configure the NSX Edge.

See [Add an Autonomous Edge as an L2 VPN Client](#) in the *NSX-T Data Center Administration Guide* for information about how to install and configure the Autonomous Edge in your on-premises vCenter Server.

View VPN Tunnel Status and Statistics

Your SDDC NSX-T Manager provides status and statistics for IPsec VPNs and L2VPN segments.

Status of VPN operations is reported on the **VPN** pages in the **Networking & Security** tab. Log messages about VPN operations are also sent to vRealize Log Insight Cloud, an optional SDDC add-on service. See [Using the vRealize Log Insight Cloud Add-On](#) and the [vRealize Log Insight Cloud Documentation](#) for more information.

Procedure

1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.


2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.


3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

4 On the **VPN** page, click **Route Based**, **Policy Based**, or **Layer 2** to list VPNs of the selected type.

Take one of the following actions:

- Click the Information icon  to display a status message that provides more information about channel (IKE Phase 1 negotiation) and tunnel status.
- Expand a row to show VPN details, then click **VIEW STATISTICS** to display traffic statistics. You can retrieve aggregated status and statistics for all tunnels or for the tunnel used by the selected VPN (0.0.0.0/0). When viewing aggregated statistics, you can click **View More** in the **Stats** column to see a list of error statistics.

- Click the Refresh icon  to refresh tunnel statistics. All VPN statistics are reset to 0 when the tunnel is disabled or re-enabled.

What to do next

For more information about troubleshooting VPN connection issues, see [Troubleshooting Virtual Private Networks \(VPN\)](#) in the *NSX-T Data Center Administration Guide*.

IPsec VPN Settings Reference

The on-premises end of any IPsec VPN must be configured to match the settings you specified for the SDDC end of that VPN.

Information in the following tables summarizes the available SDDC IPsec VPN settings. Some of the settings can be configured. Some are static. Use this information to verify that your on-premises VPN solution can be configured to match the one in your SDDC. Choose an on-premises VPN solution that supports all the static settings and any of the configurable settings listed in these tables.

Understanding how Diffie-Hellman Groups Affect IPsec VPN Performance and Security

IPsec VPN configuration requires you to choose a Diffie-Hellman (DH) group, which is used in both phases of the IKE negotiation to securely communicate private keys between endpoints over an untrusted path. DH Groups 19-21 represent a significant increase in security over groups 14-16 and consume fewer resources during encryption. The NIST [Guide to IPsec VPNs](#) (PDF) provides considerably more detail on these and other IPsec VPN configuration choices.

Note DH Groups 2 and 5 are not NIST-approved, and should be used only when required for compatibility with an older on-premises device.

As a best practice, configurable settings should be the same for both phases.

Phase 1 (IKE Profile) IPsec VPN Settings

Table 2-4. Configurable Settings

Attribute	Allowed Values	Recommended Value
Protocol	IKEv1, IKEv2, IKE FLEX	IKEv2
Encryption Algorithm	AES (128, 256), AES-GCM (128, 192, 256)	AES GCM Encryption with higher bit depths is harder to crack but creates more load on your endpoint device.

Table 2-4. Configurable Settings (continued)

Attribute	Allowed Values	Recommended Value
Tunnel/IKE Digest Algorithm	SHA1, SHA2 (256, 384, 512)	If you specify a GCM-based cipher for IKE Encryption , set IKE Digest Algorithm to None . The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher
Diffie Hellman	DH Groups 2, 5, 14-16, 19-21	DH Groups 19-21 or 14-16

Table 2-5. Static Settings

Attribute	Value
ISAKMP mode	Main mode (Disable aggressive mode)
ISAKMP/IKE SA lifetime	86400 seconds (24 hours)
IPsec Mode	Tunnel
IKE Authentication	Pre-Shared Key

Phase 2 (IPsec Profile) IPsec VPN Settings

Configurable settings are the same for Phase 1 and Phase 2.

Table 2-6. Configurable Settings

Attribute	Allowed Values	Recommended Value
Protocol	IKEv1, IKEv2, IKE FLEX	IKEv2
Encryption Algorithm	AES (128, 256), AES-GCM (128, 192, 256)	AES GCM Encryption with higher bit depths is harder to crack but creates more load on your endpoint device.
Tunnel/IKE Digest Algorithm	SHA-1, SHA2 (256, 384, 512)	If you specify a GCM-based cipher for IKE Encryption , set IKE Digest Algorithm to None . The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher
Diffie Hellman	DH Groups 2, 5, 14-16, 19-21	DH Groups 19-21 or 14-16

Table 2-7. Static Settings

Attribute	Value
Tunnel Mode	Encapsulating Security Payload (ESP)
SA lifetime	3600 seconds (one hour)

On-Premises IPsec VPN Configuration

Click **DOWNLOAD CONFIG** on the status page of any VPN to download a file that contains VPN configuration details. You can use these details to configure the on-premises end of the VPN.

Note Do not configure the on-premises side of a VPN to have an idle timeout (for example, the NSX **Session idle timeout** setting). On-premises idle timeouts can cause the VPN to become periodically disconnected.

The VMware Tech Zone [IPSec VPN Configuration Reference](#) provides detailed endpoint configuration advice, and sample configuration files for several popular endpoint devices are available on VMware {code}.

■ [Palo Alto Networks Firewall](#)

Configure Management Gateway Networking and Security

The management network and Management Gateway are largely preconfigured in your SDDC, but you'll still need to configure access to management network services like vCenter and HCX and create management gateway firewall rules to allow traffic between the management network and other networks, including your on-premises networks and other SDDC networks.

Procedure

1 [Set vCenter Server FQDN Resolution Address](#)

You can connect to the SDDC vCenter Server at either a public or private IP address. A private IP address can be resolved from an SDDC VPN. A public IP address can be resolved from the Internet.

2 [Set HCX FQDN Resolution Address](#)

You can connect to VMware HCX at either a public or private IP address. A private IP address can be resolved from an SDDC VPN. A public IP address can be resolved from the internet.

3 [Add or Modify Management Gateway Firewall Rules](#)

Maintaining the safety and security of your SDDC management infrastructure is critical. By default, the management gateway blocks traffic to all management network destinations from all sources. You must add management gateway firewall rules to allow secure traffic from trusted sources.

Set vCenter Server FQDN Resolution Address

You can connect to the SDDC vCenter Server at either a public or private IP address. A private IP address can be resolved from an SDDC VPN. A public IP address can be resolved from the Internet.

Prerequisites

Before you can access the SDDC vCenter Server at a private IP address, you'll need to set up a VPN connecting your SDDC to your on-premises datacenter. See [Create a Route-Based VPN](#) or [Create a Policy-Based VPN](#).

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Navigate to the **Settings** tab of your SDDC.
- 4 Expand **vCenter FQDN**, and click **Edit**.
- 5 Under **Resolution Address** Select either the **Public IP** address or the **Private IP** address and click **SAVE**.

Set HCX FQDN Resolution Address

You can connect to VMware HCX at either a public or private IP address. A private IP address can be resolved from an SDDC VPN. A public IP address can be resolved from the internet.

Prerequisites

Before you can access HCX at a private IP address, you'll need to set up a VPN connecting your SDDC to your on-premises datacenter. See [Create a Route-Based VPN](#) or [Create a Policy-Based VPN](#).

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Navigate to the **Settings** tab of your SDDC.
- 4 Expand **HCX FQDN**, and click **Edit**.
- 5 Under **Resolution Address** select either the **Public IP** address or the **Private IP** address and click **SAVE**.

Add or Modify Management Gateway Firewall Rules

Maintaining the safety and security of your SDDC management infrastructure is critical. By default, the management gateway blocks traffic to all management network destinations from all sources. You must add management gateway firewall rules to allow secure traffic from trusted sources.

When configuring access to the SDDC management infrastructure, it's critical that you evaluate the available connectivity options, configure the ones you need, and create management gateway firewall rules that prevent unauthorized access to the SDDC management network.

- [Configure AWS Direct Connect Between Your SDDC and On-Premises Data Center](#)

This option provides dedicated connectivity between your enterprise and the SDDC and can be used in conjunction with an IPsec VPN to encrypt traffic.

- [Configure a VPN Connection Between Your SDDC and On-Premises Data Center](#)

This option provides encrypted connectivity between your enterprise and the SDDC.

- If you can't use Direct Connect or a VPN, you can access the SDDC management network over the public internet and rely on management gateway firewall rules to prevent access by untrusted sources. This option may be appropriate for some use cases but is inherently less secure than the others.

Management Gateway firewall rules specify actions to take on network traffic from a specified source to a specified destination. Either the source or destination must be a system-defined inventory group. See [Add a Management Group](#) for information about viewing or modifying inventory groups.

Important If you must access the Management Gateway over the public Internet, it's critical to configure a management gateway firewall rule that allows traffic only from IP addresses you own or trust. For example, an enterprise that accesses the internet from an address in the CIDR block 93.184.216.34/30 should create a management gateway firewall rule that allows only traffic with a **Sources** CIDR of 93.184.216.34/30 to access the management systems including vCenter Server, ESXi, and NSX-T. Never configure a management gateway firewall rule to allow traffic originating from **Any** address. See VMware Knowledge Base article [84154](#) for more information about providing secure access to your SDDC management infrastructure.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 On the **Gateway Firewall** card, click **Management Gateway**, then click **ADD RULE** and give the new rule a **Name**.

5 Enter the parameters for the new rule.

Parameters are initialized to their default values (for example, **All** for **Sources** and **Destinations**). To edit a parameter, move the mouse cursor over the parameter value and click the pencil icon (✎) to open a parameter-specific editor.

Option	Description
Sources	<p>Select Any to allow traffic from any source address or address range.</p> <hr/> <p>Important Although you can select Any as the source address in a firewall rule, using Any as the source address in this firewall rule can enable attacks on your vCenter Server and may lead to compromise of your SDDC. As a best practice, configure this firewall rule to allow access only from trusted source addresses. See VMware Knowledge Base article 84154.</p> <hr/> <p>Select System Defined Groups and select one of the following source options:</p> <ul style="list-style-type: none"> ■ ESXi to allow traffic from your SDDC's ESXi hosts. ■ NSX Manager to allow traffic from your SDDC's NSX-T appliance. ■ vCenter to allow traffic from your SDDC's vCenter Server. <p>Select User Defined Groups to use a management group that you have defined. See Add a Management Group.</p>
Destinations	<p>Select Any to allow traffic to any destination address or address range.</p> <p>Select System Defined Groups and select one of the following destination options:</p> <ul style="list-style-type: none"> ■ ESXi to allow traffic to your SDDC's ESXi management. ■ NSX Manager to allow traffic to your SDDC's NSX-T appliance ■ vCenter to allow traffic to your SDDC's vCenter Server.
Services	Select the service types that the rule applies to. The list of service types depends on your choices for Sources and Destinations .
Action	The only action available for a new management gateway firewall rule is Allow .

The new rule is enabled by default. Slide the toggle to the left to disable it.

6 Click **PUBLISH** to create the rule.

The system gives the new rule an integer **ID** value, which is used in log entries generated by the rule.

Firewall rules are applied in order from top to bottom. Because there is a default **Drop** rule at the bottom and the rules above are always **Allow** rules, management gateway firewall rule order has no impact on traffic flow.

Example: Create a Management Gateway Firewall Rule

To create a management gateway firewall rule that enables vMotion traffic from the on-premises ESXi hosts to the ESXi hosts in the SDDC:

- 1 Create a management inventory group that contains the on-premises ESXi hosts that you want to enable for vMotion to the SDDC.

