

-->

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):

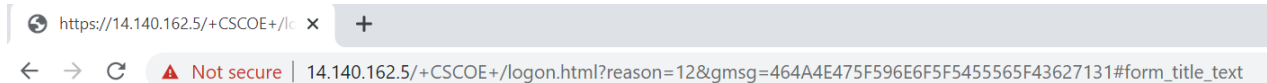
- The Data Center (SLC or GHI) your POD is scheduled on and the POD number, along with the group
- VPN Credentials and connection information
- IP Address of the Jumphost/Guacamole

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

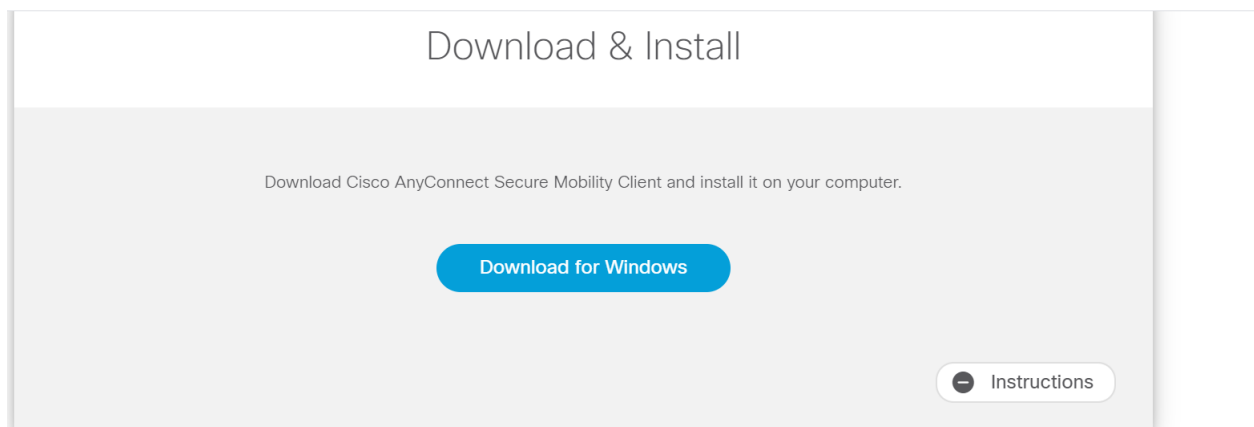
Downloading and Installing Cisco AnyConnect

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

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

A screenshot of a web-based logon form. The form has a title bar that says 'Logon'. Below the title bar, there are three input fields: 'Group' with a dropdown menu showing 'SWAT_Lab_GHI_Pod1', 'Username' with the text 'testuser', and 'Password' with a masked password field. Below these fields is a button labeled 'Logon'.

2. 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



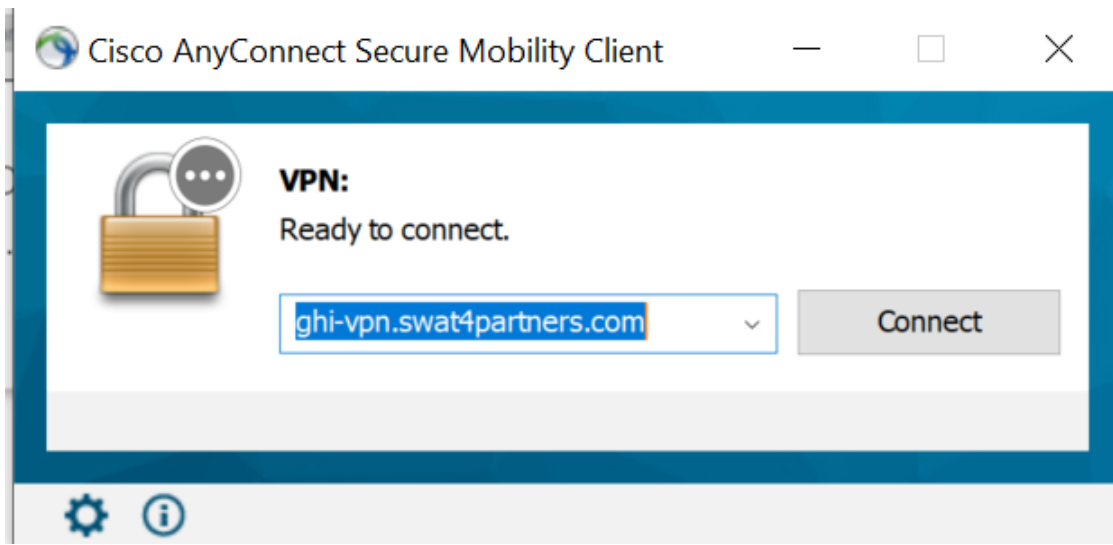
INSTRUCTIONS



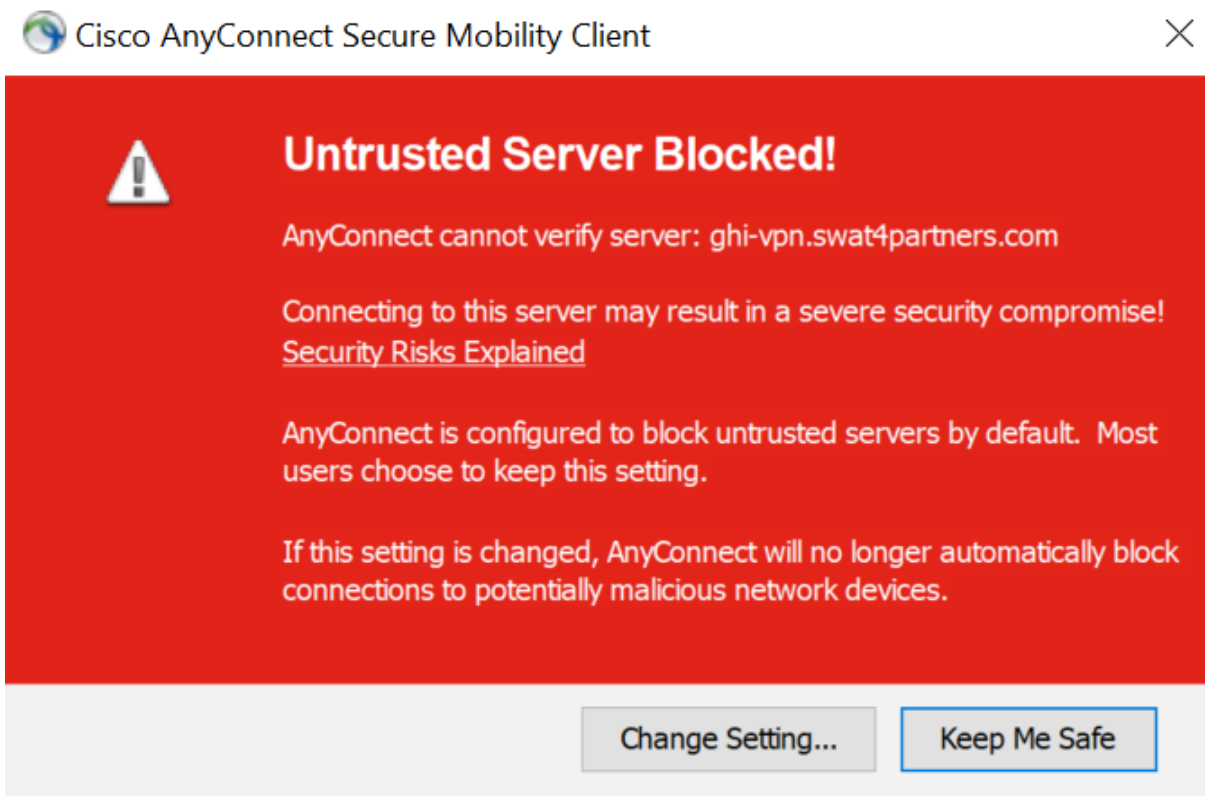
Install AnyConnect and move on to the **Connect to the Cisco SWAT SD-WAN Labs** section.

Connect to the Cisco SWAT SD-WAN Labs

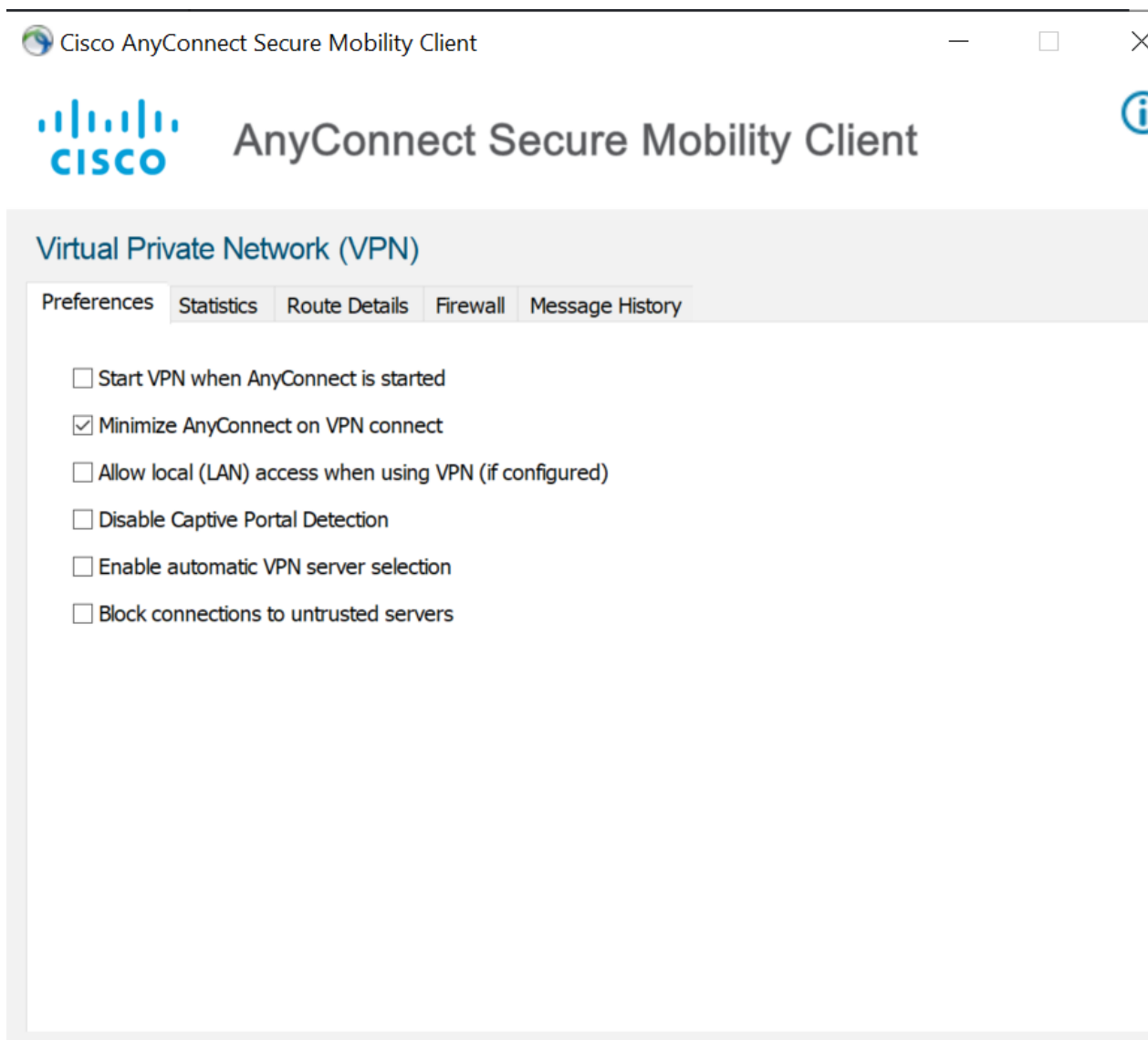
1. Once AnyConnect is installed, enter the destination URL provided to you in the email or by the SWAT contact and click on **Connect**



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!

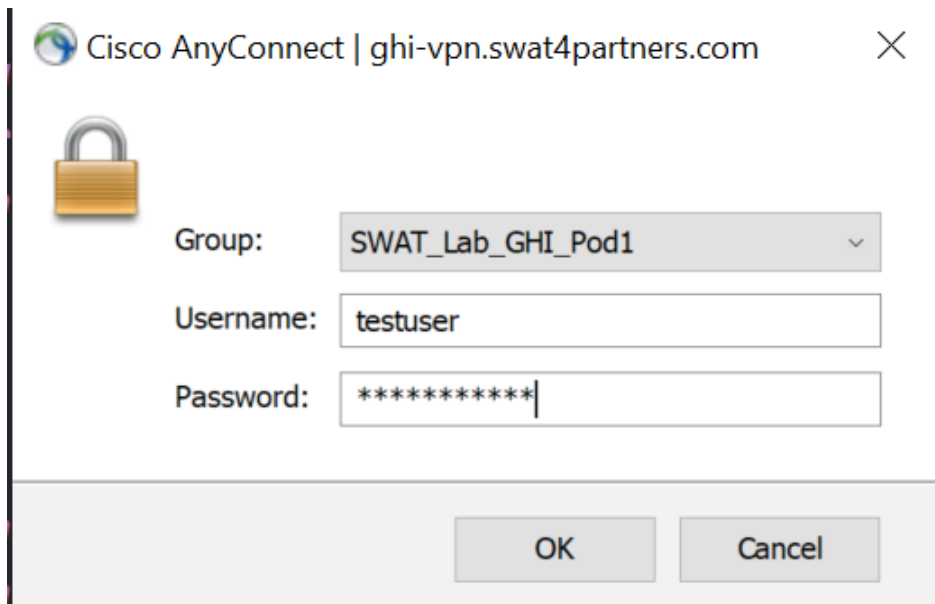
[Security Risks Explained](#)

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

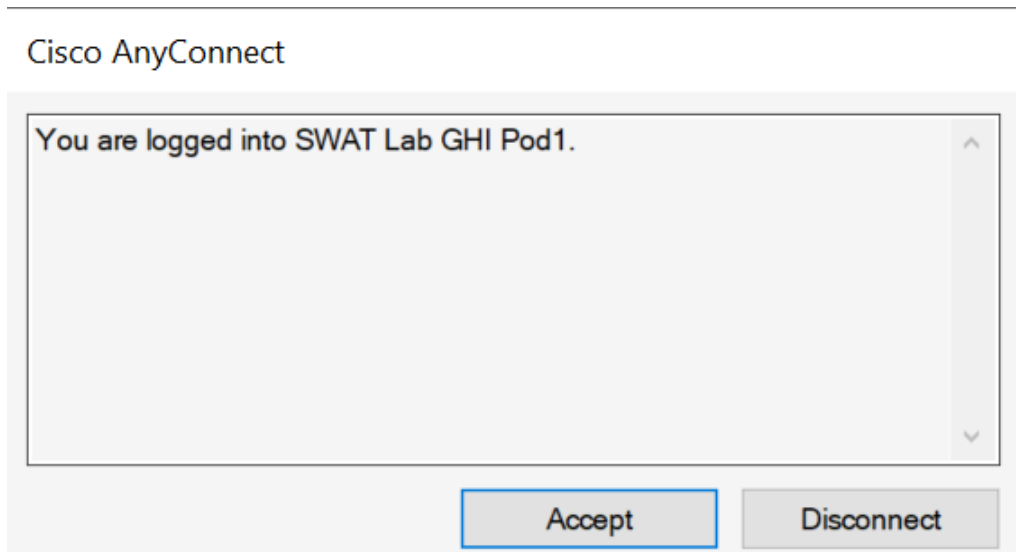
Connect Anyway

Cancel Connection

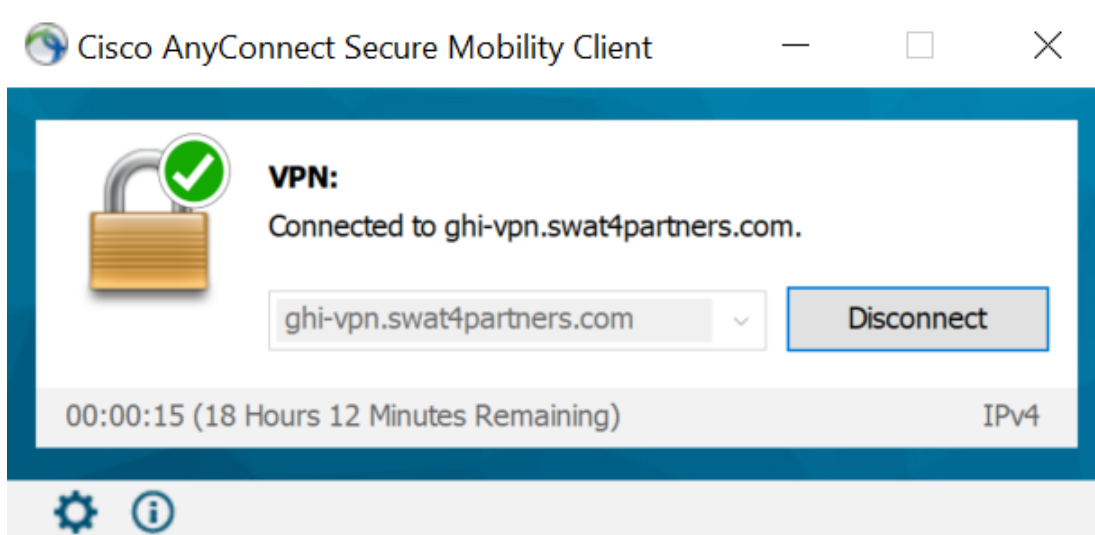
6. You should be prompted for your username/password and provided with a drop down to select a Group. Please make sure you choose the correct Group as per your POD and enter the VPN credentials provided for your POD. Click on **OK**



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

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

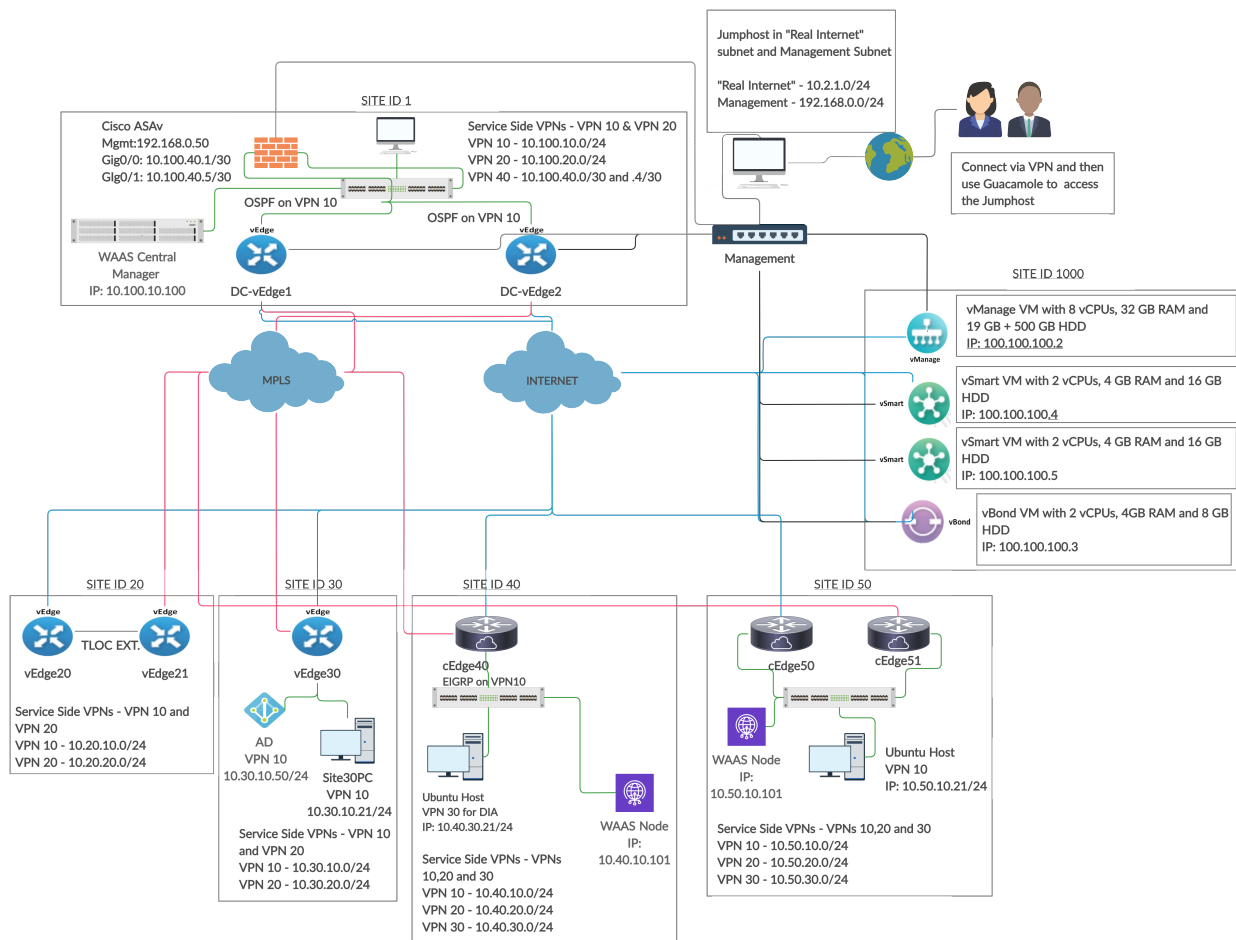
Table of Contents

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

Lab Topology

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

 **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 X is your POD number <i>e.g. sdwanpod5</i>	C1sco12345	10.2.1.50
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	sdwanpod	C1sco12345	10.2.1.20X:8080/guacamole X is your POD number
WAAS Central Manager	Browser - GUI	admin	default	10.100.10.100

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	Interface	IP	Gateway
A vManage	1000	10.255.255.1	sdwan-slc/ghi-	Network Adapter 1	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 cEdge50	50	10.255.255.51	cEdge50- podX	Network Adapter 1	Management	GigabitEthernet1	192.168.0.50/24	192.168.0.1
K cEdge50				Network Adapter 2	Internet	GigabitEthernet2	100.100.100.50/24	100.100.100.1
K cEdge50				Network Adapter 3	Site50-VPN10	GigabitEthernet3	10.50.10.2/24	
K cEdge50				Network Adapter 4	Site50-VPN20	GigabitEthernet4	10.50.20.2/24	
K cEdge50				Network Adapter 5	Site50-VPN30	GigabitEthernet5	10.50.30.2/24	
L cEdge51		10.255.255.52	cEdge51- podX	Network Adapter 1	Management	GigabitEthernet1	192.168.0.51/24	192.168.0.1
L cEdge51				Network Adapter 2	MPLS50	GigabitEthernet2	192.1.2.22/30	192.1.2.21
L cEdge51				Network Adapter 3	Site50-VPN10	GigabitEthernet3	10.50.10.3/24	
L cEdge51				Network Adapter 4	Site50-VPN20	GigabitEthernet4	10.50.20.3/24	
L cEdge51				Network Adapter 5	Site50-VPN30	GigabitEthernet5	10.50.30.3/24	
M	NA	NA	sdwan-	Network	SiteDC_VPN10	Virtual 1/0	10.100.10.100/24	10.100.10.2

WAAS Central Manager			slc/ghi-wcm-podX	Adapter 1				
N WAAS Node Site 40			sdwan-slc/ghi-site40waas-podX	Network Adapter 1	Site40-VPN10	Virtual 1/0	10.40.10.101/24	10.40.10.2
O WAAS Node Site 50			sdwan-slc/ghi-site50waas-podX	Network Adapter 1	Site50-VPN10	Virtual 1/0	10.50.10.101/24	10.50.10.2
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	10.2.1.1
Q Guacamole	NA	NA	sdwan-slc/ghi-guac-podX	Network Adapter 1	Shared_Services_VLAN101	eth0	10.2.1.20X/24	10.2.1.1
R Jumphost	NA	NA	sdwan-slc/ghi-jump-podX	Network Adapter 1	Shared_Services_VLAN101	eth0	10.2.1.22X/24	10.2.1.1
S Site 40 PC	40	NA	sdwan-slc/ghi-site40pc-podX	Network Adapter 1	Site40-VPN30	eth0	10.40.30.21/24	10.40.30.2
T Site 50 PC	50	NA	sdwan-slc/ghi-	Network Adapter 1	Site50-VPN10	eth0	10.50.10.21/24	10.50.10.100

			site50pc-podX					
U Site 30 AD	30	NA	sdwan- slc/ghi-ad- podX	Network Adapter 1	Site30-VPN10	eth0	10.30.10.50/24	10.30.10.2
U Site 30 AD				Network Adapter 2	Shared_Services_VLAN101	eth1	10.2.1.18X	
V Site 30 PC	30	NA	sdwan- slc/ghi- site30pc- podX	Network Adapter 1	Site30-VPN10	eth0	10.30.10.21/24	10.30.10.2
V Site 30 PC				Network Adapter 2	Shared_Services_VLAN101	eth1	10.2.1.16X	
W Firewall ASAv	1	NA	sdwan- slc/ghi-asa- podX	Network Adapter 1	Management	Management0/0	192.168.0.50/24	192.168.0.1
W Firewall ASAv				Network Adapter 2	SiteDC-VPN40	Gig0/0	10.100.40.1/30	10.100.40.2
W Firewall ASAv				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 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.

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.

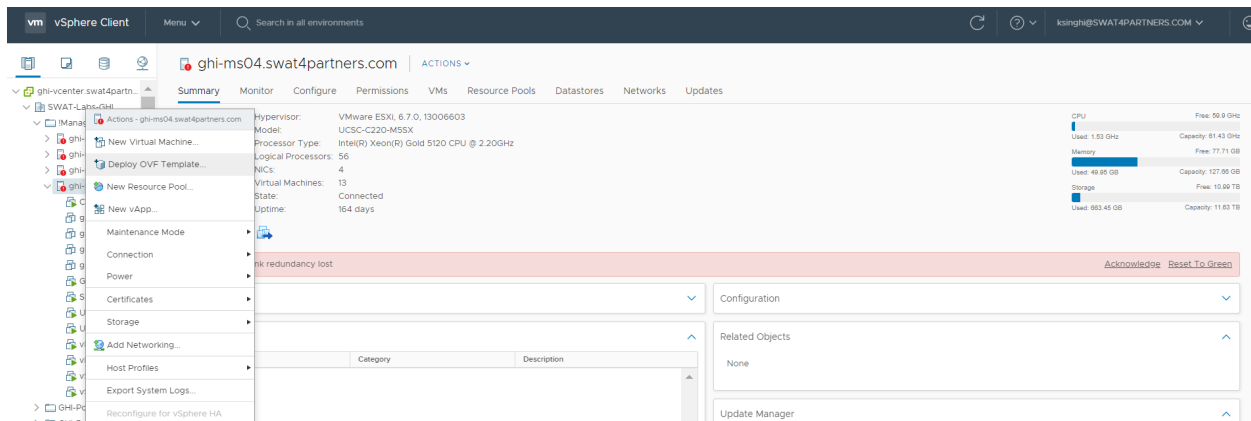
SITE ID	SYSTEM ID	VM	Network Adapter	Network	Interface	IP	Gateway
30	10.255.255.31	vEdge30-podX	Network Adapter 1	Management	eth0	192.168.0.30/24	192.168.0.1
			Network Adapter 2	MPLS30	ge0/1	192.0.2.14/30	192.0.2.13
			Network Adapter 3	Site30-VPN10	ge0/2	10.30.10.2/24	
			Network Adapter 4	Site30-VPN20	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
 - ✓ IManagement-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
- 4 Review details**
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

Review details

Verify the template details.

 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	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


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*

The screenshot shows the 'Edit Settings' window for a virtual machine named 'vEdge30'. The 'Virtual Hardware' tab is active. The settings are as follows:

Component	Value	Unit	Connect
CPU	4		<input checked="" type="checkbox"/>
Memory	2	GB	<input checked="" type="checkbox"/>
Hard disk 1	10.2248783111!	GB	<input checked="" type="checkbox"/>
Network adapter 1	Management		<input checked="" type="checkbox"/>
Network adapter 2	MPLS30		<input checked="" type="checkbox"/>
Network adapter 3	Site30-VPN10		<input checked="" type="checkbox"/>
Network adapter 4	Site30-VPN20		<input checked="" type="checkbox"/>
New Network *	Internet		<input checked="" type="checkbox"/>
CD/DVD drive 1	Host Device		<input type="checkbox"/>
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		

Buttons: ADD NEW DEVICE, CANCEL, 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

i 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

```
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



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 interface. On the left, a navigation menu is open with 'Devices' selected. The main dashboard area displays several health metrics:

- 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:** Shows a table with columns for Tunnel Endpoints and Avg. Latency (ms), but it displays 'No data'.

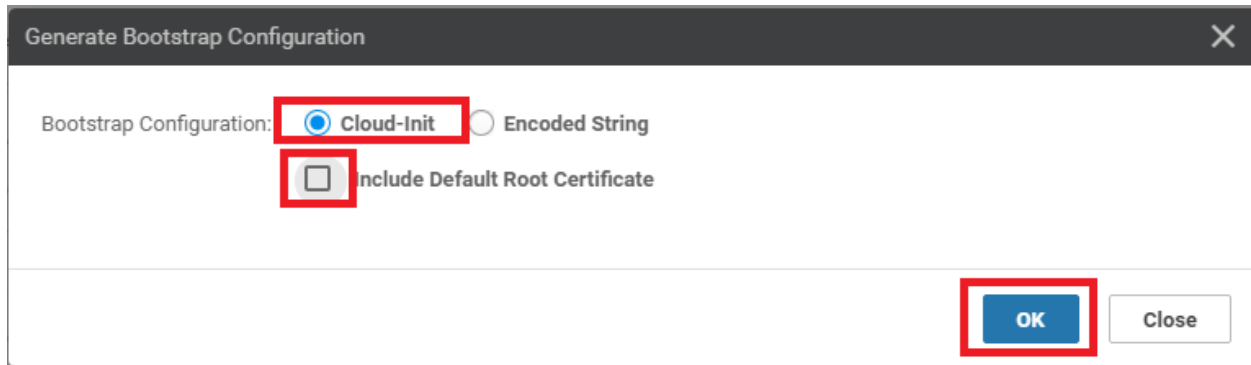
The URL at the bottom of the browser window is: <https://192.168.0.6/index.html#/app/confia/devices/vedae>

- 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

CSR1000v	CSR-04F9482E-44F0-E4DC-D30D-60C0...	Token - 4a6809836f02...	NA	NA	--	--	--	CLI	...
vEdge Cloud	e474c5fd-8ae7-d376-7cae-ba950b2e91...	7175AE0F	NA	NA	DC-vEdge1	10.255.255.11	1	CLI	...
vEdge Cloud	0cdd4f0e-f2f1-fe75-866c-469966da1c3	7DA605F5	NA	NA	DC-vEdge2	10.255.255.12	1	CLI	...
vEdge Cloud	b7fd7295-88df-7671-e914-6fe2edf11609	297060DD	NA	NA	vEdge20	10.255.255.21	20	CLI	...
vEdge Cloud	dde90f0-dc62-77e6-510f-08d96608537d	8BFD4E65	NA	NA	vEdge21	10.255.255.22	20	CLI	...
vEdge Cloud	17026153-109e-be4b-6dce-482fce43aa...	Token - 3692590e4778...	NA	NA	--	--	--	CLI	...
CSR1000v	CSR-26217DA0-1B63-8DDE-11C9-125F...	Token - 8dc7b557b60d...	NA	NA	--	--	--	CLI	...
CSR1000v	CSR-F960E020-B7C9-887F-46A8-F4537...	Token - 50cc04634ac4...	NA	NA	--	--	--	CLI	...
CSR1000v	CSR-25925FBC-07F3-0732-E127-EA95...	Token - 6ced66053d46...	NA	NA	--	--	--	CLI	...
vEdge Cloud	35bd96f9-1758-116c-4e4c-e34c706645...	Token - ed778f56f9ab0...	NA	NA	--	--	--	CLI	...
vEdge Cloud	005c424c-2d57-41fe-250d-ee991e0a4e...	Token - 56f4f54ce614d...	NA	NA	--	--	--	CLI	...
vEdge Cloud	21292349-2e9f-7aaf-28f5-a87e4d0054cb	Token - b6046deef4a2a...	NA	NA	--	--	--	CLI	...

- Running Configuration
- Local Configuration
- Delete WAN Edge
- Copy Configuration
- Generate Bootstrap Configuration
- Template Log
- Device Bring Up

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

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-----
    MIIF7DCCBNsgAwIBAgIQbsx6pacDIAm4zrz06VLUkTANBgkqhkiG9w0BAQUFADCB
    ..EMAlCA1UEBhMCVAMsE-AVBANVBAcTDZlcm1TeWdudCBkcmM6MjR8..HOYDVOOI
```

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/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
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

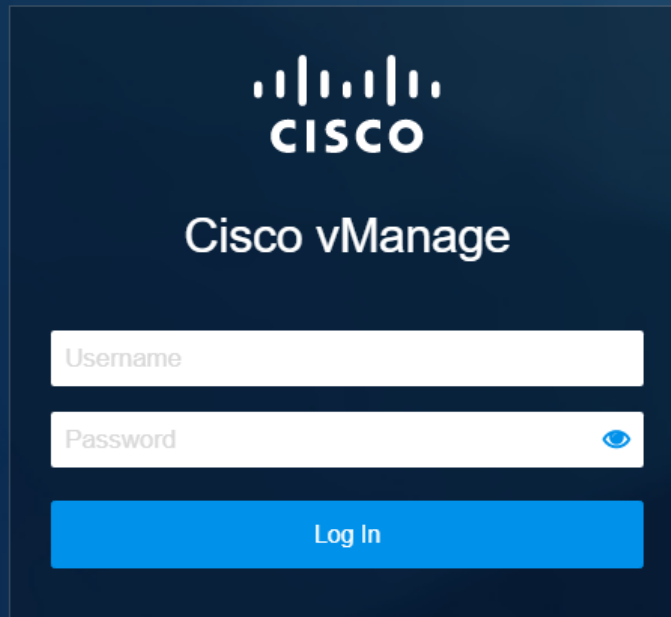
Verifying the existing lab setup

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:

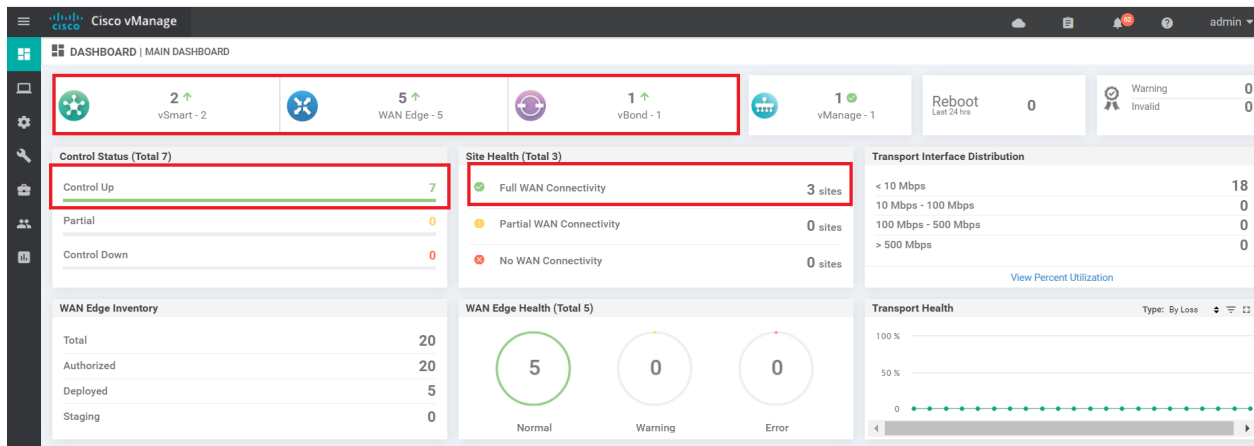
Username	Password
admin	admin

Cisco SD-WAN

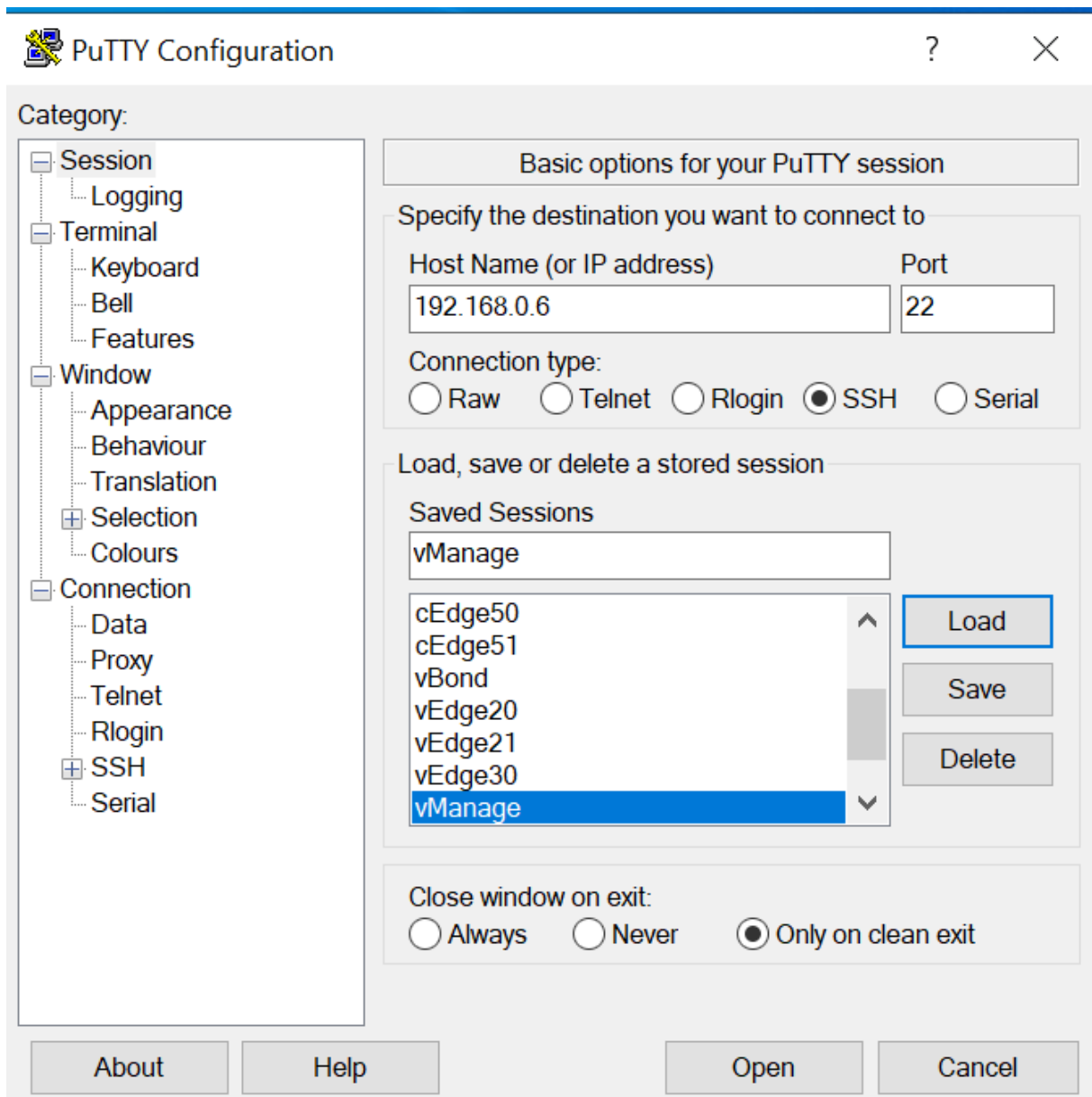


The image shows the Cisco vManage login interface. At the top, the Cisco logo is displayed above the text "Cisco vManage". Below this, there are two input fields: "Username" and "Password". The "Password" field includes a small eye icon to toggle visibility. At the bottom of the form is a blue "Log In" button.

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.



- 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**

```
vmanage# show control connections
PEER
PEER PEER PEER
CONFIGURED SITE DOMAIN PEER
INDEX TYPE PROT SYSTEM IP SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT PUBLIC IP PORT ORGANIZATION RENO
TE COLOR STATE UPTIME
-----
0 vedge dtls 10.255.255.11 10.255.255.11 1 1 100.100.100.10 12366 100.100.100.10 12366 swat-sdwanlab defa
ult up 3:19:16:27
0 vedge dtls 10.255.255.22 10.255.255.22 20 1 192.0.2.10 12366 192.0.2.10 12366 swat-sdwanlab defa
ult up 0:05:31:04
0 vsmart dtls 10.255.255.3 10.255.255.3 1000 1 100.100.100.4 12346 100.100.100.4 12346 swat-sdwanlab defa
ult up 6:17:46:09
0 vsmart dtls 10.255.255.4 10.255.255.4 1000 1 100.100.100.5 12346 100.100.100.5 12346 swat-sdwanlab defa
ult up 6:17:46:09
0 vbond dtls 10.255.255.2 10.255.255.2 0 0 100.100.100.3 12346 100.100.100.3 12346 swat-sdwanlab defa
ult up 6:17:46:10
1 vedge dtls 10.255.255.12 10.255.255.12 1 1 100.100.100.11 12366 100.100.100.11 12366 swat-sdwanlab defa
ult up 1:16:11:09
1 vedge dtls 10.255.255.21 10.255.255.21 20 1 100.100.100.20 12366 100.100.100.20 12366 swat-sdwanlab defa
ult up 0:22:34:42
1 vedge dtls 10.255.255.31 10.255.255.31 30 1 100.100.100.30 12366 100.100.100.30 12366 swat-sdwanlab defa
ult up 0:03:13:01
1 vbond dtls 0.0.0.0 - 0 0 100.100.100.3 12346 100.100.100.3 12346 swat-sdwanlab defa
ult up 6:17:46:10
```

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 ID	SYSTEM ID	VM	Network Adapter	Network	Interface	IP	Gateway
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.

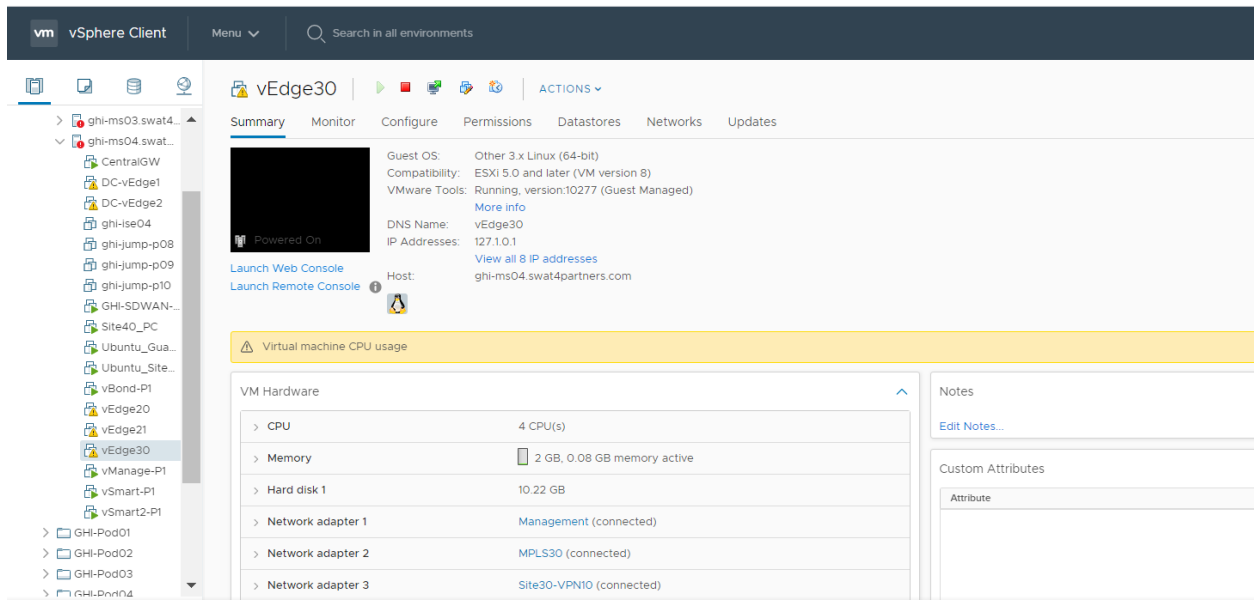
Tip: There is configuration applicable only to virtual vEdges/cEdges in some of the sections. Physical cEdges/vEdges are a lot easier to deploy, not only from a connectivity standpoint but also with respect to certificate exchange options.

Deploying the VM on vCenter

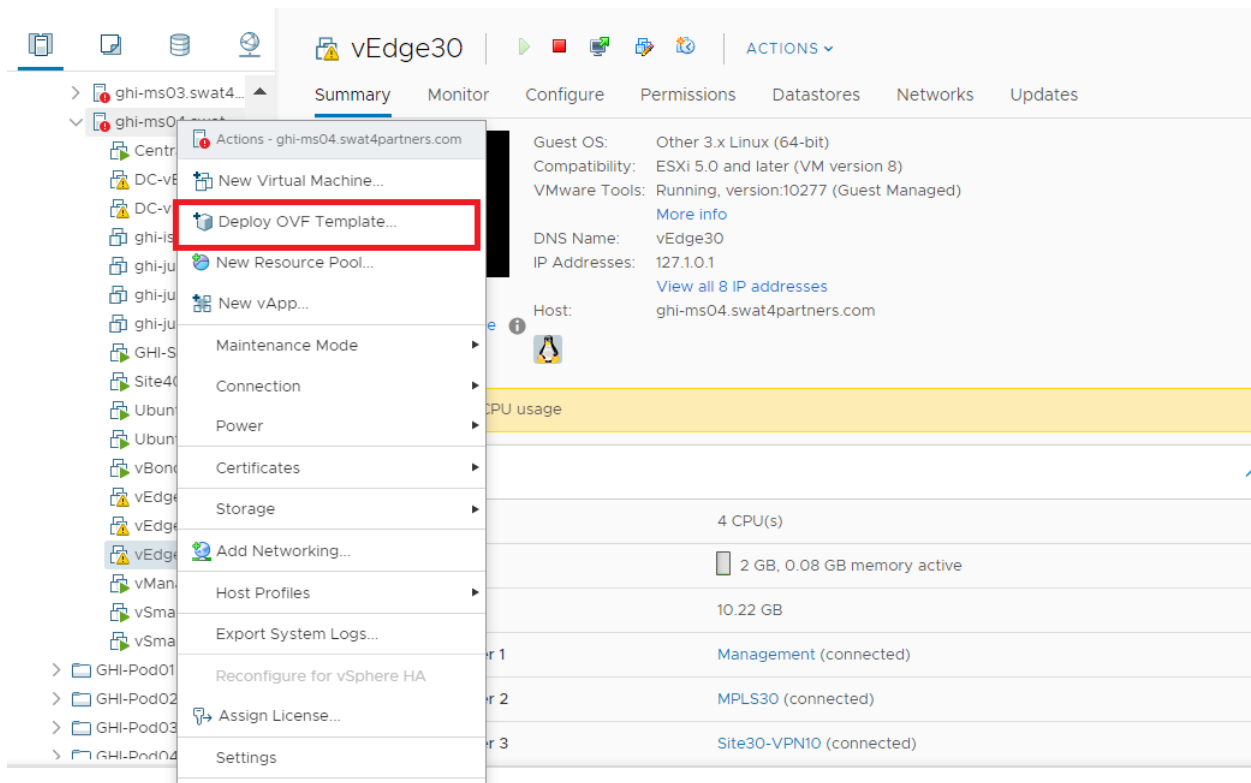
1. Click on the bookmark for vCenter or navigate to the following URL: <https://10.2.1.50/ui>. Log in with the credentials provided for your POD.



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



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

Choose Files

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)

i 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.

- ghl-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
 - ✓ IManagement-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
- 4 Review details**
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Review details

Verify the template details.

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 Large hardware profile - 4 vCPUs, 4 GB RAM
<input type="radio"/> Medium	
<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 ₁
 ghl-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 ✕

1. Bootstrap Properties		13 settings
Router Name	Hostname of this router	<input type="text"/>
Login Username	Username for remote login	<input type="text"/>
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	<input type="password"/>
	Confirm Password	<input type="password"/>
Domain Name	Network domain name (such as "cisco.com")	<input type="text"/>

[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.

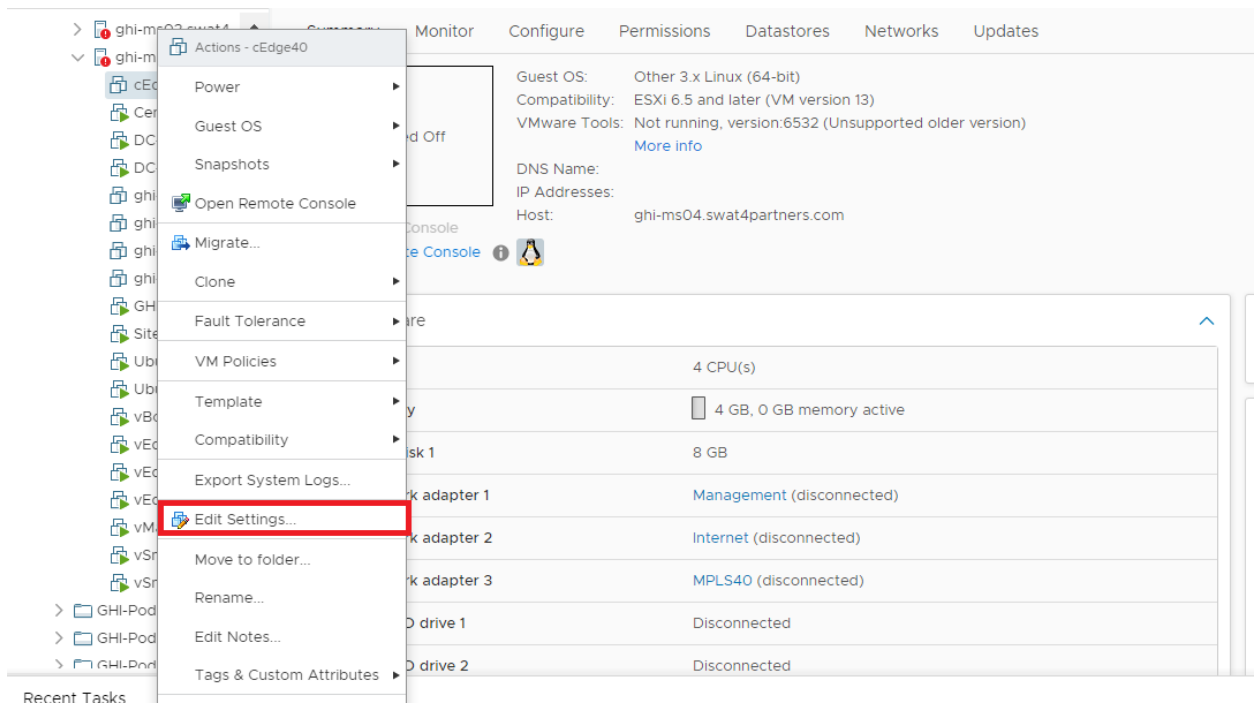
Provisioning type	Deploy from template
Name	cEdge40
Template name	csr1000v-universalk9.17.02.01r-vga
Download size	510.2 MB
Size on disk	8.5 GB
Folder	SWAT-Labs-GHI
Resource	ghi-ms04.swat4partners.com
Storage mapping	1
All disks	Datastore: ghi-ms04-ds; Format: Thick provision lazy zeroed
Network mapping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

CANCEL

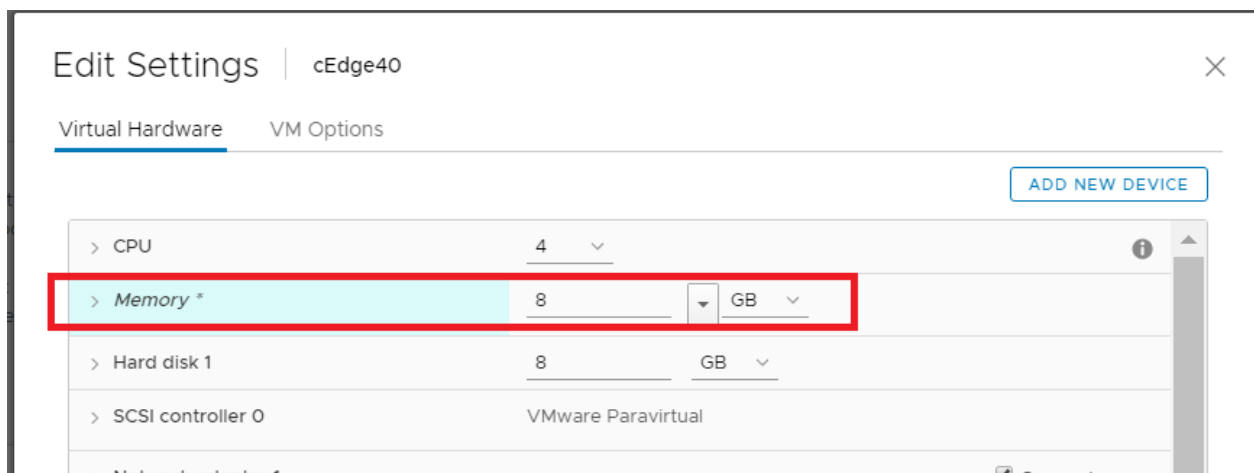
BACK

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



Virtual Hardware | VM Options

ADD NEW DEVICE

- 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

	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

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		<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 *	Internet		<input checked="" type="checkbox"/> Connect...
> New Network *	Internet		<input checked="" type="checkbox"/> Connect...
> New Network *	Internet		<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

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

ADD NEW DEVICE

> CPU	4		
> Memory *	8	GB	
> Hard disk 1	8	GB	
> 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 *	Internet		<input checked="" type="checkbox"/> Connect... (X)
> New Network *	Browse ...		<input checked="" type="checkbox"/> Connect...
> New Network *	Internet		<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

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

ADD NEW DEVICE

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

Select Network

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

ADD NEW DEVICE

> CPU	4		
> Memory *	8	GB	
> Hard disk 1	8	GB	
> 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	Interface	IP	Gateway
40	10.255.255.41	cEdge40	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	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 Jumpshot. 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)#
```

```
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

```
Router(config)#do ping 192.168.0.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.6, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#do ping 192.168.0.121
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.121, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
Router(config)#
```

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

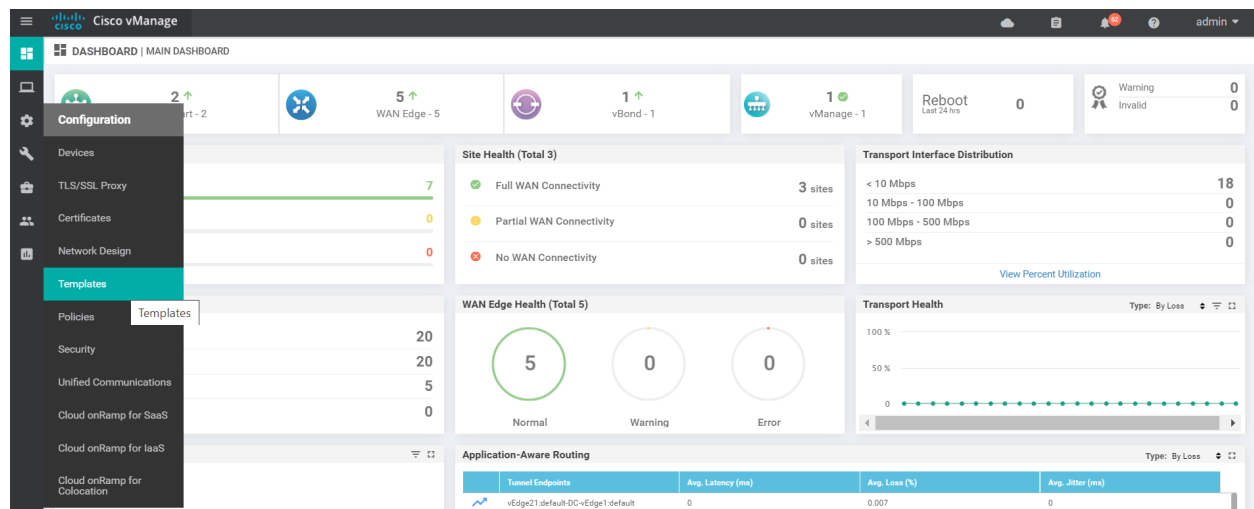
Setting up Feature Templates

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.

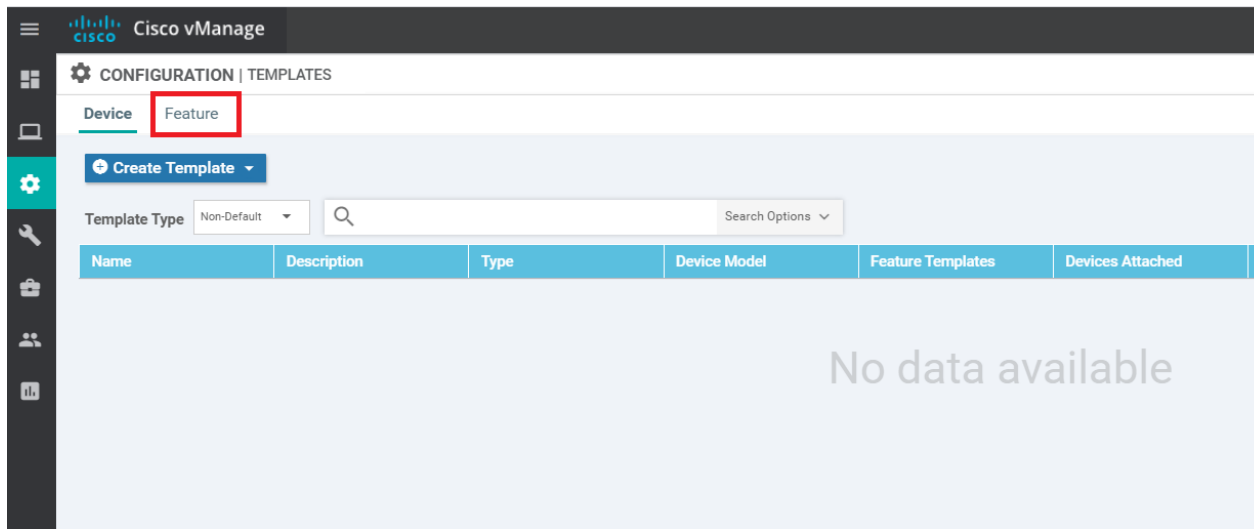
Templates are the key configuration components of the Cisco SD-WAN solution. They help with deploying large scale solutions with minimal effort. While there is quite a lot of initial configuration that goes into setting up these templates, their usefulness is highlighted when we're looking at onboarding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

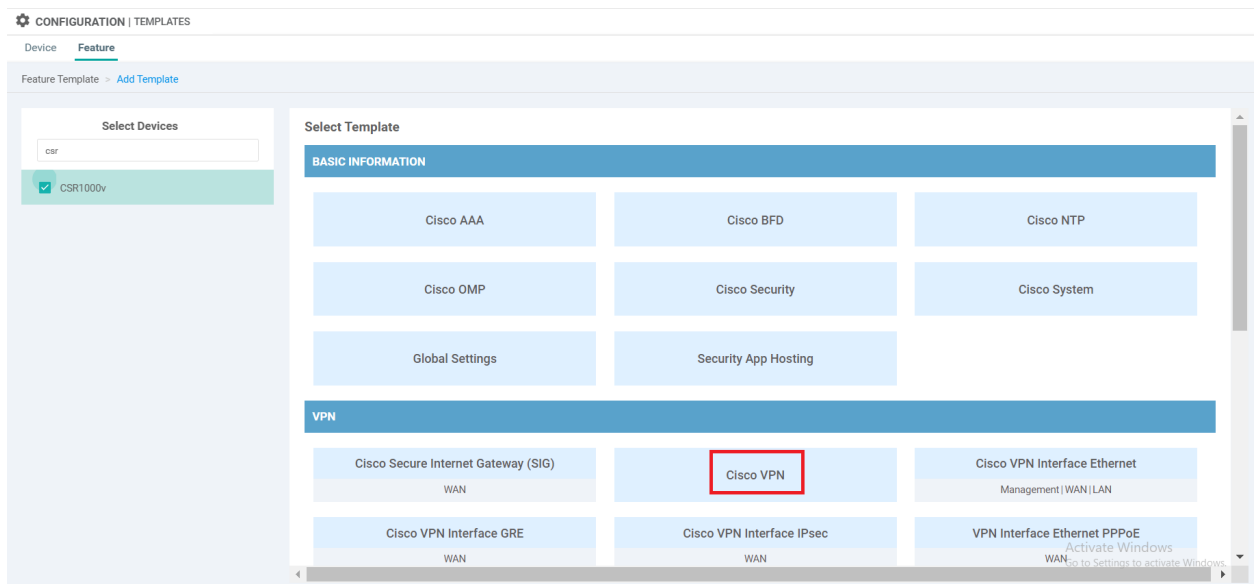
1. On the vManage GUI, navigate to **Configuration (the cog wheel icon on the left) => Templates**



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



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



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.

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Add Template > Cisco VPN

Device Type: CSR1000v

Template Name: cEdge_VPN0_dual_uplink

Description: cEdge VPN 0 Template for Dual Uplink

Basic Configuration | DNS | Advertise OMP | IPv4 Route | IPv6 Route | Service | Service Route | GRE Route | IPSEC Route | NAT

BASIC CONFIGURATION

VPN: 0

Name: [dropdown]

Enhance ECMP Keying: [dropdown] On Off

DNS

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

IPv4 ROUTE

New IPv4 Route

Optional	Prefix	Gateway	Selected Gateway Configuration	Action
No data available				

IPv6 ROUTE

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)

IPv4 ROUTE

New IPv4 Route

Mark as Optional Row

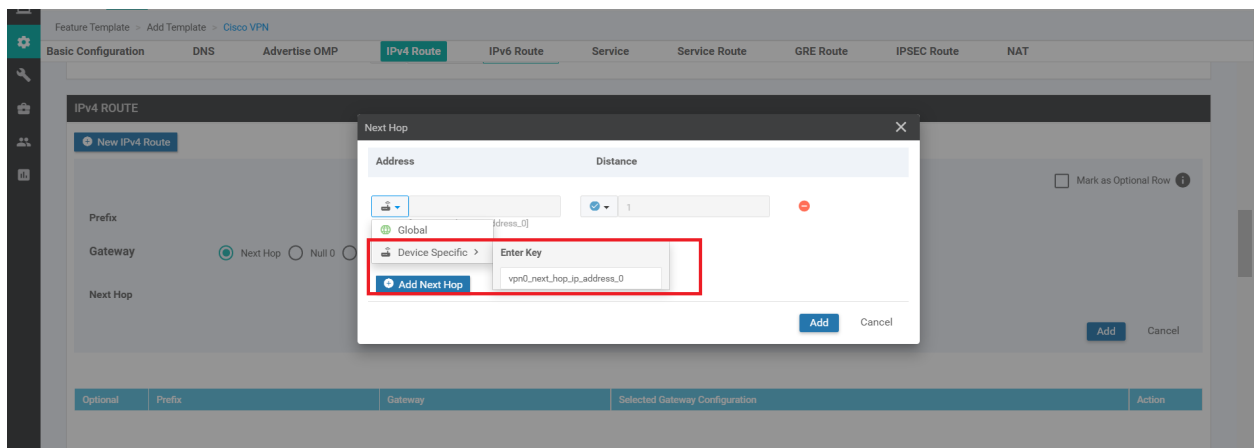
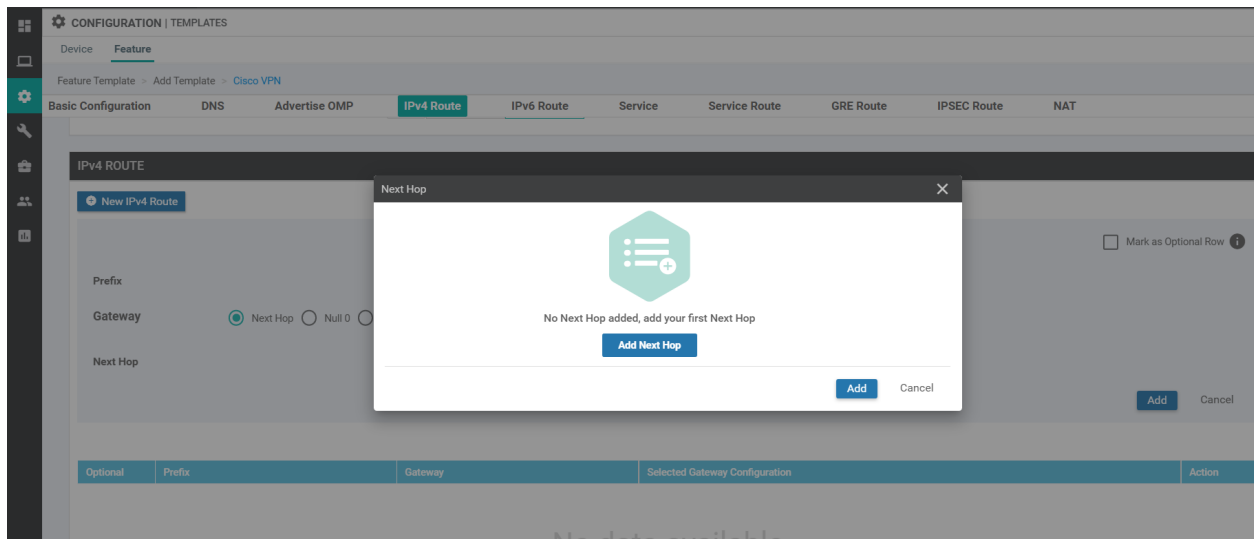
Prefix: 0.0.0.0/0

Gateway: Next Hop Null 0 VPN DHCP

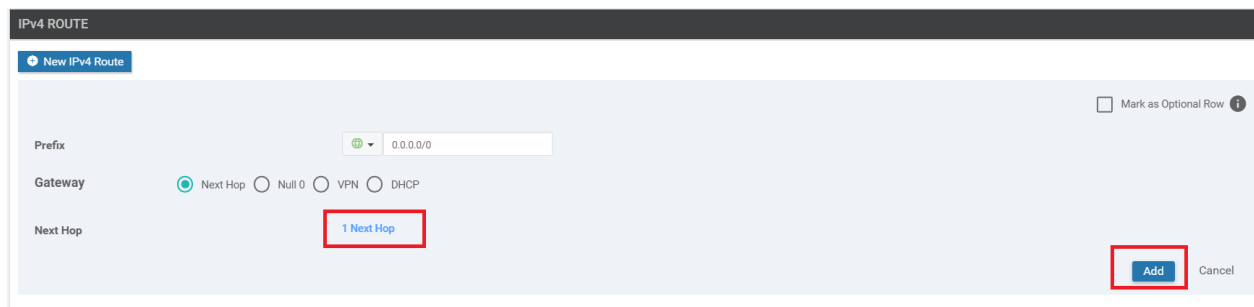
Next Hop: **Add Next Hop**

Add Cancel

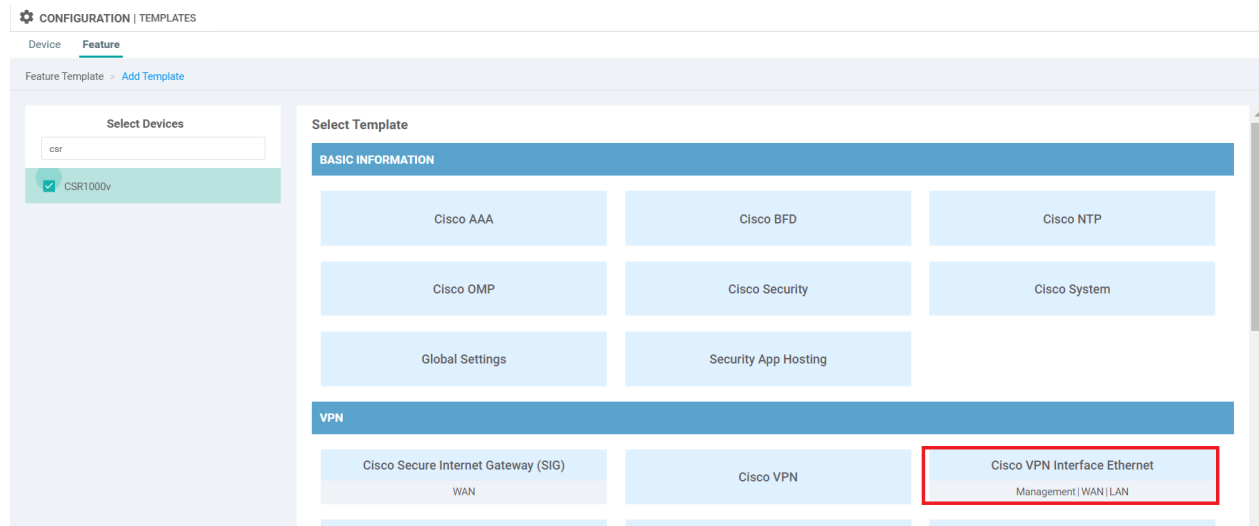
7. Click on **Add Next Hop** again and choose **Device Specific** from the Address drop down. Enter *vpn0_next_hop_ip_address_0*. Click on Add.



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	<i>inet_if_tunnel_color_value</i>
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): [+ Add](#)

DHCP Helper:

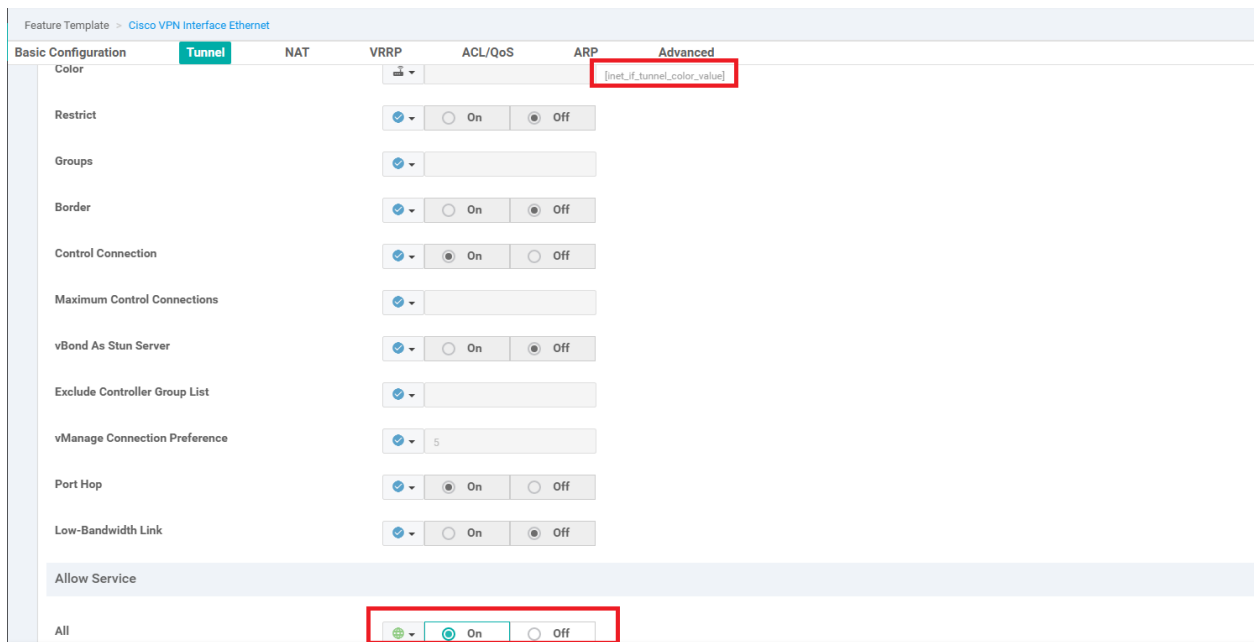
Block Non Source IP: Yes No

Bandwidth Upstream:

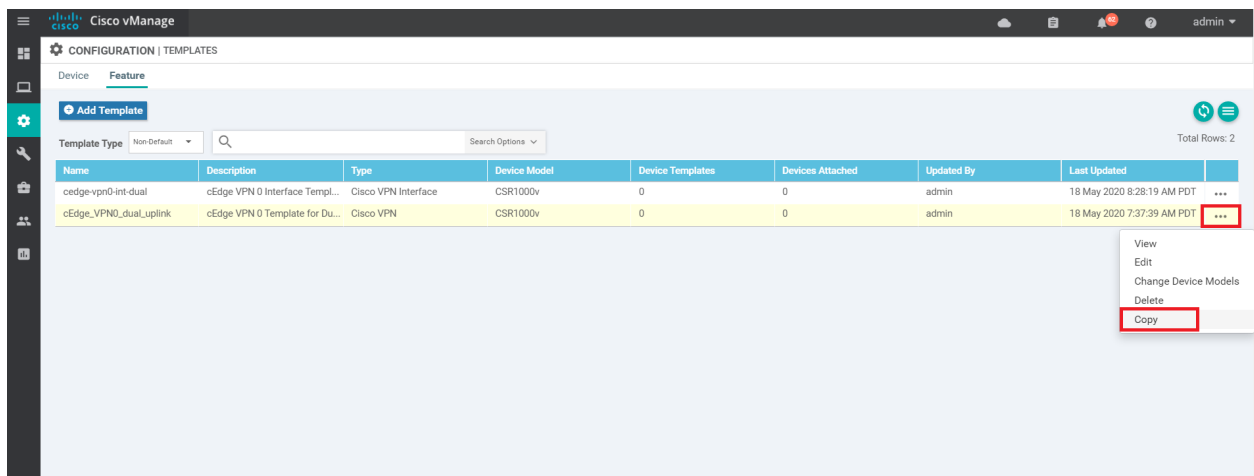
Bandwidth Downstream:

TUNNEL

Tunnel Interface: On Off



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**



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

Description

cEdge VPN 512 Template for Dual Uplinks

- 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 8:2...	

- 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	<i>cEdge_VPN512_dual_uplink</i>
	Description	NA	cEdge VPN 512 Template for Dual Uplinks
Basic Configuration	VPN	Global	512
IPv4 Route	Update IPv4 Route - Next Hop	Device Specific	<i>vpn512_next_hop_ip_address_0</i>

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Cisco VPN

Device Type: CSR1000v

Template Name:

Description:

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

DNS

Primary DNS Address (IPv4):

New IPv4 Route

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

Update IPv4 Route

Prefix: Mark as Optional Row

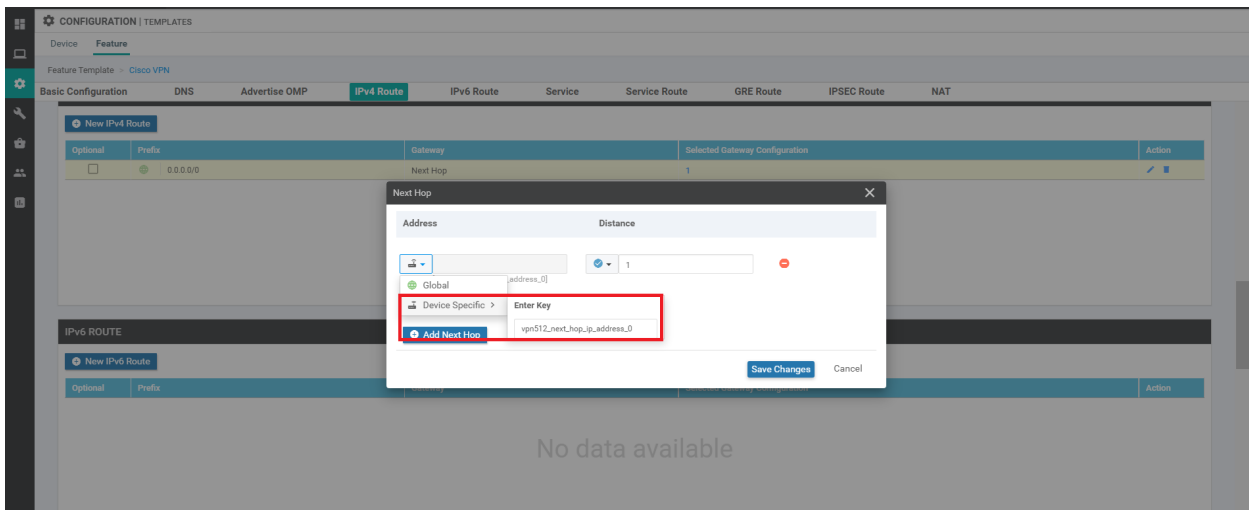
Gateway: Next Hop Null 0 VPN DHCP

Next Hop: [1 Next Hop](#)

IPv6 ROUTE

New IPv6 Route

Optional	Prefix	Gateway	Selected Gateway Configuration	Action
No data available				



- 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**

Template Copy ✕

Template Name

Description

- 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	<i>cedge-vpn512-int-dual</i>
	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	<i>vpn512_mgmt_ipv4_address</i>
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 | Tunnel | NAT | VRRP | ACL/QoS | ARP | Advanced

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: GigabitEthernet1

Description: [Empty]

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.

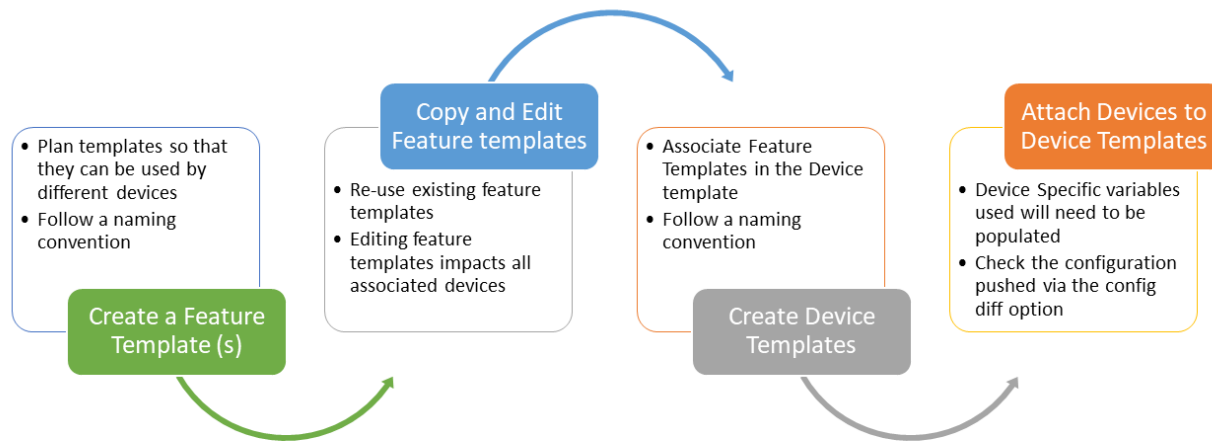
Task List

- ~~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

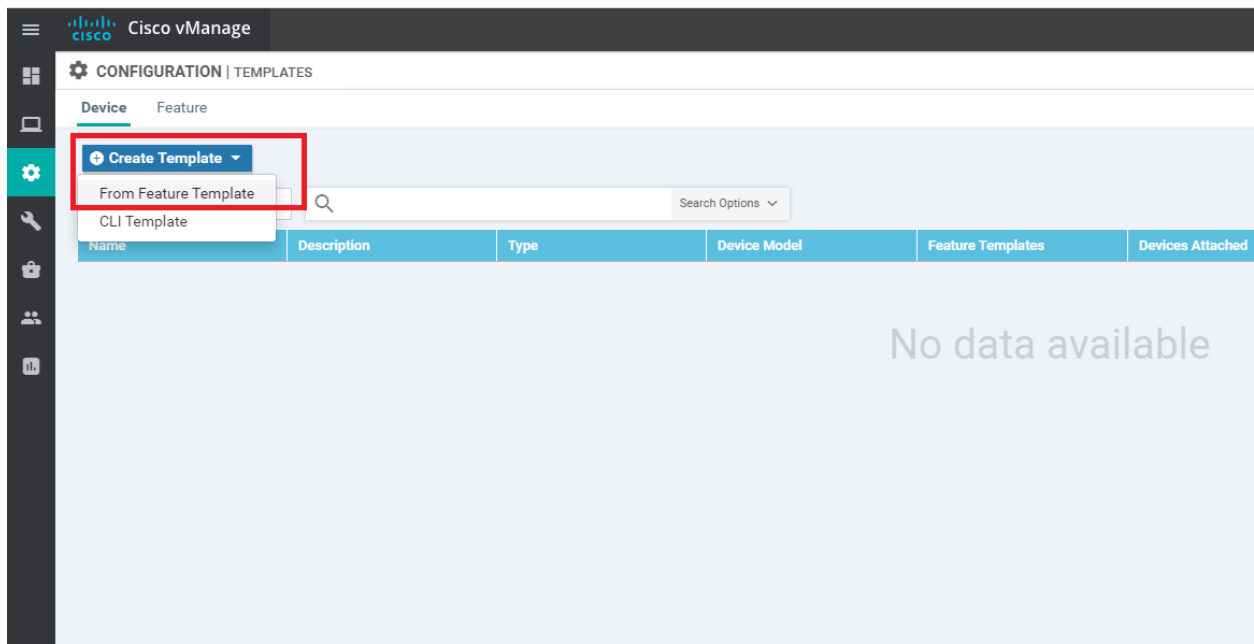
Creating and Attaching Device Templates

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

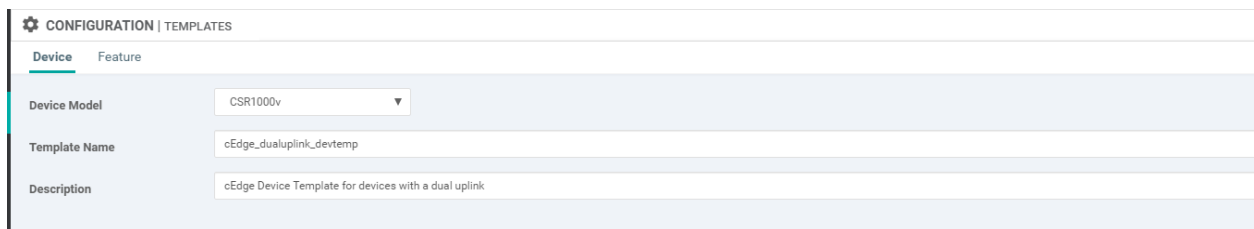
workflow for templates is given below



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



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**



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 *

Cisco VPN Interface Ethernet ⌵

Cisco VPN 512 *

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) and click on **Attach Devices**

Create Template ▾

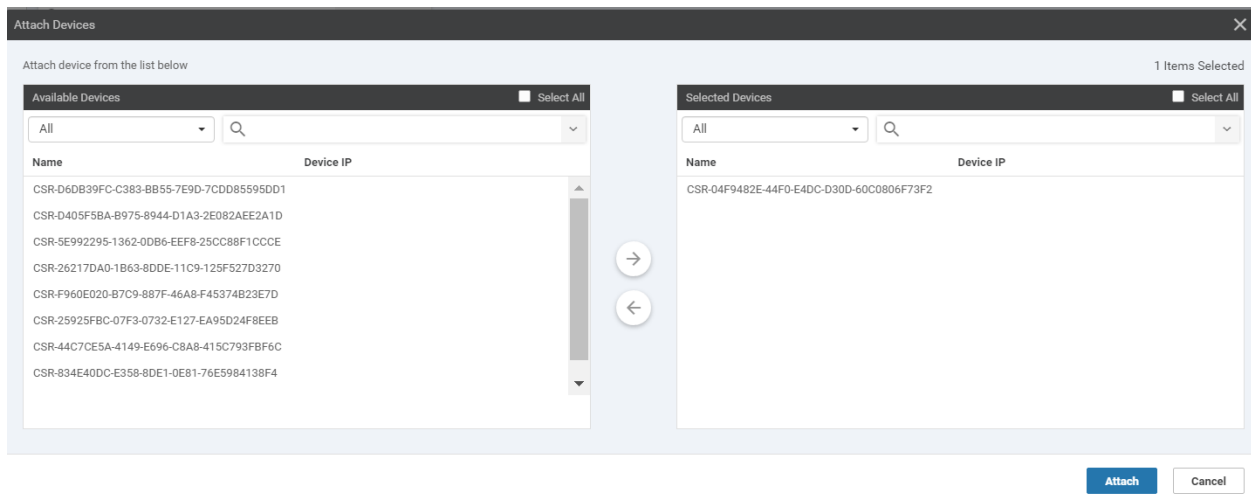
Template Type: Non-Default 🔍 Search Options ▾ Total Rows: 1

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	⋮

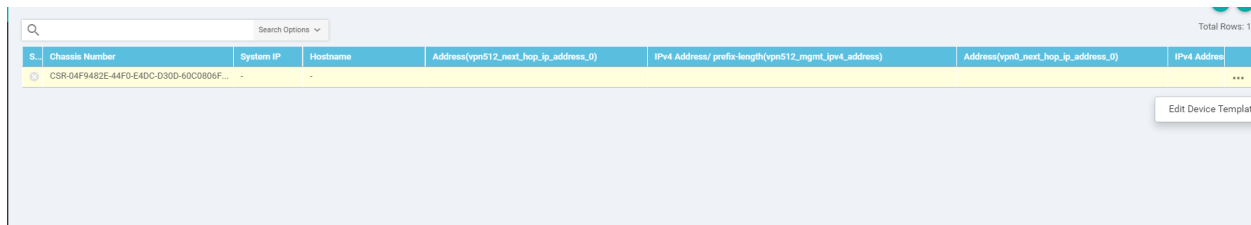
⋮

- Edit
- View
- Delete
- Copy
- Attach Devices**
- Export CSV

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.



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.

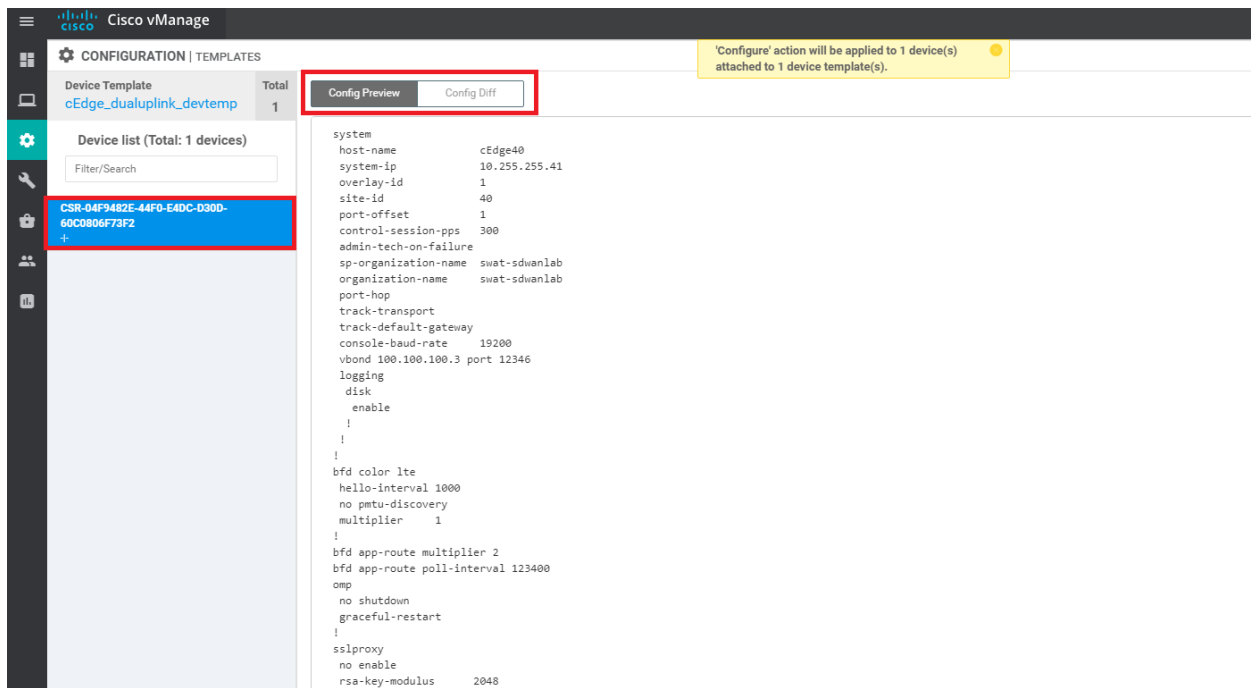
Update Device Template✕

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 PasswordUpdateCancel

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.



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 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

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 left sidebar contains a navigation menu with options: Configuration, Devices, 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 main content area shows a task view for 'Push Feature Template Configuration' with a 'Validation Success' status. Below this, a table displays device information:

Message	Chassis Number	Device Model	Hostname
Device became unreachable. Con...	CSR-04F9482E-44F0-E4DC-D30D-...	CSR1000v	

2. 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	
🔍	CSR1000v	CSR-44C7CESA-4149-E696-CBA8-415C793FBF6C	Token - fc40de6570e72...	NA	NA	--	--	--	CLI	...
🔍	CSR1000v	CSR-D6DB39FC-C383-BB55-7E9D-7CDD85595DD1	Token - f2B5ab97898...	NA	NA	--	--	--	CLI	...
🔍	CSR1000v	CSR-834E4DDC-E358-8DE1-0E81-76E5984138F4	Token - b8a9caee09c9...	NA	NA	--	--	--	CLI	...
🔍	CSR1000v	CSR-D40F5BA-8975-8944-D1A3-2E02AEE2A1D	Token - e78aaefc1ebd2...	NA	NA	--	--	--	CLI	...
🔍	CSR1000v	CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3	Token - 90ffdf29997f98...	NA	NA	--	--	--	CLI	...
🔍	CSR1000v	CSR-8E992295-1362-0DB6-EEF8-25CC88F1CCCE	Token - 1da14330e171...	NA	NA	--	--	--	CLI	...
🔍	CSR1000v	CSR-04F9482E-44FD-E4DC-D3DD-60CC0806F3F2	Token - 4a6809836f02...	NA	NA	--	--	--	vManage	...
🔍	vEdge Cloud	e474c5f5-8ce7-4376-7cac-ba950b2c9159	7175AE0F	NA	NA	DC-vEdge1	10.255.255.11			
🔍	vEdge Cloud	0cdd4f0e-f2f1-f675-866c-469966cda1c3	7DA603F5	NA	NA	DC-vEdge2	10.255.255.12			
🔍	vEdge Cloud	b7fd7295-58df-7671-e914-6fe2edff1609	297060DD	NA	NA	vEdge20	10.255.255.21			
🔍	vEdge Cloud	dde90ff0-dc62-77e6-510f-08d96608537d	88FD4E55	NA	NA	vEdge21	10.255.255.22			
🔍	vEdge Cloud	17026153-f09e-be4b-6dce-482fce43aab2	24715073	NA	NA	vEdge30	10.255.255.31			
🔍	CSR1000v	CSR-26217DA0-1B63-8DDE-11C9-125F527D3270	Token - 8dc7b557b60d...	NA	NA	--	--	--		
🔍	CSR1000v	CSR-F960E020-87C9-887F-46A8-F45374B23E7D	Token - 50cc04634ac4...	NA	NA	--	--	--		
🔍	CSR1000v	CSR-25925FBC-07F3-0732-E127-EA95D24F8EEB	Token - 6ced66053d46...	NA	NA	--	--	--	CLI	...

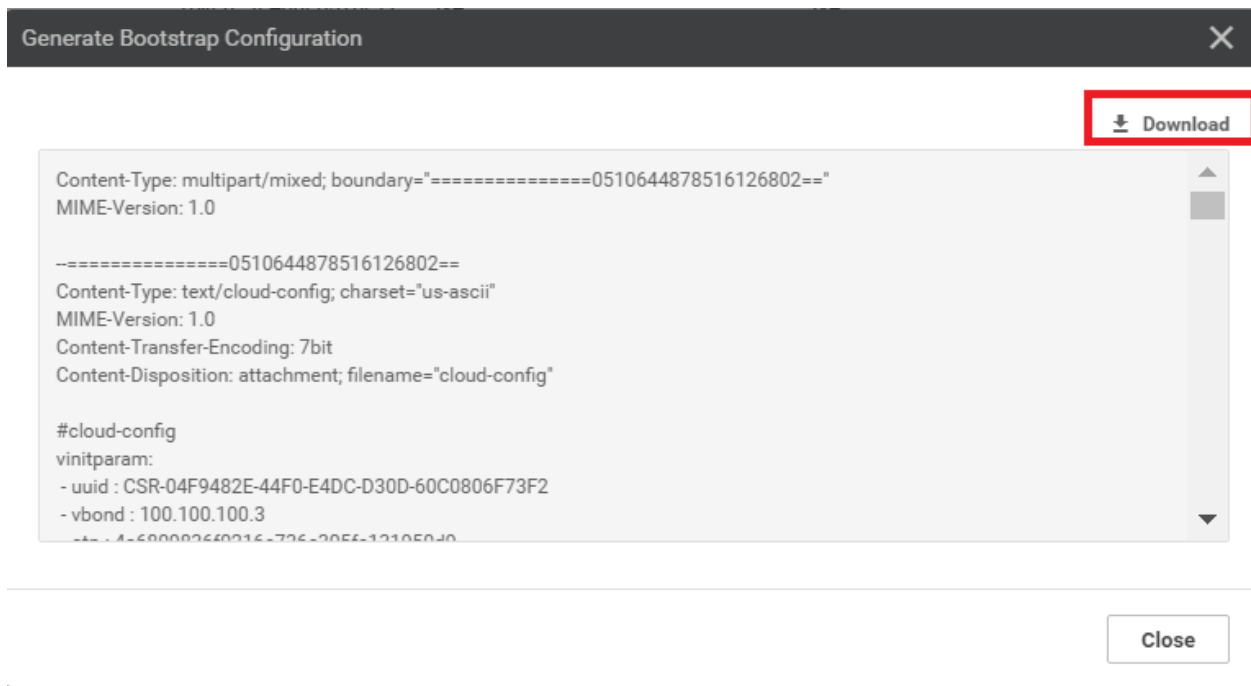
- Running Configuration
- Local Configuration
- Delete WAN Edge
- Generate Bootstrap Configuration
- Change Device Values
- Template Log
- Device Bring Up

Generate Bootstrap Configuration ✕

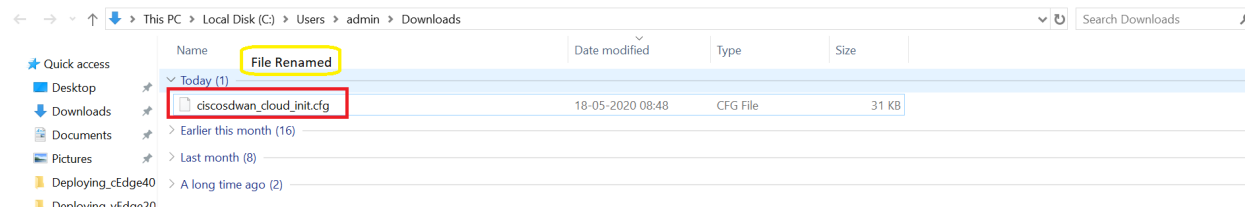
Bootstrap Configuration: **Cloud-Init** Encoded String

Include Default Root Certificate

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

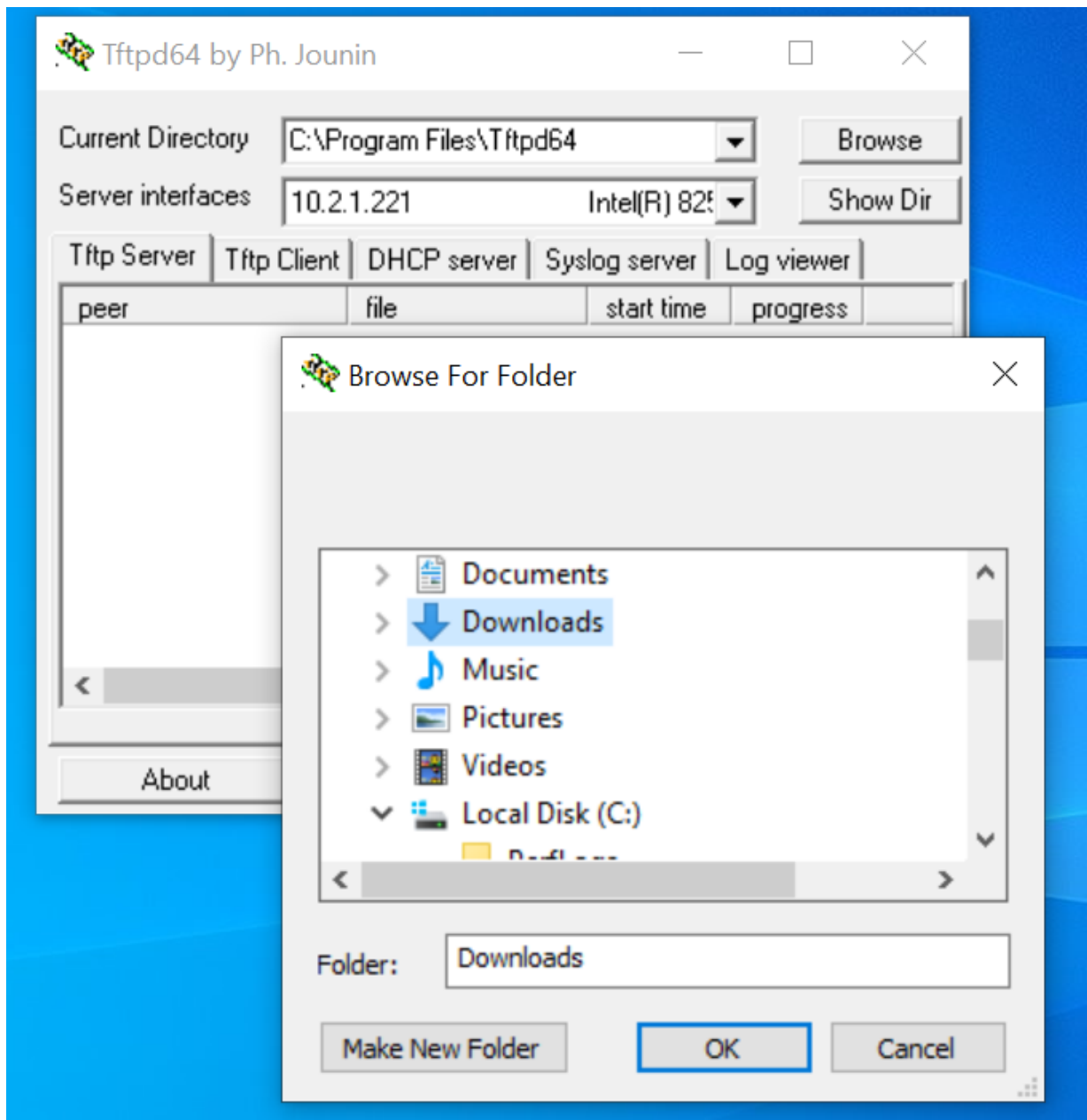


4. Rename this to *ciscosdwan_cloud_init.cfg*. Note that the name should match exactly as is enumerated here, else Bootstrapping will not work. If a file already exists with the same name, choose to overwrite.

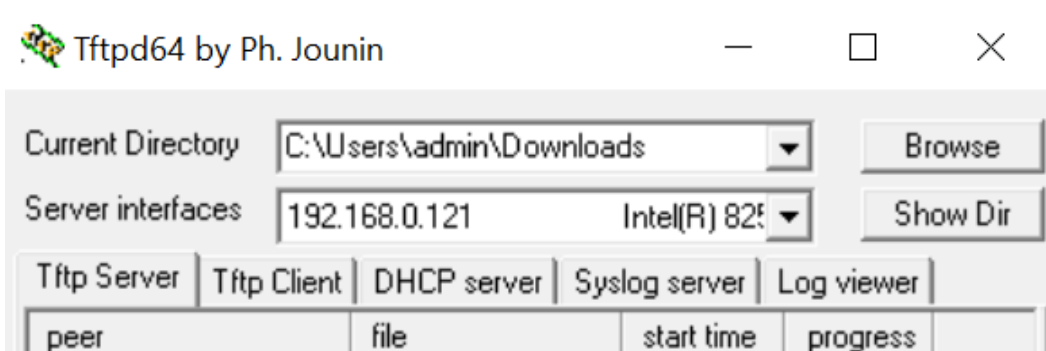


✔ **Tip:** On bootup, a cEdge looks for a file on it's USB port (if a bootable USB drive is connected) and in bootflash:. The file name must match as above for Cloud type devices (i.e. CSR1K). For physical devices, the file name should be *ciscosdwan.cfg*. If the file is present on the USB drive and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

5. From the Jumphost Desktop, start TFTP64. 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 Jump host (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): !
[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          100% 1277    838.9KB/s   00:00
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.

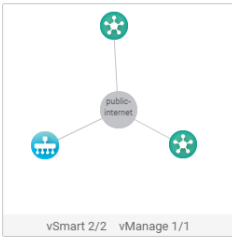
Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control	Version	Up Since	Device Groups	Connected vManage
vmanage	10.255.255.1	vManage	dfee63a5-66d2-4e50-a07b-ec4ad4...	✓	reachable	1000	--	8	20.1.1	11 May 2020 11:02:00 AM PDT	"No groups"	"10.255.255.1"
vSmart	10.255.255.3	vSmart	20607a12-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	0cdd4f0e-f2f1-f675-866c-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-44F0-E4DC-D30D-...	✓	reachable	40	5	3	17.02.01r.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	dde90ff0-dc62-77e6-510f-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)



Search Options

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

2 vSmart - 2, 6 WAN Edge - 6, 1 vBond - 1, 1 vManage - 1, Reboot 1, Warning Invalid 0

Control Status (Total 8): Control Up 8, Partial 0, Control Down 0

WAN Edge Inventory: Total 20, Authorized 20, Deployed 6, Staging 0

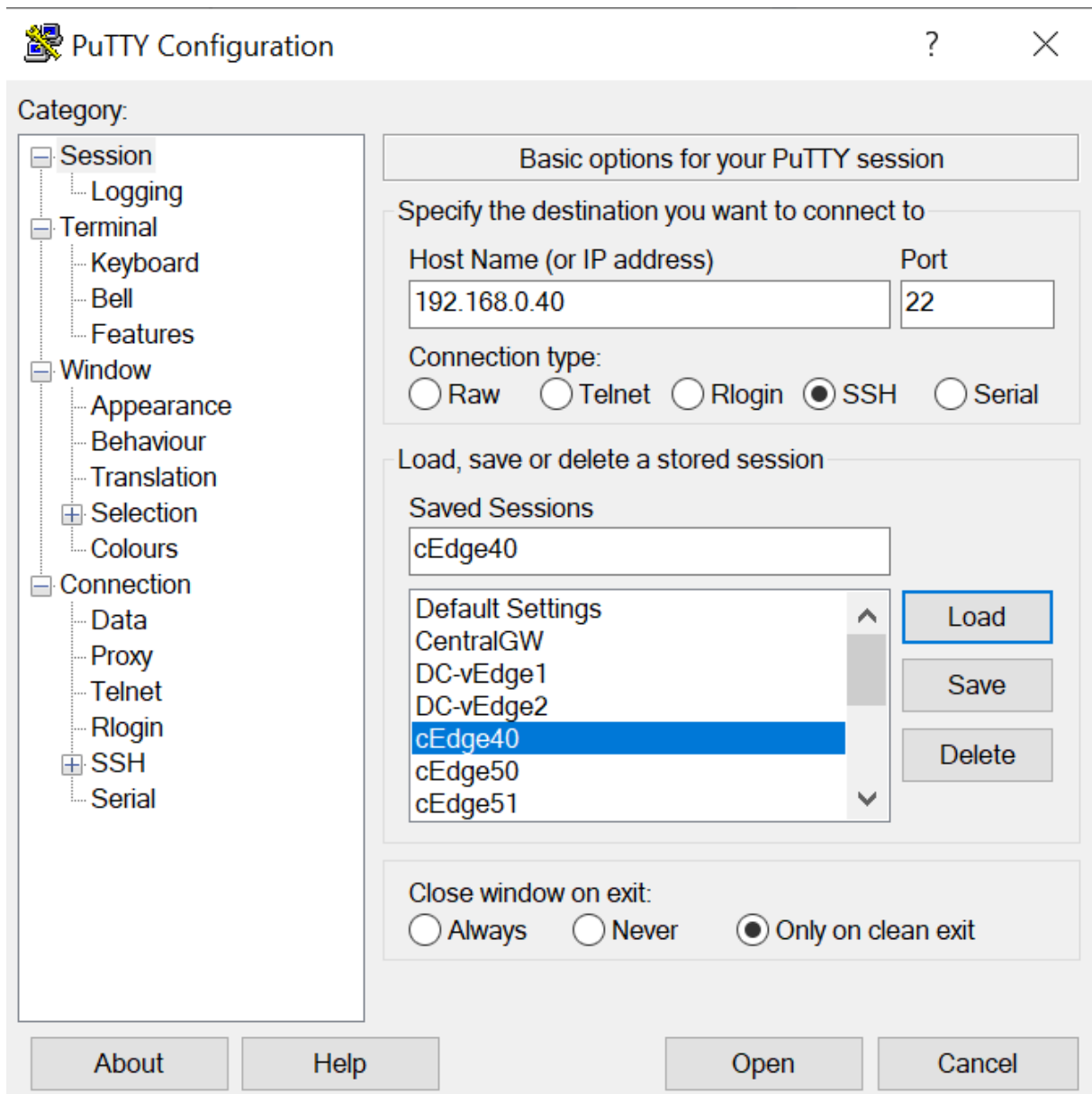
Site Health (Total 4): Full WAN Connectivity 4 sites, Partial WAN Connectivity 0 sites, No WAN Connectivity 0 sites

WAN Edge Health (Total 6): Normal 6, Warning 0, Error 0

Transport Interface Distribution: < 10 Mbps 22, 10 Mbps - 100 Mbps 0, 100 Mbps - 500 Mbps 0, > 500 Mbps 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

PEER PEER PEER CONTROLLER PEER PEER
TYPE PROT SYSTEM IP GROUP SITE DOMAIN PEER PEER
OXY STATE UPTIME ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR
-----
vsmart dtls 10.255.255.3 1000 1 100.100.100.4 12446 100.100.100.4 12446 public-internet
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-internet
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-internet
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
ⓘ	CSR1000v	CSR-44C7CE5A-4149-E696-C8A8-415C...	Token - fc40de6570e72...	NA	NA	--	--	--	CLI	--
ⓘ	CSR1000v	CSR-D6DB839FC-C383-BB55-7E9D-7CD...	Token - f28b5ab97898...	NA	NA	--	--	--	CLI	--
ⓘ	CSR1000v	CSR-834E40DC-E358-8DE1-0E81-76E59...	Token - b8a9caee09c9...	NA	NA	--	--	--	CLI	--
ⓘ	CSR1000v	CSR-D405F5BA-B975-8944-D1A3-2E08...	Token - e78aaefc1ebd2...	NA	NA	--	--	--	CLI	--
ⓘ	CSR1000v	CSR-D1837F36-6A1A-1850-7C1C-E1C6...	Token - 90ffdf29997f8...	NA	NA	--	--	--	CLI	--
ⓘ	CSR1000v	CSR-SE992295-1362-0DB6-EEF8-25CC...	Token - 1da14330e171...	NA	NA	--	--	--	CLI	--
ⓘ	CSR1000v	CSR-04F9482E-44F0-E4DC-D30D-60CC...	63201C50	NA	NA	cEdge40	10.255.255.41	40	vManage	cEdge_dualuplink_deve...
ⓘ	vEdge Cloud	e474c5fd-8ce7-d376-7cac-ba950b2c91...	7175AEDF	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                63201c50
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

```

Token is invalid since it has already been used

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=dfea63a5-66d2-4e50-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/emailAddress=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:c2:3c:41:10:
      a5:77:7f:c3:2c:35:a4:9e:7a:66:9d:ea:a9:01:ce:
      33:dc:93:1e:20:27:73:95:b8:e9:1c:af:26:dc:08:
      0a:e2:4e:e7:64:ef:0c:1f:1b:24:3e:dc:61:9e:e5:
      a3:43:80:49:00:0f:e0:1c:4c:b3:48:3b:52:a4:c3:
      ea:7e:70:fa:8c:51:c7:15:8c:0c:45:e8:89:ae:3f:
      69:fd:cd:34:90:61:90:50:2c:68:b7:52:6d:e8:99:
      06:5c:08:56:0a:53:61:5c:b8:0b:3a:4b:68:08:04:

```

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~~



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

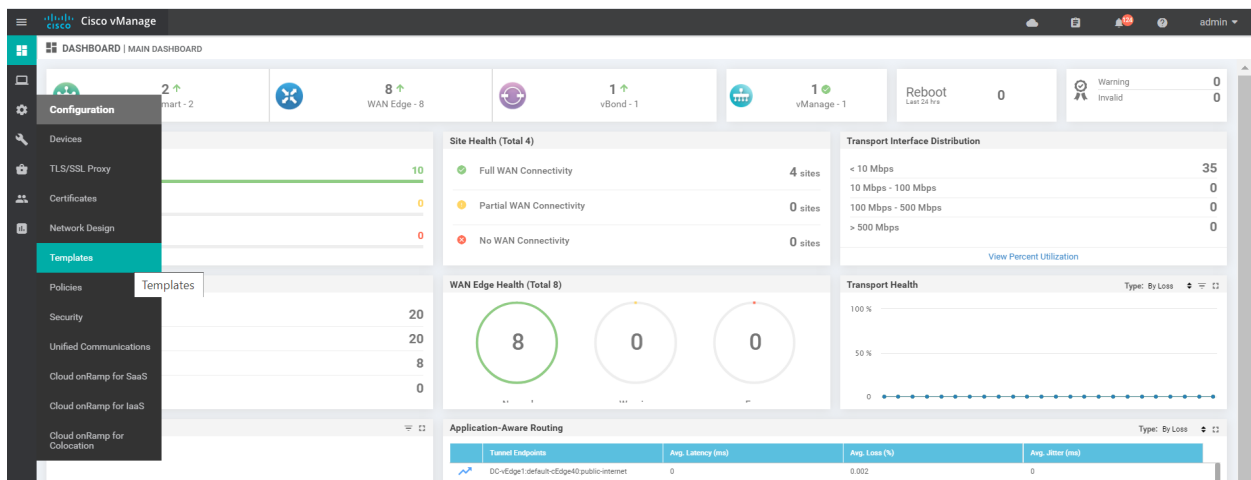
We have already seen feature templates in action and their versatility in large deployments is unmatched. Coupled with Device Specific parameters, we have a networking construct which is extremely malleable and can be applied in wide, arcing sweeps to similar devices through Device Templates that act 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**

CONFIGURATION | TEMPLATES

Device **Feature**

Add Template

Template Type: Non-Default

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

Cisco vManage

CONFIGURATION | TEMPLATES

Device **Feature**

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

NTP

OMP

System

VPN

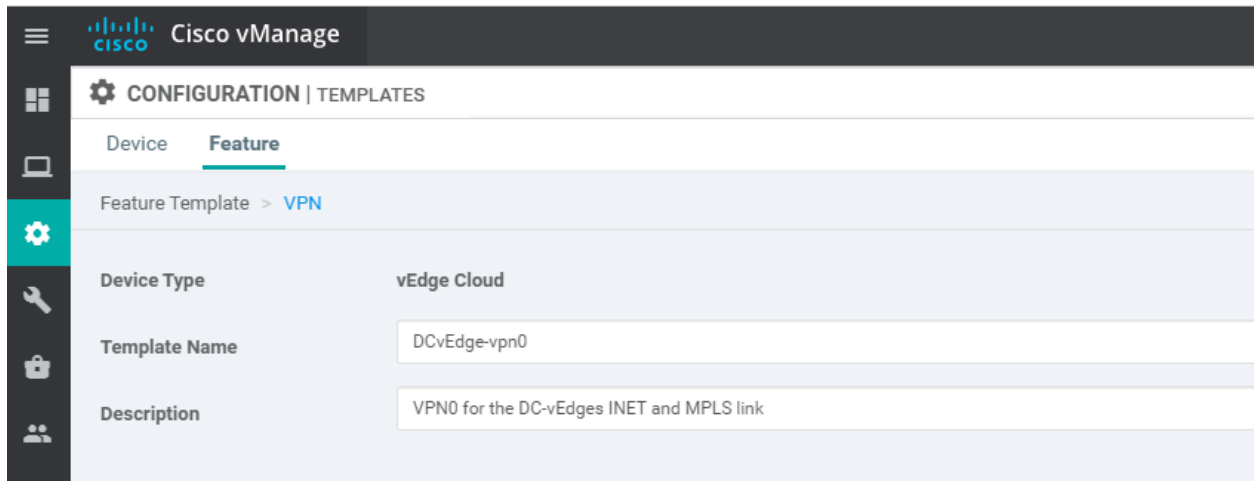
Secure Internet Gateway (SIG)
WAN

VPN

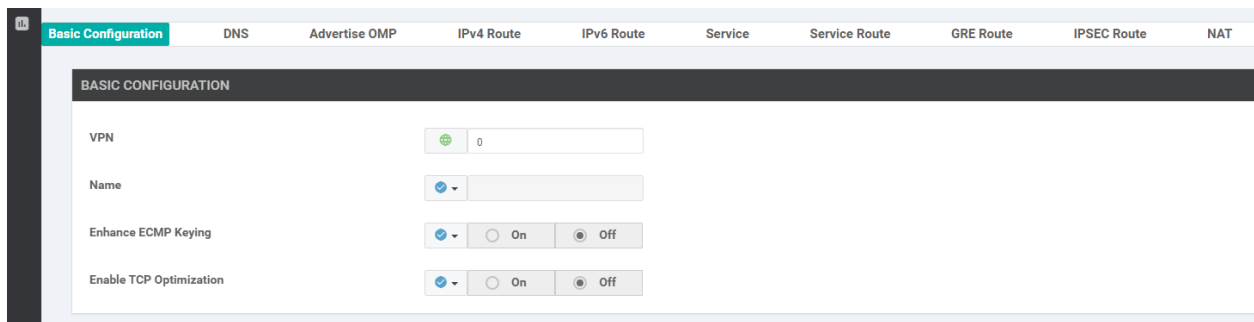
VPN Interface Cellular
WAN

VPN Interface Ethernet
Management | WAN | LAN

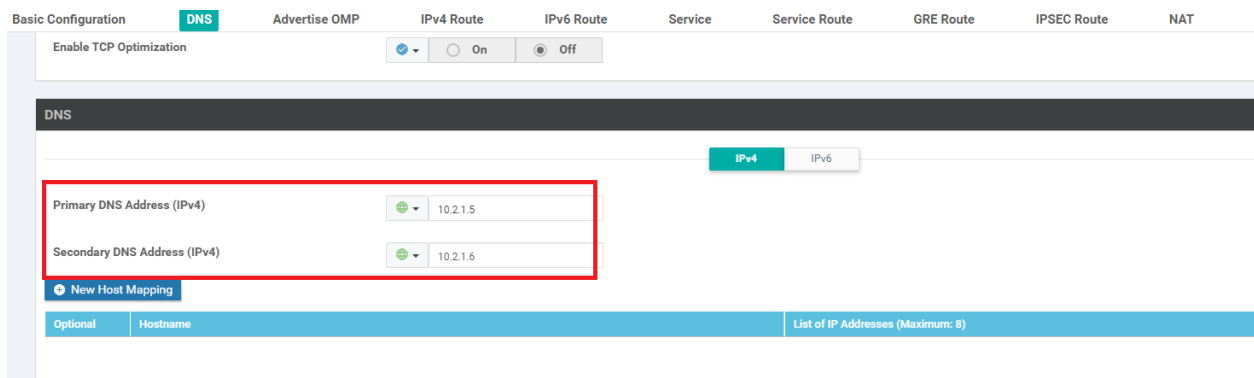
4. Give the Template a name of *DCvEdge-vpn0* and a description of *VPN0 for the DC-vEdges INET and MPLS link*



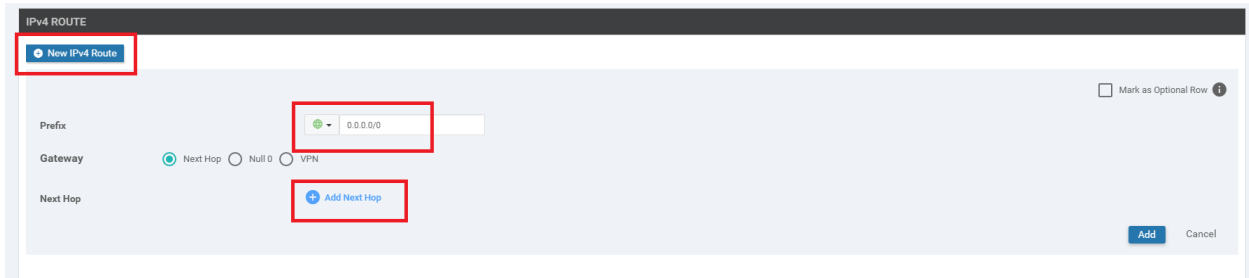
5. Under **Basic Configuration**, specify the VPN as 0 (zero)



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



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**



IPv4 ROUTE

New IPv4 Route

Prefix: 0.0.0.0/0

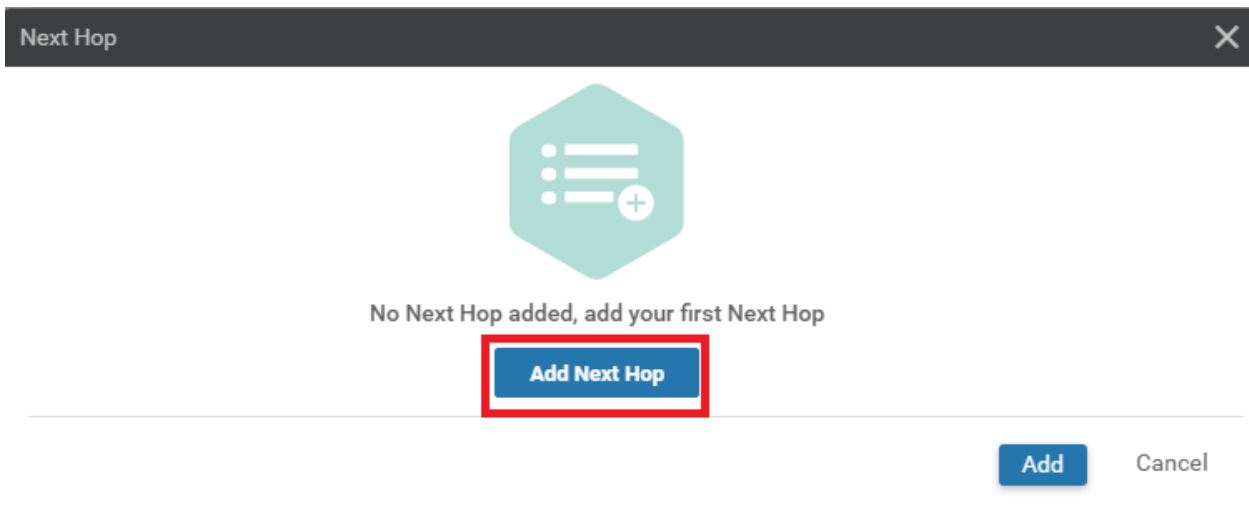
Gateway: Next Hop Null 0 VPN

Next Hop: **Add Next Hop**

Mark as Optional Row

Add Cancel

8. Click on **Add Next Hop** again in the popup window



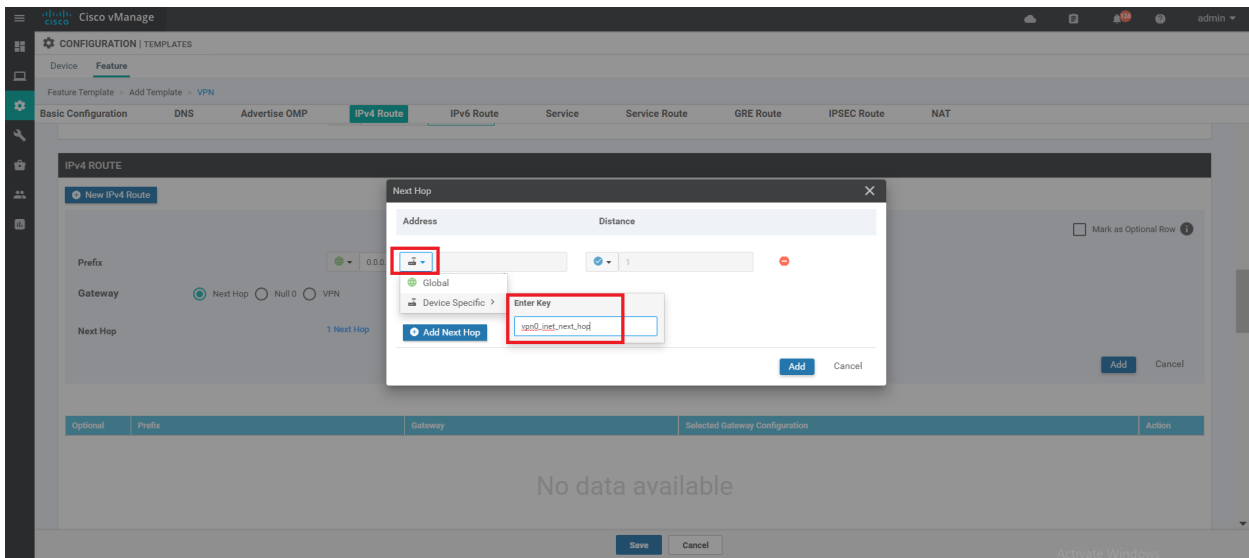
Next Hop

No Next Hop added, add your first Next Hop

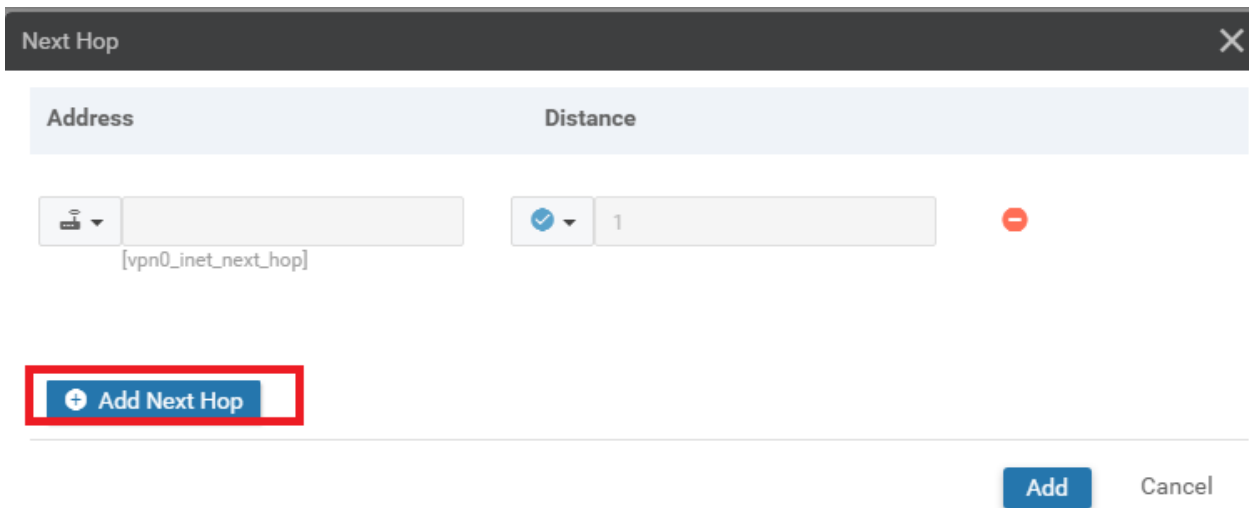
Add Next Hop

Add Cancel

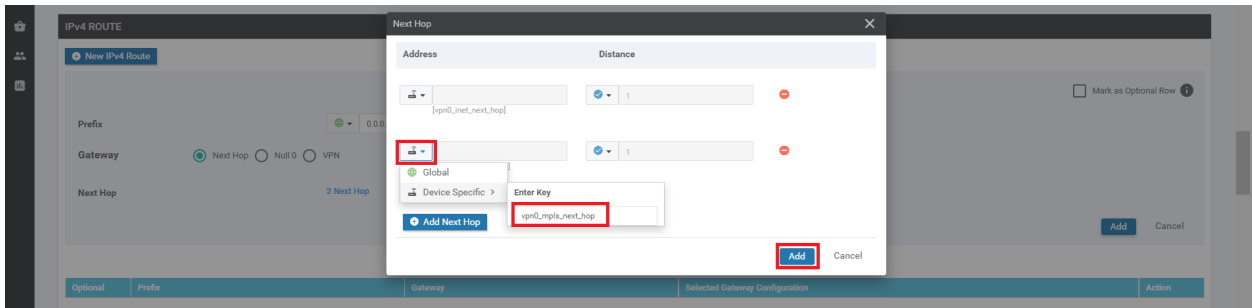
9. From the drop down, set the value to Device Specific and enter the key as *vpn0_inet_next_hop*



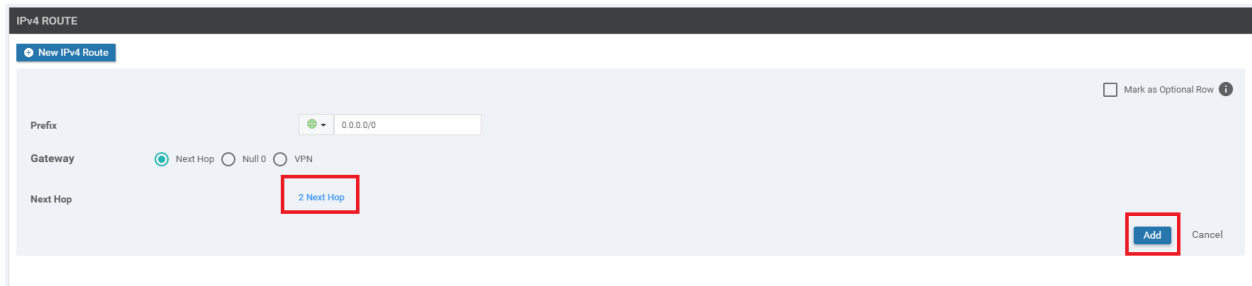
10. Click on **Add Next Hop**. We will now be adding the default route for the MPLS link



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: 0

Name: [dropdown]

Enhance ECMP Keying: [dropdown] On Off

Enable TCP Optimization: [dropdown] On Off

DNS

IPv4 IPv6

Save Cancel

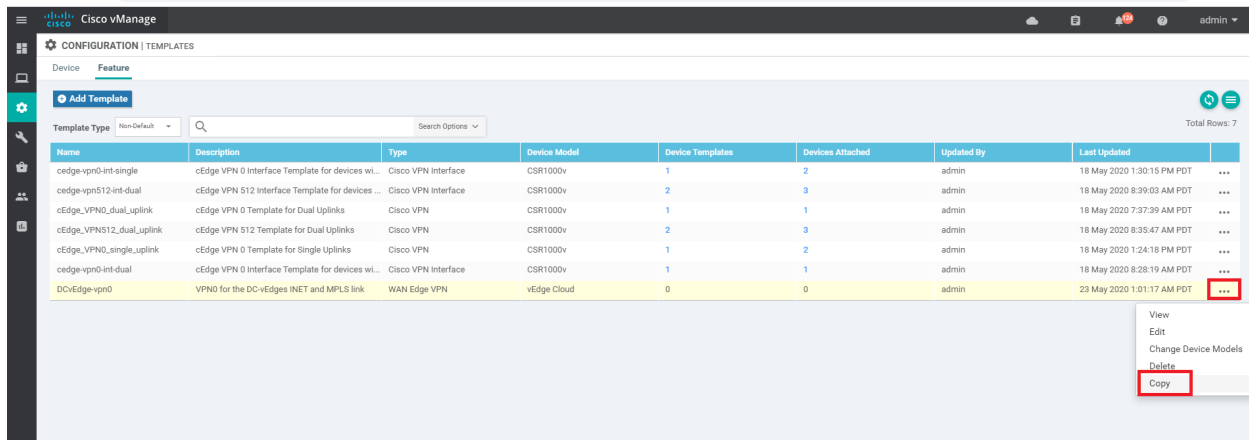
Task List

- 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

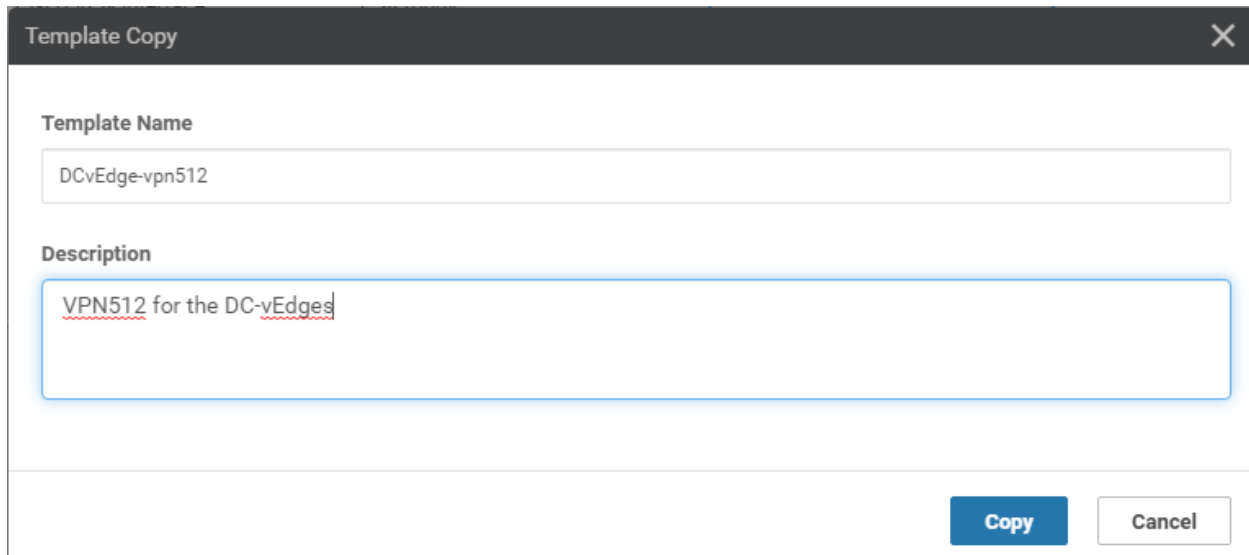
Creating the VPN512 Feature Template

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**



2. Give the Template a name of *DCvEdge-vpn512* and a description of *VPN512 for the DC-vEdges*. Click on **Copy**



3. Click on the three dots for the newly created template and click on **Edit**

Cisco vManage | CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type: Non-Default

Search Options

Total Rows: 8

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	
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_VPN512_dual_Uplink	cEdge VPN 512 Template for Dual Uplinks	Cisco VPN	CSR1000v	2	3	admin	18 May 2020 8:35:47 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	...
cEdge-vpn0-int-dual	cEdge VPN 0 Interface Template for devices wl...	Cisco VPN Interface	CSR1000v	1	1	admin	18 May 2020 8:28:19 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-single	cEdge VPN 0 Interface Template for devices wl...	Cisco VPN Interface	CSR1000v	1	2	admin	18 May 2020 1:30:15 PM PDT	...
DCvEdge-vpn512	VPN0 for the DC-vEdges INET and MPLS link	WAN Edge VPN	vEdge Cloud	0	0	admin	23 May 2020 1:12:04 AM PDT	...
cEdge_VPN0_dual_Uplink	cEdge VPN 0 Template for Dual Uplinks	Cisco VPN	CSR1000v	1	1	admin	18 May 2020 7...	...

View
Edit
Change Device Models
Delete
Copy

4. Update the Description, if it hasn't been updated and change the VPN to **512**

Feature Template - VPN

Device Type: vEdge Cloud

Template Name: DCvEdge-vpn512

Description: VPN512 for the DC-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 templates 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: 512

Name: [Dropdown]

Enhance ECMP Keying: [On/Off]

Enable TCP Optimization: [On/Off]

5. Scroll down to 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"/>	0.0.0.0/0	Next Hop	2	

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

7. Click on the minus sign to remove the MPLS next hop

Next Hop

Address	Distance	
<input type="text" value="[vpn0_inet_next_hop]"/>	<input type="text" value="1"/>	<input type="button" value="-"/>
<input type="text" value="[vpn0_mpls_next_hop]"/>	<input type="text" value="1"/>	<input type="button" value="-"/>

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" value="[vpn512_next_hop]"/>	<input type="text" value="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 Mark as Optional Row *i*

Gateway Next Hop Null 0 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

IPv4 ROUTE

+ New IPv4 Route

Optional	Prefix	Gateway	Selected Gateway Configuration
<input type="checkbox"/>	0.0.0.0/0	Next Hop	1

IPv6 ROUTE

Update Cancel

We have created our VPN512 Feature Template

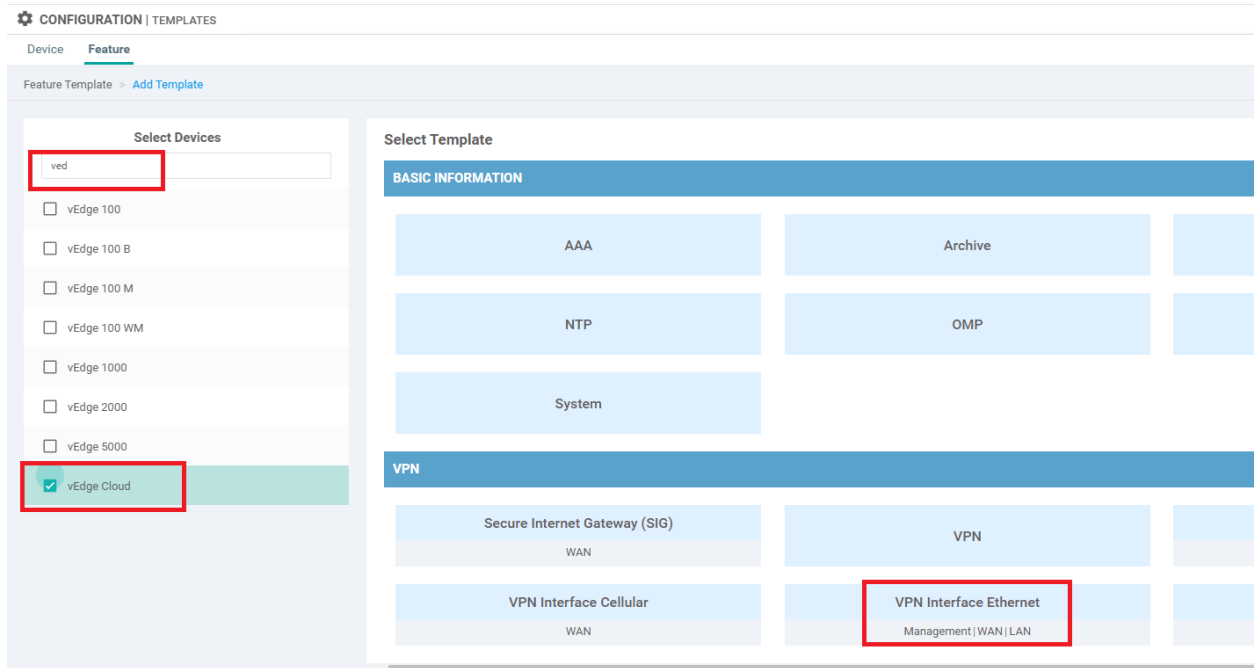
Task List

- 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



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-Edge_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:

Description:

IPv4 | IPv6

Dynamic Static

IPv4 Address:

TUNNEL

Tunnel Interface	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Per-tunnel Qos	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Color	<input type="text" value="[vpn0_inet_if_color]"/>
Restrict	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Groups	<input checked="" type="checkbox"/>
Border	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Control Connection	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Maximum Control Connections	<input checked="" type="checkbox"/>
vBond As Stun Server	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Exclude Controller Group List	<input checked="" type="checkbox"/>

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Add Template > VPN Interface Ethernet

Low-Bandwidth Link	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Allow Service	
All	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
BGP	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
DHCP	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> On <input type="checkbox"/> Off
DNS	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> On <input type="checkbox"/> Off
ICMP	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> On <input type="checkbox"/> Off
NETCONF	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
NTP	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
OSPF	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off
SSH	<input checked="" type="checkbox"/> <input type="checkbox"/> On <input checked="" type="checkbox"/> Off

Save Cancel

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**

Template Copy
✕

Template Name

Description

MPLS interface for the DC-vEdges

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>

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

BASIC CONFIGURATION

Shutdown Yes No

Interface Name

Description

IPv4 IPv6

Dynamic Static

IPv4 Address

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

Tunnel Interface On Off

Per-tunnel Qos On Off

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

vManage Connection Preference

Update Cancel

This completes the configuration of the MPLS VPN Interface Feature Template.

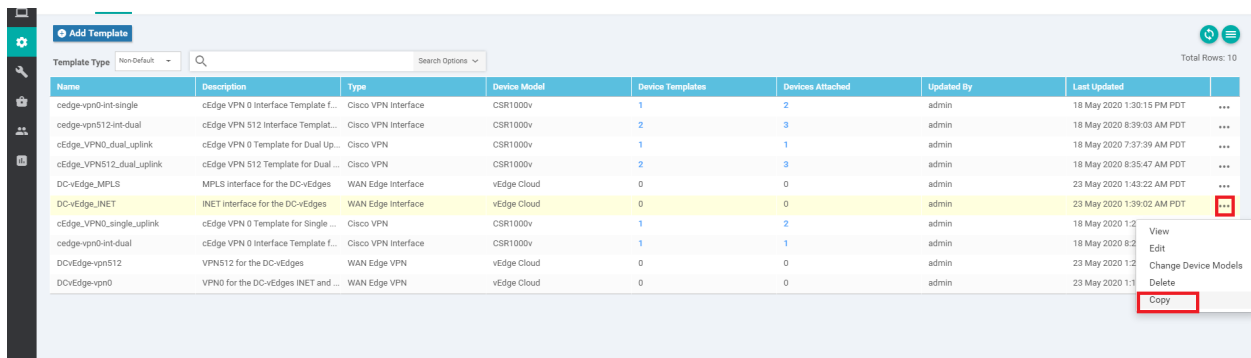
Task List

- 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	
cedge-vprn0-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_Luplink	cEdge VPN 0 Template for Dual Up...	Cisco VPN	CSR1000v	1	1	admin	18 May 2020 7:37:39 AM PDT	...
cEdge_VPN512_dual_Luplink	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_Luplink	cEdge VPN 0 Template for Single ...	Cisco VPN	CSR1000v	1	2	admin	18 May 2020 1:2...	View
cedge-vprn0-int-dual	cEdge VPN 0 Interface Template f...	Cisco VPN Interface	CSR1000v	1	1	admin	18 May 2020 8:2...	Edit
DC-vEdge-vpn512	VPN512 for the DC-vEdges	WAN Edge VPN	vEdge Cloud	0	0	admin	23 May 2020 1:2...	Change Device Models
DC-vEdge-vpn0	VPN0 for the DC-vEdges INET and ...	WAN Edge VPN	vEdge Cloud	0	0	admin	23 May 2020 1:1...	Delete
								Copy

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

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	<i>DC-vEdge_mgmt_int</i>
	Description	NA	<i>MGMT interface for the DC-vEdges</i>
Basic Configuration	Shutdown	Global	No
Basic Configuration	Interface Name	Device Specific	<i>vpn512_mgmt_if_name</i>
Basic Configuration	IPv4 Address	Device Specific	<i>vpn512_mgmt_if_ip</i>
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: No

Interface Name: [vpn512_mgmt_if_name]

Description: []

Dynamic Static

IPv4 Address: [vpn512_mgmt_if_ip]

TUNNEL

Tunnel Interface: Off

NAT

NAT: Off

VRRP

[]

Update Cancel

We have created the VPN 512 Interface Template.

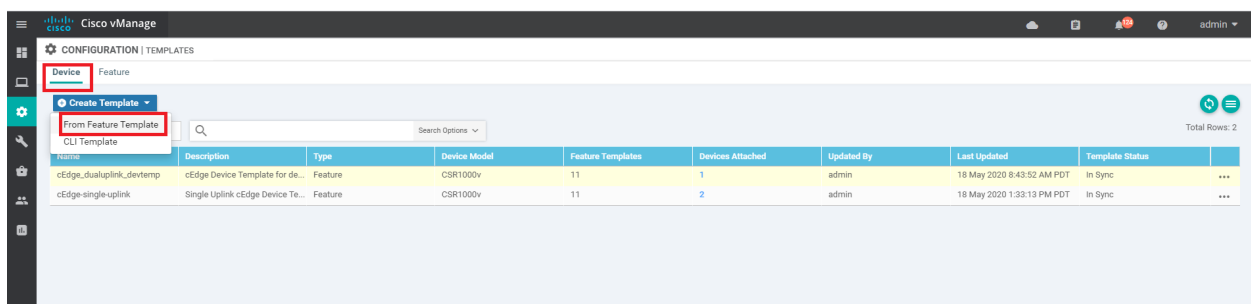
Task List

- 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**



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

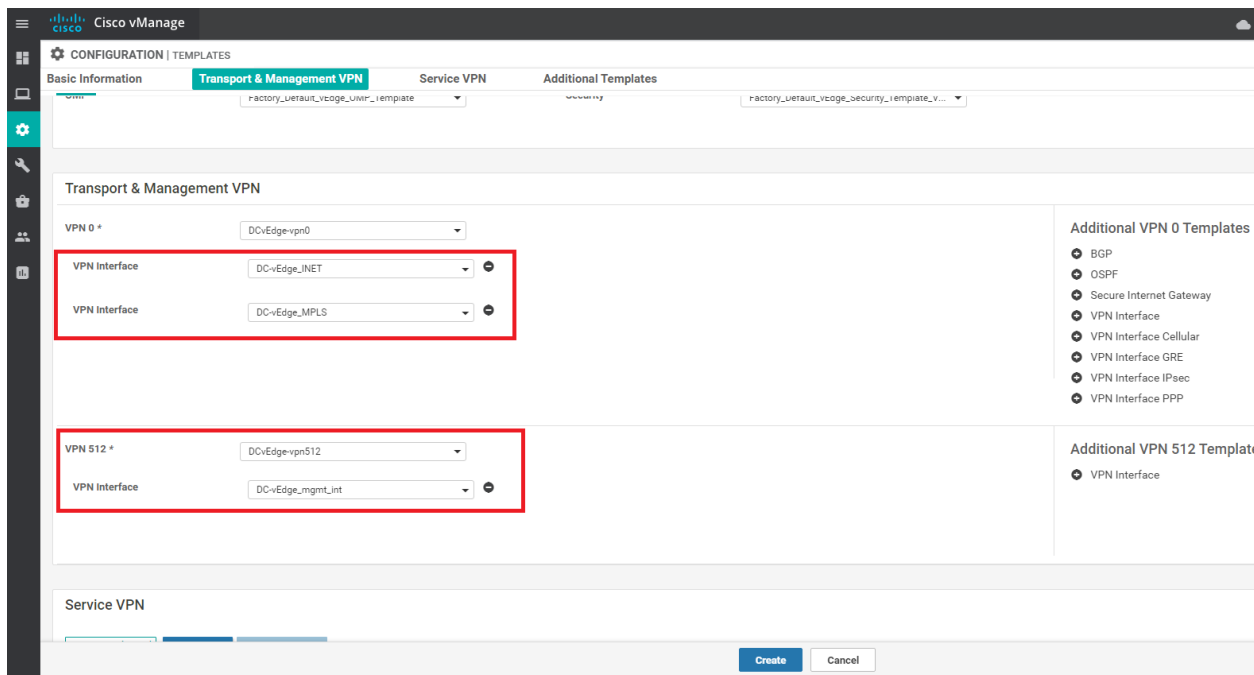
- BGP
- OSPF
- Secure Internet Gateway
- VPN Interface** Click Twice
- VPN Interface Cellular
- VPN Interface GRE
- VPN Interface IPsec
- VPN Interface PPP

VPN 512 * DCvEdge-vpn512

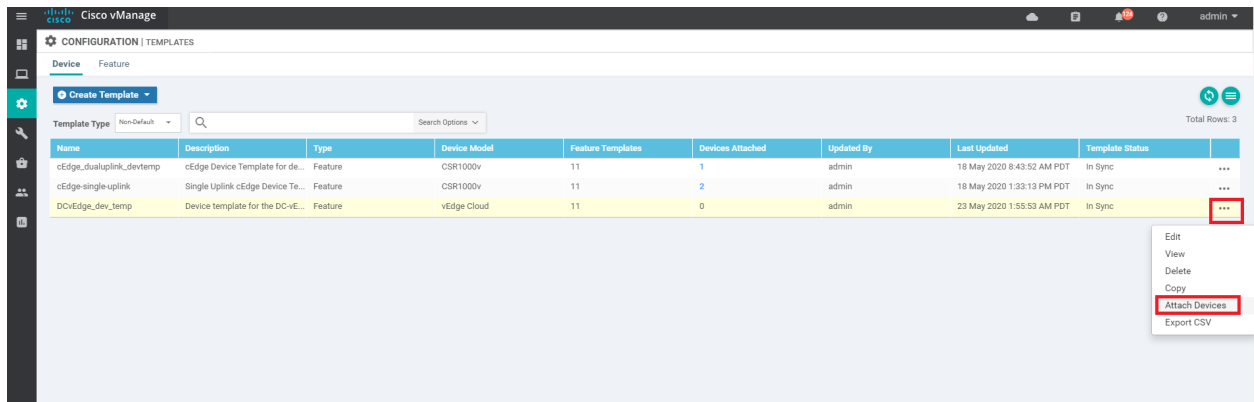
Additional VPN 512 Templates

- VPN Interface** Click Once

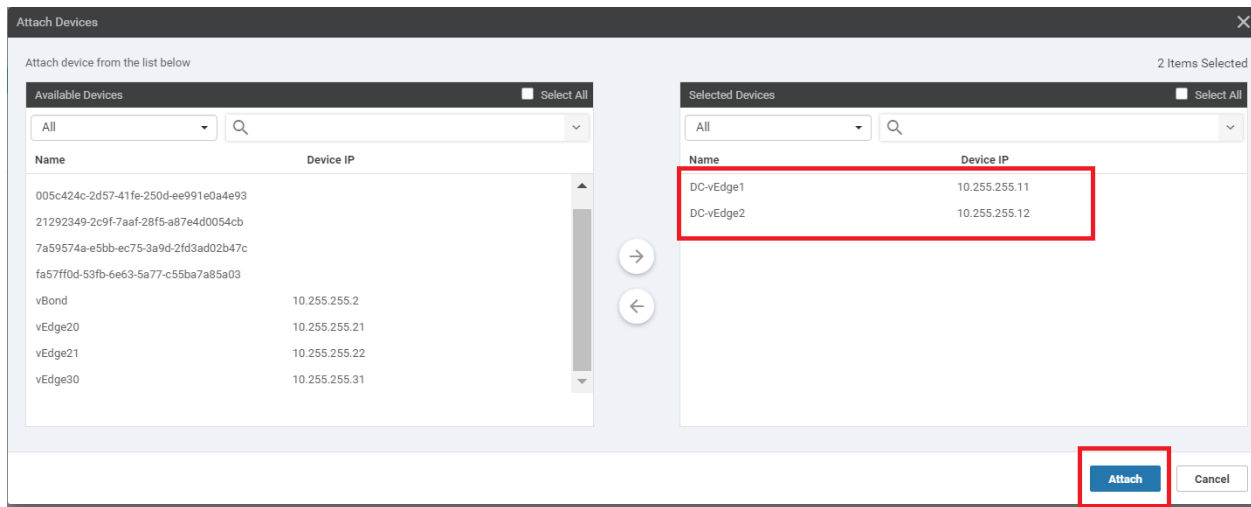
4. Populate the VPN Interface fields from the drop down as show below and click on **Create**



5. Click on the three dots next to the newly created Device Template named *DCvEdge_dev_temp* and click on **Attach Devices**



6. Move **DC-vEdge1** and **DC-vEdge2** to the list of selected devices and click on **Attach**



- 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 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

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

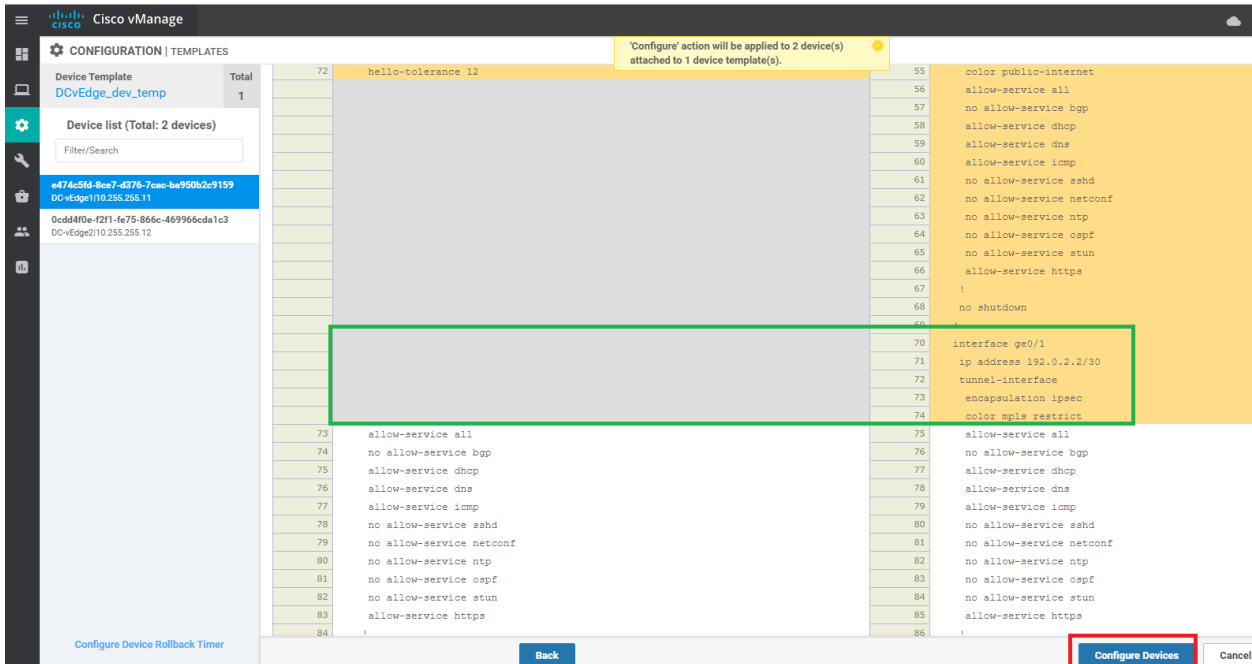
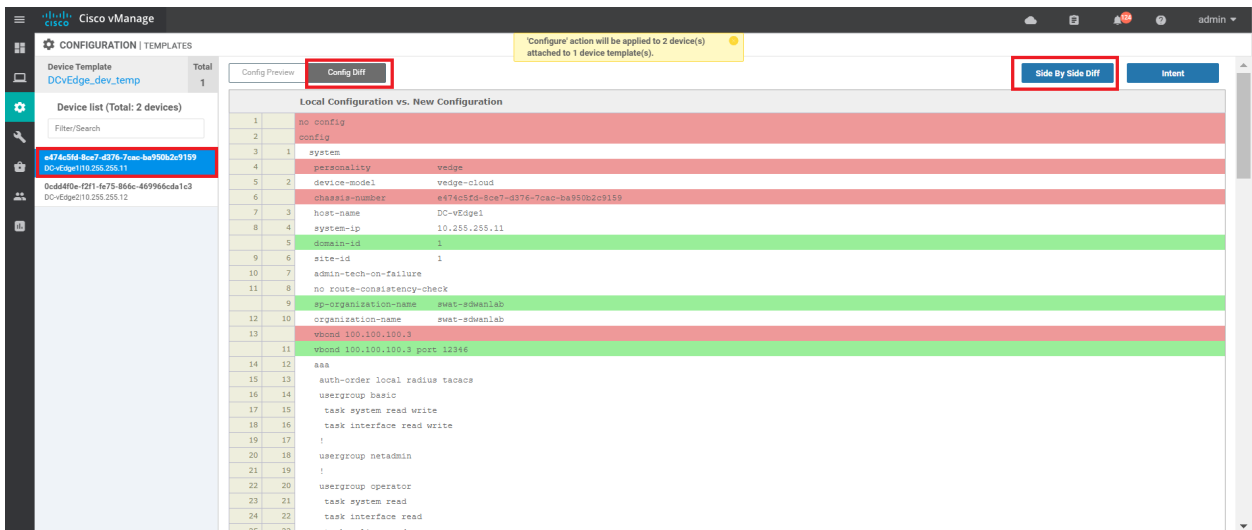
Generate Password

Update

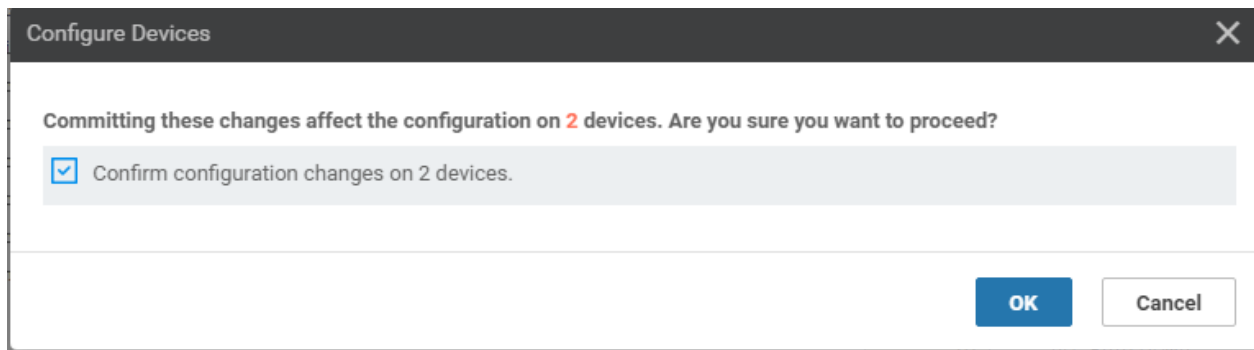
Cancel

Click on **Next** to proceed

- 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.



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

Search Options ▾

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
> ✔ Success	Done - Push Feature Template Co...	e474c5f0-8ce7-d376-7cac-ba950...	vEdge Cloud	DC-vEdge1	10.255.255.11	1	10.255.255.1
> ✔ Success	Done - Push Feature Template Co...	0cdd4f0e-f2f1-f675-866c-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

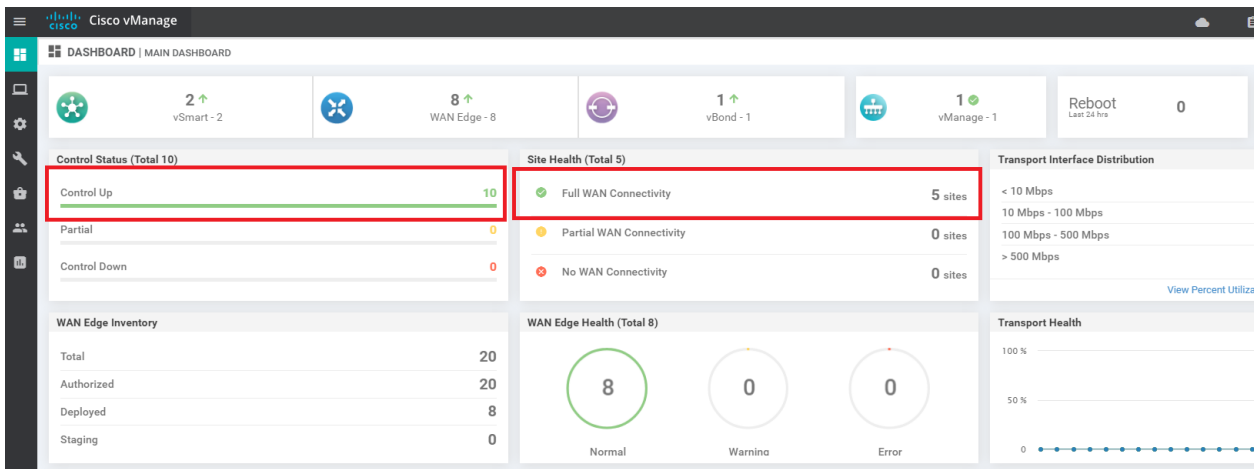
- [Creating the DC-vEdge VPN Feature Templates](#)
- [Creating the VPN0 Feature Template](#)
- [Creating the VPN512 Feature Template](#)
- [Creating the INET VPN Interface Feature Template](#)
- [Creating the MPLS VPN Interface Feature Template](#)
- [Creating the Mgmt VPN Interface Feature Template](#)
- [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
...	CSR1000v	CSR-44C7CESA-4149-E696-CBA8-415C...	Token - fc40de6570e72...	NA	NA	--	--	--	CLI	--
...	CSR1000v	CSR-06DB39FC-C383-BB55-7E9D-7CD...	Token - f28b5ab97898...	NA	NA	--	--	--	CLI	--
...	CSR1000v	CSR-834E40DC-E358-8DE1-0E81-76E59...	FA1F272A	NA	NA	cEdge60	10.255.255.51	50	vManage	cEdge-single-uplink
...	CSR1000v	CSR-0405F5BA-8975-9944-D1A3-2E08...	Token - e78aaefc1ebd2...	NA	NA	--	--	--	CLI	--
...	CSR1000v	CSR-D1837F36-6A1A-1850-7C1C-E1C6...	FB7DC382	NA	NA	cEdge61	10.255.255.52	50	vManage	cEdge-single-uplink
...	CSR1000v	CSR-5E992295-1362-0DB6-EEF8-25CC...	Token - 1da14330e171...	NA	NA	--	--	--	CLI	--
...	CSR1000v	CSR-04F9482E-44F0-E4DC-D30D-60C0...	63201C50	NA	NA	cEdge40	10.255.255.41	40	vManage	cEdge_dualuplink_deve...
...	vEdge Cloud	e474c5fd-8ce7-d376-7cac-ba950b2c91...	7175AE0F	NA	NA	DC-vEdge1	10.255.255.11	1	vManage	DCvEdge_dev_temp
...	vEdge Cloud	0cdd4f0e-f2f1-fe75-866c-469966cda1c3	7DA605F5	NA	NA	DC-vEdge2	10.255.255.12	1	vManage	DCvEdge_dev_temp
...	vEdge Cloud	b7d7295-58d1-7671-e914-6f62edff1609	297060DD	NA	NA	vEdge60	10.255.255.21	20	CLI	--
...	vEdge Cloud	dde90ff0-dc62-77e6-510f-08d9608537d	8BFD4E65	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 ▾ Total Rows: 8

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

```
cEdge51#show sdwan bfd session
```

SYSTEM IP	TX INTERVAL (msec)	TX STATE	TX UPTIME	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP	DST PUBLIC PORT	DST PUBLIC ENCAP	DST PUBLIC MU
10.255.255.11	1000	up	0:00:06:24	mpls	mpls	192.1.1.22	192.0.2.2	12406	ipsec	7
10.255.255.12	1000	up	0:00:05:47	mpls	mpls	192.1.1.22	192.0.2.6	12406	ipsec	7

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 VPN0 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 VPN0 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	
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	1	2	admin	23 May 2020 1:43:22 AM PDT	...
DC-vEdge_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-vEdge_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-vpn512	VPN512 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...	Copy

Template 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

Optional	Prefix	Gateway	Selected Gateway Configuration	Action
<input type="checkbox"/>	0.0.0.0/0	Next Hop	2	 

3. Click on **2 Next Hop**

Update IPv4 Route



Prefix Mark as Optional Row 

Gateway Next Hop Null 0 VPN

Next Hop 2 Next Hop

4. Click on the remove icon for the second next hop

Next Hop

Address	Distance	
<input type="text" value="[vpn0_inet_next_hop]"/>	<input type="text" value="1"/>	
<input type="text" value="[vpn0_mpls_next_hop]"/>	<input type="text" value="1"/>	

5. Edit the name of the INET next hop to represent something more generic, like *vpn0_next_hop*. We will use this VPN0 Template for both the vEdges at Site 20. Click on **Save Changes**

The screenshot shows a 'Next Hop' configuration window. At the top, there are two columns: 'Address' and 'Distance'. Under 'Address', there is a dropdown menu with a VPN icon and a text input field containing '[vpn0_next_hop]'. To the right, under 'Distance', there is a dropdown menu with a checkmark icon and a text input field containing '1'. Below these fields is a blue button labeled '+ Add Next Hop'. At the bottom right, there is a blue button labeled 'Save Changes' and a grey button labeled 'Cancel'. Both the 'Save Changes' button and the text input field for the address are highlighted with a red rectangular box.

6. Make sure there is just **1 Next Hop** populated and click on **Save Changes** again

The screenshot shows an 'Update IPv4 Route' configuration window. It has three main sections: 'Prefix', 'Gateway', and 'Next Hop'. The 'Prefix' section has a dropdown menu with a globe icon and a text input field containing '0.0.0.0/0'. To the right of this is a checkbox labeled 'Mark as Optional Row' with an information icon. The 'Gateway' section has three radio buttons: 'Next Hop' (which is selected), 'Null 0', and 'VPN'. The 'Next Hop' section shows '1 Next Hop' in blue text. At the bottom right, there is a blue button labeled 'Save Changes' and a grey button labeled 'Cancel'. The 'Save Changes' button is highlighted with a red rectangular box.

7. Click on **Update** on the main Feature Template screen

Basic Configuration DNS Advertise OMP **IPv4 Route** IPv6 Route Service Service Route GRE Route IPSEC Route NAT

NETWORK AGGREGATE

Network (IPv4) On Off

IPv4 ROUTE

[+ New IPv4 Route](#)

Optional	Prefix	Gateway	Selected Gateway Configuration
<input type="checkbox"/>	<input checked="" type="radio"/> 0.0.0.0/0	Next Hop	1

IPv6 ROUTE

[+ New IPv6 Route](#)

Optional	Prefix	Gateway	Selected Gateway Configuration

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**

Template Name	Description	Category	Model	Version	Author	Created	Actions
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_MPLS	MPLS interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 1:43:22 AM PDT ...
DCvEdge_INET	INET interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 1:3...
DCvEdge-vpn512	VPN512 for the DC-vEdges	WAN Edge VPN	vEdge Cloud	1	2	admin	23 May 2020 1:2...
cEdge_VPN0_single_uplink	cEdge VPN 0 Template for Single ...	Cisco VPN	CSR1000v	1	2	admin	18 May 2020 1:2...
cedge-vpn0-int-dual	cEdge VPN 0 Interface Template f...	Cisco VPN Interface	CSR1000v	1	1	admin	18 May 2020 8:2...
DCvEdge-vpn0	VPN0 for the DC-vEdges INET and ...	WAN Edge VPN	vEdge Cloud	1	2	admin	23 May 2020 1:1...

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_add</i>
Tunnel	Tunnel Interface	Global	On
Tunnel	Color	Device Specific	<i>vpn0_if_color</i>
Tunnel	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: No Yes

Interface Name: [vpn0_if_name]

Description:

IPv4
IPv6

Dynamic Static

IPv4 Address: [vpn0_if_ip_add]

Basic Configuration **Tunnel** NAT VRRP ACL/QoS ARP 802.1X Advanced

TUNNEL

Tunnel Interface On Off

Per-tunnel Qos On Off

Color

Restrict On Off

Groups On Off

Border On Off

Control Connection On Off

Maximum Control Connections

vBond As Stun Server On Off

Exclude Controller Group List

Update Cancel

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	
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

factory_vdefault_vcage_umr_t... factory_vdefault_vcage_security_t...

Transport & Management VPN

VPN 0 * Site20-vpn0

VPN Interface Site20_vpn0_int

VPN Interface DCvEdge_MPLS [Click here to remove](#)

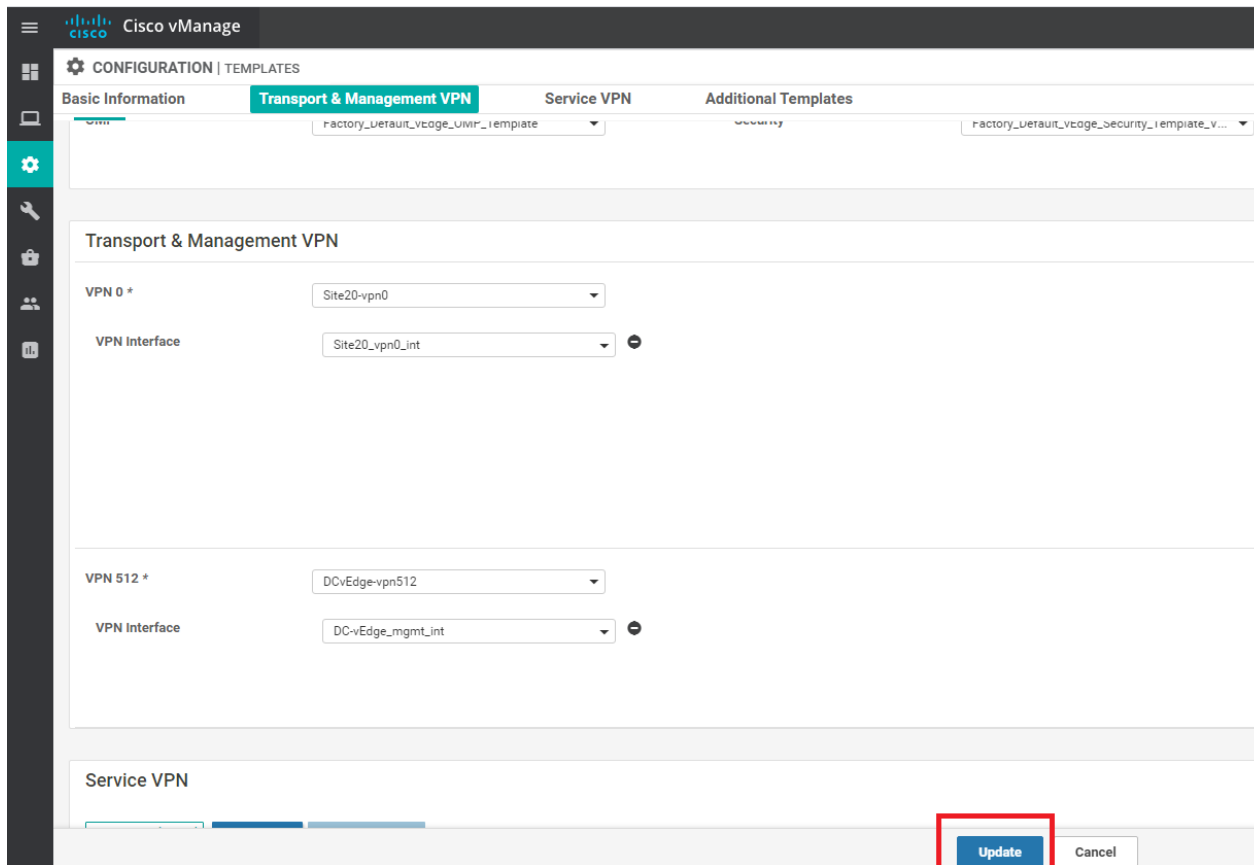
VPN 512 * DCvEdge-vpn512

VPN Interface DCvEdge_mgmt_int [Re-using the DC templates for VPN512](#)

Service VPN

Update Cancel

4. Click on **Update** once done

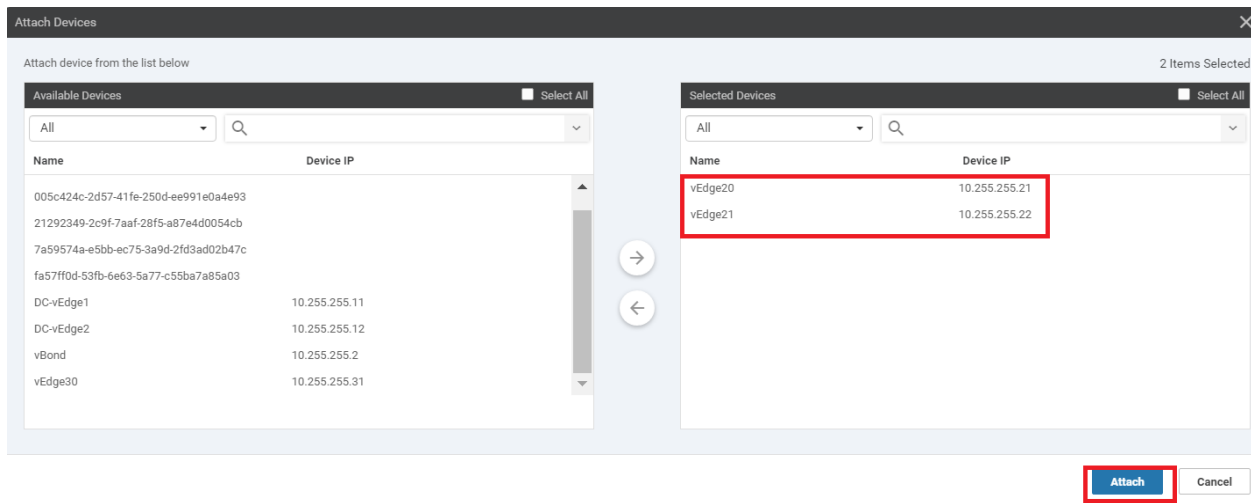


5. Click on the three dots next to the newly created *vEdge_Site20_dev_temp* Template and click on **Attach Devices**

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
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-singleuplink	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	...

- Edit
- View
- Delete
- Copy
- Attach Devices
- Export 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_add)	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_add)	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 ✕

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_if_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

Search Options ▾

S.	Chassis Number	System IP	Hostname	Address(vpn512_next_hop)	Interface Name(vpn512_mgmt_if_name)	IPv4 Address(vpn512_mgmt_if_ip_add)	Addr
✓	7fd7295-58df-7671-e914-6fe2edff1609	10.255.255.21	vEdge20	192.168.0.1	eth0	192.168.0.20/24	100.11
✓	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**

Device list (Total: 2 devices)

Filter/Search

b7fd7295-58df-7671-e914-6fe2edff1609
vEdge20 10.255.255.21

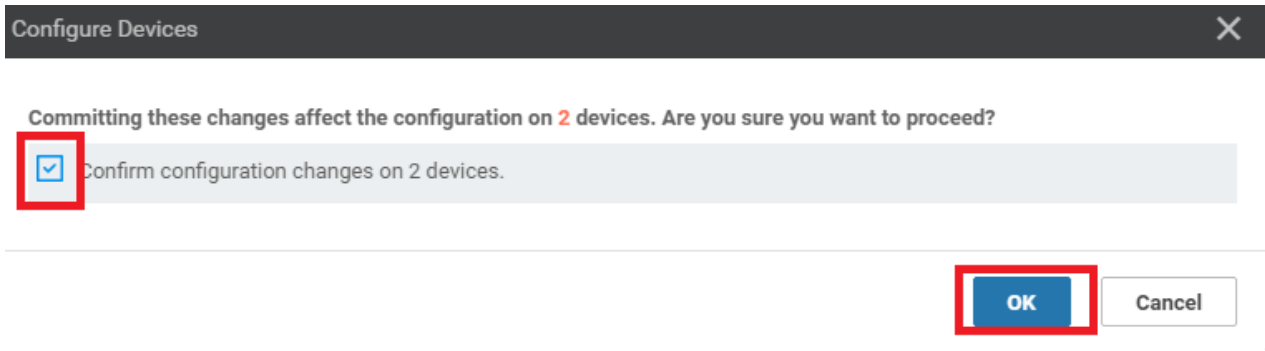
dde90ff0-dc62-77e6-510f-08d96608537d
vEdge21 10.255.255.22

Local Configuration		New Configuration	
1	no config		
2	config		
3	system	1	system
4	personality vedge		
5	device-model vedge-cloud	2	device-model vedge-cloud
6	chassis-number b7fd7295-58df-7671-e914-6fe2edff1609		
7	host-name vEdge20	3	host-name vEdge20
8	system-ip 10.255.255.21	4	system-ip 10.255.255.21
9	site-id 20	5	domain-id 1
10	admin-tech-on-failure	6	site-id 20
11	no route-consistency-check	7	admin-tech-on-failure
		8	no route-consistency-check
		9	sp-organization-name swat-sdwanlab
12	organization-name swat-sdwanlab	10	organization-name swat-sdwanlab
13	vbond 100.100.100.3	11	vbond 100.100.100.3 port 12346
14	aaa	12	aaa
15	auth-order local radius tacacs	13	auth-order local radius tacacs
16	usergroup basic	14	usergroup basic
17	task system read write	15	task system read write
18	task interface read write	16	task interface read write
19	!	17	!
20	usergroup netadmin	18	usergroup netadmin
21	!	19	!
22	usergroup operator	20	usergroup operator
23	task system read	21	task system read
24	task interface read	22	task interface read
25	task policy read	23	task policy read
26	task routing read	24	task routing read

Configure Device Rollback Timer

Back **Configure Devices** Cancel

11. Confirm this change and click on **OK**



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.

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-08d966...	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
LTIPLIER	INTERVAL (msec)	UPTIME	TRANSITIONS			
10.255.255.11	1	up	mpls	mpls	192.0.2.10	192.0.2.2
1000		0:00:01:56	0			
10.255.255.12	1	up	mpls	mpls	192.0.2.10	192.0.2.6
1000		0:00:01:56	0			
10.255.255.52	50	up	mpls	mpls	192.0.2.10	192.1.1.22
1000		0:00:01:56	0			

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	297060DD	NA	NA	vEdge20	10.255.255.21	20	vManage	vEdge_Site20_dev_temp	In S	...
vEdge Cloud	dde90ff0-dc62-77e6-510f-08d96608537d	88FD4E55	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

1. 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	
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_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	...
DCvEdge_mgmt_Lint	MGMT interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	2	4	admin	23 May 2020 1:49:11 AM PDT	...

2. 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 Copy

Template Name
vEdge30-vpn0

Description
VPN0 for the Site30 INET and MPLS link

Copy Cancel

3. 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

- 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

Template Name

vEdge30_INET

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

- 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

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_vpn0	VPND 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 vEdges	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
✕

Template Name

Description

Device template for the Site 30 vEdge

Copy

Cancel

- 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.

