

Connecting to the Cisco SWAT SD-WAN Lab Environment

Summary: Understanding the connection methodology for accessing the SWAT SD-WAN Lab Environment

Table of Contents

- [Introduction](#)
- [Downloading and Installing Cisco AnyConnect](#)
- [Connect to the Cisco SWAT SD-WAN Labs](#)

⚠ Warning: Please disable the side navigation bar if viewing this on a mobile device/small screen (there is an option to do so in the top navigation menu). The sidebar doesn't work too well with small screen devices. If the top navigation menu is not visible, look for a menu icon (three lines) in the top right corner.

Introduction

Welcome to the Cisco SWAT SD-WAN Labs. Please take a moment to go through this and the Overview section, which will cover important information about the lab.

Lab activities start from **Bringing up the DC-vEdges** but some sections might already be done, based on the chosen scenario. For most cases, Lab Activities should go as per the following order:

- Deploying Devices in Site 20 and Site 30
 - Deploying vEdge30 - Dual uplink
- Deploying Devices in Site 40 and Site 50
 - Deploying cEdge40 - Dual uplink
- Configuring Templates

Note that we are skipping a couple of portions of the lab (namely *Bringing up the DC vEdges*, *Deploying vEdge20 - Single INET uplink*, *Deploying vEdge21 - Single MPLS uplink*, *Deploying cEdge50 and cEdge51*) since these Sites have already been deployed. The sections are kept in the guide for reference.

(The rest of the sections are to be followed in order)

Connecting to the Cisco SWAT SD-WAN Labs is encompassed in this section. You will receive an email with the following information (or it will be provided to you by your SWAT contact):

- The Data Center (SLC or GHI) your POD is scheduled on and the POD number, along with the group
- VPN Credentials and connection information
- IP Address of the Jumphost/Guacamole

All lab activities need to be performed through the Jumphost/Guacamole.

Downloading and Installing Cisco AnyConnect

Note: This section needs to be done only if you **don't** have AnyConnect already installed on your workstation.

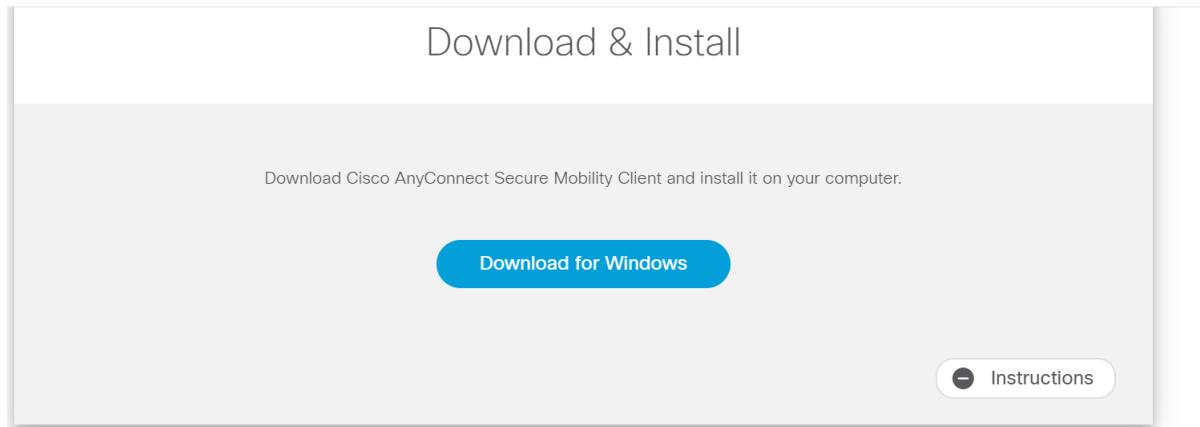
1. Click over here [here](https://14.140.162.5/+CSCOE+/lc) and you should be prompted to enter the VPN credentials. Choose the correct Group and enter the credentials provided for your POD. Click on **Login**. The URL is <https://14.140.162.5/>, for reference



| | |
|----------|-------------------|
| Group | SWAT_Lab_GHI_Pod1 |
| Username | testuser |
| Password | [REDACTED] |

Logon

- Once logged in, click on **Continue** and you should get a prompt to Download AnyConnect for your OS (Windows or Mac). Click on the Download button and save the file. Click on **Instructions** (lower right-hand corner) for a step by step procedure on how to install Cisco AnyConnect for your OS, if you are running into issues with it



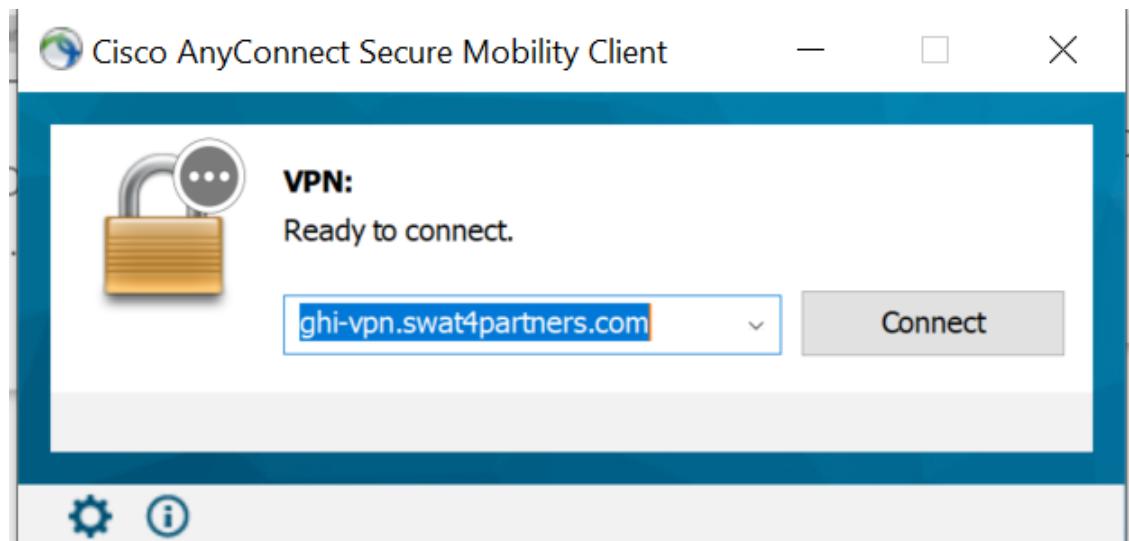
INSTRUCTIONS



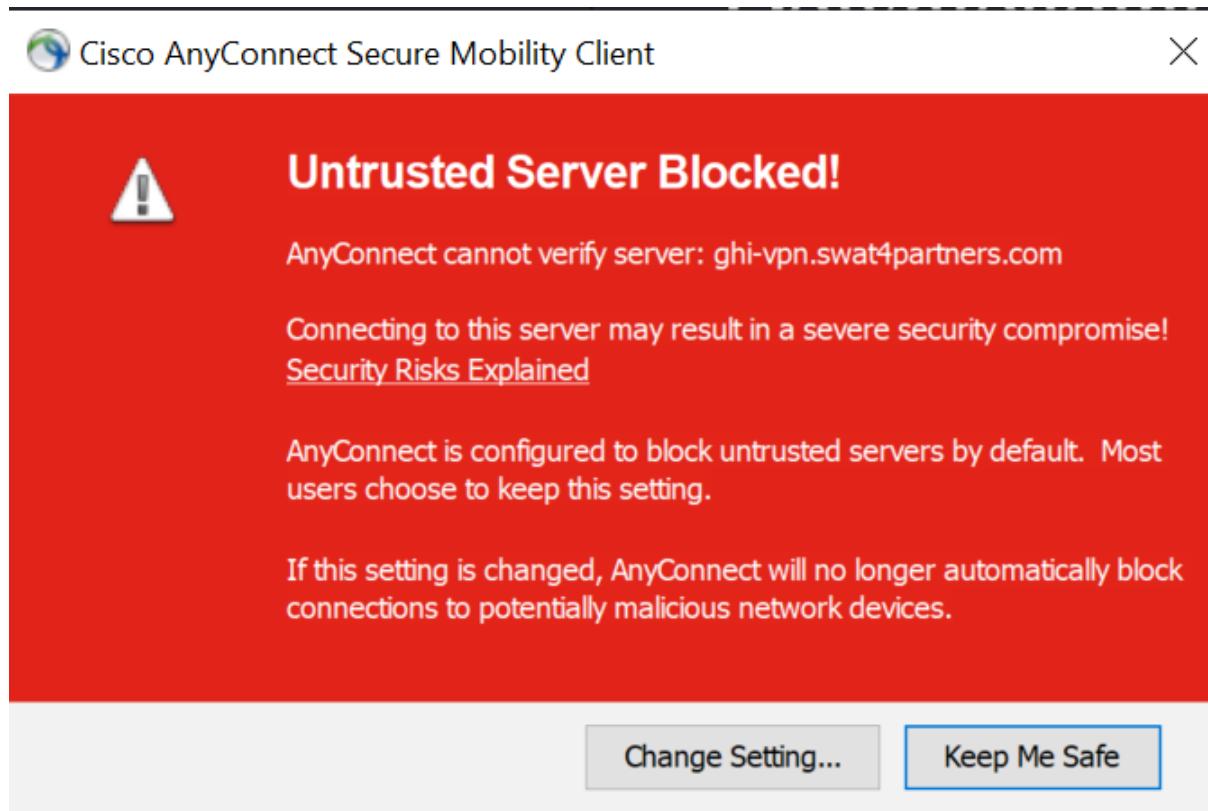
Install AnyConnect and move on to the **Connect to the Cisco SWAT SD-WAN Labs** section.

Connect to the Cisco SWAT SD-WAN Labs

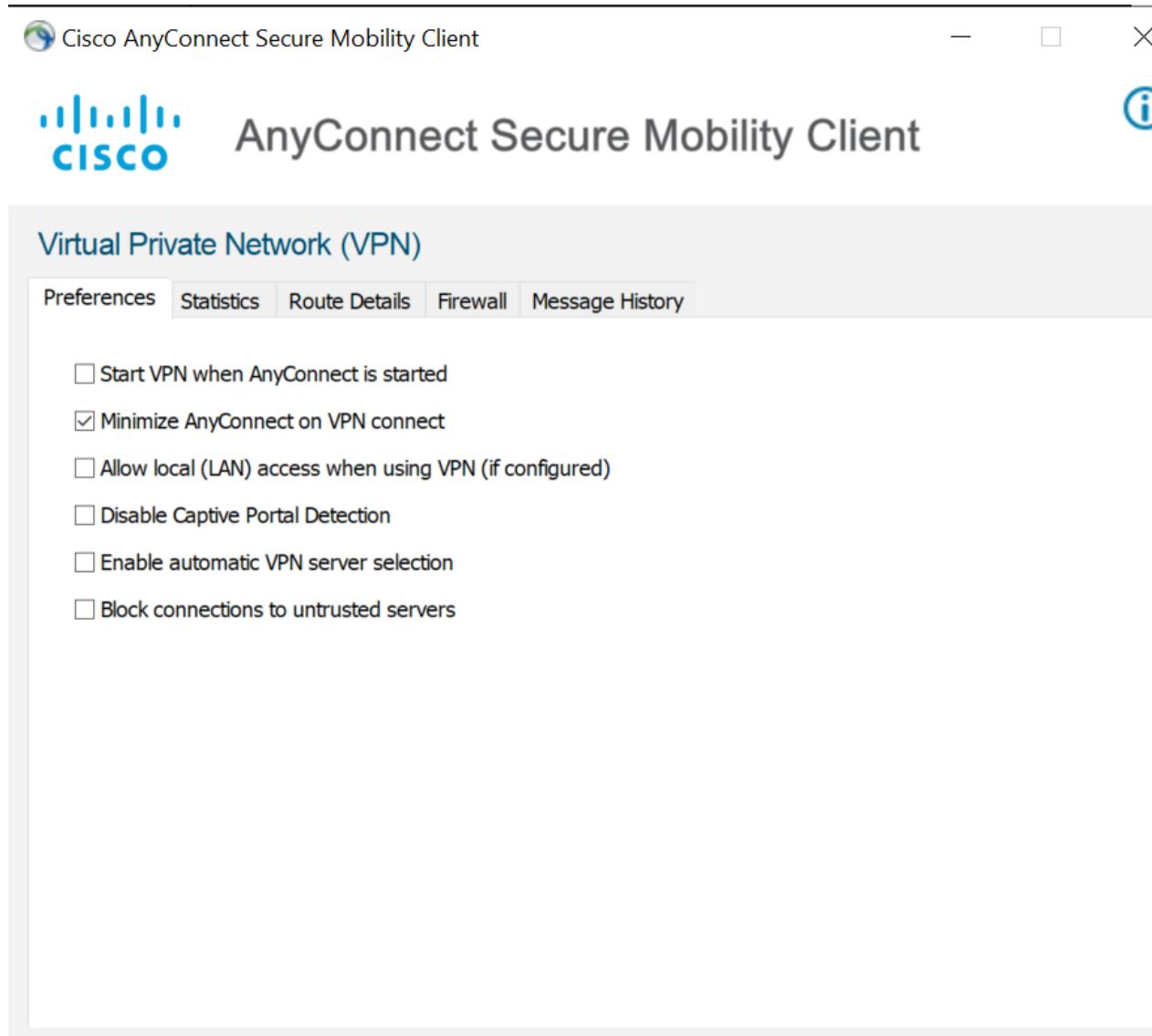
- Once AnyConnect is installed, enter the destination URL provided to you in the email or by the SWAT contact and click on **Connect**



2. If you get an error like the one below, click on **Change Setting**, else skip to Step 5



3. After clicking on **Change Setting**, make sure you **uncheck** the last option in the Preferences tab - i.e. **Block connections to untrusted servers** should be **unchecked**



4. Once unchecked, close the Preferences window and click on **Connect** again - the error should not show up anymore.
Click on **Connect Anyway** in the Security Warning



Security Warning: Untrusted Server Certificate!

AnyConnect cannot verify server: ghi-vpn.swat4partners.com

Certificate does not match the server name.

Certificate is from an untrusted source.

Connecting to this server may result in a severe security compromise!

[Security Risks Explained](#)

Most users do not connect to untrusted servers unless the reason for the error condition is known.

Connect Anyway

Cancel Connection

-
5. Click on **Connect Anyway** if you've skipped over here from Step 2. If you've come from Step 4, this is already done and you can proceed.



Security Warning: Untrusted Server Certificate!

AnyConnect cannot verify server: ghi-vpn.swat4partners.com

Certificate does not match the server name.
Certificate is from an untrusted source.

Connecting to this server may result in a severe security compromise!

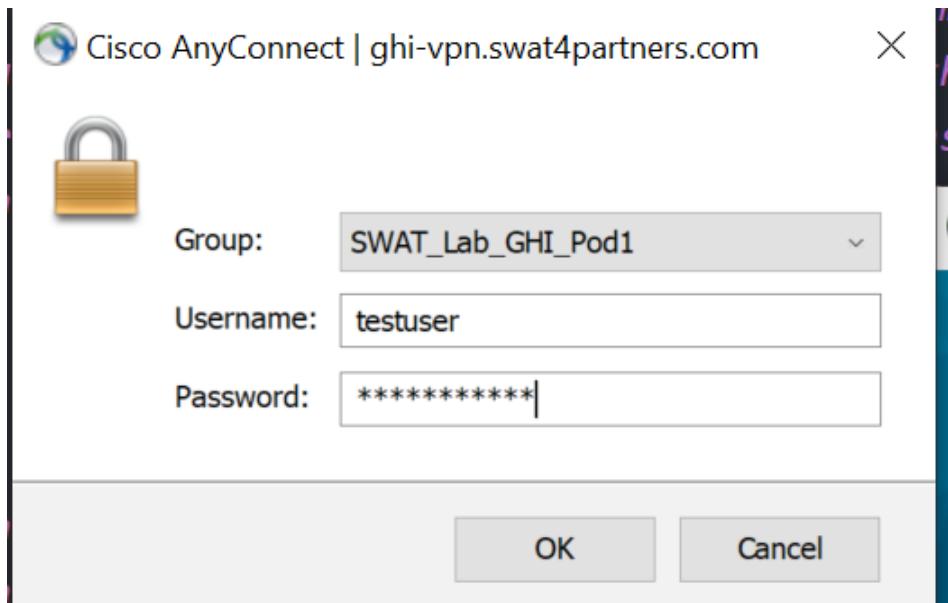
[Security Risks Explained](#)

Most users do not connect to untrusted servers unless the reason for the error condition is known.

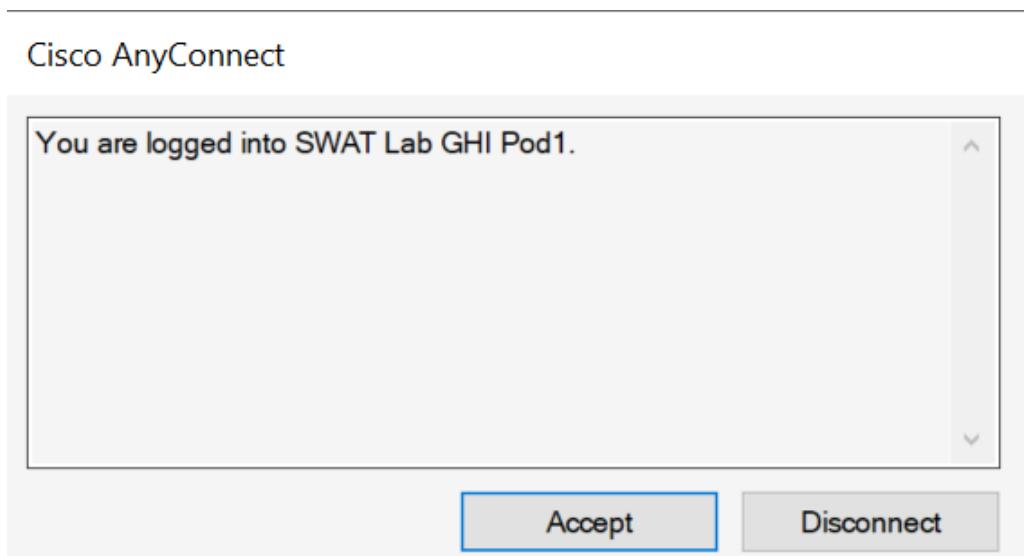
Connect Anyway

Cancel Connection

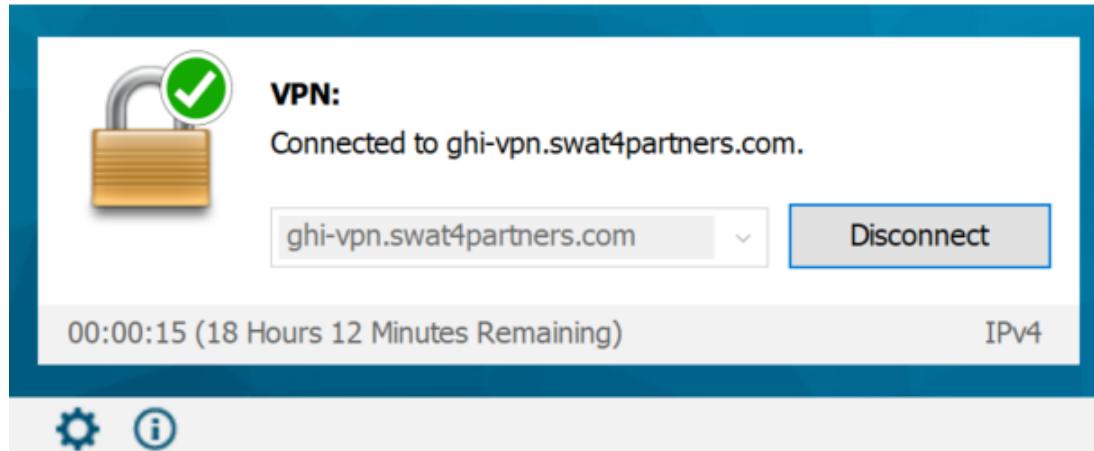
-
6. You should be prompted for your username/password and provided with a drop down to select a Group. Please make sure you choose the correct Group as per your POD and enter the VPN credentials provided for your POD. Click on **OK**



7. You should be presented with a popup - click on **Accept**



8. The VPN connection should be successful and the window will auto-minimize. Open AnyConnect and you should see your connection status to the Cisco SWAT SD-WAN Labs



You should now be able to RDP to the Jumphost for your POD. If things aren't working as expected, please use the **Need Help?** link at the top of the page (or check with your SWAT contact) to send an email to our support team and someone will get in touch with you at the earliest. If the Need Help? link isn't visible, there should be a menu on the top-right of the screen. Click on it to display the Top Navigation Bar.

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: June 6, 2020

Site last generated: Sep 1, 2020



Getting started with the SWAT SD-WAN Labs

Summary: These brief instructions will help you become familiar with the SWAT SD-WAN Lab Guide conventions.

Table of Contents

- [This header will have a generated hyperlink for navigation](#)
 - [Sub headers will look like this](#)

Given below are a few of the conventions used in this lab guide. Each point enunciated below doubles up as an example.

This header will have a generated hyperlink for navigation

In order to move around in the document and skip to particular sections, use the sidebar and/or the header hyperlink.

Sub headers will look like this

These can also be navigated to via the Index at the top of the page

A block of commands like this one
can be copied and pasted
directly to the CLI

Text in bold is usually important. Standalone commands will be distinguishable from the rest of the text

A [Hyperlink](#) will direct you to additional technical documentation associated with the section you're working on.

1. Steps to be followed as part of the lab guide have an associated image as a visual aid



2. Some steps will also have a table with information useful for that section of the guide

| Tables are | Cool |
|--------------|-----------|
| Cisco SD-WAN | is cooler |

Tip: Techtips will be highlighted like this. These include nifty tips and tricks from our SD-WAN Experts

i Note: A friendly, neighbourhood note will look like this

⚠ Important: When something important needs to be highlighted

❗ Warning: Things may go horribly wrong if these warning messages aren't taken into account

Task List

- Every major section will have a task list
- Which we will ~~strike out once complete~~

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Site last generated: Sep 1, 2020



-->

Network Details

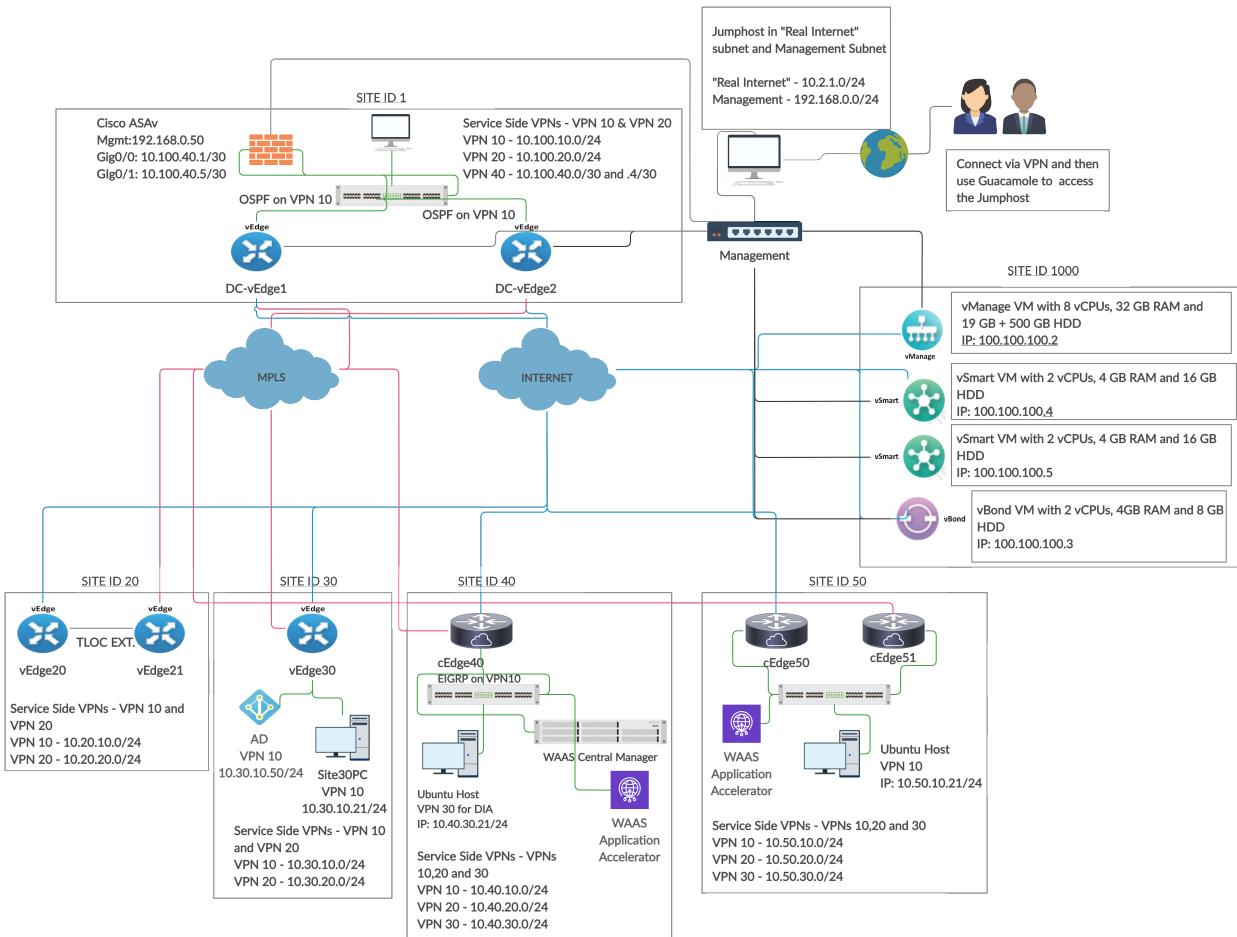
Table of Contents

- [Lab Topology](#)
- [Device Credentials](#)
- [Network schema](#)

Lab Topology

Given below is the lab topology being used for the SWAT SD-WAN Labs

i Note: There might be minor differences in the topology being used versus what you see here. We will keep this updated as far as possible



Decoding the topology:

- There are a total of 5 sites where we will have cEdges/vEdges deployed
- All sites have Service VPNs associated with them.
 - Sites with vEdges have 2 service VPNs (VPN10 and VPN20)
 - Sites with cEdges have 3 service VPNs (VPN10, VPN20 and VPN30)
- Some devices have dual uplinks (MPLS and Internet) while others have single uplinks (MPLS only or Internet only)
- Site DC (Site ID 1) is running OSPF on the LAN. Site 50 is running EIGRP on the LAN
- Site 20 will have TLOC Extensions set up and we will be peering with the MPLS side via eBGP
- cEdge40 and cEdge50 will function as AppNav-XE Controllers

Device Credentials

Given below are the access details for some key devices in the network

| Device | Access Method | Username | Password | IP Address/URL |
|-----------------------------|-----------------|----------------------|-------------|----------------------|
| vManage | Browser - GUI | admin | admin | 192.168.0.6 |
| vEdges and cEdges | Putty | admin | admin | Various |
| Central Gateway | Putty | admin | admin | 192.168.0.1 |
| Ubuntu - Site 40 PC | vCenter Console | sdwan | C1sco12345 | 10.40.30.21 |
| Ubuntu - Site 50 PC | vCenter Console | sdwan | C1sco12345 | 10.50.10.21 |
| Jumphost | RDP/Guacamole | admin | C1sco12345 | 10.2.1.22X |
| | | | | X is your POD number |
| vCenter | Browser - GUI | sdwanpodX | C1sco12345 | 10.2.1.50 |
| | | X is your POD number | | |
| | | e.g. sdwanpod5 | | |
| Site 30 AD | RDP/Guacamole | administrator | C1sco12345 | 10.30.10.50 |
| Domain: swatsdwanlab.com | | | | |
| Site 30 PC | RDP/Guacamole | swatsdwanlab\sdwan | C1sco12345 | 10.30.10.21 |
| Cisco Umbrella | Browser - GUI | ghi.pod0X@gmail.com | C1sco@12345 | login.umbrella.com |
| | | X is your POD number | | |

| | | | | |
|----------------------|---------------|----------|------------|---------------------------|
| Guacamole | Browser - GUI | sawanpod | C1sco12345 | 10.2.1.20X:8080/guacamole |
| X is your POD number | | | | |
| WAAS Central Manager | Browser - GUI | admin | admin | 10.40.30.123 |

Network schema

⚠ Important: Needless to say, these are super important and the IP Addressing scheme should be followed as enumerated in the lab guide

Use the following table to copy-paste IP Addresses as and when required through the course of the lab. There is a search function which is super handy - search with the name of the VM you are looking for so as to return complete results.

- If the POD assigned to you is in location SLC

- y (in the table below) is 1
- X is your POD number

- If the POD assigned to you is in location GHI

- y (in the table below) is 2
- X is your POD number

VM names need to be used accordingly.

| VM TAG FOR IDENTIFICATION ONLY NOT USED IN THE LAB | SITE ID | SYSTEM ID | VM Name | Network Adapter | Network Adapter | Interface | IP | Gateway |
|---|------------|--------------|-----------------|--------------------|--------------------|-----------|----------------|-------------|
| A vManage | 1000 | 10.255.255.1 | sdwan-slc/ghi-1 | Network Adapter | Management | eth1 | 192.168.0.6/24 | 192.168.0.1 |

| vmanage-podX | | | | | | | |
|----------------|--------------|----------------------------|-------------------|-------------------|------------|-------|--------------------------------|
| A vManage | | | Network Adapter 2 | Internet | | eth0 | 100.100.100.2/24 100.100.100.1 |
| B vBond | 10.255.255.2 | sdwan-slc/ghi-vbond-podX | Network Adapter 1 | Management | | eth1 | 192.168.0.7/24 192.168.0.1 |
| B vBond | | | Network Adapter 2 | Internet | | eth0 | 100.100.100.3/24 100.100.100.1 |
| C vSmart | 10.255.255.3 | sdwan-slc/ghi-vsmart-podX | Network Adapter 1 | Management | | eth1 | 192.168.0.8/24 192.168.0.1 |
| C vSmart | | | Network Adapter 2 | Internet | | eth0 | 100.100.100.4/24 100.100.100.1 |
| D vSmart2 | 10.255.255.4 | sdwan-slc/ghi-vsmart2-podX | Network Adapter 1 | Management | | eth1 | 192.168.0.9/24 192.168.0.1 |
| D vSmart2 | | | Network Adapter 2 | Internet | | eth0 | 100.100.100.5/24 100.100.100.1 |
| E DC-vEdge1 | 1 | 10.255.255.11 | DC-vEdge1-podX | Network Adapter 1 | Management | eth0 | 192.168.0.10/24 192.168.0.1 |
| E DC-vEdge1 | | | Network Adapter 2 | MPLS10 | | ge0/1 | 192.0.2.2/30 192.0.2.1 |

| | | | | | | | | |
|----------------|---------------|----------------|-------------------|-------------------|------------|-------------------|-----------------|-------------|
| E DC-vEdge1 | | | Network Adapter 3 | SiteDC_VPN10 | ge0/2 | 10.100.10.2/24 | 10.100.10.1 | |
| E DC-vEdge1 | | | Network Adapter 4 | SiteDC-VPN20 | ge0/3 | 10.100.20.2/24 | 10.100.20.1 | |
| E DC-vEdge1 | | | Network Adapter 5 | Internet | ge0/0 | 100.100.100.10/24 | 100.100.100.1 | |
| F DC-vEdge2 | 10.255.255.12 | DC-vEdge2-podX | Network Adapter 1 | Management | eth0 | 192.168.0.11/24 | 192.168.0.1 | |
| F DC-vEdge2 | | | Network Adapter 2 | MPLS11 | ge0/1 | 192.0.2.6/30 | 192.0.2.5 | |
| F DC-vEdge2 | | | Network Adapter 3 | SiteDC_VPN10 | ge0/2 | 10.100.10.3/24 | 10.100.10.1 | |
| F DC-vEdge2 | | | Network Adapter 4 | SiteDC-VPN20 | ge0/3 | 10.100.20.3/24 | 10.100.20.1 | |
| F DC-vEdge2 | | | Network Adapter 5 | Internet | ge0/0 | 100.100.100.11/24 | 100.100.100.1 | |
| G vEdge20 | 20 | 10.255.255.21 | vEdge20-podX | Network Adapter 1 | Management | eth0 | 192.168.0.20/24 | 192.168.0.1 |
| G vEdge20 | | | Network Adapter 2 | TLOCEXT_vEDGE | ge0/1 | 192.168.25.20/24 | | |
| G | | | Network | Site20-VPN10 | ge0/2 | 10.20.10.2/24 | | |

| | | | | | | | | |
|-----------|---------------|-------------------|-------------------|-----------------|-------------------|------------------|-----------------|-------------|
| vEdge20 | | Adapter 3 | | | | | | |
| G vEdge20 | | Network Adapter 4 | Site20-VPN20 | ge0/3 | 10.20.20.2/24 | | | |
| G vEdge20 | | Network Adapter 5 | Internet | ge0/0 | 100.100.100.20/24 | 100.100.100.1 | | |
| G vEdge20 | | Network Adapter 6 | TLOCEXT2_vEdge | ge0/4 | 192.168.26.20/24 | | | |
| H vEdge21 | 10.255.255.22 | vEdge21-podX | Network Adapter 1 | Management | eth0 | 192.168.0.21/24 | 192.168.0.1 | |
| H vEdge21 | | | Network Adapter 2 | TLOCEXT_vEDGE | ge0/1 | 192.168.25.21/24 | | |
| H vEdge21 | | | Network Adapter 3 | Site20-VPN10 | ge0/2 | 10.20.10.3/24 | | |
| H vEdge21 | | | Network Adapter 4 | Site20-VPN20 | ge0/3 | 10.20.20.3/24 | | |
| H vEdge21 | | | Network Adapter 5 | MPLS20 | ge0/0 | 192.0.2.10/30 | 192.0.2.9 | |
| H vEdge21 | | | Network Adapter 6 | TLOCEXT2_vEdge | ge0/4 | 192.168.26.21/24 | | |
| I vEdge30 | 30 | 10.255.255.31 | vEdge30-podX | Network Adapter | Management | eth0 | 192.168.0.30/24 | 192.168.0.1 |

| | | | | | | | | | |
|---|---------|----|-------------------|--------------|-------------------|--------------|-------------------|-----------------|---------------|
| | | | | | 1 | | | | |
| I | vEdge30 | | Network Adapter 2 | MPLS30 | | ge0/1 | 192.0.2.14/30 | 192.0.2.13 | |
| I | vEdge30 | | Network Adapter 3 | Site30-VPN10 | | ge0/2 | 10.30.10.2/24 | | |
| I | vEdge30 | | Network Adapter 4 | Site30-VPN20 | | ge0/3 | 10.30.20.2/24 | | |
| I | vEdge30 | | Network Adapter 5 | Internet | | ge0/0 | 100.100.100.30/24 | 100.100.100.1 | |
| J | cEdge40 | 40 | 10.255.255.41 | cEdge40-podX | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.40/24 | 192.168.0.1 |
| J | cEdge40 | | | | Network Adapter 2 | Internet | GigabitEthernet2 | 100.100.100.40 | 100.100.100.1 |
| J | cEdge40 | | | | Network Adapter 3 | MPLS40 | GigabitEthernet3 | 192.1.2.18/30 | 192.1.2.17 |
| J | cEdge40 | | | | Network Adapter 4 | Site40-VPN10 | GigabitEthernet4 | 10.40.10.2/24 | |
| J | cEdge40 | | | | Network Adapter 5 | Site40-VPN20 | GigabitEthernet5 | 10.40.20.2/24 | |
| J | cEdge40 | | | | Network Adapter 6 | Site40-VPN30 | GigabitEthernet6 | 10.40.30.2/24 | |

| | | | | | | | | |
|---|---------------|---------------|-------------------|-------------------|------------------|------------------|-------------------|---------------|
| K | 50 | 10.255.255.51 | cEdge50-podX | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.50/24 | 192.168.0.1 |
| K | | | | Network Adapter 2 | Internet | GigabitEthernet2 | 100.100.100.50/24 | 100.100.100.1 |
| K | | | | Network Adapter 3 | Site50-VPN10 | GigabitEthernet3 | 10.50.10.2/24 | |
| K | | | | Network Adapter 4 | Site50-VPN20 | GigabitEthernet4 | 10.50.20.2/24 | |
| K | | | | Network Adapter 5 | Site50-VPN30 | GigabitEthernet5 | 10.50.30.2/24 | |
| L | 10.255.255.52 | cEdge51-podX | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.51/24 | 192.168.0.1 | |
| L | | | Network Adapter 2 | MPLS50 | GigabitEthernet2 | 192.1.2.22/30 | | 192.1.2.21 |
| L | | | Network Adapter 3 | Site50-VPN10 | GigabitEthernet3 | 10.50.10.3/24 | | |
| L | | | Network Adapter 4 | Site50-VPN20 | GigabitEthernet4 | 10.50.20.3/24 | | |
| L | | | Network Adapter 5 | Site50-VPN30 | GigabitEthernet5 | 10.50.30.3/24 | | |
| M | NA | NA | sdwan- | Network | Site40-VPN30 | Virtual 1/0 | 10.40.30.123/24 | 10.40.30.1 |

| | | | | | | | |
|-----------------|----|--------------------------|-----------------------------|-------------------|-------------------------|------------------|--------------------|
| WAAS | | slc/ghi-wcm-podX | Adapter 1 | | | | |
| N WAAS | | sdwan-slc/ghi-waa40-podX | Network Adapter 1 | Site40-VPN30 | Virtual 1/0 | 10.40.30.46/24 | 10.40.30.1 |
| O WAAS | | sdwan-slc/ghi-waa50-podX | Network Adapter 1 | Site50-VPN30 | Virtual 1/0 | 10.50.30.46/24 | 10.50.30.1 |
| P Central GW | NA | NA | sdwan-slc/ghi-gw-podX | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.1 |
| P Central GW | | | | Network Adapter 2 | WAN-Trunk | GigabitEthernet2 | All DGs point here |
| P Central GW | | | | Network Adapter 3 | Shared_Services_VLAN101 | GigabitEthernet3 | 10.2.1.24X/24 |
| Q Guacamole | NA | NA | sdwan-slc/ghi-guac-podX | Network Adapter 1 | Shared_Services_VLAN101 | eth0 | 10.2.1.20X/24 |
| R Jumphost | NA | NA | sdwan-slc/ghi-jump-podX | Network Adapter 1 | Shared_Services_VLAN101 | eth0 | 10.2.1.22X/24 |
| S Site 40 PC | 40 | NA | sdwan-slc/ghi-site40pc-podX | Network Adapter 1 | Site40-VPN30 | eth0 | 10.40.30.21/24 |
| | | | | | | | |

| | | | | | | | | |
|---|----|----|-----------------------------|-------------------|-------------------------|---------------|-----------------|--------------|
| T | 50 | NA | sdwan-slc/ghi-site50pc-podX | Network Adapter 1 | Site50-VPN10 | eth0 | 10.50.10.21/24 | 10.50.10.100 |
| U | 30 | NA | sdwan-slc/ghi-ad-podX | Network Adapter 1 | Site30-VPN10 | eth0 | 10.30.10.50/24 | 10.30.10.2 |
| U | | | | Network Adapter 2 | Shared_Services_VLAN101 | eth1 | 10.2.1.18X | |
| V | 30 | NA | sdwan-slc/ghi-site30pc-podX | Network Adapter 1 | Site30-VPN10 | eth0 | 10.30.10.21/24 | 10.30.10.2 |
| V | | | | Network Adapter 2 | Shared_Services_VLAN101 | eth1 | 10.2.1.16X | |
| W | 1 | NA | sdwan-slc/ghi-asa-podX | Network Adapter 1 | Management | Management0/0 | 192.168.0.50/24 | 192.168.0.1 |
| W | | | | Network Adapter 2 | SiteDC-VPN40 | Gig0/0 | 10.100.40.1/30 | 10.100.40.2 |
| W | | | | Network Adapter 3 | SiteDC-VPN40_2 | Gig0/1 | 10.100.40.5/30 | 10.100.40.6 |

[Click here](#) to download a printable version of this table, for reference.



Before you begin

Table of Contents

- [Prerequisites](#)
 - [What will you need?](#)
 - [What should you know?](#)
- [Objectives](#)
 - [What will you learn?](#)

Prerequisites

What will you need?

- A workstation with Windows or MacOS installed
- Cisco AnyConnect. This can be downloaded from [here](#) after logging in with the credentials provided
- A stable internet connection that has standard Cisco AnyConnect ports allowed

Note: It is recommended to open this Lab Guide on one screen and perform lab activities on another

Important: It is HIGHLY recommended to use Google Chrome. Download the Clipboard Permission Manager Extension for Chrome. While accessing the POD via Guacamole, allow Clipboard Permission Manager access and you will be able to copy-paste content directly into the Guacamole window (Guacamole has an inconvenient way of handling copy-paste operations).

What should you know?

- Fundamental knowledge of Routing & Switching with a few details of Data Center operations

- Familiarity with Cisco SD-WAN as a solution and its architecture/protocols. A few helpful links can be found in the top navigation bar under **SD-WAN Documentation**
- Knowledge of Cisco WAAS and NGIPS concepts is an added advantage

Objectives

What will you learn?

This lab has multiple use cases that are covered as part of the tasks. We are working on expanding this list as and when new features are tested/released.

- Deploying vEdges and cEdges in a virtual environment
- Onboarding devices on vManage
 - Manual Onboarding of vEdges and cEdges
 - Day 0 bootstrapping of cEdges
- Working with Configuration Templates
 - Bringing up cEdges and vEdges with Single uplinks
 - Bringing up cEdges and vEdges with Dual uplinks
- Implementing Service VPNs and Dynamic Service Side routing using OSPF and EIGRP
 - Establishing OSPF adjacencies at DC with route redistribution
 - Establishing EIGRP adjacencies at Site 40 with route redistribution
 - Configuring VRRP at Site 50
- Implementing TLOC Extensions with eBGP Peering
- Working with Control Policies
 - Enforcing a Hub and Spoke Topology
 - Implementing a Regional Hub
- Implementing Data Policies
 - Custom traffic Engineering
 - Direct Internet Access
- Application Aware Routing

- Influencing Traffic Path selection
- Introducing Packet Loss via Policers
- Cisco SD-WAN Security
 - IPS Deployment at DIA Sites
 - URL Filtering at DIA Site
 - Cisco SD-AVC
- Cloud On-Ramp for SaaS
 - Injecting delay via a traffic shaper

Happy Labbing!

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.
Site last generated: Sep 1, 2020



Deploying and Onboarding DC-vEdge1

[Take a tour of this page](#)

Summary: Step by step process for deploying DC-vEdge1

Table of Contents

- [Verifying the existing lab setup](#)
- [Creating the DC-vEdge1 VM](#)
 - [Overview](#)
 - [Deploying the VM on vCenter](#)
- [Onboarding DC-vEdge1](#)
 - [Bootstrapping DC-vEdge1 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

⚠ Warning: This section might already be done, depending on your selected Lab Scenario. Most lab work will start [from here](#). The configuration given below can be used to review what was done to bring the Site up. If this VM is already deployed (check via vCenter), you **Do Not** need to perform these lab activities.

Task List

- Verifying the existing lab setup
- Creating the DC-vEdge1 VM
- Overview
- Deploying the VM on vCenter
- Onboarding DC-vEdge1

- Bootstrapping DC-vEdge1 (Initial Configuration)
- Installing certificates and activating the vEdge
- Onboarding Verification
- Helpful debugs and logs

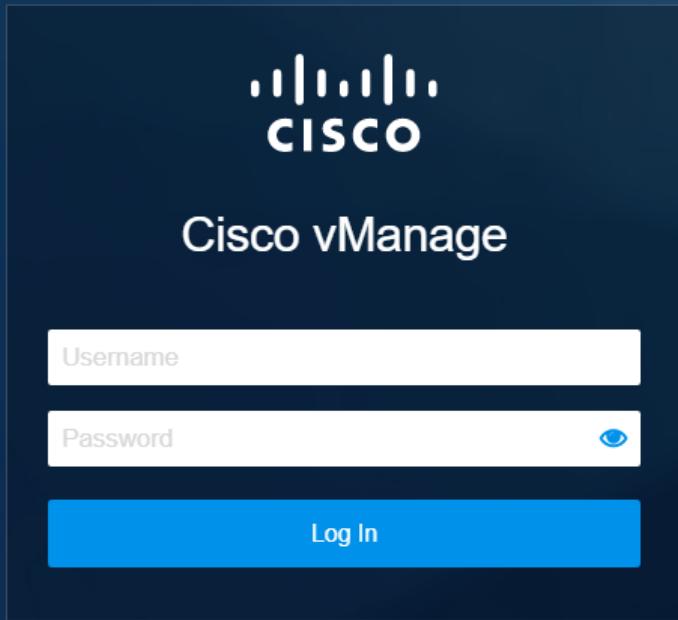
Verifying the existing lab setup

The vManage, vBond and vSmarts have been deployed and should be ready to accept control connections from vEdges and cEdges. We will start by verifying the existing setup.

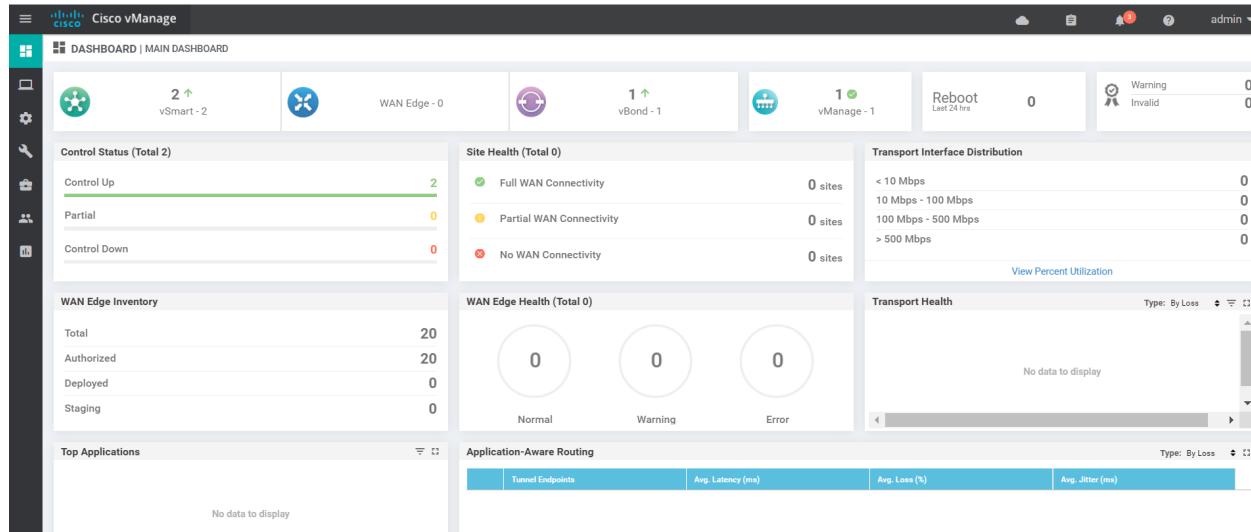
1. Log in to vManage by clicking on the bookmark or navigating to <https://192.168.0.6>. Use the following credentials:

| Username | Password |
|----------|----------|
| admin | admin |

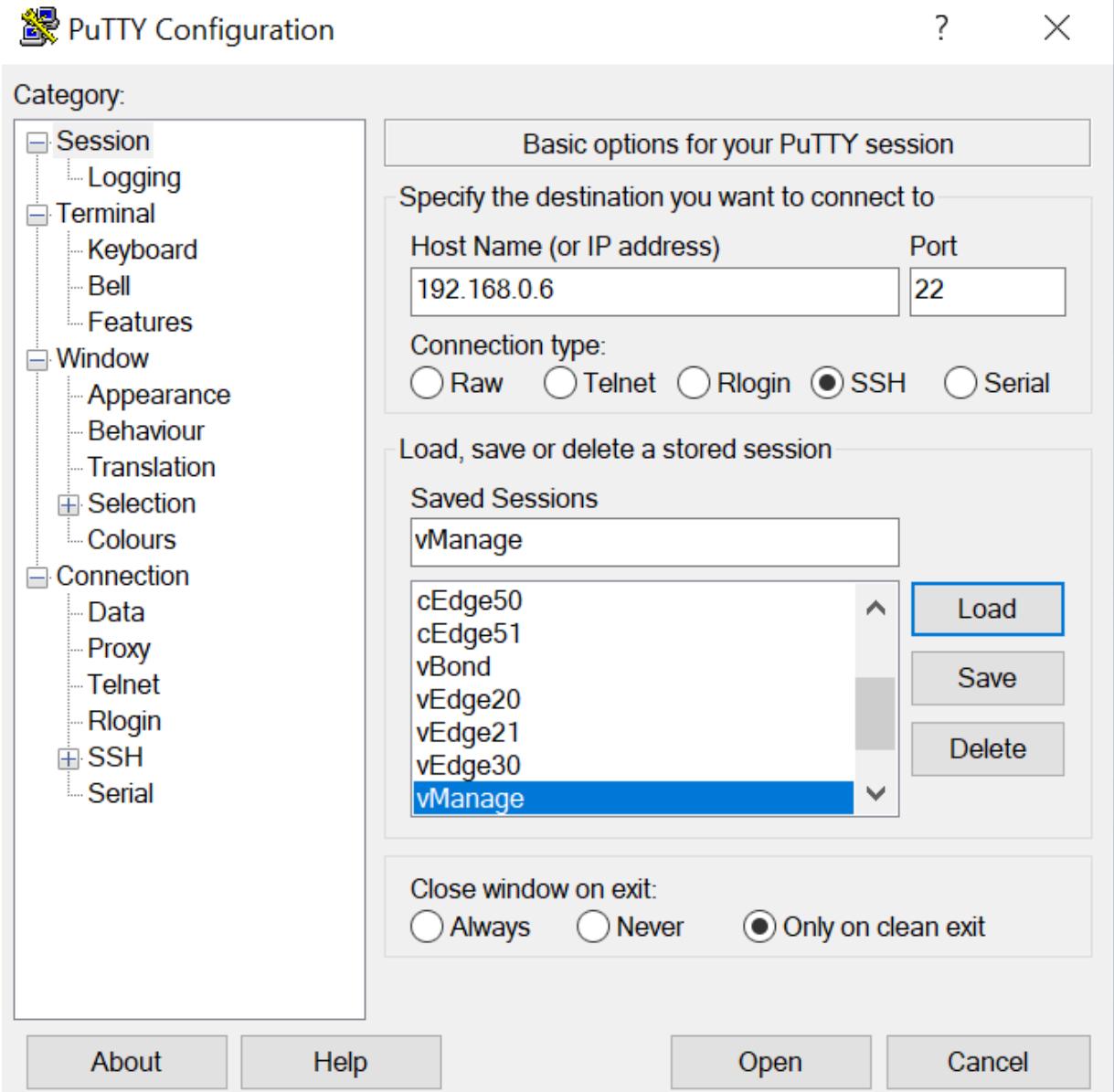
Cisco SD-WAN



2. On logging in, you should see 2 vSmarts, 1 vBond and 1 vManage along the top row and 2 control planes should be up (naming convention might vary)



3. Open and log in to the vManage via the CLI - fire up Putty and double click the saved session for vManage or SSH to 192.168.0.6. Use the same credentials as the GUI.



4. Issue `show control connections` and you should see the vManage talking to the vSmarts and the vBond.

| INDEX | TE COLOR | PEER | | | | PEER | | | |
|-------|----------|------|--------------|------------------|-----------|--------|---------------|------------|----------------|
| | | PEER | PEER PEER | CONFIGURED | SITE | DOMAIN | PEER | PRIV | PEER |
| | | TYPE | PROT STATE | SYSTEM IP UPTIME | SYSTEM IP | ID | ID | PRIVATE IP | PORT PUBLIC IP |
| 0 | vsmart | dtls | 10.255.255.3 | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12346 | 100.100.100.4 |
| ult | up | | 3:18:00:38 | | | | | | |
| 0 | vsmart | dtls | 10.255.255.4 | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12346 | 100.100.100.5 |
| ult | up | | 3:18:00:38 | | | | | | |
| 0 | vbond | dtls | 10.255.255.2 | 10.255.255.2 | 0 | 0 | 100.100.100.3 | 12346 | 100.100.100.3 |
| ult | up | | 3:18:00:38 | | | | | | |
| 1 | vbond | dtls | 0.0.0.0 | - | 0 | 0 | 100.100.100.3 | 12346 | 100.100.100.3 |
| ult | up | | 3:18:00:39 | | | | | | |

5. Additionally, you can log in to the CLI for the vBond via the saved link (and the same password as the vManage) and issue a `show orchestrator connections`

| IZATION | INSTANCE | PEER | | | | PEER | | | | PEER | | | | ORGAN | |
|---------|----------|------|--------------|--------------|------|--------|---------------|---------|---------------|--------|---------|--------|-------|----------|------------|
| | | PEER | PEER | PEER | SITE | DOMAIN | PEER | PRIVATE | PEER | PUBLIC | PORT | REMOTE | COLOR | STATE | |
| | | TYPE | PROTOCOL | SYSTEM IP | ID | ID | PRIVATE IP | PORT | PUBLIC IP | PORT | NAME | UPTIME | | | |
| 0 | vsmart | dtls | 10.255.255.3 | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12346 | 100.100.100.4 | 12346 | default | up | swat- | sdwanlab | 3:18:05:07 |
| 0 | vsmart | dtls | 10.255.255.3 | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12446 | 100.100.100.4 | 12446 | default | up | swat- | sdwanlab | 3:18:05:07 |
| 0 | vsmart | dtls | 10.255.255.4 | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12346 | 100.100.100.5 | 12346 | default | up | swat- | sdwanlab | 3:18:05:04 |
| 0 | vsmart | dtls | 10.255.255.4 | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12446 | 100.100.100.5 | 12446 | default | up | swat- | sdwanlab | 3:18:05:04 |
| 0 | vmanage | dtls | 10.255.255.1 | 10.255.255.1 | 1000 | 0 | 100.100.100.2 | 12346 | 100.100.100.2 | 12346 | default | up | swat- | sdwanlab | 3:18:04:38 |
| 0 | vmanage | dtls | 10.255.255.1 | 10.255.255.1 | 1000 | 0 | 100.100.100.2 | 12446 | 100.100.100.2 | 12446 | default | up | swat- | sdwanlab | 3:18:04:39 |

We see that the connections are up and this completes the verification activity.

Task List

- [Verifying the existing lab setup](#)
- [Creating the DC-vEdge1 VM](#)
- [Overview](#)
- [Deploying the VM on vCenter](#)
- [Onboarding DC-vEdge1](#)
- [Bootstrapping DC-vEdge1 \(Initial Configuration\)](#)
- [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

Creating the DC-vEdge1 VM

Overview

We will be deploying a vEdge in our first site (the Data Center) via vCenter. Make note of the following information for this section. The IP Addressing will not be used for some of the Network Adapters until later. X is your POD number and is used only during vCenter related activities.

Note: We will be using vEdge Clouds and CSR1000v images which are software images and don't support the standard Day 0 onboarding options. They do have a tweaked version of the Day 0 onboarding which we will be implementing later on in the lab. Hardware devices can do Day 0 onboarding (Zero Touch Provisioning)

| VM Name | System IP | Network Adapter | Network | Interface | IP Address | Default Gateway |
|----------------|---------------|-------------------|--------------|-----------|-------------------|-----------------|
| DC-vEdge1-podX | 10.255.255.11 | Network Adapter 1 | Management | eth0 | 192.168.0.10/24 | 192.168.0.1 |
| | | Network Adapter 2 | MPLS10 | ge0/1 | 192.0.2.2/30 | 192.0.2.1 |
| | | Network Adapter 3 | SiteDC_VPN10 | ge0/2 | 10.100.10.2/24 | 10.100.10.1 |
| | | Network Adapter 4 | SiteDC-VPN20 | ge0/3 | 10.100.20.2/24 | 10.100.20.1 |
| | | Network Adapter 5 | Internet | ge0/0 | 100.100.100.10/24 | 100.100.100.1 |

Tip: Plan your sites and addressing carefully. Proper planning can prevent a number of issues and will help with a successful, early deployment.

Tip: There is configuration applicable only to virtual vEdges/cEdges in some of the sections. Physical vEdges are a lot easier to deploy, not only from a connectivity standpoint but also with respect to certificate exchange options.

Task List

- [Verifying the existing lab setup](#)
- [Creating the DC-vEdge1 VM](#)
- [Overview](#)
- [Deploying the VM on vCenter](#)
- [Onboarding DC-vEdge1](#)
- [Bootstrapping DC-vEdge1 \(Initial Configuration\)](#)
- [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

Deploying the VM on vCenter

1. Click on the bookmark for vCenter or navigate to the following URL: <https://10.2.1.50/ui>. Log in with the credentials provided for your POD.



2. Notice that no vEdges/cEdges have been deployed on the host you've accessed. This is expected.

ghi-vcenter.swat4partner... ▾

- SWAT-Labs-GHI
- Management-Sha...
- ghi-ms01.swat4...
- ghi-ms02.swat4...
- ghi-ms03.swat4...
- ghi-ms04.swat4...**
- CentralGW
- ghi-ise04
- ghi-jump-p08
- ghi-jump-p09
- ghi-jump-p10
- GHI-SDWAN-...
- Site40_PC
- Ubuntu_Gua...
- Ubuntu_Site...
- VBond-P1
- vManage-P1
- vSmart-P1
- vSmart2-P1

Summary Monitor Configure Permissions VMs Resource Pools Datastores Networks Updates

Hypervisor: VMware ESXi, 6.7.0, 13006603
Model: UCSC-C220-M5SX
Processor Type: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz
Logical Processors: 56
NICs: 4
Virtual Machines: 13
State: Connected
Uptime: 164 days

Network uplink redundancy lost

Hardware Configuration

Tags Related Objects

Assigned Tag Category Description

None

3. Right click on the host and choose to Deploy OVF Template

ghi-vcenter.swat4partner... ▾

- SWAT-Labs-GHI
- ghi-ms04.swat4partners.com
- Actions - ghi-ms04.swat4partners.com
- New Virtual Machine...
- Deploy OVF Template...**
- New Resource Pool...
- New vApp...
- Maintenance Mode
- Connection
- Power
- Certificates
- Storage
- Add Networking...
- Host Profiles
- Export System Logs...
- Reconfigure for vSphere HA

Summary Monitor Configure Permissions VMs Resource Pools Datastores Networks Updates

Hypervisor: VMware ESXi, 6.7.0, 13006603
Model: UCSC-C220-M5SX
Processor Type: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz
Logical Processors: 56
NICs: 4
Virtual Machines: 13
State: Connected
Uptime: 164 days

Network uplink redundancy lost

Acknowledge Reset To Green

Configuration

Related Objects

None

Update Manager

4. Choose the Local file option and click on Choose files. Navigate to the SD-WAN images folder and select the file beginning with viptela-edge-. Click on Next.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

Local file

viptela-edge-20...ericx86-64.ova

5. Change the Virtual Machine name to **DC-vEdge1-podX** and click on Next (where X is your POD number, image below doesn't have the suffix of podX)

Note: We will only use the podX suffix over here to distinguish between different VMs in our Data Center. The rest of the guide will refer to this VM as **DC-vEdge1**

Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: DC-vEdge1

Select a location for the virtual machine.

- ▽ ghi-vcenter.swat4partners.com
 - > SWAT-Labs-GHI
 - > slc-vcenter.swat4partners.com

CANCEL

BACK

NEXT

6. Select the host assigned to you (image shown as an example only) and click on Next

Note: If the screen gets stuck over here at **Validating** then close Chrome and open the vCenter in Internet Explorer, going through the same steps. Deployment should go through. This is a known issue with Google Chrome.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

The screenshot shows a tree-based selection interface for choosing a compute resource. At the top level, there is a collapsed node labeled "SWAT-Labs-GHI". Expanding this node reveals a list of resources under "Management-Shared Services" and individual hosts. The host "ghi-ms04.swat4partners.com" is currently selected, indicated by a light blue background. Other visible hosts include "ghi-ms01.swat4partners.com", "ghi-ms02.swat4partners.com", "ghi-ms03.swat4partners.com", "GHI-Pod01" through "GHI-Pod10".

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

7. Review the details shown and click on Next

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource

Review details

Verify the template details.

4 Review details

- 5 Select storage
- 6 Select networks
- 7 Ready to complete

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

| | |
|---------------------|--|
| Publisher | No certificate present |
| Download size | 231.2 MB |
| Size on disk | 234.1 MB (thin provisioned) |
| | 10.2 GB (thick provisioned) |
| Extra configuration | <pre>time.synchronize.tools.startup = FALSE virtualHW.productCompatibility = hosted time.synchronize.restore = FALSE time.synchronize.continue = FALSE time.synchronize.shrink = FALSE time.synchronize.resume.disk = FALSE time.synchronize.tools.enable = FALSE time.synchronize.resume.host = FALSE</pre> |

CANCEL

BACK

NEXT

8. Choose the Datastore and click on Next

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select storage
Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format:

Thick Provision Lazy Zeroed

VM Storage Policy:

Datastore Default

| Name | Capacity | Provisioned | Free | T |
|-------------|----------|-------------|----------|---|
| ghi-ms04-ds | 11.63 TB | 1.1 TB | 10.99 TB | V |

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

9. Populate the VM Networks as per the image given below

⚠ Important: Please make sure that these look exactly as shown below

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details**
- ✓ 5 Select storage
- ✓ 6 Select networks**
- 7 Ready to complete

Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|----------------|---------------------|
| VM Network 3 | SiteDC-VPN20 |
| VM Network | Management |
| VM Network 2 | SiteDC_VPN10 |
| VM Network 1 | MPLS10 |

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

10. Click on **Finish** to deploy your DC-vEdge1 VM

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Ready to complete**

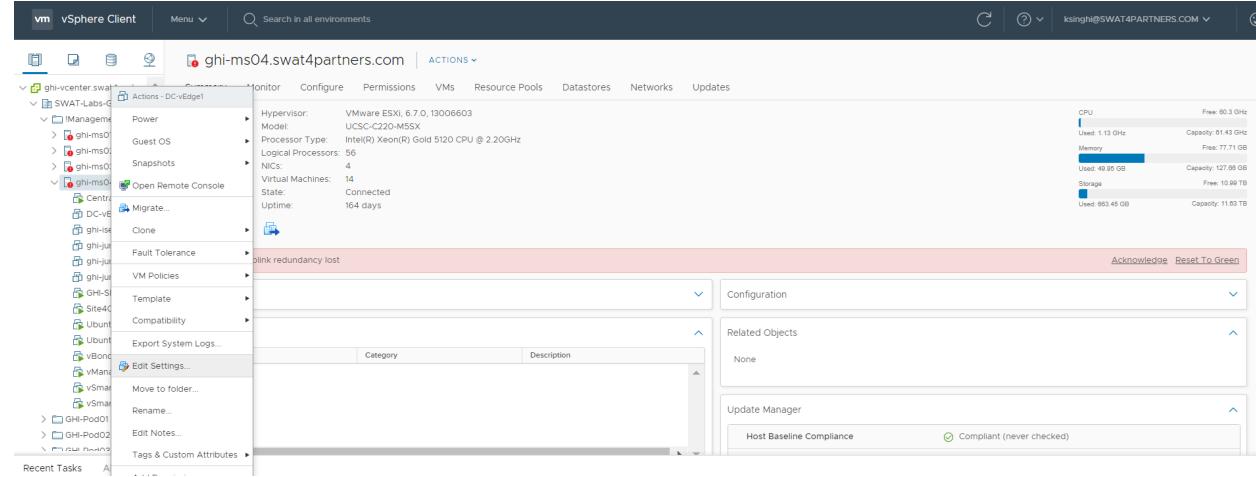
| | |
|-------------------|---|
| Provisioning type | Deploy from template |
| Name | DC-vEdge1 |
| Template name | viptela-edge-genericx86-64-20200414061026 |
| Download size | 231.2 MB |
| Size on disk | 10.2 GB |
| Folder | SWAT-Labs-GHI |
| Resource | ghi-ms04.swat4partners.com |
| Storage mapping | 1 |
| All disks | Datastore: ghi-ms04-ds; Format: Thick provision lazy zeroed |
| Network mapping | 4 |
| VM Network 3 | SiteDC-VPN20 |
| VM Network | Management |
| VM Network 2 | SiteDC_VPN10 |
| VM Network 1 | MPLS10 |

CANCEL

BACK

FINISH

11. Once the VM is deployed, right click **DC-vEdge1-podX** and click Edit settings.



12. Choose to **Add a new device** (top right corner) and select Network Adapter to add one (since our deployed VM has only 4 Network Adapters but we will need 5 for our lab)

Edit Settings | DC-vEdge1

X

Virtual Hardware VM Options

| | | |
|---|---|--|
| CD/DVD Drive | ADD NEW DEVICE | |
| Host USB Device | 4 | GB |
| Hard Disk | 2 | GB |
| RDM Disk | 10.224878311! | GB |
| Existing Hard Disk | Management | <input checked="" type="checkbox"/> Connect... |
| Network Adapter | MPLS10 | <input checked="" type="checkbox"/> Connect... |
| SCSI Controller | SiteDC_VPN10 | <input checked="" type="checkbox"/> Connect... |
| USB Controller | SiteDC_VPN20 | <input checked="" type="checkbox"/> Connect... |
| SATA Controller | | |
| NVMe Controller | | |
| Shared PCI Device | | |
| PCI Device | | |
| Serial Port | | |
| / Network Adapter | | |
| > CD/DVD drive 1 ! | Host Device | <input type="checkbox"/> Connect... |
| > Video card | Auto-detect settings | |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface | |
| > Other | Additional Hardware | |
| | | |

CANCEL

OK

13. Click on the drop down next to **New Network** and click on *Browse*

Edit Settings | DC-vEdge1

X

Virtual Hardware VM Options

ADD NEW DEVICE

| | | |
|---------------------|---|---|
| > CPU | 4 | GB |
| > Memory | 2 | GB |
| > Hard disk 1 | 10.2248783111! | GB |
| > Network adapter 1 | Management | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 2 | MPLS10 | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 3 | SiteDC_VPN10 | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 4 | SiteDC-VPN20 | <input checked="" type="checkbox"/> Connect... |
| > New Network * | MPLS10 | <input checked="" type="checkbox"/> Connect... (X) |
| > CD/DVD drive 1 | ! | <input type="checkbox"/> Connect... |
| > Video card | Browse ... settings | |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface | |
| > Other | Additional Hardware | |

CANCEL

OK

14. Choose the **Internet** Network and click on OK. Make sure the Network Adapters match with the second image below and click on OK again

⚠ Warning: The Network Adapter mapping might vary based on the version of vEdge being deployed.

Sometimes, trial and error is the easiest way to figure out which Network Adapter maps to which interface on the vEdge

Edit Settings | DC-vEdge1

Virtual Hardware VM Options

ADD NEW DEVICE

- > CPU
- > Memory
- > Hard disk 1
- > Network adapter
- > Network adapter
- > Network adapter
- > Network adapter
- > New Network
- > CD/DVD drive
- > Video card
- VMCI device
- > Other

Select Network

Filter

| Name | Distributed Switch |
|--------------------|--------------------|
| 64 | GHI-DSwitch |
| DPortGroup | GHI-DSwitch |
| GHI-Pods-mPool | GHI-DSwitch |
| GHI-vMotion | GHI-DSwitch |
| Internet | -- |
| Management | -- |
| Management_VLAN100 | GHI-DSwitch |
| MPLS10 | -- |

40 items

CANCEL

OK

Additional Hardware

CANCEL

OK

| | | |
|---------------------|--------------|--|
| > Network adapter 1 | Management | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 2 | MPLS10 | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 3 | SiteDC_VPN10 | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 4 | SiteDC-VPN20 | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 5 | Internet | <input checked="" type="checkbox"/> Connect... |

15. Click on the DC-vEdge1-podX VM and choose to power it on

vSphere Client | Menu | Search in all environments

DC-vEdge1 | ACTIONS | Power On

Summary Monitor Configuration Power On Mission Datastores Networks Updates

Guest OS: Red Hat Enterprise Linux 6 (64-bit)
Compatibility: ESXi 5.0 and later (VM version 8)
VMware Tools: Not running, not installed
More info

DNS Name:
IP Addresses:
Host: ghi-ms04.swat4partners.com

Launch Web Console | Launch Remote Console

VM Hardware

| | |
|-------------------|-----------------------------|
| CPU | 4 CPU(s) |
| Memory | 2 GB, 0 GB memory active |
| Hard disk 1 | 10.22 GB |
| Network adapter 1 | Management (disconnected) |
| Network adapter 2 | MPLS10 (disconnected) |
| Network adapter 3 | SiteDC_VPN10 (disconnected) |
| Network adapter 4 | SiteDC_VPN20 (disconnected) |
| Network adapter 5 | Internet (disconnected) |

Recent Tasks Alarms

| Task Name | Target | Status |
|-----------------------------|-----------|-------------|
| Reconfigure virtual machine | DC-vEdge1 | ✓ Completed |
| Reconfigure virtual machine | DC-vEdge1 | ✓ Completed |

Task List

- Verifying the existing lab setup
- Creating the DC-vEdge1 VM
- Overview
- Deploying the VM on vCenter
- Onboarding DC-vEdge1
- Bootstrapping DC-vEdge1 (Initial Configuration)

- Installing certificates and activating the vEdge
- Onboarding Verification
- Helpful debugs and logs

Onboarding DC-vEdge1

Bootstrapping DC-vEdge1 (Initial Configuration)

Use the following information in this section (some of the information will be used later)

| SITE ID | SYSTEM IP | VM | Network Adapter | Network Management | Interface | IP | Gateway |
|---------|---------------|-----------|-------------------|--------------------|-----------|-------------------|---------------|
| 1 | 10.255.255.11 | DC-vEdge1 | Network Adapter 1 | | eth0 | 192.168.0.10/24 | 192.168.0.1 |
| | | | Network Adapter 2 | MPLS10 | ge0/1 | 192.0.2.2/30 | 192.0.2.1 |
| | | | Network Adapter 3 | SiteDC_VPN10 | ge0/2 | 10.100.10.2/24 | 10.100.10.1 |
| | | | Network Adapter 4 | SiteDC-VPN20 | ge0/3 | 10.100.20.2/24 | 10.100.20.1 |
| | | | Network Adapter 5 | Internet | ge0/0 | 100.100.100.10/24 | 100.100.100.1 |

1. Console in to the DC-vEdge1 VM from vCenter (you should already be logged in from our last activity)

VMware Tools is not installed on this virtual machine.

| Task Name | Target | Status |
|--------------------------|--------------------------------|-----------|
| Check new notifications | ghi-vcenter.swat4partners.c... | Completed |
| Power On virtual machine | DC-vEdge1 | Completed |
| Initialize powerOn | SWAT-Labs-GHI | Completed |

- Wait for the VM to prompt you for the username and password and enter the credentials given below. If you get a message stating that they are incorrect, wait for 30 seconds and try again (since the processes need to initialize before you can log in)

| Username | Password |
|----------|----------|
| admin | admin |

Note: From version 19.2, the password will need to be reset on initial login. For this lab, we will reset the password to admin.

```
early console in decompress_kernel

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

viptela 20.1.1

vedge login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vedge
You must set an initial admin password.
Password:
Re-enter password:
vedge# _
```

3. Enter the configuration enumerated below. Unfortunately, this will need to be typed out since the console isn't copy-paste friendly

```
vedge# conf t
Entering configuration Mode terminal
vedge(config)# system
vedge(config-system)# host-name DC-vEdge1
vedge(config-system)# system-ip 10.255.255.11
vedge(config-system)# site-id 1
vedge(config-system)# organization-name "swat-sdwanlab"
vedge(config-system)# vbond 100.100.100.3
vedge(config-system)# exit
vedge(config)# vpn 0
vedge(config-vpn-0)# ip route 0.0.0.0/0 100.100.100.1
vedge(config-vpn-0)# interface ge0/0
vedge(config-interface-ge0/0)# ip address 100.100.100.10/24
vedge(config-interface-ge0/0)# no tunnel-interface
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# exit
vedge(config)# vpn 512
vedge(config-vpn-512)# ip route 0.0.0.0/0 192.168.0.1
vedge(config-vpn-512)# interface eth0
vedge(config-interface-eth0)# ip address 192.168.0.10/24
vedge(config-interface-eth0)# no shutdown
vedge(config-interface-eth0)# commit and-quit
```

```
conf t
system
host-name DC-vEdge1
system-ip 10.255.255.11
site-id 1
organization-name "swat-sdwanlab"
vbond 100.100.100.3
exit
!
vpn 0
ip route 0.0.0.0/0 100.100.100.1
interface ge0/0
ip address 100.100.100.10/24
no tunnel-interface
no shutdown
exit
!
exit
```

```
!
vpn 512
 ip route 0.0.0.0/0 192.168.0.1
interface eth0
 ip address 192.168.0.10/24
 no shutdown
!
commit and-quit
```

Tip: We are ensuring that the vEdge has basic IP Addressing and Routing to the Controllers. `no tunnel-interface` has been added under the `ge0/0` interface in VPN 0 in order to prevent control connections from being established

4. Open **Putty** and double click the saved session for DC-vEdge1 (or **SSH to 192.168.0.10**)

PutTY Configuration

?

X

Category:

- Session
- Logging
- Terminal
- Keyboard
- Bell
- Features
- Window
- Appearance
- Behaviour
- Translation
- Selection
- Colours
- Connection
- Data
- Proxy
- Telnet
- Rlogin
- SSH
- Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port
192.168.0.10 22

Connection type:

Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

DC-vEdge1

Default Settings

CentralGW

DC-vEdge1

DC-vEdge2

cEdge40

cEdge50

cEdge51

Load

Save

Delete

Close window on exit:

Always Never Only on clean exit

About

Help

Open

Cancel

5. Choose Yes to accept the certificate, if prompted

PuTTY Security Alert



WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.

The new ecdsa-sha2-nistp256 key fingerprint is:

ecdsa-sha2-nistp256 256

7c:de:34:0d:98:36:6a:64:a1:69:07:d8:68:44:d4:8f

If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.

If you want to carry on connecting but without updating the cache, hit No.

If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

Yes

No

Cancel

Help

6. Login using the same credentials as Step 2.

The screenshot shows a PuTTY terminal window titled "192.168.0.10 - PuTTY". The session log displays the following text:

```
login as: admin
Pre-authentication banner message from server:
| viptela 20.1.1
|
End of banner message from server
admin@192.168.0.10's password:
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on DC-vEdge1
DC-vEdge1#
```

Task List

- [Verifying the existing lab setup](#)
- [Creating the DC-vEdge1 VM](#)
- [Overview](#)
- [Deploying the VM on vCenter](#)
- [Onboarding DC-vEdge1](#)
- [Bootstrapping DC-vEdge1 \(Initial Configuration\)](#)
- [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

[Installing certificates and activating the vEdge](#)

Tip: Make sure the certificates and relevant files (like the .viptela Serial file) are in order before initiating a deployment. Certificate mismatches are one of the most widely seen causes for devices not being able to establish control connections with the vManage/vSmarts

1. Type `vshell` and enter `scp admin@192.168.0.6:ROOTCA.pem .` to copy the ROOTCA.pem certificate to the vEdge. Commands can be copy-pasted now since we have SSH'd in to the vEdge (there is a dot at the end of the scp command). Enter `yes` when prompted and enter the password of vManage (i.e. admin). Exit when done with this step.

```
DC-vEdge1#  
DC-vEdge1# vshell  
DC-vEdge1:~$  
DC-vEdge1:~$  
DC-vEdge1:~$ scp admin@192.168.0.6:ROOTCA.pem .  
The authenticity of host '192.168.0.6 (192.168.0.6)' can't be established.  
ECDSA key fingerprint is SHA256:xII/5CjpxITjIL0kqxe5GFQqaoWMRT2s53eM7e38vNo.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.0.6' (ECDSA) to the list of known hosts.  
viptela 20.1.1  
  
admin@192.168.0.6's password:  
ROOTCA.pem  
DC-vEdge1:~$
```

```
vshell  
scp admin@192.168.0.6:ROOTCA.pem .
```

Note: This is NOT how you would normally install certificates over to your devices. In a lab, this manual method works fine but for production environments, the other options are definitely preferred (like Cisco PKI)

2. Go to the vManage GUI (<https://192.168.0.6>) and log in, if logged out. Navigate to **Configuration => Devices** (from the left-hand side, click on the cog wheel to access the configuration options)

Cisco vManage

DASHBOARD | MAIN DASHBOARD

Configuration 2 ↑ Part - 2

WAN Edge - 0

vBond - 1 1 ↑

vManage 1 ✓

Devices

TLS/SSL Proxy Devices 2

Certificates 0

Network Design 0

Templates

Policies

Security 20

Unified Communications 0

Cloud onRamp for SaaS 0

Cloud onRamp for IaaS

Cloud onRamp for Colocation

No data to display

Site Health (Total 0)

- Full WAN Connectivity 0 sites
- Partial WAN Connectivity 0 sites
- No WAN Connectivity 0 sites

WAN Edge Health (Total 0)

Normal 0 Warning 0 Error 0

Application-Aware Routing

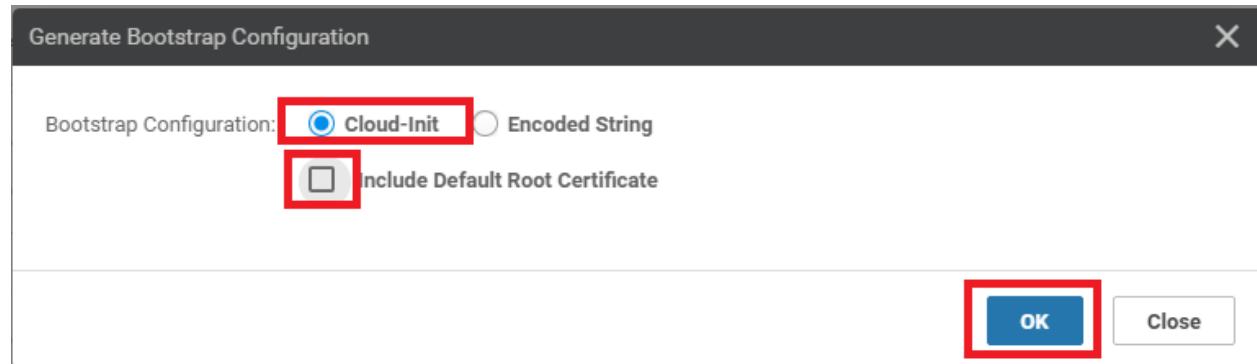
| Tunnel Endpoints | Avg. Latency (ms) |
|------------------|-------------------|
| No data | |

The screenshot shows the Cisco vManage main dashboard. On the left, a sidebar lists various management categories like Configuration, Devices, Policies, and Security. The 'Devices' section is currently selected and shows a count of 2 devices under 'TLS/SSL Proxy'. The main panel displays several key metrics: Site Health (Total 0), WAN Edge Health (Total 0), and Application-Aware Routing. Each metric includes a summary table with three columns: Normal, Warning, and Error. Below these are three large circular icons with the number '0' indicating no issues. The bottom right of the main panel shows a message 'No data'.

3. Choose any vEdge Cloud device (it doesn't matter which one you pick, as long as it is a vEdge Cloud) and click on the three dots at the extreme right-hand side. Choose **Generate Bootstrap Configuration**

The screenshot shows the Cisco vManage interface under the 'WAN Edge List' tab. A context menu is open over a row for a vEdge Cloud device. The menu items are: Running Configuration, Local Configuration, Delete WAN Edge, Copy Configuration, Generate Bootstrap Configuration, Template Log, and Device Bring Up. The 'Generate Bootstrap Configuration' option is highlighted.

4. Select **Cloud-Init** and **uncheck Include Default Root Certificate**. Click on **OK**



5. Make note of the **UUID** and the **OTP** values. These will be required to activate the vEdge. It's best to copy the string and place it in notepad, since we will need to use it in our SSH session to the DC-vEdge1 device. Alternatively, leave this popup open and we can come back to it when required

⚠ Important: The UUID and OTP/Token are super important for vEdge Cloud or cEdge CSRs. Physical devices don't have a token associated with them and are uniquely identified by their serial number

Generate Bootstrap Configuration

X

 Download

```
#cloud-config
vinitparam:
- uuid : e474c5fd-8ce7-d376-7cac-ba950b2c9159
- vbond : 100.100.100.3
- otp : b3e0663be1443f922778ca53b1a127c6
- org : swat-sdwanlab
- rcc : true
ca-certs:
remove-defaults: false
trusted:
- |
---BEGIN CERTIFICATE---
MIIF7DCCBN...Qbsx6pacDIAm4rz...06VLUkTANBgkqhkiG9w0BAQUFADC...Wd...I...M...O...H...V...O...I...
```

Close

6. Go back to the Putty session for DC-vEdge1 and enter `request root-cert-chain install /home/admin(ROOTCA.pem` to install the root cert chain. It should install successfully

```
DC-vEdge1# request root-cert-chain install /home/admin/ROOTCA.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
DC-vEdge1#
```

```
request root-cert-chain install /home/admin/ROOTCA.pem
```

7. Enter `tunnel-interface`, `encapsulation ipsec` and `allow-service all` under `interface ge0/0` to bring up the tunnel Interface. Make sure to `commit and-quit` in order to write the configuration change

```
DC-vEdge1# conf t
Entering configuration mode terminal
DC-vEdge1(config)# vpn 0
DC-vEdge1(config-vpn-0)# interface ge0/0
DC-vEdge1(config-interface-ge0/0)# tunnel-interface
DC-vEdge1(config-tunnel-interface)# encapsulation ipsec
DC-vEdge1(config-tunnel-interface)# allow-service all
DC-vEdge1(config-tunnel-interface)# commit and-quit
Commit complete.
DC-vEdge1#
```

```
config t
vpn 0
interface ge0/0
  tunnel-interface
  encapsulation ipsec
  allow-service all
exit
!
commit and-quit
```

This ensures that our vEdge is now able to establish control connections with the vManage and vSmarts via the vBond. However, these connections will not be fully formed till we don't activate the vEdge itself

8. Issue the `request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)` command. Replace the (*Enter your UUID*) and (*Enter your OTP*) fields with the UUID and OTP generated in Step 5 (image below is an example, UUID and OTP may not match).

```
DC-vEdge1#
DC-vEdge1# request vedge-cloud activate chassis-number e474c5fd-8ce7-d376-7cac-b
a950b2c9159 token b3e0663be1443f922778ca53b1a127c6
```

```
request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)
```

This completes the Onboarding section for DC-vEdge1

Task List

- [Verifying the existing lab setup](#)
- [Creating the DC-vEdge1 VM](#)
- [Overview](#)
- [Deploying the VM on vCenter](#)
- [Onboarding DC-vEdge1](#)
- [Bootstrapping DC-vEdge1 \(Initial Configuration\)](#)
- [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

Onboarding Verification

1. Wait for a couple of minutes and run `show control connections` in the DC-vEdge1 CLI. We should see that the vEdge has been able to establish a DTLS tunnel with the vManage and the vSmarts. If you don't see any output, wait for a couple of minutes and run the command again

| PEER | | | | | PEER | | | | | CONTROLLER | | | | |
|---------|------|--------------|------|------|---------------|------|-------|---------------|-------|------------|-------------|-------------|------------|----|
| TYPE | PROT | SYSTEM IP | ID | SITE | DOMAIN PEER | PRIV | PEER | PUB | PORT | PUBLIC IP | LOCAL COLOR | PROXY STATE | UPTIME | ID |
| vsmart | dtls | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | | 12346 | 100.100.100.4 | 12346 | default | No | up | 0:00:01:26 | 0 |
| vsmart | dtls | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | | 12346 | 100.100.100.5 | 12346 | default | No | up | 0:00:01:26 | 0 |
| vmanage | dtls | 10.255.255.1 | 1000 | 0 | 100.100.100.2 | | 12346 | 100.100.100.2 | 12346 | default | No | up | 0:00:01:10 | 0 |

```
show control connections
```

Tip: You can also issue `show control connections-history` in the event of failures to find out why the connection is not working as expected. A few helpful commands are `show certificate installed`, `show certificate root-ca-cert`, `show control local-properties` and `show certificate validity`. Most of these commands give us details about the status of certificates on the device and are helpful in ascertaining the root cause of failure when control connections aren't getting established.

2. On the vManage GUI, navigate to **Monitor => Network Devices** (the computer icon on the left-hand side)

| Cisco vManage | | | |
|---------------|-------------------------|--|---|
| | Configuration Devices | | |
| | Monitor | WAN Edge | |
| | Geography | Upload WAN Edge List <input checked="" type="checkbox"/> Export Bootstrap Configuration <input checked="" type="checkbox"/> Sync Smart Account | |
| | Network | Search Options | |
| | Alarms | Network | Chassis Number |
| | Events | CSR-44C7CE5A-4149-E696-C8A8-415C793FBF6C | Serial No./Token |
| | Audit Log | CSR-D6DB39FC-C383-BB55-7E9D-7CDD85595DD1 | Enterprise |
| | ACL Log | CSR-834E40DC-E358-8DE1-0E81-76E5984138F4 | |
| | | CSR-D405F5BA-B975-8944-D1A3-2E082AEE2A1D | |
| | | CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3 | |
| | | CSR1000v | Token - fc40de6570e725ba70c917d6511b8a6c |
| | | CSR1000v | NA |
| | | vEdge Cloud | Token - f28b5ab9789827383a9425d0aec4fe1a |
| | | vEdge Cloud | NA |
| | | e474c5fd-8ce7-d376-7cac-ba950b2c9159 | Token - b8a9cae09c975b49003634e8174b83b |
| | | CSR-5E992295-1362-0DB6-EEF8-25CC88F1CCCE | NA |
| | | CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2 | Token - e78aaefc1ebd2a11d900e88098a7949c |
| | | CSR1000v | NA |
| | | CSR1000v | Token - 90ffd29997ff8c9aab379f6d3b75d2d |
| | | CSR1000v | NA |
| | | CSR1000v | Token - 1da14330e1711d985d29d28603a5611d |
| | | CSR1000v | NA |
| | | vEdge Cloud | Token - 4a6809836f0216c736c305fc131950d9 |
| | | vEdge Cloud | NA |
| | | e474c5fd-8ce7-d376-7cac-ba950b2c9159 | 7175AE0F |
| | | CSR-5E992295-1362-0DB6-EEF8-25CC88F1CCCE | NA |
| | | CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2 | Token - 90adb0239fdd2018f25ad423fc6a1b9 |
| | | vEdge Cloud | NA |
| | | b7fd7295-58df-7671-e914-6fe2edff1609 | Token - 945eb9871624db4cc321c6197484ce09 |
| | | vEdge Cloud | NA |
| | | dde90ff0-dc62-77e6-510f-08d96608537d | Token - 4c583475c7d42f07e570dbcba42d3431f |
| | | vEdge Cloud | NA |
| | | 17026153-f09e-be4b-6dce-482fce43aab2 | Token - 3692590e47782dd2ae043b8a4369c145 |
| | | CSR1000v | NA |
| | | CSR26217DA0-1B63-8DDE-11C9-125F527D3270 | Token - 8dc7b557b60d4cec5c22e3c143132c0d |
| | | CSR1000v | NA |
| | | CSR-960E020-B7C9-887F-46A8-F45374B23E7D | Token - 50cc04634ac461d3d68d53f26a520c35 |
| | | CSR1000v | NA |
| | | CSR-25925FBC-07F3-0732-E127-EA95D24F8EEB | Token - 6ced66053d4698a4402a50b1b2c082f3 |
| | | vEdge Cloud | NA |
| | | 35bd96f9-1758-116c-4e4c-e34c7066459c | Token - ed778f56f9ab08994a1c1d8aa046385c |
| | | vEdge Cloud | NA |
| | | 005c424c-2d57-41fe-250d-ee991e0a4e93 | Token - 56f4f54ce614d27ba24350ec9a50572e |
| | | vEdge Cloud | NA |
| | | 21292349-2c9f-7aaf-28f5-a87e4d0054cb | Token - b6046deef4a2ae480f9cc18194152fb0 |
| | | vEdge Cloud | NA |
| | | 2frl2adn02h47c | Token - ce9fb6c06da1fhe2ha06fd5001520f62 |
| | | | NA |

3. DC-vEdge1 should show up in the list of devices

| Device Group | All | Q | Search Options | | | | | | | | | |
|---------------------|---------------|---------------------|-----------------------------------|-----------|--------------|---------|-----|---------|-----------------------------|-------------|---------------|---|
| Device Group | | | | | | | | | | | | |
| Hostname | System IP | Device Model | Chassis Number/ID | State | Reachability | Site ID | BFD | Control | Version | Up Since | Device Groups | T |
| vmanage | 10.255.255.1 | vManage | dfea63a5-66d2-4e50-a07b-ec4ad4... | reachable | 1000 | -- | 3 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | | |
| vSmart | 10.255.255.3 | vSmart | 20607a12-c0c4-4f46-a65f-5a547c... | reachable | 1000 | -- | 3 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | | |
| vSmart2 | 10.255.255.4 | vSmart | 7f332491-cb6f-4843-8bf5-060f90... | reachable | 1000 | -- | 3 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | | |
| vBond | 10.255.255.2 | vEdge Cloud (vBo... | fc31c154-99c5-4267-971d-6c9ae7... | reachable | 1000 | -- | -- | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | | |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b... | reachable | 1 | -- | 3 | 20.1.1 | 14 May 2020 7:36:00 AM PDT | "No groups" | | |

4. Click on DC-vEdge1 and navigate to **Troubleshooting => Control Connections(Live view)**. You should see the vEdge successfully connected to 2 vSmarts and 1 vManage

Cisco vManage

MONITOR Network > Troubleshooting > Control Connections(Live View)

Select Device DC-vEdge1 | 10.255.255.11 Site ID: 1 Device Model: vEdge Cloud

vSmart Control Connections (Expected: 2 | Actual: 2)

vSmart 2/2 vManage 1/1

| Controller | Local Status | Remote Status |
|--|--------------|---------------|
| DEFAULT Circuit (Expected:2 Actual:2) NAT:Not learned | | |
| vSmart 10.255.255.3(Preferred Controller) | ✓ | ✓ |
| vSmart2 10.255.255.4(Preferred Controller) | ✓ | ✓ |
| vmanage 10.255.255.1(Preferred Controller) | ✓ | ✓ |

This completes the verification activity.

Task List

- [Verifying the existing lab setup](#)
- [Creating the DC-vEdge1 VM](#)
- [Overview](#)
- [Deploying the VM on vCenter](#)
- [Onboarding DC-vEdge1](#)
- [Bootstrapping DC-vEdge1 \(Initial Configuration\)](#)
- [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

Helpful debugs and logs

Note: This section is optional and is intended as a learning activity. It is not required to go through this in order to complete the lab tasks successfully

1. On the CLI for DC-vEdge1, issue `debug vdaemon all` followed by `clear control connections`. This will tear down all the control connections and the vEdge will rebuilt the DTLS tunnels. We can capture the logs to see the process associated with the DTLS tunnels being built

```
DC-vEdge1# debug vdaemon all
DC-vEdge1#
DC-vEdge1#
DC-vEdge1#
DC-vEdge1# clear control connections
DC-vEdge1#
DC-vEdge1#
DC-vEdge1#
DC-vEdge1#
```

```
debug vdaemon all
clear control connections
```

2. Wait for a couple of minutes and go to `vshell`. Type `cat /var/log/tmplog/vdebug` to view the contents of the log file

```
DC-vEdge1# vshell
DC-vEdge1:~$ cat /var/log/tmplog/vdebug
```

3. Given below are a couple of sample outputs

```
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_DELROUTE ipv4 multicast proto boot
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_NEWRROUTE ipv4 unicast proto boot
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_NEWRROUTE 10.255.255.3/32 gate: 10.255.255.3, ifindex: 18
local7.debug: May 14 16:33:36 vedge stratis setscocktop Bad file descriptor
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_DELROUTE ipv4 multicast proto boot
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_NEWRROUTE ipv4 unicast proto boot
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_NEWRROUTE 10.255.255.4/32 gate: 10.255.255.4, ifindex: 18
local7.debug: May 14 16:33:36 vedge strav: setscocktop: Bad file descriptor
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_DELROUTE ipv4 multicast proto boot
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_NEWRROUTE 10.255.255.1, ifindex: 18
local7.debug: May 14 16:33:36 vedge strav: setscocktop: Bad file descriptor
local7.debug: May 14 16:33:36 vedge ZEBRA[1130]: RTM_NEWRROUTE 10.255.255.1/32 gate: 10.255.255.1, ifindex: 18
local7.debug: May 14 16:33:36 vedge ZEBRA[1124]: vdaemon: vdaemon: Child pid 18211 exited with status: 1
local7.debug: May 14 16:33:36 vedge ZEBRA[1124]: vdaemon: dtls verify peer cert[1919]: #v4DAEMON_DBG_MISC-1: Validating device certificate.. serial # (9850DFPA9D7604C1F) "swat-sdwanlab"
local7.debug: May 14 16:33:36 vedge ZEBRA[1124]: vconfd trap send[833]: Processing trap viptelaSecurityControlConnectionStateChange
local7.info: May 14 16:33:36 vedge ZEBRA[1124]: #Viptela-vedge-vdaemon-6:INFO-140002: Notification: 5/14/2020 16:33:36 control-connection-state-change severity-level:major host-name:"DC-edge1" system-ip:10.255.255.1 primary-primaryity:vmanage-peer-system-ip:10.255.255.1 peer-vmanage-system-ip:0.0.0.0 public-ip:100.100.100.2 public-port:12346 src-color:default remote-color:default
local7.info: May 14 16:33:36 vedge ZEBRA[1124]: uptime: "00:00:00" new-state: up
local7.debug: May 14 16:33:37 vedge strav: to snapshot current CGS content
local7.debug: May 14 16:33:37 vedge strav: snapshoted in 1 seconds
local7.debug: May 14 16:33:38 vedge strav: scrtyp: ./.../bind-9.8.1/lib/dns/mmac.link.c:350: FIPS mode is 1: MDS is only supported if the value is 0.
local7.debug: May 14 16:33:38 vedge strav: Please disable either FIPS mode or MDS.
local7.debug: May 14 16:33:38 vedge DHCP_CLIENT[1125]: dhcp_client_v6 get lease_info[3190]: Failed to get stat for /var/run/dhcpv6/eth0/lease.txt
local7.debug: May 14 16:33:38 vedge strav: eth0: error fetching interface information: Device not found
local7.debug: May 14 16:33:41 vedge last message repeated 5 times
local7.debug: May 14 16:33:41 vedge strav: sigchild signal[1043]: Child pid 18470 exited with status: 1
local7.debug: May 14 16:33:41 vedge strav: 05/14/2020 9:11:01 lib/dns/mmac.link.c:350: FIPS mode is 1: MDS is only supported if the value is 0.
local7.debug: May 14 16:33:46 vedge strav: Please disable either FIPS mode or MDS.
local7.debug: May 14 16:33:46 vedge DHCP_CLIENT[1125]: dhcp_client_v6 get lease_info[3190]: Failed to get stat for /var/run/dhcpv6/eth0/lease.txt
local7.debug: May 14 16:33:46 vedge strav: eth0: error fetching interface information: Device not found
local7.debug: May 14 16:33:47 vedge strav: eth0: error fetching interface information: Device not found
local7.debug: May 14 16:33:47 vedge ZEBRA[1130]: RTM_NEWRROUTE ipv4 multicast proto boot
local7.debug: May 14 16:33:47 vedge ZEBRA[1130]: RTM_NEWRROUTE ipv4 unicast proto boot
local7.debug: May 14 16:33:48 vedge ZEBRA[1130]: RTM_NEWRROUTE 10.255.255.3/32 gate: 10.255.255.3
local7.debug: May 14 16:33:48 vedge ZEBRA[1130]: RTM_NEWRROUTE 10.255.255.4/32 gate: 10.255.255.4
```

```
local7:debug: May 14 16:33:52 vedge VDAEMON[1124]: vdaemon_dtls_verify_peer_cert[919]: %VDAEMON_DBG_MISC-1: Validating device certificate.. serial # (9850DFAD97604C21) "swat-sdwanlab"
local7:debug: May 14 16:33:52 vedge VDAEMON[1124]: vdaemon_dtls_verify_peer_cert[919]: %VDAEMON_DBG_MISC-1: Validating device certificate.. serial # (9850DFAD97604C21) "swat-sdwanlab"
local7:debug: May 14 16:33:52 vedge VDAEMON[1124]: vdaemon_send_tloc_info[8333]: %VDAEMON_DBG_MISC-1: Sending TLOC: Ifname:ge0 color:default spi:257 smartcls:1 manage1:state:UP lr encap:0 LR hold time : 7000 pairwise-keys Disabled key-id 0
local7:debug: May 14 16:33:52 vedge VDAEMON[1124]: vdaemon_send_tloc_info[8333]: %VDAEMON_DBG_MISC-1: TLOC - v4 public 100.100.100.10:12366 private 100.100.100.10:12366 public v6 ::::0 private ::::0
local7:debug: May 14 16:33:52 vedge VDAEMON[1124]: vdaemon_send_local_tloc_msg[137]: %VDAEMON_DBG_MISC-1: Sending (Originator: 10.255.255.11 Color: 1 Encap: 2) TLOC: ADD: to TTM
local7:debug: May 14 16:33:52 vedge VDAEMON[1124]: vconfd_trap_send[833]: Processing trap vtiptelaSecurityControlConnectionStateChange
local7:info: May 14 16:33:52 vedge VDAEMON[1124]: %Viptela-vedge-vdaemon-6-INFO-140002: Notification: S/14/2016 16:33:52 control-connection-state-change severity-level:major host-name:"DC-wEdge" system-ip:10.255.255.1 peer-type:vsmart-peer-system-ip:10.255.255.3 peer-vmanage-system-ip:0.0.0.0 public-ip:100.100.100.4 public-port:12346 src-color:default remote-color:0
local7:debug: May 14 16:33:52 vedge VDAEMON[1124]: vconfd_trap_send[833]: Processing trap vtiptelaSecurityControlConnectionStateChange
local7:info: May 14 16:33:52 vedge VDAEMON[1124]: %Viptela-vedge-vdaemon-6-INFO-140002: Notification: S/14/2016 16:33:52 control-connection-state-change severity-level:major host-name:"DC-wEdge" system-ip:10.255.255.1 peer-type:vsmart-peer-system-ip:10.255.255.4 peer-vmanage-system-ip:0.0.0.0 public-ip:100.100.100.5 public-port:12346 src-color:default remote-color:0 default:uptime=0:00:00:00" new-state:up
```

Use `no debug vdaemon all` to disable the debug

This completes our onboarding activity for DC-vEdge1.

Task List

- Verifying the existing lab setup
 - Creating the DC-vEdge1 VM
 - Overview
 - Deploying the VM on vCenter
 - Onboarding DC-vEdge1
 - Bootstrapping DC-vEdge1 (Initial Configuration)
 - Installing certificates and activating the vEdge
 - Onboarding Verification
 - Helpful debugs and logs

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 15, 2020

Site last generated: Jul 23, 2020



-->

Deploying and Onboarding DC-vEdge2

Summary: Step by step process for deploying DC-vEdge2

Table of Contents

- [Creating the DC-vEdge2 VM](#)
 - Overview
 - Deploying the DC-vEdge2 VM on vCenter
- [Onboarding DC-vEdge2](#)
 - Bootstrapping DC-vEdge2 (Initial Configuration)
 - Installing certificates and activating the vEdge
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

! **Warning:** This section might already be done, depending on your selected Lab Scenario. Most lab work will start [from here](#). The configuration given below can be used to review what was done to bring the Site up. If this VM is already deployed (check via vCenter), you **Do Not** need to perform these lab activities.

Task List

- Creating the DC-vEdge2 VM
 - Overview
 - Deploying the DC-vEdge2 VM on vCenter
- Onboarding DC-vEdge2
 - Bootstrapping DC-vEdge2 (Initial Configuration)
 - Installing certificates and activating the vEdge

- Onboarding Verification
- Helpful debugs and logs

Creating the DC-vEdge2 VM

Overview

Note: There will be a number of repetitive tasks from the Deploying DC-vEdge1 section.

Note: The important steps which will guide you through this activity will be earmarked, indicating a delta from the previous section.

This is what an earmarked step will look like

We will be deploying another vEdge in our first site (the Data Center) via vCenter. Make note of the following information for this section. The IP Addressing will not be used for some of the Network Adapters until later.

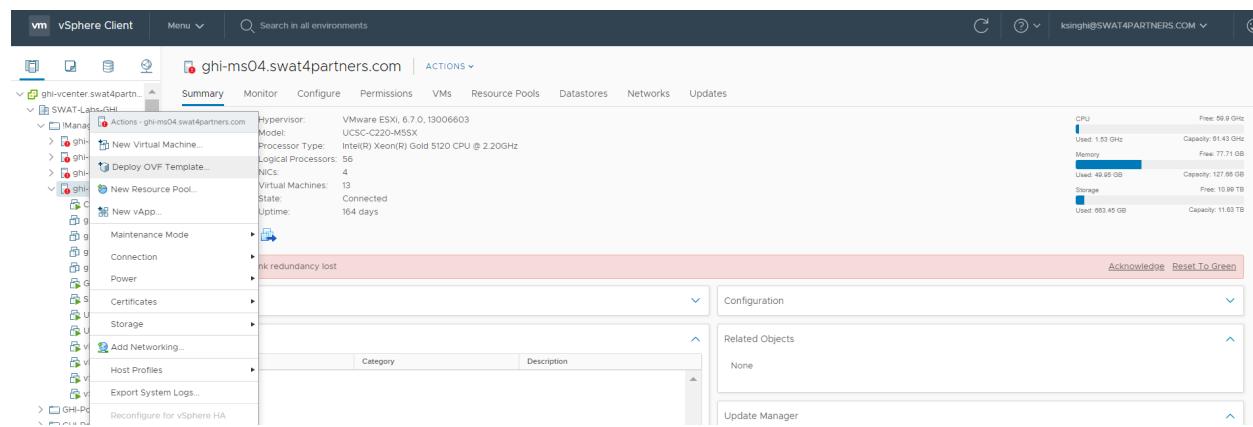
| VM Name | System IP | Network Adapter | Network | Interface | IP Address | Default Gateway |
|----------------|---------------|-------------------|--------------|-----------|-------------------|-----------------|
| DC-vEdge2-podX | 10.255.255.12 | Network Adapter 1 | Management | eth0 | 192.168.0.11/24 | 192.168.0.1 |
| | | Network Adapter 2 | MPLS11 | ge0/1 | 192.0.2.6/30 | 192.0.2.5 |
| | | Network Adapter 3 | SiteDC_VPN10 | ge0/2 | 10.100.10.3/24 | 10.100.10.1 |
| | | Network Adapter 4 | SiteDC-VPN20 | ge0/3 | 10.100.20.3/24 | 10.100.20.1 |
| | | Network Adapter 5 | Internet | ge0/0 | 100.100.100.11/24 | 100.100.100.1 |

Task List

- Creating the DC-vEdge2 VM
 - Overview
 - Deploying the DC-vEdge2 VM on vCenter
- Onboarding DC-vEdge2
 - Bootstrapping DC-vEdge2 (Initial Configuration)
 - Installing certificates and activating the vEdge
- Onboarding Verification
- Helpful debugs and logs

Deploying the DC-vEdge2 VM on vCenter

1. Click on the bookmark for vCenter or navigate to the following URL: <https://10.2.1.50/ui>. Log in with the credentials provided for your POD.
2. Right click on the host and choose to **Deploy OVF Template**



3. Choose the **Local file** option and click on **Choose files**. Navigate to the SD-WAN images folder and select the file beginning with *viptela-edge-*. Click on Next.

4. Change the Virtual Machine name to **DC-vEdge2-podX** and click on Next (where X is your POD number, image below doesn't have the suffix of podX)

Note: We will only use the podX suffix over here to distinguish between different VMs in our Data Center. The rest of the guide will refer to this VM as **DC-vEdge2**

Deploy OVF Template

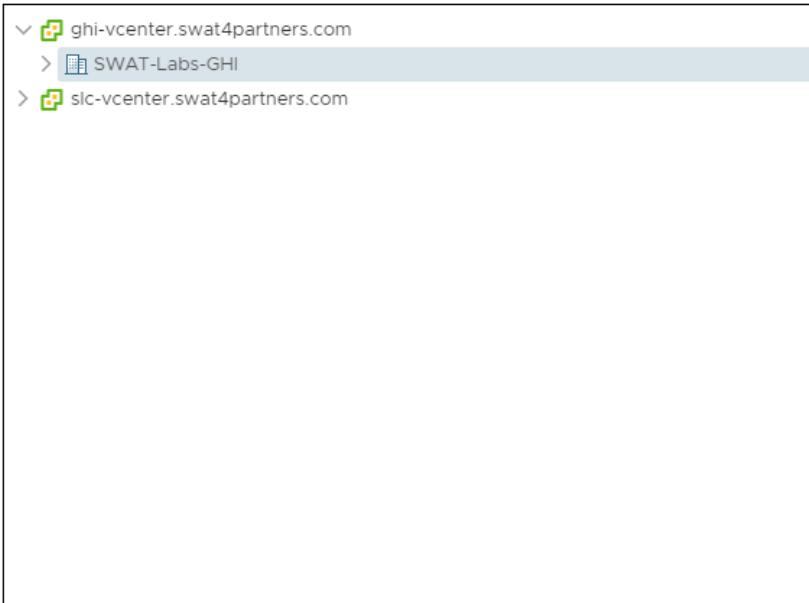
✓ 1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder
Specify a unique name and target location
Virtual machine name: DC-vEdge2

Select a location for the virtual machine.

ghi-vcenter.swat4partners.com
SWAT-Labs-GHI
slc-vcenter.swat4partners.com

CANCEL BACK NEXT



5. Select the host assigned to you (image shown as an example only) and click on Next

Note: If the screen gets stuck over here at **Validating** then close Chrome and open the vCenter in Internet Explorer, going through the same steps. Deployment should go through. This is a known issue with Google Chrome.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

The screenshot shows a list of compute resources under the 'SWAT-Labs-GHI' category. The 'ghi-ms04.swat4partners.com' item is currently selected. The list includes:

- IManagement-Shared Services
- ghi-ms01.swat4partners.com
- ghi-ms02.swat4partners.com
- ghi-ms03.swat4partners.com
- ghi-ms04.swat4partners.com** (selected)
- GHI-Pod01
- GHI-Pod02
- GHI-Pod03
- GHI-Pod04
- GHI-Pod05
- GHI-Pod06
- GHI-Pod07
- GHI-Pod08
- GHI-Pod09
- GHI-Pod10

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

6. Review the details shown and click on Next

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource

Review details
Verify the template details.

4 Review details

- 5 Select storage
- 6 Select networks
- 7 Ready to complete

| | |
|---------------------|--|
| Publisher | No certificate present |
| Download size | 231.2 MB |
| Size on disk | 234.1 MB (thin provisioned) |
| | 10.2 GB (thick provisioned) |
| Extra configuration | <pre>time.synchronize.tools.startup = FALSE virtualHW.productCompatibility = hosted time.synchronize.restore = FALSE time.synchronize.continue = FALSE time.synchronize.shrink = FALSE time.synchronize.resume.disk = FALSE time.synchronize.tools.enable = FALSE time.synchronize.resume.host = FALSE</pre> |

CANCEL

BACK

NEXT

7. Choose the Datastore and click on Next

8. Populate the VM Networks as per the image given below

⚠ Important: Please make sure that these look exactly as shown below

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**

7 Ready to complete

Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|----------------|---------------------|
| VM Network 3 | SiteDC-VPN20 |
| VM Network | Management |
| VM Network 2 | SiteDC_VPN10 |
| VM Network 1 | MPLS11 |

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

9. Click on **Finish** to deploy your DC-vEdge2-podX VM

Deploy OVF Template

| | | |
|-------------------------------|------------------------|---|
| ✓ 1 Select an OVF template | Provisioning type | Deploy from template |
| ✓ 2 Select a name and folder | Name | DC-vEdge2 |
| ✓ 3 Select a compute resource | Template name | viptela-edge-genericx86-64-20200414061026 |
| ✓ 4 Review details | Download size | 231.2 MB |
| ✓ 5 Select storage | Size on disk | 10.2 GB |
| ✓ 6 Select networks | Folder | SWAT-Labs-GHI |
| 7 Ready to complete | Resource | ghi-ms04.swat4partners.com |
| | Storage mapping | 1 |
| | All disks | Datastore: ghi-ms04-ds; Format: Thick provision lazy zeroed |
| | Network mapping | 4 |
| | VM Network 3 | SiteDC-VPN20 |
| | VM Network | Management |
| | VM Network 2 | SiteDC_VPN10 |
| | VM Network 1 | MPLS11 |
| | IP allocation settings | |
| | IP protocol | IPv4 |
| | IP allocation | Static - Manual |

CANCEL

BACK

FINISH

10. Once the VM is deployed, right click **DC-vEdge2-podX** and click Edit settings.
11. Choose to **Add a new device** (top right corner) and select Network Adapter to add one (since our deployed VM has only 4 Network Adapters but we will need 5 for our lab)
12. Click on the drop down next to **New Network** and click on *Browse*

Edit Settings | DC-vEdge2

X

Virtual Hardware VM Options

ADD NEW DEVICE

| | | |
|---------------------|---|---|
| > CPU | 4 | GB |
| > Memory | 2 | GB |
| > Hard disk 1 | 10.2248783111 | GB |
| > Network adapter 1 | Management | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 2 | MPLS11 | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 3 | SiteDC_VPN10 | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 4 | SiteDC-VPN20 | <input checked="" type="checkbox"/> Connect... |
| > New Network * | MPLS11 | <input checked="" type="checkbox"/> Connect... <input type="button" value="X"/> |
| > CD/DVD drive 1 | <input type="button" value="Browse ..."/> | <input type="checkbox"/> Connect... |
| > Video card | Auto-detect settings | |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface | |
| > Other | Additional Hardware | |

CANCEL

OK

13. Choose the **Internet** Network and click on OK. Make sure the Network Adapters match with the second image below and click on OK again

Edit Settings | DC-vEdge2

Virtual Hardware VM Options

ADD NEW DEVICE

- > CPU
- > Memory
- > Hard disk 1
- > Network adapter
- > CD/DVD drive
- > Video card
- VMCI device
- > Other

Select Network

Filter

| Name | Distributed Switch |
|--------------------|--------------------|
| 64 | GHI-DSwitch |
| DPortGroup | GHI-DSwitch |
| GHI-Pods-mPool | GHI-DSwitch |
| GHI-vMotion | GHI-DSwitch |
| Internet | -- |
| Management | -- |
| Management_VLAN100 | GHI-DSwitch |
| MPLS10 | -- |

40 items

CANCEL

OK

Additional Hardware

CANCEL

OK

| | | |
|---------------------|--------------|---|
| > Network adapter 1 | Management | <input checked="" type="checkbox"/> Connected |
| > Network adapter 2 | MPLS11 | <input checked="" type="checkbox"/> Connected |
| > Network adapter 3 | SiteDC_VPN10 | <input checked="" type="checkbox"/> Connected |
| > Network adapter 4 | SiteDC-VPN20 | <input checked="" type="checkbox"/> Connected |
| > Network adapter 5 | Internet | <input checked="" type="checkbox"/> Connected |

14. Click on DC-vEdge2-podX and choose to power it on

Task List

- [Creating the DC-vEdge2 VM](#)
 - [Overview](#)
 - [Deploying the DC-vEdge2 VM on vCenter](#)
- [Onboarding DC-vEdge2](#)
 - [Bootstrapping DC-vEdge2 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

Onboarding DC-vEdge2

Bootstrapping DC-vEdge2 (Initial Configuration)

Use the following information in this section (some of the information will be used later)

| SITE ID | SYSTEM IP | VM | Network Adapter | Network Adapter | Management | Interface | IP | Gateway |
|---------|---------------|-----------|-----------------|-----------------|--------------------|-----------|-----------------|-------------|
| 1 | 10.255.255.12 | DC-vEdge2 | 1 | Network Adapter | Management Adapter | eth0 | 192.168.0.11/24 | 192.168.0.1 |

| | | | | | |
|--|-------------------|--------------|-------|-------------------|---------------|
| | Network Adapter 2 | MPLS11 | ge0/1 | 192.0.2.6/30 | 192.0.2.5 |
| | Network Adapter 3 | SiteDC_VPN10 | ge0/2 | 10.100.10.3/24 | 10.100.10.1 |
| | Network Adapter 4 | SiteDC-VPN20 | ge0/3 | 10.100.20.3/24 | 10.100.20.1 |
| | Network Adapter 5 | Internet | ge0/0 | 100.100.100.11/24 | 100.100.100.1 |

1. Console in to the DC-vEdge2 VM from vCenter (you should already be logged in from our last activity)
2. Wait for the VM to prompt you for the username and password and enter the credentials given below. If you get a message stating that they are incorrect, wait for 30 seconds and try again (since the processes need to initialize before you can log in)

| Username | Password |
|----------|----------|
| admin | admin |

Note: From version 19.2, the password will need to be reset on initial login. For this lab, we will reset the password to admin.

3. Enter the configuration enumerated below. Unfortunately, this will need to be typed out since the console isn't copy-paste friendly

DC-vEdge2

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name DC-vEdge2
vedge(config-system)# system-ip 10.255.255.12
vedge(config-system)# site-id 1
vedge(config-system)# organization-name "swat-sdwanlab"
vedge(config-system)# vbond 100.100.100.3
vedge(config-system)# exit
vedge(config)# vpn 0
vedge(config-vpn-0)# ip route 0.0.0.0/0 100.100.100.1
vedge(config-vpn-0)# interface ge0/0
vedge(config-interface-ge0/0)# ip address 100.100.100.11/24
vedge(config-interface-ge0/0)# no tunnel-interface
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# exit
vedge(config)# vpn 512
vedge(config-vpn-512)# ip route 0.0.0.0/0 192.168.0.1
vedge(config-vpn-512)# interface eth0
vedge(config-interface-eth0)# ip address 192.168.0.11/24
vedge(config-interface-eth0)# no shutdown
vedge(config-interface-eth0)# commit and-quit
Commit complete.
DC-vEdge2#
```

```
conf t
system
host-name DC-vEdge2
system-ip 10.255.255.12
site-id 1
organization-name "swat-sdwanlab"
vbond 100.100.100.3
exit
!
vpn 0
ip route 0.0.0.0/0 100.100.100.1
interface ge0/0
ip address 100.100.100.11/24
no tunnel-interface
no shutdown
exit
!
```

```
exit
!
vpn 512
  ip route 0.0.0.0/0 192.168.0.1
  interface eth0
    ip address 192.168.0.11/24
    no shutdown
!
commit and-quit
```

4. Open **Putty** and double-click the saved session for DC-vEdge2 (or **SSH** to **192.168.0.11**)

Putty Configuration

?

X

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
- Selection
- Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

192.168.0.11 22

Connection type:

Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

DC-vEdge2

Default Settings

CentralGW

DC-vEdge1

DC-vEdge2

cEdge40

cEdge50

cEdge51

Load

Save

Delete

Close window on exit:

Always Never Only on clean exit

About

Help

Open

Cancel

5. Choose Yes to accept the certificate, if prompted

PuTTY Security Alert



WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.

The new ecdsa-sha2-nistp256 key fingerprint is:

ecdsa-sha2-nistp256 256

7c:de:34:0d:98:36:6a:64:a1:69:07:d8:68:44:d4:8f

If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.

If you want to carry on connecting but without updating the cache, hit No.

If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

Yes

No

Cancel

Help

6. Log in using the same credentials as Step 2.

Task List

- [Creating the DC-vEdge2 VM](#)
 - [Overview](#)
 - [Deploying the DC-vEdge2 VM on vCenter](#)

- Onboarding DC-vEdge2
 - [Bootstrapping DC-vEdge2 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

Installing certificates and activating the vEdge

1. Type `vshell` and enter `scp admin@192.168.0.6:ROOTCA.pem .` to copy the ROOTCA.pem certificate to the vEdge. Commands can be copy-pasted now since we have SSH'd in to the vEdge (there is a dot at the end of the scp command). Enter `yes` when prompted and enter the password of vManage (i.e. admin). Exit when done with this step.

```
vshell  
scp admin@192.168.0.6:ROOTCA.pem .
```

2. Go to the vManage GUI (<https://192.168.0.6>) and log in, if logged out. Navigate to **Configuration => Devices** (from the left-hand side, click on the cog wheel to access the configuration options)

Cisco vManage

DASHBOARD | MAIN DASHBOARD

Configuration 2 ↑ Part - 2

WAN Edge - 0

vBond - 1 1 ↑

vManag 1 ✓

Devices

TLS/SSL Proxy Devices 2

Certificates 0

Network Design 0

Templates

Policies

Security 20

Unified Communications 0

Cloud onRamp for SaaS 0

Cloud onRamp for IaaS

Cloud onRamp for Colocation

No data to display

Site Health (Total 0)

- Full WAN Connectivity 0 sites
- Partial WAN Connectivity 0 sites
- No WAN Connectivity 0 sites

WAN Edge Health (Total 0)

Normal 0 Warning 0 Error 0

Application-Aware Routing

| Tunnel Endpoints | Avg. Latency (ms) |
|------------------|-------------------|
| No data | |

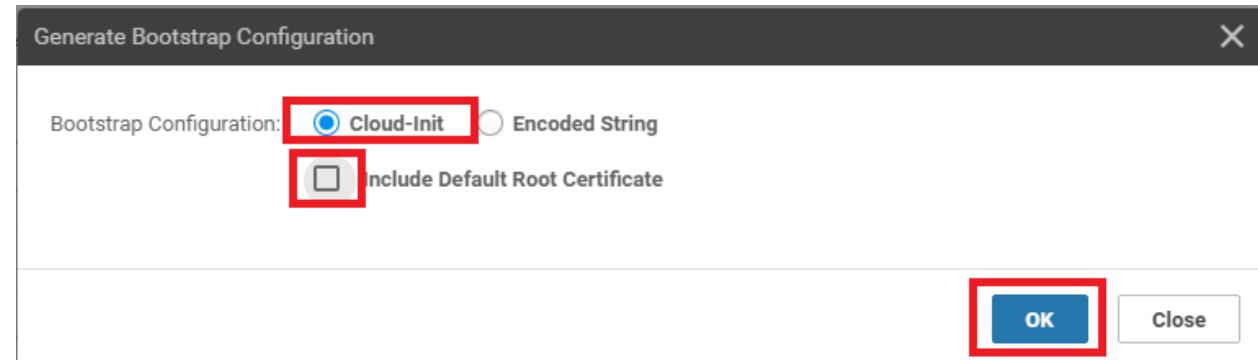
The screenshot shows the Cisco vManage main dashboard. On the left, a sidebar lists various management categories like Configuration, Devices, Policies, and Security. The 'Devices' section is currently selected and shows a count of 2. The main panel displays several key metrics: Site Health (Total 0), WAN Edge Health (Total 0), and Application-Aware Routing (No data). The URL in the browser bar is https://192.168.0.6/index.html#/app/config/devices/vedae.

- Choose any vEdge Cloud device (it doesn't matter which one you pick, as long as it is a vEdge Cloud) and click on the three dots at the extreme right-hand side. Choose to Generate Bootstrap Configuration

The screenshot shows the Cisco vManage interface with the title bar "Cisco vManage" and "vSphere - DC-vEdge2 - Summary". The main window displays a "WAN Edge List" table with 20 rows. A context menu is open over a row for a vEdge Cloud device, listing options: "Running Configuration", "Local Configuration", "Delete WAN Edge", "Copy Configuration", "Generate Bootstrap Configuration" (which is highlighted with a red box), "Template Log", and "Device Bring Up".

| State | Device Model | Chassis Number | Serial No./Token | Enterprise Cert Serial No. | Enterprise Cert Expiration Date | Hostname | System IP | Site ID | Mode | ... |
|-------------|---------------------------------------|---------------------------|------------------|----------------------------|---------------------------------|---------------|-----------|------------------|------|-----|
| CSR1000v | CSR-44C7CE5A-4149-E696-C8A8-415C... | Token: fc40de6570e72... | NA | NA | -- | -- | -- | CLI | ... | |
| CSR1000v | CSR-D6DB39FC-C3B3-BB55-7E9D-7CD... | Token: f2b5ab9798... | NA | NA | -- | -- | -- | CLI | ... | |
| CSR1000v | CSR-834E40DC-C35B-80E1-0E81-76E59... | Token: bba9cae0c9... | NA | NA | -- | -- | -- | CLI | ... | |
| CSR1000v | CSR-D405F5BA-B975-8944-D1A3-7E0B... | Token: e78aaefc1ebd2... | NA | NA | -- | -- | -- | CLI | ... | |
| CSR1000v | CSR-D1837F56-6A1A-1850-7C1C-E1C6... | Token: 90ffd2f29997ff8... | NA | NA | -- | -- | -- | CLI | ... | |
| CSR1000v | CSR-5E992295-1362-0B6E-EFF8-25CC... | Token: 1da14330e171... | NA | NA | -- | -- | -- | CLI | ... | |
| CSR1000v | CSR-04F492E-44F0-E4DC-D30D-60C0... | Token: 4e6009936f02... | NA | NA | -- | -- | -- | CLI | ... | |
| vEdge Cloud | e474c5fd-8c87-4376-7cac-ba50b2c91... | 7175AE0F | NA | NA | DC-vEdge1 | 10.255.255.11 | 1 | CLI | ... | |
| vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-469966cd1c3 | Token: 908adb0239fd... | NA | NA | -- | -- | -- | CLI | ... | |
| vEdge Cloud | b7fd7295-58af-6761-e914-6fe2edff1609 | Token: 945e9871624... | NA | NA | -- | -- | -- | ... | | |
| vEdge Cloud | ddde90f0-dc62-7e6-510f-08d96608537d | Token: 4c583475c7d4... | NA | NA | -- | -- | -- | ... | | |
| vEdge Cloud | 17026153-109e-be4b-6dce-482fc043aa... | Token: 3692590e4778... | NA | NA | -- | -- | -- | ... | | |
| CSR1000v | CSR-26217DA0-1B63-80DE-11C9-125F... | Token: 8dc7b557b60d... | NA | NA | -- | -- | -- | ... | | |
| CSR1000v | CSR-F960E020-B7C9-887F-46A8-F4537... | Token: 50cc04634ac4... | NA | NA | -- | -- | -- | ... | | |
| CSR1000v | CSR-25925FBC-07F3-0732-E127-EA95... | Token: 6ced66053d46... | NA | NA | -- | -- | -- | ... | | |
| vEdge Cloud | 35bd9619-116c-4e4c-e34c-706645... | Token: ed778f56f9ab0... | NA | NA | -- | -- | -- | ... | | |
| vEdge Cloud | 005424c-2d57-411c-250d-ee991e0a4e... | Token: 564f154c6e14d... | NA | NA | -- | -- | -- | Activate Windows | ... | |
| vEdge Cloud | 21292349-2c9f-7aaef-28f5-a87e4d0054cb | Token: b6046dee14a2a... | NA | NA | -- | -- | -- | Go to Settings | ... | |
| vEdge Cloud | 7a59574a-a5bb-ec75-3a9d-2fd3ad02h4 | Token: ce9fbfc06da1f | NA | NA | -- | -- | -- | CLI | ... | |

- Choose **Cloud-Init** and uncheck **Include Default Root Certificate**. Click on OK



- Make note of the **UUID** and the **OTP** values. These will be required to activate the vEdge. It's best to copy the string and place it in notepad, since we will need to use it in our SSH session to the DC-vEdge2 device. Alternatively, leave this popup open and we can come back to it when required

Generate Bootstrap Configuration

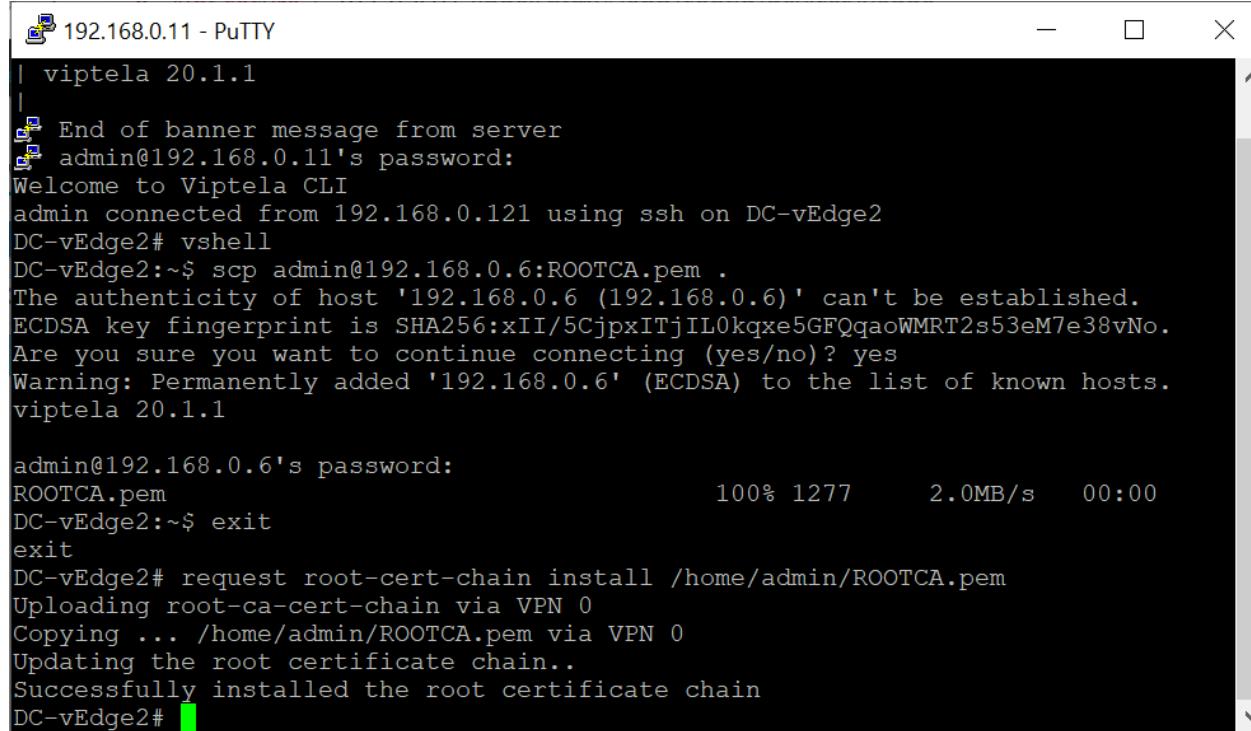
X

Download

```
#cloud-config
  ...
  - uid : 0cdd4f0e-f2f1-fe75-866c-469966cda1c3
  - vbond : 100.100.100.3
  - otp : 908adb0239ffd2018f25ad423fc6a1b9
  - org : swat-suwanlab
  - rcc : true
ca-certs:
  remove-defaults: false
  trusted:
  - |
    -----BEGIN CERTIFICATE-----
    MIIF7DCCBNsgAwIBAgIQbsx6pacDIAm4rz06VLUkTANBgkqhkiG9w0BAQUFADC
    .....
```

Close

6. Go back to the Putty session for DC-vEdge2 and enter `request root-cert-chain install /home/admin/ROOTCA.pem` to install the root cert chain. It should install successfully



```
| viptela 20.1.1
|
| End of banner message from server
| admin@192.168.0.11's password:
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on DC-vEdge2
DC-vEdge2# vshell
DC-vEdge2:~$ scp admin@192.168.0.6:ROOTCA.pem .
The authenticity of host '192.168.0.6 (192.168.0.6)' can't be established.
ECDSA key fingerprint is SHA256:xII/5CjpxITjIL0kqxe5GFQqaoWMRT2s53eM7e38vNo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.6' (ECDSA) to the list of known hosts.
viptela 20.1.1

admin@192.168.0.6's password:
ROOTCA.pem                                         100% 1277      2.0MB/s   00:00
DC-vEdge2:~$ exit
exit
DC-vEdge2# request root-cert-chain install /home/admin/ROOTCA.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
DC-vEdge2#
```

```
request root-cert-chain install /home/admin/ROOTCA.pem
```

7. Enter `tunnel-interface`, `encapsulation ipsec` and `allow-service all` under `interface ge0/0` to bring up the tunnel Interface. Make sure to `commit and-quit` in order to write the configuration change

```
config t
vpn 0
interface ge0/0
  tunnel-interface
  encapsulation ipsec
  allow-service all
exit
!
commit and-quit
```

This ensures that our vEdge is now able to establish control connections with the vManage and vSmarts via the vBond. However, these connections will not be fully formed till we don't activate the vEdge itself

8. Issue the `request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)` command. Replace the (*Enter your UUID*) and (*Enter your OTP*) fields with the UUID and OTP generated in Step 5 (image below is an example, UUID and OTP may not match).

```
Entering configuration mode terminal
DC-vEdge2(config)# vpn 0
DC-vEdge2(config-vpn-0)# interface ge0/0
DC-vEdge2(config-interface-ge0/0)# tunnel-interface
DC-vEdge2(config-tunnel-interface)# encapsulation ipsec
DC-vEdge2(config-tunnel-interface)# allow-service all
DC-vEdge2(config-tunnel-interface)# commit and-quit
Commit complete.
DC-vEdge2#
DC-vEdge2#
DC-vEdge2#
DC-vEdge2#
DC-vEdge2# request vedge-cloud activate chassis-number 0cdd4f0e-f2f1-fe75-866c-4
69966cdalc3 token 908adb0239fdd2018f25ad423fc6alb9
```

request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)

This completes the Onboarding section for DC-vEdge2

Task List

- [Creating the DC-vEdge2 VM](#)
 - [Overview](#)
 - [Deploying the DC-vEdge2 VM on vCenter](#)
- [Onboarding DC-vEdge2](#)
 - [Bootstrapping DC-vEdge2 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

Onboarding Verification

1. Wait for a couple of minutes and run `show control connections` in the DC-vEdge2 CLI. We should see that the vEdge has been able to establish a DTLS tunnel with the vManage and the vSmarts. If you don't see any output, wait for a couple of minutes and run the command again

| DC-vEdge2# show control connections | | | | | | | | | | |
|-------------------------------------|------|--------------|------|--------|---------------|-------|---------------|-----------|------------|--------------------|
| TYPE | PEER | PEER | SITE | DOMAIN | PEER | | PEER | | CONTROLLER | |
| | | | | | PRIV | PEER | PORT | PUBLIC IP | | |
| vsmart | dtls | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12446 | 100.100.100.4 | 12446 | default | No up 0:00:05:37 0 |
| vsmart | dtls | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12446 | 100.100.100.5 | 12446 | default | No up 0:00:05:37 0 |
| vmanage | dtls | 10.255.255.1 | 1000 | 0 | 100.100.100.2 | 12446 | 100.100.100.2 | 12446 | default | No up 0:00:05:37 0 |

```
show control connections
```

Tip: You can also issue `show control connections-history` in the event of failures to find out why is the connection not working as expected. A few helpful commands are `show certificate installed`, `show certificate root-ca-cert`, `show control local-properties` and `show certificate validity`. Most of these commands give us details about the status of certificates on the device and are helpful in ascertaining the root cause of failure when control connections aren't getting established.

2. On the vManage GUI, navigate to **Monitor => Network Devices** (the computer icon on the left-hand side)

Cisco vManage

CONFIGURATION | DEVICES

Monitor

Geography

Network

Alarms

Events

Audit Log

ACL Log

Upload WAN Edge List **Export Bootstrap Configuration** **Sync Smart Account**

Search Options ▾

| Network | Chassis Number | Serial No./Token | Enterprise |
|--|--|---|------------|
| CSR1000v | CSR-44C7CE5A-4149-E696-C8A8-415C793FBF6C | Token - fc40de6570e725ba70c917d6511b8a6c | NA |
| CSR-D6DB39FC-C383-BB55-7E9D-7CDD85595DD1 | CSR-834E40DC-E358-8DE1-0E81-76E5984138F4 | Token - f28b5ab9789827383a9425d0aec4fe1a | NA |
| CSR-D405F5BA-B975-8944-D1A3-2E082AEE2A1D | CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3 | Token - b8a9cae09c975b49003634e8174b83b | NA |
| CSR1000v | CSR-5E992295-1362-0DB6-EEF8-25CC88F1CCCE | Token - e78aaefc1ebd2a11d900e88098a7949c | NA |
| vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b2c9159 | 7175AE0F | NA |
| vEdge Cloud | 0cd4f0e-f2f1-fe75-866c-469966cda1c3 | Token - 908adb0239fdd2018f25ad423fc6a1b9 | NA |
| vEdge Cloud | b7fd7295-58df-7671-e914-6fe2edff1609 | Token - 945eb9871624db4cc321c6197484ce09 | NA |
| vEdge Cloud | dde90ff0-dc62-77e6-510f-08d96608537d | Token - 4c583475c7d42f07e570dbcba42d3431f | NA |
| vEdge Cloud | 17026153-f09e-be4b-6dce-482fce43aab2 | Token - 3692590e47782dd2ae043b8a4369c145 | NA |
| CSR1000v | CSR-26217DA0-1B63-8DDE-11C9-125F527D3270 | Token - 8dc7b557b60d4cec5c22e3c143132c0d | NA |
| CSR1000v | CSR-F960E020-B7C9-887F-46A8-F45374B23E7D | Token - 50cc04634ac461d3d68d53f26a520c35 | NA |
| CSR1000v | CSR-25925FBC-07F3-0732-E127-EA95D24F8EEB | Token - 6ced66053d4698a4402a50b1b2c082f3 | NA |
| vEdge Cloud | 35bd96f9-1758-116c-4e4c-e34c7066459c | Token - ed778f56f9ab08994a1c1d8aa046385c | NA |
| vEdge Cloud | 005c424c-2d57-41fe-250d-ee991e0a4e93 | Token - 56f4f54ce614d27ba24350ec9a50572e | NA |
| vEdge Cloud | 21292349-2c9f-7aaf-28f5-a87e4d0054cb | Token - b6046deef4a2ae480f9cc18194152fb0 | NA |
| | 2fd3ad02b47c | Token - ce9fb6c06da1fba2ba06fd5001520fc2 | NA |

3. DC-vEdge2 should show up in the list of devices

| VPN GROUP | | VPN SEGMENT | |
|--------------|---------------|----------------------|-----------------------------------|
| Device Group | All | Search | Search Options |
| Hostname | System IP | Device Model | Chassis Number/ID |
| vmanage | 10.255.255.1 | vManage | dfea63a5-66d2-4e50-a07b-ec4ad4... |
| vSmart | 10.255.255.3 | vSmart | 20607a12-c0c8-4f46-a65f-5a547c... |
| vSmart2 | 10.255.255.4 | vSmart | 7f332491-cb6f-4843-8bf5-060f90... |
| vBond | 10.255.255.2 | vEdge Cloud (vBo...) | fc31c154-99c5-4267-971d-6c9ae7... |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b... |
| DC-vEdge2 | 10.255.255.12 | vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-46996c... |

4. Click on DC-vEdge2 and navigate to **Troubleshooting => Control Connections(Live view)**. You should see the vEdge successfully connected to 2 vSmarts and 1 vManage

□ MONITOR Network > Troubleshooting > Control Connections(Live View)

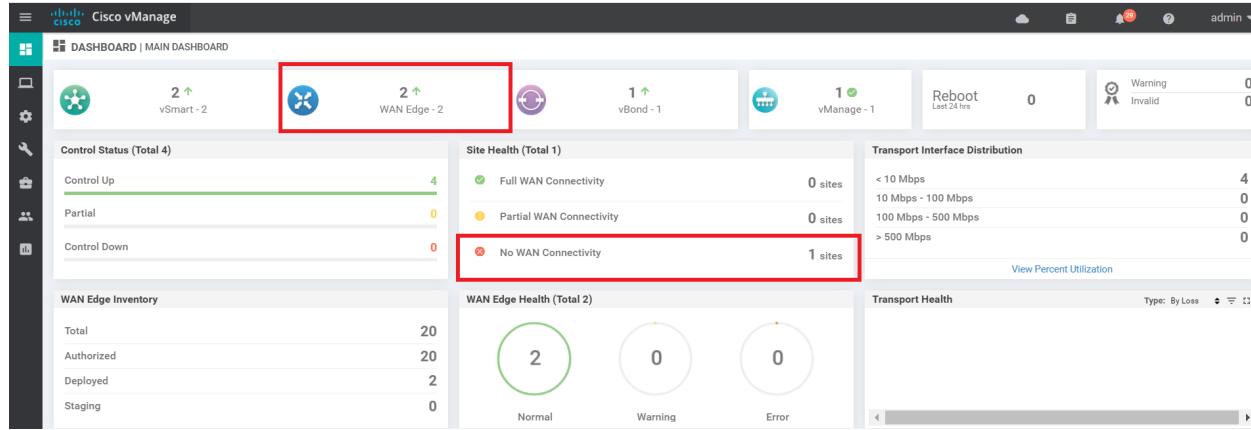
Select Device ▾ DC-vEdge2 | 10.255.255.12 Site ID: 1 Device Model: vEdge Cloud ⓘ

vSmart Control Connections (Expected: 2 | Actual: 2)

vSmart 2/2 vManage 1/1

| Controller | Local Status | Remote Status |
|--|--------------|---------------|
| DEFAULT Circuit (Expected:2 Actual:2) NAT:Not learned | | |
| vmanage 10.255.255.1(Preferred Controller) | ✓ | ✓ |
| vSmart 10.255.255.3(Preferred Controller) | ✓ | ✓ |
| vSmart2 10.255.255.4(Preferred Controller) | ✓ | ✓ |

5. On the main dashboard, notice that we now have two WAN Edges onboarded on DNAC. The site doesn't have WAN connectivity yet since BFD sessions are not being established as of now. This will change once we get more sites onboard



This completes the verification activity.

Task List

- [Creating the DC-vEdge2 VM](#)
 - [Overview](#)
 - [Deploying the DC-vEdge2 VM on vCenter](#)
- [Onboarding DC-vEdge2](#)
 - [Bootstrapping DC-vEdge2 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)
- [Helpful debugs and logs](#)

Helpful debugs and logs

Note: This section is optional and is intended as a learning activity. It is not required to go through this in order to complete the lab tasks successfully

1. On the CLI for DC-vEdge2, issue `debug vdaemon all` followed by `clear control connections`. This will tear down all the control connections and the vEdge will rebuilt the DTLS tunnels. We can capture the logs to see the process associated with the DTLS tunnels being built

```
debug vdaemon all  
clear control connections
```

2. Wait for a couple of minutes and go to `vshell`. Type `cat /var/log/tmplog/vdebug` to view the contents of the log file

3. Given below are a couple of sample outputs

```
local17.debug: May 14 16:13:32 vedge VDAEMON[1124]: vdaemon_dtis_verify_peer_cert[919]: #VDAEMON DBG_MISC-1: Validating device certificate.. serial # (9850FDA9D7604C21) "swat-sdwanlab"
local17.debug: May 14 16:13:32 vedge VDAEMON[1124]: vdaemon_dtis_verify_peer_cert[919]: #VDAEMON DBG_MISC-1: Validating device certificate.. serial # (9850FDA9D7604C22) "swat-sdwanlab"
local17.debug: May 14 16:13:32 vedge VDAEMON[1124]: vdaemon_send_tloc_info[8328]: #VDAEMON DBG_MISC-1: Sending tLOC: infamego.0 color:default spi:257 smarts:1 managed:1 state:UP LR encap:0 Lr hold time: 7000 Pairwise-Keys Disabled key-id:0
local17.debug: May 14 16:13:32 vedge VDAEMON[1124]: vdaemon_send_tloc_info[8333]: #VDAEMON DBG_MISC-1: tLOC - v4 public 100.100.100.10:12366 private 100.100.100.10:12366 public v6 ::::0 pr
tce ::::0
local17.debug: May 14 16:13:32 vedge VDAEMON[1124]: vdaemon_send_local_tloc_msg[137]: #VDAEMON DBG_MISC-1: Sending (Originator: 10.255.255.11 Color: 1 Encap: 2) tLOC: ADD: to TTM
local17.info: May 14 16:13:32 vedge VDAEMON[1124]: wvconfd_trap_send[833]: Processing trap viptelaSecurityControlConnectionStateChange
local17.info: May 14 16:13:32 vedge VDAEMON[1124]: %WvIptela-wedge-vdaemon-6-INFO=1400002: 5/14/2020 16:13:32 control-control-state-change severity-level:major host-name:""
wedgepeer-type:vsmart-peer-system-ip:10.255.255.1 peer-vmanage-system-ip:0.0.0.0 public-ip:100.100.100.4 public-port:12346 src-color:default
ctrl-color:default uptime:'00:00:00' new-state:up
local17.debug: May 14 16:13:32 vedge VDAEMON[1124]: wvconfd_trap_send[833]: Processing trap viptelaSecurityControlConnectionStateChange
local17.info: May 14 16:13:32 vedge VDAEMON[1124]: %WvIptela-wedge-vdaemon-6-INFO=1400002: Notification: 5/14/2020 16:13:32 control-control-state-change severity-level:major host-name:""
wedgepeer-type:vsmart-peer-system-ip:10.255.255.1 peer-vmanage-system-ip:0.0.0.0 public-ip:100.100.100.5 public-port:12346 src-color:default
ctrl-color:default uptime:'00:00:00' new-state:up
```

This completes our onboarding activity for DC-vEdge2.

Task List

- Creating the DC-vEdge2 VM
 - Overview
 - Deploying the DC-vEdge2 VM on vCenter
 - Onboarding DC-vEdge2
 - Bootstrapping DC-vEdge2 (Initial Configuration)
 - Installing certificates and activating the vEdge

- Onboarding Verification
- Helpful debugs and logs

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 15, 2020

Site last generated: Sep 1, 2020



Deploying a Single uplink (INET) vEdge

Summary: Deploying vEdge20 in Site 20. This vEdge has a single uplink to the Internet

Table of Contents

- [Creating the vEdge20 VM](#)
 - Overview
 - Deploying the vEdge20 VM on vCenter
- [Onboarding vEdge20](#)
 - Bootstrapping vEdge20 (Initial Configuration)
 - Installing certificates and activating the vEdge
- [Onboarding Verification](#)

⚠ Warning: This section might already be done, depending on your selected Lab Scenario. Most lab work will start [from here](#). The configuration given below can be used to review what was done to bring the Site up. If this VM is already deployed (check via vCenter), you **Do Not** need to perform these lab activities.

Task List

- Creating the vEdge20 VM
 - Overview
 - Deploying the vEdge20 VM on vCenter
- Onboarding vEdge20
 - Bootstrapping vEdge20 (Initial Configuration)
 - Installing certificates and activating the vEdge
- Onboarding Verification

Creating the vEdge20 VM

Overview

Note: There will be a number of repetitive tasks from the Deploying DC-vEdge1/DC-vEdge2 section.

Note: The important steps which will guide you through this activity will be earmarked, indicating a delta from the previous section.

This is what an earmarked step will look like

We will be deploying a vEdge at Site 20 via vCenter. Make note of the following information for this section. The IP Addressing will not be used for some of the Network Adapters until later.

| SITE ID | SYSTEM ID | VM | Network Adapter | Network | Interface | IP | Gateway |
|---------|---------------|--------------|-------------------|---------------|-----------|-------------------|---------------|
| 20 | 10.255.255.21 | vEdge20-podX | Network Adapter 1 | Management | eth0 | 192.168.0.20/24 | 192.168.0.1 |
| | | | Network Adapter 2 | TLOCEXT_vEdge | ge0/1 | 192.168.25.20/24 | |
| | | | Network Adapter 3 | Site20-VPN10 | ge0/2 | 10.20.10.2/24 | |
| | | | Network Adapter 4 | Site20-VPN20 | ge0/3 | 10.20.20.2/24 | |
| | | | Network Adapter | Internet | ge0/0 | 100.100.100.20/24 | 100.100.100.1 |

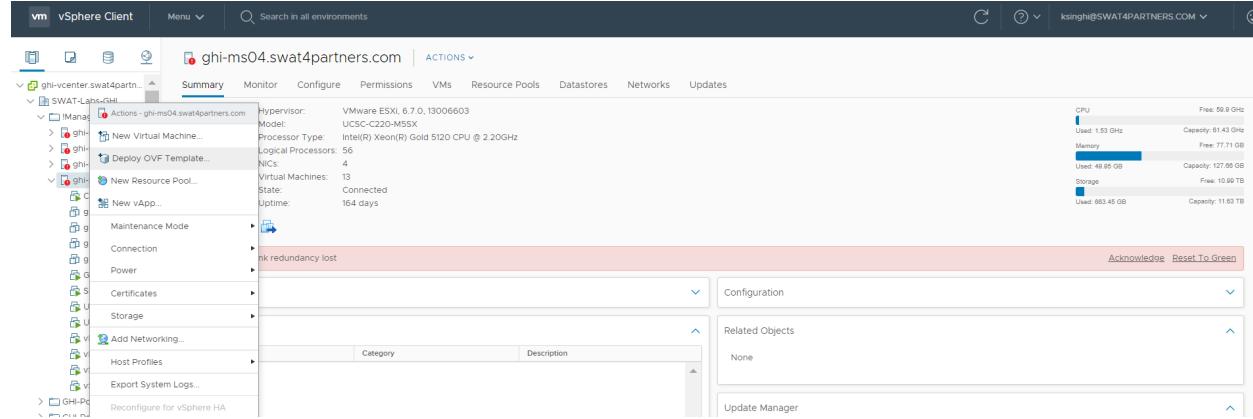
| | |
|-----------------|------------------|
| Adapter | |
| 5 | |
| Network Adapter | TLOCEXT2_vEdge |
| | ge0/4 |
| | 192.168.26.20/24 |
| 6 | |

Task List

- [Creating the vEdge20 VM](#)
 - [Overview](#)
 - [Deploying the vEdge20 VM on vCenter](#)
- [Onboarding vEdge20](#)
 - [Bootstrapping vEdge20 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)

Deploying the vEdge20 VM on vCenter

1. Click on the bookmark for vCenter or navigate to the following URL: <https://10.2.1.50/ui>. Log in with the credentials provided for your POD.
2. Right click on the host and choose to **Deploy OVF Template**



3. Choose the **Local file** option and click on **Choose files**. Navigate to the SD-WAN images folder and select the file beginning with *viptela-edge-*. Click on Next.
4. Change the Virtual Machine name to **vEdge20-podX** and click on Next (where X is your POD number, image below does not have the suffix of podX)

Note: We will only use the podX suffix over here to distinguish between different VMs in our Data Center. The rest of the guide will refer to this VM as **vEdge20**

Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

- ▽ ghi-vcenter.swat4partners.com
 - > SWAT-Labs-GHI
 - > slc-vcenter.swat4partners.com

CANCEL

BACK

NEXT

5. Select the host assigned to you (image shown as an example only) and click on Next

Note: If the screen gets stuck over here at **Validating** then close Chrome and open the vCenter in Internet Explorer, going through the same steps. Deployment should go through. This is a known issue with Google Chrome.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

The screenshot shows a tree view of compute resources. The root node is 'SWAT-Labs-GHI', which contains a folder 'Management-Shared Services' and several host entries. The host entries are: ghi-ms01.swat4partners.com, ghi-ms02.swat4partners.com, ghi-ms03.swat4partners.com, and ghi-ms04.swat4partners.com. The host ghi-ms04.swat4partners.com is currently selected, indicated by a light blue background. Below the main tree, there is a list of 'GHI-Pod' nodes from Pod01 to Pod10.

- ✓ SWAT-Labs-GHI
 - ✓ Management-Shared Services
 - ghi-ms01.swat4partners.com
 - ghi-ms02.swat4partners.com
 - ghi-ms03.swat4partners.com
 - ghi-ms04.swat4partners.com
 - GHI-Pod01
 - GHI-Pod02
 - GHI-Pod03
 - GHI-Pod04
 - GHI-Pod05
 - GHI-Pod06
 - GHI-Pod07
 - GHI-Pod08
 - GHI-Pod09
 - GHI-Pod10

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

6. Review the details shown and click on Next

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource

Review details
Verify the template details.

4 Review details

- 5 Select storage
- 6 Select networks
- 7 Ready to complete

| | |
|---------------------|--|
| Publisher | No certificate present |
| Download size | 231.2 MB |
| Size on disk | 234.1 MB (thin provisioned) |
| | 10.2 GB (thick provisioned) |
| Extra configuration | <pre>time.synchronize.tools.startup = FALSE virtualHW.productCompatibility = hosted time.synchronize.restore = FALSE time.synchronize.continue = FALSE time.synchronize.shrink = FALSE time.synchronize.resume.disk = FALSE time.synchronize.tools.enable = FALSE time.synchronize.resume.host = FALSE</pre> |

CANCEL

BACK

NEXT

7. Choose the Datastore and click on Next

8. Populate the VM Networks as per the image given below

⚠ Important: Please make sure that these look exactly as shown below

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**

7 Ready to complete

Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|----------------|---------------------|
| VM Network 3 | Site20-VPN20 |
| VM Network | Management |
| VM Network 2 | Site20-VPN10 |
| VM Network 1 | TLOCEXT_vEDGE |

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

9. Click on **Finish** to deploy your vEdge20-podX VM

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 **Select a name and folder**
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Ready to complete**

Ready to complete
Click Finish to start creation.

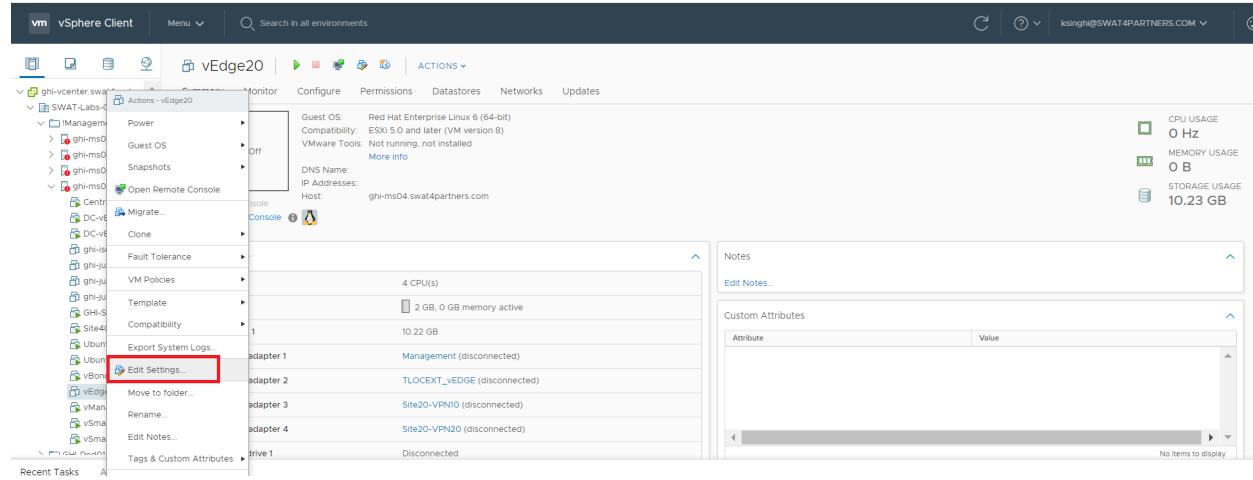
| | |
|-------------------|---|
| Provisioning type | Deploy from template |
| Name | vEdge20 |
| Template name | viptela-edge-genericx86-64-20200414061026 |
| Download size | 231.2 MB |
| Size on disk | 10.2 GB |
| Folder | SWAT-Labs-GHI |
| Resource | ghi-ms04.swat4partners.com |
| Storage mapping | 1 |
| All disks | Datastore: ghi-ms04-ds; Format: Thick provision lazy zeroed |
| Network mapping | 4 |
| VM Network 3 | Site20-VPN20 |
| VM Network | Management |
| VM Network 2 | Site20-VPN10 |
| VM Network 1 | TLOCEXT_vEDGE |

CANCEL

BACK

FINISH

10. Once the VM is deployed, right click **vEdge20-podX** and click Edit settings.



11. Choose to **Add a new device** (top right corner) and select Network Adapter to add one (since our deployed VM has only 4 Network Adapters but we will need 6 for our lab). Add another network device this way, for a total of 6 network adapters.
12. Click on the drop down next to the first **New Network** and click on *Browse*

Edit Settings | vEdge20

X

Virtual Hardware VM Options

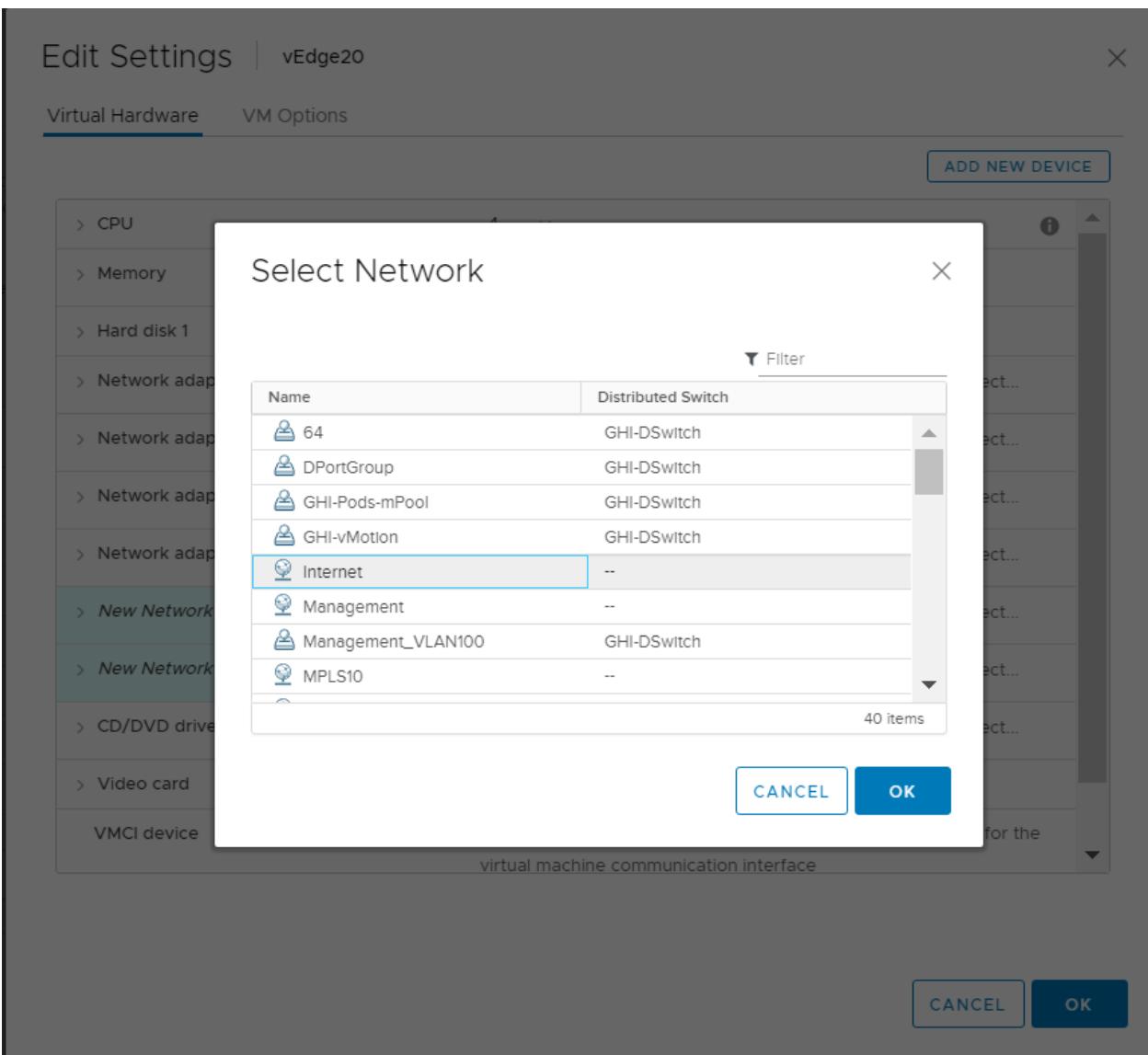
ADD NEW DEVICE

| | | |
|---|---|---|
| > CPU | 4 | v |
| > Memory | 2 | GB v |
| > Hard disk 1 | 10.224878311! | GB v |
| > Network adapter 1 | Management v | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 2 | TLOCEXT_vEDGE v | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 3 | Site20-VPN10 v | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 4 | Site20-VPN20 v | <input checked="" type="checkbox"/> Connect... |
| > New Network * | Management v | <input checked="" type="checkbox"/> Connect... X |
| > New Network * | Management Browse ... | <input checked="" type="checkbox"/> Connect... |
| > CD/DVD drive 1 ! | Host Device v | <input type="checkbox"/> Connect... |
| > Video card | Auto-detect settings v | |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface | |

CANCEL

OK

13. Choose the **Internet** Network and click on OK.



14. Click on the drop down for the second **New Network** entry, added as a result of adding two network adapters and click on *Browse*. Select the **TLOCEXT2_vEdge** Network

Edit Settings | vEdge20

X

Virtual Hardware VM Options

ADD NEW DEVICE

- > CPU
- > Memory
- > Hard disk 1
- > Network adapter
- > Network adapter
- > Network adapter
- > Network adapter
- > New Network Adapter
- > New Network Adapter
- > CD/DVD drive
- > Video card
- VMCI device

Select Network

Filter

| Name | Distributed Switch |
|----------------|--------------------|
| SiteDC-VPN10 | -- |
| SiteDC-VPN20 | -- |
| SiteDC_VPN10 | -- |
| TLOCEXT2_vEdge | -- |
| TLOCEXT_cEDGE | -- |
| TLOCEXT_vEDGE | -- |
| Uplink | -- |
| VM Network | -- |
| VPN10 | -- |

40 items

CANCEL

OK

virtual machine communication interface

CANCEL

OK

15. Make sure the Network Adapters match with the image below and click on OK

| | | |
|---------------------|-----------------|---|
| > Network adapter 1 | Management | <input checked="" type="checkbox"/> Connected |
| > Network adapter 2 | TLOC EXT_vEDGE | <input checked="" type="checkbox"/> Connected |
| > Network adapter 3 | Site20-VPN10 | <input checked="" type="checkbox"/> Connected |
| > Network adapter 4 | Site20-VPN20 | <input checked="" type="checkbox"/> Connected |
| > Network adapter 5 | Internet | <input checked="" type="checkbox"/> Connected |
| > Network adapter 6 | TLOC EXT2_vEdge | <input checked="" type="checkbox"/> Connected |

16. Click on vEdge20-podX and choose to power it on

Task List

- [Creating the vEdge20 VM](#)
 - [Overview](#)
 - [Deploying the vEdge20 VM on vCenter](#)
- [Onboarding vEdge20](#)
 - [Bootstrapping vEdge20 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)

Onboarding vEdge20

Bootstrapping vEdge20 (Initial Configuration)

Use the following information in this section (some of the information will be used later)

| SITE ID | SYSTEM ID | VM | Network Adapter | Network Management | Interface eth0 | IP 192.168.0.20/24 | Gateway 192.168.0.1 |
|---------|---------------|---------|-----------------|--------------------|----------------|--------------------|---------------------|
| 20 | 10.255.255.21 | vEdge20 | Network | Management | | | |

| | | | | |
|----------------------|----------------|-------|-------------------|---------------|
| Adapter 1 | | | | |
| Network Adapter 2 | TLOCEXT_vEdge | ge0/1 | 192.168.25.20/24 | |
| Network Adapter 3 | Site20-VPN10 | ge0/2 | 10.20.10.2/24 | |
| Network Adapter 4 | Site20-VPN20 | ge0/3 | 10.20.20.2/24 | |
| Network Adapter 5 | Internet | ge0/0 | 100.100.100.20/24 | 100.100.100.1 |
| Network Adapter 6 | TLOCEXT2_vEdge | ge0/4 | 192.168.26.20/24 | |

1. Console in to the vEdge20 VM from vCenter (you should already be logged in from our last activity)
2. Wait for the VM to prompt you for the username and password and enter the credentials given below. If you get a message stating that they are incorrect, wait for 30 seconds and try again (since the processes need to initialize before you can log in).

| Username | Password |
|----------|----------|
| admin | admin |

Note: From version 19.2, the password will need to be reset on initial login. For this lab, we will reset the password to `admin`.

3. Enter the configuration enumerated below. Unfortunately, this will need to be typed out since the console isn't copy-paste friendly

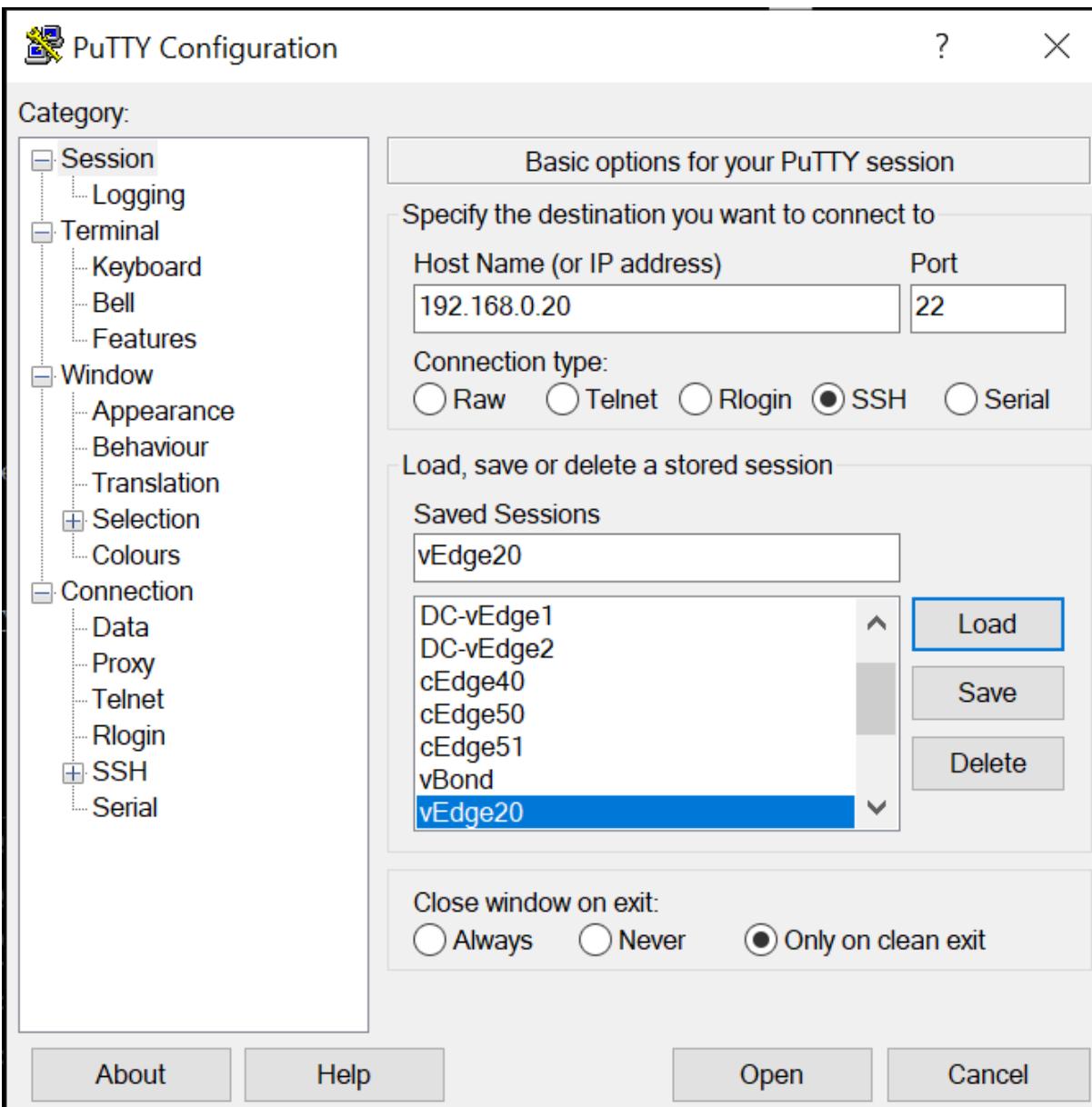
vEdge20

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vEdge20
vedge(config-system)# system-ip 10.255.255.21
vedge(config-system)# site-id 20
vedge(config-system)# organization-name "swat-sdwanlab"
vedge(config-system)# vbond 100.100.100.3
vedge(config-system)# exit
vedge(config)# vpn 0
vedge(config-vpn-0)# ip route 0.0.0.0/0 100.100.100.1
vedge(config-vpn-0)# interface ge0/0
vedge(config-interface-ge0/0)# ip address 100.100.100.20/24
vedge(config-interface-ge0/0)# no tunnel-interface
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# exit
vedge(config)# vpn 512
vedge(config-vpn-512)# ip route 0.0.0.0/0 192.168.0.1
vedge(config-vpn-512)# interface eth0
vedge(config-interface-eth0)# ip address 192.168.0.20/24
vedge(config-interface-eth0)# no shutdown
vedge(config-interface-eth0)# commit and-quit
Commit complete.
vEdge20#
```

```
conf t
system
host-name vEdge20
system-ip 10.255.255.21
site-id 20
organization-name "swat-sdwanlab"
vbond 100.100.100.3
exit
!
vpn 0
ip route 0.0.0.0/0 100.100.100.1
interface ge0/0
ip address 100.100.100.20/24
no tunnel-interface
no shutdown
exit
!
```

```
exit
!
vpn 512
  ip route 0.0.0.0/0 192.168.0.1
  interface eth0
    ip address 192.168.0.20/24
    no shutdown
!
commit and-quit
```

4. Open **Putty** and double-click the saved session for vEdge20 (or **SSH to 192.168.0.20**)



5. Choose Yes to accept the certificate, if prompted

PuTTY Security Alert



WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.

The new ecdsa-sha2-nistp256 key fingerprint is:

ecdsa-sha2-nistp256 256

7c:de:34:0d:98:36:6a:64:a1:69:07:d8:68:44:d4:8f

If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.

If you want to carry on connecting but without updating the cache, hit No.

If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

Yes

No

Cancel

Help

6. Log in using the same credentials as Step 2.

Task List

- [Creating the vEdge20 VM](#)
 - [Overview](#)
 - [Deploying the vEdge20 VM on vCenter](#)

- Onboarding vEdge20
 - [Bootstrapping vEdge20 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- Onboarding Verification

Installing certificates and activating the vEdge

1. Type `vshell` and enter `scp admin@192.168.0.6:ROOTCA.pem .` to copy the ROOTCA.pem certificate to the vEdge. Commands can be copy-pasted now since we have SSH'd in to the vEdge (there is a dot at the end of the scp command). Enter `yes` when prompted and enter the password of vManage (i.e. admin). Exit when done with this step.

```
vshell  
scp admin@192.168.0.6:ROOTCA.pem .
```

2. Go to the vManage GUI (<https://192.168.0.6>) and log in, if logged out. Navigate to **Configuration => Devices** (from the left-hand side, click on the cog wheel to access the configuration options)

Cisco vManage

DASHBOARD | MAIN DASHBOARD

Configuration 2 ↑ Part - 2

WAN Edge - 0

vBond - 1 1 ↑

vManag 1 ✓

Devices

TLS/SSL Proxy Devices 2

Certificates 0

Network Design 0

Templates

Policies

Security 20

Unified Communications 0

Cloud onRamp for SaaS 0

Cloud onRamp for IaaS

Cloud onRamp for Colocation

No data to display

Site Health (Total 0)

- Full WAN Connectivity 0 sites
- Partial WAN Connectivity 0 sites
- No WAN Connectivity 0 sites

WAN Edge Health (Total 0)

Normal 0 Warning 0 Error 0

Application-Aware Routing

| Tunnel Endpoints | Avg. Latency (ms) |
|------------------|-------------------|
| No data | |

The screenshot shows the Cisco vManage main dashboard. On the left, a sidebar lists various management categories like Configuration, Devices, Policies, and Security. The 'Devices' section is currently selected and shows a count of 2. The main panel displays several key metrics: Site Health (Total 0), WAN Edge Health (Total 0), and Application-Aware Routing (No data). Each metric includes a summary table with three columns: Normal, Warning, and Error, all of which show 0. A status bar at the bottom indicates the URL as https://192.168.0.6/index.html#/app/config/devices/vedae.

- Choose any vEdge Cloud device (it doesn't matter which one you pick, as long as it is a vEdge Cloud) and click on the three dots at the extreme right-hand side. Choose to Generate Bootstrap Configuration

CONFIGURATION | DEVICES

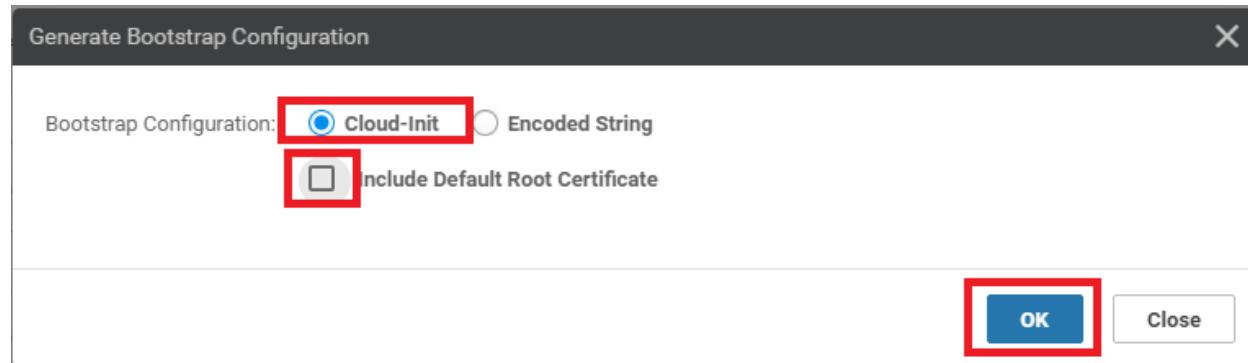
WAN Edge List Controllers

Change Mode **Upload WAN Edge List** **Export Bootstrap Configuration** **Sync Smart Account**

Total Rows: 20

| State | Device Model | Chassis Number | Serial No./Token | Enterprise Cert Serial No | Enterprise Cert Expiration Date | Hostname | System IP | Site ID | Mode | Actions |
|-------------|---------------------------------------|---------------------------------------|---------------------------|---------------------------|---------------------------------|-----------|--------------|-----------------|---------------------------------------|---------|
| CSR1000v | CSR-44C7C5A-4149-E696-C8A-415C... | CSR-44C7C5A-4149-E696-C8A-415C... | Token - fc40de6570e2... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-6DD839FC-C383-BB55-7E9D-7C0... | CSR-6DD839FC-C383-BB55-7E9D-7C0... | Token - f28b5ab7989... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-834E40DC-E358-8DE1-0E81-76E5... | CSR-834E40DC-E358-8DE1-0E81-76E5... | Token - b8a9cae09c9... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-9405F5BA-B975-8944-D1A3-2E0B... | CSR-9405F5BA-B975-8944-D1A3-2E0B... | Token - e78aaefc1ebd2... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-D1837F36-6A1A-1850-7C1C-E1C6... | CSR-D1837F36-6A1A-1850-7C1C-E1C6... | Token - 299ffdf299fffb... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-5E992295-1362-0DB6-EEF9-25CC... | CSR-5E992295-1362-0DB6-EEF9-25CC... | Token - 1da14330e171... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-04F9482E-44F0-E40C-D30D-60C0... | CSR-04F9482E-44F0-E40C-D30D-60C0... | Token - 4a6809836f02... | NA | NA | -- | -- | -- | CLI | ... |
| vEdge Cloud | e474c5fd-8ce7-d376-7cac-b950b2c91... | e474c5fd-8ce7-d376-7cac-b950b2c91... | 7175AE0F | NA | NA | DC-vEdge1 | 10.255.24... | Template Log | CLI | ... |
| vEdge Cloud | 0dd4af0e-f2f1-fe75-866c-469966cd1c3 | 0dd4af0e-f2f1-fe75-866c-469966cd1c3 | 7DA605F5 | NA | NA | DC-vEdge2 | 10.255.25... | Device Bring Up | CLI | ... |
| vEdge Cloud | b7fd7295-58df-7671-e914-6fe2edff1609 | b7fd7295-58df-7671-e914-6fe2edff1609 | Token - 945eb9871624... | NA | NA | -- | -- | -- | CLI | ... |
| vEdge Cloud | dd690ff0-dc62-7766-510f-08d966085378 | dd690ff0-dc62-7766-510f-08d966085378 | Token - 4c583475c7d4... | NA | NA | -- | -- | -- | CLI | ... |
| vEdge Cloud | 17026153-f09e-be4b-6dce-482fce43aa... | 17026153-f09e-be4b-6dce-482fce43aa... | Token - 3692590e4778... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-26217DA0-1B63-80DE-11C9-125F... | CSR-26217DA0-1B63-80DE-11C9-125F... | Token - 8dc7b557b60d... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-F960E020-B7C9-887F-46A8-F453... | CSR-F960E020-B7C9-887F-46A8-F453... | Token - 50cc04634a4... | NA | NA | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-25925FBC-07F3-0732-E127-EA95... | CSR-25925FBC-07F3-0732-E127-EA95... | Token - 6ced66053d46... | NA | NA | -- | -- | -- | CLI | ... |
| vEdge Cloud | 35bd96f9-1758-116c-4e4c-e34c70664... | 35bd96f9-1758-116c-4e4c-e34c70664... | Token - ed778f56f9ab0... | NA | NA | -- | -- | -- | CLI | ... |
| vEdge Cloud | 005c424c-2d57-41fe-250d-ee991e0a4... | 005c424c-2d57-41fe-250d-ee991e0a4... | Token - 56f4f154ce614d... | NA | NA | -- | -- | -- | CLI | ... |
| vEdge Cloud | 2129349-2c9f-7aa1-28f5-a87e4d0054cb | 2129349-2c9f-7aa1-28f5-a87e4d0054cb | Token - b0464def4a2a... | NA | NA | -- | -- | -- | Activate Windows | ... |
| | | | | | | | | | Go to Settings to activate Windows... | |

4. Choose **Cloud-Init** and uncheck **Include Default Root Certificate**. Click on **OK**



5. Make note of the **UUID** and the **OTP** values. These will be required to activate the vEdge. It's best to copy the string and place it in notepad, since we will need to use it in our SSH session to the vEdge20 device. Alternatively, leave this popup open and we can come back to it when required

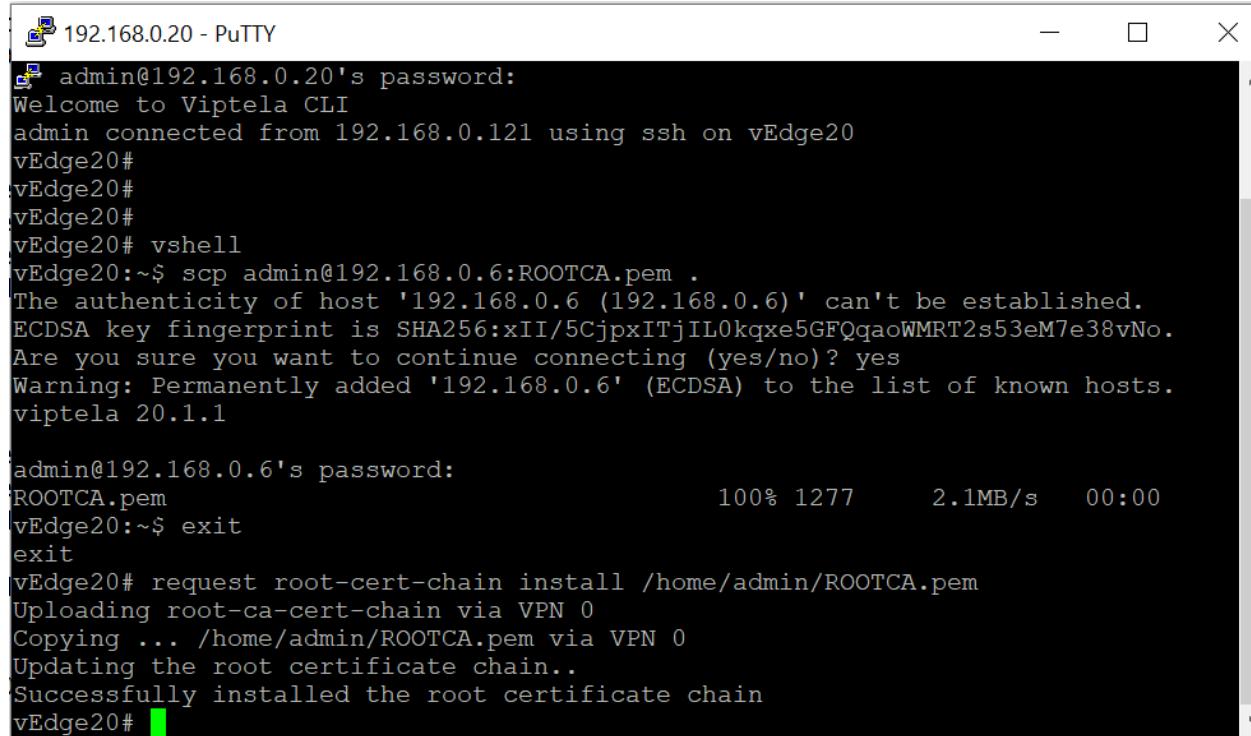
Generate Bootstrap Configuration X

Download

```
#cloud-config
vinitparam:
- uuid : b7fd7295-58df-7671-e914-6fe2edff1609
- vbond : 100.100.100.3
- otp : 945eb9871624db4cc321c6197484ce09
- org : swat-sdwanlab
- rcc : true
ca-certs:
remove-defaults: false
trusted:
- |
---BEGIN CERTIFICATE---
MIIF7DCCBNsgAwIBAgIQbsx6pacDIAm4rz06VLUkTANBgkqhkiG9w0BAQUFADC
...[REDACTED]
```

Close

6. Go back to the Putty session for vEdge20 and enter `request root-cert-chain install /home/admin/ROOTCA.pem` to install the root cert chain. It should install successfully



192.168.0.20 - PuTTY

```
admin@192.168.0.20's password:
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on vEdge20
vEdge20#
vEdge20#
vEdge20#
vEdge20# vshell
vEdge20:~$ scp admin@192.168.0.6:ROOTCA.pem .
The authenticity of host '192.168.0.6 (192.168.0.6)' can't be established.
ECDSA key fingerprint is SHA256:xII/5CjpxITjIL0kqxe5GFQqaoWMRT2s53eM7e38vNo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.6' (ECDSA) to the list of known hosts.
viptela 20.1.1

admin@192.168.0.6's password:
ROOTCA.pem                                         100% 1277      2.1MB/s   00:00
vEdge20:~$ exit
exit
vEdge20# request root-cert-chain install /home/admin/ROOTCA.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
vEdge20#
```

```
request root-cert-chain install /home/admin/ROOTCA.pem
```

7. Enter `tunnel-interface`, `encapsulation ipsec` and `allow-service all` under `interface ge0/0` to bring up the tunnel Interface. Make sure to `commit and-quit` in order to write the configuration change

```
config t
vpn 0
interface ge0/0
tunnel-interface
encapsulation ipsec
allow-service all
exit
!
commit and-quit
```

This ensures that our vEdge is now able to establish control connections with the vManage and vSmarts via the vBond. However, these connections will not be fully formed till we don't activate the vEdge itself

```
vEdge20# conf t  
Entering configuration mode terminal  
vEdge20(config)# vpn 0  
vEdge20(config-vpn-0)# interface ge0/0  
vEdge20(config-interface-ge0/0)# tunnel-interface  
vEdge20(config-tunnel-interface)# encapsulation ipsec  
vEdge20(config-tunnel-interface)# allow-service all  
vEdge20(config-tunnel-interface)# commit and-quit  
Commit complete.  
vEdge20#
```

8. Issue the `request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)` command. Replace the (*Enter your UUID*) and (*Enter your OTP*) fields with the UUID and OTP generated in Step 5 (image below is an example, UUID and OTP may not match).

```
vEdge20# request vedge-cloud activate chassis-number b7fd7295-58df-7671-e914-6fe2edff1609 token 945eb9871624db4cc321c6197484ce09  
vEdge20#  
vEdge20#  
vEdge20#  
vEdge20#  
vEdge20#
```

request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)

This completes the Onboarding section for vEdge20

Task List

- [Creating the vEdge20 VM](#)
 - [Overview](#)
 - [Deploying the vEdge20 VM on vCenter](#)
- [Onboarding vEdge20](#)
 - [Bootstrapping vEdge20 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)

Onboarding Verification

1. Wait for a couple of minutes and run `show control connections` in the vEdge20 CLI. We should see that the vEdge has been able to establish a DTLS tunnel with the vManage and the vSmarts. If you don't see any output, wait for a couple of minutes and run the command again

| PEER | | | | PEER | | | |
|---------|-------------------|------|------|---------------|---------------------|-------|------------|
| TYPE | PEER | PEER | SITE | DOMAIN | PEER | PUB | PROXY |
| PEER | PEER | PEER | ID | ID | PRIVATE IP | PORT | PUBLIC IP |
| vsmart | dtls 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12446 100.100.100.4 | 12446 | default No |
| vsmart | dtls 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12446 100.100.100.5 | 12446 | default No |
| vmanage | dtls 10.255.255.1 | 1000 | 0 | 100.100.100.2 | 12446 100.100.100.2 | 12446 | default No |

```
show control connections
```

Tip: You can also issue `show control connections-history` in the event of failures to find out why is the connection not working as expected. A few helpful commands are `show certificate installed`, `show certificate root-ca-cert`, `show control local-properties` and `show certificate validity`. Most of these commands give us details about the status of certificates on the device and are helpful in ascertaining the root cause of failure when control connections aren't getting established.

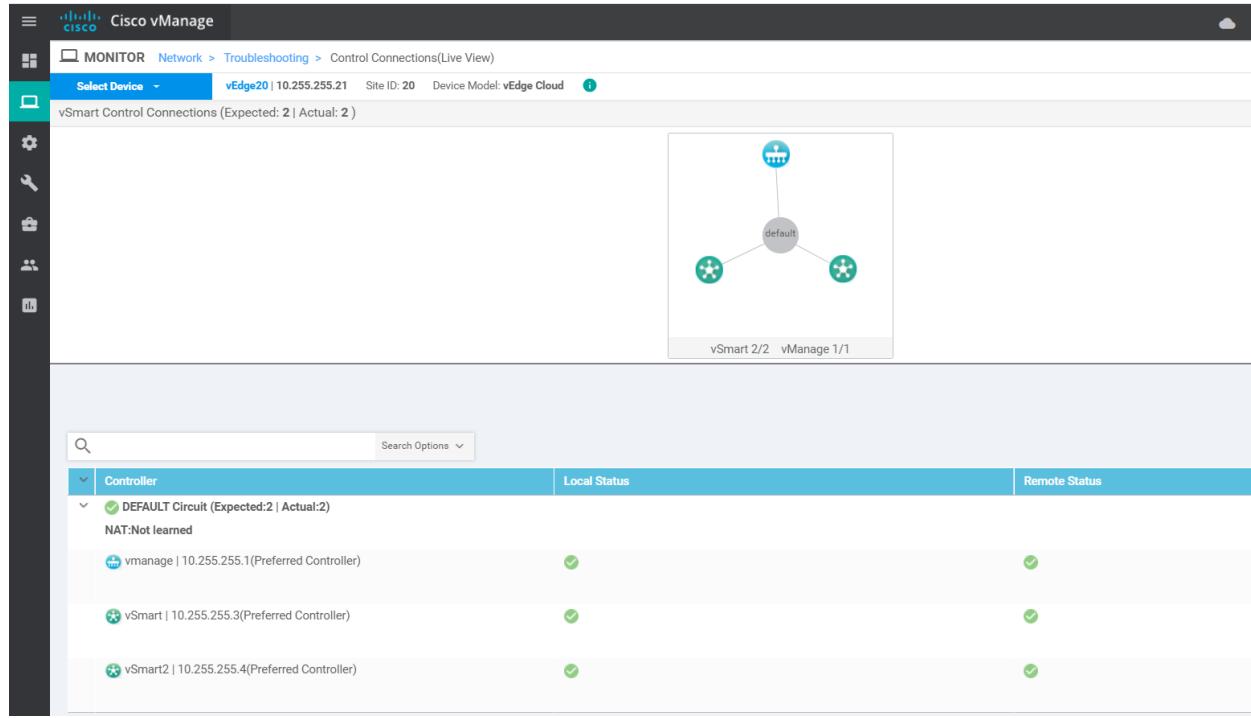
2. On the vManage GUI, navigate to **Monitor => Network Devices** (the computer icon on the left-hand side)

| Cisco vManage | | | |
|---------------|---|--|---|
| | CONFIGURATION DEVICES | | |
| | Monitors | | |
| | Upload WAN Edge List <input type="checkbox"/> Export Bootstrap Configuration <input checked="" type="checkbox"/> Sync Smart Account | | |
| | Geography | Network | Search Options ▾ |
| Alarms | Network | Chassis Number | Serial No./Token |
| | | CSR-44C7CE5A-4149-E696-C8A8-415C793FBF6C | Token - fc40de6570e725ba70c917d6511b8a6c |
| | | CSR-D6DB39FC-C383-BB55-7E9D-7CDD85595DD1 | Token - f28b5ab9789827383a9425d0aec4fe1a |
| | | CSR-834E40DC-E358-8DE1-0E81-76E5984138F4 | Token - b8a9cae09c975b49003634e8174b83b |
| | | CSR-D405F5BA-B975-8944-D1A3-2E082AEE2A1D | Token - e78aaefc1ebd2a11d900e88098a7949c |
| | | CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3 | Token - 90ffd29997ff8c9aab379f6d3b75d2d |
| | CSR1000v | CSR-5E992295-1362-0DB6-EEF8-25CC88F1CCCE | Token - 1da14330e1711d985d29d28603a5611d |
| | CSR1000v | CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2 | Token - 4a6809836f0216c736c305fc131950d9 |
| | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b2c9159 | 7175AE0F |
| | vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-469966cdca1c3 | Token - 908adb0239fdd2018f25ad423fc6a1b9 |
| | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2edff1609 | Token - 945eb9871624db4cc321c6197484ce09 |
| | vEdge Cloud | dde90ff0-dc62-77e6-510f-08d96608537d | Token - 4c583475c7d42f07e570dbcba42d3431f |
| | vEdge Cloud | 17026153-f09e-be4b-6dce-482fce43aab2 | Token - 3692590e47782d2ae043b8a4369c145 |
| | CSR1000v | CSR-26217DA0-1B63-8DDE-11C9-125F527D3270 | Token - 8dc7b557b60d4cec5c22e3c143132c0d |
| | CSR1000v | CSR-F960E020-B7C9-887F-46A8-F45374B23E7D | Token - 50cc04634ac461d3d68d53f26a520c35 |
| | CSR1000v | CSR-25925FBC-07F3-0732-E127-EA95D24F8EEB | Token - 6ced66053d4698a4402a50b1b2c082f3 |
| | vEdge Cloud | 35bd96f9-1758-116c-4e4c-e34c7066459c | Token - ed778f56f9ab08994a1c1d8aa046385c |
| | vEdge Cloud | 005c424c-2d57-41fe-250d-ee991e0a4e93 | Token - 56f4f54ce614d27ba24350ec9a50572e |
| | vEdge Cloud | 21292349-2c9f-7aafl-28f5-a87e4d0054cb | Token - b6046deef4a2ae480f9cc18194152fb0 |
| | vEdge20 | 2frl2ad0n0h47c | Token - ce9fb6c06da1fhe2ha06fd5001520f62 |

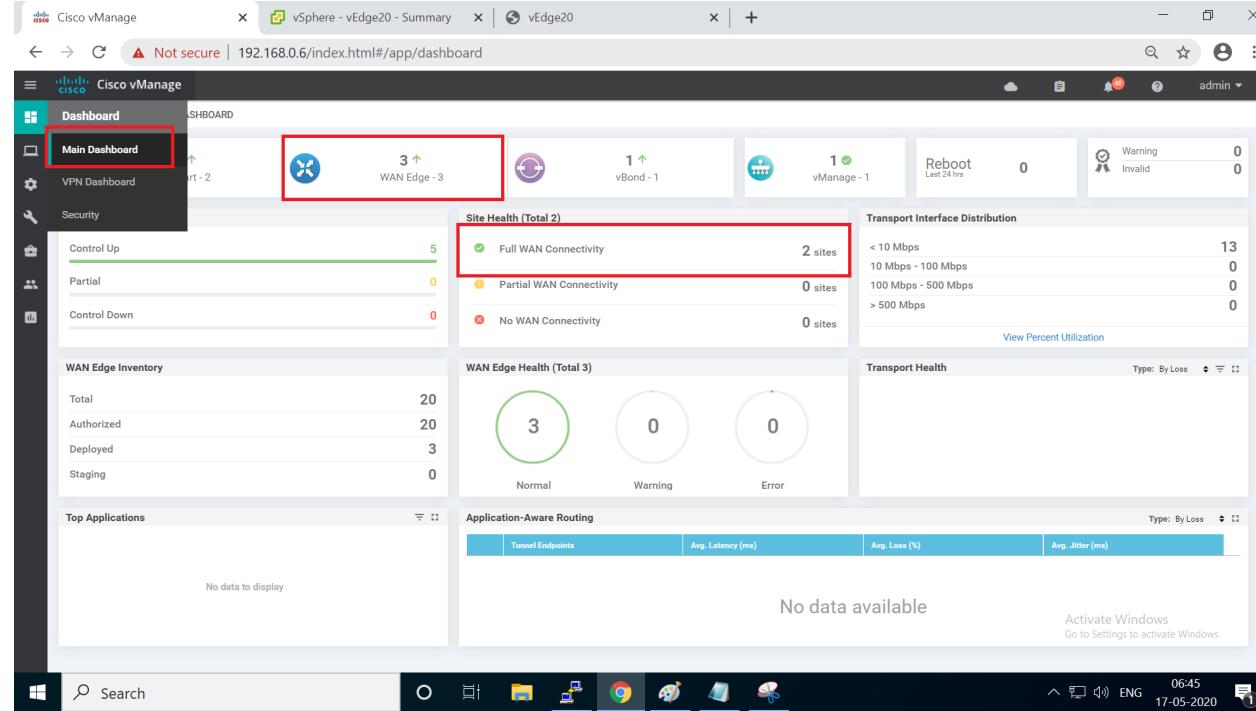
3. vEdge20 should show up in the list of devices

| Device Group | All | Search Options ▾ | Total Rows: 7 | | | | | | | | | |
|--------------|---------------|---------------------|------------------------------------|-----------|--------------|---------|-----|---------|-----------------------------|-------------|---------------|-----------|
| Hostname | System IP | Device Model | Chassis Number/ID | State | Reachability | Site ID | BFD | Control | Version | Up Since | Device Groups | Connected |
| vmanage | 10.255.255.1 | vManage | dfea63a5-66d2-4e50-a07b-ec4ad4... | reachable | 1000 | -- | 5 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | *10.25* | |
| vSmart | 10.255.255.3 | vSmart | 20607a12-c0b3-4f4b-a5f5-5a547e... | reachable | 1000 | -- | 5 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | *10.25* | |
| vSmart2 | 10.255.255.4 | vSmart | 7f332491-cb6f-4843-8bf5-060f90... | reachable | 1000 | -- | 5 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | *10.25* | |
| vBond | 10.255.255.2 | vEdge Cloud (vBo... | fc31c154-99c5-4267-971d-6c9ae7... | reachable | 1000 | -- | -- | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | *10.25* | |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950... | reachable | 1 | 1 | 3 | 20.1.1 | 14 May 2020 7:36:00 AM PDT | "No groups" | *10.25* | |
| DC-vEdge2 | 10.255.255.12 | vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-469966c... | reachable | 1 | 1 | 3 | 20.1.1 | 16 May 2020 12:24:00 PM PDT | "No groups" | *10.25* | |
| vEdge20 | 10.255.255.21 | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2ed... | reachable | 20 | 2 | 3 | 20.1.1 | 17 May 2020 5:27:00 AM PDT | "No groups" | *10.25* | |

4. Click on vEdge20 and navigate to **Troubleshooting => Control Connections(Live view)**. You should see the vEdge successfully connected to 2 vSmarts and 1 vManage



5. On the main dashboard, notice that we now have three WAN Edges onboarded on vManage. The two sites also have WAN connectivity since BFD sessions have been established.



6. This can be verified from the **Monitor => Network** page as well, where we will see active BFD sessions on all devices. Via CLI, this can be checked using `show bfd sessions`

| MONITOR NETWORK | | | | | | | | | | | | | |
|-------------------|---------------|----------------------------------|------------------------------------|---------------|--------------|---------|-----|---------|-----------------------------|-------------|-----------------|-----------|--|
| WAN - Edge | | Colocation Clusters | | | | | | | | | | | |
| VPN GROUP | | VPN SEGMENT | | | | | | | | | | | |
| Select VPN Group | | 0 items to select - confirm text | | | | | | | | | | | |
| Device Group | All | Search | Search Options | Total Rows: 7 | | | | | | | | | |
| Hostname | System IP | Device Model | Chassis Number/ID | State | Reachability | Site ID | BFD | Control | Version | Up Since | Device Groups | Connected | |
| vManage | 10.255.255.1 | vManage | dfe3a35-66d2-4e50-a07b-e4cad4... | reachable | 1000 | -- | 5 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | "10.255.255.1" | | |
| vSmart | 10.255.255.3 | vSmart | 20607a12-c0c8-4f46-a65f-5a547c... | reachable | 1000 | -- | 5 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | "10.255.255.3" | | |
| vSmart2 | 10.255.255.4 | vSmart | 7f332491-cb6f-4843-8b75-60690... | reachable | 1000 | -- | 5 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | "10.255.255.4" | | |
| vBond | 10.255.255.2 | vEdge Cloud (vBo... | fc31c154-9c95-4267-971d-6c99ae7... | reachable | 1000 | -- | -- | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | "10.255.255.2" | | |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7c8c-ba950b... | reachable | 1 | 1 | 3 | 20.1.1 | 14 May 2020 7:36:00 AM PDT | "No groups" | "10.255.255.11" | | |
| DC-vEdge2 | 10.255.255.12 | vEdge Cloud | 0dd4f0e-f211-fe75-866c-469966c... | reachable | 1 | 1 | 3 | 20.1.1 | 16 May 2020 12:24:00 PM PDT | "No groups" | "10.255.255.12" | | |
| vEdge20 | 10.255.255.21 | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2ed... | reachable | 20 | 2 | 3 | 20.1.1 | 17 May 2020 5:27:00 AM PDT | "No groups" | "10.255.255.21" | | |

```
vEdge20# show bfd sessions
      SOURCE TLOC      REMOTE TLOC          DST PUBLIC          DST PUBLIC        DETECT      TX
      SYSTEM IP      SITE ID STATE    COLOR      COLOR      SOURCE IP      IP          PORT      ENCAP      MULTIPLIER INTERVAL(msec) UPTIME
      TRANSITIONS

10.255.255.11   1     up    default    default  100.100.100.20  100.100.100.10  12366  ipsec    7       1000  0:00:45
10.255.255.12   1     up    default    default  100.100.100.20  100.100.100.11  12366  ipsec    7       1000  0:00:45
0:04

vEdge20#
```

Tip: The vEdges at DC show only one BFD session whereas vEdge20 shows two. This is because the DC-vEdges detect that they are part of the same site (via the `site-id` command), hence won't have BFD entries for each other

This completes the verification activity.

Task List

- [Creating the vEdge20 VM](#)
 - [Overview](#)
 - [Deploying the vEdge20 VM on vCenter](#)
- [Onboarding vEdge20](#)
 - [Bootstrapping vEdge20 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)
- [Onboarding Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Site last generated: Sep 1, 2020



-->

Deploying a single uplink (MPLS) vEdge

Summary: Deploying vEdge21 in Site 20. This vEdge has a single uplink (MPLS)

Table of Contents

- [Creating the vEdge21 VM](#)
 - Overview
 - Deploying the vEdge21 VM on vCenter
- [Onboarding vEdge21](#)
 - Bootstrapping vEdge21 (Initial Configuration)
 - Installing certificates and activating the vEdge

⚠ Warning: This section might already be done, depending on your selected Lab Scenario. Most lab work will start [from here](#). The configuration given below can be used to review what was done to bring the Site up. If this VM is already deployed (check via vCenter), you **Do Not** need to perform these lab activities.

Task List

- Creating the vEdge21 VM
 - Overview
 - Deploying the vEdge21 VM on vCenter
- Onboarding vEdge21
 - Bootstrapping vEdge21 (Initial Configuration)
 - Installing certificates and activating the vEdge

Creating the vEdge21 VM

Overview

⚠ Warning: Since we have gone through deploying vEdges multiple times by now, this section will just have the steps listed out. Images for every step has not been populated due to similarity with the previous sections.

ℹ Note: The important steps which will guide you through this activity will be earmarked, indicating a delta from the previous sections.

This is what an earmarked step will look like

We will be deploying another vEdge at Site 20 via vCenter. Make note of the following information for this section. The IP Addressing will not be used for some of the Network Adapters until later.

| SITE ID | SYSTEM ID | VM | Network Adapter | Network | Interface | IP | Gateway |
|---------|---------------|--------------|-------------------|---------------|-----------|------------------|-------------|
| 20 | 10.255.255.22 | vEdge21-podX | Network Adapter 1 | Management | eth0 | 192.168.0.21/24 | 192.168.0.1 |
| | | | Network Adapter 2 | TLOCEXT_vEdge | ge0/1 | 192.168.25.21/24 | |
| | | | Network Adapter 3 | Site20-VPN10 | ge0/2 | 10.20.10.3/24 | |
| | | | Network Adapter 4 | Site20-VPN20 | ge0/3 | 10.20.20.3/24 | |
| | | | | | | | |

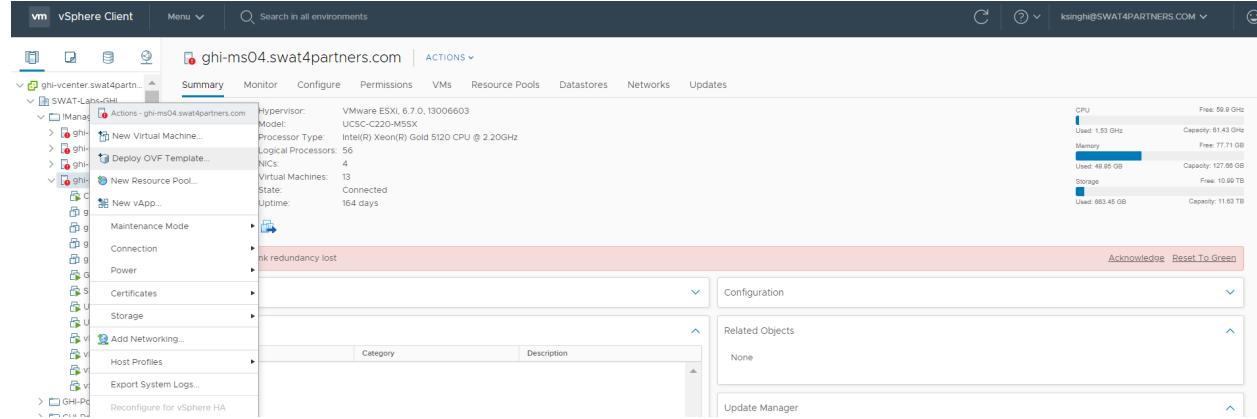
| | | | | | |
|--|-----------------|----------------|-------|------------------|-----------|
| | Network Adapter | MPLS20 | ge0/0 | 192.0.2.10/30 | 192.0.2.9 |
| | | 5 | | | |
| | Network Adapter | TLOCEXT2_vEdge | ge0/4 | 192.168.26.21/24 | |
| | | 6 | | | |

Task List

- Creating the vEdge21 VM
 - [Overview](#)
 - [Deploying the vEdge21 VM on vCenter](#)
- Onboarding vEdge21
 - [Bootstrapping vEdge21 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)

Deploying the vEdge21 VM on vCenter

1. Click on the bookmark for vCenter or navigate to the following URL: <https://10.2.1.50/ui>. Log in with the credentials provided for your POD.
2. Right click on the host and choose to **Deploy OVF Template**



3. Choose the **Local file** option and click on **Choose files**. Navigate to the SD-WAN images folder and select the file beginning with *viptela-edge-*. Click on Next.
4. Change the Virtual Machine name to **vEdge21-podX** and click on Next (where X is your POD number)

Note: We will only use the podX suffix over here to distinguish between different VMs in our Data Center. The rest of the guide will refer to this VM as **vEdge21**

5. Select the host assigned to you (image shown as an example only) and click on Next

Note: If the screen gets stuck over here at **Validating** then close Chrome and open the vCenter in Internet Explorer, going through the same steps. Deployment should go through. This is a known issue with Google Chrome.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

The screenshot shows a tree view of compute resources. The root node is 'SWAT-Labs-GHI', which contains a folder 'Management-Shared Services' and several host entries. The host entries are: ghi-ms01.swat4partners.com, ghi-ms02.swat4partners.com, ghi-ms03.swat4partners.com, and ghi-ms04.swat4partners.com. The host ghi-ms04.swat4partners.com is currently selected, indicated by a light blue background. Below the main tree, there is a list of 'Pods' from Pod01 to Pod10.

- ✓ SWAT-Labs-GHI
 - ✓ Management-Shared Services
 - ghi-ms01.swat4partners.com
 - ghi-ms02.swat4partners.com
 - ghi-ms03.swat4partners.com
 - ghi-ms04.swat4partners.com
 - GHI-Pod01
 - GHI-Pod02
 - GHI-Pod03
 - GHI-Pod04
 - GHI-Pod05
 - GHI-Pod06
 - GHI-Pod07
 - GHI-Pod08
 - GHI-Pod09
 - GHI-Pod10

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

6. Review the details shown and click on Next

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource

Review details
Verify the template details.

4 Review details

- 5 Select storage
- 6 Select networks
- 7 Ready to complete

| | |
|---------------------|--|
| Publisher | No certificate present |
| Download size | 231.2 MB |
| Size on disk | 234.1 MB (thin provisioned) |
| | 10.2 GB (thick provisioned) |
| Extra configuration | <pre>time.synchronize.tools.startup = FALSE virtualHW.productCompatibility = hosted time.synchronize.restore = FALSE time.synchronize.continue = FALSE time.synchronize.shrink = FALSE time.synchronize.resume.disk = FALSE time.synchronize.tools.enable = FALSE time.synchronize.resume.host = FALSE</pre> |

CANCEL

BACK

NEXT

7. Choose the Datastore and click on Next

8. Populate the VM Networks as per the image given below

⚠ Important: Please make sure that these look exactly as shown below

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**

7 Ready to complete

Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|----------------|---------------------|
| VM Network 3 | Site20-VPN20 |
| VM Network | Management |
| VM Network 2 | Site20-VPN10 |
| VM Network 1 | TLOCEXT_vEDGE |

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

9. Click on **Finish** to deploy your vEdge21-podX VM

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks

7 Ready to complete

| | |
|-------------------|---|
| Provisioning type | Deploy from template |
| Name | vEdge21 |
| Template name | viptela-edge-genericx86-64-20200414061026 |
| Download size | 231.2 MB |
| Size on disk | 10.2 GB |
| Folder | SWAT-Labs-GHI |
| Resource | ghi-ms04.swat4partners.com |
| Storage mapping | 1 |
| All disks | Datastore: ghi-ms04-ds; Format: Thick provision lazy zeroed |
| Network mapping | 4 |
| VM Network 3 | Site20-VPN20 |
| VM Network | Management |
| VM Network 2 | Site20-VPN10 |
| VM Network 1 | TLOCEXT_vEDGE |

CANCEL

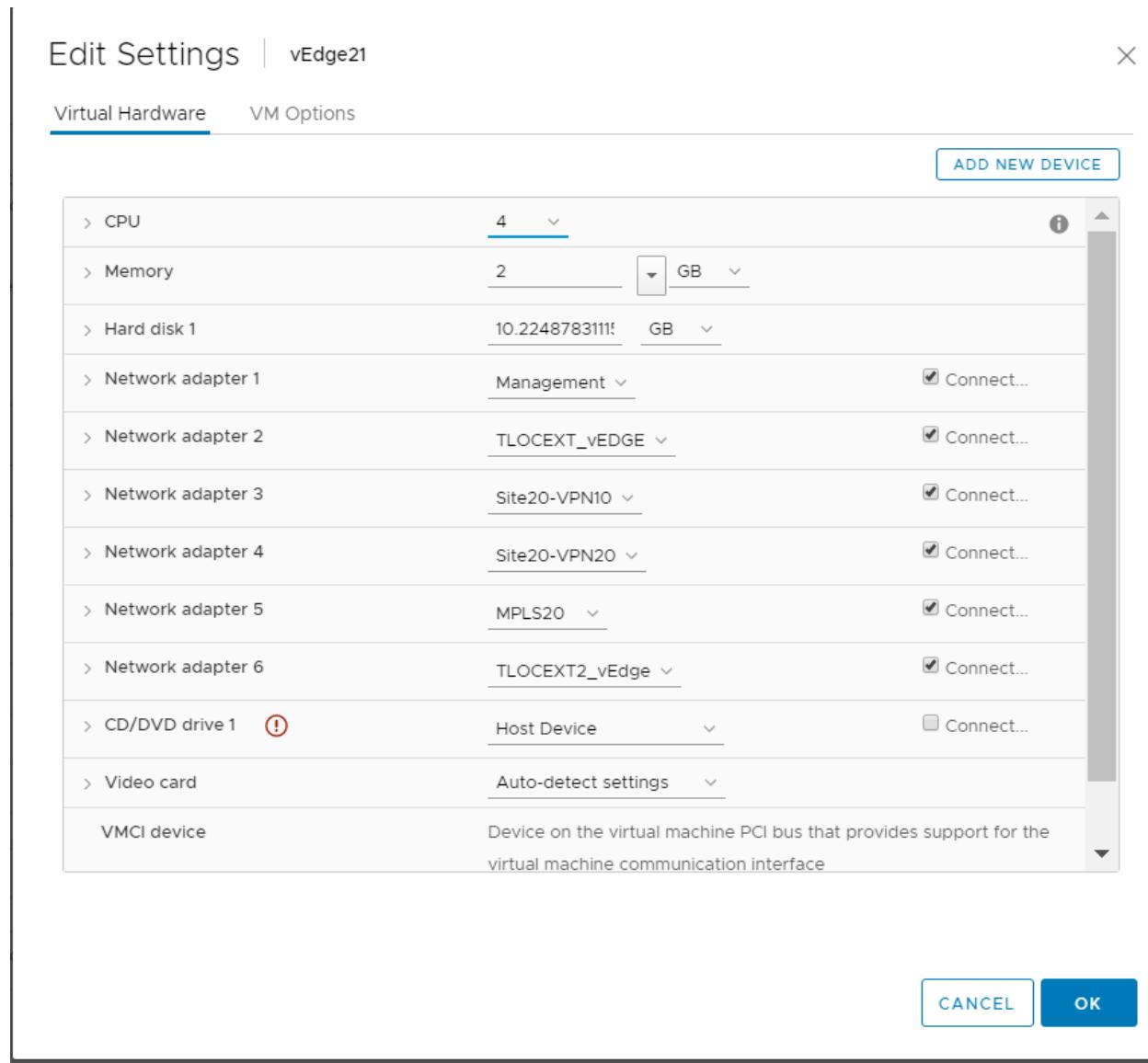
BACK

FINISH

10. Once the VM is deployed, right click **vEdge21-podX** and click Edit settings.
11. Choose to **Add a new device** (top right corner) and select Network Adapter to add one (since our deployed VM has only 4 Network Adapters but we will need 6 for our lab). Add another network device this way, for a total of 6 network adapters.
12. Click on the drop down next to the first **New Network** and click on *Browse*
13. Choose the **MPLS20** Network and click on **OK**.

14. Click on the drop down for the second **New Network** entry, added as a result of adding two network adapters and click on *Browse*. Select the **TLOCEXT2_vEdge** Network

15. Make sure the Network Adapters match with the image below and click on OK



16. Click on vEdge21-podX and choose to power it on

Task List

- [Creating the vEdge21 VM](#)
 - [Overview](#)
 - [Deploying the vEdge21 VM on vCenter](#)
- [Onboarding vEdge21](#)
 - [Bootstrapping vEdge21 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)

Onboarding vEdge21

Bootstrapping vEdge21 (Initial Configuration)

Use the following information in this section (some of the information will be used later)

| SITE ID | SYSTEM ID | VM | Network Adapter | Network | Interface | IP | Gateway |
|---------|---------------|---------|-------------------|---------------|-----------|------------------|-------------|
| 20 | 10.255.255.22 | vEdge21 | Network Adapter 1 | Management | eth0 | 192.168.0.21/24 | 192.168.0.1 |
| | | | Network Adapter 2 | TLOCEXT_vEdge | ge0/1 | 192.168.25.21/24 | |
| | | | Network Adapter 3 | Site20-VPN10 | ge0/2 | 10.20.10.3/24 | |
| | | | Network Adapter 4 | Site20-VPN20 | ge0/3 | 10.20.20.3/24 | |
| | | | Network Adapter 5 | MPLS20 | ge0/0 | 192.0.2.10/30 | 192.0.2.9 |

Network TLOC EXT2_vEdge ge0/4 192.168.26.21/24
Adapter
6

1. Console in to the vEdge21 VM from vCenter (you should already be logged in from our last activity)
2. Wait for the VM to prompt you for the username and password and enter the credentials given below. If you get a message stating that they are incorrect, wait for 30 seconds and try again (since the processes need to initialize before you can log in).

| Username | Password |
|----------|----------|
| admin | admin |

Note: From version 19.2, the password will need to be reset on initial login. For this lab, we will reset the password to admin.

3. Enter the configuration enumerated below. Unfortunately, this will need to be typed out since the console isn't copy-paste friendly

```
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vEdge21
vedge(config-system)# system-ip 10.255.255.22
vedge(config-system)# organization-name "swat-sdwanlab"
vedge(config-system)# site-id 20
vedge(config-system)# vbond 100.100.100.3
vedge(config-system)# exit
vedge(config)# vpn 0
vedge(config-vpn-0)# ip route 0.0.0.0/0 192.0.2.9
vedge(config-vpn-0)# interface ge0/0
vedge(config-interface-ge0/0)# ip address 192.0.2.10/30
vedge(config-interface-ge0/0)# no tunnel-interface
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# exit
vedge(config)# vpn 512
vedge(config-vpn-512)# ip route 0.0.0.0/0 192.168.0.1
vedge(config-vpn-512)# interface eth0
vedge(config-interface-eth0)# ip address 192.168.0.21/24
vedge(config-interface-eth0)# no shutdown
vedge(config-interface-eth0)# commit and-quit_
```

```
conf t
system
host-name vEdge21
system-ip 10.255.255.22
organization-name "swat-sdwanlab"
site-id 20
vbond 100.100.100.3
exit
!
vpn 0
ip route 0.0.0.0/0 192.0.2.9
interface ge0/0
ip address 192.0.2.10/30
no tunnel-interface
no shutdown
exit
!
exit
```

```
!
vpn 512
 ip route 0.0.0.0/0 192.168.0.1
interface eth0
 ip address 192.168.0.21/24
 no shutdown
!
commit and-quit
```

4. Open **Putty** and double-click the saved session for vEdge21 (or **SSH** to **192.168.0.21**)

5. Choose Yes to accept the certificate, if prompted

PuTTY Security Alert



WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.

The new ecdsa-sha2-nistp256 key fingerprint is:

ecdsa-sha2-nistp256 256

7c:de:34:0d:98:36:6a:64:a1:69:07:d8:68:44:d4:8f

If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.

If you want to carry on connecting but without updating the cache, hit No.

If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

Yes

No

Cancel

Help

6. Log in using the same credentials as Step 2.

Task List

- [Creating the vEdge21 VM](#)
 - [Overview](#)
 - [Deploying the vEdge21 VM on vCenter](#)

- Onboarding vEdge21
 - Bootstrapping vEdge21 (Initial Configuration)
 - Installing certificates and activating the vEdge

Installing certificates and activating the vEdge

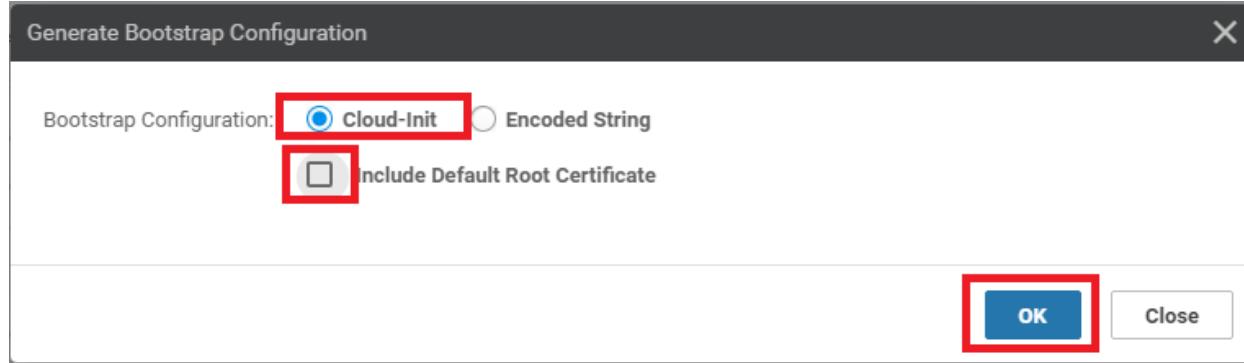
1. Type `vshell` and enter `scp admin@192.168.0.6:ROOTCA.pem .` to copy the ROOTCA.pem certificate to the vEdge. Commands can be copy-pasted now since we have SSH'd in to the vEdge (there is a dot at the end of the scp command). Enter `yes` when prompted and enter the password of vManage (i.e. admin). Exit when done with this step.

```
vshell  
scp admin@192.168.0.6:ROOTCA.pem .
```

2. Go to the vManage GUI (<https://192.168.0.6>) and log in, if logged out. Navigate to **Configuration => Devices** (from the left-hand side, click on the cog wheel to access the configuration options)

The screenshot shows the Cisco vManage Main Dashboard. On the left, a sidebar lists various management categories: Configuration (2 items), Devices (selected), TLS/SSL Proxy, Certificates, Network Design, Templates, Policies, Security, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, and Cloud onRamp for Colocation. The 'Devices' section is currently active, indicated by a teal bar at the top. The main dashboard area contains three primary sections: 'Site Health (Total 0)', 'WAN Edge Health (Total 0)', and 'Application-Aware Routing'. The 'Site Health' section displays three status counts: Full WAN Connectivity (0 sites), Partial WAN Connectivity (0 sites), and No WAN Connectivity (0 sites). The 'WAN Edge Health' section shows three circular indicators, each with a value of 0 and labeled 'Normal', 'Warning', and 'Error'. The 'Application-Aware Routing' section has a header row with columns for Tunnel Endpoints and Avg. Latency (ms), followed by a message 'No data'.

3. Choose any vEdge Cloud device (it doesn't matter which one you pick, as long as it is a vEdge Cloud) and click on the three dots at the extreme right-hand side. Choose to Generate Bootstrap Configuration
4. Choose **Cloud-Init** and **uncheck** *Include Default Root Certificate*. Click on OK



5. Make note of the **UUID** and the **OTP** values. These will be required to activate the vEdge. It's best to copy the string and place it in notepad, since we will need to use it in our SSH session to the vEdge21 device. Alternatively, leave this popup open and we can come back to it when required

| State | Device Model | Chassis Number | Username | System IP | Site ID | Mode |
|-------|--------------|---------------------------------------|--------------------------|-----------|---------|---------|
| Idle | CSR1000v | CSR-44C7CE5A-4149-E696-C8A8-415C... | | -- | -- | CLI *** |
| Idle | CSR1000v | CSR-D6DB39FC-C383-BB55-7E9D-7CD... | | -- | -- | CLI *** |
| Idle | CSR1000v | CSR-834E40DC-E358-80E1-0E81-76E59... | | -- | -- | CLI *** |
| Idle | CSR1000v | CSR-D405F5BA-B975-8944-D1A3-2E08... | | -- | -- | CLI *** |
| Idle | CSR1000v | CSR-D1837F36-6A1A-1850-7C1C-E1C6... | | -- | -- | CLI *** |
| Idle | CSR1000v | CSR-5E992295-1362-0DB6-EEF9-25CC... | | -- | -- | CLI *** |
| Idle | CSR1000v | CSR-04F9482E-44F0-E4DC-D30D-60C0... | | -- | -- | CLI *** |
| Idle | vEdge Cloud | e474c5fd-8ce7-d376-7cac-be950b2c91... | | -- | -- | CLI *** |
| Idle | vEdge Cloud | 0dd4d10e-f21f-e75-866c-469966cd1a3 | | -- | -- | CLI *** |
| Idle | vEdge Cloud | b7fd7295-58df-7671-e914-0fe2edff1609 | | -- | -- | CLI *** |
| Idle | vEdge Cloud | dd690fff-dc62-77e6-510f-08d96608537d | | -- | -- | CLI *** |
| Idle | vEdge Cloud | 17026153-f09e-be4b-6dc6-482fc43a... | | -- | -- | CLI *** |
| Idle | CSR1000v | CSR-26217DA0-1B63-8DDE-11C9-125F... | | -- | -- | CLI *** |
| Idle | CSR1000v | CSR-F960E020-B7C9-887F-46A8-F4537... | Token - 50cc04634ac4... | NA | -- | CLI *** |
| Idle | CSR1000v | CSR-25925FBC-07F3-0732-E127-EA95... | Token - 6cedf6053d46... | NA | -- | CLI *** |
| Idle | vEdge Cloud | 35bd96f9-1758-1165-4e4c-e346706645... | Token - ed778f56f9ab0... | NA | -- | CLI *** |

6. Go back to the Putty session for vEdge21 and enter `request root-cert-chain install /home/admin/RDTCAs.pem` to install the root cert chain. It should install successfully

```
request root-cert-chain install /home/admin/RDTCAs.pem
```

7. Enter `tunnel-interface`, `encapsulation ipsec` and `allow-service all` under `interface ge0/0` to bring up the tunnel Interface. Make sure to `commit and-quit` in order to write the configuration change

```
config t
vpn 0
interface ge0/0
tunnel-interface
encapsulation ipsec
allow-service all
exit
!
commit and-quit
```

This ensures that our vEdge is now able to establish control connections with the vManage and vSmarts via the vBond. However, these connections will not be fully formed till we don't activate the vEdge itself

8. Issue the `request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)` command. Replace the (*Enter your UUID*) and (*Enter your OTP*) fields with the UUID and OTP generated in Step 5.

```
request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)
```

This completes the Onboarding section for vEdge21

Task List

- [Creating the vEdge21 VM](#)
 - [Overview](#)
 - [Deploying the vEdge21 VM on vCenter](#)
- [Onboarding vEdge21](#)
 - [Bootstrapping vEdge21 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Site last generated: Sep 1, 2020



Deploying a dual uplink vEdge

[Take a tour of this page](#)

Summary: Deploying vEdge30 in Site 30. This vEdge has dual uplinks (INET and MPLS)

Table of Contents

- [Creating the vEdge30 VM on vCenter](#)
 - [Overview](#)
 - [Deploying the vEdge30 VM on vCenter](#)
- [Onboarding vEdge30](#)
 - [Bootstrapping vEdge30 \(Initial Configuration\)](#)
 - [Installing certificates and activating the vEdge](#)

Task List

- Creating the vEdge30 VM
- Overview
- Deploying the vEdge30 VM on vCenter
- Onboarding vEdge30
- Bootstrapping vEdge30 (Initial Configuration)
- Installing certificates and activating the vEdge

Creating the vEdge30 VM on vCenter

Overview

⚠ Warning: Since we have gone through deploying vEdges multiple times by now, this section will just have the steps listed out. Images for every step has not been populated due to similarity with the previous sections.

ℹ Note: The important steps which will guide you through this activity will be earmarked, indicating a delta from the previous sections.

This is what an earmarked step will look like

We will be deploying a vEdge at Site 30 via vCenter. Make note of the following information for this section. The IP Addressing will not be used for some of the Network Adapters until later.

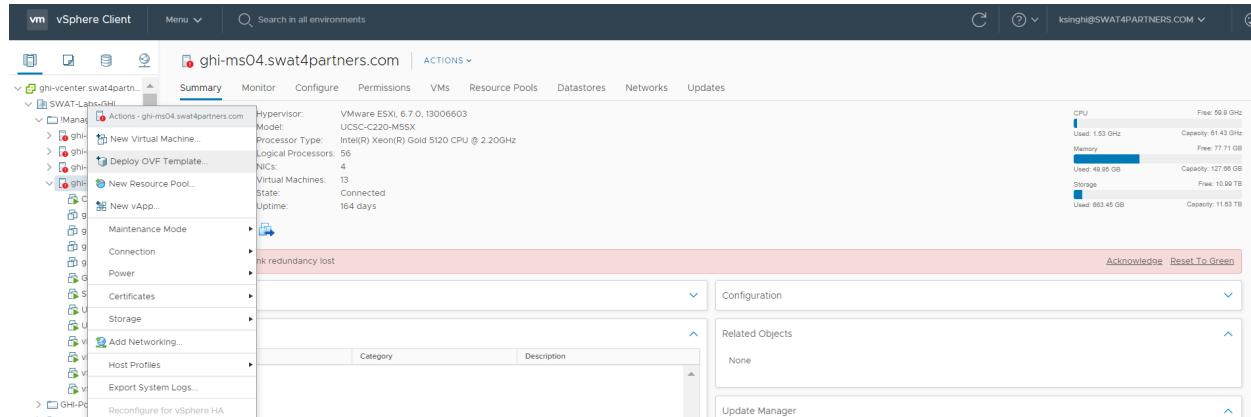
| SITE ID | SYSTEM ID | VM | Network Adapter | Network | Interface | IP | Gateway |
|---------|---------------|--------------|-------------------|--------------|-----------|-------------------|---------------|
| 30 | 10.255.255.31 | vEdge30-podX | Network Adapter 1 | Management | eth0 | 192.168.0.30/24 | 192.168.0.1 |
| | | | Network Adapter 2 | MPLS30 | ge0/1 | 192.0.2.14/30 | 192.0.2.13 |
| | | | Network Adapter 3 | Site30-VPN10 | ge0/2 | 10.30.10.2/24 | |
| | | | Network Adapter 4 | Site30-VPN20 | ge0/3 | 10.30.20.2/24 | |
| | | | Network Adapter 5 | Internet | ge0/0 | 100.100.100.30/24 | 100.100.100.1 |

Task List

- Creating the vEdge30 VM
- Overview
- Deploying the vEdge30 VM on vCenter
- Onboarding vEdge30
- Bootstrapping vEdge30 (Initial Configuration)
- Installing certificates and activating the vEdge

Deploying the vEdge30 VM on vCenter

1. Click on the bookmark for vCenter or navigate to the following URL: <https://10.2.1.50/ui>. Log in with the credentials provided for your POD.
2. Right click on the host and choose to **Deploy OVF Template**



3. Choose the **Local file** option and click on **Choose files**. Navigate to the SD-WAN images folder and select the file beginning with *viptela-edge-*. Click on Next.
4. Change the Virtual Machine name to **vEdge30-podX** and click on Next (where X is your POD number)

Note: We will only use the podX suffix over here to distinguish between different VMs in our Data Center. The rest of the guide will refer to this VM as **vEdge30**

5. Select the host assigned to you (image shown as an example only) and click on Next

Note: If the screen gets stuck over here at **Validating** then close Chrome and open the vCenter in Internet Explorer, going through the same steps. Deployment should go through. This is a known issue with Google Chrome.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource**
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a compute resource
Select the destination compute resource for this operation

- ✓ SWAT-Labs-GHI
 - ✓ Management-Shared Services
 - > ghi-ms01.swat4partners.com
 - > ghi-ms02.swat4partners.com
 - > ghi-ms03.swat4partners.com
 - > **ghi-ms04.swat4partners.com**
 - > GHI-Pod01
 - > GHI-Pod02
 - > GHI-Pod03
 - > GHI-Pod04
 - > GHI-Pod05
 - > GHI-Pod06
 - > GHI-Pod07
 - > GHI-Pod08
 - > GHI-Pod09
 - > GHI-Pod10

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

6. Review the details shown and click on Next

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource

Review details

Verify the template details.

4 Review details

- 5 Select storage
- 6 Select networks
- 7 Ready to complete

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

| | |
|---------------------|--|
| Publisher | No certificate present |
| Download size | 231.2 MB |
| Size on disk | 234.1 MB (thin provisioned) |
| | 10.2 GB (thick provisioned) |
| Extra configuration | <code>time.synchronize.tools.startup = FALSE virtualHW.productCompatibility = hosted time.synchronize.restore = FALSE time.synchronize.continue = FALSE time.synchronize.shrink = FALSE time.synchronize.resume.disk = FALSE time.synchronize.tools.enable = FALSE time.synchronize.resume.host = FALSE</code> |

CANCEL

BACK

NEXT

7. Choose the Datastore and click on Next

8. Populate the VM Networks as per the image given below

⚠ Important: Please make sure that these look exactly as shown below

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**

7 Ready to complete

Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|----------------|---------------------|
| VM Network 3 | Site30-VPN20 |
| VM Network | Management |
| VM Network 2 | Site30-VPN10 |
| VM Network 1 | MPLS30 |

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

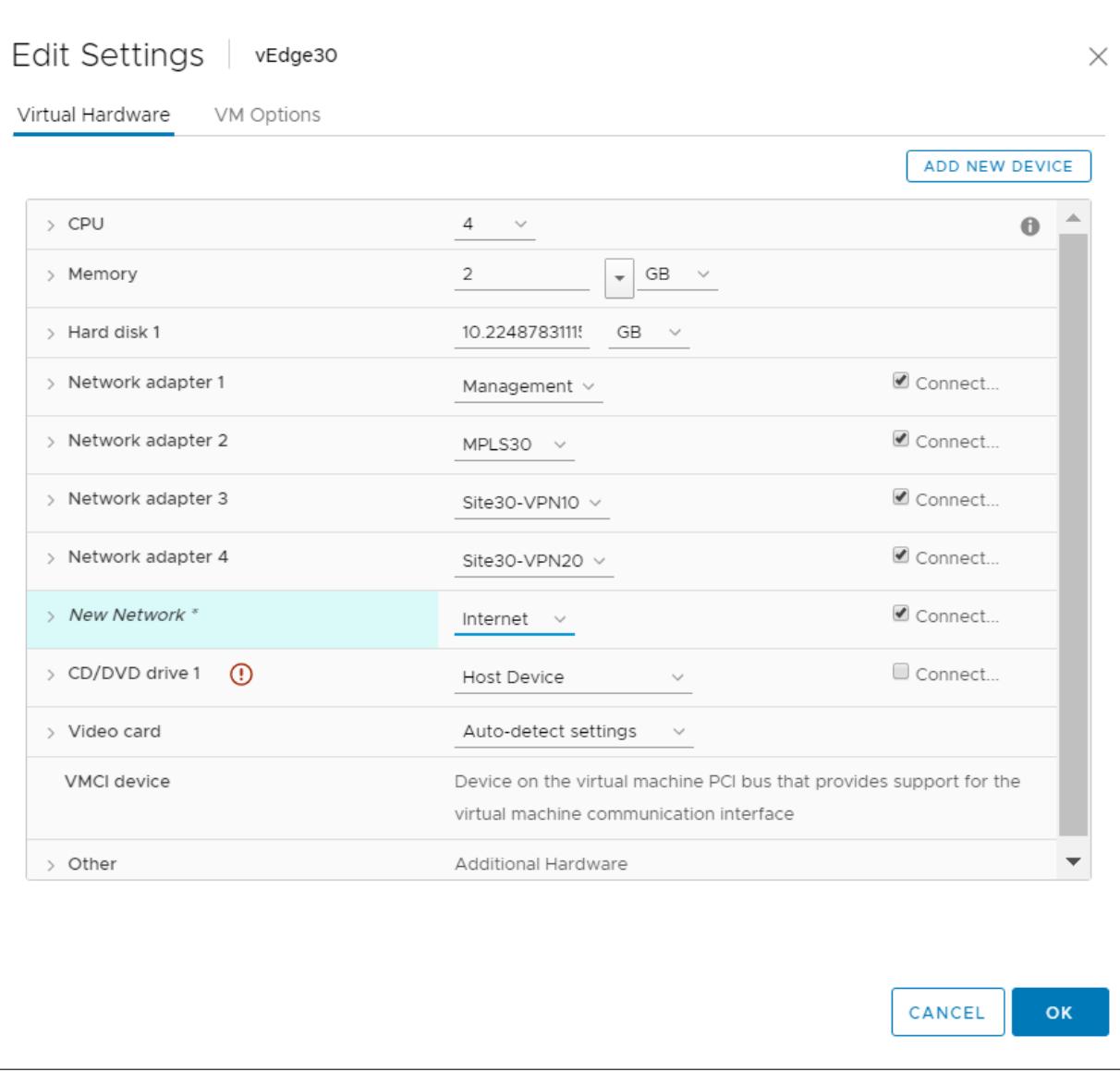
CANCEL

BACK

NEXT

9. Click on **Finish** to deploy your vEdge30-podX VM. **Please do not power on the VM at this point**
10. Once the VM is deployed, right click on **vEdge30-podX** and click Edit settings.
11. Choose to **Add a new device** (top right corner) and select Network Adapter to add one (since our deployed VM has only 4 Network Adapters but we will need 5 for our lab).
12. Click on the drop down next to the **New Network** and click on *Browse*
13. Choose the **Internet** Network and click on **OK**.

14. Make sure the Network Adapters match with the image below and click on *OK*



15. Click on vEdge30-podX and choose to power it on

Task List

- [Creating the vEdge30 VM](#)
- [Overview](#)
- [Deploying the vEdge30 VM on vCenter](#)
- [Onboarding vEdge30](#)
- [Bootstrapping vEdge30 \(Initial Configuration\)](#)
- [Installing certificates and activating the vEdge](#)

Onboarding vEdge30

Bootstrapping vEdge30 (Initial Configuration)

Use the following information in this section (some of the information will be used later)

| SITE ID | SYSTEM ID | VM | Network Adapter | Network | Interface | IP | Gateway |
|---------|---------------|---------|-------------------|--------------|-----------|-------------------|---------------|
| 30 | 10.255.255.31 | vEdge30 | Network Adapter 1 | Management | eth0 | 192.168.0.30/24 | 192.168.0.1 |
| | | | Network Adapter 2 | MPLS30 | ge0/1 | 192.0.2.14/30 | 192.0.2.13 |
| | | | Network Adapter 3 | Site30-VPN10 | ge0/2 | 10.30.10.2/24 | |
| | | | Network Adapter 4 | Site30-VPN20 | ge0/3 | 10.30.20.2/24 | |
| | | | Network Adapter 5 | Internet | ge0/0 | 100.100.100.30/24 | 100.100.100.1 |

1. Console in to the vEdge30 VM from vCenter (you should already be logged in from our last activity)
2. Wait for the VM to prompt you for the username and password and enter the credentials given below. If you get a message stating that they are incorrect, wait for 30 seconds and try again (since the processes need to initialize before you can log in).

| Username | Password |
|----------|----------|
| admin | admin |

Note: From version 19.2, the password will need to be reset on initial login. For this lab, we will reset the password to admin.

3. Enter the configuration enumerated below. Unfortunately, this will need to be typed out since the console isn't copy-paste friendly

vEdge30

```
vedge# conf t
Entering configuration mode terminal
vedge(config)# system
vedge(config-system)# host-name vEdge30
vedge(config-system)# system-ip 10.255.255.31
vedge(config-system)# organization-name "swat-sdwanlab"
vedge(config-system)# site-id 30
vedge(config-system)# vbond 100.100.100.3
vedge(config-system)# exit
vedge(config)# vpn 0
vedge(config-vpn-0)# ip route 0.0.0.0/0 100.100.100.1
vedge(config-vpn-0)# interface ge0/0
vedge(config-interface-ge0/0)# ip address 100.100.100.30/24
vedge(config-interface-ge0/0)# no tunnel-interface
vedge(config-interface-ge0/0)# no shutdown
vedge(config-interface-ge0/0)# exit
vedge(config-vpn-0)# exit
vedge(config)# vpn 512
vedge(config-vpn-512)# ip route 0.0.0.0/0 192.168.0.1
vedge(config-vpn-512)# interface eth0
vedge(config-interface-eth0)# ip address 192.168.0.30/24
vedge(config-interface-eth0)# no shutdown
vedge(config-interface-eth0)# commit and-quit
Commit complete.
vEdge30#
```

```
conf t
system
host-name vEdge30
system-ip 10.255.255.31
organization-name "swat-sdwanlab"
site-id 30
vbond 100.100.100.3
exit
!
vpn 0
ip route 0.0.0.0/0 100.100.100.1
interface ge0/0
ip address 100.100.100.30/24
no tunnel-interface
no shutdown
exit
!
```

```
exit
!
vpn 512
  ip route 0.0.0.0/0 192.168.0.1
  interface eth0
    ip address 192.168.0.30/24
    no shutdown
!
commit and-quit
```

4. Open **Putty** and double-click the saved session for vEdge30 (or **SSH to 192.168.0.30**)

5. Choose Yes to accept the certificate, if prompted

PuTTY Security Alert



WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.

The new ecdsa-sha2-nistp256 key fingerprint is:

ecdsa-sha2-nistp256 256

7c:de:34:0d:98:36:6a:64:a1:69:07:d8:68:44:d4:8f

If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.

If you want to carry on connecting but without updating the cache, hit No.

If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

Yes

No

Cancel

Help

6. Log in using the same credentials as Step 2.

Task List

- [Creating the vEdge30 VM](#)
- [Overview](#)
- [Deploying the vEdge30 VM on vCenter](#)

- Onboarding vEdge30
- [Bootstrapping vEdge30 \(Initial Configuration\)](#)
- Installing certificates and activating the vEdge

Installing certificates and activating the vEdge

1. Type `vshell` and enter `scp admin@192.168.0.6:ROOTCA.pem .` to copy the ROOTCA.pem certificate to the vEdge. Commands can be copy-pasted now since we have SSH'd in to the vEdge (there is a dot at the end of the scp command). Enter `yes` when prompted and enter the password of vManage (i.e. admin). Once the ROOTCA.pem file is copied over, type `exit` and hit Enter to go back to the vEdge CLI.

```
vshell  
scp admin@192.168.0.6:ROOTCA.pem .
```

2. Go to the vManage GUI (<https://192.168.0.6>) and log in, if logged out. Navigate to **Configuration => Devices** (from the left-hand side, click on the cog wheel to access the configuration options)

The screenshot shows the Cisco vManage Main Dashboard. On the left, a sidebar lists various management categories: Configuration (2 items), Devices (selected), TLS/SSL Proxy, Certificates, Network Design, Templates, Policies, Security, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, and Cloud onRamp for Colocation. The 'Devices' section is currently active, indicated by a teal bar at the top. The main content area includes a 'Site Health (Total 0)' section with three status counts: Full WAN Connectivity (0 sites), Partial WAN Connectivity (0 sites), and No WAN Connectivity (0 sites). Below it is a 'WAN Edge Health (Total 0)' section with three circular indicators labeled 'Normal', 'Warning', and 'Error', each showing a value of 0. Further down is an 'Application-Aware Routing' section with tabs for 'Tunnel Endpoints' and 'Avg. Latency (ms)', both showing 'No data'. At the bottom of the dashboard, there is a message 'No data to display'.

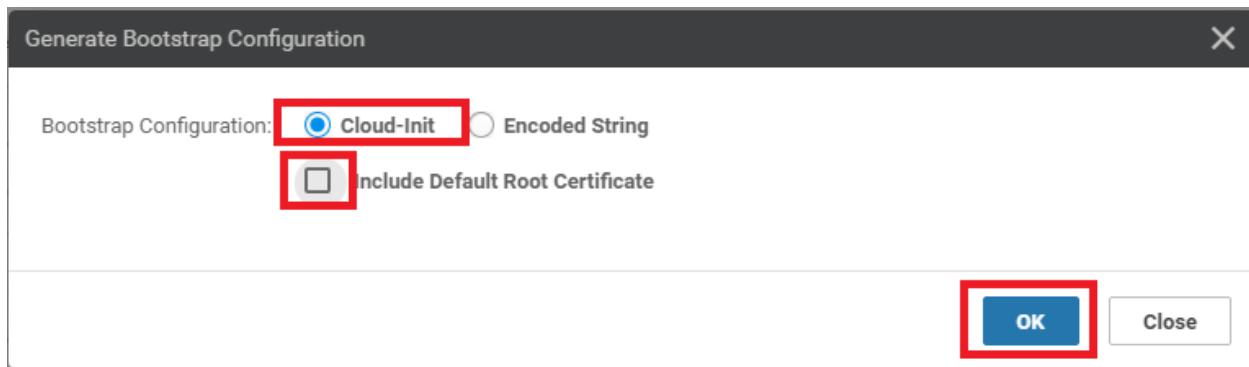
<https://192.168.0.6/index.html#/app/config/devices/vedge>

- Choose any vEdge Cloud device (it doesn't matter which one you pick, as long as it is a vEdge Cloud) and click on the three dots at the extreme right-hand side. Choose to Generate Bootstrap Configuration

The screenshot shows a list of vEdge Cloud devices. The first device in the list, 'vEdge Cloud' with Token '17026153-f09e-be4b-6dce-482fce43aa...', is highlighted with a yellow background. A context menu is open over this device, listing options: Running Configuration, Local Configuration, Delete WAN Edge, Copy Configuration, Generate Bootstrap Configuration, Template Log, and Device Bring Up. The rest of the table lists other devices like CSR1000v and CSR1000v, along with their tokens and status.

| Device Type | Model | Token | Status | Actions | |
|-------------|-------------------------------------|---------------------------------------|---------------------------|---------|----|
| vEdge Cloud | CSR1000v | CSR-04F9482E-44F0-E4DC-D30D-60C0... | NA | NA | |
| vEdge Cloud | vEdge Cloud | e474c5fd-8ce7-d376-7cae-ba950b2c91... | 7175AE0F | NA | |
| vEdge Cloud | vEdge Cloud | 0ddd4f0e-f2f1-fe75-866c-469966cd1c3 | 7DA605F5 | NA | |
| vEdge Cloud | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2edff1609 | 297060DD | NA | |
| vEdge Cloud | vEdge Cloud | dde90ff0-dc62-77e6-510f-08d96608537a | BBFD4E65 | NA | |
| vEdge Cloud | vEdge Cloud | 17026153-f09e-be4b-6dce-482fce43aa... | Token - 3692590e4778... | NA | |
| CSR1000v | CSR-26217DA0-1B63-8DDE-11C9-125F... | Token - 8dc7b557b60d... | NA | NA | |
| CSR1000v | CSR-960E020-B7C9-887F-46A8-F4537... | Token - 50cc04634a0c... | NA | NA | |
| CSR1000v | CSR-25925FBC-07F3-0732-E127-EA95... | Token - 6ced66053d46... | NA | NA | |
| vEdge Cloud | vEdge Cloud | 35bd9f69-1758-116c-4e4c-e34c706645... | Token - ed778f569bab0... | NA | NA |
| vEdge Cloud | vEdge Cloud | 005c424c-2d57-41fe-250d-ee991e0a4e... | Token - 56f4f154ce614d... | NA | NA |
| vEdge Cloud | vEdge Cloud | 21292349-2c9f-7aa5-28f5-a87e4d0054cb | Token - b6046dee4fa2a... | NA | NA |

4. Select **Cloud-Init** and **uncheck Include Default Root Certificate**. Click on **OK**



5. Make note of the **UUID** and the **OTP** values. These will be required to activate the vEdge. It's best to copy the string and place it in notepad, since we will need to use it in our SSH session to the vEdge30 device. Alternatively, leave this popup open and we can come back to it when required

Generate Bootstrap Configuration



Download

```
#cloud-config
vinitparam:
- uuid : 17026153-f09e-be4b-6dce-482fce43aab2
- vbond : 100.100.100.3
- otp : 3692590e47782dd2ae043b8a4369c145
- org : swat-sdwanlab
- rcc : true
ca-certs:
remove-defaults: false
trusted:
- |
---BEGIN CERTIFICATE---
MIIF7DCCBNsgAwIBAgIQbsx6pacDIAm4rz06VLUKTANBgkqhkiG9w0BAQUFADCB
-----END CERTIFICATE-----
```

Close

6. Go back to the Putty session for vEdge30 and enter `request root-cert-chain install /home/admin/ROOTCA.pem` to install the root cert chain. It should install successfully

```
request root-cert-chain install /home/admin/ROOTCA.pem
```

7. Enter `tunnel-interface`, `encapsulation ipsec` and `allow-service all` under `interface ge0/0` to bring up the tunnel Interface. Make sure to `commit and-quit` in order to write the configuration change

```
config t
vpn 0
interface ge0/0
tunnel-interface
encapsulation ipsec
allow-service all
exit
!
commit and-quit
```

This ensures that our vEdge is now able to establish control connections with the vManage and vSmarts via the vBond. However, these connections will not be fully formed till we don't activate the vEdge itself

8. Issue the `request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)` command. Replace the (*Enter your UUID*) and (*Enter your OTP*) fields with the UUID and OTP generated in Step 5 (image below is an example, UUID and OTP may not match).

```
vEdge30# request root-cert-chain install /home/admin/R0OTCA.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/R0OTCA.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
vEdge30#
vEdge30# conf t
Entering configuration mode terminal
vEdge30(config)# vpn 0
vEdge30(config-vpn-0)# interface ge0/0
vEdge30(config-interface-ge0/0)# tunnel-interface
vEdge30(config-tunnel-interface)# allow-service all
vEdge30(config-tunnel-interface)# encapsulation ipsec
vEdge30(config-tunnel-interface)# commit and-quit
Commit complete.
vEdge30#
vEdge30#
vEdge30#
vEdge30#
vEdge30#
vEdge30# request vedge-cloud activate chassis-number 17026153-f09e-be4b-6dce-482
fce43aab2 token 3692590e47782dd2ae043b8a4369c145
```

```
request vedge-cloud activate chassis-number (Enter your UUID) token (Enter the OTP)
```

This completes the Onboarding section for vEdge30

Task List

- [Creating the vEdge30 VM](#)
- [Overview](#)
- [Deploying the vEdge30 VM on vCenter](#)
- [Onboarding vEdge30](#)
- [Bootstrapping vEdge30 \(Initial Configuration\)](#)
- [Installing certificates and activating the vEdge](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Site last generated: Jul 23, 2020



-->

Deploying a Dual Uplink cEdge

Summary: Deploying Site 40 with a single cEdge which has both transport uplinks

Table of Contents

- [Verifying the existing lab setup](#)
- [Creating the cEdge40 VM](#)
 - [Overview](#)
 - [Deploying the VM on vCenter](#)
- [Onboarding cEdge40](#)
 - [Initial Configuration - non SD-WAN mode](#)
 - [Setting up Feature Templates](#)
 - [Creating and Attaching Device Templates](#)
 - [Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)
- [Onboarding Verification](#)

Task List

- Verifying the current lab setup
- Creating the cEdge40 VM
- Onboarding cEdge40
 - Initial Configuration - non SD-WAN mode
 - Setting up Feature Templates
 - Creating and Attaching Device Templates
 - Copying the Bootstrap file and converting to SD-WAN IOS-XE mode
- Onboarding Verification

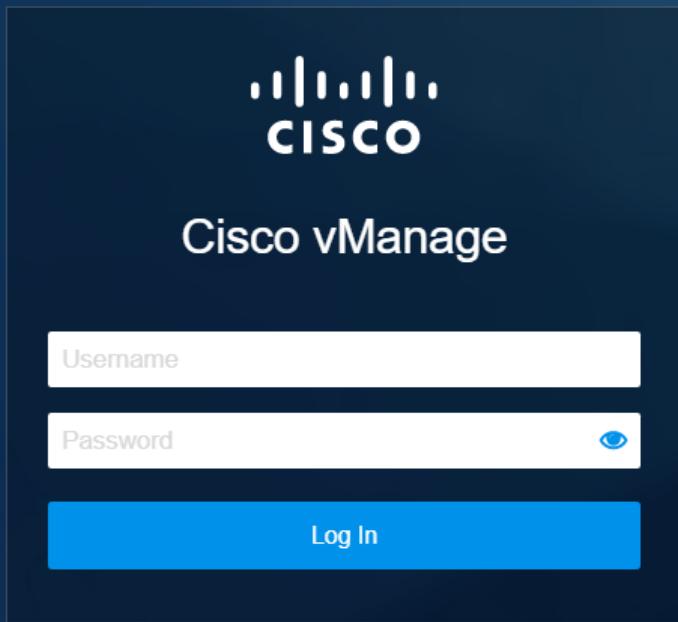
Verifying the existing lab setup

The vManage, vBond and vSmarts have been deployed along with Sites 1, 20 and 30. We will start by verifying the existing setup.