- 2 Create a management gateway rule with source ESXi and destination on-premises ESXi hosts.
- 3 Create another management gateway rule with source on-premises ESXi hosts group and destination ESXi with a vMotion service.

What to do next

You can take any or all of these optional actions with an existing firewall rule.



- Click the gear icon  to view or modify rule logging settings. Log entries are sent to the VMwarevRealize Log Insight Cloud Service. See [Using vRealize Log Insight Cloud](#) in the *VMware Cloud on AWS Operations Guide*.
- Click the graph icon  to view Rule Hits and Flow statistics for the rule.

Table 2-8. Rule Hits Statistics

Popularity Index	Number of times the rule was triggered in the past 24 hours.
Hit Count	Number of times the rule was triggered since it was created.

Table 2-9. Flow Statistics

Packet Count	Total packet flow through this rule.
Byte Count	Total byte flow through this rule.

Statistics start accumulating as soon as the rule is enabled.

Example Management Gateway Firewall Rules

Some common firewall rule configurations include opening access to the vSphere Client from the internet, allowing access to vCenter Server through the management VPN tunnel, and allowing remote console access.

Commonly Used Firewall Rules

The following table shows the Service, Source, and Destination settings for commonly-used firewall rules.

Table 2-10. Commonly-Used Firewall Rules

Use Cases	Service	Source	Destination
Provide access to vCenter Server from the internet. Use for general vSphere Client access as well as for monitoring vCenter Server	HTTPS	IP address or CIDR block from on-premises data center Important Although you can select Any as the source address in a firewall rule, using Any as the source address in this firewall rule can enable attacks on your vCenter Server and may lead to compromise of your SDDC. As a best practice, configure this firewall rule to allow access only from trusted source addresses. See VMware Knowledge Base article 84154 .	vCenter
Provide access to vCenter Server over VPN tunnel. Required for Management Gateway VPN, Hybrid Linked Mode, Content Library.	HTTPS	IP address or CIDR block from on-premises data center	vCenter
Provide access from cloud vCenter Server to on-premises services such as Active Directory, Platform Services Controller, and Content Library.	Any	vCenter	IP address or CIDR block from on-premises data center.
Provisioning operations involving network file copy traffic, such as cold migration, cloning from on-premises VMs, snapshot migration, replication, and so on.	Provisioning	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel	ESXi Management
VMRC remote console access Required for vRealize Automation	Remote Console	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel	ESXi Management
vMotion traffic over VPN	Any	ESXi Management	IP address or CIDR block from on-premises data center

Configure Compute Gateway Networking and Security

Compute Gateway networking includes a compute network with one or more segments and the DNS, DHCP, and security (gateway firewall and distributed firewall) configurations that manage network traffic for workload VMs. It can also include a layer 2 VPN and extended network that provides a single broadcast domain that spans your on-premises network and your SDDC workload network.

Procedure

1 [Create or Modify a Network Segment](#)

Network segments are logical networks for use by workload VMs in the SDDC compute network.

2 [Add or Modify Compute Gateway Firewall Rules](#)

By default, the Compute Gateway blocks traffic to all uplinks. Add Compute Gateway firewall rules to allow traffic as needed.

3 [Add or Modify Distributed Firewall Rules](#)

Distributed firewall rules apply at the VM (vNIC) level and control East-West traffic within the SDDC.

4 [Configure DNS Services](#)

VMware Cloud on AWS DNS forwarding services run in DNS zones, and enable workload VMs in the zone to resolve fully-qualified domain names to IP addresses.

5 [View Routes Learned and Advertised over VMware Transit Connect](#)

In an SDDC that is a member of an SDDC Group, you can use the **Networking & Security Transit Connect** tool to view routes learned and advertised by this SDDC in the VMware Transit Connect network created for the group.

6 [View Statistics and Manage Settings for Uplinks](#)

The **Global Configuration** page includes controls that allow you to view traffic statistics and manage Maximum Transmissible Unit (MTU) and Unicast Reverse Path Forwarding (URPF) settings for SDDC network uplinks.

Create or Modify a Network Segment

Network segments are logical networks for use by workload VMs in the SDDC compute network.

VMware Cloud on AWS supports three types of network segments: routed, extended and disconnected.

- A routed network segment (the default type) has connectivity to other logical networks in the SDDC and, through the SDDC firewall, to external networks.
- An extended network segment extends an existing L2VPN tunnel, providing a single IP address space that spans the SDDC and an on-premises network.

- A disconnected network segment has no uplink, and provides an isolated network accessible only to VMs connected to it. Disconnected segments are created when needed by VMware HCX (see [Getting started with VMware HCX](#)). You can also create them yourself, and can convert them to other segment types.

See [VMware Configuration Maximums](#) for limits on segments per SDDC and network connections per segment.

A Single Host Starter SDDC is created with a single routed network segment named `sddc-cgw-network-1`. Multi-host SDDCs are created without a default network segment, so you must create at least one for your workload VMs. When you create a segment, you start by configuring some basic parameters and specifying how DHCP requests are handled on the segment. After the segment has been created, you can take additional, optional steps to specify a segment profiles and create DHCP static bindings.


Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **Segments** page.

To create a new segment, click **ADD SEGMENT** and give the new segment a **Name** and optional **Description**.

To delete or modify a segment, click its  button and choose **Edit**. You can modify all segment properties, including segment type. You can also edit or delete the segment's DHCP configuration.

Important You cannot disable or delete a segment of any type if it has attached VMs or VIFs. Disconnect attached VMs and VIFs before deleting the segment.

- 5 Specify a segment type and connected gateway in the **Connected Gateway** drop-down, then fill in the required configuration parameters.

In the default configuration, only the Compute Gateway can be selected as the **Connected Gateway**. See [Add a Tier-1 Gateway](#) for information about creating additional Tier-1 gateways in your SDDC. Networks configured on segments connected to a secondary Tier-1 gateway will not be advertised to Direct Connect, SDDC Group (VTGW) or ESXi management hosts by default. To establish that connectivity, define a route aggregation that includes those networks

Parameter requirements depend on the segment type.

Table 2-11. Routed Segment Configuration Parameters

Parameter	Value
VPN Tunnel ID	N/A for Routed or Disconnected segment types.
Subnets	Specify an IPv4 CIDR block for the segment. The block must not overlap your management network, any of the CIDR blocks listed in Reserved Network Addresses , or any of the subnets in your connected Amazon VPC. If any part of the block is in a public IP space, it must be in one that has been allocated for your use by IANA or another regional internet registry.
URPF Mode	Choose Strict to apply Unicast Reverse Path Forwarding (URPF) strict mode, as defined by RFC3704 or None to disable URPF for this subnet.
SET DHCP CONFIG	Routed segments default to using the Compute Gateway DHCP server. Per-segment DHCP configuration, including DHCP relay, can be specified when you create or update the segment. See Configure Segment DHCP Properties .
Domain Name	(Optional) Enter a fully qualified domain name. Static bindings on the segment automatically inherit this domain name.
Tags	See Add Tags to an Object in the <i>NSX-T Data Center Administration Guide</i> for more information about tagging NSX-T objects.

Table 2-12. Extended Segment Configuration Parameters

Parameter	Value
VPN Tunnel ID	Specify the tunnel ID of an existing L2VPN tunnel. N/A for Routed or Disconnected segment types. If you have not already created an L2VPN, see Configure a Layer 2 VPN Tunnel in the SDDC .
Subnets	N/A for Extended segments.
URPF Mode	Choose Strict to apply Unicast Reverse Path Forwarding (URPF) strict mode, as defined by RFC3704 or None to disable URPF for this subnet.
Domain Name	(Optional) Enter a fully qualified domain name. Static bindings on the segment automatically inherit this domain name.
Tags	See Add Tags to an Object in the <i>NSX-T Data Center Administration Guide</i> for more information about tagging NSX-T objects.


Table 2-13. Disconnected Segment Configuration Parameters

Parameter	Value
VPN Tunnel ID	N/A for Routed or Disconnected segment types.
Subnets	Specify an IPv4 CIDR block for the segment. The block must not overlap your management network, any of the CIDR blocks listed in Reserved Network Addresses , or any of the subnets in your connected Amazon VPC. If any part of the block is in a public IP space, it must be in one that has been allocated for your use by IANA or another regional internet registry.
Domain Name	(Optional) Enter a fully qualified domain name. Static bindings on the segment automatically inherit this domain name.
URPF Mode	Choose Strict to apply Unicast Reverse Path Forwarding (URPF) strict mode, as defined by RFC3704 or None to disable URPF for this subnet.
Tags	See Add Tags to an Object in the <i>NSX-T Data Center Administration Guide</i> for more information about tagging NSX-T objects.

6 Click **SAVE** to create or update the segment.

Click **YES** if you want continue with segment configuration. If you click **NO**, you can edit the segment later if you need to.

The system creates the requested segment. This operation can take up to 15 seconds to complete. When the segment **Status** transitions to **Up** the segment is ready for use. If the

segment **Status** is **Down**, you can click the information icon  for more information about the cause of the problem.

7 (Optional) Click **SEGMENT PROFILES** to view profiles for the segment.

Every segment has a read-only profile that specifies how it handles IP discovery, MAC discovery, and related security controls. Key settings include:

- Promiscuous mode is not supported.
- MAC Learning is disabled. Only a single MAC address can be used on a NIC connected to the segment.
- BPDU filtering is enabled.
- IP address discovery (which affects the IPs added to groups using dynamic membership) is set to Trust on First Use. Detection uses ARP and DHCP snooping, as well as VMware Tools. See [Understanding IP Discovery Segment Profile](#) in the *NSX-T Data Center Administration Guide*.

8 (Optional) Configure **DHCP STATIC BINDINGS**.

- a Click **Set** to specify static bindings for VMs on the segment.

Click **ADD IPV4 STATIC BINDING**, then give the binding a **Name** and specify an IPv4 address included in the segment and a MAC address. When a VM with the specified MAC address is powered on and connected to the segment, it receives the specified address. Click **SAVE** to create the binding, then add another binding or click **APPLY** to apply the specified static bindings to the segment.

- b Click **DHCP Options** to specify DHCP Classless Static Routes (Option 121) and Generic Options.
 - Each classless static route option in DHCP for IPv4 can have multiple routes with the same destination. Each route includes a destination subnet, subnet mask, next hop router. See [RFC 3442](#) for information about classless static routes in DHCPv4. You can add a maximum of 127 classless static routes on a DHCPv4 server.
 - For adding Generic Options, select the code of the option and enter a value of the option. For binary values, the value must be in a base-64 encoded format.

What to do next

After a segment has been created and has a status of Success, you can click **VIEW STATISTICS** to view statistics for network traffic to and from the segment. You can click **VIEW RELATED GROUPS** to see a list of groups that include this segment. For more information, see [Add a Group](#) in the *NSX-T Data Center Administration Guide*.


Configure Segment DHCP Properties

DHCP configuration is a per-segment property. In the default configuration the Compute Gateway DHCP server handles DHCP requests from VMs on all routed segments. To use another DHCP server for your workload networks, you can configure the segment to use DHCP relay. You can also configure the segment to use its own local DHCP Server.

Per-segment DHCP configuration is part of the segment create/update workflow document in [Create or Modify a Network Segment](#).

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click **Networking & Security > Segments**.

To modify the DHCP configuration of an existing segment, click its  button and choose **Edit**, then **EDIT DHCP CONFIG**.

3 Choose a **DHCP Type** and specify configuration details.

Configuration details depend on the DHCP type. To specify **Settings**, toggle **DHCP Config** to **Enabled**.