- 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
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

- Choose **vEdge30** from the list and click on **Attach**

Attach Devices

Attach device from the list below 1 Items Selected

Available Devices Select All

All

Name	Device IP
21292349-2c9f-7aaf-28f5-a87e4d0054cb	
7a59574a-e5bb-ec75-3a9d-2fd3ad02b47c	
fa57ff0d-53fb-6e63-5a77-c55ba7a85a03	
DC-vEdge1	10.255.255.11
DC-vEdge2	10.255.255.12
vBond	10.255.255.2
vEdge20	10.255.255.21
vEdge21	10.255.255.22

Selected Devices Select All

All

Name	Device IP
vEdge30	10.255.255.31

Attach Cancel

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)	<input type="text" value="192.168.0.1"/>
Interface Name(vpn512_mgmt_if_name)	<input type="text" value="eth0"/>
IPv4 Address(vpn512_mgmt_if_ip_add)	<input type="text" value="192.168.0.30/24"/>
Address(vpn0_inet_next_hop)	<input type="text" value="100.100.100.1"/>
Address(vpn0_mpls_next_hop)	<input type="text" value="192.0.2.13"/>
Interface Name(vpn0_mpls_if_name)	<input type="text" value="ge0/1"/>
IPv4 Address(vpn0_mpls_if_ip_add)	<input type="text" value="192.0.2.14/30"/>
Color(vpn0_mpls_if_color)	<input type="text" value="mpls"/>
Interface Name(vpn0_inet_if_name)	<input type="text" value="ge0/0"/>
IPv4 Address(vpn0_inet_if_ip_add)	<input type="text" value="100.100.100.30/24"/>
Color(vpn0_inet_if_color)	<input type="text" value="public-internet"/>
Hostname	<input type="text" value="vEdge30"/>
System IP	<input type="text" value="10.255.255.31"/>
Site ID	<input type="text" value="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
TECT          SOURCE TLOC      REMOTE TLOC          DST PUBLIC          DST PUBLIC          DE
SYSTEM IP     SITE ID STATE      COLOR      COLOR      SOURCE IP          IP          PORT      ENCAP  MU
LTIPLER  INTERVAL (msec)  UPTIME      TRANSITIONS
-----
10.255.255.11 1      up    0:04:19:13 default    public-internet 100.100.100.30    100.100.100.10    12386    ipsec  7
1000
10.255.255.12 1      up    0:04:19:14 default    public-internet 100.100.100.30    100.100.100.11    12386    ipsec  7
1000
10.255.255.21 20     up    0:00:26:43 default    public-internet 100.100.100.30    100.100.100.20    12386    ipsec  7
1000
10.255.255.41 40     up    4:21:24:13 default    public-internet 100.100.100.30    100.100.100.40    12347    ipsec  7
1000
10.255.255.51 50     up    4:16:45:15 default    public-internet 100.100.100.30    100.100.100.50    12347    ipsec  7
1000
vEdge30#
```

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

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

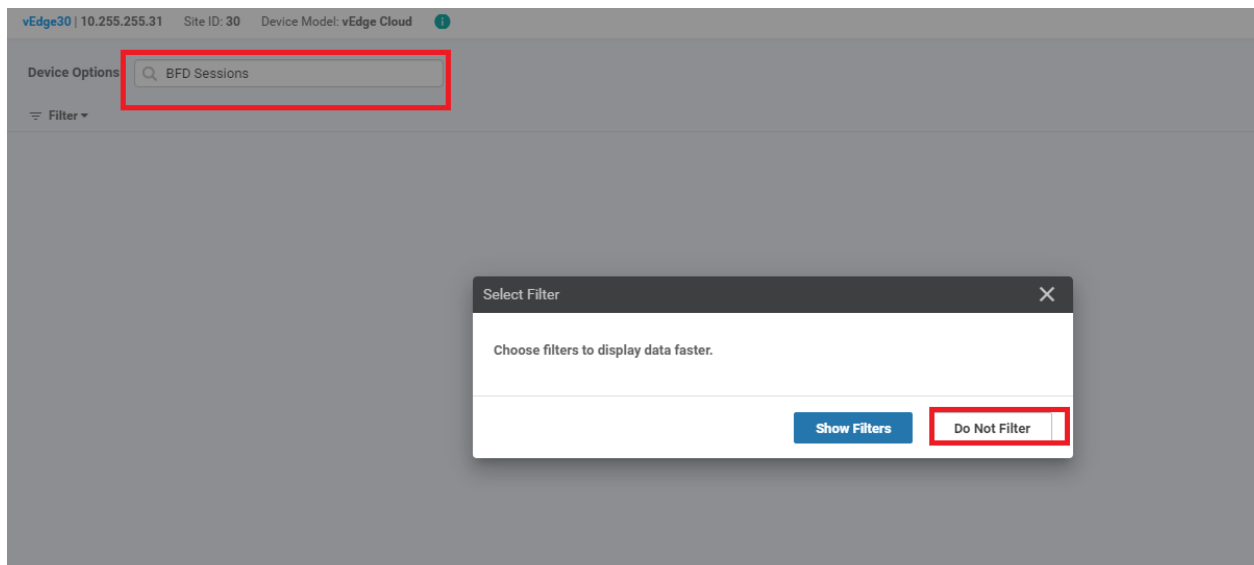
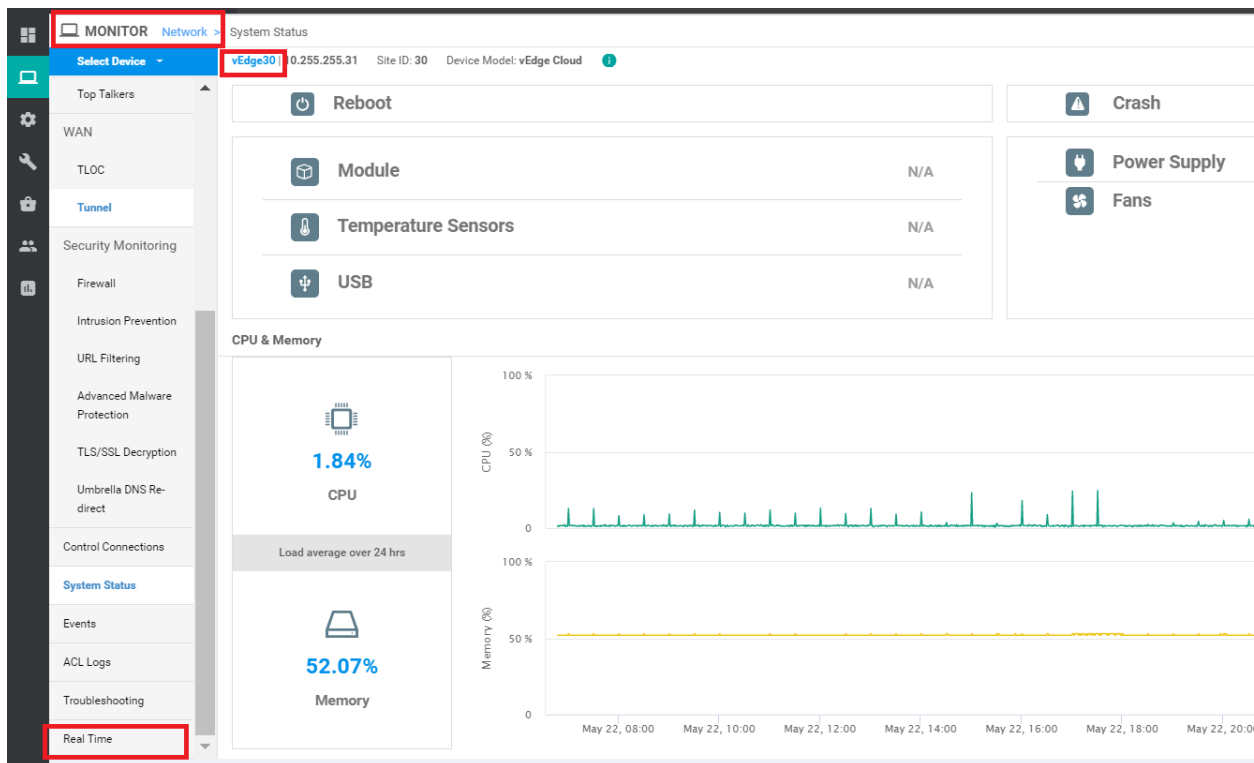
```
vEdge30# show bfd sess
```

TECT	TX	SOURCE TLOC	REMOTE TLOC	DST PUBLIC
SYSTEM IP	SITE ID	STATE	COLOR	COLOR
LTPLIER	INTERVAL(msec)	UPTIME	TRANSITIONS	SOURCE IP
				IP
10.255.255.11	1	up	public-internet	public-internet
1000		0:00:00:49	0	100.100.100.30
10.255.255.11	1	up	mpls	mpls
1000		0:00:00:30	0	192.0.2.14
10.255.255.12	1	up	public-internet	public-internet
1000		0:00:00:49	0	100.100.100.30
10.255.255.12	1	up	mpls	mpls
1000		0:00:00:30	0	192.0.2.14
10.255.255.21	20	up	public-internet	public-internet
1000		0:00:00:49	0	100.100.100.30
10.255.255.22	20	up	mpls	mpls
1000		0:00:00:30	0	192.0.2.14
10.255.255.41	40	up	public-internet	public-internet
1000		0:00:00:50	0	100.100.100.30
10.255.255.51	50	up	public-internet	public-internet
1000		0:00:00:49	0	100.100.100.30
10.255.255.52	50	up	mpls	mpls
1000		0:00:00:30	0	192.0.2.14

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

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	ipsec	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

Site 40 missing

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-CBA8-415C...	Token - fc40de6570e72...	NA	NA	--	--	--	CLI	--	...
🔒	CSR1000v	CSR-D6D839FC-C383-8B55-7E9D-7CD...	Token - f28b5ab97898...	NA	NA	--	--	--	CLI	--	...
🔒	CSR1000v	CSR-834E40DC-E358-8DE1-0E81-76E59...	FA1F272A	NA	NA	cEdge50	10.255.255.51	50	vManage	cEdge-single-uplink	In S ...
🔒	CSR1000v	CSR-D405F5BA-B975-8944-D1A3-2E08...	Token - e78aaefc1ebd2...	NA	NA	--	--	--	CLI	--	...
🔒	CSR1000v	CSR-D1837F36-6A1A-1850-7C1C-E1C6...	FB7DC382	NA	NA	cEdge51	10.255.255.52	50	vManage	cEdge-single-uplink	In S ...
🔒	CSR1000v	CSR-5E992295-1362-0DB6-EEF8-25CC...	Token - 1da14330e171...	NA	NA	--	--	--	CLI	--	...
🔒	CSR1000v	CSR-04F9482E-44F0-EADC-D30D-60C0...	63201C50	NA	NA	cEdge40	10.255.255.41	40	vManage	cEdge_dualuplink_devte...	In S ...
🔒	vEdge Cloud	e474c5fd-8ce7-d376-7cac-ba950b2e91...	7175AE0F	NA	NA	DC-vEdge1	10.255.255.11	1	vManage	DCvEdge_dev_temp	In S ...
🔒	vEdge Cloud	0cdd4f0e-f2f1-f675-866c-469966cda1c3	7DA605F5	NA	NA	DC-vEdge2	10.255.255.12	1	vManage	DCvEdge_dev_temp	In S ...
🔒	vEdge Cloud	b7fd7295-58df-7671-4914-6fe2edf11609	297D60DD	NA	NA	vEdge20	10.255.255.21	20	vManage	vEdge_Site20_dev_temp	In S ...
🔒	vEdge Cloud	dde90ff0-dc62-77e6-510f-08d96608537d	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-26217DAD-1B63-80DE-11C9-125F...	Token - 8dc7b557b60d...	NA	NA	--	--	--	CLI	--	...
🔒	CSR1000v	CSR-F960E020-87C9-887F-46A8-F4537...	Token - 50cc04634ac4...	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

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: Mark as Optional Row

Gateway: Next Hop Null 0 VPN DHCP

Next Hop: **1 Next Hop**

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

+ Add Next Hop

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 Mark as Optional Row

Gateway Next Hop Null 0 VPN 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**

IPv4 ROUTE

+ New IPv4 Route

Optional	Prefix	Gateway	Selected Gateway Configuration
<input type="checkbox"/>	0.0.0.0/0	Next Hop	2

IPv6 ROUTE

+ New IPv6 Route

Optional	Prefix	Gateway	Selected Gateway Configuration
----------	--------	---------	--------------------------------

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(in
	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	Total		
cEdge_dualuplink_devtemp	1	124	exit-address-family
		125	!
		126	!
		127	ip arp proxy disable
		128	no ip finger
		129	no ip rcmd rcp-enable
		130	no ip rcmd rsh-enable
		131	no ip domain lookup
		132	no ip dhcp use class
		133	ip multicast route-limit 2147483647
		134	ip route 0.0.0.0 0.0.0.0 100.100.100.1
		135	ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 192.168.0.1
		136	ip bootp server
		137	no ip source-route
		138	no ip http server
		139	no ip http secure-server
		140	no ip http ctc authentication
		141	no ip igmp ssm-map query dns
		142	interface GigabitEthernet1
		143	no shutdown
		144	arp timeout 1200
		145	vrf forwarding Mgmt-intf
		146	ip address 192.168.0.40 255.255.255.0
		147	no ip redirects
		148	ip mtu 1500
		149	mtu 1500
		150	negotiation auto
		151	exit
		152	interface GigabitEthernet2
		153	no shutdown
		154	arp timeout 1200
		124	exit-address-family
		125	!
		126	!
		127	ip arp proxy disable
		128	no ip finger
		129	no ip rcmd rcp-enable
		130	no ip rcmd rsh-enable
		131	no ip domain lookup
		132	no ip dhcp use class
		133	ip multicast route-limit 2147483647
		134	ip route 0.0.0.0 0.0.0.0 100.100.100.1
		135	ip route 0.0.0.0 0.0.0.0 192.1.2.17
		136	ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 192.168.0.1
		137	ip bootp server
		138	no ip source-route
		139	no ip http server
		140	no ip http secure-server
		141	no ip http ctc authentication
		142	no ip igmp ssm-map query dns
		143	interface GigabitEthernet1
		144	no shutdown
		145	arp timeout 1200
		146	vrf forwarding Mgmt-intf
		147	ip address 192.168.0.40 255.255.255.0
		148	no ip redirects
		149	ip mtu 1500
		150	mtu 1500
		151	negotiation auto
		152	exit
		153	interface GigabitEthernet2
		154	no shutdown
		155	arp timeout 1200

Device list (Total: 1 devices)
Filter/Search

CSR-04F9482E-44F0-E4DC-D30D-60C806F73F2
cEdge40110255255.41

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

Total Rows: 16

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	...
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 MPL...	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 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 8:36:47 AM PDT	...
DC-vEdge_mgmt_int	MGMT interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	3	5	admin	23 May 2020 1:4	View Edit Change Device Models
DC-vEdge_MPLS	MPLS interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 1:4	Delete Copy
DC-vEdge_INET	INET interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 1:3	...
cedge_vpn0_single_uplink	cEdge VPN 0 Template for Single ...	Cisco VPN	CSR1000v	1	2	admin	18 May 2020 1:2	...
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	...
Site20_vpn0_int	VPN0 Interface for Site20 devices	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 5:48:54 AM PDT	...
DCvEdge-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	...

- 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
✕

Template Name

Description

cEdge VPN 0 Interface Template for devices with a dual uplink - MPLS

Copy

Cancel

- 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	
vEdge00_MPLS	MPLS interface for the Site30 vEd...	WAN Edge Interface	vEdge Cloud	1	1	admin	23 May 2020 6:32:26 AM PDT	...
vEdge00-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	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_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: Yes 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

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

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	...
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	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	View
cEdge-singleuplink	Single Uplink cEdge Device Te...	Feature	CSR1000v	11	2	admin	18 May 2020 1:33:13 PM PDT	In Sync	Delete
DCvEdge_dev_temp	Device template for the DCvE...	Feature	vEdge Cloud	11	2	admin	23 May 2020 1:55:53 AM PDT	In Sync	Copy

Attach Devices
Detach Devices
Export CSV
Change Device Values

- 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**

CONFIGURATION | TEMPLATES

Basic Information **Transport & Management VPN** Service VPN Additional Templates

Cisco OMP * Factory_Default_Cisco_OMP_Jpv46_Template Cisco Security * Default_Security_Cisco_V01

Transport & Management VPN

Cisco VPN 0 * cEdge_VPN0_dualLuplink

Cisco VPN Interface Ethernet cedge-vpn0-int-dual

Cisco VPN Interface Ethernet cedge-vpn0-int-dual_mpls

Additional Cisco VPN 0 Templ

- 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_dual_uplink

Cisco VPN Interface Ethernet cedge-vpn512-int-dual

Additional Cisco VPN 512 Tem

- Cisco VPN Interface Ethernet

Service VPN

Update Cancel

- 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**

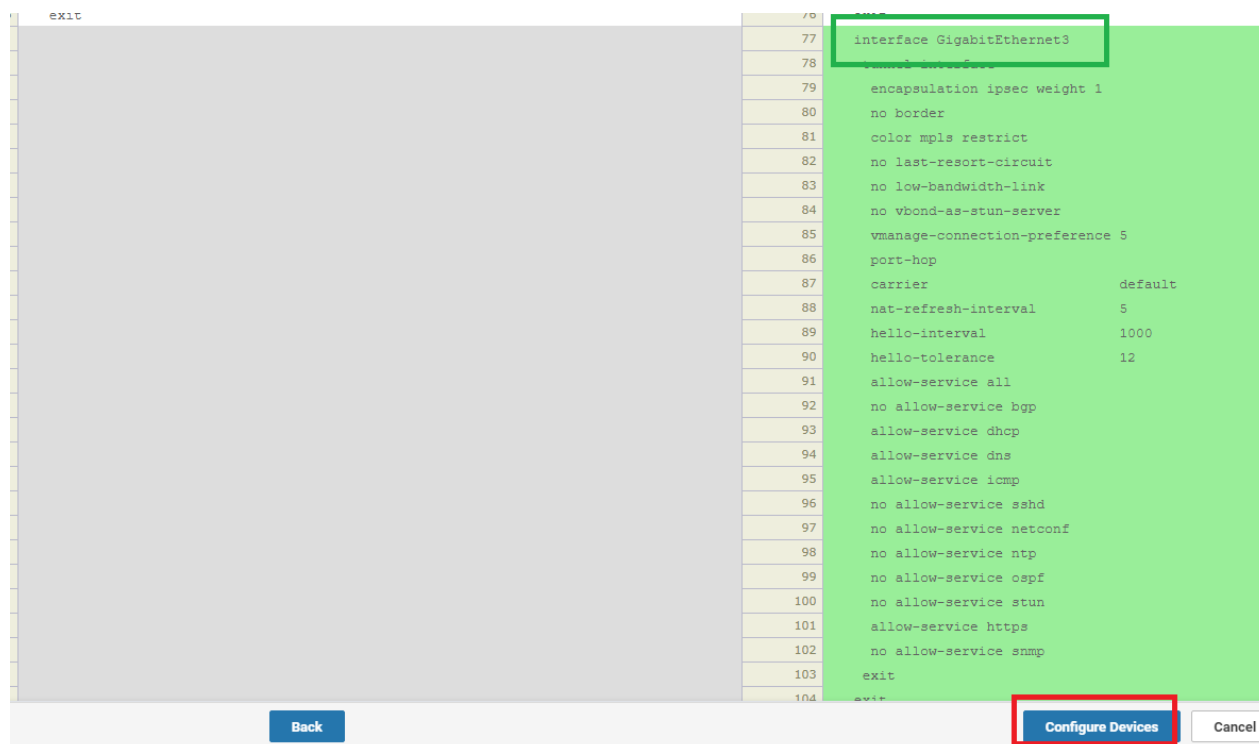
Search Options

Total Rows: 1

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
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**

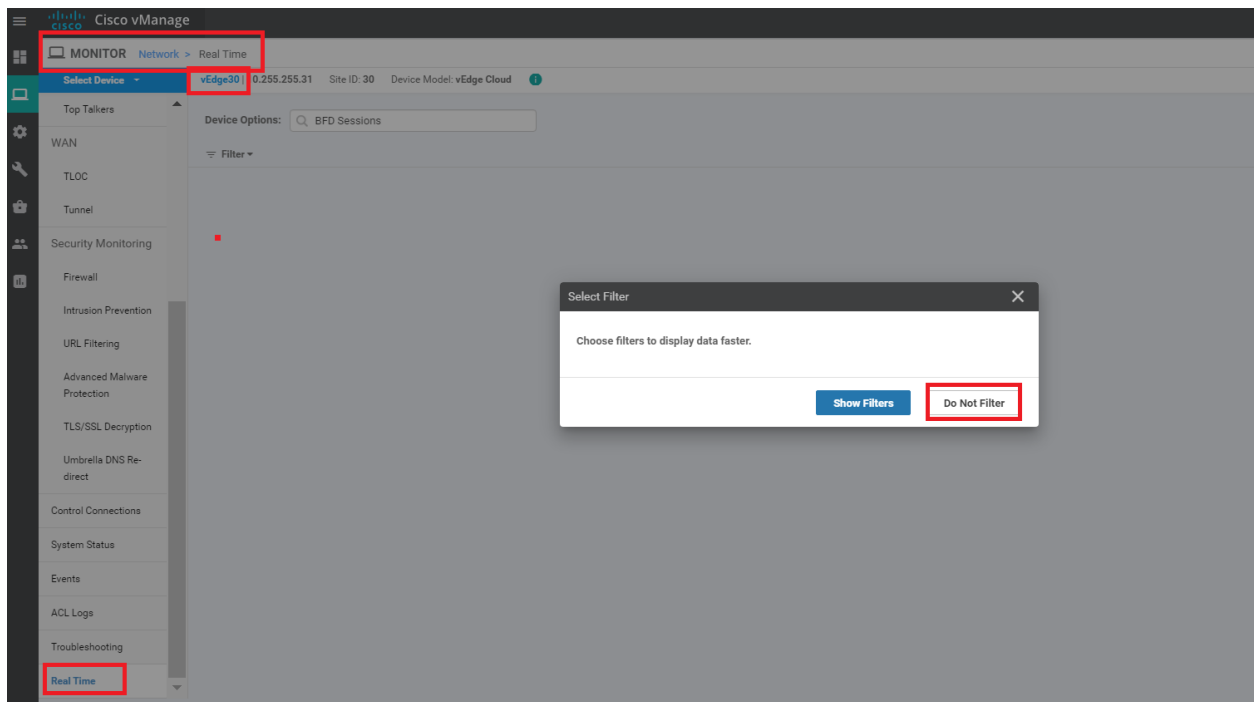


5. The configuration should be successful

Total Task: 1 | Success : 1

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template Co...	CSR-04F9482E-44F0-E4DC-D30D-...	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

Device Options: BFD Sessions

Filter

Search Options

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 for a Device Group. At the top, there is a 'Select Device' dropdown menu highlighted with a red box. Below it, the breadcrumb path is 'vEdge30 | 10.255.255.31 | Site ID: 30 | Device Model: vEdge Cloud'. The main content area is titled 'Device Group' and includes a search bar and a 'Sort by' dropdown set to 'Reachability'. A list of devices is displayed, with the first entry, 'cEdge40', highlighted by a red box. The 'cEdge40' entry shows the IP address 10.255.255.41, Site ID: 40, and is marked as 'Reachable'. Other devices listed include cEdge50, cEdge51, vEdge20, and vEdge21.

Device Name	IP Address	Site ID	Device Model	Version	Status
cEdge40	10.255.255.41	40	CSR1000v	17.02.01r.0.32	Reachable
cEdge50	10.255.255.51	50	CSR1000v	17.02.01r.0.32	Reachable
cEdge51	10.255.255.52	50	CSR1000v	17.02.01r.0.32	Reachable
vEdge20	10.255.255.21	20	vEdge Cloud	20.1.1	Reachable
vEdge21	10.255.255.22	20	vEdge Cloud	20.1.1	Reachable

The screenshot shows the Cisco vManage MONITOR page for the device 'cEdge40'. The breadcrumb path is 'MONITOR | Network > Real Time | cEdge40 | 10.255.255.41 | Site ID: 40 | Device Model: CSR1000v'. The 'Device Options' section is set to 'BFD Sessions'. A 'Select Filter' dialog box is open in the foreground, with the text 'Choose filters to display data faster.' and two buttons: '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 web interface titled "Site Devices Health: Full WAN Connectivity". It features a search bar and a table with 8 rows of data. The table columns are: Hostname, Reachability, System IP, Site ID, BFD Sessions, and Last Updated. All devices listed are in a "reachable" state.

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

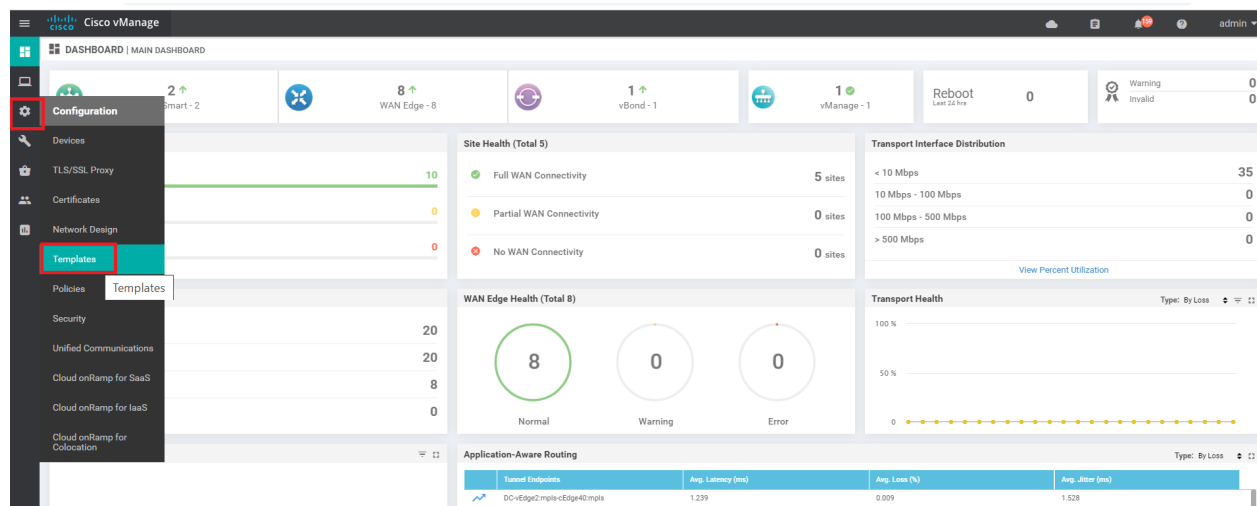
We will now create and apply Templates to the vSmarts. This will allow us to enforce Centralized Policies, which will be used in the following sections.

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**

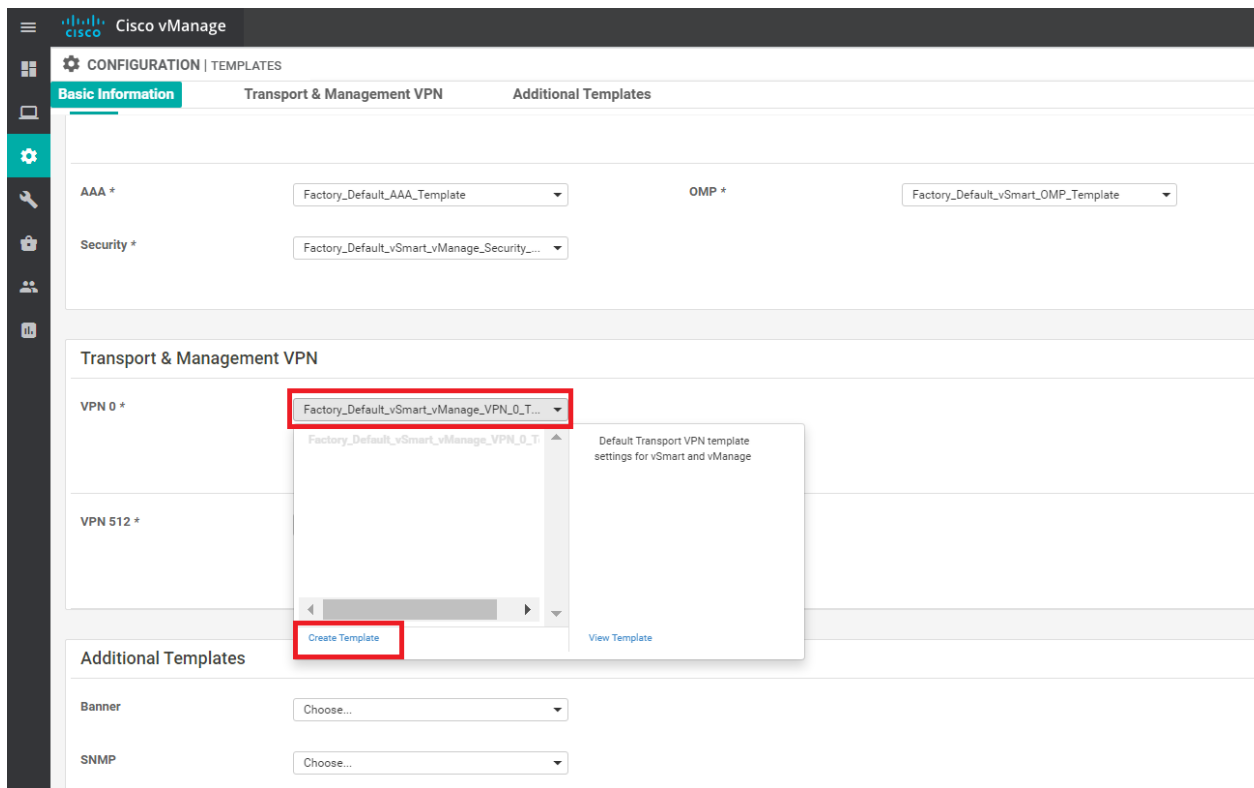
The screenshot shows the Cisco vManage interface for creating templates. The 'Device' tab is active. A red box highlights the 'Create Template' button, which has a dropdown menu open. The dropdown menu contains two options: 'From Feature Template' and 'CLI Template'. Below the dropdown is a search bar with a magnifying glass icon and a 'Search Options' dropdown. Below the search bar is a table of existing 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 form fields for creating a template. The 'Device Model' dropdown is set to 'vSmart'. The 'Template Name' field contains 'vSmart-dev-temp'. 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



5. Populate the details in the template as given below

Section	Field	Global or Device Specific (drop down)	Value
	Template Name	NA	<i>vSmart-VPN0</i>
	Description	NA	<i>VPN0 Template for the vSmarts</i>
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).

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > VPN

Device Type vSmart

Template Name vSmart-VPN0

Description VPN0 Template for the vSmarts

Basic Configuration DNS IPv4 Route IPv6 Route

BASIC CONFIGURATION

VPN VPN 0

Name

DNS


Primary DNS Address 10.2.1.5

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 

Gateway Next Hop Null 0 VPN

Next Hop **+ Add Next Hop**

7. Click on **Add Next Hop** again

Next Hop ×



No Next Hop added, add your first Next Hop

Add Next Hop

Add Cancel

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"/>

9. Click on **Add** again in the IPv4 Route section to add the route

IPv4 ROUTE

Mark as Optional Row ⓘ

Prefix

Gateway Next Hop Null 0 VPN

Next Hop [1 Next Hop](#)

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			

Save
Cancel

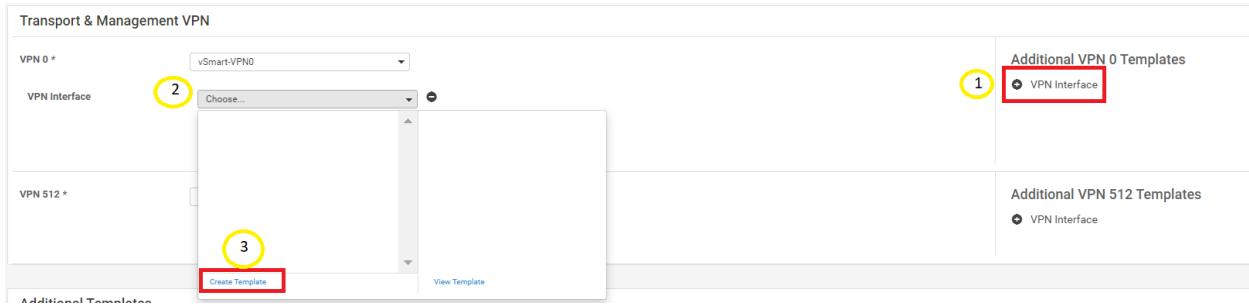
This completes the configuration of the Main VPN 0 Template. Continue with configuring the VPN 0 Interface Template.

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	<i>vSmart-VPN0-Int</i>
	Description	NA	<i>VPN0 Interface for vSmarts</i>
Basic Configuration	Shutdown	Global	No
Basic Configuration	Interface Name	Global	eth0
Basic Configuration - IP Configuration	IPv4 Address	Device Specific	<i>vpn0_if_ip_address</i>
Tunnel	Tunnel Interface	Global	On
Tunnel	Color	Global	public-internet
Tunnel - Allow Service	All	Global	On

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 On Off

Color public-internet

Allow Service

All On Off

DHCP On Off

DNS On Off

ICMP On Off

SSH On Off

NETCONF On Off

NTP On Off

STUN On Off

Save Cancel

This completes the configuration of the VPN 0 Interface Template.

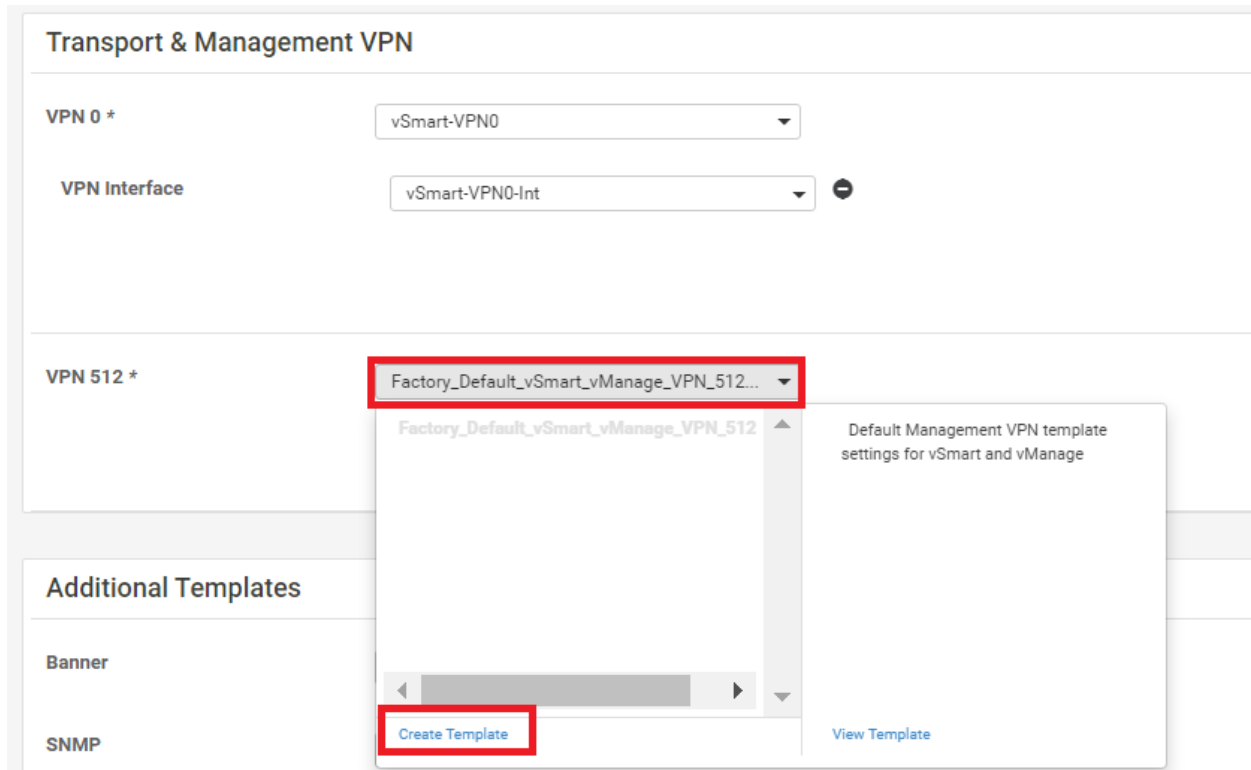
Make sure the VPN 0 and VPN 0 Interface Templates just created are selected from the drop down in the Device Template we're building before proceeding to create the VPN 512 Templates.

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	<i>vSmart-VPN512</i>
	Description	NA	<i>VPN512 Template for the vSmarts</i>
Basic Configuration	VPN	Global	VPN 512

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).

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: VPN 512

Name:

DNS

Primary DNS Address: 10.2.1.5

Secondary DNS Address: 10.2.1.6

[+ New Host Mapping](#)

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**

IPV4 ROUTE

[+ New IPv4 Route](#)


Prefix

Gateway Next Hop Null 0 VPN

Next Hop [+ Add Next Hop](#)

4. Click on **Add Next Hop** again

Next Hop ✕



No Next Hop added, add your first Next Hop

[Add Next Hop](#)

[Add](#) [Cancel](#)

5. Enter the address as *192.168.0.1*, a Global value. Click on **Add**

Next Hop

Address Distance

192.168.0.1 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

Mark as Optional Row

Prefix 0.0.0.0/0

Gateway Next Hop Null 0 VPN

Next Hop 1 Next Hop

Add Cancel

Optional	Prefix	Gateway	Selected Gateway Configuration	Action
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

VPN 0 * vSmart-VPN0 Additional VPN 0 Ten
 VPN Interface vSmart-VPN0-Int VPN Interface

VPN 512 * vSmart-VPN512 Additional VPN 512 T
 VPN Interface Choose... VPN Interface
 vSmart-VPN0-Int
 Create Template View Template

Additional Templates
 Banner
 SNMP

8. Enter the details as shown below and click on **Save**

Section	Field	Global or Device Specific (drop down)	Value
	Template Name	NA	<i>vSmart-vpn512-int</i>
	Description	NA	<i>VPN512 Interface Template for the vSmarts</i>
Basic Configuration	Shutdown	Global	No
Basic Configuration	Interface Name	Global	eth1
Basic Configuration - IP Configuration	IPv4 Address	Device Specific	<i>vpn512_if_ip_address</i>
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

Additional VPN 0 Templates

- VPN Interface

VPN 512 * vSmart-VPN512

VPN Interface vSmart-vpn512-int

Additional VPN 512 Templat

- VPN Interface

Additional Templates

Create Cancel

We have completed the Device Template (and consequently the Feature Template) configuration for our vSmarts.

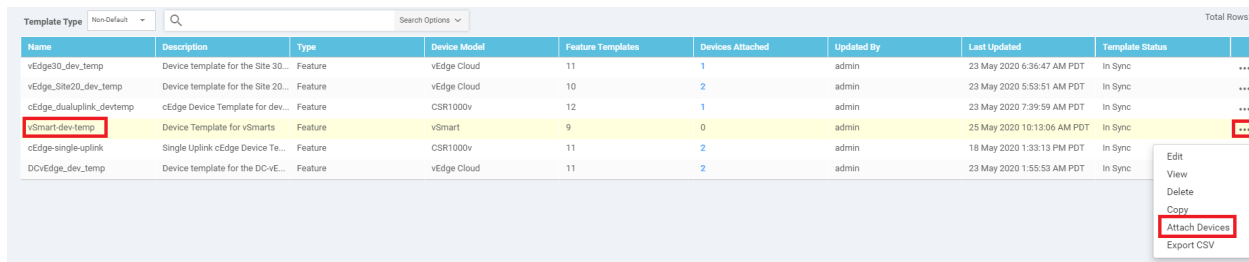
Task List

- [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

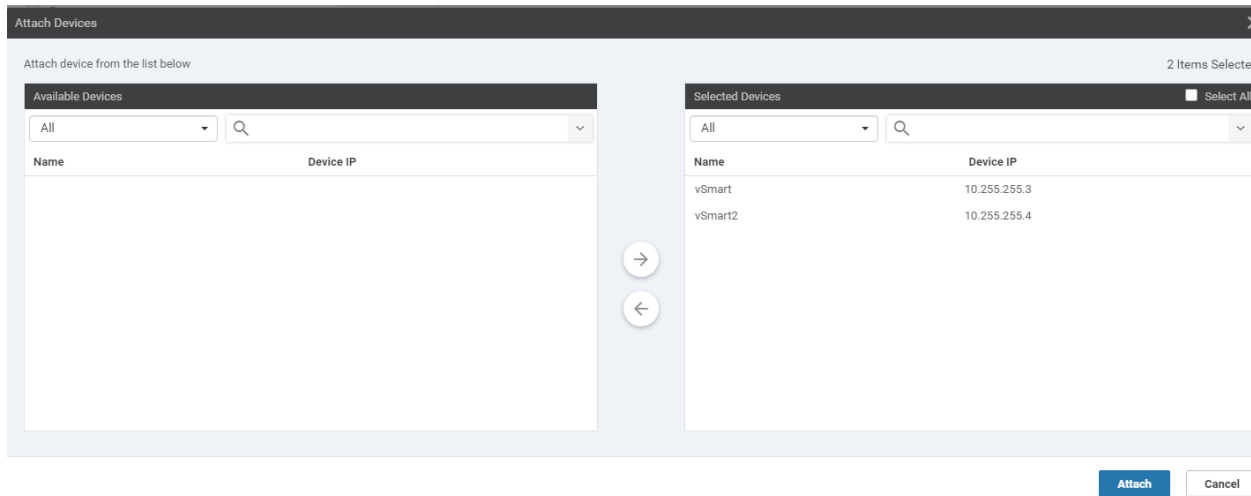
Our Device Template for the vSmarts are set up and we now need to attach them to the Template.

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**

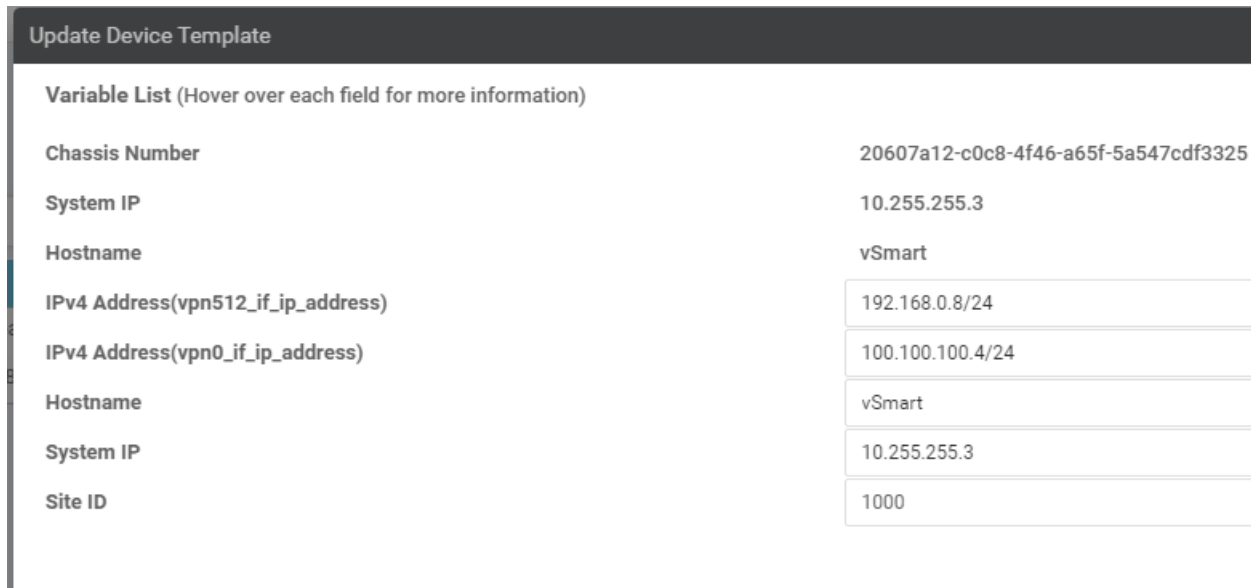


Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
vEdge30_dev_temp	Device template for the Site 30...	Feature	vEdge Cloud	11	1	admin	23 May 2020 6:36:47 AM PDT	In Sync	...
vEdge_Site20_dev_temp	Device template for the Site 20...	Feature	vEdge 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	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

- 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 a web interface for configuration management. On the left, a 'Device list (Total: 2 devices)' is displayed with two entries: '20607a12-c0c8-4f46-a65f-5a547edf3325' and '7f332491-cb6f-4843-8bf5-060f90df8dec'. The first entry is highlighted with a red box. The main area shows a 'Local Configuration vs. New Configuration' comparison table. The 'Config Diff' button is highlighted with a red box. A yellow notification banner at the top right states: 'Configure' action will be applied to 2 device(s) attached to 1 device template(s). The comparison table lists various configuration parameters and their values, with some rows highlighted in red and green.

Local Configuration vs. New Configuration	
1	1 system
2	2 device-model vsmart
3	3 chassis-number 20607a12-c0c8-4f46-a65f-5a547edf3325
4	4 host-name vSmart
5	5 system-ip 10.255.255.3
6	6 site-id 1000
7	7 admin-tech-on-failure
8	8 sp-organization-name swat-edwanlab
9	9 organization-name swat-edwanlab
10	10 vbond 100.100.100.3 port 12346
11	11 aaa
12	12 auth-order local radius tacacs

- 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		
4	host-name vSmart	3	host-name vSmart
5	system-ip 10.255.255.3	4	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		
27	!		
28	user admin	26	user admin
29	password \$6\$VMTXKLxYT/tQI9eLs129vrK39/qFGpf0LnDht2CzJwqI/FXzwDso7zXXEr9xa3vB5.kgf7zrVZ/mY43OpXBnamIvZ06iVaNZpGOLV/	27	password \$6\$siwKBC==\$wI2lUa9BSreDPI6gB8sl4E6EyiG6qnlABInrE96HJiKf6QRq1

6. Confirm the configuration change by clicking on the check box and then clicking 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.

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

Configuration | DEVICES

WAN Edge List **Controllers**

Configuration | Change Mode ▾

Search Options ▾

Total Rows: 4

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	-	-	dfeak3a5-66d2-4e50-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**

Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
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	CSR1000v	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	CSR1000v	1	1	admin	23 May 2020 7:15:33 AM PDT
INET interface for the Site30 vEdges	WAN Edge Interface	vEdge Cloud	1	1	admin	23 May 2020 6:27:24 AM PDT
vEdge VPN 512 Interface Template...	Cisco VPN Interface	CSR1000v	2	3	admin	18 May 2020 8:39:03 AM PDT
vEdge VPN 512 Template for Dual...	Cisco VPN	CSR1000v	2	3	admin	18 May 2020 8:35:47 AM PDT
VPN0 Template for the vSmarts	vSmart VPN	vSmart	1	2	admin	25 May 2020 9:51:02 AM PDT
cEdge VPN 0 Template for Dual Up...	Cisco VPN	CSR1000v	1	1	admin	23 May 2020 7:34:59 AM PDT
MGMT interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	3	5	admin	23 May 2020 1:49:11 AM PDT
MPLS interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 1:43:22 AM PDT
INET interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 1:39:02 AM PDT
cEdge VPN 0 Template for Single U...	Cisco VPN	CSR1000v	1	2	admin	18 May 2020 1:24:18 PM PDT
VPNS12 Template for the vSmarts	vSmart VPN	vSmart	1	2	admin	25 May 2020 10:07:03 AM PDT
cEdge VPN 0 Interface Template fo...	Cisco VPN Interface	CSR1000v	1	1	admin	18 May 2020 8:28:19 AM PDT
VPN0 Interface for Site20 devices	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 5:48:54 AM PDT
DC-Edge-vpn512	VPNS12 for the DC-vEdges	vEdge Cloud	3	5	admin	23 May 2020 1:25:54 AM PDT
DC-Edge-vpn0	VPN0 for the DC-vEdges INET and ...	vEdge Cloud	1	2	admin	23 May 2020 1:17:15 AM PDT
vSmart-vpn512-int	VPNS12 Interface Template for the...	vSmart Interface	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

ve

- 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**
- 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	<i>vedge-vpn10</i>
	Description	NA	<i>VPN 10 Template for</i>

				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 | 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

Enable TCP Optimization: On Off

DNS

Primary DNS Address (IPv4): 10.2.1.5

Secondary DNS Address (IPv4): 10.2.1.6

IPv4 | IPv6

Advertise OMP

IPv4 IPv6

BGP (IPv4) On Off

Static (IPv4) On Off

Connected (IPv4) On Off

OSPF External On Off

EIGRP On Off

LISP On Off

ISIS On Off

NETWORK AGGREGATE

Network (IPv4) On Off

Save Cancel

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**

Device Feature

Feature Template - Add Template

Select Devices

ve

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) VPN VPN Interface Bridge

WAN LAN

VPN Interface Cellular VPN Interface Ethernet VPN Interface GRE

WAN Management | WAN | LAN WAN

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: vedge-vpn10-int

Description: VPN 10 Interface Template for vEdges

Basic Configuration | Tunnel | NAT | VRRP | ACL/QoS | ARP | 802.1X | Advanced

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name:

Description:

IPv4 IPv6

Dynamic Static

IPv4 Address:

Secondary IP Address (Maximum: 4) [Add](#)

[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	
Site30-vpn0	VPN0 for the Site30 vEdges	WAN Edge VPN	vEdge Cloud	1	1	admin	23 May 2020 6:25:48 AM PDT	...
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	...
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	...
cedge-vpn0-int-dualMpls	cEdge VPN 0 Interface Template fo...	Cisco VPN Interface	CSR1000v	1	1	admin	23 May 2020 7:15:33 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_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_dual_uplink	cEdge VPN 0 Template for Dual Up...	Cisco VPN	CSR1000v	1	1	admin	23 May 2020 7:34:59 AM PDT	...
vedge-vpn10	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 Edit Change Device Models
vSmart-VPN512	VPN512 Template for the vSmarts	vSmart VPN	vSmart	1	2	admin	25 May 2020	Delete
DC-vEdge_MPLS	MPLS interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020	Copy
DC-vEdge_INET	INET interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020	
cEdge_VPN0_single_uplink	cEdge VPN 0 Template for Single U...	Cisco VPN	CSR1000v	1	2	admin	18 May 2020	
vSmart-VPN0_int	VPN0 interface for vSmarts	vSmart Interface	vSmart	1	9	admin	25 May 2020 9:49:00 AM PDT	...

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	...
vSmart-VPN0-Int	VPN0 Interface for vSmarts	vSmart interface	vSmart	1	2	admin	25 May 2020	View
cEdge-vpn0-int-single	cEdge VPN 0 Interface Template fo...	Cisco VPN Interface	CSR1000v	1	2	admin	18 May 2020	Edit
Site20-vpn0	VPN0 for the Site20 vEdges	WAN Edge VPN	vEdge Cloud	1	2	admin	23 May 2020	Change Device Models
DC-vEdge_MPLS	MPLS Interface for the DC-vEdges	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020	Delete
vedge-vpn20	VPN 10 Template for vEdges	WAN Edge VPN	vEdge Cloud	0	0	admin	25 May 2020 1:35:11 PM PDT	Copy

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:

Name:

Enhance ECMP Keying: On Off

Enable TCP Optimization: On Off

DNS

IPv4 | IPv6

Update Cancel

- 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: [vpn20_desc]

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](#)

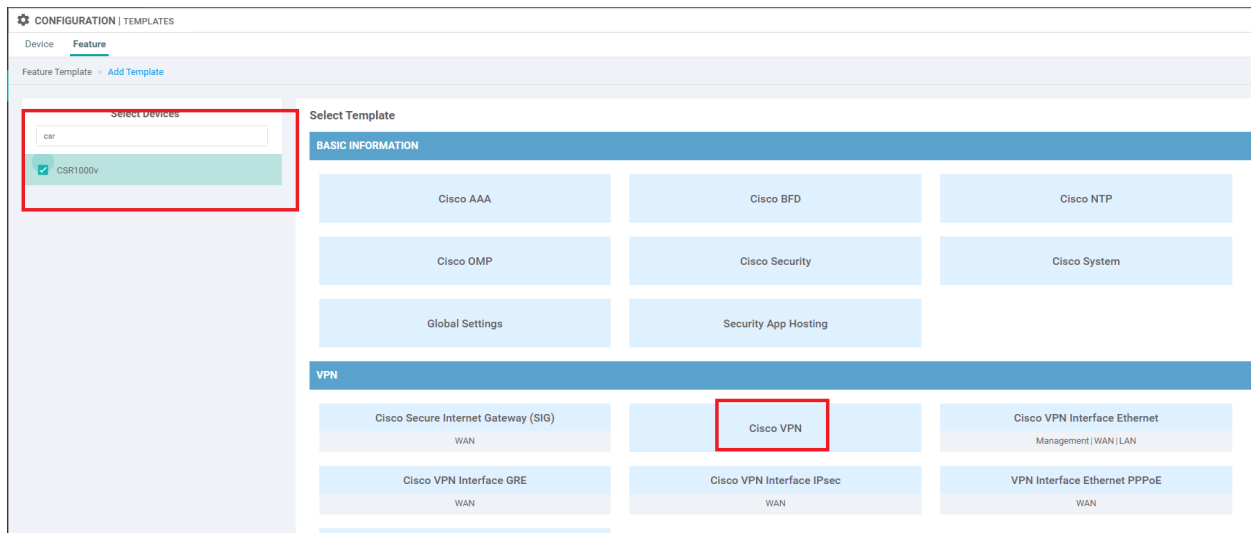
Task List

- 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: **edge-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: [dropdown]

Enhance ECMP Keying: [dropdown] On Off

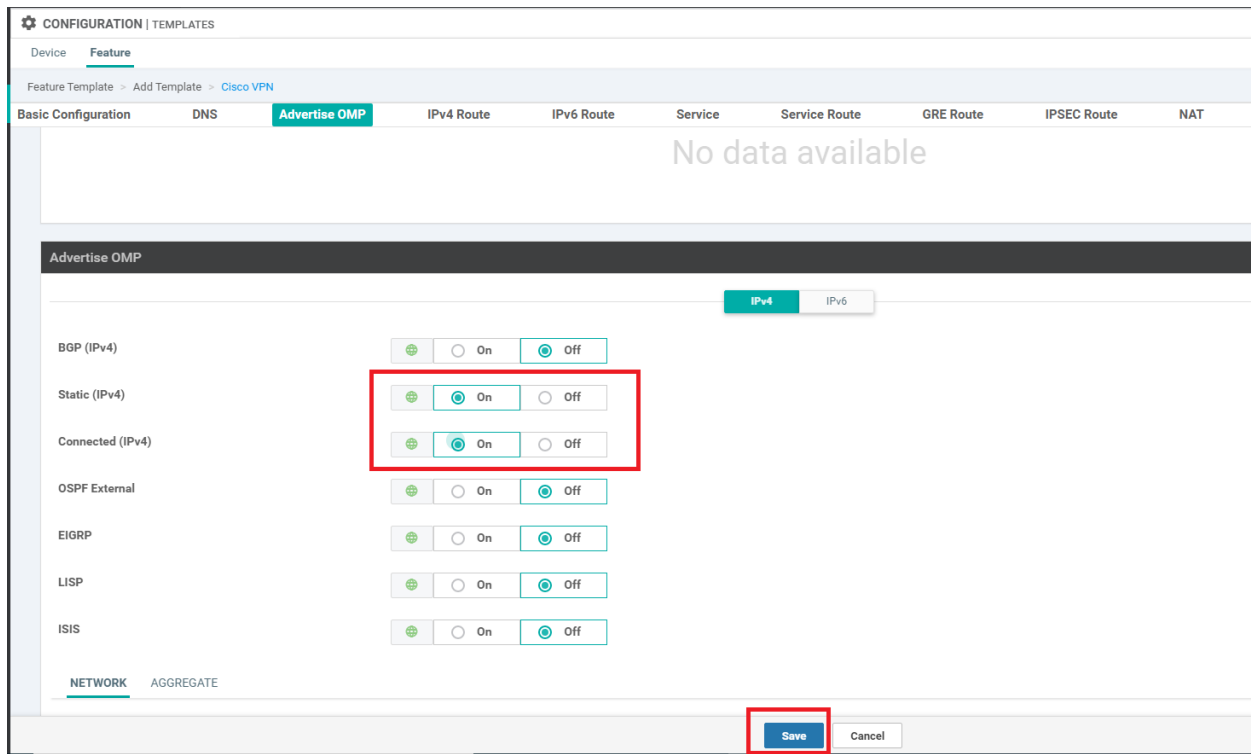
DNS

IPv4 | IPv6

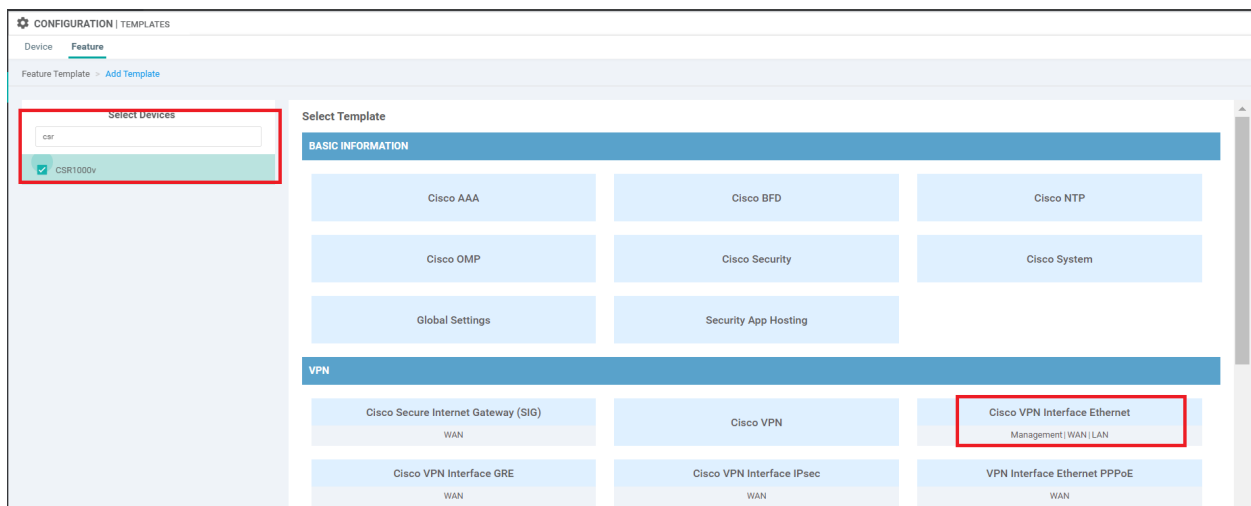
Primary DNS Address (IPv4): **10.2.1.5**

Secondary DNS Address (IPv4): **10.2.1.6**

[New Host Mapping](#)



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**



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: cedge-vpn10-int

Description: VPN 10 Interface Template for cEdges

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

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: [vpn10_if_name]

Description:

IPv4 IPv6

Dynamic Static

IPv4 Address/ prefix-length: [vpn10_if_ipv4_address]

Secondary IP Address (Maximum: 4): [Add](#)

DHCP Helper:

[Save](#) [Cancel](#)

This completes the configuration of the VPN 10 Feature Templates for the cEdges.

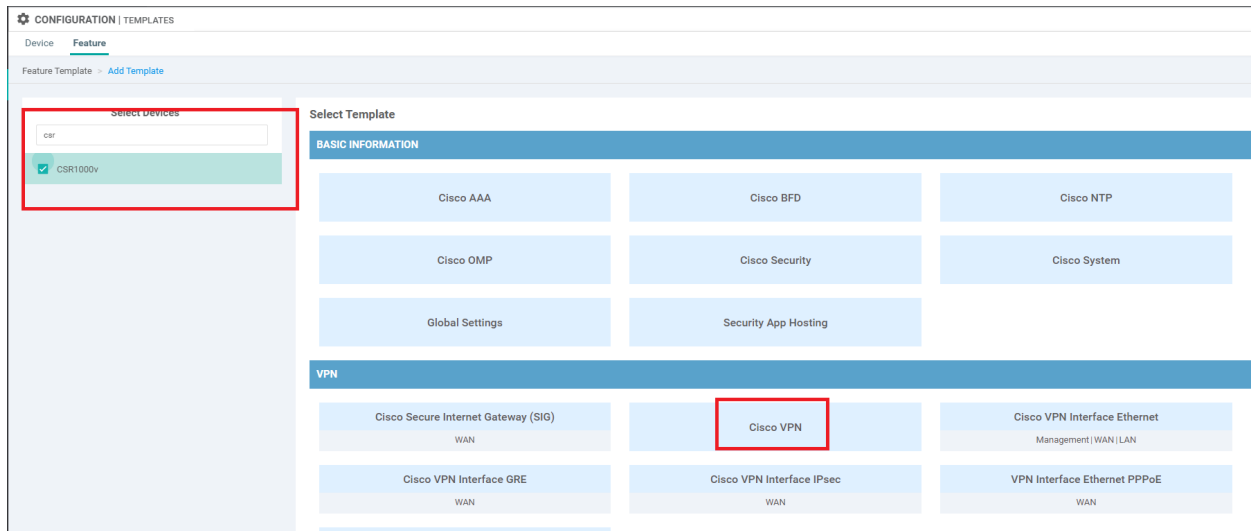
Task List

- ~~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).

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:

Name:

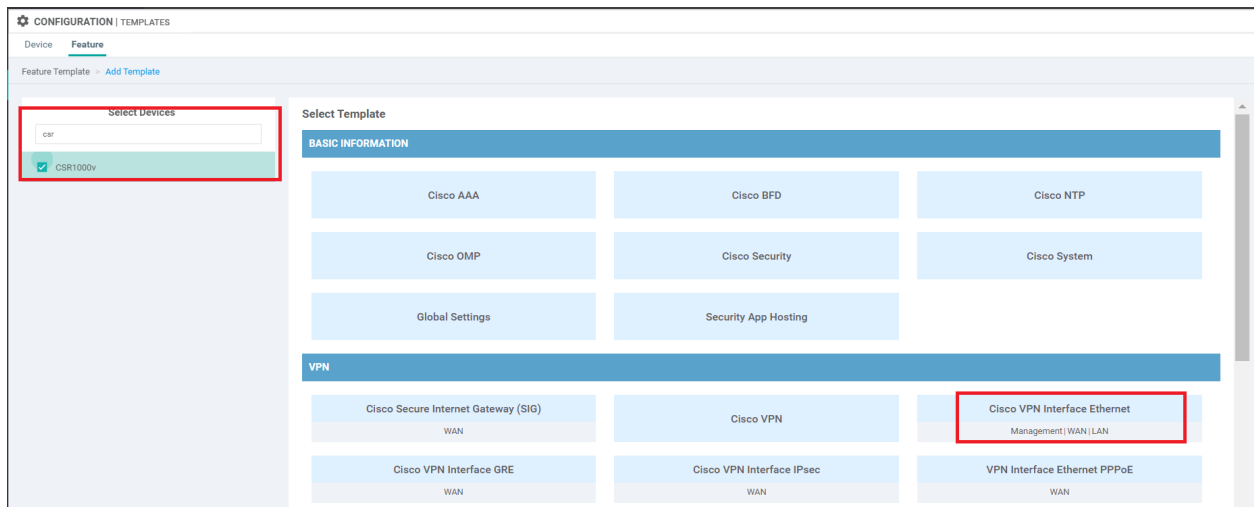
Enhance ECMP Keying: On Off

DNS

Primary DNS Address (IPv4):

Secondary DNS Address (IPv4):

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_ipv4_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

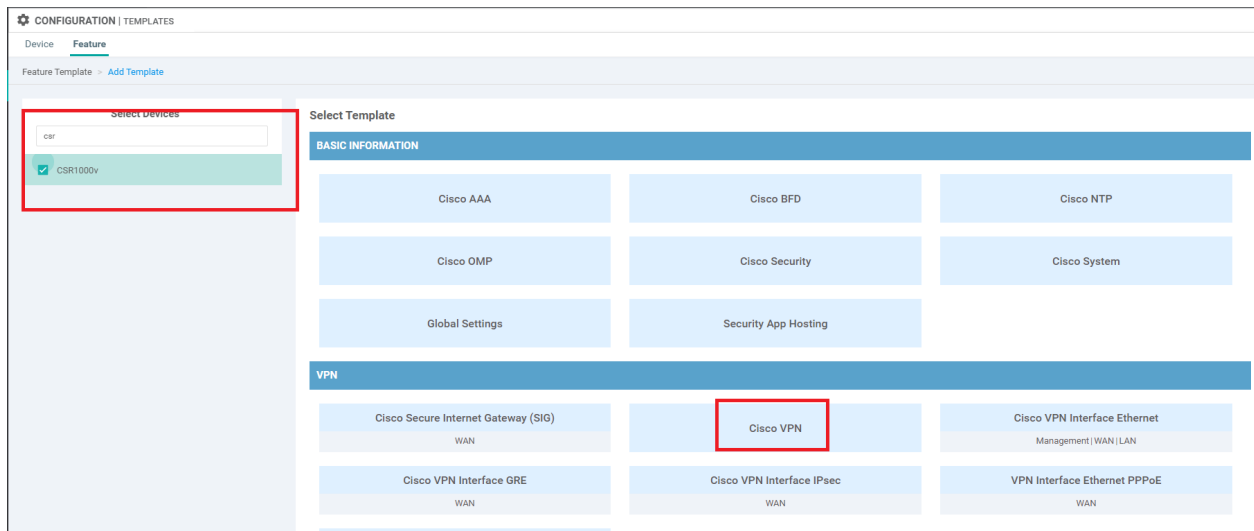
- [Configuring the cEdge VPN 10 Feature Templates](#)
- [Configuring the cEdge VPN 20 Feature Templates](#)
- [Configuring the cEdge VPN 30 Feature Templates](#)

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).

CONFIGURATION | TEMPLATES

Device Feature

Feature Template Cisco VPN

Device Type CSR1000v

Template Name cedge-vpn30

Description VPN 30 Template for the cEdges

Basic Configuration DNS Advertise OMP IPv4 Route IPv6 Route Service Service Route GRE Route IPSEC Route NAT

BASIC CONFIGURATION

VPN 30

Name cedge-vpn30

Enhance ECMP Keying Off

DNS

IPv4 IPv6

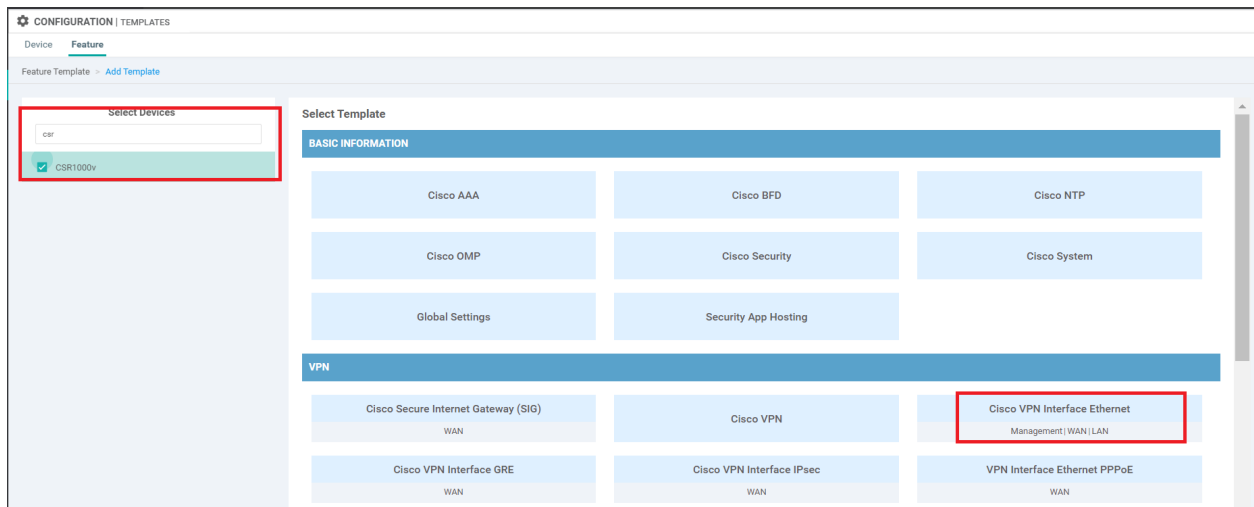
Primary DNS Address (IPv4) 10.2.1.5

Secondary DNS Address (IPv4) 10.2.1.6

New Host Mapping

Update Cancel

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

CONFIGURATION | TEMPLATES

Device Feature

Create Template

Template Type: Non-Default

Total Rows: 6

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
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	...

- Edit
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

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**

CONFIGURATION | TEMPLATES

Basic Information Transport & Management VPN

VPN Interface DCvEdge_MPLS

VPN 512+ DCvEdge-vpn512

VPN Interface DCvEdge_mgmt_int

Service VPN

0 Rows Selected Add VPN Remove VPN

Available VPN Templates

ID	Template Name
6fd47ee6-61c1-4b02-9b3e-439f5c423b74	vedge-vpn20

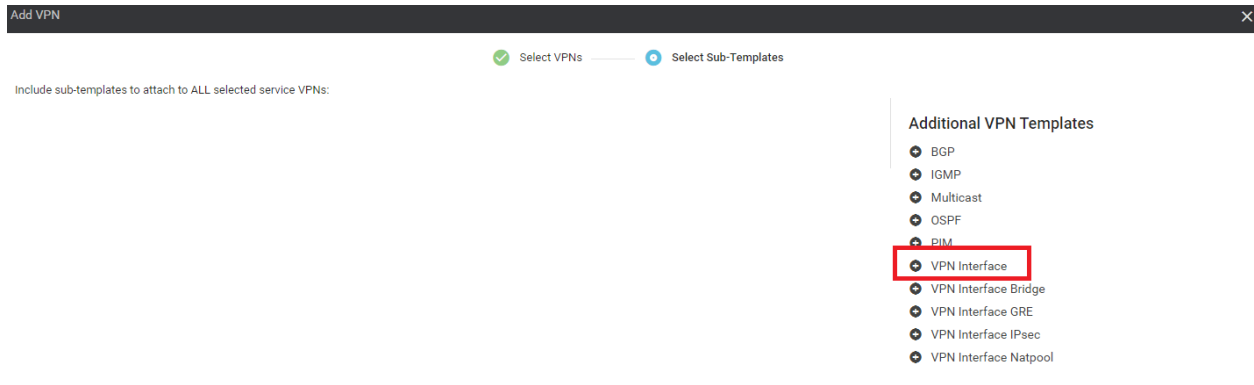
Selected VPN Templates

ID	Template Name
e9acf67d-aad6-4913-8f0a-84e255b4b033	vedge-vpn10

Create VPN Template

Next CANCEL

3. Under **Additional VPN Templates** on the left-hand side, click on **VPN Interface**



The screenshot shows a window titled "Add VPN" with a close button (X) in the top right corner. Below the title bar, there are two tabs: "Select VPNs" (which is active and has a green checkmark) and "Select Sub-Templates" (which is inactive and has a blue circle). Below the tabs, there is a text label: "Include sub-templates to attach to ALL selected service VPNs:". To the right of this label is a list titled "Additional VPN Templates". The list contains the following items, each with a plus icon to its left: BGP, IGMP, Multicast, OSPF, PIM, VPN Interface (highlighted with a red box), VPN Interface Bridge, VPN Interface GRE, VPN Interface IPsec, and VPN Interface Natpool.

4. Choose the *vedge-vpn10-int* template from the drop down and click on **Add**.

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 VPNs — Select Sub-Templates

Select one or more Service VPNs to add:

Available VPN Templates

Search

ID	Template Name
----	---------------

Selected VPN Templates

Search

ID	Template Name
6fd47ee6-61c1-4b02-9b3e-439f5c423b74	vedge-vpn20

→

←

Create VPN Template **Next** CANCEL

6. Click on **VPN Interface** under **Additional VPN Templates** and select the *vedge-vpn20-int* template from the drop down. Click on **Add**

Add VPN ✕

✔ Select VPNs ⊕ Select Sub-Templates

Include sub-templates to attach to ALL selected service VPNs:

VPN Interface: ⊖ ⊕ Sub-Templates ⌵

Additional VPN Templates

- ⊕ BGP
- ⊕ IGMP
- ⊕ Multicast
- ⊕ OSPF
- ⊕ PIM
- ⊕ VPN Interface
- ⊕ VPN Interface Bridge
- ⊕ VPN Interface GRE
- ⊕ VPN Interface IPsec
- ⊕ VPN Interface Natpool

7. Make sure the Device Template **Service VPN** section looks as below, and click on **Update**

CONFIGURATION | TEMPLATES

Basic Information **Transport & Management VPN** Service VPN Additional Templates

VPN Interface: ⊖

VPN 512 *

VPN Interface: ⊖

Service VPN

0 Rows Selected ⊕ Add VPN ⊖ Remove VPN

Search Options ⌵

☐	ID	Template Name	Sub-Templates
<input type="checkbox"/>	e9acf7d-aad6-4913-8f0a-84e255b4b033	vedge-vpn10	VPN Interface
<input type="checkbox"/>	6fd47ee6-61c1-4b02-9b3e-439f5c423b74	vedge-vpn20	VPN Interface

Additional Templates

Banner:

Update Cancel

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)

e474c5fd-8ea7-d376-7c9e-be950b2e9159
DC-vEdge1110.255.255.11

0cdd4f0e-f2f1-fe75-866c-469966cda1c3
DC-vEdge2110.255.255.12

[Configure Device Rollback Timer](#)

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	vpn 512
93	dns 10.2.1.5 primary
94	dns 10.2.1.6 secondary

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	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	omp
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	omp
112	advertise connected
113	advertise static
114	!
115	!
116	vpn 512
117	dns 10.2.1.5 primary
118	dns 10.2.1.6 secondary

[Back](#)
[Configure Devices](#)
[Cancel](#)

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](#)

- ### 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**

Service VPN

0 Rows Selected **Add VPN** **Remove VPN**

Search Search Options ▾

ID	Template Name	Sub-Templates
<input type="checkbox"/> e9acfe7d-aad6-4913-8f0a-84e255b4b033	vedge-vpn10	VPN Interface
<input type="checkbox"/> 6fd47ee6-61c1-4b02-9b3e-439f5c423b74	vedge-vpn20	VPN Interface

Additional Templates

Banner

Policy

SNMP

Security Policy

Bridge Bridge ▾

Update

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

CONFIGURATION | TEMPLATES

Device Template | vEdge_Site20_dev_temp

Search Options

Total Rows: 2

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-e914-4fa2edff1609	10.255.255.21	vEdge20	ge0/3	10.20.20.2/24	ge0/2	10.20.10.2/24	192.168...
2	dde90ff0-dc62-7766-510f-08d96608537d	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

0 Rows Selected [Add VPN](#) [Remove VPN](#)

Search Options

ID	Template Name	Sub-Templates
<input type="checkbox"/> e9acf7d-aad6-4913-8f0a-84e255b4b033	vedge-vpn10	VPN Interface
<input type="checkbox"/> 6fd47ee6-61c1-4b02-9b3e-439f5c423b74	vedge-vpn20	VPN Interface

Additional Templates

Banner

Policy

SNMP

Security Policy

Bridge Bridge

[Update](#) [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

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
<input checked="" type="checkbox"/>	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

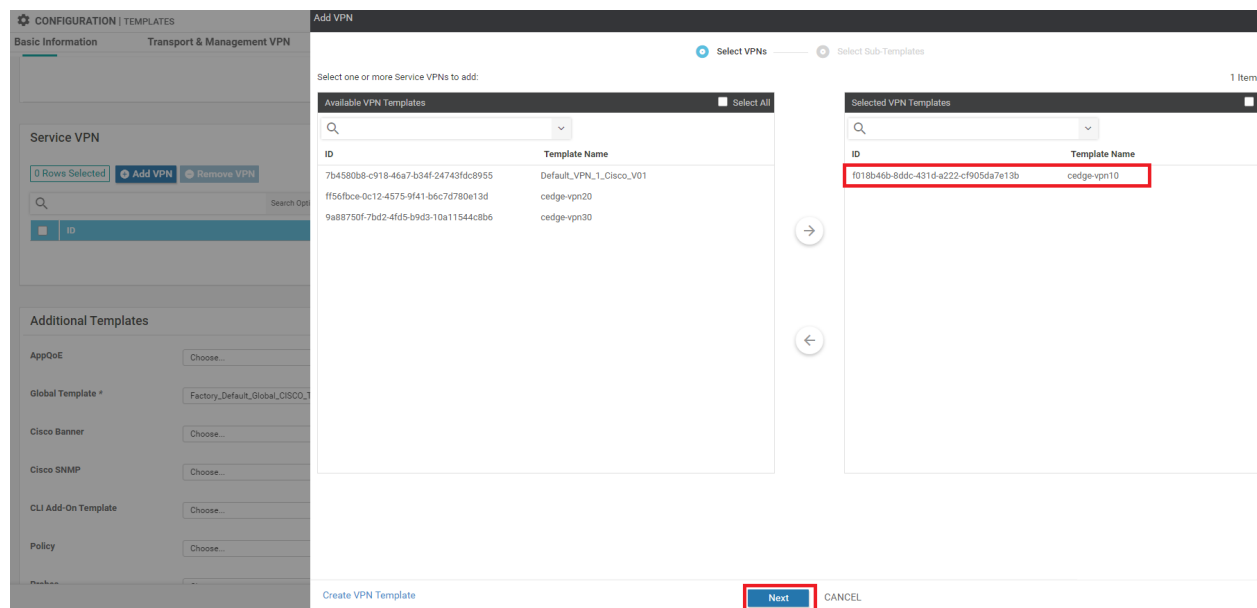
- [Updating vEdge Device Templates for Service Side VPNs](#)
 - [Updating the DC vEdge Device Template](#)
 - [Updating the Site 20 Device Template](#)
 - [Updating the Site 30 Device Template](#)
- [Updating cEdge Device Templates for Service Side VPNs](#)
 - [Updating the Site 40 Device Template](#)
 - [Updating the Site 50 Device Template](#)

Updating cEdge Device Templates for Service Side VPNs

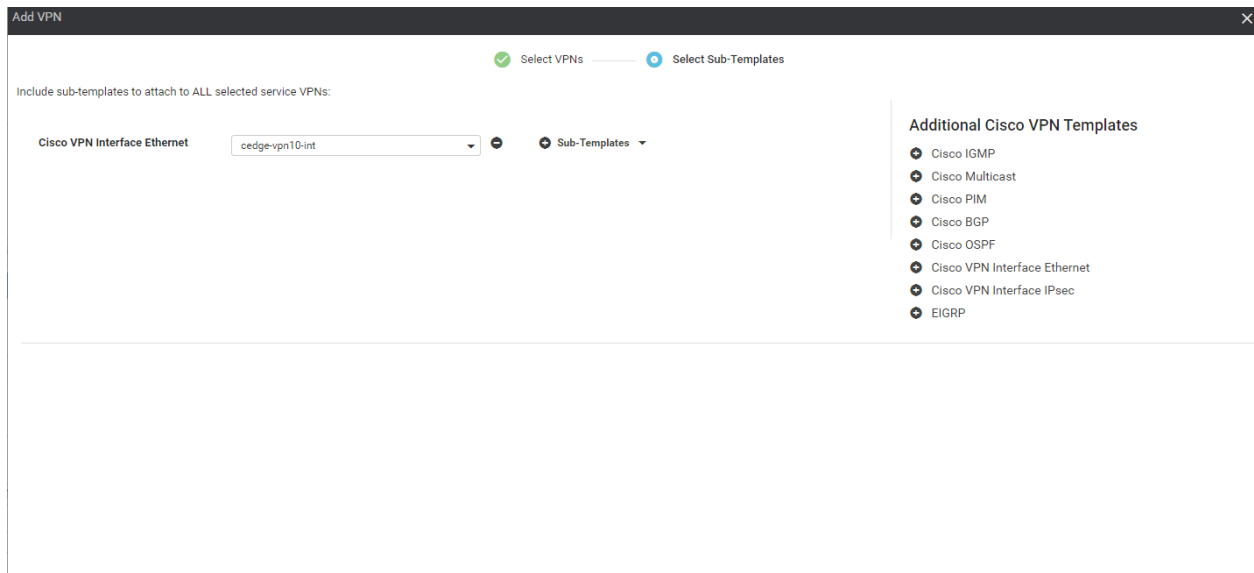
The cEdges will have 3 Service Side VPNs associated (VPN 10, VPN 20 and VPN 30) with them. We have already created the Feature Templates for these and are now going to update the Device Templates for the cEdges to reflect these Feature Templates.

Updating the Site 40 Device Template

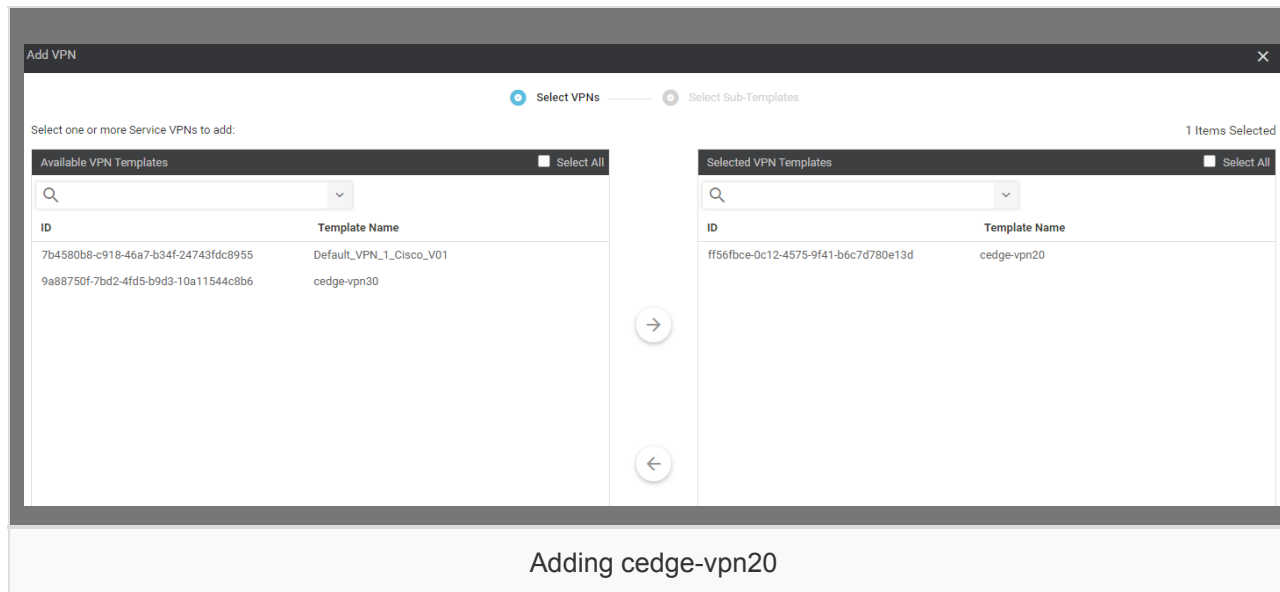
1. While on **Configuration => Templates**, click on the three dots next to *cEdge_dualuplink_devtemp* and choose to **Edit**. Scroll down to the **Service VPN** section and click on **Add VPN**. Move *cedge-vpn10* to the list of Selected VPN Templates. Click on **Next**



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



Add VPN

Select VPNs Select Sub-Templates

Include sub-templates to attach to ALL selected service VPNs:

Cisco VPN Interface Ethernet 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

Adding cedge-vpn20-int

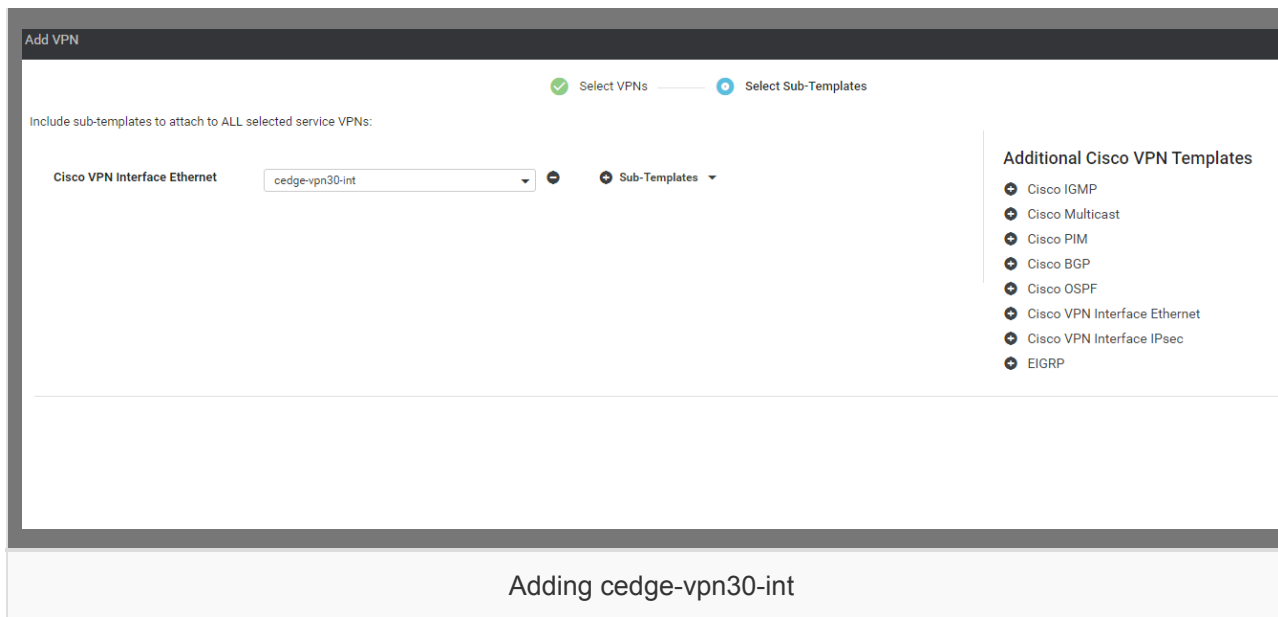
Add VPN

Select VPNs Select Sub-Templates

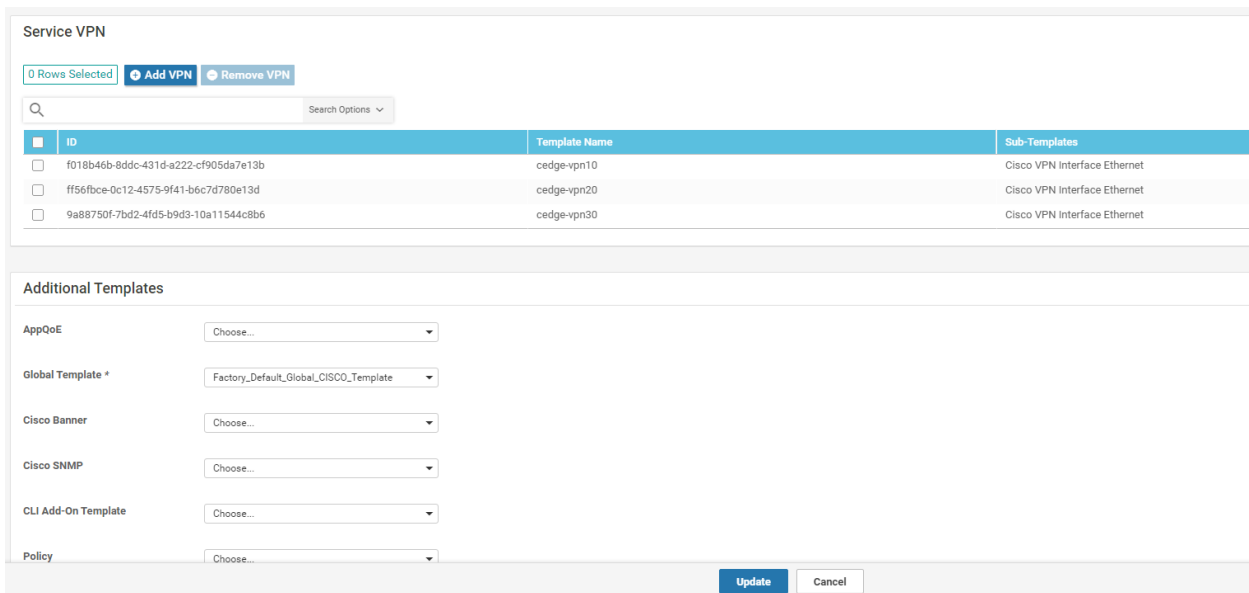
Select one or more Service VPNs to add: 1 Items Selected

Available VPN Templates		Selected VPN Templates	
ID	Template Name	ID	Template Name
7b4580b8-c918-46a7-b34f-24743fdc8955	Default_VPN_1_Cisco_V01	9a88750f-7bd2-4fd5-b9d3-10a11544c8b6	cedge-vpn30

Adding cedge-vpn30



4. Click on **Update** once done adding all three VPNs. The final Device Template page should look like this



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**

Variable List (Hover over each field for more information)

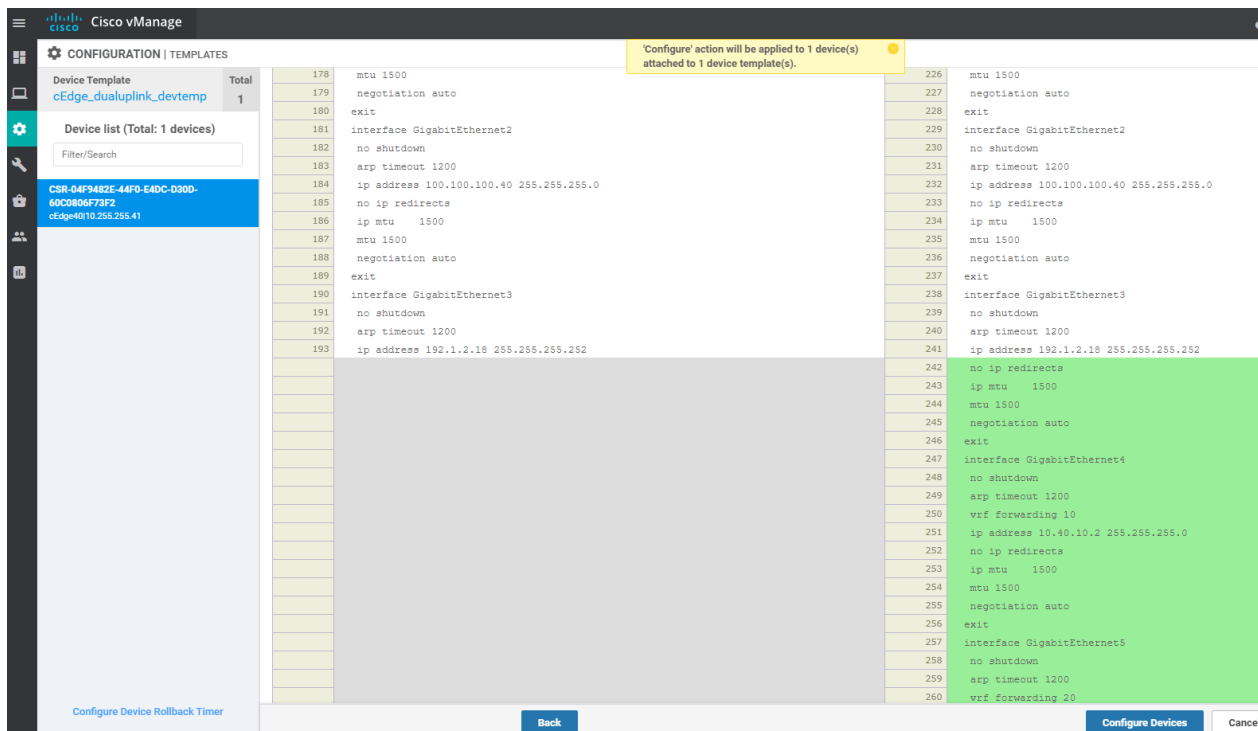
Chassis Number	CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2
System IP	10.255.255.41
Hostname	cEdge40
Address(vpn512_next_hop_ip_address_0)	192.168.0.1
IPv4 Address/ prefix-length(vpn512_mgmt_ipv4_address)	192.168.0.40/24
Address(vpn0_next_hop_ip_address_0)	100.100.100.1
IPv4 Address/ prefix-length(inet_ipv4_address)	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

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**



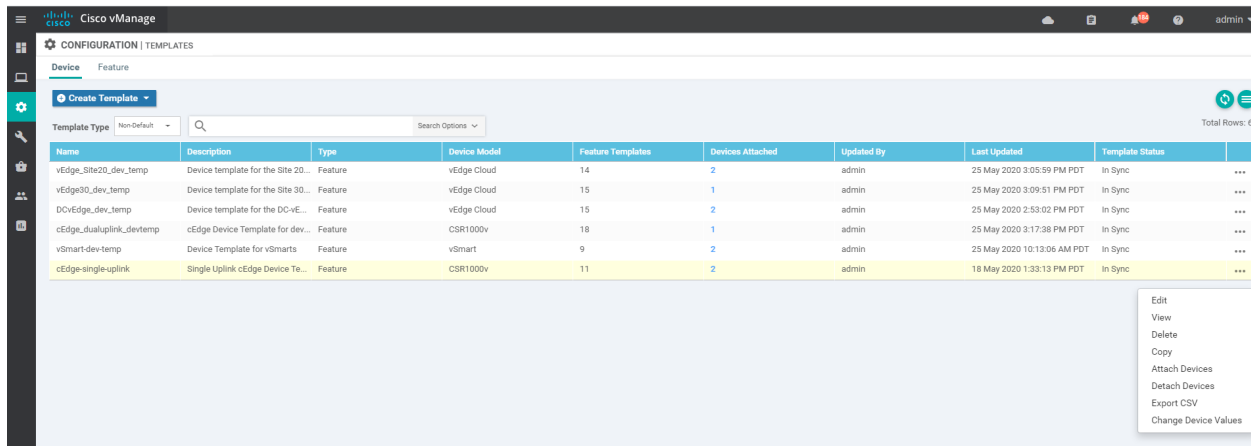
This completes the configuration of the Site 40 cEdges for Service Side VPNs.

Task List

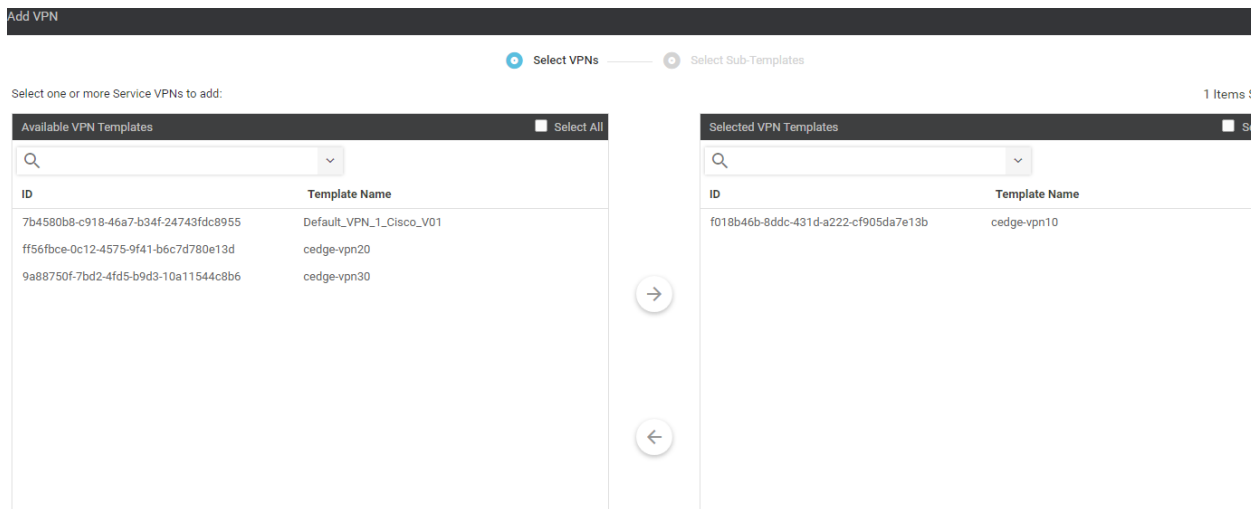
- Updating vEdge Device Templates for Service Side VPNs
 - Updating the DC vEdge Device Template
 - Updating the Site 20 Device Template
 - Updating the Site 30 Device Template
- Updating cEdge Device Templates for Service Side VPNs
 - Updating the Site 40 Device Template
 - Updating the Site 50 Device Template

Updating the Site 50 Device Template

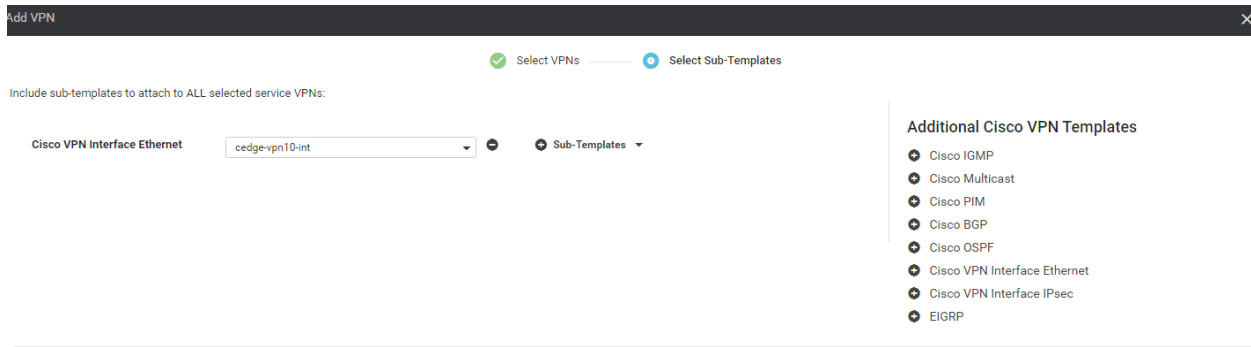
1. From **Configuration => Templates**, choose to **Edit** the *cEdge-single-uplink* Template



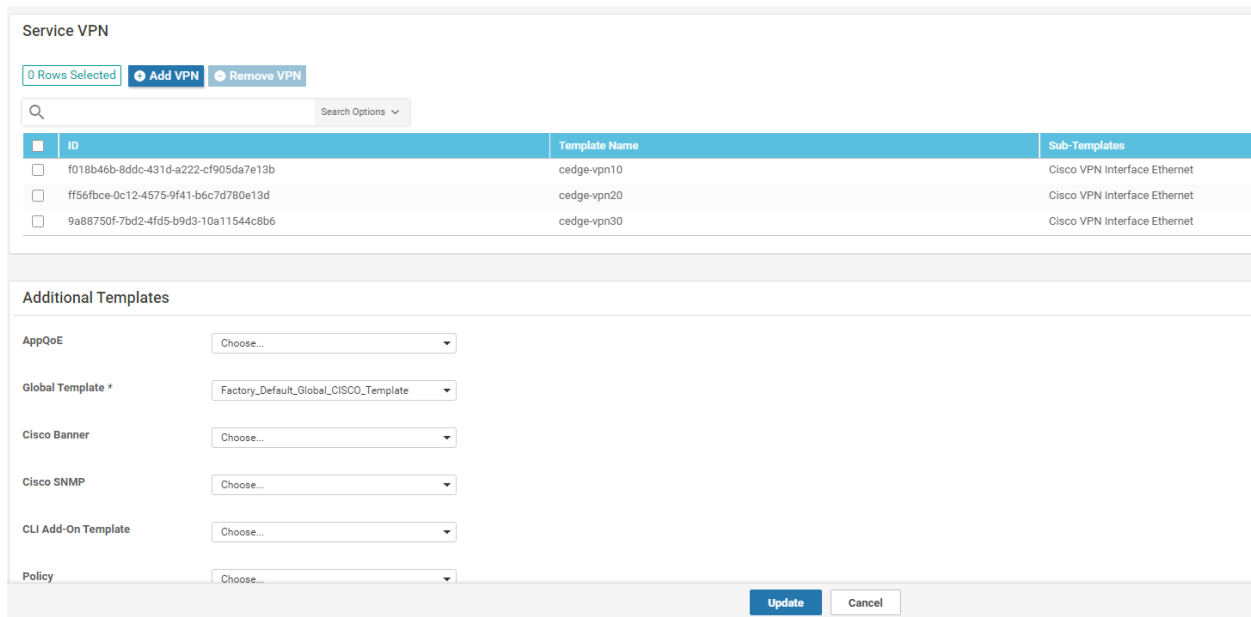
2. Under **Service VPN**, choose **Add VPN** and move *cedge-vpn10* to the list of **Selected VPN Templates** and click on **Next**



3. 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**



5. Choose to **Edit Device Template** next to cEdge50 and enter the details as shown below. Click on **Update**



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**

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)	10.50.30.3/24
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

Update

Cancel

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

```
|
| 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

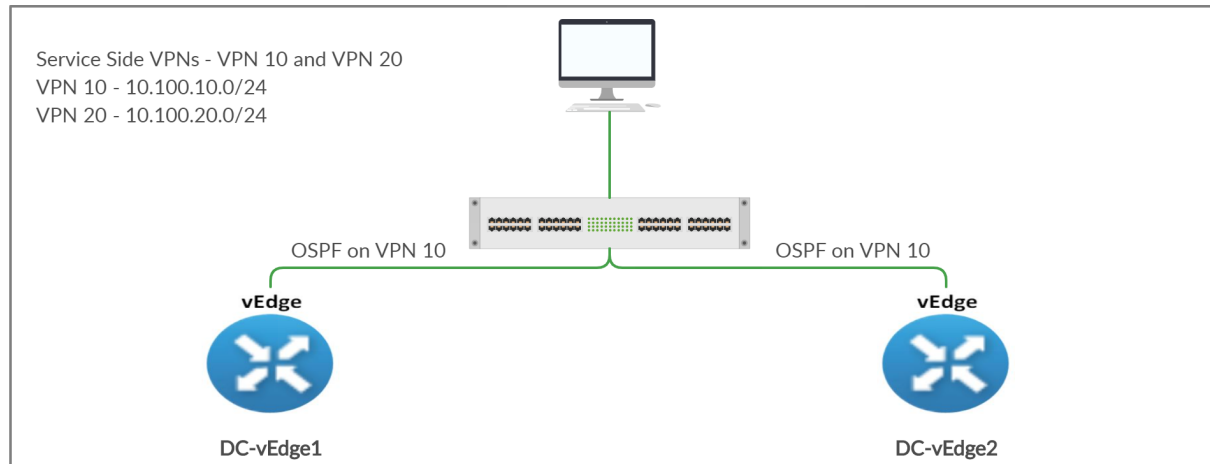
Overview

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

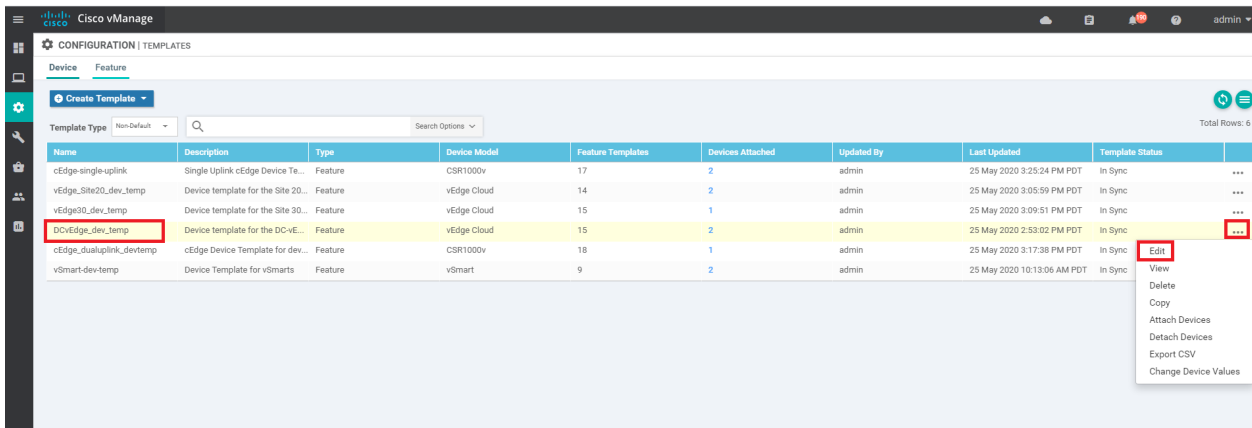


Task List

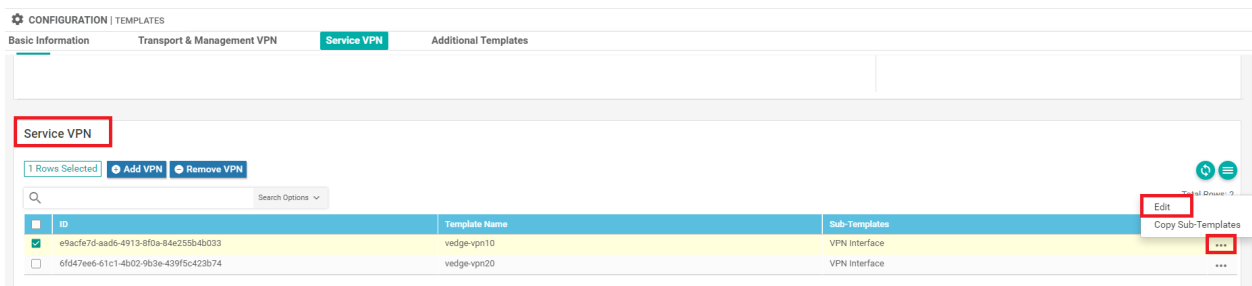
- [Overview](#)
- [Updating the vEdge Service VPN 10 with an OSPF Template](#)
- [Activity Verification](#)

Updating the vEdge Service VPN 10 with an OSPF Template

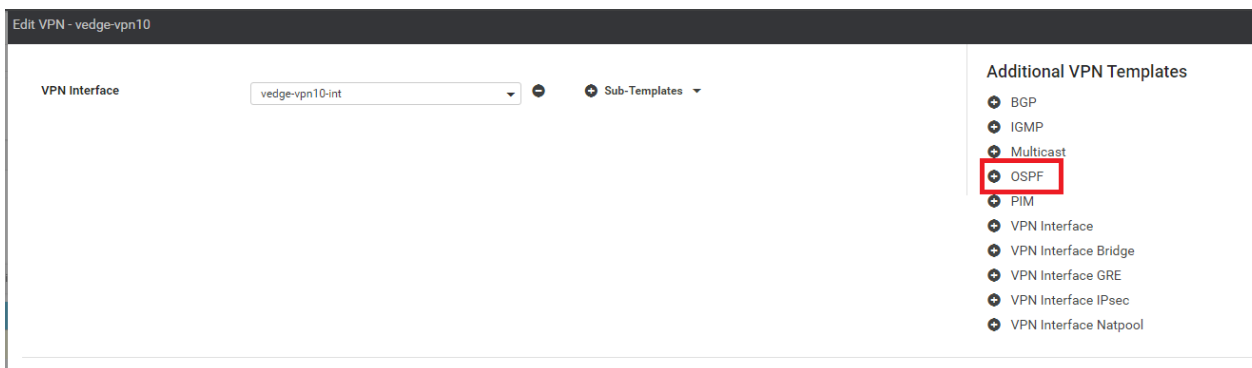
1. Go to **Configuration => Templates** and click on the three dots next to *DCvEdge_dev_temp*. Click on **Edit**



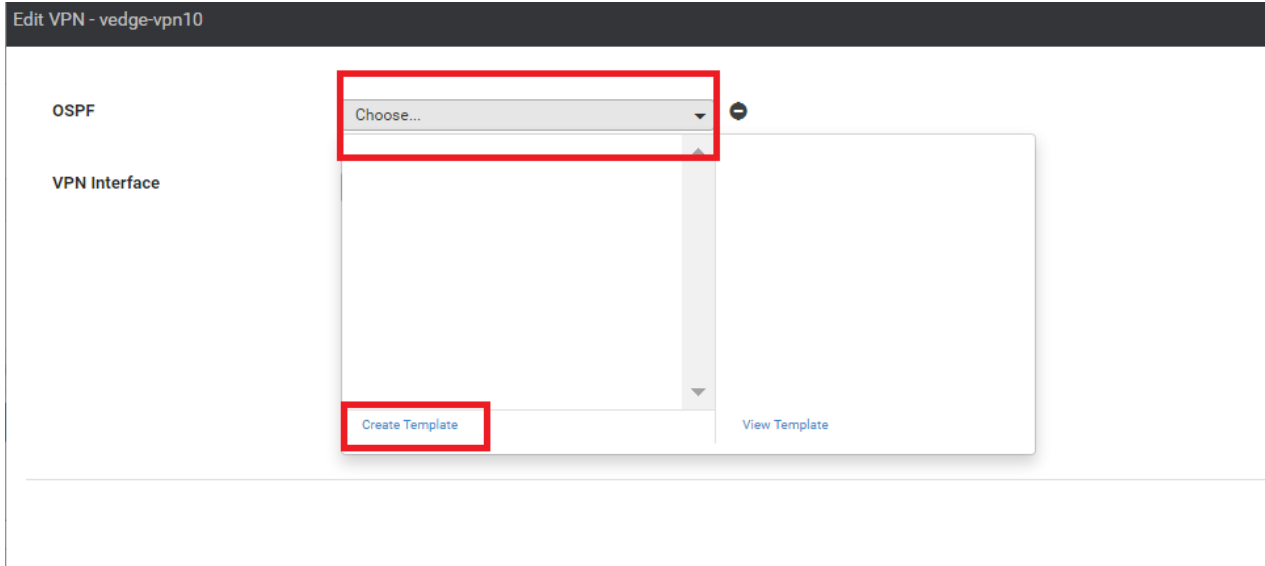
2. Under **Service VPN**, click on the three dots next to the *vedge-vpn10* template and choose to **Edit** it



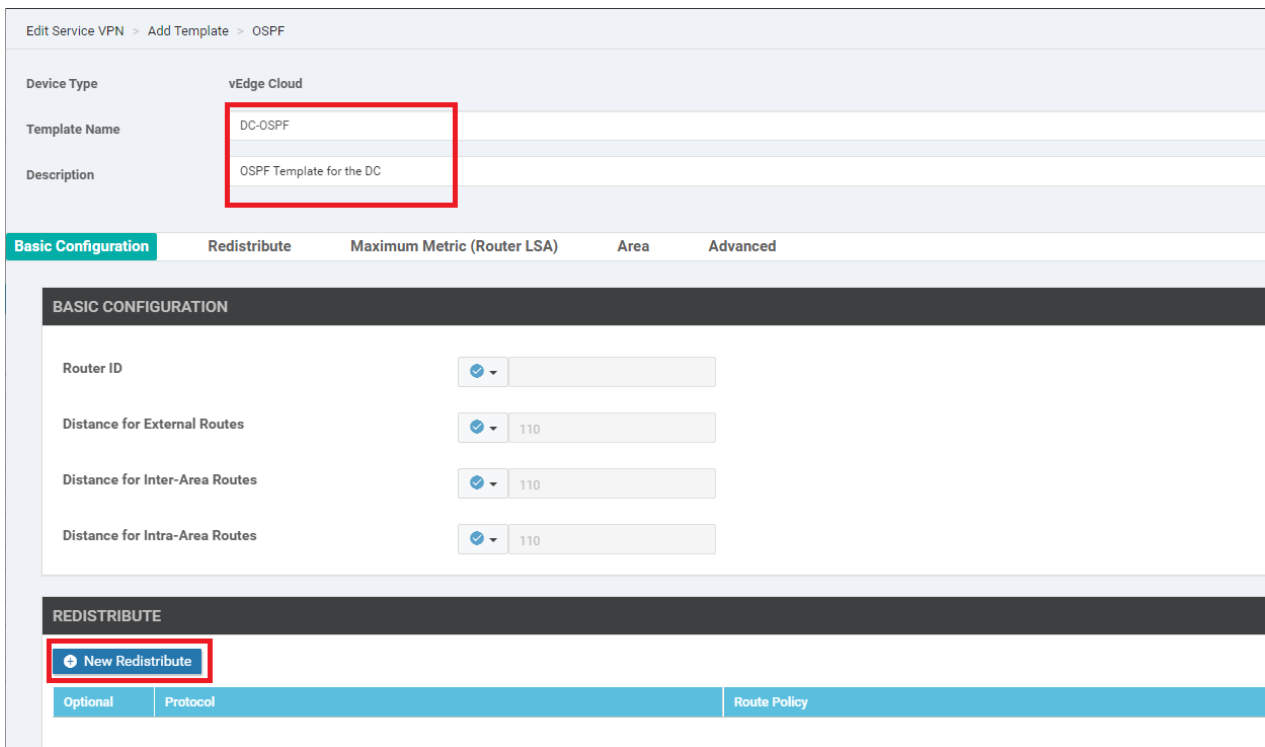
3. Click on **OSPF** under **Additional VPN Templates** to add an OSPF Template



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



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

The screenshot shows the 'REDISTRIBUTE' configuration page. At the top left, there is a '+ New Redistribute' button. Below it, the 'Protocol' dropdown menu is set to 'omp' and is highlighted with a red box. To the right of the dropdown is a checkbox labeled 'Mark as Optional Row' with an information icon. Below the 'Protocol' field is the 'Route Policy' dropdown menu. At the bottom right, the 'Add' button is highlighted with a red box, and a 'Cancel' button is visible next to it.

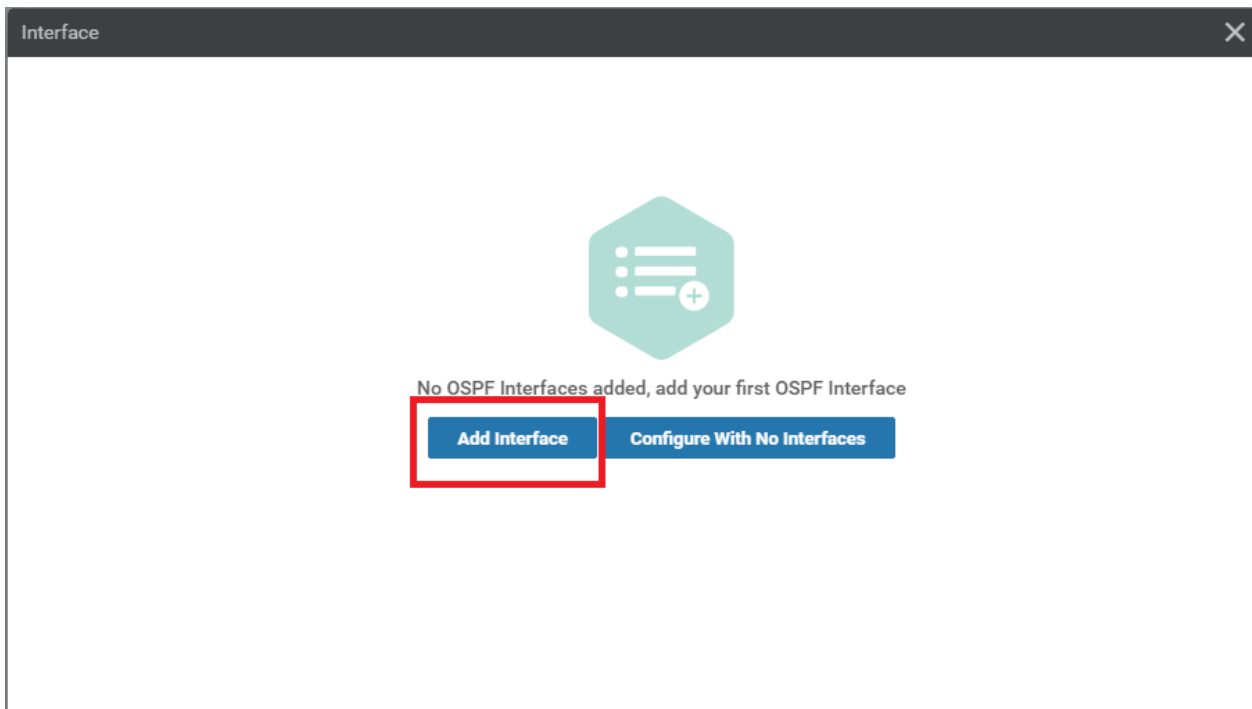
7. Under the Area section, click on **New Area**

The screenshot shows the 'AREA' configuration page. At the top left, there is a '+ New Area' button highlighted with a red box. Below it is a table with the following columns: 'Optional', 'Number', 'Area Type', 'No Summary', 'Translate', 'Interface', 'Range', and 'Action'. The table is currently empty, and the text 'No data available' is displayed in the center.

8. Set the Area Number as a Global value of **0**. Our OSPF neighbourships will be formed on Area 0. Click on **Add Interface**

The screenshot shows the 'AREA' configuration page. At the top left, there is a '+ New Area' button. Below it, the 'Area Number' field is set to '0' and is highlighted with a red box. Below the 'Area Number' field is the 'Set the area type' dropdown menu. Below that is the 'Add Interface' button, which is highlighted with a red box. At the bottom, there is an 'Add Range' button.

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

Hello Interval (seconds)

Dead Interval (seconds)

LSA Retransmission Interval (seconds)

Interface Cost

Advanced Options >

Add Cancel

11. Click on **Add** under the Area section to Add these details to the OSPF Template

AREA

New Area

Mark as Optional Row ⓘ

Area Number

Set the area type

Interface 1 Interface

Range

Add Cancel

12. Click on **Save** to save the OSPF template

AREA

+ New Area

Optional	Number	Area Type	No Summary	Translate
<input type="checkbox"/>	<input type="text" value="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

Search Options

ID	Template Name	Sub-Templates
<input type="checkbox"/> e9acf7d-aad6-4913-8f0a-84e255b4b033	vedge-vpn10	OSPF, VPN Interface
<input type="checkbox"/> 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**

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 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

CONFIGURATION | TEMPLATES

Device Template: DCvEdge_dev_temp (Total: 1)

Device list (Total: 2 devices)

Filter/Search

Configure Device Rollback Timer

Back

Configure Devices

Cancel

Configure action will be applied to 2 device(s) attached to 1 device template(s).

```

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
96 interface ge0/2
97 ip address 10.100.10.2/24
98 no shutdown
99 !
100 omp
101 advertise connected
102 advertise static
103 !
104 !
105 interface ge0/2
106 ip address 10.100.10.2/24
107 no shutdown
108 !
109 omp
110 advertise connected
111 advertise static
112 !
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 omp
122 advertise connected
123 advertise static

```

```

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
96 router
97 ospf
98 timers spf 200 1000 10000
99 redistribute omp
100 area 0
101 interface ge0/2
102 exit
103 !
104 !
105 interface ge0/2
106 ip address 10.100.10.2/24
107 no shutdown
108 !
109 omp
110 advertise connected
111 advertise static
112 !
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 omp
122 advertise connected
123 advertise static

```

Configure Devices

Committing these changes affect the configuration on 2 devices. Are you sure you want to proceed?

Confirm configuration changes on 2 devices.

Put a check mark, then click on OK

OK

Cancel

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)

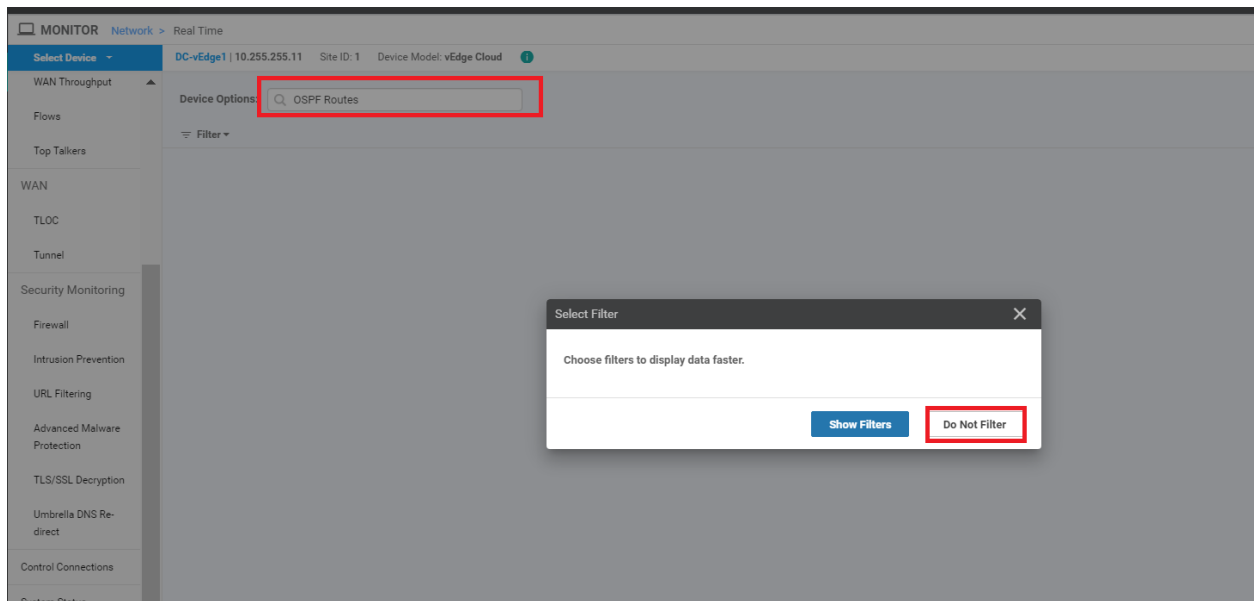
The screenshot shows the vManage GUI with the following elements:

- MONITOR** header with **Network > Real Time** breadcrumb.
- Select Device** dropdown menu showing **DC-vEdge1** (IP: 10.255.255.11, Site ID: 1, Device Model: vEdge Cloud).
- Device Options** search box containing **OSPF Neighbors**.
- Table of 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

The **Real Time** option is selected in the left-hand navigation menu.

2. Enter *OSPF Routes* in the **Device Options** and choose *Do Not Filter* if prompted



3. You should see a Route for the 10.0.0.1/32 network, among others

The screenshot shows the 'OSPF Routes' table in the network monitoring interface. The table has the following columns: VPN, Route Type, Prefix, Area ID, ID, Cost, Flags, Path Type, Dest Type, Tag, Type-2 Cost, Next Hop, If Name, and Last Updated. The first row is highlighted with a red box.

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
-----
10   10.100.10.1      ge0/2          10.0.0.1       full       1         37
10   10.100.10.3      ge0/2          10.255.255.12  full       1         37
DBsmL  RqstL  RXmtL
-----
0      0      0
0      0      0
DC-vEdge1#

```

```
DC-vEdge1# show ospf route
```

VPN	ROUTE TYPE	PREFIX	ID	AREA	COST	PATH TYPE	DEST TYPE	NEXT HOP	IF NAME
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	PROTOCOL SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	NEXTHOP VPN	TLOC IP	COLOR	ENCAP
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,
 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	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

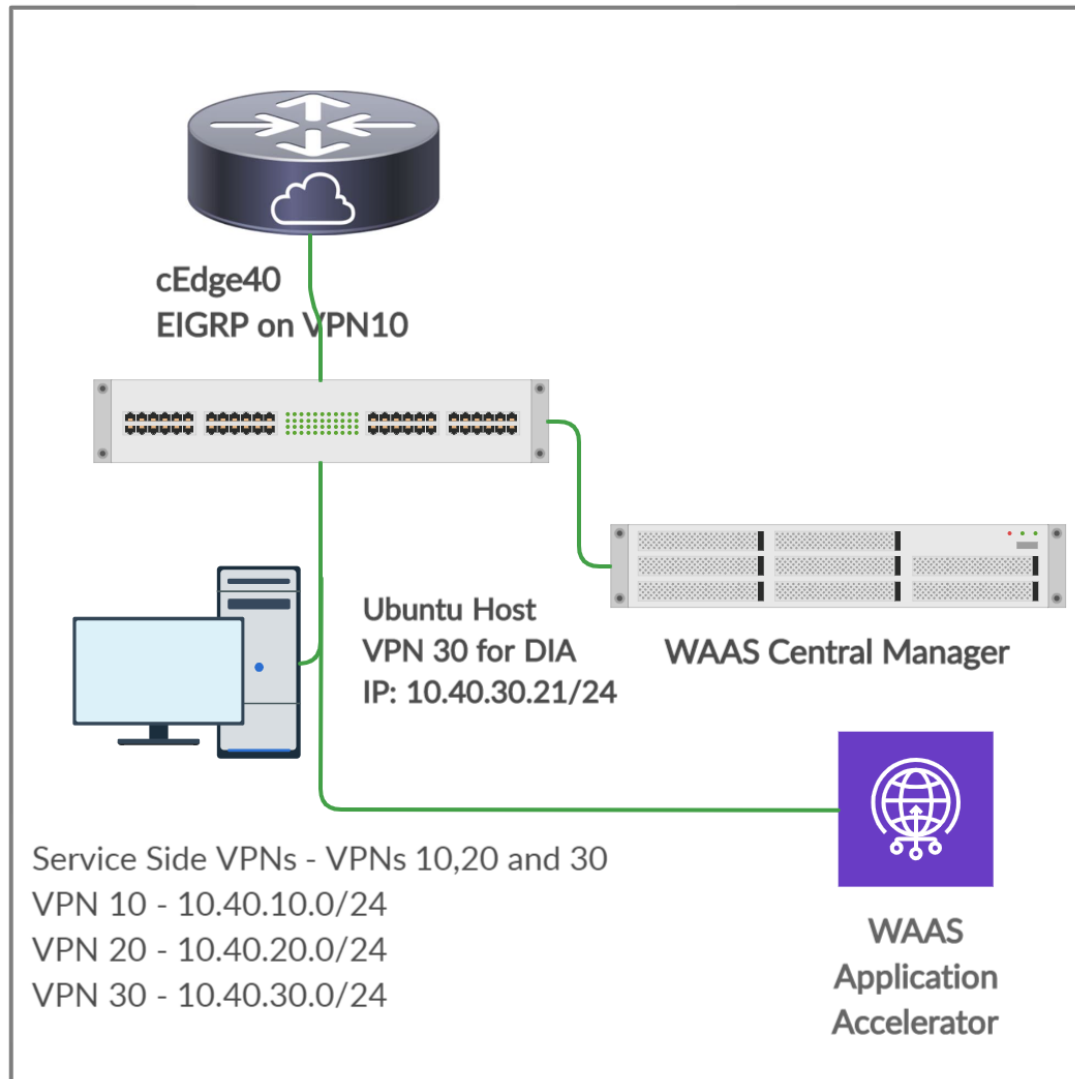
- Overview
- Updating the cEdge Service VPN 10 with an EIGRP Template
- Activity Verification and Remediation

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**

CONFIGURATION | TEMPLATES

Device Feature

Create Template

Template Type: Non-Default

Total Rows: 6

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
cEdge-singleuplink	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 11:37:08 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	...

Edit

- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

2. Under **Service VPN**, click on the three dots next to the *cedge-vpn10* template and choose to **Edit** it

Service VPN

1 Rows Selected | Add VPN | Remove VPN

Total Rows: 3

ID	Template Name	Sub-Templates	
<input checked="" type="checkbox"/> f018b46b-8d6c-431d-a222-cf905da7e13b	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	...

Edit

Copy Sub-Templates

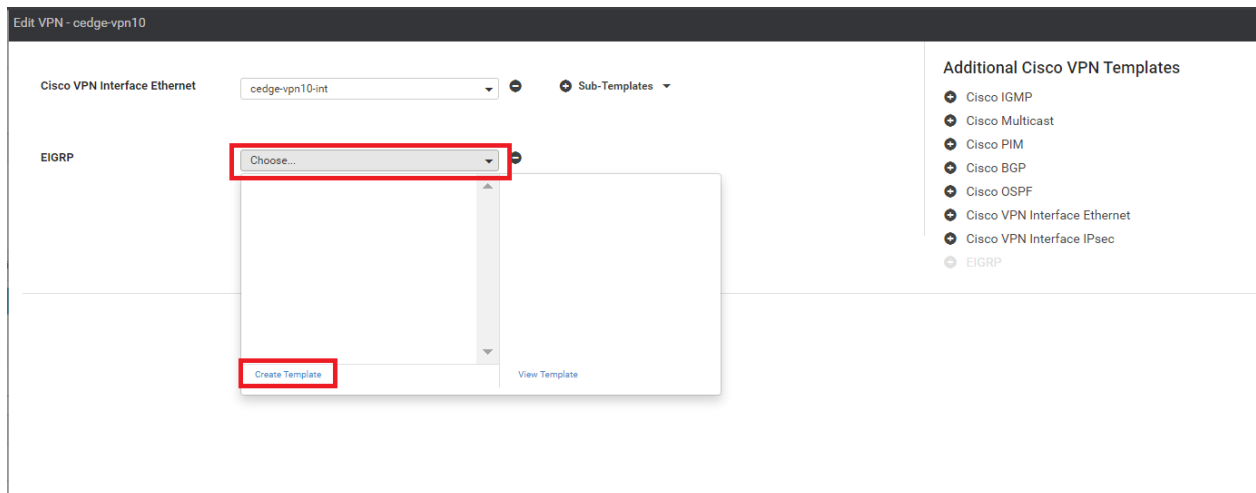
3. Click on **EIGRP** under **Additional Cisco VPN Templates** to add an EIGRP Template

Cisco VPN Interface Ethernet | cedge-vpn10-int | Sub-Templates

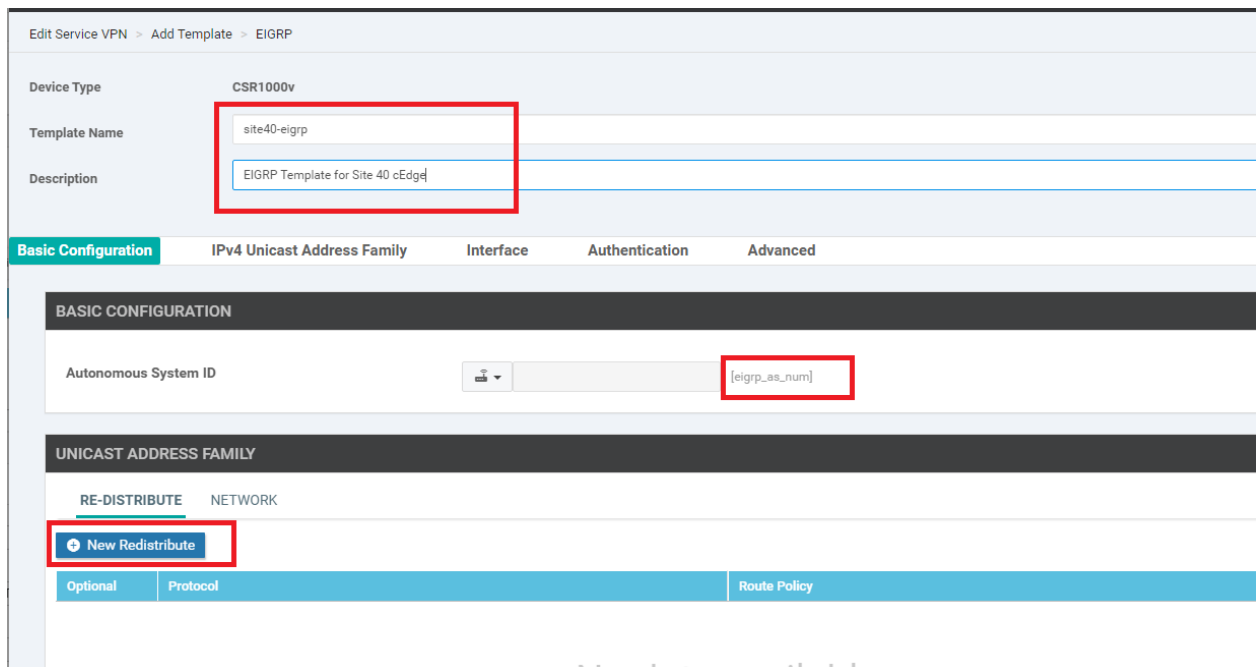
Additional Cisco VPN Templates

- 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

The screenshot shows the 'UNICAST ADDRESS FAMILY' configuration page with the 'RE-DISTRIBUTE' tab selected. A 'New Redistribute' button is visible. The 'Protocol' dropdown menu is set to 'omp' and is highlighted with a red box. The 'Route Policy' dropdown is also visible. The 'Add' button at the bottom right is highlighted with a red box.

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**

The screenshot shows the 'UNICAST ADDRESS FAMILY' configuration page with the 'NETWORK' tab selected. A 'New Network' button is visible. The 'Network Prefix' dropdown menu is set to '10.40.10.0/24' and is highlighted with a red box. The 'Add' button at the bottom right is highlighted with a red box. Numbered callouts are present: 1 points to the 'NETWORK' tab, 2 points to the 'New Network' button, 3 points to the 'Network Prefix' dropdown, and 4 points to the 'Add' button.

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

The screenshot shows the 'INTERFACE' configuration page. An 'Interface' button is visible. The 'Interface name' dropdown menu is set to 'GigabitEthernet4' and is highlighted with a red box. The 'Add' button at the bottom right is highlighted with a red box. Numbered callouts are present: 1 points to the 'Interface' button, 2 points to the 'Interface name' dropdown, and 3 points to the 'Add' button.

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"/>	 GigabitEthernet	<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**

Cisco VPN Interface Ethernet

cedge-vpn10-int



+ Sub-Templates

EIGRP

site40-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 Add VPN Remove VPN

Search Options

ID	Template Name	Sub-Templates
<input type="checkbox"/> f018b46b-8ddc-431d-a222-cf905da7e13b	cedge-vpn10	Cisco VPN Interface Ethernet, EIGRP
<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

Global Template

Cisco Banner

Cisco SNMP

CLI Add-On Template

Policy

Update Cancel

12. We are taken to the configuration page for the cEdge40. Enter the Autonomous System ID as 40 and click on **Next**

Search Options

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

Next Cancel

13. Review the side-by-side config diff (notice the EIGRP configuration added) and click on **Configure Devices**.

CONFIGURATION | TEMPLATES

Device Template: cEdge_dualuplink_devtemp | Total: 1

Device list (Total: 1 devices)

Filter/Search

CSR-04F9482E-44F0-E4DC-D300-60C004F73F2 | cEdge4010.253.255.41

Configure Device Rollback Timer

Back

Configure Devices

Cancel

'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 lkev2 diagnose error
304 no crypto isakmp diagnose error
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

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
   10.40.10.1              Gi4                (sec)         (ms)   100  0  3
0   10.40.10.1              Gi4                12 00:02:01   8
cEdge40#

```

```
show ip eigrp vrf 10 40 neighbors
```

- 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
I    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
```

- 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-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  TLOC IP  COLOR
-----
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  mpls
10    10.20.10.0/24     omp      -         -        -            -        10.255.255.21  public-internet
10    10.30.10.0/24     omp      -         -        -            -        10.255.255.31  mpls
10    10.30.10.0/24     omp      -         -        -            -        10.255.255.31  public-internet
10    10.40.10.0/24     omp      -         -        -            -        10.255.255.41  mpls
10    10.40.10.0/24     omp      -         -        -            -        10.255.255.41  public-internet
10    10.50.10.0/24     omp      -         -        -            -        10.255.255.51  public-internet
10    10.50.10.0/24     omp      -         -        -            -        10.255.255.52  mpls
10    10.100.10.0/24    ospf      IA         ge0/2    -            -        -            -
10    10.100.10.0/24    connected -         ge0/2    -            -        -            -

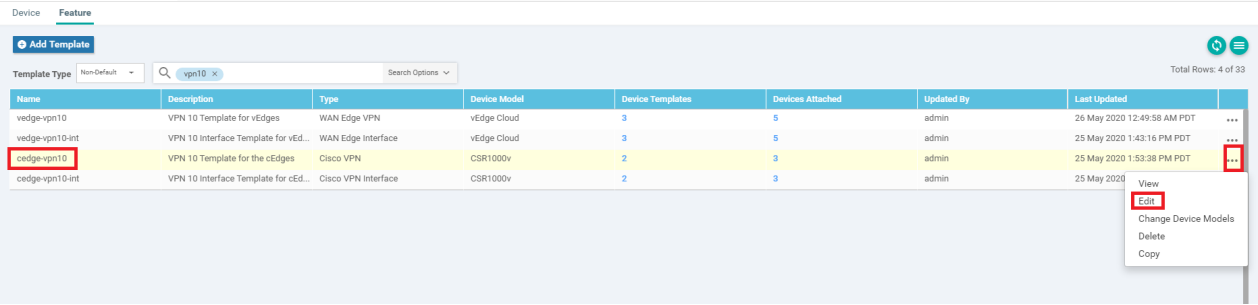
```

```

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**



5. Navigate to the **Advertise OMP** section and set EIGRP to Global - **On**. Click on **Update**

Advertise OMP

IPv4 IPv6

BGP (IPv4) On Off

Static (IPv4) On Off

Connected (IPv4) On Off

OSPF External On Off

EIGRP On Off

LISP On Off

ISIS On Off

NETWORK AGGREGATE

Network (IPv4) On Off

Update Cancel

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

Search Options

S...	Chassis Number	System IP	Hostname	Interface Name(vpn30_if_name)	IPv4 Address/ prefix-length(vpn30_if_ipv4_address)	Interface Name(vpn20_if_name)
✓	CSR-834E40DC-E358-8DE1-0E81-76E598413...	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

Next Cancel

7. Check the side-by-side configuration, noting that EIGRP routes will now be advertised into OMP. Click on **Configure Devices**

The screenshot shows a configuration comparison interface. On the left, there is a sidebar with 'Device Template' (cEdge-single-uplink) and 'Device list (Total: 2 devices)'. The main area displays two columns of configuration for 'appqoe' devices. The right column shows the proposed configuration, with the line 'advertise eigrp' highlighted in green and a red box around it. At the bottom right, the 'Configure Devices' button is highlighted with a red box.

8. Confirm the change (pushed to 3 devices) and click on OK

The screenshot shows a 'Configure Devices' dialog box. The text reads: 'Committing these changes affect the configuration of 3 devices. Are you sure you want to proceed?'. Below this, there is a checkbox labeled 'Confirm configuration changes on 3 devices.' which is checked and highlighted with a red box. At the bottom right, there are two buttons: 'OK' and 'Cancel'. The 'OK' button is highlighted with a red box.

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-E358-8DE1-0EB1-7...	CSR1000v	cEdge50	10.255.255.51	50	10.255.255.1
Success	Done - Push Feature Template Con...	CSR-D1837F36-6A1A-1850-7C1C-...	CSR1000v	cEdge51	10.255.255.52	50	10.255.255.1
Success	Done - Push Feature Template Con...	CSR-04F9482E-44FD-E4DC-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,
  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 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

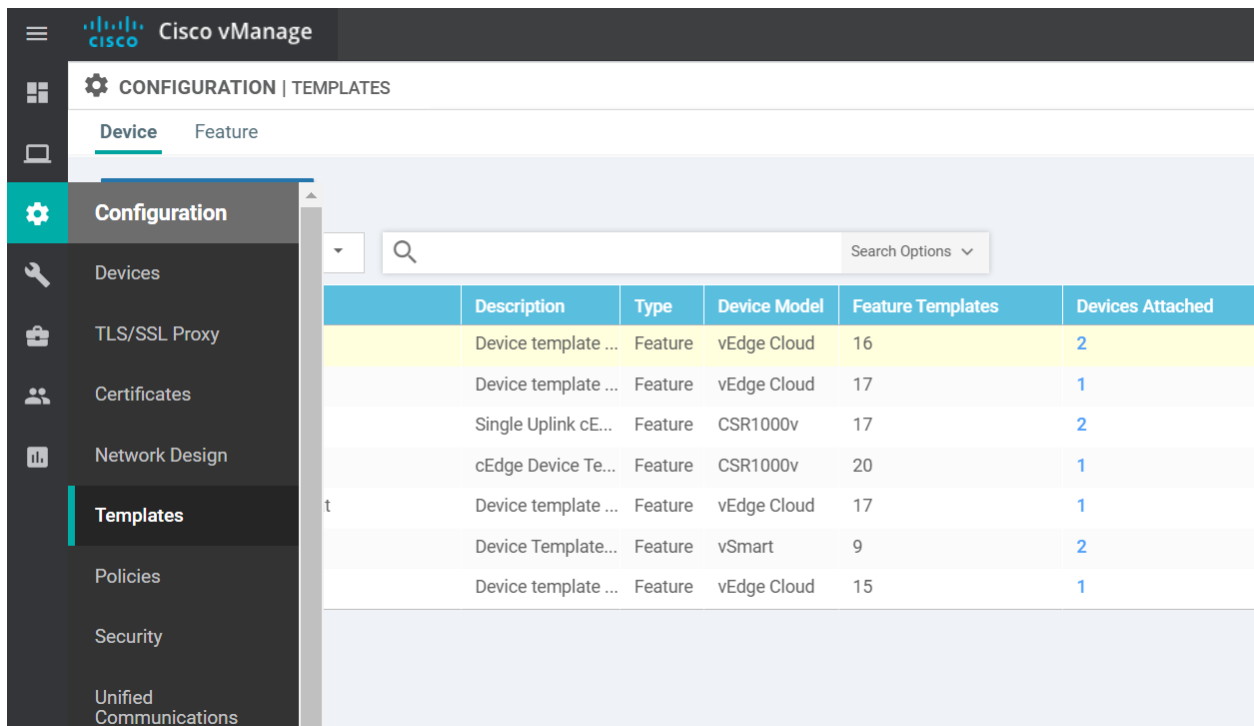
- [Editing Templates to support VRRP](#)
- [Verification and Testing](#)

Task List

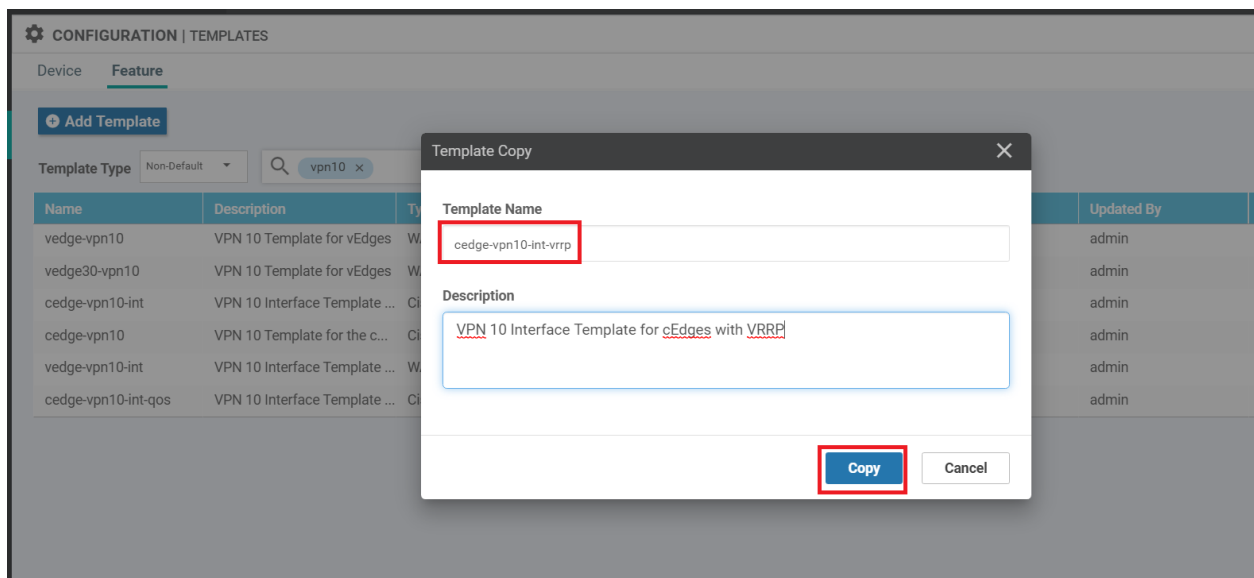
- Editing Templates to support VRRP
- Verification and Testing

Editing Templates to support VRRP

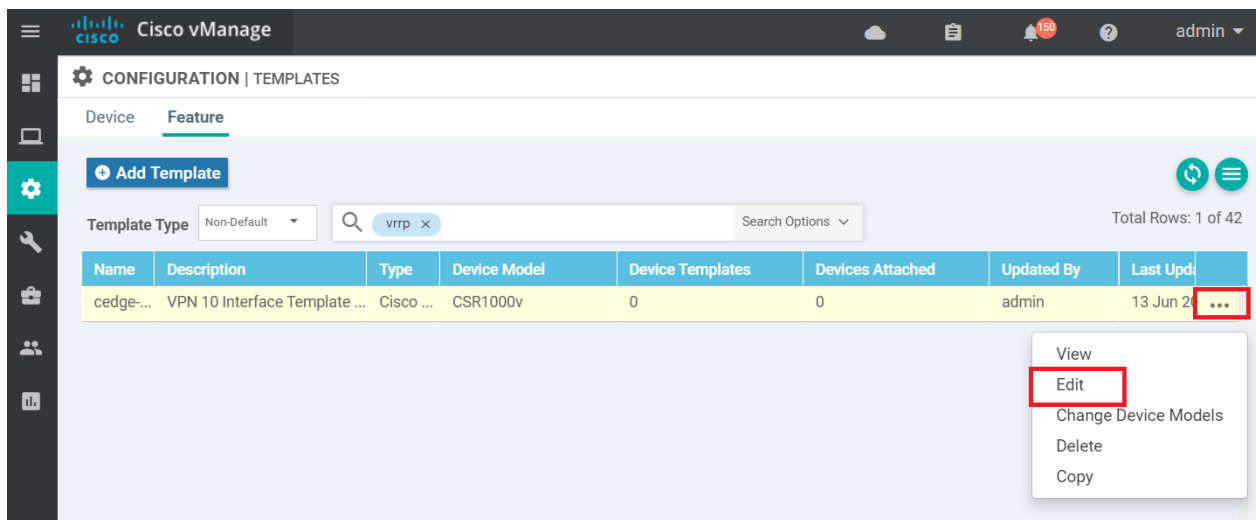
1. On the vManage GUI, navigate to **Configuration => Templates => Feature Tab**



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**



3. Click on the three dots next to the newly copied template and click on **Edit**



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 [vpn10_if_vrrp_priority] 4

Timer (milliseconds) 100

Track OMP 5 On Off

IP Address 6 10.50.10.100 7

Mark as Optional Row

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) [checked]

QoS Map [checked]

Device Rule [checked]

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**

Device Feature

Create Template

Template Type: Non-Default

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		Edit View Delete Copy Attach Devices Detach Devices Export CSV Change Device Values
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 Add VPN Remove VPN

Total Rows: 3

ID	Template Name	Sub-Templates	
<input checked="" type="checkbox"/> f018b46b-8ddc-431d-a222-cf905da7e13b	cedge-vpn10	Cisco VPN Interface Ethernet	Edit Copy Sub-Templates ...
<input type="checkbox"/> ff56fbce-0c12-4575-9f41-b6c7d780e13d	cedge-vpn20	Cisco VPN Interface Ethernet	...
<input type="checkbox"/> 9a88750f-7bd2-4fd5-b9d3-10a11544c8b6	cedge-vpn30	Cisco VPN Interface Ethernet	...

8. Populate *cedge-vpn10-int-vrrp* for the **Cisco VPN Interface Ethernet** and click on **Save**

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



Search Options

Total

<input type="checkbox"/>	ID	Template Name	Sub-Templates
<input type="checkbox"/>	f018b46b-8ddc-431d-a222-cf905da7e13b	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

AppQoS

Choose...

Global Template *

Factory_Default_Global_CISCO_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**



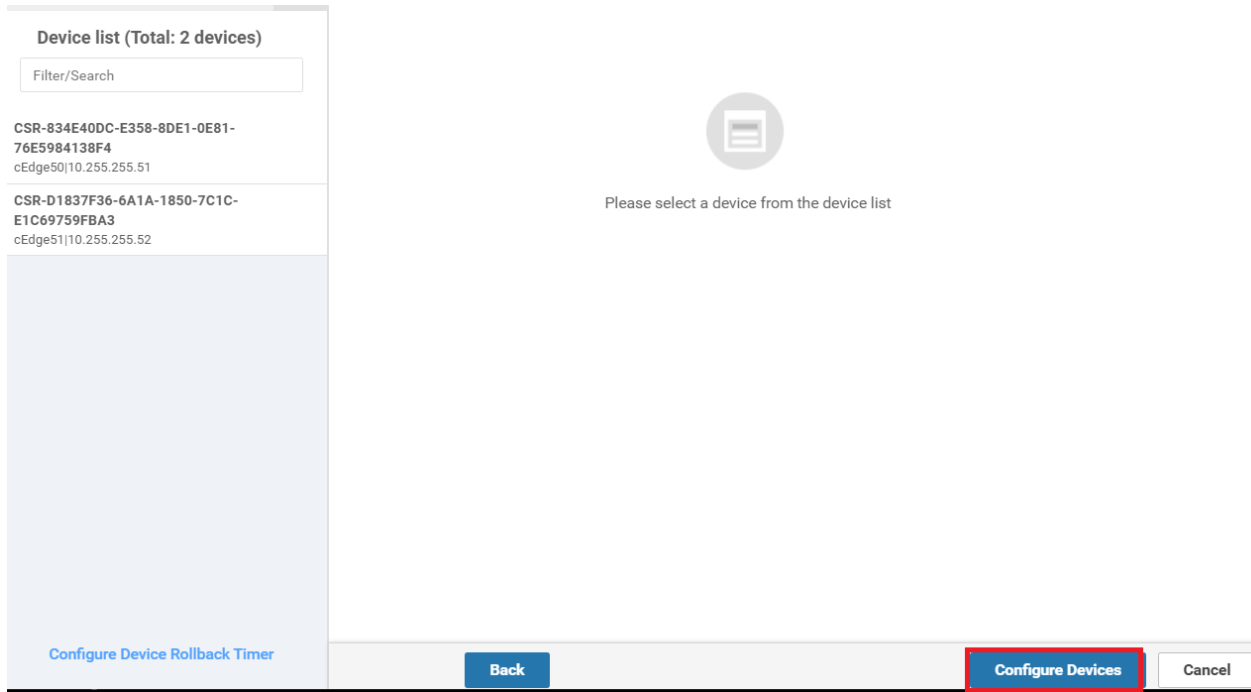
Search Options

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**



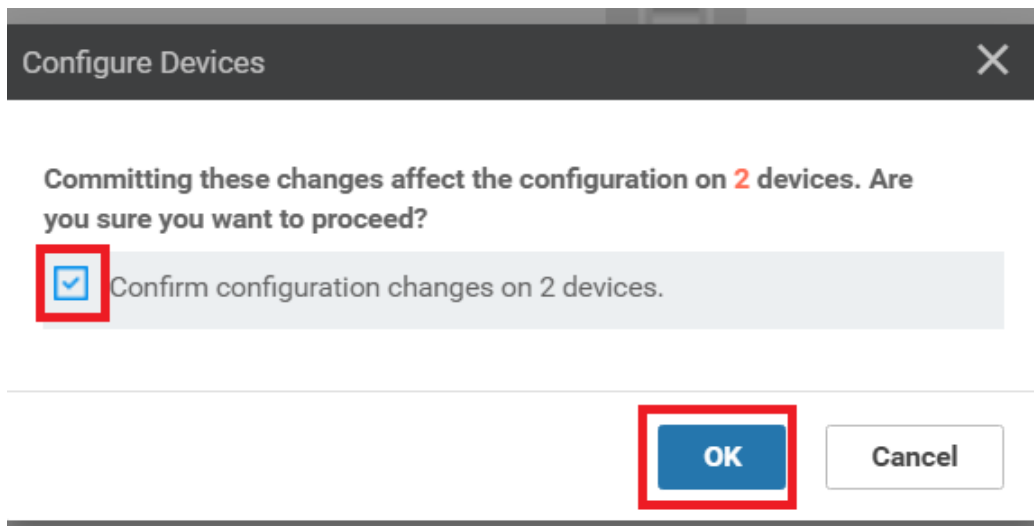
The screenshot shows a web interface for configuring devices. On the left, there is a 'Device list (Total: 2 devices)' section with a search filter. Two devices are listed:

- CSR-834E40DC-E358-8DE1-0E81-76E5984138F4
cEdge50|10.255.255.51
- CSR-D1837F36-6A1A-1850-7C1C-E1C69759FBA3
cEdge51|10.255.255.52

In the center, there is a circular icon with a document symbol and the text: 'Please select a device from the device list'.

At the bottom, there are three buttons: 'Configure Device Rollback Timer' (blue), 'Back' (blue), and 'Configure Devices' (blue, highlighted with a red border). To the right of 'Configure Devices' is a 'Cancel' button.

12. Confirm the configuration change and click on **OK**



The screenshot shows a 'Configure Devices' dialog box. The title bar says 'Configure Devices' with a close button (X). The main text reads: 'Committing these changes affect the configuration on 2 devices. Are you sure you want to proceed?'.

Below the text is a checkbox that is checked, with the text 'Confirm configuration changes on 2 devices.' next to it. The checkbox is highlighted with a red border.

At the bottom, there are two buttons: 'OK' (blue, highlighted with a red border) and 'Cancel' (white).

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

```
192.168.0.50 - PuTTY
cEdge50#show vrrp 5 Gig3
GigabitEthernet3 Group 5 - Address-Family IPv4
State is MASTER
State duration  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#

192.168.0.51 - PuTTY
cEdge51#show vrrp 5 Gig3
GigabitEthernet3 Group 5 - Address-Family IPv4
State is BACKUP
State duration  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

vm vSphere Client Menu Search in all environments

Ubuntu_Site50

Summary Monitor Configure Permissions Datastores Networks Updates

Powered On

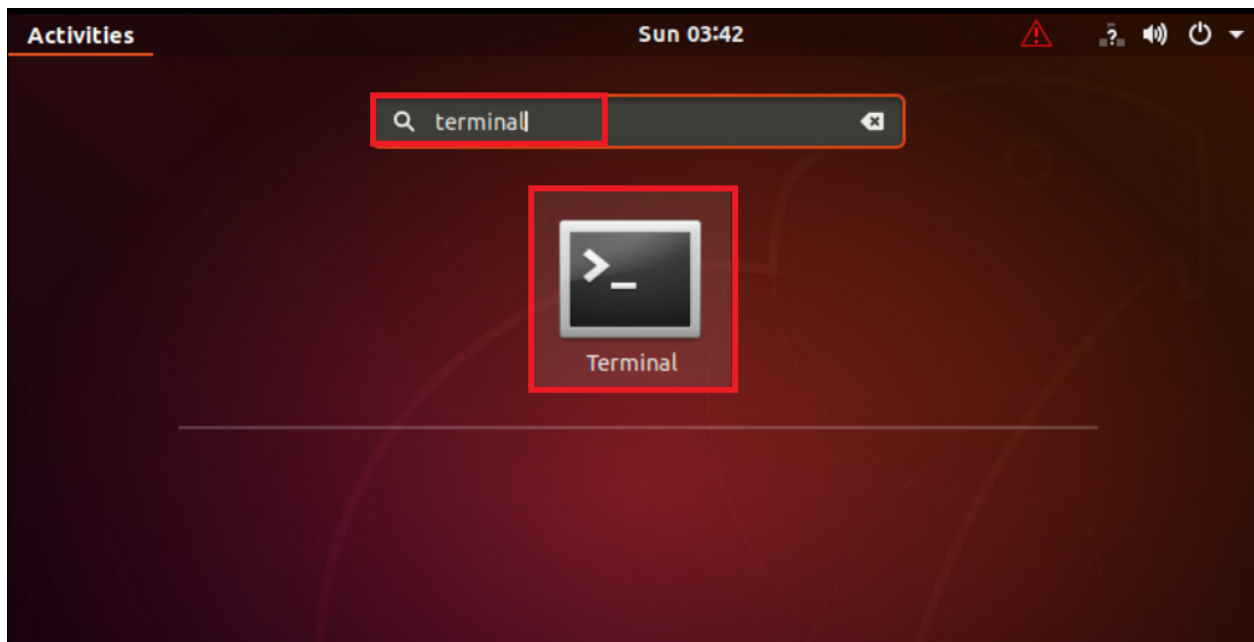
Launch Web Console
Launch Remote Console

VMware Tools is not installed on this virtual machine.

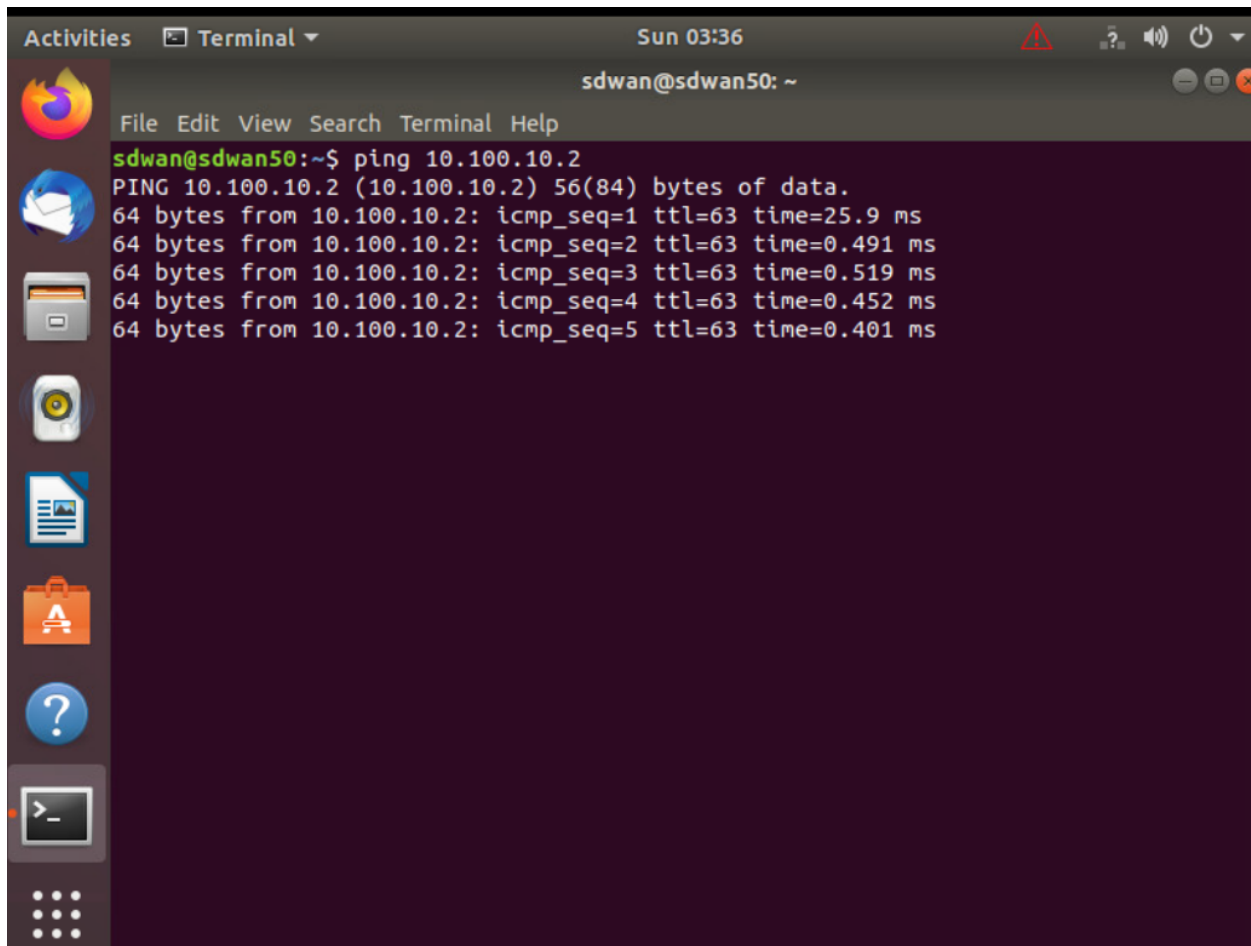
VM Hardware

> CPU	1 CPU(s)
> Memory	4 GB, 0.08 GB memory active
> Hard disk 1	40 GB

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 terminal window titled 'sdwan@sdwan50: ~' showing the output of a ping command. The window has a dark background and a light-colored text. The output shows five successful ping requests to 10.100.10.2, with the first one taking 25.9 ms and the others taking less than 1 ms. The window also shows a sidebar with various application icons and a top bar with system information.

```
sdwan@sdwan50: ~  
File Edit View Search Terminal Help  
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)

```
PutTY (inactive)
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 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#reload
Proceed with reload? [confirm]

64 bytes from 10.100.10.2: icmp_seq=40 ttl=63 time=0.538 ms
64 bytes from 10.100.10.2: icmp_seq=41 ttl=63 time=0.457 ms
64 bytes from 10.100.10.2: icmp_seq=42 ttl=63 time=0.316 ms
64 bytes from 10.100.10.2: icmp_seq=43 ttl=63 time=0.485 ms
64 bytes from 10.100.10.2: icmp_seq=43 ttl=63 time=0.472 ms
64 bytes from 10.100.10.2: icmp_seq=44 ttl=63 time=0.410 ms
64 bytes from 10.100.10.2: icmp_seq=44 ttl=63 time=0.482 ms
64 bytes from 10.100.10.2: icmp_seq=44 ttl=63 time=0.467 ms
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=0.479 ms
64 bytes from 10.100.10.2: icmp_seq=45 ttl=63 time=0.438 ms
64 bytes from 10.100.10.2: icmp_seq=46 ttl=63 time=0.480 ms
64 bytes from 10.100.10.2: icmp_seq=46 ttl=63 time=0.377 ms
64 bytes from 10.100.10.2: icmp_seq=46 ttl=63 time=0.378 ms
64 bytes from 10.100.10.2: icmp_seq=47 ttl=63 time=0.412 ms
64 bytes from 10.100.10.2: icmp_seq=47 ttl=63 time=0.417 ms
64 bytes from 10.100.10.2: icmp_seq=48 ttl=63 time=0.555 ms
64 bytes from 10.100.10.2: icmp_seq=48 ttl=63 time=0.668 ms (DUP!)
64 bytes from 10.100.10.2: icmp_seq=48 ttl=63 time=0.416 ms
64 bytes from 10.100.10.2: icmp_seq=49 ttl=63 time=0.512 ms (DUP!)
64 bytes from 10.100.10.2: icmp_seq=49 ttl=63 time=0.424 ms
64 bytes from 10.100.10.2: icmp_seq=50 ttl=63 time=0.537 ms (DUP!)
64 bytes from 10.100.10.2: icmp_seq=50 ttl=63 time=0.496 ms
64 bytes from 10.100.10.2: icmp_seq=51 ttl=63 time=1.22 ms DUP!)
64 bytes from 10.100.10.2: icmp_seq=51 ttl=63 time=0.513 ms
64 bytes from 10.100.10.2: icmp_seq=52 ttl=63 time=1.12 ms DUP!)
64 bytes from 10.100.10.2: icmp_seq=52 ttl=63 time=0.426 ms
```

5. After a few seconds, the pings should stabilise and we'll receive a response from just cEdge51

```
es Terminal Sun 05:37
sdwan@sdwan50: ~
File Edit View Search Terminal Help
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
```

- 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](#)

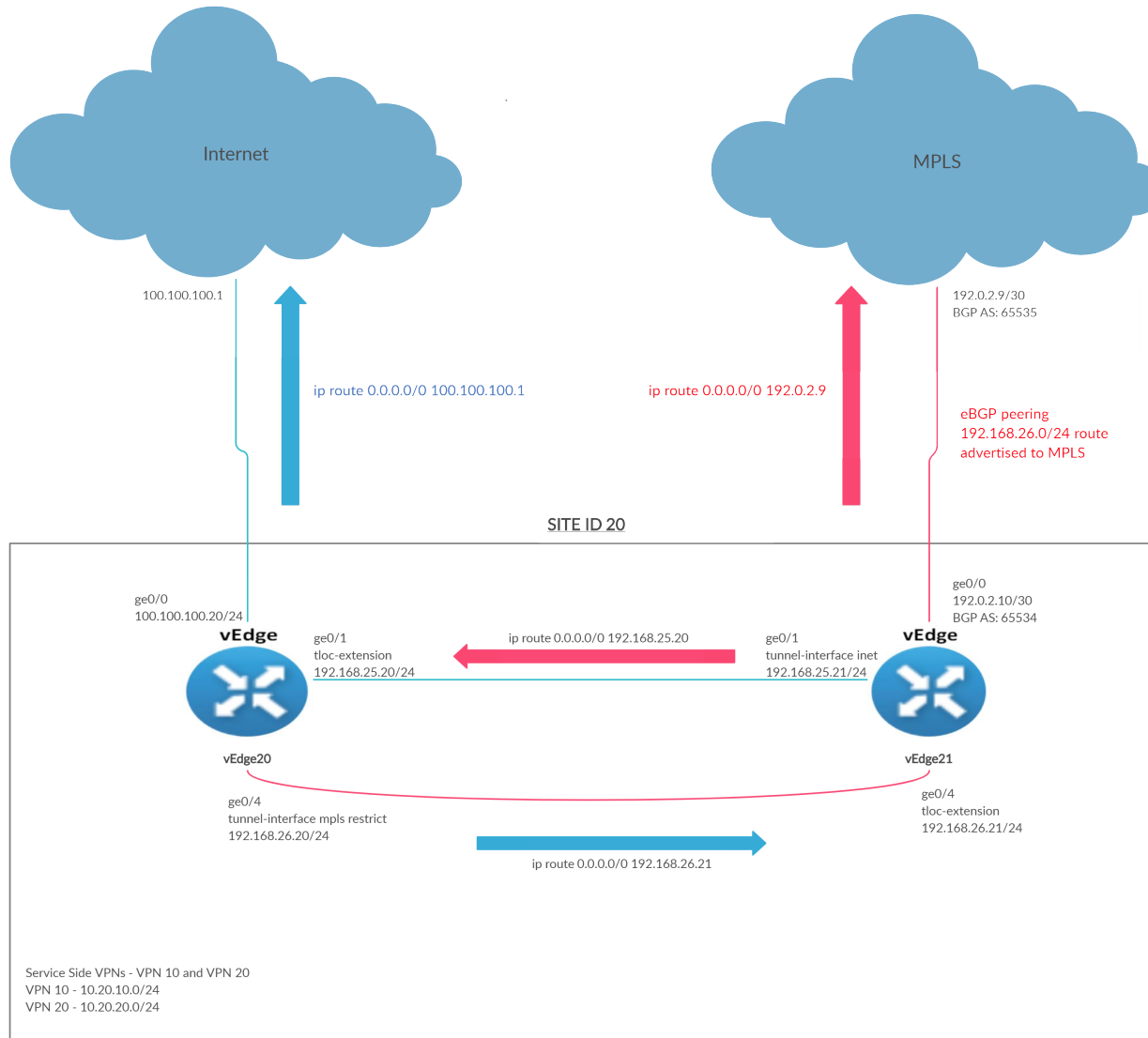
Task List

- 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`

```

vEdge20# show control connections
-----
PEER          CONTROLLER  PEER
PEER  PEER PEER  SITE  DOMAIN PEER
PEER  PEER PEER  PRIV PEER  PUB
TYPE  PROT SYSTEM IP  GROUP  ID  PRIVATE IP  PORT  LOCAL COLOR
PROXY STATE UPTIME  ID
-----
vsmart dtls 10.255.255.3 1000 1 100.100.100.4
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 100.100.100.5
No up 12:14:03:53 0
vmanage dtls 10.255.255.1 1000 0 100.100.100.2
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
PEER  PEER PEER  PRIV PEER  PUB
TYPE  PROT SYSTEM IP  GROUP  ID  PRIVATE IP  PORT  LOCAL COLOR
PROXY STATE UPTIME  ID
-----
vsmart dtls 10.255.255.3 1000 1 100.100.100.4
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 100.100.100.5
No up 12:14:03:42 0
vmanage dtls 10.255.255.1 1000 0 100.100.100.2
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
DETECT TX          SOURCE TLOC  REMOTE TLOC
SYSTEM IP  SITE ID STATE  COLOR  COLOR  PORT  SOURC
E IP  MULTIPLIER INTERVAL(msec) UPTIME  TRANSITIONS  ENCAP
-----
10.255.255.11 1 up public-internet public-internet 100.1
00.100.20 100.100.100.10 2936 ipsec
7 1000 0:14:36:27 0
10.255.255.12 1 up public-internet public-internet 100.1
00.100.20 100.100.100.11 22184 ipsec
7 1000 0:14:36:28 0
10.255.255.31 30 up public-internet public-internet 100.1
00.100.20 100.100.100.30 50308 ipsec
7 1000 0:14:41:35 0
10.255.255.41 40 up public-internet public-internet 100.1
00.100.20 100.100.100.40 12347 ipsec
7 1000 3:18:05:47 7
10.255.255.51 50 up public-internet public-internet 100.1
00.100.20 100.100.100.50 12347 ipsec
7 1000 3:18:05:47 7

vEdge21# show bfd sess
DETECT TX          SOURCE TLOC  REMOTE TLOC
SYSTEM IP  SITE ID STATE  COLOR  COLOR  PORT  SOURC
E IP  MULTIPLIER INTERVAL(msec) UPTIME  TRANSITIONS  ENCAP
-----
10.255.255.11 1 up 192.0.2.2 mpls mpls 192.0
.2.10 3:18:05:54 2 12426 ipsec
7 1000
10.255.255.12 1 up 192.0.2.6 mpls mpls 192.0
.2.10 3:18:05:54 2 12426 ipsec
7 1000
10.255.255.31 30 up 192.0.2.14 mpls mpls 192.0
.2.10 9:21:19:53 5 12366 ipsec
7 1000
10.255.255.41 40 up 192.1.2.18 mpls mpls 192.0
.2.10 2:14:56:54 0 12387 ipsec
7 1000
10.255.255.52 50 up 192.1.2.22 mpls mpls 192.0
.2.10 3:18:05:55 7 12347 ipsec
7 1000
  
```

```

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

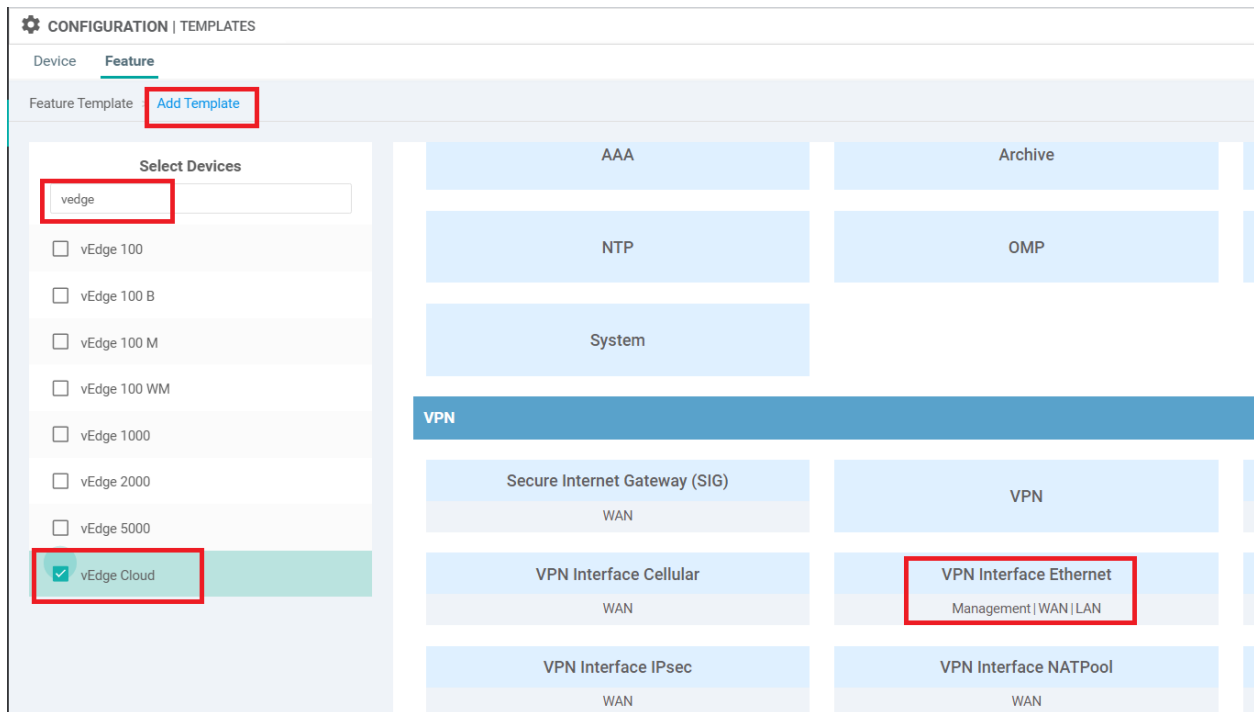
Feature Templates for TLOC Extensions

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



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

Description

IPv4 IPv6

Dynamic Static

IPv4 Address

TLOC Extension

Tracker

ICMP/ICMPv6 Redirect Disable On Off

GRE tunnel source IP

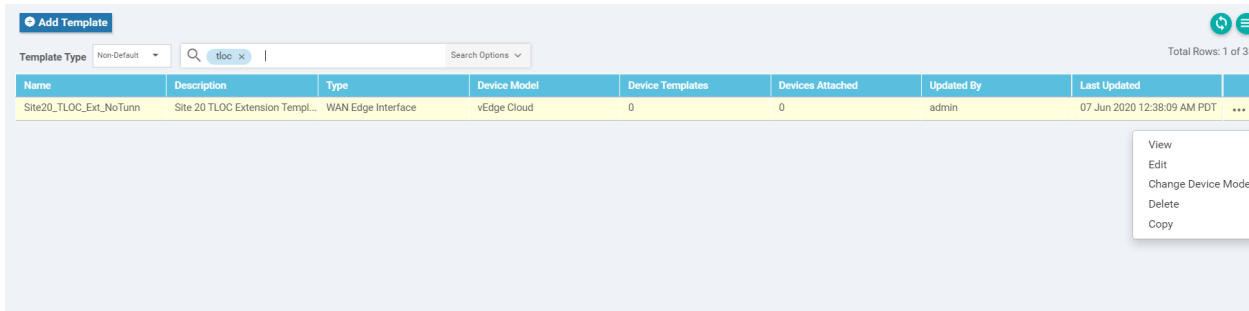
This completes configuration of the VPN Interface Template for TLOC Extension interfaces, without a Tunnel. Each participating vEdge/cEdge will have an interface that will not have a Tunnel associated with it (but will have a TLOC Extension association) and another one which will have a Tunnel (but won't 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 the 'Add Template' interface with a search filter 'tloc' applied. The table below lists the search results.