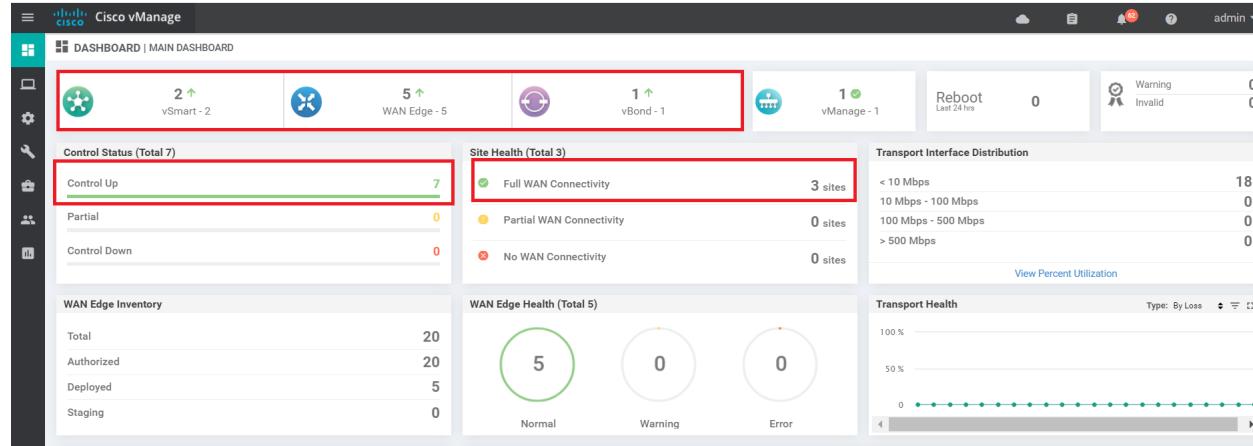
1. Log in to vManage by clicking on the bookmark or navigating to <https://192.168.0.6>. Use the following credentials:

| Username | Password |
|----------|----------|
| admin | admin |

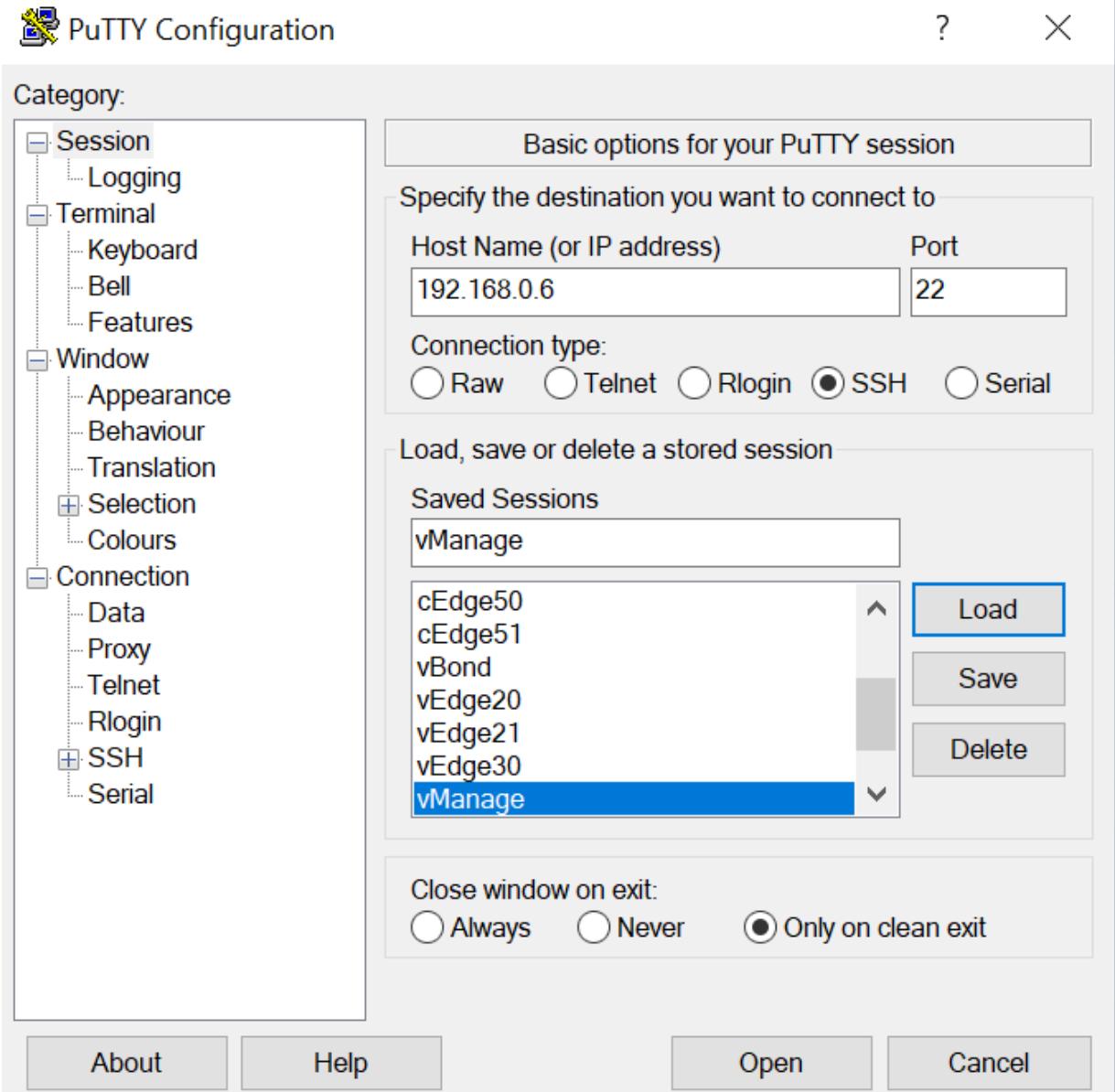
Cisco SD-WAN



2. On logging in, you should see 2 vSmarts, 1 vBond and 1 vManage along with 5 WAN Edges. 7 control planes should be up and 3 sites should have WAN connectivity. If you see 7 WAN Edges with 9 Control Planes, that is OK as well (since it depends on the scenario chosen while registering for the lab)



3. Open and log in to the vManage via the CLI - fire up Putty and double click the saved session for vManage or SSH to 192.168.0.6. Use the same credentials as the GUI.



4. Issue `show control connections` and you should see the vManage talking to the vSmarts, vBond and vEdges.
Note the **System IP** and the fact that all the connections are **up**

| INDEX | TYPE | PROT | SYSTEM IP | SYSTEM IP | ID | ID | PRIVATE IP | PEER | | PEER | | PEER | | | |
|----------|--------|--------|------------------|---------------|------|----|----------------|------------|----------------|-------------|---------------|-----------|------|--------------|------|
| | | | | | | | | CONFIGURED | SITE | DOMAIN PEER | PRIV | PEER | PUB | | |
| TE COLOR | STATE | UPTIME | | | | | | | | | PORT | PUBLIC IP | PORT | ORGANIZATION | REMO |
| 0 | vedge | dtls | 10.255.255.11 | 10.255.255.11 | 1 | 1 | 100.100.100.10 | 12366 | 100.100.100.10 | 12366 | swat-adwanlab | defa | | | |
| 0 | ult | up | 3:19:16:27 | | | | | 12366 | 192.0.2.10 | 12366 | swat-adwanlab | defa | | | |
| 0 | vedge | dtls | 10.255.255.22 | 10.255.255.22 | 20 | 1 | 192.0.2.10 | 12366 | 192.0.2.10 | 12366 | swat-adwanlab | defa | | | |
| 0 | ult | up | 0:0:0:0:0:0:0:04 | | | | | 12346 | 100.100.100.4 | 12346 | swat-adwanlab | defa | | | |
| 0 | vsmart | dtls | 10.255.255.3 | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12346 | 100.100.100.4 | 12346 | swat-adwanlab | defa | | | |
| 0 | ult | up | 6:17:46:09 | | | | | 12346 | 100.100.100.5 | 12346 | swat-adwanlab | defa | | | |
| 0 | vsmart | dtls | 10.255.255.4 | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12346 | 100.100.100.5 | 12346 | swat-adwanlab | defa | | | |
| 0 | ult | up | 6:17:46:09 | | | | | 12346 | 100.100.100.3 | 12346 | swat-adwanlab | defa | | | |
| 0 | vbond | dtls | 10.255.255.2 | 10.255.255.2 | 0 | 0 | 100.100.100.3 | 12366 | 100.100.100.3 | 12366 | swat-adwanlab | defa | | | |
| 0 | ult | up | 6:17:46:09 | | | | | 12366 | 100.100.100.11 | 12366 | swat-adwanlab | defa | | | |
| 1 | vedge | dtls | 10.255.255.12 | 10.255.255.12 | 1 | 1 | 100.100.100.11 | 12366 | 100.100.100.20 | 12366 | swat-adwanlab | defa | | | |
| 1 | ult | up | 1:16:11:09 | | | | | 12366 | 100.100.100.20 | 12366 | swat-adwanlab | defa | | | |
| 1 | vedge | dtls | 10.255.255.21 | 10.255.255.21 | 20 | 1 | 100.100.100.20 | 12366 | 100.100.100.30 | 12366 | swat-adwanlab | defa | | | |
| 1 | ult | up | 0:22:34:42 | | | | | 12366 | 100.100.100.30 | 12366 | swat-adwanlab | defa | | | |
| 1 | vedge | dtls | 10.255.255.31 | 10.255.255.31 | 30 | 1 | 100.100.100.30 | 12346 | 100.100.100.3 | 12346 | swat-adwanlab | defa | | | |
| 1 | ult | up | 0:03:13:01 | | | | | 12346 | 100.100.100.3 | 12346 | swat-adwanlab | defa | | | |
| 1 | vbond | dtls | 0.0.0.0 | - | 0 | 0 | 100.100.100.3 | 12346 | 100.100.100.3 | 12346 | swat-adwanlab | defa | | | |
| 1 | ult | up | 6:17:46:10 | | | | | 12346 | 100.100.100.3 | 12346 | swat-adwanlab | defa | | | |

Look at the System IP to see which device has the vManage established a control connection with. There should be 5 (or 7, depending on the selected lab scenario) connections to vEdges. This completes the verification activity.

Task List

- [Verifying the current lab setup](#)
- [Creating the cEdge40 VM](#)
- [Onboarding cEdge40](#)
 - Initial Configuration - non SD-WAN mode
 - Setting up Feature Templates
 - Creating and Attaching Device Templates
 - Copying the Bootstrap file and converting to SD-WAN IOS-XE mode
- [Onboarding Verification](#)

Creating the cEdge40 VM

Overview

We will be deploying a cEdge in Site 40 via vCenter. Make note of the following information for this section. The IP Addressing will not be used for some of the Network Adapters until later.

| SITE | SYSTEM ID | VM | Network Adapter | Network Management | Interface | IP | Gateway |
|------|---------------|--------------|-------------------|--------------------|------------------|-----------------|-------------|
| ID | | | | | | | |
| 40 | 10.255.255.41 | cEdge40-podX | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.40/24 | 192.168.0.1 |

| | | | | | |
|--|-------------------|--------------|------------------|----------------|---------------|
| | Network Adapter 2 | Internet | GigabitEthernet2 | 100.100.100.40 | 100.100.100.1 |
| | Network Adapter 3 | MPLS40 | GigabitEthernet3 | 192.1.2.18/30 | 192.1.2.17 |
| | Network Adapter 4 | Site40-VPN10 | GigabitEthernet4 | 10.40.10.2/24 | |
| | Network Adapter 5 | Site40-VPN20 | GigabitEthernet5 | 10.40.20.2/24 | |
| | Network Adapter 6 | Site40-VPN30 | GigabitEthernet6 | 10.40.30.2/24 | |

Tip: Plan your sites and addressing carefully. Proper planning can prevent a number of issues and will help with a successful, early deployment.

Tip: There is configuration applicable only to virtual vEdges/cEdges in some of the sections. Physical cEdges/vEdges are a lot easier to deploy, not only from a connectivity standpoint but also with respect to certificate exchange options.

Deploying the VM on vCenter

1. Click on the bookmark for vCenter or navigate to the following URL: <https://10.2.1.50/ui>. Log in with the credentials provided for your POD.



2. We should see the vEdges from previous sections of the lab deployed.

vSphere Client

vEdge30 | ACTIONS ▾

Summary Monitor Configure Permissions Datastores Networks Updates

Powered On

Guest OS: Other 3.x Linux (64-bit)
Compatibility: ESXi 5.0 and later (VM version 8)
VMware Tools: Running, version:10277 (Guest Managed)
More info
DNS Name: vEdge30
IP Addresses: 127.0.1.0
View all 8 IP addresses
Launch Web Console
Launch Remote Console Host:

Virtual machine CPU usage

VM Hardware

| | |
|-------------------|-----------------------------|
| CPU | 4 CPU(s) |
| Memory | 2 GB, 0.08 GB memory active |
| Hard disk 1 | 10.22 GB |
| Network adapter 1 | Management (connected) |
| Network adapter 2 | MPLS30 (connected) |
| Network adapter 3 | Site30-VPN10 (connected) |

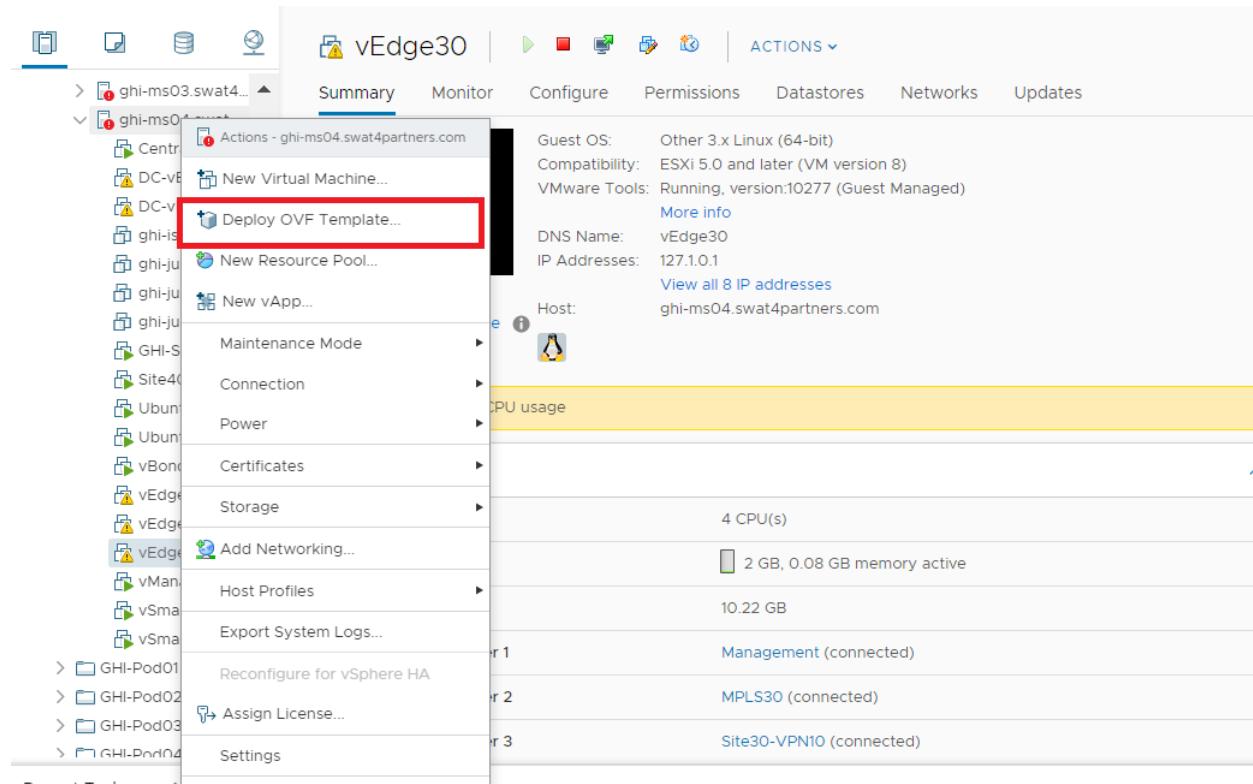
Notes

Edit Notes...

Custom Attributes

Attribute

3. Right click on the host and choose to **Deploy OVF Template**



4. Choose the **Local file** option and click on **Choose files**. Navigate to the SD-WAN images folder and select the file beginning with *csr1000v-univer*. Click on Next.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

Local file

csr1000v-univer...9.17.02.01r.ova

CANCEL

BACK

NEXT

5. Change the Virtual Machine name to **cEdge40-podX** and click on Next (X is your POD number, image below doesn't reflect the podX suffix)

Note: We will only use the podX suffix over here to distinguish between different VMs in our Data Center. The rest of the guide will refer to this VM as **cEdge40**

Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

- ▽ ghi-vcenter.swat4partners.com
 - > SWAT-Labs-GHI
 - > slc-vcenter.swat4partners.com

CANCEL

BACK

NEXT

6. Select the host assigned to you (image shown as an example only) and click on Next

Note: If the screen gets stuck over here at **Validating** then close Chrome and open the vCenter in Internet Explorer, going through the same steps. Deployment should go through. This is a known issue with Google Chrome.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

- ▼ SWAT-Labs-GHI
 - ✓ Management-Shared Services
 - > ghi-ms01.swat4partners.com
 - > ghi-ms02.swat4partners.com
 - > ghi-ms03.swat4partners.com
 - > **ghi-ms04.swat4partners.com**
 - > GHI-Pod01
 - > GHI-Pod02
 - > GHI-Pod03
 - > GHI-Pod04
 - > GHI-Pod05
 - > GHI-Pod06
 - > GHI-Pod07
 - > GHI-Pod08
 - > GHI-Pod09
 - > GHI-Pod10

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

7. Review the details shown and click on Next. Select the **Large** option (4 vCPUs and 4 GB RAM) and click on Next

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource

Review details
Verify the template details.

4 Review details

- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

| | |
|---------------|---------------------------------------|
| Publisher | No certificate present |
| Product | Cisco CSR 1000V Cloud Services Router |
| Version | 17.02.01r |
| Vendor | Cisco Systems, Inc. |
| Download size | 510.2 MB |
| Size on disk | 788.9 MB (thin provisioned) |
| | 8.5 GB (thick provisioned) |

CANCEL

BACK

NEXT

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details

5 Configuration

- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Configuration
Select a deployment configuration

| | |
|--|--|
| <input type="radio"/> Small | Description |
| <input type="radio"/> Medium | Large hardware profile - 4 vCPUs, 4 GB RAM |
| <input checked="" type="radio"/> Large | |
| <input type="radio"/> Large + DRAM Upgrade | |
| 4 Items | |

CANCEL BACK **NEXT**

8. Choose the Datastore and click on Next.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select storage
Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format:

Thick Provision Lazy Zeroed

VM Storage Policy:

Datastore Default

| Name | Capacity | Provisioned | Free | T |
|-------------|----------|-------------|----------|---|
| ghi-ms04-ds | 11.63 TB | 1.1 TB | 10.99 TB | V |

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

9. Populate the VM Networks as per the image given below

⚠ Important: Please make sure that these look exactly as shown below

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Configuration
- ✓ 6 Select storage
- 7 Select networks**
- 8 Customize template
- 9 Ready to complete

Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|------------------|---------------------|
| GigabitEthernet1 | Management |
| GigabitEthernet2 | Internet |
| GigabitEthernet3 | MPLS40 |

3 items

IP Allocation Settings

IP allocation:

Static - Manual

IP protocol:

IPv4

CANCEL

BACK

NEXT

10. Click Next on **Customize Template** and then Click on **Finish** to deploy your cEdge40 VM. **Please do not power on the VM at this point**

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details**
- ✓ 5 Configuration
- ✓ 6 Select storage
- ✓ 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template
Customize the deployment properties of this software solution.

All properties have valid values X

1. Bootstrap Properties 13 settings

| | |
|----------------|--|
| Router Name | Hostname of this router |
| Login Username | Username for remote login |
| Login Password | Password for remote login. WARNING: While this password will be stored securely within IOS, the plain-text password will be recoverable from the OVF descriptor file. |
| Password | _____ |
| Confirm | _____ |
| Password | _____ |
| Domain Name | Network domain name (such as "cisco.com") |
| _____ | _____ |

[CANCEL](#) [BACK](#) **NEXT**

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details**
- ✓ 5 Configuration
- ✓ 6 Select storage
- ✓ 7 Select networks
- ✓ 8 Customize template

9 Ready to complete

Ready to complete
Click Finish to start creation.

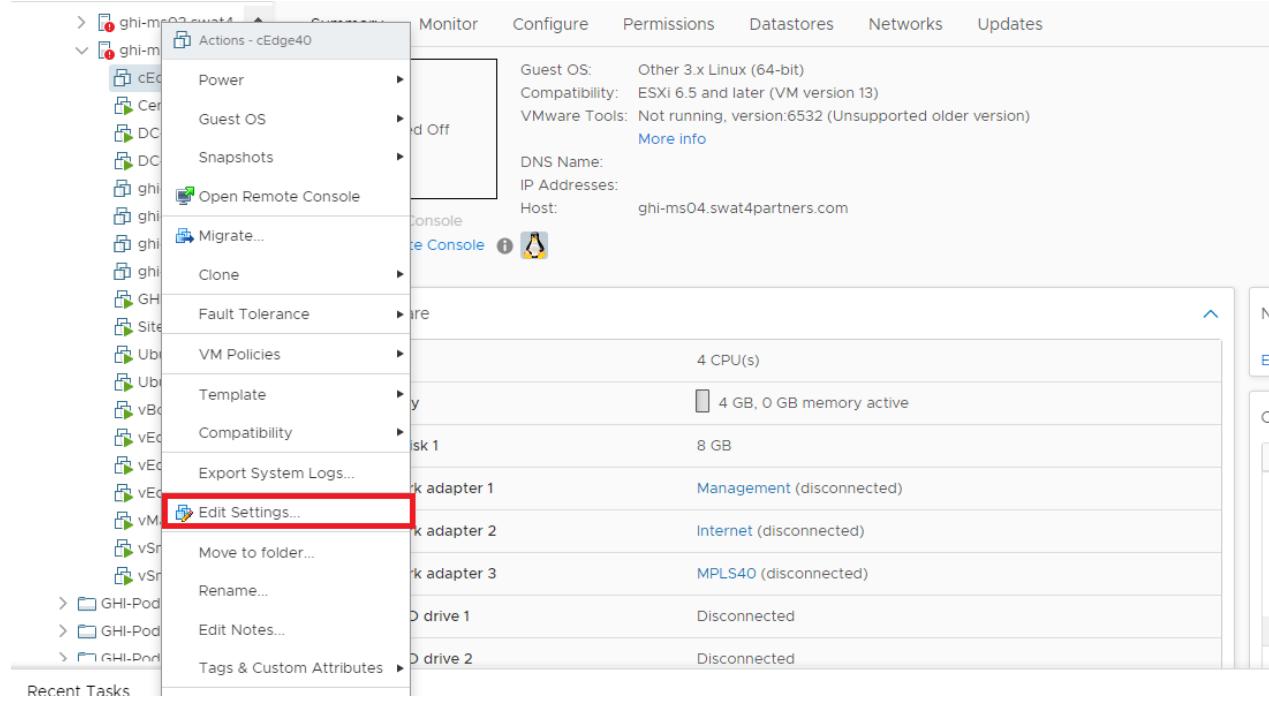
| | |
|------------------------|---|
| Provisioning type | Deploy from template |
| Name | cEdge40 |
| Template name | csr1000v-universalk9.17.02.01r-vga |
| Download size | 510.2 MB |
| Size on disk | 8.5 GB |
| Folder | SWAT-Labs-GHI |
| Resource | ghi-ms04.swat4partners.com |
| Storage mapping | 1 |
| All disks | Datastore: ghi-ms04-ds; Format: Thick provision lazy zeroed |
| Network mapping | 3 |
| GigabitEthernet1 | Management |
| GigabitEthernet2 | Internet |
| GigabitEthernet3 | MPLS40 |
| IP allocation settings | |

CANCEL

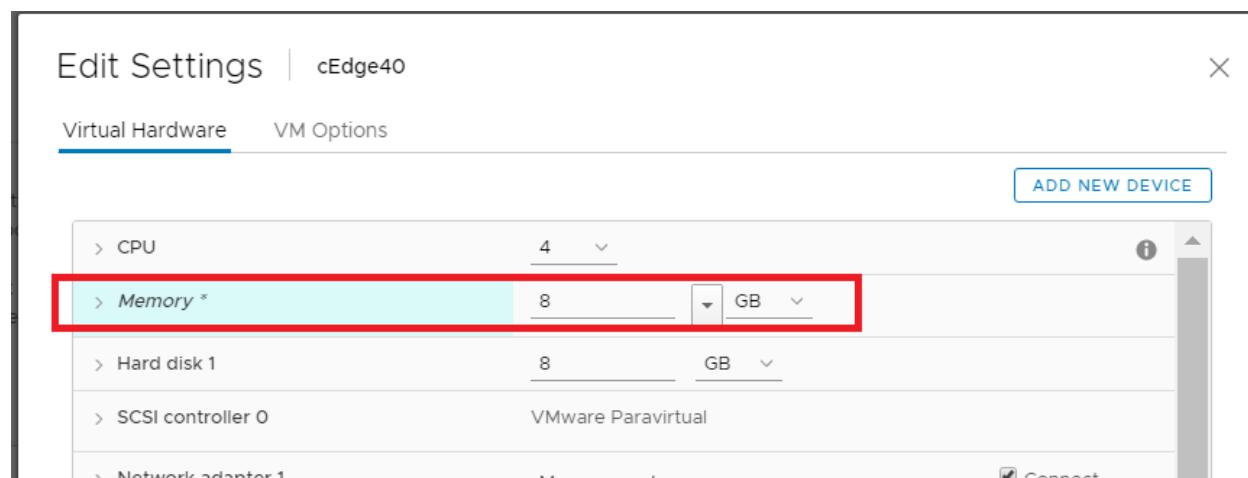
BACK

FINISH

11. Once the VM is deployed, right click **cEdge40-podX** and click Edit settings.



12. Change the memory to **8 GB** (needed since we will be deploying an IPS module on this cEdge, which requires a minimum of 8 GB RAM) and choose to **Add a new device** (top right corner). Select Network Adapter to add one (since our deployed VM has only 3 Network Adapters but we will need 6 for our lab). Do this twice more for a grand total of 6 Network Adapters



Edit Settings | cEdge40

X

Virtual Hardware VM Options

- CD/DVD Drive
- Host USB Device
- Hard Disk
- RDM Disk
- Existing Hard Disk
- Network Adapter**
- SCSI Controller
- USB Controller
- SATA Controller
- NVMe Controller
- Shared PCI Device
- PCI Device
- Serial Port

ADD NEW DEVICE

| | |
|---|---|
| 4 | ▼ |
| 8 | ▼ GB ▼ |
| 8 | GB ▼ |
| VMware Paravirtual | |
| Management | ▼ <input checked="" type="checkbox"/> Connect... |
| Internet | ▼ <input checked="" type="checkbox"/> Connect... |
| MPLS40 | ▼ <input checked="" type="checkbox"/> Connect... |
| CD/DVD drive 1 | Datastore ISO File ▼ <input checked="" type="checkbox"/> Connect... |
| CD/DVD drive 2 ! | Host Device ▼ <input type="checkbox"/> Connect... |
| Video card | Specify custom settings ▼ |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface |
| Other | Additional Hardware ▼ |

CANCEL

OK

Edit Settings | cEdge40

X

Virtual Hardware VM Options

ADD NEW DEVICE

| | | |
|---------------------|--------------------|--------------|
| > CPU | 4 | ▼ |
| > Memory * | 8 | GB ▼ |
| > Hard disk 1 | 8 | GB ▼ |
| > SCSI controller 0 | VMware Paravirtual | |
| > Network adapter 1 | Management | ✓ Connect... |
| > Network adapter 2 | Internet | ✓ Connect... |
| > Network adapter 3 | MPLS40 | ✓ Connect... |
| > New Network * | Internet | ✓ Connect... |
| > New Network * | Internet | ✓ Connect... |
| > New Network * | Internet | ✓ Connect... |
| > CD/DVD drive 1 | Datastore ISO File | ✓ Connect... |
| > CD/DVD drive 2 | Host Device | □ Connect... |

CANCEL

OK

13. Click on the drop down next to the first **New Network** and click on *Browse*

Edit Settings | cEdge40

X

Virtual Hardware VM Options

ADD NEW DEVICE

| | | |
|---|--------------------|---|
| > CPU | 4 | ▼ |
| > Memory * | 8 | GB ▼ |
| > Hard disk 1 | 8 | GB ▼ |
| > SCSI controller 0 | VMware Paravirtual | |
| > Network adapter 1 | Management | ✓ Connect... |
| > Network adapter 2 | Internet | ✓ Connect... |
| > Network adapter 3 | MPLS40 | ✓ Connect... |
| > New Network * | Internet | ✓ Connect... <input type="button" value="X"/> |
| > New Network * | Internet | ✓ Connect... |
| > New Network * | Internet | ✓ Connect... |
| > CD/DVD drive 1 | Datastore ISO File | ✓ Connect... |
| > CD/DVD drive 2 ! | Host Device | <input type="checkbox"/> Connect... |

CANCEL

OK

14. Choose the **Site40-VPN10** Network and click on OK. Do the same for the next two network adapters, allocating them to **Site40-VPN20** and **Site40-VPN30** respectively. Make sure the Network Adapters match with the second image below and click on OK again

⚠ Warning: The Network Adapter mapping might vary based on the version of cEdge being deployed. Sometimes, trial and error is the easiest way to figure out which Network Adapter maps to which interface on the cEdge

Virtual Hardware VM Options

ADD NEW DEVICE

- > CPU
- > Memory *
- > Hard disk 1
- > SCSI controller
- > Network adapter
- > Network adapter
- > Network adapter
- > New Network Adapter
- > New Network Adapter
- > New Network Adapter
- > CD/DVD drive
- > CD/DVD drive

Select Network

X

▼ Filter

| Name | Distributed Switch |
|--------------|--------------------|
| Site20-VPN20 | -- |
| Site30-VPN10 | -- |
| Site30-VPN20 | -- |
| Site40-VPN10 | -- |
| Site40-VPN20 | -- |
| Site40-VPN30 | -- |
| Site50-VPN10 | -- |
| Site50-VPN20 | -- |

40 items

CANCEL

OK

CANCEL

OK

Edit Settings | cEdge40

X

Virtual Hardware VM Options

ADD NEW DEVICE

| | | |
|---|--------------------|--|
| > CPU | 4 | v |
| > Memory * | 8 | GB v |
| > Hard disk 1 | 8 | GB v |
| > SCSI controller 0 | VMware Paravirtual | |
| > Network adapter 1 | Management | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 2 | Internet | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 3 | MPLS40 | <input checked="" type="checkbox"/> Connect... |
| > New Network * | Site40-VPN10 | <input checked="" type="checkbox"/> Connect... |
| > New Network * | Site40-VPN20 | <input checked="" type="checkbox"/> Connect... |
| > New Network * | Site40-VPN30 | <input checked="" type="checkbox"/> Connect... |
| > CD/DVD drive 1 | Datastore ISO File | <input checked="" type="checkbox"/> Connect... |
| > CD/DVD drive 2 ! | Host Device | <input type="checkbox"/> Connect... |

CANCEL

OK

15. Click on cEdge40-podX and choose to power it on

Task List

- [Verifying the current lab setup](#)

- [Creating the cEdge40 VM](#)
- [Onboarding cEdge40](#)
 - Initial Configuration - non SD-WAN mode
 - Setting up Feature Templates
 - Creating and Attaching Device Templates
 - Copying the Bootstrap file and converting to SD-WAN IOS-XE mode
- [Onboarding Verification](#)

Onboarding cEdge40

Initial Configuration - non SD-WAN mode

Use the following information in this section (some of the information will be used later)

| SITE ID | SYSTEM ID | VM | Network Adapter | Network | Management | Interface | IP | Gateway |
|------------|---------------|---------|--------------------|-----------------|--------------|------------------|-----------------|---------------|
| 40 | 10.255.255.41 | cEdge40 | Network Adapter 1 | Network Adapter | Management | GigabitEthernet1 | 192.168.0.40/24 | 192.168.0.1 |
| | | | Network Adapter 2 | Network Adapter | Internet | GigabitEthernet2 | 100.100.100.40 | 100.100.100.1 |
| | | | Network Adapter 3 | Network Adapter | MPLS40 | GigabitEthernet3 | 192.1.2.18/30 | 192.1.2.17 |
| | | | Network Adapter 4 | Network Adapter | Site40-VPN10 | GigabitEthernet4 | 10.40.10.2/24 | |
| | | | Network Adapter 5 | Network Adapter | Site40-VPN20 | GigabitEthernet5 | 10.40.20.2/24 | |
| | | | Network Adapter | Network Adapter | Site40-VPN30 | GigabitEthernet6 | 10.40.30.2/24 | |

Tip: Starting from IOS-XE 17.2, the cEdge platforms use a Universal image. One can switch from non SD-WAN mode to SD-WAN mode via a command

1. We will first console in to the cEdge and set up an IP Address with basic routing to ensure that the cEdge can reach vManage and the Jumphost. This is done by issuing `ip route 0.0.0.0 0.0.0.0 192.168.0.1` followed by `interface GigabitEthernet1` and giving an IP Address to the interface through `ip address 192.168.0.40 255.255.255.0`. Make sure you `no shut` the interface.

Additionally, we will be SCP'ing files over to the cEdge (root certificates) from vManage.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig
Router(config)#interface gigabitEthernet 1
Router(config-if)#ip address 192.168.0.40 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
Router(config)*
Router(config)*
Router(config)*
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
Router(config)*
*May 18 13:50:29.008: %LINK-3-UPDOWN: Interface GigabitEthernet1, changed state
to up
*May 18 13:50:30.008: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1, changed state to up
```

```
Router(config)#ip scp server enable
Router(config)#
Router(config)#
Router(config)#username admin priv 15 sec admin
Router(config)#do wr
Building configuration...
[OK]
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#do wr
Building configuration...
[OK]
Router(config-line)#

```

```
enable
conf t
interface GigabitEthernet1
  ip address 192.168.0.40 255.255.255.0
  no shut
  exit
ip route 0.0.0.0 0.0.0.0 192.168.0.1
ip scp server enable
username admin priv 15 sec admin
line vty 0 4
  login local
  do wr
```

2. Verify connectivity to the vManage and the JumpHost (IP of the Jumphost might vary) by pinging **192.168.0.6** and/or the IP Address of your Jumphost

Task List

- Verifying the current lab setup
 - Creating the cEdge40 VM
 - Onboarding cEdge40
 - Initial Configuration – non SD-WAN mode
 - Setting up Feature Templates

- Creating and Attaching Device Templates
- Copying the Bootstrap file and converting to SD-WAN IOS-XE mode
- Onboarding Verification

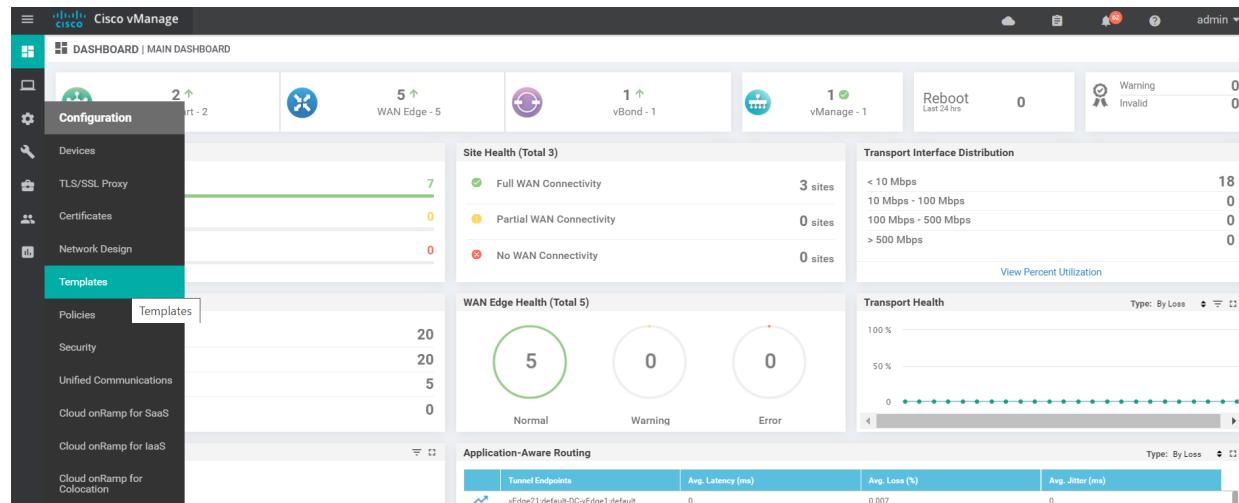
Setting up Feature Templates

Note: The Feature and Device Templates enumerated here and in the next section might already be created for you. However, it is a good practice to go through the steps below and validate the settings in the templates. This will help in familiarization with the lab setup and with fixing any deltas that might exist. If you don't see them in the configuration, please add the templates and follow the steps as enumerated below.

Templates are the key configuration components of the Cisco SD-WAN solution. They help with deploying large scale solutions with minimal effort. While there is quite a lot of initial configuration that goes into setting up these templates, their usefulness is highlighted when we're looking at onboarding multiple devices in a quick and efficient manner, reusing generic templates for devices.

Click [here](#) to access the SD-WAN Design Guide which has a section on **Configuration Templates**.

1. On the vManage GUI, navigate to **Configuration (the cog wheel icon on the left) => Templates**



2. Click on the Feature tab to access the Feature templates. Click on **Add Template**

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Feature' tab is highlighted with a red box. A 'Create Template' button is visible. The main area displays a table with columns: Name, Description, Type, Device Model, Feature Templates, Devices Attached, and Usage. A message 'No data available' is centered in the table area.

3. Search for csr and select CSR1000v on the left-hand side. This should give the option to select a template from the right. Choose **Cisco VPN** template

The screenshot shows the 'Select Template' screen. In the 'Select Devices' panel, 'csr' is searched and 'CSR1000v' is selected. The 'Select Template' panel is divided into sections: 'BASIC INFORMATION' and 'VPN'. Under 'VPN', the 'Cisco VPN' template is highlighted with a red box. Other templates listed include Cisco Secure Internet Gateway (SIG), Cisco VPN Interface GRE, Cisco VPN Interface IPsec, Cisco VPN Interface Ethernet, Cisco Security, Cisco System, Cisco AAA, Cisco BFD, Cisco NTP, Cisco OMP, Global Settings, and Security App Hosting.

4. Name your template *cEdge_VPN0_dual_uplink* and give a description of *cEdge VPN 0 Template for Dual Uplinks*. Enter the VPN as 0.

The screenshot shows the 'Configuration | Templates' section. Under 'Feature', a template named 'cEdge_VPN0_dual_uplink' is selected for a 'CSR1000v' device type. The description is 'cEdge VPN 0 Template for Dual Uplink'. The 'Basic Configuration' tab is active, displaying fields for VPN (set to 0), Name (dropdown menu), and Enhance ECMP Keying (radio buttons for On or Off). Other tabs include DNS, Advertise OMP, IPv4 Route, IPv6 Route, Service, Service Route, GRE Route, IPSEC Route, and NAT.

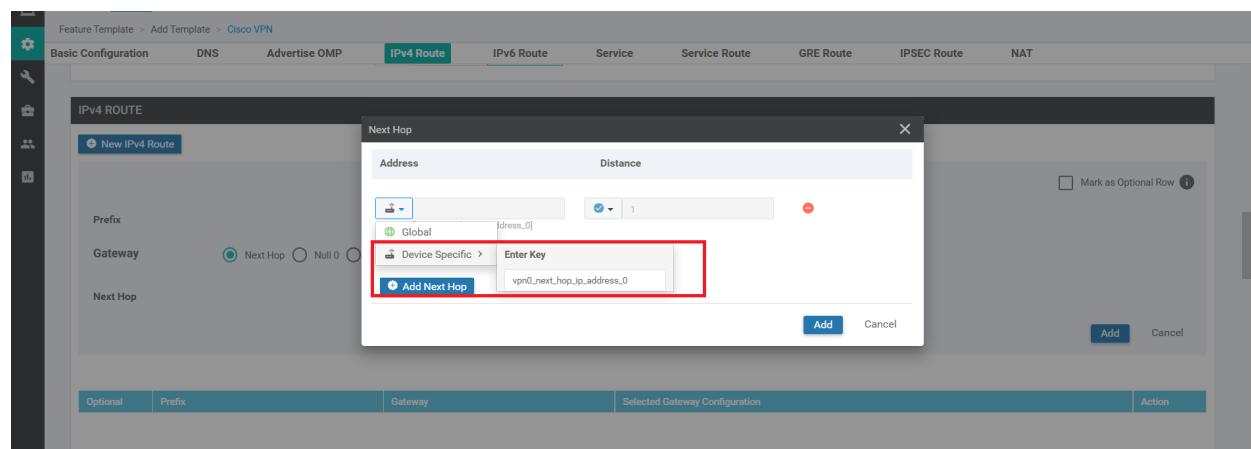
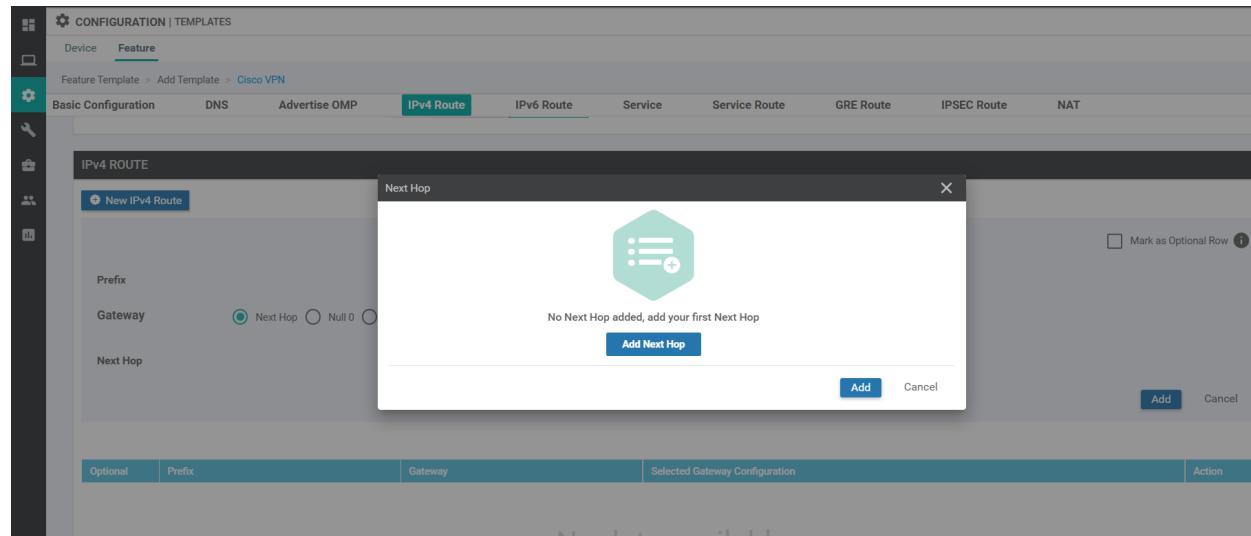
5. Click on **IPv4 Route** and then choose **New IPv4 Route**

The screenshot shows the 'IPv4 ROUTE' configuration screen. The 'New IPv4 Route' button is highlighted with a red box. Below it, there are tabs for 'Optional' and 'Prefix', and columns for 'Gateway' and 'Selected Gateway Configuration'. A message 'No data available' is displayed. At the bottom, there is an 'IPv6 ROUTE' section.

6. Enter the **Prefix** as **0.0.0.0/0** and click on **Add Next Hop**. We're adding the default route for VPN 0 (draw parallels with the manual configuration that was done on the vEdges)

The screenshot shows the 'New IPv4 Route' dialog. It has a 'Prefix' field set to '0.0.0.0/0' and a 'Gateway' section where 'Next Hop' is selected. Below is a 'Next Hop' section with an 'Add Next Hop' button. At the bottom are 'Add' and 'Cancel' buttons.

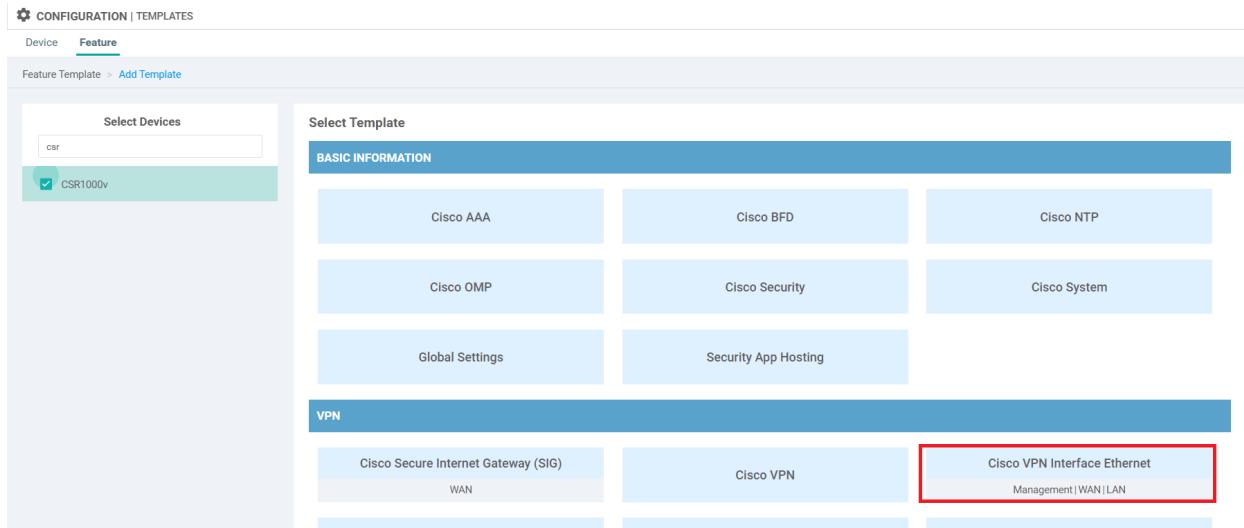
7. Click on **Add Next Hop** again and choose **Device Specific** from the Address drop down. Enter **vpn0_next_hop_ip_address_0**. Click on Add.



8. Make sure you have **1 Next Hop** showing up in the IPv4 Route window and click on **Add** again. Once on the main Template page, click on **Save** to create your Feature Template



9. Choose to **Add Template**, searching and selecting CSR1000v like before. This time, choose to add a **Cisco VPN Interface Ethernet** template



10. Populate the details as shown in the table below. Screenshots may be used as reference. Click on **Save** at the end to create your Feature Template.

| Section | Field | Global or Device Specific (drop down) | Value |
|----------------------------|------------------------------|---------------------------------------|---|
| | Template Name | NA | <i>cedge-vpn0-int-dual</i> |
| | Description | NA | cEdge VPN 0 Interface Template for Devices with a dual uplink |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Global | GigabitEthernet2 |
| Basic Configuration - IPv4 | IPv4 Address / prefix-length | Device Specific | <i>inet_ipv4_address</i> |
| Tunnel | Tunnel Interface | Global | On |

| Tunnel | Color | Device Specific | inet_if_tunnel_color_value |
|------------------------|-------|-----------------|----------------------------|
| Tunnel - Allow Service | All | Global | On |

CONFIGURATION | TEMPLATES

Device **Feature**

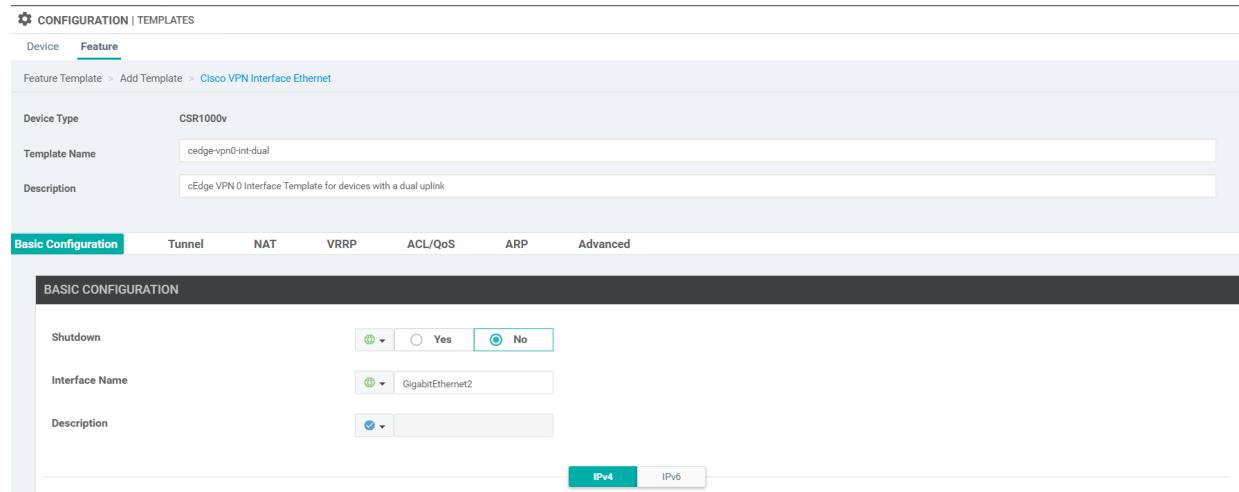
Feature Template > Add Template > Cisco VPN Interface Ethernet

Device Type: CSR1000v
 Template Name: cedge-vpn0-int-dual
 Description: cEdge VPN 0 Interface Template for devices with a dual uplink

Basic Configuration **Tunnel** **NAT** **VRRP** **ACL/QoS** **ARP** **Advanced**

BASIC CONFIGURATION

Shutdown: Yes No
 Interface Name: GigabitEthernet2
 Description:
 IPv4 IPv6



Basic Configuration **Tunnel** **NAT** **VRRP** **ACL/QoS** **ARP** **Advanced**

IPv4 **IPv6**

Dynamic Static

IPv4 Address/ prefix-length: [inet_ipv4_address]

Secondary IP Address (Maximum: 4)

DHCP Helper:

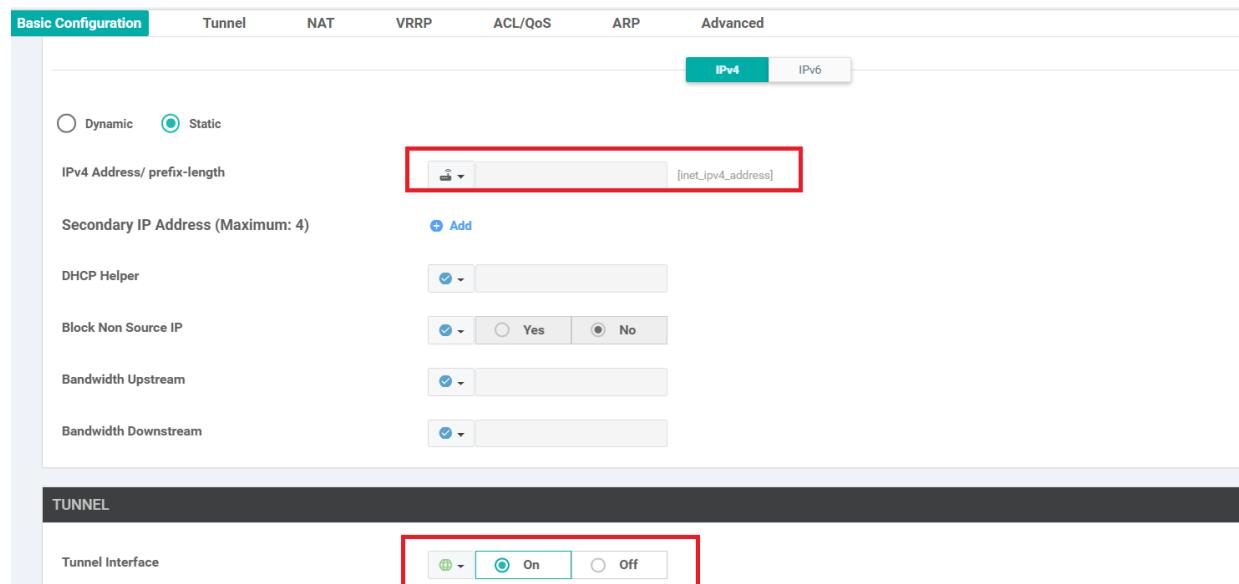
Block Non Source IP: Yes No

Bandwidth Upstream:

Bandwidth Downstream:

TUNNEL

Tunnel Interface: On Off



Feature Template > Cisco VPN Interface Ethernet

Tunnel

Basic Configuration

- Color: [inet_if_tunnel_color_value]
- Restrict: On (radio button)
- Groups:
- Border: On (radio button)
- Control Connection: On (radio button)
- Maximum Control Connections:
- vBond As Stun Server: On (radio button)
- Exclude Controller Group List:
- vManage Connection Preference: 5
- Port Hop: On (radio button)
- Low-Bandwidth Link: On (radio button)
- Allow Service:

All: On (radio button)

11. You should now see the feature template created. We now need to create the feature templates for VPN 512 and the VPN 512 Interface. The power of templates becomes apparent at this point since we can copy a template that was created previously and tweak it as per the requirement. Click on the three dots at the end of the *cEdge_VPN0_dual_uplink* template and click on **Copy**

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
|------------------------|--------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Templ... | Cisco VPN Interface | CSR1000v | 0 | 0 | admin | 18 May 2020 8:28:19 AM PDT |
| cEdge_VPN0_dual_Uplink | cEdge VPN 0 Template for Du... | Cisco VPN | CSR1000v | 0 | 0 | admin | 18 May 2020 7:37:39 AM PDT |

12. You will be prompted to name the copied template. Give it a name of *cEdge_VPN512_dual_uplink* and update the description to *cEdge VPN 512 Template for Dual Uplinks* (sometimes, the description doesn't get updated and needs

to be done again when editing the template. Reference bug ID CSCvu19244, which is fixed in vManage version 20.1.12). Click on **Copy**.

Template Copy

Template Name

cEdge_VPN512_dual_uplink

Description

cEdge VPN 512 Template for Dual Uplinks

Copy Cancel

13. Click on the three dots next to the newly created template and choose to **Edit**. Notice that the description did not get updated in the screenshot below, so we will edit it while tweaking the template

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
|--------------------------|-------------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|
| cEdge_VPN0_dual_uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000V | 0 | 0 | admin | 18 May 2020 7:37:39 AM PDT |
| cEdge_VPN512_dual_uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000V | 0 | 0 | admin | 18 May 2020 8:32:49 AM PDT |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000V | 0 | 0 | admin | 18 May 2020 8:27:20 AM PDT |

14. Populate the details as follows. To populate the IPv4 Route, click on the edit (pencil icon) next to the existing IPv4 Route and then click on **1 Next Hop**. Edit and click on **Update Changes**

| Section | Field | Global or Device Specific (drop down) | Value |
|---------|-------|--|-------|
| | | | |

| | | | |
|---------------------|------------------------------|-----------------|---|
| | Template Name | NA | cEdge_VPN512_dual_uplink |
| | Description | NA | cEdge VPN 512 Template for Dual Uplinks |
| Basic Configuration | VPN | Global | 512 |
| IPv4 Route | Update IPv4 Route - Next Hop | Device Specific | vpn512_next_hop_ip_address_0 |

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN

CSR1000v

Device Type

Template Name: cEdge_VPN512_dual_uplink

Description: cEdge VPN 512 Template for Dual Uplinks

Basic Configuration

- DNS
- Advertise OMP
- IPv4 Route
- IPv6 Route
- Service
- Service Route
- GRE Route
- IPSEC Route
- NAT

BASIC CONFIGURATION

VPN: 512

Name:

Enhance ECMP Keying: On

DNS

Primary DNS Address (IPv4):

IPv4

IPv4 ROUTE

New IPv4 Route

| Optional | Prefix | Gateway | Selected Gateway Configuration | Action |
|--------------------------|-----------|----------|--------------------------------|---|
| <input type="checkbox"/> | 0.0.0.0/0 | Next Hop | 1 | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

Update IPv4 Route

Prefix: 0.0.0.0/0

Gateway: Next Hop

Next Hop: 1 Next Hop

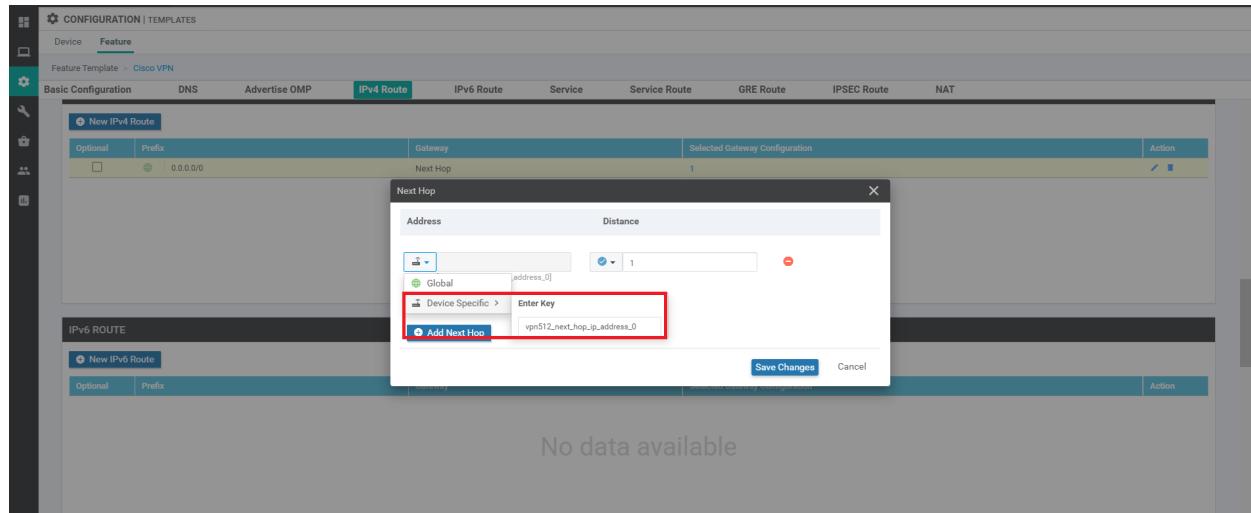
Save Changes **Cancel**

IPv6 ROUTE

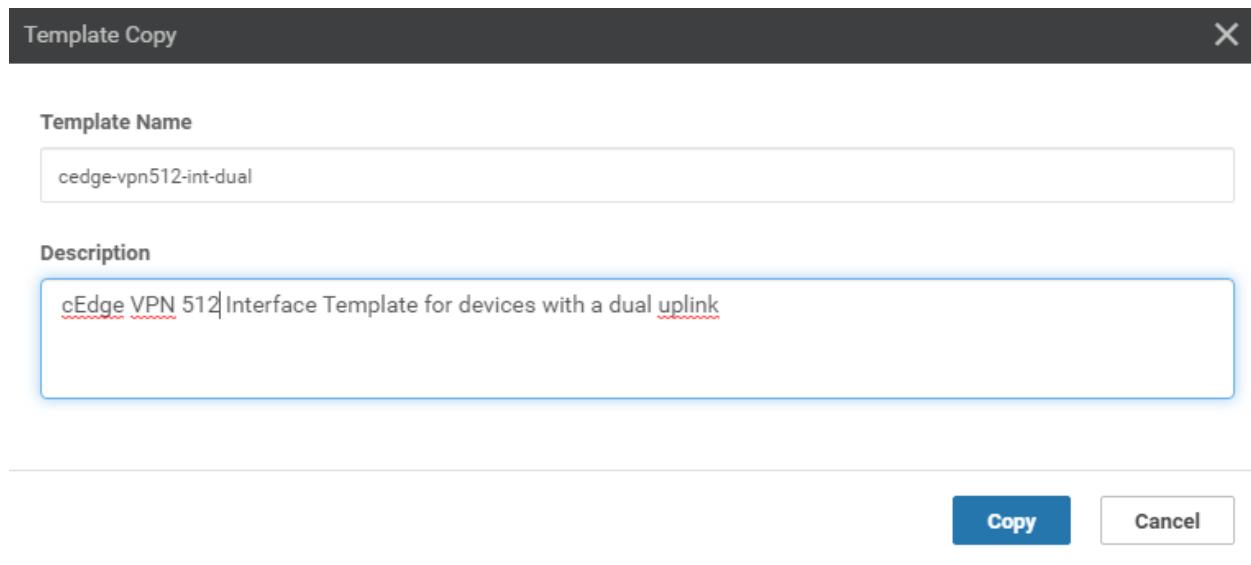
New IPv6 Route

| Optional | Prefix | Gateway | Selected Gateway Configuration | Action |
|----------|--------|---------|--------------------------------|--------|
|----------|--------|---------|--------------------------------|--------|

No data available



15. Make a copy of the VPN 0 Interface template so as to use it for VPN 512. Click on the 3 dots next to the template `cedge-vpn0-int-dual` and click on **Copy**. Update the name and description to `cedge-vpn512-int-dual` and *cEdge VPN 512 Interface Template for devices with a dual uplink* and click on **Copy**



16. Click on the three dots next to the newly copied template and choose to **Edit** it. Populate the details as given in the table below and click on **Update Changes**

| Section | Field | Global or Device Specific (drop down) | Value |
|---------|-------|---------------------------------------|-------|
| | | | |

| | | | |
|----------------------------|------------------------------|-----------------|---|
| | Template Name | NA | cedge-vpn512-int-dual |
| | Description | NA | cEdge VPN 512 Interface Template for devices with a dual uplink |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Global | GigabitEthernet1 |
| Basic Configuration - IPv4 | IPv4 Address / prefix-length | Device Specific | vpn512_mgmt_ipv4_address |
| Tunnel | Tunnel Interface | Global | Off |

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN Interface Ethernet

| | |
|---------------|---|
| Device Type | CSR1000v |
| Template Name | cedge-vpn512-int-dual |
| Description | cEdge VPN 512 Interface Template for devices with a dual uplink |

Basic Configuration

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: GigabitEthernet1

Description:

IPv4 **IPv6**

Dynamic Static

IPv4 Address/ prefix-length: [vpn512_mgmt_ipv4_address]

Secondary IP Address (Maximum: 4): Add

TUNNEL

Tunnel Interface: On Off

We are done with creating feature templates (for now) and while it was a lot of work, these templates can be reused and/or repurposed as required.

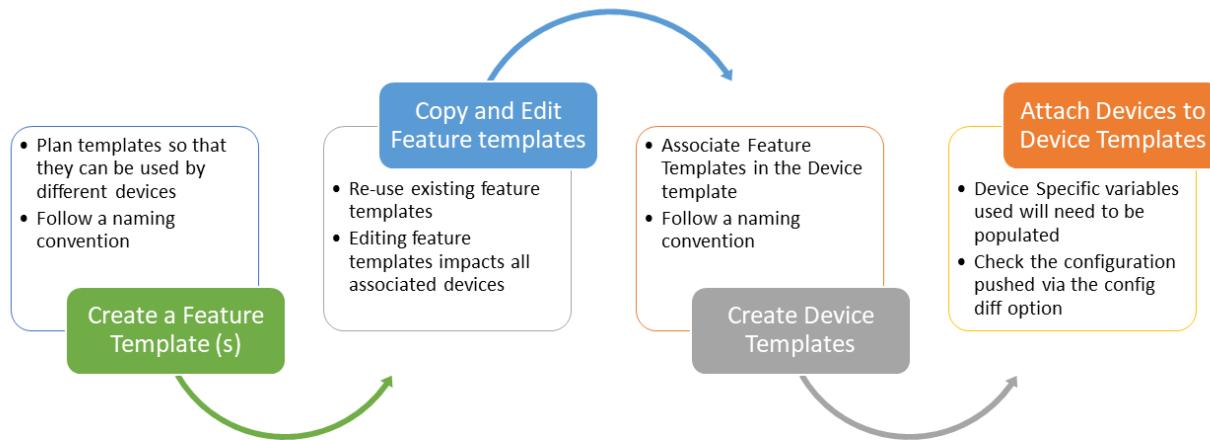
Task List

- [Verifying the current lab setup](#)
- [Creating the cEdge40 VM](#)
- Onboarding cEdge40
 - [Initial Configuration – non SD-WAN mode](#)
 - [Setting up Feature Templates](#)
 - [Creating and Attaching Device Templates](#)
 - [Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)
- Onboarding Verification

[Creating and Attaching Device Templates](#)

The feature templates created in the previous sections are referenced in Device Templates. Devices are then attached to Device Templates which pushes configuration to them, in line with the settings in the Feature templates. The general

workflow for templates is given below



1. From the **Configuration => Templates** window, make sure you're on the **Device** tab and click on **Create Template**. Choose to create a template From Feature Template

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Device' tab is selected. In the top left, there is a 'Create Template' button with a plus sign and a dropdown arrow, which is highlighted with a red box. Below it is a search bar with a magnifying glass icon and a 'Search Options' dropdown. A table header row is visible with columns: Name, Description, Type, Device Model, Feature Templates, and Devices Attached. The main content area displays the message 'No data available'.

2. Choose CSR1000v as the Device Model and enter *cedge_dualuplink_devtemp* for the **Template Name** and *cedge Device Template for devices with a dual uplink* as the **Description**

The screenshot shows the 'Create Device Template' dialog box. It has three input fields: 'Device Model' set to 'CSR1000v', 'Template Name' set to 'cEdge_dualuplink_devtemp', and 'Description' set to 'cEdge Device Template for devices with a dual uplink'.

3. In the template, navigate to the **Transport & Management VPN** section. Update the fields as per the table below, selecting templates which we created before and click on **Create** to create the Device Template

Tip: You can create templates on the fly if the template hasn't already been created. This can be done via the **Create Template** hyperlink from the drop down menu

Important: To get the option of selecting a **Cisco VPN Interface Ethernet** as shown below, click on **Cisco VPN Interface Ethernet** on the right hand side under the **Additional Templates** portion of the screen. This applies to both the VPN 0 and the VPN 512 sections

| Section | Field | Sub Field | Value (Drop Down) |
|------------------------------|---------------|------------------------------|--------------------------|
| Transport and Management VPN | Cisco VPN 0 | | cEdge_VPN0_dual_uplink |
| Transport and Management VPN | Cisco VPN 0 | Cisco VPN Interface Ethernet | cedge-vpn0-int-dual |
| Transport and Management VPN | Cisco VPN 512 | | cEdge_VPN512_dual_uplink |
| Transport and Management VPN | Cisco VPN 512 | Cisco VPN Interface Ethernet | cedge-vpn512-int-dual |

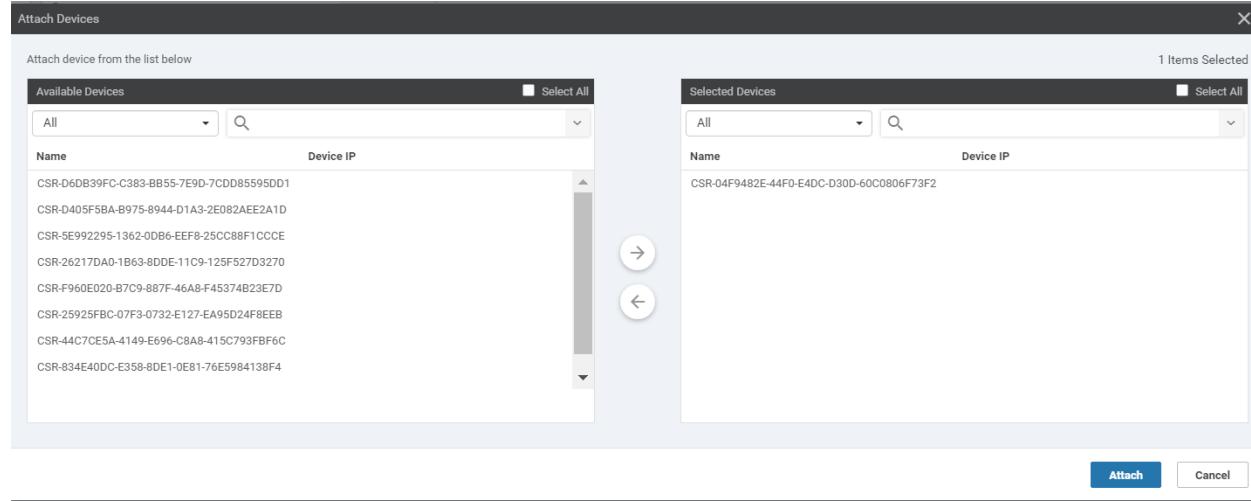
Transport & Management VPN

| | |
|------------------------------|---|
| Cisco VPN 0 * | <input type="text" value="cEdge_VPN0_dual_uplink"/> |
| Cisco VPN Interface Ethernet | <input type="text" value="cedge-vpn0-int-dual"/> |
| | |
| Cisco VPN 512 * | <input type="text" value="cEdge_VPN512_dual_uplink"/> |
| Cisco VPN Interface Ethernet | <input type="text" value="cedge-vpn512-int-dual"/> |

4. Once created, the Device Template will need to be attached to a Device for it to take effect. Click on the three dots (right-hand side) and click on **Attach Devices**

| Create Template | | | | | | | | |
|--------------------------|---------------------------------|----------------|---------------|-------------------|------------------|------------|----------------------------|-----------------|
| Template Type | Non-Default | Search Options | Total Rows: 1 | | | | | |
| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status |
| cEdge_dualuplink_devtemp | cEdge Device Template for de... | Feature | CSR1000v | 11 | 0 | admin | 18 May 2020 8:43:52 AM PDT | In Sync |

5. We will be presented with a list of devices that can be associated with this template. Choose any device, making note of the Name (e.g. the device with a name ending in **73F2** has been selected over here). Click on **Attach**



6. This should take you to a page which shows the attached device. Click on the three dots (right-hand side) and click on **Edit Device Template**. Also, make note of the cross mark next to the device name, on the left-hand side. This is the point where we need to enter details for the device specific values populated in the Feature Templates.

| Total Rows: 1 | | | | | | |
|---|-----------|----------|---------------------------------------|---|-------------------------------------|--------------|
| Chassis Number | System IP | Hostname | Address(vpn512_next_hop_ip_address_0) | IPv4 Address/ prefix-length(vpn512_mgmt_ipv4_address) | Address(vpn0_next_hop_ip_address_0) | IPv4 Address |
| CSR-04F9482E-44F0-E4DC-D30D-60C0806F... | - | - | - | - | - | ... |

Edit Device Template

7. Enter details as per the screenshot below (these can be found in the table referenced at the beginning of this page) and click on **Update**. Once the fields have been populated, the cross mark should change to a green check mark.

Update Device Template X

Variable List (Hover over each field for more information)

| | |
|---|--|
| Chassis Number | CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2 |
| System IP | - |
| Hostname | - |
| Address(vpn512_next_hop_ip_address_0) | 192.168.0.1 |
| IPv4 Address/ prefix-length(vpn512_mgmt_ipv4_address) | 192.168.0.40/24 |
| Address(vpn0_next_hop_ip_address_0) | 100.100.100.1 |
| IPv4 Address/ prefix-length(inet_ipv4_address) | 100.100.100.40/24 |
| Color(inet_if_tunnel_color_value) | public-internet ▾ |
| Hostname(host-name) | cEdge40 |
| System IP(system-ip) | 10.255.255.41 |
| Site ID(site-id) | 40 |

Generate Password Update Cancel

8. Click on the entry in the Device List to view the configuration that will be pushed to the device. Notice that the vBond IP and the Organization Name have been populated. These are taken from the vManage **Administration => Settings** page, where they need to be populated. Click on **Configure** to configure the device.

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. A device template named 'cEdge_dualuplink_devtemp' is selected, indicated by a red box around its name. The 'Config Preview' tab is active, highlighted with a red border. A yellow banner at the top right states: "'Configure' action will be applied to 1 device(s) attached to 1 device template(s.)". The configuration preview window displays the following Cisco IOS-XE configuration script:

```
system
host-name      cEdge40
system-ip       10.255.255.41
overlay-id      1
site-id         40
port-offset     1
control-session-pps 300
admin-tech-on-failure
sp-organization-name swat-sdwanlab
organization-name swat-sdwanlab
port-hop
track-transport
track-default-gateway
console-baud-rate 19200
vbond 100.100.100.3 port 12346
logging
disk
enable
!
!
bfd color lte
hello-interval 1000
no pmtu-discovery
multiplier 1
!
bfd app-route multiplier 2
bfd app-route poll-interval 123400
omp
no shutdown
graceful-restart
!
sslproxy
no enable
rsa-key-modulus 2048
```

Since this isn't a device that exists (as of now), the configuration push is scheduled for later, when a device is associated with this Device Name (the one ending in 73F2). This is done in the next section

Task List

- [Verifying the current lab setup](#)
- [Creating the eEdge40 VM](#)
- [Onboarding cEdge40](#)
 - [Initial Configuration – non SD-WAN mode](#)
 - [Setting up Feature Templates](#)
 - [Creating and Attaching Device Templates](#)
 - [Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)
- [Onboarding Verification](#)

[Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)

We will be generating a Bootstrap file and placing it in the flash of the device we want to bring up. The device (cEdge40) should come up and establish control connections with vManage, along with establishing BFD sessions with other devices.

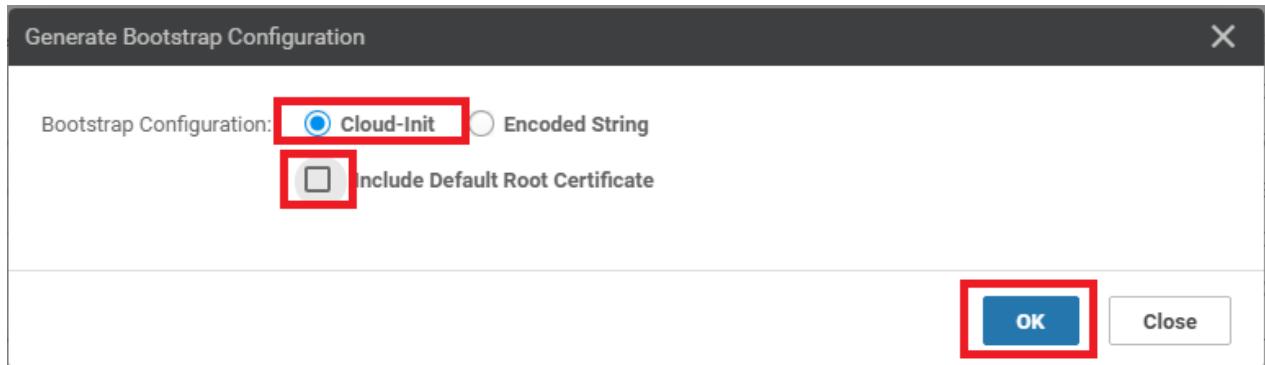
Note: While we are placing the Bootstrap file in flash for the lab, this can be put on a USB drive and plugged into the cEdge. This is usually done at a staging facility, post which the device is shipped to the customer site. Once they plug it in and power it on, the bootstrap configuration file allows the device to come up and establish control connections

1. Go to Configuration => Devices

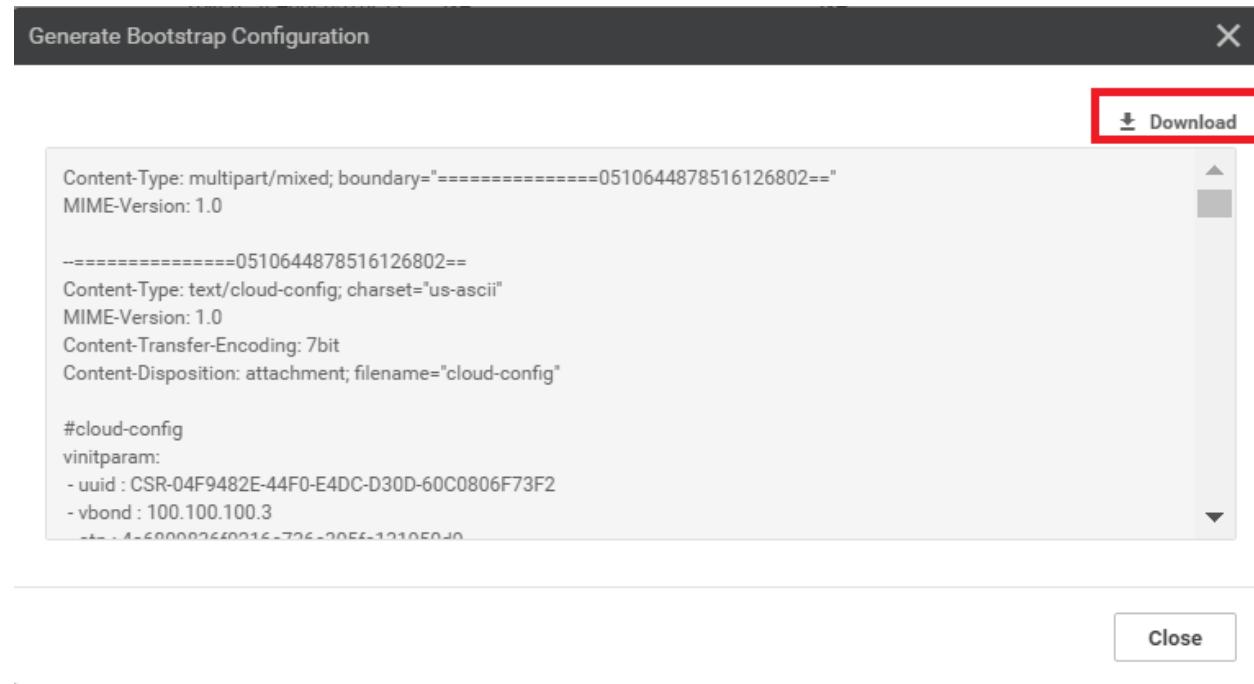
The screenshot shows the Cisco vManage web interface. The top navigation bar includes 'Login', 'cEdge40', and 'Cisco vManage'. Below the navigation is a URL bar indicating a non-secure connection to 192.168.0.6. The main content area has a dark header with 'Cisco vManage' and a 'TASK VIEW' section. Under 'TASK VIEW', there is a message: 'Push Feature Template Configuration | Validation Success'. The left sidebar contains several tabs: Configuration (selected), Devices (highlighted in teal), TLS/SSL Proxy, Certificates, Network Design, Templates, Policies, Security, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, and Cloud onRamp for Colocation. The 'Devices' tab is currently active, showing a table with columns: Message, Chassis Number, Device Model, and Hostname. A single row is visible: 'Device became unreachable. Con...', 'CSR-04F9482E-44F0-E4DC-D30D...', 'CSR1000v', and 'CSR1000v'. There is also a 'Search Options' dropdown.

- Identify the **Chassis Number** that was selected before, while attaching a Device to the Template. In this case, it ended in **73F2**. Click on the three dots on the right-hand side and click on **Generate Bootstrap Configuration**. Choose **Cloud-Init** and **uncheck Include Default Root Certificate**. Click on OK

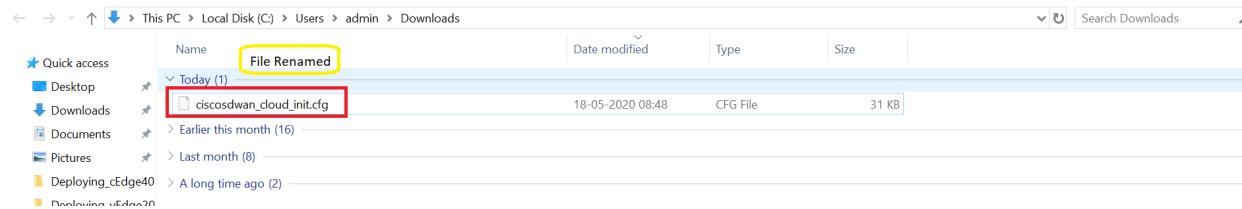
| State | Device Model | Chassis Number | Serial No./Token | Enterprise Cert Serial No. | Enterprise Cert Expiration Date | Hostname | System IP | Site ID | Mode | ... |
|-------|--------------|--|-------------------------|----------------------------|---------------------------------|-----------|---------------|---------|---------|-----|
| Idle | CSR1000v | CSR-44C7CE5A-4149-E696-C8A8-415C793FBF6C | Token -fc40de6570e72... | NA | NA | -- | -- | -- | CLI | ... |
| Idle | CSR1000v | CSR-D60B39FC-C583-BB55-7E9D-7CD085950D01 | Token -f28b5ab97898... | NA | NA | -- | -- | -- | CLI | ... |
| Idle | CSR1000v | CSR-834E400C-E358-8DE1-0E81-76E5984138F4 | Token -b89cae09c9... | NA | NA | -- | -- | -- | CLI | ... |
| Idle | CSR1000v | CSR-D405F5BA-B975-8944-D1A8-2E082AAE2A1D | Token -e78aaefc1eb02... | NA | NA | -- | -- | -- | CLI | ... |
| Idle | CSR1000v | CSR-D1837F36-6A1A-1850-C1C-E1069759FBA3 | Token -90ffd29997ff8... | NA | NA | -- | -- | -- | CLI | ... |
| Idle | CSR1000v | CSR-9E992295-1362-0B86-EF8-25C88F1CCCE | Token -1da14330e171... | NA | NA | -- | -- | -- | CLI | ... |
| Idle | CSR1000v | CSR-04F9482E-44F0-E40C-D30D-60C0906F73F2 | Token -4a6809836f02... | NA | NA | -- | -- | -- | vManage | ... |
| Idle | vEdge Cloud | e474c5f6-8ce7-d376-7cac-ba950b2c9159 | 7175AE0F | NA | NA | DC-vEdge1 | 10.255.255.11 | | | |
| Idle | vEdge Cloud | bcd4d0e-f2f1-fe75-866c-46996cda1c3 | 7DA60SF5 | NA | NA | DC-vEdge2 | 10.255.255.12 | | | |
| Idle | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2edff1609 | 297050DD | NA | NA | vEdge20 | 10.255.255.21 | | | |
| Idle | vEdge Cloud | d5de09f0-dc62-7766-510f-08496608608537d | 8BF04E65 | NA | NA | vEdge21 | 10.255.255.22 | | | |
| Idle | vEdge Cloud | 17026153-f09e-be4b-6dce-482fc4e43aab2 | 24715073 | NA | NA | vEdge30 | 10.255.255.31 | | | |
| Idle | CSR1000v | CSR-26217DA0-1B63-8DDE-11C9-125F527D3270 | Token -8dc7b557b60d... | NA | NA | -- | -- | -- | | |
| Idle | CSR1000v | CSR-F960E020-B7C9-887F-46A8-F45374B23E7D | Token -50cc04634ac4... | NA | NA | -- | -- | -- | | |
| Idle | CSR1000v | CSR-25925FBC-07F3-0732-E127-EA95D24F8EEB | Token -6ced66053d46... | NA | NA | -- | -- | -- | CLI | ... |



- Download the bootstrap file (will get saved to the Downloads folder by default). It should be a file beginning with CSR...

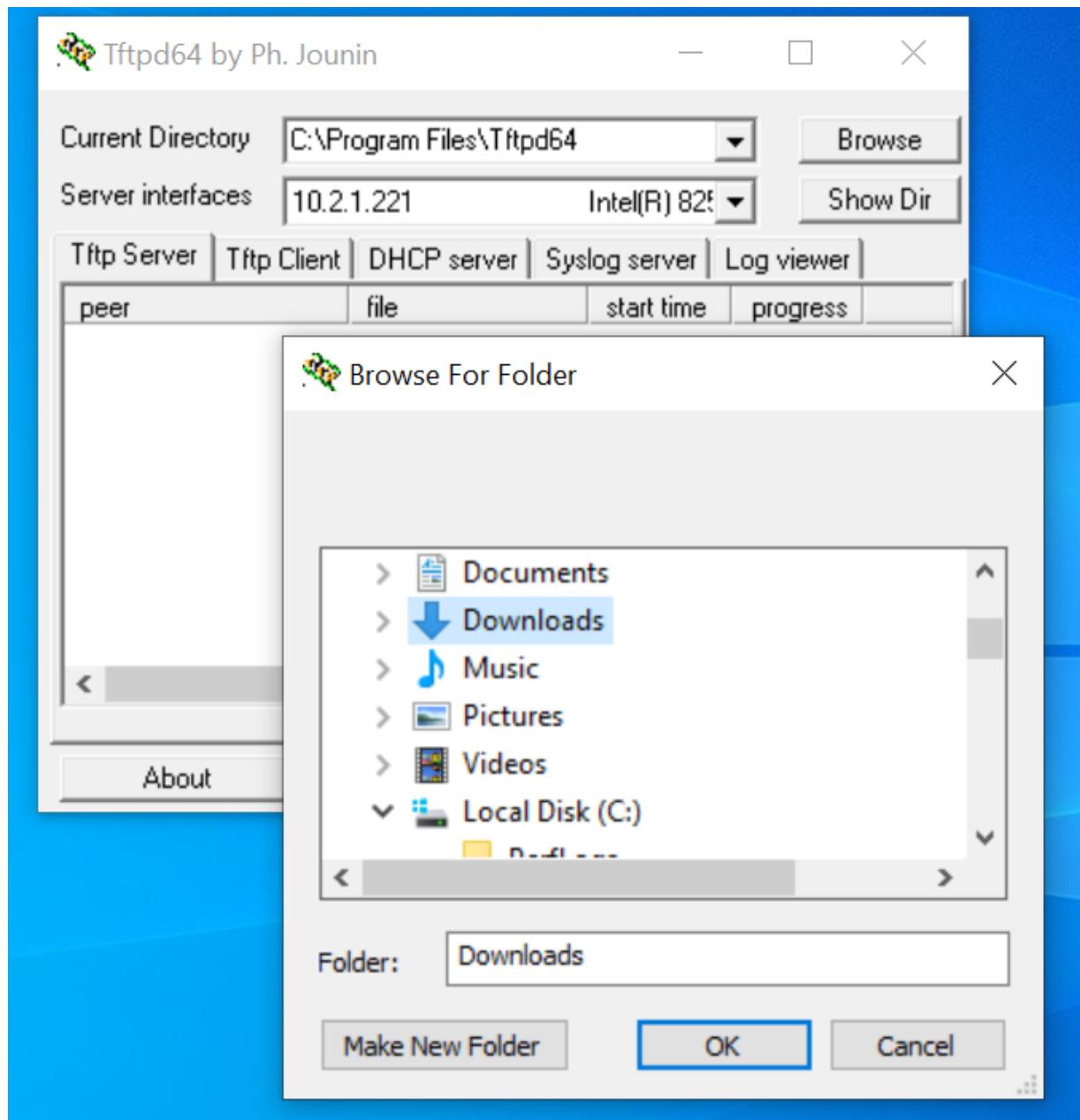


4. Rename this to *ciscosdwan_cloud_init.cfg*. Note that the name should match exactly as is enumerated here, else Bootstrapping will not work. If a file already exists with the same name, choose to overwrite.

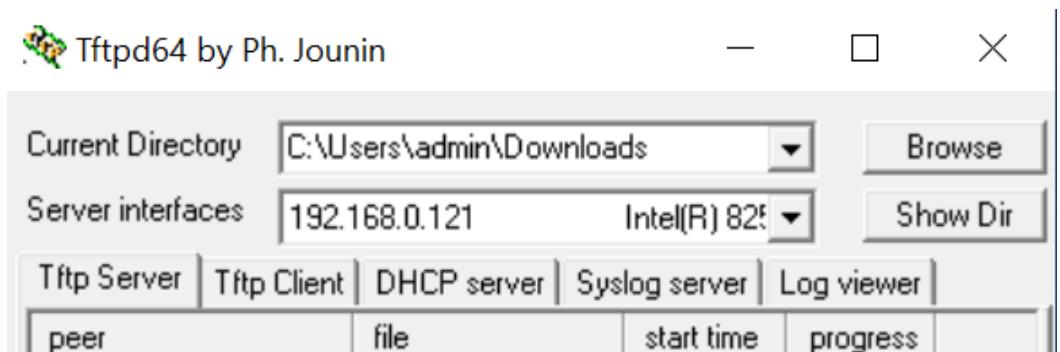


Tip: On bootup, a cEdge looks for a file on its USB port (if a bootable USB drive is connected) and in bootflash:. The file name must match as above for Cloud type devices (i.e. CSR1K). For physical devices, the file name should be *ciscosdwan.cfg*. If the file is present on the USB drive and in bootflash:, the one in bootflash: takes precedence

5. From the Jumphost Desktop, start TFTPD64. Click on Browse and choose the Downloads folder (or wherever the renamed .cfg file has been stored)



6. Choose the 192.168.0.X IP from the Server Interfaces drop down



7. Log in to the CLI of cEdge40 (we can log in via Putty now, using the saved session or by SSH'ing to 192.168.0.40) and issue `copy tftp: bootflash:`. Specify a Remote Host IP of your Jumphost (192.168.0.121 in this case). The source and destination file name should be *ciscosdwan_cloud_init.cfg*. The file should get copied over to bootflash: successfully

```
Router#copy tftp: bootflash:  
Address or name of remote host []? 192.168.0.121  
Source filename []? ciscosdwan_cloud_init.cfg  
Destination filename [ciscosdwan_cloud_init.cfg]?  
Accessing tftp://192.168.0.121/ciscosdwan_cloud_init.cfg...  
Loading ciscosdwan_cloud_init.cfg from 192.168.0.121 (via GigabitEthernet1): t  
[OK - 31186 bytes]  
  
31186 bytes copied in 0.037 secs (842865 bytes/sec)
```

```
copy tftp: bootflash:
```

8. Log in to the CLI of the vManage (again, via the saved Putty session or by SSH'ing to 192.168.0.6) and issue the following commands to SCP the ROOTCA.pem file over to cEdge40

```
192.168.0.6 - PuTTY
login as: admin
Pre-authentication banner message from server:
| viptela 20.1.1
|
|
End of banner message from server
admin@192.168.0.6's password:
Last login: Mon May 18 11:49:42 2020 from 192.168.0.121
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on vmanage
vmanage# vshell
vmanage:~$ scp ROOTCA.pem admin@192.168.0.40:ROOTCA.pem
The authenticity of host '192.168.0.40 (192.168.0.40)' can't be established.
RSA key fingerprint is SHA256:ZExBcf/5yRJqODy5DgaHUv8Hu8vMfhFMj1VPwGo6H/c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.40' (RSA) to the list of known hosts.
Password:
ROOTCA.pem
vmanage:~$
```

```
vshell
scp ROOTCA.pem admin@192.168.0.40:ROOTCA.pem
yes
admin
```

The last **admin** over there is the password of cEdge40

9. Go back to the CLI of cEdge40 and issue `controller-mode enable` from privilege mode. **Confirm** and this should lead to the device rebooting

```
Router#controller-mode enable
Enabling controller mode will erase the nvram filesystem, remove all configuration files, and reload the box!
Ensure the BOOT variable points to a valid image
Continue? [confirm]
Mode change success
```

```
controller-mode enable
```

We have completed this section of the lab and will now need to wait for the cEdge to reboot. On rebooting, it should pick up the configuration file from bootflash: and connect to the vManage/vSmarts/other vEdges. This will be verified in the next

section.

Task List

- [Verifying the current lab setup](#)
- [Creating the cEdge40 VM](#)
- [Onboarding cEdge40](#)
 - [Initial Configuration – non SD-WAN mode](#)
 - [Setting up Feature Templates](#)
 - [Creating and Attaching Device Templates](#)
 - [Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)
- [Onboarding Verification](#)

Onboarding Verification

1. On the vManage GUI, go to **Monitor => Network**. You should see the cEdge40 successfully added on vManage.

| Hostname | System IP | Device Model | Chassis Number/ID | State | Reachability | Site ID | BFD | Control | Version | Up Since | Device Groups | Connected vManage |
|-----------|---------------|---------------------|------------------------------------|-----------|--------------|---------|-----|----------------|-----------------------------|-------------|----------------|-------------------|
| vManage | 10.255.255.1 | vManage | dfeas63a5-66d2-c050-a07b-ec4ad4... | reachable | 1000 | — | 8 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | "10.255.255.1" | |
| vSmart | 10.255.255.3 | vSmart | 20607912-c0c8-4f46-a65f-5a547c... | reachable | 1000 | — | 8 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | "10.255.255.1" | |
| vSmart2 | 10.255.255.4 | vSmart | 7f332491-cb6f-4843-8bf5-060f90... | reachable | 1000 | — | 8 | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | "10.255.255.1" | |
| vBond | 10.255.255.2 | vEdge Cloud (vBo... | fc31c154-99c5-4267-971d-6c9ae7... | reachable | 1000 | — | — | 20.1.1 | 11 May 2020 11:02:00 AM PDT | "No groups" | "10.255.255.1" | |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b... | reachable | 1 | 4 | 3 | 20.1.1 | 14 May 2020 7:36:00 AM PDT | "No groups" | "10.255.255.1" | |
| DC-vEdge2 | 10.255.255.12 | vEdge Cloud | 0cdd40e-f2f1-fe75-866c-469966c... | reachable | 1 | 4 | 3 | 20.1.1 | 16 May 2020 12:24:00 PM PDT | "No groups" | "10.255.255.1" | |
| cEdge40 | 10.255.255.41 | CSR1000v | CSR-04F9482E-4AF0-E4DC-D30D... | reachable | 40 | 5 | 3 | 17.0.2.01 0.32 | 18 May 2020 9:14:00 AM PDT | "No groups" | "10.255.255.1" | |
| vEdge20 | 10.255.255.21 | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2ed... | reachable | 20 | 4 | 3 | 20.1.1 | 17 May 2020 5:27:00 AM PDT | "No groups" | "10.255.255.1" | |
| vEdge21 | 10.255.255.22 | vEdge Cloud | ddde90ff-cc62-77e6-510f-08d966... | reachable | 20 | 4 | 3 | 20.1.1 | 17 May 2020 10:52:00 PM PDT | "No groups" | "10.255.255.1" | |
| vEdge30 | 10.255.255.31 | vEdge Cloud | 17026153-f09e-be4b-6dce-482fce... | reachable | 30 | 5 | 3 | 20.1.1 | 18 May 2020 1:22:00 AM PDT | "No groups" | "10.255.255.1" | |

2. Click on cEdge40 and go to **Troubleshooting**. Select **Control Connections (Live View)** and we should see the cEdge has established control connections with vManage and the vSmarts

MONITOR Network > Troubleshooting > Control Connections(Live View)

Select Device cEdge40 | 10.255.255.41 Site ID: 40 Device Model: CSR1000v

vSmart Control Connections (Expected: 2 | Actual: 2)

vSmart 2/2 vManage 1/1

| Controller | Local Status | Remote Status |
|--|--------------|---------------|
| PUBLIC-INTERNET Circuit (Expected:2 Actual:2) NAT:Not learned | | |
| vSmart 10.255.255.3(Preferred Controller) | ✓ | ✓ |
| vSmart2 10.255.255.4(Preferred Controller) | ✓ | ✓ |
| vmanage 10.255.255.1(Preferred Controller) | ✓ | ✓ |

3. Navigate to Dashboards => Main Dashboard and we will see 4 Sites with Full WAN connectivity and 8 WAN Edges (or 6 WAN Edges, depending on the scenario chosen while requesting for these labs)

Cisco vManage

DASHBOARD | MAIN DASHBOARD

| Control Status (Total 8) | Site Health (Total 4) | Transport Interface Distribution |
|--------------------------|-------------------------------------|----------------------------------|
| Control Up | Full WAN Connectivity 4 sites | < 10 Mbps 22 |
| Partial | Partial WAN Connectivity 0 sites | 10 Mbps - 100 Mbps 0 |
| Control Down | No WAN Connectivity 0 sites | 100 Mbps - 500 Mbps 0 |
| | | > 500 Mbps 0 |

View Percent Utilization

WAN Edge Inventory

| Total | Authorized | Deployed | Staging |
|-------|------------|----------|---------|
| 20 | 20 | 6 | 0 |

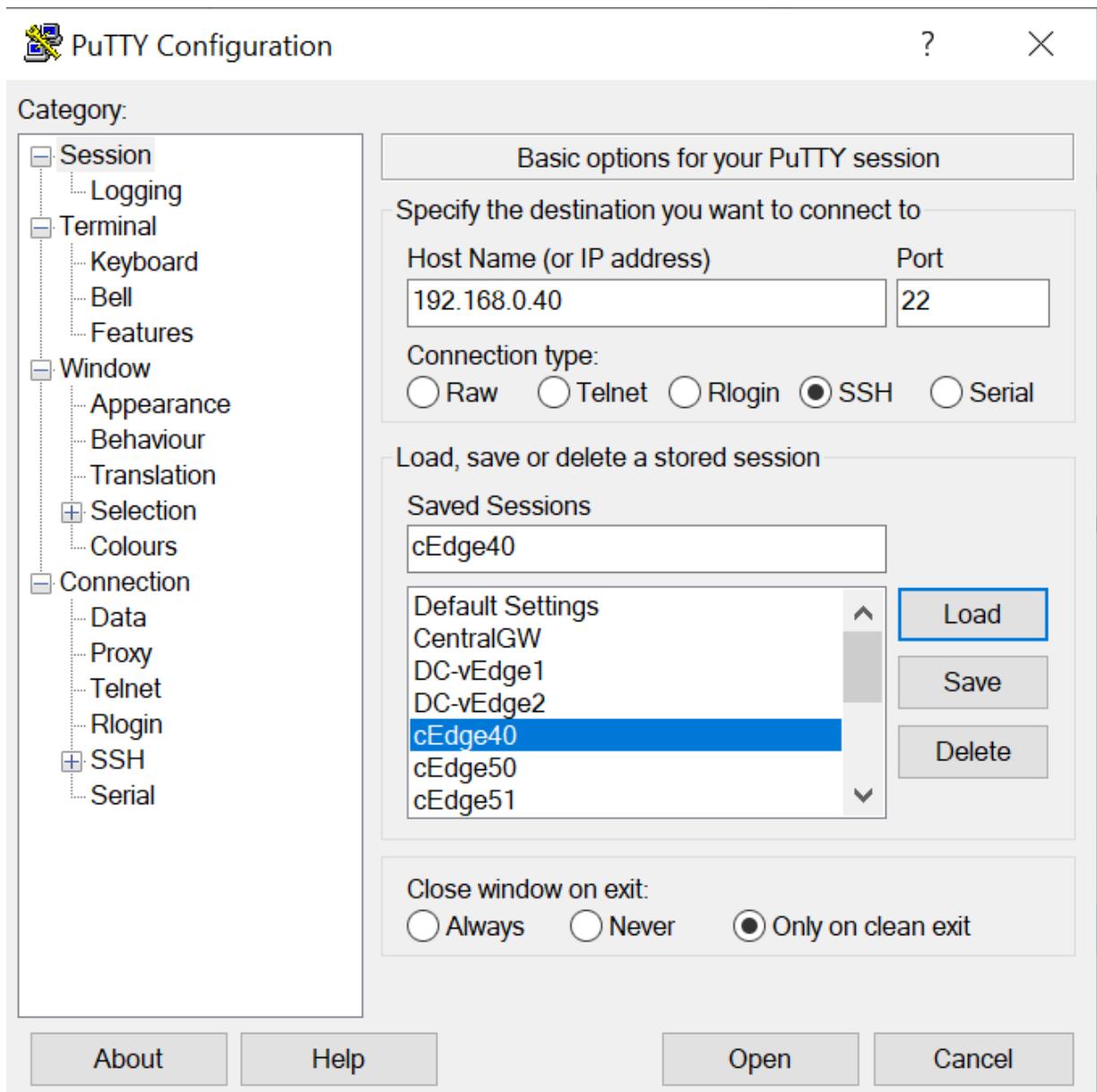
WAN Edge Health (Total 6)

| Normal | Warning | Error |
|--------|---------|-------|
| 6 | 0 | 0 |

Transport Health

Type: By Loss

4. Log in to the CLI of cEdge40 via Putty



5. Issue `show sdwan control connections` and we should see connections to the vSmarts and the vManage (same information that we saw on the GUI)

```

cEdge40# login as: admin
cEdge40# Keyboard-interactive authentication prompts from server:
! Password:
cEdge40# End of keyboard-interactive prompts from server

cEdge40#show sdwan control connections

CONTROLLER                                     PEER
PEER    PEER PEER      SITE      DOMAIN PEER      PEER
                                         GROUP
                                         ID      PRIVATE IP      PORT  PUBLIC IP      PUB
TYPE    PROT SYSTEM IP      ID      ID      PORT      LOCAL COLOR
OXY     STATE UPTIME      ID
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
vsmart  dtls 10.255.255.3   1000    1    100.100.100.4   12446 100.100.100.4   12446 public-interne
       up    0:00:18:38 0
vsmart  dtls 10.255.255.4   1000    1    100.100.100.5   12446 100.100.100.5   12446 public-interne
       up    0:00:18:38 0
vmanage dtls 10.255.255.1   1000    0    100.100.100.2   12446 100.100.100.2   12446 public-interne
       up    0:00:18:38 0
cEdge40#

```

```
show sdwan control connections
```

Tip: Inject `sdwan` in show commands that would normally be used on vEdges and they should work on cEdges.

6. On **Configuration => Devices** in the vManage GUI, you will notice that the cEdge is in vManage mode. This is because we have attached a Device Template to it. Changes to the cEdge can only be made from vManage now. We will be converting the rest of the devices (which are in **CLI** mode right now) to vManage mode over the course of the next few sections.

| State | Device Model | Chassis Number | Serial No./Token | Enterprise Cert Serial No. | Enterprise Cert Expiration Date | Hostname | System IP | Site ID | Mode | Assigned Template |
|-------------------|--------------|--------------------------------------|-------------------------|----------------------------|---------------------------------|-----------|---------------|---------|---------|--------------------------|
| Idle | CSR1000v | CSR-44C70CE5A-1419-E696-C8A8-415C... | Token: fc40de6570e72... | NA | NA | -- | -- | -- | CLI | -- |
| Idle | CSR1000v | CSR-D6D8B9F9C-C383-BB55-7E9D-7D... | Token: f2b85ab97998... | NA | NA | -- | -- | -- | CLI | -- |
| Idle | CSR1000v | CSR-834E40DC-E358-8DE1-0E81-76E59... | Token: b89caee09c9... | NA | NA | -- | -- | -- | CLI | -- |
| Idle | CSR1000v | CSR-D405F5BA-B975-8944-01A4-2E0B... | Token: e78aaef1ebd2... | NA | NA | -- | -- | -- | CLI | -- |
| Idle | CSR1000v | CSR-D1837F36-6A1A-1850-7C1C-EC6... | Token: 90ffd999ff8... | NA | NA | -- | -- | -- | CLI | -- |
| Idle | CSR1000v | CSR-5E992295-1362-0DB6-EEF9-25C... | Token: 1da14330e171... | NA | NA | -- | -- | -- | CLI | -- |
| Idle | CSR1000v | CSR-04F9482E-44F0-E4DC-030D-60C0... | 63201C50 | NA | NA | cEdge40 | 10.255.255.41 | 40 | vManage | cEdge_dualuplink_deve... |
| vEdge Cloud | | e74c5cf4-8ce1-d576-7ce8-ba950b291... | 7175AE0F | NA | NA | DC-vEdge1 | 10.255.255.11 | 1 | CLI | -- |

7. Issue `show sdwan control local-properties` on the CLI of cEdge40. Notice that the root-ca-chain-status is Installed and the certificate is installed and valid. The chassis-num is the same as what was referenced on vManage.

```
cEdge40# show sdwan control local-properties
personality vedge
sp-organization-name swat-sdwanlab
organization-name swat-sdwanlab
root-ca-chain-status Installed

certificate-status Installed
certificate-validity Valid
certificate-not-valid-before May 18 16:15:44 2020 GMT
certificate-not-valid-after May 16 16:15:44 2030 GMT

enterprise-cert-status Not-Applicable
enterprise-cert-validity Not Applicable
enterprise-cert-not-valid-before Not Applicable
enterprise-cert-not-valid-after Not Applicable

dns-name 100.100.100.3
site-id 40
domain-id 1
protocol dtls
tls-port 0
system-ip 10.255.255.41
chassis-num/unique-id CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2
serial-num 632UIC50
token Invalid

keygen-interval 1:00:00:00
retry-interval 0:00:00:15
no-activity-exp-interval 0:00:00:20
dns-cache-ttl 0:00:02:00
port-hopped FALSE
time-since-last-port-hop 0:00:00:00
embargo-check success
number-vbond-peers 0
number-active-wan-interfaces 1
```

8. We can also use `show sdwan certificate installed` to view the status of the installed certificates.

```
cEdge40#show sdwan certificate installed
Installed device certificates
-----
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 1663048784 (0x63201c50)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, CN=dfea3a5-66d2-4e50-a07b-ec4ad4a0b04e, O=Viptela
    Validity
      Not Before: May 18 16:15:44 2020 GMT
      Not After : May 16 16:15:44 2030 GMT
    Subject: C=US, ST=California, L=San Jose, OU=swat-sdwanlab, O=Viptela LLC, CN=vedge-CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2-1.viptela.com/emailAdd
ss=support@viptela.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
          Modulus:
            00:c4:1d:34:51:c8:3b:2f:0d:89:19:cc:26:bd:d4:
            f5:dd:64:0a:29:d6:17:90:8e:0d:38:64:81:40:91:
            7e:eb:e3:0d:36:59:da:36:71:d8:cc:2:3c:41:10:
            a5:77:7f:c3:2c:35:49:e7:a66:9d:ea:a9:01:ce:
            33:dc:93:1e:20:27:73:95:be:e8:1c:af:26:dc:09:
            0a:a2:4e:7f:64:ef:0c:f1:b4:3e:dc:61:3e:5:
            a3:43:80:d9:00:0f:e0:1c:4c:b3:48:cb:52:a4:c3:
            ea:7e:70:fa:8c:51:c7:15:8c:0c:45:e9:89:ae:3f:
            69:fd:cd:34:90:61:90:50:2c:68:fb:7:52:6d:e8:99:
```

9. To view the SDWAN specific running configuration on a cEdge device (other than the well known `show running-config`) use `show sdwan running-config`

```
cEdge40#show sdwan runn
cEdge40#show sdwan running-config
system
  system-ip          10.255.255.41
  overlay-id         1
  site-id            40
  port-offset        1
  control-session-pps 300
admin-tech-on-failure
  sp-organization-name swat-sdwanlab
  organization-name   swat-sdwanlab
port-hop
track-transport
track-default-gateway
  console-baud-rate 19200
  vbond 100.100.100.3 port 12346
!
```

We have completed onboarding verification

Task List

- [Verifying the current lab setup](#)
- [Creating the cEdge40 VM](#)
- [Onboarding cEdge40](#)
 - [Initial Configuration – non SD-WAN mode](#)
 - [Setting up Feature Templates](#)
 - [Creating and Attaching Device Templates](#)
 - [Copying the Bootstrap file and converting to SD-WAN IOS XE mode](#)
- [Onboarding Verification](#)



-->

Deploying Single Uplink cEdges

Summary: Deploying Site 50 - contains cEdges with single uplinks to each transport

Table of Contents

- [Creating the cEdge50 and cEdge51 VMs](#)
 - Overview
 - Deploying the VM on vCenter
- [Onboarding cEdge50 and cEdge51](#)
 - Initial Configuration - non SD-WAN mode
 - Copying and Modifying Feature Templates
 - Creating and Attaching Device Templates
 - Copying the Bootstrap file and converting to SD-WAN IOS-XE mode
- [Onboarding Verification](#)

! **Warning:** This section might already be done, depending on your selected Lab Scenario. The configuration given below can be used to review what was done to bring the Site up. If this VM is already deployed (check via vCenter), you **Do Not** need to perform these lab activities. Move to the [next section](#)

Task List

- Creating the cEdge50 and cEdge51 VMs
- Onboarding cEdge50 and cEdge51
 - Initial Configuration - non SD-WAN mode
 - Copying and modifying Feature Templates
 - Creating and Attaching Device Templates
 - Copying the Bootstrap file and converting to SD-WAN IOS-XE mode
- Onboarding Verification

⚠ Important: We will be deploying and onboarding cEdge50 and cEdge51 in parallel. Make sure that both VMs are deployed and operational, at the end of this activity. Screenshots will be concatenated into the same step for the two devices which means some steps will have to be repeated while going through the lab. Device specific variables in the Feature Templates will play an important role over here

Creating the cEdge50 and cEdge51 VMs

Overview

We will be deploying two cEdges in Site 50 via vCenter. cEdge 50 will have a single uplink (Internet), as will cEdge51 (MPLS). Make note of the following information for this section. The IP Addressing will not be used for some of the Network Adapters until later.

| SITE ID | SYSTEM ID | VM | Network Adapter | Network | Interface | IP | Gateway |
|---------------|---------------|--------------|-------------------|--------------|------------------|-------------------|---------------|
| 50 | 10.255.255.51 | cEdge50-podX | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.50/24 | 192.168.0.1 |
| | | | Network Adapter 2 | Internet | GigabitEthernet2 | 100.100.100.50/24 | 100.100.100.1 |
| | | | Network Adapter 3 | Site50-VPN10 | GigabitEthernet3 | 10.50.10.2/24 | |
| | | | Network Adapter 4 | Site50-VPN20 | GigabitEthernet4 | 10.50.20.2/24 | |
| | | | Network Adapter 5 | Site50-VPN30 | GigabitEthernet5 | 10.50.30.2/24 | |
| 10.255.255.52 | | cEdge51 | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.51/24 | 192.168.0.1 |

| | | | | | |
|--|-------------------|--------------|------------------|---------------|------------|
| | Network Adapter 2 | MPLS50 | GigabitEthernet2 | 192.1.2.22/30 | 192.1.2.21 |
| | Network Adapter 3 | Site50-VPN10 | GigabitEthernet3 | 10.50.10.3/24 | |
| | Network Adapter 4 | Site50-VPN20 | GigabitEthernet4 | 10.50.20.3/24 | |
| | Network Adapter 5 | Site50-VPN30 | GigabitEthernet5 | 10.50.30.3/24 | |

Tip: Plan your sites and addressing carefully. Proper planning can prevent a number of issues and will help with a successful, early deployment.

Tip: There is configuration applicable only to virtual vEdges/cEdges in some of the sections. Physical cEdges/vEdges are a lot easier to deploy, not only from a connectivity standpoint but also with respect to certificate exchange options.

Deploying the VM on vCenter

1. Click on the bookmark for vCenter or navigate to the following URL: <https://10.2.1.50/ui>. Log in with the credentials provided for your POD.

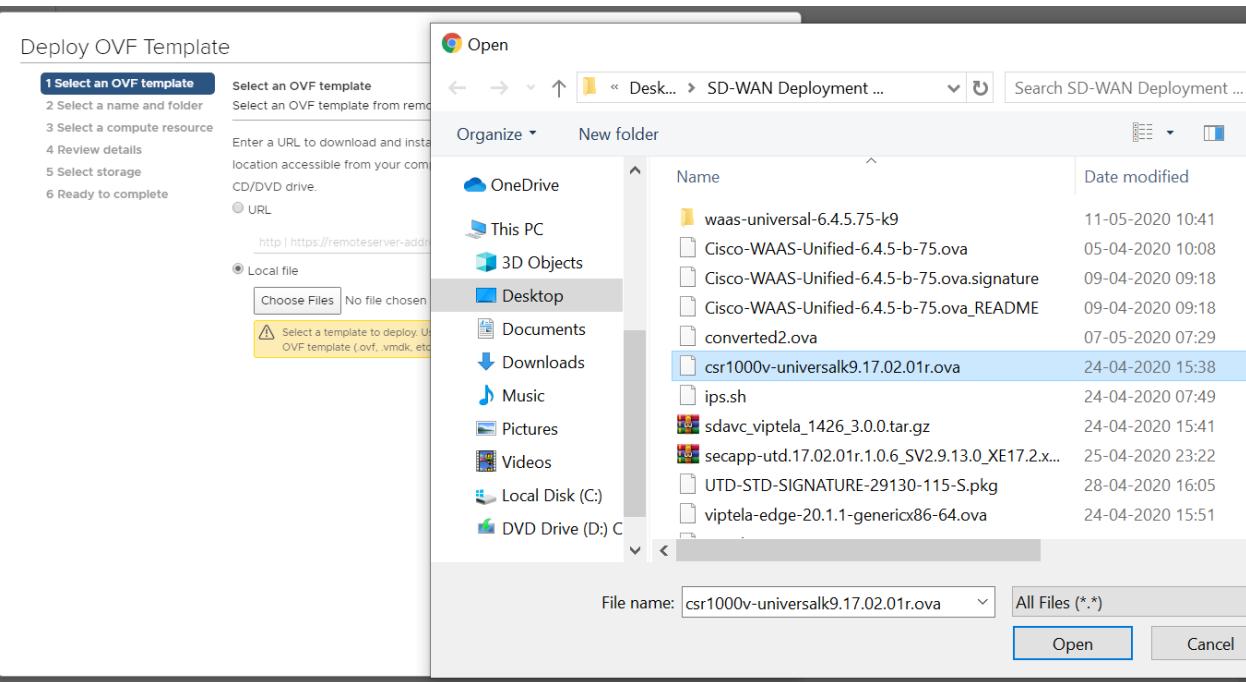


2. We should see the vEdges and cEdges from previous sections of the lab deployed.

3. Right click on the host and choose to **Deploy OVF Template**

A screenshot of the VMware vSphere host summary screen for 'vEdge30'. The left sidebar lists various hosts and resources. In the center, the host details are shown: Guest OS: Other 3.x Linux (64-bit), Compatibility: ESXi 5.0 and later (VM version 8), VMware Tools: Running, version:10277 (Guest Managed). The 'Deploy OVF Template...' option under the 'Actions' menu is highlighted with a red box. The right side shows CPU usage, memory, and network connections.

4. Choose the **Local file** option and click on **Choose files**. Navigate to the SD-WAN images folder and select the file beginning with *csr1000v-univer*. Click on Next.



5. Change the Virtual Machine name to **cEdge50-podX** or **cEdge51-podX**, depending on the VM being deployed and click on Next (where X is your POD number)

Note: We will only use the podX suffix over here to distinguish between different VMs in our Data Center. The rest of the guide will refer to these VMs as **cEdge50** and **cEdge51**.

Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

- ▽  ghi-vcenter.swat4partners.com
 - >  SWAT-Labs-GHI
 - >  slc-vcenter.swat4partners.com

CANCEL

BACK

NEXT

cEdge50

Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

- ▽  ghi-vcenter.swat4partners.com
 - >  SWAT-Labs-GHI
 - >  slc-vcenter.swat4partners.com

CANCEL

BACK

NEXT

cEdge51

6. Select the host assigned to you (image shown as an example only) and click on Next

>Note: If the screen gets stuck over here at **Validating** then close Chrome and open the vCenter in Internet Explorer, going through the same steps. Deployment should go through. This is a known issue with Google Chrome.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

- ▼ SWAT-Labs-GHI
 - ▼ Management-Shared Services
 - > ghi-ms01.swat4partners.com
 - > ghi-ms02.swat4partners.com
 - > ghi-ms03.swat4partners.com
 - > **ghi-ms04.swat4partners.com**
 - > GHI-Pod01
 - > GHI-Pod02
 - > GHI-Pod03
 - > GHI-Pod04
 - > GHI-Pod05
 - > GHI-Pod06
 - > GHI-Pod07
 - > GHI-Pod08
 - > GHI-Pod09
 - > GHI-Pod10

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

7. Review the details shown and click on Next. Select the **Small** option (1 vCPU and 4 GB RAM) and click on Next

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource

Review details
Verify the template details.

4 Review details

- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

| | |
|---------------|---------------------------------------|
| Publisher | No certificate present |
| Product | Cisco CSR 1000V Cloud Services Router |
| Version | 17.02.01r |
| Vendor | Cisco Systems, Inc. |
| Download size | 510.2 MB |
| Size on disk | 788.9 MB (thin provisioned) |
| | 8.5 GB (thick provisioned) |

CANCEL

BACK

NEXT

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details

5 Configuration

- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Configuration
Select a deployment configuration

| | |
|--|---|
| <input checked="" type="radio"/> Small | Description Minimal hardware profile - 1 vCPU, 4 GB RAM |
| <input type="radio"/> Medium | |
| <input type="radio"/> Large | |
| <input type="radio"/> Large + DRAM Upgrade | |
| 4 Items | |

CANCEL

BACK

NEXT

8. Choose the Datastore and click on Next.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select storage
Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format:

Thick Provision Lazy Zeroed

VM Storage Policy:

Datastore Default

| Name | Capacity | Provisioned | Free | T |
|-------------|----------|-------------|----------|---|
| ghi-ms04-ds | 11.63 TB | 1.1 TB | 10.99 TB | V |

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

9. Populate the VM Networks as per the image given below

⚠ Important: Please make sure that these look exactly as shown below

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 **Select a name and folder**
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Configuration
- ✓ 6 Select storage
- 7 Select networks**

8 Customize template

9 Ready to complete

Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|------------------|---------------------|
| GigabitEthernet1 | Management |
| GigabitEthernet2 | Internet |
| GigabitEthernet3 | Site50-VPN10 |

3 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

Networks for cEdge50

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Configuration
- ✓ 6 Select storage
- 7 Select networks**

8 Customize template

9 Ready to complete

Select networks
Select a destination network for each source network.

| Source Network | Destination Network |
|------------------|---------------------|
| GigabitEthernet1 | Management |
| GigabitEthernet2 | MPLS50 |
| GigabitEthernet3 | Site50-VPN10 |

3 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

Networks for cEdge51

10. Click Next on **Customize Template** and then Click on **Finish** to deploy your cEdge50-podX and cEdge51-podX VM

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details**
- ✓ 5 Configuration
- ✓ 6 Select storage
- ✓ 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template
Customize the deployment properties of this software solution.

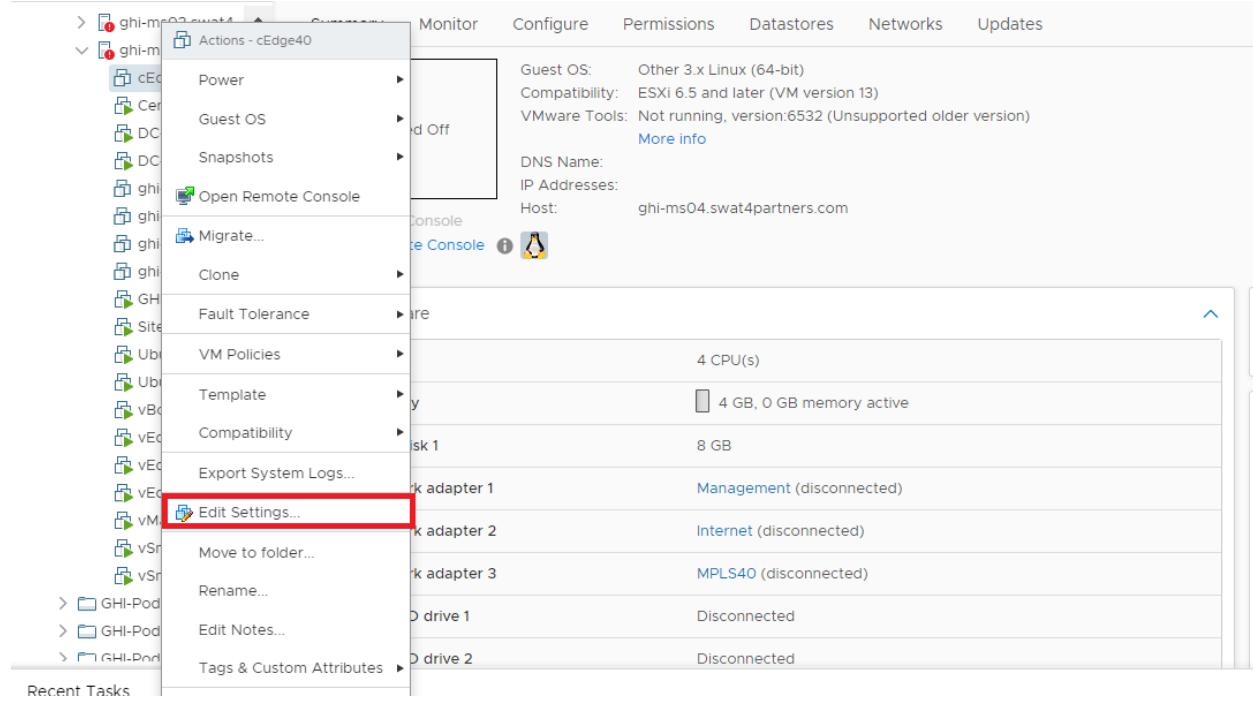
All properties have valid values

1. Bootstrap Properties 13 settings

| | |
|----------------|--|
| Router Name | Hostname of this router |
| Login Username | Username for remote login |
| Login Password | Password for remote login. WARNING: While this password will be stored securely within IOS, the plain-text password will be recoverable from the OVF descriptor file. |
| Password | _____ |
| Confirm | _____ |
| Password | _____ |
| Domain Name | Network domain name (such as "cisco.com") |

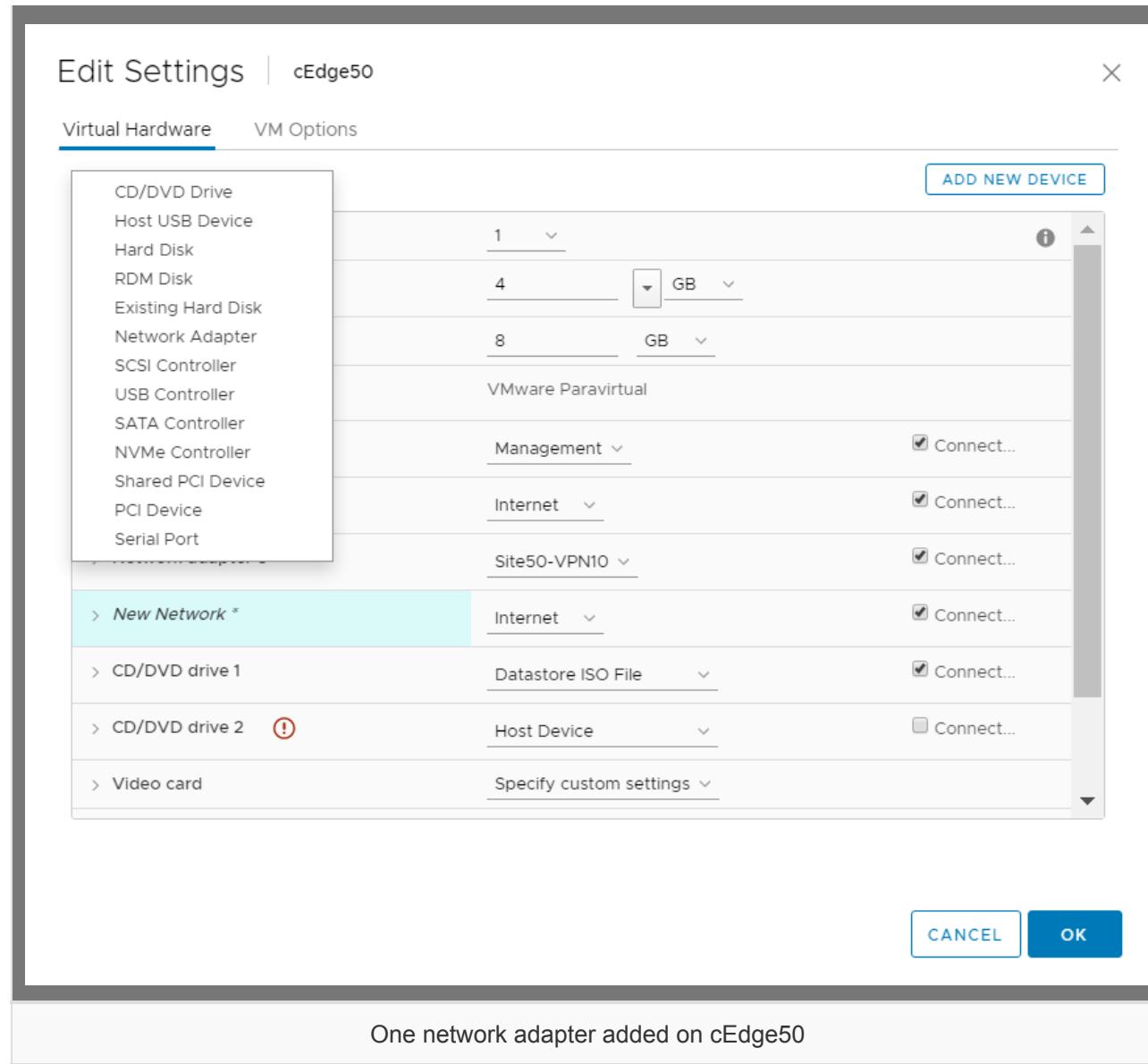
CANCEL **BACK** **NEXT**

11. Once the VM is deployed, right click **cEdge50-podX** and/or **cEdge51-podX** and click Edit settings (image shown as reference only).



12. Click on **Add New Device** (top right corner) and select Network Adapter to add one (since our deployed VM has only 3 Network Adapters but we will need 5 for our lab). Repeat this step for a total of 5 Network Adapters. This will need to be done for each VM (cEdge50-podX and cEdge51-podX)





13. After adding two new network adapters from the previous step, click on the drop down next to the first **New Network** in the list of Network Adapters and click on *Browse*
14. Choose the **Site50-VPN20** Network and click on OK. Do the same for the next network adapter, allocating it to **Site50-VPN30**. Make sure the Network Adapters match with the images below and click on OK again

⚠ Warning: The Network Adapter mapping might vary based on the version of cEdge being deployed. Sometimes, trial and error is the easiest way to figure out which Network Adapter maps to which interface on the cEdge

Edit Settings | cEdge50

[Virtual Hardware](#) [VM Options](#)

[ADD NEW DEVICE](#)

| | | |
|---------------------|--------------------|--------------|
| > CPU | 1 | ▼ |
| > Memory | 4 | ▼ GB ▼ |
| > Hard disk 1 | 8 | GB ▼ |
| > SCSI controller 0 | VMware Paravirtual | |
| > Network adapter 1 | Management | ✓ Connect... |
| > Network adapter 2 | Internet | ✓ Connect... |
| > Network adapter 3 | Site50-VPN10 | ✓ Connect... |
| > New Network * | Site50-VPN20 | ✓ Connect... |
| > New Network * | Site50-VPN30 | ✓ Connect... |
| > CD/DVD drive 1 | Datastore ISO File | ✓ Connect... |
| > CD/DVD drive 2 | Host Device | ✗ Connect... |

[CANCEL](#) [OK](#)

Networks on cEdge50

Edit Settings | cEdge51

X

Virtual Hardware VM Options

ADD NEW DEVICE

| | | |
|---------------------|--------------------|--|
| > CPU | 1 | v |
| > Memory | 4 | GB v |
| > Hard disk 1 | 8 | GB v |
| > SCSI controller 0 | VMware Paravirtual | |
| > Network adapter 1 | Management | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 2 | MPLS50 | <input checked="" type="checkbox"/> Connect... |
| > Network adapter 3 | Site50-VPN10 | <input checked="" type="checkbox"/> Connect... |
| > New Network * | Site50-VPN20 | <input checked="" type="checkbox"/> Connect... |
| > New Network * | Site50-VPN30 | <input checked="" type="checkbox"/> Connect... |
| > CD/DVD drive 1 | Datastore ISO File | <input checked="" type="checkbox"/> Connect... |
| > CD/DVD drive 2 | Host Device | <input type="checkbox"/> Connect... |

CANCEL

OK

Networks on cEdge51

15. Click on cEdge50-podX and/or cEdge51-podX and choose to power them on. Console in to the devices as well, for the next section. Wait for the cEdges to boot up completely

Power On | **Console** | **ACTIONS**

cEdge51

Summary Monitor Configure Permissions Datastores Networks Updates

Guest OS: Other 3.x Linux (64-bit)
Compatibility: ESXi 6.5 and later (VM version 13)
VMware Tools: Not running, version:6532 (Unsupported older version)
[More info](#)

DNS Name:
IP Addresses:
Host: ghi-ms04.swat4partners.com

[Launch Web Console](#) [Launch Remote Console](#)

VM Hardware

| | |
|---------------------|--------------------------|
| > CPU | 1 CPU(s) |
| > Memory | 4 GB, 0 GB memory active |
| > Hard disk 1 | 8 GB |
| > Network adapter 1 | Management (connected) |
| > Network adapter 2 | MPLS50 (connected) |
| > Network adapter 3 | Site50-VPN10 (connected) |

Recent Tasks Alarms

Task List

- [Creating the cEdge50 and cEdge51 VMs](#)
- [Onboarding cEdge50 and cEdge51](#)
 - Initial Configuration - non SD-WAN mode
 - Copying and modifying Feature Templates
 - Creating and Attaching Device Templates
 - Copying the Bootstrap file and converting to SD-WAN IOS-XE mode
- [Onboarding Verification](#)

Onboarding cEdge50 and cEdge51

Initial Configuration - non SD-WAN mode

Use the following information in this section (some of the information will be used later)

| SITE ID | SYSTEM ID | VM | Network Adapter | Network | Interface | IP | Gateway |
|---------------|---------------|---------|--------------------|--------------|------------------|-------------------|---------------|
| 50 | 10.255.255.51 | cEdge50 | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.50/24 | 192.168.0.1 |
| | | | | Internet | GigabitEthernet2 | 100.100.100.50/24 | 100.100.100.1 |
| | | | | Site50-VPN10 | GigabitEthernet3 | 10.50.10.2/24 | |
| | | | | Site50-VPN20 | GigabitEthernet4 | 10.50.20.2/24 | |
| | | | | Site50-VPN30 | GigabitEthernet5 | 10.50.30.2/24 | |
| 10.255.255.52 | 10.255.255.52 | cEdge51 | Network Adapter 1 | Management | GigabitEthernet1 | 192.168.0.51/24 | 192.168.0.1 |
| | | | | MPLS50 | GigabitEthernet2 | 192.1.2.22/30 | 192.1.2.21 |
| | | | | Site50-VPN10 | GigabitEthernet3 | 10.50.10.3/24 | |
| | | | | Site50-VPN20 | GigabitEthernet4 | 10.50.20.3/24 | |
| | | | | Site50-VPN30 | GigabitEthernet5 | 10.50.30.3/24 | |

Tip: Starting from IOS-XE 17.2, the cEdge platforms use a Universal image. One can switch from non SD-WAN mode to SD-WAN mode via a command

1. We will first console in to the cEdges and set up an IP Address with basic routing to ensure that cEdge50 and cEdge51 can reach vManage and the Jumphost. This is done by issuing `ip route 0.0.0.0 0.0.0.0 192.168.0.1` followed by `interface GigabitEthernet1` and giving an IP Address to the interface through `ip address 192.168.0.50 255.255.255.0` for cEdge50 and `ip address 192.168.0.51 255.255.255.0` for cEdge51. Make sure you `no shut` the interface.

Additionally, we will be SCP'ing files over to the cEdges (root certificates) from vManage

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int gig1
Router(config-if)#ip add 192.168.0.50 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
Router(config)#
*May 18 20:16:03.198: %LINK-3-UPDOWN: Interface GigabitEthernet1, changed state
to up
*May 18 20:16:04.202: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1, changed state to up
Router(config)#username admin priv 15 sec admin
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#ip scp server enable
Router(config)#
Router(config)#
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
```

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig1
Router(config-if)#ip add 192.168.0.51
% Incomplete command.

Router(config-if)#ip add 192.168.0.51 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.0
*May 18 20:17:32.431: %LINK-3-UPDOWN: Interface GigabitEthernet1, changed state
to up
*May 18 20:17:33.435: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1, changed state to up.1
Router(config)#username admin priv 15 sec admin
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#ip scp server enable
Router(config)#do wr
Building configuration...
[OK]
Router(config)#

```

Configuration for cEdge50

```
enable
conf t
interface GigabitEthernet1
 ip address 192.168.0.50 255.255.255.0
 no shut
 exit
ip route 0.0.0.0 0.0.0.0 192.168.0.1
ip scp server enable
username admin priv 15 sec admin
line vty 0 4
 login local
 do wr
```

Configuration for cEdge51

```
enable
conf t
interface GigabitEthernet1
 ip address 192.168.0.51 255.255.255.0
 no shut
 exit
ip route 0.0.0.0 0.0.0.0 192.168.0.1
```

```
ip scp server enable
username admin priv 15 sec admin
line vty 0 4
login local
do wr
```

2. Verify connectivity to the vManage and the JumpHost (IP of the Jumphost might vary) by pinging **192.168.0.6** and/or the IP Address of your Jumphost from the console session of both devices

Task List

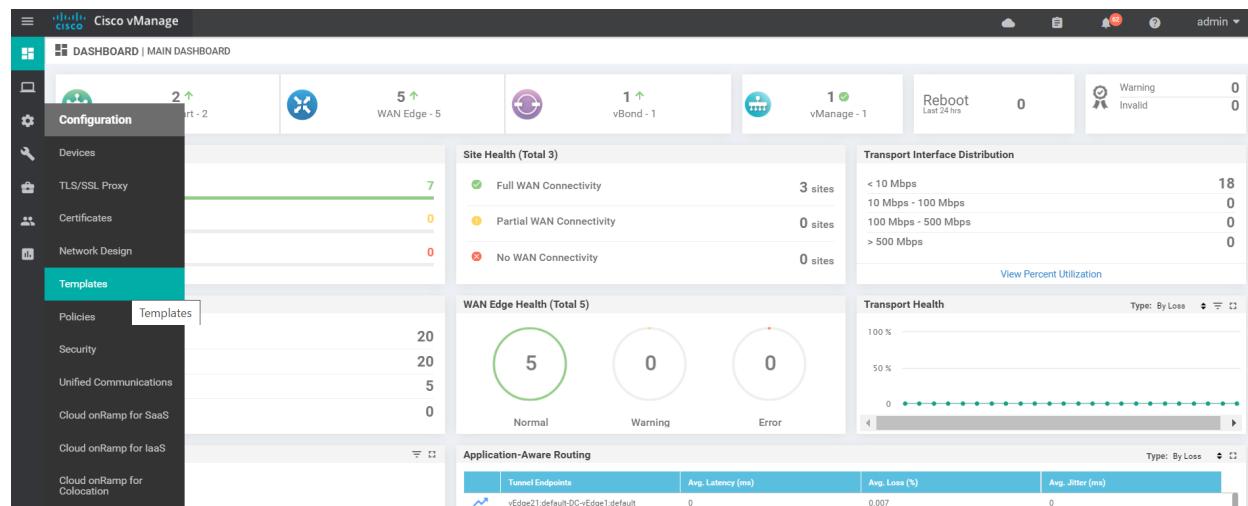
- Creating the cEdge50 and cEdge51 VMs
 - Onboarding cEdge50 and cEdge51
 - Initial Configuration – non SD-WAN mode
 - Copying and modifying Feature Templates
 - Creating and Attaching Device Templates
 - Copying the Bootstrap file and converting to SD-WAN IOS-XE mode
 - Onboarding Verification

Note: The Feature and Device Templates enumerated here and in the next section might already be created for you. However, it is a good practice to go through the steps below and validate the settings in the templates. This will help in familiarization with the lab setup and with fixing any deltas that might exist. If you don't see them in the configuration, please add the templates and follow the steps as enumerated below.

Templates are the key configuration components of the Cisco SD-WAN solution. They help with deploying large scale solutions with minimal effort. While there is quite a lot of initial configuration that goes into setting up these templates, their usefulness is highlighted when we're looking at onboarding multiple devices in a quick and efficient manner, reusing generic templates for devices.

We will make use of the templates that were created for cEdge40, repurposing them for cEdge50 and cEdge51 through the use of Device Specific parameters.

1. On the vManage GUI, navigate to **Configuration** (the cog wheel icon on the left) => **Templates**



2. Click on the Feature tab to access the Feature templates. Click on the three dots next to the **cEdge_VPN0_dual_uplink** template and click on **Copy**

The screenshot shows the Cisco vManage interface under Configuration | Templates. A table lists four templates. The fourth template, 'cEdge_VPN0_dual_uplink', has a context menu open over it. The menu includes options like View, Edit, Change Device Models, Delete, and Copy. The 'Copy' option is specifically highlighted with a red box.

3. Rename the template to **cEdge_VPN0_single_uplink** and change the description to **cEdge VPN 0 Template for Single Uplinks**. Click on **Copy**. Click on the 3 dots next to the newly copied template and click on **Edit**. The name, description and VPN should be as shown below

The screenshot shows the Cisco vManage interface under Configuration | Templates. A specific template named 'cEdge_VPN0_single_uplink' is selected. In the 'Basic Configuration' tab, the 'Template Name' is set to 'cEdge_VPN0_single_uplink' and the 'Description' is set to 'cEdge VPN 0 Template for Single Uplinks'. In the 'VPN' section, there is a route entry with a green pencil icon, which is highlighted with a red box.

4. Navigate to the **IPv4 Route** section. A route should be populated there. Click on the pencil icon to edit the route and click on **1 next hop**. Make sure the next hop is a Device Variable named **vpn0_next_hop_ip_address_0** (should already be the case, from our previous use of the parameter).

The screenshot shows the Cisco vManage interface under Configuration | IPv4 Route. A new route is being created, indicated by a green pencil icon. The 'Action' column for the first route entry has a red box highlighting the edit icon.

Update IPv4 Route

| | | |
|---|---|---|
| Prefix | <input type="text" value="0.0.0.0/0"/> | <input type="checkbox"/> Mark as Optional Row i |
| Gateway | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN <input type="radio"/> DHCP | |
| Next Hop | 1 Next Hop | |
| Save Changes Cancel | | |

5. Click on **Update** in the lower portion of the screen to update the changes
6. On the Feature Template page, click on the three dots next to *cedge-vpn0-int-dual* and click on **Copy**. Enter the Template Name as *cedge-vpn0-int-single* and a description of *cEdge VPN 0 Interface Template for devices with a single uplink*. Click on **Copy**

CONFIGURATION | TEMPLATES

Device Feature [Add Template](#)

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By |
|--------------------------|-------------------------------------|---------------------|--------------|------------------|------------------|------------|
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Templ... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin |
| cEdge_VPN0_dual_uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | | | | admin |
| cEdge_VPN512_dual_uplink | cEdge VPN 512 Template for Dual ... | Cisco VPN | | | | admin |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template f... | Cisco VPN | | | | admin |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single ... | Cisco VPN | | | | admin |

Template Copy

Template Name:

Description:

[Copy](#) [Cancel](#)

7. Click on the three dots next to the newly copied template and choose to **Edit** it. Verify the Template Name and Description and update parameters as per the following table

| Section | Field | Global or Device Specific (drop down) | Value |
|---------|-------|---------------------------------------|-------|
| | | | |

| | | | |
|----------------------------|------------------------------|-----------------|--|
| | Template Name | NA | <i>cedge-vpn0-int-single</i> |
| | Description | NA | <i>cEdge VPN 0 Interface Template for devices with a single uplink</i> |
| Basic Configuration | Interface Name | Device Specific | <i>vpn0_if_name</i> |
| Basic Configuration - IPv4 | IPv4 Address / prefix-length | Device Specific | <i>vpn0_ipv4_address</i> |
| Tunnel | Tunnel Interface | Global | On |
| Tunnel | Color | Device Specific | <i>vpn0_if_tunnel_color_value</i> |
| Tunnel | Restrict | Device Specific | <i>vpn0_if_tunnel_color_restrict</i> |
| Tunnel - Allow Service | All | Global | On |

Device Type: CSR1000v

| | |
|---------------|--|
| Template Name | <i>cedge-vpn0-int-single</i> |
| Description | <i>cEdge VPN 0 Interface Template for devices with a single uplink</i> |

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP Advanced

BASIC CONFIGURATION

| | |
|----------------|---|
| Shutdown | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Interface Name | <input type="text"/> [vpn0_if_name] |
| Description | <input type="text"/> |

IPv4 IPv6

IPv4 Address/ prefix-length

Secondary IP Address (Maximum: 4) [Add](#)

DHCP Helper

Block Non Source IP

Bandwidth Upstream

Bandwidth Downstream

TUNNEL

Tunnel Interface [On](#) [Off](#)

Per-tunnel Qos [On](#) [Off](#)

Color [\[vpn0_if_tunnel_color_value\]](#)

Restrict [On](#) [Off](#) [\[vpn0_if_tunnel_color_restrict\]](#) [\[vpn0_if_tunnel_color_restrict\]](#)

8. Make copies of the following templates, renaming the template name and description as shown below. No changes need to be made to the newly copied templates

| Template to be copied | Copied Template Name | Copied Template Description |
|--------------------------|----------------------------|---|
| cEdge_VPN512_dual_uplink | cEdge_VPN512_single_uplink | cEdge VPN 512 Template for Single Uplinks |
| cedge-vpn512-int-dual | cedge-vpn512-int-single | cEdge VPN 512 Interface Template for devices with a Single uplink |

We are done with creating feature templates for the initial onboarding of cEdge50 and cEdge51. Notice, this was less work than before since we could simply copy the template already created for cEdge40.

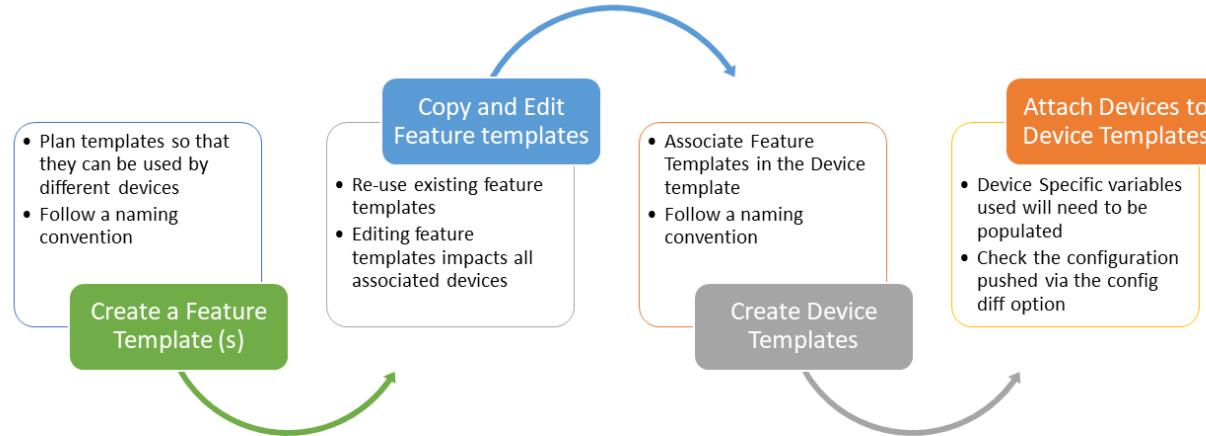
Task List

- [Creating the cEdge50 and cEdge51 VMs](#)
- [Onboarding cEdge50 and cEdge51](#)

- [Initial Configuration – non SD-WAN mode](#)
- [Copying and modifying Feature Templates](#)
- [Creating and Attaching Device Templates](#)
- [Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)
- [Onboarding Verification](#)

Creating and Attaching Device Templates

The feature templates created in the previous sections are referenced in Device Templates. Devices are then attached to Device Templates which pushes configuration to them, in line with the settings in the Feature templates. The general workflow for templates is given below



1. Go to **Configuration => Templates** and click on the three dots next to the Device Template named `cEdge_dualuplink_devtemp`. Click on **Copy**

The screenshot shows the 'CONFIGURATION | TEMPLATES' section. At the top, there are tabs for 'Device' and 'Feature', and a 'Create Template' button. Below is a search bar with 'Template Type: Non-Default' and a search icon. The main area displays a table with columns: Name, Description, Type, Device Model, Feature Templates, Devices Attached, Updated By, Last Updated, and Template Status. One row is visible: 'cEdge_dualuplink_devtemp' (cEdge Device Template for de...), Type: Feature, Device Model: CSR1000v, Feature Templates: 11, Devices Attached: 1, Updated By: admin, Last Updated: 18 May 2020 8:43:52 AM PDT, Template Status: In Sync. To the right of the table is a context menu with options: Edit, View, Delete, Copy (which is highlighted with a red box), Attach Devices, Detach Devices, Export CSV, and Change Device Values.

2. Change the template name to **cEdge-single-uplink** and the description to *Single Uplink cEdge Device Template*. Click on **Copy**

Template Copy

Template Name
cEdge-single-uplink

Description
Single Uplink cEdge Device Template

Copy **Cancel**

3. Click on the three dots next to the newly copied template and choose to **Edit** it. Make sure the details under **Transport and Management VPN** are populated as below, updating VPN0 and VPN0 Interface templates with the ones we just created. Click on **Update** once done

Tip: You can create templates on the fly if the template hasn't already been created. This can be done via the [Create Template](#) hyperlink from the drop down menu

Important: To get the option of selecting a **Cisco VPN Interface Ethernet** as shown below, click on **Cisco VPN Interface Ethernet** on the right hand side under the **Additional Templates** portion of the screen. This applies to both the VPN 0 and the VPN 512 sections

| Section | Field | Sub Field | Value (Drop Down) |
|------------------------------|---------------|------------------------------|----------------------------|
| Transport and Management VPN | Cisco VPN 0 | | cEdge_VPN0_single_uplink |
| Transport and Management VPN | Cisco VPN 0 | Cisco VPN Interface Ethernet | cedge-vpn0-int-single |
| Transport and Management VPN | Cisco VPN 512 | | cEdge_VPN512_single_uplink |
| Transport and Management VPN | Cisco VPN 512 | Cisco VPN Interface Ethernet | cedge-vpn512-int-single |

Transport & Management VPN

| | | |
|------------------------------|----------------------------|--|
| Cisco VPN 0 * | cEdge_VPN0_single_uplink | Additional Cisco VPN 0 Templates |
| Cisco VPN Interface Ethernet | cedge-vpn0-int-single | <ul style="list-style-type: none"> Cisco BGP Cisco OSPF Cisco Secure Internet Gateway Cisco VPN Interface Ethernet Cisco VPN Interface GRE Cisco VPN Interface IPsec VPN Interface Ethernet PPPoE |
| Cisco VPN 512 * | cEdge_VPN512_single_uplink | Additional Cisco VPN 512 Templates |
| Cisco VPN Interface Ethernet | cedge-vpn512-int-single | <ul style="list-style-type: none"> Cisco VPN Interface Ethernet |

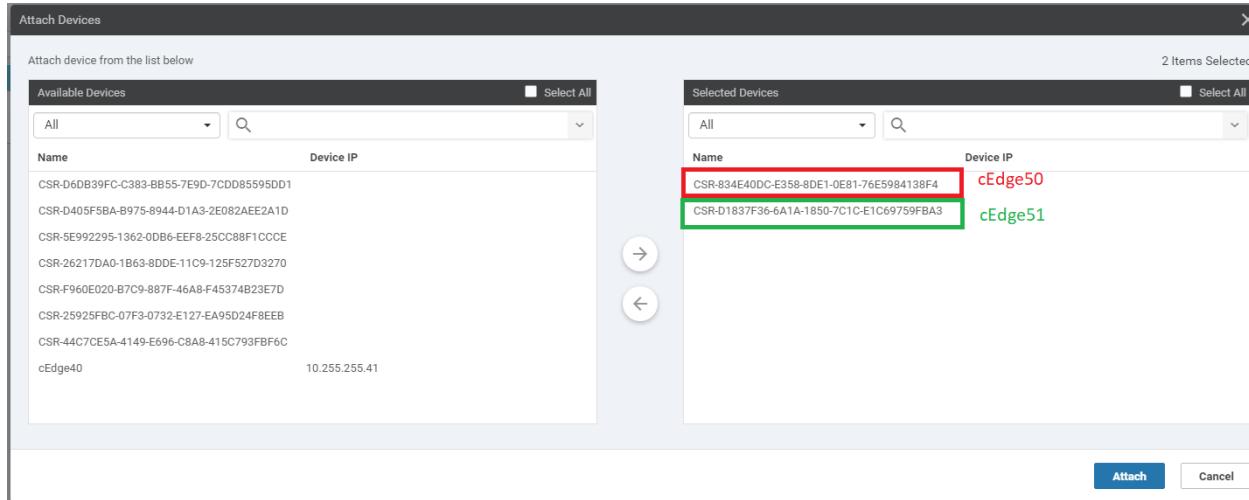
4. Once created, the Device Template will need to be attached to a Device for it to take effect. Click on the three dots (right-hand side) of the *cEdge-single-uplink* template and click on **Attach Devices**

The screenshot shows a table of device templates. The second row, labeled 'cEdge-single-uplink', has a '...' button on its right side. A context menu is open over this button, with the 'Attach Devices' option highlighted by a red circle.

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | ... |
|--------------------------|----------------------------------|---------|--------------|-------------------|------------------|------------|----------------------------|-----------------|-----|
| cEdge_dualuplink_devtemp | cEdge Device Template for de... | Feature | CSR1000v | 11 | 1 | admin | 18 May 2020 8:43:52 AM PDT | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 0 | admin | 18 May 2020 1:33:13 PM PDT | In Sync | ... |

5. We will be presented with a list of devices that can be associated with this template. Choose any two available devices that have not been attached to a template before, making note of the Name (e.g. the device with a name

ending in **38F4** has been selected for cEdge50 and the one ending in **FBA3** has been selected for cEdge51). Click on **Attach**



6. This should take you to a page which shows the attached devices. Click on the three dots (right-hand side) next to the cEdge50 Device (whatever name was selected before) and click on **Edit Device Template**. Also, make note of the cross mark next to the device name, on the left-hand side. This is the point where we need to enter details for the device specific values populated in the Feature Templates.
7. Enter details as per the screenshot below (these can be found in the table referenced at the beginning of this page) and click on **Update**. Once all the data is entered correctly, there should be a green check mark next to the corresponding device



Update Device Template

Variable List (Hover over each field for more information)

| | |
|---|--|
| Chassis Number | CSR-834E40DC-E358-8DE1-0E81-76E5984138F4 |
| System IP | - |
| Hostname | - |
| Address(vpn512_next_hop_ip_address_0) | 192.168.0.1 |
| IPv4 Address/ prefix-length(vpn512_mgmt_ipv4_address) | 192.168.0.50/24 |
| Address(vpn0_next_hop_ip_address_0) | 100.100.100.1 |
| Interface Name(vpn0_if_name) | GigabitEthernet2 |
| IPv4 Address/ prefix-length(vpn0_ipv4_address) | 100.100.100.50/24 |
| Color(vpn0_if_tunnel_color_value) | public-internet |
| Restrict(vpn0_if_tunnel_color_restrict) | <input type="checkbox"/> |
| Hostname(host-name) | cEdge50 |
| System IP(system-ip) | 10.255.255.51 |
| Site ID(site-id) | 50 |

Generate Password **Update** **Cancel**

Details to be entered for cEdge50

Note: We have selected a color for our Tunnel over here. Other devices have tunnels with the default color as of now. When we bring them into vManage mode, a color will be set on them as well

Update Device Template

Variable List (Hover over each field for more information)

| | |
|---|--|
| Chassis Number | CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3 |
| System IP | - |
| Hostname | - |
| Address(vpn512_next_hop_ip_address_0) | 192.168.0.1 |
| IPv4 Address/ prefix-length(vpn512_mgmt_ipv4_address) | 192.168.0.51/24 |
| Address(vpn0_next_hop_ip_address_0) | 192.1.2.21 |
| Interface Name(vpn0_if_name) | GigabitEthernet2 |
| IPv4 Address/ prefix-length(vpn0_ipv4_address) | 192.1.2.22/30 |
| Color(vpn0_if_tunnel_color_value) | mpls |
| Restrict(vpn0_if_tunnel_color_restrict) | <input checked="" type="checkbox"/> |
| Hostname(host-name) | cEdge51 |
| System IP(system-ip) | 10.255.255.52 |
| Site ID(site-id) | 50 |

Generate Password Update Cancel

Details to be entered for cEdge51

Note: The IP Address/Default Gateway of the VPN 0 Interface for cEdge51 is of the MPLS link. The corresponding color has been selected here, setting it to restrict. This means that the tunnel will only build tunnels with TLOCs of the same color

- Click on the entry in the Device List to view the configuration that will be pushed to the device. Notice that the vBond IP and the Organization Name have been populated. These are taken from the vManage **Administration => Settings** page, where they need to be populated. Click on **Configure** to configure the device.

Since this isn't a device that exists (as of now), the configuration push is scheduled for later, when a device is associated with this Device Name (the one ending in 73F2). This is done in the next section

Task List

- [Creating the cEdge50 and cEdge51 VMs](#)
- [Onboarding cEdge50 and cEdge51](#)
 - [Initial Configuration – non SD-WAN mode](#)
 - [Copying and modifying Feature Templates](#)
 - [Creating and Attaching Device Templates](#)
 - [Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)
- [Onboarding Verification](#)

[Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)

We will be generating a Bootstrap file for each cEdge and placing it in the flash of the device we want to bring up. The devices should come up and establish control connections with vManage, along with establishing BFD sessions with other devices. cEdge51 will not establish BFD sessions since it has the *restrict* keyword and there isn't any other tunnel with the same color of mpls.

ⓘ Note: While we are placing the Bootstrap file in flash for the lab, this can be put on a USB drive and plugged into the cEdge. This is usually done at a staging facility, post which the device is shipped to the customer site. Once they plug it in and power it on, the bootstrap configuration file allows the device to come up and establish control connections

1. Go to **Configuration => Devices**

The screenshot shows the Cisco vManage web interface. The top navigation bar includes tabs for 'Login', 'cEdge40', and 'Cisco vManage'. A warning message 'Not secure | 192.168.0.6/#/app/device/status?activity=push_file_template_configuration&pid=push_fe' is displayed. The main content area is titled 'Push Feature Template Configuration | Validation Success'. On the left, a sidebar menu lists various management categories: Configuration (selected), Devices (highlighted in teal), TLS/SSL Proxy, Certificates, Network Design, Templates, Policies, Security, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, and Cloud onRamp for Colocation. The 'Devices' section contains a table with columns: Message, Chassis Number, Device Model, and Hostname. One row is visible, showing 'Device became unreachable. Con...', 'CSR-04F9482E-44F0-E4DC-D30D...', 'CSR1000v', and 'CSR1000v'. A search bar labeled 'Search Options' is located above the table.

2. Identify the **Chassis Number** that was selected before, while attaching a Device to the Template. In this case, it ended in **38F4** for cEdge50 and **FBA3** for cEdge51. Click on the three dots on the right-hand side and click on **Generate Bootstrap Configuration** for the cEdge50 device. Choose **Cloud-Init** and **uncheck Include Default Root Certificate**. Click on OK

CONFIGURATION | DEVICES

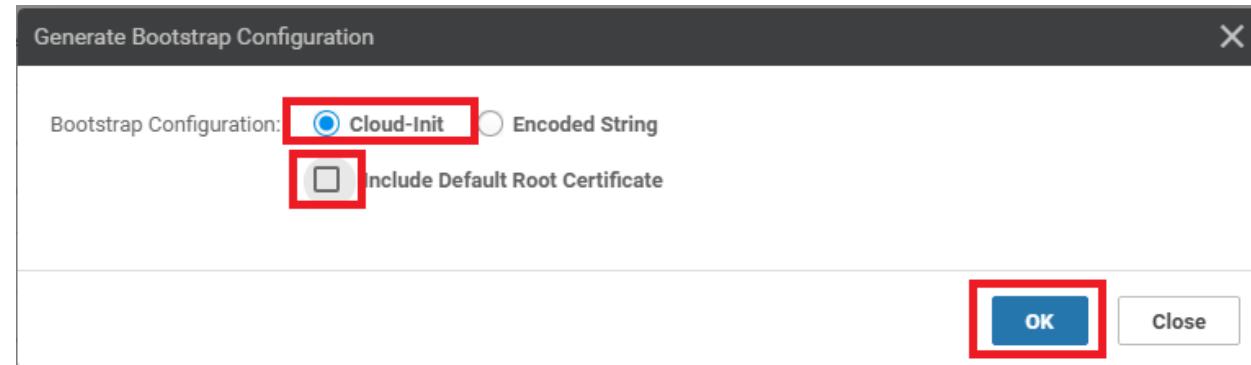
WAN Edge List Controllers

Change Mode Upload WAN Edge List Export Bootstrap Configuration Sync Smart Account

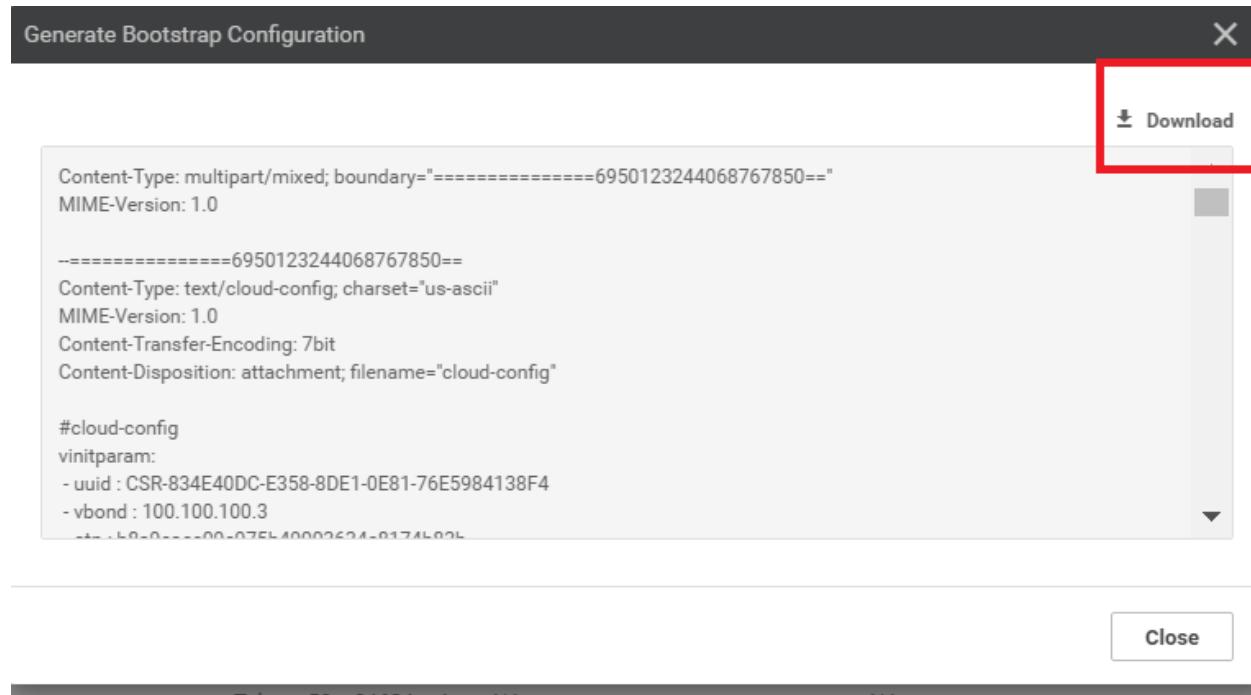
Search Options Search Options

Total Rows: 20

| State | Device Model | Chassis Number | Serial No./Token | Enterprise Cert Serial No | Enterprise Cert Expiration Date | Hostname | System IP | Site ID | Mode | ... |
|-------------|--|-------------------------|-------------------------|---------------------------|---------------------------------|----------|---------------|---------|--------|-----|
| CSR1000v | CSR-44C7CE5A-4149-E696-CB8A-415C793FBF6C | Token - fc40de6570e7... | NA | NA | -- | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-66DB39FC-C3B3-BB55-7E9D-7CD085595DD1 | Token - f28b5ab97898... | NA | NA | -- | -- | -- | -- | CLI | ... |
| CSR1000v | CSR-834E40DC-E358-80E1-0E81-76E5984138F4 | Edge50 | Token - b8a9cae09c... | NA | NA | -- | -- | -- | vManic | ... |
| CSR1000v | CSR-D40F5F8A-8975-8944-D1A3-2E0B2AE2EA1D | | Token - e7aaafc1ebd2... | NA | NA | -- | -- | -- | | |
| CSR1000v | CSR-D1837F36-6A1A-1850-7C1C-E1C69759FB3 | | Token - 90ffd29997ff... | NA | NA | -- | -- | -- | | |
| CSR1000v | CSR-S9922951362-0D86-EEF2-25CC088F1CCCE | | Token - 1da14330e171... | NA | NA | -- | -- | -- | | |
| CSR1000v | CSR-04F9482E-44FD-E4DC-D3D0-60C0806F73F2 | | 63201C50 | NA | NA | cEdge40 | 10.255.255.1 | | | |
| vEdge Cloud | e474c5f6-8c87-d376-7cac-b9950b29c159 | | 7175AE0F | NA | NA | DC+Edge1 | 10.255.255.1 | | | |
| vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-469966cdac13 | | 7DA605F5 | NA | NA | DC+Edge2 | 10.255.255.1 | | | |
| vEdge Cloud | b7fd295-58df-7671-e914-0fe2edff1609 | | 297060DD | NA | NA | vEdge20 | 10.255.255.1 | | | |
| vEdge Cloud | dde90ff0-dc62-77e6-510f-08d96608537d | | 8BF04E65 | NA | NA | vEdge21 | 10.255.255.22 | 20 | CLI | ... |
| vEdge Cloud | 17026153-f04b-6dc4-482fce3aaab2 | | 24715073 | NA | NA | vEdge30 | 10.255.255.31 | 30 | CLI | ... |
| CSR1000v | CSR-26217DAA-1B63-80DE-11C9-125F527D3270 | | Token - 8dc7b557b60... | NA | NA | -- | -- | -- | CLI | ... |

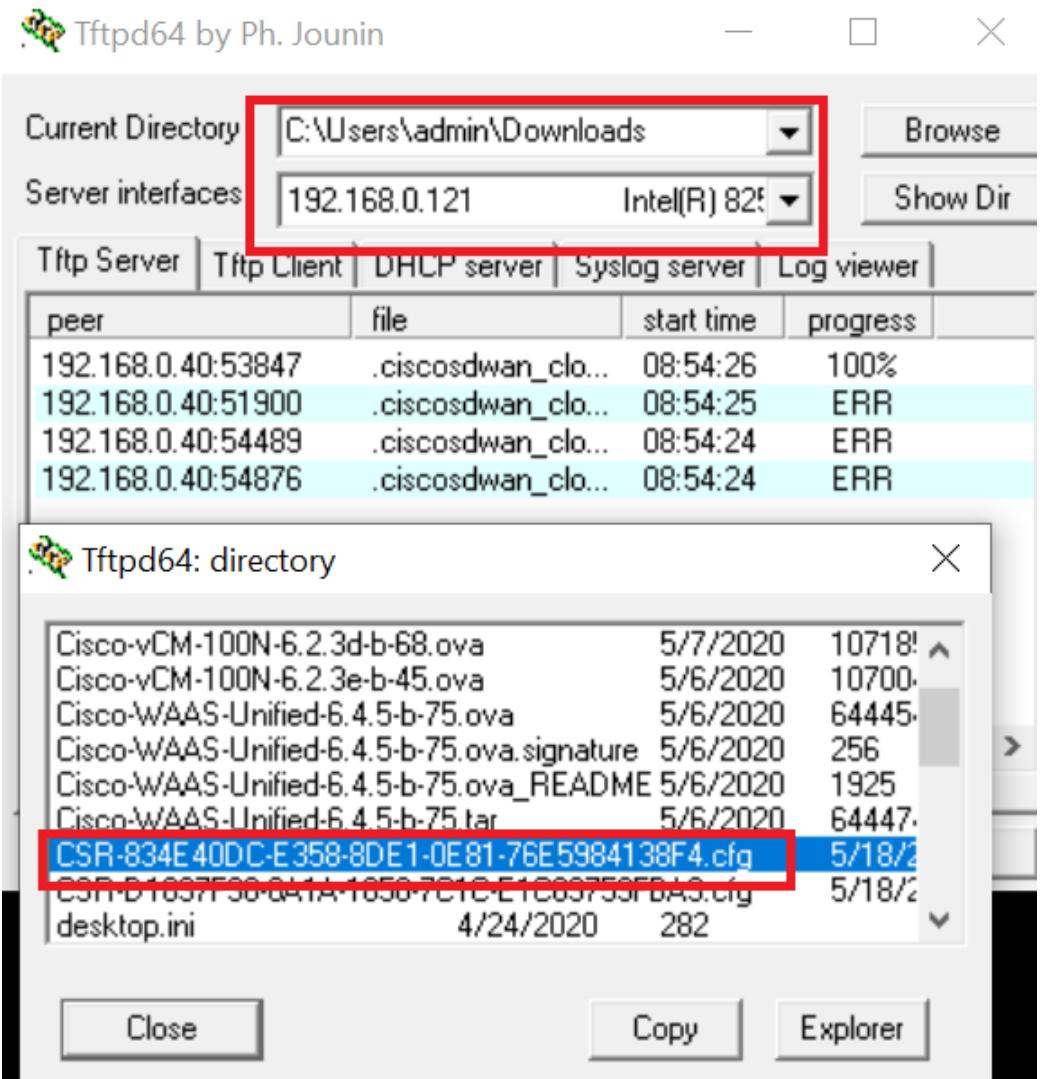


3. Download the bootstrap file (will get saved to the Downloads folder by default). It should be a file beginning with CSR...

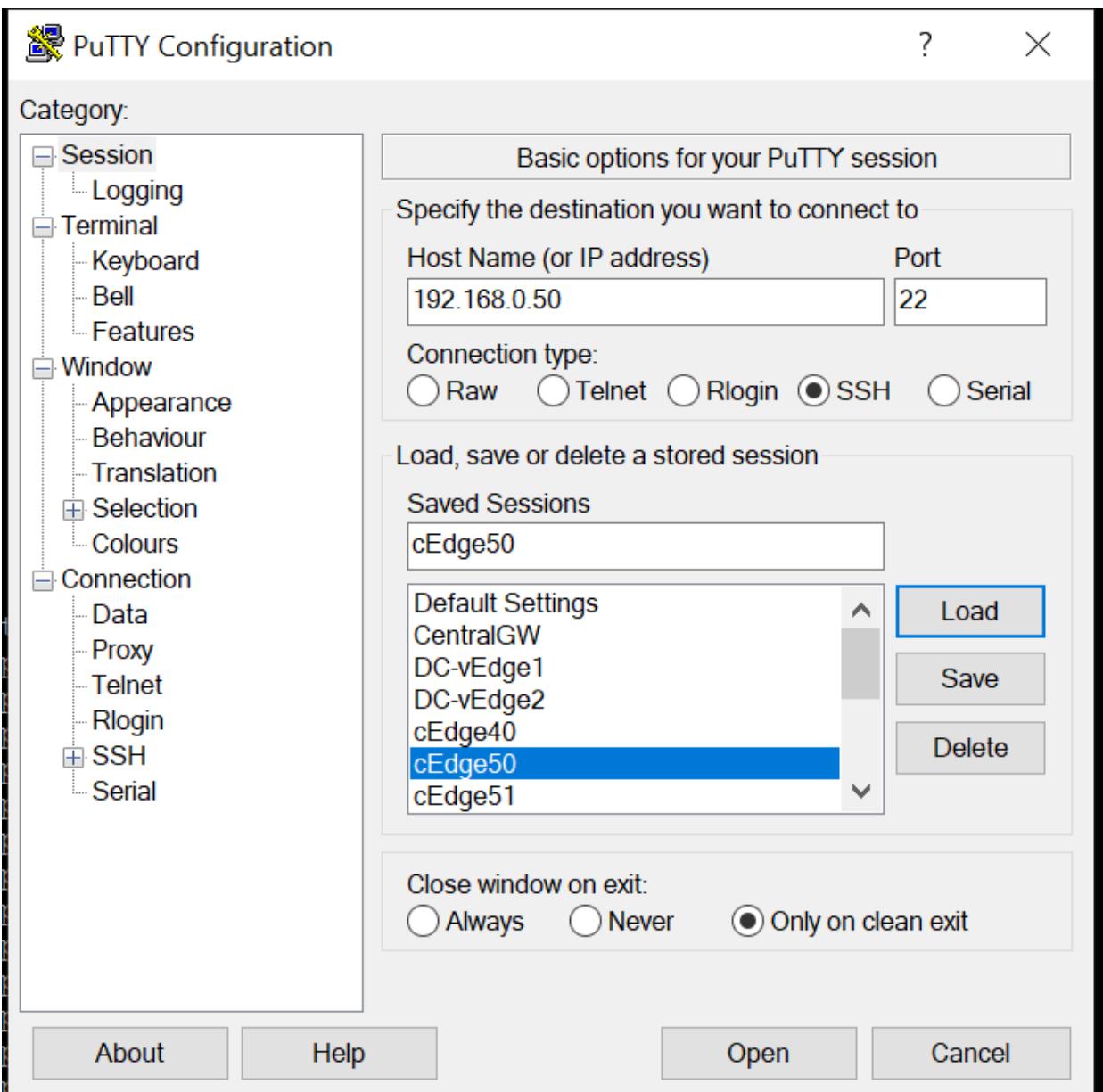


4. From the Jumphost Desktop, start TFTPD64. Click on **Browse** and choose the Downloads folder (or wherever the renamed .cfg file has been stored). Make sure the 192.168.0.X IP is chosen from the Server Interface drop down in TFTPD64. Copy the name of the file (beginning with CSR) by going to the file location. You can click on copy in TFTPD64 itself, but the name doesn't get copied sometimes. Click on **show dir** to view the files in the currently chosen folder. Clicking on **copy** copies the highlighted file name, but it is a bit flaky on the newer versions of TFTD64

Tip: On bootup, a cEdge looks for a file on its USB port (if a bootable USB drive is connected) and in bootflash:. The file name must match as above for Cloud type devices (i.e. CSR1K). For physical devices, the file name should be *ciscosdwan.cfg*. If the file is present on the USB drive and in bootflash:, the one in bootflash: takes precedence



5. Log in to the CLI of cEdge50 (we can log in via Putty now, using the saved session or by SSH'ing to 192.168.0.50) and issue `copy tftp: bootflash: .` Specify a Remote Host IP of your Jumphost (192.168.0.121 in this case). The source file name should be the one we downloaded for cEdge50 (beginning with CSR) and destination file name should be *ciscosdwan_cloud_init.cfg*. The file should get copied over to bootflash: successfully



The screenshot shows a PuTTY terminal window titled "192.168.0.50 - PuTTY". The session is logged in as "admin". The command "Router#copy tftp: flash:" is issued, followed by prompts for the remote host address (192.168.0.121), source filename (CSR-834E40DC-E358-8DE1-0E81-76E5984138F4.cfg), and destination filename (ciscosdwan_cloud init.cfg). The destination filename is highlighted with a green box. The process continues with file access, loading from the specified host and port, and a successful transfer of 31186 bytes in 0.037 seconds.

```
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

Router#copy tftp: flash:
Address or name of remote host []? 192.168.0.121
Source filename []? CSR-834E40DC-E358-8DE1-0E81-76E5984138F4.cfg
Destination filename [CSR-834E40DC-E358-8DE1-0E81-76E5984138F4.cfg]? ciscosdwan_
cloud init.cfg
Accessing tftp://192.168.0.121/CSR-834E40DC-E358-8DE1-0E81-76E5984138F4.cfg...
Loading CSR-834E40DC-E358-8DE1-0E81-76E5984138F4.cfg from 192.168.0.121 (via GigabitEthernet1): !
[OK - 31186 bytes]

31186 bytes copied in 0.037 secs (842865 bytes/sec)
Router#
```

```
copy tftp: bootflash:
```

6. **Repeat steps 1 to 5** for cEdge51, downloading the bootstrap file for it (starting with CSR) and TFTP'ing it over to cEdge51.

```
192.168.0.51 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

Router#copy tftp: flash:
Address or name of remote host []? 192.168.0.121
Source filename []? CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3.cfg
Destination filename [CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3.cfg]? ciscosdwan_
cloud_init.cfg
Accessing tftp://192.168.0.121/CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3.cfg...
Loading CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3.cfg from 192.168.0.121 (via GigabitEthernet1): !
[OK - 31179 bytes]

31179 bytes copied in 0.036 secs (866083 bytes/sec)
Router#
```

7. Log in to the CLI of vManage (again, via the saved Putty session or by SSH'ing to 192.168.0.6) and issue the following commands to SCP the ROOTCA.pem file over to cEdge50 and cEdge51

```
login as: admin
Pre-authentication banner message from server:
| viptela 20.1.1
End of banner message from server
admin@192.168.0.6's password:
Last login: Mon May 18 16:08:15 2020 from 192.168.0.121
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on vmanage
vmanage# vshell
vmanage:-$ scp ROOTCA.pem admin@192.168.0.50:ROOTCA.pem
Pushing PEM file to cEdge 50
The authenticity of host '192.168.0.50 (192.168.0.50)' can't be established.
RSA key fingerprint is SHA256:MTxP4+Hp/RX5RVcn0f5XRf8Cja+RDeiVggQpzXlcIAA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.50' (RSA) to the list of known hosts.
Password:
ROOTCA.pem
100% 1277 580.2KB/s 00:00
Connection to 192.168.0.50 closed by remote host.
vmanage:-$ scp ROOTCA.pem admin@192.168.0.51:ROOTCA.pem
Pushing PEM file to cEdge51
The authenticity of host '192.168.0.51 (192.168.0.51)' can't be established.
RSA key fingerprint is SHA256:SQyw3W7OkCRL64DA1/AJn0UH/zgfbP6Ppu2G6PxP4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.51' (RSA) to the list of known hosts.
Password:
ROOTCA.pem
100% 1277 637.3KB/s 00:00
vmanage:->
```

```
vshell
scp ROOTCA.pem admin@192.168.0.50:ROOTCA.pem
yes
admin
```

```
scp ROOTCA.pem admin@192.168.0.51:ROOTCA.pem
yes
admin
```

The last **admin** over there is the password of cEdge50/cEdge51

8. Go back to the CLI of cEdge50 and cEdge51 and issue `controller-mode enable` from privilege mode. **Confirm** and this should lead to the devices rebooting

```
Router#controller
Router#controller-mode enable
Enabling controller mode will erase the nvram filesystem, remove all configuration files, and reload the box!
Ensure the BOOT variable points to a valid image
Continue? [confirm] █
```

```
controller-mode enable
```

We have completed this section of the lab and will now need to wait for the cEdges to reboot. On rebooting, they should pick up the configuration file from bootflash: and connect to the vManage/vSmarts/other vEdges. This will be verified in the next section.

Task List

- [Creating the cEdge50 and cEdge51 VMs](#)
- [Onboarding cEdge50 and cEdge51](#)
 - [Initial Configuration – non SD-WAN mode](#)
 - [Copying and modifying Feature Templates](#)
 - [Creating and Attaching Device Templates](#)
 - [Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)
- [Onboarding Verification](#)

Onboarding Verification

1. On the vManage GUI, go to **Monitor => Network**. You should see cEdge50 and cEdge51 successfully added on vManage.

| Hostname | System IP | Device Model | Chassis Number/ID | State | Reachability | Site ID | BFD | Control | Version | Up Since |
|----------------|----------------------|---------------------|---------------------------------------|----------|------------------|-----------|----------|----------|-----------------------------|-----------------------------------|
| vManage | 10.255.255.1 | vManage | dfea63a5-66d2-4e50-a07b-ec4ad4... | ✓ | reachable | 1000 | - | 10 | 20.1.1 | 11 May 2020 11:02:00 AM PDT |
| vSmart | 10.255.255.3 | vSmart | 20607a12-c0c8-4f46-a65f-5a547c... | ✓ | reachable | 1000 | - | 10 | 20.1.1 | 11 May 2020 11:02:00 AM PDT |
| vSmart2 | 10.255.255.4 | vSmart | 7f332491-cb6f-4843-8bf5-060f90... | ✓ | reachable | 1000 | - | 10 | 20.1.1 | 11 May 2020 11:02:00 AM PDT |
| vBond | 10.255.255.2 | vEdge Cloud (vBo... | fc31c154-99c5-4267-971d-ec9ae7... | ✓ | reachable | 1000 | - | 20.1.1 | 11 May 2020 11:02:00 AM PDT | |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b... | ✓ | reachable | 1 | 5 | 3 | 20.1.1 | 14 May 2020 7:36:00 AM PDT |
| DC-vEdge2 | 10.255.255.12 | vEdge Cloud | 0cd4f0e-f2f1-fe75-866c-469966c... | ✓ | reachable | 1 | 5 | 3 | 20.1.1 | 16 May 2020 12:24:00 PM PDT |
| cEdge40 | 10.255.255.41 | CSR1000v | CSR-04F9482E-44F0-E4DC-D3D... | ✓ | reachable | 40 | 6 | 3 | 17.02.01r.0.32 | 18 May 2020 9:14:00 AM PDT |
| cEdge50 | 10.255.255.51 | CSR1000v | CSR-834E40DC-E358-8DE1-0E81... | ✓ | reachable | 50 | 6 | 3 | 17.02.01r.0.32 | 18 May 2020 1:53:00 PM PDT |
| cEdge51 | 10.255.255.52 | CSR1000v | CSR-D1837F36-6A1A-1850-7C1C... | ✓ | reachable | 50 | - | 3 | 17.02.01r.0.32 | 18 May 2020 1:54:00 PM PDT |
| vEdge20 | 10.255.255.21 | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2ed... | ✓ | reachable | 20 | 5 | 3 | 20.1.1 | 17 May 2020 5:27:00 AM PDT |
| vEdge21 | 10.255.255.22 | vEdge Cloud | ddc90ff0-dc62-77e6-510f-08d966... | ✓ | reachable | 20 | 5 | 3 | 20.1.1 | 17 May 2020 10:52:00 PM PDT |
| vEdge30 | 10.255.255.31 | vEdge Cloud | 17026153-f09e-be4b-6dce-482fce... | ✓ | reachable | 30 | 6 | 3 | 20.1.1 | 18 May 2020 1:22:00 AM PDT |

2. Clicking on cEdge50 or cEdge51 and going to **Troubleshooting => Control Connections (Live View)** will show us that the cEdges have established control connections with vManage and the vSmarts. We can check this via the CLI

`show sdwan control connections` as well

```
cEdge50#show sdwan control connections
          CONTROLLER
PEER    PEER PEER SITE      DOMAIN PEER
          GROUP
          TYPE   PROT SYSTEM IP   ID     ID   PRIVATE IP
          OXY STATE UPTIME
          ID

-----
vsmart  dtls 10.255.255.3  1000   1   100.100.100.4           12346 100.100.100.4
       up   0:00:18:09  0
vsmart  dtls 10.255.255.4  1000   1   100.100.100.5           12346 100.100.100.5
       up   0:00:18:09  0
vmanage dtls 10.255.255.1  1000   0   100.100.100.2           12346 100.100.100.2
       up   0:00:18:09  0

cEdge50#
cEdge50#
```

Control Connections for cEdge50

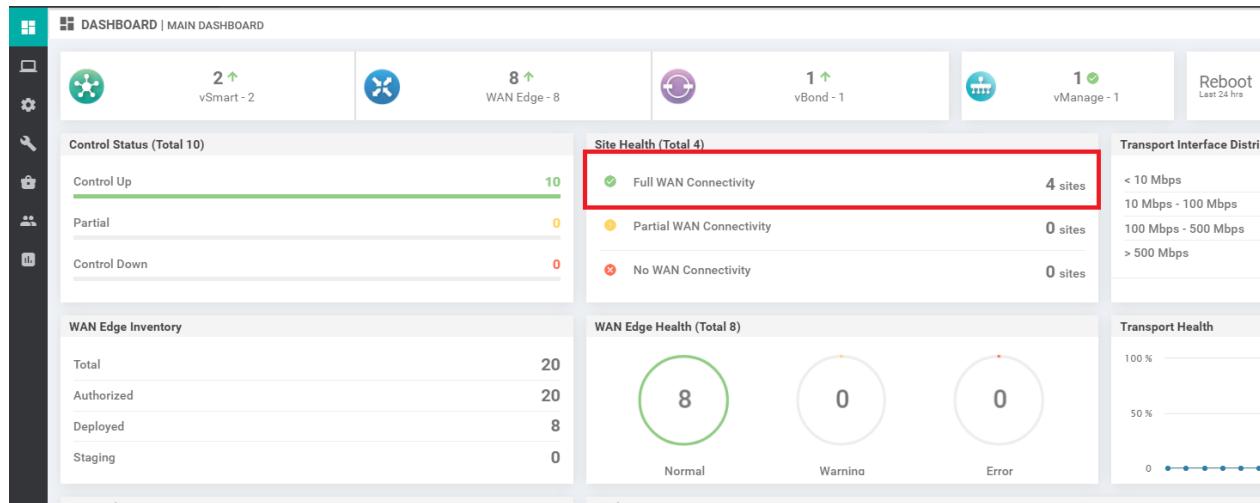
| cEdge51#show sdwan control connections | | | | | | |
|--|------------|--------------|------------|------|---------------|---------------------|
| PEER | PEER | PEER | CONTROLLER | | PEER | |
| | | | GROUP | SITE | DOMAIN | PEER |
| TYPE | PROT | SYSTEM IP | ID | ID | PRIVATE IP | PR |
| OXY STATE | UPTIME | ID | | | PORT | PUBLIC IP |
| vsmart | dtls | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12346 100.100.100.4 |
| up | 0:00:18:23 | 0 | | | | 12346 mpls |
| vsmart | dtls | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12346 100.100.100.5 |
| up | 0:00:18:23 | 0 | | | | 12346 mpls |
| vmanage | dtls | 10.255.255.1 | 1000 | 0 | 100.100.100.2 | 12346 100.100.100.2 |
| up | 0:00:18:23 | 0 | | | | 12346 mpls |

cEdge51#

Control Connections for cEdge51

```
show sdwan control connections
```

3. Navigate to **Dashboards => Main Dashboard** and we will see 4 Sites with Full WAN connectivity and 8 WAN Edges



Tip: We should be seeing 5 sites with full WAN connectivity, but one of the WAN Edges (cEdge51) has not been able to establish any BFD sessions yet, hence the site itself doesn't have full WAN connectivity

4. The previous observation can be seen if we click on **Full WAN connectivity**. Notice that Site 50 is missing from this list. Once we ensure that there are BFD sessions with cEdge51, the issue should be resolved

Site Devices Health: Full WAN Connectivity

Total Rows: 6

| Hostname | Reachability | System IP | Site ID | BFD Sessions | Last Updated | ... |
|-----------|--------------|---------------|---------|--------------|----------------------------|-----|
| DC-vEdge1 | reachable | 10.255.255.11 | 1 | 5 | 21 May 2020 2:00:09 AM PDT | ... |
| vEdge21 | reachable | 10.255.255.22 | 20 | 5 | 21 May 2020 2:00:11 AM PDT | ... |
| vEdge20 | reachable | 10.255.255.21 | 20 | 5 | 21 May 2020 2:00:09 AM PDT | ... |
| DC-vEdge2 | reachable | 10.255.255.12 | 1 | 5 | 21 May 2020 2:00:09 AM PDT | ... |
| vEdge30 | reachable | 10.255.255.31 | 30 | 6 | 21 May 2020 2:00:09 AM PDT | ... |
| cEdge40 | reachable | 10.255.255.41 | 40 | 6 | 21 May 2020 2:00:09 AM PDT | ... |

5. Issue `show sdwan bfd sessions` and we should see that cEdge50 has established BFD sessions, whereas cEdge51 has not

```
cEdge50#
cEdge50#
cEdge50#show sdwan bfd sessions
      SOURCE TLOC      REMOTE TLOC
      DST PUBLIC      DST PUBLIC      DB
TECT TX SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MU
MULTIPLIER INTERVAL(msec) UPTIME TRANSITIONS

-----
```

| TECT | TX | SYSTEM IP | SITE ID | STATE | COLOR | COLOR | SOURCE IP | IP | PORT | ENCAP | MU |
|---------------|----|------------|-----------------|-----------------|-------|-------|----------------|----------------|-------|-------|----|
| 10.255.255.11 | 1 | up | public-internet | default | 1 | 1 | 100.100.100.50 | 100.100.100.10 | 12366 | ipsec | 7 |
| 1000 | | 0:00:22:03 | | | | | | | | | |
| 10.255.255.12 | 1 | up | public-internet | default | 1 | 1 | 100.100.100.50 | 100.100.100.11 | 12366 | ipsec | 7 |
| 1000 | | 0:00:22:03 | | | | | | | | | |
| 10.255.255.21 | 20 | up | public-internet | default | 1 | 1 | 100.100.100.50 | 100.100.100.20 | 12366 | ipsec | 7 |
| 1000 | | 0:00:22:03 | | | | | | | | | |
| 10.255.255.22 | 20 | up | public-internet | default | 1 | 1 | 100.100.100.50 | 192.0.2.10 | 12366 | ipsec | 7 |
| 1000 | | 0:00:22:03 | | | | | | | | | |
| 10.255.255.31 | 30 | up | public-internet | default | 1 | 1 | 100.100.100.50 | 100.100.100.30 | 12366 | ipsec | 7 |
| 1000 | | 0:00:22:04 | | | | | | | | | |
| 10.255.255.41 | 40 | up | public-internet | public-internet | 1 | 1 | 100.100.100.50 | 100.100.100.40 | 12347 | ipsec | 7 |
| 1000 | | 0:00:22:03 | | | | | | | | | |

BFD sessions - cEdge50

```
cEdge51#show sdwan bfd sessions
cEdge51#
```

BFD sessions - cEdge51

show sdwan bfd sessions

At this point, we have completed onboarding verification

Task List

- [Creating the cEdge50 and cEdge51 VMs](#)
- [Onboarding cEdge50 and cEdge51](#)
 - [Initial Configuration – non SD-WAN mode](#)
 - [Copying and modifying Feature Templates](#)
 - [Creating and Attaching Device Templates](#)
 - [Copying the Bootstrap file and converting to SD-WAN IOS-XE mode](#)
- [Onboarding Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: Feb 25, 2016

Site last generated: Sep 1, 2020



Feature and Device Templates for the DC-vEdges

[Take a tour of this page](#)

Summary: Create Feature and Device Templates for the DC-vEdges in order to bring them in vManage mode.

Table of Contents

- [Overview](#)
- [Creating the DC-vEdge VPN Feature Templates](#)
 - [Creating the VPN0 Feature Template](#)
 - [Creating the VPN512 Feature Template](#)
 - [Creating the INET VPN Interface Feature Template](#)
 - [Creating the MPLS VPN Interface Feature Template](#)
 - [Creating the Mgmt VPN Interface Feature Template](#)
- [Creating a Device Template and Attaching Devices](#)
- [Activity Verification](#)

Task List

- Creating the DC-vEdge VPN Feature Templates
- Creating the VPN0 Feature Template
- Creating the VPN512 Feature Template
- Creating the INET VPN Interface Feature Template
- Creating the MPLS VPN Interface Feature Template
- Creating the Mgmt VPN Interface Feature Template

- Creating a Device Template and Attaching Devices
- Activity Verification

Overview

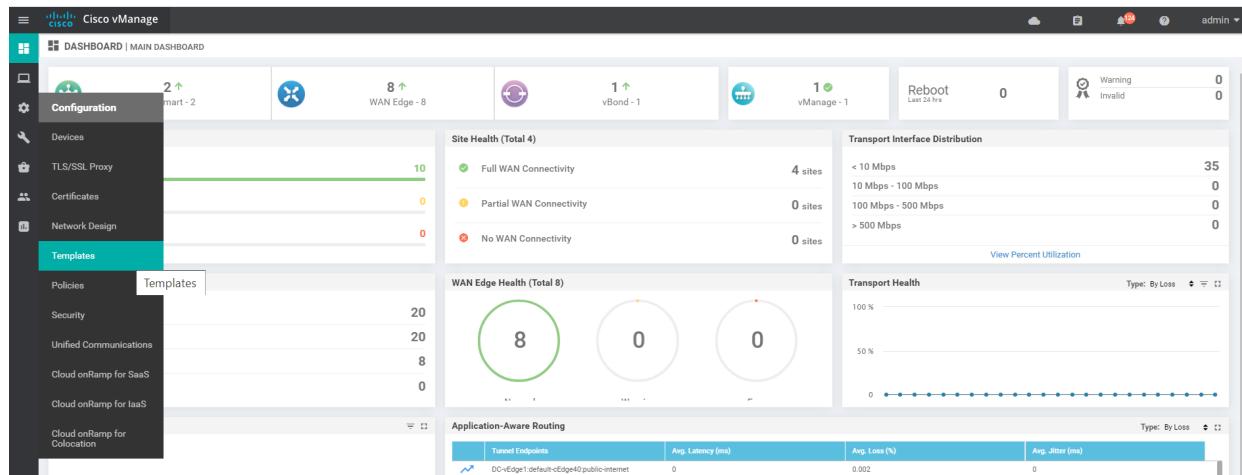
We have already seen feature templates in action and their versatility in large deployments is unmatched. Coupled with Device Specific parameters, we have a networking construct which is extremely malleable and can be applied in wide, arcing sweeps to similar devices through Device Templates that act as containers for grouping multiple Feature Templates.

In this section, we will be creating feature templates for our DC-vEdges. We will then apply these Feature Templates to Device Templates. Devices will be attached to these Device Templates, thereby ensuring that the DC-vEdges are controlled by vManage.

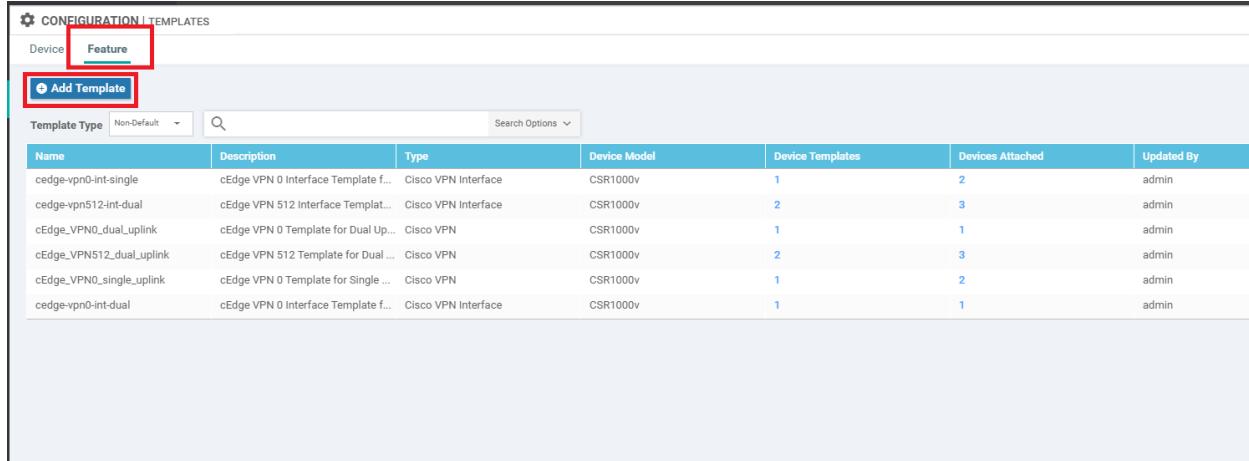
Creating the DC-vEdge VPN Feature Templates

Creating the VPN0 Feature Template

1. On the vManage GUI, navigate to **Configuration => Templates**

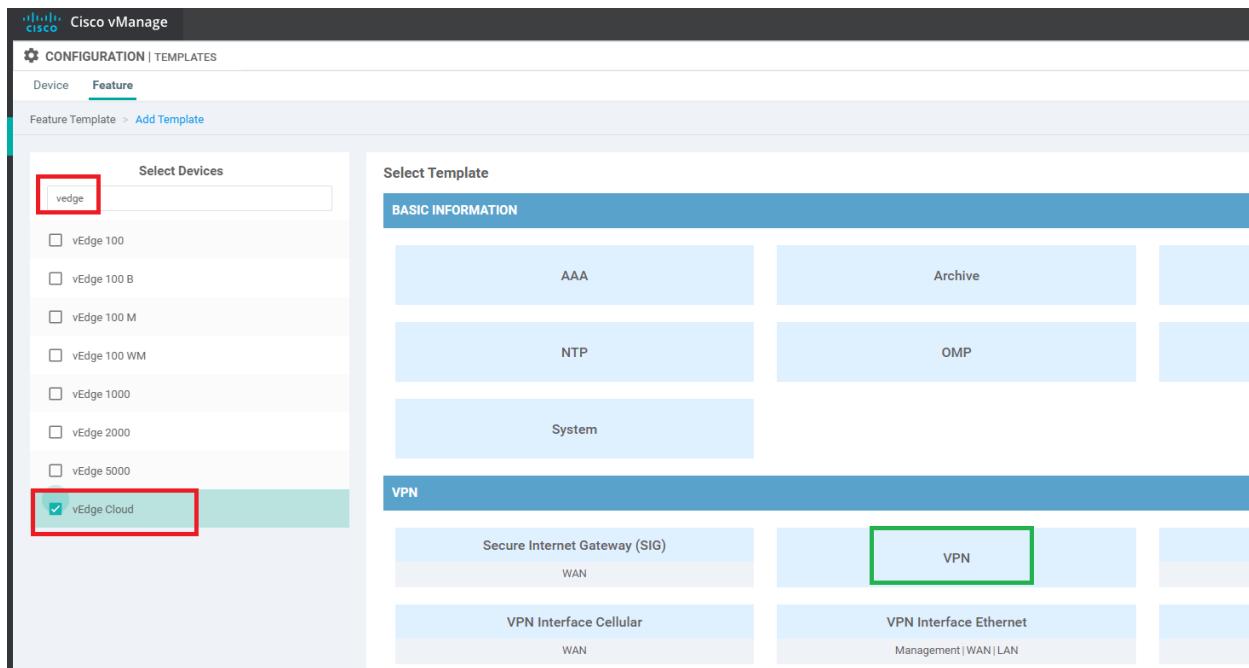


2. Click on the **Feature** tab and click on **Add Template**



| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By |
|--------------------------|-------------------------------------|---------------------|--------------|------------------|------------------|------------|
| cedge-vpn0-int-single | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin |
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Templat... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin |
| cEdge_VPN0_Dual_Uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin |
| cEdge_VPN512_Dual_uplink | cEdge VPN 512 Template for Dual ... | Cisco VPN | CSR1000v | 2 | 3 | admin |
| cEdge_VPN0_Single_Uplink | cEdge VPN 0 Template for Single ... | Cisco VPN | CSR1000v | 1 | 2 | admin |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin |

3. Search for **vedge** in the search box and put a check mark next to **vEdge Cloud**. This will give the options to select Feature Templates applicable to the selected device type. Click on **VPN** to start configuring a VPN Template. This is going to be our VPN Template for VPN 0



Select Devices

- vEdge 100
- vEdge 100 B
- vEdge 100 M
- vEdge 100 WM
- vEdge 1000
- vEdge 2000
- vEdge Cloud

Select Template

BASIC INFORMATION

- AAA
- Archive
- NTP
- OMP
- System

VPN

- Secure Internet Gateway (SIG)
WAN
- VPN
- VPN Interface Cellular
WAN
- VPN Interface Ethernet
Management | WAN | LAN

4. Give the Template a name of **DCvEdge-vpn0** and a description of **VPN0 for the DC-vEdges INET and MPLS link**

The screenshot shows the Cisco vManage interface under the Configuration | Templates section. The Feature tab is selected. A Feature Template named 'VPN' is selected. The Device Type is set to 'vEdge Cloud'. The Template Name is 'DCvEdge-vpn0' and the Description is 'VPN0 for the DC-vEdges INET and MPLS link'.

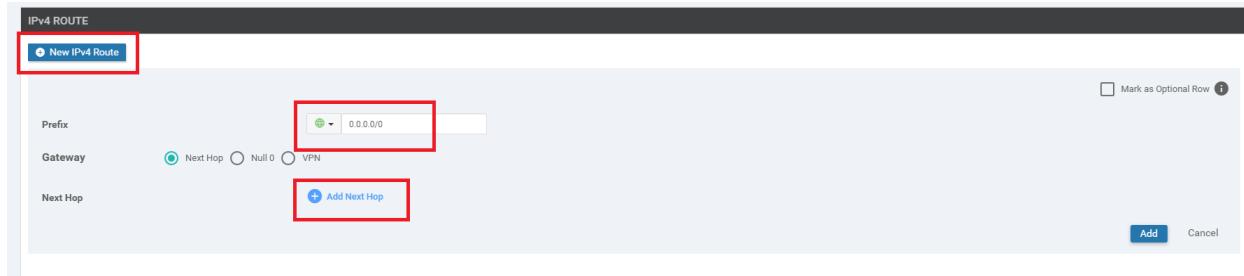
5. Under **Basic Configuration**, specify the VPN as 0 (zero)

The screenshot shows the Basic Configuration tab selected. Under the BASIC CONFIGURATION section, the VPN field is set to 0.

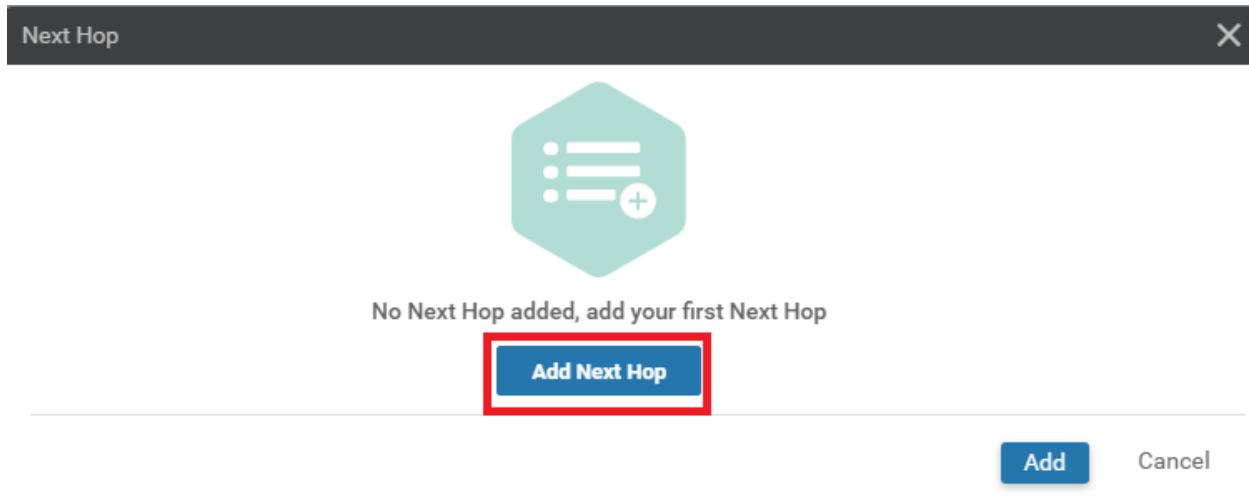
6. Populate the Primary and Secondary DNS Address as 10.y.1.5 and 10.y.1.6 respectively, where y is 1 if you're on the SLC DC and 2 if you're on the GHI DC (the email with lab details should enumerate which DC you're on). Set the drop down to **Global** in order to enter the IPs. The option to enter the Secondary DNS server will pop up once the Primary is populated

The screenshot shows the DNS tab selected. Under the DNS section, the Primary DNS Address (IPv4) is set to 10.2.1.5 and the Secondary DNS Address (IPv4) is set to 10.2.1.6. Both fields are highlighted with a red box.

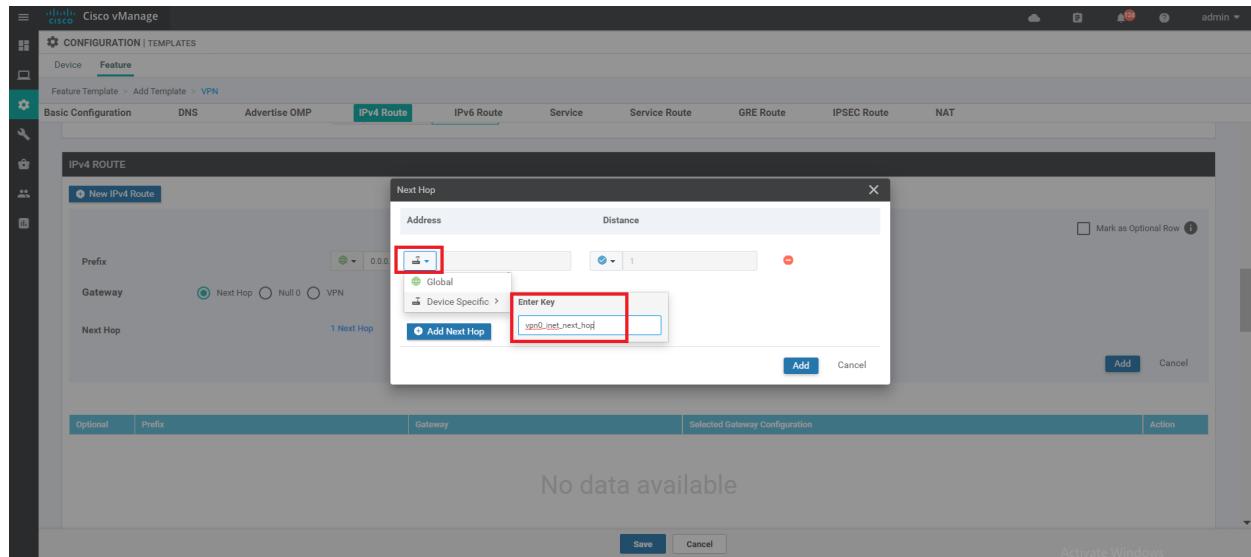
7. Under **IPv4 Route**, click on **New IPv4 Route** and specify the Prefix as Global. Populate **0.0.0.0/0** as the prefix and click on **Add Next Hop**



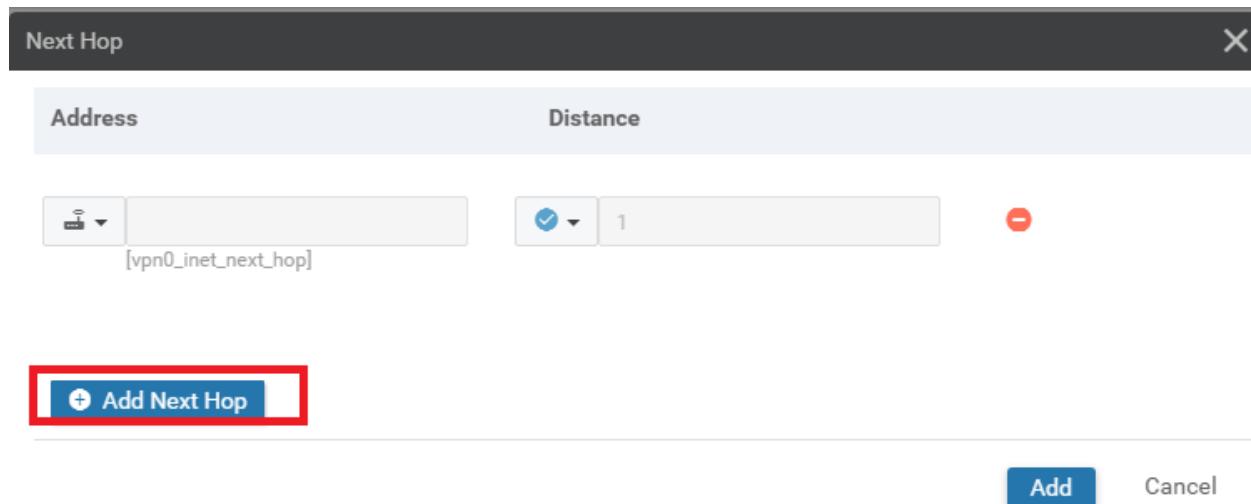
8. Click on **Add Next Hop** again in the popup window



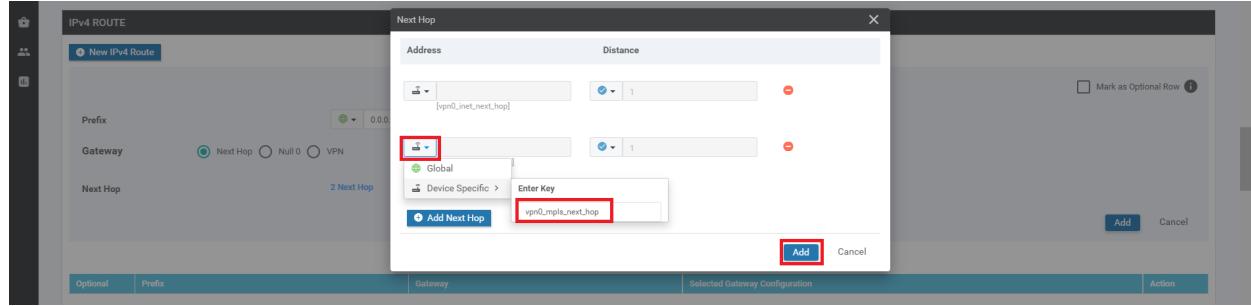
9. From the drop down, set the value to Device Specific and enter the key as *vpn0_inet_next_hop*



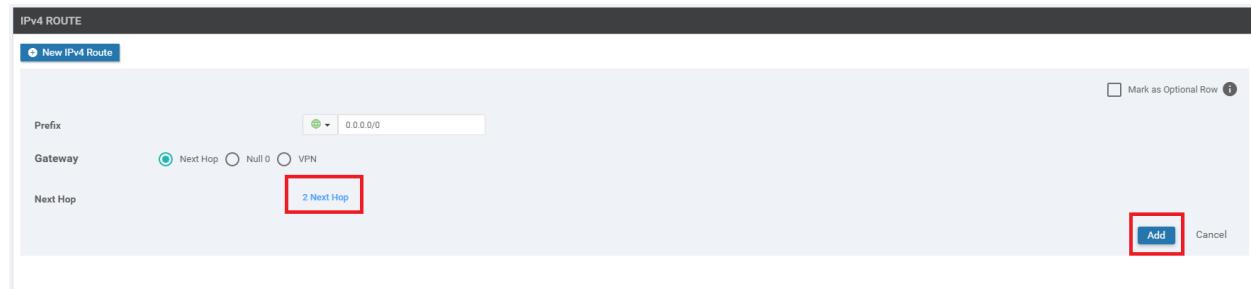
10. Click on **Add Next Hop**. We will now be adding the default route for the MPLS link



11. Choose **Device Specific** from the drop down and give it a name of *vpn0_mpls_next_hop*. Click on **Add**



12. Make sure the IPv4 Route screen shows **2 Next Hop** and click on Add



13. Back at the main Feature Template page, click on **Save**. This will create our VPN 0 Feature Template

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > **VPN**

Device Type vEdge Cloud

Template Name DCvEdge-vpn0-inet

Description VPN0 for the DC-vEdges INET link

Basic Configuration DNS Advertise OMP IPv4 Route IPv6 Route Service Service Route GRE Route IPSEC Route NAT

BASIC CONFIGURATION

VPN

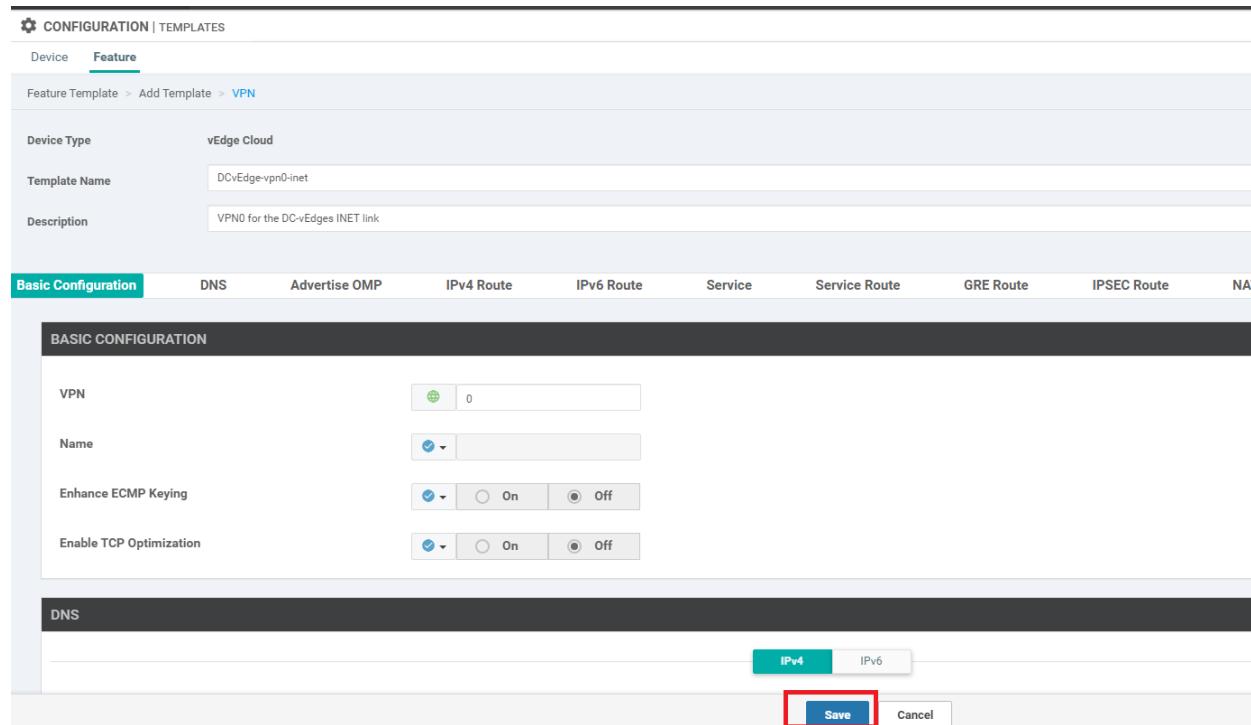
Name

Enhance ECMP Keying On Off

Enable TCP Optimization On Off

DNS

IPv4



Task List

- Creating the DC-vEdge VPN Feature Templates
- [Creating the VPN0 Feature Template](#)
- Creating the VPN512 Feature Template
- Creating the INET VPN Interface Feature Template
- Creating the MPLS VPN Interface Feature Template
- Creating the Mgmt VPN Interface Feature Template
- Creating a Device Template and Attaching Devices
- Activity Verification

Creating the VPN512 Feature Template

We will make use of the just created VPN 0 Feature Template to create our VPN 512 Feature Template.

1. On the **Configuration => Templates** page navigate to the Feature tab and look for **DCvEdge-vpn0**. Click on the three dots for this template and click on **Copy**

The screenshot shows the Cisco vManage interface under Configuration > Templates. The Feature tab is selected. A table lists various templates, including 'DCvEdge-vpn0'. A context menu is open over the 'DCvEdge-vpn0' row, with the 'Copy' option highlighted.

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------|--|---------------------|--------------|------------------|------------------|------------|----------------------------|---------|
| cedge-vpn0-int-single | cEdge VPN 0 Interface Template for devices wi... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Template for devices ... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| cEdge_VPN0_dual_uplink | cEdge VPN 0 Template for Dual Uplinks | Cisco VPN | CSR1000v | 1 | 1 | admin | 18 May 2020 7:37:39 AM PDT | ... |
| cEdge_VPN512_dual_uplink | cEdge VPN 512 Template for Dual Uplinks | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 8:35:47 AM PDT | ... |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single Uplinks | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 1:24:18 PM PDT | ... |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template for devices wi... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 18 May 2020 8:28:19 AM PDT | ... |
| DCvEdge-vpn0 | VPN0 for the DC-vEdges (INET and MPLS link) | WAN Edge VPN | vEdge Cloud | 0 | 0 | admin | 23 May 2020 1:01:17 AM PDT | ... |

2. Give the Template a name of **DCvEdge-vpn512** and a description of **VPN512 for the DC-vEdges**. Click on **Copy**

The screenshot shows the 'Template Copy' dialog box. It contains fields for 'Template Name' (set to 'DCvEdge-vpn512') and 'Description' (set to 'VPN512 for the DC-vEdges'). At the bottom are 'Copy' and 'Cancel' buttons, with 'Copy' highlighted.

Template Copy

Template Name

DCvEdge-vpn512

Description

VPN512 for the DC-vEdges

Copy Cancel

3. Click on the three dots for the newly created template and click on **Edit**

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Feature' tab is selected. A table lists various feature templates, including 'cEdge_vpn512_int-dual', 'cEdge_VPN512_dual_uplink', 'DCvEdge-vpn0', 'cEdge_vpn0-int-dual', 'cEdge_VPN0_single_uplink', 'cedge_vpn0-int-single', 'DCvEdge-vpn512', and 'cEdge_VPN0_dual_uplink'. The 'cEdge_vpn512_int-dual' row is selected, and a context menu is open, with the 'Edit' option highlighted.

4. Update the Description, if it hasn't been updated and change the VPN to 512

The screenshot shows the 'Feature Template > VPN' configuration page. It displays basic information like Device Type (vEdge Cloud) and Template Name (DCvEdge-vpn512). The 'Description' field contains 'VPNS12 for the DC-vEdges'. In the 'BASIC CONFIGURATION' section, the 'VPN' dropdown is set to '512' and is highlighted with a red box. Below it, the 'Name' and 'Enhance ECMP Keying' sections are shown.

5. Scroll down to the IPv4 Route section and click on the pencil icon to edit the 0.0.0.0/0 Route

The screenshot shows the 'IPv4 ROUTE' configuration page. It lists a single route entry with Prefix '0.0.0.0/0', Gateway '2', and Next Hop '1'. The 'Action' column for this entry is highlighted with a red box, indicating where to click to edit the route.

6. Click on 2 Next Hop. We will be removing the MPLS next hop entry and modifying the name of the INET next hop for the management network

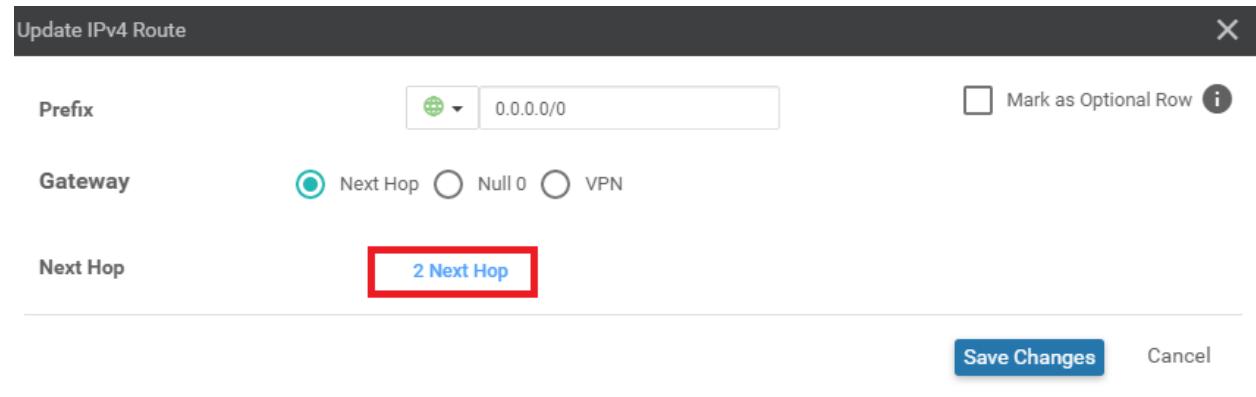
Update IPv4 Route

Prefix Mark as Optional Row i

Gateway Next Hop Null 0 VPN

Next Hop 2 Next Hop

Save Changes Cancel



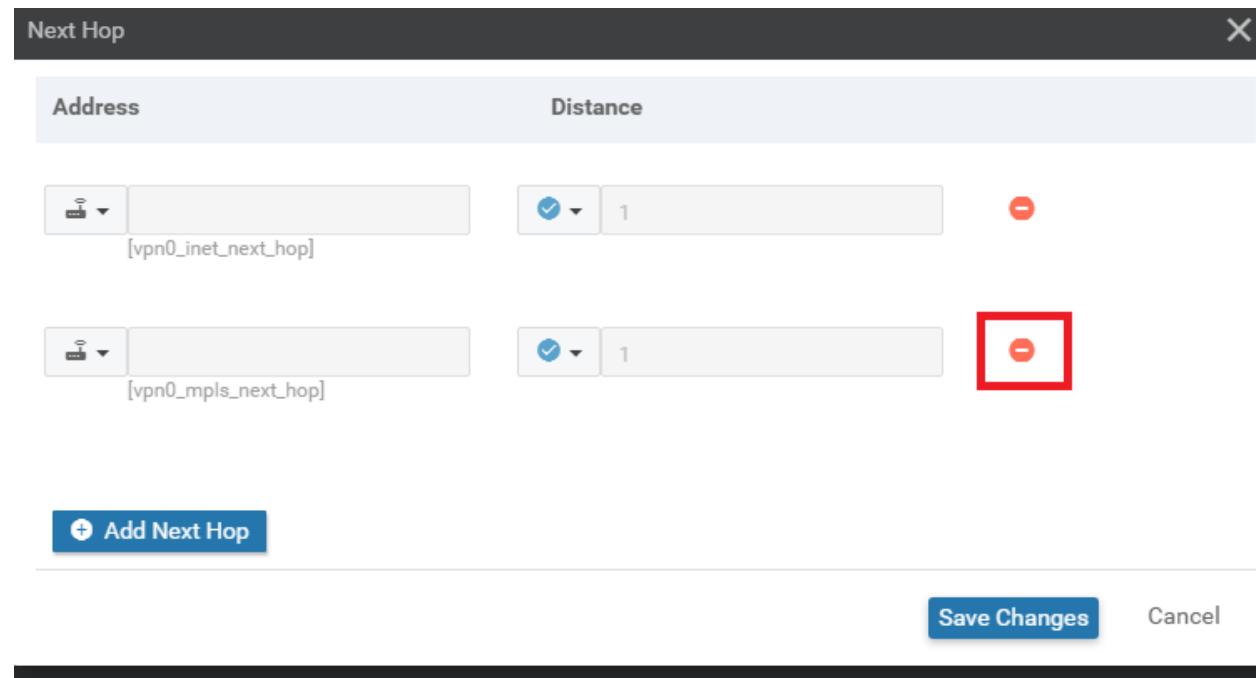
7. Click on the minus sign to remove the MPLS next hop

Next Hop

| Address | Distance |
|---|--|
| <input type="text" value="vpn0_inet_next_hop"/> v | <input checked="" type="radio"/> 1 - |
| <input type="text" value="vpn0_mpls_next_hop"/> v | <input checked="" type="radio"/> 1 - |

Add Next Hop +

Save Changes Cancel



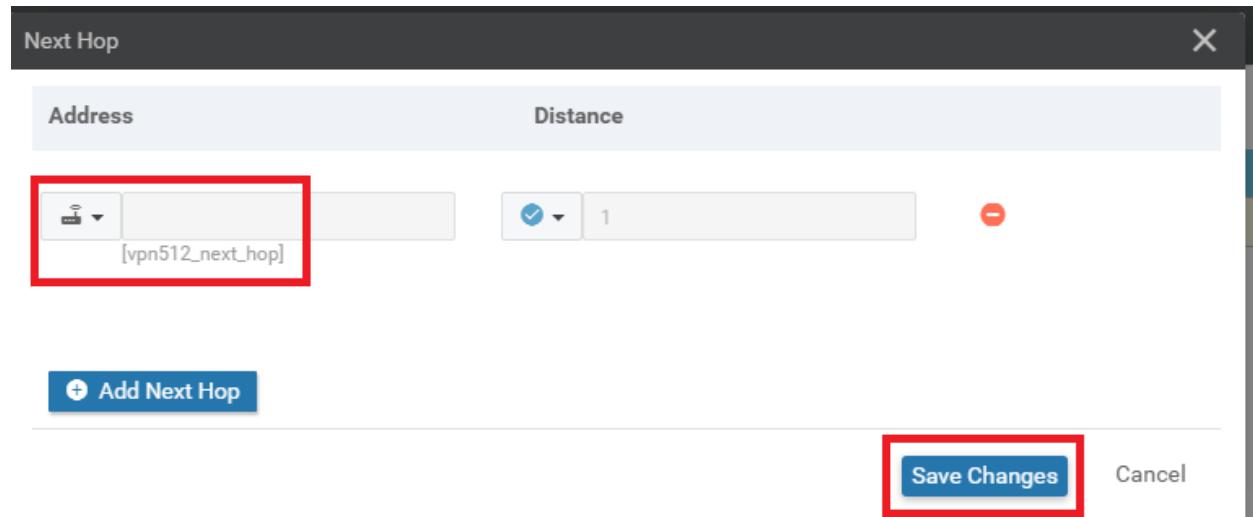
8. Update the Device Specific information for the first entry to `vpn512_next_hop`. Click on **Save Changes**

Next Hop

| Address | Distance |
|--|------------------------|
| <input type="text"/> [vpn512_next_hop] | <input type="text"/> 1 |

Add Next Hop

Save Changes Cancel

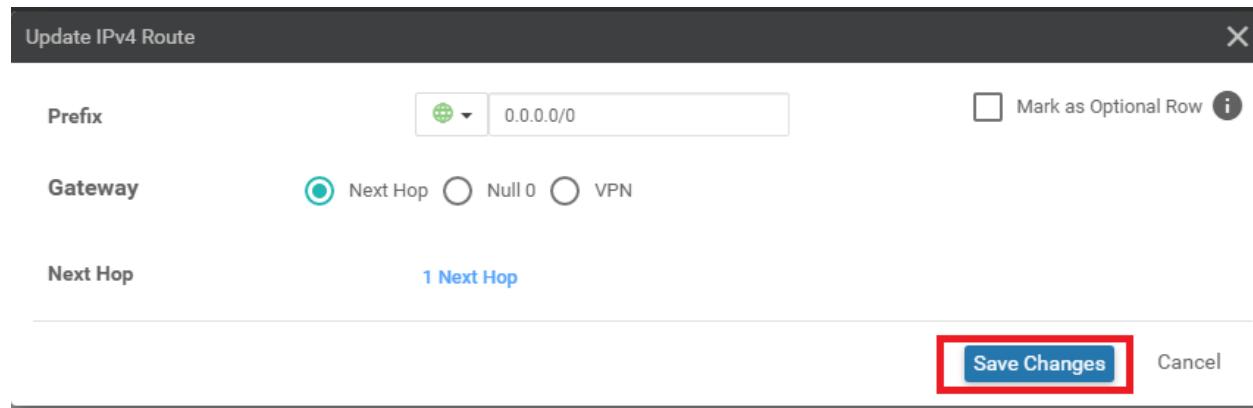


9. Click on **Save Changes** again. The Update IPv4 Route page should now reflect 1 Next Hop

Update IPv4 Route

| | | |
|----------|--|---|
| Prefix | <input type="text"/> 0.0.0.0/0 | <input type="checkbox"/> Mark as Optional Row  |
| Gateway | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN | |
| Next Hop | 1 Next Hop | |

Save Changes Cancel



10. Click on **Update** on the main feature template page to save the changes that we have made. The Selected Gateway Configuration should have the number 1 against it

The screenshot shows the 'IPv4 ROUTE' configuration screen. A modal window is open for 'New IPv4 Route'. In the 'Gateway' section, a dropdown menu labeled 'Selected Gateway Configuration' is open, showing the number '1' with a red box around it. At the bottom right of the modal, there are 'Update' and 'Cancel' buttons, with 'Update' also having a red box around it.

We have created our VPN512 Feature Template

Task List

- Creating the DC-vEdge VPN Feature Templates
- [Creating the VPN0 Feature Template](#)
- [Creating the VPN512 Feature Template](#)
- Creating the INET VPN Interface Feature Template
- Creating the MPLS VPN Interface Feature Template
- Creating the Mgmt VPN Interface Feature Template
- Creating a Device Template and Attaching Devices
- Activity Verification

Creating the INET VPN Interface Feature Template

We are now going to set up the VPN Interface Feature Templates for the Internet link. This template specifies the configuration for the interfaces in a VPN. There will be two interfaces in VPN 0 (INET and MPLS) and one interface in VPN 512. Let's start off with configuring the INET interface.

1. From **Configuration => Templates** on the Feature tab, Add a new template. Search for *ved* in the search box and choose the vEdge Cloud Device. Click on **VPN Interface Ethernet** to start creating our VPN Interface Template

The screenshot shows the 'Feature' tab selected in the top navigation. In the 'Select Devices' section, a search bar contains 'ved'. Below it is a list of vEdge models: vEdge 100, vEdge 100 B, vEdge 100 M, vEdge 100 WM, vEdge 1000, vEdge 2000, and vEdge 5000. The 'vEdge Cloud' option is checked and highlighted with a red box. In the 'Select Template' section, there are two main sections: 'BASIC INFORMATION' and 'VPN'. Under 'BASIC INFORMATION', there are boxes for AAA, Archive, NTP, and OMP. Under 'VPN', there are boxes for Secure Internet Gateway (SIG) WAN, VPN, VPN Interface Cellular WAN, and VPN Interface Ethernet Management|WAN|LAN. The 'VPN Interface Ethernet' box is highlighted with a red box.

2. Populate the details on this page as given below. Screenshots can be used for reference. Click on **Save** once the fields have been populated

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|----------------|---------------------------------------|---|
| | Template Name | NA | <i>DC-vEdge_INET</i> |
| | Description | NA | <i>INET interface for the DC-vEdges</i> |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | <i>vpn0_inet_if_name</i> |
| Basic Configuration | IPv4 Address | Device Specific | <i>vpn0_inet_if_ip</i> |
| Tunnel | Tunnel | Global | On |

| Interface | | | |
|------------------------|-------|-----------------|---------------------------|
| Tunnel | Color | Device Specific | <i>vpn0_inet_if_color</i> |
| Tunnel - Allow Service | All | Global | On |

Feature Template > Add Template > **VPN Interface Ethernet**

| | |
|---------------|----------------------------------|
| Template Name | DC-vEdge_INET |
| Description | INET interface for the DC-vEdges |

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: [vpn0_inet_if_name]

Description:

IPv4 **IPv6**

Dynamic Static

IPv4 Address: [vpn0_inet_if_ip]

TUNNEL

Tunnel Interface On Off

Per-tunnel QoS On Off

Color [vpn0_inet_if_color]

Restrict On Off

Groups

Border On Off

Control Connection On Off

Maximum Control Connections

vBond As Stun Server On Off

Exclude Controller Group List

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > VPN Interface Ethernet

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

Low-Bandwidth Link On Off

Allow Service

All On Off

BGP On Off

DHCP On Off

DNS On Off

ICMP On Off

NETCONF On Off

NTP On Off

OSPF On Off

SSH On Off

This completes the configuration of our INET Interface Feature Template. Notice that we will be populating quite a few details when the Device is attached to a Device Template which contains this Feature Template.

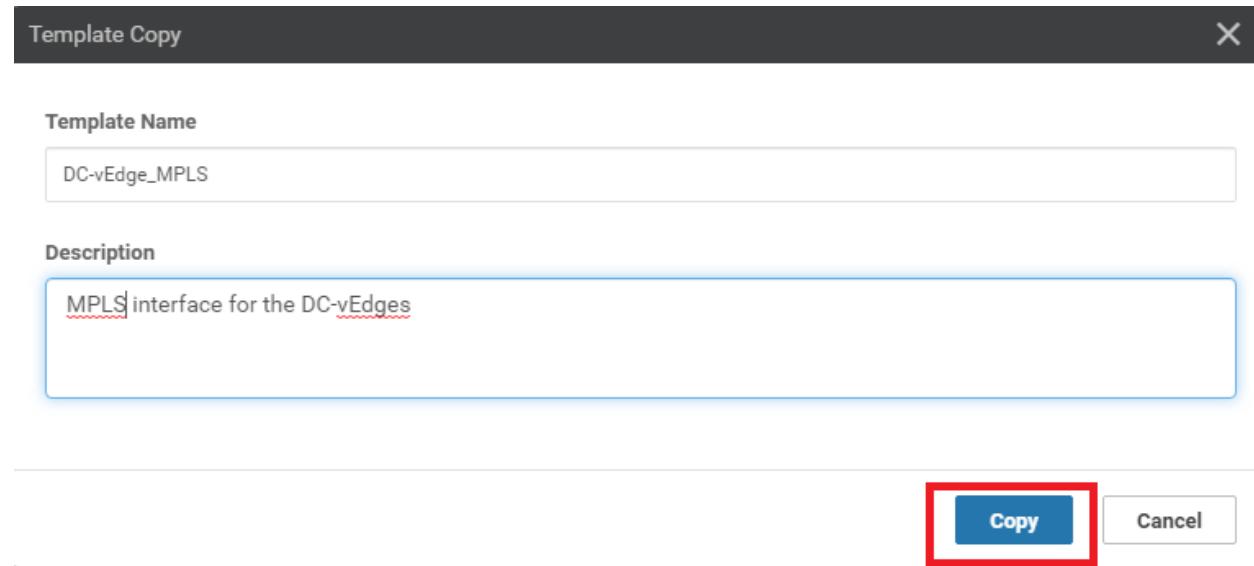
Task List

- [Creating the DC-vEdge VPN Feature Templates](#)
- [Creating the VPN0 Feature Template](#)
- [Creating the VPN512 Feature Template](#)
- [Creating the INET VPN Interface Feature Template](#)
- Creating the MPLS VPN Interface Feature Template
- Creating the Mgmt VPN Interface Feature Template
- Creating a Device Template and Attaching Devices
- Activity Verification

Creating the MPLS VPN Interface Feature Template

We are now going to set up the VPN Interface Feature Template for the MPLS link, making a copy from the INET template that we created in the previous section.

1. Identify the *DC-vEdge_INET* Feature Template from **Configuration => Templates => Feature tab**. Click on the three dots in the extreme right-hand side of the template and click Copy. Name it *DC-vEdge_MPLS* with a Description of *MPLS interface for the DC-vEdges*. Click on **Copy**



2. Click on the 3 dots next to the copied template and choose to **Edit**. Modify the details as per the table given below and click on **Update** (we have changed the Device Specific names to reflect mpls and set the restrict to On)

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|------------------|---------------------------------------|---|
| | Template Name | NA | <i>DC-vEdge_MPLS</i> |
| | Description | NA | <i>MPLS interface for the DC-vEdges</i> |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | <i>vpn0_mpls_if_name</i> |
| Basic Configuration | IPv4 Address | Device Specific | <i>vpn0_mpls_if_ip</i> |
| Tunnel | Tunnel Interface | Global | On |
| Tunnel | Color | Device Specific | <i>vpn0_mpls_if_color</i> |

| | | | |
|--------|----------|--------|----|
| Tunnel | Restrict | Global | On |
|--------|----------|--------|----|

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

BASIC CONFIGURATION

Shutdown: No (highlighted by red box)

Interface Name: [vpn0_mpls_if_name]

Description: [vpn0_mpls_if_color]

IPv4 Address: [vpn0_mpls_if_ip]

Dynamic (radio button) Static (radio button, highlighted by green box)

Basic Configuration **Tunnel** NAT VRRP ACL/QoS ARP 802.1X Advanced

Tunnel Interface: On (highlighted by red box)

Per-tunnel Qos: On Off

Color: [vpn0_mpls_if_color]

Restrict: On (highlighted by red box)

Groups: [vpn0_mpls_if_group]

Border: On Off

Control Connection: On Off

Maximum Control Connections: [5]

vBond As Stun Server: On Off

Exclude Controller Group List: [vpn0_mpls_if_excluded_groups]

vManage Connection Preference: [5]

Update (button highlighted by red box)

This completes the configuration of the MPLS VPN Interface Feature Template.

Task List

- Creating the DC-vEdge VPN Feature Templates
- [Creating the VPN0 Feature Template](#)
- [Creating the VPN512 Feature Template](#)
- [Creating the INET VPN Interface Feature Template](#)
- [Creating the MPLS VPN Interface Feature Template](#)
- Creating the Mgmt VPN Interface Feature Template
- Creating a Device Template and Attaching Devices
- Activity Verification

Creating the Mgmt VPN Interface Feature Template

Just like before, we will make a copy of the DC-vEdge_INET Feature Template and use that for our VPN 512 Management Interface Template.

1. Locate the DC-vEdge_INET template created before, click on the 3 dots at the end and choose to **Copy** the template

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Action |
|--------------------------|-------------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|----------------------|
| cedge-vpn0-int-single | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Templat... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| cEdge_VPN0_dual_uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin | 18 May 2020 7:37:39 AM PDT | ... |
| cEdge_VPN512_dual_uplink | cEdge VPN 512 Template for Dual ... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 8:35:47 AM PDT | ... |
| DC-vEdge_MPLS | MPLS Interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 23 May 2020 1:43:22 AM PDT | ... |
| DC-vEdge_INET | INET interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 23 May 2020 1:39:02 AM PDT | ... |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single ... | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 1:2 | View |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 18 May 2020 8:2 | Edit |
| DCvEdge-vpn512 | VPN512 for the DC-vEdges | WAN Edge VPN | vEdge Cloud | 0 | 0 | admin | 23 May 2020 1:2 | Change Device Models |
| DCvEdge-vpn0 | VPN0 for the DC-vEdges INET and ... | WAN Edge VPN | vEdge Cloud | 0 | 0 | admin | 23 May 2020 1:1 | Delete |

2. Rename it to *DC-vEdge_mgmt_int* with a Description of *MGMT interface for the DC-vEdges*. Click on **Copy**

Template Copy

Template Name

Description

MGMT interface for the DC-vEdges

Copy **Cancel**

3. Click on the 3 dots next to the newly created template and choose to **Edit**. Populate the details in the template as per the following table and click on **Update**. The Tunnel Interface has been set to Off

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|------------------|---------------------------------------|----------------------------------|
| | Template Name | NA | DC-vEdge_mgmt_int |
| | Description | NA | MGMT interface for the DC-vEdges |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | vpn512_mgmt_if_name |
| Basic Configuration | IPv4 Address | Device Specific | vpn512_mgmt_if_ip |
| Tunnel | Tunnel Interface | Global | Off |

Feature Template > VPN Interface Ethernet

| | |
|---------------|----------------------------------|
| Template Name | DC-vEdge_mgmt_int |
| Description | MGMT interface for the DC-vEdges |

This feature template is shared by both Cisco vEdge and IOS-XE SDWAN devices. Please use to IOS-XE SDWAN feature temp

Basic Configuration **Tunnel** **NAT** **VRRP** **ACL/QoS** **ARP** **802.1X** **Advanced**

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: [vpn512_mgmt_if_name]

Description: [vpn512_mgmt_if_desc]

IPv4 IPv6

Dynamic Static

IPv4 Address: [vpn512_mgmt_if_ip]

TUNNEL

Tunnel Interface: On Off

NAT

NAT: On Off

VRRP

IPv4 IPv6

Update **Cancel**

We have created the VPN 512 Interface Template.

Task List

- [Creating the DC vEdge VPN Feature Templates](#)
- [Creating the VPN0 Feature Template](#)
- [Creating the VPN512 Feature Template](#)
- [Creating the INET VPN Interface Feature Template](#)
- [Creating the MPLS VPN Interface Feature Template](#)
- [Creating the Mgmt VPN Interface Feature Template](#)
- [Creating a Device Template and Attaching Devices](#)
- [Activity Verification](#)

Creating a Device Template and Attaching Devices

Most of the work has already been done, with respect to creating the building blocks for our Device Templates. All that's left is ensuring we create a Device Template with the corresponding Feature Templates and associate the Devices with the Template.

1. Navigate to the **Configuration => Templates** section and make sure you're on the **Device** tab. Click on **Create Template => From Feature Template**

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status |
|--------------------------|----------------------------------|---------|--------------|-------------------|------------------|------------|----------------------------|-----------------|
| cEdge_dualuplink_devtemp | cEdge Device Template for de... | Feature | CSR1000v | 11 | 1 | admin | 18 May 2020 8:43:52 AM PDT | In Sync |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync |

2. Choose Device Model as **vEdge Cloud**, and give the Template a name of **DCvEdge_dev_temp**. Give it a Description of *Device template for the DC-vEdges*

| Device | Feature |
|--------------------------|-----------------------------------|
| Device Model | vEdge Cloud |
| Template Name | DCvEdge_dev_temp |
| Description | Device template for the DC-vEdges |
| Basic Information | Transport & Management VPN |
| Service VPN | Additional Templates |

Basic Information

3. Under **Transport and Management** choose the VPN 0 template as *DCvEdge-vpn0* and the VPN 512 Template as *DCvEdge-vpn512*. Click twice on **VPN Interface** under *Additional VPN 0 Templates*. This will add two VPN Interfaces where we can associate our VPN Interface Templates. Click once on **VPN Interface** under *Additional VPN 512 Templates* to add a VPN Interface for VPN 512

| Transport & Management VPN | |
|------------------------------|--|
| VPN 0 * | DCvEdge-vpn0 |
| Additional VPN 0 Templates | <ul style="list-style-type: none"> <input type="radio"/> BGP <input type="radio"/> OSPF <input checked="" type="radio"/> Secure Internet Gateway <input checked="" type="radio"/> VPN Interface Click Twice <input type="radio"/> VPN Interface Cellular <input type="radio"/> VPN Interface GRE <input type="radio"/> VPN Interface IPsec <input type="radio"/> VPN Interface PPP |
| VPN 512 * | DCvEdge-vpn512 |
| Additional VPN 512 Templates | <ul style="list-style-type: none"> <input checked="" type="radio"/> VPN Interface Click Once |

4. Populate the VPN Interface fields from the drop down as show below and click on **Create**

Transport & Management VPN

VPN 0 * DCvEdge-vpn0

VPN Interface DC-vEdge_INET

VPN Interface DC-vEdge_MPLS

VPN 512 * DCvEdge-vpn512

VPN Interface DC-vEdge_mgmt_int

Additional VPN 0 Templates

- BGP
- OSPF
- Secure Internet Gateway
- VPN Interface
- VPN Interface Cellular
- VPN Interface GRE
- VPN Interface IPsec
- VPN Interface PPP

Additional VPN 512 Templates

- VPN Interface

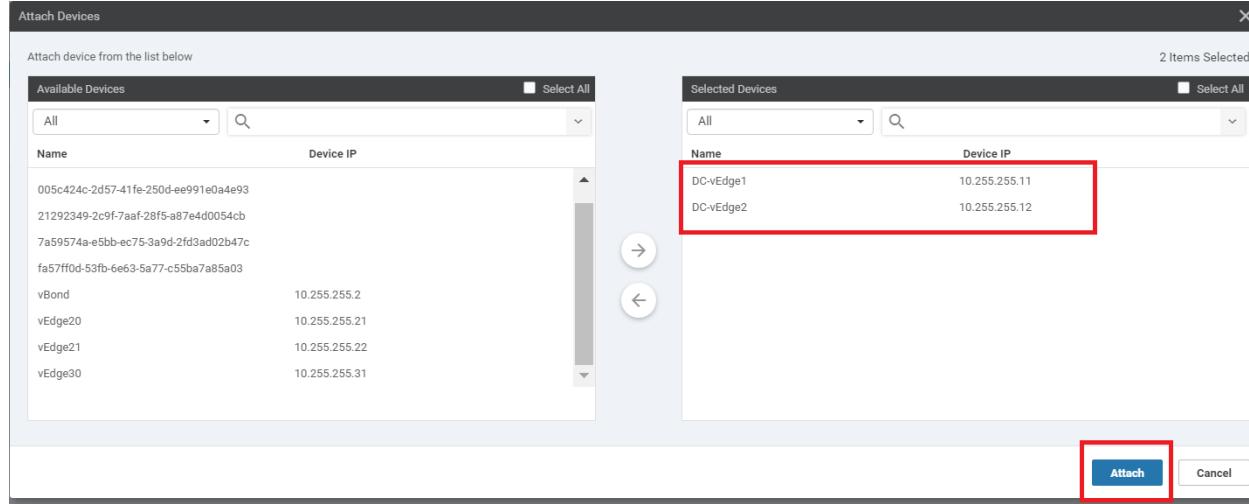
Create **Cancel**

5. Click on the three dots next to the newly created Device Template named *DCvEdge_dev_temp* and click on **Attach Devices**

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status |
|--------------------------|----------------------------------|---------|--------------|-------------------|------------------|------------|----------------------------|-----------------|
| cEdge_dualuplink_devtemp | cEdge Device Template for d... | Feature | CSR100v | 11 | 1 | admin | 18 May 2020 8:43:52 AM PDT | In Sync |
| cEdge-singleuplink | Single Uplink cEdge Device Te... | Feature | CSR100v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 11 | 0 | admin | 23 May 2020 1:55:53 AM PDT | In Sync |

Attach Devices

6. Move **DC-vEdge1** and **DC-vEdge2** to the list of selected devices and click on **Attach**



7. Click on the three dots next to DC-vEdge1 and choose **Edit Device Template**. Enter the details as shown below (these are the Device Specific parameters we had defined in the Feature Templates, along with some parameters that are part of the Default Templates pre-populated in the Device Template). Click on **Update** once everything has been populated exactly as shown below. This information can also be picked up from the table given in the topology section

Update Device Template

Variable List (Hover over each field for more information)

| | |
|-------------------------------------|--------------------------------------|
| Chassis Number | e474c5fd-8ce7-d376-7cac-ba950b2c9159 |
| System IP | 10.255.255.11 |
| Hostname | DC-vEdge1 |
| Address(vpn512_next_hop) | 192.168.0.1 |
| Interface Name(vpn512_mgmt_if_name) | eth0 |
| IPv4 Address(vpn512_mgmt_if_ip) | 192.168.0.10/24 |
| Address(vpn0_inet_next_hop) | 100.100.100.1 |
| Address(vpn0_mpls_next_hop) | 192.0.2.1 |
| Interface Name(vpn0_mpls_if_name) | ge0/1 |
| IPv4 Address(vpn0_mpls_if_ip) | 192.0.2.2/30 |
| Color(vpn0_mpls_if_color) | mpls |
| Interface Name(vpn0_inet_if_name) | ge0/0 |
| IPv4 Address(vpn0_inet_if_ip) | 100.100.100.10/24 |
| Color(vpn0_inet_if_color) | public-internet |
| Hostname | DC-vEdge1 |
| System IP | 10.255.255.11 |
| Site ID | 1 |

Generate Password **Update** (Red Box) **Cancel**

8. Click on the three dots next to DC-vEdge2 and choose **Edit Device Template**. Enter the details as shown below. Click on **Update** once done

Update Device Template X

Variable List (Hover over each field for more information)

| | |
|-------------------------------------|--------------------------------------|
| Chassis Number | 0cdd4f0e-f2f1-fe75-866c-469966cda1c3 |
| System IP | 10.255.255.12 |
| Hostname | DC-vEdge2 |
| Address(vpn512_next_hop) | 192.168.0.1 |
| Interface Name(vpn512_mgmt_if_name) | eth0 |
| IPv4 Address(vpn512_mgmt_if_ip) | 192.168.0.11/24 |
| Address(vpn0_inet_next_hop) | 100.100.100.1 |
| Address(vpn0_mpls_next_hop) | 192.0.2.5 |
| Interface Name(vpn0_mpls_if_name) | ge0/1 |
| IPv4 Address(vpn0_mpls_if_ip) | 192.0.2.6/30 |
| Color(vpn0_mpls_if_color) | mpls |
| Interface Name(vpn0_inet_if_name) | ge0/0 |
| IPv4 Address(vpn0_inet_if_ip) | 100.100.100.11/24 |
| Color(vpn0_inet_if_color) | public-internet |
| Hostname | DC-vEdge2 |
| System IP | 10.255.255.12 |
| Site ID | 1 |

Generate Password Update Cancel

Click on **Next** to proceed

9. At this point, you can simply click on **Configure Devices** to start pushing the configuration to the devices, or you can click on an individual device on the left-hand side and followed by Config Diff and then Side by Side to view a comparison of the current configuration on the device vs. what will be pushed out. This is great for reviewing the configuration that is going to be pushed and for learning the syntax. Note that we are adding the MPLS interface and relevant configuration on our devices, which wasn't done before.

Cisco vManage

CONFIGURATION | TEMPLATES

Device Template Total 1

DCvEdge_dev_temp

Device list (Total: 2 devices)

Filter/Search

Configure **Config Diff**

'Configure' action will be applied to 2 device(s) attached to 1 device template(s).

Local Configuration vs. New Configuration