DHCP Type	Description
Local DHCP Server	<p>Select this option to create a local DHCP server that has an IP address on the segment.</p> <p>It is a DHCP server that is local to the segment and not available to the other segments in the network. A Segment DHCP server provides a dynamic IP assignment service only to the VMs that are attached to the segment.</p> <p>You can configure all DHCP settings, including DHCP ranges, DHCP Options, and static bindings on the segment.</p> <p>For disconnected segments, this type is selected by default.</p>
DHCP Relay	<p>Select this option to relay DHCP client requests to a target DHCP server. The target DHCP server can be in any SDDC subnet or outside the SDDC (on-premises). A DHCP relay service handles only DHCP requests from VMs on its segment.</p> <hr/> <p>Note DHCP requests from VMs in a segment use the segment's gateway address as the source IP. To allow this traffic through the CGW firewall, you need a rule that allows packets with this source address to reach the remote DHCP server. Including the segment object as a group member does not include the gateway IP in the group. You must add it to the group as an IP address. See VMware Knowledge Base article 79595 for related information.</p>
Gateway DHCP Server	<p>This DHCP configuration type is analogous to a central DHCP service that dynamically assigns IP and other network configuration to the VMs on all the segments that are connected to the gateway and using Gateway DHCP. Depending on the type of DHCP profile you attach to the gateway, you can configure a Gateway DHCP server or a Gateway DHCP relay on the segment.</p> <p>By default, segments that are connected to a tier-1 or tier-0 gateway use Gateway DHCP. If needed, you can choose to configure a DHCP local server or a DHCP relay on the segment.</p> <p>To configure Gateway DHCP on a segment, a DHCP profile must be attached to the gateway. See Create or Modify a DHCP Profile.</p>

- a Enable the DHCP configuration settings on the subnet by clicking the **DHCP Config** toggle button.
- b In the **DHCP Server Address** text box, enter the IP addresses.
 - If you are configuring a DHCP local server, server IP address is required. A maximum of two server IP addresses are supported. One IPv4 address and one IPv6 address. For an IPv4 address, the prefix length must be ≤ 30 , and for an IPv6 address, the prefix length must be ≤ 126 . The server IP addresses must belong to the subnets that you have specified in this segment. The DHCP server IP address must not overlap with the IP addresses in the DHCP ranges and DHCP static binding. The DHCP server profile might contain server IP addresses, but these IP addresses are ignored when you configure a local DHCP server on the segment.

After a local DHCP server is created, you can edit the server IP addresses on the **Set DHCP Config** page. However, the new IP addresses must belong to the same subnet that is configured in the segment.

- If you are configuring a DHCP relay, this step is not applicable. The server IP addresses are fetched automatically from the DHCP relay profile and displayed below the profile name.
- If you are configuring a Gateway DHCP server, this text box is not editable. The server IP addresses are fetched automatically from the DHCP profile that is attached to the connected gateway.

Remember, the Gateway DHCP server IP addresses in the DHCP server profile can be different from the subnet that is configured in the segment. In this case, the Gateway DHCP server connects with the IPv4 subnet of the segment through an internal relay service, which is autocreated when the Gateway DHCP server is created. The internal relay service uses any one IP address from the subnet of the Gateway DHCP server IP address. The IP address used by the internal relay service acts as the default gateway on the Gateway DHCP server to communicate with the IPv4 subnet of the segment.

After a Gateway DHCP server is created, you can edit the server IP addresses in the DHCP profile of the gateway. However, you cannot change the DHCP profile that is attached to the gateway.

DHCP Ranges, if specified, must meet the following requirements:

- IP addresses in the DHCP ranges must belong to the subnet that is configured on the segment. DHCP ranges cannot contain IP addresses from multiple subnets.
 - IP ranges must not overlap with the DHCP Server IP address and the DHCP static binding IP addresses.
 - IP ranges in the DHCP IP pool must not overlap each other.
 - Number of IP addresses in any DHCP range must not exceed 65536.
- c (Optional) Edit the lease time in seconds.

Default value is 86400. Valid range of values is 60–4294967295. The lease time configured in the DHCP server configuration takes precedence over the lease time that you specified in the DHCP profile.

- d (Optional) Enter the IP address of the domain name server (DNS) to use for name resolution. A maximum of two DNS servers are permitted.

When not specified, no DNS is assigned to the DHCP client. DNS server IP addresses must belong to the same subnet as the subnet's gateway IP address.

- e (Optional) Click **Options** to configure DHCP options.

For information about **CLASSLESS STATIC ROUTES** and other DHCP **Options**, see [RFC3442](#) and [Create a DHCP Server](#) in the *NSX-T Data Center Administration Guide*.

- 4 (Optional) Specify a DHCP Profile. If your SDDC includes more than one DHC Profile, you can use the **DHCP Profile** drop-down menu to select the name of DHCP server profile you want this segment to use.

See [Create or Modify a DHCP Profile](#).

- 5 Click **APPLY** to apply the DHCP configuration to the segment.

Create or Modify a DHCP Profile

A DHCP profile specifies a DHCP server type and configuration. You can use the default profile or create others as needed.

A DHCP profile can be used to configure DHCP servers of DHCP relay servers anywhere in your SDDC network. See [Add a DHCP Profile](#) in the *NSX-T Data Center Administration Guide*.

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Select **Networking & Security > DHCP**.
- 3 Click **ADD DHCP PROFILE** and give the profile a **Name**.

Choose a **Profile Type** and provide the required configuration parameters.

- For a **DHCP Server**, specify an IPv4 **Server IP Address** and optionally change the **Lease Time**.
- For a **DHCP Relay**, specify the **Server IP Address** as the address of the target DHCP server. If the target DHCP server is on-premises, be sure that your on-premises firewall allows DHCP traffic (ports 67 and 68) to reach this address. Lease time is controlled by the target server configuration.

Either type of DHCP profile can be tagged.

- 4 Click **SAVE** to create the profile.

The new profile is available for use when you specify the DHCP configuration of a routed segment. See [Create or Modify a Network Segment](#). The **Where Used** column lists segments that specify this profile.

Add or Modify Compute Gateway Firewall Rules

By default, the Compute Gateway blocks traffic to all uplinks. Add Compute Gateway firewall rules to allow traffic as needed.

Compute Gateway firewall rules specify actions to take on network traffic from a specified source to a specified destination. Actions can be either allow (allow the traffic) or drop (drop all packets matching the specified source and destination). Sources and destinations can be chosen from a list of a physical network interfaces, or the generic specification **All Uplinks**, which applies to all traffic leaving the gateway and going to the VPC interface, Internet interface, or Intranet (Direct Connect) interface.

Note A firewall rule applied to **All Uplinks** does not apply to the **VPN Tunnel Interface** (VTI), which is a virtual interface and not a physical uplink. The **VPN Tunnel Interface** must be specified explicitly in the **Applied To** parameter of any firewall rule that manages workload VM communications over a route-based VPN.

The Compute Gateway includes a **Default VTI Rule** that drops all traffic to the VTI and a **Default Uplink Rule** that drops traffic to **All Uplinks**. To enable workload VMs to communicate over the VTI, modify this rule or move it to a lower rank in the rule hierarchy, after more permissive rules.

All traffic attempting to pass through the firewall is subjected to the rules in the order shown in the rules table, beginning at the top. A packet allowed by the first rule is passed on to the second rule, and so on through subsequent rules until the packet is dropped, rejected, or hits a default rule.

Prerequisites

Compute Gateway firewall rules require named inventory groups for Source and Destination values. See [Add or Modify a Compute Group](#).


Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 On the **GATEWAY FIREWALL** page, click **Compute Gateway**.
- 5 To add a rule, click **ADD RULE** and give the new rule a **Name**.

6 Enter the parameters for the new rule.

Parameters are initialized to their default values (for example, **All** for **Sources** and **Destinations**). To edit a parameter, move the mouse cursor over the parameter value and click the pencil icon () to open a parameter-specific editor.

Option	Description
Sources	Click Any in the Sources column and select an inventory group for source network traffic, or click ADD GROUP to create a new user-defined inventory group to use for this rule. Click SAVE .
Destinations	Click Any in the Destinations column and select an inventory group for destination network traffic, or click CREATE NEW GROUP to create a new user-defined inventory group to use for this rule. Click SAVE .
Services	Click Any in the Services column and select a service from the list. Click SAVE .
Applied To	<p>Define the type of traffic that the rule applies to:</p> <ul style="list-style-type: none"> ■ Select VPN Tunnel Interface if you want the rule to apply to traffic over the route-based VPN. ■ Select VPC Interface if you want the rule to apply to traffic over the linked AWS VPC connection. ■ Select Internet Interface if you want the rule to apply to traffic over the Internet, including over policy-based VPNs using public IP. ■ Select Intranet Interface if you want the rule to allow traffic over AWS Direct Connect, VMware Transit Connect, and policy-based VPNs using private IP. ■ All Uplinks if you want the rule to apply to the VPC Interface, the Internet Interface, and the Intranet Interface, but not to the VPN Tunnel Interface. <p>Note The VPN Tunnel Interface is not classified as an uplink.</p>
Action	<ul style="list-style-type: none"> ■ Select Allow to allow all L2 and L3 traffic to pass through the firewall. ■ Select Drop to drop packets that match any specified Sources, Destinations, and Services. This is a silent action with no notification to the source or destination systems. Dropping the packet causes the connection to be retried until the retry threshold is reached. ■ Select Reject to reject packets that match any specified Sources, Destinations, and Services. This action returns a "destination unreachable message" to the sender. For TCP packets, the response includes a TCP RST message. For UDP, ICMP and other protocols, the response includes an "administratively prohibited" code (9 or 10). The sender is notified immediately (without any re-tries) when connection cannot be established.

The new rule is enabled by default. Slide the toggle to the left to disable it.

7 Click **PUBLISH** to create the rule.

The system gives the new rule an integer **ID** value, which is used in log entries generated by the rule.

What to do next

You can take any or all of these optional actions with an existing firewall rule.



- Click the gear icon  to view or modify rule logging settings. Log entries are sent to the VMwarevRealize Log Insight Cloud Service. See [Using vRealize Log Insight Cloud](#) in the *VMware Cloud on AWS Operations Guide*.
- Click the graph icon  to view Rule Hits and Flow statistics for the rule.

Table 2-14. Rule Hits Statistics

Popularity Index	Number of times the rule was triggered in the past 24 hours.
Hit Count	Number of times the rule was triggered since it was created.

Table 2-15. Flow Statistics

Packet Count	Total packet flow through this rule.
Byte Count	Total byte flow through this rule.

Statistics start accumulating as soon as the rule is enabled.

- Reorder firewall rules.

A rule created from the **ADD NEW RULE** button is placed at the top of the list of rules. Firewall rules are applied in order from top to bottom. To change the position of a rule in the list, select it and drag it to a new position. Click **PUBLISH** to publish the change.

Add or Modify Distributed Firewall Rules

Distributed firewall rules apply at the VM (vNIC) level and control East-West traffic within the SDDC.

All traffic attempting to pass through the distributed firewall is subjected to the rules in the order shown in the rules table, beginning at the top. A packet allowed by the first rule is passed on to the second rule, and so on through subsequent rules until the packet is dropped, rejected, or hits the default rule, which allows all traffic.

Distributed firewall rules are grouped into policies. Policies are organized by category. Each category has an evaluation precedence. Rules in a category that has a higher precedence are evaluated before rules in category that has a lower precedence.

Table 2-16. Distributed Firewall Rule Categories

Category Evaluation Precedence	Category Name	Description
1	Ethernet	Applied to all layer 2 SDDC network traffic. Note Rules in this category require MAC addresses as sources and destinations. IP addresses are accepted but ignored.
2	Emergency	Used for quarantine and allow rules.
3	Infrastructure	Define access to shared services. Global rules, AD, DNS, NTP, DHCP, backup, management servers.
4	Environment	Rules between security zones such as production zones, development zones, or zones dedicated to specific business purposes.
5	Application	Rules between applications, application tiers, or microservices.