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	...

A context menu is open over the first row, showing the following options: View, Edit, Change Device Models, Delete, and Copy.

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 🔍 tloc x Search Options Total Rows: 2 of 39

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	⋮

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]

Basic Configuration **Tunnel** NAT VRRP ACL/QoS ARP 802.1X Advanced

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

Update Cancel

Make sure you allow service all in the configuration above

This completes the configuration of our second feature template.

Task List

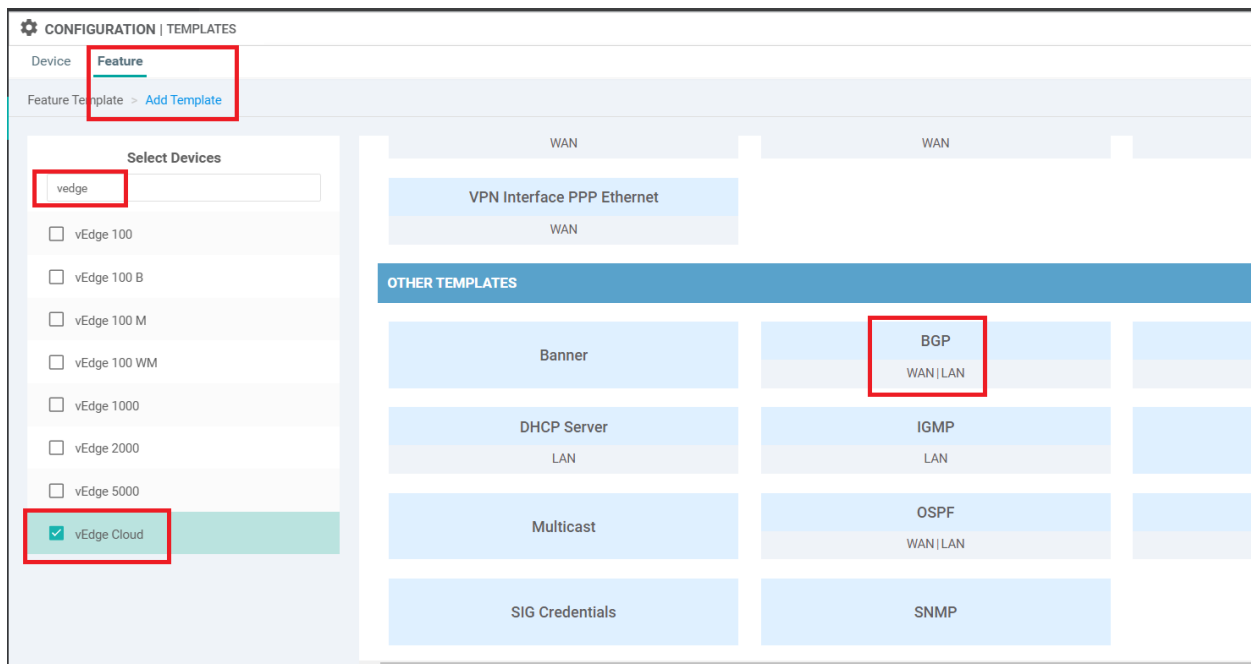
- Overview
- Feature Templates for TLOC Extensions
 - Creating the VPN Interface Template for the TLOC-EXT interface
 - Creating the VPN Interface Template for the Tunnel interface

- 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

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > BGP

Template Name: vedge21_mpls_bgp_tloc

Description: BGP Peering Template for TLOC Extension on the MPLS link

Basic Configuration | Unicast Address Family | Neighbor | Advanced

BASIC CONFIGURATION

Shutdown: Yes No [bgp_shutdown]

AS Number: 65534

Router ID:

Propagate AS Path: On Off

- 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

Basic Configuration | **Unicast Address Family** | Neighbor | Advanced

UNICAST ADDRESS FAMILY

IPv4 | IPv6

Maximum Paths: 2

RE-DISTRIBUTE | **NETWORK** | AGGREGATE ADDRESS

New Network

Network Prefix: 192.168.26.0/24

Add Cancel

Mark as Optional Row

- 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.

The screenshot shows the 'NEIGHBOR' configuration page. At the top, there are tabs for 'IPv4' and 'IPv6'. A 'New Neighbor' button is located in the top left corner. The main form contains several fields: 'Address' (192.0.2.9), 'Description' (checkbox), 'Remote AS' (65535), 'Address Family' (radio buttons for 'On' and 'Off'), 'Address Family' (dropdown menu showing 'ipv4-unicast'), 'Maximum Number of Prefixes' (checkbox), and 'Route Policy In' (radio buttons for 'On' and 'Off'). A red box highlights the 'Add' button on the right side of the form. A red text box at the bottom right says: '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**

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	View
Site20_vpn0_int	VPN0 Interface for Site20 dev...	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020	Edit
Site20_TLOC_Ext_NoTunn	Site 20 TLOC Extension Templ...	WAN Edge Interface	vEdge Cloud	0	0	admin	07 Jun 2020	Change Device Models Delete Copy

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

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]"/>	<input checked="" type="checkbox"/> 1	-
<input type="text" value="[tloc_ext_next_hop_ip]"/>	<input checked="" type="checkbox"/> 1	-

+ Add Next Hop 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 🌐 Mark as Optional Row ⓘ

Gateway Next Hop Null 0 VPN

Next Hop 2 Next Hop

Save Changes

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

+ New IPv4 Route

Optional	Prefix	Gateway	Selected	Gateway Configuration
<input type="checkbox"/>	🌐 0.0.0.0/0	Next Hop	2	

IPv6 ROUTE

+ New IPv6 Route

Optional	Prefix	Gateway	Selected	Gateway Configuration
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**

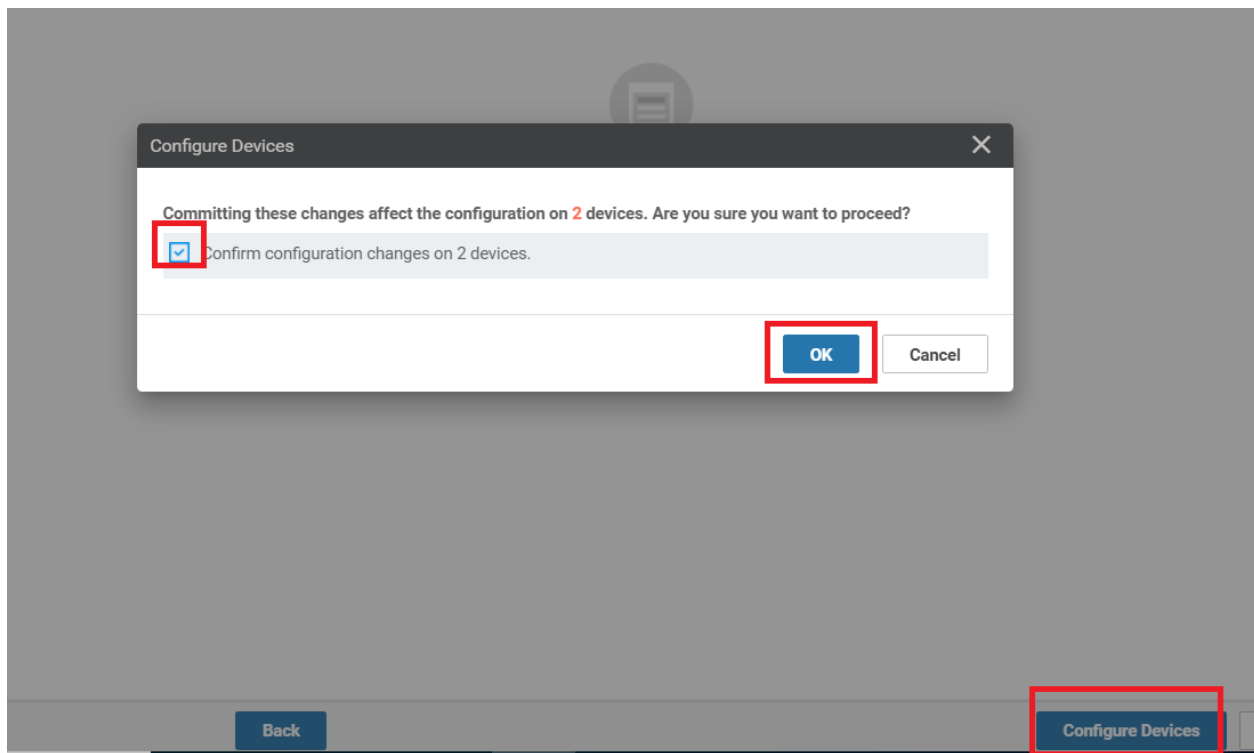
Search Options ▾

S...	Chassis Number	System IP	Hostname	ess(vpn512_mgmt_if_ip_add)	Address(vpn0_next_hop)	Address(tloc_ext_ next_hop_ip)	In
✓	b7fd7295-58df-7671-e914-6fe2edff1609	10.255.255.21	vEdge20	20/24	100.100.100.1	192.168.26.21	g
✓	dde90ff0-dc62-77e6-510f-08d96608537d	10.255.255.22	vEdge21	21/24	192.0.2.9	192.168.25.20	g

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**

Device Feature

Create Template

Template Type: Non-Default

Total Rows: 6

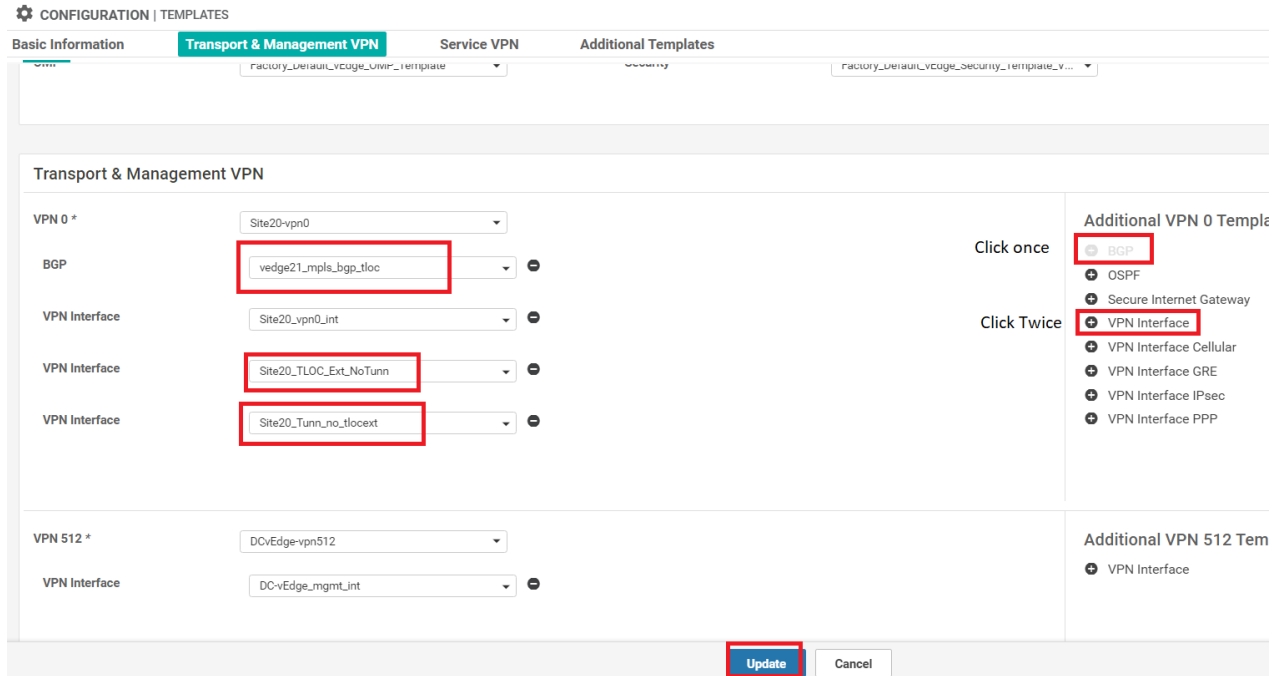
Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
DOvEdge_dev_temp	Device template for the D...	Feature	vEdge Cloud	16	2	admin	28 May 2020 4:58:07 AM ...	In Sync	...
cEdge-single-uplink	Single Uplink cEdge Devi...	Feature	CSR1000v	17	2	admin	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	...

Context menu for vEdge_Site20_dev_temp:

- Edit
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

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**



- 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

Update Device Template

Variable List (Hover over each field for more information)

Address(vpn0_next_nop)	100.100.100.1
Interface Name(vpn0_if_name)	ge0/0
IPv4 Address(vpn0_if_ip_add)	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
Interface Name(vpn20_if_name)	ge0/3
IPv4 Address(vpn20_if_ipv4_address)	10.20.20.2/24
Interface Name(vpn10_if_name)	ge0/2
IPv4 Address(vpn10_if_ipv4_address)	10.20.10.2/24
Address(tloc_ext_next_hop_ip)	192.168.26.21
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)	<input checked="" type="checkbox"/>
Interface Name(if_name_notunn_tlocext)	ge0/1
IPv4 Address(if_ipv4_address_notunn)	192.168.25.20/24
Shutdown(bgp_shutdown)	<input checked="" type="checkbox"/>

Generate Password

Update Cancel

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_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
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).

		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	107	no shutdown
69	!	108	!
70	ip route 0.0.0.0/0 192.0.2.9	109	ip route 0.0.0.0/0 192.0.2.9
71	ip route 0.0.0.0/0 192.168.25.20	110	ip route 0.0.0.0/0 192.168.25.20
72	!	111	!
73	vpn 10	112	vpn 10
74	dns 10.2.1.5 primary	113	dns 10.2.1.5 primary
75	dns 10.2.1.6 secondary	114	dns 10.2.1.6 secondary
76	interface ge0/2	115	interface ge0/2
77	ip address 10.20.10.3/24	116	ip address 10.20.10.3/24

Back
Configure Devices

✔ **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.

14. 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: vpn0 x | 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 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 6:25:48 AM PDT	...
Site20_vpn0_int_nat	Interface for Site20 dev...	WAN Edge interface	vEdge Cloud	1	1	admin	07 Jun 2020 2:49:54 AM PDT	...
Site20_vpn0_int	Interface for Site20 dev...	WAN Edge interface	vEdge Cloud	1	1	admin	07 Jun 2020 2:46:50 AM PDT	...
cEdge_VPN0_dual_L	VPN 0 Template for Du...	Cisco VPN	CSR1000v	1	1	admin	23 May 2020 7:34:59 AM PDT	...
cedge-vpn0-int-dualLmplis	cEdge VPN 0 Interface Templa...	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

IPv4 | IPv6

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 | Total Rows: 7

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 cEdge 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			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_Ovrp_Template Security 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

VPN 512 * DCvEdge-vpn512

VPN Interface DC-vEdge_mgmt_int

Update Cancel

Change the VPN Interface to reflect the NAT enabled interface template. Click on Update and attach vEdge20.

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.

	Template	
1:07 A...	In Sync	Edit
1:01 A...	In Sync	View
1:53 A...	In Sync	Delete
3:06 ...	In Sync	Copy
1:40 P...	In Sync	Attach Devices
1:59 A...	In Sync	Detach Devices
1:21 A...	In Sync	Export CSV
		Change Device Values
		...

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		DOMAIN PEER	PEER		PEER				
		GROUP	SITE		PRIV	PEER	PUB	LOCAL	COLOR	FR	
TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	LOCAL	COLOR	FR
OKY	STATE	UPTIME	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	LOCAL	COLOR	FR
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# show bfd sess
```

SYSTEM IP	TX	SITE ID	STATE	COLOR	TLOC	REMOTE TLOC	SOURCE IP	DST PUBLIC IP	DST PUBLIC PORT	ENCAP	MUM
10.255.255.11	1	1000	up	public-internet	1	public-internet	100.100.100.20	100.100.100.10	2936	ipsec	7
			0:00:03:28								
10.255.255.11	1	1000	up	mpls	1	mpls	192.168.26.20	192.0.2.2	12426	ipsec	7
			0:00:03:14								
10.255.255.12	1	1000	up	public-internet	1	public-internet	100.100.100.20	100.100.100.11	22184	ipsec	7
			0:00:03:28								
10.255.255.12	1	1000	up	mpls	1	mpls	192.168.26.20	192.0.2.6	12426	ipsec	7
			0:00:03:13								
10.255.255.31	30	1000	up	public-internet	1	public-internet	100.100.100.20	100.100.100.30	50308	ipsec	7
			0:00:03:29								
10.255.255.31	30	1000	up	mpls	1	mpls	192.168.26.20	192.0.2.14	12366	ipsec	7
			0:00:03:13								
10.255.255.41	40	1000	up	public-internet	8	public-internet	100.100.100.20	100.100.100.40	12347	ipsec	7
			0:00:03:28								
10.255.255.41	40	1000	up	mpls	1	mpls	192.168.26.20	192.1.2.18	12387	ipsec	7
			0:00:03:13								
10.255.255.51	50	1000	up	public-internet	1	public-internet	100.100.100.20	100.100.100.50	12347	ipsec	7
			0:00:03:28								
10.255.255.52	50	1000	up	mpls	1	mpls	192.168.26.20	192.1.2.22	12347	ipsec	7
			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		DOMAIN PEER	PEER		PEER			
		GROUP	SITE		PRIV	PEER	PUB	LOCAL	COLOR	
TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	LOCAL	COLOR
OKY	STATE	UPTIME	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	LOCAL	COLOR
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`

```
vEdge20# show control connections
```

PEER	PEER PEER	CONTROLLER		DOMAIN	PEER	PEER		PEER					
		GROUP	SITE			PRIV	PEER	PUB	LOCAL	COLOR			
TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	PORT	PUBLIC	IP	PORT	LOCAL	COLOR
XY	STATE	UPTIME	ID	ID	PRIVATE	IP	IP	PORT	PUBLIC	IP	PORT	LOCAL	COLOR
vsmart	dtls	10.255.255.3	100	1	100.100.100.4			12446	100.100.100.4		12446	public-internet	
up		0:00:02:01	0										
vsmart	dtls	10.255.255.4	100	1	100.100.100.5			12446	100.100.100.5		12446	public-internet	
up		0:00:01:44	0										
vsmart	dtls	10.255.255.3	100	1	100.100.100.4			12446	100.100.100.4		12446	mpls	
up		0:00:01:44	0										
vsmart	dtls	10.255.255.4	100	1	100.100.100.5			12446	100.100.100.5		12446	mpls	
up		0:00:01:44	0										
vmanage	dtls	10.255.255.1	1000	0	100.100.100.2			12846	100.100.100.2		12846	public-internet	
up		0:00:02:01	0										

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`

```
vEdge21# show control connections
```

PEER	PEER PEER	CONTROLLER		DOMAIN	PEER	PEER		PEER						
		GROUP	SITE			PRIV	PEER	PUB	LOCAL	COLOR	PR			
TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	PORT	PUBLIC	IP	PORT	LOCAL	COLOR	PR
XY	STATE	UPTIME	ID	ID	PRIVATE	IP	IP	PORT	PUBLIC	IP	PORT	LOCAL	COLOR	PR
vsmart	dtls	10.255.255.3	1000	1	100.100.100.4			12346	100.100.100.4		12346	mpls		No
up		12:15:19:15	0											
vsmart	dtls	10.255.255.4	1000	1	100.100.100.5			12346	100.100.100.5		12346	mpls		No
up		12:15:19:00	0											
vsmart	dtls	10.255.255.3	1000	1	100.100.100.4			12346	100.100.100.4		12346	public-internet		No
up		0:00:01:30	0											
vsmart	dtls	10.255.255.4	1000	1	100.100.100.5			12346	100.100.100.5		12346	public-internet		No
up		0:00:01:30	0											
vmanage	dtls	10.255.255.1	1000	0	100.100.100.2			12346	100.100.100.2		12346	mpls		No
up		14:19:27:07	0											

```
vEdge21# show bfd sess
```

TECT	TX	SYSTEM	IP	SITE	ID	STATE	UPTIME	SOURCE	TLOC	REMOTE	TLOC	SOURCE	IP	DST	PUBLIC	DST	PUBLIC	ENCAP	DE
		10.255.255.11	1000	1	up	3:19:21:21	2	mpls		mpls		192.0.2.10		192.0.2.2		12426		ipsec	7
		10.255.255.11	1000	1	up	0:00:02:20	0	public-internet		public-internet		192.168.25.21		100.100.100.10		2936		ipsec	7
		10.255.255.12	1000	1	up	3:19:21:21	2	mpls		mpls		192.0.2.10		192.0.2.6		12426		ipsec	7
		10.255.255.12	1000	1	up	0:00:02:20	0	public-internet		public-internet		192.168.25.21		100.100.100.11		22184		ipsec	7
		10.255.255.31	1000	30	up	9:22:35:21	5	mpls		mpls		192.0.2.10		192.0.2.14		12366		ipsec	7
		10.255.255.31	1000	30	up	0:00:02:20	0	public-internet		public-internet		192.168.25.21		100.100.100.30		50308		ipsec	7
		10.255.255.41	1000	40	up	2:16:12:21	0	mpls		mpls		192.0.2.10		192.1.2.18		12387		ipsec	7
		10.255.255.41	1000	40	up	0:00:02:20	0	public-internet		public-internet		192.168.25.21		100.100.100.40		12347		ipsec	7
		10.255.255.51	1000	50	up	0:00:02:20	0	public-internet		public-internet		192.168.25.21		100.100.100.50		12347		ipsec	7
		10.255.255.52	1000	50	up	3:19:21:22	7	mpls		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

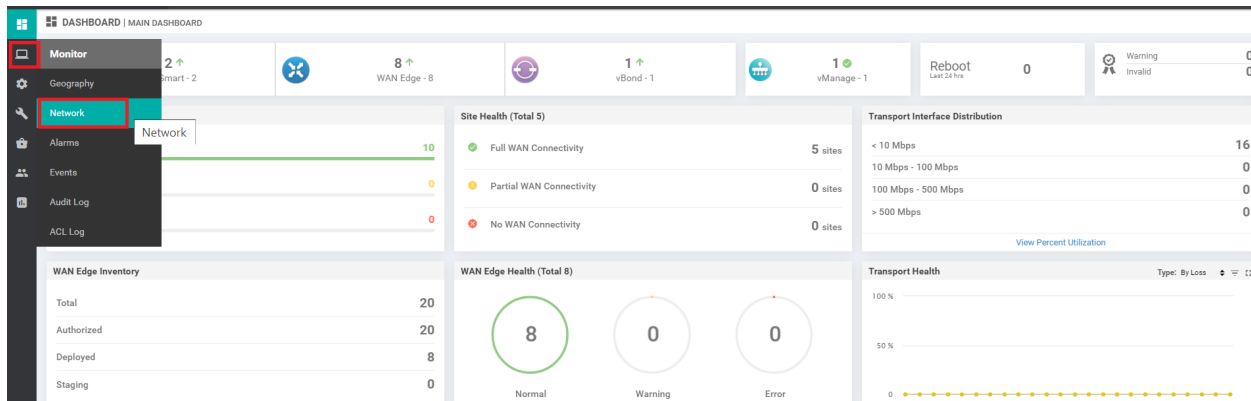
Overview

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.

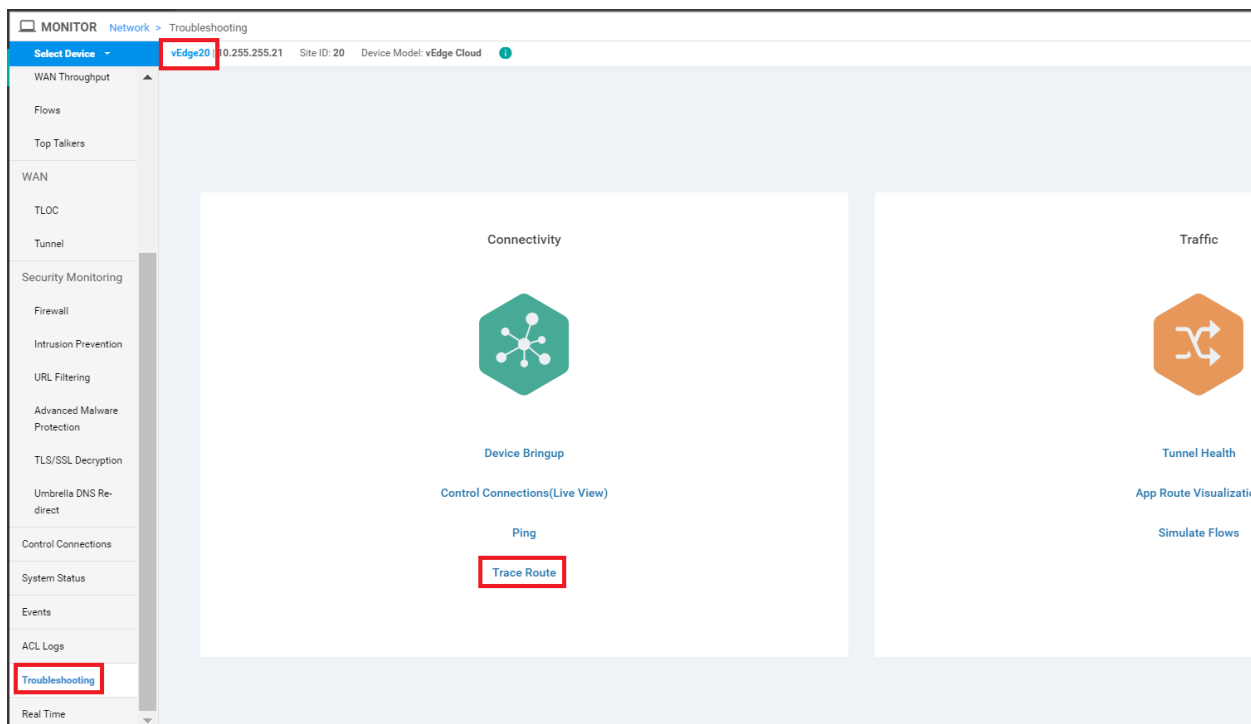
Cisco SD-WAN Policies allow us to enforce a custom topology, thereby controlling the data flow within our network. We will be setting up a Hub and Spoke topology for VPN 20 at all Branch sites, steering data to the DC site, post which it will be

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)

The screenshot shows a configuration panel for a traceroute test. The 'Destination IP' is set to 10.30.20.2, the 'VPN' is 'VPN - 20', and the 'Source/Interface for VPN - 20' is 'ge0/3 - ipv4 - 10.20.20.2'. A red box highlights these fields. Below the configuration is an 'Advanced Options' section and a 'Start' button. The 'Output' section shows the traceroute results: 'Traceroute -m 15 -w 1 -s 10.20.20.2 10.30.20.2 in VPN 20', 'traceroute to 10.30.20.2 (10.30.20.2), 15 hops max, 60 byte packets', and '1 10.30.20.2 (10.30.20.2) 0.343 ms 0.414 ms 0.415 ms'. A diagram shows a direct connection from 'ge0/3 - ipv4 - 10.20.20.2' to '10.30.20.2' with a latency of 0.39ms. A green box highlights the diagram, and a green text annotation says 'Traffic is going directly to Site 30'.

4. Run another test, this time to the **Destination IP** of 10.40.20.2. Traffic again flows directly between the sites

The screenshot shows the same configuration panel as above, but with the 'Destination IP' set to 10.40.20.2, highlighted by a red box. The 'Advanced Options' section is expanded. The 'Output' section shows the traceroute results: 'Traceroute -m 15 -w 1 -s 10.20.20.2 10.40.20.2 in VPN 20', 'traceroute to 10.40.20.2 (10.40.20.2), 15 hops max, 60 byte packets', and '1 10.40.20.2 (10.40.20.2) 215.054 ms **'. A diagram shows a direct connection from 'ge0/3 - ipv4 - 10.20.20.2' to '10.40.20.2' with a latency of 215.05ms.

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 - 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, 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  TLOC IP    COLOR
-----
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
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	CSR1000v	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	CSR1000v	1	1	admin	23 May 2020 7:15:33 AM PDT
INET interface for the Site30 vEdges	WAN Edge Interface	vEdge Cloud	1	1	admin	23 May 2020 6:27:24 AM PDT
cEdge VPN 512 Interface Template...	Cisco VPN Interface	CSR1000v	2	3	admin	18 May 2020 8:39:03 AM PDT
VPN 10 Template for the cEdges	Cisco VPN	CSR1000v	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	CSR1000v	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 1:48:16 PM PDT
cEdge VPN 0 Template for Dual Up...	Cisco VPN	CSR1000v	1	1	admin	23 May 2020 7:34:59 AM PDT
VPN 20 Template for the cEdges	Cisco VPN	CSR1000v	2	3	admin	25 May 2020 1:55:27 PM PDT
VPN 30 Interface Template for cEd...	Cisco VPN Interface	CSR1000v	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_NET	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-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_Luplink	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	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_Luplink	cEdge VPN 0 Template for Dual Up...	Cisco VPN	CSR1000v	1	1	admin	23 May 2020 10:07:03 AM PDT	View
cedge-vpn20	VPN 20 Template for the cEdges	Cisco VPN	CSR1000v	2	3	admin	25 May 2020 1:38:04 PM PDT	Edit
cedge-vpn30-int	VPN 30 Interface Template for cEd...	Cisco VPN Interface	CSR1000v	2	3	admin	25 May 2020 1:38:04 PM PDT	Change Device Models
DC-vEdge_mgmt_int	MGMT interface for the DC-vEdges	WAN Edge interface	vEdge Cloud	3	5	admin	23 May 2020 10:07:03 AM PDT	Delete
vSmart_VPN512	VPN512 Template for the vSmarts	vSmart VPN	vSmart	1	2	admin	25 May 2020 10:07:03 AM PDT	Copy
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	...
VPN vEdge_MBI_0	MBI 0 interface for the VPN vEdges	WAN Edge interface	vEdge Cloud	1	2	admin	23 May 2020 1:45:22 AM PDT	...

- Rename the template *vedge-vpn20-DC* with a Description of *VPN 20 Template for vEdges at the Data Center* and click on **Copy**

Template Copy ✕

Template Name

vedge-vpn20-DC

Description

VPN 20 Template for vEdges at the Data Center

Copy
Cancel

- 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: 20

Name: Po2

Enhance ECMP Keying: On Off

Enable TCP Optimization: On Off

- 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

New IPv4 Route 1

Prefix: 0.0.0.0/0 2

Gateway: Next Hop Null 0 VPN

Enable Null0: On Off 4

Distance: 1

5 **Add** Cancel

Optional	Prefix	Gateway	Selected Gateway Configuration	Action
No data available				

6 **Update** Cancel

- Go to **Configuration => Templates => Device Tab** and locate the *DCvEdge_dev_temp*. Click on the three dots to the template and choose to **Edit**

Device Feature

Create Template

Template Type: Non-Default

Total Rows: 6

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
vEdge30_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

Edit
View
Delete
Copy
Attach Devices
Detach Devices
Export CSV

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)

Service VPN

1 Rows Selected Add VPN Remove VPN

Total Rows: 2

ID	Template Name	Sub-Templates
e9acf7d-aa66-4913-8f0a-84e255b4b033	vedge-vpn10	OSPF, VPN Interface
6fd47ee6-61c1-4b02-9b3e-439f5c423b74	vedge-vpn20	VPN Interface

8. Confirm removal of the VPN by clicking on **Remove**

Remove VPN Confirmation

Are you sure you want to remove the selected Service VPN(s)

Remove Cancel

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**

Service VPN

0 Rows Selected Add VPN Remove VPN

Available VPN Templates

ID	Template Name
6fd47ee6-61c1-4b02-9b3e-439f5c423b74	vedge-vpn20

Selected VPN Templates

ID	Template Name
b939aaa7-2e26-4eaf-9b35-f28cd8744b43	vedge-vpn20-DC

10. Click on **VPN Interface** under **Additional VPN Templates** 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**

VPN Interface

Sub-Templates

Additional VPN Templates

- + BGP
- + IGMP
- + Multicast
- + OSPF
- + PIM
- + **VPN Interface**
- + VPN Interface Bridge
- + VPN Interface GRE
- + VPN Interface IPsec
- + VPN Interface Natpool

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 Add
✓	e474c5fd-8ce7-d376-7cac-ba950b2c9159	10.255.255.11	DC-vEdge1	ge0/3	10.100.20.2/24	ge0/2	10.100.10
✓	0cdd4f0e-f2f1-fe75-866c-469966cda1c3	10.255.255.12	DC-vEdge2	ge0/3	10.100.20.3/24	ge0/2	10.100.10

Next Cancel

Device Template	Total
DCvEdge_dev_temp	1

Device list (Total: 2 devices)

Filter/Search

e474c5fd-8ae7-d376-7cac-ba950b2e9159
DC-vEdge110.255.255.11

Dcdd4f0e-f2f1-fe75-866c-469966cda1c3
DC-vEdge2110.255.255.12

```

101 exit
102 exit
103 !
104 !
105 interface ge0/2
106 ip address 10.100.10.2/24
107 no shutdown
108 !
109 cmp
110 advertise connected
111 advertise static
112 !
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
124 !
125 !
126 vpn 512
127 dns 10.2.1.5 primary
128 dns 10.2.1.6 secondary
129 interface eth0
130 ip address 192.168.0.10/24
131 no shutdown
132 !
133 !
134 !
135 !
136 !
137 !
138 !
139 !
140 !
141 !
142 !
143 !
144 !
145 !
146 !
147 !
148 !
149 !
150 !
151 !
152 !
153 !
154 !
155 !
156 !
157 !
158 !
159 !
160 !
161 !
162 !
163 !
164 !
165 !
166 !
167 !
168 !
169 !
170 !
171 !
172 !
173 !
174 !
175 !
176 !
177 !
178 !
179 !
180 !
181 !
182 !
183 !
184 !
185 !
186 !
187 !
188 !
189 !
190 !
191 !
192 !
193 !
194 !
195 !
196 !
197 !
198 !
199 !
200 !
201 !
202 !
203 !
204 !
205 !
206 !
207 !
208 !
209 !
210 !
211 !
212 !
213 !
214 !
215 !
216 !
217 !
218 !
219 !
220 !
221 !
222 !
223 !
224 !
225 !
226 !
227 !
228 !
229 !
230 !
231 !
232 !
233 !
234 !
235 !
236 !
237 !
238 !
239 !
240 !
241 !
242 !
243 !
244 !
245 !
246 !
247 !
248 !
249 !
250 !
251 !
252 !
253 !
254 !
255 !
256 !
257 !
258 !
259 !
260 !
261 !
262 !
263 !
264 !
265 !
266 !
267 !
268 !
269 !
270 !
271 !
272 !
273 !
274 !
275 !
276 !
277 !
278 !
279 !
280 !
281 !
282 !
283 !
284 !
285 !
286 !
287 !
288 !
289 !
290 !
291 !
292 !
293 !
294 !
295 !
296 !
297 !
298 !
299 !
300 !
301 !
302 !
303 !
304 !
305 !
306 !
307 !
308 !
309 !
310 !
311 !
312 !
313 !
314 !
315 !
316 !
317 !
318 !
319 !
320 !
321 !
322 !
323 !
324 !
325 !
326 !
327 !
328 !
329 !
330 !
331 !
332 !
333 !
334 !
335 !
336 !
337 !
338 !
339 !
340 !
341 !
342 !
343 !
344 !
345 !
346 !
347 !
348 !
349 !
350 !
351 !
352 !
353 !
354 !
355 !
356 !
357 !
358 !
359 !
360 !
361 !
362 !
363 !
364 !
365 !
366 !
367 !
368 !
369 !
370 !
371 !
372 !
373 !
374 !
375 !
376 !
377 !
378 !
379 !
380 !
381 !
382 !
383 !
384 !
385 !
386 !
387 !
388 !
389 !
390 !
391 !
392 !
393 !
394 !
395 !
396 !
397 !
398 !
399 !
400 !
401 !
402 !
403 !
404 !
405 !
406 !
407 !
408 !
409 !
410 !
411 !
412 !
413 !
414 !
415 !
416 !
417 !
418 !
419 !
420 !
421 !
422 !
423 !
424 !
425 !
426 !
427 !
428 !
429 !
430 !
431 !
432 !
433 !
434 !
435 !
436 !
437 !
438 !
439 !
440 !
441 !
442 !
443 !
444 !
445 !
446 !
447 !
448 !
449 !
450 !
451 !
452 !
453 !
454 !
455 !
456 !
457 !
458 !
459 !
460 !
461 !
462 !
463 !
464 !
465 !
466 !
467 !
468 !
469 !
470 !
471 !
472 !
473 !
474 !
475 !
476 !
477 !
478 !
479 !
480 !
481 !
482 !
483 !
484 !
485 !
486 !
487 !
488 !
489 !
490 !
491 !
492 !
493 !
494 !
495 !
496 !
497 !
498 !
499 !
500 !
501 !
502 !
503 !
504 !
505 !
506 !
507 !
508 !
509 !
510 !
511 !
512 !
513 !
514 !
515 !
516 !
517 !
518 !
519 !
520 !
521 !
522 !
523 !
524 !
525 !
526 !
527 !
528 !
529 !
530 !
531 !
532 !
533 !
534 !
535 !
536 !
537 !
538 !
539 !
540 !
541 !
542 !
543 !
544 !
545 !
546 !
547 !
548 !
549 !
550 !
551 !
552 !
553 !
554 !
555 !
556 !
557 !
558 !
559 !
560 !
561 !
562 !
563 !
564 !
565 !
566 !
567 !
568 !
569 !
570 !
571 !
572 !
573 !
574 !
575 !
576 !
577 !
578 !
579 !
580 !
581 !
582 !
583 !
584 !
585 !
586 !
587 !
588 !
589 !
590 !
591 !
592 !
593 !
594 !
595 !
596 !
597 !
598 !
599 !
600 !
601 !
602 !
603 !
604 !
605 !
606 !
607 !
608 !
609 !
610 !
611 !
612 !
613 !
614 !
615 !
616 !
617 !
618 !
619 !
620 !
621 !
622 !
623 !
624 !
625 !
626 !
627 !
628 !
629 !
630 !
631 !
632 !
633 !
634 !
635 !
636 !
637 !
638 !
639 !
640 !
641 !
642 !
643 !
644 !
645 !
646 !
647 !
648 !
649 !
650 !
651 !
652 !
653 !
654 !
655 !
656 !
657 !
658 !
659 !
660 !
661 !
662 !
663 !
664 !
665 !
666 !
667 !
668 !
669 !
670 !
671 !
672 !
673 !
674 !
675 !
676 !
677 !
678 !
679 !
680 !
681 !
682 !
683 !
684 !
685 !
686 !
687 !
688 !
689 !
690 !
691 !
692 !
693 !
694 !
695 !
696 !
697 !
698 !
699 !
700 !
701 !
702 !
703 !
704 !
705 !
706 !
707 !
708 !
709 !
710 !
711 !
712 !
713 !
714 !
715 !
716 !
717 !
718 !
719 !
720 !
721 !
722 !
723 !
724 !
725 !
726 !
727 !
728 !
729 !
730 !
731 !
732 !
733 !
734 !
735 !
736 !
737 !
738 !
739 !
740 !
741 !
742 !
743 !
744 !
745 !
746 !
747 !
748 !
749 !
750 !
751 !
752 !
753 !
754 !
755 !
756 !
757 !
758 !
759 !
760 !
761 !
762 !
763 !
764 !
765 !
766 !
767 !
768 !
769 !
770 !
771 !
772 !
773 !
774 !
775 !
776 !
777 !
778 !
779 !
780 !
781 !
782 !
783 !
784 !
785 !
786 !
787 !
788 !
789 !
790 !
791 !
792 !
793 !
794 !
795 !
796 !
797 !
798 !
799 !
800 !
801 !
802 !
803 !
804 !
805 !
806 !
807 !
808 !
809 !
810 !
811 !
812 !
813 !
814 !
815 !
816 !
817 !
818 !
819 !
820 !
821 !
822 !
823 !
824 !
825 !
826 !
827 !
828 !
829 !
830 !
831 !
832 !
833 !
834 !
835 !
836 !
837 !
838 !
839 !
840 !
841 !
842 !
843 !
844 !
845 !
846 !
847 !
848 !
849 !
850 !
851 !
852 !
853 !
854 !
855 !
856 !
857 !
858 !
859 !
860 !
861 !
862 !
863 !
864 !
865 !
866 !
867 !
868 !
869 !
870 !
871 !
872 !
873 !
874 !
875 !
876 !
877 !
878 !
879 !
880 !
881 !
882 !
883 !
884 !
885 !
886 !
887 !
888 !
889 !
890 !
891 !
892 !
893 !
894 !
895 !
896 !
897 !
898 !
899 !
900 !
901 !
902 !
903 !
904 !
905 !
906 !
907 !
908 !
909 !
910 !
911 !
912 !
913 !
914 !
915 !
916 !
917 !
918 !
919 !
920 !
921 !
922 !
923 !
924 !
925 !
926 !
927 !
928 !
929 !
930 !
931 !
932 !
933 !
934 !
935 !
936 !
937 !
938 !
939 !
940 !
941 !
942 !
943 !
944 !
945 !
946 !
947 !
948 !
949 !
950 !
951 !
952 !
953 !
954 !
955 !
956 !
957 !
958 !
959 !
960 !
961 !
962 !
963 !
964 !
965 !
966 !
967 !
968 !
969 !
970 !
971 !
972 !
973 !
974 !
975 !
976 !
977 !
978 !
979 !
980 !
981 !
982 !
983 !
984 !
985 !
986 !
987 !
988 !
989 !
990 !
991 !
992 !
993 !
994 !
995 !
996 !
997 !
998 !
999 !
1000 !

```

Configure Device Rollback Timer

Back

Configure Devices

Cancel

12. Confirm the change on 2 devices (the DC-vEdges)

Configure Devices ✕

Committing these changes affect the configuration on **2** devices. Are you sure you want to proceed?

Confirm configuration changes on 2 devices.

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 SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	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 SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	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

```
vEdge20#
```

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](#)

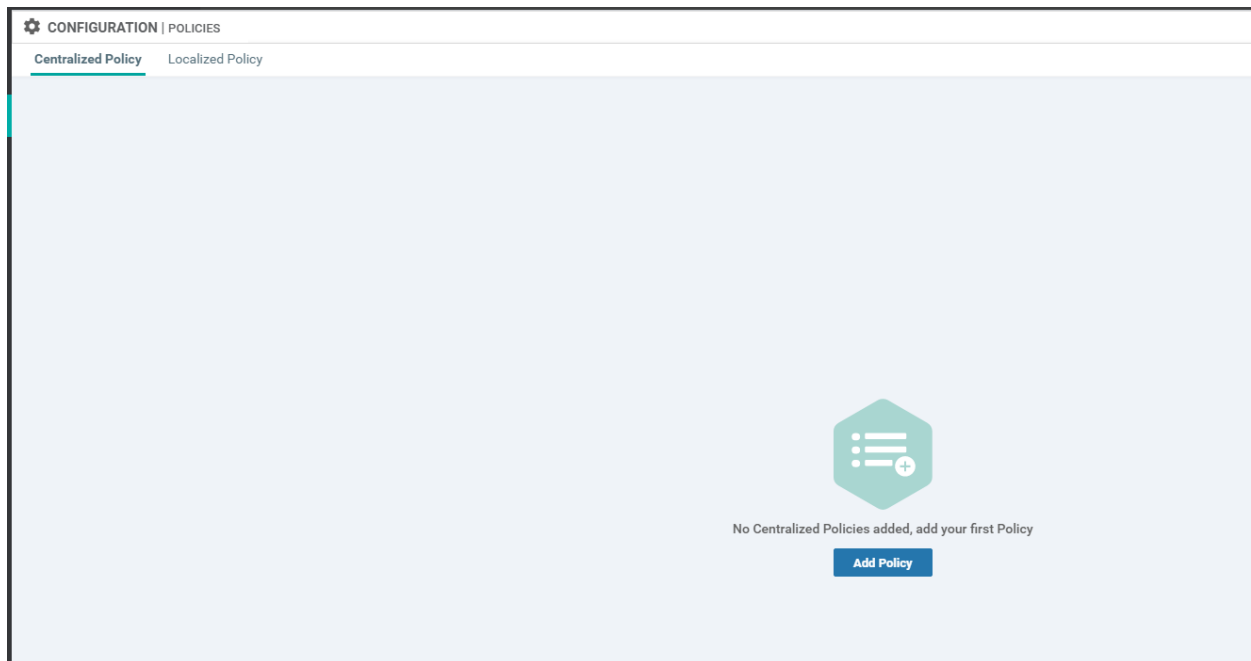
Creating the Policy

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.

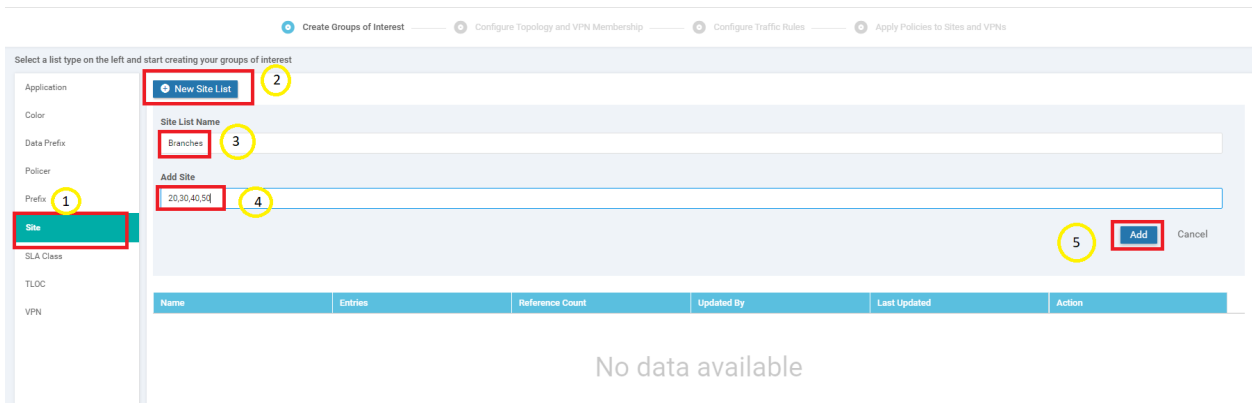
Configuring Network Constructs

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**

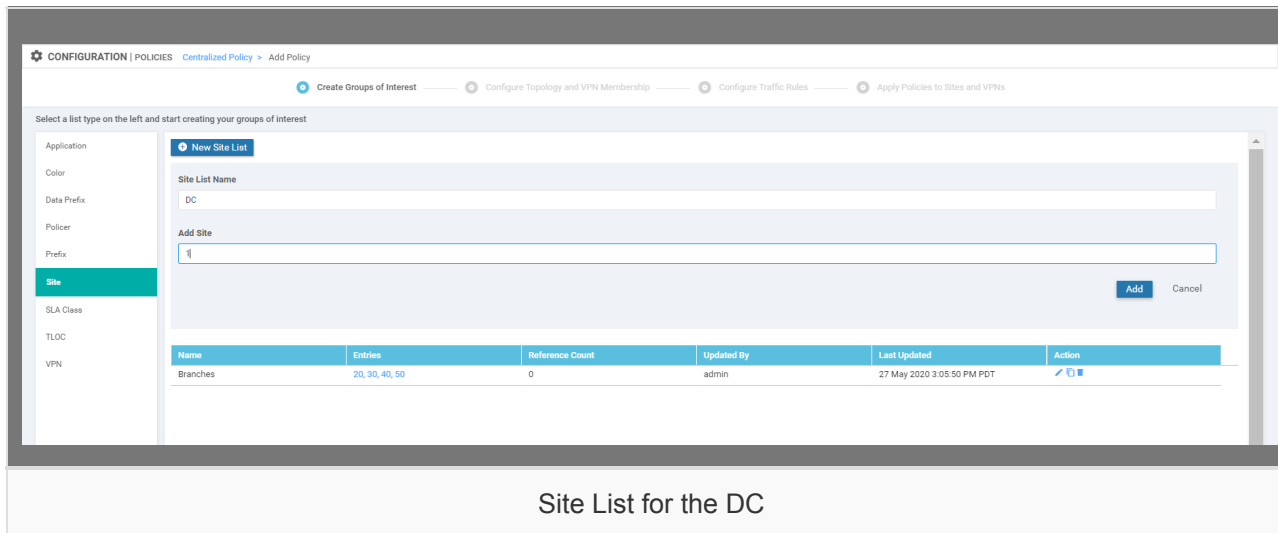


3. We will first create a Site List. Click on **Sites** and then choose **New Site List**. Give it a name of *Branches* and enter *20,30,40,50* in the **Add Site** section. Click on **Add**



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



Site List for the DC

4 Create Groups of Interest — 5 Configure Topology and VPN Membership — 6 Configure Traffic Rules — 7 Apply Policies to Sites and VPNs

Select a list type on the left and start creating your groups of interest

Application

Color

Data Prefix

Policer

Prefix

Site

SLA Class

TLOC

VPN

New Site List

Site List Name
Site30

Add Site

30

Add Cancel

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

CONFIGURATION | POLICIES Centralized Policy > Add Policy

4 Create Groups of Interest — 5 Configure Topology and VPN Membership — 6 Configure Traffic Rules — 7 Apply Policies to Sites and VPNs

Select a list type on the left and start creating your groups of interest

Application

Color

Data Prefix

Policer

Prefix

Site

SLA Class

TLOC

VPN

New Site List

Site List Name
Site40

Add Site

40

Add Cancel

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

Application **New Site List**

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	/ +

Application: Application, Color, Data Prefix, Policer, Prefix, **Site**, SLA Class, TLOC, VPN

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**

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 VPN List** 2

VPN List Name Corporate 3

Add VPN 10 4

5 **Add** Cancel

VPN 1

Name	Entries	Reference Count	Updated By	Last Updated	Action
No data available					

Application: Application, Color, Data Prefix, Policer, Prefix, Site, SLA Class, TLOC, **VPN**

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

Cisco vManage

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
- Color
- Data Prefix
- Policer
- Prefix
- Site
- SLA Class
- TLOC**
- VPN

New TLOC List

TLOC List

List Name
DC-TLOCs

TLOC IP	Color	Encap	Preference
10.255.255.11	public-internet	ipsec	0-4294967295

Add TLOC Click Add TLOC multiple times to add all TLOCs from DC

Save Cancel

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

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

- Application
- Color
- Data Prefix
- Policer
- Prefix
- Site
- SLA Class
- TLOC**
- VPN

+ New TLOC List

	Name	TLOC	Color	Encap	Preference	Reference Co...	Updated By
▼	DC-TLOCs					0	admin
		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	--		

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)**

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest — Configure Topology and VPN Membership — Conf

Specify your network topology

Topology VPN Membership

+ Add Topology ▾

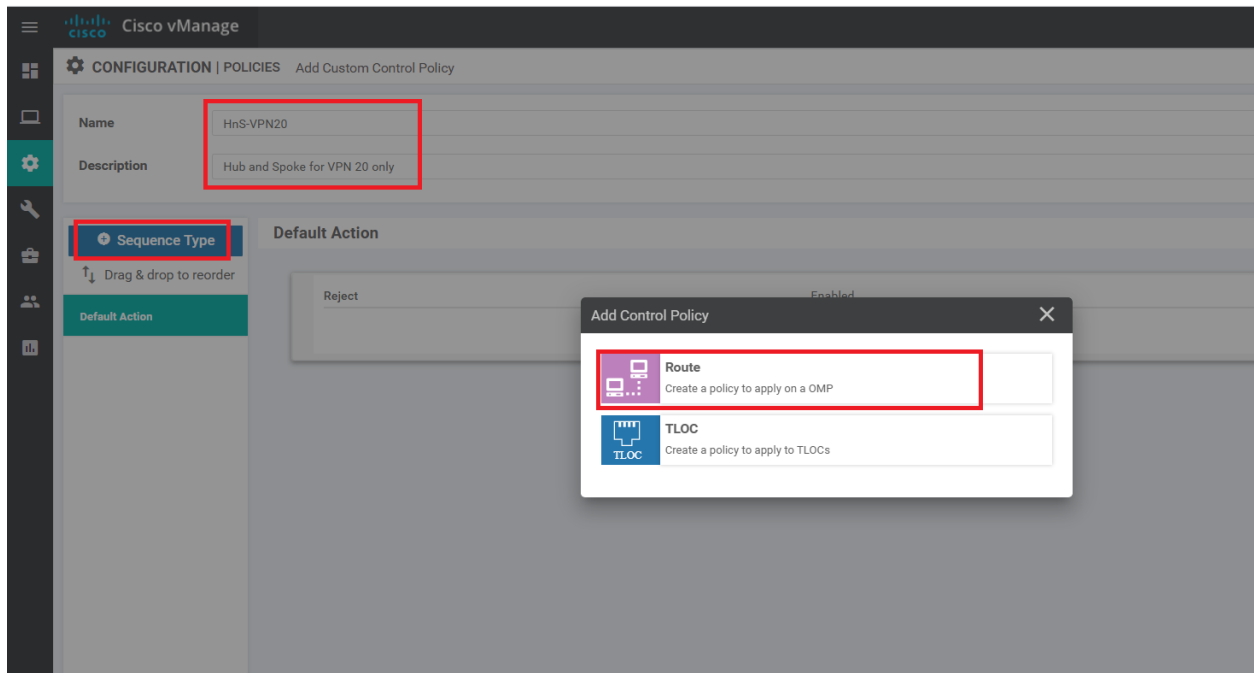
- Hub-and-Spoke
- Mesh
- Custom Control (Route & TLOC)
- Import Existing Topology

Search Options ▾

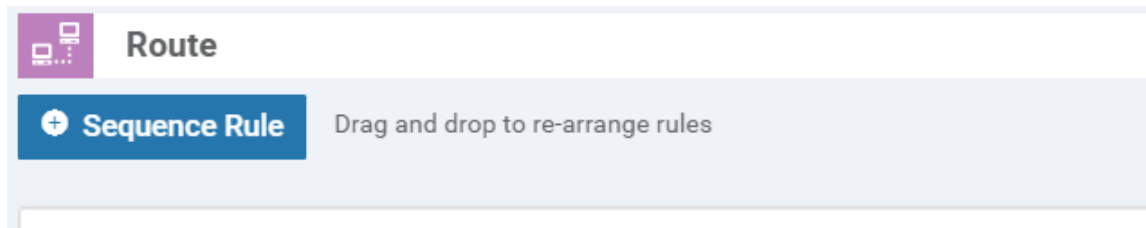
Type	Description	Reference Count
------	-------------	-----------------

No data available

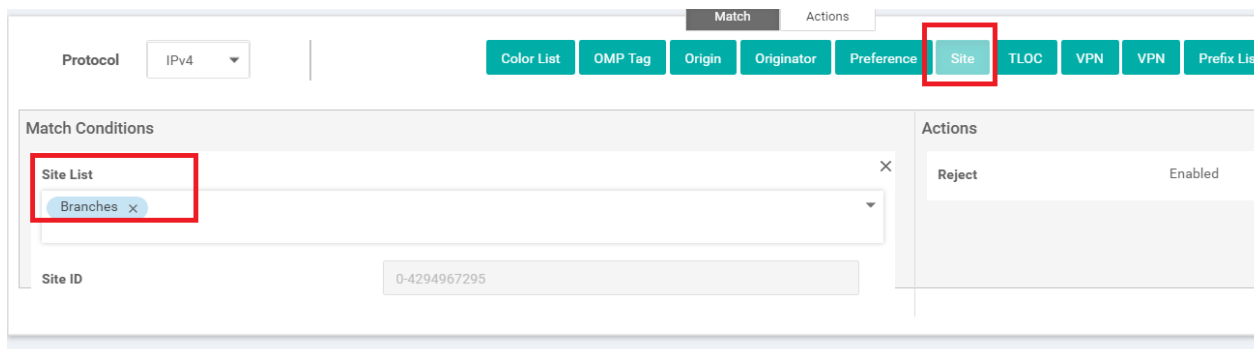
2. Specify a **Name** of *HnS-VPN20* with a Description of *Hub and Spoke for VPN 20 only*. Click on **Sequence Type** and choose to add a **Route** Control Policy



3. Click on **Sequence Rule** to add a new rule



4. Under **Match** click on **Site** and populate *Branches* in the **Site List** (this is one of the Site Lists we had created before)



5. Still under **Match**, click on **VPN** and choose *PoS* in the **VPN List**

Match Conditions

Site List: Branches

Site ID: 0-4294967295

VPN List: PoS

VPN ID: 0-65536

Actions: Reject (Enabled)

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**

Route

Sequence Rule

Protocol: IPv4

Match: Actions

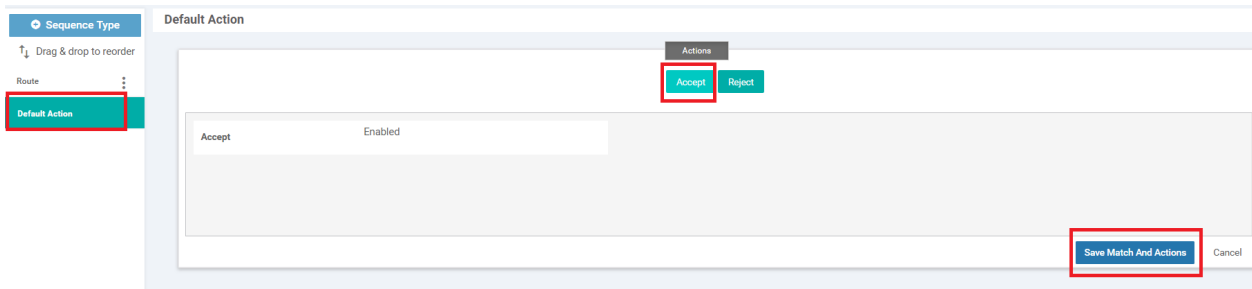
Export To: OMP Tag, Preference, Service, TLOC Action, TLOC

Match Conditions: Site List (Branches), Site ID (0-4294967295), VPN List (PoS), VPN ID (0-65536)

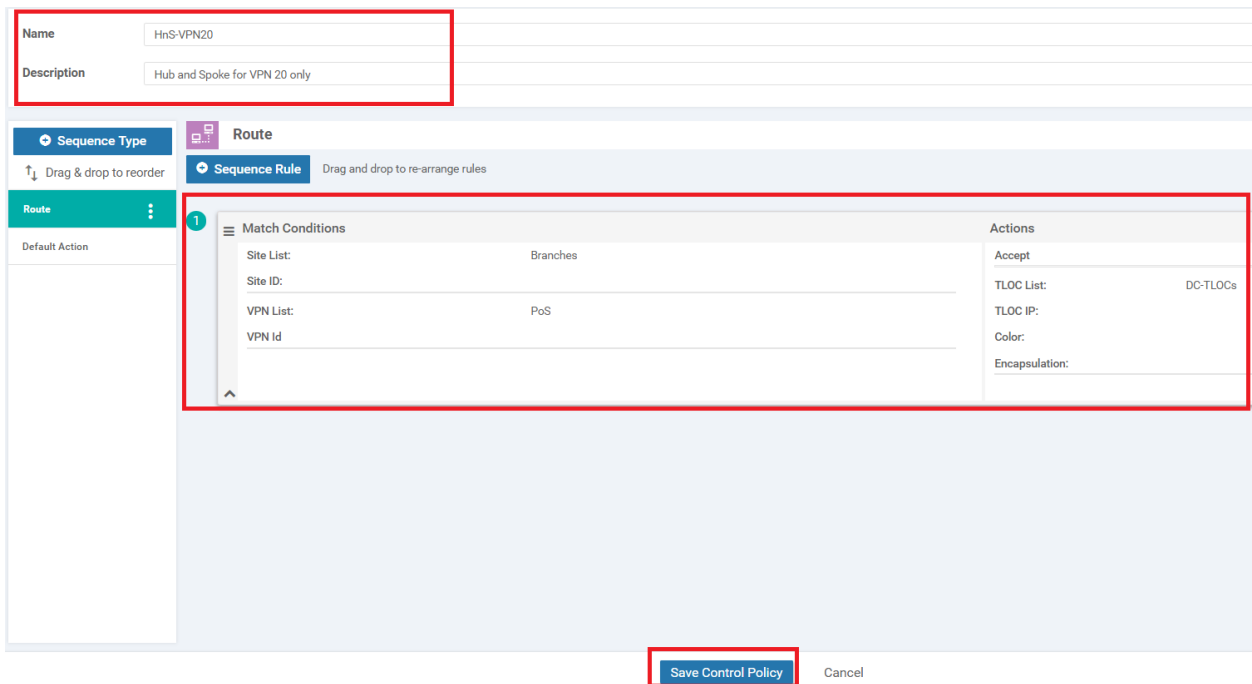
Actions: Accept (Enabled), TLOC List (DC-TLOCs), TLOC IP (Example: 10.0.0.1), Color (Select a color list), Encapsulation (Select an encap)

Save Match And Actions

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

Search Options

Name	Type	Description	Reference Count	Updated By	
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)

Search Options

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**

Add policies to sites and VPNs

Policy Name: Hub-n-Spoke-VPN20-only
Policy Description: Hub and Spoke policy for VPN 20 only

Topology | Application-Aware Routing | Traffic Data | Cflowd

HnS-VPN20 CUSTOM CONTROL

New Site List (1)

Inbound Site List
Select one or more site lists

Outbound Site List (2)
Branches (3)

Add (3) Cancel

Direction	Site List	Action
-----------	-----------	--------

BACK | Preview | Save Policy (4) | CANCEL

Activate Windows
Go to Settings to activate Windows.

✓ **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

CONFIGURATION | POLICIES Custom Options

Centralized Policy Localized Policy

[Add Policy](#) Total Rows: 1

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	...

View
 Preview
 Copy
 Edit
 Delete
Activate

12. Confirm the activation by clicking on **Activate**

Activate Policy
✕

Policy will be applied to the reachable vSmarts:
 10.255.255.3, 10.255.255.4

Activate
Cancel

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 | 10.255.255.21 Site ID: 20 Device Model: vEdge Cloud

Device Options: IP Routes

Filter VPN ID: 20

Total Rows: 11

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	Ne
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	10.20.20.0/24	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

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

Destination IP * 10.30.20.2 VPN VPN - 20 Source/Interface for VPN - 20 ge0/3 - ipv4 - 10.20.20.2

Advanced Options >

Start

Output

```
Traceroute -m 15 -w 1 -s 10.20.20.2 10.30.20.2 in VPN 20
traceroute to 10.30.20.2 (10.30.20.2), 15 hops max, 60 byte packets
 1 10.100.20.3 (10.100.20.3) 0.299 ms 0.366 ms 0.368 ms
 2 10.30.20.2 (10.30.20.2) 0.558 ms 0.666 ms 0.768 ms
```

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

MONITOR Network > Troubleshooting > Traceroute

Select Device vEdge20 | 10.255.255.21 Site ID: 20 Device Model: vEdge Cloud Troubleshooting

Destination IP * 10.40.20.2 VPN VPN-20 Source/Interface for VPN - 20 ge0/3 - ipv4 - 10.20.20.2

Advanced Options >

Start

Output

Traceroute -m 15 -w 1 -s 10.20.20.2 10.40.20.2 in VPN 20
 traceroute to 10.40.20.2 (10.40.20.2), 15 hops max, 60 byte packets

1 10.100.20.3 (10.100.20.3) 0.362 ms 0.445 ms 0.446 ms
 2 10.40.20.2 (10.40.20.2) 1.009 ms **

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

Destination IP * 10.40.10.2 VPN VPN-10 Source/Interface for VPN - 10 ge0/2 - ipv4 - 10.20.10.2

Advanced Options >

Start

Output

Traceroute -m 15 -w 1 -s 10.20.10.2 10.40.10.2 in VPN 10
 traceroute to 10.40.10.2 (10.40.10.2), 15 hops max, 60 byte packets

1 10.40.10.2 (10.40.10.2) 0.848 ms **

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

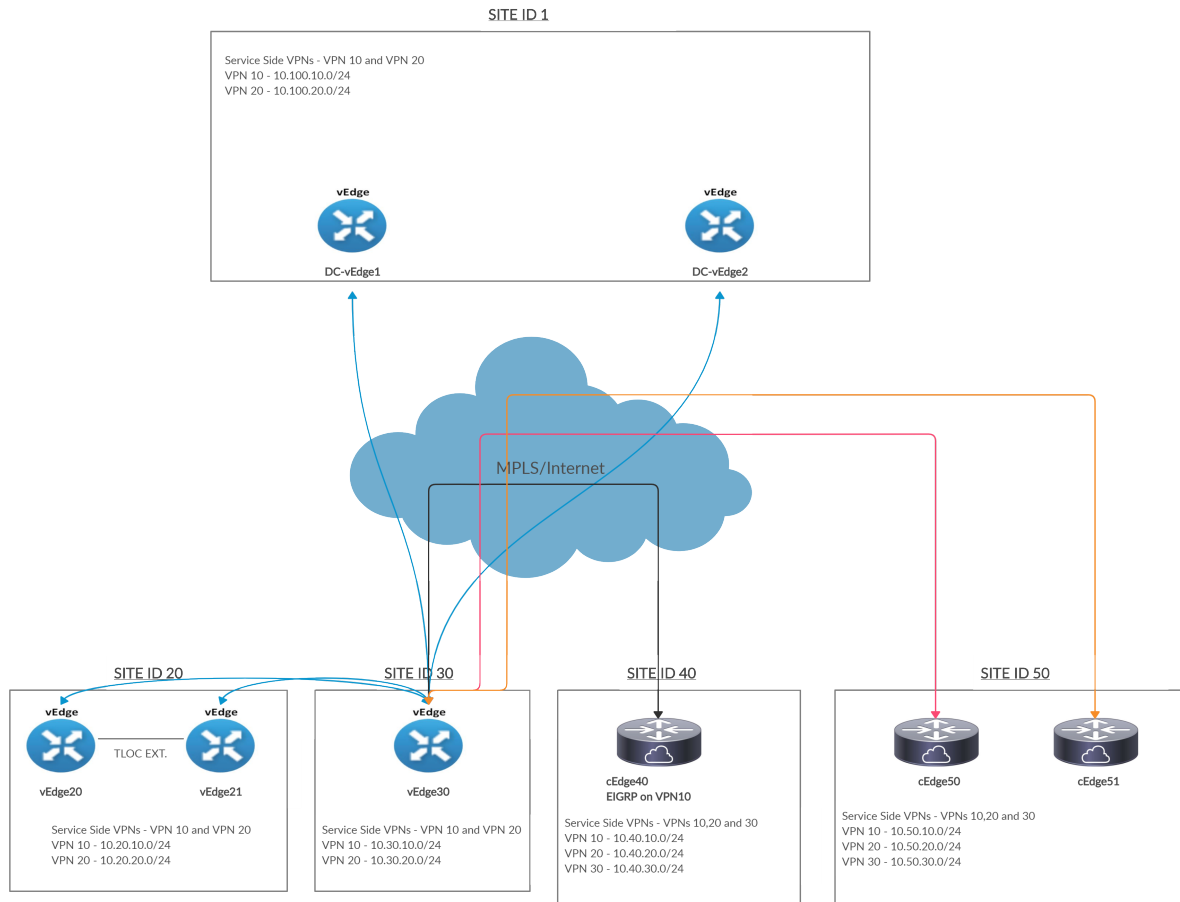
- [Pre-Configuration](#)
- [Adding the Policy](#)
 - [Setting up Site Lists](#)
 - [Adding Custom Control Policies](#)
 - [Policy for Traffic from Site 20 to the Regional Hub](#)
 - [Policy for Traffic from the Fabric to Site 20](#)
 - [Saving and Activating the Policy](#)
- [Verification](#)

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

CONFIGURATION | POLICIES Custom Options ▾

Centralized Policy Localized Policy

[Add Policy](#) ↻ ☰

Search Options ▾ Total Rows: 1

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	⋮

- View
- Preview
- Copy
- Edit
- Delete
- Deactivate

2. Confirm the Deactivation

Deactivate Policy
✕

Policy will be removed from the following vSmart.
10.255.255.3, 10.255.255.4

Would you like to remove policy from reachable vSmarts?

Deactivate
Cancel

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

vEdge20 | 10.255.255.21 Site ID: 20 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
--	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

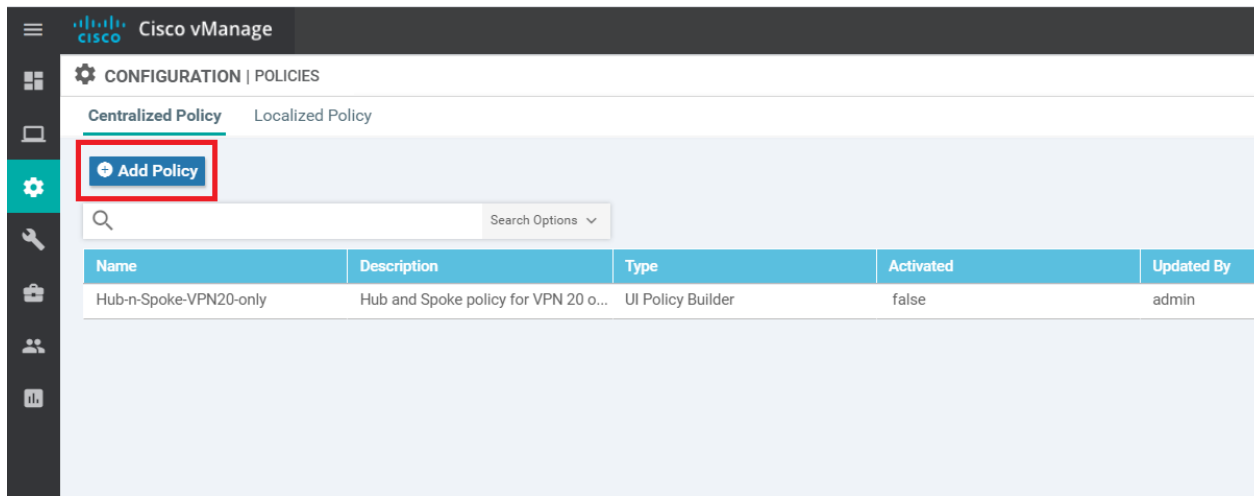
Task List

- ~~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

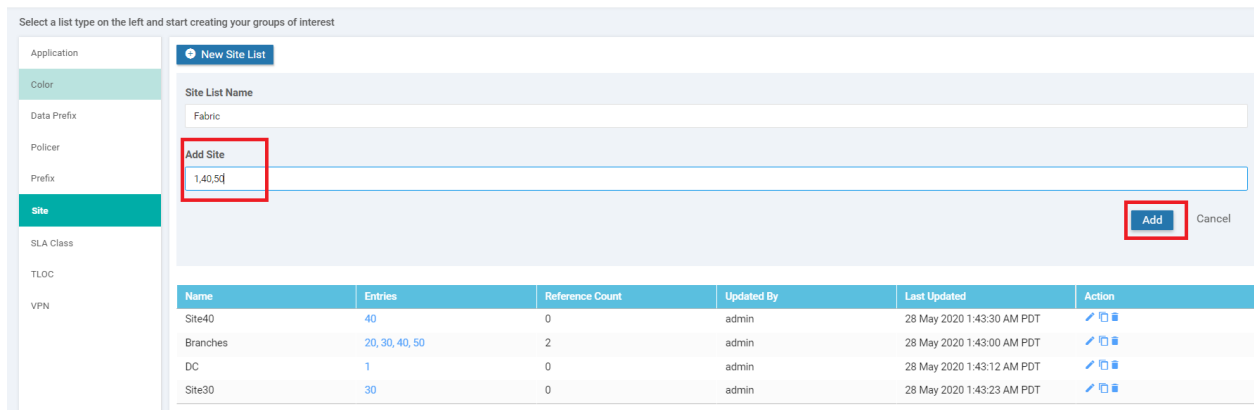
Adding the Policy

Setting up Site Lists

1. Go to **Configuration => Policies** and click on **Add Policy**



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**



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

1 Create Groups of Interest
2 Configure Topology and VPN Membership
3 Configure Traffic Rules
4 Apply Policies to Sites and VPNs

Select a list type on the left and start creating your groups of interest

- Application
- Color
- Data Prefix
- Policer
- Prefix
- Site
- SLA Class
- TLOC
- VPN

+ New Site List

Site List Name

Add Site

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	✎ 🗑
Fabric	1, 40, 50	0	admin	28 May 2020 5:38:49 AM PDT	✎ 🗑

CANCEL

Task List

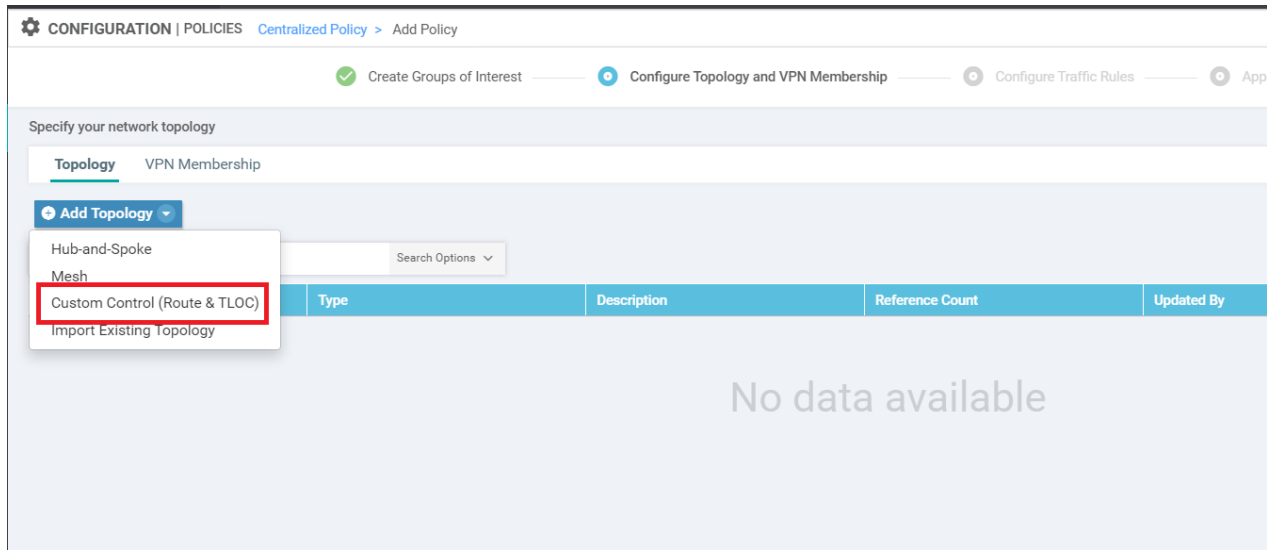
- ~~Pre-Configuration~~
- Adding the Policy
 - ~~Setting up Site Lists~~
 - Adding Custom Control policies
 - Policy for Traffic from Site 20 to the Regional Hub
 - Policy for Traffic from the Fabric to Site 20
 - Saving and Activating the Policy
- Verification

Adding Custom Control Policies

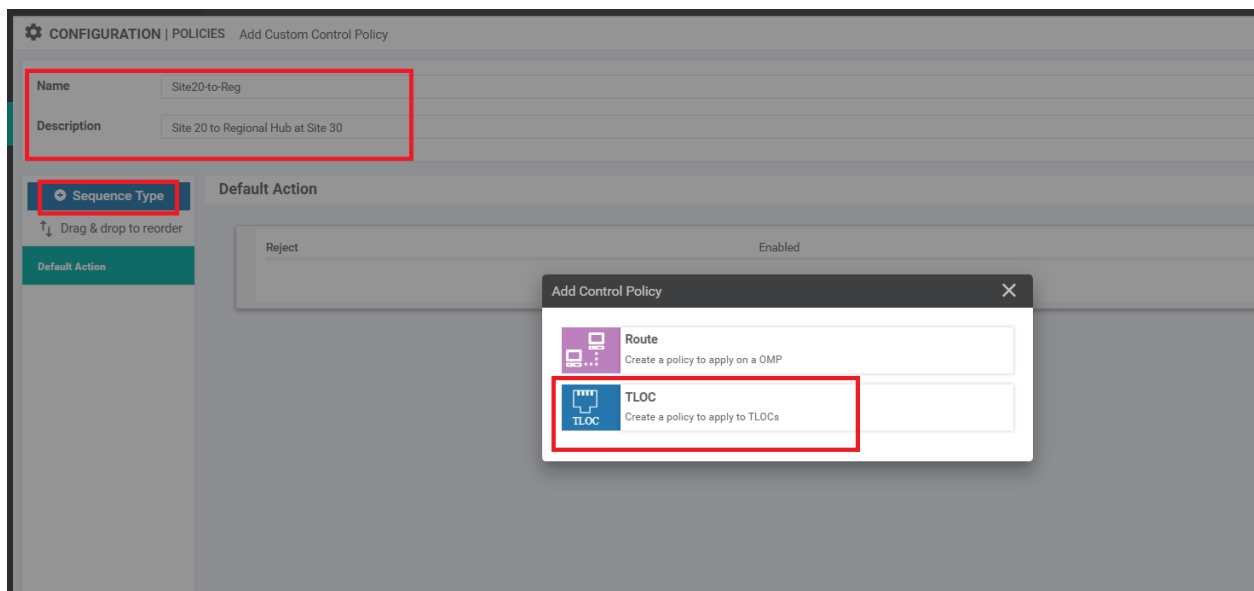
We will be adding two policies in this section - one for traffic destined to the rest of the network from Site 20 and one for traffic destined to Site 20.

Policy for Traffic from Site 20 to the Regional Hub

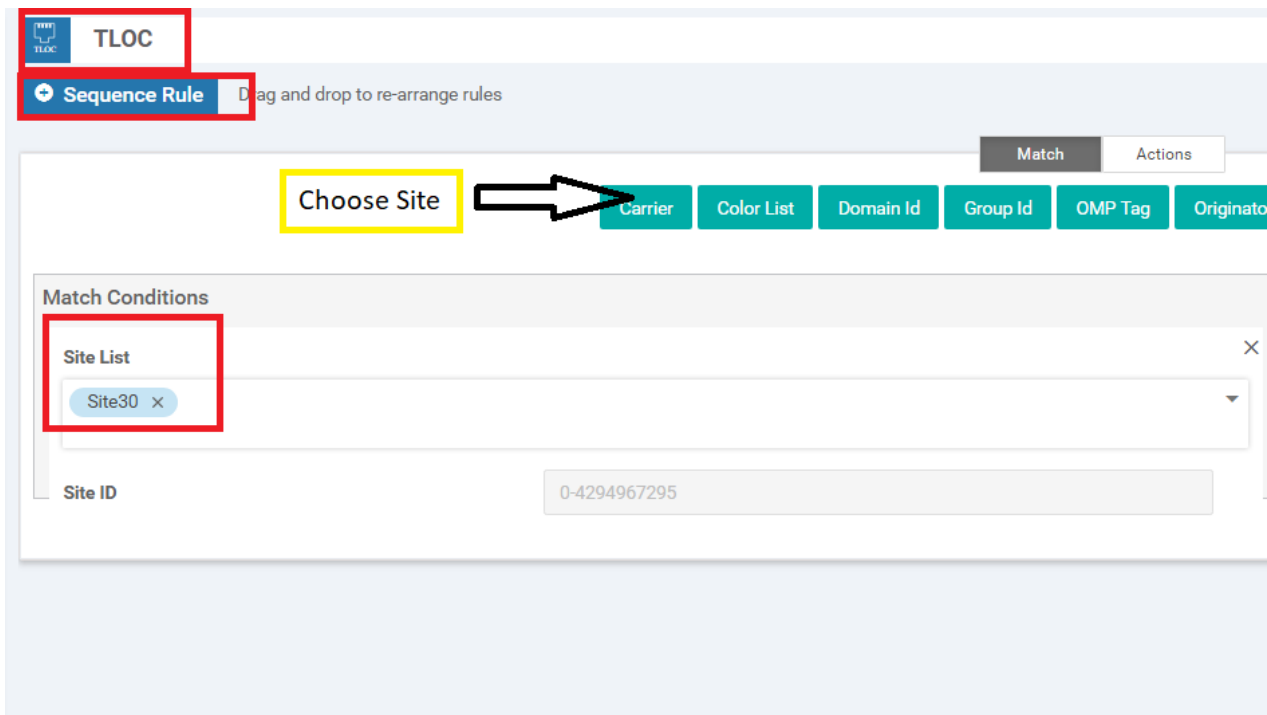
1. Continuing from the previous section, click on **Add Topology** and choose to add a **Custom Control (Route and TLOC)** topology



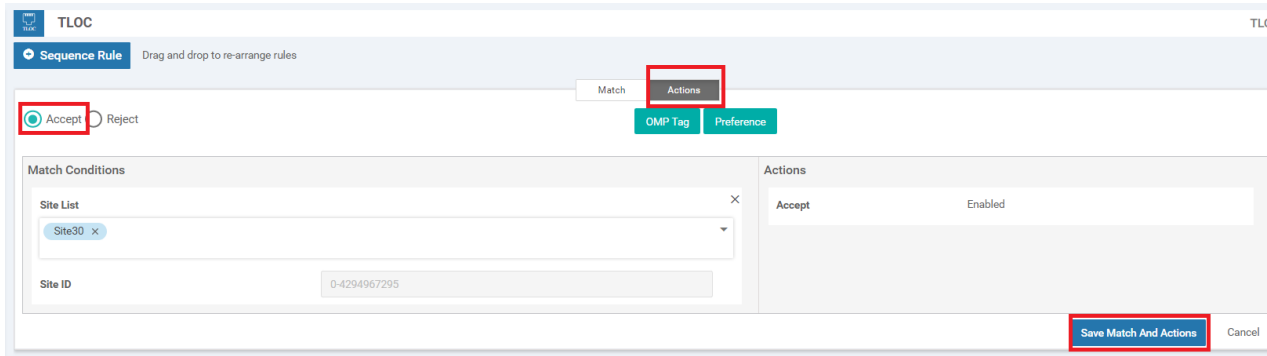
2. Give this Control Policy a Name of *Site20-to-Reg* and a Description of *Site 20 to Regional Hub at Site 30*. Click on **Sequence Type** and choose **TLOC**



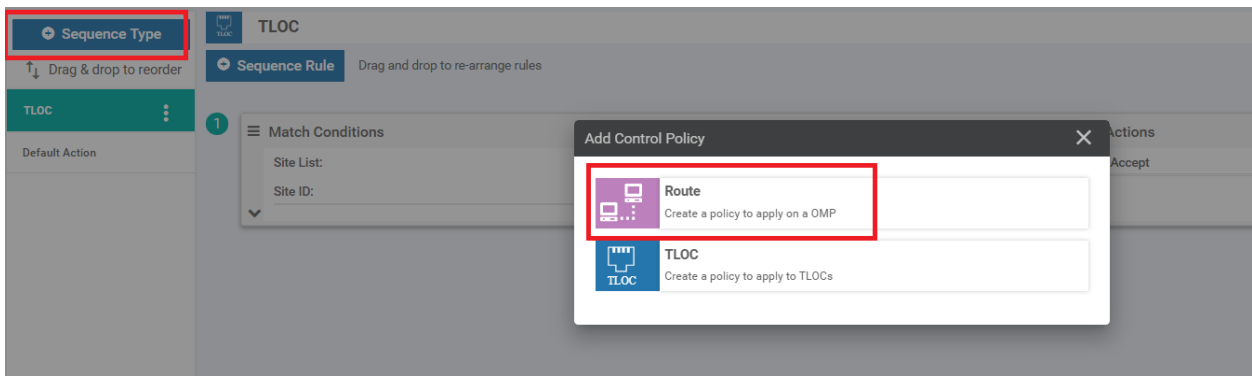
3. Choose to add a **Sequence Rule** and click on **Site** under **Match**. Populate the Site List as *Site30*



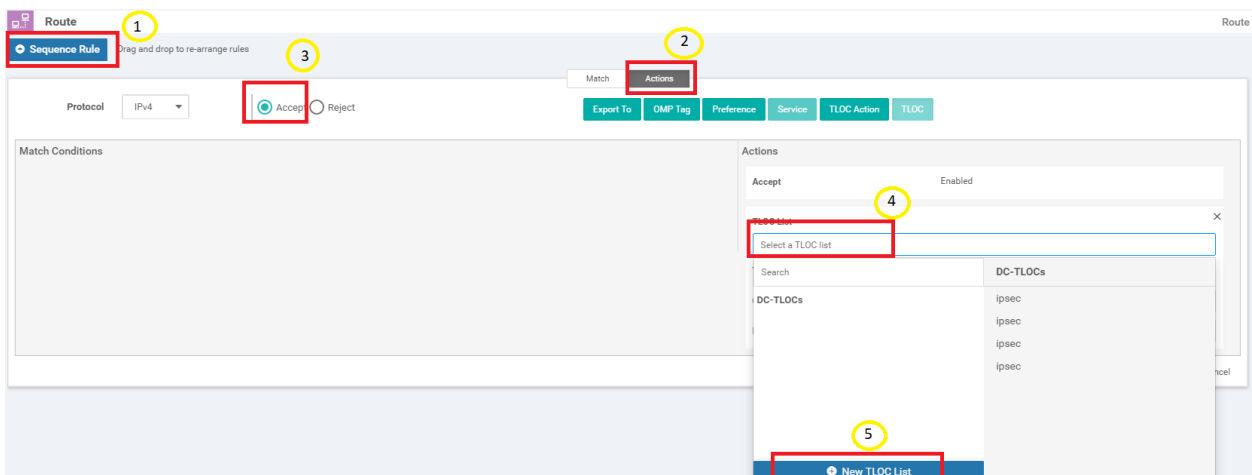
4. Go to the **Actions** tab and choose **Accept**. Click on **Save Match and Actions**



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 ✕

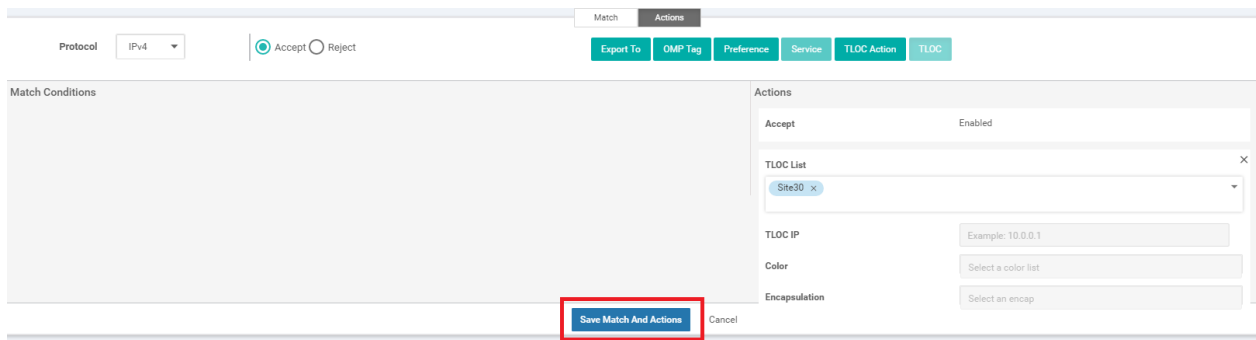
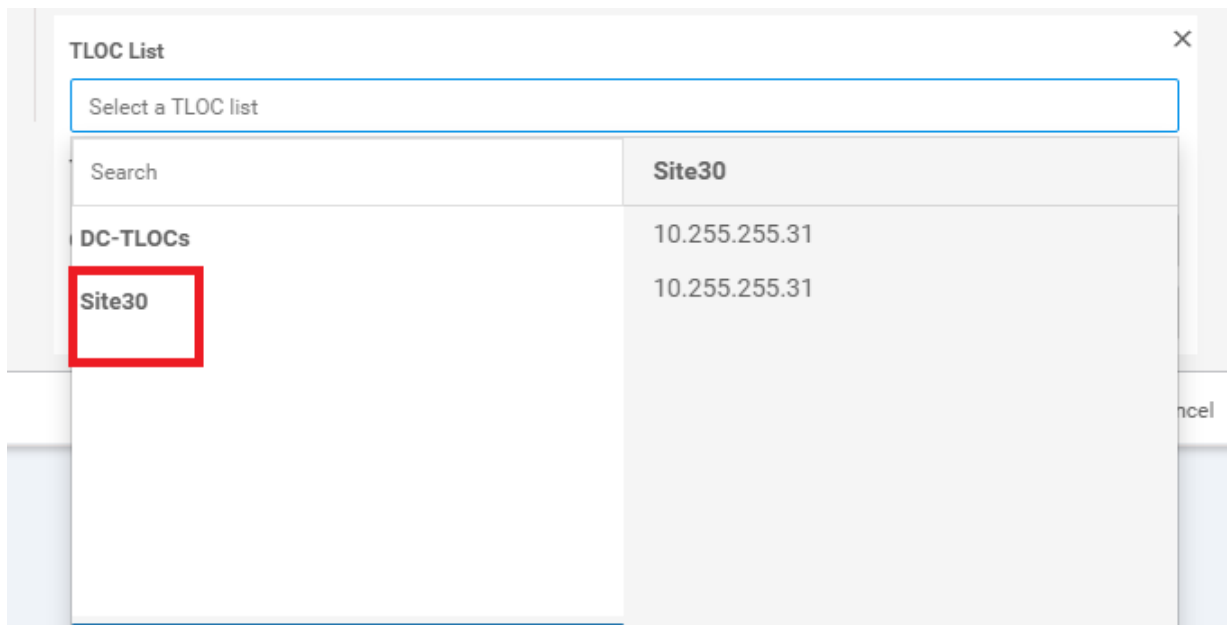
List Name
Site30

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**



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

Name: Site20-to-Reg
 Description: Site 20 to Regional Hub at Site 30

Sequence Type: Route

Sequence Rule: Match Conditions

Actions: Accept, TLOC List: Site30

Save Control Policy Cancel

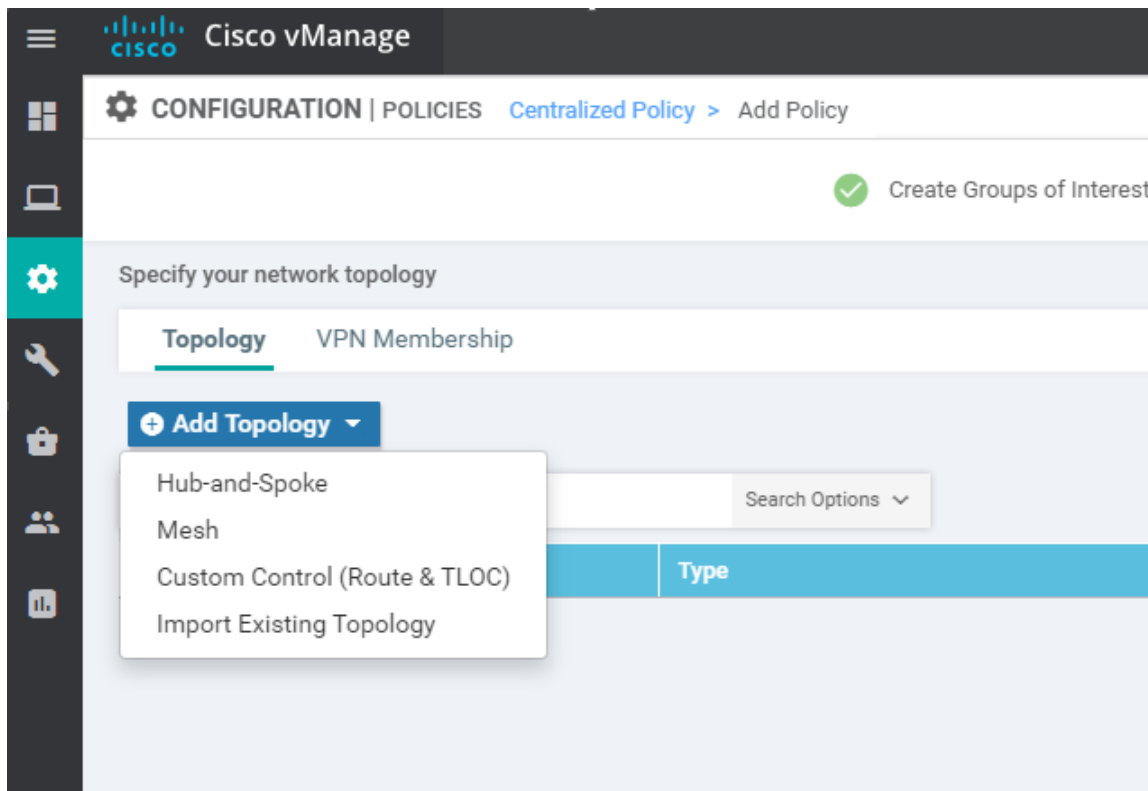
Continue with the next section for configuring another Control Policy.

Task List

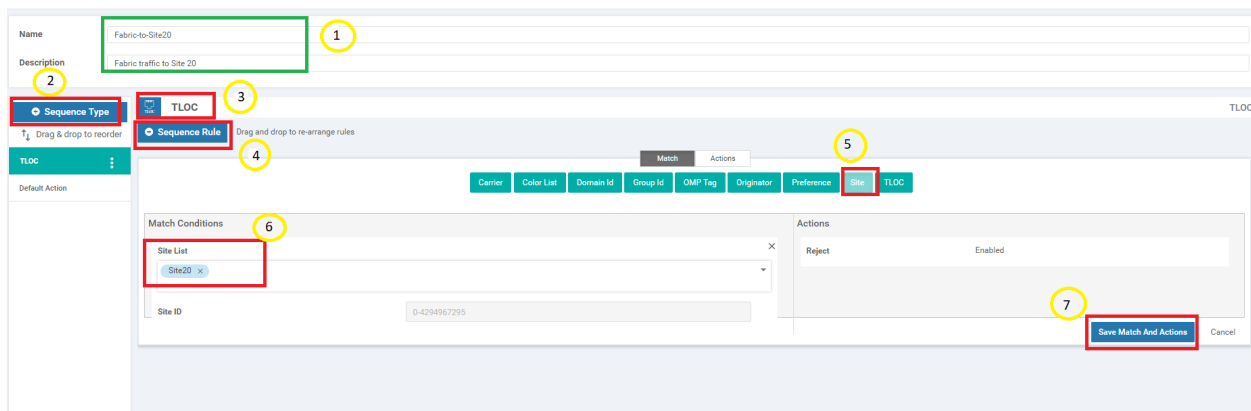
- ~~Pre-Configuration~~
- Adding the Policy
 - ~~Setting up Site Lists~~
 - Adding Custom Control policies
 - ~~Policy for Traffic from Site 20 to the Regional Hub~~
 - Policy for Traffic from the Fabric to Site 20
 - Saving and Activating the Policy
- Verification

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**

The screenshot shows the 'Route' configuration page. The 'Match Conditions' section is highlighted with a red box and contains a 'Site List' dropdown menu with 'Site20' selected and a 'Site ID' field with the value '0-4294967295'. The 'Actions' section is also highlighted with a red box and contains an 'Accept' checkbox that is checked and labeled 'Enabled', a 'TLOC List' dropdown menu with 'Site30' selected, and fields for 'TLOC IP', 'Color', and 'Encapsulation'. A 'Save Match And Actions' button is visible at the bottom right of the 'Actions' section.

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**

The screenshot shows the 'Default Action' configuration page. The 'Default Action' section is highlighted with a red box and contains an 'Accept' checkbox that is checked and labeled 'Enabled'. The 'Actions' section is also highlighted with a red box and contains an 'Accept' button and a 'Reject' button. A 'Save Match And Actions' button is visible at the bottom right of the 'Default Action' section.

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**

Add policies to sites and VPNs

Policy Name: Site20-Regional-Hub-Site30

Policy Description: Regional Policy for Site 20 to Site 30

Topology: Application-Aware Routing, Traffic Data, Cflowd

New Site List

Inbound Site List

Select one or more site lists

Outbound Site List

Fabric

Add Cancel

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**

Site20-to-Reg CUSTOM CONTROL

New Site List

Inbound Site List

Select one or more site lists

Outbound Site List

Site20

Add Cancel

Direction	Site List	Action
-----------	-----------	--------

BACK Preview Save Policy CANCEL

Activate Windows
Go to Settings to activate Windows.

3. Click on the three dots next to the *Site20-Regional-Hub-Site30* policy and choose to **Activate** it

CONFIGURATION | POLICIES Custom Options

Centralized Policy Localized Policy

[Add Policy](#) 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	...
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	

View
Preview
Copy
Edit
Delete
Activate

4. Confirm the Activation

Activate Policy ✕

Policy will be applied to the reachable vSmarts:
10.255.255.3, 10.255.255.4

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**

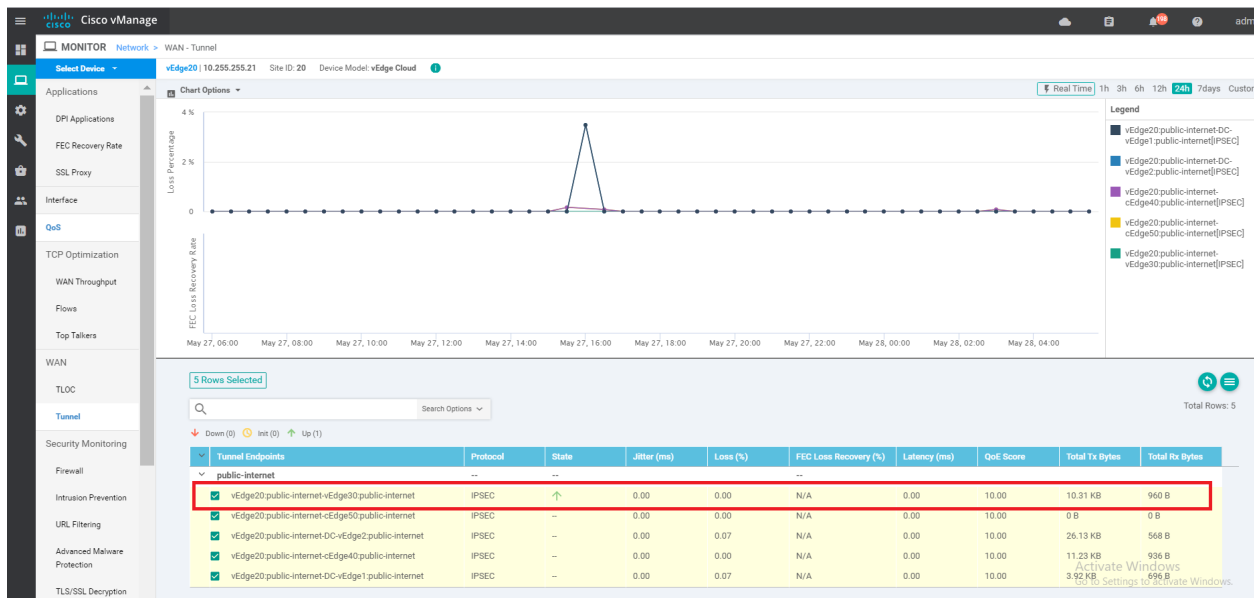
The screenshot shows the vManage GUI's Troubleshooting > Traceroute page. The configuration fields are: Destination IP: 10.100.10.1, VPN: VPN - 10, and Source/Interface for VPN - 10: ge0/2 - ipv4 - 10.20.10.2. The Start button is visible. The Output section contains the following text:

```
Traceroute -m 15 -w 1 -s 10.20.10.2 10.100.10.1 in VPN 10
traceroute to 10.100.10.1 (10.100.10.1), 15 hops max, 60 byte packets
 1 10.30.10.2 (10.30.10.2) 0.277 ms 0.344 ms 0.350 ms
 2 10.100.10.3 (10.100.10.3) 0.442 ms 0.534 ms 0.538 ms
 3 10.100.10.1 (10.100.10.1) 1.228 ms * *
```

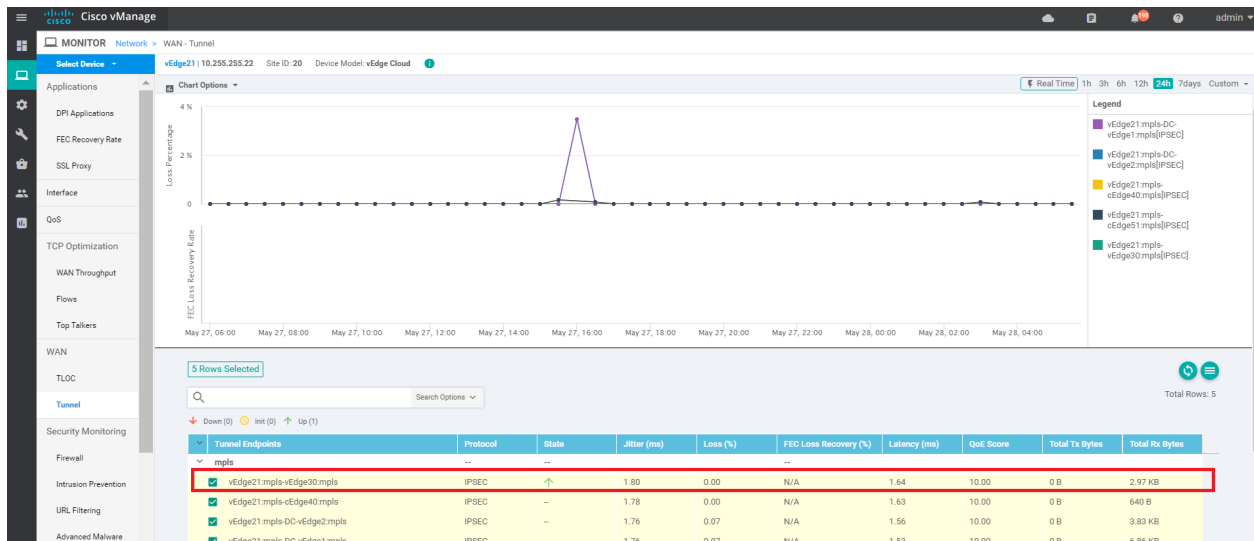
The diagram shows the path of the traceroute. It starts at the source interface **ge0/2 - ipv4 - 10.20.10.2**. The first hop is to **10.30.10.2** with a delay of **0.32ms**. The second hop is to **10.100.10.3** with a delay of **0.50ms**. The final hop is to the destination **10.100.10.1** with a delay of **1.23ms**.

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.

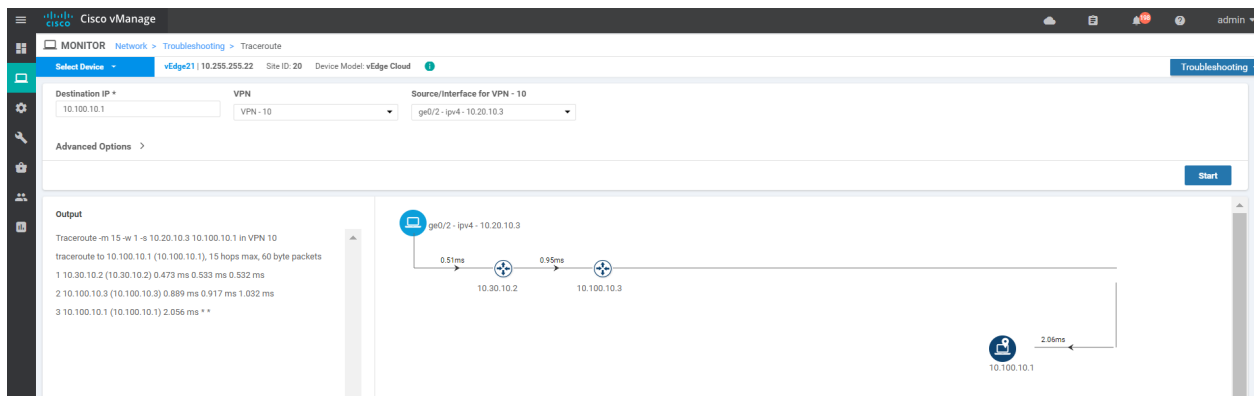
2. Click on **Tunnel** on the left-hand side and notice that vEdge20 has a single Up tunnel with vEdge30 on public-internet and one on mpls. Other tunnels are not up (as expected)



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

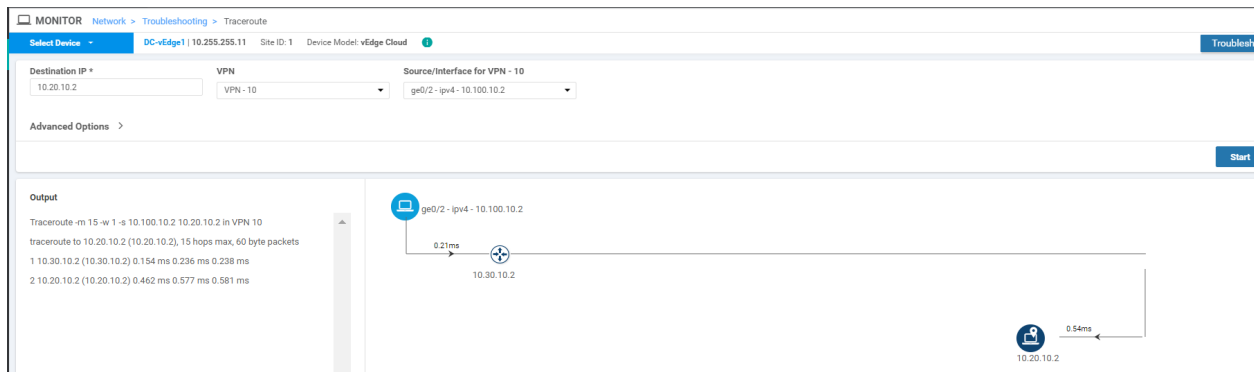


4. Go to **Troubleshooting => Trace Route** and enter the same details as before (i.e. a Destination of **10.100.10.1**, VPN of **VPN - 10** and a Source/Interface of **ge0/2**). Click on **Start**



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

- 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 displays the Cisco vManage interface. The top navigation bar shows 'Cisco vManage'. Below it, the breadcrumb path is 'DASHBOARD | MAIN DASHBOARD'. The left sidebar is open to the 'Network' menu, which is highlighted in teal. The main content area shows a summary for 'WAN Edge - 8' with a blue circular icon containing a white cross. Below this, there are four horizontal bars representing different categories: 'Network' (10), 'Alarms' (0), 'Events' (0), and 'Audit Log' (0). To the right of these bars, there is a 'Site Health' section with three status indicators: a green checkmark, a yellow warning icon, and a red error icon. Below the bars, there is a table with the following data:

Total	20
Authorized	20
Deployed	8
Staging	0

At the bottom, there is a 'Top Applications' section with a filter icon and a refresh icon. The text 'No data to display' is shown below this section.

2. Click on **vEdge30** and scroll down the list on the left-hand side to **Troubleshooting**

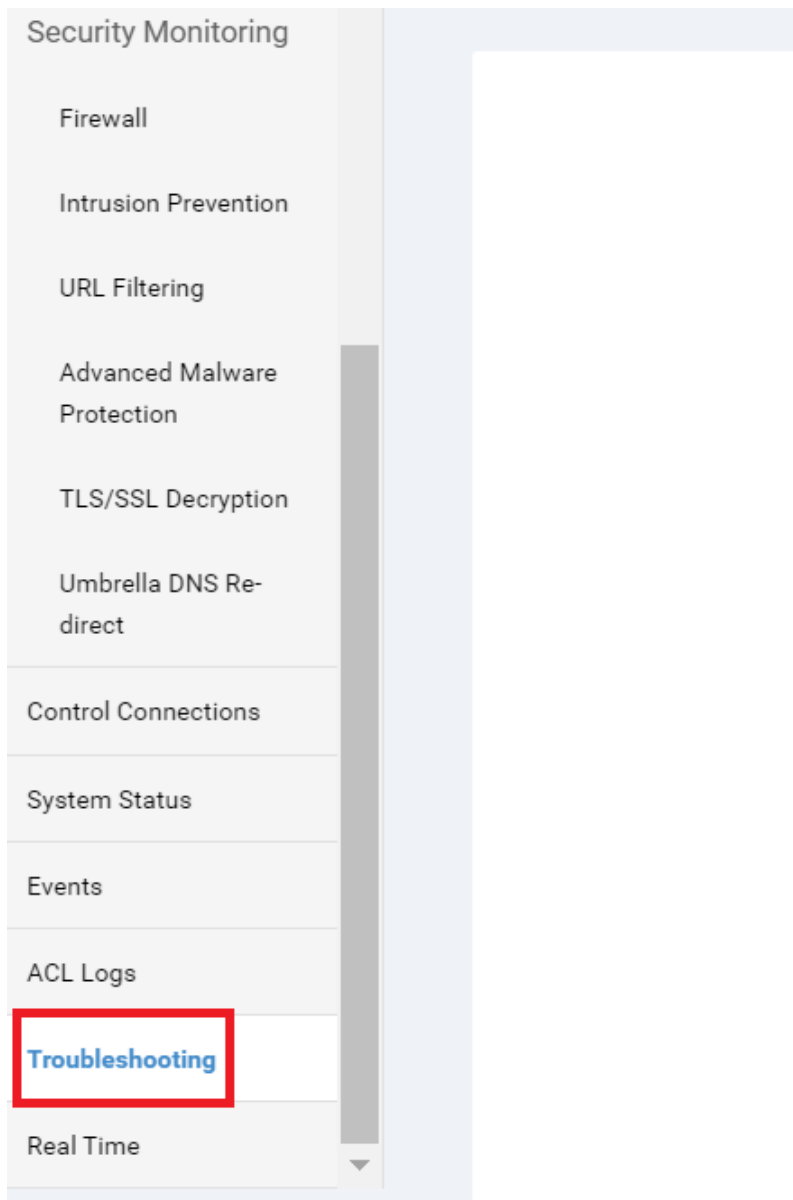
Device Group

All

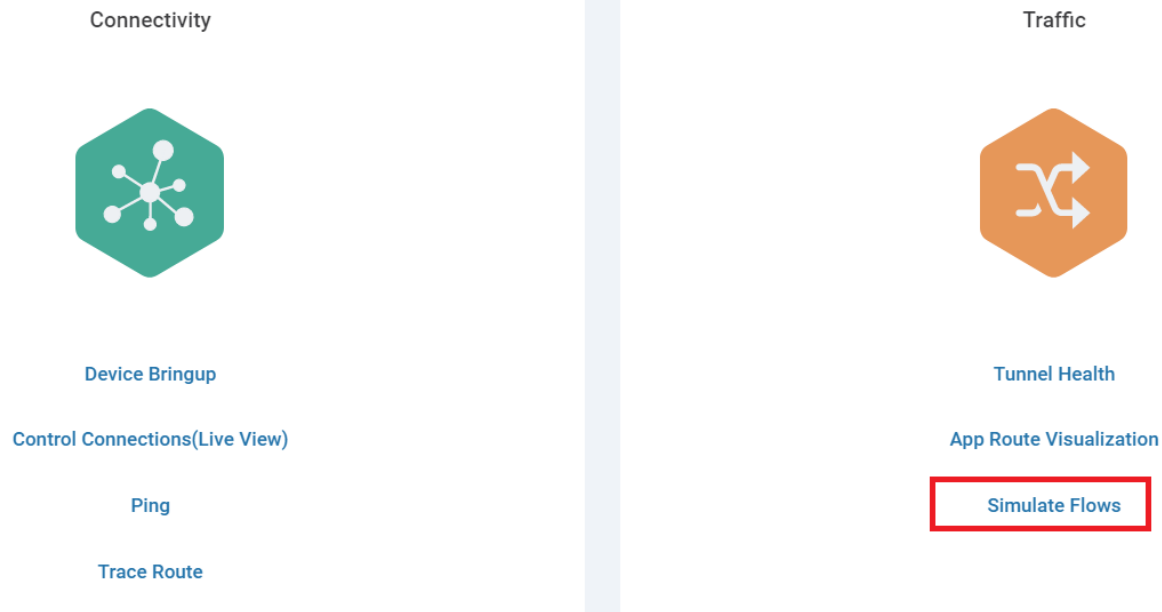


Search Options

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



3. Click on **Simulate Flows**



4. Enter *VPN - 10* as the VPN, *ge0/2 - ipv4 - 10.30.10.2* 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

Advanced Options >

Simulate

Output: Total next hops: 4 | IPSec : 4

→ vpn	Remote System IP	10.255.255.12
← vpn	Encapsulation	IPSec
→ public-internet	Remote System IP	10.255.255.12
← public-internet	Encapsulation	IPSec
→ vpn	Remote System IP	10.255.255.11
← vpn	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**

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 ftp

Advanced Options >

Simulate

Output: Total next hops: 4 | IPsec: 4

Transport	Remote System IP	Encapsulation	IPsec
mpls	10.255.255.12	IPsec	IPsec
public-internet	10.255.255.12	IPsec	IPsec
mpls	10.255.255.11	IPsec	IPsec
public-internet	10.255.255.11	IPsec	IPsec

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

VPN	Source/Interface for VPN - 10*	Source IP*
	ge0/2 - ipv4 - 10.30.10.2	10.30.10.2

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

```
graph LR; Laptop[Laptop] --> Router((vEdge 10.255.2)); Router --> Out1[ ]; Router --> Out2[ ]; Router --> Out3[ ]; Router --> Out4[ ];
```

2. Under Centralized Policy, click on **Add Policy** to create a new Policy

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

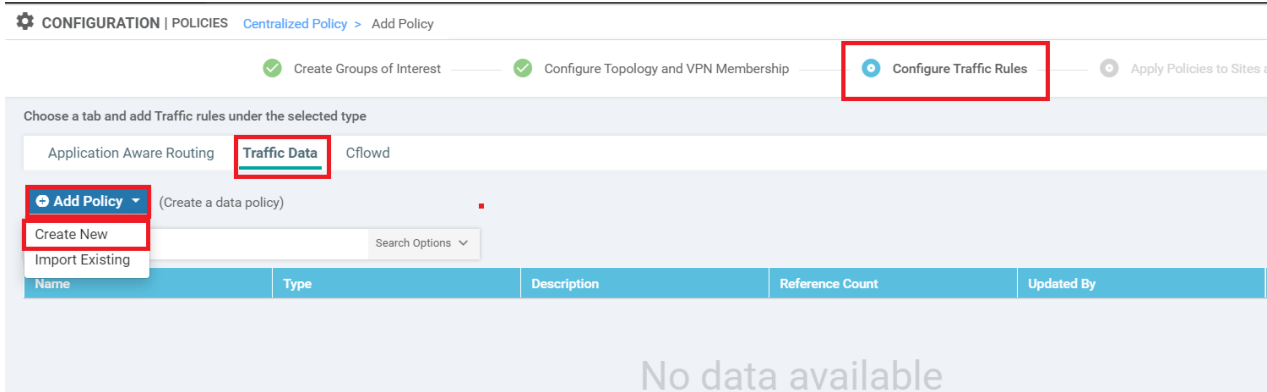
+ New Site List

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

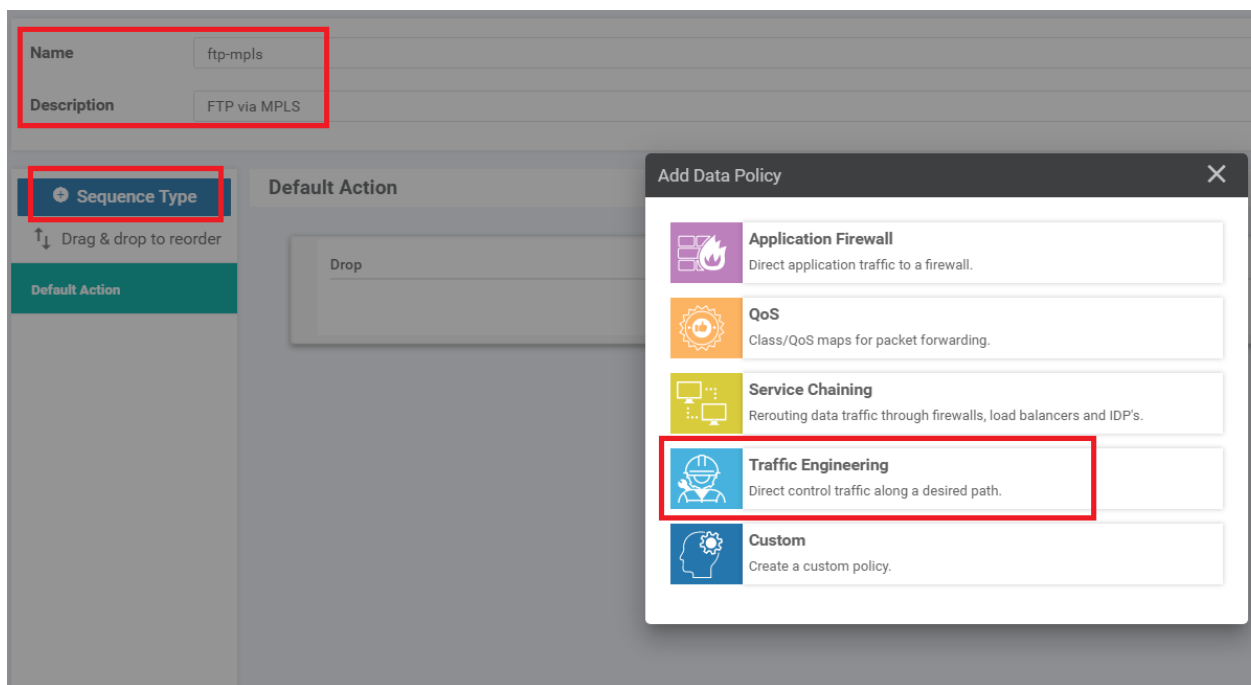
Next

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**



- 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



- 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**

The screenshot shows the 'Traffic Engineering' configuration page. At the top, there is a 'Sequence Rule' button and a 'Drag and drop to re-arrange rules' instruction. Below this, there are tabs for 'Match' and 'Actions'. The 'Match' tab is active, and the 'Application/Application Family List' field is selected. A dropdown menu is open, showing 'Google_Apps' and 'Microsoft_Apps'. A 'New Application List' button is visible at the bottom.

7. Give the Application List Name as *ftp* and select **File Transfer Protocol** and **File Transfer Protocol Data** under the **Select Application** drop down

Application List ✕

Application List Name
ftp

Application Application Family

Select Application

File Transfer Protocol ✕ File Transfer Protocol Data ✕

file transfer protocol

File Transfer Protocol

File Transfer Protocol Data

File Transfer Protocol Secure

Trivial File Transfer Protocol

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

Application List

Application List Name

ftp

Application Application Family

Select Application

File Transfer Protocol x File Transfer Protocol Data x

Save Cancel

9. From the **Application/Application Family List** drop down, choose the *ftp* Application List we just created

Traffic Engineering

Sequence Rule Drag and drop to re-arrange rules

Application/Application Family List

Select an application list

Search

	ftp
Google_Apps	ftp
Microsoft_Apps	ftp-data
ftp	

Accept

+ New Application List

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**

Match Conditions

Application/Application Family List

ftp x

Actions

Accept Enabled

Local TLOC List: Color

mpls x

Local TLOC List: Encapsulation

IPSEC x

Restrict

Save Match And Actions Cancel

11. Choose **Default Action** on the left-hand side and click on the pencil icon to edit the default action

Sequence Type

Drag & drop to reorder

Traffic Engineering

Default Action

Default Action

Drop Enabled

12. Select **Accept** and click on **Save Match and Actions**

Actions

Accept Drop

Accept Enabled

Save Match And Actions Cancel

13. Back at the Data Policy window, click on **Save Data Policy**

Name: ftp-mpls

Description: FTP via MPLS

Traffic Engineering

Sequence Type: Traffic Engineering

Sequence Rule: Drag and drop to re-arrange rules

Match Conditions:

Application/Application Family List:	ftp
--------------------------------------	-----

Actions:

Accept
Local TLOC List: mpls

Save Data Policy CANCEL

14. At the main Policy window, click on **Next**

Choose a tab and add Traffic rules under the selected type

Application Aware Routing **Traffic Data** Cflowd

Add Policy (Create a data policy)

Search Options

Name	Type	Description	Reference Count	Updated By
ftp-mpls	Data	FTP via MPLS	0	admin

BACK **Next** CANCEL

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**

The screenshot shows the 'Add policies to sites and VPNs' configuration page. The form is filled with the following information:

- Policy Name:** traffic-engineering-ftp
- Policy Description:** Traffic Engineering for FTP
- Tabs:** Topology, Application-Aware Routing, **Traffic Data**, Cflowd
- Topology:** ftp-mpls
- Buttons:** **New Site List and VPN List** (highlighted)
- Radio Buttons:** From Service, From Tunnel, All
- Select Site List:** Site30 x
- Select VPN List:** Corporate x
- Buttons:** Add (highlighted), Save Policy (highlighted)

2. This should create our *traffic-engineering-ftp* policy. Click on the three dots next to it and choose **Activate**

Add Policy

Search Options

Total Rows: 3

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
Site20-Regional-Hub-Site30	Regional Policy for Site 20 to Sit...	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 2...	UI Policy Builder	false	admin	05282020T100134900	28 May 2020 3	...

- 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**

Activate Policy

Policy will be applied to the reachable vSmarts:

10.255.255.3, 10.255.255.4

Activate
Cancel

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 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

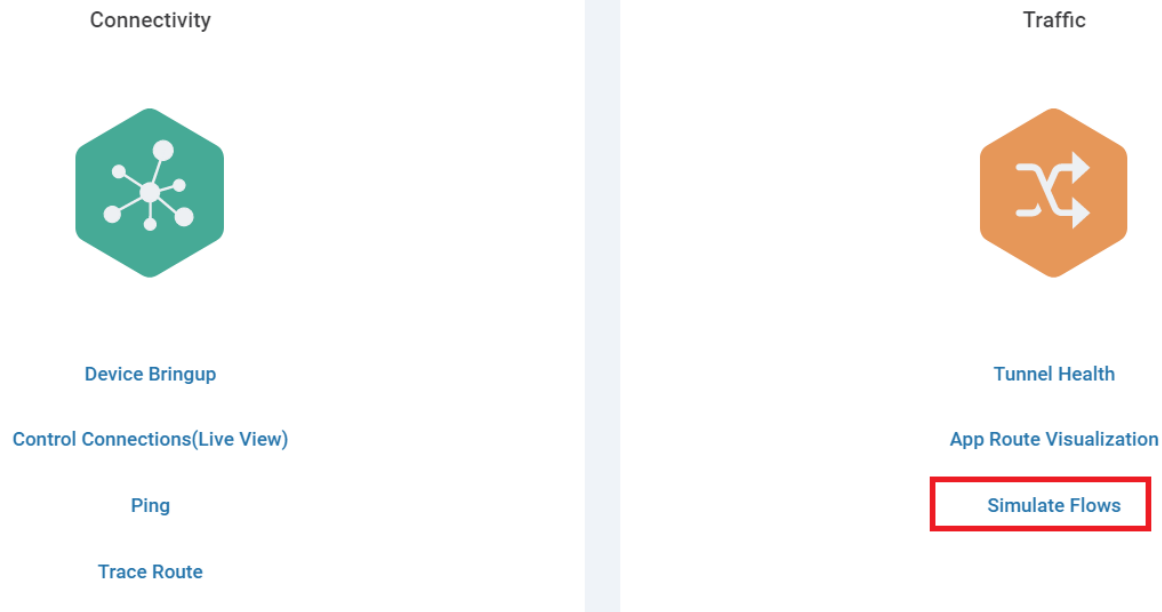
System Status

Events

ACL Logs

Troubleshooting

Real Time



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' configuration page. The input fields are:

- VPN*:** VPN - 10
- Source/Interface for VPN - 10*:** ge0/2 - ipv4 - 10.30.10.2
- Source IP*:** 10.30.10.2
- Destination IP*:** 10.0.0.1
- Application:** Choose

The **Simulate** button is highlighted with a red box. The output shows a flow starting from a source icon to a destination IP (10.255.255.31), which then branches into four paths:

- mpls / ← mpls: Remote System IP 10.255.255.12, Encapsulation, IPsec
- public-internet / ← public-internet: Remote System IP 10.255.255.12, Encapsulation, IPsec
- mpls / ← mpls: Remote System IP 10.255.255.11, Encapsulation, IPsec
- public-internet / ← public-internet: Remote System IP 10.255.255.11, Encapsulation, IPsec

Total next hops: 4 | IPsec : 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**

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 ftp

Advanced Options >

Simulate

Output: Total next hops: 2 | IPSec: 2

```
graph LR; S(( )) --> C((10.255.255.31)); C --> D1[Remote System IP 10.255.255.12  
IPSec Encapsulation]; C --> D2[Remote System IP 10.255.255.11  
IPSec Encapsulation];
```

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](#)

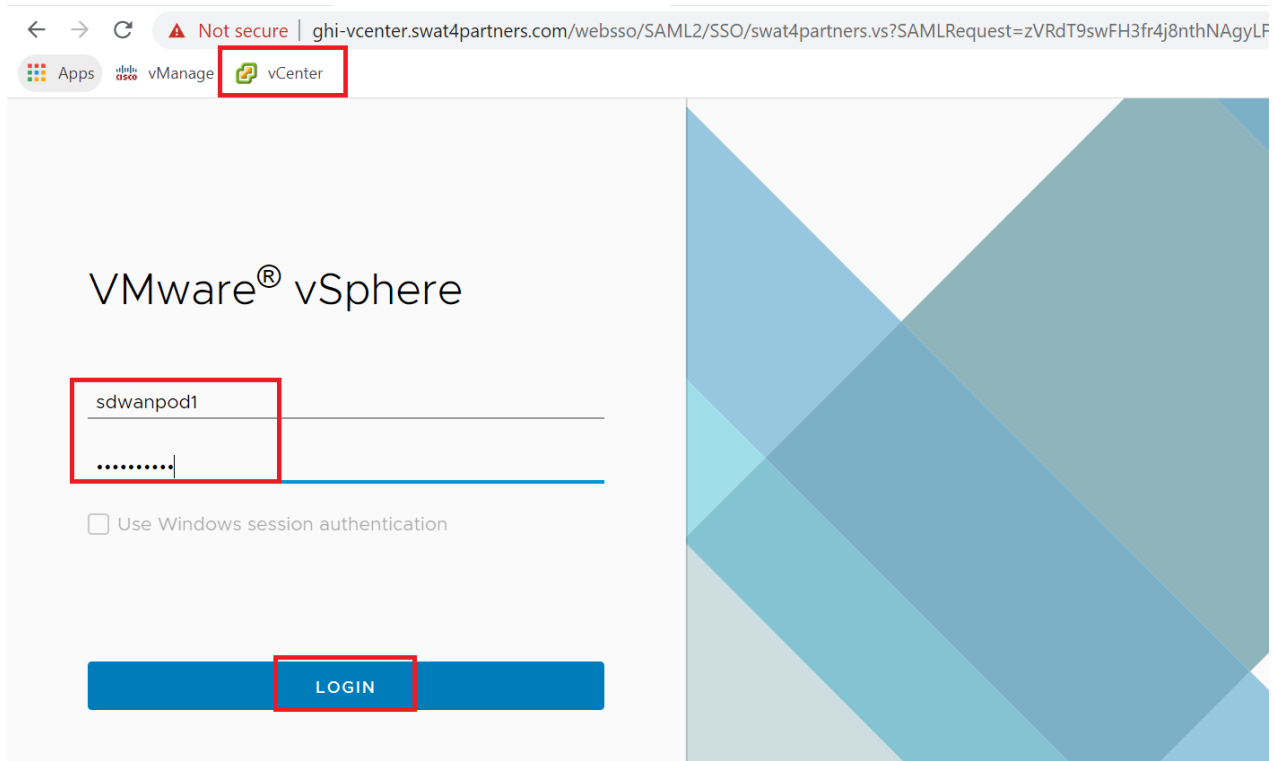
Task List

- Overview
- Creating and Activating a Policy
- Verification

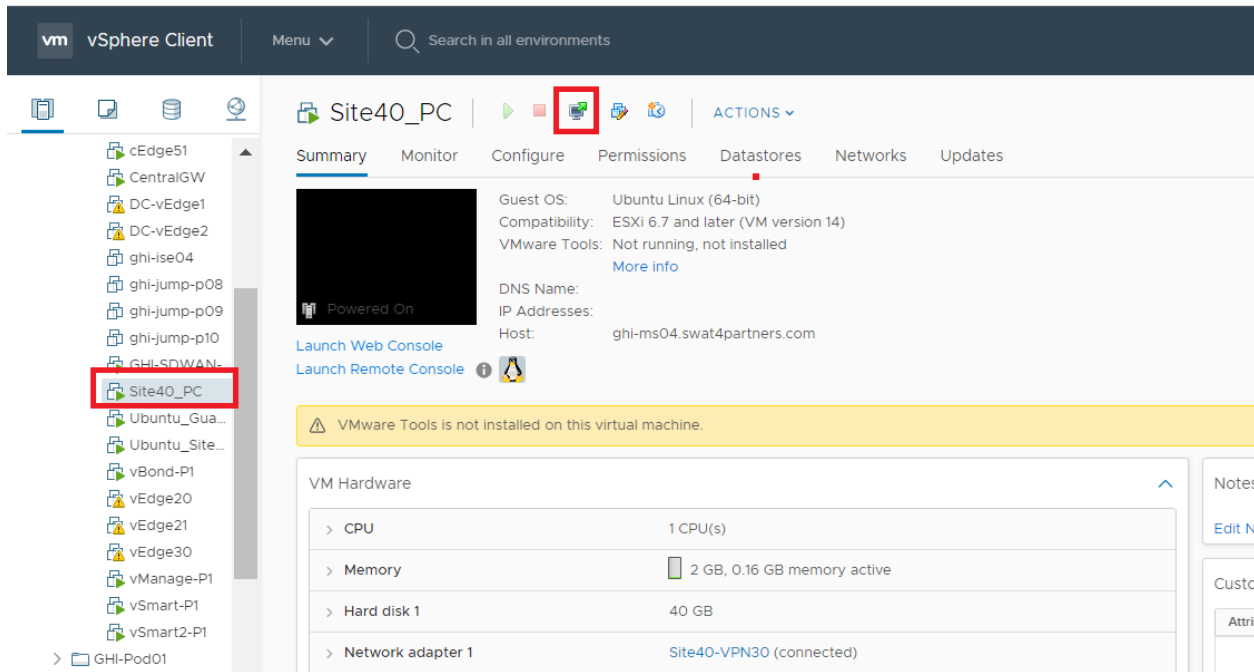
Overview

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**

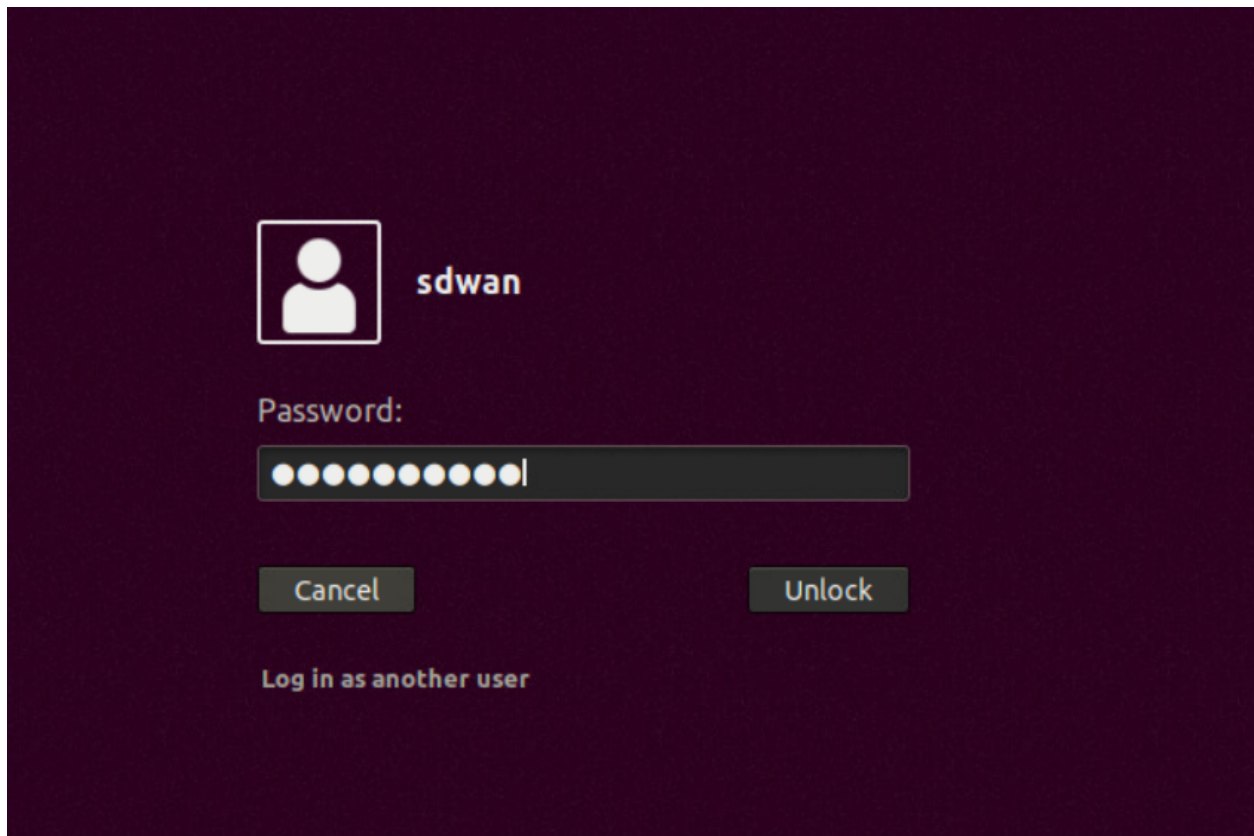


2. Locate the Site40 PC (it will be named *sdwan-YYY-site40pc-podX* where YYY are some characters and X is your POD number, image uses Site40_PC). Click on it and click on the icon to open a console session. Choose to open the Web Console, if prompted

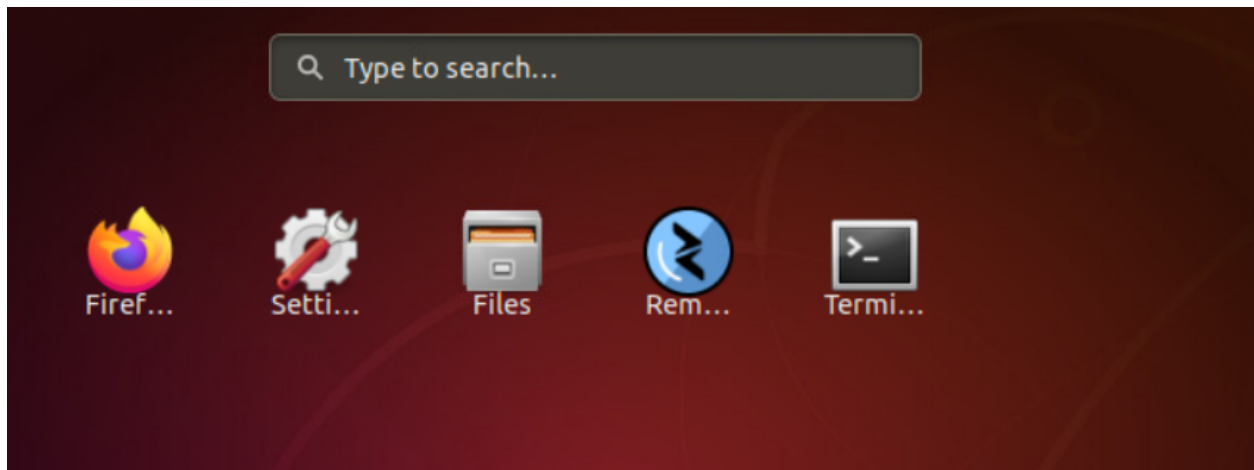


3. Navigate to the console window/tab and click on the *sdwan* user to log in. The password is *C1sco12345*

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

```
File Edit View Search Terminal Help
sdwan@10-40-30-21:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 10.40.30.2 icmp_seq=1 Destination Host Unreachable
From 10.40.30.2 icmp_seq=2 Destination Host Unreachable
From 10.40.30.2 icmp_seq=3 Destination Host Unreachable
From 10.40.30.2 icmp_seq=4 Destination Host Unreachable
From 10.40.30.2 icmp_seq=5 Destination Host Unreachable
From 10.40.30.2 icmp_seq=6 Destination Host Unreachable
```

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

Total Rows: 34

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	
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_int	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 11:32:28 PM
vSmart-vpn512-int	VPN512 Interface Template ...	vSmart Interface	vSmart	1	2	admin	25 May 2020 11:32:28 PM
DCvEdge-vpn0	VPN0 for the DC-vEdges IN...	WAN Edge VPN	vEdge Cloud	1	2	admin	23 May 2020 11:32:28 PM

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 Global On Off

NAT Type Global 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

Search Options ▾

S...	Chassis Number	System IP	Hostname	Interface Name(vpn30_if_name)	IPv4 Address/ prefix-length(vpn30_if_ipv4_address)
✓	CSR-04F9482E-44F0-E4DC-D30D-60C0806F...	10.255.255.41	cEdge40	GigabitEthernet6	10.40.30.2/24

Next
Cancel

☰
⚙️
🏠
🔑
📦
👤
📄

Cisco vManage

CONFIGURATION | TEMPLATES

Device Template: cEdge_dualuplink_devtemp Total: 1

Config Preview | Config Diff Inline

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

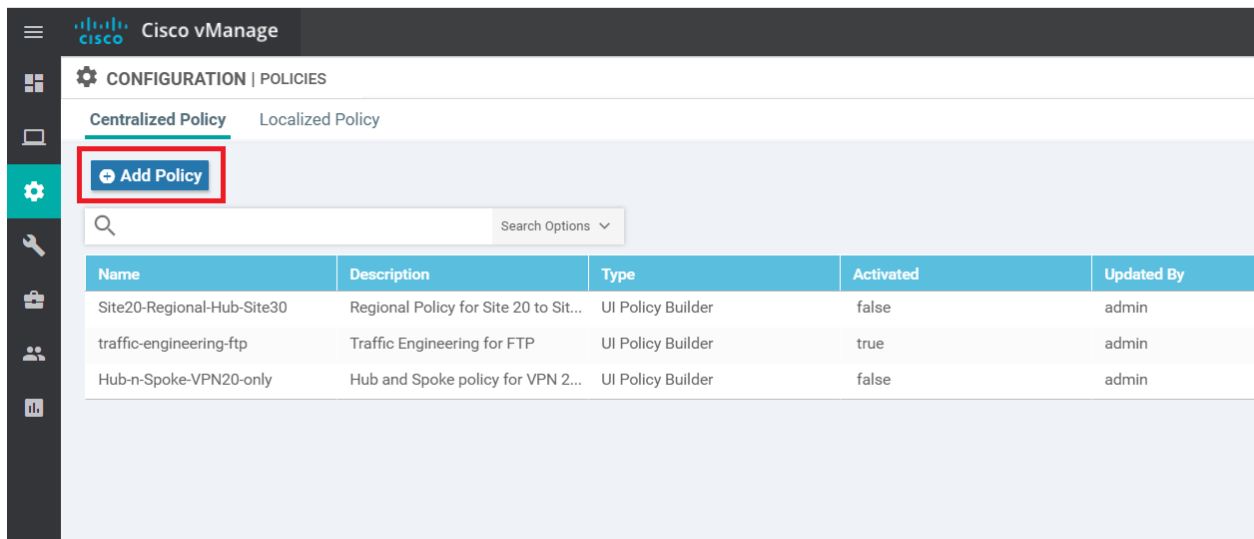
Local Configuration			New Configuration		
1	system		1	system	
2	host-name	cEdge40	2	host-name	cEdge40
3	system-ip	10.255.255.41	3	system-ip	10.255.255.41
4	overlay-id	1	4	overlay-id	1
5	site-id	40	5	site-id	40
6	port-offset	1	6	port-offset	1
7	control-session-pps	300	7	control-session-pps	300
8	admin-tech-on-failure		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	

Configure Devices
Back

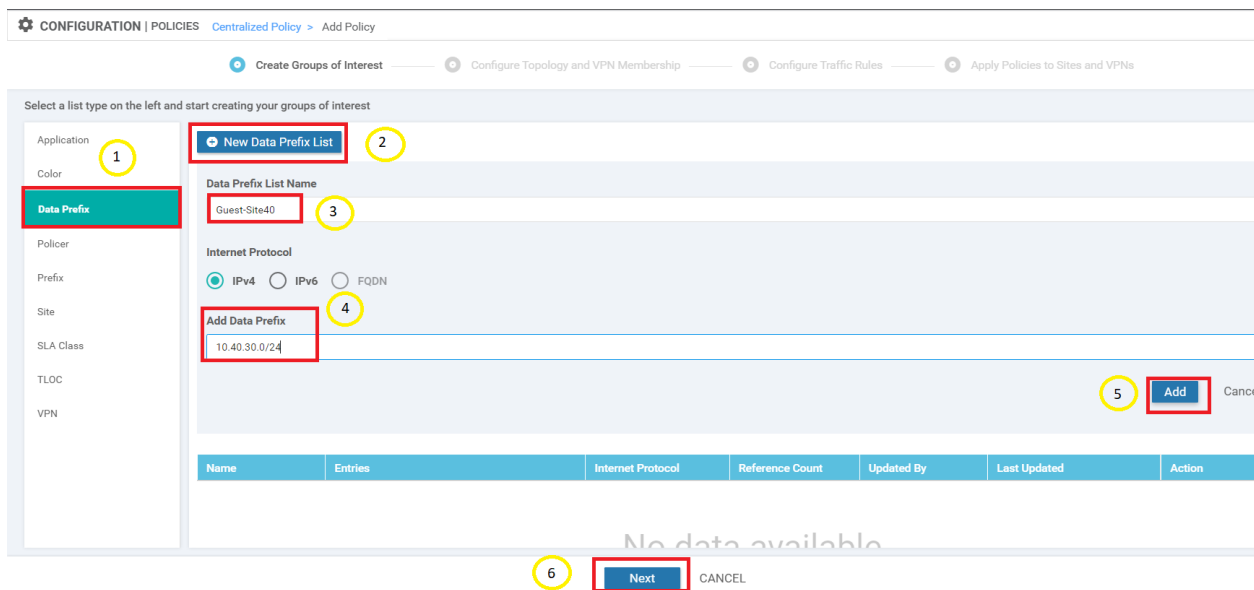
Configure Device Rollback Timer

NAT should now be enabled on the public-internet transport

4. Navigate to **Configuration => Policies** on the vManage GUI and click on **Add Policy**



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)



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 Search Options ▾

 Import Existing

Name	Type	Description	Reference Count	Updated By
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






Description

➕ Sequence Type

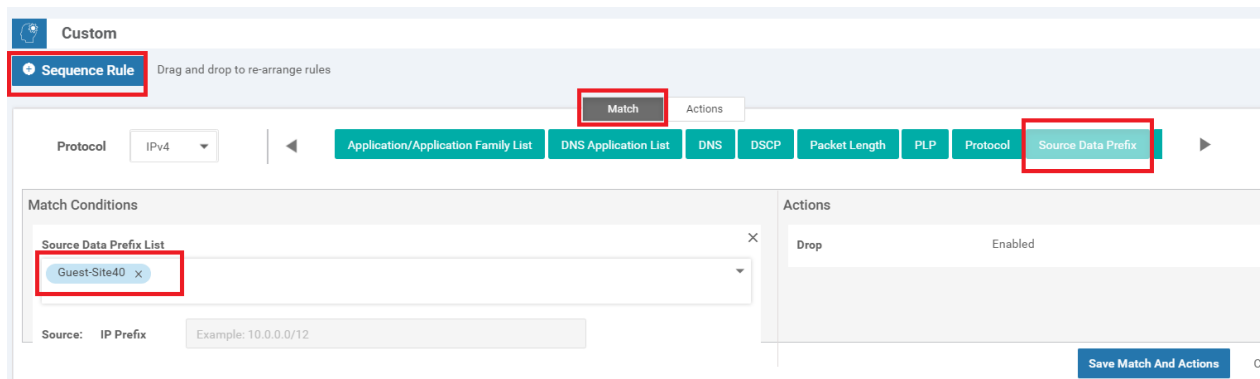
Default Action

Drop

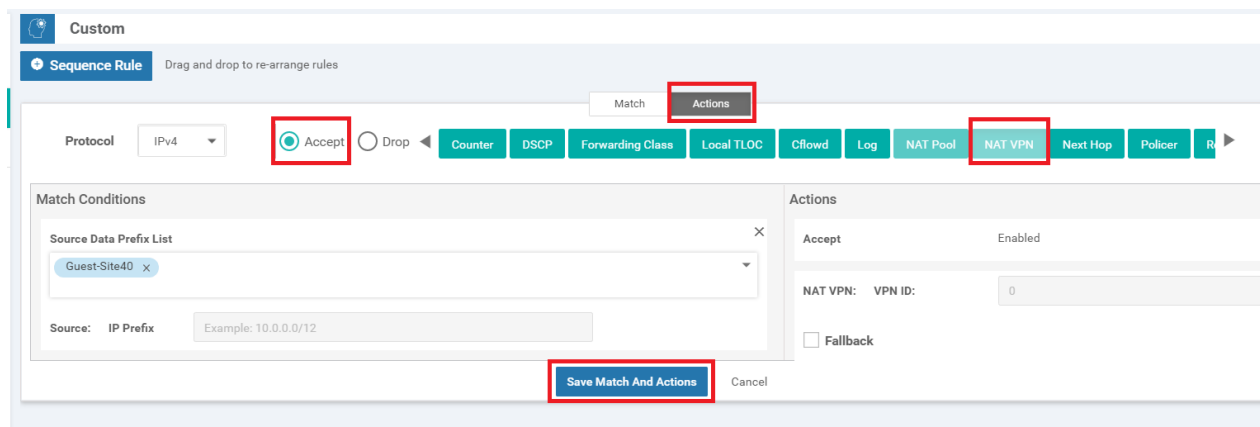
Add Data Policy ✕

-  **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.

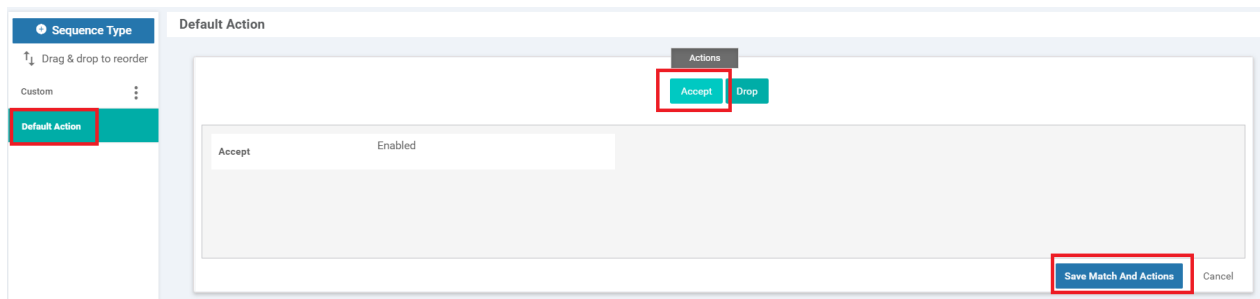
8. Click on **Sequence Rule** and select **Source Data Prefix** under Match. Populate *Guest-Site40* in the Source Data Prefix List (we just created this Data Prefix list)



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**

Sequence Type

↑↓ Drag & drop to reorder

Custom

Default Action

Default Action

Accept Enabled

Save Data Policy CANCEL

12. Make sure the Data Policy we just added shows up and click on **Next**

Application Aware Routing **Traffic Data** Cflowd

Add Policy (Create a data policy)

Search Search Options

Name	Type	Description	Reference Count	Updated By
Guest-DIA	Data	Guest DIA at Site 40	0	admin

BACK Next CANCEL

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**

Add policies to sites and VPNs

Policy Name: Site40-Guest-DIA (1)

Policy Description: DIA Policy for Site 40 Guests (1)

Topology: Application-Aware Routing | **Traffic Data** (2) | Cflowd

Guest-DIA

New Site List and VPN List (3)

From Service From Tunnel All

Select Site List: Site40 x (4)

Select VPN List: Guest x (5)

Add (6) Cancel

BACK Preview **Save Policy** (7) CANCEL

14. Locate your *Site40-Guest-DIA* and click on the three dots next to it. Choose to Activate the policy

Site40-Guest-DIA	DIA Policy for Site 40 Guests	UI Policy Builder	false	admin	06032020T142511667	03 Jun 2020 7:25:11 AM PDT	...
------------------	-------------------------------	-------------------	-------	-------	--------------------	----------------------------	-----

- View
- Preview
- Copy
- Edit
- Delete
- Activate**

This completes the configuration of our DIA Policy.

Task List

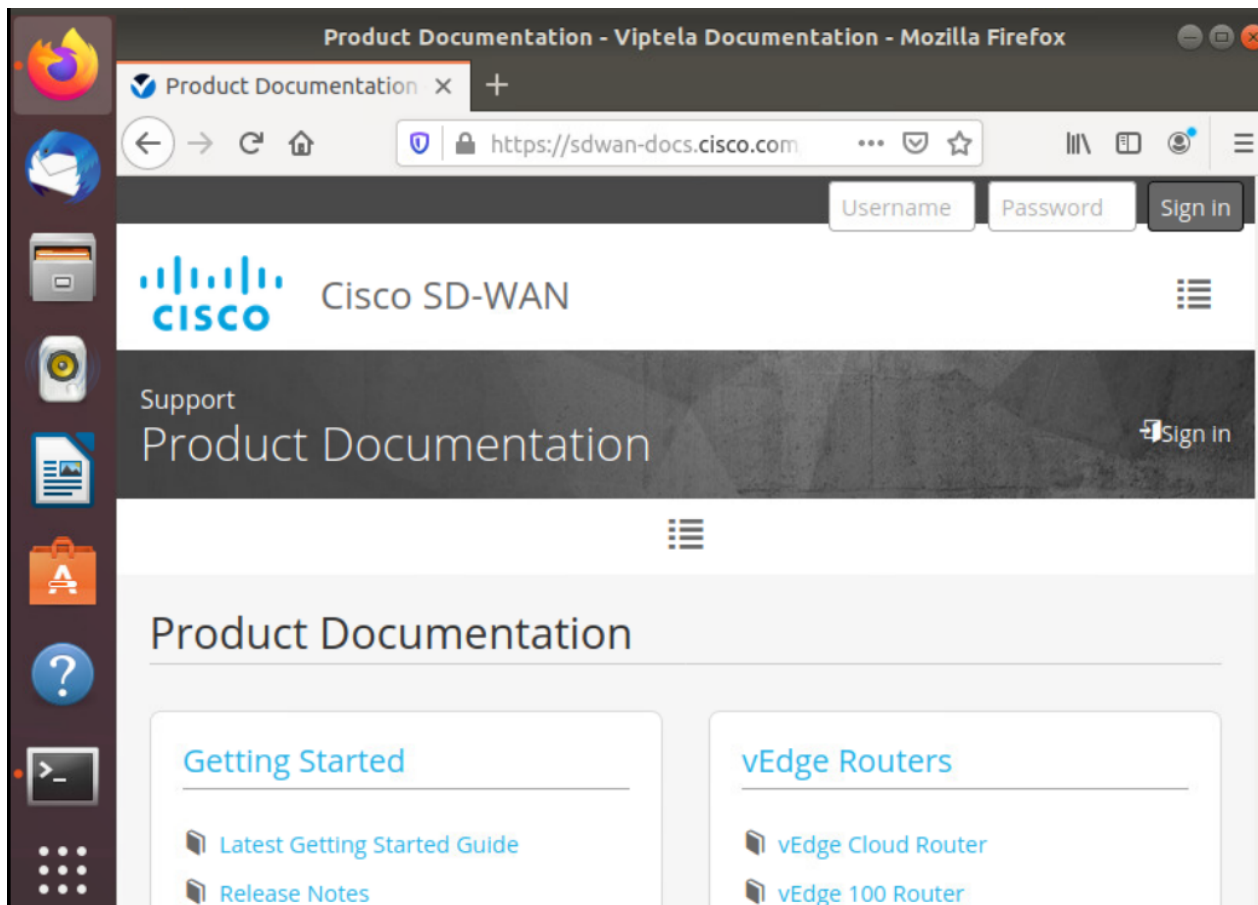
- [Overview](#)
- [Creating and Activating a Policy](#)
- [Verification](#)

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**

Cisco vManage

DASHBOARD | MAIN DASHBOARD

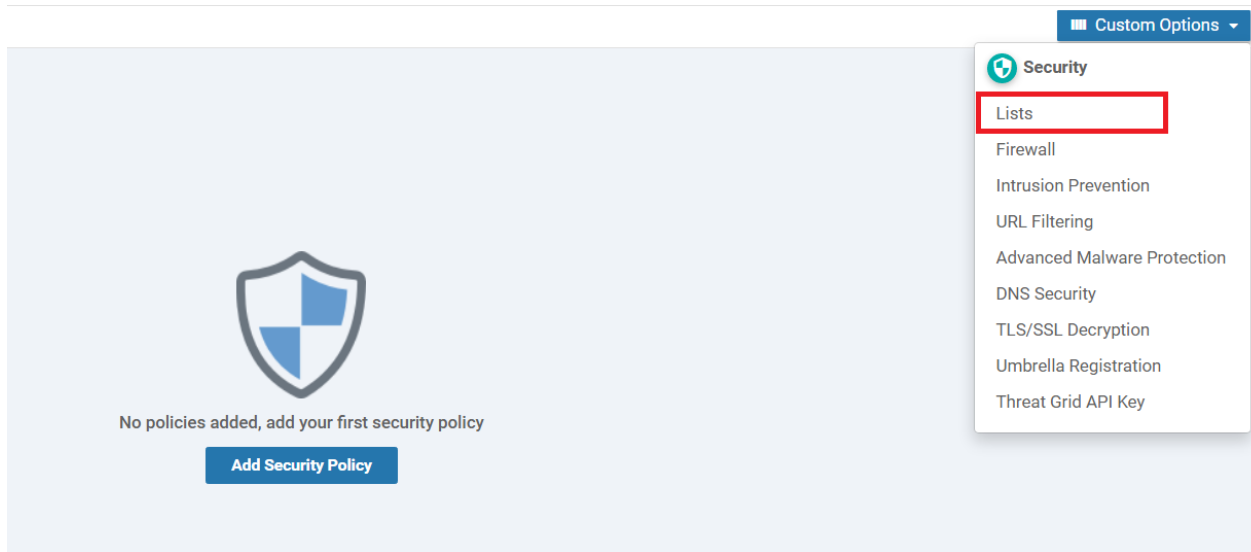
Configuration 2 ↑

WAN Edge - 8

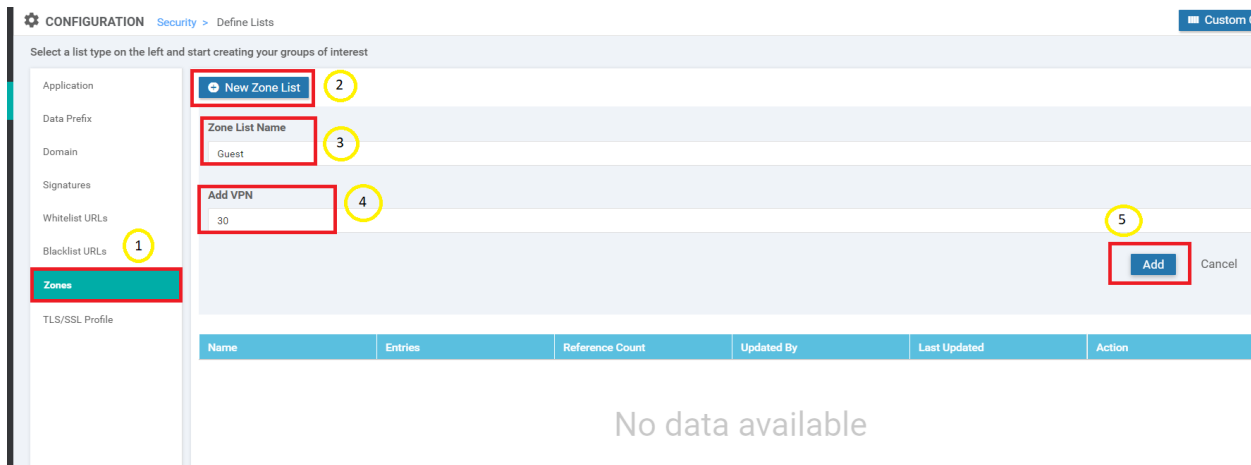
- Configuration
- Devices
- TLS/SSL Proxy 10
- Certificates 0
- Network Design 0
- Templates
- Policies 20
- Security 20
- Unified Communications 8
- Cloud onRamp for SaaS 0
- Cloud onRamp for IaaS
- Cloud onRamp for Colocation

No data to display

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**



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

Add VPN

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)

Application

New Zone List

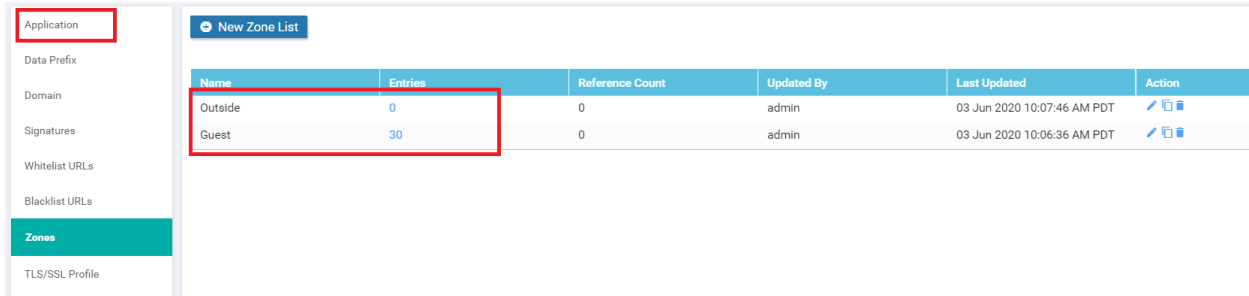
Name	Entries	Reference Count	Updated By	Last Updated	Action
Outside	0	0	admin	03 Jun 2020 10:07:46 AM PDT	✎ 🗑
Guest	30	0	admin	03 Jun 2020 10:06:36 AM PDT	✎ 🗑

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

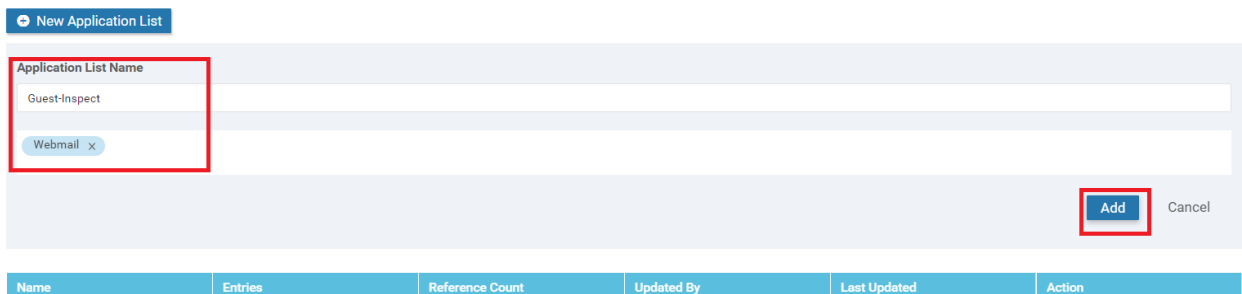
1. From the previous section, click on **Application** in the top left corner of the screen after verifying that both the Zone Lists are visible



2. 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



3. Click on **Add** to add this Application List



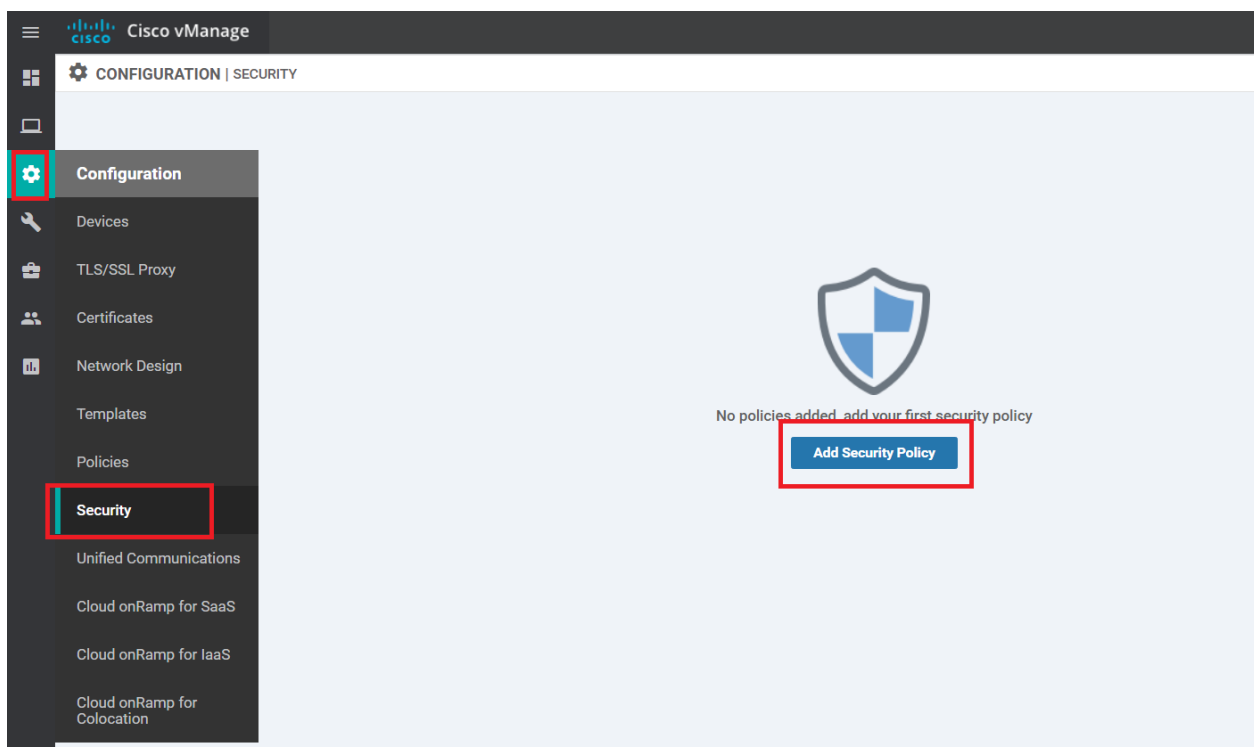
We have created an Application List which can potentially identify Gmail, Mail.ru etc. traffic. We will now create our policy.

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



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*



Create VPN zones and define your 5-tuple and Application behavior within these zones.

+ Add Firewall Policy ▾

- Create New
- Copy from Existing

4. Click on **Apply Zone Pairs**

CONFIGURATION | SECURITY Add Firewall Policy

Sources Apply Zone-Pairs Destinations ×

0 Rules

Name Description

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 Search Options ▾ Default Action **Drop** ▾ Total Rows: 0

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**

Apply Zone-Pair(s) ✕

Target Zone-Pair

Source Zone Guest x → Destination Zone Outside x +

Save Cancel

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**

Sources: Guest → Apply Zone-Pairs → Destinations: Outside

0 Rules

Name: Guest-FW Description: Guest Traffic Firewall

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 Total Rows: 0

Order	Name	Action	Log	Source Data Prefix	Source Port	Destination Data Prefix	Destination Port	Protocol	Application List To Drop
Total Rows: 0									

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

and/or

FQDN (Fully-Qualified Domain Name) ⓘ

FQDN List

Select a fqdn list

FQDN

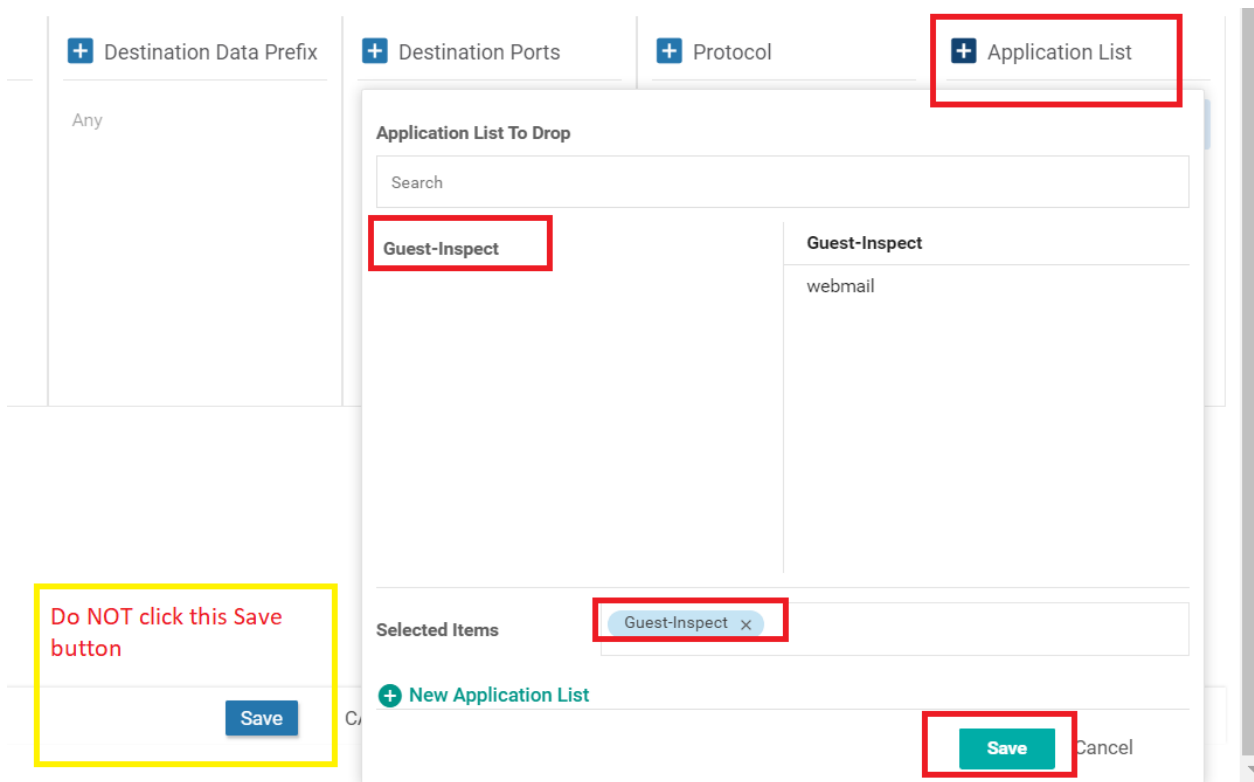
Example: cisco.com and not more than 120 characters

Any

Save Cancel

Do NOT click this Save button Save CANCEL

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 Action

Source / Destination

+ Source Data Prefix	+ Source Port	+ Destination Data Prefix	+ Destination Ports	+ Pro
<input type="button" value="IPv4 List: Guest-Site40"/>	Any	Any	Any	Any

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

- 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

- 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 Name Action Log

Source / Destination

Source Data Prefix	Source Port	Destination Data Prefix	Destination Ports	Protocol
IPv4 List: Guest-Site40	Any	Any	80 443	Any

CANCEL

13. Make sure the Firewall Policy looks as below and click on **Save Firewall Policy**

Sources: Guest → 2 Rules → Destinations: Outside

Name: Description:

Add Rule (Drag and drop the Order cell to re-arrange rules and click on the other cells to inline add/edit the values)

Order	Name	Action	Log	Source Data Prefix	Source Port	Destination Data Prefix	Destination Port	Protocol	Application List To Drop
1	Inspect Web App Guest	Inspect	N/A	Guest-Site40	Any	Any	Any	Any	Guest-Inspect
2	TCP Guest Pass Web	Pass	<input checked="" type="checkbox"/>	Guest-Site40	Any	Any	80 443	Any	Any

CANCEL


14. Click on **Next** and then **Next** again at the URL Filtering and TLS/SSL Decryption sections

Add Firewall Policy (Add a Firewall configuration)

Search Options

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.

i 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

- 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 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_dev...	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	...

- Edit
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

2. Under the **Additional Templates** section, populate the **Security Policy** as *Site40-Guest-DIA* and click on **Update**

Additional Templates

AppQoS

Global Template *

Cisco Banner

Cisco SNMP

CLI Add-On Template

Policy

Probes

Security Policy

3. Choose **Next** and then **Configure Devices** to push the Security Policy to cEdge40

Device Template | cEdge_dualuplink_devtemp

Search Options ▾

S...	Chassis Number	System IP	Hostname	Interface Name(vpn30_if_name)	IPv4 Address/ prefix-length(vpn30_if_ipv4_address)
✓	CSR-04F9482E-44F0-E4DC-D30D-60C0806F...	10.255.255.41	cEdge40	GigabitEthernet6	10.40.30.2/24

Next Cancel

Cisco vManage

CONFIGURATION | TEMPLATES

Device Template: cEdge_dualuplink_devtemp | Total: 1

Device list (Total: 1 device(s))

Filter/Search

CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2
cEdge40|10.255.255.41

Configure Device Rollback Timer

Back

Configure Devices

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

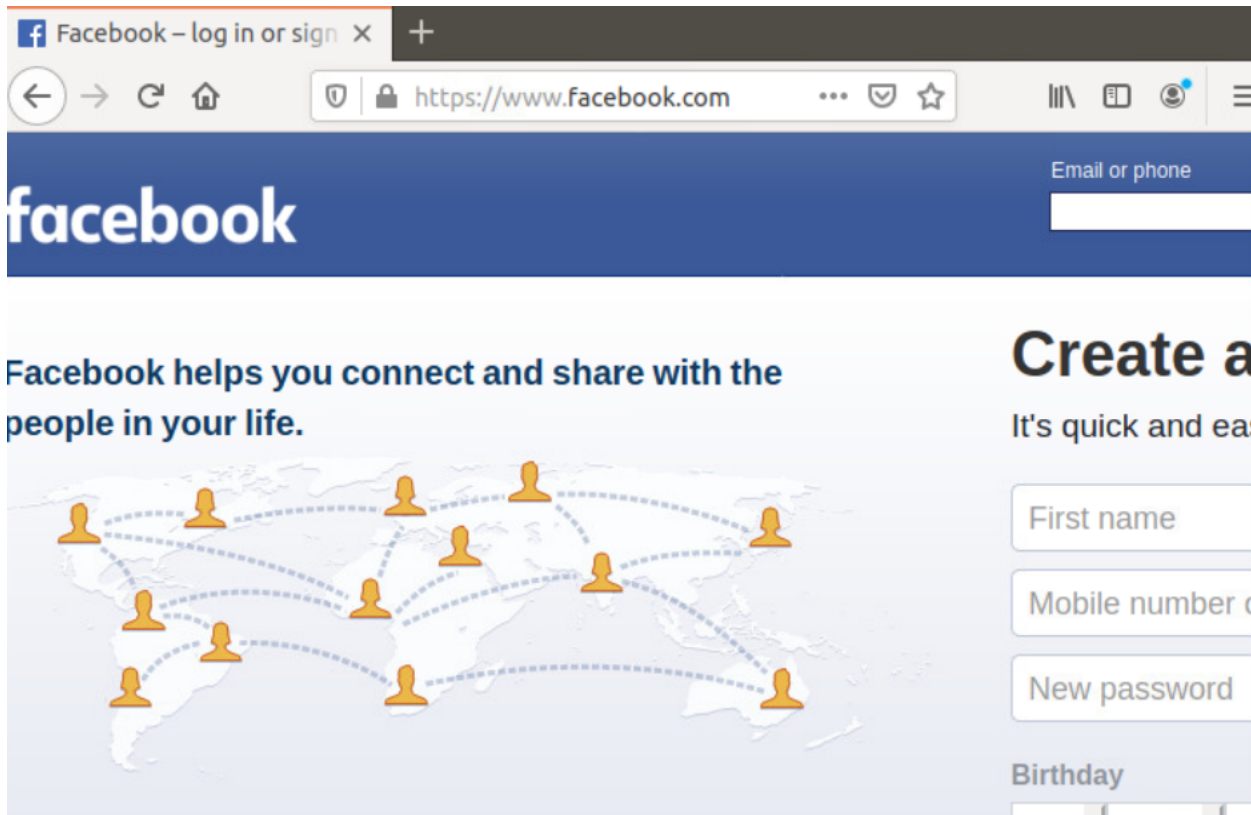
```

235 class-map match-any Guest-Inspect-cm
236 match protocol attribute applicati
237 match protocol attribute applicati
238 match protocol attribute applicati
239 match protocol attribute applicati
240 match protocol attribute applicati
241 match protocol attribute applicati
242 match protocol attribute applicati
243 match protocol attribute applicati
244 match protocol attribute applicati
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-Tr
259 class Guest-Inspect-cm0_
260 deny

```

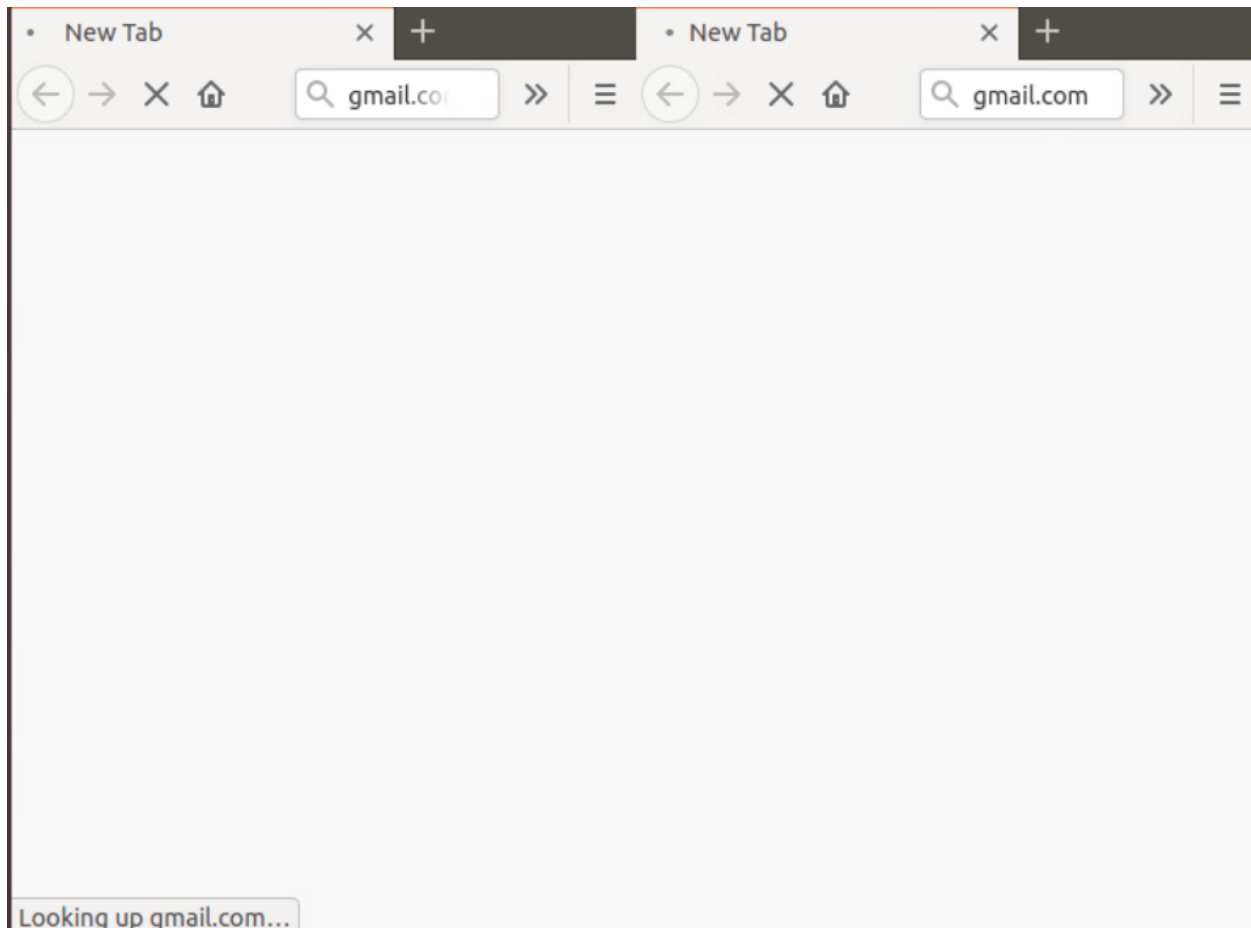
- Open the Console session to the Site 40 PC (log in to vCenter => locate the site40pc VM and open the Web Console) and navigate to www.facebook.com. It should work indicating that Web Traffic is allowed. Log in to the cEdge40 CLI

via Putty and issue a `show logg`. We should see some activity there

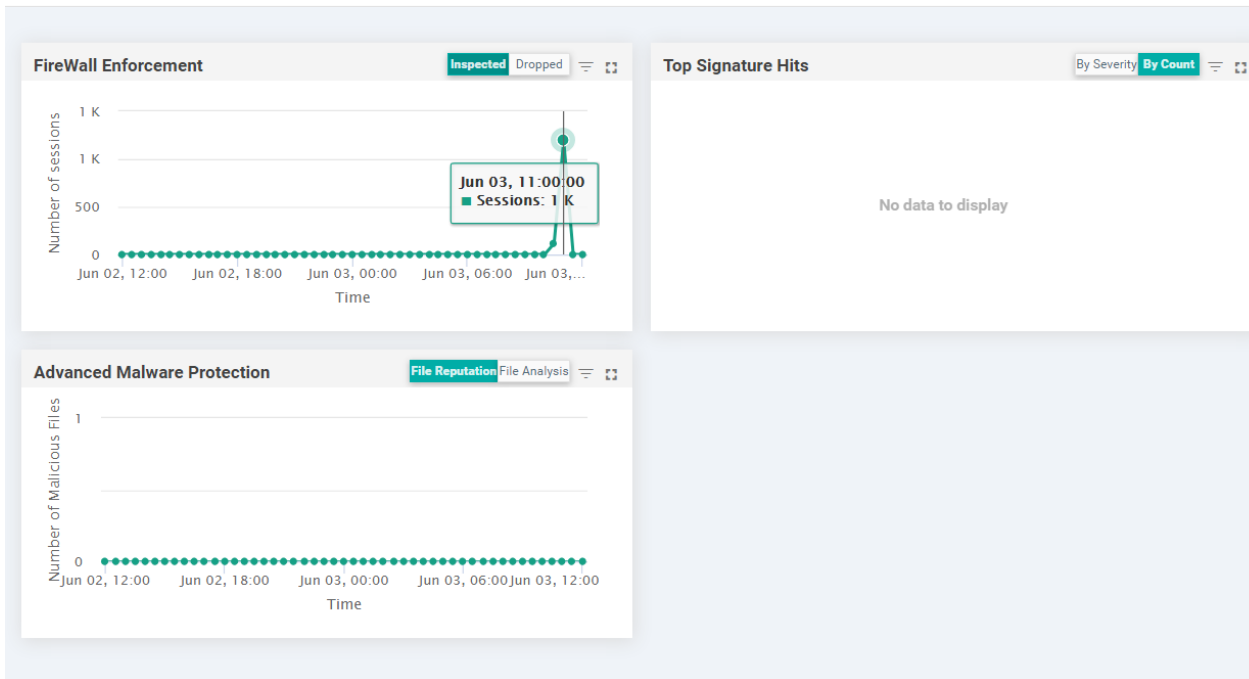


```
*Jun 3 19:03:34.241: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001392528385401610 %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(ZP_Guest_Outside_Guest-FW:Guest-FW-seq-1-cm):Start session: initiator (10.40.30.21:40698) -- responder (31.13.79.26:443) from GigabitEthernet6 (srcvrf:dstvrf)-(30:global)
*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_Outside_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:global)
*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_Outside_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:global)
*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_Outside_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:global)
*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_Guest-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_Guest-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 Troubleshooting

VPN*: VPN - 10 Source/Interface for VPN - 10*: GigabitEthernet4 - ipv4 - 10.40.10.2 Source IP*: 10.40.10.2 Destination IP*: 10.100.10.2 Application: Choose

Advanced Options >

Simulate

Output: Total next hops: 4 | IPSec: 4

Flow Diagram:

- 10.255.255.41
- public-internet Remote System IP 10.255.255.12 Encapsulation IPSec
- ← public-internet
- mpls Remote System IP 10.255.255.11 Encapsulation IPSec
- ← mpls
- public-internet Remote System IP 10.255.255.11 Encapsulation IPSec
- ← public-internet
- mpls Remote System IP 10.255.255.12 Encapsulation IPSec
- ← mpls

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

VPN* **VPN - 10** Source/Interface for VPN - 10* **GigabitEthernet4 - ipv4 - 10.40.10.2** Source IP* **10.40.10.2** Destination IP* **10.100.10.2** Application **Choose**

Advanced Options

Path Tunnel Service

Protocol* **1** Source Port Destination Port DSCP **46** All Paths

Simulate

Output: Total next hops: 4 | IPSec : 4

Activate Windows
Go to Settings to activate Windows.