```

1 no config
2 config
3 system
4 personality vedge
5 device-model vedge-cloud
6 chassis-number e74c5fd-9ce7-d376-7cac-be950b2c9159
7 host-name DC-vEdge1
8 system-ip 10.255.255.11
9 domain-id 1
10 site-id 1
11 admin-tech-on-failure
12 no route-consistency-check
13 organization-name swat-swanlab
14 organization-name swat-swanlab
15 vbond 100.100.100.3
16 vbond 100.100.100.3 port 12346
17 aaa
18 auth-order local radius tacacs
19 usergroup basic
20 task system read write
21 task interface read write
22 !
23 usergroup netadmin
24 usergroup operator
25 task system read
26 task interface read
27 !
28 usergroup netadmin
29 !
30 usergroup operator
31 task system read
32 task interface read
33 !
34 !
35 !
36 !
37 !
38 !
39 !
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 !
49 !
50 !
51 !
52 !
53 !
54 !
55 color public-internet
56 allow-service all
57 no allow-service bgp
58 allow-service dhcp
59 allow-service dns
60 allow-service icmp
61 no allow-service sshd
62 no allow-service netconf
63 no allow-service ntp
64 no allow-service ospf
65 no allow-service stun
66 allow-service https
67 !
68 no shutdown
69 !
70 interface ge0/1
71 ip address 192.0.2.2/30
72 tunnel-interface
73 encapsulation ipsec
74 color mpls restrict
75 allow-service all
76 no allow-service bgp
77 allow-service dhcp
78 allow-service dns
79 allow-service icmp
80 no allow-service sshd
81 no allow-service netconf
82 no allow-service ntp
83 no allow-service ospf
84 no allow-service stun
85 allow-service https
86 !

```

Side By Side Diff Intent

Cisco vManage

CONFIGURATION | TEMPLATES

Device Template Total 1

DCvEdge_dev_temp

Device list (Total: 2 devices)

Filter/Search

Configure action will be applied to 2 device(s) attached to 1 device template(s).

hello-tolerance 12

```

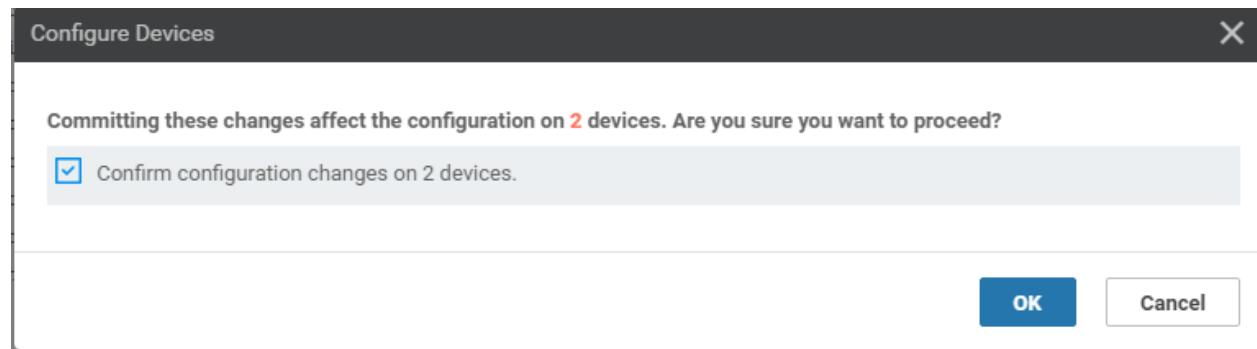
55 color public-internet
56 allow-service all
57 no allow-service bgp
58 allow-service dhcp
59 allow-service dns
60 allow-service icmp
61 no allow-service sshd
62 no allow-service netconf
63 no allow-service ntp
64 no allow-service ospf
65 no allow-service stun
66 allow-service https
67 !
68 no shutdown
69 !
70 interface ge0/1
71 ip address 192.0.2.2/30
72 tunnel-interface
73 encapsulation ipsec
74 color mpls restrict
75 allow-service all
76 no allow-service bgp
77 allow-service dhcp
78 allow-service dns
79 allow-service icmp
80 no allow-service sshd
81 no allow-service netconf
82 no allow-service ntp
83 no allow-service ospf
84 no allow-service stun
85 allow-service https
86 !

```

Configure Device Rollback Timer

Back Configure Devices Cancel

10. On clicking on **Configure Devices**, you will need to put a check mark next to **Confirm configuration changes on 2 devices** and click on **OK**



11. Once complete, you should see a **Success** message against each device that was configured

| Push Feature Template Configuration Validation Success Initiated By: admin | | | | | | | | |
|--|--|----------------|---------------|----------|--------------|---------|------------|--|
| Total Task: 2 Success : 2 | | | | | | | | |
| <input type="text"/> Q Search Options ▾ | | | | | | | | |
| Status | Message | Chassis Number | Device Model | Hostname | System IP | Site ID | vManage IP | |
| > Success | Done - Push Feature Template Co... e474c5fd-8ce7-d376-7cac-6a950... vEdge Cloud | DC-vEdge1 | 10.255.255.11 | 1 | 10.255.255.1 | | | |
| > Success | Done - Push Feature Template Co... 0cdd4f0e-f2f1-fe75-866c-469966... vEdge Cloud | DC-vEdge2 | 10.255.255.12 | 1 | 10.255.255.1 | | | |

Tip: In case a loss of connectivity occurs as a result of the configuration changes that were pushed to the Devices, there is an automatic rollback timer of 6 minutes which kicks in. Devices will revert to their previous configuration in this case. The rollback timer can be configured (on the final page before we choose to configure our devices, there is a hyperlink in the bottom left hand corner)

Task List

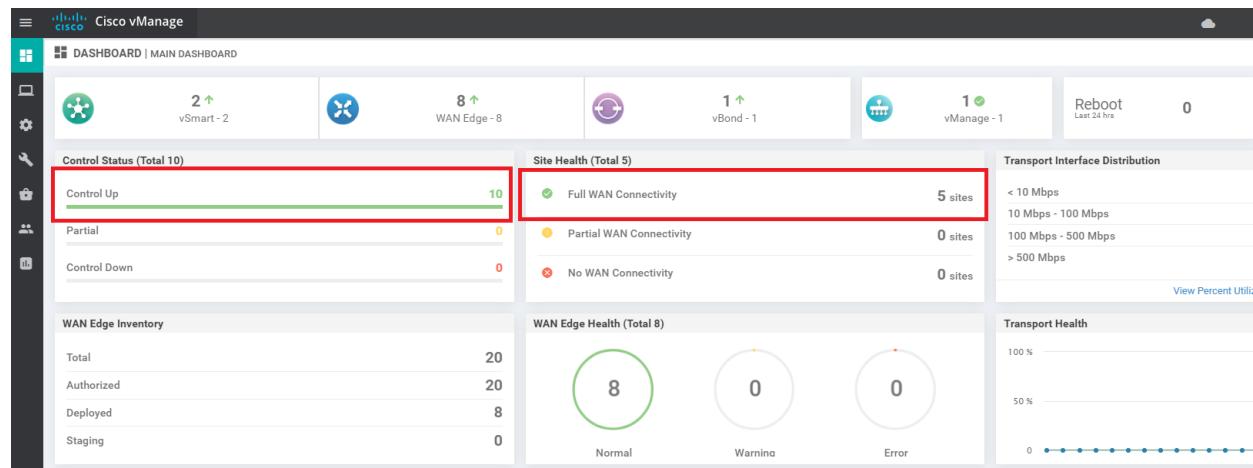
- [Creating the DC-vEdge VPN Feature Templates](#)
- [Creating the VPN0 Feature Template](#)
- [Creating the VPN512 Feature Template](#)
- [Creating the INET VPN Interface Feature Template](#)
- [Creating the MPLS VPN Interface Feature Template](#)
- [Creating the Mgmt VPN Interface Feature Template](#)
- [Creating a Device Template and Attaching Devices](#)
- [Activity Verification](#)

Activity Verification

1. Go to Configuration => Devices and you should see that the two DC-vEdges are now in vManage mode

| State | Device Model | Chassis Number | Serial No./Token | Enterprise Cert Serial No | Enterprise Cert Expiration Date | Hostname | System IP | Site ID | Mode | Assigned Template | Actions | | |
|-------------|---------------------------------------|------------------------------------|--------------------------|---------------------------|---------------------------------|---------------|---------------|---------|------------------|--------------------------|---------|-----|-----|
| | | | | | | | | | | | ... | ... | ... |
| CSR1000v | CSR-44C7CE5A-4149-E696-C8A8-415C... | CSR-D60B39FC-C383-BB55-7E9D-7CD... | Token - fc40de6570e72... | NA | NA | --- | --- | --- | CLI | -- | ... | ... | ... |
| CSR1000v | CSR-834E40DC-E358-8DE1-0E81-76E59... | FATF272A | NA | NA | NA | cEdge450 | 10.255.255.51 | 50 | vManage | cEdge-single-uplink | ... | ... | ... |
| CSR1000v | CSR-D405F5BA-B975-8944-D1A3-2E08... | Token - e78aaefc1ebd2... | NA | NA | NA | --- | --- | --- | CLI | -- | ... | ... | ... |
| CSR1000v | CSR-D1837F36-6A7A-1850-7C1C-E1C6... | F8FD7C382 | NA | NA | NA | cEdge51 | 10.255.255.52 | 50 | vManage | cEdge-single-uplink | ... | ... | ... |
| CSR1000v | CSR-5E992295-1362-0DB6-EEF8-25CC... | Token - 1da14330e171... | NA | NA | NA | --- | --- | --- | CLI | -- | ... | ... | ... |
| CSR1000v | CSR-04F9482E-44F0-E40C-3D0D-60C0... | 63201C50 | NA | NA | NA | cEdge40 | 10.255.255.41 | 40 | vManage | cEdge_dualuplink_deve... | ... | ... | ... |
| vEdge Cloud | e474c5f0-8ce7-d376-7cac-ba950b2c91... | 7175AEOF | NA | NA | DC-Edge1 | 10.255.255.11 | 1 | vManage | DCvEdge_dev_temp | ... | ... | ... | ... |
| vEdge Cloud | 0cd4f0e-f2f1-f67-866c-469966cda1c3 | 7DA605F5 | NA | NA | DC-Edge2 | 10.255.255.12 | 1 | vManage | DCvEdge_dev_temp | ... | ... | ... | ... |
| vEdge Cloud | b7fd7295-58df-7671-e914-6f2edff160... | 297060DD | NA | NA | vEdge20 | 10.255.255.21 | 20 | CLI | -- | ... | ... | ... | ... |
| vEdge Cloud | dd60ff0-dc62-77e6-510f-08d9660b537d | 88FD4E65 | NA | NA | vEdge21 | 10.255.255.22 | 20 | CLI | -- | ... | ... | ... | ... |

2. On checking the main dashboard (**Dashboard => Main Dashboard**) we should see 5 sites with full WAN connectivity
(if you recall, we previously could see only 4 sites with full WAN connectivity and Site 50 wasn't showing up at all. This was because BFD sessions weren't established on the MPLS link)



3. If we click on **Full WAN Connectivity**, Site 50 now shows up

| Site Devices Health: Full WAN Connectivity | | | | | | |
|--|--------------|---------------|---------|--------------|----------------------------|-----|
| Search Options | | | | | | |
| Hostname | Reachability | System IP | Site ID | BFD Sessions | Last Updated | |
| DC-vEdge1 | reachable | 10.255.255.11 | 1 | 6 | 23 May 2020 2:34:53 AM PDT | ... |
| vEdge21 | reachable | 10.255.255.22 | 20 | 5 | 23 May 2020 2:22:45 AM PDT | ... |
| vEdge20 | reachable | 10.255.255.21 | 20 | 5 | 23 May 2020 2:22:45 AM PDT | ... |
| DC-vEdge2 | reachable | 10.255.255.12 | 1 | 6 | 23 May 2020 2:35:31 AM PDT | ... |
| vEdge30 | reachable | 10.255.255.31 | 30 | 6 | 23 May 2020 2:22:45 AM PDT | ... |
| cEdge51 | reachable | 10.255.255.52 | 50 | 2 | 23 May 2020 2:35:33 AM PDT | ... |
| cEdge50 | reachable | 10.255.255.51 | 50 | 6 | 23 May 2020 2:22:46 AM PDT | ... |
| cEdge40 | reachable | 10.255.255.41 | 40 | 6 | 23 May 2020 2:22:46 AM PDT | ... |

4. Use Putty to access **cEdge51** and issue `show bfd sessions`. We now see BFD sessions with DC-vEdge1 and DC-vEdge2, on the MPLS link

| TECT | TX | SOURCE TLOC | REMOTE TLOC | DST PUBLIC | DST PUBLIC | DE | | | |
|---------------|----------------|-------------|-------------|------------|------------|-----------|-------|-------|----|
| SYSTEM IP | SITE ID | STATE | COLOR | COLOR | SOURCE IP | IP | PORT | ENCAP | MU |
| LTIPLIER | INTERVAL(msec) | UPTIME | TRANSITIONS | | | | | | |
| 10.255.255.11 | 1 | up | mpls | mpls | 192.1.2.22 | 192.0.2.2 | 12406 | ipsec | 7 |
| 1000 | | 0:00:06:24 | 0 | | | | | | |
| 10.255.255.12 | 1 | up | mpls | mpls | 192.1.2.22 | 192.0.2.6 | 12406 | ipsec | 7 |
| 1000 | | 0:00:05:47 | 0 | | | | | | |

This completes the verification activity

Task List

- [Creating the DC-vEdge VPN Feature Templates](#)
- [Creating the VPN0 Feature Template](#)
- [Creating the VPN512 Feature Template](#)
- [Creating the MPLS VPN Interface Feature Template](#)
- [Creating the MPLS VPN Interface Feature Template](#)
- [Creating the Mgmt VPN Interface Feature Template](#)
- [Creating a Device Template and Attaching Devices](#)
- [Activity Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 21, 2020

Site last generated: Jul 23, 2020



Templates for vEdges in Site 20

Summary: Create Feature and Device Templates for the Site 20 vEdges

Table of Contents

- [Overview](#)
- [Creating the Site 20 Feature Templates
 - \[Creating the VPNO Feature Template\]\(#\)
 - \[Creating the INET and MPLS VPN Interface Feature Template\]\(#\)](#)
- [Modifying a Device Template and Attaching Devices](#)

Task List

- Creating the Site 20 Feature Templates
 - Creating the VPNO Feature Template
 - Creating the INET and MPLS VPN Interface Feature Template
- Modifying a Device Template and Attaching Devices

Overview

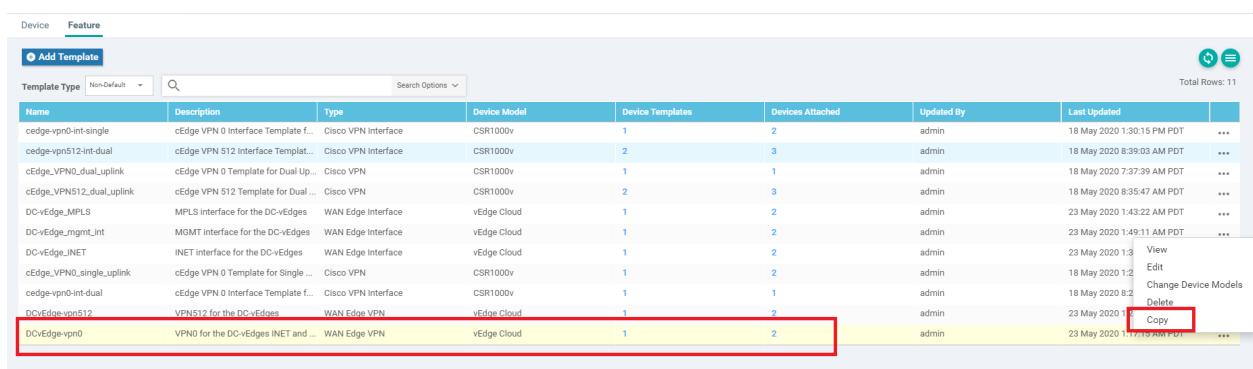
We can take the Feature Templates created for the DC-vEdges and use them as a starting point for configuring the Feature Templates at Site 20. Necessary changes based on the topology will need to be made (for example, things like a single uplink at the Site20 devices vs. a dual uplink at the DC devices)

Creating the Site 20 Feature Templates

Creating the VPN0 Feature Template

We will set up the VPN templates for VPN 0 in Site 20 by making a copy of the *DCvEdge-vpn0* Feature Template created before

1. Identify the *DCvEdge-vpn0* Feature Template from **Configuration => Templates => Feature tab**. Click on the three dots in the extreme right-hand side of the template and click Copy. Name it *Site20-vpn0* with a Description of *VPN0 for the Site 20 vEdges*. Click on **Copy** again



| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------|-------------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|----------------------|
| cedge-vpn0-int-single | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Templat... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| cEdge_VPN0_dual_Uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin | 18 May 2020 7:37:39 AM PDT | ... |
| cEdge_VPN512_dual_Uplink | cEdge VPN 512 Template for Dual ... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 8:35:47 AM PDT | ... |
| DCvEdge_MPLS | MPLS interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:43:22 AM PDT | ... |
| DCvEdge_mgmt_int | MGMT interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:49:11 AM PDT | ... |
| DCvEdge_INET | INET interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:3 | View |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single ... | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 1:2 | Edit |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 18 May 2020 8:2 | Change Device Models |
| DCvEdge-vnn512 | VNN512 for the DC-vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1: | Delete |
| DCvEdge-vpn0 | VPN0 for the DC-vEdges INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:17:30 AM PDT | Copy |



Template Name
Site20-vpn0

Description
VPN0 for the Site 20 vEdges

Copy Cancel

2. Locate the *Site20-vpn0* template just created and click on the three dots at the end of it. Click on **Edit**. Identify the IPv4 Route section - there should be a route populated there for 0.0.0.0/0. Edit this route by clicking on the **pencil** icon

| IPv4 ROUTE | | | | |
|--------------------------|---|----------|--------------------------------|---|
| New IPv4 Route | | Gateway | Selected Gateway Configuration | Action |
| Optional | Prefix | Next Hop | 2 | <input checked="" type="checkbox"/>  |
| <input type="checkbox"/> |  0.0.0.0 | Next Hop | 2 | |

3. Click on 2 Next Hop

Update IPv4 Route X

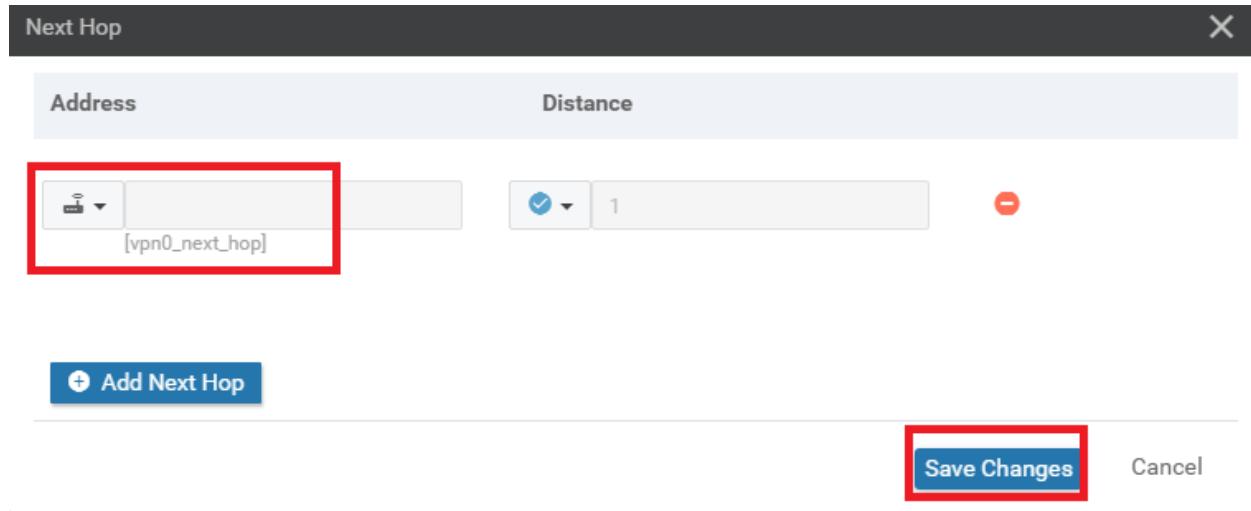
| | | |
|---|--|---|
| Prefix |  0.0.0.0 | <input type="checkbox"/> Mark as Optional Row  |
| Gateway | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN | |
| Next Hop | 2 Next Hop | |
| <input style="margin-right: 10px;" type="button" value="Save Changes"/> <input type="button" value="Cancel"/> | | |

4. Click on the remove icon for the second next hop

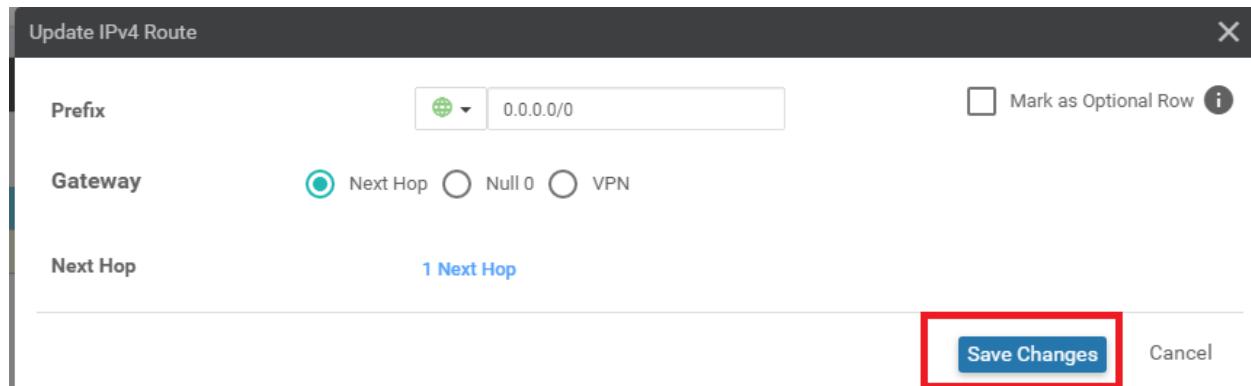
Next Hop X

| Address | Distance | |
|--|---|---|
|  [vpn0_inet_next_hop] |  1 |  |
|  [vpn0_mpls_next_hop] |  1 |  |
| <input style="margin-bottom: 10px;" type="button" value="Add Next Hop"/> <input style="margin-right: 10px;" type="button" value="Save Changes"/> <input type="button" value="Cancel"/> | | |

5. Edit the name of the INET next hop to represent something more generic, like `vpn0_next_hop`. We will use this VPNO Template for both the vEdges at Site 20. Click on **Save Changes**



6. Make sure there is just 1 **Next Hop** populated and click on **Save Changes** again



7. Click on **Update** on the main Feature Template screen

The screenshot shows the 'IPv4 Route' and 'IPv6 Route' sections of the configuration interface. In the IPv4 Route section, a new route is being created with the prefix '0.0.0.0/0'. In the IPv6 Route section, an update operation is in progress.

This completes the configuration of the VPN 0 Feature Template for Site 20.

Task List

- Creating the Site 20 Feature Templates
 - [Creating the VPN0 Feature Template](#)
 - Creating the INET and MPLS VPN Interface Feature Template
 - Modifying a Device Template and Attaching Devices

[Creating the INET and MPLS VPN Interface Feature Template](#)

We will copy and edit the *DC-vEdge_MPLS* Interface Feature Template for our INET and MPLS VPN Interface Feature Templates at Site 20.

1. Navigate to the **Configuration => Templates** section and make sure you're on the **Feature** tab. Click on the three dots next to the *DC-vEdge_MPLS* and click on **Copy**

| | | | | | | | | |
|--------------------------|-------------------------------------|---------------------|-------------|---|---|-------|----------------------------|--------------------------------------|
| DC-Edge_mgmt_int | MGMT interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:49:11 AM PDT | ... |
| DC-Edge_MPLS | MPLS interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:43:22 AM PDT | ... |
| DC-vEdge_INET | INET interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:3 | View |
| DCvEdge-vpn512 | VPNs12 for the DC-vEdges | WAN Edge VPN | vEdge VPN | 1 | 2 | admin | 23 May 2020 1:2 | Edit |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single ... | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 1:2 | Change Device Models |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 18 May 2020 8:2 | Delete |
| DCvEdge-vpn0 | VPN0 for the DC-vEdges INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:1 | Copy |

2. Rename the Template to **Site20_vpn0_int** and the Description as **VPN0 Interface for Site20 devices**. Click on **Copy**

Template Copy

Template Name
Site20_vpn0_int

Description
VPN0 Interface for Site20 devices

Copy **Cancel**

3. Edit the newly created template by clicking on the 3 dots next to it and choosing Edit. Update the details as per the table below, referencing the screenshots. Click on **Update** once done

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|---------------|---------------------------------------|--|
| | Template Name | NA | <i>Site20_vpn0_int</i> |
| | Description | NA | <i>VPN0 Interface for Site20 devices</i> |
| Basic Configuration | Shutdown | Global | No |
| Basic | Interface | Device Specific | <i>vpn0_if_name</i> |

| Configuration | Name | | |
|------------------------|--------------|-----------------|-------------------------------|
| Basic Configuration | IPv4 Address | Device Specific | <i>vpn0_if_ip_addr</i> |
| Tunnel Interface | Tunnel | Global | On |
| Tunnel Color | Color | Device Specific | <i>vpn0_if_color</i> |
| Tunnel Restrict | Restrict | Device Specific | <i>vpn0_if_color_restrict</i> |
| Tunnel - Allow Service | All | Global | On |

Feature Template > **VPN Interface Ethernet**

| | |
|---------------|-----------------------------------|
| Template Name | Site20_vpn0_int |
| Description | VPN0 Interface for Site20 devices |

This feature template is shared by both Cisco vEdge and IOS-XE SDWAN devices. Please use the [Template Migration](#) tool to migrate the vEdge feature templates to IOS-XE SDWAN feature templates.

Basic Configuration [Tunnel](#) [NAT](#) [VRRP](#) [ACL/QoS](#) [ARP](#) [802.1X](#) [Advanced](#)

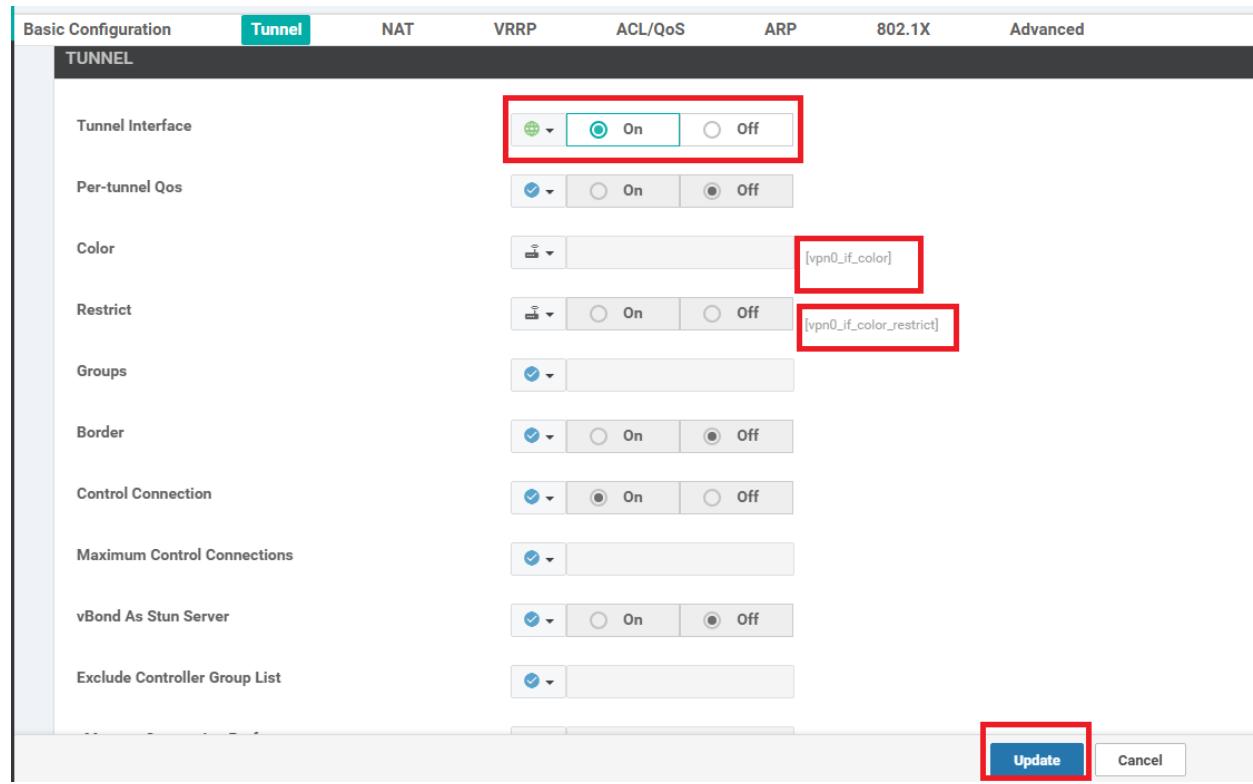
BASIC CONFIGURATION

| | |
|----------------|---|
| Shutdown | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Interface Name | <input type="text"/> [vpn0_if_name] |
| Description | <input type="text"/> |

[IPv4](#) [IPv6](#)

Dynamic Static

IPv4 Address



We have completed configuring the VPN 0 Interface Template for the Site 20 Devices. This template will be used for the INET and MPLS links at Site 20. Notice how easy it has become to add configuration, once the initial template has been built?

Task List

- [Creating the Site 20 Feature Templates](#)
- [Creating the VPN0 Feature Template](#)
- [Creating the INET and MPLS VPN Interface Feature Template](#)
- [Modifying a Device Template and Attaching Devices](#)

Modifying a Device Template and Attaching Devices

1. Go to **Configuration => Templates** and make sure you're on the Device tab. Click on the three dots next to the **DCvEdge_dev_temp**. Click on **Copy**

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Actions |
|--------------------------|----------------------------------|---------|--------------|-------------------|------------------|------------|----------------------------|-----------------|---------|
| cEdge_dualuplink_devtemp | cEdge Device Template for de... | Feature | CSR1000v | 11 | 1 | admin | 18 May 2020 8:43:52 AM PDT | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync | ... |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 11 | 2 | admin | 23 May 2020 1:55:53 AM PDT | In Sync | ... |

2. Rename the Template **vEdge_Site20_dev_temp** and give it a Description of *Device template for the Site 20 vEdges*. Click on **Copy**

Template Copy

Template Name
vEdge_Site20_dev_temp

Description
Device template for the Site 20 vEdges

Copy Cancel

3. Click on the three dots next to the newly created template and click on **Edit**. Update the **Transport and Management VPN** section as per the screenshot below. Remember to remove the 2nd VPN Interface under VPN 0. We will be re-using the VPN 512 Templates created for the DC-vEdges.

Cisco vManage

CONFIGURATION | TEMPLATES

Basic Information Transport & Management VPN Service VPN Additional Templates

Transport & Management VPN

VPN 0 *

VPN Interface Site20_vpn0

VPN Interface Site20_vpn0_int

VPN Interface DC-vEdge_MPLS

Click here to remove

VPN 512 *

DCvEdge-vpn512

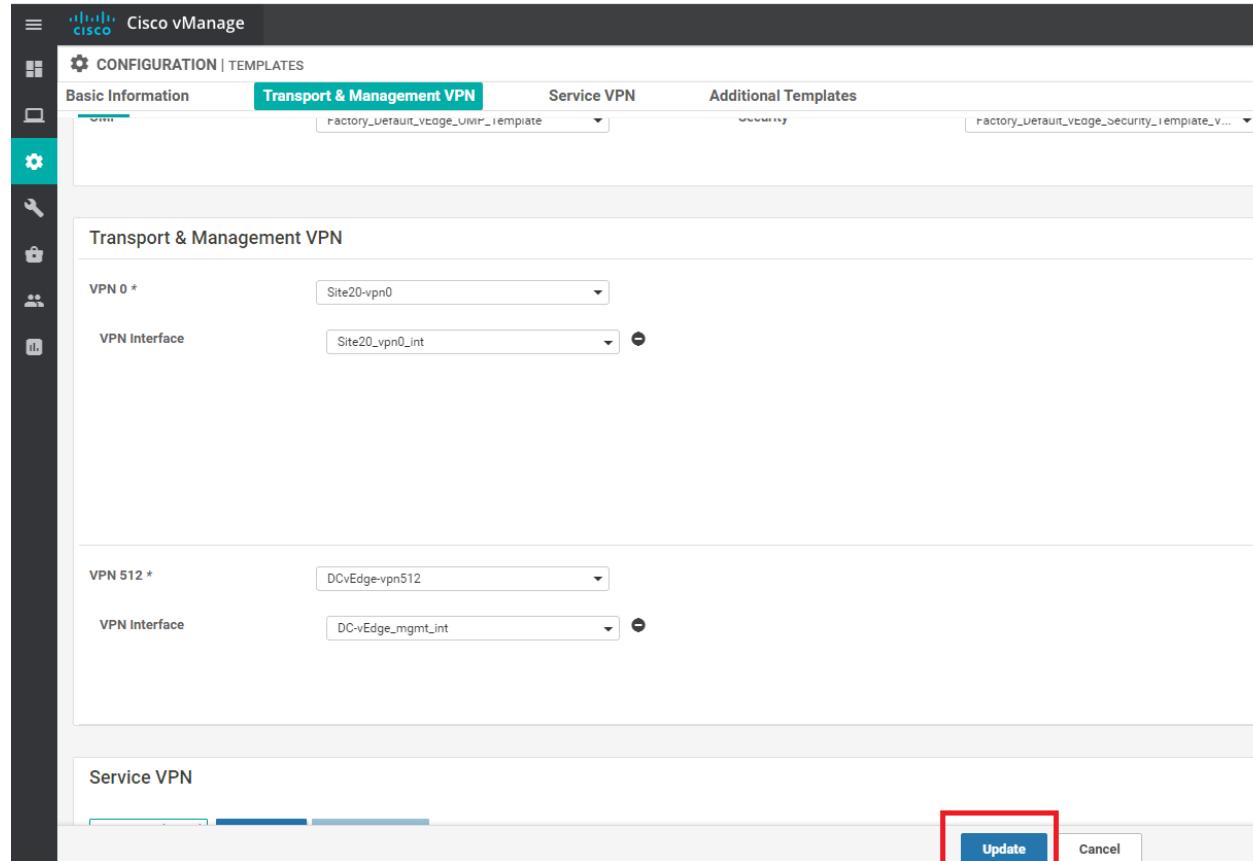
VPN Interface DC-vEdge_mgmt_int

Re-using the DC templates for VPN512

Service VPN

Update Cancel

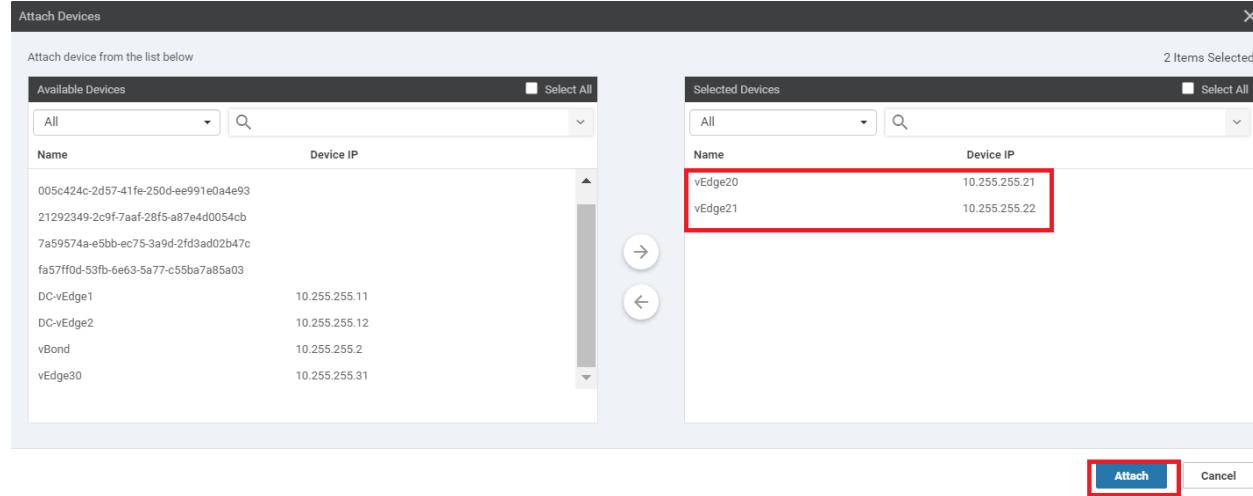
4. Click on **Update** once done



5. Click on the three dots next to the newly created `vEdge_Site20_dev_temp` Template and click on **Attach Devices**

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Actions |
|------------------------------|-----------------------------------|---------|--------------|-------------------|------------------|------------|----------------------------|-----------------|--|
| cEdge_dualuplink_devtemp | cEdge Device Template for de... | Feature | CSR1000v | 11 | 1 | admin | 18 May 2020 8:43:52 AM PDT | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the Site 2... | Feature | vEdge Cloud | 10 | 0 | admin | 23 May 2020 5:53:51 AM PDT | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync | ... |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 11 | 2 | admin | 23 May 2020 1:55:53 AM PDT | In Sync | <ul style="list-style-type: none">EditViewDeleteCopyAttach DevicesExport CSV |

6. Choose **vEdge20** and **vEdge21** from the list and click on **Attach**



7. The two devices should show up in the list. Click on the three dots next to vEdge20 and choose to **Edit Device Template**. Populate the details as shown below and click on **Update**

Update Device Template

Variable List (Hover over each field for more information)

| | |
|--------------------------------------|--------------------------------------|
| Chassis Number | b7fd7295-58df-7671-e914-6fe2edff1609 |
| System IP | 10.255.255.21 |
| Hostname | vEdge20 |
| Address(vpn512_next_hop) | 192.168.0.1 |
| Interface Name(vpn512_mgmt_if_name) | eth0 |
| IPv4 Address(vpn512_mgmt_if_ip_addr) | 192.168.0.20/24 |
| Address(vpn0_next_hop) | 100.100.100.1 |
| Interface Name(vpn0_if_name) | ge0/0 |
| IPv4 Address(vpn0_if_ip_addr) | 100.100.100.20/24 |
| Color(vpn0_if_color) | public-internet |
| Restrict(vpn0_if_color_restrict) | <input type="checkbox"/> |
| Hostname | vEdge20 |
| System IP | 10.255.255.21 |
| Site ID | 20 |

Generate Password **Update** **Cancel**

8. Similarly, click on the dots next to vEdge21 and choose to **Edit Device Template**. Populate the details as shown below and click on **Update**

Update Device Template X

Variable List (Hover over each field for more information)

| | |
|-------------------------------------|--------------------------------------|
| Chassis Number | dde90ff0-dc62-77e6-510f-08d96608537d |
| System IP | 10.255.255.22 |
| Hostname | vEdge21 |
| Address(vpn512_next_hop) | 192.168.0.1 |
| Interface Name(vpn512_mgmt_if_name) | eth0 |
| IPv4 Address(vpn512_mgmt_ip_add) | 192.168.0.21/24 |
| Address(vpn0_next_hop) | 192.0.2.9 |
| Interface Name(vpn0_if_name) | ge0/0 |
| IPv4 Address(vpn0_if_ip_add) | 192.0.2.10/30 |
| Color(vpn0_if_color) | mpls |
| Restrict(vpn0_if_color_restrict) | <input checked="" type="checkbox"/> |
| Hostname | vEdge21 |
| System IP | 10.255.255.22 |
| Site ID | 20 |

Generate Password **Update** **Cancel**

9. Both devices should now have a check mark next to them. Click on **Next**

Device Template | vEdge_Site20_dev_temp

| S. | Chassis Number | System IP | Hostname | Address(vpn512_next_hop) | Interface Name(vpn512_mgmt_if_name) | IPv4 Address(vpn512_mgmt_if_ip_addr) | Address |
|----|--------------------------------------|---------------|----------|--------------------------|-------------------------------------|--------------------------------------|---------|
| 1 | b7fd7295-58df-7671-e914-6fe2edff1609 | 10.255.255.21 | vEdge20 | 192.168.0.1 | eth0 | 192.168.0.20/24 | 100.11 |
| 2 | dde90ff0-dc62-77e6-510f-08d96608537d | 10.255.255.22 | vEdge21 | 192.168.0.1 | eth0 | 192.168.0.21/24 | 192.0. |

Next Cancel

10. You can click on **Configure Devices** or choose to view the Side-by-Side Config Diff by clicking on the Device, choosing the Config Diff box and then clicking on Side by Side. Click on **Configure Devices**

Device Template
vEdge_Site20_dev_temp Total 1

Config Preview **Config Diff** Info

Device list (Total: 2 devices) Filter/Search

| | |
|--|--------------------------|
| b7fd7295-58df-7671-e914-6fe2edff1609 vEdge20 10.255.255.21 vEdge21 10.255.255.22 | Configure Devices |
|--|--------------------------|

Local Configuration New Configuration

```

1 no config
2 config
3 system
4 personality vedge
5 device-model vedge-cloud
6 chassis-number b7fd7295-58df-7671-e914-6fe2edff1609
7 host-name vEdge20
8 system-ip 10.255.255.21
9 site-id 20
10 admin-tech-on-failure
11 no route-consistency-check
12 organization-name swat-sdwanlab
13 vbond 100.100.100.3
14 aaa
15 auth-order local radius tacacs
16 usergroup basic
17 task system read write
18 task interface read write
19 !
20 usergroup netadmin
21 !
22 usergroup operator
23 task system read
24 task interface read
25 task policy read
26 task routing read

```

```

1 system
2 device-model vedge-cloud
3 host-name vEdge20
4 system-ip 10.255.255.21
5 domain-id 1
6 site-id 20
7 admin-tech-on-failure
8 no route-consistency-check
9 organization-name swat-sdwanlab
10 organization-name swat-sdwanlab
11 vbond 100.100.100.3 port 12346
12 aaa
13 auth-order local radius tacacs
14 usergroup basic
15 task system read write
16 task interface read write
17 !
18 usergroup netadmin
19 !
20 usergroup operator
21 task system read
22 task interface read
23 task policy read
24 task routing read

```

Configure Device Rollback Timer Back **Configure Devices** Cancel

11. Confirm this change and click on **OK**

Configure Devices



Committing these changes affect the configuration on **2** devices. Are you sure you want to proceed?



Confirm configuration changes on 2 devices.

OK

Cancel

12. Once the configuration updates have gone through successfully, log in to the CLI for vEdge21 and issue a `show bfd sessions`. You can also check this from the GUI by navigating to **Monitor => Network**, clicking on vEdge21 and choosing **Real-Time => BFD Sessions** in the Device Options. Choose Do Not Filter.

| Search Options ▾ | | | | | | | | | |
|------------------|---------|------------------------------------|-----------------------------------|--------------|----------|---------------|---------|--------------|--|
| | Status | Message | Chassis Number | Device Model | Hostname | System IP | Site ID | vManage IP | |
| > | Success | Done - Push Feature Template Co... | b7fd7295-58df-7671-e914-6fe2ed... | vEdge Cloud | vEdge20 | 10.255.255.21 | 20 | 10.255.255.1 | |
| > | Success | Done - Push Feature Template Co... | dde90ff0-dc62-77e6-510f-08d96... | vEdge Cloud | vEdge21 | 10.255.255.22 | 20 | 10.255.255.1 | |

| vEdge21# show bfd sess | | | | | | | | | | |
|------------------------|----|-------------|---------|-------------|-------|------------|------------|----|--------|--|
| TECT | TX | SOURCE TLOC | | REMOTE TLOC | | DST PUBLIC | | | | |
| | | SYSTEM IP | SITE ID | STATE | COLOR | COLOR | SOURCE IP | IP | PUBLIC | |
| MULTIPLIER | | | | | | | | | | |
| INTERVAL (msec) | | | | | | | | | | |
| 10.255.255.11 | 1 | up | mpls | mpls | 0 | 192.0.2.10 | 192.0.2.2 | | | |
| 1000 | | 0:00:01:56 | | | | | | | | |
| 10.255.255.12 | 1 | up | mpls | mpls | 0 | 192.0.2.10 | 192.0.2.6 | | | |
| 1000 | | 0:00:01:56 | | | | | | | | |
| 10.255.255.52 | 50 | up | mpls | mpls | 0 | 192.0.2.10 | 192.1.2.22 | | | |
| 1000 | | 0:00:01:56 | | | | | | | | |

13. On the vManage GUI, navigate to **Configuration => Devices** and you should see the two vEdges at Site 20 in vManage mode

| | | | | | | | | | | | |
|--|-------------|--------------------------------------|----------|----|----|---------|---------------|----|---------|-----------------------|----------|
| | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2edff1609 | 2970600D | NA | NA | vEdge20 | 10.255.255.21 | 20 | vManage | vEdge_Site20_dev_temp | In S ... |
| | vEdge Cloud | dde90ff0-dc62-77e6-510f-08d9608537d | 88FD4E65 | NA | NA | vEdge21 | 10.255.255.22 | 20 | vManage | vEdge_Site20_dev_temp | In S ... |

We have successfully placed the devices in Site 20 under the control of vManage.

Task List

- [Creating the Site 20 Feature Templates](#)
 - [Creating the VPN0 Feature Template](#)

- [Creating the INET and MPLS VPN Interface Feature Template](#)
- [Modifying a Device Template and Attaching Devices](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Site last generated: Sep 1, 2020



Site 30 vEdge Templates

Summary: Creating Feature and Device Templates for the vEdge in Site 30

Table of Contents

- [Overview](#)
- [Creating the Site 30 Feature Templates](#)
- [Modifying a Device Template and Attaching Devices](#)

Task List

- Creating the Site 30 Feature Templates
- Modifying a Device Template and Attaching Devices

Overview

vEdge30 and the DC-vEdges are quite similar from a configuration standpoint. The templates already created for the DC-vEdges can be re-used for Site 30, but we will be making a copy of those templates and applying the renamed copies to the Device Template for Site 30. This is because DC and Branch sites will generally have some configuration changes down the line which will not apply to both sites. It's a good practice to keep the number of templates to a minimum, keeping in mind the treatment given to different sites. If Site 30 and the DC Site share the same template, any changes made on one will affect the other.

Creating the Site 30 Feature Templates

We will set up the VPN templates for VPN 0 in Site 30 by making a copy of the *DCvEdge-vpn0* Feature Template created before. No other major changes will be made to the template itself

- From Configuration => Templates => Feature tab search in the search box for *dc*. We should see a few templates, out of which we will be making copies of *DCvEdge-vpn0*, *DC-vEdge_INET* and *DC-vEdge_MPLS* for use at Site 30

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|-------------------|-------------------------------------|--------------------|--------------|------------------|------------------|------------|----------------------------|---------|
| DC-vEdge_MPLS | MPLS Interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:43:22 AM PDT | ... |
| DC-vEdge_INET | INET Interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:39:02 AM PDT | ... |
| DCvEdge-vpn512 | VPN512 for the DC-vEdges | WAN Edge VPN | vEdge Cloud | 2 | 4 | admin | 23 May 2020 1:25:54 AM PDT | ... |
| DCvEdge-vpn0 | VPN0 for the DC-vEdges INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:17:15 AM PDT | ... |
| DC-vEdge_mgmt_int | MGMT interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 2 | 4 | admin | 23 May 2020 1:49:11 AM PDT | ... |

- Click on the three dots next to *DCvEdge-vpn0* and choose **Copy**. Rename the template to *vEdge30-vpn0* with a description of *VPN0 for the Site30 INET and MPLS link*. Click on **Copy**

Template Name
vEdge30-vpn0

Description
VPN0 for the Site30 INET and MPLS link

Copy Cancel

- Click on the dots next to the newly created template and choose to **Edit**. Make sure the Template Name and Description match. Click on **Update**

Feature Template > VPN

Device Type vEdge Cloud

Template Name vEdge30-vpn0

Description VPN0 for the Site30 INET and MPLS link

4. Repeat steps 2 and 3 above, making copies of *DC-vEdge_INET* and *DC-vEdge_MPLS*, renaming them to *vEdge30_INET* and *vEdge30_MPLS* respectively. Update the descriptions as necessary, while copying the template and (if required - note that the description does not get updated at times while copying) by editing the template and choosing to **Update**

Template Copy

X

Template Name

Description

INET interface for the Site30 vEdges

Copy **Cancel**

⚙ CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > **VPN Interface Ethernet**

| | |
|---------------|--------------------------------------|
| Device Type | vEdge Cloud |
| Template Name | vEdge30_MPLS |
| Description | MPLS interface for the Site30 vEdges |

5. If we go back to the main **Configuration => Templates => Feature Tab**, and search for *vedge30* in the search string, there should be 3 templates visible

| Template Type | Non-Default | <input type="text" value="vedge30"/> | Search Options | Total Rows: 3 of 16 | | | | |
|---------------|---------------------------------------|--------------------------------------|----------------|---------------------|------------------|------------|----------------------------|-----|
| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | ... |
| vEdge30_MPLS | MPLS interface for the Site30 vEd... | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 23 May 2020 6:32:26 AM PDT | ... |
| vEdge30_vpno | VPNO for the Site30 INET and MPL... | WAN Edge VPN | vEdge Cloud | 0 | 0 | admin | 23 May 2020 6:25:48 AM PDT | ... |
| vEdge30_INET | INET interface for the Site30 vEdg... | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 23 May 2020 6:27:24 AM PDT | ... |

Thus, we have simply made copies of the DC-vEdge Feature Templates and updated the name/description so as to apply different configuration to the two Sites (Site 30 and DC) down the line, if required.

Task List

- [Creating the Site 30 Feature Templates](#)
- [Modifying a Device Template and Attaching Devices](#)

Modifying a Device Template and Attaching Devices

1. Go to **Configuration => Templates** and make sure you're on the Device tab. Click on the three dots next to the **DCvEdge_dev_temp**. Click on **Copy**. Rename the Template **vEdge30_dev_temp** and give it a Description of *Device template for the Site 30 vEdge*. Click on **Copy**

Template Copy X

Template Name

Description

X

Device template for the Site 30 vEdge

Copy
Cancel

2. Click on the three dots next to the newly created template and click on **Edit**. Update the **Transport and Management VPN** section as per the screenshot below. We will be re-using the VPN 512 Templates created for the DC-vEdges. Click on **Update** once done.

Transport & Management VPN

VPN 0 *

vEdge30-vpn0

VPN Interface

vEdge30_INET

VPN Interface

vEdge30_MPLS

Copied and renamed the feature templates

Additional VPN 0 Templates

- BGP
- OSPF
- Secure Internet Gateway
- VPN Interface
- VPN Interface Cellular
- VPN Interface GRE
- VPN Interface IPsec
- VPN Interface PPP

VPN 512 *

DCvEdge-vpn512

VPN Interface

DC-vEdge_mgmt_int

Re-using VPN512 Templates

Additional VPN 512 Templates

- VPN Interface

Update Cancel

3. Click on the three dots next to the newly created **vEdge30_dev_temp** Template and click on **Attach Devices**

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Action |
|--------------------------|-----------------------------------|---------|--------------|-------------------|------------------|------------|----------------------------|-----------------|--------|
| cEdge_dualuplink_devtemp | cEdge Device Template for de... | Feature | CSR1000v | 11 | 1 | admin | 18 May 2020 8:43:52 AM PDT | In Sync | ... |
| vEdge30_dev_temp | Device template for the Site 3... | Feature | vEdge Cloud | 11 | 0 | admin | 23 May 2020 6:36:47 AM PDT | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the Site 2... | Feature | vEdge Cloud | 10 | 2 | admin | 23 May 2020 5:53:51 AM PDT | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync | ... |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 11 | 2 | admin | 23 May 2020 1:55:53 AM PDT | In Sync | ... |

Create Template

Non-Default

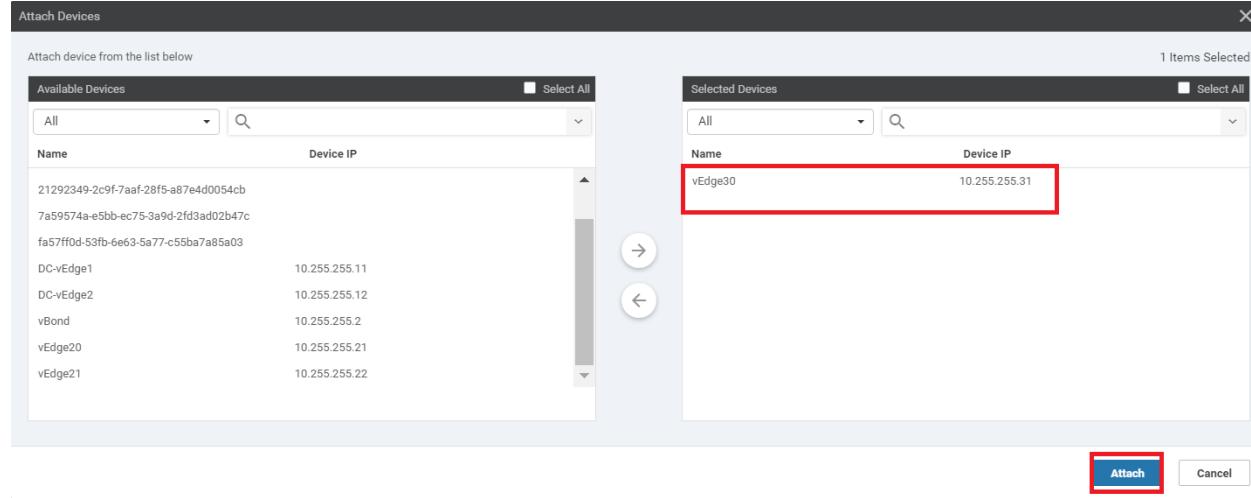
Search Options

Total Rows: 5

Device Feature

...
Edit View Delete Copy
Attach Devices
Export CSV

4. Choose **vEdge30** from the list and click on **Attach**



5. The device should show up in the list. Click on the three dots next to vEdge30 and choose to **Edit Device Template**. Populate the details as shown below and click on **Update**

Update Device Template

Variable List (Hover over each field for more information)

| | |
|-------------------------------------|--------------------------------------|
| Chassis Number | 17026153-f09e-be4b-6dce-482fce43aab2 |
| System IP | 10.255.255.31 |
| Hostname | vEdge30 |
| Address(vpn512_next_hop) | 192.168.0.1 |
| Interface Name(vpn512_mgmt_if_name) | eth0 |
| IPv4 Address(vpn512_mgmt_if_ip_add) | 192.168.0.30/24 |
| Address(vpn0_inet_next_hop) | 100.100.100.1 |
| Address(vpn0_mpls_next_hop) | 192.0.2.13 |
| Interface Name(vpn0_mpls_if_name) | ge0/1 |
| IPv4 Address(vpn0_mpls_if_ip_add) | 192.0.2.14/30 |
| Color(vpn0_mpls_if_color) | mpls |
| Interface Name(vpn0_inet_if_name) | ge0/0 |
| IPv4 Address(vpn0_inet_if_ip_add) | 100.100.100.30/24 |
| Color(vpn0_inet_if_color) | public-internet |
| Hostname | vEdge30 |
| System IP | 10.255.255.31 |
| Site ID | 30 |

Generate Password **Update** **Cancel**

6. **DO NOT** click on Next or Configure Devices at this point. Log in to the CLI for vEdge30 and issue a `show bfd sessions`.

| vEdge30# show bfd sess | | | SOURCE TLOC | REMOTE TLOC | DST PUBLIC | DST PUBLIC | D | | | | |
|------------------------|----------------|-----------|-------------|-------------|--------------|-----------------|----------------|----------------|-------|-------|---|
| TECT | TX | SYSTEM IP | SITE ID | STATE | COLOR | COLOR | SOURCE IP | IP | PORT | ENCAP | M |
| LTIPLIER | INTERVAL(msec) | UPTIME | | | TTRANSITIONS | | | | | | |
| 10.255.255.11 | 1 | 1000 | 0:04:19:13 | up | default | public-internet | 100.100.100.30 | 100.100.100.10 | 12386 | ipsec | 7 |
| 10.255.255.12 | 1 | 1000 | 0:04:19:14 | up | default | public-internet | 100.100.100.30 | 100.100.100.11 | 12386 | ipsec | 7 |
| 10.255.255.21 | 20 | 1000 | 0:00:26:43 | up | default | public-internet | 100.100.100.30 | 100.100.100.20 | 12386 | ipsec | 7 |
| 10.255.255.41 | 40 | 1000 | 4:21:24:13 | up | default | public-internet | 100.100.100.30 | 100.100.100.40 | 12347 | ipsec | 7 |
| 10.255.255.51 | 50 | 1000 | 4:16:45:15 | up | default | public-internet | 100.100.100.30 | 100.100.100.50 | 12347 | ipsec | 7 |

7. Back at the vManage GUI, click on **Next** and then **Configure Devices**. You can view the side-by-side difference, making note of the fact that we are adding an MPLS interface

| Device Template | | Total | | |
|---|---|-------|----------------------|-----------------------------------|
| vEdge30_dev_temp | 1 | | | |
| Device list (Total: 1 devices) | | | | |
| Filter/Search | | | | |
| 17026153-109e-be4b-6dce-482fc43aeb2 vEdge30 10.255.255.31 | | | | |
| <pre> 66 vpn 0 67 interface ge0/0 68 ip address 100.100.100.30/24 69 ipv6 dhcp-client 70 tunnel-interface 71 encapsulation ipsec 72 hello-tolerance 12 73 allow-service all 74 no allow-service bgp 75 allow-service dhcp 76 allow-service dns 77 78 48 vpn 0 49 dns 10.2.1.5 primary 50 dns 10.2.1.6 secondary 51 interface ge0/0 52 ip address 100.100.100.30/24 53 tunnel-interface 54 encapsulation ipsec 55 color public-internet 56 allow-service all 57 no allow-service bgp 58 allow-service dhcp 59 allow-service dns 60 allow-service sshd 61 no allow-service icmp 62 no allow-service netconf 63 no allow-service ntp 64 no allow-service ospf 65 no allow-service stun 66 allow-service https 67 68 no shutdown 69 70 interface ge0/1 71 ip address 192.0.2.14/30 72 tunnel-interface 73 encapsulation ipsec 74 color mpls restrict 75 allow-service all 76 no allow-service bgp 77 allow-service dhcp 78 allow-service dns </pre> | | | | |
| Configure Device Rollback Timer | | | Back | Configure Devices |

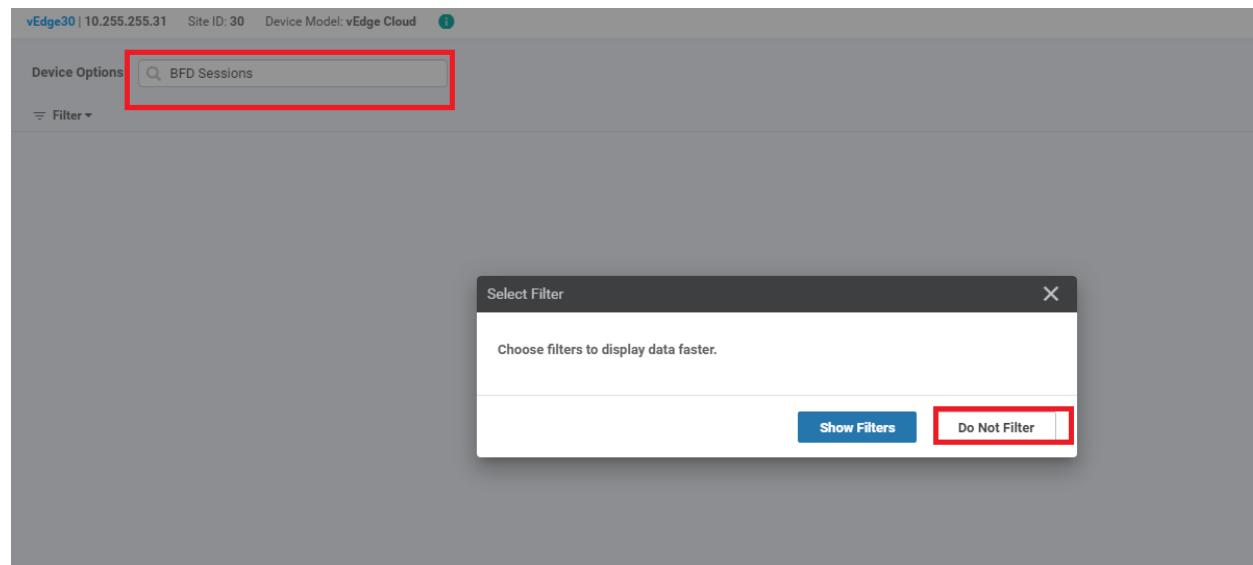
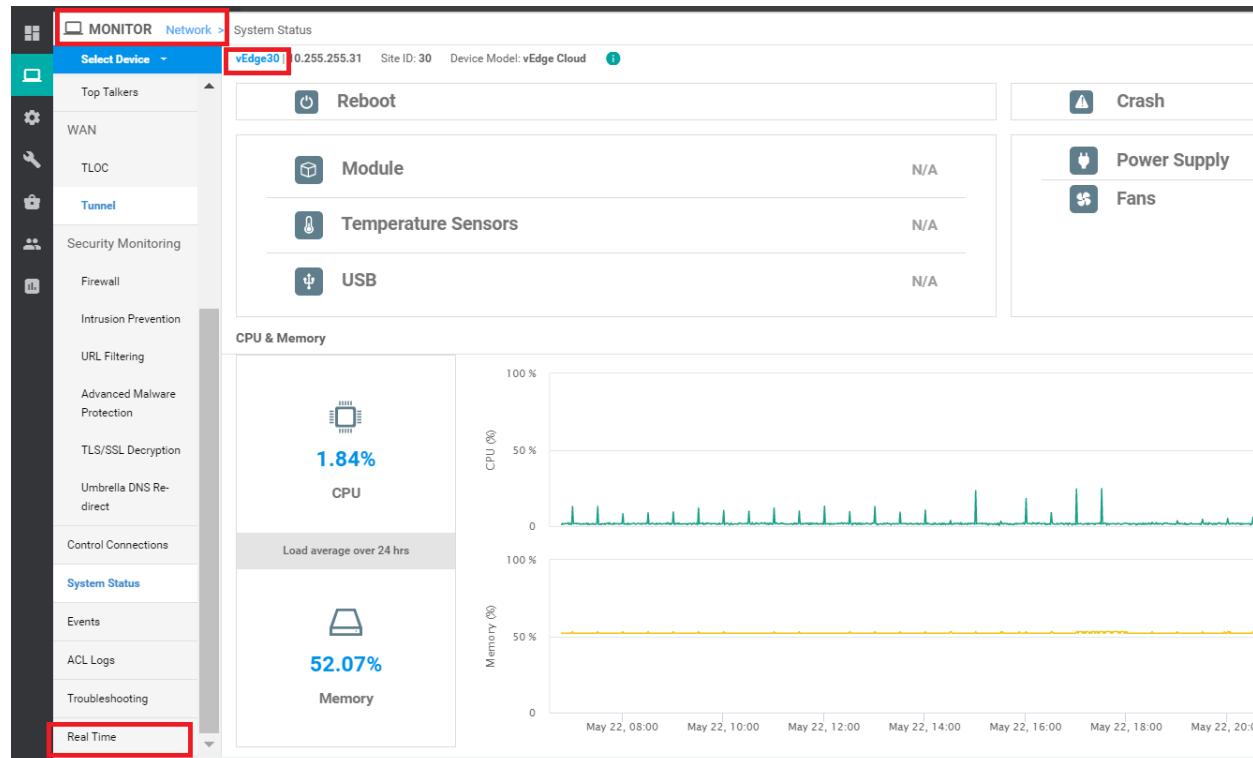
8. Once the configuration goes through, log back into the CLI of vEdge30 and issue `show bfd sessions`. You should see BFD sessions on the mpls TLOC as well

| TECT SYSTEM IP LTIPPLIER | TX SITE ID INTERVAL(msec) | STATE UPTIME | SOURCE TLOC | REMOTE TLOC | SOURCE IP | DST PUBLIC IP |
|--------------------------------|---------------------------------|------------------|----------------------|----------------------|----------------|------------------|
| | | | COLOR TRANSITIONS | COLOR | | |
| 10.255.255.11 | 1 | up 0:00:00:49 | public-internet 0 | public-internet 0 | 100.100.100.30 | 100.100.100.10 |
| 10.255.255.11 | 1 | up 0:00:00:30 | mpls 0 | mpls 0 | 192.0.2.14 | 192.0.2.2 |
| 10.255.255.12 | 1 | up 0:00:00:49 | public-internet 0 | public-internet 0 | 100.100.100.30 | 100.100.100.11 |
| 10.255.255.12 | 1 | up 0:00:00:30 | mpls 0 | mpls 0 | 192.0.2.14 | 192.0.2.6 |
| 10.255.255.21 | 20 | up 0:00:00:49 | public-internet 0 | public-internet 0 | 100.100.100.30 | 100.100.100.20 |
| 10.255.255.22 | 20 | up 0:00:00:30 | mpls 0 | mpls 0 | 192.0.2.14 | 192.0.2.10 |
| 10.255.255.41 | 40 | up 0:00:00:50 | public-internet 0 | public-internet 0 | 100.100.100.30 | 100.100.100.40 |
| 10.255.255.51 | 50 | up 0:00:00:49 | public-internet 0 | public-internet 0 | 100.100.100.30 | 100.100.100.50 |
| 10.255.255.52 | 50 | up 0:00:00:30 | mpls 0 | mpls 0 | 192.0.2.14 | 192.1.2.22 |

9. On the vManage GUI, if you click on **Full WAN Connectivity** on the Main Dashboard, you will see that vEdge30 has a total of 9 BFD sessions

| Site Devices Health: Full WAN Connectivity | | | | | |
|--|--------------|---------------|---------|--------------|--------------------------------|
| Hostname | Reachability | System IP | Site ID | BFD Sessions | Last Updated |
| DC-vEdge1 | reachable | 10.255.255.11 | 1 | 7 | 23 May 2020 6:45:37 AM PDT ... |
| vEdge21 | reachable | 10.255.255.22 | 20 | 4 | 23 May 2020 6:45:37 AM PDT ... |
| vEdge20 | reachable | 10.255.255.21 | 20 | 5 | 23 May 2020 6:45:18 AM PDT ... |
| DC-vEdge2 | reachable | 10.255.255.12 | 1 | 7 | 23 May 2020 6:45:37 AM PDT ... |
| vEdge30 | reachable | 10.255.255.31 | 30 | 9 | 23 May 2020 6:45:52 AM PDT ... |
| cEdge51 | reachable | 10.255.255.52 | 50 | 4 | 23 May 2020 6:45:38 AM PDT ... |
| cEdge50 | reachable | 10.255.255.51 | 50 | 5 | 23 May 2020 6:45:19 AM PDT ... |
| cEdge40 | reachable | 10.255.255.41 | 40 | 5 | 23 May 2020 6:45:19 AM PDT ... |

10. To see the BFD sessions, we can also go to **Monitor => Network**, click on vEdge30. Choose Real-Time from the left hand side and put **BFD Sessions** in the Device Options. Choose Do Not Filter



11. We will see the same information as what was visible on the CLI in Step 8. Note that Site40 is missing from this list. That is because we haven't added the MPLS configuration to Site 40 yet. This will be done in the next section.

Device Options: Filter ▾

Search Options ▾ Total Rows: 9

| System IP | Site ID | State | Source TLOC Color | Remote TLOC Color | Source IP | Destination Public IP | Destination Public Port | Encapsulation | Source Port | Detect Multiplier |
|---------------|---------|-------|-------------------|-------------------|----------------|-----------------------|-------------------------|-----------------|-------------|-------------------|
| 10.255.255.11 | 1 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.10 | 12386 | ipsec | 12386 | 7 |
| 10.255.255.12 | 1 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.11 | 12386 | ipsec | 12386 | 7 |
| 10.255.255.21 | 20 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.20 | 12386 | ipsec | 12386 | 7 |
| 10.255.255.41 | 40 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.40 | 12347 | ipsec | 12386 | 7 |
| 10.255.255.51 | 50 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.50 | 12347 | ipsec | 12386 | 7 |
| 10.255.255.11 | 1 | up | mpls | mpls | 192.0.2.14 | 192.0.2.2 | 12406 | ipsec | 12366 | 7 |
| 10.255.255.12 | 1 | up | mpls | mpls | 192.0.2.14 | 192.0.2.6 | 12406 | Site 40 missing | 12366 | 7 |
| 10.255.255.22 | 20 | up | mpls | mpls | 192.0.2.14 | 192.0.2.10 | 12386 | ipsec | 12366 | 7 |
| 10.255.255.52 | 50 | up | mpls | mpls | 192.0.2.14 | 192.1.2.22 | 12347 | ipsec | 12366 | 7 |

12. Navigate to Configuration => Devices and you will see that all devices are now in vManage mode

CONFIGURATION | DEVICES

WAN Edge List Controllers

Search Options ▾ Total Rows: 20

| State | Device Model | Chassis Number | Serial No./Token | Enterprise Cert Serial No. | Enterprise Cert Expiration Date | Hostname | System IP | Site ID | Mode | Assigned Template | Dev |
|-------------|---------------------------------------|--------------------------|------------------|----------------------------|---------------------------------|---------------|-----------|---------|--------------------------|-------------------|-----|
| CSR1000v | CSR-44C7CE5A-4149-E696-C8A8-415C... | Token - fc40de6570e72... | NA | NA | - | - | - | - | CLI | - | ... |
| CSR1000v | CSR-06B89FC-C363-BB55-7E9D-7C0... | Token - f28Sab97898... | NA | NA | - | - | - | - | CLI | - | ... |
| CSR1000v | CSR-E4E40DC-E358-8DE1-0E81-76E59... | FA1F272A | NA | NA | cEdge50 | 10.255.255.51 | 50 | vManage | cEdge-single-uplink | In S | ... |
| CSR1000v | CSR-D405FB8A-B975-8944-D1A3-ZEB0... | Token - e78aaefc1ebd2... | NA | NA | - | - | - | - | CLI | - | ... |
| CSR1000v | CSR-D1837F36-6A1A-185D-7C1C-E1C... | F87DC882 | NA | NA | cEdge51 | 10.255.255.52 | 50 | vManage | cEdge-single-uplink | In S | ... |
| CSR1000v | CSR-5E992295-1362-0B66-EEF8-25C0... | Token - 1da14330e171... | NA | NA | - | - | - | - | CLI | - | ... |
| CSR1000v | CSR-049482E-44FD-EADC-D30D-600C... | 63201C5... | NA | NA | cEdge40 | 10.255.255.41 | 40 | vManage | cEdge_dualuplink_deve... | In S | ... |
| vEdge Cloud | e474c5f9-86d7-4376-7c8d-ba950b2c91... | 7175A0E... | NA | NA | DC-vEdge1 | 10.255.255.11 | 1 | vManage | DCvEdge_dev_temp | In S | ... |
| vEdge Cloud | 0cdd40fe-f2f1-fc75-866c-469966cd1c3 | 7D405F... | NA | NA | DC-vEdge2 | 10.255.255.12 | 1 | vManage | DCvEdge_dev_temp | In S | ... |
| vEdge Cloud | b7fd7295-58df-7671-e914-6fe2edff1609 | 297060DD | NA | NA | vEdge20 | 10.255.255.21 | 20 | vManage | vEdge_Site20_dev_temp | In S | ... |
| vEdge Cloud | dde90ff0-dcc6277eb-510f-08d8666085374 | 88FD4E65 | NA | NA | vEdge21 | 10.255.255.22 | 20 | vManage | vEdge_Site20_dev_temp | In S | ... |
| vEdge Cloud | 17026153-f09e-be4b-6dce-482fce43aa... | 24715073 | NA | NA | vEdge30 | 10.255.255.31 | 30 | vManage | vEdge30_dev_temp | In S | ... |
| CSR1000v | CSR-26217DAO-1B63-8DDE-11C9-125F... | Token - 8dc7b557b60d... | NA | NA | - | - | - | - | CLI | - | ... |
| CSR1000v | CSR-F960ED20-B7C9-887F-46A8-F4537... | Token - 50cc04634ac... | NA | NA | - | - | - | - | CLI | - | ... |

This completes our Configuration for bringing Site 30 under the control of vManage.

Task List

- [Creating the Site 30 Feature Templates](#)
- [Modifying a Device Template and Attaching Devices](#)



Updating the Site 40 cEdge Template

Summary: Updating the Template at Site 40 to include the MPLS link

Table of Contents

- [Overview](#)
- [Updating and Creating the Site 40 Feature Templates](#)
 - [Updating the VPN0 Feature Template](#)
 - [Creating the MPLS VPN Interface Feature Template](#)
- [Modifying the Device Template](#)

Task List

- Updating and Creating the Site 40 Feature Templates
 - Updating the VPN0 Feature Template
 - Creating the MPLS VPN Interface Feature Template
- Modifying the Device Template

Overview

While the Site40 cEdge is already in vManage mode, we will be looking at updating a Template in this section. The MPLS link on cEdge40 is unconfigured and we will be setting that up. VPN 0 also requires a default route next hop associated with the MPLS link.

Updating and Creating the Site 40 Feature Templates

Updating the VPN0 Feature Template

1. Go to **Configuration => Templates => Feature tab**. Click on the three dots next to the *cEdge_VPN0_dual_uplink* template and click on **Edit**. Scroll down to the IPv4 Route section and click on pencil icon to update the default route

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN

Device Type CSR1000v

Template Name cEdge_VPN0_dual_uplink

Description cEdge VPN 0 Template for Dual Uplinks

IPv4 ROUTE

| IPv4 ROUTE | | | | |
|--------------------------|-----------|----------|--------------------------------|--------|
| New IPv4 Route | | | | |
| Optional | Prefix | Gateway | Selected Gateway Configuration | Action |
| <input type="checkbox"/> | 0.0.0.0/0 | Next Hop | 1 | |

2. Click on **1 Next Hop** to edit the next hops associated with the 0.0.0.0/0 route

Update IPv4 Route

Prefix 0.0.0.0/0 Mark as Optional Row

Gateway Next Hop Null 0 VPN DHCP

Next Hop

Save Changes Cancel

3. Click on **Add Next Hop**, choose **Device Specific** from the drop down in the newly added hop and give it a tag of *vpn0_mpls_next_hop_ip_address*. Click on **Save Changes**

Next Hop

| Address | Distance |
|---------------------------------|----------|
| [vpn0_next_hop_ip_address_0] | 1 |
| [vpn0_mpls_next_hop_ip_address] | 1 |

1 Add Next Hop **2** **3** Save Changes Cancel

4. Make sure that the Update IPv4 Route screen shows **2 Next Hop** and click on **Save Changes** again

Update IPv4 Route

| | | |
|----------|---|---|
| Prefix | 0.0.0.0/0 | <input type="checkbox"/> Mark as Optional Row |
| Gateway | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN <input type="radio"/> DHCP | |
| Next Hop | 2 Next Hop | Save Changes Cancel |

5. You should be back at the main Feature Template page for *cEdge_VPN0_dual_uplink*. Click on **Update**

The screenshot shows two stacked configuration pages from the vManage interface:

- IPv4 ROUTE**: A table with columns for Optional, Prefix (0.0.0.0/0), Gateway (Next Hop), and Selected Gateway Configuration (2). An 'Add' button is visible.
- IPv6 ROUTE**: A table with columns for Optional, Prefix, Gateway, and Selected Gateway Configuration. An 'Add' button is visible.

6. We can add the details of the next hop (which was configured as a Device Specific parameter) on this page itself, without going through the Edit Device Template screen. This is only recommended when minor changes are needed. Double click the *Address(vpn0_mpls_next_hop_ip_address)* field and enter 192.1.2.17

Device Template | cEdge_dualuplink_devtemp

Search Options ▾

| S... | Chassis Number | System IP | Hostname | Address(vpn0_next_hop_ip_address_0) | Address(vpn0_mpls_next_hop_ip_address) | IPv4 Address/ prefix-length |
|---|----------------|-----------|---------------|-------------------------------------|--|-----------------------------|
| CSR-04F9482E-44F0-E4DC-D30D-60C0806F... | 10.255.255.41 | cEdge40 | 100.100.100.1 | 192.1.2.17 | 100.100.100.40/24 | |

7. Click on **Next** and then click on **Configure Devices**. Check the side by side difference, if needed, to view the ip route statement pushed by vManage

Device Template **cEdge_dualuplink_devtemp** Total 1

Device list (Total: 1 devices)

CSR-04F9482E-44F0-E4DC-D3D-60C0B06F73F2
cEdge4010.255.255.41

```

exit-address-family
!
ip arp proxy disable
no ip finger
no ip rcmd rcp-enable
no ip rcmd rsh-enable
no ip domain lookup
no ip dhcp use class
ip multicast route-limit 2147483647
ip route 0.0.0.0 0.0.0.0 100.100.100.1

ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 192.168.0.1
ip bootp server
no ip source-route
no ip http server
no ip http secure-server
no ip http ctc authentication
no ip igmp ssm-map query dns
interface GigabitEthernet1
no shutdown
arp timeout 1200
vrf forwarding Mgmt-intf
ip address 192.168.0.40 255.255.255.0
no ip redirects
ip mtu 1500
mtu 1500
negotiation auto
exit
interface GigabitEthernet2
no shutdown
arp timeout 1200

```

Configure Device Rollback Timer

Back **Configure Devices** **Can**

Task List

- Updating and Creating the Site 40 Feature Templates
 - [Updating the VPN0 Feature Template](#)
 - [Creating the MPLS VPN Interface Feature Template](#)
- Modifying the Device Template

Creating the MPLS VPN Interface Feature Template

1. Go to **Configuration => Templates => Feature tab**. Click on the three dots next to the *cedge-vpn0-int-dual* template and click on **Copy**.

CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type Non-Default Q Search Options

Total Rows: 16

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------|--------------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|----------------------|
| Site20-vpn0 | VPN0 for the Site20 vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 5:41:03 AM PDT | ... |
| cEdge-vpn0-int-single | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| vEdge30-vpn0 | VPN0 for the Site30 INET and MPLS | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:25:48 AM PDT | ... |
| vEdge30_INET | INET interface for the Site30 vEdges | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:27:24 AM PDT | ... |
| cEdge-vpn512-int-dual | cEdge VPN 512 Interface Template... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| cEdge_VPN0_dual_uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin | 18 May 2020 7:37:39 AM PDT | ... |
| cEdge_VPN512_dual_uplink | cEdge VPN 512 Template for Dual ... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 8:38:47 AM PDT | ... |
| DC-vEdge_mgmt_int | MGMT interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 23 May 2020 1:40:10 AM PDT | View |
| DC-vEdge_MPLS | MPLS interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:40:10 AM PDT | Edit |
| DC-vEdge_INET | INET interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:39:53 AM PDT | Change Device Models |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single ... | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 1:25:40 AM PDT | Delete |
| cEdge-vpn0-int-dual | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 18 May 2020 8:28:19 AM PDT | Copy |
| Site20_vpn0_int | VPN0 Interface for Site20 devices | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 5:48:54 AM PDT | ... |
| DCEdge-vpn512 | VPN512 for the DC-vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 23 May 2020 1:25:54 AM PDT | ... |
| DCvEdge-vpn0 | VPN0 for the DC-vEdges INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:17:15 AM PDT | ... |
| vEdge30_MPLS | MPLS Interface for the Site30 vEd... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:32:26 AM PDT | ... |

2. Rename the template to **cedge-vpn0-int-dual_mpls** with a Description of **cEdge VPN 0 Interface Template for devices with a dual uplink - MPLS**. Click on **Copy**

Template Copy

X

Template Name

Description

cEdge VPN 0 Interface Template for devices with a dual uplink - MPLS

Copy **Cancel**

3. Click on the dots next to the newly created template and choose to **Edit**

Device Feature

Add Template

Template Type Non-Default Search Options Total Rows: 5 of 17

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------|--------------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|---------|
| vEdge30_MPLS | MPLS interface for the Site30 vEd... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:32:26 AM PDT | ... |
| vEdge30-vpn0 | VPN0 for the Site30 INET and MPL... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:25:48 AM PDT | ... |
| DCvEdge-vpn0 | VPNO for the DC-vEdges INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:17:15 AM PDT | ... |
| DC-vEdge_MPLS | MPLS interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:43:22 AM PDT | ... |
| cedge-vpn0-int-dual_mpls | cEdge VPN 0 Interface Template f... | Cisco VPN Interface | CSR1000v | 0 | 0 | admin | 23 May 2020 6:57:56 AM PDT | ... |

View
Edit
Change Device Models
Delete
Copy

4. Make sure the Name and Description match as below. Update the **Interface Name** to *GigabitEthernet3* and the **IPv4 Address/ Prefix Length** to *mpls_ipv4_address*

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN Interface Ethernet

Device Type CSR1000v

Template Name cedge-vpn0-int-dual_mpls

Description cEdge VPN 0 Interface Template for devices with a dual uplink - MPLS

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP Advanced

BASIC CONFIGURATION

Shutdown No

Interface Name GigabitEthernet3

Description

IPv4 IPv6

Dynamic Static

IPv4 Address/ prefix-length [mpls_ipv4_address]

5. Under the **Tunnel** section, update the **Color** to *mpls_if_tunnel_color_value* and set **Restrict** to Global from the drop down and On (radio button). Click on **Update**

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP Advanced

TUNNEL

Tunnel Interface On Off

Per-tunnel QoS On Off

Color [mpls_if_tunnel_color_value]

Restrict On Off

Groups

Border On Off

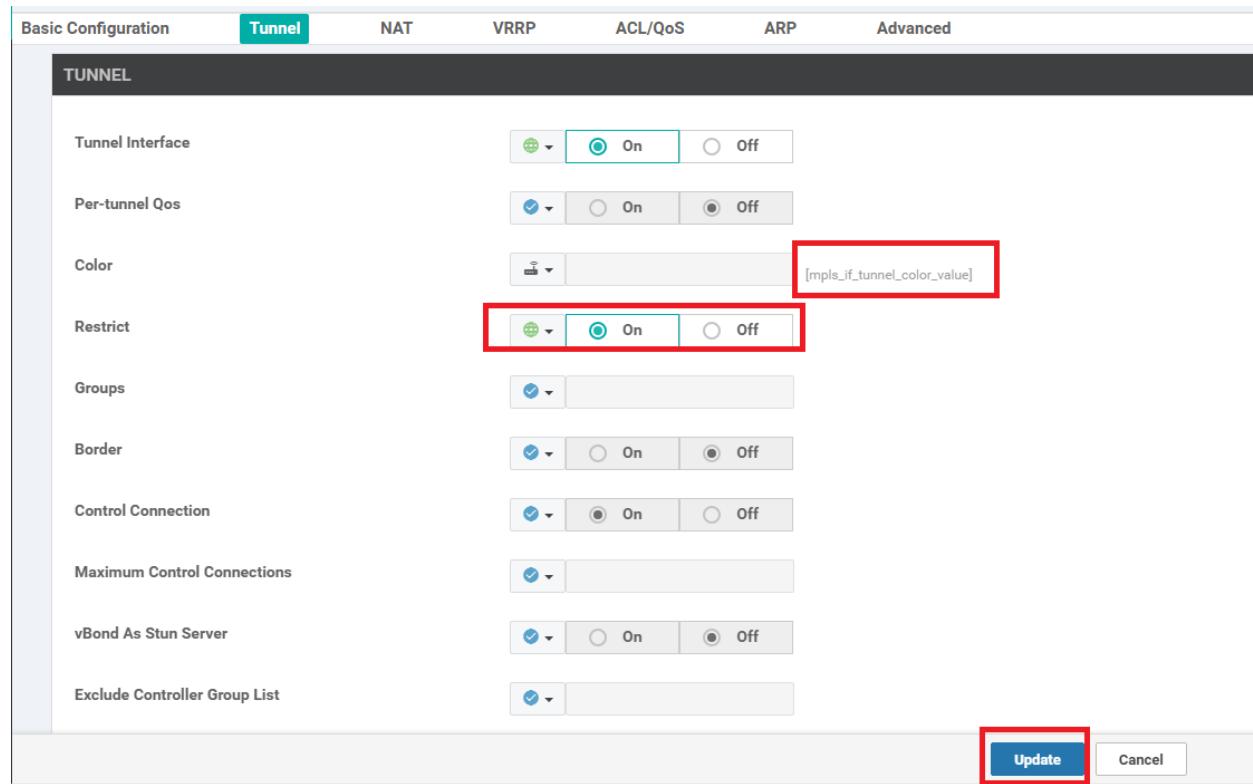
Control Connection On Off

Maximum Control Connections

vBond As Stun Server On Off

Exclude Controller Group List

Update **Cancel**



Task List

- [Updating and Creating the Site 40 Feature Templates](#)
 - [Updating the VPN0 Feature Template](#)
 - [Creating the MPLS-VPN Interface Feature Template](#)
- [Modifying the Device Template](#)

Modifying the Device Template

We now need to associate the template created in the previous step with the Device Template being used by cEdge40.

1. Go to **Configuration => Templates** and make sure you're on the Device tab. Click on the three dots next to the `cEdge_dualuplink_devtemp` template. Click on **Edit**.

CONFIGURATION | TEMPLATES

Device Feature

Create Template

Template Type Non-Default Search Options

Total Rows: 5

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | ... |
|--------------------------|-----------------------------------|---------|--------------|-------------------|------------------|------------|----------------------------|-----------------|-------------------------------------|
| cEdge_dualuplink_devtemp | cEdge Device Template for de... | Feature | CSR1000v | 11 | 1 | admin | 18 May 2020 8:43:52 AM PDT | In Sync | <input type="button" value="Edit"/> |
| vEdge30_dev_temp | Device template for the Site 3... | Feature | vEdge Cloud | 11 | 1 | admin | 23 May 2020 6:36:47 AM PDT | In Sync | <input type="button" value="Edit"/> |
| vEdge_Site20_dev_temp | Device template for the Site 2... | Feature | vEdge Cloud | 10 | 2 | admin | 23 May 2020 5:53:51 AM PDT | In Sync | <input type="button" value="Edit"/> |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync | <input type="button" value="Edit"/> |
| DCvEdge_dev_temp | Device template for the DC-VE... | Feature | vEdge Cloud | 11 | 2 | admin | 23 May 2020 1:55:53 AM PDT | In Sync | <input type="button" value="Edit"/> |

2. Update the **Transport and Management VPN** section as per the screenshot below. You will need to click on **+ Cisco VPN Interface Ethernet** under **Additional Cisco VPN 0 Templates** in order to add a Cisco VPN Interface under VPN 0. Populate **cedge-vpn0-int-dual_mpls** and click on **Update**
0. Populate **cedge-vpn0-int-dual_mpls** and click on **Update**

CONFIGURATION | TEMPLATES

Basic Information Transport & Management VPN Service VPN Additional Templates

Cisco OMP * Factory_Default_Cisco_OMP_ipv40_Template Cisco Security + Default_Security_Cisco_V01

Transport & Management VPN

| | | |
|------------------------------|---------------------------------|--|
| Cisco VPN 0 * | cEdge_VPN0_dual_uplink | Additional Cisco VPN 0 Temp: |
| Cisco VPN Interface Ethernet | cedge-vpn0-int-dual | <input checked="" type="radio"/> Cisco BGP |
| Cisco VPN Interface Ethernet | cedge-vpn0-int-dual_mpls | <input checked="" type="radio"/> Cisco OSPF |
| Cisco VPN 512 * | cEdge_VPN512_dual_uplink | <input checked="" type="radio"/> Cisco Secure Internet Gateway |
| Cisco VPN Interface Ethernet | cedge-vpn512-int-dual | <input checked="" type="radio"/> Cisco VPN Interface Ethernet |
| Cisco VPN Interface Ethernet | | <input checked="" type="radio"/> Cisco VPN Interface GRE |
| Cisco VPN Interface Ethernet | | <input checked="" type="radio"/> Cisco VPN Interface IPsec |
| Cisco VPN Interface Ethernet | | <input checked="" type="radio"/> VPN Interface Ethernet PPPoE |

Service VPN

Update **Cancel**

3. We should get the option to populate the details for cEdge40. These can be entered directly on the page, like before. Populate the two fields as shown below. Click **Next**

Search Options

Total Rows: 1

| S... | Chassis Number | System IP | Hostname | Address(vpn0_mpls_next_hop_ip_address) | IPv4 Address/ prefix-length(mpls_ipv4_address) | Color(mpls_if_tunnel_color_value) | IPv4 Address/ prefix-l |
|-------------------------------------|---|---------------|----------|--|--|-----------------------------------|------------------------|
| <input checked="" type="checkbox"/> | CSR-04F9482E-44FD-E4DC-D300-60C0806F... | 10.255.255.41 | cEdge40 | 192.1.2.17 | 192.1.2.18/30 | mpls | 100.100.100.40/24 |

Edit directly, click Next

4. Note that **GigabitEthernet3** is being configured (can be checked via the Config Diff page) and click on **Configure Devices**

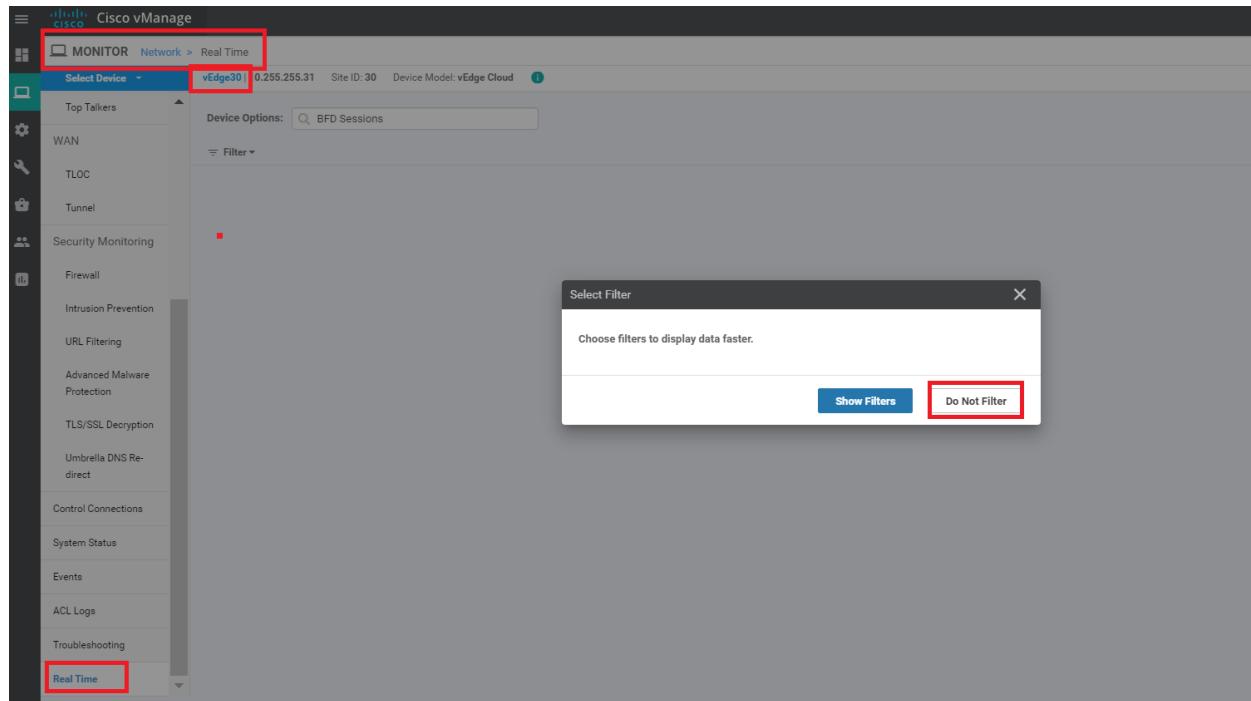
```
exit
77  interface GigabitEthernet3
78    !<!-->
79      encapsulation ipsec weight 1
80      no border
81      color mpls restrict
82      no last-resort-circuit
83      no low-bandwidth-link
84      no vbond-as-stun-server
85      vmanage-connection-preference 5
86      port-hop
87      carrier           default
88      nat-refresh-interval 5
89      hello-interval     1000
90      hello-tolerance   12
91      allow-service all
92      no allow-service bgp
93      allow-service dhcp
94      allow-service dns
95      allow-service icmp
96      no allow-service sshd
97      no allow-service netconf
98      no allow-service ntp
99      no allow-service ospf
100     no allow-service stun
101     allow-service https
102     no allow-service snmp
103     exit
104   avir
```

Back Configure Devices Cancel

5. The configuration should be successful

| Total Task: 1 Success : 1 | | | | | | | | |
|-----------------------------|---------|------------------------------------|---------------------------------|--------------|----------|---------------|---------|--------------|
| Search Options | | | | | | | | |
| | Status | Message | Chassis Number | Device Model | Hostname | System IP | Site ID | vManage IP |
| > | Success | Done - Push Feature Template Co... | CSR-04F9482E-44FD-E4DC-030D-... | CSR1000v | cEdge40 | 10.255.255.41 | 40 | 10.255.255.1 |

6. Go to **Monitor => Network** and choose **vEdge30** (yes, we're choosing vEdge30 and not the cEdge we just configured). Click on **Real Time** and specify **BFD Sessions** in the Device Options field. Choose Do Not Filter



7. We should see that vEdge30 has established BFD sessions over the MPLS link with cEdge40

| BFD Sessions | | | | | | | | | | |
|----------------|----------------------------|---------|-------|-------------------|-------------------|----------------|-----------------------|-------------------------|---------------|-------------|
| Total Rows: 10 | | | | | | | | | | |
| System IP | Last Updated | Site ID | State | Source TLOC Color | Remote TLOC Color | Source IP | Destination Public IP | Destination Public Port | Encapsulation | Source Port |
| 10.255.255.11 | 23 May 2020 7:45:58 AM PDT | 1 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.10 | 12386 | ipsec | 12386 |
| 10.255.255.12 | 23 May 2020 7:45:58 AM PDT | 1 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.11 | 12386 | ipsec | 12386 |
| 10.255.255.21 | 23 May 2020 7:45:58 AM PDT | 20 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.20 | 12386 | ipsec | 12386 |
| 10.255.255.41 | 23 May 2020 7:45:58 AM PDT | 40 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.40 | 12347 | ipsec | 12386 |
| 10.255.255.51 | 23 May 2020 7:45:58 AM PDT | 50 | up | public-internet | public-internet | 100.100.100.30 | 100.100.100.50 | 12347 | ipsec | 12386 |
| 10.255.255.11 | 23 May 2020 7:45:58 AM PDT | 1 | up | mpls | mpls | 192.0.2.14 | 192.0.2.2 | 12406 | ipsec | 12366 |
| 10.255.255.12 | 23 May 2020 7:45:58 AM PDT | 1 | up | mpls | mpls | 192.0.2.14 | 192.0.2.6 | 12406 | ipsec | 12366 |
| 10.255.255.22 | 23 May 2020 7:45:58 AM PDT | 20 | up | mpls | mpls | 192.0.2.14 | 192.0.2.10 | 12386 | ipsec | 12366 |
| 10.255.255.41 | 23 May 2020 7:45:58 AM PDT | 40 | up | mpls | mpls | 192.0.2.14 | 192.1.2.18 | 12367 | ipsec | 12366 |
| 10.255.255.52 | 23 May 2020 7:45:58 AM PDT | 50 | up | mpls | mpls | 192.0.2.14 | 192.1.2.22 | 12347 | ipsec | 12366 |

8. Click the Select Device drop down and click on cEdge40. Choose Do Not Filter.

The screenshot shows the Cisco vManage interface. At the top, there is a header bar with the text "Select Device", "vEdge30 | 10.255.255.31", "Site ID: 30", "Device Model: vEdge Cloud", and an information icon. Below the header is a search bar with dropdown menus for "Device Group" (set to "All") and "Search". A "Sort by" dropdown is set to "Reachability". The main area displays a list of devices:

| Device | IP Address | Site ID | Model | Version |
|---------|---------------|-------------|-------------|-------------------------|
| cEdge40 | 10.255.255.41 | Site ID: 40 | CSR1000v | Version: 17.02.01r.0.32 |
| cEdge50 | 10.255.255.51 | Site ID: 50 | CSR1000v | Version: 17.02.01r.0.32 |
| cEdge51 | 10.255.255.52 | Site ID: 50 | CSR1000v | Version: 17.02.01r.0.32 |
| vEdge20 | 10.255.255.21 | Site ID: 20 | vEdge Cloud | Version: 20.1.1 |
| vEdge21 | 10.255.255.22 | Site ID: 20 | vEdge Cloud | Version: 20.1.1 |

The first device, cEdge40, is highlighted with a red box.

The screenshot shows the Cisco vManage interface for the selected device "cEdge40 | 10.255.255.41 | Site ID: 40 | Device Model: CSR1000v". The left sidebar has a "Select Device" dropdown. The main pane shows "Device Options" with a search bar for "BFD Sessions" and a "Filter" button. A modal window titled "Select Filter" is open, containing the message "Choose filters to display data faster." with two buttons at the bottom: "Show Filters" and "Do Not Filter". The "Do Not Filter" button is highlighted with a red box.

9. The BFD sessions will show up, and we can verify that cEdge40 has established BFD sessions on the MPLS link as well

| | | | | | | | | | | |
|---------------|----------------------------|----|----|------|------|------------|------------|-------|-------|-------|
| 10.255.255.11 | 23 May 2020 7:49:30 AM PDT | 1 | up | mpls | mpls | 192.1.2.18 | 192.0.2.2 | 12406 | ipsec | 12367 |
| 10.255.255.12 | 23 May 2020 7:49:30 AM PDT | 1 | up | mpls | mpls | 192.1.2.18 | 192.0.2.6 | 12406 | ipsec | 12367 |
| 10.255.255.22 | 23 May 2020 7:49:30 AM PDT | 20 | up | mpls | mpls | 192.1.2.18 | 192.0.2.10 | 12386 | ipsec | 12367 |
| 10.255.255.31 | 23 May 2020 7:49:30 AM PDT | 30 | up | mpls | mpls | 192.1.2.18 | 192.0.2.14 | 12366 | ipsec | 12367 |
| 10.255.255.52 | 23 May 2020 7:49:30 AM PDT | 50 | up | mpls | mpls | 192.1.2.18 | 192.1.2.22 | 12347 | ipsec | 12367 |

10. Given below is a snapshot of the **Full WAN Connectivity** page from the main dashboard (verification only, nothing to be done here)

The screenshot shows a table titled "Site Devices Health: Full WAN Connectivity" with 8 rows of data. The columns are: Hostname, Reachability, System IP, Site ID, BFD Sessions, and Last Updated. The data is as follows:

| Hostname | Reachability | System IP | Site ID | BFD Sessions | Last Updated |
|-----------|--------------|---------------|---------|--------------|----------------------------|
| DC-vEdge1 | reachable | 10.255.255.11 | 1 | 8 | 23 May 2020 7:43:50 AM PDT |
| vEdge21 | reachable | 10.255.255.22 | 20 | 5 | 23 May 2020 7:43:49 AM PDT |
| vEdge20 | reachable | 10.255.255.21 | 20 | 5 | 23 May 2020 6:45:18 AM PDT |
| DC-vEdge2 | reachable | 10.255.255.12 | 1 | 8 | 23 May 2020 7:43:50 AM PDT |
| vEdge30 | reachable | 10.255.255.31 | 30 | 10 | 23 May 2020 7:43:50 AM PDT |
| cEdge51 | reachable | 10.255.255.52 | 50 | 5 | 23 May 2020 7:43:51 AM PDT |
| cEdge50 | reachable | 10.255.255.51 | 50 | 5 | 23 May 2020 6:45:19 AM PDT |
| cEdge40 | reachable | 10.255.255.41 | 40 | 10 | 23 May 2020 7:46:18 AM PDT |

This completes our re-configuration for the Site 40 cEdge.

Task List

- [Updating and Creating the Site 40 Feature Templates](#)
 - [Updating the VPN0 Feature Template](#)
 - [Creating the MPLS-VPN Interface Feature Template](#)
- [Modifying the Device Template](#)



Applying Templates to the vSmarts

Summary: Applying Templates to the vSmarts in order to bring them in vManage mode. This will allow policy enforcement

Table of Contents

- [Configuring VPN 0 Templates for vSmarts
 - Configuring the main VPN 0 template
 - Configuring the VPN 0 Interface Template](#)
- [Configuring VPN 512 Templates for vSmarts](#)
- [Attaching vSmarts to the Device Template and Verification](#)

Task List

- Configuring VPN 0 Templates for vSmarts
 - Configuring the main VPN 0 template
 - Configuring the VPN 0 Interface Template
- Configuring VPN 512 Templates for vSmarts
 - Configuring the main VPN 512 template
 - Configuring the VPN 512 Interface Template
- Attaching vSmarts to the Device Template and Verification

Configuring VPN 0 Templates for vSmarts

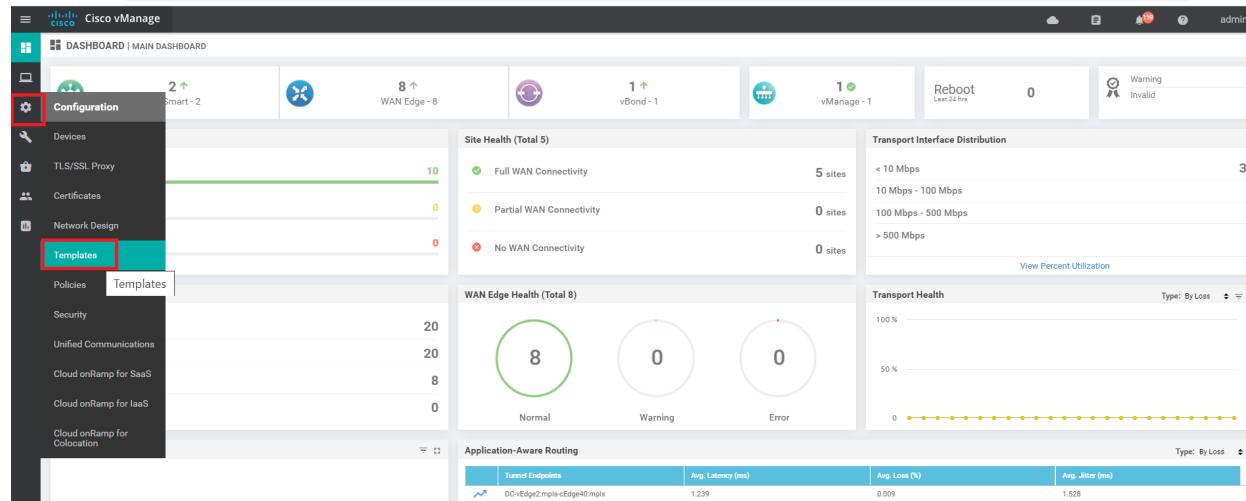
We will now create and apply Templates to the vSmarts. This will allow us to enforce Centralized Policies, which will be used in the following sections.

Unlike before, we will create a Device Template and set up our Feature Templates on the fly. You will notice that vSmart Templates are simpler than the other Templates we've used so far.

Note: We will start by creating the overarching Device Template and create Feature Templates from within the Device Template. Hence, most of the sections outlined below are part of the same flow (i.e. Device Template) and follow one after the other, usually on the same Device Template page.

Configuring the main VPN 0 template

1. Go to Configuration => Templates



2. While on the Device Tab (we're creating Device Templates), click on **Create Template** and choose **From Feature Template**

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Device' tab is selected. A red box highlights the '+ Create Template' button, which has a dropdown menu open showing 'From Feature Template' and 'CLI Template'. Below this is a table listing device templates:

| Name | Description | Type | Device Model |
|--------------------------|------------------------------------|---------|--------------|
| vEdge30_dev_temp | Device template for the Site 30... | Feature | vEdge Cloud |
| vEdge_Site20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud |
| cEdge_dualuplink_devtemp | cEdge Device Template for dev... | Feature | CSR1000v |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud |

3. Select the Device Model as *vSmart*, populate the Template Name as *vSmart-dev-temp* and the Description as *Device Template for vSmarts*

The screenshot shows the 'CONFIGURATION | TEMPLATES' screen with the 'Device' tab selected. The 'Device Model' dropdown is set to 'vSmart'. The 'Template Name' field contains 'vSmart-dev-temp' and the 'Description' field contains 'Device Template for vSmarts'.

4. Under **Transport and Management VPN**, click on the drop down next to **VPN 0**. Click on **Create Template**. This is where we're creating our Feature Templates on the fly

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Basic Information' tab is selected. In the 'Transport & Management VPN' section, there is a dropdown menu for 'VPN 0 *' which is currently set to 'Factory_Default_vSmart_vManage_VPN_0_Template'. Below this dropdown, there is a 'Create Template' button highlighted with a red box. A tooltip for the dropdown indicates it is a 'Default Transport VPN template settings for vSmart and vManage'.

5. Populate the details in the template as given below

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------------|-----------------------|--|-------------------------------|
| | Template Name | NA | vSmart-VPN0 |
| | Description | NA | VPN0 Template for the vSmarts |
| Basic Configuration | VPN | Global | VPN 0 |
| Basic Configuration - DNS | Primary DNS Address | Global | 10.y.1.5 |
| Basic Configuration - DNS | Secondary DNS Address | Global | 10.y.1.6 |

Over here, y is 1 if you're on the SLC DC and 2 if you're on the GHI DC (the email with lab details should enumerate which DC you're on).

The screenshot shows the 'CONFIGURATION | TEMPLATES' section. Under 'Device', a 'Feature Template' is being added for 'VPN'. The 'Device Type' is set to 'vSmart', the 'Template Name' is 'vSmart-VPN0', and the 'Description' is 'VPN0 Template for the vSmarts'. The 'Basic Configuration' tab is selected, displaying fields for 'VPN' (set to 'VPN 0') and 'Name' (with a checked checkbox). Below this, the 'DNS' tab is shown, containing fields for 'Primary DNS Address' (10.2.1.5) and 'Secondary DNS Address' (10.2.1.6).

6. Under **IPv4 Route** click on New IPv4 Route and specify the Prefix as **0.0.0.0/0**. Click on **Add Next Hop**

IPV4 ROUTE

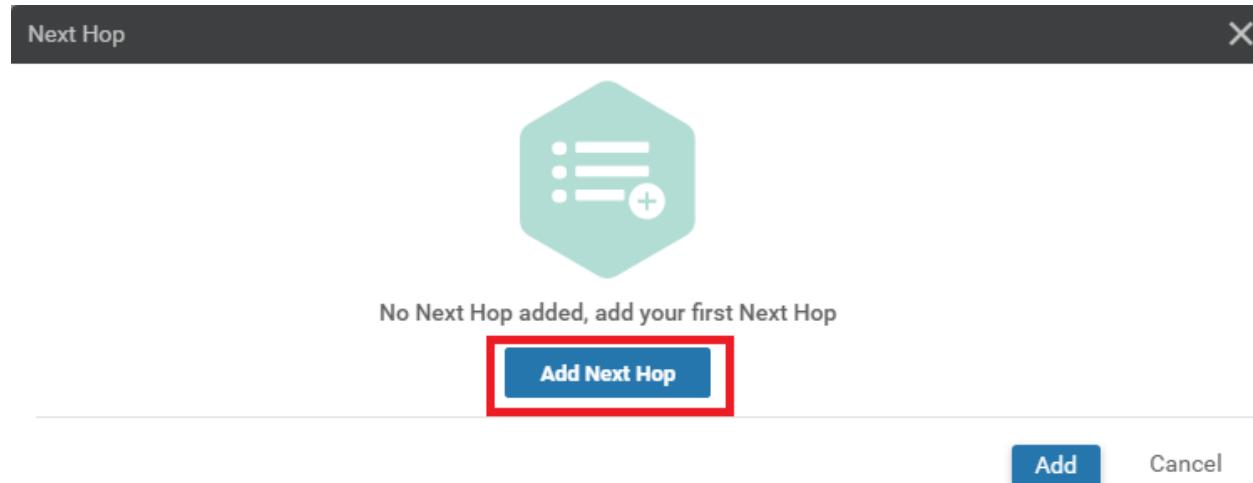
New IPv4 Route

Prefix: 0.0.0.0/0

Gateway: Next Hop

Next Hop: Add Next Hop

7. Click on **Add Next Hop** again



8. Enter the Address as *100.100.100.1*, making it a Global value. Click on **Add**

Next Hop

| Address | Distance |
|--|--------------------------------|
| <input type="text" value="100.100.100.1"/> | <input type="text" value="1"/> |

Add Next Hop

Add Cancel

9. Click on **Add** again in the IPv4 Route section to add the route

IPV4 ROUTE

New IPv4 Route

| | | |
|----------|--|---|
| Prefix | <input type="text" value="0.0.0.0/0"/> | <input type="checkbox"/> Mark as Optional Row |
| Gateway | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN | |
| Next Hop | 1 Next Hop | Add Cancel |

10. Click on **Save** to save this Feature Template

IPV4 ROUTE

[New IPv4 Route](#)

| Optional | Prefix | Gateway | Selected Gateway Configuration |
|--------------------------|-----------|----------|--------------------------------|
| <input type="checkbox"/> | 0.0.0.0/0 | Next Hop | 1 |

IPV6 ROUTE

[New IPv6 Route](#)

| Optional | Prefix | Gateway | Selected Gateway Configuration |
|-------------------|--------|---------|--------------------------------|
| No data available | | | |

This completes the configuration of the Main VPN 0 Template. Continue with configuring the VPN 0 Interface Template.

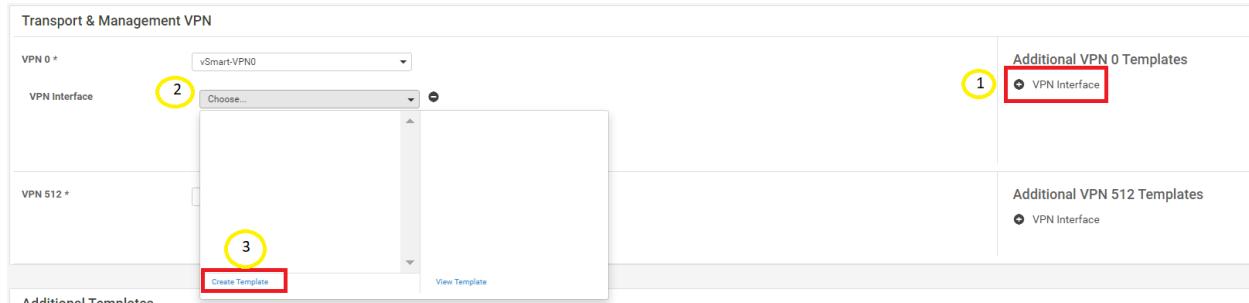
Task List

- Configuring VPN 0 Templates for vSmarts
 - [Configuring the main VPN 0 template](#)
 - Configuring the VPN 0 Interface Template
- Configuring VPN 512 Templates for vSmarts
 - Configuring the main VPN 512 template
 - Configuring the VPN 512 Interface Template
- Attaching vSmarts to the Device Template and Verification

[Configuring the VPN 0 Interface Template](#)

1. Click on **VPN Interface** from the Additional VPN 0 Templates section and click on the drop down for VPN Interface.

Click on **Create Template** to create the VPN Interface Feature Template



2. Populate the details as given below and click on **Save**

| Section | Field | Global or Device Specific (drop down) | Value |
|--|------------------|--|----------------------------|
| | Template Name | NA | vSmart-VPN0-Int |
| | Description | NA | VPN0 Interface for vSmarts |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Global | eth0 |
| Basic Configuration - IP Configuration | IPv4 Address | Device Specific | vpn0_if_ip_address |
| Tunnel | Tunnel Interface | Global | On |
| Tunnel | Color | Global | public-internet |
| Tunnel - Allow Service | All | Global | On |

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > [VPN Interface Ethernet](#)

Device Type

vSmart

Template Name

vSmart-VPN0-Int

Description

VPN0 Interface for vSmarts

Basic Configuration

Tunnel

ARP

Advanced

BASIC CONFIGURATION

Shutdown

Yes No

Interface Name

eth0

Description

IP Configuration

Dynamic Static

IPv4 Address

[vpn0_if_ip_address]

[Basic Configuration](#)[Tunnel](#)[ARP](#)[Advanced](#)

TUNNEL

Tunnel Interface Off

Color

Allow Service

All Off

DHCP On Off

DNS On Off

ICMP On Off

SSH On Off

NETCONF On Off

NTP On Off

STUN On Off

This completes the configuration of the VPN 0 Interface Template.

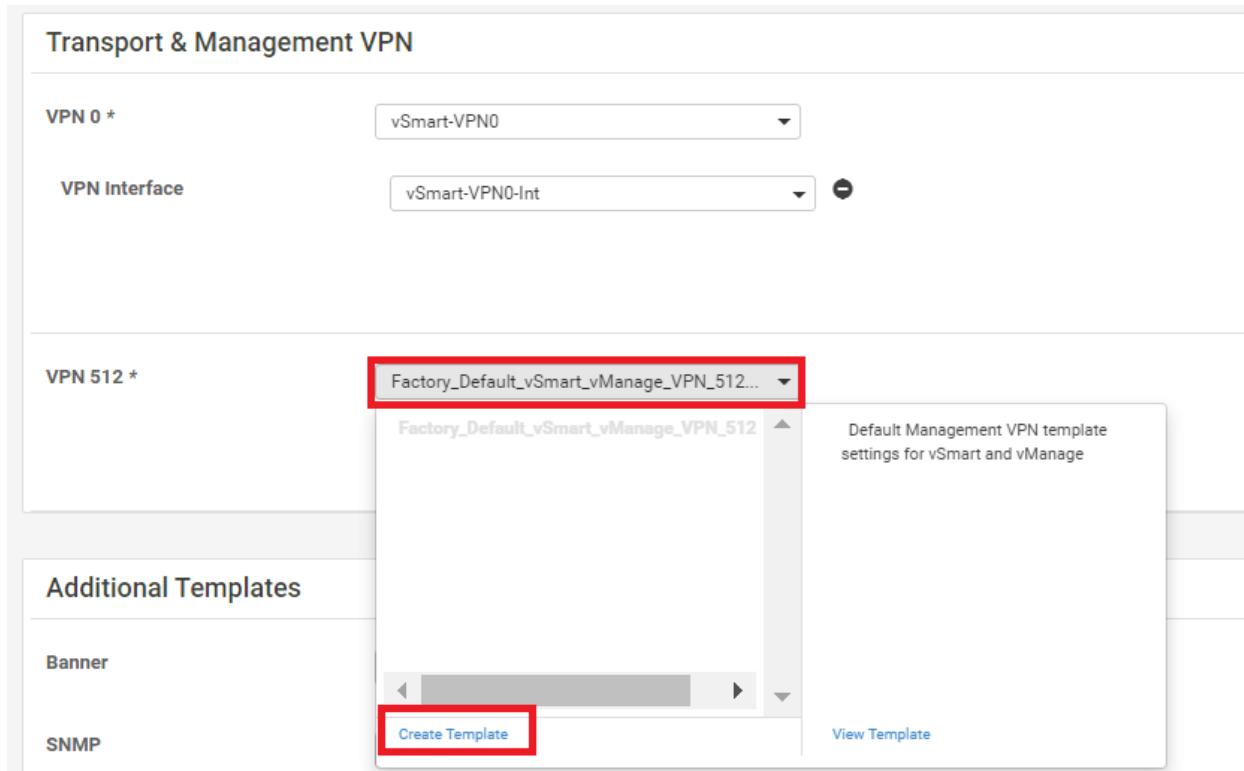
Make sure the VPN 0 and VPN 0 Interface Templates just created are selected from the drop down in the Device Template we're building before proceeding to create the VPN 512 Templates.

Task List

- [Configuring VPN 0 Templates for vSmarts](#)
 - [Configuring the main VPN 0 template](#)
 - [Configuring the VPN 0 Interface Template](#)
- [Configuring VPN 512 Templates for vSmarts](#)
- [Attaching vSmarts to the Device Template and Verification](#)

Configuring VPN 512 Templates for vSmarts

1. On the Device Template page itself, click on the drop down next to **VPN 512** under the **Transport and Management VPN** section. Click on **Create Template**



2. Enter the details as shown below

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|---------------|--|---------------------------------|
| | Template Name | NA | vSmart-VPN512 |
| | Description | NA | VPN512 Template for the vSmarts |
| Basic Configuration | VPN | Global | VPN 512 |

| | | | |
|---------------------|-----------------------|--------|----------|
| Basic Configuration | Primary DNS Address | Global | 10.y.1.5 |
| Basic Configuration | Secondary DNS Address | Global | 10.y.1.6 |

Over here, y is 1 if you're on the SLC DC and 2 if you're on the GHI DC (the email with lab details should enumerate which DC you're on).

Device Feature

Feature Template > Add Template > [VPN](#)

| | |
|---------------|---------------------------------|
| Device Type | vSmart |
| Template Name | vSmart-VPN512 |
| Description | VPN512 Template for the vSmarts |

Basic Configuration DNS IPv4 Route IPv6 Route

BASIC CONFIGURATION

VPN

Name

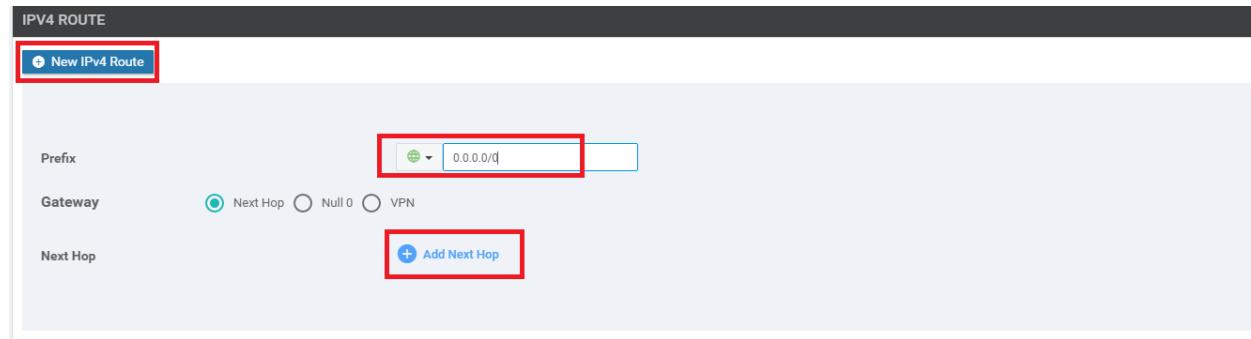
DNS

Primary DNS Address

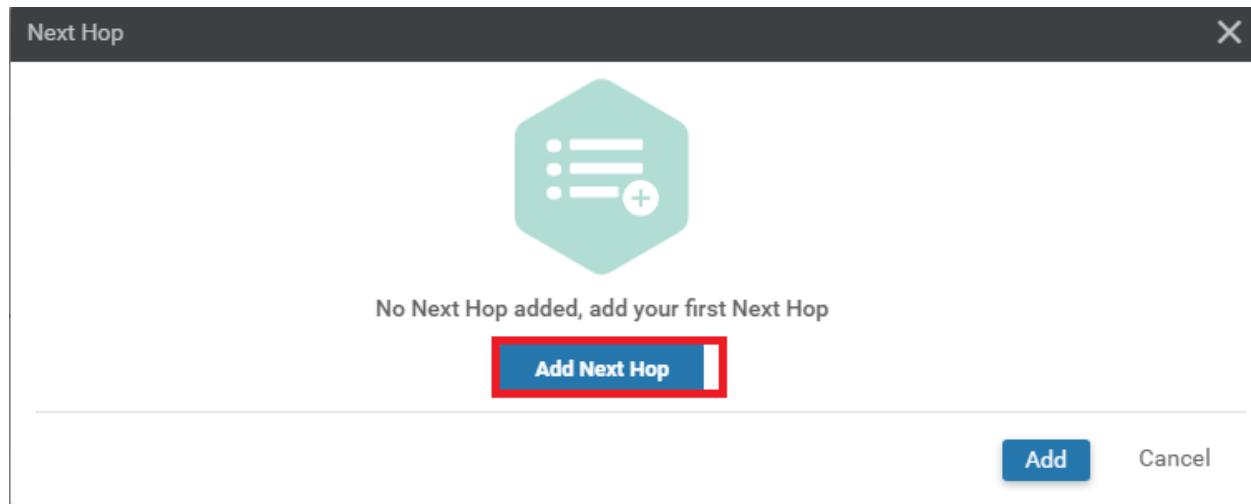
Secondary DNS Address

[Optional](#) [Hostname](#) [List of IP A](#)

3. Under **IPv4 Route** click on New IPv4 Route and specify the Prefix as **0.0.0.0/0**. Click on **Add Next Hop**



4. Click on **Add Next Hop** again



5. Enter the address as *192.168.0.1*, a Global value. Click on **Add**

Next Hop

| Address | Distance |
|--|--------------------------------|
| <input type="text" value="192.168.0.1"/> | <input type="text" value="1"/> |

[+ Add Next Hop](#)

[Add](#) [Cancel](#)

6. Click on **Add** again to add the IPv4 Route and then click on **Save**

IPV4 ROUTE

[New IPv4 Route](#)

| Prefix | Gateway | Next Hop | Action |
|--------------------------------------|--|------------|--|
| <input type="text" value="0.0.0.0"/> | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN | 1 Next Hop | Add Cancel |

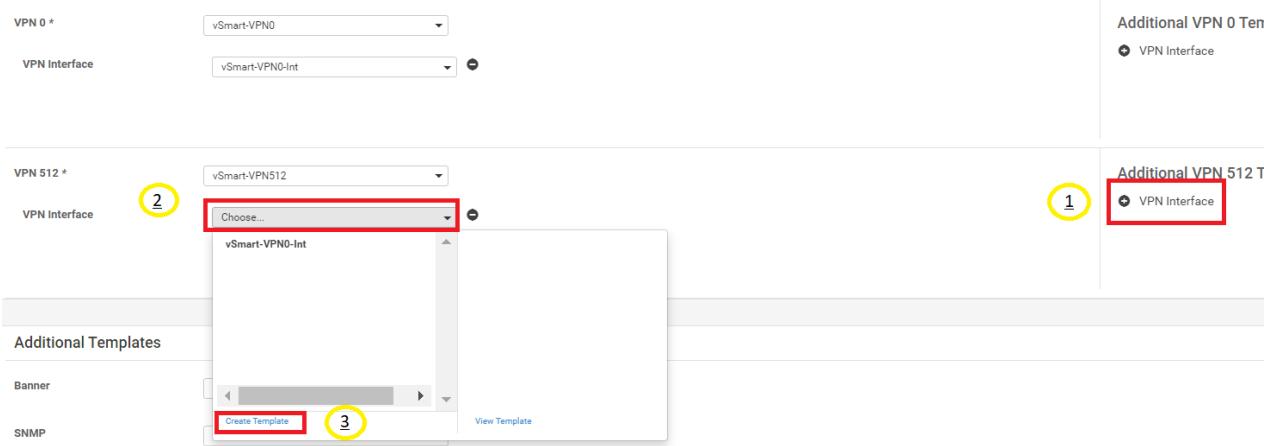
No data available

Click save AFTER clicking on Add above

[Save](#) [Cancel](#)

7. Back on the main Device Template page, make sure **vSmart-VPN512** is selected as the Template. Click on **VPN Interface** under **Additional VPN 512 Templates** and click on the drop down. Choose to **Create Template**. We're creating the VPN 512 Interface Feature Template at this point

Transport & Management VPN



8. Enter the details as shown below and click on **Save**

| Section | Field | Global or Device Specific (drop down) | Value |
|--|------------------|--|---|
| | Template Name | NA | vSmart-vpn512-int |
| | Description | NA | VPN512 Interface Template for the vSmarts |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Global | eth1 |
| Basic Configuration - IP Configuration | IPv4 Address | Device Specific | vpn512_if_ip_address |
| Tunnel | Tunnel Interface | Global | Off |

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > VPN Interface Ethernet

Device Type vSmart

Template Name vSmart-vpn512-int

Description VPN512 Interface Template for the vSmarts

Basic Configuration Tunnel ARP Advanced

BASIC CONFIGURATION

Shutdown Yes No

Interface Name eth1

Description

IP Configuration

Dynamic Static

IPv4 Address [vpn512_if_ip_address]

IPv6 Configuration

Save Cancel

9. Make sure the **Transport and Management VPN** section is populated as shown below and click on **Create**.

Transport & Management VPN

VPN 0 * vSmart-VPN0

VPN Interface vSmart-VPN0-Int

VPN 512 * vSmart-VPN512

VPN Interface vSmart-vpn512-int

Additional VPN 0 Templates

VPN Interface

Additional VPN 512 Templates

VPN Interface

Additional Templates

Create Cancel

We have completed the Device Template (and consequently the Feature Template) configuration for our vSmarts.

Task List

- [Configuring VPN 0 Templates for vSmarts](#)
 - [Configuring the main VPN 0 template](#)
 - [Configuring the VPN 0 Interface Template](#)
- [Configuring VPN 512 Templates for vSmarts](#)
- [Attaching vSmarts to the Device Template and Verification](#)

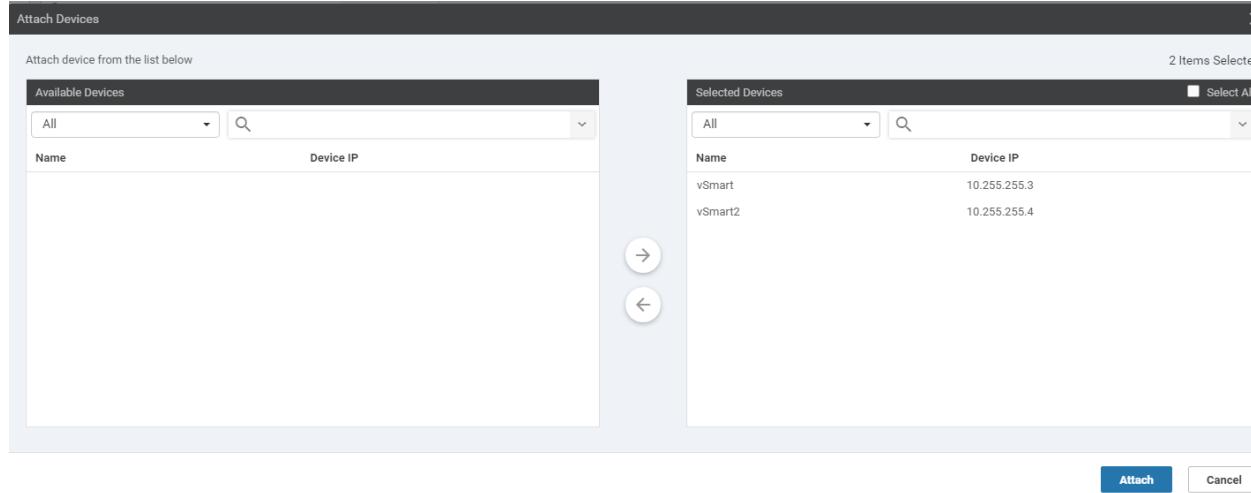
Attaching vSmarts to the Device Template and Verification

Our Device Template for the vSmarts are set up and we now need to attach them to the Template.

1. Click on **Configuration => Templates** (if not already there) and click the three dots next to the **vSmart-dev-temp** we just created. Click on **Attach Devices**

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Actions |
|--------------------------|------------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|---------|
| vEdge30_dev_temp | Device template for the Site 30... | Feature | vEdge Cloud | 11 | 1 | admin | 23 May 2020 6:36:47 AM PDT | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud | 10 | 2 | admin | 23 May 2020 5:53:51 AM PDT | In Sync | ... |
| cEdge_dualuplink_devtemp | cEdge Device Template for dev... | Feature | CSR1000v | 12 | 1 | admin | 23 May 2020 7:39:59 AM PDT | In Sync | ... |
| vSmart-dev-temp | Device Template for vSmarts | Feature | vSmart | 9 | 0 | admin | 25 May 2020 10:13:06 AM PDT | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync | |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 11 | 2 | admin | 23 May 2020 1:55:53 AM PDT | In Sync | |

2. Choose both the vSmarts and click on **Attach**



3. You can populate the details in the Device Template window itself since there isn't much. If you're more comfortable with the **Edit Device Template** option, use that to enter the values and click on **Next**. Details to be entered are shown in the images below

Update Device Template

Variable List (Hover over each field for more information)

| | |
|------------------------------------|--------------------------------------|
| Chassis Number | 20607a12-c0c8-4f46-a65f-5a547cdf3325 |
| System IP | 10.255.255.3 |
| Hostname | vSmart |
| IPv4 Address(vpn512_if_ip_address) | 192.168.0.8/24 |
| IPv4 Address(vpn0_if_ip_address) | 100.100.100.4/24 |
| Hostname | vSmart |
| System IP | 10.255.255.3 |
| Site ID | 1000 |

Update Device Template

Variable List (Hover over each field for more information)

Chassis Number 7f332491-cb6f-4843-8bf5-060f90df8dec

System IP 10.255.255.4

Hostname vSmart2

IPv4 Address(vpn512_if_ip_address) 192.168.0.9/24

IPv4 Address(vpn0_if_ip_address) 100.100.100.5/24

Hostname vSmart2

System IP 10.255.255.4

Site ID 1000

4. Click on the Device List on the left-hand side and click on **Config Diff**. Choose **Side By Side Diff** to review the configuration difference

The screenshot shows the 'CONFIGURATION | TEMPLATES' section with a device template named 'vSmart-dev-temp'. A 'Device list (Total: 2 devices)' table is visible, with the first row (highlighted by a red box) showing '20607a12-cb6f-4843-8bf5-060f90df8dec' and 'vSmart2(10.255.255.4)'. The 'Config Diff' tab is selected, and a yellow banner at the top right states: "'Configure' action will be applied to 2 device(s) attached to 1 device template(s.)". Below the tabs, there are two panes: 'Local Configuration vs. New Configuration' and 'Side By Side Diff'. The 'Local Configuration vs. New Configuration' pane displays a list of configuration differences:

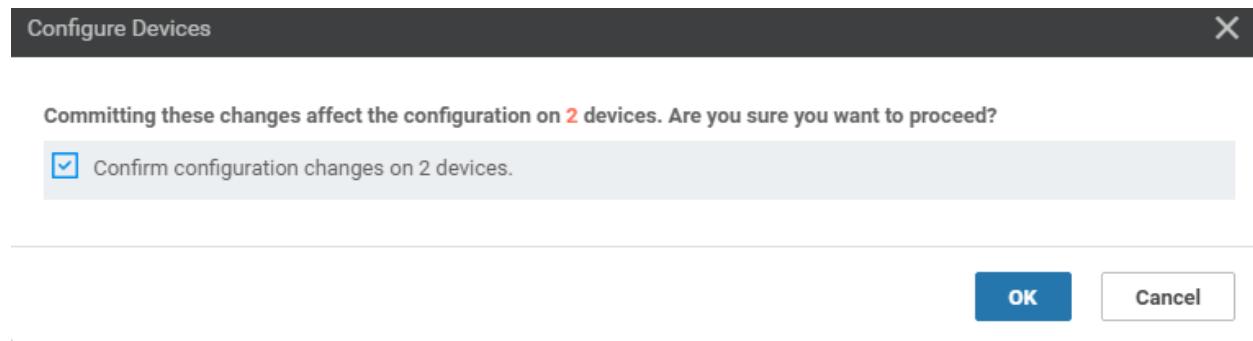
| Line | Setting | Value |
|------|--------------------------------|--------------------------------------|
| 1 | system | vsmart |
| 2 | device-model | vSmart |
| 3 | chassis-number | 20607a12-cb6f-4843-8bf5-060f90df8dec |
| 4 | host-name | vSmart |
| 5 | system-ip | 10.255.255.4 |
| 6 | domain-id | 1 |
| 7 | site-id | 1000 |
| 8 | admin-tech-on-failure | |
| 9 | sp-organization-name | swat-swanlab |
| 10 | organization-name | swat-swanlab |
| 11 | vbond 100.100.100.3 port 12346 | |
| 12 | aaa | |
| 13 | auth-order local radius tacacs | |

5. Once done reviewing the configuration difference, click on **Configure Devices**

| Local Configuration | | New Configuration | |
|---------------------|---|-------------------|--|
| 1 | system | 1 | system |
| 2 | device-model vSmart | 2 | device-model vSmart |
| 3 | chassis-number 20607a12-c0c8-4f46-a65f-5a547cdf3325 | 3 | host-name vSmart |
| 4 | host-name vSmart | 4 | system-ip 10.255.255.3 |
| 5 | system-ip 10.255.255.3 | 5 | domain-id 1 |
| 6 | site-id 1000 | 6 | site-id 1000 |
| 7 | admin-tech-on-failure | 7 | admin-tech-on-failure |
| 8 | sp-organization-name swat-sdwanlab | 8 | sp-organization-name swat-sdwanlab |
| 9 | organization-name swat-sdwanlab | 9 | organization-name swat-sdwanlab |
| 10 | vbond 100.100.100.3 port 12346 | 10 | vbond 100.100.100.3 port 12346 |
| 11 | aaa | 11 | aaa |
| 12 | auth-order local radius tacacs | 12 | auth-order local radius tacacs |
| 13 | usergroup basic | 13 | usergroup basic |
| 14 | task system read write | 14 | task system read write |
| 15 | task interface read write | 15 | task interface read write |
| 16 | ! | 16 | ! |
| 17 | usergroup netadmin | 17 | usergroup netadmin |
| 18 | ! | 18 | ! |
| 19 | usergroup operator | 19 | usergroup operator |
| 20 | task system read | 20 | task system read |
| 21 | task interface read | 21 | task interface read |
| 22 | task policy read | 22 | task policy read |
| 23 | task routing read | 23 | task routing read |
| 24 | task security read | 24 | task security read |
| 25 | ! | 25 | ! |
| 26 | usergroup tenantadmin | 26 | user admin |
| 27 | ! | 27 | password \$6\$siwKBQ==SwT21Ua9BSreDPI6gB8s14E6P yiG6gnLABTnxE96Hj1KF6QRq1 |
| 28 | user admin | | |
| 29 | password \$6\$VMTXKLxYT/tQI8eLS12SvrK39/qFGpF0LnDhct2CzJwq1/FXzwDso7zXkEr9xa3vB5.kgf 7zrVZ/mY43OpxBnamTvZ061VaNZpGOLV/ | | |

[Back](#)[Configure Devices](#)[Cancel](#)

6. Confirm the configuration change by clicking on the check box and then clicking OK



7. Wait for the vSmarts to be configured successfully

TASK VIEW

Push Feature Template Configuration | Validation Success

Total Task: 2 | Success : 2

| Search Options | Status | Message | Chassis Number | Device Model | Hostname |
|----------------|---------|-------------------------------------|-----------------------------------|--------------|----------|
| > | Success | Done - Push Feature Template Con... | 20607a12-c0c8-4f46-a65f-5a547c... | vSmart | vSmart |
| > | Success | Done - Push Feature Template Con... | 7f332491-cb6f-4843-8bf5-060f90... | vSmart | vSmart2 |

8. Navigate to Configuration => Devices and go to the **Controllers** tab. You should see the vSmarts in vManage mode

| Hostname | System IP | Site ID | Mode | Assigned Template | Device Status | Certificate Status | Policy Name | Policy Version | UUID |
|----------|--------------|---------|---------|-------------------|---------------|--------------------|-------------|----------------|----------------------------|
| vmanage | 10.255.255.1 | 1000 | CLI | - | In Sync | Installed | - | - | dfea63a5-66d2-4e50-a07b... |
| vSmart | 10.255.255.3 | 1000 | vManage | vSmart-dev-temp | In Sync | Installed | - | - | 20607a12-c0c8-4f46-a65f... |
| vSmart2 | 10.255.255.4 | 1000 | vManage | vSmart-dev-temp | In Sync | Installed | - | - | 7f332491-cb6f-4843-8bf5... |
| vBond | 10.255.255.2 | 1000 | CLI | - | In Sync | Installed | - | - | fc31c154-99c5-4267-971d... |

This completes our activity of attaching Device Templates to the vSmarts.

Note: If you check the main dashboard screen on vManage at this point, it's possible there will be 2 Control Connections that are down. Log in to the vSmarts via Putty (or SSH to 192.168.0.8 and 192.168.0.9) and issue a `clear control connections`. After a few seconds, all control connections (i.e. 10 of them) should be up.

Task List

- [Configuring VPN 0 Templates for vSmarts](#)
 - [Configuring the main VPN 0 template](#)
 - [Configuring the VPN 0 Interface Template](#)
- [Configuring VPN 512 Templates for vSmarts - Attaching vSmarts to the Device Template and Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 25, 2020

Site last generated: Sep 1, 2020



-->

Service Side VPN configuration - vEdges

Summary: Configure the Service Side VPNs for the vEdges at DC, Site 20 and Site 30

Table of Contents

- [Configuring the vEdge VPN 10 Feature Templates](#)
- [Configuring the vEdge VPN 20 Feature Templates](#)

Task List

- Configuring the vEdge VPN 10 Feature Templates
- Configuring the vEdge VPN 20 Feature Template

Configuring the vEdge VPN 10 Feature Templates

We are now going to set up the Service Side VPNs for our vEdges. The process is very similar to what we've done in the past, and many of the tasks are repetitive in nature.

1. Click on **Configuration => Templates => Feature Tab**

| Configuration Templates | | | | | | | | |
|-----------------------------|--------------------------------------|---------------------|--------------|------------------|------------------|------------|-----------------------------|---------|
| | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
| TLS/SSL Proxy | VPN0 for the Site20 vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 5:41:03 AM PDT | ... |
| Certificates | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR100v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| Network Design | VPN0 for the Site30 INET and MPL... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:25:48 AM PDT | ... |
| Templates | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR100v | 1 | 1 | admin | 23 May 2020 7:15:33 AM PDT | ... |
| Policies | INET Interface for the Site30 vEd... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:27:24 AM PDT | ... |
| Security | vEdge VPN 512 Interface Template... | Cisco VPN Interface | CSR100v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| Unified Communications | VPN0 Template for the vSmart | vSmart VPN | vSmart | 1 | 2 | admin | 25 May 2020 9:51:02 AM PDT | ... |
| Cloud onRamp for SaaS | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR100v | 1 | 1 | admin | 23 May 2020 7:34:59 AM PDT | ... |
| Cloud onRamp for IaaS | MGMT interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 23 May 2020 1:49:11 AM PDT | ... |
| Cloud onRamp for Colocation | MPLS interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:43:22 AM PDT | ... |
| Site20_vpn0_int | INET Interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:39:02 AM PDT | ... |
| DCvEdge-vpn512 | cEdge VPN 0 Template for Single U... | Cisco VPN | CSR100v | 1 | 2 | admin | 18 May 2020 1:24:18 PM PDT | ... |
| DCvEdge-vpn0 | VPN512 Template for the vSmart | vSmart VPN | vSmart | 1 | 2 | admin | 25 May 2020 10:07:03 AM PDT | ... |
| vSmart-vpn512-int | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR100v | 1 | 1 | admin | 18 May 2020 8:28:19 AM PDT | ... |
| | VPN0 for Site20 devices | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 5:48:54 AM PDT | ... |
| | VPN512 for the DC-vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 23 May 2020 1:25:54 AM PDT | ... |
| | VPN0 for the DC-vEdges INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:17:15 AM PDT | ... |
| | VPN512 Interface Template for the... | vSmart Interface | vSmart | 1 | 2 | admin | 25 May 2020 10:11:50 AM PDT | ... |

2. Choose to add a new Template. Search for **ve** and choose the vEdge Cloud. Select the Template as a **VPN Template**

Feature Template > Add Template

Select Devices

- vEdge 100
- vEdge 100 B
- vEdge 100 M
- vEdge 100 WM
- vEdge 1000
- vEdge 2000
- vEdge 5000
- vEdge Cloud

Select Template

BASIC INFORMATION

- AAA
- Archive
- BFD
- NTP
- OMP
- Security
- System

VPN

- Secure Internet Gateway (SIG)
WAN
- VPN
Management | WAN | LAN
- VPN Interface Bridge
LAN
- VPN Interface Cellular
WAN
- VPN Interface Ethernet
Management | WAN | LAN
- VPN Interface GRE
WAN

3. Populate the details as below. Click on **Save** once done

| Section | Field | Global or Device Specific (drop down) | Value |
|---------|---------------|---------------------------------------|---------------------|
| | Template Name | NA | vedge-vpn10 |
| | Description | NA | VPN 10 Template for |

| vEdges | | | |
|---------------------|-----------------------|--------|----------|
| Basic Configuration | VPN | Global | 10 |
| DNS | Primary DNS Address | Global | 10.y.1.5 |
| DNS | Secondary DNS Address | Global | 10.y.1.6 |
| Advertise OMP | Static (IPv4) | Global | On |
| Advertise OMP | Connected (IPv4) | Global | On |

Over here, y is 1 if you're on the SLC DC and 2 if you're on the GHI DC (the email with lab details should enumerate which DC you're on).

Feature Template > Add Template > **VPN**

| | |
|---------------|----------------------------|
| Template Name | vedge-vpn10 |
| Description | VPN 10 Template for vEdges |

Basic Configuration

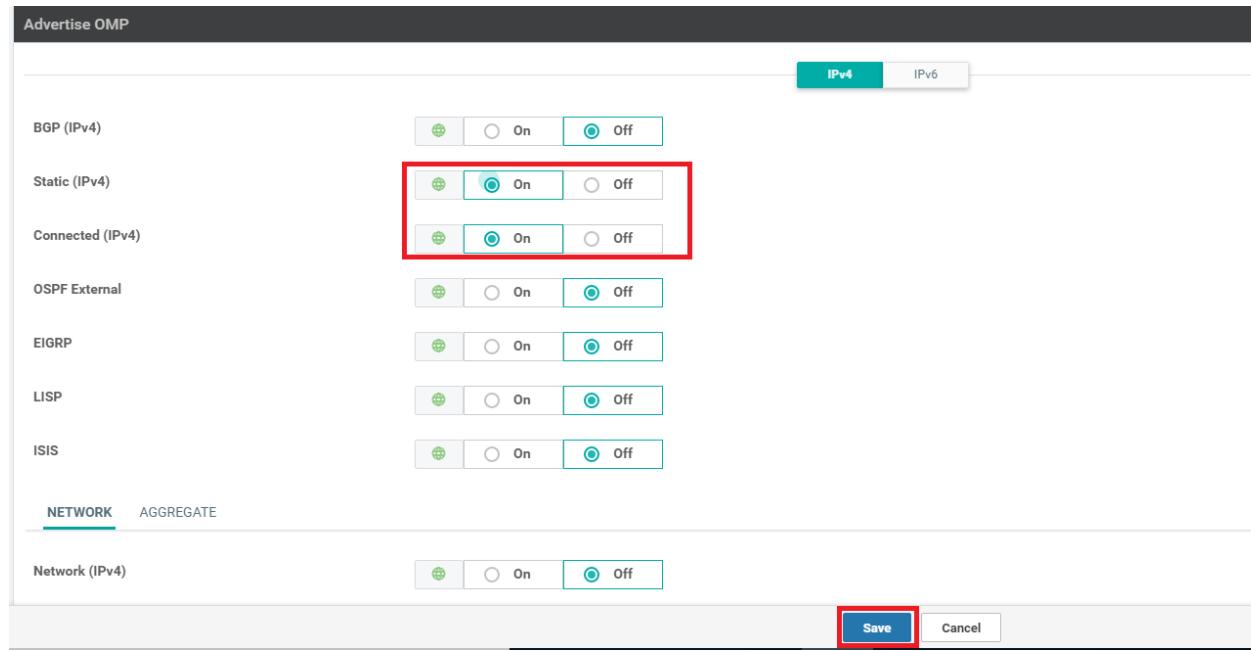
BASIC CONFIGURATION

| | |
|-------------------------|--|
| VPN | 10 |
| Name | <input checked="" type="checkbox"/> |
| Enhance ECMP Keying | <input checked="" type="checkbox"/> <input type="radio"/> On <input type="radio"/> Off |
| Enable TCP Optimization | <input checked="" type="checkbox"/> <input type="radio"/> On <input type="radio"/> Off |

DNS

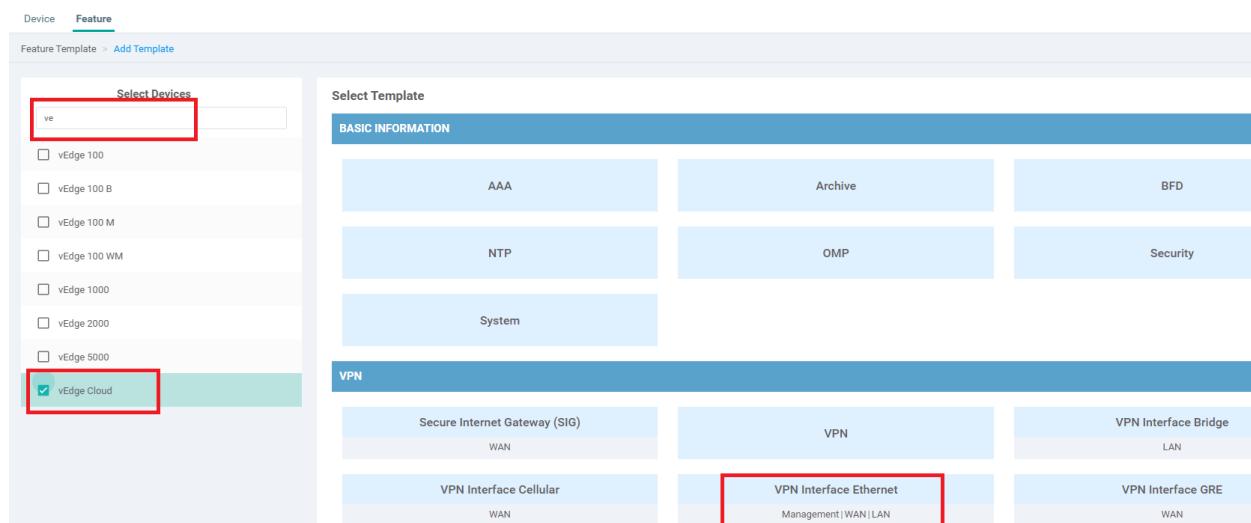
| | |
|------------------------------|----------|
| Primary DNS Address (IPv4) | 10.2.1.5 |
| Secondary DNS Address (IPv4) | 10.2.1.4 |

IPv4 **IPv6**



This creates the VPN template for VPN 10. We will make a copy of this template and create an almost identical template for VPN 20 later on.

4. We now create the vEdge VPN 10 Interface Template. While on the **Configuration => Templates => Feature Tab** page, click on **Add Template** and search for **ve**. Choose the Device as vEdge Cloud and the Template as **VPN Interface Ethernet**



5. Enter the details as shown below and click on **Save** to create the VPN 10 Interface Feature Template

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|----------------|---------------------------------------|---|
| | Template Name | NA | <i>vedge-vpn10-int</i> |
| | Description | NA | <i>VPN 10 Interface Template for vEdges</i> |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | <i>vpn10_if_name</i> |
| Basic Configuration | IPv4 Address | Device Specific | <i>vpn10_if_ipv4_address</i> |

Feature Template > Add Template > **VPN Interface Ethernet**

Device Type: vEdge Cloud

| |
|--|
| Template Name: <i>vedge-vpn10-int</i> |
| Description: <i>VPN 10 Interface Template for vEdges</i> |

Basic Configuration (selected tab)

BASIC CONFIGURATION

| |
|---|
| Shutdown: <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Interface Name: <input type="button"/> <i>[vpn10_if_name]</i> |
| Description: <input type="button"/> |

IPV4 (selected tab)

| |
|---|
| <input type="radio"/> Dynamic <input checked="" type="radio"/> Static |
| IPv4 Address: <input type="button"/> <i>[vpn10_if_ipv4_address]</i> |
| Secondary IP Address (Maximum: 4): <input type="button"/> Add |

Buttons: Save, Cancel

We have finished creating the vEdge VPN 10 Feature Templates needed for Service Side VPNs.

Task List

- Configuring the vEdge VPN 10 Feature Templates
- Configuring the vEdge VPN 20 Feature Template

Configuring the vEdge VPN 20 Feature Templates

1. Locate the *vedge-vpn10* template created and click on the three dots next to it. Choose to **Copy** the template.
Rename the template to *vedge-vpn20* with a Description of *VPN 20 Template for vEdges*. Click on **Copy**

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | ... |
|--------------------------|---------------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|----------------------|
| <i>vedge-vpn10</i> | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| cEdge_vpn0_int-single | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 23 May 2020 6:25:48 AM PDT | ... |
| vEdge30 vpn0 | VPN0 for the Site30 INET and MPL... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 23 May 2020 7:15:33 AM PDT | ... |
| cEdge_vpn0_int-dual_mpls | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 23 May 2020 6:27:24 AM PDT | ... |
| vEdge30_INET | INET interface for the Site30 vEdg... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:27:24 AM PDT | ... |
| cEdge_vpn512_int-dual | cEdge VPN 512 Interface Template... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 8:39:00 AM PDT | ... |
| cEdge_VPN512_dual_uplink | cEdge VPN 512 Template for Dual Up... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 8:35:47 AM PDT | ... |
| cEdge_VPN0_dual_uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin | 23 May 2020 7:34:59 AM PDT | ... |
| <i>vedge-vpn10</i> | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 0 | 0 | admin | 25 May 2020 1:32:55 PM PDT | ... |
| DC-vEdge_mgmt_int | MGMT Interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 23 May 2020 | View |
| vSmart-VPN512 | VPN512 Template for the vSmarts | vSmart VPN | vSmart | 1 | 2 | admin | 25 May 2020 | Edit |
| DC-vEdge_MPLS | MPLS interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 | Change Device Models |
| DC-vEdge_INET | INET interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 | Delete |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single U... | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 | Copy |
| vSmart-VPN512_int | VPN512 Interface for vSmarts | vSmart Interface | vSmart | 1 | 2 | admin | 25 May 2020 9:59:40 AM PDT | ... |

Template Copy

Template Name

vedge-vpn20

Description

VPN 20 Template for vEdges

Copy

Cancel

2. Choose to edit the newly created *vedge-vpn20* template. Make sure the Description is updated and change the VPN field to 20. Click on **Update**

| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single U... | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 | View |
|--------------------------|--------------------------------------|---------------------|-------------|---|---|-------|----------------------------|----------------------|
| vSmart-VPN0-Int | VPNO Interface for vSmarts | vSmart Interface | vSmart | 1 | 2 | admin | 25 May 2020 | Edit |
| cedge-vpn0-int-single | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 | Change Device Models |
| Site20-vpn0 | VPN0 for the Site20 vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 | Delete |
| DC-vEdge_MPLS | MPLS interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 | Copy |
| vedge-vpn20 | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 0 | 0 | admin | 25 May 2020 1:35:11 PM PDT | ... |

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > **VPN**

Device Type vEdge Cloud

Template Name **vedge-vpn20**

Description **VPN 20 Template for vEdges**

This feature template is shared by both Cisco vEdge and IOS-XE SDWAN devices. Please use the [Template Migration](#) tool to migrate the vEdge feature to IOS-XE SDWAN feature templates.

Basic Configuration DNS Advertise OMP IPv4 Route IPv6 Route Service Service Route GRE Route IPSEC Route NAT

BASIC CONFIGURATION

VPN **20**

Name

Enhance ECMP Keying

Enable TCP Optimization

DNS

IPv4 IPv6

Update Cancel

3. At the Feature Templates page, locate the *vedge-vpn10-int* Template and click on the 3 dots next to it. Choose to **Copy** the template. Name the copied template *vedge-vpn20-int* with a Description of *VPN 20 Interface Template for vEdges*. Click on **Copy**

Template Copy

Template Name
vedge-vpn20-int

Description
VPN 20 Interface Template for vEdges

Copy Cancel

4. Locate the newly created *vedge-vpn20-int* Template and click on the three dots next to it. Choose to **Edit**. Update the **Description**, **Interface Name** and **IPv4 Address** to reflect vpn20 instead of vpn10, as shown below and click on **Update**

Device Feature

Feature Template > VPN Interface Ethernet

Device Type vEdge Cloud

Template Name vedge-vpn20-int

Description VPN 20 Interface Template for vEdges

This feature template is shared by both Cisco vEdge and IOS-XE SDWAN devices. Please use the [Template Migration](#) tool to migrate the vEdge feature to IOS-XE SDWAN feature templates.

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

BASIC CONFIGURATION

Shutdown Yes No

Interface Name [vpn20_if_name]

Description

IPv4 **IPv6**

Dynamic Static

IPv4 Address [vpn20_if_ipv4_address]

This completes the configuration of the vEdge VPN 20 Feature Templates for Service Side VPNs.

Task List

- [Configuring the vEdge VPN 10 Feature Templates](#)
- [Configuring the vEdge VPN 20 Feature Template](#)

Site last generated: Sep 1, 2020



Configuring Service Side VPNs - cEdges

Summary: Configure the Service Side VPNs for the cEdges at Sites 40 and 50

Table of Contents

- [Configuring the cEdge VPN 10 Feature Templates](#)
- [Configuring the cEdge VPN 20 Feature Templates](#)
- [Configuring the cEdge VPN 30 Feature Templates](#)

Task List

- Configuring the cEdge VPN 10 Feature Templates
- Configuring the cEdge VPN 20 Feature Templates
- Configuring the cEdge VPN 30 Feature Templates

⚠ Important: Most of the steps in this section are quite repetitive and very similar to the previous section where we configured the Service Side VPN Templates for the vEdges. Thus, the steps will be quite brief, augmented by images which can be used as reference points to complete this section. This will also serve as a way to increase familiarity with creating and managing Templates.

Configuring the cEdge VPN 10 Feature Templates

1. Create a new VPN Template by navigating to **Configuration => Templates => Feature Tab** and choosing to **Add Template**. Search for **csr** and select the **CSR1000V Device Type**, along with selecting the **Cisco VPN** template

2. Populate the details in the Template as shown below and click on **Save**. This will create the VPN 10 Template for cEdges

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|-----------------------|--|---------------------------------------|
| | Template Name | NA | <i>cedge-vpn10</i> |
| | Description | NA | <i>VPN 10 Template for the cEdges</i> |
| Basic Configuration | VPN | Global | 10 |
| DNS | Primary DNS Address | Global | 10.y.1.5 |
| DNS | Secondary DNS Address | Global | 10.y.1.6 |
| Advertise OMP | Static (IPv4) | Global | On |
| Advertise OMP | Connected (IPv4) | Global | On |

Over here, y is 1 if you're on the SLC DC and 2 if you're on the GHI DC (the email with lab details should enumerate which DC you're on).

Device **Feature**

Feature Template > Add Template > [Cisco VPN](#)

| | |
|---------------|--------------------------------|
| Device Type | CSR1000v |
| Template Name | cedge-vpn10 |
| Description | VPN 10 Template for the cEdges |

Basic Configuration DNS Advertise OMP IPv4 Route IPv6 Route Service Service Route GRE Route IPSEC Route NAT

BASIC CONFIGURATION

VPN 10

Name

Enhance ECMP Keying On Off

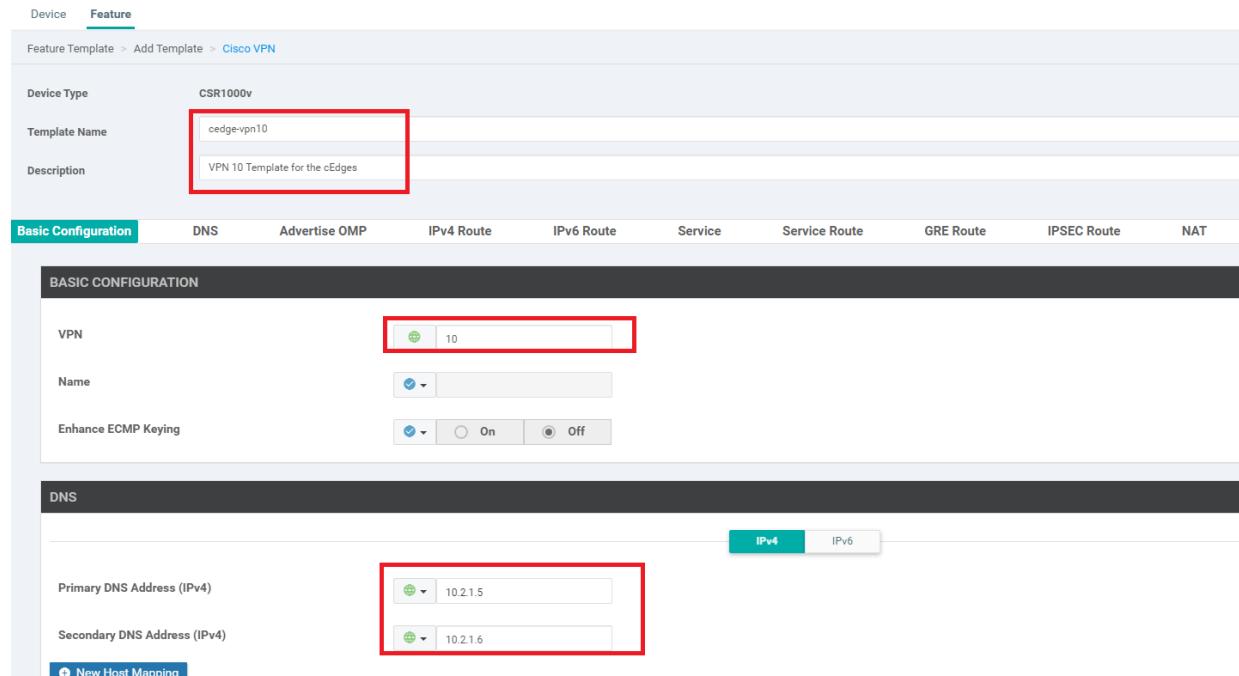
DNS

IPv4 **IPv6**

Primary DNS Address (IPv4) 10.2.1.5

Secondary DNS Address (IPv4) 10.2.1.6

[New Host Mapping](#)



The screenshot shows the 'Feature' tab selected in the 'CONFIGURATION | TEMPLATES' interface. Under 'Feature Template > Add Template > Cisco VPN', the 'Advertise OMP' tab is active. The 'IPv4' tab is selected. The configuration section displays various protocols with 'On' or 'Off' status buttons. The 'Static (IPv4)' and 'Connected (IPv4)' sections are highlighted with a red box, and their 'On' buttons are also highlighted with a red box. At the bottom right, the 'Save' button is highlighted with a red box.

3. We will now create the VPN 10 Interface Template for cEdges. While on the **Configuration => Templates => Feature** Tab page, click on **Add Template** and search for **csr**. Choose the Device as CSR1000v and the Template as **Cisco VPN Interface Ethernet**

The screenshot shows the 'Add Template' dialog. In the 'Select Devices' section, 'CSR1000v' is selected and highlighted with a red box. In the 'Select Template' section, the 'VPN' tab is selected. Under the 'VPN' tab, the 'Cisco VPN Interface Ethernet' template is highlighted with a red box. The 'Management | WAN | LAN' category is also highlighted with a red box.

4. Populate the details as shown below and click on **Save**

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|--------------------------------|--|---|
| | Template Name | NA | <i>cedge-vpn10-int</i> |
| | Description | NA | <i>VPN 10 Interface Template for cEdges</i> |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | <i>vpn10_if_name</i> |
| Basic Configuration | IPv4 Address/ prefix-length | Device Specific | <i>vpn10_if_ipv4_address</i> |

Device **Feature**

Feature Template > Add Template > [Cisco VPN Interface Ethernet](#)

| | |
|---------------|---|
| Device Type | CSR1000v |
| Template Name | <input type="text" value="cedge-vpn10-int"/> |
| Description | <input type="text" value="VPN 10 Interface Template for cEdges"/> |

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP Advanced

BASIC CONFIGURATION

| | |
|--|---|
| Shutdown | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Interface Name | <input type="text" value="vpn10_if_name"/> |
| Description | <input type="text"/> |
| <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 | |
| IPv4 Address/ prefix-length | <input type="text" value="vpn10_if_ipv4_address"/> |
| Secondary IP Address (Maximum: 4) | <input type="button" value="Add"/> |
| DHCP Helper | <input type="text"/> |

Save **Cancel**

This completes the configuration of the VPN 10 Feature Templates for the cEdges.

Task List

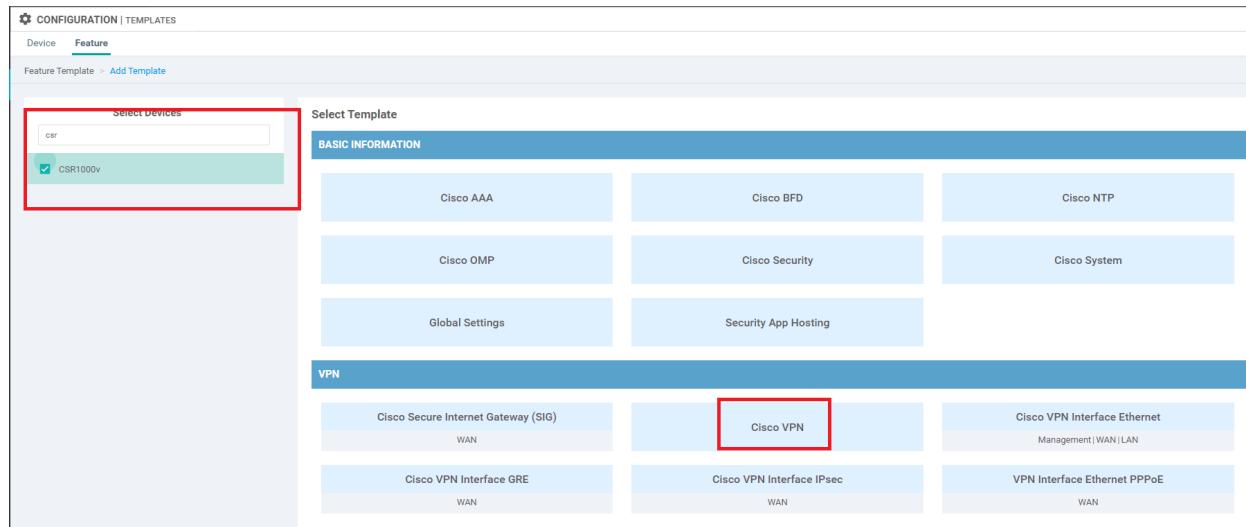
- Configuring the cEdge VPN 10 Feature Templates
- Configuring the cEdge VPN 20 Feature Templates
- Configuring the cEdge VPN 30 Feature Templates

Configuring the cEdge VPN 20 Feature Templates

As indicated before, creating the templates is a repetitive task so we will be going through pretty much the same steps as before, changing `vpn10` to `vpn20` wherever applicable.

1. Create a new VPN Template by navigating to **Configuration => Templates => Feature Tab** and choosing to **Add Template**. Search for csr and select the CSR1000V Device Type, along with selecting the **Cisco VPN** template.

Alternatively, you can create a copy of the `cedge-vpn10` template, rename it to `cedge-vpn20` and then edit the specifics clicking on **Update** to save the changes (followed in step 2 below).



2. Populate the details in the Template as shown below and click on **Save**. This will create the VPN 20 Template for cEdges

| Section | Field | Global or Device Specific (drop down) | Value |
|---------|-------|--|-------|
|---------|-------|--|-------|

| | | | |
|---------------------|-----------------------|--------|---------------------------------------|
| | Template Name | NA | <i>cedge-vpn20</i> |
| | Description | NA | <i>VPN 20 Template for the cEdges</i> |
| Basic Configuration | VPN | Global | 20 |
| DNS | Primary DNS Address | Global | 10.y.1.5 |
| DNS | Secondary DNS Address | Global | 10.y.1.6 |
| Advertise OMP | Static (IPv4) | Global | On |
| Advertise OMP | Connected (IPv4) | Global | On |

Over here, y is 1 if you're on the SLC DC and 2 if you're on the GHI DC (the email with lab details should enumerate which DC you're on).

S CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN

Device Type CSR1000v

Template Name cedge-vpn20

Description VPN 20 Template for the cEdges

Basic Configuration DNS Advertise OMP IPv4 Route IPv6 Route Service Service Route GRE Route IPSEC Route NAT

BASIC CONFIGURATION

VPN 20

Name

Enhance ECMP Keying On Off

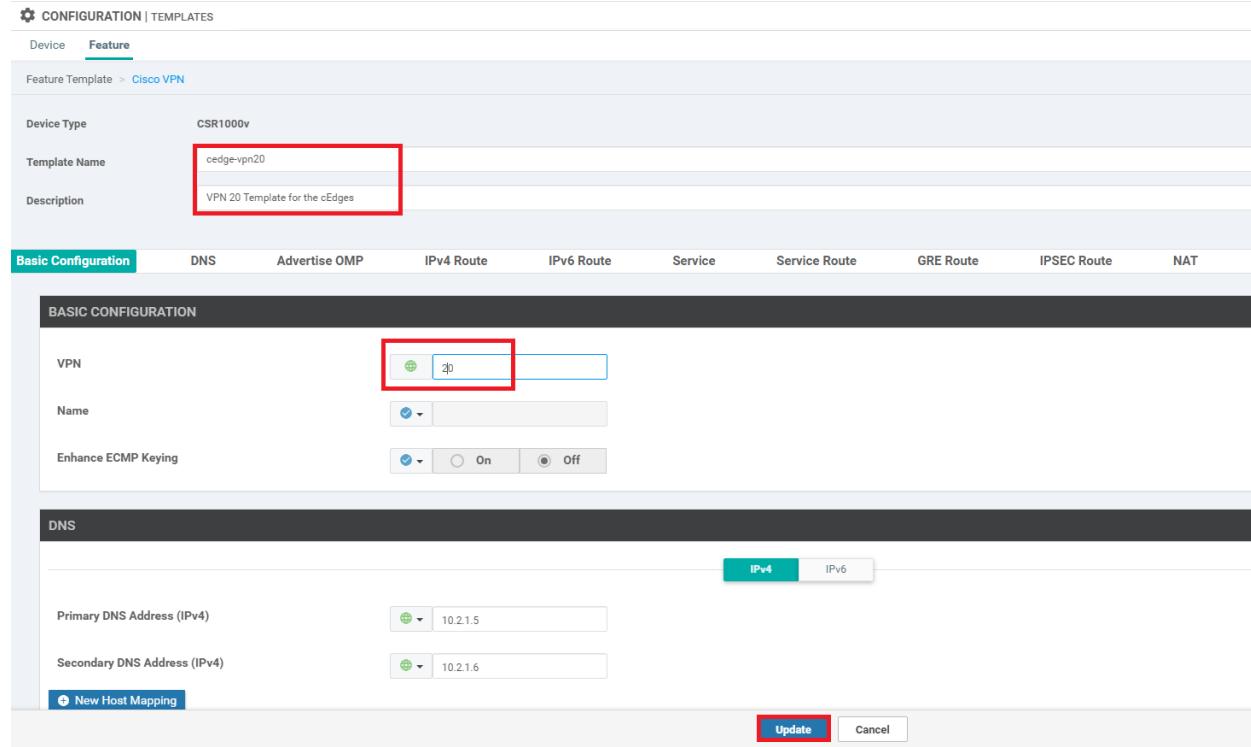
DNS

IPv4 **IPv6**

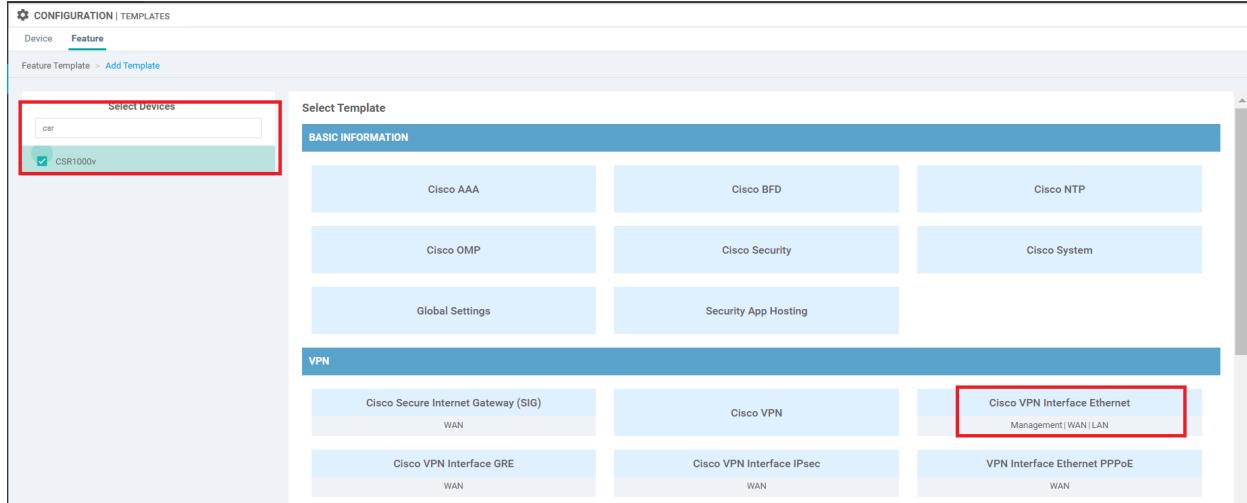
Primary DNS Address (IPv4)

Secondary DNS Address (IPv4)

New Host Mapping + Update Cancel



3. We will now create the VPN 20 Interface Template for cEdges. While on the **Configuration => Templates => Feature** Tab page, click on **Add Template** and search for **csr**. Choose the Device as CSR1000v and the Template as **Cisco VPN Interface Ethernet**. Once again, alternatively, make a copy of the *cedge-vpn10-int* template and rename it to *cedge-vpn20-int*, updating the description. Then Edit this newly created template and **Update** (followed in step 4 below)



4. Populate the details as shown below and click on **Save**

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|--------------------------------|--|---|
| | Template Name | NA | <i>cedge-vpn20-int</i> |
| | Description | NA | <i>VPN 20 Interface Template for cEdges</i> |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | <i>vpn20_if_name</i> |
| Basic Configuration | IPv4 Address/ prefix-length | Device Specific | <i>vpn20_if_ipv4_address</i> |

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN Interface Ethernet

Device Type: CSR1000v
Template Name: cedge-vpn20-int
Description: VPN 20 Interface Template for cEdges

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP Advanced

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: [vpn20_if_name]

Description:

IPv4 **IPv6**

Dynamic Static

IPv4 Address/ prefix-length: [vpn20_if_ip4_address]

Secondary IP Address (Maximum: 4): Add

DHCP Helper:

Update **Cancel**

This completes the configuration of the VPN 20 Feature Templates for the cEdges.

Task List

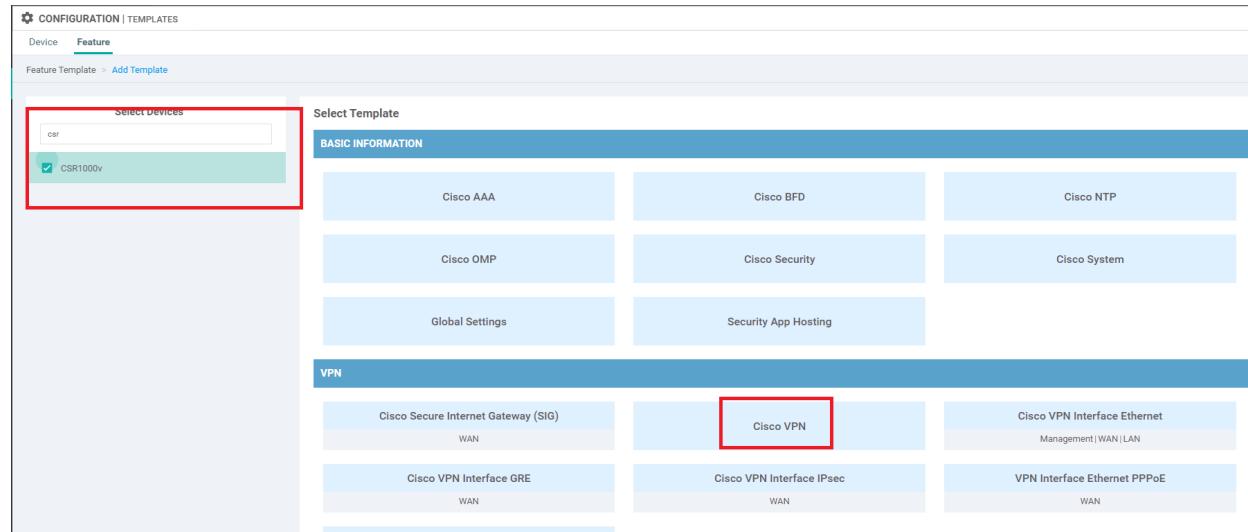
- [Configuring the cEdge VPN 10 Feature Templates](#)
- [Configuring the cEdge VPN 20 Feature Templates](#)
- [Configuring the cEdge VPN 30 Feature Templates](#)

Configuring the cEdge VPN 30 Feature Templates

As indicated before, creating the templates is a repetitive task so we will be going through pretty much the same steps as before, changing *vpn10* to *vpn30* wherever applicable.

1. Create a new VPN Template by navigating to **Configuration => Templates => Feature Tab** and choosing to **Add Template**. Search for *csr* and select the CSR1000V Device Type, along with selecting the **Cisco VPN** template.

Alternatively, you can create a copy of the `cedge-vpn10` template, rename it to `cedge-vpn30` and then edit the specifics clicking on **Update** to save the changes (followed in step 2 below).



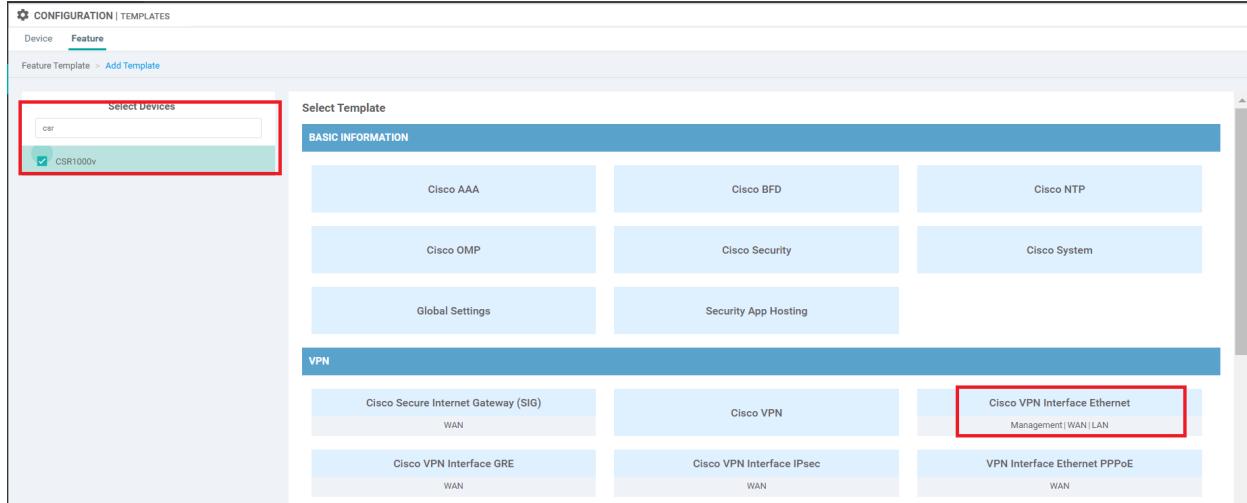
2. Populate the details in the Template as shown below and click on **Save**. This will create the VPN 30 Template for cEdges

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|-----------------------|--|---------------------------------------|
| | Template Name | NA | <i>cedge-vpn30</i> |
| | Description | NA | <i>VPN 30 Template for the cEdges</i> |
| Basic Configuration | VPN | Global | 30 |
| DNS | Primary DNS Address | Global | 10.y.1.5 |
| DNS | Secondary DNS Address | Global | 10.y.1.6 |
| Advertise OMP | Static (IPv4) | Global | On |
| Advertise OMP | Connected (IPv4) | Global | On |

Over here, y is 1 if you're on the SLC DC and 2 if you're on the GHI DC (the email with lab details should enumerate which DC you're on).

The screenshot shows the 'Feature' tab selected in the 'Configuration | Templates' interface. A new template named 'cedge-vpn30' is being created for a 'CSR1000v' device. The 'Template Name' field contains 'cedge-vpn30'. The 'Description' field is set to 'VPN 30 Template for the cEdges'. The 'Basic Configuration' tab is active, displaying sections for 'BASIC CONFIGURATION' and 'DNS'. In the 'BASIC CONFIGURATION' section, the 'VPN' field has the value '30' highlighted with a red box. In the 'DNS' section, the 'IPv4' tab is selected, showing 'Primary DNS Address (IPv4)' as 10.2.1.5 and 'Secondary DNS Address (IPv4)' as 10.2.1.6. A 'New Host Mapping' button is visible. At the bottom right of the configuration area, there are 'Update' and 'Cancel' buttons, with 'Update' also highlighted with a red box.

3. We will now create the VPN 30 Interface Template for cEdges. While on the **Configuration => Templates => Feature Tab** page, click on **Add Template** and search for **csr**. Choose the Device as CSR1000v and the Template as **Cisco VPN Interface Ethernet**. Once again, alternatively, make a copy of the *cedge-vpn10-int* template and rename it to *cedge-vpn30-int*, updating the description. Then Edit this newly created template and **Update** (followed in step 4 below)



4. Populate the details as shown below and click on **Save**

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|--------------------------------|--|---|
| | Template Name | NA | <i>cedge-vpn30-int</i> |
| | Description | NA | <i>VPN 30 Interface Template for cEdges</i> |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | <i>vpn30_if_name</i> |
| Basic Configuration | IPv4 Address/ prefix-length | Device Specific | <i>vpn30_if_ipv4_address</i> |

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN Interface Ethernet

Device Type: CSR1000v
Template Name: cedge-vpn30-int
Description: VPN 30 Interface Template for cEdges

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP Advanced

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: [vpn30_if_name]

Description:

IPv4 **IPv6**

Dynamic Static

IPv4 Address/ prefix-length: [vpn30_if_ipv4_address]

Secondary IP Address (Maximum: 4): Add

DHCP Helper:

Update **Cancel**

This completes the configuration of the VPN 30 Feature Templates for the cEdges.

Task List

- [Configuring the cEdge VPN 10 Feature Templates](#)
- [Configuring the cEdge VPN 20 Feature Templates](#)
- [Configuring the cEdge VPN 30 Feature Templates](#)

Site last generated: Sep 1, 2020



-->

Updating Device Templates with Service Side VPNs

Summary: Associate the Service Side VPN Templates with the Device Templates

Table of Contents

- [Updating vEdge Device Templates for Service Side VPNs](#)
 - [Updating the DC-vEdge Device Template](#)
 - [Updating the Site 20 Device Template](#)
 - [Updating the Site 30 Device Template](#)
- [Updating cEdge Device Templates for Service Side VPNs](#)
 - [Updating the Site 40 Device Template](#)
 - [Updating the Site 50 Device Template](#)

Task List

- Updating vEdge Device Templates for Service Side VPNs
 - Updating the DC-vEdge Device Template
 - Updating the Site 20 Device Template
 - Updating the Site 30 Device Template
- Updating cEdge Device Templates for Service Side VPNs
 - Updating the Site 40 Device Template
 - Updating the Site 50 Device Template

Updating vEdge Device Templates for Service Side VPNs

Since our Feature Templates for Service Side VPNs are ready, we will now update the Device Templates to push the corresponding configuration to the Devices.

Updating the DC-vEdge Device Template

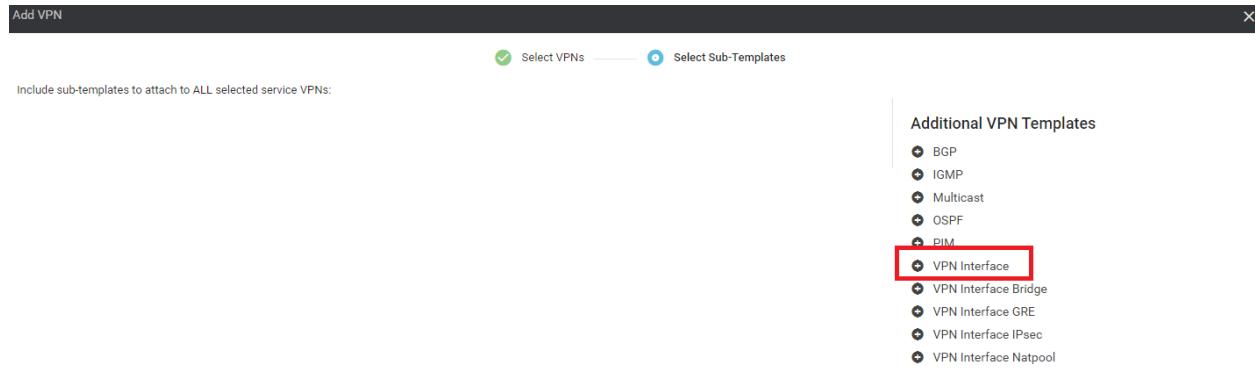
1. On the vManage GUI, go to **Configuration => Templates**. You should be on the **Device** tab. Locate the **DCvEdge_dev_temp** and click on the 3 dots next to it. Choose to **Edit** the template

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Actions |
|--------------------------|------------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|---------|
| vEdge30_dev_temp | Device template for the Site 30... | Feature | vEdge Cloud | 11 | 1 | admin | 23 May 2020 6:36:47 AM PDT | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud | 10 | 2 | admin | 23 May 2020 5:53:51 AM PDT | In Sync | ... |
| cEdge_dualuplink_devtemp | cEdge Device Template for dev... | Feature | CSR1000v | 12 | 1 | admin | 23 May 2020 7:39:59 AM PDT | In Sync | ... |
| vSmart-dev-temp | Device Template for vSmarts | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 AM PDT | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync | ... |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 11 | 2 | admin | 23 May 2020 1:55:53 AM PDT | In Sync | ... |

2. Scroll down to the **Service VPN** section and click on **Add VPN**. Move **vedge-vpn10** to the list of **Selected VPN Templates** and click on **Next**

The screenshot shows the 'Add VPN' dialog box overlaid on the main vManage interface. In the 'Available VPN Templates' list, there is one item: 'vedge-vpn20'. In the 'Selected VPN Templates' list, there is one item: 'vedge-vpn10'. At the bottom of the dialog, there are 'Next' and 'CANCEL' buttons, with 'Next' highlighted by a red box.

3. Under **Additional VPN Templates** on the left-hand side, click on **VPN Interface**



4. Choose the *vedge-vpn10-int* template from the drop down and click on **Add**.

Add VPN

Select VPNs ————— Select Sub-Templates

Include sub-templates to attach to ALL selected service VPNs:

VPN Interface

vedge-vpn10-int ▾



+ Sub-Templates ▾

BACK

Add

CANCEL

5. Click on **Add VPN** under **Service VPN** again (to add the VPN 20 service VPN) and move *vedge-vpn20* under **Selected VPN Templates**. Click on **Next**

Add VPN

Select one or more Service VPNs to add:

Available VPN Templates

| ID | Template Name |
|----|---------------|
| | |

Selected VPN Templates

| ID | Template Name |
|--------------------------------------|---------------|
| 6fd47ee6-61c1-4b02-9b3e-439f5c423b74 | vedge-vpn20 |

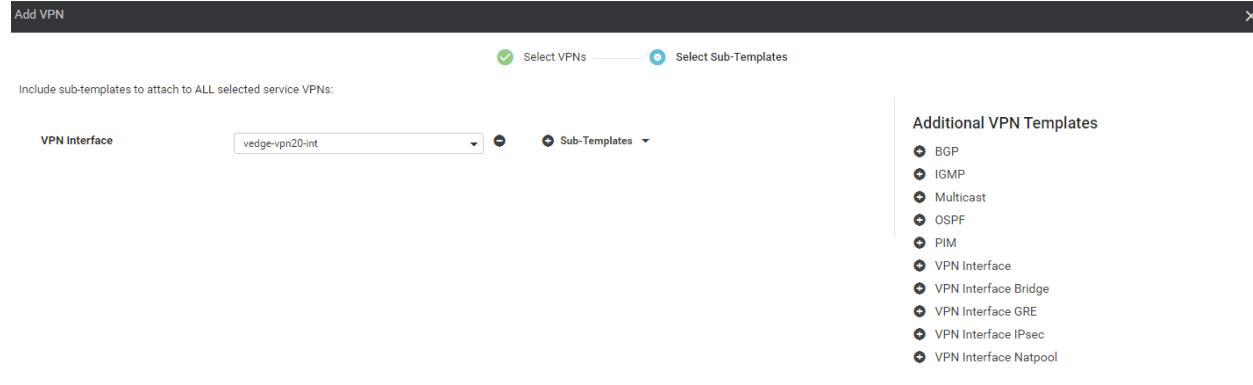
→ ←

Create VPN Template

Next CANCEL

The screenshot shows the 'Add VPN' configuration screen. On the left, there's a list of 'Available VPN Templates' with a search bar and dropdown menu. On the right, the 'Selected VPN Templates' list shows a single entry: '6fd47ee6-61c1-4b02-9b3e-439f5c423b74' with the name 'vedge-vpn20'. A red box highlights this entry. At the bottom, there are 'Create VPN Template' and 'Next' buttons, with 'Next' being the one highlighted by a red box.

6. Click on **VPN Interface** under **Additional VPN Templates** and select the *vedge-vpn20-int* template from the drop down. Click on **Add**



7. Make sure the Device Template **Service VPN** section looks as below, and click on **Update**

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|---------------|
| e9acf7d-aad6-4913-8f0a-84e255b4b033 | vedge-vpn10 | VPN Interface |
| 6fd47ee6-61c1-4b02-9b3e-439f5c423b74 | vedge-vpn20 | VPN Interface |

8. Enter the details as shown in the figure below and click on **Next**. These details can be found in the Overview => Topology and IP Addressing section of the guide

Update Device Template

Variable List (Hover over each field for more information)

| System IP | 10.255.255.11 |
|-------------------------------------|-------------------|
| Hostname | DC-vEdge1 |
| Address(vpn512_next_hop) | 192.168.0.1 |
| Interface Name(vpn512_mgmt_if_name) | eth0 |
| IPv4 Address(vpn512_mgmt_if_ip) | 192.168.0.10/24 |
| Address(vpn0_inet_next_hop) | 100.100.100.1 |
| Address(vpn0_mpls_next_hop) | 192.0.2.1 |
| Interface Name(vpn0_mpls_if_name) | ge0/1 |
| IPv4 Address(vpn0_mpls_if_ip) | 192.0.2.2/30 |
| Color(vpn0_mpls_if_color) | mpls |
| Interface Name(vpn0_inet_if_name) | ge0/0 |
| IPv4 Address(vpn0_inet_if_ip) | 100.100.100.10/24 |
| Color(vpn0_inet_if_color) | public-internet |
| Hostname | DC-vEdge1 |
| System IP | 10.255.255.11 |
| Site ID | 1 |
| Interface Name(vpn20_if_name) | ge0/3 |
| IPv4 Address(vpn20_if_ipv4_address) | 10.100.20.2/24 |
| Interface Name(vpn10_if_name) | ge0/2 |
| IPv4 Address(vpn10_if_ipv4_address) | 10.100.10.2/24 |

Generate Password **Update** **Cancel**

Update Device Template

Variable List (Hover over each field for more information)

| | |
|-------------------------------------|-------------------|
| System IP | 10.255.255.12 |
| Hostname | DC-vEdge2 |
| Address(vpn512_next_hop) | 192.168.0.1 |
| Interface Name(vpn512_mgmt_if_name) | eth0 |
| IPv4 Address(vpn512_mgmt_if_ip) | 192.168.0.11/24 |
| Address(vpn0_inet_next_hop) | 100.100.100.1 |
| Address(vpn0_mpls_next_hop) | 192.0.2.5 |
| Interface Name(vpn0_mpls_if_name) | ge0/1 |
| IPv4 Address(vpn0_mpls_if_ip) | 192.0.2.6/30 |
| Color(vpn0_mpls_if_color) | mpls |
| Interface Name(vpn0_inet_if_name) | ge0/0 |
| IPv4 Address(vpn0_inet_if_ip) | 100.100.100.11/24 |
| Color(vpn0_inet_if_color) | public-internet |
| Hostname | DC-vEdge2 |
| System IP | 10.255.255.12 |
| Site ID | 1 |
| Interface Name(vpn20_if_name) | ge0/3 |
| IPv4 Address(vpn20_if_ipv4_address) | 10.100.20.3/24 |
| Interface Name(vpn10_if_name) | ge0/2 |
| IPv4 Address(vpn10_if_ipv4_address) | 10.100.10.3/24 |

Generate Password **Update** **Cancel**

9. Check the side by side configuration to see the commands that will be added and click on **Configure Devices**.
Confirm the change and click on **OK**

Device list (Total: 2 devices)

Filter/Search

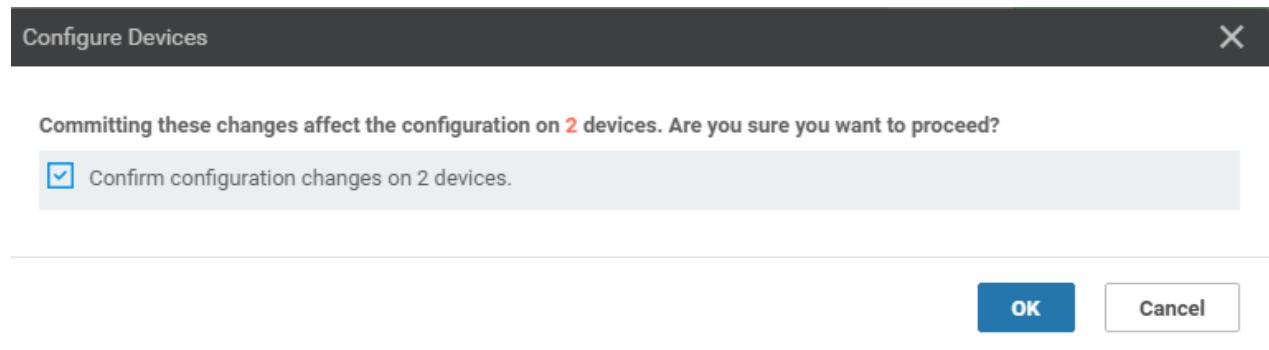
```

86 !
87 no shutdown
88 !
89 ip route 0.0.0.0/0 100.100.100.1
90 ip route 0.0.0.0/0 192.0.2.1
91 !
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
92  vpn 512
93    dns 10.2.1.5 primary
94    dns 10.2.1.6 secondary

```

Configure Device Rollback Timer

Back Configure Devices Cancel



Task List

- Updating vEdge Device Templates for Service Side VPNs
 - [Updating the DC-vEdge Device Template](#)
 - Updating the Site 20 Device Template
 - Updating the Site 30 Device Template
- Updating cEdge Device Templates for Service Side VPNs

- Updating the Site 40 Device Template
- Updating the Site 50 Device Template

Updating the Site 20 Device Template

Follow the same steps as the previous section, making changes as required.

1. From **Configuration => Templates** locate the *vedge_Site20_dev_temp* Device Template and click on the three dots. Choose to **Edit**.
2. Scroll to the **Service VPN** section and click on **Add VPN**. Move *vedge-vpn10* to the list of Selected VPN Templates and click on **Next**
3. Click on **VPN Interface** under **Additional VPN Templates** and select *vedge-vpn10-int* from the drop down. Click on **Add**
4. Repeat Steps 1 to 3, choosing the *vedge-vpn20* VPN Template and the *vedge-vpn20-int* VPN Interface Template as applicable. Your final Device Template page should look like the image below. Click on **Update**

The screenshot shows the 'Service VPN' configuration page. At the top, there are buttons for 'Add VPN' and 'Remove VPN'. Below is a table with columns: ID, Template Name, and Sub-Templates. Two rows are listed:

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|---------------|
| e9acfe7d-aad6-4913-8f0a-84e255b4b033 | vedge-vpn10 | VPN Interface |
| 6fd47ee6-61c1-4b02-9b3e-439f5c423b74 | vedge-vpn20 | VPN Interface |

Below the table is the 'Additional Templates' section, which includes dropdown menus for Banner, Policy, SNMP, and Security Policy. At the bottom, there is a 'Bridge' section with a radio button for 'Bridge' and a 'Update' button.

5. Enter the details as shown below and click on **Next**. Click on **Configure Devices** and confirm the selection. You can also reference the table in the Overview => Topology and IP Addressing section of the guide for the device details

| S. | Chassis Number | System IP | Hostname | Interface Name(vpn20_if_name) | IPv4 Address(vpn20_if_ipv4_address) | Interface Name(vpn10_if_name) | IPv4 Address(vpn10_if_ipv4_address) | Address |
|----|--------------------------------------|---------------|----------|-------------------------------|-------------------------------------|-------------------------------|-------------------------------------|-------------|
| 1 | b7fd7295-58df-7671-e914-6fe2edff1609 | 10.255.255.21 | vEdge20 | ge0/3 | 10.20.20.2/24 | ge0/2 | 10.20.10.2/24 | 192.168 ... |
| 2 | dde90ff0-dcb2-77e6-510f-08d9608537d | 10.255.255.22 | vEdge21 | ge0/3 | 10.20.20.3/24 | ge0/2 | 10.20.10.3/24 | 192.168 ... |

Task List

- Updating vEdge Device Templates for Service Side VPNs
 - [Updating the DC vEdge Device Template](#)
 - [Updating the Site 20 Device Template](#)
 - [Updating the Site 30 Device Template](#)
- Updating cEdge Device Templates for Service Side VPNs
 - [Updating the Site 40 Device Template](#)
 - [Updating the Site 50 Device Template](#)

Updating the Site 30 Device Template

Follow the same steps as the previous section, making changes as required.

1. From **Configuration => Templates** locate the *vedge30_dev_temp* Device Template and click on the three dots. Choose to **Edit**.
2. Scroll to the **Service VPN** section and click on **Add VPN**. Move *vedge-vpn10* to the list of Selected VPN Templates and click on **Next**
3. Click on **VPN Interface** under **Additional VPN Templates** and select *vedge-vpn10-int* from the drop down. Click on **Add**
4. Repeat Steps 1 to 3, choosing the *vedge-vpn20* VPN Template and the *vedge-vpn20-int* VPN Interface Template as applicable. Your final Device Template page should look like the image below. Click on **Update**

Service VPN

The screenshot shows the 'Service VPN' configuration page. At the top, there are buttons for '0 Rows Selected', 'Add VPN', and 'Remove VPN'. Below this is a search bar and a table with columns: ID, Template Name, and Sub-Templates. Two rows are listed:

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|---------------|
| e9acf7d-aad5-4913-8f0a-84e255b4b033 | vedge-vpn10 | VPN Interface |
| 6fd47ee6-61c1-4b02-9b3e-439f5c423b74 | vedge-vpn20 | VPN Interface |

Below the table is a section titled 'Additional Templates' with dropdown menus for Banner, Policy, SNMP, and Security Policy. At the bottom, there are tabs for 'Bridge' and 'Bridge' (selected), and buttons for 'Update' and 'Cancel'.

5. Enter the details as shown below and click on **Next**. Click on **Configure Devices**. You can also reference the table in the Overview => Topology and IP Addressing section of the guide for the device details

The screenshot shows a table with a single row of data. The columns are: Chassis Number, System IP, Hostname, Interface Name(vpn20_if_name), IPv4 Address(vpn20_if_ipv4_address), Interface Name(vpn10_if_name), IPv4 Address(vpn10_if_ipv4_address), and Address. The data is as follows:

| Chassis Number | System IP | Hostname | Interface Name(vpn20_if_name) | IPv4 Address(vpn20_if_ipv4_address) | Interface Name(vpn10_if_name) | IPv4 Address(vpn10_if_ipv4_address) | Address |
|--------------------------------------|---------------|----------|-------------------------------|-------------------------------------|-------------------------------|-------------------------------------|-------------|
| 17026153-f09e-be4b-6dce-482fce43aab2 | 10.255.255.31 | vEdge30 | ge0/3 | 10.30.20.2/24 | ge0/2 | 10.30.10.2/24 | 192.168 ... |

Task List

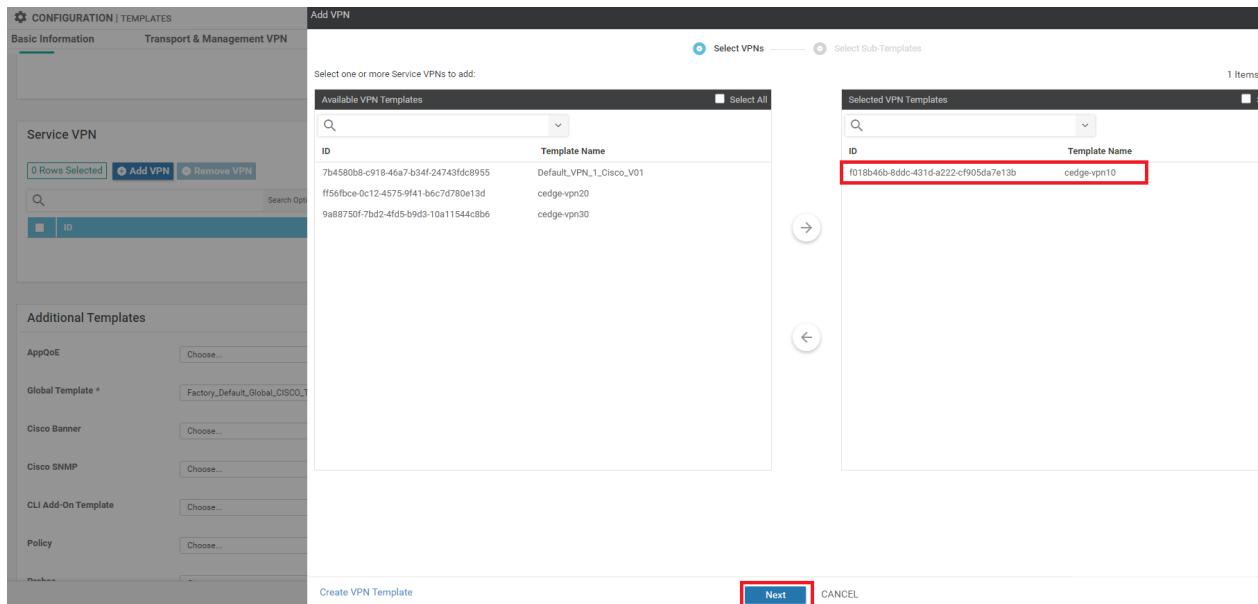
- [Updating vEdge Device Templates for Service Side VPNs](#)
 - [Updating the DC vEdge Device Template](#)
 - [Updating the Site 20 Device Template](#)
 - [Updating the Site 30 Device Template](#)
- [Updating cEdge Device Templates for Service Side VPNs](#)
 - [Updating the Site 40 Device Template](#)
 - [Updating the Site 50 Device Template](#)

Updating cEdge Device Templates for Service Side VPNs

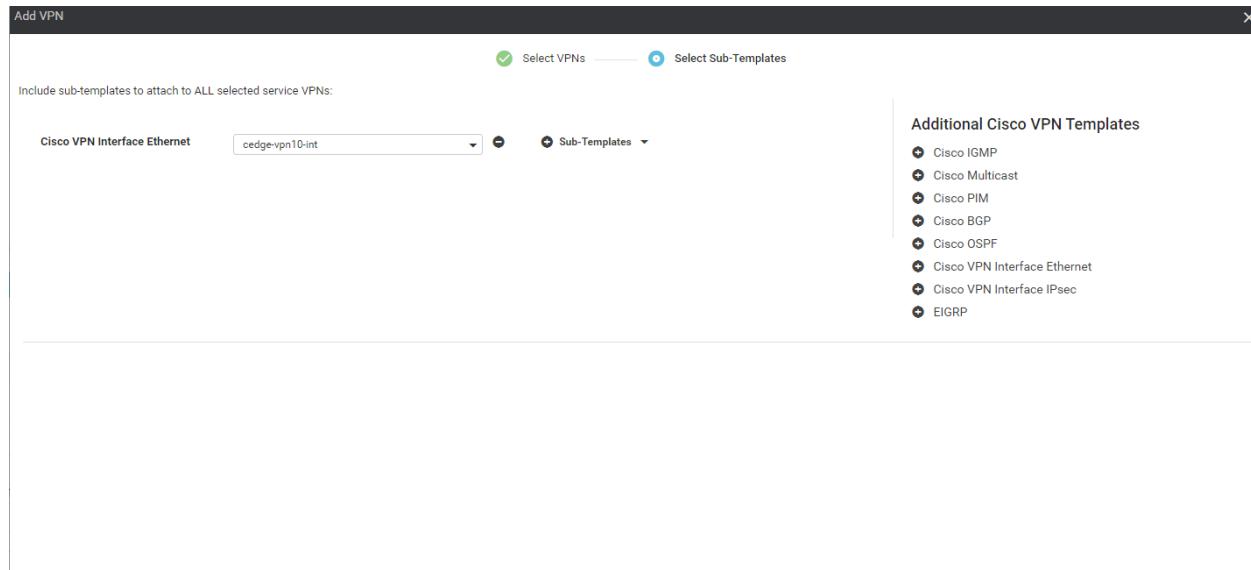
The cEdges will have 3 Service Side VPNs associated (VPN 10, VPN 20 and VPN 30) with them. We have already created the Feature Templates for these and are now going to update the Device Templates for the cEdges to reflect these Feature Templates.

Updating the Site 40 Device Template

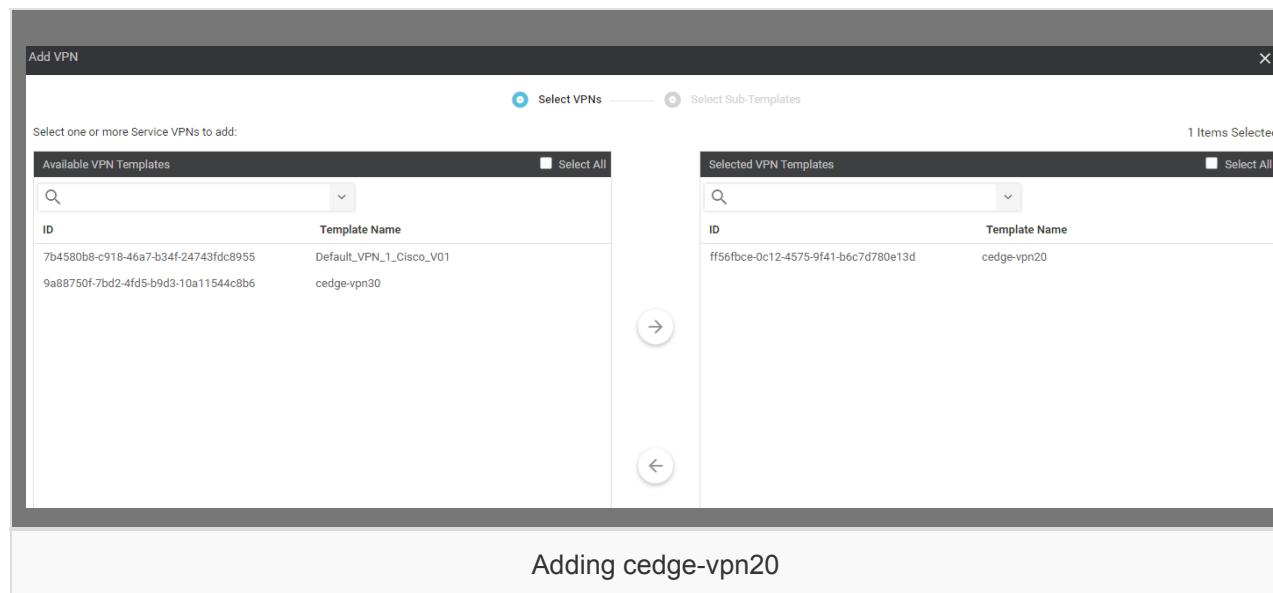
1. While on **Configuration => Templates**, click on the three dots next to *cEdge_dualuplink_devtemp* and choose to **Edit**. Scroll down to the **Service VPN** section and click on **Add VPN**. Move *cedge-vpn10* to the list of Selected VPN Templates. Click on **Next**

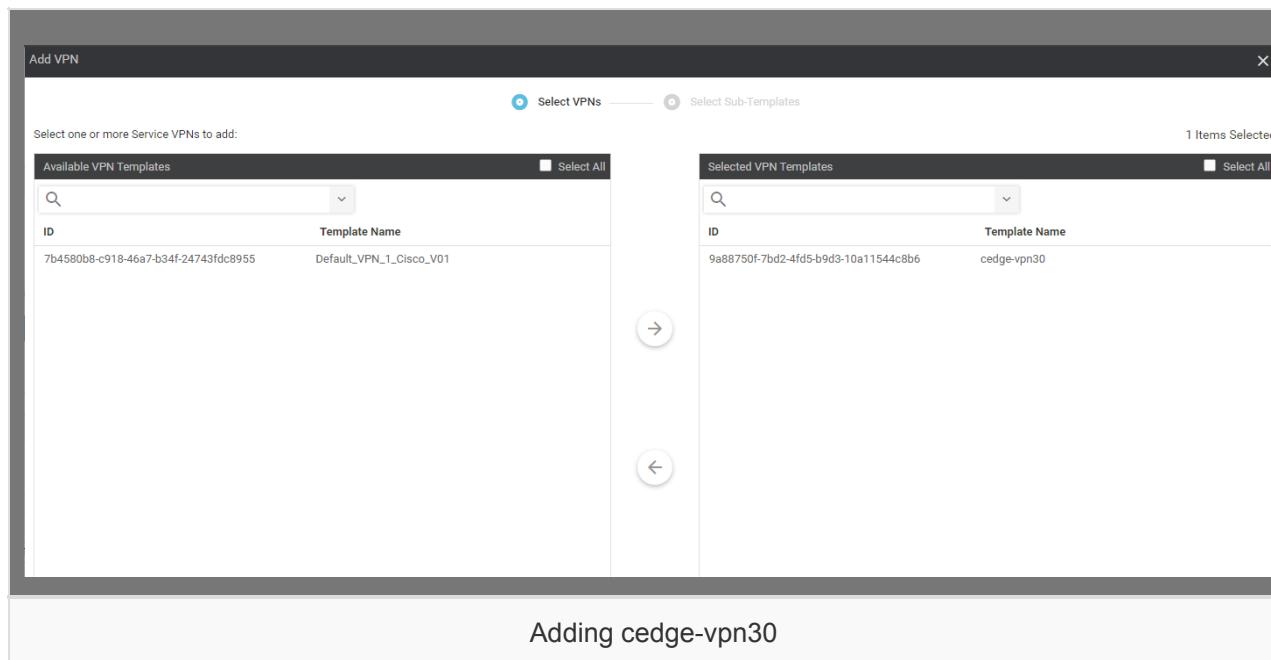
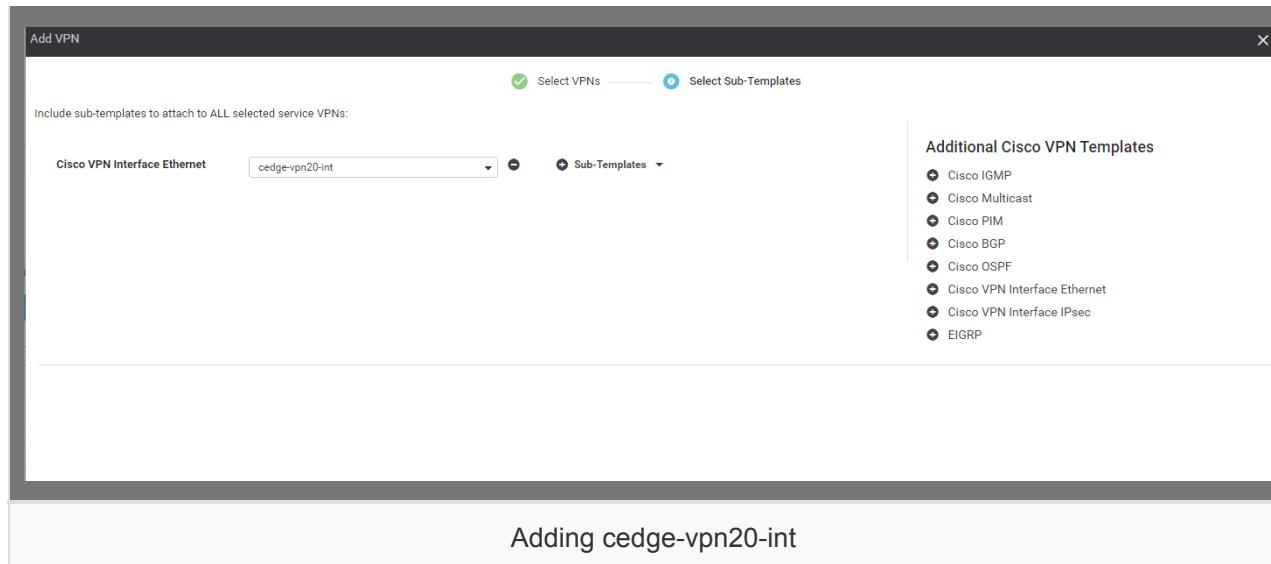


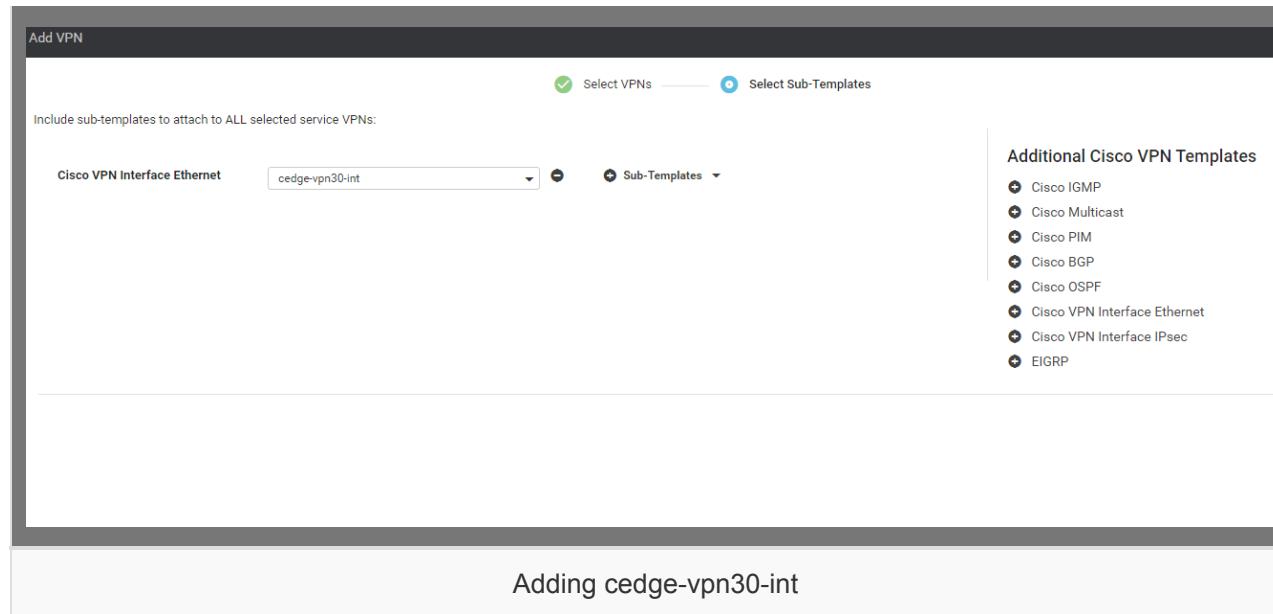
2. Click on **Cisco VPN Interface Ethernet** under Additional Cisco VPN Templates and choose *cedge-vpn10-int* in the drop down. Click on **Add**



3. Repeat steps 1 and 2 for `cedge-vpn20`, `cedge-vpn20-int` and then for `cedge-vpn30`, `cedge-vpn30-int`. Reference the images given below







Adding cedge-vpn30-int

4. Click on **Update** once done adding all three VPNs. The final Device Template page should look like this

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|------------------------------|
| f018b46b-8ddc-431d-a222-cf905da7e13b | cedge-vpn10 | Cisco VPN Interface Ethernet |
| ff56fbce-0c12-4575-9f41-b6c7d780e13d | cedge-vpn20 | Cisco VPN Interface Ethernet |
| 9a88750f-7bd2-4fd5-b9d3-10a11544c8b6 | cedge-vpn30 | Cisco VPN Interface Ethernet |

5. Click on the three dots next to the device and choose **Edit Device Template**. Enter the details as shown (details are also available in the Overview => Topology and IP Addressing section of the lab guide). Click on **Update**

Update Device Template

Variable List (Hover over each field for more information)

| | |
|---|--|
| Chassis Number | CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2 |
| System IP | 10.255.255.41 |
| Hostname | cEdge40 |
| Address(vpn512_next_hop_ip_address_0) | 192.168.0.1 |
| IPv4 Address/ prefix-length(vpn512_mgmt_ipv4_address) | 192.168.0.40/24 |
| Address(vpn0_next_hop_ip_address_0) | 100.100.100.1 |
| IPv4 Address/ prefix-length(inet_ipv4_address) | 100.100.100.40/24 |
| Color(inet_if_tunnel_color_value) | public-internet |
| Hostname(host-name) | cEdge40 |
| System IP(system-ip) | 10.255.255.41 |
| Site ID(site-id) | 40 |
| Address(vpn0_mpls_next_hop_ip_address) | 192.1.2.17 |
| IPv4 Address/ prefix-length(mpls_ipv4_address) | 192.1.2.18/30 |
| Color(mpls_if_tunnel_color_value) | mpls |
| Interface Name(vpn30_if_name) | GigabitEthernet6 |
| IPv4 Address/ prefix-length(vpn30_if_ipv4_address) | 10.40.30.2/24 |
| Interface Name(vpn20_if_name) | GigabitEthernet5 |
| IPv4 Address/ prefix-length(vpn20_if_ipv4_address) | 10.40.20.2/24 |
| Interface Name(vpn10_if_name) | GigabitEthernet4 |
| IPv4 Address/ prefix-length(vpn10_if_ipv4_address) | 10.40.10.2/24 |

Buttons:

- Generate Password
- Update
- Cancel

6. Choose side-by-side config diff if you want to view the configuration changes being made. Click on **Configure Devices**

The screenshot shows the Cisco vManage interface under the Configuration > Templates section. A device template named `cEdge_dualuplink_devtemp` is selected, indicated by a blue background. The configuration code for this template is displayed in a large text area. A yellow callout box at the top right states: "'Configure' action will be applied to 1 device(s) attached to 1 device template(s.)". Below the configuration code are three buttons: "Back", "Configure Devices" (which is highlighted in blue), and "Cancel".