See [Security Terminology](#) in the *NSX-T Data Center Administration Guide* for more information about Distributed Firewall terminology.

Prerequisites

Distributed firewall rules require inventory groups as sources and destinations and must be applied to a service, which can be a predefined service or a custom service that you define for your SDDC. You can create these groups and services while you are creating a rule, but it can speed up the process if you take care of some of this beforehand. See [Add or Modify a Compute Group](#) and [Add a Custom Service](#).

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **Distributed Firewall** page.

Click **Category Specific Rules** and select a category to view and modify policies and rules in that category, or click **All Rules** to view (but not modify) rules in all policies and categories.

5 (Optional) Change the default connectivity strategy.

The Distributed Firewall includes default rules that apply to all layer 2 and layer 3 traffic. These rules are evaluated after all other rules in their category, and allow traffic that doesn't match a preceding rule to pass through the firewall. You can change either or both of these rules to be more restrictive, but you cannot disable either rule.

- To change the **Default Layer2 Rule**, expand the **Default Layer2 Section** in the **Ethernet** category and change the **Action** on that rule to **Drop**.
- To change the **Default Layer3 Rule**, expand the **Default Layer3 Section** in the **Application** category and change the **Action** on that rule to **Drop** or **Reject**.

Click **PUBLISH** to update the rule.

6 To add a policy, open the appropriate category, click **ADD POLICY** and give the new policy a **Name**.

A new policy is added at the top of the policy list for its category. To add a policy before or after an existing policy, click the vertical ellipsis button at the beginning of the policy row to open the policy settings menu, then click **Add Policy Above** or **Add Policy Below**.

By default, the **Applied To** column is set to **DFW**, and the rule is applied to all workloads. You can also apply the rule or policy to selected groups. **Applied To** defines the scope of enforcement per rule, and is used mainly for optimization of host resource consumption. It helps in defining a targeted policy for specific zones and tenants, without interfering with other policy defined for other tenants and zones.

Note Groups consisting of only IP addresses, MAC Addresses, or Active Directory groups cannot be used in the **Applied To** text box.

7 To add a rule, select a policy, click **ADD RULE**, and give the rule a **Name**.

8 Enter the parameters for the new rule.

Parameters are initialized to their default values (for example, **All** for **Sources** and **Destinations**). To edit a parameter, move the mouse cursor over the parameter value and


click the pencil icon () to open a parameter-specific editor.

Option	Description
Sources	Click Any in the Sources column and select an inventory group for source network traffic, or click ADD GROUP to create a new user-defined inventory group to use for this rule. Click SAVE .
Destinations	Click Any in the Destinations column and select an inventory group for destination network traffic, or click ADD GROUP to create a new user-defined inventory group to use for this rule. Click SAVE .
Services	Click Any in the Services column and select a service from the list. Click SAVE .

Option	Description
Applied To	The rule inherits its Applied To value from the containing policy.
Action	<ul style="list-style-type: none"> ■ Select Allow to allow all L2 and L3 traffic to pass through the firewall. ■ Select Drop to drop packets that match any specified Sources, Destinations, and Services. This is a silent action with no notification to the source or destination systems. Dropping the packet causes the connection to be retried until the retry threshold is reached. ■ Select Reject to reject packets that match any specified Sources, Destinations, and Services. This action returns a "destination unreachable message" to the sender. For TCP packets, the response includes a TCP <code>RST</code> message. For UDP, ICMP and other protocols, the response includes an "administratively prohibited" code (9 or 10). The sender is notified immediately (without any re-tries) when connection cannot be established.

The new rule is enabled by default. Slide the toggle to the left to disable it.

9 (Optional) Configure advanced settings.

To change the directionality or logging behavior of the rule, click the gear icon  to open the **Settings** page.

Direction

By default, this value is **In/Out** and applies the rule to all sources and destinations. You can change this to **In** to apply the rule only to incoming traffic from a source, or **Out** to apply it only to outgoing traffic to a destination. Changing this value can cause asymmetric routing and other traffic anomalies, so be sure you understand the likely outcome for all sources and destinations before you change the default value for **Direction**.

Logging

Logging for a new rule is disabled by default. Slide the toggle to the right to enable logging of rule actions.

10 Click **PUBLISH** to create the rule.

The system gives the new rule an integer **ID** value, which is used to identify the rule in log entries it generates.

What to do next

You can take any or all of these optional actions with an existing firewall rule.



- Click the gear icon  to view or modify rule logging settings. Log entries are sent to the VMwarevRealize Log Insight Cloud Service. See [Using vRealize Log Insight Cloud](#) in the *VMware Cloud on AWS Operations Guide*.
- Click the graph icon  to view Rule Hits and Flow statistics for the rule.

Table 2-17. Rule Hits Statistics

Popularity Index	Number of times the rule was triggered in the past 24 hours.
Hit Count	Number of times the rule was triggered since it was created.

Table 2-18. Flow Statistics

Packet Count	Total packet flow through this rule.
Byte Count	Total byte flow through this rule.

Statistics start accumulating as soon as the rule is enabled.

- Reorder firewall rules.

A rule created from the **ADD NEW RULE** button is placed at the top of the list of rules in the policy. Firewall rules in each policy are applied in order from top to bottom. To change the position of a rule in the list, select it and drag it to a new position. Click **PUBLISH** to publish the change.

Manage Distributed Firewall Rules

Traffic attempting to pass through the firewall is subjected to the rules in the order shown in the **ALL RULES**.

The order of distributed firewall rules in the **ALL RULES** list is the union of the ordered list of policies and the ordered list of rules in each policy. You can reorder the distributed firewall sections and rules within a section. You can also edit existing distributed firewall configuration, delete, or clone a firewall rule or section.

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Select **Networking & Security > Distributed Firewall**.
- 3 (Optional) Modify policy settings.

Click the vertical ellipsis button at the beginning of the policy row to take bulk actions, which affect all rules in the policy. You cannot modify these settings if the policy includes any rules.

- 4 (Optional) Reorder policies.

A policy created from the **ADD POLICY** button is placed at the top of the list of policies. Firewall rules in each policy are applied in policy order from top to bottom. To change the position of a policy (and all the rules it contains) in the list, select it and drag it to a new position. Click **PUBLISH** to publish the change.

- 5 (Optional) Clone or copy a rule.

Click  at the beginning of the rule row, then click:

- **Clone Rule** to make a copy of the rule in this policy.

- **Copy Rule** to make a copy of the rule that you can add to another policy.

6 (Optional) Add or delete a rule.

Click  at the beginning of the rule row, then click:

- **Add Rule** to add a rule in this policy.
- **Delete Rule** to delete the rule from this policy.

7 (Optional) Save or view distributed firewall configurations.

Distributed firewall configurations in VMware Cloud on AWS are similar to the [Firewall Drafts](#) feature of on-premises NSX-T. Click **ACTIONS > View** to view a list of saved configurations. Click **ACTIONS > Save** to save the current configuration. Configurations are auto-saved by default. Click **ACTIONS > Settings > General Settings** to disable **Auto Save Drafts**.

8 (Optional) Configure Identity Firewall settings

This option is available if you have enabled NSX-T Advanced Firewall features. See [Chapter 4 About NSX Advanced Firewall Features](#) for more information. Before you can use this feature, you have to enable it and apply it to one or more SDDC clusters.

- On the **Distributed Firewall** tab, click **ACTIONS > Settings > General Settings** and toggle **Identity Firewall Status** to **Enable**.
- Click the **Identity Firewall Settings** tab and choose the SDDC clusters where you want to enable this feature.

Manage the Distributed Firewall Exclusion List

The Distributed Firewall Exclusion List lets you specify inventory groups to exclude from distributed firewall coverage. East-West network traffic to and from members of excluded groups is exempt from distributed firewall rules that would otherwise apply.

The Distributed Firewall exclusion list lets you keep specific inventory groups from being considered by distributed firewall rules. By default, management VMs and appliances, such as vCenter and NSX-T controllers are on the exclusion list. You can edit the list to add or remove entries.


Procedure

- Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- Open the **Distributed Firewall** page.

5 Click **ACTIONS > Settings > Exclusion List** to display the **Exclusion List** page.

- To add an existing group to the exclusion list, click **ADD GROUP** and select an existing **Group Name**.
- To create a group, from the **Manage Exclusion List**, click **ADD GROUP**, fill in the **Group Name**, then click **Set Members** to open the inventory group creation page. See [Add or Modify a Compute Group](#) for more information about using this page.
- To remove a group from the list, click the  button at the beginning of the group row and choose **Delete**.

6 Click **APPLY** to save your changes.

Configure DNS Services

VMware Cloud on AWS DNS forwarding services run in DNS zones, and enable workload VMs in the zone to resolve fully-qualified domain names to IP addresses.

Your SDDC includes default DNS zones for the Management Gateway and Compute Gateway. Each zone includes a preconfigured DNS service. Use the **DNS Services** tab on the **DNS Services** page to view or update properties of DNS services for the default zones. To create additional DNS zones or configure additional properties of DNS services in any zone, use the **DNS Zones** tab.

For more information about DNS configuration choices for VMware Cloud on AWS, see [DNS Strategies for VMware Cloud on AWS](#).

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **DNS** page.
- 5 Click **DNS Services** to open the **DNS Services** page.
- 6 View or edit DNS service parameters.

Most gateway DNS service parameters are read-only but you can click the vertical ellipses button and choose **Edit DNS Server IPs** to add or modify the server IP addresses for this service.

- 7 Click **SAVE**.

Add a DNS Zone

Each DNS zone in your SDDC network represents a piece of the DNS namespace that you manage yourself.

DNS zones in the SDDC fall into two categories:

- Default zones, where the servers listen for DNS queries from all SDDC VMs on a subnet in the zone.
- FQDN zones, where the servers listen for DNS requests forwarded from a default zone.

The compute and management gateways are each configured with a single default DNS zone. You can add up to four more zones of either type to either gateway to provide the flexibility of having multiple DNS servers and subdomains. See [Add a DNS Zone](#) in the *NSX-T Data Center Administration Guide* for more information about how NSX-T implements DNS zones.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **DNS** page.
- 5 Click **DNS Zones** to open the **DNS Zones** page.
- 6 To add a default zone, select **ADD DNS ZONE > Add Default Zone**

You can add or modify IP addresses for the Management Gateway and Compute Gateway DNS forwarders in the default DNS zone. DNS queries from VMs in the default zone are sent to these IP addresses by default if they don't match the criteria for any FQDN zone.

- a Enter a name and optionally a description. You use this **Name** if you create DNS firewall rules that apply to traffic in this zone.
- b Enter the IP addresses of up to three DNS servers. All of the DNS servers you specify must be configured identically.
- c (Optional) Enter an IP address in the **Source IP** field.

- 7 To add an FQDN zone, select **ADD DNS ZONE > Add FQDN Zone**

Specify one or more FQDNs to enable DNS forwarding. A DNS forwarder is associated with a default DNS zone and up to five FQDN DNS zones. When it receives a DNS query from a

VM in the zone, the DNS forwarder compares the domain name in the query with the domain names in the FQDN DNS zones. If a match is found, the query is forwarded to the DNS servers specified in the FQDN DNS zone. Otherwise the query is forwarded to the DNS servers specified in the default DNS zone.

- a Enter a name and optionally a description. You use this **Name** if you create DNS firewall rules that apply to traffic in this zone.
- b Enter a FQDN for the domain. This must be a fully qualified domain name, such as example.com.
- c Enter the IP address of up to three DNS servers.
- d (Optional) Enter an IP address in the **Source IP** field.