- 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

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest
 Configure Topology and VPN Membership
 Configure Traffic Rules
 Add Policy

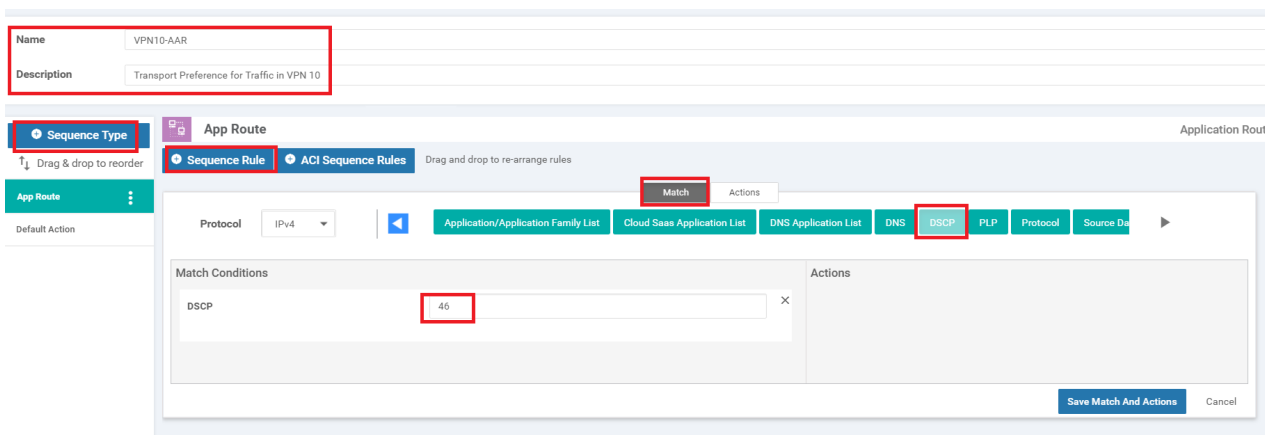
Choose a tab and add Traffic rules under the selected type

[Application Aware Routing](#)
[Traffic Data](#)
[Cflowd](#)

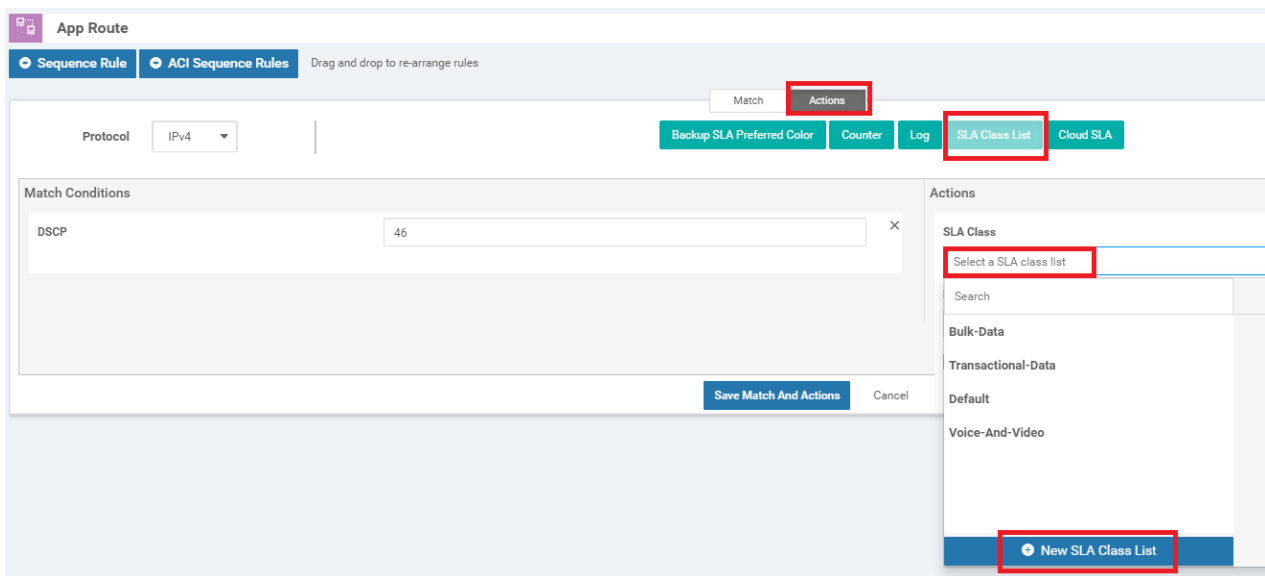
(Create an application-aware routing policy)

Name	Type	Description	Reference Count	Updated By
No data available				

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 [X]

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

Match **Actions**

Protocol IPv4

Backup SLA Preferred Color Counter Log SLA Class List Cloud SLA

Match Conditions

DSCP 46

Actions

SLA Class

Voice-SLA

Preferred Color

mpls

Save Match And Actions Cancel Strict

6. Ensure your App Route looks like the image below and click on **Save Application Aware Routing Policy**. Click **Next**

1

Match Conditions	Actions
DSCP: 46	SLA Class: List Voice-SLA Preferred Color mpl 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

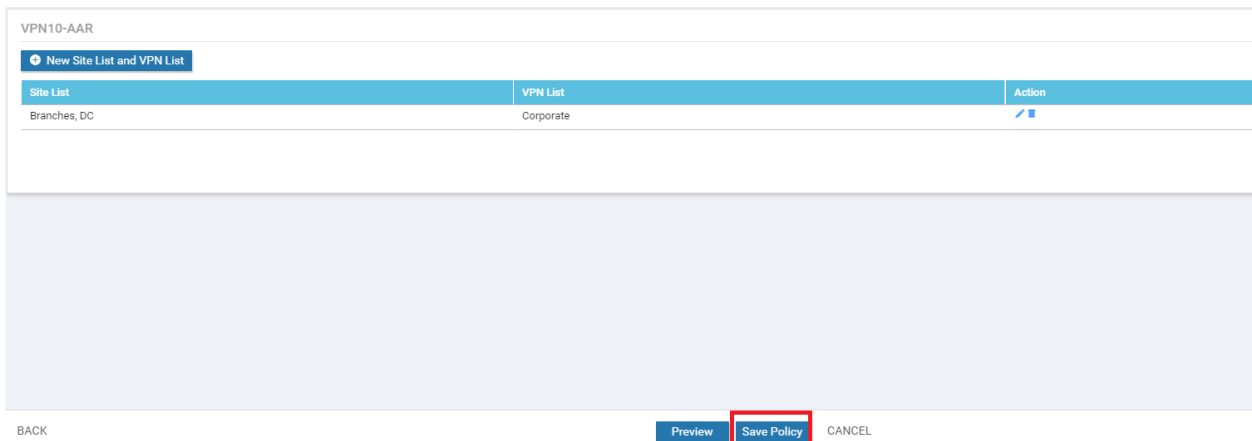
New Site List and VPN List

Select Site List: Branches x DC x

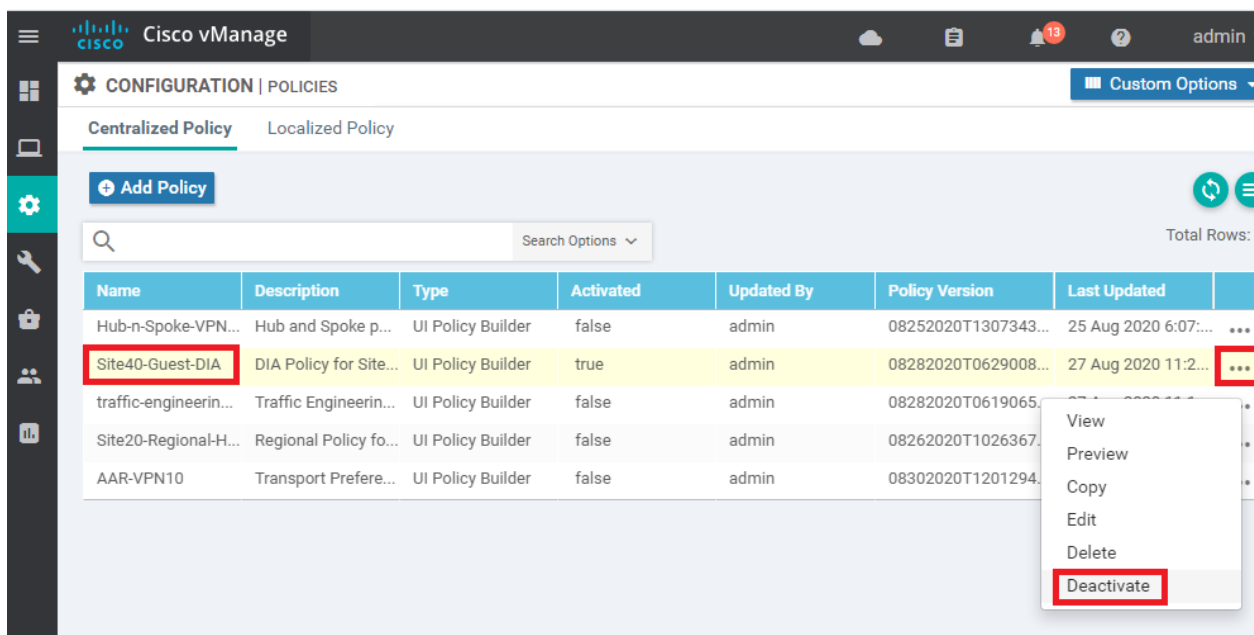
Select VPN List: Corporate x

Add
Cancel

8. Click on **Save Policy** in the lower middle part of the screen to save our AAR Policy



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



Deactivate Policy

Policy will be removed from the following vSmart.
10.255.255.3, 10.255.255.4

Would you like to remove policy from reachable vSmarts?

Deactivate **Cancel**

Add Policy Total Rows: 5

Search Options

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
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 A	View
traffic-engineering-ftp	Traffic Engineering for FTP	UI Policy Builder	false	admin	06032020T131902822	03 Jun 2020 6:19:02 A	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 A	Copy
Site40-Guest-DIA	DIA Policy for Site 40 Guests	UI Policy Builder	true	admin	06032020T142511667	03 Jun 2020 7:25:11 A	Edit
							Delete
							Activate

Activate Policy

Policy will be applied to the reachable vSmarts:
10.255.255.3, 10.255.255.4

Activate **Cancel**

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

The screenshot displays the 'Simulate Flows' configuration interface in the vManage GUI. The configuration is as follows:

- VPN*:** VPN-10
- Source/Interface for VPN-10*:** GigabitEthernet4 - ipv4 - 10.40.10.2
- Source IP*:** 10.40.10.2
- Destination IP*:** 10.100.10.2
- Application:** Choose

The **Simulate** button is highlighted. The output section shows a flow diagram with the following details:

- Total next hops:** 4 | **IPSec:** 4
- Source IP:** 10.255.255.41
- Path 1:** public-internet (Encapsulation) / Remote System IP 10.255.255.12 / IPsec
- Path 2:** mpls (Encapsulation) / Remote System IP 10.255.255.11 / IPsec
- Path 3:** public-internet (Encapsulation) / Remote System IP 10.255.255.11 / IPsec
- Path 4:** mpls (Encapsulation) / Remote System IP 10.255.255.12 / IPsec

2. On the same screen, click on **Advanced Options** and set the DSCP to 46. Click on **Simulate**

VPN: VPN-10 | Source/Interface for VPN-10: GigabitEthernet4 - ipv4 - 10.40.10 | Source IP: 10.40.10.2 | Destination IP: 10.100.10.2 | Application: Choose | Custom Application (created in CLI):

Advanced Options

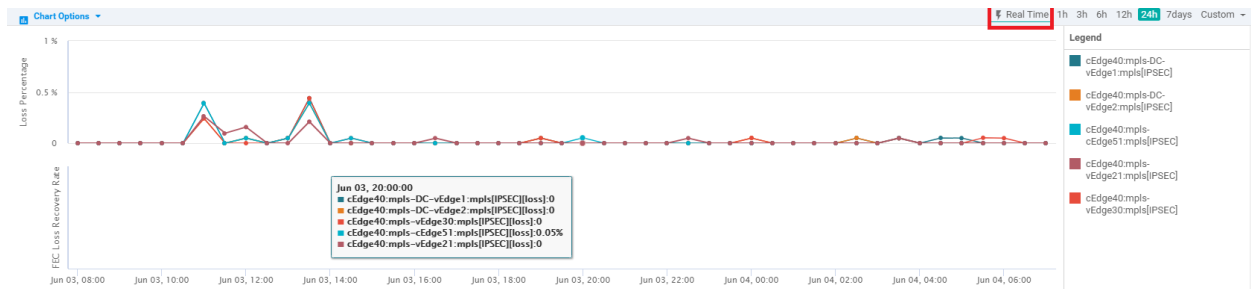
Path: Tunnel Service | Protocol: 1 | Source Port: | Destination Port: | DSCP: 46 | All Paths

Simulate

Output: Total next hops: 2 | IPSec: 2

VoIP Traffic is now traversing the MPLS link as the preferred route.

- 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

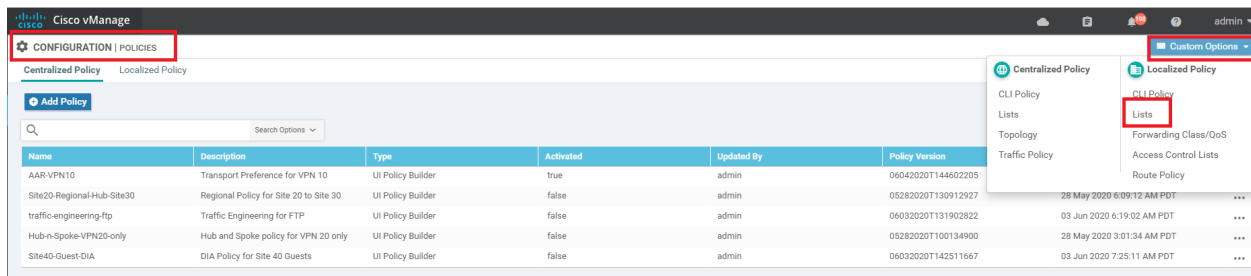
Configuring a Policer to simulate network impairment

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**



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 Custom Options

Select a list type on the left and start creating your groups of interest

AS Path
Community
Data Prefix
Extended Community
Class Map
Mirror
Policer
Prefix

New Policer List

Policer List Name
AARImpair-Police-P[]

Burst (bps) 15000 Exceed Drop Rate (bps) 7000

Add Cancel

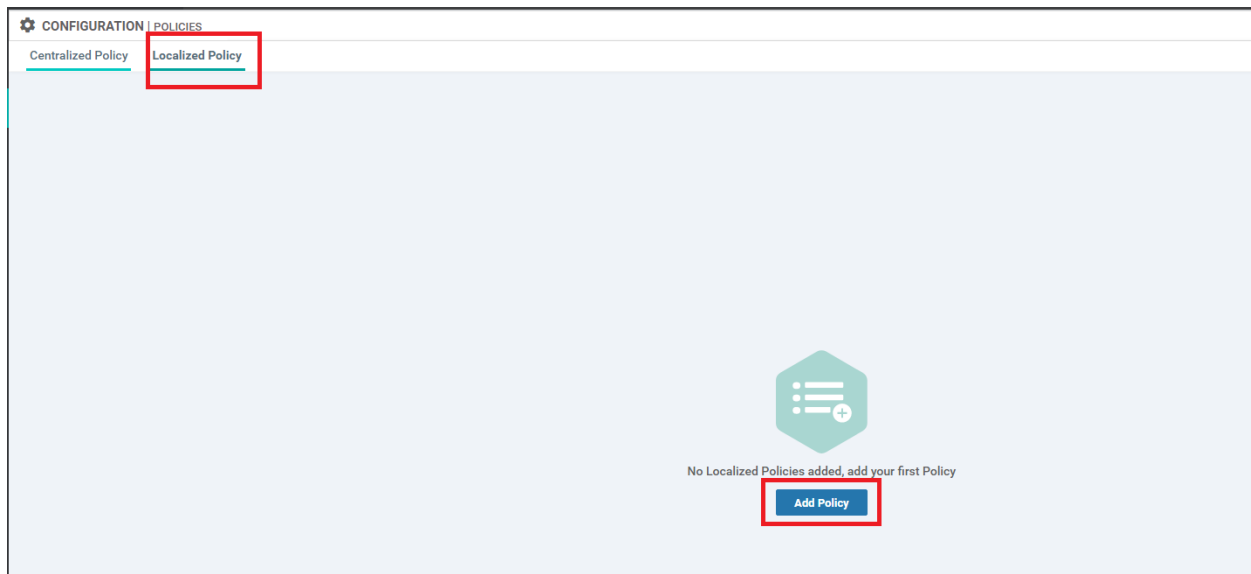
Name	Burst	Exceed	Rate	Reference Count	Updated By	Last Updated	Action
No data available							

Task List

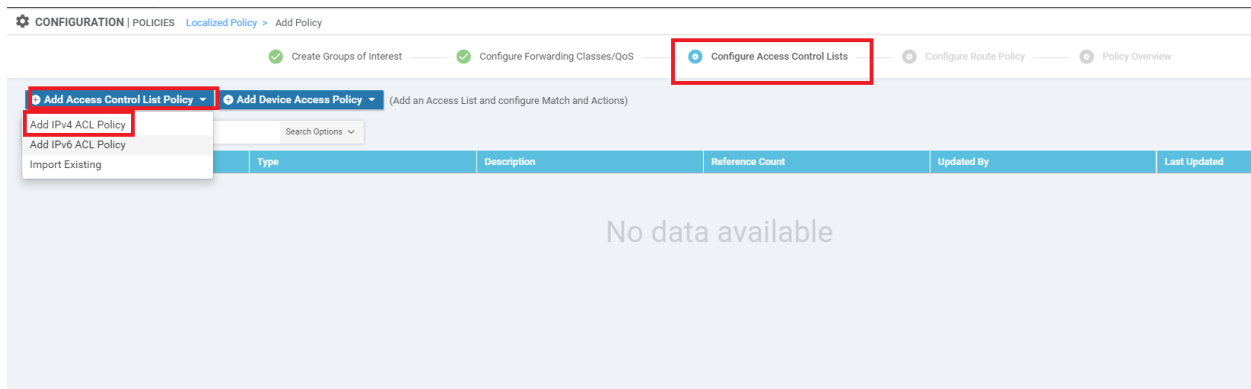
- ~~Overview~~
- ~~Creating and Activating the AAR Policy~~
- ~~Viewing modified traffic flows and current network statistics~~
- Configuring a Policer to simulate network impairment
- ~~Creating a Policer List~~
- Configuring the IPv4 ACL Policy
- Applying the Policer on the MPLS link
- Viewing changed statistics and resultant traffic flows

Configuring the IPv4 ACL Policy

1. Go to the **Localized Policy** tab and click on **Add Policy**



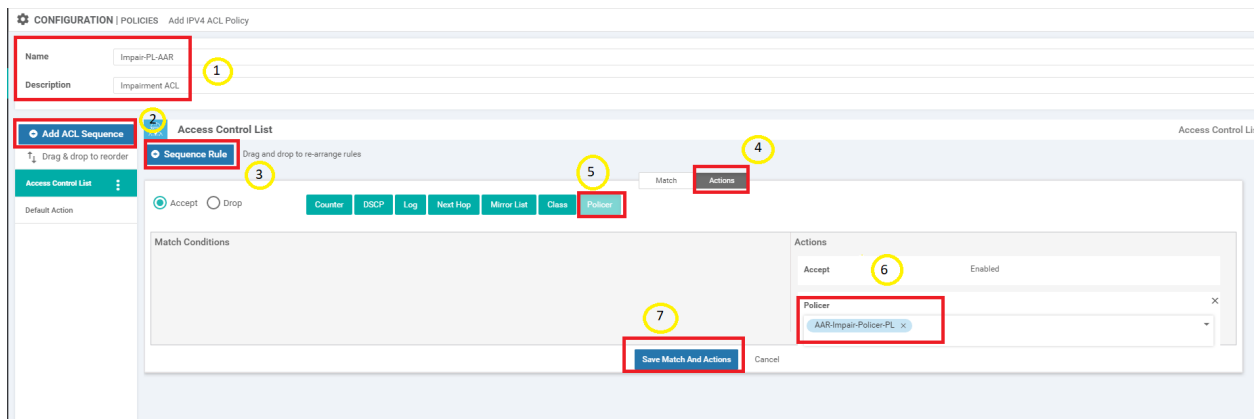
2. Click **Next** till you are at the **Configure Access Control Lists** page. Click on **Add Access Control List Policy** and choose **Add IPv4 ACL Policy**



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

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

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**

The screenshot shows the 'Feature' tab of the 'Template' section in the NCM interface. The 'cedge-vpn0-int-dual_mpls' template is highlighted in yellow, and its 'More Actions' menu is open, showing the 'Copy' option.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	
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 12:54:12 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 Edit Change Device Models
cEdge_VPN0_single_uplink	cEdge VPN 0 Template for Single U...	Cisco VPN	CSR1000v	1	2	admin	18 May 2020	Delete
cedge-vpn0-int-single	cEdge VPN 0 Interface Template fo...	Cisco VPN Interface	CSR1000v	1	2	admin	18 May 2020	Copy
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
site40-elgrp	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

Description

3. Click on the three dots next to this newly copied template and click on **Edit**

Template Name	Description	Model	Count	Created By	Created At	Actions
cedge-vpn30-int	VPN 30 Interface Template for cEdg...	Cisco VPN Interface	2	admin	25 May 2020 2:03:37 PM PDT	...
cedge-vpn30	VPN 30 Template for the cEdges	Cisco VPN	2	admin	25 May 2020 1:57:26 PM PDT	...
cedge-vpn0-int-dual_mpls-impair	cEdge VPN 0 Interface Template fo...	Cisco VPN Interface	0	admin	04 Jun 2020 9:20:05 AM PDT	...
CEdge_VPN0_single_uplink	cEdge VPN 0 Template for Single U...	Cisco VPN	1	admin	18 May 2020 11:22:10 AM PDT	...
cedge-vpn20-int	VPN 20 Interface Template for cEd...	Cisco VPN Interface	2	admin	25 May 2020 1:57:26 PM PDT	View, Edit
cedge-vpn10-int	VPN 10 Interface Template for cEd...	Cisco VPN Interface	2	admin	25 May 2020 1:57:26 PM PDT	View, Edit, Change Device Models
site40-eigrp	EIGRP Template for Site 40 cEdge	EIGRP	1	admin	26 May 2020 11:22:10 AM PDT	Delete, Copy

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)

QoS Map

Rewrite Rule

Ingress ACL - IPv4 On Off

IPv4 Ingress Access List

Egress ACL - IPv4 On Off

IPv4 Egress Access List

Ingress ACL - IPv6 On Off

Egress ACL - IPv6 On Off

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

Total Rows: 6

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	List Updated	Template Status
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
vEdgeV0_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

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 *

Cisco VPN Interface Ethernet

Cisco VPN Interface Ethernet

Cisco VPN 512 *

Cisco VPN Interface Ethernet

Service VPN

0 Rows Selected

Search Options

7. Scroll down to the **Additional Templates** section and update the **Policy** to *Policer-AAR-Impairment*. Click on **Update**. Click on **Next**

Additional Templates

AppQoS

Global Template *

Cisco Banner

Cisco SNMP

CLI Add-On Template

Policy

Probes

Security Policy

8. You can choose to view the Side by Side or simply click on **Configure Devices**

The screenshot displays a configuration management interface with a side-by-side comparison of configurations for two devices. On the left, the configuration for 'cEdge_dualuplink_devtemp' is shown, and on the right, the configuration for 'Impair-PL-AAR' is shown. The configurations are identical, including settings for interfaces, tunnel-interfaces, encapsulation, and various services. A 'Configure Devices' button is highlighted in red at the bottom right.

Line	Configuration	Line	Configuration
74	no allow-service snmp	74	no allow-service snmp
75	exit	75	exit
76	exit	76	exit
77	interface GigabitEthernet3	77	interface GigabitEthernet3
78	tunnel-interface	78	tunnel-interface
79	encapsulation ipsec weight 1	79	encapsulation ipsec weight 1
80	no border	80	no border
81	color mpls restrict	81	color mpls restrict
82	no last-resort-circuit	82	no last-resort-circuit
83	no low-bandwidth-link	83	no low-bandwidth-link
84	no vbond-as-stun-server	84	no vbond-as-stun-server
85	vmanage-connection-preference 5	85	vmanage-connection-preference 5
86	port-hop	86	port-hop
87	carrier default	87	carrier default
88	nat-refresh-interval 5	88	nat-refresh-interval 5
89	hello-interval 1000	89	hello-interval 1000
90	hello-tolerance 12	90	hello-tolerance 12
91	allow-service all	91	allow-service all
92	no allow-service bgp	92	no allow-service bgp
93	allow-service dhcp	93	allow-service dhcp
94	allow-service dns	94	allow-service dns
95	allow-service icmp	95	allow-service icmp
96	no allow-service sshd	96	no allow-service sshd
97	no allow-service netconf	97	no allow-service netconf
98	no allow-service ntp	98	no allow-service ntp
99	no allow-service ospf	99	no allow-service ospf
100	no allow-service stun	100	no allow-service stun
101	allow-service https	101	allow-service https
102	no allow-service snmp	102	no allow-service snmp
103	exit	103	exit
104		104	access-list Impair-PL-AAR in
105		105	access-list Impair-PL-AAR out

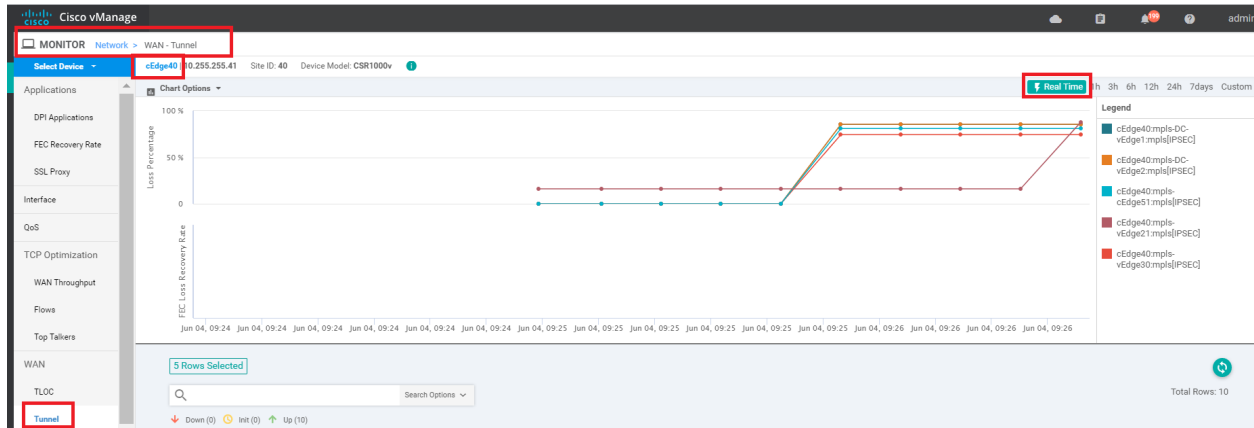
This completes the implementation of our Policer on the MPLS link to simulate network impairment.

Task List

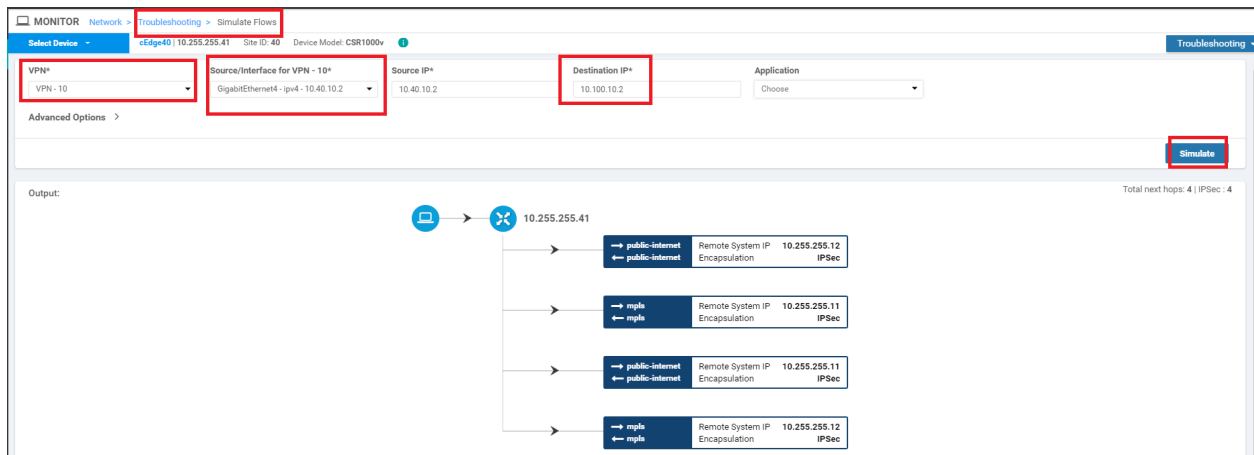
- [Overview](#)
- [Creating and Activating the AAR Policy](#)
- [Viewing modified traffic flows and current network statistics](#)
- [Configuring a Policer to simulate network impairment](#)
- [Creating a Policer List](#)
- [Configuring the IPv4 ACL Policy](#)
- [Applying the Policer on the MPLS link](#)
- [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](#)

MONITOR Network > Troubleshooting > Simulate Flows

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

VPN*: VPN-10 Source/Interface for VPN-10*: GigabitEthernet4-ipv4-10.40.10.2 Source IP*: 10.40.10.2 Destination IP*: 10.100.10.2 Application: Choose

Advanced Options

Path: Tunnel Service Protocol*: 1 Source Port: Destination Port: DSCP: 46 All Paths

Simulate

Output: Total next hops: 2 | IPsec: 2

```
graph LR; S(( )) --> D((10.255.255.41)); D --> P1[public-internet]; P1 --> R1[Remote System IP 10.255.255.11]; R1 --> E1[Encapsulation]; E1 --> I1[IPsec]; I1 --> D; D --> P2[public-internet]; P2 --> R2[Remote System IP 10.255.255.12]; R2 --> E2[Encapsulation]; E2 --> I2[IPsec]; I2 --> D;
```

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 * cEdge_VPN512_dual_uplink

Cisco VPN Interface Ethernet cedge-vpn512-int-dual

Service VPN

0 Rows Selected Add VPN Remove VPN

Search Options

ID	Template Name
<input type="checkbox"/> f018b46b-8ddc-431d-a222-cf905da7e13b	cedge-vpn10
<input type="checkbox"/> ff56fbce-0c12-4575-9f41-b6c7d780e13d	cedge-vpn20
<input type="checkbox"/> 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)

VPN - 10 GigabitEthernet4 - ipv4 - 10.40.10.10.40.10.2 10.100.10.2 Choose

Advanced Options

Path Tunnel Service Protocol Source Port Destination Port DSCP All Paths

1 45

Simulate

Output: Total next hops: 2 | IPSec: 2

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 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~~

©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

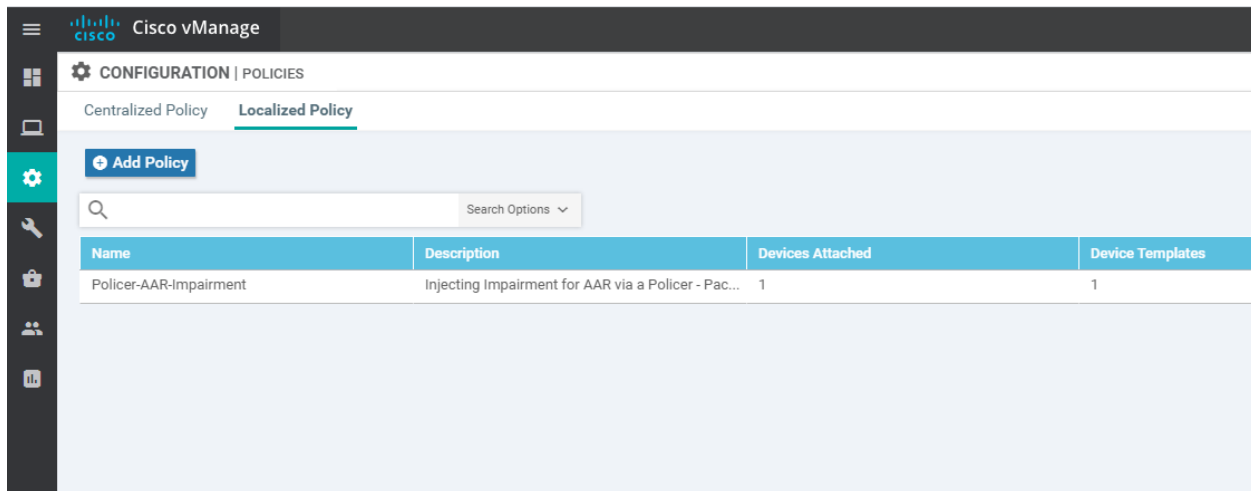
Queue, with corresponding strategies for other types of traffic.

Create a Localized Policy

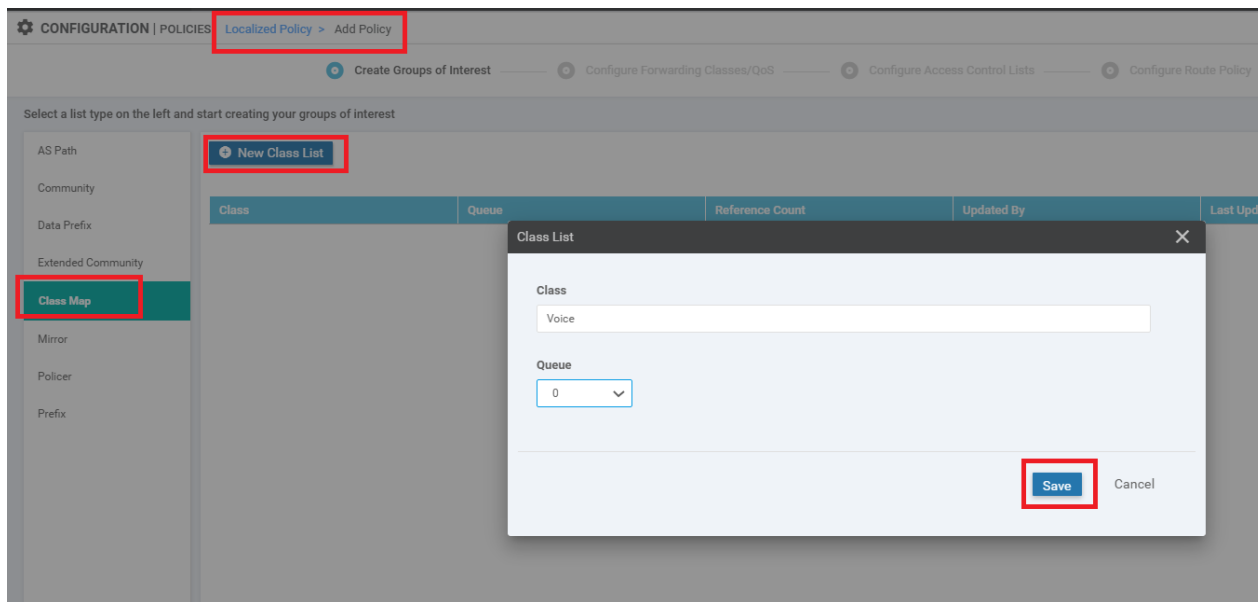
QoS in the SD-WAN world is implemented via Localized Policies. Differences in Localized and Centralized Policies can be found [over here](#).

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**



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**



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

Community

Data Prefix

Extended Community

Class Map

Mirror

Policer

Prefix

[New Class List](#)

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

[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](#)

Add and Configure a QoS Map

QoS Map Policy Rewrite

[Add QoS Map](#) (Add and Configure QoS Map)

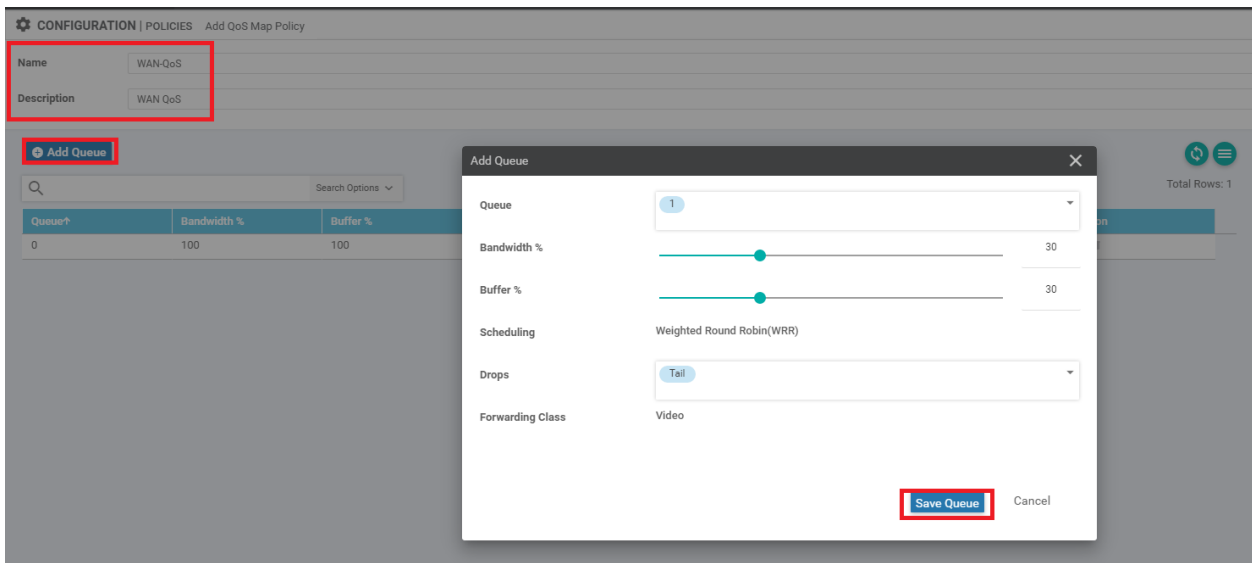
Create New Search Options

Import Existing

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 [X]

Queue

Bandwidth % 40

Buffer % 40

Scheduling Weighted Round Robin(WRR)

Drops

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 [X]

Queue

Bandwidth % 10

Buffer % 10

Scheduling Weighted Round Robin(WRR)

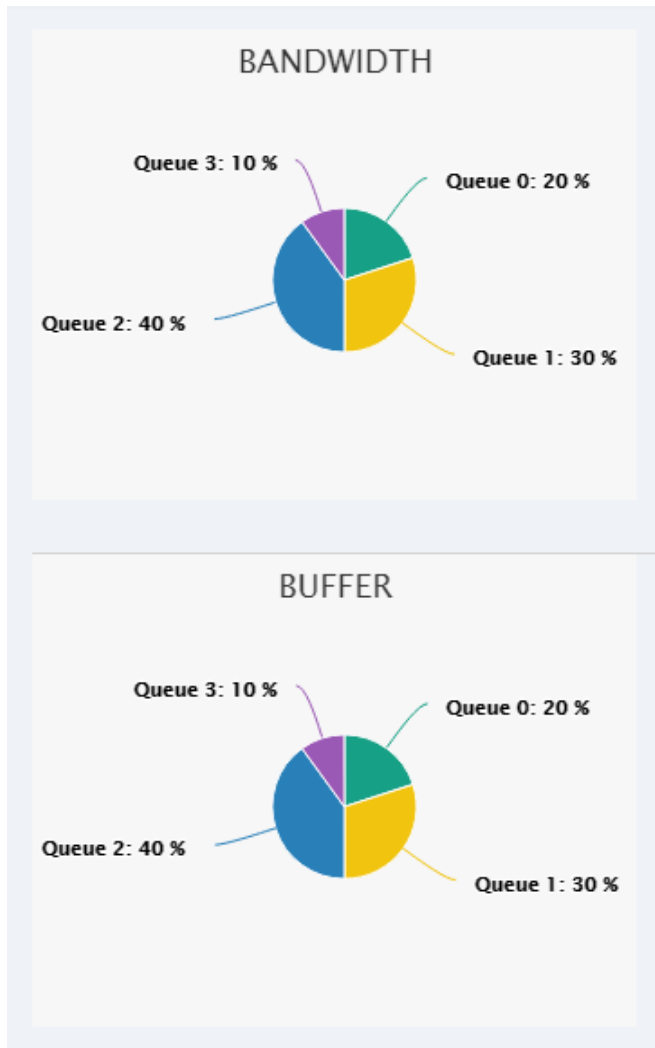
Drops

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**

⊕ Add Queue

Search Options ▾

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	✎

Save Policy CANCEL

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.

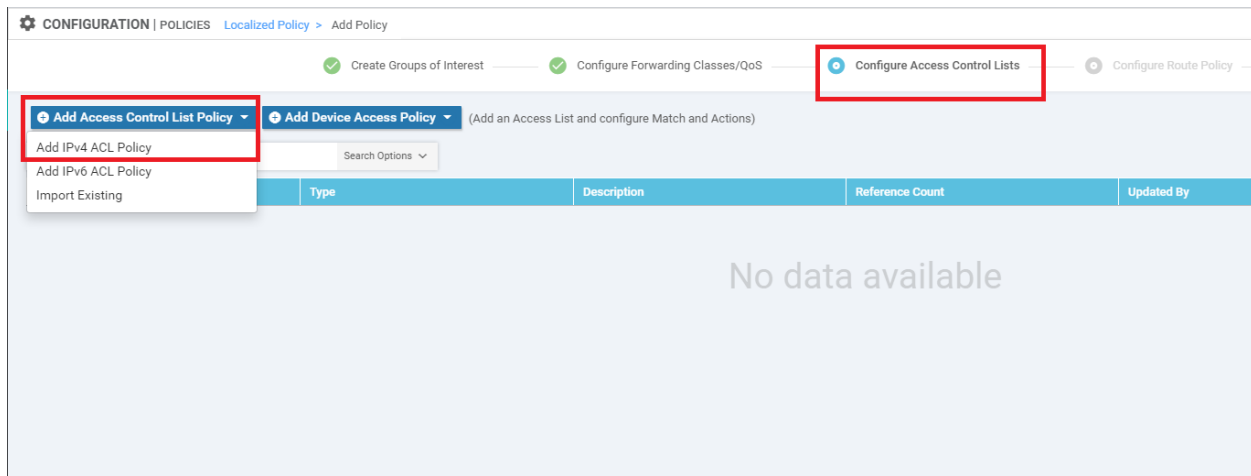
This completes the QoS Map configuration. We will continue with building our Main Policy in the next section.

Task List

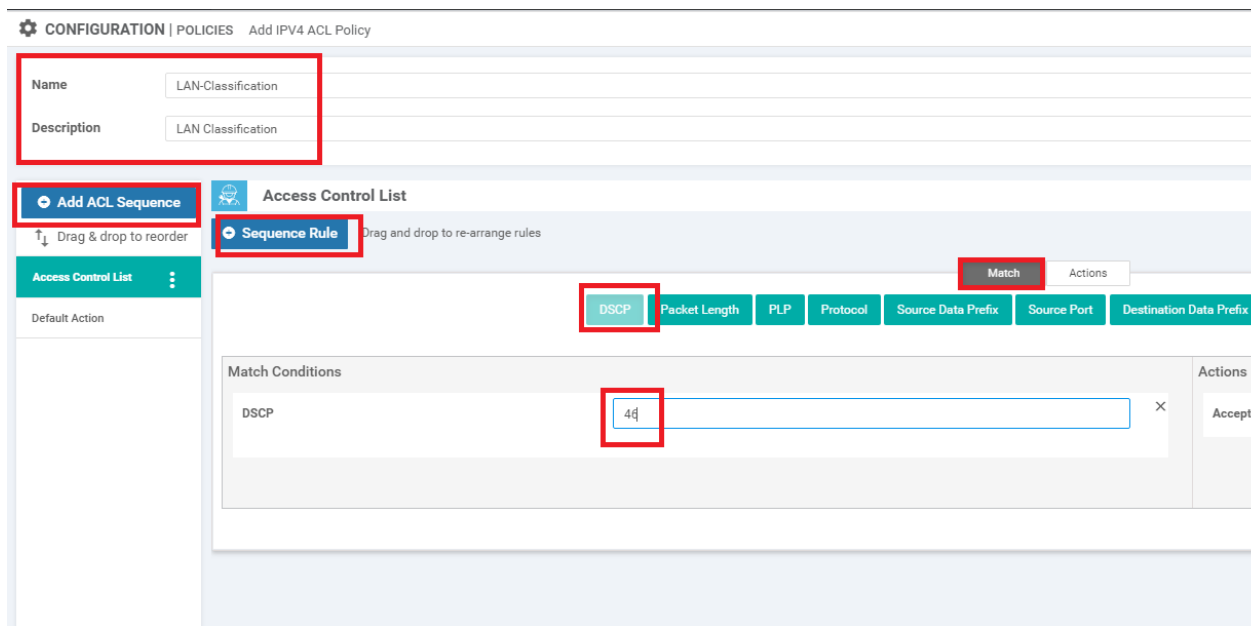
- Create a Localized Policy
 - ~~Add a Class List and a QoS Map~~
 - Configure the IPv4 ACL Policy
 - Complete and apply the localized policy
- Apply the ACL and QoS Map
- Activity Verification

Configure the IPv4 ACL Policy

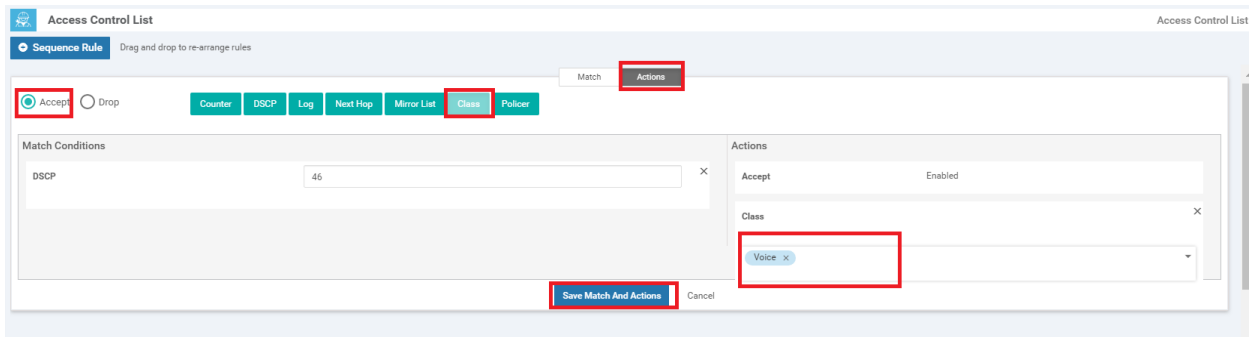
1. Continuing from the QoS Map which we just built, you show now be at the **Configure Access Control Lists** page. An ACL Policy can be used for classification of traffic on the LAN. Click on **Add Access Control List Policy** and choose to **Add IPv4 ACL Policy**



- 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

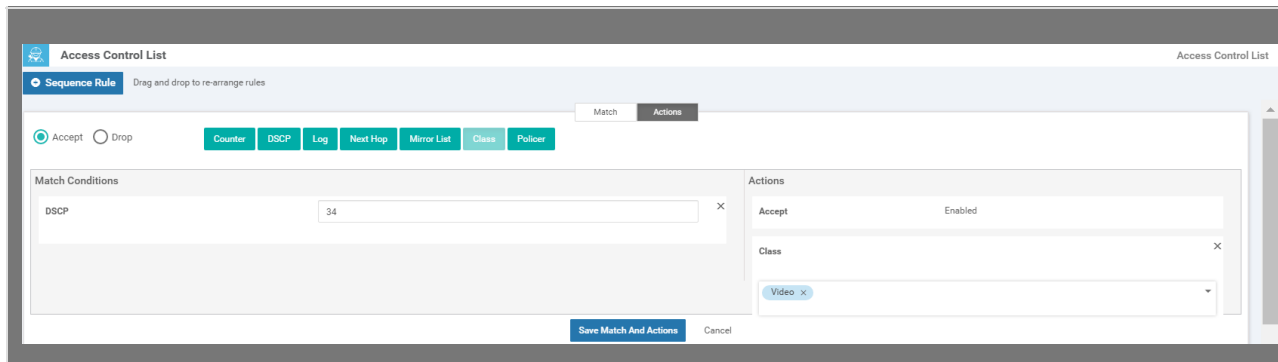


- Click on the **Actions** tab and make sure the **Accept** radio button is selected. Click on **Class** and select the *Voice Class List* which we created before. Click on **Save Match and Actions**



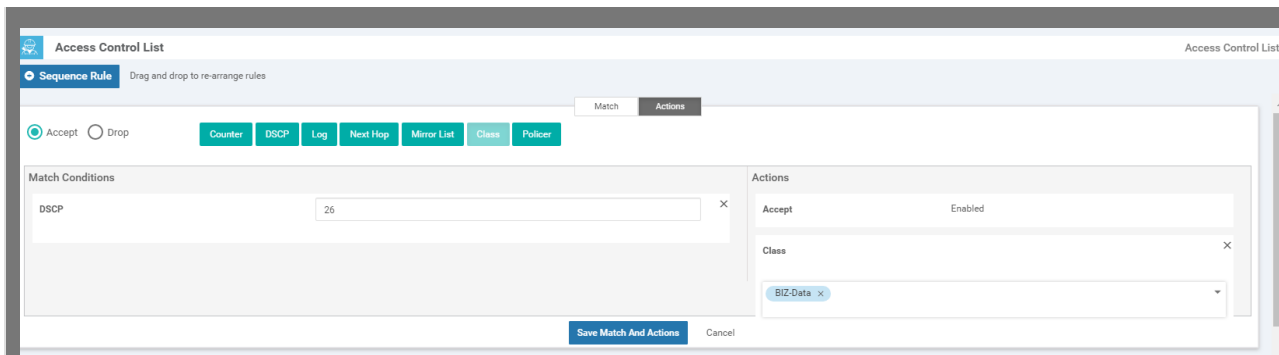
4. Click on **Sequence Rule** and follow the same procedure to create rules as per the following table. Use the images below the table for reference (the actions tab should always have the Accept radio button selected). Make sure that you click on **Save Match and Actions** once done creating each rule

DSCP	Class
34	Video
26	BIZ-Data
Leave Blank	Best-Effort

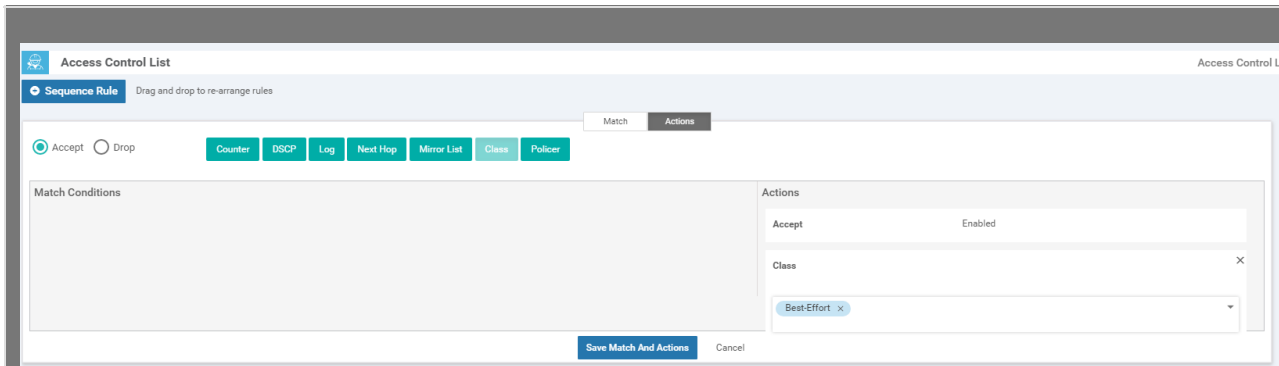


Sequence Rule for Video





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

Access Control List

➤ Add ACL Sequence | ⚙️ Access Control List

⬆️ Drag & drop to reorder | ⚙️ Sequence Rule Drag and drop to re-arrange rules

Match Conditions	Actions
1 DSCP: 46	Accept Class: Voice
2 DSCP: 34	Accept Class: Video
3 DSCP: 26	Accept Class: BIZ-Data
4	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**

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
Policy Description

Policy Settings

Netflow
 Application
 Cloud QoS
 Cloud QoS Service side
 Implicit ACL Logging

Log Frequency

BACK
 Preview
 Save Policy
 CANCEL

- 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
Template Name
Description

Basic Information Transport & Management VPN Service VPN **Additional Templates**

Basic Information

Cisco System *

Cisco Logging*

- 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

4. Click on **Next** and then **Configure Devices**. You can view the side by side configuration, if you want to

Cisco vManage

CONFIGURATION | TEMPLATES

Device Template: cEdge_dualuplink_devtemp (Total: 1)

Device list (Total: 1 devices)

Filter/Search

CSR-04F9482E-44F0-E4DC-030D-60C0806F73F2
cEdge4010.255.255.41

Configure Device Rollback Timer

Back Can

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

```

266 !
267 !
268 policy-map type inspect avc ftp-pm_
269 class ftp-cm0_
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-cm0_
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

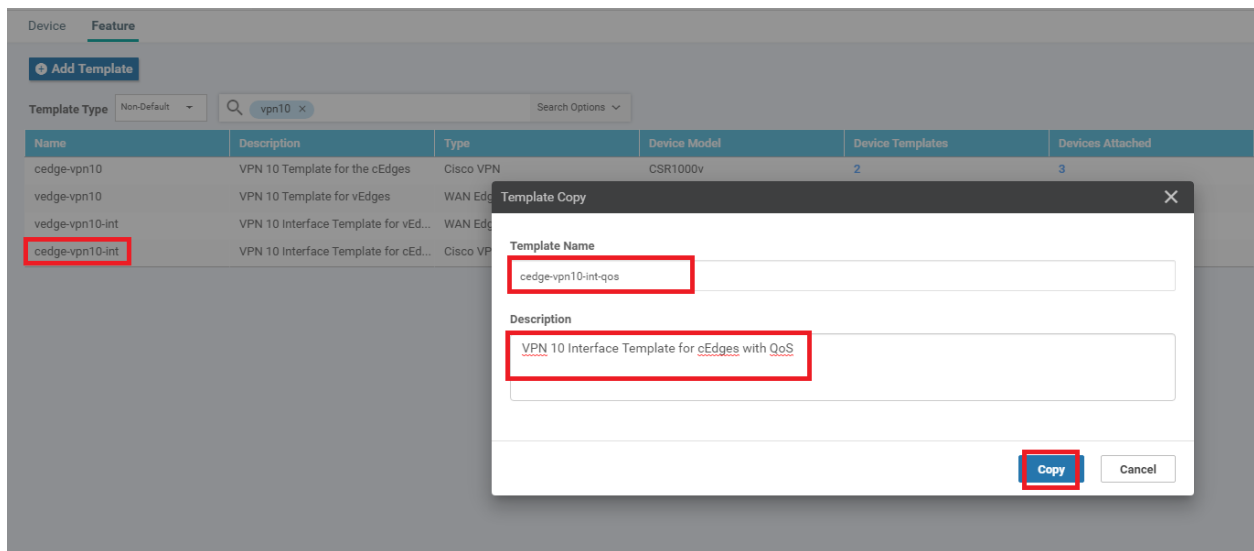
Apply the ACL and QoS Map

We have created the QoS strategy for our network, the only thing that's left is to apply and test our QoS configuration.

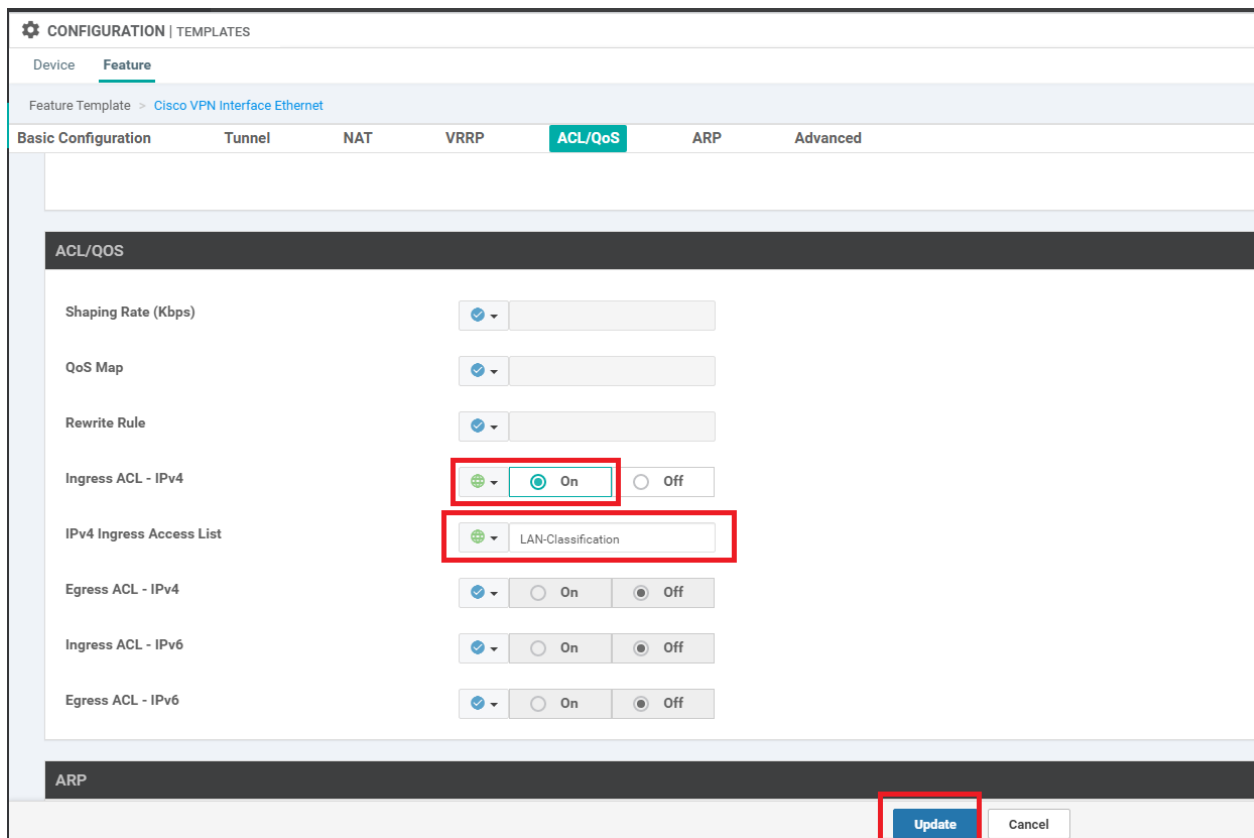
To apply the configuration, we will be modifying the Service VPN 10 interface such that traffic is classified on the basis of the ACL we created, in the inbound direction.

The QoS Map will be applied in the outbound direction on the WAN interfaces (INET and MPLS)

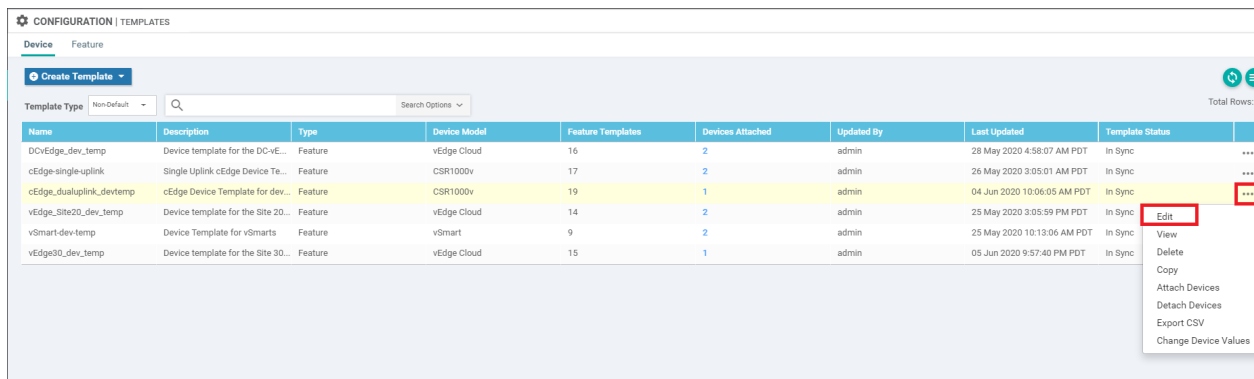
1. Navigate to **Configuration => Templates => Feature Tab** and locate the *cedge-vpn10-int* Feature Template. Click on the three dots next to it and choose to **Copy** the Template. Give a name of *cedge-vpn10-int-qos* to the copied template with a Description of *VPN 10 Interface Template for cEdges 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**



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**



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

Search Options

ID	Template Name	Sub-Templates
<input checked="" type="checkbox"/> f018b46b-8ddc-431d-a222-cf905da7e13b	cedge-vpn10	Cisco VPN Interface Ethernet, EIGRP
<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

Total Rows: 3

Edit Copy Sub-Templates

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 Sub-Templates

EIGRP

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

CONFIGURATION | TEMPLATES

Device Template: cEdge_dualuplink_devtemp (Total: 1)

Device list (Total: 1 devices)

Filter/Search

CSR-04F9482E-44F0-E4DC-D3DD-60C0806F73F2
cEdge4010.255.255.41

Configure Device Rollback Timer

Back

Configure Devices

Ca

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

```

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 exit
105
106 appqoe
107 no toptop enable
108 !
109 omp
110 no shutdown
111 send-path-limit 4
112 ecmp-limit 4
113 graceful-restart
114 no as-dot-notation
115 timers
116 holdtime 60
117 advertisement-interval 1
118 graceful-restart-timer 43200
119 eor-timer 300
120 exit
121 address-family ipv4 vrf 10
122 advertise connected
123 advertise static
124 advertise eigrp
125 !
126 address-family ipv4 vrf 20
127 advertise connected
128 advertise static
129
130
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 exit
105 interface GigabitEthernet4
106 access-list LAN-Classification in
107 exit
108 appqoe
109 no toptop enable
110 !
111 omp
112 no shutdown
113 send-path-limit 4
114 ecmp-limit 4
115 graceful-restart
116 no as-dot-notation
117 timers
118 holdtime 60
119 advertisement-interval 1
120 graceful-restart-timer 43200
121 eor-timer 300
122 exit
123 address-family ipv4 vrf 10
124 advertise connected
125 advertise static
126 advertise eigrp
127 !
128 address-family ipv4 vrf 20
129 advertise connected
130 advertise static

```

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

Add Template

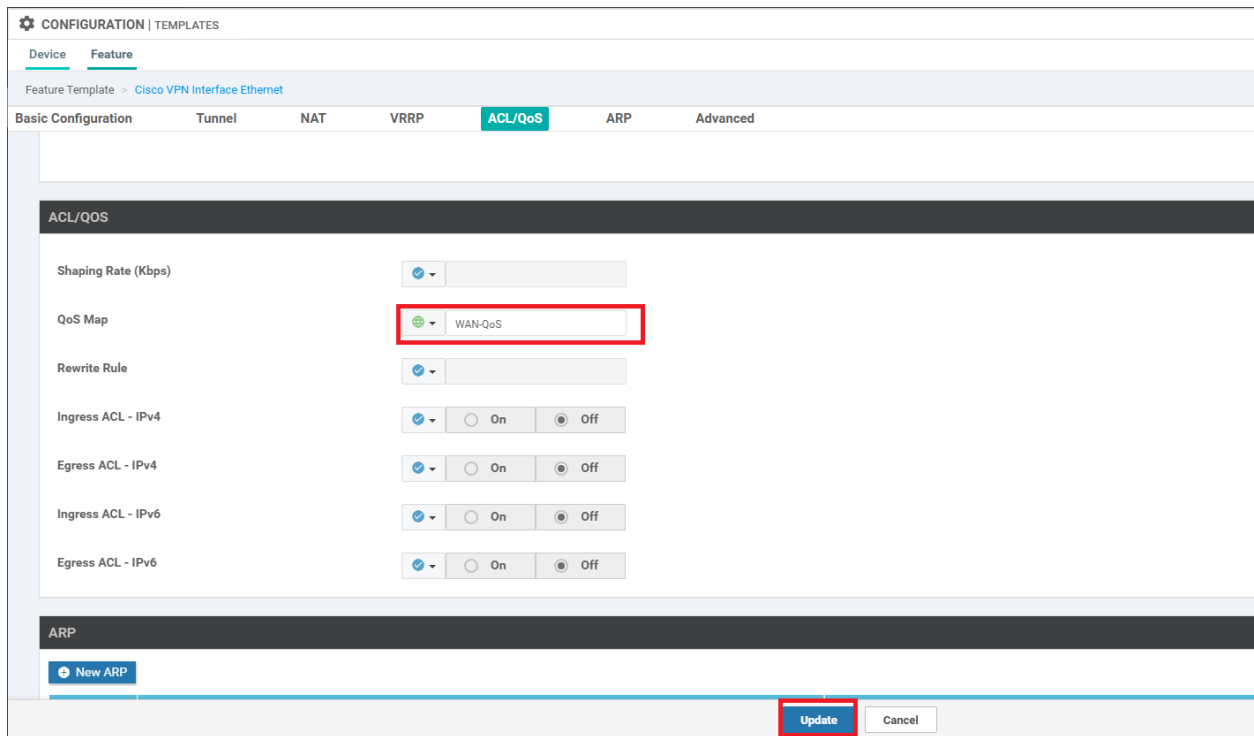
Template Type: Non-Default

Search: cedge

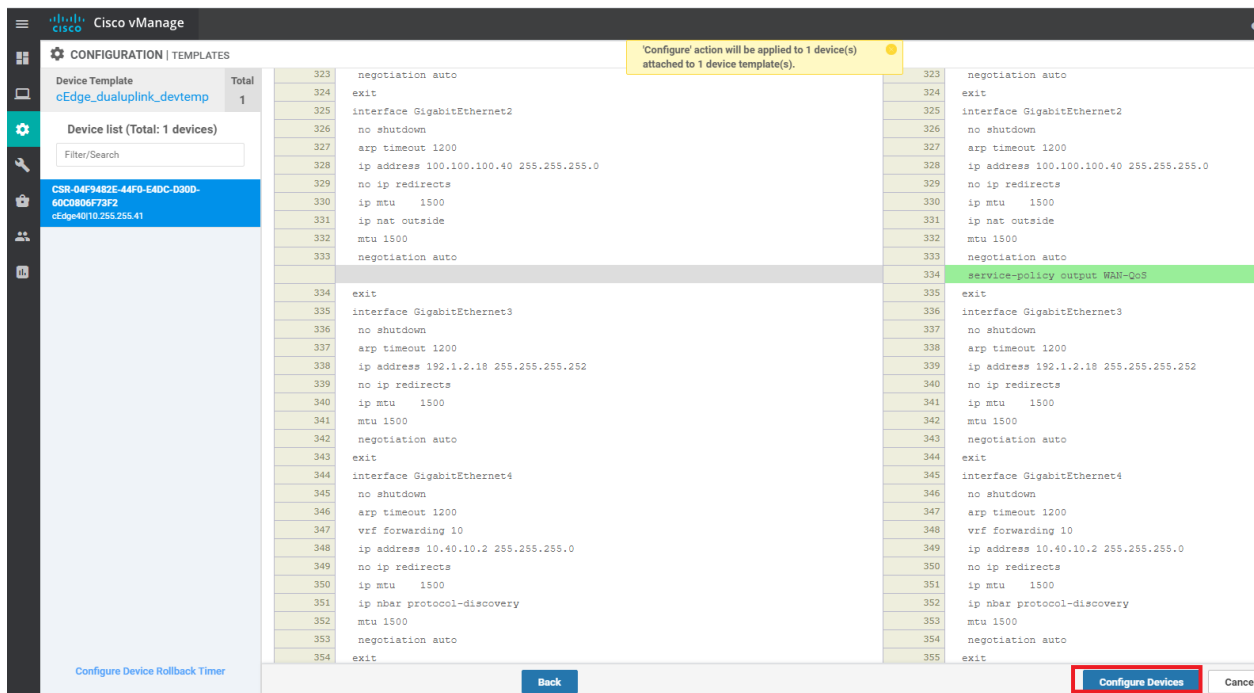
Total Rows: 16 of 36

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	
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-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-vpn512-int-dual	cEdge VPN 512 Interface Template...	Cisco VPN Interface	CSR1000v	2	3	admin	18 May 2020	View
cedge-vpn10	VPN 10 Template for the cEdges	Cisco VPN	CSR1000v	2	3	admin	26 May 2020	Edit
cEdge_VPN512_dual_uplink	cEdge VPN 512 Template for Dual ...	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

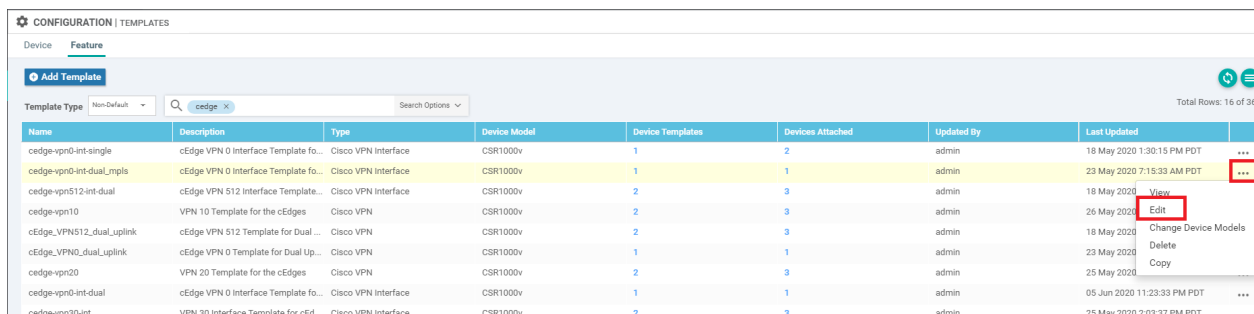
8. Under the **ACL/QOS** section, specify the **QoS Map** as a Global value and enter *WAN-QoS* (case sensitive, should match with the QOS Map we created before). Click on **Update**



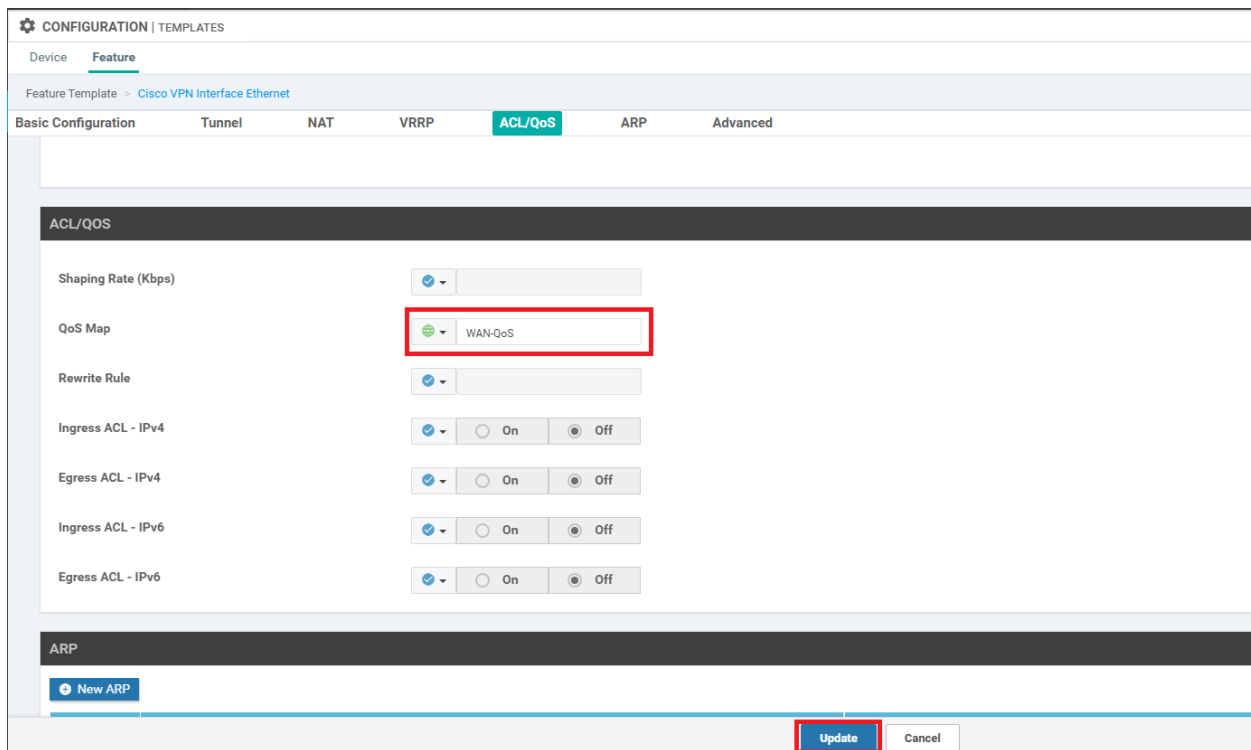
9. Click on **Next** and then **Configure Devices**. If you want, inspect the side-by-side configuration before clicking on **Configure Devices** and you will notice that the WAN-QoS Policy will be applied to GigabitEthernet2 (WAN VPN 0 Interface for INET)



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



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**



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.

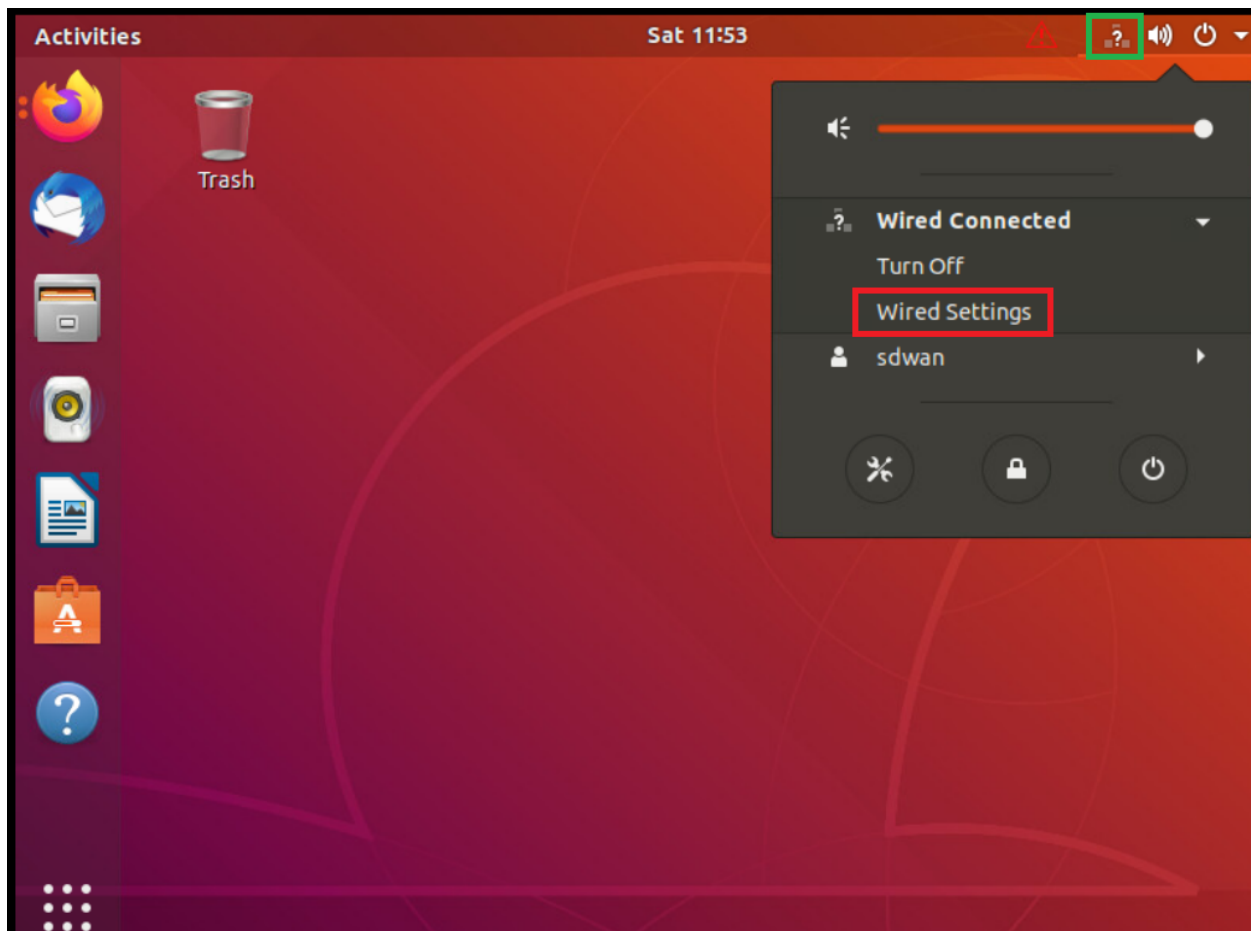
Task List

- [Create a Localized Policy](#)

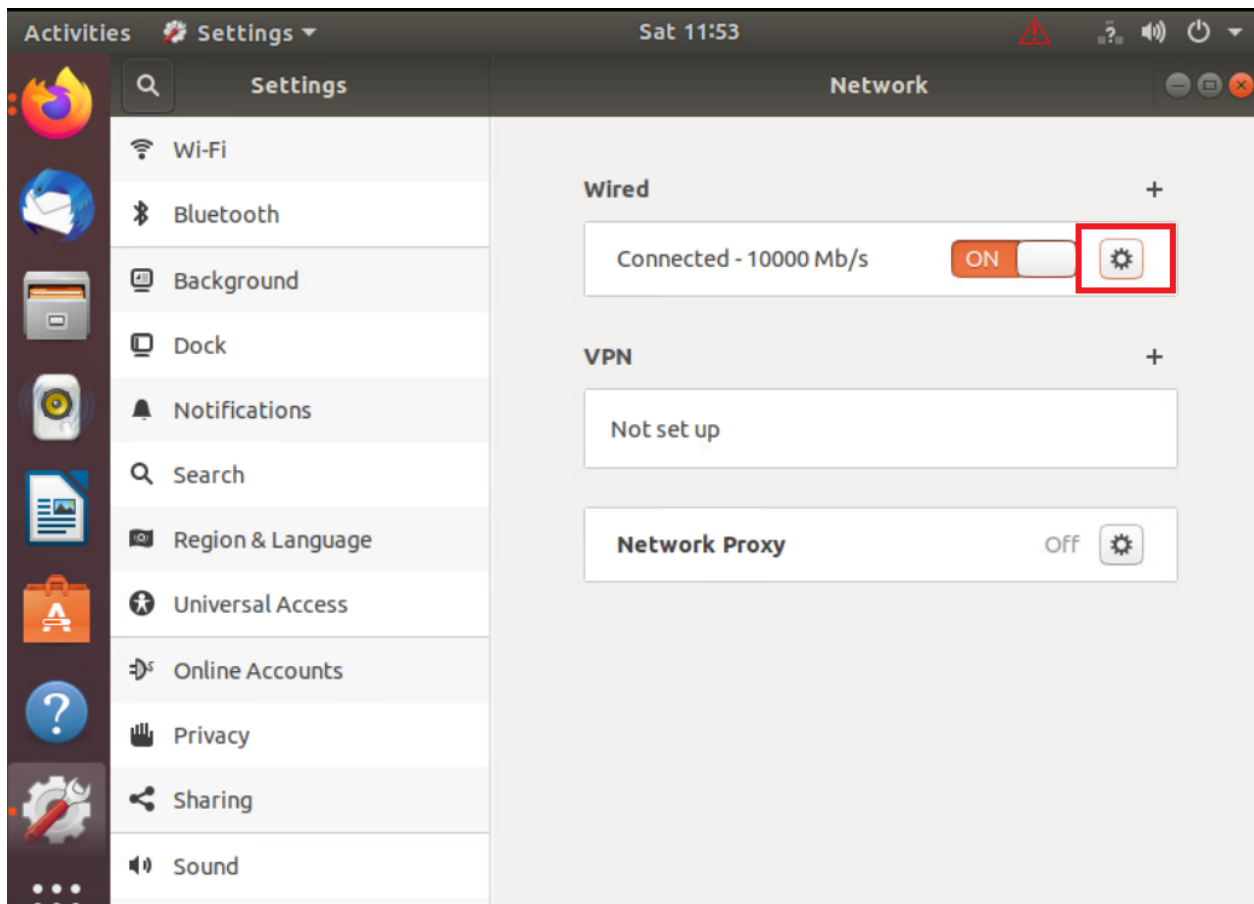
- Add a Class List and a QoS Map
- Configure the IPv4 AGL Policy
- Complete and apply the localized policy
- Apply the AGL and QoS Map
- Activity Verification

Activity Verification

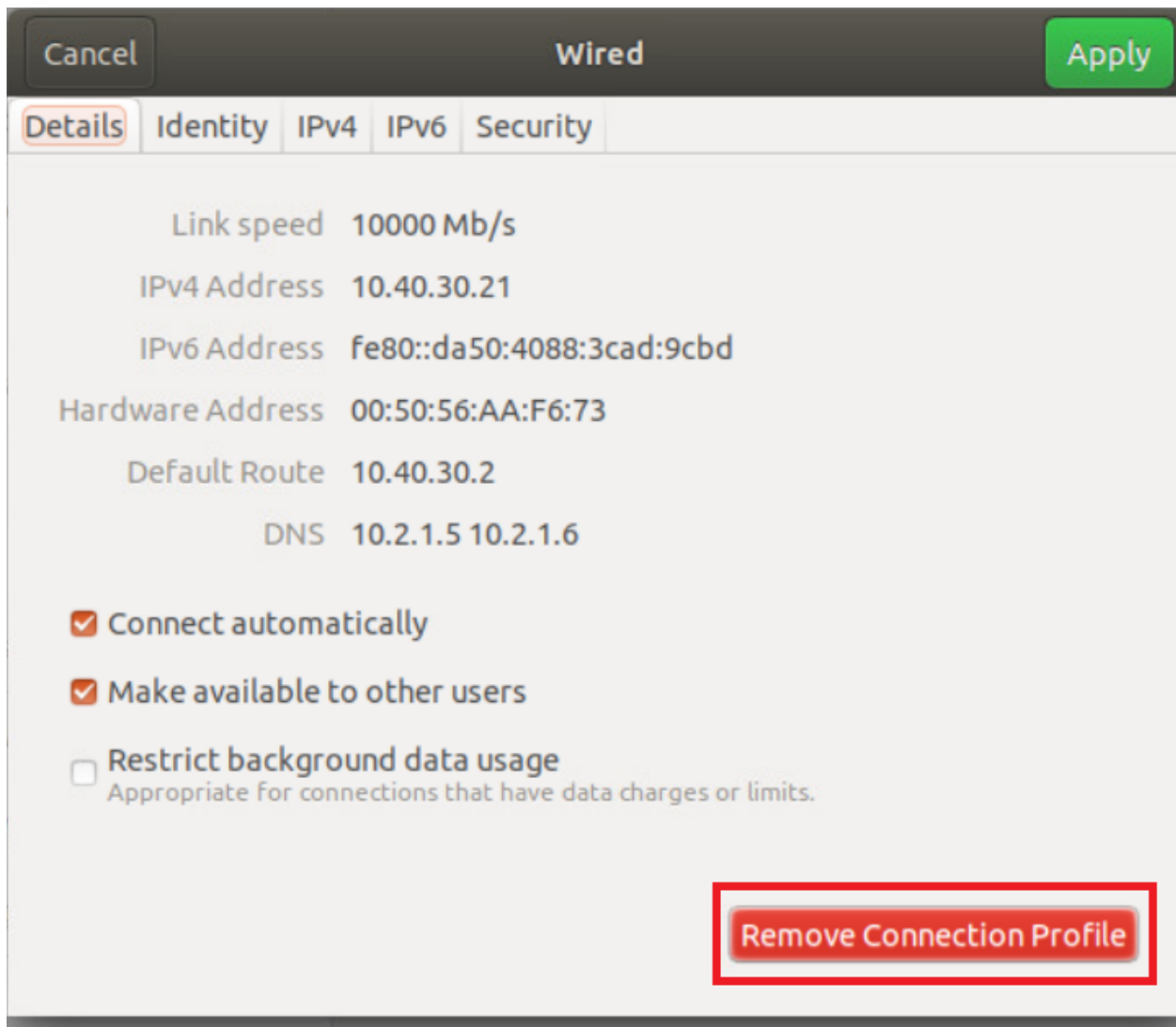
1. Log in to vCenter (use the bookmark or go to 10.2.1.50/ui) using the credentials provided to you. Locate the sdwan-
slc/ghi-site40pc-podX VM and click on it. Open the Web Console to the Site 40 PC VM and log in. The Username is
sdwan and the password is C1sco12345. Click the network icon in the top-right corner and go to Wired Settings



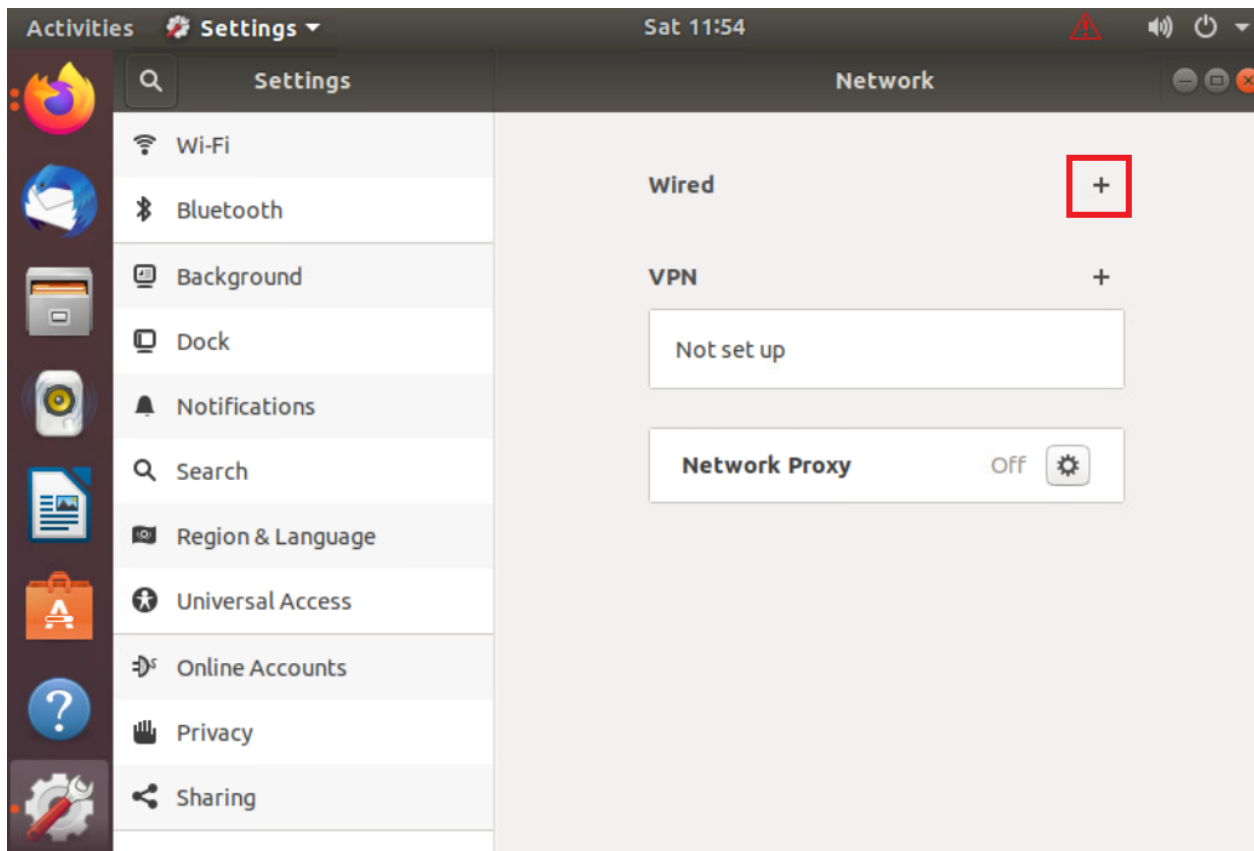
2. Click on the cog wheel/gear icon



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).

Cancel **New Profile** Add

Identity IPv4 IPv6 Security

IPv4 Method Automatic (DHCP) Link-Local Only
 Manual Disable

Addresses

Address	Netmask	Gateway	
10.40.10.21	255.255.255.0	10.40.10.2	✕
			✕

DNS Automatic OFF

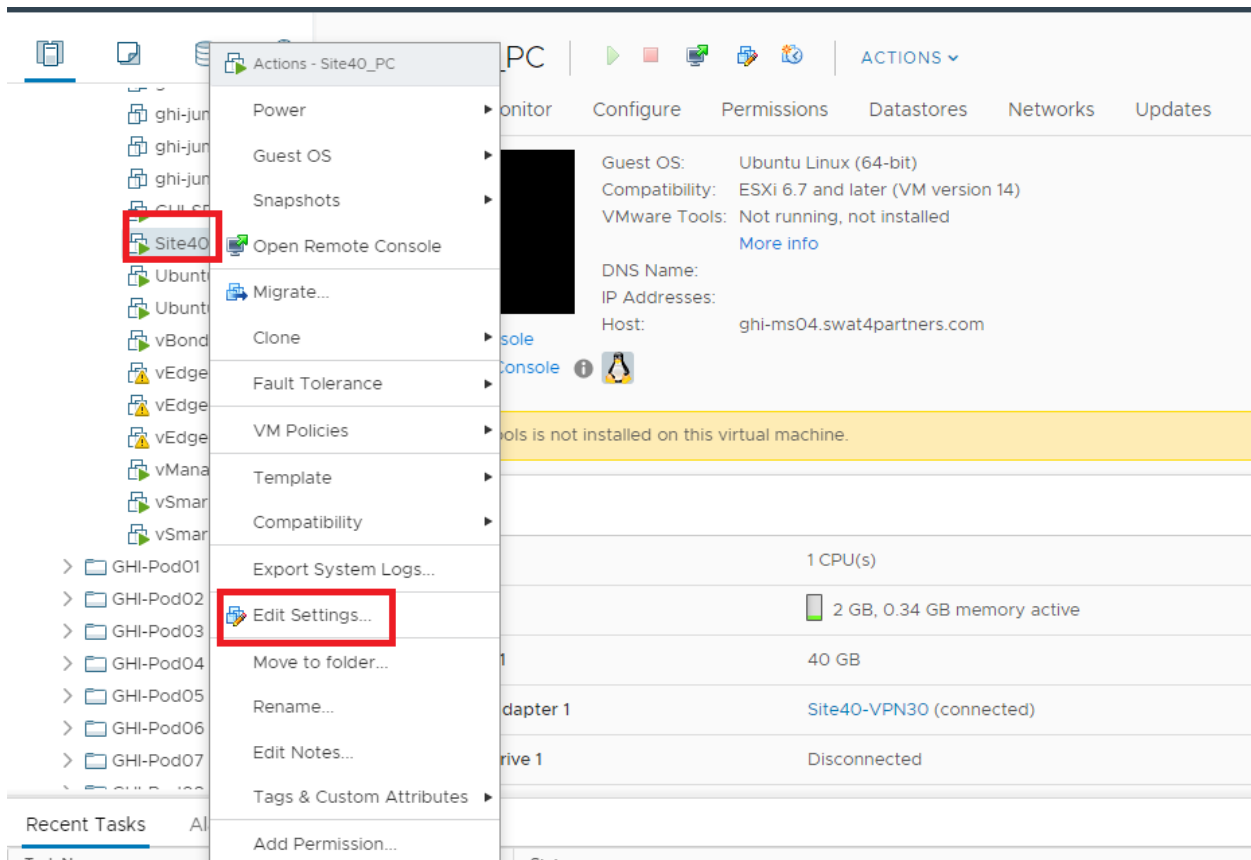
10.2.1.5, 10.2.1.6

Separate IP addresses with commas

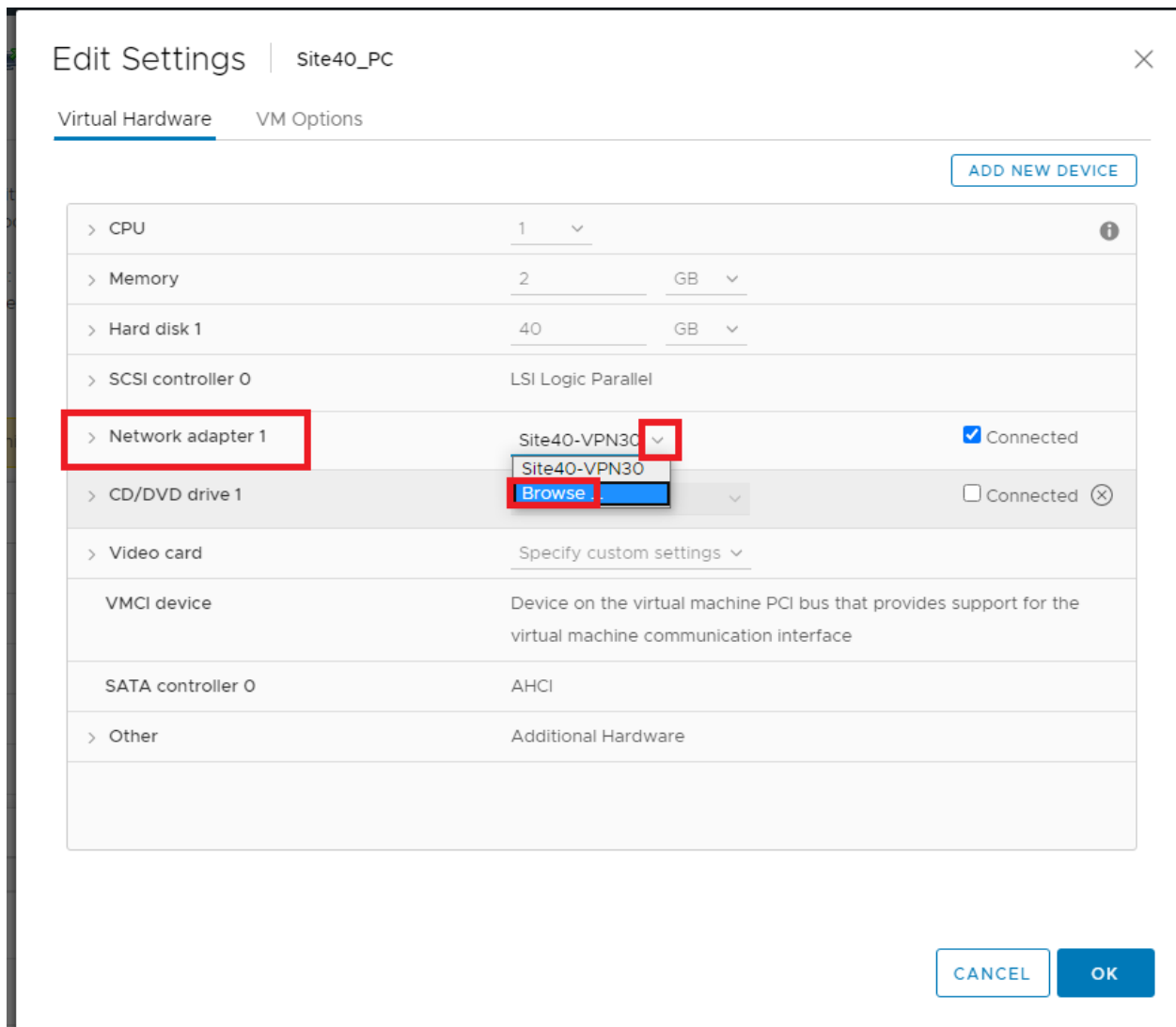
Routes Automatic ON

Address	Netmask	Gateway	Metric	
				✕

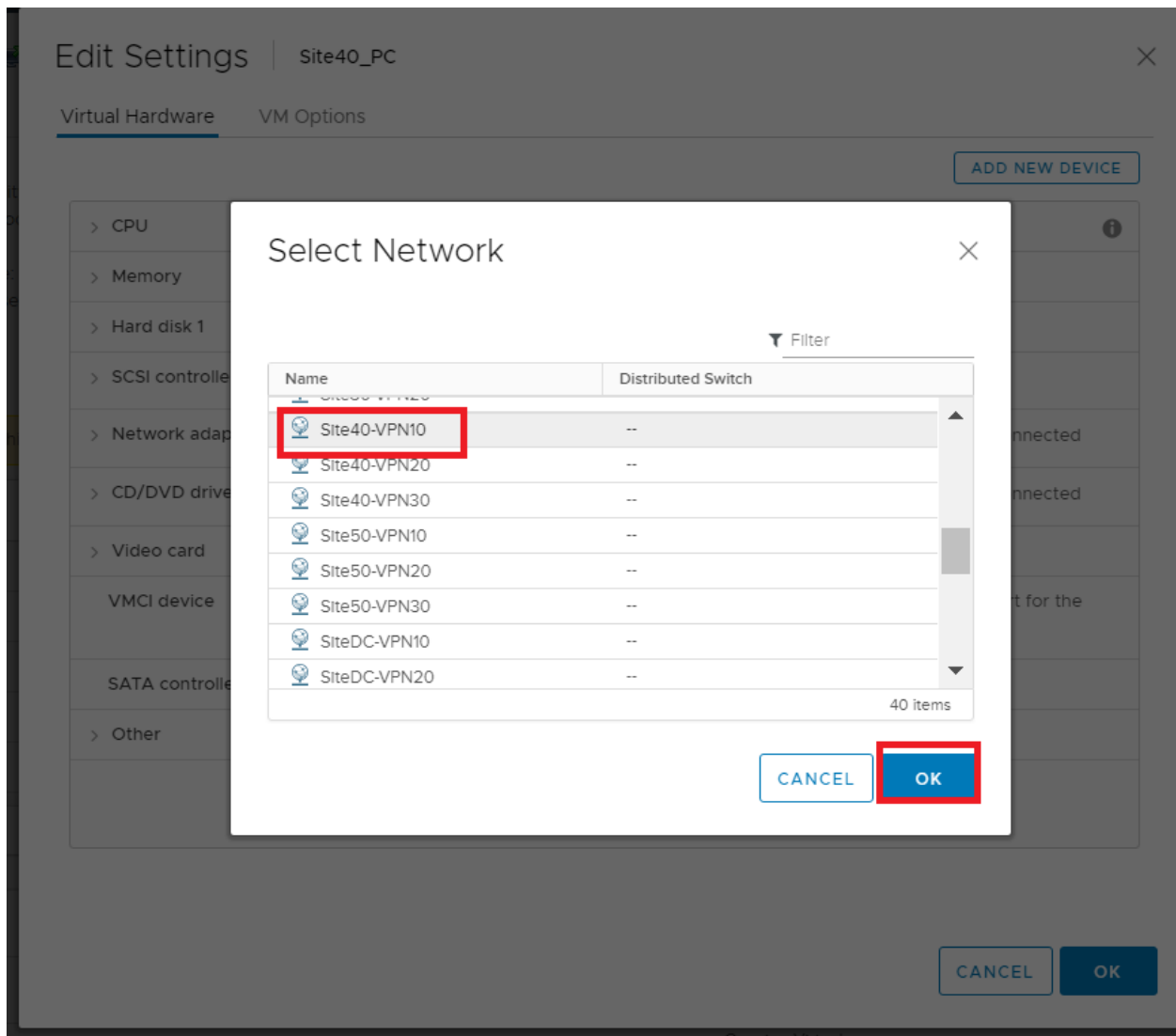
6. Back at the vCenter screen, right click on the Site40PC (named sdwan-slc/ghi-site40pc-podX) for your POD and click on **Edit Settings** (image as an example only)



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.



- 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 pkts/bytes	Random drop pkts/bytes	Tail drop 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
class Transmitted Random drop Tail drop Minimum Maximum Mark
pkts/bytes pkts/bytes pkts/bytes thresh thresh 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 AGL Policy
 - Complete and apply the localized policy
- Apply the AGL 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



Dynamic On-Demand Tunnels

Summary: Configuring Dynamic On-Demand Tunnels between Site 30 and Site 40 with DC as the backup route

Table of Contents

- [Overview](#)
- [Exploring the current setup](#)
- [Configuring a Control Policy for Dynamic Tunnels](#)
- [Configuring OMP Templates](#)
- [Enabling Dynamic Tunnels](#)
- [Activity Verification](#)

Task List

- Overview
- Exploring the current setup
- Configuring a Control Policy for Dynamic Tunnels
- Configuring OMP Templates
- Enabling Dynamic Tunnels
- Activity Verification

Overview

IPSEC tunnels are established between TLOCs in a full mesh fashion between devices in the SD-WAN overlay. This leads to multiple, potentially idle tunnels remaining up between sites and an overhead of traffic traversing the WAN links (due to BFD).

With version 20.3 of vManage, Cisco SD-WAN allows the creation of on-demand tunnels between sites - i.e. tunnels will only be set up when there is traffic traversing the sites.

The following configuration components come into play when setting up Dynamic On-Demand Tunnels:

- Control Policies
- OMP Templates (max path and ECMP limits)
- System Templates (for configuring Dynamic Tunnels)

We will set up Dynamic On-Demand Tunnels between vEdge30 and cEdge40 with the DC-vEdges functioning as backup forwarding nodes.

Task List

- [Overview](#)
- [Exploring the current setup](#)
- [Configuring a Control Policy for Dynamic Tunnels](#)
- [Configuring OMP Templates](#)
- [Enabling Dynamic Tunnels](#)
- [Activity Verification](#)

Exploring the current setup

1. Open a CLI session to vEdge30 using the saved session in Putty (or SSH to 192.168.0.30). Log in via the credentials mentioned below and enter the command `show omp tlocs | tab`. Notice that TLOC routes learnt from cEdge40 are Chosen, Installed and Resolved (C,I,R) or Chosen, Resolved (C,R)

Username	Password
admin	admin

```
vEdge30# show omp tlocs | tab
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
S -> stale
Ext -> extranet
Stg -> staged
IA -> On-demand inactive
Inv -> invalid
```

ADDRESS FAMILY	TLOC IP	COLOR	ENCAP	FROM PEER	STATUS	PSEUDO KEY	PUBLIC IP	PUBLIC PORT	PRIVATE IP
ipv4	10.255.255.11	mpls	ipsec	10.255.255.3	C,I,R	1	192.0.2.2	12346	192.0.2.2
				10.255.255.4	C,R	1	192.0.2.2	12346	192.0.2.2
	10.255.255.11	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.10	12346	100.100.100.10
				10.255.255.4	C,R	1	100.100.100.10	12346	100.100.100.10
	10.255.255.12	mpls	ipsec	10.255.255.3	C,I,R	1	192.0.2.6	12346	192.0.2.6
				10.255.255.4	C,R	1	192.0.2.6	12346	192.0.2.6
	10.255.255.12	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.11	12346	100.100.100.11
				10.255.255.4	C,R	1	100.100.100.11	12346	100.100.100.11
	10.255.255.21	mpls	ipsec	10.255.255.3	C,I,R	1	192.168.26.20	12346	192.168.26.20
				10.255.255.4	C,R	1	192.168.26.20	12346	192.168.26.20
	10.255.255.21	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.20	12366	100.100.100.20
				10.255.255.4	C,R	1	100.100.100.20	12366	100.100.100.20
	10.255.255.22	mpls	ipsec	10.255.255.3	C,I,R	1	192.0.2.10	12366	192.0.2.10
				10.255.255.4	C,R	1	192.0.2.10	12366	192.0.2.10
	10.255.255.22	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.20	56264	192.168.25.21
				10.255.255.4	C,R	1	100.100.100.20	56264	192.168.25.21
	10.255.255.31	mpls	ipsec	0.0.0.0	C,Red,R	1	192.0.2.14	12346	192.0.2.14
				0.0.0.0	C,Red,R	1	100.100.100.30	12346	100.100.100.30
	10.255.255.41	mpls	ipsec	10.255.255.3	C,I,R	1	192.1.2.18	12347	192.1.2.18
				10.255.255.4	C,R	1	192.1.2.18	12347	192.1.2.18
	10.255.255.41	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.40	12347	100.100.100.40
				10.255.255.4	C,R	1	100.100.100.40	12347	100.100.100.40
	10.255.255.51	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.50	12367	100.100.100.50
				10.255.255.4	C,R	1	100.100.100.50	12367	100.100.100.50
	10.255.255.52	mpls	ipsec	10.255.255.3	C,I,R	1	192.1.2.22	12367	192.1.2.22
				10.255.255.4	C,R	1	192.1.2.22	12367	192.1.2.22

```
show omp tlocs | tab
```

- Log in to cEdge40 via the saved session in Putty (or SSH to 192.168.0.40). Use the same credentials as above and enter the command `show sdwan omp tlocs`. Look for the TLOC route entries for 10.255.255.31 (vEdge30) and these are also Chosen, Installed and Resolved (C,I,R) or Chosen, Resolved (C,R)


```
-----  
tloc entries for 10.255.255.31  
      mpls  
      ipsec  
-----
```

```
      RECEIVED FROM:  
peer          10.255.255.3  
status        C,I,R  
loss-reason   not set  
lost-to-peer  not set  
lost-to-path-id not set  
  Attributes:  
    attribute-type  installed  
    encap-key       not set  
    encap-proto     0  
    encap-spi       258  
    encap-auth      sha1-hmac,ah-sha1-hmac  
    encap-encrypt   aes256  
    public-ip       192.0.2.14  
    public-port     12346  
    private-ip      192.0.2.14  
    private-port    12346
```

```
      RECEIVED FROM:  
peer          10.255.255.4  
status        C,R  
loss-reason   not set  
lost-to-peer  not set  
lost-to-path-id not set  
  Attributes:  
    attribute-type  installed  
    encap-key       not set  
    encap-proto     0  
    encap-spi       258  
    encap-auth      sha1-hmac,ah-sha1-hmac  
    encap-encrypt   aes256  
    public-ip       192.0.2.14  
    public-port     12346
```

```
private-ip      192.0.2.14
private-port    12346
```

```
-----  
tloc entries for 10.255.255.31  
      public-internet  
      ipsec  
-----
```

RECEIVED FROM:

```
peer      10.255.255.3  
status    C,I,R  
loss-reason  not set  
lost-to-peer  not set  
lost-to-path-id not set
```

Attributes:

```
  attribute-type  installed  
  encap-key       not set  
  encap-proto     0  
  encap-spi       258  
  encap-auth      sha1-hmac,ah-sha1-hmac  
  encap-encrypt   aes256  
  public-ip       100.100.100.30  
  public-port     12346  
  private-ip      100.100.100.30  
  private-port    12346
```



```
RECEIVED FROM:
peer          10.255.255.4
status        C,R
loss-reason   not set
lost-to-peer  not set
lost-to-path-id not set
Attributes:
  attribute-type installed
  encap-key     not set
  encap-proto   0
  encap-spi     258
  encap-auth    sha1-hmac,ah-sha1-hmac
  encap-encrypt aes256
  public-ip     100.100.100.30
  public-port   12346
  private-ip    100.100.100.30
  private-port  12346
```

```
show sdwan omp tlocs
```

3. Back at vEdge30, check the OMP routes for VPN 10 and VPN 20 subnets behind cEdge40. Run the commands `show omp routes 10.40.10.0/24` and `show omp routes 10.40.20.0/24`. vEdge30 routes traffic for the subnets directly to cEdge40 (normal full mesh operation of SD-WAN)

```
vEdge30# show omp routes 10.40.10.0/24
```

```
Code:
```

```
C -> chosen  
I -> installed  
Red -> redistributed  
Rej -> rejected  
L -> looped  
R -> resolved  
S -> stale  
Ext -> extranet  
Inv -> invalid  
Stg -> staged  
IA -> On-demand inactive  
U -> TLOC unresolved
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
10	10.40.10.0/24	10.255.255.3	66	1002	C,I,R	installed	10.255.255.41	public-internet
		10.255.255.3	88	1002	C,I,R	installed	10.255.255.41	mpls
		10.255.255.4	108	1002	C,R	installed	10.255.255.41	mpls
		10.255.255.4	109	1002	C,R	installed	10.255.255.41	public-internet

```
vEdge30# show omp routes 10.40.20.0/24
```

```
Code:
```

```
C -> chosen  
I -> installed  
Red -> redistributed  
Rej -> rejected  
L -> looped  
R -> resolved  
S -> stale  
Ext -> extranet  
Inv -> invalid  
Stg -> staged  
IA -> On-demand inactive  
U -> TLOC unresolved
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
20	10.40.20.0/24	10.255.255.3	65	1003	C,I,R	installed	10.255.255.41	public-internet
		10.255.255.3	87	1003	C,I,R	installed	10.255.255.41	mpls
		10.255.255.4	110	1003	C,R	installed	10.255.255.41	mpls
		10.255.255.4	111	1003	C,R	installed	10.255.255.41	public-internet

```
show omp routes 10.40.10.0/24
show omp routes 10.40.20.0/24
```

4. Similarly, cEdge40 routes traffic for the vEdge30 VPN 10 and VPN 20 subnets directly to vEdge30. Run the commands `show sdwan omp routes 10.30.10.0/24` and `show sdwan omp routes 10.30.20.0/24` on cEdge40

```
cEdge40#show sdwan omp routes 10.30.10.0/24
```

```
Code:
```

```
C -> chosen  
I -> installed  
Red -> redistributed  
Rej -> rejected  
L -> looped  
R -> resolved  
S -> stale  
Ext -> extranet  
Inv -> invalid  
Stg -> staged  
IA -> On-demand inactive  
U -> TLOC unresolved
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
10	10.30.10.0/24	10.255.255.3	57	1003	C,I,R	installed	10.255.255.31	mpls
		10.255.255.3	58	1003	C,I,R	installed	10.255.255.31	public-internet
		10.255.255.4	57	1003	C,R	installed	10.255.255.31	mpls
		10.255.255.4	58	1003	C,R	installed	10.255.255.31	public-internet

```
cEdge40#show sdwan omp routes 10.30.20.0/24
```

```
Code:
```

```
C -> chosen  
I -> installed  
Red -> redistributed  
Rej -> rejected  
L -> looped  
R -> resolved  
S -> stale  
Ext -> extranet  
Inv -> invalid  
Stg -> staged  
IA -> On-demand inactive  
U -> TLOC unresolved
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
20	10.30.20.0/24	10.255.255.3	55	1004	C,I,R	installed	10.255.255.31	mpls
		10.255.255.3	56	1004	C,I,R	installed	10.255.255.31	public-internet
		10.255.255.4	55	1004	C,R	installed	10.255.255.31	mpls
		10.255.255.4	56	1004	C,R	installed	10.255.255.31	public-internet

```
--More--
```

```
show sdwan omp routes 10.30.10.0/24
show sdwan omp routes 10.30.20.0/24
```

Task List

- [Overview](#)
- [Exploring the current setup](#)
- [Configuring a Control Policy for Dynamic Tunnels](#)
- [Configuring OMP Templates](#)
- [Enabling Dynamic Tunnels](#)
- [Activity Verification](#)

Configuring a Control Policy for Dynamic Tunnels

1. On the vManage GUI, navigate to **Configuration => Policies**

Cisco vManage

DASHBOARD | MAIN DASHBOARD

Smart - 2

WAN Edge - 8

Configuration

Devices

TLS/SSL Proxy

Certificates

Network Design

Templates

Policies

Security

Unified Communications

Cloud onRamp for SaaS

Cloud onRamp for IaaS

Cloud OnRamp for Multi-Cloud

Cloud OnRamp for Colocation

Site Health (Total 5)

- Full WAN Connectivity
- Partial WAN Connectivity
- No WAN Connectivity

WAN Edge Health (Total 8)

8

Normal

Application-Aware Routing

Tunnel Endpoints

- DC-vEdge1:public-internet-vEdg
- vEdge21:public-internet-DC-vEc

Smart - 2	2 ↑
WAN Edge - 8	8 ↑
TLS/SSL Proxy	10
Certificates	0
Network Design	0
Security	20
Unified Communications	20
Cloud onRamp for SaaS	8
Cloud onRamp for IaaS	0

2. We will create a new policy for Dynamic On-Demand Tunnels. Click on **Add Policy**

Centralized Policy

Localized Policy

A blue button with a white plus sign icon and the text "Add Policy". The button is highlighted with a red rectangular border.

Search Options ▾

Name	Description	Type
Hub-n-Spoke-VPN20-only	Hub and Spoke policy for VPN 20 only	UI Policy Builder
Site40-Guest-DIA	DIA Policy for Site 40 Guests	UI Policy Builder
traffic-engineering-ftp	Traffic Engineering for FTP	UI Policy Builder
Site20-Regional-Hub-Site30	Regional Policy for Site 20 to Site 30	UI Policy Builder
AAR-VPN10	Transport Preference for VPN 10	UI Policy Builder

3. Click on **Site** and then on **New Site List** to create a New Site List

Select a list type on the left and start creating your groups of interest

Application

Color

Data Prefix

Policer

Prefix

Site

SLA Class

TLOC

VPN

+ New Site List

Name	Entries	Referenc
Site30	30	2
Branches	20, 30, 40, 50	3
Fabric	1, 40, 50	1
Site20	20	2
Site40	40	1
DC	1	1

4. Name the Site List *Site30_40* and enter *30,40* in the Add Site field. Click on **Add**

+ New Site List

Site List Name













Site30_40

Add Site

30,40

Add

Cancel

Name	Entries	Reference Count	Updated By	Last Updated	Action
Site30	30	2	admin	25 Aug 2020 6:02:15 AM ...	  
Branches	20, 30, 40, 50	3	admin	25 Aug 2020 6:01:57 AM ...	  
Fabric	1, 40, 50	1	admin	26 Aug 2020 3:19:55 AM ...	  
Site20	20	2	admin	26 Aug 2020 3:20:10 AM ...	  

Next

CANCEL

5. Make sure the Site List looks like the image below and click on **Next**

Name	Entries	Reference Count	Updated By	Last Updated
Site30	30	2	admin	25 Aug 2020 6:02:15 AM ...
Branches	20, 30, 40, 50	3	admin	25 Aug 2020 6:01:57 AM ...
Site30_40	30, 40	0	admin	06 Dec 2020 3:04:15 PM ...
Fabric	1, 40, 50	1	admin	26 Aug 2020 3:19:55 AM ...
Site20	20	2	admin	26 Aug 2020 3:20:10 AM ...
Site40	40	1	admin	25 Aug 2020 6:02:20 AM ...
DC	1	1	admin	25 Aug 2020 6:02:09 AM ...

Next CANCEL

6. Click on **Add Topology** and then on **Custom Control (Route & TLOC)** to create a new control policy

Specify your network topology

Topology VPN Membership

+ Add Topology ▾

- Hub-and-Spoke
- Mesh
- Custom Control (Route & TLOC)
- Import Existing Topology

Search Options ▾

	Description	Reference Count
No data available		

7. Give the control policy a **Name** of *site30-40-dynamic-tunnels* and a **Description** of *Dynamic Tunnels between Site 30 and 40 with DC as a backup*. Click on **Sequence Type** and choose **Route**

CONFIGURATION | POLICIES Add Custom Control Policy

Name site30-40-dynamic-tunnels

Description Dynamic Tunnels between Site 30 and 40 with DC as backup

Sequence Type

Drag & drop to reorder

Default Action

Reject

Add Control Policy

- Route
Create a policy to apply on a OMP
- TLOC
Create a policy to apply to TLOCs

8. Click on **Sequence Rule** and select **Site**. Populate the Site List *Site30_40* and click on **Actions**

Name: site30-40-dynamic-tunnels

Description: Dynamic Tunnels between Site 30 and 40 with DC as backup

Sequence Type: Route **1**

Sequence Rule: Drag and drop to re-arrange rules

Match: Actions **4**

Protocol: IPv4

Color List OMP Tag Origin Originator Preference **Site** **2** TLOC VPN VPN Prefix List

Match Conditions

Site List **3**

Site30_40 x

Actions

Reject Enabled

9. Set the Action to **Accept** and click on **TLOC Action** and **TLOC**. Populate TLOC Action as *Backup* and the TLOC List as *DC-TLOCs*. Click on **Save Match and Actions**

Route Ro

Sequence Rule Drag and drop to re-arrange rules

Match Conditions

Site List ×

Site30_40 ×

Site ID ×

0-4294967295

Actions

Accept Enabled

TLOC Action ×

Backup ×

TLOC List ×

DC-TLOCs ×

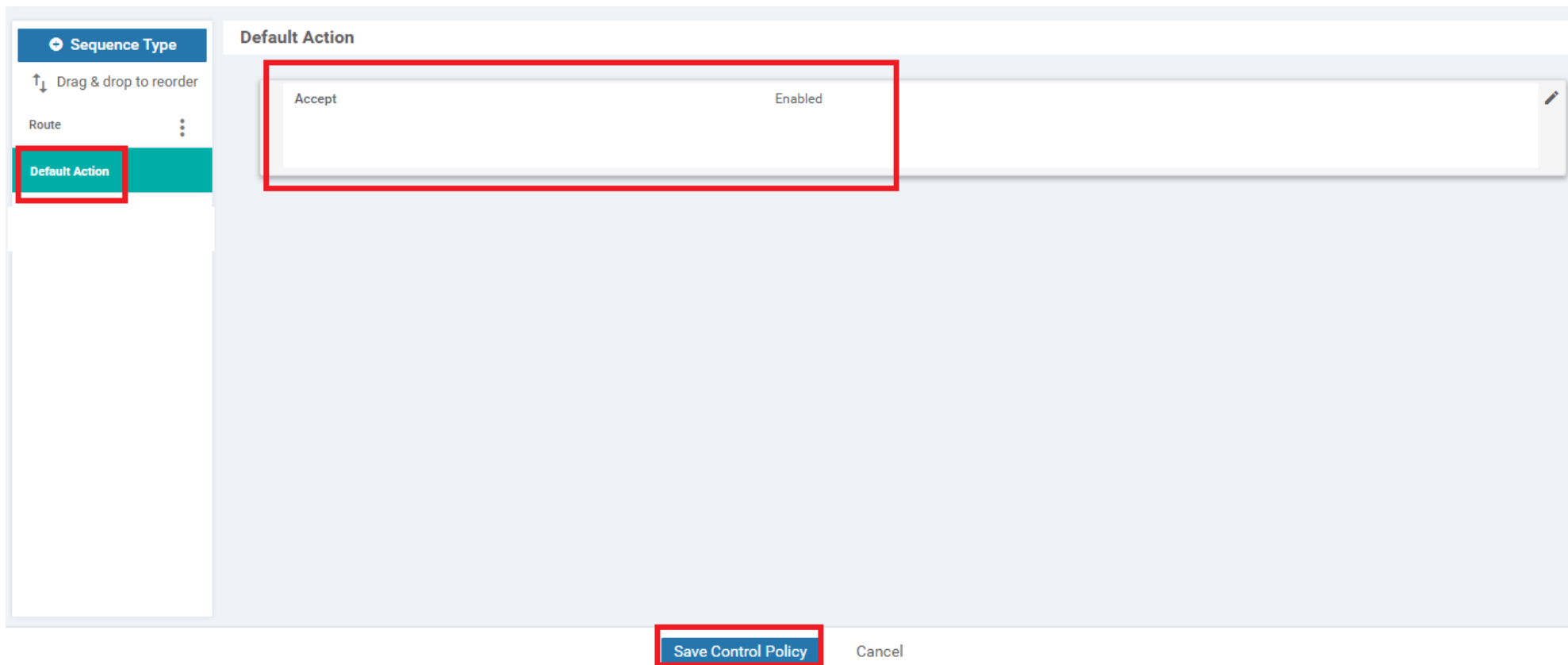
TLOC IP Example: 10.0.0.1

Color Select a color list

Encapsulation Select an encap

Save Match And Actions Cancel

- Click on **Default Action** and then the pencil icon to change the default of Reject Enabled to Accept Enabled. Click on Accept and choose to Save. Make sure the Default Action is set to Accept Enabled and click on **Save Control Policy**



11. Click **Next** till you're at the **Apply Policies to Sites and VPNs** tab and give the policy a Name of *Dynamic-Tunnels-Site30_40* with a Description of *Dynamic Tunnels between Site 30 and Site 40*. Under **Topology**, click on **New Site List** for the *site30-40-dynamic-tunnels* policy and choose the **Site30_40** Site List under **Outbound Site List**. Click on **Add** and then click on **Preview** to view the CLI output of the policy

Add policies to sites and VPNs

Policy Name **1**

Policy Description

Topology Application-Aware Routing Traffic Data Cflowd

site30-40-dynamic-tunnels CUSTOM CONTROL

+ New Site List **2**

Inbound Site List

Outbound Site List
 3 **4**

Add Cancel

Direction	Site List	Action
-----------	-----------	--------

BACK


```

viptela-policy:policy
control-policy site30-40-dynamic-tunnels
sequence 1
match route
site-list Site30_40
prefix-list _AnyIpv4PrefixList
!
action accept
set
tloc-action backup
tloc-list DC-TLOCs
!
!
!
default-action accept
!
lists
site-list Site30_40
site-id 30
site-id 40
!
tloc-list DC-TLOCs
tloc 10.255.255.11 color public-internet encap ipsec
tloc 10.255.255.11 color mpls encap ipsec
tloc 10.255.255.12 color public-internet encap ipsec
tloc 10.255.255.12 color mpls encap ipsec
!
prefix-list _AnyIpv4PrefixList
ip-prefix 0.0.0.0/0 le 32
!
!
!
apply-policy
site-list Site30_40
control-policy site30-40-dynamic-tunnels out
!
!

```

12. We will notice that the control policy is setting the TLOC of Site 30 and Site 40 OMP Routes to the *DC-TLOCs* TLOC list. It is also setting a **tloc-action backup** to populate the *ultimate tloc* value in the OMP route, pointing to the other site TLOC (rather than punting traffic out the DC-TLOCs). Click on **Save Policy**

This completes the Control Policy required for Dynamic On-Demand Tunnels.

Task List

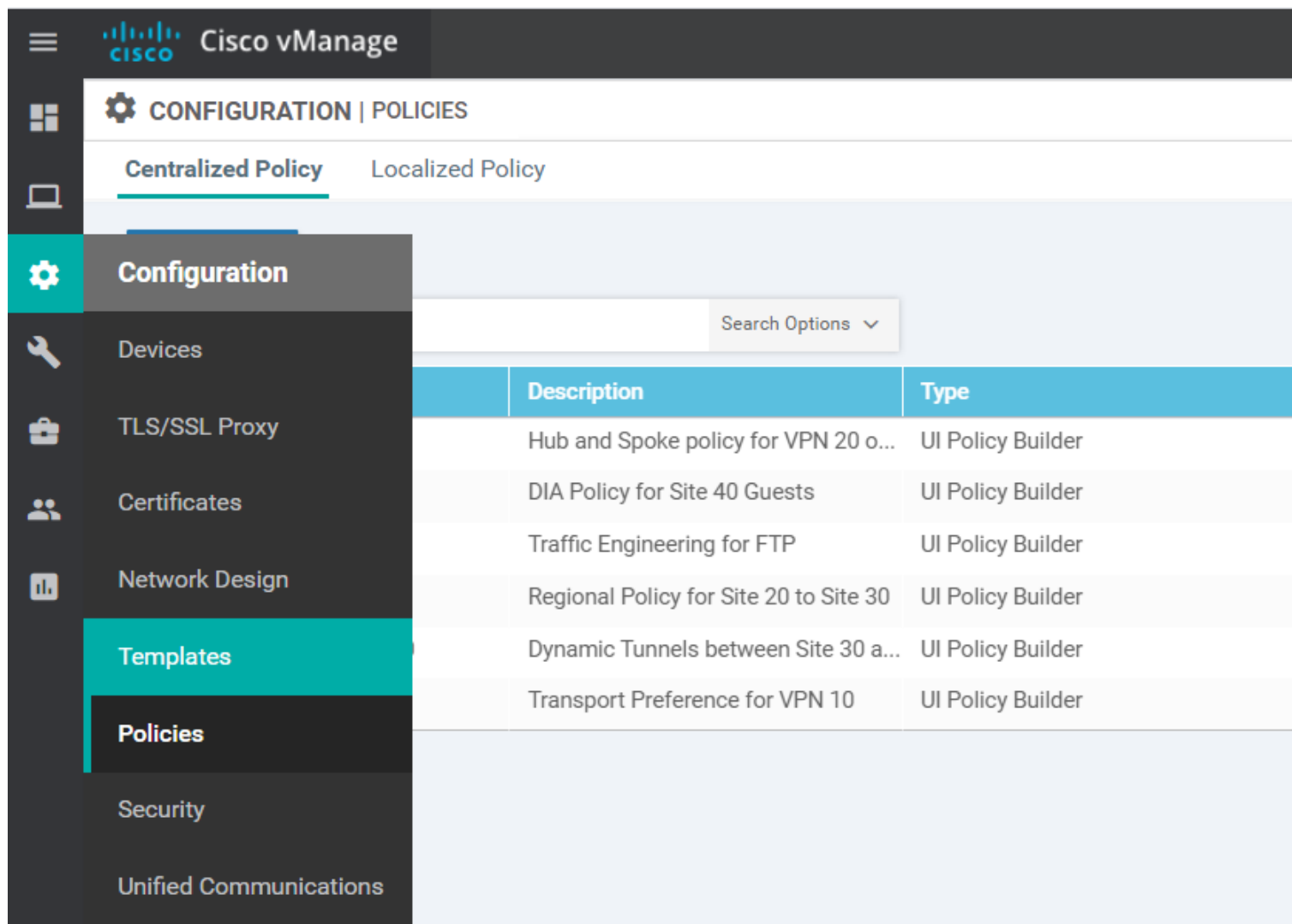
- [Overview](#)
- [Exploring the current setup](#)
- [Configuring a Control Policy for Dynamic Tunnels](#)
- [Configuring OMP Templates](#)

- Enabling Dynamic Tunnels
- Activity Verification

Configuring OMP Templates

We will be applying OMP Templates to the vSmarts and the WAN Edges at Site 30 and Site 40.

1. On the vManage GUI, go to **Configuration => Templates**



The screenshot shows the Cisco vManage interface. The top navigation bar includes the Cisco logo and the text "Cisco vManage". Below this, the main navigation area is titled "CONFIGURATION | POLICIES". There are two tabs: "Centralized Policy" (selected) and "Localized Policy". A left-hand sidebar menu is open, showing various configuration categories: Configuration (selected), Devices, TLS/SSL Proxy, Certificates, Network Design, Templates (highlighted), Policies, Security, and Unified Communications. The main content area displays a table of policies. A search bar with "Search Options" is visible above the table. The table has three columns: "Description" and "Type".

Description	Type
Hub and Spoke policy for VPN 20 o...	UI Policy Builder
DIA Policy for Site 40 Guests	UI Policy Builder
Traffic Engineering for FTP	UI Policy Builder
Regional Policy for Site 20 to Site 30	UI Policy Builder
Dynamic Tunnels between Site 30 a...	UI Policy Builder
Transport Preference for VPN 10	UI Policy Builder

2. Click on the **Feature** tab and then click on **Add Template**

The screenshot shows the 'CONFIGURATION | TEMPLATES' interface. At the top, there are two tabs: 'Device' and 'Feature'. The 'Feature' tab is selected and highlighted with a red box. Below the tabs, there is a blue button with a plus sign and the text 'Add Template', also highlighted with a red box. To the right of the button, there is a dropdown menu for 'Template Type' set to 'Non-Default' and a search bar with a magnifying glass icon. Below these elements is a table with the following columns: Name, Description, Type, and Device Model.

Name	Description	Type	Device Model
cedge-vpn20	VPN 20 Template for the c...	Cisco VPN	CSR1000v
DC-OSPF	OSPF Template for the DC	OSPF	vEdge Cloud
cEdge_VPN0_singl...	cEdge VPN 0 Template for ...	Cisco VPN	CSR1000v
cedge-vpn0-int-single	cedge VPN 0 Interface Tem...	Cisco VPN Interfac...	CSR1000v
cedge-vpn0-int-dual...	cEdge VPN 0 Interface Tem...	Cisco VPN Interfac...	CSR1000v
cEdge_VPN512_sin...	cEdge VPN 512 Template f...	Cisco VPN	CSR1000v

3. Search for *vSmart* in the **Select Devices** section and select the vSmart Device. Click on **OMP** under Basic Configuration to start configuring an OMP Template for the vSmarts

Select Devices

vsmar

vSmart

Select Template

BASIC INFORMATION

AAA

Archive

NTP

OMP

Security

System

VPN

VPN

VPN Interface Ethernet

Management | WAN | LAN

4. Give the template a name of *vsmart-omp-dt* with a Description of *OMP modification for Dynamic Tunnels - vSmart*. Set the **Number of Paths Advertised per Prefix** to a Global value of 16 and click on **Save**

Device Type	vSmart
Template Name	vsmart-omp-dt
Description	OMP modification for Dynamic Tunnels - vSmart

Basic Configuration**Timers****BASIC CONFIGURATION**

Graceful Restart for OMP

 On Off

Graceful Restart Timer (seconds)



43200

Number of Paths Advertised per Prefix



16

Send Backup Paths

 On Off**Save**

Cancel

5. We will now apply this Feature Template to the vSmart Device Template. Go to the Device tab in Templates and locate the *vSmart-dev-temp* Device Template. Click on the three dots next to it and choose to **Edit** the template

Device Feature

[+ Create Template](#)

Template Type: Non-Default Search Options

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template	
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:3...	In Sync	...
cEdge-single...	Single Uplink cE...	Feature	CSR1000v	17	2	admin	24 Aug 2020 6:16...	In Sync	...
cedge_dualup...	cedge Device Te...	Feature	CSR1000v	19	1	admin	31 Aug 2020 3:06...	In Sync	...
DCvEdge_dev...	Device template ...	Feature	vEdge Cloud	16	2	admin	25 Aug 2020 6:00...	In Sync	...
vEdge30_dev...	Device template ...	Feature	vEdge Cloud	15	1	admin	24 Aug 2020 5:52...	In Sync	...
vSmart-dev-te...	Device Template...	Feature	vSmart	9	2	admin	24 Aug 2020 3:03...	In Sync	...
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:4...	In Sync	...

Edit

- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

6. Under **OMP**, set the template to *vsmart-omp-dt*. Click on **Update**. Click on **Next** and **Configure Devices**

Basic Information

Transport & Management VPN

Additional Templates

Logging*

Factory_Default_Logging_Template_V01

- + Archive
- + NTP

AAA *

Factory_Default_AAA_Template

OMP *

vsmart-omp-dt

Security *

Factory_Default_vSmart_vManage_Security_...

Transport & Management VPN

VPN 0 *

vSmart-VPN0

Additional VPN 0 Templat

VPN Interface

vSmart-VPN0-Int

- + VPN Interface

Update

Cancel

S...	Chassis Number	System IP	Hostname	IPv4 Address(vpn512_if_ip_address)	IPv4 Address(vpn512_if_ip_address)
✓	7c8a0e49-5557-45e0-a8cb-d7ff63f33d6b	10.255.255.3	vSmart	192.168.0.8/24	100.100.100.4/24
✓	c76f87e0-30a8-4205-b47d-40750e59bb1c	10.255.255.4	vSmart2	192.168.0.9/24	100.100.100.5/24

Next

Cancel

'Configure' action will be applied to 2 device(s) attached to 1 device template(s).

Device Template	Total
vSmart-dev-temp	1

Device list (Total: 2 devices)

Filter/Search

7c8a0e49-5557-45e0-a8cb-d7ff63f33d6b
vSmart|10.255.255.3

c76f87e0-30a8-4205-b47d-40750e59bb1c
vSmart2|10.255.255.4



Please select a device from the device list

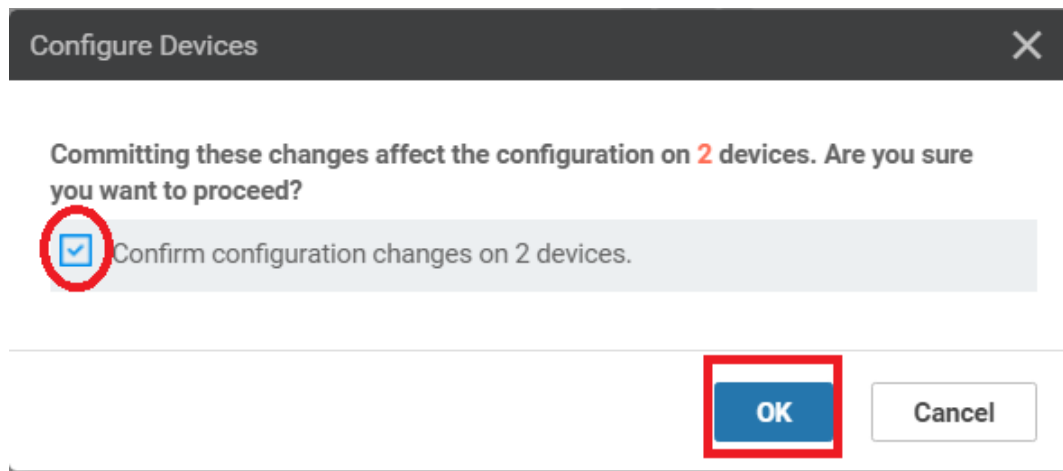
Configure Device Rollback Timer

Back

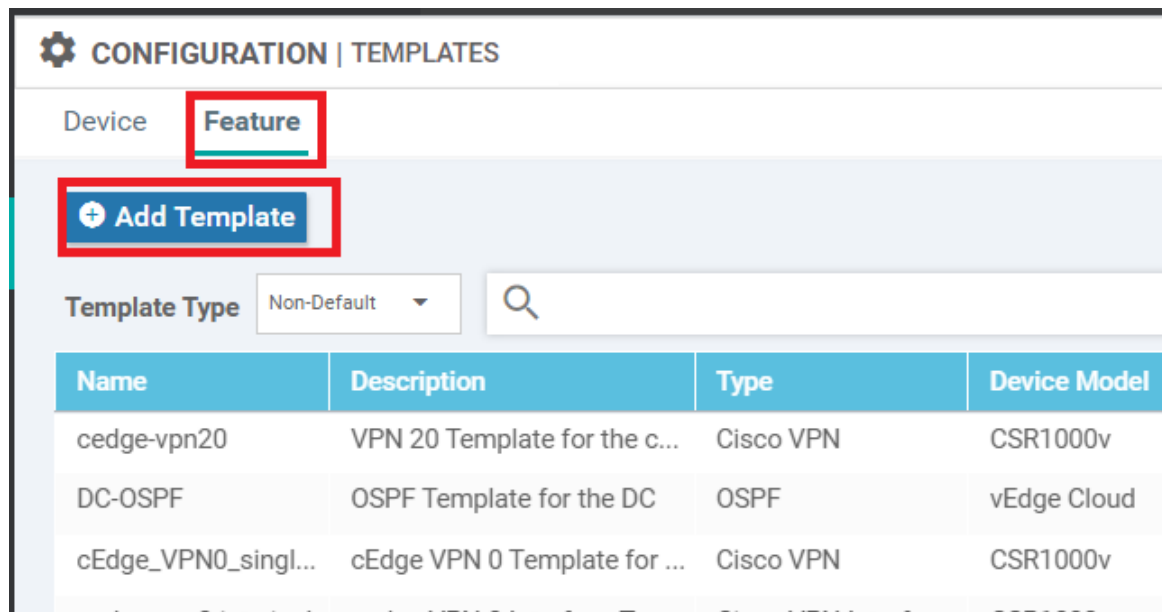
Configure Devices

Cancel

7. Confirm the configuration change and click on **OK**



8. Navigate to **Configuration => Templates => Feature Tab** and click on **Add Template**



9. Search for *vedge* and select **vEdge Cloud**. Click on **OMP**

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)

VPN

VI

10. Give the template a name of *vedge-omp-dt* with a Description of *OMP modification for Dynamic Tunnels - vEdge*. Set the **ECMP Limit** to a Global value of 16 and click on **Save**

Basic Configuration Timers Advertise

BASIC CONFIGURATION

Graceful Restart for OMP

On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown

Yes No

TIMERS

Save Cancel

11. Navigate to **Configuration => Templates => Feature Tab** and click on **Add Template**. Search for **csr** and select **CSR1000v**. Click on **Cisco OMP**

Device Feature

Feature Template > [Add Template](#)

Select Devices

 CSR1000v

Select Template

BASIC INFORMATION

Cisco AAA

Cisco BFD

Cisco NTP

Cisco OMP

Cisco Security

Cisco System

Global Settings

Security App Hosting

VPN

12. Give the template a name of *cedge-omp-dt* with a Description of *OMP modification for Dynamic Tunnels - cEdge*. Set the **ECMP Limit** to a Global value of 16 and click on **Save**

Device **Feature**

Feature Template > Add Template > Cisco OMP

Template Name	cedge-omp-dt
Description	OMP modification for Dynamic Tunnels - cEdge

Basic Configuration Timers Advertise

BASIC CONFIGURATION

Graceful Restart for OMP	<input checked="" type="checkbox"/> <input type="radio"/> On <input type="radio"/> Off
Overlay AS Number	<input checked="" type="checkbox"/> <input type="text"/>
Graceful Restart Timer (seconds)	<input checked="" type="checkbox"/> 43200
Number of Paths Advertised per Prefix	<input checked="" type="checkbox"/> 4
ECMP Limit	<input checked="" type="checkbox"/> 16

Save Cancel

13. We will now attach the OMP templates just created to **vEdge30** and **cEdge40**. Navigate to **Configuration => Templates**. While on the Device Tab, locate the *vEdge30_dev_temp* template and click on the three dots next to it. Choose to **Edit** the template

Device Feature

+ Create Template

Template Type Non-Default



Search Options

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:3...	In Sync
cEdge-single-...	Single Uplink cE...	Feature	CSR1000v	17	2	admin	24 Aug 2020 6:16...	In Sync
cedge_dualup...	cedge Device Te...	Feature	CSR1000v	19	1	admin	31 Aug 2020 3:06...	In Sync
DCvEdge_dev...	Device template ...	Feature	vEdge Cloud	16	2	admin	25 Aug 2020 6:00...	In Sync
vEdge30_dev...	Device template ...	Feature	vEdge Cloud	15	1	admin	24 Aug 2020 5:52...	In Sync
vSmart-dev-te...	Device Template...	Feature	vSmart	9	2	admin	06 Dec 2020 3:24...	In Sync
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:4...	In Sync

- Edit
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

14. Update the **OMP** template as *vedge-omp-dt* and click on **Update**. Click **Next** and **Configure Devices** to push the changes to vEdge30

Basic Information Transport & Management VPN Service VPN Additional Templates

Basic Information

System *	Factory_Default_vEdge_System_Template	Additional System Templates + Archive + NTP
Logging*	Factory_Default_Logging_Template_V01	
AAA	Factory_Default_AAA_Template	
BFD *	Factory_Default_BFD_Template_V01	
OMP *	vedge-omp-dt	
Security *	Factory_Default_vEdge_Security_Template_V...	

Transport & Management VPN

Update Cancel

15. Navigate to **Configuration => Templates**. While on the Device Tab, locate the *cEdge_dualuplink_devtemp* template and click on the three dots next to it. Choose to **Edit** the template

Device Feature

+ Create Template



Total Rows: 7

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:3...	In Sync	...
cEdge-single...	Single Uplink cE...	Feature	CSR1000v	17	2	admin	24 Aug 2020 6:16:...	In Sync	...
cedge_dualup...	cedge Device Te...	Feature	CSR1000v	19	1	admin	31 Aug 2020 3:06:...	In Sync	...
DCvEdge_dev...	Device template ...	Feature	vEdge Cloud	16	2	admin	25 Aug 2020 6:00:...	In Sync	
vEdge30_dev...	Device template ...	Feature	vEdge Cloud	15	1	admin	06 Dec 2020 3:33:...	In Sync	
vSmart-dev-te...	Device Template...	Feature	vSmart	9	2	admin	06 Dec 2020 3:24:...	In Sync	
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:4...	In Sync	

- Edit
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

16. Update the **Cisco OMP** template as *cedge-omp-dt* and click on **Update**. Click **Next** and **Configure Devices** to push the changes to cEdge40

Basic Information

Transport & Management VPN

Service VPN

Additional Templates

Cisco AAA

Factory_Default_AAA_CISCO_Template

Cisco BFD *

Default_BFD_Cisco_V01

Cisco OMP *

cedge-omp-dt

Cisco Security *

Default_Security_Cisco_V01

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

Update

Cancel

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

Device Template	Total
cedge_dualuplink_devtemp	1

Device list (Total: 1 devices)

CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2
cEdge40|10.255.255.41



Please select a device from the device list

[Configure Device Rollback Timer](#)

[Back](#) [Configure Devices](#) [Cancel](#)

This completes the configuration of our OMP Feature Templates for vEdge30 and cEdge40 to support Dynamic On-Demand Tunnels.

Task List

- [Overview](#)
- [Exploring the current setup](#)
- [Configuring a Control Policy for Dynamic Tunnels](#)
- [Configuring OMP Templates](#)
- [Enabling Dynamic Tunnels](#)
- [Activity Verification](#)

Enabling Dynamic Tunnels

We will now add some basic configuration on the DC-vEdges and enable Dynamic On-Demand Tunnels via System templates.

1. Navigate to **Configuration => Templates => Feature Tab** and locate the *DCvEdge-vpn0* Feature Template. Click on the three dots next to it and choose to **Edit** the template

The screenshot shows the 'CONFIGURATION | TEMPLATES' interface. The 'Feature' tab is active. A table lists various templates, with 'DCvEdge-vpn0' highlighted in yellow. A context menu is open over the 'DCvEdge-vpn0' row, showing options: View, Edit, Change Device Models, Delete, and Copy. The 'Edit' option is highlighted with a red box. The table has 9 columns: Name, Description, Type, Device Model, Device Templates, Devices Attached, Updated By, Last Updated, and an action column with three dots.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	
DC-OSPF	OSPF Template for the DC	OSPF	vEdge Cloud	1	2	admin	24 Aug 2020 6:04:1...	...
DC-vEdge_INET	INET interface for the DC-v...	WAN Edge Interface	vEdge Cloud	1	2	admin	24 Aug 2020 2:03:2...	...
DC-vEdge_mgmt_int	MGMT interface for the DC-...	WAN Edge Interface	vEdge Cloud	4	5	admin	24 Aug 2020 2:07:0...	...
DCvEdge-vpn0	VPN0 for the DC-vEdges IN...	WAN Edge VPN	vEdge Cloud	1	2	admin	24 Aug 2020 1:59:3...	...
DC-vEdge_MPLS	MPLS interface for the DC-...	WAN Edge Interface	vEdge Cloud	1	2	admin	24 Aug 2020 2:05:2...	...
vedge-vpn20-DC	VPN 20 Template for vEdge...	WAN Edge VPN	vEdge Cloud	1	2	admin		
DCvEdge-vpn512	VPN512 for the DC-vEdges	WAN Edge VPN	vEdge Cloud	4	5	admin		

2. Scroll down to the **Service** section and click on **New Service**. Set the Service Type as *TE* and click on **Add**. Click on **Update**. Click on **Next** and **Configure Devices**. Confirm the configuration change

The screenshot shows a web interface for configuring services. At the top, there is a dark header with the word "SERVICE" in white. Below the header, there is a light blue section containing a "New Service" button (circled in red and labeled with a yellow circle containing the number 1). To the right of this button is a "Service Type" dropdown menu (circled in red and labeled with a yellow circle containing the number 2) which is currently set to "TE". To the right of the dropdown menu are "Add" and "Cancel" buttons (the "Add" button is circled in red and labeled with a yellow circle containing the number 3). Below this section is a table with the following columns: "Service Type", "IP Addresses (Maximum: 4)", "Interfaces", "Tracking", and "Action". The table is currently empty, and the text "No data available" is displayed in the center. At the bottom of the page, there is a "Update" button (circled in red and labeled with a yellow circle containing the number 4) and a "Cancel" button.

CONFIGURATION | TEMPLATES

Device Template	Total
DCvEdge_dev_temp	1

Device list (Total: 2 devices)

Filter/Search

e474c5fd-8ce7-d376-7cac-ba950b2c9159
DC-vEdge1|10.255.255.11

0cdd4f0e-f2f1-fe75-866c-469966cda1c3
DC-vEdge2|10.255.255.12

Configure Device Rollback Timer

Back Configure Devices Cancel

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

- On the vManage GUI, go to **Configuration => Templates**. Click on the **Feature** tab and then click on **Add Template**. Search for *vedge* in the **Select Devices** section and select the vEdge Cloud. Click on **System** under Basic Configuration to start configuring a System Template for vEdge30

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)

VPN

4. Give the template a name of *vedge-system-dt* with a Description of *System modification for Dynamic Tunnels - vEdge*. Under Advanced, set **On-Demand Tunnel** to a Global value of *On* and the **On-Demand Tunnel Idle Timeout (min)** to 5. Click on **Save**

Device Type **vEdge Cloud**

Template Name	vedge-system-dt
Description	System modification for Dynamic Tunnels - vEdge

Basic Configuration

GPS

Tracker

Advanced

BASIC CONFIGURATION

Site ID	<input type="text"/>	[system_site_id]
System IP	<input type="text"/>	[system_system_ip]

Basic Configuration GPS Tracker **Advanced**

ICMP Error Rate (pps) 100

Allow Same-Site Tunnel On Off

Route Consistency Check On Off

Collect Admin Tech on Reboot On Off

Idle Timeout

Eco Friendly Mode On Off

On-demand Tunnel On Off

On-demand Tunnel Idle Timeout(min) 5

Save Cancel

5. Go to **Configuration => Templates**. Click on the **Feature** tab and then click on **Add Template**. Search for **csr** in the **Select Devices** section and select the **CSR1000v**. Click on **Cisco System** under Basic Configuration to start configuring a System Template for cEdge40

Device **Feature**

Feature Template > [Add Template](#)

Select Devices

CSR1000v

Select Template

BASIC INFORMATION

Cisco AAA

Cisco BFD

Cisco NTP

Cisco OMP

Cisco Security

Cisco System

Global Settings

Security App Hosting

VPN

6. Give the template a name of *cedge-system-dt* with a Description of *System modification for Dynamic Tunnels - cEdge*. Under Advanced, set **On-Demand Tunnel** to a Global value of *On* and the **On-Demand Tunnel Idle Timeout (min)** to 5. Click on **Save**

Device Feature

Feature Template > Add Template > Cisco System

Device Type **CSR1000v**

Template Name

Description

Basic Configuration

GPS

Tracker

Advanced

BASIC CONFIGURATION

Site ID

[system_site_id]

System IP

[system_system_ip]

Basic Configuration

GPS

Tracker

Advanced

Port Offset

Track Transport

On Off

Track Interface

Gateway Tracking

On Off

Collect Admin Tech on Reboot

On Off

Idle Timeout

On-demand Tunnel

On Off

On-demand Tunnel Idle Timeout(min)

Save

Cancel

7. We will now attach the System templates just created to **vEdge30** and **cEdge40**. Navigate to **Configuration => Templates**. While on the Device Tab, locate the *vEdge30_dev_temp* template and click on the three dots next to it. Choose to **Edit** the template

Cisco vManage CONFIGURATION | TEMPLATES

Device Feature

+ Create Template

Template Type: Non-Default

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:3...	In Sync
cEdge-single...	Single Uplink cE...	Feature	CSR1000v	17	2	admin	24 Aug 2020 6:16:...	In Sync
cedge_dualup...	cedge Device Te...	Feature	CSR1000v	19	1	admin	06 Dec 2020 3:34:...	In Sync
DCvEdge_dev...	Device template ...	Feature	vEdge Cloud	16	2	admin	25 Aug 2020 6:00:...	In Sync
vEdge30_dev...	Device template ...	Feature	vEdge Cloud	15	1	admin	06 Dec 2020 3:33:...	In Sync
vSmart-dev-te...	Device Template...	Feature	vSmart	9	2	admin	06 Dec 2020 3:24:...	In Sync
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:4...	In Sync

- Edit
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

8. Update the **System** template as *vedge-system-dt* and click on **Update**. Click **Next** and **Configure Devices** to push the changes to vEdge30

Device Feature

Device Model

vEdge Cloud

Template Name

vEdge30_dev_temp

Description

Device template for the Site 30 vEdge

Basic Information

Transport & Management VPN

Service VPN

Additional Templates

Basic Information

System *

vedge-system-dt

Logging*

Factory_Default_Logging_Template_V01

AAA

Factory_Default_AAA_Template

BFD *

Factory_Default_BFD_Template_V01

Update

Cancel

9. Navigate to **Configuration => Templates**. While on the Device Tab, locate the *cEdge_dualuplink_devtemp* template and click on the three dots next to it. Choose to **Edit** the template

Device Feature

+ Create Template



Template Type

Non-Default



Search Options

Total Rows: 7

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:3...	In Sync	...
cEdge-single-...	Single Uplink cE...	Feature	CSR1000v	17	2	admin	24 Aug 2020 6:16...	In Sync	...
cedge_dualup...	cedge Device Te...	Feature	CSR1000v	19	1	admin	06 Dec 2020 3:34...	In Sync	...
DCvEdge_dev...	Device template ...	Feature	vEdge Cloud	16	2	admin	25 Aug 2020 6:00...	In Sync	
vEdge30_dev...	Device template ...	Feature	vEdge Cloud	15	1	admin	06 Dec 2020 3:39...	In Sync	
vSmart-dev-te...	Device Template...	Feature	vSmart	9	2	admin	06 Dec 2020 3:24...	In Sync	
vEdge_Site20...	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:4...	In Sync	

- Edit
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

10. Update the **Cisco System** template as *cedge-system-dt* and click on **Update**. Click **Next** and **Configure Devices** to push the changes to cEdge40

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 * cedge-system-dt

Cisco Logging* Default_Logging_Cisco_V01

Cisco AAA Factory_Default_AAA_CISCO_Template

Cisco BFD * Default_BFD_Cisco_V01

Update Cancel

This completes the configuration of our System Feature Templates for vEdge30 and cEdge40 to enable Dynamic On-Demand Tunnels.

Task List

- [Overview](#)
- [Exploring the current setup](#)
- [Configuring a Control Policy for Dynamic Tunnels](#)
- [Configuring OMP Templates](#)
- [Enabling Dynamic Tunnels](#)
- [Activity Verification](#)

Activity Verification

1. Log in to the CLI of *DC-vEdge1* and *DC-vEdge2* using the saved Putty session (or SSH to 192.168.0.10 and 192.168.0.11, respectively). Use the credentials given below. Issue `clear control connections` on both devices

Username	Password
admin	admin

```
192.168.0.10 - PuTTY
login as: admin
Pre-authentication banner message from server:
| viptela 20.3.1
|
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Last login: Sun Dec 6 22:11:27 2020 from 192.168.0.121
Welcome to Viptela CLI
admin connected from 192.168.0.121 using ssh on DC-vEdge1
DC-vEdge1# clear control connections
DC-vEdge1#
DC-vEdge1#
DC-vEdge1#
DC-vEdge1#
DC-vEdge1#
DC-vEdge1#
```

2. Log in to the CLI of *vEdge30* using the saved Putty session (or SSH to 192.168.0.30). Use the same credentials as above and issue `show omp tlocs | tab`. Notice that the TLOC Routes for *cEdge40* are learnt by *vEdge30*, but they are in an inactive state

```

vEdge30# show omp tlocs | tab
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
S -> stale
Ext -> extranet
Stg -> staged
IA -> On-demand inactive
Inv -> invalid

```

ADDRESS FAMILY	TLOC IP	COLOR	ENCAP	FROM PEER	STATUS	PSEUDO KEY	PUBLIC IP	PUBLIC PORT	PRIVATE IP	PRIVATE PORT	PUBLIC IPV6	PRIVATE IPV6	PRIVATE IPV6	BFD STATUS	
ipv4	10.255.255.11	mpls	ipsec	10.255.255.3	C,I,R	1	192.0.2.2	12346	192.0.2.2	12346	::	0	0	up	
				10.255.255.4	C,R	1	192.0.2.2	12346	192.0.2.2	12346	::	0	0	0	up
	10.255.255.11	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.10	12346	100.100.100.10	12346	::	0	0	up	
				10.255.255.4	C,R	1	100.100.100.10	12346	100.100.100.10	12346	::	0	0	0	up
	10.255.255.12	mpls	ipsec	10.255.255.3	C,I,R	1	192.0.2.6	12346	192.0.2.6	12346	::	0	0	up	
				10.255.255.4	C,R	1	192.0.2.6	12346	192.0.2.6	12346	::	0	0	0	up
	10.255.255.12	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.11	12346	100.100.100.11	12346	::	0	0	0	up
				10.255.255.4	C,R	1	100.100.100.11	12346	100.100.100.11	12346	::	0	0	0	up
	10.255.255.21	mpls	ipsec	10.255.255.3	C,I,R	1	192.168.26.20	12346	192.168.26.20	12346	::	0	0	0	up
				10.255.255.4	C,R	1	192.168.26.20	12346	192.168.26.20	12346	::	0	0	0	up
	10.255.255.21	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.20	12366	100.100.100.20	12366	::	0	0	0	up
				10.255.255.4	C,R	1	100.100.100.20	12366	100.100.100.20	12366	::	0	0	0	up
	10.255.255.22	mpls	ipsec	10.255.255.3	C,I,R	1	192.0.2.10	12366	192.0.2.10	12366	::	0	0	0	up
				10.255.255.4	C,R	1	192.0.2.10	12366	192.0.2.10	12366	::	0	0	0	up
	10.255.255.22	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.20	56264	192.168.25.21	12346	::	0	0	0	up
				10.255.255.4	C,R	1	100.100.100.20	56264	192.168.25.21	12346	::	0	0	0	up
	10.255.255.31	mpls	ipsec	0.0.0.0	C,Red,R	1	192.0.2.14	12346	192.0.2.14	12346	::	0	0	0	up
	10.255.255.31			public-internet	ipsec	0.0.0.0	C,Red,R	1	100.100.100.30	12346	100.100.100.30	12346	::	0	0
	10.255.255.41	mpls	ipsec	10.255.255.3	C,I,R	1	192.1.2.18	12346	192.1.2.18	12346	::	0	0	0	inact
	10.255.255.41			public-internet	ipsec	10.255.255.4	C,R	1	192.1.2.18	12346	192.1.2.18	12346	::	0	0
10.255.255.41	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.40	12346	100.100.100.40	12346	::	0	0	0	inact	
10.255.255.41			public-internet	ipsec	10.255.255.4	C,R	1	100.100.100.40	12346	100.100.100.40	12346	::	0	0	0
10.255.255.51	public-internet	ipsec	10.255.255.3	C,I,R	1	100.100.100.50	12367	100.100.100.50	12367	::	0	0	0	up	
10.255.255.51			public-internet	ipsec	10.255.255.4	C,R	1	100.100.100.50	12367	100.100.100.50	12367	::	0	0	0
10.255.255.52	mpls	ipsec	10.255.255.3	C,I,R	1	192.1.2.22	12367	192.1.2.22	12367	::	0	0	0	up	
10.255.255.52			mpls	ipsec	10.255.255.4	C,R	1	192.1.2.22	12367	192.1.2.22	12367	::	0	0	0

3. Run the commands `show system on-demand` and `show system on-demand remote-system` on vEdge30. You will notice that vEdge30 shows itself as On-Demand yes and Status *Active*. However, the Status of cEdge40 is *inactive*

```

vEdge30#
vEdge30# show system on-demand
SITE-ID      SYSTEM-IP      ON-DEMAND      STATUS      IDLE-TIMEOUT-CFG (min)
-----
30           10.255.255.31  yes            active      5

vEdge30# show system on-demand remote-system
SITE-ID      SYSTEM-IP      ON-DEMAND      STATUS      IDLE-TIMEOUT-EXPIRY (sec)
-----
1            10.255.255.11  no             -          -
1            10.255.255.12  no             -          -
20           10.255.255.21  no             -          -
20           10.255.255.22  no             -          -
40           10.255.255.41  yes            inactive   -
50           10.255.255.51  no             -          -
50           10.255.255.52  no             -          -

```

- Run the command `show omp routes | tab` on vEdge30. Notice that the OMP Routes for the VPN 10 subnet at cEdge40 (10.40.10.0/24) are in an Unresolved, On-Demand Inactive state (U,IA)

```
vEdge30# show omp routes | tab
```

```
Code:
```

```
C -> chosen  
I -> installed  
Red -> redistributed  
Rej -> rejected  
L -> looped  
R -> resolved  
S -> stale  
Ext -> extranet  
Inv -> invalid  
Stg -> staged  
IA -> On-demand inactive  
U -> TLOC unresolved
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR	ENCAP	PREFERENCE
10	10.0.0.1/32	10.255.255.3	55	1003	C,I,R	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.3	56	1003	C,I,R	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.3	102	1003	C,I,R	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.3	105	1003	C,I,R	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.4	86	1003	C,R	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.4	87	1003	C,R	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.4	125	1003	C,R	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.4	130	1003	C,R	installed	10.255.255.12	public-internet	ipsec	-
10	10.20.10.0/24	10.255.255.3	80	1003	C,I,R	installed	10.255.255.21	mpls	ipsec	-
		10.255.255.3	82	1003	C,I,R	installed	10.255.255.21	public-internet	ipsec	-
		10.255.255.3	83	1003	C,I,R	installed	10.255.255.22	public-internet	ipsec	-
		10.255.255.3	86	1003	C,I,R	installed	10.255.255.22	mpls	ipsec	-
		10.255.255.4	98	1003	C,R	installed	10.255.255.21	mpls	ipsec	-
		10.255.255.4	99	1003	C,R	installed	10.255.255.21	public-internet	ipsec	-
		10.255.255.4	100	1003	C,R	installed	10.255.255.22	mpls	ipsec	-
		10.255.255.4	101	1003	C,R	installed	10.255.255.22	public-internet	ipsec	-
10	10.30.10.0/24	0.0.0.0	66	1003	C,Red,R	installed	10.255.255.31	mpls	ipsec	-
		0.0.0.0	69	1003	C,Red,R	installed	10.255.255.31	public-internet	ipsec	-
10	10.40.10.0/24	10.255.255.3	66	1002	U,IA	installed	10.255.255.41	public-internet	ipsec	-
		10.255.255.3	98	1002	U,IA	installed	10.255.255.41	mpls	ipsec	-
		10.255.255.4	109	1002	U,IA	installed	10.255.255.41	public-internet	ipsec	-
10	10.40.11.0/24	10.255.255.4	121	1002	U,IA	installed	10.255.255.41	mpls	ipsec	-
		10.255.255.3	67	1002	U,IA	installed	10.255.255.41	public-internet	ipsec	-
		10.255.255.3	100	1002	U,IA	installed	10.255.255.41	mpls	ipsec	-
		10.255.255.4	107	1002	U,IA	installed	10.255.255.41	public-internet	ipsec	-
10	10.50.10.0/24	10.255.255.4	122	1002	U,IA	installed	10.255.255.41	mpls	ipsec	-
		10.255.255.3	19	1002	C,I,R	installed	10.255.255.51	public-internet	ipsec	-
		10.255.255.3	20	1002	C,I,R	installed	10.255.255.52	mpls	ipsec	-

5. On the vManage GUI, navigate to **Configuration => Policies** and locate the *Dynamic-Tunnels-Site30_40* policy. Click on the three dots next to it and choose to Activate this policy. Click on **Activate** and **Configure Devices** if prompted

CONFIGURATION | POLICIES Custom Options ▾

Centralized Policy Localized Policy

[+ Add Policy](#) ↻ ☰

Search Search Options ▾ Total Rows: 6

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
Hub-n-Spoke-VPN20-only	Hub and Spoke policy for ...	UI Policy Builder	false	admin	08252020T130734383	25 Aug 2020 6:07:34 AM
Site40-Guest-DIA	DIA Policy for Site 40 Gue...	UI Policy Builder	false	admin	08282020T062900849	27 Aug 2020 11:29:00 P...	...
traffic-engineering-ftp	Traffic Engineering for FTP	UI Policy Builder	false	admin	08282020T061906584	27 Aug 2020 11:19:06 P...	...
Site20-Regional-Hub-Site30	Regional Policy for Site 2...	UI Policy Builder	false	admin	08262020T102636751	26 Aug 2020 3:26:36 AM
Dynamic-Tunnels-Site30_...	Dynamic Tunnels betwee...	UI Policy Builder	false	admin	12062020T231246475	06 Dec 2020 3:12:46 PM
AAR-VPN10	Transport Preference for ...	UI Policy Builder	true	admin	08302020T120129495	30 Aug	<ul style="list-style-type: none"> View Preview Copy Edit Delete Activate

6. Once the policy is active, go to the CLI of vEdge30 and run `show omp routes | tab` again. We now see that the traffic to the VPN 10 subnet at cEdge40 (10.40.10.0/24) is being routed via the DC-vEdges, with the direct routes to cEdge40 in an Installed, Unresolved and On-Demand Inactive state (I,U,IA)

VPN	PREFIX	FROM PEER	ID	LABEL	STATUS	TYPE	TLOC IP	COLOR	ENCAP	PREFERENCE		
10	10.0.0.1/32	10.255.255.3	55	1003	C,I,R	installed	10.255.255.11	mpls	ipsec	-		
		10.255.255.3	56	1003	C,I,R	installed	10.255.255.11	public-internet	ipsec	-		
		10.255.255.3	102	1003	C,I,R	installed	10.255.255.12	mpls	ipsec	-		
		10.255.255.3	105	1003	C,I,R	installed	10.255.255.12	public-internet	ipsec	-		
		10.255.255.4	86	1003	C,R	installed	10.255.255.11	mpls	ipsec	-		
		10.255.255.4	87	1003	C,R	installed	10.255.255.11	public-internet	ipsec	-		
		10.255.255.4	125	1003	C,R	installed	10.255.255.12	mpls	ipsec	-		
		10.255.255.4	130	1003	C,R	installed	10.255.255.12	public-internet	ipsec	-		
		10	10.20.10.0/24	10.255.255.3	80	1003	C,I,R	installed	10.255.255.21	mpls	ipsec	-
				10.255.255.3	82	1003	C,I,R	installed	10.255.255.21	public-internet	ipsec	-
10.255.255.3	83			1003	C,I,R	installed	10.255.255.22	public-internet	ipsec	-		
10.255.255.3	86			1003	C,I,R	installed	10.255.255.22	mpls	ipsec	-		
10.255.255.4	98			1003	C,R	installed	10.255.255.21	mpls	ipsec	-		
10.255.255.4	99			1003	C,R	installed	10.255.255.21	public-internet	ipsec	-		
10.255.255.4	100			1003	C,R	installed	10.255.255.22	mpls	ipsec	-		
10.255.255.4	101			1003	C,R	installed	10.255.255.22	public-internet	ipsec	-		
10	10.30.10.0/24			0.0.0.0	66	1003	C,Red,R	installed	10.255.255.31	mpls	ipsec	-
				0.0.0.0	69	1003	C,Red,R	installed	10.255.255.31	public-internet	ipsec	-
10	10.40.10.0/24	10.255.255.3	109	1003	C,I,R	installed	10.255.255.11	mpls	ipsec	-		
		10.255.255.3	110	1003	Inv,U	installed	10.255.255.11	public-internet	ipsec	-		
		10.255.255.3	111	1003	C,I,R	installed	10.255.255.12	mpls	ipsec	-		
		10.255.255.3	112	1003	Inv,U	installed	10.255.255.12	public-internet	ipsec	-		
		10.255.255.3	113	1002	I,U,IA	installed	10.255.255.41	mpls	ipsec	-		
		10.255.255.3	114	1003	Inv,U	installed	10.255.255.11	mpls	ipsec	-		
		10.255.255.3	115	1003	C,I,R	installed	10.255.255.11	public-internet	ipsec	-		
		10.255.255.3	116	1003	Inv,U	installed	10.255.255.12	mpls	ipsec	-		
		10.255.255.3	117	1003	C,I,R	installed	10.255.255.12	public-internet	ipsec	-		
		10.255.255.3	118	1002	I,U,IA	installed	10.255.255.41	public-internet	ipsec	-		
		10.255.255.4	151	1003	C,R	installed	10.255.255.11	mpls	ipsec	-		
		10.255.255.4	152	1003	Inv,U	installed	10.255.255.11	public-internet	ipsec	-		
		10.255.255.4	153	1003	C,R	installed	10.255.255.12	mpls	ipsec	-		
		10.255.255.4	154	1003	Inv,U	installed	10.255.255.12	public-internet	ipsec	-		
		10.255.255.4	155	1002	U,IA	installed	10.255.255.41	mpls	ipsec	-		
		10.255.255.4	156	1003	Inv,U	installed	10.255.255.11	mpls	ipsec	-		
		10.255.255.4	157	1003	C,R	installed	10.255.255.11	public-internet	ipsec	-		
		10.255.255.4	158	1003	Inv,U	installed	10.255.255.12	mpls	ipsec	-		
		10.255.255.4	159	1003	C,R	installed	10.255.255.12	public-internet	ipsec	-		
		10.255.255.4	160	1002	U,IA	installed	10.255.255.41	public-internet	ipsec	-		
10	10.40.11.0/24	10.255.255.3	129	1003	C,I,R	installed	10.255.255.11	mpls	ipsec	-		
		10.255.255.3	130	1003	Inv,U	installed	10.255.255.11	public-internet	ipsec	-		
		10.255.255.3	131	1003	C,I,R	installed	10.255.255.12	mpls	ipsec	-		

7. Log in to the CLI of vEdge30 and run a Traceroute to 10.40.10.2 via the CLI `traceroute VPN 10 10.40.10.2`. We will see that the initial path will traverse an IP in VPN 10 at the DC-vEdges (10.100.10.3 in this example) and will then start going directly to cEdge40. This is because the initial packet takes the backup DC-vEdge route after which the Tunnel between vEdge30 and cEdge40 is established. Run `show system on-demand` and `show system on-demand remote` and we will see that the Tunnel to cEdge40 is now active, with the Idle timeout counting down from 300 seconds (i.e. 5 minutes, as we had configured in the System Template)

```

vEdge30# traceroute vpn 10 10.40.10.2
Traceroute 10.40.10.2 in VPN 10
traceroute to 10.40.10.2 (10.40.10.2), 30 hops max, 60 byte packets
 1 10.100.10.3 (10.100.10.3) 0.230 ms 0.294 ms 0.297 ms
 2 * 10.40.10.2 (10.40.10.2) 2.366 ms *
vEdge30# show system on-demand
SITE-ID      SYSTEM-IP      ON-DEMAND      STATUS      IDLE-TIMEOUT-CFG(min)
-----
30          10.255.255.31  yes            active      5

vEdge30# show system on-demand remote
SITE-ID      SYSTEM-IP      ON-DEMAND      STATUS      IDLE-TIMEOUT-EXPIRY(sec)
-----
1           10.255.255.11  no             -           -
1           10.255.255.12  no             -           -
20          10.255.255.21  no             -           -
20          10.255.255.22  no             -           -
40          10.255.255.41  yes            active      274
50          10.255.255.51  no             -           -
50          10.255.255.52  no             -           -