```

178 mtu 1500
179 negotiation auto
180 exit
181 interface GigabitEthernet2
182 no shutdown
183 arp timeout 1200
184 ip address 100.100.100.40 255.255.255.0
185 no ip redirects
186 ip mtu 1500
187 mtu 1500
188 negotiation auto
189 exit
190 interface GigabitEthernet3
191 no shutdown
192 arp timeout 1200
193 ip address 192.1.2.18 255.255.255.252
226 mtu 1500
227 negotiation auto
228 exit
229 interface GigabitEthernet2
230 no shutdown
231 arp timeout 1200
232 ip address 100.100.100.40 255.255.255.0
233 no ip redirects
234 ip mtu 1500
235 mtu 1500
236 negotiation auto
237 exit
238 interface GigabitEthernet3
239 no shutdown
240 arp timeout 1200
241 ip address 192.1.2.18 255.255.255.252
242 no ip redirects
243 ip mtu 1500
244 mtu 1500
245 negotiation auto
246 exit
247 interface GigabitEthernet4
248 no shutdown
249 arp timeout 1200
250 vrf forwarding 10
251 ip address 10.40.10.2 255.255.255.0
252 no ip redirects
253 ip mtu 1500
254 mtu 1500
255 negotiation auto
256 exit
257 interface GigabitEthernet5
258 no shutdown
259 arp timeout 1200
260 vrf forwarding 20

```

This completes the configuration of the Site 40 cEdges for Service Side VPNs.

Task List

- [Updating vEdge Device Templates for Service Side VPNs](#)
 - [Updating the DC vEdge Device Template](#)
 - [Updating the Site 20 Device Template](#)
 - [Updating the Site 30 Device Template](#)
- [Updating cEdge Device Templates for Service Side VPNs](#)
 - [Updating the Site 40 Device Template](#)
 - [Updating the Site 50 Device Template](#)

Updating the Site 50 Device Template

1. From **Configuration => Templates**, choose to **Edit** the `cEdge-single-uplink` Template

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Device' tab is selected. A context menu is open over the last row of the table, listing options: Edit, View, Delete, Copy, Attach Devices, Detach Devices, Export CSV, and Change Device Values.

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Action |
|--------------------------|------------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|--------|
| vEdge_Site20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 PM PDT | In Sync | ... |
| vEdge30_dev_temp | Device template for the Site 30... | Feature | vEdge Cloud | 15 | 1 | admin | 25 May 2020 3:09:51 PM PDT | In Sync | ... |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 15 | 2 | admin | 25 May 2020 2:53:02 PM PDT | In Sync | ... |
| cEdge_dualuplink_devtemp | cEdge Device Template for dev... | Feature | CSR1000v | 18 | 1 | admin | 25 May 2020 3:17:36 PM PDT | In Sync | ... |
| vSmart-dev-temp | Device Template for vSmarts | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 AM PDT | In Sync | ... |
| cedge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 11 | 2 | admin | 18 May 2020 1:33:13 PM PDT | In Sync | ... |

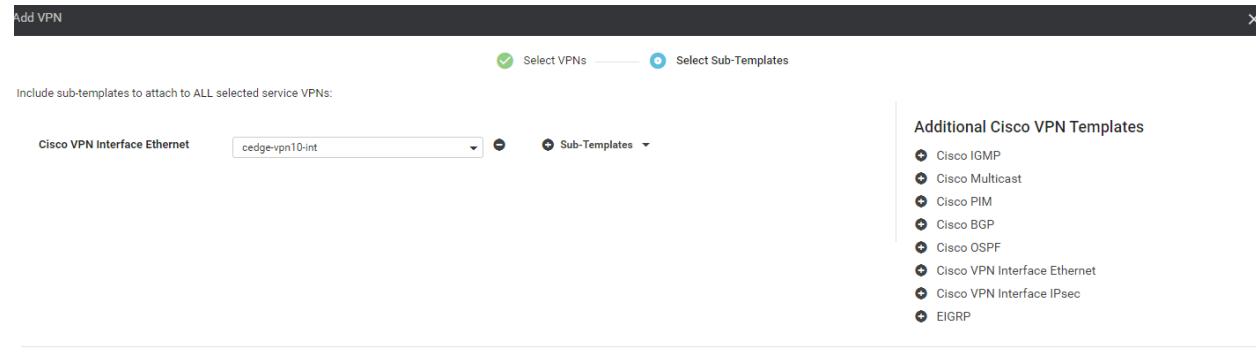
- Under **Service VPN**, choose **Add VPN** and move *cedge-vpn10* to the list of **Selected VPN Templates** and click on **Next**

The screenshot shows the 'Add VPN' configuration page. It has two main sections: 'Available VPN Templates' and 'Selected VPN Templates'. An arrow button between them indicates the direction of template movement.

| ID | Template Name |
|--------------------------------------|-------------------------|
| 7b4580b8-c918-46a7-b34f-24743fdc8955 | Default_VPN_1_Cisco_V01 |
| ff56fbce-0c12-4575-9f41-b6c7d780e13d | cedge-vpn20 |
| 9a88750f-7bd2-4fd5-b9d3-10a11544c8b6 | cedge-vpn30 |

| ID | Template Name |
|--------------------------------------|---------------|
| f018b46b-8ddc-431d-a222-cf905da7e13b | cedge-vpn10 |

- Click on **Cisco VPN Interface Ethernet** under Additional Cisco VPN Templates and choose *cedge-vpn10-int* in the drop down. Click on **Add**



4. Perform Steps 2 and 3 for *cedge-vpn20*, *cedge-vpn20-int* and *cedge-vpn30*, *cedge-vpn30-int*. The final Device Template should look like the image below. Click on **Update**

| Service VPN | | | |
|--------------------------|--------------------------------------|---------------|------------------------------|
| Actions | | Details | |
| <input type="checkbox"/> | ID | Template Name | Sub-Templates |
| <input type="checkbox"/> | f018b46b-8ddc-431d-a222-cf905da7e19b | cedge-vpn10 | Cisco VPN Interface Ethernet |
| <input type="checkbox"/> | ff56fbce-0c12-4575-9f41-b6c7d780e13d | cedge-vpn20 | Cisco VPN Interface Ethernet |
| <input type="checkbox"/> | 9a88750f-7bd2-4fd5-b9d3-10a11544c8b6 | cedge-vpn30 | Cisco VPN Interface Ethernet |

| Additional Templates | |
|----------------------|---------------------------------------|
| AppQoE | Choose... |
| Global Template * | Factory_Default_Global_CISCO_Template |
| Cisco Banner | Choose... |
| Cisco SNMP | Choose... |
| CLI Add-On Template | Choose... |
| Policy | Choose... |

5. Choose to **Edit Device Template** next to cEdge50 and enter the details as shown below. Click on **Update**

Update Device Template X

Variable List (Hover over each field for more information)

| | |
|---|--|
| Chassis Number | CSR-834E40DC-E358-8DE1-0E81-76E5984138F4 |
| System IP | 10.255.255.51 |
| Hostname | cEdge50 |
| Address(vpn512_next_hop_ip_address_0) | 192.168.0.1 |
| IPv4 Address/ prefix-length(vpn512_mgmt_ipv4_address) | 192.168.0.50/24 |
| Address(vpn0_next_hop_ip_address_0) | 100.100.100.1 |
| Interface Name(vpn0_if_name) | GigabitEthernet2 |
| IPv4 Address/ prefix-length(vpn0_ipv4_address) | 100.100.100.50/24 |
| Color(vpn0_if_tunnel_color_value) | public-internet |
| Restrict(vpn0_if_tunnel_color_restrict) | <input type="checkbox"/> |
| Hostname(host-name) | cEdge50 |
| System IP(system-ip) | 10.255.255.51 |
| Site ID(site-id) | 50 |
| Interface Name(vpn30_if_name) | GigabitEthernet5 |
| IPv4 Address/ prefix-length(vpn30_if_ipv4_address) | 10.50.30.2/24 |
| Interface Name(vpn20_if_name) | GigabitEthernet4 |
| IPv4 Address/ prefix-length(vpn20_if_ipv4_address) | 10.50.20.2/24 |
| Interface Name(vpn10_if_name) | GigabitEthernet3 |
| IPv4 Address/ prefix-length(vpn10_if_ipv4_address) | 10.50.10.2/24 |

Generate Password Update Cancel

6. Choose to **Edit Device Template** next to cEdge51 and enter the details as shown below. Click on **Update**

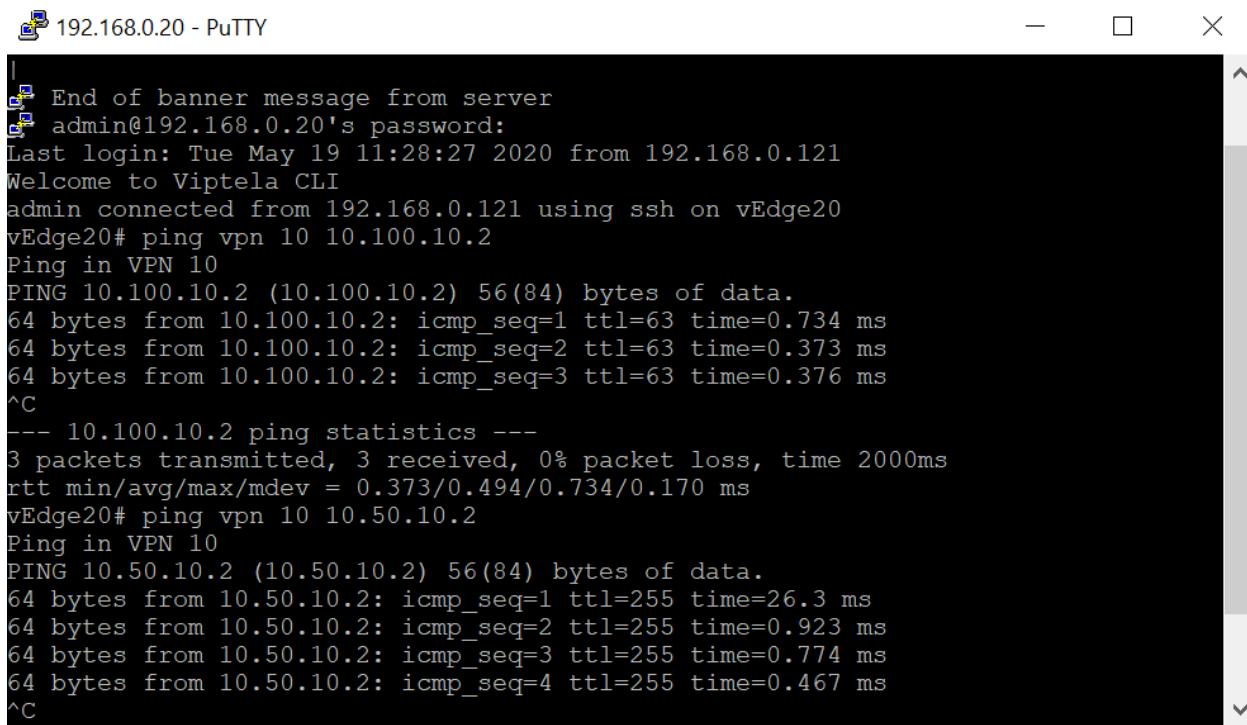
Update Device Template X

Variable List (Hover over each field for more information)

| | |
|---|--|
| Chassis Number | CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3 |
| System IP | 10.255.255.52 |
| Hostname | cEdge51 |
| Address(vpn512_next_hop_ip_address_0) | 192.168.0.1 |
| IPv4 Address/ prefix-length(vpn512_mgmt_ipv4_address) | 192.168.0.51/24 |
| Address(vpn0_next_hop_ip_address_0) | 192.1.2.21 |
| Interface Name(vpn0_if_name) | GigabitEthernet2 |
| IPv4 Address/ prefix-length(vpn0_ipv4_address) | 192.1.2.22/30 |
| Color(vpn0_if_tunnel_color_value) | mpls |
| Restrict(vpn0_if_tunnel_color_restrict) | <input checked="" type="checkbox"/> |
| Hostname(host-name) | cEdge51 |
| System IP(system-ip) | 10.255.255.52 |
| Site ID(site-id) | 50 |
| Interface Name(vpn30_if_name) | GigabitEthernet5 |
| IPv4 Address/ prefix-length(vpn30_if_ipv4_address) | 10.50.3.0/24 |
| Interface Name(vpn20_if_name) | GigabitEthernet4 |
| IPv4 Address/ prefix-length(vpn20_if_ipv4_address) | 10.50.20.3/24 |
| Interface Name(vpn10_if_name) | GigabitEthernet3 |
| IPv4 Address/ prefix-length(vpn10_if_ipv4_address) | 10.50.10.3/24 |

Generate Password

7. Click on **Next** and choose to **Configure Devices**. Confirm the change.
8. For verification, open a Putty session to **vEdge20** and try to ping some of the Service VPN IPs. Enter `ping vpn 10 10.100.10.2` and then `ping vpn 10 10.50.10.2`. The pings should be successful



192.168.0.20 - PuTTY

```
|  
| End of banner message from server  
| admin@192.168.0.20's password:  
Last login: Tue May 19 11:28:27 2020 from 192.168.0.121  
Welcome to Viptela CLI  
admin connected from 192.168.0.121 using ssh on vEdge20  
vEdge20# ping vpn 10 10.100.10.2  
Ping in VPN 10  
PING 10.100.10.2 (10.100.10.2) 56(84) bytes of data.  
64 bytes from 10.100.10.2: icmp_seq=1 ttl=63 time=0.734 ms  
64 bytes from 10.100.10.2: icmp_seq=2 ttl=63 time=0.373 ms  
64 bytes from 10.100.10.2: icmp_seq=3 ttl=63 time=0.376 ms  
^C  
--- 10.100.10.2 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2000ms  
rtt min/avg/max/mdev = 0.373/0.494/0.734/0.170 ms  
vEdge20# ping vpn 10 10.50.10.2  
Ping in VPN 10  
PING 10.50.10.2 (10.50.10.2) 56(84) bytes of data.  
64 bytes from 10.50.10.2: icmp_seq=1 ttl=255 time=26.3 ms  
64 bytes from 10.50.10.2: icmp_seq=2 ttl=255 time=0.923 ms  
64 bytes from 10.50.10.2: icmp_seq=3 ttl=255 time=0.774 ms  
64 bytes from 10.50.10.2: icmp_seq=4 ttl=255 time=0.467 ms  
^C
```

```
ping vpn 10 10.100.10.2  
ping vpn 10 10.50.10.2
```

This completes the configuration of our Service Side VPNs for the vEdges and cEdges in our network.

Task List

- [Updating vEdge Device Templates for Service Side VPNs](#)
 - [Updating the DC-vEdge Device Template](#)
 - [Updating the Site 20 Device Template](#)
 - [Updating the Site 30 Device Template](#)
- [Updating cEdge Device Templates for Service Side VPNs](#)
 - [Updating the Site 40 Device Template](#)
 - [Updating the Site 50 Device Template](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 26, 2020

Site last generated: Sep 1, 2020



-->

Dynamic Service Side routing at the DC

Summary: Implementing Dynamic Service Side Routing at the DC - OSPF

Table of Contents

- [Overview](#)
- [Updating the vEdge Service VPN 10 with an OSPF Template](#)
- [Activity Verification](#)

Task List

- Overview
- Updating the vEdge Service VPN 10 with an OSPF Template
- Activity Verification

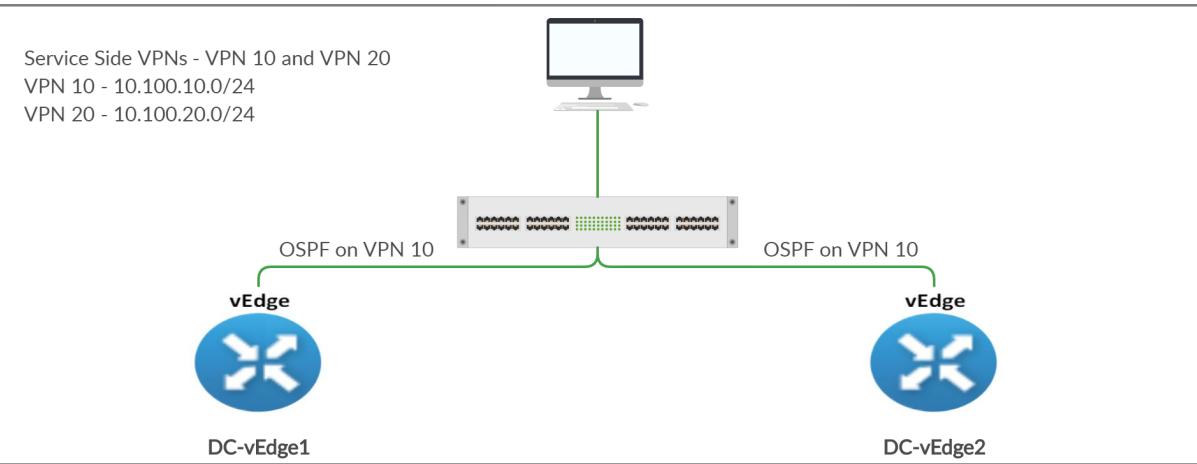
Overview

Sites in Cisco SD-WAN will generally have an L3 device on the LAN other than the vEdges/cEdges. These devices might be servicing LAN users and advertising their routes via an IGP of choice. We need to make sure that these routes are advertised across the SD-WAN Fabric. While static routing can be used to achieve this, it is time consuming and extremely prone to errors. Thus, running a Dynamic Routing Protocol between the WAN Edge devices and the L3 devices, is usually preferred.

We will run OSPF on VPN 10 in the DC with an L3 Device (called the Central Gateway). The Central Gateway has been configured with the corresponding OSPF configuration. Once OSPF neighbourship is established between the Central Gateway and our DC-vEdges, we will try to reach a route being advertised by the Central Gateway ($10.0.0.1/32$) from vEdge30.

Given below is the section of the topology that we will be working on for this activity.

SITE ID 1



Task List

- [Overview](#)
- [Updating the vEdge Service VPN 10 with an OSPF Template](#)
- [Activity Verification](#)

Updating the vEdge Service VPN 10 with an OSPF Template

1. Go to **Configuration => Templates** and click on the three dots next to *DCvEdge_dev_temp*. Click on **Edit**

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Device' tab is selected. A table lists various device templates. One row, 'vEdgeSite20_dev_temp', is highlighted with a yellow background. A context menu is open over this row, with the 'Edit' option highlighted by a red box.

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status |
|-----------------------------|------------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 17 | 2 | admin | 25 May 2020 3:25:24 PM PDT | In Sync |
| vEdge_Site20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 PM PDT | In Sync |
| vEdge30_dev_temp | Device template for the Site 30... | Feature | vEdge Cloud | 15 | 1 | admin | 25 May 2020 3:09:51 PM PDT | In Sync |
| vEdgeSite20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud | 15 | 2 | admin | 25 May 2020 2:53:02 PM PDT | In Sync |
| cEdge_dualuplink_devtemp | cEdge Device Template for dev... | Feature | CSR1000v | 18 | 1 | admin | 25 May 2020 3:17:38 PM PDT | In Sync |
| vSmart-dev-temp | Device Template for vSmart | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 AM PDT | In Sync |

2. Under **Service VPN**, click on the three dots next to the *vedge-vpn10* template and choose to **Edit** it

The screenshot shows the 'Service VPN' tab selected in the 'CONFIGURATION | TEMPLATES' section. A table lists VPN templates. The 'vedge-vpn10' template is selected and highlighted with a yellow background. A context menu is open over this row, with the 'Edit' option highlighted by a red box.

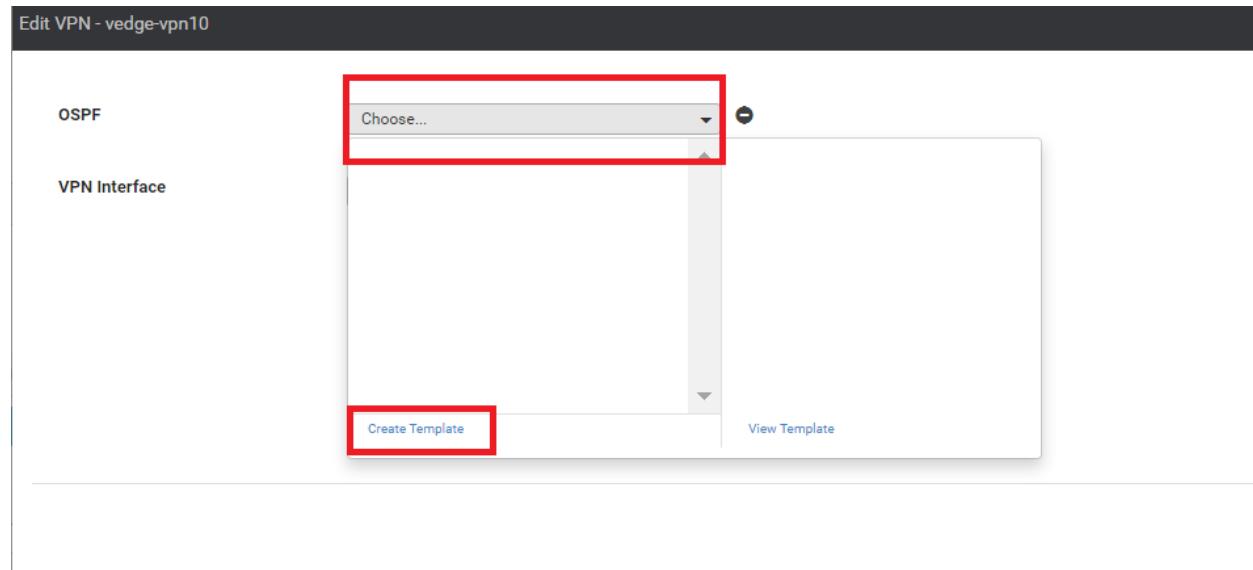
| ID | Template Name | Sub-Templates |
|--|---------------|---------------|
| <input checked="" type="checkbox"/> e9acf67d-aad6-4913-8f0a-84e255b4b033 | vedge-vpn10 | VPN Interface |
| <input type="checkbox"/> 6fd47ee6-61c1-4b02-9b3e-439f5c423b74 | vedge-vpn20 | VPN Interface |

3. Click on **OSPF** under Additional VPN Templates to add an OSPF Template

The screenshot shows the 'Edit VPN - vedge-vpn10' configuration page. On the right, a sidebar titled 'Additional VPN Templates' lists various protocols and interfaces. The 'OSPF' option is highlighted with a red box.

- BGP
- IGMP
- Multicast
- OSPF**
- PIM
- VPN Interface
- VPN Interface Bridge
- VPN Interface GRE
- VPN Interface IPsec
- VPN Interface Natpool

4. Click on the OSPF drop down and click on **Create Template** to create a new OSPF Template. We are creating our Templates on the fly over here, but could have created them before hand from the Feature Templates, if required



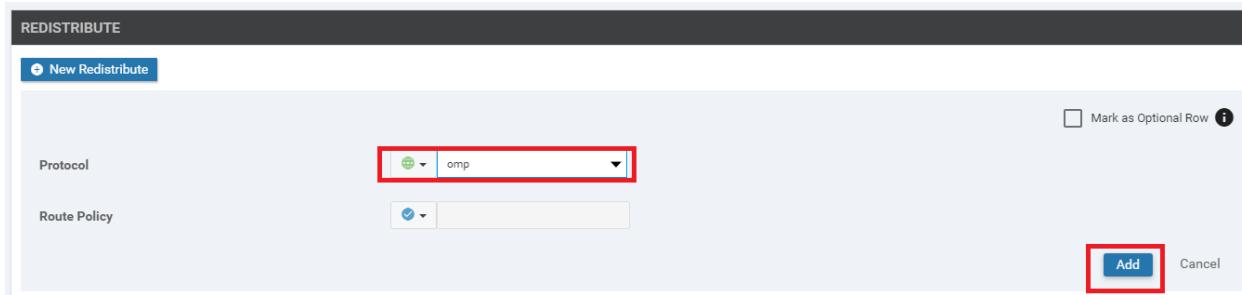
5. Give the template a name of **DC-OSPF** and a Description of **OSPF Template for the DC**. Click on **New Redistribute** under the **Redistribute** section

The screenshot shows the 'Edit Service VPN > Add Template > OSPF' configuration page. At the top, it specifies a 'Device Type' of 'vEdge Cloud'. Below that, the 'Template Name' is set to 'DC-OSPF' and the 'Description' is 'OSPF Template for the DC', both highlighted with a red box.

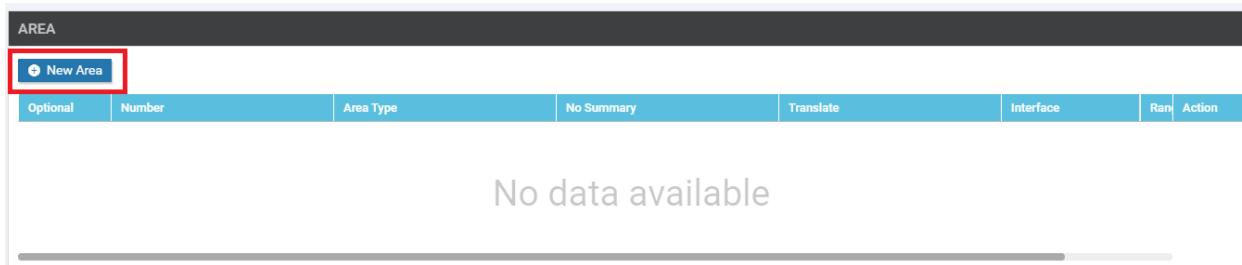
The page includes tabs for 'Basic Configuration', 'Redistribute', 'Maximum Metric (Router LSA)', 'Area', and 'Advanced'. The 'Basic Configuration' tab is active. Under 'BASIC CONFIGURATION', there are fields for 'Router ID' (with a dropdown menu), 'Distance for External Routes' (set to 110), 'Distance for Inter-Area Routes' (set to 110), and 'Distance for Intra-Area Routes' (set to 110).

The 'REDISTRIBUTE' tab is visible at the bottom, containing a 'New Redistribute' button, which is highlighted with a red box. Below this tab are buttons for 'Optional' and 'Protocol'.

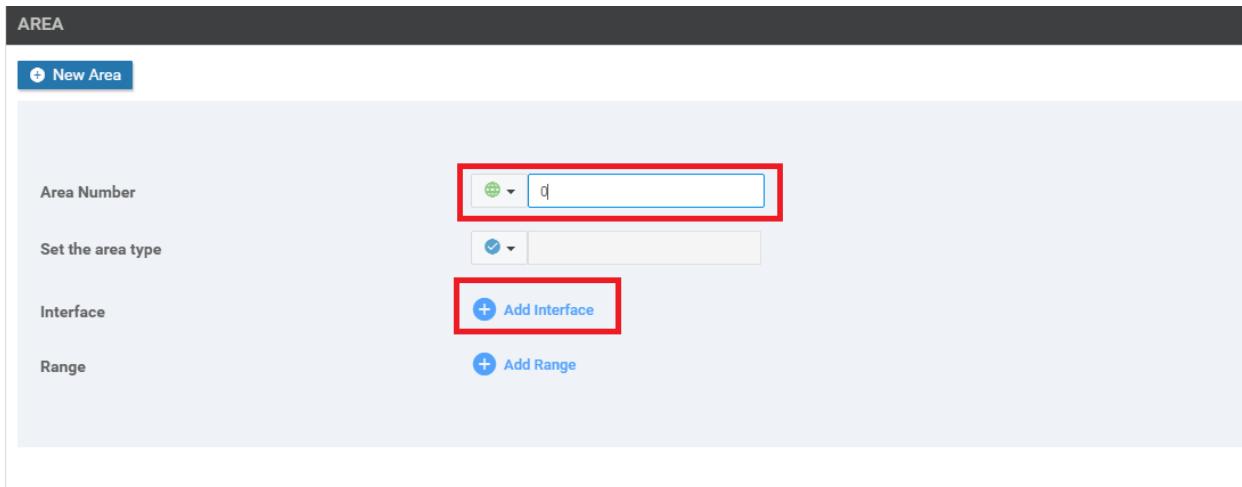
6. No routes get redistributed into OSPF but we want to ensure that WAN Routes are advertised into the DC LAN. For this purpose, choose **OMP** and click on **Add**. This will redistribute OMP routes into OSPF



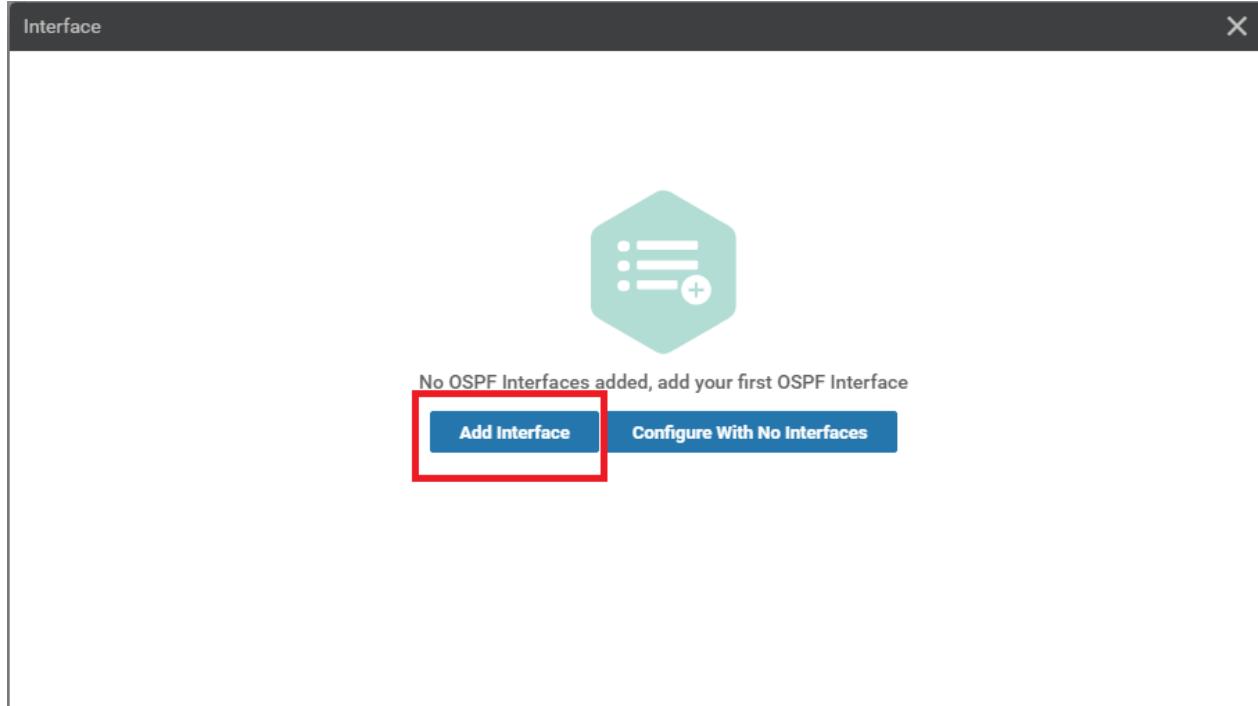
7. Under the Area section, click on **New Area**



8. Set the Area Number as a Global value of **0**. Our OSPF neighbourships will be formed on Area 0. Click on **Add Interface**



9. Click on **Add Interface** again to add the OSPF Interfaces



10. Specify the Interface Name as a Global value of `ge0/2` and click on **Add**. This is our LAN facing Interface in VPN 10

Interface

Add Interface

ge0/2

Interface Name: ge0/2

Hello Interval (seconds): 10

Dead Interval (seconds): 40

LSA Retransmission Interval (seconds): 5

Interface Cost:

Advanced Options >

Add Cancel

This screenshot shows the 'Interface' configuration dialog. On the left, there's a sidebar with a red 'Add Interface' button and a list containing 'ge0/2'. The main area has a red box around the 'Interface Name' field, which contains 'ge0/2'. Below it are fields for 'Hello Interval (seconds)', 'Dead Interval (seconds)', and 'LSA Retransmission Interval (seconds)'. At the bottom right are 'Add' and 'Cancel' buttons.

11. Click on **Add** under the Area section to Add these details to the OSPF Template

AREA

New Area

Area Number: 0

Set the area type:

Interface: 1 Interface

Range: + Add Range

Add Cancel

This screenshot shows the 'AREA' configuration dialog. It has a 'New Area' button at the top. Below are fields for 'Area Number' (set to 0), 'Set the area type', and 'Interface' (set to 1 Interface). There's also a 'Range' section with a '+ Add Range' button. At the bottom right are 'Add' and 'Cancel' buttons.

12. Click on **Save** to save the OSPF template

AREA

+ New Area

| Optional | Number | Area Type | No Summary | Translate |
|--------------------------|--------|-------------------------------------|------------|-----------|
| <input type="checkbox"/> | 0 | <input checked="" type="checkbox"/> | | |

ADVANCED

Reference Bandwidth (Mbps) 100

RFC 1583 Compatible On Off

Originate On Off

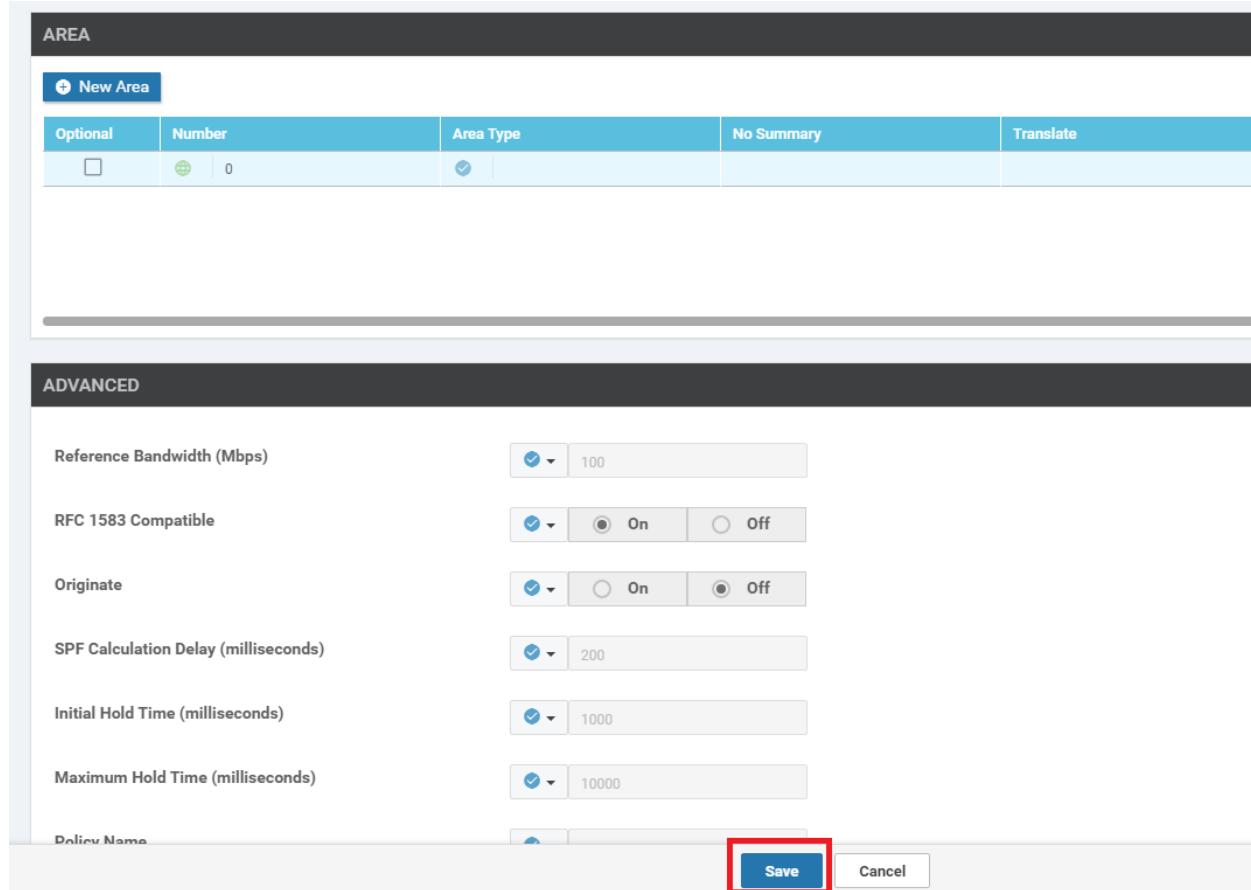
SPF Calculation Delay (milliseconds) 200

Initial Hold Time (milliseconds) 1000

Maximum Hold Time (milliseconds) 10000

Policy Name

Save **Cancel**



13. This should take you back to the *vedge-vpn10* Template configuration window. If it doesn't, navigate to it manually and populate the *DC-OSPF* template in the OSPF field. Click on **Save**

Edit VPN - vedge-vpn10

OSPF

VPN Interface Sub-Templates

CANCEL

14. Make sure that the VPN 10 Service VPN has **OSPF**, **VPN Interface** tacked on to it and click on **Update**

Service VPN

0 Rows Selected | Add VPN | Remove VPN

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|---------------------|
| e9acf7d-aad6-4913-8f0a-84e255b4b033 | vedge-vpn10 | OSPF, VPN Interface |
| 6fd47ee6-61c1-4b02-9b3e-439f5c423b74 | vedge-vpn20 | VPN Interface |

Additional Templates

Banner Choose...

Update **Cancel**

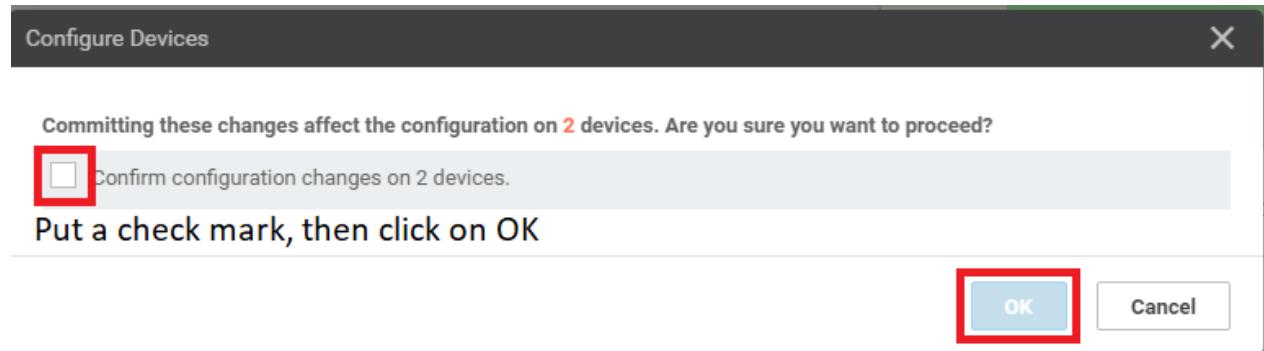
15. We are taken to the configuration page for the individual devices at the DC. There is nothing that needs to be configured, so we can click on **Next**

| S... | Chassis Number | System IP | Hostname | Interface Name(vpn20_if_name) | IPv4 Address(vpn20_if_ip4_address) | Interface Name(vpn10_if_name) | IPv4 A... |
|-------------------------------------|--------------------------------------|---------------|-----------|-------------------------------|------------------------------------|-------------------------------|-----------|
| <input checked="" type="checkbox"/> | e474c5fd-8ce7-d376-7cac-ba950b2c9159 | 10.255.255.11 | DC-vEdge1 | ge0/3 | 10.100.20.2/24 | ge0/2 | 10.100... |
| <input checked="" type="checkbox"/> | 0cdd4f0e-f2f1-fe75-866c-469966cda1c3 | 10.255.255.12 | DC-vEdge2 | ge0/3 | 10.100.20.3/24 | ge0/2 | 10.100... |

Next **Cancel**

16. Review the side-by-side config diff (notice the OSPF configuration added) and click on **Configure Devices**. Confirm this configuration change

| Device Template | | Total | 'Configure' action will be applied to 2 device(s) attached to 1 device template(s). | |
|--|----------------------------------|-------|---|--|
| DCvEdge_dev_temp | 1 | | | |
| Device list (Total: 2 devices) | | | | |
| Filter/Search | | | | |
| e474cfcd-8ce7-d376-7cac-be950b2c9159 DC-Edge1 10.255.255.11 | | | | |
| 0cd4f10e-f2f1-fe75-866c-469966cda1c3 DC-Edge2 10.255.255.12 | | | | |
| | | | | |
| 89 | ip route 0.0.0.0/0 100.100.100.1 | | | |
| 90 | ip route 0.0.0.0/0 192.0.2.1 | | | |
| 91 | ! | | | |
| 92 | vpn 10 | | | |
| 93 | dns 10.2.1.5 primary | | | |
| 94 | dns 10.2.1.6 secondary | | | |
| | | | | |
| 95 | interface ge0/2 | | | |
| 96 | ip address 10.100.10.2/24 | | | |
| 97 | no shutdown | | | |
| 98 | ! | | | |
| 99 | cmp | | | |
| 100 | advertise connected | | | |
| 101 | advertise static | | | |
| 102 | ! | | | |
| 103 | ! | | | |
| 104 | vpn 20 | | | |
| 105 | dns 10.2.1.5 primary | | | |
| 106 | dns 10.2.1.6 secondary | | | |
| 107 | interface ge0/3 | | | |
| 108 | ip address 10.100.20.2/24 | | | |
| 109 | no shutdown | | | |
| 110 | ! | | | |
| 111 | cmp | | | |
| 112 | advertise connected | | | |
| 113 | advertise static | | | |
| | | | | |
| 95 | ip route 0.0.0.0/0 100.100.100.1 | | | |
| 96 | ip route 0.0.0.0/0 192.0.2.1 | | | |
| 97 | ! | | | |
| 98 | vpn 10 | | | |
| 99 | dns 10.2.1.5 primary | | | |
| 100 | dns 10.2.1.6 secondary | | | |
| 101 | router | | | |
| 102 | ospf | | | |
| 103 | timers spf 200 1000 10000 | | | |
| 104 | redistribute ospf | | | |
| 105 | area 0 | | | |
| 106 | interface ge0/2 | | | |
| 107 | exit | | | |
| 108 | exit | | | |
| 109 | ! | | | |
| 110 | cmp | | | |
| 111 | advertise connected | | | |
| 112 | advertise static | | | |
| 113 | ! | | | |
| 114 | vpn 20 | | | |
| 115 | dns 10.2.1.5 primary | | | |
| 116 | dns 10.2.1.6 secondary | | | |
| 117 | interface ge0/3 | | | |
| 118 | ip address 10.100.20.2/24 | | | |
| 119 | no shutdown | | | |
| 120 | ! | | | |
| 121 | cmp | | | |
| 122 | advertise connected | | | |
| 123 | advertise static | | | |



This completes the OSPF related configuration on VPN 10 for the DC-vEdges.

Task List

- Overview
 - Updating the vEdge Service VPN 10 with an OSPF Template
 - Activity Verification

Activity Verification

1. On the vManage GUI, navigate to **Monitor => Network**. Click on **DC-vEdge1** and then on **Real Time**. Enter **OSPF Neighbors** in the **Device Options** and choose *Do Not Filter*, if prompted. You should see 2 OSPF Neighbors (Central Gateway and DC-vEdge2)

The screenshot shows the vManage interface under the 'Network > Real Time' section. The 'Select Device' dropdown is set to 'DC-vEdge1'. The 'Device Options' field contains 'OSPF Neighbors'. The main table displays two OSPF neighbors:

| VPN | Address | If Index | If Name | Neighbor ID | State | Priority | Dead Interval Timer | DB Summary List | Link State Req List |
|-----|-------------|----------|---------|---------------|-------|----------|---------------------|-----------------|---------------------|
| 10 | 10.100.10.1 | 0 | ge0/2 | 10.0.0.1 | full | 1 | 37 | 0 | 0 |
| 10 | 10.100.10.3 | 0 | ge0/2 | 10.255.255.12 | full | 1 | 34 | 0 | 0 |

2. Enter **OSPF Routes** in the **Device Options** and choose *Do Not Filter* if prompted

The screenshot shows the vEdge Cloud Network Monitor interface. On the left, there's a sidebar with various monitoring categories like WAN Throughput, Flows, Top Talkers, Security Monitoring, Firewall, Intrusion Prevention, URL Filtering, Advanced Malware Protection, TLS/SSL Decryption, Umbrella DNS Redirect, Control Connections, and System Status. The main area has a search bar labeled "Device Options" with "OSPF Routes" typed into it, which is also highlighted with a red box. Below the search bar is a "Filter" dropdown menu. A modal window titled "Select Filter" is open in the center, containing the instruction "Choose filters to display data faster." with two buttons at the bottom: "Show Filters" and "Do Not Filter", with "Do Not Filter" also highlighted with a red box.

3. You should see a Route for the 10.0.0.1/32 network, among others

This screenshot shows the same Network Monitor interface as above, but now the OSPF Routes table is visible. The table has columns for VPN, Route Type, Prefix, Area ID, ID, Cost, Flags, Path Type, Dest Type, Tag, Type-2 Cost, Next Hop, If Name, and Last Updated. One row in the table, corresponding to the 10.0.0.1/32 route, is highlighted with a red box. The table shows four total rows.

| VPN | Route Type | Prefix | Area ID | ID | Cost | Flags | Path Type | Dest Type | Tag | Type-2 Cost | Next Hop | If Name | Last Updated |
|-----|------------|-----------------|---------|----|------|-------|------------|-----------|-----|-------------|-------------|---------|----------------------|
| 10 | router | 10.0.0.1/32 | 0 | 0 | 10 | 2 | intra-area | router | - | - | 10.100.10.1 | ge0/2 | 25 May 2020 11:45... |
| 10 | router | 10.255.255.1... | 0 | 0 | 10 | 2 | intra-area | router | - | - | 10.100.10.3 | ge0/2 | 25 May 2020 11:45... |
| 10 | network | 10.0.0.1/32 | 0 | 0 | 11 | 0 | intra-area | network | - | - | 10.100.10.1 | ge0/2 | 25 May 2020 11:45... |
| 10 | network | 10.100.10.0/24 | 0 | 0 | 10 | 0 | intra-area | network | - | - | 0.0.0.0 | ge0/2 | 25 May 2020 11:45... |

4. The same information can be verified via the CLI. Log in to DC-vEdge1 and issue `show ospf neigh`, `show ospf route` and `show ip route ospf`

```
DC-vEdge1# show ospf neigh
DBsmL -> Database Summary List
RqstL -> Link State Request List
RXmtL -> Link State Retransmission List
      SOURCE
VPN   IP ADDRESS      INTERFACE      ROUTER ID      STATE      PRIORITY      DEAD
      SOURCE
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
10    10.100.10.1     ge0/2        10.0.0.1       full       1           37          0           0           0
10    10.100.10.3     ge0/2        10.255.255.12  full       1           37          0           0           0
DC-vEdge1#
```

```
DC-vEdge1# show ospf route
```

| VPN | ROUTE | | ID | AREA | COST | PATH | DEST | | IF | NAME |
|-----|---------|------------------|----|------|------|------------|---------|-------------|-------|------|
| | TYPE | PREFIX | | | | | TYPE | NEXT HOP | | |
| 10 | router | 10.0.0.1/32 | 0 | 0 | 10 | intra-area | router | 10.100.10.1 | ge0/2 | |
| 10 | router | 10.255.255.12/32 | 0 | 0 | 10 | intra-area | router | 10.100.10.3 | ge0/2 | |
| 10 | network | 10.0.0.1/32 | 0 | 0 | 11 | intra-area | network | 10.100.10.1 | ge0/2 | |
| 10 | network | 10.100.10.0/24 | 0 | 0 | 10 | intra-area | network | 0.0.0.0 | ge0/2 | |

```
DC-vEdge1# 
```

```
DC-vEdge1# show ip route ospf
```

```
Codes Proto-sub-type:
```

```
IA -> ospf-intra-area, IE -> ospf-inter-area,  
E1 -> ospf-external1, E2 -> ospf-external2,  
N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,  
e -> bgp-external, i -> bgp-internal
```

```
Codes Status flags:
```

```
F -> fib, S -> selected, I -> inactive,  
B -> blackhole, R -> recursive
```

| VPN | PREFIX | PROTOCOL | SUB TYPE | NEXTHOP IF NAME | NEXTHOP ADDR | NEXTHOP VPN | | TLOC IP | COLOR | ENCAP |
|-----|----------------|----------|----------|-----------------|--------------|-------------|----|---------|-------|-------|
| | | | | | | TYPE | IP | | | |
| 10 | 10.0.0.1/32 | ospf | IA | ge0/2 | 10.100.10.1 | - | - | - | - | - |
| 10 | 10.100.10.0/24 | ospf | IA | ge0/2 | - | - | - | - | - | - |

```
DC-vEdge1# 
```

```
show ospf neigh  
show ospf route  
show ip route ospf
```

5. Log in to the CLI of **vEdge-30** and issue a `show ip route`. You will notice that a route to `10.0.0.1/32` has been learnt via OMP. Intra-Area and Inter-Area routes are injected into OMP by default

| vEdge30# show ip route | | | | | | | | | | | |
|--|------------------|-----------|------|----------|-----------------|--------------|---------------|-----------------|-------|-------|--------|
| Codes Proto-sub-type: IA -> ospf-intra-area, IE -> ospf-inter-area, E1 -> ospf-external1, E2 -> ospf-external2, NL -> ospf-nssa-external1, N2 -> ospf-nssa-external2, e -> bgp-external, i -> bgp-internal Codes Status flags: F -> fib, S -> selected, I -> inactive, B -> blackhole, R -> recursive | | | | | | | | | | | |
| VPN | PREFIX | PROTOCOL | PROT | SUB TYPE | NEXTHOP IF NAME | NEXTHOP ADDR | NEXTHOP VPN | TLOC IP | COLOR | ENCAP | STATUS |
| 0 | 0.0.0.0/0 | static | - | ge0/0 | 100.100.100.1 | - | - | - | - | F,S | |
| 0 | 0.0.0.0/0 | static | - | ge0/1 | 192.0.2.13 | - | - | - | - | F,S | |
| 0 | 10.255.255.31/32 | connected | - | system | - | - | - | - | - | F,S | |
| 0 | 100.100.100.0/24 | connected | - | ge0/0 | - | - | - | - | - | F,S | |
| 0 | 192.0.2.12/30 | connected | - | ge0/1 | - | - | - | - | - | F,S | |
| 10 | 10.0.0.1/32 | omp | - | - | - | - | 10.255.255.11 | mpls | ipsec | F,S | |
| 10 | 10.0.0.1/32 | omp | - | - | - | - | 10.255.255.11 | public-internet | ipsec | F,S | |
| 10 | 10.0.0.1/32 | omp | - | - | - | - | 10.255.255.12 | mpls | ipsec | F,S | |
| 10 | 10.0.0.1/32 | omp | - | - | - | - | 10.255.255.12 | public-internet | ipsec | F,S | |
| 10 | 10.20.10.0/24 | omp | - | - | - | - | 10.255.255.21 | public-internet | ipsec | F,S | |
| 10 | 10.20.10.0/24 | omp | - | - | - | - | 10.255.255.22 | mpls | ipsec | F,S | |
| 10 | 10.30.10.0/24 | connected | - | ge0/2 | - | - | - | - | - | F,S | |
| 10 | 10.40.10.0/24 | omp | - | - | - | - | 10.255.255.41 | mpls | ipsec | F,S | |
| 10 | 10.40.10.0/24 | omp | - | - | - | - | 10.255.255.41 | public-internet | ipsec | F,S | |
| 10 | 10.50.10.0/24 | omp | - | - | - | - | 10.255.255.51 | public-internet | ipsec | F,S | |
| 10 | 10.50.10.0/24 | omp | - | - | - | - | 10.255.255.52 | mpls | ipsec | F,S | |
| 10 | 10.100.10.0/24 | omp | - | - | - | - | 10.255.255.11 | mpls | ipsec | F,S | |
| 10 | 10.100.10.0/24 | omp | - | - | - | - | 10.255.255.11 | public-internet | ipsec | F,S | |
| 10 | 10.100.10.0/24 | omp | - | - | - | - | 10.255.255.12 | mpls | ipsec | F,S | |
| 10 | 10.100.10.0/24 | omp | - | - | - | - | 10.255.255.12 | public-internet | ipsec | F,S | |
| 20 | 10.20.20.0/24 | omp | - | - | - | - | 10.255.255.21 | public-internet | ipsec | F,S | |
| 20 | 10.20.20.0/24 | omp | - | - | - | - | 10.255.255.22 | mpls | ipsec | F,S | |
| 20 | 10.30.20.0/24 | connected | - | ge0/3 | - | - | - | - | - | F,S | |
| 20 | 10.40.20.0/24 | omp | - | - | - | - | 10.255.255.41 | mpls | ipsec | F,S | |

```
show ip route
```

6. Issue `ping 10.0.0.1 vpn 10` from vEdge30 to verify connectivity with the advertised LAN side route at the DC.

The pings should be successful

```
vEdge30#
vEdge30# ping 10.0.0.1 vpn 10
Ping in VPN 10
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=254 time=0.436 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=254 time=0.302 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=254 time=0.426 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=254 time=0.331 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=254 time=0.318 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=254 time=0.291 ms
64 bytes from 10.0.0.1: icmp_seq=7 ttl=254 time=0.419 ms
64 bytes from 10.0.0.1: icmp_seq=8 ttl=254 time=0.388 ms
```

This completes the OSPF configuration and verification of connectivity at the DC site.

Task List

- Overview

- [Updating the vEdge Service VPN 10 with an OSPF Template](#)
- [Activity Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 26, 2020

Site last generated: Sep 1, 2020



Dynamic Service Side Routing at Site 40

Summary: Implementing Dynamic Service Side routing at Site 40 - EIGRP

Table of Contents

- [Overview](#)
- [Updating the cEdge Service VPN 10 with an EIGRP Template](#)
- [Activity Verification and Remediation](#)

Task List

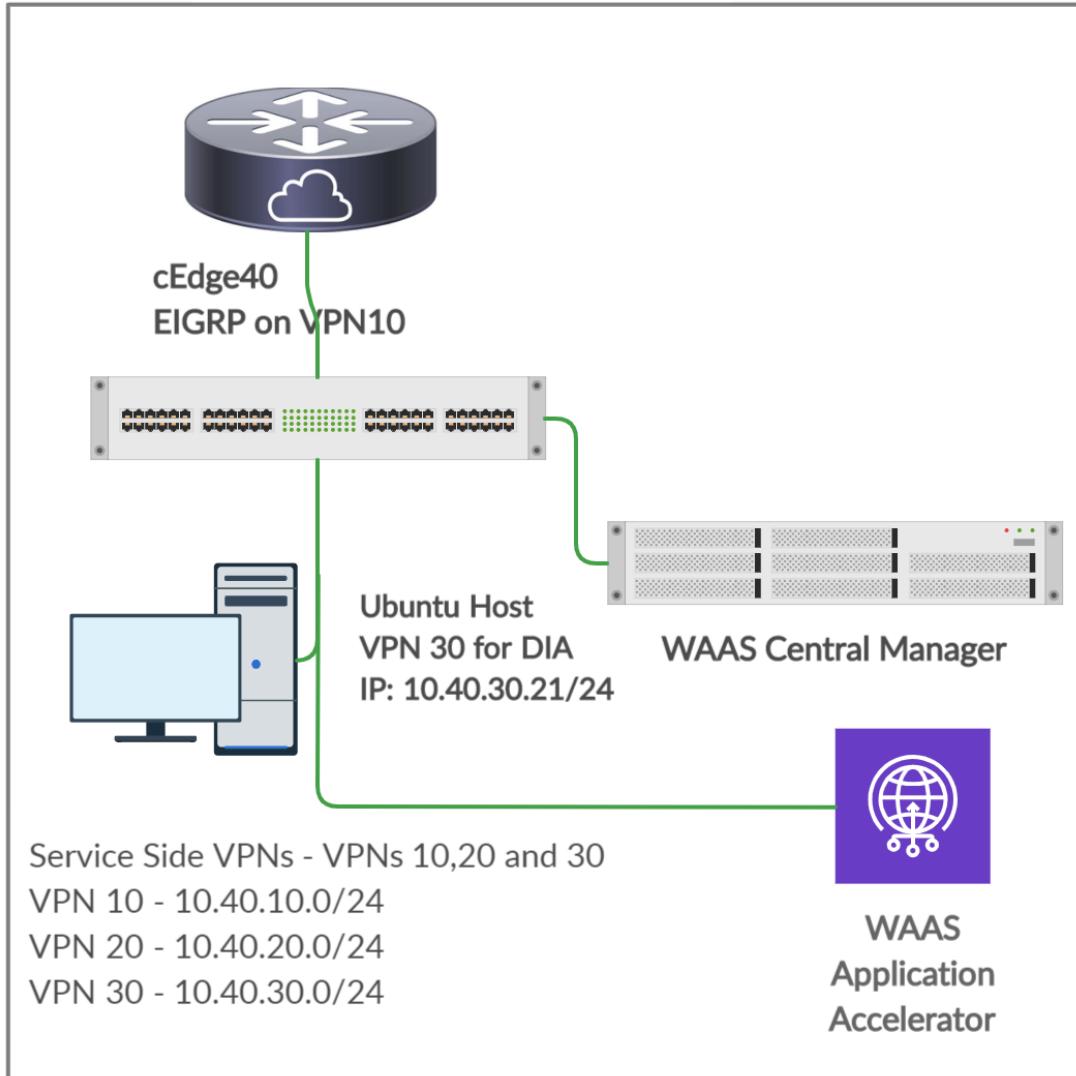
- Overview
- Updating the cEdge Service VPN 10 with an EIGRP Template
- Activity Verification and Remediation

Overview

We will run EIGRP on VPN 10 in Site 40 with an L3 Device. The L3 device has been configured with the corresponding EIGRP configuration. Once EIGRP neighbourship is established between the L3 Device and cEdge40, we will try to reach a route being advertised by the L3 Device (10.40.11.0/24) from the DC-vEdges.

Given below is the section of the topology that we will be working on for this activity

SITE ID 40



- Overview
- Updating the cEdge Service VPN 10 with an EIGRP Template
- Activity Verification and Remediation

Updating the cEdge Service VPN 10 with an EIGRP Template

1. Go to **Configuration => Templates** and click on the three dots next to **cEdge_dualuplink_devtemp**. Click on **Edit**

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Actions |
|---------------------------------|------------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|---------|
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 17 | 2 | admin | 25 May 2020 3:25:24 PM PDT | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 PM PDT | In Sync | ... |
| vEdge30_dev_temp | Device template for the Site 30... | Feature | vEdge Cloud | 15 | 1 | admin | 25 May 2020 3:09:51 PM PDT | In Sync | ... |
| DCvEdge_dev_temp | Device template for the DCvE... | Feature | vEdge Cloud | 16 | 2 | admin | 25 May 2020 3:13:08 PM PDT | In Sync | ... |
| cEdge_dualuplink_devtemp | cEdge Device Template for dev... | Feature | CSR1000v | 18 | 1 | admin | 25 May 2020 3:17:38 PM PDT | In Sync | ... |
| vSmart-dev-temp | Device Template for vSmarts | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 AM PDT | In Sync | ... |

2. Under **Service VPN**, click on the three dots next to the **cedge-vpn10** template and choose to **Edit** it

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|------------------------------|
| f018b46b-8ddc-431d-a222-cf905da7e13b | cedge-vpn10 | Cisco VPN Interface Ethernet |
| ff5fbfce-0c12-4575-9f41-b5c7d780e13d | cedge-vpn20 | Cisco VPN Interface Ethernet |
| 9a88750f-7bd2-4fd5-b9d3-10a1154ac8b6 | cedge-vpn30 | Cisco VPN Interface Ethernet |

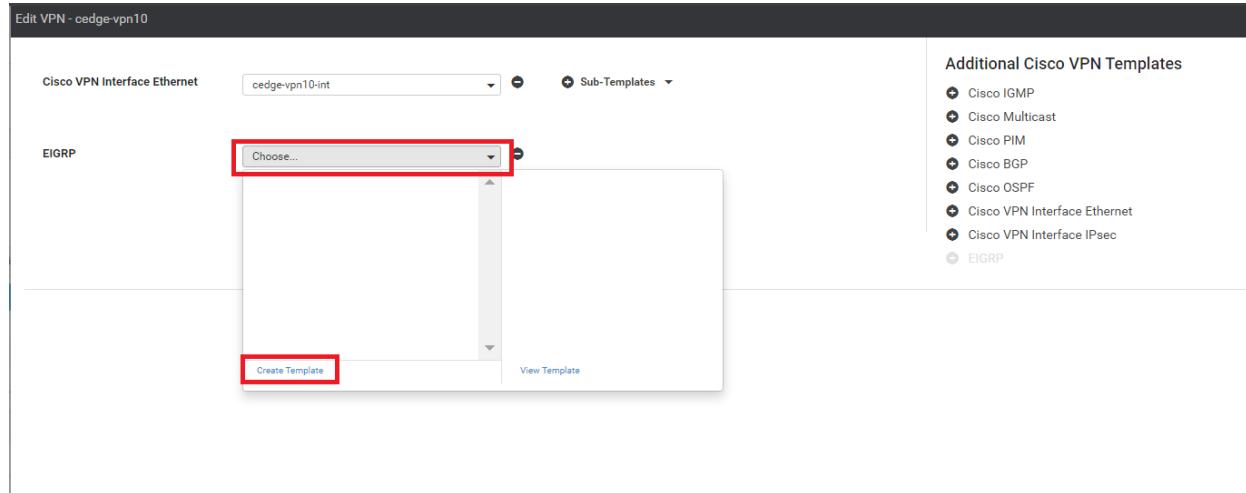
3. Click on **EIGRP** under **Additional Cisco VPN Templates** to add an EIGRP Template

| Cisco VPN Interface Ethernet | | Sub-Templates |
|------------------------------|-----------------|---------------|
| Cisco VPN Interface Ethernet | cedge-vpn10-int | Sub-Templates |

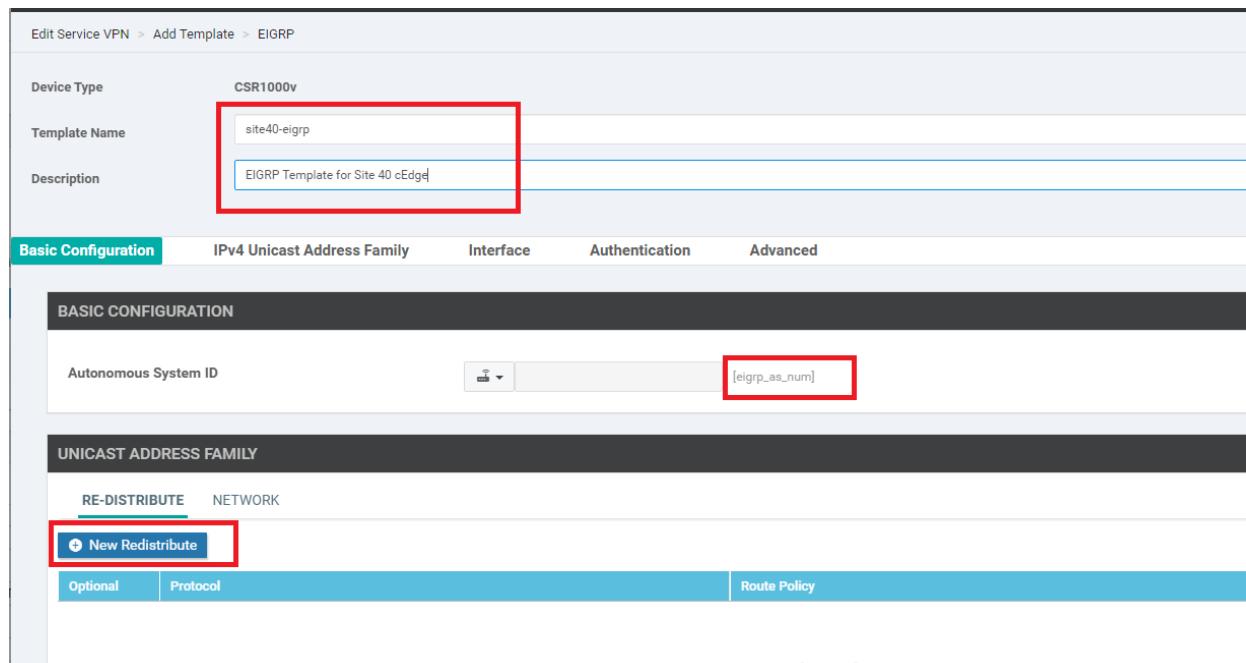
Additional Cisco VPN Templates

- ⊕ Cisco IGMP
- ⊕ Cisco Multicast
- ⊕ Cisco PIM
- ⊕ Cisco BGP
- ⊕ Cisco OSPF
- ⊕ Cisco VPN Interface Ethernet
- ⊕ Cisco VPN Interface IPsec
- ⊕ EIGRP**

4. Click on the EIGRP drop down and click on **Create Template** to create a new EIGRP Template. We are creating our Templates on the fly over here, but could have created them before hand from the Feature Templates, if required

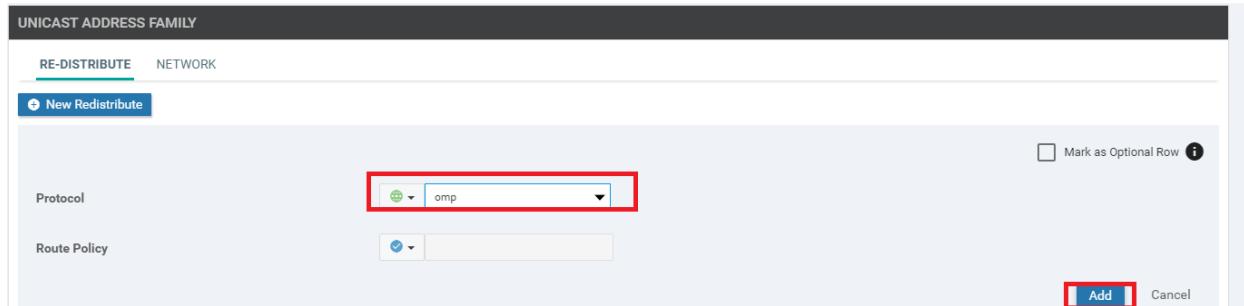


5. Give the template a name of *site40-eigrp* and a Description of *EIGRP Template for Site 40 cEdge*. Populate the **Autonomous System ID** as a Device Variable with a value of *eigrp_as_num*. Click on **New Redistribute** under the Unicast Address Family => Re-Distribute section

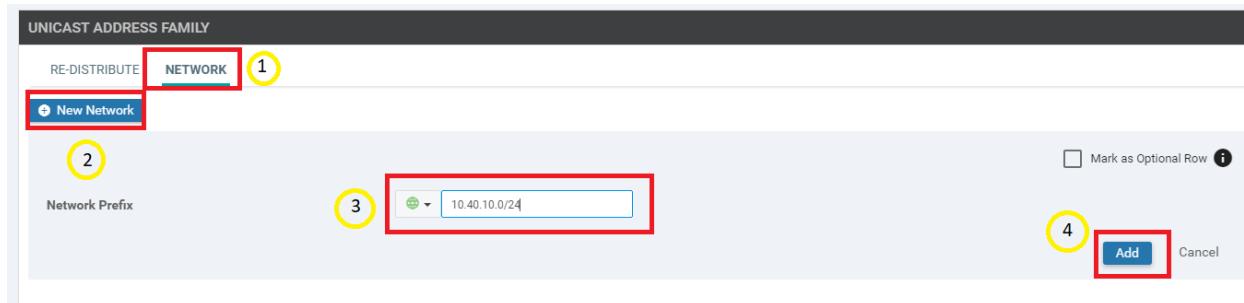


6. No routes get redistributed into EIGRP but we want to ensure that WAN Routes are advertised into the Site 40 LAN.

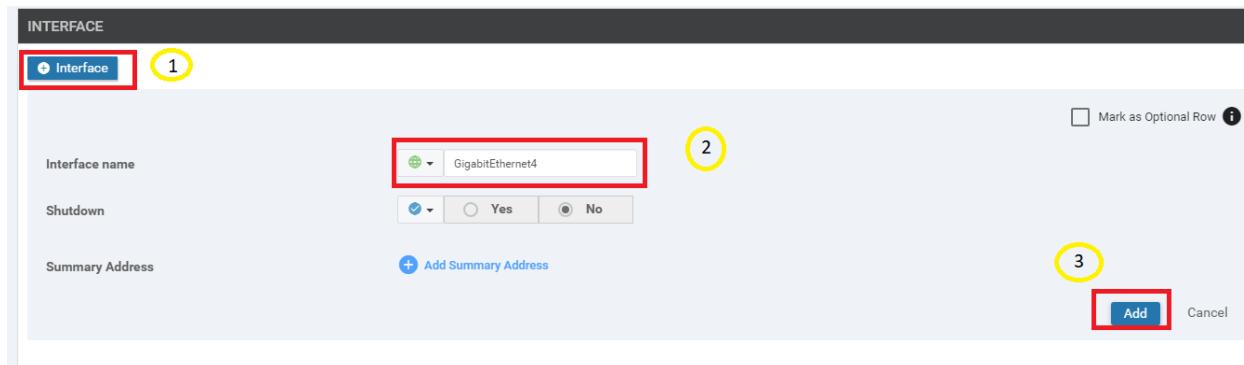
For this purpose, choose **OMP** and click on **Add**. This will redistribute OMP routes into EIGRP



7. Under the Unicast Address Family section, click on the **Network** tab. Click on **New Network** and Enter a Global Network Prefix of 10.40.10.0/24. Click on **Add**



8. Under **Interface**, click on *Interface* to add a new one. Enter the **Interface Name** as *GigabitEthernet4* and click on **Add**. This is our LAN facing interface in VPN 10 on cEdge40



9. Make sure the EIGRP template looks like the image given below and click on **Save** to save the template

BASIC CONFIGURATION

Autonomous System ID [eigrp_as_num]

UNICAST ADDRESS FAMILY

RE-DISTRIBUTE NETWORK

+ New Redistribute

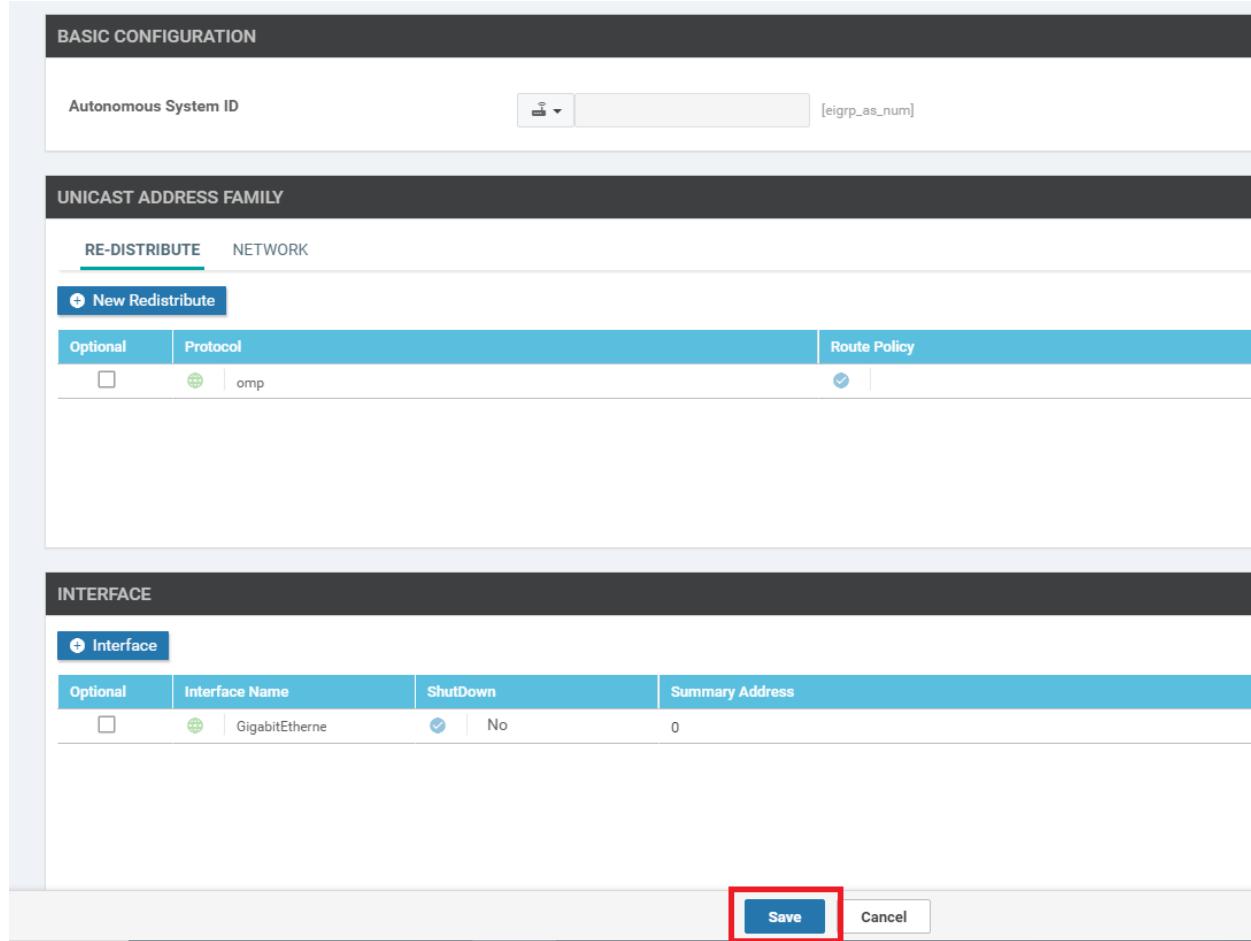
| Optional | Protocol | Route Policy |
|--------------------------|----------|-------------------------------------|
| <input type="checkbox"/> | omp | <input checked="" type="checkbox"/> |

INTERFACE

+ Interface

| Optional | Interface Name | ShutDown | Summary Address |
|--------------------------|----------------|-------------------------------------|-----------------|
| <input type="checkbox"/> | GigabitEtherne | <input checked="" type="checkbox"/> | No 0 |

Save **Cancel**



10. This should take you back to the *cedge-vpn10* Template configuration window. Populate the *site40-eigrp* template in the EIGRP field. Click on **Save**

Edit VPN - cedge-vpn10

Cisco VPN Interface Ethernet   Sub-Templates 

EIGRP 

 Save

CANCEL

11. Make sure that the VPN 10 Service VPN has *Cisco VPN Interface Ethernet*, *EIGRP* tacked on to it and click on **Update**

Service VPN

[0 Rows Selected]

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|-------------------------------------|
| f018b46b-8ddc-431d-a222-cf905da7e13b | cedge-vpn10 | Cisco VPN Interface Ethernet, EIGRP |
| ff56fbce-0c12-4575-9f41-b6c7d780e13d | cedge-vpn20 | Cisco VPN Interface Ethernet |
| 9a88750f-7bd2-4fd5-b9d3-10a11544c8b6 | cedge-vpn30 | Cisco VPN Interface Ethernet |

Additional Templates

| | |
|---------------------|---------------------------------------|
| AppQoE | Choose... |
| Global Template * | Factory_Default_Global_CISCO_Template |
| Cisco Banner | Choose... |
| Cisco SNMP | Choose... |
| CLI Add-On Template | Choose... |
| Policy | Choose... |

12. We are taken to the configuration page for the cEdge40. Enter the Autonomous System ID as 40 and click on **Next**

| S... | Chassis Number | System IP | Hostname | vpn20_if_name) | IPv4 Address/ prefix-length(vpn20_if_ipv4_address) | Autonomous System ID(eigrp_as_num) |
|-------------------------------------|---|---------------|----------|----------------|--|------------------------------------|
| <input checked="" type="checkbox"/> | CSR-04F9482E-44F0-E4DC-D30D-60C0806F... | 10.255.255.41 | cEdge40 | | 10.40.20.2/24 | 40 |

13. Review the side-by-side config diff (notice the EIGRP configuration added) and click on **Configure Devices**.

CONFIGURATION | TEMPLATES

| Device Template | Total |
|--------------------------|-------|
| cEdge_dualuplink_devtemp | 1 |

Device list (Total: 1 devices)

```

CSR-04F9482E-44F0-E4DC-D30D-  
80C0006F73F2  
cEdge40(10.255.255.41)
  
```

Filter/Search

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

```

301 aaa authorization exec default local
302 aaa session-id common
303 no crypto ikev2 diagnose error
304 no crypto isakmp diagnose error
305 router eigrp eigrp-name
306 address-family ipv4 vrf 10 autonomous-system 40
307 af-interface GigabitEthernet4
308 no dampening-change
309 no dampening-interval
310 hello-interval 5
311 hold-time 15
312 split-horizon
313 exit-af-interface
314 !
315 network 10.40.10.0 0.0.0.255
316 topology base
317 redistribute ospf
318 exit-af-topology
319 !
320 exit-address-family
321 !
322 !
323 snmp-server ifindex persist
324 line con 0
325 login authentication default
326 speed 19200
327 stopbits 1
328 !
329 line vty 0 4
330 transport input ssh
331 !
332 line vty 5 80
333 transport input ssh
334 !
  
```

Configure Device Rollback Timer

Back Configure Devices Cancel

This completes the EIGRP related configuration on VPN 10 for the Site 40 cEdge.

Task List

- [Overview](#)
- [Updating the cEdge Service VPN 10 with an EIGRP Template](#)
- [Activity Verification and Remediation](#)

Activity Verification and Remediation

1. Log in to the CLI of cEdge40 via Putty. The username and password are `admin`. Enter `show ip eigrp vrf 10 40 neighbors` to view the EIGRP neighbours in VPN 10, AS 40. We will see one neighbour (the L3 Device)

```
cEdge40#show ip eigrp vrf 10 40 neighbors
EIGRP-IPv4 VR(eigrp-name) Address-Family Neighbors for AS(40)
          VRF(10)
H   Address           Interface      Hold Uptime    SRTT     RTO   Q   Seq
   (sec)          (ms)          Cnt Num
0   10.40.10.1        Gi4            12  00:02:01    8    100  0   3
cEdge40#
```

show ip eigrp vrf 10 40 neighbors

2. Run `show ip route vrf 10` - you should see a `10.40.11.0/24` route learnt via EIGRP

```
cEdge40#show ip route vrf 10

Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
m        10.0.0.1/32 [251/0] via 10.255.255.12, 00:59:19, sdwan_system_ip
                  [251/0] via 10.255.255.11, 00:59:19, sdwan_system_ip
m        10.20.10.0/24 [251/0] via 10.255.255.22, 09:21:30, sdwan_system_ip
                  [251/0] via 10.255.255.21, 09:21:30, sdwan_system_ip
m        10.30.10.0/24 [251/0] via 10.255.255.31, 09:21:30, sdwan_system_ip
C        10.40.10.0/24 is directly connected, GigabitEthernet4
L        10.40.10.2/32 is directly connected, GigabitEthernet4
D        10.40.11.0/24 [90/2570240] via 10.40.10.1, 00:02:54, GigabitEthernet4
m        10.50.10.0/24 [251/0] via 10.255.255.52, 09:13:08, sdwan_system_ip
                  [251/0] via 10.255.255.51, 09:13:08, sdwan_system_ip
m        10.100.10.0/24 [251/0] via 10.255.255.12, 09:21:30, sdwan_system_ip
                  [251/0] via 10.255.255.11, 09:21:30, sdwan_system_ip
```

show ip route vrf 10

3. Log in via Putty to **DC-vEdge1** and try to ping an IP in the `10.40.11.0/24` network. Type `ping vpn 10 10.40.11.1` - the pings should fail. Issue `show ip route vpn 10` and you will notice that there is no route for the `10.40.11.0/24` subnet

```

DC-vEdge1# ping vpn 10 10.40.11.1
Ping in VPN 10
PING 10.40.11.1 (10.40.11.1) 56(84) bytes of data.
From 127.1.0.2 icmp_seq=1 Destination Net Unreachable
From 127.1.0.2 icmp_seq=2 Destination Net Unreachable
From 127.1.0.2 icmp_seq=3 Destination Net Unreachable
From 127.1.0.2 icmp_seq=4 Destination Net Unreachable
^C
--- 10.40.11.1 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 2999ms

DC-vEdge1# show ip route vpn 10
Codes Proto-sub-type:
 IA -> ospf-intra-area, IE -> ospf-inter-area,
 E1 -> ospf-external, E2 -> ospf-external2,
 N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
 e -> bgp-external, i -> bgp-internal
Codes Status flags:
 F -> fib, S -> selected, I -> inactive,
 B -> blackhole, R -> recursive

      VPN   PREFIX          PROTOCOL      NEXTHOP      NEXTHOP      NEXTHOP
           SUB TYPE     IF NAME    ADDR     VPN   TLOC IP   COLOR
-----+-----+-----+-----+-----+-----+-----+-----+-----+
 10  10.0.0.1/32      ospf        IA      ge0/2  10.100.10.1  -    -    -
 10  10.20.10.0/24     osp         -      -      -      -  10.255.255.22 mpls
 10  10.20.10.0/24     osp         -      -      -      -  10.255.255.21 public-internet
 10  10.30.10.0/24     osp         -      -      -      -  10.255.255.31 mpls
 10  10.30.10.0/24     osp         -      -      -      -  10.255.255.31 public-internet
 10  10.40.10.0/24     osp         -      -      -      -  10.255.255.41 mpls
 10  10.40.10.0/24     osp         -      -      -      -  10.255.255.41 public-internet
 10  10.50.10.0/24     osp         -      -      -      -  10.255.255.51 public-internet
 10  10.50.10.0/24     osp         -      -      -      -  10.255.255.52 mpls
 10  10.100.10.0/24    ospf        IA      ge0/2  -      -    -
 10  10.100.10.0/24    connected   -      ge0/2  -      -    -

```

```

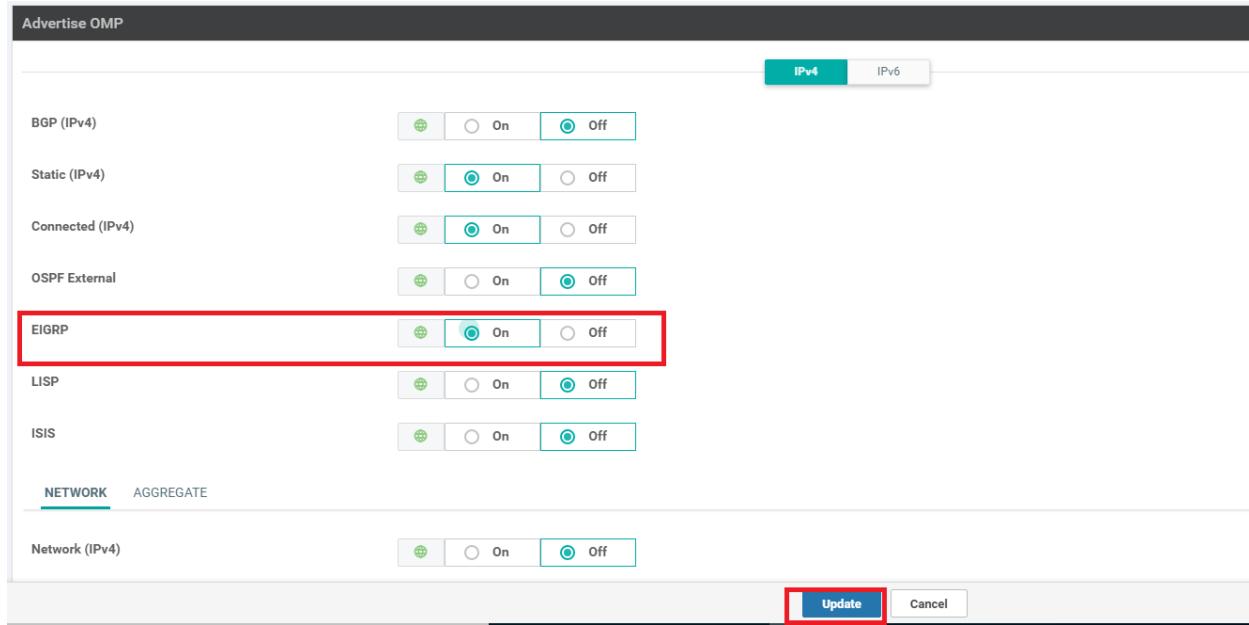
ping vpn 10 10.40.11.1
show ip route vpn 10

```

4. This is due to the fact that EIGRP routes aren't advertised into OMP. To remedy this, we will need to modify our cEdge Template. Go to **Configuration => Templates => Feature tab** and click on the three dots next to *cedge-vpn10*. Choose to **Edit**

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------|--------------------------------------|---------------------|--------------|------------------|------------------|------------|-----------------------------|---|
| vEdge-vpn10 | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 25 May 2020 12:49:58 AM PDT | ... |
| vEdge-vpn10-int | VPN 10 Interface Template for vEd... | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 25 May 2020 1:43:16 PM PDT | ... |
| cedge-vpn10 | VPN 10 Template for the cEdges... | Cisco VPN | CSR1000v | 2 | 3 | admin | 25 May 2020 1:53:38 PM PDT | ... |
| cedge-vpn10-int | VPN 10 Interface Template for cEd... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 25 May 2020 | View Edit Change Device Models Delete Copy |

5. Navigate to the **Advertise OMP** section and set EIGRP to Global - **On**. Click on **Update**



6. Click **Next** on the Device page since we don't have to update any values. Note that this change will be pushed to multiple devices, even those that don't have EIGRP configured (e.g. Site 50 Devices). We need to make sure that this change is pushed to the Site 40 cEdge

| Chassis Number | System IP | Hostname | Interface Name(vpn30_if_name) | IPv4 Address/ prefix-length(vpn30_if_ip4_address) | Interface Name(vpn20_if_name) |
|--|---------------|----------|-------------------------------|---|-------------------------------|
| CSR-834E40DC-E358-8DE1-0E81-7E6598413... | 10.255.255.51 | cEdge50 | GigabitEthernet5 | 10.50.30.2/24 | GigabitEthernet4 |
| CSR-D1837F36-6A1A-1850-7C1C-E1C69759... | 10.255.255.52 | cEdge51 | GigabitEthernet5 | 10.50.30.3/24 | GigabitEthernet4 |

At the bottom right are 'Next' and 'Cancel' buttons, with 'Next' highlighted by a red box.

7. Check the side-by-side configuration, noting that EIGRP routes will now be advertised into OMP. Click on **Configure Devices**

```

Device Template Total
cEdge-single-uplink 2

Device list (Total: 2 devices)
Filter/Search

CSR-824E400C-E358-8DE1-0E81-
76E98413BF4
cEdge5|10.255.255.51

CSR-D1837F36-6A1A-1850-7C1C-
E1C69759FBA3
cEdge5|10.255.255.52

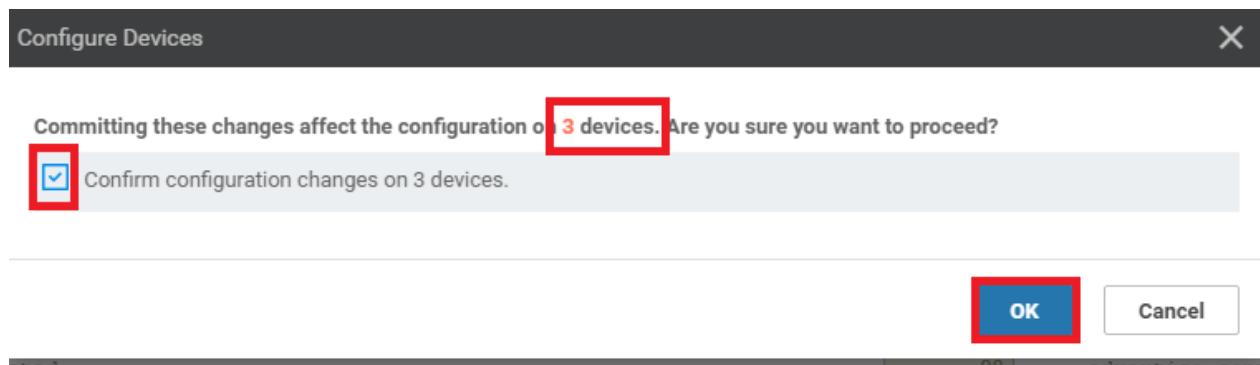
77 appqoe
78 no tcptopt enable
79 !
80 omp
81 no shutdown
82 send-path-limit 4
83 ecmp-limit 4
84 graceful-restart
85 no as-dot-notation
86 timers
87 holdtime 60
88 advertisement-interval 1
89 graceful-restart-timer 43200
90 eor-timer 300
91 exit
92 address-family ipv4 vrf 10
93 advertise connected
94 advertise static
95 !
96 address-family ipv4 vrf 20
97 advertise connected
98 advertise static
99 !
100 address-family ipv4 vrf 30
101 advertise connected
102 advertise static
103 !
104 address-family ipv4
105 advertise connected
106 advertise static
107 !
108 address-family ipv6
109 advertise connected
110 advertise static
111

77 appqoe
78 no tcptopt enable
79 !
80 omp
81 no shutdown
82 send-path-limit 4
83 ecmp-limit 4
84 graceful-restart
85 no as-dot-notation
86 timers
87 holdtime 60
88 advertisement-interval 1
89 graceful-restart-timer 43200
90 eor-timer 300
91 exit
92 address-family ipv4 vrf 10
93 advertise connected
94 advertise static
95 advertise eigrp
96 !
97 address-family ipv4 vrf 20
98 advertise connected
99 advertise static
100 !
101 address-family ipv4 vrf 30
102 advertise connected
103 advertise static
104 !
105 address-family ipv4
106 advertise connected
107 advertise static
108 !
109 address-family ipv6
110 advertise connected
111 advertise static

```

Configure Device Rollback Timer Back **Configure Devices** Cancel

8. Confirm the change (pushed to 3 devices) and click on OK



9. Wait for the change to successfully go through

| | Status | Message | Chassis Number | Device Model | Hostname | System IP | Site ID | vManage IP |
|---|---------|-------------------------------------|----------------------------------|--------------|----------|---------------|---------|--------------|
| > | Success | Done - Push Feature Template Con... | CSR-834E40DC-E358-8DE1-0E81-7... | CSR1000v | cEdge50 | 10.255.255.51 | 50 | 10.255.255.1 |
| > | Success | Done - Push Feature Template Con... | CSR-D1837F36-6A0A-1B50-7C1C... | CSR1000v | cEdge51 | 10.255.255.52 | 50 | 10.255.255.1 |
| > | Success | Done - Push Feature Template Con... | CSR-04F9482E-44F0-E40C-D30D... | CSR1000v | cEdge40 | 10.255.255.41 | 40 | 10.255.255.1 |

10. Once successful, go to the CLI for **DC-vEdge1** and issue `show ip route vpn 10` again. You should see routes for `10.40.11.0/24`

| DC-vEdge1# show ip route vpn 10 | | | | | | | | |
|---|----------------|-----------|----------------------|--------------------|-----------------|----------------|---------------|----|
| Codes Proto-sub-type: | | | | | | | | |
| IA -> ospf-intra-area, IE -> ospf-inter-area, | | | | | | | | |
| El -> ospf-externall, E2 -> ospf-external2, | | | | | | | | |
| N1 -> ospf-nssa-externall, N2 -> ospf-nssa-external2, | | | | | | | | |
| e -> bgp-external, i -> bgp-internal | | | | | | | | |
| Codes Status flags: | | | | | | | | |
| F -> fib, S -> selected, I -> inactive, | | | | | | | | |
| B -> blackhole, R -> recursive | | | | | | | | |
| VPN | PREFIX | PROTOCOL | PROTOCOL SUB TYPE | NEXTHOP IF NAME | NEXTHOP ADDR | NEXTHOP VPN | TLOC | IP |
| 10 | 10.0.0.1/32 | ospf | IA | ge0/2 | 10.100.10.1 | - | - | |
| 10 | 10.20.10.0/24 | omp | - | - | - | - | 10.255.255.22 | |
| 10 | 10.20.10.0/24 | omp | - | - | - | - | 10.255.255.21 | |
| 10 | 10.30.10.0/24 | omp | - | - | - | - | 10.255.255.31 | |
| 10 | 10.30.10.0/24 | omp | - | - | - | - | 10.255.255.31 | |
| 10 | 10.40.10.0/24 | omp | - | - | - | - | 10.255.255.41 | |
| 10 | 10.40.10.0/24 | omp | - | - | - | - | 10.255.255.41 | |
| 10 | 10.40.11.0/24 | omp | - | - | - | - | 10.255.255.41 | |
| 10 | 10.40.11.0/24 | omp | - | - | - | - | 10.255.255.41 | |
| 10 | 10.50.10.0/24 | omp | - | - | - | - | 10.255.255.51 | |
| 10 | 10.50.10.0/24 | omp | - | - | - | - | 10.255.255.52 | |
| 10 | 10.100.10.0/24 | ospf | IA | ge0/2 | - | - | - | |
| 10 | 10.100.10.0/24 | connected | - | ge0/2 | - | - | - | |

```
show ip route vpn 10
```

11. Run a ping to `10.40.11.1` via the CLI `ping vpn 10 10.40.11.1`. It should be successful

```
DC-vEdge1# ping vpn 10 10.40.11.1
Ping in VPN 10
PING 10.40.11.1 (10.40.11.1) 56(84) bytes of data.
64 bytes from 10.40.11.1: icmp_seq=2 ttl=253 time=0.457 ms
64 bytes from 10.40.11.1: icmp_seq=3 ttl=253 time=0.494 ms
64 bytes from 10.40.11.1: icmp_seq=4 ttl=253 time=0.464 ms
64 bytes from 10.40.11.1: icmp_seq=5 ttl=253 time=0.632 ms
64 bytes from 10.40.11.1: icmp_seq=6 ttl=253 time=0.532 ms
^C
--- 10.40.11.1 ping statistics ---
6 packets transmitted, 5 received, 16% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.457/0.515/0.632/0.070 ms
DC-vEdge1#
```

```
ping vpn 10 10.40.11.1
```

This completes the EIGRP verification and remediation activity.

Task List

- [Overview](#)
- [Updating the eEdge Service VPN 10 with an EIGRP Template](#)
- [Activity Verification and Remediation](#)



-->

Configuring Virtual Router Redundancy Protocol

Summary: Using Configuration Templates to set up VRRP as a First Hop Redundancy Protocol at Site 50.

Table of Contents

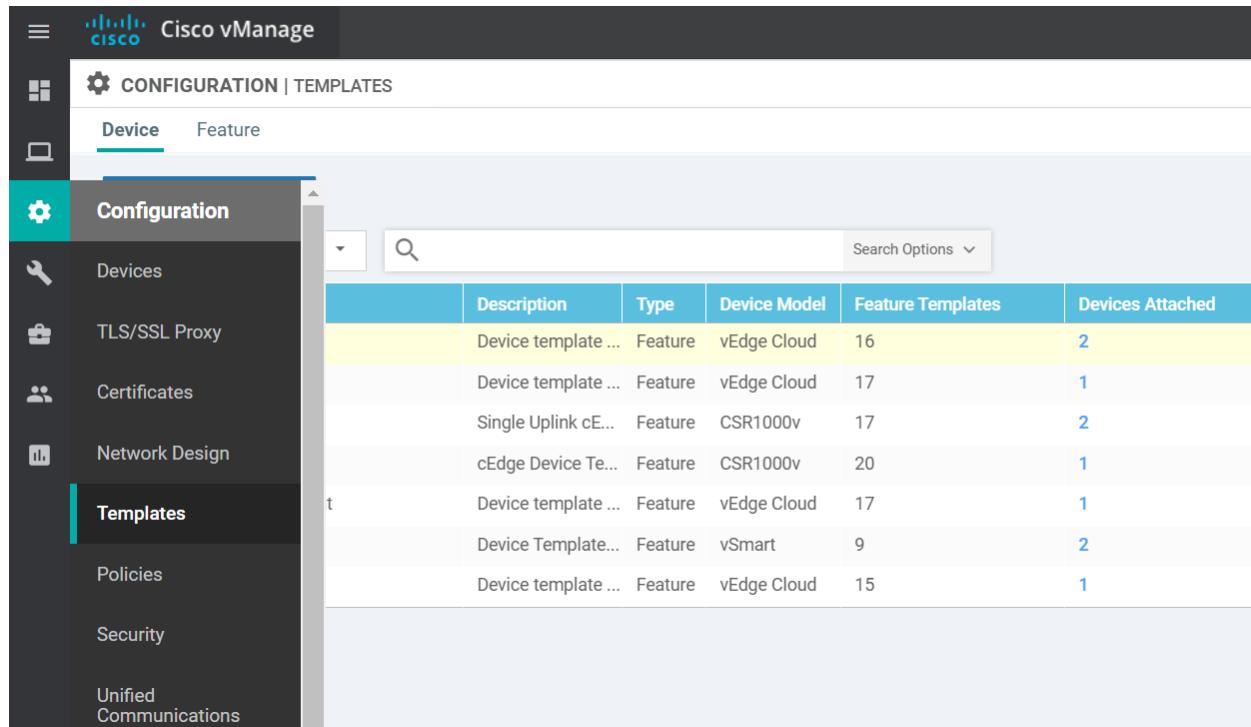
- [Editing Templates to support VRRP](#)
- [Verification and Testing](#)

Task List

- Editing Templates to support VRRP
- Verification and Testing

Editing Templates to support VRRP

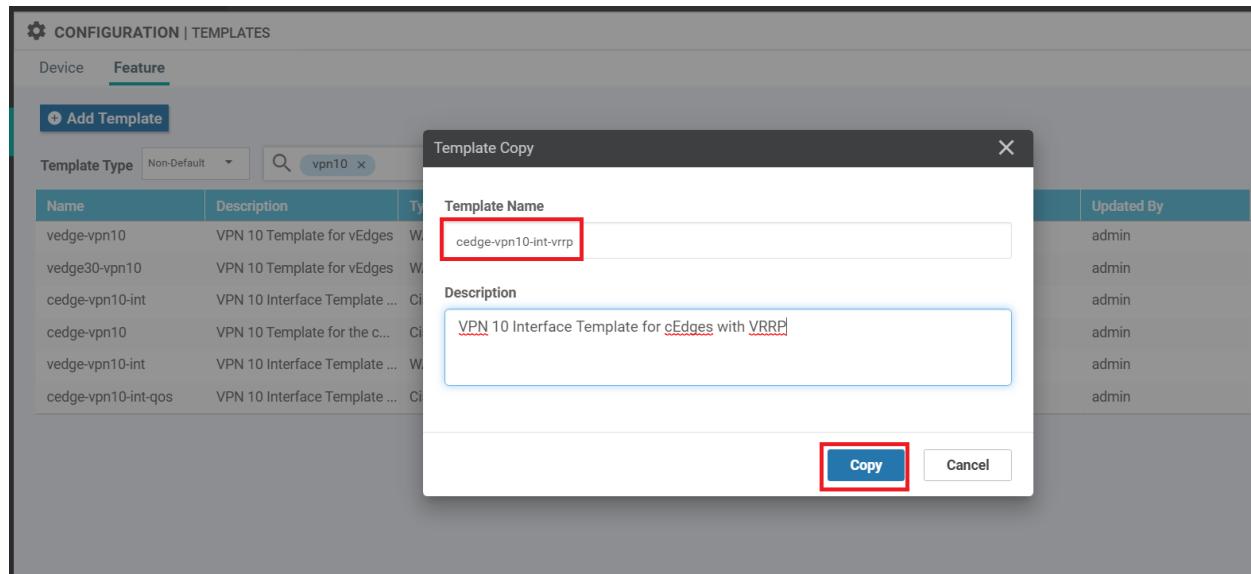
1. On the vManage GUI, navigate to **Configuration => Templates => Feature Tab**



The screenshot shows the Cisco vManage interface under the Configuration | Templates section. The left sidebar has a 'Device' tab selected. The main area is titled 'Configuration' and lists various templates. A search bar at the top right includes a magnifying glass icon and a 'Search Options' dropdown. The table below has columns: Description, Type, Device Model, Feature Templates, and Devices Attached. The data rows include:

| | Description | Type | Device Model | Feature Templates | Devices Attached |
|---------------------|-------------|-------------|--------------|-------------------|------------------|
| Device template ... | Feature | vEdge Cloud | 16 | 2 | |
| Device template ... | Feature | vEdge Cloud | 17 | 1 | |
| Single Uplink cE... | Feature | CSR1000v | 17 | 2 | |
| cEdge Device Te... | Feature | CSR1000v | 20 | 1 | |
| Device template ... | Feature | vEdge Cloud | 17 | 1 | |
| Device Template... | Feature | vSmart | 9 | 2 | |
| Device template ... | Feature | vEdge Cloud | 15 | 1 | |

2. Locate the *cedge-vpn10-int* template and click on the three dots next to it. Choose to **Copy** and name the copied template *cedge-vpn10-int-vrrp*. Enter a Description of *VPN 10 Interface Template for cEdges with VRRP*. Click on **Copy**



The screenshot shows the 'Template Copy' dialog box over the main configuration screen. The dialog has fields for 'Template Name' (set to 'cedge-vpn10-int-vrrp') and 'Description' (set to 'VPN 10 Interface Template for cEdges with VRRP'). At the bottom are 'Copy' and 'Cancel' buttons, with the 'Copy' button highlighted by a red box.

3. Click on the three dots next to the newly copied template and click on **Edit**

The screenshot shows the Cisco vManage interface under the Configuration | Templates section. A table lists templates, with one row highlighted for a 'VRRP' template named 'edge...'. To the right of this row is a context menu with options: View, Edit (which is highlighted with a red box), Change Device Models, Delete, and Copy. The menu is titled 'More Options'.

4. Navigate to the VRRP section and click on **New VRRP**. Update the parameters as shown in the table below, using the image for reference. click on **Add**

| Field | Global or Device Specific (Drop Down) | Value |
|------------|---------------------------------------|-------------------------------|
| Group ID | Global | 5 |
| Priority | Device Specific | <i>vpn10_if_vrrp_priority</i> |
| Track OMP | Global | On |
| IP Address | Global | 10.50.10.100 |

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP Advanced

IPv4 IPv6

New VRRP 1

| | | |
|----------------------|----------------|----------------------------|
| Group ID | 2 | 5 |
| Priority | 3 | 4 [vpn10_if.vrrp.priority] |
| Timer (milliseconds) | 100 | |
| Track OMP | On | 5 |
| IP Address | 6 10.50.10.100 | |

Add Cancel

5. Click on **Update**

New VRRP

| Optional | Group ID | Priority | Timer | Track OMP | Track Prefix List |
|--------------------------|----------|------------|-------|-----------|-------------------|
| <input type="checkbox"/> | 5 | [vpn10...] | 100 | On | |

ACL/QOS

Shaping Rate (Kbps)

QoS Map

Dynamic Rule

Update Cancel

6. Go to the Device tab in **Configuration => Templates** and locate the *cEdge-single-uplink* Device Template. Click on the three dots next to it and click **Edit**

 CONFIGURATION | TEMPLATES

Device Feature

 Total Rows: 7

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated |
|---------------------------|---------------------|---------|--------------|-------------------|------------------|------------|-------------------|
| DCvEdge_dev_temp | Device template ... | Feature | vEdge Cloud | 16 | 2 | admin | 28 May 2020 4 ... |
| vEdge_Site20_dev_temp | Device template ... | Feature | vEdge Cloud | 17 | 1 | admin | 07 Jun 2020 6 ... |
| cEdge-single-uplink | Single Uplink cE... | Feature | CSR1000v | 17 | 2 | admin | 26 May 2020 3 ... |
| cEdge_dualuplink_devtemp | cEdge Device Te... | Feature | CSR1000v | 20 | 1 | admin | |
| vEdge_Site20_dev_temp_nat | Device template ... | Feature | vEdge Cloud | 17 | 1 | admin | |
| vSmart-dev-temp | Device Template... | Feature | vSmart | 9 | 2 | admin | |
| vEdge30_dev_temp | Device template ... | Feature | vEdge Cloud | 15 | 1 | admin | |

7. Scroll down to the **Service VPN** section and click on the three dots next to **cedge-vpn10**. Choose to **Edit**

Service VPN

1 Rows Selected |  

Total Rows: 3

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|------------------------------|
| f018b46b-8ddc-431d-a222-cf905da7e13b | cedge-vpn10 | Cisco VPN Interface Ethernet |
| ff56fbce-0c12-4575-9f41-b6c7d780e13d | cedge-vpn20 | Cisco VPN Interface Ethernet |
| 9a88750f-7bd2-4fd5-b9d3-10a11544c8b6 | cedge-vpn30 | Cisco VPN Interface Ethernet |

8. Populate **cedge-vpn10-int-vrrp** for the **Cisco VPN Interface Ethernet** and click on **Save**

Edit VPN - cedge-vpn10

Cisco VPN Interface Ethernet

+ Sub-Templates ▾

cedge-vpn10-int-vrrp



Save

CANCEL

9. Back at the main Device Template screen, click on **Update**

Service VPN

0 Rows Selected | [+ Add VPN](#) | [- Remove VPN](#)

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|------------------------------|
| f018b46b-8ddc-431d-a222-cf905da7e13b | cedge-vpn10 | Cisco VPN Interface Ethernet |
| ff56fbce-0c12-4575-9f41-b6c7d780e13d | cedge-vpn20 | Cisco VPN Interface Ethernet |
| 9a88750f-7bd2-4fd5-b9d3-10a11544c8b6 | cedge-vpn30 | Cisco VPN Interface Ethernet |

Additional Templates

AppQoE

Global Template *

[Update](#) | [Cancel](#)

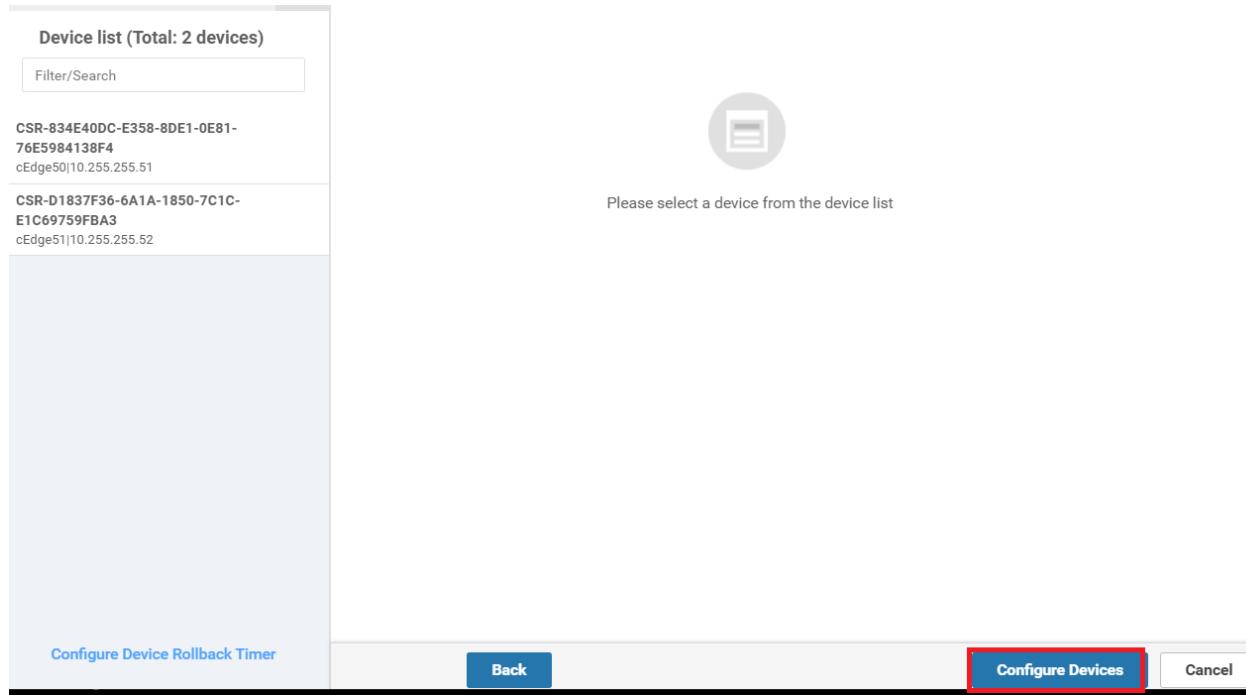
10. Enter a Priority of **110** for cEdge50 and a priority of **100** for cEdge51. This will ensure that cEdge50 becomes the MASTER, if available. Click on **Next**

Search Options ▾

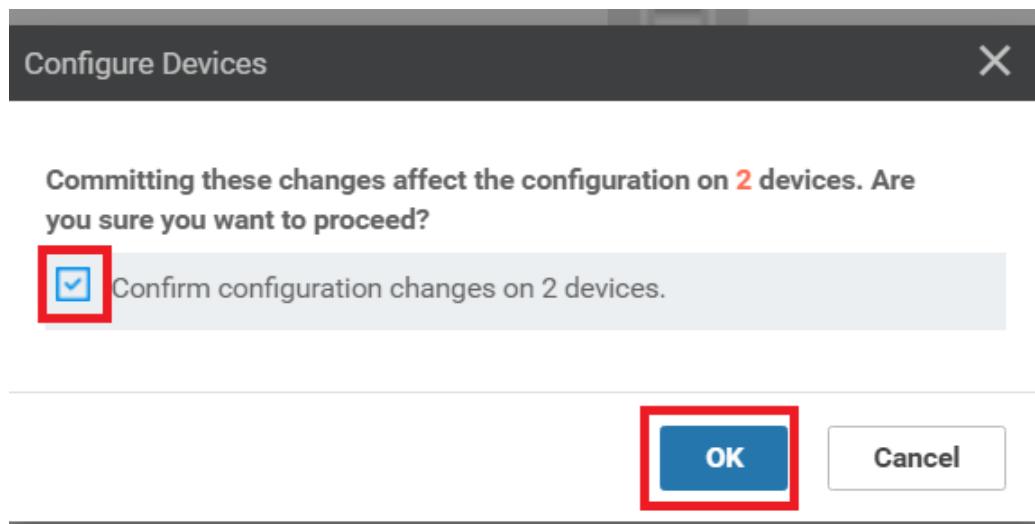
| S... | Chassis Number | System IP | Hostname | Priority(vpn10_if_vrrp_priority) | Ad |
|-------------------------------------|--|---------------|----------|----------------------------------|----|
| <input checked="" type="checkbox"/> | CSR-834E40DC-E358-8DE1-0E81-76E598413... | 10.255.255.51 | cEdge50 | 110 | 19 |
| <input checked="" type="checkbox"/> | CSR-D1837F36-6A1A-1850-7C1C-E1C69759... | 10.255.255.52 | cEdge51 | 100 | 19 |

[Next](#) | [Cancel](#)

11. Click on **Configure Devices**



12. Confirm the configuration change and click on **OK**



13. Once the configuration change goes through, log in to the CLI of cEdge50 and cEdge51 via Putty and enter the command `show vrrp 5 Gig3` on both. We should see that cEdge50 is the MASTER and cEdge51 is the BACKUP

The image shows two PuTTY windows side-by-side. The left window is titled '192.168.0.50 - PuTTY' and the right window is titled '192.168.0.51 - PuTTY'. Both windows display the output of the command 'show vrrp 5 Gig3'. In the first window, the state is 'MASTER' and the priority is 110. In the second window, the state is 'BACKUP' and the priority is 100. Both outputs provide detailed information about the VRRP group, including the virtual IP address (10.50.10.100), virtual MAC address (0000.5E00.0105), advertisement interval (100 msec), and master information.

```
cEdge50#show vrrp 5 Gig3
Group 5 interface: GigabitEthernet3 - Address-Family IPv4
State is MASTER
  State duration 1 mins 13.461 secs
  Virtual IP address is 10.50.10.100
  Virtual MAC address is 0000.5E00.0105
  Advertisement interval is 100 msec
  Preemption enabled
  Priority is 110
    Track object omp state UNDEFINED shutdown
  Master Router is 10.50.10.2 (local), priority is 110
  Master Advertisement interval is 100 msec (expires in 20 msec)
  Master Down interval is unknown
  FLAGS: 1/1

cEdge50#
```



```
cEdge51#show vrrp 5 Gig3
Group 5 interface: GigabitEthernet3 - Address-Family IPv4
State is BACKUP
  State duration 1 mins 22.500 secs
  Virtual IP address is 10.50.10.100
  Virtual MAC address is 0000.5E00.0105
  Advertisement interval is 100 msec
  Preemption enabled
  Priority is 100
    Track object omp state UNDEFINED shutdown
  Master Router is 10.50.10.2, priority is 110
  Master Advertisement interval is 100 msec (learned)
  Master Down interval is 360 msec (expires in 331 msec)
  FLAGS: 0/1

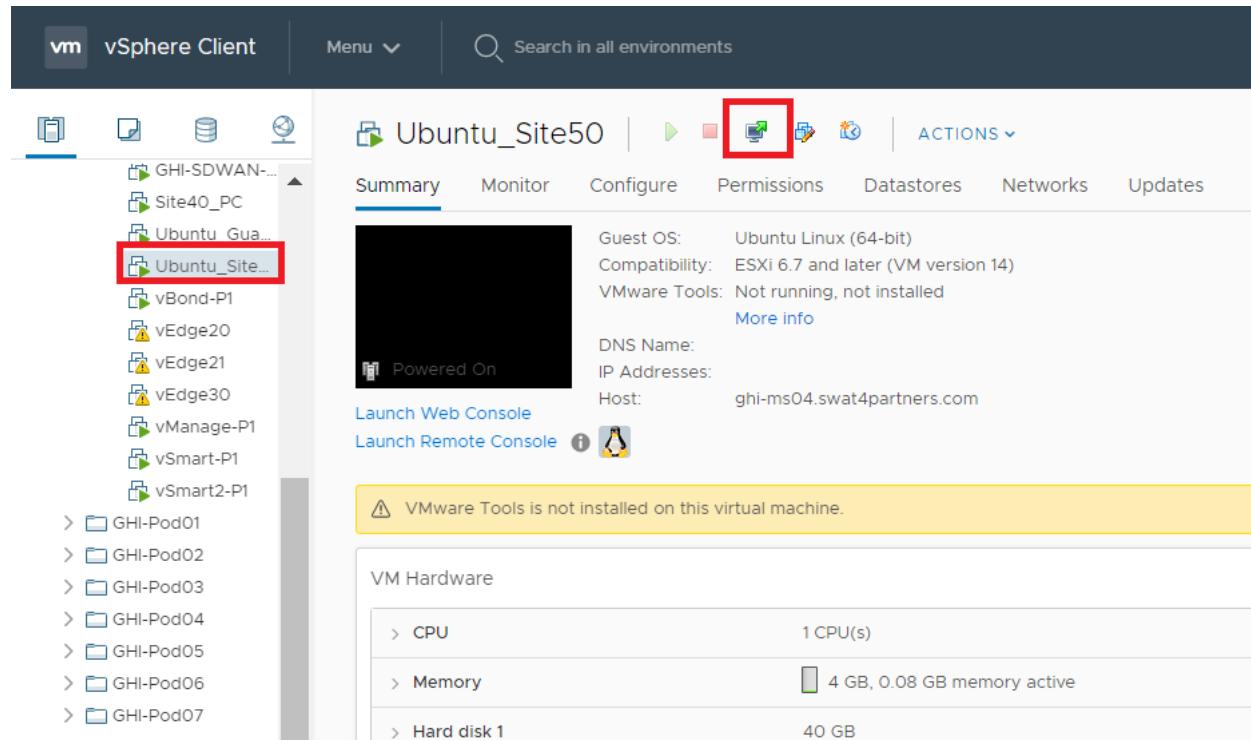
cEdge51#
```

Task List

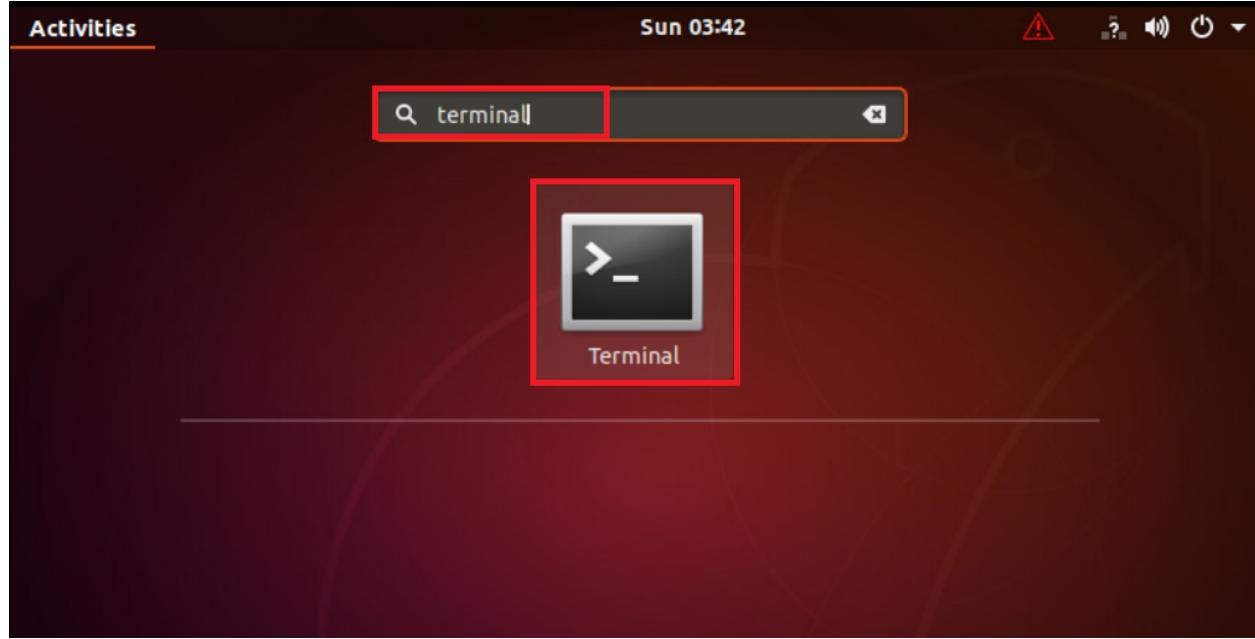
- [Editing Templates to support VRRP](#)
- [Verification and Testing](#)

Verification and Testing

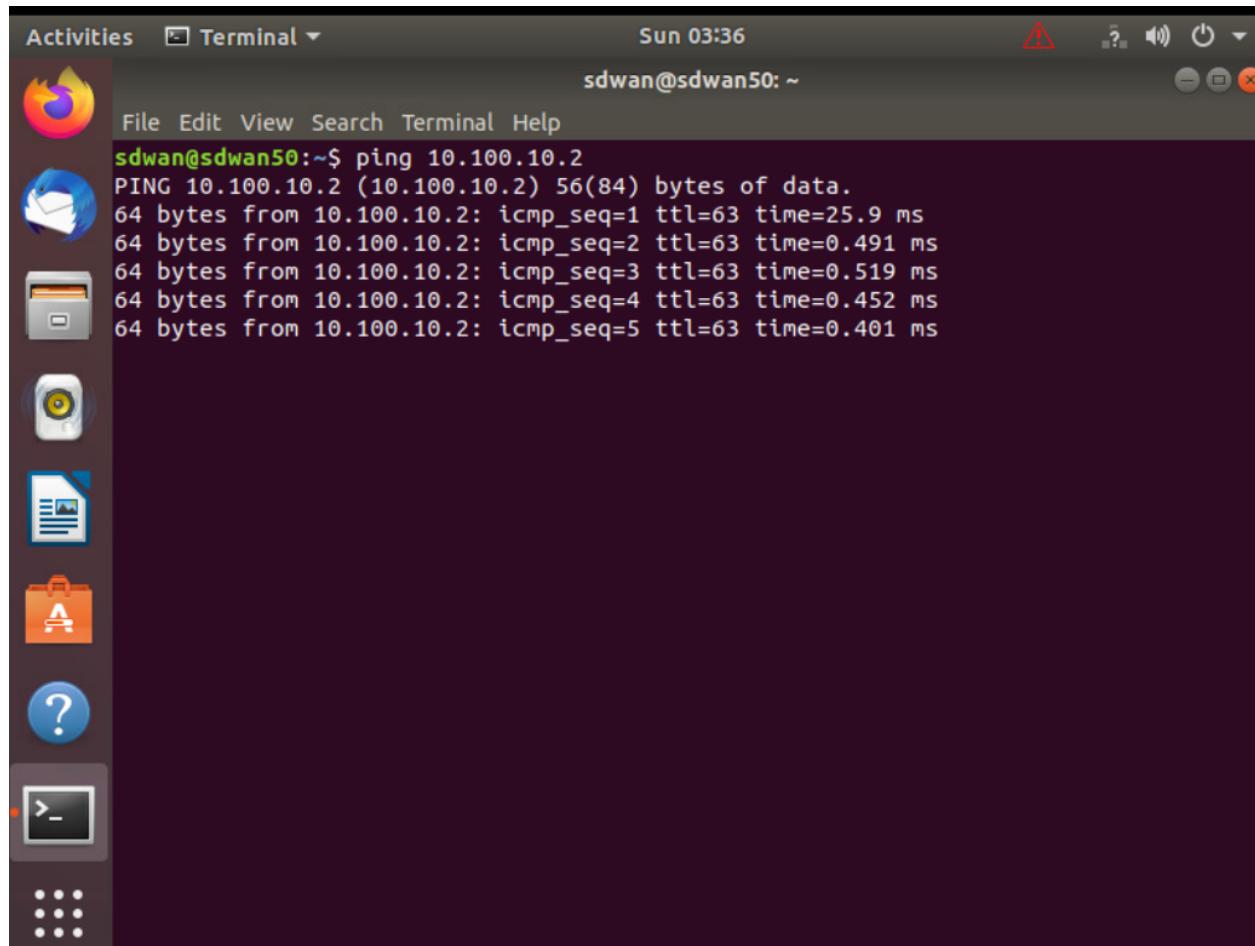
1. Log in to vCenter via the Bookmark in Chrome (or go to the URL 10.2.1.50/ui). Use the credentials provided to you for your POD. Locate the *sdwan-slc/ghi-site50pc-podX* VM (in the image it is named Ubuntu_Site50) and click on the Console icon. Choose Web Console, if prompted



2. Log in to the Site50 PC (if the VM hangs after entering the credentials, please reboot the VM for your POD and try again) and click on the Start button equivalent on Ubuntu. Search for *terminal* and click on the icon to open Terminal



3. Enter `ping 10.100.10.2`. The pings should be successful. Let the pings run

A screenshot of an Ubuntu desktop environment. On the left is a vertical dock with icons for various applications: Firefox, Evolution, Nautilus, System Settings, Help, Dash, and a terminal window icon. The main window is a terminal window titled "sdwan@sdwan50: ~". The terminal shows the command "ping 10.100.10.2" being run, followed by its output: PING 10.100.10.2 (10.100.10.2) 56(84) bytes of data. 64 bytes from 10.100.10.2: icmp_seq=1 ttl=63 time=25.9 ms 64 bytes from 10.100.10.2: icmp_seq=2 ttl=63 time=0.491 ms 64 bytes from 10.100.10.2: icmp_seq=3 ttl=63 time=0.519 ms 64 bytes from 10.100.10.2: icmp_seq=4 ttl=63 time=0.452 ms 64 bytes from 10.100.10.2: icmp_seq=5 ttl=63 time=0.401 ms. The terminal window has a dark background and light-colored text.

```
sdwan@sdwan50:~$ ping 10.100.10.2
PING 10.100.10.2 (10.100.10.2) 56(84) bytes of data.
64 bytes from 10.100.10.2: icmp_seq=1 ttl=63 time=25.9 ms
64 bytes from 10.100.10.2: icmp_seq=2 ttl=63 time=0.491 ms
64 bytes from 10.100.10.2: icmp_seq=3 ttl=63 time=0.519 ms
64 bytes from 10.100.10.2: icmp_seq=4 ttl=63 time=0.452 ms
64 bytes from 10.100.10.2: icmp_seq=5 ttl=63 time=0.401 ms
```

4. Back at the CLI for cEdge50, enter the commands to reload this Router. In privilege mode, type `reload` and confirm. You will notice Duplicate (DUP!) ping packets on the Terminal screen. This is happening since there is a short while when both Routers respond to the pings (since we've done a soft reboot of the router)

cEdge50#show vrrp 5 Gig3
GigabitEthernet3 - Group 5 - Address-Family IPv4
State is MASTER
State duration 1 mins 13.461 secs
Virtual IP address is 10.50.10.100
Virtual MAC address is 0000.5E00.0105
Advertisement interval is 100 msec
Preemption enabled
Priority is 110
Track object 0 state UNDEFINED shutdown
Master Router is 10.50.10.2 (local), priority is 110
Master Advertisement interval is 100 msec (expires in 20 msec)
Master Down interval is unknown
FLAGS: 1/1

cEdge50#reload
Proceed with reload? [confirm] █

time=0.538 ms
time=0.457 ms
time=0.316 ms
time=0.485 ms
time=0.472 ms
time=0.410 ms
time=0.482 ms
time=0.467 ms
time=0.424 ms
time=0.479 ms
time=0.438 ms
time=0.480 ms
time=0.377 ms

64 bytes from 10.100.10.2: icmp_seq=40 ttl=63 time=0.378 ms
64 bytes from 10.100.10.2: icmp_seq=41 ttl=63 time=0.412 ms
64 bytes from 10.100.10.2: icmp_seq=42 ttl=63 time=0.417 ms
64 bytes from 10.100.10.2: icmp_seq=43 ttl=63 time=0.555 ms
64 bytes from 10.100.10.2: icmp_seq=43 ttl=63 time=0.668 ms (DUP!)

64 bytes from 10.100.10.2: icmp_seq=44 ttl=63 time=0.416 ms
64 bytes from 10.100.10.2: icmp_seq=44 ttl=63 time=0.512 ms (DUP!)

64 bytes from 10.100.10.2: icmp_seq=45 ttl=63 time=0.424 ms
64 bytes from 10.100.10.2: icmp_seq=45 ttl=63 time=0.537 ms (DUP!)

64 bytes from 10.100.10.2: icmp_seq=46 ttl=63 time=0.496 ms
64 bytes from 10.100.10.2: icmp_seq=46 ttl=63 time=1.22 ms (DUP!)

64 bytes from 10.100.10.2: icmp_seq=47 ttl=63 time=0.513 ms
64 bytes from 10.100.10.2: icmp_seq=47 ttl=63 time=1.12 ms (DUP!)

64 bytes from 10.100.10.2: icmp_seq=48 ttl=63 time=0.426 ms (DUP!)

5. After a few seconds, the pings should stabilise and we'll receive a response from just cEdge51

A screenshot of a terminal window titled "Terminal". The window shows a list of ICMP packets received from the IP address 10.100.10.2. The output is as follows:

```
64 bytes from 10.100.10.2: icmp_seq=47 ttl=63 time=0.513 ms
64 bytes from 10.100.10.2: icmp_seq=47 ttl=63 time=1.12 ms (DUP!)
64 bytes from 10.100.10.2: icmp_seq=48 ttl=63 time=0.426 ms
64 bytes from 10.100.10.2: icmp_seq=49 ttl=63 time=0.464 ms
64 bytes from 10.100.10.2: icmp_seq=50 ttl=63 time=0.617 ms
64 bytes from 10.100.10.2: icmp_seq=51 ttl=63 time=0.766 ms
64 bytes from 10.100.10.2: icmp_seq=52 ttl=63 time=0.776 ms
64 bytes from 10.100.10.2: icmp_seq=53 ttl=63 time=0.564 ms
64 bytes from 10.100.10.2: icmp_seq=54 ttl=63 time=0.509 ms
64 bytes from 10.100.10.2: icmp_seq=55 ttl=63 time=0.595 ms
64 bytes from 10.100.10.2: icmp_seq=56 ttl=63 time=0.624 ms
64 bytes from 10.100.10.2: icmp_seq=57 ttl=63 time=0.624 ms
64 bytes from 10.100.10.2: icmp_seq=58 ttl=63 time=0.548 ms
64 bytes from 10.100.10.2: icmp_seq=59 ttl=63 time=0.621 ms
64 bytes from 10.100.10.2: icmp_seq=60 ttl=63 time=0.557 ms
64 bytes from 10.100.10.2: icmp_seq=61 ttl=63 time=0.616 ms
64 bytes from 10.100.10.2: icmp_seq=62 ttl=63 time=0.619 ms
64 bytes from 10.100.10.2: icmp_seq=63 ttl=63 time=0.539 ms
64 bytes from 10.100.10.2: icmp_seq=64 ttl=63 time=0.580 ms
64 bytes from 10.100.10.2: icmp_seq=65 ttl=63 time=0.677 ms
64 bytes from 10.100.10.2: icmp_seq=66 ttl=63 time=0.598 ms
64 bytes from 10.100.10.2: icmp_seq=67 ttl=63 time=0.508 ms
64 bytes from 10.100.10.2: icmp_seq=68 ttl=63 time=0.594 ms
64 bytes from 10.100.10.2: icmp_seq=69 ttl=63 time=0.506 ms
64 bytes from 10.100.10.2: icmp_seq=70 ttl=63 time=0.635 ms
64 bytes from 10.100.10.2: icmp_seq=71 ttl=63 time=0.572 ms
64 bytes from 10.100.10.2: icmp_seq=72 ttl=63 time=0.457 ms
```

6. Issue `show vrrp 5 Gig3` on the CLI of cEdge51 and you will notice that it is now the MASTER. Also, the priority of cEdge51 has been set to 100 - this will play a role once cEdge50 comes up

```
cEdge51#show vrrp 5 Gig3
GigabitEthernet3      Group 5 - Address-Family IPv4
  State is MASTER
    State duration 47.149 secs
    Virtual IP address is 10.50.10.100
    Virtual MAC address is 0000.5E00.0105
    Advertisement interval is 100 msec
    Preemption enabled
    Priority is 100
      Track object omp state UNDEFINED shutdown
    Master Router is 10.50.10.3 (local), priority is 100
    Master Advertisement interval is 100 msec (expires in 12 msec)
    Master Down interval is unknown
    FLAGS: 1/1

cEdge51#
```

7. Wait for cEdge50 to come up (approx. 5 minutes). Once you're able to SSH to it, issue `show vrrp 5 Gig3` - you will notice it has taken the role of MASTER (look at the priority - it's 110, meaning cEdge50 will always be the MASTER if available). Had we left both the devices at the default priority of 100, cEdge51 would have continued being the MASTER even after cEdge50 came back up.

Changing the priority of cEdge50 to a higher value and forcing it to be the MASTER might cause issues since it's possible that the LAN/VRRP side of the Router comes up post a reboot before the WAN/OMP side is ready. This might lead to a few dropped packets

```
cEdge50#  
cEdge50#  
cEdge50#  
cEdge50#show vrrp 5 Gig3  
GigabitEthernet3 - Group 5 - Address-Family IPv4  
  State is MASTER  
    State duration 2 mins 16.237 secs  
    Virtual IP address is 10.50.10.100  
    Virtual MAC address is 0000.5E00.0105  
    Advertisement interval is 100 msec  
    Preemption enabled  
    Priority is 110  
      Track object omp state UP shutdown  
      Master Router is 10.50.10.2 (local), priority is 110  
      Master Advertisement interval is 100 msec (expires in 33 msec)  
      Master Down interval is unknown  
    FLAGS: 1/1  
  
cEdge50#
```

Thus, we have set up a First Hop Redundancy Protocol at Site 50. This completes our Verification and Testing.

Task List

- [Editing Templates to support VRRP](#)
- [Verification and Testing](#)



TLOC Extensions at Site 20

Summary: Configuring TLOC Extensions for transport redundancy.

Table of Contents

- [Overview](#)
- [Feature Templates for TLOC Extensions](#)
 - [Creating the VPN Interface Template for the TLOC-EXT interface](#)
 - [Creating the VPN Interface Template for the Tunnel interface](#)
 - [Creating the BGP Template for the MPLS link](#)
- [Updating the VPN and Device Templates](#)
- [Activity Verification](#)

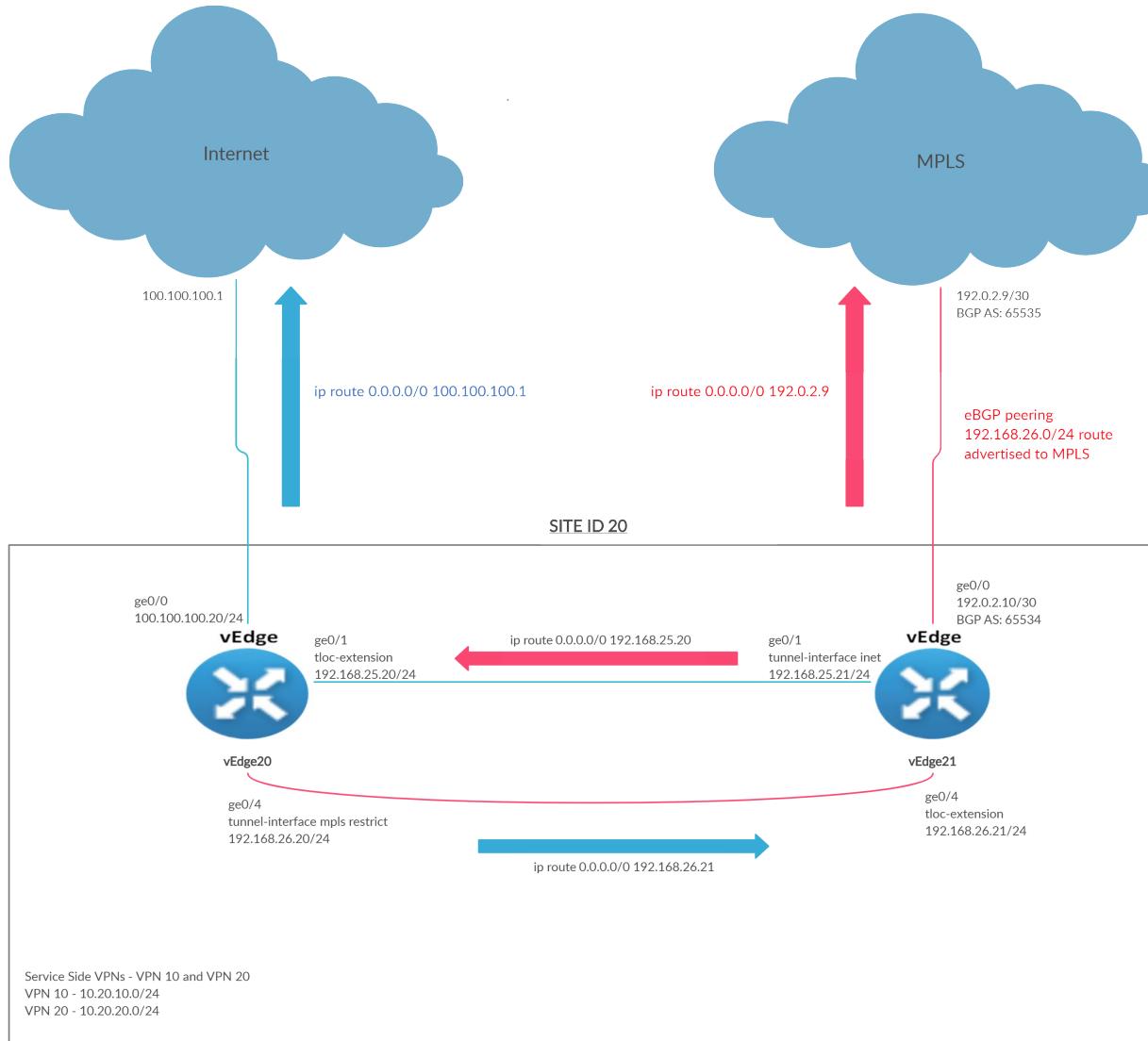
Task List

- Overview
- Feature Templates for TLOC Extensions
 - Creating the VPN Interface Template for the TLOC-EXT interface
 - Creating the VPN Interface Template for the Tunnel interface
 - Creating the BGP Template for the MPLS link
- Updating the VPN and Device Templates
- Activity Verification

Overview

A number of sites have a couple of routers in place, but transport connectivity to just one of the available transports. In the event of a link failure, there is no mechanism for traffic to be redirected over the other transport. That's where TLOC Extensions come in.

TLOC Extensions allow vEdge/cEdge routers with a single transport to utilize the link on another vEdge/cEdge router at the same site. Given below is a graphical representation of what we're trying to achieve in this section of the lab.



vEdge20 is connected to the Internet transport whereas vEdge21 is connected to MPLS. If the Internet link goes down, vEdge20 doesn't have a way to utilize the MPLS link available at vEdge21. TLOC Extensions seek to remedy this.

vEdge/cEdge routers build IPSec tunnels across directly connected transports AND across the transport connected to the neighbouring vEdge/cEdge router to facilitate transport redundancy.

Without TLOC Extensions, the vEdges at Site 20 look something like the images below. Note that both have control connections to the vSmarts and vManage via the directly connected transport, which can be checked using the CLI `show control connections`

```
192.168.0.20 - PuTTY
login as: admin
Pre-authentication banner message from server:
| viptela 20.1.1
|
| End of banner message from server
| admin@192.168.0.20's password:
Last login: Sun May 31 12:06:48 2020 from 192.168.0.121
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on vEdge20
vEdge20# show control connections

          PEER           CONTROLLER           PEER
PEER   PEER PEER      SITE      DOMAIN PEER      PUB
PRIV PEER
GROUP
TYPE   PROT SYSTEM IP ID     ID     PRIVATE IP PORT LOCAL COLOR
PORT  PUBLIC IP
PROXY STATE UPTIME ID
-----vSmart dtls 10.255.255.3 1000    1     100.100.100.4 12446 public-internet
12446 100.100.100.4
No up 12:14:03:53 0
vSmart dtls 10.255.255.4 1000    1     100.100.100.5 12446 public-internet
12446 100.100.100.5
No up 12:14:03:53 0
vmanage dtls 10.255.255.1 1000    0     100.100.100.2 12446 public-internet
12446 100.100.100.2
No up 14:18:11:28 0
vEdge20# vEdge21# show control connections

          PEER           CONTROLLER           PEER
PEER   PEER PEER      SITE      DOMAIN PEER      PUB
PRIV PEER
GROUP
TYPE   PROT SYSTEM IP ID     ID     PRIVATE IP PORT LOCAL COLOR
PORT  PUBLIC IP
PROXY STATE UPTIME ID
-----vSmart dtls 10.255.255.3 1000    1     100.100.100.4 12346 mpls
12346 100.100.100.4
No up 12:14:03:56 0
vSmart dtls 10.255.255.4 1000    1     100.100.100.5 12346 mpls
12346 100.100.100.5
No up 12:14:03:42 0
vmanage dtls 10.255.255.1 1000    0     100.100.100.2 12346 mpls
12346 100.100.100.2
No up 14:18:11:48 0
vEdge21#
```

BFD sessions are established across the directly connected transport as well. Check via the CLI `show bfd sessions`

```
vEdge20# show bfd sess

          SOURCE TLOC      REMOTE TLOC
          DST PUBLIC      DST PUBLIC
DETECT TX
SYSTEM IP SITE ID STATE COLOR      COLOR      SOURC
E IP      IP          PORT      ENCAP
MULTIPLIER INTERVAL(msec) UPTIME      TRANSITIONS
-----10.255.255.11 1 up  public-internet public-internet 100.1
00.100.20 1000 0:14:36:27 0
10.255.255.12 1 up  public-internet public-internet 100.1
00.100.20 1000 0:14:36:28 0
10.255.255.31 30 up  public-internet public-internet 100.1
00.100.20 1000 0:14:41:35 0
10.255.255.41 40 up  public-internet public-internet 100.1
00.100.20 1000 3:18:05:47 7
10.255.255.51 50 up  public-internet public-internet 100.1
00.100.20 1000 3:18:05:47 7
vEdge21# show bfd sess

          SOURCE TLOC      REMOTE TLOC
          DST PUBLIC      DST PUBLIC
DETECT TX
SYSTEM IP SITE ID STATE COLOR      COLOR      SOURC
E IP      IP          PORT      ENCAP
MULTIPLIER INTERVAL(msec) UPTIME      TRANSITIONS
-----10.255.255.11 1 up  mpls      mpls      192.0
2.10 1000 192.0.2.2 12426 ipsec
10.255.255.12 1 up  mpls      mpls      192.0
2.10 1000 192.0.2.6 12426 ipsec
10.255.255.31 30 up  mpls      mpls      192.0
2.10 1000 192.0.2.14 12366 ipsec
10.255.255.41 40 up  mpls      mpls      192.0
2.10 1000 192.1.2.18 12387 ipsec
10.255.255.52 50 up  mpls      mpls      192.0
2.10 1000 192.1.2.22 12347 ipsec
10.255.255.52 50 up  mpls      mpls      192.0
2.10 1000 192.1.2.22 12347 ipsec
10.255.255.52 50 up  mpls      mpls      192.0
2.10 1000 3:18:05:55 7
```

```
show control connections
show bfd sessions
```

Task List

- [Overview](#)
- Feature Templates for TLOC Extensions
 - Creating the VPN Interface Template for the TLOC-EXT interface
 - Creating the VPN Interface Template for the Tunnel interface
 - Creating the BGP Template for the MPLS link
- Updating the VPN and Device Templates
- Activity Verification

Feature Templates for TLOC Extensions

We will need to create a total of three Feature Templates for this section which will be applied to vEdge20 and vEdge21 Device Templates.

Towards the end of the lab, we will copy and modify the VPN 0 feature template used by the INET interface on vEdge20 to allow for NAT. Both vEdges at Site20 use the same feature template for VPN 0 ge0/0 so making a change on one will impact the other as well. Hence, we will be breaking off the vEdge20 VPN Interface template from the one being used. This new template will be identical to the VPN 0 interface template being used at this Site, except for NAT being enabled on ge0/0.

[Creating the VPN Interface Template for the TLOC-EXT interface](#)

1. On the vManage GUI, click on **Configuration => Templates** and go to the **Feature** tab. click on **Add Template** and search for *vedge*. Select *vEdge Cloud* from the list and choose **VPN Interface Ethernet** to create an Interface Template

CONFIGURATION | TEMPLATES

Device Feature **Add Template**

Select Devices
vedge

- vEdge 100
- vEdge 100 B
- vEdge 100 M
- vEdge 100 WM
- vEdge 1000
- vEdge 2000
- vEdge 5000
- vEdge Cloud

| AAA | Archive |
|-------------------------------|------------------------|
| NTP | OMP |
| System | |
| VPN | |
| Secure Internet Gateway (SIG) | VPN |
| WAN | |
| VPN Interface Cellular | VPN Interface Ethernet |
| WAN | Management WAN LAN |
| VPN Interface IPsec | VPN Interface NATPool |
| WAN | WAN |

2. Enter the details as shown in the table below. Use the images for reference. Click on **Save** once done

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|----------------|--|---|
| | Template Name | NA | <i>Site20_TLOC_Ext_NoTunn</i> |
| | Description | NA | <i>Site 20 TLOC Extension Template without Tunnel Configuration</i> |
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | <i>if_name_notunn_tlocext</i> |
| Basic Configuration | IPv4 Address | Device Specific | <i>if_ipv4_address_notunn</i> |
| Advanced | TLOC | Global | ge0/0 |

Extension

Device **Feature**

Feature Template > Add Template > VPN Interface Ethernet

Template Name: Site20_TLOC_Ext_NoTunn
Description: Site 20 TLOC Extension Template without Tunnel Configuration

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: [if_name_notunn_tlocext]

Description:

IPv4 IPv6

Dynamic Static

IPv4 Address: [if_ipv4_address_notunn]

Save Cancel

TLOC Extension

ge0/0

Tracker

ICMP/ICMPv6 Redirect Disable

On Off

GRE tunnel source IP

Save Cancel

This completes configuration of the VPN Interface Template for TLOC Extension interfaces, without a Tunnel. Each participating vEdge/cEdge will have an interface that will not have a Tunnel associated with it (but will have a TLOC Extension association) and another one which will have a Tunnel (but won't have a TLOC Extension associated with it).

Task List

- [Overview](#)
- Feature Templates for TLOC Extensions
 - [Creating the VPN Interface Template for the TLOC-EXT interface](#)
 - [Creating the VPN Interface Template for the Tunnel interface](#)
 - [Creating the BGP Template for the MPLS link](#)
- [Updating the VPN and Device Templates](#)
- [Activity Verification](#)

Creating the VPN Interface Template for the Tunnel interface

1. Navigate to **Configuration => Templates => Feature tab** and search for *tloc*. You should get one template (the one we just created). Click on the three dots next to it and choose **Copy**

The screenshot shows a table of feature templates. The columns are: Name, Description, Type, Device Model, Device Templates, Devices Attached, Updated By, and Last Updated. There is a search bar at the top with 'tloc' entered. A context menu is open over the first row, listing: View, Edit, Change Device Models, Delete, and Copy.

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
|------------------------|---------------------------------|--------------------|--------------|------------------|------------------|------------|-----------------------------|
| Site20_TLOC_Ext_NoTunn | Site 20 TLOC Extension Templ... | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 07 Jun 2020 12:38:09 AM PDT |

2. Rename the Template to *Site20_Tunn_no_tlocext* with a Description of *Site 20 Template with Tunnel Configuration no TLOC-Ext*. Click on **Copy**

Template Copy

Template Name

Description

Site 20Template with Tunnel Configuration no TLOC-Ext

Copy
Cancel

3. Click on the three dots next to the newly created template and choose to **Edit**

| CONFIGURATION TEMPLATES | | | | | | | |
|------------------------------|---------------------------------|----------------------------|--------------|------------------|------------------|------------|-----------------------------|
| Device | Feature | | | | | | |
| Add Template | | Template Type: Non-Default | | Search: tloc | Search Options | | |
| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
| Site20_TLOC_Ext_NoTunn | Site 20 TLOC Extension Templ... | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 07 Jun 2020 12:38:09 AM PDT |
| Site20_Tunn_no_tlocext | Site 20 TLOC Extension Templ... | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 07 Jun 2020 12:39:34 AM PDT |

Total Rows: 2 of 39

View
Edit
 Change Device Models
 Delete
 Copy

4. Update the details as in the table below. Use the images for reference and click on **Update** when done

| Section | Field | Global or Device Specific (drop down) | Value |
|---------------------|----------------|---------------------------------------|-------------------------------|
| Basic Configuration | Shutdown | Global | No |
| Basic Configuration | Interface Name | Device Specific | <i>if_name_tunn_notlocext</i> |

| | | | |
|------------------------|------------------|-----------------|--------------------------------------|
| Basic Configuration | IPv4 Address | Device Specific | <i>if_ipv4_address_tunn</i> |
| Tunnel | Tunnel Interface | Global | On |
| Tunnel | Color | Device Specific | <i>tloc_if_tunnel_color_value</i> |
| Tunnel | Restrict | Device Specific | <i>tloc_if_tunnel_color_restrict</i> |
| Tunnel - Allow Service | All | Global | On |
| Advanced | TLOC Extension | Default | |

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > VPN Interface Ethernet

Device Type vEdge Cloud

Template Name Site20_Tunn_no_tlocext

Description Site 20 Template with Tunnel Configuration no TLOC-Ext

This feature template is shared by both Cisco vEdge and IOS-XE SDWAN devices. Please use the [Template Migration tool](#) to migrate to IOS-XE SDWAN feature templates.

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

BASIC CONFIGURATION

Shutdown Yes No

Interface Name [if_name_tunn_notlocext]

Description

IPv4 **IPv6**

Dynamic Static

IPv4 Address [if_ipv4_address_tunn]

TUNNEL

Tunnel Interface On Off

Per-tunnel Qos On Off

Color [tloc_if_tunnel_color_value]

Restrict On Off [tloc_if_tunnel_color_restrict]

Groups

Border On Off

Control Connection On Off

Autonegotiation On Off

TLOC Extension ge0/0

Tracker

ICMP/ICMPv6 Redirect Disable On Off

GRE tunnel source IP

Make sure you allow service all in the configuration above

Update **Cancel**

This completes the configuration of our second feature template.

Task List

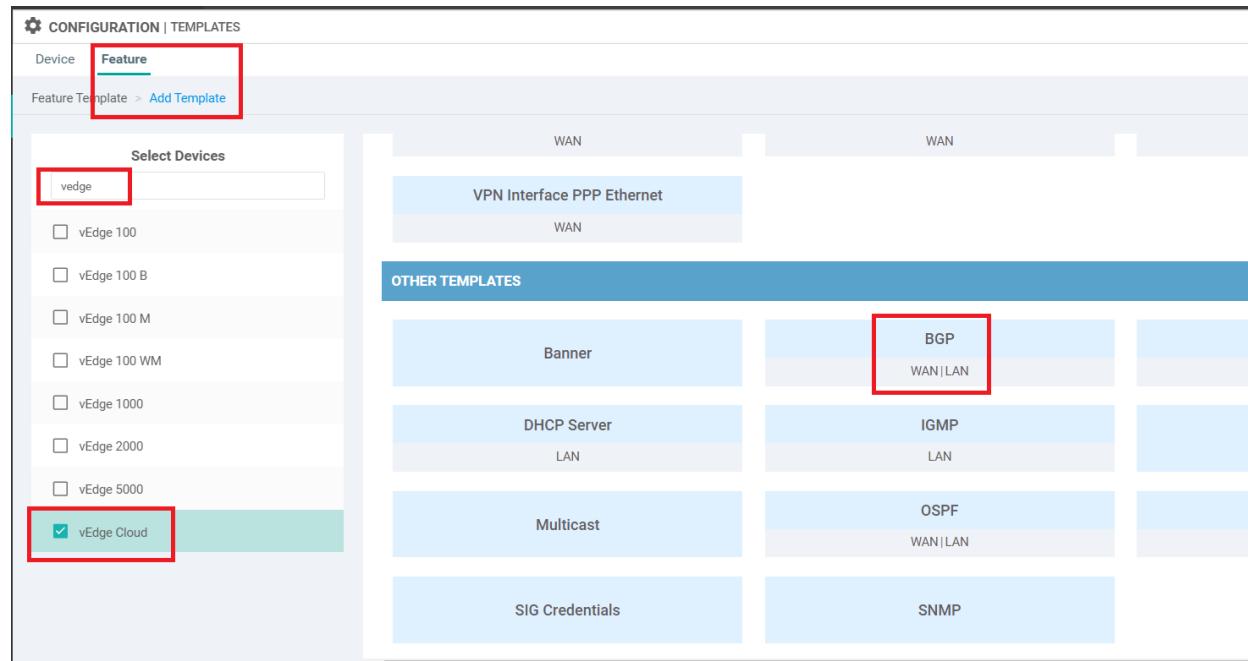
- [Overview](#)
- [Feature Templates for TLOC Extensions](#)
 - [Creating the VPN Interface Template for the TLOC-EXT interface](#)
 - [Creating the VPN Interface Template for the Tunnel interface](#)

- Creating the BGP Template for the MPLS link
- Updating the VPN and Device Templates
- Activity Verification

Creating the BGP Template for the MPLS link

We will now set up the BGP template for eBGP peering on the MPLS link. This is so that the TLOC extension subnet (192.168.26.0/24 in this case) can be advertised to the MPLS network.

1. On the vManage GUI, go to **Configuration => Templates => Feature tab**. Click on **Add Template** and search for **vedge**. Select **vEdge Cloud** and scroll down to the Other Templates section. Choose **BGP**



2. Enter the Template Name as `vedge21_mpls_bgp_tloc` and the Description as *BGP Peering Template for TLOC Extension on the MPLS link*. Set **Shutdown** to a Device Specific variable of `bgp_shutdown`. Set AS Number to a global value of 65534. This will be the AS number on our vEdge21 for BGP Peering

The screenshot shows the 'Configuration | Templates' interface. Under the 'Feature' tab, a 'BGP' template is selected. The template name is 'vedge21_mpls_bgp_tloc' and its description is 'BGP Peering Template for TLOC Extension on the MPLS link'. The 'Basic Configuration' tab is active, displaying fields for Shutdown (with a dropdown menu and a red box around it), AS Number (with a dropdown menu and a red box around it), Router ID (with a dropdown menu), and Propagate AS Path (with a dropdown menu and radio buttons for On and Off).

3. Under **Unicast Address Family**, set the Maximum Paths to 2. Click on the **Network** tab and click on **New Network**. Enter the **Network Prefix** as a global value of **192.168.26.0/24** and click on **Add**. This is the subnet which will be advertised in BGP.

The screenshot shows the 'Unicast Address Family' tab under 'Basic Configuration'. It has tabs for IPv4 and IPv6. Under 'IPv4', the 'Maximum Paths' field is set to 2. The 'RE-DISTRIBUTE' section has a 'NETWORK' button highlighted with a red box. Below it, a 'New Network' button is also highlighted with a red box. In the 'Network Prefix' section, the value '192.168.26.0/24' is entered in the input field, which is also highlighted with a red box. An 'Add' button at the bottom right is also highlighted with a red box.

4. Under **Neighbor**, click on **New Neighbor** and enter details as per the table below. Click on **Add** (don't miss this - far right corner) to Add the Neighbor details and then click on **Save** (bottom-middle of the screen) to Save this template

| Section | Field | Global or Device Specific (drop down) | Value |
|----------|----------------|---------------------------------------|--------------|
| Neighbor | Address | Global | 192.0.2.9 |
| Neighbor | Remote AS | Global | 65535 |
| Neighbor | Address Family | Global | On |
| Neighbor | Address Family | Global | ipv4-unicast |

Tip: We are setting many of the fields to Global values since this is a lab environment. In production, it is recommended to set certain fields as Device Specific variables so that the templates can be re-used as and when required, for disparate device configurations. The best case scenario is to have as much common configuration between devices/sites as is possible (global values) and then create Device Specific variables for the uncommon parameters.

NEIGHBOR

IPv4 IPv6

+ New Neighbor

Address: 192.0.2.9

Description: (dropdown)

Remote AS: 65535

Address Family: On (radio button selected)

Address Family: ipv4-unicast (dropdown menu)

Maximum Number of Prefixes: (dropdown)

Route Policy In: (dropdown)

Click Add once all these parameters are configured to save the changes.

This completes the configuration of our BGP Template.

Task List

- [Overview](#)

- Feature Templates for TLOC Extensions
 - Creating the VPN Interface Template for the TLOC-EXT interface
 - Creating the VPN Interface Template for the Tunnel interface
 - Creating the BGP Template for the MPLS link
- Updating the VPN and Device Templates
- Activity Verification

Updating the VPN and Device Templates

We will start by updating the existing VPN template for Site 20 (named *Site20-vpn0*) to include a default route with a next hop to the corresponding TLOC Extension interface (i.e. to 192.168.26.21 on vEdge20 and 192.168.25.20 on vEdge21). Device Specific variables will be used.

1. Navigate to **Configuration => Templates => Feature tab** on the vManage GUI. Search for *site20* and you should see the *Site20-vpn0* template. Click on the three dots next to it and choose to **Edit**

The screenshot shows the vManage Feature tab interface. The search bar contains 'site20'. A table lists four templates: 'Site20-vpn0' (selected), 'Site20_Tunn_no_tlocext', 'Site20_vpn0_int', and 'Site20_TLOC_Ext_NoTunn'. The 'Site20-vpn0' row has a red box around its name. A context menu is open over the row, with 'Edit' highlighted and a red box around it. Other options in the menu include 'View', 'Change Device Models', 'Delete', and 'Copy'. The top navigation bar has 'Feature' selected, and the bottom right corner shows 'Total Rows: 4 of 40'.

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
|------------------------|----------------------------------|--------------------|--------------|------------------|------------------|------------|----------------------------|
| Site20-vpn0 | VPN0 for the Site20 vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 5:41:03 AM PDT |
| Site20_Tunn_no_tlocext | Site 20 TLOC Extension Templ... | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 07 Jun 2020 |
| Site20_vpn0_int | VPN0 Interface for Site20 dev... | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 |
| Site20_TLOC_Ext_NoTunn | Site 20 TLOC Extension Templ... | WAN Edge Interface | vEdge Cloud | 0 | 0 | admin | 07 Jun 2020 |

2. Scroll down to the **IPv4 Route** section and click on the pencil icon next to **0.0.0.0/0** route to edit it

The screenshot shows the vManage IPv4 Route section. A table lists routes. The first row, '0.0.0.0/0' (Gateway: Next Hop), has an edit icon (pencil) in the 'Action' column highlighted with a red box.

| Optional | Prefix | Gateway | Selected Gateway Configuration | Action |
|--------------------------|-----------|----------|--------------------------------|--------|
| <input type="checkbox"/> | 0.0.0.0/0 | Next Hop | 1 | |

3. Click on **1 Next Hop** in the **Update IPv4 Route** popup

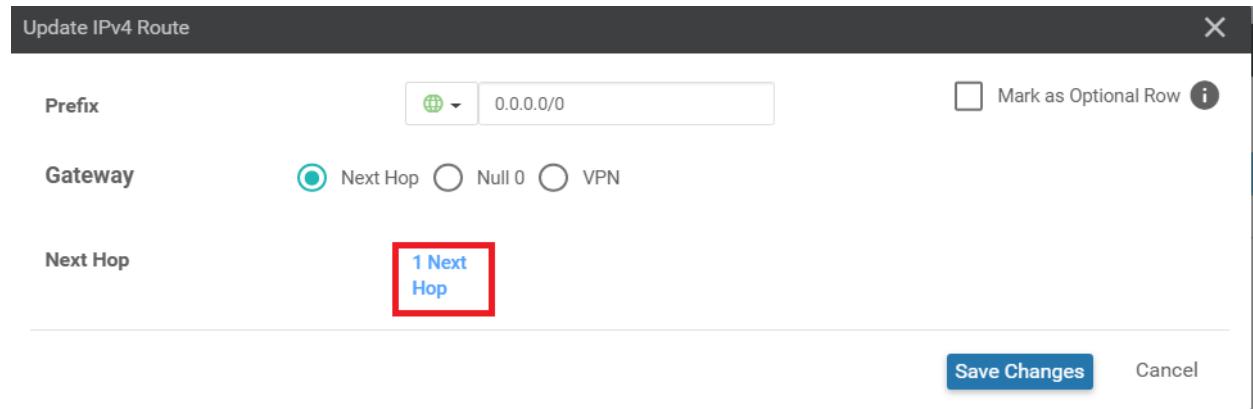
Update IPv4 Route

Prefix Mark as Optional Row i

Gateway Next Hop Null 0 VPN

Next Hop 1 Next Hop

Save Changes Cancel

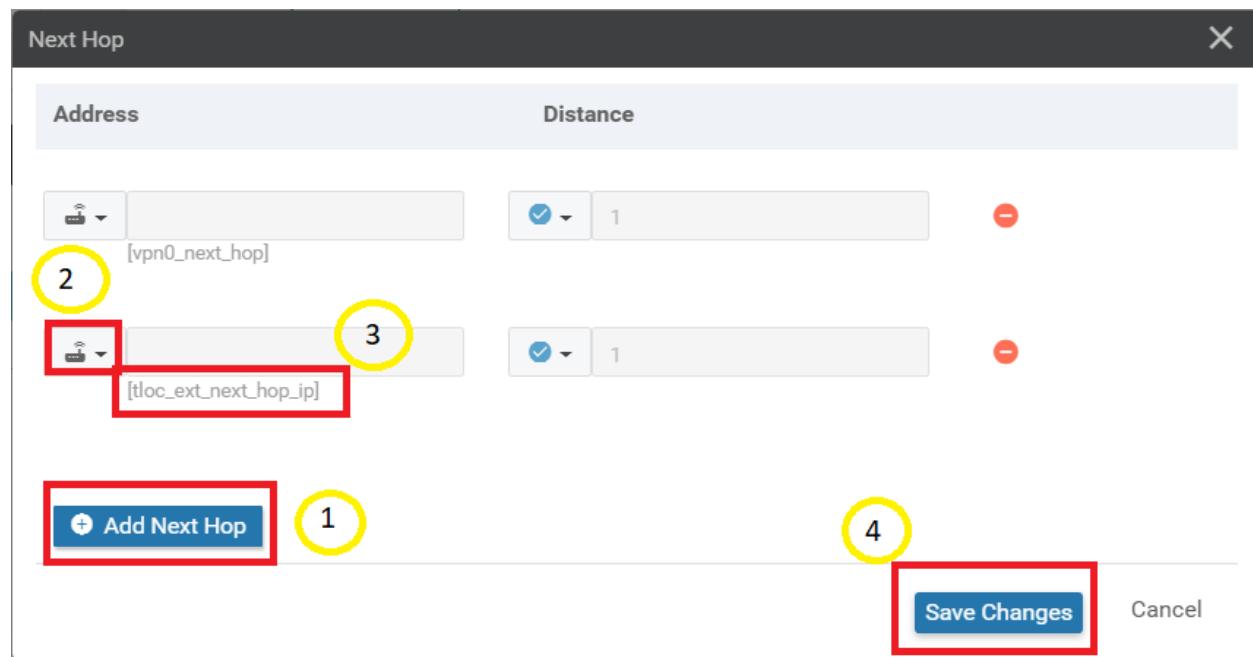


4. Click on **Add Next Hop** and set the new hop address to **Device Specific** with a name of `tloc_ext_next_hop_ip`. Click on **Save Changes**

Next Hop

| Address | Distance |
|---|----------------------------------|
| <input type="text" value="vpn0_next_hop"/> 2 | <input type="text" value="1"/> - |
| <input type="text" value="tloc_ext_next_hop_ip"/> 3 | <input type="text" value="1"/> - |

Add Next Hop 1 Save Changes Cancel



5. Click on **Save Changes** again, making sure that the Update IPv4 Routes field now shows **2 Next Hop**

Update IPv4 Route

| | | |
|----------|--|---|
| Prefix | <input type="text" value="0.0.0.0/0"/> <input type="button" value=""/> | <input type="checkbox"/> Mark as Optional Row |
| Gateway | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN | |
| Next Hop | 2 Next Hop | |
| | | <input type="button" value="Save Changes"/> <input type="button" value="Cancel"/> |

6. Back at the VPN Feature template, make sure that the number 2 shows up under Selected Gateway Configuration and click on **Update**

| IPv4 ROUTE | | | |
|--|--|--|--|
| <input type="button" value="New IPv4 Route"/> Optional <input type="checkbox"/> Prefix <input type="text" value="0.0.0.0/0"/> Gateway <input type="radio"/> Next Hop Selected Gateway Configuration 2 | | | |

| IPv6 ROUTE | | | |
|---|--|--|--|
| <input type="button" value="New IPv6 Route"/> Optional <input type="checkbox"/> Prefix Gateway Selected Gateway Configuration <input type="button" value="Update"/> <input type="button" value="Cancel"/> | | | |

7. Populate the details for the Address (tloc_ext_next_hop_ip) for the two vEdges. vEdge20 should have 192.168.26.21 and vEdge21 should have 192.168.25.20 as the next hop IP. Click on **Next**

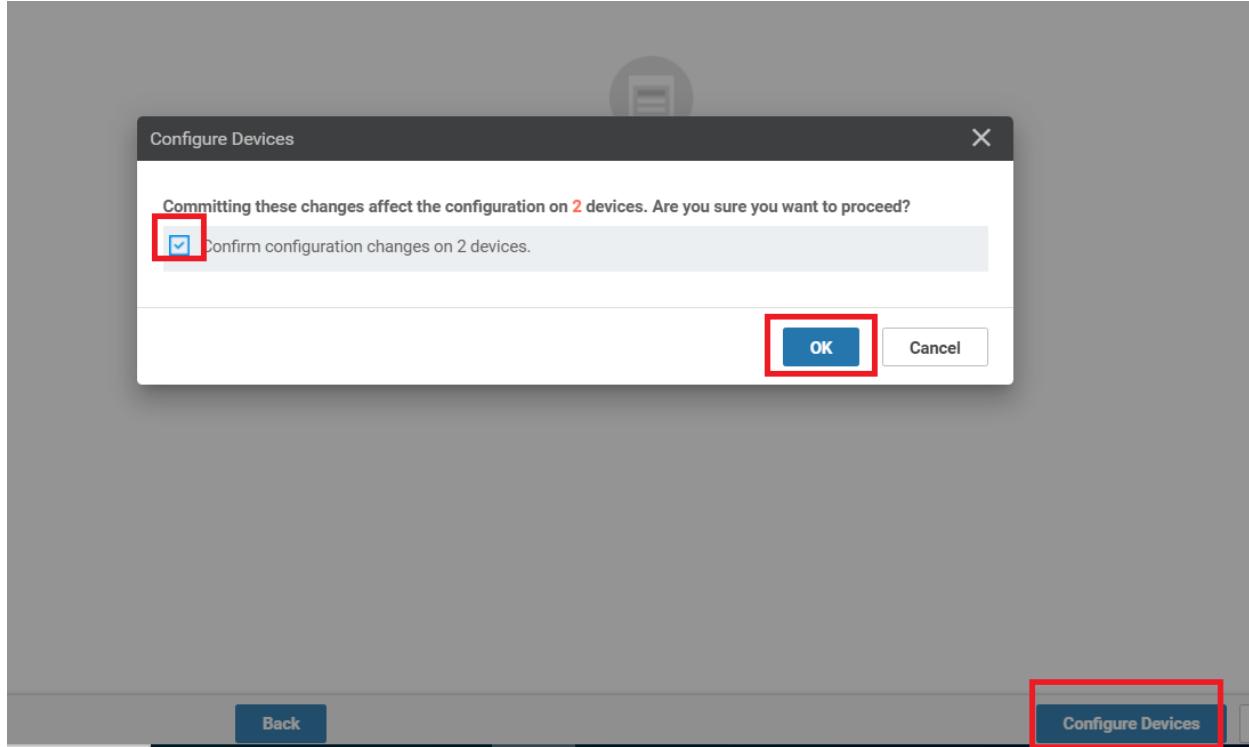
Search Options ▾

| S... | Chassis Number | System IP | Hostname | ress(vpn512_mgmt_if_ip_addr) | Address(vpn0_next_hop) | Address(tloc_ext, next_hop_ip) | Ir... |
|-------------------------------------|--------------------------------------|---------------|----------|------------------------------|------------------------|--------------------------------|-------|
| <input checked="" type="checkbox"/> | b7fd7295-58df-7671-e914-6fe2edff1609 | 10.255.255.21 | vEdge20 | 20/24 | 100.100.100.1 | 192.168.26.21 | gr... |
| <input checked="" type="checkbox"/> | dde90ff0-dc62-77e6-510f-08d96608537d | 10.255.255.22 | vEdge21 | 21/24 | 192.0.2.9 | 192.168.25.20 | gr... |

Enter these details then click Next

Next Cancel

8. You can view the side by side configuration if needed, and click on **Configure Devices**. Choose the confirm the changes and click on **OK**



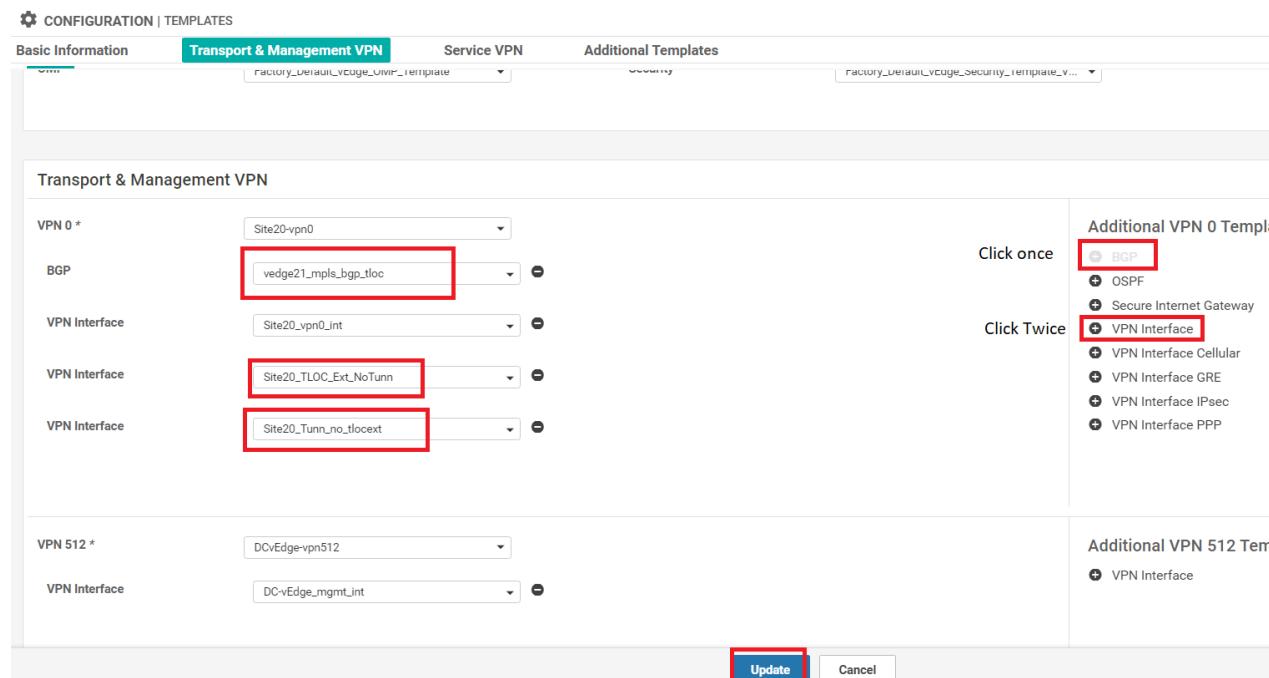
9. To edit the Device Template and bring everything together, navigate to **Configuration => Templates** on the vManage GUI. Make sure you're on the Device tab and locate the *vedge_Site20_dev_temp* template. Click on the three dots next to it and choose to **Edit**

A screenshot of the 'Device Templates' list in vManage. The 'Device' tab is selected. A 'Create Template' button is at the top left. The table has columns: Name, Description, Type, Device Model, Feature Templates, Devices Attached, Updated By, Last Updated, and Template Status. A search bar and options for 'Search Options' and filters are at the top right. A total of 6 rows are shown. The row for 'vEdge_Site20_dev_temp' is highlighted with a yellow background and has a red box around its '...' button. A context menu is open over this row, with 'Edit' highlighted by a red box. Other options in the menu include View, Delete, Copy, Attach Devices, Detach Devices, Export CSV, and Change Device Values.

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status |
|--------------------------|------------------------------|---------|--------------|-------------------|------------------|------------|----------------------------|-----------------|
| DCvEdge_dev_temp | Device template for the D... | Feature | vEdge Cloud | 16 | 2 | admin | 28 May 2020 4:58:07 AM ... | In Sync |
| cEdge-single-uplink | Single Uplink cEdge Devi... | Feature | CSR1000v | 17 | 2 | admin | 26 May 2020 3:05:01 AM ... | In Sync |
| vEdge_Site20_dev_temp | Device template for the S... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 PM ... | In Sync |
| vSmart-dev-temp | Device Template for vSm... | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 A... | In Sync |
| vEdge30_dev_temp | Device template for the S... | Feature | vEdge Cloud | 15 | 1 | admin | 05 Jun 2020 9:57:40 PM ... | In Sync |
| cEdge_dualuplink_devtemp | cEdge Device Template f... | Feature | CSR1000v | 20 | 1 | admin | 06 Jun 2020 3:48:59 AM ... | In Sync |

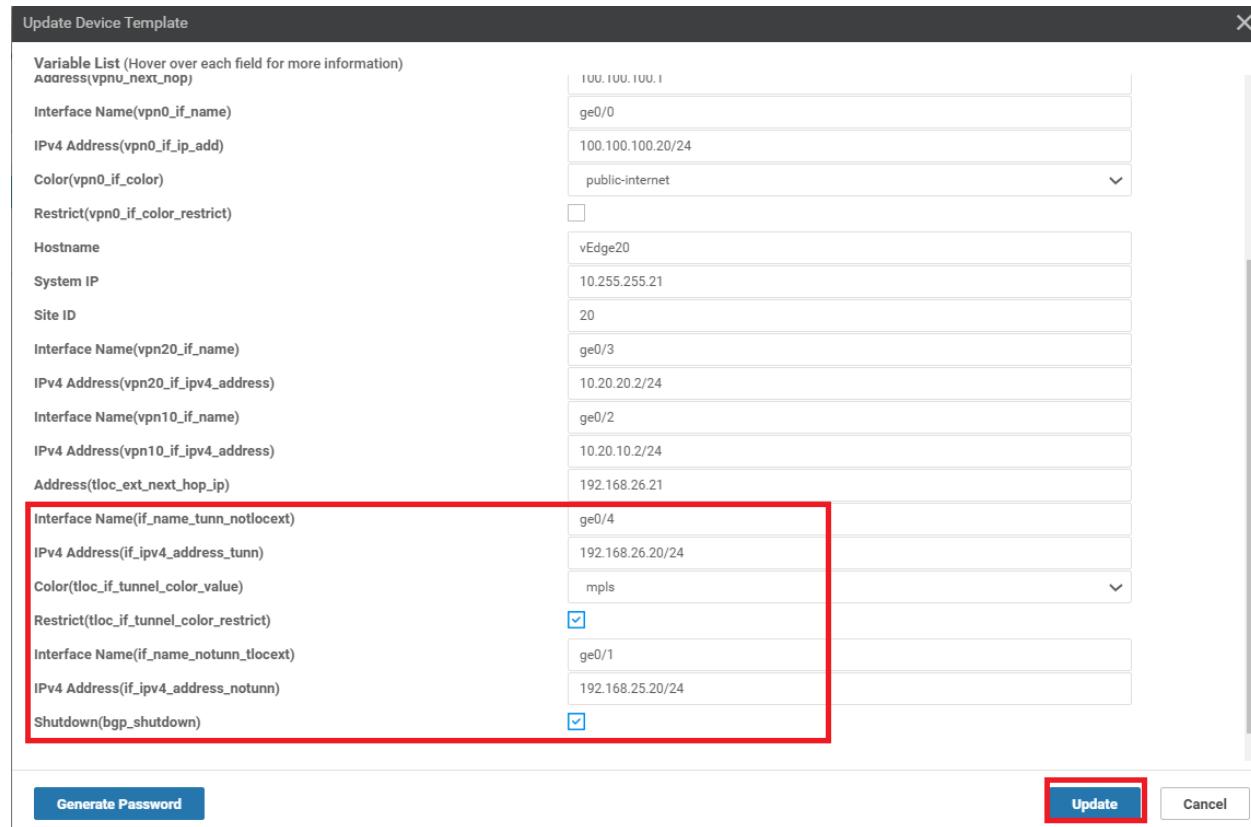
10. Under **Transport & Management VPN**, click on **BGP** under Additional VPN 0 Templates. Click on **VPN Interface** twice to add two VPN Interfaces over on the left-hand side. Populate the BGP template we created in the BGP field

(named *vedge21_mpls_bgp_tloc*). Populate *Site20_TLOC_Ext_NoTunn* under the first VPN Interface and *Site20_Tunn_no_tlocext* under the second VPN Interface. Click on **Update**



11. Click on the three dots next to vEdge20 and choose **Edit Device Template**. Enter the details as shown in the table below, referencing the image and click on **Update**

| Field | Value |
|--|------------------|
| Interface Name (if_name_tunn_notlocext) | ge0/4 |
| IPv4 Address (if_ipv4_address_tunn) | 192.168.26.20/24 |
| Color (tloc_if_tunnel_color_value) | mpls |
| Restrict (tloc_if_tunnel_color_restrict) | Checked |
| Interface Name (if_name_notunn_tlocext) | ge0/1 |
| IPv4 Address (if_ipv4_address_notunn) | 192.168.25.20/24 |
| Shutdown (bgp_shutdown) | Checked |



12. Click on the three dots next to vEdge21 and choose **Edit Device Template**. Enter the details as shown in the table below, referencing the image and click on **Update** and then click on **Next**

| Field | Value |
|--|------------------|
| Interface Name (if_name_tunn_notlocext) | ge0/1 |
| IPv4 Address (if_ipv4_address_tunn) | 192.168.25.21/24 |
| Color (tloc_if_tunnel_color_value) | public-internet |
| Restrict (tloc_if_tunnel_color_restrict) | Unchecked |
| Interface Name (if_name_notunn_tlocext) | ge0/4 |
| IPv4 Address (if_ipv4_address_notunn) | 192.168.26.21/24 |
| Shutdown (bgp_shutdown) | Unchecked |

Update Device Template

Variable List (Hover over each field for more information)

| | |
|---|-------------------------------------|
| Address(vpn0_if_ip_address) | 192.0.2.9 |
| Interface Name(vpn0_if_name) | ge0/0 |
| IPv4 Address(vpn0_if_ip_address) | 192.0.2.10/30 |
| Color(vpn0_if_color) | mpls |
| Restrict(vpn0_if_color_restrict) | <input checked="" type="checkbox"/> |
| Hostname | vEdge21 |
| System IP | 10.255.255.22 |
| Site ID | 20 |
| Interface Name(vpn20_if_name) | ge0/3 |
| IPv4 Address(vpn20_if_ipv4_address) | 10.20.20.3/24 |
| Interface Name(vpn10_if_name) | ge0/2 |
| IPv4 Address(vpn10_if_ipv4_address) | 10.20.10.3/24 |
| Address(tloc_ext_next_hop_ip) | 192.168.25.20 |
| Interface Name(if_name_tunn_notlocext) | ge0/1 |
| IPv4 Address(if_ipv4_address_tunn) | 192.168.25.21/24 |
| Color(tloc_if_tunnel_color_value) | public-internet |
| Restrict(tloc_if_tunnel_color_restrict) | <input type="checkbox"/> |
| Interface Name(if_name_notunn_tlocext) | ge0/4 |
| IPv4 Address(if_ipv4_address_notunn) | 192.168.26.21/24 |
| Shutdown(bgp_shutdown) | <input type="checkbox"/> |

Generate Password **Update** **Cancel**

13. View the side-by-side configuration (optional) and click on **Configure Devices**. Confirm the configuration change on 2 devices

'Configure' action will be applied to 2 device(s)
attached to 1 device template(s). X

```

87    tunnel-interface
88      encapsulation ipsec
89      color public-internet
90      allow-service all
91      no allow-service bgp
92      allow-service dhcp
93      allow-service dns
94      allow-service icmp
95      no allow-service sshd
96      no allow-service netconf
97      no allow-service ntp
98      no allow-service ospf
99      no allow-service stun
100     allow-service https
101   !
102   no shutdown
103   !
104   interface ge0/4
105     ip address 192.168.26.21/24
106     tloc-extension ge0/0

68   no shutdown
69   !
70   ip route 0.0.0.0/0 192.0.2.9
71   ip route 0.0.0.0/0 192.168.25.20
72   !
73   vpn 10
74     dns 10.2.1.5 primary
75     dns 10.2.1.6 secondary
76     interface ge0/2
77       ip address 10.20.10.3/24
107  no shutdown
108  !
109  ip route 0.0.0.0/0 192.0.2.9
110  ip route 0.0.0.0/0 192.168.25.20
111  !
112  vpn 10
113  dns 10.2.1.5 primary
114  dns 10.2.1.6 secondary
115  interface ge0/2
116  ip address 10.20.10.3/24

```

Configure Devices Cancel

Tip: It's important to make another change to the Internet transport so that our TLOC Extension configuration works as expected. We need to enable NAT on the VPN Interface associated with the Internet link. Unfortunately, NAT can't be enabled/disabled via Device Specific parameters so we will need to copy the VPN Interface template, tweak it and then copy the Device Template to reference the new VPN Interface template. We will then attach vEdge20 to this template.

- From the vManage GUI, navigate to **Configuration => Templates**. On the Feature tab, search for *vpn0*. Locate the *site20_vpn0_int* template and make a copy of it, renaming to *site20_vpn0_int_nat* and updating the description accordingly

Device Feature

Add Template

Template Type Non-Default Search Options

Total Rows: 13 of 41

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | ... |
|--------------------------|----------------------------------|---------------------|--------------|------------------|------------------|------------|-----------------------------|-----|
| cEdge-vpn0-int-single | cEdge VPN 0 Interface Temp... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| vEdge30-vpn0 | VPN0 for the Site30 INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:25:48 AM PDT | ... |
| Site20_vpn0_int_nat | NAT | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 07 Jun 2020 2:49:54 AM PDT | ... |
| Site20_vpn0_int | Interface for Site20 devi... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 07 Jun 2020 2:46:50 AM PDT | ... |
| cEdge_VPN0_dual_L3 | VPN0 Template for Du... | Cisco VPN | CSR1000v | 1 | 1 | admin | 23 May 2020 7:34:59 AM PDT | ... |
| cEdge-vpn0-int-dual_mpls | cEdge VPN 0 Interface Temp... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 05 Jun 2020 11:26:42 PM PDT | ... |

15. Click on the three dots next to the new `site20_vpn0_int_nat` template and choose to **Edit**. Set NAT to a global value of On and click on **Update**

NAT

Edit the newly copied template and enable NAT. Click Update.

NAT On Off

Refresh Mode outbound

Log NAT flow creations or deletions On Off

UDP Timeout 1

TCP Timeout 60

Block ICMP On Off

Respond To Ping On Off

Update **Cancel**

16. Make sure you're on the **Configuration => Templates** Device tab and locate the `vEdge_Site20_dev_temp` template. Make a copy of it, renaming to `vEdge_Site20_dev_temp_nat` and updating the description accordingly

Template Type Non-Default Search Options

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | ... |
|---------------------------|----------------------------|---------|--------------|-------------------|------------------|------------|--------------------------|-----------------|-----|
| DCvEdge_dev_temp | Device template for the... | Feature | vEdge Cloud | 16 | 2 | admin | 28 May 2020 4:58:07 A... | In Sync | ... |
| cEdge-single-uplink | Single Uplink vEdge De... | Feature | CSR1000v | 17 | 2 | admin | 26 May 2020 3:05:01 A... | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the... | Feature | vEdge Cloud | 17 | 1 | admin | 07 Jun 2020 1:15:59 A... | In Sync | ... |
| vEdge_Site20_dev_temp_nat | Renamed template | Cloud | vEdge Cloud | 17 | 1 | admin | 07 Jun 2020 2:50:41 A... | In Sync | ... |

17. Choose to **Edit** the newly created `vEdge_Site20_dev_temp_nat` via the three dots next to it and update the VPN Interface field under **Transport & Management VPN** to reflect the VPN Interface template we created in step 14/15. The name of the newly created VPN Interface template is `site20_vpn0_int_nat`. Click on **Update**

CONFIGURATION | TEMPLATES

Basic Information Transport & Management VPN Service VPN Additional Templates

factory_Default_vEdge_VinIP_Template factory_Default_vEdge_Sec

Transport & Management VPN

VPN 0 * Site20-vpn0

BGP vedge21_mpls_bgp_tloc

VPN Interface Site20_vpn0_int_nat

VPN Interface Site20_TLOC_Ext_NoTunn

VPN Interface Site20_Tunn_no_tlocext

Change the VPN Interface to reflect the NAT enabled interface template. Click on Update and attach vEdge20.

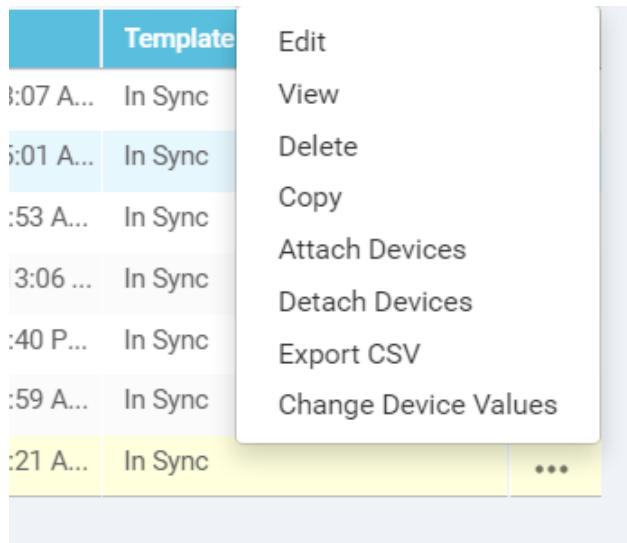
VPN 512 * DCvEdge-vpn512

VPN Interface DC-vEdge_mgmt_int

Update Cancel

18. Click on the three dots next to the *vEdge_Site20_dev_temp_nat* device template and click on **Attach**. Choose the vEdge20 device and Attach it. Click Next/Configure Device as the prompts pop up (nothing will need to be populated since we're using a device template copied from before with NAT set to On)

⚠ Important: Wait for the template to attach. If it gives an error/failure then the templates will go out of sync. To resync, click on the three dots next to *vEdge_Site20_dev_temp* and choose **Change Device Values**. Hit Next and Configure Devices. Now try step 18 above again.



This completes the configuration of TLOC Extensions at Site 20.

Task List

- [Overview](#)
- [Feature Templates for TLOC Extensions](#)
 - [Creating the VPN Interface Template for the TLOC-EXT interface](#)
 - [Creating the VPN Interface Template for the Tunnel interface](#)
 - [Creating the BGP Template for the MPLS link](#)
- [Updating the VPN and Device Templates](#)
- [Activity Verification](#)

Activity Verification

1. To verify that our configuration is working, log in to the CLI of vEdge20 and vEdge21. Issue the same commands as before and compare with the output we had taken at the start of this section ([click here](#) to compare the output).

Output of `show control connections` and `show bfd sessions` given below

| vEdge20# show control connections | | | | | | | |
|-----------------------------------|------------|--------------|------------|--------|---------------|---------------------|--------------------------|
| PEER | PEER | PEER | CONTROLLER | | PEER | | PEER |
| | | | SITE | DOMAIN | PEER | PRIV | |
| TYPE | PROT | SYSTEM | IP | ID | ID | PRIVATE IP | PORT |
| OXY | STATE | UPTIME | ID | | | | PORT |
| vsmart | dtls | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12446 100.100.100.4 | 12446 public-internet No |
| up | 0:00:01:00 | 0 | | | | | |
| vsmart | dtls | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12446 100.100.100.5 | 12446 public-internet No |
| up | 0:00:01:00 | 0 | | | | | |
| vsmart | dtls | 10.255.255.3 | 1000 | 1 | 100.100.100.4 | 12446 100.100.100.4 | 12446 mpls No |
| up | 0:00:00:57 | 0 | | | | | |
| vsmart | dtls | 10.255.255.4 | 1000 | 1 | 100.100.100.5 | 12446 100.100.100.5 | 12446 mpls No |
| up | 0:00:00:57 | 0 | | | | | |
| vmanage | dtls | 10.255.255.1 | 1000 | 0 | 100.100.100.2 | 12446 100.100.100.2 | 12446 public-internet No |
| up | 0:00:01:15 | 0 | | | | | |

| vEdge20# vEdge20# show bfd sess | | | | | | | | | | | | |
|---------------------------------|-----------------|-------------|-----------------|-------------|-----------------|----------------|----------------|-------|-----------|------|-------|--------|
| TECT | TX | SOURCE TLOC | | REMOTE TLOC | | DST PUBLIC | | | | | | |
| | | SYSTEM | IP | SITE | ID | STATE | COLOR | COLOR | SOURCE IP | IP | DST | PUBLIC |
| LTIPLIER | INTERVAL(mssec) | UPTIME | | | | | | | | PORT | ENCAP | MU |
| 10.255.255.11 | 1 | up | public-internet | 1 | public-internet | 100.100.100.20 | 100.100.100.10 | 2936 | ipsec | 7 | | |
| 1000 | | 0:00:03:28 | | | | | | | | | | |
| 10.255.255.11 | 1 | up | mpls | 1 | mpls | 192.168.26.20 | 192.0.2.2 | 12426 | ipsec | 7 | | |
| 1000 | | 0:00:03:14 | | | | | | | | | | |
| 10.255.255.12 | 1 | up | public-internet | 1 | public-internet | 100.100.100.20 | 100.100.100.11 | 22184 | ipsec | 7 | | |
| 1000 | | 0:00:03:28 | | | | | | | | | | |
| 10.255.255.12 | 1 | up | mpls | 1 | mpls | 192.168.26.20 | 192.0.2.6 | 12426 | ipsec | 7 | | |
| 1000 | | 0:00:03:13 | | | | | | | | | | |
| 10.255.255.31 | 30 | up | public-internet | 1 | public-internet | 100.100.100.20 | 100.100.100.30 | 50308 | ipsec | 7 | | |
| 1000 | | 0:00:03:29 | | | | | | | | | | |
| 10.255.255.31 | 30 | up | mpls | 1 | mpls | 192.168.26.20 | 192.0.2.14 | 12366 | ipsec | 7 | | |
| 1000 | | 0:00:03:13 | | | | | | | | | | |
| 10.255.255.41 | 40 | up | public-internet | 1 | public-internet | 100.100.100.20 | 100.100.100.40 | 12347 | ipsec | 7 | | |
| 1000 | | 0:00:03:28 | | | | | | | | | | |
| 10.255.255.41 | 40 | up | mpls | 8 | mpls | 192.168.26.20 | 192.1.2.18 | 12387 | ipsec | 7 | | |
| 1000 | | 0:00:03:13 | | | | | | | | | | |
| 10.255.255.51 | 50 | up | public-internet | 1 | public-internet | 100.100.100.20 | 100.100.100.50 | 12347 | ipsec | 7 | | |
| 1000 | | 0:00:03:28 | | | | | | | | | | |
| 10.255.255.52 | 50 | up | mpls | 8 | mpls | 192.168.26.20 | 192.1.2.22 | 12347 | ipsec | 7 | | |
| 1000 | | 0:00:03:13 | | | | | | | | | | |

Note: If you get output that looks like the image below for vEdge20 (i.e. there are 3 mpls TLOC control connections and 2 public-internet connections, issue a `clear control connections`, wait for a couple of minutes and run `show control connections` again. The output should match with what we see above.

| vEdge20# show control connections | | | | | | | |
|-----------------------------------|------------|--------------|------------|--------|---------------|---------------------|-----------------------|
| PEER | PEER | PEER | CONTROLLER | | PEER | | PEER |
| | | | SITE | DOMAIN | PEER | PRIV | |
| TYPE | PROT | SYSTEM | IP | ID | ID | PRIVATE IP | PORT |
| OXY | STATE | UPTIME | ID | | | | PORT |
| vsmart | dtls | 10.255.255.3 | 100 | 1 | 100.100.100.4 | 12446 100.100.100.4 | 12446 public-internet |
| up | 0:00:16:09 | 0 | | | | | |
| vsmart | dtls | 10.255.255.4 | 100 | 1 | 100.100.100.5 | 12446 100.100.100.5 | 12446 public-internet |
| up | 0:00:16:09 | 0 | | | | | |
| vsmart | dtls | 10.255.255.3 | 100 | 1 | 100.100.100.4 | 12446 100.100.100.4 | 12446 mpls |
| up | 0:01:57:47 | 0 | | | | | |
| vsmart | dtls | 10.255.255.4 | 100 | 1 | 100.100.100.5 | 12446 100.100.100.5 | 12446 mpls |
| up | 0:01:57:47 | 0 | | | | | |
| vmanage | dtls | 10.255.255.1 | 1000 | 0 | 100.100.100.2 | 12846 100.100.100.2 | 12846 mpls |
| up | 0:01:47:14 | 0 | | | | | |

Issued `clear control connections`

| PEER | PEER | CONTROLLER | | | PEER | | | PEER | | | |
|---------|-------------------|------------|------|--------------|---------------|----|-------|---------------|-------|-----------------|------|
| | | SITE | | GROUP | DOMAIN PEER | | PRIV | PEER | PUB | | |
| | | TYPE | PROT | | SYSTEM IP | ID | | | PORT | PUBLIC IP | PORT |
| vsmart | dtls 10.255.255.3 | 100 | 1 | 0:00:02:01 0 | 100.100.100.4 | | 12446 | 100.100.100.4 | 12446 | public-internet | |
| vsmart | dtls 10.255.255.4 | 100 | 1 | 0:00:01:44 0 | 100.100.100.5 | | 12446 | 100.100.100.5 | 12446 | public-internet | |
| vsmart | dtls 10.255.255.3 | 100 | 1 | 0:00:01:44 0 | 100.100.100.4 | | 12446 | 100.100.100.4 | 12446 | mpls | |
| vsmart | dtls 10.255.255.4 | 100 | 1 | 0:00:01:44 0 | 100.100.100.5 | | 12446 | 100.100.100.5 | 12446 | mpls | |
| vmanage | dtls 10.255.255.1 | 1000 | 0 | 0:00:02:01 0 | 100.100.100.2 | | 12846 | 100.100.100.2 | 12846 | public-internet | |

2. Similarly, log in to vEdge21 and compare the output of the same commands ([click here](#) to compare the output).

Commands are again `show control connections` and `show bfd sessions`

| PEER | PEER | CONTROLLER | | | PEER | | | PEER | | | |
|---------|-------------------|------------|------|--------------|---------------|----|-------|---------------|-------|-----------------|------|
| | | SITE | | GROUP | DOMAIN PEER | | PRIV | PEER | PUB | | |
| | | TYPE | PROT | | SYSTEM IP | ID | | | PORT | PUBLIC IP | PORT |
| vsmart | dtls 10.255.255.3 | 1000 | 1 | 0:00:01:30 0 | 100.100.100.4 | | 12346 | 100.100.100.4 | 12346 | mpls | No |
| vsmart | dtls 10.255.255.4 | 1000 | 1 | 0:00:01:30 0 | 100.100.100.5 | | 12346 | 100.100.100.5 | 12346 | mpls | No |
| vsmart | dtls 10.255.255.3 | 1000 | 1 | 0:00:01:30 0 | 100.100.100.4 | | 12346 | 100.100.100.4 | 12346 | public-internet | No |
| vsmart | dtls 10.255.255.4 | 1000 | 1 | 0:00:01:30 0 | 100.100.100.5 | | 12346 | 100.100.100.5 | 12346 | public-internet | No |
| vmanage | dtls 10.255.255.1 | 1000 | 0 | 0:00:02:01 0 | 100.100.100.2 | | 12346 | 100.100.100.2 | 12346 | mpls | No |

| TECT | TX | SOURCE TLOC | | | REMOTE TLOC | | | DST PUBLIC | | | DST PUBLIC | | |
|---------------|----|-------------|---------|-------|-----------------|-------------|-----------------|---------------|----------------|-------|------------|----|--|
| | | SYSTEM IP | SITE ID | STATE | COLOR | TRANSITIONS | COLOR | SOURCE IP | IP | PORT | ENCAP | MO | |
| | | | | | | | | | | | | | |
| 10.255.255.11 | 1 | 1000 | 1 | up | mpls | 2 | mpls | 192.0.2.10 | 192.0.2.2 | 12426 | ipsec | 7 | |
| 10.255.255.11 | 1 | 1000 | 1 | up | public-internet | 0 | public-internet | 192.168.25.21 | 100.100.100.10 | 2936 | ipsec | 7 | |
| 10.255.255.12 | 1 | 1000 | 1 | up | mpls | 2 | mpls | 192.0.2.10 | 192.0.2.6 | 12426 | ipsec | 7 | |
| 10.255.255.12 | 1 | 1000 | 1 | up | public-internet | 0 | public-internet | 192.168.25.21 | 100.100.100.11 | 22184 | ipsec | 7 | |
| 10.255.255.31 | 30 | 1000 | 30 | up | mpls | 5 | mpls | 192.0.2.10 | 192.0.2.14 | 12366 | ipsec | 7 | |
| 10.255.255.31 | 30 | 1000 | 30 | up | public-internet | 5 | public-internet | 192.168.25.21 | 100.100.100.30 | 50308 | ipsec | 7 | |
| 10.255.255.41 | 40 | 1000 | 40 | up | mpls | 0 | mpls | 192.0.2.10 | 192.1.2.18 | 12387 | ipsec | 7 | |
| 10.255.255.41 | 40 | 1000 | 40 | up | public-internet | 0 | public-internet | 192.168.25.21 | 100.100.100.40 | 12347 | ipsec | 7 | |
| 10.255.255.51 | 50 | 1000 | 50 | up | public-internet | 0 | public-internet | 192.168.25.21 | 100.100.100.50 | 12347 | ipsec | 7 | |
| 10.255.255.52 | 50 | 1000 | 50 | up | mpls | 7 | mpls | 192.0.2.10 | 192.1.2.22 | 12347 | ipsec | 7 | |

We now see that the vEdges have established control connections over the transport connected to their counterpart at the same site. BFD sessions are also established across the platform transports. Thus, we should see control connections and bfd sessions across *mpls* on vEdge20 and across *public-internet* on vEdge21, along with their directly connected transport connections/sessions.

Task List

- [Overview](#)
- [Feature Templates for TLOC Extensions](#)
 - [Creating the VPN Interface Template for the TLOC-EXT interface](#)
 - [Creating the VPN Interface Template for the Tunnel interface](#)
 - [Creating the BGP Template for the MPLS link](#)
- [Updating the VPN and Device Templates](#)
- [Activity Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: July 3, 2016

Site last generated: Sep 1, 2020



Configuring a Hub and Spoke topology

[Take a tour of this page](#)

Summary: Moving the SD-WAN topology from the default of full mesh to a Hub and Spoke for a particular VPN while leaving the other VPNs in full mesh.

Table of Contents

- [Overview](#)
- [Creating a new DC VPN 20 Feature Template](#)
- [Creating the Policy](#)
 - [Configuring Network Constructs](#)
 - [Adding a Custom Control Policy](#)
- [Activity Verification](#)

Task List

- Overview
- Creating a new DC VPN 20 Feature Template
- Creating the Policy
- Configuring Network Constructs
- Adding a Custom Control Policy
- Activity Verification

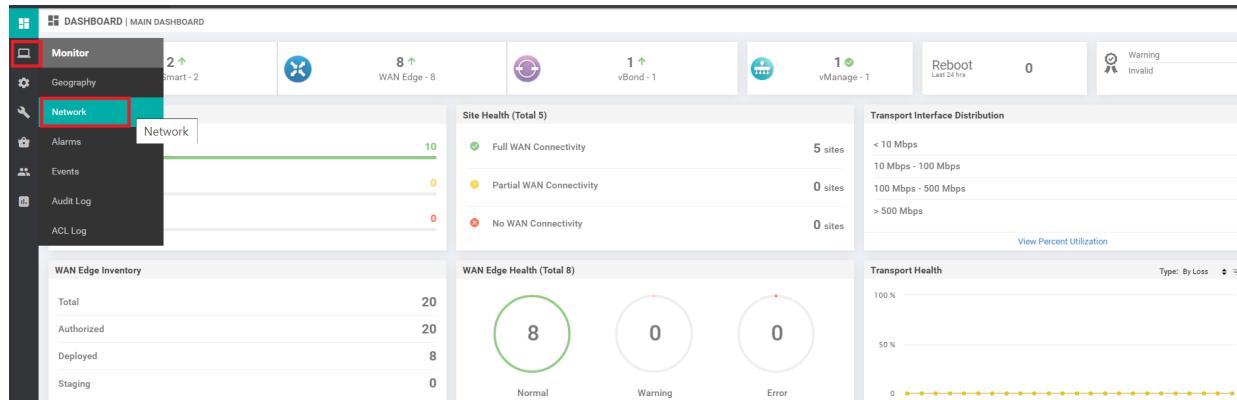
Overview

Cisco SD-WAN builds out a full mesh network between sites by default for all VPNs. This might not be desirable in some cases, where there is a requirement of a Hub and Spoke or a partial mesh topology.

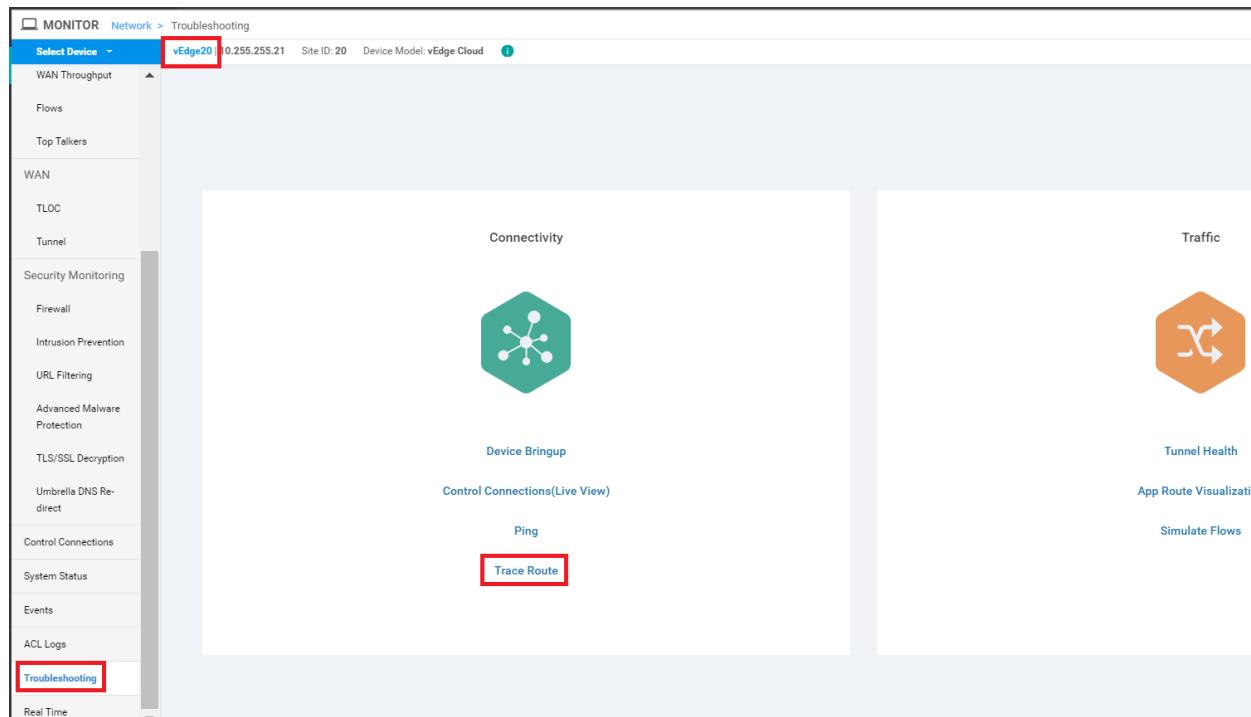
Cisco SD-WAN Policies allow us to enforce a custom topology, thereby controlling the data flow within our network. We will be setting up a Hub and Spoke topology for VPN 20 at all Branch sites, steering data to the DC site, post which it will be

routed to its destination. Other VPNs in the network will retain full mesh connectivity. First, let's check the current status of the connectivity.

1. Log in to the vManage GUI and navigate to **Monitor => Network**

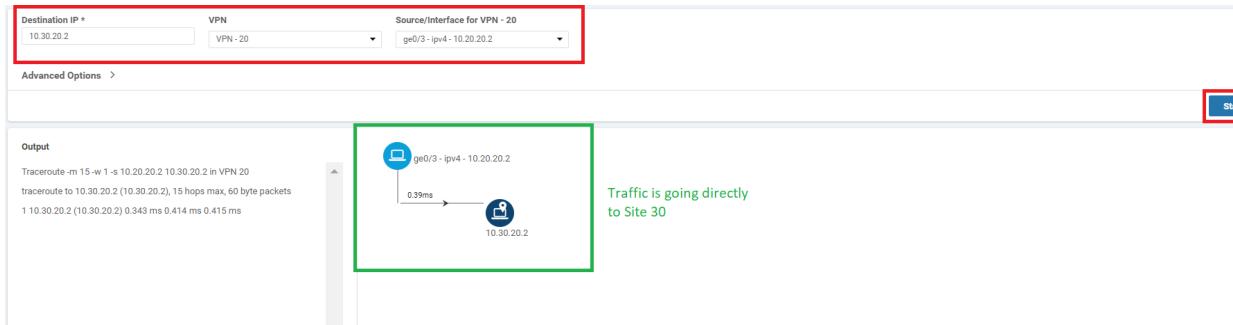


2. Click on **vEdge20** and scroll down to **Troubleshooting**. Click on it and then choose **Trace Route**

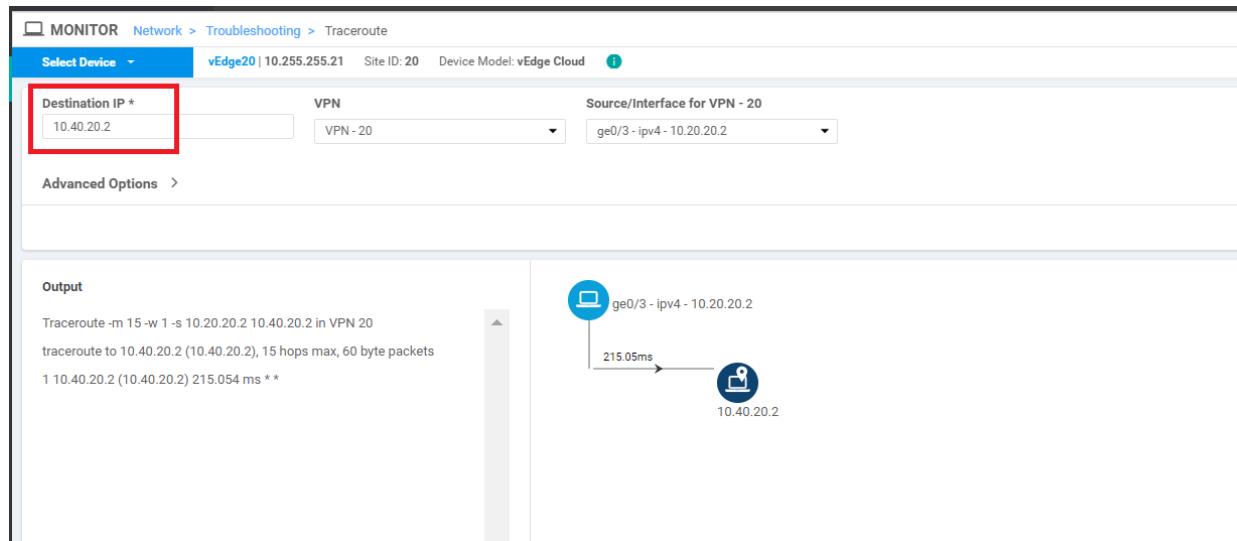


3. Enter the **Destination IP** as 10.30.20.2, choose **VPN** as **VPN - 20** and populate the **Source/Interface** as **ge0/3**. Click on **Start**. You will notice that traffic is flowing directly between the two sites (i.e. Site 20 and Site 30) in VPN 20 (if

there are multiple hops shown in the image in your POD, run the test again)



4. Run another test, this time to the **Destination IP** of 10.40.20.2. Traffic again flows directly between the sites



5. Log in to the CLI of **cEdge40** via Putty and issue a `show ip route vrf 20`. We will see that routes point directly to the sites, thereby facilitating full mesh connectivity

```
cEdge40#show ip route vrf 20

Routing Table: 20
Codes: L - local, C - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
      n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      H - NHRP, G - NHRP registered, g - NHRP registration summary
      o - ODR, P - periodic downloaded static route, l - LISB
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 10.255.255.12 to network 0.0.0.0

m*   0.0.0.0/0 [251/0] via 10.255.255.12, 3d00h, sdwan_system_ip
      [251/0] via 10.255.255.11, 3d00h, sdwan_system_ip
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
m     10.20.20.0/24 [251/0] via 10.255.255.22, 00:00:22, sdwan_system_ip
      [251/0] via 10.255.255.21, 00:00:22, sdwan_system_ip
m     10.30.20.0/24 [251/0] via 10.255.255.31, 2d23h, sdwan_system_ip
C     10.40.20.0/24 is directly connected, GigabitEthernet5
L     10.40.20.2/32 is directly connected, GigabitEthernet5
m     10.50.20.0/24 [251/0] via 10.255.255.52, 2d23h, sdwan_system_ip
      [251/0] via 10.255.255.51, 2d23h, sdwan_system_ip
m     10.100.20.0/24 [251/0] via 10.255.255.12, 3d01h, sdwan_system_ip
      [251/0] via 10.255.255.11, 3d01h, sdwan_system_ip
cEdge40#
```

```
show ip route vrf 20
```

6. Log in to the CLI of **vEdge20** and issue a `show ip route vpn 20`. Once again, routes are pointing directly to the corresponding site, which is expected behaviour (you will see routes on the mpls color as well). We will be looking at changing this in the upcoming sections

```
vEdge20# show ip route vpn 20
Codes Proto-sub-type:
IA -> ospf-intra-area, IE -> ospf-inter-area,
E1 -> ospf-external1, E2 -> ospf-external2,
N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
e -> bgp-external, i -> bgp-internal
Codes Status flags:
F -> fib, S -> selected, I -> inactive,
B -> blackhole, R -> recursive

VPN  PREFIX          PROTOCOL      PROTOCOL      NEXTHOP      NEXTHOP      NEXTHOP      COLOR
      SUB TYPE      IF NAME    ADDR        VPN       TLOC IP
-----+-----+-----+-----+-----+-----+-----+-----+
20   10.20.20.0/24  connected    -           ge0/3      -           -           -
20   10.30.20.0/24  omp         -           -           -           10.255.255.31  public-internet
20   10.40.20.0/24  omp         -           -           -           10.255.255.41  public-internet
20   10.50.20.0/24  omp         -           -           -           10.255.255.51  public-internet
20   10.100.20.0/24 omp        -           -           -           10.255.255.11  public-internet
20   10.100.20.0/24 omp        -           -           -           10.255.255.12  public-internet

vEdge20#
```

Task List

- Overview
- Creating a new DC VPN 20 Feature Template
- Creating the Policy
- Configuring Network Constructs
- Adding a Custom Control Policy
- Activity Verification

Creating a new DC VPN 20 Feature Template

Note: This section is optional. We will be testing just inter-site traffic so the changes in this section won't come into play, but if VPN 20 has to route all traffic through the DC, it might encompass Internet traffic as well. In this event, the following configuration is needed to steer all unknown prefixes to the DC.

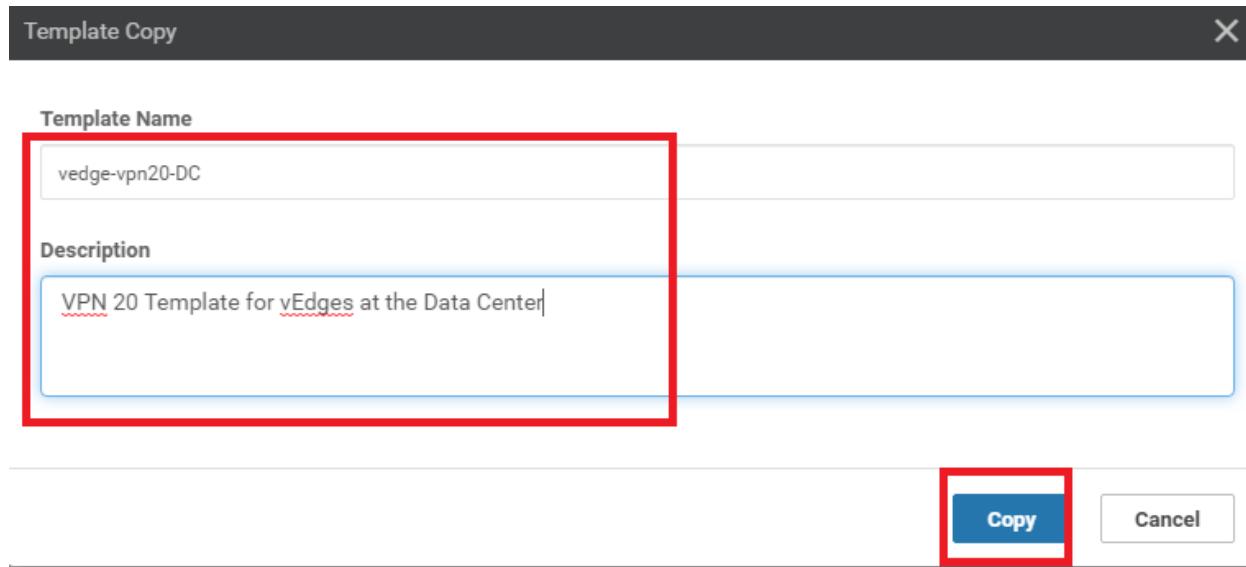
1. Go to **Configure => Templates => Feature tab** on the vManage GUI

| Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------------------|---------------------|--------------|------------------|------------------|------------|-----------------------------|---------|
| VPN0 for the Site20 vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 5:41:03 AM PDT | ... |
| cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR100v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| VPN0 for the Site30 INET and MPL... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:25:48 AM PDT | ... |
| cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR100v | 1 | 1 | admin | 23 May 2020 7:15:33 AM PDT | ... |
| INET Interface for the Site30 vEd... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:27:24 AM PDT | ... |
| cEdge VPN 512 Interface Template... | Cisco VPN Interface | CSR100v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| VPN 10 Template for the cEdges | Cisco VPN | CSR100v | 2 | 3 | admin | 26 May 2020 12:54:12 AM PDT | ... |
| VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 26 May 2020 12:49:58 AM PDT | ... |
| cEdge VPN 512 Template for Dual ... | Cisco VPN | CSR100v | 2 | 3 | admin | 18 May 2020 8:35:47 AM PDT | ... |
| VPN 20 Template for vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 25 May 2020 1:38:04 PM PDT | ... |
| VPN 10 Interface Template for vEd... | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 25 May 2020 1:43:16 PM PDT | ... |
| cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR100v | 1 | 1 | admin | 23 May 2020 7:34:59 AM PDT | ... |
| VPN 20 Template for the cEdges | Cisco VPN | CSR100v | 2 | 3 | admin | 25 May 2020 1:55:27 PM PDT | ... |
| VPN 30 Interface Template for cEd... | Cisco VPN Interface | CSR100v | 2 | 3 | admin | 25 May 2020 2:03:37 PM PDT | ... |
| MGMT Interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 23 May 2020 1:49:11 AM PDT | ... |

2. Locate the **vedge-vpn20** Feature Template and click on the dots next to it. Choose to make a **Copy** of this template

| | | | | | | | | |
|--------------------------|--------------------------------------|---------------------|-------------|---|---|-------|-----------------------------|-----|
| vEdge30_INET | INET interface for the Site30 vEdges | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:27:44 AM PDT | ... |
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Template... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| cedge-vpn10 | VPN 10 Template for the cEdges | Cisco VPN | CSR1000v | 2 | 3 | admin | 26 May 2020 12:54:12 AM PDT | ... |
| vedge-vpn10 | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 26 May 2020 12:49:58 AM PDT | ... |
| cEdge_VPN512_dual_Uplink | cEdge VPN 512 Template for Dual ... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 8:35:47 AM PDT | ... |
| vedge-vpn20 | VPN 20 Template for vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 25 May 2020 1:38:04 PM PDT | ... |
| vedge-vpn10-DC | VPN 10 Interface Template for vEd... | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 25 May 2020 1:38:04 PM PDT | ... |
| cEdge_VPN0_dual_Uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin | 23 May 2020 1:38:04 PM PDT | ... |
| cedge-vpn20 | VPN 20 Template for the cEdges | Cisco VPN | CSR1000v | 2 | 3 | admin | 25 May 2020 1:38:04 PM PDT | ... |
| cedge-vpn30-int | VPN 30 Interface Template for cEd... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 25 May 2020 1:38:04 PM PDT | ... |
| DC-vEdge_mgmt_int | MGMT interface for the DC-vEdges | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 23 May 2020 1:38:04 PM PDT | ... |
| vSmart-VPN512 | VPN512 Template for the vSmart | vSmart VPN | vSmart | 1 | 2 | admin | 25 May 2020 10:01:03 AM PDT | ... |
| vedge-vpn20-int | VPN 20 Interface Template for vEd... | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 25 May 2020 1:47:22 PM PDT | ... |

3. Rename the template `vedge-vpn20-DC` with a Description of `VPN 20 Template for vEdges at the Data Center` and click on **Copy**



4. Click on the dots next to the newly created template and choose to **Edit** it. Make sure that the Template Name and Description match and modify the **Name** field under Basic Configuration to a Global value of PoS

Device Feature

Feature Template > [VPN](#)

| | |
|---------------|----------------------------|
| Device Type | vEdge Cloud |
| Template Name | vedge-vpn20-DC |
| Description | VPN 20 Template for vEdges |

This feature template is shared by both Cisco vEdge and IOS-XE SDWAN devices. Please use the [Temp](#) templates to IOS-XE SDWAN feature templates.

Basic Configuration DNS Advertise OMP IPv4 Route IPv6 Route Service Service Route GRE Route

BASIC CONFIGURATION

VPN

Name Po\$

Enhance ECMP Keying On Off

Enable TCP Optimization On Off

5. Under **IPv4 Route** click on **New IPv4 Route**. Enter a Prefix of **0.0.0.0/0** and set the Gateway as **Null 0**. Toggle **Enable Null0** to a Global value of **On** and click on **Add**. Click on **Update** to update this Feature Template

IPv4 ROUTE

1

2

3 Next Hop Null 0 VPN

4 On Off

5

6 Cancel

No data available

6. Go to **Configuration => Templates => Device Tab** and locate the **DCvEdge_dev_temp**. Click on the three dots to the template and choose to **Edit**

The screenshot shows a table of device templates. A context menu is open over the row for 'vEdge_site20_dev_temp'. The menu options are: Edit, View, Delete, Copy, Attach Devices, Detach Devices, and Export CSV.

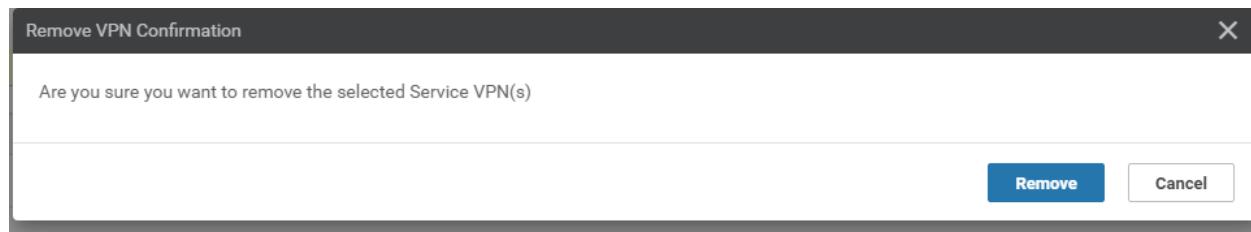
| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status |
|--------------------------|-----------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 17 | 2 | admin | 26 May 2020 3:05:01 AM PDT | In Sync |
| vEdge_Site20_dev_temp | Device template for the Site 2... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 PM PDT | In Sync |
| vEdgeSite30_dev_temp | Device template for the Site 3... | Feature | vEdge Cloud | 15 | 1 | admin | 25 May 2020 3:09:51 PM PDT | In Sync |
| cEdge_dualuplink_devtemp | cEdge Device Template for de... | Feature | CSR1000v | 19 | 1 | admin | 26 May 2020 12:31:48 AM PDT | In Sync |
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 16 | 2 | admin | 27 May 2020 2:54:22 PM PDT | In Sync |
| vSmart-dev-temp | Device Template for vSmarts | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 AM PDT | In Sync |

7. Scroll to the **Service VPN** section, select the *vedge-vpn20* Template and choose **Remove VPN** (don't worry, we will be adding it again, with the template we just created in steps 4 and 5)

The screenshot shows a table of service VPN templates. The 'Remove VPN' button is highlighted with a red box. The table has columns: ID, Template Name, and Sub-Templates.

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|---------------------|
| e9acf7d-aad6-4913-8f0a-84e255b4b033 | vedge-vpn10 | OSPF, VRN Interface |
| 6fd47ee6-61c1-4b02-9b3e-439f5c423b74 | vedge-vpn20 | VPN Interface |

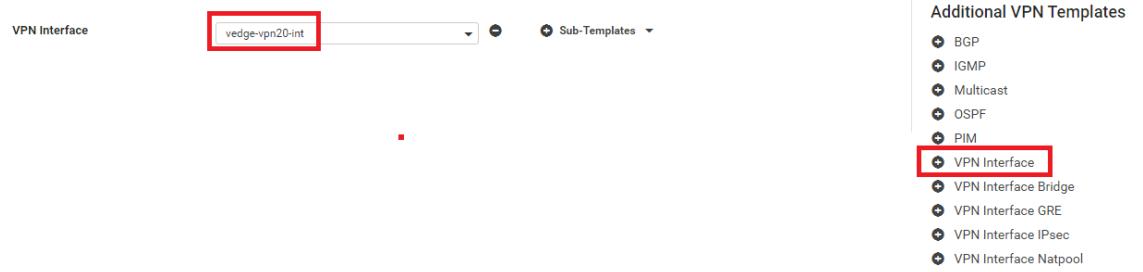
8. Confirm removal of the VPN by clicking on **Remove**



9. Back on the Device Template, click on **Add VPN** under **Service VPN**. Move the *vedge-vpn20-DC* Template to the Selected VPN Templates section and click on **Next**

The screenshot shows the 'Service VPN' section. The 'Add VPN' button is highlighted with a red box. The 'Selected VPN Templates' list contains one item: 'vedge-vpn20-DC'.

10. Click on **VPN Interface** under **Additional VPN Tempaltes** and populate *vedge-vpn20-int* in the VPN Interface drop down. Click on **Add**. This should take you back to the Device Template page. Click on **Update**



11. Click on **Next** followed by **Configure Devices** in the ensuing pages (you can choose to check the side-by-side configuration before choosing to Configure Devices)

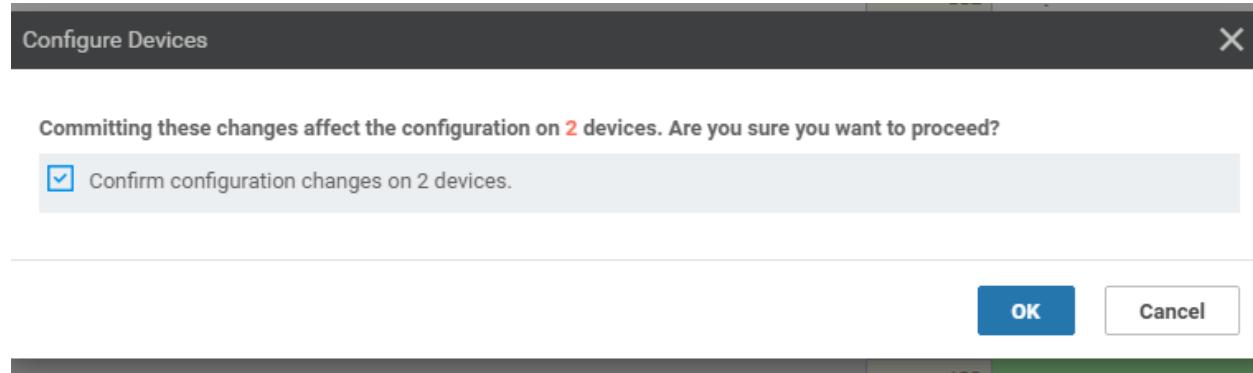
Device Template | DCvEdge_dev_temp

Search Options ▾

| S. | Chassis Number | System IP | Hostname | Interface Name(vpn20_if_name) | IPv4 Address(vpn20_if_ipv4_address) | Interface Name(vpn10_if_name) | IPv4 Address(vpn10_if_ipv4_address) |
|----|--------------------------------------|---------------|-----------|-------------------------------|-------------------------------------|-------------------------------|-------------------------------------|
| 1 | e474c5fd-8ce7-d376-7cac-ba950b2c9159 | 10.255.255.11 | DC-vEdge1 | ge0/3 | 10.100.20.2/24 | ge0/2 | 10.100.10.1/24 |
| 2 | 0cdd4f0e-f2f1-fe75-866c-469966cda1c3 | 10.255.255.12 | DC-vEdge2 | ge0/3 | 10.100.20.3/24 | ge0/2 | 10.100.10.2/24 |

Next Cancel

12. Confirm the change on 2 devices (the DC-vEdges)



13. Once complete, go to the CLI of vEdge20 via Putty and issue `show ip route vpn 20` again. You should notice default routes pointing to the DC-vEdges (at this point, site to site traffic will still not go via the DC-vEdges. For this, we will need to implement control policies)

```

vEdge20# show ip route vpn 20
Codes Proto-sub-type:
IA -> ospf-intra-area, IE -> ospf-inter-area,
E1 -> ospf-external1, E2 -> ospf-external2,
N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
e -> bgp-external, i -> bgp-internal
Codes Status flags:
F -> fib, S -> selected, I -> inactive,
B -> blackhole, R -> recursive
Before adding the null route

```

| VPN | PREFIX | PROTOCOL | PROTOCOL | NEXTHOP SUB TYPE | IF NAME | NEXTHOP ADDR | NEXTHOP VPN | TLOC IP | COLOR | ENCAP |
|-----|----------------|-----------|----------|------------------|---------|--------------|---------------|-----------------|-------|-------|
| 20 | 10.20.20.0/24 | connected | - | ge0/3 | - | - | - | - | - | - |
| 20 | 10.30.20.0/24 | omp | - | - | - | - | 10.255.255.31 | public-internet | ipsec | |
| 20 | 10.40.20.0/24 | omp | - | - | - | - | 10.255.255.41 | public-internet | ipsec | |
| 20 | 10.50.20.0/24 | omp | - | - | - | - | 10.255.255.51 | public-internet | ipsec | |
| 20 | 10.100.20.0/24 | omp | - | - | - | - | 10.255.255.11 | public-internet | ipsec | |
| 20 | 10.100.20.0/24 | omp | - | - | - | - | 10.255.255.12 | public-internet | ipsec | |

```

vEdge20# show ip route vpn 20
Codes Proto-sub-type:
IA -> ospf-intra-area, IE -> ospf-inter-area,
E1 -> ospf-external1, E2 -> ospf-external2,
N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
e -> bgp-external, i -> bgp-internal
Codes Status flags:
F -> fib, S -> selected, I -> inactive,
B -> blackhole, R -> recursive
After adding the null route

```

| VPN | PREFIX | PROTOCOL | PROTOCOL | NEXTHOP SUB TYPE | IF NAME | NEXTHOP ADDR | NEXTHOP VPN | TLOC IP | COLOR | ENCAP |
|-----|----------------|-----------|----------|------------------|---------|--------------|---------------|-----------------|-------|-------|
| 20 | 0.0.0.0/0 | omp | - | - | - | - | 10.255.255.11 | public-internet | ipsec | |
| 20 | 0.0.0.0/0 | omp | - | - | - | - | 10.255.255.12 | public-internet | ipsec | |
| 20 | 10.20.20.0/24 | connected | - | ge0/3 | - | - | - | - | - | - |
| 20 | 10.30.20.0/24 | omp | - | - | - | - | 10.255.255.31 | public-internet | ipsec | |
| 20 | 10.40.20.0/24 | omp | - | - | - | - | 10.255.255.41 | public-internet | ipsec | |
| 20 | 10.50.20.0/24 | omp | - | - | - | - | 10.255.255.51 | public-internet | ipsec | |
| 20 | 10.100.20.0/24 | omp | - | - | - | - | 10.255.255.11 | public-internet | ipsec | |
| 20 | 10.100.20.0/24 | omp | - | - | - | - | 10.255.255.12 | public-internet | ipsec | |

```
show ip route vpn 20
```

We have completed updating our Device Template to support a Hub and Spoke topology for VPN 20. Enforcement of the Hub and Spoke topology will be done in the following sections.

Task List

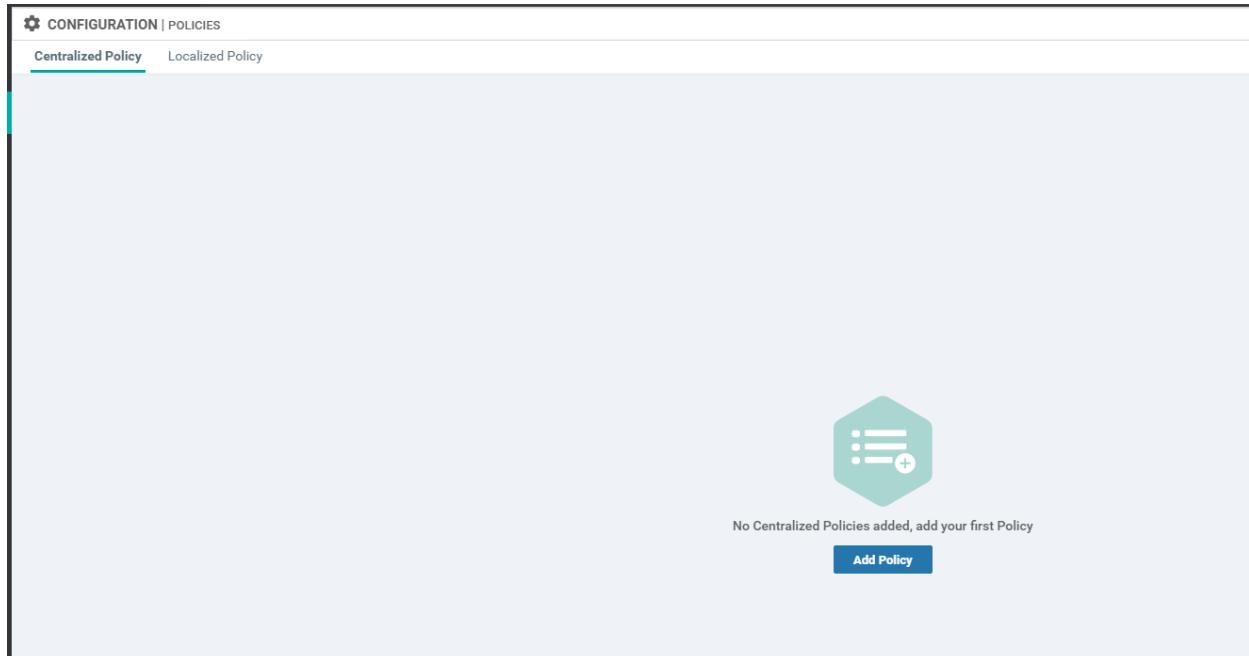
- [Overview](#)
- [Creating a new DC-VPN 20 Feature Template](#)
- [Creating the Policy](#)
- [Configuring Network Constructs](#)
- [Adding a Custom Control Policy](#)
- [Activity Verification](#)

Creating the Policy

We will now start enforcement of the Hub and Spoke topology via Control Policies. This is kicked off by creating a Policy which encompasses various Network Constructs (like Site Lists, VPN Lists etc.) that are used within the Policy.

Configuring Network Constructs

1. First, let's create our overarching policy. Through this policy, we will create our Network Constructs. Click on **Configuration => Policies** in the vManage GUI to start configuring the Policy
2. Click on **Add Policy**



3. We will first create a Site List. Click on **Sites** and then choose **New Site List**. Give it a name of *Branches* and enter *20,30,40,50* in the **Add Site** section. Click on **Add**

Select a list type on the left and start creating your groups of interest

| |
|---|
| Application |
| Color |
| Data Prefix |
| Police |
| Prefix 1 |
| Site 2 |
| SLA Class |
| TLOC |
| VPN |

New Site List 3

Site List Name
Branches 4

Add Site
20.30.40.50 5

Add Cancel

No data available

4. Three more Site Lists need to be created in a similar fashion. Some won't be used right now, but it's best to create them while we're here. Use the table and images below as reference points

| Site List Name | Add Site |
|----------------|----------|
| DC | 1 |
| Site30 | 30 |
| Site40 | 40 |

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Select a list type on the left and start creating your groups of interest

| |
|-------------|
| Application |
| Color |
| Data Prefix |
| Police |
| Prefix |
| Site |
| SLA Class |
| TLOC |
| VPN |

New Site List

Site List Name
DC

Add Site
Branches

Add Cancel

Name Entries Reference Count Updated By Last Updated Action

Branches 20, 30, 40, 50 0 admin 27 May 2020 3:05:50 PDT

Site List for the DC

Select a list type on the left and start creating your groups of interest

New Site List

Site List Name: Site30

Add Site: 3q

Action Table:

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|----------|----------------|-----------------|------------|----------------------------|--------|
| Branches | 20, 30, 40, 50 | 0 | admin | 27 May 2020 3:05:50 PM PDT | |
| DC | 1 | 0 | admin | 27 May 2020 3:06:14 PM PDT | |

Site List for Site 30

Select a list type on the left and start creating your groups of interest

New Site List

Site List Name: Site40

Add Site: 4q

Action Table:

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|----------|----------------|-----------------|------------|----------------------------|--------|
| Branches | 20, 30, 40, 50 | 0 | admin | 27 May 2020 3:05:50 PM PDT | |
| Site30 | 30 | 0 | admin | 27 May 2020 3:06:46 PM PDT | |
| DC | 1 | 0 | admin | 27 May 2020 3:06:14 PM PDT | |

Site List for Site 40

5. Once all the Site Lists are configured, it should look like this

Select a list type on the left and start creating your groups of interest

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|----------|----------------|-----------------|------------|----------------------------|--------|
| Branches | 20, 30, 40, 50 | 0 | admin | 27 May 2020 3:05:50 PM PDT | |
| Site30 | 30 | 0 | admin | 27 May 2020 3:06:46 PM PDT | |
| DC | 1 | 0 | admin | 27 May 2020 3:06:14 PM PDT | |
| Site40 | 40 | 0 | admin | 27 May 2020 3:07:10 PM PDT | |

6. Click on **VPN** on the left-hand side and click on **New VPN List**. Specify the VPN List Name as *Corporate* and enter **10** under **Add VPN**. Click on **Add**

Select a list type on the left and start creating your groups of interest

Create Groups of Interest Configure Topology and VPN Membership Configure Traffic Rules Apply Policies to Sites and VPNs

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|-------------------|---------|-----------------|------------|--------------|--------|
| No data available | | | | | |

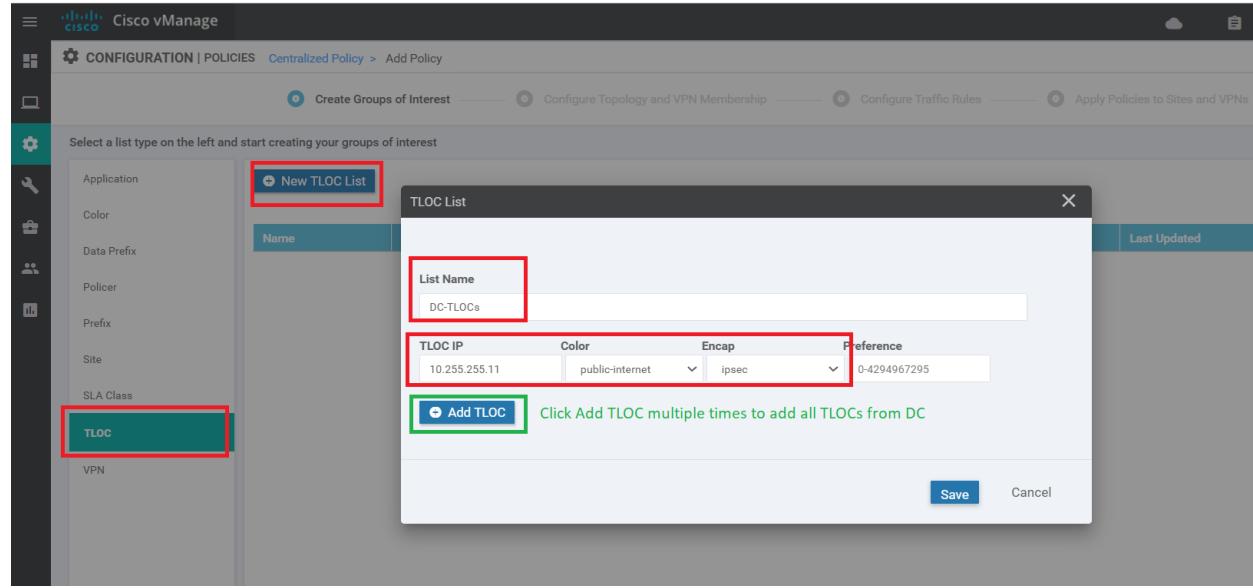
7. Repeat Step 6 two more times to create VPN Lists for *PoS* and *Guest*. They will have VPNs of 20 and 30 associated with them, respectively

 New VPN List

| Name | Entries | Reference Count | Updated By | Last Updated |
|-----------|---------|-----------------|------------|----------------------------|
| Corporate | 10 | 0 | admin | 27 May 2020 3:12:35 PM PDT |
| PoS | 20 | 0 | admin | 27 May 2020 3:12:44 PM PDT |
| Guest | 30 | 0 | admin | 27 May 2020 3:13:07 PM PDT |

8. Click on **TLOC** on the left-hand side then click on **New TLOC List**. Give a List Name of *DC-TLOCs*. Specify the following values (click **Add TLOC** 3 times - this will add the number of rows we need)

| TLOC IP | Color | Encap |
|---------------|-----------------|-------|
| 10.255.255.11 | public-internet | ipsec |
| 10.255.255.11 | mpls | ipsec |
| 10.255.255.12 | public-internet | ipsec |
| 10.255.255.12 | mpls | ipsec |



TLOC List

List Name

DC-TLOCs

| TLOC IP | Color | Encap | Preference |
|---------------|-----------------|-------|--------------|
| 10.255.255.11 | public-internet | ipsec | 0-4294967295 |
| 10.255.255.11 | mpls | ipsec | 0-4294967295 |
| 10.255.255.12 | public-internet | ipsec | 0-4294967295 |
| 10.255.255.12 | mpls | ipsec | 0-4294967295 |

[+ Add TLOC](#)

[Save](#) [Cancel](#)

The screenshot shows a modal dialog titled "TLOC List". At the top left is a "List Name" field containing "DC-TLOCs". Below it is a table with four rows, each representing a TLOC entry. The columns are labeled "TLOC IP", "Color", "Encap", and "Preference". Each row contains the same values: TLOC IP 10.255.255.11 or 10.255.255.12, Color public-internet or mpls, Encap ipsec, and Preference 0-4294967295. To the right of each row is a small red minus sign icon. At the bottom left is a blue button with a plus sign and the text "+ Add TLOC". At the bottom right are two buttons: "Save" (blue) and "Cancel" (gray).

9. The **DC-TLOCs** list should look like the following image. Click on **Next**

Select a list type on the left and start creating your groups of interest

| | New TLOC List | | | | | | |
|-------------|---------------|---------------|-----------------|-------|------------|-----------------|------------|
| | Name | TLOC | Color | Encap | Preference | Reference Co... | Updated By |
| Application | | | | | | 0 | admin |
| Color | | | | | | | |
| Data Prefix | | | | | | | |
| Policer | | 10.255.255.11 | public-internet | ipsec | -- | | |
| Prefix | | 10.255.255.11 | mpls | ipsec | -- | | |
| Site | | 10.255.255.12 | public-internet | ipsec | -- | | |
| SLA Class | | 10.255.255.12 | mpls | ipsec | -- | | |
| TLOC | | | | | | | |
| VPN | | | | | | | |

Next CANCEL

We will pause here since configuration of the Network Constructs is complete for our Control Policy. These will be used as building blocks for our policies. Configuration of the policy itself will continue in the next section (carrying on from the page we're at in the vManage GUI).

Task List

- [Overview](#)
- [Creating a new DC-VPN 20 Feature Template](#)
- [Creating the Policy](#)
- [Configuring Network Constructs](#)
- [Adding a Custom Control Policy](#)
- [Activity Verification](#)

Adding a Custom Control Policy

Continuing from the previous section, let's build out our Custom Control Policy to enforce a Hub and Spoke Topology on VPN 20

1. You should be at the **Configure Topology and VPN Membership** page after the previous section. Click on **Add Topology** and choose **Custom Control (Route & TLOC)**

The screenshot shows the Juniper Configuration interface for 'Centralized Policy > Add Policy'. At the top, there are three tabs: 'Create Groups of Interest' (green checkmark), 'Configure Topology and VPN Membership' (blue circle), and 'Configure Groups of Interest' (grey circle). Below the tabs, a section titled 'Specify your network topology' contains two tabs: 'Topology' (underlined) and 'VPN Membership'. Under 'Topology', a dropdown menu is open, showing options: 'Hub-and-Spoke', 'Mesh', 'Custom Control (Route & TLOC)', and 'Import Existing Topology'. The 'Custom Control (Route & TLOC)' option is highlighted. To the right of the dropdown is a search bar labeled 'Search Options'. Below the search bar is a table with columns: Type, Description, and Reference Count. The table displays the message 'No data available'.

2. Specify a **Name** of *HnS-VPN20* with a Description of *Hub and Spoke for VPN 20 only*. Click on **Sequence Type** and choose to add a **Route** Control Policy

Cisco vManage

CONFIGURATION | POLICIES Add Custom Control Policy

Name: HnS-VPN20

Description: Hub and Spoke for VPN 20 only

Sequence Type

Default Action

Route

TLOC

3. Click on **Sequence Rule** to add a new rule

Route

Sequence Rule

Drag and drop to re-arrange rules

4. Under **Match** click on **Site** and populate *Branches* in the **Site List** (this is one of the Site Lists we had created before)

Protocol: IPv4

Match

Actions

Color List OMP Tag Origin Originator Preference Site TLOC VPN VPN Prefix List

Site List

Branches

Actions

Reject Enabled

Site ID: 0-4294967295

5. Still under **Match**, click on **VPN** and choose *PoS* in the **VPN List**

The screenshot shows the 'Match' tab of a configuration interface. At the top, there are tabs for 'Protocol' (set to 'IPv4'), 'Color List', 'OMP Tag', 'Origin', 'Originator', 'Preference', 'Site', 'TLOC', 'VPN' (which is highlighted with a red box), and 'Prefix List'. Below these tabs, the 'Match Conditions' section contains fields for 'Site List' (with 'Branches' selected), 'Site ID' (0-4294967295), 'VPN List' (with 'PoS' selected, highlighted with a red box), and 'VPN ID' (0-65536). To the right, the 'Actions' section shows 'Reject' and 'Enabled' status.

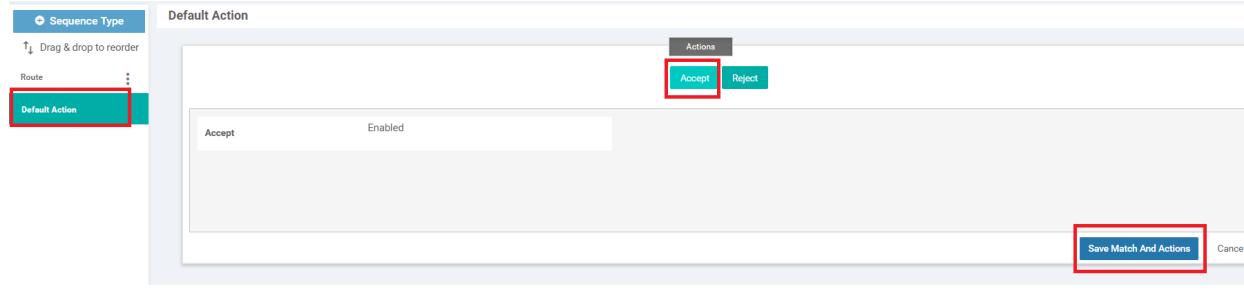
Through these two match conditions, we have specified that this rule applies to the site list Branches (which contains Site IDs 20, 30, 40 and 50) and to the PoS VPN (which has VPN 20 in it)

6. Move over to the **Actions** tab and click on **Accept**. Then click on **TLOC** and populate *DC-TLOCs* in the **TLOC List**.

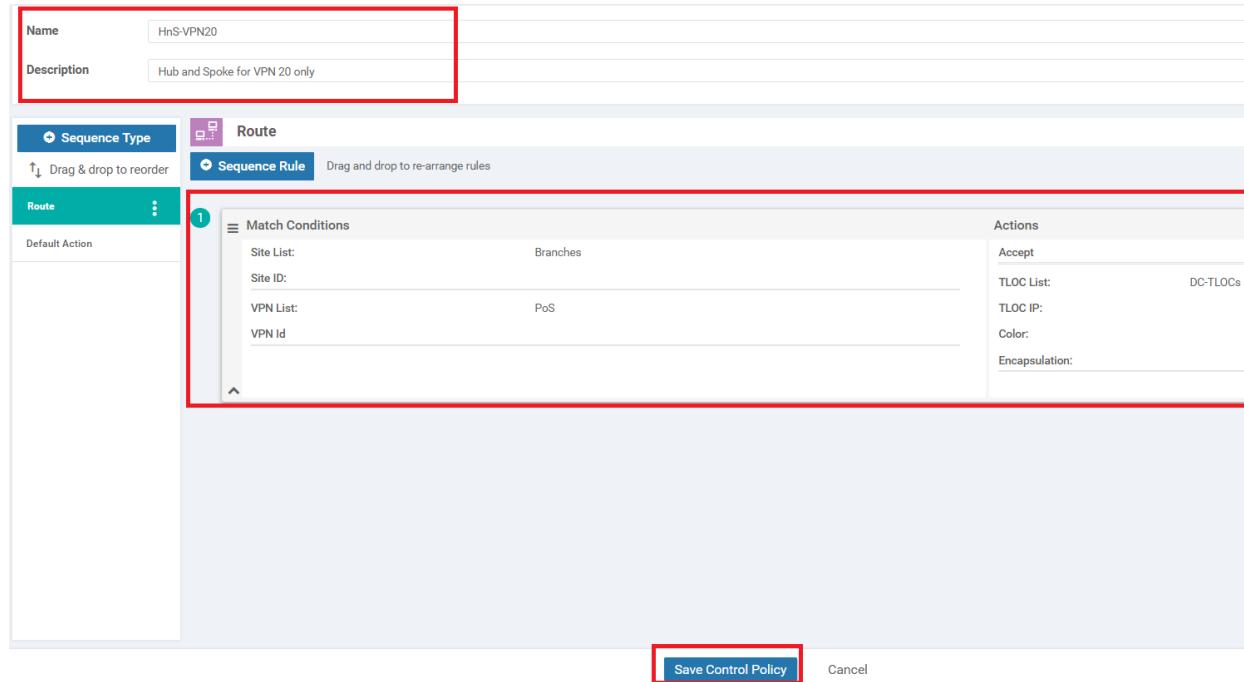
Click on **Save Match and Actions**

The screenshot shows the 'Actions' tab of a configuration interface. At the top, there are tabs for 'Route' (highlighted with a purple box), 'Sequence Rule' (highlighted with a blue box), and 'Route'. Under 'Sequence Rule', there are buttons for 'Accept' (highlighted with a red box) and 'Reject'. Below these are tabs for 'Match' (highlighted with a red box) and 'Actions' (highlighted with a yellow circle labeled 1). In the 'Actions' section, there are tabs for 'Export To', 'OMP Tag', 'Preference', 'Service', 'TLOC Action' (highlighted with a red box), and 'TLOC' (highlighted with a yellow circle labeled 3). The 'TLOC' section contains an 'Accept' button ('Enabled') and an 'Actions' section. The 'Actions' section includes a 'TLOC List' field (highlighted with a red box and labeled 4) containing 'DC-TLOCs x', and fields for 'TLOC IP' (Example: 10.0.0.1), 'Color' (Select a color list), and 'Encapsulation' (Select an encapsulation). A 'Save Match And Actions' button is at the bottom right (highlighted with a yellow circle labeled 5).

7. Go to the **Default Action** and click on **Accept**. Click **Save Match and Actions**



8. The **HnS-VPN20** policy should look like the image below. Click on **Save Control Policy**



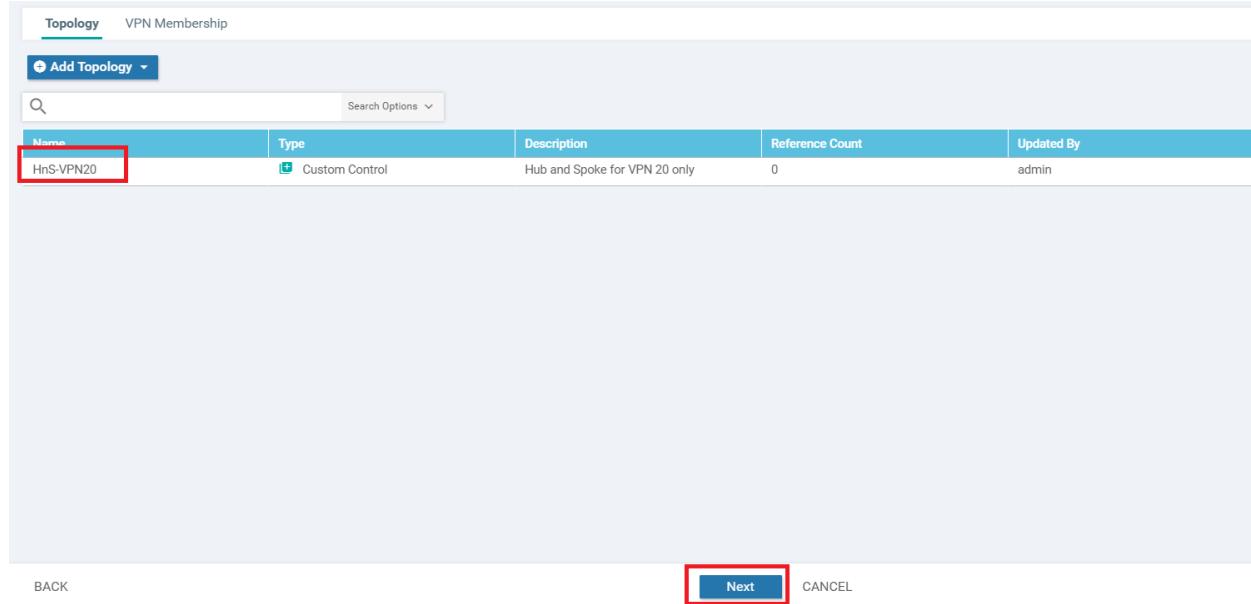
9. Click on **Next** since we don't want to add any more Policies and then **Next** again (since we aren't doing any Application Aware Routing, Data Policies or Netflow policies as of now)

Topology VPN Membership

Add Topology ▾

| Name | Type | Description | Reference Count | Updated By | L |
|-----------|----------------|-------------------------------|-----------------|------------|---|
| HnS-VPN20 | Custom Control | Hub and Spoke for VPN 20 only | 0 | admin | 2 |

BACK **Next** CANCEL



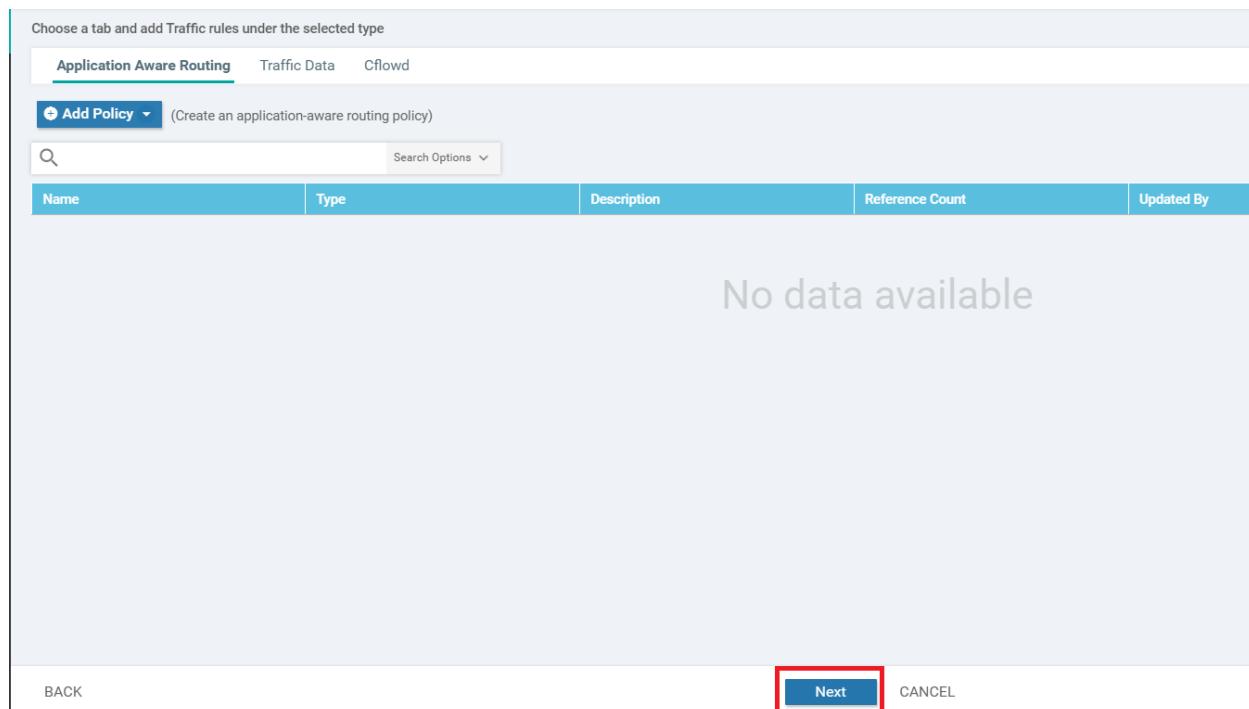
Choose a tab and add Traffic rules under the selected type

Application Aware Routing Traffic Data Cflowd

Add Policy ▾ (Create an application-aware routing policy)

| Name | Type | Description | Reference Count | Updated By |
|-------------------|------|-------------|-----------------|------------|
| No data available | | | | |

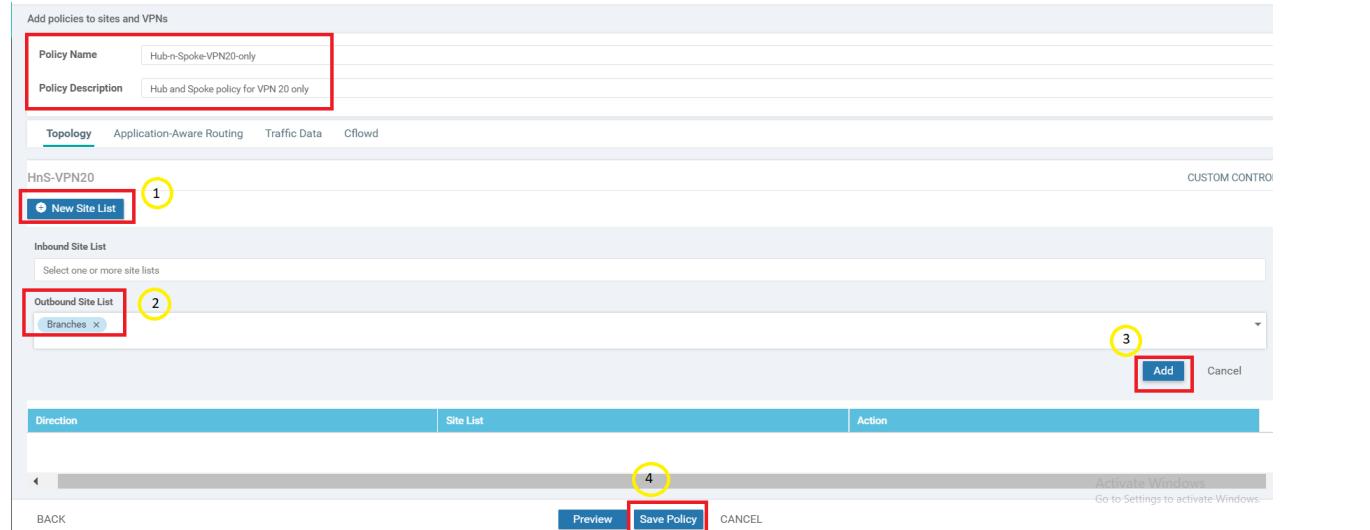
BACK **Next** CANCEL



10. You should be presented with a screen which asks for a Policy Name, among other things. This can be a bit confusing since we just gave a Policy Name before (called *HnS-VPN20*). The easiest way to wrap your head around this is think

of creating a Master Policy and before we can name this Master Policy, we are asked to create Sub-Policies in it. So far, we have just created a Sub Policy and given it a name. At this point, we are being asked to give a name to our Master Policy, which will then need to be applied.

Enter a **Policy Name** of *Hub-n-Spoke-VPN20-only* and give a Policy Description of *Hub and Spoke policy for VPN 20 only*. Click on **New Site List** under HnS-VPN20 and populate *Branches* in the **Outbound Site List**. Click on **Add**



Tip: Control Policies (such as the one you just built) are enforced by vSmart. Hence, the policy you just created is from the perspective of vSmart. The application of this policy is enforced in an outbound direction towards branch sites (i.e. Branches Site List). Think of how a BGP Route-Reflector would modify the next-hop of routes it receives before sending them back out to neighbors.

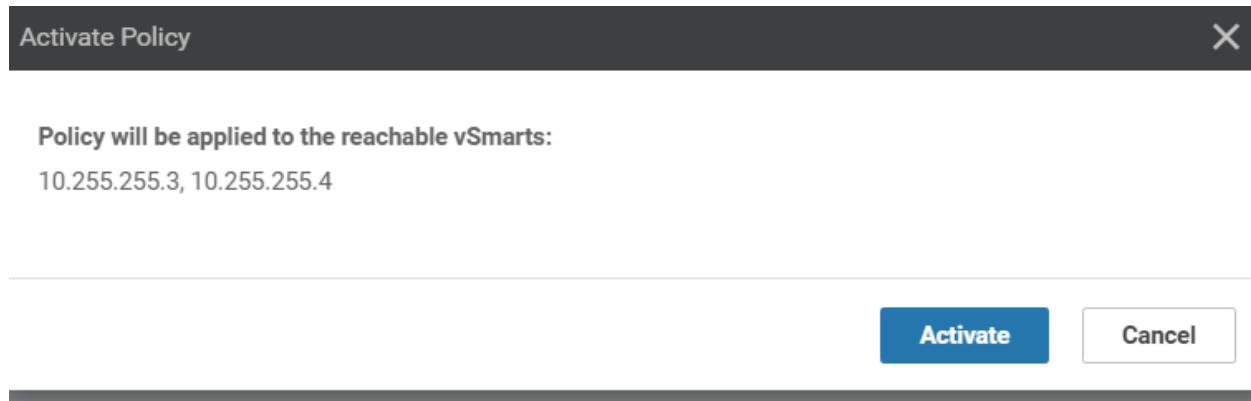
Click on **Save Policy**

11. Back at the main Policy page, we should see the *Hub-n-Spoke-VPN20-only* Master Policy created. Click on the three dots next to it and choose to **Activate** the policy

The screenshot shows a table of policies. One row is selected, highlighted with a red border. The columns are: Name, Description, Type, Activated, Updated By, Policy Version, Last Updated, and an ellipsis button. The 'Activated' column for the selected row shows 'false'. The 'Last Updated' column shows '28 May 2020 3:01:34 AM PDT'. To the right of the table is a context menu with the following options: View, Preview, Copy, Edit, Delete, and Activate. The 'Activate' option is highlighted with a red border.

| Name | Description | Type | Activated | Updated By | Policy Version | Last Updated | |
|------------------------|--------------------------------------|-------------------|-----------|------------|--------------------|----------------------------|-----|
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 20 o... | UI Policy Builder | false | admin | 05282020T100134900 | 28 May 2020 3:01:34 AM PDT | ... |

12. Confirm the activation by clicking on **Activate**



This completes our policy creation and activation. We will verify functionality in the upcoming section.

Task List

- [Overview](#)
- [Creating a new DC VPN 20 Feature Template](#)
- [Creating the Policy](#)
- [Configuring Network Constructs](#)
- [Adding a Custom Control Policy](#)
- [Activity Verification](#)

Activity Verification

1. Log in to **cEdge40** via Putty and run `show ip route vrf 20`. When compared to the output of this command taken before we applied our policy, we see that all routes are now pointing to the DC-vEdges. Check Step 5 of [Overview](#) for the earlier output