8 (Optional) Tag the DNS zone.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

9 Click **SAVE**.

View Routes Learned and Advertised over VMware Transit Connect

In an SDDC that is a member of an SDDC Group, you can use the **Networking & Security Transit Connect** tool to view routes learned and advertised by this SDDC in the VMware Transit Connect network created for the group.

In an SDDC group, all network traffic between group members travels over a VMware Transit Connect network. Routing between compute networks of all SDDCs in a group is managed automatically by VMware Transit Connect as subnets are added and deleted. The **Transit Connect** and **SDDC Group** tools provide information about routes over that network. For information about creating an SDDC group or adding an SDDC to one, see [Creating and Managing SDDC Deployment Groups](#) in the *VMware Cloud on AWS Operations Guide*.

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 On the **Networking & Security** tab, click **Transit Connect**, or just click the **SDDC Group** icon on the **Overview** page.

The **Transit Connect** page displays lists of **Routes Learned** by this SDDC from other SDDCs in the group, and **Routes Advertised** by this SDDC to other SDDCs in the group. Click the download icon (↓) to download either list in CSV format.

View Statistics and Manage Settings for Uplinks

The **Global Configuration** page includes controls that allow you to view traffic statistics and manage Maximum Transmissible Unit (MTU) and Unicast Reverse Path Forwarding (URPF) settings for SDDC network uplinks.

In the default configuration:

- The MTU for the **Services** uplink (which carries traffic to the connected VPC) is set to 8900 bytes. The MTU for other uplinks is set to 1500 bytes.
- URPF is enabled in Strict mode and packets are forwarded to SDDC uplinks only if they are received on the interface that provides the best reverse path to the source of the packet. Packets that do not meet this criterion are dropped.

You can edit these settings on the **Global Configuration** page of the **Networking & Security** tab.

Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click **Networking & Security > Global Configuration**.

This page shows the **MTU** and **URPF** settings for each of the SDDC uplinks. Each uplink also has a **VIEW STATISTICS** button that you can click to see traffic statistics for the uplink.

- a Manage MTU and URPF settings.


To change the MTU setting for an uplink, click **EDIT** and enter a new value. URPF Strict mode, as defined by [RFC3704](#), is required for the Internet Uplink. To change the URPF setting for another uplink, click **EDIT** and choose one of the following values.

Strict	Apply URPF to this uplink in Strict mode.
None	Disable URPF for this uplink.

Click **SAVE** to apply your changes.

- b Click **VIEW STATISTICS** see traffic statics for the uplink.

Statistics collected for each uplink include data (in KB), total packets, and dropped

packets. Click the Refresh icon  to refresh statistics.

Add a Tier-1 Gateway

Every new SDDC includes a default Tier-1 gateway named the Compute Gateway (CGW). You can create and configure additional Tier-1 gateways if you need them. Each Tier-1 gateway sits between the SDDC Tier-0 gateway and an arbitrary number of compute network segments

Additional Tier-1 gateways provide a way for an SDDC network administrator to dedicate workload network capacity to specific projects, tenants, or other units of administration within a VMware Cloud on AWS organization.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.

3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

4 Click **Tier-1 Gateways > ADD TIER-1 GATEWAY**, then give the new gateway a **Name** and optional **Description**.

5 Specify the gateway **Type**.

Type	Traffic Pattern
Routed	Segment traffic is routed through the new gateway.
Isolated	Segment traffic cannot traverse the new gateway. Local segments can connect with each other. Segments are not added to the routing table.
NATted	Segment traffic cannot traverse the new gateway until you create NAT rules for it (see Create or Modify NAT Rules). Local segments can connect with each other. Segments are not added to the routing table.

6 (Optional) Tag the new gateway.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

7 Click **SAVE** to create or configure the gateway.

8 Configure DHCP for the gateway.

Click **Set DHCP Configuration** to open the DHCP Configuration page. The default DHCP configuration **Type** for a new gateway is **No Dynamic IP Address Allocation**. In this configuration, the gateway does not provide DHCP services. If you want the gateway to provide DHCP services, choose a **Type** of **DHCP Server** and specify a **DHCP Server Profile**. You can create a new profile or use an existing one. See [Create or Modify a DHCP Profile](#).

9 Click **Additional Settings**.

Select an **Ingress QoS Profile** and an **Egress QoS Profile** for traffic limitations. These profiles are used to set information rate and burst size for permitted traffic. See [Add a Gateway QoS Profile](#) for more information on creating QoS profiles. VMware Cloud on AWS does not support IPv6, so the **ND Profile** and **DAD Profile** options do not apply.

10 (Optional) Configure static routes for the gateway.

This option is not available in the VMC Console **Networking & Security** tab.

You can configure a non-default route for any type of gateway. A static default route (0.0.0.0/0) can be configured only for an Isolated gateway. On the NSX Manager **Networking** tab, click **Tier-1 Gateways**. When you create or edit a Tier-1 gateway, click **STATIC ROUTES** to create or modify static routes and next hops for the gateway.

Configure a Multi-Edge SDDC With Traffic Groups

In the default configuration, your SDDC network has a single edge (TO) router through which all North-South traffic flows. This edge supports the default traffic group, which is not configurable. If you need additional bandwidth for the subset of this traffic routed to SDDC group members, a Direct Connect Gateway attached to an SDDC group, VMware HCX Service Mesh, or to the Connected VPC, you can reconfigure your SDDC to be Multi-Edge by creating traffic groups, each of which creates an additional TO router.

A traffic group uses an association map to associate a prefix list of CIDR blocks to one of the TO gateways that support non-default traffic groups in your SDDC. Prefix lists are independent of gateways and consist of source IP addresses. Traffic from those addresses is routed to the TO edge that supports the associated traffic group. You can create and update prefix lists at any time, but you cannot remove a prefix list if it is included in an association map. Associating a prefix list with a traffic group routes all traffic from CIDR blocks in the list through the TO router created for the group.

Note VPN traffic, as well as DX traffic to a private VIF must pass through on the default TO and cannot be routed to a non-default traffic group. In addition, because NAT rules always run on the default TO router, additional TO routers cannot handle traffic affected by SNAT or DNAT rules. This includes traffic to and from the SDDC's native Internet connection. It also includes traffic to the Amazon S3 service, which uses a NAT rule and must go through the default TO. Keep these limitations in mind when you create prefix lists.

Prerequisites

- Before you can create traffic groups, you must use VMware Transit Connect™ to connect your SDDC to a VMware Managed Transit Gateway (VTGW). See [Creating and Managing SDDC Deployment Groups](#) in the *VMware Cloud on AWS Operations Guide*.
- Traffic groups can be created only in SDDCs that have large-size management appliances and at least four hosts. See [Upsize SDDC Management Appliances](#) for information about changing an SDDC's management appliance size from medium to large. See [Add Hosts](#) for information about adding hosts to an SDDC.
- The number of traffic groups that a multi-AZ (stretched cluster) SDDC can support depends on the number of hosts that the SDDC provides in each region, and can be represented with a formula like this:

$$TG = (hosts-per-region - 2) / 2$$

where *TG* represents the maximum number of traffic groups that the SDDC can support and *hosts-per-region* is the number of hosts the SDDC deploys in each of the regions it occupies.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.

3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

4 Create a traffic group. On the **Traffic Groups** tab of the **Traffic Groups** page, click **ADD TRAFFIC GROUP** and give the new traffic group a **Name**, then click **SAVE** to create the traffic group and an additional TO router for it.


The **Status** of the traffic group transitions to **In Progress** while the new TO edge is being created. It can take up to 30 minutes for the process to complete. When it does, the **Status** of the traffic group transitions to **Success** and you can create an association map for it.

5 Create a prefix list.

Because Multi-Edge SDDCs use source-based routing in their traffic groups, prefix lists must contain source addresses, not destination addresses.


- a On the **IP Prefix List** tab of the **Traffic Groups** page, click **ADD IP PREFIX LIST** and give the new prefix list a **Name** and optional **Description**.
- b Click **Set** to display the **Set Prefixes** window, then click **ADD PREFIX** and fill in the CIDR block of an SDDC network segment that includes the source addresses of workload VMs whose traffic you want to include in the traffic group (and route over the additional edge).

Important You cannot use the SDDC management CIDR block here or the CIDR block of a segment that provides the local IP address of a VPN. If you add any of these CIDRs to a prefix list, you won't be able to use the list in an association map.



Click **ADD** to add the specified prefix to the list. To add prefixes or edit the ones already on the list, click  to open the prefixes editor.

- c Click **APPLY** to apply your changes to the prefix list.
- d When you're done adding or editing prefixes, click **SAVE** to save or create the prefix list.

6 Associate a prefix list with a gateway. On the **Traffic Groups** tab of the **Traffic Groups** page, find the traffic group you want to work with, then click and select **Edit**.

Click the plus icon  in the **ASSOCIATION MAPS** area, give the mapping a **Name** and select an existing prefix list from the **Prefixes** drop-down. Select a gateway from the **Gateway** drop-down, and click **SAVE** to create the association map.

7 (Optional) To remove a traffic group, you must first remove its association maps.

- a Find the traffic group on the **Traffic Groups** page. Click its  button, then select **Edit**.
- b Click the minus icon  to the right of the **Status** label under **Association Maps** to select the map for deletion, then click **SAVE** to delete the map.
- c Click **CLOSE EDITING**, then return to the traffic group on the **Traffic Groups** page. Click its ellipsis button and then select **Delete**.

It can take up to 30 minutes to remove a traffic group. Removing the traffic group removes the TO router that was created to support it. HCX, if in use, creates its own association map, which you can view but not modify. To remove an association map created by HCX, you have to uninstall HCX. See [Uninstalling VMware HCX](#) in the *VMware HCX User Guide*.

Example: Route Table Changes After Adding a Traffic Group

This simplified example shows the effect of creating traffic group and associating it with a prefix list of just two host routes (/32).

Initial configuration

Assume these values for route table entries in the default traffic group and the Compute Gateway (CGW) before adding the first traffic group (which creates an additional TO router).

Table 2-19. Default Routes

Subnet	Next Hop
0.0.0.0/0	Internet Gateway
192.168.150.51/24	CGW
192.168.151.0/24	CGW
VTGW, DXGW subnets	VTGW, DXGW connections
Management CIDR	MGW

Table 2-20. CGW Routes With the Default Traffic Group

Subnet	Next Hop
0.0.0.0/0	Default TO
192.168.150.0/24	Default TO
192.168.151.0/24	Default TO

Multi-Edge configuration

After the first traffic group is created, new routes are added on the default T0. Assuming that the prefix list associated with the traffic group has these entries:

```
192.168.150.100/32
192.168.151.51/32
```

then the route tables for the default T0, new T0, and CGW end up like this.

Table 2-21. Default T0 Routes After Adding a Traffic Group

Subnet	Next Hop
0.0.0.0/0	Internet Gateway
192.168.150.0/24	CGW
192.168.150.100/32	New T0
192.168.151.0/24	CGW
192.168.151.51/32	New T0
VTGW, DXGW subnets	VTGW, DXGW connections
Management CIDR	MGW

The new routes (192.168.150.100/32 and 192.168.151.51/32 in the example tables) use the new T0 as their next-hop, and the new T0 uses longest-prefix matching to route that traffic to the CGW.

Table 2-22. Routes on the New Traffic Group

Subnet	Next Hop
0.0.0.0/0	Default T0
192.168.150.100/32	CGW
192.168.151.51/32	CGW
VTGW, DXGW subnets	VTGW, DXGW connections
Management CIDR	MGW

The CGW route table is updated to create the traffic group by specifying the new T0 router as the next hop for the new routes.