```

8. Subsequent traffic will go directly over the Tunnel between vEdge30 and cEdge40, as long as the Tunnel is active. This can be verified by running `traceroute vpn 10 10.40.10.2` on vEdge30

```

vEdge30# traceroute vpn 10 10.40.10.2
Traceroute 10.40.10.2 in VPN 10
traceroute to 10.40.10.2 (10.40.10.2), 30 hops max, 60 byte packets
 1 10.40.10.2 (10.40.10.2) 3.347 ms * *
vEdge30# █

```

9. `show omp routes 10.40.10.0/24` indicates that the Chosen, Installed, Resolved (C,I,R) route for the 10.40.10.0 subnet is the direct path to cEdge40


```

vEdge30# show omp routes 10.40.10.0/24
Code:
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
S -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA -> On-demand inactive
U -> TLOC unresolved

```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR	ENCAP	PREFERENCE
10	10.40.10.0/24	10.255.255.3	109	1003	R	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.3	110	1003	Inv,U	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.3	111	1003	R	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.3	112	1003	Inv,U	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.3	113	1002	C,I,R	installed	10.255.255.41	mpls	ipsec	-
		10.255.255.3	114	1003	Inv,U	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.3	115	1003	R	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.3	116	1003	Inv,U	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.3	117	1003	R	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.3	118	1002	C,I,R	installed	10.255.255.41	public-internet	ipsec	-
		10.255.255.4	151	1003	R	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.4	152	1003	Inv,U	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.4	153	1003	R	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.4	154	1003	Inv,U	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.4	155	1002	C,R	installed	10.255.255.41	mpls	ipsec	-
		10.255.255.4	156	1003	Inv,U	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.4	157	1003	R	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.4	158	1003	Inv,U	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.4	159	1003	R	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.4	160	1002	C,R	installed	10.255.255.41	public-internet	ipsec	-

```

vEdge30#

```

- Wait for approximately 5 minutes and we will find that the Tunnel between vEdge30 and cEdge40 transitions to an *inactive* state after the Idle Timeout expires, assuming there is no traffic between the two Sites

```

vEdge30# show system on remote
SITE-ID      SYSTEM-IP      ON-DEMAND      STATUS      IDLE-TIMEOUT-EXPIRY(sec)
-----
1            10.255.255.11  no              -           -
1            10.255.255.12  no              -           -
20           10.255.255.21  no              -           -
20           10.255.255.22  no              -           -
40           10.255.255.41  yes             active      1
50           10.255.255.51  no              -           -
50           10.255.255.52  no              -           -

vEdge30#
vEdge30#
vEdge30# show system on remote
SITE-ID      SYSTEM-IP      ON-DEMAND      STATUS      IDLE-TIMEOUT-EXPIRY(sec)
-----
1            10.255.255.11  no              -           -
1            10.255.255.12  no              -           -
20           10.255.255.21  no              -           -
20           10.255.255.22  no              -           -
40           10.255.255.41  yes             inactive    -
50           10.255.255.51  no              -           -
50           10.255.255.52  no              -           -

```

11. Once the tunnel is inactive, `show omp routes 10.40.10.0/24` shows the traffic path traversing the DC-vEdges again, with the direct path to cEdge40 in I,U,IA

```
vEdge30# show omp routes 10.40.10.0/24
```

```
Code:
```

```
C -> chosen  
I -> installed  
Red -> redistributed  
Rej -> rejected  
L -> looped  
R -> resolved  
S -> stale  
Ext -> extranet  
Inv -> invalid  
Stg -> staged  
IA -> On-demand inactive  
U -> TLOC unresolved
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR	ENCAP	PREFERENCE
10	10.40.10.0/24	10.255.255.3	109	1003	C,I,R	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.3	110	1003	Inv,U	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.3	111	1003	C,I,R	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.3	112	1003	Inv,U	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.3	113	1002	I,U,IA	installed	10.255.255.41	mpls	ipsec	-
		10.255.255.3	114	1003	Inv,U	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.3	115	1003	C,I,R	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.3	116	1003	Inv,U	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.3	117	1003	C,I,R	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.3	118	1002	I,U,IA	installed	10.255.255.41	public-internet	ipsec	-
		10.255.255.4	151	1003	C,R	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.4	152	1003	Inv,U	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.4	153	1003	C,R	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.4	154	1003	Inv,U	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.4	155	1002	U,IA	installed	10.255.255.41	mpls	ipsec	-
		10.255.255.4	156	1003	Inv,U	installed	10.255.255.11	mpls	ipsec	-
		10.255.255.4	157	1003	C,R	installed	10.255.255.11	public-internet	ipsec	-
		10.255.255.4	158	1003	Inv,U	installed	10.255.255.12	mpls	ipsec	-
		10.255.255.4	159	1003	C,R	installed	10.255.255.12	public-internet	ipsec	-
		10.255.255.4	160	1002	U,IA	installed	10.255.255.41	public-internet	ipsec	-

This completes the configuration and verification of Dynamic On-Demand Tunnels.

Task List

- [Overview](#)
- [Exploring the current setup](#)
- [Configuring a Control Policy for Dynamic Tunnels](#)
- [Configuring OMP Templates](#)
- [Enabling Dynamic Tunnels](#)
- [Activity Verification](#)

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

Page last updated: Dec 8, 2020

Site last generated: Dec 14, 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

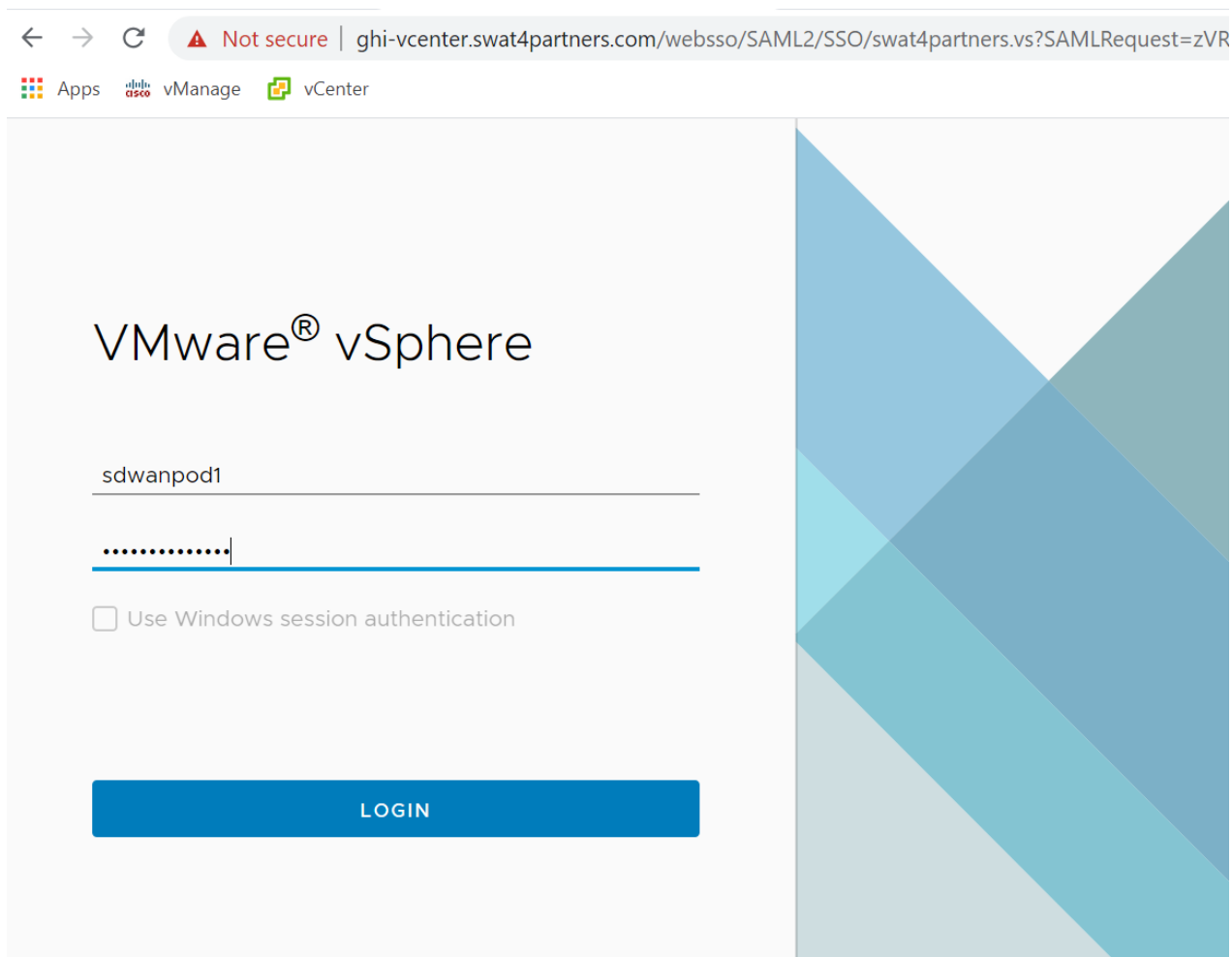
We will be performing some initial configuration in the network before it can support the IPS module. Key points to be noted:

- 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

vm vSphere Client | Menu | Search in all environments

Site40_PC | ACTIONS

Summary | Monitor | Configure | Permissions | Datastores | Networks | Updates

Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Not running, not installed
[More info](#)

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

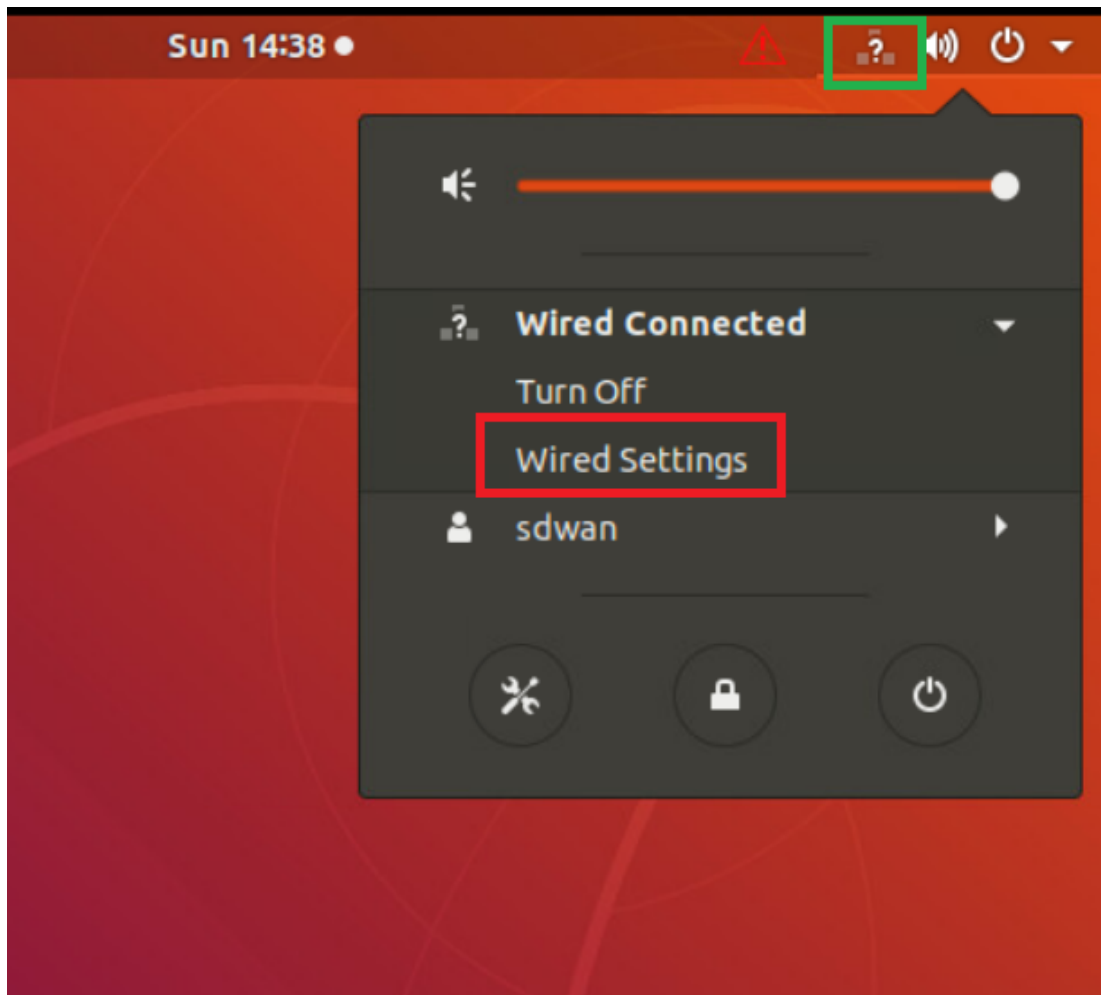
[Launch Web Console](#)
[Launch Remote Console](#)

VMware Tools is not installed on this virtual machine.

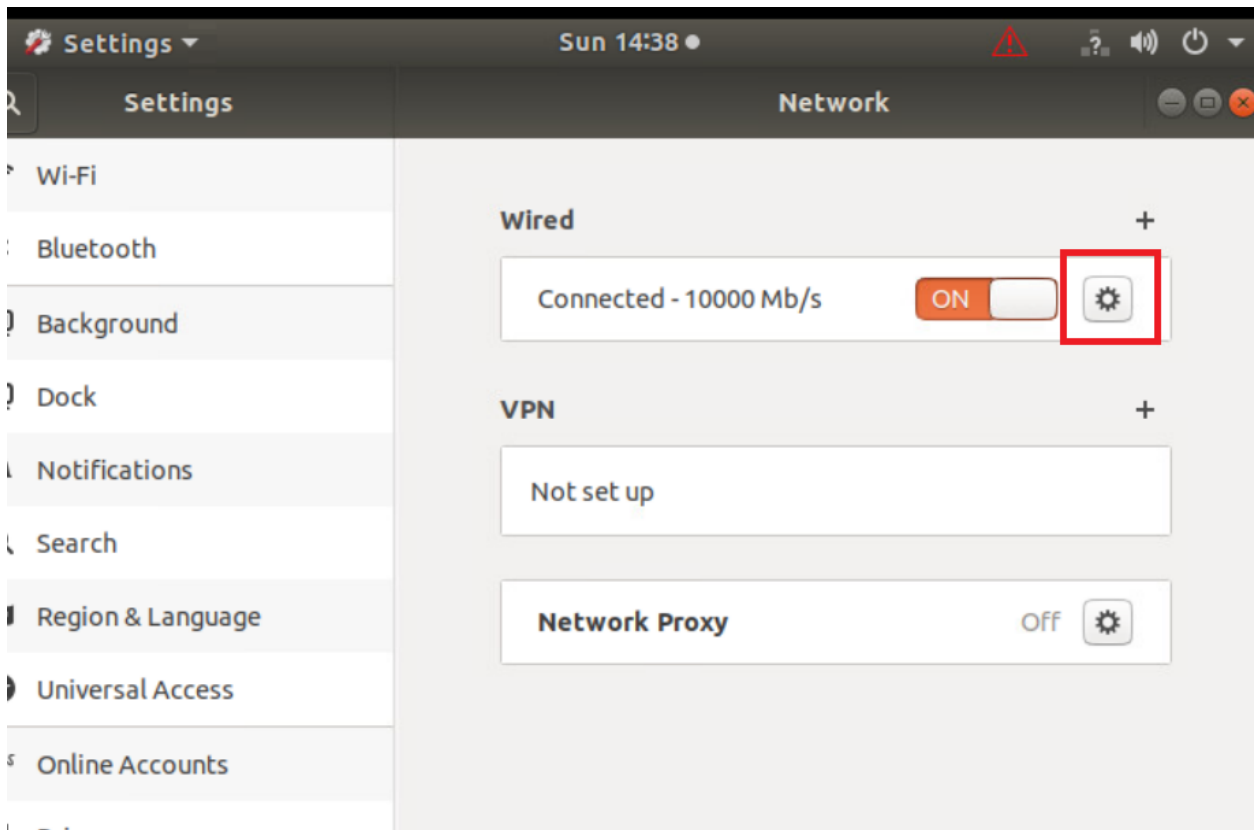
VM Hardware

> CPU	1 CPU(s)
> Memory	2 GB, 0.08 GB memory active
> Hard disk 1	40 GB

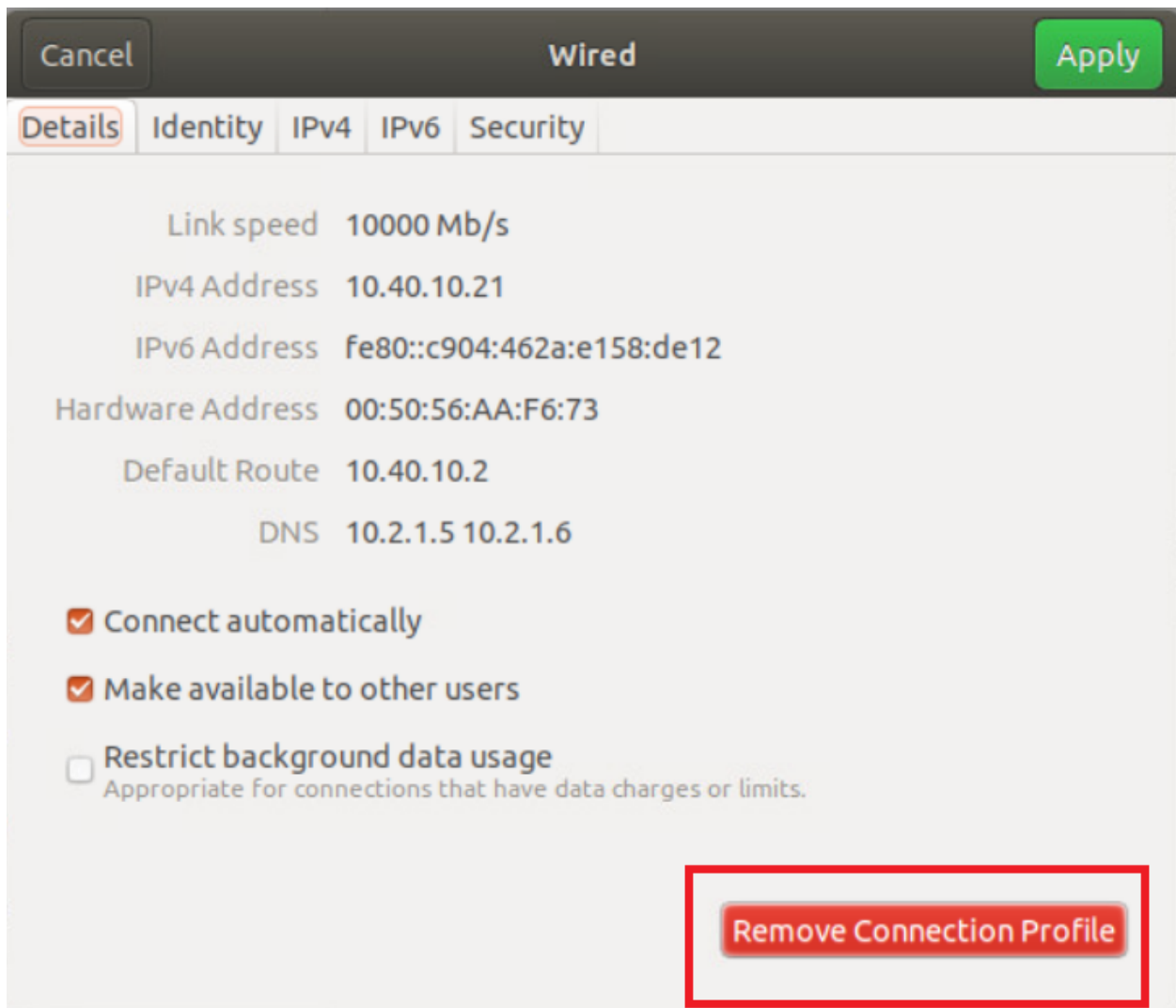
3. Log in to the PC and click on the network icon in the top-right corner. Expand **Wired Connected** and click on **Wired Settings**



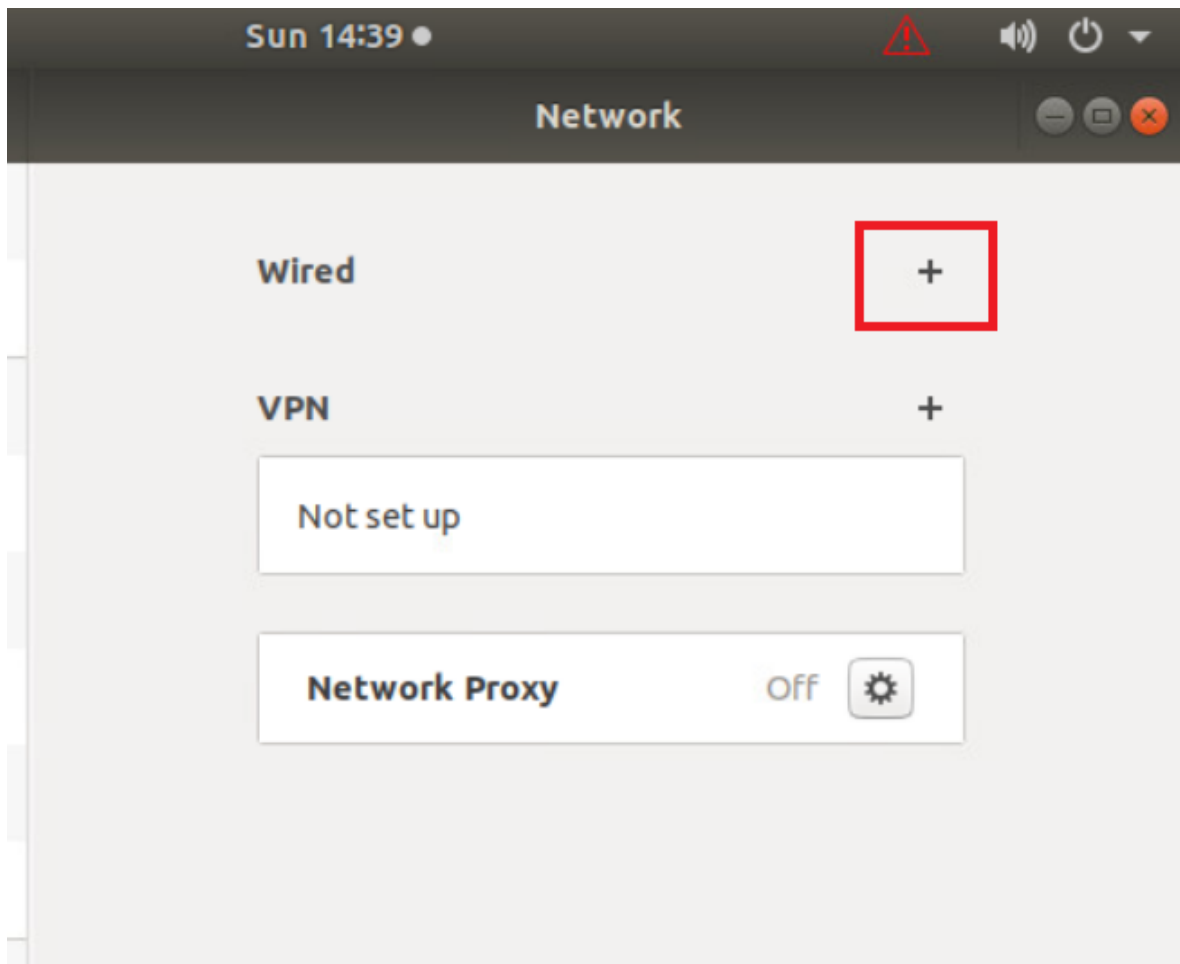
4. Click on the cog wheel/gear icon



5. Click on **Remove Connection Profile**

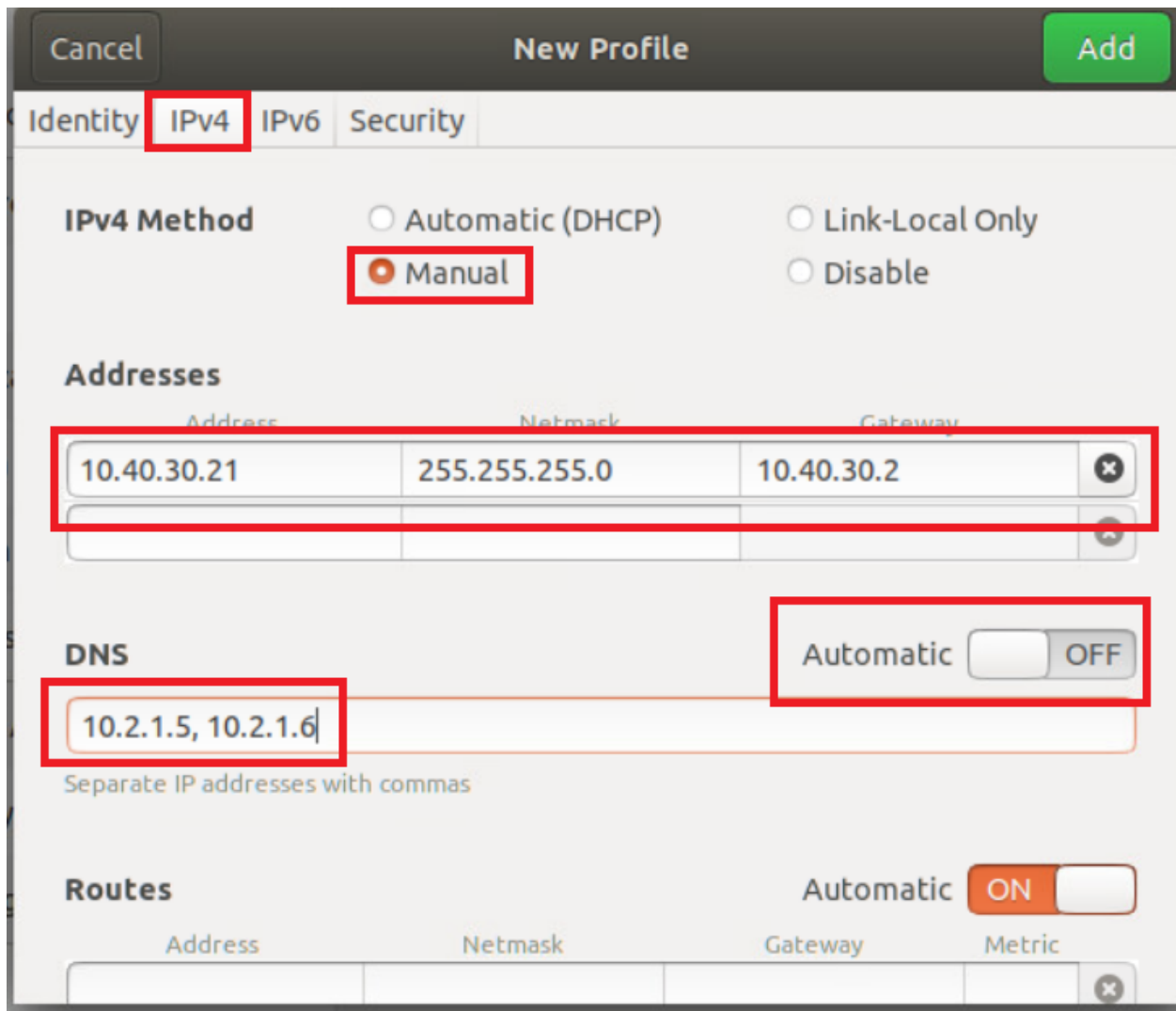


6. If you still see a cog wheel/gear icon next to *Wired*, click on it and choose to **Remove Connection Profile** again. Once the + icon can be seen next to **Wired**, click on it

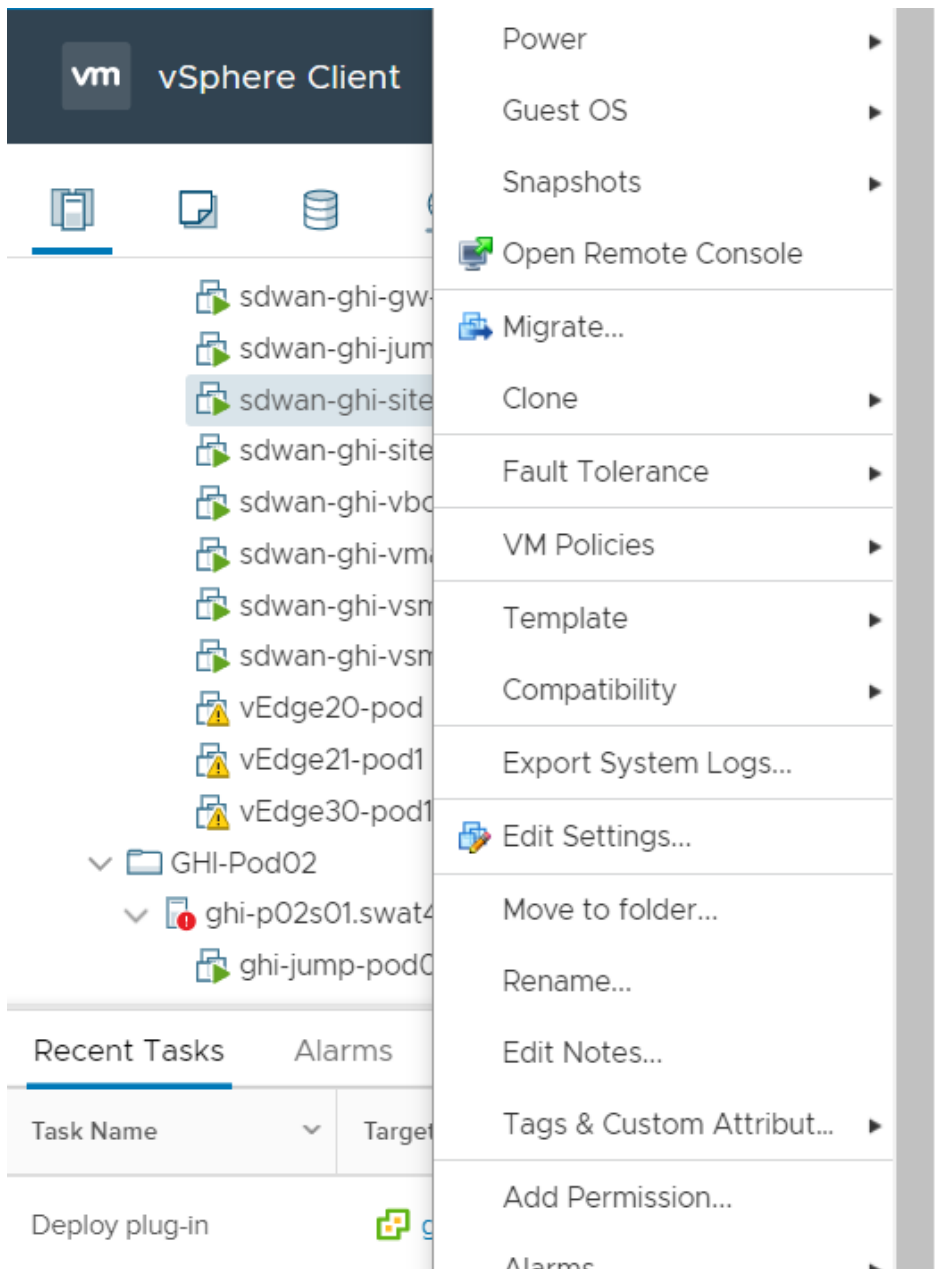


7. Go to the **IPv4** tab and click on **Manual** for the IPv4 Method. Enter details as given below and click on **Add**. Over here, *y* is 1 if you're connected to the SLC DC and 2 if you're connected to the GHI DC. The email sent with lab access details should enumerate which DC you're POD is on

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



8. Back at the vCenter GUI, right click on your Site 40 PC and choose **Edit Settings**



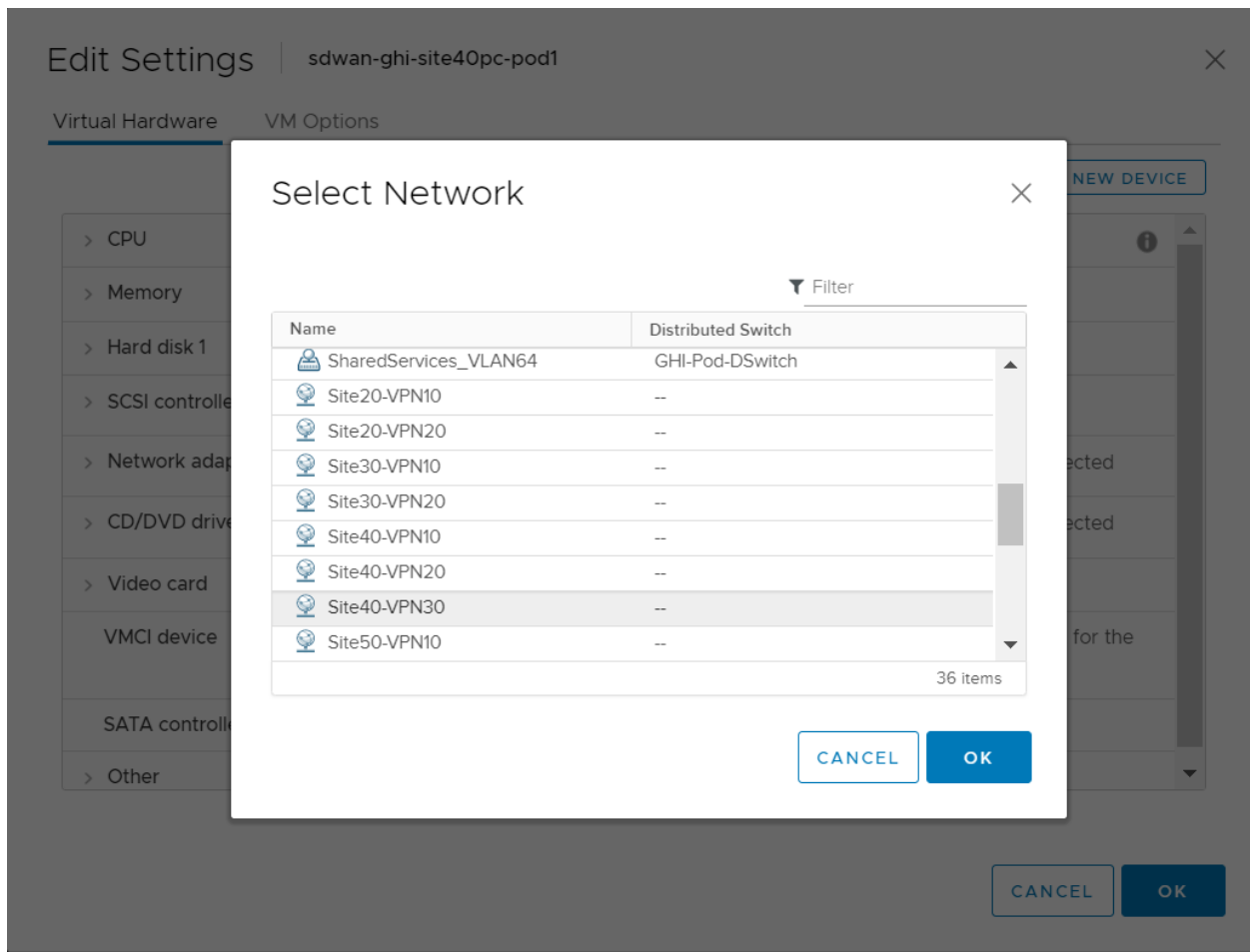
9. Click on the drop down next to **Network Adapter 1** and click on **Browse**

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	▼	<input type="checkbox"/> Connected
	Browse ...		
> 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-DIA*. Click on the three dots next to it and choose to **Activate**. Confirm the Activation

CONFIGURATION | POLICIES Custom Options

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	...

View

Preview

Copy

Edit

Delete

Activate

Activate Policy ✕

Policy will be applied to the reachable vSmarts:

10.255.255.3, 10.255.255.4

Activate
Cancel

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

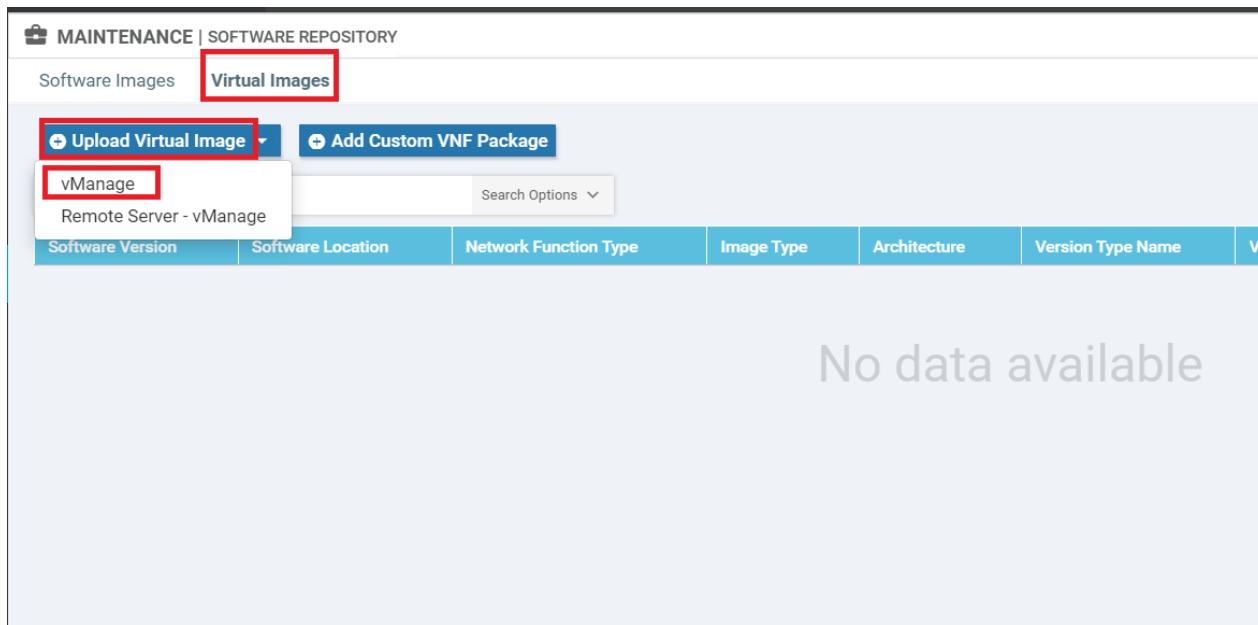
Upload Image to vManage

1. On the vManage GUI, go to **Maintenance => Software Repository**

The screenshot shows the Cisco vManage interface. At the top, the Cisco logo and 'Cisco vManage' are visible. Below the header, the 'TASK VIEW' section displays a task titled 'Push vSmart Policy' with a green checkmark and the text 'Validation Success'. Below this, it shows 'Total Task: 2 | Success : 2'. A search bar with 'Search Options' is present. A sidebar menu is open, listing categories: Maintenance, Software Repository (highlighted in teal), Software Upgrade, Device Reboot, and Security. The main content area shows a table with two rows, both indicating 'Done - Push vSmart Policy'.

Message
Done - Push vSmart Policy
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**



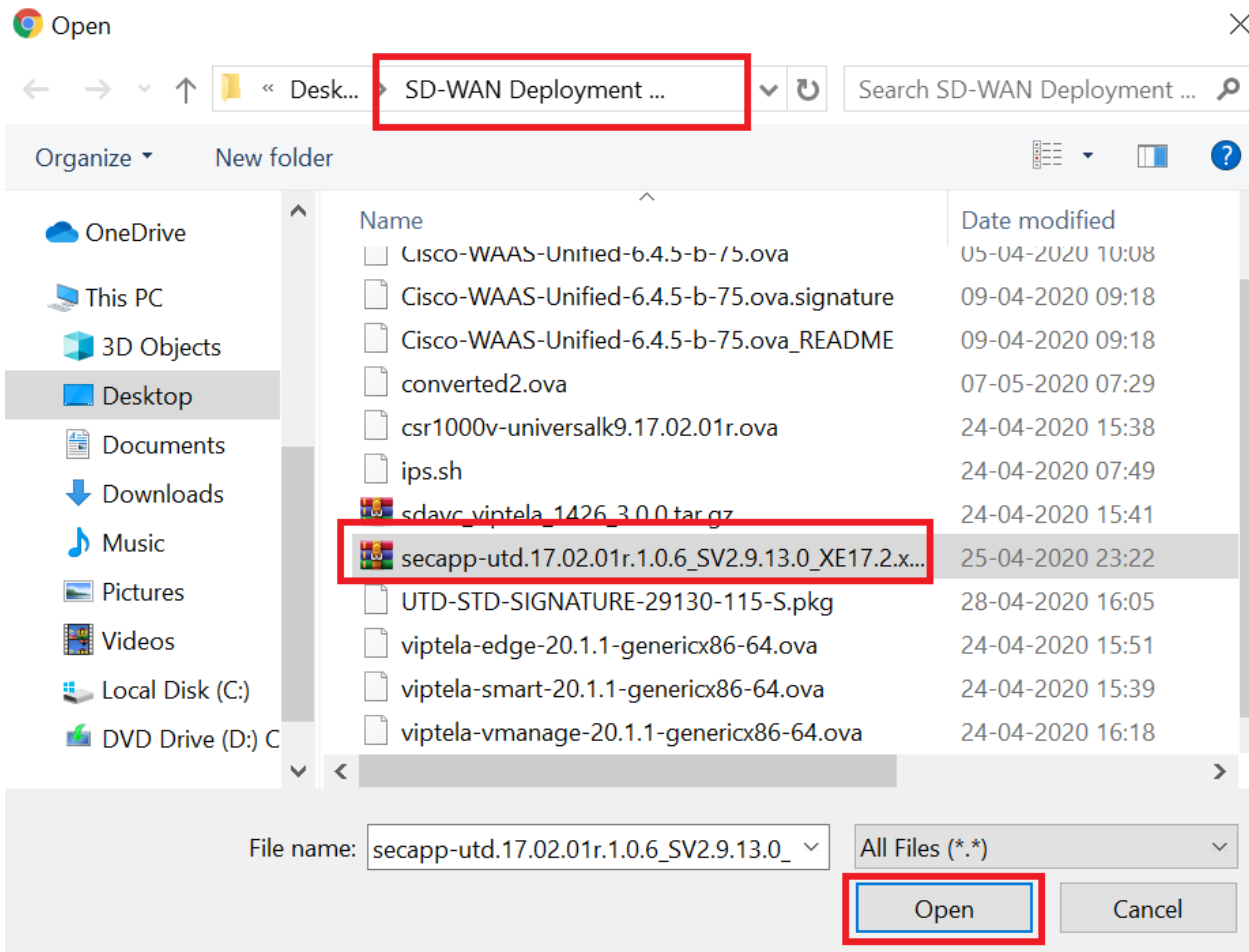
Drag and Drop File

Or

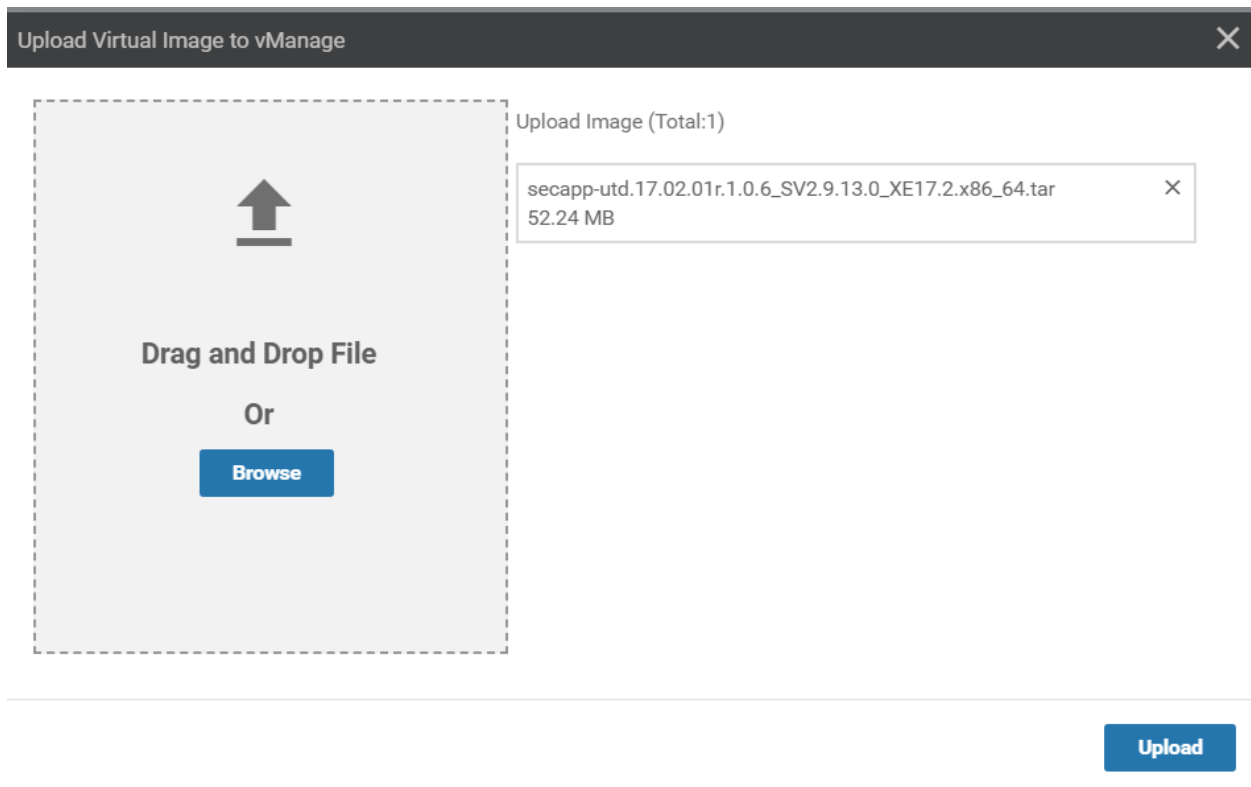
Browse

No Images Uploaded

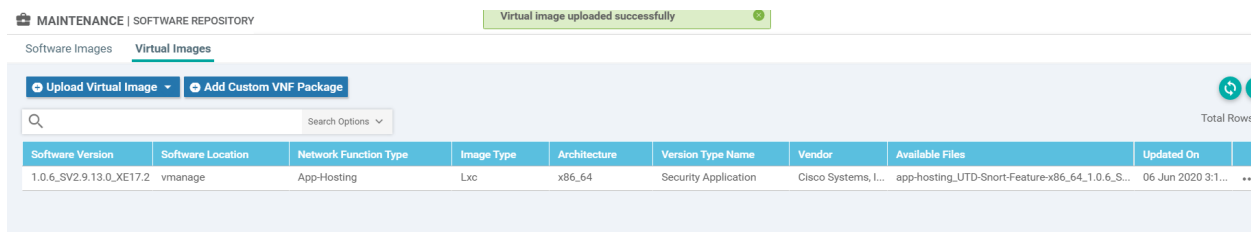
Upload



4. Click on **Upload**



5. Once the file is uploaded, it should show up under Virtual Images



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**

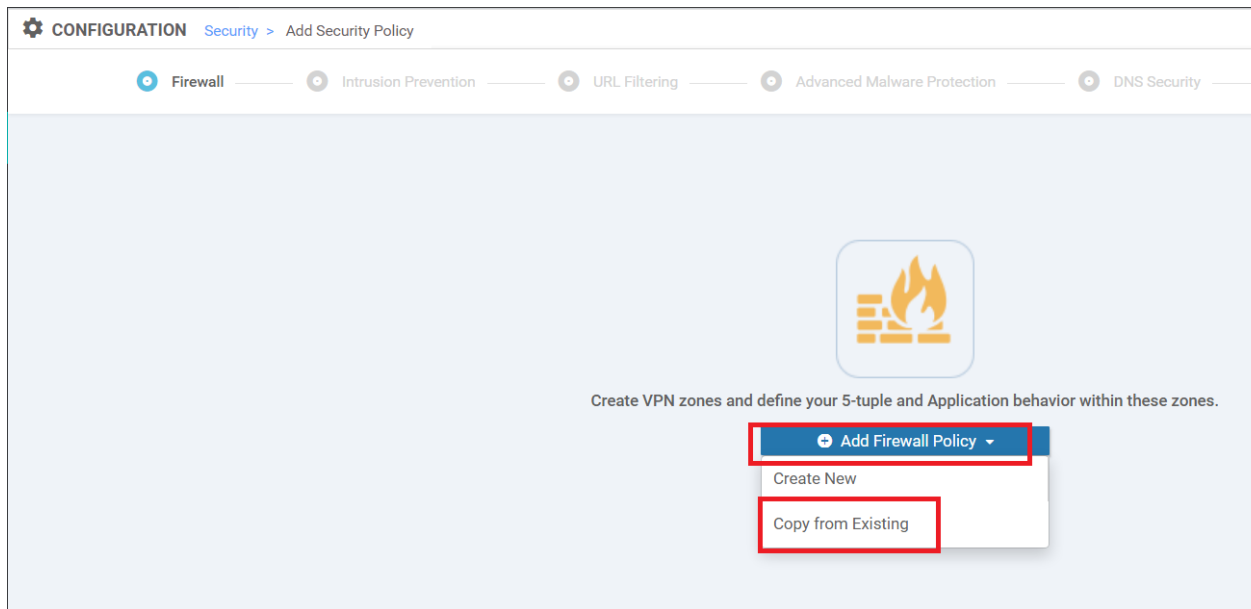
Add Security Policy

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

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 ✕

Policy

Policy Name

Policy Description

4. The Firewall Policy we just copied should show up. Click on **Next**

Firewall — Intrusion Prevention — URL Filtering — Advanced Malware Protection — D

+ Add Firewall Policy (Add a Firewall configuration)

Search Options ▾

Name	Type	Description	Reference Count
Guest-FW_concat	zoneBasedFW	Guest Traffic Firewall with IPS	0

Next CANCEL

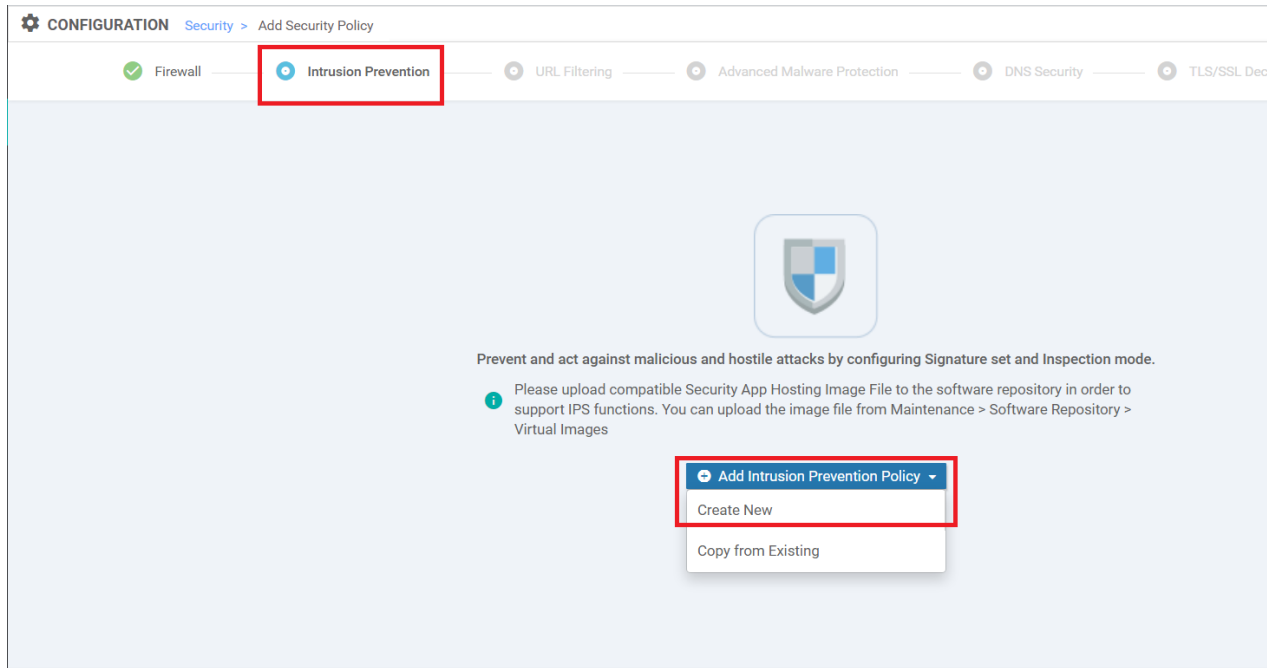
Configuration of the Security Policy continues in the next section.

Task List

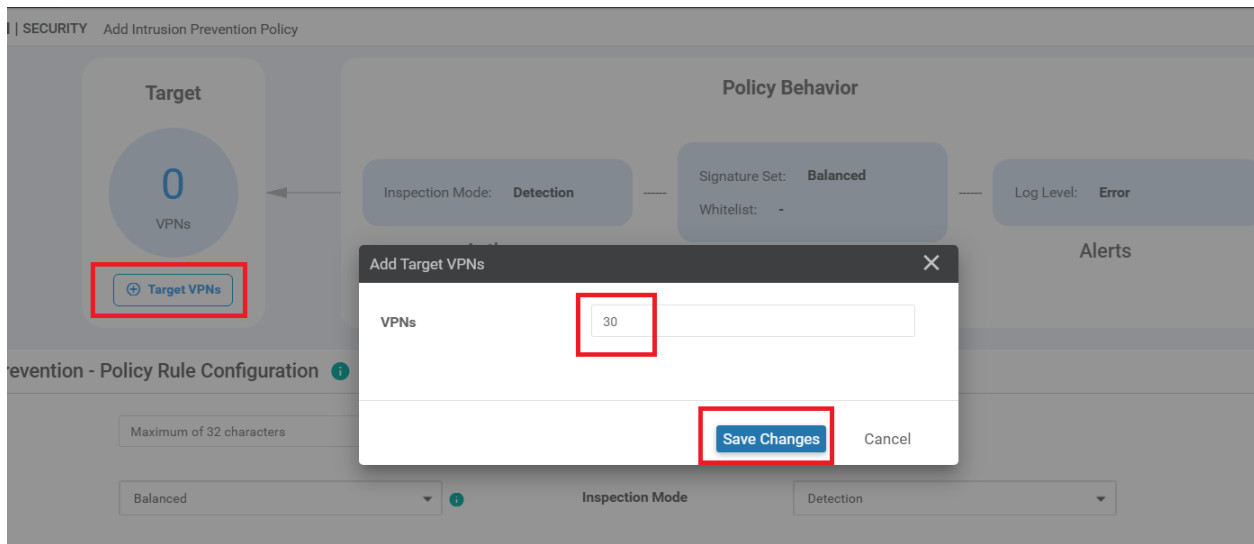
- ~~Overview~~
- ~~Initial Configuration~~
- ~~Revert Site 40 PC changes and enable DIA~~
- ~~Upload Image to vManage~~
- Add the Security Policy
- ~~Firewall Policy Update~~
- Add the IPS Policy and Finalize the Security Policy
- Updating the Application List and Device Template
- Verifying installation 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**

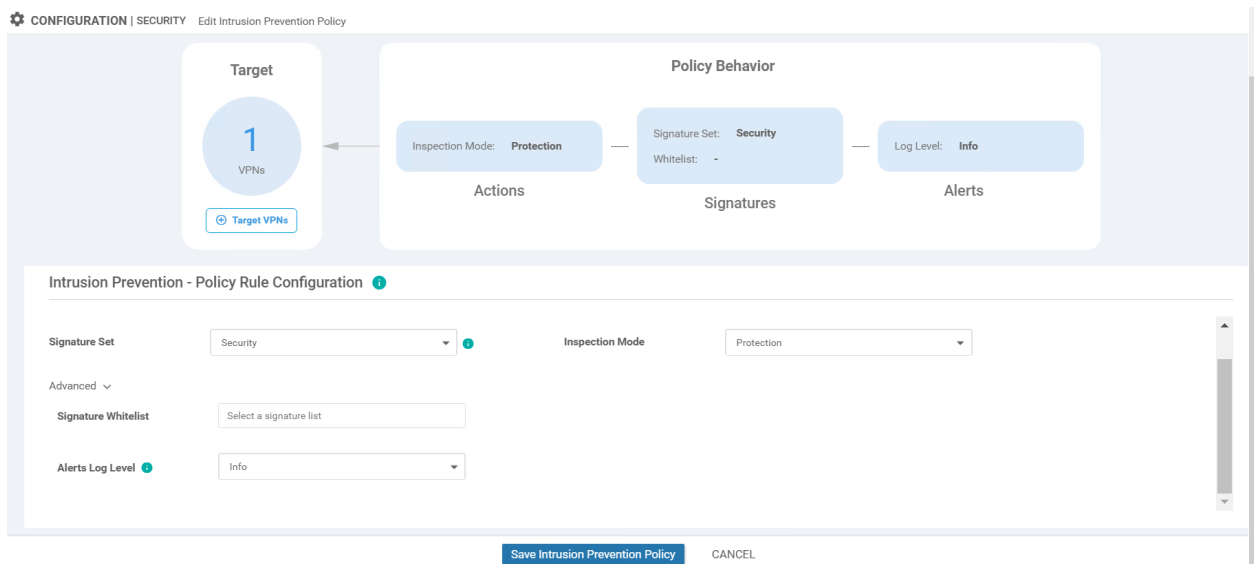


2. Click on **Target VPNs** and enter a VPN of 30. Click on **Save Changes**




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
<i>Guest-IPS</i>	Security	Protection	Info



4. Back at the main Security Policy page, click on **Next** 5 times

Name	Type	Reference Count	Updated By	Last
Guest-IPS	 IntrusionPrevention	0	admin	06

BACK 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
<i>Guest-FW-IPS-DIA</i>	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:

Security Policy Description:

Additional Policy Settings

Firewall

Direct Internet Applications: Bypass firewall policy and allow all Internet traffic to/from VPN 0

TCP SYN Flood Limit: Enabled

High Speed Logging: VPN Server IP: Port:

Audit Trail: On (Applicable only for the rules with Inspect action)

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

External Syslog Server: VPN Server IP:

Failure Mode:

BACK CANCEL

This completes the configuration of our Security Policy.

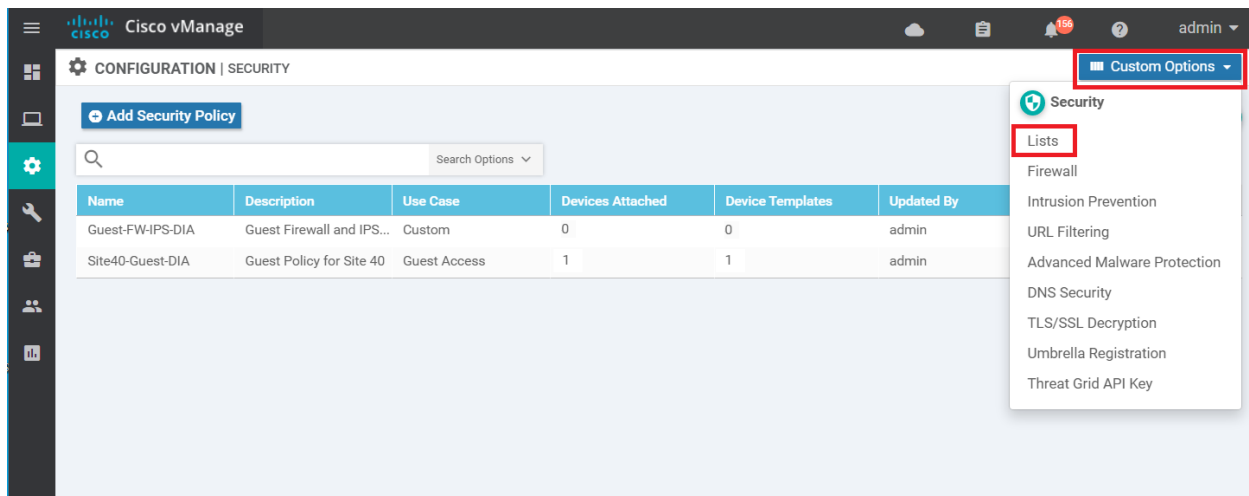
Task List

- [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

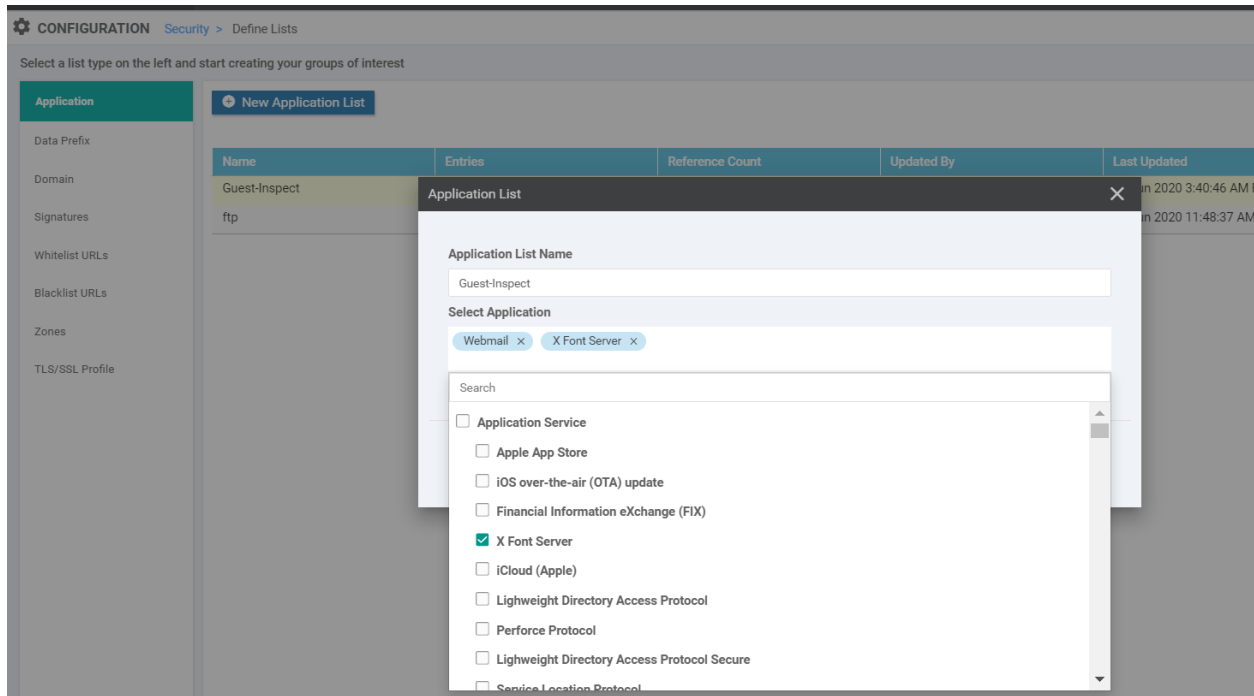
1. On the vManage GUI, go to **Configuration => Security**. Click on **Custom Lists** (top right-hand corner) and choose **Lists**



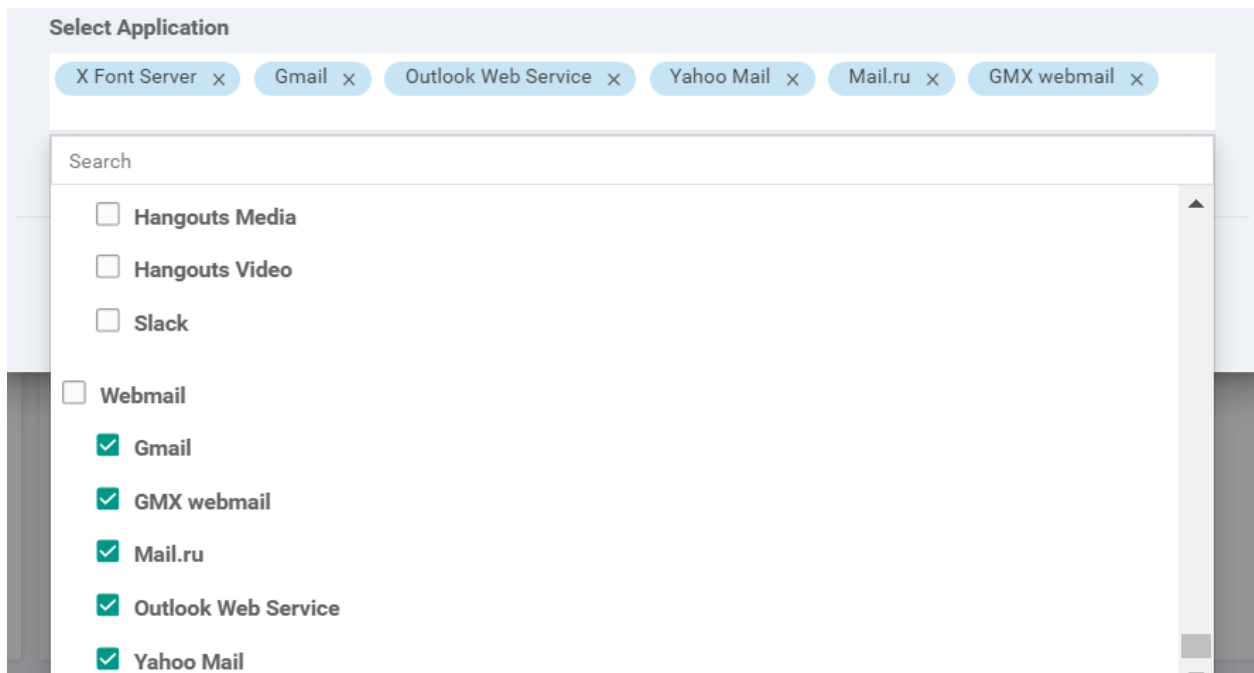
The screenshot shows the Cisco vManage GUI with the 'CONFIGURATION | SECURITY' page. A dropdown menu 'Custom Options' is open, showing a list of security features. The 'Lists' option is highlighted with a red box. Below the dropdown, a table displays security policies.

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

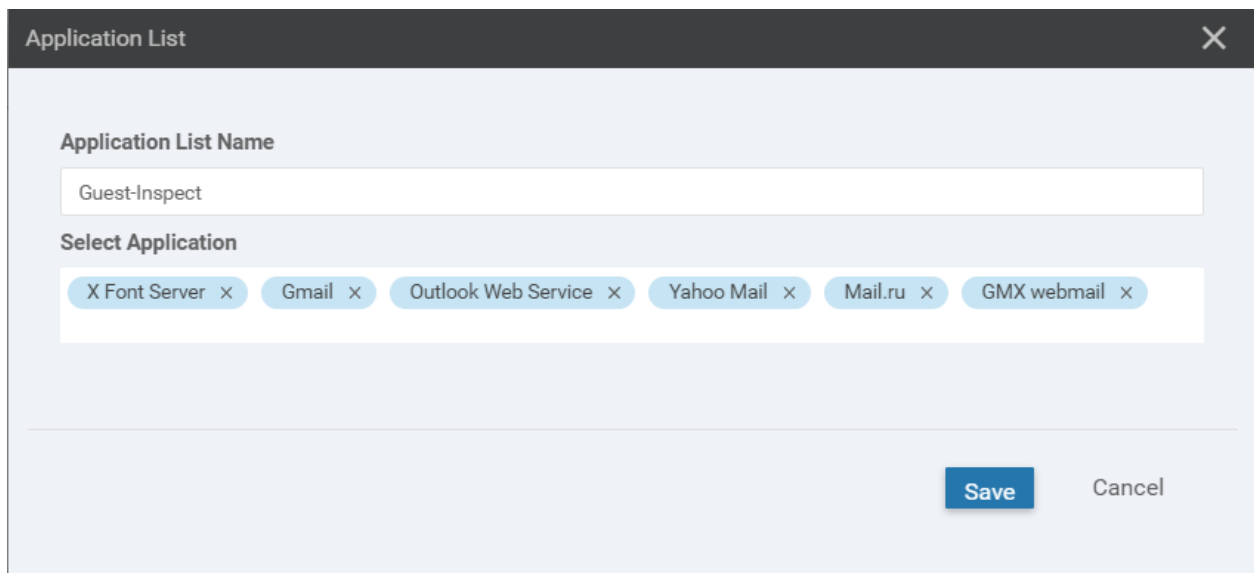
2. Identify the *Guest-Inspect* Application List and click on the **pencil** icon on the right-hand side to edit it. Under **Select Application**, check **X Font Server** (or any application that you want, this is a dummy entry)



3. Scroll down the list and **uncheck** Webmail, but check all the other Applications under Webmail



4. Click outside the box and choose to **Save** the Application List. Click on **Activate**, if prompted. Click on **Next** followed by **Configure Devices**



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

Total Rows: 6

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 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 SI...	Feature	vEdge Cloud	15	1	admin	05 Jun 2020 9:57:40 PM ...	In Sync	...

Edit
View
Delete
Copy
Attach Devices
Detach Devices
Export CSV
Change Device Values

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: Choose...

Global Template *: Factory_Default_Global_CISCO_Template

Cisco Banner: Choose...

Cisco SNMP: Choose...

CLI Add-On Template: Choose...

Policy: QoS_Policy

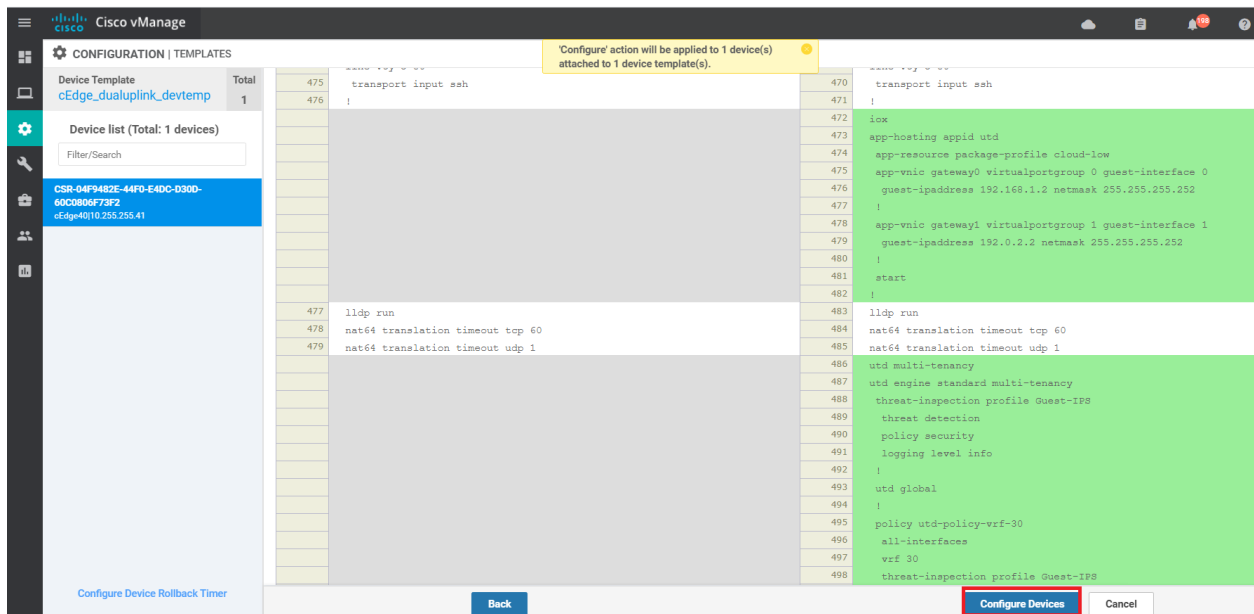
Probes: Choose...

Security Policy: Guest-FW-IPS-DIA

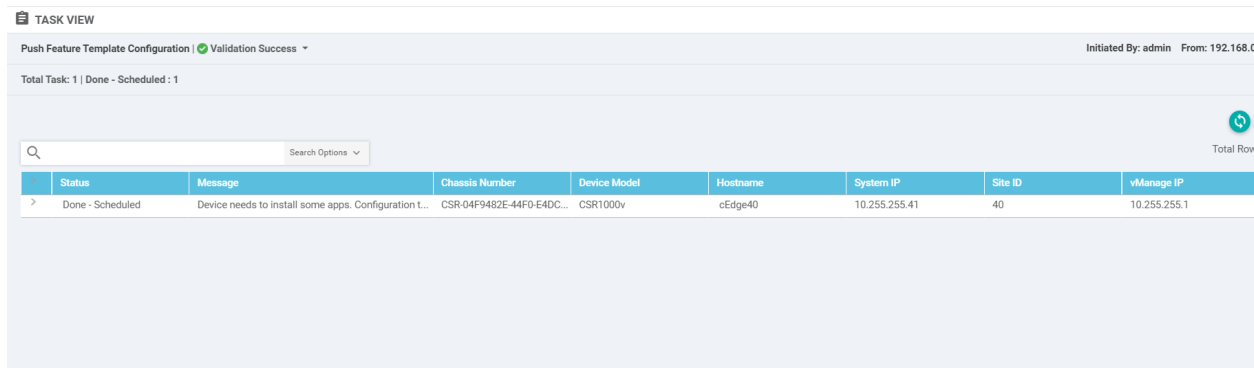
Container Profile *: Factory_Default_UTD_Template ⓘ

Update Cancel

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



8. 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



9. 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)

CONFIGURATION | DEVICES

WAN Edge List Controllers

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

Search Options

Device Model	Chassis Number	Hostname	System IP	Mode	Assigned Template	Device Status	Valid
CSR1000v	CSR-44C7CE5A-4149-E696-C8A8-415C...	--	--	CLI	--		valid
CSR1000v	CSR-D6DB39FC-C383-BB55-7E9D-7CD...	--	--	CLI	--		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	--		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	--		valid
CSR1000v	CSR-04F9482E-44F0-E4DC-D30D-60C0...	cEdge40	10.255.255.41	vManage	cEdge_dualuplink_devtemp	Service Install Pending - D...	valid
vEdge Cloud	e474c5fd-8ce7-d376-7cac-ba950b2e91...	DC-vEdge1	10.255.255.11	vManage	DCvEdge_dev_temp	In Sync	valid
vEdge Cloud	0cdd4f0e-f2f1-fe75-866c-469966cda1c3	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	--		valid
CSR1000v	CSR-F960E020-B7C9-887F-46A8-F4537...	--	--	CLI	--		valid
CSR1000v	CSR-25925FBC-07F3-0732-E127-EA95...	--	--	CLI	--		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

1. 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	--		ve
CSR1000v	CSR-D6DB39FC-C383-BB55-7E9D-7CD...	--	--	CLI	--		ve
CSR1000v	CSR-834E40DC-E358-8DE1-0E81-76E59...	cEdge50	10.255.255.51	vManage	cEdge-single-uplink	In Sync	ve
CSR1000v	CSR-D405F5BA-B975-8944-D1A3-2E08...	--	--	CLI	--		ve
CSR1000v	CSR-D1837F36-6A1A-1850-7C1C-E1C6...	cEdge51	10.255.255.52	vManage	cEdge-single-uplink	In Sync	ve
CSR1000v	CSR-5E992295-1362-0DB6-EEF8-25CC...	--	--	CLI	--		ve
CSR1000v	CSR-04F9482E-44F0-E4DC-D30D-60C0...	cEdge40	10.255.255.41	vManage	cEdge_dualuplink_devtemp	In Sync	ve
vEdge Cloud	e474c5fd-8ce7-d376-7cac-ba950b2c91...	DC-vEdge1	10.255.255.11	vManage	DCvEdge_dev_temp	In Sync	ve
vEdge Cloud	0cdd4f0e-f2f1-fe75-866c-469966cda1c3	DC-vEdge2	10.255.255.12	vManage	DCvEdge_dev_temp	In Sync	ve
vEdge Cloud	b7fd7295-58df-7671-e914-6fe2edff1609	vEdge20	10.255.255.21	vManage	vEdge_Site20_dev_temp	In Sync	ve
vEdge Cloud	dde90ff0-dc62-77e6-510f-08d96608537d	vEdge21	10.255.255.22	vManage	vEdge_Site20_dev_temp	In Sync	ve
vEdge Cloud	17026153-f09e-be4b-6dce-482fce43aa...	vEdge30	10.255.255.31	vManage	vEdge30_dev_temp	In Sync	ve
CSR1000v	CSR-26217DA0-1B63-8DDE-11C9-125F...	--	--	CLI	--		ve
CSR1000v	CSR-F960E020-B7C9-887F-46A8-F4537...	--	--	CLI	--		ve

2. 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
```

3. 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


```
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

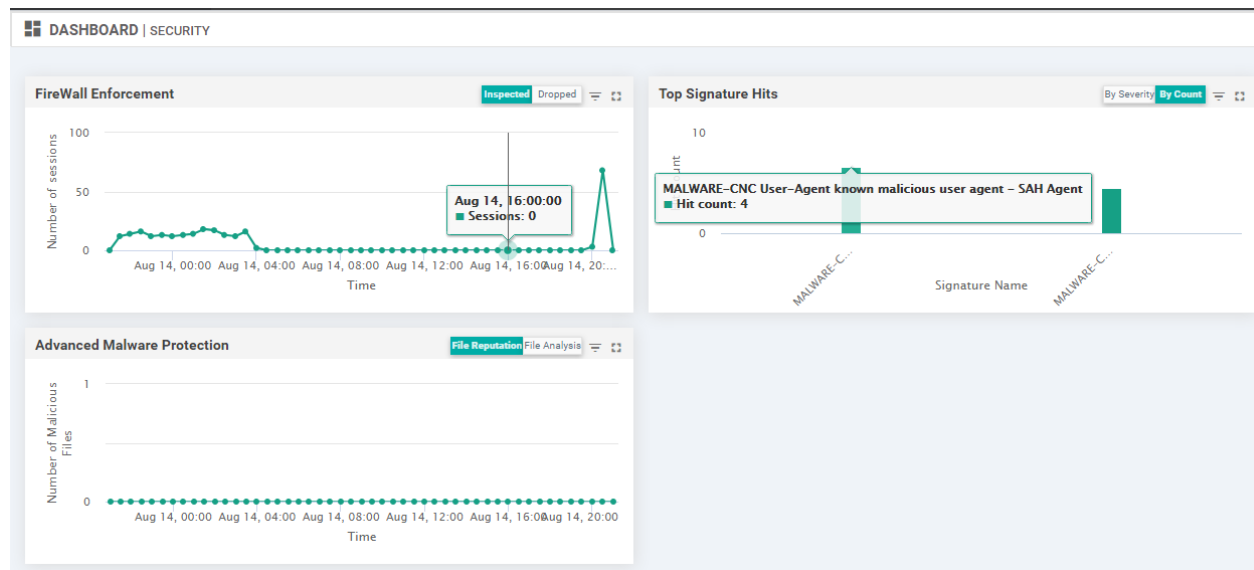
```
sdwan@10-40-30-21:~$ ./ips.sh
Triggering IPS Signatures
Task 1/3
Task 2/3
Task 3/3
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*Tasks Completed
sdwan@10-40-30-21:~$
```

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] {TC
P} 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 Custom Options


Add Security Policy 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	View Preview Edit Delete

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.

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

- Create New
- Copy from Existing

3. Click on **Target VPNs** and enter a Target VPN of 30. Click on **Save Changes**

Edit Target VPNs ✕

VPNs

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

Web Categories

Web Reputation

Advanced ▾

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 i

Content Body

Redirect URL i

Alerts and Logs i

Alerts Blacklist Whitelist Reputation/Category

6. Make sure the *URLF-NoShopping* URL Filtering policy shows up and click on **Save Policy Changes**

Search Options ▾

Name	Type	Reference Count	Updated By
URLF-NoShopping	urlFiltering	0	admin

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-14P1482E-14F0-E4DC-D30D-60C0806F73F2
cEdge4010.235.255.41

Configure Device Rollback Timer

```

485 nat64 translation timeout udp 1
486 utd multi-tenancy
487 utd engine standard multi-tenancy
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
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-vrf-30
496 all-interfaces
497 vrf 30
498 threat-inspection profile Guest-IPS

```

```

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

```

Back
Configure Devices
Cancel

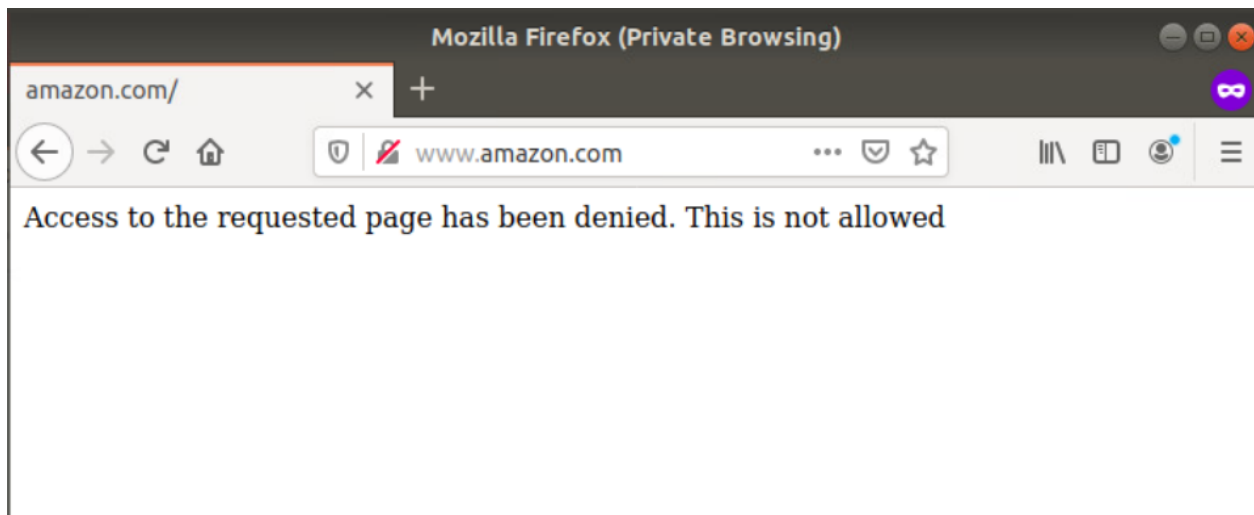
Task List

- ~~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 sdwan-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**

Virtual image uploaded successfully

Software Images **Virtual Images**

Upload Virtual Image Add Custom VNF Package

Search Options

Software Version	Software Location	Network Function Type	Image Type	Architecture	Version Type Name	Vendor
3.0.0	vmanage		Container	x86_64	sdavc_container	Cisco Syst
	vmanage	App-Hosting	Lxc	x86_64	Security Application	Cisco Syst

Administration

- Settings
- Manage Users
- Cluster Management**
- Integration Management
- Disaster Recovery
- VPN Groups
- VPN Segments

2. Click on the three dots next to **vmanage** and click on **Edit**

Service Configuration Service Reachability

Add vManage

Click hostname or status icon for more information

Normal Warning Error Disabled

Hostname	IP Address	Status	Application Server	Statistics Database	Configuration Database	Messaging Server	SD-AVC	UUID	
localhost	localhost	Ready	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	dfea63a5-66d2-4e50-a07...	...

Device Connected

- Edit**
- Remove

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**

Edit vManage

vManage IP Address
100.100.100.2

Username
admin

Password
.....

Select Services

- Application Server
- Statistics Database
- Configuration Database
- Messaging Server
- SD-AVC

Update Cancel

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

! Inorder to apply these changes the device will need to be rebooted.

Do you want to make these changes?

Reboot Time = 10 minutes

OK Cancel



5. 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

Service Configuration Service Reachability

[Add vManage](#)

Click hostname or status icon for more information ✔ No

Hostname	IP Address	Status	Application Server	Statistics Database	Configuration Database	Messaging Server	SD-AVC
vmanage	100.100.100.2	Ready	✔	✔	✔	✔	✔

6. 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

```
133 : 1300
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
```


- 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)

CONFIGURATION | POLICIES

Centralized Policy **Localized Policy** Custom Options

Add Policy Search Options Total Rows: 2

Name	Description	Devices Attached	Device Templates	Updated By	Last Updated	
Policer-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	...

View
Preview
Copy
Edit
Delete

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 Non-Default Search Options Total Rows: 7

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
DCvEdge_dev_temp	Device template for the DC-v...	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-singleuplink	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 vSmarts	Feature	vSmart	9	2	admin	25 May 2020 10:13:06 AM P...	In Sync	...
vEdge30_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	...

Edit 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 i

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 displays the Cisco SD-AVC monitoring interface. The main content area is titled "All Devices" and shows a "Summary" section with the following metrics:

- Classification Score: 67%
- First Packet Classification: 80%
- Total Usage: 10.52 KB
- SD-AVC Coverage Ratio: 0%
- Asymmetry Index: 0 / 10

Below the summary is a "Timeline" graph showing "Total (bps)" bandwidth usage from 08:55 to 09:05. The usage starts at 0 and increases to approximately 180 bps.

At the bottom, a table lists applications with their usage and business relevance:

Application	Usage	Business Relevance
Interior Gateway Routing Protocol	61.85% (6.50 KB)	relevant
HTTP	25.89% (2.72 KB)	default

On the right side, the "SD-AVC Monitoring" panel shows 1 Segment and 1 Device. The "Devices" section is highlighted with a red box, showing 1 device with a warning icon. Below it, the "Connectors" section shows "Cloud Connector" with a power icon, and the "Installed Protocol Packs" section shows "Protocol Pack 47.0".

System Time: 2020-06-07 09:07
Uptime: 14 minutes
About
© 2020 Cisco Systems, Inc.

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

← cEdge40 (Device) Change

Summary

Classification Score	First Packet Classification	Total Usage	SD-AVC Coverage Ratio	Asymmetry Index
67% ▼ -33%	80% ▲ 1000%	10.52 KB ▲ 1000%	0% ▲ 0%	0 / 10

Timeline

Bandwidth

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.

- 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

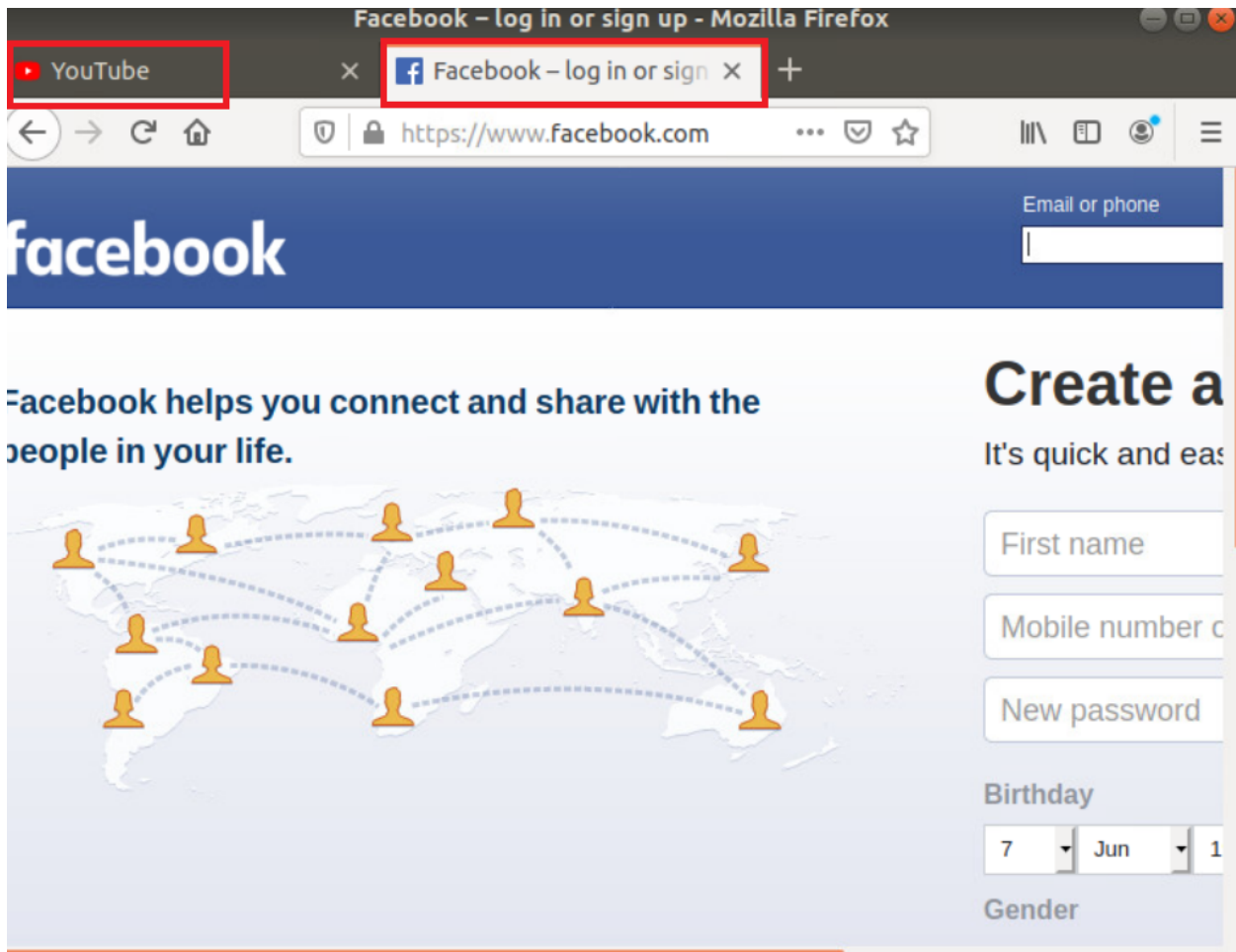
cEdge40#
```

```
show avc sd-service info summary
```

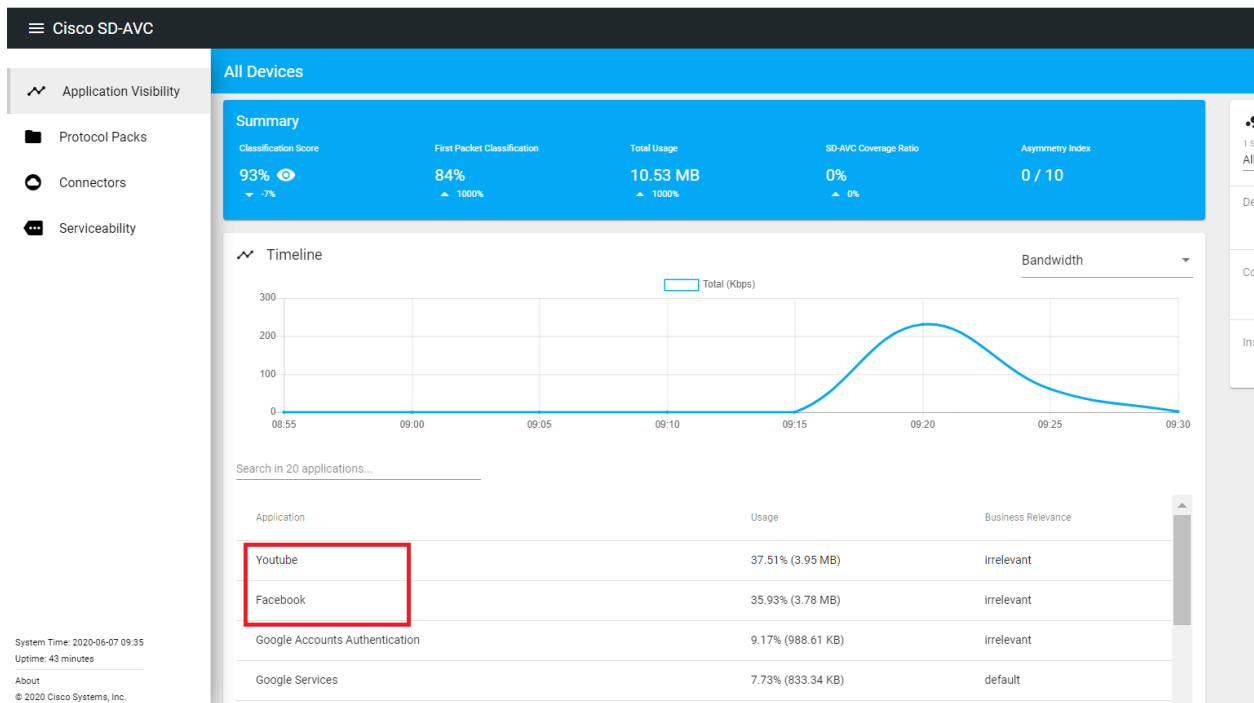
4. We can also run `show avc sd-service info connect` to view detailed information about the connection to the Controller

```
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
Not valid : 0
```

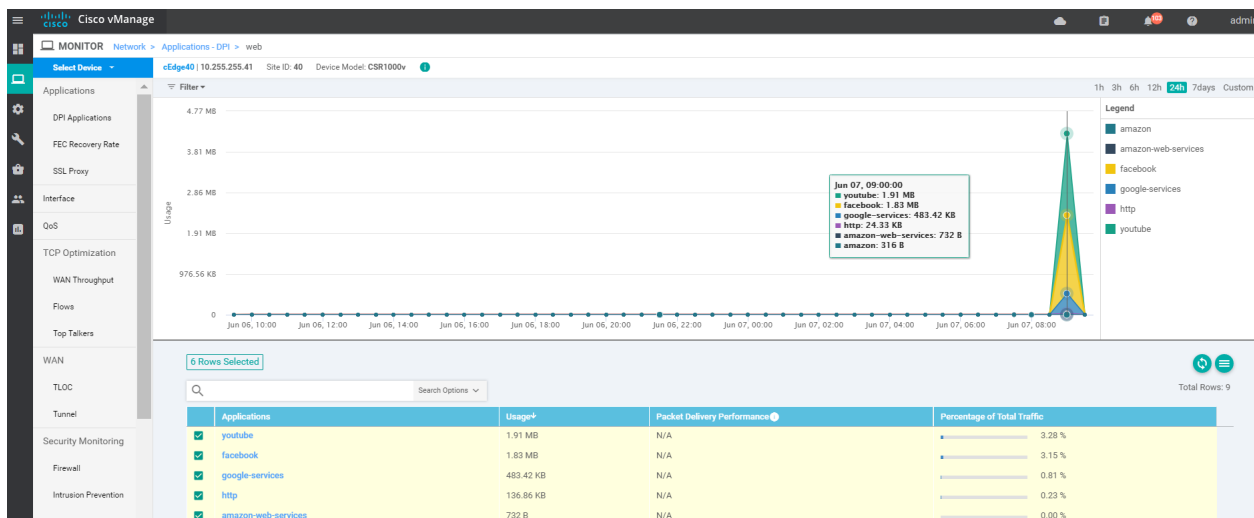
5. Log in to the Site40 PC by accessing vCenter (use the bookmark or access 10.2.1.50/ui). Log in using the credentials provided and click on the sdwan-slc/ghi-site40pc-podX. Click on the console icon to open a Web Console. Open Firefox and go to youtube.com and facebook.com. For good measure, open about 4 tabs of these sites



6. 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



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



Configuring AMP and TLS/SSL Proxy

Summary: Configuring Advanced Malware Protection and TLS/SSL Proxy.

Table of Contents

- [Overview](#)
- [Pre-Work and Testing](#)
- [Initial Configuration](#)
 - [Configuring NTP and DNS](#)
 - [Setting up vManage as the CA](#)
- [Enabling AMP and Testing](#)
- [Configuring the Decryption Policy](#)
- [Activity Verification](#)

Task List

- Overview
- Pre-work and Testing
- Initial Configuration
 - Configuring NTP and DNS
 - Setting up vManage as the CA
- Enabling AMP and Testing
- Configuring the Decryption Policy
- Activity Verification

Overview

Starting with IOS-XE 17.2.1r, the cEdges can function as transparent TLS/SSL Proxy devices. Encrypted traffic can be decrypted by the cEdge which is then analyzed by the Unified Threat Defense (UTD) engine to identify risks hidden in encrypted traffic. Some of the benefits of a TLS Proxy are:

- Transparent inspection of encrypted traffic for threats
- Threat and Malware protection for TLS traffic
- Security Policy enforcement on decrypted traffic

TLS proxy devices act as a man-in-the-middle (MitM) to decrypt encrypted TLS traffic traveling across the WAN, and send it to UTD for inspection. TLS Proxy thus allows devices to identify risks that are hidden by end-to-end encryption over TLS channels. The data is re-encrypted post inspection before being sent to its final destination.

Task List

- [Overview](#)
- [Pre-work and Testing](#)
- [Initial Configuration](#)
 - [Configuring NTP and DNS](#)
 - [Setting up vManage as the CA](#)
- [Enabling AMP and Testing](#)
- [Configuring the Decryption Policy](#)
- [Activity Verification](#)

Pre-Work and Testing

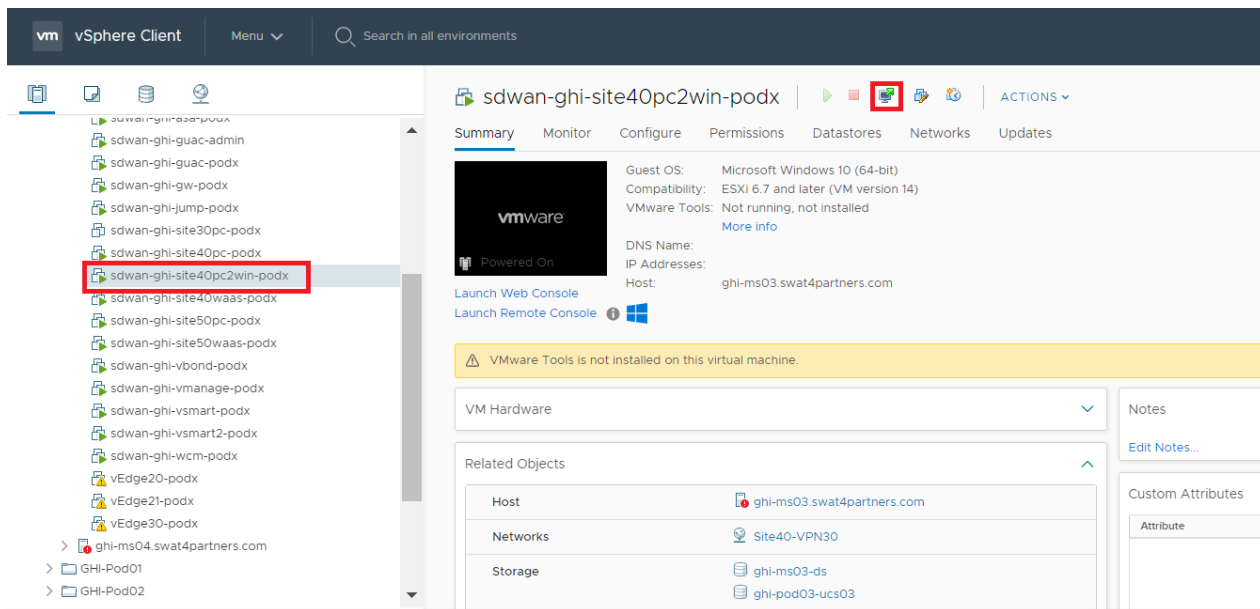
We will first perform some initial testing without AMP and TLS/SSL Proxy functionality enabled.

1. Log in to vCenter (10.2.1.50/ui if connected to the GHI DC and 10.1.1.50/ui if connected to the SJC DC) via the saved bookmark using the username/password for your POD. Locate the *sdwan-sjc/ghi-site40pc2win-podX* VM and click on it. Click on the console icon to open a console session to the PC (choose Web Console if prompted)

Username	Password
sdwanpodX	C1sco12345

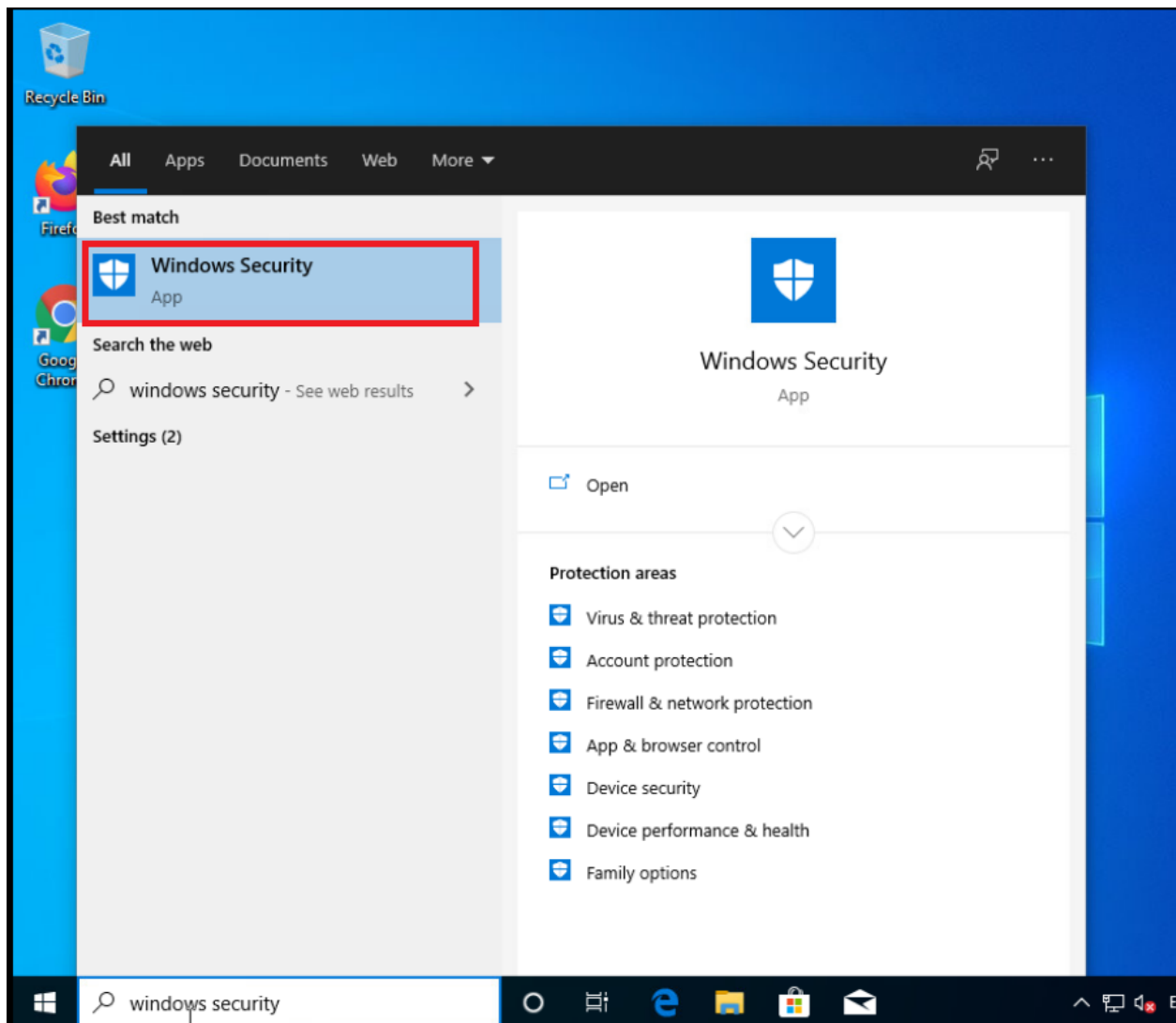
where X is your POD number

e.g. sdwanpod5

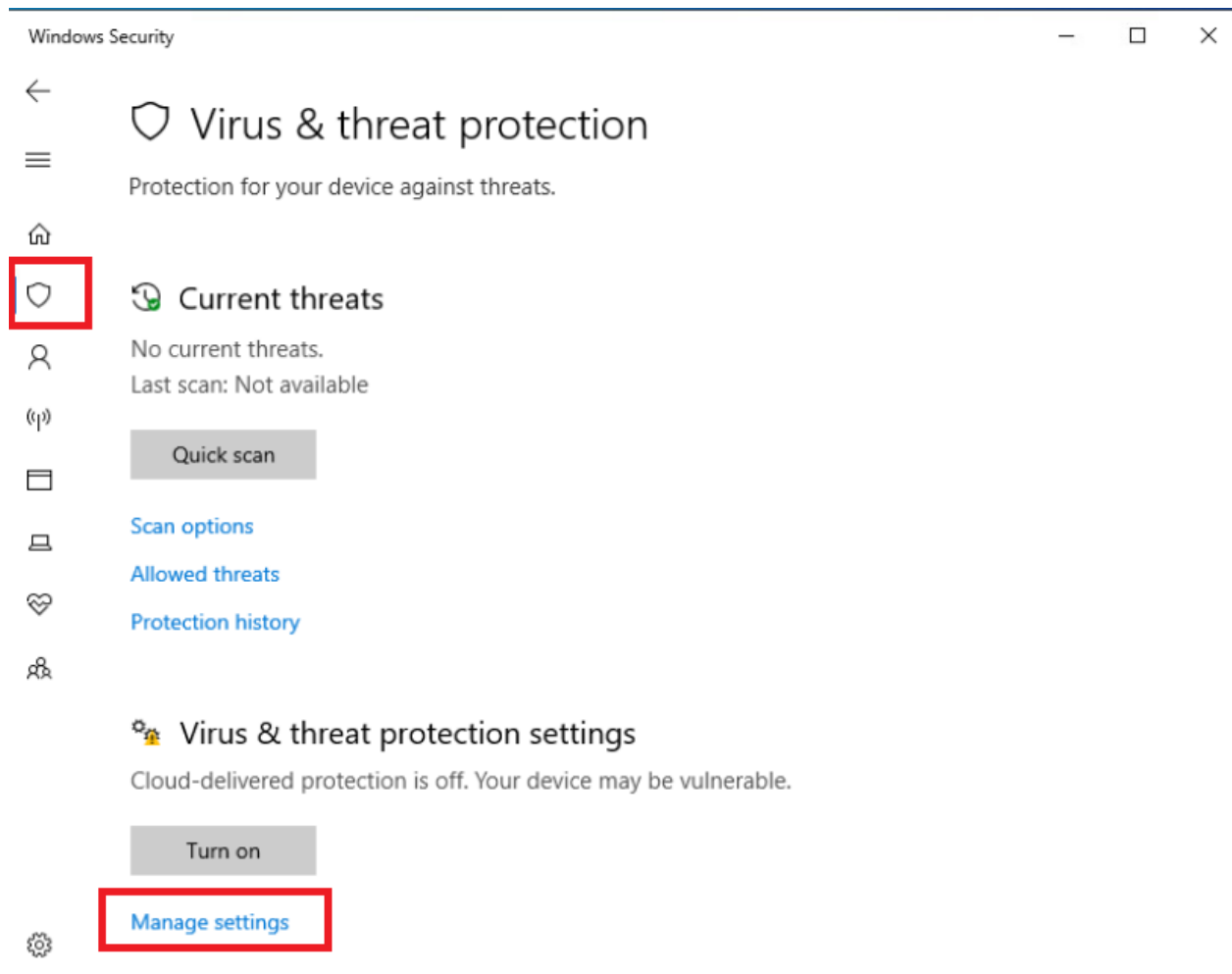


2. Log in to the Windows PC at Site 40 and click on **Start**. Search for *Windows Security* and click on the **Windows Security** icon

Username	Password
admin	C1sco12345



3. Click on the *Virus and Threat Protection* icon on the left hand side and then on *Manage Settings*



4. Set the **Real-Time Protection** slider to the *Off* position. If this PC is rebooted, the slider will need to be set to *Off* again



Virus & threat protection settings



View and update Virus & threat protection settings for Windows Defender Antivirus.



Real-time protection



Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.



On


Set this to Off



Cloud-delivered protection



Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

 Cloud-delivered protection is off. Your device may be [Dismiss](#) vulnerable.



5. Click on **Yes** to allow the changes. Real-time protection should now be off

User Account Control



Do you want to allow this app to make changes to your device?



Windows Security

Verified publisher: Microsoft Windows

[Show more details](#)

Yes

No




Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

 Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

6. Open Google Chrome and navigate to eicar.org/?page_id=3950 or use the **Malware Test** bookmark. Scroll down and click on the **eicar_com.zip** HTTPS download link. This will initiate a download of a sample malware file

from an unknown person is simply to decline politely.

A third set of requests come from exactly the people you might think would be least likely to want viruses „users of anti-virus software“. They want some way of checking that they have deployed their software correctly, or of deliberately generating a „virus incident in order to test their corporate procedures, or of showing others in the organisation what they would see if they were hit by a virus“.

Reasons for testing anti-virus software

Obviously, there is considerable intellectual justification for testing anti-virus software against real viruses. If you are an anti-virus vendor, then you do this (or should do it!) before every release of your product, in order to ensure that it really works. However, you do not (or should not!) perform your tests in a „real“ environment. You use (or should use!) a secure, controlled and independent laboratory environment within which your virus collection is maintained.

Using real viruses for testing in the real world is rather like setting fire to the dustbin in your office to see whether the smoke detector is working.

Download area using the standard protocol HTTP

– Sorry, HTTP download ist temporarily not provided. –

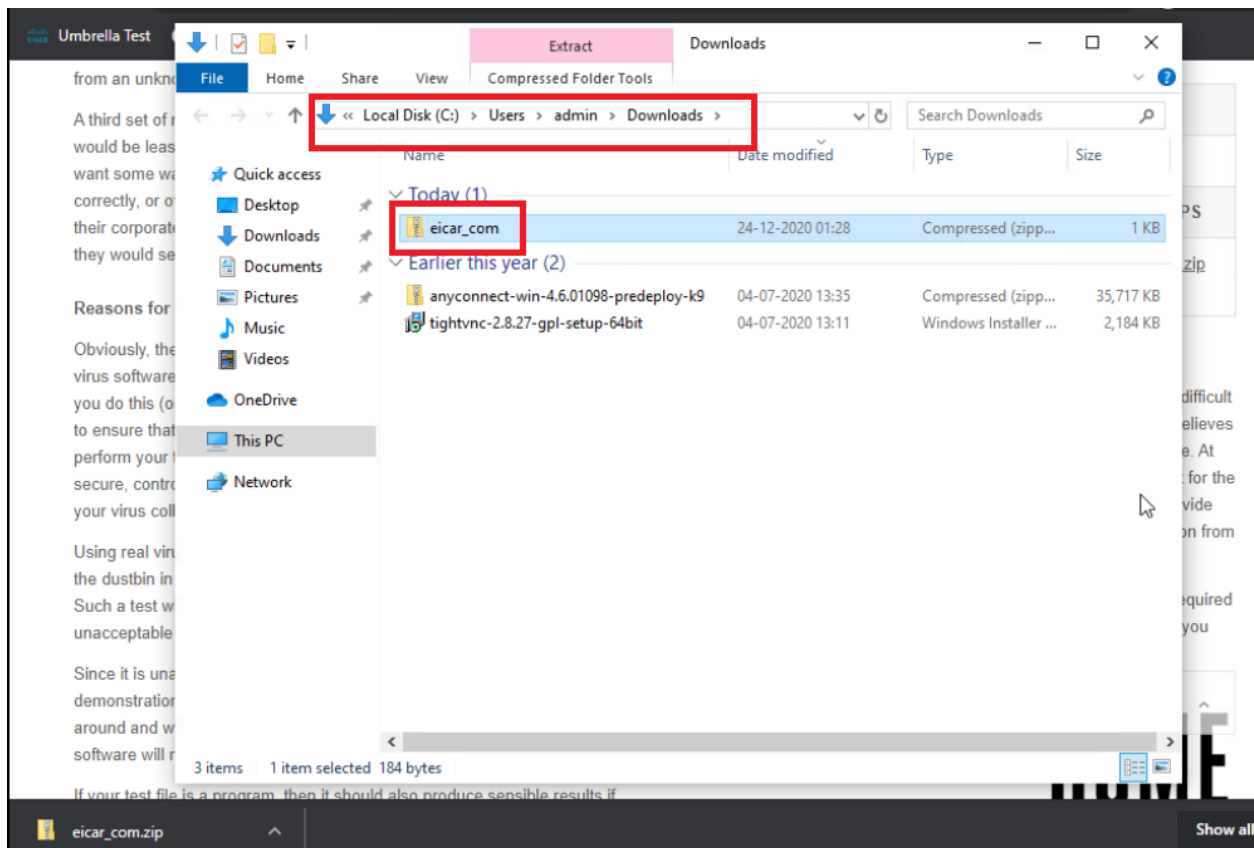
Download area using the secure, SSL enabled protocol HTTPS

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes
---------------------------------------	---	--	--

How to delete the test file from your PC

We understand (from the many emails we receive) that it might be difficult for you to delete the test file from your PC. After all, your scanner believes it is a virus infected file and does not allow you to access it anymore. At this point we must refer to our standard answer concerning support for the test file. We are sorry to tell you that EICAR cannot and will not provide AV scanner specific support. The best source to get such information from is the vendor of the tool which you purchased.

7. The download will go through and we should see the **eicar_com.zip** sample malware file in the Downloads folder. Delete the file (press Shift + Delete after clicking on the file to permanently delete it) since we will be performing this test multiple times



We thus saw that a known malware file was downloaded via HTTPS since:

- There is no malware protection mechanism in place
- The traffic is encrypted

Task List

- [Overview](#)
- [Pre-work and Testing](#)
- [Initial Configuration](#)
 - [Configuring NTP and DNS](#)
 - [Setting up vManage as the CA](#)
- [Enabling AMP and Testing](#)
- [Configuring the Decryption Policy](#)
- [Activity Verification](#)

Initial Configuration

SSL/TLS Proxy configuration requires a few pre-requisites to be in place. These are:

- TLS Proxy devices and the clients should have their times in sync
- A device will need to be set up as a CA. There are a few options: Enterprise CA, Enterprise CA with SCEP enabled, vManage as CA and vManage as an Intermediate CA
- Traffic flows must be symmetric and pinned to a particular link, if there are multiple links

We will be setting up the vManage as the CA, along with configuring NTP and DNS for our network.

Configuring NTP and DNS

1. Log in to the CLI of vManage via the saved session in Putty (or SSH to 192.168.0.6) using the username and password given below. Enter the commands enumerated here to update the DNS and NTP servers

Username	Password
admin	admin

```
vmanage(config)# system
vmanage(config-system)# ntp server pool.ntp.org
vmanage(config-server-pool.ntp.org)# exit
vmanage(config-ntp)# exit
vmanage(config-system)# exit
vmanage(config)# vpn 0
vmanage(config-vpn-0)# dns 8.8.8.8
vmanage(config-vpn-0)# dns 4.2.2.2 secondary
vmanage(config-vpn-0)# commit and-quit
Commit complete.
vmanage#
vmanage#
vmanage#
vmanage#
```

```
config t
system
ntp server pool.ntp.org
exit
exit
exit
vpn 0
dns 8.8.8.8
dns 4.2.2.2 secondary
commit and-quit
```

2. Run `show ntp assoc` after a few seconds to verify that the vManage is now sync'd to pool.ntp.org

```
vmanage#
vmanage# show ntp assoc
```

IDX	ASSOCID	STATUS	CONF	REACHABILITY	AUTH	CONDITION	LAST EVENT	COUNT
1	38257	961a	yes	yes	none	sys.peer	sys_peer	1

```
vmanage#
```

3. Log in to the vManage GUI by using the bookmark in Chrome (or by going to 192.168.0.6 via a browser). Navigate to **Configuration => Templates** and head over to the **Feature** tab. Click on **Add Template**



2 ↑

Smart - 2



8 ↑

WAN Edge - 8

Configuration

Devices

TLS/SSL Proxy

Certificates

Network Design

Templates

Policies

Security

Unified Communications

Cloud onRamp for SaaS

Cloud onRamp for IaaS

Cloud OnRamp for Multi-Cloud

Templates

10

0

0

20

20

8

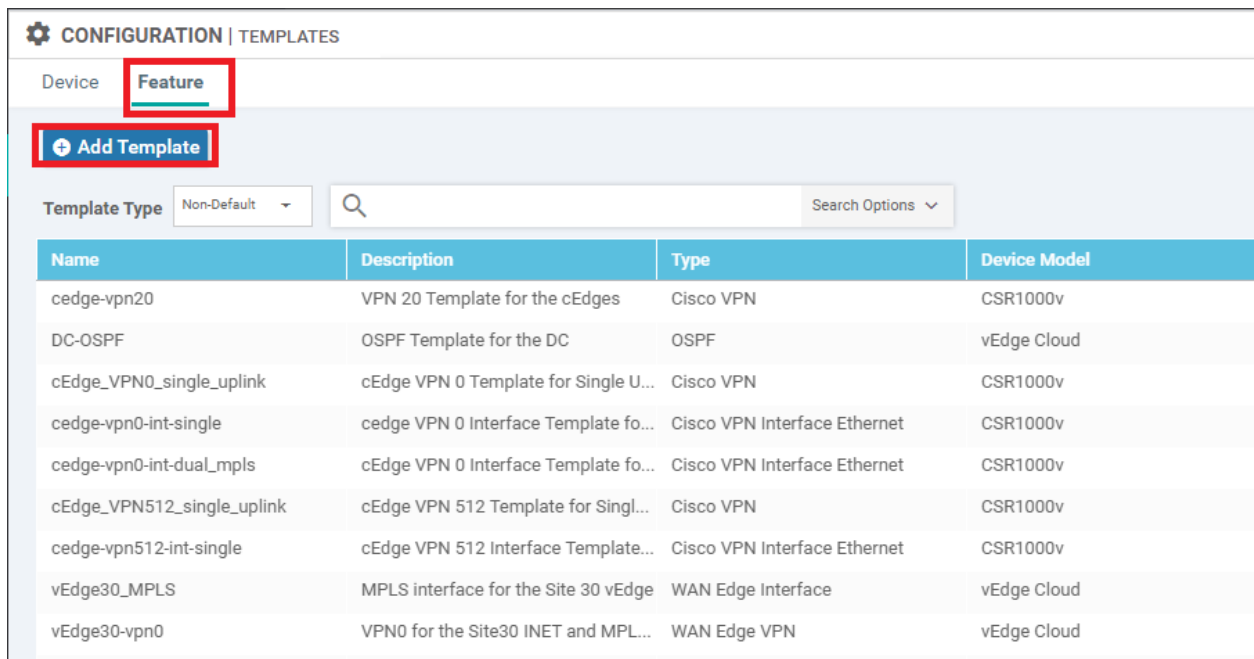
0



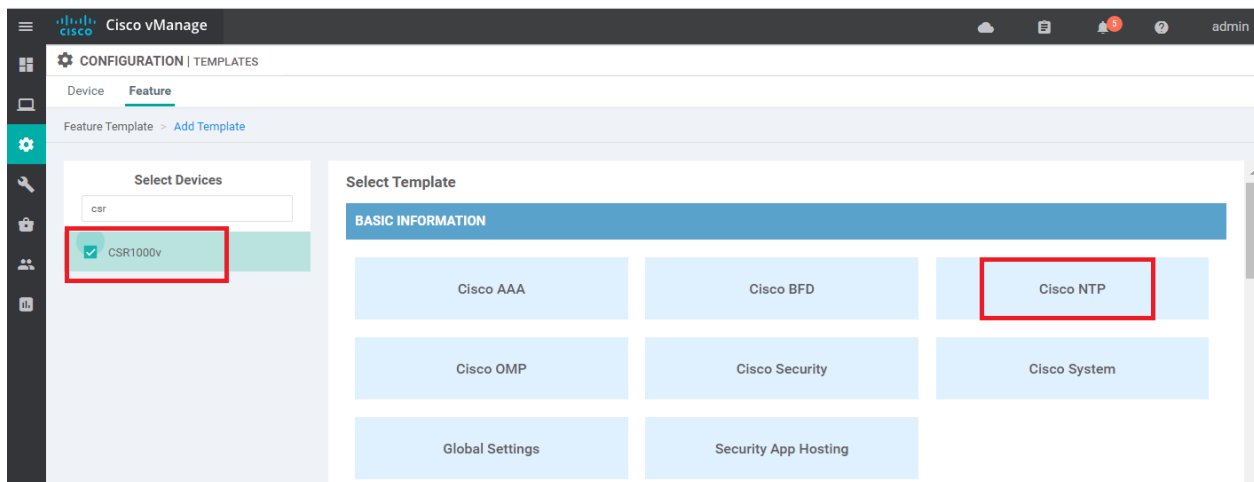
Si

W

A



4. Search for *csr* and select the **CSR1000v** device. Click on **Cisco NTP** to create an NTP Feature Template for the cEdges



5. Populate the name and description per the table given below and click on **New Server**. Enter the details as per the table, screenshot given for reference. Click on **Add** once all the server details have been populated and then click on **Save** to save the template

Section	Field	Global or Device Specific (drop down)	Value

Template Name			<i>cedge40-ntp</i>
Description			<i>NTP Template for cEdge40</i>
Server	Hostname/IP Address	Global	pool.ntp.org
Server	Source Interface	Global	GigabitEthernet2

Feature Template > Add Template > Cisco NTP

Template Name: 1

Description: 1

Server Master Authentication

SERVER

2

Mark as Optional Row

Hostname/IP Address: 3

Authentication Key ID:

VPN ID:

Version:

Source Interface: 4

Prefer: On Off

5

6

6. At the **Feature Templates** tab, locate the *cEdge_VPN0_dual_uplink* template 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: vpn0

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
cEdge_VPN0_single_upl...	cEdge VPN 0 Template for ...	Cisco VPN	CSR1000v	1	2	admin	20 Aug 2020 8:22:25 A...
cEdge-vpn0-int-single	cEdge VPN 0 Interface Tem...	Cisco VPN Interface Eth...	CSR1000v	1	2	admin	20 Aug 2020 8:26:09 A...
cEdge-vpn0-int-dual_mpls	cEdge VPN 0 Interface Tem...	Cisco VPN Interface Eth...	CSR1000v	1	1	admin	31 Aug 2020 3:09:06 A...
vEdge30-vpn0	VPN0 for the Site30 INET a...	WAN Edge VPN	vEdge Cloud	1	1	admin	24 Aug 2020 2:37:32 A...
Site20-vpn0	VPN0 for the Site 20 vEdges	WAN Edge VPN	vEdge Cloud	2	2	admin	24 Aug 2020 10:35:30 P...
DCvEdge-vpn0	VPN0 for the DC-vEdges IN...	WAN Edge VPN	vEdge Cloud	1	2	admin	24 Aug 2020 1:59:31 A...
cEdge_VPN0_dual_uplink	cEdge VPN 0 Template for ...	Cisco VPN	CSR1000v	1	1	admin	24 Aug 2020 2:46:30 A...
cEdge-vpn0-int-dual	cEdge VPN 0 Interface Tem...	Cisco VPN Interface Eth...	CSR1000v	1	1	admin	31 Aug 2020 8:26:09 A...
Site20_vpn0_int	VPN0 Interface for Site20 d...	WAN Edge Interface	vEdge Cloud	1	1	admin	24 Aug 2020 10:35:30 P...
vSmart-VPN0	VPN0 Template for the vs...	vSmart VPN	vSmart	1	2	admin	24 Aug 2020 2:37:32 A...
vSmart-VPN0-int	VPN0 Interface for vSmarts	vSmart Interface	vSmart	1	2	admin	24 Aug 2020 10:35:30 P...
cEdge-vpn0-int-dual	cEdge VPN 0 Interface Tem...	Cisco VPN Interface Eth...	CSR1000v	1	1	admin	31 Aug 2020 8:26:09 A...

Total Rows: 13 of 44

More menu options: View, Edit, Change Device Models, Delete, Copy

7. Populate the **Primary DNS Address** and **Secondary DNS Address** as 8.8.8.8 and 4.2.2.2 respectively. Click on **Update**

DNS

IPv4 | IPv6

Primary DNS Address (IPv4): 8.8.8.8

Secondary DNS Address (IPv4): 4.2.2.2

New Host Mapping

Optional	Hostname	List of IP Addresses (Maximum: 8)
----------	----------	-----------------------------------

Update | Cancel

8. Click on **Next** and **Configure Devices**. You can choose to view the side by side configuration if needed

CONFIGURATION | TEMPLATES

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

Device Template: **cedge_dualuplink_devtemp** Total: 1

Device list (Total: 1 devices)

Filter/Search

CSR-04F9A82E-44F0-E4DC-D30D-60C0806F73F2
cEdge4010.255.255.41

215	!	215	!
216	!	216	!
217	ip arp proxy disable	217	ip arp proxy disable
218	no ip finger	218	no ip finger
219	no ip rcmd rcp-enable	219	no ip rcmd rcp-enable
220	no ip rcmd rsh-enable	220	no ip rcmd rsh-enable
221	no ip domain lookup	221	no ip dhcp use class
222	no ip dhcp use class	222	ip name-server 4.2.2.2 8.8.8.8
223	ip name-server vrf 10 10.2.1.5 10.2.1.6	223	ip name-server vrf 10 10.2.1.5 10.2.1.6
224	ip name-server vrf 20 10.2.1.5 10.2.1.6	224	ip name-server vrf 20 10.2.1.5 10.2.1.6
225	ip name-server vrf 30 10.2.1.5 10.2.1.6	225	ip name-server vrf 30 10.2.1.5 10.2.1.6
226	ip route 0.0.0.0 0.0.0.0 100.100.100.1	226	ip route 0.0.0.0 0.0.0.0 100.100.100.1
227	ip route 0.0.0.0 0.0.0.0 192.1.2.17	227	ip route 0.0.0.0 0.0.0.0 192.1.2.17
228	ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 192.168.0.1	228	ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 192.168.0.1
229	ip bootp server	229	ip bootp server
230	no ip source-route	230	no ip source-route
231	ip access-list extended Guest-FW_concat-seq-Inspect_Web_A pp_Guest-acl_	231	ip access-list extended Guest-FW_concat-seq-Inspect_Web_A pp_Guest-acl_
232	11 permit object-group Guest-FW_concat-seq-Inspect_Web_A pp_Guest-service-og_ object-group Guest-Site40 any	232	11 permit object-group Guest-FW_concat-seq-Inspect_Web_A pp_Guest-service-og_ object-group Guest-Site40 any
233	!	233	!

Configure Device Rollback Timer

Back **Configure Devices** Cancel

9. Go to **Configuration => Templates** and locate the *cedge_dualuplink_devtemp* Device Template. Click on the three dots next to it and choose to **Edit** the template

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
vEdge_Site20_dev_temp	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:3...	In Sync
cEdge-single-uplink	Single Uplink cE...	Feature	CSR1000v	17	2	admin	24 Aug 2020 6:16...	In Sync
cedge_dualuplink_devtemp	cedge Device Te...	Feature	CSR1000v	20	1	admin	31 Aug 2020 4:30...	In Sync
DCvEdge_dev_temp	Device template ...	Feature	vEdge Cloud	16	2	admin	25 Aug 2020 6:00...	In Sync
vEdge30_dev_temp	Device template ...	Feature	vEdge Cloud	15	1	admin	24 Aug 2020 5:52...	In Sync
vSmart-dev-temp	Device Template...	Feature	vSmart	9	2	admin	24 Aug 2020 3:03...	In Sync
vEdge_Site20_dev_temp_nat	Device template ...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:4...	In Sync

Edit

- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

10. Click on **Cisco NTP** to add an NTP Feature Template and populate the *cedge40-ntp* template we created. Click on **Update**

Basic Information Transport & Management VPN Service VPN Additional Templates

Basic Information

Cisco System * Default_System_Cisco_V01

Cisco Logging* Default_Logging_Cisco_V01

Cisco NTP cedge40-ntp

Additional Cisco System Templates

- Cisco Logging
- Cisco NTP

Update Cancel

11. Click on **Next** and **Configure Devices**

CONFIGURATION | TEMPLATES

Device Template Total

cedge_dualuplink_devtemp 1

Device list (Total: 1 devices)

Filter/Search

CSR-04F9482E-44F0-E4DC-D30D-60C0806F73F2
cEdge4010.255.255.41

475	line con 0	475	line con 0
476	login authentication default	476	login authentication default
477	speed 19200	477	speed 19200
478	stopbits 1	478	stopbits 1
479	!	479	!
480	line vty 0 4	480	line vty 0 4
481	transport input ssh	481	transport input ssh
482	!	482	!
483	line vty 5 80	483	line vty 5 80
484	transport input ssh	484	transport input ssh
485	!	485	!
486	!	486	ntp server pool.ntp.org source GigabitEthernet2 version 4
487	!	487	ntp source GigabitEthernet2
488	iox	488	iox
489	app-hosting appid utd	489	app-hosting appid utd
490	app-resource package-profile cloud-low	490	app-resource package-profile cloud-low
491	app-vnic gateway0 virtualportgroup 0 guest-interface 0	491	app-vnic gateway0 virtualportgroup 0 guest-interface 0
492	guest-ipaddress 192.168.1.2 netmask 255.255.255.252	492	guest-ipaddress 192.168.1.2 netmask 255.255.255.252
493	!	493	!
494	app-vnic gateway1 virtualportgroup 1 guest-interface 1	494	app-vnic gateway1 virtualportgroup 1 guest-interface 1
495	guest-ipaddress 192.0.2.2 netmask 255.255.255.252	495	guest-ipaddress 192.0.2.2 netmask 255.255.255.252
496	!	496	!

Configure Device Rollback Timer

Back **Configure Devices** Cancel

12. Once the configuration is pushed successfully, log in via Putty to cEdge40 using the saved session (or SSH to 192.168.0.40) and issue a `show ntp assoc` to verify DNS resolution of the NTP server and a state of `sys.peer`

```
cEdge40#show ntp assoc
address      ref clock      st   when  poll reach  delay  offset  disp
*~162.159.200.123 10.35.14.16   3    7    64    1 84.948  1.208 188.48
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

This completes the DNS and NTP configuration required for TLS/SSL Proxy setup.

Task List

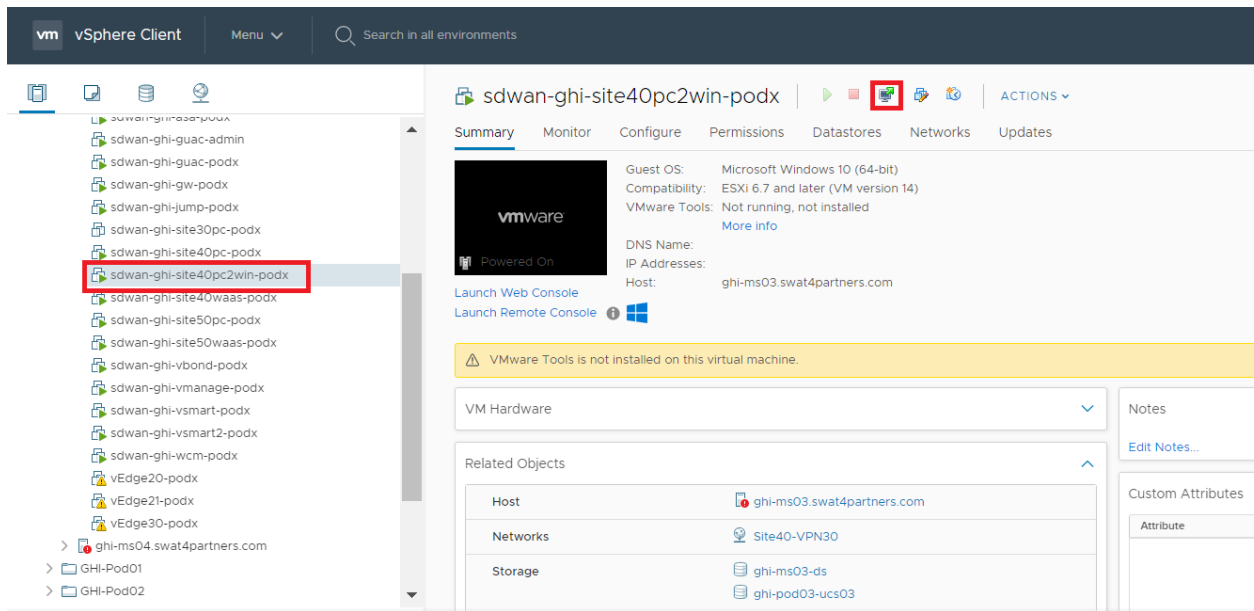
- ~~Overview~~
- ~~Pre-work and Testing~~
- Initial Configuration
 - ~~Configuring NTP and DNS~~
 - Setting up vManage as the CA
- Enabling AMP and Testing
- Configuring the Decryption Policy
- Activity Verification

Setting up vManage as the CA

We will now set up vManage as the CA and install the certificate on our client PC at Site 40.

1. Log in to vCenter (10.2.1.50/ui if connected to the GHI DC and 10.1.1.50/ui if connected to the SJC DC) via the saved bookmark using the username/password for your POD. Locate the *sdwan-sjc/ghi-site40pc2win-podX* VM and click on it. Click on the console icon to open a console session to the PC (choose Web Console if prompted)

Username	Password
sdwanpodX	C1sco12345
<i>where X is your POD number</i>	
e.g. sdwanpod5	



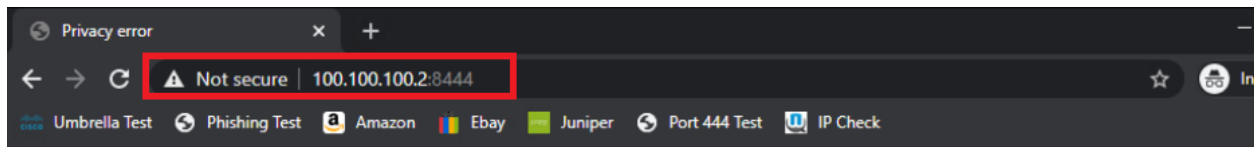
2. Log in to the Windows PC at Site 40 and open Google Chrome. Navigate to 100.100.100.2 and log in to vManage, after accepting any certificate errors

Site 40 PC2 credentials:

Username	Password
admin	C1sco12345

vManage credentials:

Username	Password
admin	admin



Access vManage via the IP 100.100.100.2 from the site40pc2win VM console



Your connection is not private

Attackers might be trying to steal your information from **100.100.100.2** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID



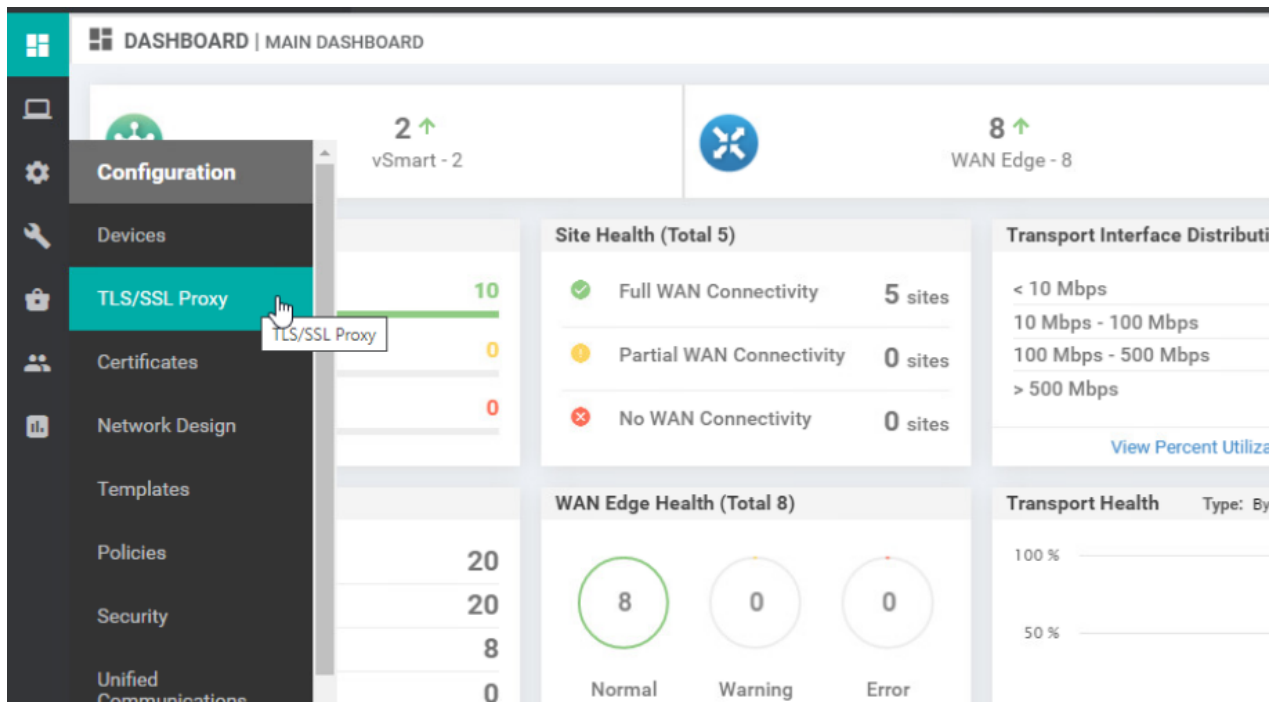
Hide advanced

Back to safety

This server could not prove that it is **100.100.100.2**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 100.100.100.2 \(unsafe\)](#)

3. Go to **Configuration => TLS/SSL Proxy**



4. Select **vManage as CA** and enter the details as per the following table. Click on **Save Certificate Authority**

Field	Value
Common Name	tlsproxy
Organization	swat-sdwanlab
Organizational Unit	Cisco
Locality	SJ
State/Province	CA
Country Code	US
Email	abc@cisco.com
Validity Period	10 years

Enterprise CA Recommended with SCEP Enabled
 Use this option to manage certificate issuance from an Enterprise CA. Best suited for Enterprises that have their own internal CA.

vManage As CA
 Use this option to manage certificate issuance from vManage. Best suited for Enterprises that do not own an internal CA.

Generate vManage Certificate
 Set vManage as Intermediate CA
 Use this option to delegate vManage as a CA to manage proxy device certificate issuance. Best suited for Enterprises that do not own their internal CA.

Common Name:
 Organization:
 Organizational Unit:
 Locality:
 State/Province: Country Code:

Email:
 Validity Period:

CSR Download
 Fill form and click button 'Save Certificate Authority'

Finger Print 1

1 Your TLS/SSL Proxy will be set incomplete until the certificate installation process and policy configuration is completed.
[View recommended steps to complete configuration for vManage as Root CA](#)

Save Certificate Authority

5. Click on **Download** and download the root certificate, which we will be installing on the Site 40 PC2 itself

View Root Certificate

Root Certificate 1 of 1 **tlsproxy_vmanage** Last Updated: 24 Dec 2020 10:29:37 UTC

Download
 tlsproxy_vmanage

```


[
  [
    Version: V3
    Subject: CN=tlsproxy, OU=Cisco, O=swat-sdwanlab, L=SJ, ST=CA, C=US
    Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

    Key: com.cisco.ciscossl.provider.ciscojce.trust.RSAPublicKeyImpl{
      2048 bits,
      modulus=dbbcd57beef6630031e464edfa353ef8b3ad8dbe8550b2d497a00db690f6cdfa7a05f4a390a45235dd2160f7b97c0a422b60f371a8c5c6cec73e2074ea140cb387
      524059dcb9917d19a1910f472454a690327c127b62fa69c6b87018cdad1d119fce141514d35214a0c773e6d7fe9c4cbaa8e48c86d43eaca2f156e15f4f7b043ba53cbeaffc2
      1448805ec5fa3500a7660fa4099418be9b2f27023122885cb722a06817cf74ee5a30d2bfdb00da977456428d483531b651bdef2c525db8a1433128faacc4ddcc58cc78746e
      be3678eab827740098942412e2c5745b82e62e1499ff40fe43b30643fee0d032fbd17fa3c6707bd2f15beca51d9d26a5158207d,
      public exponent=10001
    }
    Validity: [From: Thu Dec 24 10:29:37 UTC 2020,
      To: Tue Dec 24 10:29:37 UTC 2030]
    Issuer: CN=tlsproxy, OU=Cisco, O=swat-sdwanlab, L=SJ, ST=CA, C=US
    SerialNumber: [ ff54aec2 5dfea30d 00457a8d 1fdcb8a 66d07100 7e989463 13d7bfcf c5d0a1db]

    Certificate Extensions: 2
    [1]: ObjectId: 2.5.29.19 Criticality=true
    BasicConstraints:[
      CA:true
      PathLen:1
    ]
  ]
]
  
```


6. Click on **Start** on the Site 40 PC2 and search for *certificates*. Click on *Manage computer certificates*, which should open the Microsoft Management Console. Click on **Yes** to allow MMC to make changes

Best match

 **Manage user certificates** >
Control panel


Settings

 **Manage computer certificates** >


 **Manage file encryption certificates** >

Search the web

 certificate - See web results >


 certificate for aadhaar enrolment update form >


 certificate download >

 certificate online >

 certificate verification >

 certificate for aadhaar >


 certificate border >

 certificate border png images >

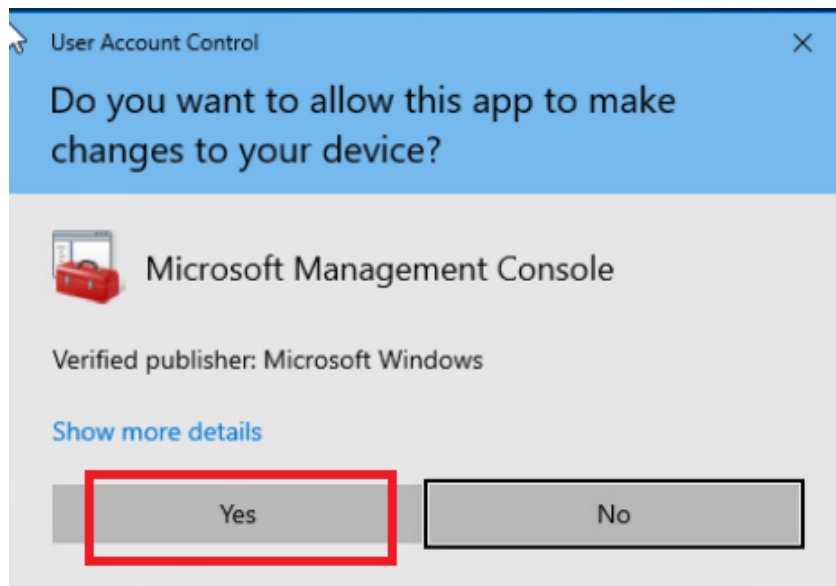


Manage computer certificates

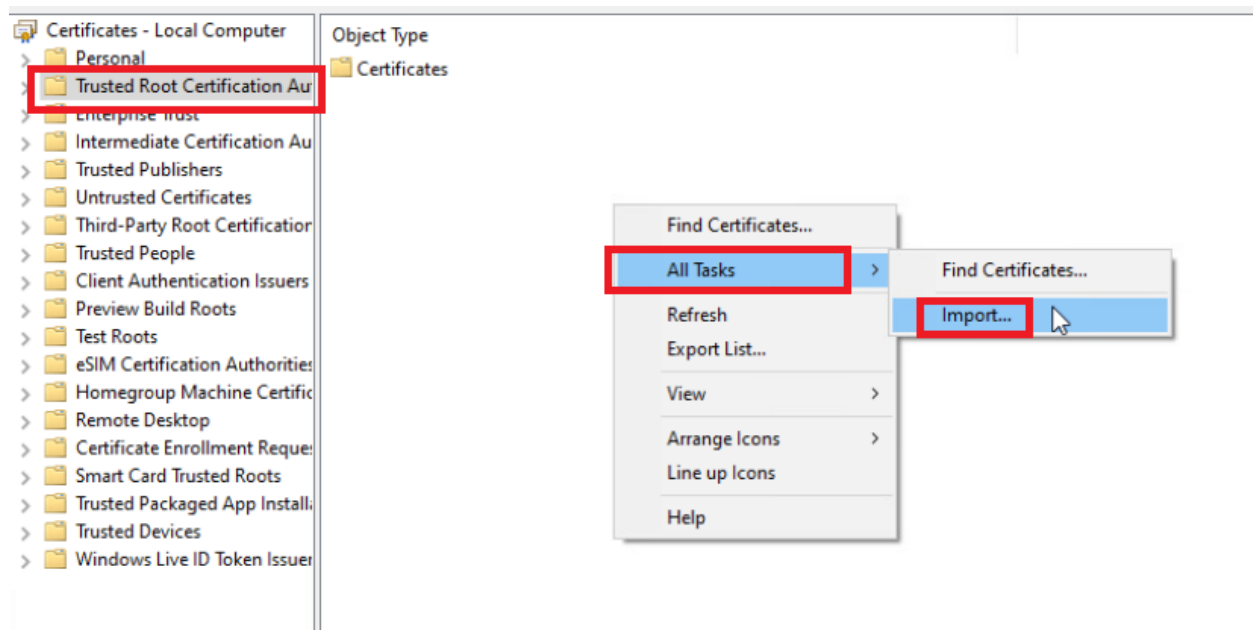
Control panel

 Open

On the site40pc2win PC, click "Start" and search for certificates. Click on "Manage computer certificates" to open the Microsoft Management Console.



7. Click on **Trusted Root Certification Authorities** and then right click in the blank white space on the right hand window pane. Choose **All Tasks => Import**



8. Click **Next** in the Certificate Import Wizard

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

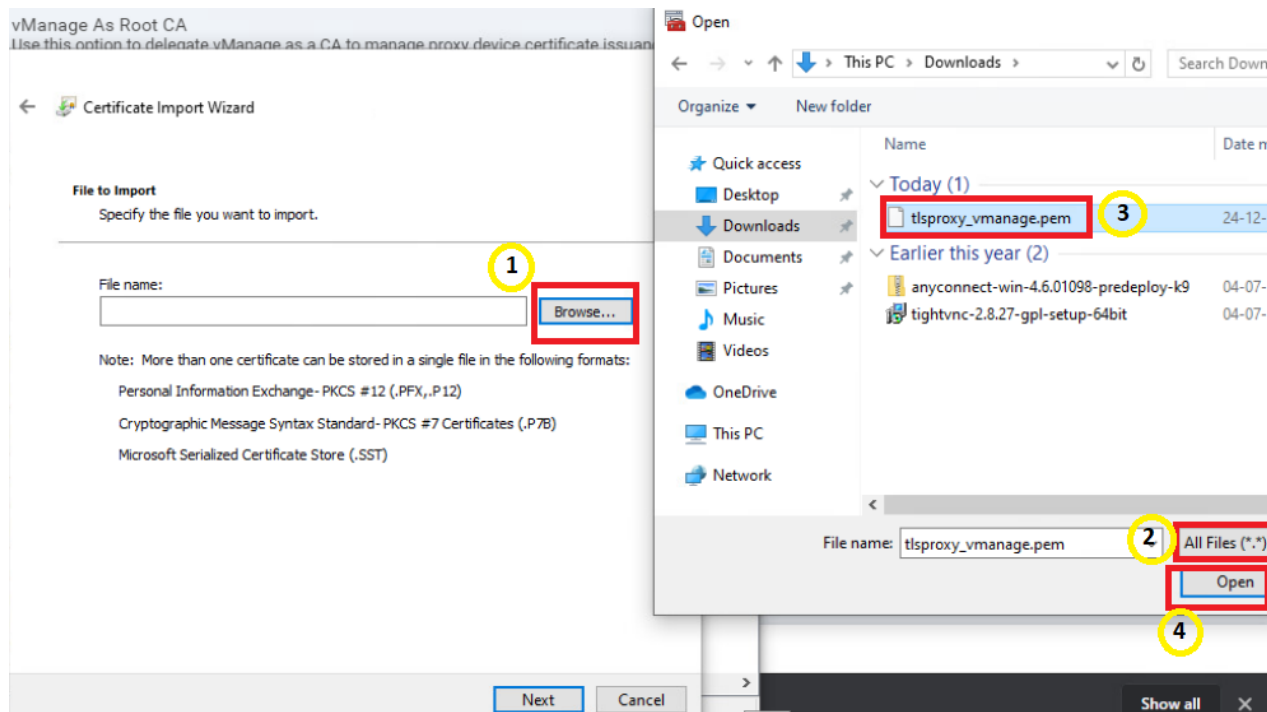
- Current User
 Local Machine

To continue, click Next.

Next

Cancel

9. Click on **Browse** and set the File Type to **All Files**. Select *Downloads* and click on the *tlsproxy_vmanage.pem* file we downloaded and click on **Open**



10. Click on **Next** and ensure that the certificate store is set to **Trusted Root Certification Authorities**. Click on **Next**

File to Import

Specify the file you want to import.

File name:

C:\Users\admin\Downloads\tlsproxy_vmanage.pem

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

Automatically select the certificate store based on the type of certificate

Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

Next

Cancel

11. Click on **Finish** and then **OK** once the import is successful

Completing the Certificate Import Wizard

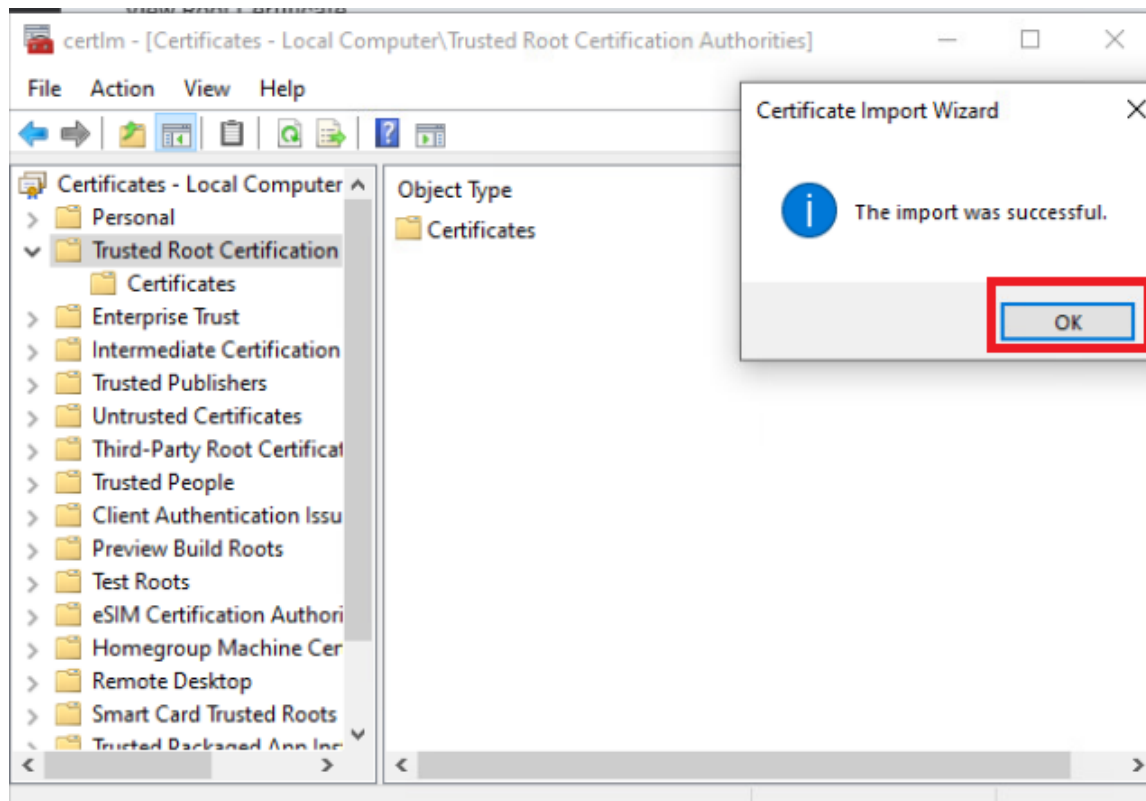
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\admin\Downloads\tlsproxy_vmanage.pem

Finish

Cancel



We have successfully set up the initial configuration for TLS/SSL Proxy in a Cisco SD-WAN environment.

Task List

- [Overview](#)
- [Pre-work and Testing](#)
- [Initial Configuration](#)
 - [Configuring NTP and DNS](#)
 - [Setting up vManage as the CA](#)
- [Enabling AMP and Testing](#)
- [Configuring the Decryption Policy](#)
- [Activity Verification](#)

Enabling AMP and Testing


Advanced Malware Protection will be enabled in this section and we will try to download a sample malware file via HTTPS. Since the TLS/SSL Proxy isn't configured yet, we expect the file to be downloaded despite AMP being enabled. This is due to the fact that traffic is encrypted and AMP cannot analyse encrypted communication.

1. Navigate to **Configuration => Security** on the vManage GUI and locate the *Guest-FW-IPS-DIA* policy. Click on the three dots next to it and choose to **Edit**

DASHBOARD | MAIN DASHBOARD



2 ↑
Smart - 2



8 ↑
WAN Edge - 8

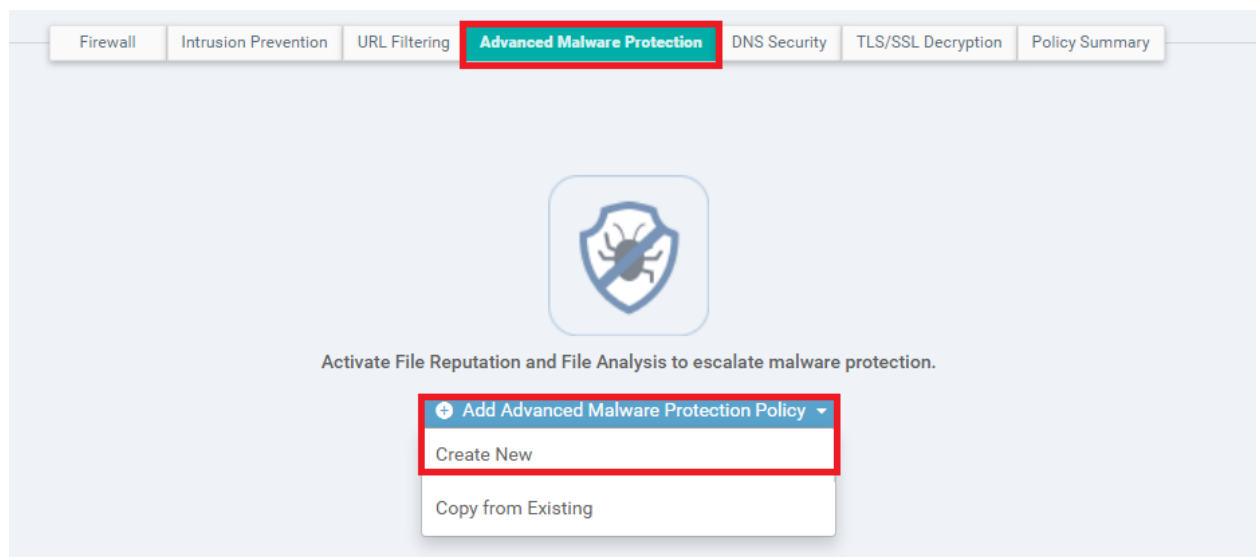
TLS/SSL Proxy	10
Certificates	0
Network Design	0
Templates	
Policies	
Security	20
Unified Communications	20
Cloud onRamp for SaaS	8
Cloud onRamp for IaaS	0

Cloud OnRamp for Multi-Cloud

Name	Description	Use Case	Devices Attached	Device Templates	Updated By	Last Updated	
Site40-Guest-DIA	Guest Policy for Site 40	Guest Access	0	0	admin	27 Aug 2020 11:40:20 PM P...	...
Guest-FW-IPS-DIA	Guest Firewall and IPS DIA	Custom	1	1	admin	31 Aug 2020 5:03:08 AM PDT	...

- View
- Preview
- Edit**
- Delete

2. Click on the **Advanced Malware Protection** tab and then on **Add Advanced Malware Protection Policy**. Choose *Create New*



3. Enter the details enumerated in the table below and click on **Save Advanced Malware Protection Policy**. When the **Custom VPN Configuration** radio button is selected, you will get a help walkthrough which will instruct you how to specify custom VPNs. Click on *Got It* and then click on **Target VPNs**. Enter 30 as the Target VPN

Field	Value
Policy Name	<i>amp-policy</i>
VPN	Custom VPN Configuration
Target VPN	30
AMP Cloud Region	NAM
Alerts Log Level	Info
File Analysis	Disabled

Target

1
 VPNs

Target VPNs

Policy Behavior

AMP Cloud Region: **NAM**

TG Cloud Region: -
File Types List: -

Reputation Alert Level: **Info**
Analysis Alert Level: -

File Reputation

File Analysis

Alerts

Advanced Malware Protection - Policy Rule Configuration

Policy Name:

Match All VPN
 Custom VPN Configuration

File Reputation

AMP Cloud Region:

Alerts Log Level:

File Analysis:

Save Advanced Malware Protection Policy
CANCEL

4. Click on **Next** and then **Configure Devices**. You can choose to view the side by side configuration, if required

CONFIGURATION | TEMPLATES

Device Template

edge_dualuplink_devtemp

Total: 1

Device list (Total: 1 devices)

Filter/Search

CSR-04F9482E-44FD-E4DC-D30D-69C0806F73F2
 cf5ge4010.255.255.41

Configure Device Rollback Timer

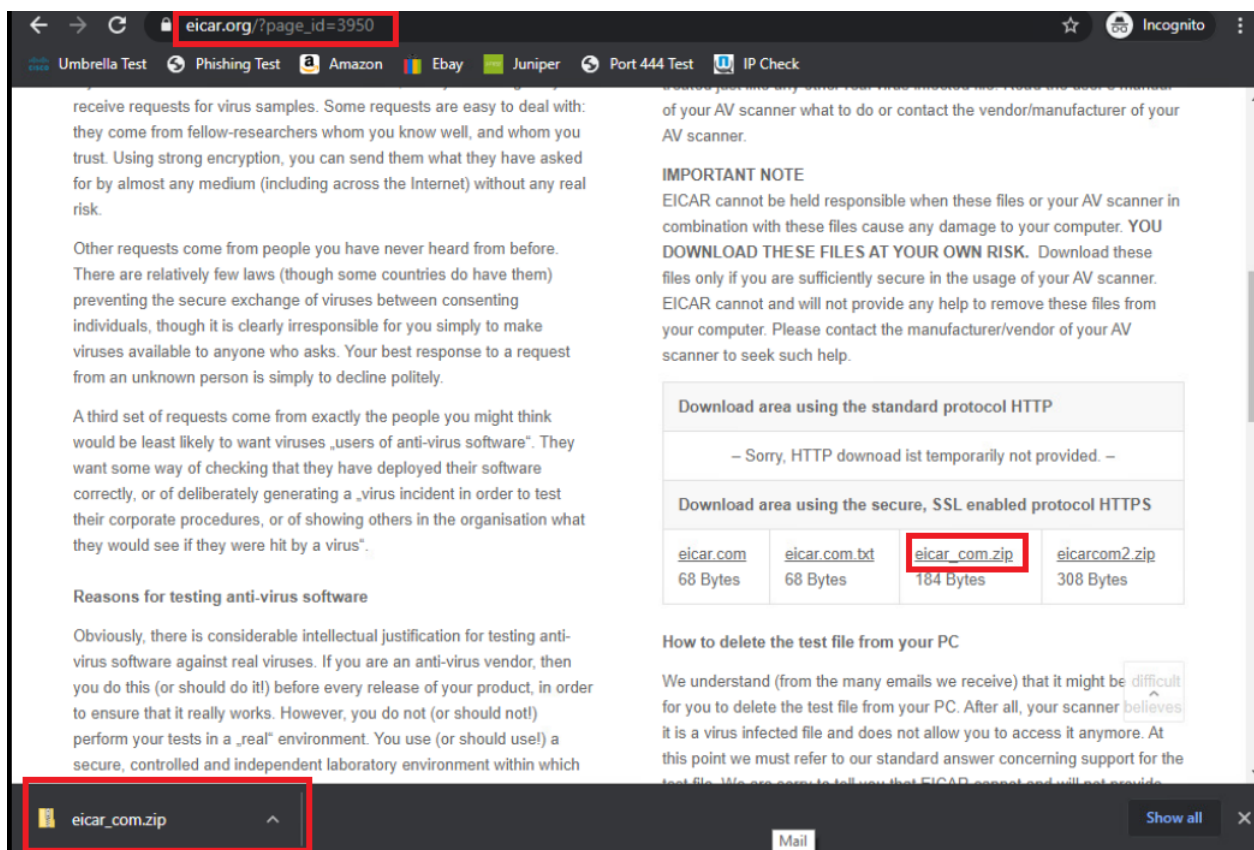
'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

515	reputation	515	reputation
516	block-threshold high-risk	516	block-threshold high-risk
517	!	517	!
518	!	518	!
519	threat-inspection profile Guest-IPS	519	threat-inspection profile Guest-IPS
520	threat protection	520	threat protection
521	policy security	521	policy security
522	logging level info	522	logging level info
523	!	523	!
524	utd global	524	utd global
525	!	525	!
526	policy utd-policy-vrf-30	526	policy utd-policy-vrf-30
527	all-interfaces	527	all-interfaces
528	vrf 30	528	vrf 30
529	threat-inspection profile Guest-IPS	529	threat-inspection profile Guest-IPS
530	web-filter url profile URLF-NoShopping	530	web-filter url profile URLF-NoShopping
531	exit	531	exit
532	!	532	!
533	policy	533	policy
534	app-visibility	534	app-visibility
535	no flow-visibility	535	no flow-visibility

525 file-reputation
 526 cloud-server cloud-lsr-asn.amp.cisco.com
 527 est-server cloud-lsr-est.amp.cisco.com
 528 !
 529 !
 530 file-reputation profile amp-policy-fr-profile
 531 alert level info
 532 !
 533 file-inspection profile amp-policy-fi-profile
 534 reputation profile amp-policy-fr-profile
 535 !
 536 policy utd-policy-vrf-30
 537 all-interfaces
 538 file-inspection profile amp-policy-fi-profile

Back
Configure Devices
Cancel

5. Go back to the Site40PC2 (Windows) via the console session in vCenter. [Click here](#) and go through Step 1 to access the PC. Open Google Chrome and use the **Malware Test** bookmark or navigate to eicar.org/?page_id=3950. Download the **eicar_com.zip** sample malware file and you will notice that the file gets downloaded successfully



We have enabled AMP in our SD-WAN environment and tested that HTTPS communication isn't analysed/blocked by AMP due to its encrypted nature, despite downloading a known malware file.

Task List

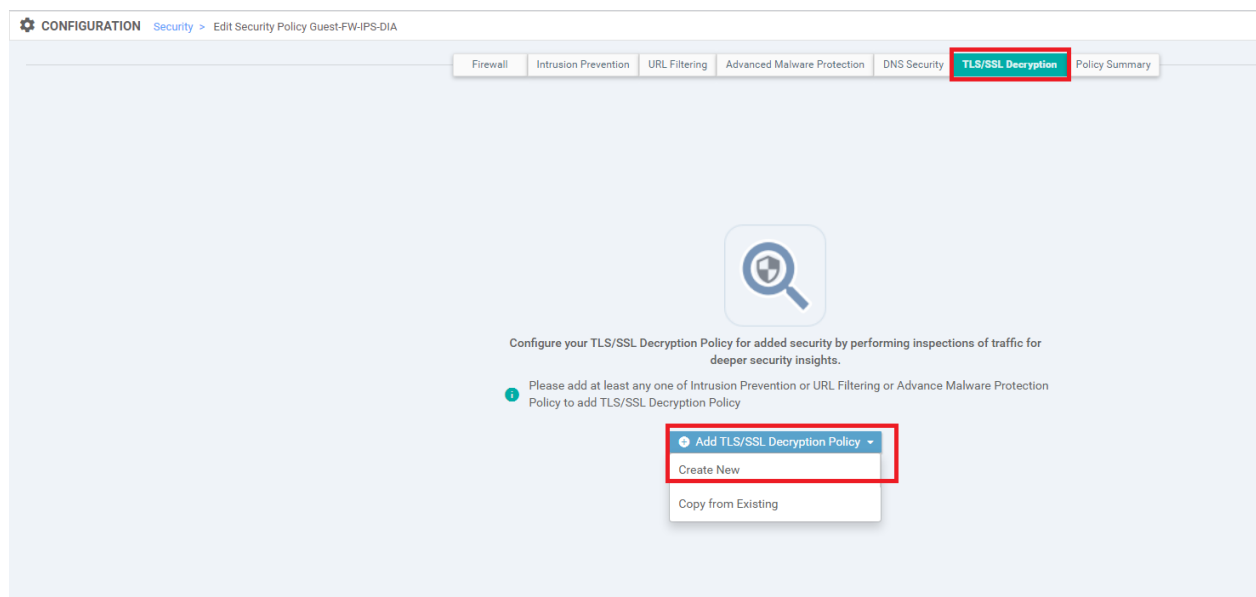
- [Overview](#)
- [Pre-work and Testing](#)
- [Initial Configuration](#)
 - [Configuring NTP and DNS](#)
 - [Setting up vManage as the CA](#)

- [Enabling AMP and Testing](#)
- [Configuring the Decryption Policy](#)
- [Activity Verification](#)

Configuring the Decryption Policy

We will now configure cEdge40 as the TLS/SSL Proxy device.

1. Navigate to **Configuration => Security** and locate the *Guest-FW-IPS-DIA* policy. Click on the three dots next to it and choose to Edit the policy. Click on the **TLS/SSL Decryption** tab and click on **Add TLS/SSL Decryption Policy**



2. Make sure that the vManage shows up as the CA and click on **Enable SSL Decryption**

Certificate Authority vManage as Root CA

SSL Decryption Disabled



Inspecting Encrypted Connections

i Certificate Authority configuration has been completed! You may now enable SSL Decryption and then define your policy.

[Enable SSL Decryption](#)

3. Give the policy a name of *vpn30-tls-decrypt* and create a Network Rule by clicking on **Add Rule**

Policy Name

Network URLs

+ Add Rule (Drag and drop the Order cell to re-arrange rules and click on the cell to inline add/edit the values)

Search Search Options Default Action **No Decrypt**

Order	Name	Action	Source VPNs	Source Networks	Source Ports	Destin
No data available						

4. Set the name of the rule to *decrypt-all-vpn30* and choose **Decrypt** for the Action. Click on **Source VPN** and set the Source VPN to *30*. Click on **Save** and then **Save** again in order to save this rule

New Decryption Rule

Order 1 Name decrypt-all-vpn30 Action Decrypt

Source / Destination Applications

Source VPNs	Source Networks	Source Ports	Destination VPNs	Destination Networks	Destir
30	Any	Any	Any	Any	Any

Graphic Preview

Save CANCEL

5. Make sure that the policy has a Decrypt rule added and click on **Save TLS/SSL Decryption Policy**

Network URLs

Add Rule (Drag and drop the Order cell to re-arrange rules and click on the cell to inline add/edit the values)

Search Options ▾ Default Action No Decrypt ▾

Order	Name	Action	Source VPNs	Source Networks	Source Ports	D
> 1	decrypt-all-vpn30	Decrypt	30	Any	Any	A

Advanced Settings >

Save TLS/SSL Decryption Policy CANCEL

- At the main policy page, click on **Save Policy Changes** and then choose **Next** and **Configure Devices**. You can view the side by side configuration if needed

Search Options ▾

Name	Type	Reference Count	Updated By
vpn30-tls-decrypt	sslDecryption	0	admin

Preview Save Policy Changes CANCEL

```

600 !
601 !
602 !
603 !
604 !
634 !
635 utd-tls-decrypt vpn30-tls-decrypt
636 sequence 1
637 seq-name decrypt-all-vpn30
638 match
639 source-vpn 30
640 !
641 action utd
642 tls decrypt
643 !
644 !
645 default-action utd
646 tls do-not-decrypt
647 !
648 !
649 !
650 !
651 !
652 !

```

Back Configure Devices Cancel

We have configured a decryption policy for cEdge40.

Task List

- ~~Overview~~
- ~~Pre-work and Testing~~
- ~~Initial Configuration~~
 - ~~Configuring NTP and DNS~~
 - ~~Setting up vManage as the CA~~
- ~~Enabling AMP and Testing~~
- ~~Configuring the Decryption Policy~~
- Activity Verification

Activity Verification

1. Once the changes have been pushed successfully, log in to the CLI of cEdge40 via Putty using the saved session (or SSH to 192.168.0.40). Issue `clear utd engine standard logging events` and then `show sslproxy status`. The SSL and TCP Proxy Operational State should be RUNNING and Clear Mode should be set to False

Username	Password
admin	admin

```

cEdge40#clear utd engine standard logging events
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#
cEdge40#clear utd engine standard logging events
cEdge40#show sslproxy status
=====
                        SSL Proxy Status
=====

Configuration
-----
CA Cert Bundle           : /bootflash/vmanage-admin/sslProxyDefaultCAbundl
e.pem
CA TP Label             : PROXY-SIGNING-CA
Cert Lifetime           : 730
EC Key type              : P256
RSA Key Modulus         : 2048
Cert Revocation         : NONE
Expired Cert             : drop
Untrusted Cert          : drop
Unknown Status          : drop
Unsupported Protocol Ver : drop
Unsupported Cipher Suites : drop
Failure Mode Action     : close
Min TLS Ver             : TLS Version 1

Status
-----
SSL Proxy Operational State : RUNNING
TCP Proxy Operational State : RUNNING
Clear Mode                   : FALSE

cEdge40#

```

```

clear utd engine standard logging events
show sslproxy status

```

2. There should be some traffic being generated from Site40. Issue `show sslproxy statistics` and make note of some connections being proxied. Run `show utd engine standard logging events` - there might be some events logged, depending on what's open on the Site 40 clients

```
cEdge40#show sslproxy statistics
=====
                SSL Proxy Statistics
=====
Connection Statistics:
Total Connections      : 3
Proxied Connections    : 1
Non-proxied Connections : 2
Clear Connections      : 0
Active Proxied Connections : 0
Active Non-proxied Connections : 2
Active Clear Connections : 0
Max Conc Proxied Connections : 1
Max Conc Non-proxied Connections : 2
Max Conc Clear Connections : 0
Total Closed Connections : 1
```

```
cEdge40#show utd engine standard logging events
cEdge40#
cEdge40#
cEdge40#
cEdge40#
```

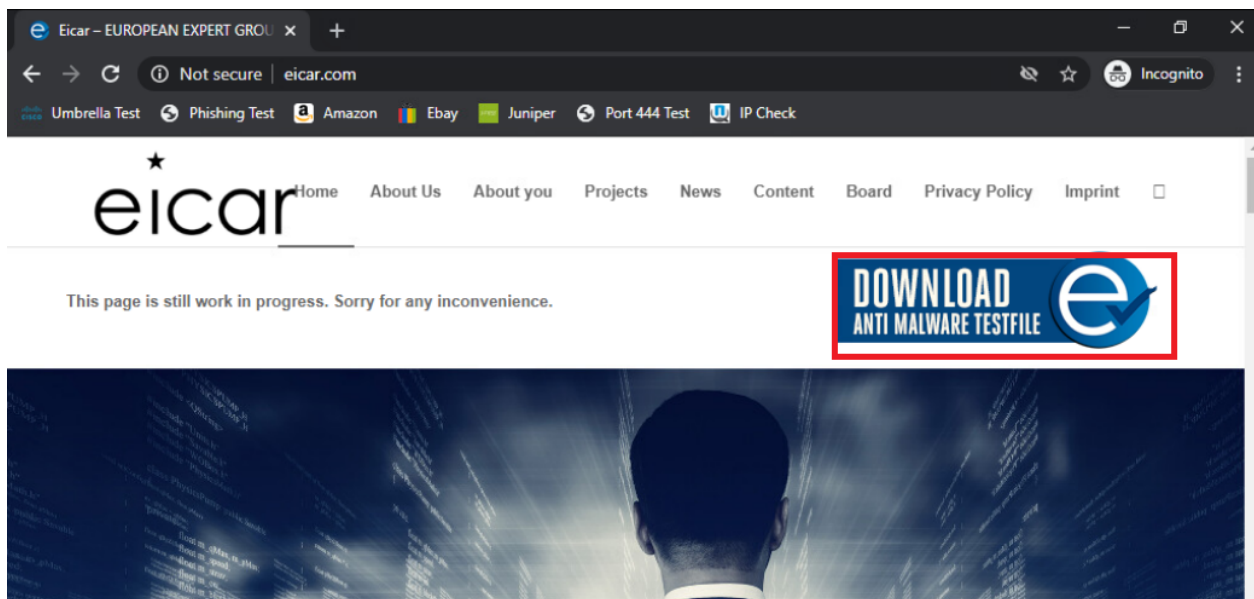
```
cEdge40#show utd engine standard logging events
cEdge40#
cEdge40#
cEdge40#show utd engine standard logging events
2020/12/24-10:53:21.667045 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: dns.google] *
* [Category: Proxy Avoid and Anonymizers] ** [Reputation: 10] [VRF: 30] [TCP] 10.40.30.22:50440 -> 8.8.4.4:443
2020/12/24-10:53:21.667171 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: dns.google] *
* [Category: Proxy Avoid and Anonymizers] ** [Reputation: 10] [VRF: 30] [TCP] 10.40.30.22:50442 -> 8.8.4.4:443
```

```
show sslproxy statistics
show utd engine standard logging events
```

3. Run `clear utd engine standard logging events` and then `show utd engine standard logging events`. We shouldn't see too much activity here, but some events will be logged automatically over time (like the dns.google events seen before)