```
cEdge40#show ip route vrf 20

Routing Table: 20
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
      n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      H - NHRP, G - NHRP registered, g - NHRP registration summary
      o - ODR, P - periodic downloaded static route, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 10.255.255.12 to network 0.0.0.0

m*   0.0.0.0/0 [251/0] via 10.255.255.12, 00:00:23, sdwan_system_ip
      [251/0] via 10.255.255.11, 00:00:23, sdwan_system_ip
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
m     10.20.20.0/24 [251/0] via 10.255.255.12, 00:00:23, sdwan_system_ip
      [251/0] via 10.255.255.11, 00:00:23, sdwan_system_ip
m     10.30.20.0/24 [251/0] via 10.255.255.12, 00:00:23, sdwan_system_ip
      [251/0] via 10.255.255.11, 00:00:23, sdwan_system_ip
C     10.40.20.0/24 is directly connected, GigabitEthernet5
L     10.40.20.2/32 is directly connected, GigabitEthernet5
m     10.50.20.0/24 [251/0] via 10.255.255.12, 00:00:23, sdwan_system_ip
      [251/0] via 10.255.255.11, 00:00:23, sdwan_system_ip
m     10.100.20.0/24 [251/0] via 10.255.255.12, 00:00:23, sdwan_system_ip
      [251/0] via 10.255.255.11, 00:00:23, sdwan_system_ip

cEdge40#
cEdge40#
```

2. On the vManage GUI, go to **Monitor => Network** and click on **vEdge20**. Scroll down on the left-hand side and click on **Real Time**. Enter *IP Routes* in **Device Options** and choose to Filter. Filter on the basis of VPN ID 20. We will notice similar output as what was seen for cEdge40

MONITOR Network > Real Time

Select Device vEdge20 | Site ID: 20 Device Model: vEdge Cloud

Device Options: IP Routes

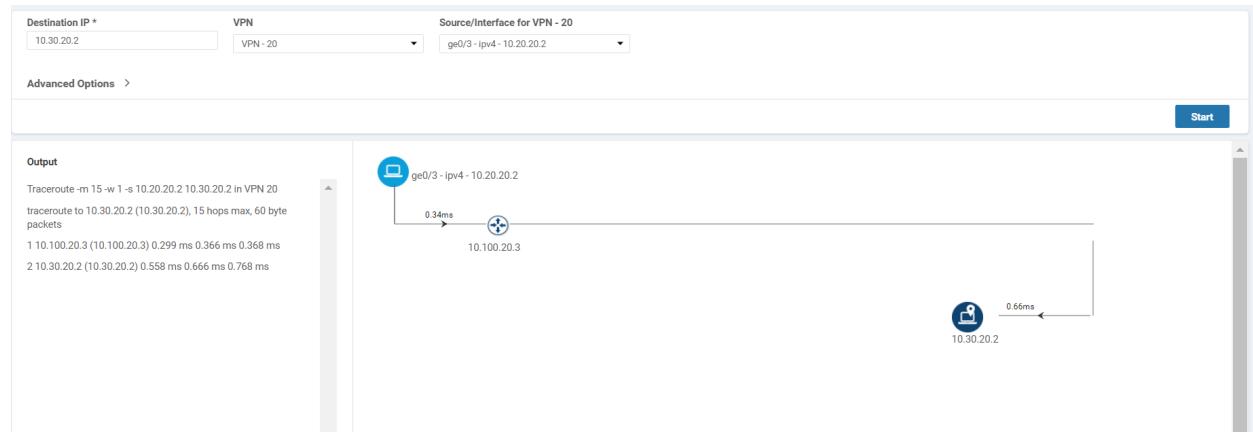
Filter: VPN ID: 20

| VPN ID | AF Type | Prefix | Protocol | Next Hop If Name | Next Hop Address | Next Hop VPN | TLOC IP | TLOC Color | TLOC Encap | Next Hop Label | Next Hop Interface |
|--------|---------|----------------|-----------|------------------|------------------|--------------|---------------|-----------------|------------|----------------|--------------------|
| 20 | ipv4 | 0.0.0.0/0 | omp | — | — | — | 10.255.255.11 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 0.0.0.0/0 | omp | — | — | — | 10.255.255.12 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 10.20.0.0/24 | connected | ge0/3 | — | — | — | — | — | — | ip |
| 20 | ipv4 | 10.30.20.0/24 | omp | — | — | — | 10.255.255.11 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 10.30.20.0/24 | omp | — | — | — | 10.255.255.12 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 10.40.20.0/24 | omp | — | — | — | 10.255.255.11 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 10.40.20.0/24 | omp | — | — | — | 10.255.255.12 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 10.50.20.0/24 | omp | — | — | — | 10.255.255.11 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 10.50.20.0/24 | omp | — | — | — | 10.255.255.12 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 10.100.20.0/24 | omp | — | — | — | 10.255.255.11 | public-internet | ipsec | 1004 | ip |
| 20 | ipv4 | 10.100.20.0/24 | omp | — | — | — | 10.255.255.12 | public-internet | ipsec | 1004 | ip |

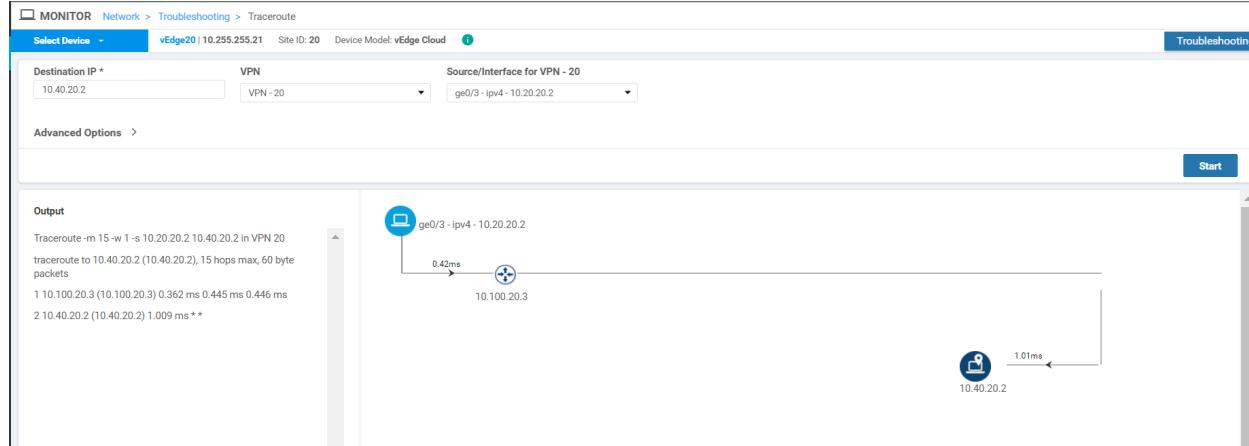
Total Rows: 11

Activate Windows
Go to Settings to activate Windows.

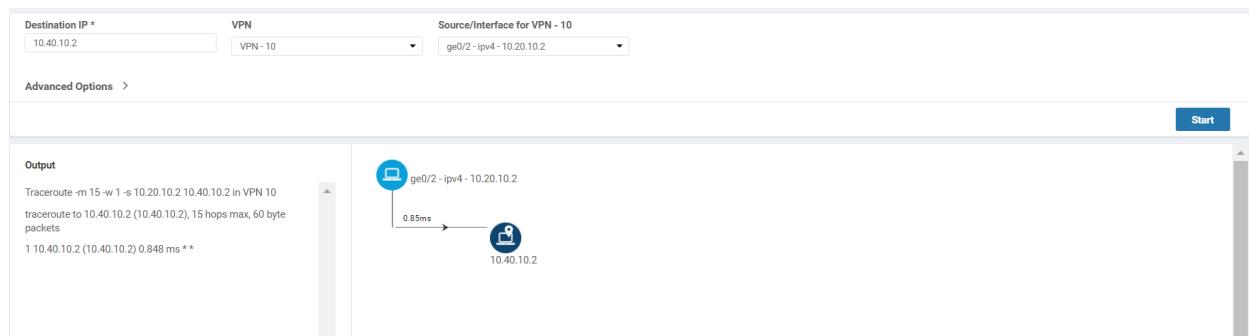
3. Go to **Troubleshooting** and choose Trace Route. Enter the **Destination IP** as 10.30.20.2 with a VPN of **VPN - 20** and a Source/Interface of **ge0/3**. Traffic is now reaching the destination via the DC-vEdge



4. Run the traceroute for 10.40.20.2 and we see that traffic is being routed through the DC-vEdge in this case as well



5. Try to do a traceroute to 10.40.10.2, changing the VPN to VPN - 10 and the Source/Interface to ge0/2 and we will notice that VPN 10 still has full mesh connectivity



Thus, all traffic from VPN 20 in the Branches is being steered to the DC-vEdges in a Hub and Spoke topology, whereas traffic still utilizes a Mesh topology for other VPNs.

Task List

- [Overview](#)
- [Creating a new DC-VPN 20 Feature Template](#)
- [Creating the Policy](#)
- [Configuring Network Constructs](#)
- [Adding a Custom Control Policy](#)
- [Activity Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 26, 2020

Site last generated: Jul 23, 2020



-->

Setting up a Regional Hub

Summary: Steering all traffic from Site 20 to a Regional Hub (Site 30).

Table of Contents

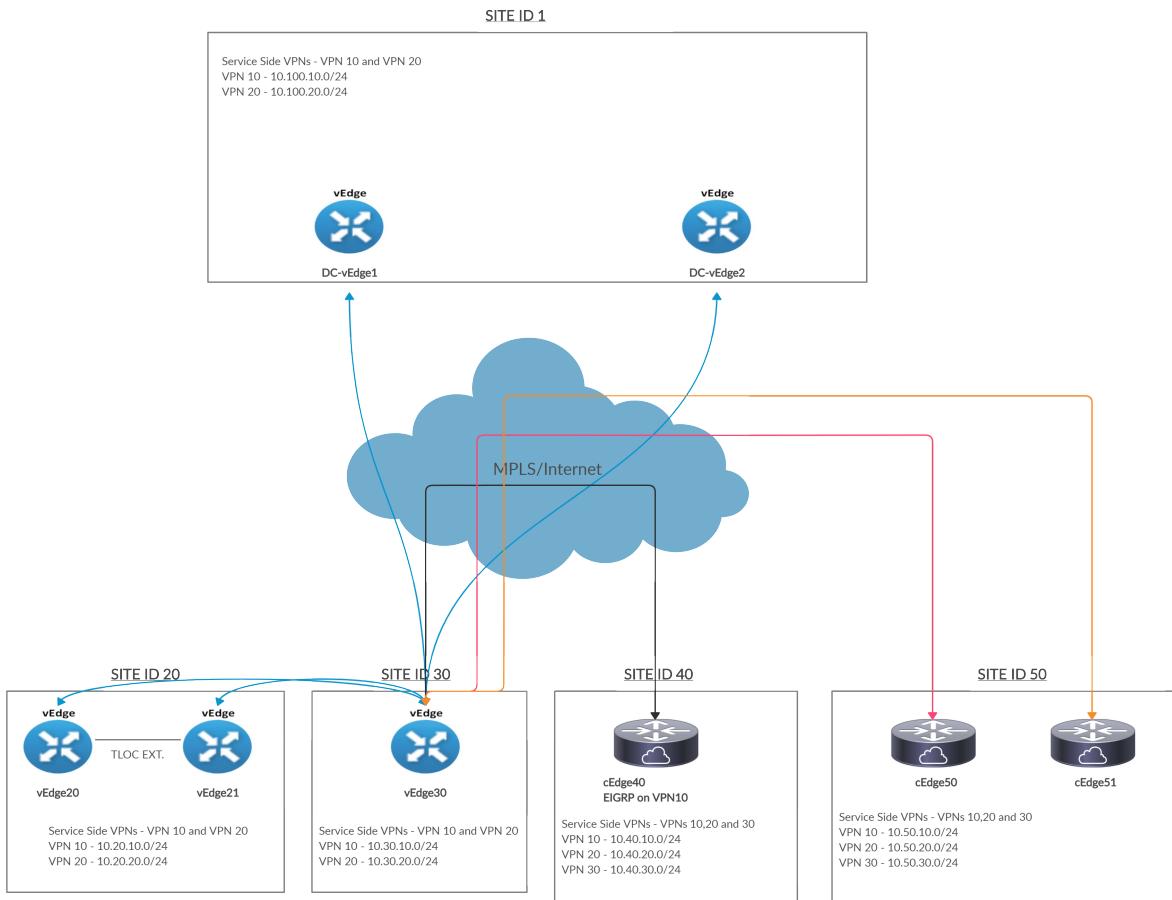
- [Pre-Configuration](#)
- [Adding the Policy](#)
 - [Setting up Site Lists](#)
 - [Adding Custom Control Policies](#)
 - [Policy for Traffic from Site 20 to the Regional Hub](#)
 - [Policy for Traffic from the Fabric to Site 20](#)
 - [Saving and Activating the Policy](#)
- [Verification](#)

Task List

- Pre-Configuration
- Adding the Policy
 - Setting up Site Lists
 - Adding Custom Control policies
 - Policy for Traffic from Site 20 to the Regional Hub
 - Policy for Traffic from the Fabric to Site 20
 - Saving and Activating the Policy
- Verification

Pre-Configuration

In this section, we will ensure that whenever communication has to happen in/out of Site 20, it goes through Site 30. This means there will be two parts to the configuration - how Site 20 talks to other sites, and how other sites talk to Site 20. Site 30 will function as a Regional Hub for Site 20. Given below is the traffic flow we're looking to achieve.



Notice that all sites communicate to Site 20 via Site 30. Conversely, Site 20 punts all outbound traffic to Site 30.

1. We will first deactivate the Hub and Spoke policy created for VPN 20. On the vManage GUI, navigate to **Configuration => Policies** and click on the three dots next to the *Hub-n-Spoke-VPN20-only* policy. Choose to **Deactivate it**

The screenshot shows the 'CONFIGURATION | POLICIES' section. Under 'Centralized Policy', there is a table with one row. The row details are:

| Name | Description | Type | Activated | Updated By | Policy Version | Last Updated | ... |
|------------------------|--------------------------------------|-------------------|-----------|------------|--------------------|----------------------------|-----|
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 20 o... | UI Policy Builder | true | admin | 05282020T100134900 | 28 May 2020 3:01:34 AM PDT | |

A context menu is open over the last column of the table, listing the following options: View, Preview, Copy, Edit, Delete, and Deactivate. The 'Deactivate' option is highlighted with a red box.

2. Confirm the Deactivation

The screenshot shows a confirmation dialog box with the title 'Deactivate Policy'. The message inside the box states: 'Policy will be removed from the following vSmart.
10.255.255.3, 10.255.255.4'. Below this, a question is asked: 'Would you like to remove policy from reachable vSmarts?'. At the bottom of the dialog are two buttons: a blue 'Deactivate' button and a white 'Cancel' button.

3. Verify that traffic for VPN 20 is now flowing per the default Mesh topology. Navigate to **Monitor => Network** and click on **vEdge20**. Scroll down on the left-hand side to **Real Time** and enter **IP Routes** in the Device Options. Choose to Filter on the basis of VPN ID 20

| IP Routes | | | | | | | |
|------------------|--------|----------------|----------------|-----------|------------------|--------------|---------------|
| Device Options: | | Search Options | | | | | |
| Next Hop If Name | VPN ID | AF Type | Prefix | Protocol | Next Hop Address | Next Hop VPN | TLOC IP |
| - | 20 | ipv4 | 0.0.0.0/0 | omp | - | -- | 10.255.255.11 |
| - | 20 | ipv4 | 0.0.0.0/0 | omp | - | -- | 10.255.255.12 |
| ge0/3 | 20 | ipv4 | 10.20.20.0/24 | connected | - | -- | - |
| - | 20 | ipv4 | 10.30.20.0/24 | omp | - | -- | 10.255.255.31 |
| - | 20 | ipv4 | 10.40.20.0/24 | omp | - | -- | 10.255.255.41 |
| - | 20 | ipv4 | 10.50.20.0/24 | omp | - | -- | 10.255.255.51 |
| - | 20 | ipv4 | 10.100.20.0/24 | omp | - | -- | 10.255.255.11 |
| - | 20 | ipv4 | 10.100.20.0/24 | omp | - | -- | 10.255.255.12 |

Task List

- [Pre-Configuration](#)
- [Adding the Policy](#)
 - [Setting up Site Lists](#)
 - [Adding Custom Control policies](#)
 - Policy for Traffic from Site 20 to the Regional Hub
 - Policy for Traffic from the Fabric to Site 20
 - [Saving and Activating the Policy](#)
- [Verification](#)

Adding the Policy

Setting up Site Lists

1. Go to **Configuration => Policies** and click on **Add Policy**

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | POLICIES' section. The 'Centralized Policy' tab is selected. A red box highlights the 'Add Policy' button in the top-left corner of the main content area. Below it is a search bar and a table listing a single policy entry:

| Name | Description | Type | Activated | Updated By |
|------------------------|--------------------------------------|-------------------|-----------|------------|
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 20 o... | UI Policy Builder | false | admin |

2. Click on **Site** and choose to add a **New Site List**. Populate the Site List Name as *Fabric* and Add Site of *1,40,50* (i.e. all the Sites other than the Regional Hub and Regional Spoke sites). Click on **Add**

The screenshot shows the 'New Site List' configuration screen. On the left sidebar, 'Site' is selected. The main area shows a 'Site List Name' input field with 'Fabric' typed in. Below it is an 'Add Site' input field containing '1,40,50', which is also highlighted with a red box. To the right are 'Add' and 'Cancel' buttons, with 'Add' also highlighted with a red box. At the bottom is a table of existing site lists:

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|----------|-------------|-----------------|------------|----------------------------|--------|
| Site40 | 40 | 0 | admin | 28 May 2020 1:43:30 AM PDT | |
| Branches | 20,30,40,50 | 2 | admin | 28 May 2020 1:43:00 AM PDT | |
| DC | 1 | 0 | admin | 28 May 2020 1:43:12 AM PDT | |
| Site30 | 30 | 0 | admin | 28 May 2020 1:43:23 AM PDT | |

3. Click on **New Site List** again and give this Site List a Name of *Site20* with an Add Site of *20*. Click on **Add**. Click on **Next** to move on to the **Configure Topology and VPN Membership** page, which we will continue configuring in the next section

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership Configure Traffic Rules Apply Policies to Sites and VPNs

Select a list type on the left and start creating your groups of interest

| | |
|-------------|--|
| Application | New Site List |
| Color | |
| Data Prefix | |
| Policer | |
| Prefix | |
| Site | Site List Name Site20 Add Site 2d |
| SLA Class | |
| TLOC | |
| VPN | |

[Add](#)

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|----------|----------------|-----------------|------------|----------------------------|---|
| Site40 | 40 | 0 | admin | 28 May 2020 1:43:30 AM PDT | Edit Delete |
| Branches | 20, 30, 40, 50 | 2 | admin | 28 May 2020 1:43:00 AM PDT | Edit Delete |
| DC | 1 | 0 | admin | 28 May 2020 1:43:12 AM PDT | Edit Delete |
| Site30 | 30 | 0 | admin | 28 May 2020 1:43:23 AM PDT | Edit Delete |
| Fabric | 1, 40, 50 | 0 | admin | 28 May 2020 5:38:49 AM PDT | Edit Delete |

[Next](#) CANCEL

Task List

- [Pre-Configuration](#)
- [Adding the Policy](#)
 - [Setting up Site Lists](#)
 - [Adding Custom Control policies](#)
 - [Policy for Traffic from Site 20 to the Regional Hub](#)
 - [Policy for Traffic from the Fabric to Site 20](#)
 - [Saving and Activating the Policy](#)
- [Verification](#)

Adding Custom Control Policies

We will be adding two policies in this section - one for traffic destined to the rest of the network from Site 20 and one for traffic destined to Site 20.

Policy for Traffic from Site 20 to the Regional Hub

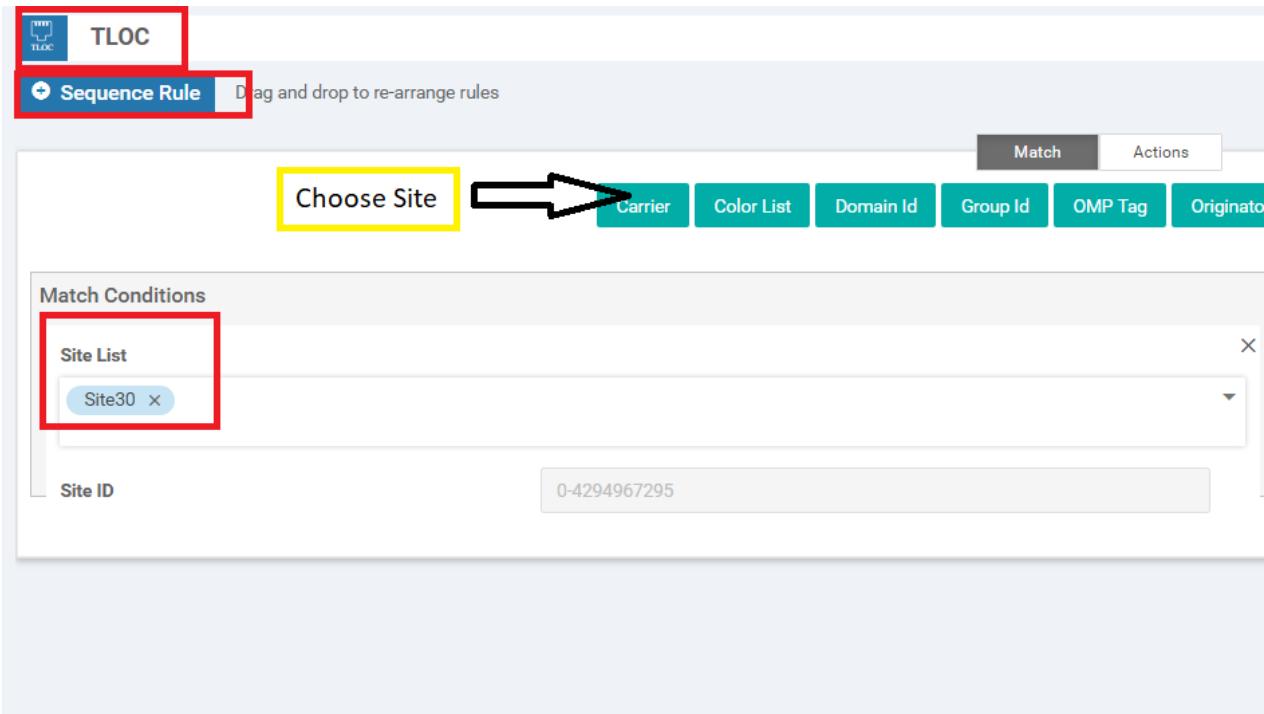
1. Continuing from the previous section, click on **Add Topology** and choose to add a **Custom Control (Route and TLOC)** topology

The screenshot shows the 'CONFIGURATION | POLICIES' interface with the 'Centralized Policy > Add Policy' path selected. The 'Topology' tab is active. A dropdown menu titled 'Add Topology' is open, showing options: 'Hub-and-Spoke', 'Mesh', and 'Custom Control (Route & TLOC)'. The 'Custom Control (Route & TLOC)' option is highlighted with a red box. Below the dropdown is a search bar labeled 'Search Options' and a link 'Import Existing Topology'. A table header with columns 'Type', 'Description', 'Reference Count', and 'Updated By' is visible, followed by the message 'No data available'.

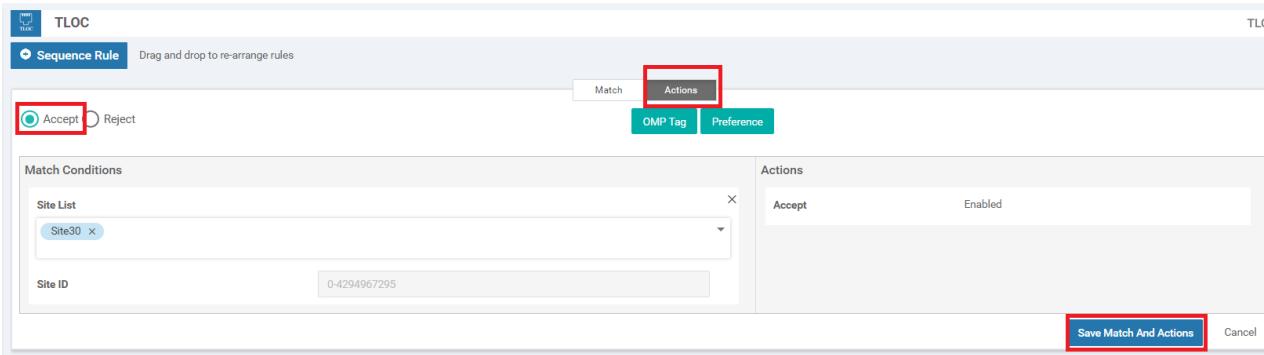
2. Give this Control Policy a Name of *Site20-to-Reg* and a Description of *Site 20 to Regional Hub at Site 30*. Click on **Sequence Type** and choose **TLOC**

The screenshot shows the 'CONFIGURATION | POLICIES' interface with the 'Add Custom Control Policy' path selected. The 'Name' field is set to 'Site20-to-Reg' and the 'Description' field is set to 'Site 20 to Regional Hub at Site 30'. The 'Sequence Type' dropdown is open, showing 'Route' and 'TLOC'. A modal window titled 'Add Control Policy' is open, showing two options: 'Route' and 'TLOC', with 'TLOC' highlighted with a red box.

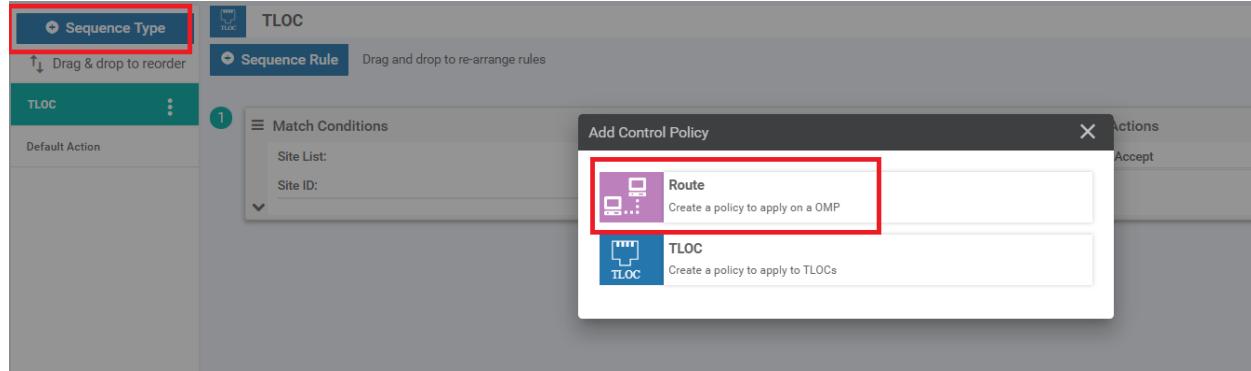
3. Choose to add a **Sequence Rule** and click on **Site** under **Match**. Populate the Site List as *Site30*



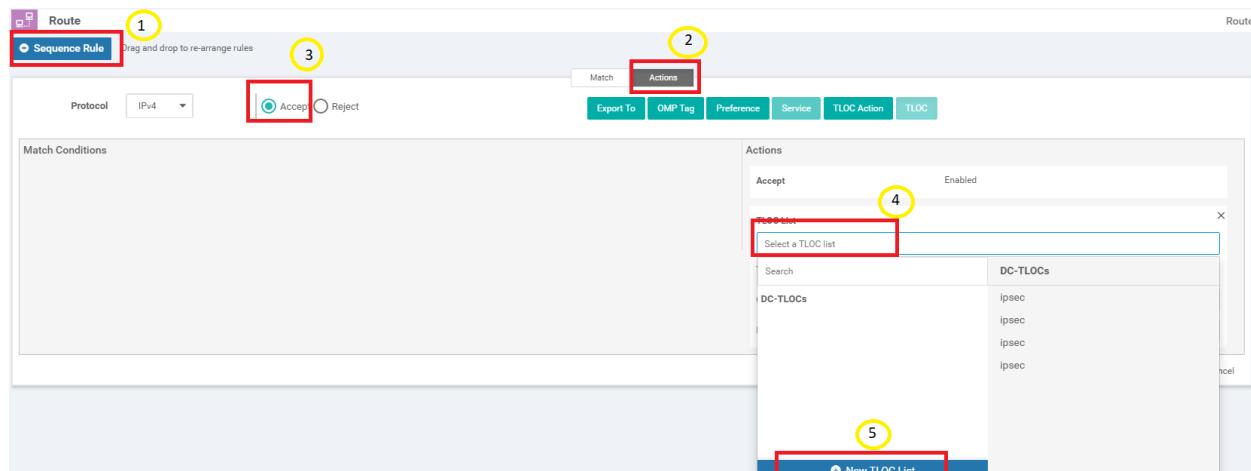
4. Go to the **Actions** tab and choose **Accept**. Click on **Save Match and Actions**



5. Click on **Sequence Type** again and this time choose **Route**



6. Click on **Sequence Rule** and go to the **Actions** tab. Click on **Accept** and click on **TLOC**. Click on the drop down for selecting a TLOC List and click on *New TLOC List*



7. Enter *Site30* as the List Name and choose to **Add TLOC**. This should give two rows. The TLOC IP is 10.255.255.31 (in both rows) and the Encap is *ipsec*. One row should have the color *public-internet* whereas the other row should have *mpls*. Click on **Save**

TLOC List

List Name
Site30

| TLOC IP | Color | Encap | Preference |
|---------------|-----------------|-------|--------------|
| 10.255.255.31 | public-internet | ipsec | 0-4294967295 |
| - | | | |
| 10.255.255.31 | mpls | ipsec | 0-4294967295 |
| - | | | |

+ Add TLOC

Save Cancel

8. Click on the drop-down for the TLOC List and choose the Site30 List we just created. Click on **Save Match and Actions**

TLOC List

Select a TLOC list

| Search | Site30 |
|---------------|---------------|
| DC-TLOCs | 10.255.255.31 |
| Site30 | 10.255.255.31 |

Cancel

Protocol: IPv4 | Accept | Reject | Export To | OMP Tag | Preference | Service | TLOC Action | TLOC

Match Conditions

Actions

Accept: Enabled

TLOC List: Site30

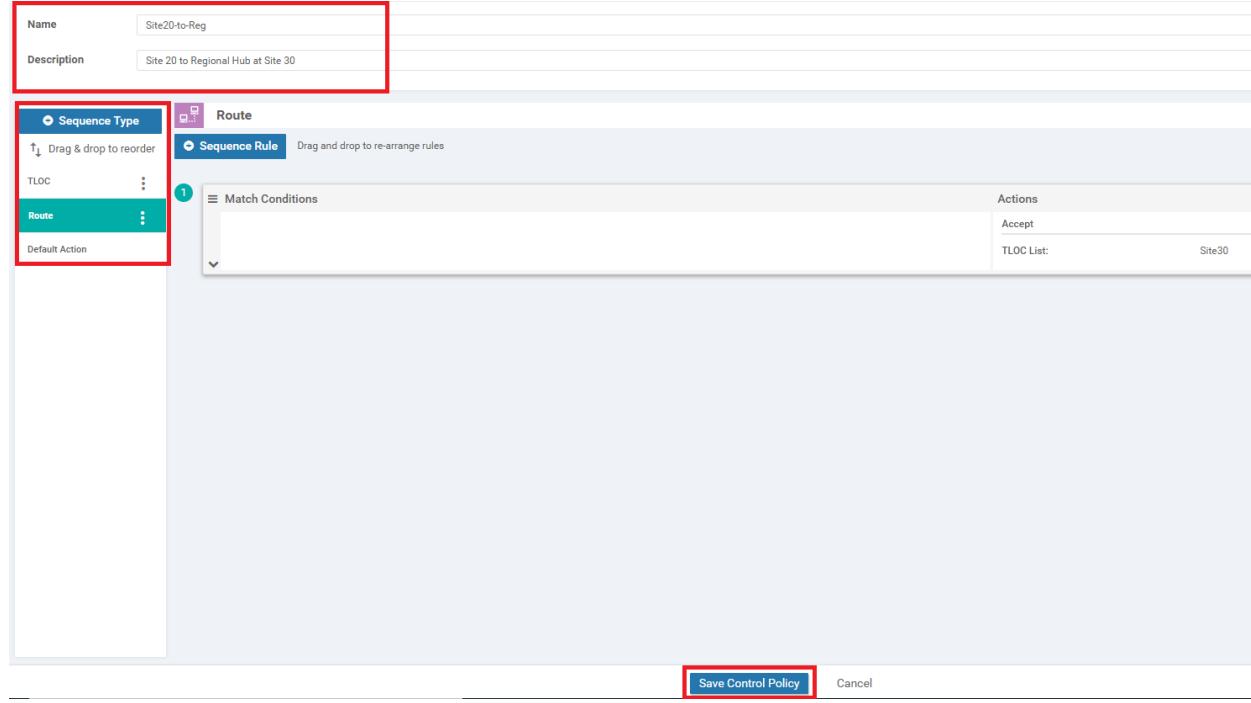
TLOC IP: Example: 10.0.0.1

Color: Select a color list

Encapsulation: Select an encaps

Save Match And Actions

9. Make sure the configuration looks like the image given below and click on **Save Control Policy**. Note that there are two Sequence Types - a TLOC and a Route, along with the Default Action



Continue with the next section for configuring another Control Policy.

Task List

- [Pre-Configuration](#)
- [Adding the Policy](#)
 - [Setting up Site Lists](#)
 - [Adding Custom Control policies](#)
 - [Policy for Traffic from Site 20 to the Regional Hub](#)
 - [Policy for Traffic from the Fabric to Site 20](#)
 - [Saving and Activating the Policy](#)
 - [Verification](#)

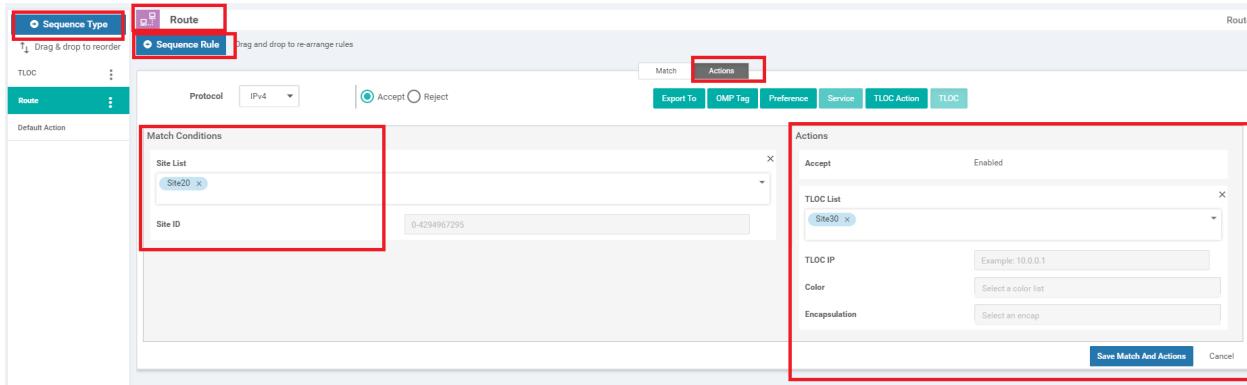
Policy for Traffic from the Fabric to Site 20

1. Back at the **Configure Topology and VPN Membership** page, click on **Add Topology**. We will add another **Custom Control (Route & TLOC)** policy

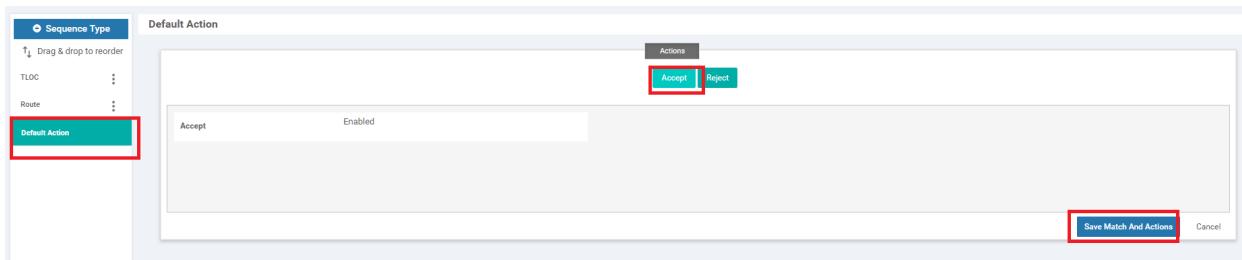
2. Give this Control Policy a name of *Fabric-to-Site20* with a Description of *Fabric traffic to Site 20*. Click on **Sequence Type** and choose **TLOC**. Click on **Sequence Rule** and select **Site** under Match. Populate *Site20* in the Site List. Click on **Save Match and Actions** since the default of Reject Enabled is what we want for this Control Policy

3. Click on **Sequence Type** again and choose **Route**. Click on **Sequence Rule** and choose **Site** under the Match tab. Populate *Site20* in the Site List. Click on the Actions tab and choose **Accept**. Click on **TLOC** and populate *Site30* from

the TLOC List drop down. Click on **Save Match and Actions**



4. Click on **Default Action** and choose **Accept**. Save *Match and Actions* to complete configuration of this Control Policy and click on **Save Control Policy**



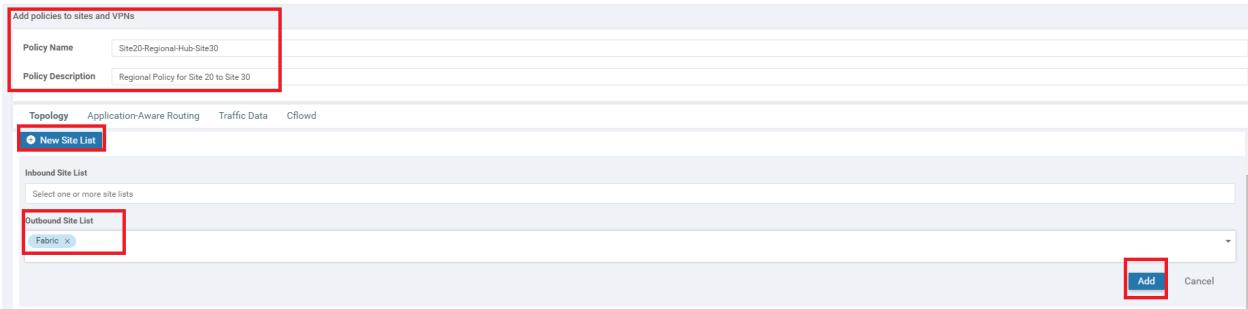
We will complete configuration of the Policy in the next section.

Task List

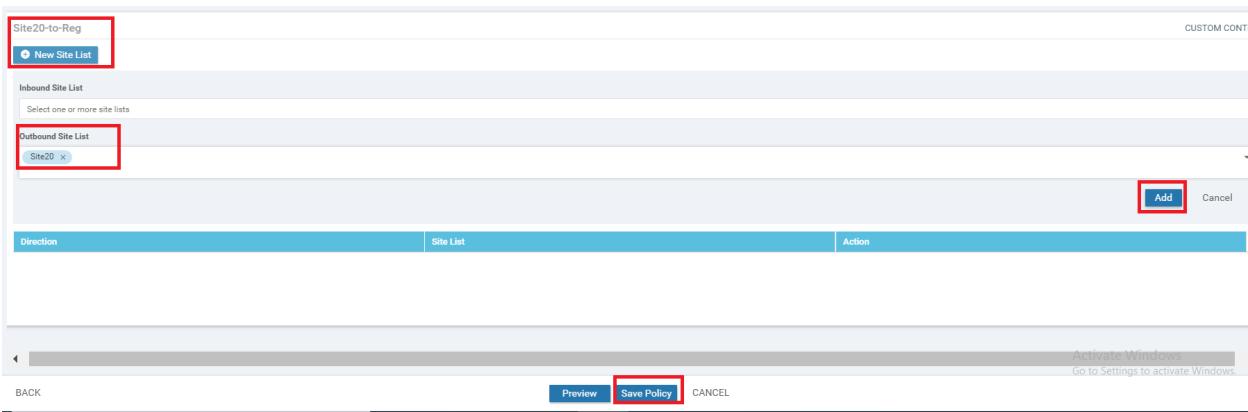
- [Pre-Configuration](#)
- [Adding the Policy](#)
 - [Setting up Site Lists](#)
 - [Adding Custom Control policies](#)
 - [Policy for Traffic from Site 20 to the Regional Hub](#)
 - [Policy for Traffic from the Fabric to Site 20](#)
 - [Saving and Activating the Policy](#)
- [Verification](#)

Saving and Activating the Policy

1. Click on **Next** two times from the page you're on at the end of the previous section (this should take you to the **Apply Policies to Sites and VPNs** page). Enter the Policy Name as *Site20-Regional-Hub-Site30* and the Description as *Regional Policy for Site 20 to Site 30*. Click on **New Site List** and populate *Fabric* in the Outbound Site List for the *Fabric-to-Site20* Custom Control Policy. Click on **Add**



2. Under the *Site20-to-Reg* Custom Control policy, click on **New Site List** and populate *Site20* in the Outbound Site List. Click on **Add** and then click on **Save Policy**



3. Click on the three dots next to the *Site20-Regional-Hub-Site30* policy and choose to **Activate** it

CONFIGURATION | POLICIES

Centralized Policy Localized Policy

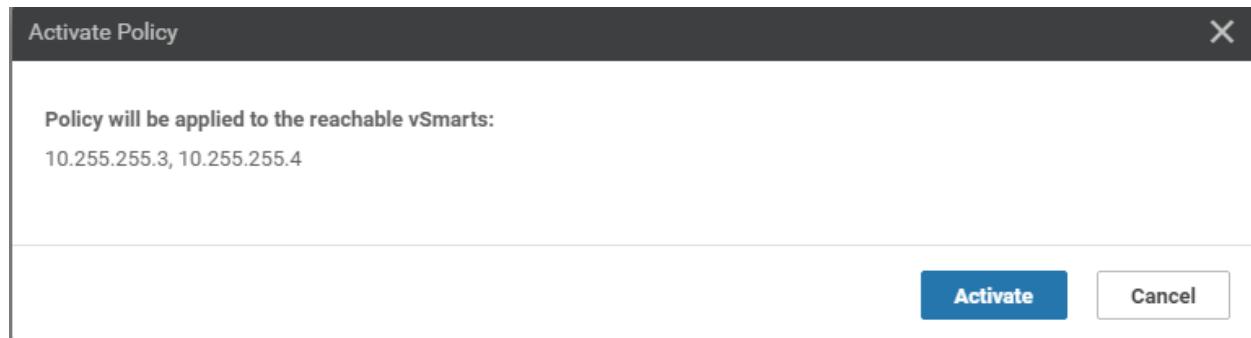
Add Policy

Search Options ▾

Total Rows: 2

| Name | Description | Type | Activated | Updated By | Policy Version | Last Updated | ... |
|----------------------------|--|-------------------|-----------|------------|--------------------|----------------------------|-----------------|
| Site20-Regional-Hub-Site30 | Regional Policy for Site 20 to Site 30 | UI Policy Builder | false | admin | 05282020T130912927 | 28 May 2020 6:09:12 AM PDT | Activate |
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 20 only | UI Policy Builder | false | admin | 05282020T100134900 | 28 May 2020 3:01:34 AM PDT | |

4. Confirm the Activation



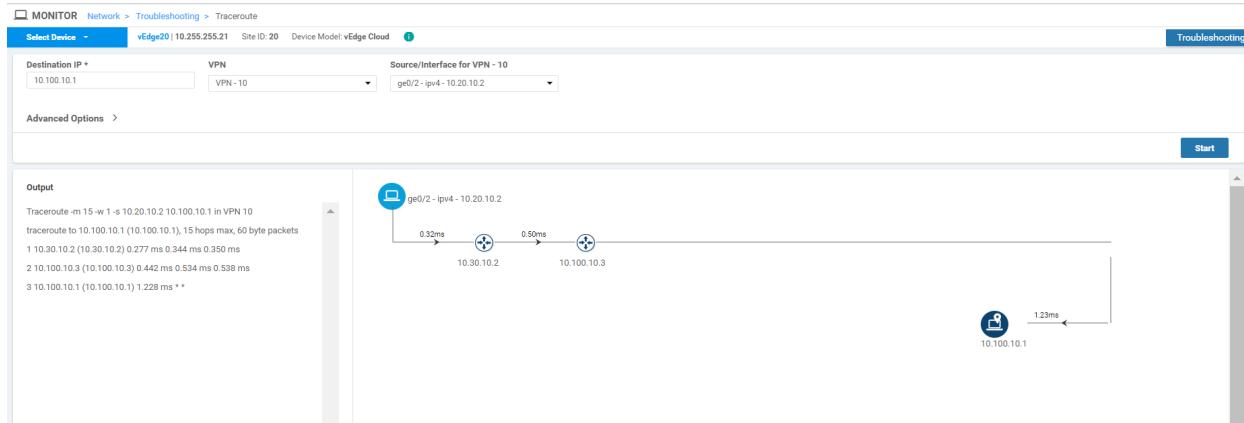
This completes the configuration of our Policy for making Site 30 a Regional Hub to Site 20. We will verify the configuration done in the next section.

Task List

- [Pre-Configuration](#)
- [Adding the Policy](#)
 - [Setting up Site Lists](#)
 - [Adding Custom Control policies](#)
 - [Policy for Traffic from Site 20 to the Regional Hub](#)
 - [Policy for Traffic from the Fabric to Site 20](#)
 - [Saving and Activating the Policy](#)
- [Verification](#)

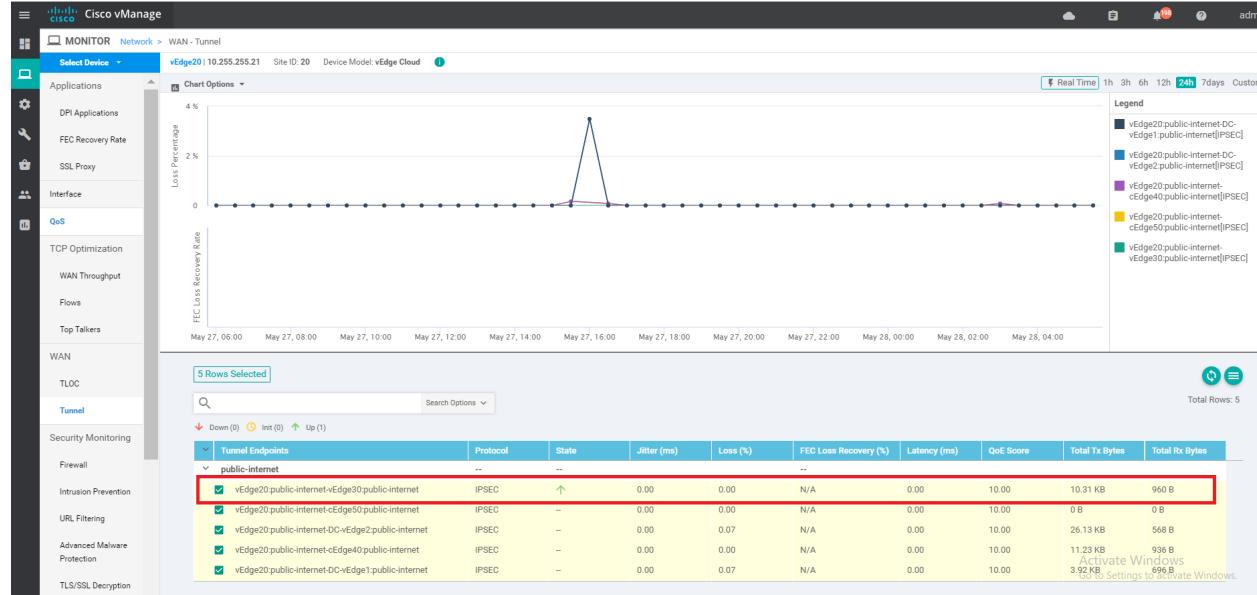
Verification

1. On the vManage GUI, navigate to **Monitor => Network** and click on **vEdge20**. Scroll down to Troubleshooting (on the left-hand side) and click on Trace Route. Enter the Destination IP as **10.100.10.1** with a VPN of **VPN - 10** and a Source/Interface of **ge0/2**. Click on **Start**

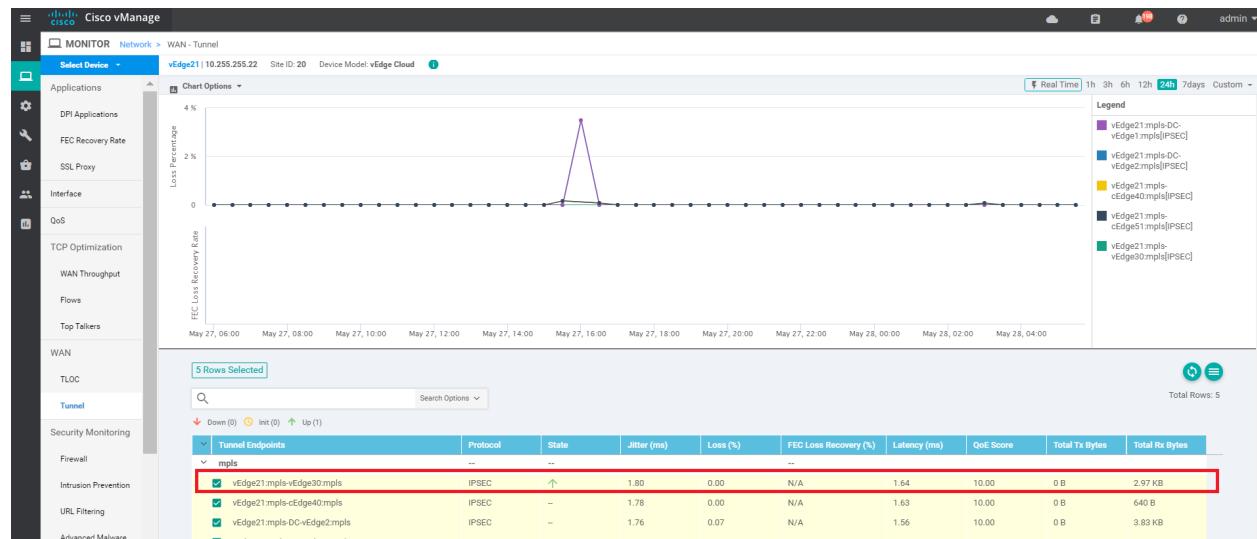


Notice that the traffic destined for the DC Service Side VPN is going through Site30 (10.30.10.2) and then getting routed over to the DC-vEdge.

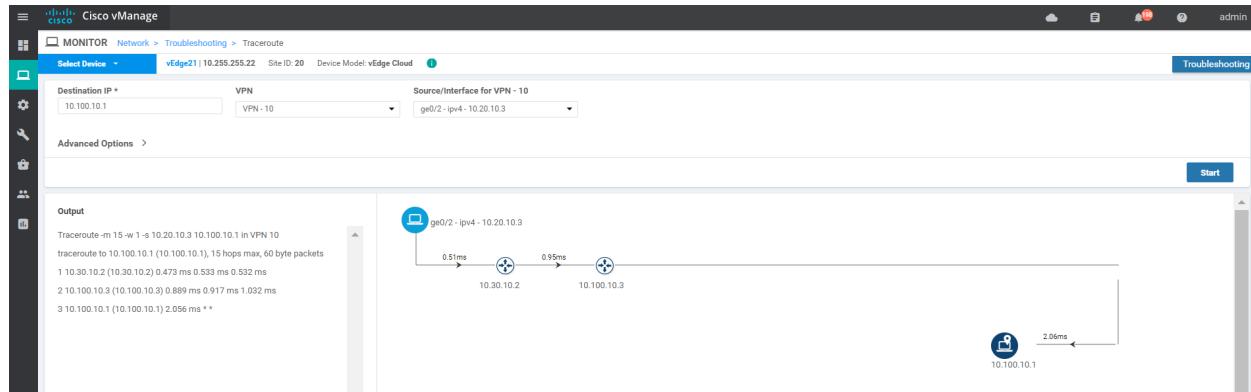
2. Click on **Tunnel** on the left-hand side and notice that vEdge20 has a single Up tunnel with vEdge30 on public-internet and one on mpls. Other tunnels are not up (as expected)



3. Click on **Select Device** in the top left-hand corner and choose **vEdge21**. You will notice a similar output here with respect to the Tunnels

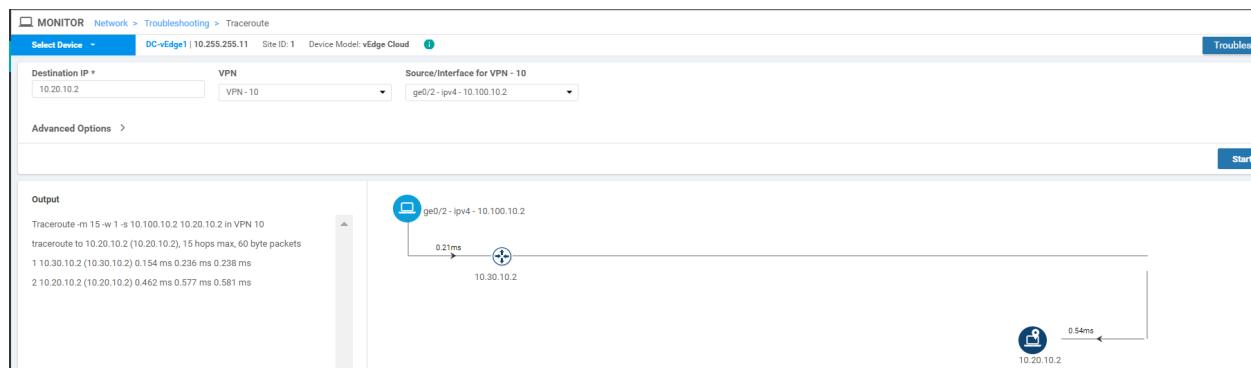


4. Go to **Troubleshooting => Trace Route** and enter the same details as before (i.e. a Destination of 10.100.10.1, VPN of VPN - 10 and a Source/Interface of ge0/2). Click on **Start**



We see that traffic from vEdge21 destined for the DC-vEdge Service Side VPN traverses vEdge30 (10.30.10.2) before being punted over to the DC-vEdge

5. To verify traffic flows towards Site20, choose **Select Device** from the top left-hand corner and select DC-vEdge1. Enter the Destination IP of 10.20.10.2 with a VPN of VPN - 10 and a Source/Interface of ge0/2. Click on Start



Notice that over here as well, traffic from the DC-vEdge goes to Site20 through Site30.

This completes the configuration of our Regional Hub.

Task List

- [Pre-Configuration](#)
- [Adding the Policy](#)
- [Setting up Site Lists](#)
- [Adding Custom Control policies](#)

- [Policy for Traffic from Site 20 to the Regional Hub](#)
- [Policy for Traffic from the Fabric to Site 20](#)
- [Saving and Activating the Policy](#)
- [Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 29, 2020

Site last generated: Sep 1, 2020



Implementing Custom Traffic Engineering

[Take a tour of this page](#)

Summary: Influencing Path selection and facilitating custom traffic engineering in Cisco SD-WAN

Table of Contents

- [Overview](#)
- [Deploying a Policy](#)
 - [Setting up Groups of Interest and Traffic Rules](#)
 - [Applying and Activating the Policy](#)
- [Verification](#)

Task List

- Overview
- Deploying a Policy
- Setting up Groups of Interest and Traffic Rules
- Applying and Activating the Policy
- Verification

Overview

The Cisco SD-WAN solution builds a full mesh topology by default and there isn't any traffic engineering that is in place out of the box. The ability to steer application traffic per the network requirements via a specific path is something that can be achieved via data policies. We can leverage data policies to match specific traffic and send it via the preferred transport. To verify current functionality:

1. Log in to the vManage GUI and navigate to **Monitor => Network**

The screenshot shows the Cisco vManage Main Dashboard. The left sidebar has a teal header "DASHBOARD | MAIN DASHBOARD" and a list of navigation items: Monitor (selected), Geography, Network (highlighted with a tooltip "Network"), Alarms, Events, Audit Log, Total (20), Authorized (20), Deployed (8), Staging (0), Top Applications (No data to display), and Application Health (WAN Edge - 8). The main area displays network status with a blue circular icon containing a white "X" and the text "WAN Edge - 8". A legend on the right shows Site Health: F (green checkmark), P (yellow circle), and N (red X).

2. Click on **vEdge30** and scroll down the list on the left-hand side to **Troubleshooting**

| Device Group | All | | Search Options | | |
|--------------|---------------|---------------------|------------------------------------|-------|--------------|
| Hostname | System IP | Device Model | Chassis Number/ID | State | Reachability |
| vManage | 10.255.255.1 | vManage | dfea63a5-66d2-4e50-a07b-ec4ad4... | | reachable |
| vSmart | 10.255.255.3 | vSmart | 20607a12-c0c8-4f46-a65f-5a547c... | | reachable |
| vSmart2 | 10.255.255.4 | vSmart | 7f332491-cb6f-4843-8bf5-060f90... | | reachable |
| vBond | 10.255.255.2 | vEdge Cloud (vBo... | fc31c154-99c5-4267-971d-6c9ae7... | | reachable |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b... | | reachable |
| DC-vEdge2 | 10.255.255.12 | vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-469966c... | | reachable |
| cEdge40 | 10.255.255.41 | CSR1000v | CSR-04F9482E-44F0-E4DC-D30D... | | reachable |
| cEdge50 | 10.255.255.51 | CSR1000v | CSR-834E40DC-E358-8DE1-0E81... | | reachable |
| cEdge51 | 10.255.255.52 | CSR1000v | CSR-D1837F36-6A1A-1850-7C1C... | | reachable |
| vEdge20 | 10.255.255.21 | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2ed... | | reachable |
| vEdge21 | 10.255.255.22 | vEdge Cloud | dde90ff0-dc62-77e6-510f-08d966... | | reachable |
| vEdge30 | 10.255.255.31 | vEdge Cloud | 17026153-f09e-be4b-6dce-482fce... | | reachable |

Security Monitoring

Firewall

Intrusion Prevention

URL Filtering

Advanced Malware

Protection

TLS/SSL Decryption

Umbrella DNS Re-
direct

Control Connections

System Status

Events

ACL Logs

Troubleshooting

Real Time

3. Click on **Simulate Flows**

Connectivity



Device Bringup

Control Connections(Live View)

Ping

Trace Route

Traffic



Tunnel Health

App Route Visualization

Simulate Flows

4. Enter VPN - 10 as the VPN, ge0/2 as the Source/Interface and 10.0.0.1 as the Destination IP. Click on **Simulate**

VPN* Source/Interface for VPN - 10* Source IP* Destination IP* Application

VPN - 10 ge0/2 - ipv4 - 10.30.10.2 10.30.10.2 10.0.0.1 Choose

Advanced Options >

Simulate

Output:

Total next hops: 4 | IPSec : 4

10.255.255.31

| | |
|--------|--------------------------------|
| → mpls | Remote System IP 10.255.255.12 |
| ← mpls | Encapsulation IPSec |

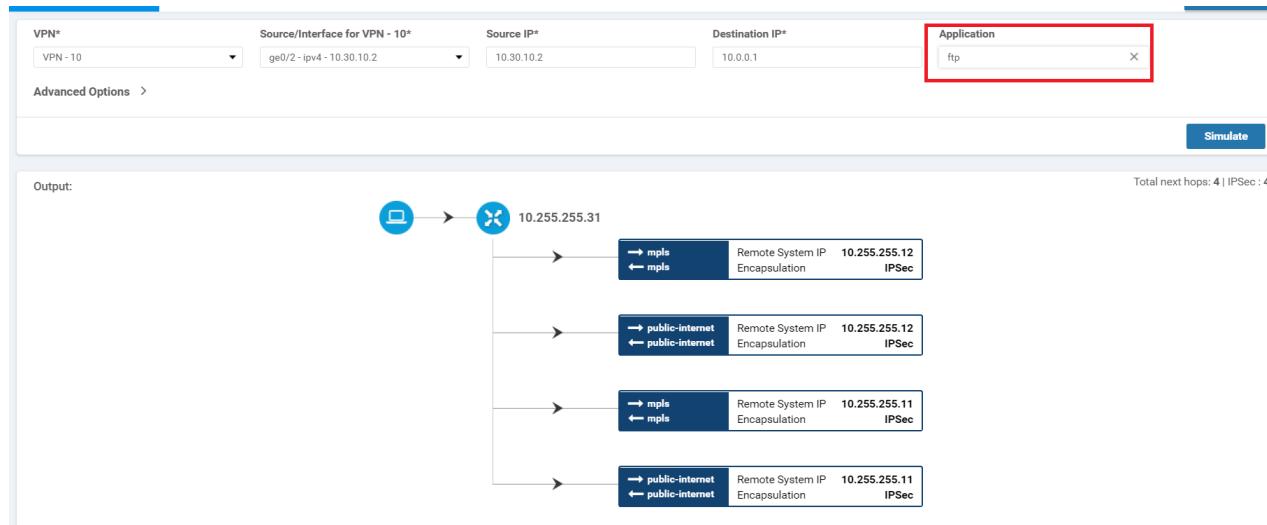
| | |
|-------------------|--------------------------------|
| → public-internet | Remote System IP 10.255.255.12 |
| ← public-internet | Encapsulation IPSec |

| | |
|--------|--------------------------------|
| → mpls | Remote System IP 10.255.255.11 |
| ← mpls | Encapsulation IPSec |

| | |
|-------------------|--------------------------------|
| → public-internet | Remote System IP 10.255.255.11 |
| ← public-internet | Encapsulation IPSec |

We find that general traffic uses all possible available transports to send data to the other side.

5. Keep all details the same, but this time choose **ftp** under Application. Click **Simulate**



Once again, ftp traffic is also attempting to take all possible transports.

In our example, we will assume that the requirement is to send FTP traffic over the MPLS link (preferred).

Task List

- [Overview](#)
- [Deploying a Policy](#)
- [Setting up Groups of Interest and Traffic Rules](#)
- [Applying and Activating the Policy](#)
- [Verification](#)

Deploying a Policy

We begin by creating a Policy and identifying **Groups of Interest** (or interesting traffic). The policy is then expanded to encompass a Data Policy.

[Setting up Groups of Interest and Traffic Rules](#)

1. On the vManage GUI, navigate to **Configuration => Policies**.

Cisco vManage

MONITOR Network > Troubleshooting > Simulate Flows

Select Device: vEdge30 | 10.255.255.31 Site ID: 30 Device Model: vEdge Cloud

Configuration

Devices

TLS/SSL Proxy

Certificates

Network Design

Templates

Policies

Security

Unified Communications

Cloud onRamp for SaaS

Cloud onRamp for IaaS

Cloud onRamp for Colocation

Source/Interface for VPN - 10*: ge0/2 - ipv4 - 10.30.10.2

Source IP*: 10.30.10.2

10.255.2

```
graph LR; Laptop((Laptop)) --> Cloud((10.255.2)); Cloud --> A(( )); Cloud --> B(( )); Cloud --> C(( )); Cloud --> D(( )); Cloud --> E(( ));
```

2. Under Centralized Policy, click on **Add Policy** to create a new Policy

CONFIGURATION | POLICIES

Centralized Policy Localized Policy

+ Add Policy



Search Options ▾

| Name | Description | Type | Activated |
|----------------------------|---------------------------------------|-------------------|-----------|
| Site20-Regional-Hub-Site30 | Regional Policy for Site 20 to Sit... | UI Policy Builder | true |
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 2... | UI Policy Builder | false |

3. We will be making use of the **Site30** Site List created before. Click on **Next** two times

[**New Site List**](#)

| Name | Entries | Reference Count |
|----------|----------------|-----------------|
| Site40 | 40 | 0 |
| Branches | 20, 30, 40, 50 | 2 |
| DC | 1 | 0 |
| Site20 | 20 | 2 |
| Site30 | 30 | 1 |
| Fabric | 1, 40, 50 | 1 |

[Next](#)

CANCEL

4. Make sure you are under **Configure Traffic Rules**. Click on the **Traffic Data** tab and choose to Add Policy. Click on **Create New**

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership **Configure Traffic Rules** Apply Policies to Sites

Choose a tab and add Traffic rules under the selected type

Traffic Data (Create a data policy)

Add Policy Create New Import Existing

| Name | Type | Description | Reference Count | Updated By |
|-------------------|------|-------------|-----------------|------------|
| No data available | | | | |

5. Given the policy a name of *ftp-mpls* and a description of *FTP via MPLS*. Click on **Sequence Type** and choose **Traffic Engineering** as the Data Policy

The screenshot shows the 'Add Data Policy' dialog box overlaid on a policy configuration interface. The dialog lists several options: Application Firewall, QoS, Service Chaining, **Traffic Engineering** (which is highlighted with a red box), and Custom. The main interface shows a policy named 'ftp-mpls' with a description 'FTP via MPLS'. The 'Sequence Type' section is also highlighted with a red box.

6. Click on **Sequence Rule** and choose **Application/Application Family List** as the match condition. Click on the drop-down for the Application/Application Family List and click on **New Application List**

Traffic Engineering

Sequence Rule Drag and drop to re-arrange rules

Protocol IPv4 | Application/Application Family List | Match Actions

Match Conditions

Application/Application Family List

Select an application list

Search

Google_Apps

Microsoft_Apps

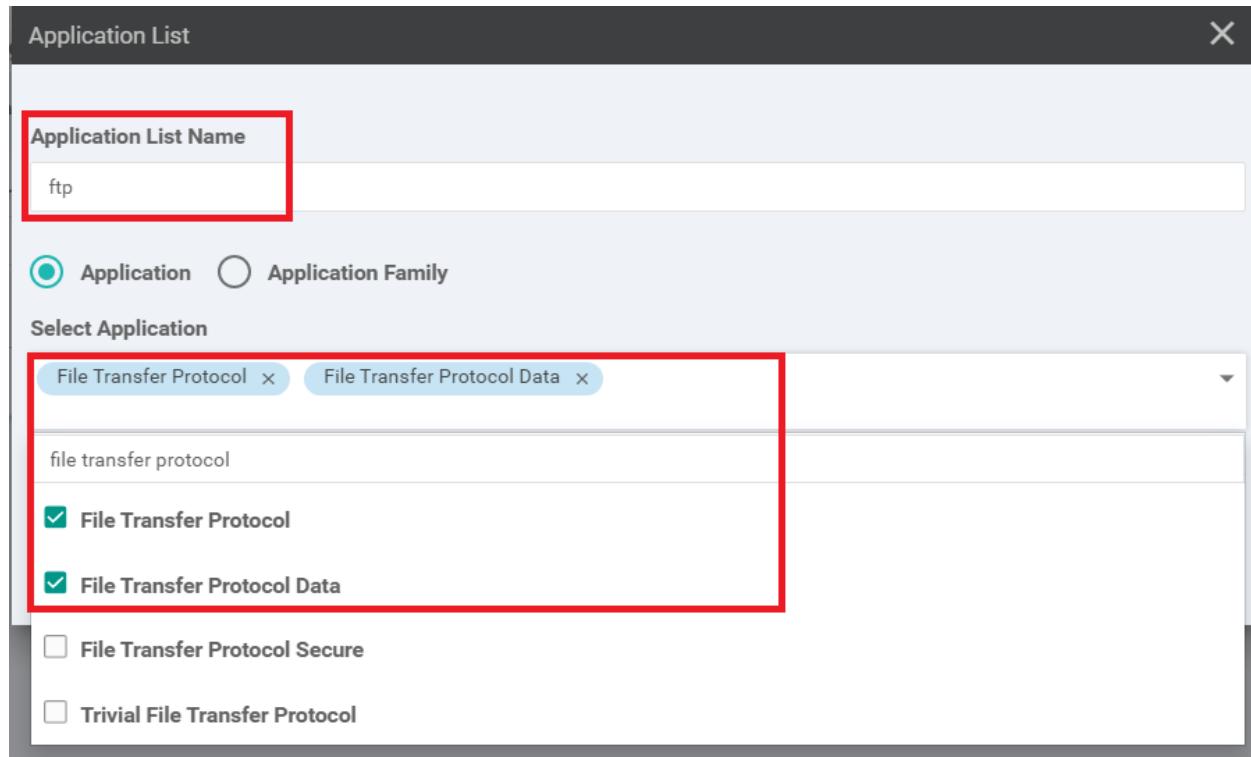
Actions

Accept

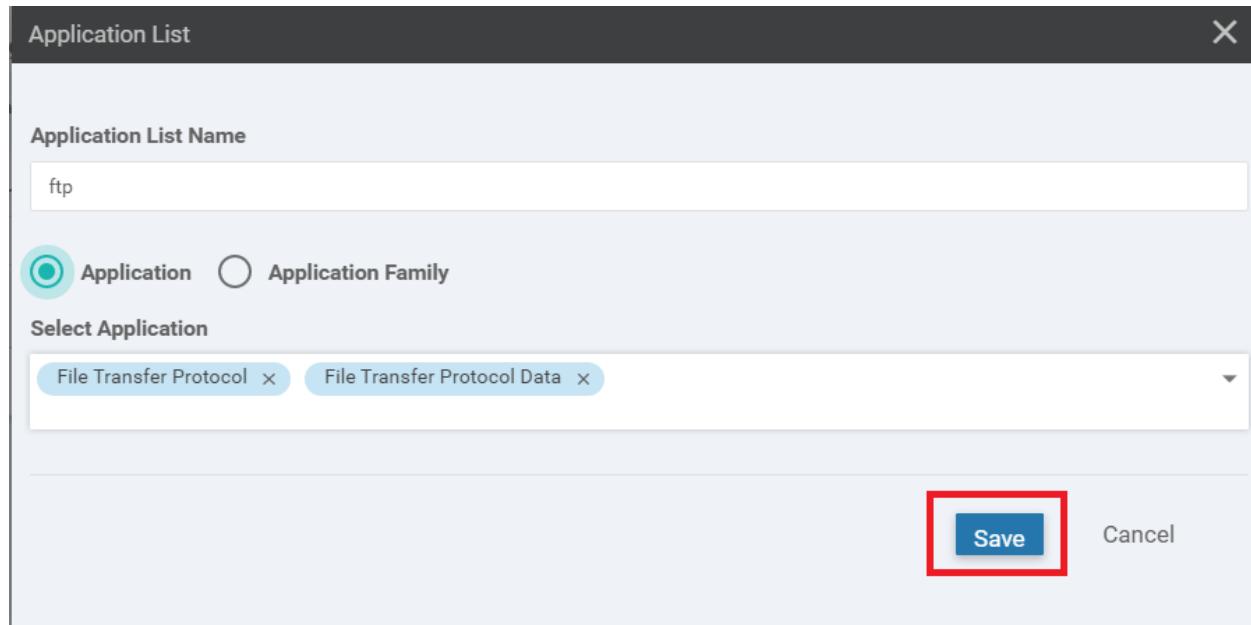
New Application List

The screenshot shows the 'Traffic Engineering' section with a 'Sequence Rule' selected. The 'Match' tab is active. In the 'Match Conditions' section, the 'Application/Application Family List' tab is selected, indicated by a red box around its header. Below it, there's a search bar and two application lists: 'Google_Apps' and 'Microsoft_Apps'. To the right, under 'Actions', there's an 'Accept' button. At the bottom of the modal, there's a blue button labeled 'New Application List' with a plus sign icon, also highlighted with a red box.

7. Give the Application List Name as *ftp* and select **File Transfer Protocol** and **File Transfer Protocol Data** under the **Select Application** drop down



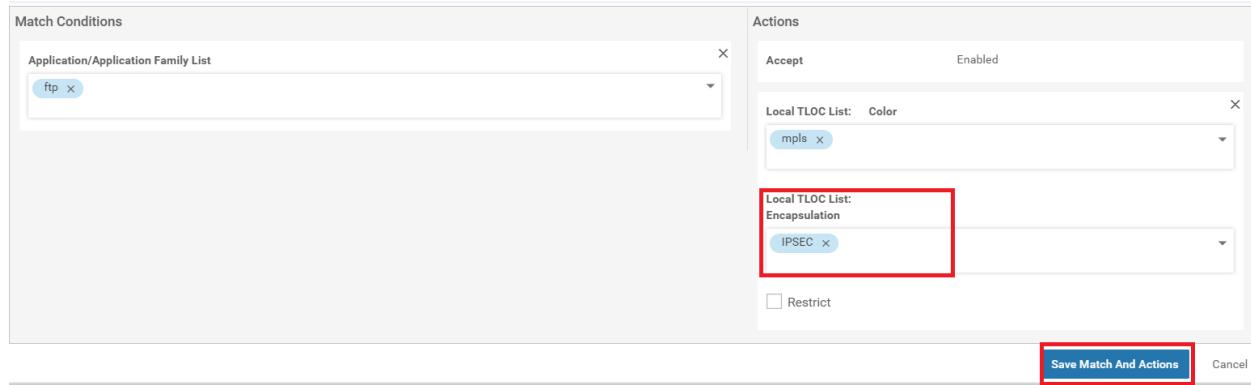
8. Make sure the Application List looks like the image below and click on **Save**. We are defining the *interesting* traffic over here via this Application List



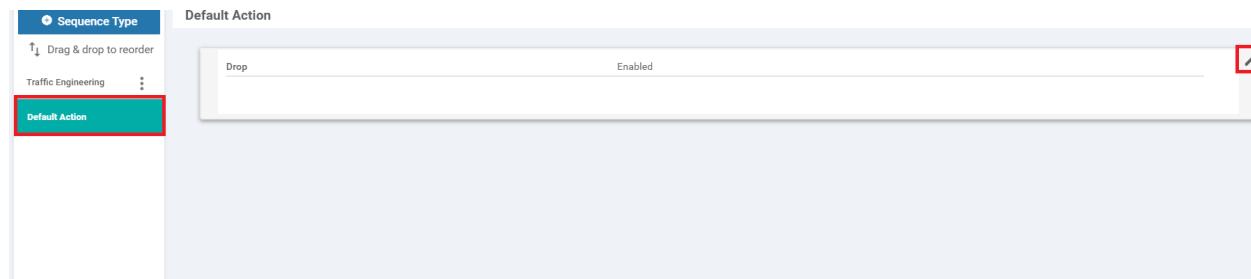
9. From the **Application/Application Family List** drop down, choose the *ftp* Application List we just created

The screenshot shows the 'Traffic Engineering' interface with a 'Sequence Rule' configuration. A modal window titled 'Application/Application Family List' is displayed, prompting the user to 'Select an application list'. Inside the modal, there is a search bar and a list of application lists. The 'ftp' list is selected and highlighted with a red box. To the right of the modal, an 'Accept' button is visible.

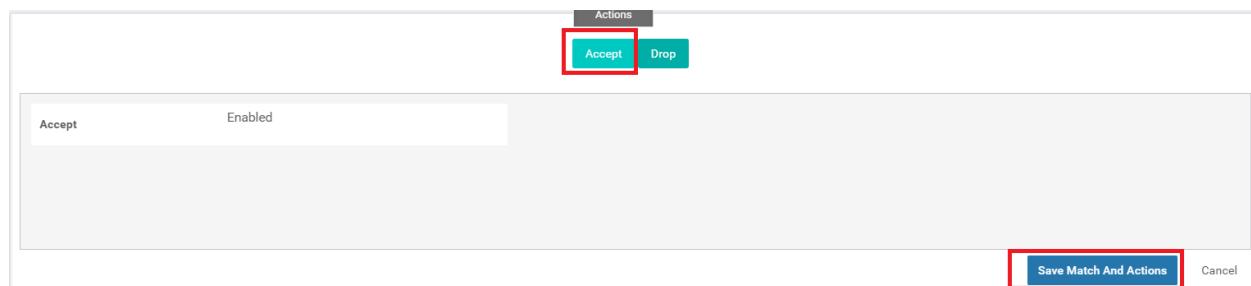
10. Click on the **Actions** tab and choose **Accept**. Select **Local TLOC** and choose the **Local TLOC List: Color** as *mpls*. Set the Local TLOC List: Encapsulation to **IPSEC**. Click on **Save Match and Actions**



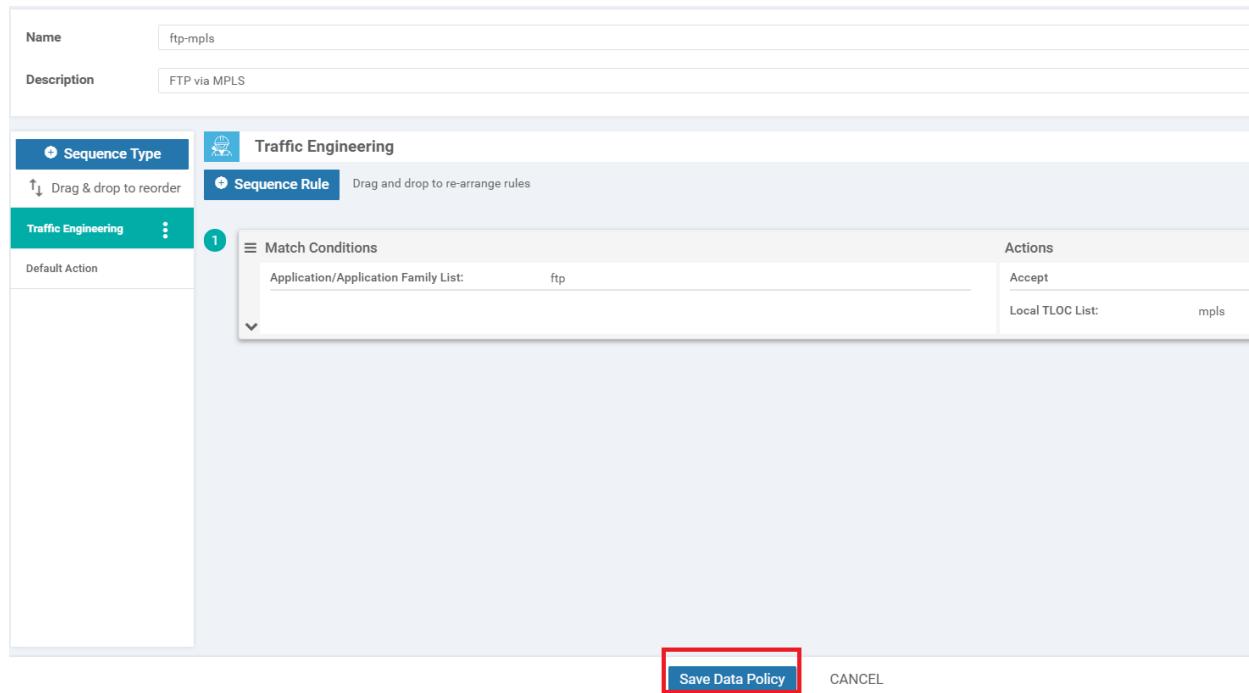
11. Choose **Default Action** on the left-hand side and click on the pencil icon to edit the default action



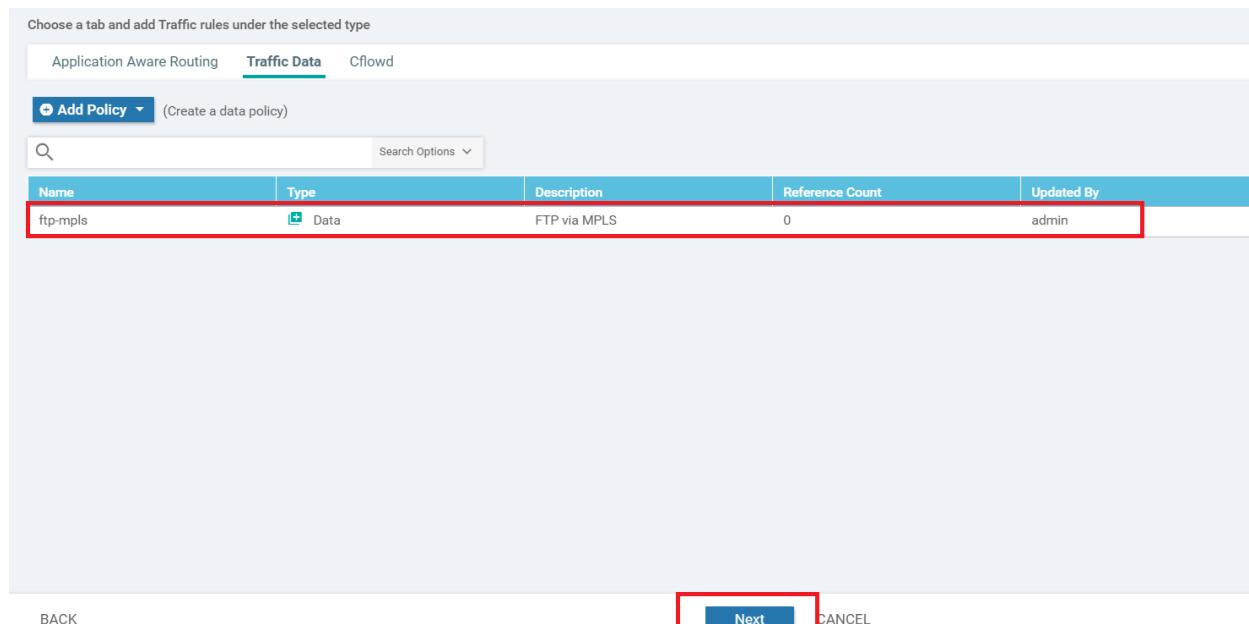
12. Select **Accept** and click on **Save Match and Actions**



13. Back at the Data Policy window, click on **Save Data Policy**



14. At the main Policy window, click on **Next**



Continue to the steps in the [next section](#).

Task List

- Overview
- Deploying a Policy
- ~~Setting up Groups of Interest and Traffic Rules~~
- Applying and Activating the Policy
- Verification

Applying and Activating the Policy

Continuing from the [Setting up Groups of Interest and Traffic Rules](#), we will now finalize our policy and activate it.

1. Give the Policy a name of *traffic-engineering-ftp* and a description of *Traffic Engineering for FTP*. Click on the **Traffic Data** tab and click on **New Site List and VPN List**. Leave the **From Service** radio button selected and populate *Site30* in Select Site List and *Corporate* in the Select VPN List. Click on **Add** and then click on **Save Policy**

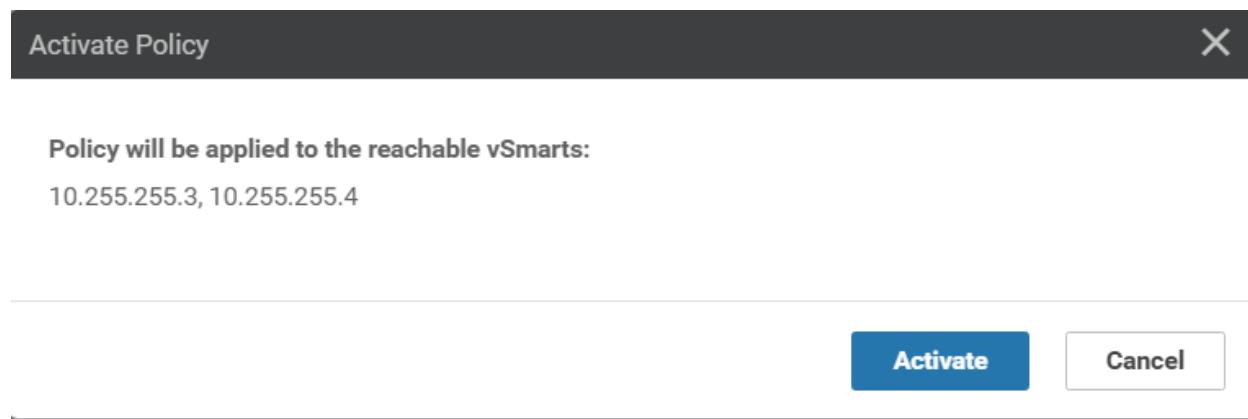


2. This should create our *traffic-engineering-ftp* policy. Click on the three dots next to it and choose **Activate**

| Name | Description | Type | Activated | Updated By | Policy Version | Last Updated | Actions |
|----------------------------|--|-------------------|-----------|------------|--------------------|----------------------------|--|
| Site20-Regional-Hub-Site30 | Regional Policy for Site 20 to Site 30 | UI Policy Builder | true | admin | 05282020T130912927 | 28 May 2020 6:09:12 AM PDT | ... |
| traffic-engineering-ftp | Traffic Engineering for FTP | UI Policy Builder | false | admin | 06032020T131902822 | 03 Jun 2020 6:19:02 AM PDT | ... |
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 20 | UI Policy Builder | false | admin | 05282020T100134900 | 28 May 2020 3:00:00 AM PDT | View Preview Copy Edit Delete Activate |

Tip: At this point we have created multiple policies and are activating them as we go along. However, this is not a standard practice. At a time, only one policy can be active so all our Policy requirements are generally concatenated into a single policy. Separate policies have been created in the lab for simplicity.

3. Click on **Activate**



We have now deployed our Policy.

Task List

- [Overview](#)
- [Deploying a Policy](#)
- [Setting up Groups of Interest and Traffic Rules](#)
- [Applying and Activating the Policy](#)
- [Verification](#)

Verification

In order to verify that traffic flows have changed, we will be comparing the output in the [Overview](#) section to out put which will be taken here.

1. On the vManage GUI, go to **Monitor => Network** and select vEdge30. Scroll down to **Troubleshooting** on the left-hand side and click on **Simulate Flows**

| Device Group | All | Search | Search Options | | |
|----------------|---------------|---------------------|------------------------------------|-------|--------------|
| Hostname | System IP | Device Model | Chassis Number/ID | State | Reachability |
| vmanage | 10.255.255.1 | vManage | dfea63a5-66d2-4e50-a07b-ec4ad4... | ✓ | reachable |
| vSmart | 10.255.255.3 | vSmart | 20607a12-c0c8-4f46-a65f-5a547c... | ✓ | reachable |
| vSmart2 | 10.255.255.4 | vSmart | 7f332491-cb6f-4843-8bf5-060f90... | ✓ | reachable |
| vBond | 10.255.255.2 | vEdge Cloud (vBo... | fc31c154-99c5-4267-971d-6c9ae7... | ✓ | reachable |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b... | ✓ | reachable |
| DC-vEdge2 | 10.255.255.12 | vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-469966c... | ✓ | reachable |
| cEdge40 | 10.255.255.41 | CSR1000v | CSR-04F9482E-44F0-E4DC-D30D... | ✓ | reachable |
| cEdge50 | 10.255.255.51 | CSR1000v | CSR-834E40DC-E358-8DE1-0E81... | ✓ | reachable |
| cEdge51 | 10.255.255.52 | CSR1000v | CSR-D1837F36-6A1A-1850-7C1C... | ✓ | reachable |
| vEdge20 | 10.255.255.21 | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2ed... | ✓ | reachable |
| vEdge21 | 10.255.255.22 | vEdge Cloud | dde90ff0-dc62-77e6-510f-08d966... | ✓ | reachable |
| vEdge30 | 10.255.255.31 | vEdge Cloud | 17026153-f09e-be4b-6dce-482fce... | ✓ | reachable |

Security Monitoring

Firewall

Intrusion Prevention

URL Filtering

Advanced Malware

Protection

TLS/SSL Decryption

Umbrella DNS Re-
direct

Control Connections

System Status

Events

ACL Logs

Troubleshooting

Real Time

Connectivity



Device Bringup

Control Connections(Live View)

Ping

Trace Route

Traffic



Tunnel Health

App Route Visualization

Simulate Flows

2. Enter VPN - 10 for the **VPN** and ge0/2 for the **Source/Interface**. The **Destination IP** will be 10.0.0.1. Click on **Simulate**

The screenshot shows the 'Simulate Flows' page in the vEdge Cloud monitor. The 'VPN*' dropdown is set to 'VPN - 10'. The 'Source/Interface for VPN - 10*' dropdown is set to 'ge0/2 - ipv4 - 10.30.10.2'. The 'Source IP*' field is set to '10.30.10.2' and the 'Destination IP*' field is set to '10.0.0.1'. The 'Simulate' button is highlighted with a red box. Below the form, a flow diagram illustrates the path of traffic from a source to a destination through different transport layers. The diagram shows three main stages: 1. A connection from a laptop icon to a vEdge 30 device icon (IP address 10.255.255.31). 2. The traffic then moves through an 'mpls' layer (encapsulation 'IPSec') to a 'public-internet' layer (encapsulation 'IPSec'). 3. Finally, it moves through another 'mpls' layer (encapsulation 'IPSec') to a 'public-internet' layer (encapsulation 'IPSec') before reaching the destination. The total number of hops is indicated as 4.

We can see that general traffic is still attempting to use all possible transports.

3. Set the **Application** to *ftp* and click on **Simulate**

Screenshot of a network configuration interface showing a VPN policy setup. The 'Application' field is highlighted with a red box, containing the value 'ftp'. The 'Simulate' button is also highlighted with a red box. The 'Output' section shows a flow diagram starting from a computer icon, passing through a switch node labeled '10.255.255.31', and then splitting into two parallel paths. Each path contains an 'mpls' box with arrows indicating bidirectional traffic. The top path leads to a box labeled 'Remote System IP 10.255.255.12 Encapsulation IPSec'. The bottom path leads to a box labeled 'Remote System IP 10.255.255.11 Encapsulation IPSec'. A note at the top right states 'Total next hops: 2 | IPSec : 2'.

FTP Traffic now flows via the MPLS transport, as per our requirement.

This completes the verification activity for this section.

Task List

- [Overview](#)
- [Deploying a Policy](#)
- [Setting up Groups of Interest and Traffic Rules](#)
- [Applying and Activating the Policy](#)
- [Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: May 29, 2020

Site last generated: Jul 23, 2020



-->

Implementing Direct Internet Access

Summary: Setting up a Direct Internet Access policy for Guest Users at Site 40

Table of Contents

- [Overview](#)
- [Creating and Activating a Policy](#)
- [Verification](#)

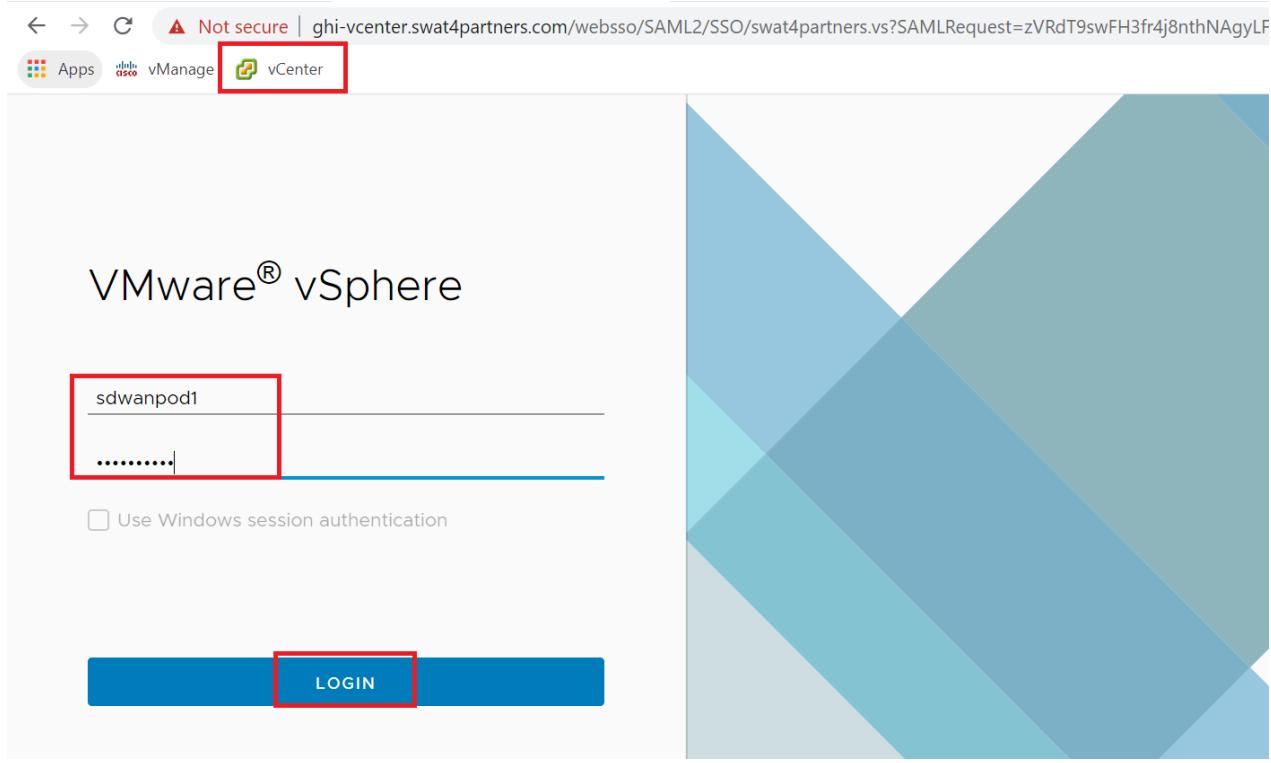
Task List

- Overview
- Creating and Activating a Policy
- Verification

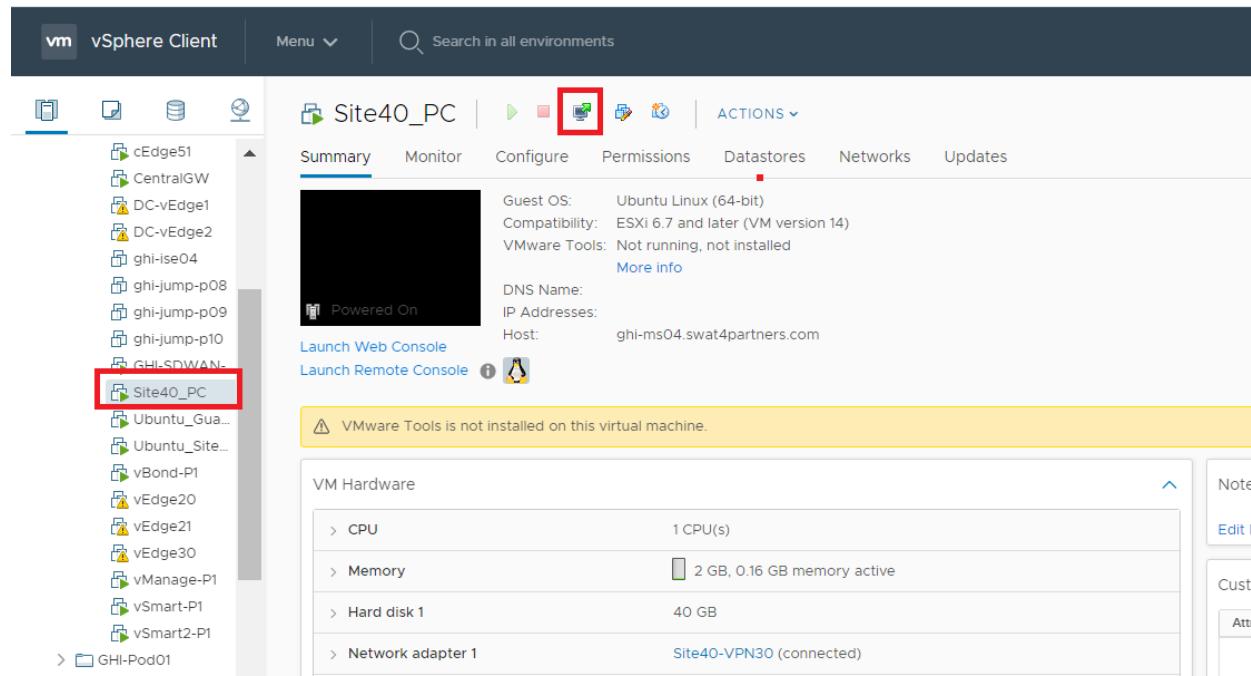
Overview

We will now shift focus to setting up our DIA site at Site40. Guest users will connect on VPN 30 and we need to ensure they have access to the Internet. We will first verify that the PC at Site 40 does not have Internet access. The WAN Interface at Site 40 on *public-internet* will then be updated for NAT and a Policy will be applied (which will include a Data Prefix list and a Data Policy) to allow users on VPN 30 to access the Internet.

1. Click on the bookmark for vCenter in Google Chrome or navigate to <https://10.2.1.50/ui>. Enter the credentials provided for your POD and click on **Login**

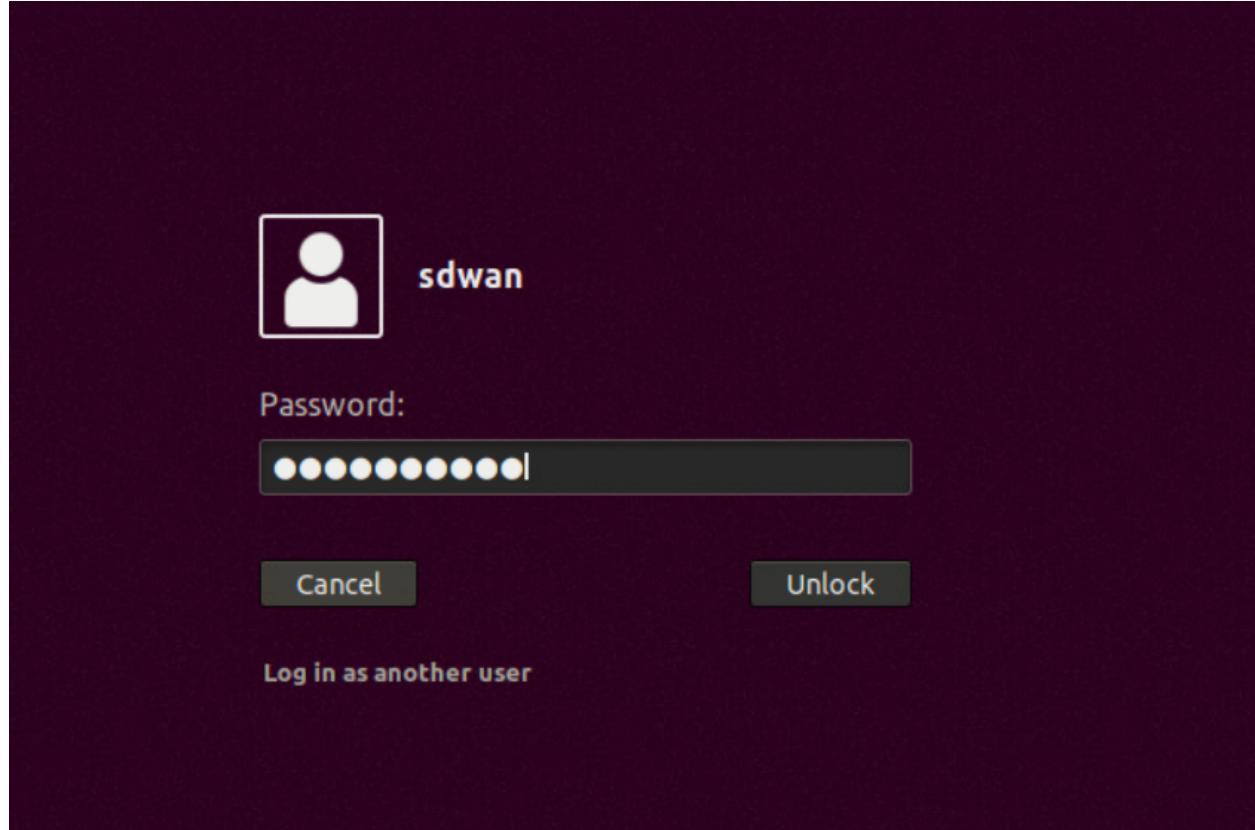


- Locate the Site40 PC (it will be named *sdwan-YYY-site40pc-podX* where YYY are some characters and X is your POD number, image uses Site40_PC). Click on it and click on the icon to open a console session. Choose to open the Web Console, if prompted

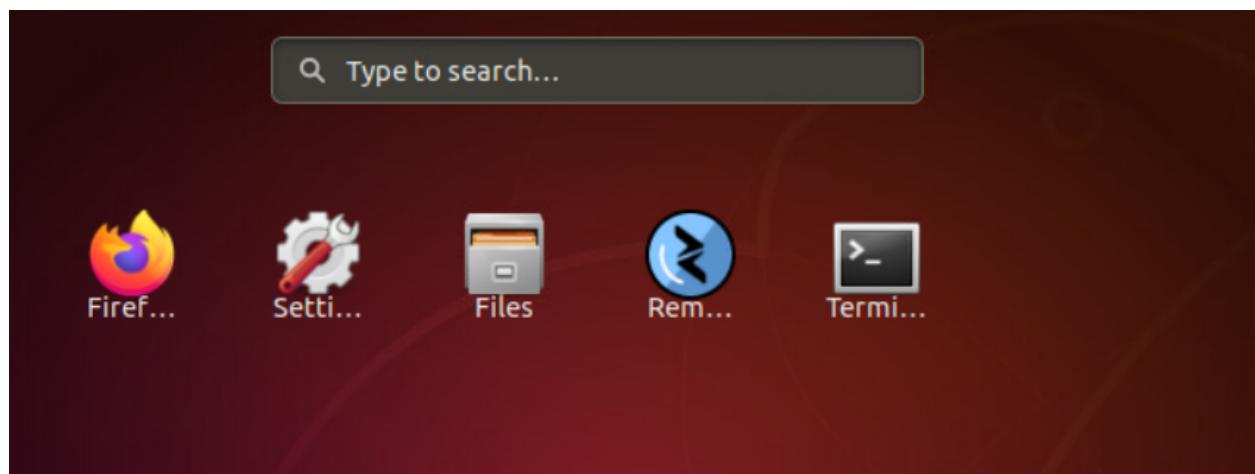


3. Navigate to the console window/tab and click on the *sdwan* user to log in. The password is *C1sco12345*

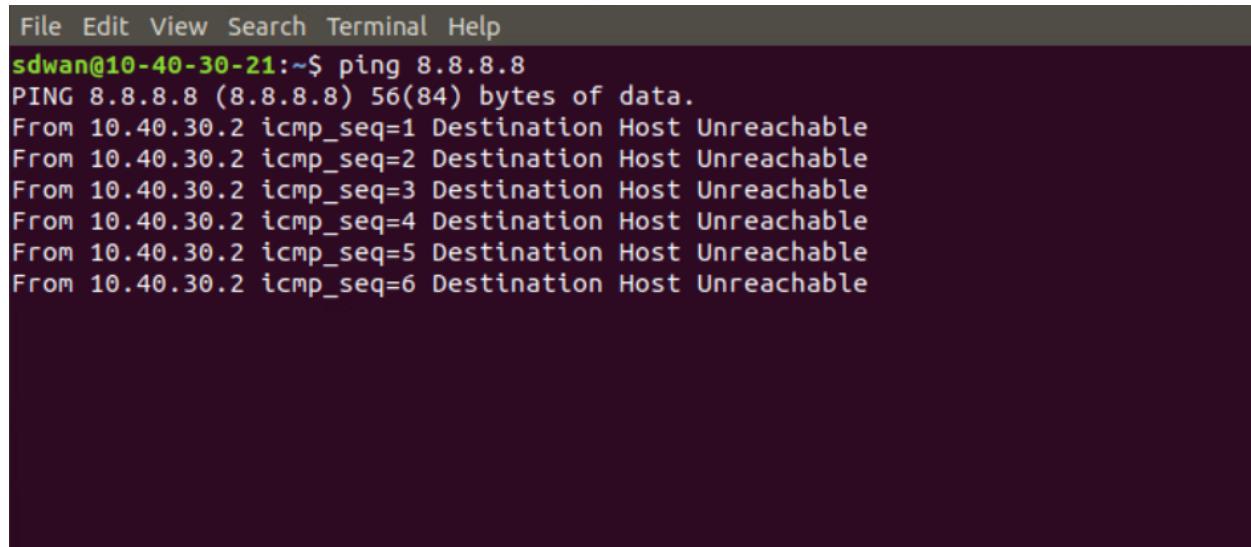
Note: If the machine hangs at the login window and doesn't show the Ubuntu Desktop, please power off and power on the Site40PC VM for your POD from vCenter.



4. Click on the Ubuntu equivalent of the Start button - it's the button in the bottom left hand corner and search for **terminal**. Open the terminal application



5. Type `ping 8.8.8.8` and hit Enter. Pings should fail



A terminal window titled "File Edit View Search Terminal Help". The command `sdwan@10-40-30-21:~$ ping 8.8.8.8` is run, followed by six lines of output: "PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data." and "From 10.40.30.2 icmp_seq=1 Destination Host Unreachable" repeated six times.

We have thus verified that the Guest VPN user (with an IP of 10.40.30.21) doesn't have internet access.

Task List

- [Overview](#)
- [Creating and Activating a Policy](#)
- [Verification](#)

Creating and Activating a Policy

We will start by enabling NAT on the Internet interface and then continue with our Policy.

1. On the vManage GUI, navigate to **Configuration => Templates => Feature Tab**. Locate the `cedge-vpn0-int-dual` template created before and click on the three dots next to it. Choose to **Edit** the template

CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type Non-Default Search Options

Total Rows: 34

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------|---------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|---------|
| DC-vEdge_INET | INET Interface for the DC-vE... | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 1:39:02 AM PDT | ... |
| DC OSPF | OSPF Template for the DC | OSPF | vEdge Cloud | 1 | 2 | admin | 25 May 2020 11:32:28 PM | ... |
| cedge-vpn30 | VPN 30 Template for the cE... | Cisco VPN | CSR1000v | 2 | 3 | admin | 25 May 2020 1:57:26 PM PDT | ... |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for S... | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 1:24:18 PM PDT | ... |
| vSmart-VPN0-Int | VPN0 Interface for vSmarts | vSmart Interface | vSmart | 1 | 2 | admin | 25 May 2020 9:59:00 AM PDT | ... |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Tem... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 18 May 2020 8:28:19 AM PDT | ... |
| Site20_vpn0_Ext | VPN0 Interface for Site20 d... | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May 2020 11:32:28 PM | ... |
| DCvEdge-vpn512 | VPN512 for the DC-vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 23 May 2020 11:32:28 PM | ... |
| cedge-vpn20-int | VPN 20 Interface Template ... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 25 May 2020 1:24:18 PM PDT | ... |
| vSmart-vpn512-int | VPNs12 Interface Template ... | vSmart Interface | vSmart | 1 | 2 | admin | 25 May 2020 1:24:18 PM PDT | ... |
| DCvEdge-vpn0 | VPN0 for the DC-Edges IN... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 25 May 2020 1:24:18 PM PDT | ... |

2. Scroll down to the **NAT** section and set NAT to a Global value of **On**. Click on **Update**

Basic Configuration Tunnel **NAT** VRRP ACL/QoS ARP Advanced

NAT

IPv4 IPv6

NAT **On** **Off**

NAT Type **Interface** **Pool** **Loopback**

UDP Timeout 1

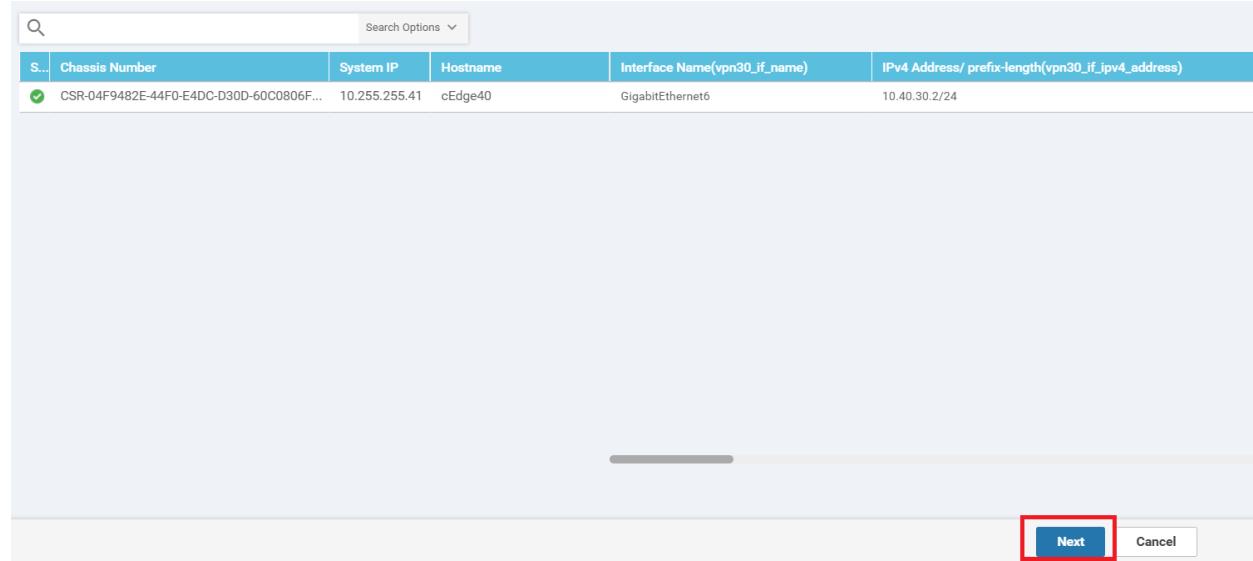
TCP Timeout 60

+ New Static NAT

| | | | | |
|----------|-----------|--------------|----------------------|----------|
| Optional | Source IP | Translate IP | Static NAT Direction | Source V |
|----------|-----------|--------------|----------------------|----------|

Update Cancel

3. Click on **Next** since we don't need to change anything on the device settings and then click on **Configure Devices**. You can view the side-by-side configuration if you want to



'Configure' action will be applied to 1 device(s)
attached to 1 device template(s).

| Local Configuration | New Configuration |
|--------------------------------------|--------------------------------------|
| 1 system | 1 system |
| 2 host-name cEdge40 | 2 host-name cEdge40 |
| 3 system-ip 10.255.255.41 | 3 system-ip 10.255.255.41 |
| 4 overlay-id 1 | 4 overlay-id 1 |
| 5 site-id 40 | 5 site-id 40 |
| 6 port-offset 1 | 6 port-offset 1 |
| 7 control-session-pps 300 | 7 control-session-pps 300 |
| 8 admin-tech-on-failure | 8 admin-tech-on-failure |
| 9 sp-organization-name swat-sdwanlab | 9 sp-organization-name swat-sdwanlab |
| 10 organization-name swat-sdwanlab | 10 organization-name swat-sdwanlab |
| 11 port-hop | 11 port-hop |
| 12 track-transport | 12 track-transport |
| 13 track-default-gateway | 13 track-default-gateway |
| 14 console-baud-rate 19200 | 14 console-baud-rate 19200 |
| 15 vbond 100.100.100.3 port 12346 | 15 vbond 100.100.100.3 port 12346 |
| 16 logging | 16 logging |
| 17 disk | 17 disk |
| 18 enable | 18 enable |
| 19 ! | 19 ! |
| 20 ! | 20 ! |
| 21 ! | 21 ! |
| 22 bfd color lte | 22 bfd color lte |

NAT should now be enabled on the public-internet transport

4. Navigate to Configuration => Policies on the vManage GUI and click on Add Policy

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | POLICIES' section. The 'Centralized Policy' tab is selected. A red box highlights the 'Add Policy' button in the top-left corner of the main content area. Below it is a search bar and a table listing existing policies.

| Name | Description | Type | Activated | Updated By |
|----------------------------|---------------------------------------|-------------------|-----------|------------|
| Site20-Regional-Hub-Site30 | Regional Policy for Site 20 to Sit... | UI Policy Builder | false | admin |
| traffic-engineering-ftp | Traffic Engineering for FTP | UI Policy Builder | true | admin |
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 2... | UI Policy Builder | false | admin |

5. Select **Data Prefix List** on the left-hand side under Create Groups of Interest and choose **New Data Prefix List**. Give it a name of *Guest-Site40* and specify the **Add Data Prefix** as *10.40.30.0/24*. Click on **Add** and then click on **Next** (please click on Add BEFORE clicking on Next else the Data Prefix List will not get added)

The screenshot shows the 'Create Groups of Interest' wizard, step 1 of 6. The 'Data Prefix' option is selected on the left sidebar. A red box highlights the 'New Data Prefix List' button. The main form shows the 'Data Prefix List Name' set to 'Guest-Site40'. The 'Internet Protocol' section has 'IPv4' selected. The 'Add Data Prefix' field contains '10.40.30.0/24'. The 'Add' button is highlighted with a red box. Step numbers 1 through 6 are circled in yellow to guide the user through the process.

Click on **Next** on the **Configure Topology and VPN Membership** screen.

6. On the **Configure Traffic Rules** screen, click on the **Traffic Data** tab and choose **Add Policy**. Click on **Create New**

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership Configure Traffic Rules

Choose a tab and add Traffic rules under the selected type

Application Aware Routing **Traffic Data** Cflowd

Add Policy (Create a data policy)

Create New Import Existing

No data available

7. Give the Data Policy a name of **Guest-DIA** with a Description of **Guest DIA at Site 40**. Click on **Sequence Type** and choose **Custom**

CONFIGURATION | POLICIES Add Data Policy

Name: Guest-DIA
Description: Guest DIA at Site 40

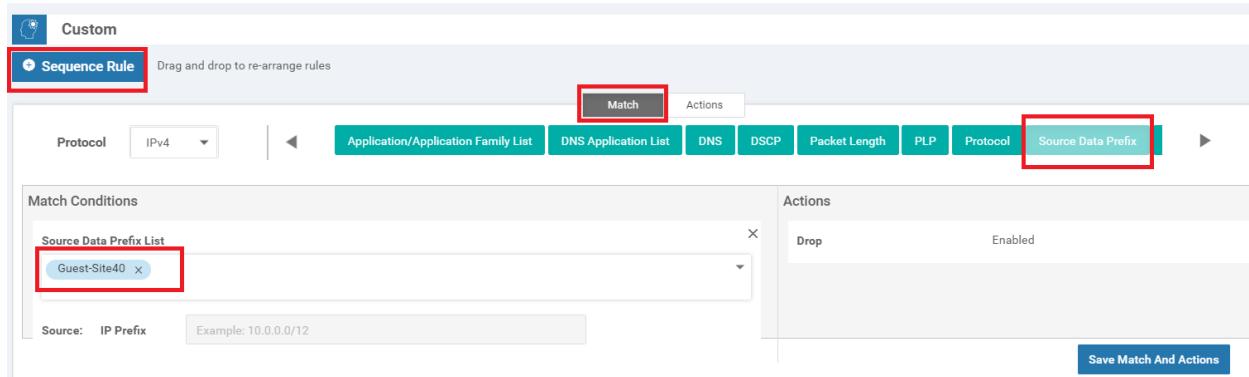
+ Sequence Type Drag & drop to reorder

Default Action: Drop

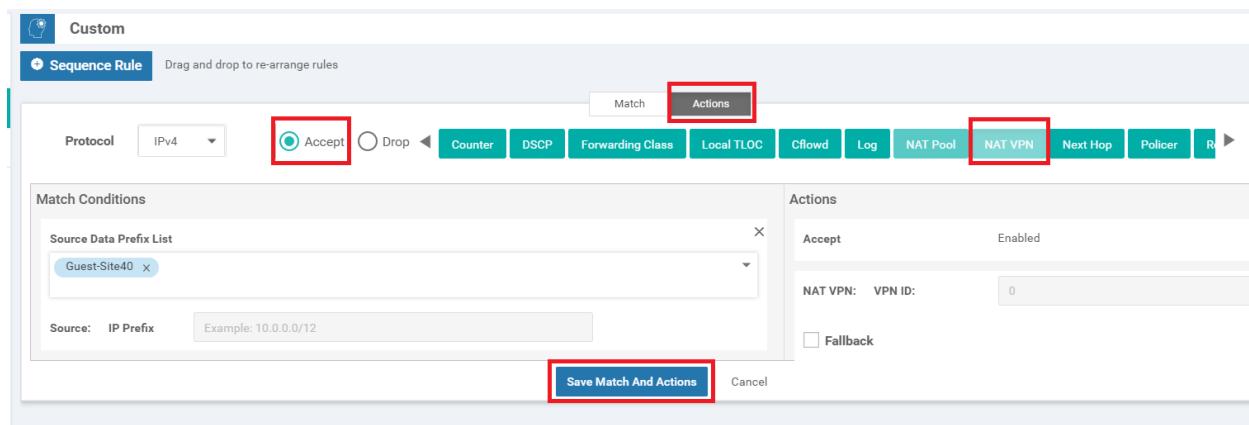
Add Data Policy

- Application Firewall**: Direct application traffic to a firewall.
- QoS**: Class/QoS maps for packet forwarding.
- Service Chaining**: Rerouting data traffic through firewalls, load balancers and IDP's.
- Traffic Engineering**: Direct control traffic along a desired path.
- Custom**: Create a custom policy.

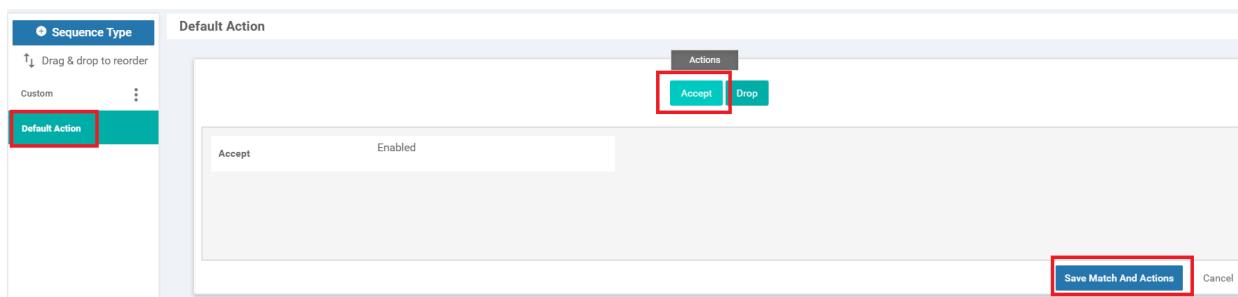
8. Click on **Sequence Rule** and select **Source Data Prefix** under Match. Populate **Guest-Site40** in the Source Data Prefix List (we just created this Data Prefix list)



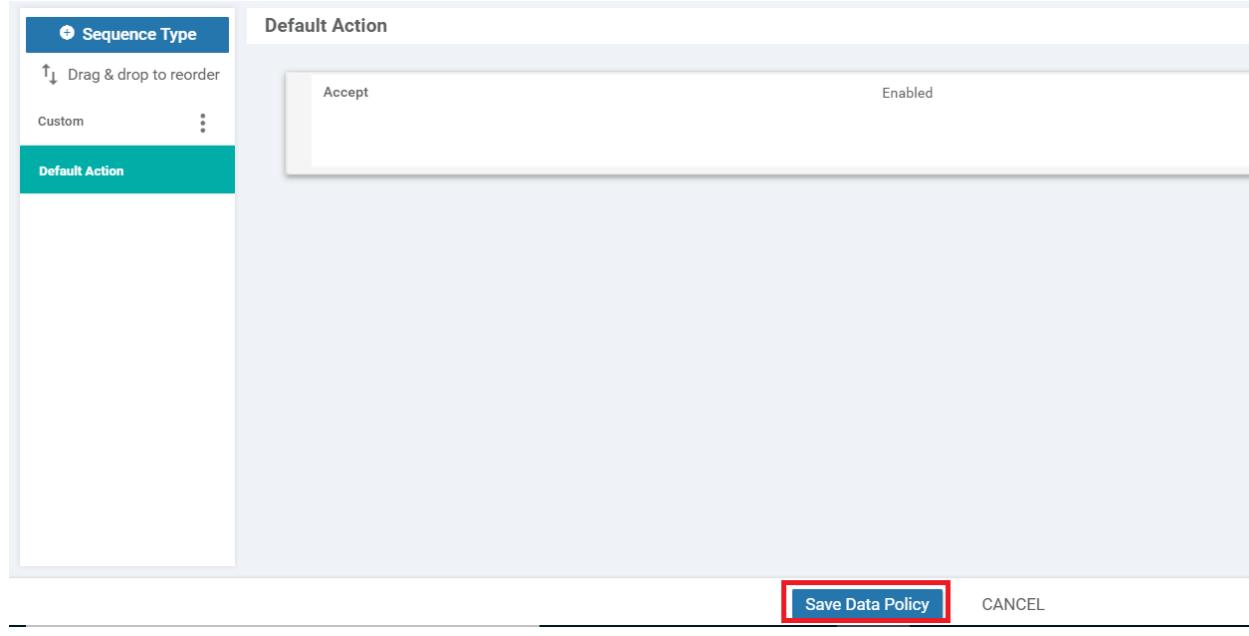
9. Click on the **Actions** tab and choose the **Accept** radio button. Select **NAT VPN** and click on **Save Match and Actions**



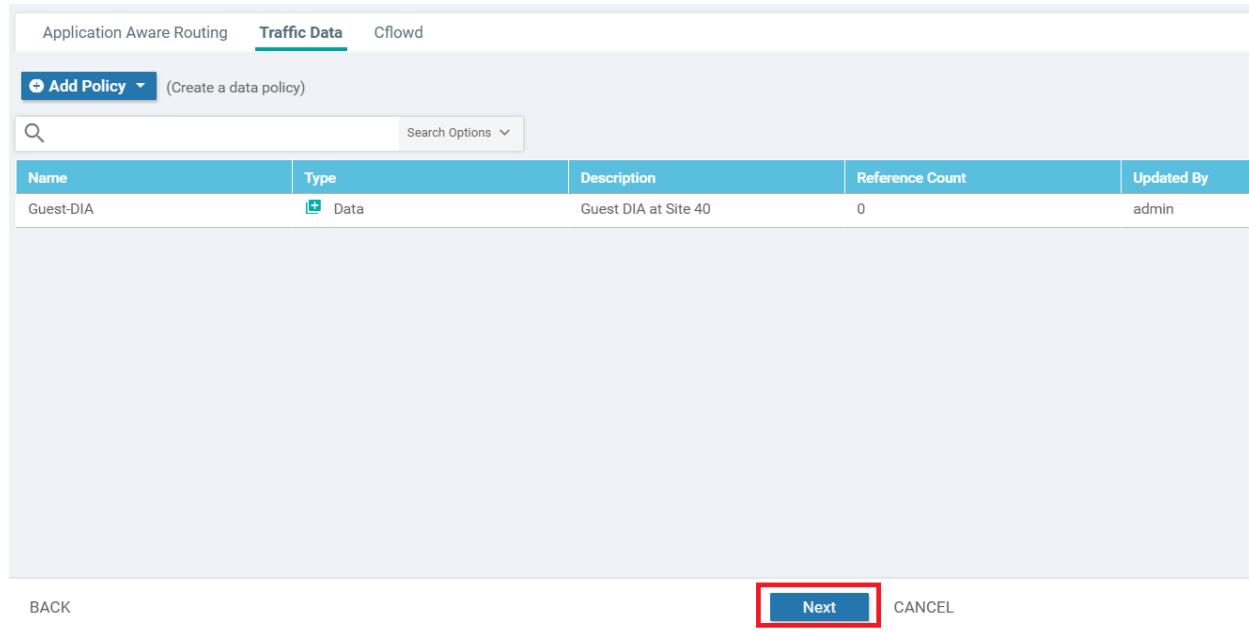
10. Click on **Default Action** over on the left-hand side and choose **Accept**. Click on **Save Match and Actions**



11. Click on **Save Data Policy**

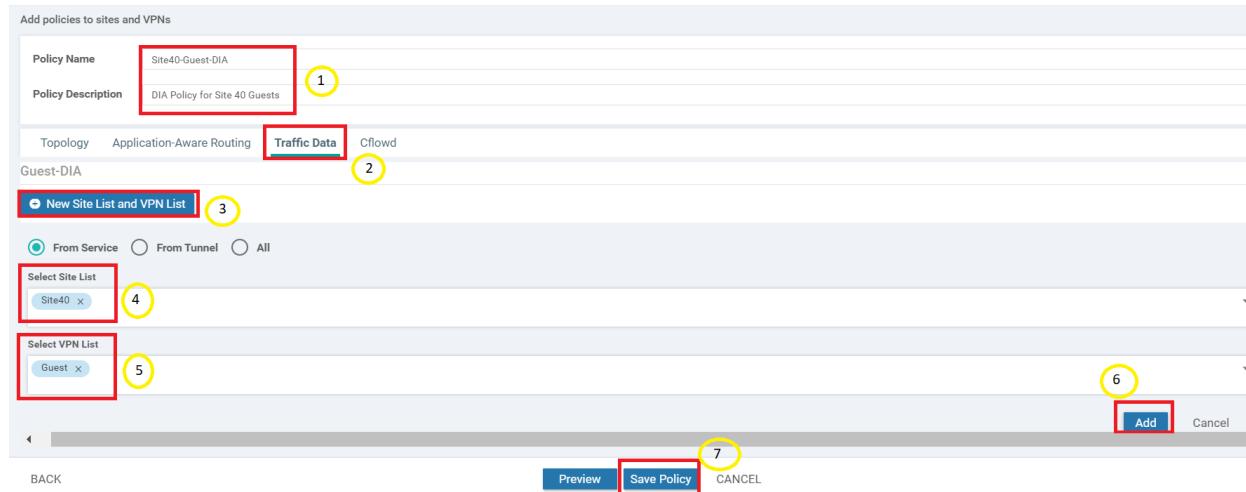


12. Make sure the Data Policy we just added shows up and click on **Next**



13. Enter the Policy Name as *Site40-Guest-DIA* and a Description of *DIA Policy for Site 40 Guests*. Click on the **Traffic Data** tab and choose **New Site List** and **VPN List**. Leave the radio button on *From Service* and choose *Site40* under

Select Site List. Choose Guest under Select VPN List. Click on **Add**. Once added, click on **Save Policy**



14. Locate your Site40-Guest-DIA and click on the three dots next to it. Choose to Activate the policy



This completes the configuration of our DIA Policy.

Task List

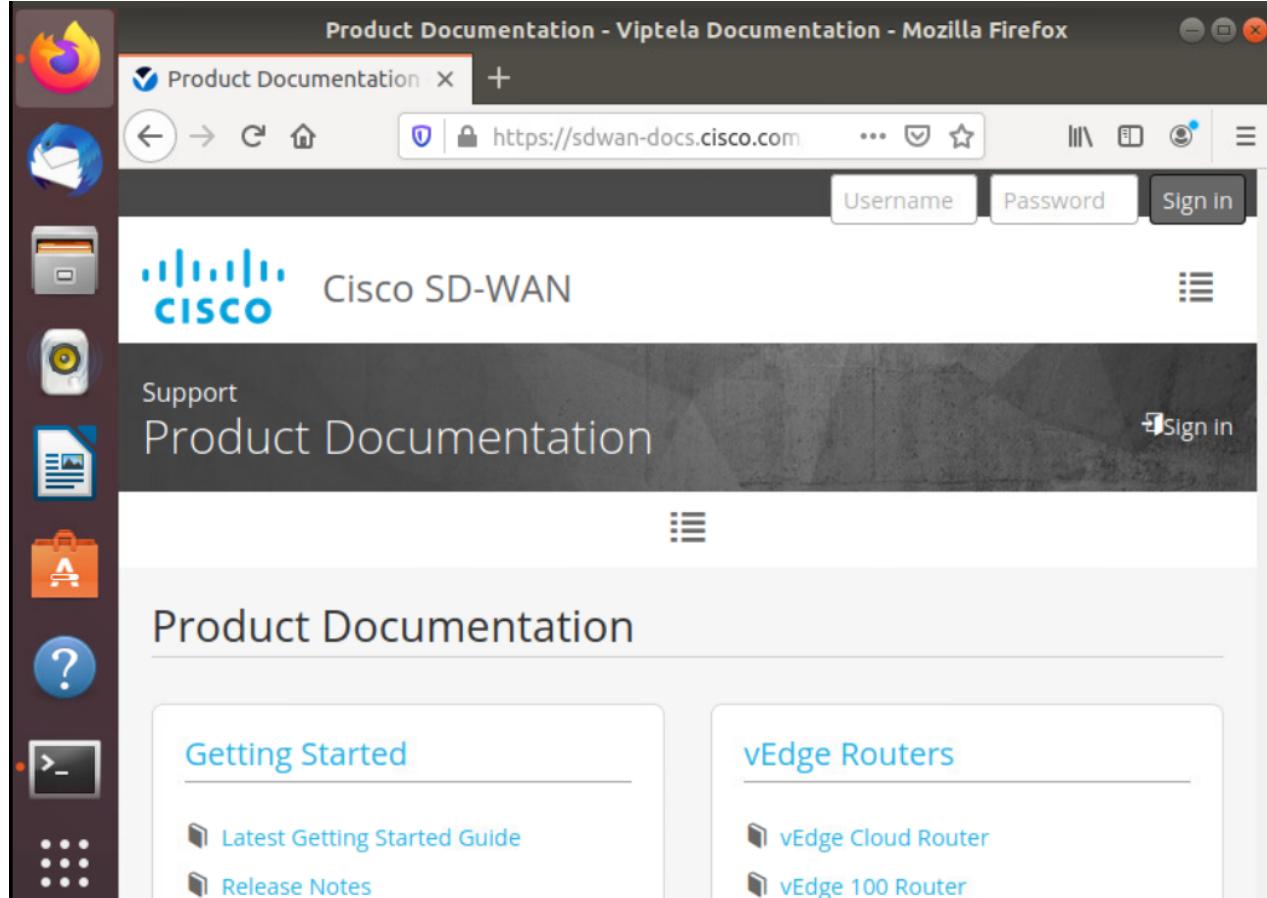
- [Overview](#)
- [Creating and Activating a Policy](#)
- [Verification](#)

Verification

1. To verify, log in to vCenter and Console to the Site40 PC, as enumerated in the [Overview](#) section. On Terminal, enter `ping 8.8.8.8`. The pings should succeed

```
sdwan@10-40-30-21:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=4.81 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=4.51 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=4.61 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=4.61 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=4.51 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=53 time=4.62 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=53 time=5.29 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 4.512/4.713/5.295/0.265 ms
sdwan@10-40-30-21:~$
```

2. Click on the Mozilla Firefox icon on the Site40 PC and try to browse to sdwan-docs.cisco.com (or any other website).
It should work



Task List

- [Overview](#)
- [Creating and Activating a Policy](#)
- [Verification](#)



-->

Configuring a Zone Based Firewall for Guest DIA users

Summary: Implementing a Zone Base Firewall at Site 40 for Guest Direct Internet Access users

Table of Contents

- [Overview](#)
- [Setting up Lists](#)
 - [Configuring Zones](#)
 - [Configuring an Application List](#)
- [Creating a Security Policy](#)
- [Applying the Policy and Verification](#)

Task List

- Overview
- Setting up Lists
 - Configuring Zones
 - Configuring an Application List
- Creating a Security Policy
- Applying the Policy and Verification

Overview

Since we have users on the Guest network accessing the Internet through the DIA VPN, we might want to lock down what they can/cannot access. Cisco SD-WAN has an in-built Zone Based Firewall which can perform Deep Packet Inspection,

allowing and/or blocking/inspecting traffic as need be. While this is a slightly stripped down version of a ZBF, it is quite robust in functionality and offers an intuitive GUI (in the form of vManage) for deploying Firewall Rules.

In this section we will be configuring and deploying a Zone Based Firewall in our network. Guest users will be able to access most Web content but they won't be able to access Web based emails (like Gmail). We will see the corresponding activity on the ZBF in the CLI and on the GUI.

Task List

- [Overview](#)
- [Setting up Lists](#)
 - [Configuring Zones](#)
 - [Configuring an Application List](#)
- [Creating a Security Policy](#)
- [Applying the Policy and Verification](#)

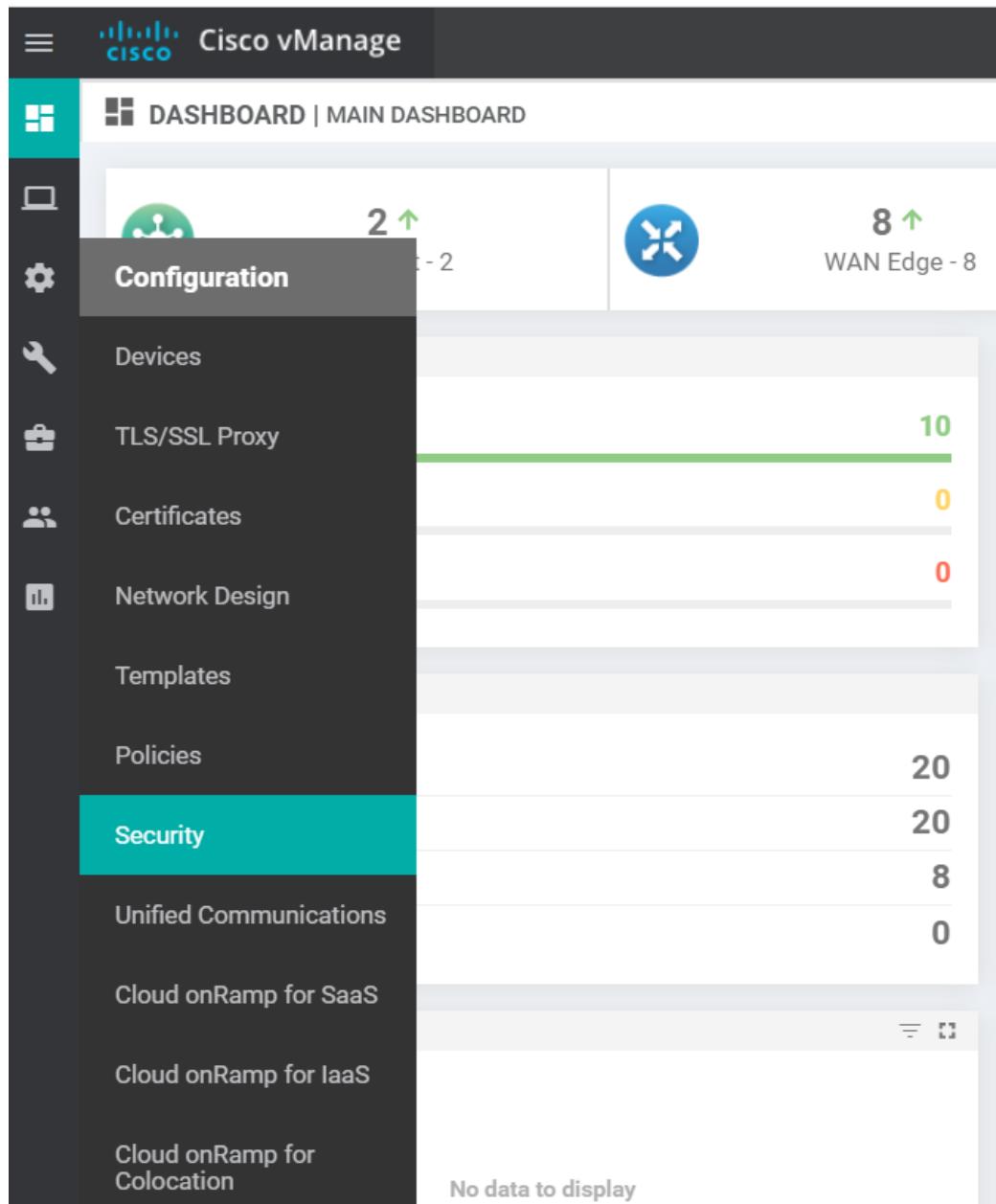
Setting up Lists

We start off by configuring a few Lists that form the building blocks of our ZBF. The following lists will be created

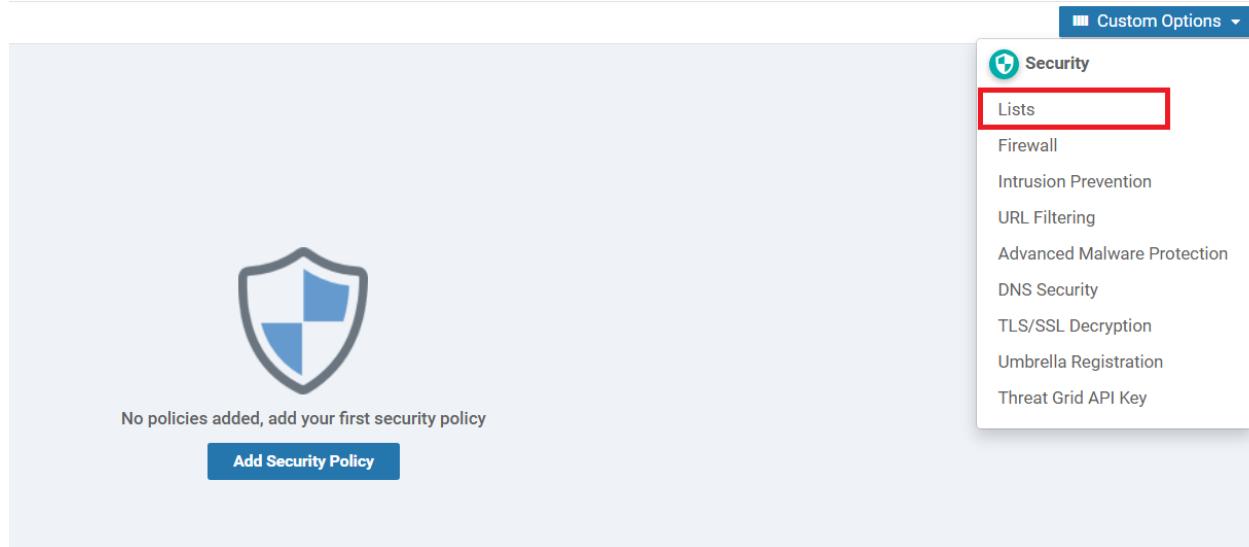
- Zone List for identifying the Guest and Outside zones
- Application List for identifying webmail traffic and allowing all other TCP traffic to ports 80 and 443

Configuring Zones

1. On the vManage GUI, go to **Configuration => Security**



2. Click on **Custom Options** in the top right corner of the screen and click on **Lists**



3. Click on **Zones** on the left-hand side and choose to create a **New Zone List**. Give the Zone List Name as *Guest* and Add VPN as *30*. Click on **Add**

The screenshot shows the 'Zones' configuration page. On the left, a sidebar lists categories: Application, Data Prefix, Domain, Signatures, Whitelist URLs, Blacklist URLs (numbered 1), Zones (highlighted with a red box), and TLS/SSL Profile. The main area is titled 'Define Lists' and contains a form for creating a new zone list. The steps are numbered: 2 (click 'New Zone List'), 3 (enter 'Guest' in 'Zone List Name'), 4 (enter '30' in 'Add VPN'), and 5 (click 'Add'). A 'Cancel' button is also visible. Below the form, a table header is shown with columns: Name, Entries, Reference Count, Updated By, Last Updated, and Action. The message 'No data available' is displayed at the bottom.

4. Click on **New Zone List** again and give the Zone List Name as *Outside*. Specify the Add VPN as *0*. Click on **Add**

New Zone List

Zone List Name
Outside

Add VPN
0

Add Cancel

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|-------|---------|-----------------|------------|-----------------------------|--------|
| Guest | 30 | 0 | admin | 03 Jun 2020 10:06:36 AM PDT | |

5. Make sure that there are two Zone Lists in the configuration and move to the next section of the guide (while staying on the same page)

New Zone List

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|---------|---------|-----------------|------------|-----------------------------|--------|
| Outside | 0 | 0 | admin | 03 Jun 2020 10:07:46 AM PDT | |
| Guest | 30 | 0 | admin | 03 Jun 2020 10:06:36 AM PDT | |

Task List

- [Overview](#)
- [Setting up Lists](#)
 - [Configuring Zones](#)
 - [Configuring an Application List](#)
- [Creating a Security Policy](#)
- [Applying the Policy and Verification](#)

Configuring an Application List

- From the previous section, click on **Application** in the top left corner of the screen after verifying that both the Zone Lists are visible

The screenshot shows the 'Application' tab selected in the sidebar. The main area displays a table titled 'New Zone List' with two entries: 'Outside' and 'Guest'. The 'Guest' entry is highlighted with a red box. The table columns are: Name, Entries, Reference Count, Updated By, Last Updated, and Action.

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|---------|---------|-----------------|------------|-----------------------------|---|
| Outside | 0 | 0 | admin | 03 Jun 2020 10:07:46 AM PDT | Edit Delete |
| Guest | 30 | 0 | admin | 03 Jun 2020 10:06:36 AM PDT | Edit Delete |

- Once Application is selected, click on **New Application List** and give the Application List Name of *Guest-Inspect*. Choose *Webmail* from the drop down, making sure all the sub-items under webmail are selected as well

The screenshot shows the 'New Application List' configuration page. Step 1 highlights the 'Application' tab in the sidebar. Step 2 highlights the 'New Application List' button. Step 3 highlights the 'Application List Name' field containing 'Guest-Inspect'. Step 4 highlights the 'Webmail' dropdown menu, which is expanded to show several options, with 'Webmail' itself being checked.

- Click on **Add** to add this Application List

The screenshot shows a confirmation dialog for adding the application list. It contains the 'Application List Name' field with 'Guest-Inspect' and the 'Webmail' dropdown menu. The 'Add' button is highlighted with a red box.

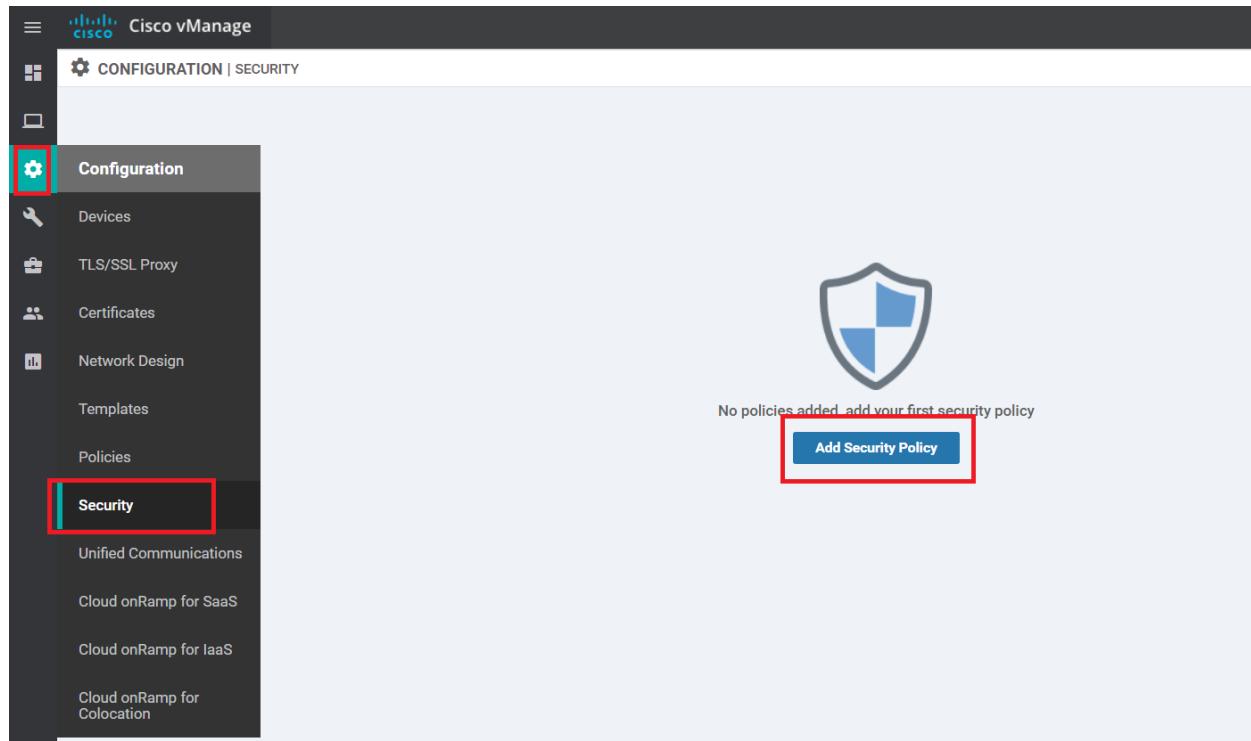
We have created an Application List which can potentially identify Gmail, Mail.ru etc. traffic. We will now create our policy.

Task List

- [Overview](#)
- [Setting up Lists](#)
 - [Configuring Zones](#)
 - [Configuring an Application List](#)
- [Creating a Security Policy](#)
- [Applying the Policy and Verification](#)

Creating a Security Policy

1. On the vManage GUI, navigate to **Configuration => Security** and click on **Add Security Policy**



2. Choose **Guest Access** and click on Proceed

Add Security Policy



Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.



Compliance

Application Firewall | Intrusion Prevention | TLS/SSL Decryption



Guest Access

Application Firewall | URL Filtering | TLS/SSL Decryption



Direct Cloud Access

Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption



Direct Internet Access

Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security | TLS/SSL Decryption



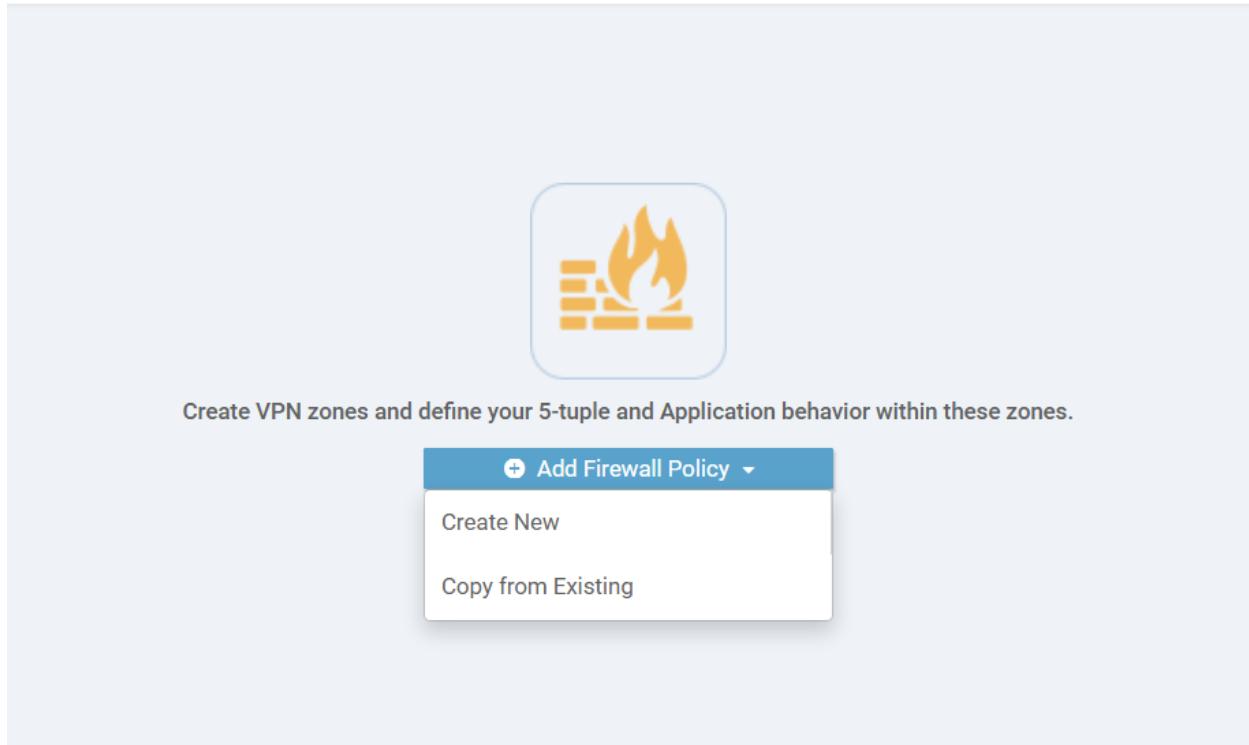
Custom

Build your ala carte policy by combining a variety of security policy blocks

Proceed

Cancel

3. Under Firewall, choose to **Add Firewall Policy**. Click on *Create New*



4. Click on **Apply Zone Pairs**

CONFIGURATION | SECURITY Add Firewall Policy

Sources Destinations

Apply Zone-Pairs

0 Rules

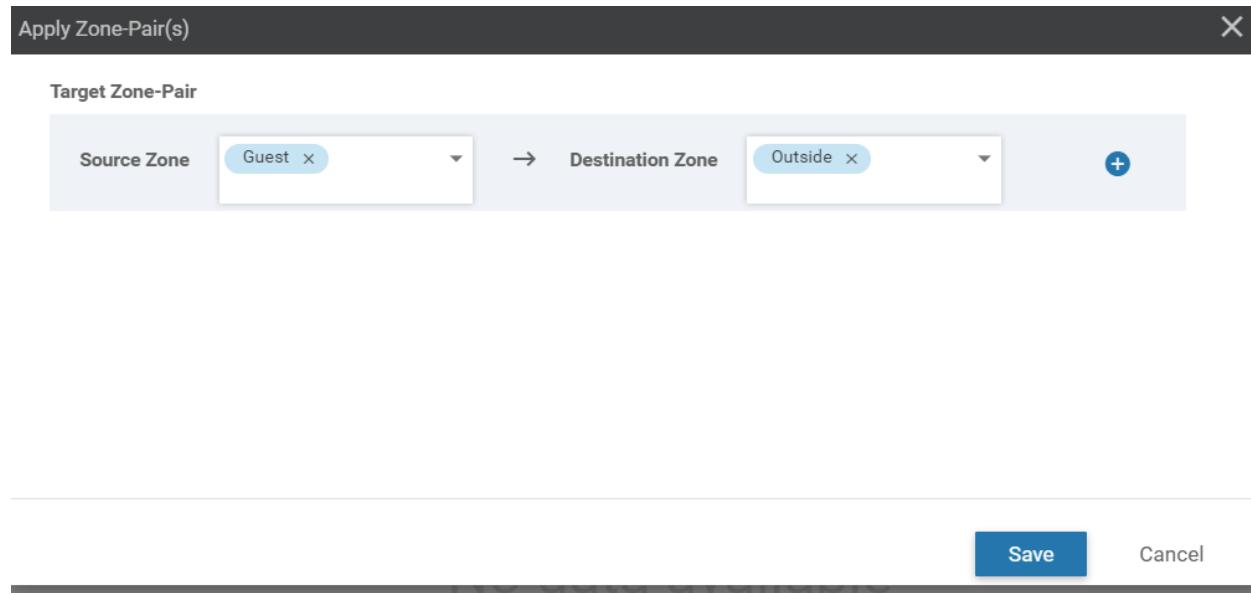
Name Maximum of 32 characters Description Description of the configuration

Add Rule (Drag and drop the Order cell to re-arrange rules and click on the other cells to inline add/edit the values)

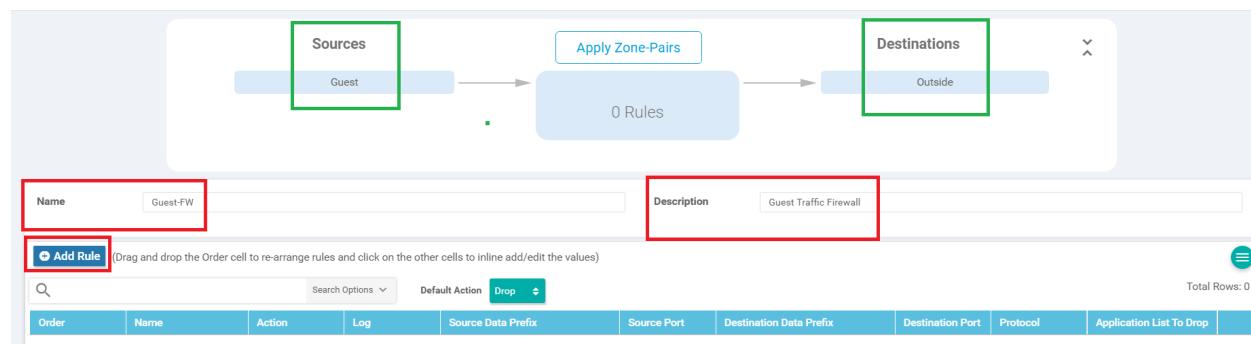
Search Options Default Action Drop

| Order | Name | Action | Log | Source Data Prefix | Source Port | Destination Data Prefix | Destination Port | Protocol | Application List To Drop |
|-------|------|--------|-----|--------------------|-------------|-------------------------|------------------|----------|--------------------------|
| | | | | | | | | | |

5. Set the **Source Zone** as *Guest* and the **Destination Zone** as *Outside*. Click on **Save**



6. Ensure that *Guest* appears under Sources and *Outside* appears under Destinations. Give the Policy a name of *Guest-FW* and a Description of *Guest Traffic Firewall*. Click on **Add Rule**



7. Click on **Source Data Prefix** and choose *Guest-Site40* as the **IPv4 Prefix List**. Click on the Green **Save** button (be careful, don't click on the Blue Save button)

Order 1 ▾ Name Rule 1 Action Drop ▾ Log

Source / Destination

+ Source Data Prefix + Source Port + Destination Data Prefix + Destination Ports + Protocol

Source Data Prefix

IPv4 Prefix
IPv4 Prefix List
Guest-Site40 x

IPv4
Example: 10.0.0.0/12

IPv4 Variable
Variable Name

FQDN (Fully-Qualified Domain Name) ⓘ
FQDN List
Select a fqdn list

and/or FQDN
Example: cisco.com and not more than 120 characters

Any

Save Cancel

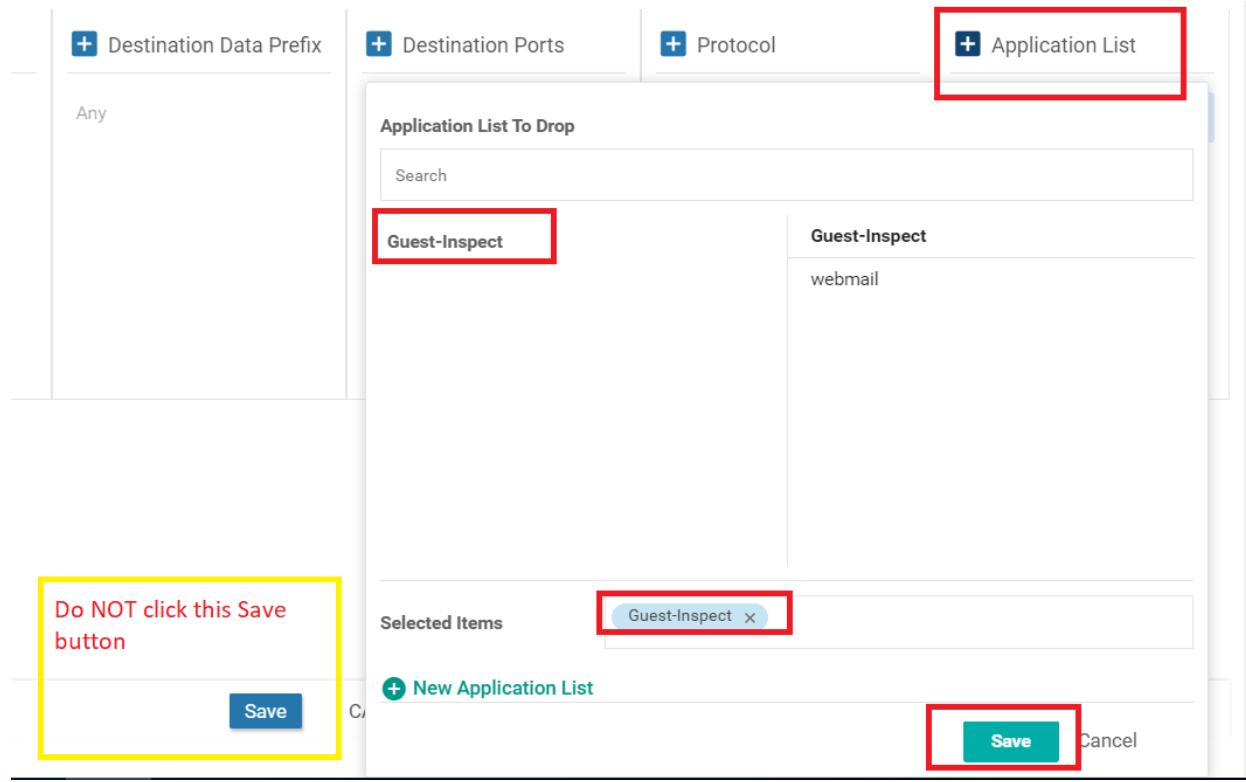
Do NOT click this Save button

Save

CANCEL

The screenshot shows a network rule configuration interface. At the top, there are fields for Order (1), Name (Rule 1), Action (Drop), and Log. Below this is a section titled "Source / Destination" with five tabs: "Source Data Prefix", "Source Port", "Destination Data Prefix", "Destination Ports", and "Protocol". The "Source Data Prefix" tab is active. Under "Source Data Prefix", there are three sections: "IPv4 Prefix" (with a dropdown menu showing "Guest-Site40" which is highlighted with a red box), "IPv4" (with an example field "10.0.0.0/12"), and "IPv4 Variable" (with a "Variable Name" field). To the right, there are sections for "FQDN (Fully-Qualified Domain Name)" (with a "FQDN List" dropdown menu and a note "Select a fqdn list") and "FQDN" (with an example field "cisco.com and not more than 120 characters"). On the far right, there is a "Protocol" section with the value "Any". At the bottom, there are two "Save" buttons: a blue one on the left labeled "Do NOT click this Save button" and a green one on the right labeled "Save". There is also a "Cancel" button.

8. Click on **Application List** and select the *Guest-Inspect* list we created. Click on the Green **Save** button (again, please don't click on the Blue Save button)



9. Give the Firewall Rule a name of *Inspect Web App Guest* and set the Action as **Inspect**. Click on **Save** (this time, we click the Blue Save button). Ensure that the Source Data Prefix and the Application List is populated

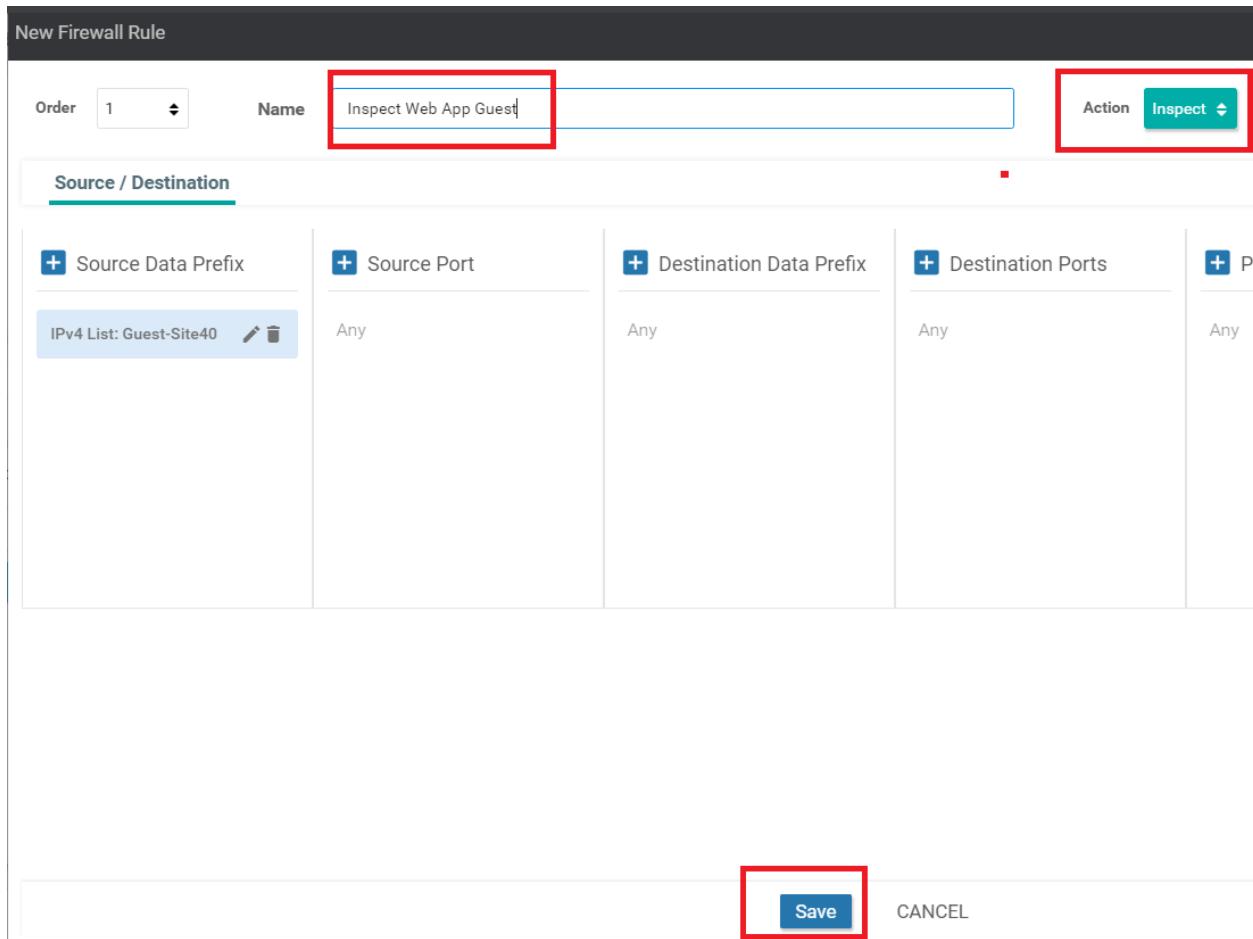
New Firewall Rule

Order 1 ▾ Name Inspect Web App Guest Action Inspect ▾

Source / Destination

| Source Data Prefix | Source Port | Destination Data Prefix | Destination Ports | Protocol |
|---|-------------|-------------------------|-------------------|----------|
| IPv4 List: Guest-Site40 Edit Delete | Any | Any | Any | Any |

Save CANCEL



10. Click on **Add Rule** again and select the **Source Data Prefix** IPv4 Prefix List as *Guest-Site40*. Click on the Green **Save** button

+ Source Data Prefix + Source Port + Destination Data Prefix + Destination Ports

Source Data Prefix

IPv4 Prefix

IPv4 Prefix List
Guest-Site40 ×

IPv4
Example: 10.0.0.0/12

IPv4 Variable
Variable Name

FQDN (Fully-Qualified Domain Name) i

FQDN List
Select a fqdn list

and/or **FQDN**
Example: cisco.com and not more than 120 characters

Save **Cancel**

11. Click on **Destination Ports** and set the Destination Ports as 80 443 (there is a space between the port numbers).
Click on the Green **Save** button

+ Destination Ports + Protocol +

Destination Ports
80 443

Save **Cancel**

12. Make sure the Firewall Rule looks like the image below and specify a Name of *TCP Guest Pass Web*. Specify the **Action** as *Pass* and put a check mark against Log. Click on the Blue **Save** button

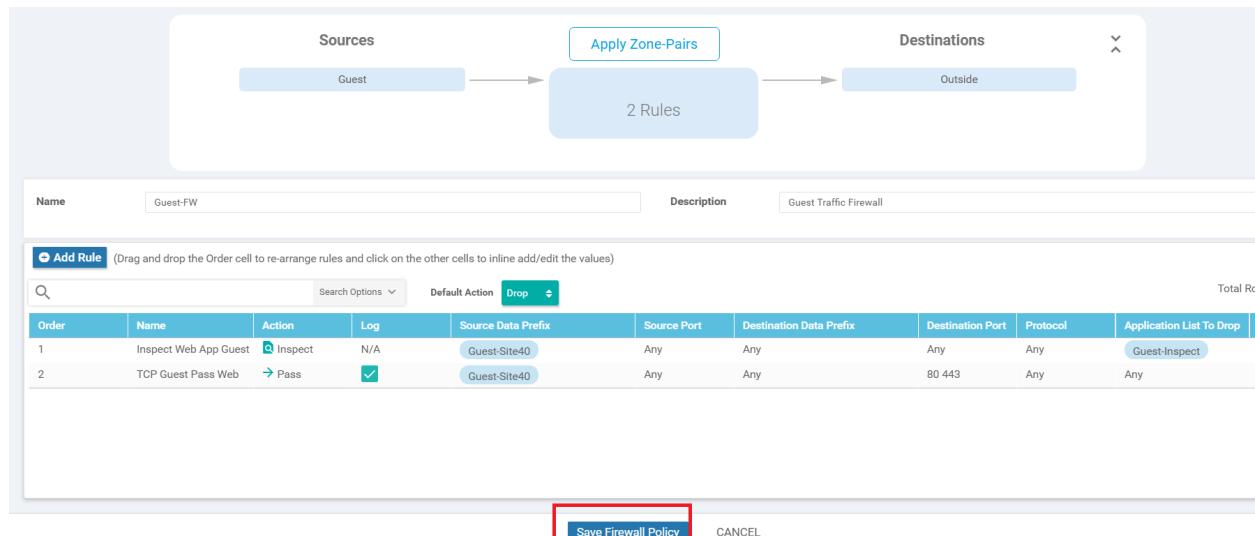
Order 2 Name **TCP Guest Pass Web** Action **Pass** Log

Source / Destination

| Source Data Prefix | Source Port | Destination Data Prefix | Destination Ports | Protocol |
|-------------------------|-------------|-------------------------|-------------------|----------|
| IPv4 List: Guest-Site40 | Any | Any | 80 443 | Any |

Save CANCEL

13. Make sure the Firewall Policy looks as below and click on **Save Firewall Policy**



14. Click on **Next** and then **Next** again at the URL Filtering and TLS/SSL Decryption sections

Add Firewall Policy (Add a Firewall configuration)

| Name | Type | Description | Reference Count | Updated By |
|----------|-------------|------------------------|-----------------|------------|
| Guest-FW | zoneBasedFW | Guest Traffic Firewall | 0 | admin |

Next CANCEL



Enhance your security by allowing or disallowing pre-defined web categories or custom created URL lists.

i Please upload compatible Security App Hosting Image File to the software repository in order to support URL-F functions. You can upload the image file from Maintenance > Software Repository > Virtual Images

+ Add URL Filtering Policy

Next CANCEL



Configure your TLS/SSL Decryption Policy for added security by performing inspections of traffic for deeper security insights.

-  Please add at least any one of Intrusion Prevention or URL Filtering or Advance Malware Protection Policy to add TLS/SSL Decryption Policy

 Add TLS/SSL Decryption Policy ▾

Next

CANCEL

15. At the Policy Summary page, give a Security Policy Name of *Site40-Guest-DIA* and a Description of *Guest Policy for Site 40*. Under Additional Policy Settings set the TCP SYN Flood Limit to Enabled and 5000. Enable **Audit Trail** as well and click on **Save Policy**

Firewall URL Filtering TLS/SSL Decryption Policy Summary

Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name Site40-Guest-DIA
Security Policy Description Guest Policy for Site 40

Additional Policy Settings

Firewall

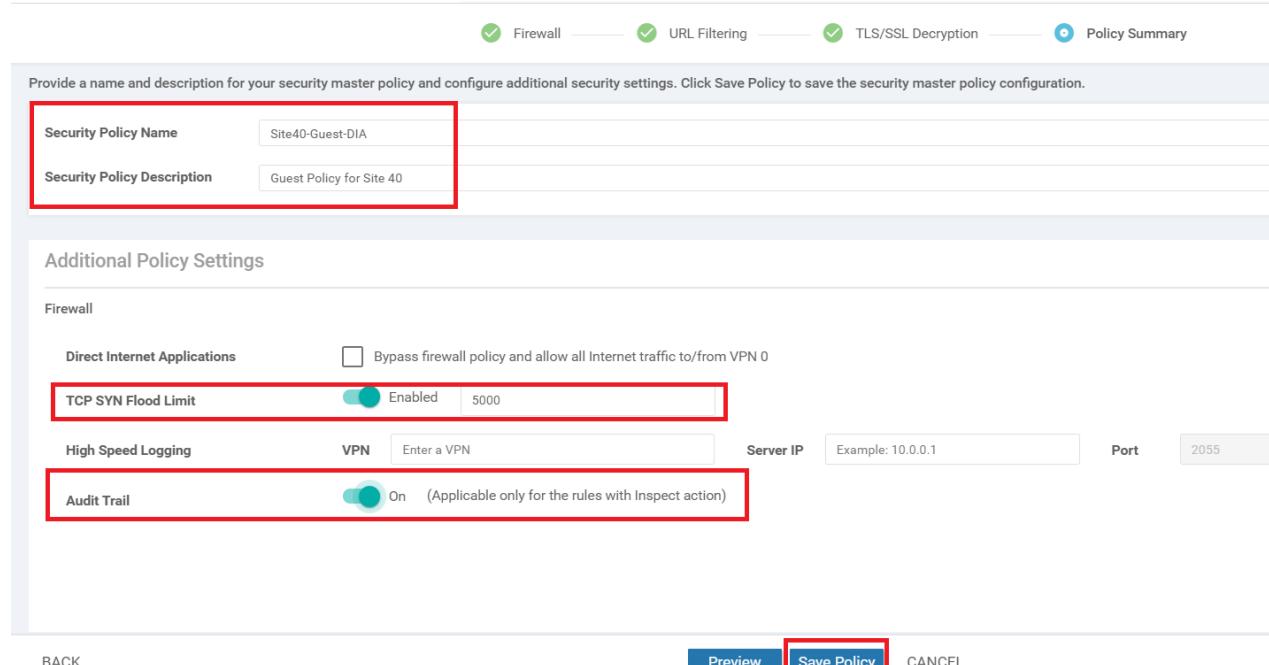
Direct Internet Applications Bypass firewall policy and allow all Internet traffic to/from VPN 0

TCP SYN Flood Limit Enabled 5000

High Speed Logging VPN Enter a VPN Server IP Example: 10.0.0.1 Port 2055

Audit Trail On (Applicable only for the rules with Inspect action)

BACK Preview **Save Policy** CANCEL



This completes the process of creating the Security Policy.

Task List

- [Overview](#)
- [Setting up Lists](#)
 - [Configuring Zones](#)
 - [Configuring an Application List](#)
- [Creating a Security Policy](#)
- [Applying the Policy and Verification](#)

Applying the Policy and Verification

1. Go to **Configuration => Templates** and click on the three dots next to the *cEdge_dualuplink_devtemp* Device Template. Choose to **Edit** it

| | | | | | | | | | |
|--------------------------|----------------------------|---------|-------------|----|----------|-------|--------------------------|---------|------------|
| vEdge_Site20_dev_temp | Device template for the... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 P... | In Sync | ... |
| vEdge30_dev_temp | Device template for the... | Feature | vEdge Cloud | 15 | 1 | admin | 25 May 2020 3:09:51 P... | In Sync | ... |
| cEdge_dualuplink_devt... | cEdge Device Template... | Feature | CSR1000v | 19 | 1 | admin | 26 May 2020 12:31:48 ... | In Sync | ... |
| vSmart-dev-temp | Device Template for vS... | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 ... | In Sync | |

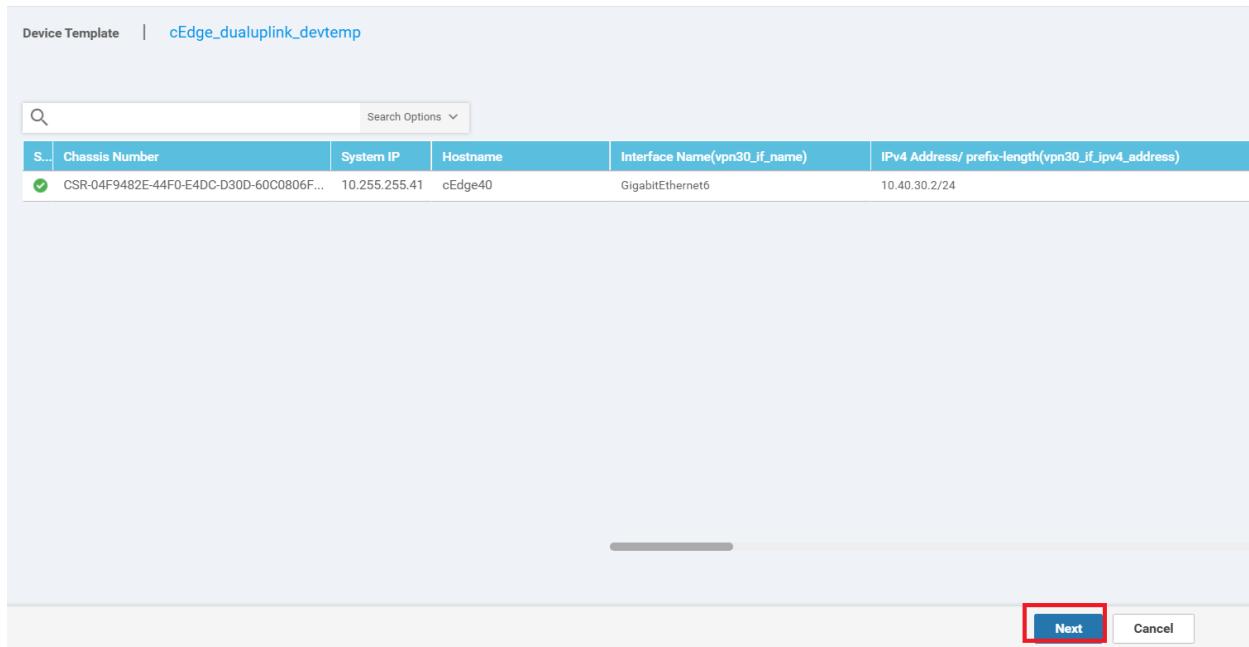
2. Under the **Additional Templates** section, populate the **Security Policy** as *Site40-Guest-DIA* and click on **Update**

Additional Templates

| | |
|---------------------|---------------------------------------|
| AppQoE | Choose... |
| Global Template * | Factory_Default_Global_CISCO_Template |
| Cisco Banner | Choose... |
| Cisco SNMP | Choose... |
| CLI Add-On Template | Choose... |
| Policy | Choose... |
| Probes | Choose... |
| Security Policy | Site40-Guest-DIA |

Update **Cancel**

3. Choose **Next** and then **Configure Devices** to push the Security Policy to cEdge40



```

235 class-map match-any Guest-Inspect-cm
236 match protocol attribute application
237 match protocol attribute application
238 match protocol attribute application
239 match protocol attribute application
240 match protocol attribute application
241 match protocol attribute application
242 match protocol attribute application
243 match protocol attribute application
244 match protocol attribute application
245 !
246 policy-map type inspect Guest-FW
247 class Guest-FW-seq-1-cm_
248   inspect audit-trail-pmap_
249   service-policy avc Guest-Inspect-p
250 !
251 class Guest-FW-seq-11-cm_
252   inspect audit-trail-pmap_
253 !
254 class class-default
255   drop
256 !
257 !
258 policy-map type inspect avc Guest-Inspe
259 class Guest-Inspect-cm0_
260   deny

```

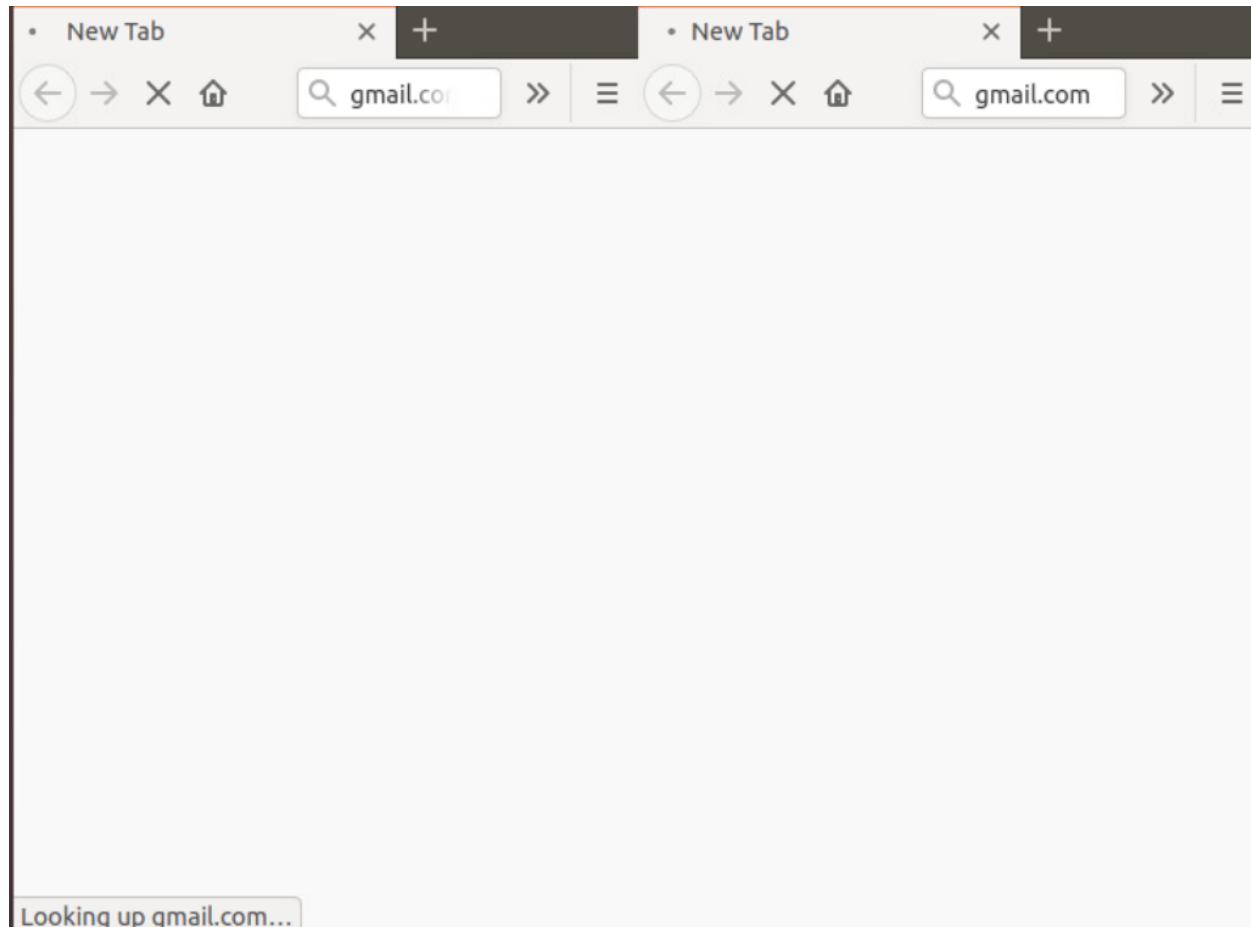
4. Open the Console session to the Site 40 PC (log in to vCenter => locate the site40pc VM and open the Web Console) and navigate to www.facebook.com. It should work indicating that Web Traffic is allowed. Log in to the cEdge40 CLI

via Putty and issue a `show logg`. We should see some activity there

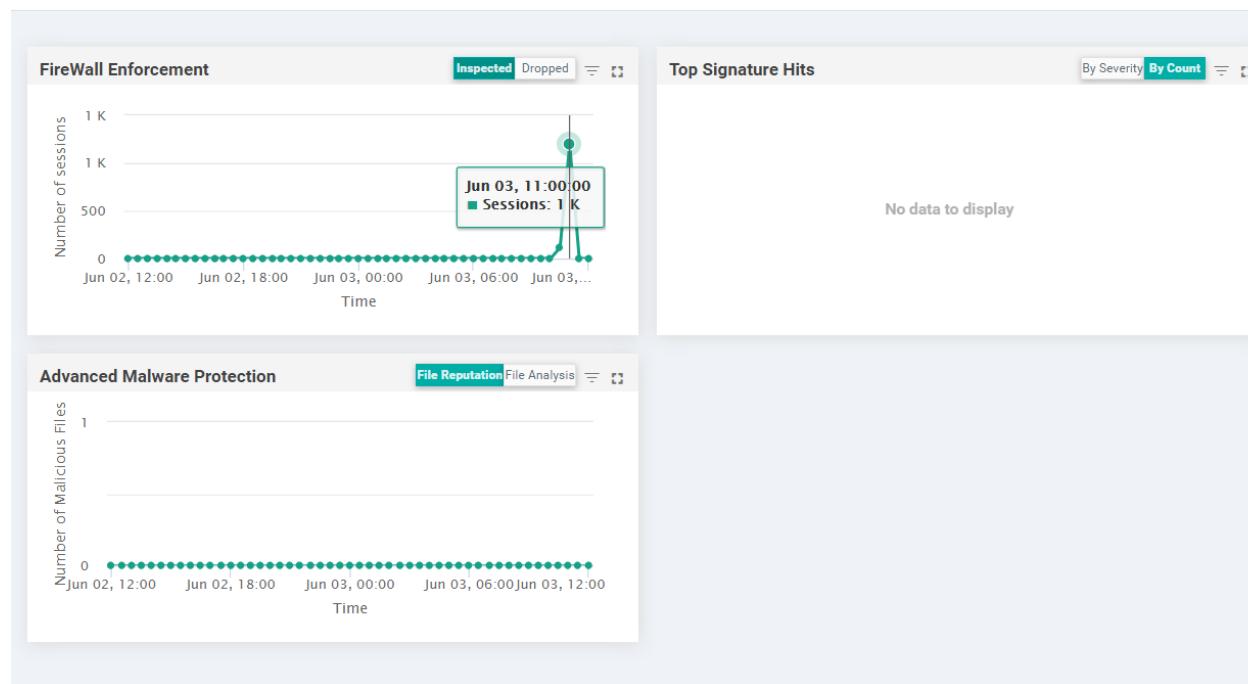


```
*Jun  3 19:03:34.241: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001392528385401618 %FW-6-SESS AUDIT TRAIL START: (target:class)-(ZP Guest Outs ide_Guest-FW:Guest-FW-seq-1-cm_):Start session: initiator (10.40.30.21:40698) -- responder (31.13.79.26:443) from GigabitEthernet6 (srcvrf:dstvrf)-(30:glo bal)
*Jun  3 19:03:34.243: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001392528387497980 %FW-6-SESS AUDIT TRAIL START: (target:class)-(ZP Guest Outs ide_Guest-FW:Guest-FW-seq-1-cm_):Start session: initiator (10.40.30.21:40700) -- responder (31.13.79.26:443) from GigabitEthernet6 (srcvrf:dstvrf)-(30:glo bal)
*Jun  3 19:03:34.246: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001392528389875649 %FW-6-SESS AUDIT TRAIL START: (target:class)-(ZP Guest Outs ide_Guest-FW:Guest-FW-seq-1-cm_):Start session: initiator (10.40.30.21:40702) -- responder (31.13.79.26:443) from GigabitEthernet6 (srcvrf:dstvrf)-(30:glo bal)
*Jun  3 19:03:34.255: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001392528399569956 %FW-6-SESS AUDIT TRAIL START: (target:class)-(ZP Guest Outs ide_Guest-FW:Guest-FW-seq-1-cm_):Start session: initiator (10.40.30.21:40704) -- responder (31.13.79.26:443) from GigabitEthernet6 (srcvrf:dstvrf)-(30:glo bal)
*Jun  3 19:03:34.288: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001392528431937511 %FW-6-SESS AUDIT TRAIL: (target:class)-(ZP Guest Outside_Gu est-FW:Guest-FW-seq-1-cm_):Stop session: initiator (10.40.30.21:40670) sent 792 bytes -- responder (31.13.79.26:443) sent 3423 bytes, from GigabitEthernet6
*Jun  3 19:03:34.618: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001392528762066188 %FW-6-SESS AUDIT TRAIL: (target:class)-(ZP Guest Outside_Gu est-FW:Guest-FW-seq-1-cm_):Stop session: initiator (10.40.30.21:40690) sent 0 bytes -- responder (31.13.79.26:443) sent 0 bytes, from GigabitEthernet6
```

5. Open up a few tabs on the Site 40 PC (2 to 3 of them) and try to access www.gmail.com on all tabs. This should fail



6. On the vManage GUI, navigate to **Dashboard => Security** and you should see spikes in the Firewall Enforcement dashlet (continue with the lab and check back after approximately 15 minutes to see this)



Thus, our ZBF is working as expected, blocking webmail traffic on the Guest VPN while allowing other traffic on ports 80 and 443.

Task List

- [Overview](#)
- [Setting up Lists](#)
 - [Configuring Zones](#)
 - [Configuring an Application List](#)
- [Creating a Security Policy](#)
- [Applying the Policy and Verification](#)



Configuring Application Aware Routing

[Take a tour of this page](#)

Summary: Manipulate the path taken by traffic based on network parameters like latency, loss and jitter.

Table of Contents

- [Overview](#)
- [Creating and Activating the AAR Policy](#)
- [Viewing modified traffic flows and current network statistics](#)
- [Configuring a Policer to simulate network impairment](#)
 - [Creating a Policer List](#)
 - [Configuring the IPv4 ACL Policy](#)
- [Applying the Policer on the MPLS link](#)
- [Viewing changed statistics and resultant traffic flows](#)

Task List

- Overview
- Creating and Activating the AAR Policy
- Viewing modified traffic flows and current network statistics
- Configuring a Policer to simulate network impairment
- Creating a Policer List
- Configuring the IPv4 ACL Policy
- Applying the Policer on the MPLS link
- Viewing changed statistics and resultant traffic flows

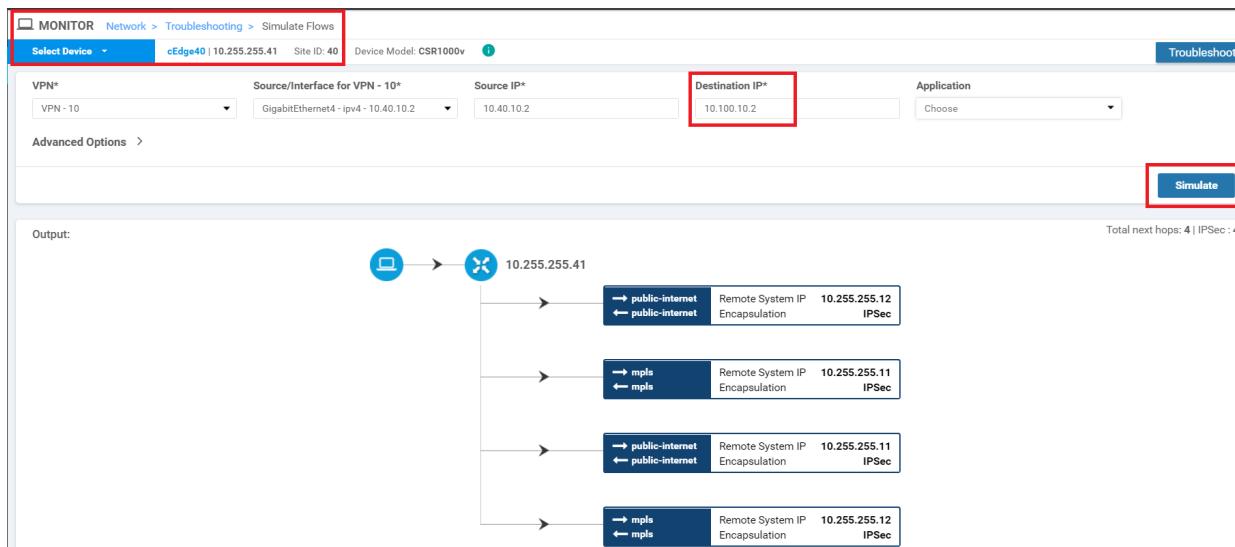
Overview

While we can use Traffic Engineering to steer traffic towards a particular preferred transport, Application Aware Routing takes things to a different level by not only allowing us to punt traffic over a preferred path, but also define SLA parameters for traffic to be redirected if network conditions aren't favourable for the type of traffic.

To set a baseline, we will first see how traffic flows on VPN 10 (let's assume that this VPN has Voice traffic in it). We will then implement AAR and SLA Classes to route traffic out a preferred transport and switch the chosen transport if SLA parameters are not met.

To check existing traffic flows, follow the steps below:

1. Navigate to **Monitor => Network** and select **cEdge40** from the list. Scroll down on the left-hand side and click on **Troubleshooting**. Choose **Simulate Flows**. Choose a VPN of **VPN - 10** and a Source/Interface of **GigabitEthernet4**. Enter the Destination IP as **10.100.10.2** and click on **Simulate**. Notice that traffic is attempting to use all available transports. If you receive an error of "Failed to run service path" as shown in the second image below, log in to vCenter and right click on the cEdge40 VM for your POD. Choose Edit Settings and uncheck the "Connected" check box for Network Adapter 4. Click on OK. Wait for 10 seconds and check the same checkbox again. Now try to simulate the flow



MONITOR Network > Troubleshooting > Simulate Flows

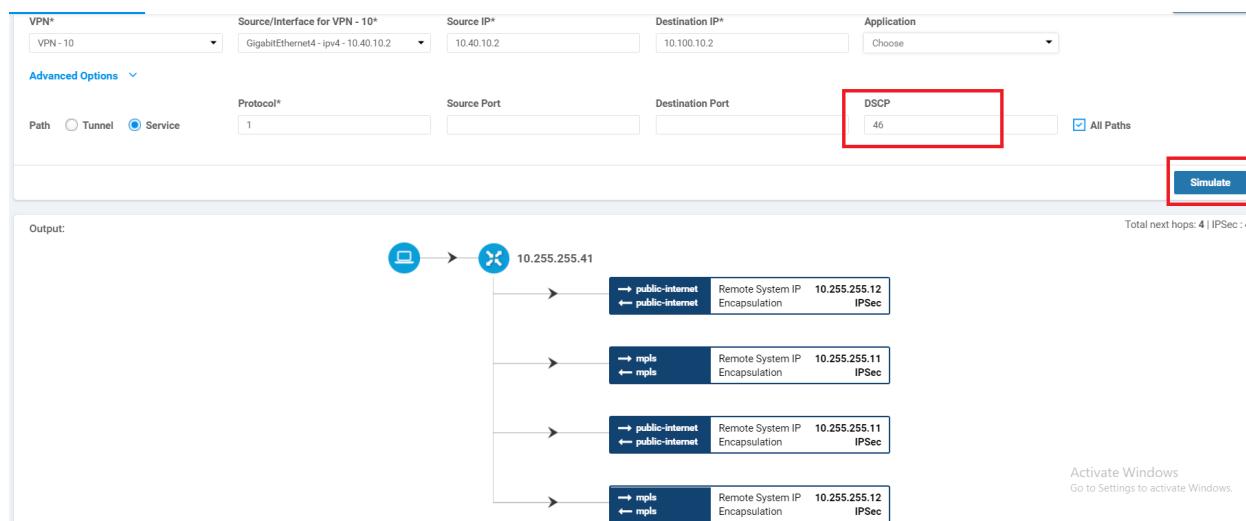
Select Device: cEdge40 | 10.255.255.41 Site ID: 40 Device Model: CSR1000v

VPN*: VPN - 10* Source/Interface for VPN - 10*: GigabitEthernet4 - ipv4 - 10.40.10.2* Source IP*: 10.40.10.2

Advanced Options >

Failed to run service path
Interface GigabitEthernet6 not up

2. Click on **Advanced Options** and enter the DSCP value as 46 (i.e. VoIP RTP traffic). Click on **Simulate**. This traffic also uses all possible transports, which might not be ideal for our network



Task List

- Overview
- Creating and Activating the AAR Policy
- Viewing modified traffic flows and current network statistics
- Configuring a Policer to simulate network impairment
- Creating a Policer List
- Configuring the IPv4 ACL Policy
- Applying the Policer on the MPLS link
- Viewing changed statistics and resultant traffic flows

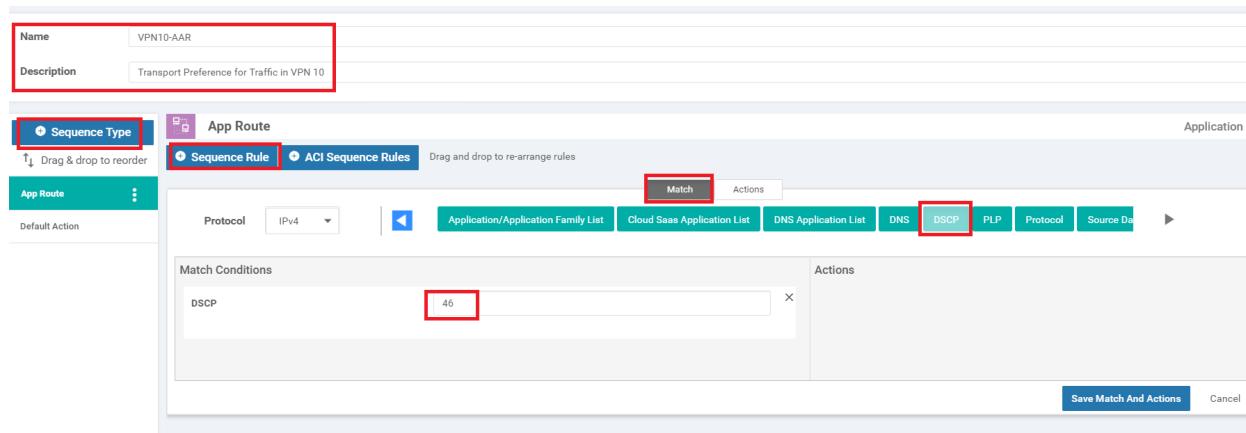
Creating and Activating the AAR Policy

We will now set up an AAR Policy for VoIP (i.e. DSCP 46) traffic.

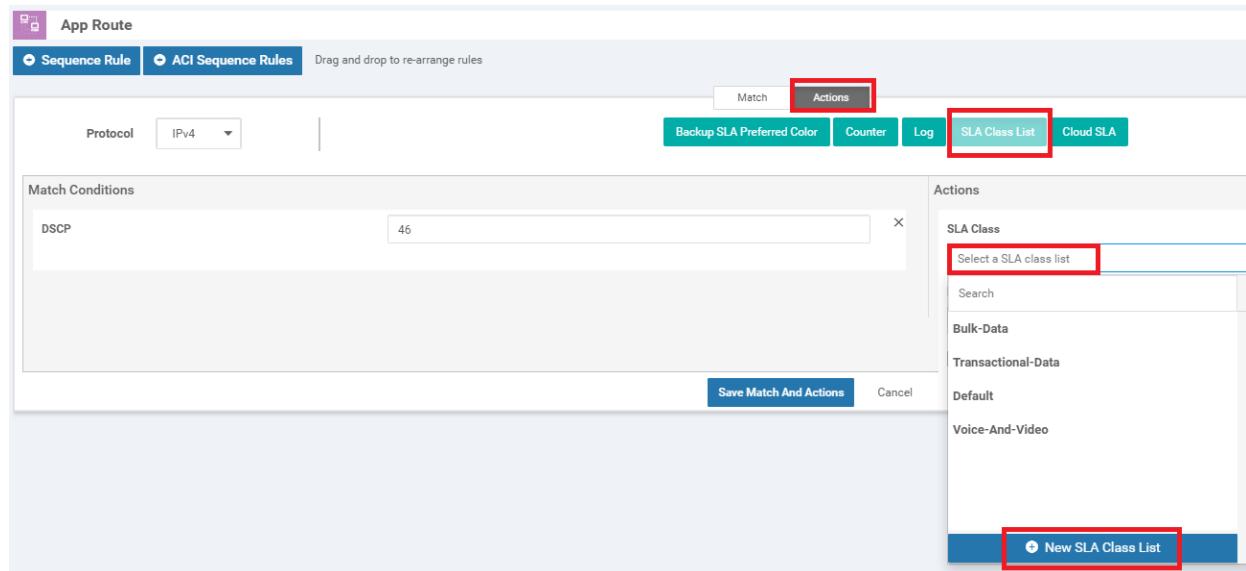
1. On the vManage GUI, go to **Configuration => Policies** and click **Add Policy**. Click on **Next** twice (till you get to the Configure Traffic Rules page) and click on **Add Policy** under Application Aware Routing. We thus have an overarching Policy (let's call it the Main Policy) and an application-aware routing policy within it. As of now, we will configure the AAR routing policy. Towards the end, we will enter the details of the Main Policy

The screenshot shows the 'CONFIGURATION | POLICIES' section of the vManage interface. The 'Centralized Policy > Add Policy' path is selected. The 'Configure Traffic Rules' tab is active. In the main content area, there is a message 'Choose a tab and add Traffic rules under the selected type' above three tabs: 'Application Aware Routing' (selected), 'Traffic Data', and 'Cflowd'. Below these tabs is a dropdown menu labeled 'Add Policy' with the sub-option '(Create an application-aware routing policy)'. Underneath this is a search bar with 'Search Options' and a 'Create New' button. A table header is visible with columns: Name, Type, Description, Reference Count, and Updated By. At the bottom of the screen, there are navigation buttons: 'BACK', 'Next', and 'CANCEL'.

2. Give this AAR Policy a name of VPN10-AAR and a Description of *Transport Preference for Traffic in VPN 10*. Click on **Sequence Type** and then click on **Sequence Rule**. Under Match, select DSCP and enter a DSCP value of **46** under Match Conditions



3. Click on the Actions tab and choose **SLA Class List**. Click on the box under SLA Class and choose **New SLA Class List**



4. Give the SLA Class a Name of **Voice-SLA** and specify the **Loss %** as **1**. Enter **200** for the **Latency** and **15** for the **Jitter**. Click on **Save**

SLA Class

SLA Class List Name
Voice-SLA

| Loss (%) | Latency (ms) | Jitter (ms) |
|----------|--------------|-------------|
| 1 | 200 | 15 |

Save **Cancel**

5. Still under actions, select the *Voice-SLA* SLA Class that we just created and set the Preferred Color to *mpls*. Click on **Save Match and Actions**

App Route

Sequence Rule **ACI Sequence Rules** Drag and drop to re-arrange rules

Protocol: IPv4

Actions

Match Conditions: DSCP 46

Actions:

- SLA Class: Voice-SLA
- Preferred Color: mpls

Save Match And Actions

6. Ensure your App Route looks like the image below and click on **Save Application Aware Routing Policy**. Click **Next**

Match Conditions

DSCP: 46

Actions

SLA Class: List Voice-SLA

Preferred Color: mpls

Strict

Save Application Aware Routing Policy CANCEL

7. At the **Apply Policies to Sites and VPNs** page, give the Policy a Name of *AAR-VPN10* and a Description of *Transport Preference for VPN 10*. Click on the Application Aware Routing tab and click on **New Site List and VPN List**. Under **Select Site List** choose *Branches* and *DC*. Under **Select VPN List** choose *Corporate*. Click on **Add**

Add policies to sites and VPNs

Policy Name: AAR-VPN10

Policy Description: Transport Preference for VPN 10

Topology Application-Aware Routing Traffic Data Cflowd

VPN10-AAR

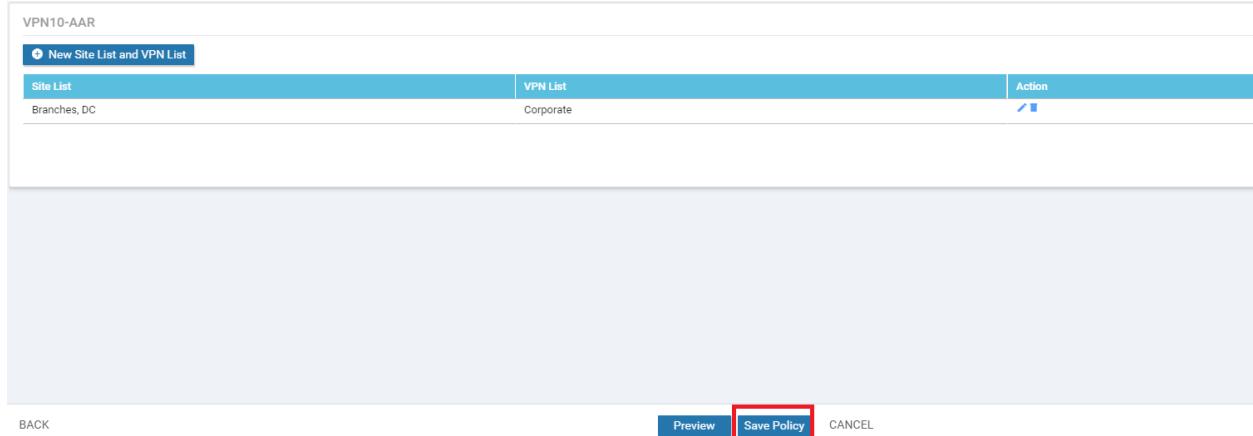
New Site List and VPN List

Select Site List: Branches x DC x

Select VPN List: Corporate x

Add Cancel

8. Click on **Save Policy** in the lower middle part of the screen to save our AAR Policy

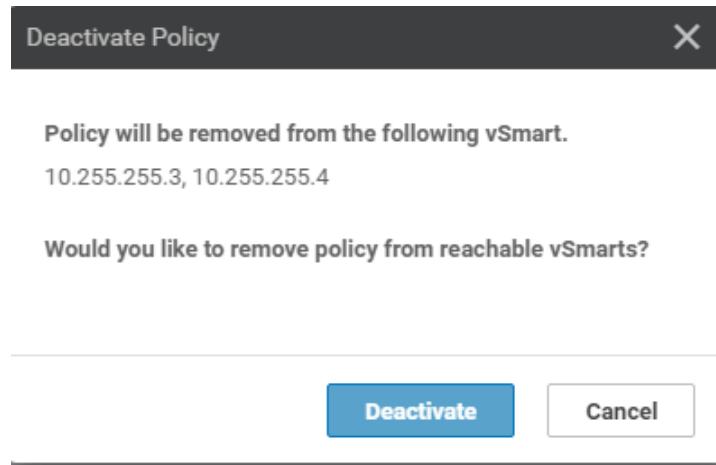


BACK

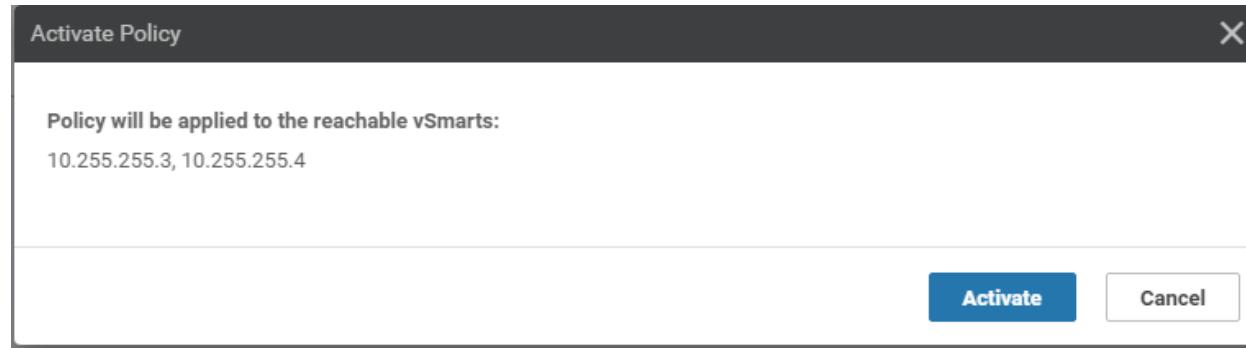
Preview Save Policy CANCEL

9. Click on the three dots next to the *Site40-Guest-DIA* policy created before and choose to **Deactivate** it (this needs to be done due to a bug present in version 20.3.x of vManage, else Activation of the AAR policy we just created will give an error of a "bad-element" in the configuration). Confirm the Deactivation. Once done, click on the three dots next to the *AAR-VPN10* policy we just created and choose to **Activate** it. Click on **Activate** again

| Name | Description | Type | Activated | Updated By | Policy Version | Last Updated | Actions |
|------------------------|------------------------|-------------------|-----------|------------|---------------------|---------------------|---------|
| Hub-n-Spoke-VPN... | Hub and Spoke p... | UI Policy Builder | false | admin | 08252020T1307343... | 25 Aug 2020 6:07... | ... |
| Site40-Guest-DIA | DIA Policy for Site... | UI Policy Builder | true | admin | 08282020T0629008... | 27 Aug 2020 11:2... | ... |
| traffic-engineering... | Traffic Engineerin... | UI Policy Builder | false | admin | 08282020T0619065... | 27 Aug 2020 11:2... | ... |
| Site20-Regional-H... | Regional Policy fo... | UI Policy Builder | false | admin | 08262020T1026367... | 27 Aug 2020 11:2... | ... |
| AAR-VPN10 | Transport Prefere... | UI Policy Builder | false | admin | 08302020T1201294... | 27 Aug 2020 11:2... | ... |

A screenshot of a table listing policies. The first row, "AAR-VPN10", is highlighted with a red box. A context menu is open over this row, with the "Activate" option highlighted and also enclosed in a red box. Other options in the menu include View, Preview, Copy, Edit, Delete, and ... (ellipsis).

| Name | Description | Type | Activated | Updated By | Policy Version | Last Updated | Actions |
|----------------------------|--|-------------------|-----------|------------|--------------------|----------------------------|-------------------------|
| AAR-VPN10 | Transport Preference for VPN 10 | UI Policy Builder | false | admin | 06042020T144602205 | 04 Jun 2020 7:46:02 AM PDT | ... |
| Site20-Regional-Hub-Site30 | Regional Policy for Site 20 to Site 30 | UI Policy Builder | false | admin | 05282020T130912927 | 28 May 2020 6:09:12 AM PDT | View |
| traffic-engineering-ftp | Traffic Engineering for FTP | UI Policy Builder | false | admin | 06032020T131902822 | 03 Jun 2020 6:19:02 AM PDT | Preview |
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 20 only | UI Policy Builder | false | admin | 05282020T100134900 | 28 May 2020 3:01:34 AM PDT | Copy |
| Site40-Guest-DIA | DIA Policy for Site 40 Guests | UI Policy Builder | true | admin | 06032020T142511667 | 03 Jun 2020 7:25:11 AM PDT | Edit |



Task List

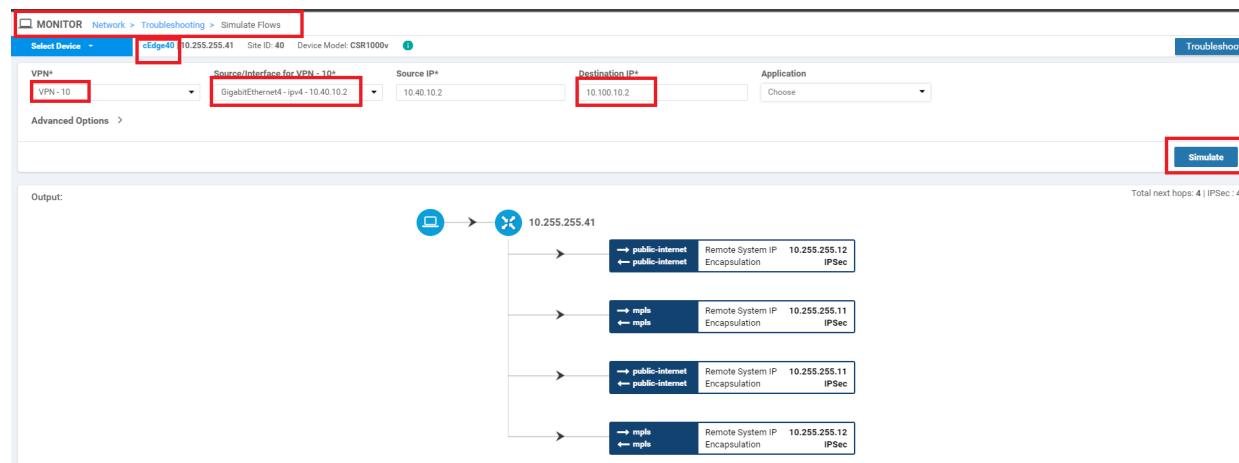
- [Overview](#)
- [Creating and Activating the AAR Policy](#)

- Viewing modified traffic flows and current network statistics
- Configuring a Policer to simulate network impairment
- Creating a Policer List
- Configuring the IPv4 ACL Policy
- Applying the Policer on the MPLS link
- Viewing changed statistics and resultant traffic flows

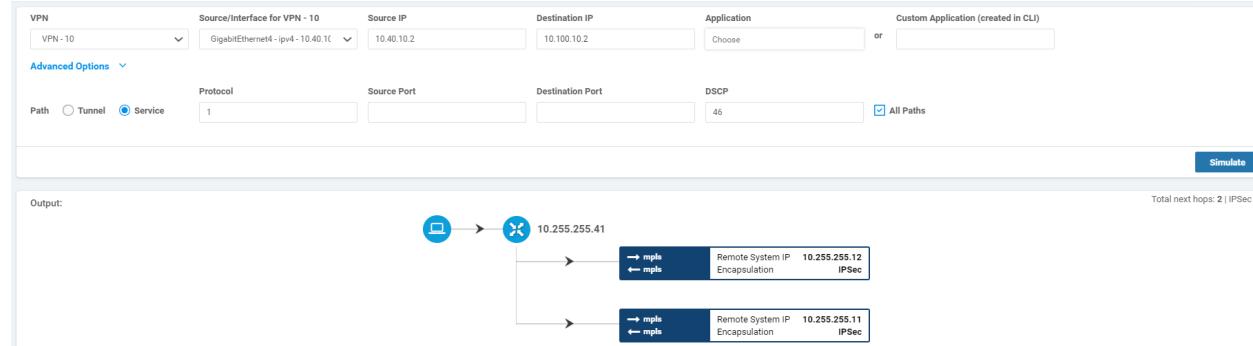
Viewing modified traffic flows and current network statistics

To view the changes made by the Policy on our network, follow the steps below.

1. On the vManage GUI, go to **Monitor => Network** and click on cEdge40. Choose **Troubleshooting** from the left-hand column and click on **Simulate Flows**. Enter the VPN as **VPN - 10** and the Source/Interface as **GigabitEthernet4**. Set a Destination IP of **10.100.10.2** and click on **Simulate**. We find that traffic is taking all possible transports, just like before. This is expected since we haven't defined anything for regular traffic



2. On the same screen, click on **Advanced Options** and set the DSCP to 46. Click on **Simulate**



VoIP Traffic is now traversing the MPLS link as the preferred route.

3. We will now check the current network statistics. Go to **Monitor => Network => cEdge40 => Tunnel** and put a check mark against all the *mpls* Tunnel Endpoints. Click on Real-Time after scrolling up to the chart and make sure Packet Loss/Latency is checked under **Chart Options**. We may see negligible packet loss occurring (let the chart run for 5 minutes before analysing, it should get updated every few seconds)



Task List

- [Overview](#)
- [Creating and Activating the AAR Policy](#)
- [Viewing modified traffic flows and current network statistics](#)
- Configuring a Policer to simulate network impairment
- Creating a Policer List
- Configuring the IPv4 ACL Policy
- Applying the Policer on the MPLS link
- Viewing changed statistics and resultant traffic flows

Configuring a Policer to simulate network impairment

In order to simulate impairment in the network (Packet Loss and Latency), we can use a Policer and a Shaper. Over here, we will configure a Policer which will be applied to the MPLS link in order to simulate Packet Loss.

Later on, we will leverage a Shaper to simulate Latency.

Creating a Policer List

1. On the vManage GUI, navigate to **Configuration => Policies**. Click on **Custom Options** (top right-hand corner). Under **Localized Policy** click on **Lists**

The screenshot shows the Cisco vManage interface under the Configuration > Policies section. A red box highlights the 'CONFIGURATION | POLICIES' tab. Another red box highlights the 'Custom Options' dropdown menu, which is open to show options like Centralized Policy, CLI Policy, Lists, Topology, Traffic Policy, and Localized Policy. Under Localized Policy, a third red box highlights the 'Lists' option. The main table lists various policy entries, and the 'Add Policy' button is visible at the top left.

2. Click on **Policer** (left-hand side) to create Policer configuration which will simulate network impairment on our MPLS link (Packet Loss). Click on **New Policer List** and give it a name of **AAR-Impair-Policer-PL**. Specify the **Burst** as **15000** and **Exceed** as **Drop**. The **Rate** should be **7000**. Click on **Add**

| Field | Value |
|-------------------|-----------------------|
| Policer List Name | AAR-Impair-Policer-PL |
| Burst (bps) | 15000 |
| Exceed | Drop |
| Rate (bps) | 7000 |

CONFIGURATION | POLICIES Localized Policy > Define Lists

Select a list type on the left and start creating your groups of interest

New Policer List

Policer List Name: AARImpair-Policer-PL

Burst (bps): 15000

Exceed: Drop

Rate (bps): 7000

Add Cancel

| Name | Burst | Exceed | Rate | Reference Count | Updated By | Last Updated | Action |
|------|-------|--------|------|-----------------|------------|--------------|--------|
| | | | | | | | |

No data available

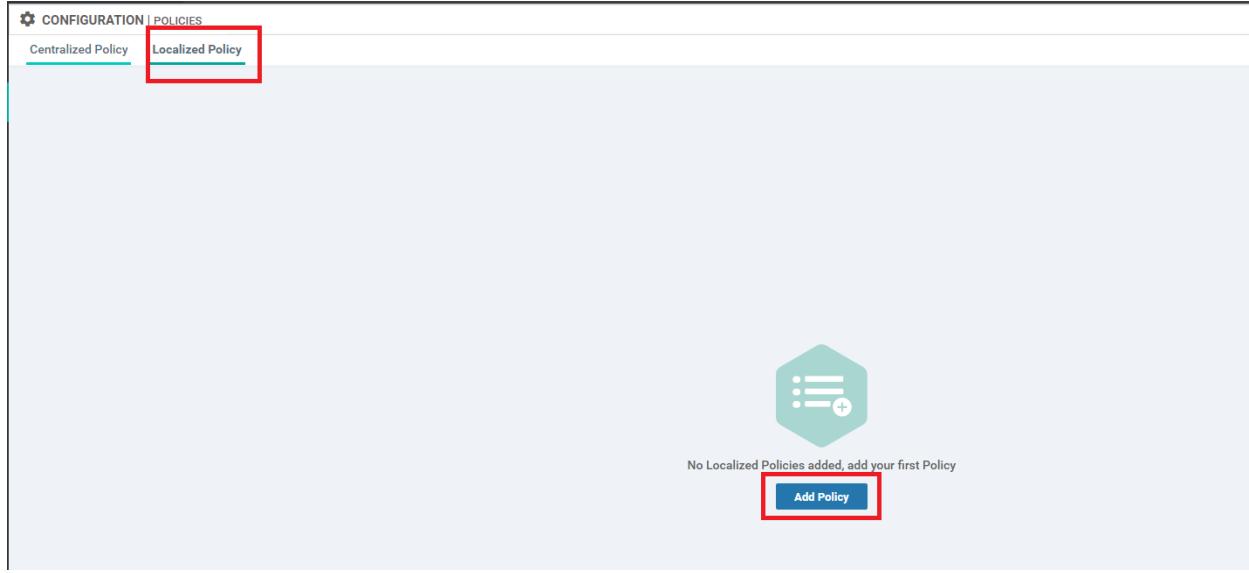
The screenshot shows the 'Localized Policy > Define Lists' section of the Juniper configuration interface. On the left sidebar, the 'Policer' tab is selected and highlighted in green. In the main area, a 'New Policer List' dialog is open. It contains fields for 'Policer List Name' (set to 'AARImpair-Policer-PL'), 'Burst (bps)' (set to '15000'), 'Exceed' (set to 'Drop'), and 'Rate (bps)' (set to '7000'). At the bottom right of the dialog is an 'Add' button, which is also highlighted with a red box. Below the dialog, a table header is visible with columns for Name, Burst, Exceed, Rate, Reference Count, Updated By, Last Updated, and Action. The message 'No data available' is displayed below the table.

Task List

- [Overview](#)
- [Creating and Activating the AAR Policy](#)
- [Viewing modified traffic flows and current network statistics](#)
- Configuring a Policer to simulate network impairment
- [Creating a Policeer List](#)
- [Configuring the IPv4 ACL Policy](#)
- [Applying the Policer on the MPLS link](#)
- [Viewing changed statistics and resultant traffic flows](#)

Configuring the IPv4 ACL Policy

1. Go to the **Localized Policy** tab and click on **Add Policy**

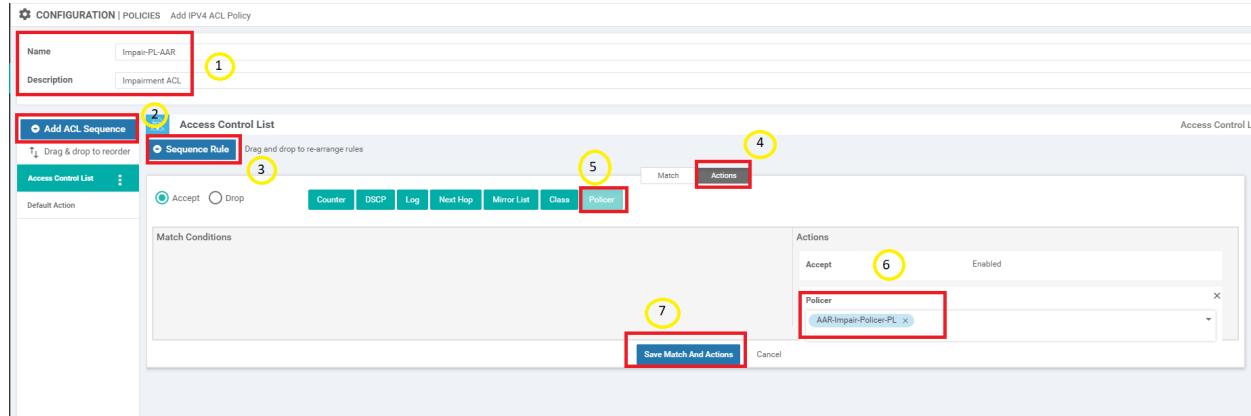


2. Click **Next** till you are at the **Configure Access Control Lists** page. Click on **Add Access Control List Policy** and choose **Add IPv4 ACL Policy**

3. Enter a name of *Impair-PL-AAR* with a Description of *Impairment ACL*. Click on **Add ACL Sequence** and click on **Sequence Rule**. Go to the **Actions** tab and make sure the Accept radio button is selected. Choose **Policer** and select the *AAR-Impair-Policer-PL* we created before. Click on **Save Match and Actions**. Refer to the table and image below

| Step | Field | Value |
|------|-------------|----------------|
| 1 | Name | Impair-PL-AAR |
| | Description | Impairment ACL |

| | |
|---|-------------------------------|
| 2 | Add ACL Sequence |
| 3 | Sequence Rule |
| 4 | Actions |
| 5 | Policer |
| 6 | Policer AAR-Impair-Policer-PL |
| 7 | Save Match and Actions |



4. Click on **Save Access Control List Policy**

Access Control List

Sequence Rule Drag and drop to re-arrange rules

1 Match Conditions Actions

Accept

Policer: AAR-Impair-Policer-PL

Save Access Control List Policy CANCEL

5. On the **Policy Overview** page (this is our Main Policy), enter a Policy Name of *Policer-AAR-Impairment* and a Description of *Injecting Impairment for AAR via a Policer - Packet Loss*. Click on **Save Policy**

CONFIGURATION | POLICIES Localized Policy > Add Policy

Create Groups of Interest Configure Forwarding Classes/QoS Configure Access Control Lists Configure Route Policy Policy Overview

Enter name and description for your localized master policy

Policy Name: Policer-AAR-Impairment

Policy Description: Injecting Impairment for AAR via a Policer - Packet Loss

Policy Settings

Netflow Application Cloud QoS Cloud QoS Service side Implicit ACL Logging

Log Frequency: Enter in seconds (maximum 2147483647)

BACK Preview Save Policy CANCEL

We have completed configuration of our Policer. It needs to be applied to a link in order to simulate network impairment.

Task List

- Overview
- Creating and Activating the AAR Policy
- Viewing modified traffic flows and current network statistics
- Configuring a Policer to simulate network impairment
- Creating a Policer List
- Configuring the IPv4 ACL Policy
- Applying the Policer on the MPLS link
- Viewing changed statistics and resultant traffic flows

Applying the Policer on the MPLS link

1. Navigate to Configuration => Templates => Feature Tab and locate the *cedge-vpn0-int-dual_mpls* VPN Interface template. Click on the 3 dots next to it and choose to **Copy**

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------|--------------------------------------|---------------------|--------------|------------------|------------------|------------|-----------------------------|-----------------------------------|
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Template... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| cedge-vpn30-int | VPN 30 Interface Template for cEd... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 25 May 2020 2:03:37 PM PDT | ... |
| cedge-vpn30 | VPN 30 Template for the cEdges... | Cisco VPN | CSR1000v | 2 | 3 | admin | 25 May 2020 1:57:26 PM PDT | ... |
| cedge_vpn512_dual_uplink | cEdge VPN 512 Template for Dual ... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 8:35:47 AM PDT | ... |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 03 Jun 2020 7:01:36 AM PDT | ... |
| cedge-vpn10 | VPN 10 Template for the cEdges... | Cisco VPN | CSR1000v | 2 | 3 | admin | 26 May 2020 1:54:12 AM PDT | ... |
| cedge-vpn10-int | VPN 10 Interface Template for cEd... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 25 May 2020 2:00:25 PM PDT | ... |
| cedge-vpn0-int-dual_mpls | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 23 May 2020 7:15:33 AM PDT | ... |
| cedge-vpn20-int | VPN 20 Interface Template for cEd... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 25 May 2020 | View |
| cEdge_VPN0_single_uplink | cEdge VPN 0 Template for Single U... | Cisco VPN | CSR1000v | 1 | 2 | admin | 18 May 2020 | Edit |
| cedge-vpn0-int-single | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 | Change Device Models |
| cEdge_VPN0_dualUplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin | 23 May 2020 | Delete |
| cedge-vpn20 | VPN 20 Template for the cEdges... | Cisco VPN | CSR1000v | 2 | 3 | admin | 25 May 2020 | Copy |
| site40-eigrp | EIGRP Template for Site 40 cEdge | EIGRP | CSR1000v | 1 | 1 | admin | 26 May 2020 12:30:21 AM PDT | ... |

2. Rename it to *cedge-vpn0-int-dual_mpls-impair* and a Description *cEdge VPN 0 Interface Template for Devices with a dual uplink - MPLS with Impairment*. Click on **Copy**

Template Copy

Template Name

cedge-vpn0-int-dual_mpls-impair

Description

cEdge VPN 0 Interface Template for devices with a dual uplink - MPLS with Impairment

Copy **Cancel**

3. Click on the three dots next to this newly copied template and click on **Edit**

4. Navigate to the ACL/QoS section and modify the following fields. Click on **Update**

| Field | Global or Device Specific (drop down) | Value |
|--------------------------|---------------------------------------|---------------|
| Ingress ACL - IPv4 | Global | On |
| IPv4 Ingress Access List | Global | Impair-PL-AAR |
| Egress ACL - IPv4 | Global | On |
| IPv4 Egress Access List | Global | Impair-PL-AAR |

ACL/QOS

| | |
|---------------------|---|
| Shaping Rate (Kbps) | <input checked="" type="checkbox"/> |
| QoS Map | <input checked="" type="checkbox"/> |
| Rewrite Rule | <input checked="" type="checkbox"/> |
| Ingress ACL - IPv4 | <input checked="" type="radio"/> On <input type="radio"/> Off IPv4 Ingress Access List <input checked="" type="checkbox"/> Impair-PL-AAR |
| Egress ACL - IPv4 | <input checked="" type="radio"/> On <input type="radio"/> Off IPv4 Egress Access List <input checked="" type="checkbox"/> Impair-PL-AAR |
| Ingress ACL - IPv6 | <input checked="" type="checkbox"/> On <input type="radio"/> Off |
| Egress ACL - IPv6 | <input checked="" type="checkbox"/> On <input type="radio"/> Off |

Update **Cancel**

These should match (case sensitive) with what was created in the IPv4 ACL policy

5. Under **Configuration => Templates** go to the **Device** tab and locate the *cedge_dualuplink_devtemp* template. Click on the three dots next to it and choose to **Edit**

Device **Feature**

Create Template

Template Type: Non-Default **Search Options**

Total Rows: 6

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Actions |
|---------------------------------|------------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|---------|
| DCvEdge_dev_temp | Device template for the DC-vE... | Feature | vEdge Cloud | 16 | 2 | admin | 28 May 2020 4:58:07 AM PDT | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 17 | 2 | admin | 26 May 2020 3:05:01 AM PDT | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 PM PDT | In Sync | ... |
| cEdge_dualuplink_devtemp | cEdge Device Template for dev... | Feature | CSR1000v | 19 | 1 | admin | 04 Jun 2020 8:44:24 AM PDT | In Sync | ... |
| vEdge30_dev_temp | Device template for the Site 30... | Feature | vEdge Cloud | 15 | 1 | admin | 25 May 2020 3:09:51 PM PDT | In Sync | ... |
| vSmart-dev-temp | Device Template for vSmarts | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 AM PDT | In Sync | ... |

Edit **View** **Delete** **Copy** **Attach Devices** **Detach Devices** **Export CSV** **Change Device Values**

6. Under Transport & Management VPN, update the **Cisco VPN Interface Ethernet** from *cedge-vpn0-int-dual_mpls* to *cedge-vpn0-int-dual_mpls-impair*. Make sure this is done on the VPN interface for the MPLS link

Transport & Management VPN

| | |
|------------------------------|---------------------------------|
| Cisco VPN 0 * | cEdge_VPN0_dual_uplink |
| Cisco VPN Interface Ethernet | cedge-vpn0-int-dual |
| Cisco VPN Interface Ethernet | cedge-vpn0-int-dual_mpls-impair |

| | |
|------------------------------|--------------------------|
| Cisco VPN 512 * | cEdge_VPN512_dual_uplink |
| Cisco VPN Interface Ethernet | cedge-vpn512-int-dual |

Service VPN

0 Rows Selected [+ Add VPN](#) [- Remove VPN](#)

| Search Options | Update | Cancel |
|----------------|--------|--------|
|----------------|--------|--------|

7. Scroll down to the **Additional Templates** section and update the **Policy** to *Policer-AAR-Impairment*. Click on **Update**.
Click on **Next**

Additional Templates

| | |
|---------------------|---------------------------------------|
| AppQoE | Choose... |
| Global Template * | Factory_Default_Global_CISCO_Template |
| Cisco Banner | Choose... |
| Cisco SNMP | Choose... |
| CLI Add-On Template | Choose... |
| Policy | Policer-AAR-Impairment |
| Probes | Choose... |
| Security Policy | Site40-Guest-DIA |

[Update](#) [Cancel](#)

8. You can choose to view the Side by Side or simply click on **Configure Devices**

```
Device Template      Total  
cEdge_dualuplink_devtemp    1  
  
Device list (Total: 1 devices)  
Filter/Search  
  
CSR-04F9482E-44F0-E4DC-D300-  
60C0806F73F2  
cEdge4010.255.255.41  
  
Configure Device Rollback Timer  
  
no allow-service snmp  
exit  
exit  
interface GigabitEthernet3  
tunnel-interface  
encapsulation ipsec weight 1  
no border  
color mpls restrict  
no last-resort-circuit  
no low-bandwidth-link  
no Vbond-as-stun-server  
vmanage-connection-preference 5  
port-hop  
carrier           default  
nat-refresh-interval 5  
hello-interval    1000  
hello-tolerance   12  
allow-service all  
no allow-service bgp  
allow-service dhcp  
allow-service dns  
allow-service icmp  
no allow-service sshd  
no allow-service netconf  
no allow-service ntp  
no allow-service ospf  
no allow-service stun  
allow-service https  
no allow-service snmp  
exit  
  
no allow-service snmp  
exit  
exit  
interface GigabitEthernet3  
tunnel-interface  
encapsulation ipsec weight 1  
no border  
color mpls restrict  
no last-resort-circuit  
no low-bandwidth-link  
no Vbond-as-stun-server  
vmanage-connection-preference 5  
port-hop  
carrier           default  
nat-refresh-interval 5  
hello-interval    1000  
hello-tolerance   12  
allow-service all  
no allow-service bgp  
allow-service dhcp  
allow-service dns  
allow-service icmp  
no allow-service sshd  
no allow-service netconf  
no allow-service ntp  
no allow-service ospf  
no allow-service stun  
allow-service https  
no allow-service snmp  
exit  
access-list Impair-PL-AAR in  
access-list Impair-PL-AAR out
```

Configure Devices

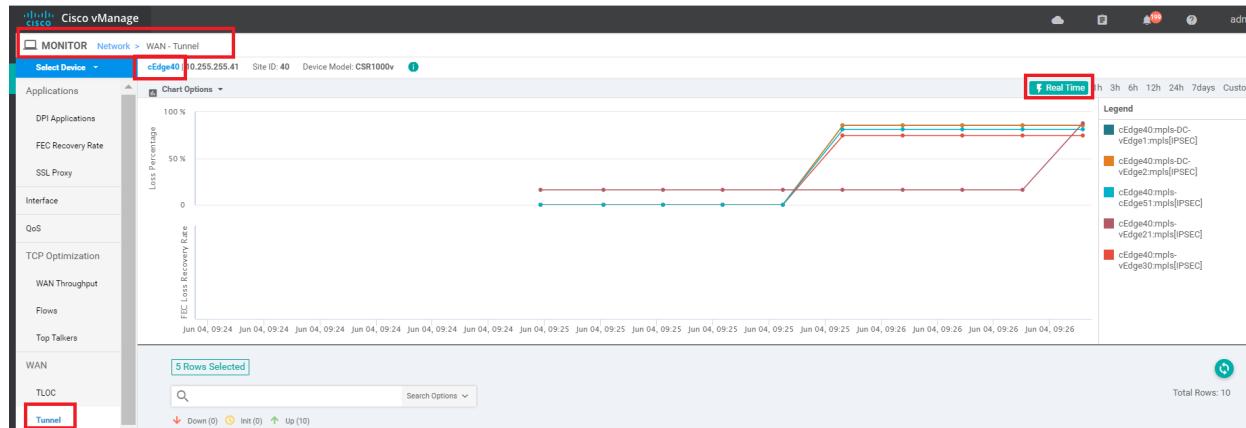
This completes the implementation of our Policer on the MPLS link to simulate network impairment.

Task List

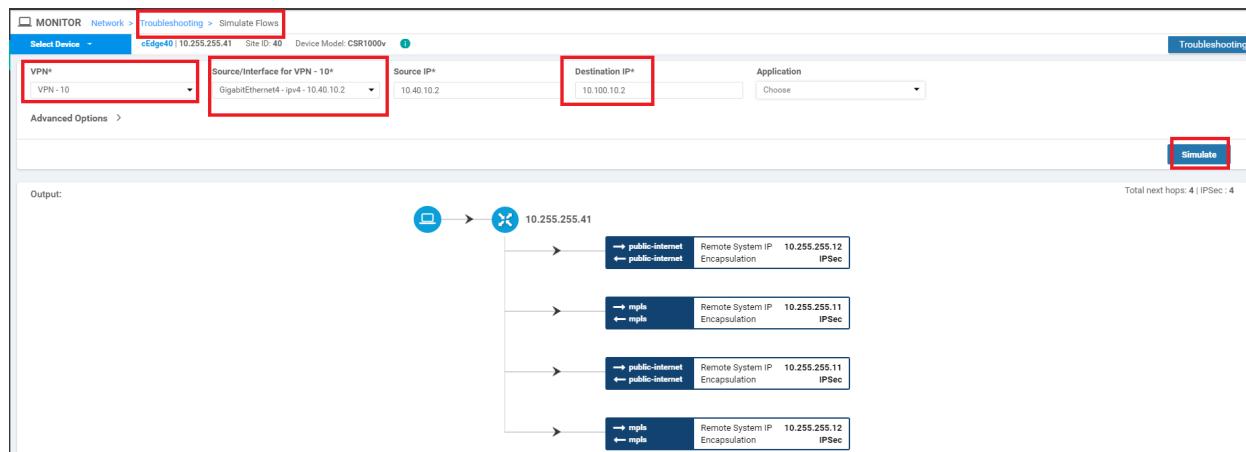
- [Overview](#)
- [Creating and Activating the AAR Policy](#)
- [Viewing modified traffic flows and current network statistics](#)
- [Configuring a Policer to simulate network impairment](#)
- [Creating a Policer List](#)
- [Configuring the IPv4 ACL Policy](#)
- [Applying the Policer on the MPLS link](#)
- [Viewing changed statistics and resultant traffic flows](#)

Viewing changed statistics and resultant traffic flows

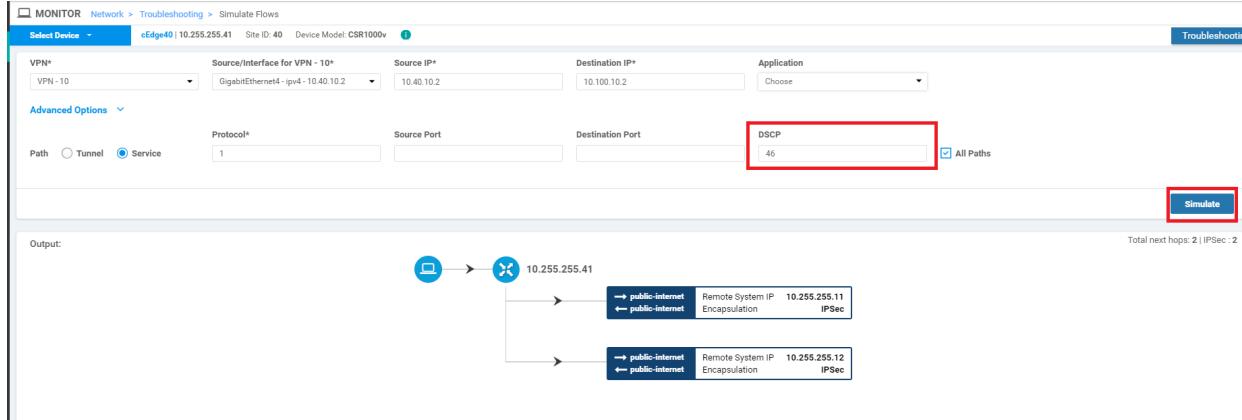
1. Navigate to **Monitor => Network** and click on cEdge40. Click on **Tunnel** on the left-hand side and make sure all the **MPLS** Tunnel Endpoint entries are selected, with the public-internet entries being unchecked. Click on **Real Time** (top right corner) and the Chart Options drop-down (top left corner) is set to Loss Percentage/FEC Loss Recovery Rate. Let this run for a few minutes - you will notice a spike in Packet Loss



2. Head over to **Troubleshooting** (left-hand side, might need to scroll down) and click on **Simulate Flows**. Enter the **VPN as VPN - 10**, the **Source/Interface** as *GigabitEthernet4* and the **Destination IP** as *10.100.10.2*. Click on **Simulate**. There should be no change in traffic flow for General traffic, which will still use all available transports



3. Under **Advanced Options**, set DSCP to a value of 46 and click on **Simulate**. You will notice that VoIP traffic (i.e. DSCP 46) is now taking the Internet path since MPLS doesn't conform to the SLA requirements that we defined. Compare the current traffic flow with the one in Step 2 [over here](#)



4. We will now revert the configuration to what it was pre-impairment. Go to **Configuration => Templates** and locate the **cEdge_dualuplink_devtemp**. Click on the three dots next to it and **Edit**. Change the Cisco VPN Interface Ethernet value under **Transport & Management VPN** back to **cedge-vpn0-int-dual_mpls** and click on **Update**. Click on **Next** and **Configure Devices**

CONFIGURATION | TEMPLATES

Basic Information **Transport & Management VPN** **Service VPN** **Additional Templates**

Cisco VPN 0 * cEdge_VPN0_dual_uplink

Cisco VPN Interface Ethernet cedge-vpn0-int-dual

Cisco VPN Interface Ethernet cedge-vpn0-int-dual_mpls

Cisco VPN 512 *

Cisco VPN Interface Ethernet cedge-vpn512-int-dual

Service VPN

0 Rows Selected **Add VPN** **Remove VPN**

| ID | Template Name |
|--------------------------------------|---------------|
| f018b46b-8ddc-431d-a222-cf905da7e13b | cedge-vpn10 |
| ff56fbce-0c12-4575-9f41-b6c7d780e20 | cedge-vpn20 |
| 9a88750f-7bd2-4fd5-b9d3-10a11544c8b6 | cedge-vpn30 |

Update Cancel

5. Wait for approximately 3 minutes and head over to **Monitor => Network => cEdge40 => Troubleshooting => Traffic Flows**. Enter the same details as in Step 3 above and click on **Simulate**. VoIP traffic should traverse over the MPLS link again

VPN Source/Interface for VPN - 10 Source IP Destination IP Application Custom Application (created in CLI)

Advanced Options

VPN - 10 GigabitEthernet4 - ipv4 - 10.40.1.1 10.40.10.2 10.100.10.2 Choose or

Protocol Source Port Destination Port DSCP

Path Tunnel Service 1 All Paths

Simulate

Total next hops: 2 | IPSec : 2

Output:

This completes the Application Aware Routing section of the lab.

Task List

- [Overview](#)
- [Creating and Activating the AAR Policy](#)
- [Viewing modified traffic flows and current network statistics](#)
- [Configuring a Policeer to simulate network impairment](#)
- [Creating a Policeer List](#)
- [Configuring the IPv4 ACL Policy](#)
- [Applying the Policeer on the MPLS link](#)
- [Viewing changed statistics and resultant traffic flows](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: June 3, 2020

Site last generated: Jul 23, 2020



-->

Configuring Low Latency Queuing and QoS

Summary: SD-WAN allows configuration of various QoS strategies to better support your business. Configure QoS with LLQ for VoIP traffic

Table of Contents

- [Create a Localized Policy](#)
 - [Add a Class List and a QoS Map](#)
 - [Configure the IPv4 ACL Policy](#)
 - [Complete and apply the localized policy](#)
- [Apply the ACL and QoS Map](#)
- [Activity Verification](#)

Task List

- Create a Localized Policy
 - Add a Class List and a QoS Map
 - Configure the IPv4 ACL Policy
 - Complete and apply the localized policy
- Apply the ACL and QoS Map
- Activity Verification

While Application Aware Routing allows us to choose the path taken by traffic and switch paths based on SLA parameters, QoS strategies in SD-WAN allow packets to be marked with standard DSCP values which are then utilized to prioritize packets accordingly.

Let's assume that our Corporate VPN (VPN 10) has, among other traffic, VoIP packets flowing through it. We would want to follow some QoS strategy to ensure that these VoIP (RTP, Video and Signalling) packets are placed in a Low Latency

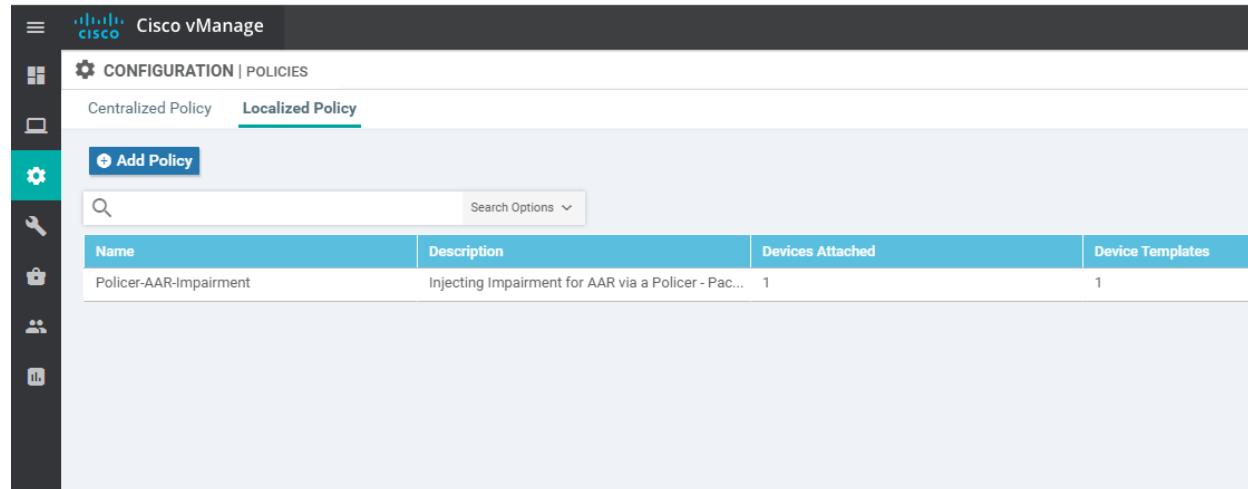
Queue, with corresponding strategies for other types of traffic.

Create a Localized Policy

QoS in the SD-WAN world is implemented via Localized Policies. Differences in Localized and Centralized Policies can be found [over here](#).

Add a Class List and a QoS Map

1. On the vManage GUI, click on **Configuration => Policies** and choose the **Localized Policy** tab. Click on **Add Policy**



The screenshot shows the Cisco vManage interface. The top navigation bar has the Cisco logo and 'Cisco vManage'. Below it, the 'CONFIGURATION | POLICIES' section is selected. Under 'POLICIES', the 'Localized Policy' tab is active, indicated by a green underline. To its left is the 'Centralized Policy' tab. A vertical sidebar on the left contains icons for Home, Configuration, Policies, Monitoring, Devices, Groups, and Help. In the main content area, there is a search bar with a magnifying glass icon and a 'Search Options' dropdown. Below the search bar is a table header with columns: Name, Description, Devices Attached, and Device Templates. A single row is listed: 'Name' is 'Policer-AAR-Impairment', 'Description' is 'Injecting Impairment for AAR via a Policer - Pac...', 'Devices Attached' is '1', and 'Device Templates' is '1'. At the top left of the main content area, there is a blue 'Add Policy' button with a plus sign icon. The entire window has a light gray background.

2. Under **Create Groups of Interest** click on **Class Map** on the left-hand side. Click on **New Class List** and specify the Class as **Voice**. The Queue should be **0**. Click on **Save**

The screenshot shows the Juniper Network Configuration interface under the 'POLICIES' section. A red box highlights the 'Localized Policy > Add Policy' link. Below it, a red box highlights the 'New Class List' button. On the left sidebar, 'Class Map' is selected and highlighted with a red box. The main area displays a 'Class List' dialog box with the following fields:

| Class | Queue |
|-------|-------|
| Voice | 0 |

A red box highlights the 'Save' button at the bottom right of the dialog.

This creates our Class List for VoIP traffic and puts the traffic in Queue 0.

3. Click on **New Class List** and create 3 more Class Lists, as shown below. Remember to hit **Save** after each Class List is created

| Class | Queue |
|-------------|-------|
| Video | 1 |
| BIZ-Data | 2 |
| Best-Effort | 3 |

Once all the Class Lists are created, click on **Next**

Select a list type on the left and start creating your groups of interest

| AS Path | New Class List | | | | |
|-----------|----------------|-------|-----------------|------------|----------------------------|
| Community | Class | Queue | Reference Count | Updated By | Last Updated |
| | Voice | 0 | 0 | admin | 04 Jun 2020 9:49:00 AM PDT |
| | Video | 1 | 0 | admin | 04 Jun 2020 9:49:17 AM PDT |
| | BIZ-Data | 2 | 0 | admin | 04 Jun 2020 9:49:27 AM PDT |
| | Best-Effort | 3 | 0 | admin | 04 Jun 2020 9:49:42 AM PDT |

Class Map

Mirror
Policer
Prefix

Next CANCEL

4. The Class Lists are referenced in QoS Maps. Under **Configure Forwarding Classes/QoS**, make sure you're on the QoS Map tab and click on **Add QoS Map**

CONFIGURATION | POLICIES Localized Policy > Add Policy

Create Groups of Interest Configure Forwarding Classes/QoS Configure Access Control Lists Configure Route Policy

QoS Map Policy Rewrite

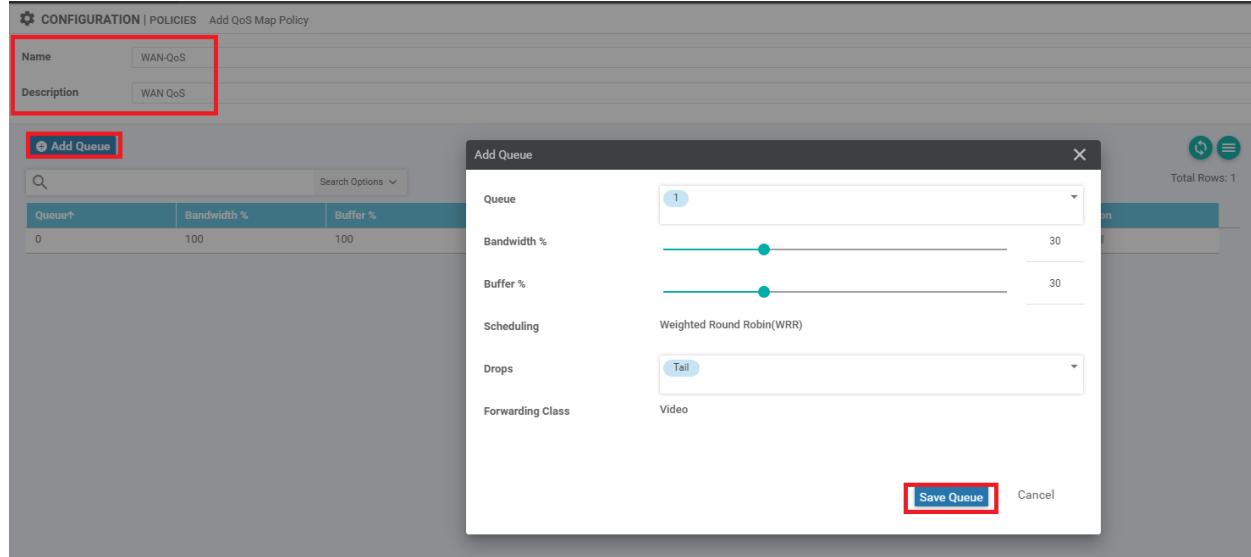
Add QoS Map (Add and Configure QoS Map)

Create New Import Existing Search Options

| Name | Type | Description | Reference Count | Updated By |
|-------------------|------|-------------|-----------------|------------|
| No data available | | | | |

5. Give the QoS Map a Name of *WAN-QoS* and a Description of *WAN QoS*. Click on **Add Queue**. Specify the following details and click on **Save Queue**

| Queue | Bandwidth % | Buffer % | Scheduling | Drops | Forwarding Class |
|-------|-------------|----------|---------------------------|-------|------------------------|
| 1 | 30 | 30 | Wighted Round Robin (WRR) | Tail | Video (Auto Populated) |



6. Click on **Add Queue** and add a couple more queues as per the table given below. Remember to click on **Save Queue** after you're done setting up the Queue

| Queue | Bandwidth % | Buffer % | Scheduling | Drops | Forwarding Class |
|-------|-------------|----------|----------------------------|--------------|------------------------------|
| 2 | 40 | 40 | Weighted Round Robin (WRR) | Random Early | BIZ-Data (Auto Populated) |
| 3 | 10 | 10 | Weighted Round Robin (WRR) | Random Early | Best-Effort (Auto Populated) |

CONFIGURATION | POLICIES Add QoS Map Policy

Name: WAN-QoS
Description: WAN QoS

Add Queue

| Queue | Bandwidth % | Buffer % |
|-------|-------------|----------|
| 0 | 70 | 70 |
| 1 | 30 | 30 |

Add Queue

Queue: 2

Bandwidth %: 40

Buffer %: 40

Scheduling: Weighted Round Robin(WRR)

Drops: Random Early

Forwarding Class: BIZ-Data

Save Queue **Cancel**

Queue 2

CONFIGURATION | POLICIES Edit QoS Map Policy

Name: WAN-QoS
Description: WAN QoS

Add Queue

| Queue | Bandwidth % | Buffer % |
|-------|-------------|----------|
| 0 | 30 | 30 |
| 1 | 30 | 30 |
| 2 | 40 | 40 |

Add Queue

Queue: 3

Bandwidth %: 10

Buffer %: 10

Scheduling: Weighted Round Robin(WRR)

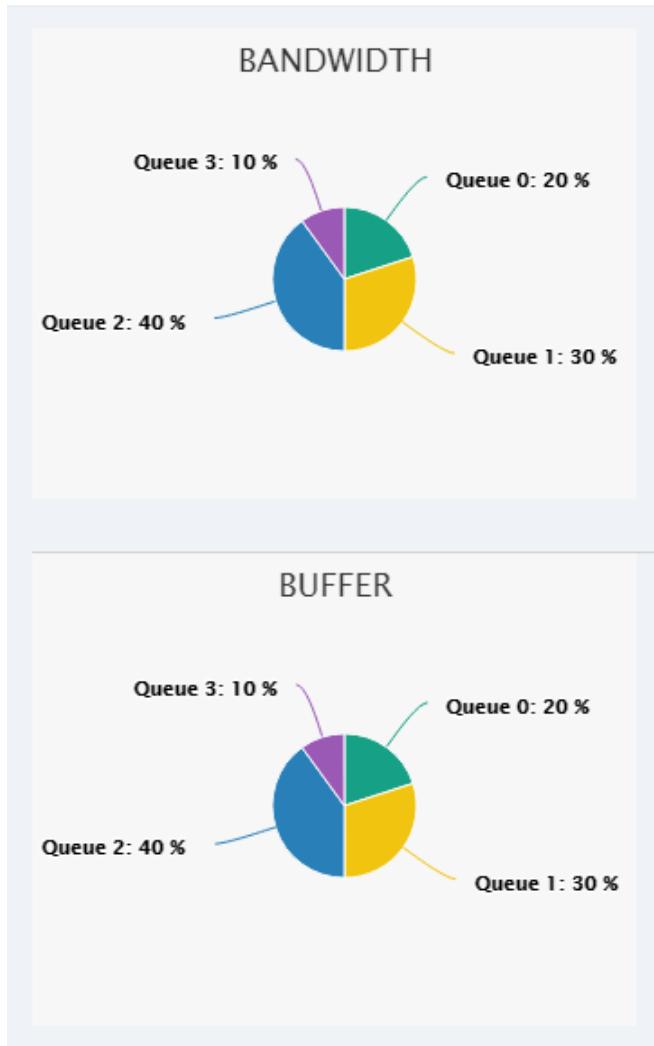
Drops: Random Early

Forwarding Class: Best-Effort

Save Queue **Cancel**

Queue 3

7. The wagon wheel that shows Queue Bandwidth and Buffer allocation should change to reflect the settings in the Queues that were just created



8. The QoS Map queues should look like the image below. Click on **Save Policy** to save your QoS Map and then click on **Next**

| Queue↑ | Bandwidth % | Buffer % | Burst | Scheduling Type | Drop Type | Forwarding Class | Action |
|--------|-------------|----------|-------|---------------------------|--------------|------------------|--------|
| 0 | 20 | 20 | 15000 | Low Latency Queuing(LLQ) | Tail | Control | |
| 1 | 30 | 30 | - | Weighted Round Robin(WRR) | Tail | Video | |
| 2 | 40 | 40 | - | Weighted Round Robin(WRR) | Random Early | BIZ-Data | |
| 3 | 10 | 10 | - | Weighted Round Robin(WRR) | Random Early | Best-Effort | |

Notice that the Queue 0 Forwarding Class is populated as **Control**. Control network traffic (not related to VoIP) is also included in Queue 0 by default. Any traffic that's mapped to Queue 0 is regarded as LLQ traffic.

This completes the QoS Map configuration. We will continue with building our Main Policy in the next section.

Task List

- Create a Localized Policy
 - [Add a Class List and a QoS Map](#)
 - [Configure the IPv4 ACL Policy](#)
 - [Complete and apply the localized policy](#)
- [Apply the ACL and QoS Map](#)
- [Activity Verification](#)

Configure the IPv4 ACL Policy

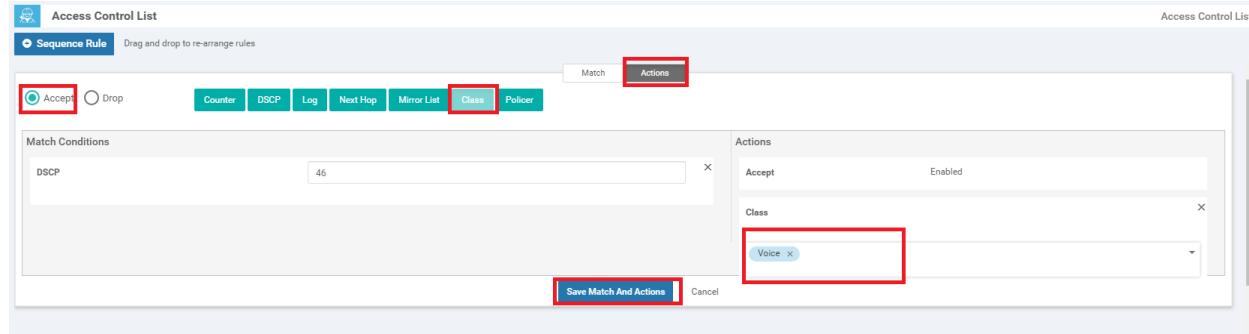
1. Continuing from the QoS Map which we just built, you should now be at the **Configure Access Control Lists** page. An ACL Policy can be used for classification of traffic on the LAN. Click on **Add Access Control List Policy** and choose to **Add IPv4 ACL Policy**

The screenshot shows the 'Add Policy' interface. At the top, there are several configuration options: 'Create Groups of Interest' (green checkmark), 'Configure Forwarding Classes/QoS' (green checkmark), 'Configure Access Control Lists' (blue circle, highlighted with a red box), and 'Configure Route Policy' (grey circle). Below these are two dropdown menus: 'Add Access Control List Policy' (selected) and 'Add Device Access Policy'. Under 'Add Access Control List Policy', there are three options: 'Add IPv4 ACL Policy' (selected), 'Add IPv6 ACL Policy', and 'Import Existing'. A search bar labeled 'Search Options' is also present. To the right, a table header is visible with columns: Type, Description, Reference Count, and Updated By.

2. Give the ACL Policy a Name of *LAN-Classification* and a Description of *LAN Classification*. Click on **Add ACL Sequence** and then click on **Sequence Rule**. Make sure you're on the Match tab and click on **DSCP**. Enter a DSCP value of **46**. This specifies our match criteria

The screenshot shows the 'Add IPv4 ACL Policy' configuration page. In the 'Name' field, 'LAN-Classification' is entered. In the 'Description' field, 'LAN Classification' is entered. On the left, there's a sidebar with 'Add ACL Sequence' (selected) and 'Access Control List'. The main area shows an 'Access Control List' with a 'Sequence Rule' section. A 'Match' tab is selected. Under 'Match Conditions', there is a 'DSCP' entry with the value '46' (highlighted with a red box). An 'Actions' column contains an 'Accept' button.

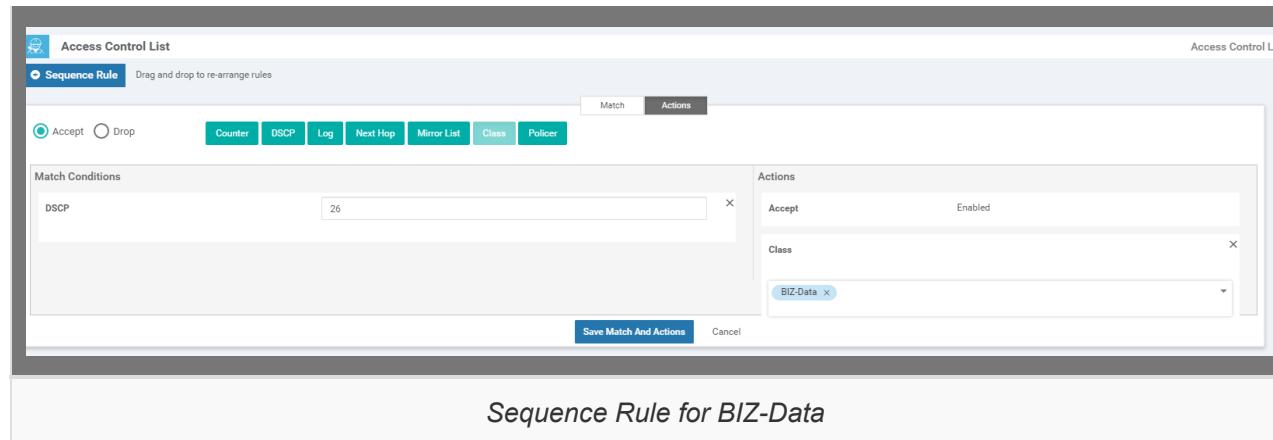
3. Click on the **Actions** tab and make sure the **Accept** radio button is selected. Click on **Class** and select the *Voice* Class List which we created before. Click on **Save Match and Actions**



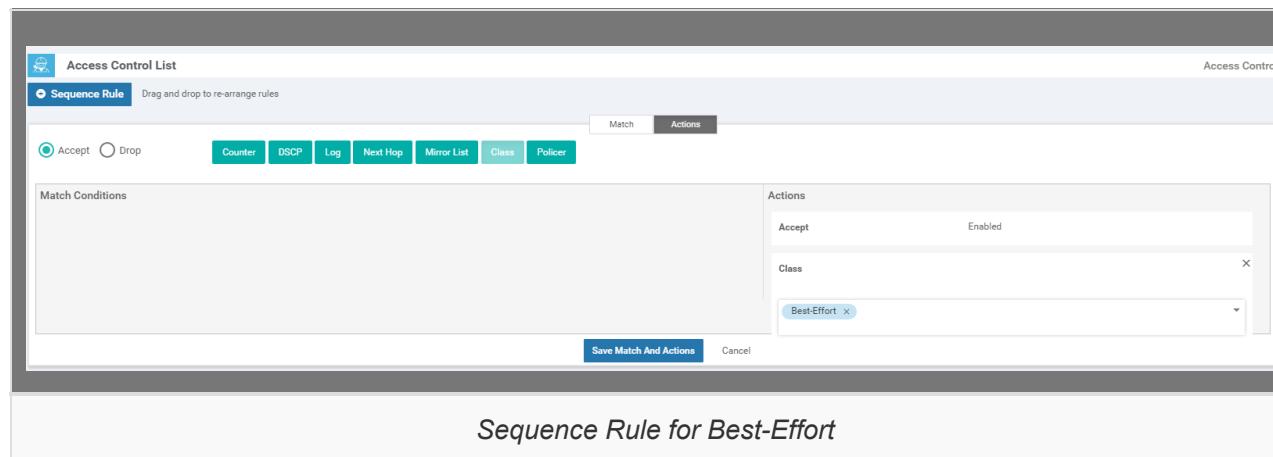
4. Click on **Sequence Rule** and follow the same procedure to create rules as per the following table. Use the images below the table for reference (the actions tab should always have the Accept radio button selected). Make sure that you click on **Save Match and Actions** once done creating each rule

| DSCP | Class |
|-------------|-------------|
| 34 | Video |
| 26 | BIZ-Data |
| Leave Blank | Best-Effort |

Sequence Rule for Video



Sequence Rule for BIZ-Data



Sequence Rule for Best-Effort

5. Verify that the Access Control List Policy looks like the image below (i.e. you should see 4 sequence rules, one for each Class List with the corresponding DSCP values as match conditions) and click on **Save Access Control List Policy**

Name LAN-Classification

Description LAN Classification

Add ACL Sequence **Access Control List** **Sequence Rule** Drag and drop to re-order **Sequence Rule** Drag and drop to re-arrange rules

Access Control List **Default Action**

Match Conditions **Actions**
DSCP: 46 Accept
Class: Voice

Match Conditions **Actions**
DSCP: 34 Accept
Class: Video

Match Conditions **Actions**
DSCP: 26 Accept
Class: BIZ-Data

Match Conditions **Actions**
Accept
Class: Best-Effort

Save Access Control List Policy CANCEL

6. Click on **Next** twice and you should be at the **Policy Overview** page, which continues in the next section.

Task List

- Create a Localized Policy
 - [Add a Class List and a QoS Map](#)
 - [Configure the IPv4 ACL Policy](#)
 - Complete and apply the localized policy
- Apply the ACL and QoS Map
- Activity Verification

Complete and apply the localized policy

1. Continuing from the previous section, while on the **Policy Overview** page, give your policy a Name of **QoS_Policy** and a Description of QoS Policy. Under **Policy Settings**, put a check mark next to **Application** and set the Log Frequency to 30 (this will come into play if you are going through the SD-AVC configuration section). Click on **Save Policy**

Enter name and description for your localized master policy

Policy Name: QoS_Policy

Policy Description: QoS Policy

Policy Settings

Netflow Application Cloud QoS Cloud QoS Service side Implicit ACL Logging

Log Frequency: 3d

BACK Preview **Save Policy** CANCEL

2. Navigate to Configuration => Templates and locate the `cedge_dualuplink_devtemp` Device Template. Click on the three dots next to it and choose to **Edit**. Click on **Additional Templates**

CONFIGURATION | TEMPLATES

Device Feature

Device Model: CSR1000v

Template Name: cEdge_dualuplink_devtemp

Description: cEdge Device Template for devices with a dual uplink

Basic Information Transport & Management VPN Service VPN **Additional Templates**

Basic Information

Cisco System *: Default_System_Cisco_V01

Cisco Logging*: Default_Logging_Cisco_V01

3. Populate **QoS_Policy** in the **Policy** drop down. If you have gone through the Guest DIA configuration, note that this will break Guest DIA functionality. In the real world, the QoS Policy we configured should be included within the same policy. Click on **Update**

Additional Templates

| | |
|---------------------|---------------------------------------|
| AppQoE | Choose... |
| Global Template * | Factory_Default_Global_CISCO_Template |
| Cisco Banner | Choose... |
| Cisco SNMP | Choose... |
| CLI Add-On Template | Choose... |
| Policy | QoS_Policy |
| Probes | Choose... |
| Security Policy | Site40-Guest-DIA |

Update **Cancel**

4. Click on **Next** and then **Configure Devices**. You can view the side by side configuration, if you want to

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. On the left, a sidebar lists icons for Device Template, Device list, and a specific device entry: 'CSR-04F94B2E-44F0-E4DC-D30D-60C0B06F7F2'. The main area displays a configuration script with line numbers from 266 to 322. A yellow callout box at the top right states: "'Configure' action will be applied to 1 device(s) attached to 1 device template(s.)". At the bottom right of the configuration window, there are 'Back', 'Configure Devices' (which is highlighted with a red box), and 'Can' buttons.