Table 2-23. CGW Routes With an Additional Traffic Group

Subnet	Next Hop
0.0.0.0/0	Default T0
192.168.150.0/24	Default T0
192.168.150.100/32	New T0

Table 2-23. CGW Routes With an Additional Traffic Group (continued)

Subnet	Next Hop
192.168.151.0/24	Default TO
192.168.151.51/32	New TO

Enable AWS Managed Prefix List Mode for the Connected Amazon VPC

AWS Managed Prefix List Mode can simplify route table management in a Multi-Edge SDDC and enable support in any SDDC for custom route tables and route aggregation.

When you enable AWS Managed Prefix Lists, VMware Cloud on AWS creates a VPC prefix list populated with the default Compute Gateway prefixes and any other prefix list aggregations you have created. The Managed Prefix List is made available as an AWS resource share. Once you accept this resource, you can add prefix lists to the Connected VPC route tables.

VMware Cloud on AWS uses the Managed Prefix List to update the main route table. When a prefix list is added to a route table and that entry in the route table is pointed to a destination ENI, the prefix list replaces the individual CIDRs it includes. Because it is a managed object, the prefix list gets updated automatically whenever new segments or aggregations are configured. In addition, the route table entries for that prefix list are updated to point to the correct ENI whenever the active Edge instance's host changes. You are responsible for adding Connected VPC prefix lists to any custom route tables that you've created. In a multi-edge SDDC, you'll need to manually update prefix lists for the each additional NSX-T edge.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Click **Connected VPC** to open the **Connected Amazon VPC** page.

The **Traffic Groups** table on this page shows the default traffic group and its active AWS network interface ID.

5 Enable **AWS Managed Prefix List Mode**.

Note Once you enable AWS Managed Prefix List mode, you cannot disable it without opening a VMware Support request to have your account unlinked.

- a Toggle **AWS Managed Prefix List Mode** to **Enabled**.

Review the message and click **ENABLE** or **CANCEL**. If you click **ENABLE**, **AWS Managed Prefix List Mode** transitions to **ACTION PENDING** and you are prompted to accept the AWS resource share containing the managed prefix list.

- b Log into the AWS console with an identity that has permission to accept a resource share and click **Resource Access Manager > Shared with me**.

The resource **Name** has the form `managed-prefix-list-resource-share-vpc-ID` and a **Status** of **Pending**. Click the resource **Name** to open the resource **Summary** card, then click **Accept resource share** and confirm acceptance,

- c In the VMC Console, return to the **Connected Amazon VPC** tab and wait for **AWS Managed Prefix List Mode** to change from **Pending** to **Enabled**.

AWS resource association can take up to ten minutes.

In the main route table, the individual routes to their SDDC are replaced by a prefix list pointing to the active ENI for their SDDC. The **Traffic Groups** table now includes the **Prefix List ID**, **Prefix List Name**, and **Route Tables Programmed** for the default traffic group. Click the **Prefix List Name** to view the list.

What to do next

Add the prefix list to a custom route table in the Connected VPC. This allows AWS resources in subnets associated with that custom route table to communicate with the SDDC.

VMware Cloud on AWS automatically detects the additional route table and updates the prefix list to point to the correct ENI. After the initial update, you can manually configure the route table to point to the same ENI that the prefix list uses. Otherwise, this update and subsequent updates happen automatically whenever VMware Cloud on AWS detects the addition of the prefix list to a new route table.

Note Like all AWS prefix lists, the new prefix list is subject to [AWS VPC route table quotas](#). Each entry in the prefix list counts as a single route, so be sure that any route table you add it to has sufficient capacity.

After VMware Cloud on AWS detects a custom route table with the prefix list (this takes 5 to 10 minutes in most cases) that route table entry gets updated to point to the active ENI if it wasn't already, and the custom route table is added to the **Traffic Groups** table. This route table is updated as soon as the active ENI changes.

Working With Inventory Groups

VMware Cloud on AWS network administrators can use NSX-T inventory objects to define collections of services, groups, context profiles, and virtual machines to use in firewall rules.

Firewall rules typically apply to a group of VMs that have certain common characteristics including:

- names that follow a naming convention (like Win* for Windows VMs or Photon* for Photon VMs)
- IP addresses within a specific range or CIDR block
- tags

They can also apply to network services, which are distinguished by characteristics like service type and network protocol. The NSX-T **Inventory** page simplifies the process of creating groups of VMs that have similar needs for firewall protection. It also allows you to add new network services to the built-in list of services, so that you can include those services in firewall rules.

VMware Cloud on AWS creates management groups and a service inventory in all new SDDCs. It also maintains a list of your workload VMs and their tags. You can add or modify your own inventory groups of management or compute VMs.

See [Inventory](#) in the *NSX-T Data Center Administration Guide*.

Add a Management Group

Management inventory groups contain SDDC infrastructure components. Use these groups in management gateway firewall rules.

Pre-defined management inventory groups are created automatically for SDDC infrastructure components such as vCenter and NSX Manager. You cannot modify a pre-defined management group, but you can create additional management inventory groups by specifying the CIDR blocks to which group members are connected.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **Inventory** page.
- 5 On the **Groups** page, click **MANAGEMENT GROUPS**, then click **ADD GROUP** and give the group a **Name** and an optional **Description**.
- 6 Click **Set Members** to open the **Select Members** page.


Enter one or more IP addresses of management VMs in CIDR format.

7 (Optional) Tag the group.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

8 Click **SAVE** to create the group.

What to do next

To can modify or delete any management group that you created, click its  icon and choose **Edit** or **Delete**.

Add or Modify a Compute Group

Compute inventory groups categorize compute VMs using criteria such as names, IP addresses, and tags.

Because compute inventory groups are made up of the compute VMs you deploy on your compute network segments, VMware Cloud on AWS cannot create them for you. You'll need to create them yourself before you can develop compute gateway firewall rules.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **Inventory** page.
- 5 On the **Groups** page, click **Compute Groups**, then click **ADD GROUP** and give the group a **Name** and an optional **Description**.

To modify an existing group, select it and click the ellipsis button at the beginning of the group row.

6 Click **Set Members** to open the **Select Members** page.

Management groups contain VMs on the Management Network. Management group members must be specified by IP address. Compute groups contain VMs or network objects such as segments in the Compute network. There are several ways to designate membership in a compute group.

Option	Description
Membership Criteria	<p>Click ADD CRITERIA and use the drop-down controls to specify one or more criteria in the form of</p> <p><i>Object Type, Property, Condition, Value</i></p> <p>tuples. For example, a group with these criteria:</p> <p><i>Virtual Machine Name Contains db_</i></p> <p>includes VMs whose names contain the string <code>db_</code> in the group. You can also create groups of tagged network segments, segment ports, or IP sets by specifying a tag, or</p> <p><i>Segment Tag Equals testbeds</i></p> <p>to include network segments that have the tag <code>testbeds</code>.</p> <p>Objects that match all of the selected criteria are included in the group.</p>
Members	Select a membership category from the Select Category drop-down list, then select members from the list.
IP Addresses	Enter an IP address, CIDR block, or a range of IP addresses in the form <i>ip-ip</i> (for example <code>192.168.1.1-192.168.1.100</code>) or click Import to import these values from a file.
MAC Addresses	Enter one or more MAC addresses. Separate multiple addresses with commas.
AD Groups	Groups with Active Directory members can be used in the source text box of a distributed firewall rule for Identity Firewall. Groups can contain both AD and compute members.

7 (Optional) Tag the group.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

8 Click **SAVE** to create the group.

What to do next

To review group members, select a group and click **View Members** to review the list of group members to view group members and membership criteria. Click **Where Used** to see a list of firewall rules that include the group.

Add a Custom Service

Firewall rules often apply to traffic from a network service. A new SDDC includes inventory entries for most of the common network service types, but you can add custom services if you need to.

When you create a firewall rule, you can specify that it applies to network traffic from one or more of the services defined in your SDDC's **Services** inventory. The default list includes VMware services such as remote console and provisioning, standard services such as IKE, ICMP, and TCP, and many well-known third party services. You can add services to this list by selecting values, typically ports and protocols, from a list of service types and additional service properties.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **Inventory** page.
The **Services** card lists the predefined services.
- 5 Click **ADD SERVICE** and give the service a **Name**.
- 6 Click **Set Service Entries** to open the **Set Service Entries** page.
- 7 On the **Set Service Entries** page, click **ADD SERVICE ENTRY**.

To view the list of known services, use the drop-down controls to scroll through the **Service Type** and **Additional Properties** lists. To add a service, select a **Service Type** from the drop-down menu and specify **Additional Properties** such as Source or Destination Ports of the service, then click **APPLY**.

- 8 (Optional) Provide a service **Description** and tag the service.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

- 9 Click **SAVE** to create the service definition.

View Virtual Machine Inventory

VMware Cloud on AWS maintains an inventory of workload virtual machines in your SDDC. VMs are listed by name and number of tags.


The **Virtual Machines** inventory is generated automatically. You can edit the tags assigned to a VM in this list, but you cannot add or remove VMs. The system does that automatically as VMs are created and destroyed.


Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Click **Inventory** > **Virtual Machines**.

If a virtual machine has any tags, the number of tags is shown in the **Tags** column. Click the number to view the tags. To add or remove VM tags, click  at the beginning of the VM row

and select **Edit** to display the tag editor. Click  to add more tags.

See [Add Tags to an Object](#) in the *NSX-T Data Center Administration Guide* for more information about tagging NSX-T objects.

About Context Profiles

Context profiles are a VMware Cloud on AWS add-on feature available only in an SDDC that has activated the NSX Advanced Firewall Add-On.

There are two types of profiles: context profiles and layer 7 access profiles. Profiles enable creating attributes key value pairs such as layer 7 App Id, and Domain Names. After a profile has been defined, it can be used in one or more distributed firewall rules, and gateway firewall rules.

For information about how to install and use the NSX Advanced Firewall add-on, see [Chapter 4 About NSX Advanced Firewall Features](#). You can read more about context profiles and how to use them in VMware Cloud on AWS [here](#).

Managing Workload Connections

Workload VMs on routed segments or HCX extended networks with MON enabled can connect to the Internet by default. NAT rules, Compute Gateway firewall rules, and distributed firewall rules, as well as default routes advertised by a VPN, DX, or VTGWconnection all give you fine-grained control over Internet access.

Workload VMs can use private IP addresses to communicate with other workloads in the same SDDC or SDDC group. When a workload VM uses a public IP address, it gets the **Source NAT Public IP** shown on the **Overview** page unless it is subject to a custom NAT rule that applies to all traffic.

Workload traffic is subject to several kinds of special handling during firewall rule processing:

- Workload-to-workload traffic is not subject to CGW firewall rules.

- Distributed firewall rule processing by a source VM uses the destination public IP address and source public IP of the destination VM, and must be IP-based. Distributed firewall rules based on VM attributes do not affect workload-to-workload traffic.
- Workload VM communication to the vCenter Server public IP is subject to MGW firewall rules, but the workload VM IP is translated to its public IP before the firewall rule is applied.

Note All VMs on a network segment should use the same MTU. The MTU for traffic internal to the SDDC or over DX is capped at 8900 bytes. The maximum MTU for network traffic to other endpoints may be lower. See [VMware Configuration Maximums](#).