```
cEdge40#clear utd engine standard logging events
cEdge40#
cEdge40#
cEdge40#show utd engine standard logging events
cEdge40#
```

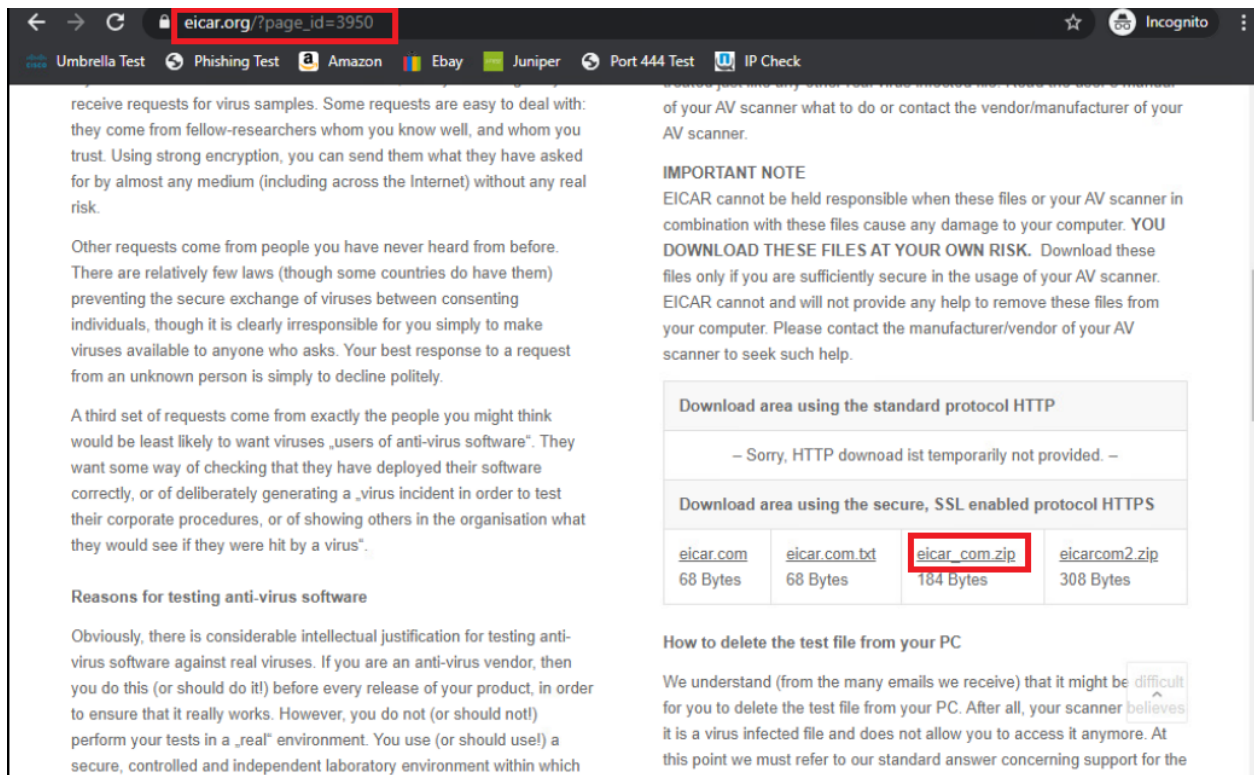
4. Open Google Chrome on the *Site40PC2Win* VM (or navigate to *eicar.com* in a browser)



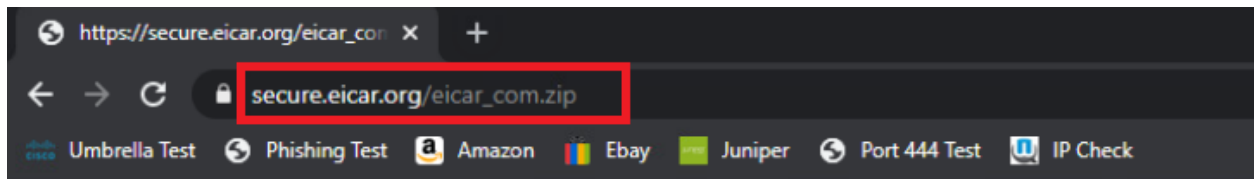
5. Wait for a few seconds (might need to refresh for the site to load) and issue `show utd engine standard logging events` in the cEdge40 CLI. You should see some traffic now being analysed by AMP, being flagged with *Unknown Disposition*. This traffic will be allowed

```
cEdge40#show utd engine standard logging events
2020/12/24-10:53:50.189777 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: dns.google] *
* [Category: Proxy Avoid and Anonymizers] ** [Reputation: 10] [VRF: 30] (TCP) 10.40.30.22:50465 -> 8.8.4.4:443
2020/12/24-10:53:50.569879 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: dns.google] *
* [Category: Proxy Avoid and Anonymizers] ** [Reputation: 10] [VRF: 30] (TCP) 10.40.30.22:50466 -> 8.8.4.4:443
2020/12/24-10:54:05.015394 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: dns.google] *
* [Category: Proxy Avoid and Anonymizers] ** [Reputation: 10] [VRF: 30] (TCP) 10.40.30.22:50468 -> 8.8.4.4:443
2020/12/24-10:54:06.068024 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: dns.google] *
* [Category: Proxy Avoid and Anonymizers] ** [Reputation: 10] [VRF: 30] (TCP) 10.40.30.22:50470 -> 8.8.4.4:443
2020/12/24-10:54:06.961916 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: dns.google] *
* [Category: Proxy Avoid and Anonymizers] ** [Reputation: 10] [VRF: 30] (TCP) 10.40.30.22:50477 -> 8.8.4.4:443
2020/12/24-10:54:19.130734 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Allow [**] UTD AMP DISPOSITION UNKNOWN [**] SHA: 4639E45204CC274CAAB
01161E16B77FE2DF2A3E9A6D57A43741C572F75AA2B12 Malware: None Filename: home_b-2.pngscroll-to-anchor.min.js?ver=5.2.396dl Filetype: PNG [VRF: 30] (TCP) 89.238.
73.97:443 -> 10.40.30.22:50469
2020/12/24-10:54:19.699531 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Allow [**] UTD AMP DISPOSITION UNKNOWN [**] SHA: EF31B211BA4CA7B7A6A
F31F151AFDD5364BC4F746FE68BA55F6D6D9A1B630734 Malware: None Filename: cropped-e-32x32.pngto-anchor.min.js?ver=5.2.396dl Filetype: PNG [VRF: 30] (TCP) 89.238.
73.97:443 -> 10.40.30.22:50469
cEdge40#
cEdge40#
```

6. On Chrome at the Site40PC2Win, click on the **Malware Test** bookmark or navigate to *eicar.org/?page_id=3950* and click on the **eicar_com.zip** hyperlink to download the file



7. You will notice that the file download is now blocked



8. From the CLI of cEdge40, issue `show utd engine standard logging events` and we will see the file download being blocked


```
2020/12/24-10:55:04.846961 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: secure.eicar.org/eicar_com.zip] [**] [Category: Malware Sites] [**] [Reputation: 10] [VRF: 30] [TCP] 89.238.73.97:443 -> 10.40.30.22:50492
2020/12/24-10:55:06.192386 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Category/Reputation [**] [URL: secure.eicar.org/eicar_com.zip] [**] [Category: Malware Sites] [**] [Reputation: 10] [VRF: 30] [TCP] 89.238.73.97:443 -> 10.40.30.22:50497
2020/12/24-10:55:06.338466 UTC [**] [Hostname: 10.255.255.41] [**] [Instance_ID: 1] [**] Drop [**] UTD AMP DISPOSITION MALICIOUS [**] SHA: 2546DCFFC5AD954D4DD64FBF056671CD5A00F2471CB7A5BFD4AC23B6E9EEDAD Malware: Win.Ransomware.Eicar::95.sbx.tg Filename: Filetype: ZIP [VRF: 30] [TCP] 89.238.73.97:443 -> 10.40.30.22:50497
cEdge40#
cEdge40#
```

We have thus configured cEdge40 as a TLS/SSL Proxy device that is decrypting encrypted traffic, acting as a man-in-the-middle.

Task List

- [Overview](#)
- [Pre-work and Testing](#)
- [Initial Configuration](#)
 - [Configuring NTP and DNS](#)
 - [Setting up vManage as the CA](#)
- [Enabling AMP and Testing](#)
- [Configuring the Decryption Policy](#)
- [Activity Verification](#)

©2021 Cisco Systems Inc. and/or its affiliates. All rights reserved. Cisco Partner Confidential.

Page last updated: Dec 25, 2020

Site last generated: Jun 14, 2021



-->

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

Use the URL provided for your POD

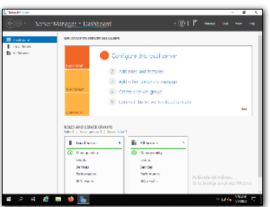


The login screen features the Apache Guacamole logo at the top, followed by the text "APACHE GUACAMOLE". Below this is a red-bordered box containing a username field with "sdwanpod" and a password field with masked characters. A "Login" button is positioned at the bottom of the red box.

RECENT CONNECTIONS



POD3-Site30PC



POD3-AD



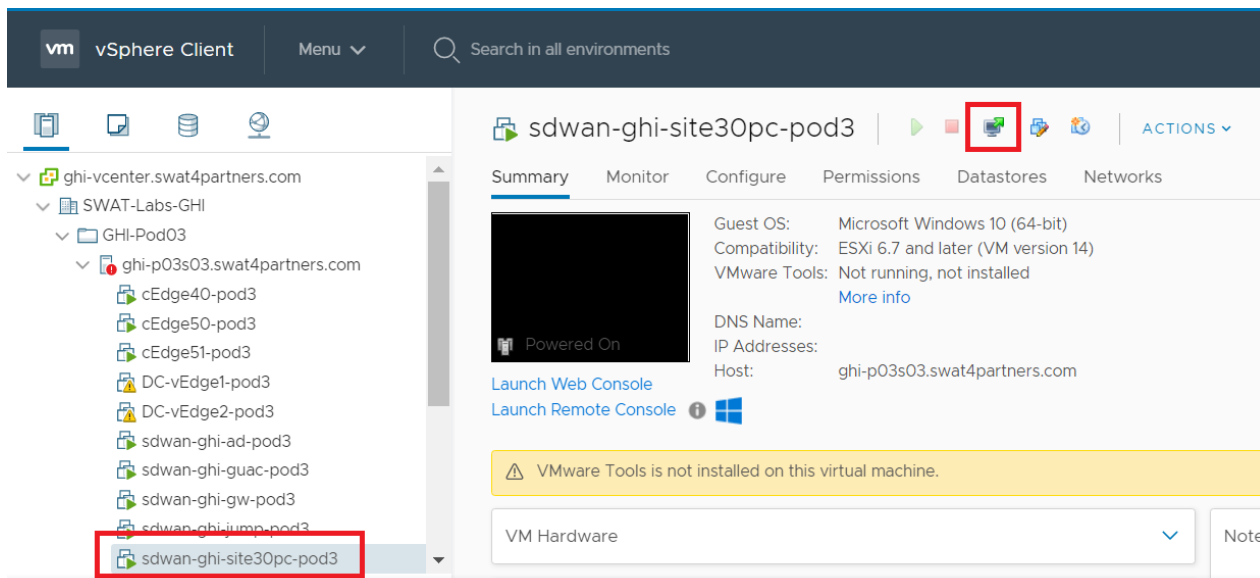
POD3-Jumphost

ALL CONNECTIONS

Filter

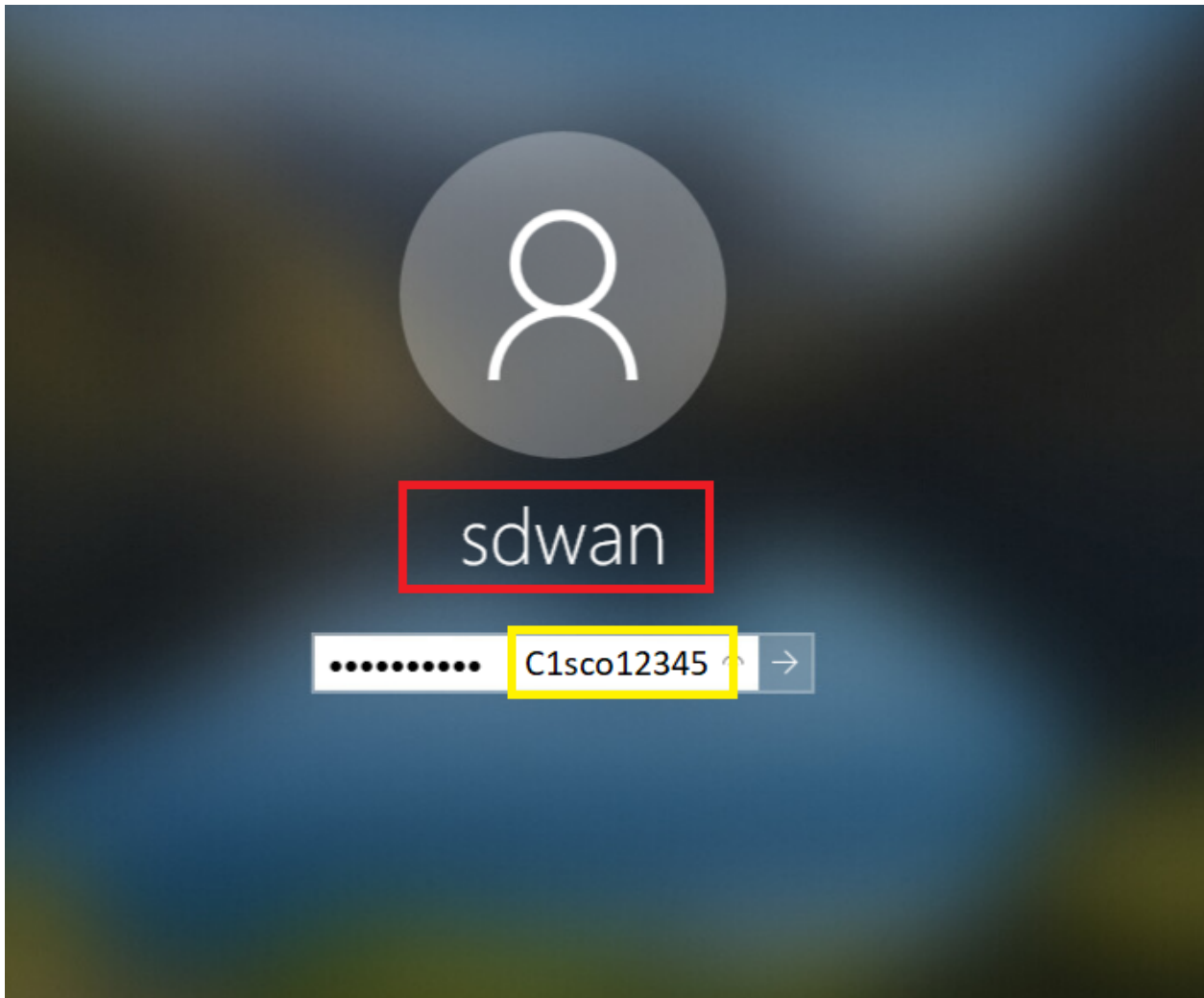
- POD3-AD
- POD3-Jumphost
- POD3-Site30PC

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

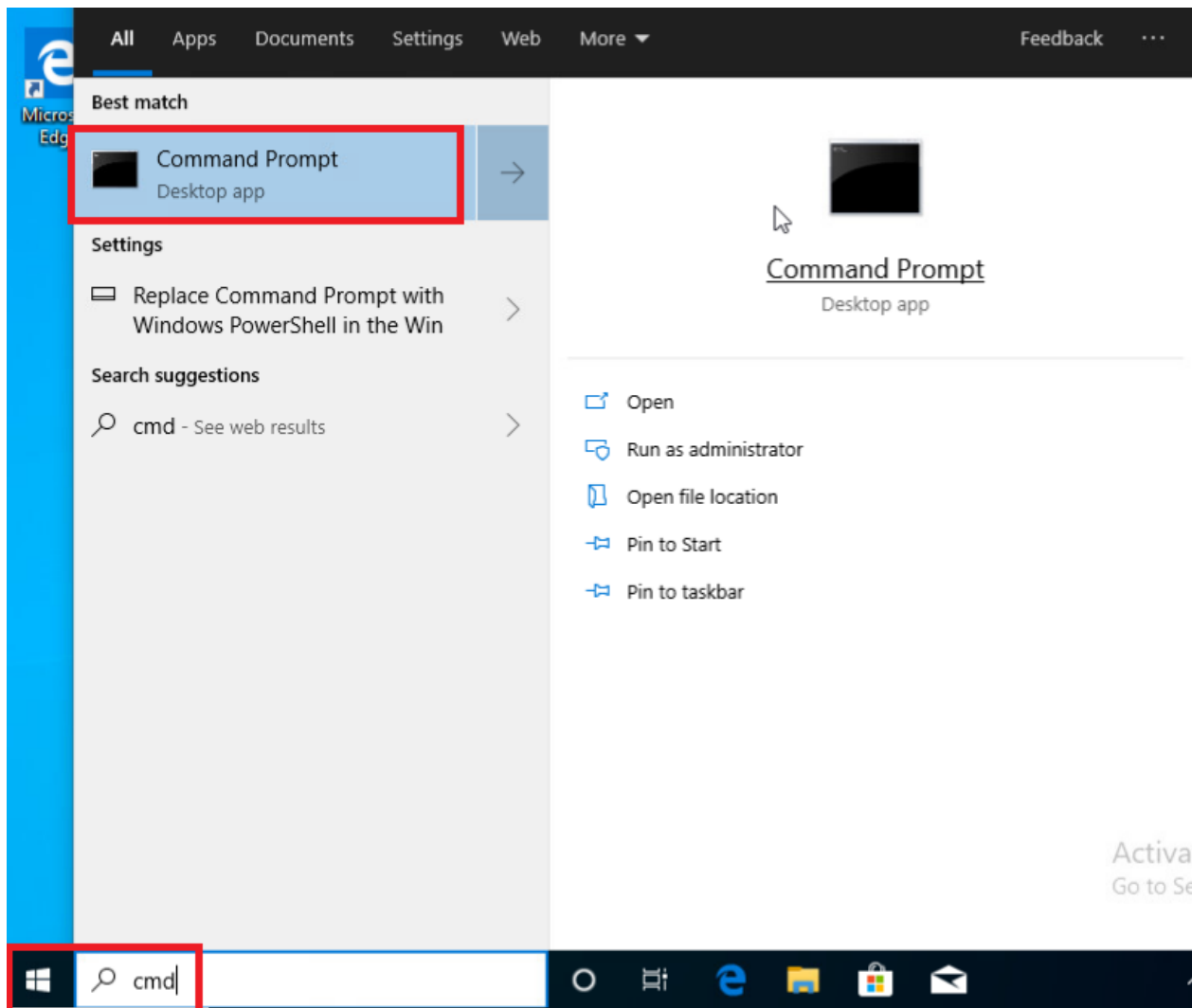


2. Depending on the connection method, you may need to enter credentials again to log in to the Site 30 PC. Please enter the credentials shown below, if prompted

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.
```

```
Reply from 10.30.10.2: Destination net unreachable.
```

```
Reply from 10.30.10.2: Destination net unreachable.
```

```
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 displays the Cisco vManage interface. The top navigation bar shows 'Cisco vManage' and 'DASHBOARD | MAIN DASHBOARD'. A left-hand navigation menu is open, with 'Configuration' selected and 'Templates' highlighted with a red box. The main dashboard area shows several widgets: 'Smart - 2' (2 up), 'WAN Edge - 8' (8 up), and 'vBond - 1' (1 up). Below these are 'Site Health (Total 5)' and 'WAN Edge Health (Total 8)' sections. The 'Site Health' section shows 'Full WAN Connectivity' (10), 'Partial WAN Connectivity' (0), and 'No WAN Connectivity' (0). The 'WAN Edge Health' section shows 'Normal' (8) and 'Warning' (0). At the bottom, there is an 'Application-Aware Routing' section with a table showing 'Tunnel Endpoints' and 'Avg. Latency'.

Tunnel Endpoints	Avg. Latency
vEdoe30:public-internet-vEdoe21:public-internet	0

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 | vedge30 | Search Options

Total Rows: 3 of 41

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
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)

Secondary DNS Address (IPv4)

+ 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 type="text" value="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 ⓘ

Gateway Next Hop Null 0 VPN

Next Hop 2 Next Hop

Next Hop

Address	Distance	
<input type="text" value=""/> <small>[vpn0_inet_next_hop]</small>	<input type="text" value="1"/>	<input type="button" value="−"/>
<input type="text" value=""/> <small>[vpn0_mpls_next_hop]</small>	<input type="text" value="1"/>	<input type="button" value="−"/>

10. Click on **Save Changes**

Next Hop

Address	Distance
<input type="text" value="vpn0_inet_next_hop"/>	<input checked="" type="checkbox"/> 1

11. Ensure that the **Update IPv4 Route** window shows **1 Next Hop** and click on **Save Changes**

Update IPv4 Route

Prefix Mark as Optional Row

Gateway Next Hop Null 0 VPN

Next Hop

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

Gateway Next Hop Null 0 VPN

Next Hop [+ Add Next Hop](#)

13. Click on **Add Next Hop** again

Next Hop ×



No Next Hop added, add your first Next Hop

[Add Next Hop](#)

[Add](#) [Cancel](#)

14. Enter a Global value of *192.0.2.13* in the **Address** field and click on **Add**

Next Hop

Address Distance

192.0.2.13 1

+ Add Next Hop

Add Cancel

15. Click on **Add** again to add the route

IPv4 ROUTE

+ New IPv4 Route

Mark as Optional Row

Prefix 192.0.2.0/24

Gateway Next Hop Null 0 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

Gateway Next Hop Null 0 VPN

Next Hop **+ Add Next Hop**

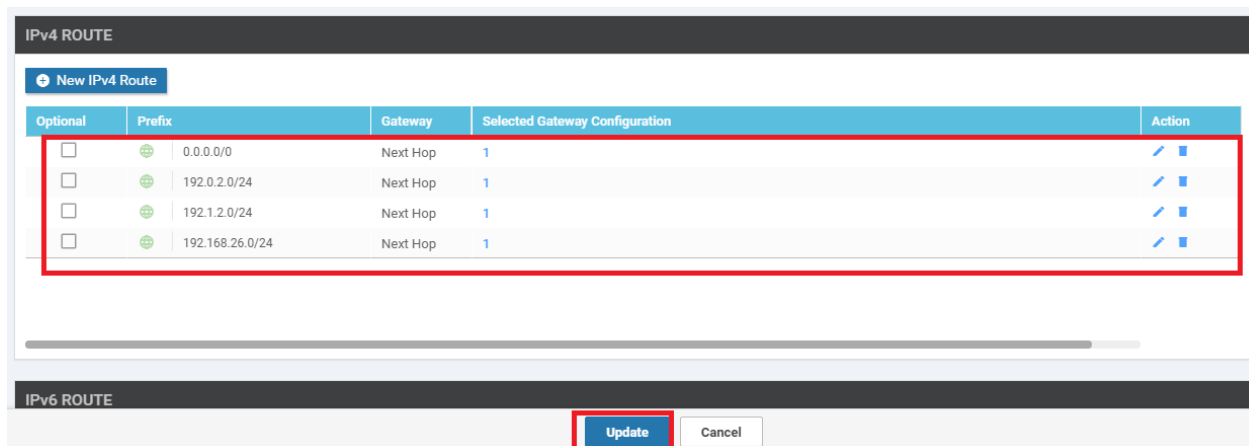
Next Hop

Address	Distance
<input type="text" value="192.0.2.13"/>	<input type="text" value="1"/>

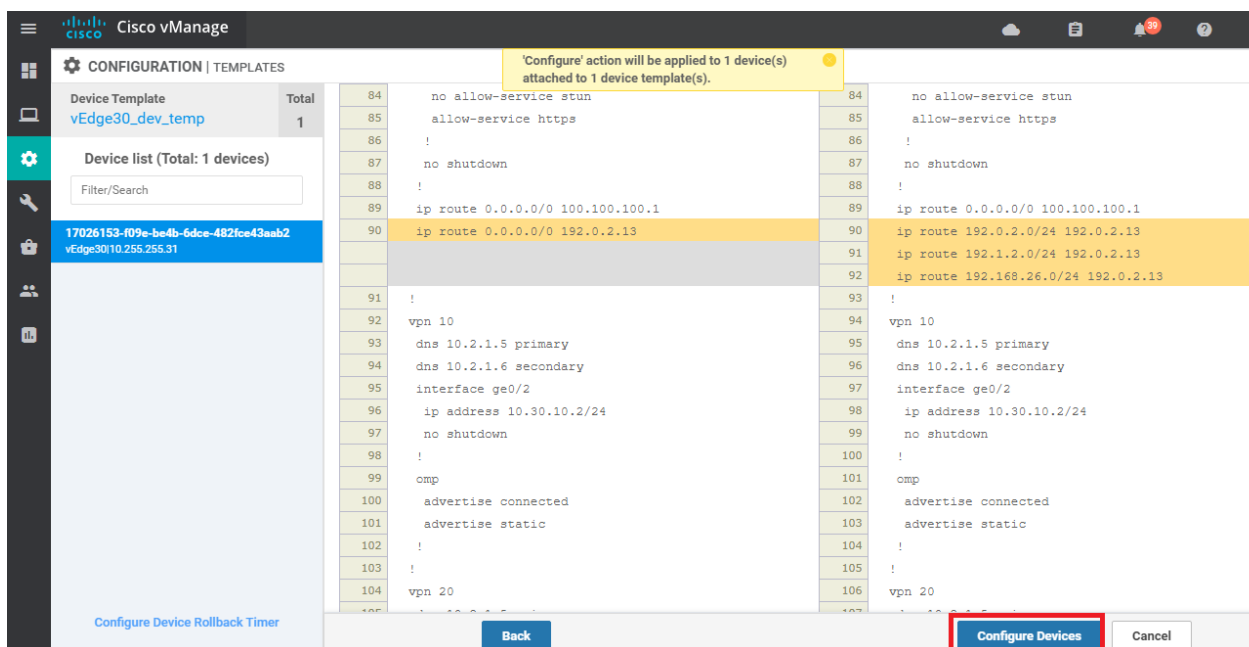
+ Add Next Hop

Add Cancel

17. Make sure there are 4 routes created, as shown below and click on **Update**



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



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 | mpls x | 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_tl...	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...

Context menu for vEdge30_MPLS: View, **Edit**, Change Device Models, Delete, Copy

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: [dropdown]

Border: [dropdown] On Off

Control Connection: [dropdown] On Off

Maximum Control Connections: [dropdown]

vBond As Stun Server: [dropdown] On Off

Exclude Controller Group List: [dropdown]

vManage Connection Preference: [dropdown] 5

Port Hop: [dropdown] On 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: inet x | 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 IN...	WAN Edge VPN	vEdge Cloud	1	2	admin	18 Jun 2020 9:33:30
DC-vEdge_INET	INET interface for the DC-v...	WAN Edge Interface	vEdge Cloud	1	2	admin	18 Jun 2020 9:41:03
vEdge30-vpn0	VPN0 for the Site30 INET a...	WAN Edge VPN	vEdge Cloud	1	1	admin	02 Jul 2020 9:13:07 P...	...
vEdge30_INET	INET interface for the Site3...	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

Basic Configuration | Tunnel | **NAT** | VRRP | ACL/QoS | ARP | 802.1X | Advanced

NAT

IPv4 IPv6

NAT On Off

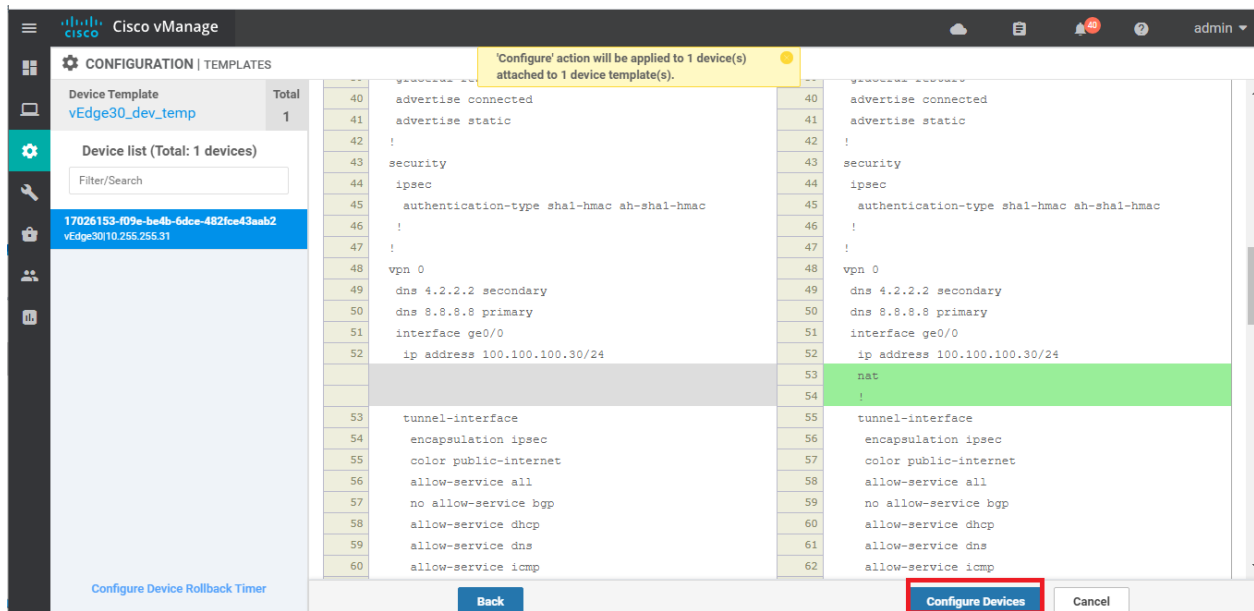
Refresh Mode: outbound

Log NAT flow creations or deletions: On Off

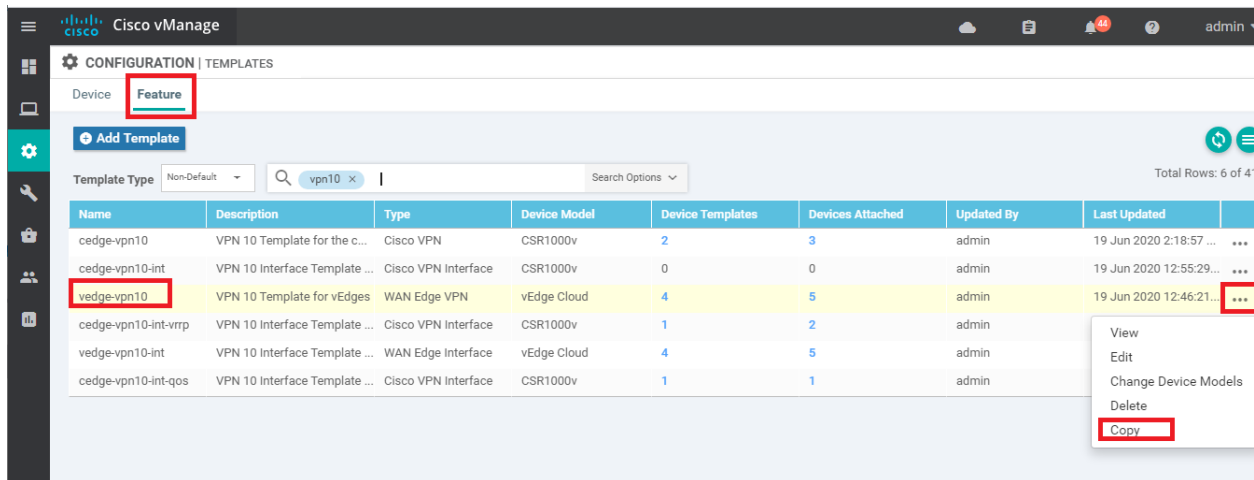
UDP Timeout: 1

TCP Timeout: 60

Update 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**



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

Template Type Non-Default

vpn10

Total Rows: 7 of 42

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		

View Edit Change Device Models Delete Copy

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**.

DNS

IPv4 IPv6

Primary DNS Address (IPv4)

Secondary DNS Address (IPv4)

[+ New Host Mapping](#)

Optional	Hostname	List of IP Addresses (Maximum: 8)	Action
----------	----------	-----------------------------------	--------

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

CONFIGURATION | TEMPLATES

Device Feature

[+ Create Template](#)

Template Type: Non-Default Search Options

Total Rows: 7

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	

- Edit
- View
- Delete
- Copy
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

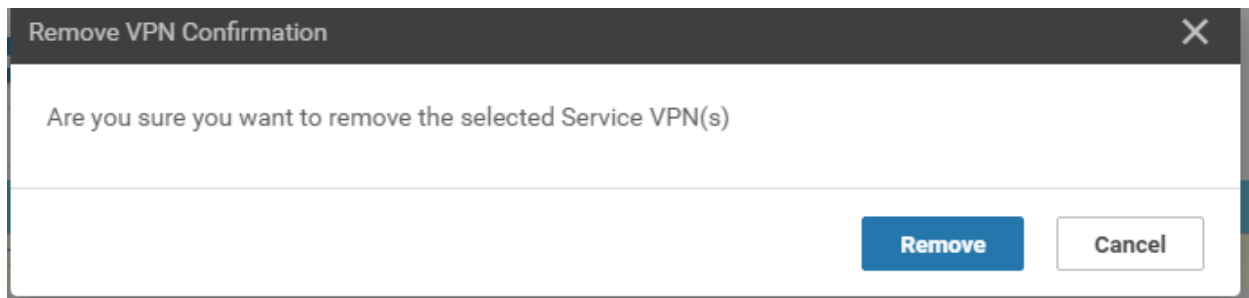
27. In the **Service VPN** section, select the *vedge-vpn10* Template Name entry and click on **Remove VPN**. Confirm the removal

Service VPN

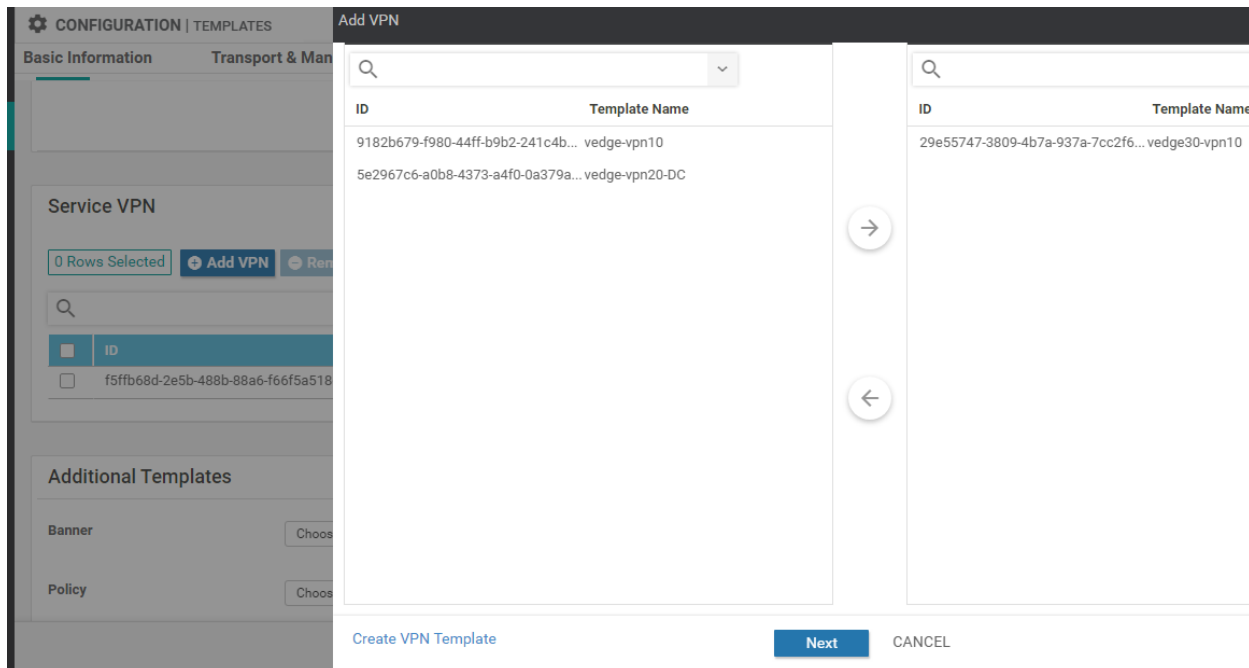
1 Rows Selected [+ Add VPN](#) [- Remove VPN](#)

Search Options

<input type="checkbox"/>	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**

Add VPN

Select VPNs
 Select Sub-Templates

Include sub-templates to attach to ALL selected service VPNs:

VPN Interface: vedge-vpn10-int Sub-Templates

Additional VPN Templates

- BGP
- IGMP
- Multicast
- OSPF
- PIM
- VPN Interface
- VPN Interface Bridge
- VPN Interface GRE
- VPN Interface IPsec
- VPN Interface Natpool

BACK Add CANCEL

30. Back at the Device Template, click on **Update** followed by **Next** and **Configure Devices**

Service VPN

0 Rows Selected + Add VPN - Remove VPN

Search Search Options Tot:

<input type="checkbox"/>	ID	Template Name	Sub-Templates
<input type="checkbox"/>	f5ffb68d-2e5b-488b-88a6-f66f5a518cee	vedge-vpn20	VPN Interface
<input type="checkbox"/>	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

PutTY Configuration

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

192.168.0.1 22

Connection type:

Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

CentralGW

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

```
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**

Cisco vManage

CONFIGURATION | POLICIES

Centralized Policy Localized Policy

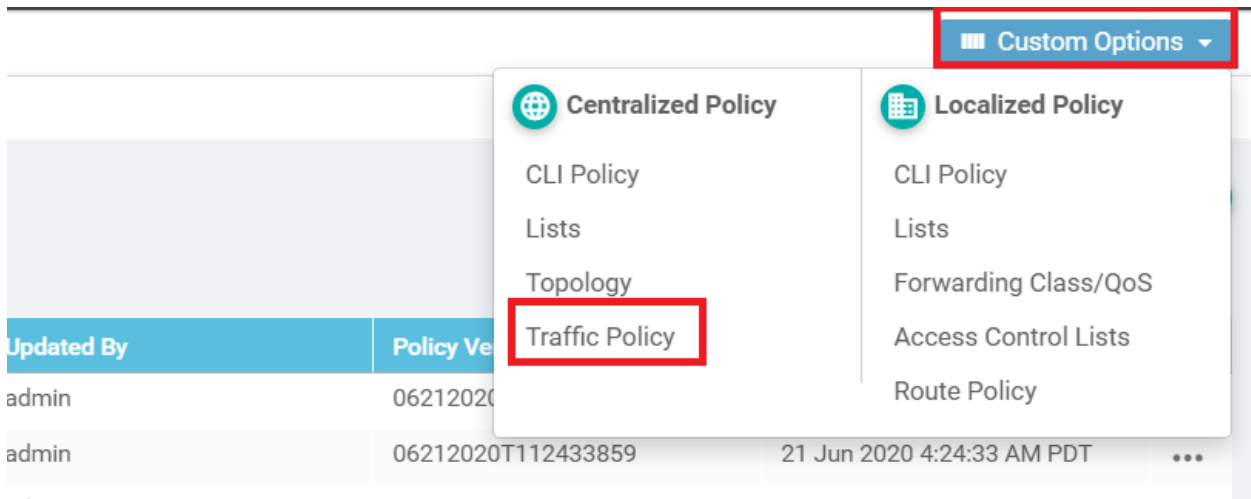
Configuration

- Devices
- TLS/SSL Proxy
- Certificates
- Network Design
- Templates
- Policies**
- Security
- Unified Communications
- Cloud onRamp for SaaS
- Cloud onRamp for IaaS
- Cloud onRamp for Colocation

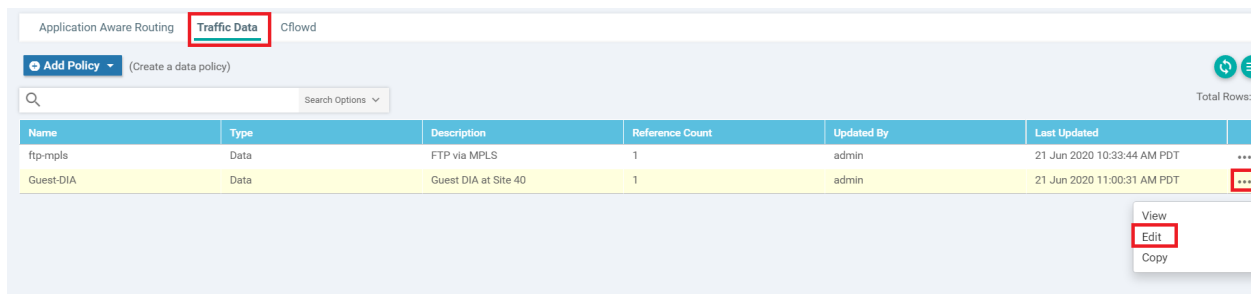
Search Options

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

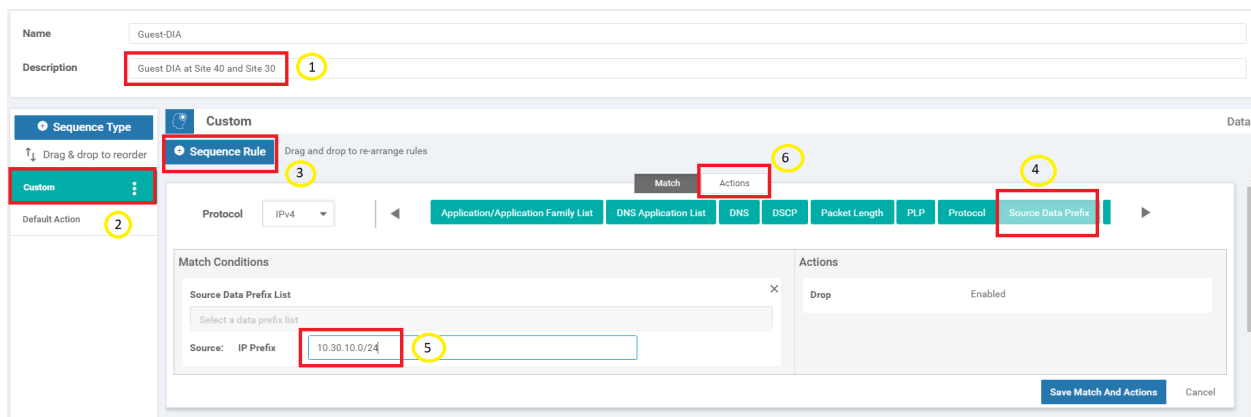
2. Click on **Custom Options** in the top right-hand corner and click on **Traffic Policy**



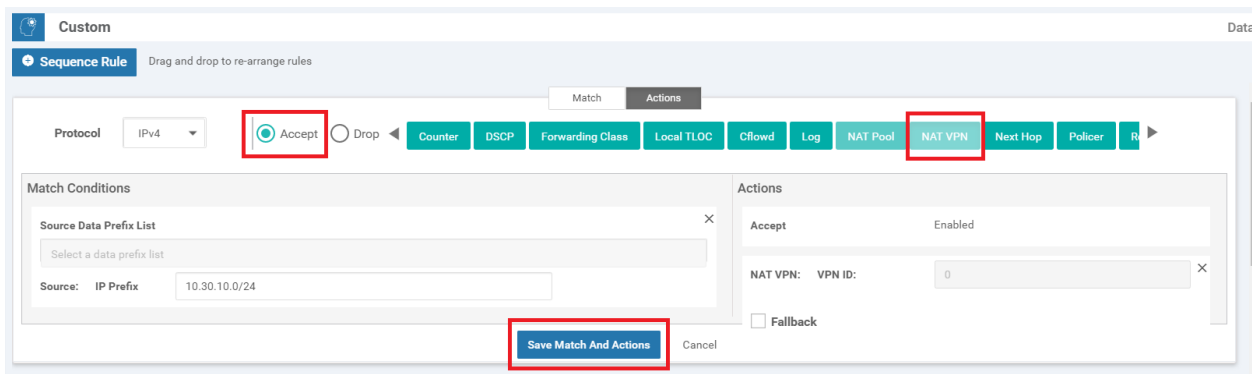
3. Click on the **Traffic Data** tab and locate the *Guest-DIA* Policy. Click on the three dots next to it and choose to **Edit**



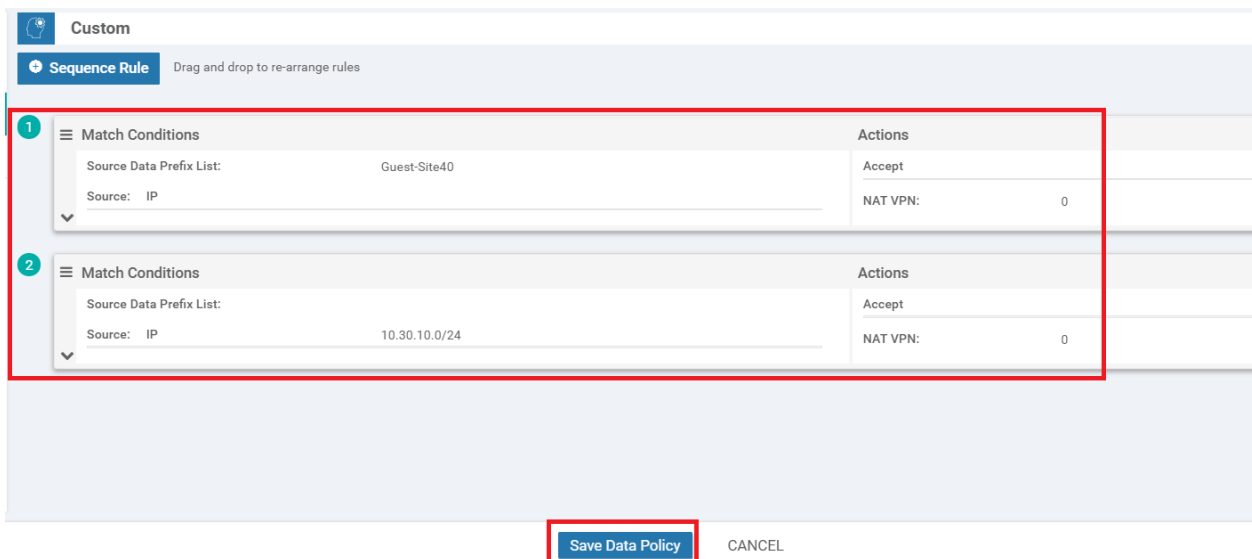
4. Update the **Description** to *Guest DIA at Site 40 and Site 30* and make sure you're on the **Custom** Sequence Type. Click on **Sequence Rule** to add a new rule and select **Source Data Prefix** under Match (might need to use the scroll buttons so that the option becomes visible). Enter a *Source: IP Prefix* of *10.30.10.0/24* and click on **Actions**



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**

Activate Policy

Policy will be applied to the reachable devices:
10.255.255.3, 10.255.255.5

Activate **Cancel**

Cisco vManage admin

CONFIGURATION | TEMPLATES

'Configure' action will be applied to 2 device(s) attached to 1 device template(s).

Device Template	Total
vSmart-dev-temp	1

Please select a device from the device list

Device list (Total: 2 devices)

Filter/Search

- 20607a12-c0c8-4f46-a65f-5a547cdf3325
vSmart1|10.255.255.3
- 7f332491-cb6f-4843-8bf5-060f90df8dec
vSmart2|10.255.255.5

Configure Device Rollback Timer **Back** **Configure Devices** **Cancel**

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**

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

CONFIGURATION | POLICIES Centralized Policy > Edit Policy

Policy Application Topology Traffic Rules

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

From Service From Tunnel All

Select Site List Site30 x

Select VPN List Corporate x

Add Cancel

Site List	VPN List	Direction	Action
-----------	----------	-----------	--------

Preview Save Policy Changes CANCEL

9. Choose to **Activate** the configuration

Activate Policy

Policy will be applied to the reachable devices:
10.255.255.3, 10.255.255.5

Activate Cancel

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

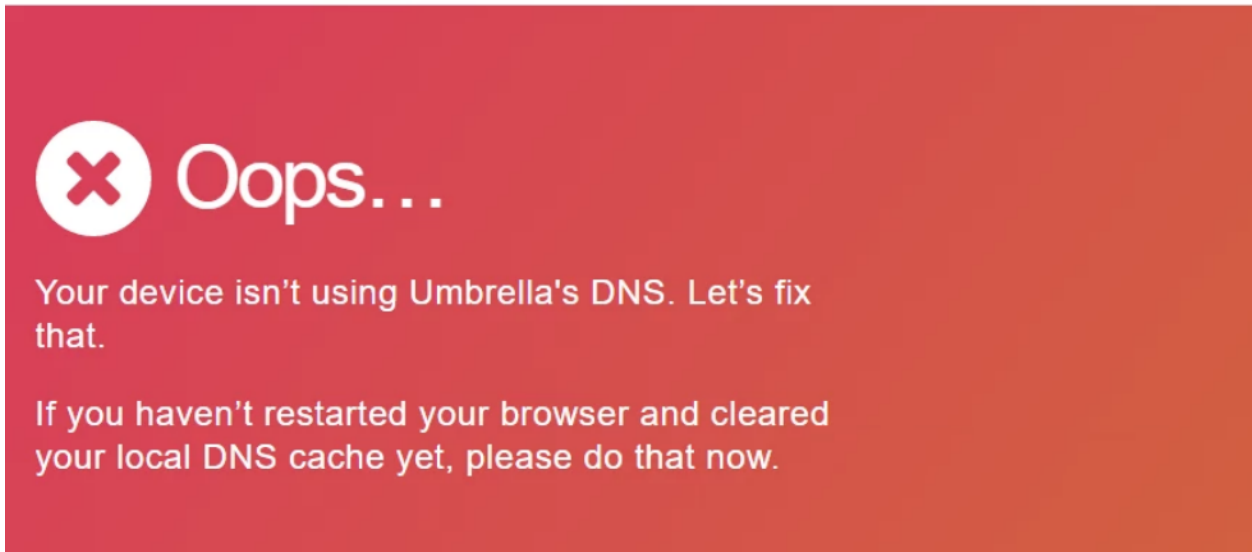
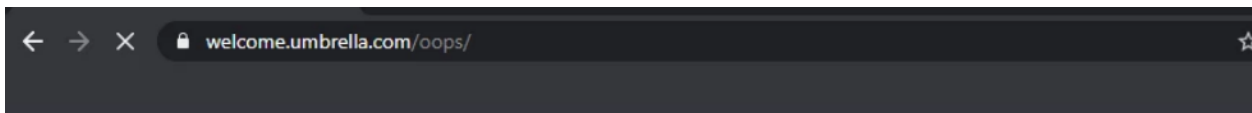
- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- Life without Cisco Umbrella
- Basic Configuration for Umbrella
- Making Umbrella Ours
 - API Keys and AD Configuration

- 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

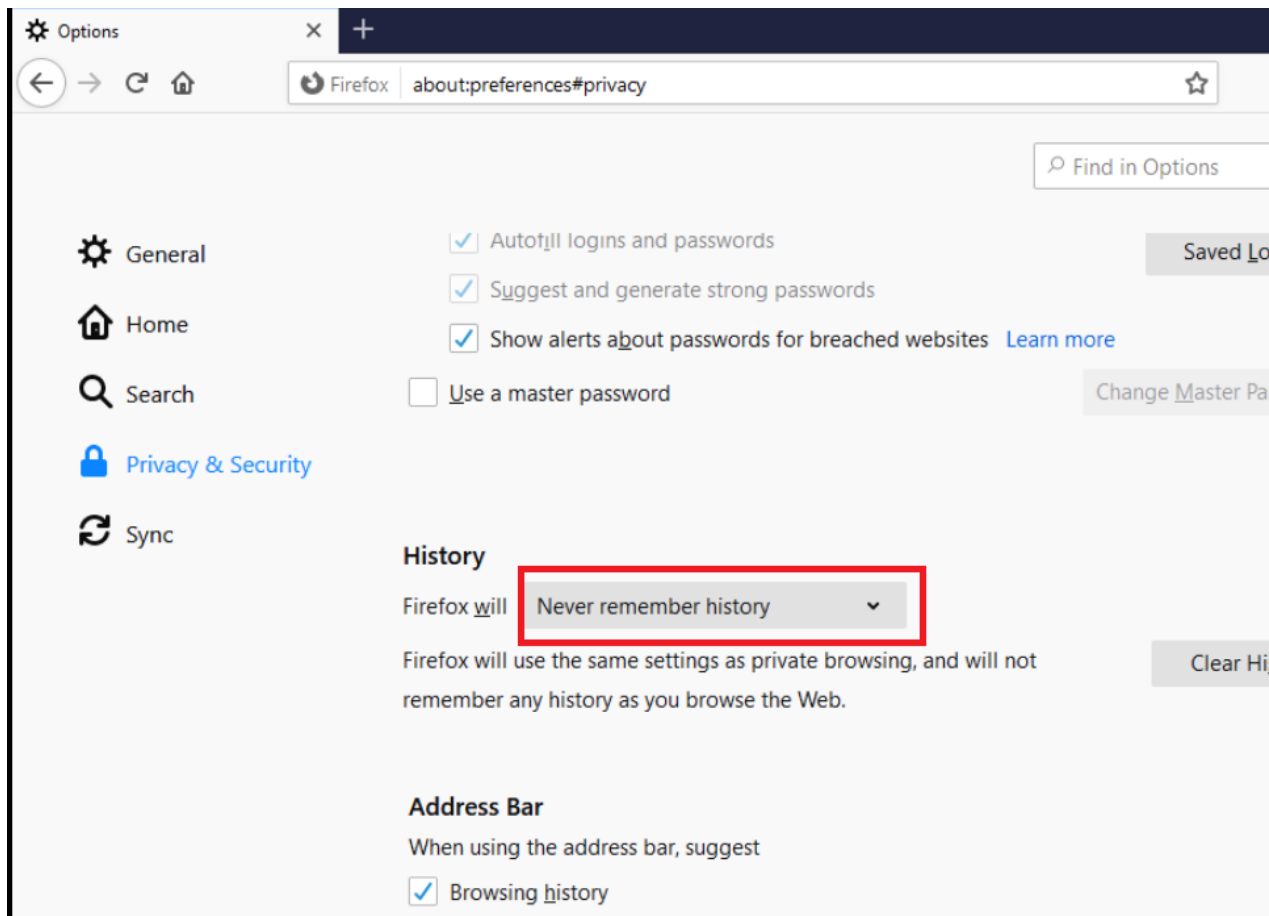
As of now, the Site 30 PC has connectivity to the Internet and is pointing to the DNS Server of *10.30.10.50*. DNS Queries sent to this DNS Server are redirected to 8.8.8.8 or 4.2.2.2. We will run a quick check from our Site 30 PC to verify that we are NOT connected to Cisco Umbrella as of now.

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**



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



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

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](#)

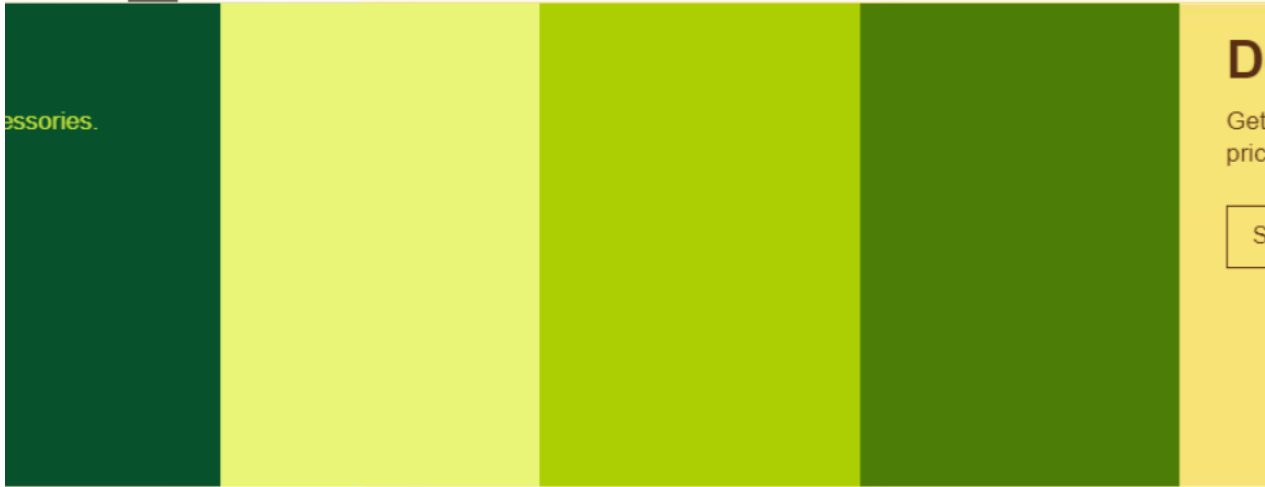
Shop by Category



AmazonBasics



Electronics



Popular Destinations | [See all](#) →

yahoo!



Sign in



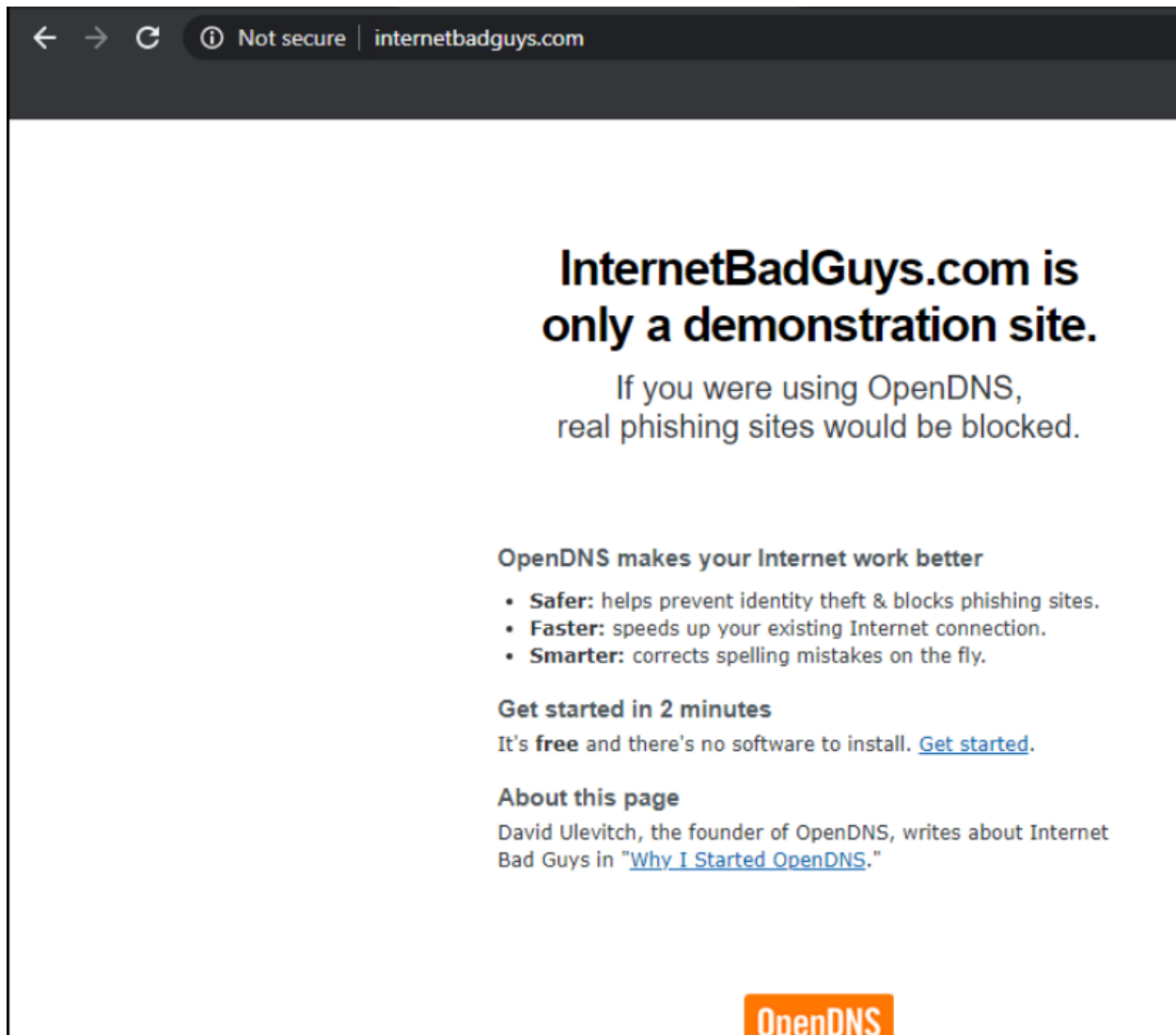
- Mail
- Coronavirus
- Cricket
- News
- Finance
- Lifestyle
- Movies
- Women
- More...

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



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

Apache Guacamole x +

← → ↻ Not secure | 10.2.1.203:8080/guacamole/#/

Use the URL provided for your POD



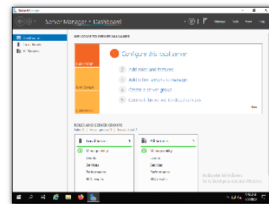
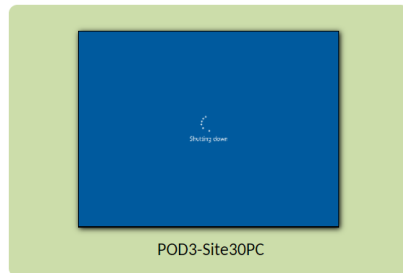
APACHE GUACAMOLE

sdwanpod

.....

Login

RECENT CONNECTIONS



ALL CONNECTIONS

Filter

- POD3-AD
- POD3-Jumphost
- POD3-Site30PC

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*

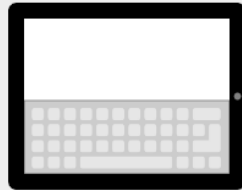
Input method

 None

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.

Press Ctrl + Alt + Shift to
open this Window (via
Guacamole)

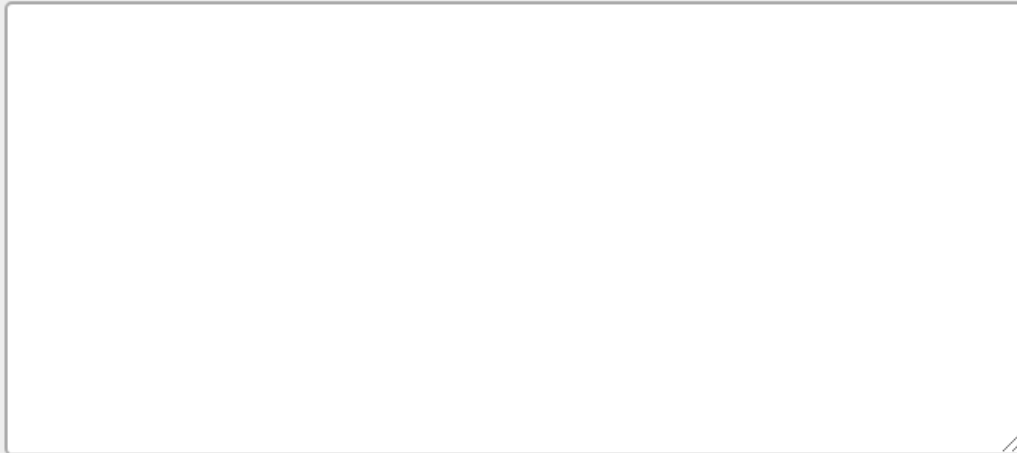




This will bring you to the login screen. Press **Ctrl + Alt + Shift** on your keyboard to bring up the Guacamole settings window again and choose **None** for the Input Method

Clipboard

Text copied/cut within Guacamole will appear here. Changes to the text below will affect the remote clipboard.



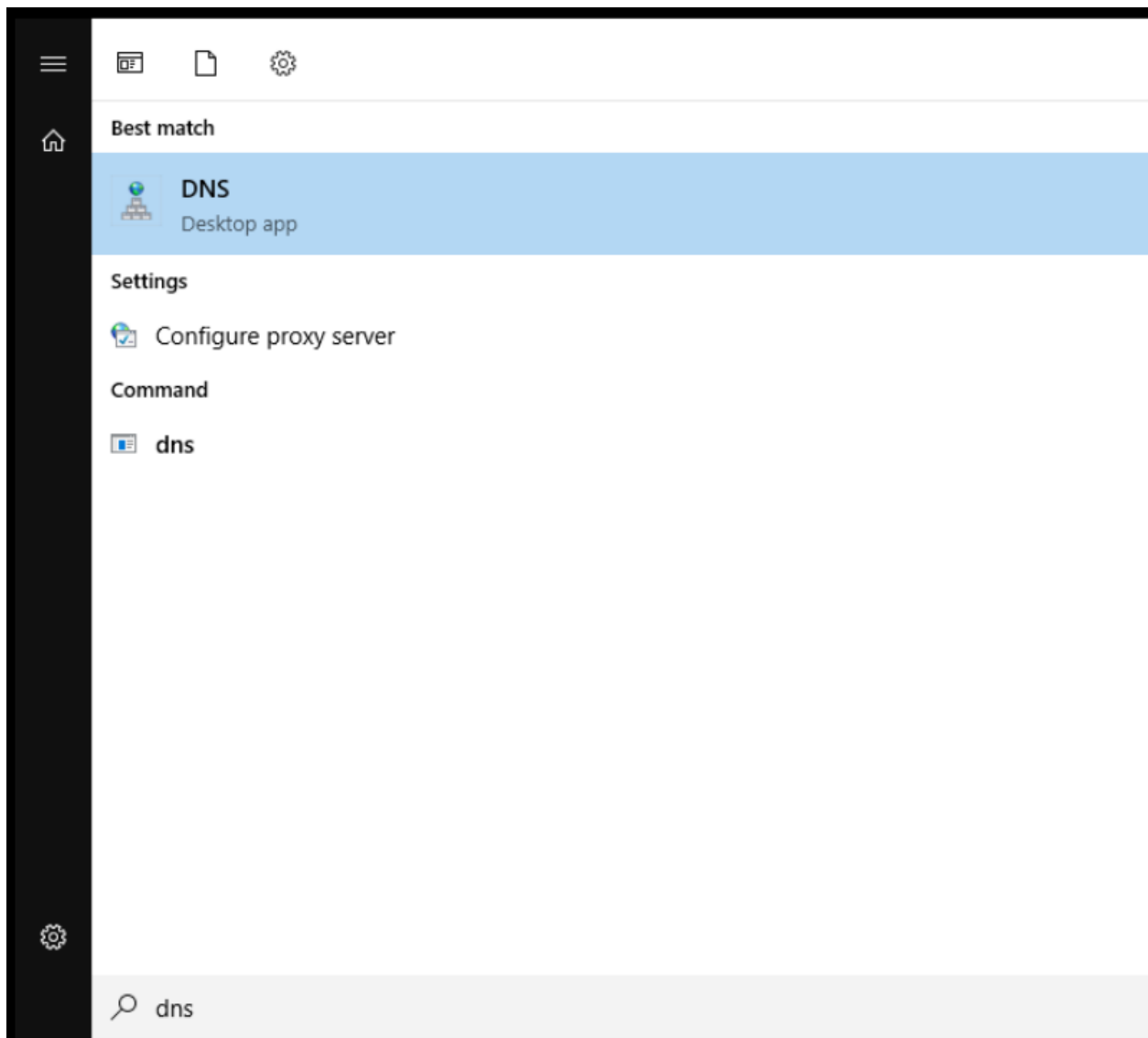
Input method

None

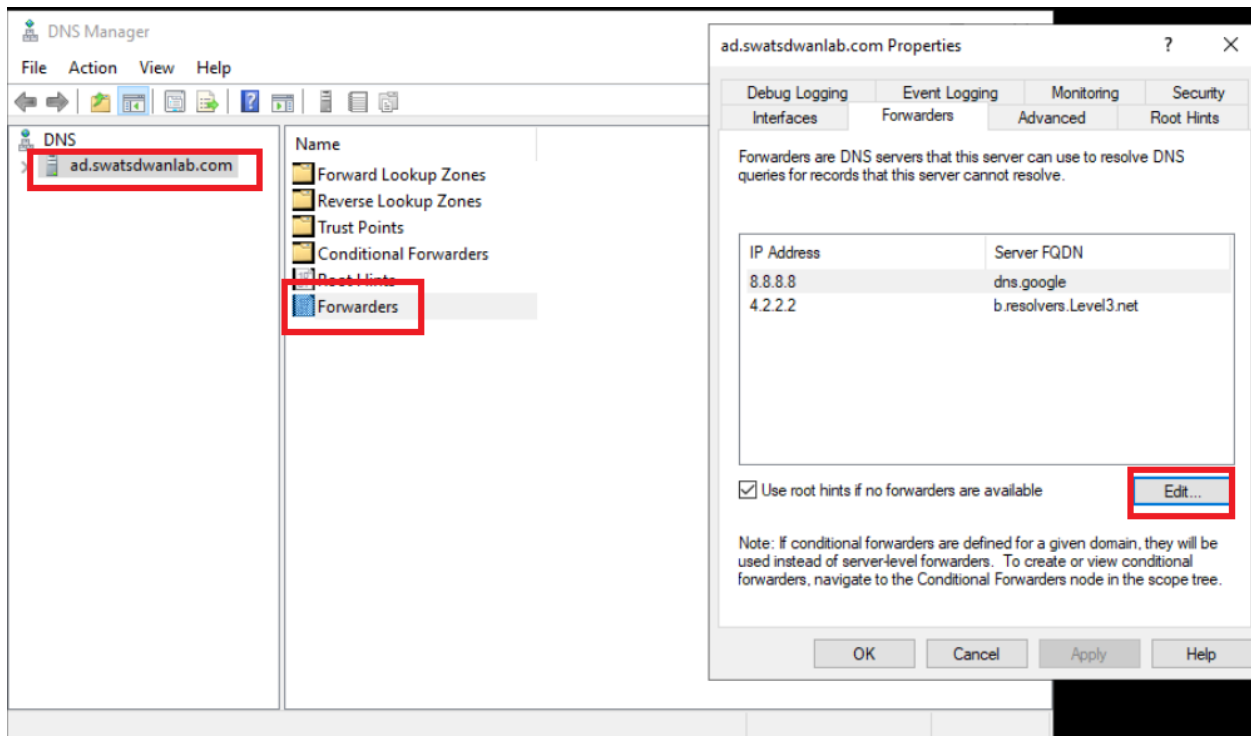
No input method is used. Keyboard input is accepted from a connected, physical keyboard.

This will remove the virtual keyboard from the screen and you can continue typing like normal to enter the password.

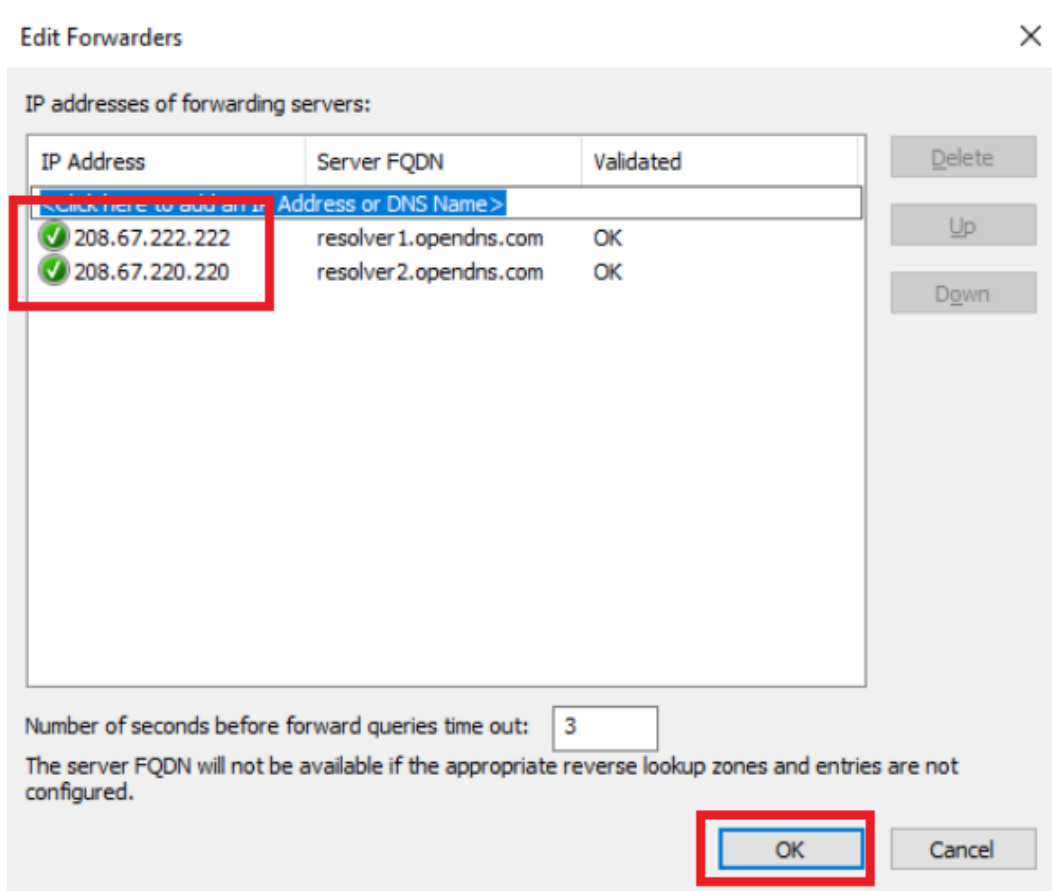
3. Once logged in to the AD PC, click on **Start** and search for *DNS*. Open the DNS application



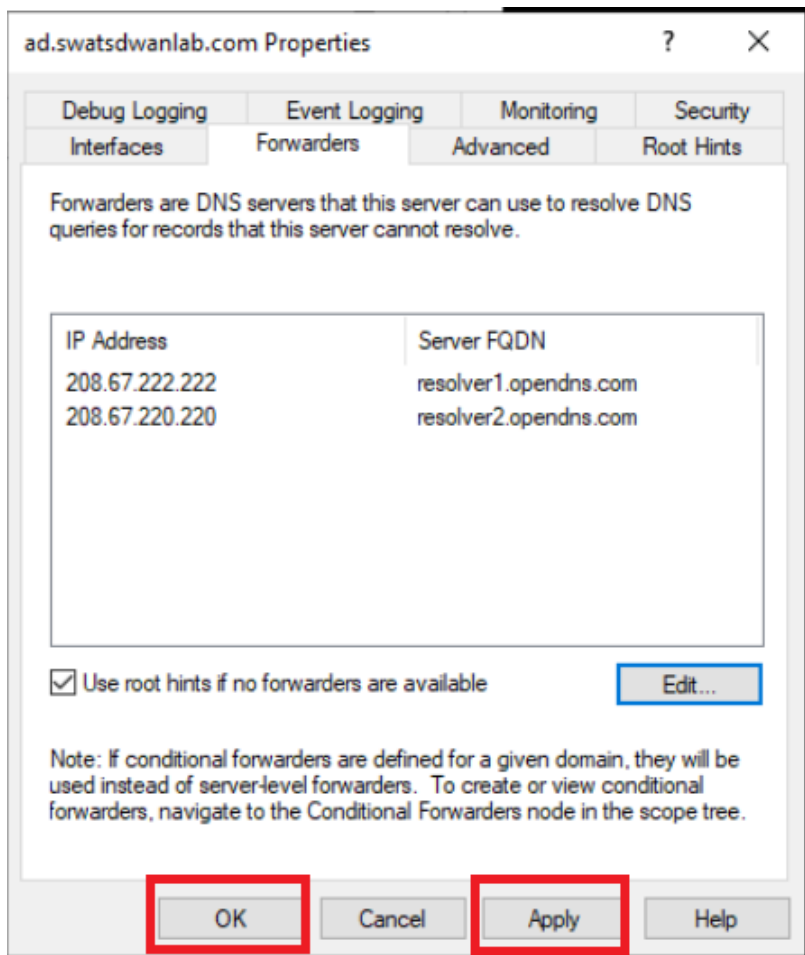
4. Select *ad.swatsdwanlab.com* and double-click Forwarders. There will be two Forwarders listed (*8.8.8.8* and *4.2.2.2*). Click on **Edit**

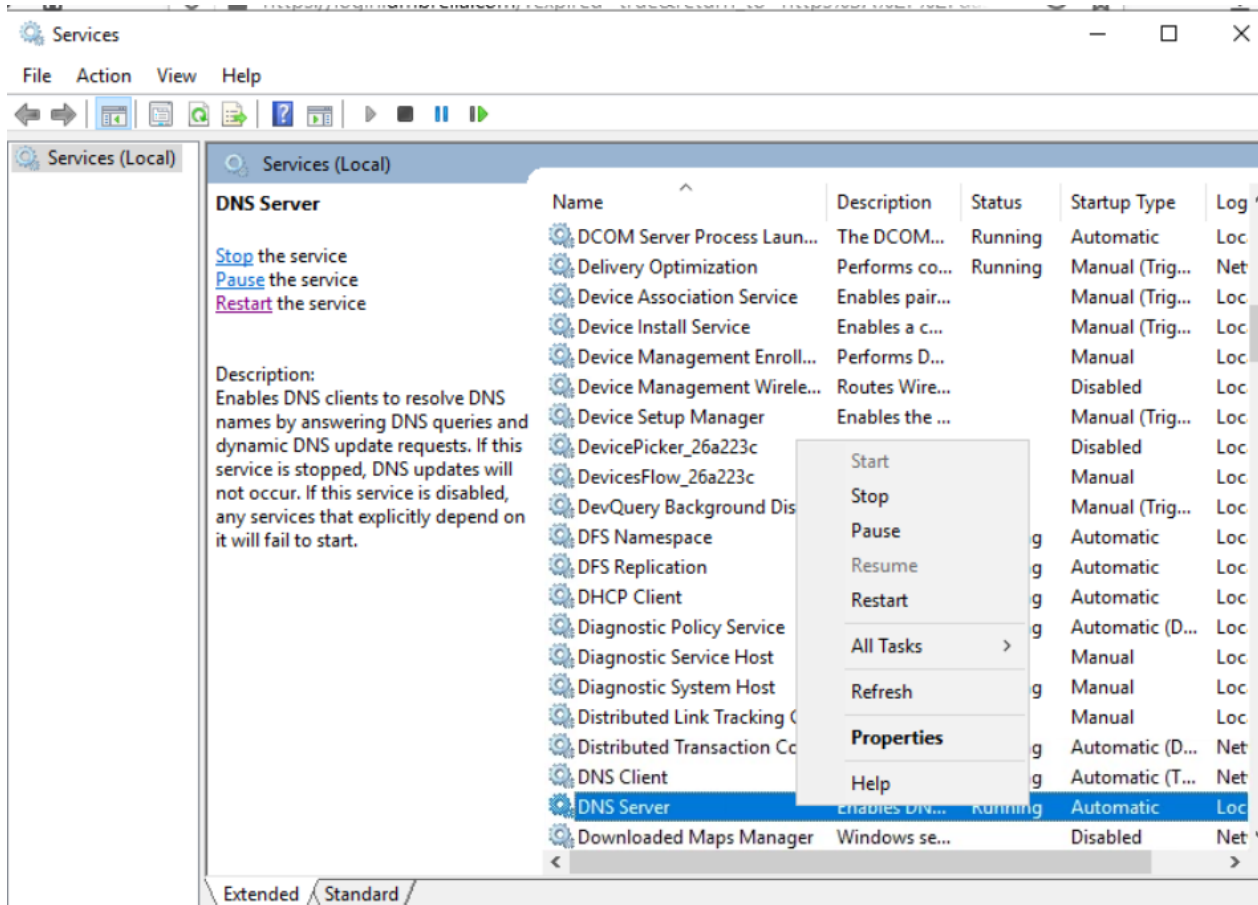


5. Change the Forwarder IPs to *208.67.222.222* and *208.67.220.220*. Make sure no other Forwarders are present on this window. Click on **OK**

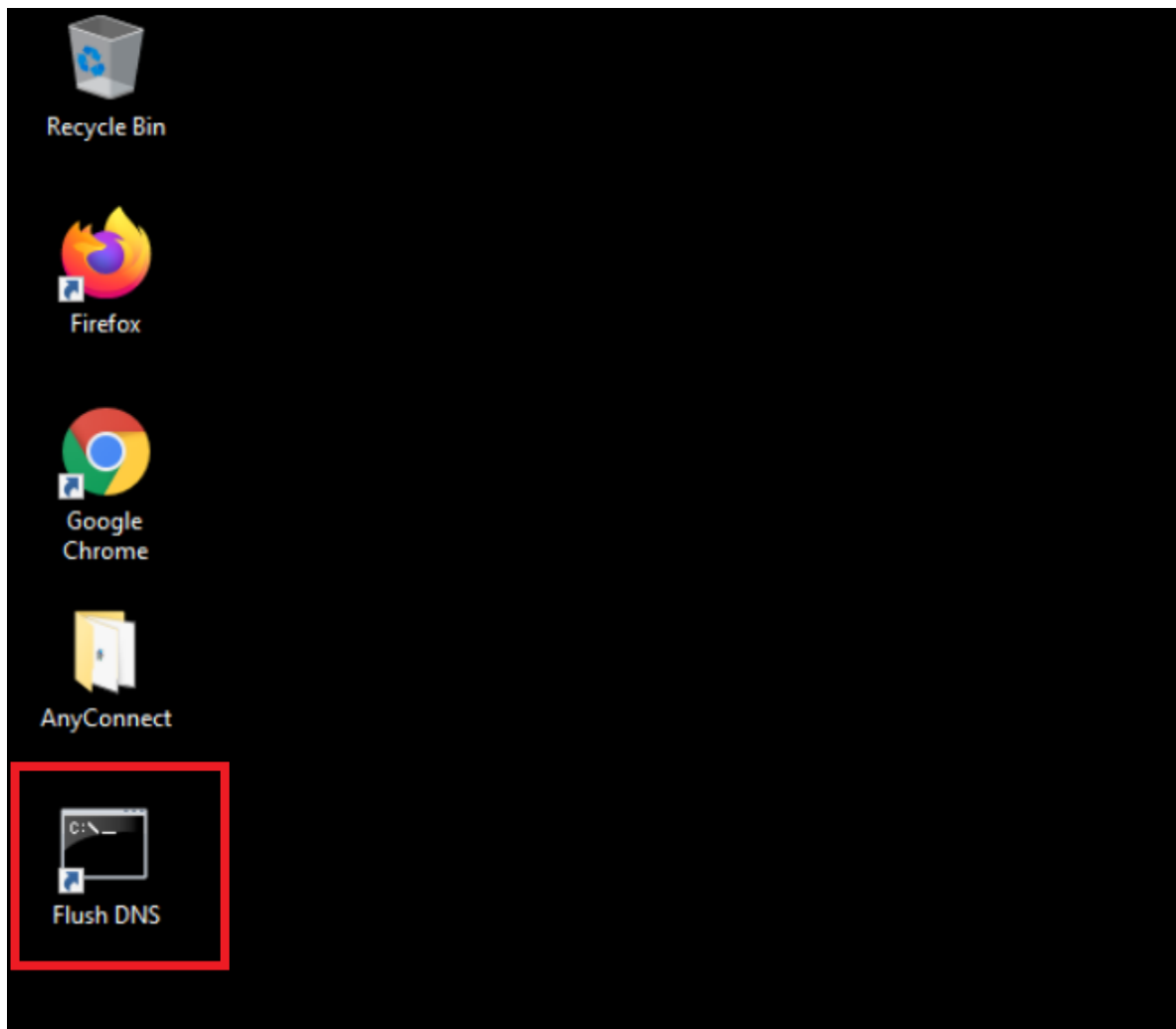


6. Click on **Apply** and then **OK** to apply the configuration change. Click on Start and type **services.msc**. Hit Enter and look for the DNS Server service. Right click on it and restart the service



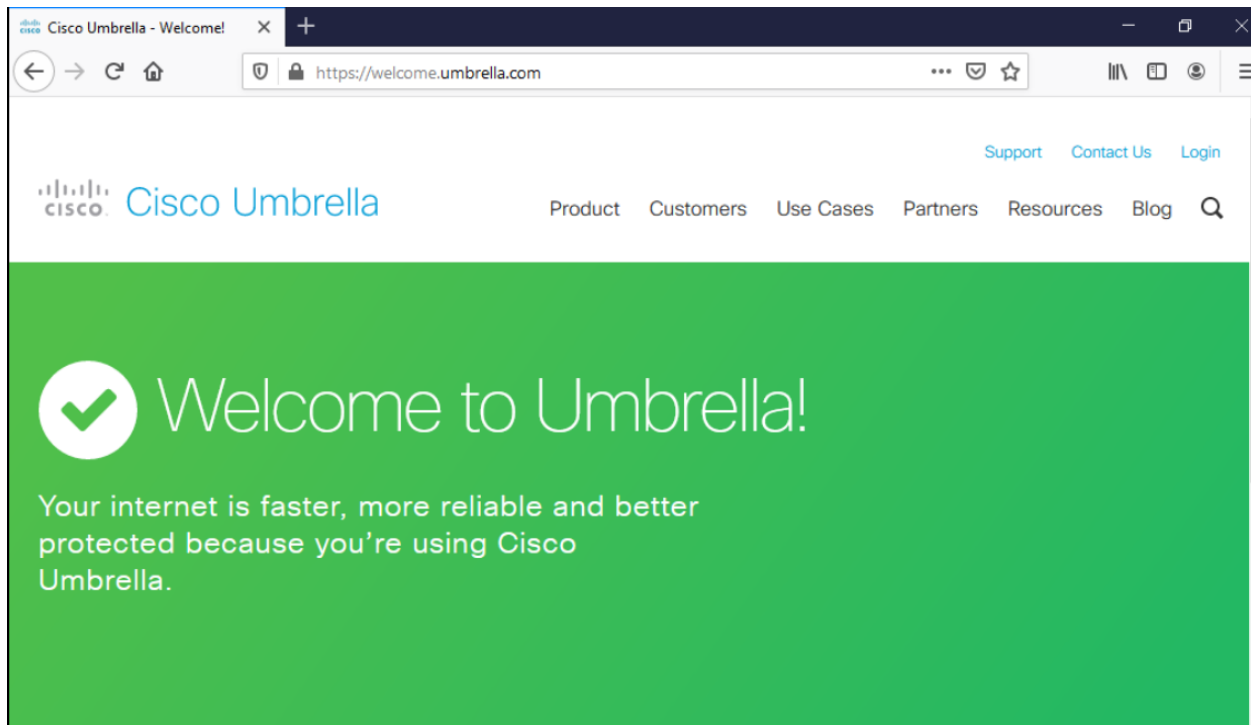


7. Head back to the Site 30 PC and click on the **Flush DNS** shortcut on the Desktop

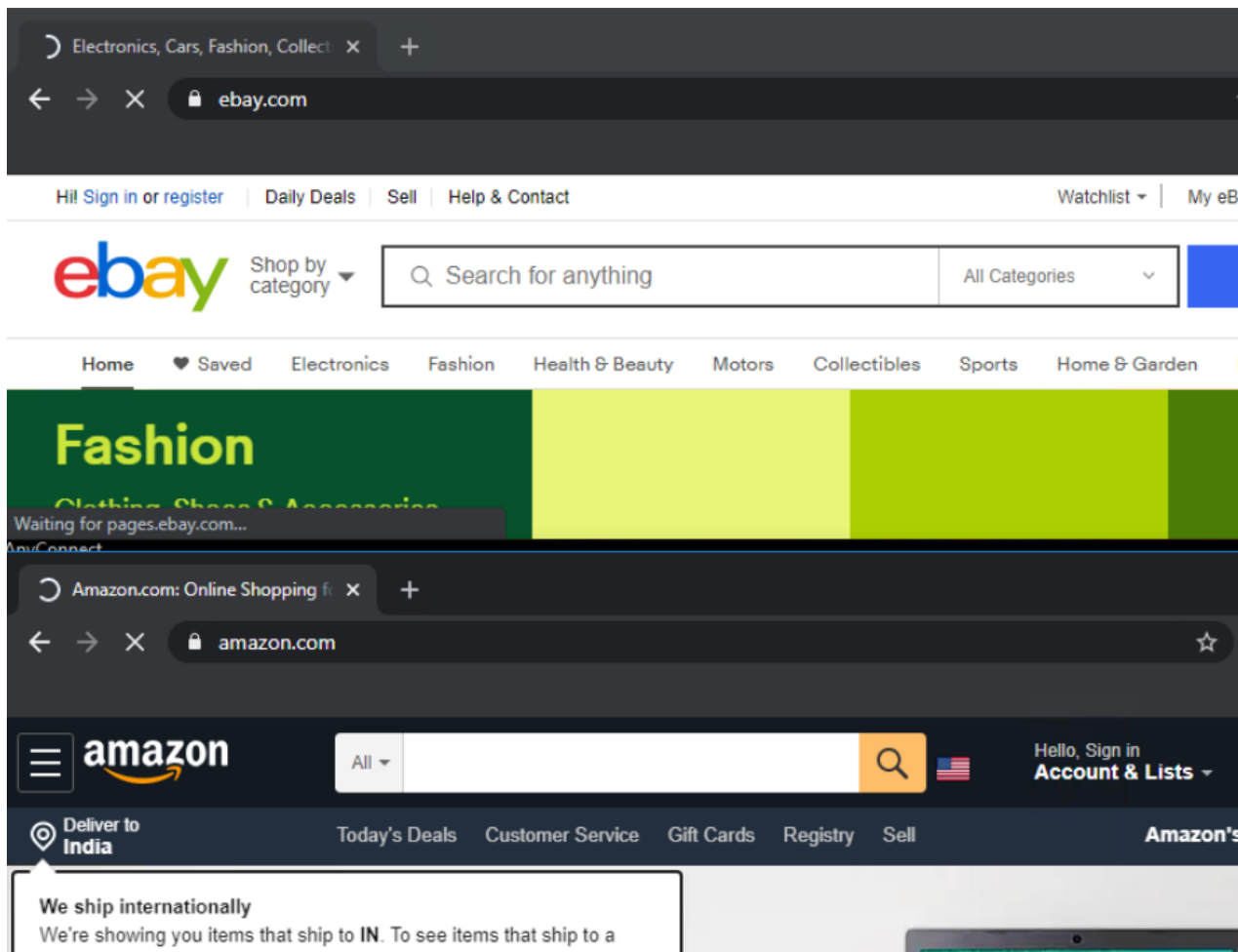


```
Flush DNS
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Windows\System32>
```

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




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

Phishing Site Blocked

phish.opendns.com/main?url=internetbadguys.com&server=hkg15&prefs=&tagging=&nref



 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

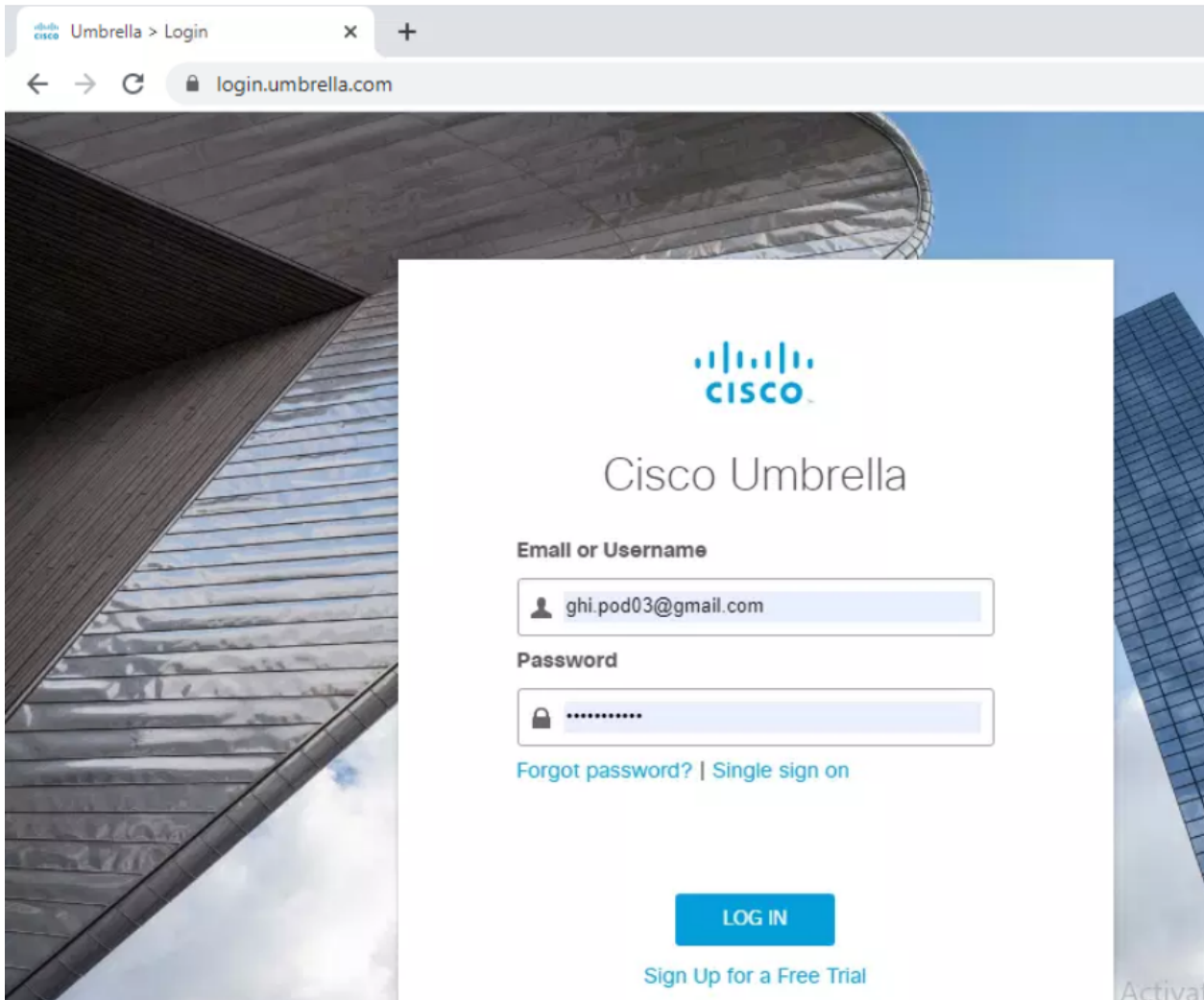
Three pieces of the puzzle that uniquely identify our Enterprise Network on Umbrella are given below:

- Organization (this is a numeric string, allocated by Umbrella. Not to be confused with the SD-WAN organization name)
- API Key

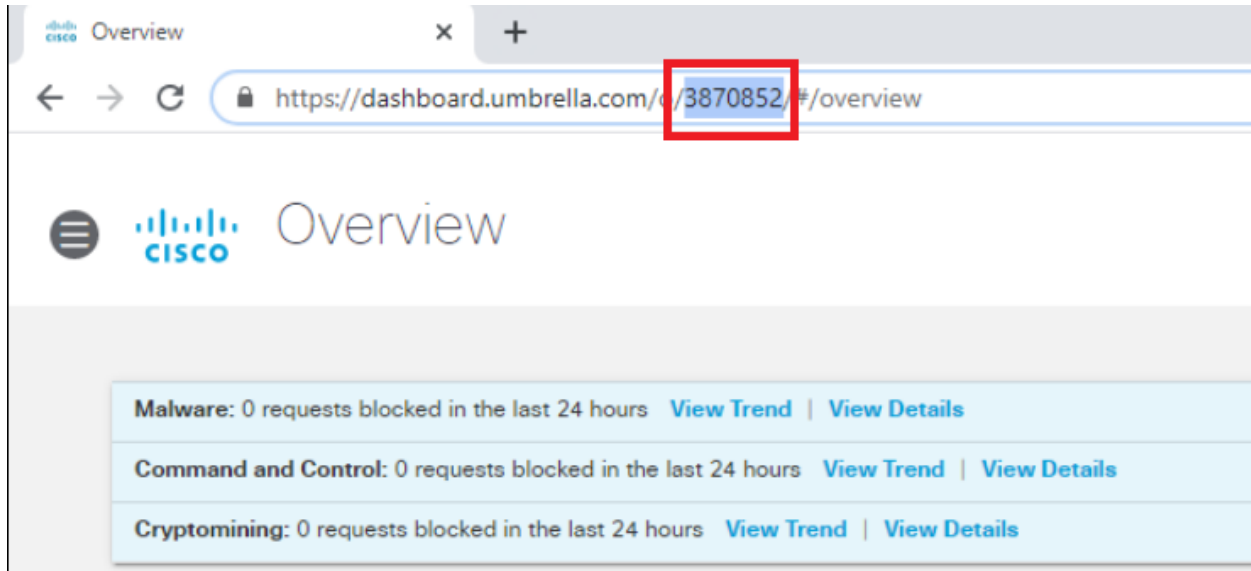
- Secret

1. From your Jumphost, open a browser and go to login.umbrella.com. Login using the username/password for your POD

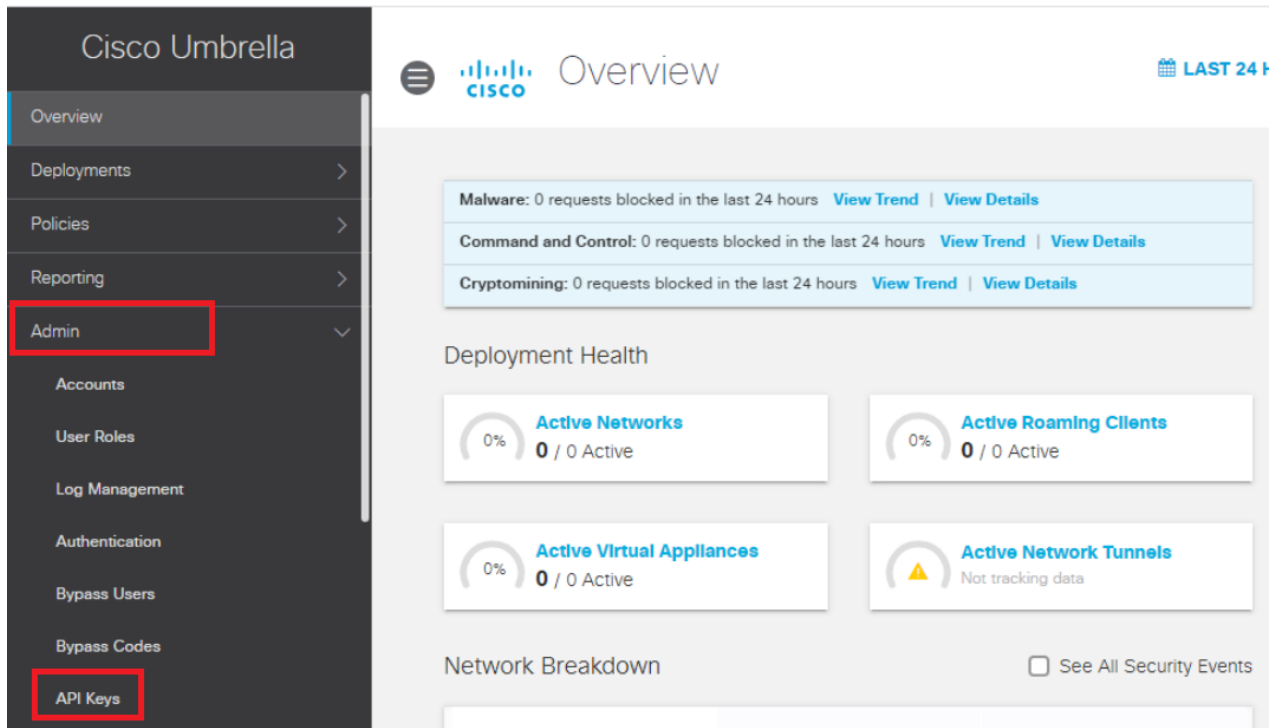
Username	Password
ghi.pod0X@gmail.com	C1sco@12345
X is your POD number	



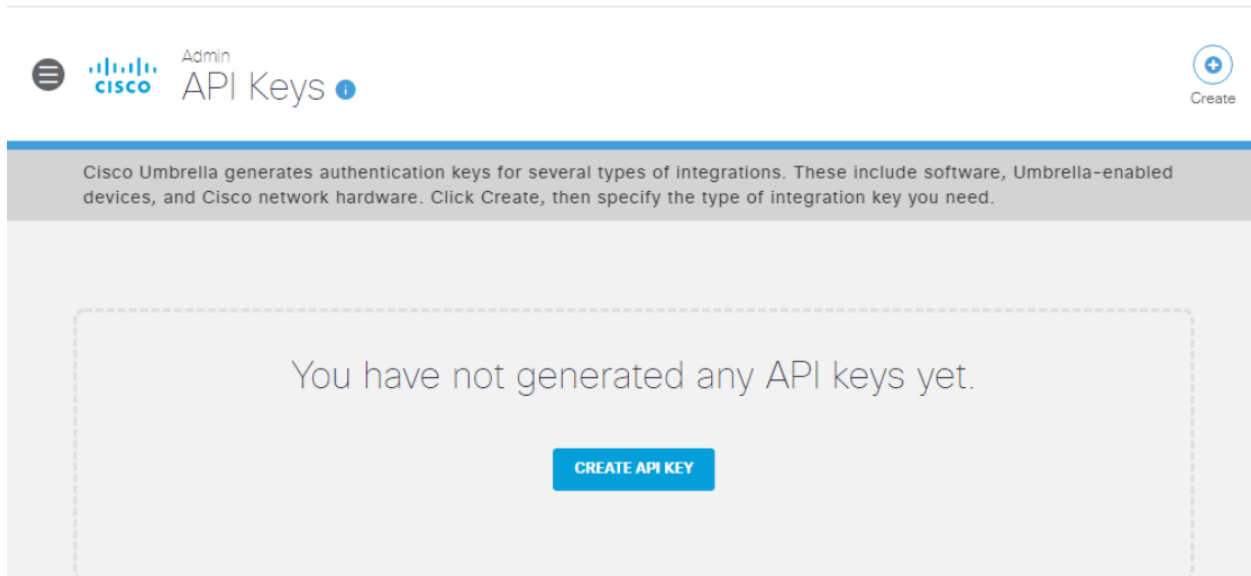
2. Once logged in, the URL will contain your Organization ID. It will vary per POD. Copy it in a notepad file on the Jumphost since we will be needing it later



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



4. Click on **Create API Key**



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 details.

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**

Untitled - Notepad

File Edit Format View Help

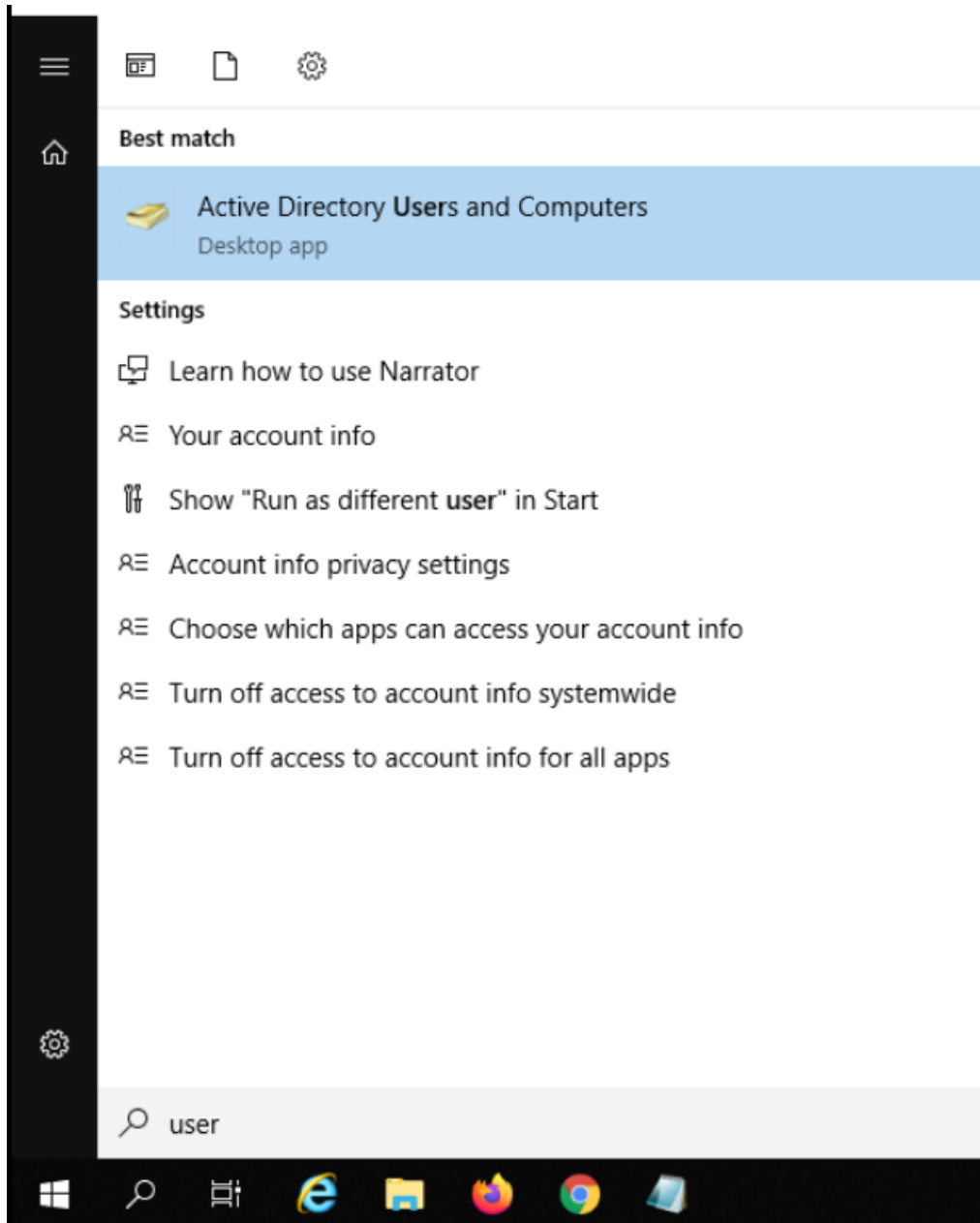
Org: 3870852
Key: 8cbbd34d46614584a8f11a9b2c6cb861
Secret: fcdea273e6ed4e2f9722a3c13ee1a79d

Windows (CRLF)

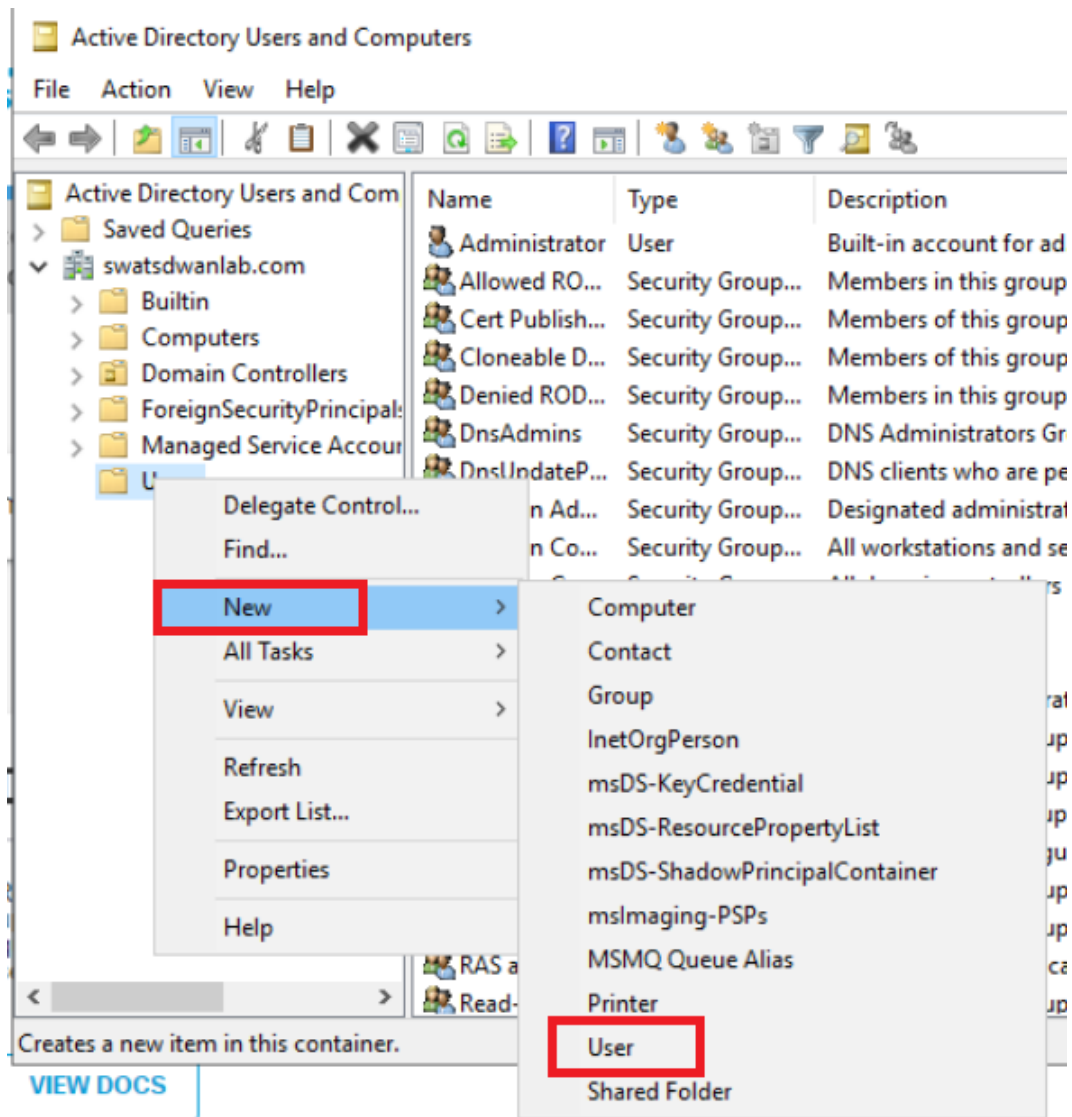
Copy the Org, API Key and Secret to a notepad file (will be needed later)

✔ **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



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.

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: swatsdwanlab.com/Users'. Below this, there are several input fields: 'First name' (OpenDNS_Connector), 'Initials' (empty), 'Last name' (empty), and 'Full name' (OpenDNS_Connector). The 'User logon name' field is highlighted with a red box and contains 'OpenDNS_Connector'. To its right is a dropdown menu showing '@swatsdwanlab.com'. Below these is the 'User logon name (pre-Windows 2000):' section with two fields: 'SWATSDWANLAB\' and 'OpenDNS_Connector'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

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 ✕

 Create in: swatsdwanlab.com/Users

Password:

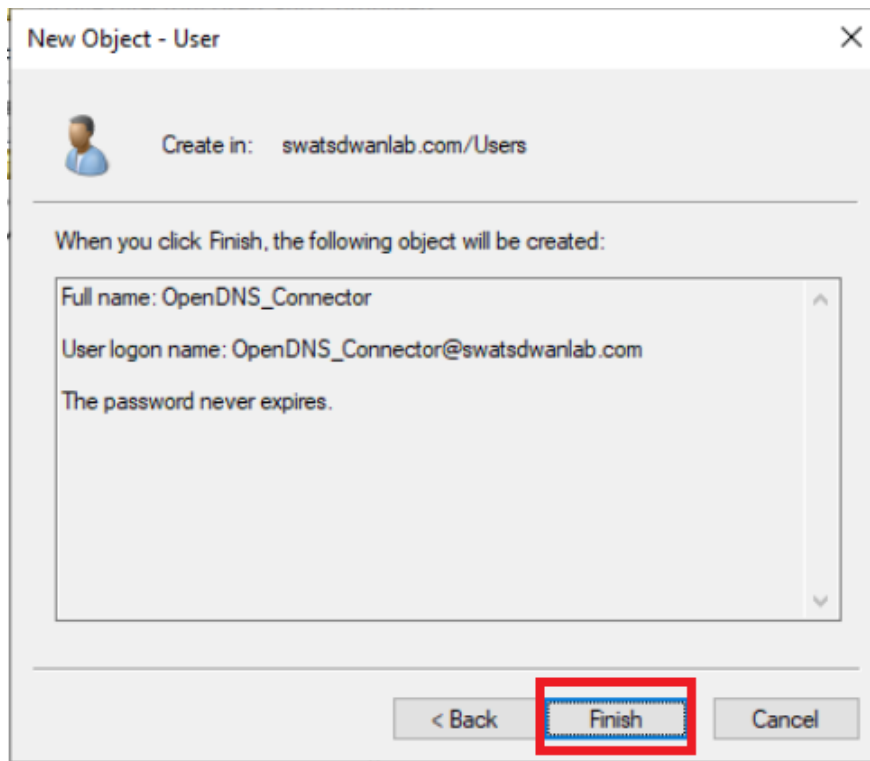
Confirm password:

User must change password at next logon

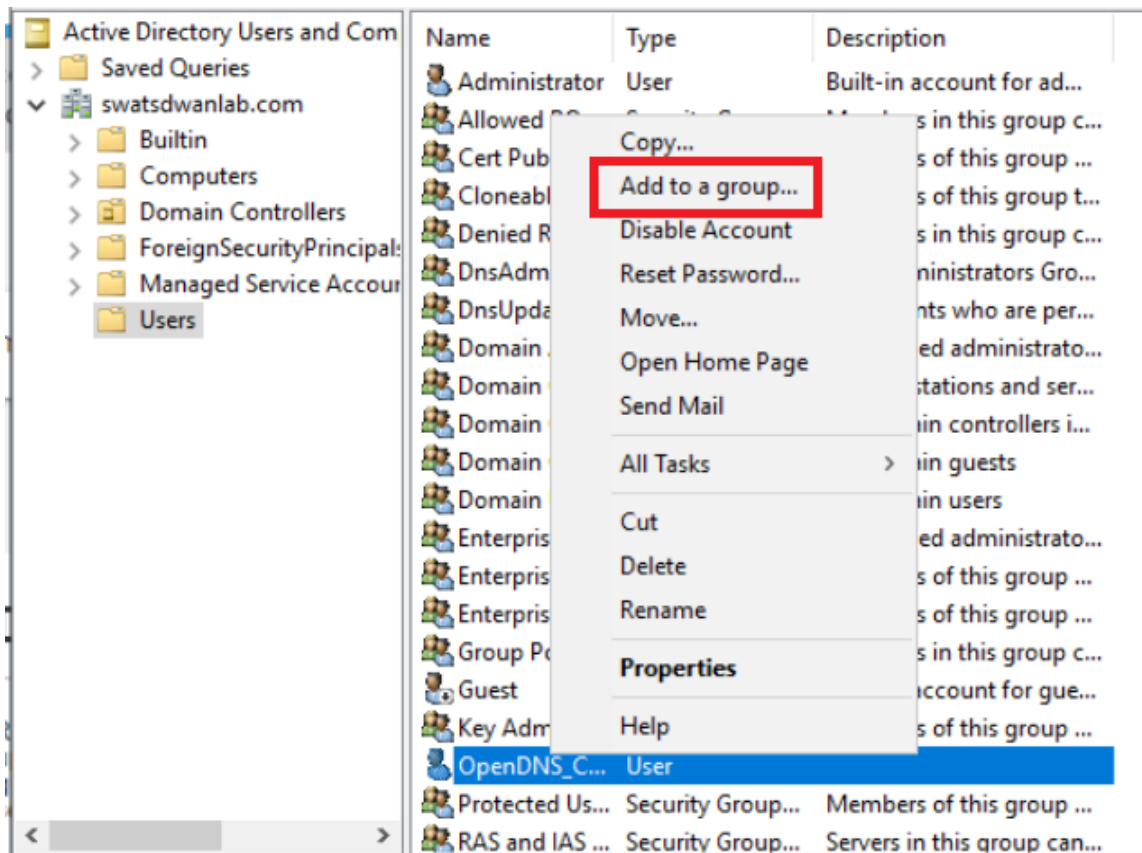
User cannot change password

Password never expires

Account is disabled



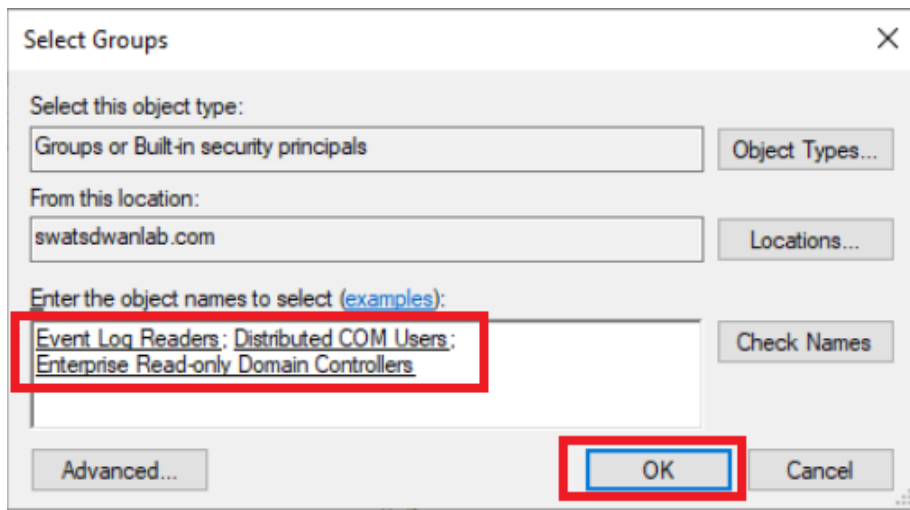
11. The user we just created needs to be a part of certain Groups in order to function properly. Right click on the newly created *OpenDNS_Connector* user and click on **Add to a group**



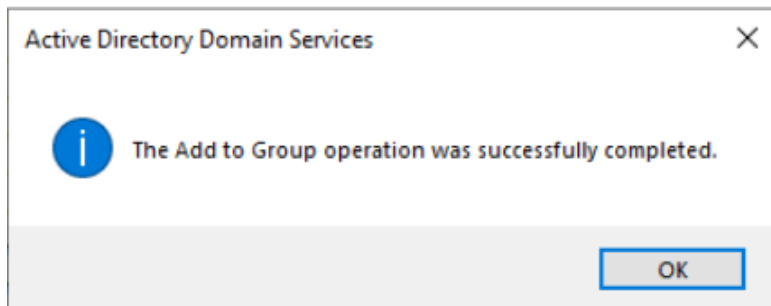
12. Add the user to the following groups and click on **OK**:

- 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	

Cisco Umbrella

Admin
API Keys ⓘ

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

Cisco Umbrella generates authentication keys for sev software, Umbrella-enabled devices, and Cisco netw type of integration key you need.

Umbrella Management	Key: 8cbbd34d46
---------------------	--------------------

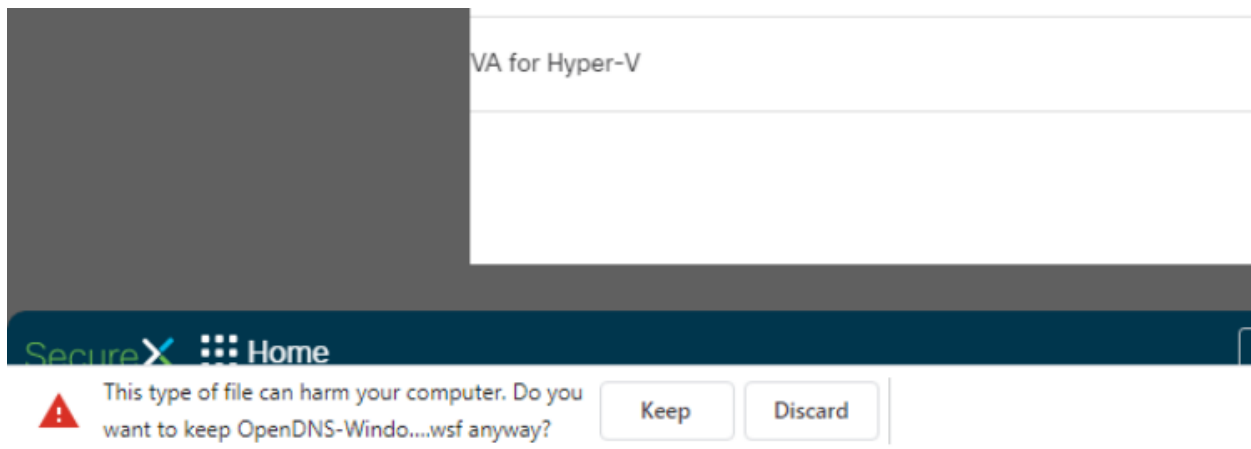
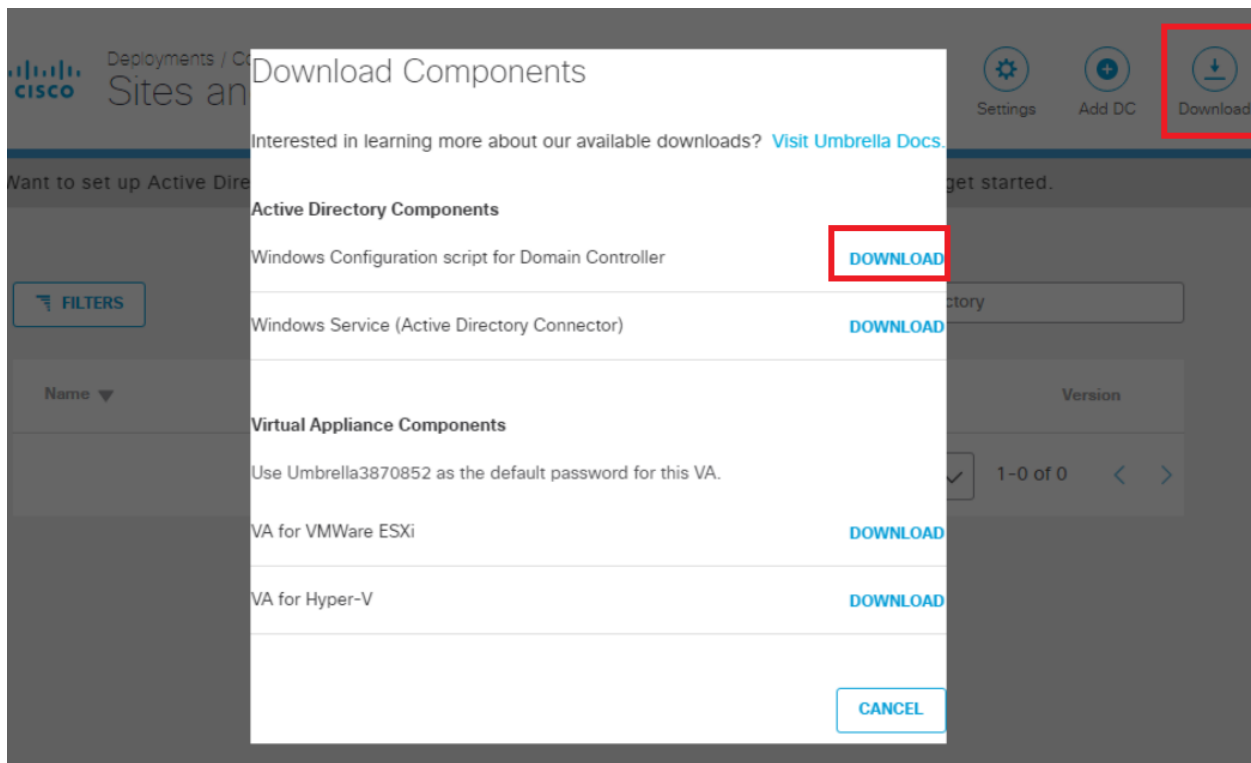
Documentation

Read here to get authentication set up for your first endpoint queries, explore what you can do and search for any answers you need.

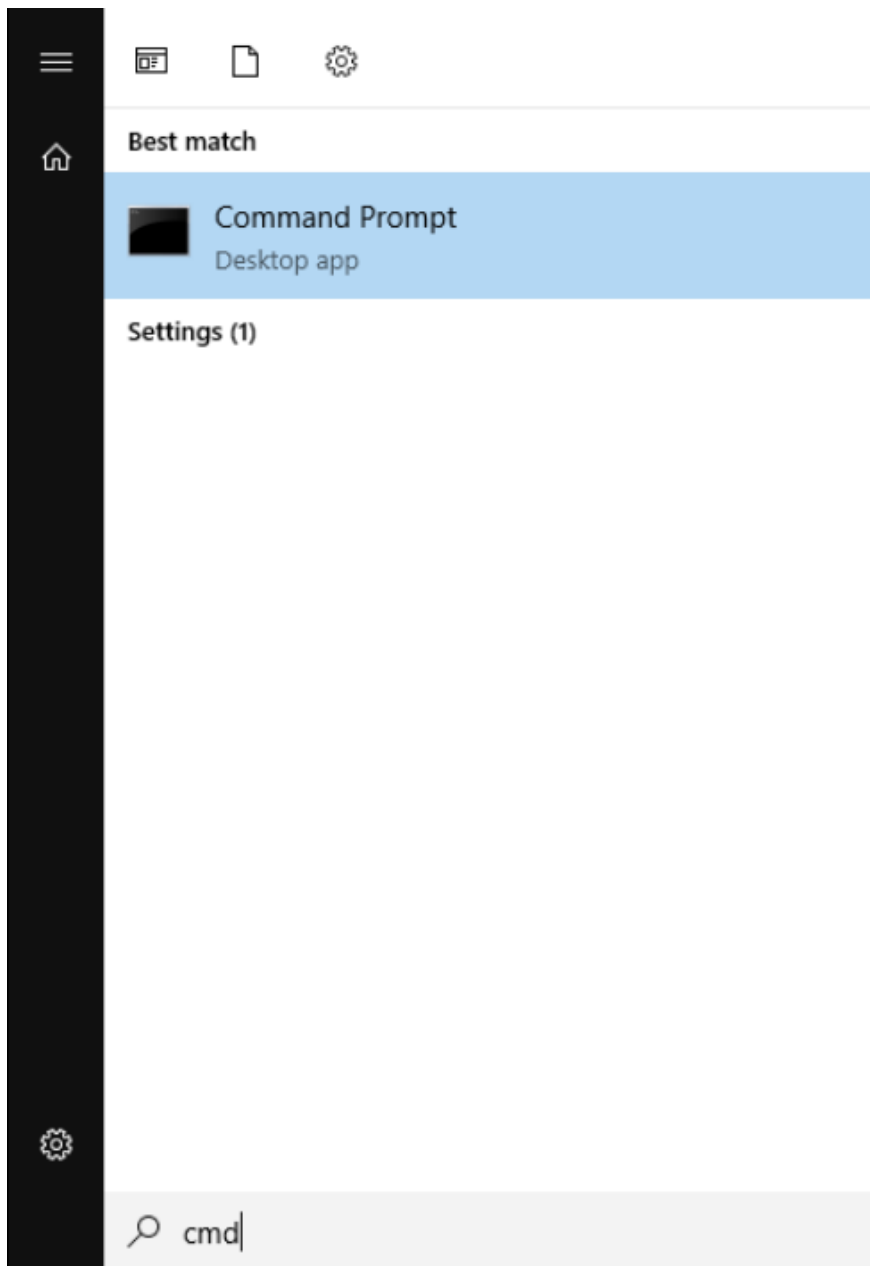
Our Le...

Some of our different auth than what you and have unic

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 Controlle
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

Deployments / Configuration
Cisco Sites and Active Directory

Settings Add DC Download

Want to set up Active Directory integration or deploy Virtual Appliances? Click Download above to get started.

FILTERS Search Sites and Active Directory

Name ▼	Internal IP	Site	Type	Status	Version
AD.swatsdwanlab.com	10.30.10.50	Default Site	Domain Controller	Run: a minute ago	---

Page: 1 Results Per Page: 10 1-1 of 1

Task List

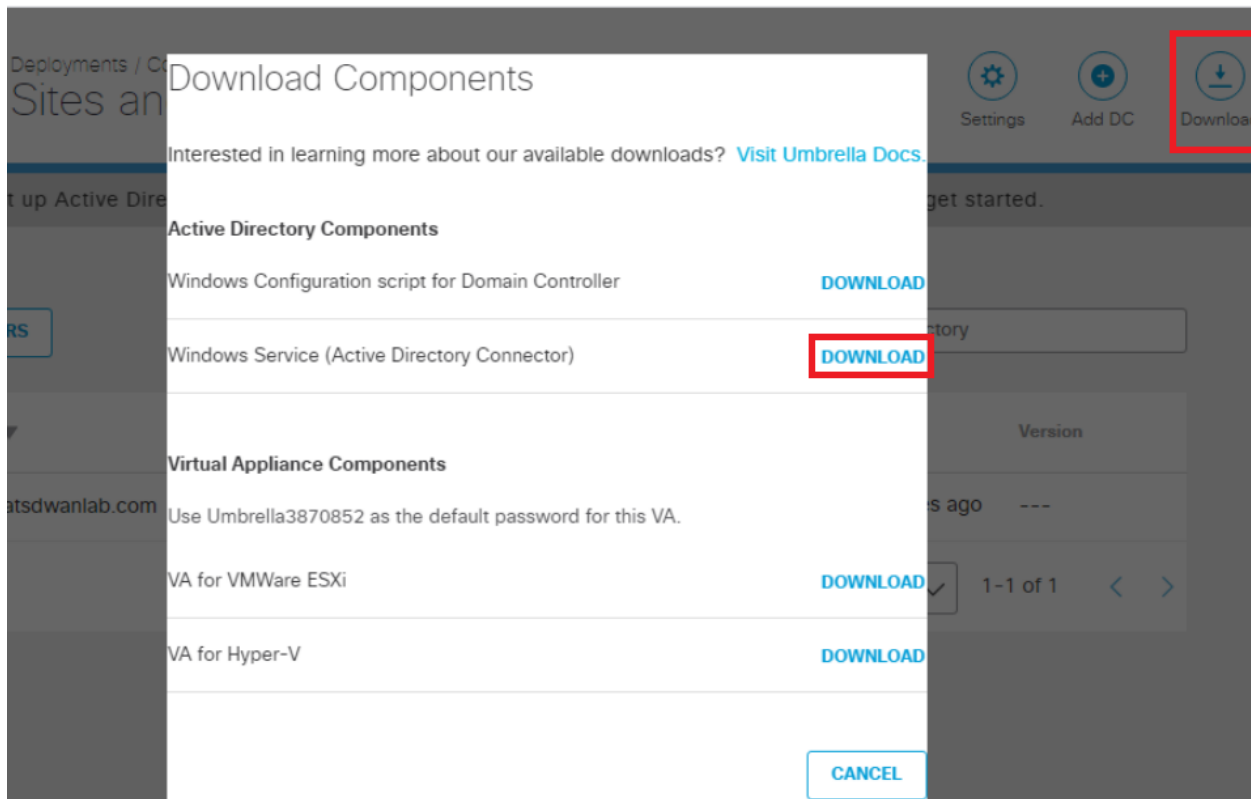
- Overview
- Pre-Work
- Enabling Site 30 for DIA
- Life without Cisco Umbrella
- Basic Configuration for Umbrella
- Making Umbrella Ours
 - API Keys and AD Configuration
 - DC Configuration Download

- AD Connectors
- Roaming Computer Configuration
- Building a DNS Policy
- Setting up IPSEC Tunnels
- Configuring a Firewall Policy
- Configuring a Web Policy

AD Connectors

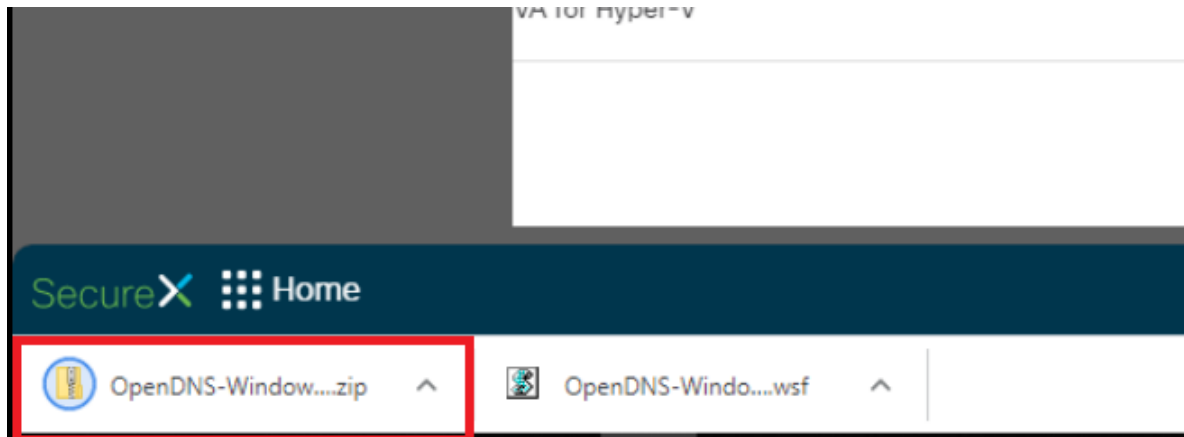
AD Connectors allow Umbrella to see your AD structure and reference AD Groups/Users in Policies.

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)**

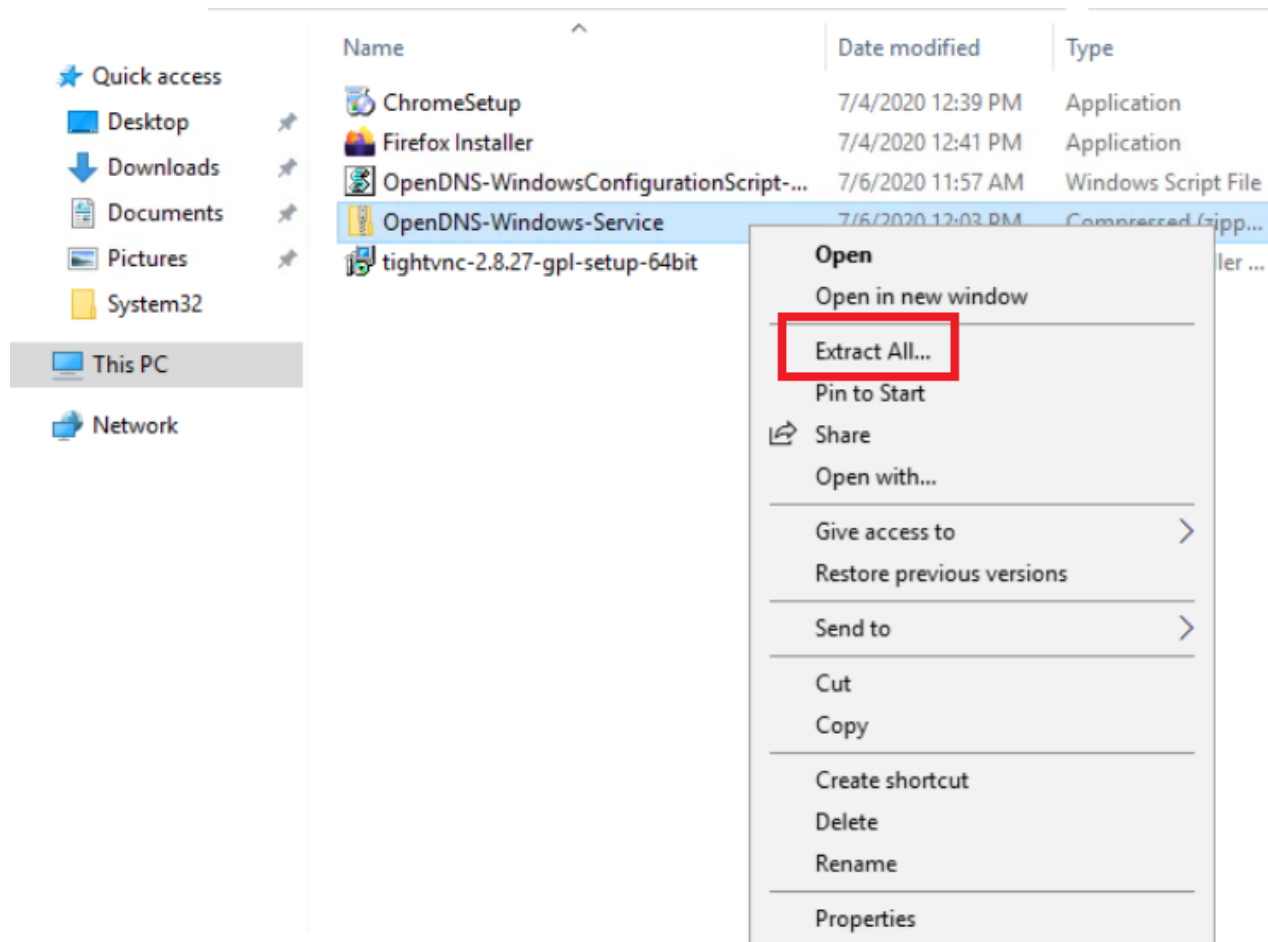


2. This will download a .zip file named *OpenDNS-Windows-Service.zip*. Click on the up arrow next to the downloaded file and choose to Open File Location (browser specific - Firefox has a folder icon in the list of downloads which takes you

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

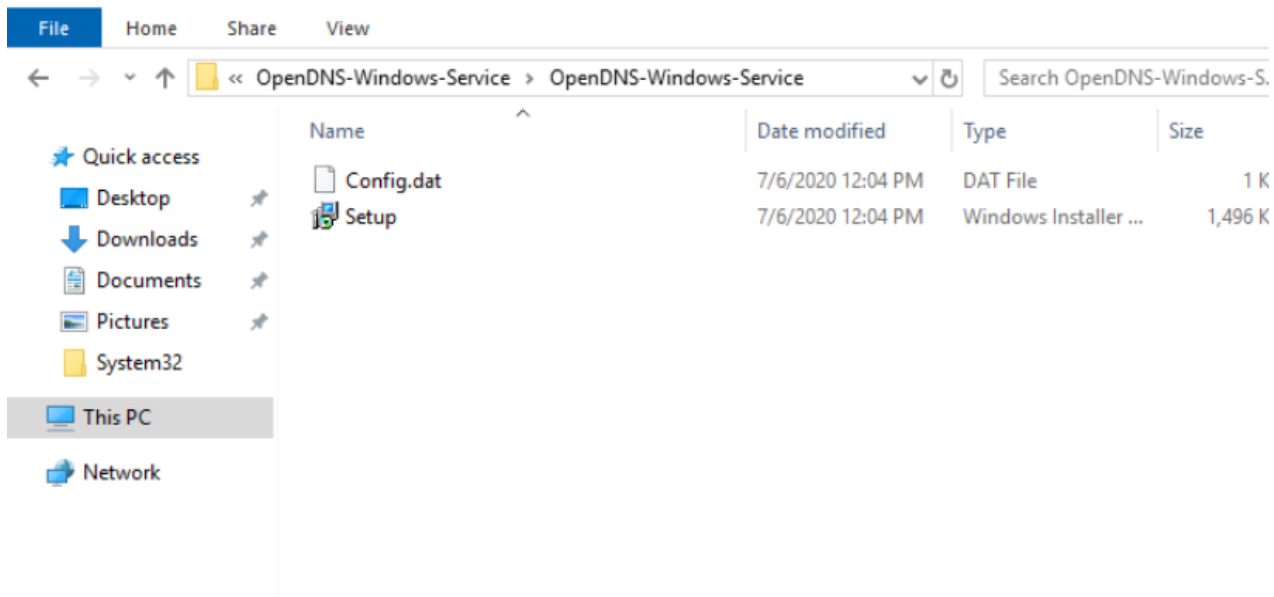
Browse...

Show extracted files when complete

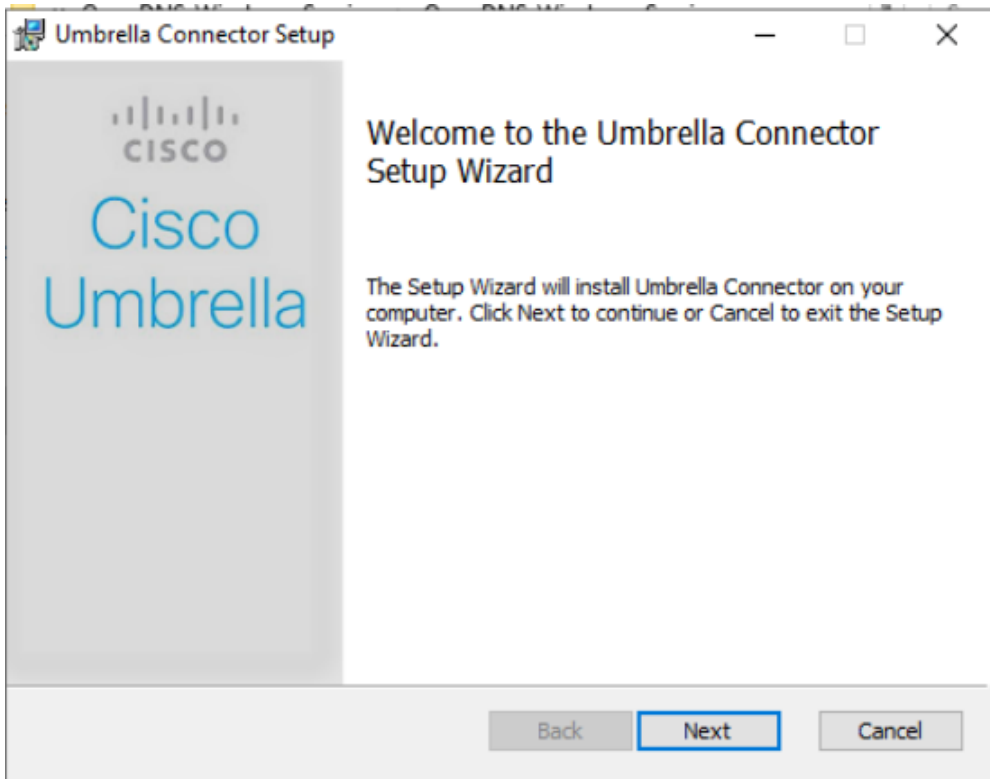
Extract

Cancel

5. 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

Destination Folder

Click Next to install to the default folder or click Change to choose another.



Install Umbrella Connector to:

C:\Program Files (x86)\OpenDNS\

Change...

Umbrella Connector Setup

Active Directory Credentials

Please supply your credentials to access Active Directory for monitoring.

CISCO

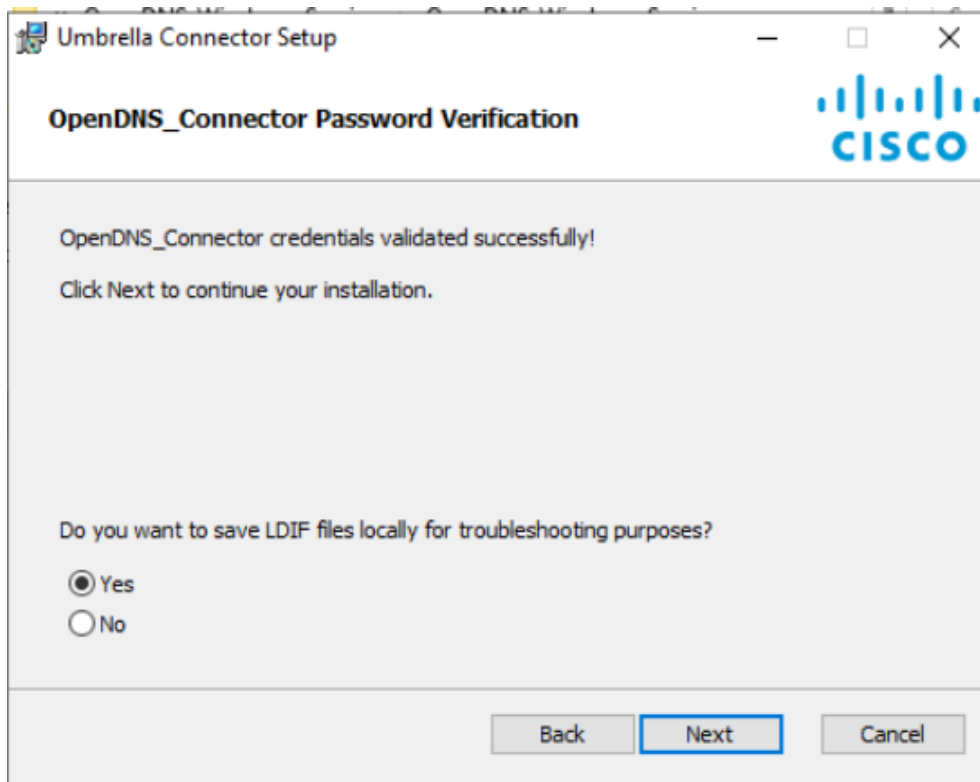
Username:
OpenDNS_Connector

Password:
C1sco12345

This password will be verified with the Domain Controller when you click 'Next'.

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

Umbrella Connector Setup



Ready to install Umbrella Connector

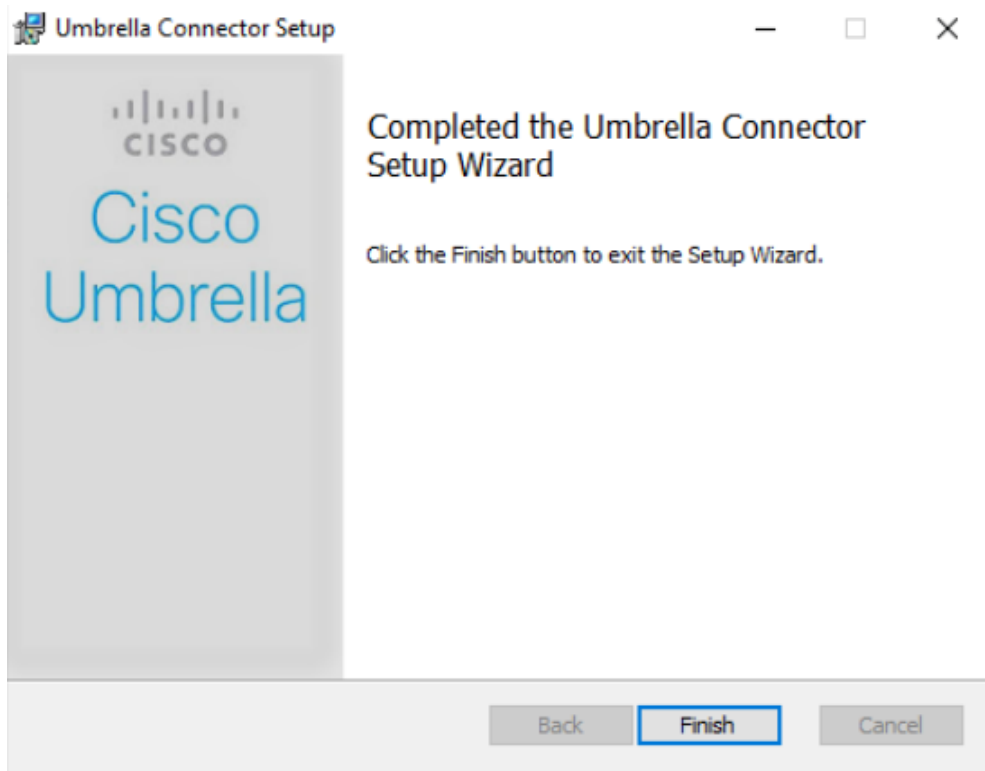


Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

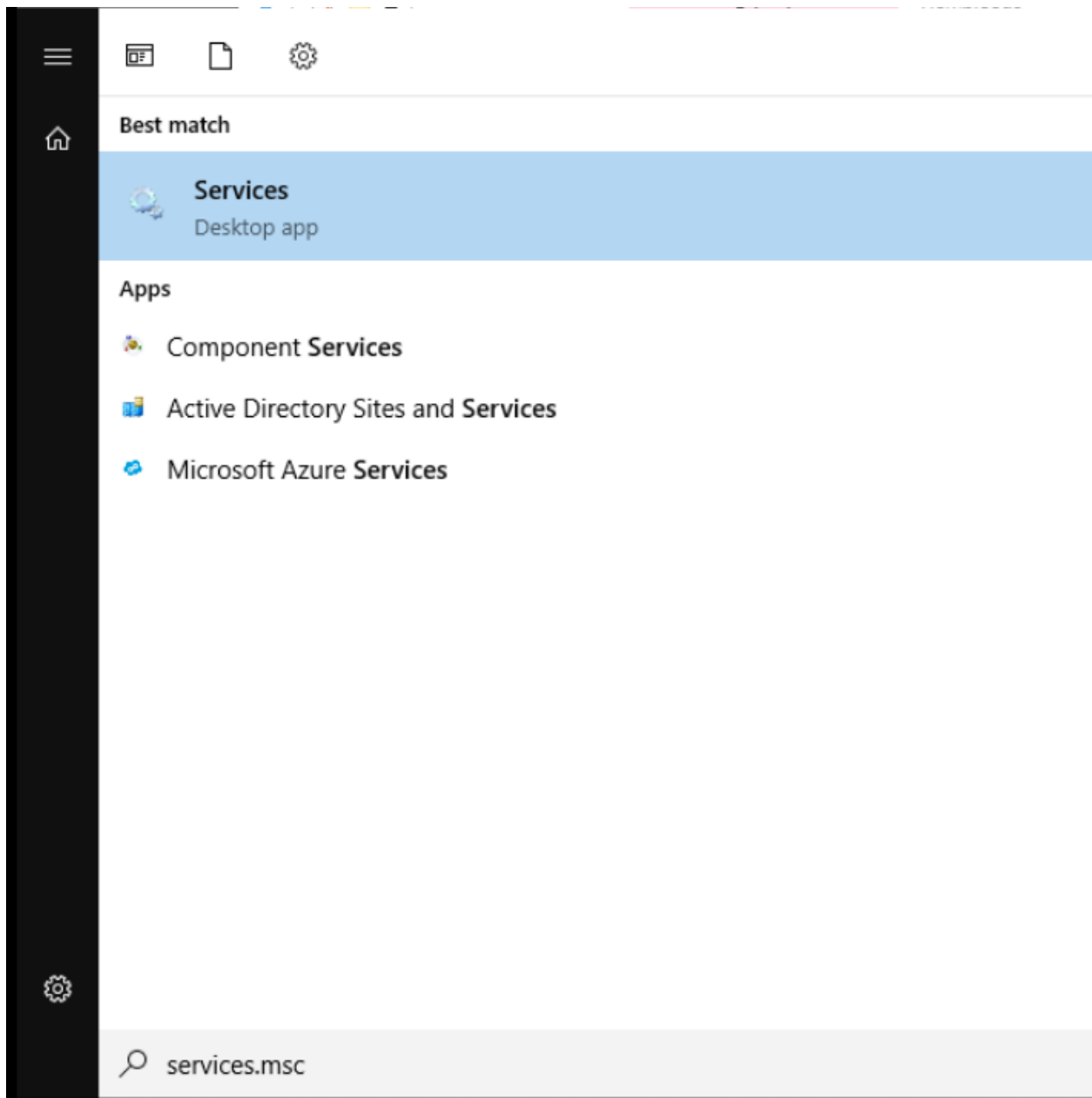
Back

Install

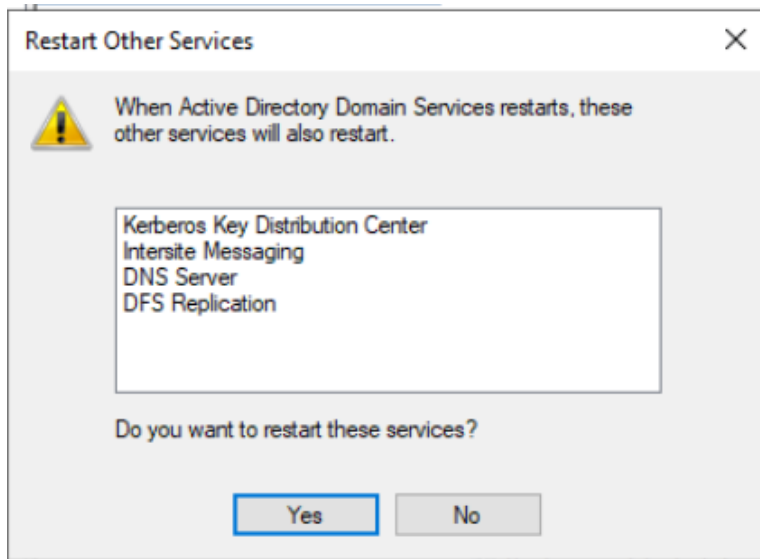
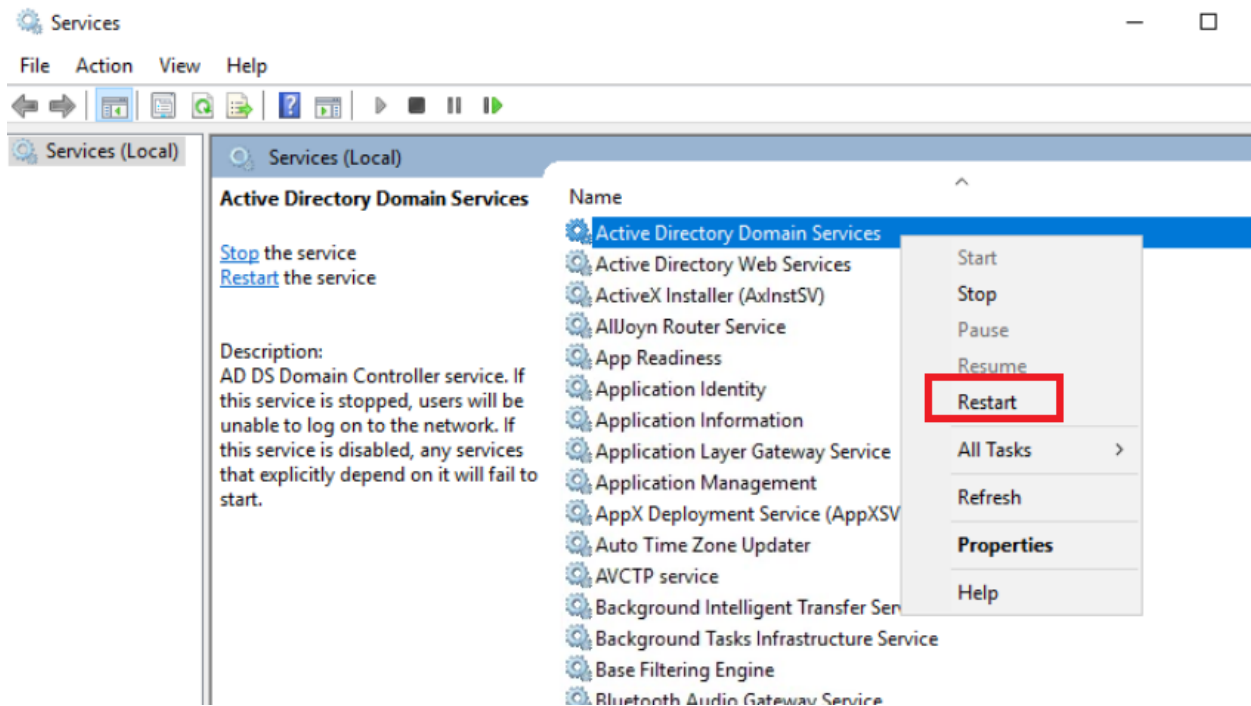
Cancel



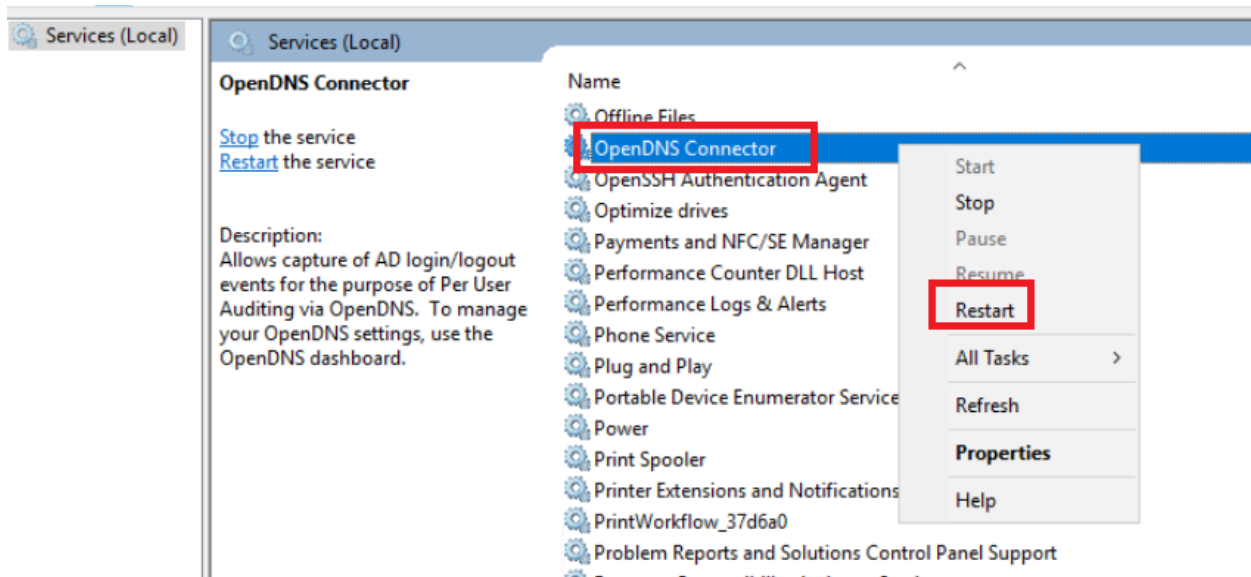
9. On the AD PC, click on Start and search for *services.msc*. Click on the **Services** Desktop app



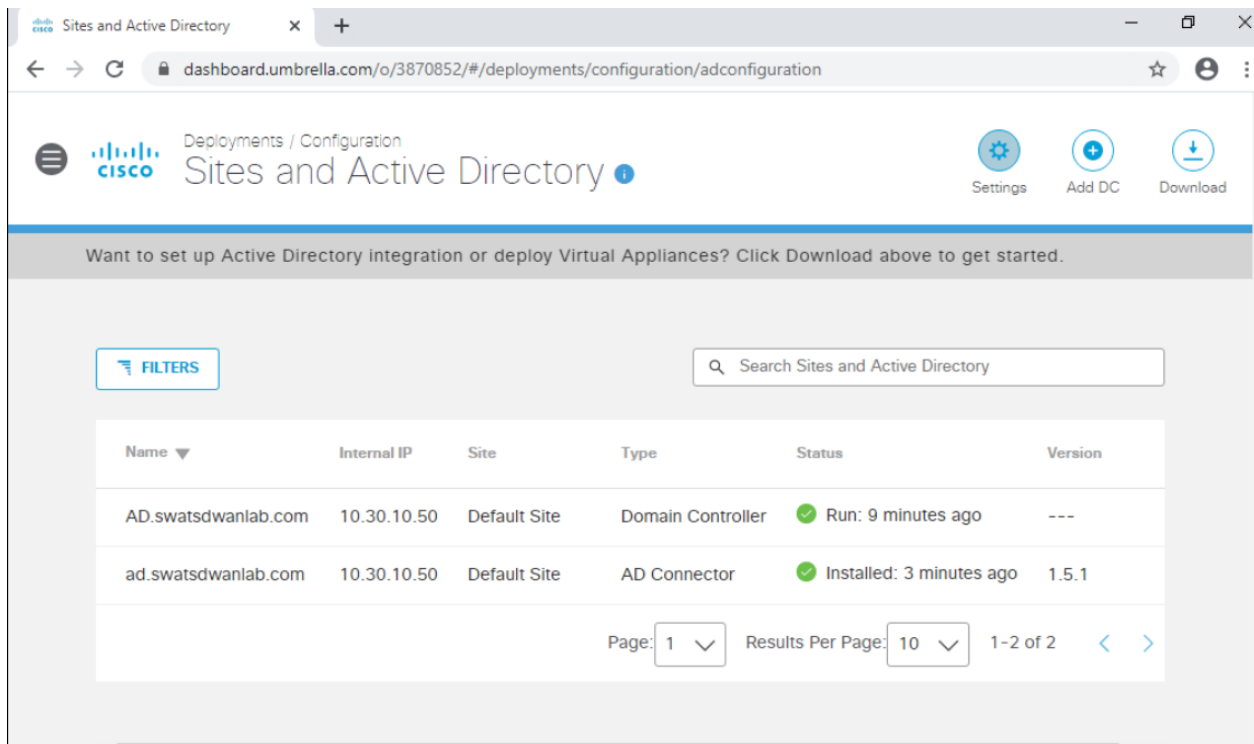
10. Right click on **Active Directory Domain Services** and choose to *Restart* the service. Select **Yes** to restart other related services as well



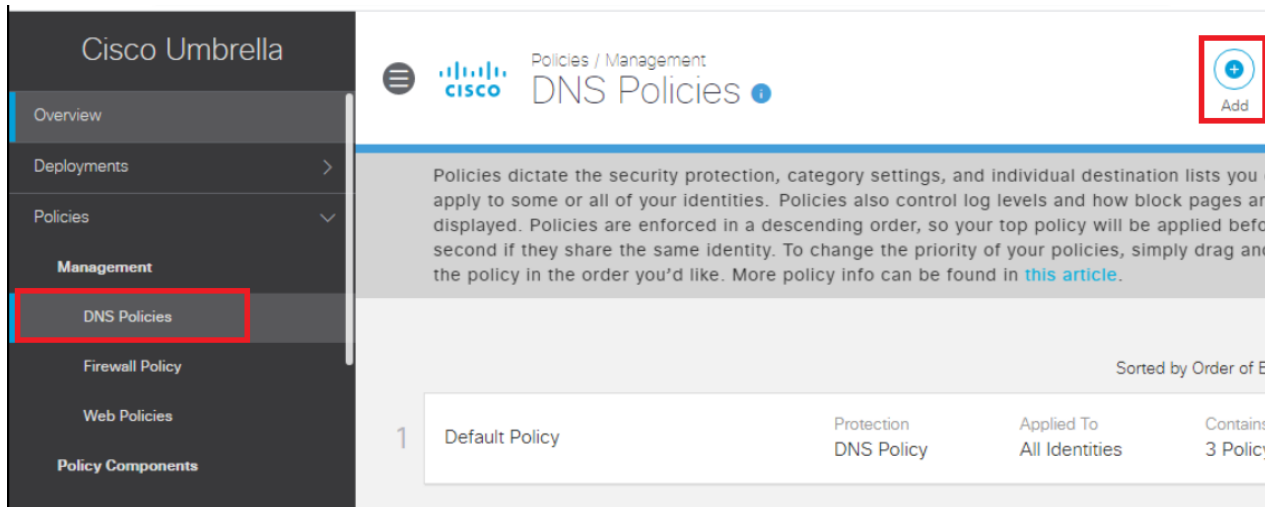
11. Once the services have restarted, locate the **OpenDNS Connector** service. Right click it and *Restart* this service as well



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)



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



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 >
- 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)

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.

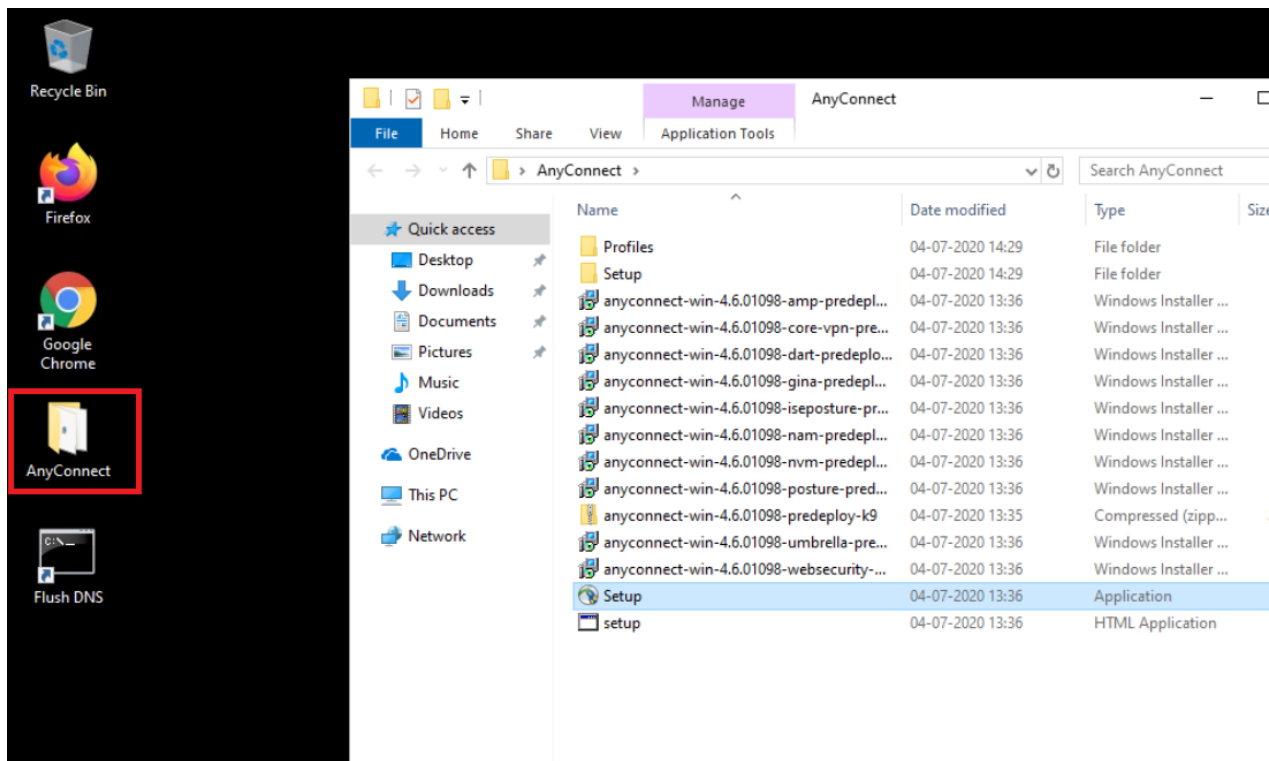
Task List

- ~~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

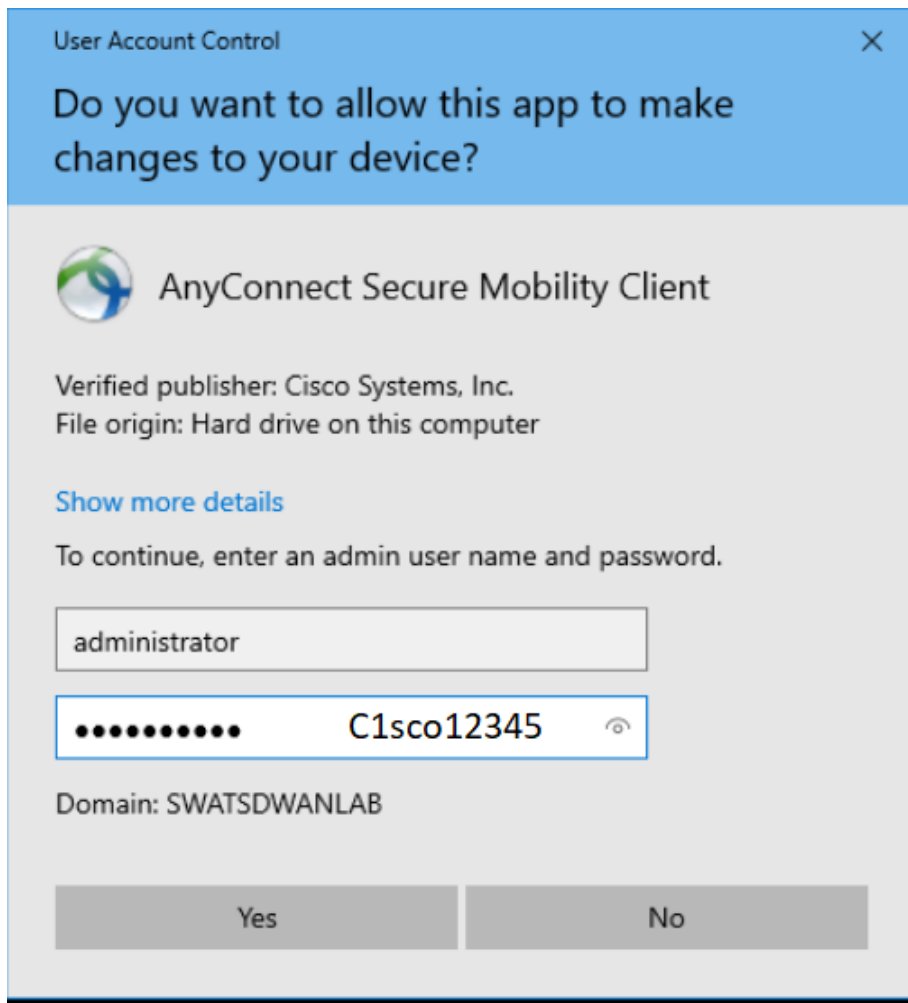
Cisco AnyConnect is used to identify Roaming Computers and include them within our DNS Policies. This is what will be leveraged in our lab environment to build and apply a DNS Policy.