```
266 !  
267 !  
268 policy-map type inspect avc ftp-pm_  
269 class ftp-cmo_  
270 deny  
271 !  
272 !  
273 interface GigabitEthernet1  
274 no shutdown  
275 arp timeout 1200  
276 vrf forwarding Mgmt-intf  
277 ip address 192.168.0.40 255.255.255.0  
278 no ip redirects  
279 ip mtu 1500  
280 mtu 1500  
290 !  
291 !  
292 policy-map WAN-QoS  
293 class Queue0  
294 priority level 1  
295 police rate percent 20  
296 !  
297 !  
298 class Queue1  
299 bandwidth remaining ratio 30  
300 !  
301 class class-default  
302 bandwidth remaining ratio 40  
303 random-detect precedence-based  
304 !  
305 class Queue3  
306 bandwidth remaining ratio 10  
307 random-detect precedence-based  
308 !  
309 !  
310 policy-map type inspect avc ftp-pm_  
311 class ftp-cmo_  
312 deny  
313 !  
314 !  
315 interface GigabitEthernet1  
316 no shutdown  
317 arp timeout 1200  
318 vrf forwarding Mgmt-intf  
319 ip address 192.168.0.40 255.255.255.0  
320 no ip redirects  
321 ip mtu 1500  
322 mtu 1500
```

We have completed application of the QoS Policy for our Device. This will create the QoS Maps and inject the corresponding Queues in the Scheduler.

Tip: vManage pushes the forwarding class names as Queue0, Queue1 etc. along with the created Class Names. Queue0, Queue1 etc. are the ones which are actually used in the qos-map but the settings are based on the defined class names (e.g. Voice, Video, BIZ-Data etc. for our lab). This is expected behaviour. Additionally, you will **NOT** see Queue 2 in the QoS policy-map interface output since that is used for Best Effort traffic by default. However, if we were to map the Queues to 0 for Voice, 1 for Video, 3 for BIZ-Data and 4 for Best-Effort, all 4 queues will show up.

Task List

- [Create a Localized Policy](#)
 - [Add a Class List and a QoS Map](#)
 - [Configure the IPv4 ACL Policy](#)
 - [Complete and apply the localized policy](#)
- [Apply the ACL and QoS Map](#)
- [Activity Verification](#)

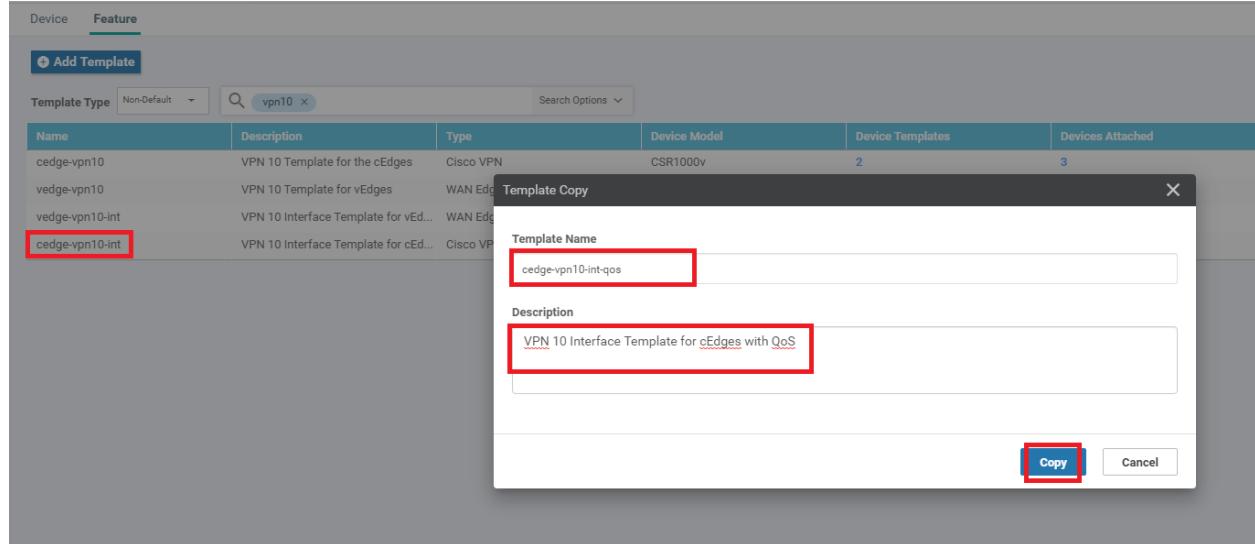
Apply the ACL and QoS Map

We have created the QoS strategy for our network, the only thing that's left is to apply and test our QoS configuration.

To apply the configuration, we will be modifying the Service VPN 10 interface such that traffic is classified on the basis of the ACL we created, in the inbound direction.

The QoS Map will be applied in the outbound direction on the WAN interfaces (INET and MPLS)

1. Navigate to **Configuration => Templates => Feature Tab** and locate the `cedge-vpn10-int` Feature Template. Click on the three dots next to it and choose to **Copy** the Template. Give a name of `cedge-vpn10-int-qos` to the copied template with a Description of *VPN 10 Interface Template for cEdges with QoS* and click on **Copy**



2. Locate the newly copied `cedge-vpn10-int-qos` Feature Template and click on the three dots next to it. Choose to **Edit** the template. Make sure the Description is updated and scroll down to the ACL/QoS section. Set **Ingress ACL - IPv4** to a Global value of **On** and enter *LAN-Classification* as the **IPv4 Ingress Access List**. This needs to match with the ACL we created (case sensitive). Click on **Update**

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN Interface Ethernet

| Basic Configuration | Tunnel | NAT | VRRP | ACL/QoS | ARP | Advanced |
|--|---|-----|------|---------|-----|----------|
| ACL/QoS | | | | | | |
| Shaping Rate (Kbps) | <input checked="" type="checkbox"/> <input type="text"/> | | | | | |
| QoS Map | <input checked="" type="checkbox"/> <input type="text"/> | | | | | |
| Rewrite Rule | <input checked="" type="checkbox"/> <input type="text"/> | | | | | |
| Ingress ACL - IPv4 | <input checked="" type="checkbox"/> <input checked="" type="radio"/> On <input type="radio"/> Off | | | | | |
| <input checked="" type="checkbox"/> LAN-Classification | | | | | | |
| Egress ACL - IPv4 | <input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off | | | | | |
| Ingress ACL - IPv6 | <input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off | | | | | |
| Egress ACL - IPv6 | <input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off | | | | | |
| ARP | | | | | | |
| <input style="border: 2px solid red; padding: 2px;" type="button" value="Update"/> <input type="button" value="Cancel"/> | | | | | | |

3. Navigate to the Device tab in **Configuration => Templates** and locate the *cedge_dualuplink_devtemp*. Click on the three dots next to it and choose **Edit**

CONFIGURATION | TEMPLATES

Device Feature

Create Template

Template Type Non-Default Search Options

Total Rows: 6

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Actions |
|---------------------------------|------------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|---|
| DCvEdge_dev_temp | Device template for the DC-VE... | Feature | vEdge Cloud | 16 | 2 | admin | 28 May 2020 4:58:07 AM PDT | In Sync | <input type="button" value="..."/> |
| cEdge-single-uplink | Single Uplink cEdge Device Te... | Feature | CSR1000v | 17 | 2 | admin | 26 May 2020 3:05:01 AM PDT | In Sync | <input type="button" value="..."/> |
| cEdge_dualuplink_devtemp | cEdge Device Template for dev... | Feature | CSR1000v | 19 | 1 | admin | 04 Jun 2020 10:06:05 AM PDT | In Sync | <input type="button" value="..."/> |
| vEdge_Site20_dev_temp | Device template for the Site 20... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 PM PDT | In Sync | <input type="button" value="Edit"/> |
| vSmart-dev-temp | Device Template for vSmarts | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 AM PDT | In Sync | <input type="button" value="View"/> <input type="button" value="Delete"/> <input type="button" value="Copy"/> <input type="button" value="Attach Devices"/> <input type="button" value="Detach Devices"/> <input type="button" value="Export CSV"/> <input type="button" value="Change Device Values"/> |
| vEdge30_dev_temp | Device template for the Site 30... | Feature | vEdge Cloud | 15 | 1 | admin | 05 Jun 2020 9:57:40 PM PDT | In Sync | |

4. In the **Service VPN** section, click on the three dots next to the *cedge-vpn10* Template and choose **Edit**

| Service VPN | | | |
|--|---------------|-------------------------------------|---|
| 1 Rows Selected | | Add VPN | Remove VPN |
| ID | Template Name | Sub-Templates | |
| <input checked="" type="checkbox"/> f018b46b-8ddc-431d-a222-cf905da7e13b | cedge-vpn10 | Cisco VPN Interface Ethernet, EIGRP | Edit Copy Sub-Templates ... |
| <input type="checkbox"/> ff56fbce-0c12-4575-9f41-b6c7d780e13d | cedge-vpn20 | Cisco VPN Interface Ethernet | ... |
| <input type="checkbox"/> 9a88750f-7bd2-4fd5-b9d3-10a11544c9b6 | cedge-vpn30 | Cisco VPN Interface Ethernet | ... |

5. Change the template under **Cisco VPN Interface Ethernet** to **cedge-vpn1-int-qos** and click on **Save**

Edit VPN - cedge-vpn10

| | | |
|------------------------------|--|-------------------------------|
| Cisco VPN Interface Ethernet | <input type="text" value="cedge-vpn10-int-qos"/> | Sub-Templates |
| EIGRP | <input type="text" value="site40-eigrp"/> | |

[Save](#) [CANCEL](#)

6. Click on **Next** and choose to **Configure Devices**. The side-by-side configuration can be viewed and we should see the *LAN-Classification* ACL being applied on GigabitEthernet4 (Service VPN Interface for VPN 10) in the incoming direction

| Device Template | | Total | 'Configure' action will be applied to 1 device(s) attached to 1 device template(s). | |
|---|----------------------------|-------|---|-----|
| cEdge_dualuplink_devtemp | 1 | 98 | no allow-service ntp | 98 |
| Device list (Total: 1 devices) | | | | |
| Filter/Search | | | | |
| CSR-04F9482E-44F0-E4DC-D30D- | 60C0806F73F2 | 100 | no allow-service ospf | 99 |
| cEdge40 10.255.255.41 | | 101 | no allow-service stun | 100 |
| | | 102 | allow-service https | 101 |
| | | 103 | no allow-service snmp | 102 |
| Device Template | exit | 104 | exit | 103 |
| | | | | 104 |
| | | | | 105 |
| CSR-04F9482E-44F0-E4DC-D30D- | 60C0806F73F2 | 106 | interface GigabitEthernet4 | 106 |
| cEdge40 10.255.255.41 | | 107 | access-list LAN-Classification in | 107 |
| | | | | 108 |
| Device Template | exit | 109 | | 109 |
| | | | | 110 |
| CSR-04F9482E-44F0-E4DC-D30D- | 60C0806F73F2 | 111 | appqoe | 111 |
| cEdge40 10.255.255.41 | | 112 | no tcpopt enable | 112 |
| | | 113 | ! | 113 |
| Device Template | ! cmp | 114 | no shutdown | 114 |
| | | 115 | send-path-limit 4 | 115 |
| CSR-04F9482E-44F0-E4DC-D30D- | 60C0806F73F2 | 116 | ecmp-limit 4 | 116 |
| cEdge40 10.255.255.41 | | 117 | graceful-restart | 117 |
| | | 118 | no as-dot-notation | 118 |
| Device Template | timers | 119 | holdtime 60 | 119 |
| | | 120 | advertisement-interval 1 | 120 |
| CSR-04F9482E-44F0-E4DC-D30D- | 60C0806F73F2 | 121 | graceful-restart-timer 43200 | 121 |
| cEdge40 10.255.255.41 | | 122 | eor-timer 300 | 122 |
| | | 123 | exit | 123 |
| Device Template | address-family ipv4 vrf 10 | 124 | address-family ipv4 vrf 10 | 124 |
| | | 125 | advertise connected | 125 |
| CSR-04F9482E-44F0-E4DC-D30D- | 60C0806F73F2 | 126 | advertise static | 126 |
| cEdge40 10.255.255.41 | | 127 | advertise eigrp | 127 |
| | | 128 | ! | 128 |
| Device Template | address-family ipv4 vrf 20 | 129 | address-family ipv4 vrf 20 | 129 |
| | | 130 | advertise connected | 130 |
| | | | advertise static | 130 |
| Configure Device Rollback Timer | | Back | Configure Devices | |

7. Head back over to **Configuration => Template => Feature Tab** and locate the *cedge-vpn0-int-dual* template. Click on the three dots next to it and click **Edit**. We will be updating the VPN 0 Internet interface with the QoS Map we created before

| Device | Feature | Template Overview | | | | | | | Total Rows: 16 of 16 | |
|---------------------------|--------------------------------------|---------------------|--------------|------------------|------------------|------------|----------------------------|--------------------------------------|----------------------|--|
| Add Template | | Template Type | Non-Default | Search | Search Options | | | | | |
| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions | | |
| cedge-vpn0-int-single | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | View | Edit | |
| cedge-vpn0-int-dual_mlps | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 23 May 2020 7:15:33 AM PDT | View | Edit | |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 03 Jun 2020 7:01:36 AM PDT | View | Edit | |
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Template... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 | View | Edit | |
| cedge-vpn10 | VPN 10 Template for the cEdges | Cisco VPN | CSR1000v | 2 | 3 | admin | 26 May 2020 | View | Edit | |
| ctedge_VPN512_dual_Uplink | cEdge VPN 512 Template for Dual U... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 | Change Device Models | | |
| cedge_VPN0_dual_Uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin | 23 May 2020 | Delete | | |
| cedge-vpn20 | VPN 20 Template for the cEdges | Cisco VPN | CSR1000v | 2 | 3 | admin | 25 May 2020 | Copy | | |

8. Under the **ACL/QOS** section, specify the **QoS Map** as a Global value and enter WAN-QoS (case sensitive, should match with the QOS Map we created before). Click on **Update**

S CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco VPN Interface Ethernet

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP Advanced

ACL/QoS

Shaping Rate (Kbps)

QoS Map (WAN-QoS)

Rewrite Rule

Ingress ACL - IPv4 (On)

Egress ACL - IPv4 (On)

Ingress ACL - IPv6 (On)

Egress ACL - IPv6 (On)

ARP

New ARP

Update Cancel

The screenshot shows the configuration interface for a Cisco VPN Interface Ethernet. The 'ACL/QoS' tab is active. In the 'QoS Map' section, a dropdown menu is open, and the option 'WAN-QoS' is selected. This selection is highlighted with a red rectangular box. Below this, there are sections for Rewrite Rule, Ingress/Egress ACLs for both IPv4 and IPv6, all set to 'On'. The 'ARP' section has a 'New ARP' button and an 'Update' button, which is also highlighted with a red rectangular box. At the bottom right of the main configuration area, there are 'Update' and 'Cancel' buttons.

9. Click on **Next** and then **Configure Devices**. If you want, inspect the side-by-side configuration before clicking on **Configure Devices** and you will notice that the WAN-QoS Policy will be applied to GigabitEthernet2 (WAN VPN 0 Interface for INET)

The screenshot shows the Cisco vManage interface under the Configuration > Templates section. A device template named "cEdge_dualuplink_devtemp" is selected, indicated by a blue border. The configuration code area displays a large block of CLI-style configuration commands. A yellow callout box at the top right states: "'Configure' action will be applied to 1 device(s) attached to 1 device template(s.)". At the bottom right of the configuration area, there are three buttons: "Back", "Configure Devices" (highlighted with a red box), and "Cancel".

```

323 negotiation auto
324 exit
325 interface GigabitEthernet2
326 no shutdown
327 arp timeout 1200
328 ip address 100.100.100.40 255.255.255.0
329 no ip redirects
330 ip mtu 1500
331 ip nat outside
332 mtu 1500
333 negotiation auto
334 service-policy output WAN-QoS
335 exit
336 interface GigabitEthernet3
337 no shutdown
338 arp timeout 1200
339 ip address 192.1.2.18 255.255.255.252
340 no ip redirects
341 ip mtu 1500
342 mtu 1500
343 negotiation auto
344 exit
345 interface GigabitEthernet4
346 no shutdown
347 arp timeout 1200
348 vrf forwarding 10
349 ip address 10.40.10.2 255.255.255.0
350 no ip redirects
351 ip mtu 1500
352 mtu 1500
353 negotiation auto
354 exit
355

```

10. Under the Configuration => Template => Feature Tab locate the `cedge-vpn0-int-dual_mpls` template. Click on the three dots next to it and click **Edit**. We will be updating the VPN 0 MPLS interface with the QoS Map we created before

The screenshot shows the Cisco vManage interface under the Configuration > Templates > Feature tab. A template named "cedge-vpn0-int-dual_mpls" is selected, highlighted with a yellow background. A context menu is open over this row, with the "Edit" option highlighted with a red box. Other options in the menu include "View", "Change Device Models", "Delete", and "Copy". The table header includes columns for Name, Description, Type, Device Model, Device Templates, Devices Attached, Updated By, Last Updated, and actions. The table shows 16 of 36 total rows.

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------|--------------------------------------|---------------------|--------------|------------------|------------------|------------|-----------------------------|-------------|
| cedge-vpn0-int-single | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| cedge-vpn0-int-dual_mpls | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 23 May 2020 7:15:33 AM PDT | ... |
| cedge-vpn512-int-dual | cEdge VPN 512 Interface Template... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 | Edit |
| cedge-vpn10 | VPN 10 Template for the cEdges | Cisco VPN | CSR1000v | 2 | 3 | admin | 26 May 2020 | ... |
| cEdge_VPN512_dual_uplink | cEdge VPN 512 Template for Dual ... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 | ... |
| cEdge_VPN0_dual_uplink | cEdge VPN 0 Template for Dual Up... | Cisco VPN | CSR1000v | 1 | 1 | admin | 23 May 2020 | ... |
| cedge-vpn20 | VPN 20 Template for the cEdges | Cisco VPN | CSR1000v | 2 | 3 | admin | 25 May 2020 | ... |
| cedge-vpn0-int-dual | cEdge VPN 0 Interface Template fo... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 05 Jun 2020 11:23:33 PM PDT | ... |
| carinaunifire | VPN 50 Interface Template for cEd... | Cisco VPN Interface | CSR1000v | 2 | 2 | admin | 24 Mar 2020 7:09:27 PM PDT | ... |

11. Under the **ACL/QOS** section, specify the **QoS Map** as a Global value and enter **WAN-QoS** (case sensitive, should match with the QOS Map we created before). Click on **Update**

The screenshot shows the 'Feature' tab selected in the top navigation bar. Below it, the 'Cisco VPN Interface Ethernet' feature template is chosen. The main content area has tabs for 'Basic Configuration', 'Tunnel', 'NAT', 'VRRP', 'ACL/QoS' (which is active and highlighted in green), 'ARP', and 'Advanced'. Under the 'ACL/QoS' tab, there are several configuration sections: 'Shaping Rate (Kbps)', 'QoS Map' (with a dropdown menu showing 'WAN-QoS' highlighted by a red box), 'Rewrite Rule', and four pairs of 'Ingress ACL - IPv4/IPv6' and 'Egress ACL - IPv4/IPv6' settings, each with an 'On' or 'Off' radio button. At the bottom of the page, under the 'ARP' tab, there is a 'New ARP' button. A horizontal bar at the very bottom contains 'Update' and 'Cancel' buttons, with 'Update' also highlighted by a red box.

12. Click on **Next** and then **Configure Devices**. If you want, inspect the side-by-side configuration before clicking on **Configure Devices** and you will notice that the WAN-QoS Policy will be applied to GigabitEthernet3 (WAN VPN 0 Interface for MPLS). Check the configuration pushed by logging in to the CLI for cEdge40 via Putty and issuing `show running | sec interface Gig`. We should see the WAN_QoS policy applied under GigabitEthernet2 and GigabitEthernet3

```
interface GigabitEthernet1
no shutdown
arp timeout 1200
vrf forwarding Mgmt-intf
ip address 192.168.0.40 255.255.255.0
no ip redirects
ip mtu    1500
mtu 1500
negotiation auto
exit
interface GigabitEthernet2
no shutdown
arp timeout 1200
ip address 100.100.100.40 255.255.255.0
no ip redirects
ip mtu    1500
ip nat outside
mtu 1500
negotiation auto
service-policy output WAN-QoS
exit
interface GigabitEthernet3
no shutdown
arp timeout 1200
ip address 192.1.2.18 255.255.255.252
no ip redirects
ip mtu    1500
mtu 1500
negotiation auto
service-policy output WAN-QoS
exit
```

This completes the configuration of our QoS Policy in VPN 10 at Site 40.

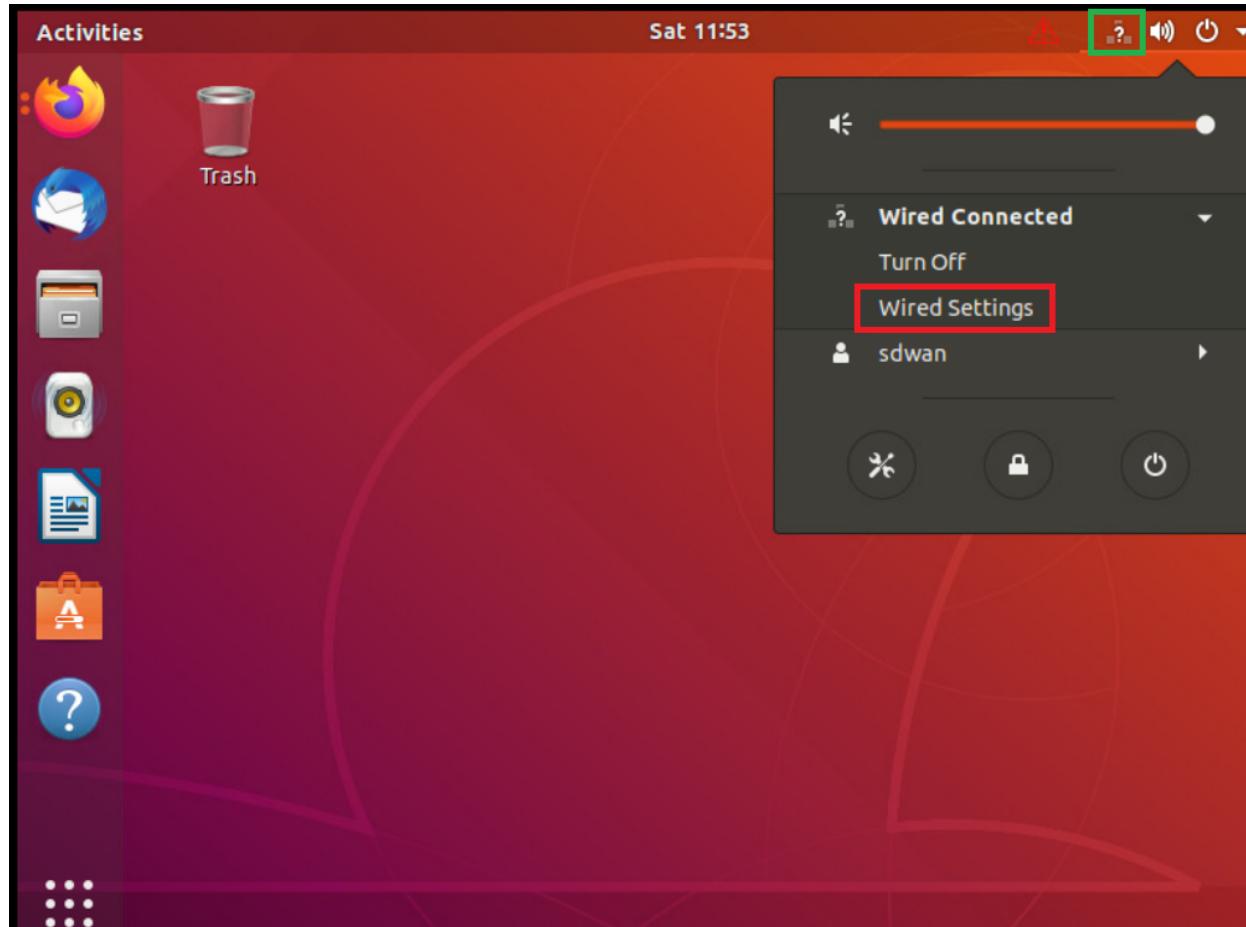
Task List

- [Create a Localized Policy](#)

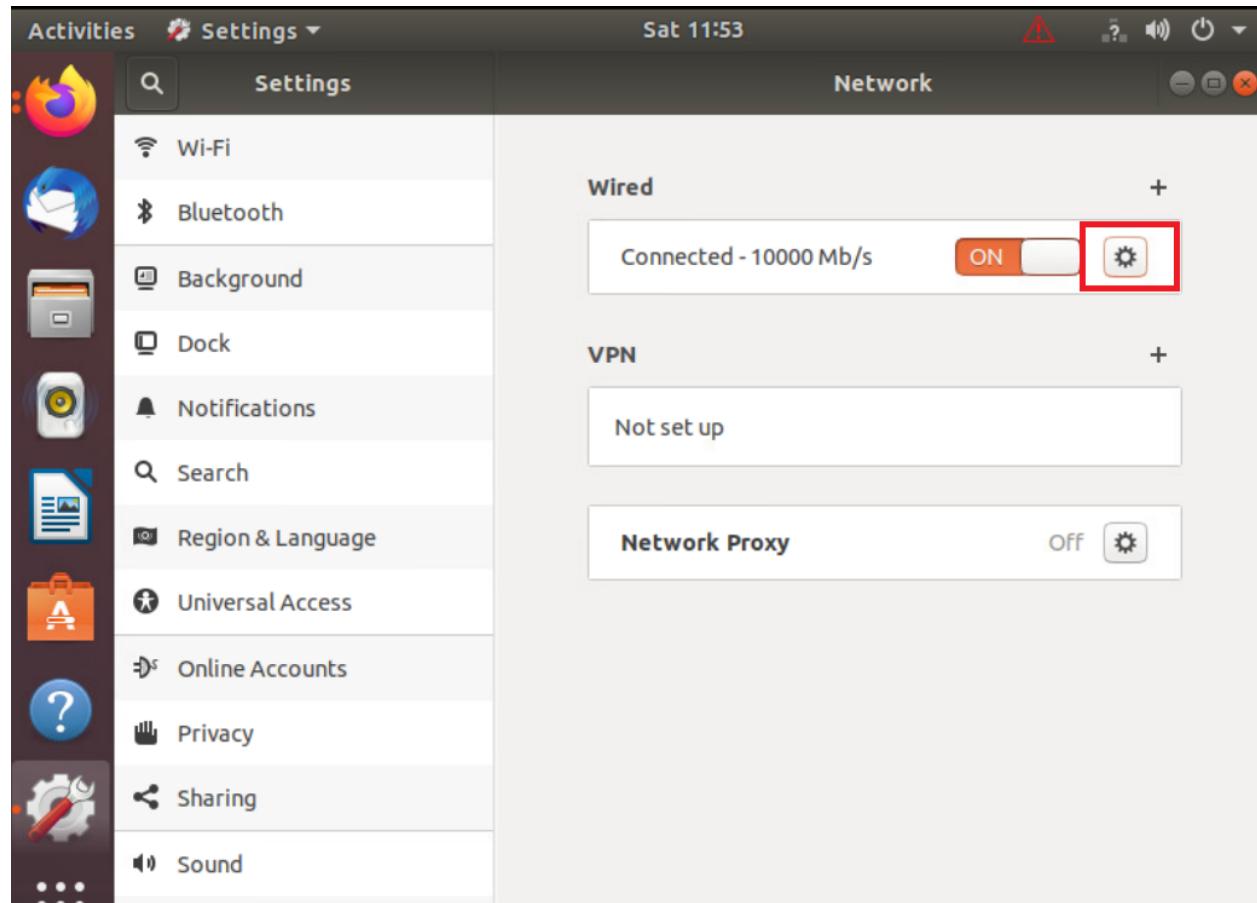
- Add a Class List and a QoS Map
- Configure the IPv4 ACL Policy
- Complete and apply the localized policy
- Apply the ACL and QoS Map
- Activity Verification

Activity Verification

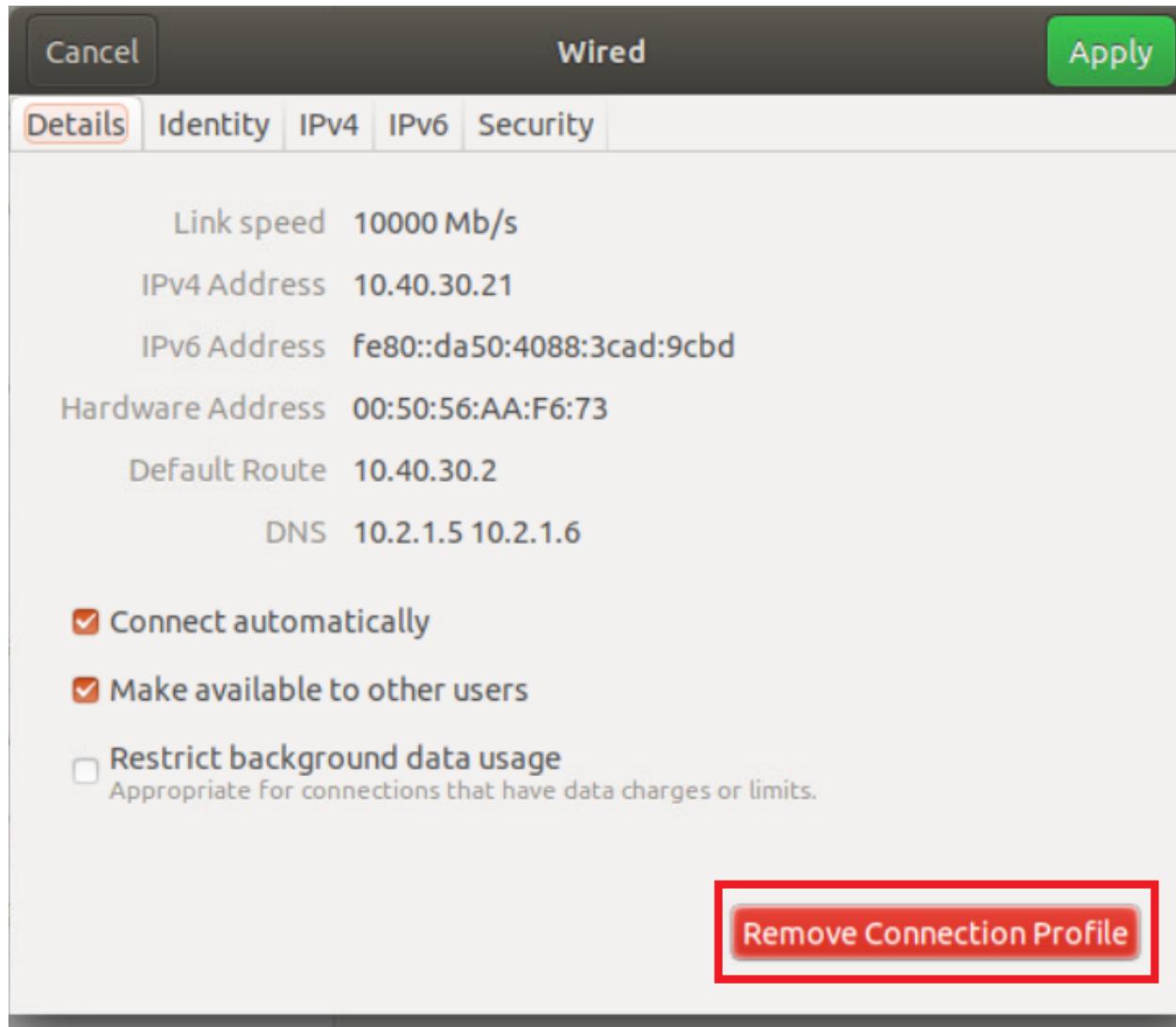
1. Log in to vCenter (use the bookmark or go to 10.2.1.50/ui) using the credentials provided to you. Locate the sdwan-slc/ghi-site40pc-podX VM and click on it. Open the Web Console to the Site 40 PC VM and log in. The Username is sdwan and the password is C1sco12345. Click the network icon in the top-right corner and go to Wired Settings



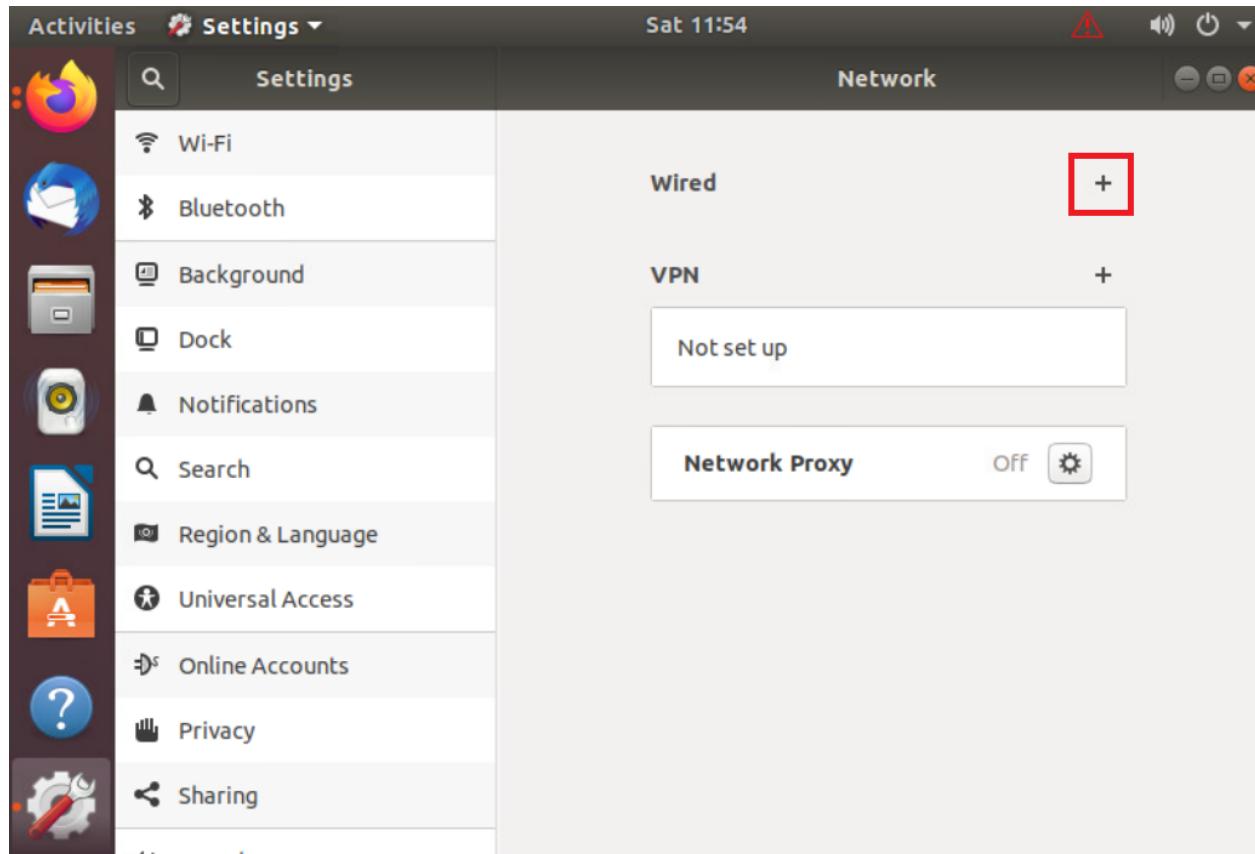
2. Click on the cog wheel/gear icon



3. Click on Remove Connection Profile



4. The + sign should show up next to **Wired**. If you still see a cog wheel/gear icon, click on it and choose Remove Connection Profile again. Once the + icon is visible, click on it



5. Go to the **IPv4** tab and set the **IPv4 Method** as Manual. Enter the following details and click on **Add**

| Address | Netmask | Gateway | DNS |
|--------------------|---------------|------------|-----------------|
| 10.40.10.21 | 255.255.255.0 | 10.40.10.2 | Automatic - Off |
| 10.y.1.5, 10.y.1.6 | | | |

Over here, y is 1 if you're on the SLC DC and 2 if you're on the GHI DC (the email with lab details should enumerate which DC you're on).

New Profile

Add

Identity IPv4 IPv6 Security

IPv4 Method

Automatic (DHCP)
 Manual
 Link-Local Only
 Disable

Addresses

| Address | Netmask | Gateway |
|-------------|---------------|------------|
| 10.40.10.21 | 255.255.255.0 | 10.40.10.2 |
| | | |

DNS

Automatic OFF

10.2.1.5, 10.2.1.6

Separate IP addresses with commas

Routes

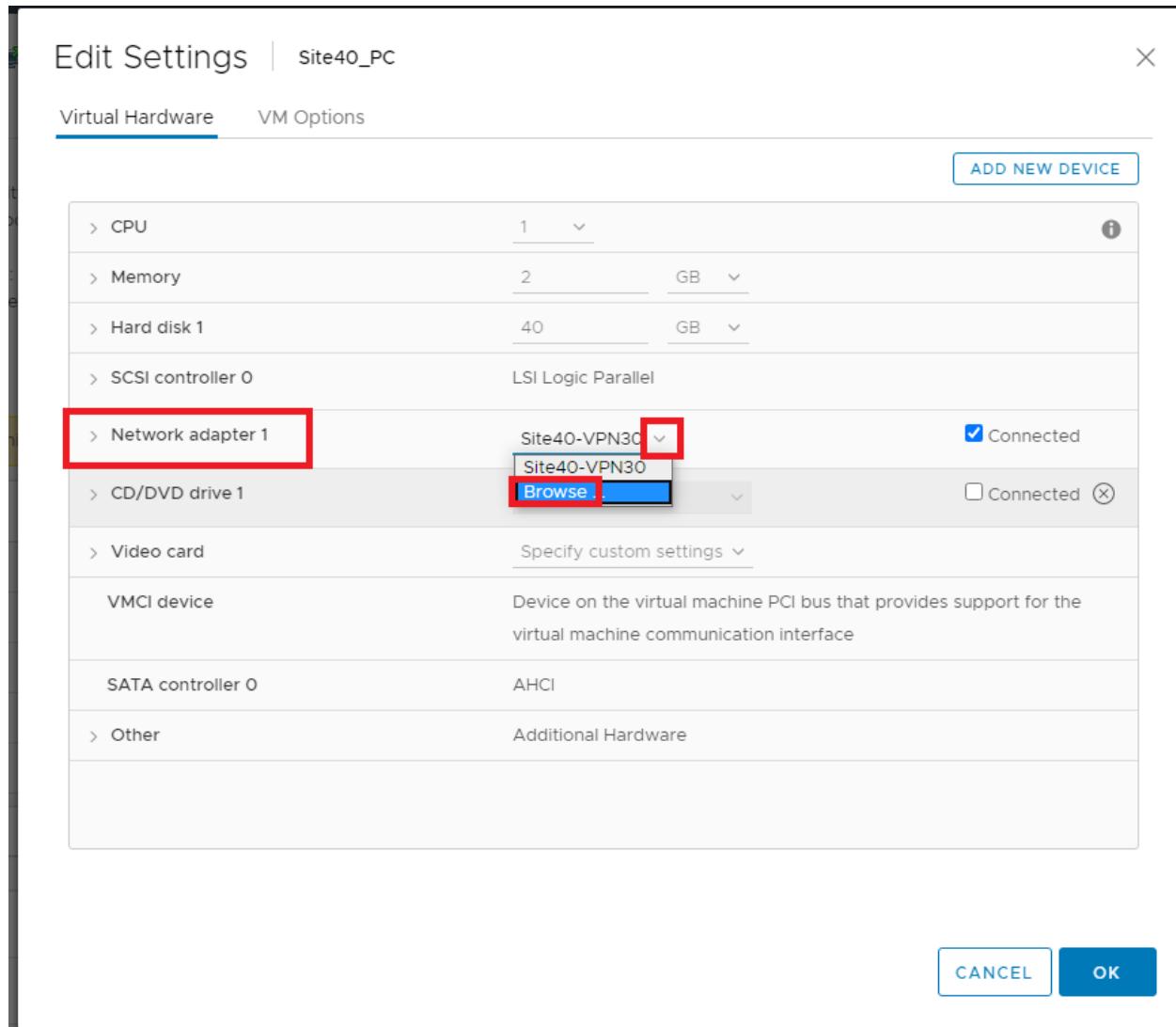
Automatic ON

| Address | Netmask | Gateway | Metric |
|---------|---------|---------|--------|
| | | | |

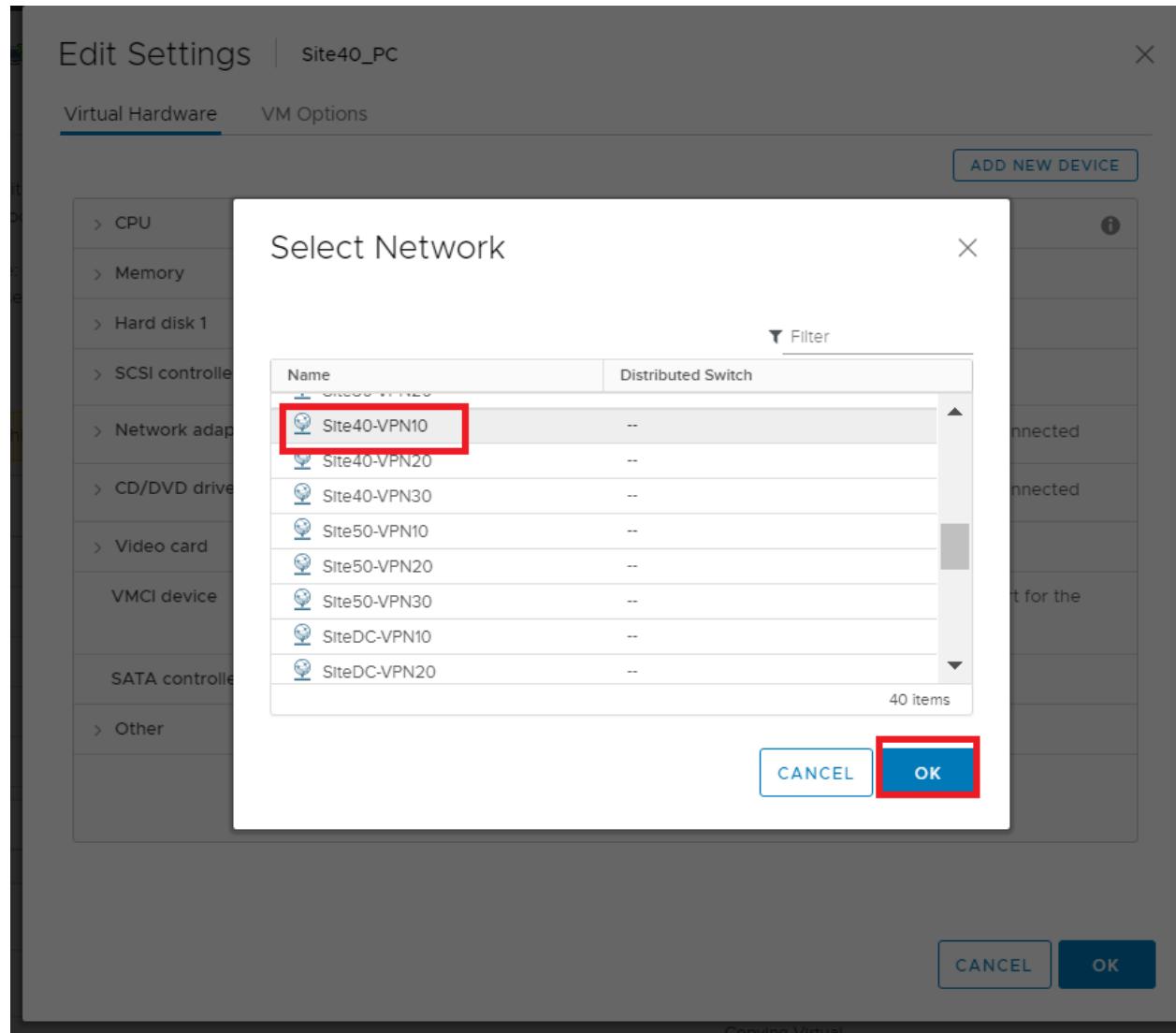
6. Back at the vCenter screen, right click on the Site40PC (named sdwan-slc/ghi-site40pc-podX) for your POD and click on **Edit Settings** (image as an example only)

The screenshot shows the vSphere Web Client interface. On the left, a tree view lists various objects, including several GHI-Pod entries and a Site40 entry, which is highlighted with a red box. The main pane displays the details for the selected VM, Site40_PC. The 'Actions' menu is open, showing options like Power, Monitor, Configure, Permissions, Datastores, Networks, and Updates. Under the 'Configure' section, there is a 'VM Tools' status message: 'VMware Tools is not installed on this virtual machine.' Below this, system specifications are listed: 1 CPU(s), 2 GB, 0.34 GB memory active, 1 hard drive (40 GB), and two network adapters (Network Adapter 1: Site40-VPN30 connected, Network Adapter 2: Disconnected).

7. Under **Network Adapter 1** click on the drop down and click **Browse**



8. Select **Site40-VPN10** from the list of Networks and click on **OK**. Click on **OK** again.



9. Log in to the cEdge40 CLI via Putty and issue `clear policy-map counters`. Confirm that you want to clear the counters. Now issue a `show policy-map interface Gig2` and a `show policy-map interface Gig3`. You will notice the number of packets incrementing in Queue0 (this includes VoIP packets via configuration and Control packets by default). Run the two commands given above multiple times and take notice of Queue3 and Queue0. Queue3 should not increment, whereas Queue0 will keep incrementing

```
cEdge40#show policy-map interface Gig2
GigabitEthernet2

Service-policy output: WAN-QoS

queue stats for all priority classes:
  Queueing
  priority level 1
  queue limit 512 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 143/24133

Class-map: Queue0 (match-any)
143 packets, 24133 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 0
  police:
    rate 20 %
    rate 200000000 bps, burst 6250000 bytes
    conformed 143 packets, 24133 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0000 bps, exceeded 0000 bps
  Priority: Strict, b/w exceed drops: 0

  Priority Level: 1

Class-map: Queue3 (match-any)
0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 3
  Queueing
  queue limit 1041 packets
```

```
show policy-map interface Gig2
show policy-map interface Gig3
```

10. Go back to the Site 40 PC and open Terminal. Type `ping 10.100.10.2`. Let the pings run for a few seconds, making note of how many packets did we receive a response for (look at the icmp_seq field) and then stop the pings by pressing Ctrl + C. We let the ping run for 70 packets

```
sdwan@10-40-30-21:~$ ping 10.100.10.2
PING 10.100.10.2 (10.100.10.2) 56(84) bytes of data.
64 bytes from 10.100.10.2: icmp_seq=1 ttl=63 time=0.582 ms
64 bytes from 10.100.10.2: icmp_seq=2 ttl=63 time=0.635 ms
64 bytes from 10.100.10.2: icmp_seq=3 ttl=63 time=0.472 ms
64 bytes from 10.100.10.2: icmp_seq=4 ttl=63 time=0.549 ms
64 bytes from 10.100.10.2: icmp_seq=5 ttl=63 time=0.534 ms
64 bytes from 10.100.10.2: icmp_seq=6 ttl=63 time=0.406 ms
64 bytes from 10.100.10.2: icmp_seq=7 ttl=63 time=0.350 ms
64 bytes from 10.100.10.2: icmp_seq=8 ttl=63 time=0.549 ms
64 bytes from 10.100.10.2: icmp_seq=9 ttl=63 time=0.512 ms
64 bytes from 10.100.10.2: icmp_seq=10 ttl=63 time=0.452 ms
64 bytes from 10.100.10.2: icmp_seq=11 ttl=63 time=0.441 ms
64 bytes from 10.100.10.2: icmp_seq=12 ttl=63 time=0.466 ms
64 bytes from 10.100.10.2: icmp_seq=13 ttl=63 time=0.449 ms
64 bytes from 10.100.10.2: icmp_seq=14 ttl=63 time=0.542 ms
64 bytes from 10.100.10.2: icmp_seq=15 ttl=63 time=0.412 ms
64 bytes from 10.100.10.2: icmp_seq=16 ttl=63 time=0.411 ms
64 bytes from 10.100.10.2: icmp_seq=17 ttl=63 time=0.662 ms
64 bytes from 10.100.10.2: icmp_seq=18 ttl=63 time=0.443 ms
64 bytes from 10.100.10.2: icmp_seq=19 ttl=63 time=0.596 ms
64 bytes from 10.100.10.2: icmp_seq=20 ttl=63 time=0.536 ms
```

11. Issue `show policy-map interface Gig2` and `show policy-map interface Gig3` again on the cEdge40 CLI.
Queue3 in one of the outputs (depends on the path taken by the packets) should reflect an increment in the number of packets

```
Service-policy output: WAN-QoS
```

```
queue stats for all priority classes:  
  Queueing  
  priority level 1  
  queue limit 512 packets  
  (queue depth/total drops/no-buffer drops) 0/0/0  
  (pkts output/bytes output) 1712/308203
```

```
Class-map: Queue0 (match-any)  
  1712 packets, 308203 bytes  
  5 minute offered rate 14000 bps, drop rate 0000 bps  
  Match: qos-group 0  
  police:  
    rate 20 %  
    rate 200000000 bps, burst 6250000 bytes  
    conformed 1712 packets, 308203 bytes; actions:  
      transmit  
    exceeded 0 packets, 0 bytes; actions:  
      drop  
    conformed 14000 bps, exceeded 0000 bps  
  Priority: Strict, b/w exceed drops: 0
```

```
Priority Level: 1
```

```
Class-map: Queue3 (match-any)  
  70 packets, 10920 bytes  
  5 minute offered rate 0000 bps, drop rate 0000 bps  
  Match: qos-group 3  
  Queueing  
  queue limit 1041 packets  
  (queue depth/total drops/no-buffer drops) 0/0/0  
  (pkts output/bytes output) 70/10920  
  bandwidth remaining ratio 10  
  Exp-weight-constant: 9 (1/512)  
  Mean queue depth: 0 packets  
    class      Transmitted          Random drop          Tail drop  
              pkts/bytes            pkts/bytes            pkts/bytes  
    0           70/10920             0/0                 0/0  
    1           0/0                 0/0                 0/0
```

Thus, traffic is being matched as per our QoS strategy. However, we won't be able to test other queues since ESXi (the VMWare environment in which our lab is running) doesn't allow packet tags to be propagated over Standard vSwitches (the virtual switch). Queue0 shows up since this traffic is generated natively by the Router in question.

An extended ping directly from the Router yields unpredictable results, with traffic usually getting matched to class class-default (optional - you can try this out).

```
cEdge40#clear policy-map count
Clear policy-map counters on all interfaces [confirm]
cEdge40#
cEdge40#
cEdge40#
cEdge40#ping vrf 10
Protocol [ip]:
Target IP address: 10.100.10.2
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 10.40.10.2
DSCP Value [0]: 34
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.100.10.2, timeout is 2 seconds:
Packet sent with a source address of 10.40.10.2
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 1/1/1 ms
cEdge40#
```

| Mean queue depth: 0 packets | Transmitted pkts/bytes | Random drop pkts/bytes | Tail drop pkts/bytes | Minimum thresh | Maximum thresh | Mark prob |
|-----------------------------|---------------------------|---------------------------|-------------------------|-------------------|-------------------|--------------|
| 0 | 0/0 | 0/0 | 0/0 | 260 | 520 | 1/10 |
| 1 | 0/0 | 0/0 | 0/0 | 292 | 520 | 1/10 |
| 2 | 0/0 | 0/0 | 0/0 | 325 | 520 | 1/10 |
| 3 | 0/0 | 0/0 | 0/0 | 357 | 520 | 1/10 |
| 4 | 0/0 | 0/0 | 0/0 | 390 | 520 | 1/10 |
| 5 | 0/0 | 0/0 | 0/0 | 422 | 520 | 1/10 |
| 6 | 0/0 | 0/0 | 0/0 | 455 | 520 | 1/10 |
| 7 | 0/0 | 0/0 | 0/0 | 487 | 520 | 1/10 |

```
Class-map: class-default (match-any)
 100 packets, 17200 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: any

 queue limit 1041 packets
 (queue depth/total drops/no-buffer drops) 0/0/0
 (pkts output/bytes output) 100/17200
cEdge40#show policy-map interf gi3
GigabitEthernet3
```

This completes our QoS activity verification.

Task List

- [Create a Localized Policy](#)
 - [Add a Class List and a QoS Map](#)
 - [Configure the IPv4 ACL Policy](#)
 - [Complete and apply the localized policy](#)
- [Apply the ACL and QoS Map](#)
- [Activity Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: June 2, 2020

Site last generated: Sep 1, 2020



Installing and Configuring the IPS module on cEdges

[Take a tour of this page](#)

Summary: Installing an IPS Engine on cEdges and testing signature detection for DIA Guest users

Table of Contents

- [Overview](#)
- [Initial Configuration
 - Revert Site 40 PC changes and enable DIA
 - Upload Image to vManage](#)
- [Add the Security Policy
 - Firewall Policy Update
 - Add the IPS Policy and Finalize the Security Policy](#)
- [Updating the Application List and Device Template](#)
- [Verifying installation and performing signature updates](#)
- [Activity Verification](#)

Task List

- Overview
- Initial Configuration
- Revert Site 40 PC changes and enable DIA
- Upload Image to vManage
- Add the Security Policy

- Firewall Policy Update
- Add the IPS Policy and Finalize the Security Policy
- Updating the Application List and Device Template
- Verifying installation and performing signature updates
- Activity Verification

Overview

An Intrusion Prevention System (IPS) allows the network to detect anomalies based on known signatures and block/report them. The IPS module in Cisco SD-WAN can be deployed on Cisco IOS-XE SD-WAN Devices, working in Detect or Prevention mode. This solution is an on-prem on-box feature providing PCI compliance.

Snort is leveraged on Cisco SD-WAN IOS-XEW Devices for IPS and IDS capabilities.

Task List

- [Overview](#)
- [Initial Configuration](#)
- Revert Site 40 PC changes and enable DIA
- [Upload Image to vManage](#)
- [Add the Security Policy](#)
- [Firewall Policy Update](#)
- [Add the IPS Policy and Finalize the Security Policy](#)
- [Updating the Application List and Device Template](#)
- [Verifying installation and performing signature updates](#)
- [Activity Verification](#)

Initial Configuration

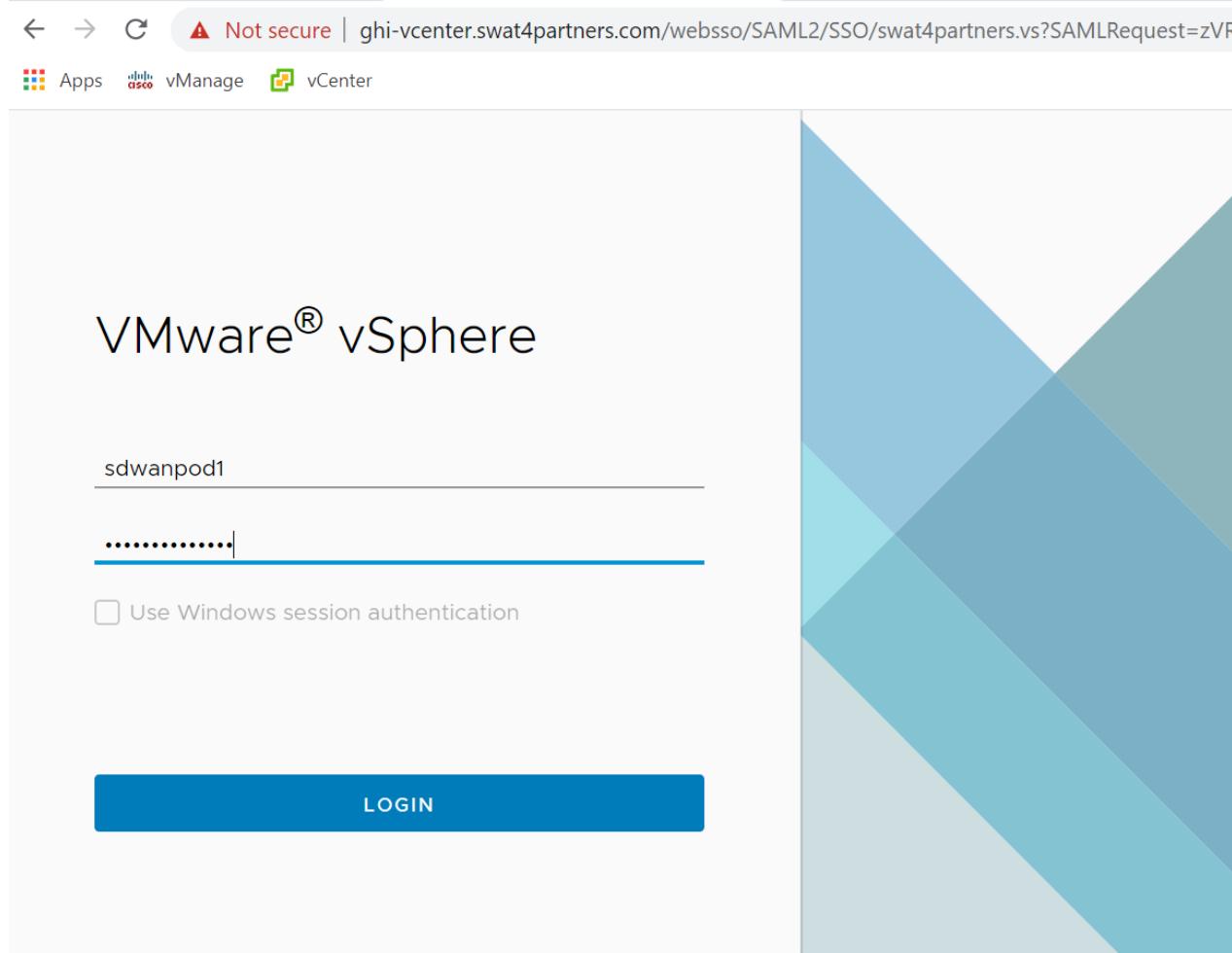
We will be performing some initial configuration in the network before it can support the IPS module. Key points to be noted:

- The cEdge should have a minimum of 4 vCPUs and 8 GB RAM (already done)
- Site 40 PC settings will be reverted

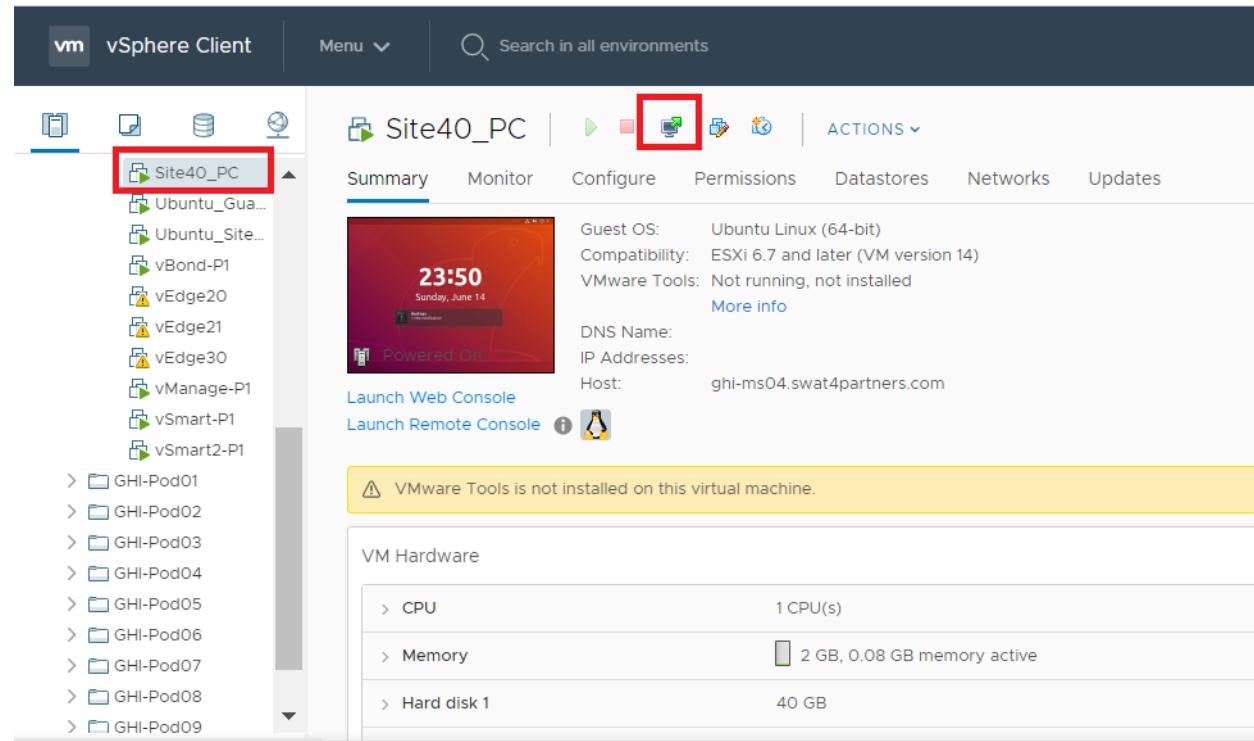
- Images uploaded to vManage for deployment

Revert Site 40 PC changes and enable DIA

1. Log in to vCenter via the bookmark in Chrome, or via the URL (10.2.1.50/ui). Use the credentials provided for your POD. Click on **Login**



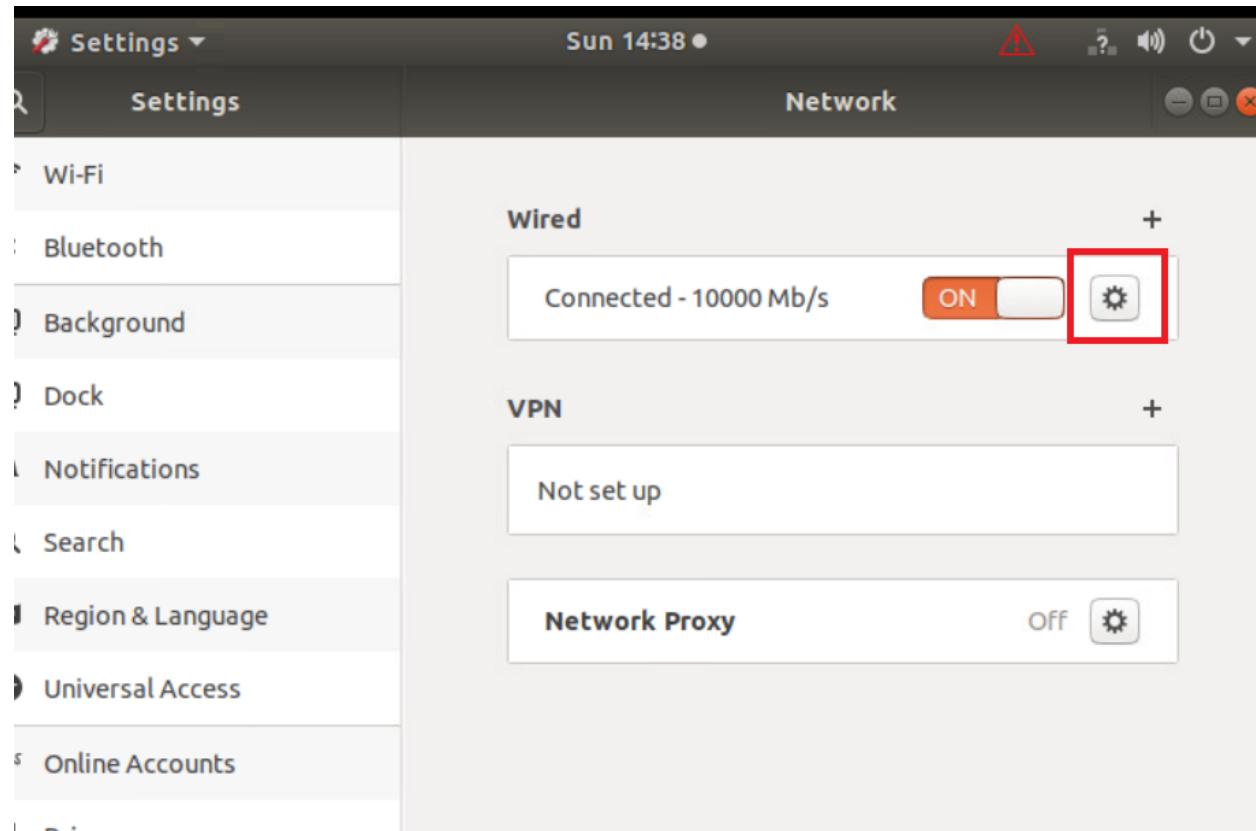
2. Locate your Site 40 PC (image below shows Site40_PC, VM name for your POD should be sdwan-slc/ghi-site40pc-podX) and choose to open the console. Select Web Console, if prompted



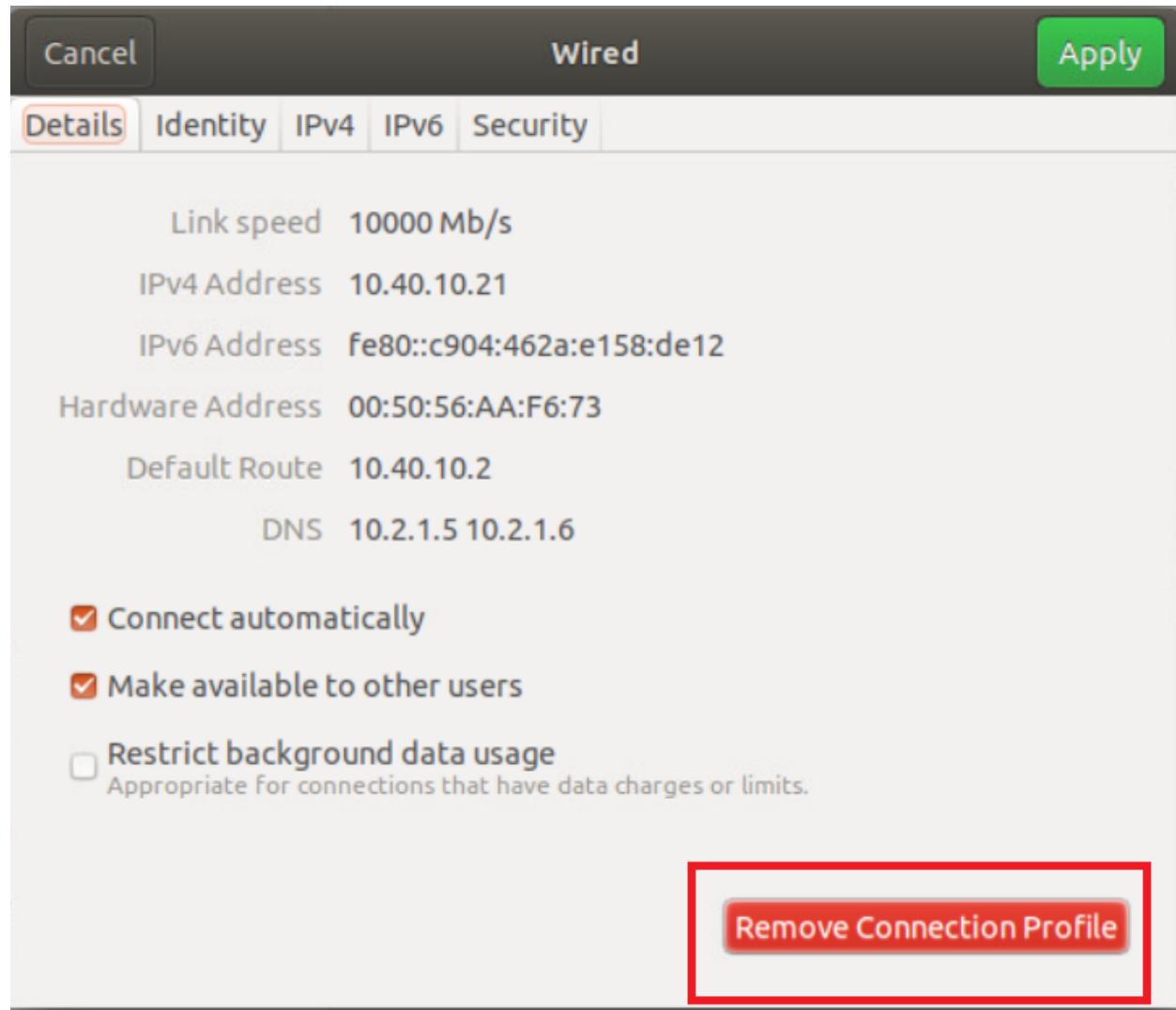
3. Log in to the PC and click on the network icon in the top-right corner. Expand **Wired Connected** and click on **Wired Settings**



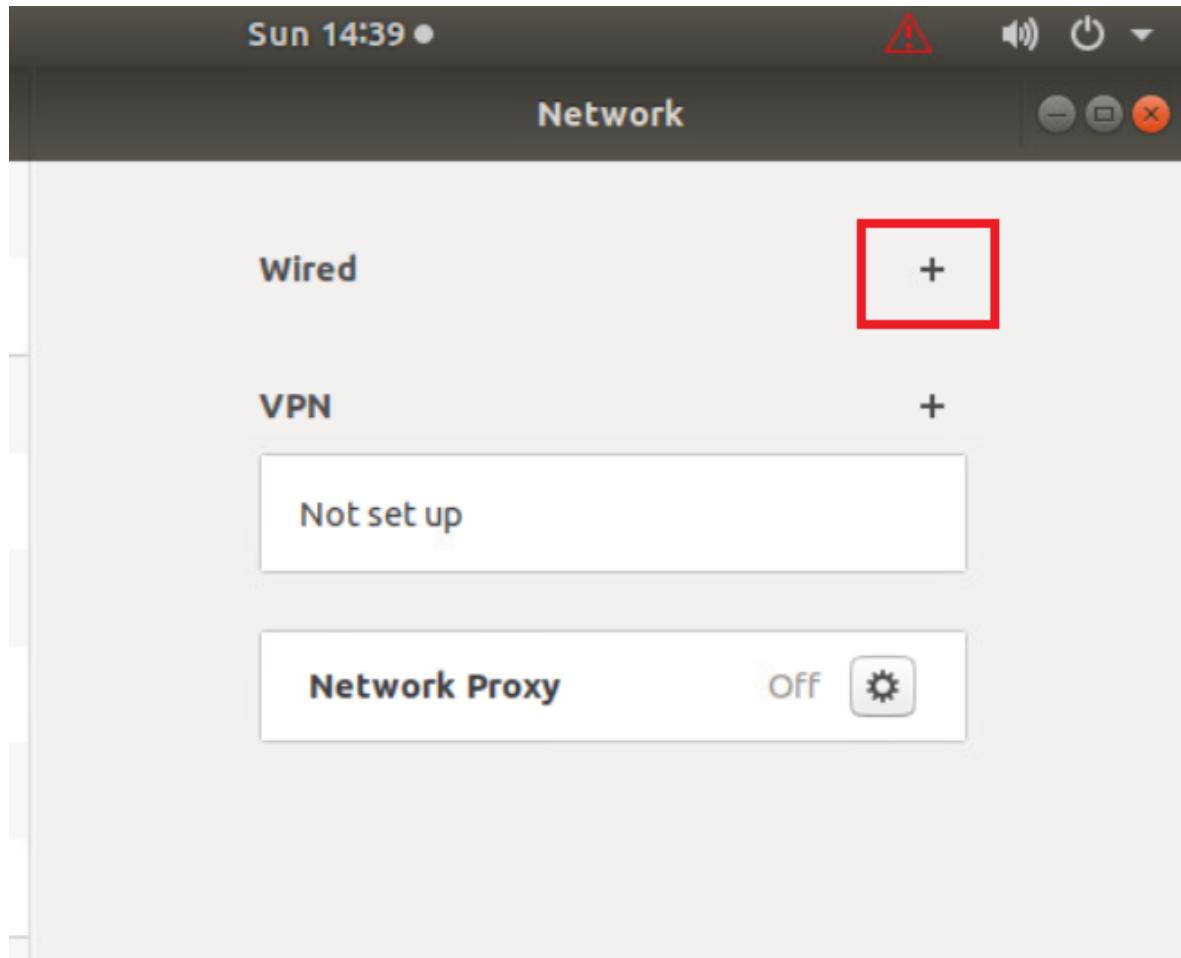
4. Click on the cog wheel/gear icon



5. Click on **Remove Connection Profile**



6. If you still see a cog wheel/gear icon next to **Wired**, click on it and choose to **Remove Connection Profile** again. Once the + icon can be seen next to **Wired**, click on it



7. Go to the **IPv4** tab and click on **Manual** for the IPv4 Method. Enter details as given below and click on **Add**. Over here, y is 1 if you're connected to the SLC DC and 2 if you're connected to the GHI DC. The email sent with lab access details should enumerate which DC you're POD is on

| Address | Netmask | Gateway | DNS |
|--------------------|---------------|------------|-----------------|
| 10.40.30.21 | 255.255.255.0 | 10.40.30.2 | Automatic - Off |
| 10.y.1.5, 10.y.1.6 | | | |

New Profile

Cancel Add

Identity IPv4 IPv6 Security

IPv4 Method Automatic (DHCP) Manual Link-Local Only Disable

Addresses

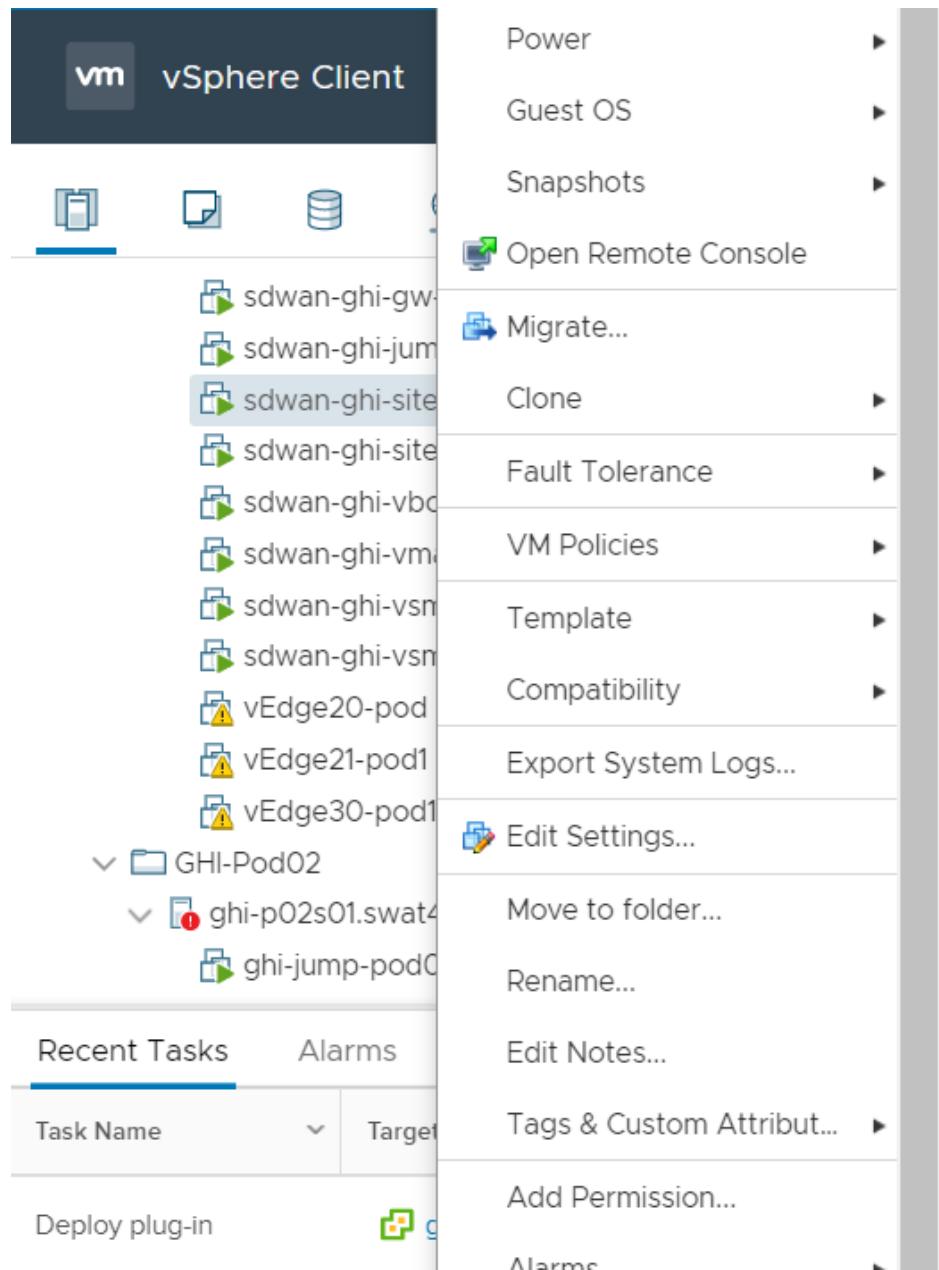
| Address | Netmask | Gateway |
|-------------|---------------|------------|
| 10.40.30.21 | 255.255.255.0 | 10.40.30.2 |
| | | |
| | | |

DNS Automatic OFF
10.2.1.5, 10.2.1.6
Separate IP addresses with commas

Routes Automatic ON

| Address | Netmask | Gateway | Metric |
|---------|---------|---------|--------|
| | | | |

8. Back at the vCenter GUI, right click on your Site 40 PC and choose **Edit Settings**



9. Click on the drop down next to **Network Adapter 1** and click on **Browse**

Edit Settings | sdwan-ghi-site40pc-pod1

X

Virtual Hardware VM Options

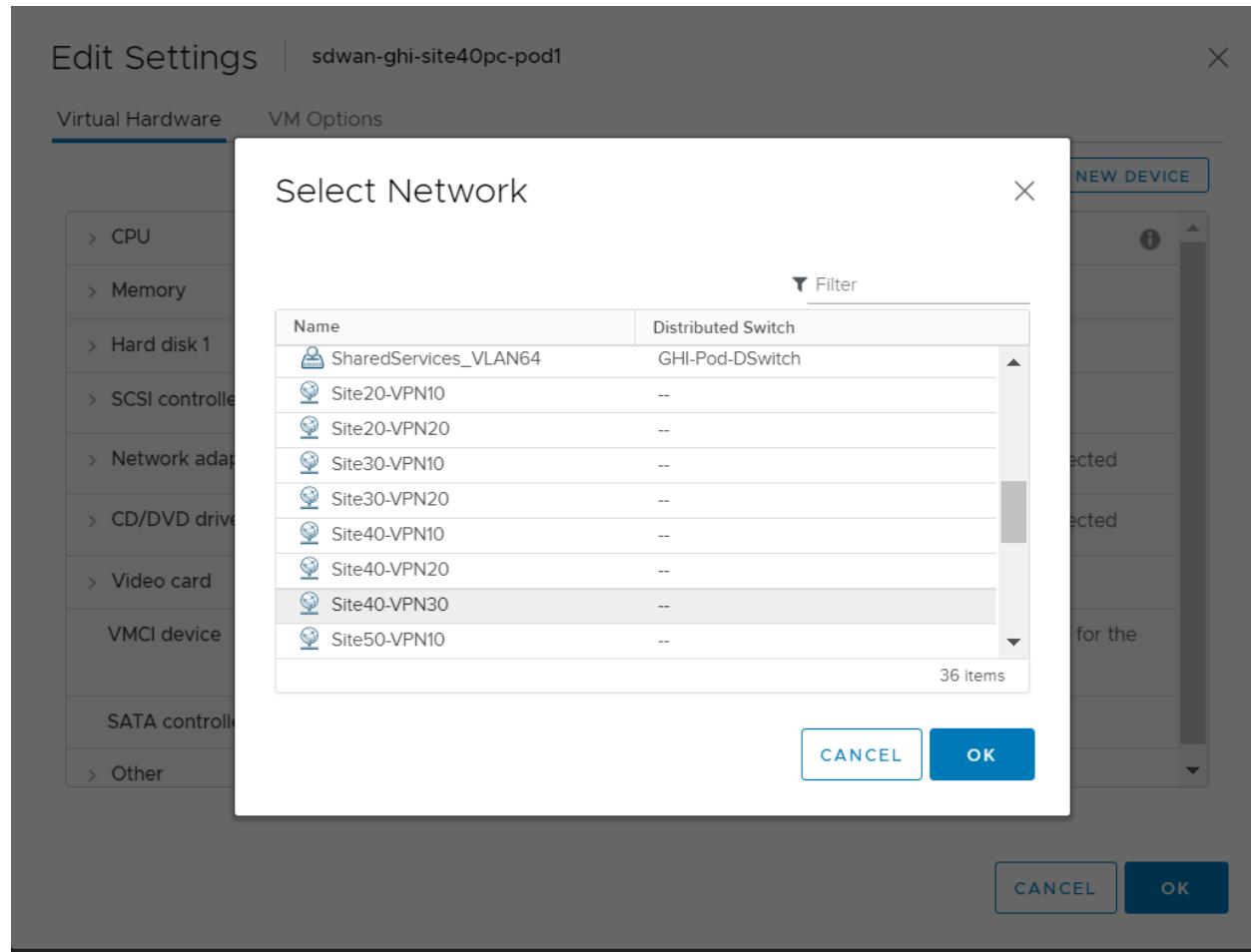
ADD NEW DEVICE

| | | |
|---------------------|---|---|
| > CPU | 1 | ▼ |
| > Memory | 2 | GB ▼ |
| > Hard disk 1 | 40 | GB ▼ |
| > SCSI controller 0 | LSI Logic Parallel | |
| > Network adapter 1 | Site40-VPN10 ▼ | <input checked="" type="checkbox"/> Connected |
| > CD/DVD drive 1 | Site40-VPN10 Browse ... ▼ | <input type="checkbox"/> Connected |
| > Video card | Specify custom settings ▼ | |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface | |
| SATA controller 0 | AHCI | |
| > Other | Additional Hardware | ▼ |

CANCEL

OK

10. Choose the *Site40-VPN30* network and click on **OK**. This should take you to the Edit Settings page, click on **OK** again



11. On the vManage GUI, go to **Configuration => Policies** and locate the *Site40-Guest-D/A*. Click on the three dots next to it and choose to **Activate**. Confirm the Activation

CONFIGURATION | POLICIES

Centralized Policy Localized Policy

Add Policy

Search Options

Total Rows: 5

| Name | Description | Type | Activated | Updated By | Policy Version | Last Updated | ... |
|----------------------------|---------------------------------------|-------------------|-----------|------------|--------------------|----------------------------|-----|
| AAR-VPN10 | Transport Preference for VPN 10 | UI Policy Builder | true | admin | 06042020T144602205 | 04 Jun 2020 7:46:02 AM PDT | ... |
| Site20-Regional-Hub-Site30 | Regional Policy for Site 20 to Sit... | UI Policy Builder | false | admin | 05282020T130912927 | 28 May 2020 6:09:12 AM PDT | ... |
| traffic-engineering-ftp | Traffic Engineering for FTP | UI Policy Builder | false | admin | 06032020T131902822 | 03 Jun 2020 6:19:02 AM PDT | ... |
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VPN 2... | UI Policy Builder | false | admin | 05282020T100134900 | 28 May 2020 3:01:34 AM PDT | ... |
| Site40-Guest-DIA | DIA Policy for Site 40 Guests | UI Policy Builder | false | admin | 06032020T142511667 | 03 Jun 2020 7:25:11 AM PDT | ... |



12. Go back to the console for the Site 40 PC and open Terminal. (**Start => search for terminal => click on the icon**).

Type `ping 8.8.8.8` and hit Enter to verify Internet connectivity

```
sdwan@10-40-30-21:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=4.96 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=4.82 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=4.68 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=4.80 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=4.57 ms
```

We have set the Site 40 PC back to what it was, before our QoS section.

Task List

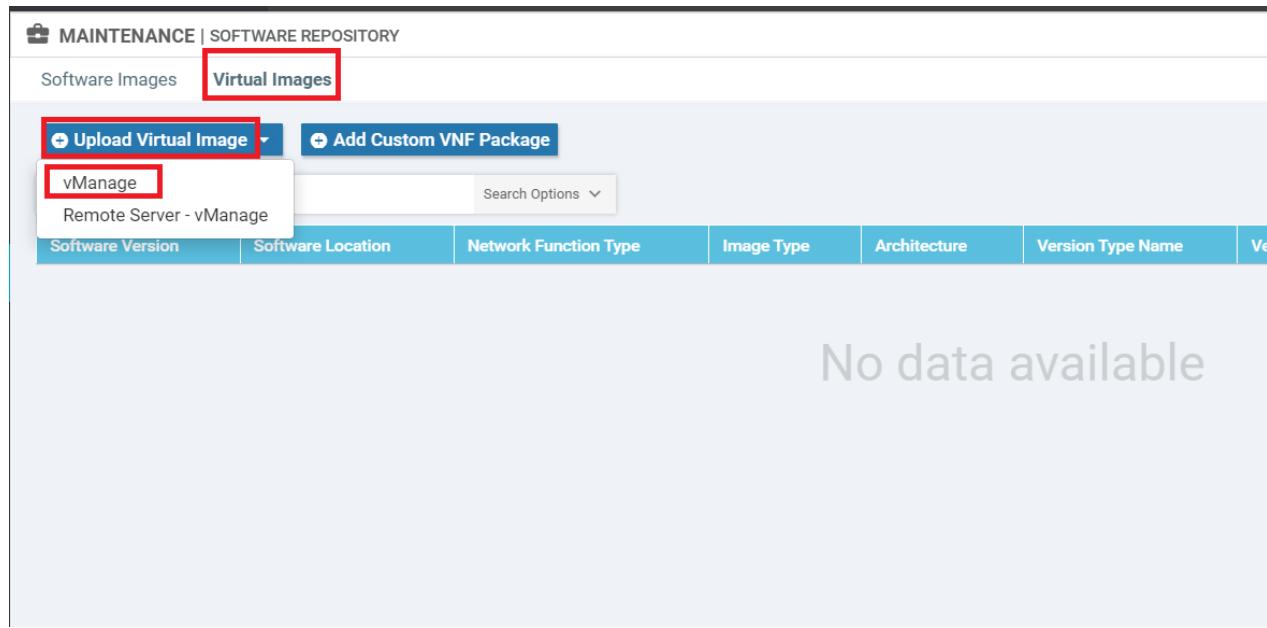
- [Overview](#)
- [Initial Configuration](#)
- [~~Revert Site 40 PC changes and enable DIA~~](#)
- [Upload Image to vManage](#)
- [Add the Security Policy](#)
- [Firewall Policy Update](#)
- [Add the IPS Policy and Finalize the Security Policy](#)
- [Updating the Application List and Device Template](#)
- [Verifying installation and performing signature updates](#)
- [Activity Verification](#)

Upload Image to vManage

1. On the vManage GUI, go to **Maintenance => Software Repository**

The screenshot shows the Cisco vManage interface. The top navigation bar includes the Cisco logo and the title "Cisco vManage". On the left, a vertical sidebar lists several icons: a grid (Devices), a monitor (Network), a gear (Configuration), a wrench (Maintenance), a briefcase (Software Repository), a person (User), and a server (Software Upgrade). The "Maintenance" icon is currently selected. The main content area is titled "TASK VIEW" and displays a summary: "Push vSmart Policy | Validation Success" with a green checkmark icon. Below this, it says "Total Task: 2 | Success : 2". A search bar labeled "Search Options" is present. A "Message" section contains two entries: "Done - Push vSmart Policy" and "Done - Push vSmart Policy".

2. Click on the **Virtual Images** tab and then click **Upload Virtual Image**. Choose **vManage**



3. Click on **Browse** and make sure you're in the *SD-WAN Deployment Files* folder. This folder can be found on the Desktop of your Jumphost. Select the file starting with *secapp-utd...* and click on **Open**



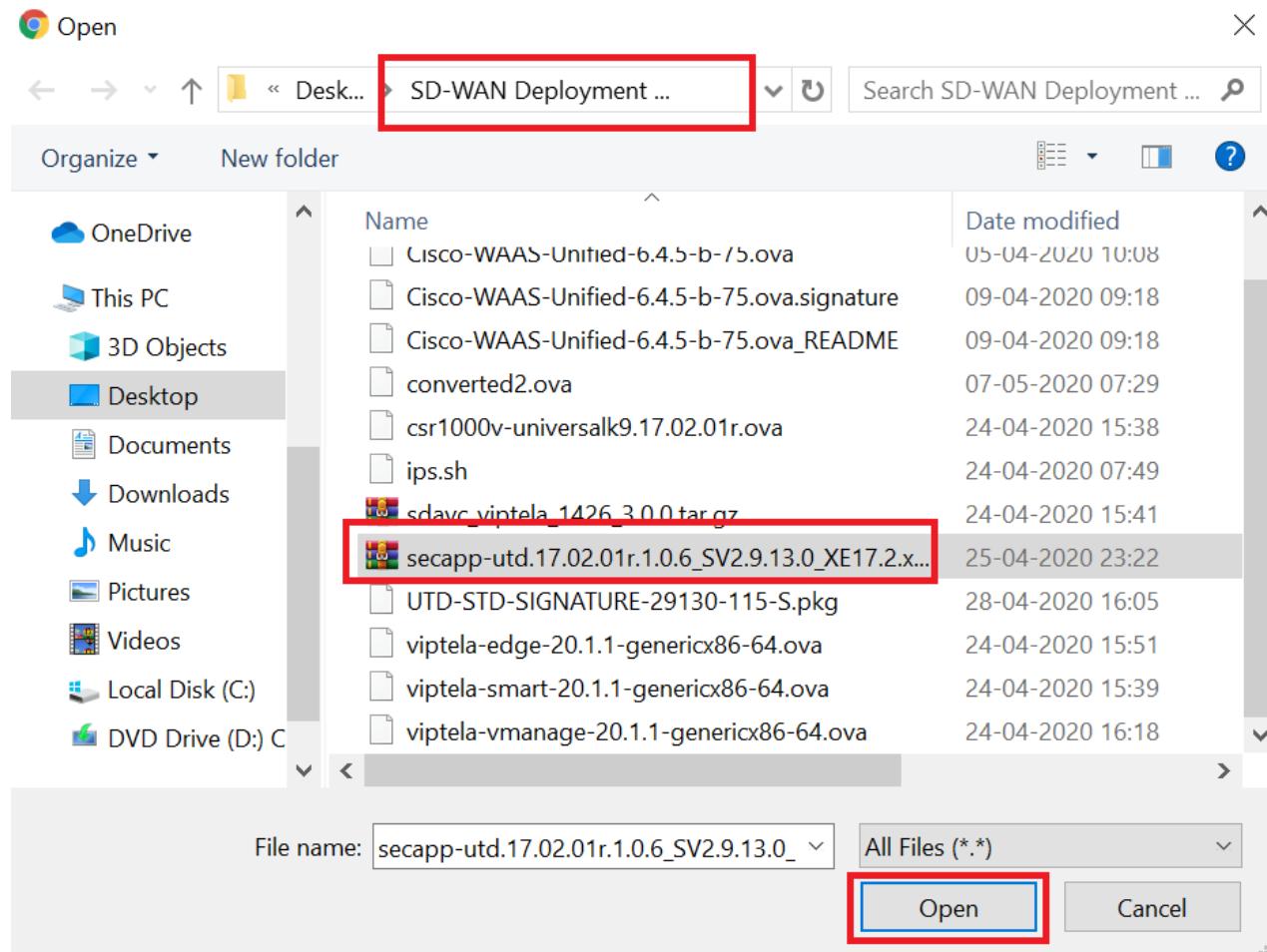
Drag and Drop File

Or

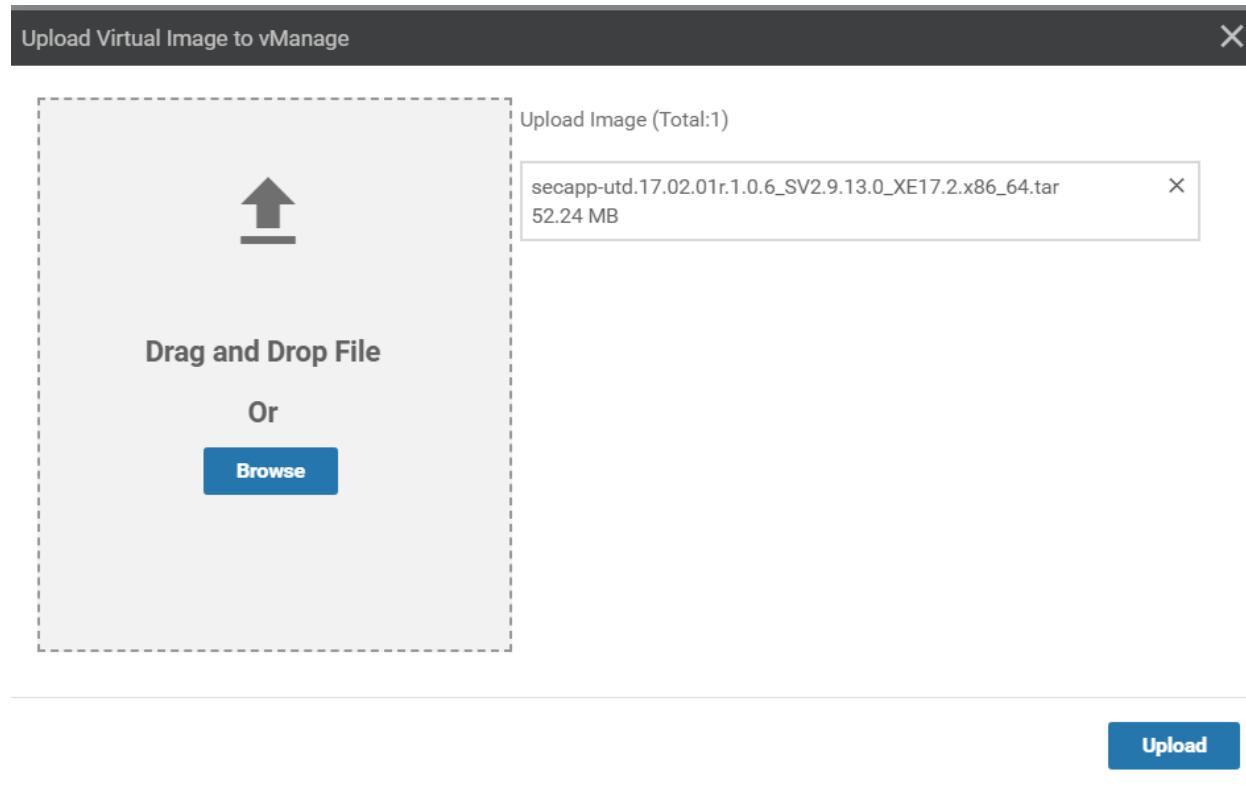
Browse

No Images Uploaded

Upload



4. Click on **Upload**



5. Once the file is uploaded, it should show up under Virtual Images

MAINTENANCE | SOFTWARE REPOSITORY

Virtual image uploaded successfully

| Software Version | Software Location | Network Function Type | Image Type | Architecture | Version Type Name | Vendor | Available Files | Updated On |
|-------------------------|-------------------|-----------------------|------------|--------------|----------------------|---------------------|---|--------------------|
| 1.0.6_SV2.9.13.0_XE17.2 | vmanage | App-Hosting | Lxc | x86_64 | Security Application | Cisco Systems, I... | app-hosting_UTD-Snort-Feature-x86_64_1.0.6_S... | 06 Jun 2020 3:1... |

Task List

- [Overview](#)
- [Initial Configuration](#)
- [Revert Site 40 PC changes and enable DIA](#)
- [Upload Image to vManage](#)

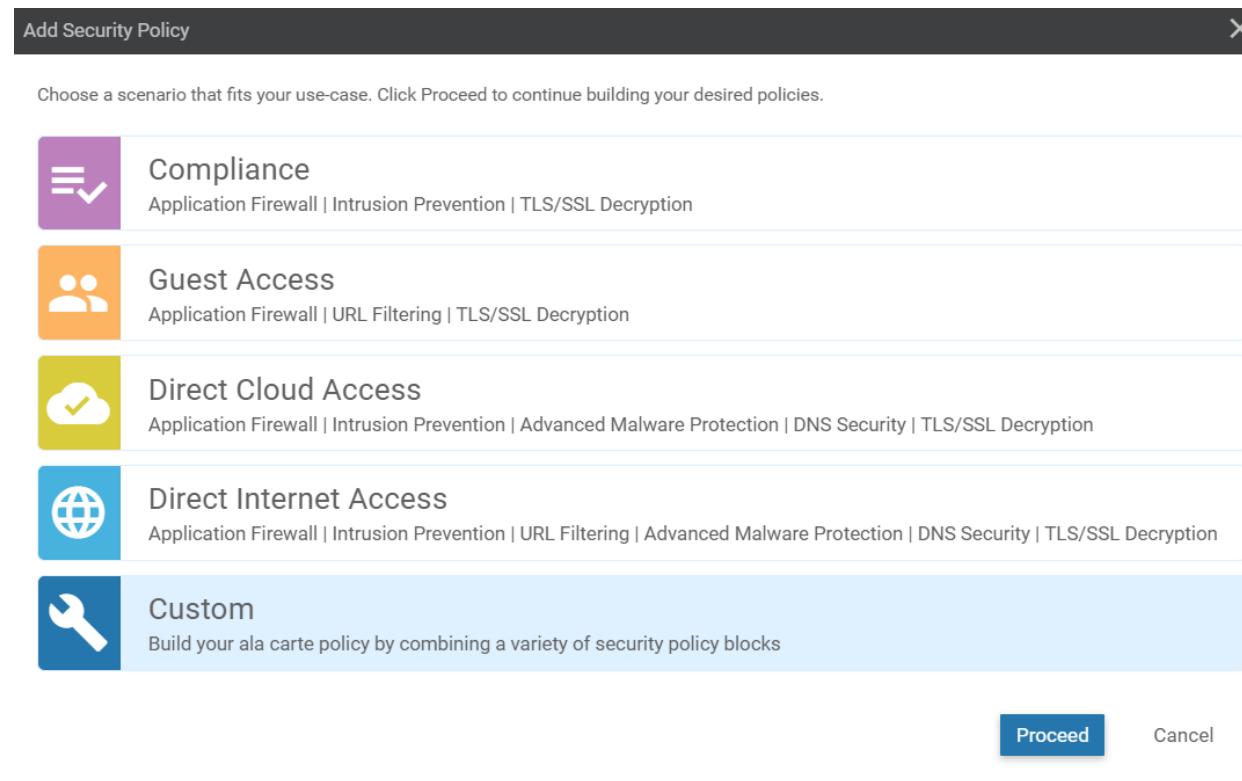
- Add the Security Policy
- Firewall Policy Update
- Add the IPS Policy and Finalize the Security Policy
- Updating the Application List and Device Template
- Verifying installation and performing signature updates
- Activity Verification

Add the Security Policy

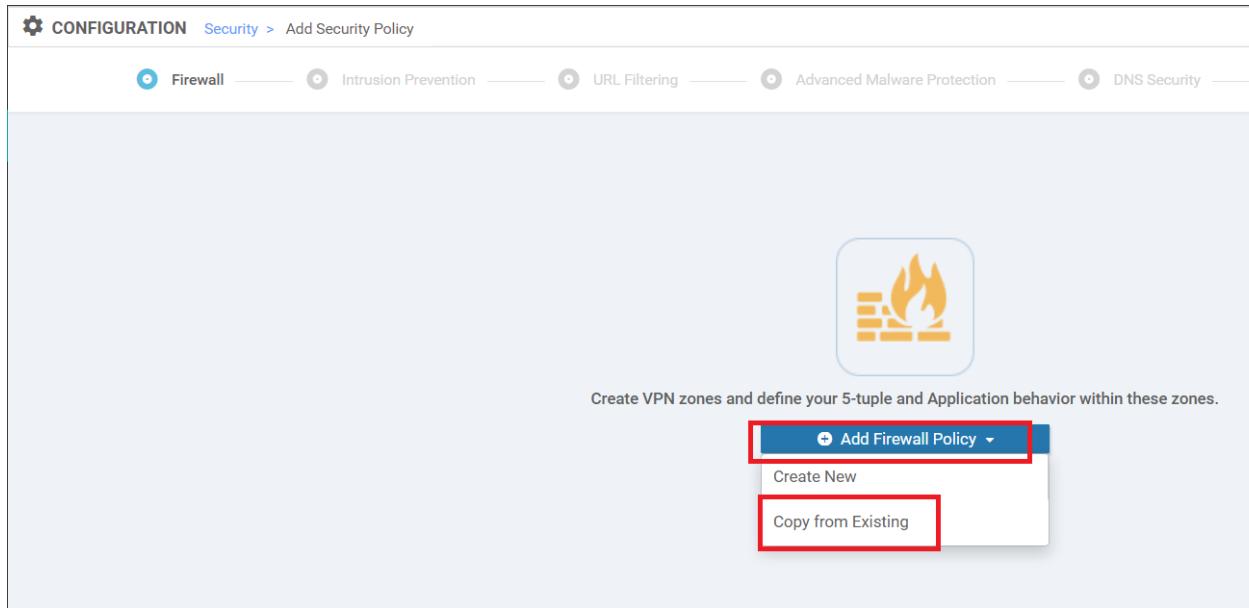
A Security Policy will be applied to the Device Template for cEdge40 to trigger IPS installation and functionality. We will be setting up the policy over here, including the previously created Firewall Policy in our overarching Security Policy.

Firewall Policy Update

1. On the vManage GUI, navigate to **Configuration => Security** and choose **Add Security Policy**. Select **Custom** and click on **Proceed**



2. Under **Firewall**, click on **Add Firewall Policy** and choose **Copy from Existing**. We already have a Firewall Policy in place but the Security Policy type chosen for it was Guest Access, which doesn't have an option of including an IPS policy. Hence, we will create a new custom policy which will include the Firewall Policy created before



3. Select *Guest-FW* as the Policy and specify the Policy Name as *Guest-FW_concat*. Give a Description of *Guest Traffic Firewall with IPS*. Click on **Copy**

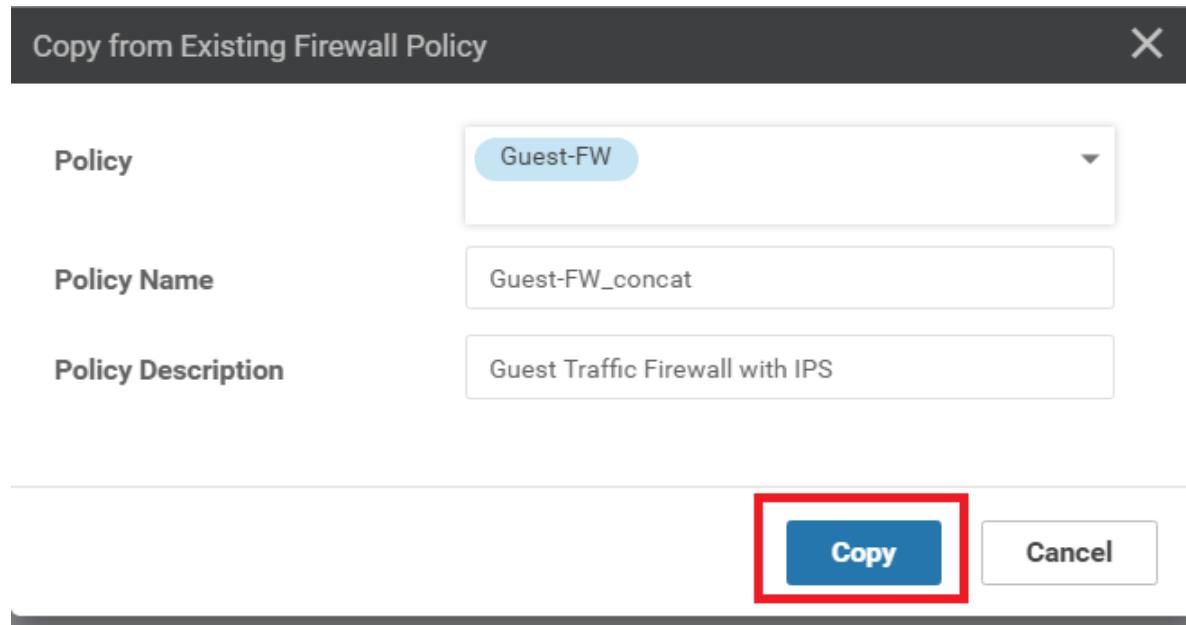
Copy from Existing Firewall Policy X

Policy Guest-FW

Policy Name Guest-FW_concat

Policy Description Guest Traffic Firewall with IPS

Copy Cancel



4. The Firewall Policy we just copied should show up. Click on **Next**

Add Firewall Policy (Add a Firewall configuration)

| Name | Type | Description | Reference Count |
|-----------------|-------------|---------------------------------|-----------------|
| Guest-FW_concat | zoneBasedFW | Guest Traffic Firewall with IPS | 0 |

Next CANCEL

Configuration of the Security Policy continues in the next section.

Task List

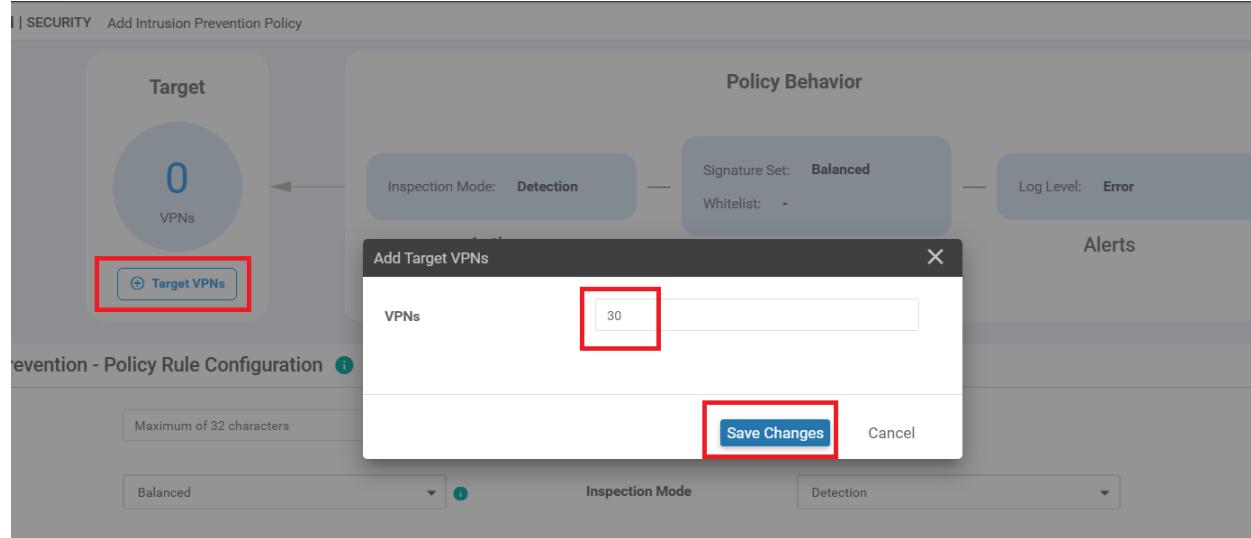
- [Overview](#)
- [Initial Configuration](#)
- [Revert Site 40 PC changes and enable DIA](#)
- [Upload Image to vManage](#)
- [Add the Security Policy](#)
- [Firewall Policy Update](#)
- [Add the IPS Policy and Finalize the Security Policy](#)
- [Updating the Application List and Device Template](#)
- [Verifying installation and performing signature updates](#)
- [Activity Verification](#)

Add the IPS Policy and Finalize the Security Policy

1. Under the **Intrusion Prevention** page, click on **Add Intrusion Prevention** and choose **Create New**

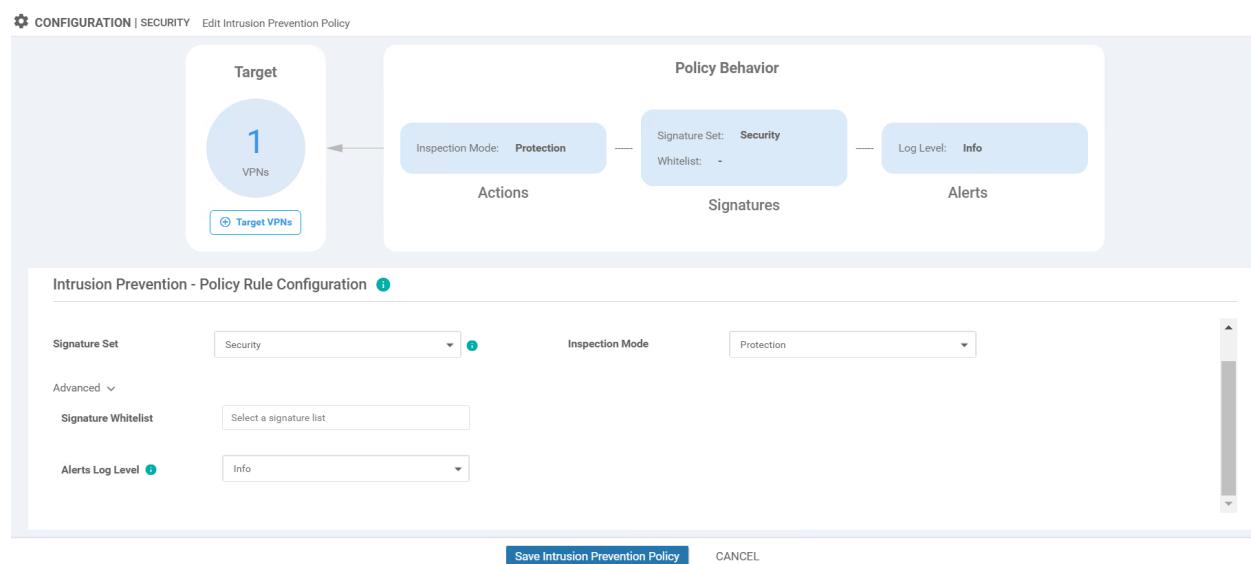
The screenshot shows the 'Add Security Policy' interface. At the top, there are tabs for Firewall, Intrusion Prevention, URL Filtering, Advanced Malware Protection, DNS Security, and TLS/SSL Decryption. The 'Intrusion Prevention' tab is selected and highlighted with a red box. Below the tabs is a large shield icon. A text box contains the instruction: 'Prevent and act against malicious and hostile attacks by configuring Signature set and Inspection mode.' A note below it says: 'Please upload compatible Security App Hosting Image File to the software repository in order to support IPS functions. You can upload the image file from Maintenance > Software Repository > Virtual Images.' A dropdown menu titled 'Add Intrusion Prevention Policy' is open, with 'Create New' highlighted by a red box.

2. Click on **Target VPNs** and enter a VPN of 30. Click on **Save Changes**



3. Under the Intrusion Prevention - Policy Rule Configuration, enter the following details and click on **Save Intrusion Prevention Policy**

| Policy Name | Signature Set | Inspection Mode | Alerts Log Level |
|-------------|---------------|-----------------|------------------|
| Guest-IPS | Security | Protection | Info |



4. Back at the main Security Policy page, click on **Next** 5 times

| Name | Type | Reference Count | Updated By | Last Updated On |
|-----------|---------------------|-----------------|------------|-----------------|
| Guest-IPS | IntrusionPrevention | 0 | admin | 06 |

Click Next 5 Times Next CANCEL

5. Enter the details as shown in the table below and click on **Save Policy**

| Security Policy Name | Security Policy Description | TCP SYN Flood Limit | Audit Trail |
|----------------------|-----------------------------|---------------------|-------------|
| Guest-FW-IPS-DIA | Guest Firewall and IPS DIA | Enabled 5000 | On |

Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

| | |
|-----------------------------|----------------------------|
| Security Policy Name | Guest-FW-IPS-DIA |
| Security Policy Description | Guest Firewall and IPS DIA |

Additional Policy Settings

Firewall

| | | | |
|------------------------------|--|--|--|
| Direct Internet Applications | <input type="checkbox"/> Bypass firewall policy and allow all Internet traffic to/from VPN 0 | | |
| TCP SYN Flood Limit | Enabled <input checked="" type="checkbox"/> 5000 | | |
| High Speed Logging | VPN <input type="text" value="Enter a VPN"/> | Server IP <input type="text" value="Example: 10.0.0.1"/> | Port <input type="text" value="2055"/> |
| Audit Trail | <input checked="" type="checkbox"/> On (Applicable only for the rules with Inspect action) | | |

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

| | | |
|------------------------|--|--|
| External Syslog Server | VPN <input type="text" value="Enter a VPN"/> | Server IP <input type="text" value="Example: 10.0.0.1"/> |
| Failure Mode | Open <input type="button" value="▼"/> | |

BACK Preview Save Policy CANCEL

This completes the configuration of our Security Policy.

Task List

- Overview
- Initial Configuration
- Revert Site 40 PC changes and enable DIA
- Upload Image to vManage
- Add the Security Policy
- Firewall Policy Update
- Add the IPS Policy and Finalize the Security Policy
- Updating the Application List and Device Template
- Verifying installation and performing signature updates
- Activity Verification

Updating the Application List and Device Template

The Application List attached to the Firewall Policy that we had earlier will need to be instantiated again before we can use it. For that, we will make a dummy modification to the Application List

1. On the vManage GUI, go to **Configuration => Security**. Click on **Custom Lists** (top right-hand corner) and choose **Lists**

The screenshot shows the Cisco vManage interface. The top navigation bar has 'Cisco vManage' and 'admin'. A red box highlights the 'Custom Options' dropdown in the top right. A secondary red box highlights the 'Lists' option under the 'Security' section of the dropdown menu. The main content area shows a table of security policies:

| Name | Description | Use Case | Devices Attached | Device Templates | Updated By |
|------------------|---------------------------|--------------|------------------|------------------|------------|
| Guest-FW-IPS-DIA | Guest Firewall and IPS... | Custom | 0 | 0 | admin |
| Site40-Guest-DIA | Guest Policy for Site 40 | Guest Access | 1 | 1 | admin |

2. Identify the *Guest-Inspect* Application List and click on the **pencil** icon on the right-hand side to edit it. Under **Select Application**, check **X Font Server** (or any application that you want, this is a dummy entry)

The screenshot shows the FortiGate configuration interface under the 'Security' tab, specifically the 'Define Lists' section. On the left sidebar, 'Application' is selected. In the main area, a table lists application entries: 'Guest-Inspect' and 'ftp'. A modal window titled 'New Application List' is open over the table. Inside the modal, the 'Application List Name' field contains 'Guest-Inspect'. Below it, the 'Select Application' section shows two selected items: 'Webmail' and 'X Font Server'. A scrollable list of other applications is shown, with 'X Font Server' having a checked checkbox. Other listed applications include Application Service, Apple App Store, iOS over-the-air (OTA) update, Financial Information eXchange (FIX), iCloud (Apple), Lightweight Directory Access Protocol, Perforce Protocol, Lightweight Directory Access Protocol Secure, and Service Location Protocol.

3. Scroll down the list and **uncheck** Webmail, but check all the other Applications under Webmail

Select Application

X Font Server Gmail Outlook Web Service Yahoo Mail Mail.ru GMX webmail

Search

Hangouts Media
 Hangouts Video
 Slack
 Webmail
 Gmail
 GMX webmail
 Mail.ru
 Outlook Web Service
 Yahoo Mail

4. Click outside the box and choose to **Save** the Application List. Click on **Activate**, if prompted. Click on **Next** followed by **Configure Devices**

Application List

X

Application List Name
Guest-Inspect

Select Application

X Font Server Gmail Outlook Web Service Yahoo Mail Mail.ru GMX webmail

Save Cancel

5. Go to **Configuration => Templates** and click on the three dots next to `cedge_dualuplink_devtemp`. Click on **Edit**

CONFIGURATION | TEMPLATES

Device Feature

Create Template

Template Type Non-Default Search Options

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Actions |
|--------------------------|-------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|---------|
| DCvEdge_dev_temp | Device template for the D... | Feature | vEdge Cloud | 16 | 2 | admin | 28 May 2020 4:58:07 AM ... | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Devic... | Feature | CSR1000v | 17 | 2 | admin | 26 May 2020 3:05:01 AM ... | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the Si... | Feature | vEdge Cloud | 14 | 2 | admin | 25 May 2020 3:05:59 PM ... | In Sync | ... |
| cEdge_dualuplink_devtemp | cEdge Device Template fo... | Feature | CSR1000v | 19 | 1 | admin | 05 Jun 2020 11:31:59 PM ... | In Sync | ... |
| vSmart-dev-temp | Device Template for vSma... | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 A... | In Sync | ... |
| vEdge30_dev_temp | Device template for the Sl... | Feature | vEdge Cloud | 15 | 1 | admin | 05 Jun 2020 9:57:40 PM ... | In Sync | ... |

6. Navigate to the **Additional Templates** section and populate the **Security Policy** field with the policy we just created - **Guest-FW-IPS-DIA**. Click on **Update**

Additional Templates

| | |
|---------------------|---|
| AppQoE | <input type="button" value="Choose..."/> |
| Global Template * | <input type="button" value="Factory_Default_Global_CISCO_Template"/> |
| Cisco Banner | <input type="button" value="Choose..."/> |
| Cisco SNMP | <input type="button" value="Choose..."/> |
| CLI Add-On Template | <input type="button" value="Choose..."/> |
| Policy | <input type="button" value="QoS_Policy"/> |
| Probes | <input type="button" value="Choose..."/> |
| Security Policy | <input type="button" value="Guest-FW-IPS-DIA"/> |
| Container Profile * | <input type="button" value="Factory_Default_UTD_Template"/>  |

7. Click on **Next** and you can choose to view the side-by-side configuration. Click on **Configure Devices**. If you do choose to view the configuration, notice the UTD related commands being pushed by vManage - they are for the IPS module

```

    transport input ssh
    !
    470    transport input ssh
    471    !
    472    iox
    473    app-hosting appid utd
    474    app-resource package-profile cloud-low
    475    app-vnic gateway1 virtualportgroup 0 guest-interface 0
    476    guest-ipaddress 192.168.1.2 netmask 255.255.255.252
    477    !
    478    app-vnic gateway1 virtualportgroup 1 guest-interface 1
    479    guest-ipaddress 192.0.2.2 netmask 255.255.255.252
    480    !
    481    start
    482    !
    483    lldp run
    484    nat64 translation timeout tcp 60
    485    nat64 translation timeout udp 1
    486    utd multi-tenancy
    487    utd engine standard multi-tenancy
    488    threat-inspection profile Guest-IPS
    489    threat detection
    490    policy security
    491    logging level info
    492    !
    493    utd global
    494    !
    495    policy utd-policy-wrf-30
    496    all-interfaces
    497    vrf 30
    498    threat-inspection profile Guest-IPS

```

Configure Device Rollback Timer

Back Configure Devices Cancel

- The status of this change will show up as **Done - Scheduled**. This is expected since the IPS engine has to be installed on the cEdge

Push Feature Template Configuration | Validation Success

Initiated By: admin From: 192.168.0.12

Total Task: 1 | Done - Scheduled : 1

| | Status | Message | Chassis Number | Device Model | Hostname | System IP | Site ID | vManage IP |
|---|------------------|---|--|--------------|----------|---------------|---------|--------------|
| > | Done - Scheduled | Device needs to install some apps. Configuration t... | CSR-04F9482E-44F0-E4DC-D300-60C0B06F73F2 | CSR1000v | cEdge40 | 10.255.255.41 | 40 | 10.255.255.1 |

- Navigate to **Configuration => Devices** and locate the cEdge40 Device. You will notice that the Device Status is **Service Install Pending** (might have to scroll to the right or remove columns to see this)

| WAN Edge List | | | | | | | | |
|-------------------------------------|---------------------------------------|--------------------------------------|---------------|--|--------------------------|------------------------------------|---------|--|
| Configuration Devices | | | | | | | | |
| WAN Edge List | | Controllers | | | | | | |
| Change Mode | | Upload WAN Edge List | | Export Bootstrap Configuration | | Sync Smart Account | | |
| <input type="text"/> Search Options | | | | | | | | |
| Device Model | Chassis Number | Hostname | System IP | Mode | Assigned Template | Device Status | Validit | |
| CSR1000v | CSR-44C7CE5A-4149-E696-C8A8-415C... | -- | -- | CLI | -- | In Sync | valid | |
| CSR1000v | CSR-D6DB39FC-C383-BB55-7E9D-7CD... | -- | -- | CLI | -- | In Sync | valid | |
| CSR1000v | CSR-834E40DC-E358-8DE1-0E81-76E59... | cEdge50 | 10.255.255.51 | vManage | cEdge-single-uplink | In Sync | valid | |
| CSR1000v | CSR-D405F5BA-B975-8944-D1A3-2E08... | -- | -- | CLI | -- | In Sync | valid | |
| CSR1000v | CSR-D1837F36-6A1A-1850-7C1C-E1C6... | cEdge51 | 10.255.255.52 | vManage | cEdge-single-uplink | In Sync | valid | |
| CSR1000v | CSR-5E992295-1362-0DB6-EEF8-25CC... | -- | -- | CLI | -- | In Sync | valid | |
| CSR1000v | CSR-04F5482E-44F0-E4DC-D30D-60C0... | cEdge40 | 10.255.255.41 | vManage | cEdge_dualuplink_devtemp | Service Install Pending - D... | valid | |
| vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b2c91... | DC-vEdge1 | 10.255.255.11 | vManage | DCvEdge_dev_temp | In Sync | valid | |
| vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-46996cd1c3 | DC-vEdge2 | 10.255.255.12 | vManage | DCvEdge_dev_temp | In Sync | valid | |
| vEdge Cloud | b7fd7295-58df-7671-e914-6fe2edff1609 | vEdge20 | 10.255.255.21 | vManage | vEdge_Site20_dev_temp | In Sync | valid | |
| vEdge Cloud | dde90ff0-dc62-77e6-510f-08d96608537d | vEdge21 | 10.255.255.22 | vManage | vEdge_Site20_dev_temp | In Sync | valid | |
| vEdge Cloud | 17026153-f09e-be4b-6dce-482fce43aa... | vEdge30 | 10.255.255.31 | vManage | vEdge30_dev_temp | In Sync | valid | |
| CSR1000v | CSR-26217DA0-1B63-8DDE-11C9-125F... | -- | -- | CLI | -- | In Sync | valid | |
| CSR1000v | CSR-F960E020-B7C9-887F-46A8-F4537... | -- | -- | CLI | -- | In Sync | valid | |
| CSR1000v | CSR-25925FBC-07F3-0732-E127-EA95... | -- | -- | CLI | -- | In Sync | valid | |

Since it takes approximately 5 minutes for the install process to go through, this will be a perfect time to grab a cup of tea/coffee! We will validate the installation in the next section.

Task List

- [Overview](#)
- [Initial Configuration](#)
- [Revert Site 40 PC changes and enable DIA](#)
- [Upload Image to vManage](#)
- [Add the Security Policy](#)
- [Firewall Policy Update](#)
- [Add the IPS Policy and Finalize the Security Policy](#)
- [Updating the Application List and Device Template](#)
- [Verifying installation and performing signature updates](#)
- [Activity Verification](#)

Verifying installation and performing signature updates

- After you're done with the cup of tea/coffee, check the **Configuration => Devices** page again. cEdge40 should now be **In Sync**

| Device Model | Chassis Number | Hostname | System IP | Mode | Assigned Template | Device Status | V |
|--------------|---------------------------------------|-----------|---------------|---------|--------------------------|---------------|----|
| CSR1000v | CSR-44C7CE5A-4149-E696-C8A8-415C... | -- | -- | CLI | -- | | V4 |
| CSR1000v | CSR-D6DB39FC-C383-BB55-7E9D-7CD... | -- | -- | CLI | -- | | V4 |
| CSR1000v | CSR-834E40DC-E358-8DE1-0E81-76E59... | cEdge50 | 10.255.255.51 | vManage | cEdge-single-uplink | In Sync | V4 |
| CSR1000v | CSR-D405F5BA-B975-8944-D1A3-2E08... | -- | -- | CLI | -- | | V4 |
| CSR1000v | CSR-D1837F36-6A1A-1850-7C1C-E1C6... | cEdge51 | 10.255.255.52 | vManage | cEdge-single-uplink | In Sync | V4 |
| CSR1000v | CSR-5E992295-1362-0DB6-EEF8-25CC... | -- | -- | CLI | -- | | V4 |
| CSR1000v | CSR-04F9482E-44F0-E4DC-D30D-60C0... | cEdge40 | 10.255.255.41 | vManage | cEdge_dualuplink_devtemp | In Sync | V4 |
| vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b2c91... | DC-vEdge1 | 10.255.255.11 | vManage | DCvEdge_dev_temp | In Sync | V4 |
| vEdge Cloud | 0cdd4f0e-f2f1-fe75-866c-469966cda1c3 | DC-vEdge2 | 10.255.255.12 | vManage | DCvEdge_dev_temp | In Sync | V4 |
| vEdge Cloud | b7fd7295-50df-7671-e914-6fe2edff1609 | vEdge20 | 10.255.255.21 | vManage | vEdge_Site20_dev_temp | In Sync | V4 |
| vEdge Cloud | dde90ff0-dc62-77e6-510f-08d96608537d | vEdge21 | 10.255.255.22 | vManage | vEdge_Site20_dev_temp | In Sync | V4 |
| vEdge Cloud | 17026153-f09e-be4b-6dce-482fce43aa... | vEdge30 | 10.255.255.31 | vManage | vEdge30_dev_temp | In Sync | V4 |
| CSR1000v | CSR-26217DA0-1B63-8DDE-11C9-125F... | -- | -- | CLI | -- | | V4 |
| CSR1000v | CSR-F960E020-B7C9-887F-46A8-F4537... | -- | -- | CLI | -- | | V4 |

- Log in to the CLI of cEdge40 via Putty and enter the `show utd engine standard status` command. The **Overall system status** should be *Green* and the Engine should be *Running*. If the **Signature** is version *29.0.c*, proceed to the next step else skip to [Activity Verification](#)

```

cEdge40#show utd engine standard status
Engine version      : 1.0.6_SV2.9.13.0_XE17.2
Profile            : Cloud-Low
System memory      :
    Usage   : 6.50 %
    Status  : Green
Number of engines   : 1

Engine       Running     Health     Reason
=====
Engine (#1): Yes        Green      None
=====

Overall system status: Green

Signature update status:
=====
Current signature package version: 29.0.c
Last update status: None
Last successful update time: None
Last failed update time: None
Last failed update reason: None
Next update scheduled at: None
Current status: Idle

cEdge40#
cEdge40#
cEdge40#
```

show utd engine standard status

- To update the signatures, run the command `copy scp: bootflash:`. Details to be entered are given below, confirm the signature update

| Address or name of remote host | Source username | Source filename | Destination filename | Password |
|-----------------------------------|--------------------|---------------------------------------|---------------------------------------|----------|
| 100.100.100.1 | admin | UTD-STD-SIGNATURE- 29130-115-S.pkg | UTD-STD-SIGNATURE- 29130-115-S.pkg | admin |

```
cEdge40#copy scp: bootflash:  
Address or name of remote host []? 100.100.100.1  
Source username [admin]?  
Source filename []? UTD-STD-SIGNATURE-29130-115-S.pkg  
Destination filename [UTD-STD-SIGNATURE-29130-115-S.pkg]?  
Password:  
!!!!!!
```

Once the image is copied over to the bootflash: of cEdge40, run the command `utd signature update file bootflash:UTD-STD-SIGNATURE-29130-115-S.pkg`. Confirm the signature update

```
cEdge40#utd signature update file bootflash:UTD-STD-SIGNATURE-29130-115-S.pkg  
% This operation may cause the UTD service to restart which will briefly interrupt services.  
Proceed with signature update? [confirm]  
cEdge40#
```

```
copy scp: bootflash:  
utd signature update file bootflash:UTD-STD-SIGNATURE-29130-115-S.pkg
```

4. Run `show utd engine standard status` to check if the signature package version matches with the image below

192.168.0.40 - PuTTY

```
cEdge40#show utd engine standard status
Engine version      : 1.0.6_SV2.9.13.0_XE17.2
Profile            : Cloud-Low
System memory      :
    Usage   : 20.50 %
    Status  : Green
Number of engines   : 1

Engine     Running   Health   Reason
=====
Engine(#1) : Yes       Green    None
=====

Overall system status: Green

Signature update status:
=====
Current signature package version: 29130.115.s
Last update status: Successful
Last successful update time: Sat Jun  6 11:02:12 2020 UTC
Last failed update time: None
Last failed update reason: None
Next update scheduled at: None
Current status: Idle
```

```
show utd engine standard status
```

Task List

- [Overview](#)
- [Initial Configuration](#)
- [Revert Site 40 PC changes and enable DIA](#)
- [Upload Image to vManage](#)
- [Add the Security Policy](#)
- [Firewall Policy Update](#)
- [Add the IPS Policy and Finalize the Security Policy](#)
- [Updating the Application List and Device Template](#)
- [Verifying installation and performing signature updates](#)
- [Activity Verification](#)

Activity Verification

1. Log in to vCenter and console in to your Site 40 PC again, like before ([click here](#) to review the process). Open Terminal and type `ping 8.8.8.8` to verify that Internet connectivity is still there

```
sdwan@10-40-30-21:~$  
sdwan@10-40-30-21:~$  
sdwan@10-40-30-21:~$  
sdwan@10-40-30-21:~$  
sdwan@10-40-30-21:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=5.91 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=20.7 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=22.0 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=22.1 ms  
64 bytes from 8.8.8.8: icmp_seq=6 ttl=53 time=21.5 ms  
64 bytes from 8.8.8.8: icmp_seq=7 ttl=53 time=22.6 ms  
64 bytes from 8.8.8.8: icmp_seq=8 ttl=53 time=7.49 ms
```

2. Still in Terminal, run `./ips.sh` to trigger a few HTTP connections which will trigger the IPS

```
sdwan@10-40-30-21:~$ ./ips.sh  
Triggering IPS Signatures  
Task 1/3  
Task 2/3  
Task 3/3  
X50!P%@AP[4\PZX54(P^)7CC)7]$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*Tasks Compl  
eted  
sdwan@10-40-30-21:~$
```

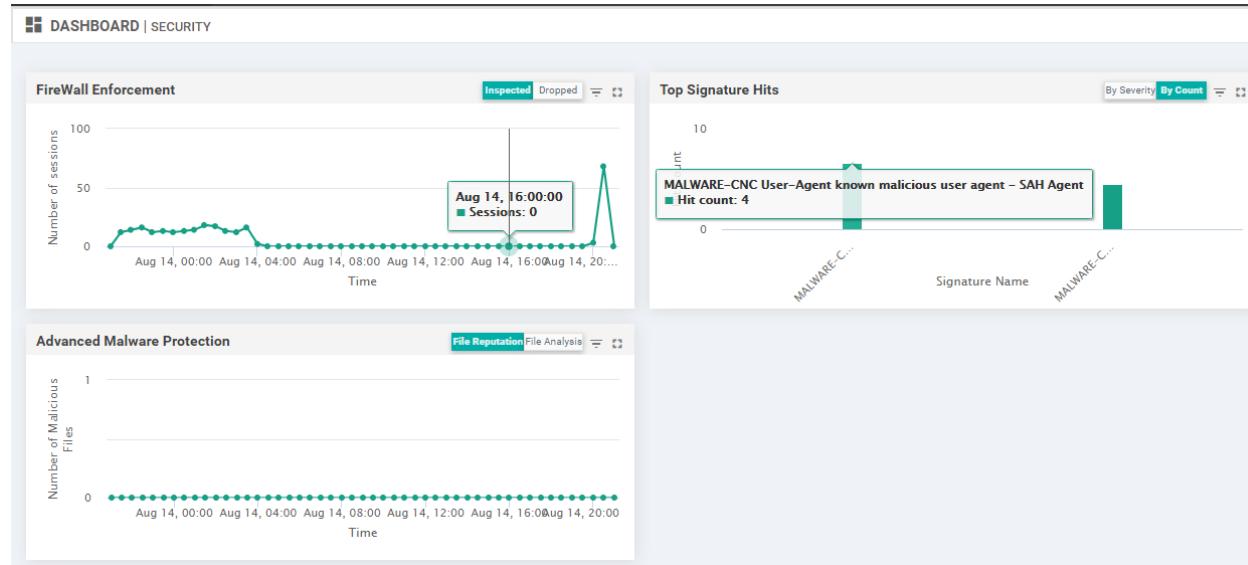
3. Back at the cEdge40 CLI, issue `show utd engine standard logging events`. You should see alerts triggered as a result of running the ips.sh file (this file attempts to download some simulated malware). Thus, our IPS engine is working as expected

```

cEdge40#
cEdge40#
cEdge40#
cEdge40#show utd engine standard logging events
2020/08/31-11:48:36.902790 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] [1:5808:10] MALWARE-CNC User-Agent known malicious user agent - SAH Agent [**] [Classification: Misc activity] [Priority: 3] [VRF: 30] {TCP} 10.40.30.21:45224 -> 89.238.73.97:80
2020/08/31-11:48:36.902790 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] [1:7187:13] MALWARE-CNC User-Agent known malicious user agent - SAH Agent [**] [Classification: Information Leak] [Priority: 2] [VRF: 30] {TCP} 10.40.30.21:45224 -> 89.238.73.97:80
2020/08/31-11:48:37.068710 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] [1:21475:4] MALWARE-CNC User-Agent known malicious user-agent string core-project [**] [Classification: Misc activity] [Priority: 3] [VRF: 30] {TCP} 10.40.30.21:45226 -> 89.238.73.97:80
cEdge40#
cEdge40#

```

4. We can view this information on the vManage GUI as well. Go to **Dashboard => Security** and you should see some **Signature** hits. The dashboard does take some time to get populated (it's never too soon for another cup of tea/coffee!)



This completes the verification activity.

Task List

- [Overview](#)
- [Initial Configuration](#)
- [Revert Site 40 PC changes and enable DIA](#)
- [Upload Image to vManage](#)
- [Add the Security Policy](#)
- [Firewall Policy Update](#)
- [Add the IPS Policy and Finalize the Security Policy](#)
- [Updating the Application List and Device Template](#)
- [Verifying installation and performing signature updates](#)
- [Activity Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: June 3, 2020

Site last generated: Jul 23, 2020



-->

Configuring URL Filtering

Summary: Configuring URL Filtering for DIA Guest Users

Table of Contents

- [Updating the Security Policy](#)
- [Verification](#)

Task List

- Updating the Security Policy
- Verification

Updating the Security Policy

URL Filtering allows networks to block traffic to certain sites by utilizing URL-based policies. It is implemented using the Snort Engine.

1. On the vManage GUI, navigate to **Configuration => Security**. Locate the *Guest-FW-IPS-DIA* policy and click on the three dots next to it. Choose to **Edit** the policy. We will add URL Filtering capabilities to the same policy which we used for IPS deployment

CONFIGURATION | SECURITY

Add Security Policy

Search Options ▾

Total Rows: 2

| Name | Description | Use Case | Devices Attached | Device Templates | Updated By | Last Updated | ... |
|------------------|----------------------------|--------------|------------------|------------------|------------|----------------------------|-----|
| Guest-FW-IPS-DIA | Guest Firewall and IPS DIA | Custom | 1 | 1 | admin | 06 Jun 2020 3:38:04 AM PDT | |
| Site40-Guest-DIA | Guest Policy for Site 40 | Guest Access | 0 | 0 | admin | 03 Jun 2020 10:4 | |

2. Click on the **URL Filtering** tab and then click on **Add URL Filtering Policy**. Choose **Create New**

Security > Edit Security Policy Guest-FW-IPS-DIA

Firewall Intrusion Prevention **URL Filtering** Advanced Malware Protection DNS Security TLS/SSL Decryption Policy Summary

Enhance your security by allowing or disallowing pre-defined web categories or custom created URL lists.

Info Please upload compatible Security App Hosting Image File to the software repository in order to support URL-F functions. You can upload the image file from Maintenance > Software Repository > Virtual Images

Add URL Filtering Policy ▾

Create New (highlighted with a red box)

Copy from Existing

3. Click on **Target VPNs** and enter a Target VPN of 30. Click on **Save Changes**

Edit Target VPNs

VPNs 30

Save Changes Cancel

4. Enter *URLF-NoShopping* for the **Policy Name**. Set the **Web Categories** to Block and add *auctions* and *shopping* to the categories. Set the **Web Reputation** to High Risk

URL Filtering - Policy Rule Configuration i

| | |
|--------------------|---|
| Policy Name | URLF-NoShopping |
| Web Categories | Block auctions X shopping X |
| Web Reputation | High Risk |
| Advanced ▾ | |
| Whitelist URL List | Select a whitelist url list |

5. Specify *This is not allowed!* in the **Content Body** and make sure all the **Alerts** are selected. Click on **Save URL Filtering Policy**

URL Filtering - Policy Rule Configuration ⓘ

Content Body

Redirect URL ⓘ

Alerts and Logs ⓘ

Alerts Blacklist Whitelist Reputation/Category

Save URL Filtering Policy CANCEL

6. Make sure the *URLF-NoShopping* URL Filtering policy shows up and click on **Save Policy Changes**

| Name | Type | Reference Count | Updated By |
|-----------------|--------------|-----------------|------------|
| URLF-NoShopping | urlFiltering | 0 | admin |

Preview Save Policy Changes CANCEL

7. Click on **Next** and choose to **Configure Devices**. You can check the side-by-side configuration if needed, making note of the `web-filter` and `block page-profile` configuration being pushed by vManage. This is our URL-F configuration

Device Template
cEdge_dualuplink_devtemp Total 1

Device list (Total: 1 devices)

Filter/Search

CSR-04F9482E-44F0-E4DC-D300-
60C0B00F73F2
cEdge40|10.255.255.41

```

485 nat64 translation timeout udp 1
486 utd multi-tenancy
487 utd engine standard multi-tenancy
488 web-filter block page profile block-URLF-NoShopping
489 text Access to the requested page has been denied. This is not allowed.
490 !
491 web-filter url profile URLF-NoShopping
492 alert blacklist categories-reputation whitelist
493 categories block
494 auctions
495 shopping
496 !
497 block page-profile block-URLF-NoShopping
498 log level error
499 reputation
500 block-threshold high-risk
501 !
502 !
503 threat-inspection profile Guest-IPS
504 threat detection
505 policy security
506 logging level info
507 !
508 utd global
509 !
510 policy utd-policy-vrf-30
511 all-interfaces
512 vrf 30
513 threat-inspection profile Guest-IPS

```

Activate Windows
Go to Settings to activate Windows.

Configure Device Rollback Timer

[Back](#) [Configure Devices](#) [Cancel](#)

Task List

- [Updating the Security Policy](#)
- [Verification](#)

Verification

Wait for a few minutes before going through the verification steps enumerated below.

1. Log in to the Site40 PC by accessing vCenter (use the bookmark or access 10.2.1.50/ui). Log in using the credentials provided and click on the sdnw-slc/ghi-site40pc-podX. Click on the console icon to open a Web Console. Open an **Incognito window** in Chrome or a **Private Browsing** tab in Mozilla Firefox. Try to access <http://www.amazon.com>. The page should get blocked, giving the message we had customized



2. Log in to the CLI for **cEdge40** via Putty and issue `show utd engine standard logging events`. This will show us amazon.com being blocked with a category of **shopping** attached to it

```
2020/08/15-04:41:06.182754 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: www.amazon.com/] ** [Category: Shopping] ** [Reputation: 81] [VRF: 30] {TCP} 10.40.30.21:43530 -> 13.35.130.68:80  
2020/08/15-04:41:06.498757 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: www.amazon.com/favicon.ico] ** [Category: Shopping] ** [Reputation: 81] [VRF: 30] {TCP} 10.40.30.21:43532 -> 13.35.130.68:80  
cEdge40#  
cEdge40#
```

URL Filtering is working as expected in our lab environment.

Task List

- [Updating the Security Policy](#)
- [Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: June 3, 2020

Site last generated: Sep 1, 2020



-->

Software Defined Application Visibility and Control

Summary: Installing and Configuring SD-AVC in a Cisco SD-WAN environment for DPI and First Packet Identification

Table of Contents

- [Enabling AVC on vManage and Verification](#)
- [Checking Policy configuration for AVC](#)
- [Verification](#)

Task List

- Enabling AVC on vManage and Verification
- Checking Policy configuration for AVC
- Verification

Enabling AVC on vManage and Verification

vManage acts as the SD-AVC Network Controller and the cEdges act as SD-AVC clients. In order to make vManage the AVC Controller, we need to enable the functionality on the GUI. In previous versions of vManage, this entailed uploading an SD-AVC image to vManage but with version 20.3.x, the AVC container comes bundled with the vManage image. It just needs to be enabled.

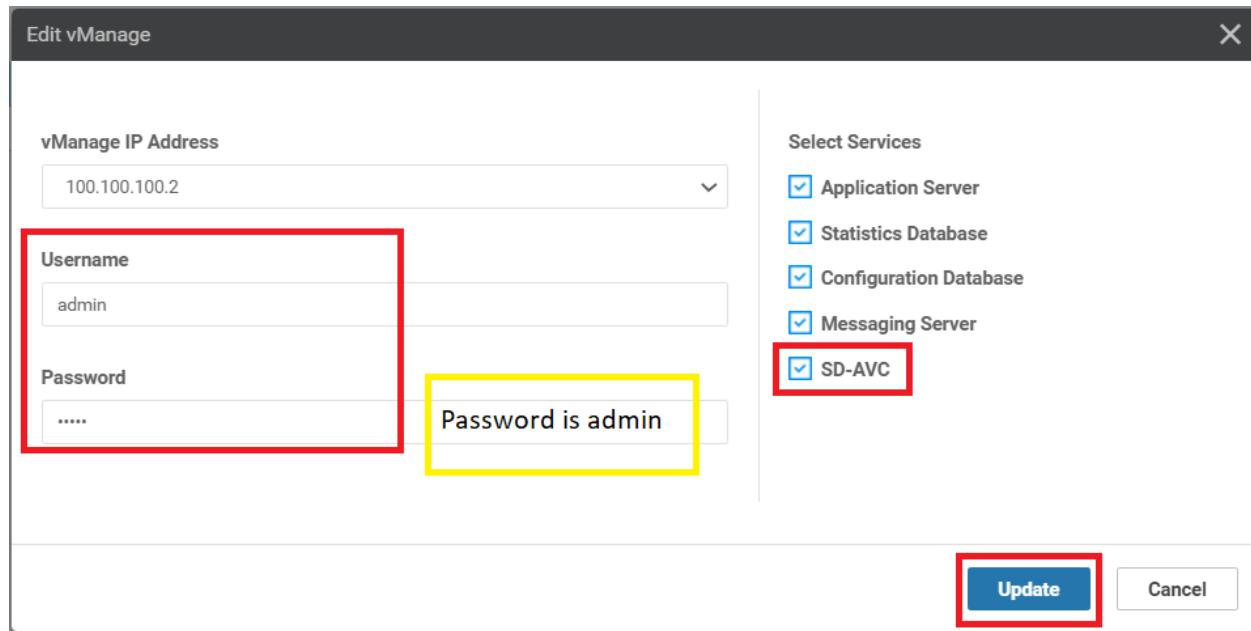
1. Navigate to **Administration => Cluster Management**

The screenshot shows the Cisco vManage interface. The top navigation bar includes the Cisco logo and the title "Cisco vManage". Below the navigation bar, there is a banner with the text "Virtual image uploaded successfully". The main content area has two tabs: "Software Images" and "Virtual Images", with "Virtual Images" being the active tab. Underneath these tabs are two buttons: "Upload Virtual Image" and "Add Custom VNF Package". A search bar and a "Search Options" dropdown are also present. A table displays several rows of virtual images, with one row highlighted in yellow. The columns in the table are: Software Version, Software Location, Network Function Type, Image Type, Architecture, Version Type Name, and Vendor. The first row shows values: 3.0.0, vmanage, Container, x86_64, sdavc_container, Cisco System. The second row, which is highlighted, shows values: Administration, vmanage, App-Hosting, Lxc, x86_64, Security Application, Cisco System. On the left side of the interface, there is a vertical sidebar with various management options: Settings, Manage Users, Cluster Management (which is currently selected), Integration Management, Disaster Recovery, VPN Groups, and VPN Segments.

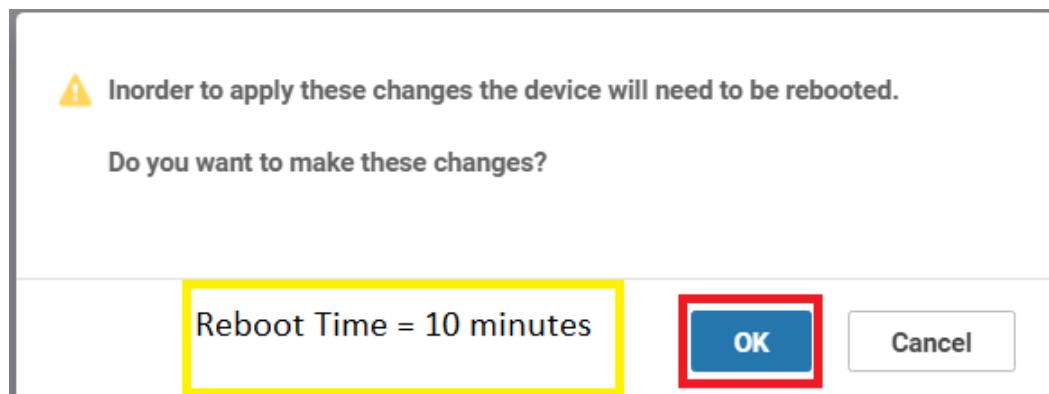
2. Click on the three dots next to **vmanage** and click on **Edit**

The screenshot shows the "Service Configuration" page. At the top, there are tabs for "Service Configuration" and "Service Reachability", with "Service Configuration" being the active tab. Below the tabs is a button "Add vManage". A note says "Click hostname or status icon for more information". To the right, there is a legend: "Normal" (green circle), "Warning" (yellow circle), "Error" (red circle), and "Disabled" (grey circle). The main content is a table with columns: Hostname, IP Address, Status, Application Server, Statistics Database, Configuration Database, Messaging Server, SD-AVC, and UUID. One row in the table is highlighted in yellow, representing the "vmanage" entry. The "Hostname" column shows "localhost", the "IP Address" column shows "localhost", the "Status" column shows "Ready", and the "UUID" column shows "dfea63a5-66d2-4e50-a07...". To the right of the table, there is a small box with the text "Device Connected" and three options: "Edit" (which is highlighted with a red box), "Remove", and "Edit".

3. Enter the username of **admin** and a password of **admin**. Put a check mark next to SD-AVC (this will automatically check Application Server as well) and click on **Update**



4. The vManage will reboot once we click on **OK**. Click **OK** and the vManage should go down. It will take approximately 10 minutes for the server to come back up completely





- After the vManage comes up, log in to the GUI and navigate to **Administration => Cluster Management**. The SD-
AVC column should have a green check mark

The screenshot shows the "Service Configuration" tab of the Cisco vManage interface. At the top, there are tabs for "Service Configuration" and "Service Reachability", with "Service Configuration" being the active tab. A button labeled "Add vManage" is visible. Below the tabs, there is a note: "Click hostname or status icon for more information". The main area is a table with the following columns: Hostname, IP Address, Status, Application Server, Statistics Database, Configuration Database, Messaging Server, and SD-VC. A single row is present, showing "vmanage" as the hostname, "100.100.100.2" as the IP address, "Ready" as the status, and green checkmarks in all other columns except SD-VC, which also has a green checkmark. A red box highlights the "SD-VC" column header.

| Hostname | IP Address | Status | Application Server | Statistics Database | Configuration Database | Messaging Server | SD-VC |
|----------|---------------|--------|--------------------|---------------------|------------------------|------------------|-------|
| vmanage | 100.100.100.2 | Ready | ✓ | ✓ | ✓ | ✓ | ✓ |

- Log in to the CLI for vManage via Putty and run the command `request nms container-manager status`. We
should see the NMS Container Manager enabled

```
ISS - 1000

vmanage# request nms container-manager status
NMS container manager
    Enabled: true
    Status: running PID:6300 for 9911s
vmanage#
vmanage#
vmanage#
vmanage#
vmanage# █
```

```
request nms container-manager status
```

7. We can also run `request nms-container sdavc_container status` and `request nms-container sdavc_container diag` and this should show that the sdavc_container is UP, along with a few more details of the container itself

```
vmanage# request nms-container sdavc_container status
Container: sdavc container
Created: 11 minutes ago ago
Status: Up 11 minutes
vmanage# request nms-container sdavc_container diag
  cpuUsagePercent : 0
  availableDiskMemoryNumCores : 11094294528
  dnsConnected : True
  totalMemory : 5368709120
  totalMemoryUsage : 2364580864
  avcDashboardTotalMemory : 622395392
  logsDiskMemory : 133868
  avcDashboardFreeMemory : 508916176
  id : 1
  totalPacketDrops : 0
  totalDiskMemory : 15970770944
  avcNumCores : 8
  syslogIP :
  totalPackets : 183
  activeFtpConnections : 0
  lastPacketDrops : 0
  avcFreeMemory : 2585906592
  mysqlDiskMemory : 47215233
  avcWarnLogNum : 223
  ppsRate : 0
  avcTotalMemory : 2787508224
  dnsServers : [{u'canOverride': False, u'server': u'10.2.1.5'}]
  externalApi : {u'status': u'OK', u'needRestart': False}
  avcErrorLogNum : 0
-----
      Service Details
-----
Service : AVC service
  pid : 396
  etime : 11:30
  user : sdavc
  cpu : 12.2
  rss : 1606768
```

```
request nms-container sdavc_container status
request nms-container sdavc_container diag
```

Task List

- Enabling AVC on vManage and Verification
- Checking Policy configuration for AVC
- Verification

Checking Policy configuration for AVC

The configuration we had done for QoS also had the relevant configuration required for SD-AVC to function. Our policy configuration done for QoS coincidentally allows the cEdge to become an SD-AVC Agent as well. In this section, we will review the configuration in place for the cEdges to become SD-AVC agents.

⚠ Important: No changes need to be made in this section. It is just for information and review purpose.

1. On the vManage GUI, navigate to **Configuration => Policies** and click on the **Localized Policy** tab. Locate the **QoS_Policy** created before and click on the three dots next to it. Choose to **Edit** (we won't be making any changes, just review)

| Name | Description | Devices Attached | Device Templates | Updated By | Last Updated |
|-----------------------|---|------------------|------------------|------------|-----------------------------|
| Police-AAR-Impairment | Injecting Impairment for AAR via a Policer - Pac... | 0 | 0 | admin | 04 Jun 2020 8:39:13 AM PDT |
| QoS_Policy | QoS Policy | 2 | 2 | admin | 04 Jun 2020 10:04:29 AM PDT |

2. Go to the **Policy Overview** tab and make note of the name of the Policy (**QoS_Policy**). Under **Policy Settings**, the **Application** check box has been checked - this is what triggers configuration that makes the cEdge an SD-AVC Agent. Click on **Cancel** to exit out of the Policy

CONFIGURATION | POLICIES Localized Policy > Edit Policy

Policy Overview Forwarding Class/QoS Access Control Lists Route Policy

Enter name and description for your localized master policy

Policy Name: QoS_Policy
Policy Description: QoS Policy

Policy Settings

Netflow Application Cloud QoS Cloud QoS Service side Implicit ACL Logging

Log Frequency: 30

3. This policy is called in the Device Template. Navigate to Configuration => Templates and click on the three dots next to `cedge_dualuplink_devtemp`. Choose to **Edit** (we won't be making any changes, just review)

CONFIGURATION | TEMPLATES

Device Feature

Create Template

Template Type: NonDefault

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status | Action |
|---------------------------------|----------------------------------|---------|--------------|-------------------|------------------|------------|-----------------------------|-----------------|--------|
| DCvEdge_dev_temp | Device template for the DCv... | Feature | vEdge Cloud | 16 | 2 | admin | 28 May 2020 4:58:07 AM PDT | In Sync | ... |
| vEdge_Site20_dev_temp | Device template for the Site ... | Feature | vEdge Cloud | 17 | 1 | admin | 07 Jun 2020 6:57:21 AM PDT | In Sync | ... |
| cEdge-single-uplink | Single Uplink cEdge Device T... | Feature | CSR1000v | 17 | 2 | admin | 26 May 2020 3:05:01 AM PDT | In Sync | ... |
| vEdge_Site20_dev_temp_nat | Device template for the Site ... | Feature | vEdge Cloud | 17 | 1 | admin | 07 Jun 2020 6:56:52 AM PDT | In Sync | ... |
| vSmart-dev-temp | Device Template for vSmart | Feature | vSmart | 9 | 2 | admin | 25 May 2020 10:13:06 AM PDT | In Sync | ... |
| vEdge20_dev_temp | Device template for the Site ... | Feature | vEdge Cloud | 15 | 1 | admin | 05 Jun 2020 9:57:40 PM PDT | In Sync | ... |
| cEdge_dualuplink_devtemp | cEdge Device Template for d... | Feature | CSR1000v | 20 | 1 | admin | 06 Jun 2020 3:48:59 AM PDT | In Sync | ... |

Total Rows: 7

Actions for cEdge_dualuplink_devtemp:

- Edit (highlighted with a red box)
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

4. Under the Additional Templates section, we have the `QoS_Policy` Policy populated, which ensures that the cEdge40 device is configured for SD-AVC. Click **Cancel** to exit out of the Device Template

Additional Templates

| | |
|---------------------|---------------------------------------|
| AppQoE | Choose... |
| Global Template * | Factory_Default_Global_CISCO_Template |
| Cisco Banner | Choose... |
| Cisco SNMP | Choose... |
| CLI Add-On Template | Choose... |
| Policy | QoS_Policy |
| Probes | Choose... |
| Security Policy | Guest-FW-IPS-DIA |
| Container Profile * | Factory_Default_UTD_Template |

Task List

- [Enabling AVC on vManage and Verification](#)
- [Checking Policy configuration for AVC](#)
- [Verification](#)

Verification

1. Open a new browser window/tab and navigate to <https://100.100.100.2:10502/>. This is the SD-AVC portal running as a container on vManage. Notice that one device is being monitored by SD-AVC and it is showing some traffic with the specific application layer protocol seen (output might vary). Click on the *Devices* 1 too view details about the Device

The screenshot shows the Cisco SD-AVC interface. At the top, there are two tabs: 'Cisco vManage' and 'Cisco SD-AVC'. The 'Cisco SD-AVC' tab is active, indicated by a blue bar and the title 'Cisco SD-AVC'. The address bar shows 'Not secure | 192.168.0.6:10502/#/admin/summary'. Below the tabs, there are navigation links: 'Apps', 'vManage', and 'vCenter'. On the left, a sidebar menu includes 'Application Visibility', 'Protocol Packs', 'Connectors', and 'Serviceability'. The main content area is titled 'All Devices' and displays a 'Summary' section with metrics: Classification Score (67%), First Packet Classification (80%), Total Usage (10.52 KB), SD-AVC Coverage Ratio (0%), and Asymmetry Index (0 / 10). Below this is a 'Timeline' chart showing bandwidth usage over time, with a red box highlighting the chart area. A table below the timeline lists applications and their usage: Interior Gateway Routing Protocol (61.85% usage) and HTTP (25.89% usage). A red box highlights this table. On the right side, there is a 'SD-AVC Monitoring' section showing 1 segment and 1 device, with a red box highlighting the 'Devices' section. Below this are sections for 'Connectors' (Cloud Connector) and 'Installed Protocol Packs' (Protocol Pack 47.0). A message at the bottom right says 'Activate Windows'.

2. We are taken to the Device Specific AVC page for cEdge40. At the top, we have a summary of the statistics and insights from AVC's standpoint

Cisco SD-AVC

Application Visibility

Protocol Packs

Connectors

Serviceability

cEdge40 (Device) Change

Summary

| Classification Score | First Packet Classification | Total Usage | SD-AVC Coverage Ratio | Asymmetry Index |
|----------------------|-----------------------------|-------------|-----------------------|-----------------|
| 67% | 80% | 10.52 KB | 0% | 0 / 10 |

Timeline

Bandwidth

Total (bps)

Search in 4 applications...

| Application | Usage | Business Relevance |
|-----------------------------------|------------------|--------------------|
| Interior Gateway Routing Protocol | 61.85% (6.50 KB) | relevant |
| HTTP | 25.89% (2.72 KB) | default |

System Time: 2020-06-07 09:09
Uptime: 17 minutes
About
© 2020 Cisco Systems, Inc.

A red box highlights the top section of the summary table.

3. Log in to the CLI of cEdge40 via Putty and run the command `show avc sd-service info summary`. You should see that the cEdge is connected to the SD-AVC controller, along with details of the controller

```
cEdge40#show avc sd-service info summary
```

```
Status: CONNECTED
```

```
Device ID: cEdge40
Device segment name: swat-sdwanlab
Device address: 10.255.255.41
Device OS version: 17.03.01a
Device type: CSR1000V
```

```
Active controller:
```

```
Type    : Primary
IP     : 10.255.255.1
Status: Connected
Version       : 4.0.0
Last connection: *13:12:55.000 UTC Mon Aug 31 2020
```

```
Active SDAVC import files:
```

```
Protocol pack:           Not loaded
Secondary protocol pack: Not loaded
Rules pack:              pp_update_swat-sdwanlab_v2_20200831130906163.pack
```

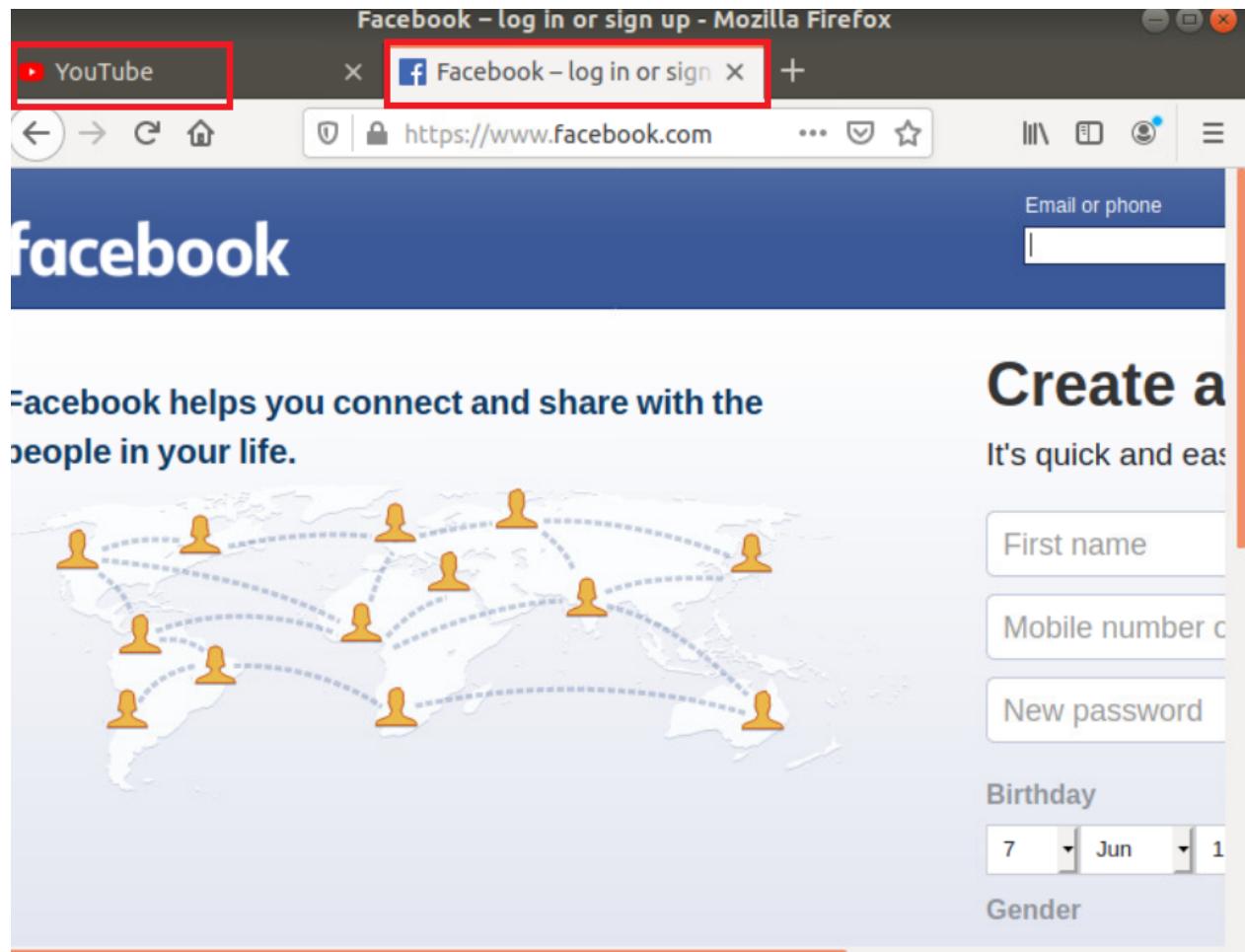
```
cEdge40#
```

```
show avc sd-service info summary
```

4. We can also run `show avc sd-service info connect` to view detailed information about the connection to the Controller

```
cEdge40#show avc sd-service info connect
Connection Status:
  Connection: CONNECTED
  Last disconnection: Never
  Mode      : Standalone
  connectivityTimeout (sec)      : 900
  connectivityCheckInterval (sec) : 30
  connectivityCheckInterval was changed: TRUE
Active controller:
  Type   : Primary
  IP     : 10.255.255.1
  Status: Connected
  Last connection      : *16:09:58.000 UTC Sun Jun 7 2020 (6 seconds ago)
  bypass   : FALSE
  force down: FALSE
HA Debug info
Monitor task:
  Task has started:          TRUE
  Task is running:           FALSE
  Task is waiting for timeout: FALSE
  Task interval: 1
  Task failed to update period: 0
  Task failed to stop       : 0
High Availability task:
  Task has started:          FALSE
  Task failed to start      : 0
  Scheduler failed to create : 0
  Scheduler failed to delete : 0
  Task failed to lock       : 0
  HA notification failed    : 0
Primary controller connection:
  Failed to copy: 4244
  Net valid : 0
```

5. Log in to the Site40 PC by accessing vCenter (use the bookmark or access 10.2.1.50/ui). Log in using the credentials provided and click on the sdwan-slc/ghi-site40pc-podX. Click on the console icon to open a Web Console. Open Firefox and go to youtube.com and facebook.com. For good measure, open about 4 tabs of these sites



- Once the sites have loaded, click on **Application Visibility** (top left-hand corner) and you should notice the AVC controller detect YouTube and Facebook traffic. This normally takes approximately 5 minutes to show up on the SD-
AVC dashboard

Cisco SD-AVC

Application Visibility

- Protocol Packs
- Connectors
- Serviceability

All Devices

Summary

| | | | | |
|-----------------------------|------------------------------------|-------------------------|-----------------------------|---------------------------|
| Classification Score 93% | First Packet Classification 84% | Total Usage 10.53 MB | SD-AVC Coverage Ratio 0% | Asymmetry Index 0 / 10 |
|-----------------------------|------------------------------------|-------------------------|-----------------------------|---------------------------|

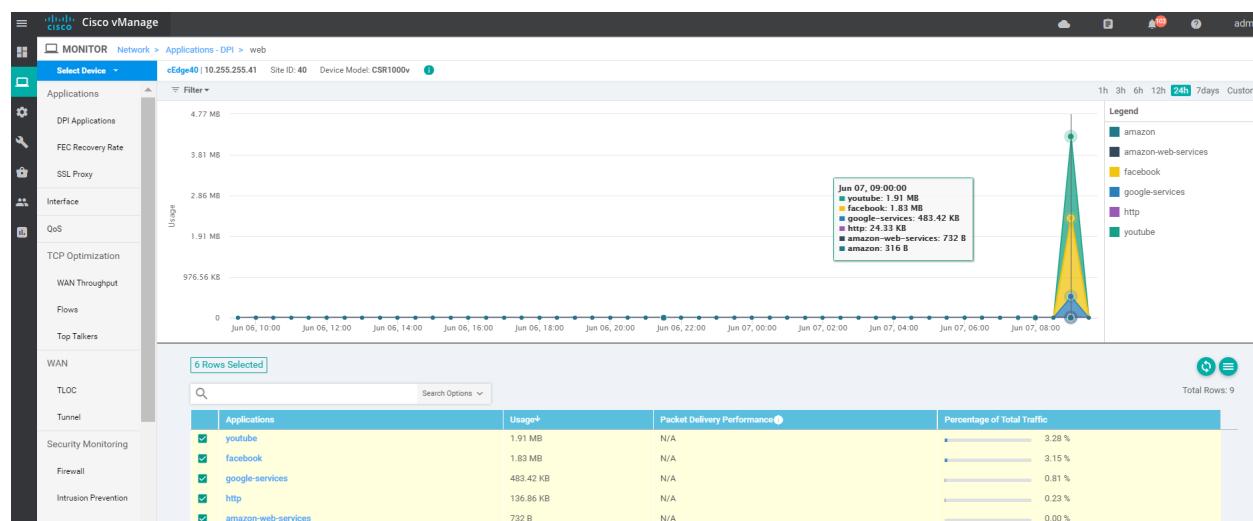
Timeline

Search in 20 applications...

| Application | Usage | Business Relevance |
|--------------------------------|-------------------|--------------------|
| Youtube | 37.51% (3.95 MB) | irrelevant |
| Facebook | 35.93% (3.78 MB) | irrelevant |
| Google Accounts Authentication | 9.17% (988.61 KB) | irrelevant |
| Google Services | 7.73% (833.34 KB) | default |

System Time: 2020-06-07 09:35
Uptime: 43 minutes
About © 2020 Cisco Systems, Inc.

7. This information can be viewed on vManage as well. From the vManage GUI, navigate to **Monitor => Network**. Click on cEdge40 and then click on **DPI Applications**. Choose the **Web** traffic and you will notice Youtube and Facebook traffic pop up over there with detailed statistics associated with the traffic. This might take some time to get populated - wait for about 15 minutes and use the refresh button



This completes SD-AVC setup and verification.

Task List

- [Enabling AVC on vManage and Verification](#)
- [Checking Policy configuration for AVC](#)
- [Verification](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: June 3, 2020

Site last generated: Sep 1, 2020



-->

Integrating Cisco SD-WAN and Umbrella

Summary: Cisco SD-WAN Security with Umbrella integration.

Table of Contents

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella ours](#)
 - [API Keys and AD Configuration](#)
 - [DC Configuration Download](#)
 - [AD Connectors](#)
 - [Roaming Computer Configuration](#)
- [Building a DNS Policy](#)
- [Setting up IPSEC Tunnels](#)
- [Configuring a Firewall Policy](#)
- [Configuring a Web Policy](#)

Task List

- Overview
- Pre-Work
- Enabling Site 30 for DIA
- Life without Cisco Umbrella
- Basic Configuration for Umbrella
- Making Umbrella Ours

- API Keys and AD Configuration
 - DC Configuration Download
 - AD Connectors
 - Roaming Computer Configuration
- Building a DNS Policy
- Setting up IPSEC Tunnels
 - Configuring a Firewall Policy
 - Configuring a Web Policy

Overview

Cisco Umbrella offers flexible, cloud-delivered security when and how you need it. It combines multiple security functions into one solution, so you can extend protection to devices, remote users, and distributed locations anywhere. Umbrella is the easiest way to effectively protect your users everywhere in minutes.

The Umbrella portfolio includes, among others, the following Security functions:

- DNS Layer Security
- Cloud-delivered Firewall (IPSEC Tunnel)
- Secure Web Gateway (IPSEC Tunnel)

In this section, we will deploy DNS Layer Security as an Umbrella feature and then see how SD-WAN can simplify Tunnel creation and Cloud-Delivered Firewall/SWG functionality.

Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - API Keys and AD Configuration
 - DC Configuration Download
 - AD Connectors
 - Roaming Computer Configuration

- Building a DNS Policy
- Setting up IPSEC Tunnels
- Configuring a Firewall Policy
- Configuring a Web Policy

Pre-Work

We will need to change a few settings with respect to the DNS servers to ensure that the Umbrella infrastructure isn't utilized by the SD-WAN solution. As of now, all DNS traffic is being queried via the Umbrella resolvers.

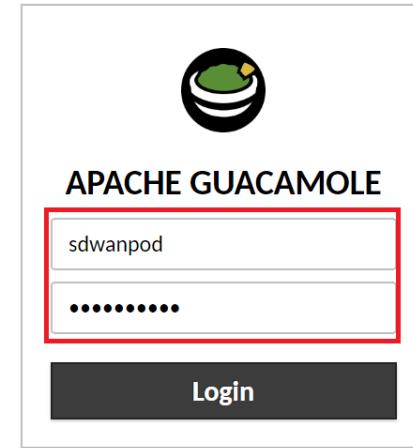
Additionally, we will be working on the Site 30 PC which is part of an AD domain (swatsdwanlab.com). The Domain Controller is at 10.30.10.50, which is also acting as the DNS server for the Site 30 PC.

1. Connect to the Site 30 PC to verify that Site to Site communication is operational but the Internet cannot be accessed.

Log in to Guacamole (10.2.1.20X:8080/guacamole, where X is your POD number) with the credentials given below and click on the PODX-Site30PC option.

Alternatively, you can RDP to 10.2.1.16X (where X is your POD number) from the Jumphost. RDP to the Site 30 PC will only work from the Jumphost

| Connection Method | Username | Password |
|-------------------|--------------------|------------|
| Guacamole | sdwanpod | C1sco12345 |
| RDP | swatsdwanlab\sdwan | C1sco12345 |



This section displays three recent connections:

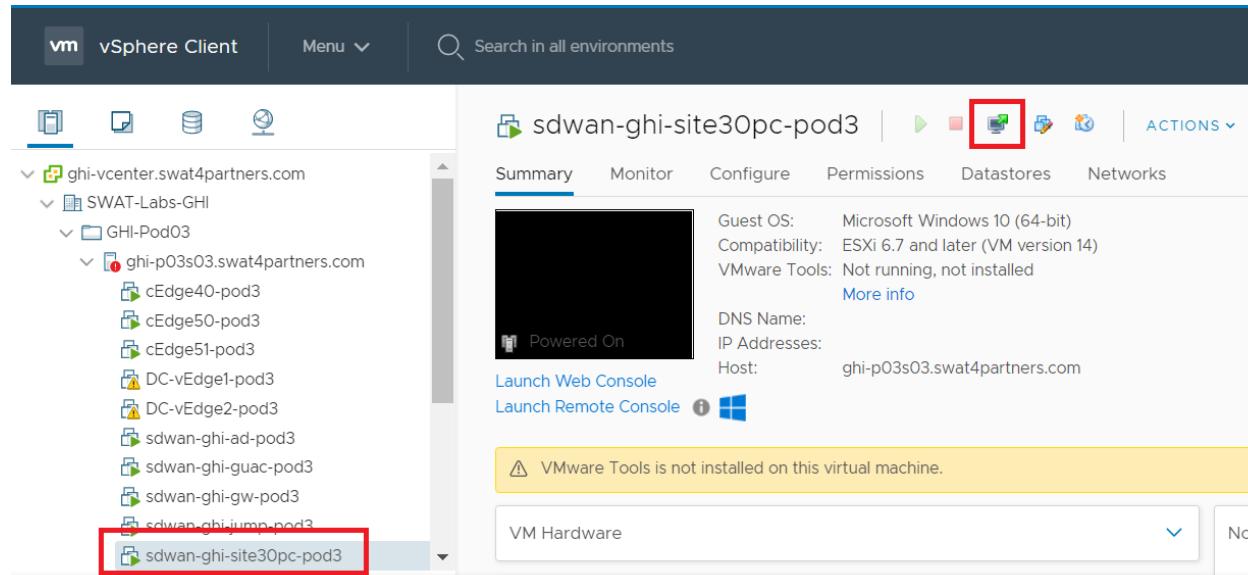
- POD3-Site30PC**: A blue square with a white circular progress indicator in the center, set against a light green background.
- POD3-AD**: A screenshot of a Windows Server Manager interface showing the "Configure this local server" wizard.
- POD3-Jumphost**: A solid black square.

This section displays a list of all connections:

- POD3-AD**
- POD3-Jumphost**
- POD3-Site30PC** (highlighted with a red border)

A search bar labeled "Filter" is located at the top right of the list area.

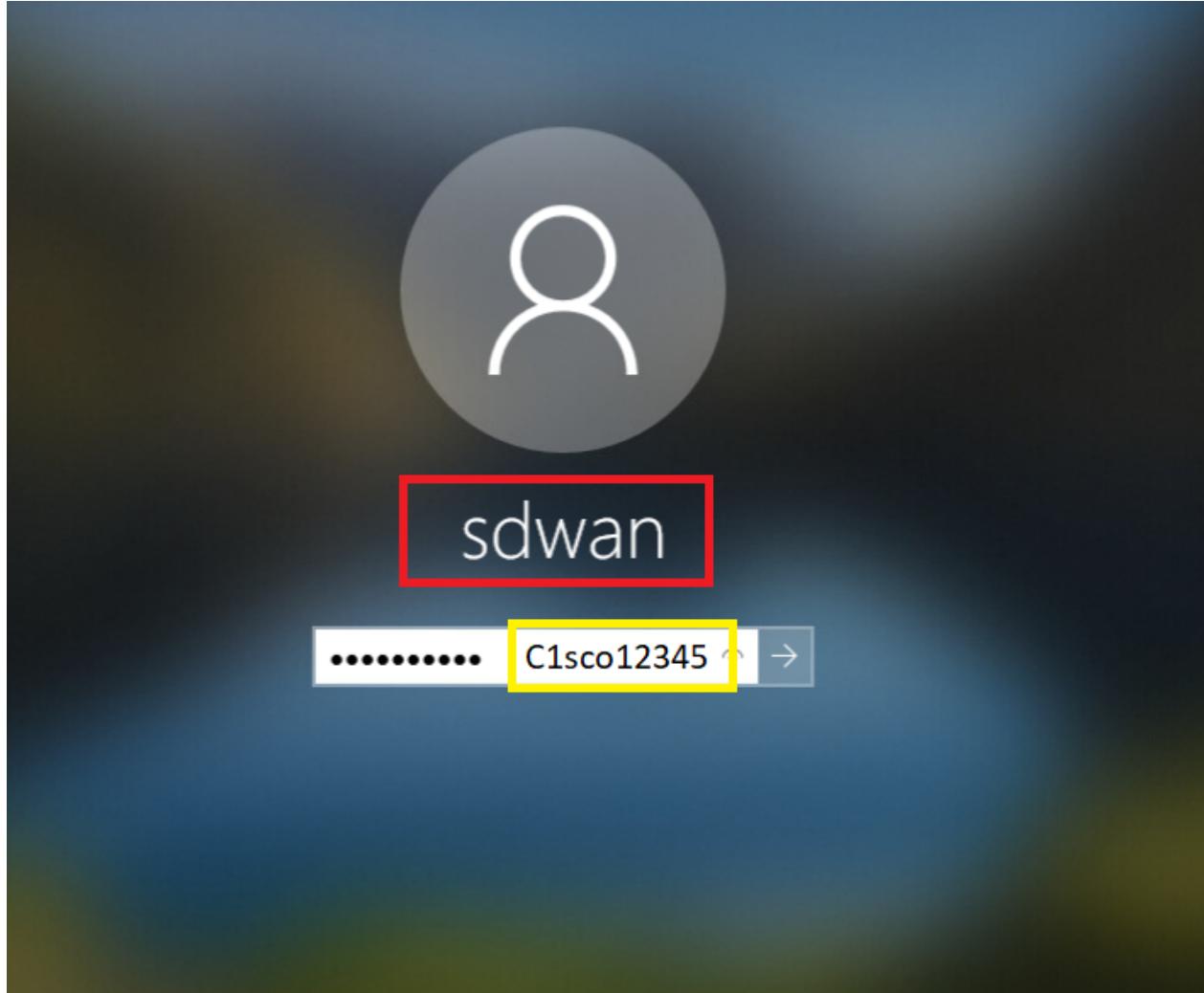
vCenter (accessible via the bookmark or 10.2.1.50/ui and the credentials provided for your POD) can also be used to console to the Site30 PC



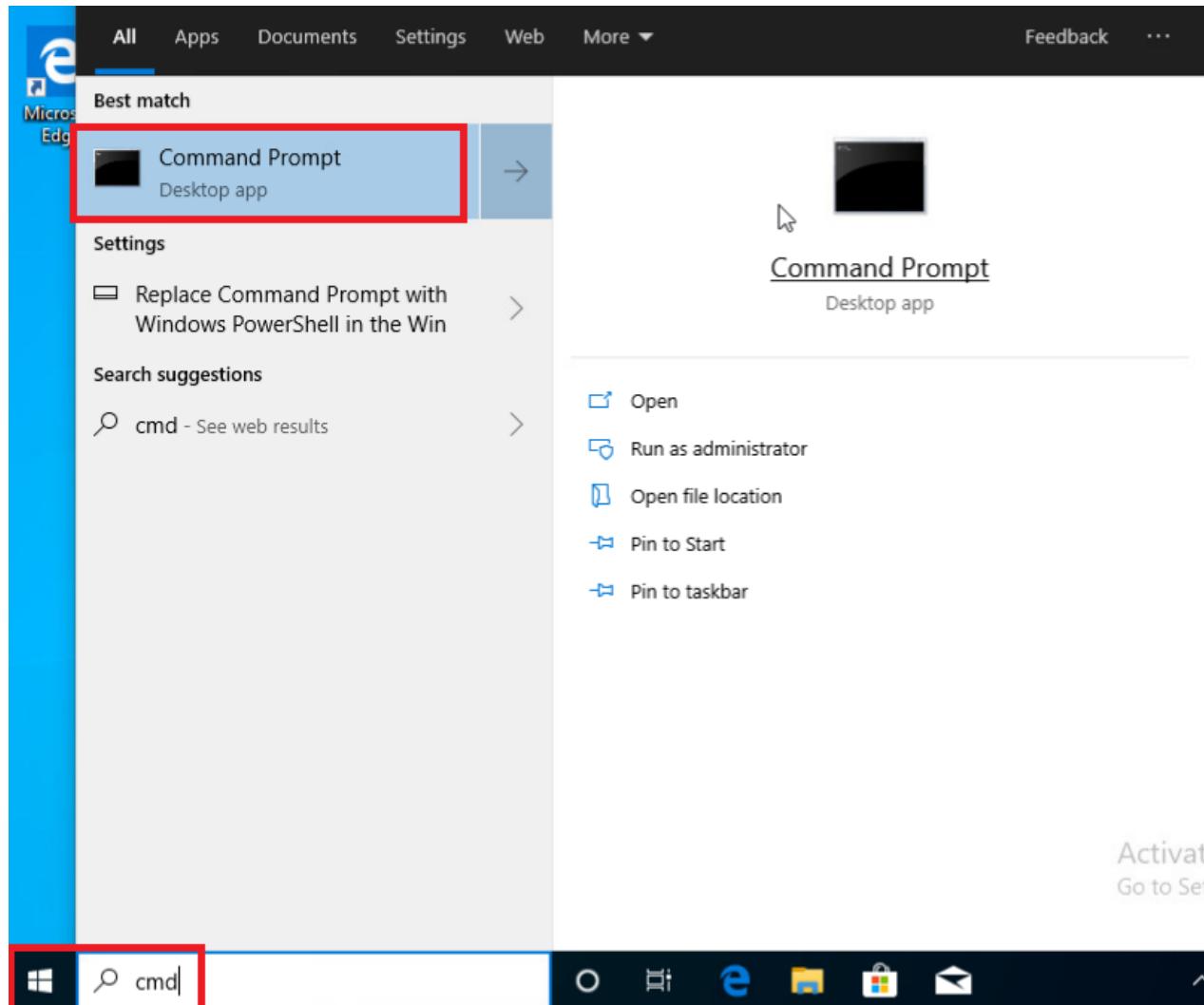
The screenshot shows the vSphere Client interface. In the left sidebar, under the 'SWAT-Labs-GHI' folder, the 'GHI-Pod03' folder is expanded, showing several sub-entities including 'ghi-p03s03.swat4partners.com' which contains multiple network components like 'cEdge40-pod3', 'cEdge50-pod3', etc. A red box highlights the 'ghi-p03s03.swat4partners.com' entry. In the main content area, the 'sdwan-ghi-site30pc-pod3' virtual machine is selected. Its summary card shows it is 'Powered On'. The 'Actions' bar at the top right has a 'Launch Web Console' button highlighted with a red box. Below the summary card, a yellow warning box states 'VMware Tools is not installed on this virtual machine.' At the bottom of the screen, there are tabs for 'VM Hardware' and 'Notes'.

2. Depending on the connection method, you may need to enter credentials again to log in to the Site 30 PC. Please enter the credentials shown below, if prompted

| Connection Method | Username | Password |
|-------------------|--------------------|--------------|
| Guacamole | Not Required | Not Required |
| RDP | swatsdwanlab\sdwan | C1sco12345 |
| vCenter | swatsdwanlab\sdwan | C1sco12345 |



3. Click on **Start** and type **cmd**. Click on the *Command Prompt* App that pops up in the search results



4. Type `ipconfig` and Hit Enter. Also, type `ping 10.0.0.1` and Hit Enter. The pings should work. On typing `ping 8.8.8.8`, the pings should fail indicating that there is no Internet connectivity

Command Prompt

```
Microsoft Windows [Version 10.0.18362.239]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\sdwan>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . : swatsdwanlab.com
  Link-local IPv6 Address . . . . . : fe80::a48b:47fb:dce:120a%5
    IPv4 Address. . . . . : 10.30.10.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.30.10.2

C:\Users\sdwan>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Request timed out.
Reply from 10.0.0.1: bytes=32 time<1ms TTL=253
Reply from 10.0.0.1: bytes=32 time<1ms TTL=253
Reply from 10.0.0.1: bytes=32 time<1ms TTL=253

Ping statistics for 10.0.0.1:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\sdwan>
```

```
C:\Users\sdwan>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 10.30.10.2: Destination net unreachable.

Ping statistics for 8.8.8.8:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\sdwan>ping www.cisco.com
Ping request could not find host www.cisco.com. Please check the name and try again.

C:\Users\sdwan>
```

```
ipconfig  
ping 10.0.0.1  
ping 8.8.8.8
```

5. Go to the vManage GUI and navigate to **Configuration => Templates**

The screenshot shows the Cisco vManage Main Dashboard. On the left, a sidebar menu is open under the 'Configuration' tab, with 'Templates' highlighted by a red box. The main dashboard area displays several key metrics and status indicators:

- Smart - 2**: Shows 2 uplinks.
- WAN Edge - 8**: Shows 8 uplinks.
- vBond - 1**: Shows 1 uplink.
- Site Health (Total 5)**: Status breakdown:
 - Full WAN Connectivity: 4 (green)
 - Partial WAN Connectivity: 1 (yellow)
 - No WAN Connectivity: 0 (red)
- WAN Edge Health (Total 8)**: Status breakdown:
 - Normal: 8 (green circle)
 - Warning: 0 (grey circle)
- Application-Aware Routing**: Shows tunnel endpoints: vEdge30:public-internet <--> vEdge21:public-internet with an average latency of 0 ms.

6. Click on the **Feature** tab and locate the *vEdge30-vpn0* Feature Template. Click on the three dots next to it and choose to **Edit**

CONFIGURATION | TEMPLATES

Device **Feature**

Add Template

Template Type Non-Default Search Options

Total Rows: 3 of 41

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------|---------------------------------|--------------------|--------------|------------------|------------------|------------|-------------------------|---------|
| vEdge30_MPLS | MPLS interface for the Site... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 18 Jun 2020 11:23:54... | ... |
| vEdge30_INET | INET interface for the Site3... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 18 Jun 2020 11:24:34... | ... |
| vEdge30-vpn0 | VPN0 for the Site30 INET a... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 18 Jun 2020 11:25:15... | ... |

View
Edit ...
Change Device Models
Delete
Copy

7. Scroll to the **DNS** section and update the **Primary DNS Address (IPv4)** to 8.8.8.8 and the **Secondary DNS Address (IPv4)** to 4.2.2.2

DNS

IPv4 **IPv6**

Primary DNS Address (IPv4)
8.8.8.8

Secondary DNS Address (IPv4)
4.2.2.2

+ New Host Mapping

8. Locate the **IPv4 Route** section and click on the pencil icon to edit the **0.0.0.0/0** route

IPv4 ROUTE

New IPv4 Route

| Optional | Prefix | Gateway | Selected Gateway Configuration | Action |
|--------------------------|--|----------|--------------------------------|--------|
| <input type="checkbox"/> | <input checked="" type="radio"/> 0.0.0.0/0 | Next Hop | 2 | |

9. Click on **2 Next Hop** and remove the *vpn0_mpls_next_hop* option by clicking on the red minus icon

Update IPv4 Route

Prefix Mark as Optional Row [i](#)

Gateway Next Hop Null 0 VPN

Next Hop [2 Next Hop](#)

[Save Changes](#) [Cancel](#)

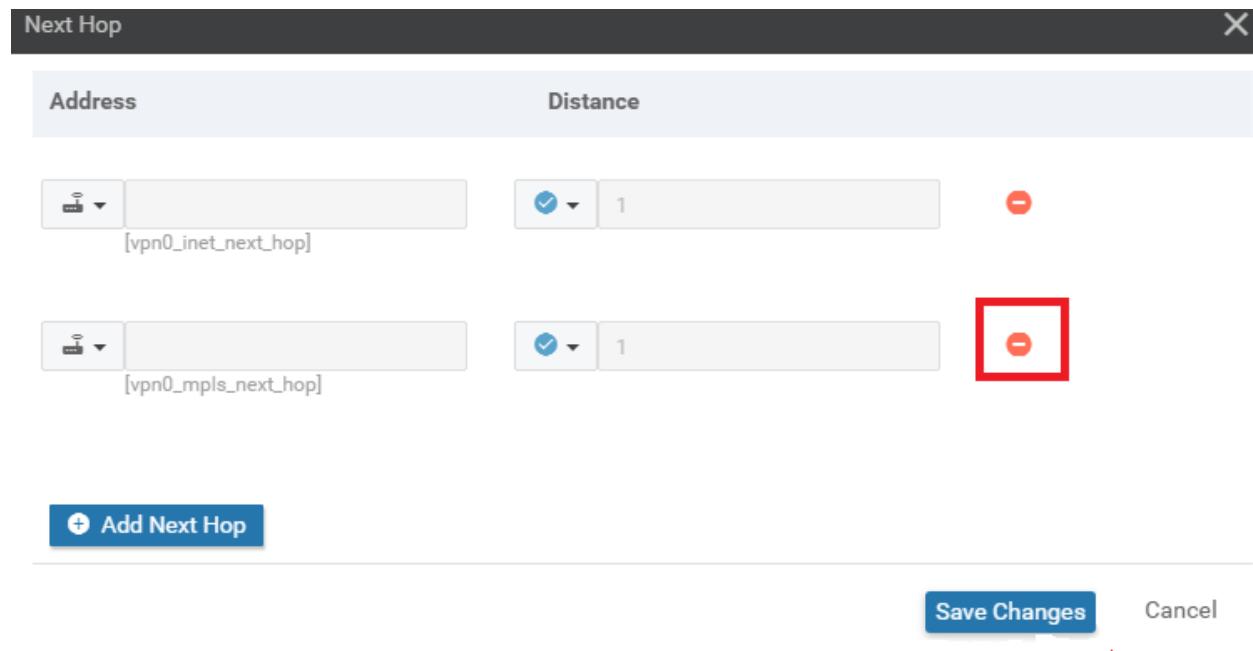


Next Hop

| Address | Distance |
|---|---|
| <input type="text" value="vpn0_inet_next_hop"/> | <input checked="" type="radio"/> 1 - |
| <input type="text" value="vpn0_mpls_next_hop"/> | <input checked="" type="radio"/> 1 - |

[+ Add Next Hop](#)

[Save Changes](#) [Cancel](#)



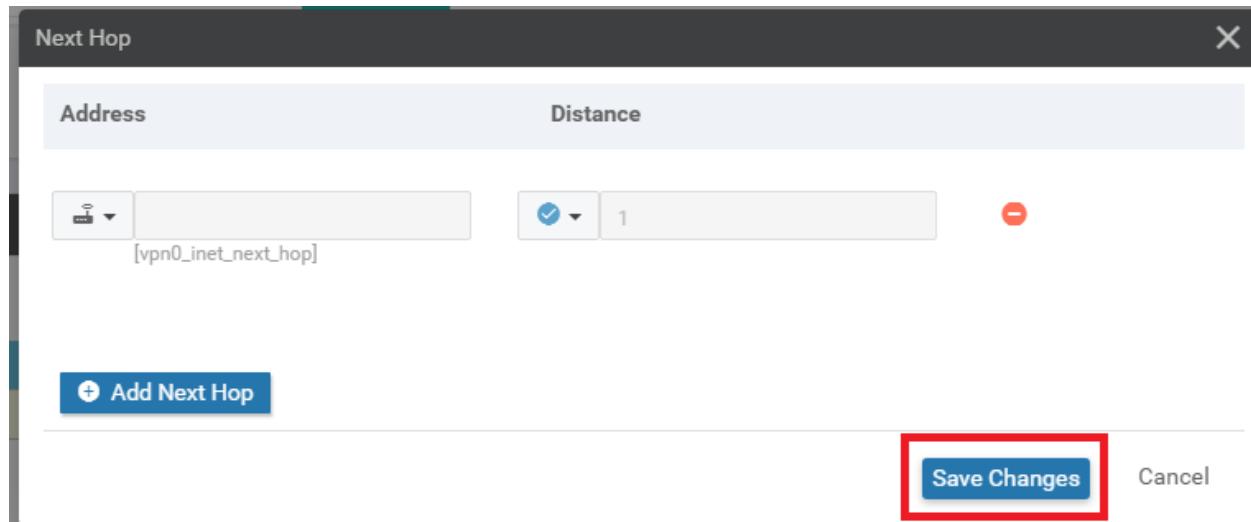
10. Click on **Save Changes**

Next Hop

| Address | Distance |
|---|--|
| <input type="text"/> [vpn0_inet_next_hop] | <input checked="" type="checkbox"/> 1 <input type="button"/> |

Add Next Hop

Save Changes **Cancel**

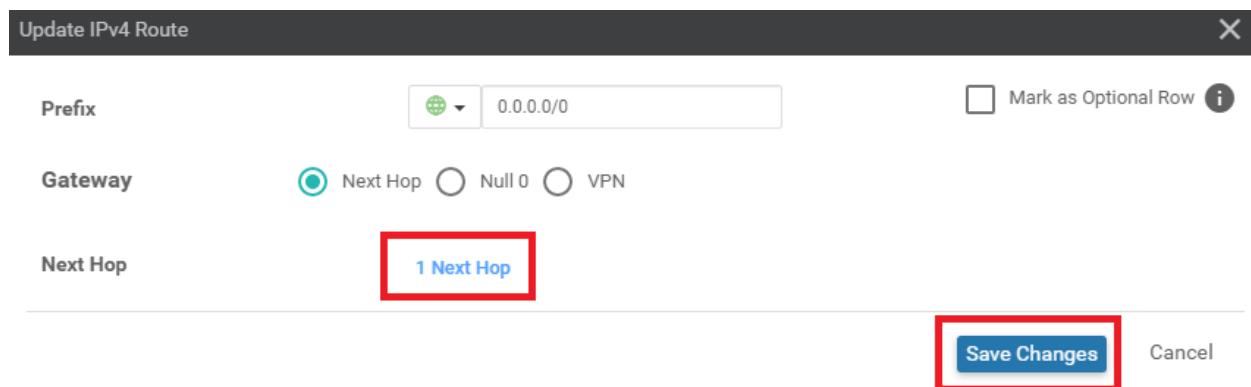


11. Ensure that the **Update IPv4 Route** window shows **1 Next Hop** and click on **Save Changes**

Update IPv4 Route

| | | |
|----------|--|---|
| Prefix | <input type="text"/> 0.0.0.0/0 | <input type="checkbox"/> Mark as Optional Row  |
| Gateway | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN | |
| Next Hop | 1 Next Hop | |

Save Changes **Cancel**



12. Click on **New IPv4 Route** and enter a Prefix of 192.0.2.0/24. Click on **Add Next Hop**

IPv4 ROUTE

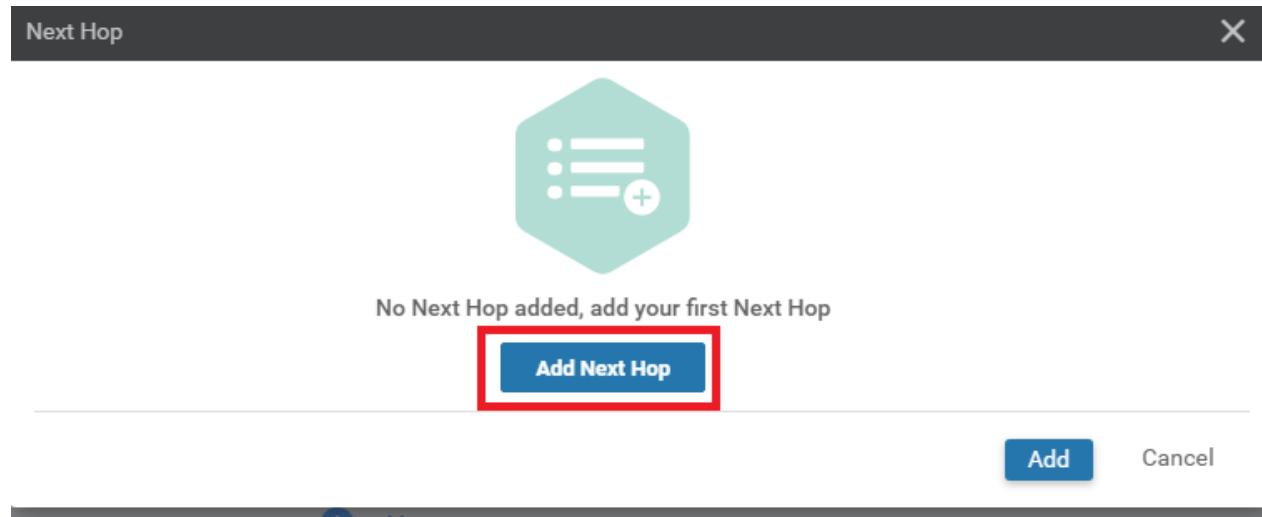
New IPv4 Route

Prefix: 192.0.2.0/24

Gateway: Next Hop

Next Hop: **Add Next Hop**

13. Click on **Add Next Hop** again



14. Enter a Global value of 192.0.2.13 in the **Address** field and click on **Add**

Next Hop

| Address | Distance |
|---|--------------------------------|
| <input type="text" value="192.0.2.13"/> | <input type="text" value="1"/> |

Add Next Hop

Add Cancel

15. Click on **Add** again to add the route

IPv4 ROUTE

New IPv4 Route

| | | |
|----------|--|---|
| Prefix | <input type="text" value="192.0.2.0/24"/> | <input type="checkbox"/> Mark as Optional Row |
| Gateway | <input checked="" type="radio"/> Next Hop <input type="radio"/> Null 0 <input type="radio"/> VPN | |
| Next Hop | 1 Next Hop | |

Add Cancel

16. We will be adding 2 more routes. Repeat steps 12 to 15 for the routes enumerated below, using the images as reference. These routes and the ones in the previous steps are being added to maintain BFD sessions on the MPLS link in our SD-WAN network and to ensure that the TLOC extension configured before works as expected (hence the 192.168.26.0/24 route shown below). The 192.0.2.0/24 and 192.1.2.0/24 routes being added correspond to our MPLS subnets across the SD-WAN Network

| Field | Global or Device Specific (Drop Down) | Value |
|------------------------|---------------------------------------|--------------|
| Prefix | Global | 192.1.2.0/24 |
| Add Next Hop - Address | Global | 192.0.2.13 |

| Field | Global or Device Specific (Drop Down) | Value |
|------------------------|---------------------------------------|-----------------|
| Prefix | Global | 192.168.26.0/24 |
| Add Next Hop - Address | Global | 192.0.2.13 |

IPv4 ROUTE

New IPv4 Route

Prefix: 192.1.2.0/24

Gateway: Next Hop

Next Hop: **Add Next Hop**

Next Hop

| | |
|---------------------|-------------|
| Address: 192.0.2.13 | Distance: 1 |
| Add Next Hop | Add |

17. Make sure there are 4 routes created, as shown below and click on **Update**

The screenshot shows the Cisco vManage interface with two tabs: "IPv4 ROUTE" and "IPv6 ROUTE". The "IPv4 ROUTE" tab is active, displaying a table with columns: "Optional", "Prefix", "Gateway", "Selected Gateway Configuration", and "Action". The table contains four entries, each with a checkbox in the "Optional" column and a green globe icon in the "Prefix" column. The "Gateway" column shows "Next Hop" and the value "1" for all entries. The "Action" column contains icons for edit, delete, and refresh. A red box highlights the entire table area. Below the table, there is a progress bar.

IPv4 ROUTE

New IPv4 Route

| Optional | Prefix | Gateway | Selected Gateway Configuration | Action |
|--------------------------|-----------------|----------|--------------------------------|--------|
| <input type="checkbox"/> | 0.0.0.0/0 | Next Hop | 1 | |
| <input type="checkbox"/> | 192.0.2.0/24 | Next Hop | 1 | |
| <input type="checkbox"/> | 192.1.2.0/24 | Next Hop | 1 | |
| <input type="checkbox"/> | 192.168.26.0/24 | Next Hop | 1 | |

IPv6 ROUTE

Update **Cancel**

18. Click on **Next** and then **Configure Devices**. You can view the side by side configuration difference, if required. Notice that the default route pointing to the MPLS next hop is being removed and 3 routes are being added in place of it

The screenshot shows the Cisco vManage interface with the "CONFIGURATION | TEMPLATES" tab selected. On the left, a sidebar shows "Device Template" and "vEdge30_dev_temp" with a total of 1 device. The main pane displays a configuration diff between "vEdge30_dev_temp" and "vEdge3010.255.255.31". The configuration code is shown in two columns, with changes highlighted in yellow. A yellow box at the top right indicates: "'Configure' action will be applied to 1 device(s) attached to 1 device template(s.)". The "Configure Devices" button is highlighted with a red box at the bottom right.

Cisco vManage

CONFIGURATION | TEMPLATES

Device Template Total 1

vEdge30_dev_temp

Device list (Total: 1 devices)

Filter/Search

17026153-f09e-be4b-6dce-482fce43ash2
vEdge3010.255.255.31

'Configure' action will be applied to 1 device(s) attached to 1 device template(s.)

```

84 no allow-service stun
85 allow-service https
86 !
87 no shutdown
88 !
89 ip route 0.0.0.0/0 100.100.100.1
90 ip route 0.0.0.0/0 192.0.2.13
91 !
92 vpn 10
93 dns 10.2.1.5 primary
94 dns 10.2.1.6 secondary
95 interface ge0/2
96 ip address 10.30.10.2/24
97 no shutdown
98 !
99 omp
100 advertise connected
101 advertise static
102 !
103 !
104 vpn 20

```

```

84 no allow-service stun
85 allow-service https
86 !
87 no shutdown
88 !
89 ip route 0.0.0.0/0 100.100.100.1
90 ip route 192.0.2.0/24 192.0.2.13
91 ip route 192.1.2.0/24 192.0.2.13
92 ip route 192.168.26.0/24 192.0.2.13
93 !
94 vpn 10
95 dns 10.2.1.5 primary
96 dns 10.2.1.6 secondary
97 interface ge0/2
98 ip address 10.30.10.2/24
99 no shutdown
100 !
101 omp
102 advertise connected
103 advertise static
104 !
105 !
106 vpn 20

```

Configure Device Rollback Timer

Back **Configure Devices** **Cancel**

19. Navigate to the **Configuration => Templates => Feature tab** and click on the three dots next to *vedge30_MPLS*.
Click on **Edit**

CONFIGURATION | TEMPLATES

Device **Feature**

+ Add Template

Template Type Non-Default | Search Options | Total Rows: 7 of 41

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
|------------------------|--------------------------------|---------------------|--------------|------------------|------------------|------------|------------------------------|
| cedge-vpn0-int-dual... | cEdge VPN 0 Interface Tem... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 21 Jun 2020 4:42:58 ... |
| DC-vEdge_MPLS | MPLS interface for the DC-... | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | |
| DCvEdge-vpn0 | VPN0 for the DC-vEdges IN... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | |
| cedge-vpn0-int-dual... | cEdge VPN 0 Interface Tem... | Cisco VPN Interface | CSR1000v | 0 | 0 | admin | |
| vedge21_mpls_bgp_t... | BGP Peering Template for ... | BGP | vEdge Cloud | 2 | 2 | admin | |
| vEdge30_MPLS | MPLS interface for the Site... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 18 Jun 2020 11:23:54 ... |
| vEdge30-vpn0 | VPN0 for the Site30 INET a... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 02 Jul 2020 9:13:07 P... *** |

20. Under Tunnel, set the **Control Connection** to *Off* and click on **Update**. Click on **Next** and then **Configure Devices**

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > **VPN Interface Ethernet**

Basic Configuration **Tunnel** NAT VRRP ACL/QoS ARP 802.1X Advanced

| | |
|-------------------------------|---|
| Groups | <input checked="" type="checkbox"/> |
| Border | <input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off |
| Control Connection | <input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off |
| Maximum Control Connections | <input checked="" type="checkbox"/> |
| vBond As Stun Server | <input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off |
| Exclude Controller Group List | <input checked="" type="checkbox"/> |
| vManage Connection Preference | <input checked="" type="checkbox"/> 5 |
| Port Hop | <input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off |

Update **Cancel**

21. Back at the **Configuration => Templates => Feature tab**, locate the **vEdge30_INET** Feature Template. Click on the three dots next to it and choose to **Edit**. Set **NAT** to a Global value of *On* and click on **Update**. Click **Next** and **Configure Devices** on the corresponding screens, viewing the side by side configuration difference if required

Cisco vManage

CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type Non-Default Search Options Total Rows: 4 of 41

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
|---------------|---|--------------------|--------------|------------------|------------------|------------|--------------------------|
| DCvEdge-vpn0 | VPN0 for the DC-vEdges INET | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 18 Jun 2020 9:33:30 ... |
| DC-vEdge_INET | INET interface for the DC-v... ...edges | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 18 Jun 2020 9:41:03 ... |
| vEdge30-vpn0 | VPN0 for the Site30 INET a... ...edges | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 02 Jul 2020 9:13:07 P... |
| vEdge30_INET | INET interface for the Site30 INET a... ...edges | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 18 Jun 2020 11:24:34... |

View
Edit
Change Device Models
Delete
Copy

Cisco vManage

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > VPN Interface Ethernet

NAT Tunnel VRRP ACL/QoS ARP 802.1X Advanced

NAT

IPv4 IPv6

NAT

On Off

Refresh Mode

Log NAT flow creations or deletions

UDP Timeout

TCP Timeout

Update Cancel

```

40 advertise connected
41 advertise static
42 !
43 security
44 ipsec
45 authentication-type sha1-hmac ah-sha1-hmac
46 !
47 !
48 vpn 0
49 dns 4.2.2.2 secondary
50 dns 8.8.8.8 primary
51 interface ge0/0
52 ip address 100.100.100.30/24
53
54 !
55 tunnel-interface
56 encapsulation ipsec
57 color public-internet
58 allow-service all
59 no allow-service bgp
60 allow-service dhcp
61 allow-service dns
62 allow-service icmp

```

Configure Device Rollback Timer

Back **Configure Devices** **Cancel**

22. We will now add a VPN 10 Template for vEdge30 since there will be settings applicable just to this Site for Umbrella connectivity. On **Configuration => Templates => Feature tab** locate the *vedge-vpn10* Template. Click on the three dots next to it and choose **Copy**

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|----------------------|-------------------------------|---------------------|--------------|------------------|------------------|------------|-------------------------|---------|
| cedge-vpn10 | VPN 10 Template for the c... | Cisco VPN | CSR1000v | 2 | 3 | admin | 19 Jun 2020 2:18:57 ... | ... |
| cedge-vpn10-int | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 0 | 0 | admin | 19 Jun 2020 12:55:29... | ... |
| vedge-vpn10 | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 4 | 5 | admin | 19 Jun 2020 12:46:21... | ... |
| cedge-vpn10-int-vrrp | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | | |
| vedge-vpn10-int | VPN 10 Interface Template ... | WAN Edge Interface | vEdge Cloud | 4 | 5 | admin | | |
| cedge-vpn10-int-qos | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | | |

23. Rename the Template to *vedge30-vpn10* and update the description accordingly. Click on **Copy**

Template Copy

Template Name
vedge30-vpn10

Description
VPN 10 Template for vEdge30

Copy **Cancel**

24. Click on the three dots next to the newly copied template and choose to **Edit**

Cisco vManage

CONFIGURATION | TEMPLATES

Device **Feature**

Add Template

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | ... |
|----------------------|-------------------------------|---------------------|--------------|------------------|------------------|------------|--------------------------|-----|
| cedge-vpn10-int | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 0 | 0 | admin | 19 Jun 2020 12:55:29... | ... |
| vedge-vpn10-int | VPN 10 Interface Template ... | WAN Edge Interface | vEdge Cloud | 4 | 5 | admin | 19 Jun 2020 12:47:49... | ... |
| cedge-vpn10-int-vrrp | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 19 Jun 2020 2:00:08 ... | ... |
| vedge30-vpn10 | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 0 | 0 | admin | 02 Jul 2020 9:26:49 P... | ... |
| cedge-vpn10-int-qos | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | | |
| vedge-vpn10 | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 4 | 5 | admin | | |
| cedge-vpn10 | VPN 10 Template for the c... | Cisco VPN | CSR1000v | 2 | 3 | admin | | |

Total Rows: 7 of 42

25. Update the **DNS entries** to **8.8.8.8** for the **Primary DNS Address (IPv4)** and **4.2.2.2** for the **Secondary DNS Address (IPv4)**. Click on **Update**.

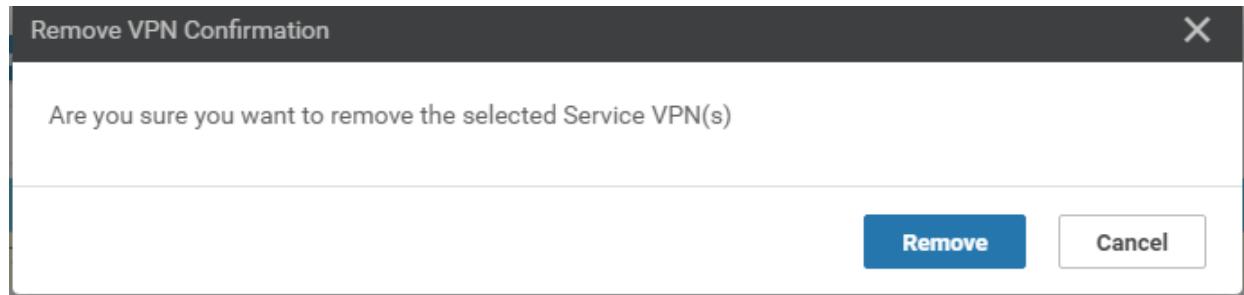


26. On the vManage GUI, navigate to **Configuration => Templates => Device Tab** and locate the **vEdge30_dev_temp** Template. Click on the three dots next to it and choose to **Edit** the template

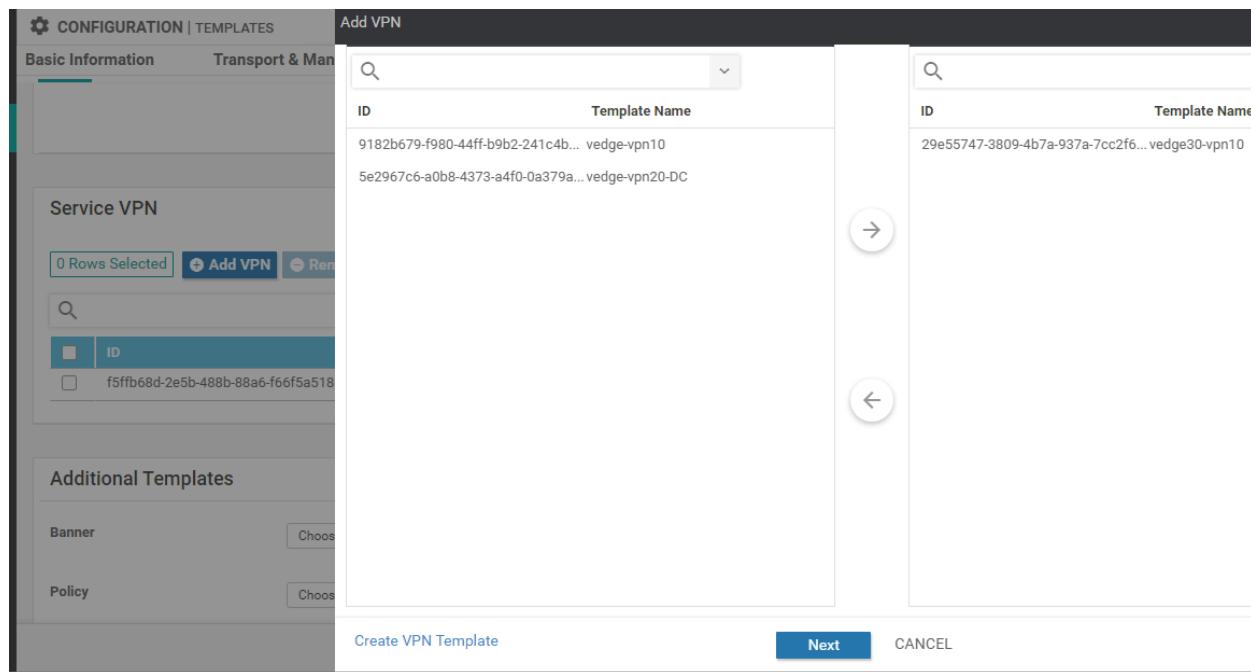
| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status |
|---------------------------|---------------------|---------|--------------|-------------------|------------------|------------|----------------------|-----------------|
| cEdge-single-uplink | Single Uplink cE... | Feature | CSR1000v | 17 | 2 | admin | 19 Jun 2020 2:01:... | In Sync |
| vEdge30_dev_temp | Device template ... | Feature | vEdge Cloud | 15 | 1 | admin | 19 Jun 2020 1:21:... | In Sync |
| vEdge_Site20_dev_temp_nat | Device template ... | Feature | vEdge Cloud | 17 | 1 | admin | 19 Jun 2020 3:53:... | In Sync |
| cedge_dualuplink_devtemp | cedge Device Te... | Feature | CSR1000v | 20 | 1 | admin | 21 Jun 2020 5:57:... | In Sync |
| vSmart-dev-temp | Device Template... | Feature | vSmart | 9 | 2 | admin | 19 Jun 2020 12:1... | In Sync |
| vEdge_Site20_dev_temp | Device template ... | Feature | vEdge Cloud | 17 | 1 | admin | 19 Jun 2020 3:46:... | In Sync |
| DCvEdge_dev_temp | Device template ... | Feature | vEdge Cloud | 16 | 2 | admin | 21 Jun 2020 4:07:... | In Sync |

27. In the **Service VPN** section, select the **vedge-vpn10** Template Name entry and click on **Remove VPN**. Confirm the removal

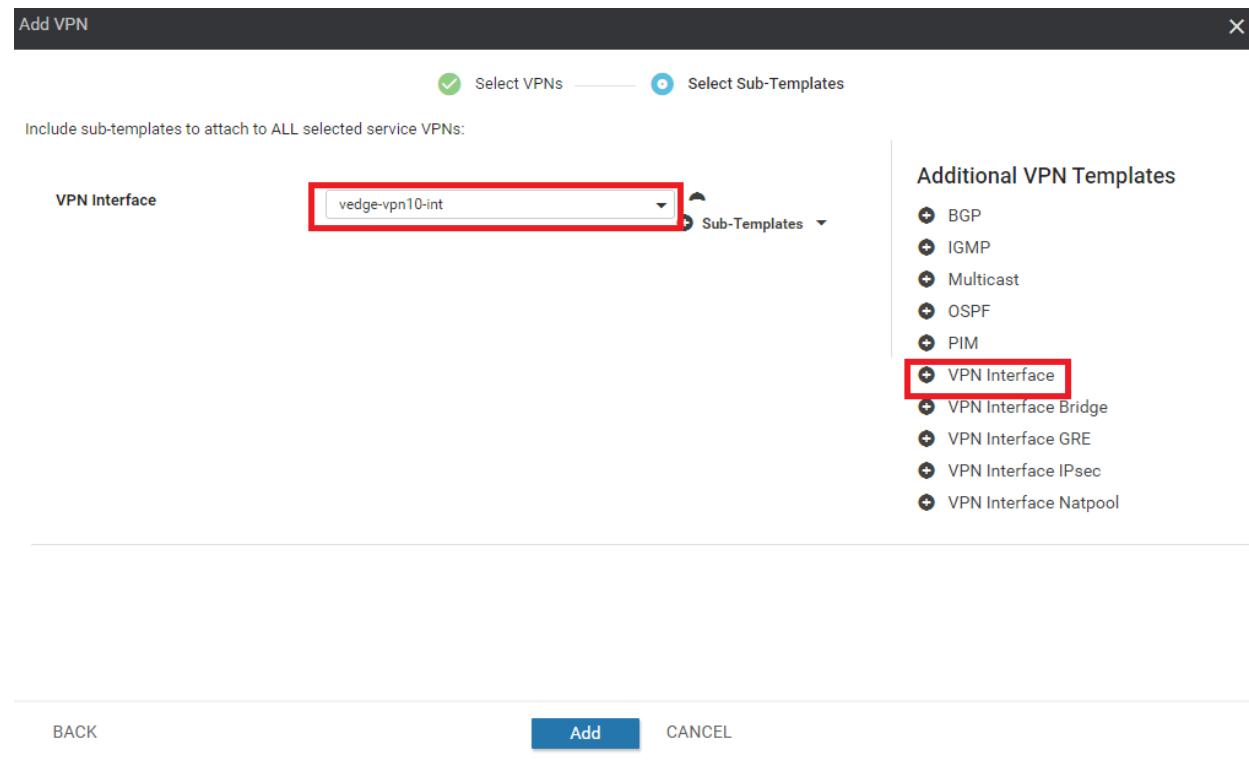
| ID | Template Name | Sub-Templates |
|--|---------------|---------------|
| <input checked="" type="checkbox"/> 9182b679-f980-44ff-b9b2-241c4b967ad0 | vedge-vpn10 | VPN Interface |
| <input type="checkbox"/> f5ffb68d-2e5b-488b-88a6-f66f5a518cee | vedge-vpn20 | VPN Interface |



28. Click on **Add VPN** under Service VPN and move the *vedge30-vpn10* Template to the right hand side. Click on **Next**



29. Under **Additional VPN Templates** click on **VPN Interface** and select *vedge-vpn10-int* in the **VPN Interface** drop-down. Click on **Add**



30. Back at the Device Template, click on **Update** followed by **Next** and **Configure Devices**

Service VPN

0 Rows Selected | + Add VPN | - Remove VPN

| ID | Template Name | Sub-Templates |
|--------------------------------------|---------------|---------------|
| f5ffb68d-2e5b-488b-88a6-f66f5a518cee | vedge-vpn20 | VPN Interface |
| 29e55747-3809-4b7a-937a-7cc2f602c576 | vedge30-vpn10 | VPN Interface |

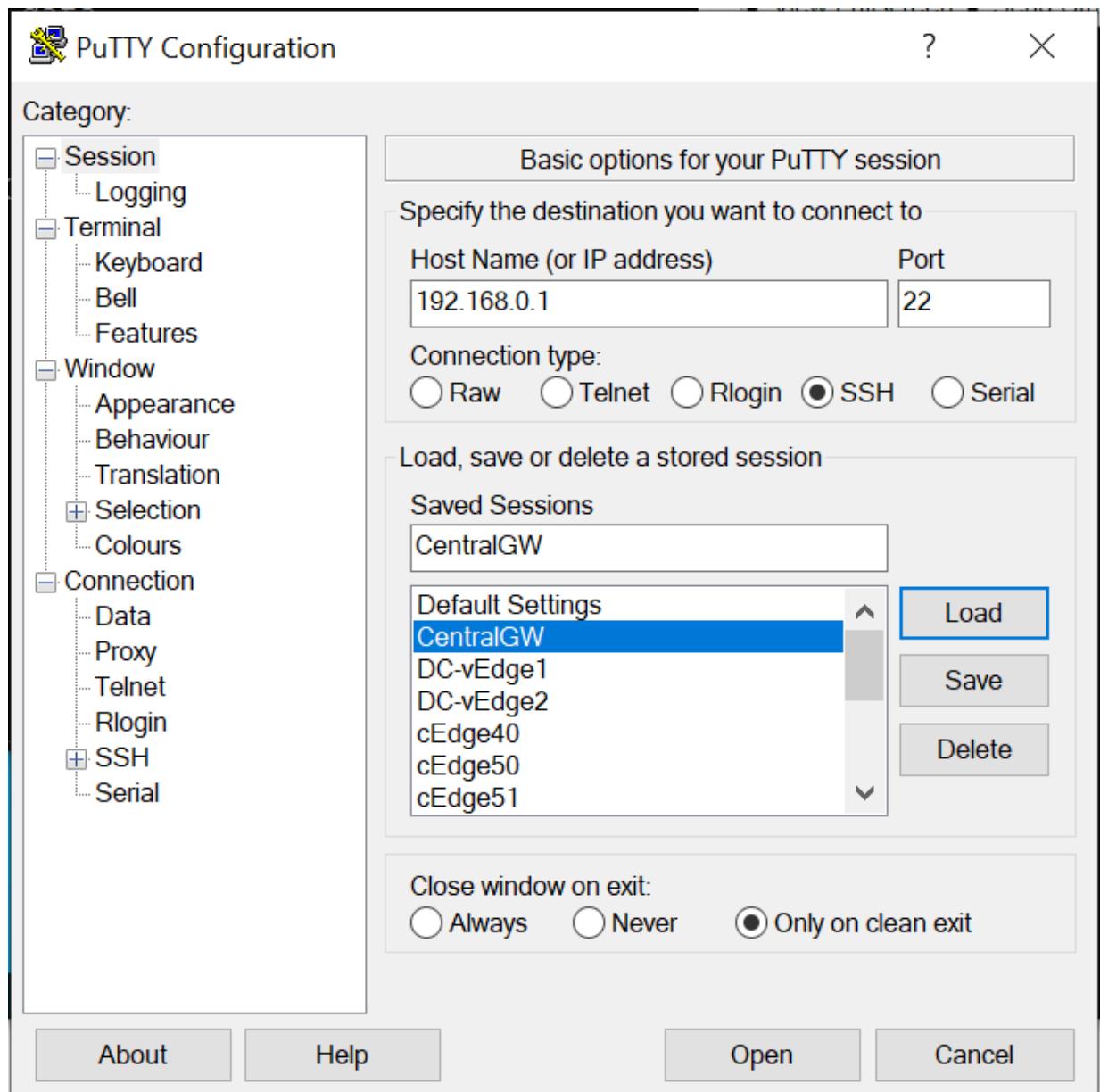
Additional Templates

Banner: Choose...

Update Cancel

31. Log in to the CentralGW via the saved Putty session (or SSH to 192.168.0.1) using the credentials below. Enter `config t` followed by `interface gig 2.31` and then `ip nat inside` to allow the VPN 10 subnet at Site 30 to be NAT'd. Type `do wr` to save the configuration done on the CentralGW

| | |
|----------|----------|
| Username | Password |
| admin | admin |



```
CentralGW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CentralGW(config)#int gig 2.31
CentralGW(config-subif)#ip nat inside
CentralGW(config-subif) #
```

```
config t
interface gig 2.31
ip nat inside
do wr
```

This completes the pre-work that we needed to do at Site 30.

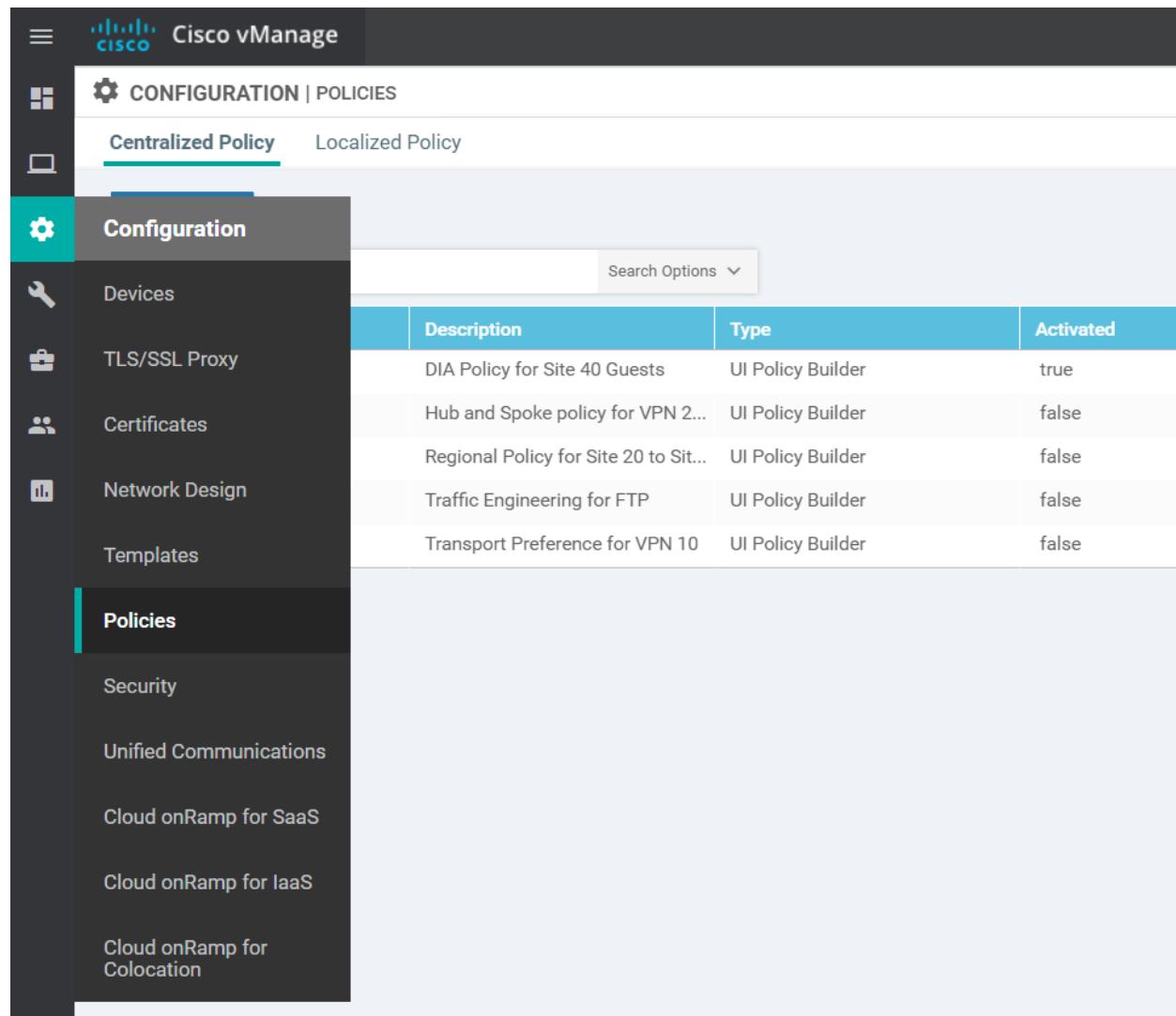
Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - [API Keys and AD Configuration](#)
 - [DC Configuration Download](#)
 - [AD Connectors](#)
 - [Roaming Computer Configuration](#)
- [Building a DNS Policy](#)
- [Setting up IPSEC Tunnels](#)
- [Configuring a Firewall Policy](#)
- [Configuring a Web Policy](#)

Enabling Site 30 for DIA

To facilitate communication to the Internet from Site 30, we will be enabling DIA at Site 30 for VPN 10.

1. On the vManage GUI, go to **Configuration => Policies**



The screenshot shows the Cisco vManage interface under the Configuration tab. The left sidebar has a 'Centralized Policy' section with 'Configuration' selected, followed by 'Devices', 'TLS/SSL Proxy', 'Certificates', 'Network Design', and 'Templates'. Below these are sections for 'Policies' like 'Security', 'Unified Communications', 'Cloud onRamp for SaaS', 'Cloud onRamp for IaaS', and 'Cloud onRamp for Colocation'. The main content area displays a table of policies:

| | Description | Type | Activated |
|--|---------------------------------------|-------------------|-----------|
| | DIA Policy for Site 40 Guests | UI Policy Builder | true |
| | Hub and Spoke policy for VPN 2... | UI Policy Builder | false |
| | Regional Policy for Site 20 to Sit... | UI Policy Builder | false |
| | Traffic Engineering for FTP | UI Policy Builder | false |
| | Transport Preference for VPN 10 | UI Policy Builder | false |

2. Click on **Custom Options** in the top right-hand corner and click on **Traffic Policy**

The screenshot shows a table of policy versions. The first row has 'Updated By' as 'admin' and 'Policy Version' as '06212020'. The second row has 'Updated By' as 'admin' and 'Policy Version' as '06212020T112433859'. A red box highlights the 'Traffic Policy' tab in the top navigation bar. Another red box highlights the 'Traffic Policy' link in the dropdown menu.

| Updated By | Policy Version |
|------------|--------------------|
| admin | 06212020 |
| admin | 06212020T112433859 |

3. Click on the **Traffic Data** tab and locate the *Guest-DIA* Policy. Click on the three dots next to it and choose to **Edit**

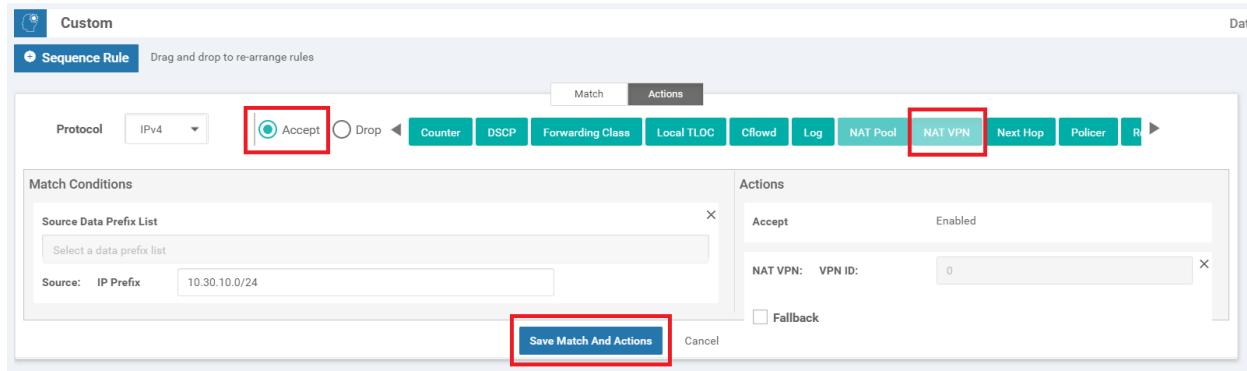
The screenshot shows the 'Traffic Data' tab selected. It lists two policies: 'ftp-mpls' and 'Guest-DIA'. The 'Guest-DIA' row has three dots next to it, which are highlighted with a red box. A context menu is open over the row, with the 'Edit' option highlighted by a red box.

| Name | Type | Description | Reference Count | Updated By | Last Updated |
|-----------|------|----------------------|-----------------|------------|-----------------------------|
| ftp-mpls | Data | FTP via MPLS | 1 | admin | 21 Jun 2020 10:33:44 AM PDT |
| Guest-DIA | Data | Guest DIA at Site 40 | 1 | admin | 21 Jun 2020 11:00:31 AM PDT |

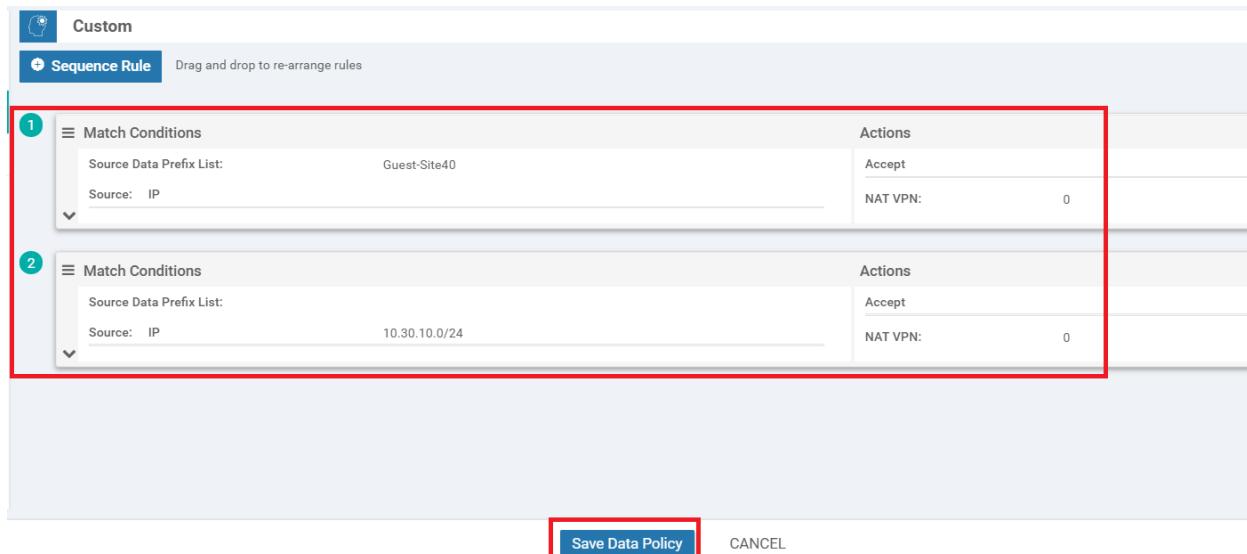
4. Update the **Description** to *Guest DIA at Site 40 and Site 30* and make sure you're on the **Custom** Sequence Type. Click on **Sequence Rule** to add a new rule and select **Source Data Prefix** under Match (might need to use the scroll buttons so that the option becomes visible). Enter a *Source: IP Prefix* of *10.30.10.0/24* and click on **Actions**

The screenshot shows the 'Sequence Rule' configuration dialog. Step 1 highlights the 'Description' field with the value 'Guest DIA at Site 40 and Site 30'. Step 2 highlights the 'Sequence Type' dropdown set to 'Custom'. Step 3 highlights the 'Sequence Rule' button. Step 4 highlights the 'Source Data Prefix' button under the 'Match' section. Step 5 highlights the 'Source: IP Prefix' input field with the value '10.30.10.0/24'. Step 6 highlights the 'Actions' section.

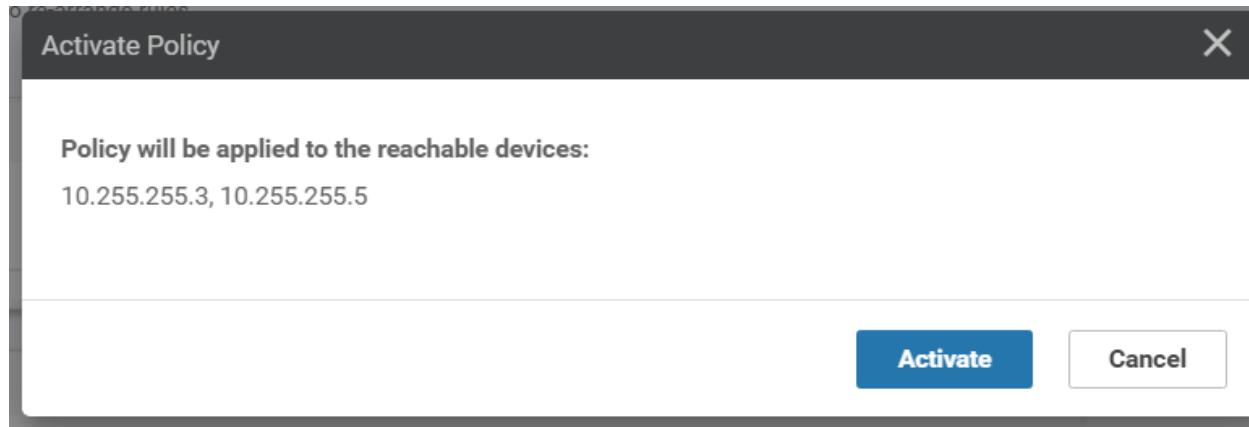
5. Select the **Accept** radio button and choose **NAT VPN**. Click on **Save Match and Actions** to save this rule



6. Make sure that there are two rules under the Custom Sequence Type. One rule is for Site 40 DIA and the other is for Site 30 VPN 10 (10.30.10.0/24) DIA. Click on **Save Data Policy**



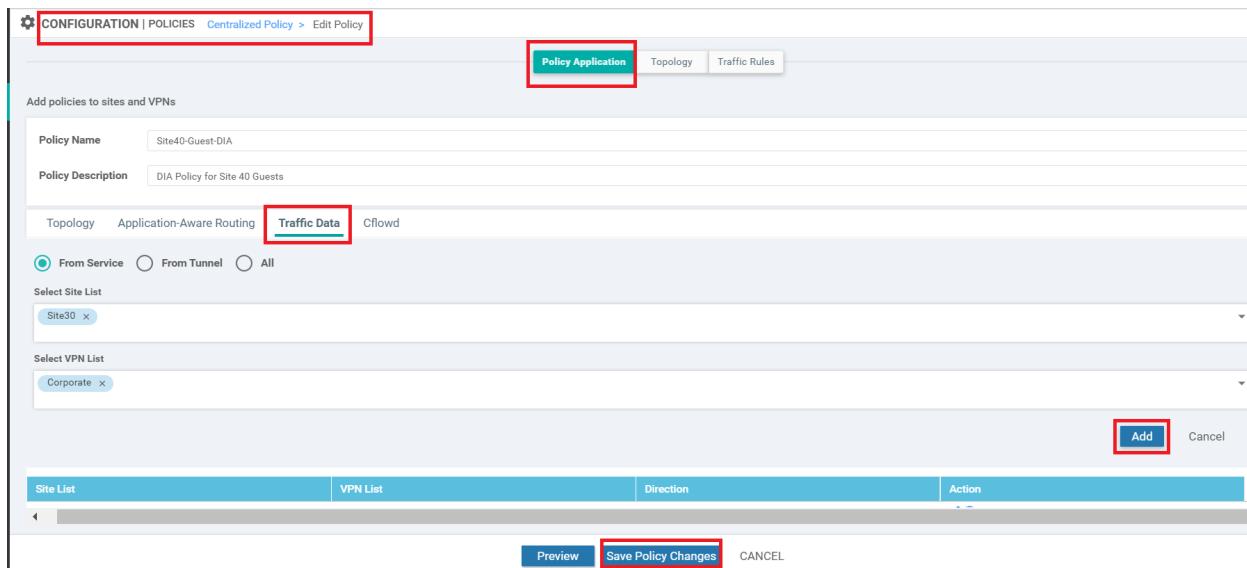
7. Click on **Activate** and then **Configure Devices**. Confirm the configuration change and click on **OK**



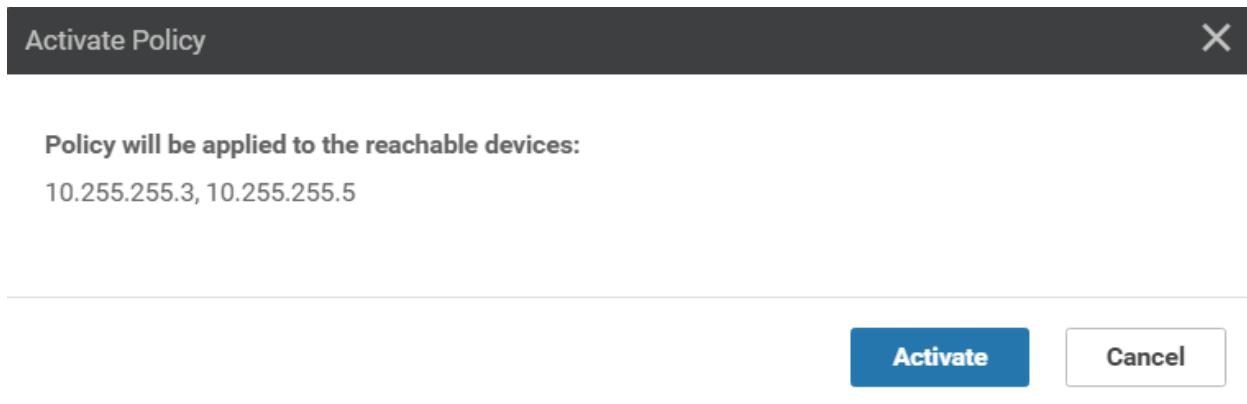
The Cisco vManage interface showing the "CONFIGURATION | TEMPLATES" section. A device template named "vSmart-dev-temp" is selected, with a total of 1 device. The "Device list (Total: 2 devices)" shows two entries: "20607a12-c0c8-4f46-a65f-5a547cdf3325" (vSmart|10.255.255.3) and "7f332491-cb6f-4843-8bf5-060f90df8dec" (vSmart2|10.255.255.5). A yellow notification bar at the top right states: "'Configure' action will be applied to 2 device(s) attached to 1 device template(s)". Below the device list, there is a "Configure Device Rollback Timer" button. At the bottom of the screen are three buttons: "Back", "Configure Devices" (highlighted with a red box), and "Cancel".



8. Once the configuration change has been pushed successfully, navigate to **Configuration => Policies** and click on the three dots next to the **Site40-Guest-DIA** policy. Choose to **Edit** it. Make sure you're on the **Policy Application** page and click on the **Traffic Data** tab. Click on **New Site List and VPN List**. Leave the *From Service* radio button checked and click on the **Select Site List** box. Choose **Site30**. Click on the **Select VPN List** box and choose **Corporate**. Click on **Add**. Click on **Save Policy Changes** to save the changes we just made



9. Choose to **Activate** the configuration



10. Go to the Site 30 PC via your chosen connection method (Guacamole/RDP/vCenter Console) and open Command Prompt (Start => type cmd => click on Command Prompt). Type `ping 8.8.8.8` and hit Enter. Pings should work. To verify DNS resolution, type `ping www.cisco.com` and hit Enter

```
C:\Users\sdwan>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1050ms TTL=116
Reply from 8.8.8.8: bytes=32 time=1154ms TTL=116
Reply from 8.8.8.8: bytes=32 time=1071ms TTL=116
Reply from 8.8.8.8: bytes=32 time=778ms TTL=116

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 778ms, Maximum = 1154ms, Average = 1013ms

C:\Users\sdwan>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [104.121.253.199] with 32 bytes of data:
Reply from 104.121.253.199: bytes=32 time=190ms TTL=55
Reply from 104.121.253.199: bytes=32 time=309ms TTL=55
Reply from 104.121.253.199: bytes=32 time=403ms TTL=55
Reply from 104.121.253.199: bytes=32 time=566ms TTL=55