Attach a VM to or Detach a Workload VM from a Compute Network Segment

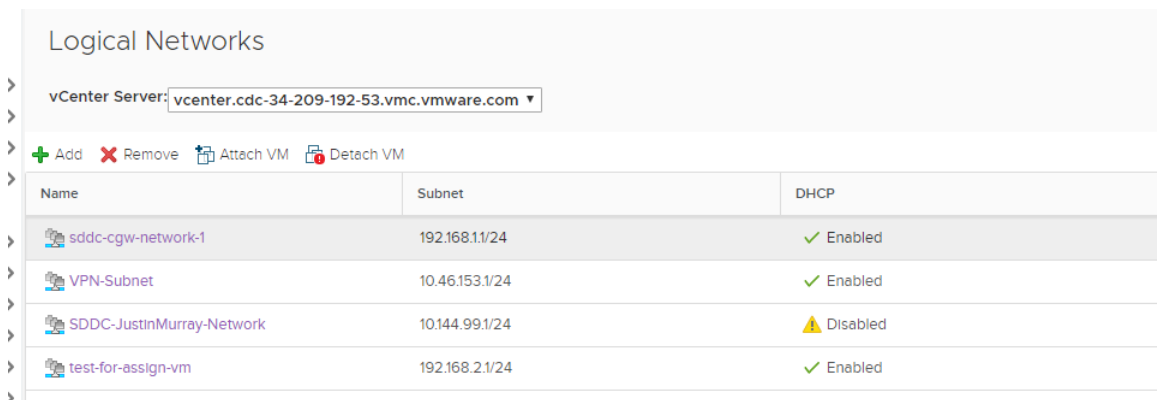
Use the vSphere Client to manage attachment of workload VMs to compute network segments.

Prerequisites

Your SDDC compute network must have at least one segment. See [Create or Modify a Network Segment](#).

Procedure

- 1 Log in to the vSphere Client for your SDDC.
- 2 Select **Menu > Global Inventory Lists**.
- 3 Select **Logical Networks**.
- 4 In the **vCenter Server** drop down menu, select the vCenter Server that manages the logical network you want to use.
- 5 Click next to the logical network name to select it.



Name	Subnet	DHCP
sddc-cgw-network-1	192.168.11/24	✓ Enabled
VPN-Subnet	10.46.153.1/24	✓ Enabled
SDDC-JustinMurray-Network	10.144.99.1/24	⚠ Disabled
test-for-assign-vm	192.168.2.1/24	✓ Enabled

- 6 Select whether to attach or detach VMs.
 - Click **Attach VM** to attach VMs to the selected network.
 - Click **Detach VM** to detach VMs from the selected network.

- 7 Select the virtual machine(s) you want to attach or detach, click >> to move them to the **Selected Objects** column, and click **Next**.
- 8 For each VM, select the virtual NIC you want to attach and click **Next**.
- 9 Click **Finish**.

Request or Release a Public IP Address

You can request public IP addresses to assign to workload VMs to allow access to these VMs from the Internet. VMware Cloud on AWS provisions the IP address from AWS.

As a best practice, release the public IP addresses that are not in use.

Prerequisites

Verify that your VM has a static IP address assigned from its logical network.


Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **Public IPs** page.
- 5 To request a new public IP address, click **REQUEST NEW IP**.

You can optionally enter your notes about the request.

- 6 To release a public IP address that you no longer need, click  and select **Release IP**.

Requests to release a public IP fail if the address is in use by a NAT rule.

- 7 Click **SAVE**.

After a few moments, a new public IP address is provisioned.

What to do next

After the public IP address is provisioned, configure NAT rules to direct traffic from the public IP address to the internal IP address of a VM in your SDDC. See [Create or Modify NAT Rules](#).

Create or Modify NAT Rules

Network Address Translation (NAT) controls how IP addresses in packet headers appear on either side of a gateway. Rules that run on the Compute Gateway map Internet traffic as it enters and leaves the gateway. Rules that run on other Tier-1 gateways map traffic between the gateway and other SDDC network interfaces.

NAT rules run on the Compute Gateway and on any additional Tier-1 gateways that you create. See [Add a Tier-1 Gateway](#) for information about creating additional Tier-1 gateways in your SDDC.

NAT rules that run on the SDDC's Internet interface (the Compute Gateway) map internal source or destination IP addresses on packets from compute network segments to addresses that are usable on the public Internet. To create a NAT rule, you provide the internal address of a workload VM or service and an external IP address of your choice. NAT rules that run on the **Internet** interface require a public IP address. See [Request or Release a Public IP Address](#).

Firewall rules, which examine packet source and destination addresses, run on these gateways and process traffic after it has been transformed by any applicable NAT rules. When you create a NAT rule, you can specify whether a VM's internal or external IP address and port number are exposed to firewall rules that affect network traffic to and from that VM.

Important Inbound traffic to the SDDC's public IP address is always processed by the NAT rules you create. Outbound traffic (reply packets from SDDC workload VMs) is routed along the advertised routes and is processed by NAT rules when the default route for your SDDC network goes through the SDDC's Internet interface. But if the default route goes through a Direct Connect, VPN, or VTGW connection or has been added as a static route to a VPC, NAT rules run for inbound traffic but not for outbound traffic, creating an asymmetric path that leaves the VM unreachable at its public IP address. This asymmetry can arise when, for example, if 0.0.0.0/0 is advertised through BGP or there is a policy-based VPN with a remote network of 0.0.0.0/0. When the default route is advertised from the on-premises environment, you must configure NAT rules on the on-premises network, using the on-premises Internet connection and public IPs.

Prerequisites

- To create a NAT rule on the Compute Gateway (**Internet** interface), you must have obtained a public IP address for use by a VM in this SDDC. See [Request or Release a Public IP Address](#).
- The VM must be connected to a routed compute network segment. You can create NAT rules for VMs whether they have static or dynamic (DHCP) addresses, but bear in mind that NAT rules for VMs using DHCP address assignment can be invalidated when the VM is assigned an internal address that no longer matches the one specified in the rule.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

4 Click **NAT > Internet** to add NAT rules that run on the default Compute Gateway.

a Click **ADD NAT RULE** and give the rule a **Name**.

b Configure **Internet** NAT rule options:

Option	Description
Public IP	Choose from the drop-down list of public IP address that have been provisioned for this SDDC. See Request or Release a Public IP Address .
Service	<ul style="list-style-type: none"> ■ Select All Traffic to create a rule that applies to both inbound (DNAT) and outbound (SNAT) traffic to or from the specified Internal IP. ■ Select one of the listed services to create an inbound (DNAT) rule that applies only to traffic using that protocol and port. Any services created using Add a Custom Service are also listed here. <p>Note Because services that use multiple destination ports cannot be subject to a NAT rule, they don't appear on this list.</p>
Public Port	<p>If you specified Service as All Traffic, the default public port is Any.</p> <p>If you selected a particular Service, then the rule applies to the assigned public port for that service.</p>
Internal IP	Enter the internal IP address of the VM. This address must be on a routed SDDC network segment.
Internal Port	<p>Displays the internal port used by the selected Service. To use a custom port, Add a Custom Service, then select that Service in the NAT rule.</p> <p>If you specified Service as All Traffic, the default internal port is Any.</p> <p>If you selected a particular Service, then the rule applies to the assigned public port for that service.</p>
Firewall	Specify how traffic subject to this NAT rule is exposed to gateway firewall rules. By default, these firewall rules match the combination of Internal IP and Internal Port . Select Match External Address to have firewall rules match the combination of External IP and External Port . (Distributed firewall rules never apply to external addresses or ports.)

You can create multiple NAT rules that use the same **Public IP** and **Internal IP** with **All Traffic**. If you do this, each **Internal IP** uses the **Public IP** for outbound (SNAT) traffic, but only the first matching rule will be used for inbound (DNAT) traffic. The system creates (but does not display) a default outbound rule. This rule is used for all **Internal IP** addresses that do not match a specific NAT rule that applies to **All Traffic**. The IP used for this rule is displayed in the **Default Compute Gateway** summary on the **Networking & Security Overview** page as **Source NAT Public IP**.

c Choose a **Priority** for the rule.

A lower value means a higher precedence for this rule.

d (Optional) Toggle **Logging** to log rule actions.

e The new rule is enabled by default. Toggle **Enable** to disable it.

f Click **SAVE** to create the rule.

- 5 (Optional) If you have created additional an Tier-1 gateway, click **NAT > Tier-1 Gateway** to add NAT rules that run on that gateway.

- a Choose a **Gateway** where you want the rule to run.
- b Click **ADD NAT RULE** and give the rule a **Name**.
- c Configure **Tier-1 Gateway** NAT rule options:

Option	Description:
Action	<p>One of:</p> <p>SNAT</p> <p>Source NAT. Changes the source address in the packet header. See Configure Source NAT on a Tier-1 Router.</p> <p>DNAT</p> <p>Destination NAT. Changes the destination address in the packet header. See Configure Destination NAT on a Tier-1 Router.</p> <p>Specify a Translated Port if you need to.</p> <p>Reflexive</p> <p>Stateless NAT configuration to avoid asymmetrical routes. See Reflexive NAT</p> <p>No SNAT</p> <p>Disable source NAT.</p> <p>No DNAT</p> <p>Disable destination NAT.</p>
Match	For SNAT, enter a source address to use. For DNAT, enter a destination address to use.
Translated	Enter an IPv4 address or CIDR block to use for the translated SNAT or DNAT address.
Apply To	Choose specific interfaces or labels to define the traffic that you want the rule to affect.
Firewall	Specify how traffic subject to this NAT rule is exposed to gateway firewall rules. By default, these firewall rules match the combination of Internal IP and Internal Port . Select Match External Address to have firewall rules match the combination of External IP and External Port . (Distributed firewall rules never apply to external addresses or ports.)

- d Choose a **Priority** for the rule.
A lower value means a higher precedence for this rule.
- e (Optional) Toggle **Logging** to log rule actions.
- f The new rule is enabled by default. Toggle **Enable** to disable it.
- g Click **SAVE** to create the rule.

Creating Firewall Rules to Manage Traffic Between the Compute and Management Networks

In the default configuration, firewall rules prevent VMs on the compute network from accessing VMs on the management network. To allow individual workload VMs to access management VMs, create Workload and Management inventory groups, then create management gateway firewall rules that reference them.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Create Compute inventory groups: one for the management network and one for the workload VM that you want to have access to it.

On the **Inventory** page, Click **Groups > Compute Groups** and create two groups:

- Click **ADD GROUP > Set Members**, then open the **IP Addresses** page, click **Enter IP Address**, and type the CIDR block of the management network. Click **APPLY**, then **SAVE** to create the group.
- Click **ADD GROUP > Set Members**, then click the **Membership Criteria > ADD CRITERIA** and specify a **Virtual Machine** in your vSphere inventory. Click **APPLY**, then **SAVE** to create the group.

- 5 Create a Management Group that includes the management network that you want to access from the Compute Group.

On the **Inventory** page, Click **Groups > Management Groups**. On the **Select Members** page, click **Enter IP Address**, and type the CIDR block of the management network. Click **APPLY**, then **SAVE** to create the group.

- 6 Create a management gateway firewall rule allowing inbound traffic to vCenter Server and ESXi.

See [Add or Modify Management Gateway Firewall Rules](#) for information about creating management gateway firewall rules. Assuming your workload VMs only need to access vSphere, PowerCLI, or OVFtool, then the rule need only allow access on port 443.

Table 2-24. Management Gateway Rule to Allow Inbound Traffic to ESXi and vCenter

Name	Source	Destination	Services	Action
Inbound to ESXi	Workload VM private IP	ESXi	HTTPS (TCP 443)	Allow
Inbound to vCenter private IP	Workload VM private IP	vCenter private IP	HTTPS (TCP 443)	Allow
Inbound to vCenter public IP	Workload VM with NATted IP	vCenter public IP	HTTPS (TCP 443)	Allow

Configure Monitoring and Troubleshooting Features

3

Use NSX-T IPFIX and Port Mirroring functionality to monitor and troubleshoot SDDC networking and security.