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

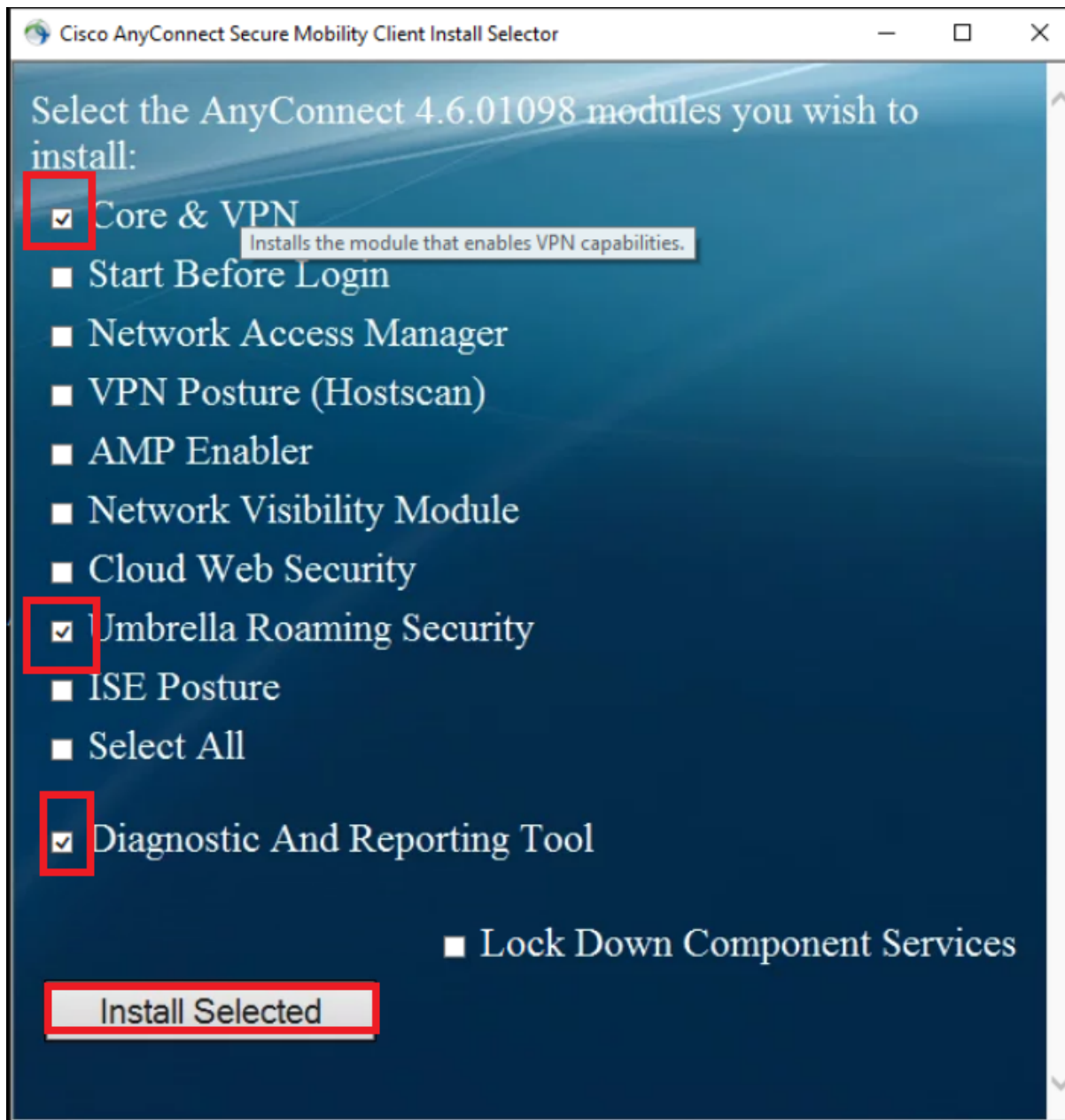


2. Enter the following credentials when prompted for a username/password and click on **Yes**

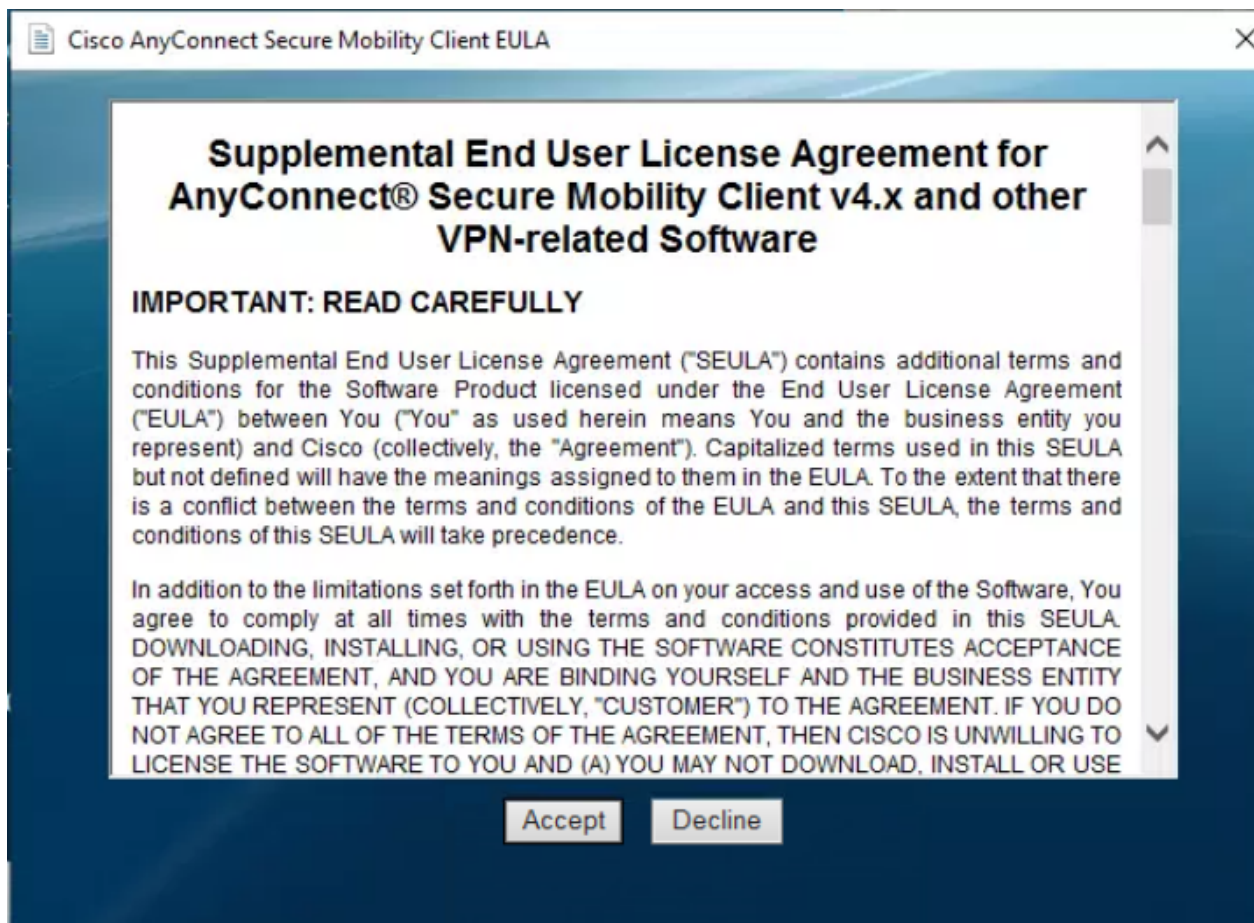
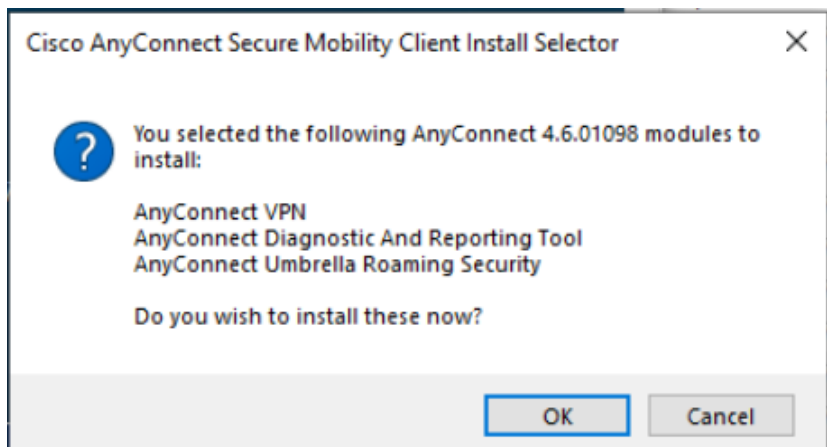
Username	Password
administrator	C1sco12345



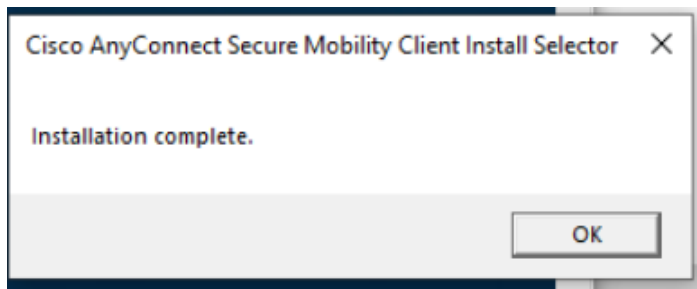
3. Remove the check mark against all modules *except* **Core & VPN**, **Umbrella Roaming Security** and **Diagnostic And Reporting Tool**. Click on **Install Selected** to install the selected modules



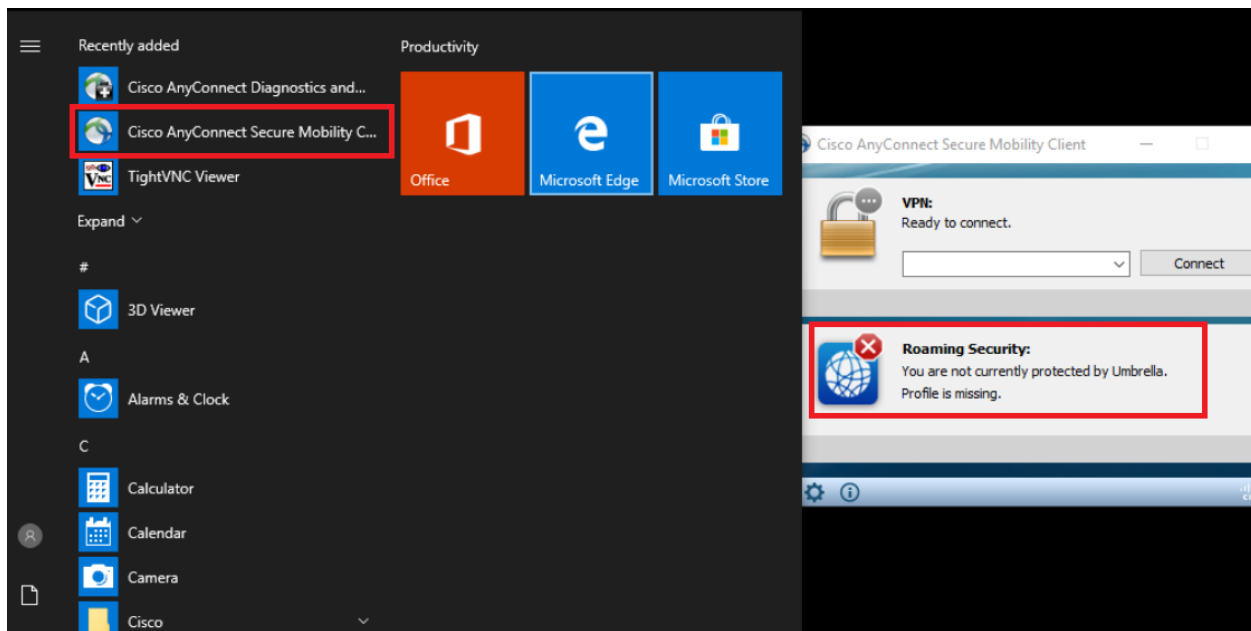
4. Click on **OK** and **Accept** the License Agreement



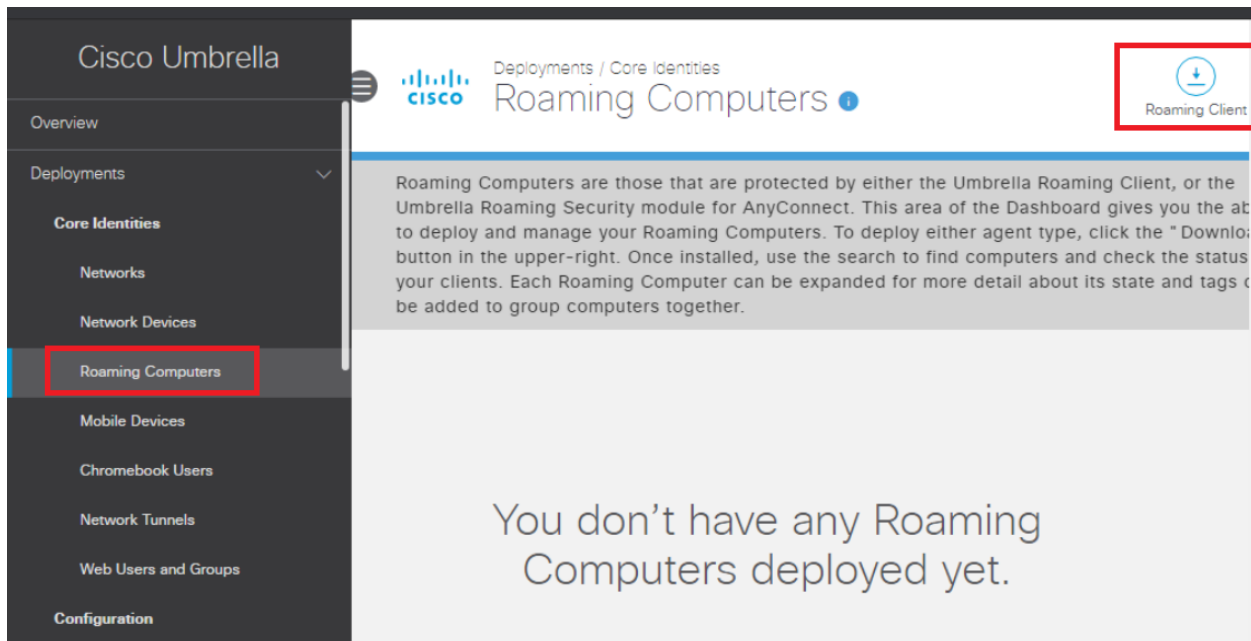
5. Once installation is complete, click on **OK**



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




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+
---	--

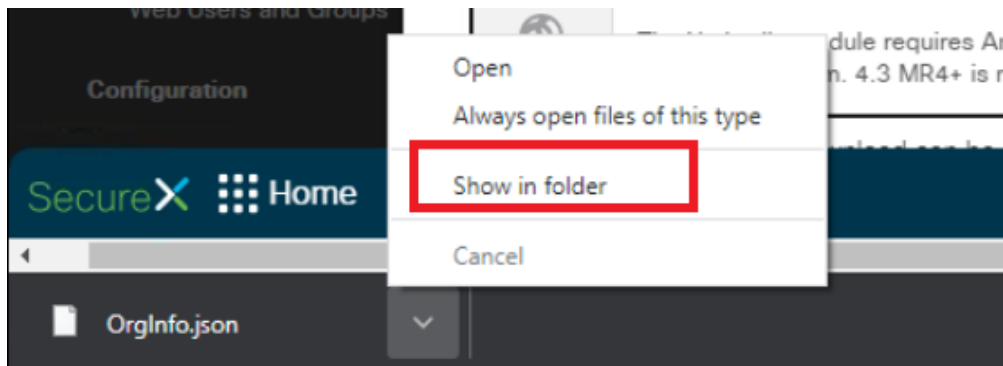
AnyConnect Umbrella Roaming Security Module

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.](#)

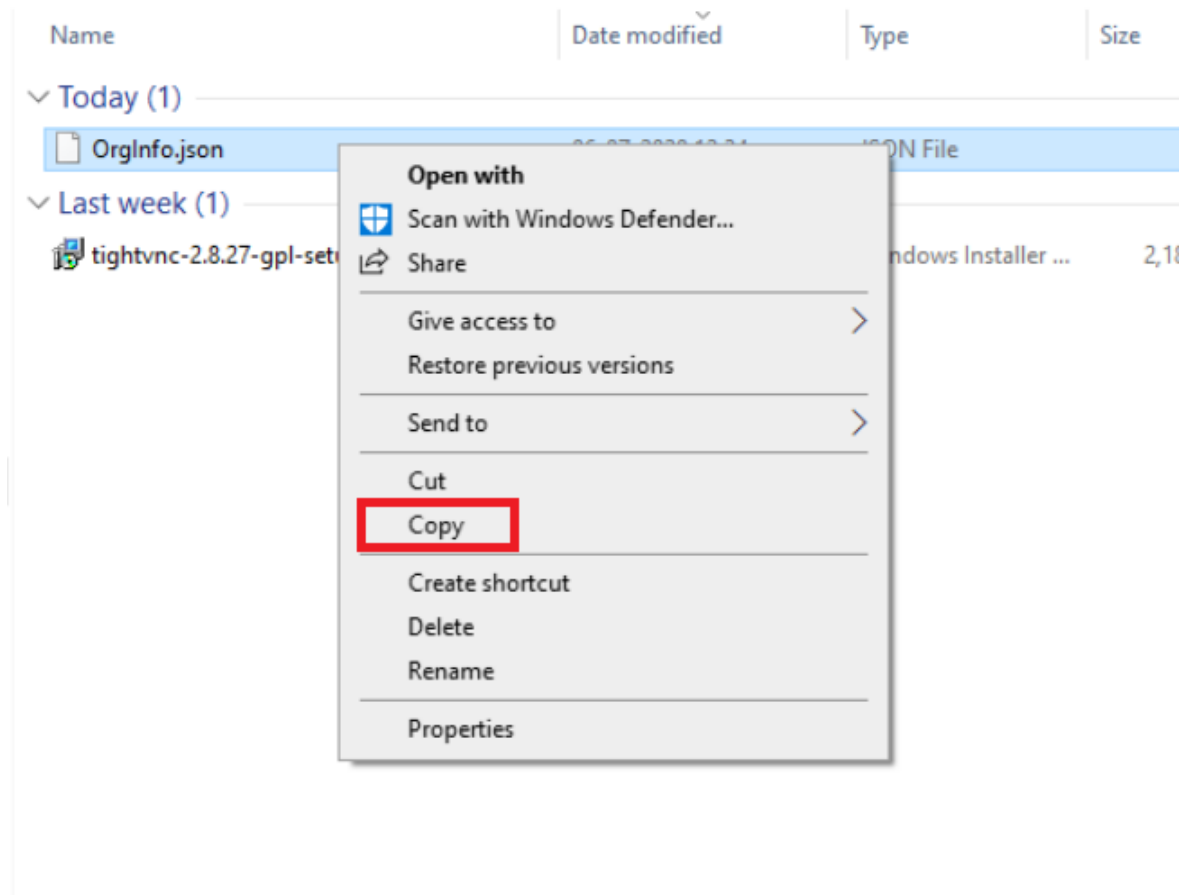
	Download Module Profile The Umbrella module requires AnyConnect for Windows or macOS, version 4.3 MR1 minimum. 4.3 MR4+ is recommended.
--	---

The AnyConnect 4.x client download can be found [here](#) (requires contract).

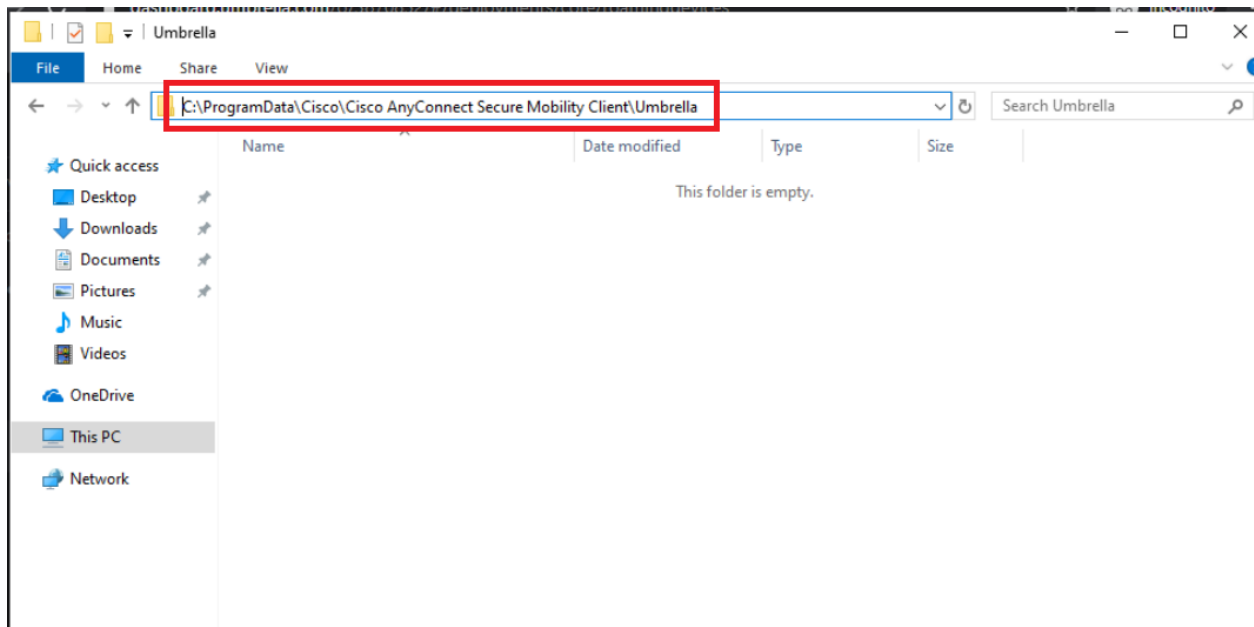
9. This will download a file called *OrgInfo.json*. Click on the arrow next to the file download and choose **Show in folder** (again, browser specific - Firefox has a folder icon to go to the download location)



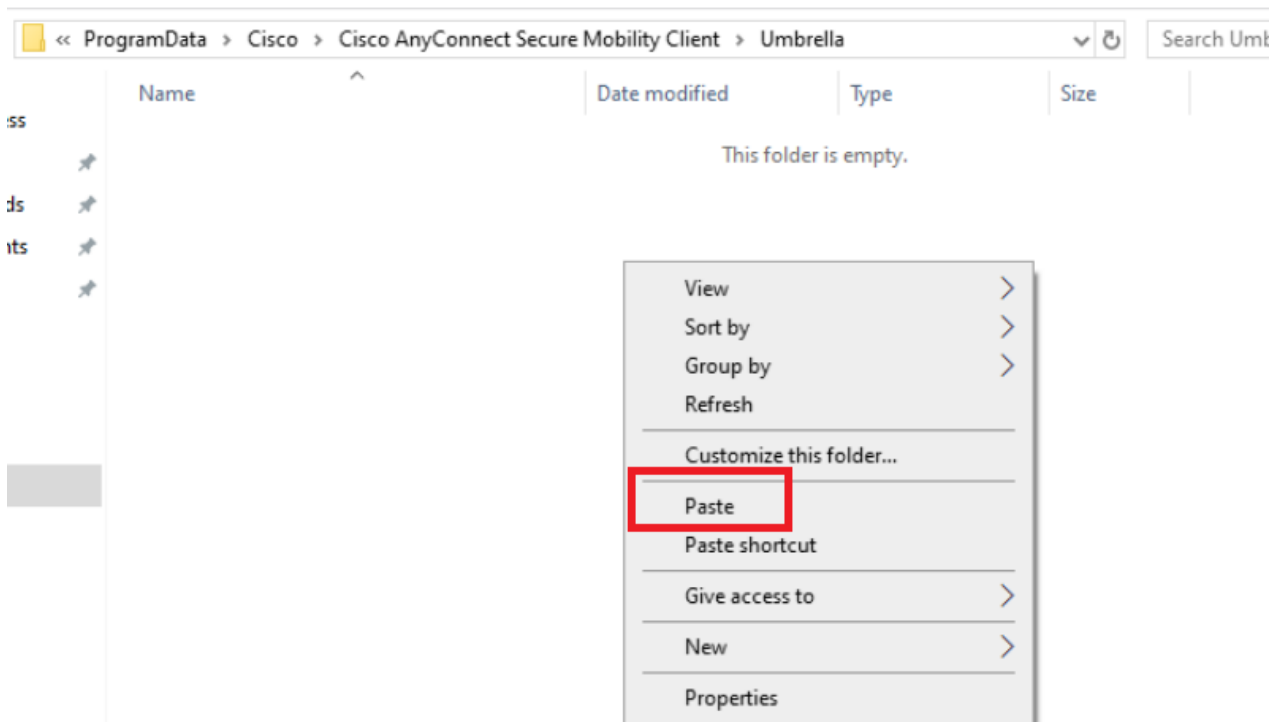
10. Right click on *OrgInfo.json* and click on **Copy**



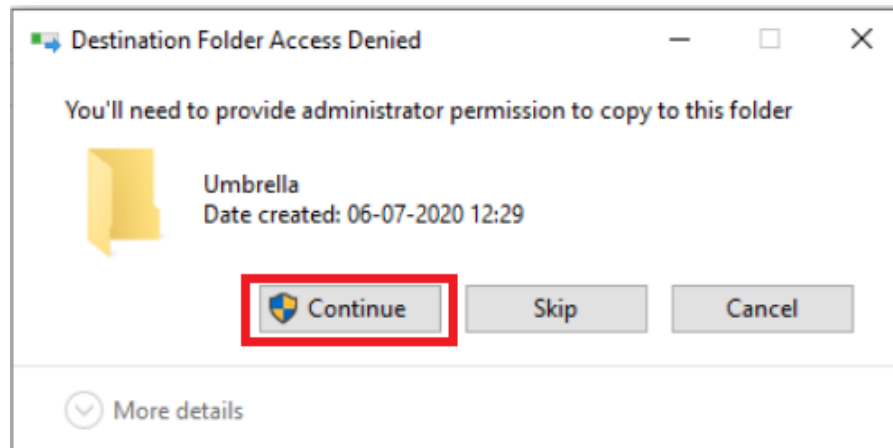
11. Open Windows Explorer and enter the following path (you will not be able to see this folder since it's hidden by default. There is an option to view hidden files and folders in Windows, but we can browse directly to the location)-
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella



12. Paste the file we copied before (OrgInfo.json)

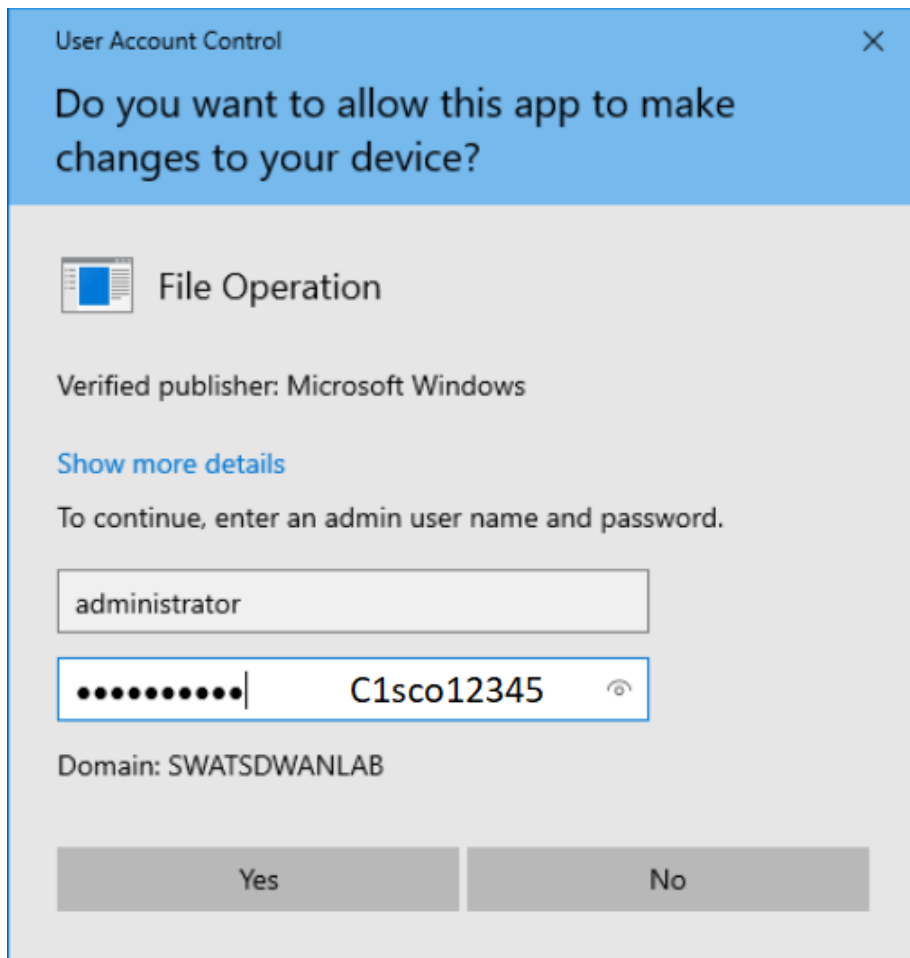


13. Click on **Continue**

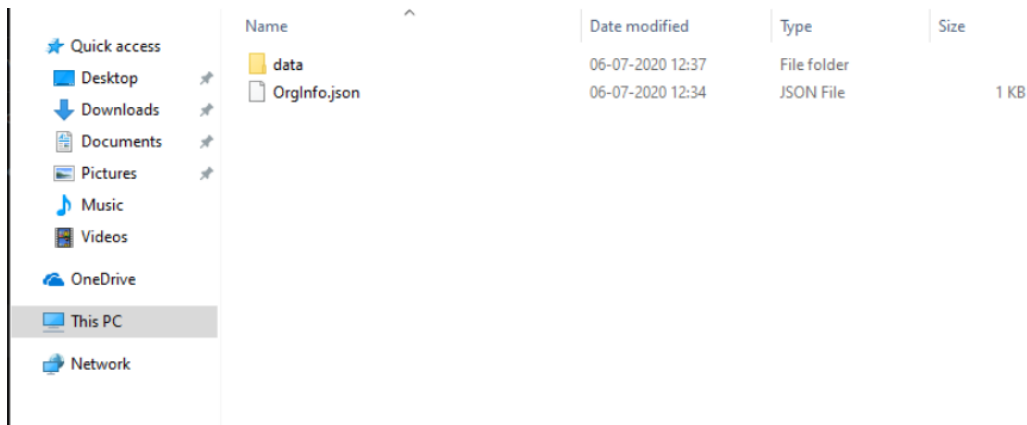


14. Enter the username/password as shown below

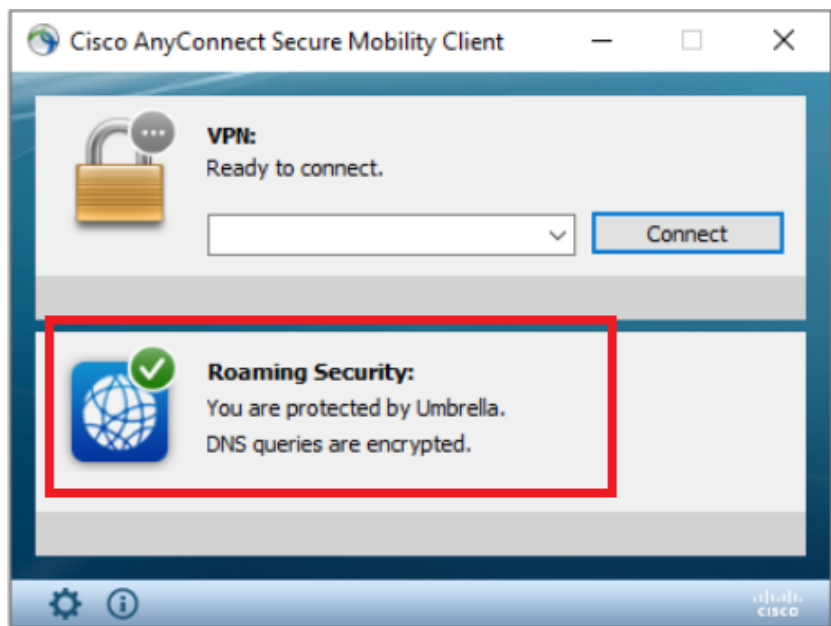
Username	Password
administrator	C1sco12345




15. 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



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

 Roaming Computers 1 Roaming Client Settings

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.

Q Search Advanced ▾

1 Total

<input type="checkbox"/>	Identity Name ▲	Status	Tags	Last Sync ▼
<input type="checkbox"/>	site30pc	Protected & Encrypted at the DNS Layer ✔ DNS Layer Encryption: enabled		a minute ago ▾

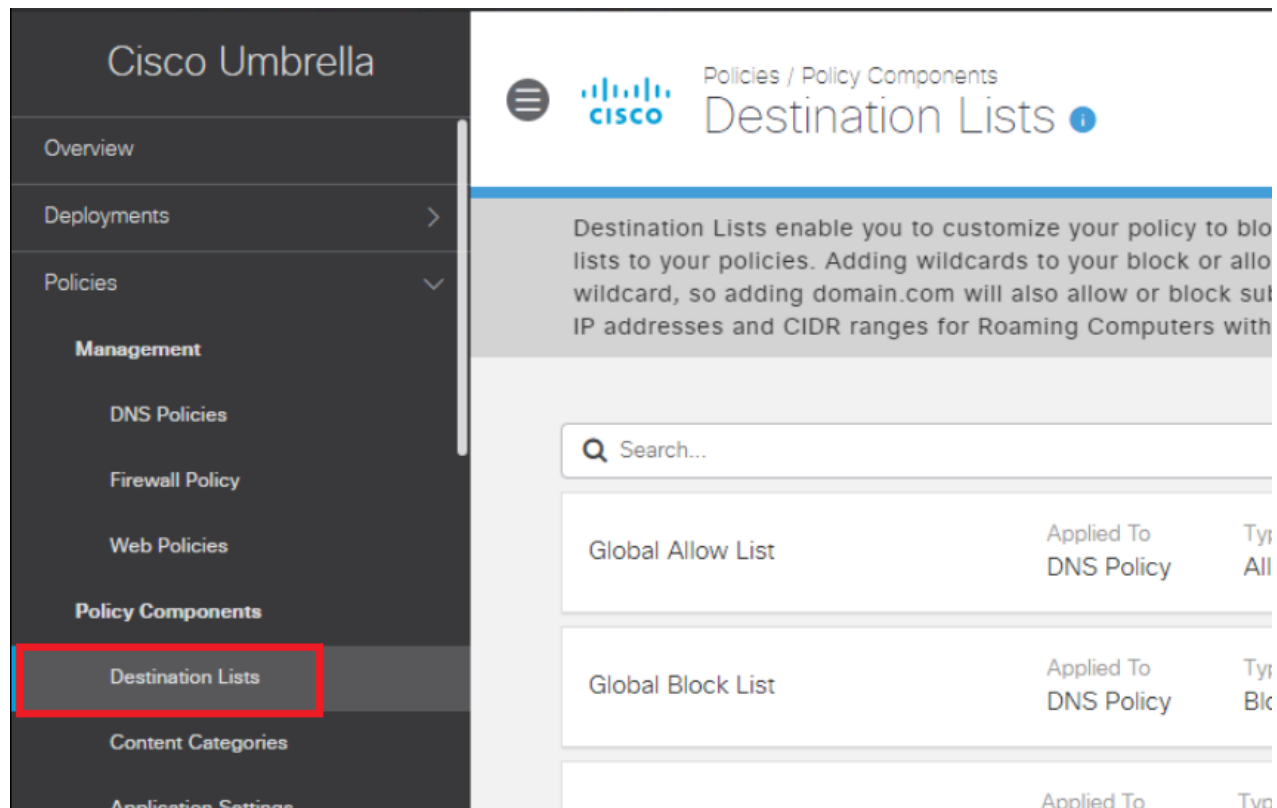
We will use the Roaming Computer as an Identity to enforce DNS Policies (the next section).

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

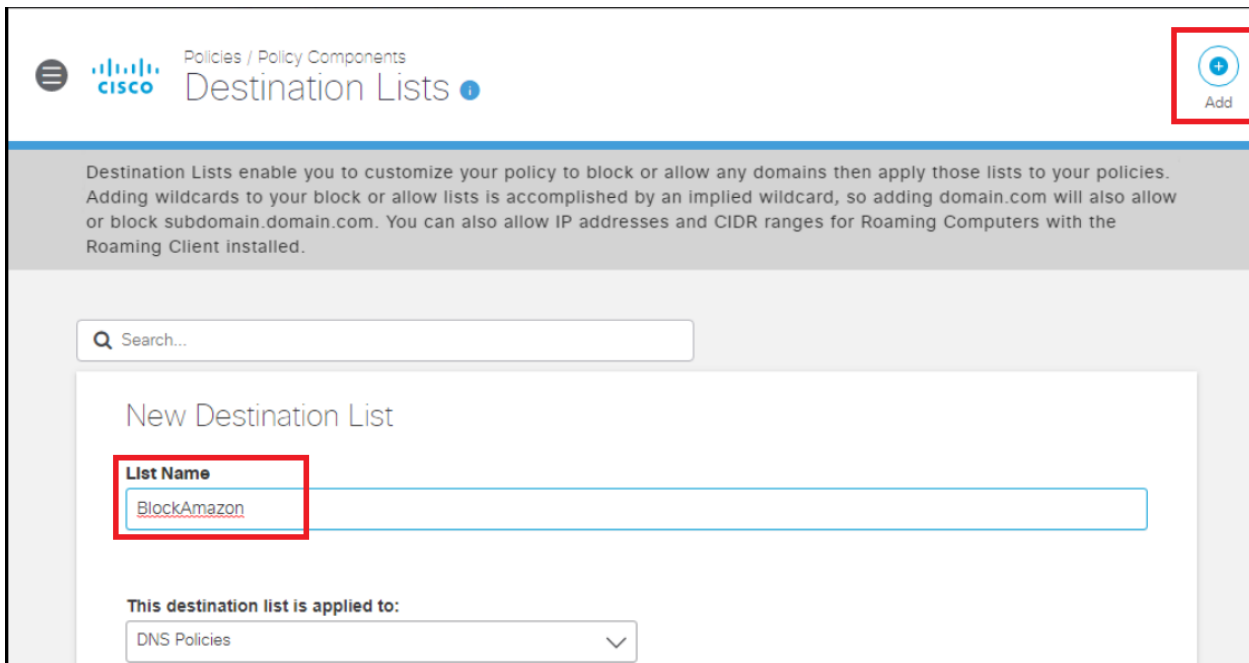
1. Log in to the Cisco Umbrella GUI (you can now log in from your own workstation since Umbrella is on the Cloud). [Click here](#) and reference Step 1 to review the login procedure. Navigate to **Policies => Policy Components => Destination Lists**. You will notice a few default Lists already created



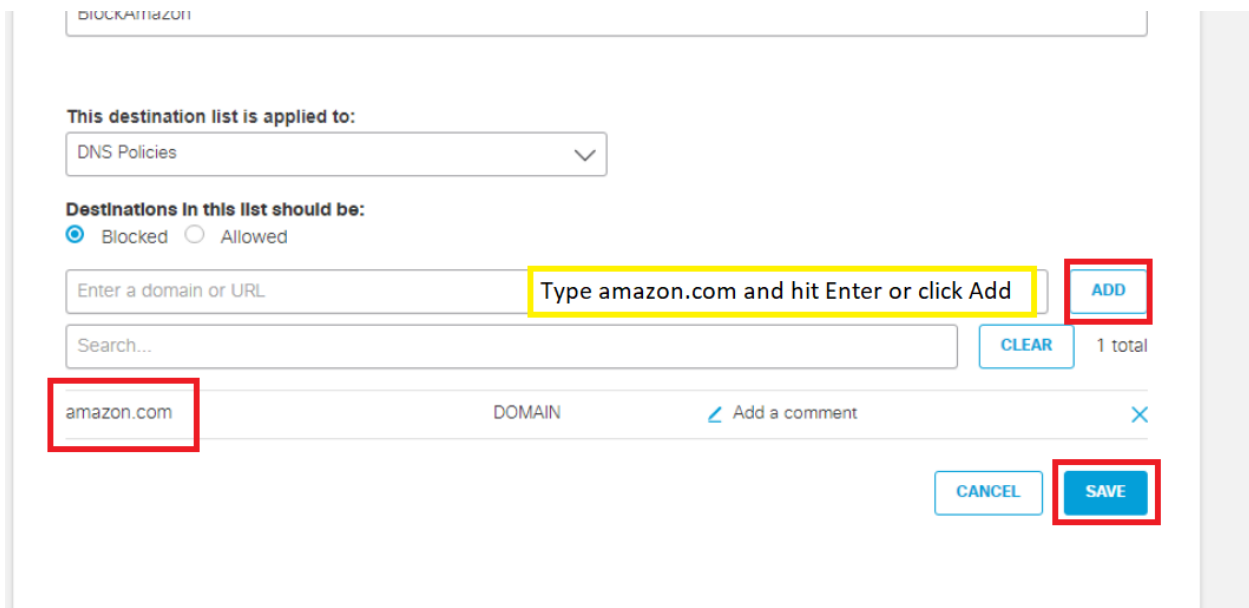
The screenshot displays the Cisco Umbrella interface. On the left, a dark sidebar contains a navigation menu with 'Destination Lists' highlighted in a red box. The main content area is titled 'Policies / Policy Components Destination Lists' and includes a search bar and a table of existing lists.

Name	Applied To	Type
Global Allow List	DNS Policy	All
Global Block List	DNS Policy	Blk

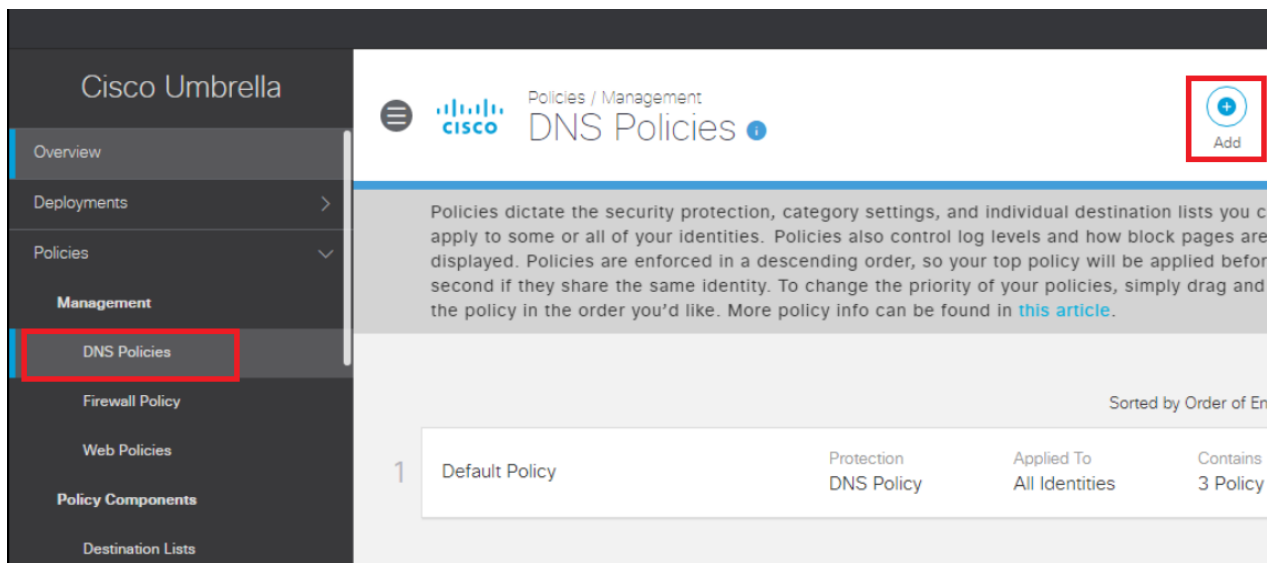
2. Click on **Add** in the top right-hand corner and give your List a name of *BlockAmazon*. Leave the **This destination list is applied to** field at *DNS Policies*



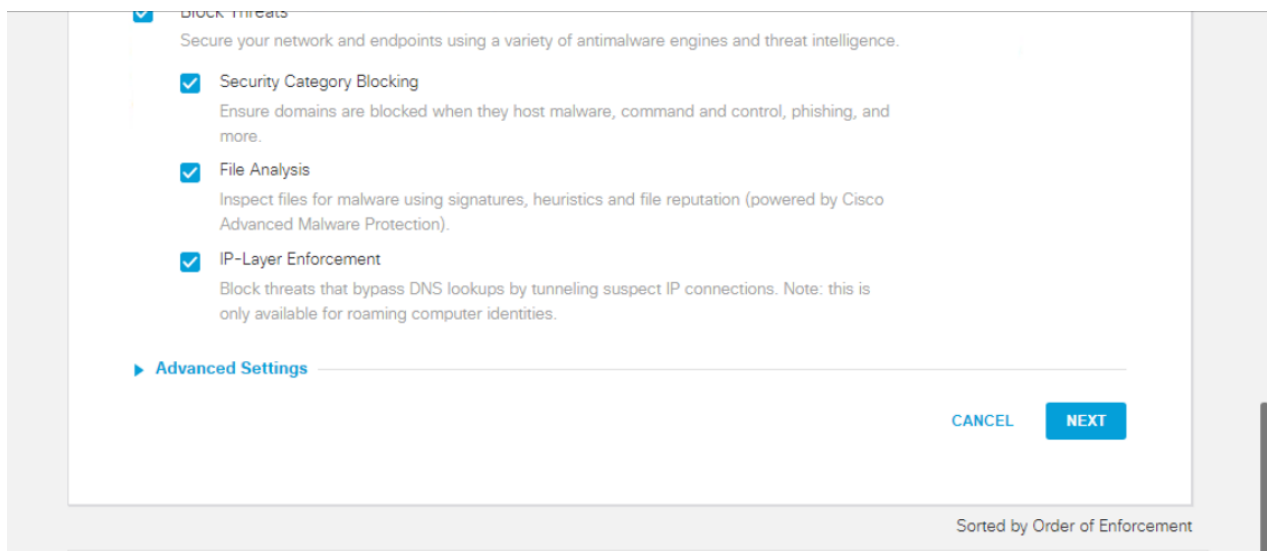
3. Scroll down to the **Destinations in this list should be** field and make sure it is set to **Blocked**. Type amazon.com in the *Enter a domain or URL* box and hit Enter (or click on Add). This should place amazon.com in the list (blocked). Click on **Save**



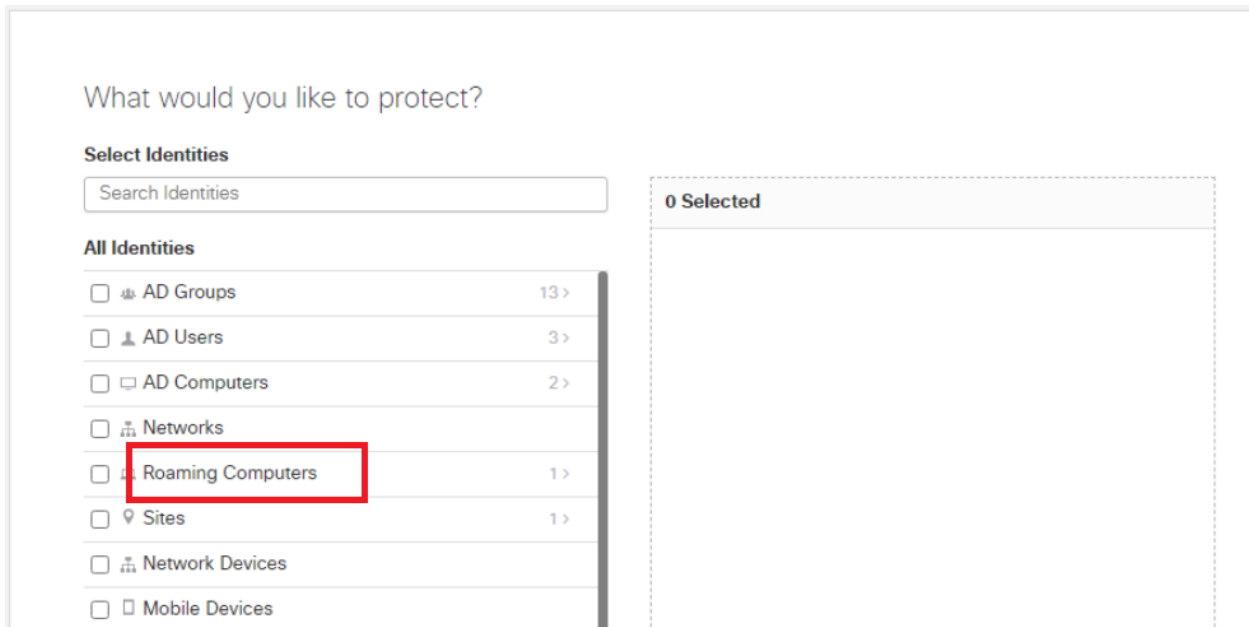
4. Navigate to **Policies => Management => DNS Policies** and click on **Add** to add a new DNS Policy



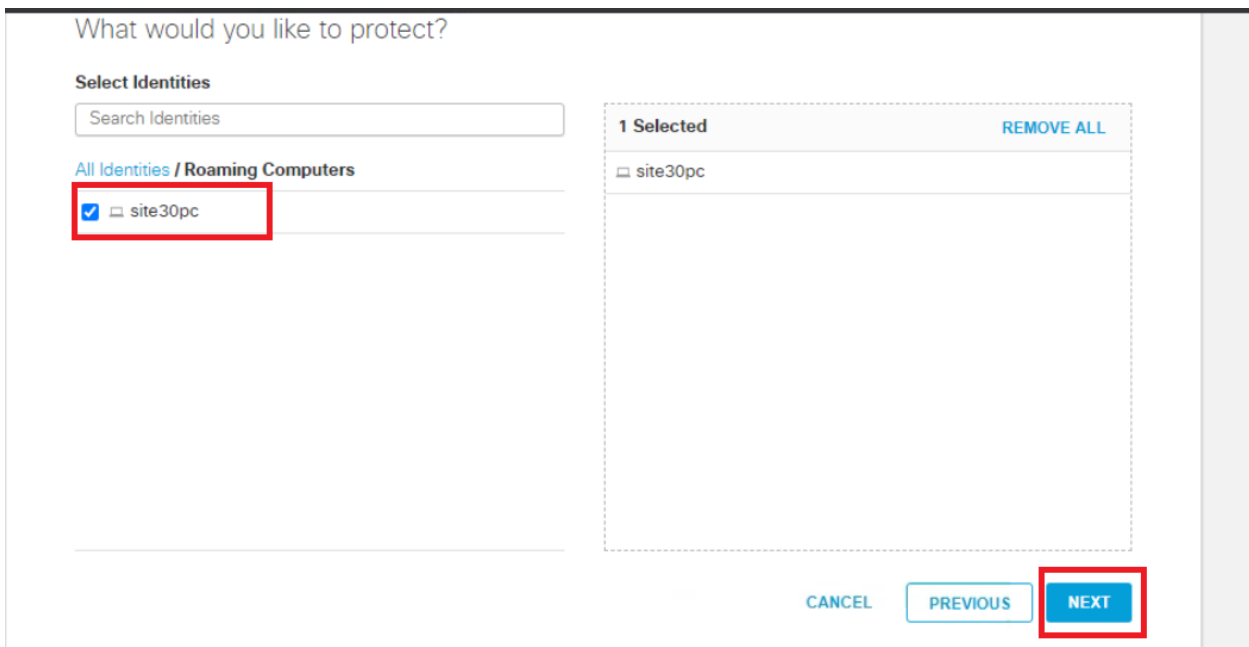
5. Scroll down on the **How would you like to be protected?** page and click on **Next** without making any changes



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



7. Put a check mark next to *site30pc* and it should show up in the right-hand window. Click on **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

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 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

- 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.

Search...

Select All Showing: All Lists 5 Total

All Destination Lists

<input checked="" type="checkbox"/> <input type="checkbox"/> BlockAmazon	1 >
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> Global Allow List	0 >
<input checked="" type="checkbox"/> <input type="checkbox"/> Global Block List	0 >
<input type="checkbox"/> <input checked="" type="checkbox"/> MSP Default Allow List	0 >
<input type="checkbox"/> <input type="checkbox"/> MSP Default Block List	0 >

1 Allow Lists Applied

<input checked="" type="checkbox"/> Global Allow List	0
---	---

2 Block Lists Applied [REMOVE ALL](#)

<input type="checkbox"/> BlockAmazon	1
<input type="checkbox"/> 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 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

1 Anyconnect Roaming Client

[Edit](#)



Security Setting Applied: Centralized Default Settings

Command and Control Callbacks, Malware, and Phishing Attacks will be blocked
No integration is enabled.

[Edit](#) [Disable](#)



Content Setting Applied: Moderate

Blocks all adult-related websites and illegal activity.

[Edit](#) [Disable](#)



Application Setting Applied: Default Settings

eBay will be blocked.

[Edit](#) [Disable](#)



3 Destination Lists Enforced

2 Block Lists

1 Allow List

[Edit](#)



File Analysis Enabled

File Inspection Enabled

[Edit](#)



Umbrella Default Block Page Applied

[Edit](#) [Preview Block Page](#)

Click on Save **AFTER**
entering the Policy Name

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 1



Add



Policy Tester

Sorted by Order of Enforcement

1

DNSPolicy1

Protection
DNS Policy

Applied To
1 Identity

Contains
4 Policy Settings

Last Modified
Jul 6, 2020



2

Default Policy

Protection
DNS Policy

Applied To
All Identities

Contains
3 Policy Settings

Last Modified
Jul 3, 2020



Policy Name
DNSPolicy1

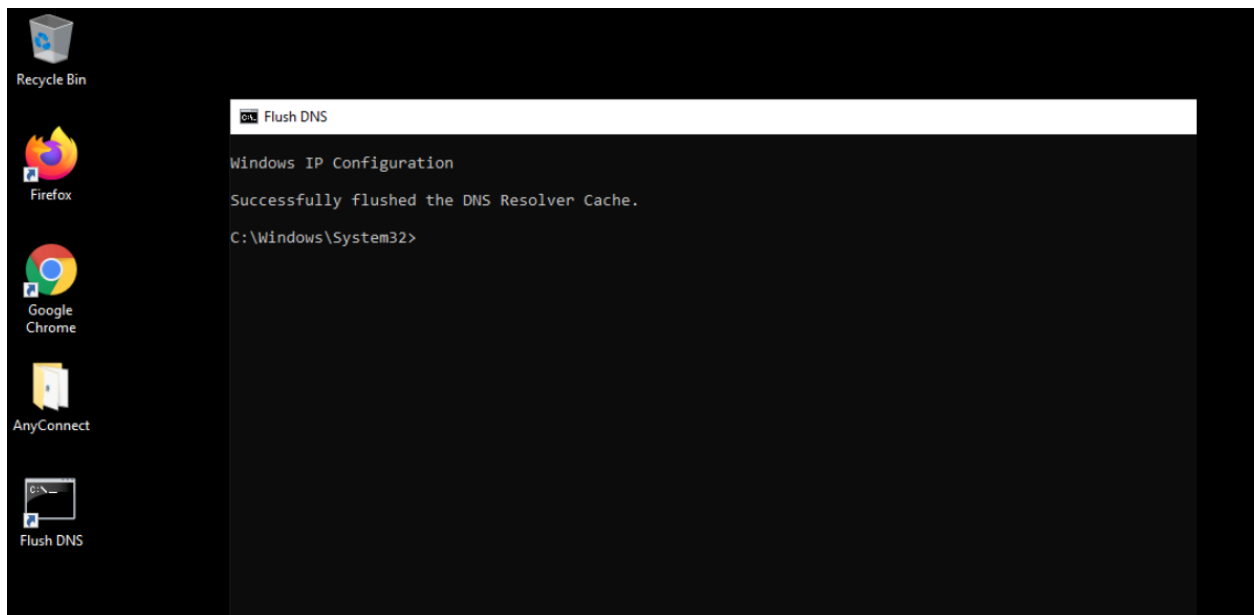
- 1 Identity Affected**
1 Anyconnect Roaming Client
[Edit Identity](#)
- Security Setting Applied: Centralized Default Settings**
Command and Control Callbacks, Malware, and Phishing Attacks will be blocked
No integration is enabled.
[Edit](#) [Disable](#)
- Content Setting Applied: Moderate**
Blocks all adult-related websites and illegal activity.
[Edit](#) [Disable](#)
- Application Setting Applied: Default Settings**
eBay will be blocked.
[Edit](#) [Disable](#)

▲ **Advanced Settings**

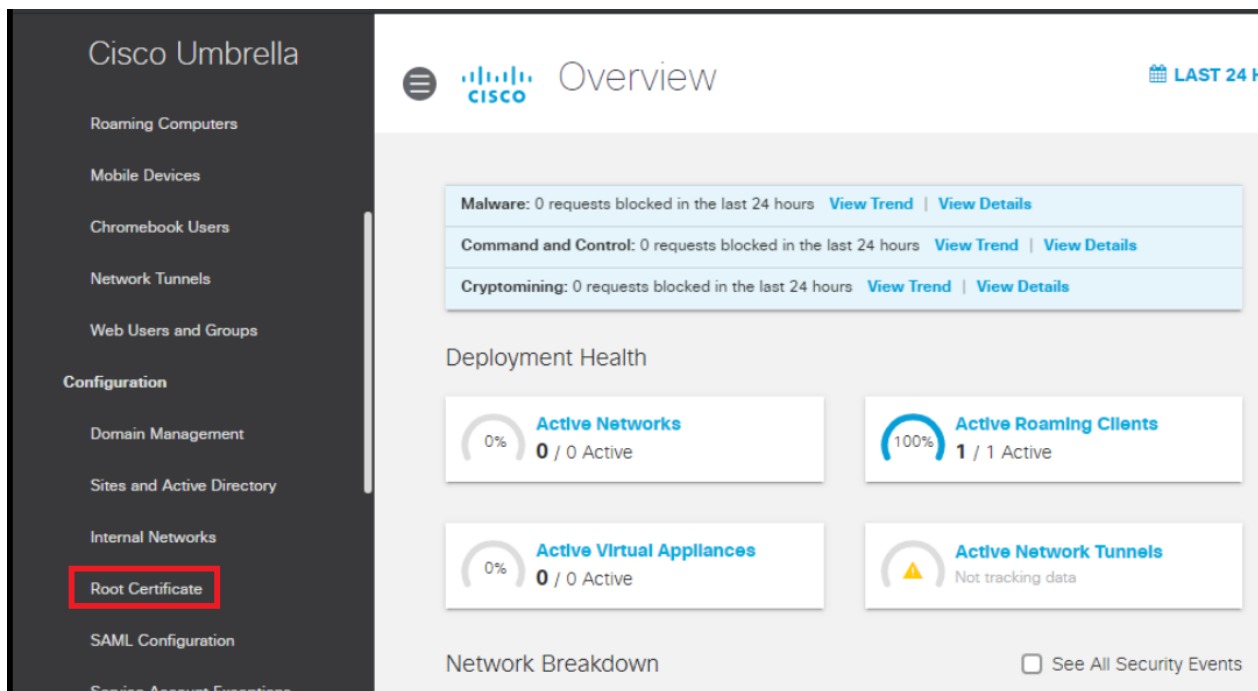
- Enable Intelligent Proxy**
Gain visibility into threats, content, or apps by proxying web connections for risky domains.
- SSL Decryption**
Enabling SSL decryption allows the intelligent proxy to inspect traffic over HTTPS and block custom URLs in destination lists.
Turning on SSL decryption allows HTTPS URL blocking.

- 3 Destination Lists Enforced**
2 Block Lists
1 Allow List
[Edit](#)
- File Analysis Enabled**
File Inspection Enabled
[Edit](#)
- Umbrella Default Block Page Applied**
[Edit](#) [Preview Block Page](#)

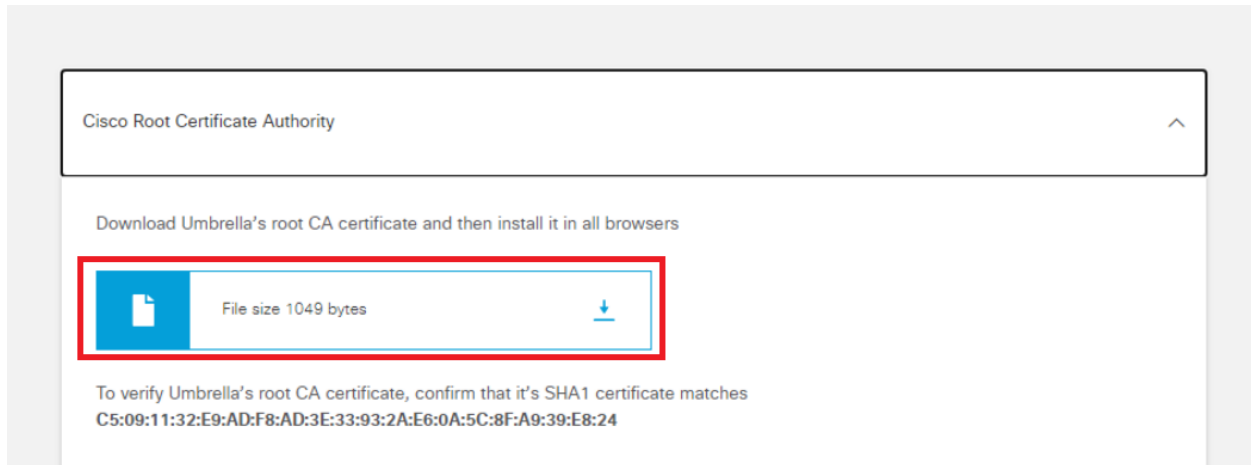
15. We are now going to test our DNS Policy, but before doing so, the Cisco Umbrella root certificate will need to be downloaded and installed on the Site 30 PC. Head over to the Site 30 PC via your preferred connection method (Guacamole/RDP/vCenter Console). [Click here](#) and go through Step 1 to review how to connect to the Site 30 PC. Double-click the **Flush DNS** icon on the Desktop to clear the DNS cache



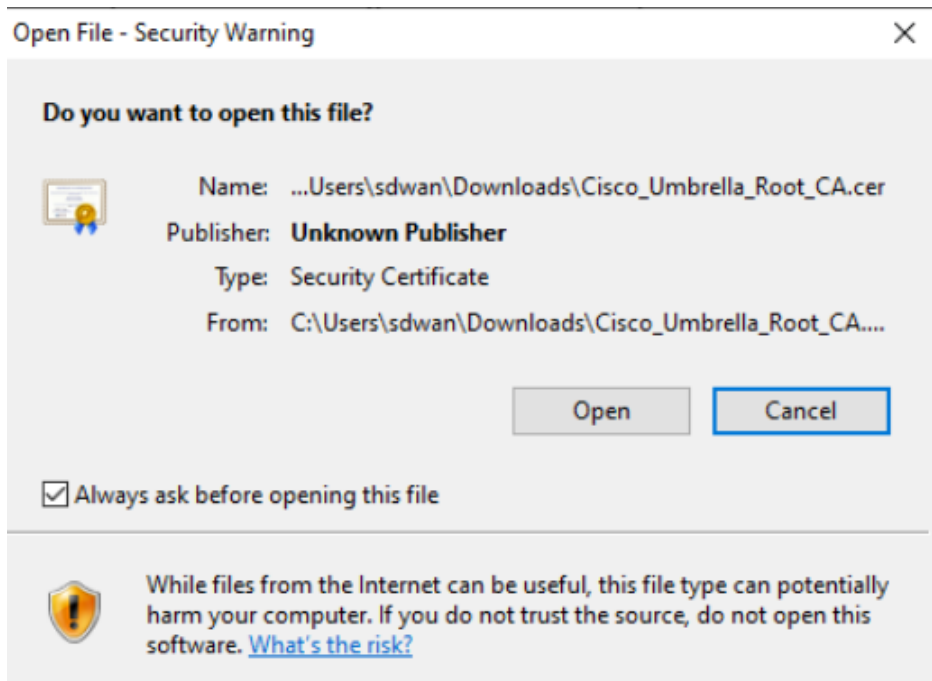
16. Log in to Umbrella on the Site 30 PC (login.umbrella.com). [Click here](#) and reference Step 1 to review the login procedure, but make sure you log in to Umbrella via the Site 30 PC. Navigate to **Deployment => Configuration => Root Certificate**



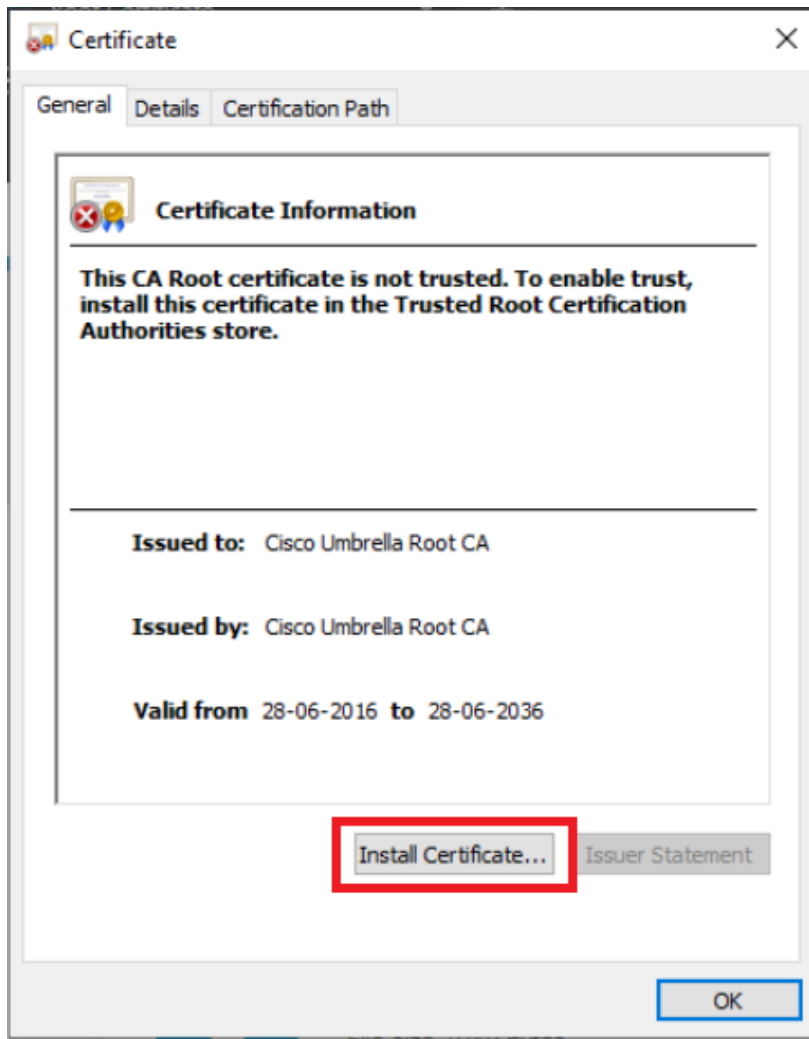
17. Expand **Cisco Root Certificate Authority** and download the root CA certificate



18. Click on Keep, if prompted and open the downloaded file. Choose **Open** in the Security Warning



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

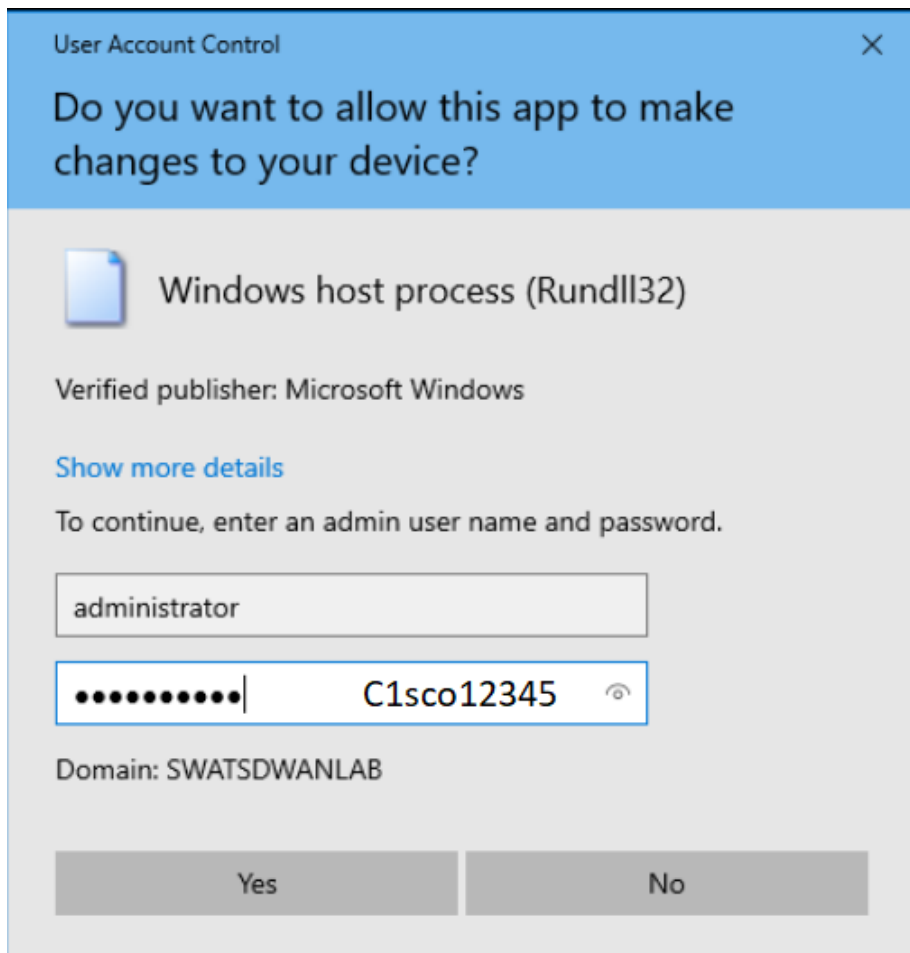
Current User

Local Machine

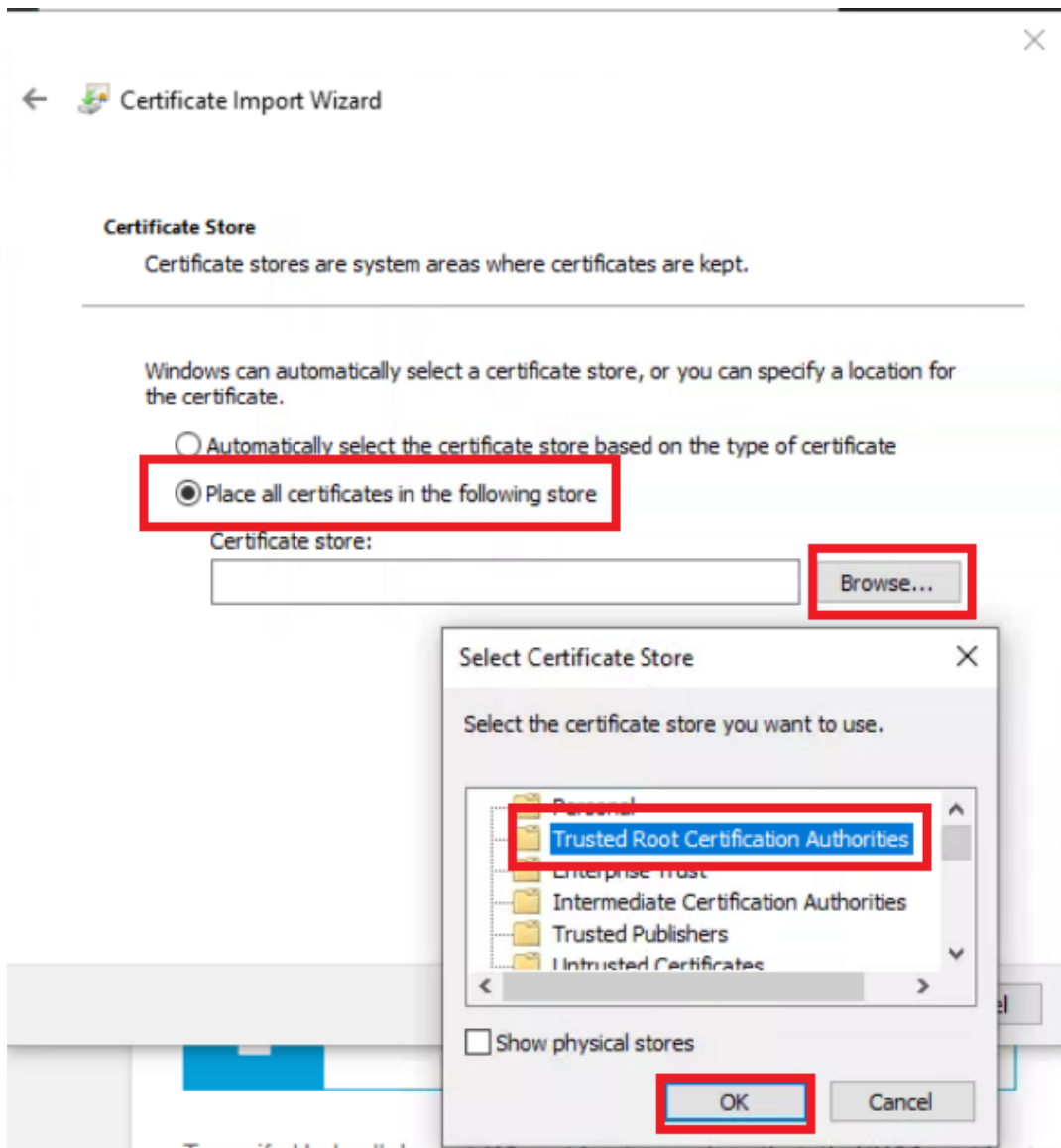
To continue, click Next.

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

Completing the Certificate Import Wizard

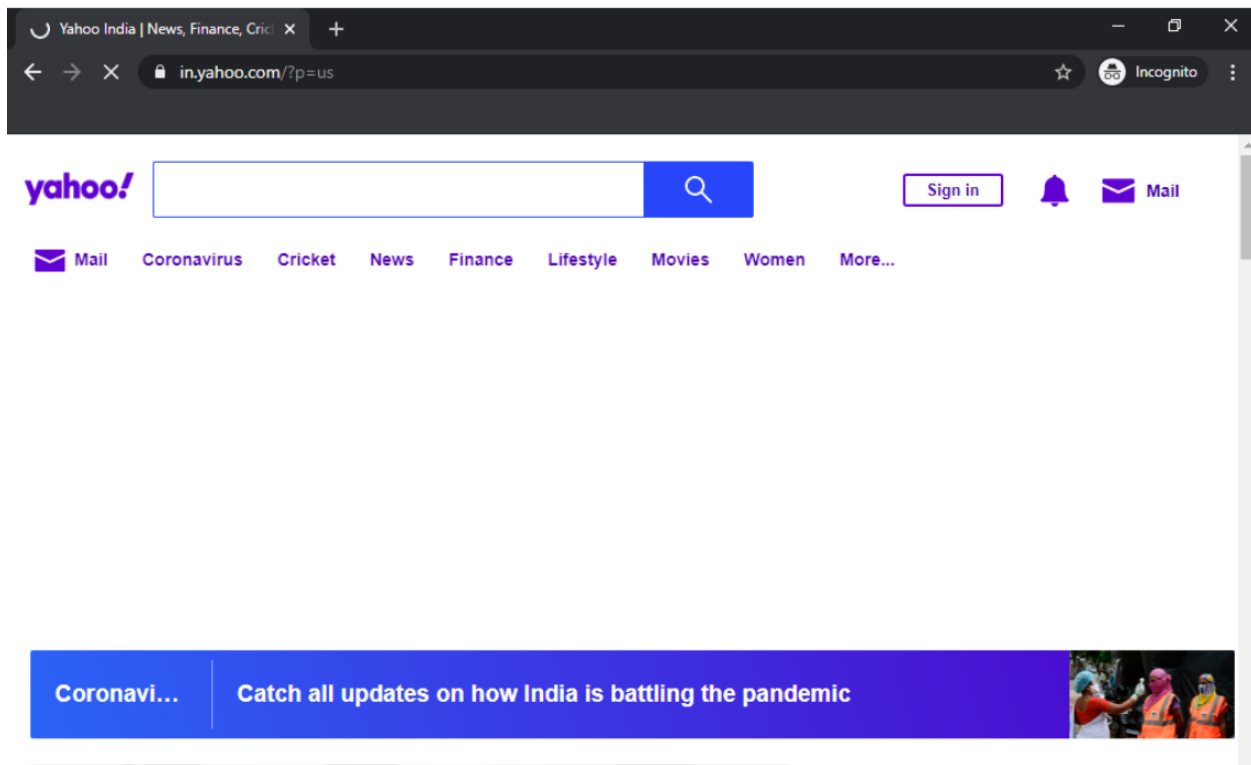
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Finish Cancel


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

Site Blocked

block.opendns.com/main?url=66786691807915688078&server=hkg15&prefs=&tagging=&nref

 Cisco Umbrella

 This site is blocked.

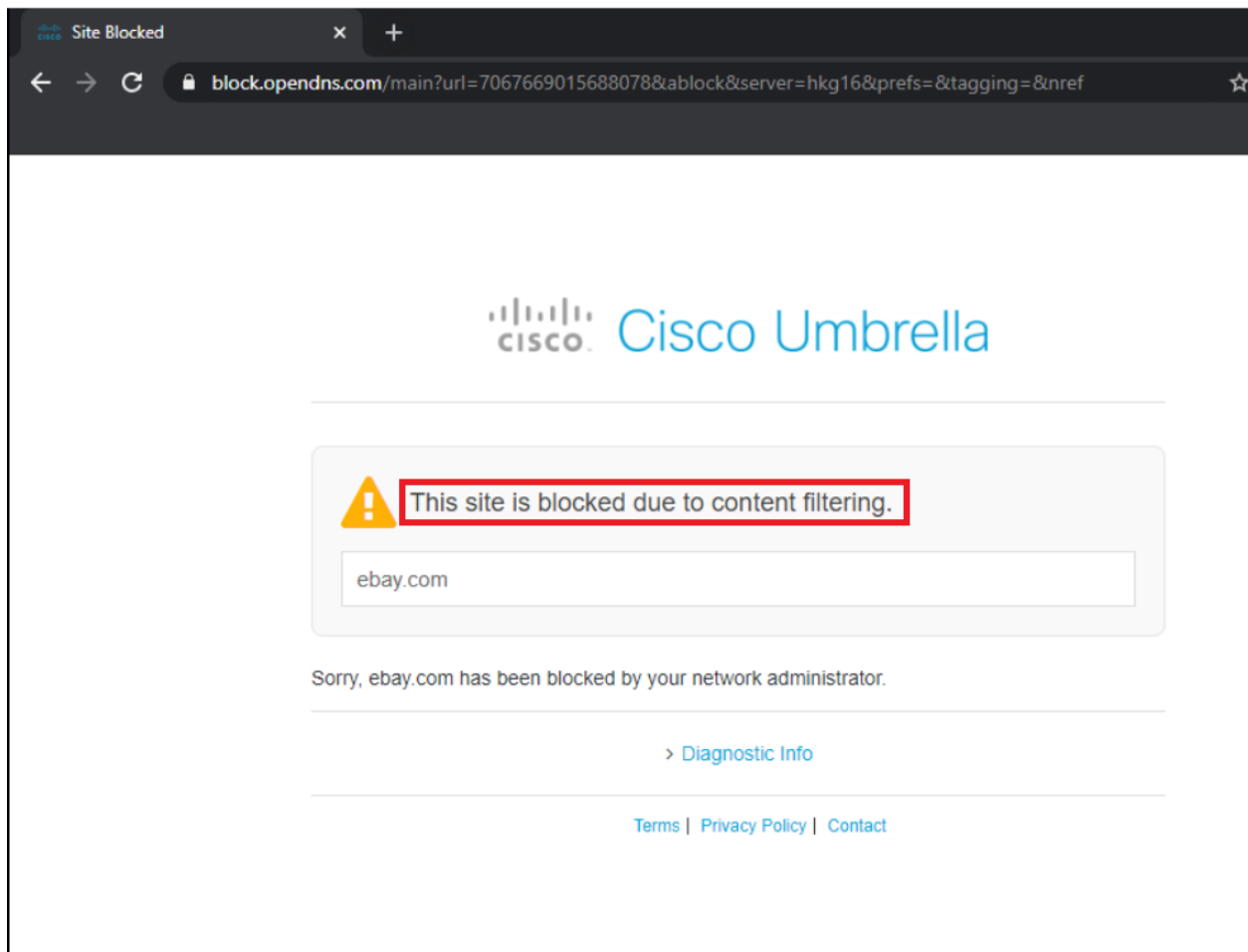
amazon.com

Sorry, **amazon.com** has been blocked by your network administrator.

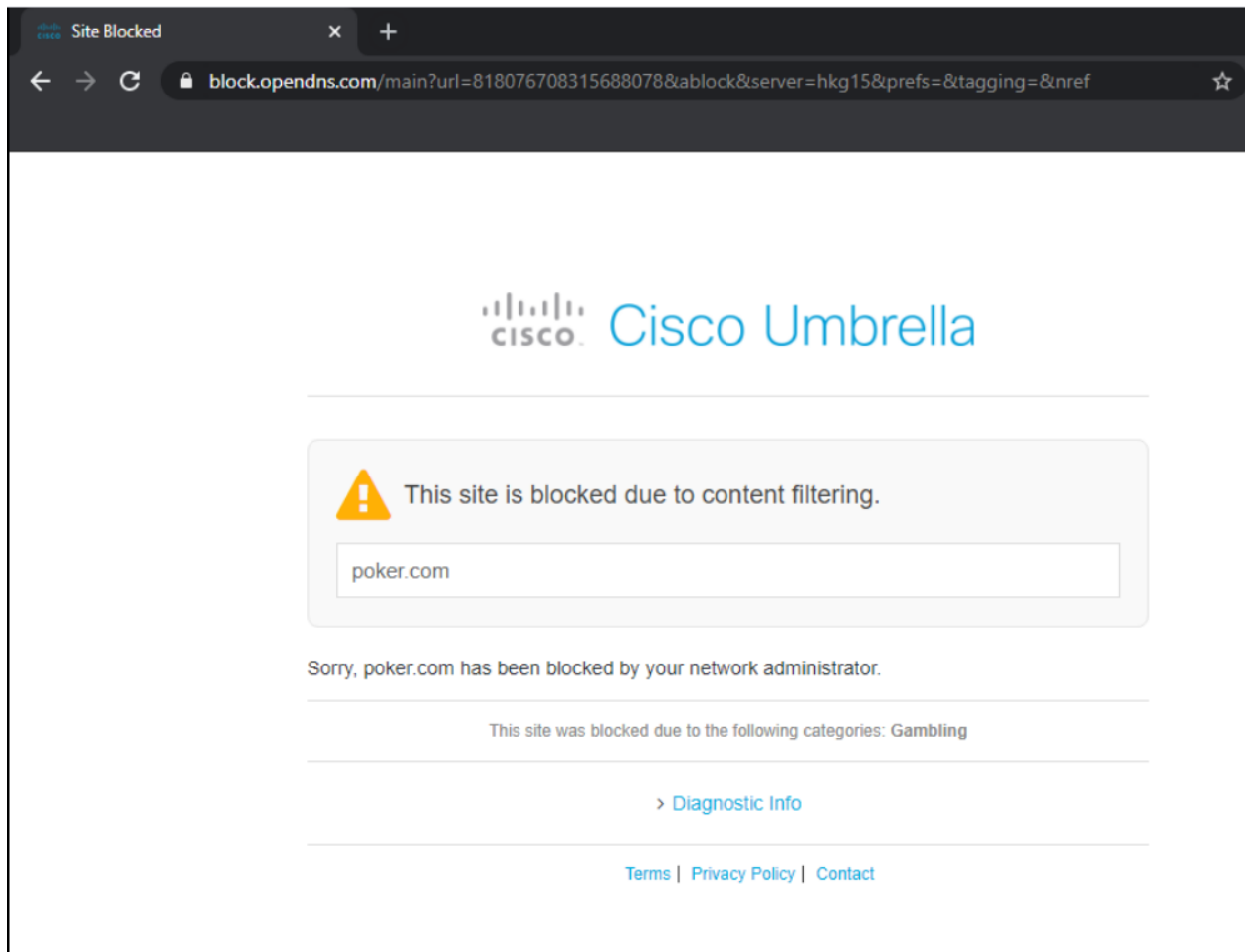
[> Diagnostic Info](#)

[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*



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

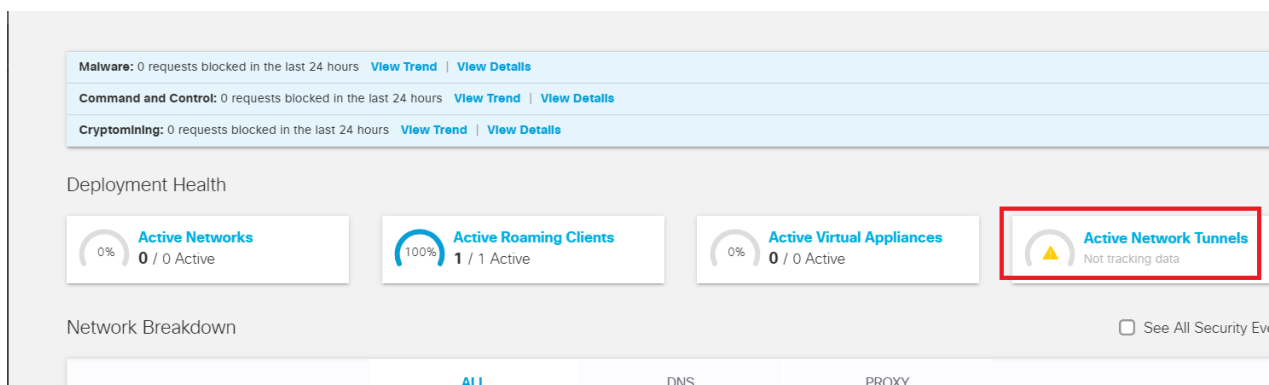
- [Overview](#)
- [Pre-Work](#)
- [Enabling Site 30 for DIA](#)
- [Life without Cisco Umbrella](#)
- [Basic Configuration for Umbrella](#)
- [Making Umbrella Ours](#)

- ~~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**

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**

VPN Interface PPP Ethernet

WAN

OTHER TEMPLATES

Banner	BGP WAN LAN
DHCP Server LAN	IGMP LAN
Multicast	OSPF WAN LAN
SIG Credentials	SNMP

- 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

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 100
- vEdge 100 B
- vEdge 100 M
- vEdge 100 WM
- vEdge 1000
- vEdge 2000
- vEdge 5000
- vEdge Cloud

The diagram shows a hierarchy of features. At the top are AAA and Archive. Below them are NTP and OMP. Then System. A large blue bar labeled VPN spans across. Underneath the VPN bar, 'Secure Internet Gateway (SIG)' is highlighted with a red box, with 'WAN' listed below it. To the right of SIG is another 'VPN' feature. Below these are 'VPN Interface Cellular' (with 'WAN' below it) and 'VPN Interface Ethernet' (with 'Management | WAN | LAN' below it).

5. Give it a **Template Name** of *SIG-Template* and a Description of *SIG Template*

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Add Template > [Secure Internet Gateway \(SIG\)](#)

Template Name

Description

Configuration

SIG Provider Umbrella

[+ Add Tunnel](#)

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	<i>ipsec1</i>
Source Interface	Global	<i>ge0/0</i>
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: [Empty]

Source Interface: ge0/0

Data-Center: Primary Secondary

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	<i>ipsec2</i>
Source Interface	Global	<i>ge0/0</i>
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)

Description

Source Interface

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
<input type="checkbox"/> ipsec1	<input checked="" type="checkbox"/>	<input type="text" value="ge0/0"/>	<input type="text" value="Primary"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300
<input type="checkbox"/> ipsec2	<input checked="" type="checkbox"/>	<input type="text" value="ge0/0"/>	<input type="text" value="Secondary"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300

High Availability

Active Backup

Pair-1

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

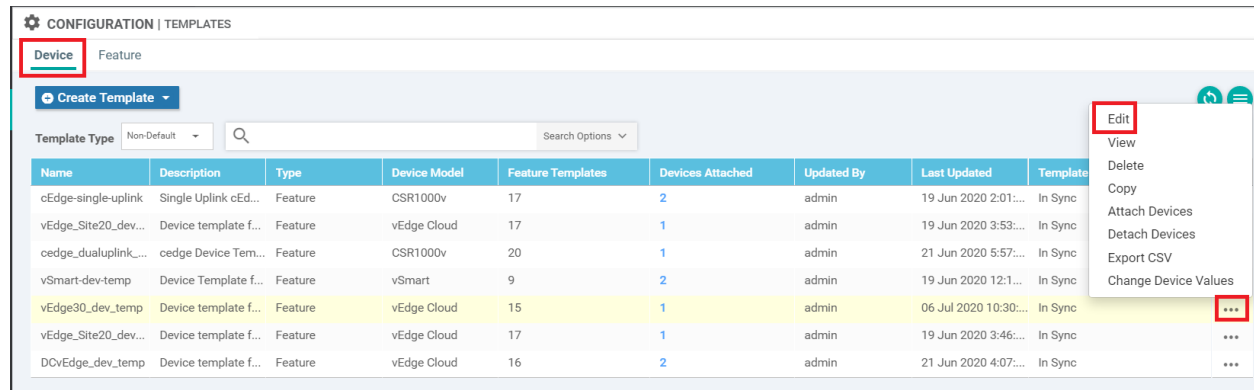
```

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



- Go to the **Transport & Management VPN** section click on **Secure Internet Gateway** under **Additional VPN 0 Templates**. Select the *SIG-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

This will be clickable when the page is opened and will get greyed out once added under the Transport & Management VPN section

12. Scroll down to the **Additional Templates** section and populate *SIG-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	Total	34	!	34	!
vEdge30_dev_temp	1	35	!	35	!
Device list (Total: 1 devices)		36	!	36	!
Filter/Search		37	omp	37	omp
17026153-f09e-be4b-6dce-482fce43aab2		38	no shutdown	38	no shutdown
vEdge30(10.255.255.31)		39	graceful-restart	39	graceful-restart
		40	advertise connected	40	advertise connected
		41	advertise static	41	advertise static
		42	!	42	!
		43	security	43	secure-internet-gateway
		44	ipsec	44	umbrella org-id 3870852
		45	authentication-type sha1-hmac ah-shal-hmac	45	umbrella api-key 8cbbd34d46614584a8f11a9b2c6cb861
		46	!	46	umbrella api-secret fcdea273e6ed4e2f9722a3c13ee1a79d
		47	!	47	!
		48	vpn 0	48	security
		49	dns 4.2.2.2 secondary	49	ipsec
		50	dns 8.8.8.8 primary	50	authentication-type sha1-hmac ah-shal-hmac
				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	!
				58	!

14. If you scroll down, *interface ipsec1* and *interface ipsec2* configuration can be viewed. Click on **Configure Devices**

Device Template	Total	98	!
vEdge30_dev_temp	1	99	interface ipsec1
Device list (Total: 1 devices)		100	ip unnumbered
Filter/Search		101	tunnel-source-interface ge0/0
17026153-f09e-be4b-6dce-482fce43aab2		102	tunnel-destination dynamic
vEdge30(10.255.255.31)		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 aes256-cbc-shal
		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-shal
		119	perfect-forward-secrecy group-16
		120	!
		121	mtu 1400
		122	no shutdown
		123	!

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 4b65a5150acalea1
  cipher-suite aes256-cbc-sha1
  dh-group     "14 (MODP-2048)"
  state        IKE_UP_IPSEC_UP
  uptime       0:00:00:18
  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       0:00:00:05
  tunnel-uptime 0:00:00:05
vEdge30#
```

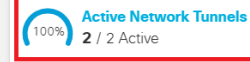
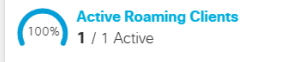
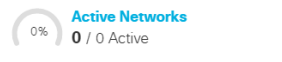
16. Log in to the Umbrella GUI. On the main overview page, you should see **Active Network Tunnels 2/2 Active**

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](#)

Cryptomining: 0 requests blocked in the last 24 hours [View Trend](#) | [View Details](#)

Deployment Health

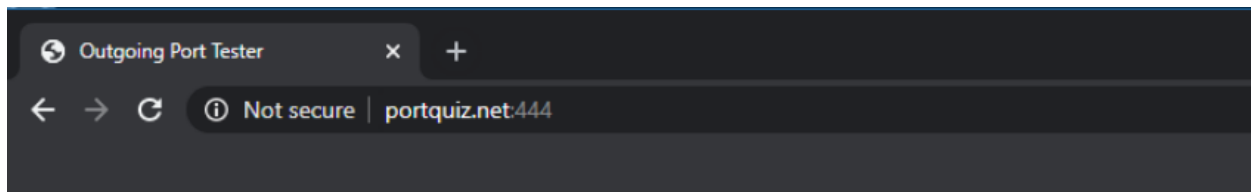


Network Breakdown

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 '^]'.

$ 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

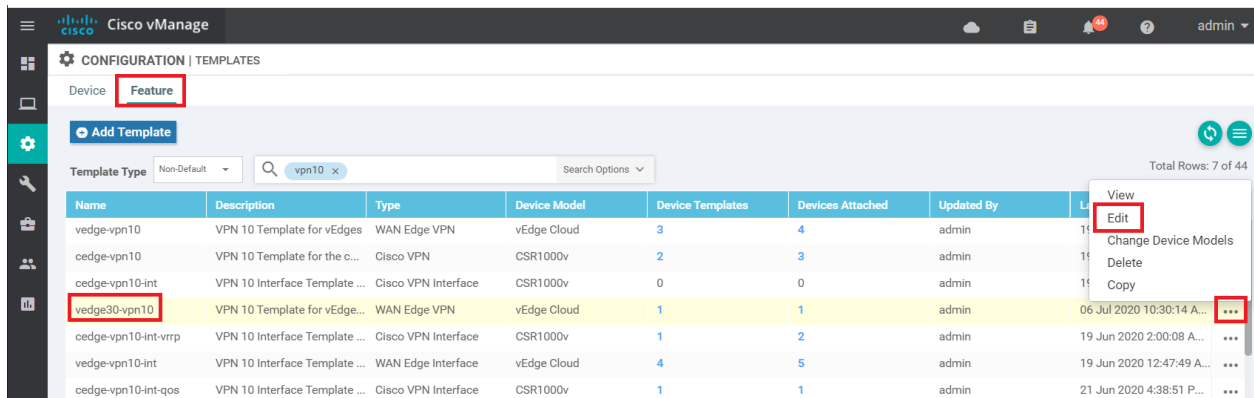
$ wget -qO- portquiz.net:444
Port 444 test successful!
Your IP: 14.140.162.5

# For Windows PowerShell users
PS C:\> Test-NetConnection -InformationLevel detailed -ComputerName portquiz.net -Port 444
```

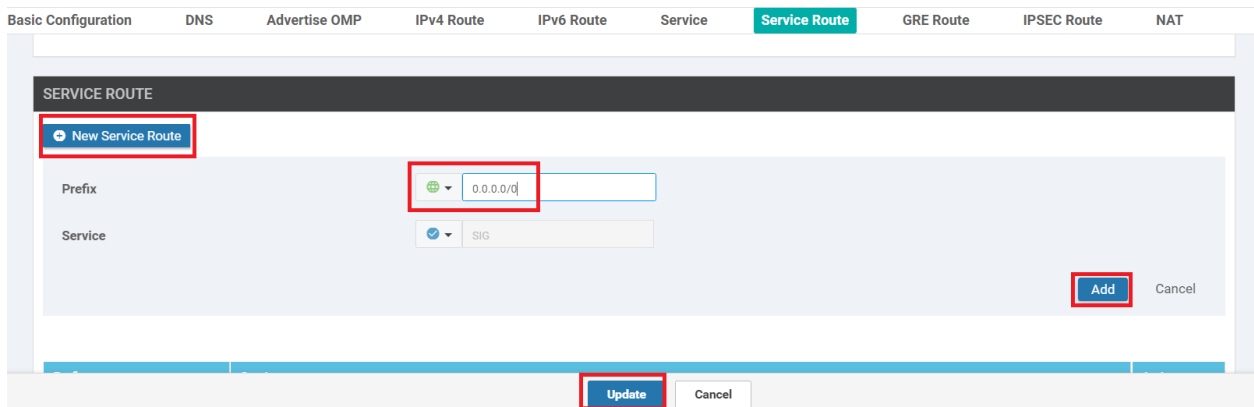
Test a port using your browser

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



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 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 computer, for example, Cisco ASA. The number of tunnels you can add depends on the number of compatible devices you are using. For more information

2 Total

Network Tunnels ▼	Status	Device Type	Last Active
SITE30SYS10x255x255x31Fipsec1	✔ Active	Viptela vEdge	Just Now
SITE30SYS10x255x255x31Fipsec2	✔ 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

Cisco Umbrella Policies / Management Firewall Policy

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](#).

FILTERS Search Firewall Rule names or descriptions

1 Total

<input type="checkbox"/>	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

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

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: Jul 6, 2020
Start Time: 02:12 AM
TO
Expiration Date: Mon DD YYYY
Expiration Time: -- -- -- --

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](#).

FILTERS

2 Total

<input type="checkbox"/>	Priority	Name	Status	Action	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit	
<input type="checkbox"/>	1	block444	Enabled	Block	TCP	Any IPs Any Ports	Any IPs 1 Port	▲ 0/24hrs	▲ No Hits	...
<input type="checkbox"/>	2	Default Rule	Enabled	Allow	Any	Any IPs Any Ports	Any IPs Any Ports	▲ 0/24hrs	Jul 04, 2020 - 01:39am	...

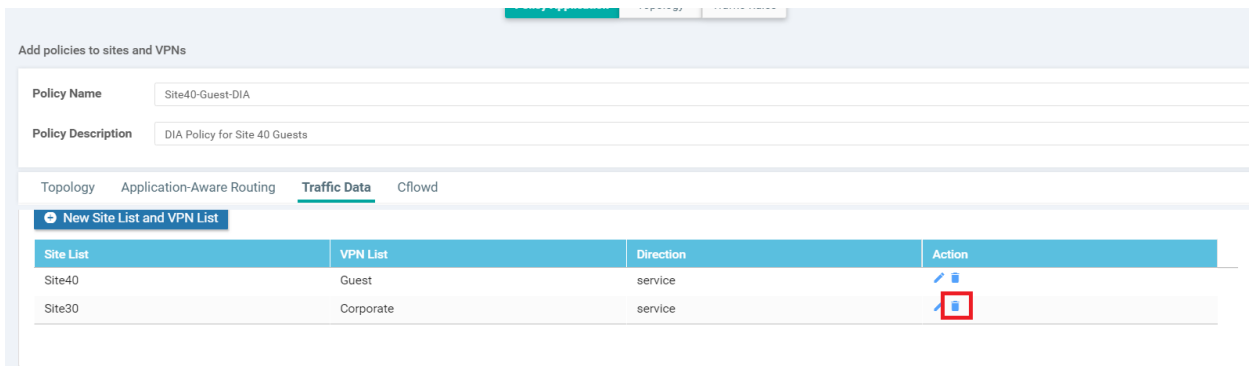
7. On the Site 30 PC, open a browser and go to whatismyip.com. The Public IPv4 address should show up as **14.140.162.5**. We will remove DIA configuration at Site 30 and check the Public IP again

The screenshot shows a web browser at whatismyip.com. The main content area displays:

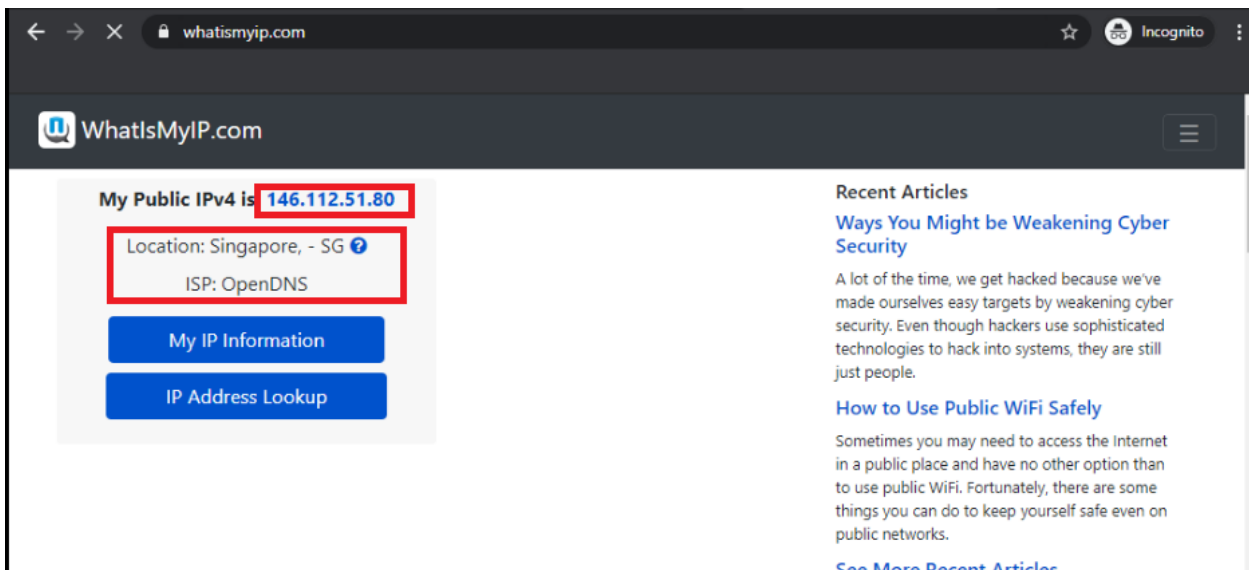
- My Public IPv4 is:** 14.140.162.5 (highlighted with a red box)
- Location:** Mohali, PB IN (highlighted with a red box)
- ISP: Tata Communications Limited
- Buttons: My IP Information, IP Address Lookup

 There is also a Google Ads banner and a 'Recent Articles' section on the right side of the page.

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



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



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.

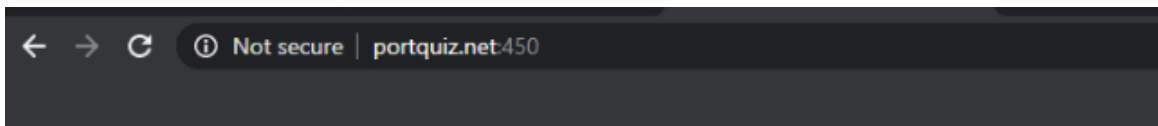
Try:

- 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: Priority Order: Last Before Default

Description:

14. Set the **Protocol** as ICMP

Rule Criteria
Specify protocol, IPs, network tunnels, and ports to be blocked or allowed.

Protocol:

Source Tunnels: Search and add specific source tunnels

Source IPs/CIDRs: Add IP address or CIDRs in comma-delimited format

Destination IPs/CIDRs: 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

blockyahoo

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

✕

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**

What would you like to protect?

Select Identities

Search Identities

All Identities

- Networks
- Roaming Computers 1 >
- Groups
- Tunnels 2 >

2 Selected REMOVE ALL

- Tunnels 2

[CANCEL](#)
[PREVIOUS](#)
[NEXT](#)

3. Click the Radio Button next to **Decrypt Blocked Traffic Only** on the **HTTP Inspection** window and click on **Next**

HTTPS Inspection

Configure how Umbrella should handle HTTPS traffic. [See HTTPS Inspection](#)

- Enable HTTPS Inspection
HTTPS traffic is intercepted and decrypted to provide security and policy enforcement at the URL layer, and visibility into the URL path. By default, HTTPS inspection attempts to decrypt all HTTPS traffic. For any HTTPS traffic that should not be decrypted, create a bypass inspection group.
- Decrypt Blocked Traffic Only**
Enable this feature for policies that should not inspect HTTPS traffic, but where HTTPS block pages are required.
- Disable HTTPS Inspection
HTTPS traffic is not intercepted. Domain layer security and policy enforcement still apply, and only domain layer visibility is possible.

Install Root Certificate Without a certificate installed, users will not be able to connect to some HTTPS sites and SSL connections could be broken. Your root certificates are available under Deployments > Configuration > Root Certificates. [View Distributing Root Certificates](#) [VIEW ROOT CERTIFICATES](#)

[CANCEL](#)
[PREVIOUS](#)
[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.

Select All Showing: All Lists ▾ 0 Total

All Destination Lists
 blockyadoo 1 >

1 Block Lists Applied REMOVE ALL
 blockyadoo 1

CANCEL PREVIOUS NEXT

5. Click **Next** on **File Analysis**, **File Type Control** and **Set Block Page Settings**. Give the Policy a name of *Webblockyadoo* and click on **Save**. The policy should show up above the *Default Web Policy*

Policies / Management

Web Policies +

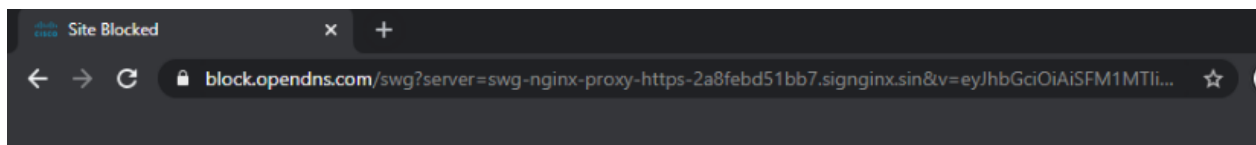
Add

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in [this article](#).

Sorted by Order of Enforcement

1	Webblockyadoo	Protection Web Policy	Applied To 2 Identities	Contains 5 Policy Settings	Last Modified Jul 6, 2020	▾
2	Default Web Policy	Protection Web Policy	Applied To All Identities	Contains 2 Policy Settings	Last Modified Jul 3, 2020	▾

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*



Cisco Umbrella

 This site is blocked due to content filtering.

yahoo.com

Sorry, yahoo.com has been blocked by your network administrator.

[> Report an incorrect block](#)

This site was blocked by the Cisco Umbrella proxy.

[> Diagnostic Info](#)

[Terms](#) | [Privacy Policy](#) | [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

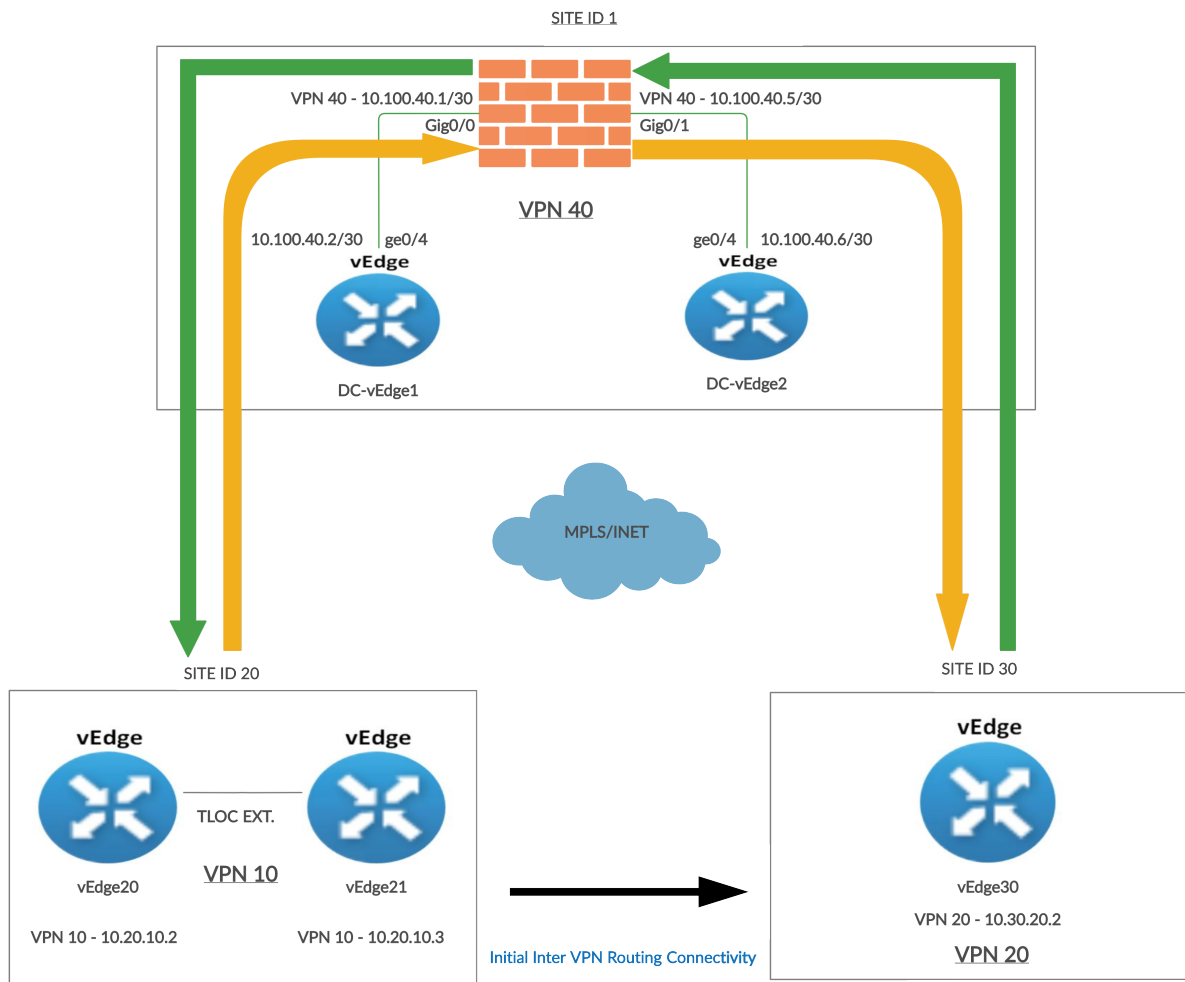
Overview

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

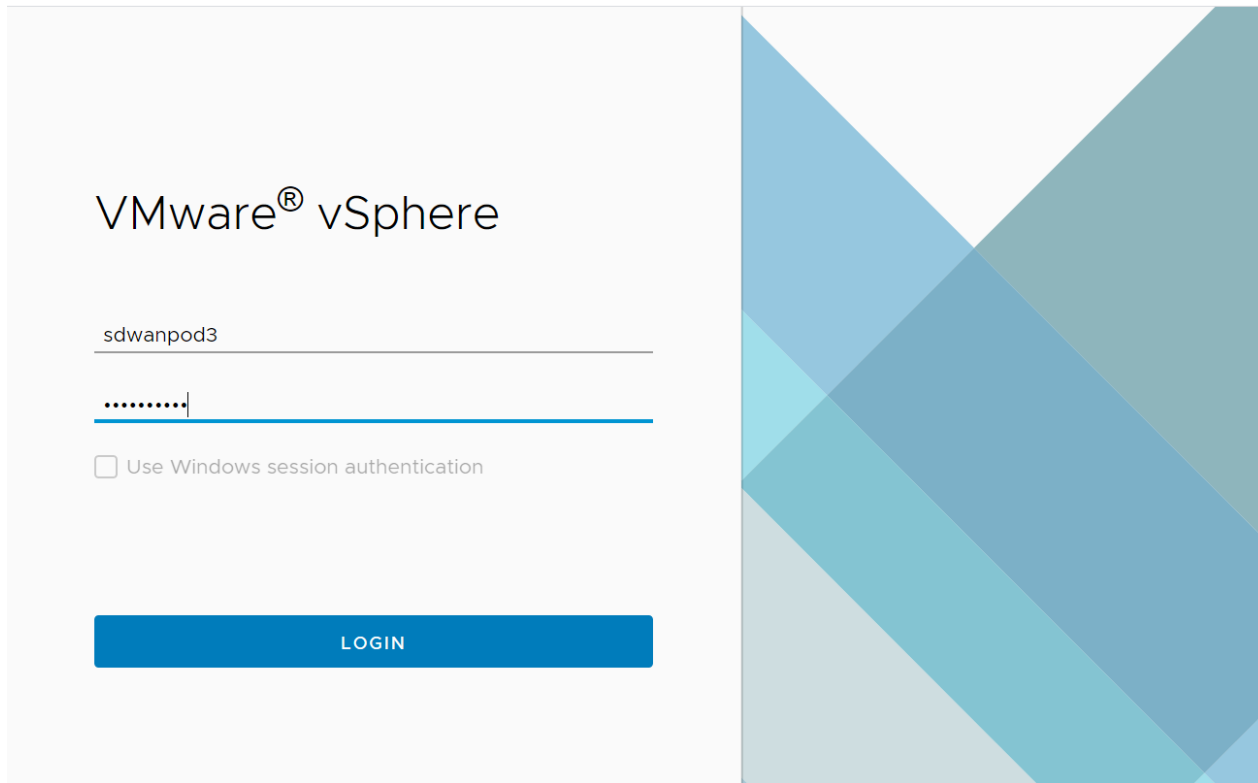
- [Overview](#)
- [Configure VPN 40 on DC-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)

Configure VPN 40 on DC-vEdges

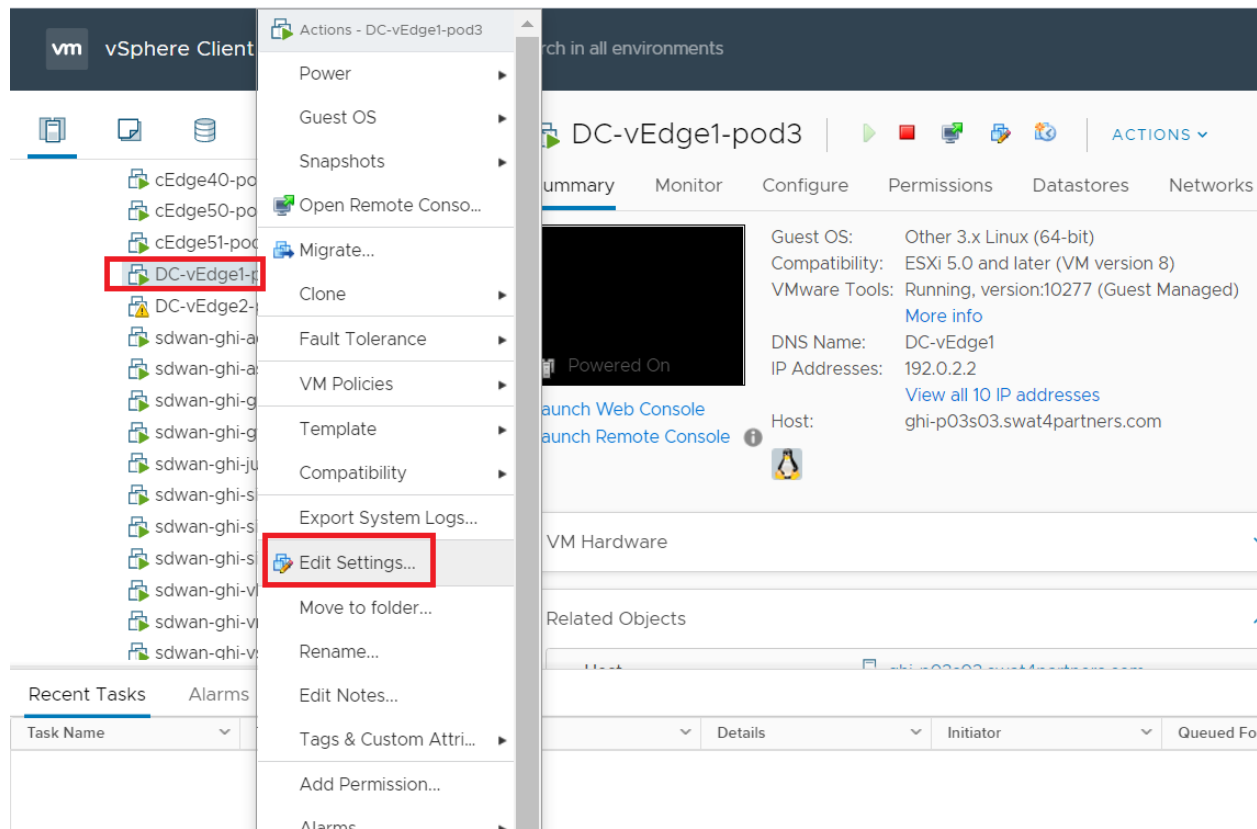
We will configure VPN 40 at the DC Site and ensure connectivity between the DC-vEdges and the ASA v Firewall.

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

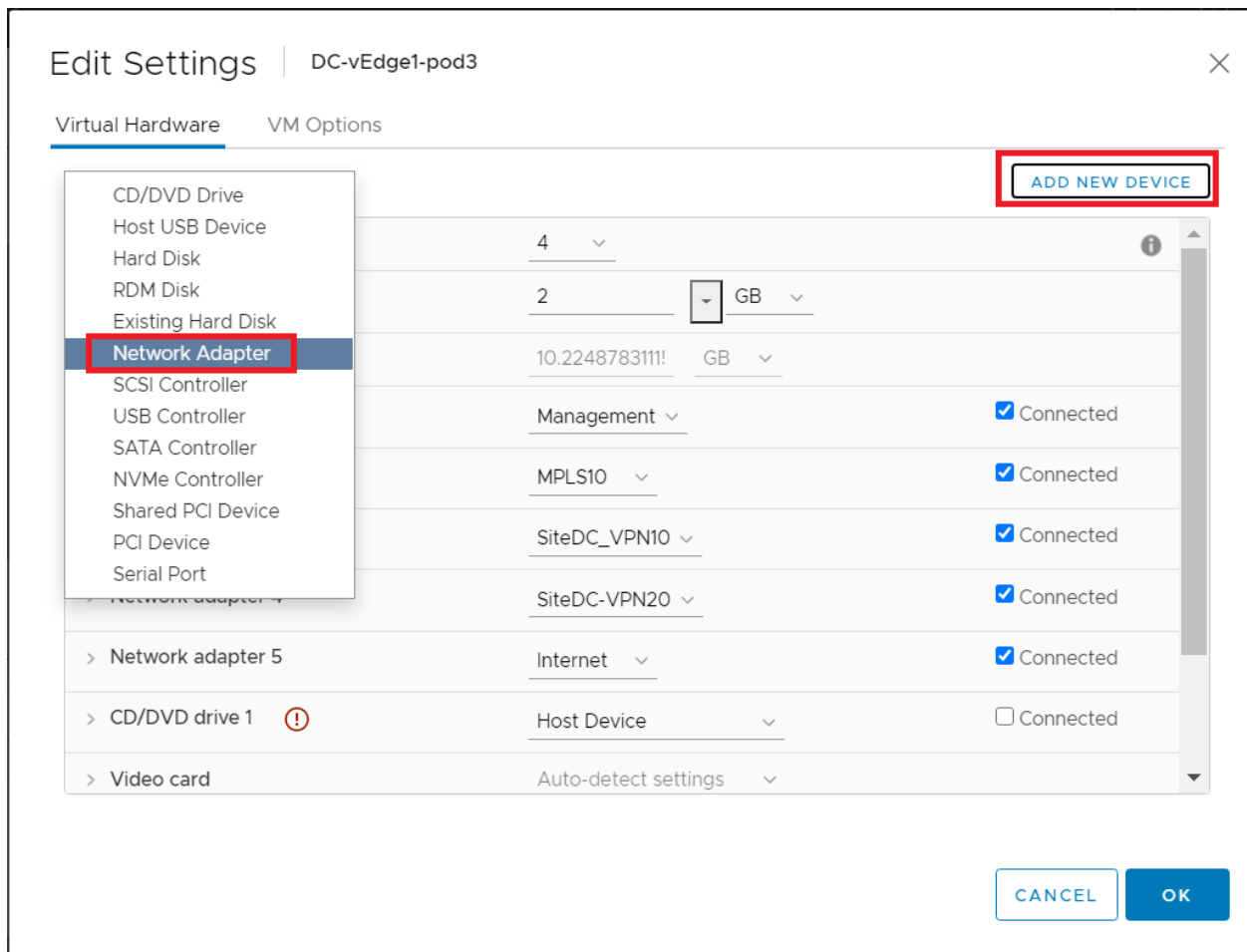
Username	Password
sdwanpodX	C1sco12345
(X is your POD number)	



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



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**



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 <input type="button" value="X"/>
> New Network *	Browse ...	<input checked="" type="checkbox"/> Connected
> CD/DVD drive 1 <input type="button" value="!"/>	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



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



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**

Edit Settings | DC-vEdge1-pod3

Virtual Hardware | VM Options

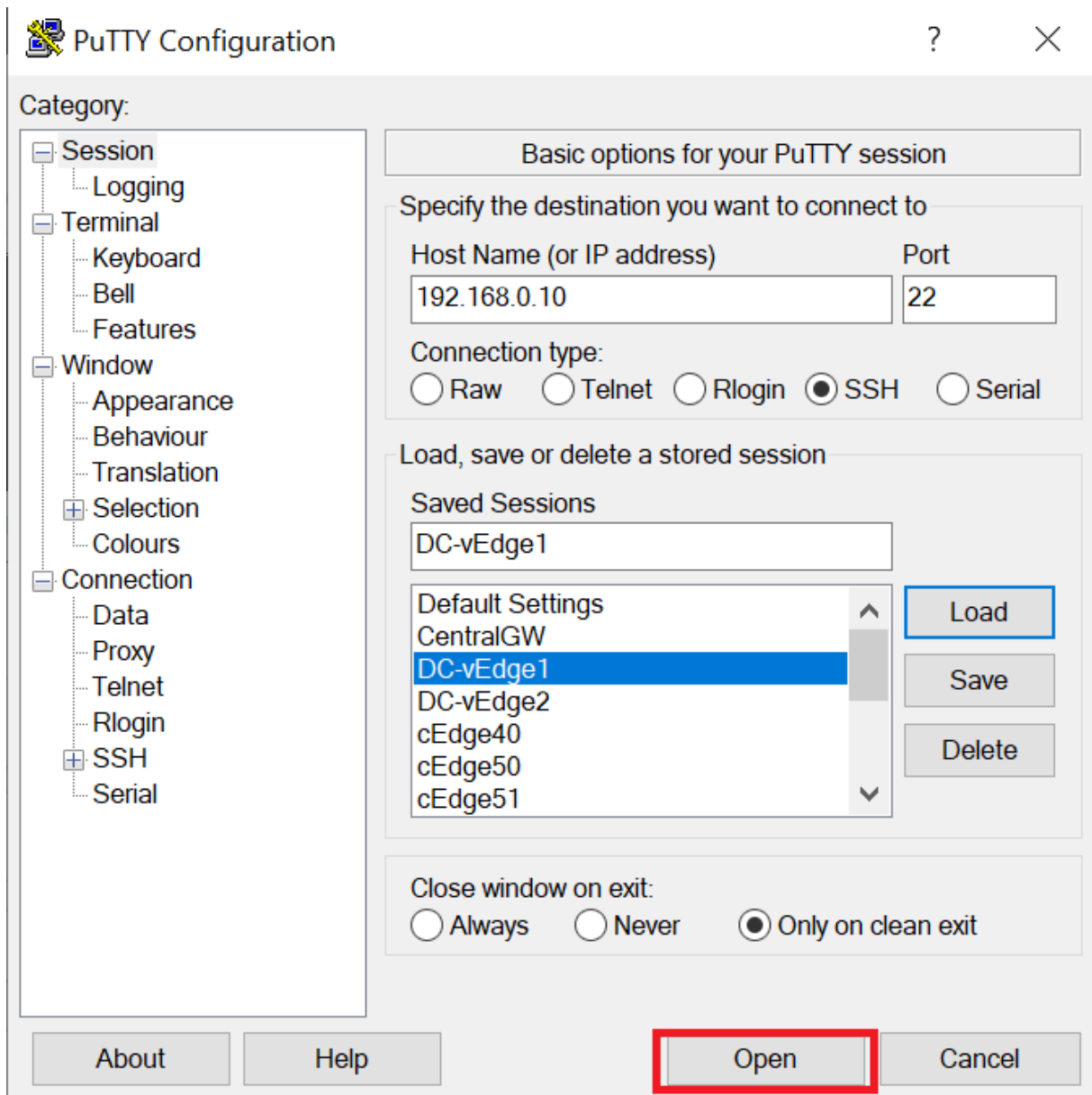
ADD NEW DEVICE

> 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 *	SiteDC_VPN10	<input checked="" type="checkbox"/> Connected
> New Network *	SiteDC-VPN40	<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	

CANCEL 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

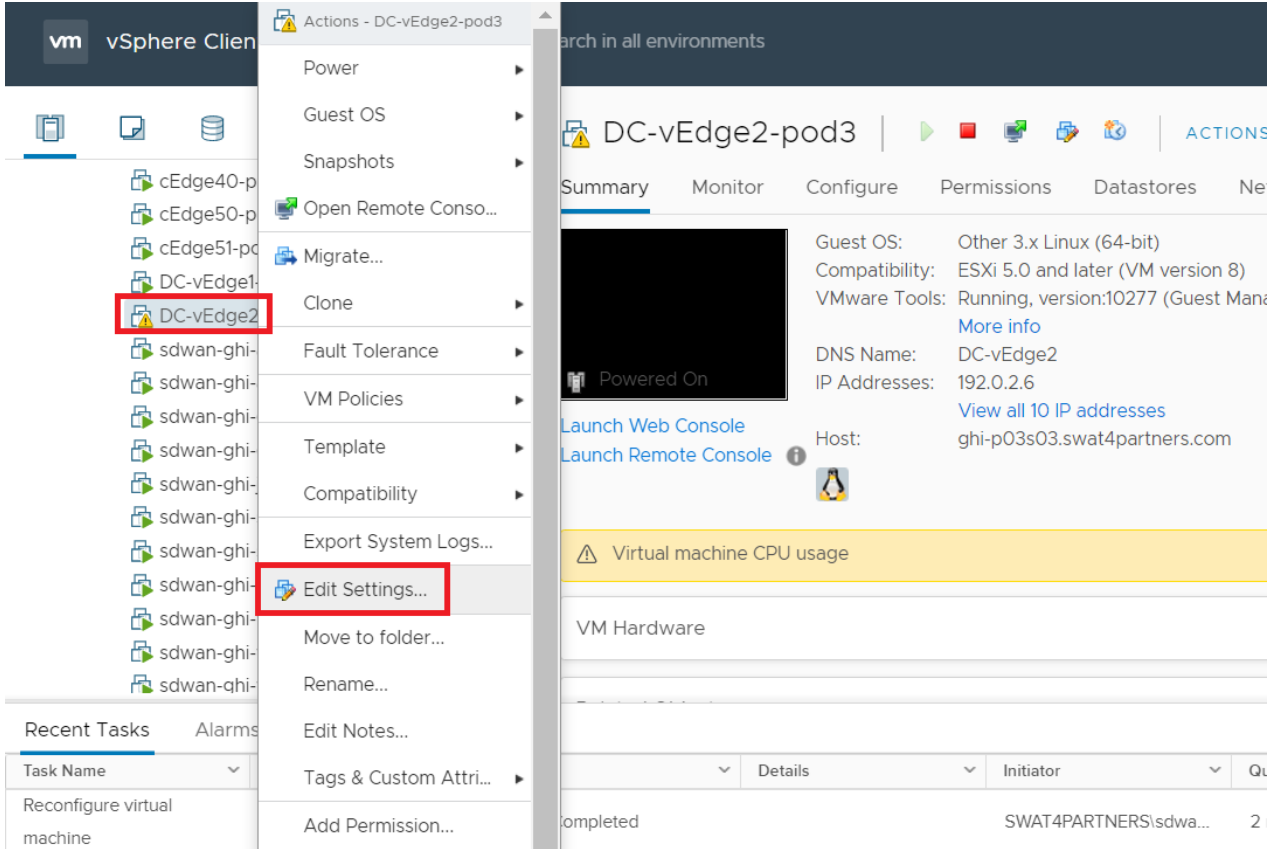


9. Type `reboot` and then `yes` to confirm the reboot

```
<C>
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**

DC-vEdge2-pod3

Virtual Hardware VM Options

ADD NEW DEVICE

> Network adapter 3	SiteDC_VPN10	Connected
> Network adapter 4	SiteDC-VPN20	Connected
> Network adapter 5	Internet	Connected
> New Network *	Internet	Connected
> New Network *	Browse ...	Connected
> CD/DVD drive 1	Host Device	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

12. Select *SiteDC_VPN10* and click on **OK**

Select Network



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

- 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



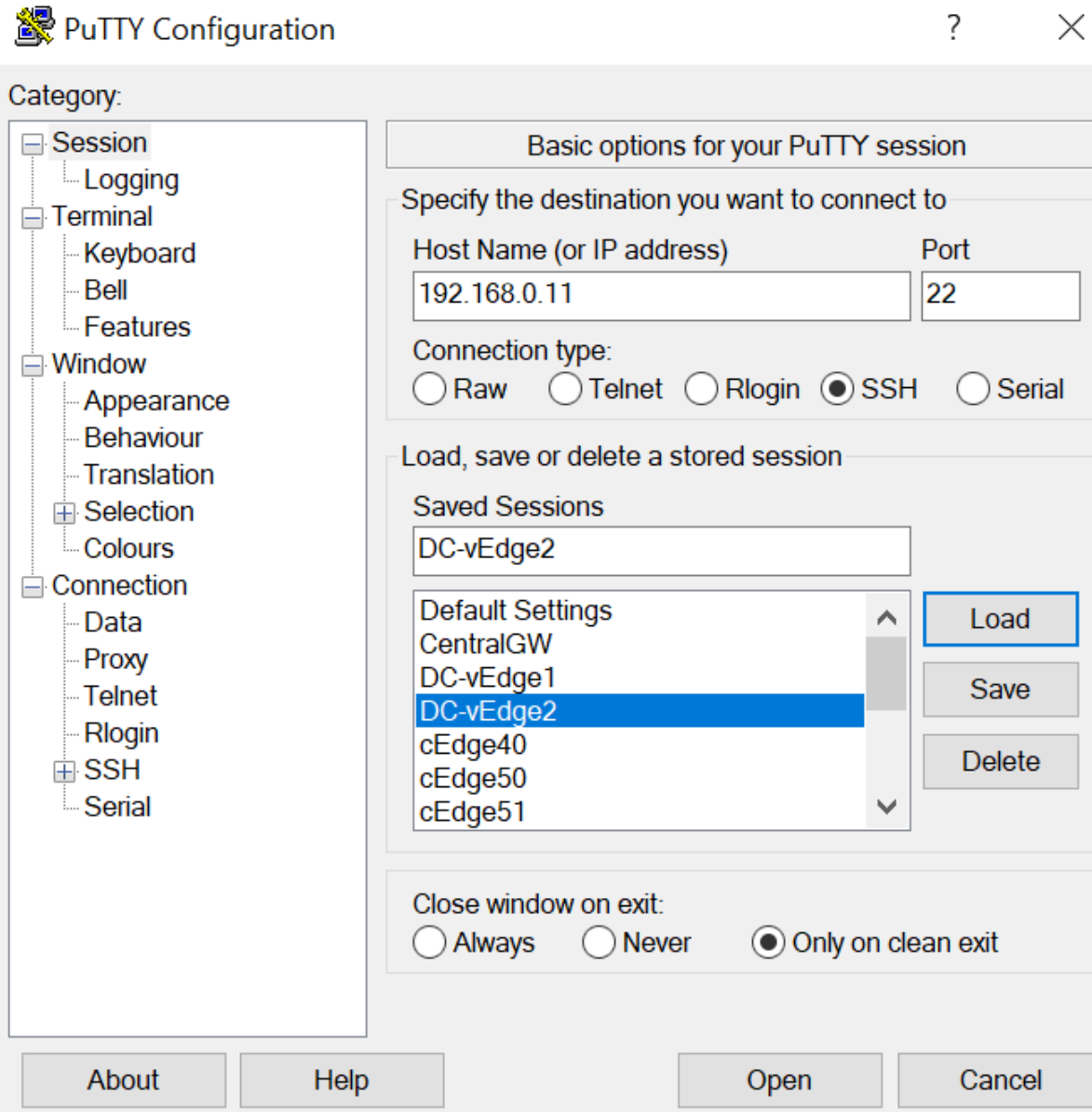
ADD NEW DEVICE

> 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



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
  ge0/1
  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
  |             Output modifiers
  <cr>
DC-vEdge2# show interface █
```

show interface ?

16. Type `reboot` and then `yes` to confirm the reboot

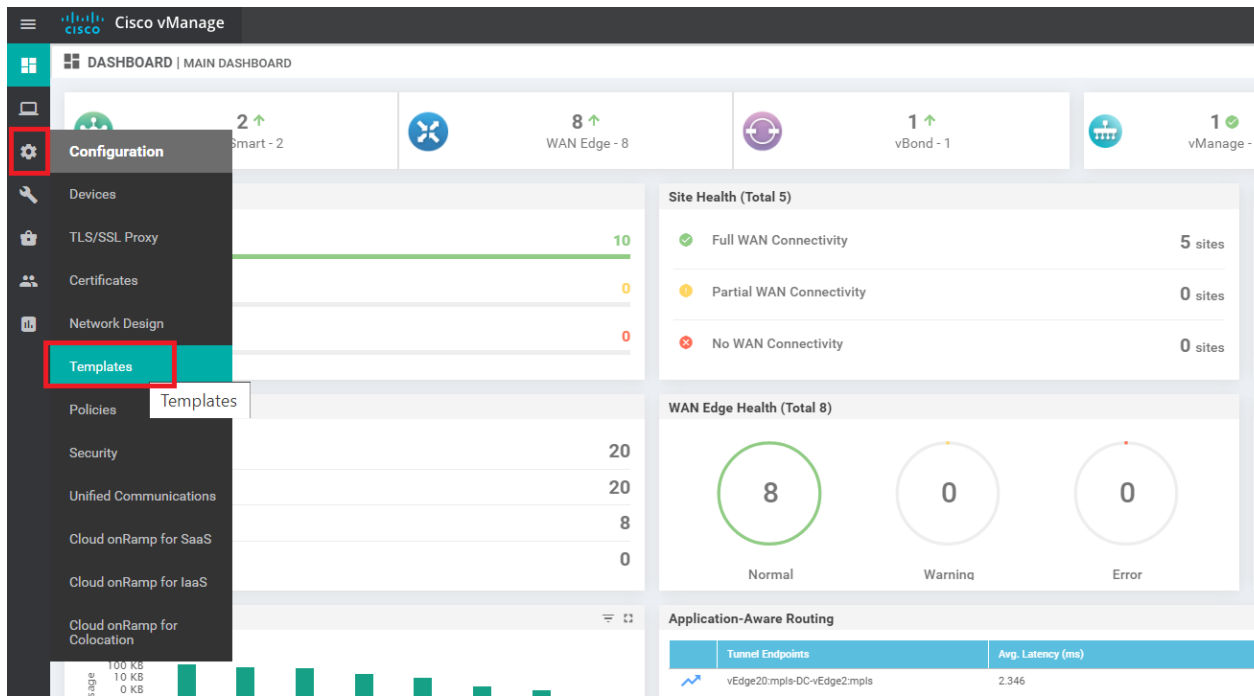
```
192.168.0.11 - PuTTY
arp-stats      Display ARP statistics
description    Display interface information
detail         Display detailed interface information
errors         Display error statistics
eth0
eth1
ge0/0
ge0/1
ge0/2
ge0/3
packet-sizes   Display packet sizes
port-stats     Display port statistics
queue         Display queue statistics
sfp           Display SFP information
statistics     Display interface statistics
system
vpn           VPN ID
|            Output modifiers
<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
  |            Output modifiers
  <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**



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 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 🌐 40

Name -

Enhance ECMP Keying - On Off

21. Scroll down to the **Advertise OMP** section and set **Static (IPv4)** and **Connected (IPv4)** to **On**

The screenshot shows the 'Advertise OMP' configuration page with the 'IPv4' tab selected. The following table summarizes the configuration options:

Protocol	On	Off
BGP (IPv4)	<input type="radio"/>	<input checked="" type="radio"/>
Static (IPv4)	<input checked="" type="radio"/>	<input type="radio"/>
Connected (IPv4)	<input checked="" type="radio"/>	<input type="radio"/>
OSPF External	<input type="radio"/>	<input checked="" type="radio"/>
EIGRP	<input type="radio"/>	<input checked="" type="radio"/>
LISP	<input type="radio"/>	<input checked="" type="radio"/>

22. Go to the **Service** section and click on **New Service**. Select the **Service Type** as *netvc1* and enter an **IPv4 Address** of *10.100.40.1*. Click on **Add**

The screenshot shows the 'SERVICE' configuration page. The 'New Service' button is highlighted with a red box. The configuration details are as follows:

- Service Type: netvc1
- IP Address: (selected), Interface:
- IPv4 address: 10.100.40.1
- Buttons: Add (highlighted with a red box), Cancel

23. Click on **New Service** again and select the **Service Type** as *netvc2*. 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

vedge

vEdge 100

vEdge 100 B

vEdge 100 M

vEdge 100 WM

vEdge 1000

vEdge 2000

vEdge 5000

vEdge Cloud

System

VPN

Secure Internet Gateway (SIG) WAN

VPN

VPN Interface Cellular WAN

VPN Interface Ethernet Management | WAN | LAN

VPN Interface IPsec WAN

VPN Interface NATPool WAN

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**

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:

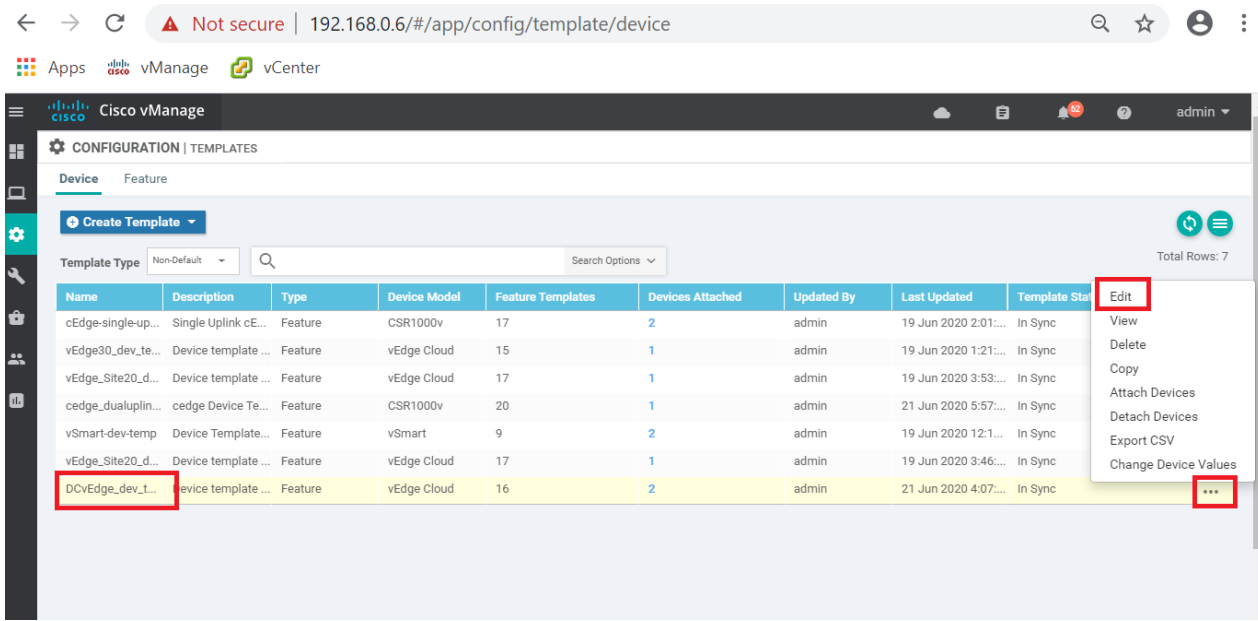
IPv4 IPv6

Dynamic Static

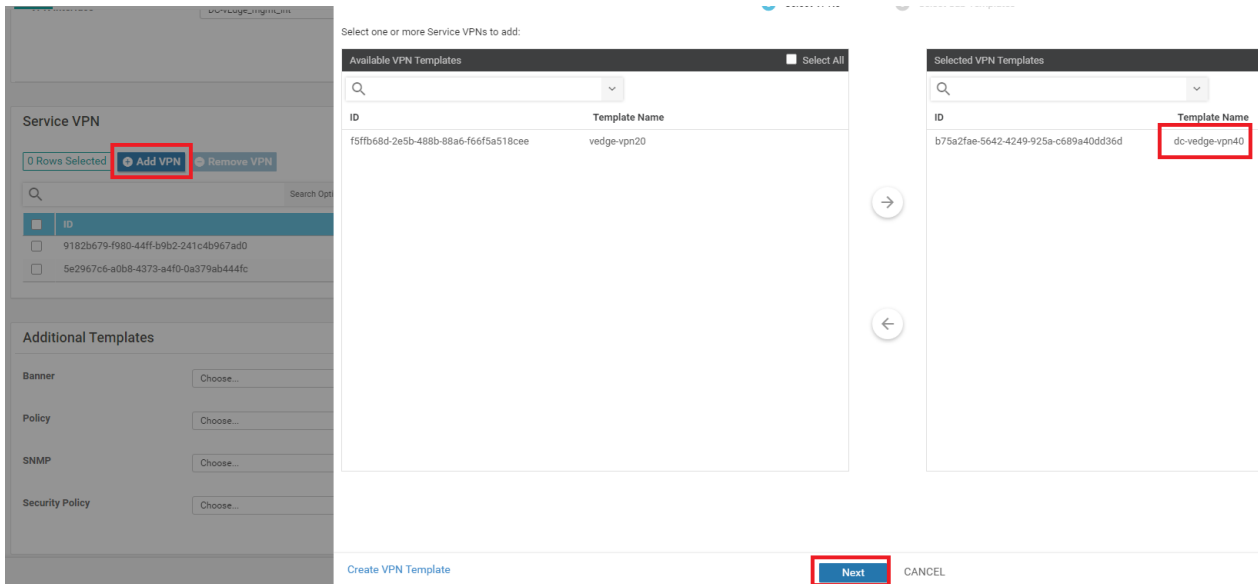
IPv4 Address:

Secondary IP Address (Maximum: 4)

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



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**



28. Click on **VPN Interface** under **Additional VPN Templates** and select *dc-vedge-vpn40-int1* under the VPN Interface drop down. Click on **Add**

Add VPN

Select VPNs Select Sub-Templates

Include sub-templates to attach to ALL selected service VPNs:

VPN Interface: dc-vedge-vpn40-int1 2 Sub-Templates

Additional VPN Templates

- BGP
- IGMP
- Multicast
- OSPF 1
- PIM
- VPN Interface
- VPN Interface Bridge
- VPN Interface GRE
- VPN Interface IPsec
- VPN Interface Natpool

3

BACK Add CANCEL

29. Make sure the Service VPN section shows the addition of the VPN 40 Template and click on **Update**

Service VPN

0 Rows Selected Add VPN Remove VPN

Search Search Options

ID	Template Name	Sub-Templates
<input type="checkbox"/> 9182b679-f980-44ff-b9b2-241c4b967ad0	vedge-vpn10	OSPF, VPN Interface
<input type="checkbox"/> 5e2967c6-a0b8-4373-a4f0-0a379ab444fc	vedge-vpn20-DC	VPN Interface
<input type="checkbox"/> b75a2fae-5642-4249-925a-c689a40dd36d	dc-vedge-vpn40	VPN Interface

Additional Templates

Banner:

Policy:

SNMP:

Security Policy:

Update Cancel

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

Search Options

Total Rows: 2

S...	Chassis Number	System IP	Hostname	IPv4 Address(vpn40_if_ipv4_address)	Interface Name(vpn20_if_name)	IPv4 Addr
<input checked="" type="checkbox"/>	0cdd4f0e-f2f1-fe75-866c-469966cda1c3	10.255.255.12	DC-vEdge2	10.100.40.6/30	ge0/3	10.100.20.: ...
<input checked="" type="checkbox"/>	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-469966cda1c3
DC-vEdge2|10.255.255.12

e474c5fd-8ce7-d376-7cac-ba950b2c9159
DC-vEdge1|10.255.255.11

Configure Device Rollback Timer

```

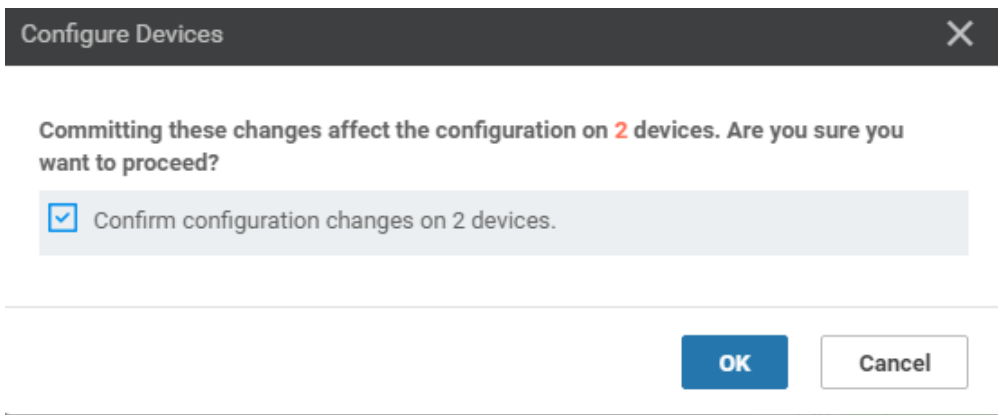
120 no shutdown
121 !
122 ip route 0.0.0.0/0 null0
123 omp
124 advertise connected
125 advertise static
126 !
127 !
128 vpn 512
129 dns 10.2.1.5 primary
130
131
132
133
134
135 omp
136 advertise connected
137 advertise static
138 !
139 !
140 vpn 512
141 dns 10.2.1.5 primary
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

vpn 40
service netavc1 address 10.100.40.1
service netavc2 address 10.100.40.5
interface ge0/4
ip address 10.100.40.2/30
no shutdown
!

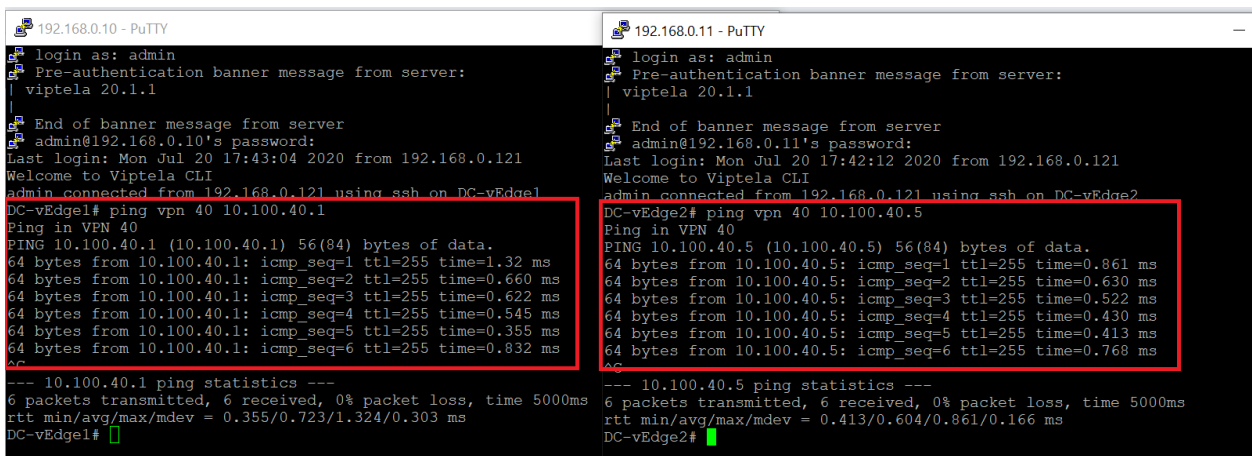
Back **Configure Devices** Cancel

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`



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

CONFIGURATION | TEMPLATES

Device Feature

+ Add Template

Template Type: Non-Default | Search: dc x | Search Options | Total Rows: 9 of 43

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 9:41:03	View Edit
DCvEdge-vpn512	VPN512 for the DC-vEdges	WAN Edge VPN	vEdge Cloud	4	5	admin	18 Jun 2020 9:46:20	Change Device Models Delete Copy
DCvEdge-vpn0	VPN0 for the DC-vEdges IN...	WAN Edge VPN	vEdge Cloud	1	2	admin	18 Jun 2020 9:41:03	...
DC-OSPF	OSPF Template for the DC	OSPF	vEdge Cloud	1	2	admin	18 Jun 2020 9:41:03	...
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

IPv4 ROUTE

+ New IPv4 Route

Optional	Prefix	Gateway	Selected Gateway Configuration		Distance	Action
<input type="checkbox"/>	0.0.0.0/0	Null 0	Enable Null	On	1	Trash icon

Update Cancel

3. To check the current routing tables for VPN 10 and VPN 20, navigate to **Monitor => Network**

The screenshot shows the Cisco vManage interface. The left sidebar has the 'Network' menu item highlighted with a red box. The main dashboard displays several widgets: 'WAN Edge Inventory' showing 20 total devices (8 deployed, 0 staging), 'WAN Edge Health' showing 8 Normal, 0 Warning, and 0 Error status, and 'Site Health' showing 5 sites with Full WAN Connectivity, 0 sites with Partial WAN Connectivity, and 0 sites with No WAN Connectivity. The 'Network' menu also shows 10 items, 0 events, and 0 ACL Log entries.

4. Click on **vEdge20**

Device Group: All 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	0cdd4f0e-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. The left sidebar has a red box around the 'Real Time' menu item. The main content area shows the 'Device Options' field with 'ip route' entered. Below it, a blue button labeled 'IP Routes' is highlighted. A search bar is present above a table of properties.

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

The screenshot shows a 'Select Filter' dialog box with a close button (X) in the top right corner. The text inside reads 'Choose filters to display data faster.' At the bottom, there are two buttons: 'Show Filters' (highlighted with a red box) and 'Do Not Filter'.

6. Enter a **VPN ID** of *10* and click on **Search** to filter the routes for VPN 10 on vEdge20

VPN ID:

AF Type:

Prefix:

Protocol:

[Reset All](#)

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

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
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

Inter VPN Routing has not been set up so we don't see any routes pointing to the VPN 20 subnet.

8. Click on **Select Devices** (top left-hand corner) and choose **vEdge30** from the drop down. Click on **Show Filters**

Device Options:

Filter ▾

VPN ID

AF Type

Prefix

Protocol

[Reset All](#)

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

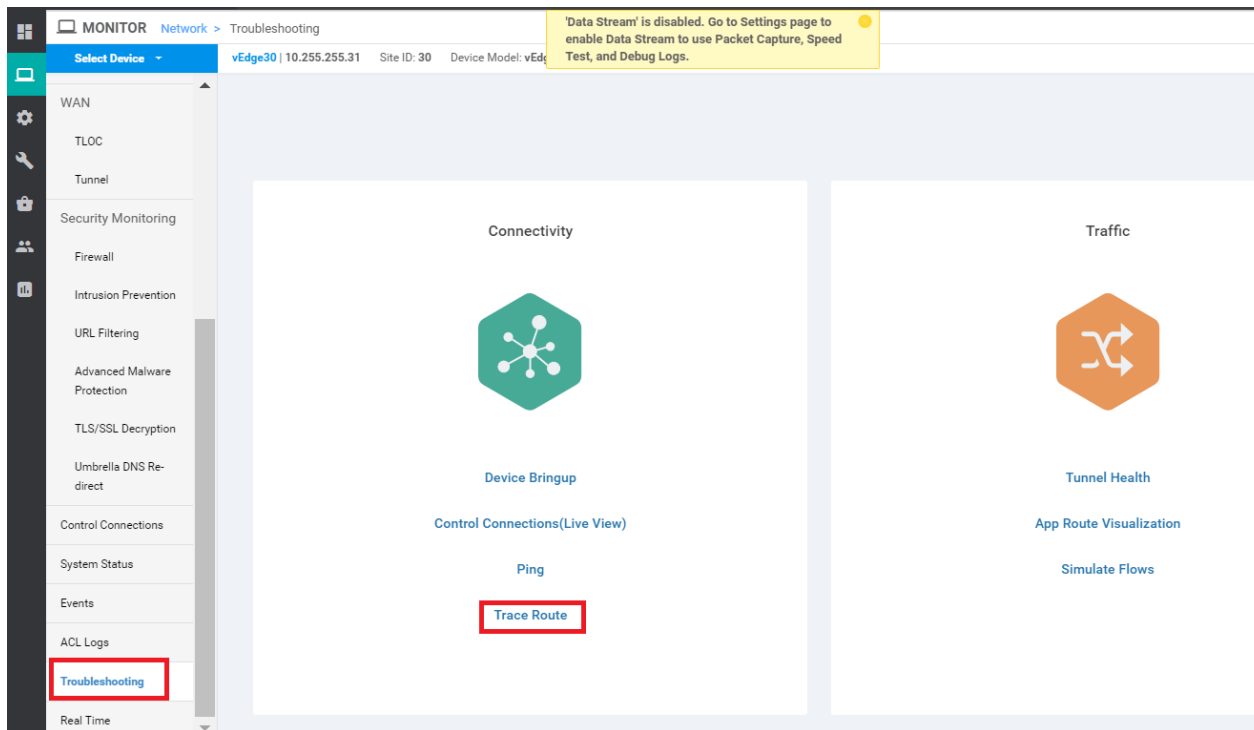
Device Options:

Filter ▾ VPN ID: 20

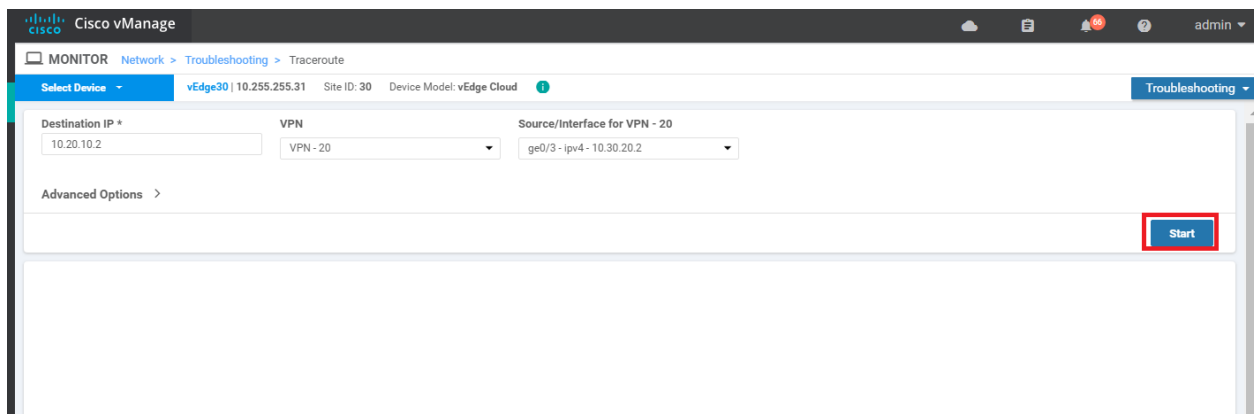
Search Options ▾

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

Select Device v | vEdge30 | 10.255.255.31 | Site ID: 30 | Device Model: vEdge Cloud | Troubleshooting

Destination IP * 10.20.10.2 | VPN VPN - 20 | Source/Interface for VPN - 20 ge0/3 - ipv4 - 10.30.20.2

Advanced Options >

Start

Output