Ping statistics for 104.121.253.199:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 190ms, Maximum = 566ms, Average = 367ms
```

We have enabled DIA at Site 30 for VPN 10. This will be used to showcase DNS security provided by Umbrella. Once we proceed through the lab activity and have set up Tunnels to Umbrella, the DIA configuration will be removed to force traffic out the tunnels.

Task List

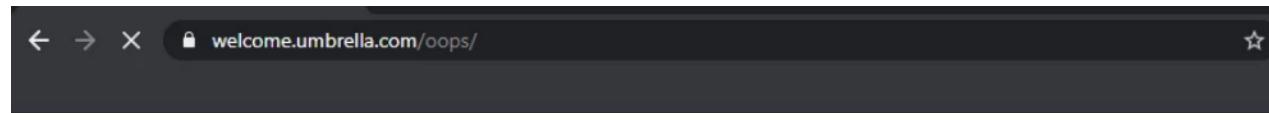
- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - [API Keys and AD Configuration](#)

- DC Configuration Download
- AD Connectors
- Roaming Computer Configuration
- Building a DNS Policy
- Setting up IPSEC Tunnels
- Configuring a Firewall Policy
- Configuring a Web Policy

Life without Umbrella

As of now, the Site 30 PC has connectivity to the Internet and is pointing to the DNS Server of 10.30.10.50. DNS Queries sent to this DNS Server are redirected to 8.8.8.8 or 4.2.2.2. We will run a quick check from our Site 30 PC to verify that we are NOT connected to Cisco Umbrella as of now.

1. Access the Site 30 PC via your preferred method (Guacamole/RDP/vCenter Console). [Click here](#) and go through Step 1 to review how to connect to the Site 30 PC. Open a browser of your choice (Firefox and Chrome should be available) and go to welcome.umbrella.com. You can also use the bookmark for **Umbrella Test**



Product Customers Use Cases Partners Resources

Support Create Account Log In



Oops...

Your device isn't using Umbrella's DNS. Let's fix that.

If you haven't restarted your browser and cleared your local DNS cache yet, please do that now.

The Umbrella page should display the image shown above. This is an indication that our network isn't protected by Umbrella (yet).

If using Firefox, make sure to change the browser **Options** for Privacy and Security, setting Firefox to **Never remember history**. This will require a browser restart

The screenshot shows the Firefox Options window with the URL `about:preferences#privacy`. The left sidebar has categories: General, Home, Search, Privacy & Security (which is selected and highlighted in blue), and Sync. The main content area has sections for History and Address Bar.

History

Firefox will Never remember history ▼

Firefox will use the same settings as private browsing, and will not remember any history as you browse the Web.

Address Bar

When using the address bar, suggest

Browsing history

2. Access websites like www.amazon.com, www.ebay.com and www.yahoo.com by typing them out in the browser or by using the handy bookmarks available. All the sites should be accessible since we don't have any sort of access control/filtering enabled as of now

amazon.com

amazon All Search

Hello, Sign in Account & Lists Returns & Order

Deliver to India Today's Deals Customer Service Gift Cards Registry Sell Amazon's response

We ship over 45 million products around the world

You are on amazon.com. You can also shop on Amazon India for millions of products with fast local delivery. Click here to go to amazon.in

Shop by Category

AmazonBasics

Electronics



Shop by category ▾

 Search for anything

All Categories ▾

Search

Home

Saved

Electronics

Fashion

Health & Beauty

Motors

Collectibles

Sports

Home & Garden

Deals

essories.

D

Get
price

S

Popular Destinations | See all ➔



yahoo!



Sign in



Mail N

Mail Coronavirus Cricket News Finance Lifestyle Movies Women More...

Coronavi...

Catch all updates on how India is battling the pandemic



100 Chinese soldiers

Trending Now

3. Access internetbadguys.com by typing it out in the browser or using the bookmark. This is a website that simulates a phishing attack. Since we aren't protected, the website pops right up



InternetBadGuys.com is only a demonstration site.

If you were using OpenDNS,
real phishing sites would be blocked.

OpenDNS makes your Internet work better

- **Safer:** helps prevent identity theft & blocks phishing sites.
- **Faster:** speeds up your existing Internet connection.
- **Smarter:** corrects spelling mistakes on the fly.

Get started in 2 minutes

It's **free** and there's no software to install. [Get started.](#)

About this page

David Ulevitch, the founder of OpenDNS, writes about Internet Bad Guys in "[Why I Started OpenDNS](#)."

OpenDNS

Life without Umbrella doesn't look too good since we are open to the simplest of phishing attacks. We will be incorporating a fundamental layer of protection in our network followed by a more elaborate DNS Policy, Cloud Delivered Firewall and Secure Web Gateway solution.

Task List

- [Overview](#)

- Pre-Work
- Enabling Site 30 for DIA
- Life without Cisco Umbrella
- Basic Configuration for Umbrella
- Making Umbrella Ours
 - API Keys and AD Configuration
 - DC Configuration Download
 - AD Connectors
 - Roaming Computer Configuration
- Building a DNS Policy
- Setting up IPSEC Tunnels
- Configuring a Firewall Policy
- Configuring a Web Policy

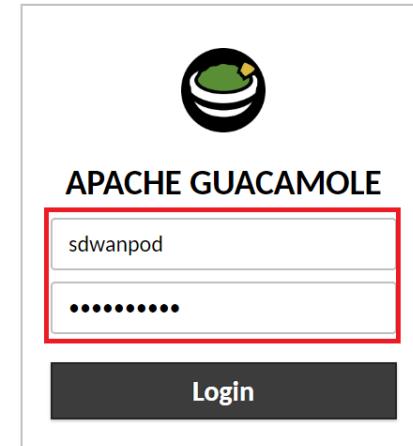
Basic Configuration for Umbrella

Let's start off by giving some basic DNS-layer Security to our devices.

1. Connect to the sdwan-ghi-ad-podX machine by logging in to Guacamole (10.2.1.20X:8080/guacamole, where X is your POD number) with the credentials given below and click on the PODX-AD option.

Alternatively, you can RDP to 10.2.1.18X (where X is your POD number) from the Jumphost. RDP to the AD PC will only work from the Jumphost

| Connection Method | Username | Password |
|-------------------|----------------------------|------------|
| Guacamole | sdwanpod | C1sco12345 |
| RDP | swatsdwanlab\Administrator | C1sco12345 |



This section displays three recent connections:

- POD3-Site30PC**: A blue square with a white circular icon in the center, labeled "Starting done".
- POD3-AD**: A screenshot of a Windows Server Manager window showing the "Configure this local server" wizard.
- POD3-Jumphost**: A solid black square.

This section displays a list of all connections:

- POD3-AD**: Selected, indicated by a red box around its checkbox icon.
- POD3-Jumphost**
- POD3-Site30PC**

A "Filter" search bar is located at the top right of the list area.

vCenter (accessible via the bookmark or 10.2.1.50/ui and the credentials provided for your POD) can also be used to console to the AD PC

2. Depending on the connection method, you may need to enter credentials again to log in to the AD PC. Please enter the credentials shown below, if prompted

| Connection Method | Username | Password |
|-------------------|----------------------------|--------------|
| Guacamole | Not Required | Not Required |
| RDP | swatsdwanlab\Administrator | C1sco12345 |
| vCenter | swatsdwanlab\Administrator | C1sco12345 |

If using Guacamole to access the AD PC, you will be notified to press Ctrl + Alt + Del to unlock the computer.

Guacamole doesn't have an option to send key combinations. We use the Guacamole virtual keyboard to send Ctrl + Alt + Del. While on the Guacamole window, press **Ctrl + Alt + Shift** together. This will open the Guacamole settings window. Choose **On-screen keyboard** under Input Method and it should display the virtual keyboard. Using the mouse, click on *Ctrl*, then *Alt*, then *Del*

POD3-AD

sdwanpod ▾

None

Press Ctrl + Alt + Shift to open this Window (via Guacamole)

No input method is used. Keyboard input is accepted from a connected, physical keyboard.

Text input

Allow typing of text, and emulate keyboard events based on the typed text. This is necessary for devices such as mobile phones that lack a physical keyboard.



On-screen keyboard

Display and accept input from the built-in Guacamole on-screen keyboard. The on-screen keyboard allows typing of key combinations that may otherwise be impossible (such as Ctrl-Alt-Del).



Mouse emulation mode

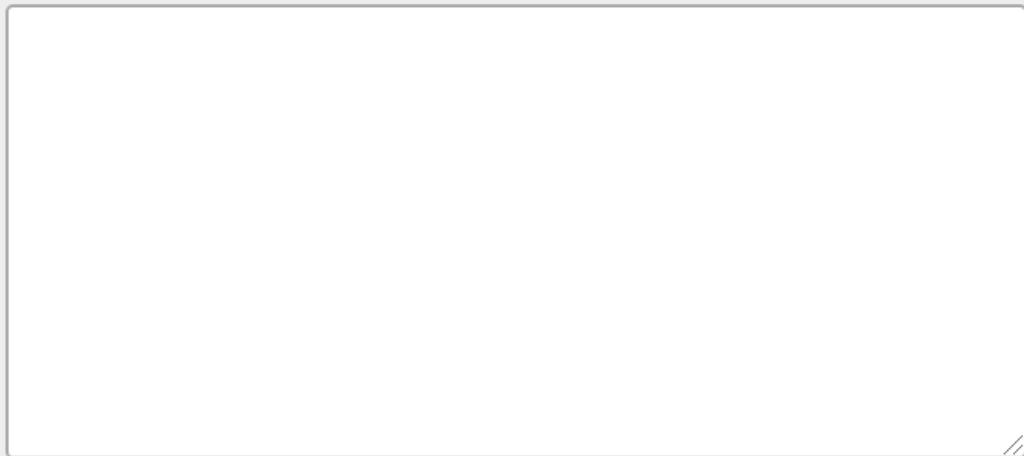
Determines how the remote mouse behaves with respect to touches.



This will bring you to the login screen. Press **Ctrl + Alt + Shift** on your keyboard to bring up the Guacamole settings window again and choose **None** for the Input Method

Clipboard

Text copied/cut within Guacamole will appear here. Changes to the text below will affect the remote clipboard.



Input method

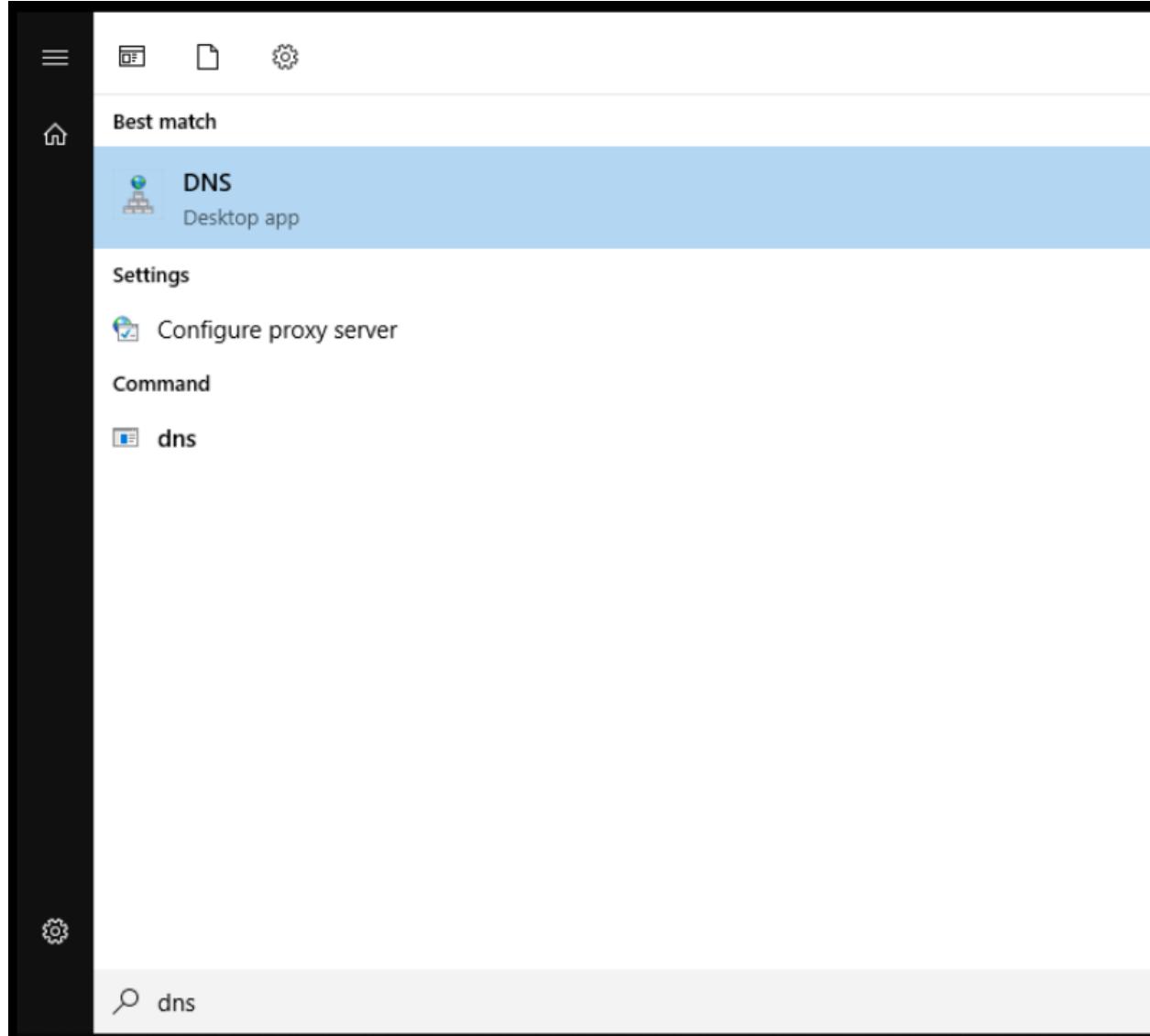


None

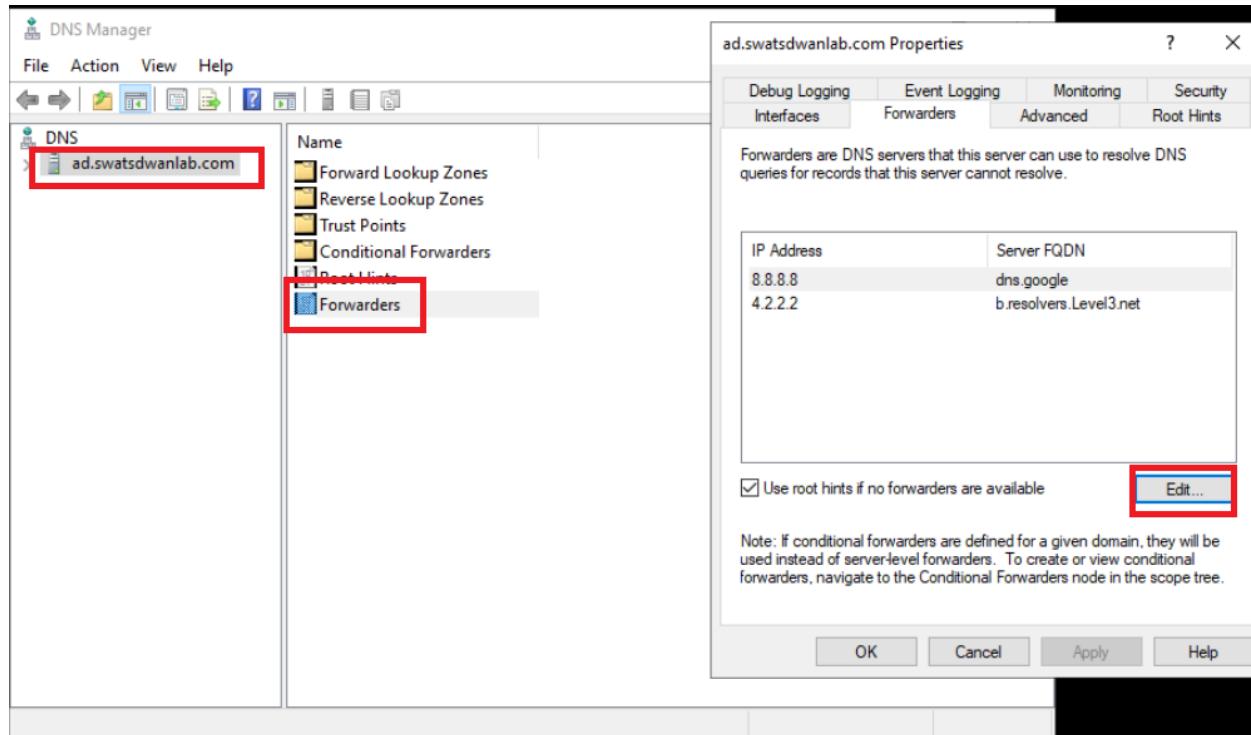
No input method is used. Keyboard input is accepted from a connected, physical keyboard.

This will remove the virtual keyboard from the screen and you can continue typing like normal to enter the password.

3. Once logged in to the AD PC, click on **Start** and search for *DNS*. Open the DNS application

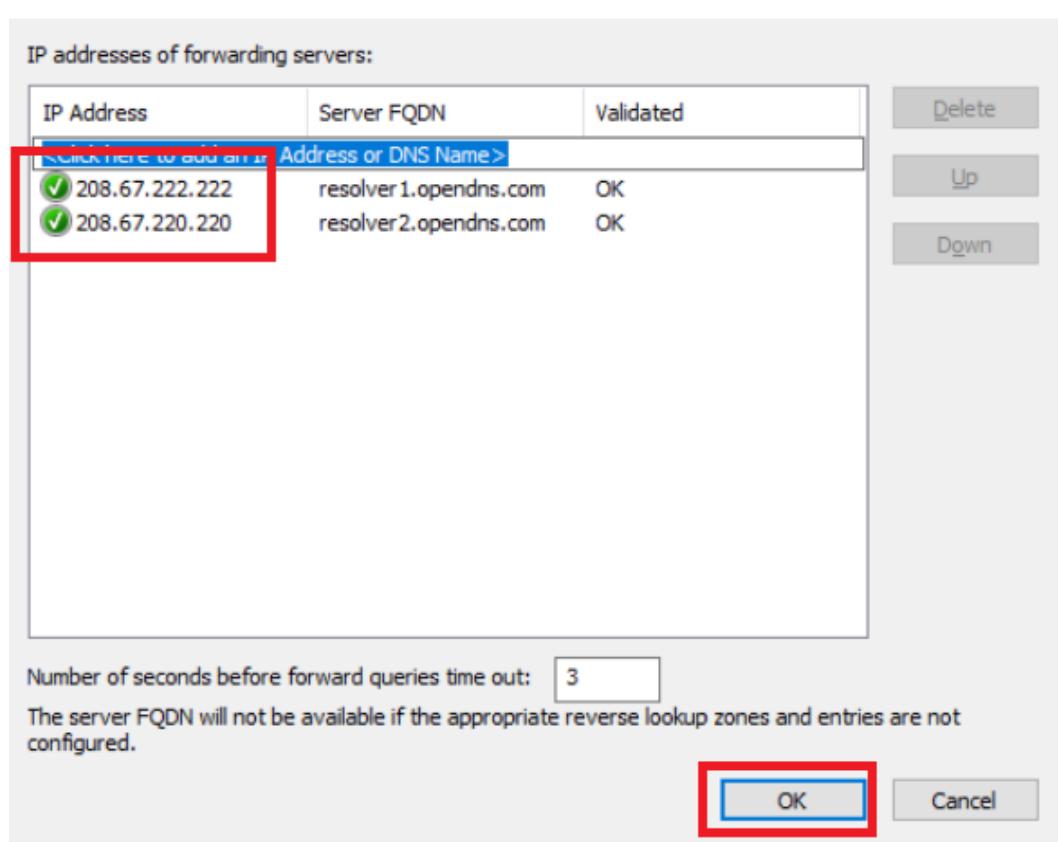


4. Select `ad.swatswanlab.com` and double-click Forwarders. There will be two Forwarders listed (`8.8.8.8` and `4.2.2.2`).
Click on **Edit**

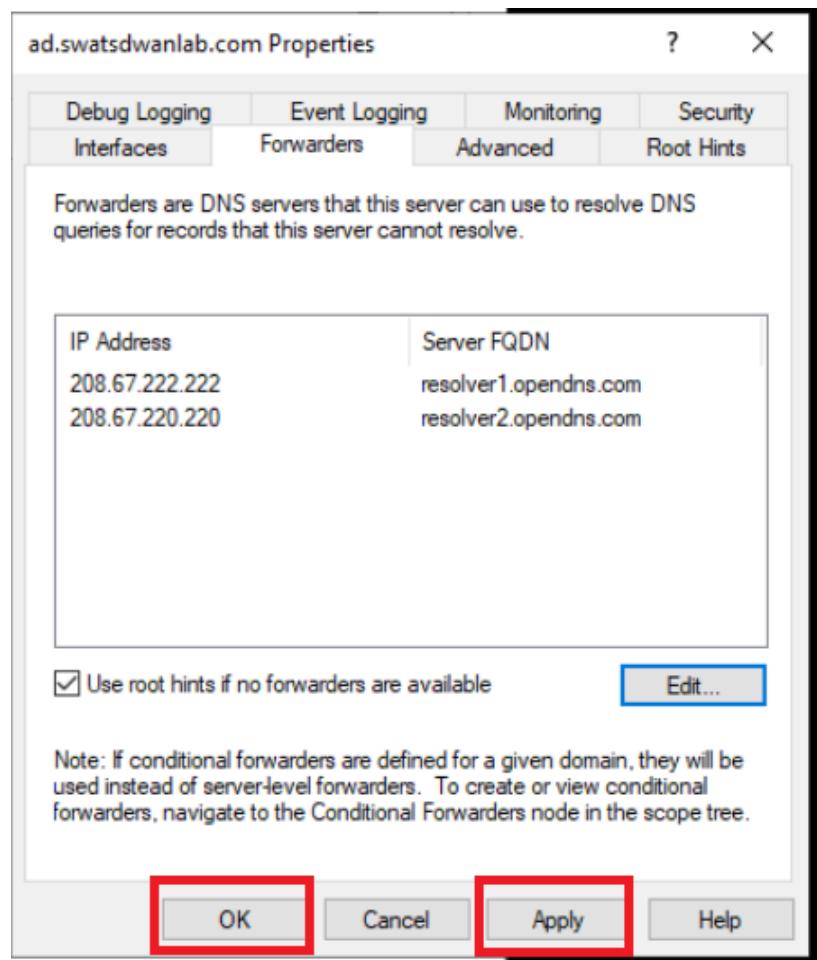


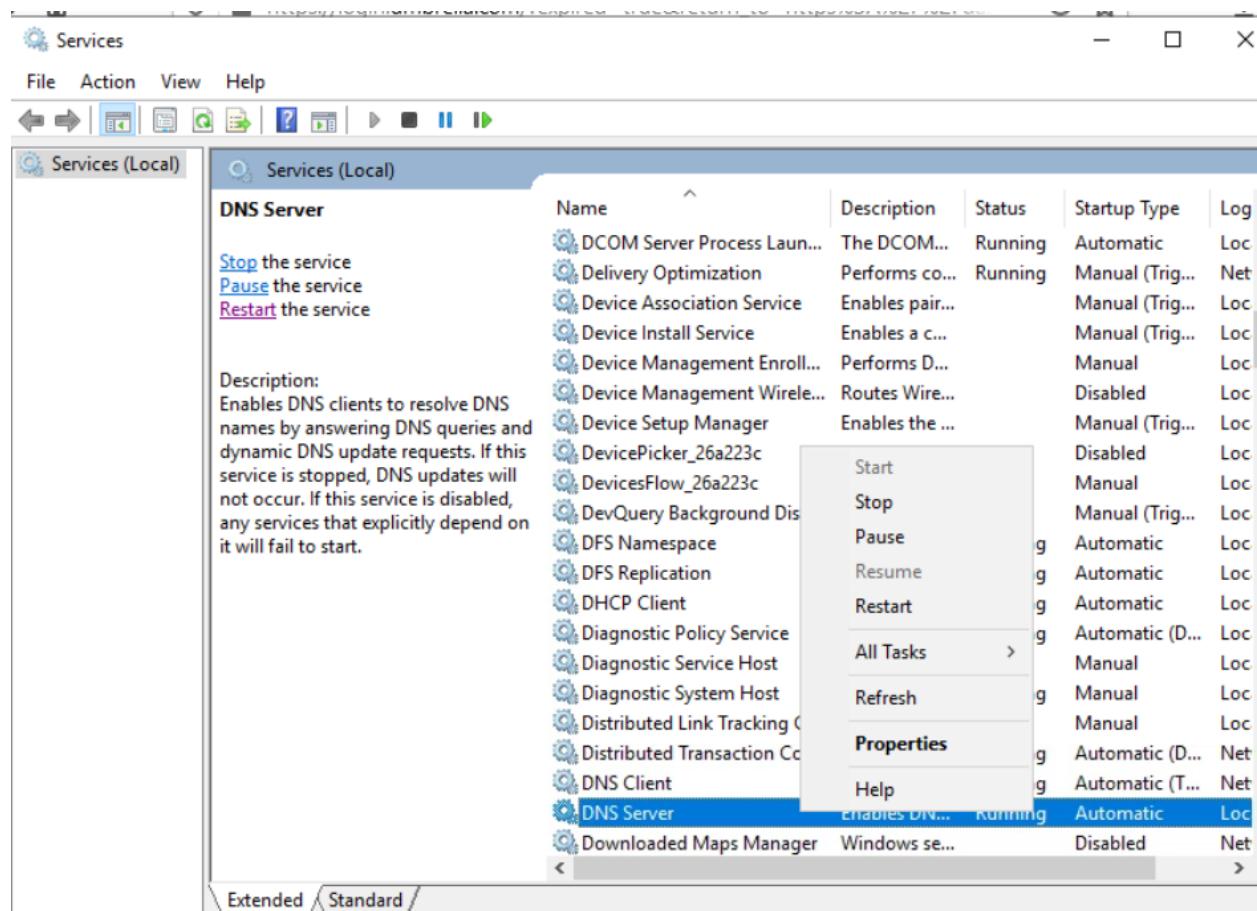
5. Change the Forwarder IPs to 208.67.222.222 and 208.67.220.220. Make sure no other Forwarders are present on this window. Click on **OK**

Edit Forwarders

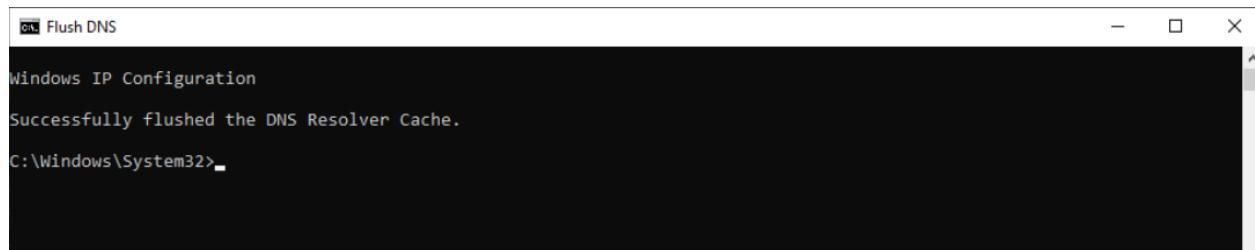
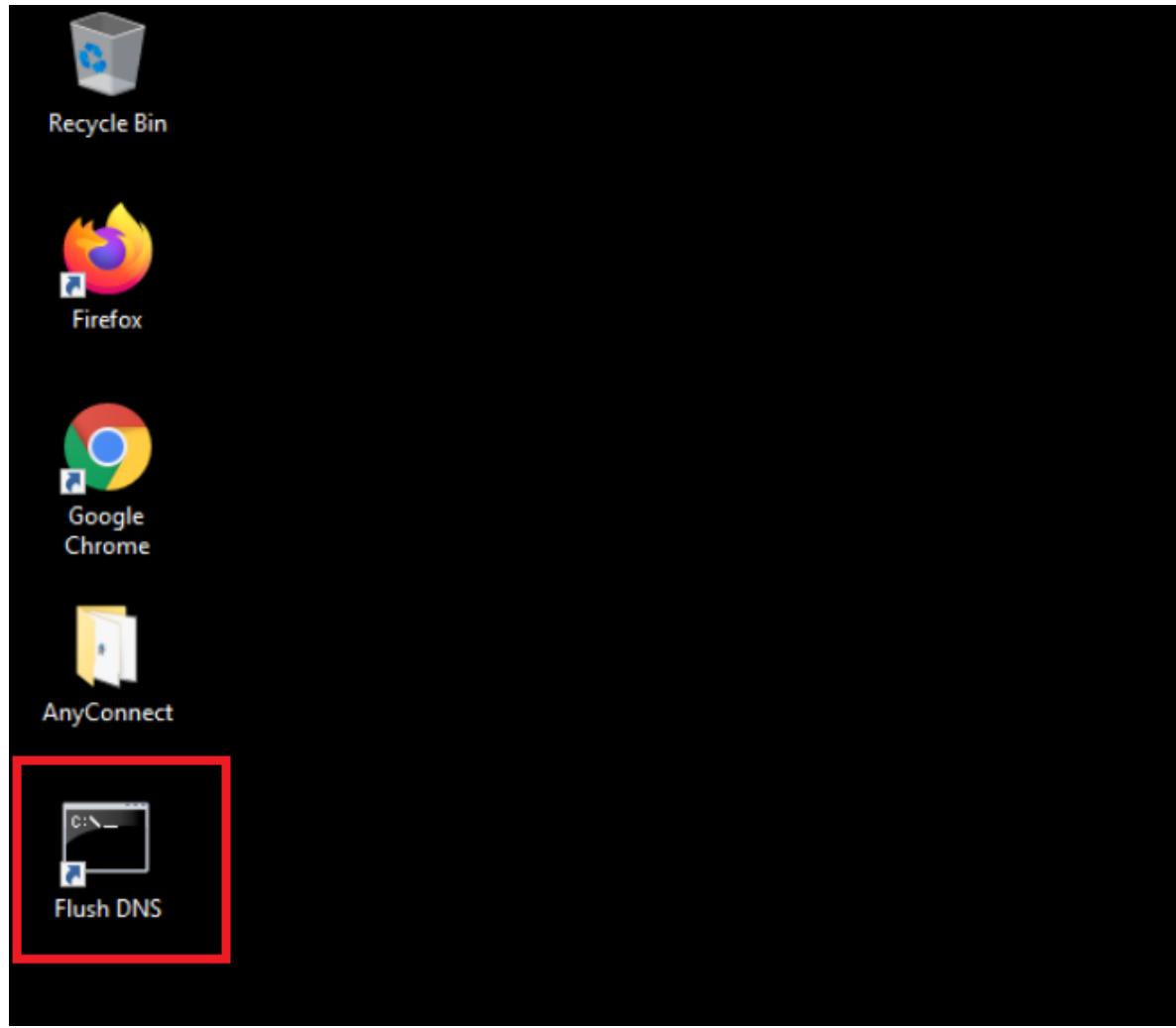


6. Click on **Apply** and then **OK** to apply the configuration change. Click on Start and type **services.msc**. Hit Enter and look for the DNS Server service. Right click on it and restart the service

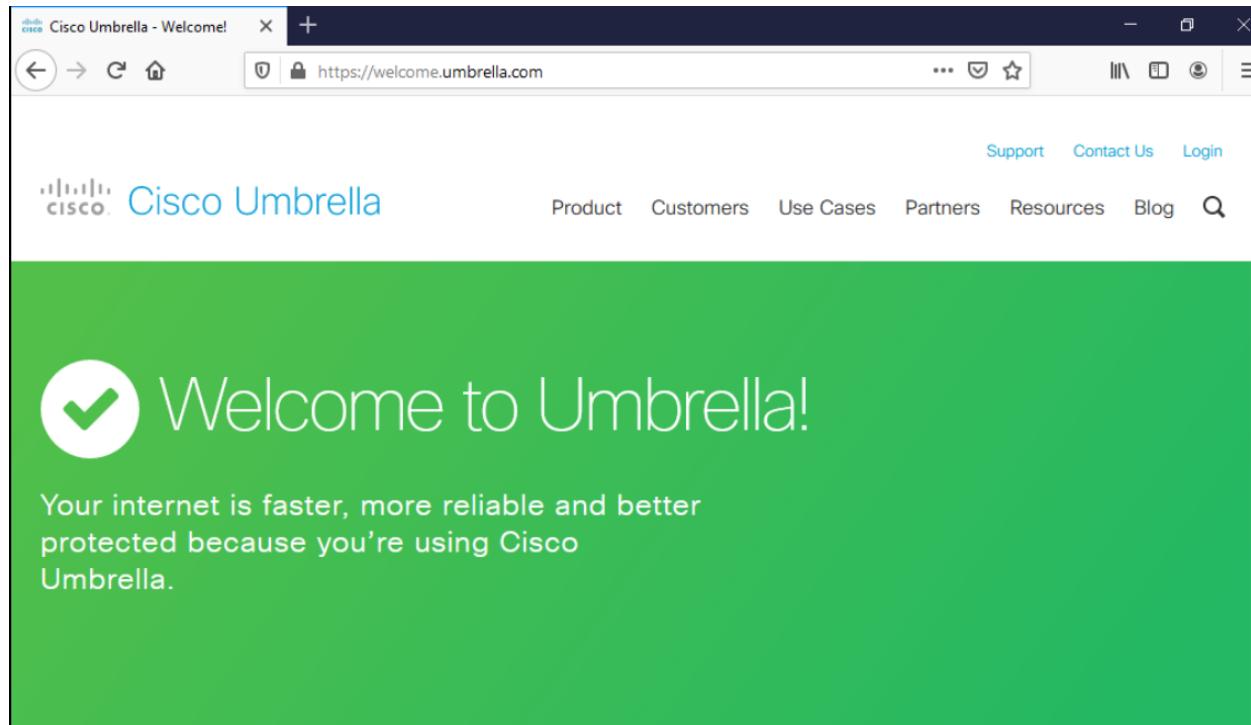




7. Head back to the Site 30 PC and click on the **Flush DNS** shortcut on the Desktop



8. Close any open browsers and re-open the browser. Go to welcome.umbrella.com or use the Umbrella Test bookmark.
We should see a **Welcome to Umbrella** page



9. Access to amazon.com and ebay.com should still be intact, since we haven't applied any policies yet

The image shows a web browser window with two tabs open. The top tab is for ebay.com, displaying the homepage with a search bar and navigation menu. The bottom tab is for Amazon.com, also showing its homepage with a search bar and navigation menu. Both tabs show a 'Waiting for pages.ebay.com...' message.

10. Enter internetbadguys.com in the browser and the traffic will be blocked. We have thus got a fundamental layer of security by simply pointing our DNS Server to the OpenDNS resolvers

cisco Phishing Site Blocked

← → C phish.opendns.com/main?url=internetbadguys.com&server=hkg15&prefs=&tagging=&nref

Cisco Umbrella

 This site is blocked due to a phishing threat.

internetbadguys.com

Phishing is a fraudulent attempt to get you to provide personal information under false pretenses. [Learn phishing tips to protect you, your family, or your business](#)

Sorry, internetbadguys.com has been blocked by your network administrator.

[Report an incorrect block](#)

[Diagnostic Info](#)

[Terms](#) | [Privacy Policy](#) | [Contact](#)

Note: If the site still opens, Flush the DNS cache on the Site 30 PC by clicking the Flush DNS shortcut on the desktop.

Tip: This is the simplest way to redirect traffic to Umbrella. However, if a user changes the DNS Server IP Address on their PCs, they can bypass the Umbrella redirect completely. It is recommended to deploy policies via vManage such that vEdges/cEdges can intercept DNS traffic destined for a manually entered DNS server (like 8.8.8.8) and redirect it to Umbrella.

Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - API Keys and AD Configuration
 - DC Configuration Download
 - AD Connectors
 - Roaming Computer Configuration
- [Building a DNS Policy](#)
- [Setting up IPSEC Tunnels](#)
- [Configuring a Firewall Policy](#)
- [Configuring a Web Policy](#)

Making Umbrella ours

The previous section ensured that DNS queries were redirected to Umbrella, giving us a basic layer of protection. To apply custom DNS policies, we will need to ensure that our setup can be uniquely identified by Umbrella, post which DNS Policies can be set up for the organization. Umbrella can be used to identify traffic coming from a public IP/IP Range. This helps with creating custom policies for a particular organization. In our lab, multiple devices will be talking to the outside world via the same Public IP, hence this approach will not work for us.

Instead, we can get extremely granular and apply a policy to a specific user/group of users based on identities used to uniquely identify them. We can also pinpoint individual workstations by leveraging Cisco AnyConnect, thereby encompassing Roaming Computers in our DNS policies.

[API Keys and AD Configuration](#)

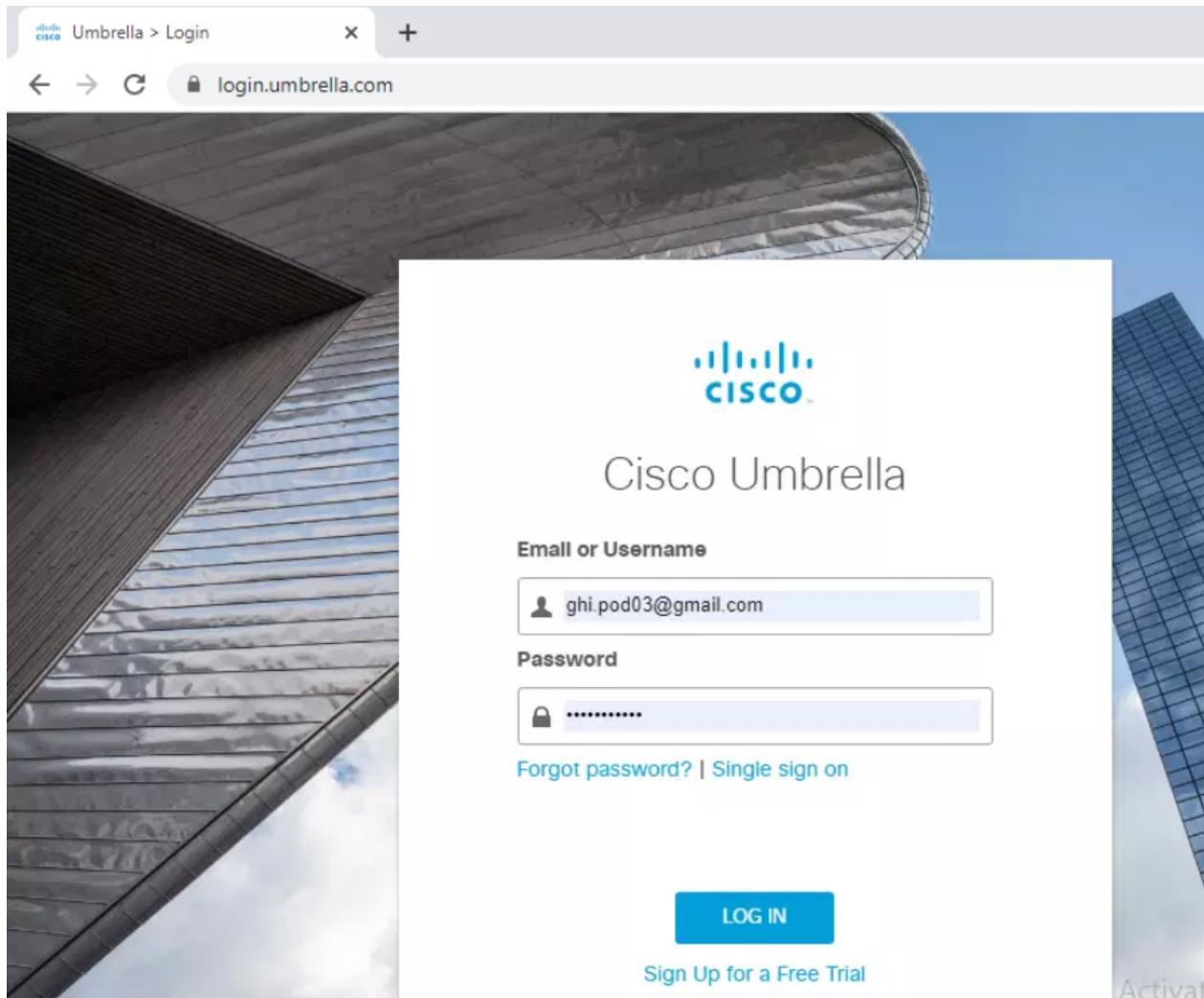
Three pieces of the puzzle that uniquely identify our Enterprise Network on Umbrella are given below:

- Organization (this is a numeric string, allocated by Umbrella. Not to be confused with the SD-WAN organization name)
- API Key

- Secret

1. From your Jumphost, open a browser and go to login.umbrella.com. Login using the username/password for your POD

| Username | Password |
|----------------------|-------------|
| ghi.pod0X@gmail.com | C1sco@12345 |
| X is your POD number | |



2. Once logged in, the URL will contain your Organization ID. It will vary per POD. Copy it in a notepad file on the Jumphost since we will be needing it later

The screenshot shows a web browser window with the Cisco logo in the top left corner. The title bar says "Overview". The address bar contains the URL <https://dashboard.umbrella.com/o/3870852/#/overview>, with the organization ID "3870852" highlighted by a red box. The main content area is titled "Overview" and displays three sections: "Malware: 0 requests blocked in the last 24 hours" with links to "View Trend" and "View Details"; "Command and Control: 0 requests blocked in the last 24 hours" with links to "View Trend" and "View Details"; and "Cryptomining: 0 requests blocked in the last 24 hours" with links to "View Trend" and "View Details".

3. API Keys and the Secret needs to be generated on Umbrella. Navigate to **Admin => API Keys**. If the sidebar isn't visible, click on the menu icon (three horizontal lines) next to the Cisco Logo

The screenshot shows the Cisco Umbrella Overview page. On the left, a sidebar menu is open under the 'Admin' section, with 'API Keys' also highlighted by a red box. The main content area displays deployment health metrics for Malware, Command and Control, and Cryptomining, followed by a 'Deployment Health' section with four status cards: Active Networks (0%), Active Roaming Clients (0%), Active Virtual Appliances (0%), and Active Network Tunnels (Not tracking data). A 'Network Breakdown' section is partially visible at the bottom.

4. Click on **Create API Key**

The screenshot shows the 'API Keys' creation page. At the top, there is a message: 'Cisco Umbrella generates authentication keys for several types of integrations. These include software, Umbrella-enabled devices, and Cisco network hardware. Click Create, then specify the type of integration key you need.' Below this, a message states 'You have not generated any API keys yet.' A prominent blue 'CREATE API KEY' button is centered at the bottom of the page.

5. Select the radio button next to **Umbrella Management** and click on **Create**

What should this API do?

Choose the API that you would like to use.

Umbrella Network Devices

Integrate Umbrella-enabled hardware with your organization's networks. This also enables you to create, update, list, and delete identities in Umbrella.

Legacy Network Devices

A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.

Umbrella Reporting

Enables API access to query for Security Events and traffic to specific Destinations

Umbrella Management

Manage organizations, networks, roaming clients and more using the Umbrella Management API

CANCEL

CREATE

6. This will generate the API Key and Secret. Click on the copy icon next to each and paste it in the notepad which contains the Organization ID. Save this notepad file on the Desktop of the Jumphost, giving it any name

⚠ Important: Make sure that the Key and Secret are copied to notepad before proceeding since the Secret is visible on this page only.

Put a check mark next to the *To keep it secure...* statement and click on **Close**



Cisco Umbrella generates authentication keys for several types of devices, and Cisco network hardware. Click Create, then specify the key type and click Next Step.

Umbrella Management

Key:
8cbbd34d46614584a8f11a9b2c6cb861

The API Key and secret pair enable you to manage the deployment of networks, roaming clients and other core-identity types.

Your Key: 8cbbd34d46614584a8f11a9b2c6cb861 

Your Secret: fcdea273e6ed4e2f9722a3c13ee1a79d 

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

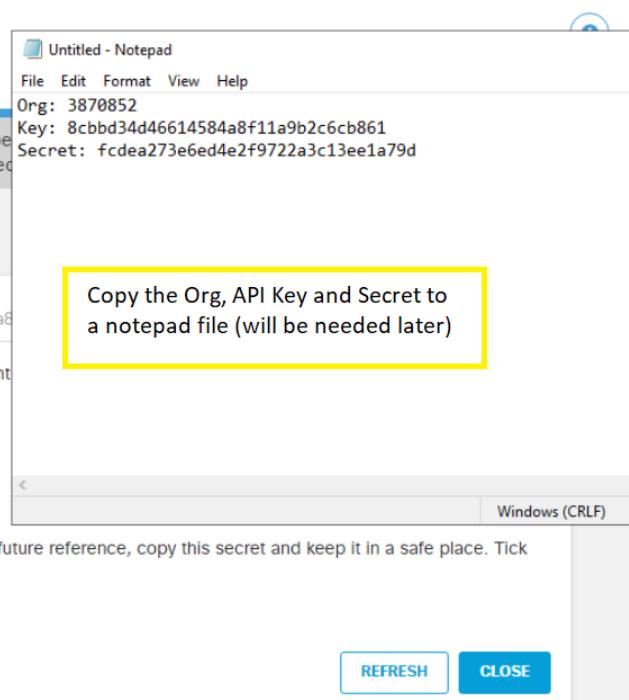
Check out the [documentation](#) for step by step instructions.

[DELETE](#)

[REFRESH](#)

[CLOSE](#)

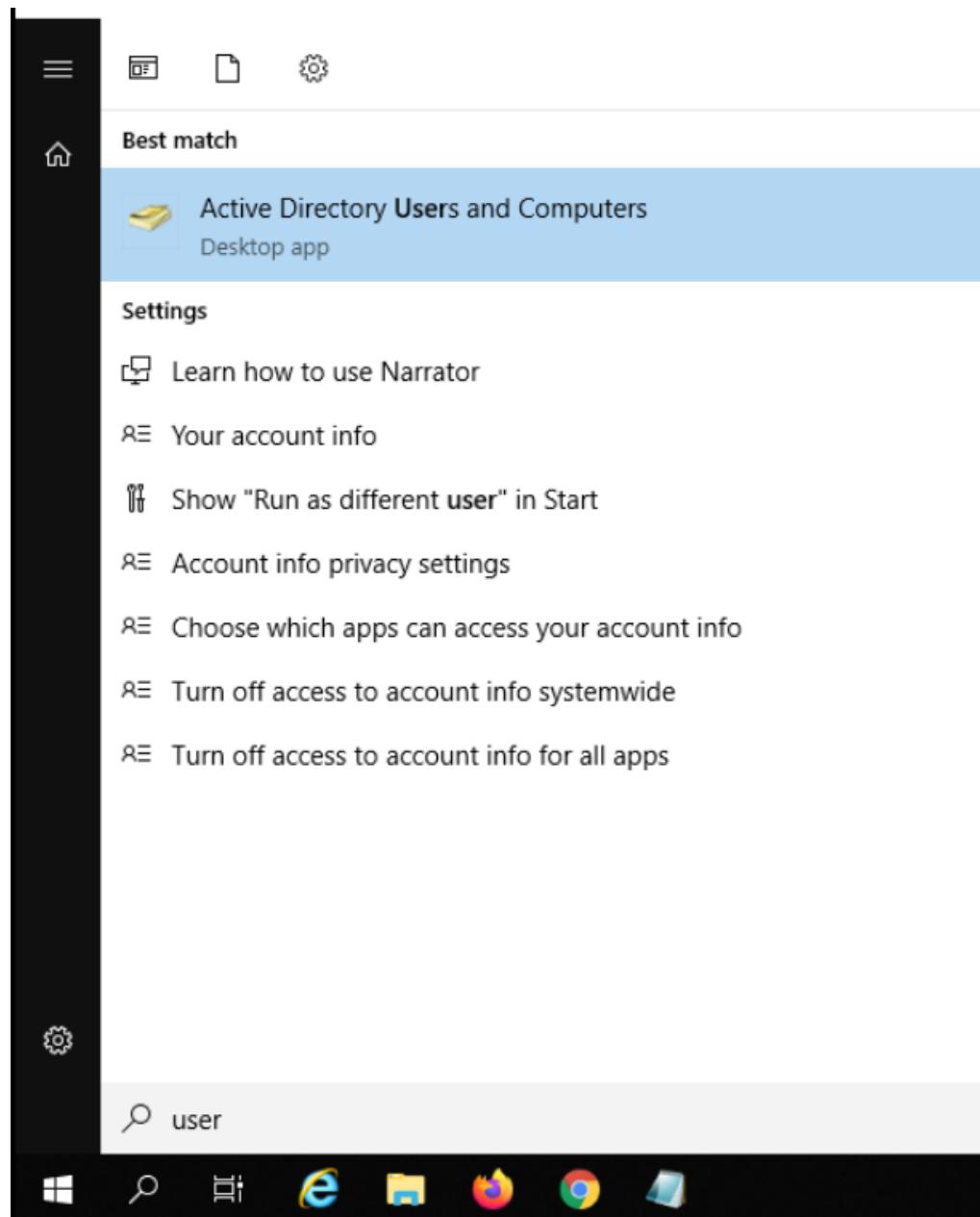
Copy the Org, API Key and Secret to a notepad file (will be needed later)



 **Tip:** If the key needs to be re-generated (usually required if the secret is misplaced), the Refresh button will allow you to generate a new API Key and Secret.

7. Log in to the AD PC (10.2.1.18X) via your preferred method (Guacamole/RDP/vCenter Console) and click on Start.

Search for Active Directory Users and Computers and open the App



8. Make sure `swatsdwanlab.com` is expanded and right click on **Users**. Click on **New** and click on **User** to create a new user

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com
Saved Queries
swatsdwanlab.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Account
U

Delegate Control...
Find...
New
All Tasks
View
Refresh
Export List...
Properties
Help

RAS a
Creates a new item in this container.
VIEW DOCS

Name Type Description

Administrator User Built-in account for ad

Allowed RO... Security Group... Members in this group

Cert Publish... Security Group... Members of this group

Cloneable D... Security Group... Members of this group

Denied ROD... Security Group... Members in this group

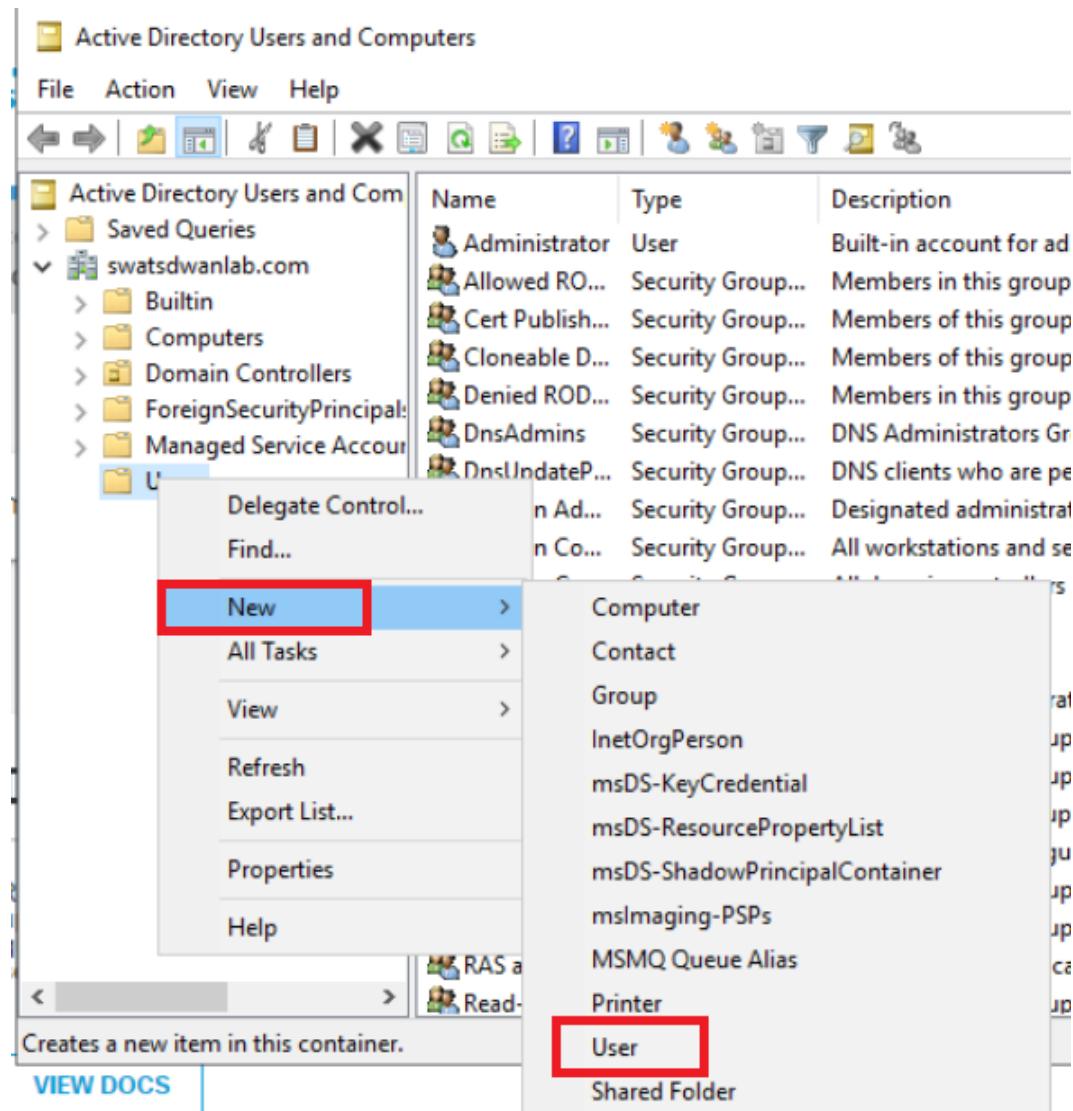
DnsAdmins Security Group... DNS Administrators Gr

DnsLIndateP... Security Group... DNS clients who are pe

n Ad... Security Group... Designated administrat

n Co... Security Group... All workstations and se

Computer
Contact
Group
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Printer
User
Shared Folder



9. Populate the fields as shown in the table below and click on **Next**

| Field | Value |
|-----------------|-------------------|
| First Name | OpenDNS_Connector |
| User logon name | OpenDNS_Connector |

Note: The User logon name field had to match with what is given here in previous versions of vManage. The name can now be populated as a custom value, if required, but we will use the default logon name.

New Object - User

Create in: swatsdwanlab.com/Users

First name: OpenDNS_Connector Initials:

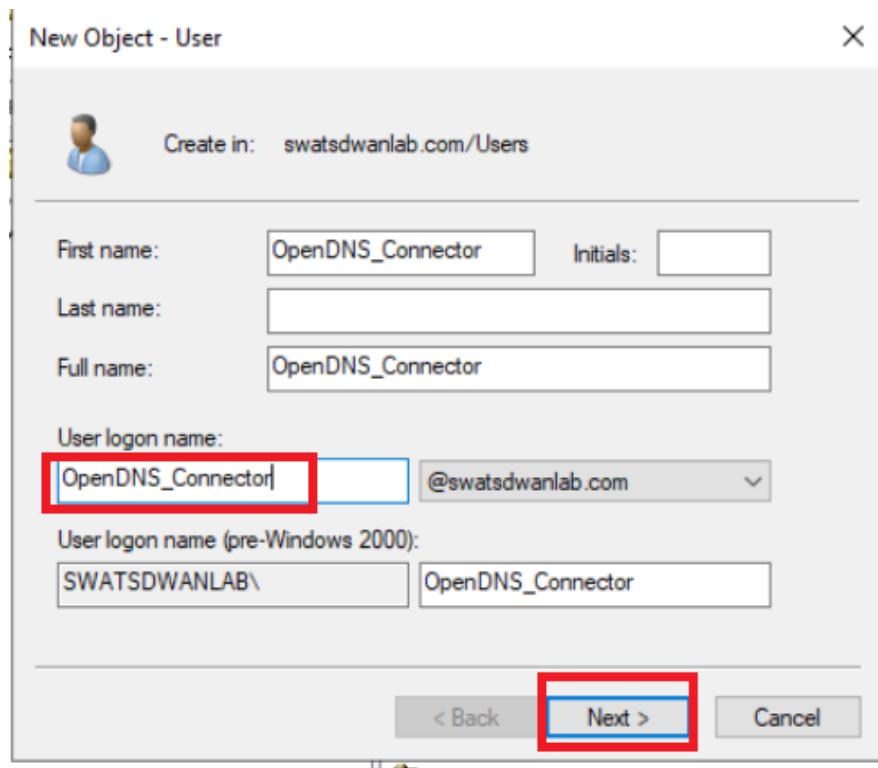
Last name:

Full name: OpenDNS_Connector

User logon name:

User logon name (pre-Windows 2000):

< Back **Next >** Cancel



10. Enter a password of **C1sco12345** in the Password and Confirm Password fields. Uncheck *User must change password at next logon* and check *Password never expires*. If you check Password never expires directly, it will automatically uncheck User must change password at next logon but will give a notification prompt (choose OK). Click on **Next** and then **Finish**

New Object - User X

Create in: swatsdwanlab.com/Users

Password: C1sco12345 C1sco12345

Confirm password:

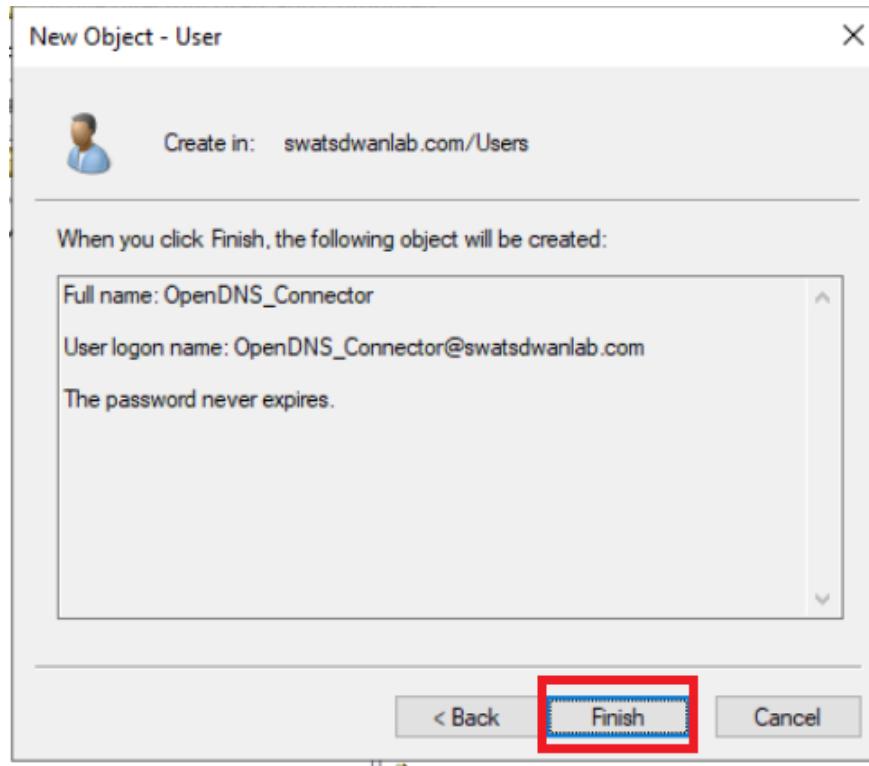
User must change password at next logon

User cannot change password

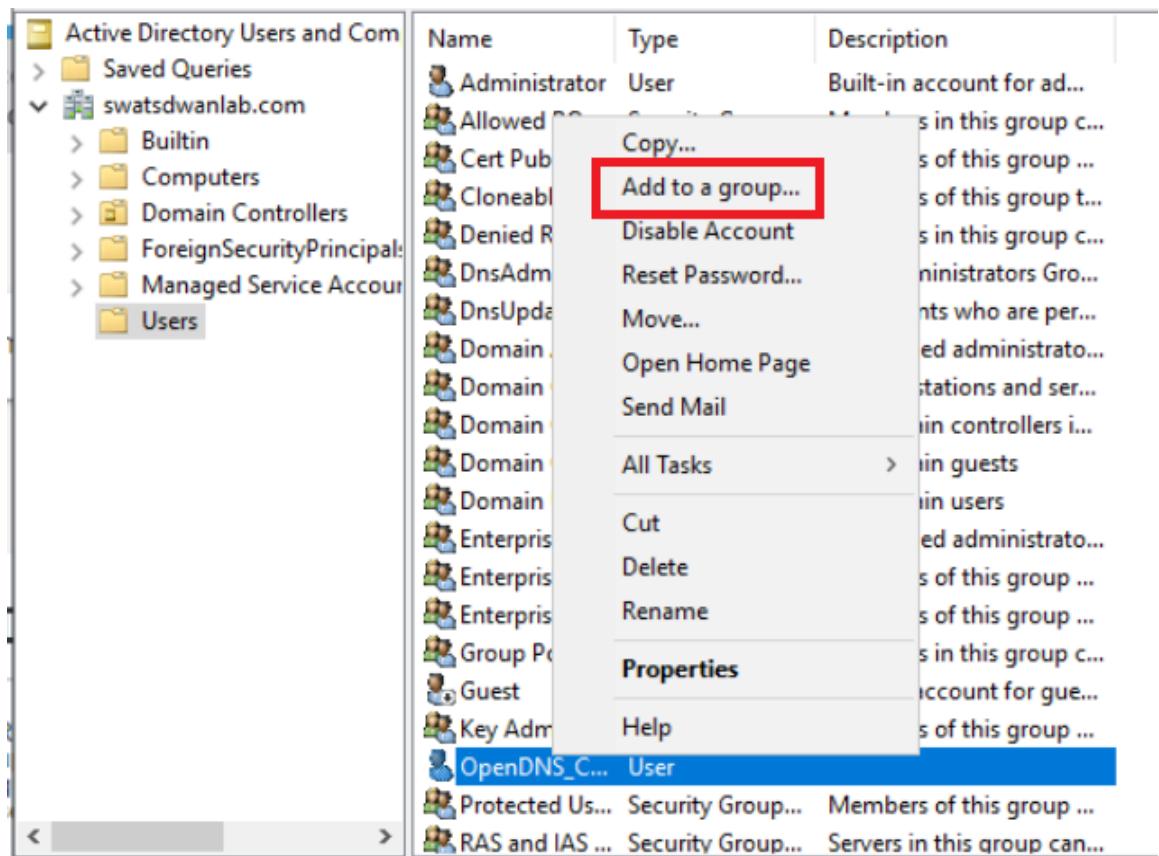
Password never expires Password never expires

Account is disabled

< Back Next > Cancel



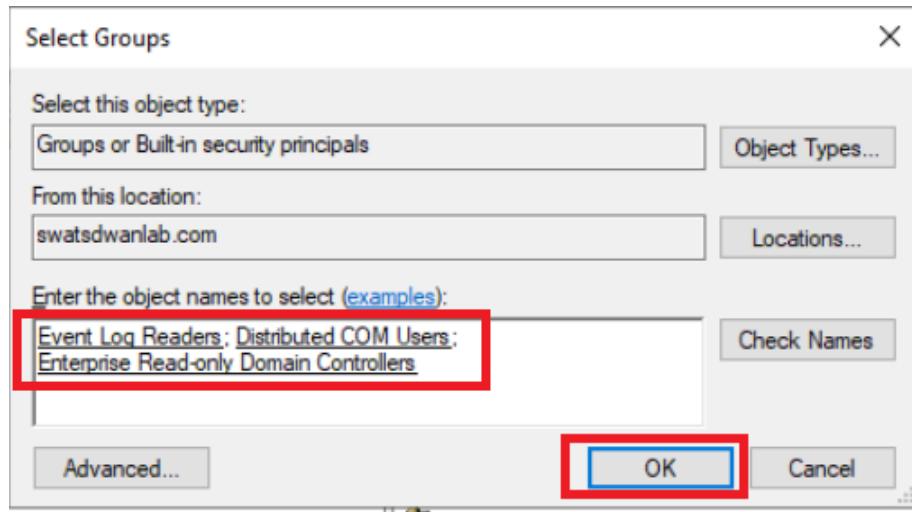
11. The user we just created needs to be a part of certain Groups in order to function properly. Right click on the newly created **OpenDNS_Connector** user and click on **Add to a group**



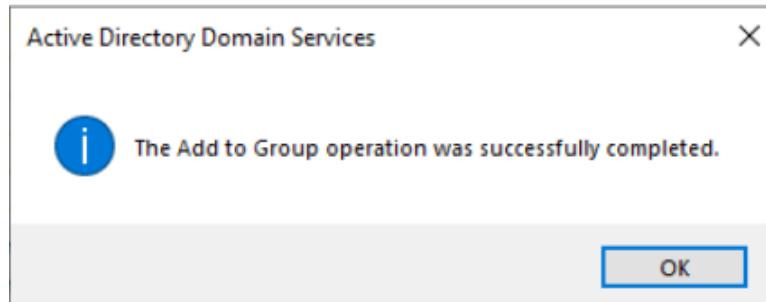
12. Add the user to the following groups and click on OK:

- Event Log Readers
- Distributed COM Users
- Enterprise Read-only Domain Controllers

Note: Enter the first few characters of the Group you want to add this User to and click on *Check Names*. That should auto-populate the Group or give you a selection to choose the group.



13. Click on **OK** to confirm the addition of the user to the Groups



We have generated the API Key and Secret which will be needed later in the integration with Cisco Umbrella. We have also set up an AD User which will be required for AD Connector functionality.

Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
- [API Keys and AD Configuration](#)

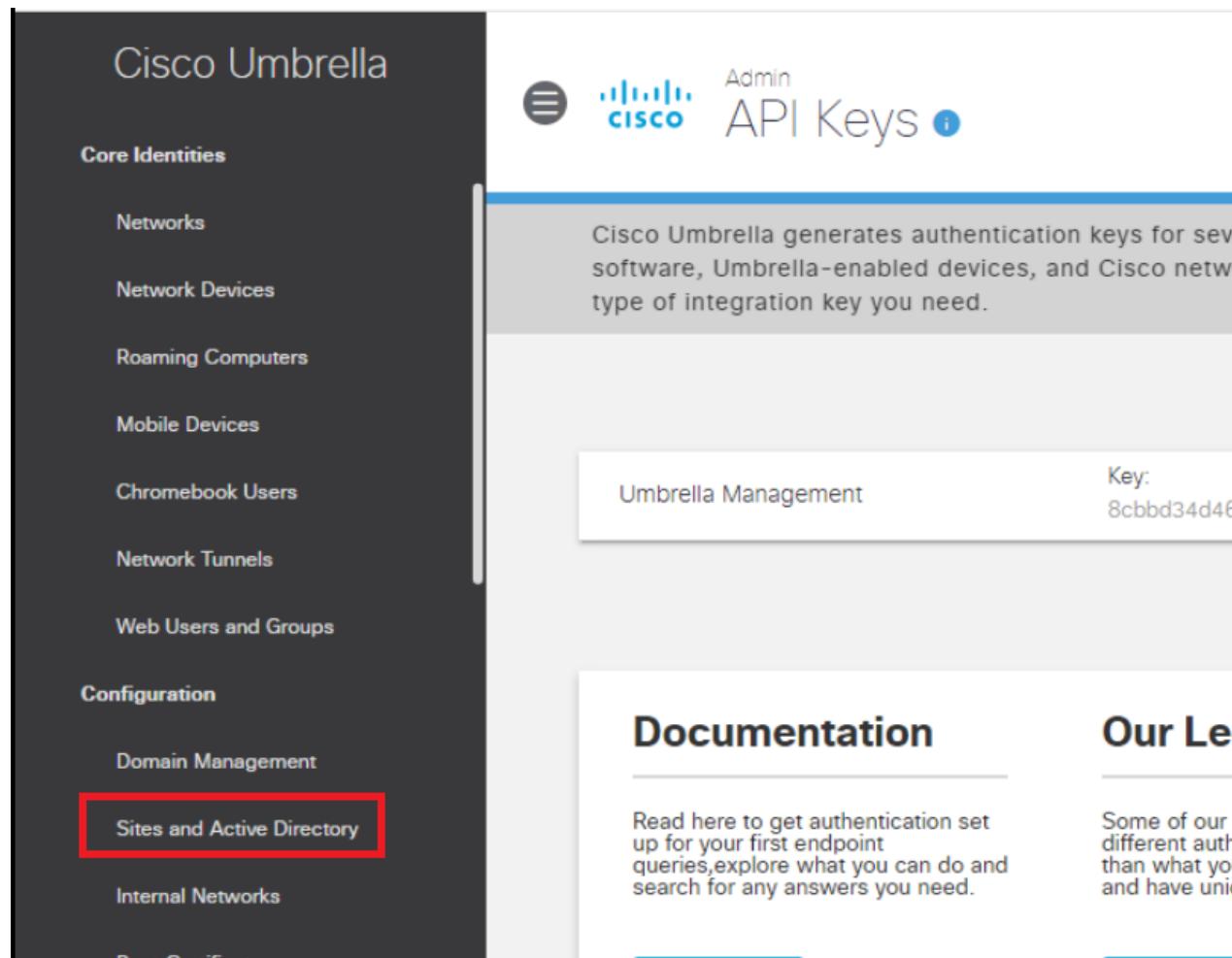
- DC Configuration Download
- AD Connectors
- Roaming Computer Configuration
- Building a DNS Policy
- Setting up IPSEC Tunnels
- Configuring a Firewall Policy
- Configuring a Web Policy

DC Configuration Download

To uniquely identify our SD-WAN network, we will be connecting AD to Umbrella and syncing AD Groups and Users. This is done by downloading and running a configuration script on the Domain Controller (all read-write DCs) and by deploying an AD Connector. A user is required for the AD Connector to work - this was created in the previous section.

1. From your **AD PC**, open a browser and go to login.umbrella.com. Login using the username/password for your POD.
Go to **Deployments => Configuration => Sites and Active Directory**

| Username | Password |
|----------------------|-------------|
| ghi.pod0X@gmail.com | C1sco@12345 |
| X is your POD number | |



The screenshot shows the Cisco Umbrella interface. On the left, a dark sidebar lists 'Core Identities' (Networks, Network Devices, Roaming Computers, Mobile Devices, Chromebook Users, Network Tunnels, Web Users and Groups) and 'Configuration' (Domain Management, Sites and Active Directory, Internal Networks, Root Certificate). The 'Sites and Active Directory' option is highlighted with a red box. At the top right, there's a 'Admin' section with a 'Cisco' logo and 'API Keys'. Below it, a message says: 'Cisco Umbrella generates authentication keys for several software, Umbrella-enabled devices, and Cisco network type of integration key you need.' A table lists an 'Umbrella Management' entry with a 'Key: 8cbbd34d46'. To the right, two sections are partially visible: 'Documentation' (with a sub-instruction about authentication setup) and 'Our Le...' (with a note about different auth types).

Cisco Umbrella

Core Identities

- Networks
- Network Devices
- Roaming Computers
- Mobile Devices
- Chromebook Users
- Network Tunnels
- Web Users and Groups

Configuration

- Domain Management
- Sites and Active Directory
- Internal Networks
- Root Certificate

Admin

API Keys *i*

Cisco Umbrella generates authentication keys for several software, Umbrella-enabled devices, and Cisco network type of integration key you need.

| | |
|---------------------|--------------------|
| Umbrella Management | Key: 8cbbd34d46 |
|---------------------|--------------------|

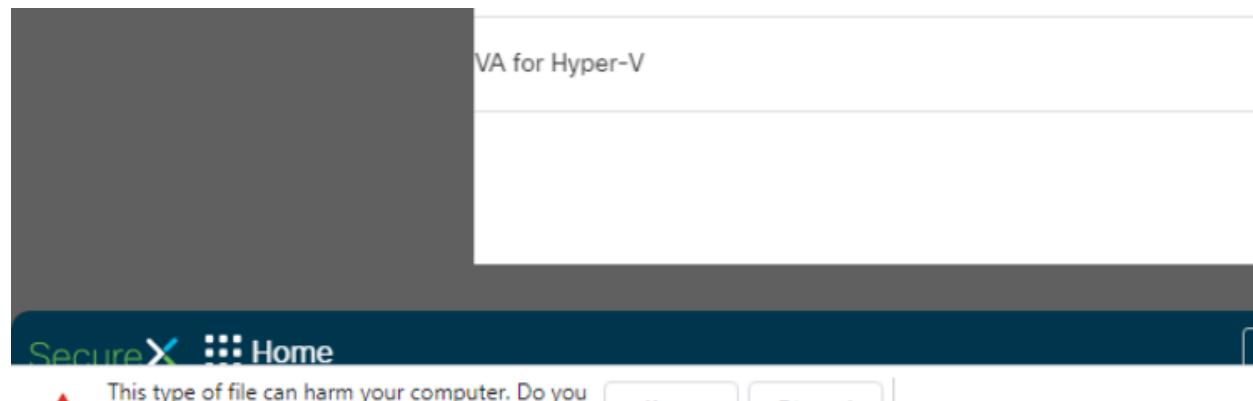
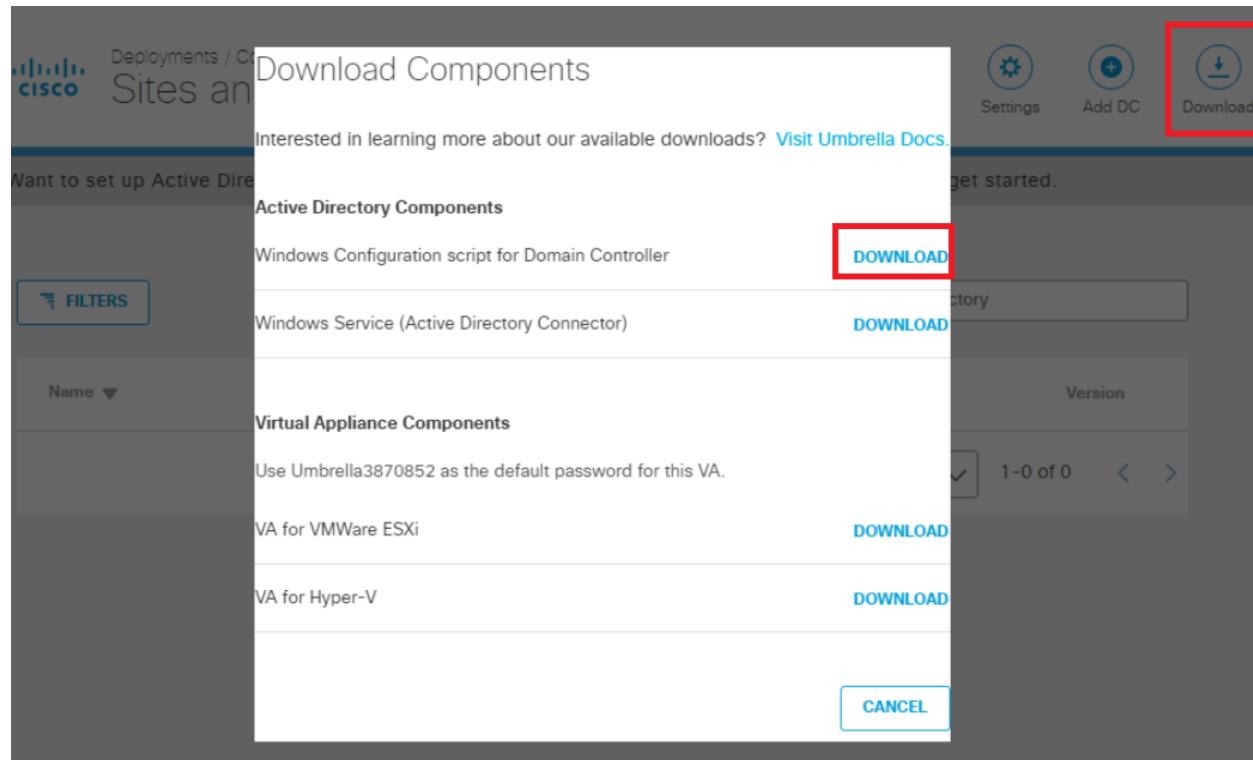
Documentation

Read here to get authentication set up for your first endpoint queries, explore what you can do and search for any answers you need.

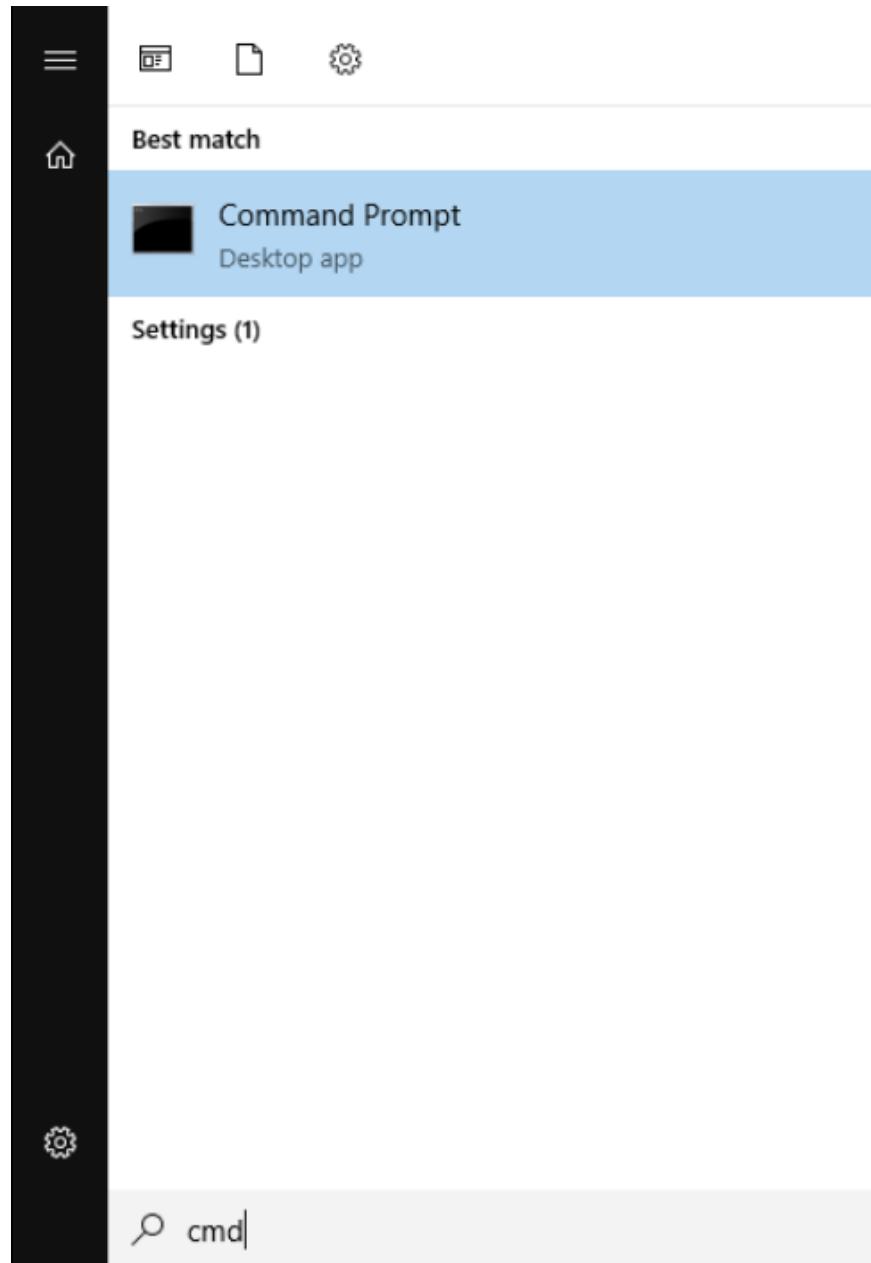
Our Le...

Some of our integration keys are different auth types than what you may have used and have unique requirements.

2. Click on the **Download** button in the top right-hand corner and download the **Windows Configuration script for Domain Controller**. Choose to **Keep** the file, if prompted (browser specific)



3. Click on Start and search for **cmd**. Click on the Command Prompt App



4. Type `cd Downloads` to access the Downloads folder and hit Enter. Enter the `cscript` command, followed by the Configuration File you just downloaded. The file name will be different from what is shown below - enter the name of the configuration file downloaded by you (type `cscript OpenDNS` and hit Tab on the keyboard - the name will auto complete) and hit **Enter**

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd Downloads

C:\Users\Administrator\Downloads>cscript OpenDNS-WindowsConfigurationScript-2020-07-06.wsf
```

Configuration Script name will vary

5. Enter 2 when asked to Enter the IP to be used. We will be using the 10.30.10.50 IP. This is the IP that will show up on Umbrella. Proceed through the script by Entering y for any other prompts that show up

```
Multiple IPs detected
1) 10.2.1.183
2) 10.30.10.50

Please enter the number of the IP you would like to use: 2
```

Administrator: Command Prompt - cscript OpenDNS-WindowsConfigurationScript-2020-07-06.wsf

```
OpenDNS_Connector member of Group DN : CN=Distributed COM Users,CN=BuiltIn,DC=s  
DCOM Group Domain : CN=Distributed COM Users,CN=BuiltIn,DC=swatsdwanlab,DC=com  
OpenDNS_Connector member of Group DN : CN=Enterprise Read-only Domain Controller  
OpenDNS_Connector member of Group DN : CN=Event Log Readers,CN=BuiltIn,DC=swats  
OpenDNS_Connector member of Group DN : CN=Distributed COM Users,CN=BuiltIn,DC=s
```

```
*****
```

Local Platform Configuration

```
Local OS: Windows Server 2019  
Functional Level: Server 2016 Forest  
Local IP: 10.30.10.50  
Domain: swatsdwanlab.com (SWATSDWANLAB)  
Label: AD  
Firewall Enabled: True
```

```
Remote Admin Enabled: False  
AD User Exists: True  
RDC Permissions Set: False  
WMI Permissions Set: False
```

```
Audit Policy Set: True  
Manage Event Log Policy Set: False
```

```
Event Log Readers MemberOf: True  
Distributed COM MemberOf: True  
*****
```

```
Your platform is supported for auto-configure.  
Do you want us to auto configure this Domain Controller (y or n)? y
```

```
Configuring system...  
Setting Remote Admin permissions on firewall...  
Setting WMI permissions...  
Setting RDC permissions...  
RDC Permissions Set: True  
Auto Config complete in full!
```

```
Would you like to register this Domain Controller (y or n)? y
```

6. The configuration script should complete successfully

```
Would you like to register this Domain Controller (y or n)? y
Registering Domain Controller in cloud...
Register Success!
Updating DC status in cloud...
Update success!
```

```
C:\Users\Administrator\Downloads>
```

7. Head over to the Umbrella page and refresh the Sites and Active Directory page. The DC just added should show up.
The status sometimes takes an hour to get updated

The screenshot shows the 'Sites and Active Directory' section of the Cisco Umbrella interface. At the top, there are navigation icons for Deployments / Configuration, Settings, Add DC, and Download. A message encourages setting up Active Directory integration or deploying Virtual Appliances. Below this is a search bar labeled 'Search Sites and Active Directory'. A table lists one Domain Controller entry:

| Name | Internal IP | Site | Type | Status | Version |
|---------------------|-------------|--------------|-------------------|-------------------|---------|
| AD.swatsdwanlab.com | 10.30.10.50 | Default Site | Domain Controller | Run: a minute ago | --- |

At the bottom of the table, pagination controls show 'Page: 1' and 'Results Per Page: 10', indicating 1 result on 1 page.

Task List

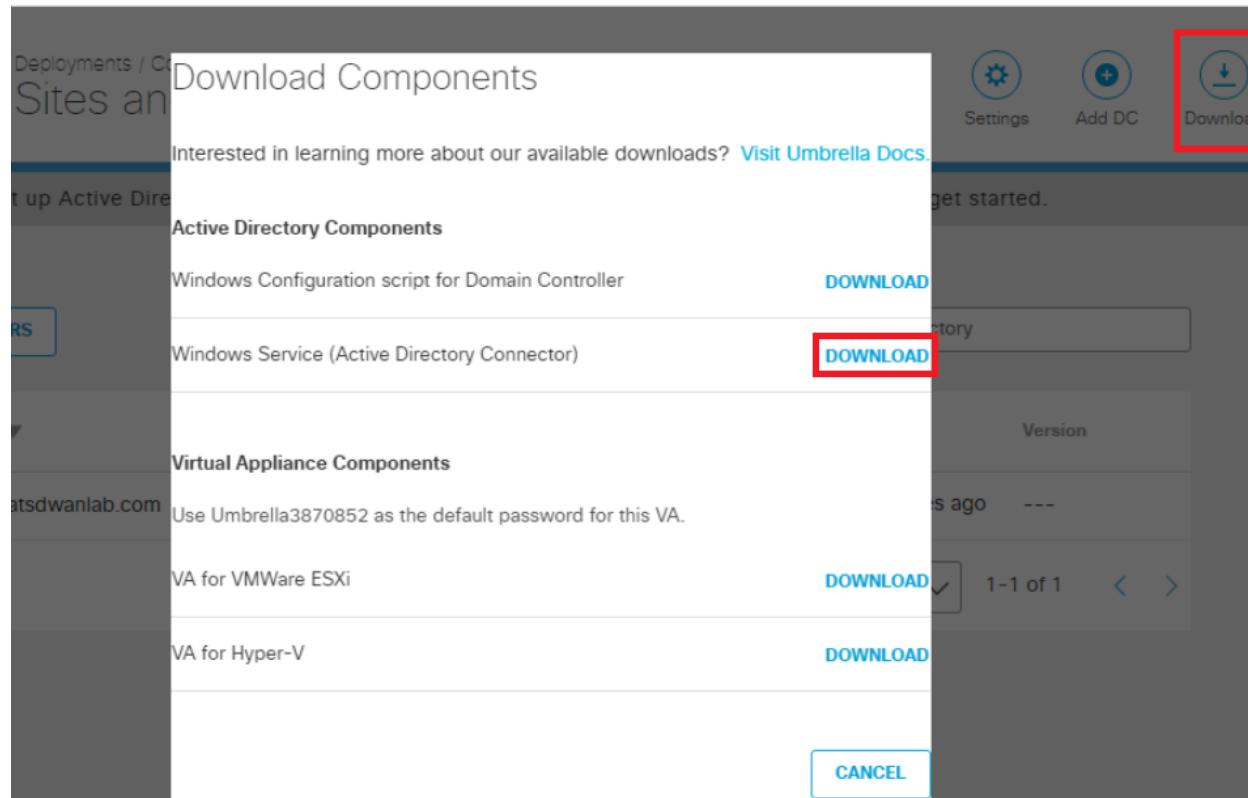
- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - [API Keys and AD Configuration](#)
 - [DC Configuration Download](#)

- AD Connectors
- Roaming Computer Configuration
- Building a DNS Policy
- Setting up IPSEC Tunnels
- Configuring a Firewall Policy
- Configuring a Web Policy

AD Connectors

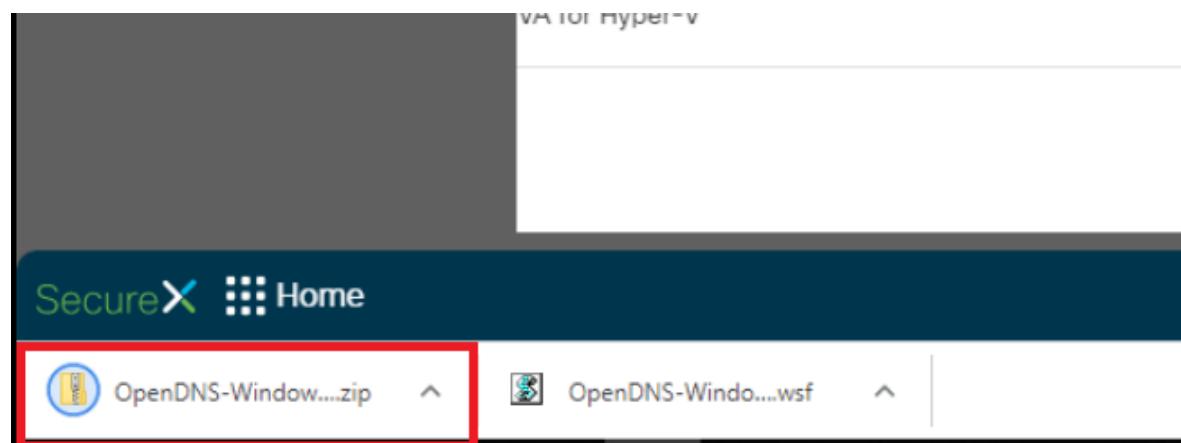
AD Connectors allow Umbrella to see your AD structure and reference AD Groups/Users in Policies.

1. From the AD PC, make sure you are logged in to Umbrella and navigate to **Deployment => Configuration => Sites and Active Directory**. Click on the **Download** button in the top right-hand corner and download the **Windows Service (Active Directory Connector)**

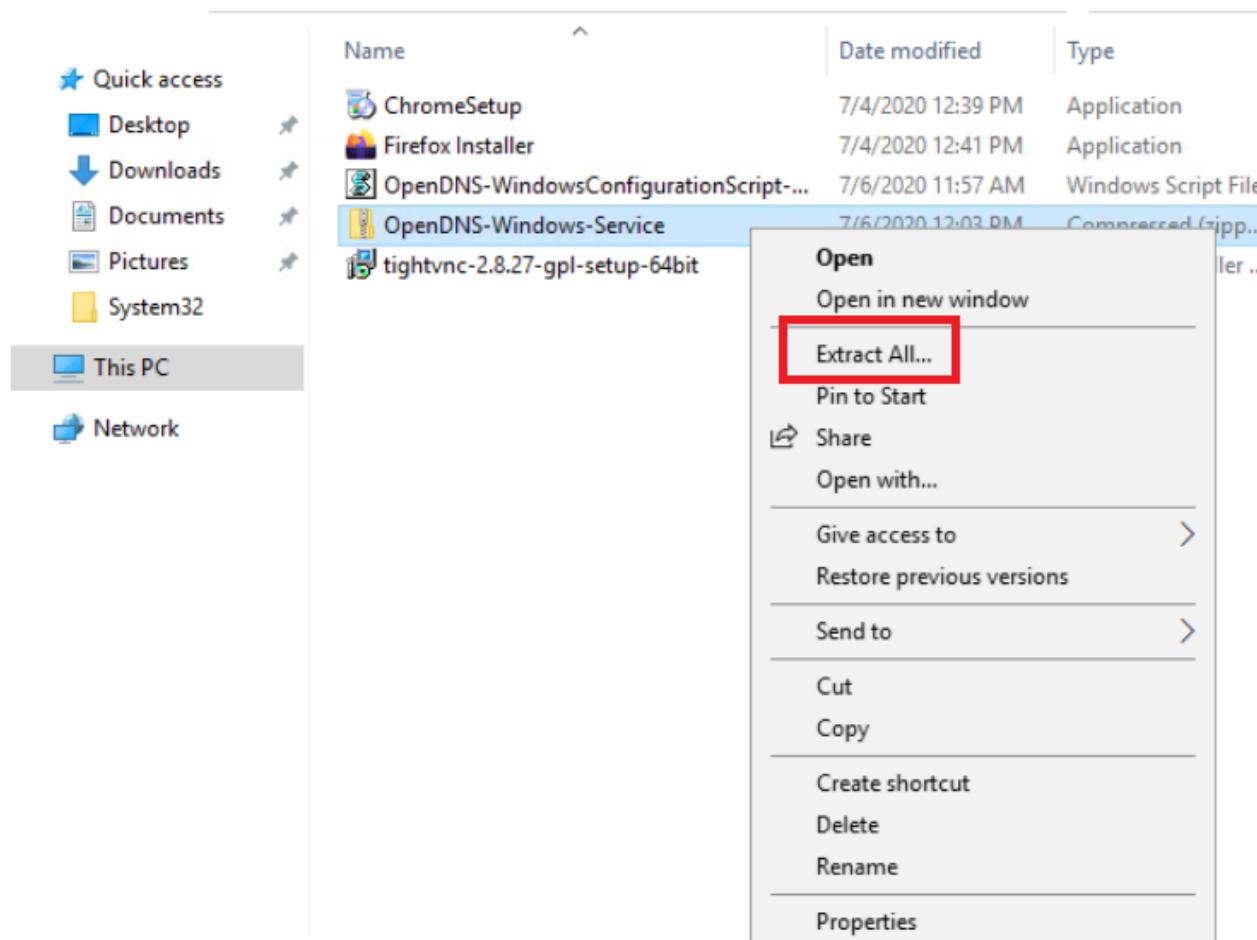


2. This will download a .zip file named *OpenDNS-Windows-Service.zip*. Click on the up arrow next to the downloaded file and choose to Open File Location (browser specific - Firefox has a folder icon in the list of downloads which takes you

to the location)



3. Right click on the file and choose **Extract All**



4. The file will be extracted to the path shown in the image by default. Click on **Extract**



← Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

C:\Users\Administrator\Downloads\OpenDNS-Windows-Service

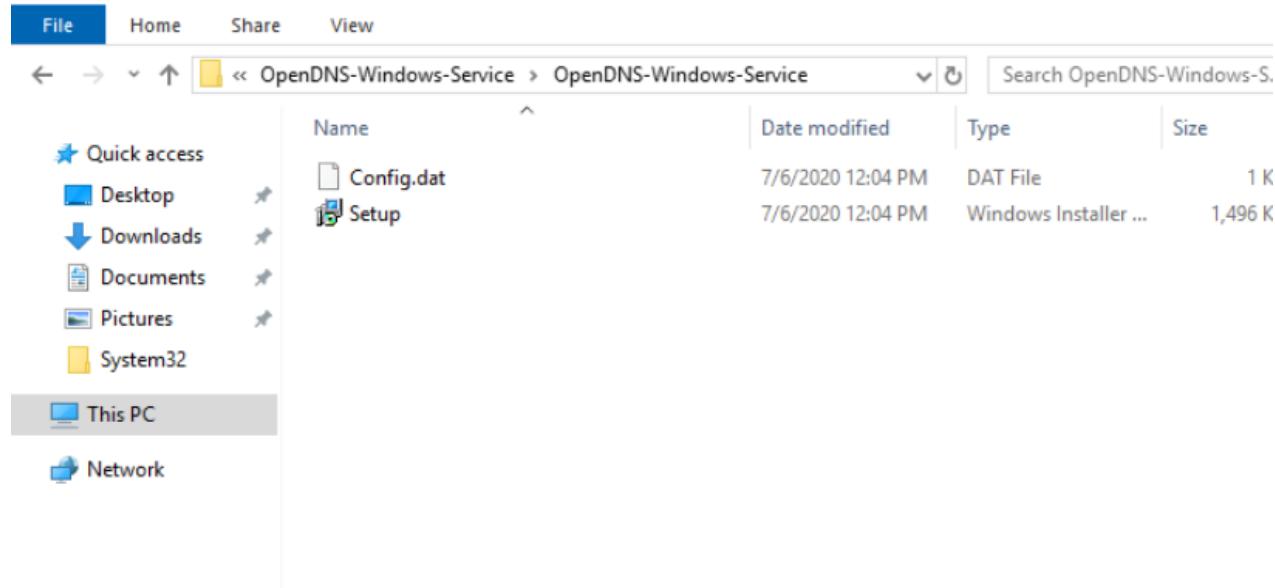
[Browse...](#)

Show extracted files when complete

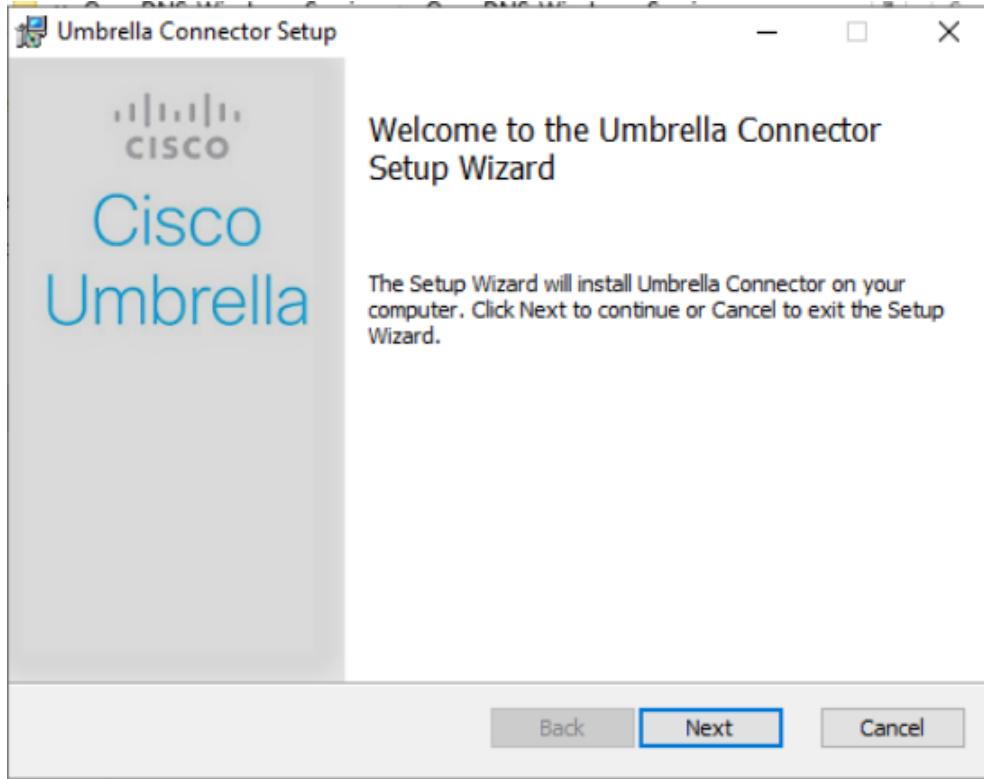
[Extract](#)

[Cancel](#)

- Once extracted, the contents of the .zip will open in a new window. Double click **Setup** to start the AD Connector Installer



6. Click on **Next** at the Welcome and Destination folder screens. Enter a password of **C1sco12345**, leaving the Username at the default of *OpenDNS_Connector*. These should match with the user we created in Active Directory.
Click on **Next**



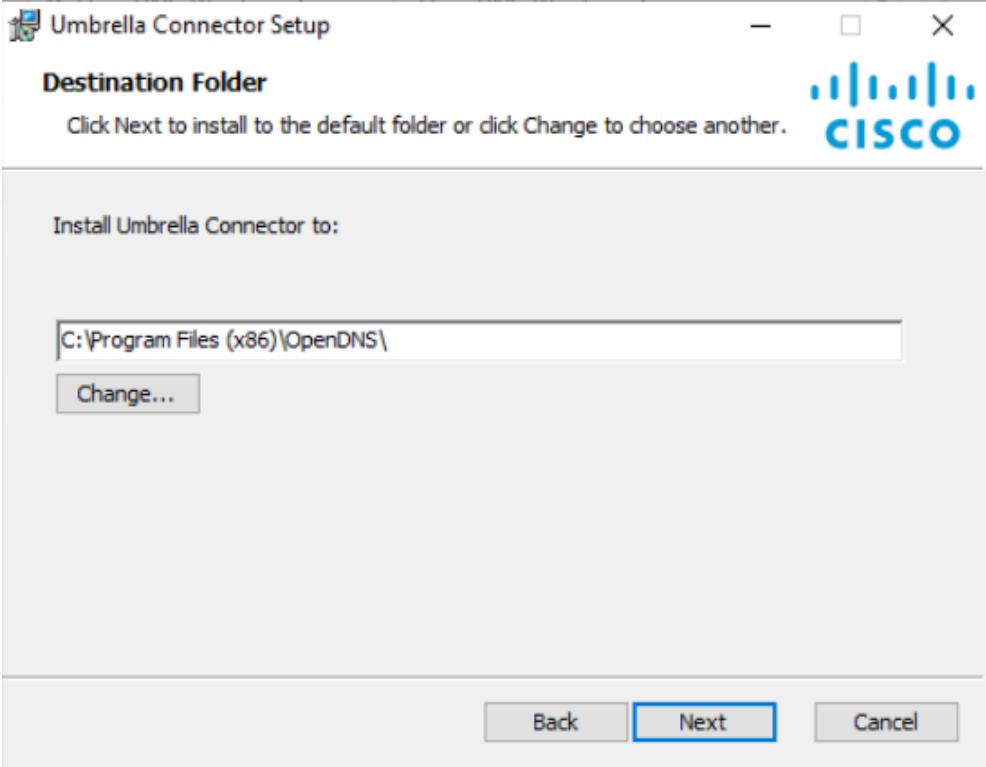
Welcome to the Umbrella Connector Setup Wizard

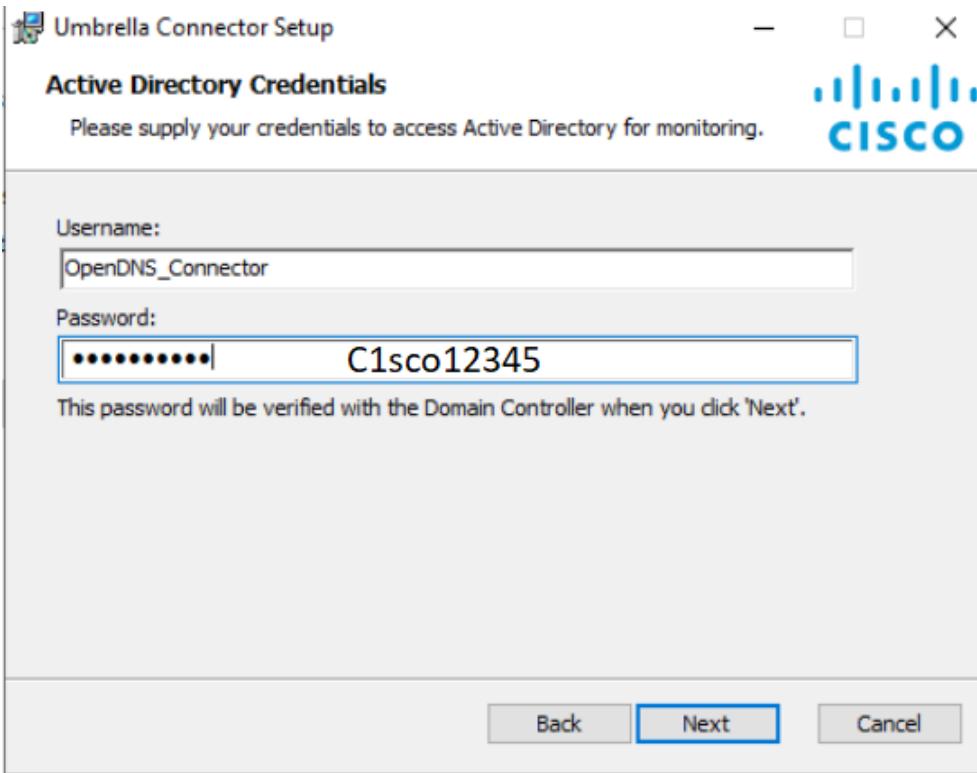
The Setup Wizard will install Umbrella Connector on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Back

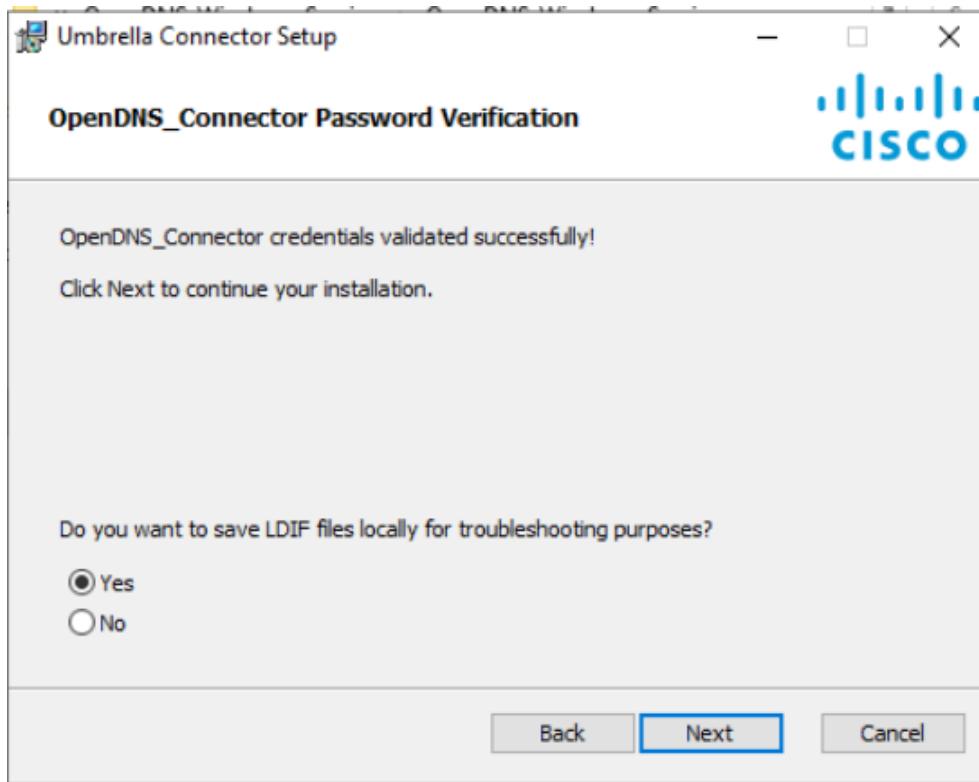
Next

Cancel





7. The credentials should be validated successfully. Click on **Next**



8. Click on **Install** to begin the installation and **Finish** once the installation is complete



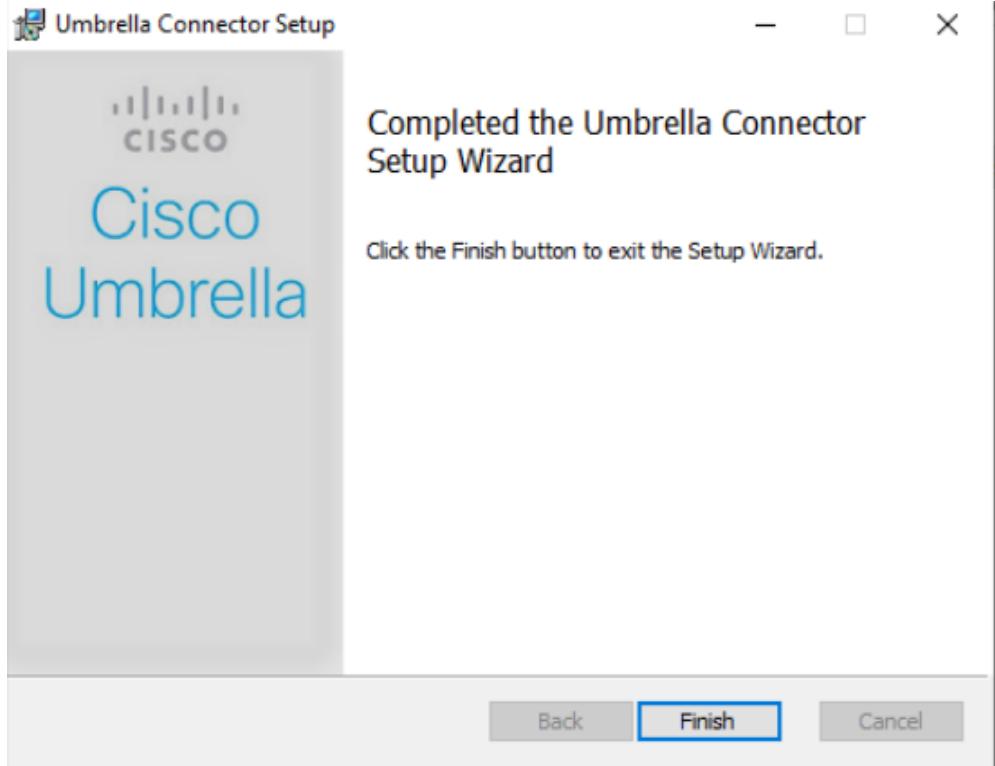
Ready to install Umbrella Connector

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

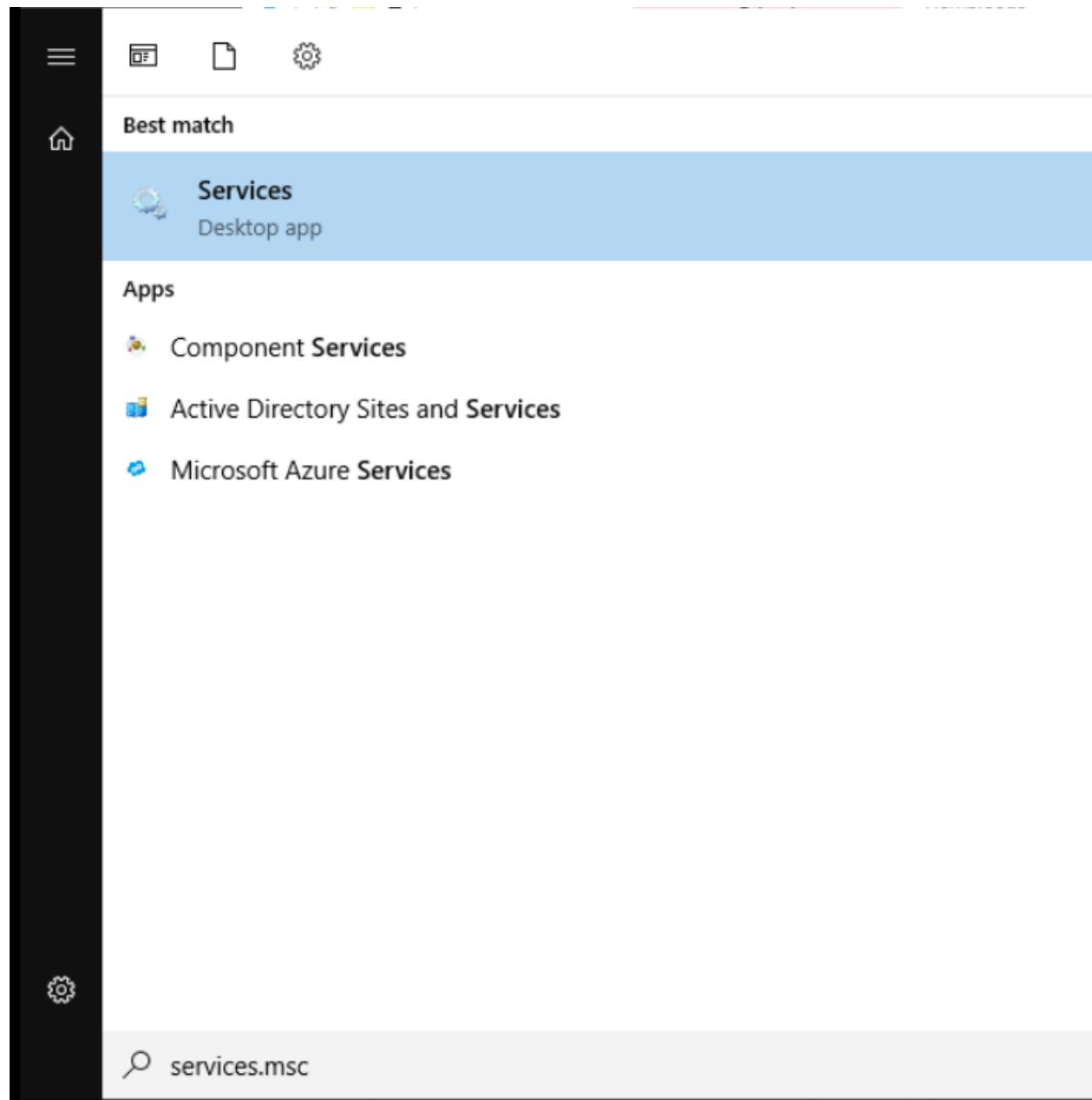
Back

Install

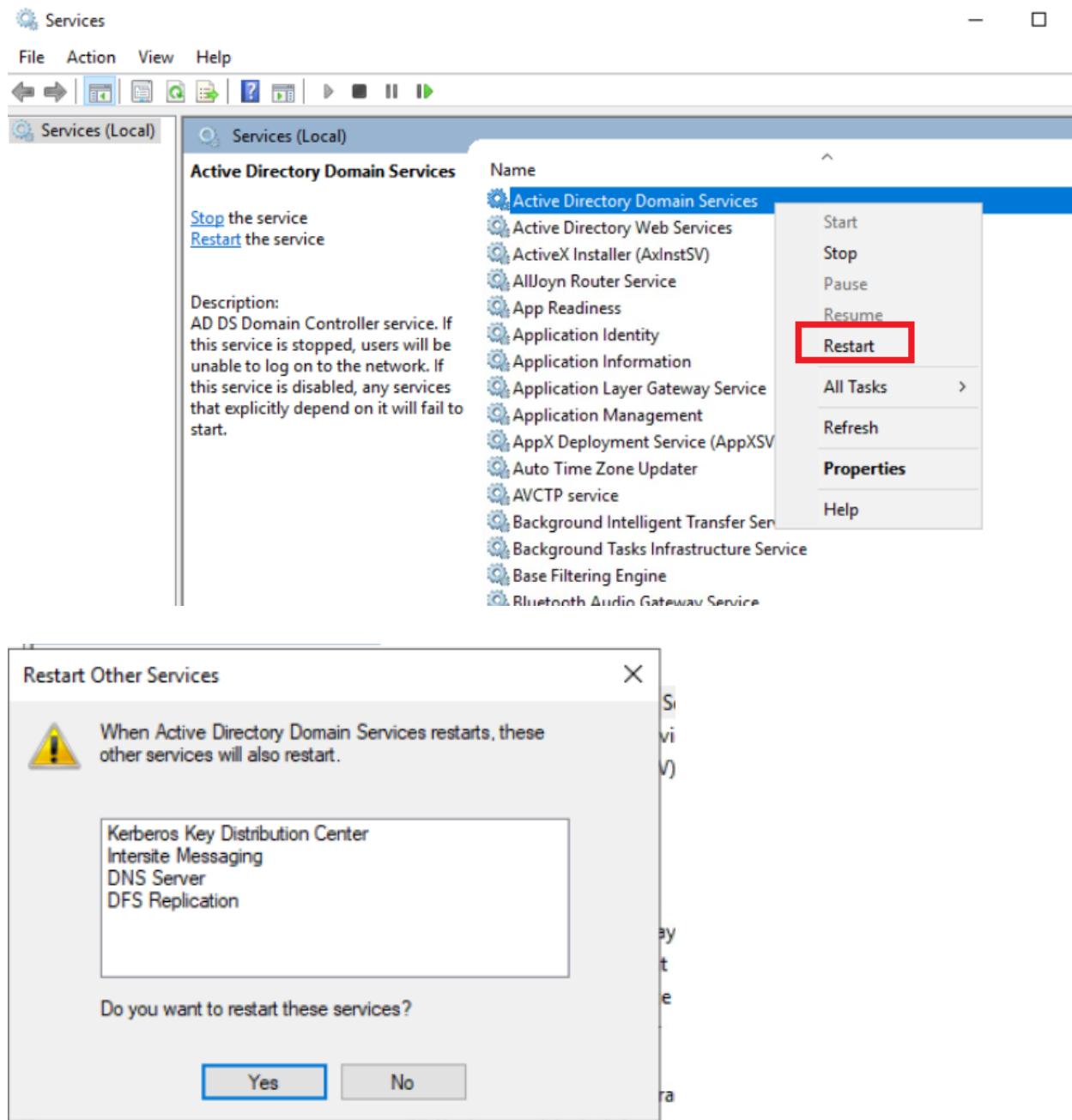
Cancel



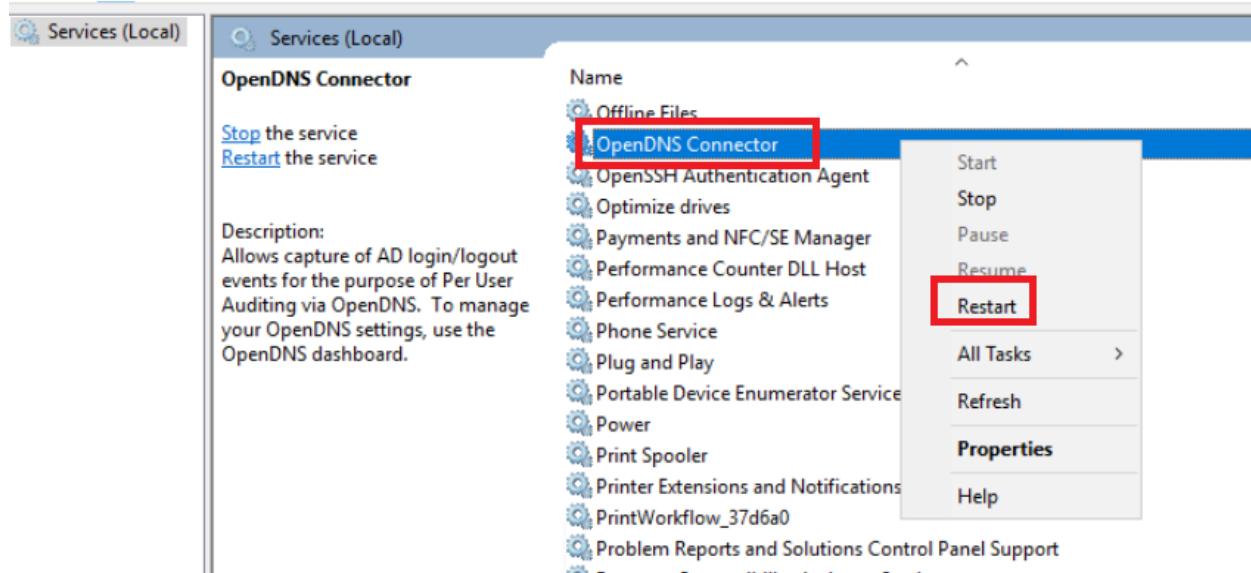
9. On the AD PC, click on Start and search for `services.msc`. Click on the **Services** Desktop app



10. Right click on **Active Directory Domain Services** and choose to *Restart* the service. Select **Yes** to restart other related services as well



11. Once the services have restarted, locate the **OpenDNS Connector** service. Right click it and *Restart* this service as well



12. Head over to Umbrella and navigate to **Deployments => Configuration => Sites and Active Directory**. Refresh the page if you're already on it and the AD Connector will show up over there. Don't worry if you don't see a green check mark (it takes time to reflect correctly)

The screenshot shows the Cisco Umbrella GUI for 'Sites and Active Directory'. At the top, there's a navigation bar with tabs for 'Sites and Active Directory' and a search bar. Below the header, a message encourages setting up Active Directory integration or deploying Virtual Appliances. A 'Download' button is available above the main table. The main area contains a table with columns: Name, Internal IP, Site, Type, Status, and Version. Two entries are listed:

| Name | Internal IP | Site | Type | Status | Version |
|---------------------|-------------|--------------|-------------------|--------------------------|---------|
| AD.swatsdwanlab.com | 10.30.10.50 | Default Site | Domain Controller | Run: 9 minutes ago | --- |
| ad.swatsdwanlab.com | 10.30.10.50 | Default Site | AD Connector | Installed: 3 minutes ago | 1.5.1 |

At the bottom, there are pagination controls (Page: 1, Results Per Page: 10, 1-2 of 2) and navigation arrows.

13. On the Umbrella GUI, go to **Policies => Management => DNS Policies** and click on **Add** to create a new DNS Policy. We won't be adding the policy right now but will just check if our AD schema is visible on Umbrella

The screenshot shows the Cisco Umbrella GUI under the 'Management' section, specifically the 'DNS Policies' page. The left sidebar has a red box around the 'DNS Policies' item. The main content area has a heading 'DNS Policies' with an 'Add' button highlighted by a red box. Below the heading is a descriptive text about policies. A table at the bottom lists one policy: 'Default Policy'.

| Protection | Applied To | Contains |
|------------|----------------|----------|
| DNS Policy | All Identities | 3 Policy |

14. Click on **Next**

Create or modify lists to explicitly block or allow destinations. Note: global block and global allow destination lists are applied by default.

Application Control

Block or allow access to applications individually or by group.

Block Threats

Secure your network and endpoints using a variety of antimalware engines and threat intelligence.

Security Category Blocking

Ensure domains are blocked when they host malware, command and control, phishing, and more.

File Analysis

Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

IP-Layer Enforcement

Block threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for roaming computer identities.

► Advanced Settings

CANCEL

NEXT

15. You should see **AD Groups** and **AD Users** under *All Identities*, with a number next to it (13 and 3 respectively in this screenshot). A number is an indication that Umbrella can now see our AD configuration

What would you like to protect?

Select Identities

Search Identities

All Identities

-  AD Groups 13 >
-  AD Users 3 > **Red Box**
-  AD Computers 2 >
-  Networks
-  Roaming Computers
-  Sites 1 >

0 Selected

16. Click on **AD Users** (click on the word AD Users, don't click on the checkbox next to it) and you will see 3 Users, imported from AD indicating that AD and Umbrella have been successfully linked. Click on **Cancel**

What would you like to protect?

Select Identities

Search Identities

All Identities / AD Users

-  Administrator (Administrator@swa...)
-  OpenDNS_Connector (OpenDNS_...)
-  sdwan (sdwan@swatsdwanlab.com) **Red Box**

0 Selected

Click on Cancel after
checking the AD user

This completes the configuration needed for linking AD with Umbrella. While we can reference the AD Groups/Users in our DNS Policies, it is possible to become even more granular and link individual workstations to Umbrella, thereby

encompassing the remote workers use case. We will configure this in the next section.

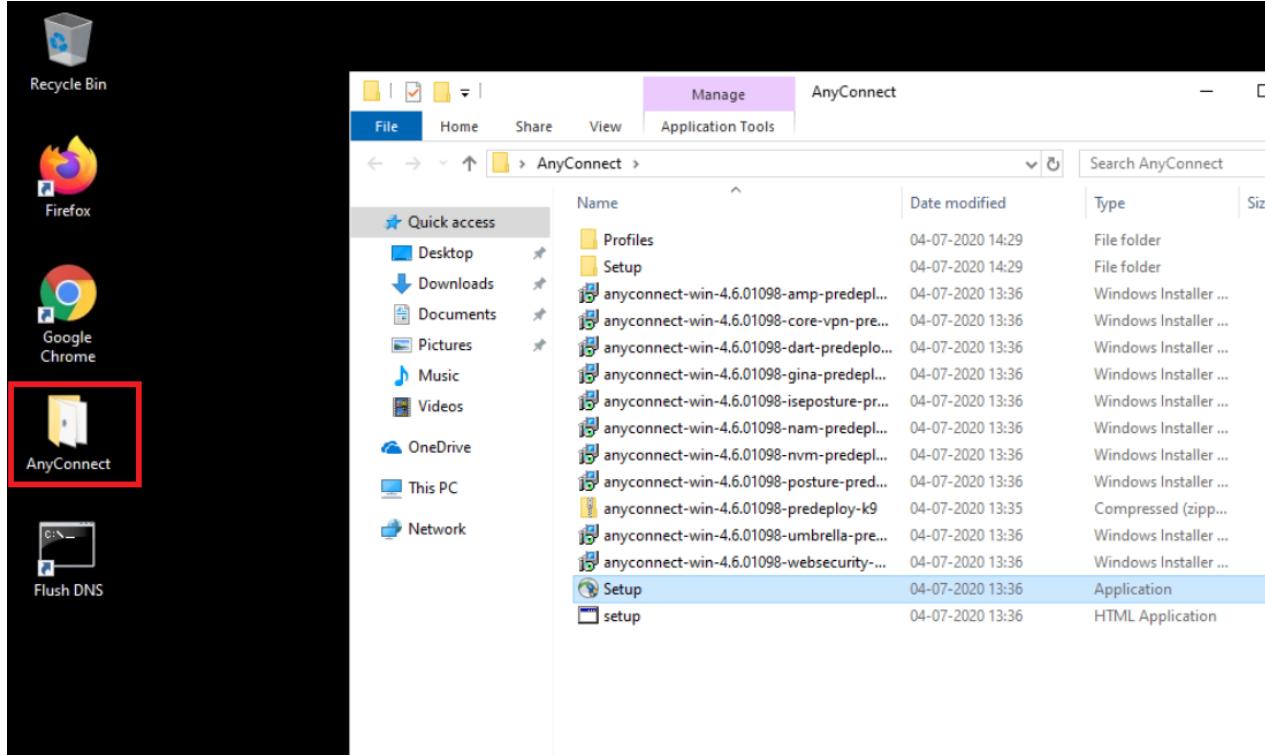
Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - [API Keys and AD Configuration](#)
 - [DC Configuration Download](#)
 - [AD Connectors](#)
 - [Roaming Computer Configuration](#)
- [Building a DNS Policy](#)
- [Setting up IPSEC Tunnels](#)
- [Configuring a Firewall Policy](#)
- [Configuring a Web Policy](#)

Roaming Computer Configuration

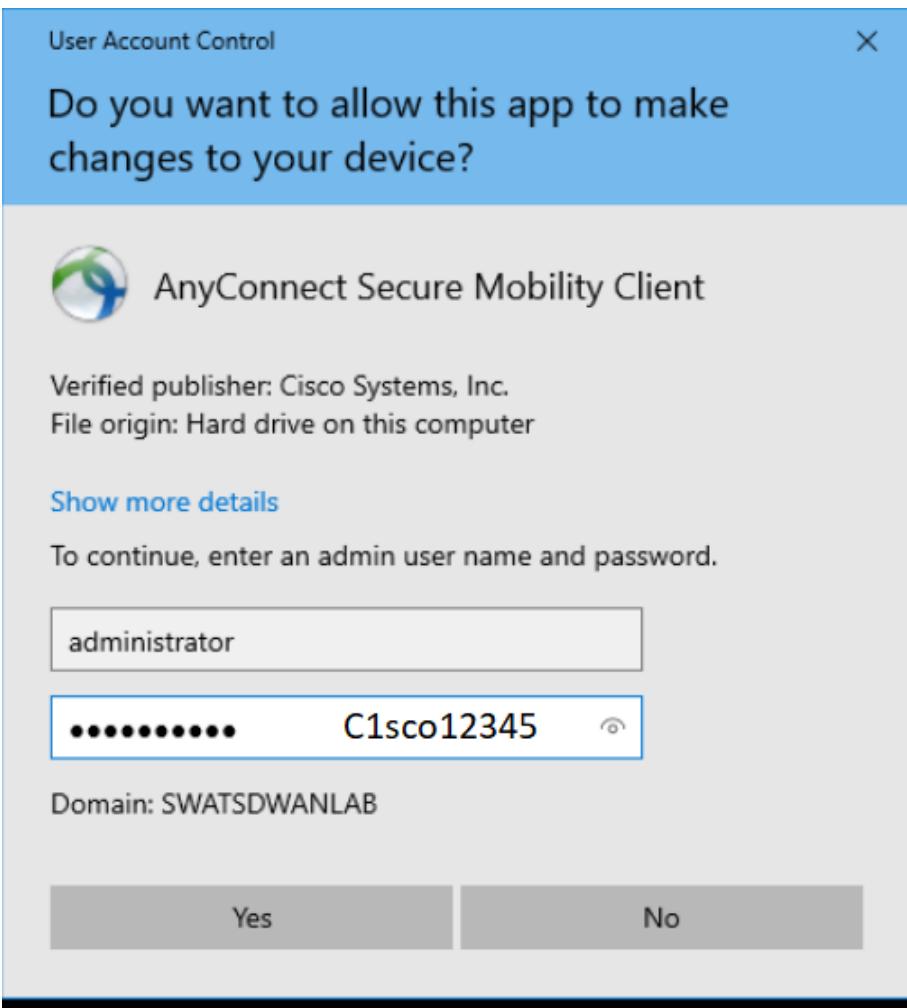
Cisco AnyConnect is used to identify Roaming Computers and include them within our DNS Policies. This is what will be leveraged in our lab environment to build and apply a DNS Policy.

1. Access the Site 30 PC via your preferred method (Guacamole/RDP/vCenter Console) and log in. [Click here](#) and go through Step 1 to review how to connect to the Site 30 PC. Open the **AnyConnect** folder on the Desktop and double-click **Setup** to start installing AnyConnect

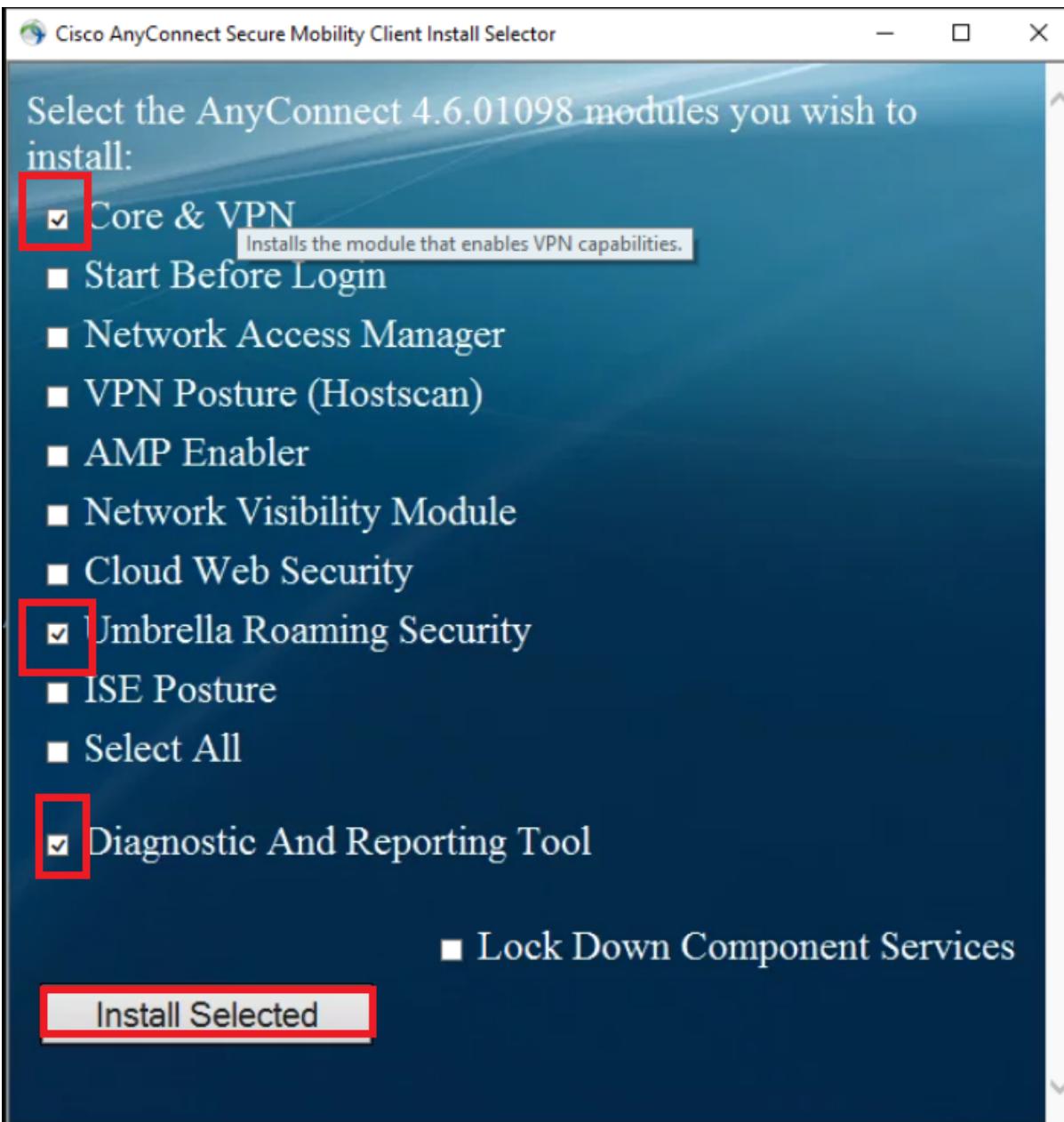


2. Enter the following credentials when prompted for a username/password and click on **Yes**

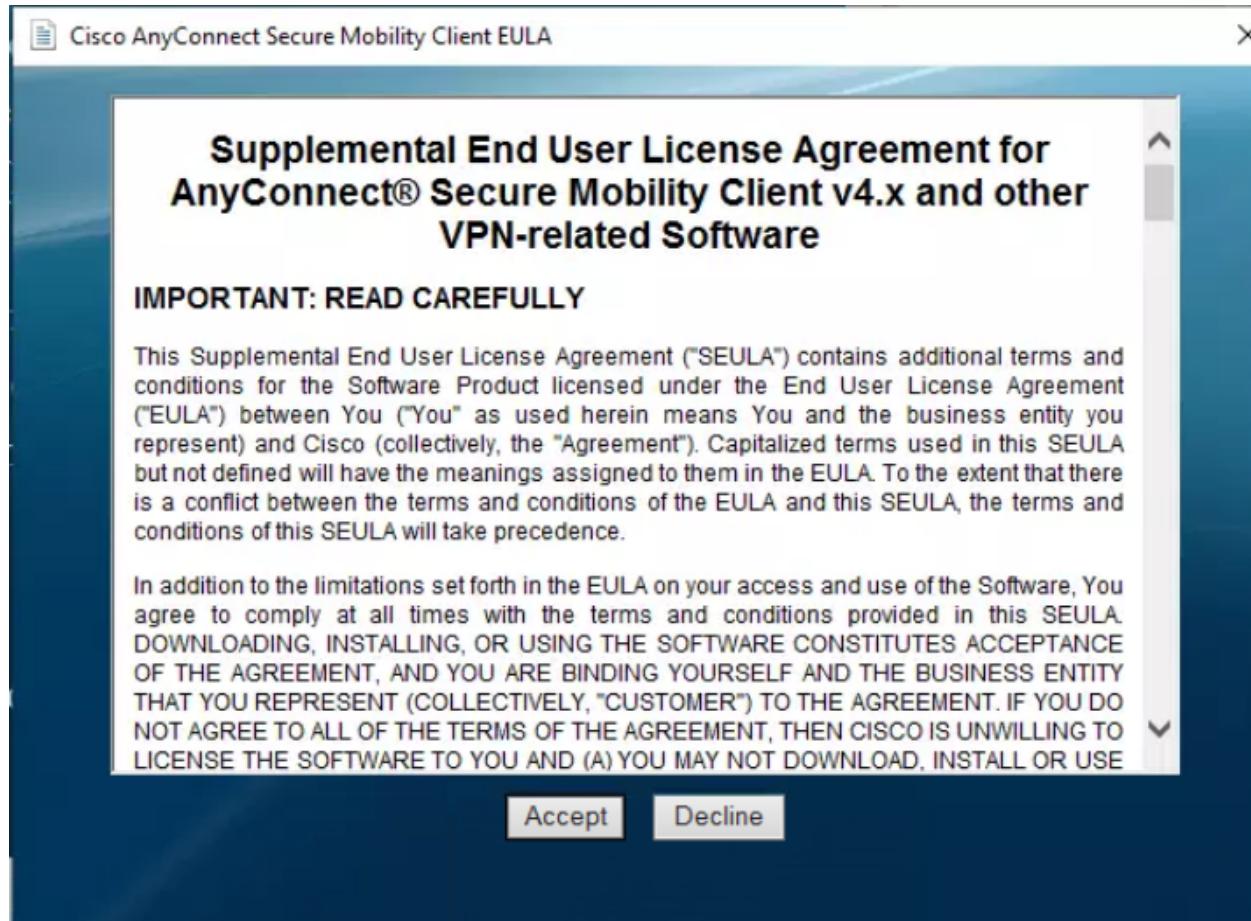
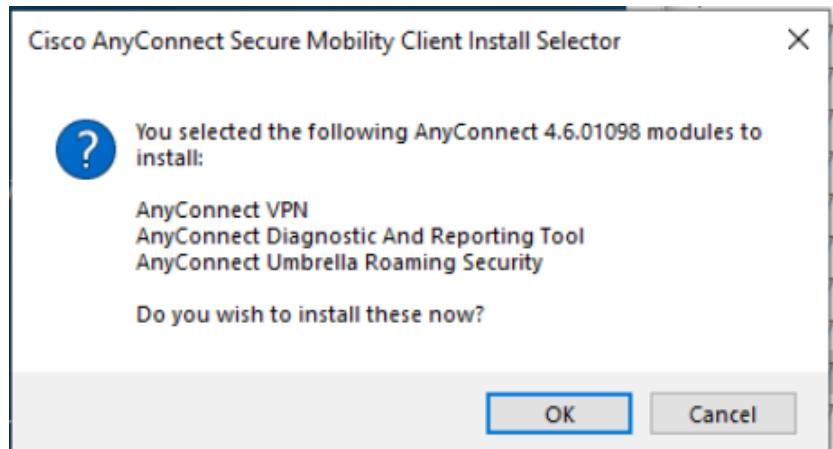
| Username | Password |
|---------------|------------|
| administrator | C1sco12345 |



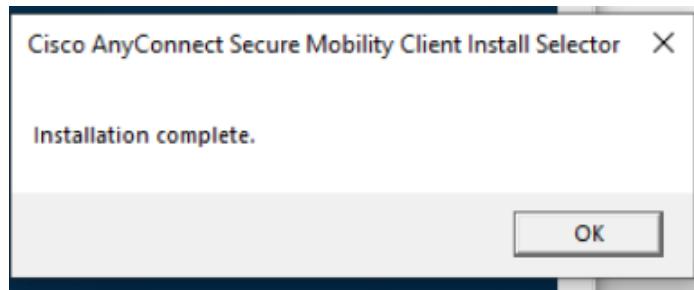
3. Remove the check mark against all modules **except Core & VPN, Umbrella Roaming Security and Diagnostic And Reporting Tool**. Click on **Install Selected** to install the selected modules



4. Click on **OK** and **Accept** the License Agreement

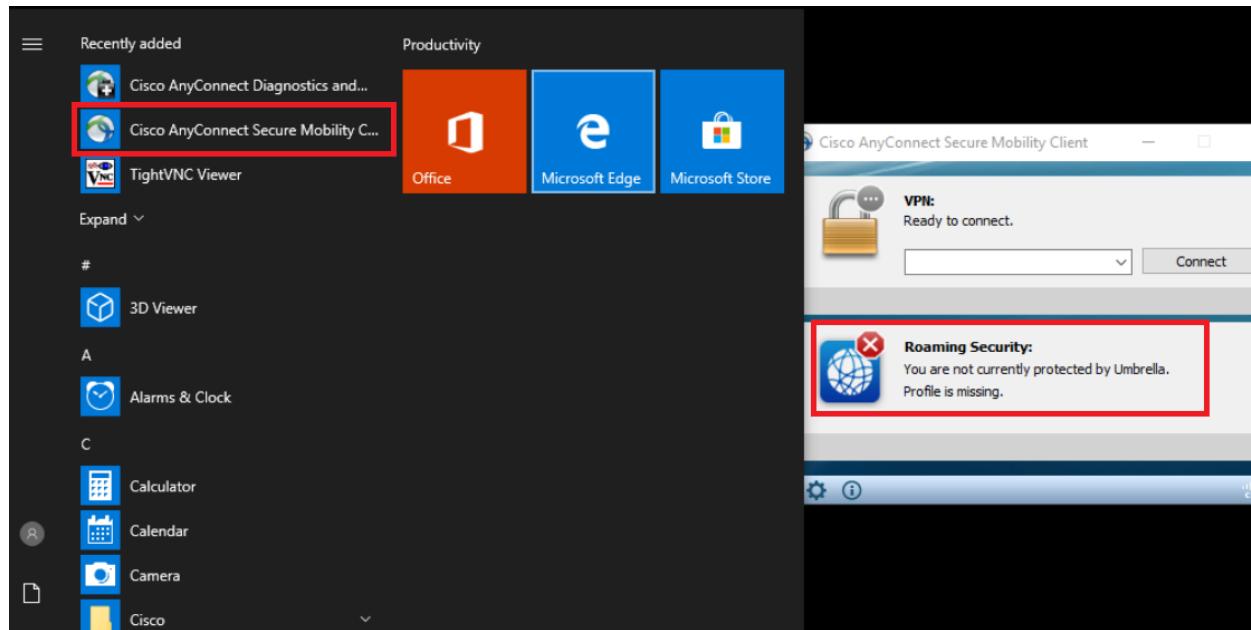


5. Once installation is complete, click on **OK**

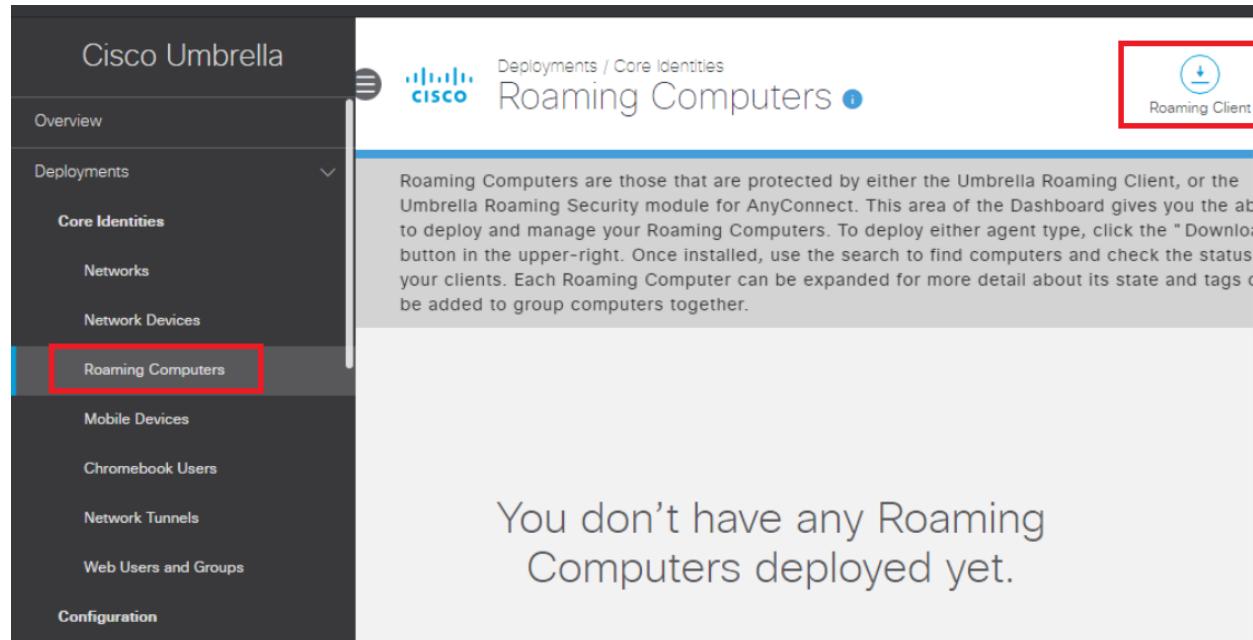


6. Open **Cisco AnyConnect Secure Mobility Client** by clicking on Start (it will show up in the *Recently Added* section).

Notice that Roaming Security is flagged as unprotected by Umbrella. We will need to copy a profile unique to our Organization so that this workstation shows up on Umbrella as a Roaming Computer



7. From the **Site 30 PC**, log in to Umbrella. [Click here](#) and reference Step 1 to review the login procedure, but make sure you log in to Umbrella via the Site 30 PC and **not** the AD PC. Go to **Deployments => Core Identities => Roaming Computers** and click on **Roaming Client** in the top right-hand corner



The screenshot shows the Cisco Umbrella dashboard. On the left, a sidebar menu lists various categories: Overview, Deployments (with Core Identities, Networks, Network Devices), Roaming Computers (which is selected and highlighted with a red box), Mobile Devices, Chromebook Users, Network Tunnels, Web Users and Groups, and Configuration. The main content area has a header "Deployments / Core Identities" and "Roaming Computers" with a blue information icon. A red box highlights the "Roaming Client" download button in the top right corner. Below it, a large message states: "Roaming Computers are those that are protected by either the Umbrella Roaming Client, or the Umbrella Roaming Security module for AnyConnect. This area of the Dashboard gives you the ability to deploy and manage your Roaming Computers. To deploy either agent type, click the "Download" button in the upper-right. Once installed, use the search to find computers and check the status of your clients. Each Roaming Computer can be expanded for more detail about its state and tags can be added to group computers together." At the bottom center, it says "You don't have any Roaming Computers deployed yet."

8. Click on **Download Module Profile**

⚠ For your [internal domains](#) to resolve, you must add them to the [internal domains list](#). It's important to add them before you deploy!

Cisco Umbrella Roaming Client



[Download Windows Client](#)

Supported Versions: Windows Vista, 7, 8, 10



[Download macOS Client](#)

Supported Versions: macOS 10.11+

AnyConnect Umbrella Roaming Security Module

Cisco AnyConnect can be configured to enable an Umbrella Roaming Security module which provides similar functionality to the roaming client. There are many deployment options, and each requires the customized profile downloaded below. [For full documentation, read here.](#)

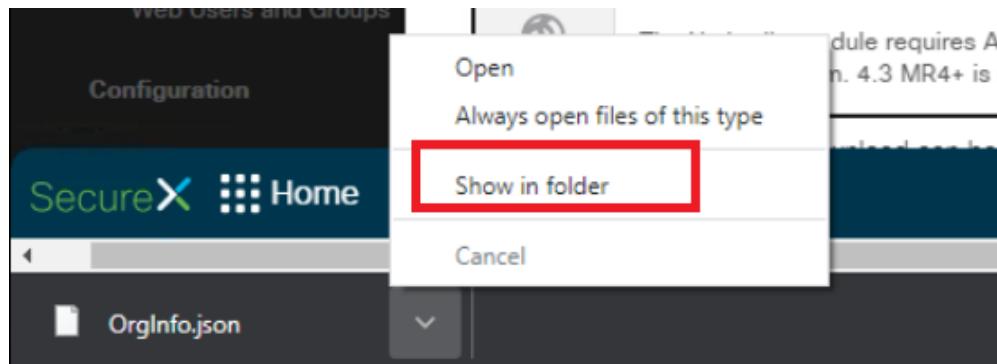


[Download Module Profile](#)

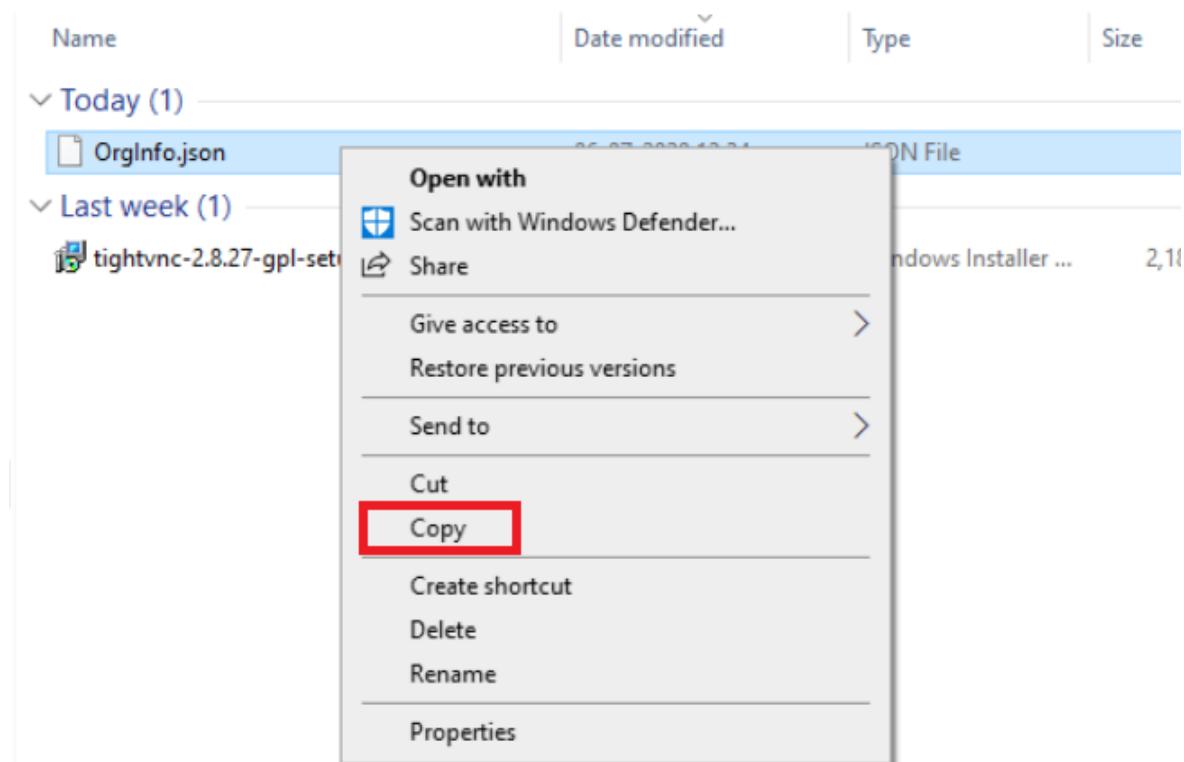
The Umbrella module requires AnyConnect for Windows or macOS, version 4.3 MR1 minimum. 4.3 MR4+ is recommended.

The AnyConnect 4.x client download can be found [here](#) (requires contract).

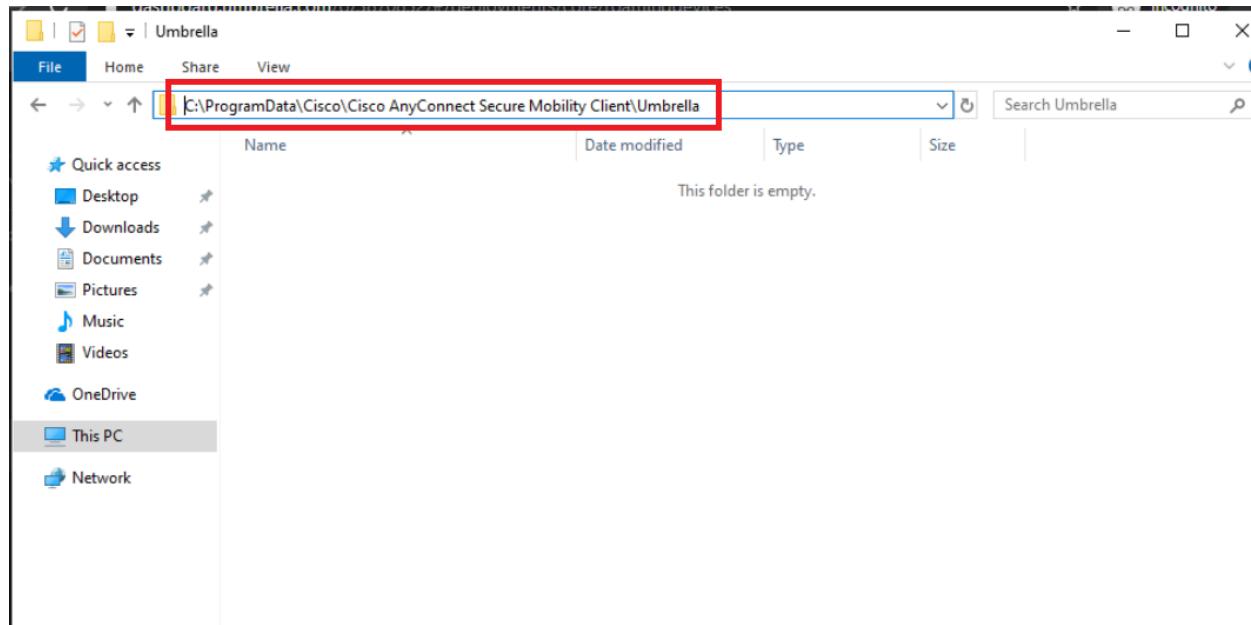
9. This will download a file called *OrgInfo.json*. Click on the arrow next to the file download and choose **Show in folder** (again, browser specific - Firefox has a folder icon to go to the download location)



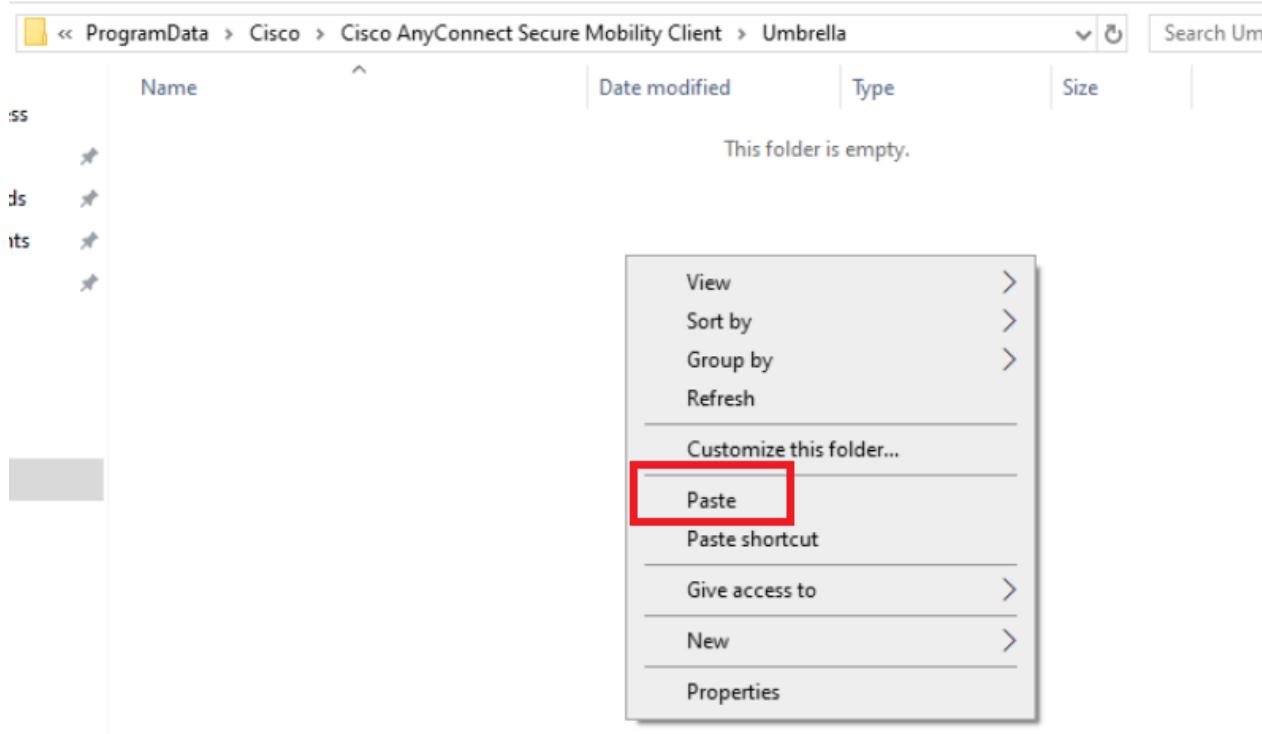
10. Right click on *OrgInfo.json* and click on **Copy**



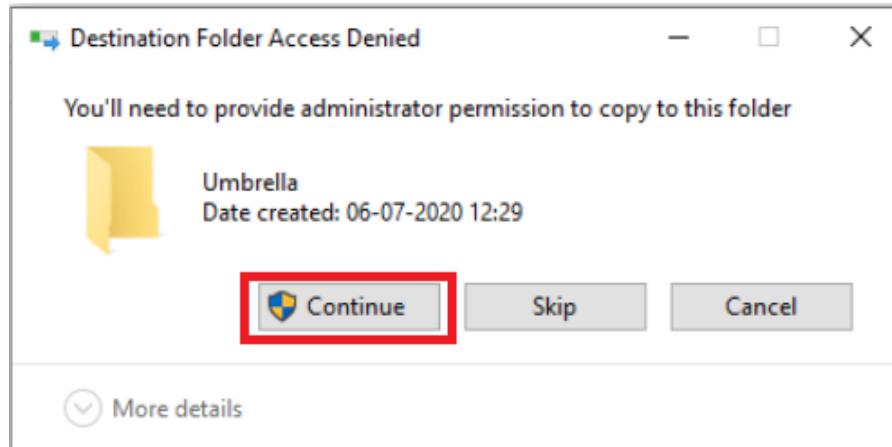
11. Open Windows Explorer and enter the following path (you will not be able to see this folder since it's hidden by default. There is an option to view hidden files and folders in Windows, but we can browse directly to the location)-
`C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella`



12. Paste the file we copied before (OrgInfo.json)

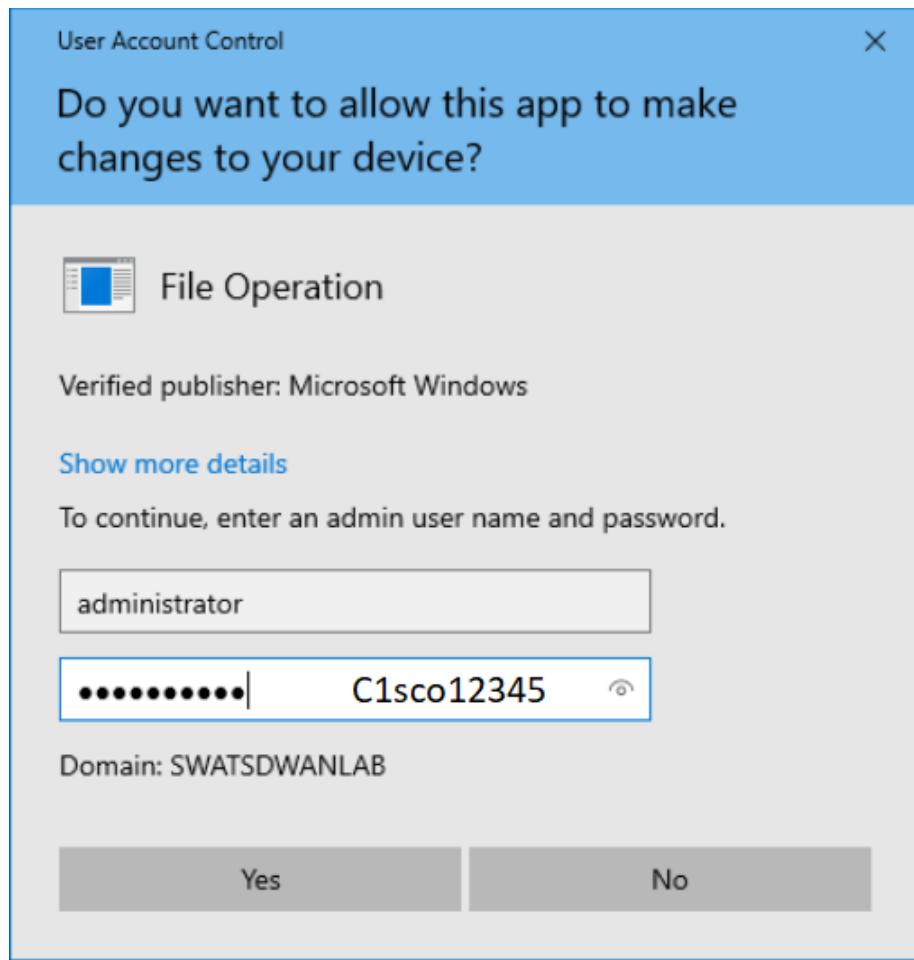


13. Click on **Continue**



14. Enter the username/password as shown below

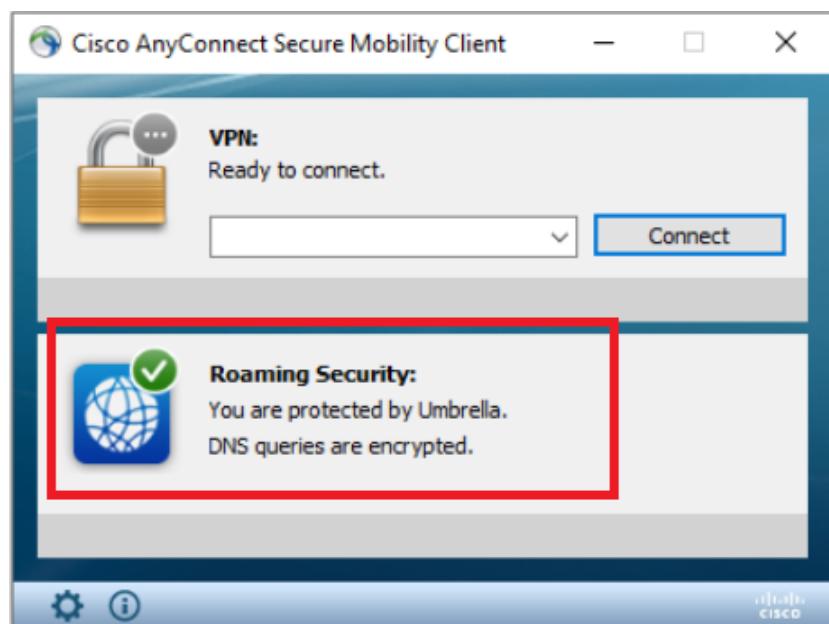
| Username | Password |
|---------------|------------|
| administrator | C1sco12345 |



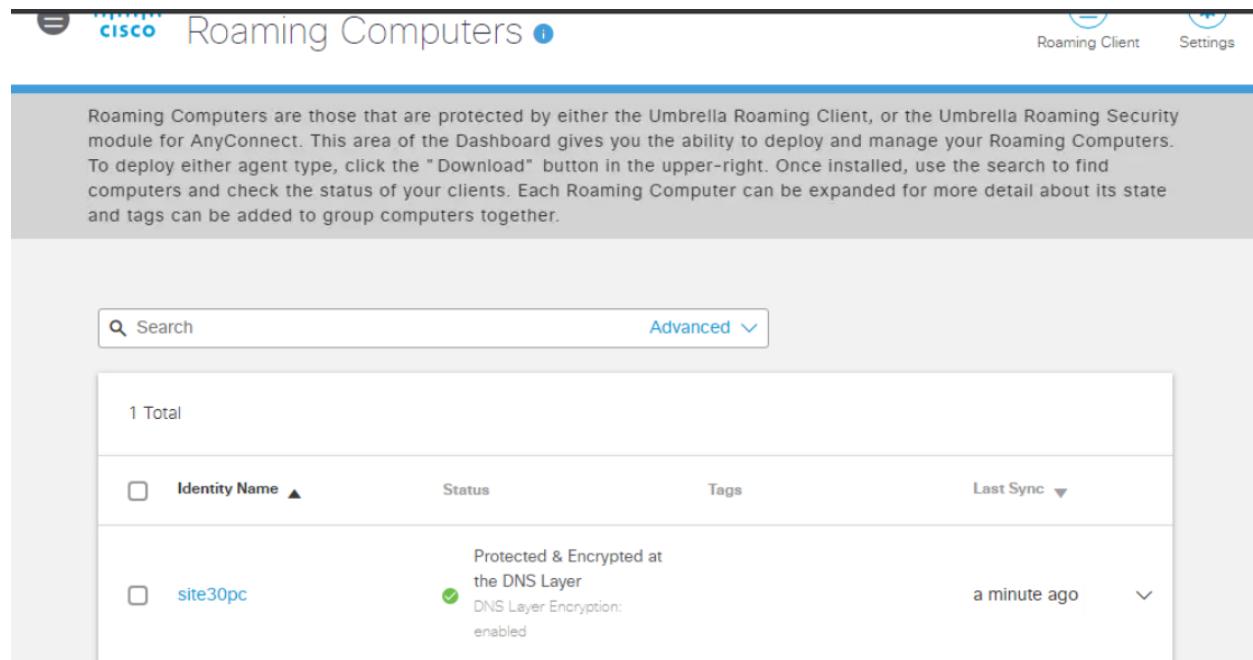
- Once the file is placed in the folder, it should auto-generate another folder called **data**. If this doesn't show up, close Cisco AnyConnect and re-open

| | Name | Date modified | Type | Size |
|--|--------------|------------------|-------------|------|
| | data | 06-07-2020 12:37 | File folder | |
| | OrgInfo.json | 06-07-2020 12:34 | JSON File | 1 KB |

16. AnyConnect should now show that you are protected by Umbrella



17. Back at the Umbrella GUI, refresh the **Roaming Computers** page. The Site 30 PC will show up as a Roaming Computer



The screenshot shows the Cisco Umbrella Roaming Computers dashboard. At the top, there's a header with the Cisco logo and the title "Roaming Computers". On the right side of the header are links for "Roaming Client" and "Settings". Below the header, a grey banner provides information about roaming computers and their protection. The main area has a search bar and an "Advanced" dropdown. A table lists one roaming computer, "site30pc", with columns for Identity Name, Status, Tags, and Last Sync. The status row indicates "Protected & Encrypted at the DNS Layer" with a green checkmark and "DNS Layer Encryption: enabled".

| | Identity Name | Status | Tags | Last Sync |
|--------------------------|---------------|---|------|--------------|
| <input type="checkbox"/> | site30pc | Protected & Encrypted at the DNS Layer ✓ DNS Layer Encryption: enabled | | a minute ago |

We will use the Roaming Computer as an Identity to enforce DNS Policies (the next section).

Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - [API Keys and AD Configuration](#)
 - [DC Configuration Download](#)
 - [AD Connectors](#)
 - [Roaming Computer Configuration](#)
- [Building a DNS Policy](#)
- [Setting up IPSEC Tunnels](#)
- [Configuring a Firewall Policy](#)
- [Configuring a Web Policy](#)

Building a DNS Policy

1. Log in to the Cisco Umbrella GUI (you can now log in from your own workstation since Umbrella is on the Cloud).

[Click here](#) and reference Step 1 to review the login procedure. Navigate to **Policies => Policy Components =>**

Destination Lists. You will notice a few default Lists already created

Cisco Umbrella

Overview

Deployments >

Policies

Management

DNS Policies

Firewall Policy

Web Policies

Policy Components

Destination Lists

Content Categories

Application Settings

Policies / Policy Components

Destination Lists

Destination Lists enable you to customize your policy to block or allow specific lists to your policies. Adding wildcards to your block or allow lists is supported, so adding domain.com will also allow or block subdomains, IP addresses and CIDR ranges for Roaming Computers with

Search...

| | Applied To | Type |
|-------------------|------------|-------|
| Global Allow List | DNS Policy | All |
| Global Block List | DNS Policy | Block |

2. Click on **Add** in the top right-hand corner and give your List a name of *BlockAmazon*. Leave the **This destination list is applied to** field at *DNS Policies*

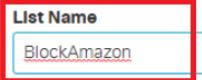
Policies / Policy Components

Destination Lists

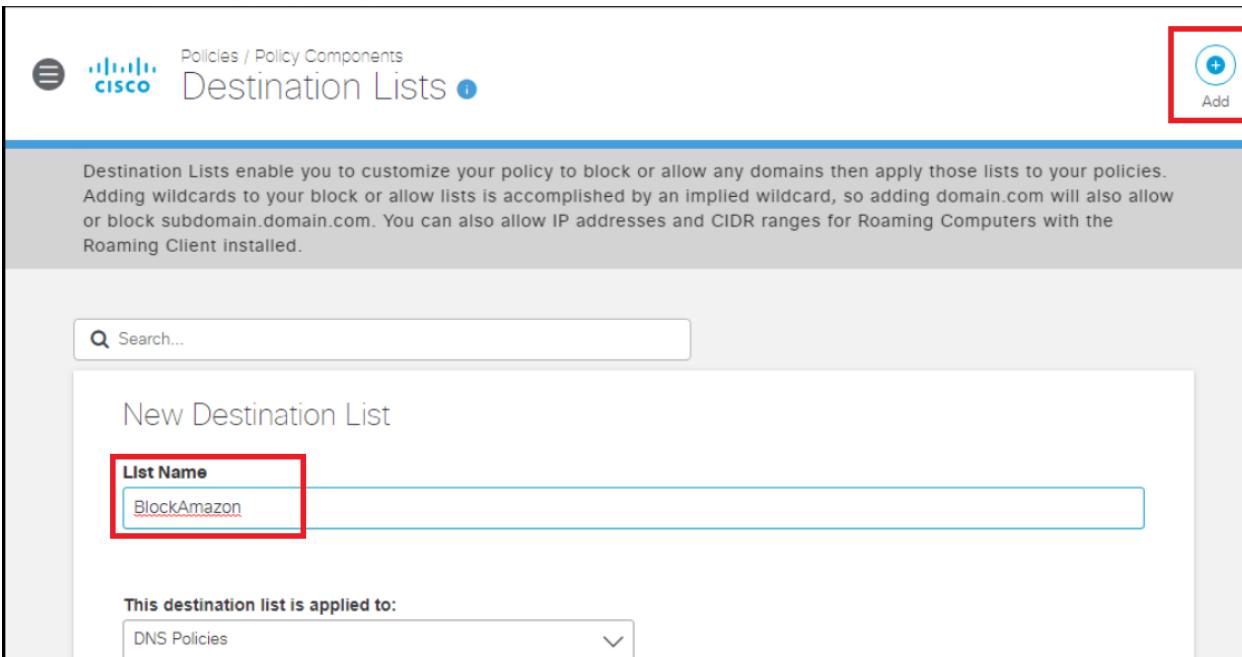
Destination Lists enable you to customize your policy to block or allow any domains then apply those lists to your policies. Adding wildcards to your block or allow lists is accomplished by an implied wildcard, so adding domain.com will also allow or block subdomain.domain.com. You can also allow IP addresses and CIDR ranges for Roaming Computers with the Roaming Client installed.

Search...

New Destination List

List Name  BlockAmazon

This destination list is applied to:  DNS Policies

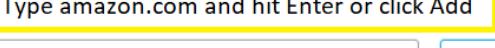


3. Scroll down to the **Destinations in this list should be** field and make sure it is set to **Blocked**. Type amazon.com in the *Enter a domain or URL* box and hit Enter (or click on Add). This should place amazon.com in the list (blocked). Click on **Save**

BlockAmazon

This destination list is applied to:  DNS Policies

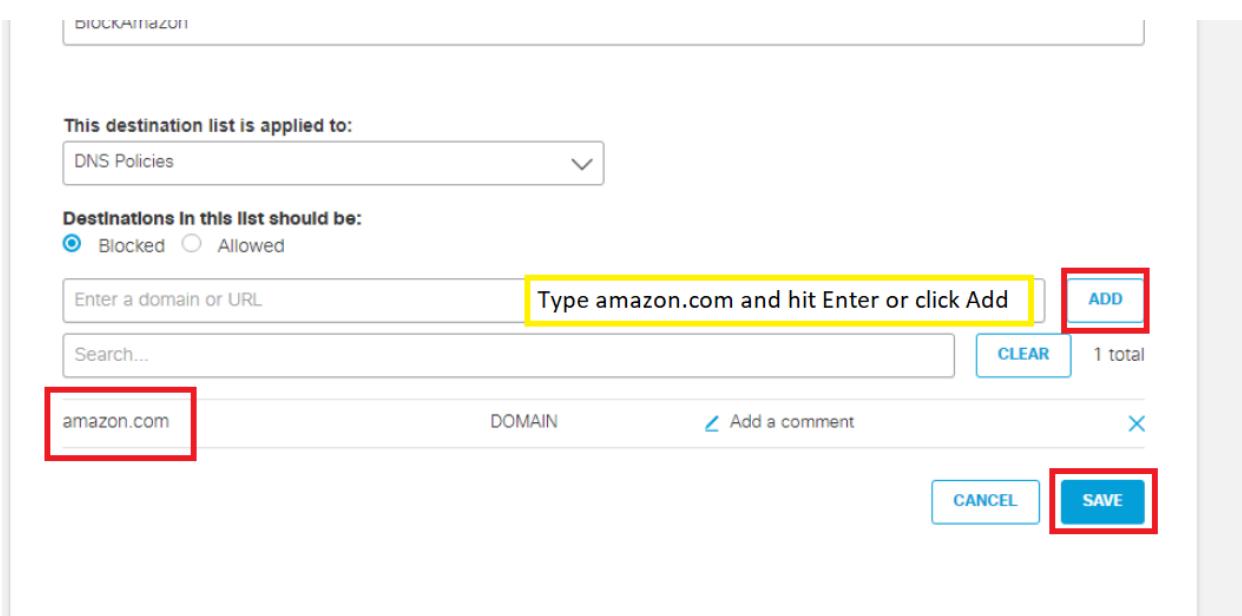
Destinations In this list should be: Blocked Allowed

Enter a domain or URL  Type amazon.com and hit Enter or click Add 

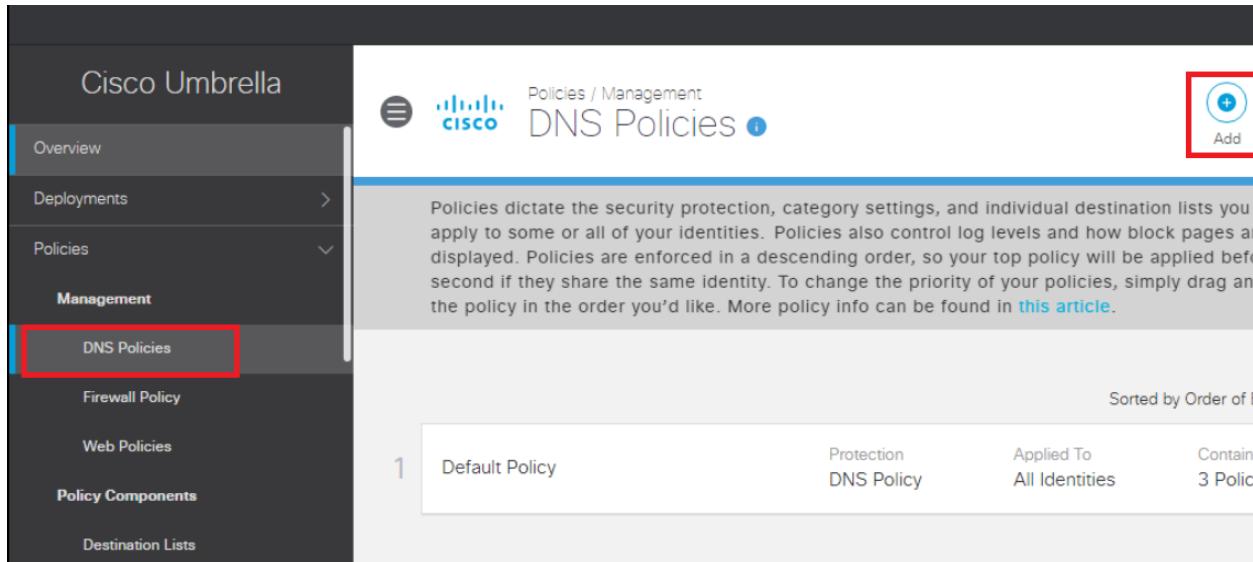
Search...  CLEAR 1 total

| amazon.com | DOMAIN | Add a comment | X |
|------------|--------|---------------|---|
| amazon.com | | | X |

 CANCEL  SAVE

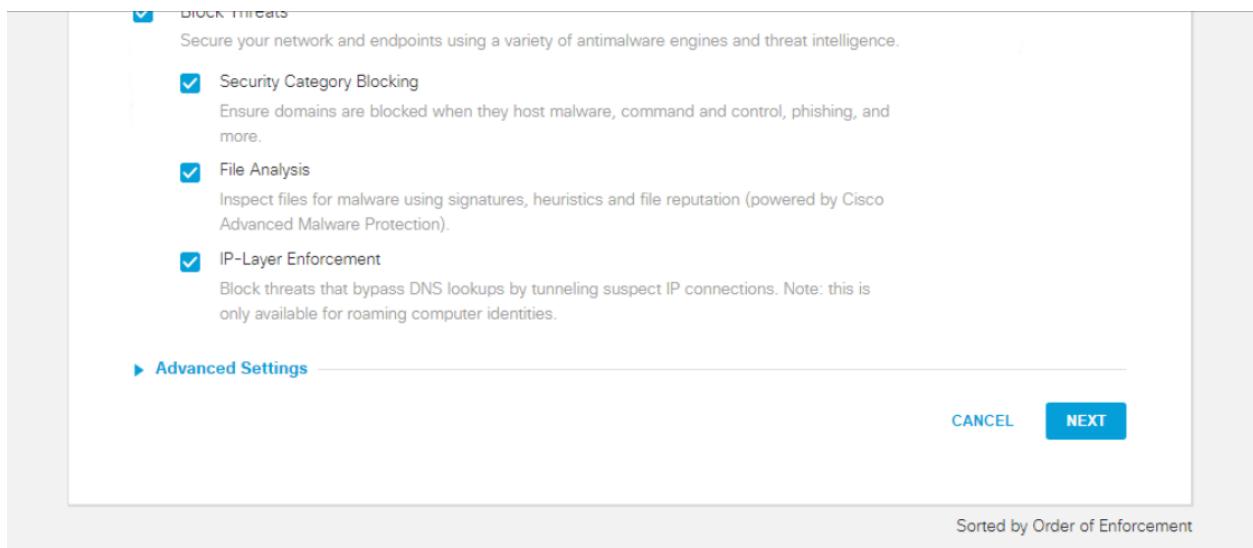


4. Navigate to Policies => Management => DNS Policies and click on Add to add a new DNS Policy



The screenshot shows the Cisco Umbrella interface. On the left, there's a sidebar with 'Cisco Umbrella' at the top, followed by 'Overview', 'Deployments', 'Policies' (with a dropdown arrow), 'Management' (which is expanded), 'DNS Policies' (highlighted with a red box), 'Firewall Policy', 'Web Policies', 'Policy Components', and 'Destination Lists'. The main content area is titled 'Policies / Management' and 'DNS Policies'. It contains a brief description of policies and an 'Add' button (also highlighted with a red box). Below this, a table lists one policy: 'Default Policy' under 'Protection' (DNS Policy), 'Applied To' (All Identities), and 'Contains' (3 Policy). The table is sorted by Order of Enforcement.

5. Scroll down on the **How would you like to be protected?** page and click on **Next** without making any changes



This screenshot shows a configuration page for 'BLOCK THREATS'. It includes a checkbox for 'Security Category Blocking' (checked) which describes blocking domains hosting malware, C2, phishing, etc. Another checked checkbox is 'File Analysis' which inspects files for malware using signatures, heuristics, and file reputation. A third checked checkbox is 'IP-Layer Enforcement' which blocks threats bypassing DNS lookups. Below these options is a 'Advanced Settings' link. At the bottom are 'CANCEL' and 'NEXT' buttons. The text 'Sorted by Order of Enforcement' is visible at the bottom of the page.

6. On the **What would you like to protect?** page, click on **Roaming Computers**. Don't click on the checkbox next to it, but on the actual phrase itself

What would you like to protect?

Select Identities

Search Identities

All Identities

- AD Groups 13 >
- AD Users 3 >
- AD Computers 2 >
- Networks
- Roaming Computers 1 >
- Sites 1 >
- Network Devices
- Mobile Devices

0 Selected

7. Put a check mark next to *site30pc* and it should show up in the right-hand window. Click on **Next**

What would you like to protect?

Select Identities

Search Identities

All Identities / Roaming Computers

- site30pc

1 Selected REMOVE ALL

site30pc

CANCEL

PREVIOUS

NEXT

8. Click **Next** in the Security Settings

 **Phishing Attacks**

Fraudulent websites that aim to trick users into handing over personal or financial information.

 **Dynamic DNS**

Block sites that are hosting dynamic DNS content.

 **Potentially Harmful Domains**

Domains that exhibit suspicious behavior and may be part of an attack.

 **DNS Tunneling VPN**

VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.

 **Cryptomining**

Cryptomining allows organizations to control cryptominer access to mining pools and web miners.

[CANCEL](#)

[PREVIOUS](#)

[NEXT](#)

9. Select **Moderate** on the **Limited Content Access** page and make note of the categories that are being blocked. Click on **Next**

High

Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

Moderate

Blocks all adult-related websites and illegal activity.

Low

Blocks pornography.

Custom

Create a custom grouping of category types.

Categories To Block -Moderate

These are the categories we will block. Note: if you want to make changes create a custom setting

Adware Alcohol

Dating Drugs

Gambling German Youth Protection

Hate / Discrimination Internet Watch Foundation

Lingerie / Bikini Nudity

Pornography Proxy / Anonymizer

Sexuality Tasteless

Terrorism Weapons

[CANCEL](#)

[PREVIOUS](#)

[NEXT](#)

10. Search for ebay in the Search Box on the **Control Applications** page under **Applications to Control** and put a check mark next to eBay. Make sure it is set to **Block** and click on **Next**. Click on **Proceed** on the Application Control

Change Summary page

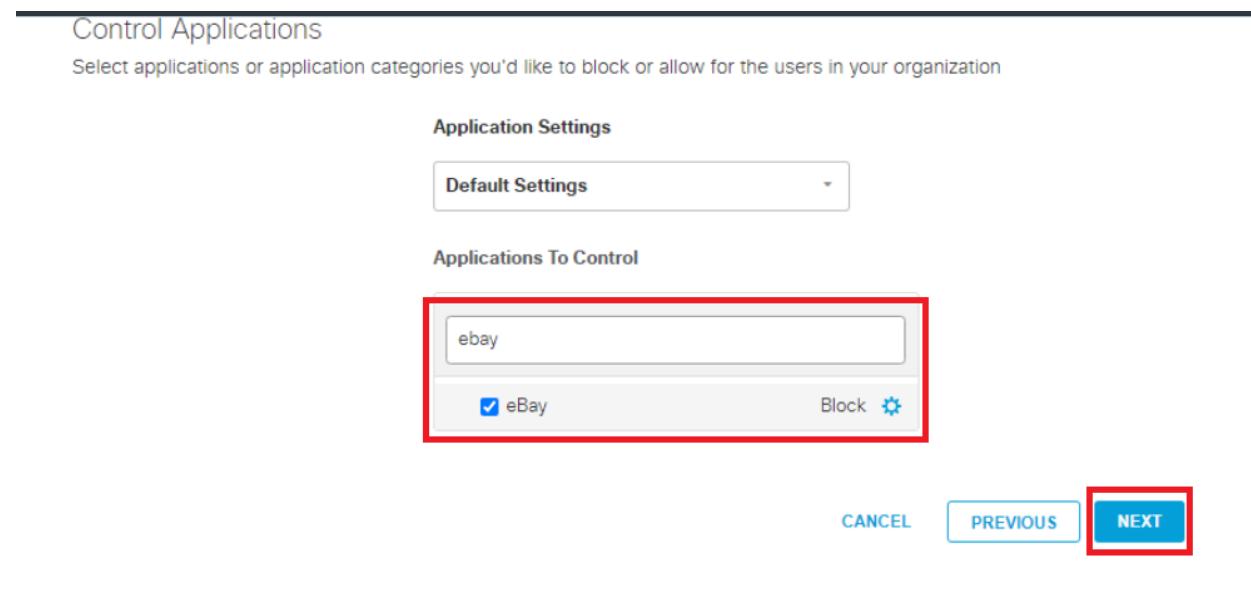
Control Applications
Select applications or application categories you'd like to block or allow for the users in your organization

Application Settings
Default Settings

Applications To Control

ebay
 eBay Block

CANCEL PREVIOUS **NEXT**



Application Control Change Summary
Please review the summary and changes before proceeding to the next step.

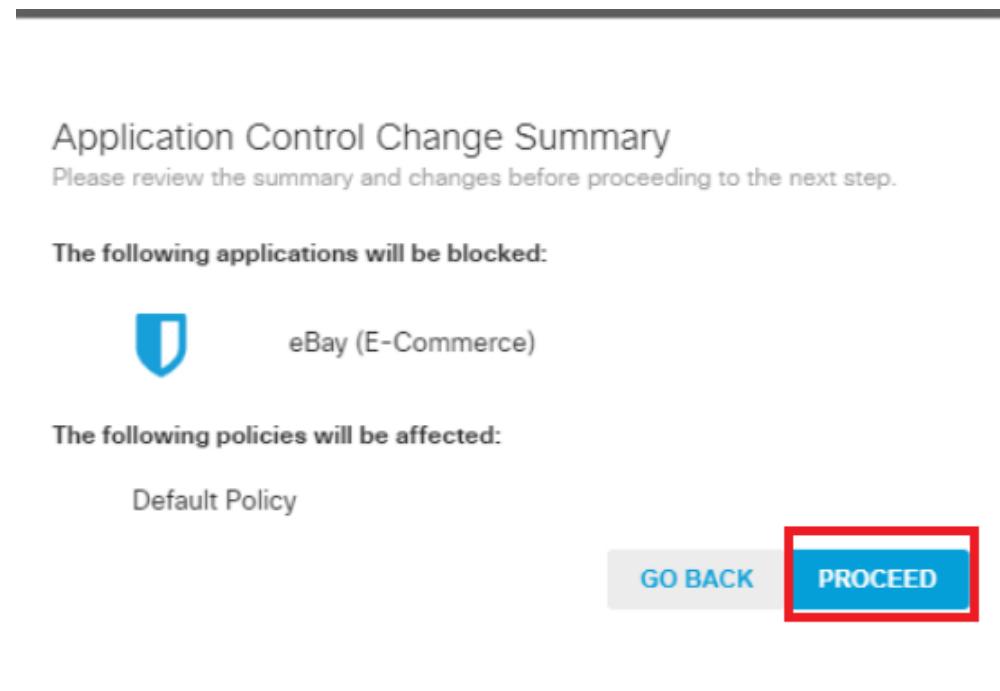
The following applications will be blocked:

 eBay (E-Commerce)

The following policies will be affected:

Default Policy

GO BACK **PROCEED**



11. Put a check mark next to **BlockAmazon** on the **Apply Destination Lists** page. This will apply the List we created before to the policy being built right now. You should see BlockAmazon on the right hand-side under **2 Block Lists**

Applied. Click on **Next**

Apply Destination Lists [ADD NEW LIST](#)

Search for and apply the appropriate block or allow Destination Lists for this policy. Click Add New List to create a Destination List.

Select All Showing: [All Lists ▾](#) 5 Total

All Destination Lists

| | |
|---|-----|
| <input checked="" type="checkbox"/>  BlockAmazon | 1 > |
| <input checked="" type="checkbox"/>  Global Allow List | 0 > |
| <input checked="" type="checkbox"/>  Global Block List | 0 > |
| <input type="checkbox"/>  MSP Default Allow List | 0 > |
| <input type="checkbox"/>  MSP Default Block List | 0 > |

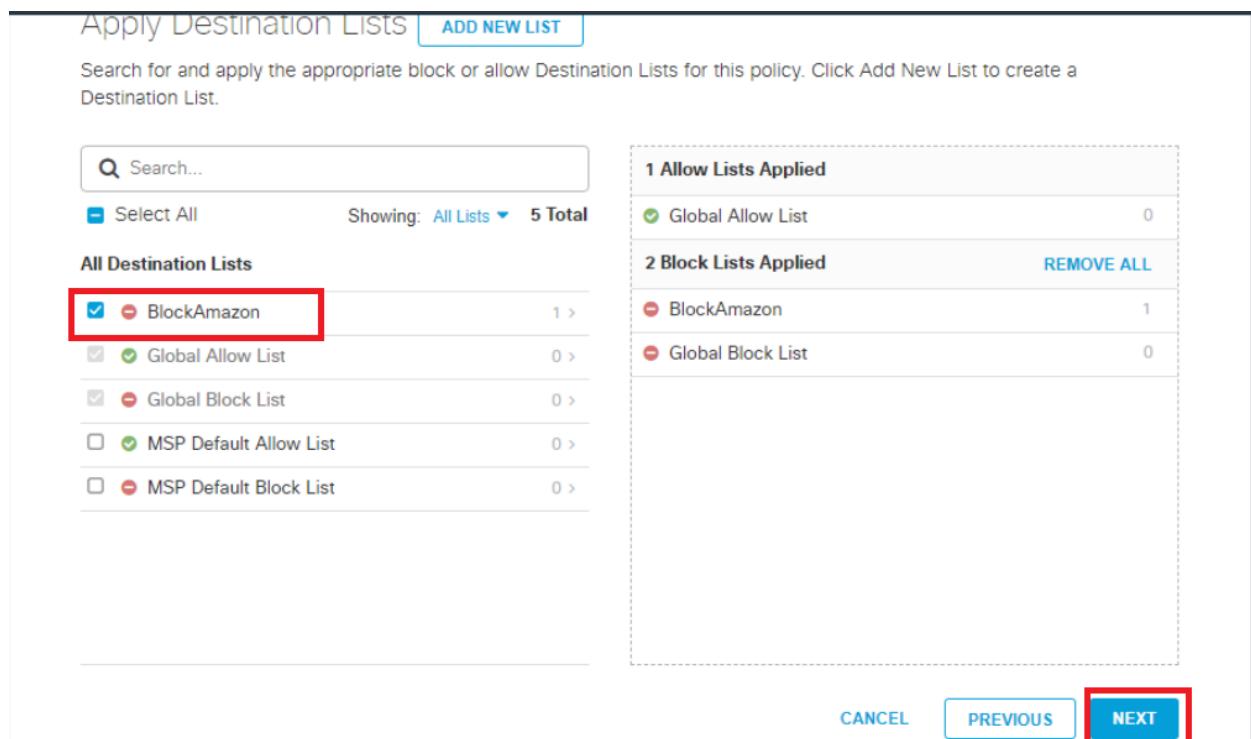
1 Allow Lists Applied

| | |
|---|---|
|  Global Allow List | 0 |
|---|---|

2 Block Lists Applied [REMOVE ALL](#)

| | |
|---|---|
|  BlockAmazon | 1 |
|  Global Block List | 0 |

[CANCEL](#) [PREVIOUS](#) [NEXT](#)



12. Click on **Next** on the **File Analysis** and **Set Block Page Settings** pages without making any changes



+4 4 More

5 File Analysis

6 Block Pages

Summary

File Analysis

Inspect files for malicious behaviors using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics.

File Inspection

Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

CANCEL

PREVIOUS

NEXT

Set Block Page Settings

Define the appearance and bypass options for your block pages.

Use Umbrella's Default Appearance

[Preview Block Page »](#)

Use a Custom Appearance

[Choose an existing appearance](#)

» [BYPASS USERS](#)

» [BYPASS CODES](#)

CANCEL

PREVIOUS

NEXT

13. Once on the **Policy Summary** page, give your Policy a Name of **DNSPolicy1**. Click on **Save**

Policy Summary

| Policy Name | DNSPolicy1 |
|--|--|
| 1 Identity Affected | 3 Destination Lists Enforced |
| 1 Anyconnect Roaming Client | 2 Block Lists 1 Allow List |
| Edit | Edit |
| Security Setting Applied: Centralized Default Settings | File Analysis Enabled |
| Command and Control Callbacks, Malware, and Phishing Attacks will be blocked | File Inspection Enabled |
| No integration is enabled. | Edit |
| Edit Disable | Edit Preview Block Page |
| Content Setting Applied: Moderate | Umbrella Default Block Page Applied |
| Blocks all adult-related websites and illegal activity. | Edit Preview Block Page |
| Edit Disable | <div style="border: 2px solid yellow; padding: 5px; width: fit-content;">Click on Save <u>AFTER</u> entering the Policy Name</div> |
| Application Setting Applied: Default Settings | |
| eBay will be blocked. | |
| Edit Disable | |

14. Our DNS Policy is now created. It might take 5 minutes for the policy to be applied. Click on the *DNSPolicy1* policy and enable **SSL Decryption**. Scroll down and click on **Save**

Policies / Management

DNS Policies

Add Policy Tester

| Sorted by Order of Enforcement | | | | |
|--------------------------------|----------------|-----------------------|----------------|-------------------|
| | Name | Type | Applied To | Contains |
| 1 | DNSPolicy1 | Protection DNS Policy | 1 Identity | 4 Policy Settings |
| 2 | Default Policy | Protection DNS Policy | All Identities | 3 Policy Settings |

Policy Name
DNSPolicy1

1 Identity Affected
1 Anyconnect Roaming Client
[Edit Identity](#)

3 Destination Lists Enforced
2 Block Lists
1 Allow List
[Edit](#)

Security Setting Applied: Centralized Default Settings
Command and Control Callbacks, Malware, and Phishing Attacks will be blocked
No integration is enabled.
[Edit](#) [Disable](#)

File Analysis Enabled
File Inspection Enabled
[Edit](#)

Content Setting Applied: Moderate
Blocks all adult-related websites and illegal activity.
[Edit](#) [Disable](#)

Umbrella Default Block Page Applied
[Edit](#) [Preview Block Page](#)

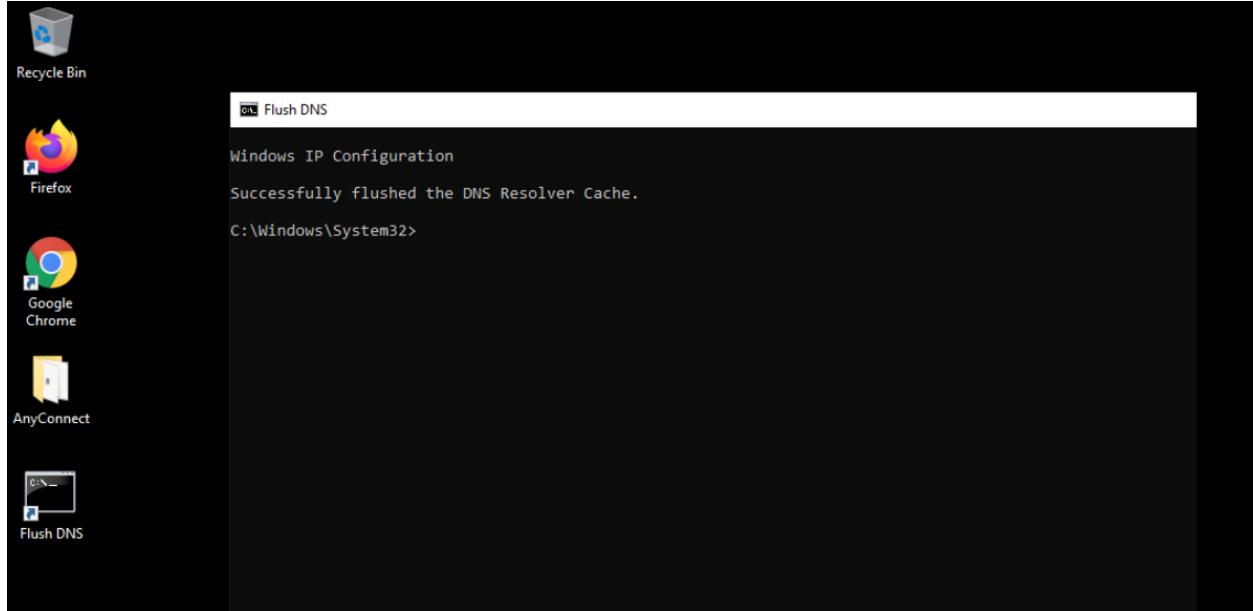
Application Setting Applied: Default Settings
eBay will be blocked.
[Edit](#) [Disable](#)

Advanced Settings

Enable Intelligent Proxy
Gain visibility into threats, content, or apps by proxying web connections for risky domains.

SSL Decryption
Enabling SSL decryption allows the intelligent proxy to inspect traffic over HTTPS and block custom URLs in destination lists.
Turning on SSL decryption allows HTTPS URL blocking.

15. We are now going to test our DNS Policy, but before doing so, the Cisco Umbrella root certificate will need to be downloaded and installed on the Site 30 PC. Head over to the Site 30 PC via your preferred connection method (Guacamole/RDP/vCenter Console). [Click here](#) and go through Step 1 to review how to connect to the Site 30 PC. Double-click the **Flush DNS** icon on the Desktop to clear the DNS cache



16. Log in to Umbrella on the Site 30 PC (login.umbrella.com). [Click here](#) and reference Step 1 to review the login procedure, but make sure you log in to Umbrella via the Site 30 PC. Navigate to **Deployment => Configuration => Root Certificate**

A screenshot of the Cisco Umbrella web interface. On the left is a dark sidebar with a list of navigation items: Roaming Computers, Mobile Devices, Chromebook Users, Network Tunnels, Web Users and Groups, Configuration, Domain Management, Sites and Active Directory, Internal Networks, Root Certificate (which is highlighted with a red box), SAML Configuration, and Service Account Exceptions. The main content area is titled "Overview" and shows "LAST 24 HOURS". It includes sections for Deployment Health with metrics like "Active Networks" (0%), "Active Roaming Clients" (100%), "Active Virtual Appliances" (0%), and "Active Network Tunnels" (Not tracking data). Above the deployment health section, there are three boxes for Malware, Command and Control, and Cryptomining, each stating 0 requests blocked in the last 24 hours with "View Trend" and "View Details" links.

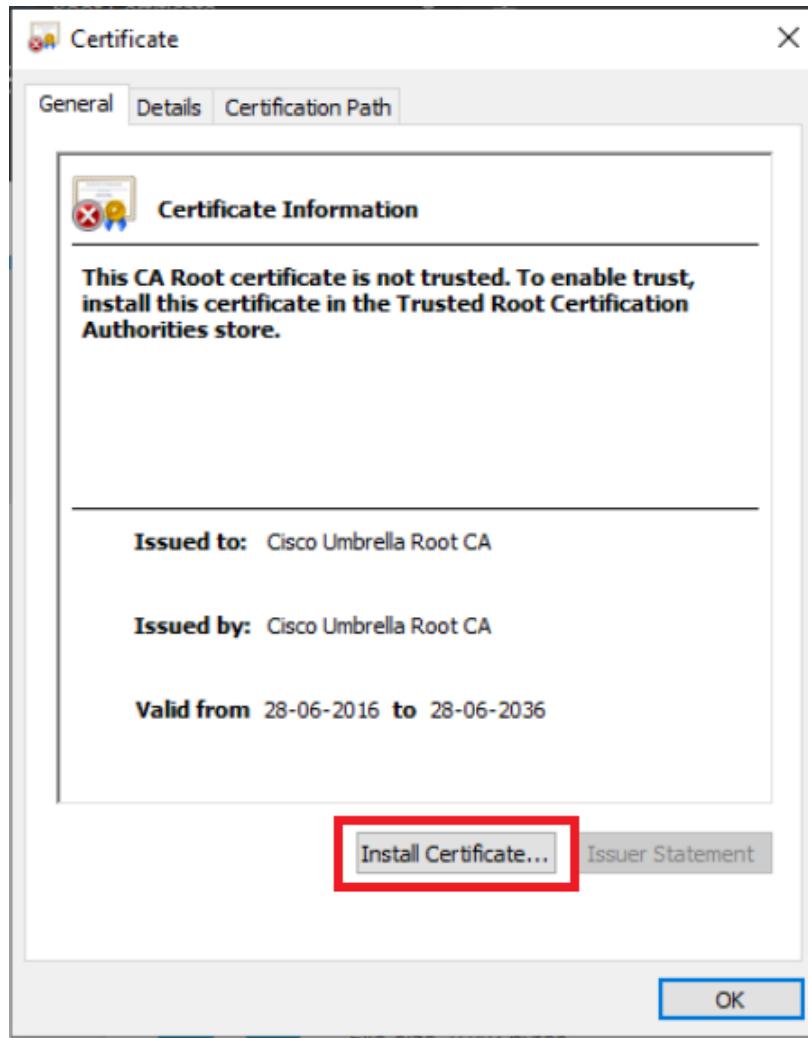
17. Expand **Cisco Root Certificate Authority** and download the root CA certificate

The screenshot shows a web page titled "Cisco Root Certificate Authority". Below the title, there is a message: "Download Umbrella's root CA certificate and then install it in all browsers". A download link is present, indicated by a blue button with a downward arrow icon and the text "File size 1049 bytes". This link is highlighted with a red box. Below the download link, there is a verification message: "To verify Umbrella's root CA certificate, confirm that it's SHA1 certificate matches C5:09:11:32:E9:AD:F8:AD:3E:33:93:2A:E6:0A:5C:8F:A9:39:E8:24".

18. Click on Keep, if prompted and open the downloaded file. Choose **Open** in the Security Warning

The screenshot shows a "Open File - Security Warning" dialog box. The title bar says "Open File - Security Warning". The main content asks "Do you want to open this file?". It displays the following details about the file:
Name: ...Users\sdwan\Downloads\Cisco_Umbrella_Root_CA.cer
Publisher: Unknown Publisher
Type: Security Certificate
From: C:\Users\sdwan\Downloads\Cisco_Umbrella_Root_CA....
At the bottom, there are two buttons: "Open" (highlighted with a blue border) and "Cancel". Below the buttons, there is a checked checkbox: "Always ask before opening this file". At the very bottom, there is a warning message: "While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. [What's the risk?](#)".

19. Click on **Install Certificate**



20. Select **Local Machine** and click on **Next**. Enter the credentials shown below and click on **Yes**

| Username | Password |
|---------------|------------|
| administrator | C1sco12345 |



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

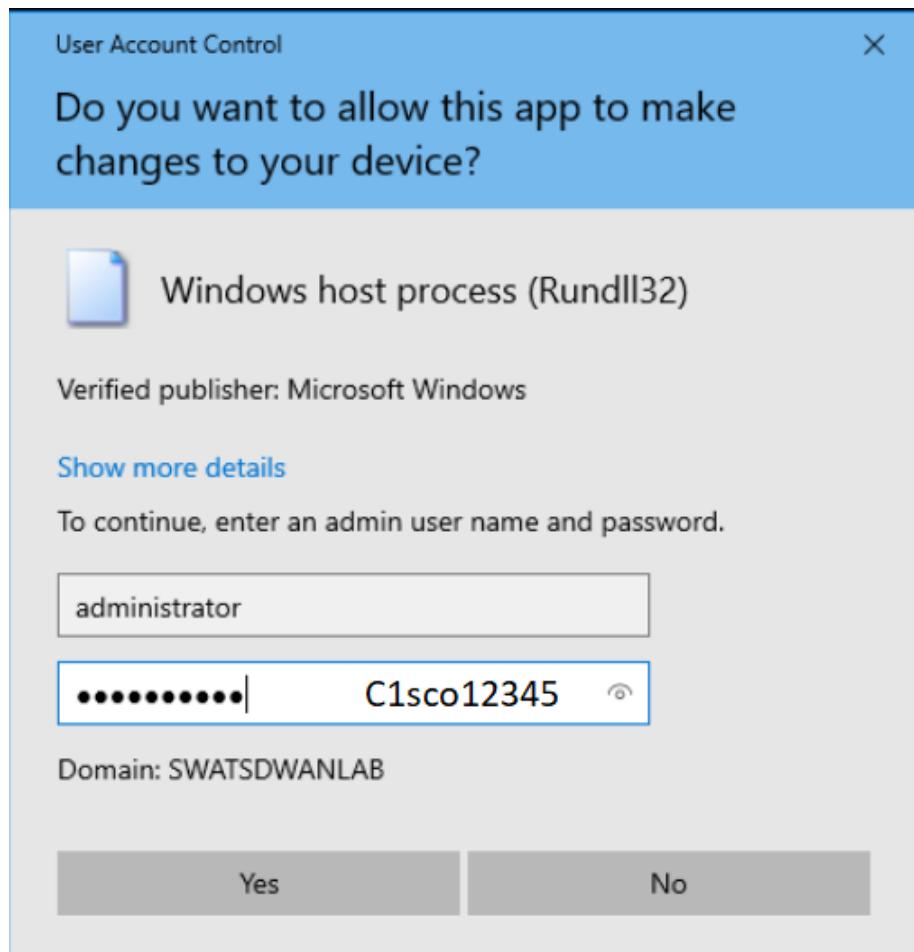
- Current User
 Local Machine

To continue, click Next.

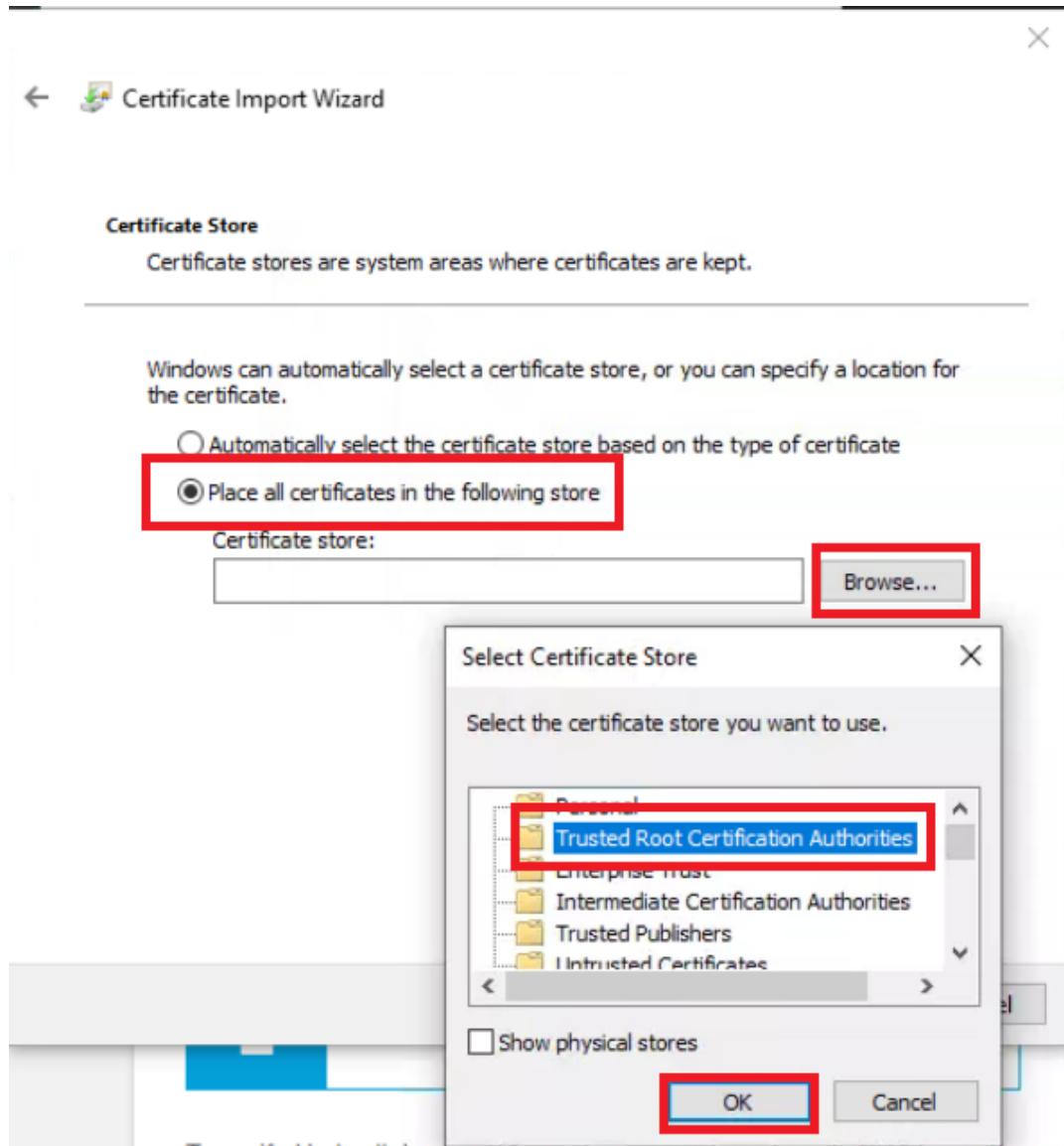


Next

Cancel



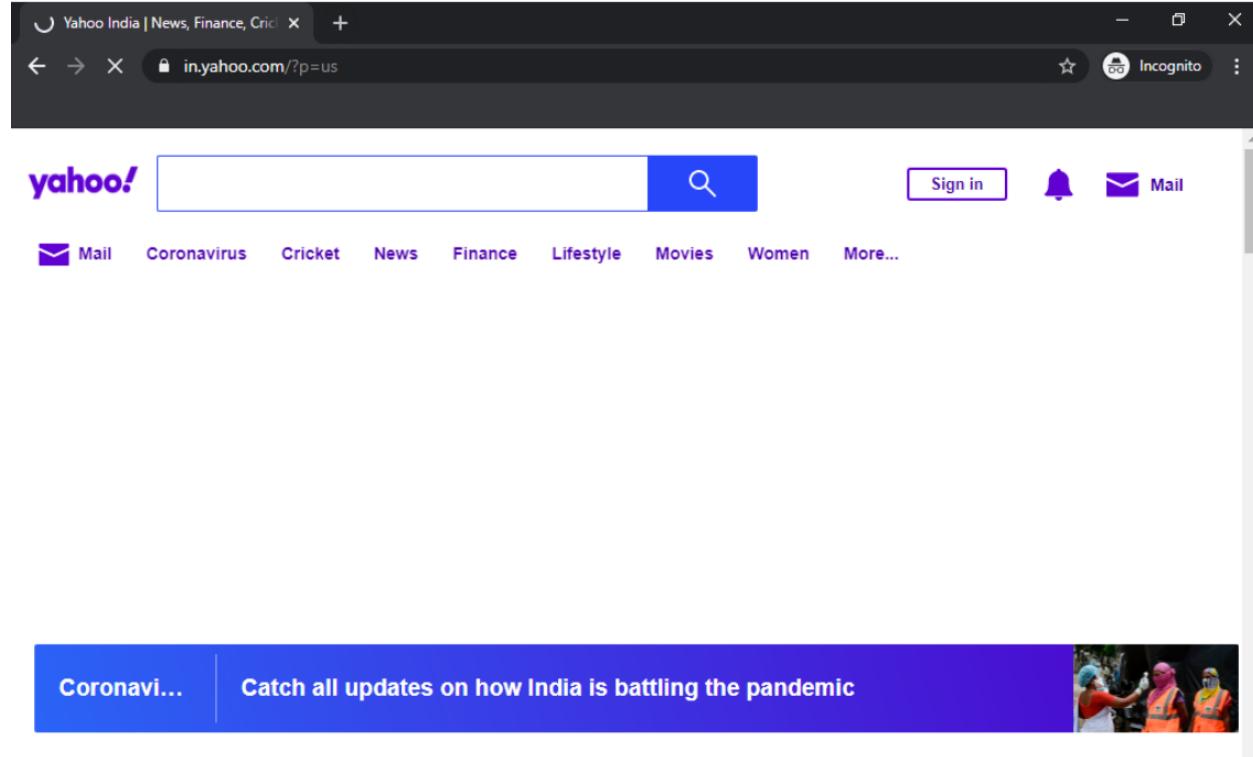
21. Choose the radio button next to **Place all certificates in the following store** and click on **Browse**. Click on **Trusted Root Certification Authorities** and hit **OK**



22. Click on **Finish** and then **OK**. Close the browser you were using and re-open before proceeding to the next step



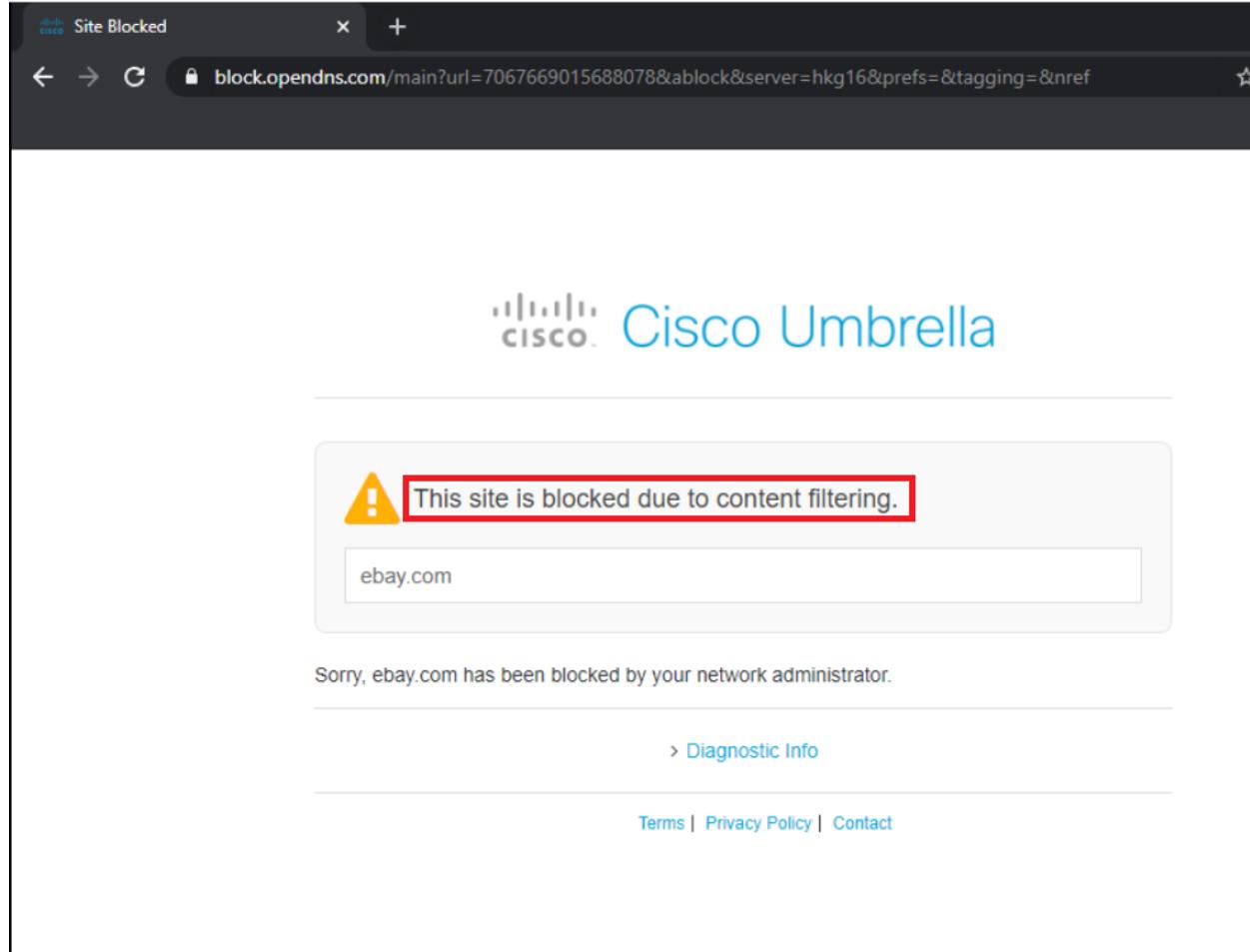
23. On the browser, go to yahoo.com. The page should open since we haven't applied any policy for it



24. Now try going to amazon.com. We will find that it is blocked with the text **The site is blocked** indicating this has been done by the administrator via a Block List. Amazon was opening before, but our company policy doesn't allow it and we have thus leveraged Cisco Umbrella's DNS Policy functionality to block specific destinations

The screenshot shows a web browser window with the title "Site Blocked". The address bar contains the URL "block.opendns.com/main?url=66786691807915688078&server=hkg15&prefs=&tagging=&nref". The main content area displays the Cisco Umbrella logo and a message stating "This site is blocked." with a yellow warning icon. Below this, the URL "amazon.com" is shown in a red box. A message at the bottom says "Sorry, amazon.com has been blocked by your network administrator." There is a link to "Diagnostic Info" and navigation links for "Terms | Privacy Policy | Contact".

25. Try to browse to ebay.com. This will also be blocked but the text will read **This site is blocked due to content filtering**. This is because we blocked eBay in the Control Applications section of our policy



26. Try to go to poker.com. This will also be blocked (with the same text as the previous step). Over here, our **Limited Content Access** level of *Moderate* is coming in to play. Note the subtext mentioning *This site was blocked due to the following categories: Gambling*

The screenshot shows a browser window with the title "Site Blocked". The address bar contains the URL "block.opendns.com/main?url=818076708315688078&ablock&server=hkg15&prefs=&tagging=&nref". The main content area displays the Cisco Umbrella logo and a message stating "This site is blocked due to content filtering." with a yellow warning icon. Below this, the URL "poker.com" is shown in a text input field. A message below the input field says "Sorry, poker.com has been blocked by your network administrator." Another message indicates the block was due to "Gambling". There is a link to "Diagnostic Info". At the bottom, there are links for "Terms", "Privacy Policy", and "Contact".

This completes the DNS Security part of our configuration. We have successfully deployed a DNS Policy, blocking sites that are not allowed by our company policy.

Task List

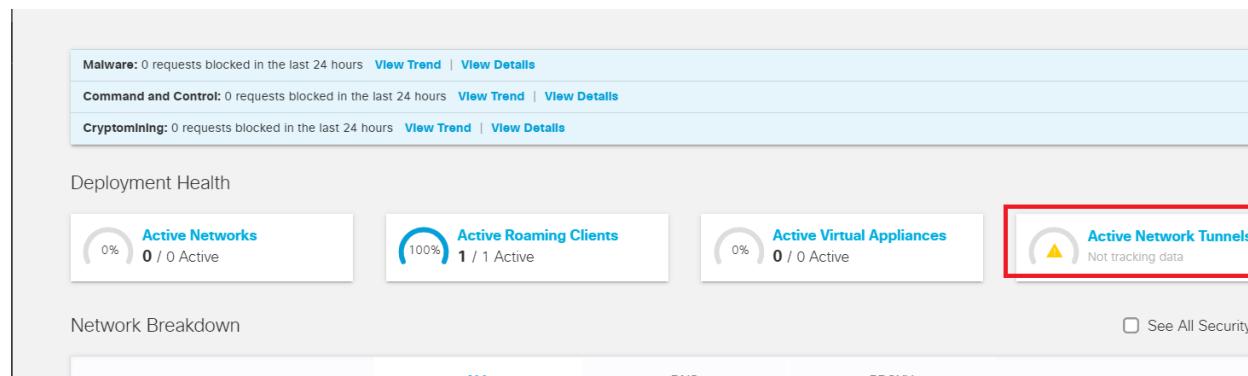
- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)

- [API Keys and AD Configuration](#)
- [DC Configuration Download](#)
- [AD Connectors](#)
- [Roaming Computer Configuration](#)
- [Building a DNS Policy](#)
- [Setting up IPSEC Tunnels](#)
- [Configuring a Firewall Policy](#)
- [Configuring a Web Policy](#)

Setting up IPSEC Tunnels

The main focus of SD-WAN and Umbrella integration is around Secure Internet Gateway (SIG) functionality. So far, we have run through a DNS policy which is the first layer of security in the network. For deeper packet inspection, we can utilize Umbrella and SD-WAN's SIG functionality which will create IPSEC tunnels between our vEdges/cEdges and Cisco Umbrella. Traffic will be sent to Umbrella over the IPSEC tunnels and will be subject to Firewall and Web policies.

1. Open a browser and log in to Cisco Umbrella from your Jumphost. [Click here](#) and reference Step 1 to review the login procedure, but make sure you log in to Umbrella via the **Jumphost** and **not** any other workstation. The main overview page will show that we have 1/1 Active Roaming Client and no Active Network Tunnels



2. Log in to the vManage GUI via the bookmark (or go to 192.168.0.6) with the Username and Password given below. Navigate to **Configuration => Templates => Feature Tab** and click **Add Template**. Search for **vedge** and select the **vEdge Cloud** device. Click on **SIG Credentials** under Other Templates

| Username | Password |
|----------|----------|
| admin | admin |

CONFIGURATION | TEMPLATES

Device **Feature**

Select Devices
vedge

vEdge 100

vEdge 100 B

vEdge 100 M

vEdge 100 WM

vEdge 1000

vEdge 2000

vEdge 5000

vEdge Cloud

VPN Interface PPP Ethernet
WAN

OTHER TEMPLATES

Banner

BGP
WAN | LAN

DHCP Server
LAN

IGMP
LAN

Multicast

OSPF
WAN | LAN

SIG Credentials

SNMP

3. Put the **Template Name** as *SIG-Creds* and a Description of *SIG Credentials*. Enter the Organization ID, Registration Key (i.e. API Key) and Secret copied and saved to notepad before. Click on **Save**

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Add Template > **SIG Credentials**

| | |
|---------------|-----------------|
| Template Name | SIG-Creds |
| Description | SIG Credentials |

Basic Details

SIG Provider Umbrella

Organization ID

Registration Key

Secret

Get Keys

Save **Cancel**

Enter the Organization ID, API Key and Secret copied to Notepad earlier and click Save

4. Back at the Templates page, make sure you're still on the **Feature Tab** and click on **Add Template**. Search for vedge and select **vEdge Cloud**. Click on **Secure Internet Gateway (SIG)** under VPN

CONFIGURATION | TEMPLATES

Device Feature

Feature Template [Add Template](#)

Select Devices
vedge

vEdge 100

vEdge 100 B

vEdge 100 M

vEdge 100 WM

vEdge 1000

vEdge 2000

vEdge 5000

vEdge Cloud

AAA Archive

NTP OMP

System

VPN

Secure Internet Gateway (SIG)
WAN

VPN

VPN Interface Cellular
WAN

VPN Interface Ethernet
Management | WAN | LAN

The screenshot shows the 'Feature' tab selected in the configuration interface. On the left, a sidebar lists various device models, with 'vEdge Cloud' checked and highlighted by a red box. To the right, features are organized into categories: 'AAA', 'Archive', 'NTP', 'OMP', 'System', and 'VPN'. Under 'VPN', the 'Secure Internet Gateway (SIG)' feature is specifically highlighted with a red box around its name and 'WAN' sub-option.

5. Give it a **Template Name** of *S/G-Template* and a Description of *S/G Template*

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > Secure Internet Gateway (SIG)

Template Name

Description

Configuration

SIG Provider Umbrella

[+ Add Tunnel](#)

This screenshot shows the configuration details for the 'Secure Internet Gateway (SIG)' template. It includes fields for 'Template Name' (set to 'SIG-Template') and 'Description' (set to 'SIG Template'), both of which are highlighted with red boxes. At the bottom, there's a 'Configuration' section with a 'SIG Provider' field set to 'Umbrella' (indicated by a blue radio button). A prominent blue button labeled '+ Add Tunnel' is located at the bottom left.

6. Click on **Add Tunnel** and enter the details given in the table below. Click on **Add** once done

| Parameter | Global or Device Specific (Drop Down) | Value |
|-------------------------|---------------------------------------|---------|
| Interface Name (1..255) | Global | ipsec1 |
| Source Interface | Global | ge0/0 |
| Data-Center | NA | Primary |

Feature Template > Add Template > Secure Internet Gateway (SIG)

Add Tunnel

Basic Settings

Tunnel Type: IPsec

Interface Name (1..255): ipsec1

Description:

Source Interface: ge0/0

Data-Center: Primary

Advanced Options >

Add Cancel

7. Click on **Add Tunnel** again to add a second IPSEC Tunnel. Enter the details given below and click on **Add**

| Parameter | Global or Device Specific (Drop Down) | Value |
|-------------------------|---------------------------------------|-----------|
| Interface Name (1..255) | Global | ipsec2 |
| Source Interface | Global | ge0/0 |
| Data-Center | NA | Secondary |

Device Feature

Feature Template > Add Template > [Secure Internet Gateway \(SIG\)](#)

Add Tunnel

Basic Settings

Tunnel Type IPsec

Interface Name (1..255) ipsec2

Description

Source Interface ge0/0

Data-Center Primary Secondary

Advanced Options >

Add Cancel

Save Cancel

8. Populate *ipsec1* under Active and *ipsec2* under Backup. Click on **Save**

Configuration

SIG Provider Umbrella

| Tunnel Name | Description | Source Interface | SIG Tunnel Data Center | Shutdown | TCP MSS |
|-------------|-------------------------------------|------------------|------------------------|--|--|
| ipsec1 | <input checked="" type="checkbox"/> | ge0/0 | Primary | <input checked="" type="checkbox"/> No | <input checked="" type="checkbox"/> 1300 |
| ipsec2 | <input checked="" type="checkbox"/> | ge0/0 | Secondary | <input checked="" type="checkbox"/> No | <input checked="" type="checkbox"/> 1300 |

High Availability

Active Backup

Pair-1 ipsec1 ipsec2

Save Cancel

9. Log in to vEdge30 via the saved Putty session. Enter `ping global-a.vpn.sig.umbrella.com`. Pings should be successful. Press Ctrl + c to stop the pings

| | |
|----------|----------|
| Username | Password |
| admin | admin |

```

vEdge30#
vEdge30#
vEdge30#
vEdge30#
vEdge30# ping global-a.vpn.sig.umbrella.com
Ping in VPN 0
PING global-a.vpn.sig.umbrella.com (146.112.113.8) 56(84) bytes of data.
64 bytes from 146.112.113.8 (146.112.113.8): icmp_seq=1 ttl=48 time=87.3 ms
64 bytes from 146.112.113.8 (146.112.113.8): icmp_seq=2 ttl=48 time=87.5 ms
64 bytes from 146.112.113.8 (146.112.113.8): icmp_seq=3 ttl=48 time=87.3 ms
64 bytes from 146.112.113.8 (146.112.113.8): icmp_seq=4 ttl=48 time=87.3 ms
^C
--- global-a.vpn.sig.umbrella.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 87.330/87.414/87.555/0.225 ms
vEdge30#

```

ping global-a.vpn.sig.umbrella.com

- Back on the vManage GUI, navigate to **Configuration => Templates**. Under the Device tab, locate the *vedge30_dev_temp* template and click on the three dots next to it. Choose to **Edit** the template

| Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template |
|---------------------|----------------------|---------|--------------|-------------------|------------------|------------|----------------------|----------|
| cEdge-single-uplink | Single Uplink cEd... | Feature | CSR1000v | 17 | 2 | admin | 19 Jun 2020 2:01... | In Sync |
| vEdge_Site20_dev... | Device template f... | Feature | vEdge Cloud | 17 | 1 | admin | 19 Jun 2020 3:53... | In Sync |
| cedge_dualuplink... | cedge Device Tem... | Feature | CSR1000v | 20 | 1 | admin | 21 Jun 2020 5:57... | In Sync |
| vSmart-dev-temp | Device Template f... | Feature | vSmart | 9 | 2 | admin | 19 Jun 2020 12:1... | In Sync |
| vEdge30_dev_temp | Device template f... | Feature | vEdge Cloud | 15 | 1 | admin | 06 Jul 2020 10:30... | In Sync |
| vEdge_Site20_dev... | Device template f... | Feature | vEdge Cloud | 17 | 1 | admin | 19 Jun 2020 3:46... | In Sync |
| DCvEdge_dev_temp | Device template f... | Feature | vEdge Cloud | 16 | 2 | admin | 21 Jun 2020 4:07... | In Sync |

- Go to the **Transport & Management VPN** section click on **Secure Internet Gateway** under **Additional VPN 0 Templates**. Select the *S/G-Template* from the drop down

Transport & Management VPN

| | |
|-------------------------|--------------|
| VPN 0 * | vEdge30-vpn0 |
| Secure Internet Gateway | SIG-Template |
| VPN Interface | vEdge30_INET |
| VPN Interface | vEdge30_MPLS |

Additional VPN 0 Templates

- BGP
- OSPF
- Secure Internet Gateway
- VPN Interface
- VPN Interface Cellular
- VPN Interface GRE
- VPN Interface IPsec
- VPN Interface PPP

12. Scroll down to the **Additional Templates** section and populate S/G-Creds for the **SIG Credentials**. Click on **Update**

Cisco vManage

CONFIGURATION | TEMPLATES

Basic Information Transport & Management VPN Service VPN Additional Templates

| | |
|-------------------|-----------|
| Banner | Choose... |
| Policy | Choose... |
| SNMP | Choose... |
| Security Policy | Choose... |
| SIG Credentials * | SIG-Creds |

Bridge Bridge

Update **Cancel**

13. Click on **Next**. You can view the side-by-side configuration if required. Make note of the *secure-internet-gateway* and *ha-pairs* configuration

Device Template **vEdge30_dev_temp** Total 1

Device list (Total: 1 devices)

Filter/Search

17026153-f09e-be4b-6dce-482fce43aab2
vEdge30|10.255.255.31

```

34 !
35 !
36 !
37 ospf
38 no shutdown
39 graceful-restart
40 advertise connected
41 advertise static
42 !
43 security
44 ipsec
45 authentication-type sha1-hmac ah-sha1-hmac
46 !
47 !
48 vpn 0
49 dns 4.2.2.2 secondary
50 dns 8.8.8.8 primary
51 !
52 !
53 vpn 0
54 dns 4.2.2.2 secondary
55 dns 8.8.8.8 primary
56 service sig ha-pairs interface-pair ipsec1 ipsec2
57 !

```

14. If you scroll down, *interface ipsec1* and *interface ipsec2* configuration can be viewed. Click on **Configure Devices**

CONFIGURATION | TEMPLATES

Device Template **vEdge30_dev_temp** Total 1

Device list (Total: 1 devices)

Filter/Search

17026153-f09e-be4b-6dce-482fce43aab2
vEdge30|10.255.255.31

Configure Device Rollback Timer

Back

'Configure' action will be applied to 1 device(s)
attached to 1 device template(s).

```

98 !
99 interface ipsec1
100 ip unnumbered
101 tunnel-source-interface ge0/0
102 tunnel-destination dynamic
103 tunnel-set secure-internet-gateway-umbrella
104 tunnel-dc-preference primary-dc
105 dead-peer-detection interval 10 retries 3
106 ike
107 version 2
108 rekey 14400
109 cipher-suite aes256cbc-sha1
110 group 14
111 authentication-type
112 pre-shared-key-dynamic
113 !
114 !
115 ipsec
116 rekey 3600
117 replay-window 512
118 cipher-suite null-sha1
119 perfect-forward-secrecy group-16
120 !
121 mtu 1400
122 no shutdown
123 !

```

Configure Devices **Cancel**

15. Wait for a couple of minutes and log in to the Putty session for *vedge30*. Issue the command `show ipsec ike sessions`. You will see 2 sessions which should be in a state of **IKE_UP_IPSEC_UP**. If the sessions are in any other state, wait for a couple more minutes and issue the same command again

```
vEdge30# show ipsec ike sessions
ipsec ike sessions 0 ipsec1
version      2
source-ip    100.100.100.30
source-port   4500
dest-ip      146.112.113.8
dest-port    4500
initiator-spi 334290dd49b0c4e3
responder-spi 4b65a5150aca1eal
cipher-suite  aes256-cbc-sha1
dh-group     "14 (MODP-2048)"
state        IKE_UP_IPSEC_UP
uptime       0:00:00.16
tunnel-uptime 0:00:00:18
ipsec ike sessions 0 ipsec2
version      2
source-ip    100.100.100.30
source-port   4500
dest-ip      146.112.112.8
dest-port    4500
initiator-spi 741dcc6fa8253761
responder-spi 6fd2ceb40aca1872
cipher-suite  aes256-cbc-sha1
dh-group     "14 (MODP-2048)"
state        IKE_UP_IPSEC_UP
uptime       0:00:00.03
tunnel-uptime 0:00:00:05
vEdge30#
```

16. Log in to the Umbrella GUI. On the main overview page, you should see **Active Network Tunnels 2/2 Active**

The screenshot shows the Cisco Umbrella Overview dashboard. At the top left is the Cisco logo. To its right is a red-bordered box containing the word "Overview". On the far right is a "LAST 24 HOURS" dropdown menu. Below the header, there are three sections: "Malware", "Command and Control", and "Cryptominer". Each section has a "View Trend" and "View Details" link. Under "Deployment Health", there are four cards: "Active Networks" (0% active), "Active Roaming Clients" (100% active, 1/1), "Active Virtual Appliances" (0% active, 0/0), and "Active Network Tunnels" (100% active, 2/2). The "Active Network Tunnels" card is also red-bordered. Below these cards is a "Network Breakdown" section with a checkbox for "See All Security Events".

Malware: 0 requests blocked in the last 24 hours [View Trend](#) | [View Details](#)

Command and Control: 0 requests blocked in the last 24 hours [View Trend](#) | [View Details](#)

Cryptominer: 0 requests blocked in the last 24 hours [View Trend](#) | [View Details](#)

Deployment Health

Active Networks 0% 0 / 0 Active

Active Roaming Clients 100% 1 / 1 Active

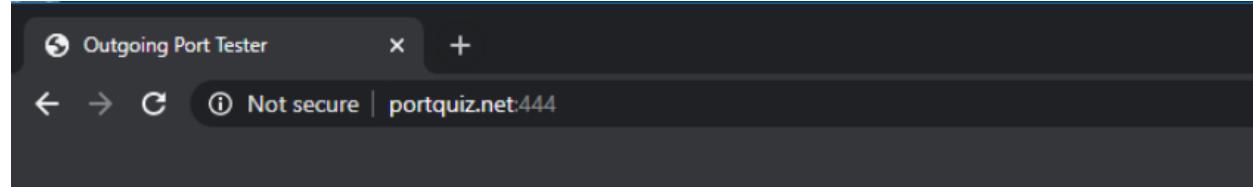
Active Virtual Appliances 0% 0 / 0 Active

Active Network Tunnels 100% 2 / 2 Active

Network Breakdown See All Security Events

This is an indication that our IPSEC Tunnels to Umbrella are up.

17. Head over to the Site 30 PC and open a web browser. Click on the *Outgoing Port Tester (444)* bookmark or go to <http://portquiz.net:444>. The page should load correctly



Outgoing port tester

This server listens on all TCP ports, allowing you to test any outbound TCP port.

You have reached this page on port **444**.

Your network allows you to use this port. (Assuming that your network is not doing advanced traffic filtering.)

Network service: snpp

Your outgoing IP: 14.140.162.5

Test a port using a command

```
$ telnet portquiz.net 444
Trying ...
Connected to portquiz.net.
Escape character is '^J'.

$ nc -v portquiz.net 444
Connection to portquiz.net 444 port [tcp/daytime] succeeded!

$ curl portquiz.net:444
Port 444 test successful!
Your IP: 14.140.162.5

$ wget -qO- portquiz.net:444
Port 444 test successful!
Your IP: 14.140.162.5

# For Windows PowerShell users
PS C:\> Test-NetConnection -InformationLevel detailed -ComputerName portquiz.net -Port 444
```

Test a port using your browser

In your browser address bar: <http://portquiz.net:XXXX>

18. Head back over to the vManage GUI and go to **Configuration => Templates => Feature Tab**. Locate the *vedge30-vpn10* template and click on the three dots next to it. Choose to **Edit** the template

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Feature' tab is selected. A search bar at the top right contains 'vpn10'. The main table lists various templates, including 'vedge30-vpn10' which is highlighted with a red box. A context menu is open over this row, with the 'Edit' option highlighted by another red box.

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
|----------------------|-------------------------------|---------------------|--------------|------------------|------------------|------------|---------------------------|
| vedge-vpn10 | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 3 | 4 | admin | 19 Jun 2020 2:00:08 A... |
| cedge-vpn10 | VPN 10 Template for the c... | Cisco VPN | CSR1000v | 2 | 3 | admin | 19 Jun 2020 2:00:08 A... |
| cedge-vpn10-int | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 0 | 0 | admin | 19 Jun 2020 2:00:08 A... |
| vedge30-vpn10 | VPN 10 Template for vEdge... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 06 Jul 2020 10:30:14 A... |
| cedge-vpn10-int-vrrp | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 19 Jun 2020 2:00:08 A... |
| vedge-vpn10-int | VPN 10 Interface Template ... | WAN Edge Interface | vEdge Cloud | 4 | 5 | admin | 19 Jun 2020 12:47:49 A... |
| cedge-vpn10-int-qos | VPN 10 Interface Template ... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 21 Jun 2020 4:38:51 P... |

19. Scroll down to the **Service Route** section and click on **New Service Route**. Enter a global **Prefix** for **0.0.0.0/0** and click on **Add**. Click on **Update** followed by **Next** and **Configure Devices**

This screenshot shows the 'Service Route' configuration dialog. The 'New Service Route' button is highlighted with a red box. The 'Prefix' field contains '0.0.0.0/0' and is also highlighted with a red box. The 'Add' button is highlighted with a red box. At the bottom, there are 'Update' and 'Cancel' buttons, with 'Update' also highlighted with a red box.

This will ensure that all the traffic hitting VPN 10 on vEdge30 is punted over the newly established IPSEC Tunnels to Umbrella.

20. On the Umbrella GUI, click on **Active Network Tunnels** and you will see the naming convention automatically populated for our 2 Tunnels. Both tunnels should be in an **Active** state (if the status is unknown, wait for some time and revisit this page)



To add a Firewall policy, you must first add a network tunnel. This network tunnel creates a secure connection between Umbrella and a compatible device, for example, Cisco ASA. The number of tunnels you can add depends on the number of compatible devices you are using. For more information, see [Adding Network Tunnels](#).

2 Total

Network Tunnels ▾

Status

Device Type

Last Active

SITE30SYS10x255x255x31!Ipsec1

✓ Active

Viptela vEdge

Just Now

SITE30SYS10x255x255x31!Ipsec2

✓ Active

Viptela vEdge

Just Now

Tip: The naming convention can be broken down as the Site ID, followed by the word SYS (for System IP) and then the System IP of the device in question with the dots replaced by x. The last few characters reference the Interface (IF) followed by the Interface Name (ipsec1 and ipsec2 in our case).

We have completed IPSEC Tunnel configuration for our vEdge30 device. Through the Service Route, we have ensured that all traffic is punted over the Tunnels to Umbrella (this is not in effect yet, more changes will be made to force traffic over the Tunnels).

Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - [API Keys and AD Configuration](#)
 - [DC Configuration Download](#)

- AD Connectors
 - Roaming Computer Configuration
 - Building a DNS Policy
 - Setting up IPSEC Tunnels
 - Configuring a Firewall Policy
 - Configuring a Web Policy

Configuring a Firewall Policy

1. Log in to Cisco Umbrella from your Jumphost, if not already logged in. Navigate to **Policies** => **Management** => **Firewall Policy** and click on **Add** in the top right-hand corner

The screenshot shows the Cisco Umbrella Policies / Management interface. The left sidebar has a 'Management' section with 'DNS Policies' and 'Firewall Policy' selected, which is highlighted with a red box. The main area displays a table of Firewall Rules. The table header includes columns for Priority, Name, Status, Action, Protocol, Source Criteria, Destination Criteria, Hit Count, and Last Hit. One rule is listed: 'Default Rule' with Priority 1, Enabled status, Allow action, Any protocol, and Any criteria for both source and destination. A 'FILTERS' button and a search bar are also visible.

| Priority | Name | Status | Action | Protocol | Source Criteria | Destination Criteria | Hit Count | Last Hit |
|--------------------------|----------------|------------------------|----------------------|----------|----------------------|----------------------|----------------------|------------------------|
| <input type="checkbox"/> | 1 Default Rule | ● Enabled | ✓ Allow | Any | Any IPs Any Ports | Any IPs Any Ports | 0/24hrs | Jul 04, 2020 - 01:39am |

2. Enter the rule name as *block444*. We will be blocking TCP traffic to port 444 via this Firewall Policy.

Rule Details

Define basic characteristics of the firewall rules.

| | |
|-------------|-----------------------|
| Rule Name | Priority Order |
| block444 | Last Before Default ▾ |
| Description | |

3. Scroll down and set the Protocol to TCP. Set the **Destination Ports** to **Specify Port** and enter the port number 444

Specify protocol, IPs, network tunnels, and ports to be blocked or allowed.

Protocol
TCP

Source Tunnels
Any Search and add specific source tunnels

Source IPs/CIDRs
Any Add IP address or CIDRs in comma-delimited format

Source Ports
Any Add ports, port ranges in comma-delimited format

Destination IPs/CIDRs
Any Add IP address or CIDRs in comma-delimited format

Destination Ports
Specify Port 444

The screenshot shows a configuration page for specifying network rules. At the top, it says 'Specify protocol, IPs, network tunnels, and ports to be blocked or allowed.' Below this, there are sections for 'Protocol' (set to 'TCP'), 'Source Tunnels' (set to 'Any'), 'Source IPs/CIDRs' (set to 'Any'), 'Source Ports' (set to 'Any'), 'Destination IPs/CIDRs' (set to 'Any'), and 'Destination Ports' (set to 'Specify Port' with '444' entered). The 'Protocol' and 'Destination Ports' sections are highlighted with red boxes.

4. Set the **Rule Action** to *Block Traffic* and Enable Logging

Hit Counter
Configure the default time interval to display for this rule

Time Interval
Last 24 Hours ▾

Rule Action
Block or allow traffic that meets the rule criteria.

Block Traffic
 Allow Traffic

Logging Enabled
Logs for this firewall rule will be captured in Activity.

Firewall Rule Enabled
This rule is active.

5. Under **Rule Schedule** set the **Start Date** to the earliest available and make sure **Does Not Expire** is checked. Click on **Save**

Rule Schedule
Define the start and end date of the rule.

Time Zone
(UTC + 5.5) Asia / Calcutta ▾

| Start Date | Start Time | Expiration Date | Expiration Time |
|-------------|------------|-----------------|-----------------|
| Jul 6, 2020 | 02:12 AM | TO | Mon DD YYYY |

Does Not Expire

Set the start date to the earliest available

6. The Firewall Policy of *block444* should show up above the **Default Rule**

Use this policy to control network traffic based on IP, port, and protocol. Rules are evaluated from the top down. For more information about Firewall Policy, view [Manage Firewall](#).

| Firewall Policies | | | | | | | | | |
|-------------------|--------------|--|--------|--------|----------------------|----------------------|----------------------|------------------------|----------|
| Filters | | Search Firewall Rule names or descriptions | | | | | | | |
| 2 Total | | | | | | | | | |
| # | Priority | Name | Status | Action | Protocol | Source Criteria | Destination Criteria | Hit Count | Last Hit |
| 1 | block444 | Enabled | Block | TCP | Any IPs Any Ports | Any IPs 1 Port | 0/24hrs | No Hits | ... |
| 2 | Default Rule | Enabled | Allow | Any | Any IPs Any Ports | Any IPs Any Ports | 0/24hrs | Jul 04, 2020 - 01:39am | ... |

7. On the Site 30 PC, open a browser and go to whatismyip.com. The Public IPv4 address should show up as **14.140.162.5**. We will remove DIA configuration at Site 30 and check the Public IP again

The screenshot shows a web browser window with the URL whatismyip.com in the address bar. The page displays the text "WhatIsMyIP.com". Below it, the message "My Public IPv4 is: 14.140.162.5" is highlighted with a red box. Underneath, "Location: Mohali, PB IN" is also highlighted with a red box. Further down, "ISP: Tata Communications Limited" is listed. There are two blue buttons: "My IP Information" and "IP Address Lookup". To the right of the main content, there is a sidebar titled "Recent Articles" with links to "Ways You Might be Weakening C Security" and "How to Use Public WiFi Safely". There is also an advertisement for Google Ads.

8. On the vManage GUI, navigate to **Configuration => Policies** and click on the three dots next to the **Site40-Guest-DIA** policy. Click on **Edit**. Under the **Policy Application** page, click on the **Traffic Data** tab. Delete the Site30 Site List/VPN List and click on **Save Policy Changes**. Choose to **Activate** the configuration, if prompted

Add policies to sites and VPNs

Policy Name: Site40-Guest-DIA
Policy Description: DIA Policy for Site 40 Guests

Topology Application-Aware Routing Traffic Data Cflowd

New Site List and VPN List

| Site List | VPN List | Direction | Action |
|-----------|-----------|-----------|--------|
| Site40 | Guest | service | |
| Site30 | Corporate | service | |

9. Once the policy changes have been pushed successfully, go back to the Site 30 PC and use a browser to go to whatismyip.com again. The Public IPv4 address should now be in the 146.112.A.B address space - this is the Singapore Umbrella Server

WhatIsMyIP.com

My Public IPv4 is **146.112.51.80**

Location: Singapore, - SG ?
ISP: OpenDNS

My IP Information
IP Address Lookup

Recent Articles

[Ways You Might be Weakening Cyber Security](#)

A lot of the time, we get hacked because we've made ourselves easy targets by weakening cyber security. Even though hackers use sophisticated technologies to hack into systems, they are still just people.

[How to Use Public WiFi Safely](#)

Sometimes you may need to access the Internet in a public place and have no other option than to use public WiFi. Fortunately, there are some things you can do to keep yourself safe even on public networks.

[See More Recent Articles](#)

10. Use the bookmark to navigate to **Outgoing Port Tester (444)** or go to <http://portquiz.net:444>. The site will not load



This site can't be reached

[portquiz.net](#) took too long to respond.

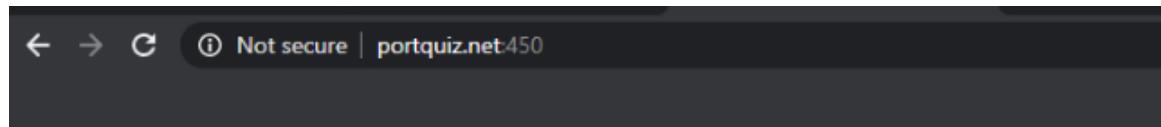
Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_TIMED_OUT

[Reload](#)

11. Try to access <http://portquiz.net:450> and the site should load right up, indicating that TCP connections to port 444 are being blocked (in line with our Firewall Policy)



Outgoing port tester

This server listens on all TCP ports, allowing you to test any outbound TCP port.

You have reached this page on port **450**.

Your network allows you to use this port. (Assuming that your network is not doing advanced traffic filtering.)

Network service: unknown

Your outgoing IP: 146.112.113.196

Test a port using a command

```
$ telnet portquiz.net 450
Trying ...
Connected to portquiz.net.
Escape character is '^]'.

$ nc -v portquiz.net 450
Connection to portquiz.net 450 port [tcp/daytime] succeeded!

$ curl portquiz.net:450
Port 450 test successful!
Your IP: 146.112.113.196

$ wget -qO- portquiz.net:450
Port 450 test successful!
Your IP: 146.112.113.196

# For Windows PowerShell users
PS C:\> Test-NetConnection -InformationLevel detailed -ComputerName portquiz.net -Port 450
```

Test a port using your browser

In your browser address bar: <http://portquiz.net:XXXX>

12. Other than using the Cloud Delivered Firewall to block specific ports, we can also block ICMP packets. Open a command prompt on the Site 30 PC and type `ping cisco.com`. Hit Enter. The pings should be successful

```
C:\Windows\System32>ping cisco.com
Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=288ms TTL=234
Reply from 72.163.4.185: bytes=32 time=287ms TTL=234

Ping statistics for 72.163.4.185:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 287ms, Maximum = 288ms, Average = 287ms
Control-C
^C
```

13. Go to the Umbrella GUI and navigate to **Policies => Management => Firewall Policy**. Click on **Add** to add a new policy and name it *blockicmp*

Rule Details

Define basic characteristics of the firewall rules.

| | |
|-----------|---------------------|
| Rule Name | Last Before Default |
| blockicmp | ▼ |

Description

Rule Criteria

Specify protocol, IPs, network tunnels, and ports to be blocked or allowed.