By default, SDDC ESXi hosts have access to the overlay network, allowing them to communicate with monitoring and troubleshooting applications deployed as VM workloads in your SDDC. However, you must configure the firewall to allow traffic between the ESXi hosts and the logical segment the workload VMs are attached to. See [Creating Firewall Rules to Manage Traffic Between the Compute and Management Networks](#).

- [Configure IPFIX](#)

IPFIX (Internet Protocol Flow Information Export) is a standard for the format and export of network flow information for troubleshooting, auditing, or collecting analytics information.

- [Configure Port Mirroring](#)

Port mirroring lets you replicate and redirect all of the traffic coming from a source. The mirrored traffic is sent encapsulated within a Generic Routing Encapsulation (GRE) tunnel to a collector so that all of the original packet information is preserved while traversing the network to a remote destination.

- [View Connected VPC Information and Troubleshoot Problems With the Connected VPC](#)

The Connected Amazon VPC contains your SDDC and all its networks. Information about this VPC, including the active ENI, VPC subnet, and VPC ID, is available on the **Connected VPC** page.

Configure IPFIX

IPFIX (Internet Protocol Flow Information Export) is a standard for the format and export of network flow information for troubleshooting, auditing, or collecting analytics information.

You can configure flow monitoring on a logical segment. All the flows from the VMs connected to that logical segment are captured and sent to the IPFIX collector. The collector names are specified as a parameter for each IPFIX switch profile.

Note In an SDDC that is a member of an SDDC group, all outbound traffic from hosts to destinations outside the SDDC network is routed to the VTGW or private VIF regardless of other routing configurations in the SDDC. This includes IPFIX and Port Mirroring traffic. See [Creating and Managing SDDC Deployment Groups with VMware Transit Connect](#) in the *VMware Cloud on AWS Operations Guide*.

Prerequisites

Verify that a logical segment is configured. See [Create or Modify a Network Segment](#).

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **IPFIX** page.

See [Network Monitoring](#) in the *NSX-T Data Center Administration Guide* for more information about using IPFX.

Configure Port Mirroring

Port mirroring lets you replicate and redirect all of the traffic coming from a source. The mirrored traffic is sent encapsulated within a Generic Routing Encapsulation (GRE) tunnel to a collector so that all of the original packet information is preserved while traversing the network to a remote destination.

Port mirroring is used in the following scenarios:

- Troubleshooting - Analyze the traffic to detect intrusion and debug and diagnose errors on a network.
- Compliance and monitoring - Forward all of the monitored traffic to a network appliance for analysis and remediation.

Port mirroring includes a source group where the data is monitored and a destination group where the collected data is copied to. The source group membership criteria require VMs to be grouped based on the workload such as web group or application group. The destination group membership criteria require VMs to be grouped based on IP addresses. Port mirroring has one enforcement point, where you can apply policy rules to your SDDC environment.

The traffic direction for port mirroring is Ingress, Egress, or Bi Directional traffic:

- Ingress is the outbound network traffic from the VM to the logical network.
- Egress is the inbound network traffic from the logical network to the VM.
- Bi Directional is the traffic from the VM to the logical network and from the logical network to the VM. This is the default option.

Note In an SDDC that is a member of an SDDC group, all outbound traffic from hosts to destinations outside the SDDC network is routed to the VTGW or private VIF regardless of other routing configurations in the SDDC. This includes IPFIX and Port Mirroring traffic. See [Creating and Managing SDDC Deployment Groups with VMware Transit Connect](#) in the *VMware Cloud on AWS Operations Guide*.

Prerequisites

Important Port mirroring can generate a lot of network traffic. As a best practice, limit its use to a maximum of 6 VMs at a time for short periods of troubleshooting and remediation.

Verify that workload groups with IP address and VM membership criteria are available. See [Add or Modify a Compute Group](#).

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Open the **Port Mirroring** page.

See [Network Monitoring](#) in the *NSX-T Data Center Administration Guide* for more information about using port mirroring.

View Connected VPC Information and Troubleshoot Problems With the Connected VPC

The Connected Amazon VPC contains your SDDC and all its networks. Information about this VPC, including the active ENI, VPC subnet, and VPC ID, is available on the **Connected VPC** page.

VMware Cloud on AWS uses AWS account linking and AWS CloudFormation to obtain the permissions it needs to access a your AWS account. When the accounts are linked, VMware Cloud on AWS runs a CloudFormation template that creates IAM roles and grants permissions for several VMware accounts to assume those roles. The role names are listed on the SDDC's **Connected VPC** page. Details about those roles and permissions are published in [AWS Roles and Permissions](#) in the *VMware Cloud on AWS Operations Guide*.

Assuming these roles grants VMware Cloud on AWS the rights to create, delete and assign ENIs and modify route tables in your VPC. The roles also permit enumeration of the subnets and VPCs in the account so that VMware Cloud on AWS can map the available resources and present them in the SDDC creation process. These capabilities are needed at the beginning of the SDDC creation workflow, whenever an SDDC is upgraded, and may be needed at other times during the life of the SDDC when VPCs and their subnets need to be verified, and when route tables and ENIs need to be examined and modified. If an organization member compromises the connected VPC by doing things like deleting or modifying IAM roles or modifying the main route table, it can have a variety of impacts on SDDC operations, including:

- VMware Cloud on AWS will be unable to add, replace, or remove hosts in the SDDC management cluster.
- VMware Cloud on AWS will be unable to update the main route table when routes change or the active NSX-T Edge changes hosts during an upgrade. This can break connectivity between the SDDC and native AWS services. See [Routing Between Your SDDC and the Connected VPC](#) for details.
- The affected organization will no longer be able to deploy SDDCs linked to that account.

Note Re-running the VMware Cloud on AWS CloudFormation template does not affect existing SDDCs, which continue to use the IAM roles shown on their **Connected Amazon VPC** page. If an existing SDDC is exhibiting any of these symptoms, contact VMware Support.

Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.

You can also use the VMC Console **Networking & Security** tab for this workflow. The **Networking & Security** tab combines NSX-T **Networking** tab features like VPN, NAT, and DHCP with **Security** tab features like firewalls.

- 4 Click **Connected VPC** to open the **Connected Amazon VPC** page.

This page includes the following information:

AWS Account ID

The AWS account ID you specified when you created your SDDC.

VPC ID

The AWS ID of this VPC.

VPC Subnet

The AWS ID of the VPC subnet you specified when you created your SDDC.

Active Network Interface

The identifier for the ENI used by VMC in this VPC.

IAM Role Names

AWS Identity and Access Management role names defined in this VPC. See [AWS Roles and Permissions](#) in the *VMware Cloud on AWS Operations Guide*.

Cloud Formation Stack Names

The name of the AWS Cloud Formation stack used to create your SDDC

Service Access

A list of AWS services enabled in this VPC.

About NSX Advanced Firewall Features

4

The NSX Advanced Firewall add-on enables your SDDC to use advanced NSX-T features.

NSX-T Advanced Firewall for VMware Cloud on AWS features include:

- NSX-T [Layer 7 Context Profile](#)
- NSX-T [Distributed IDS/IPS](#)
- NSX-T [Identity Firewall](#)

To activate the NSX-T Advanced Firewall Add-On in your SDDC, open the **Add-Ons** tab and click **ACTIVATE** on the **NSX Advanced Firewall Add-On** card. After the add-on is activated, NSX-T advanced security features become available in our SDDC.

You can find detailed documentation for all of these features in the *VNSX-T Product Documentation*. There are a few operational differences between how the features work on on-premises NSX-T and how they work in VMware Cloud on AWS. For example, most of the procedures in the *NSX-T Product Documentation* include a step telling you to log in with admin privileges to an NSX Manager. This step isn't needed in VMware Cloud on AWS since clicking **OPEN NSX MANAGER** or opening the **Networking & Security** tab gives you admin access to the NSX manager in your SDDC. Other differences are listed in the following sections.

Using Context Profiles in the SDDC

Click the **Inventory Context Profiles**. You can specify a context profile in a distributed firewall rule by updating the value in the **Profiles** column of the **Distributed Firewall** grid. For more information, see [Layer 7 Firewall Rule Workflow](#) in the *NSX-T Product Documentation*.

In VMware Cloud on AWS, context profiles are supported only for use with Distributed Firewall rules. They cannot be used with MGW or CGW firewall rules.

Using Distributed IDS/IPS in the SDDC

Click **Security > Distributed IDS/IPS**. For more information, see [Distributed IDS/IPS](#) in the *NSX-T Product Documentation*.

When using this feature in VMware Cloud on AWS, keep these operational differences in mind:

Per-Cluster enablement

To use this feature, enable it on one or more SDDC clusters. On the **Distributed IDS/IPS** page, click the **Settings** tab, then select one or more clusters under **Enable Intrusion Detection and Prevention for Cluster(s)**. Because vMotion does not currently check the IDS/IPS -enablement status of a cluster before migrating VMs, we recommend enabling this feature on all clusters so that migration does not affect the application of IDS/IPS to any workload VM.

No access to hosts

Because VMware Cloud on AWS does not allow you to access SDDC hosts, you cannot [Verify Distributed IDS Status on Host](#). In addition, [Distributed IDS/IPS Events](#) are not available.

Logging

In VMware Cloud on AWS, events generated by this feature are logged to VMware vRealize Log Insight Cloud.

Using Identity Firewall in the SDDC

Click the **System > Identity Firewall AD** to add an SDDC Active Directory domain so that you can create user-based Identity firewall rules. When using this feature in VMware Cloud on AWS, keep these operational differences in mind:

Enable the feature for one or more SDDC clusters

Before you can use this feature, you have to take the "Configure Identity Firewall settings" step in [Manage Distributed Firewall Rules](#) to enable the feature and apply it to one or more SDDC clusters.

Create a firewall rule to allow Active Directory access

If you're using Active Directory, you'll also need to create a Management Gateway Firewall rule to allow NSX-T to access the Active Directory server you want to use. This feature doesn't work if access to Active Directory is interrupted in your SDDC, so it's important to make sure that the firewall rule you create here remains valid in the face of changes to the Active Directory server. For more information, see [Add an Active Directory](#) in the *NSX-T Product Documentation*.

Distributed FQDN filtering

In VMware Cloud on AWS, NSX-T FQDN filtering is supported only for use with Distributed Firewall rules. It cannot be used with MGW or CGW firewall rules. To use this feature, start by adding a DNS snooping rule, described in [Filtering Specific Domains \(FQDN/URLs\)](#), as the first rule in the policy. You must also enable the predefined **FQDNfiltering-spoofguard-profile** segment profile for all segments on which you want to support FQDN filtering. See [Create or Modify a Network Segment](#) for information about applying a segment profile to an SDDC network segment.

Logging

In VMware Cloud on AWS, events generated by this feature are logged to VMware vRealize Log Insight Cloud.

Deactivating the NSX Advanced Firewall Add-On

Before you can deactivate the NSX-T Advanced Firewall add-on, you must remove all firewall rules that reference add-on features. This includes:

- All distributed firewall rules that include a context profile
- All distributed IDS/IPS rules and profiles
- All identity-based firewall rules

After you have removed these objects, you can deactivate the add-on:

- 1 Open the **Add-Ons** tab in your SDDC.
- 2 On the **NSX Advanced Firewall Add-On** card, click **ACTIONS > Deactivate**.
- 3 Review the list of objects that must be removed prior to deactivation. When you are sure that the objects have been removed, click **CONFIRM DEACTIVATION**.

Billing for the add-on stops as soon as deactivation is completed.