14. Set the **Protocol** as ICMP

Rule Criteria

Specify protocol, IPs, network tunnels, and ports to be blocked or allowed.

| | |
|----------|------|
| Protocol | ICMP |
|----------|------|

Source Tunnels

| | |
|-----|--|
| Any | Search and add specific source tunnels |
|-----|--|

Source IPs/CIDRs

| | |
|-----|---|
| Any | Add IP address or CIDRs in comma-delimited format |
|-----|---|

Destination IPs/CIDRs

| | |
|-----|---|
| Any | Add IP address or CIDRs in comma-delimited format |
|-----|---|

15. Make sure the Start Date is the earliest available and the Rule Action is set to block traffic, with logging enabled. Click on **Save** to save the firewall policy

Define the start and end date of the rule.

Time Zone
(UTC + 5.5) Asia / Calcutta

Start Date: Jul 6, 2020 Start Time: 02:52 AM TO Expiration Date: Mon DD YYYY Expiration Time:

Does Not Expire Choose the earliest available start date

Rule Action

Block or allow traffic that meets the rule criteria.

Block Traffic Allow Traffic

Logging Enabled
Logs for this firewall rule will be captured in Activity.

Firewall Rule Enabled
This rule is active.

Save the Firewall Policy

16. Wait for approximately 5 minutes and try to ping cisco.com from the Site 30 PC again. Pings should now be blocked

```
C:\Windows\System32>ping cisco.com

Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 72.163.4.185:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Windows\System32>
```

We have thus used a Firewall Policy to block traffic to a particular destination port and block a certain protocol. This completes our configuration of a Cloud Delivered Firewall.

Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - [API Keys and AD Configuration](#)
 - [DC Configuration Download](#)
 - [AD Connectors](#)
 - [Roaming Computer Configuration](#)
- [Building a DNS Policy](#)
- [Setting up IPSEC Tunnels](#)
- [Configuring a Firewall Policy](#)
- [Configuring a Web Policy](#)

Configuring a Web Policy

We will now apply a Web Policy to all traffic traversing the IPSEC Tunnels.

1. On the Umbrella GUI, navigate to **Policies => Policy Components => Destination Lists** and click on **Add**. Name the list *blockyahoo* and make sure that the **Blocked** radio button is selected. The **This Destination List is applied to** field should be **Web Policies**. Enter *yahoo.com* in the **Enter a domain, URL, IPv4 or CIDR** box and click on **Add**. Once yahoo.com shows up in the lower half of the screen, click on **Save**

New Destination List

If you want to block or allow a domain or URL, you can use destination lists to manage access.

List Name

This destination list is applied to:

Web Policies

Destinations in this list should be:

Blocked Allowed

Enter yahoo.com and click on Add

Enter a domain, URL, IPv4 or CIDR

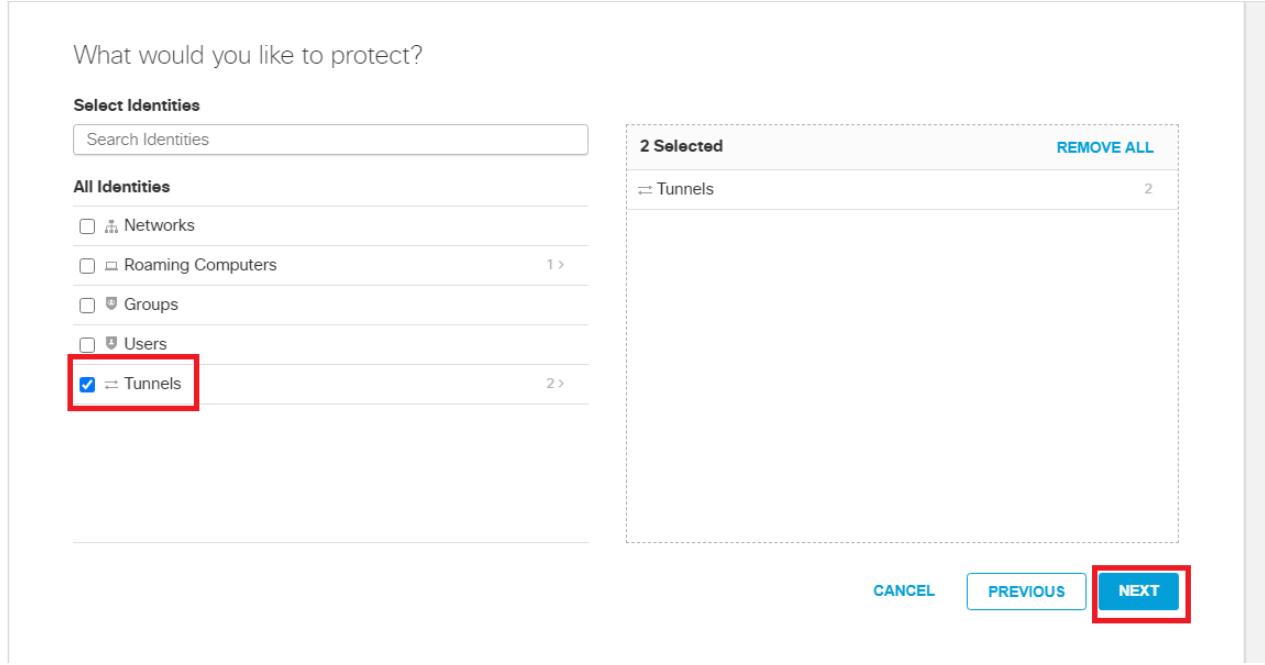
ADD UPLOAD

Search... CLEAR 1 total

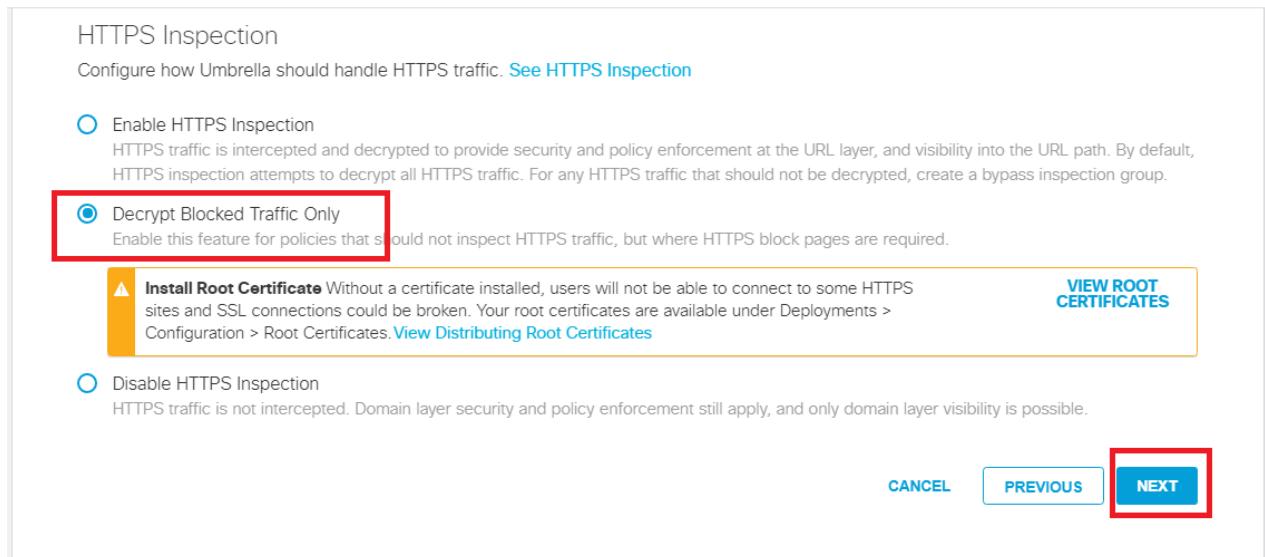
yahoo.com DOMAIN Add a comment X

CANCEL SAVE

2. Go to **Policies => Management => Web Policies** and click on **Add**. Click **Next** on the **How would you like to be protected?** window and put a check mark next to **Tunnels** in the **What would you like to protect?** window. Click on **Next**



3. Click the Radio Button next to **Decrypt Blocked Traffic Only** on the **HTTP Inspection** window and click on **Next**



4. Click **Next** for **Security Settings**, **Limit Content Access**, **Tenant Controls** and **Control Applications**. Put a check mark next to the **blockyahoo** Destination List and click on **Next**

Apply Destination Lists [ADD NEW LIST](#)

Search for and apply the appropriate block or allow Destination Lists for this policy. Click Add New List to create a Destination List.

The screenshot shows the 'Apply Destination Lists' section. On the left, there's a search bar and a 'Select All' checkbox. Below that is a list titled 'All Destination Lists' containing one item: 'blockyahoo' with a checked checkbox. A red box highlights the 'blockyahoo' entry. On the right, a summary box shows '1 Block Lists Applied' with 'blockyahoo' listed and a 'REMOVE ALL' button. At the bottom are 'CANCEL', 'PREVIOUS', and 'NEXT' buttons, with 'NEXT' being highlighted by a red box.

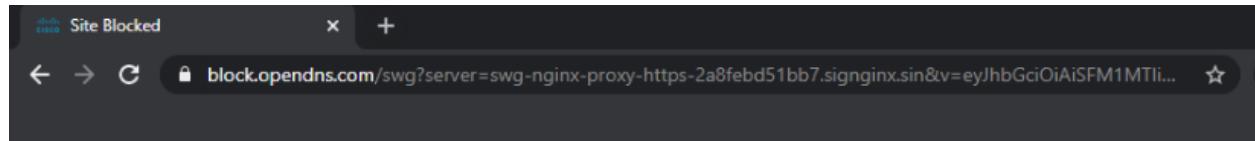
5. Click **Next** on **File Analysis, File Type Control** and **Set Block Page Settings**. Give the Policy a name of **Webblockyahoo** and click on **Save**. The policy should show up above the *Default Web Policy*

The screenshot shows the 'Web Policies' list. At the top, there's a header with 'Policies / Management' and a 'Cisco' logo. To the right is an 'Add' button with a plus sign. Below the header, a message explains that policies dictate security protection, category settings, and destination lists. It also notes that policies are enforced in descending order. A link to 'this article' is provided for more information. The main table lists two policies:

| | Name | Protection | Applied To | Contains | Last Modified | Actions |
|---|--------------------|------------|----------------|-------------------|---------------|---------|
| 1 | Webblockyahoo | Web Policy | 2 Identities | 5 Policy Settings | Jul 6, 2020 | |
| 2 | Default Web Policy | Web Policy | All Identities | 2 Policy Settings | Jul 3, 2020 | |

The table is sorted by Order of Enforcement. The 'Webblockyahoo' policy is listed first, followed by the 'Default Web Policy'. The 'Webblockyahoo' row has a red box around its name.

6. Wait for a few minutes and head over to the Site 30 PC. Click on the **Flush DNS** icon on the Desktop and open a new browser window. Try to access yahoo.com (you can use the bookmark). Traffic to Yahoo, which was working before, should now be blocked. Make note of the subtext *This site was blocked by the Cisco Umbrella proxy*



A screenshot of the Cisco Umbrella blocking page. At the top, the Cisco logo and "Cisco Umbrella" are visible. Below that, a large orange warning box contains the text "This site is blocked due to content filtering." with a yellow exclamation mark icon. A text input field shows "yahoo.com". Below the warning box, the message "Sorry, yahoo.com has been blocked by your network administrator." is displayed. A link "Report an incorrect block" is shown. Further down, the text "This site was blocked by the Cisco Umbrella proxy." is displayed, followed by a link "Diagnostic Info". At the bottom, there are links for "Terms", "Privacy Policy", and "Contact".

We have completed integration and configuration of Umbrella with our SD-WAN environment.

Task List

- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)

- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)
 - [API Keys and AD Configuration](#)
 - [DC Configuration Download](#)
 - [AD Connectors](#)
 - [Roaming Computer Configuration](#)
- [Building a DNS Policy](#)
- [Setting up IPSEC Tunnels](#)
- [Configuring a Firewall Policy](#)
- [Configuring a Web Policy](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: June 3, 2020

Site last generated: Sep 1, 2020



-->

Inter VPN Routing and Service Chaining

Summary: Implementing Inter VPN Routing between Site 20 VPN 10 and Site 30 VPN 20, along with Service Chaining (Firewall).

Table of Contents

- [Overview](#)
- [Configure VPN 40 on DC-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)

Task List

- Overview
- Configure VPN 40 on DC-vEdges
- Configuration Cleanup and Routing Verification
- Setting up VPN Lists
- Inter VPN Routing Policies
- Inter VPN Routing Verification
- Policies for Service Chaining
- Activity Verification

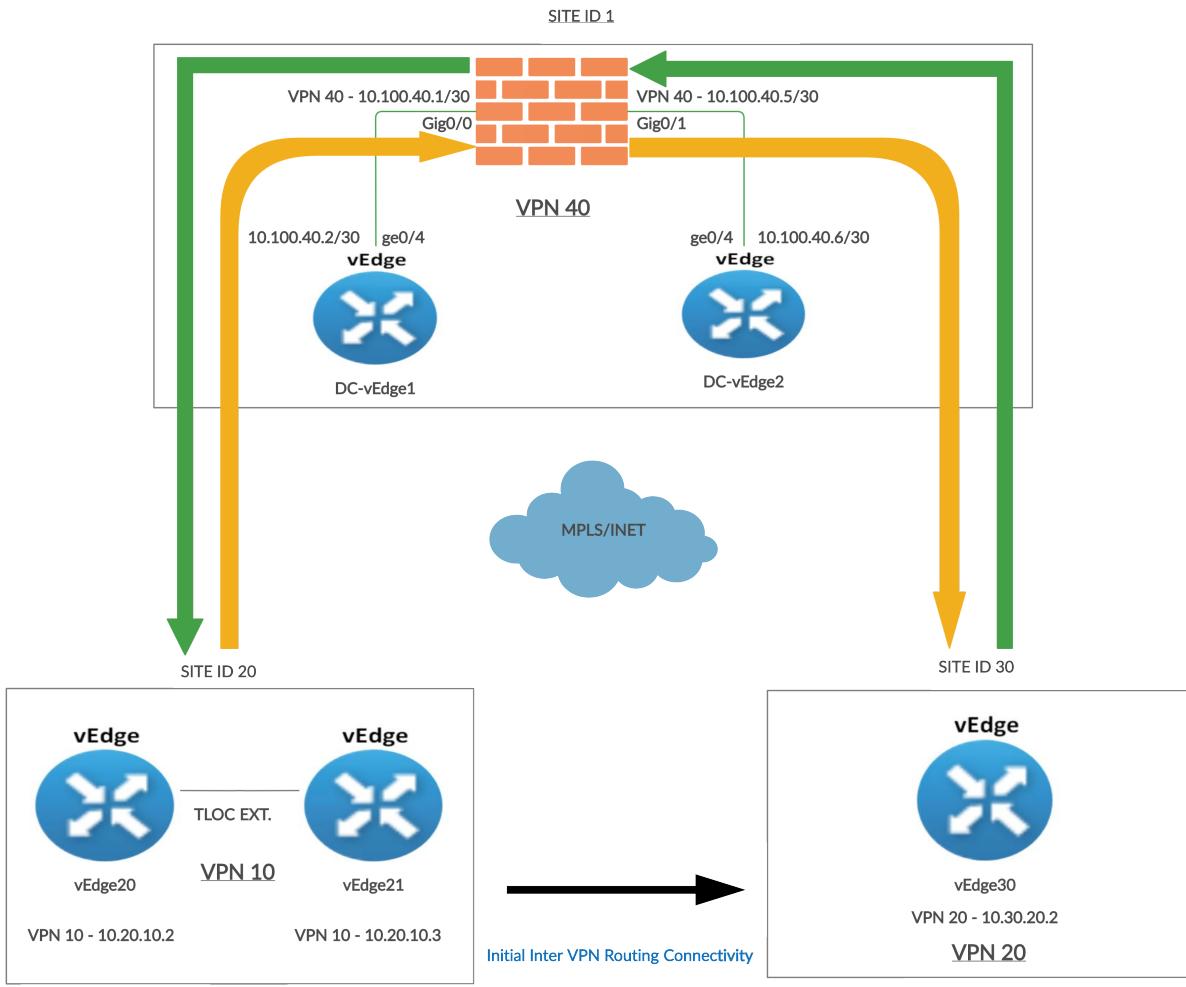
Overview

As of now, devices in different VPNs cannot communicate with each other. VPN 10 devices can talk to other VPN 10 devices but not to VPN 20. In this section, we will be setting up Inter VPN routing.

Additionally, there might be a requirement where we need to send traffic from one VPN to another through a firewall. This feature is known as Service Chaining (other devices like Load Balancers can also be part of the Service Chain) and is used widely in real-world SD-WAN Deployments.

We will be focussing on ensuring devices in Site 20 VPN 10 can communicate with devices in Site 30 VPN 20. Initially, this will be direct communication between the two VPNs. A firewall will then be inserted in the path so that all traffic between the VPNs traverses the firewall, which will be located at Site-DC in VPN 40.

Diagrammatically, our topology will look as below:



The Black arrow between Site 20 and Site 30 indicates the traffic flow when Inter VPN Routing configuration is done for the first time. Traffic flows directly between the two Sites.

The Orange arrow is the traffic flow from Site 20 VPN 10 to Site 30 VPN 20 once Service Chaining is configured.

Source IP: 10.20.10.2 or 10.20.10.3

Destination IP: 10.30.20.2

The Green arrow is the traffic flow from Site 30 VPN 20 to Site 20 VPN 10 once Service Chaining is configured.

Source IP: 10.30.20.2

Destination IP: 10.20.10.2 or 10.20.10.3

Task List

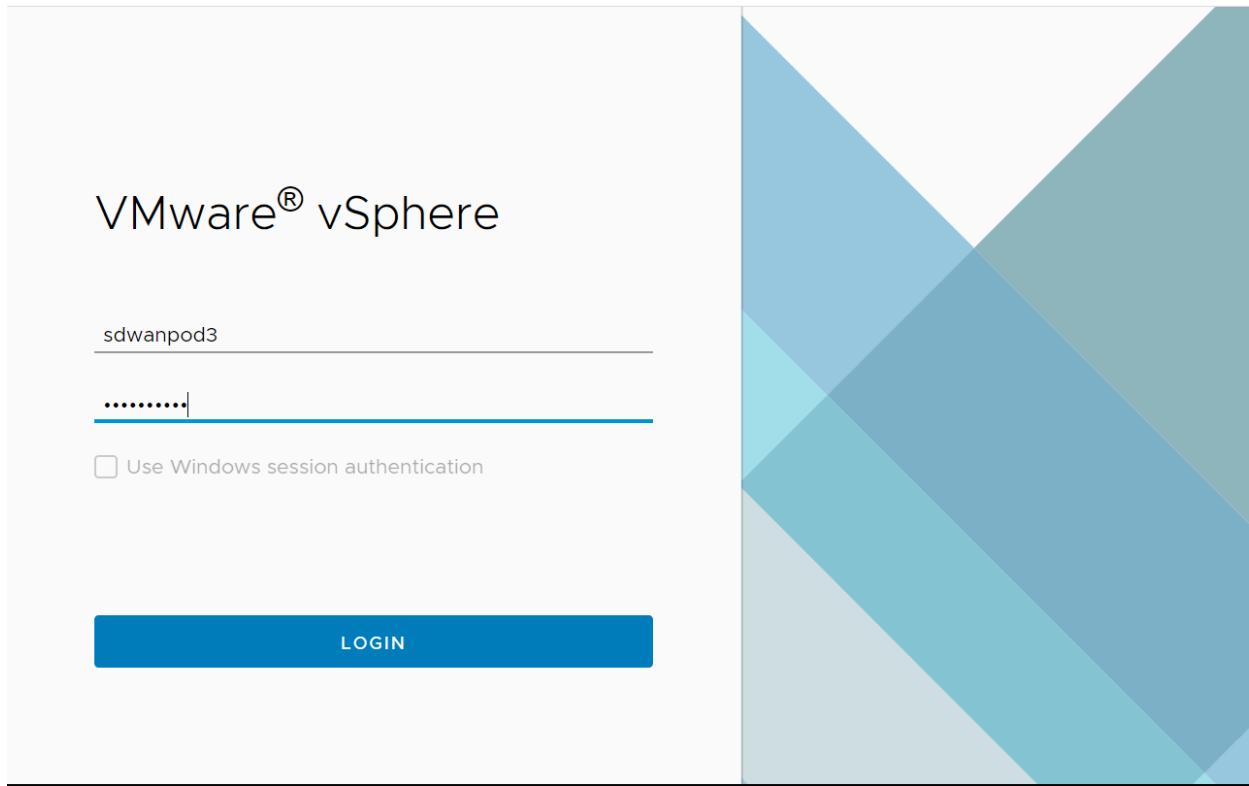
- [Overview](#)
- [Configure VPN 40 on DC-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)

Configure VPN 40 on DC-vEdges

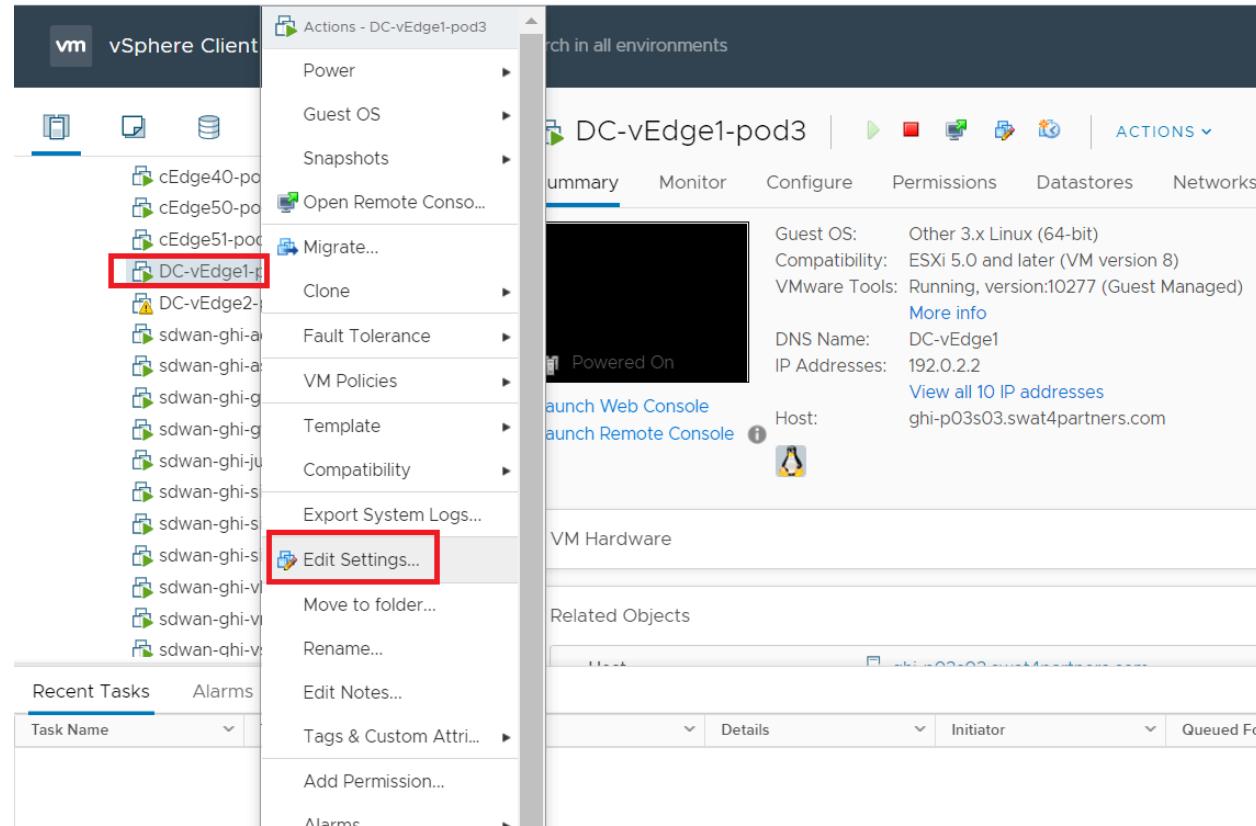
We will configure VPN 40 at the DC Site and ensure connectivity between the DC-vEdges and the ASA Firewall.

1. Log in to vCenter using the bookmark or by going to 10.2.1.50/ui from a web browser. Use the credentials for your POD

| Username | Password |
|------------------------|------------|
| sdwanpodX | C1sco12345 |
| (X is your POD number) | |



2. Right click on the **DC-vEdge1-podX** VM (where X is your POD number) and go to **Edit Settings**



3. Click on **Add New Device** and choose to add a new **Network Adapter**. Repeat this process to add another Network Adapter

Edit Settings | DC-vEdge1-pod3

X

Virtual Hardware VM Options

| | | |
|-------------------|----------------------|---|
| Network adapter 5 | Management | <input checked="" type="checkbox"/> Connected |
| MPLS10 | | <input checked="" type="checkbox"/> Connected |
| SiteDC_VPN10 | | <input checked="" type="checkbox"/> Connected |
| SiteDC-VPN20 | | <input checked="" type="checkbox"/> Connected |
| Internet | | <input checked="" type="checkbox"/> Connected |
| CD/DVD drive 1 | Host Device | <input type="checkbox"/> Connected |
| Video card | Auto-detect settings | |

CANCEL

OK

4. You should have two new network adapters. Click on the drop down next to the assigned network (Internet in the image below) for the first network adapter and click **Browse**

Edit Settings | DC-vEdge1-pod3

Virtual Hardware VM Options

ADD NEW DEVICE

| | | |
|---|---|--|
| > Network adapter 2 | MPLS10 | <input checked="" type="checkbox"/> Connected |
| > Network adapter 3 | SiteDC_VPN10 | <input checked="" type="checkbox"/> Connected |
| > Network adapter 4 | SiteDC-VPN20 | <input checked="" type="checkbox"/> Connected |
| > Network adapter 5 | Internet | <input checked="" type="checkbox"/> Connected |
| > New Network * | Internet | <input checked="" type="checkbox"/> Connected × |
| > New Network * | Internet | <input checked="" type="checkbox"/> Connected |
| > New Network * | Browse ... | |
| > CD/DVD drive 1 ! | Host Device | <input type="checkbox"/> Connected |
| > Video card | Auto-detect settings | |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface | |

CANCEL

OK

5. Choose *SiteDC_VPN10* and click on **OK**

Select Network

X

▼ Filter

| Name | Distributed Switch |
|----------------|--------------------|
| Site40-VPN30 | -- |
| Site50-VPN10 | -- |
| Site50-VPN20 | -- |
| Site50-VPN30 | -- |
| SiteDC-VPN20 | -- |
| SiteDC-VPN40 | -- |
| SiteDC-VPN40_2 | -- |
| SiteDC_VPN10 | -- |
| TLOCEXT2_vEdge | -- |

40 items

CANCEL

OK

6. This takes you back to the **Edit Settings** page. Click on the drop down next to the assigned network for the second network adapter and click **Browse**. Select *SiteDC-VPN40* and click on **OK**

Select Network

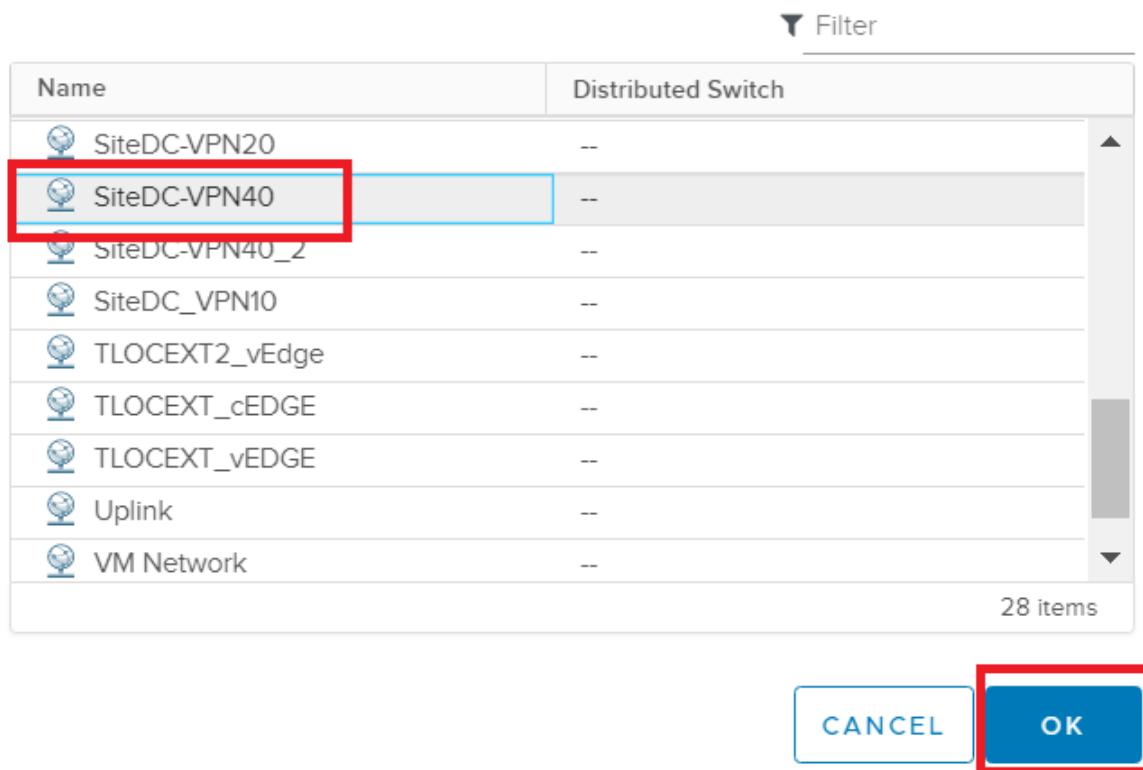
X

Filter

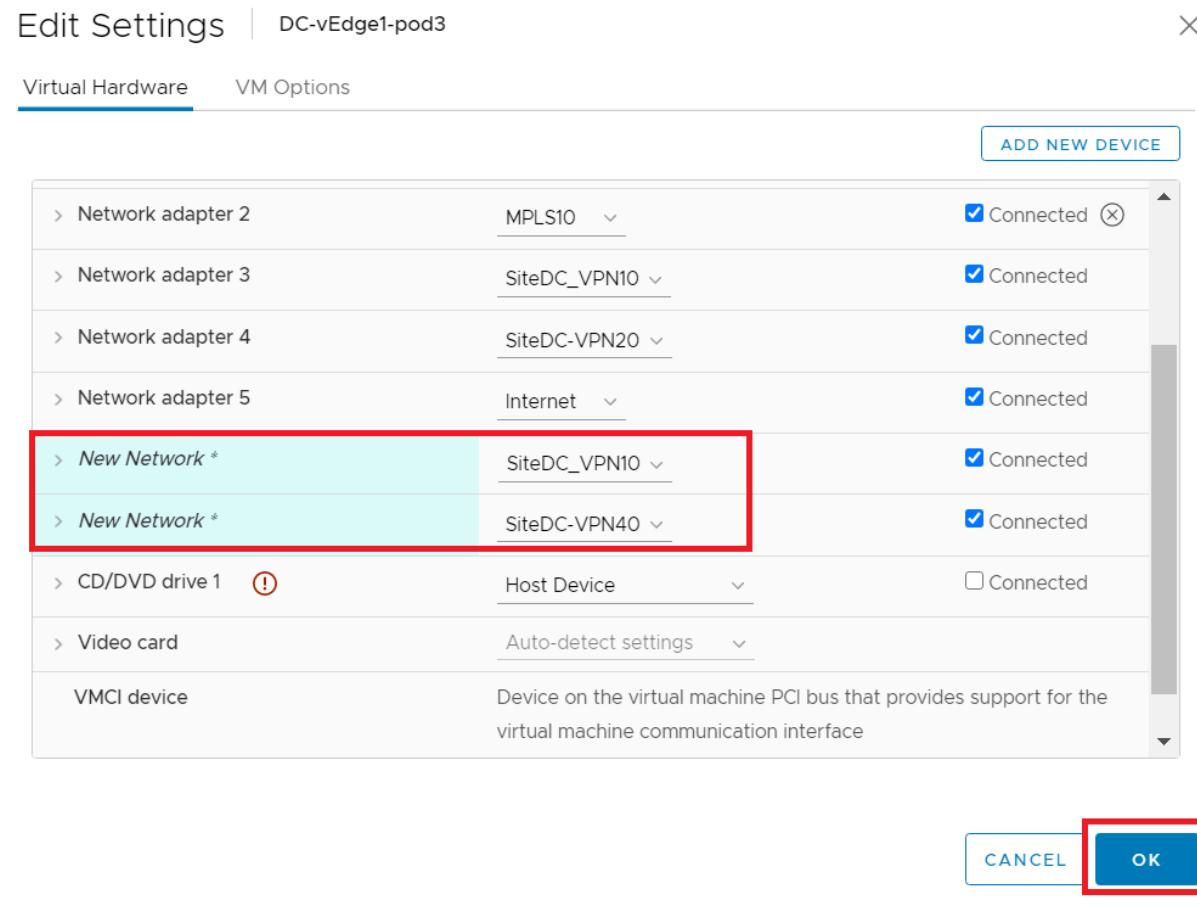
| Name | Distributed Switch |
|----------------|--------------------|
| SiteDC-VPN20 | -- |
| SiteDC-VPN40 | -- |
| SiteDC-VPN40_2 | -- |
| SiteDC_VPN10 | -- |
| TLOCEXT2_vEdge | -- |
| TLOCEXT_cEDGE | -- |
| TLOCEXT_vEDGE | -- |
| Uplink | -- |
| VM Network | -- |

28 items

CANCEL OK

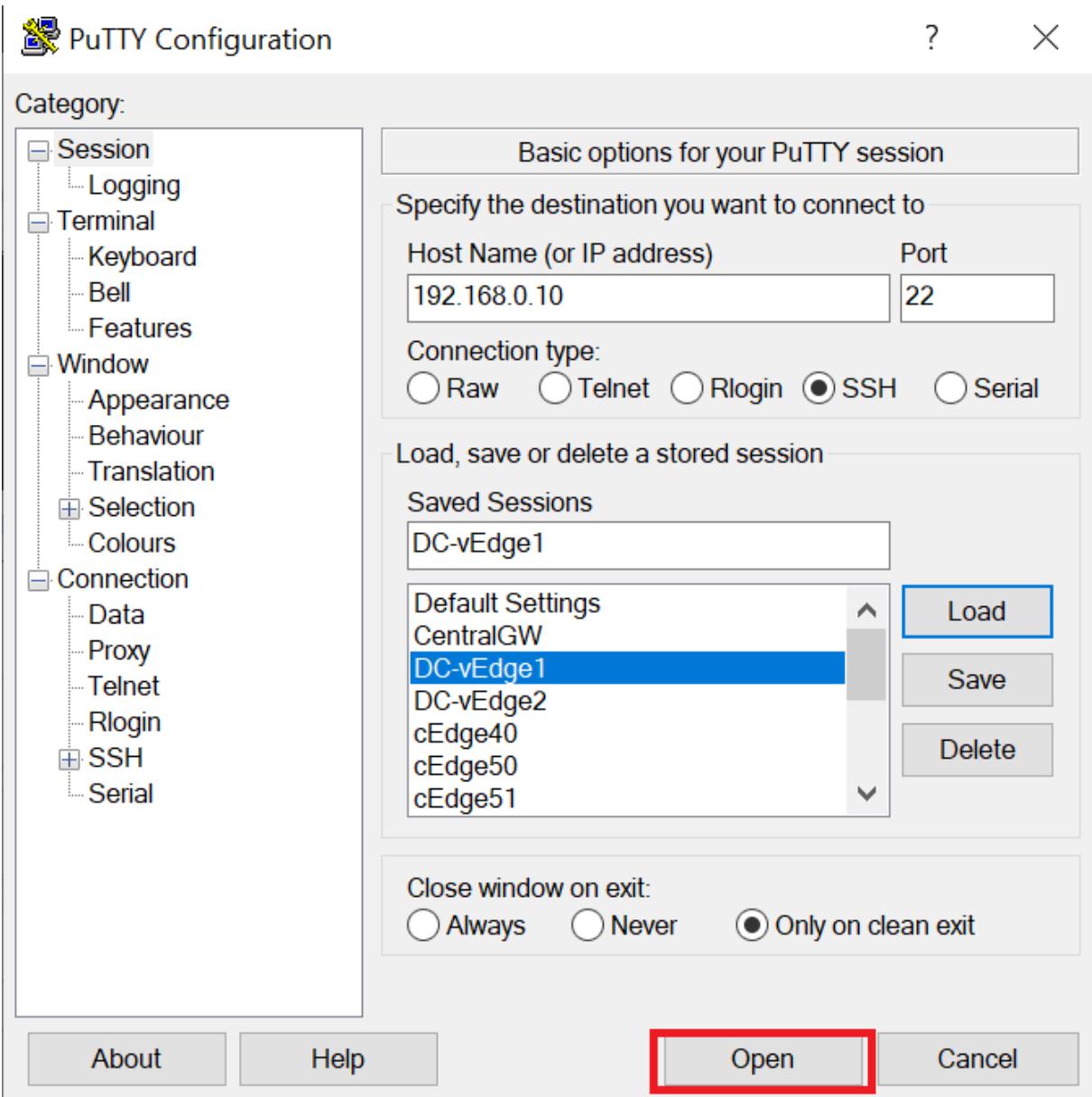


7. Make sure the settings match with the image given below and click on **OK**



8. Log in to **DC-vEdge1** via Putty. You can use the saved session or SSH to 192.168.0.10 along with the credentials given below

| Username | Password |
|----------|----------|
| admin | admin |

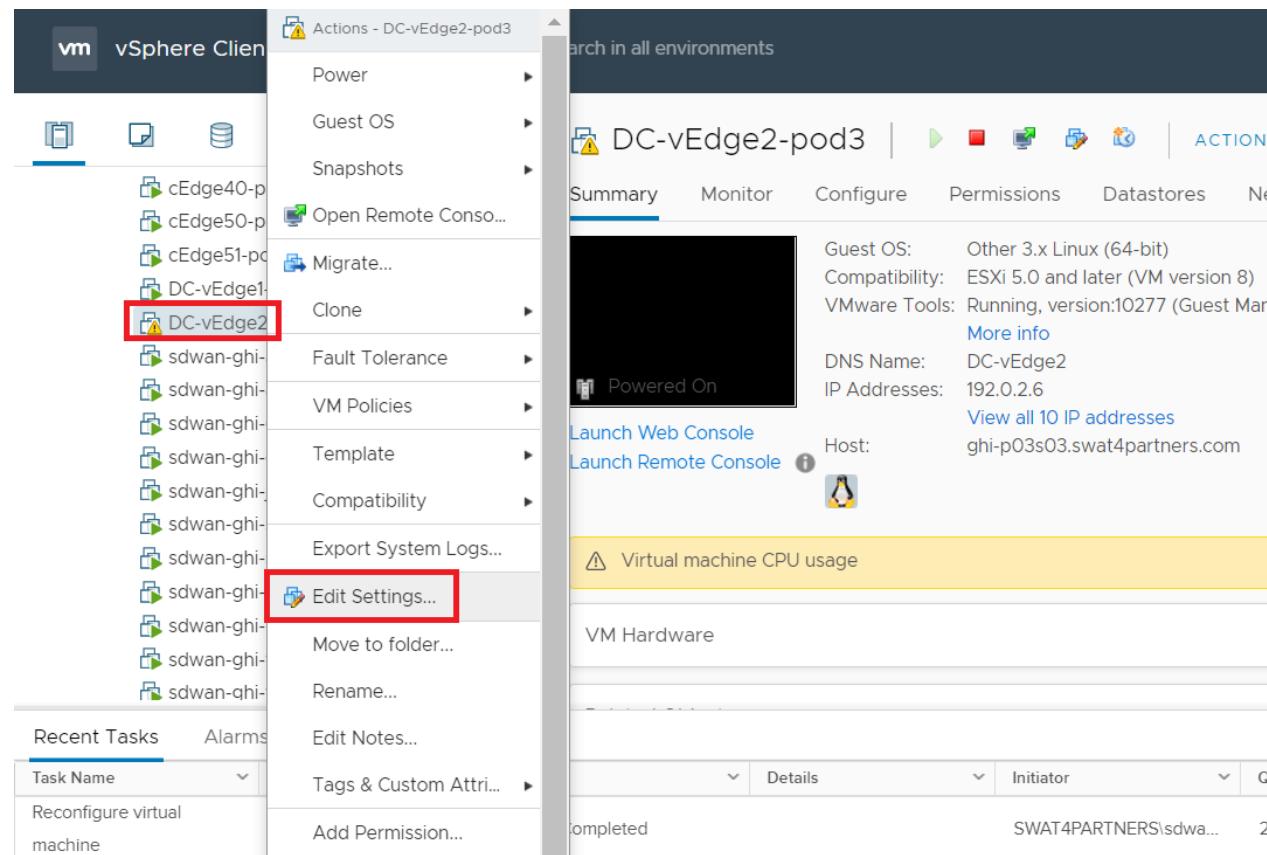


9. Type `reboot` and then `yes` to confirm the reboot

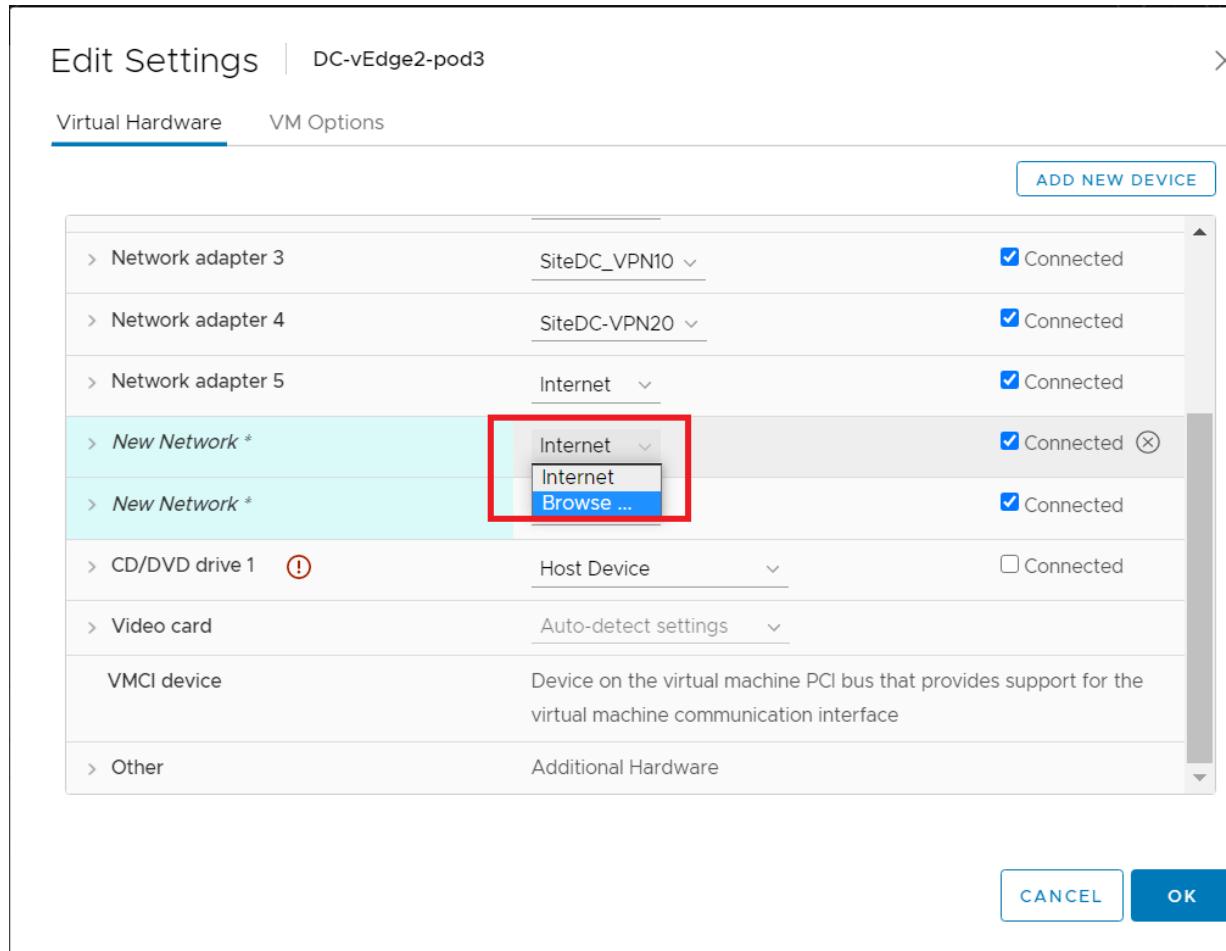
```
<CLI>
DC-vEdge1# reboot
Are you sure you want to reboot? [yes,NO] yes
DC-vEdge1# Mon Jul 20 17:39:11 UTC 2020: The system is going down for reboot NOW!
[
```

```
reboot
yes
```

10. While the DC-vEdge1 vEdge is rebooting, head over to vCenter and right click on the **DC-vEdge2-podX** VM. Click on **Edit Settings**



11. Like before, add two network adapters by clicking on **Add New Device** and selecting **Network Adapter**. Make sure you add two network adapters. Click on the drop down for the first Network Adapter and choose **Browse**



12. Select *SiteDC_VPN10* and click on **OK**

Select Network

X

▼ Filter

| Name | Distributed Switch |
|----------------|--------------------|
| Site40-VPN30 | -- |
| Site50-VPN10 | -- |
| Site50-VPN20 | -- |
| Site50-VPN30 | -- |
| SiteDC-VPN20 | -- |
| SiteDC-VPN40 | -- |
| SiteDC-VPN40_2 | -- |
| SiteDC_VPN10 | -- |
| TLOCEXT2_vEdge | -- |

40 items

CANCEL

OK

13. Click on the drop down next to the second network adapter and click on browse. Select SiteDC-VPN40_2 and click on OK. The network adapters should look like the image below

Edit Settings | DC-vEdge2-pod3

Virtual Hardware VM Options

ADD NEW DEVICE

| | | |
|---------------------|---|---|
| > Network adapter 3 | SiteDC_VPN10 ▾ | <input checked="" type="checkbox"/> Connected |
| > Network adapter 4 | SiteDC-VPN20 ▾ | <input checked="" type="checkbox"/> Connected |
| > Network adapter 5 | Internet ▾ | <input checked="" type="checkbox"/> Connected |
| > New Network * | SiteDC_VPN10 ▾ | <input checked="" type="checkbox"/> Connected |
| > New Network * | SiteDC-VPN40_2 ▾ | <input checked="" type="checkbox"/> Connected |
| > CD/DVD drive 1 ⓘ | Host Device ▾ | <input type="checkbox"/> Connected |
| > Video card | Auto-detect settings ▾ | |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface | |
| > Other | Additional Hardware | |

CANCEL

OK

14. Log in to *DC-vEdge2* via Putty, using the credentials below

| Username | Password |
|----------|----------|
| admin | admin |

PuTTY Configuration

?

X

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
- + Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - + SSH
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

192.168.0.11 22

Connection type:

Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

DC-vEdge2

Default Settings

CentralGW

DC-vEdge1

DC-vEdge2

cEdge40

cEdge50

cEdge51

Load

Save

Delete

Close window on exit:

Always Never Only on clean exit

About

Help

Open

Cancel

15. Type `show interface ?` and notice that there are 4 "ge" interfaces

192.168.0.11 - PuTTY

```
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on DC-vEdge2
DC-vEdge2# show interface ?
Possible completions:
arp-stats      Display ARP statistics
description    Display interface information
detail        Display detailed interface information
errors         Display error statistics
eth0
eth1
ge0/0          ge0/0
ge0/1          ge0/1
ge0/2          ge0/2
ge0/3          ge0/3
packet-sizes   Display packet sizes
port-stats     Display port statistics
queue          Display queue statistics
sfp            Display SFP information
statistics    Display interface statistics
system
vpn           VPN ID
|
<cr>
DC-vEdge2# show interface
```

```
show interface ?
```

16. Type `reboot` and then `yes` to confirm the reboot

192.168.0.11 - PuTTY

```
arp-stats      Display ARP statistics
description   Display interface information
detail        Display detailed interface information
errors        Display error statistics
eth0
eth1
ge0/0
ge0/1
ge0/2
ge0/3
packet-sizes  Display packet sizes
port-stats    Display port statistics
queue         Display queue statistics
sfp           Display SFP information
statistics    Display interface statistics
system
vpn          VPN ID
|
<cr>
DC-vEdge2# reboot
Are you sure you want to reboot? [yes,NO] yes
DC-vEdge2# Mon Jul 20 17:42:37 UTC 2020: The system is going down for reboot NOW!
!
```

```
reboot
yes
```

17. Once *DC-vEdge1* and *DC-vEdge2* are back up, log in to either device and issue `show interface ?` again. You will notice two additional interfaces - `ge0/4` and `ge0/5`

```
DC-vEdge1# show interface ?
Possible completions:
arp-stats      Display ARP statistics
description   Display interface information
detail        Display detailed interface information
errors         Display error statistics
eth0
ge0/0
ge0/1
ge0/2
ge0/3
ge0/4
ge0/5
packet-sizes  Display packet sizes
port-stats    Display port statistics
queue         Display queue statistics
sfp           Display SFP information
statistics   Display interface statistics
system
vpn          VPN ID
|
<cr>
DC-vEdge1# show interface
```

18. Log in to the vManage GUI using the bookmark or by going to 192.168.0.6 on a web browser. Click on **Configuration => Templates**

The screenshot shows the Cisco vManage Main Dashboard. On the left, a sidebar menu is open under the 'Configuration' tab, with the 'Templates' tab highlighted by a red box. The main dashboard displays several key metrics:

- Smart - 2**: 2 up, 2 down.
- WAN Edge - 8**: 8 up, 0 down.
- vBond - 1**: 1 up, 0 down.
- vManage - 1**: 1 up, 0 down.

Site Health (Total 5):

- Full WAN Connectivity: 5 sites
- Partial WAN Connectivity: 0 sites
- No WAN Connectivity: 0 sites

WAN Edge Health (Total 8):

- Normal: 8
- Warning: 0
- Error: 0

Application-Aware Routing:

| Tunnel Endpoints | Avg. Latency (ms) |
|-----------------------------|-------------------|
| vEdge20:mpls-DC-vEdge2:mpls | 2.346 |

19. Go to the **Feature** tab and click on **Add Template**. Search for **vedge** and put a check mark next to **vEdge Cloud**. Choose **VPN** to create a VPN Template

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template

Select Devices

vEdge

- vEdge 100
- vEdge 100 B
- vEdge 100 M
- vEdge 100 WM
- vEdge 1000
- vEdge 2000
- vEdge 5000
- vEdge Cloud

Select Template

BASIC INFORMATION

- AAA
- Archive
- NTP
- OMP
- System

VPN

- Secure Internet Gateway (SIG)
WAN
- VPN**
- VPN Interface Cellular
WAN
- VPN Interface Ethernet
Management|WAN|LAN
- VPN Interface IPsec
- VPN Interface NATPool

20. Give a **Template Name** of `dc-vedge-vpn40` and a Description of *vEdge VPN 40 Template for Service Chaining*. Put the VPN as *40*

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > **VPN**

Device Type vEdge Cloud

Template Name `dc-vedge-vpn40`

Description vEdge VPN 40 Template for Service Chaining

Basic Configuration DNS Advertise OMP IPv4 Route IPv6 Route Service Service Route GRE Route IPSEC Route

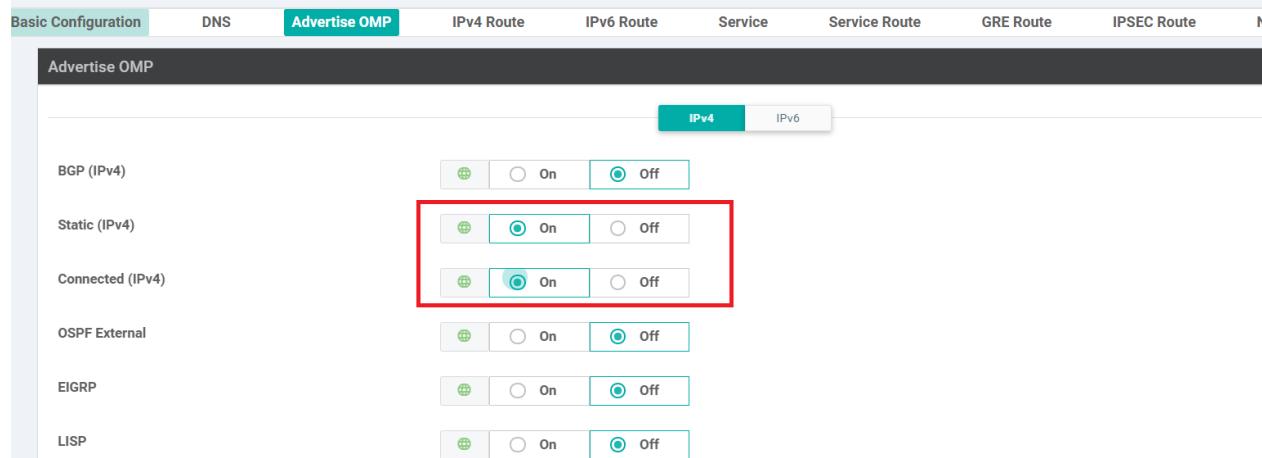
BASIC CONFIGURATION

VPN

Name

Enhance ECMP Keying On Off

21. Scroll down to the **Advertise OMP** section and set **Static (IPv4)** and **Connected (IPv4)** to **On**



22. Go to the **Service** section and click on **New Service**. Select the **Service Type** as *netsvc1* and enter an **IPv4 Address** of *10.100.40.1*. Click on **Add**



23. Click on **New Service** again and select the **Service Type** as *netsvc2*. Enter an **IPv4 Address** of *10.100.40.5*. Click on **Add** then click on **Save** to save the VPN Template configuration

SERVICE

New Service

| | |
|-------------------|-------------|
| Service Type | netsvc2 |
| IP Address | Interface |
| IPv4 address | 10.100.40.5 |
| Add Cancel | |

| Service Type | IP Addresses (Maximum: 4) | Interfaces | Action |
|--------------|---------------------------|------------|---------------------------|
| netsvc1 | 10.100.40.1 | | Edit Delete |

Save Cancel

24. At the Configuration => Templates => Feature Tab page, click on Add Template. Search for vedge and select vEdge Cloud. Choose VPN Interface Ethernet as the Template Type

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > **Add Template**

| | |
|---|---|
| Select Devices | <input type="text" value="vedge"/> <input type="checkbox"/> vEdge 100 <input type="checkbox"/> vEdge 100 B <input type="checkbox"/> vEdge 100 M <input type="checkbox"/> vEdge 100 WM <input type="checkbox"/> vEdge 1000 <input type="checkbox"/> vEdge 2000 <input type="checkbox"/> vEdge 5000 <input checked="" type="checkbox"/> vEdge Cloud |
| System VPN <ul style="list-style-type: none"> <input type="checkbox"/> Secure Internet Gateway (SIG) WAN <input type="checkbox"/> VPN Interface Ethernet Management WAN LAN <input type="checkbox"/> VPN Interface Cellular WAN <input type="checkbox"/> VPN Interface IPsec WAN <input type="checkbox"/> VPN Interface NATPool WAN <input type="checkbox"/> VPN Interface PPP Ethernet | |

25. Give a **Template Name** of *dc-vedge-vpn40-int1* with a Description of DC vEdge VPN 40 interface. Set **Shutdown** to No and the **Interface Name** as a Global value of *ge0/4*. Set the **IPv4 Address** to a Device Specific value of *vpn40_if_ipv4_address* and click on **Save**

⚙️ CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > [VPN Interface Ethernet](#)

| | |
|---------------|---------------------------|
| Device Type | vEdge Cloud |
| Template Name | dc-vedge-vpn40-int1 |
| Description | DC vEdge VPN 40 interface |

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

BASIC CONFIGURATION

Shutdown Yes No

Interface Name ge0/4

Description

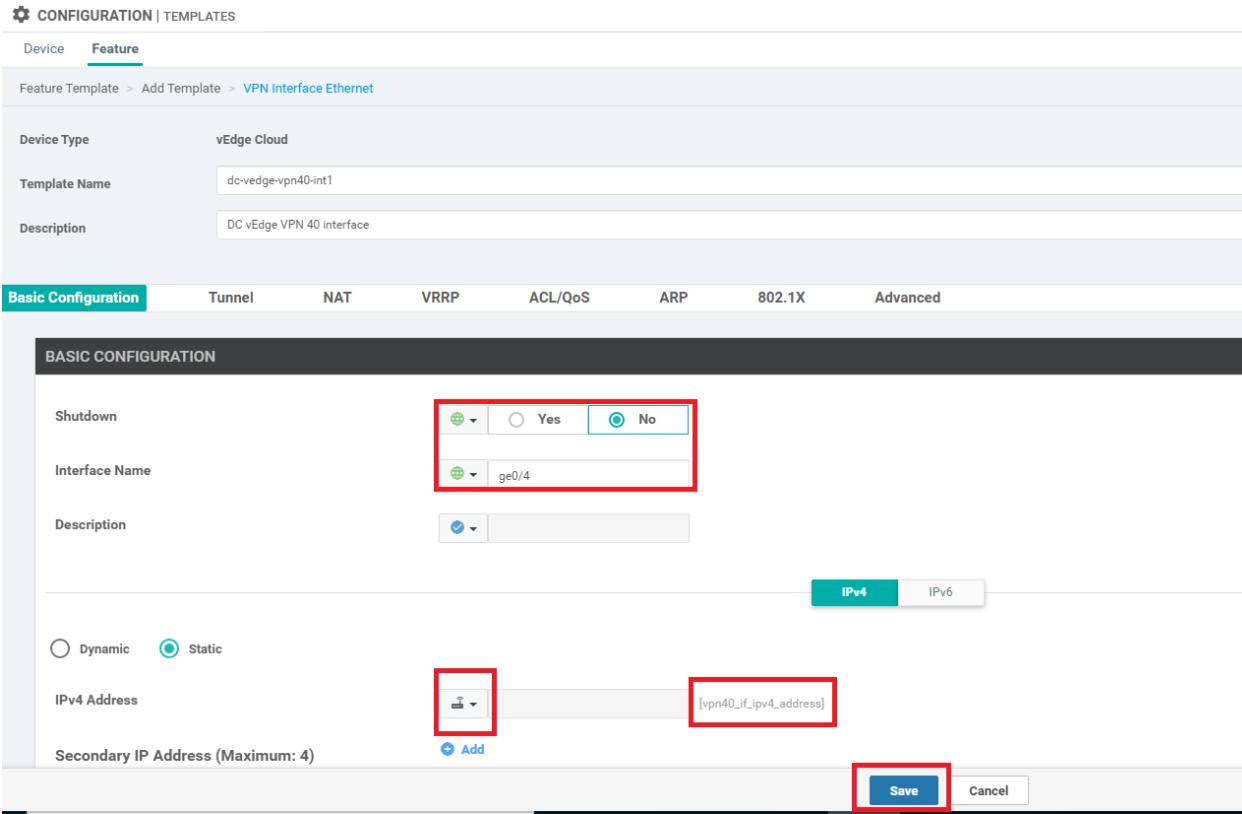
IPv4 **IPv6**

Dynamic Static

IPv4 Address [vpn40_if_ipv4_address]

Secondary IP Address (Maximum: 4) Add

Save **Cancel**



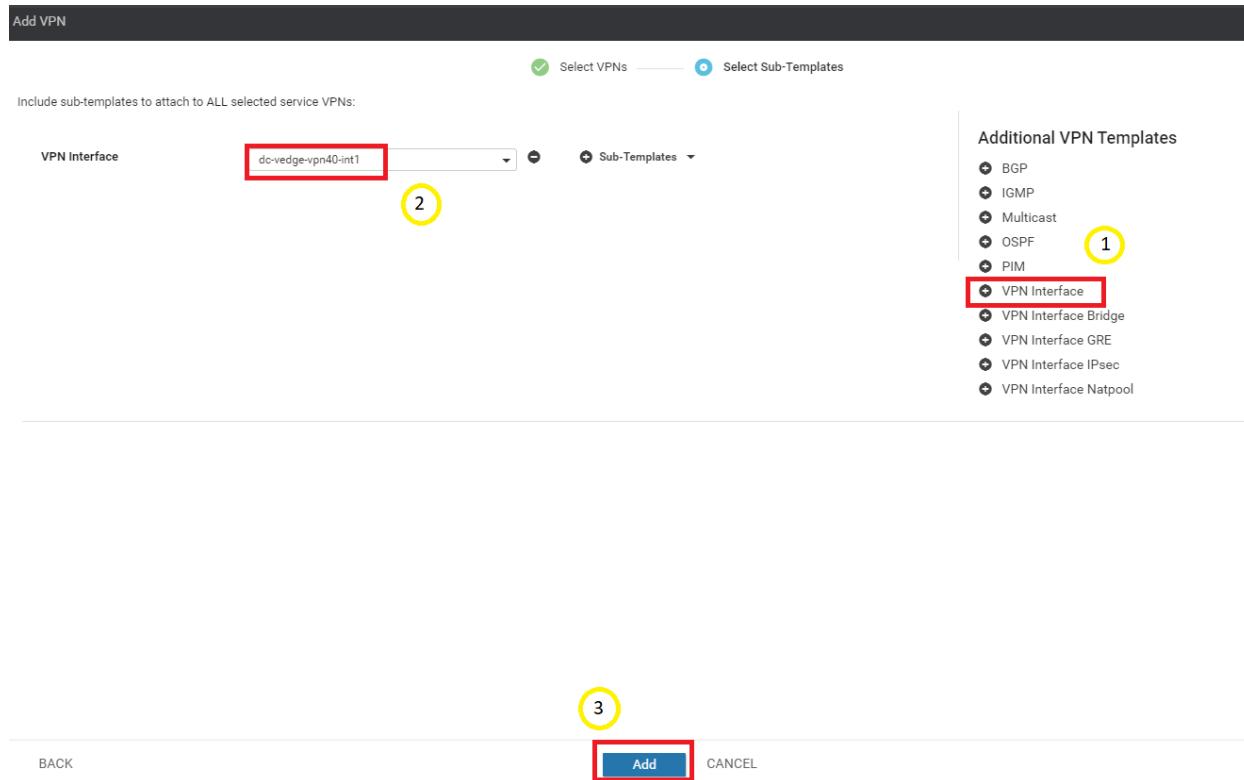
26. Go to **Configuration => Templates** on the vManage GUI and make sure you're on the **Device** tab. Locate the *DCvEdge_dev_temp* template and click on the three dots next to it. Choose to **Edit** the template

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | TEMPLATES' section. The 'Device' tab is selected. A table lists various device templates, including 'cEdge-single-up...', 'vEdge30_dev_t...', 'vEdge_Site20_d...', 'cedge_dualuplink...', 'vSmart-dev-temp...', 'vEdge_Site20_d...', and 'DCvEdge_dev_t...'. The 'DCvEdge_dev_t...' row is highlighted with a red box. A context menu is open over this row, with the 'Edit' option highlighted and another red box around it. Other options in the menu include View, Delete, Copy, Attach Devices, Detach Devices, Export CSV, and Change Device Values.

27. Scroll down to the **Service VPN** section and click on **Add VPN**. Move the *dc-vedge-vpn40* template to the right-hand side and click on **Next**

The screenshot shows the 'Create VPN Template' dialog. In the 'Service VPN' section, the 'Add VPN' button is highlighted with a red box. Below it, there's a table for 'Available VPN Templates' with one entry: 'vedge-vpn20'. To the right, a 'Selected VPN Templates' table shows one entry: 'dc-vedge-vpn40', which is also highlighted with a red box. At the bottom, there are 'Create VPN Template' and 'Next' buttons, with 'Next' highlighted with a red box.

28. Click on **VPN Interface** under **Additional VPN Templates** and select *dc-vedge-vpn40-int1* under the VPN Interface drop down. Click on **Add**



29. Make sure the Service VPN section shows the addition of the VPN 40 Template and click on **Update**

The screenshot shows the 'Service VPN' configuration interface. At the top, there are buttons for '0 Rows Selected', 'Add VPN', and 'Remove VPN'. Below is a search bar and a 'Search Options' dropdown. A table lists three templates: 'vedge-vpn10' (Sub-Templates: OSPF, VPN Interface), 'vedge-vpn20-DC' (Sub-Templates: VPN Interface), and 'dc-vedge-vpn40' (Sub-Templates: VPN Interface). The 'dc-vedge-vpn40' row is selected and highlighted with a red box. Below the table is an 'Additional Templates' section with dropdowns for Banner, Policy, SNMP, and Security Policy. At the bottom is a 'Update' button (highlighted with a red box) and a 'Cancel' button.

30. Enter the **IPv4 Address** field for *vpn40_if_ipv4_address* as 10.100.40.2/30 (for DC-vEdge1) and 10.100.40.6/30 (for DC-vEdge2). Click on **Next**

CONFIGURATION | TEMPLATES

Device Template | DCvEdge_dev_temp

Total Rows: 2

| S. | Chassis Number | System IP | Hostname | IPv4 Address(vp40_if_ip4_address) | Interface Name(vp20_if_name) | IPv4 Addr |
|----|--------------------------------------|---------------|-----------|-----------------------------------|------------------------------|---------------|
| 1 | 0cdd4f0e-f2f1-fe75-866c-469966cd1c3 | 10.255.255.12 | DC-Edge2 | 10.100.40.6/30 | ge0/3 | 10.100.20.*** |
| 2 | e474c5fd-8ce7-d376-7cac-ba950b2c9159 | 10.255.255.11 | DC-vEdge1 | 10.100.40.2/30 | ge0/3 | 10.100.20.*** |

Next **Cancel**

31. Click on **Configure Devices**. You can choose to view the side by side configuration, if required, noting the addition of vpn 40 with the corresponding service addresses

DCvEdge_dev_temp 1

Device list (Total: 2 devices)

Filter/Search

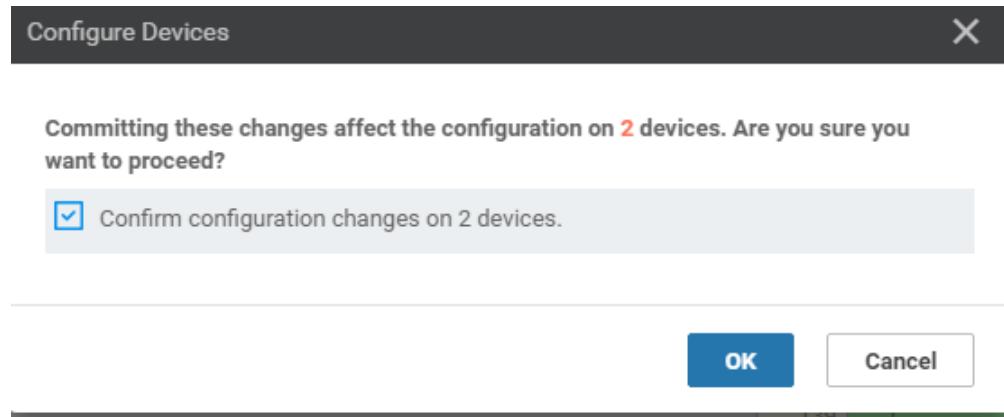
| | | | |
|---|---|---|---|
| 0cdd4f0e-f2f1-fe75-866c-469966cd1c3 DC-Edge2 10.255.255.12 | 120 no shutdown 121 ! 122 ip route 0.0.0.0/0 null0 123 ospf 124 advertise connected 125 advertise static 126 ! 127 ! | 120 no shutdown 121 ! 122 ip route 0.0.0.0/0 null0 123 ospf 124 advertise connected 125 advertise static 126 ! 127 ! | 128 vpn 40 129 service netsvc1 address 10.100.40.1 130 service netsvc2 address 10.100.40.5 131 interface ge0/4 132 ip address 10.100.40.2/30 133 no shutdown 134 ! 135 ospf 136 advertise connected 137 advertise static 138 ! 139 ! |
| e474c5fd-8ce7-d376-7cac-ba950b2c9159 DC-vEdge1 10.255.255.11 | 128 vpn 512 129 dns 10.2.1.5 primary 130 ip address 10.2.1.5/24 secondary... | 140 vpn 512 141 dns 10.2.1.5 primary 142 ip address 10.2.1.5/24 secondary... | |

Configure Device Rollback Timer

Main Dashboard

Back **Configure Devices** **Cancel**

32. Confirm the configuration change by clicking on the check box and clicking on **OK**



33. Once the configuration update goes through, log in to the CLI of **DC-vEdge1** and **DC-vEdge2** via Putty and issue the following commands. You should see successful ping responses:

On DC-vEdge1 - `ping vpn 40 10.100.40.1` On DC-vEdge2 - `ping vpn 40 10.100.40.5`

```

192.168.0.10 - PuTTY
login as: admin
Pre-authentication banner message from server:
| viptela 20.1.1
|
End of banner message from server
admin@192.168.0.10's password:
Last login: Mon Jul 20 17:43:04 2020 from 192.168.0.121
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on DC-vEdge1
DC-vEdge1# ping vpn 40 10.100.40.1
Ping in VPN 40
PING 10.100.40.1 (10.100.40.1) 56(84) bytes of data.
64 bytes from 10.100.40.1: icmp_seq=1 ttl=255 time=1.32 ms
64 bytes from 10.100.40.1: icmp_seq=2 ttl=255 time=0.660 ms
64 bytes from 10.100.40.1: icmp_seq=3 ttl=255 time=0.622 ms
64 bytes from 10.100.40.1: icmp_seq=4 ttl=255 time=0.545 ms
64 bytes from 10.100.40.1: icmp_seq=5 ttl=255 time=0.355 ms
64 bytes from 10.100.40.1: icmp_seq=6 ttl=255 time=0.832 ms
...
--- 10.100.40.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.355/0.723/1.324/0.303 ms
DC-vEdge1# 

192.168.0.11 - PuTTY
login as: admin
Pre-authentication banner message from server:
| viptela 20.1.1
|
End of banner message from server
admin@192.168.0.11's password:
Last login: Mon Jul 20 17:42:12 2020 from 192.168.0.121
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on DC-vEdge2
DC-vEdge2# ping vpn 40 10.100.40.5
Ping in VPN 40
PING 10.100.40.5 (10.100.40.5) 56(84) bytes of data.
64 bytes from 10.100.40.5: icmp_seq=1 ttl=255 time=0.861 ms
64 bytes from 10.100.40.5: icmp_seq=2 ttl=255 time=0.630 ms
64 bytes from 10.100.40.5: icmp_seq=3 ttl=255 time=0.522 ms
64 bytes from 10.100.40.5: icmp_seq=4 ttl=255 time=0.430 ms
64 bytes from 10.100.40.5: icmp_seq=5 ttl=255 time=0.413 ms
64 bytes from 10.100.40.5: icmp_seq=6 ttl=255 time=0.768 ms
...
--- 10.100.40.5 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.413/0.604/0.861/0.166 ms
DC-vEdge2# 

```

This completes the configuration needed for adding VPN 40 to the DC-vEdges.

Task List

- Overview
- Configure VPN 40 on DC-vEdges
- Configuration Cleanup and Routing Verification
- Setting up VPN Lists

- Inter VPN Routing Policies
- Inter VPN Routing Verification
- Policies for Service Chaining
- Activity Verification

Configuration Cleanup and Routing Verification

1. On the vManage GUI, go to **Configuration => Templates => Feature Tab**. Locate the *vedge-vpn20-DC* template and click on the three dots next to it. Choose to **Edit** the template

The screenshot shows the 'TEMPLATES' section under 'Feature'. A table lists various templates. The first row, 'vedge-vpn20-DC', has its '...' column highlighted with a red box. A context menu is open over this row, showing options: View, Edit (which is highlighted with a red box), Change Device Models, Delete, and Copy.

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated |
|---------------------|--------------------------------|--------------------|--------------|------------------|------------------|------------|--------------------------|
| vedge-vpn20-DC | VPN 20 Template for vEdge... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 21 Jun 2020 4:06:06 ... |
| DC-vEdge_MPLS | MPLS interface for the DC-... | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 18 Jun 2020 9:46:20 ... |
| DCvEdge-vpn512 | VPN512 for the DC-vEdges | WAN Edge VPN | vEdge Cloud | 4 | 5 | admin | 18 Jun 2020 9:41:03 ... |
| DCvEdge-vpn0 | VPN0 for the DC-vEdges IN... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 18 Jun 2020 9:46:20 ... |
| DC-OSPF | OSPF Template for the DC | OSPF | vEdge Cloud | 1 | 2 | admin | 19 Jun 2020 12:38:18 ... |
| dc-vedge-vpn40 | vEdge VPN 40 Template for... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 20 Jul 2020 12:38:18 ... |
| DC-vEdge_mgmt_int | MGMT interface for the DC-... | WAN Edge Interface | vEdge Cloud | 4 | 5 | admin | 18 Jun 2020 9:46:20 ... |
| DC-vEdge_INET | INET interface for the DC-v... | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 18 Jun 2020 9:41:03 ... |
| dc-vedge-vpn40-int1 | DC vEdge VPN 40 interface | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 20 Jul 2020 12:38:18 ... |

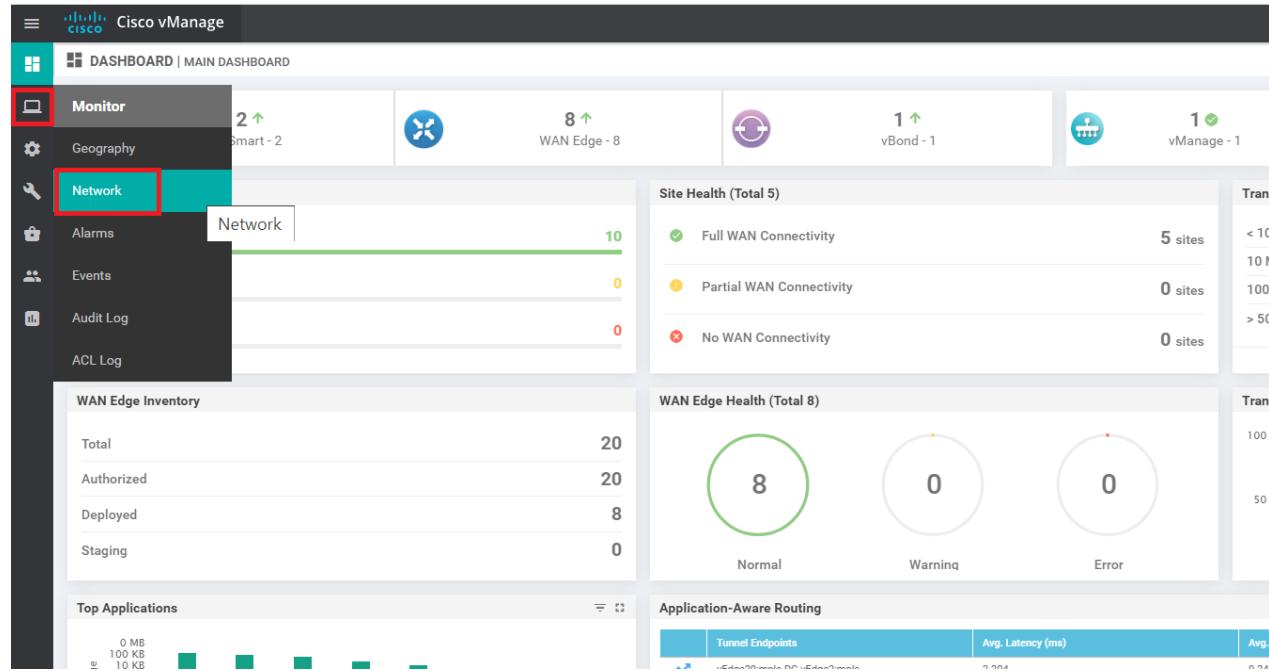
2. Scroll down to the IPv4 Route section and delete the route populated (it should be a null route) by clicking on the **trash icon**. Click on **Update**. Click **Next** and **Configure Devices** to push the update out

The screenshot shows the 'IPv4 ROUTE' configuration page. It displays a single route entry with the following details:

- Optional:** Unchecked
- Prefix:** 0.0.0.0/0
- Gateway:** Null 0
- Selected Gateway Configuration:** Enable Null, On
- Action:** A trash icon (highlighted with a red box)
- Distance:** 1

 At the bottom, there are 'Update' and 'Cancel' buttons.

3. To check the current routing tables for VPN 10 and VPN 20, navigate to **Monitor => Network**



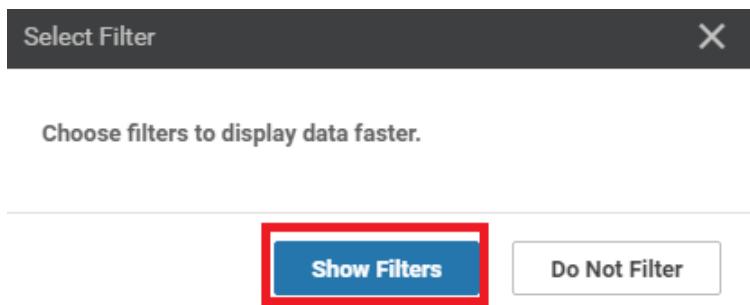
4. Click on vEdge20

| Device Group | All | Search | Search Options | | | |
|----------------|---------------|---------------------|-------------------------------------|-------|--------------|---------|
| Hostname | System IP | Device Model | Chassis Number/ID | State | Reachability | Site ID |
| vmanage | 10.255.255.1 | vManage | dfea63a5-66d2-4e50-a07b-ec4ad4... | ✓ | reachable | 1000 |
| vSmart | 10.255.255.3 | vSmart | 20607a12-c0c8-4f46-a65f-5a547c... | ✓ | reachable | 1000 |
| vSmart2 | 10.255.255.5 | vSmart | 7f332491-cb6f-4843-8bf5-060f90... | ✓ | reachable | 1000 |
| vBond | 10.255.255.2 | vEdge Cloud (vBo... | fc31c154-99c5-4267-971d-6c9ae7... | ✓ | reachable | 1000 |
| DC-vEdge1 | 10.255.255.11 | vEdge Cloud | e474c5fd-8ce7-d376-7cac-ba950b... | ✓ | reachable | 1 |
| DC-vEdge2 | 10.255.255.12 | vEdge Cloud | 0cddd4f0e-f2f1-fe75-866c-469966c... | ✓ | reachable | 1 |
| cEdge40 | 10.255.255.41 | CSR1000v | CSR-04F9482E-44F0-E4DC-D30D... | ✓ | reachable | 40 |
| cEdge50 | 10.255.255.51 | CSR1000v | CSR-834E40DC-E358-8DE1-0E81... | ✓ | reachable | 50 |
| cEdge51 | 10.255.255.52 | CSR1000v | CSR-D1837F36-6A1A-1850-7C1C... | ✓ | reachable | 50 |
| vEdge20 | 10.255.255.21 | vEdge Cloud | b7fd7295-58df-7671-e914-6fe2ed... | ✓ | reachable | 20 |
| vEdge21 | 10.255.255.22 | vEdge Cloud | dde90ff0-dc62-77e6-510f-08d966... | ✓ | reachable | 20 |
| vEdge30 | 10.255.255.31 | vEdge Cloud | 17026153-f09e-be4b-6dce-482fce... | ✓ | reachable | 30 |

5. Go to **Real Time** in the left menu and enter *ip route* in the **Device Options** field. Click on **IP Routes** to see the current routes and choose **Show Filters**

The screenshot shows the Cisco vManage interface. On the left, there's a sidebar with various monitoring and configuration tabs. The 'Real Time' tab is highlighted with a red box. In the main content area, the device selected is 'vEdge20 | 10.255.255.21'. The 'Device Options' field contains 'ip route'. Below it, the 'IP Routes' button is also highlighted with a red box. A search bar and search options are present. A table displays device properties and their values:

| Property | Value |
|---------------|-----------------------------|
| Device groups | [No groups] |
| Domain ID | 1 |
| Hostname | vEdge20 |
| Last Updated | 20 Jul 2020 10:44:48 AM PDT |
| Latitude | Not Configured |
| Longitude | Not Configured |
| Personality | WAN Edge |
| Site ID | 20 |
| Timezone | UTC |
| Vbond | 100.100.100.3 |



6. Enter a **VPN ID** of **10** and click on **Search** to filter the routes for VPN 10 on vEdge20

| | | |
|---------------------------|-----------------|-----------------------|
| VPN ID | 10 | X |
| AF Type | Select AF Type | |
| Prefix | | |
| Protocol | Select Protocol | |
| Reset All | Search | Close |

7. Since Inter VPN Routing hasn't been configured yet, we will see routes that are part of VPN 10 only. Subnets from other VPNs will not show up over here. We can thus infer that there won't be inter VPN connectivity as of now

vEdge20 | 10.255.255.21 Site ID: 20 Device Model: vEdge Cloud ⓘ

Device Options: Filter ▾ VPN ID: 10

Inter VPN Routing has not been set up so we don't see any routes pointing to the VPN 20 subnet.

| Next Hop If Name | VPN ID | AF Type | Prefix | Protocol | Next Hop Address | Next Hop VPN | TLOC IP | TLOC Color | TLOC Encap | Next Hop Label |
|------------------|--------|---------|----------------|-----------|------------------|--------------|---------------|-----------------|------------|----------------|
| ge0/2 | 10 | ipv4 | 10.20.10.0/24 | connected | -- | -- | -- | -- | -- | -- |
| -- | 10 | ipv4 | 10.30.10.0/24 | omp | -- | -- | 10.255.255.31 | mpls | ipsec | 1003 |
| -- | 10 | ipv4 | 10.30.10.0/24 | omp | -- | -- | 10.255.255.31 | public-internet | ipsec | 1003 |
| -- | 10 | ipv4 | 10.40.10.0/24 | omp | -- | -- | 10.255.255.41 | mpls | ipsec | 1002 |
| -- | 10 | ipv4 | 10.40.10.0/24 | omp | -- | -- | 10.255.255.41 | public-internet | ipsec | 1002 |
| -- | 10 | ipv4 | 10.40.11.0/24 | omp | -- | -- | 10.255.255.41 | mpls | ipsec | 1002 |
| -- | 10 | ipv4 | 10.40.11.0/24 | omp | -- | -- | 10.255.255.41 | public-internet | ipsec | 1002 |
| -- | 10 | ipv4 | 10.50.10.0/24 | omp | -- | -- | 10.255.255.51 | public-internet | ipsec | 1002 |
| -- | 10 | ipv4 | 10.50.10.0/24 | omp | -- | -- | 10.255.255.52 | mpls | ipsec | 1002 |
| -- | 10 | ipv4 | 10.100.10.0/24 | omp | -- | -- | 10.255.255.11 | mpls | ipsec | 1003 |
| -- | 10 | ipv4 | 10.100.10.0/24 | omp | -- | -- | 10.255.255.11 | public-internet | ipsec | 1003 |
| -- | 10 | ipv4 | 10.100.10.0/24 | omp | -- | -- | 10.255.255.12 | public-internet | ipsec | 1003 |
| -- | 10 | ipv4 | 10.100.10.0/24 | omp | -- | -- | 10.255.255.12 | mpls | ipsec | 1003 |

8. Click on **Select Devices** (top left-hand corner) and choose vEdge30 from the drop down. Click on **Show Filters**

MONITOR Network > Real Time

Select Device vEdge20 | 10.255.255.21 Site ID: 20 Device Model: vEdge Cloud

Device Group Search

All Search Options

Sort by Reachability

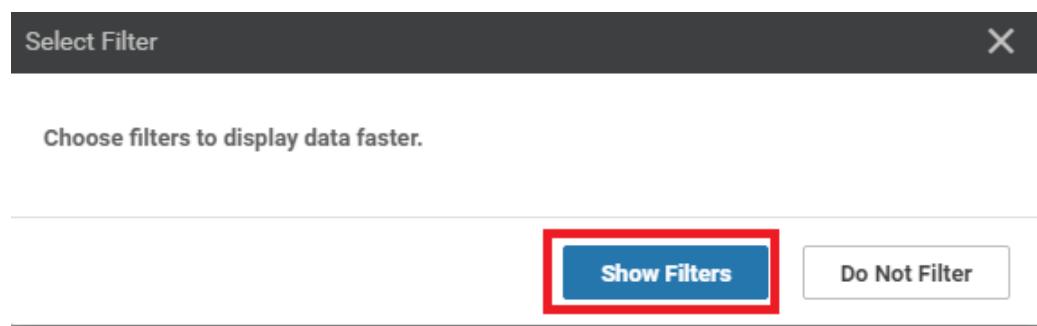
Reachable

| | Protocol | Next Hop Address |
|--|--|------------------|
| cEdge40 10.255.255.41 Site ID: 40 Reachable | CSR1000v Version: 17.02.01r.0.32 | connected -- |
| cEdge50 10.255.255.51 Site ID: 50 Reachable | CSR1000v Version: 17.02.01r.0.32 | omp -- |
| cEdge51 10.255.255.52 Site ID: 50 Reachable | CSR1000v Version: 17.02.01r.0.32 | omp -- |
| vEdge20 10.255.255.21 Site ID: 20 Reachable | vEdge Cloud Version: 20.1.1 | omp -- |
| vEdge21 10.255.255.22 Site ID: 20 Reachable | vEdge Cloud Version: 20.1.1 | omp -- |
| vEdge30 10.255.255.31 Site ID: 30 Reachable | vEdge Cloud Version: 20.1.1 | omp -- |
| Control Connections | 10 ipv4 10.100.10.0/24 | omp -- |
| System Status | -- 10 ipv4 10.100.10.0/24 | omp -- |

vEdge20 | 10.255.255.21 | Site ID: 20 | vEdge Cloud | Version: 20.1.1

vEdge21 | 10.255.255.22 | Site ID: 20 | vEdge Cloud | Version: 20.1.1

vEdge30 | 10.255.255.31 | Site ID: 30 | vEdge Cloud | Version: 20.1.1



9. Enter 20 in the **VPN ID** and click on **Search**

Device Options:

[Filter ▾](#)

| | | |
|---------------------------|---|-----------------------|
| VPN ID | 20 | X |
| AF Type | Select AF Type | |
| Prefix | | |
| Protocol | Select Protocol | |
| Reset All | Search | Close |

10. This shows all the routes learnt by vEdge30 in VPN 20. There aren't any routes subnets in other VPNs, as of now

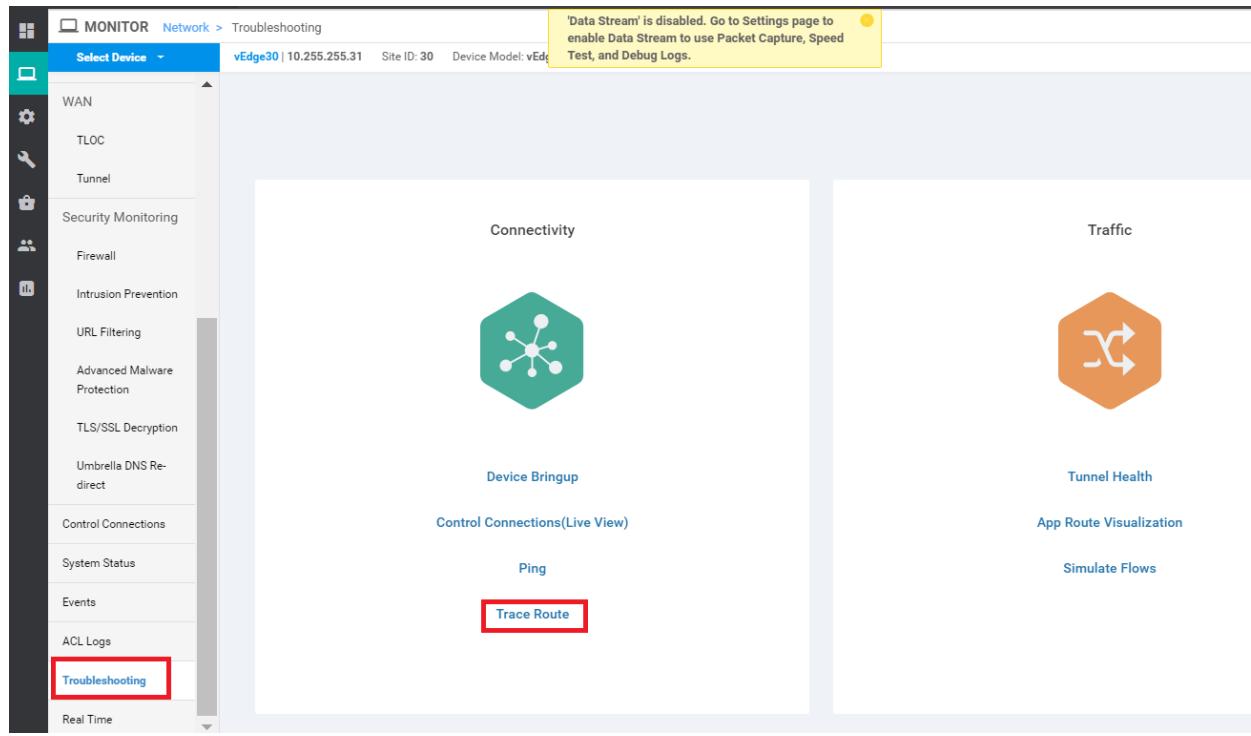
vEdge30 | 10.255.255.31 Site ID: 30 Device Model: vEdge Cloud ⓘ

Device Options:

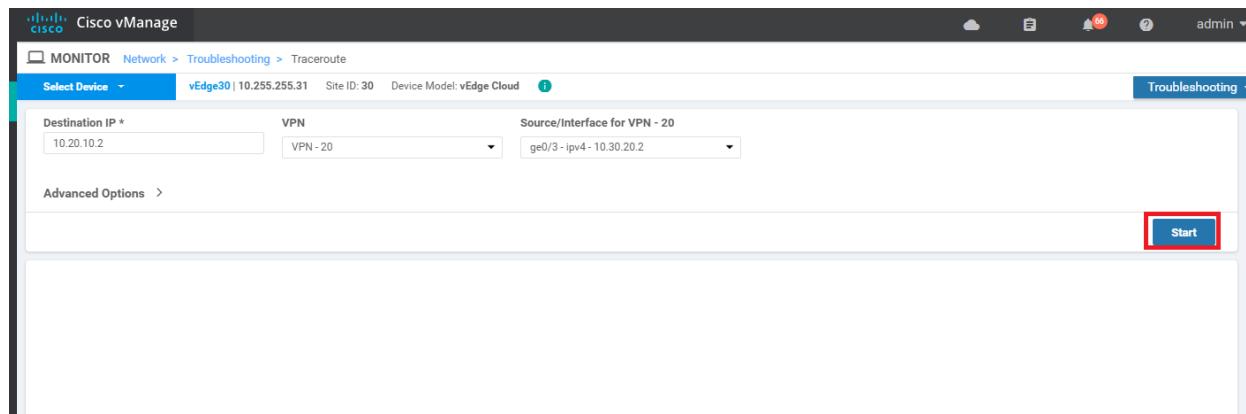
[Filter ▾](#) [VPN ID: 20](#)

| Search Options ▾ | | | | | | | | | | |
|------------------|--------|---------|----------------|-----------|------------------|--------------|---------------|-----------------|------------|----------------|
| Next Hop If Name | VPN ID | AF Type | Prefix | Protocol | Next Hop Address | Next Hop VPN | TLOC IP | TLOC Color | TLOC Encap | Next Hop Label |
| - | 20 | ipv4 | 10.20.20.0/24 | omp | -- | -- | 10.255.255.21 | mpls | ipsec | 1004 |
| - | 20 | ipv4 | 10.20.20.0/24 | omp | -- | -- | 10.255.255.21 | public-internet | ipsec | 1004 |
| - | 20 | ipv4 | 10.20.20.0/24 | omp | -- | -- | 10.255.255.22 | mpls | ipsec | 1004 |
| - | 20 | ipv4 | 10.20.20.0/24 | omp | -- | -- | 10.255.255.22 | public-internet | ipsec | 1004 |
| ge0/3 | 20 | ipv4 | 10.30.20.0/24 | connected | -- | -- | -- | -- | -- | -- |
| - | 20 | ipv4 | 10.40.20.0/24 | omp | -- | -- | 10.255.255.41 | mpls | ipsec | 1003 |
| - | 20 | ipv4 | 10.40.20.0/24 | omp | -- | -- | 10.255.255.41 | public-internet | ipsec | 1003 |
| - | 20 | ipv4 | 10.50.20.0/24 | omp | -- | -- | 10.255.255.51 | public-internet | ipsec | 1003 |
| - | 20 | ipv4 | 10.50.20.0/24 | omp | -- | -- | 10.255.255.52 | mpls | ipsec | 1003 |
| - | 20 | ipv4 | 10.100.20.0/24 | omp | -- | -- | 10.255.255.11 | mpls | ipsec | 1004 |
| - | 20 | ipv4 | 10.100.20.0/24 | omp | -- | -- | 10.255.255.11 | public-internet | ipsec | 1004 |
| - | 20 | ipv4 | 10.100.20.0/24 | omp | -- | -- | 10.255.255.12 | public-internet | ipsec | 1004 |
| - | 20 | ipv4 | 10.100.20.0/24 | omp | -- | -- | 10.255.255.12 | mpls | ipsec | 1004 |

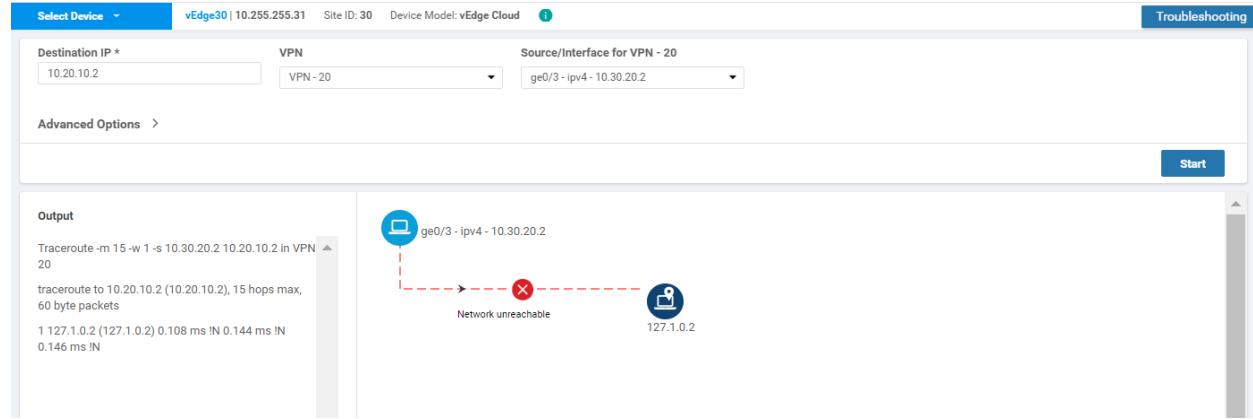
11. On the left hand slide, click on Troubleshooting and select Traceroute (note that this is being done on vEdge30)



12. Enter a **Destination IP** of 10.20.10.2 and select **VPN 20** from the **VPN** drop down. Populate the **Source/Interface** as **ge0/3** and click on **Start**

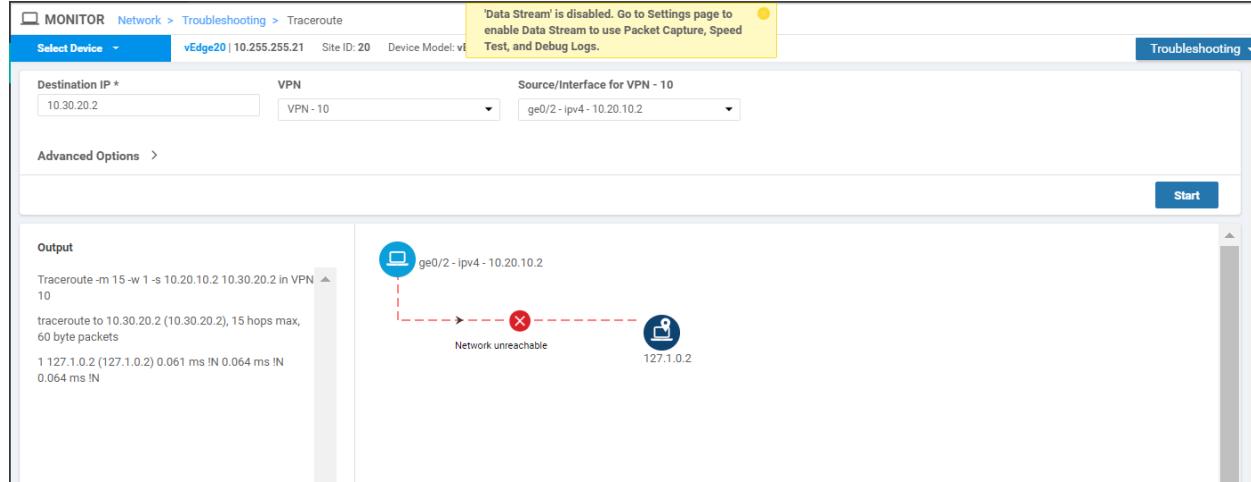


13. As expected, the traceroute should fail



14. Click on **Select Device** in the top left-hand corner and choose *vEdge20*. Run the traceroute again, changing the **Destination IP** to **10.30.20.2**, **VPN** to **VPN 10** and the **Source/Interface** to **ge0/2**. Click on **Start** and this should fail as well

| Device | IP Address | Site ID | Device Model |
|---------|---------------|---------|--------------|
| vEdge30 | 10.255.255.31 | 30 | vEdge Cloud |
| vEdge20 | 10.255.255.21 | 20 | vEdge Cloud |
| vEdge21 | 10.255.255.22 | 20 | vEdge Cloud |
| vEdge30 | 10.255.255.31 | 30 | vEdge Cloud |



We have established that Inter VPN communication is not happening between Site 20 and Site 30 as of now.

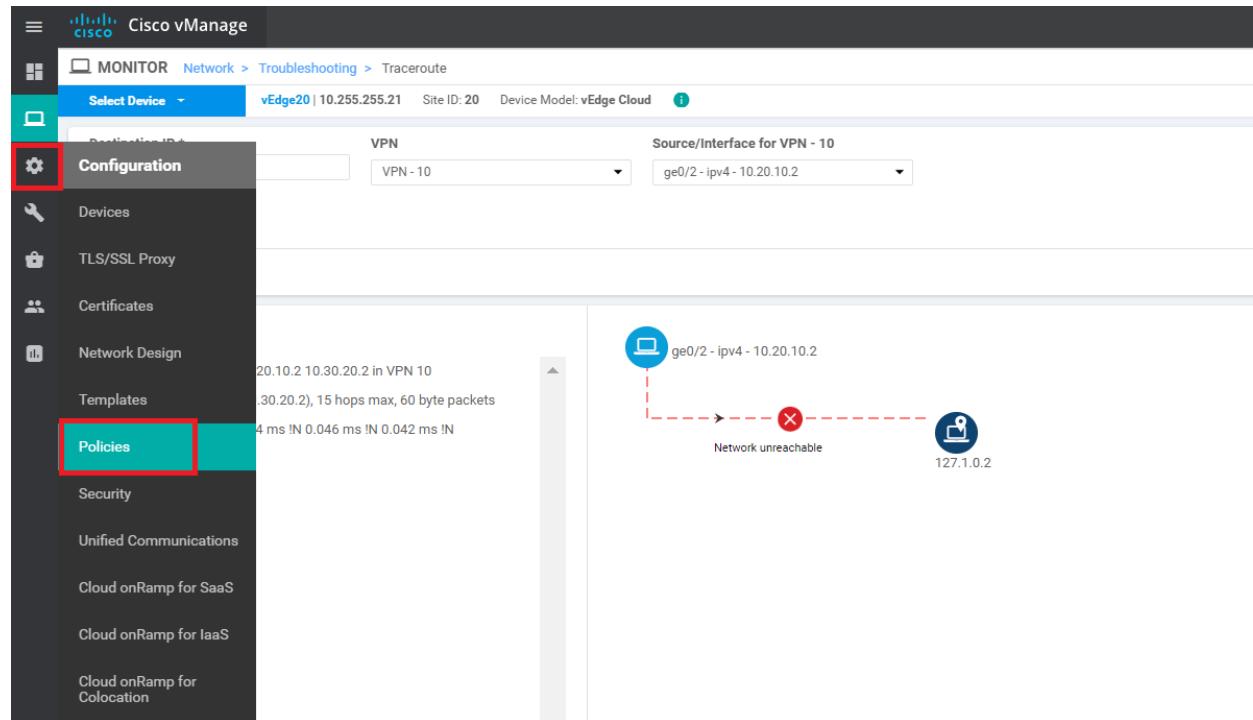
Task List

- [Overview](#)
- [Configure VPN 40 on DC-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)

Setting up VPN Lists

In order to facilitate inter VPN connectivity, we will be setting up VPN Lists that can be used in our Policies.

1. On the vManage GUI, go to **Configuration => Policies**



2. Click on **Custom Options** in the top right-hand corner and click on **Lists** (under Centralized Policy)

This screenshot shows the "Centralized Policy" section of the Cisco vManage interface. At the top, there are tabs for "Centralized Policy" and "Localized Policy". Under "Centralized Policy", there are four main categories: "CLI Policy", "Lists", "Topology", and "Traffic Policy". The "Lists" option is highlighted with a red box. A dropdown menu labeled "Custom Options" is open, showing sub-options: "Centralized Policy", "CLI Policy", "Lists", "Forwarding Class/QoS", "Access Control Lists", and "Route Policy". The "Lists" option in this dropdown is also highlighted with a red box. To the left of the policy sections, there is a table with columns "Updated By", "Policy Version", and "Last Updated". The table lists five entries, all updated by "admin".

| Updated By | Policy Version | Last Updated |
|------------|--------------------|-----------------------------|
| admin | 06212020T180221721 | 21 Jun 2020 4:24:33 AM PDT |
| admin | 06212020T112433859 | 21 Jun 2020 5:07:26 AM PDT |
| admin | 06212020T114417139 | 21 Jun 2020 10:35:13 AM PDT |
| admin | 06212020T17351344 | 21 Jun 2020 3:34:12 PM PDT |

3. Select **VPN** and click on **New VPN List**. Enter a **VPN List Name** of *FW* and put *40* for the **Add VPN** field. Click on **Add**

The screenshot shows a dialog box titled "Select a list type on the left and start creating your groups of interest". On the left, there is a sidebar with various options: Application, Color, Data Prefix, Policer, Prefix, Site, SLA Class, TLOC, and **VPN**, which is highlighted with a red box. In the main area, there is a "New VPN List" button with a red box around it. Below it, the "VPN List Name" field contains "FW". Under "Add VPN", the value "40" is entered. At the bottom right, there is an "Add" button with a red box around it and a "Cancel" link.

4. Click on **New VPN List** again and Put a **VPN List Name** of *Corp_FW*. Put *10,40* in the **Add VPN** field. Click on **Add**

The screenshot shows a dialog box for creating a new VPN list. The "New VPN List" button is highlighted with a red box. The "VPN List Name" field contains "Corp_FW". In the "Add VPN" field, the value "10,40" is entered. At the bottom right, there is an "Add" button with a red box around it and a "Cancel" link.

5. Click on **New VPN List** again and Put a **VPN List Name** of *PoS_FW*. Put *20,40* in the **Add VPN** field. Click on **Add**

The screenshot shows a dialog box for creating a new VPN list. The "New VPN List" button is highlighted with a red box. The "VPN List Name" field contains "PoS_FW". In the "Add VPN" field, the value "20,40" is entered. At the bottom right, there is an "Add" button with a red box around it and a "Cancel" link.

6. Make sure that the following VPN lists show up, before proceeding

[New VPN List](#)

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|-----------|---------|-----------------|------------|----------------------------|---|
| PoS_FW | 20, 40 | 0 | admin | 20 Jul 2020 3:00:14 PM PDT | Edit Delete Details |
| FW | 40 | 0 | admin | 20 Jul 2020 2:58:21 PM PDT | Edit Delete Details |
| PoS | 20 | 1 | admin | 21 Jun 2020 4:16:01 AM PDT | Edit Delete Details |
| Corporate | 10 | 3 | admin | 21 Jun 2020 4:15:35 AM PDT | Edit Delete Details |
| Guest | 30 | 1 | admin | 21 Jun 2020 4:16:14 AM PDT | Edit Delete Details |
| Corp_FW | 10, 40 | 0 | admin | 20 Jul 2020 2:59:41 PM PDT | Edit Delete Details |

Task List

- [Overview](#)
- [Configure VPN 40 on DC-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)

Inter VPN Routing Policies

1. Navigate to **Configuration => Policies** and locate the **Site40-Guest-DIA Policy**. Click on the three dots next to it and choose to **Edit** the policy

CONFIGURATION | POLICIES

Centralized Policy Localized Policy

Add Policy

Search Options

Total Rows: 5

| Name | Description | Type | Activated | Updated By | Policy Version | Last Updated | ... |
|----------------------------|------------------------------------|-------------------|-----------|------------|--------------------|-----------------------------|-----|
| Site40-Guest-DIA | DIA Policy for Site 40 Guests | UI Policy Builder | true | admin | 06212020T180221721 | 21 Jun 2020 11:02:21 AM PDT | |
| Hub-n-Spoke-VPN20-only | Hub and Spoke policy for VP... | UI Policy Builder | false | admin | 06212020T112433859 | 21 Jun 2020 4:21:33 PM PDT | |
| Site20-Regional-Hub-Site30 | Regional Policy for Site 20 to ... | UI Policy Builder | false | admin | 06212020T114417139 | 21 Jun 2020 5:00:00 PM PDT | |
| traffic-engineering-ftp | Traffic Engineering for FTP | UI Policy Builder | false | admin | 06212020T17351344 | 21 Jun 2020 10:35:13 PM PDT | |
| AAR-VPN10 | Transport Preference for VP... | UI Policy Builder | false | admin | 06212020T223412311 | 21 Jun 2020 3:44:12 PM PDT | |

2. Click on the **Topology** tab (top of the screen) and click on **Add Topology**. Choose to add a *Custom Control (Route & TLOC)* policy

CONFIGURATION | POLICIES **Centralized Policy > Edit Policy**

Topology **VPN Membership**

Add Topology

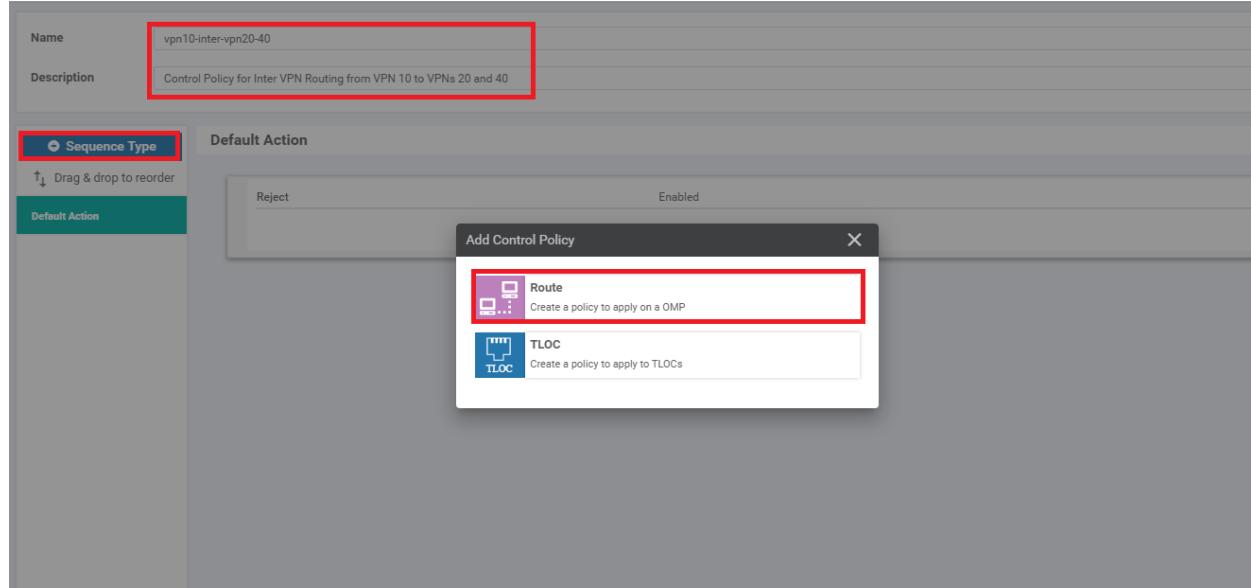
- Hub-and-Spoke
- Mesh
- Custom Control (Route & TLOC)** (highlighted with a red box)
- Import Existing Topology

Specify your network topology

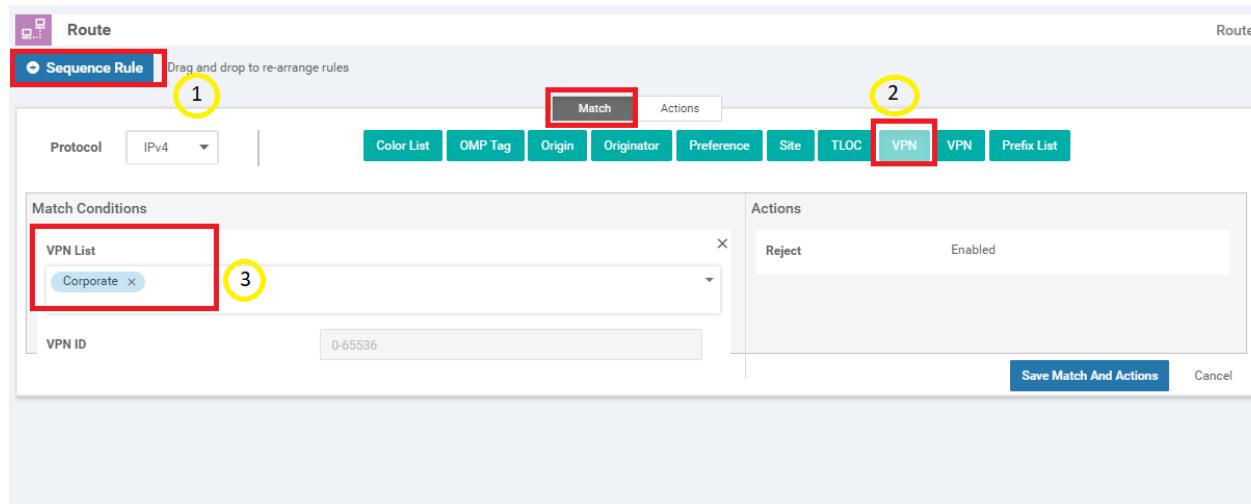
Policy Application **Topology** Traffic Rules

No data available

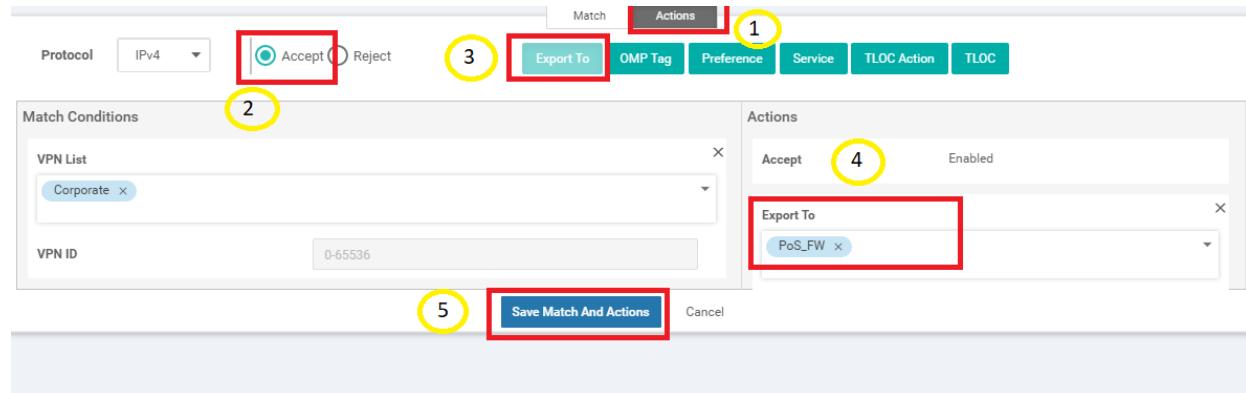
3. Give the policy a **Name** of *vpn10-inter-vpn20-40* with a Description of *Control Policy for Inter VPN Routing from VPN 10 to VPNs 20 and 40*. Click on **Sequence Type** and choose **Route**



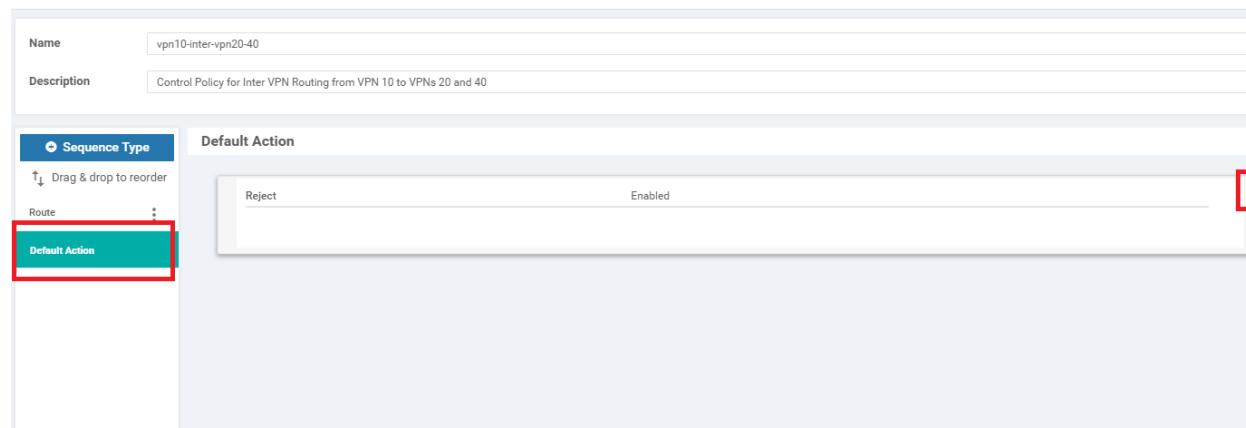
4. Click on **Sequence Rule** and add a **VPN** match. Select **Corporate** from the **VPN List** drop down



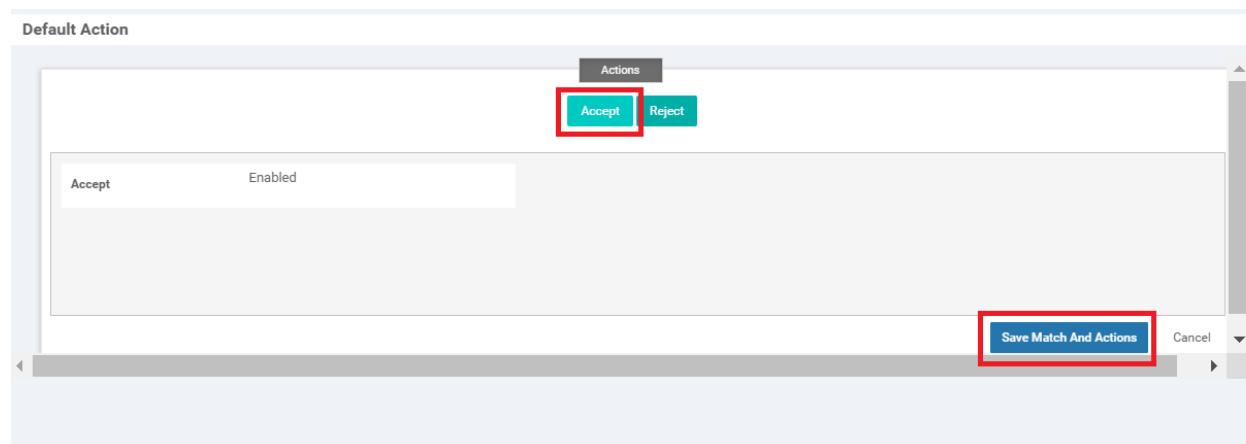
5. Click on the **Actions** tab and select the **Accept** radio button. Click on **Export To** and select **PoS_FW** from the drop down under Actions. Click on **Save Match And Actions**



6. Select **Default Action** on the left-hand side and click on the pencil icon to edit the Default Action



7. Click on **Accept** and then **Save Match And Actions**



8. Click **Save Control Policy**

Name: vpn10-inter-vpn20-40

Description: Control Policy for Inter VPN Routing from VPN 10 to VPNs 20 and 40

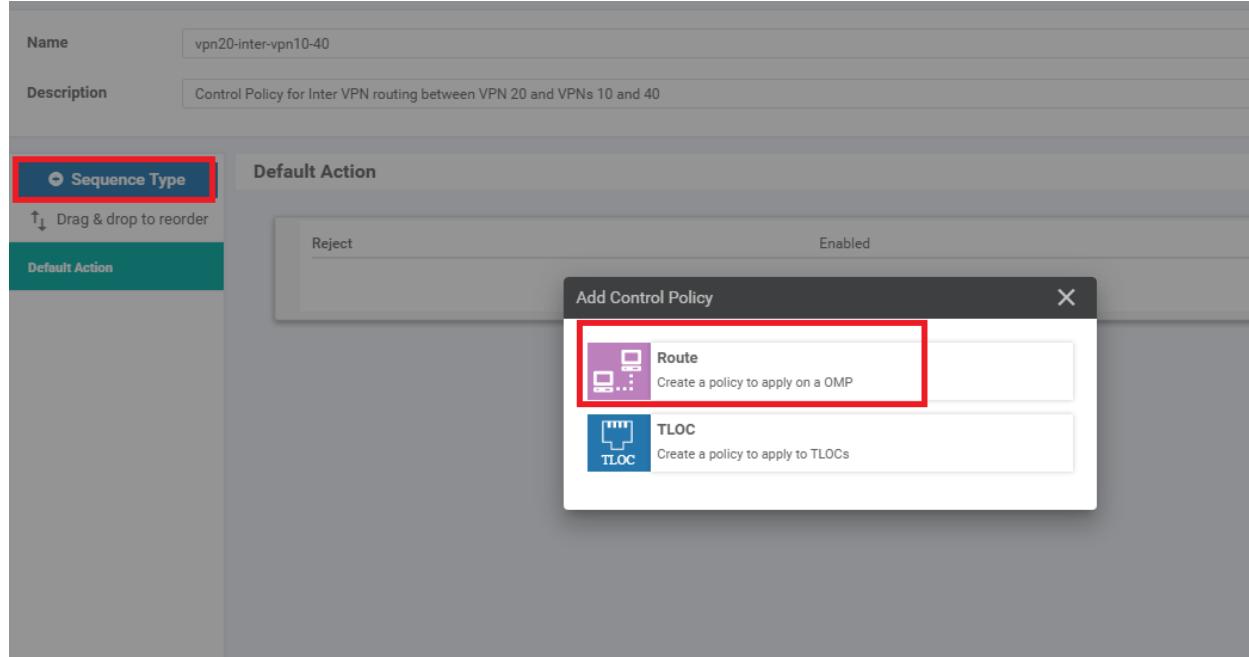
Sequence Type: Route

Default Action:

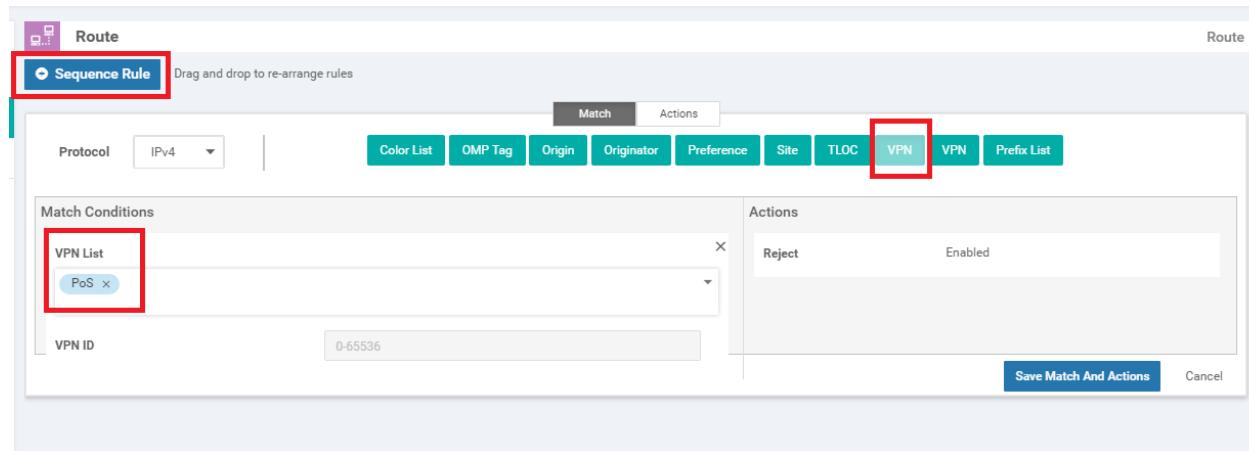
| Action | Status |
|--------|---------|
| Accept | Enabled |

Save Control Policy Cancel

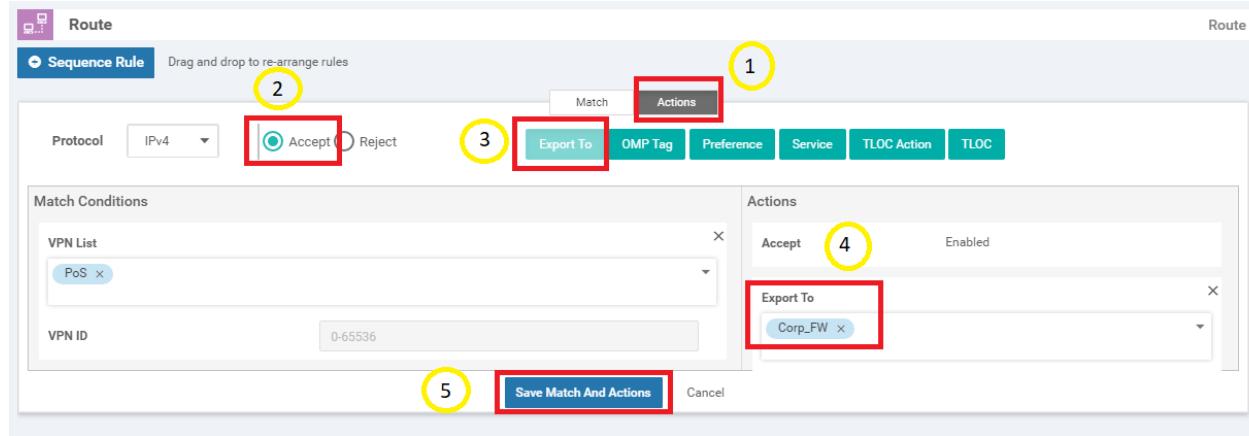
9. Click on **Add Topology** and add another *Custom Control (Route & TLOC)* policy. Give it a **Name** of *vpn20-inter-vpn10-40* with a Description of *Control Policy for Inter VPN routing between VPN 20 and VPNs 10 and 40*. Click on **Sequence Type** and select **Route**



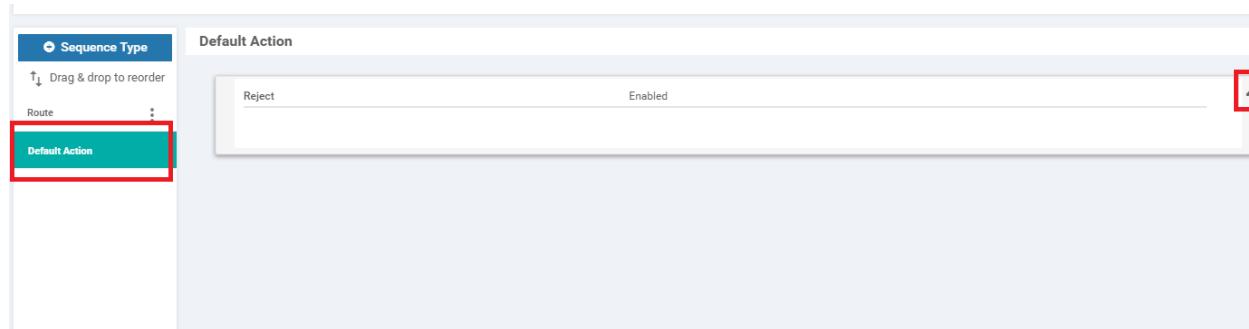
10. Click on **Sequence Rule** and select VPN as the match. Select *PoS* from the **VPN List**



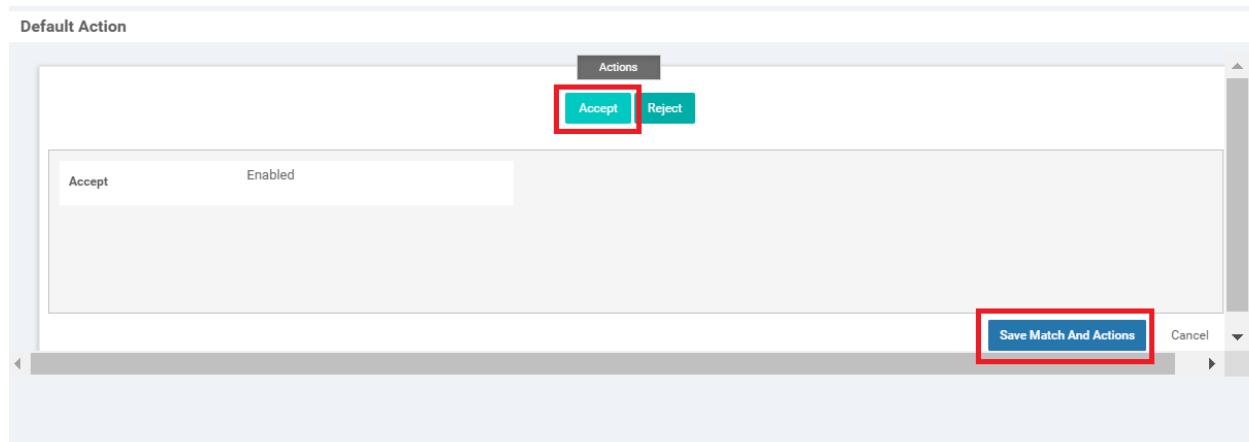
11. Click on the **Actions** tab and select the **Accept** radio button. Click on **Export To** and select the **Corp_FW** VPN list in the **Export To** drop down under Actions. To save the rule, click on **Save Match And Actions**



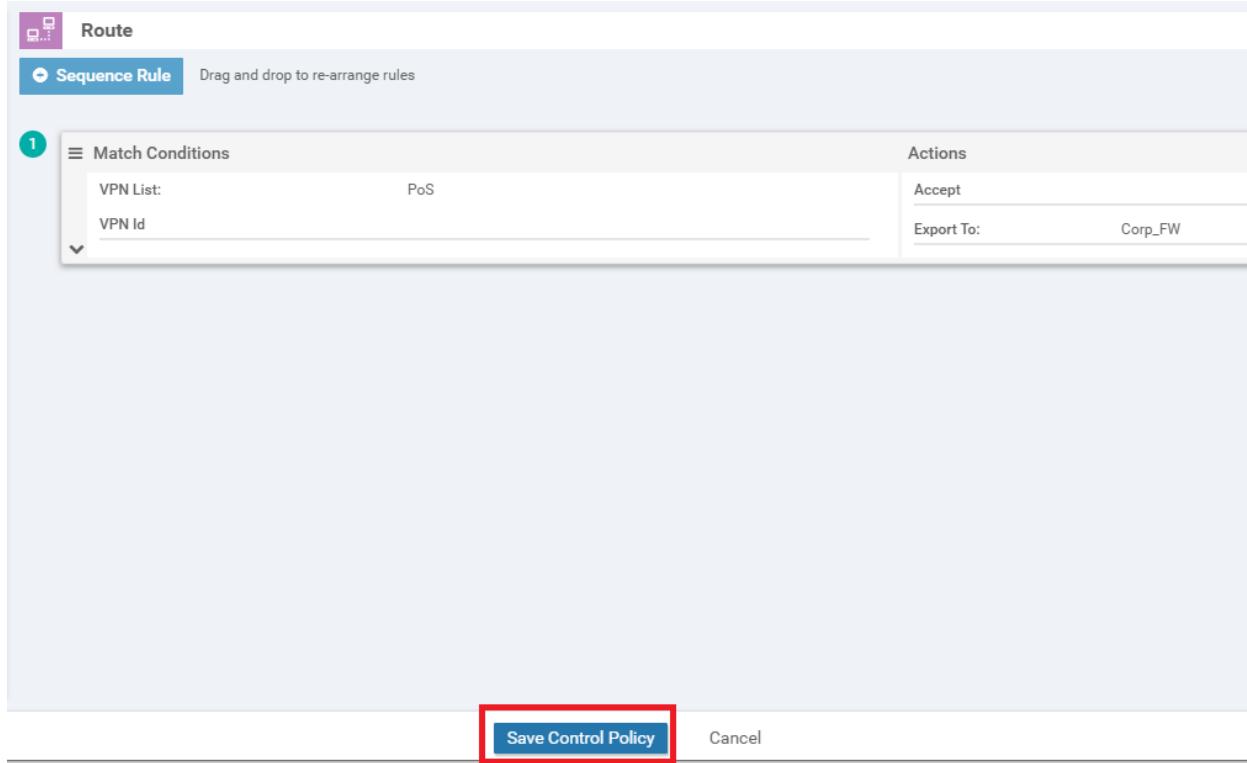
12. Click on **Default Action** on the left-hand side and click the **Pencil** icon to edit the Default Action



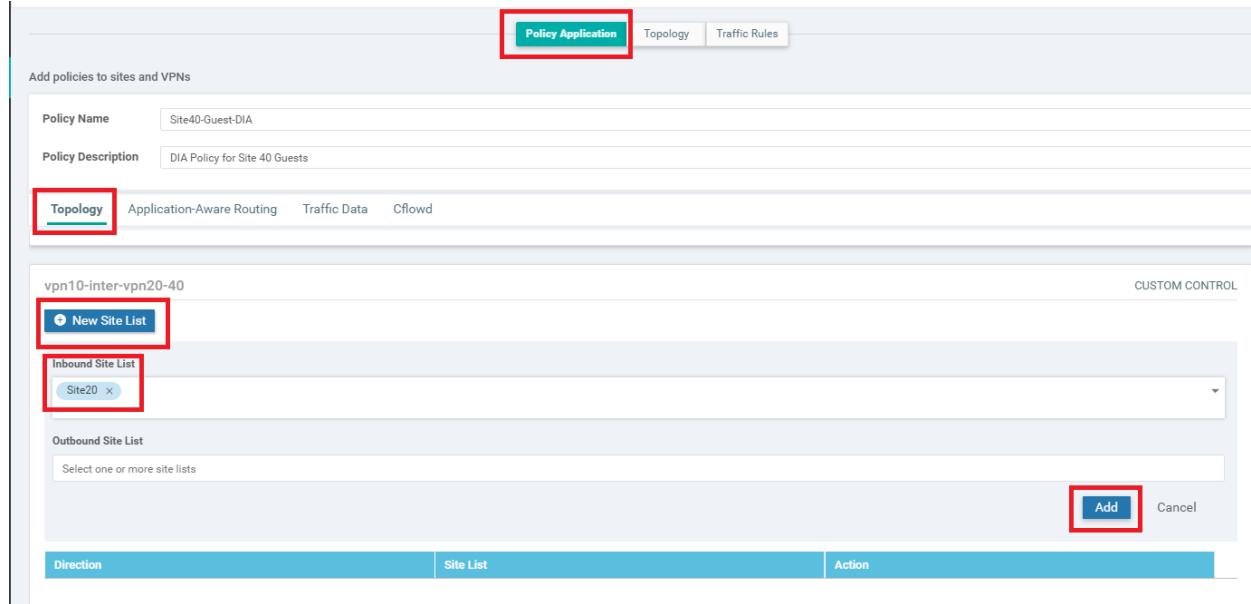
13. Select **Accept** and click **Save Match And Actions**



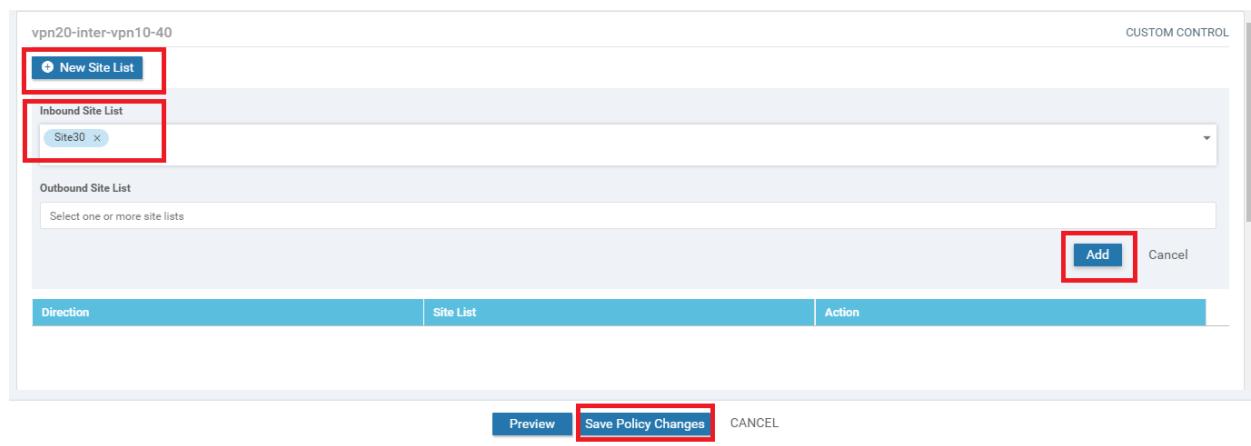
14. Click on **Save Control Policy**



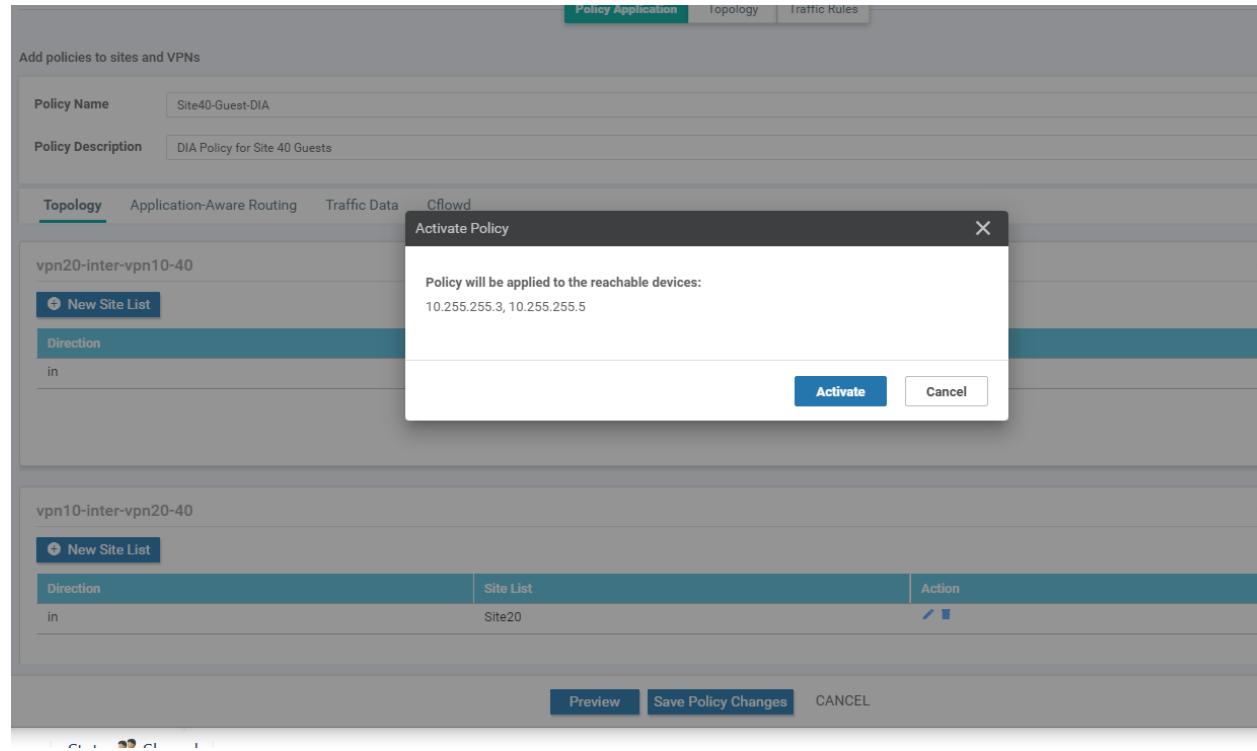
15. You should be back at the main policy screen. Click on the **Policy Application** tab and make sure you're under the **Topology** sub-tab (should not be under the main Topology tab). Click on **New Site List** under the entry for *vpn10-inter-vpn20-40* and select the **Inbound Site List** as *Site20*. Click on **Add**



16. Click on **New Site List** under the entry for **vpn20-inter-vpn10-40** and select the **Inbound Site List** as **Site30**. Click on **Add**. Click on **Save Policy Changes**



17. Click on **Activate** to push the changes to the vSmarts



We have set up the policies for Inter VPN Routing.

Task List

- [Overview](#)
- [Configure VPN 40 on DC-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)

Inter VPN Routing Verification

1. On the vManage GUI, navigate to **Monitor => Network** and click on **vEdge20**. Scroll down along the left-hand side menu and click on **Real Time**. Enter **IP Routes** in the **Device Options** and select IP Routes when it pops up. Choose **Show Filters** and enter a **VPN ID** of 10. Click on **Search**. The Routing Table for VPN 10 on vEdge20 should show routes to subnets at Site 30 VPN 20

The screenshot shows the vManage Network - Real Time interface. The top navigation bar includes 'MONITOR' and 'Network > Real Time'. Below this, the 'Select Device' dropdown is set to 'vEdge20 | 10.255.255.21 Site ID: 20 Device Model: vEdge Cloud'. The left sidebar lists various monitoring categories like Security Monitoring, Firewall, Intrusion Prevention, etc. The main content area displays a table titled 'IP Routes' with the following columns: Next Hop If Name, VPN ID, AF Type, Prefix, Protocol, Next Hop Address, Next Hop VPN, TLOC IP, TLOC Color, and TLOC Encap. A filter bar at the top of the table says 'Filter > VPN ID: 10'. The table contains several rows, with the last four rows (VPN ID 10, AF Type ipv4, Prefix 10.30.20.0/24) highlighted by a red box.

| Next Hop If Name | VPN ID | AF Type | Prefix | Protocol | Next Hop Address | Next Hop VPN | TLOC IP | TLOC Color | TLOC Encap |
|------------------|--------|---------|----------------|-----------|------------------|--------------|---------------|-----------------|------------|
| ge0/2 | 10 | ipv4 | 10.20.10.0/24 | connected | - | - | - | - | - |
| -- | 10 | ipv4 | 10.30.10.0/24 | omp | - | - | 10.255.255.31 | mpls | ipsec |
| -- | 10 | ipv4 | 10.30.10.0/24 | omp | - | - | 10.255.255.31 | public-internet | ipsec |
| -- | 10 | ipv4 | 10.30.20.0/24 | omp | - | - | 10.255.255.31 | mpls | ipsec |
| -- | 10 | ipv4 | 10.30.20.0/24 | omp | - | - | 10.255.255.31 | public-internet | ipsec |
| -- | 10 | ipv4 | 10.40.10.0/24 | omp | - | - | 10.255.255.41 | mpls | ipsec |
| -- | 10 | ipv4 | 10.40.10.0/24 | omp | - | - | 10.255.255.41 | public-internet | ipsec |
| -- | 10 | ipv4 | 10.40.11.0/24 | omp | - | - | 10.255.255.41 | mpls | ipsec |
| -- | 10 | ipv4 | 10.40.11.0/24 | omp | - | - | 10.255.255.41 | public-internet | ipsec |
| -- | 10 | ipv4 | 10.50.10.0/24 | omp | - | - | 10.255.255.51 | public-internet | ipsec |
| -- | 10 | ipv4 | 10.50.10.0/24 | omp | - | - | 10.255.255.52 | mpls | ipsec |
| -- | 10 | ipv4 | 10.100.10.0/24 | omp | - | - | 10.255.255.11 | mpls | ipsec |
| -- | 10 | ipv4 | 10.100.10.0/24 | omp | - | - | 10.255.255.11 | public-internet | ipsec |
| -- | 10 | ipv4 | 10.100.10.0/24 | omp | - | - | 10.255.255.12 | public-internet | ipsec |
| -- | 10 | ipv4 | 10.100.10.0/24 | omp | - | - | 10.255.255.12 | mpls | ipsec |

2. Click on **Select Device** in the top left-hand corner and click on **vEdge30**

MONITOR Network > Real Time

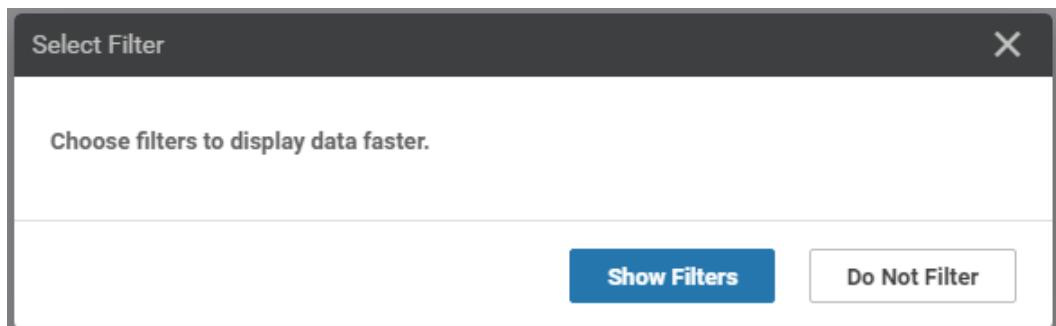
Select Device vEdge20 | 10.255.255.21 Site ID: 20 Device Model: vEdge Cloud i

| Device Group | Search |
|--|---|
| All | <input type="text"/> Search Options !F |
| Sort by Reachability !F | |
| Reachable | |
| cEdge40 10.255.255.41 Site ID: 40 Reachable | CSR1000v Version: 17.02.01r.0.32 |
| cEdge50 10.255.255.51 Site ID: 50 Reachable | CSR1000v Version: 17.02.01r.0.32 |
| cEdge51 10.255.255.52 Site ID: 50 Reachable | CSR1000v Version: 17.02.01r.0.32 |
| vEdge20 10.255.255.21 Site ID: 20 Reachable | vEdge Cloud Version: 20.1.1 |
| vEdge21 10.255.255.22 Site ID: 20 Reachable | vEdge Cloud Version: 20.1.1 |
| vEdge30 10.255.255.31 Site ID: 30 Reachable | vEdge Cloud Version: 20.1.1 |
| Control Connections | -- 10 IPv4 10.100.10.0/24 |
| Control Connections | -- 10 IPv4 10.100.10.0/24 |

Protocol Next Hop

- connected --
- omp --

3. Click **Show Filters** and enter a VPN ID of 20. Click on **Search**



| | | |
|---------------------------|------------------------|-----------------------|
| VPN ID | 20 | X |
| AF Type | Select AF Type | |
| Prefix | | |
| Protocol | Select Protocol | |
| Reset All | Search | Close |

4. You should see routes for Site 20 VPN 10

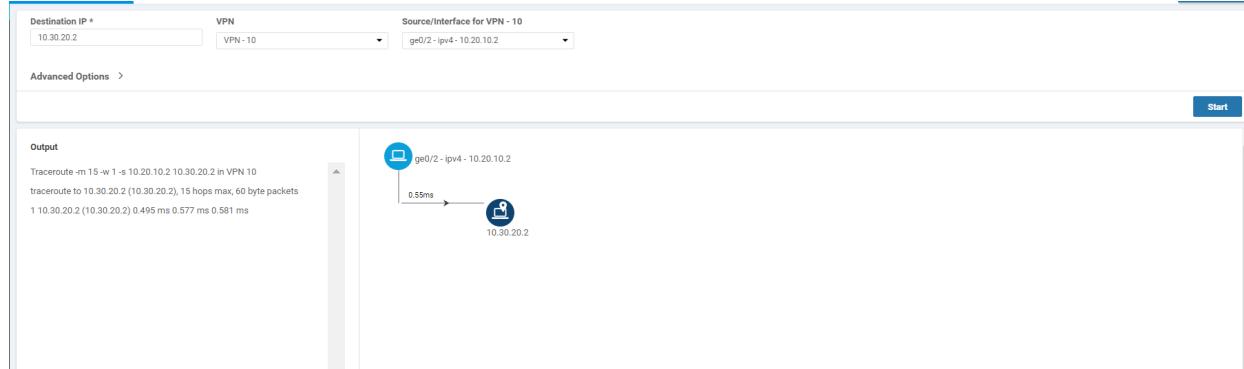
Edge30 | 10.255.255.31 Site ID: 30 Device Model: vEdge Cloud ⓘ

Device Options: IP Routes

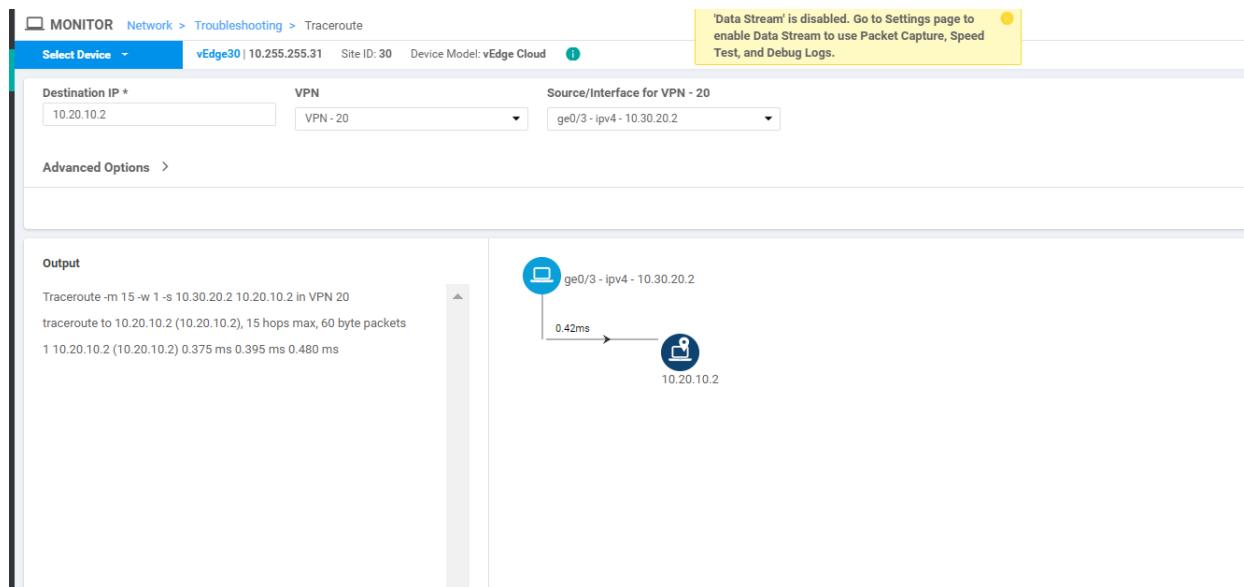
Filter: VPN ID: 20

| Next Hop If Name | VPN ID | AF Type | Prefix | Protocol | Next Hop Address | Next Hop VPN | TLOC IP | TLOC Color | TLOC Encap | Next Hop Label |
|------------------|--------|---------|----------------|-----------|------------------|--------------|---------------|-----------------|------------|----------------|
| -- | 20 | ipv4 | 10.20.10.0/24 | omp | -- | -- | 10.255.255.21 | mpls | ipsec | 1003 |
| -- | 20 | ipv4 | 10.20.10.0/24 | omp | -- | -- | 10.255.255.21 | public-internet | ipsec | 1003 |
| -- | 20 | ipv4 | 10.20.10.0/24 | omp | -- | -- | 10.255.255.22 | public-internet | ipsec | 1003 |
| -- | 20 | ipv4 | 10.20.10.0/24 | omp | -- | -- | 10.255.255.22 | mpls | ipsec | 1003 |
| -- | 20 | ipv4 | 10.20.20.0/24 | omp | -- | -- | 10.255.255.21 | mpls | ipsec | 1004 |
| -- | 20 | ipv4 | 10.20.20.0/24 | omp | -- | -- | 10.255.255.21 | public-internet | ipsec | 1004 |
| -- | 20 | ipv4 | 10.20.20.0/24 | omp | -- | -- | 10.255.255.22 | public-internet | ipsec | 1004 |
| -- | 20 | ipv4 | 10.20.20.0/24 | omp | -- | -- | 10.255.255.22 | mpls | ipsec | 1004 |
| ge0/3 | 20 | ipv4 | 10.30.20.0/24 | connected | -- | -- | -- | -- | -- | -- |
| -- | 20 | ipv4 | 10.40.20.0/24 | omp | -- | -- | 10.255.255.41 | public-internet | ipsec | 1003 |
| -- | 20 | ipv4 | 10.40.20.0/24 | omp | -- | -- | 10.255.255.41 | mpls | ipsec | 1003 |
| -- | 20 | ipv4 | 10.50.20.0/24 | omp | -- | -- | 10.255.255.51 | public-internet | ipsec | 1003 |
| -- | 20 | ipv4 | 10.50.20.0/24 | omp | -- | -- | 10.255.255.52 | mpls | ipsec | 1003 |
| -- | 20 | ipv4 | 10.100.20.0/24 | omp | -- | -- | 10.255.255.11 | mpls | ipsec | 1004 |
| -- | 20 | ipv4 | 10.100.20.0/24 | omp | -- | -- | 10.255.255.12 | mpls | ipsec | 1004 |
| -- | 20 | ipv4 | 10.100.20.0/24 | omp | -- | -- | 10.255.255.12 | public-internet | ipsec | 1004 |
| -- | 20 | ipv4 | 10.100.20.0/24 | omp | -- | -- | 10.255.255.11 | public-internet | ipsec | 1004 |

5. Click on **Troubleshooting** on the left-hand side and make sure you have **vEdge20** as the selected device. Enter a **Destination IP** of **10.30.20.2** with a **VPN** of **VPN - 10**. Select a **Source/Interface** of **ge0/2** (once again, verify that you're at the vEdge20 device. If not, click on the Select Device drop down from the top left-hand corner and select vEdge20). Click on **Start**. Notice that we now have direct Inter VPN connectivity from Site 20 VPN 10 to Site 30 VPN 20



- Click on **Select Device** in the top left-hand corner and select **vEdge30**. Enter a **Destination IP** of **10.20.10.2** with a **VPN** of **VPN - 20** and a **Source/Interface** of **ge0/3**. Click on **Start**. Notice that we now have direct Inter VPN Connectivity from Site 30 VPN 20 to Site 20 VPN 10



This completes the verification of our Inter VPN Routing configuration.

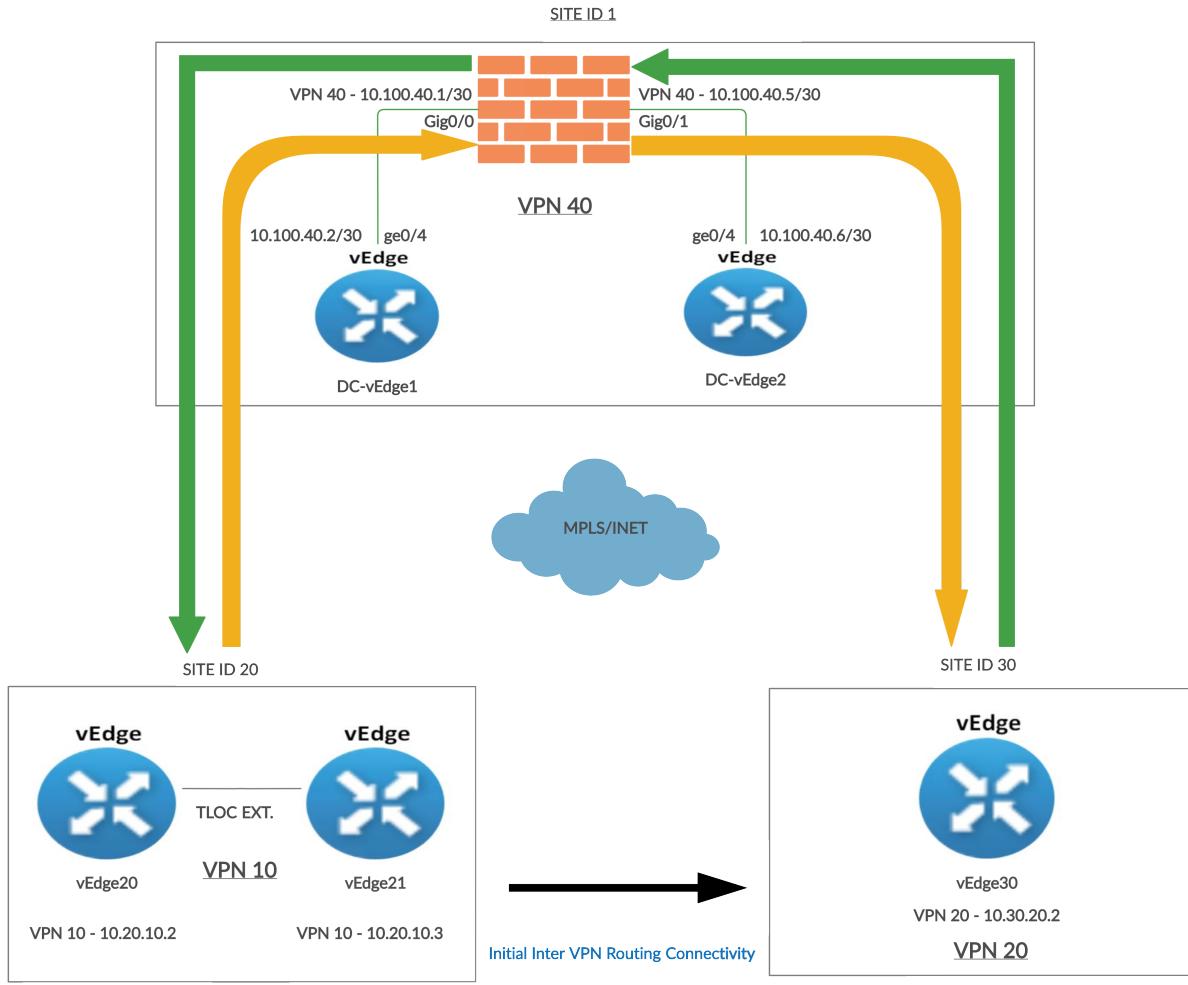
Task List

- Overview
- Configure VPN 40 on DC-vEdges

- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- Policies for Service Chaining
- Activity Verification

Policies for Service Chaining

Direct connectivity between two VPNs might not be a desirable scenario. There might be a requirement to enforce certain rules when two VPNs are communicating with each other. That's where Service Chaining comes into the picture, where we route Inter VPN traffic through an intermediary device (like a Firewall) to enforce our policies/rules. To reiterate, the traffic flow should look like the diagram below at the end of this section vs. the direct connectivity that we have between VPNs right now.



The Black arrow between Site 20 and Site 30 indicates the traffic flow when Inter VPN Routing configuration is done for the first time. Traffic flows directly between the two Sites.

The Orange arrow is the traffic flow from Site 20 VPN 10 to Site 30 VPN 20 once Service Chaining is configured.

Source IP: 10.20.10.2 or 10.20.10.3

Destination IP: 10.30.20.2

The Green arrow is the traffic flow from Site 30 VPN 20 to Site 20 VPN 10 once Service Chaining is configured.

Source IP: 10.30.20.2

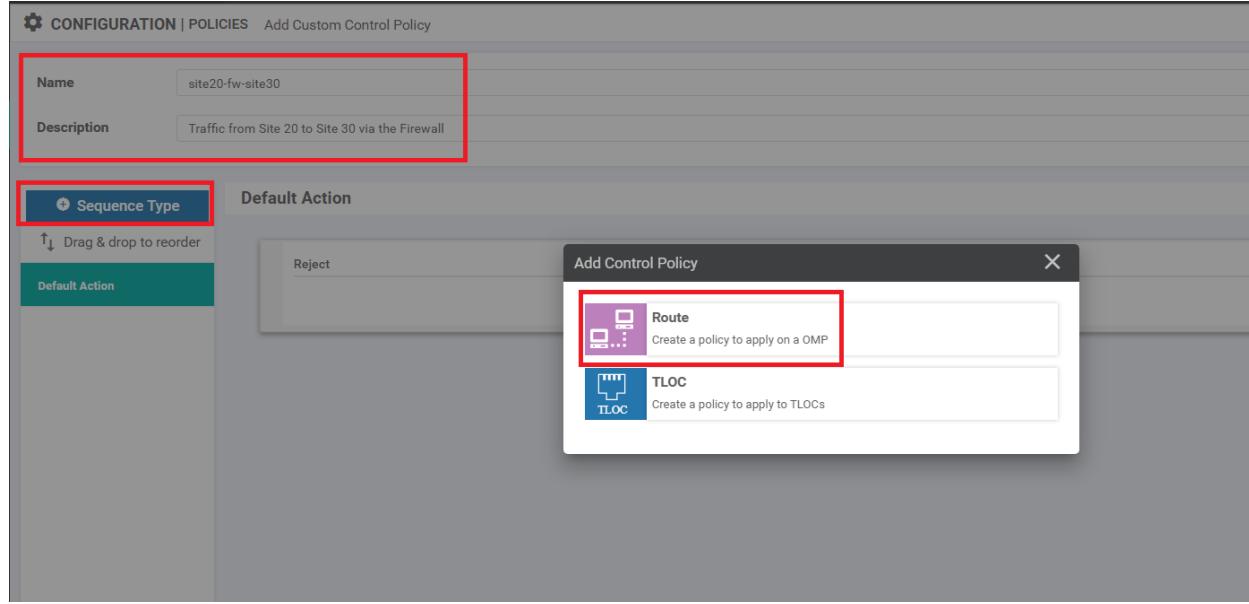
Destination IP: 10.20.10.2 or 10.20.10.3

1. On the vManage GUI, go to **Configuration => Policies**. Locate the **Site40-Guest-DIA** policy and click on the three dots next to it. Choose to **Edit** the policy. Make sure you're on the **Topology** tab and click on **Add Topology**. Choose to add a *Custom Control (Route and TLOC)* topology

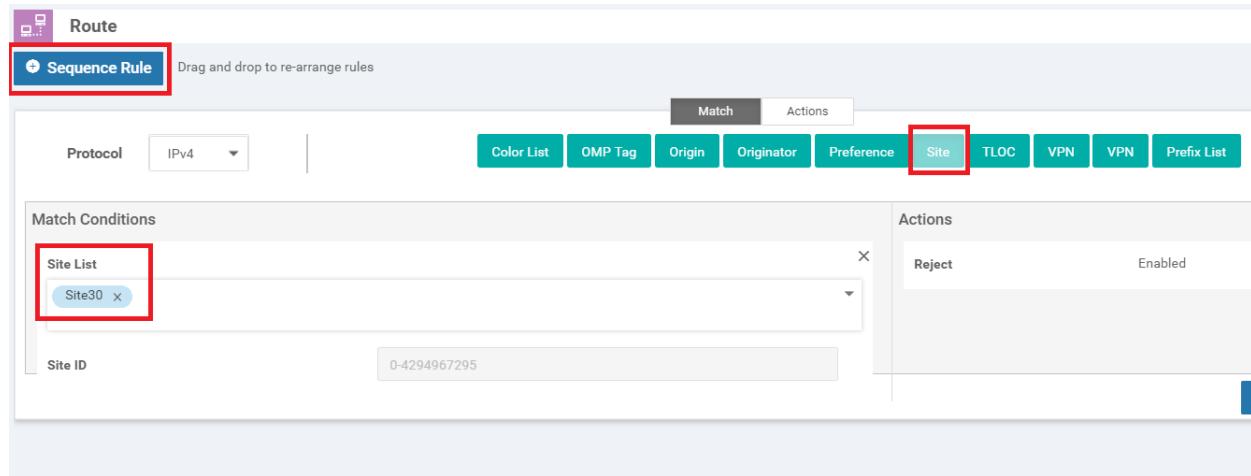
The screenshot shows the Cisco vManage interface under Configuration > Policies > Centralized Policy > Edit Policy. The Topology tab is selected. A red box highlights the 'Add Topology' button. Another red box highlights the 'Custom Control (Route & TLOC)' option in the dropdown menu. The table below lists two existing topologies: 'Import Existing Topology' and 'vpn20-inter-vpn10-40'. The table has columns for Type, Description, Reference Count, and Updated By.

| Type | Description | Reference Count | Updated By |
|----------------|---|-----------------|------------|
| Custom Control | Control Policy for Inter VPN Routing fr... | 1 | admin |
| Custom Control | Control Policy for Inter VPN routing bet... | 1 | admin |

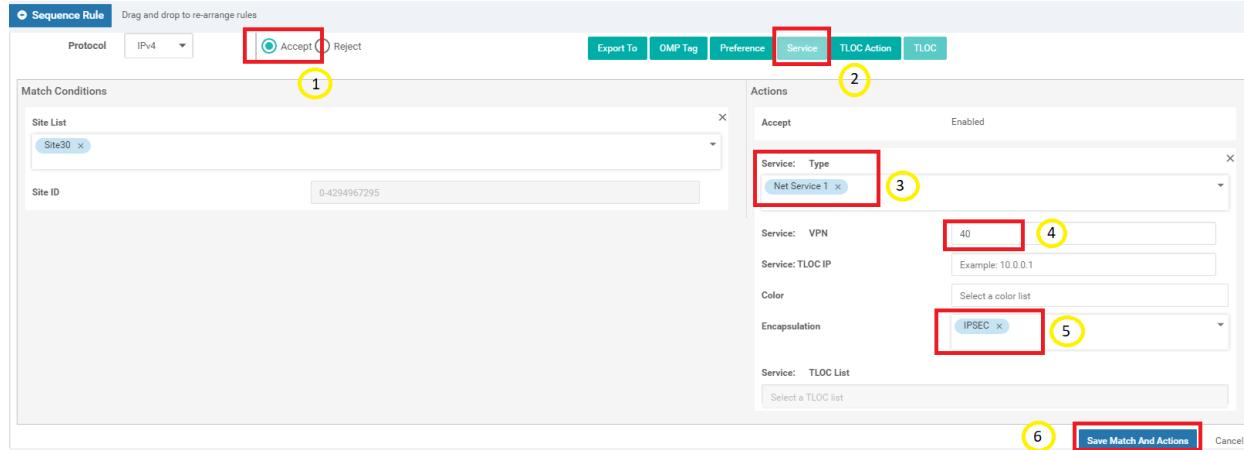
2. Give the Custom Control Policy a **Name** of *site20-fw-site30* and a Description of *Traffic from Site 20 to Site 30 via the Firewall*. Click on **Sequence Type** and choose **Route**



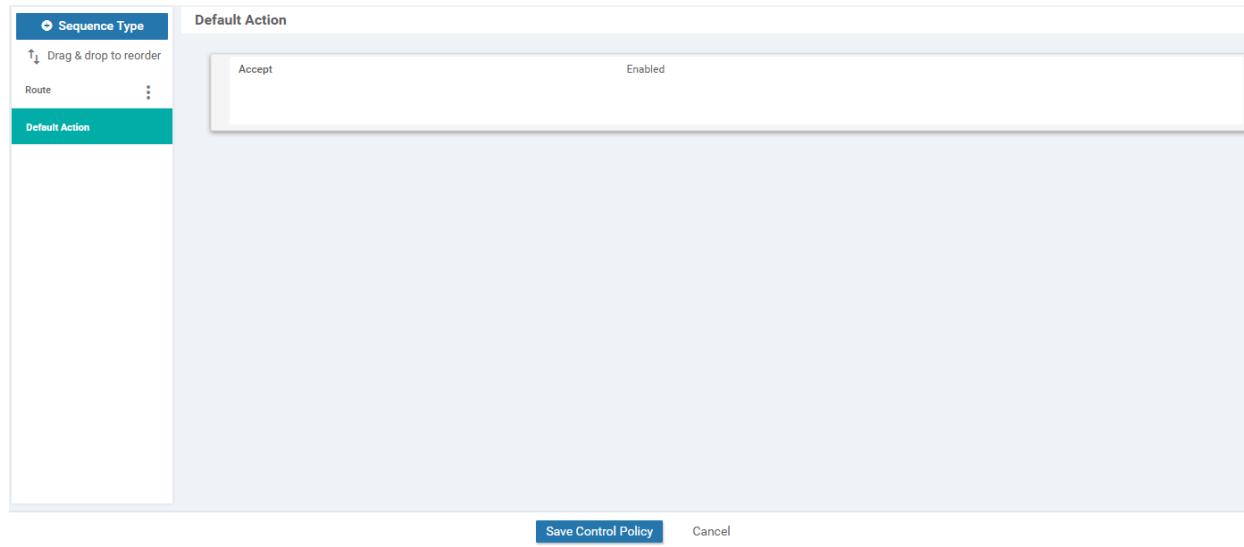
3. Click on **Sequence Rule** and select **Site** for a Match Condition. Click on the **Site List** drop down and choose *Site 30*.
Click on the **Actions** tab



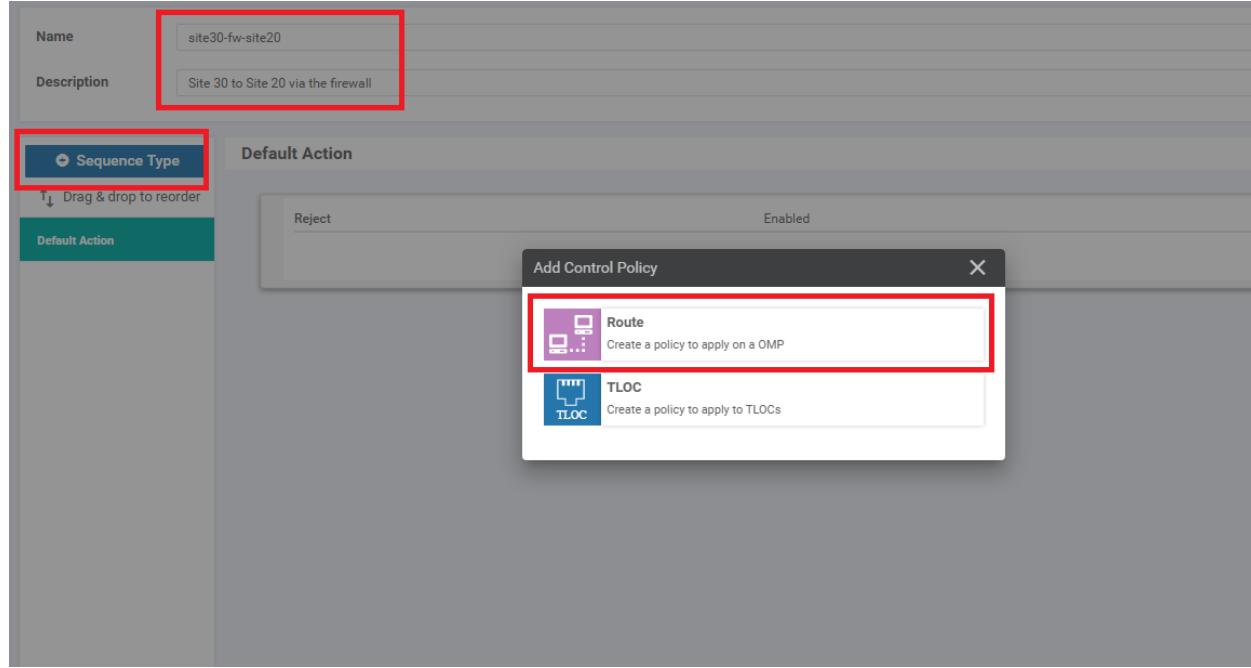
4. Select the **Accept** radio button and choose **Service**. Under Actions select the **Service: Type** as *Net Service 1* and specify a **Service: VPN** of *40*. Select an **Encapsulation** of *IPSEC* and click on **Save Match And Actions** to save this rule



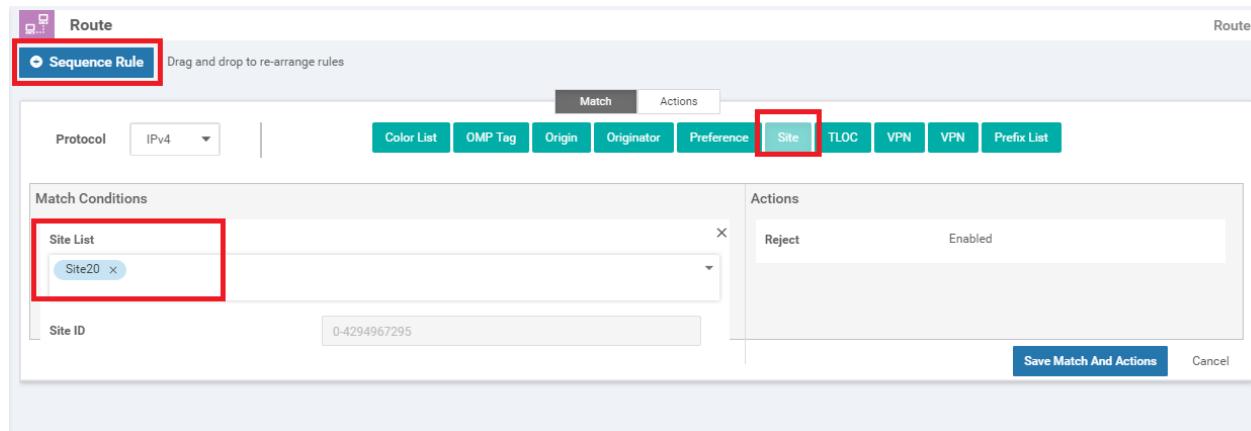
5. Click on **Default Action** on the left-hand side and click the pencil icon. Select Accept and then **Save Match And Actions**. The Default Action should change to **Accept Enabled**. Click on **Save Control Policy**



6. Make sure you're on the **Topology** tab and click on **Add Topology**. Choose to add a *Custom Control (Route and TLOC)* topology. Give the Custom Control Policy a **Name** of *site30-fw-site20* and a **Description** of *Site 30 to Site 20 via the firewall*. Click on **Sequence Type** and choose **Route**



7. Click on **Sequence Rule** and then select **Site**. Choose *Site 20* in the **Site List** under **Match Conditions**. Click on **Actions**



8. Select the **Accept** radio button and choose **Service**. Under Actions select the **Service: Type** as *Net Service 2* and specify a **Service: VPN** of *40*. Select an **Encapsulation** of *IPSEC* and click on **Save Match And Actions** to save this rule

The screenshot shows the 'Route' section of a configuration tool. At the top, there's a header with a 'Route' icon and the word 'Route'. Below it, a blue bar says 'Sequence Rule' and 'Drag and drop to re-arrange rules'. The main area has a step counter '1' and a title 'Match Conditions'. It lists 'Site List: Site20' and 'Site ID:'. To the right is a 'Actions' panel with a 'Accept' section. Under 'Accept', there are fields for 'Service:' (set to 'VPN') and 'Type' (set to 'Net Service 2'). Other sections like 'TLOC IP:', 'Color:', 'Encapsulation:', and 'IPSEC' are also present. A red box highlights the 'Type' field. At the bottom of the Actions panel are buttons for 'Edit', 'Delete', and 'Cancel'.

9. Click on **Default Action** on the left-hand side and click the pencil icon. Select Accept and then **Save Match And Actions**. The Default Action should change to **Accept Enabled**. Click on **Save Control Policy**

This screenshot shows a 'Default Action' configuration dialog. On the left, there's a list with 'Accept' selected. To its right, the status 'Enabled' is shown with a red box around it. At the bottom of the dialog are two buttons: 'Save Control Policy' (highlighted with a red box) and 'Cancel'.

10. Go to the **Policy Application** tab and locate the *site30-fw-site20* and *site20-fw-site30* entries. For *site30-fw-site20*, click on **New Site List** and choose *Site30* in the out direction. Click on **Add**. Similarly, for *site20-fw-site30*, click on **New Site List** and choose *Site20* in the out direction. Click on **Add**. Click on **Save Policy Changes**. Activate the change when prompted to do so

The screenshot shows the Policy Application interface with two policy entries:

- site30-fw-site20**:
 - Direction: out
 - Site List: Site30
- site20-fw-site30**:
 - Direction: out
 - Site List: Site20

At the bottom, there are three buttons: Preview, Save Policy Changes (highlighted with a red box), and CANCEL.

Task List

- [Overview](#)
- [Configure VPN 40 on DC-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter-VPN Routing Policies](#)
- [Inter-VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)

Activity Verification

1. Log in to the CLI of **vEdge20** via Putty (username and password given below) and enter `ping vpn 10 10.100.40.2` to test connectivity between Site 20 VPN 10 and Site DC VPN 40. The pings should fail

| Username | Password |
|----------|----------|
| admin | admin |

```
vEdge20# ping vpn 10 10.100.40.2
ping to VPN 10
PING 10.100.40.2 (10.100.40.2) 56(84) bytes of data.
From 127.1.0.2 icmp_seq=1 Destination Net Unreachable
From 127.1.0.2 icmp_seq=2 Destination Net Unreachable
From 127.1.0.2 icmp_seq=3 Destination Net Unreachable
From 127.1.0.2 icmp_seq=4 Destination Net Unreachable
From 127.1.0.2 icmp_seq=5 Destination Net Unreachable
From 127.1.0.2 icmp_seq=6 Destination Net Unreachable
From 127.1.0.2 icmp_seq=7 Destination Net Unreachable
From 127.1.0.2 icmp_seq=8 Destination Net Unreachable
From 127.1.0.2 icmp_seq=9 Destination Net Unreachable
From 127.1.0.2 icmp_seq=10 Destination Net Unreachable
From 127.1.0.2 icmp_seq=11 Destination Net Unreachable
From 127.1.0.2 icmp_seq=12 Destination Net Unreachable
From 127.1.0.2 icmp_seq=13 Destination Net Unreachable
From 127.1.0.2 icmp_seq=14 Destination Net Unreachable
From 127.1.0.2 icmp_seq=15 Destination Net Unreachable
^C
--- 10.100.40.2 ping statistics ---
15 packets transmitted, 0 received, +15 errors, 100% packet loss, time 13999ms

vEdge20#
```

This is due to the fact that we haven't set up inter VPN connectivity between VPN 10/VPN 20 and VPN 40. It is vital to ensure that the source and destination VPNs can access the Service Subnet.

2. On the vManage GUI, navigate to **Configuration => Policies**. Click on **Custom Options** on the top right-hand corner and select **Lists** (under Centralized Policy). Click on **VPN** in the left-hand menu and then **New VPN List**. Enter a **VPN List Name** of **Corp_PoS** and put **10,20** in the **Add VPN** field. Click on **Add**

Select a list type on the left and start creating your groups of interest

| Name | Entries | Reference Count | Updated By | Last Updated | Action |
|-----------|---------|-----------------|------------|----------------------------|--|
| PoS_FW | 20, 40 | 1 | admin | 20 Jul 2020 3:00:14 PM PDT | Edit Details Delete |
| FW | 40 | 0 | admin | 20 Jul 2020 2:58:21 PM PDT | Edit Details Delete |
| PoS | 20 | 2 | admin | 21 Jun 2020 4:16:01 AM PDT | Edit Details Delete |
| Corporate | 10 | 4 | admin | 21 Jun 2020 4:15:35 AM PDT | Edit Details Delete |
| Guest | 30 | 1 | admin | 21 Jun 2020 4:16:14 AM PDT | Edit Details Delete |
| Corp_FW | 10, 40 | 1 | admin | 20 Jul 2020 2:59:41 PM PDT | Edit Details Delete |

3. Go to **Configuration => Policies** and locate the **Site40-Guest-DIA Policy**. Click on the three dots next to it and choose to **Edit** the policy. Click on the **Topology** tab (top of the screen) and click on **Add Topology**. Choose to add a **Custom Control (Route & TLOC)** policy. Give the policy a **Name** of **vpn40-inter-vpn10-20** with a Description of **Control Policy for Inter VPN Routing from VPN 40 to VPNs 10 and 20**. Click on **Sequence Type** and choose **Route**

Name: vpn40-inter-vpn10-20
Description: Control Policy for Inter VPN Routing from VPN 40 to VPNs 10 and 20

Sequence Type

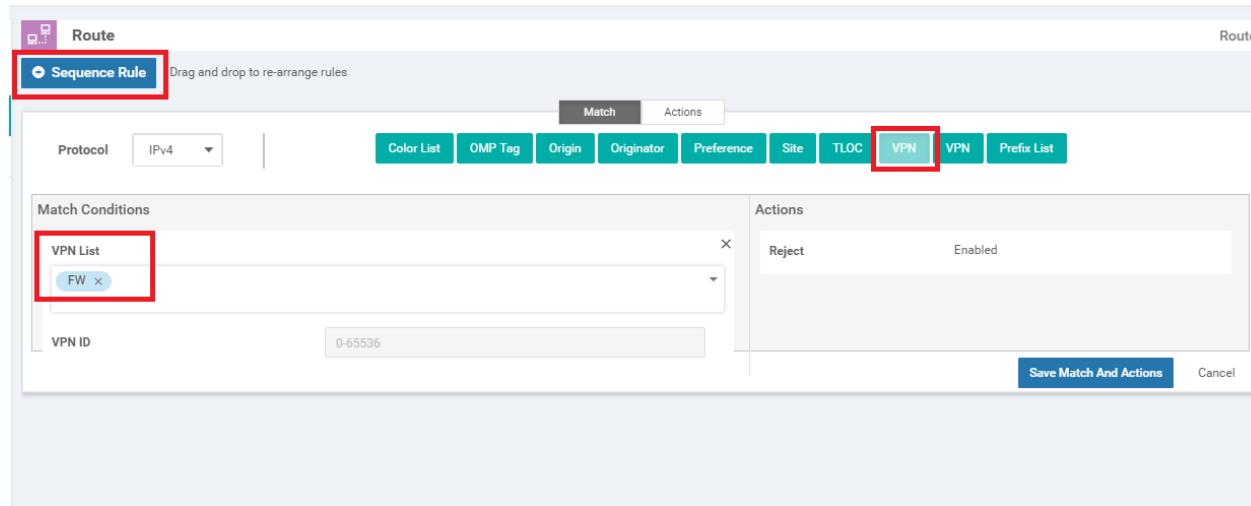
Default Action

Reject Enabled

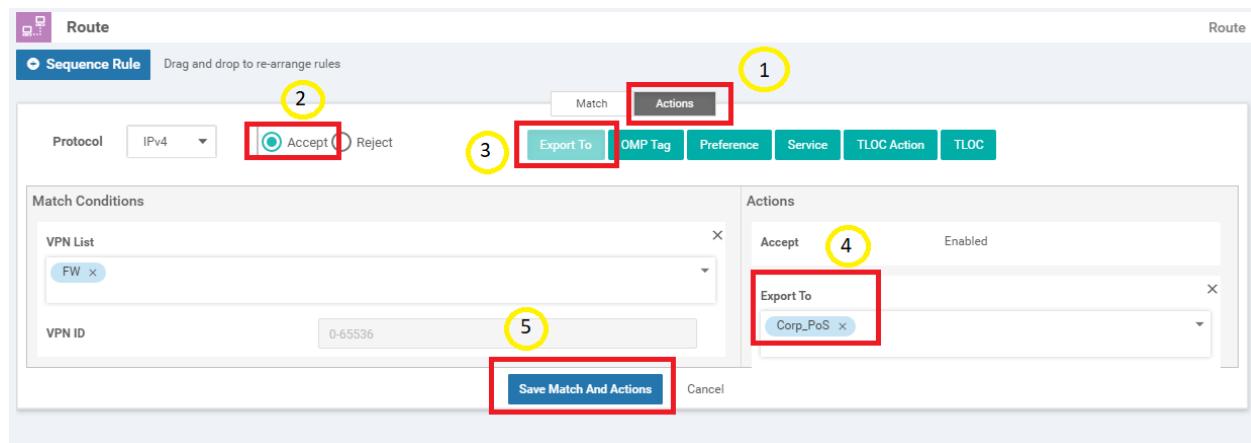
Add Control Policy

- Route: Create a policy to apply on a OMP
- TLOC: Create a policy to apply to TLOCs

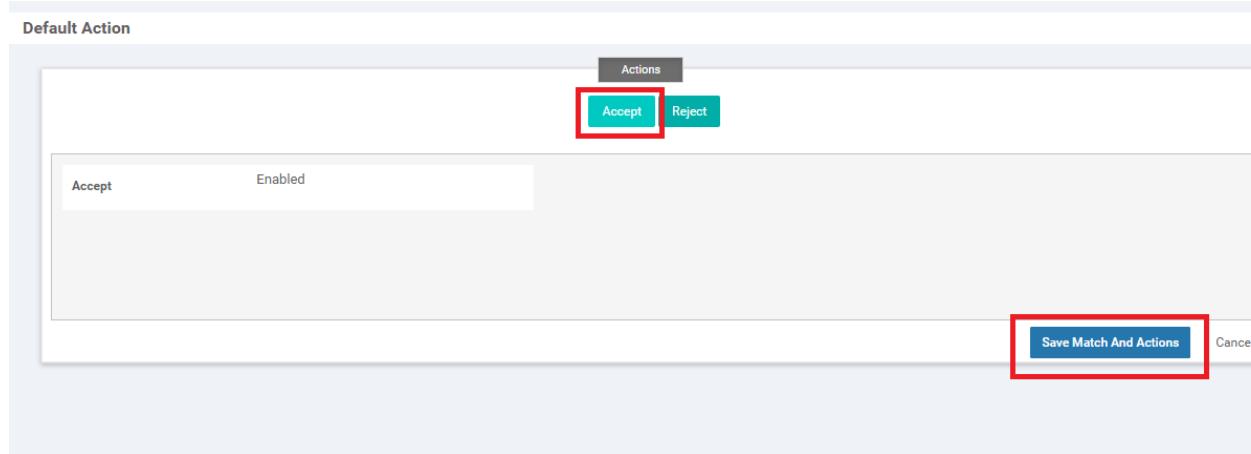
4. Click on **Sequence Rule** and add a **VPN** match. Select **FW** from the **VPN List** drop down



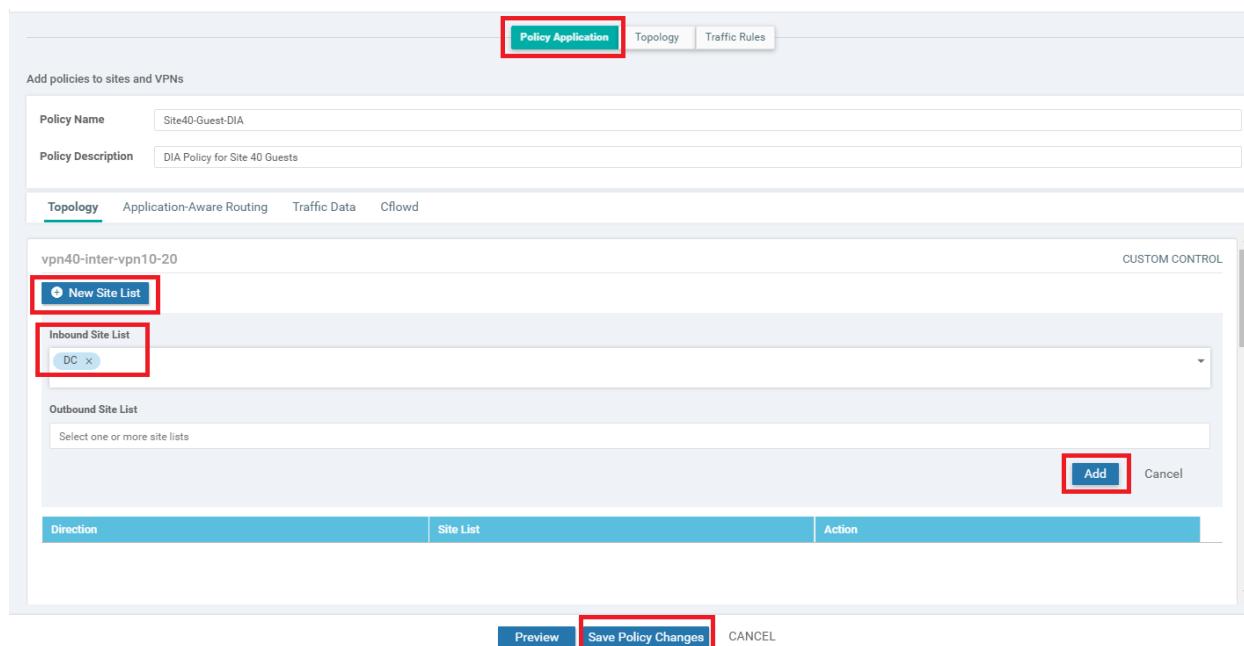
5. Click on the **Actions** tab and select the **Accept** radio button. Click on **Export To** and select **Corp_PoS** from the drop down under Actions. Click on **Save Match And Actions**



6. Select **Default Action** on the left-hand side and click on the pencil icon to edit the Default Action. Click on **Accept** and then **Save Match And Actions**. Click **Save Control Policy**



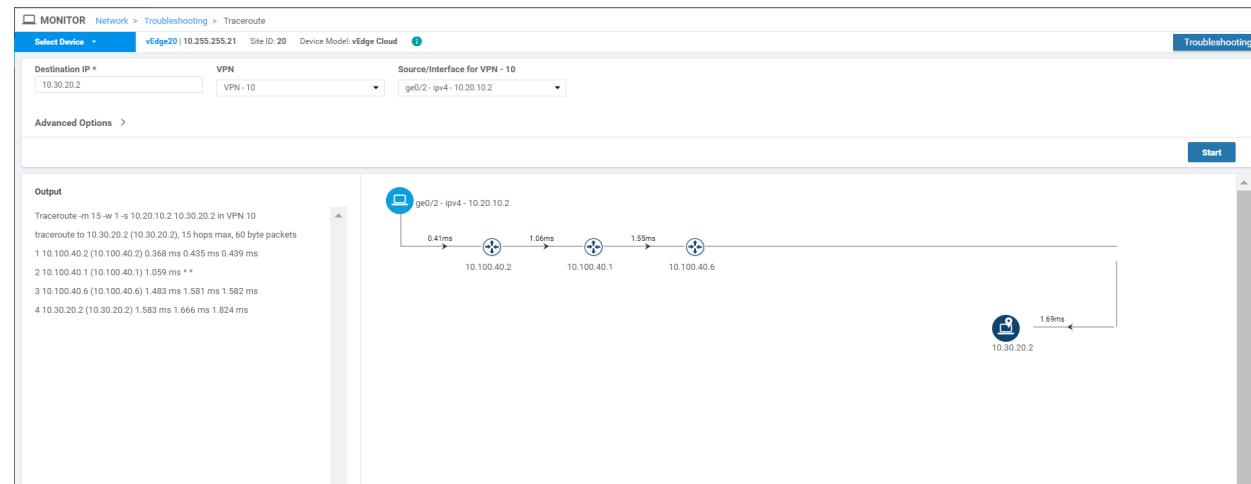
7. You should be back at the main policy screen. Click on the **Policy Application** tab and make sure you're under the **Topology** sub-tab (should not be under the main Topology tab). Click on **New Site List** under the entry for *vpn40-inter-vpn10-20* and select the **Inbound Site List** as DC. Click on **Add**. Click on **Save Policy Changes**. Click on **Activate** to push the changes to the vSmarts



8. Head back over to the CLI of vEdge20 and type `ping vpn 10 10.100.40.2`. The pings should now be successful. Type `ping vpn 10 10.100.40.1` to ping the Firewall. This should also work

```
vEdge20# ping vpn 10 10.100.40.2
Ping in VPN 10
PING 10.100.40.2 (10.100.40.2) 56(84) bytes of data.
64 bytes from 10.100.40.2: icmp_seq=1 ttl=64 time=0.488 ms
64 bytes from 10.100.40.2: icmp_seq=2 ttl=64 time=0.343 ms
64 bytes from 10.100.40.2: icmp_seq=3 ttl=64 time=0.351 ms
^C
--- 10.100.40.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.343/0.394/0.488/0.066 ms
vEdge20# ping vpn 10 10.100.40.1
Ping in VPN 10
PING 10.100.40.1 (10.100.40.1) 56(84) bytes of data.
64 bytes from 10.100.40.1: icmp_seq=2 ttl=254 time=1.86 ms
64 bytes from 10.100.40.1: icmp_seq=3 ttl=254 time=0.785 ms
64 bytes from 10.100.40.1: icmp_seq=4 ttl=254 time=0.684 ms
^C
--- 10.100.40.1 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.684/1.111/1.865/0.535 ms
vEdge20#
```

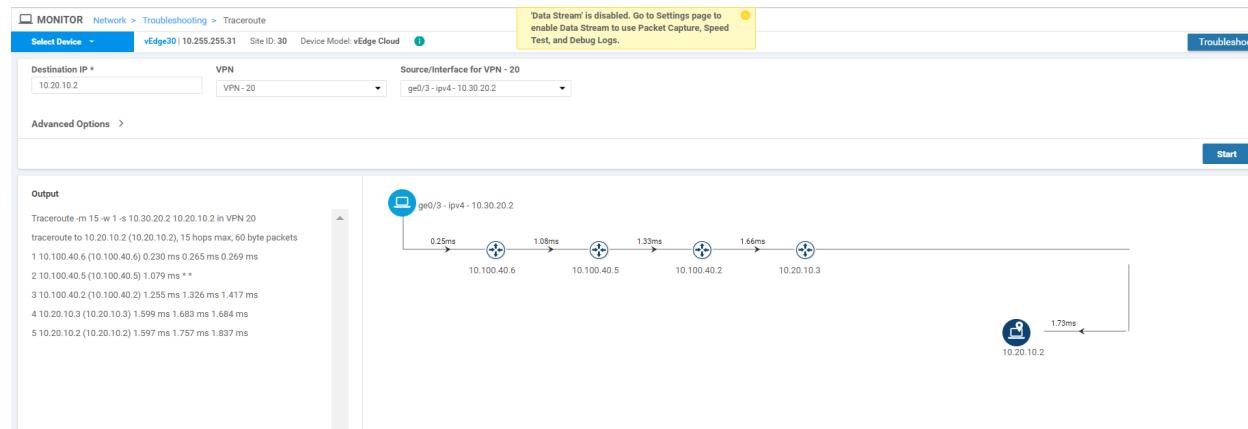
9. On the vManage GUI, go to **Monitor => Network** and select **vEdge20**. Click on **Troubleshooting** along the left-hand menu and choose **Traceroute**. Enter a **Destination IP** of **10.30.20.2** and a **VPN** of **VPN - 10**. Set the **Source/Interface** as **ge0/2** and click on **Start**. We are thus doing a traceroute from Site 20 VPN 10 to Site 30 VPN 20



Notice that traffic doesn't flow directly between the sites. Instead, it traverses the Firewall (IP of 10.100.40.1 in this case) and then goes to Site 30 VPN 20.

10. Click on **Select Device** in the top left-hand corner and select **vEdge30**. Enter a **Destination IP** of **10.20.10.2** and a **VPN** of **VPN - 20**. Specify a **Source/Interface** of **ge0/3** and click on **Start**. We are doing a traceroute from Site 30

VPN 20 to Site 20 VPN 10



In this case as well, traffic traverses the Firewall (IP of 10.100.40.5) and then goes to Site 20 VPN 10.

This completes the Service Chaining lab activity.

Task List

- [Overview](#)
- [Configure VPN 40 on DC-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)



Configuring Cloud OnRamp for SaaS

Summary: Implementing Cloud OnRamp for SaaS in Cisco SD-WAN

Table of Contents

- [Overview](#)
- [Prerequisite configuration for Cloud OnRamp](#)
- [Configuring Cloud OnRamp for SaaS](#)
- [Verification and Testing](#)

Task List

- Overview
- Prerequisite configuration for Cloud OnRamp
- Configuring Cloud OnRamp for SaaS
- Verification and Testing

Overview

With the changing network landscape, the way in which applications are consumed has also undergone a massive overhaul. Applications being hosted in the cloud (Public/Private) are a common occurrence, rather than the exception.

Cloud OnRamp for SaaS monitors widely used Cloud Applications and arrives at a vQoE score (Viptela Quality of Experience). Loss and latency are used to calculate the vQoE score and based on this, the solution routes traffic to the Cloud Application via the optimal path. The vQoE value is calculated periodically to ensure persistent optimal application performance.

Task List

- Overview
- Prerequisite configuration for Cloud OnRamp
- Configuring Cloud OnRamp for SaaS
- Verification and Testing

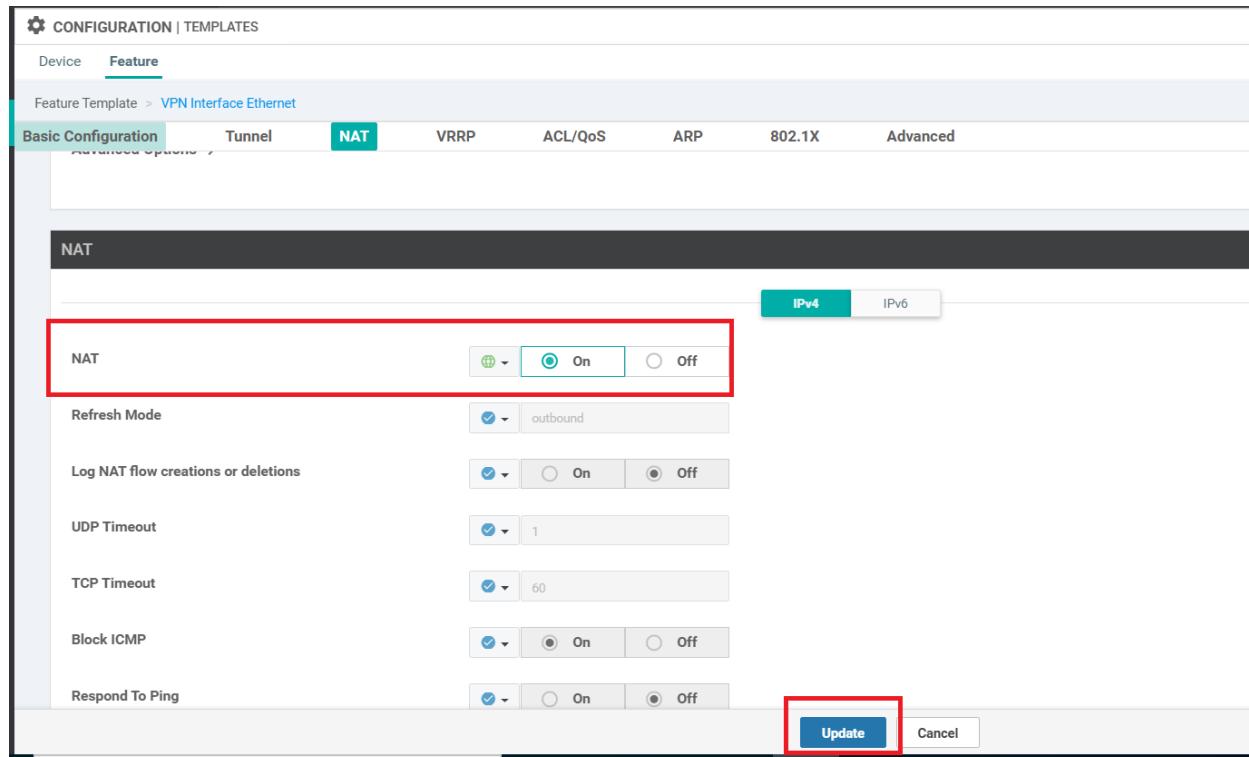
Prerequisite configuration for Cloud OnRamp

1. On the vManage GUI, navigate to **Configuration => Templates => Feature Tab**. Locate the **vEdge30_INET** template and click on the three dots next to it. Choose to **Edit** the template

The screenshot shows the vManage Configuration | Templates page with the Feature tab selected. A context menu is open over the row for the vEdge30_INET template, with the 'Edit' option highlighted.

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|--------------------------|---|---------------------------|--------------------|------------------|------------------|--------------|------------------------------------|----------------------|
| Site20-vpn0 | VPN0 for the Site20 vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 5:41:03 AM PDT | ... |
| cEdge-vpn0-int-single | cEdge VPN 0 Interface Templa... | Cisco VPN Interface | CSR1000v | 1 | 2 | admin | 18 May 2020 1:30:15 PM PDT | ... |
| vEdge30-vpn0 | VPN0 for the Site30 INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:25:49 AM PDT | ... |
| cEdge-vpn512-int-dual | cEdge VPN 512 Interface Tem... | Cisco VPN Interface | CSR1000v | 2 | 3 | admin | 18 May 2020 8:39:03 AM PDT | ... |
| cEdge_VPN512_dual_uplink | cEdge VPN 512 Template for ... | Cisco VPN | CSR1000v | 2 | 3 | admin | 18 May 2020 8:35:47 AM PDT | ... |
| vedge-vpn10-int | VPN 10 Interface Template for... | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 25 May 2020 1:43:16 PM PDT | ... |
| vEdge30_INET | INET interface for the Site30 v... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 05 Jun 2020 10:03:58 PM PDT | ... |
| cEdge_VPN0_dual_uplink | cEdge VPN 0 Template for Du... | Cisco VPN | CSR1000v | 1 | 1 | admin | 23 May 1 | ... |
| vedge-vpn20-DC | VPN 20 Template for vEdge... | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 27 May 1 | View |
| cEdge-vpn0-int-dual_mpls | cEdge VPN 0 Interface Templa... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 05 Jun 2 | Edit |
| cEdge-vpn0-int-dual | cEdge VPN 0 Interface Templa... | Cisco VPN Interface | CSR1000v | 1 | 1 | admin | 06 Jun 2 | Change Device Models |
| cEdge-vpn20 | VPN 20 Template for the cEdg... | Cisco VPN | CSR1000v | 2 | 3 | admin | 25 May 2 | Delete |
| | | | | | | | | Copy |

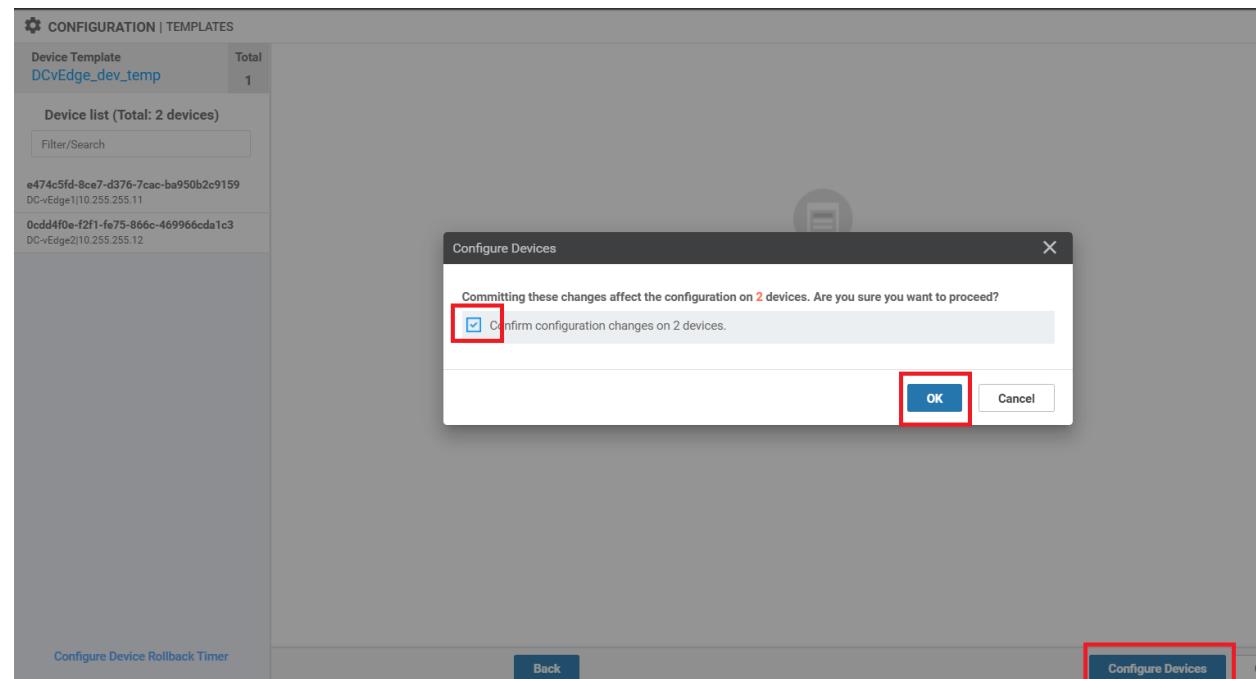
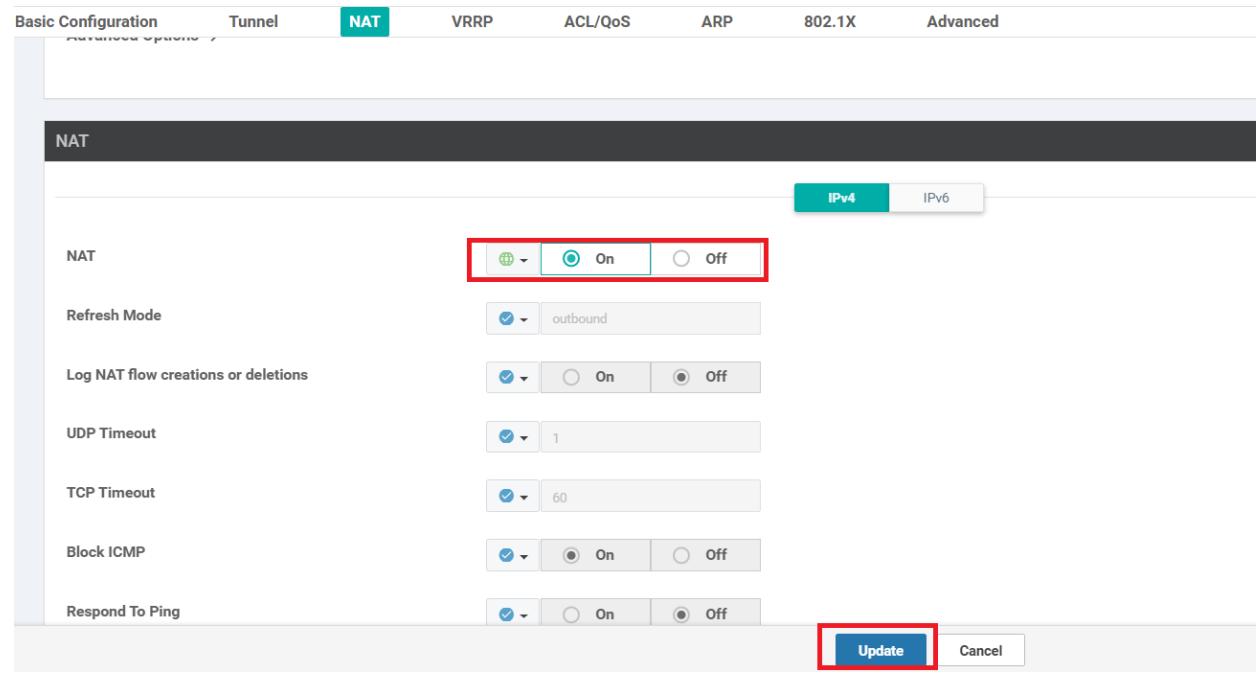
2. Scroll down to the NAT section and set NAT to a global value of **On**. Click on **Update**



3. Click on **Next and Configure Device**. There are no changes to be made here since we are simply enabling NAT on the interface.
4. On the vManage GUI, go to **Configuration => Templates => Feature Tab**. Locate the *DC-vEdge_INET* template and click on the three dots next to it. Choose to **Edit** the template

The screenshot shows the 'Templates' list in the 'Configuration | Templates' section. The 'Feature' tab is selected. A search bar at the top has 'dc' entered. The table lists various templates, including 'vedge-vpn20-DC', 'DC-Edge_mgmt_int', 'DC-Edge_MPLS', 'DC-vEdge_INET' (which is highlighted with a red box), 'DC-OSPF', 'DCvEdge-vpn512', and 'DCvEdge-vpn0'. The 'DC-vEdge_INET' row has a context menu open, with the 'Edit' option highlighted with a red box.

5. Scroll down to the NAT section and set **NAT** to a Global value of **On**. Click on **Update**. Click **Next/Configure Devices** to finish the update to the devices. Confirm the change on two devices and click **OK**



We have enabled NAT on all the interfaces that will be communicating directly with the SaaS applications. There are other prerequisites that need to be taken into consideration while deploying this in production (a few examples are devices should

be in vManage mode, DNS server details populated in VPN 0 etc.) but these have been fulfilled in our SD-WAN Network.

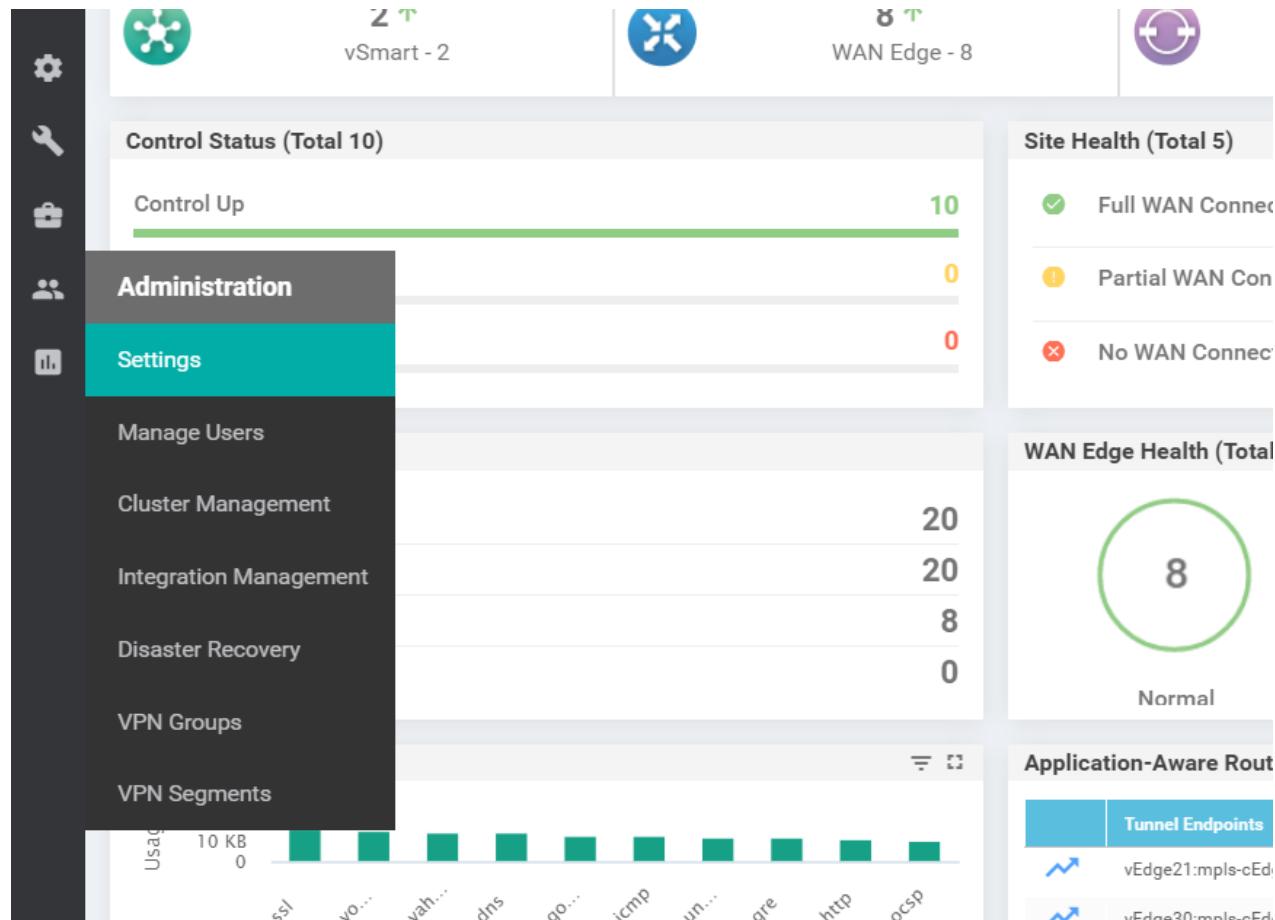
Task List

- [Overview](#)
- [Prerequisite configuration for Cloud OnRamp](#)
- Configuring Cloud OnRamp for SaaS
- Verification and Testing

Configuring Cloud OnRamp for SaaS

Go through the following steps in order to configure Cloud OnRamp for SaaS in our SD-WAN network.

1. On the vManage GUI, navigate to **Administration => Settings**

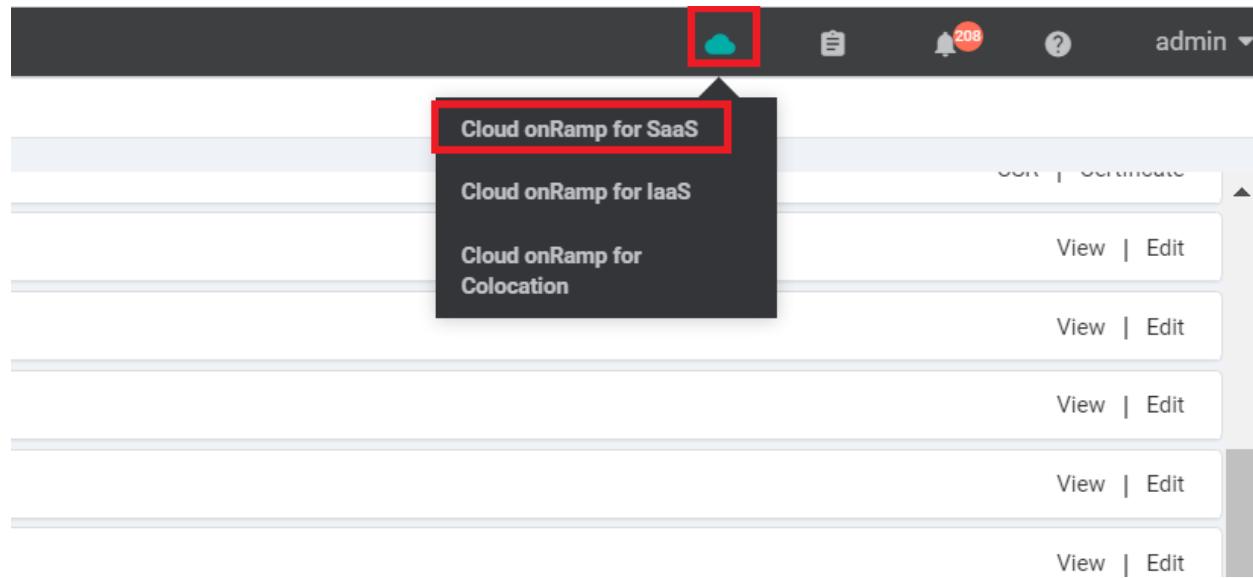


2. Locate the **Cloud onRamp for SaaS** section and click on **Edit**. Set the radio button to **Enabled** and click on **Save**.

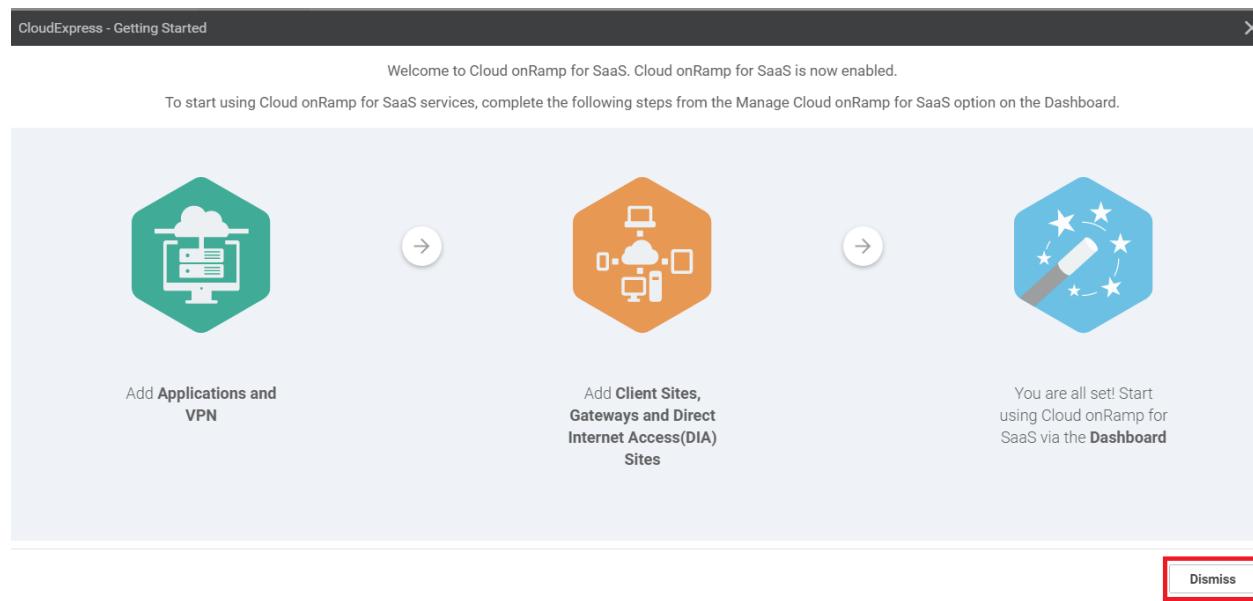
Cloud OnRamp for SaaS needs to be enabled system wide before it can be used

The screenshot shows the 'Statistics Setting' page. In the 'Cloud onRamp for SaaS' section, the 'Enable CloudExpress' radio button is set to 'Enabled' (highlighted with a red box). A 'Save' button is also highlighted with a red box. Other sections include 'Manage Encrypted Password' (Disabled) and 'vAnalytics' (Disabled), each with 'View | Edit' links.

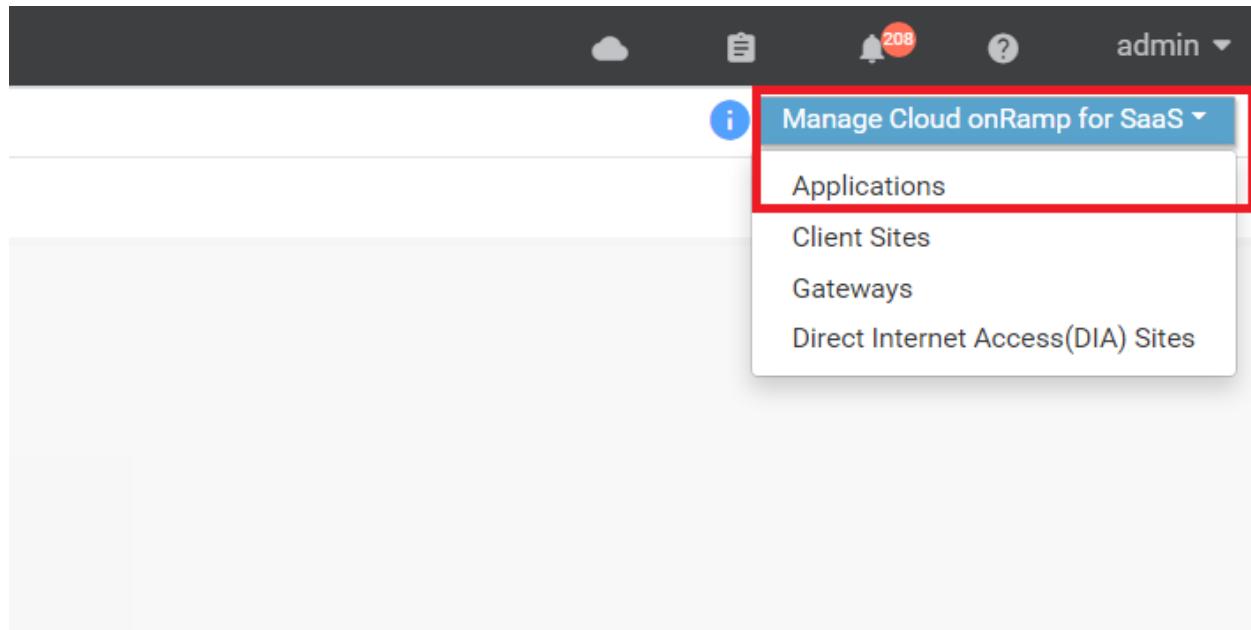
3. Once enabled, click on the **Cloud** icon in the top right-hand of the screen and click on **Cloud onRamp for SaaS**



4. Click on **Dismiss**



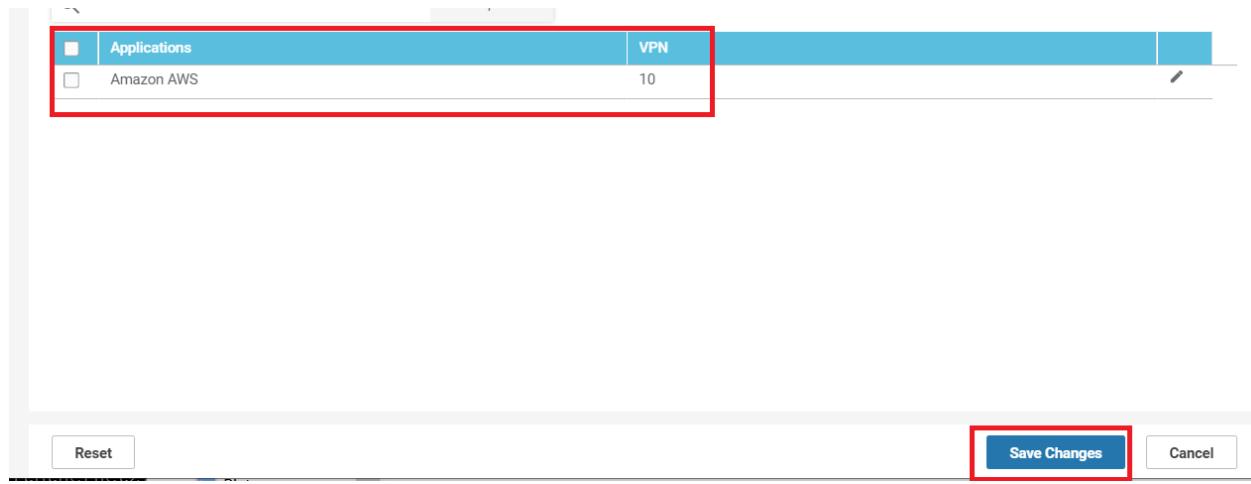
5. Click on **Manage Cloud onRamp for SaaS** (top right-hand corner) and click on **Applications**



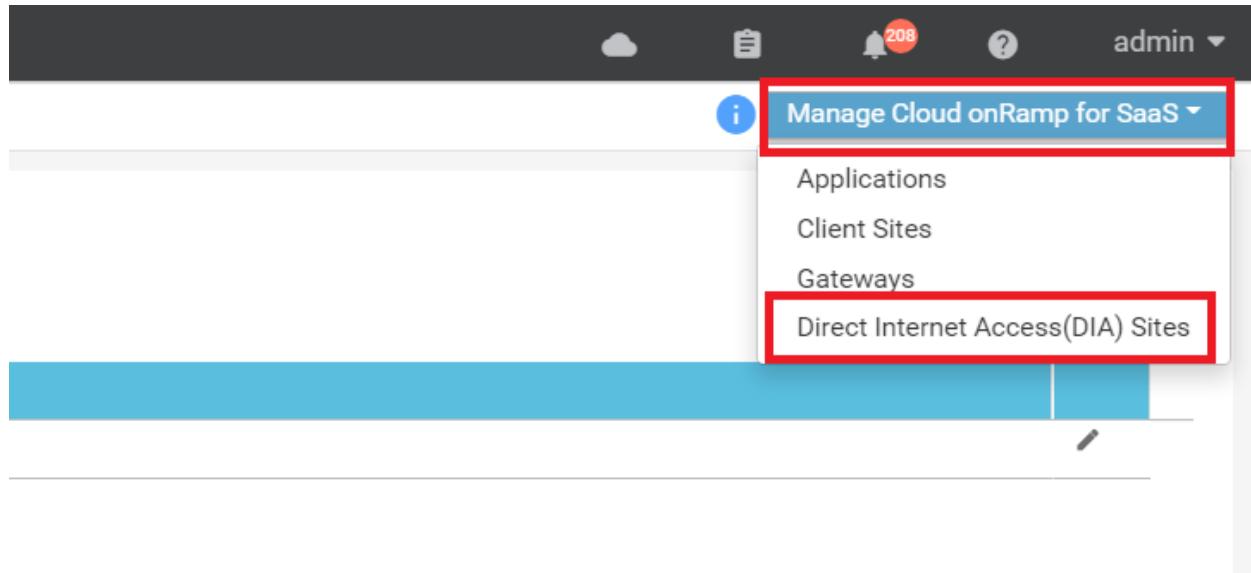
6. Specify a random application (example shows Amazon AWS, but you can choose something else like Oracle or Google Apps) and populate a **VPN** of 10

A screenshot of a modal dialog box titled 'Add Applications & VPN'. The dialog has two input fields: 'Applications' containing 'Amazon AWS' and 'VPN' containing '10'. At the bottom right are two buttons: a blue 'Add' button with a red box around it, and a white 'Cancel' button.

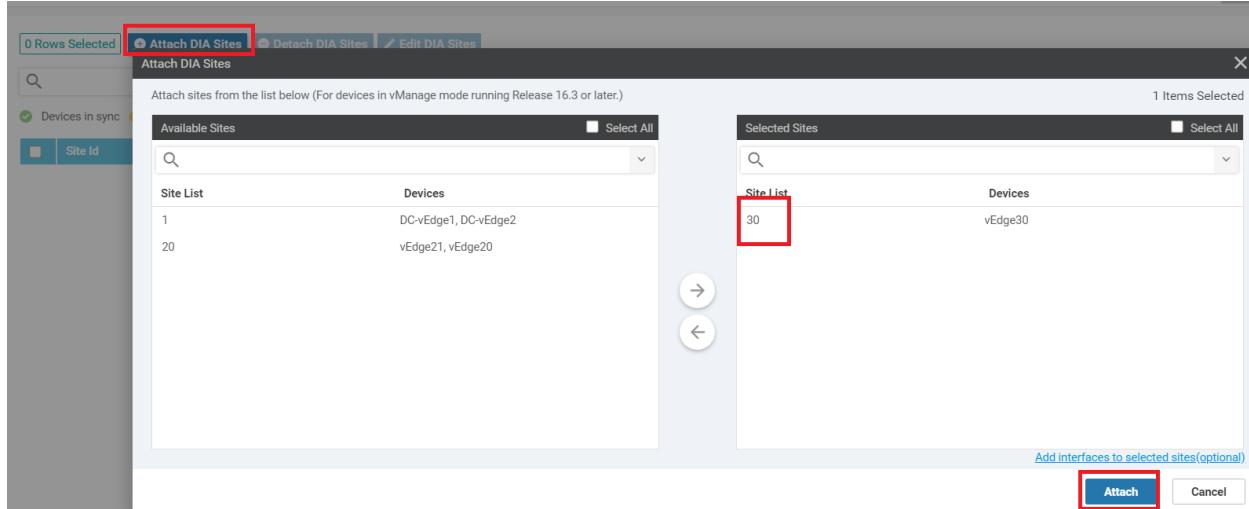
7. Make sure the chosen Application shows up and click on **Save Changes**



8. Click on **Cloud onRamp for SaaS** (top right-hand corner) again and click on **Direct Internet Access (DIA) Sites**



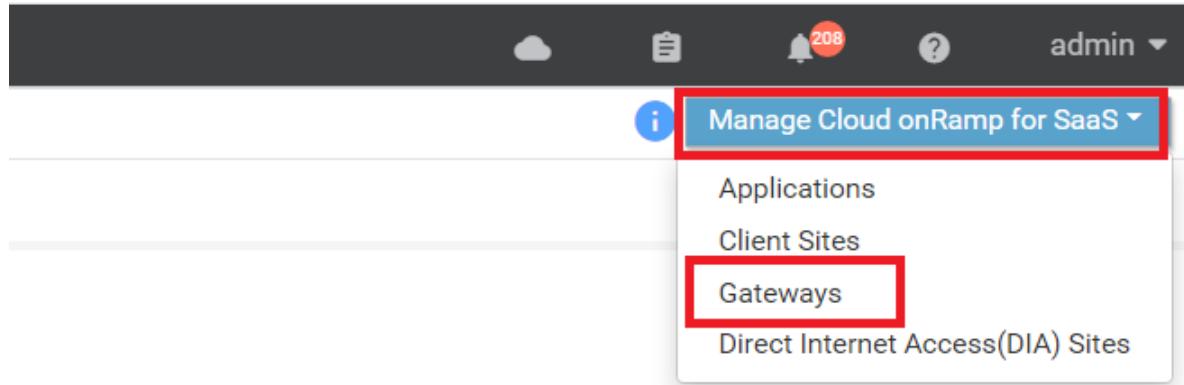
9. Click on **Attach DIA Sites** and move Site 30 to the **Selected Sites** section. Click on **Attach**



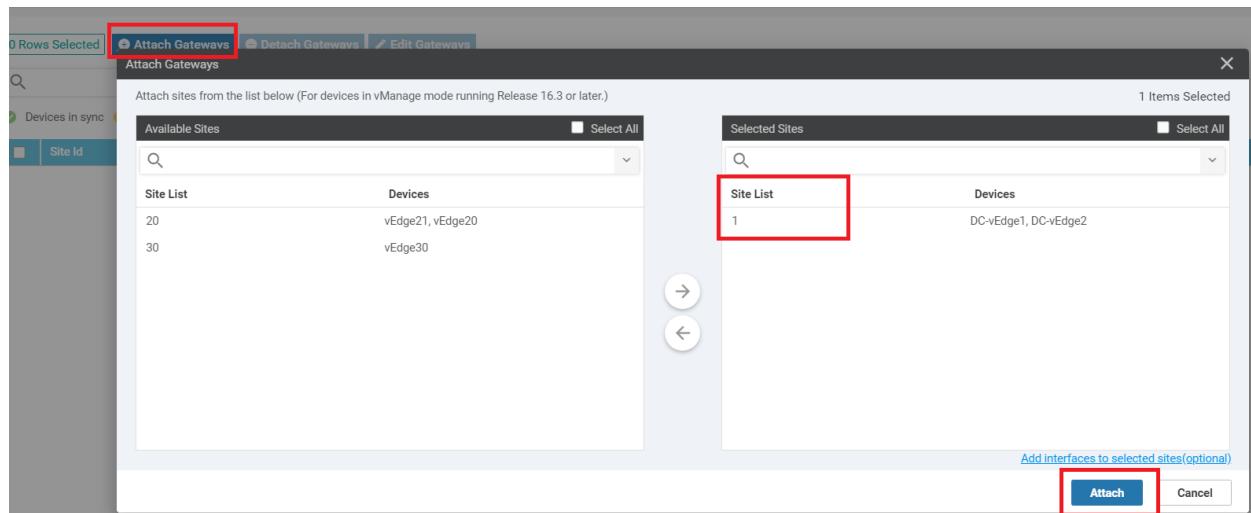
10. Wait for the task to go through successfully. Once it is done, click on the **Cloud** icon in the top right corner and click **Cloud onRamp for SaaS**

The screenshot shows the Cisco vManage interface with a dark header bar. The header includes the Cisco logo, the title 'Cisco vManage', and a 'Cloud' icon (highlighted with a red box) in the top right. Below the header is a 'TASK VIEW' section. It displays a single task entry: 'Push Feature Template Configuration | Validation Success' (highlighted with a red box). The task was initiated by 'admin' and completed successfully. At the bottom, there is a table with columns: Status, Message, Chassis Number, Device Model, Hostname, System IP, Site ID, and vManage IP. The first row shows a 'Success' status (highlighted with a red box), message 'Done - Push Feature Template...', chassis number '17026153-f09e-be4b-6dce-48...', device model 'vEdge Cloud', hostname 'vEdge30', system IP '10.255.255.31', site ID '30', and vManage IP '10.255.255.31'.

11. Click on **Manage Cloud onRamp for SaaS** and choose Gateways



12. Click on **Attach Gateways** and move Site 1 to the Selected Sites. Click on **Attach**



13. If you go to **Configuration => Cloud OnRamp for SaaS** (or click the Cloud icon and go to Cloud onRamp for SaaS), you should see the selected Application with 3 Devices attached to it. Click on the Application and the three Devices should be tagged with a vQoE Status of Bad. Their vQoE score is 0.0, indicating that information hasn't been collected to arrive at a score. We will need to wait for some time (another tea/coffee?)

| Sites List | Hostname | vQoE Status | vQoE Score | DIA Status | Selected Interface | Activated Gateway | Local Color |
|------------|-----------|-------------|------------|------------|--------------------|-------------------|-------------|
| 1 | DC-vEdge1 | | 0.0 | none | N/A | N/A | N/A |
| 30 | vEdge30 | | 0.0 | none | N/A | N/A | N/A |
| 1 | DC-vEdge2 | | 0.0 | none | N/A | N/A | N/A |

14. If you refresh the screen, you should notice devices gradually showing up with their vQoE score. Notice that vEdge30 is selecting a local path to the selected Application

| Sites List | Hostname | vQoE Status | vQoE Score | DIA Status | Selected Interface | Activated Gateway | Local Color | Remote Color |
|------------|-----------|-------------|------------|------------|--------------------|-------------------|-------------|--------------|
| 1 | DC-vEdge1 | | 0.0 | none | N/A | N/A | N/A | N/A |
| 30 | vEdge30 | | 10.0 | local | ge0/0 | N/A | N/A | N/A |
| 1 | DC-vEdge2 | | 0.0 | none | N/A | N/A | N/A | N/A |

| Sites List | Hostname | vQoE Status | vQoE Score | DIA Status | Selected Interface | Activated Gateway | Local Color | Remote Color |
|------------|-----------|-------------|------------|------------|--------------------|-------------------|-------------|--------------|
| 1 | DC-vEdge1 | | 10.0 | local | ge0/0 | N/A | N/A | N/A |
| 30 | vEdge30 | | 10.0 | local | ge0/0 | N/A | N/A | N/A |
| 1 | DC-vEdge2 | | 10.0 | local | ge0/0 | N/A | N/A | N/A |

Through the DIA configuration, we have provided vEdge30 with a local breakout to the Application and by adding Site 1 as the Gateway, traffic can be punted over the MPLS link to the DC site and sent out the Internet breakout there, in the event of the local Site30 Internet breakout facing issues.

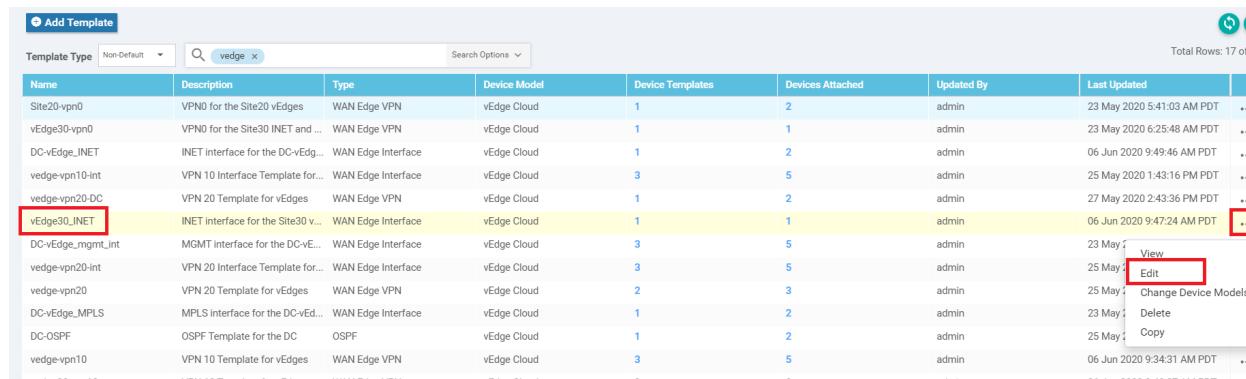
Task List

- Overview

- Prerequisite configuration for Cloud OnRamp
- Configuring Cloud OnRamp for SaaS
- Verification and Testing

Verification and Testing

1. Navigate to Configuration => Template => Feature Tab and locate the vEdge30_INET template. Click on the three dots next to it and choose to Edit



The screenshot shows a table of network templates. The 'vEdge30_INET' row is highlighted with a red box. A context menu is open over this row, with the 'Edit' option also highlighted with a red box.

| Name | Description | Type | Device Model | Device Templates | Devices Attached | Updated By | Last Updated | Actions |
|-------------------|------------------------------------|--------------------|--------------|------------------|------------------|------------|----------------------------|----------------------|
| Site20-vpn0 | VPN0 for the Site20 vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 23 May 2020 5:41:03 AM PDT | ... |
| vEdge30-vpn0 | VPN0 for the Site30 INET and ... | WAN Edge VPN | vEdge Cloud | 1 | 1 | admin | 23 May 2020 6:25:48 AM PDT | ... |
| DC-vEdge_INET | INET Interface for the DC-vEdg... | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 06 Jun 2020 9:49:46 AM PDT | ... |
| vedge-vpn10-int | VPN 10 Interface Template for... | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 25 May 2020 1:43:16 PM PDT | ... |
| vedge-vpn20-DC | VPN 20 Template for vEdges | WAN Edge VPN | vEdge Cloud | 1 | 2 | admin | 27 May 2020 2:43:36 PM PDT | ... |
| vEdge30_INET | INET Interface for the Site30 v... | WAN Edge Interface | vEdge Cloud | 1 | 1 | admin | 06 Jun 2020 9:47:24 AM PDT | ... |
| DC-vEdge_mgmt_int | MGMT Interface for the DC-vEd... | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 23 May | View |
| vedge-vpn20-int | VPN 20 Interface Template for... | WAN Edge Interface | vEdge Cloud | 3 | 5 | admin | 25 May | Edit |
| vedge-vpn20 | VPN 20 Template for vEdges | WAN Edge VPN | vEdge Cloud | 2 | 3 | admin | 25 May | Change Device Models |
| DC-vEdge_MPLS | MPLS interface for the DC-vEd... | WAN Edge Interface | vEdge Cloud | 1 | 2 | admin | 23 May | Delete |
| DC OSPF | OSPF Template for the DC | OSPF | vEdge Cloud | 1 | 2 | admin | 25 May | Copy |
| vedge-vpn10 | VPN 10 Template for vEdges | WAN Edge VPN | vEdge Cloud | 3 | 5 | admin | 06 Jun 2020 9:34:31 AM PDT | ... |

2. Scroll down to the **ACL/QOS** section and specify a **Shaping Rate (Kbps)** of 1. This will inject delay on our INET link connected to vEdge30. Click on **Update**

Basic Configuration Tunnel NAT VRRP **ACL/QoS** ARP 802.1X Advanced

NO data available

ACL/QoS

Shaping Rate (Kbps) 1

QoS Map

Rewrite Rule

Ingress ACL - IPv4 On Off

Egress ACL - IPv4 On Off

Ingress ACL - IPv6 On Off

Egress ACL - IPv6 On Off

Update Cancel

3. Click on **Next/Configure Devices**. You can check the side-by-side configuration to see that the shaping rate is applied to interface ge0/0

CONFIGURATION | TEMPLATES

| Device Template | Total |
|------------------|-------|
| vEdge30_dev_temp | 1 |

Device list (Total: 1 devices)

Filter/Search

```

17026153-f09e-be4b-6dce-482fce43aeb2
vEdge30|10.255.255.31

dns 10.2.1.5 primary
dns 10.2.1.6 secondary
interface ge0/0
ip address 100.100.100.30/24
nat
!
tunnel-interface
encapsulation ipsec
color public-internet
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
no shutdown
qos-map WAN-QoS
!
interface ge0/1
ip address 192.0.2.14/30
tunnel-interface
encapsulation ipsec

```

Configure Device Rollback Timer

Back

Configure Devices

'Configure' action will be applied to 1 device(s)
attached to 1 device template(s).

4. Wait for some time and traffic to the chosen Application from vEdge30 (check via Cloud icon => Cloud onRamp for SaaS => click on the Application) should have a DIA status of **gateway**, indicating that the DC Gateway is being used to contact Amazon AWS (in this example). The local/remote color is *mpls* with the system-ip of the gateway being used

CONFIGURATION Cloud onRamp for SaaS > Amazon AWS

Manage Cloud onRamp for SaaS

Bad (0-5) Average (5-8) Good (8-10)

VPN List: VPN-10 | Search Options | Total Rows: 3

| Sites List | Hostname | vQoE Status | vQoE Score | DIA Status | Selected Interface | Activated Gateway | Local Color | Remote Color |
|------------|-----------|--|---|------------|--------------------|-------------------|-------------|--------------|
| 1 | DC-vEdge1 | ⚠️ | 7.0 ↗️ | local | ge0/0 | N/A | N/A | N/A |
| 30 | vEdge30 | ⚠️ | 7.0 ↗️ | gateway | N/A | 10.255.255.11 | mpls | mpls |
| 1 | DC-vEdge2 | 🟢 | 10.0 ↗️ | local | ge0/0 | N/A | N/A | N/A |

The vQoE score might vary, as shown in the image below (it usually takes approximately 15 to 20 minutes for the expected results to show up)

| Sites List | Hostname | vQoE Status | vQoE Score | DIA Status | Selected Interface | Activated Gateway | Local Color | Remote Color |
|------------|-----------|-------------|------------|------------|--------------------|-------------------|-------------|--------------|
| 1 | DC-vEdge1 | ✓ | 10.0 ↗ | local | ge0/0 | N/A | N/A | N/A |
| 1 | DC-vEdge2 | ✓ | 10.0 ↗ | local | ge0/0 | N/A | N/A | N/A |
| 30 | vEdge30 | ✓ | 10.0 ↗ | gateway | N/A | 10.255.255.11 | mpls | mpls |

5. Go back to the *vEdge30-INET* Feature template (refer to Steps 1 and 2 of this section) and set the **Shaping Rate (Kbps)** to the Default value. Click on **Update**. Click on **Next/Configure Devices**

Basic Configuration Tunnel NAT VRRP **ACL/QoS** ARP 802.1X Advanced

ACL/QoS

Shaping Rate (Kbps) (highlighted by a red box)

QoS Map

Rewrite Rule

Ingress ACL - IPv4 On Off

Egress ACL - IPv4 On Off

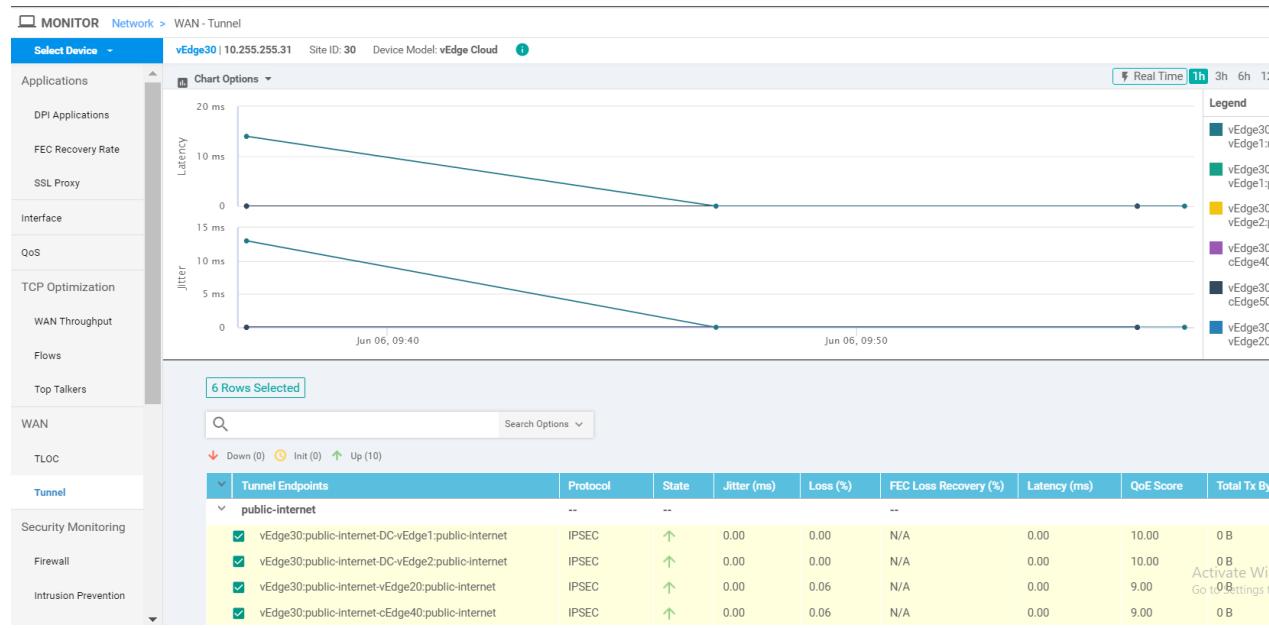
Ingress ACL - IPv6 On Off

Egress ACL - IPv6 On Off

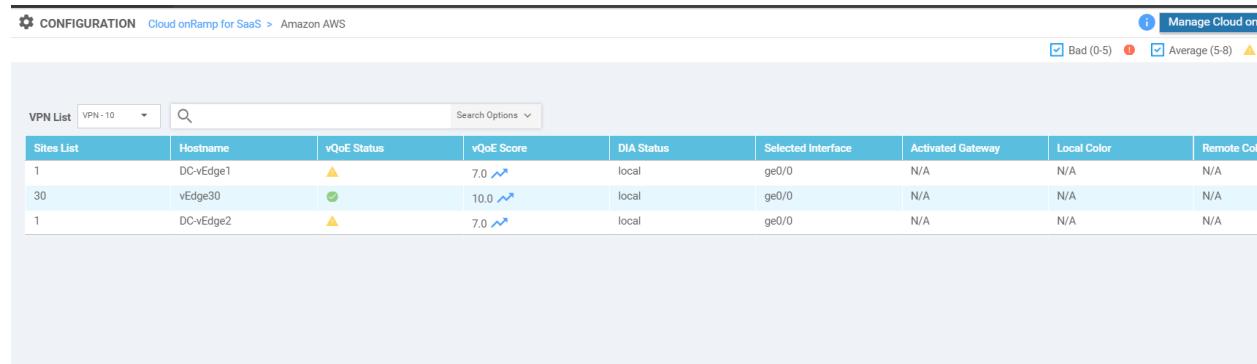
Ingress Policer On Off

Update (highlighted by a red box) Cancel

6. Navigate to **Monitor => Network** and click on **Tunnel**. Make sure all the public-internet Tunnel Endpoints are selected. You should see the latency on the link drop



7. Cloud OnRamp for SaaS takes a few minutes to converge, so monitor the **Cloud icon => Cloud onRamp for SaaS => Application** page - in time, you should see vEdge30 sending data via the local internet breakout



CONFIGURATION Cloud onRamp for SaaS > Amazon AWS

Manage Cloud onRamp for SaaS

Bad (0-5) Average (5-8) Good (8-10)

VPN List VPN - 10 Search Options Total Rows: 3

| Sites List | Hostname | vQoE Status | vQoE Score | DIA Status | Selected Interface | Activated Gateway | Local Color | Remote Color |
|------------|-----------|--------------------------------------|--|------------|--------------------|-------------------|-------------|--------------|
| 1 | DC-vEdge1 | ✓ | 10.0 ↗ | local | ge0/0 | N/A | N/A | N/A |
| 30 | vEdge30 | ✓ | 10.0 ↗ | local | ge0/0 | N/A | N/A | N/A |
| 1 | DC-vEdge2 | ✓ | 10.0 ↗ | local | ge0/0 | N/A | N/A | N/A |

This completes the Cloud OnRamp for SaaS lab.

Task List

- [Overview](#)
- [Prerequisite configuration for Cloud OnRamp](#)
- [Configuring Cloud OnRamp for SaaS](#)
- [Verification and Testing](#)

©2020 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: June 3, 2020

Site last generated: Sep 1, 2020