```

Traceroute -m 15 -w 1 -s 10.30.20.2 10.20.10.2 in VPN
20
traceroute to 10.20.10.2 (10.20.10.2), 15 hops max,
60 byte packets
 1 127.1.0.2 (127.1.0.2) 0.108 ms IN 0.144 ms IN
 0.146 ms IN
  
```

- 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

Cisco vManage

MONITOR Network > Troubleshooting > Traceroute

Select Device v | vEdge30 | 10.255.255.31 | Site ID: 30 | Device Model: vEdge Cloud

Device Group Search

All Search Options

Sort by Reachability

Device Name	IP Address	Site ID	Device Model	Version	Reachability
cEdge40	10.255.255.41	40	CSR1000v	17.02.01r.0.32	Reachable
cEdge50	10.255.255.51	50	CSR1000v	17.02.01r.0.32	Reachable
cEdge51	10.255.255.52	50	CSR1000v	17.02.01r.0.32	Reachable
vEdge20	10.255.255.21	20	vEdge Cloud	20.1.1	Reachable
vEdge21	10.255.255.22	20	vEdge Cloud	20.1.1	Reachable
vEdge30	10.255.255.31	30	vEdge Cloud	20.1.1	Reachable

Source/Interface for VPN - 20 10.30.20.2

The screenshot displays the vManage GUI's Traceroute tool. At the top, a yellow notification states: "Data Stream is disabled. Go to Settings page to enable Data Stream to use Packet Capture, Speed Test, and Debug Logs." The configuration fields are: Destination IP: 10.30.20.2, VPN: VPN - 10, and Source/Interface for VPN: ge0/2 - ipv4 - 10.20.10.2. The 'Start' button is visible. The 'Output' section contains the following text: "Traceroute -m 15 -w 1 -s 10.20.10.2 10.30.20.2 in VPN 10", "traceroute to 10.30.20.2 (10.30.20.2), 15 hops max, 60 byte packets", and "1 127.1.0.2 (127.1.0.2) 0.061 ms !N 0.064 ms !N". To the right, a diagram shows a red dashed line connecting the source interface to the destination IP, with a red 'X' and the text "Network unreachable" in the middle.

We have established that Inter VPN communication is not happening between Site 20 and Site 30 as of now.

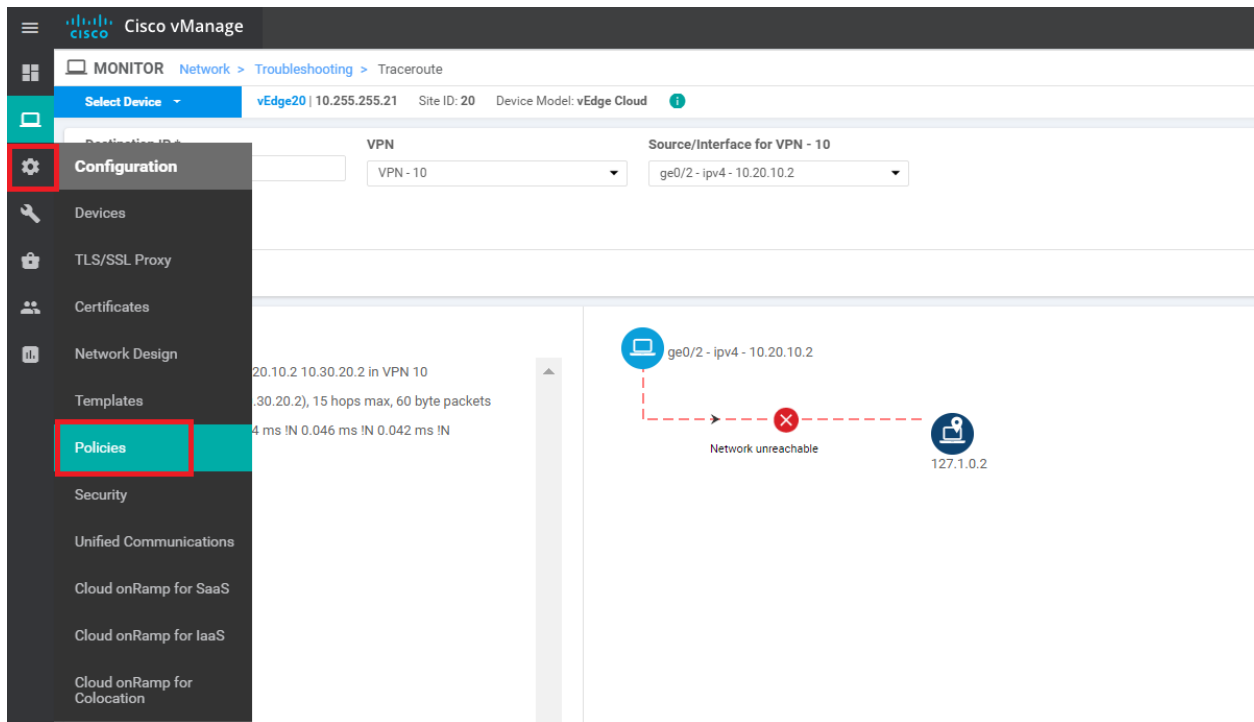
Task List

- [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](#)

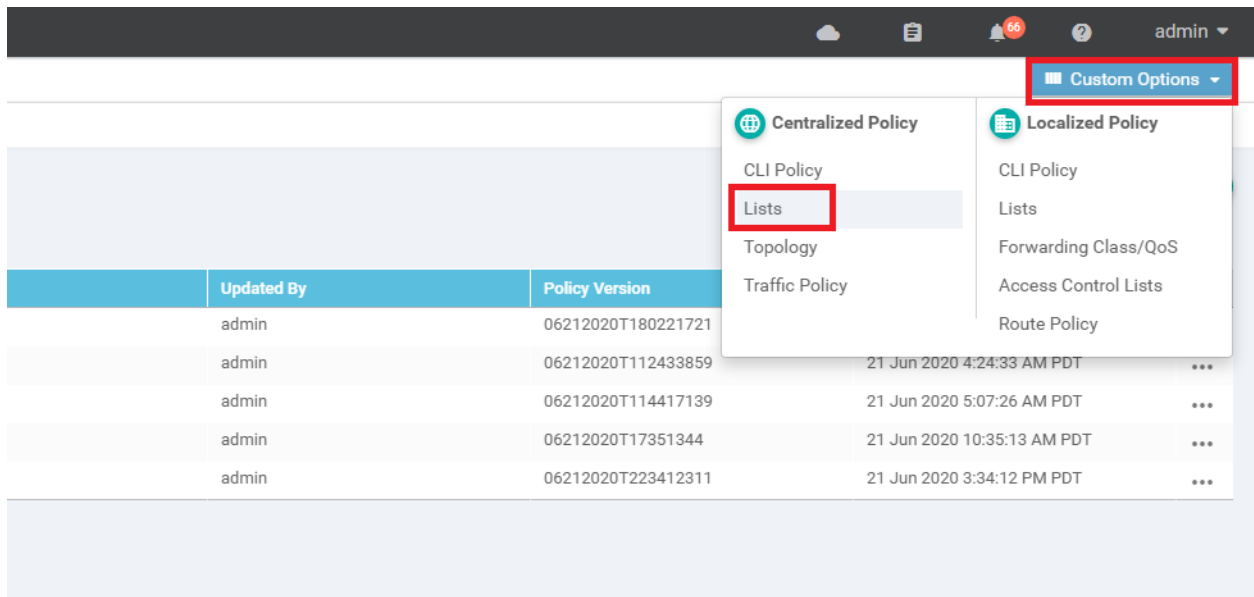
Setting up VPN Lists

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)



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**

Select a list type on the left and start creating your groups of interest

Application: **New VPN List**

VPN List Name: FW

Add VPN: 40

Add Cancel

Name	Entries	Reference Count	Updated By	Last Updated	Action
PoS	20	1	admin	21 Jun 2020 4:16:01 AM PDT	
Corporate	10	3	admin	21 Jun 2020 4:15:35 AM PDT	
Guest	30	1	admin	21 Jun 2020 4:16:14 AM PDT	

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**

New VPN List

VPN List Name: Corp_FW

Add VPN: 10,40

Add Cancel

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**

New VPN List

VPN List Name: PoS_FW

Add VPN: 20,40

Add Cancel

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	/ □ ■
FW	40	0	admin	20 Jul 2020 2:58:21 PM PDT	/ □ ■
PoS	20	1	admin	21 Jun 2020 4:16:01 AM PDT	/ □ ■
Corporate	10	3	admin	21 Jun 2020 4:15:35 AM PDT	/ □ ■
Guest	30	1	admin	21 Jun 2020 4:16:14 AM PDT	/ □ ■
Corp_FW	10, 40	0	admin	20 Jul 2020 2:59:41 PM PDT	/ □ ■

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 Custom Options

Centralized Policy Localized Policy

+ Add Policy 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 4:4...	View
Site20-Regional-Hub-Site30	Regional Policy for Site 20 to ...	UI Policy Builder	false	admin	06212020T114417139	21 Jun 2020 5:0...	Preview
traffic-engineering-ftp	Traffic Engineering for FTP	UI Policy Builder	false	admin	06212020T17351344	21 Jun 2020 10:...	Copy
AAR-VPN10	Transport Preference for VP...	UI Policy Builder	false	admin	06212020T223412311	21 Jun 2020 3:...	Edit
							Delete
							Deactivate

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

Policy Application **Topology** Traffic Rules

Specify your network topology

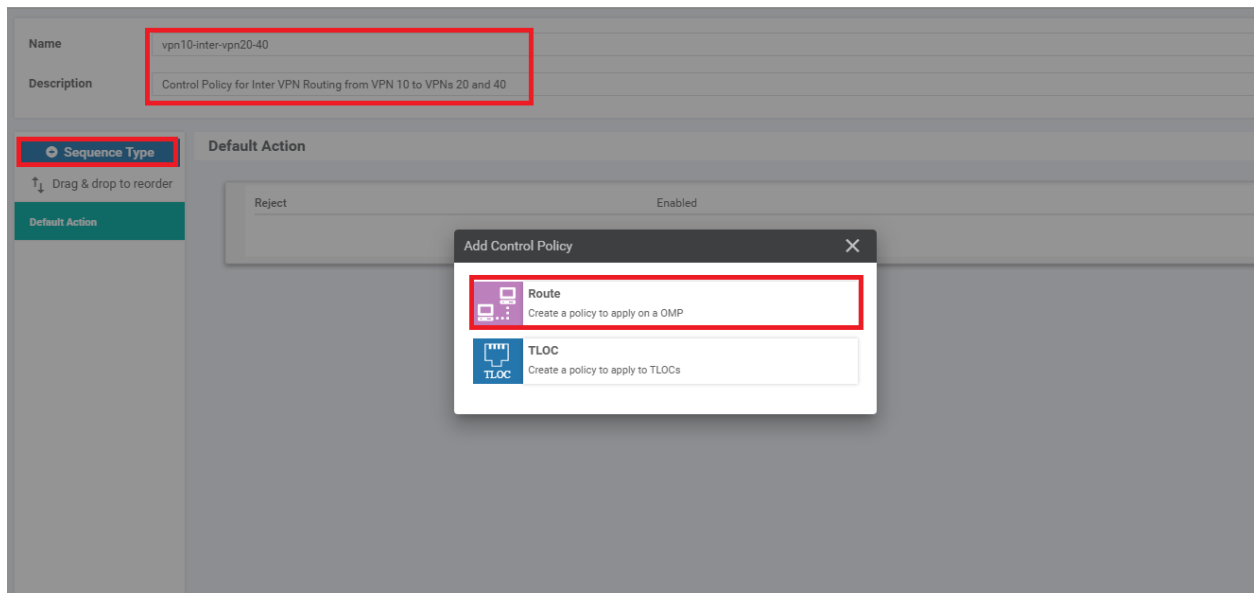
Topology VPN Membership

+ Add Topology

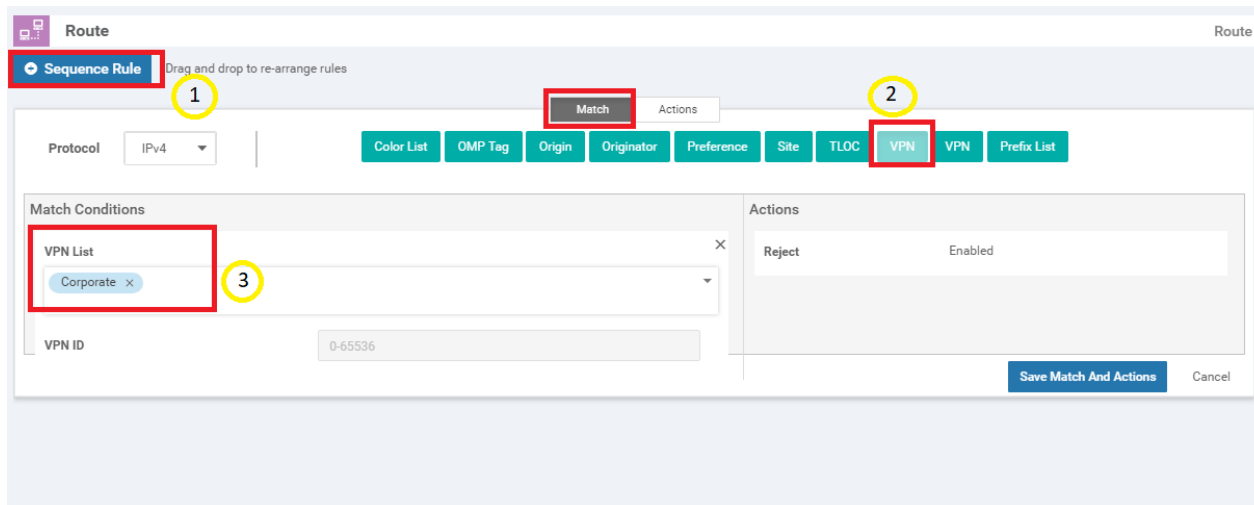
- Hub-and-Spoke
- Mesh
- Custom Control (Route & TLOC)
- Import Existing Topology

Type	Description	Reference Count	Updated By	Last Updated
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**

Match **Actions**

Protocol IPv4 Accept Reject

Export To OMP Tag Preference Service TLOC Action TLOC

Match Conditions

VPN List Corporate

VPN ID 0-65536

Actions

Accept Enabled

Export To PoS_FW

Save Match And Actions Cancel

6. Select **Default Action** on the left-hand side and click on the **pencil** icon to edit the Default Action

Name vpn10-inter-vpn20-40

Description Control Policy for Inter VPN Routing from VPN 10 to VPNs 20 and 40

Sequence Type

Drag & drop to reorder

Route

Default Action

Default Action

Reject Enabled

7. Click on **Accept** and then **Save Match And Actions**

Default Action

Actions

Accept Reject

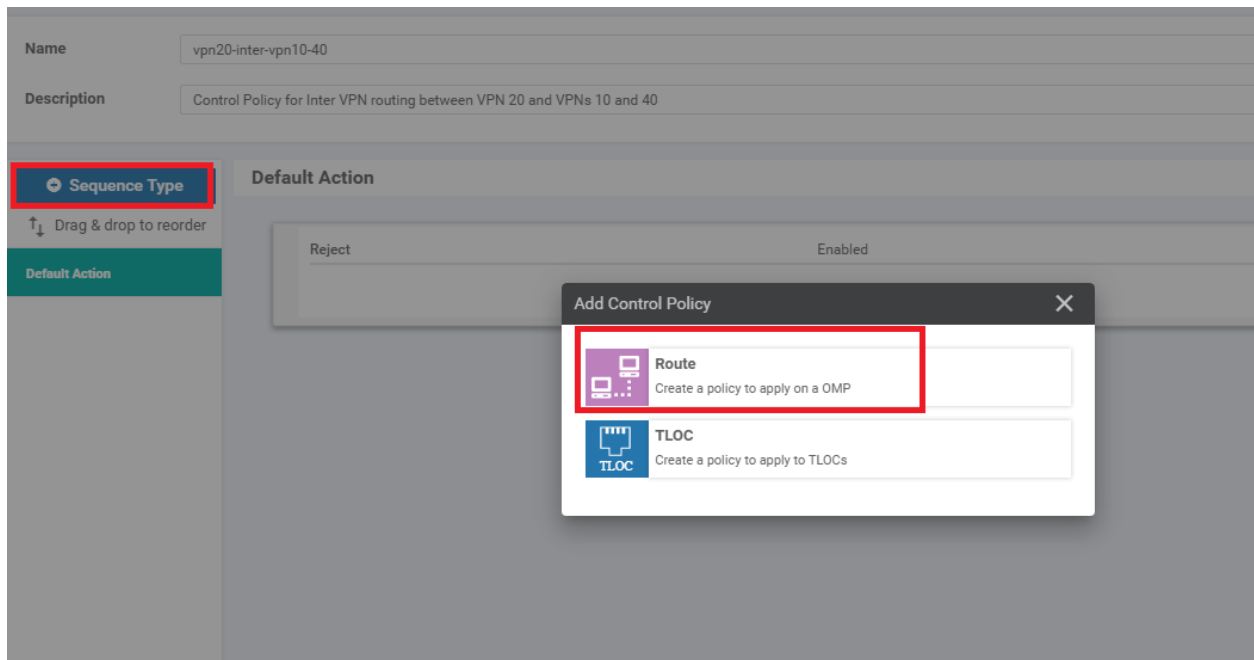
Accept Enabled

Save Match And Actions Cancel

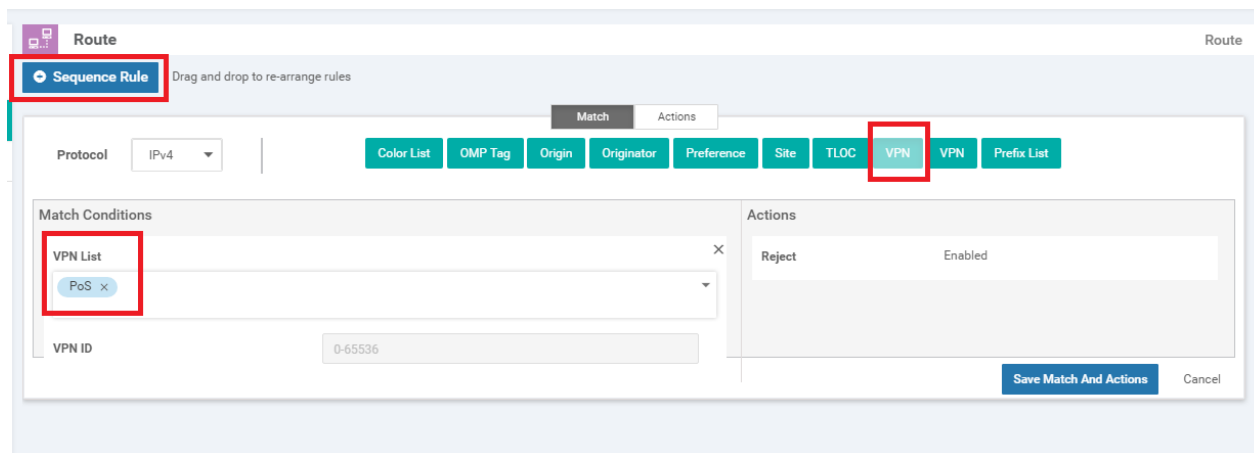
8. Click **Save Control Policy**

The screenshot displays a configuration window for a control policy. At the top, there are two input fields: 'Name' with the value 'vpn10-inter-vpn20-40' and 'Description' with the value 'Control Policy for Inter VPN Routing from VPN 10 to VPNs 20 and 40'. Below these fields is a sidebar on the left with a 'Sequence Type' section containing 'Route' and a 'Default Action' section. The main area is titled 'Default Action' and contains a single entry: 'Accept' with a status of 'Enabled'. At the bottom of the window, there are two buttons: 'Save Control Policy' (highlighted with a red box) and 'Cancel'.

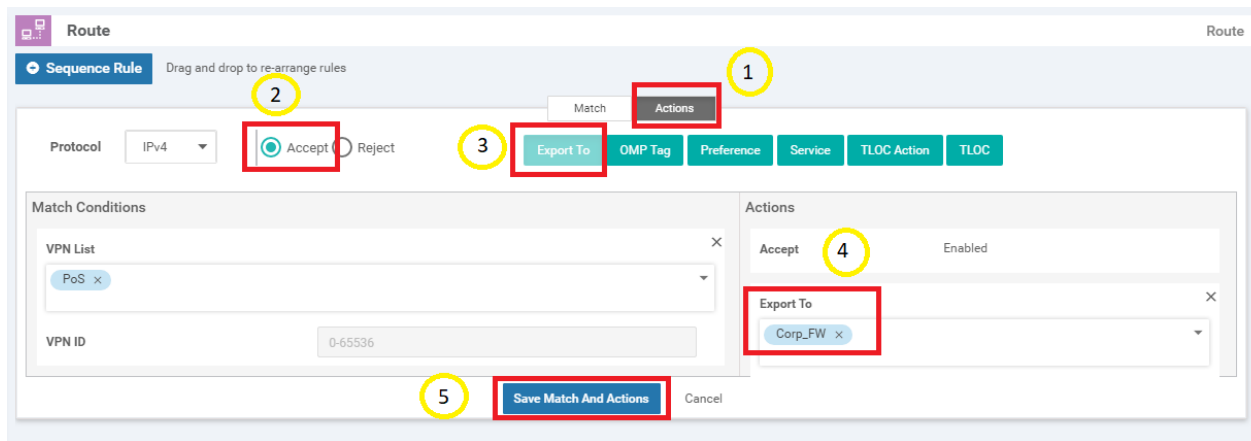
9. Click on **Add Topology** and add another *Custom Control (Route & TLOC)* policy. Give it a **Name** of *vpn20-inter-vpn10-40* with a Description of *Control Policy for Inter VPN routing between VPN 20 and VPNs 10 and 40*. Click on **Sequence Type** and select **Route**



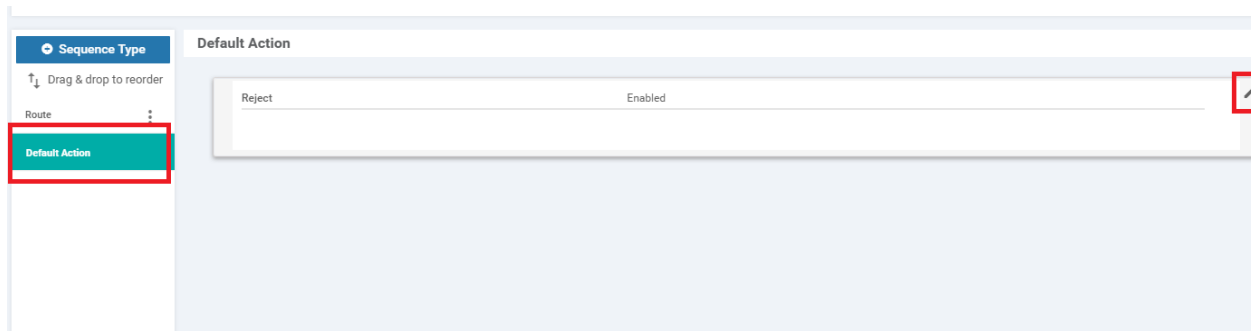
10. Click on **Sequence Rule** and select VPN as the match. Select *PoS* from the **VPN List**



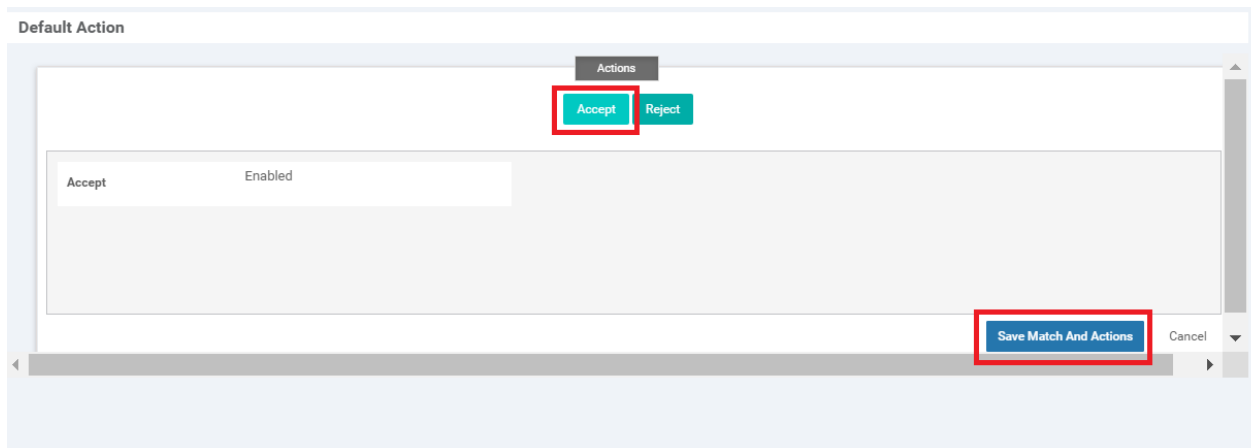
11. Click on the **Actions** tab and select the **Accept** radio button. Click on **Export To** and select the *Corp_FW* VPN list in the **Export To** drop down under Actions. To save the rule, click on **Save Match And Actions**



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**

Route

Sequence Rule Drag and drop to re-arrange rules

1

Match Conditions	Actions
VPN List: PoS	Accept
VPN Id	Export To: Corp_FW

Save Control Policy Cancel

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**

Policy Application
Topology
Traffic Rules

Add policies to sites and VPNs

Policy Name

Policy Description

Topology
Application-Aware Routing
Traffic Data
Cflowd

vpn10-inter-vpn20-40 CUSTOM CONTROL

+ New Site List

Inbound Site List

Site20 x

Outbound Site List

Select one or more site lists

Add
Cancel

Direction	Site List	Action

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**

vpn20-inter-vpn10-40 CUSTOM CONTROL

+ New Site List

Inbound Site List

Site30 x

Outbound Site List

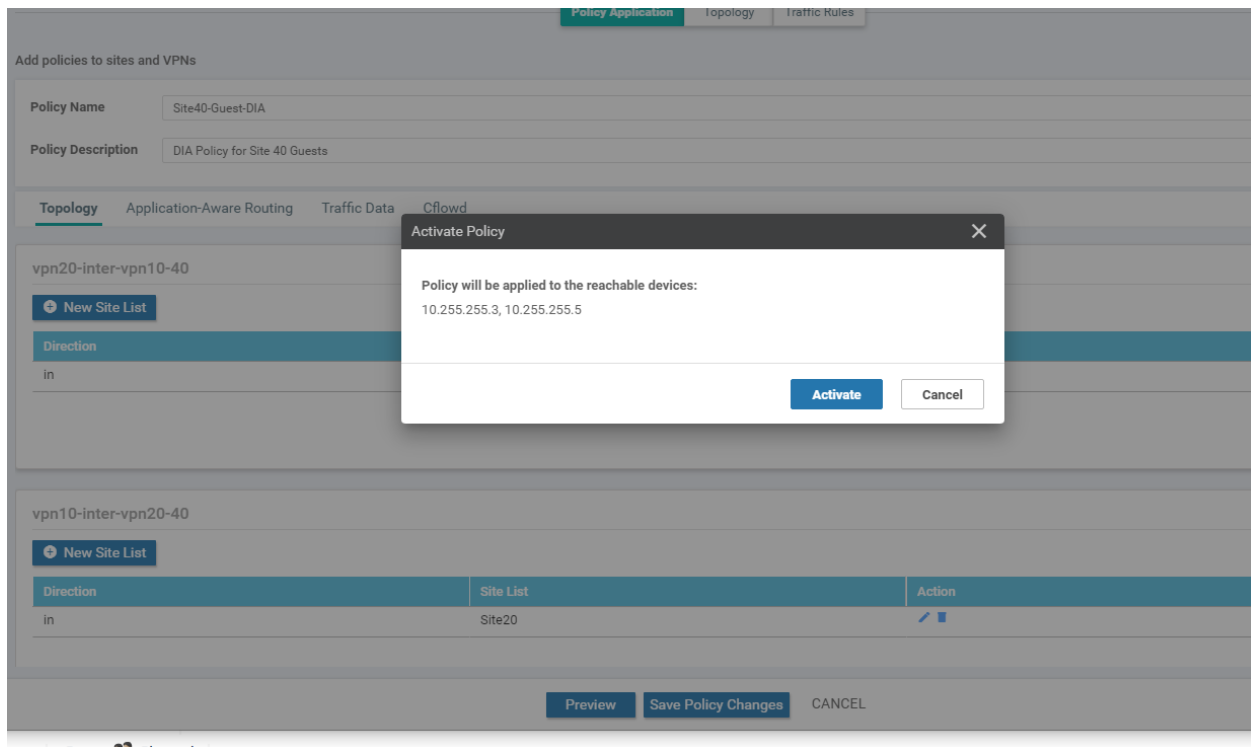
Select one or more site lists

Add
Cancel

Direction	Site List	Action

Preview
Save Policy Changes
CANCEL

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

MONITOR Network > Real Time

Select Device vEdge20 | 10.255.255.21 Site ID: 20 Device Model: vEdge Cloud

Device Options: IP Routes

Filter VPN ID: 10

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

Device Group Search

All Search Options

Sort by Reachability

Device Name	IP Address	Site ID	Device Model	Version	Protocol	Next Hop
Reachable						
cEdge40	10.255.255.41	40	CSR1000v	17.02.01r.0.32	connected	--
Reachable						
cEdge50	10.255.255.51	50	CSR1000v	17.02.01r.0.32	omp	--
Reachable						
cEdge51	10.255.255.52	50	CSR1000v	17.02.01r.0.32	omp	--
Reachable						
vEdge20	10.255.255.21	20	vEdge Cloud	20.1.1	omp	--
Reachable						
vEdge21	10.255.255.22	20	vEdge Cloud	20.1.1	omp	--
Reachable						
vEdge30	10.255.255.31	30	vEdge Cloud	20.1.1	omp	--
Reachable						
Control Connections					10	ipv4 10.100.10.0/24
					10	ipv4 10.100.10.0/24

3. Click **Show Filters** and enter a **VPN ID** of 20. Click on **Search**

Select Filter

Choose filters to display data faster.

Show Filters Do Not Filter

VPN ID:

AF Type:

Prefix:

Protocol:

[Reset All](#)

4. You should see routes for Site 20 VPN 10

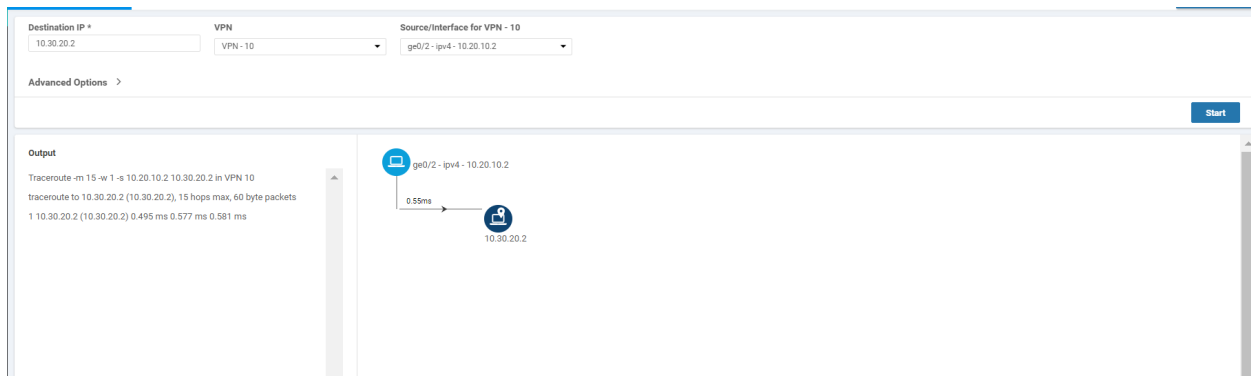
vEdge30 | 10.255.255.31 | Site ID: 30 | Device Model: vEdge Cloud

Device Options:

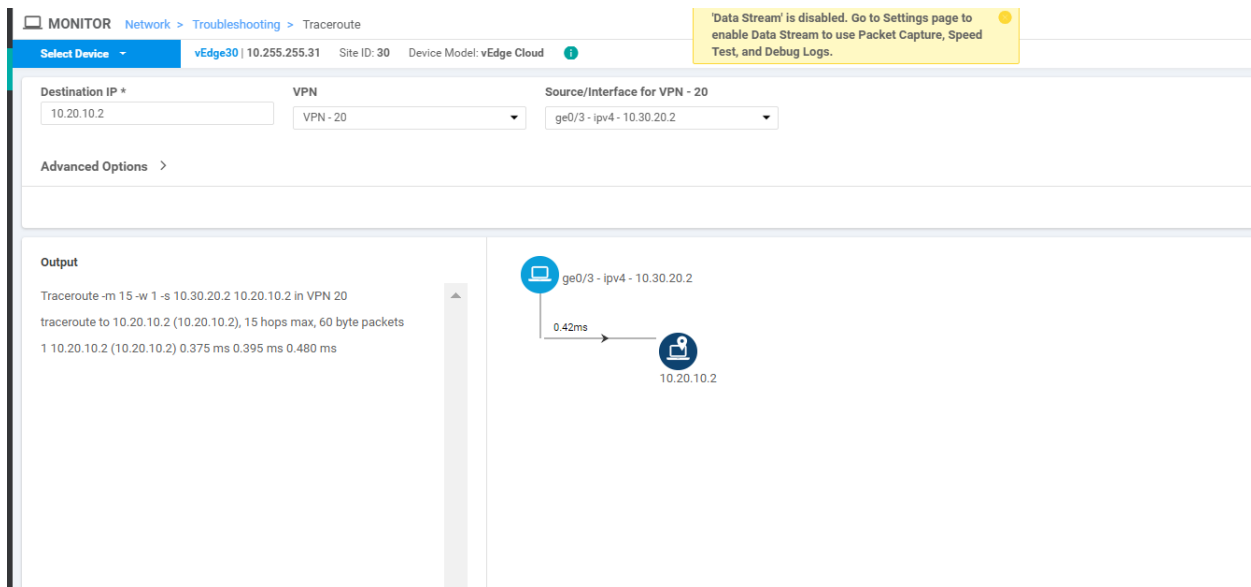
Filter: VPN ID: 20

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



6. 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.

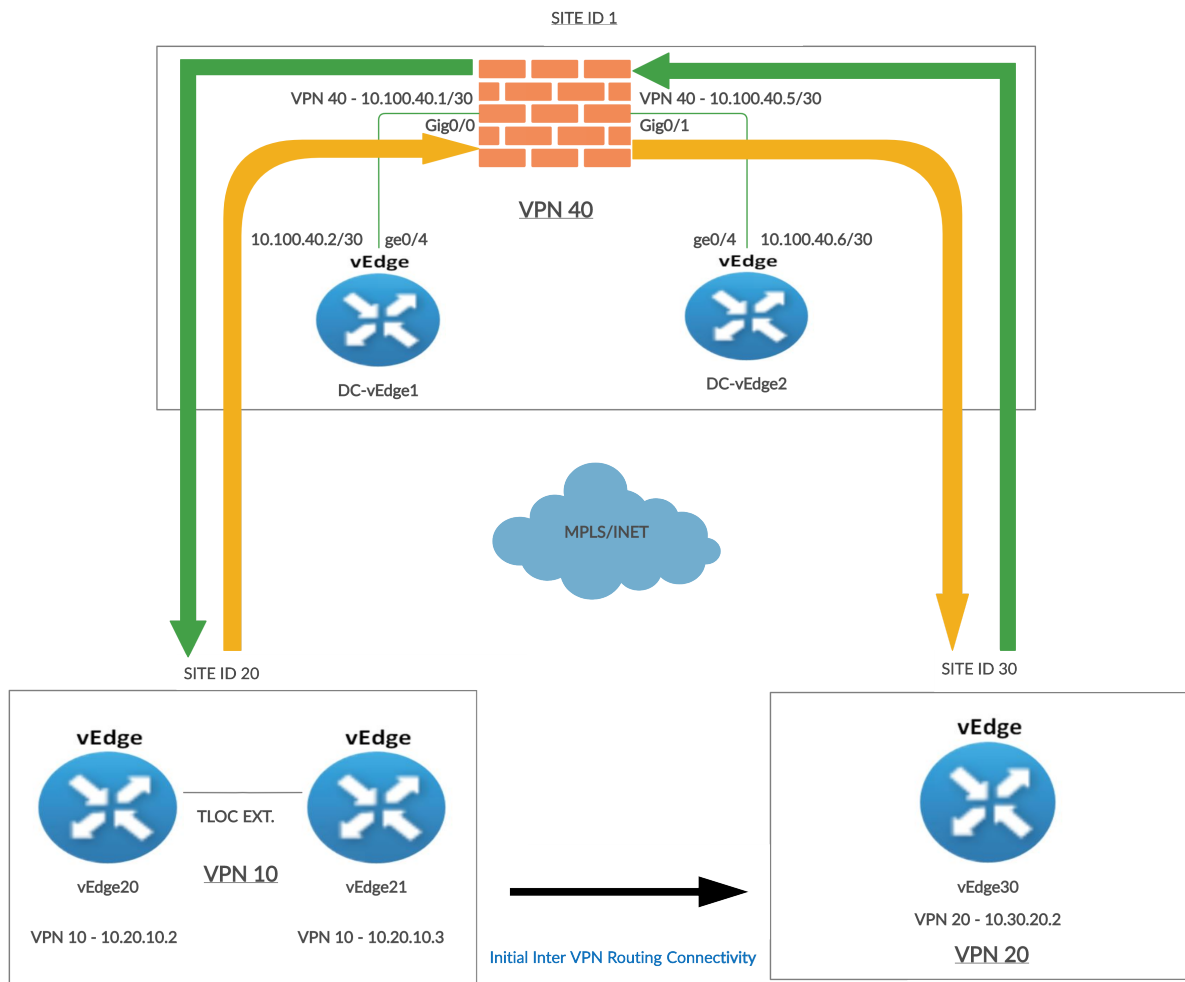
Task List

- [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

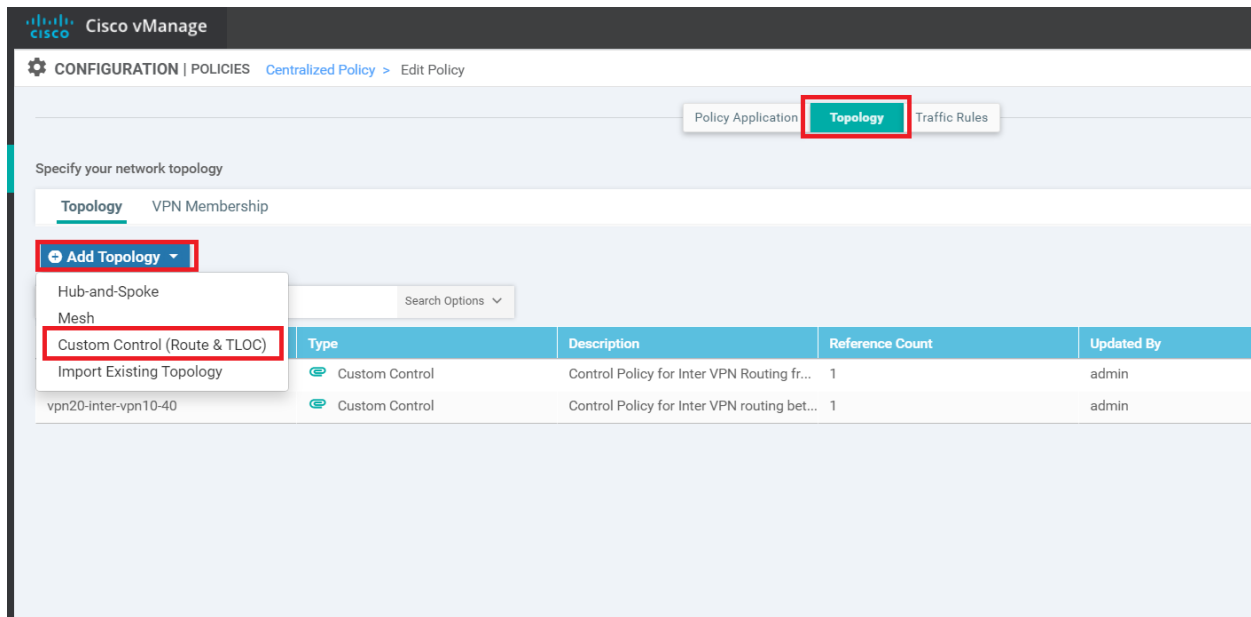
Destination IP: 10.30.20.2

The Green arrow is the traffic flow from Site 30 VPN 20 to Site 20 VPN 10 once Service Chaining is configured.

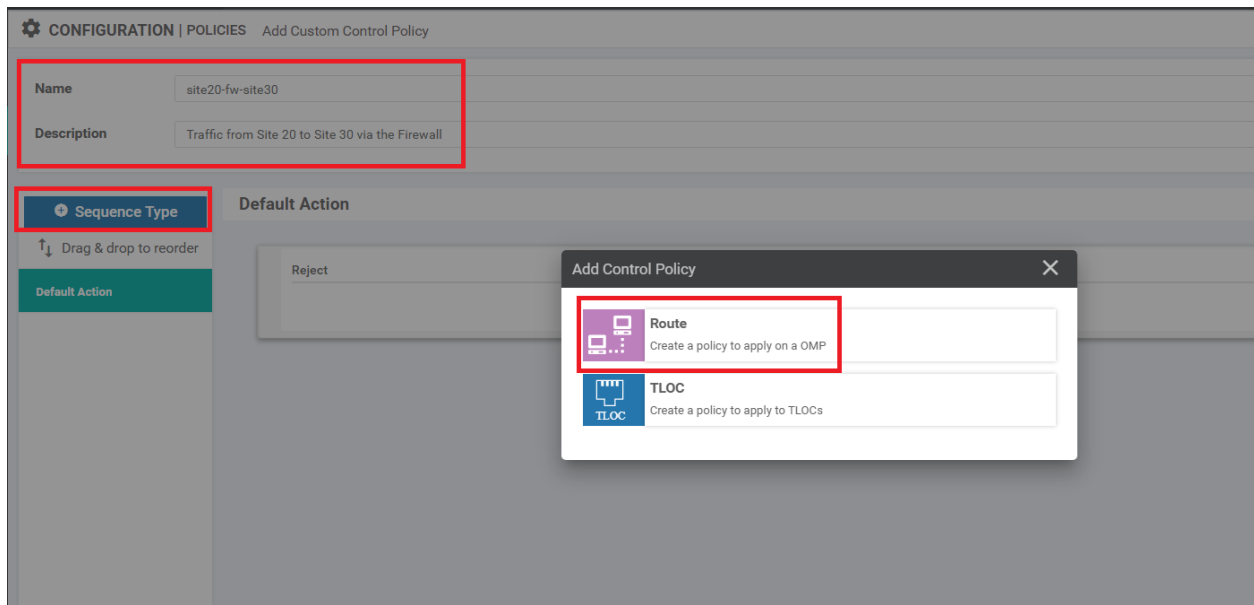
Source IP: 10.30.20.2

Destination IP: 10.20.10.2 or 10.20.10.3

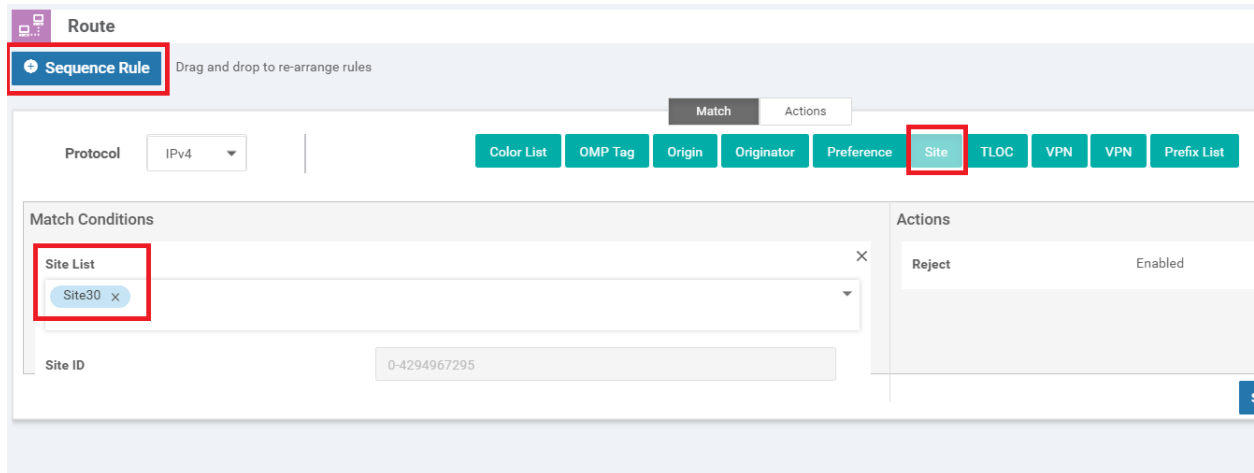
1. On the vManage GUI, go to **Configuration => Policies**. Locate the *Site40-Guest-DIA* policy and click on the three dots next to it. Choose to **Edit** the policy. Make sure you're on the **Topology** tab and click on **Add Topology**. Choose to add a *Custom Control (Route and TLOC)* topology



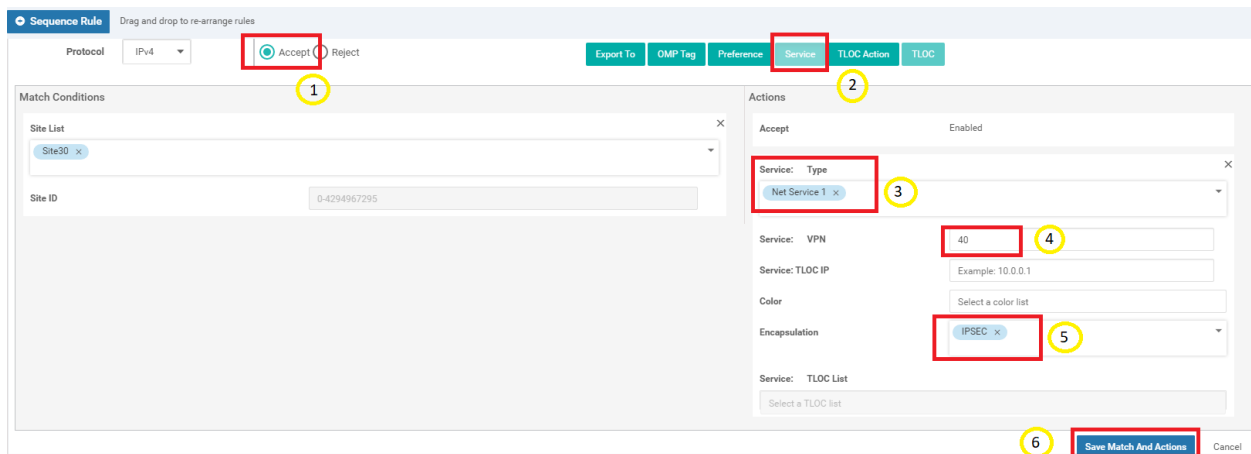
2. Give the Custom Control Policy a **Name** of *site20-fw-site30* and a Description of *Traffic from Site 20 to Site 30 via the Firewall*. Click on **Sequence Type** and choose **Route**



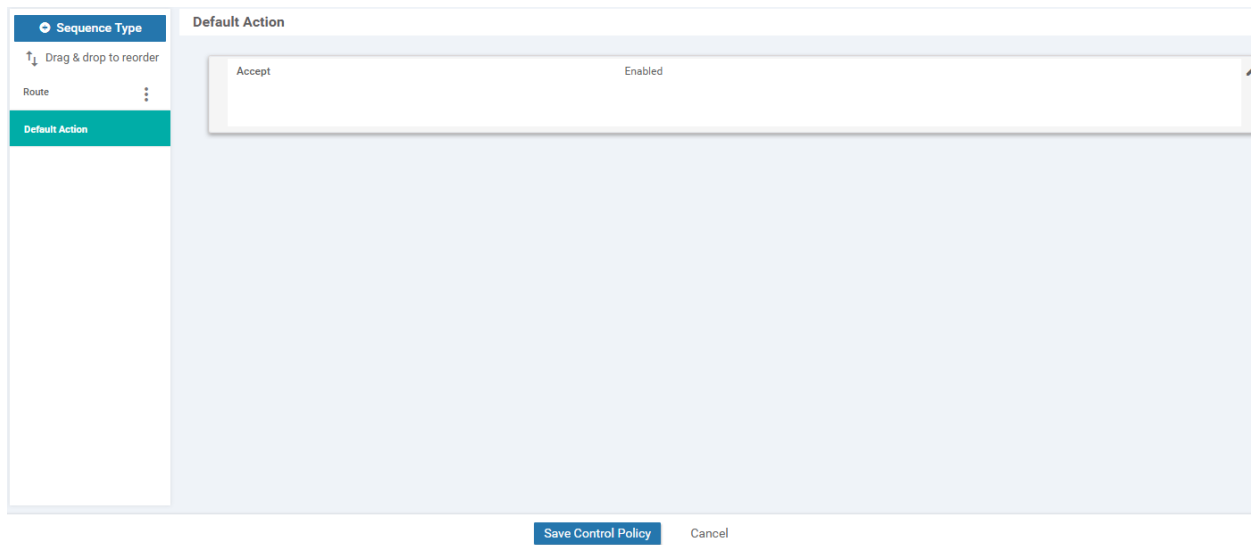
3. Click on **Sequence Rule** and select **Site** for a Match Condition. Click on the **Site List** drop down and choose *Site 30*. Click on the **Actions** tab



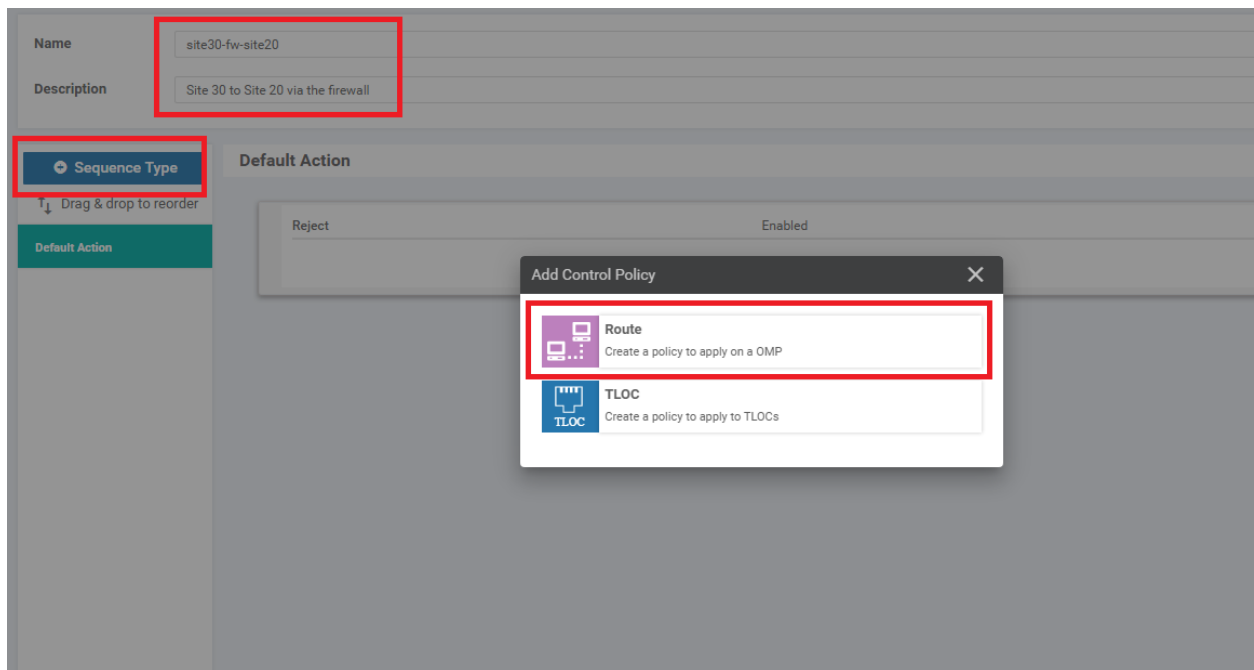
4. Select the **Accept** radio button and choose **Service**. Under Actions select the **Service: Type** as *Net Service 1* and specify a **Service: VPN** of *40*. Select an **Encapsulation** of *IPSEC* and click on **Save Match And Actions** to save this rule



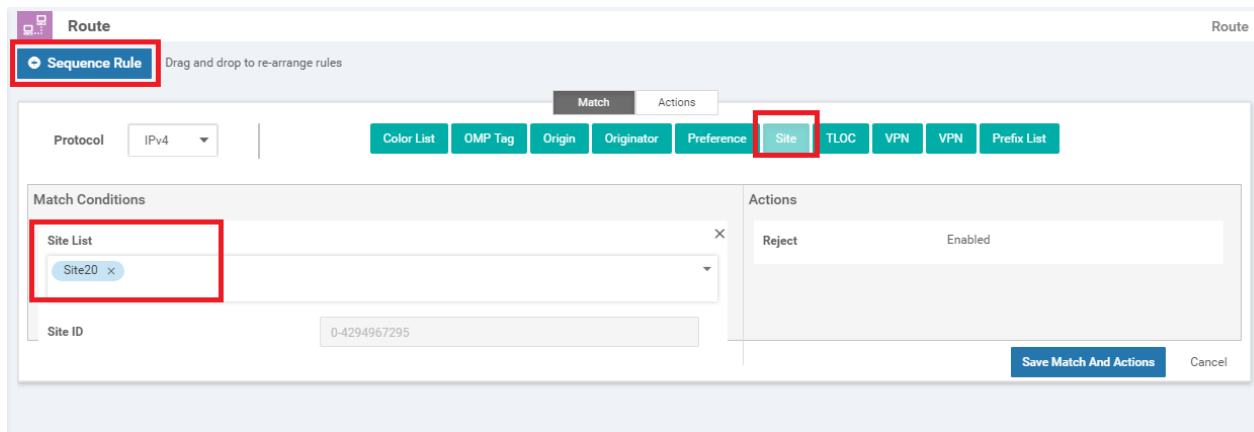
- Click on **Default Action** on the left-hand side and click the pencil icon. Select Accept and then **Save Match And Actions**. The Default Action should change to **Accept Enabled**. Click on **Save Control Policy**



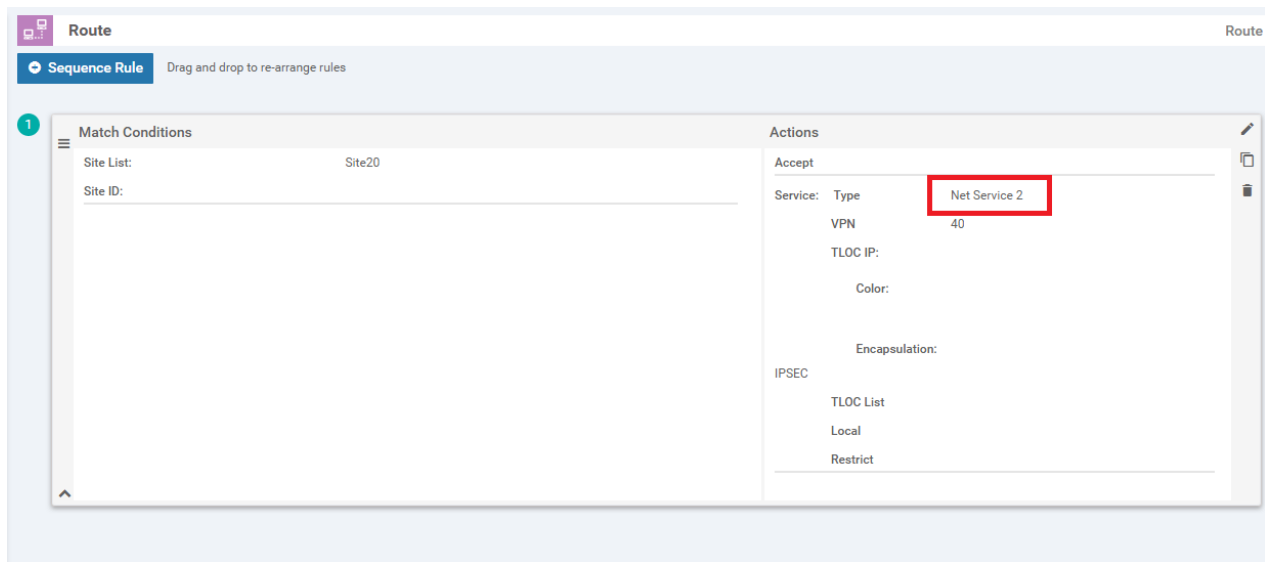
- Make sure you're on the **Topology** tab and click on **Add Topology**. Choose to add a *Custom Control (Route and TLOC)* topology. Give the Custom Control Policy a **Name** of *site30-fw-site20* and a Description of *Site 30 to Site 20 via the firewall*. Click on **Sequence Type** and choose **Route**



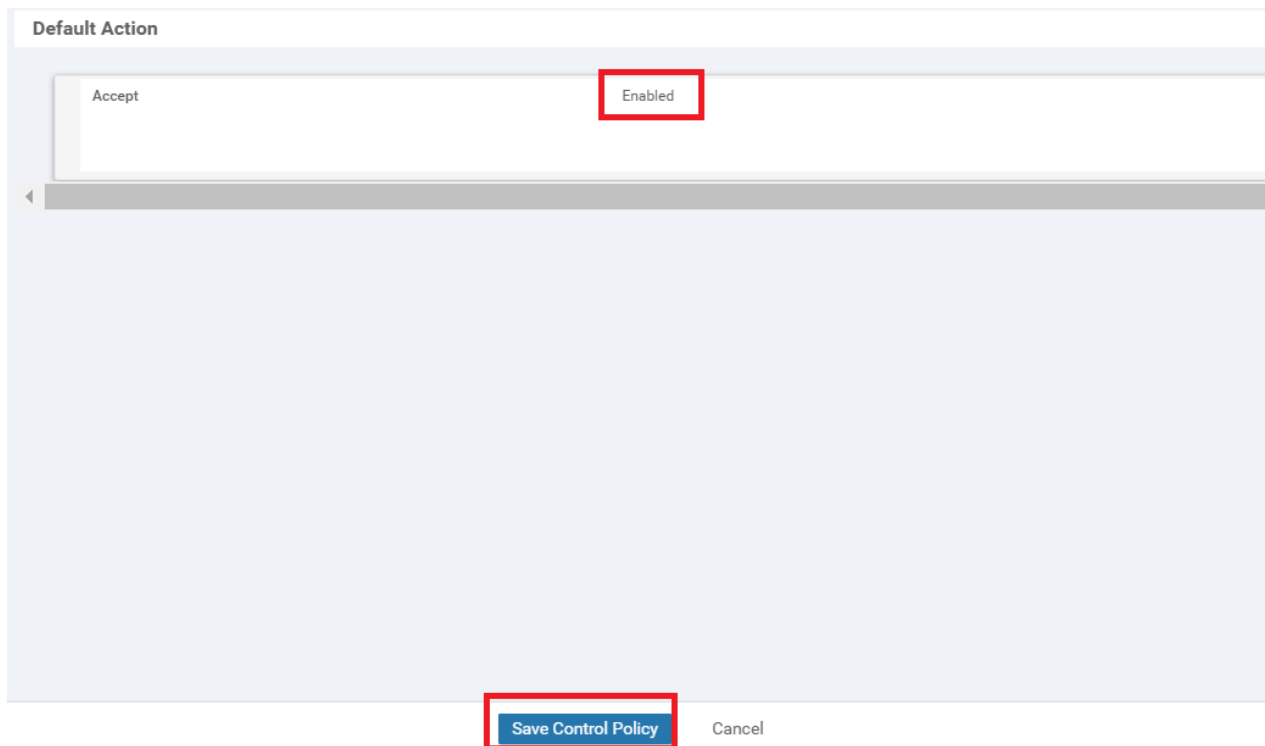
- Click on **Sequence Rule** and then select **Site**. Choose *Site 20* in the **Site List** under **Match Conditions**. Click on **Actions**



- 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





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**





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 configuration interface for two policies. The first policy, *site30-fw-site20*, has a table with the following data:

Direction	Site List	Action
out	Site30	 

The second policy, *site20-fw-site30*, has a table with the following data:

Direction	Site List	Action
out	Site20	 

At the bottom of the interface, there are three buttons: **Preview**, **Save Policy Changes**, 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 in 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**

CONFIGURATION | POLICIES Centralized Policy > Define Lists Custom Options

Select a list type on the left and start creating your groups of interest

Application **New VPN List**

Color

Data Prefix

Policer

Prefix

Site

SLA Class

TLOC

VPN

VPN List Name

Corp_PoS

Add VPN

10.20

Add Cancel

Name	Entries	Reference Count	Updated By	Last Updated	Action
PoS_FW	20, 40	1	admin	20 Jul 2020 3:00:14 PM PDT	
FW	40	0	admin	20 Jul 2020 2:58:21 PM PDT	
PoS	20	2	admin	21 Jun 2020 4:16:01 AM PDT	
Corporate	10	4	admin	21 Jun 2020 4:15:35 AM PDT	
Guest	30	1	admin	21 Jun 2020 4:16:14 AM PDT	
Corp_FW	10, 40	1	admin	20 Jul 2020 2:59:41 PM PDT	

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

Drag & drop to reorder

Default Action

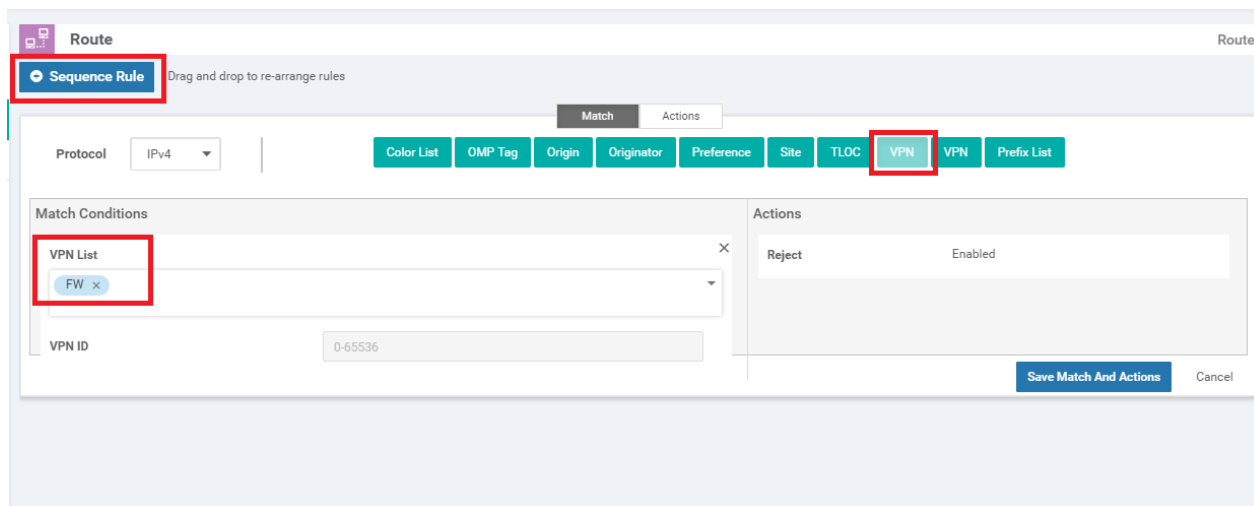
Reject Enabled

Add Control Policy

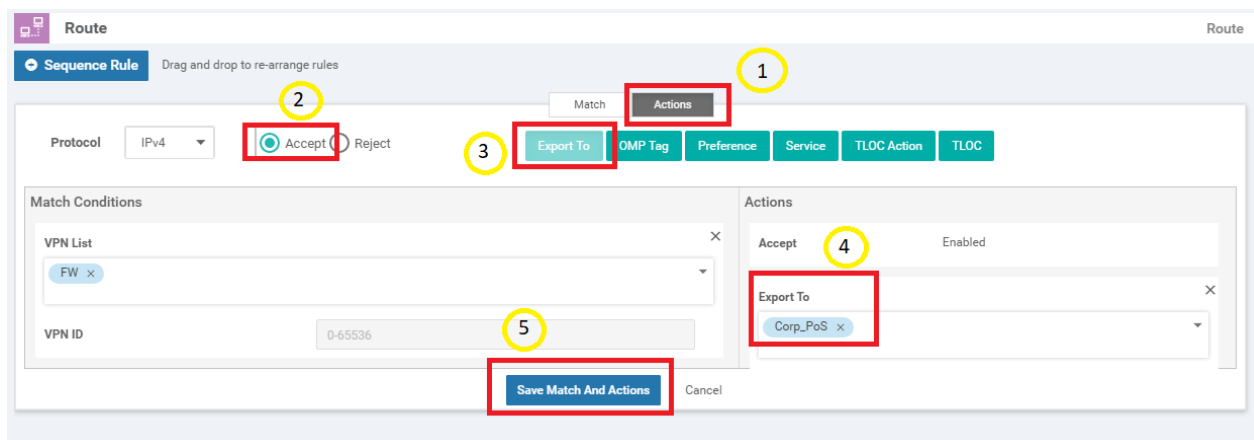
Route
Create a policy to apply on a OMP

TLOC
Create a policy to apply to TLOCs

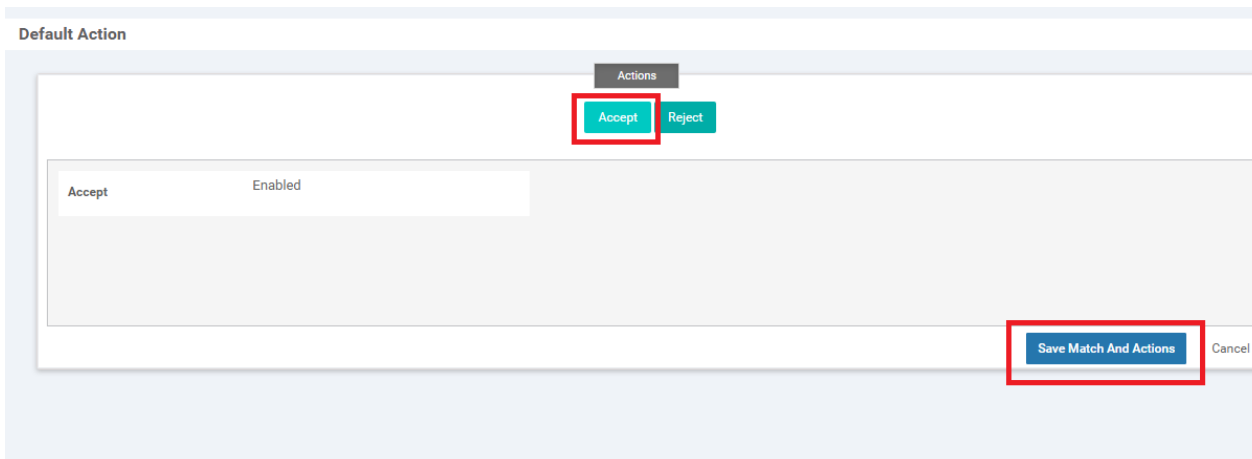
4. Click on **Sequence Rule** and add a **VPN** match. Select *FW* from the **VPN List** drop down



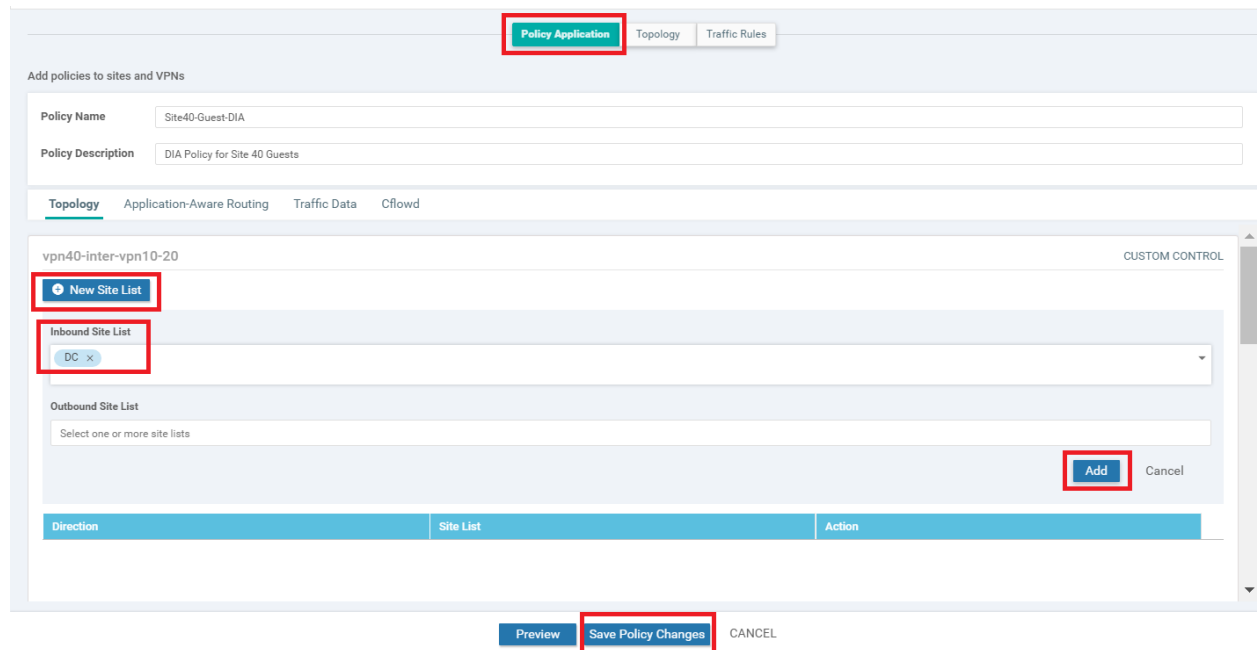
5. Click on the **Actions** tab and select the **Accept** radio button. Click on **Export To** and select *Corp_PoS* from the drop down under Actions. Click on **Save Match And Actions**



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**



- 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



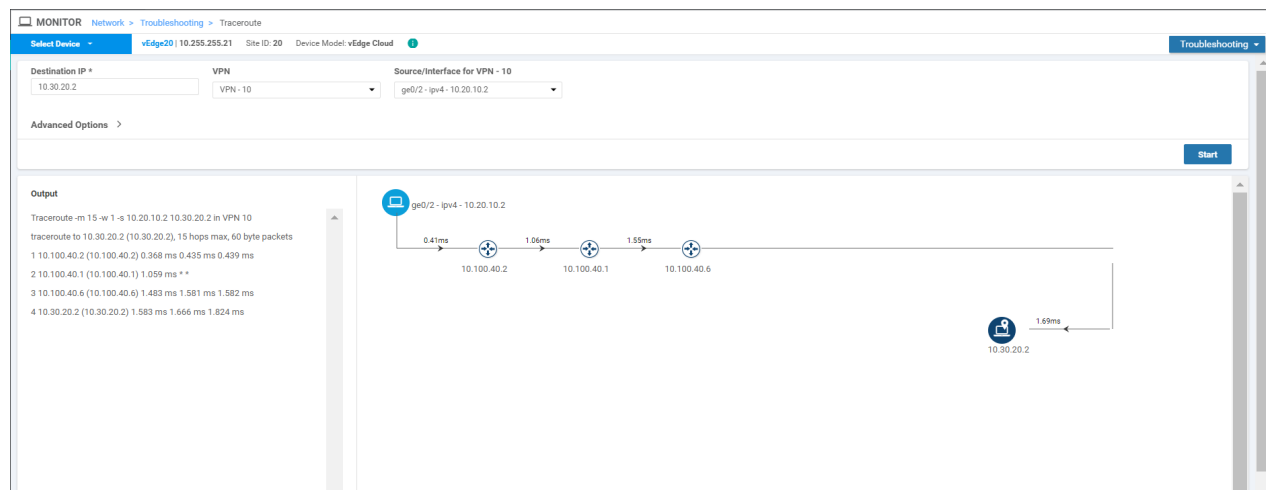
- Head back over to the CLI of vEdge20 and type `ping vpn 10 10.100.40.2`. The pings should now be successful. Type `ping vpn 10 10.100.40.1` to ping the Firewall. This should also work

```

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#

```

- 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.

- 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

The screenshot shows a network monitoring interface with the following configuration and output:

Configuration:
Destination IP: 10.20.10.2
Source/Interface for VPN - 20: ge0/3 - ipv4 - 10.30.20.2

Output:
Traceroute -m 15 -w 1 -s 10.30.20.2 10.20.10.2 in VPN 20
traceroute to 10.20.10.2 (10.20.10.2), 15 hops max, 60 byte packets
1 10.100.40.6 (10.100.40.6) 0.230 ms 0.265 ms 0.269 ms
2 10.100.40.5 (10.100.40.5) 1.079 ms * *
3 10.100.40.2 (10.100.40.2) 1.255 ms 1.326 ms 1.417 ms
4 10.20.10.3 (10.20.10.3) 1.599 ms 1.683 ms 1.684 ms
5 10.20.10.2 (10.20.10.2) 1.597 ms 1.757 ms 1.837 ms

The diagram illustrates the path from the source interface ge0/3 - ipv4 - 10.30.20.2 through hops 10.100.40.6, 10.100.40.5, 10.100.40.2, and 10.20.10.3 to the destination 10.20.10.2.

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 DG-vEdges](#)
- [Configuration Cleanup and Routing Verification](#)
- [Setting up VPN Lists](#)
- [Inter VPN Routing Policies](#)
- [Inter VPN Routing Verification](#)
- [Policies for Service Chaining](#)
- [Activity Verification](#)



Integrating Cisco WAAS with SD-WAN

Summary: Integrating Cisco WAAS with SD-WAN using AppNav-XE

Table of Contents

- [Overview](#)
- [Adding WAAS Nodes to WCM](#)
- [Downloading vManage certs and Enabling DIA at Site DC](#)
- [Integrating vManage and WCM](#)
- [Discovering the AppNav-XE Controllers](#)
- [Setting up the AppNav Clusters](#)
- [Verification and Testing](#)

Task List

- Overview
- Adding WAAS Nodes to WCM
- Downloading vManage certs and Enabling DIA at Site DC
- Integrating vManage and WCM
- Discovering the AppNav-XE Controllers
- Setting up the AppNav Clusters
- Verification and Testing

Overview

Cisco WAAS and SD-WAN can be integrated for traffic interception and redirection to WAAS Nodes for optimization. This brings WAAS capabilities to Cisco IOS-XE SD-WAN by enabling the AppNav-XE feature on compatible devices.

Cisco SD-WAN Devices are configured with AppNav-XE redirection policies and WAAS nodes are configured with optimization policies from WAAS Central Manager (WCM).

The AppNav-XE SD-WAN Device and the WAAS Nodes together form a cluster known as an AppNav-XE cluster.

The WCM registers as a third party controller to vManage.

The components of the WAAS SD-WAN solution are:

- WAAS Central Manager (WCM) - used for centralized management of WAAS Nodes and AppNav-XE on Cisco SD-WAN Devices
- AppNav-XE Service Controller (SC) running on WAN Edges which contain redirection policies
- WAAS Nodes or Service Nodes (SN) which contain optimization policies

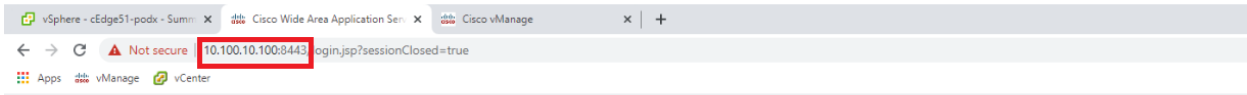
Task List

- [Overview](#)
- [Adding WAAS Nodes to WCM](#)
- [Downloading vManage certs and Enabling DIA at Site DC](#)
- [Integrating vManage and WCM](#)
- [Discovering the AppNav-XE Controllers](#)
- [Setting up the AppNav Clusters](#)
- [Verification and Testing](#)

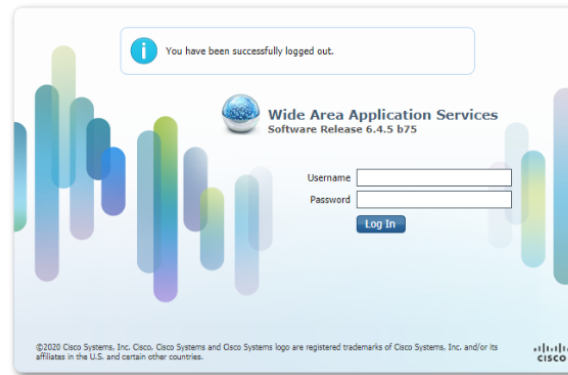
Adding WAAS Nodes to WCM

1. Open the WCM GUI by navigating to the IP Address of WCM (10.100.10.100) or using the bookmark on your Jumphost and entering the credentials as enumerated below

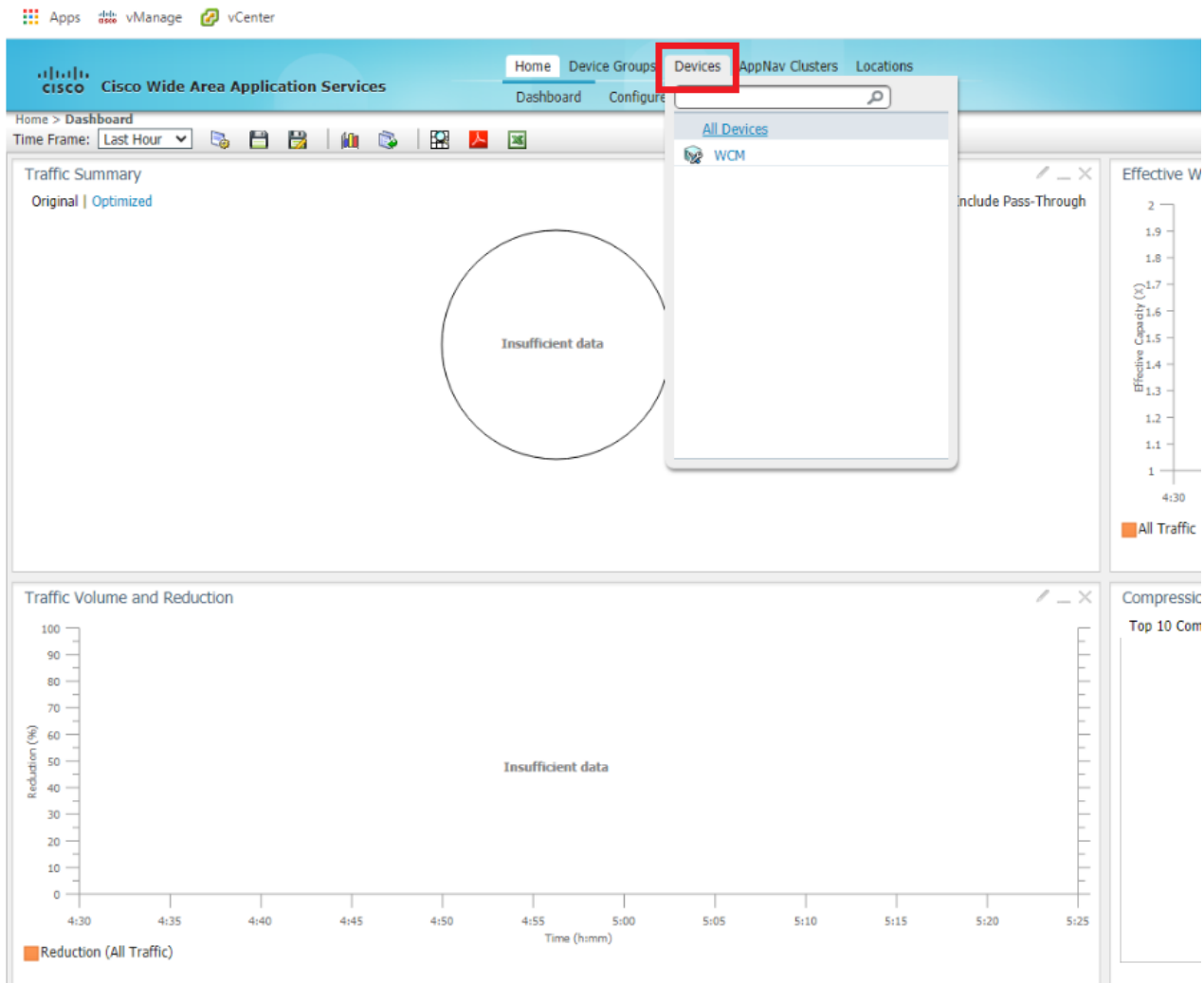
Username	Password
admin	default



Username: admin
Password: default



2. Once logged in, click on **Device** and notice that there aren't any nodes added to WCM as of now. We will be adding the WAAS Nodes to WCM in this section



3. Open vCenter (10.2.1.50/ui or via the bookmark) and log in using the credentials provided for your POD. Locate the *sdwan-ghi-site40waas* VM and click on it. Click on the **Open Console** icon and choose **Web Console** if prompted. Click on **OK**. Initial setup of the WAAS Nodes is done via the CLI

- ghi-vcenter.swat4partners.com
 - SWAT-Labs-GHI
 - Management-Shared Services
 - ghi-ms01.swat4partners.com
 - ghi-ms02.swat4partners.com
 - ghi-ms03.swat4partners.com
 - cEdge40-podx
 - cEdge50-podx
 - cEdge51-podx
 - DC-vEdge1-podx
 - DC-vEdge2-podx
 - sdwan-ghi-ad-podx
 - sdwan-ghi-asa-podx
 - sdwan-ghi-guac-admin
 - sdwan-ghi-guac-podx
 - sdwan-ghi-gw-podx
 - sdwan-ghi-jump-podx
 - sdwan-ghi-site30pc-podx
 - sdwan-ghi-site40waas-podx
 - sdwan-ghi-site50pc-podx
 - sdwan-ghi-site50waas-podx
 - sdwan-ghi-vbond-podx
 - sdwan-ghi-vmanage-podx
 - sdwan-ghi-vsmart-podx
 - sdwan-ghi-vsmart2-podx
 - sdwan-ghi-wcm-podx
 - vEdge20-podx
 - vEdge21-podx
 - vEdge30-podx
- ghi-ms04.swat4partners.com
- GHI-Pod01
- GHI-Pod02

sdwan-ghi-site40waas-podx

Summary Monitor Configure Permissions Datastores Networks Updates

Powered On

Guest OS: Other 2.6.x Linux (64-bit)
Compatibility: ESXi 5.5 and later (VM version 10)
VMware Tools: Not running, version:2147483647 (Guest Managed)
[More info](#)

DNS Name:
IP Addresses:
Host: ghi-ms03.swat4partners.com

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

VM Hardware

Related Objects

Host	ghi-ms03.swat4partners.com
Networks	Site40-VPN10
Storage	ghi-ms03-ds

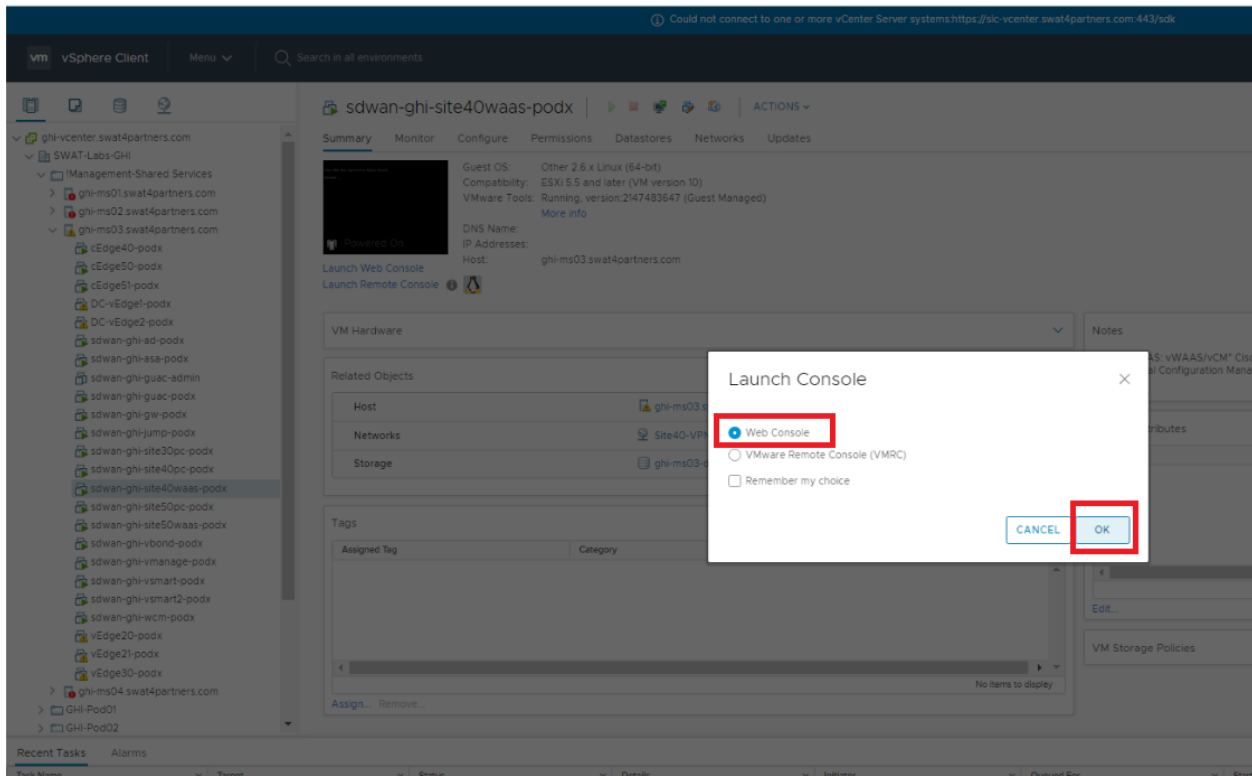
Tags

Assigned Tag	Category	Description
--------------	----------	-------------

[Assign...](#) [Remove...](#)

Recent Tasks Alarms

Task Name	Target	Status	Details	Initiator
Power On virtual machine	sdwan-ghi-site50waas-podx	Completed		SWAT4PARTNERS\echemble
Initialize powering On	SWAT-Labs-GHI	Completed		SWAT4PARTNERS\echemble



4. Enter the username and password as enumerated below to log in to the WAAS Node

Username	Password
admin	default

```
sdwan-ghi-site40waas-podx

Cisco Wide Area Application Engine Console

Username: _
```

Username: admin
Password: default

5. Type **setup** and hit Enter to begin initial setup of the WAAS Node

```
sdwan-ghi-site40waas-podx

Cisco Wide Area Application Engine Console

Username: admin
Password:
System Initialization Finished.
NO-HOSTNAME#setup_
```

6. Press any key to continue

WARNING

Changing any of the network settings from a telnet session may render the device inaccessible on the network. Therefore it is suggested that you have access to the console before modifying the network settings.
** Also, please disable console logging on WAE to avoid screen getting flooded by system messages.
Please press any key to continue ...

7. We will now be presented with a few ways in which the node can be configured. Type *n* to begin configuring all parameters of the WAAS Node. In some of the prompts during this setup, you **don't** need to press Enter for the input to take effect

```
sdwan-ghi-site0waas-podx                                     Enforce US Keybo

Parameter                                                    Default Value
Device Mode                                                  Application Accelerator
1. Interception Method                                       WCCP
2. Time Zone                                                  UTC 0 0
3. Management Interface                                       Virtual 1/0
   Autosense                                                  Disabled
4. DHCP                                                       Enabled
5. IPv6                                                        Disabled

Type n at this point

ESC Quit ? Help _____ WAAS Default Configuration _____
Press 'y' to configure other parameters retaining above defaults, 'n' to
configure all, <1-5> to change specific default [y]:
```

8. At the *Select Interception Method* type 2 to set the interception method to AppNav. This is the only supported interception method in SD-WAN WAAS


```
sdwan-ghi-site40waas-podx

Parameter                               Default Value
Device Mode                             Application Accelerator
1. Interception Method                  WCCP
2. Time Zone                            UTC 0 0
3. Management Interface                  Virtual 1/0
   Autosense                            Disabled
4. DHCP                                 Enabled
5. IPv6                                  Disabled

ESC Quit ? Help _____ WAAS Default Configuration _____
1. WCCP
2. AppNav Controller
3. UPATH
4. Other
Select Interception Method [1]: _ Type 2
```

9. Hit **Enter** at the *Enter Time Zone* prompt to choose the default time zone of UTC

```
sdwan-ghi-site40waas-podx

Parameter                               Configured Value
Device Mode                             Application Accelerator
1. Interception Method                  AppNav Controller
2. Time Zone                            UTC 0 0
3. Management Interface                  Virtual 1/0
   Autosense                            Disabled
4. DHCP                                 Enabled
5. IPv6                                  Disabled

ESC Quit ? Help _____ WAAS Default Configuration _____
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)> [UTC 0 0]:
```

10. Hit **Enter** at the *Select Management Interface* prompt to select *Virtual 1/0* as the management interface

Parameter	Configured Value
Device Mode	Application Accelerator
1. Interception Method	AppNav Controller
2. Time Zone	UTC 0 0
3. Management Interface	Virtual 1/0
Autosense	Disabled
4. DHCP	Enabled
5. IPv6	Disabled

```
ESC Quit ? Help _____ WAAS Default Configuration _____
No.      Interface Name      IP Address      Network Mask
1.       Virtual 1/0         dhcp
2.       Virtual 2/0         dhcp
Select Management Interface [1]: _
```

11. Type *n* at the *Enable DHCP for Management Interface* to disable DHCP on the selected management interface. We will be entering an IP Address manually

```
sdwan-ghi-site40waas-podx                                     Enforce US Keyboard L1

Parameter              Configured Value
Device Mode            Application Accelerator
1. Interception Method AppNav Controller
2. Time Zone           UTC 0 0
3. Management Interface Virtual 1/0
   Autosense           Disabled
4. DHCP                Enabled
5. IPv6                Disabled

ESC Quit ? Help _____ WAAS Default Configuration _____
Enable DHCP for Management Interface? (y/n)[y]: _ Type n
```

12. Hit **Enter** at the *Enable IPv6 on Device* prompt such that IPv6 is not enabled

```
sdwan-ghi-site40waas-podx

Parameter              Configured Value
Device Mode            Application Accelerator
1. Interception Method AppNav Controller
2. Time Zone           UTC 0 0
3. Management Interface Virtual 1/0
   Autosense           Disabled
4. DHCP                Disabled
5. IPv6                Disabled

ESC Quit ? Help _____ WAAS Default Configuration _____
Enable IPv6 on Device?(y/n)[n]: _
```

13. Type an IP Address of *10.40.10.101/24* and hit **Enter**

```
sdwan-ghi-site40waas-podx                                     Enforce US Keyboard Layout

Parameter              Configured Value
Device Mode            Application Accelerator
1. Interception Method AppNav Controller
2. Time Zone           UTC 0 0
3. Management Interface Virtual 1/0
   Autosense           Disabled
4. DHCP                Disabled
5.   IPv6              Disabled
   Speed               1000(full-duplex)
6.   IP Address

ESC Quit ? Help _____ WAAS Remaining Configuration _____
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]: 10.40.10.101/24_
```

14. Type a Default Gateway address of *10.40.10.2* and hit **Enter**

```
sdwan-ghi-site40waas-podx                                     Enter

Parameter              Configured Value
Device Mode            Application Accelerator
1. Interception Method AppNav Controller
2. Time Zone           UTC 0 0
3. Management Interface Virtual 1/0
   Autosense           Disabled
4. DHCP                Disabled
5.   IPv6              Disabled
   Speed               1000(full-duplex)
6.   IP Address        10.40.10.101
7.   IP Network Mask   255.255.255.0
8.   IP Default Gateway Not Configured

ESC Quit ? Help _____ WAAS Remaining Configuration _____
Enter Default Gateway IP Address [Not configured]: 10.40.10.2_
```

15. Type *10.100.10.100* at the *Enter Central Manager IP Address* prompt and hit **Enter**

```
sdwan-ghi-site40waas-podx Enforce US Keyboard Layout View Fullscreen

Parameter                Configured Value
Device Mode              Application Accelerator
1. Interception Method   AppNav Controller
2. Time Zone             UTC 0 0
3. Management Interface  Virtual 1/0
   Autosense             Disabled
4. DHCP                  Disabled
5.   IPv6                Disabled
   Speed                 1000(full-duplex)
6.   IP Address          10.40.10.101
7.   IP Network Mask    255.255.255.0
8. IP Default Gateway    10.40.10.2
9. CM IP Address

ESC Quit ? Help _____ WAAS Remaining Configuration _____
Enter Central Manager IP Address (WARNING: An invalid entry will cause SETUP to
take a long time when applying WAAS configuration) [None]: 10.100.10.100_
```

16. Hit **Enter** at the *Enter Domain Name Server IP Address* prompt. We will not be using DNS

```
sdwan-ghi-site40waas-podx Enforce

Parameter                Configured Value
Device Mode              Application Accelerator
1. Interception Method   AppNav Controller
2. Time Zone             UTC 0 0
3. Management Interface  Virtual 1/0
   Autosense             Disabled
4. DHCP                  Disabled
5.   IPv6                Disabled
   Speed                 1000(full-duplex)
6.   IP Address          10.40.10.101
7.   IP Network Mask    255.255.255.0
8. IP Default Gateway    10.40.10.2
9. CM IP Address         10.100.10.100
10. DNS IP Address

ESC Quit ? Help _____ WAAS Remaining Configuration _____
Enter Domain Name Server IP Address [Not configured]:
```

17. Type *swatsdwanlab.com* at the *Enter Domain Name(s)* prompt and hit **Enter**

```

Parameter                               Configured Value
Device Mode                             Application Accelerator
1. Interception Method                   AppNav Controller
2. Time Zone                             UTC 0 0
3. Management Interface                   Virtual 1/0
   Autosense                             Disabled
4. DHCP                                  Disabled
5. IPv6                                  Disabled
   Speed                                  1000(full-duplex)
6. IP Address                             10.40.10.101
7. IP Network Mask                       255.255.255.0
8. IP Default Gateway                     10.40.10.2
9. CM IP Address                          10.100.10.100
10. DNS IP Address                        None
11. Domain Name(s)

[ESC] Quit [?] Help _____ WAAS Remaining Configuration _____
Enter Domain Name(s) (Not configured): swatsdwanlab.com

```

18. Type *Site40-WaaS* as the Hostname and hit **Enter**

```

Parameter                               Configured Value
Device Mode                             Application Accelerator
1. Interception Method                   AppNav Controller
2. Time Zone                             UTC 0 0
3. Management Interface                   Virtual 1/0
   Autosense                             Disabled
4. DHCP                                  Disabled
5. IPv6                                  Disabled
   Speed                                  1000(full-duplex)
6. IP Address                             10.40.10.101
7. IP Network Mask                       255.255.255.0
8. IP Default Gateway                     10.40.10.2
9. CM IP Address                          10.100.10.100
10. DNS IP Address                        None
11. Domain Name(s)                       swatsdwanlab.com
12. Host Name

[ESC] Quit [?] Help _____ WAAS Remaining Configuration _____
Enter Host Name (None): Site40-WaaS_

```

19. Hit **Enter** when asked about the license to accept the default of Enterprise Licenses

Parameter	Configured Value
2. Time Zone	UTC 0 0
3. Management Interface	Virtual 1/0
Autosense	Disabled
4. DHCP	Disabled
5. IPv6	Disabled
Speed	1000(full-duplex)
6. IP Address	10.40.10.101
7. IP Network Mask	255.255.255.0
8. IP Default Gateway	10.40.10.2
9. CM IP Address	10.100.10.100
10. DNS IP Address	None
11. Domain Name(s)	swatsdwanlab.com
12. Host Name	Site40-WaaS
13. NTP Server Address	None
14. License	

ESC Quit ? Help _____ WAAS Remaining Configuration _____

The product supports the following licenses:

1. Transport
2. Enterprise

Enter the license(s) you purchased [2]: _

20. Hit **Enter** to implement the configuration changes

Parameter	Configured Value
2. Time Zone	UTC 0 0
3. Management Interface	Virtual 1/0
Autosense	Disabled
4. DHCP	Disabled
5. IPv6	Disabled
Speed	1000(full-duplex)
6. IP Address	10.40.10.101
7. IP Network Mask	255.255.255.0
8. IP Default Gateway	10.40.10.2
9. CM IP Address	10.100.10.100
10. DNS IP Address	None
11. Domain Name(s)	swatsdwanlab.com
12. Host Name	Site40-WaaS
13. NTP Server Address	None
14. License	Enterprise

ESC Quit ? Help ? CLI _____ WAAS Final Configuration _____

Press 'y' to implement above configured parameters, <F2> to see all configuration, 'd' to toggle defaults display, <1-14> to change specific parameter [y]:

21. Hit **Enter** again

```
Parameter                Configured Value
2. Time Zone              UTC 0 0
3. Management Interface  Virtual 1/0
   Autosense              Disabled
4. DHCP                  Disabled
5.   IPv6                Disabled
   Speed                 1000(full-duplex)
6.   IP Address          10.40.10.101
7.   IP Network Mask    255.255.255.0
8. IP Default Gateway    10.40.10.2
9. CM IP Address         10.100.10.100
10. DNS IP Address       None
11. Domain Name(s)      swatsdwanlab.com
12. Host Name            Site40-WaaS
13. NTP Server Address   None
14. License              Enterprise
ESC Quit ? Help ? CLI _____ WAAS Final Configuration _____
Service Node specific configurations must be performed using Central Manager
.....
Please press ENTER to continue ... _
```

22. Once the connectivity check to WCM passes, hit **Enter** to skip running diagnostics

```
sdwan-ghi-site40waas-podx

Parameter                Configured Value
2. Time Zone              UTC 0 0
3. Management Interface  Virtual 1/0
   Autosense              Disabled
4. DHCP                  Disabled
5.   IPv6                Disabled
   Speed                 1000(full-duplex)
6.   IP Address          10.40.10.101
7.   IP Network Mask    255.255.255.0
8. IP Default Gateway    10.40.10.2
9. CM IP Address         10.100.10.100
10. DNS IP Address       None
11. Domain Name(s)      swatsdwanlab.com
12. Host Name            Site40-WaaS
13. NTP Server Address   None
14. License              Enterprise
ESC Quit ? Help ? CLI _____ WAAS Final Configuration _____
Testing Central-Manager reachability ...
```



```
Want to run Diagnostics(y/n)? [n]_
```

23. Repeat from Step 3 for the *sdwan-ghi-site50waas* node, making necessary changes to the Hostname and IP Address/Default Gateway. All other parameters remain the same. Reference the image given below

```
sdwan-ghi-site50waas-podx Enforce US Keyboard Layout
```

Parameter	Configured Value
2. Time Zone	UTC 0 0
3. Management Interface	Virtual 1/0
Autosense	Disabled
4. DHCP	Disabled
5. IPv6	Disabled
Speed	1000(full-duplex)
6. IP Address	10.50.10.101
7. IP Network Mask	255.255.255.0
8. IP Default Gateway	10.50.10.2
9. CM IP Address	10.100.10.100
10. DNS IP Address	None
11. Domain Name(s)	swatsdwanlab.com
12. Host Name	Site50-WaaS
13. NTP Server Address	None
14. License	Enterprise

```
ESC Quit ? Help ? CLI WAAS Final Configuration  
Service Node specific configurations must be performed using Central Manager  
.....  
Please press ENTER to continue ...
```

24. Log in to WCM and navigate to **Devices** - you should see the two WAAS Nodes we just configured on WCM



You have been logged out due to inactivity.



Wide Area Application Services

Software Release 6.4.5 b75

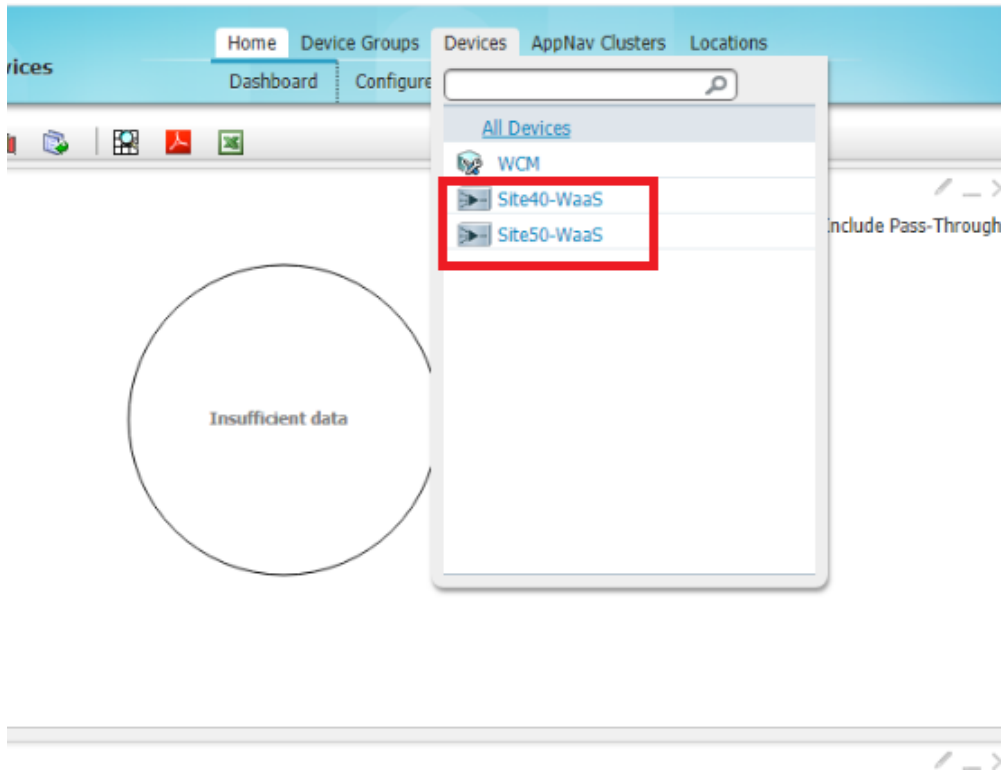
Username

Password

[Log In](#)

©2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.





25. If you click on **All Devices**, you will see the *Site40-WaaS* and *Site50-WaaS* nodes in an online state. If there are alarms for the Device Status, it's OK since Core Dump files are generated sometimes


Devices > All Devices

Advanced Search | Export Table | View All Devices | Refresh Table | Activate all inactive Devices | Print Table

Filter: Device Name Match if: contains Go Clear Filter

Device Name	Services	IP Address	Management Status	Device Status	Location	Software Version	Device Type
Site40-WaaS	Application Accelerator	10.40.10.101	Online	●●●●	Site40-WaaS-location	6.4.5	OE-VWAAS-ESX
Site50-WaaS	Application Accelerator	10.50.10.101	Online	●●●●	Site50-WaaS-location	6.4.5	OE-VWAAS-ESX
WCM	CM (Primary)	10.100.10.100	Online	●●●●		6.4.5	OE-VWAAS-ESX

26. While on the Home page, click on **Devices => Site40-WaaS**. You will see a *WAAS-GLOBAL* optimization policy attached to it under *Configuration Details*. This is the default policy that is attached to all new WAAS Nodes


Cisco Wide Area Application Services
Home Device Groups De

Site40-WaaS | Config

Devices > Site40-WaaS > Dashboard

Time Frame: Last Hour

Device Info

Memory:	3096MB
Device ID:	00:50:56:aa:f7:2f
RAID Level:	None
Disk Encryption:	Disabled
Local Disks:	1/1

▼ Configuration Details


Assignments:	1 Device Group(s)
AppNav Cluster:	waas/1
WAAS Node:	Yes
Gateway:	10.40.10.2
License Type:	Perpetual
License Status:	Enterprise
Optimization Policy:	WAAS-GLOBAL (204 Optimization Policy Rules)
Interception:	AppNav Controller

27. Navigate to *Device Groups* => *AllWAASGroup* on the WCM GUI and there will be a check box *Automatically assign all newly activated devices to this group* which assigns the WAAS Node to this group and hence the WAAS-GLOBAL policy

Home Device Groups Devices AppNav Clusters





Site40

- All Device Groups
- AllWAASExpressGroup
- AllWAASGroup**

 Cisco Wide Area Application Services

Home Device Groups Devices AppNav Cluster
AllWAASGroup | Configure | Monitor |

Device Groups > AllWAASGroup > Device Group Home

Modifying Device Group, AllWAASGroup  Delete  Request Full Update  Reboot  Force Group Settings

Name: *

Automatically assign all newly activated devices to this group

▶ Pages configured for this device group

▶ Select pages to hide from table of contents of this device group

Note: * - Required Field

28. To view the settings of the WAAS-GLOBAL policy, navigate to **Configure => Optimization Policies**. In the WAAS-GLOBAL policy, click on **Restore Default** to view the policies

Cisco Wide Area Application Services

Home | Device Groups | Devices | AppNav Clusters | Locations

AllWAASGroup | Configure | Monitor | Admin

Device Groups > AllWAASGroup > Device Group Home

Modifying Device Group, AllWAASGroup [Delete] [Request Full Update] [Reboot]

Name: * AllWAASGroup

Automatically assign all newly activated devices to this group

Pages configured for this device group

Select pages to hide from table of contents of this device group

Baseline group for all WAAS Services

Note: * - Required Field

- Acceleration
 - Enabled Features
 - Accelerator Threshold
 - TCP Settings
 - TCP Adaptive Buffering Settings
 - DRE Settings
 - HTTP/HTTPS Settings
 - Video Settings
 - SMB Settings
 - SMB Preposition Settings
 - MAPI Settings
 - ICA Settings
 - Optimization Class-Map
 - Optimization Policies
 - SSL Accelerated Services
- File Services
 - SMB Dynamic Shares
- Caching
 - Akamai Conne
- Storage
 - Disk Error Har
 - Disk Encryptio
 - Extended Obj
 - Cache Size Ma
- Security
 - Secure Store
 - Windows Dom
 - SSL
 - Peering Servic
 - Management
 - AAA

Cisco Wide Area Application Services

Device Groups > AllWAASGroup > Configure > Acceleration > Optimization Policies

Print Refresh Restore Default

Current applied settings from Device Group, AllWAASGroup

Name: * WAAS-GLOBAL

Description:

Enable Service Policy

DSCP: copy

Submit Reset

Optimization Policy Rules for "WAAS-GLOBAL"

- Wait for a few seconds and click on **Refresh**. The policies should now show up. These are the default optimization policies being applied to the WAAS Nodes

Home Device Groups Devices AppNav Clusters Locations

AIWASGroup | Configure | Monitor | Admin

Device Groups > AIWASGroup > Configure > Acceleration > Optimization Policies

Print Refresh Restore Default

Current applied settings from Device Group, AIWASGroup

Name: WAAS-GLOBAL

Description:

Enable Service Policy

DSCP: copy

Submit Reset

Optimization Policy Rules for "WAAS-GLOBAL"

Add Policy Rule Insert Edit Delete Move to Save Moved Rows

Position	Class-Map	Source IP	Destination IP	Source Ports	Destination Po...	Protocol	Application	Action	Accelerate
<input type="checkbox"/>	1					mapi	Email-and-Mes...	TFO with DRE Bidirectional and LZ	MAPI Adaptor
<input type="checkbox"/>	2					ms-ad-rep	Replication	TFO with DRE Bidirectional and LZ	None
<input type="checkbox"/>	3					ms-exch-nspl	Email-and-Mes...	Passthrough	None
<input type="checkbox"/>	4					ms-frf	Email-and-Mes...	Passthrough	None
<input type="checkbox"/>	5					ms-frs	Replication	TFO with DRE Bidirectional and LZ	None
<input type="checkbox"/>	6					ms-sql	SQL	TFO with DRE Bidirectional and LZ	None
<input type="checkbox"/>	7					ms-frsapi	Replication	TFO with DRE Bidirectional and LZ	None
<input type="checkbox"/>	8					netlogon	Authentication	Passthrough	None
<input type="checkbox"/>	9			522 1503 1731			Conferencing	Passthrough	None
<input type="checkbox"/>	10			2492			Enterprise-Ap...	TFO Only	None
<input type="checkbox"/>	11			1184			Remote-Desktop	TFO Only	None
<input type="checkbox"/>	12			443			SSL	TFO Only	None
<input type="checkbox"/>	13			80 3128 8000 8080 8088			Web	TFO with DRE Bidirectional and LZ	HTTP Adaptor
<input type="checkbox"/>	14			7000 - 7009			File-System	TFO with DRE Bidirectional and LZ	None
<input type="checkbox"/>	15			1680			Remote-Desktop	Passthrough	None
<input type="checkbox"/>	16			10080			Backup	TFO Only	None
<input type="checkbox"/>	17			5190 - 5193			Instant-Messa...	Passthrough	None

This completes the addition and verification of WAAS Nodes on WCM.

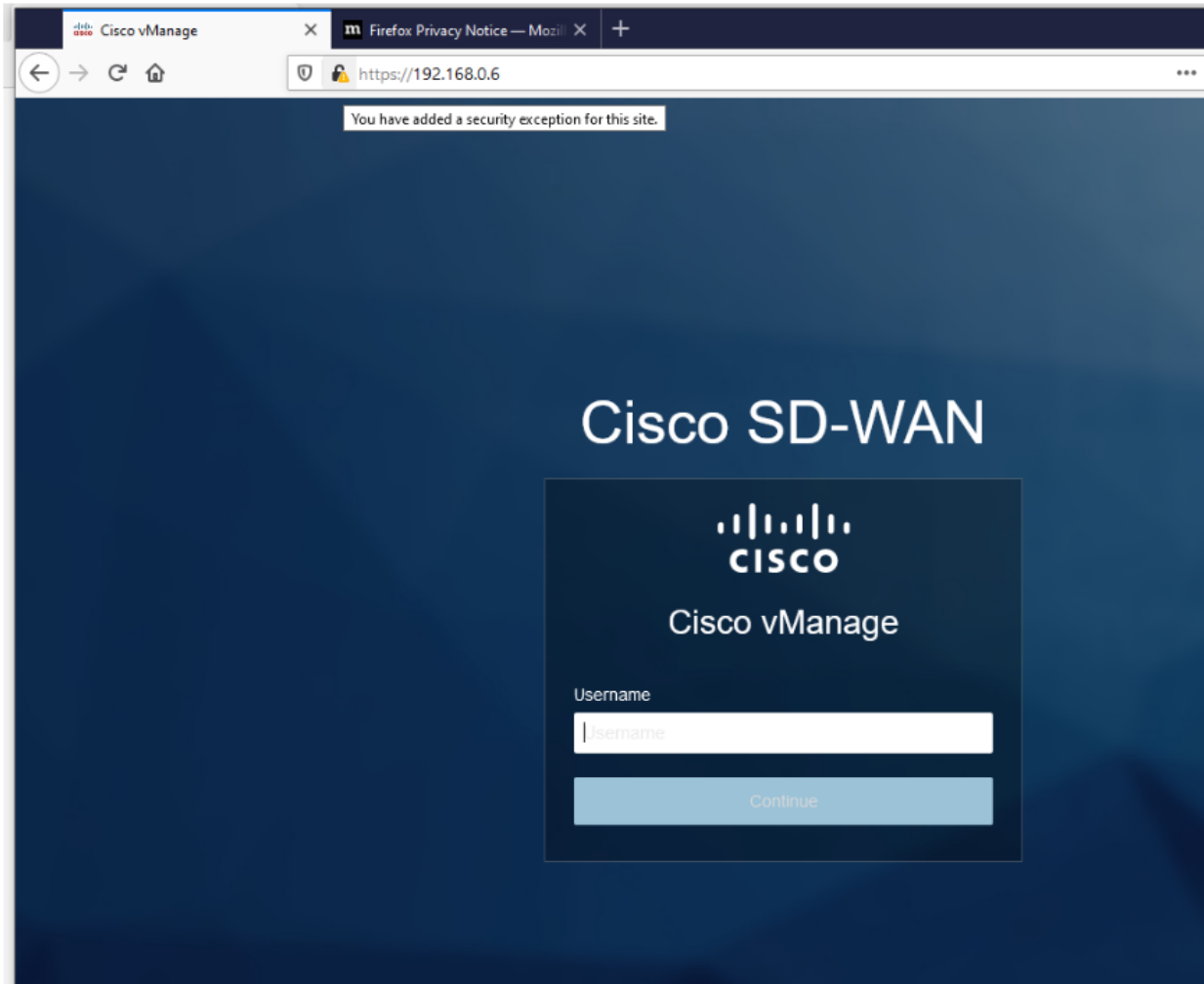
Task List

- [Overview](#)
- [Adding WAAS Nodes to WCM](#)
- [Downloading vManage certs and Enabling DIA at Site DC](#)
- [Integrating vManage and WCM](#)
- [Discovering the AppNav-XE Controllers](#)
- [Setting up the AppNav Clusters](#)
- [Verification and Testing](#)

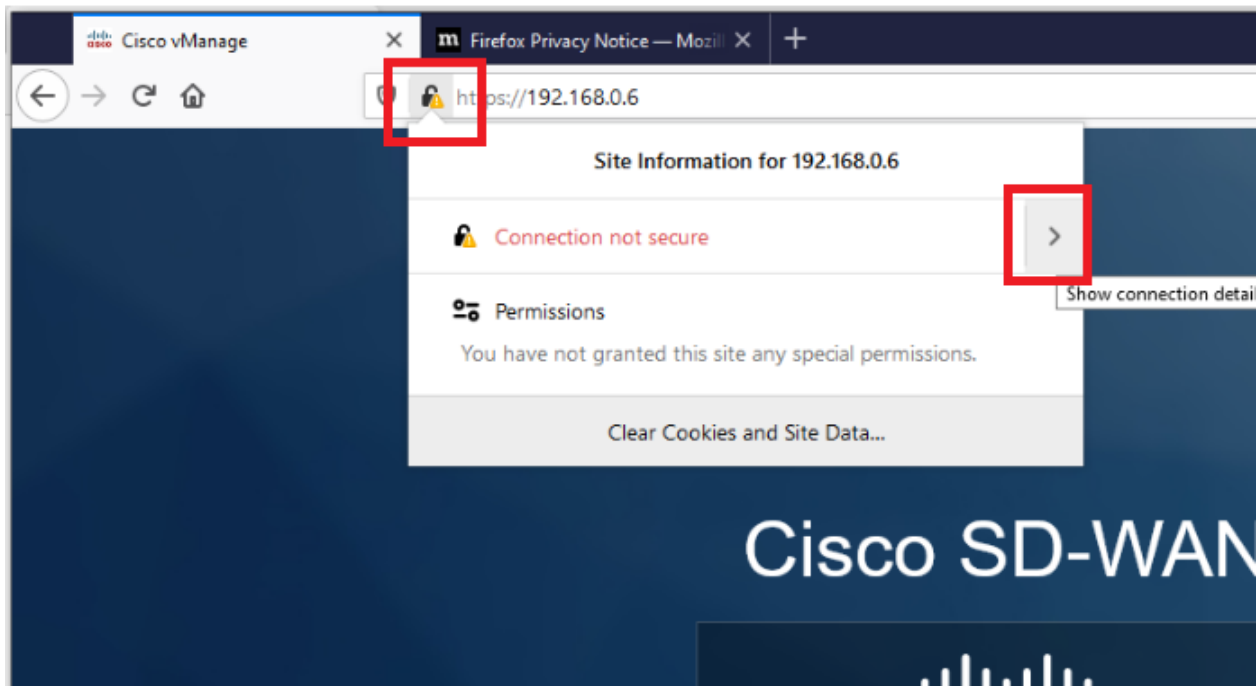
Downloading vManage certs and Enabling DIA at Site DC

Go through the following steps in order to prepare for adding the AppNav-XE controllers on WCM.

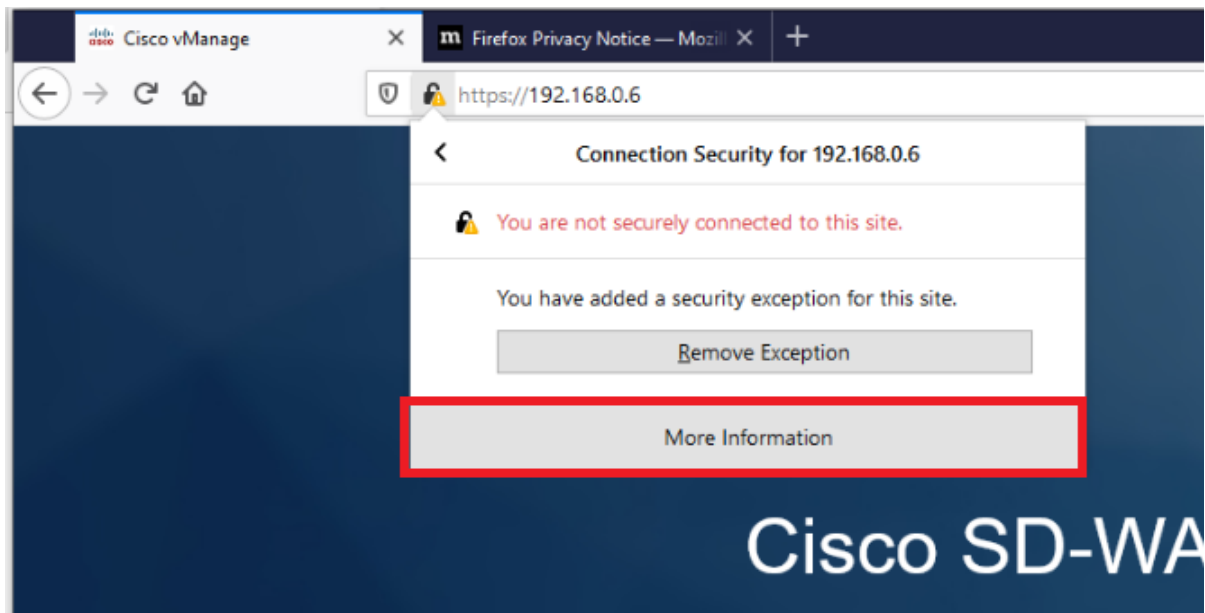
1. Open Firefox and navigate to the vManage GUI (<https://192.168.0.6>). We are using Firefox over here since the vManage web certs need to be downloaded. Accept any warnings that you receive



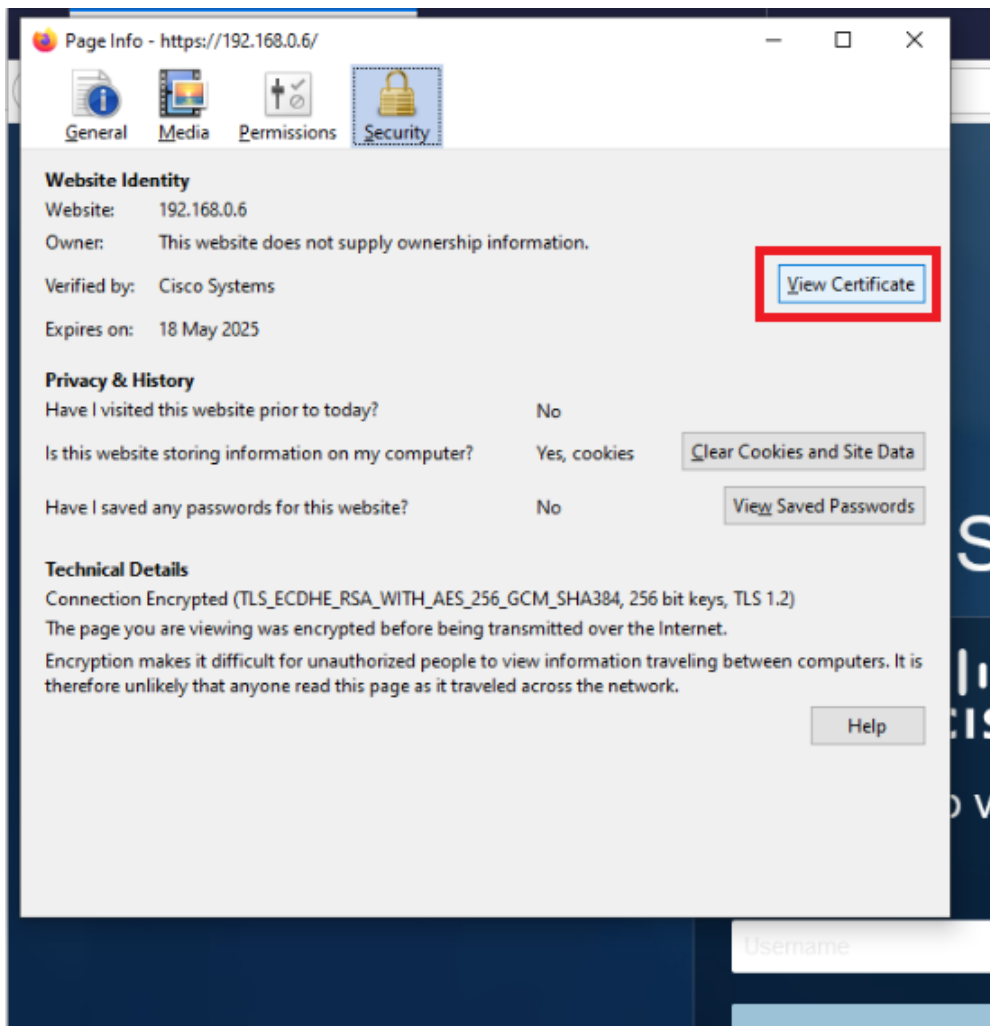
2. Click on the lock icon in the address bar and expand *Connection not secure*



3. Click on **More Information**



4. Click on **View Certificate**



5. Click on **PEM (cert)** to download the *vmange.pem* certificate. Choose to Save the File to the default location, which is the *Downloads* folder

Common Name vmanage

Issuer Name _____

Country US

State/Province CA

Locality San Jose

Organization Cisco Systems

Organizational Unit Cisco SDWAN

Common Name vmanage

Validity _____

Not Before 5/19/2020, 5:01:37 PM (Pacific Daylight Time)

Not After 5/18/2025, 5:01:37 PM (Pacific Daylight Time)

Public Key Info _____

Algorithm RSA

Key Size 2048

Exponent 65537

Modulus ED:86:98:EE:0F:68:60:43:8D:1D:4D:FA:26:C1:A6:0F:A1:AE:5A:CB:54:3B:FF:37:04:3D:26:6A:11:5F:A4:A3:C

Miscellaneous _____

Serial Number 63:A3:7C:AF

Signature Algorithm SHA-256 with RSA Encryption

Version 3

Download [PEM \(cert\)](#) [PEM \(chain\)](#)

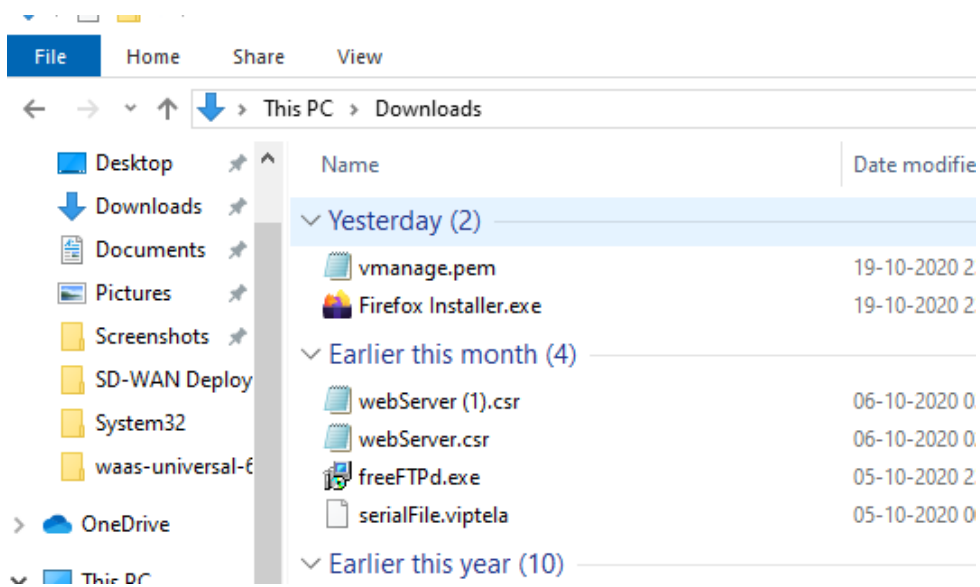
Fingerprints _____

SHA-256 B7:6F:50:DB:B8:93:B6:CF:59:C4:46:C0:59:40:A5:2F:EA:FB:CF:F3:A3:D1:43:BE:C8:9D:FE:4A:6E:D0:05:3F

SHA-1 40:B4:4E:88:7A:53:42:A8:C3:98:73:EC:7F:E4:B8:B7:51:C7:14:AD

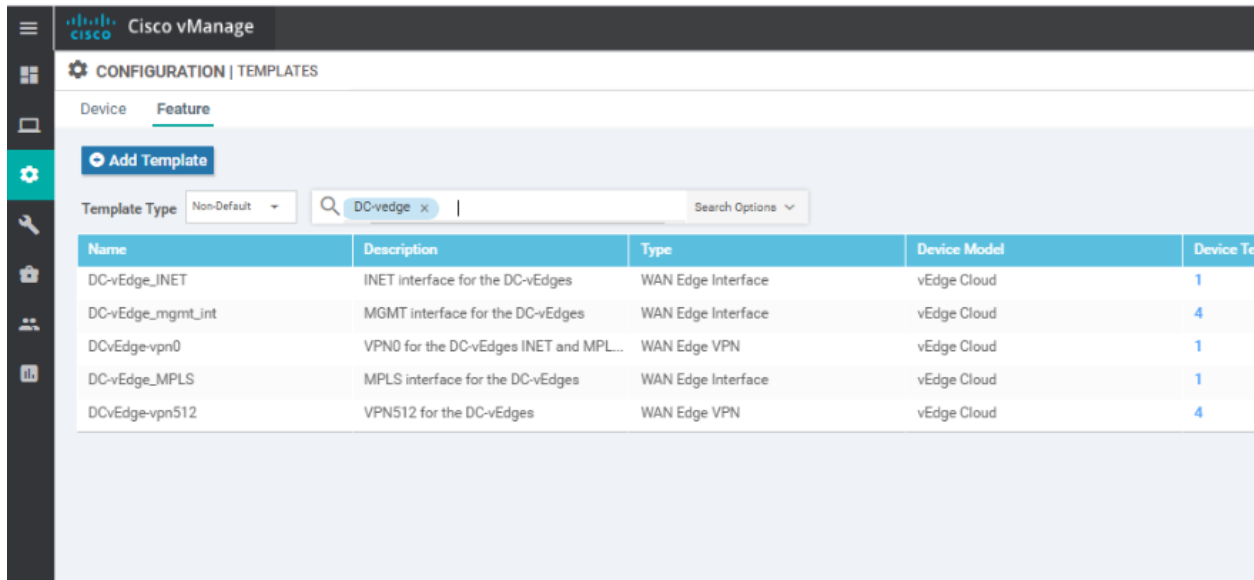
Basic Constraints _____

Certificate Authority Yes

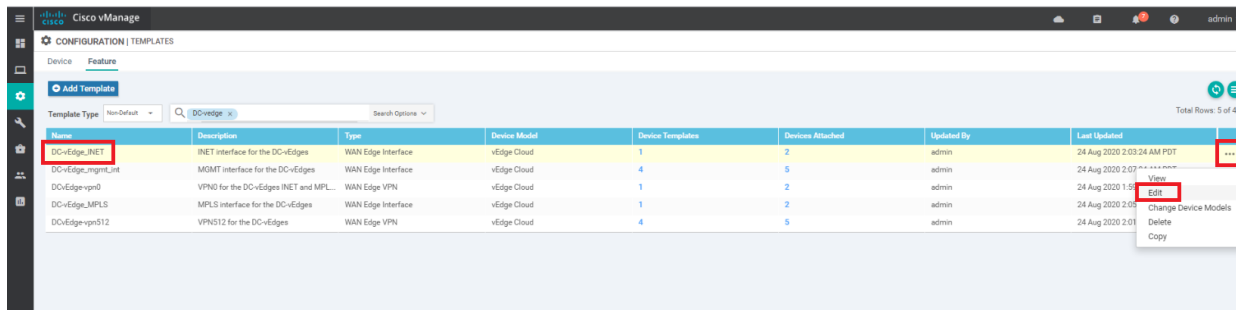


6. We will now enable NAT at the DC site so that the WCM and vManage can communicate with each other. Log in to the vManage GUI (can use Chrome or Firefox now) and navigate to **Configuration => Templates => Feature Tab** and filter the results by typing *DC-vEdge* in the search bar

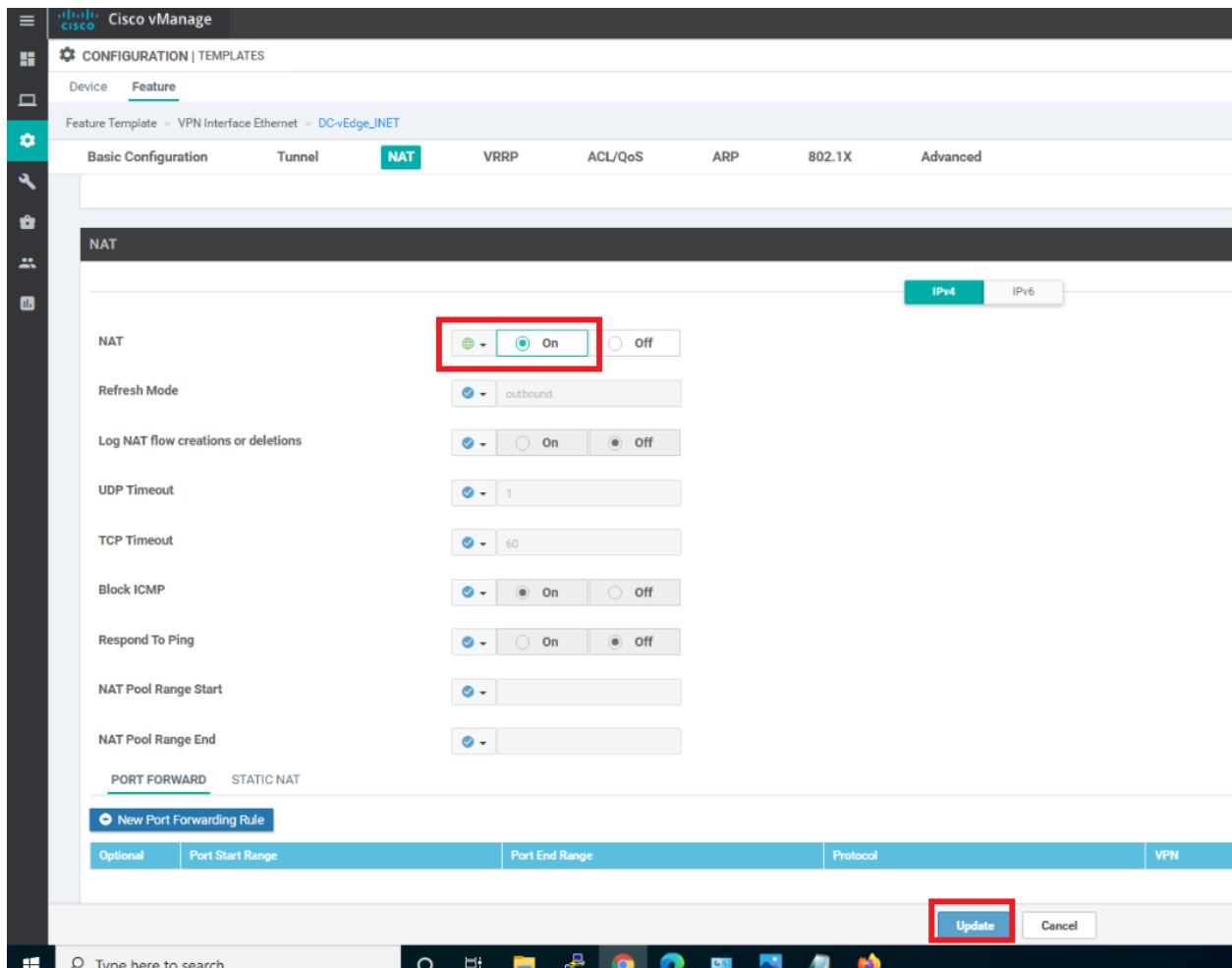
Username	Password
admin	admin



7. Locate the *DC-vEdge_INET* Feature Template and click on the three dots next to it. Choose to **Edit** the template



8. Scroll down to the **NAT** section and set it to a *Global* value of **On**. Click on **Update**



9. Click on **Next**, click on **Configure Devices**, confirm the change and click on OK

Cisco vManage

CONFIGURATION | TEMPLATES

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	DCvEdge1	ge0/3	10.100.20.2/24	ge0/2	10.100.10.2/24
2	0cdd4f0e-f2f1-4e75-866c-46996cda1c3	10.255.255.12	DCvEdge2	ge0/3	10.100.20.3/24	ge0/2	10.100.10.3/24

Next Cancel

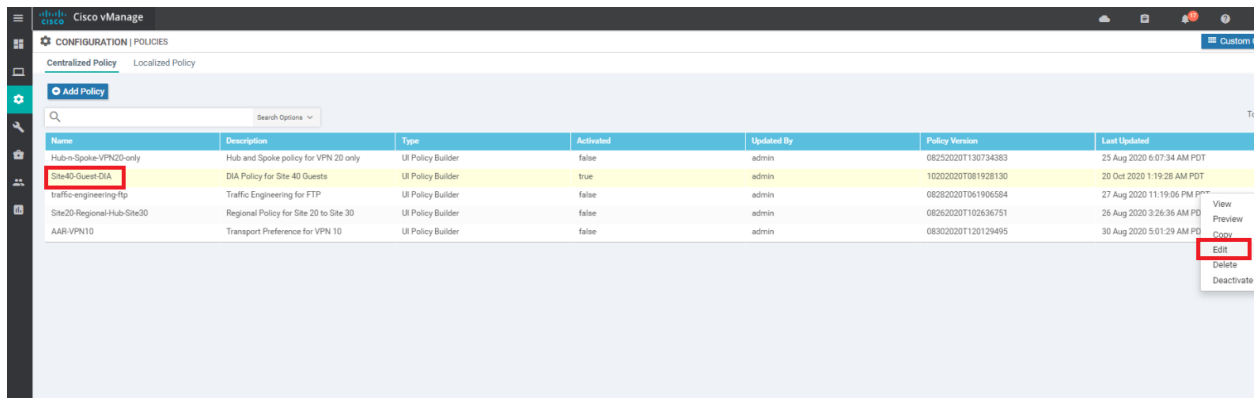
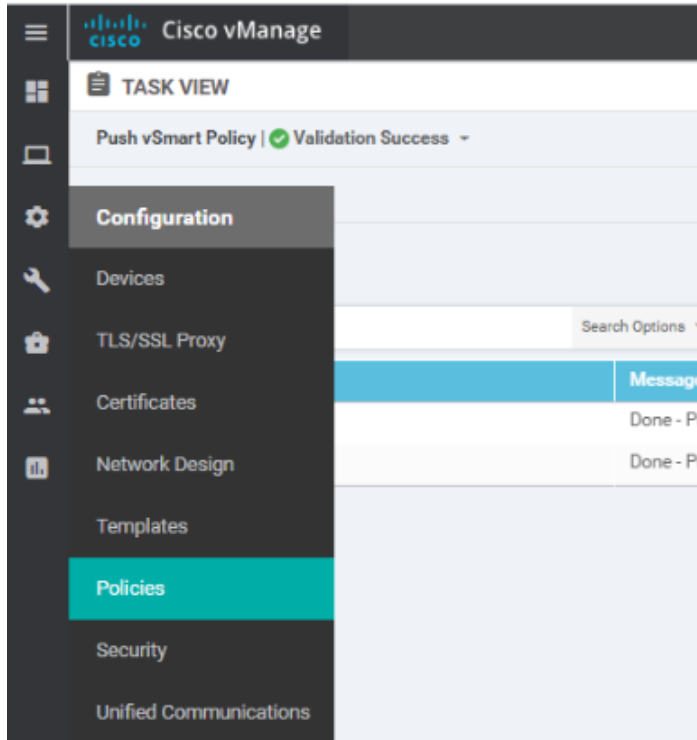
Configure Devices

Committing these changes affect the configuration on 2 devices. Are you sure you want to proceed?

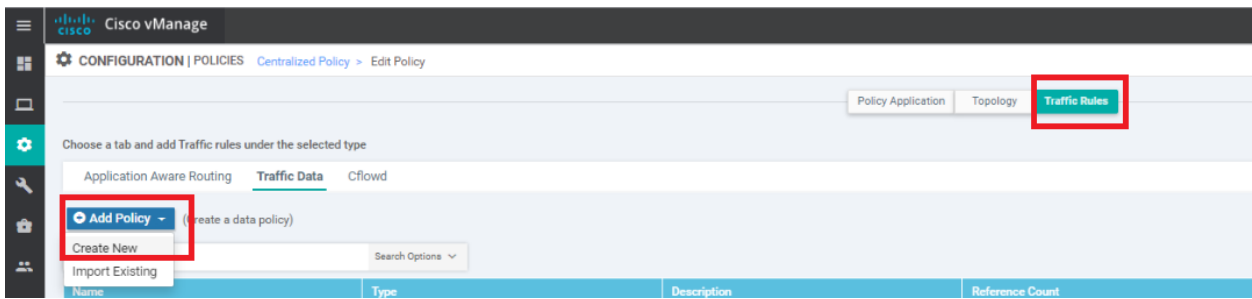
Confirm configuration changes on 2 devices.

OK Cancel

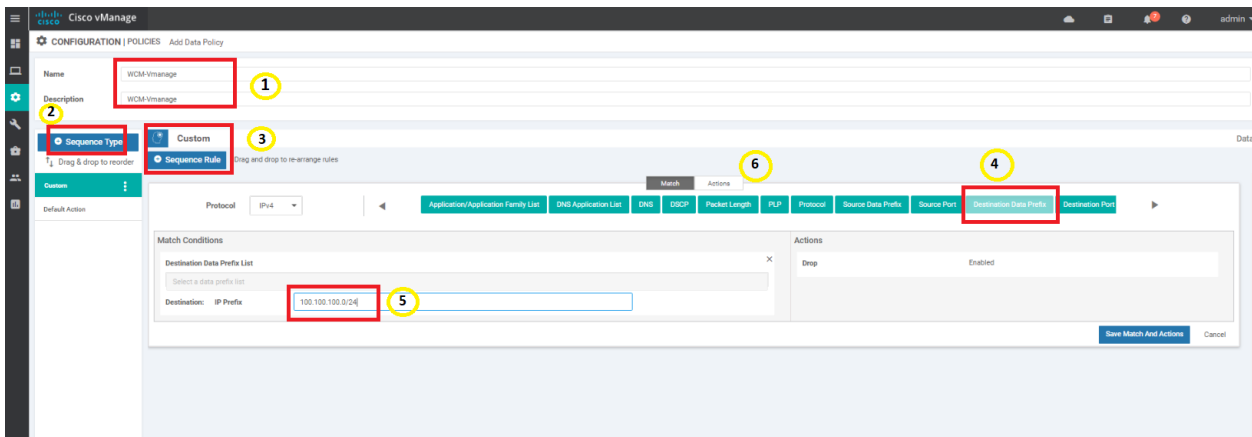
10. Click on **Configuration => Policies** and locate the *Site40-Guest-DIA* policy. Click on the three dots next to it and choose to **Edit** the policy. If the policy isn't active, first activate the policy and then Edit



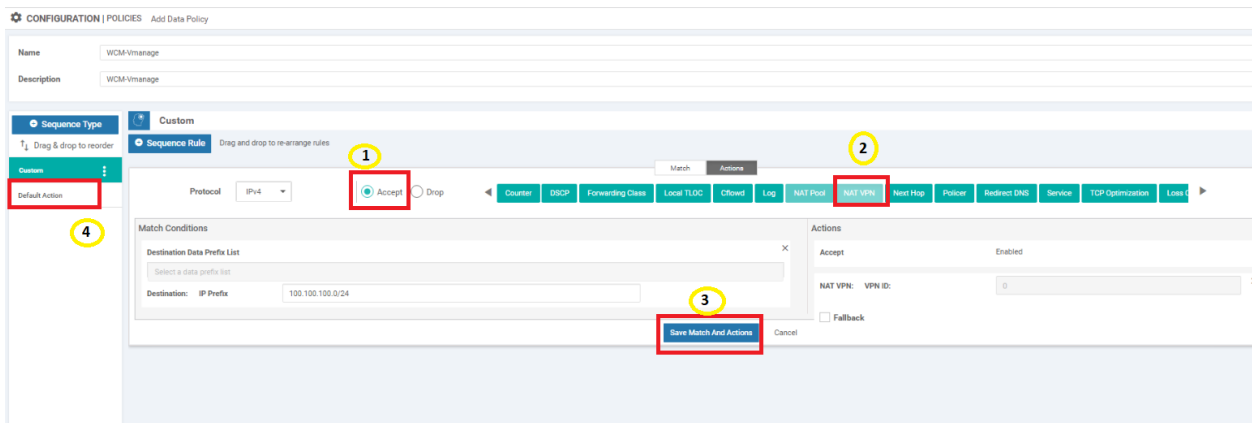
11. Click on the **Traffic Rules** tab and navigate to the *Traffic Data* sub-tab. Click on **Add Policy** and choose *Create New*



- Enter a name and description of *WCM-vManage*. Click on **Sequence Type** and choose *Custom*. Click on **Sequence Rule** and select **Destination Data Prefix** under Match. Enter a Destination: IP Prefix of *100.100.100.0/24* and click on **Actions**



- On the **Actions** tab, click on the **Accept** radio button and choose **NAT VPN**. Click on **Save Match and Actions**. Once saved, click on *Default Action* on the left hand side



14. Edit the default action by clicking on the pencil icon and choosing Accept to be enabled. Click on **Save** to ensure that the default action is saved and then save the policy as well

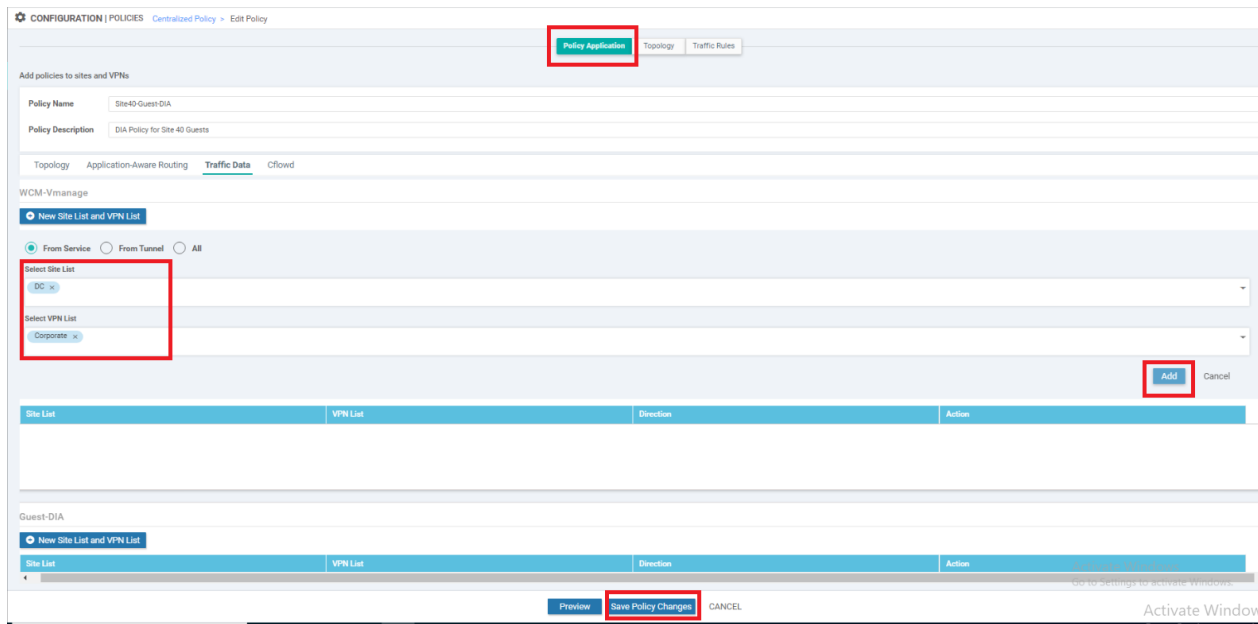
The screenshot shows the configuration page for a policy named 'WCM-Vmanage'. The 'Name' and 'Description' fields both contain 'WCM-Vmanage'. On the left, there is a 'Sequence Type' section with a 'Default Action' tab selected. The main area shows the 'Default Action' configuration, which includes a list of actions. One action is 'Accept', and its status is 'Enabled', which is highlighted with a red box.

15. Once the policy is saved, you should see a new Data Policy called *WCM-vManage*

The screenshot shows the 'CONFIGURATION | POLICIES' page in Cisco vManage. The 'Traffic Rules' tab is selected. Below the tabs, there is a table of policies. The table has columns for Name, Type, Description, Reference Count, Updated By, and Last Updated. Two policies are listed: 'Guest-DIA' and 'WCM-Vmanage'.

Name	Type	Description	Reference Count	Updated By	Last Updated
Guest-DIA	Data	Guest DIA at Site 40	1	admin	27 Aug 2020 11:28:12 PM PDT
WCM-Vmanage	Data	WCM-Vmanage	0	admin	19 Oct 2020 11:28:16 PM PDT

16. Click on the **Policy Application** tab and then click on the *Traffic Data* sub tab. Under the *WCM-vManage* policy, click on **New Site List and VPN List**. Leave the direction as *From Service* and choose **DC** under *Select Site List*. Choose **Corporate** under *Select VPN List*. Click on **Add** and then click on **Save Policy Changes**. Choose to Activate if prompted



17. Once the policy is updated successfully, open Putty and log in to the CLI of WCM (10.100.10.100 or use the saved session). Ping the following destinations to ensure connectivity

- 100.100.100.2
- 10.40.10.2
- 10.50.10.2 and 10.50.10.3

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

Connection type:
 Raw Telnet Rlogin SSH

Load, save or delete a stored session

Saved Sessions

Default Settings
CentralGW
DC-vEdge1
DC-vEdge2
WCM
cEdge40
cEdge50

Close window on exit:
 Always Never Only on clean exit

10.100.10.100 - PuTTY

login as: admin

admin@10.100.10.100's password:

WARNING: Device is configured with a (well known) default username and password. Please change it in order to avoid unwanted access to the device.

Last login: Tue Oct 20 07:14:14 2020 from 10.100.10.30

System Initialization Finished.

WCM#ping 100.100.100.2

PING 100.100.100.2 (100.100.100.2) 56(84) bytes of data.

64 bytes from 100.100.100.2: icmp_req=1 ttl=63 time=0.229 ms

64 bytes from 100.100.100.2: icmp_req=2 ttl=63 time=0.197 ms

^C

--- 100.100.100.2 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1000ms

rtt min/avg/max/mdev = 0.197/0.213/0.229/0.016 ms

WCM#

WCM#

WCM#ping 10.40.10.2

PING 10.40.10.2 (10.40.10.2) 56(84) bytes of data.

64 bytes from 10.40.10.2: icmp_req=1 ttl=254 time=0.501 ms

64 bytes from 10.40.10.2: icmp_req=2 ttl=254 time=0.481 ms

^C

--- 10.40.10.2 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 999ms

rtt min/avg/max/mdev = 0.481/0.491/0.501/0.010 ms

WCM#

WCM#ping 10.50.10.2

PING 10.50.10.2 (10.50.10.2) 56(84) bytes of data.

64 bytes from 10.50.10.2: icmp_req=1 ttl=254 time=0.386 ms

64 bytes from 10.50.10.2: icmp_req=2 ttl=254 time=0.439 ms

64 bytes from 10.50.10.2: icmp_req=3 ttl=254 time=0.293 ms

^C

--- 10.50.10.2 ping statistics ---

3 packets transmitted, 3 received, 0% packet loss, time 2000ms

rtt min/avg/max/mdev = 0.293/0.372/0.439/0.064 ms

WCM#

WCM#

WCM#ping 10.50.10.3

PING 10.50.10.3 (10.50.10.3) 56(84) bytes of data.

64 bytes from 10.50.10.3: icmp_req=1 ttl=254 time=0.565 ms

64 bytes from 10.50.10.3: icmp_req=2 ttl=254 time=0.532 ms

^C

--- 10.50.10.3 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1000ms

rtt min/avg/max/mdev = 0.532/0.548/0.565/0.028 ms

WCM#

```
ping 100.100.100.2
ping 10.40.10.2
ping 10.50.10.2
ping 10.50.10.3
```

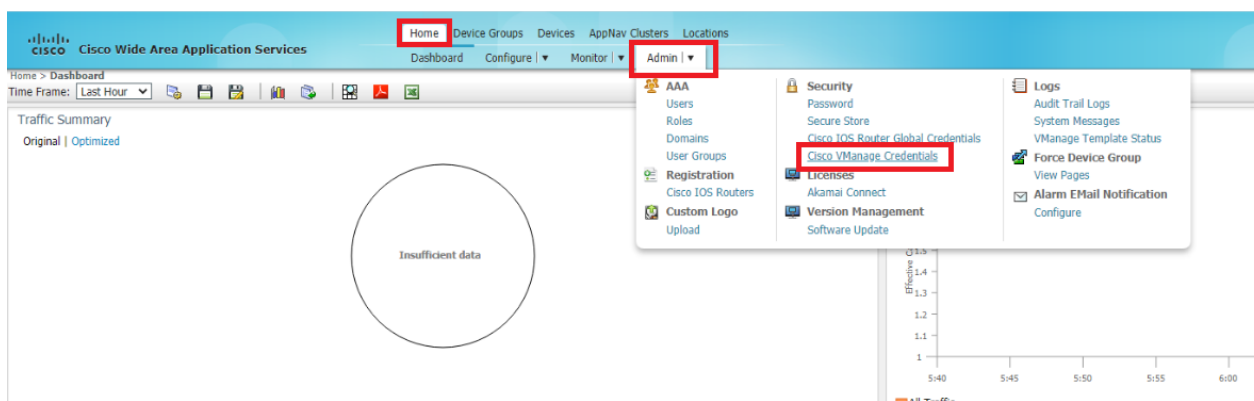
We have completed configuration needed for ensuring WCM can talk to vManage. We have also downloaded the vManage web cert which will be required for the integration.

Task List

- [Overview](#)
- [Adding WAAS Nodes to WCM](#)
- [Downloading vManage certs and Enabling DIA at Site-DC](#)
- [Integrating vManage and WCM](#)
- [Discovering the AppNav-XE Controllers](#)
- [Setting up the AppNav Clusters](#)
- [Verification and Testing](#)

Integrating vManage and WCM

1. Log in to WCM and make sure you're on the **Home** tab. Under **Admin**, click on **Cisco vManage Credentials**



2. Enter the details of vManage as enumerated below and click on **Choose File**. Select the *vmanage.pem* certificate downloaded before in the Downloads folder and click on **Upload**

Hostname or FQDN	IP Address	Username	Password
vmanage	100.100.100.2	admin	admin



vManage Registration Details:

Host Name or FQDN: *	<input type="text" value="vmanage"/>	Launch vManage
IP Address:	<input type="text" value="100.100.100.2"/>	
User Name: *	<input type="text" value="admin"/>	
Password: *	<input type="password" value="....."/>	

Upload Trusted Certificate Bundle (PEM encoded) file .

No file chosen

Enable Revocation Check for vManage Registration

vManage certificate is already uploaded

- If Host name is not DNS resolvable,Please enter IP address with Host name.
- vManage Host name or FQDN should match with SSL certificate Common Name or Subject Alternative Name fields in the Certificate.Otherwise vManage partner registration will fail.
- Performing changes to credentials may impact communication between Central Manager and vManage.
- Please launch vManage and check Administration->Integration management page for WCM partner registration status.
- To Re-Import Certificate, Choose File Press Re-Import Button and then Submit. Old Certificate Details will be Removed and only New Certificate details will Added.

Open

← → ↑ ↓ This PC > Downloads >

Organize ▾ New folder

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Screenshots
- SD-WAN Deployment Files
- System32
- waas-universal-6.4.5.75-k9

OneDrive

This PC

- 3D Objects
- C on ACHAMBIA-H6XLR
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)

Network

Name Date modified

Today (2)

vmanage.pem 19-10-2020 23:11

Firefox Int 19-10-2020 23:09

Earlier this

webServer (1).csr 06-10-2020 03:11

webServer.csr 06-10-2020 02:33

freeFTPd.exe 05-10-2020 23:34

serialFile.viptela 05-10-2020 00:16

Earlier this year (10)

FileZilla_Server-0_9_60_2.exe 07-05-2020 07:41

FileZilla_3.48.0_win64_sponsored-setup.exe 07-05-2020 07:40

VMware-viclient-all-6.0.0-2502222.exe 07-05-2020 06:38

VMware-ovftool-4.2.0-5965791-win.x86_64.msi 07-05-2020 06:26

winrar-x64-590.exe 06-05-2020 21:02

Template.csv 30-04-2020 23:32

pscp.exe 28-04-2020 16:18

VMware-VMRC-11.1.0-15913118.zip 26-04-2020 18:24

Tftpd64-4.64-setup.exe 26-04-2020 17:14


putty-64bit-0.73-installer.msi 24-04-2020 16:45

A long time ago (2)

cisco_x509_verify_release.py 09-02-2018 01:35

WAAS-CCO_RELEASE.cer 28-11-2016 03:09

Type: PEM File
Size: 1.27 KB
Date modified: 19-10-2020 23:11

 Cisco Wide Area Application Services

Home Device Groups Devices AppNa

Dashboard Configure ▼ Monitor |

Home > Admin > Security > Cisco VManage Credentials

Print Refresh

vManage Registration Details:

Host Name or FQDN: *

IP Address:

User Name: *

Password: *

Upload Trusted Certificate Bundle (PEM encoded) file .

vmanage.pem

Enable Revocation Check for vManage Registration

i If Host name is not DNS resolvable,Please enter IP address with Host name.

i vManage Host name or FQDN should match with SSL certificate Common Name or Subject Alternative Name fields in the C

i Performing changes to credentials may impact communication between Central Manager and vManage.

i Please launch vManage and check Administration->Integration management page for WCM partner registration status.

i To Re-Import Certificate, Choose File Press Re-Import Button and then Submit. Old Certificate Details will be Removed and

3. Once the certificate has been uploaded successfully, click on **Submit**. You should see a notification in the bottom right hand corner indicating that the changes were submitted successfully

vManage Registration Details:

Host Name or FQDN: [Launch vManage](#)

IP Address:

User Name:

Password:

Upload Trusted Certificate Bundle (PEM encoded) file

No file chosen

Enable Revocation Check for vManage Registration

vManage certificate is already uploaded

⚠ If Host name is not DNS resolvable please enter IP address with Host name.
⚠ vManage Host name or FQDN should match with SSL certificate Common Name or Subject Alternative Name fields in the Certificate. Otherwise vManage partner registration will fail.
⚠ Performing changes to credentials may impact communication between Central Manager and vManage.
⚠ Please launch vManage and check Administration->Integration management page for WCM partner registration status.
⚠ To Re-Import Certificate, Choose File Press Re-Import Button and then Submit. Old Certificate Details will be Removed and only New Certificate details will Added.

Activate Windows
G...
Success: activate Windows.
Change Subscription

Alaris 1

4. Back at the vManage GUI, navigate to **Administration => Integration Management**. The WCM should show up over here

Cisco vManage

TASK VIEW

Push Feature Template Configuration | ✔ Validation Success ▾

Total Task: 2 | Success : 2

Search Options ▾

- Administration
- Settings
- Manage Users
- Cluster Management
- Integration Management**
- Disaster Recovery
- VPN Groups
- VPN Segments

Message

Done - Push Feature Template C

Done - Push Feature Template C

ADMINISTRATION | INTEGRATION MANAGEMENT

Showing list of third-party controllers registered on vManage Associate Sites for each controller from the 'Actions' menu icon in the table.

Search Options ▾ Total Rows: 1

Controller Name	Description	Partner Id	Platform	Updated By	Date Registered	Devices	
WCM	n/a	WCM	wcm	admin	19 Oct 2020	0	⋮

At this point, WCM and vManage have been integrated. We will now prep the cEdges so that they can be discovered by WCM as AppNav-XE Controllers.

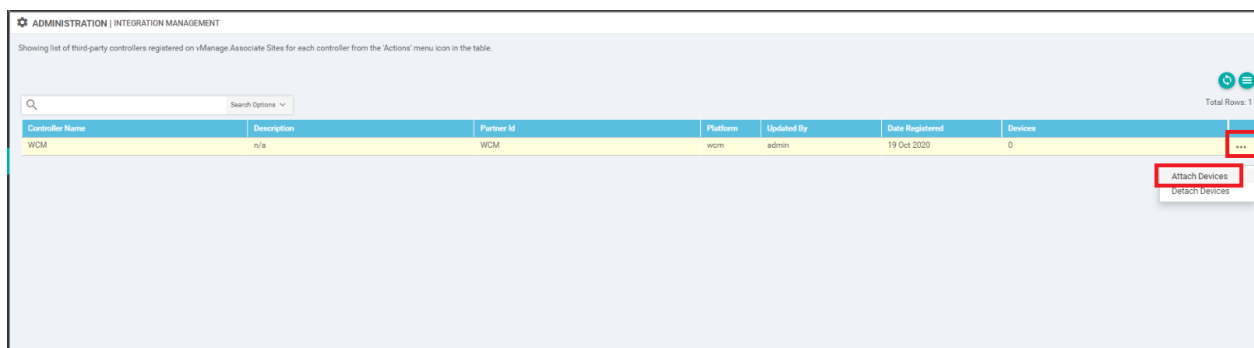
Task List

- [Overview](#)
- [Adding WAAS Nodes to WCM](#)
- [Downloading vManage certs and Enabling DIA at Site DC](#)
- [Integrating vManage and WCM](#)
- [Discovering the AppNav-XE Controllers](#)
- [Setting up the AppNav Clusters](#)
- [Verification and Testing](#)

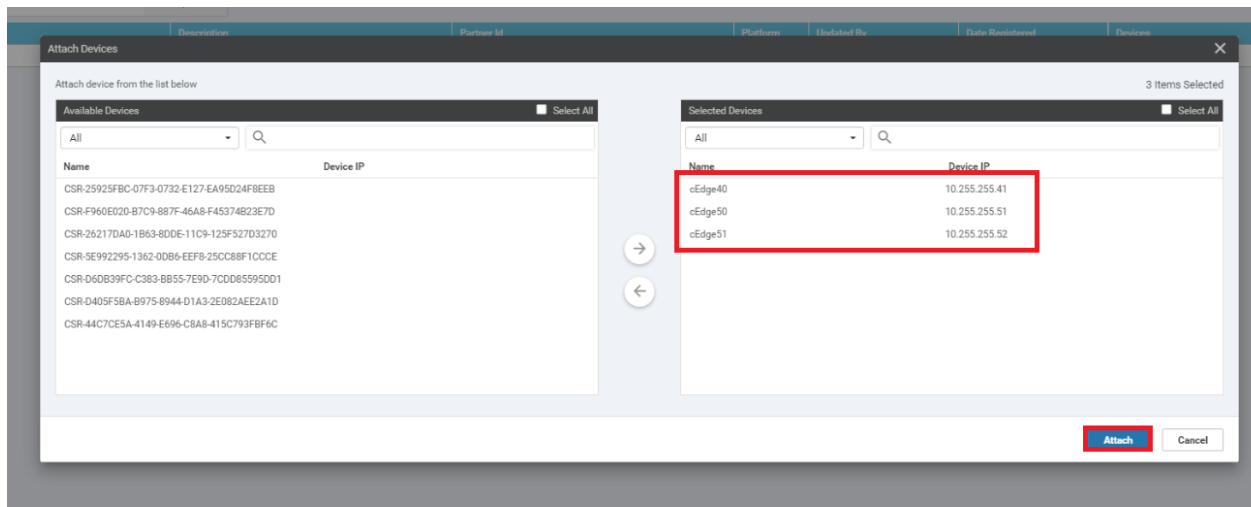
Discovering the AppNav-XE Controllers

Before the WAN Edge devices can be discovered as AppNav-XE Controllers, we will need to make some changes on them.

1. On the **Administration => Integration Management** page of vManage, click on the three dots next to the WCM entry and click on **Attach Devices**

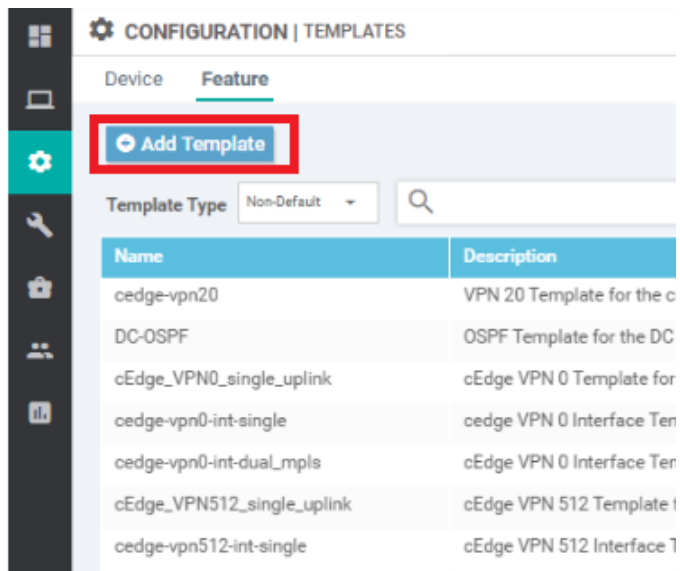


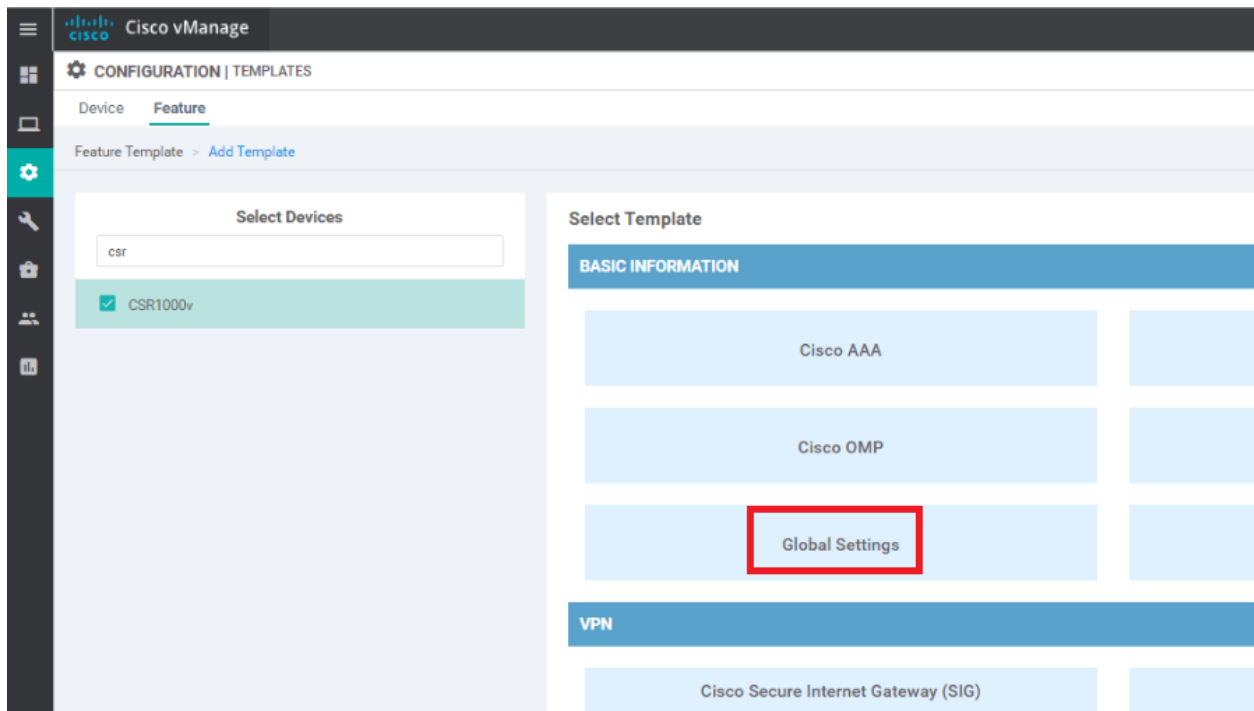
2. Select *cEdge40*, *cEdge50* and *cEdge51* and move them over to the right hand side. Click on **Attach**. You should now see 3 devices attached to WCM



Controller Name	Description	Partner Id	Platform	Updated By	Date Registered	Devices
WCM	n/a	WCM	wcm	admin	19 Oct 2020	3

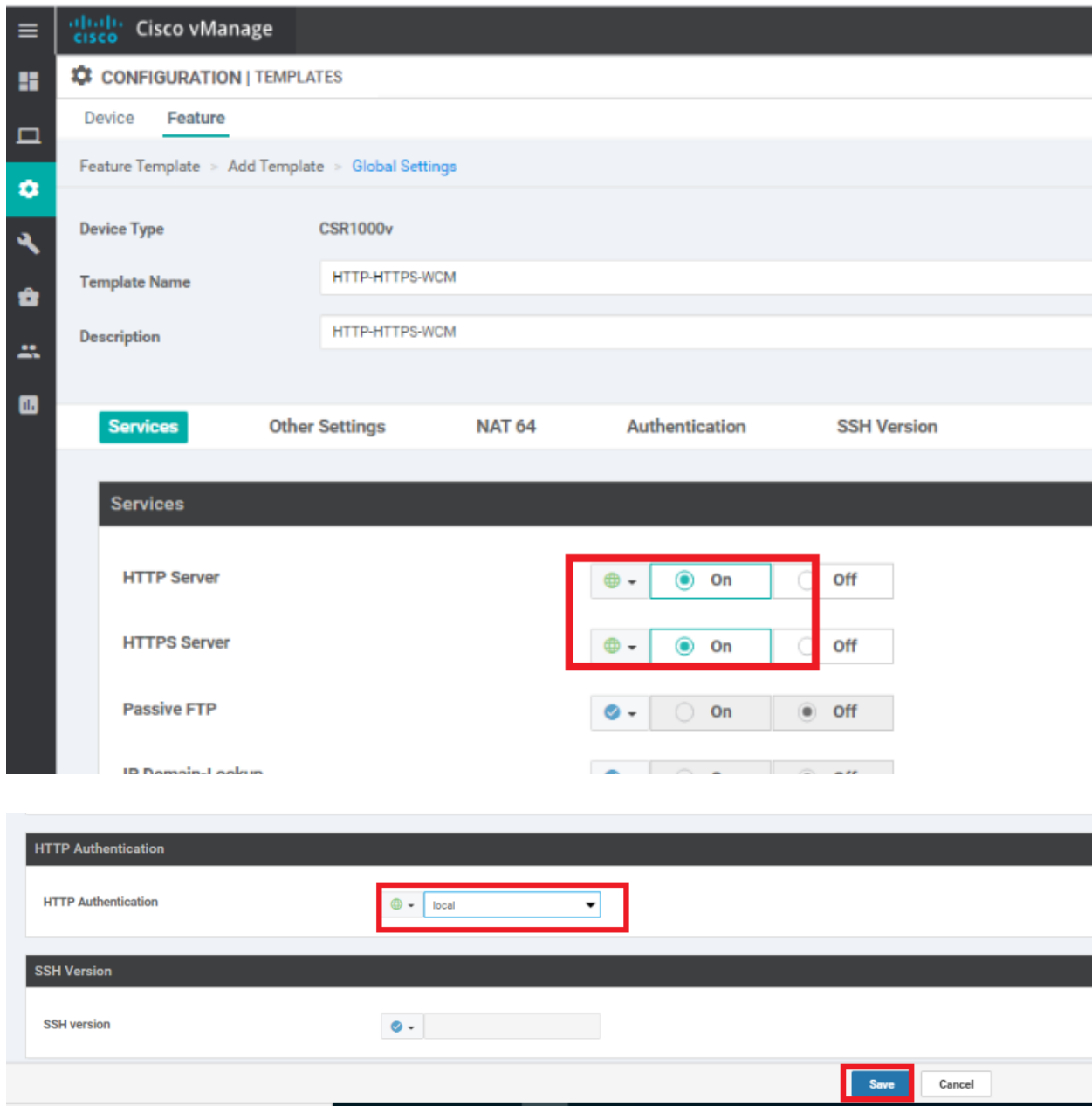
3. Go to **Configuration => Templates => Feature Tab** and click on **Add Template**. Search for and select the **CSR100v** and click on **Global Settings**





4. Enter the following details for the Template and click on **Save**

Section	Field	Global or Device Specific (drop down)	Value
	Template Name		<i>HTTP-HTTPS-WCM</i>
	Description		<i>HTTP-HTTPS-WCM</i>
Services	HTTP Server	Global	On
Services	HTTPS Server	Global	On
HTTP Authentication	HTTP Authentication	Global	local



5. We will now associate this template to the cEdges that will be functioning as AppNav-XE Controllers. Navigate to **Configuration => Templates**. Locate the *cEdge-single-uplink* template and click on the three dots next to it. Choose to **Edit** the template

Cisco vManage

CONFIGURATION | TEMPLATES

Device Feature

Create Template

Template Type: Non-Default

Total Rows: 7

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status
vEdge_Site20_dev_temp	Device template for the Site 20 vEd...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:37:11 PM PDT	In Sync
vEdge-single-uplink	Single Uplink vEdge Device Templa...	Feature	CSR1000v	17	2	admin	24 Aug 2020 6:16:36 AM PDT	In Sync
cedge_duaplink_devtemp	cedge Device Template for devices...	Feature	CSR1000v	20	1	admin	31 Aug 2020 4:30:16 AM PDT	In Sync
DCvEdge_dev_temp	Device template for the DC vEdges	Feature	vEdge Cloud	16	2	admin	25 Aug 2020 6:00:01 AM PDT	In Sync
vEdge30_dev_temp	Device template for the Site 30 vEd...	Feature	vEdge Cloud	15	1	admin	24 Aug 2020 5:52:23 AM PDT	In Sync
vSmart-dev-temp	Device Template for vSmarts	Feature	vSmart	9	2	admin	24 Aug 2020 3:03:09 AM PDT	In Sync
vEdge_Site20_dev_temp_net	Device template for the Site 20 vEd...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:43:47 PM PDT	In Sync

More actions menu for vEdge-single-uplink: Edit, View, Delete, Copy, Attach Devices, Detach Devices, Export CSV, Change Device Values

6. Under **Additional Templates**, set the *Global Template* to the *HTTP-HTTPS-WCM* template we just created and click and **Update**. Click on **Next** and **Configure Devices**, confirming the configuration change on two devices

Cisco vManage

CONFIGURATION | TEMPLATES

Basic Information Transport & Management VPN Service VPN **Additional Templates**

Service VPN

0 Rows Selected Add VPN Remove VPN

Search Options

ID	Template Name	Sub-T
<input type="checkbox"/> 807ccd6b-7982-4d47-9c31-0d078da56aea	cedge-vpn10	Cisco
<input type="checkbox"/> 104e9fe4-ccc1-46a3-801c-13d89a6c04a5	cedge-vpn20	Cisco
<input type="checkbox"/> 6591ab7a-90ae-4229-9a85-3dc95f1d7875	cedge-vpn30	Cisco

Additional Templates

AppQoSE Choose...

Global Template * HTTP-HTTPS-WCM

Cisco Banner Choose...

Cisco SNMP Choose...

CLI Add-On Template Choose...

Policy Choose...

Probes Choose...

Security Policy Choose...

Update Cancel

Cisco vManage

CONFIGURATION | TEMPLATES

Device Template | cEdge-single-uplink

Search Options

S.	Chassis Number	System IP	Hostname	Interface Name(vpn30_if_name)	IPv4 Address/ prefix-length(vpn30_if_ipv4_address)	Interface Name(vpn20_if_name)	IPv4 Address/ prefix-length
1	CSR-834E40DC-E358-8DE1-0EB1-76E598413...	10.255.255.51	cEdge50	GigabitEthernet5	10.50.30.2/24	GigabitEthernet4	10.50.20.2/24
2	CSR-D1837F36-6A1A-1850-7C1C-E1C69759...	10.255.255.52	cEdge51	GigabitEthernet5	10.50.30.3/24	GigabitEthernet4	10.50.20.3/24

Next Cancel

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

7. Repeat the procedure of updating the Global Template for the *cedge_dualuplink_devtemp* Device Template

The screenshot shows the Cisco vManage interface for managing templates. The page title is 'CONFIGURATION | TEMPLATES'. A 'Create Template' button is visible at the top left. Below it is a search bar and a 'Search Options' dropdown. The main content is a table with 7 rows and 9 columns. The row for 'cedge_dualuplink_devtemp' is highlighted in yellow. A context menu is open over the 'cedge_dualuplink_devtemp' row, with the 'Edit' option selected. The table data is as follows:

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status
vEdge_Site20_dev_templ	Device template for the Site 20 vEd...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:37:11 PM PDT	In Sync
vEdge-singleuplink	Single Uplink cEdge Device Templa...	Feature	CSR1000v	17	2	admin	19 Oct 2020 11:41:50 PM PDT	In Sync
cedge_dualuplink_devtemp	cedge Device Template for devices...	Feature	CSR1000v	20	1	admin	31 Aug 2020 4:30:16 AM PDT	In Sync
DCvEdge_dev_templ	Device template for the DC-vEdges	Feature	vEdge Cloud	16	2	admin	25 Aug 2020 6:00:01 AM PDT	In Sync
vEdge30_dev_templ	Device template for the Site 30 vEd...	Feature	vEdge Cloud	15	1	admin	24 Aug 2020 5:52:23 AM PDT	In Sync
vSmart-dev-temp	Device Template for vSmarts	Feature	vSmart	9	2	admin	24 Aug 2020 3:03:09 AM PDT	In Sync
vEdge_Site20_dev_templ_net	Device template for the Site 20 vEd...	Feature	vEdge Cloud	17	1	admin	24 Aug 2020 10:43:47 PM PDT	In Sync

Cisco vManage

CONFIGURATION | TEMPLATES

Basic Information Transport & Management VPN Service VPN **Additional Templates**

0 Rows Selected Add VPN Remove VPN

Search Options

ID	Template Name
807ccd6b-7982-4d47-9c31-0d078da56aea	cedge-vpn10
104e9fe4-ccc1-46a3-801c-13d86a6c04a5	cedge-vpn20
6591ab7a-90ae-4229-9a85-3dc95f1d7875	cedge-vpn30

Additional Templates

AppQoS Choose...

Global Template * HTTP-HTTPS-WCM ⓘ

Cisco Banner Choose...

Cisco SNMP Choose...

CLI Add-On Template Choose...

Policy QoS_Policy

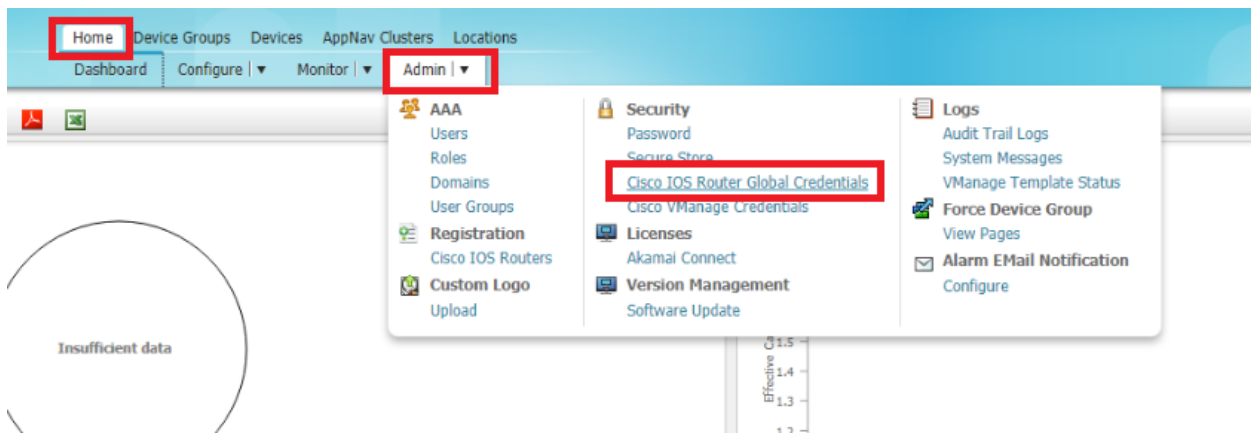
Probes Choose...

Security Policy Guest-FW-IPS-DIA

Container Profile * Factory_Default_UTD_Template ⓘ

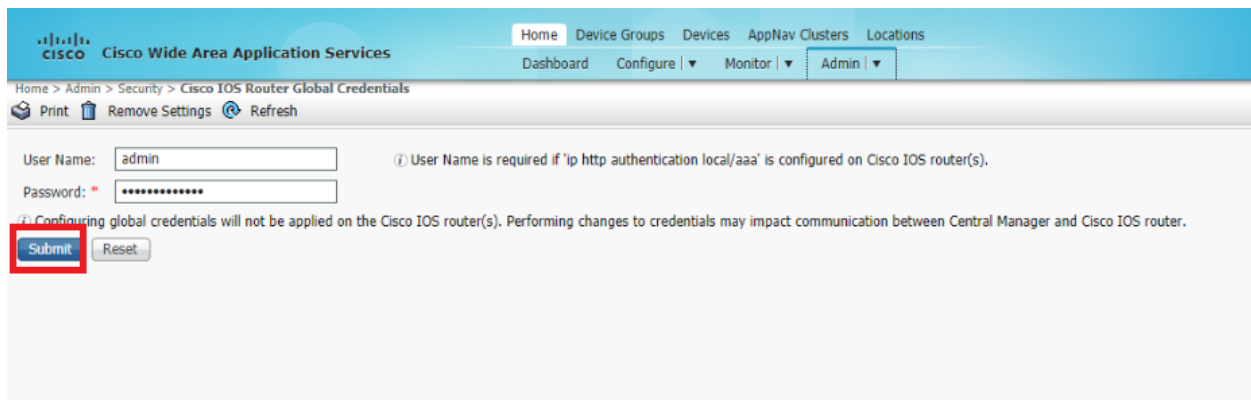
Update Cancel

8. On the WCM GUI, make sure you're on the **Home** tab and click on **Cisco IOS Global Router Credentials** under **Admin**

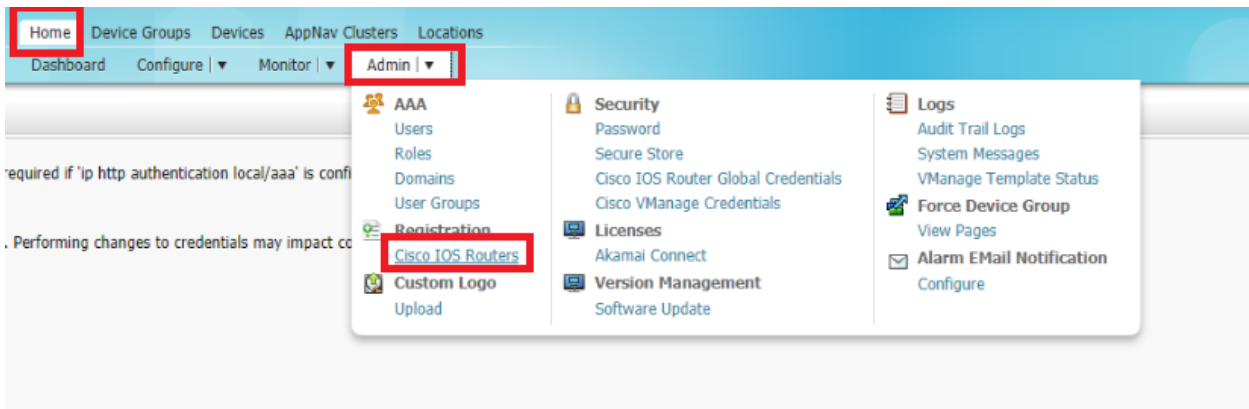


9. Enter the username and password of the WAN Edges and click on **Submit**

Username	Password
admin	admin



10. Again under **Admin**, go to **Cisco IOS Routers**



11. Enter the IP Addresses of your WAN Edges and feed in the username/password of the devices. Set the Authentication to local and enter the WCM IP of 10.100.10.100 and click on **Register**. The IP Addresses should be entered as *10.40.10.2, 10.50.10.2, 10.50.10.3*

Username	Password
admin	admin

CISCO Cisco Wide Area Application Services

Home Device Groups Devices AppNav Clusters Locations
Dashboard Configure | Monitor | Admin |

Home > Admin > Registration > Cisco IOS Routers
Cisco IOS Router Registration

Router IP address type: IPv4
Router IP address entry method: Manual Import CSV file

IP Address(es): ⓘ Comma separated list up to 50 Ipv4 address entries

Username:
Password: *
HTTP Authentication Type:
Central Manager IP Address: * ⓘ Update the Central Manager IP Address if NATed environment is used.

Recreate TrustPoint ⓘ Use this configuration to clean and recreate the default 'Self Signed TrustPoint' in Router.

ⓘ SSH v2 must be enabled on routers.
ⓘ These credentials are used once to register all the listed routers, which should have the same credentials.
ⓘ These credentials are not used for communication between the Central Manager and the routers after registration finishes.
ⓘ HTTP Authentication Type and Recreate Trustpoint are applicable only for Appnav-XE controllers. For Appnav-SDWAN controllers, configuration commands are handled by vManage.
ⓘ Upload self-signed pem certificate in Device Home>Admin>Authentication>Identity Certificate after successful registration for Appnav-SDWAN controller to come online.

Registration Status

IP Address	Hostname	Router type	Status
No data available			

12. You should see the Registration status update in the lower half of the screen. If it doesn't show the WAN Edges, refresh the page. The WAN Edges should register successfully

Cisco Wide Area Application Services

Home | Device Groups | Devices | AppNav Clusters | Locations

Dashboard | Configure | Monitor | Admin

Home > Admin > Registration > Cisco IOS Routers

Cisco IOS Router Registration

Router IP address type: IPv4

Router IP address entry method: Manual Import CSV file

IP Address(es): ⓘ Comma separated list up to 50 Ipv4 address entries

Username:

Password: *

HTTP Authentication Type:

Central Manager IP Address: * ⓘ Update the Central Manager IP Address if NATed environment is used.

Recreate TrustPoint ⓘ Use this configuration to clean and recreate the default 'Self Signed TrustPoint' in Router.

ⓘ SSH v2 must be enabled on routers.
 ⓘ These credentials are used once to register all the listed routers, which should have the same credentials.
 ⓘ These credentials are not used for communication between the Central Manager and the routers after registration finishes.
 ⓘ HTTP Authentication Type and Recreate Trustpoint are applicable only for Appnav-XE controllers. For Appnav-SDWAN controllers, configuration commands are handled by vManage.
 ⓘ Upload self-signed pem certificate in Device Home>Admin>Authentication>Identity Certificate after successful registration for Appnav-SDWAN controller to come online.

Registration Status			
IP Address	Hostname	Router type	Status
10.40.10.2	cEdge40	AppNav-SDWA...	✔ Successfully processed the registration request
10.50.10.2	cEdge50	AppNav-SDWA...	✔ Successfully processed the registration request
10.50.10.3	cEdge51	AppNav-SDWA...	✔ Successfully processed the registration request

13. In order to complete the registration, we will need to upload the certificate of each device on WCM. Log in to the CLI of *cEdge40* via Putty and issue the command `show crypto pki certificate pem`. Copy the certificate and paste it in Notepad. Make sure there aren't any additional characters at the end (sometimes, a new line is copied as well and this can cause issues while pasting the certificate)

```
show crypto pki certificate pem
```

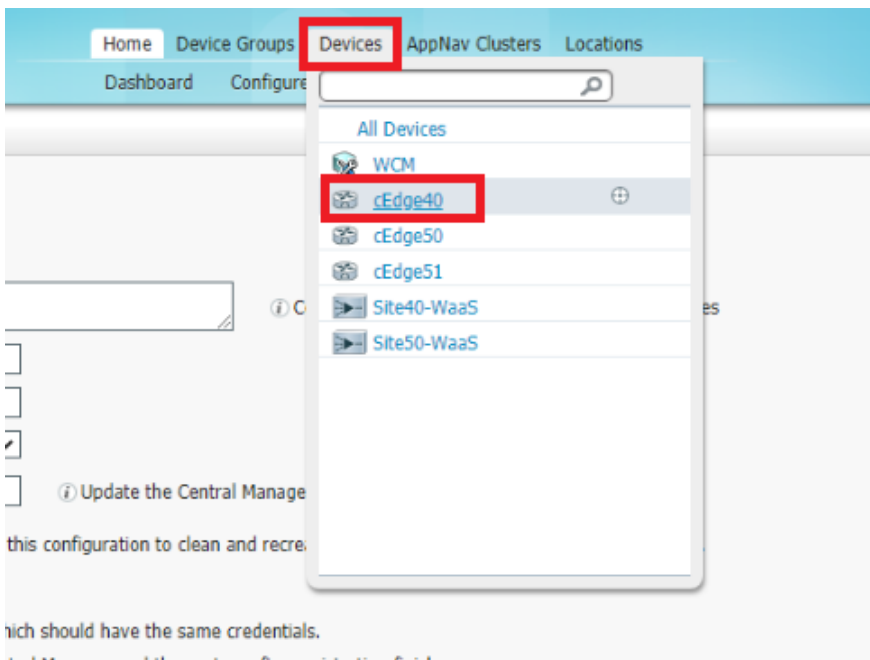
Username	Password
admin	admin

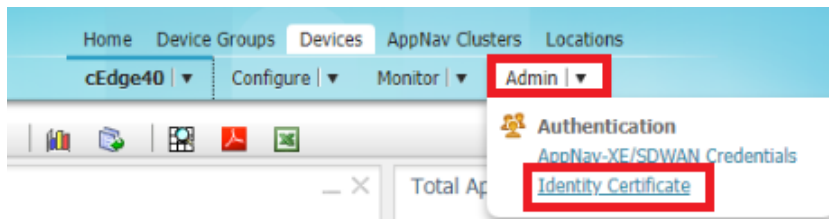

```
-----END CERTIFICATE-----

-----Trustpoint: SLA-TrustPoint-----
% The specified trustpoint is not enrolled (SLA-TrustPoint).
% Only export the CA certificate in PEM format.
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIDITCCAqmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAYMQ4wDAYDVQQKEwVDaXNj
bzEgMB4GA1UEAxMXQ21zY28gTG1jZW5zaW5nIFJvb3QgQ0EwHhcNMTMwNTMwMTk0
ODQ3WWhcNMzgwNTMwMTk0ODQ3WjAyMQ4wDAYDVQQKEwVDaXNjYzEgMB4GA1UEAxMX
Q21zY28gTG1jZW5zaW5nIFJvb3QgQ0EwggEiMA0GCsQGSIB3DQEBAAUAA4IBDwAw
ggEKAoIBAQCmVl2WEx4F9xRepywsl0bmFyIuofHv9k3LtMeYISqR8ZV2NeUcTgN
hxFEHhqvBxqcrM0I1j1IBw5TXhGLvI5xln3FbmMC11buly9DP6+o3AKi/fY81bu
SgToDdtv0clgsf0Y/8aclm+miVeiYX3nEE/cX+opVqxzkKPrKlQ2rchHosXatVPr
aamlNVjp8+PAvSPPWLlxigjmlJEg8yDnlI5x1647zITxBoTHS8jgD10bpCtCxou3
x0eQlrTLLWLqL1Bdx7BipGgR2VvoJQ/EXV1fuI8n0ZHFxw12YfmkzT2Ziyeouw09
TmlwaXy634vfX0No1RNeRN/Hxs8E3X/RAGMBAAGjQjBAMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBRRJ3IVLPTH1Gz5qF2Bq8zM900xz
6DANBgkqhkiG9w0BAQsFAAOCAQEAUH8k05MqZ0YCXZ/0OK5cbU32sE1jHHgkDakF
YE7c3v9P7St3/EYOzWNV291EaB46VnOrkJPtSwYePYvZiYe/5Ay9nhrsoMIh1btc
j6hWhs2YtkZVdbFGjfxmqEZ6PFRNv1cAat8PDc+DUBU8BP98Ieh4rBG6nNJVqSMs
fKe35sGvdPYVLpm3sfz5u+1z3n9b3euGxx47SRdlMITfsNoGuSr+f010ip4HuFc3
86WL4RpIoinDfB5pOfCGEIDdzRbWus7K7rx8+YQoeHs1ICzoYORharYjzb0jDjr7
QYYWqUCT4E1NEKt1J+hvc5MuNbWlYv2uAnUVb3GhsvDW199/KA==
-----END CERTIFICATE-----

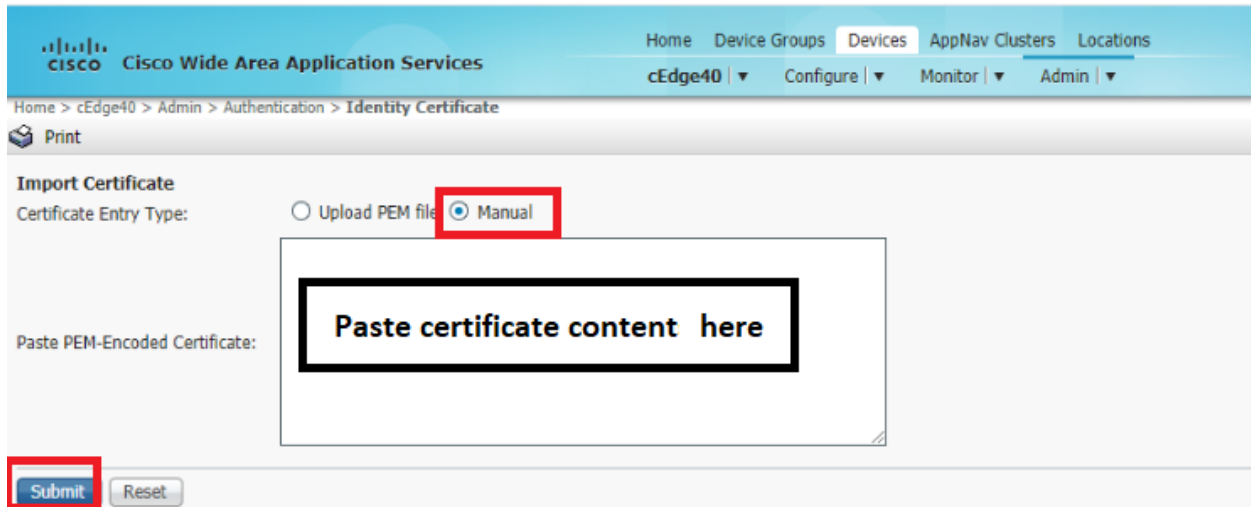
cEdge40#
```


14. On the WCM GUI, go to **Devices => cEdge40**. Once on the cEdge40 page, click on **Admin => Identity Certificate**





15. Select the *Certificate Entry Type* as Manual and paste the certificate we just copied in the box. Click on **Submit**. If you look at the certificate info tab, the contents of the certificate should be visible



 Cisco Wide Area Application Services

[Home](#)
[Device Groups](#)
[Devices](#)
[AppNav Clusters](#)
[Locations](#)

[cEdge40](#) | [Configure](#) | [Monitor](#) | [Admin](#)

Home > cEdge40 > Admin > Authentication > Identity Certificate

Print

Import Certificate

Certificate Entry Type: Upload PEM file Manual

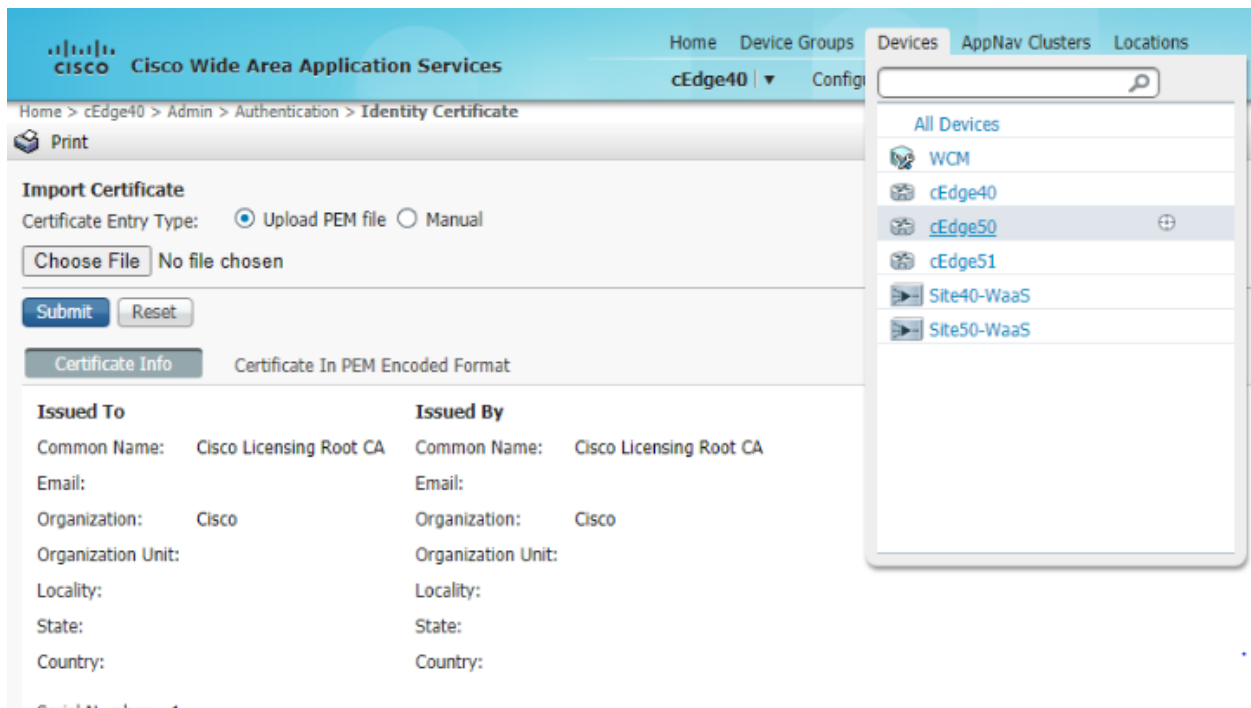
Choose File No file chosen

Submit Reset

Certificate Info Certificate In PEM Encoded Format

Issued To		Issued By	
Common Name:	Cisco Licensing Root CA	Common Name:	Cisco Licensing Root CA
Email:		Email:	
Organization:	Cisco	Organization:	Cisco
Organization Unit:		Organization Unit:	
Locality:		Locality:	
State:		State:	
Country:		Country:	
Serial Number: 1			
Validity			
Issued On:	Thu May 30 19:48:47 UTC 2013		
Expires On:	Sun May 30 19:48:47 UTC 2038		
Fingerprint			
SHA1:	5C:A9:5F:B6:E2:98:0E:C1:5A:FB:68:1B:BB:7E:62:B5:AD:3F:A8:B8		
Base64:	XKIfuKYDsFa+2gbu35ita0/qLg=		
Key			
Type:	SHA256WITHRSA		
Size (Bits):	2048		

16. Repeat steps 13 till 15 for *cEdge50* and *cEdge51*, copying their respective certificates to the WCM GUI



This completes the discovery and registration of the AppNav-XE Controllers to WCM.

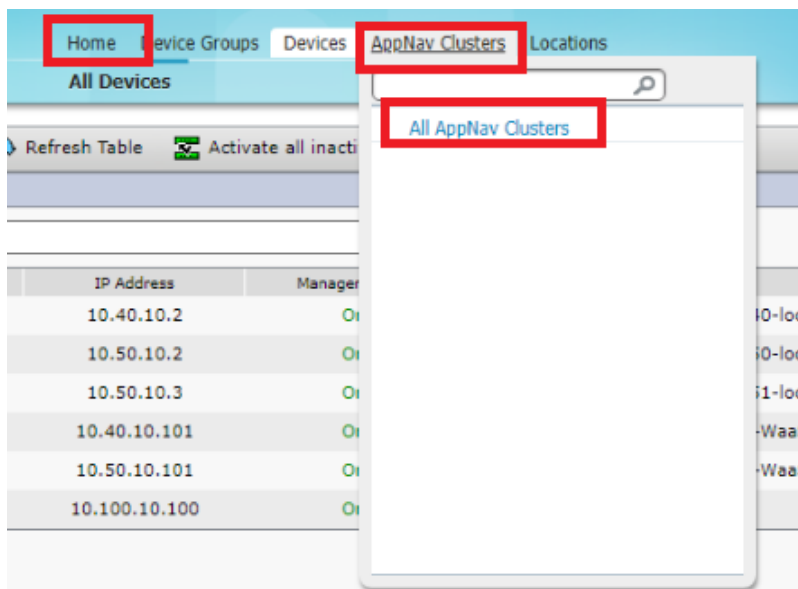
Task List

- [Overview](#)
- [Adding WAAS Nodes to WCM](#)
- [Downloading vManage certs and Enabling DIA at Site DG](#)
- [Integrating vManage and WCM](#)
- [Discovering the AppNav-XE Controllers](#)
- [Setting up the AppNav Clusters](#)
- [Verification and Testing](#)

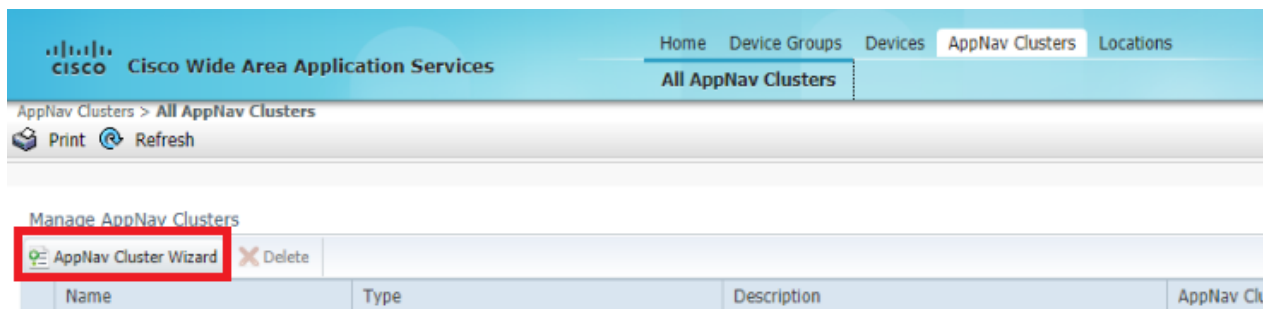
Setting up the AppNav Clusters

We will be setting up two AppNav Clusters in the lab. One will be at Site 40 and another at Site 50.

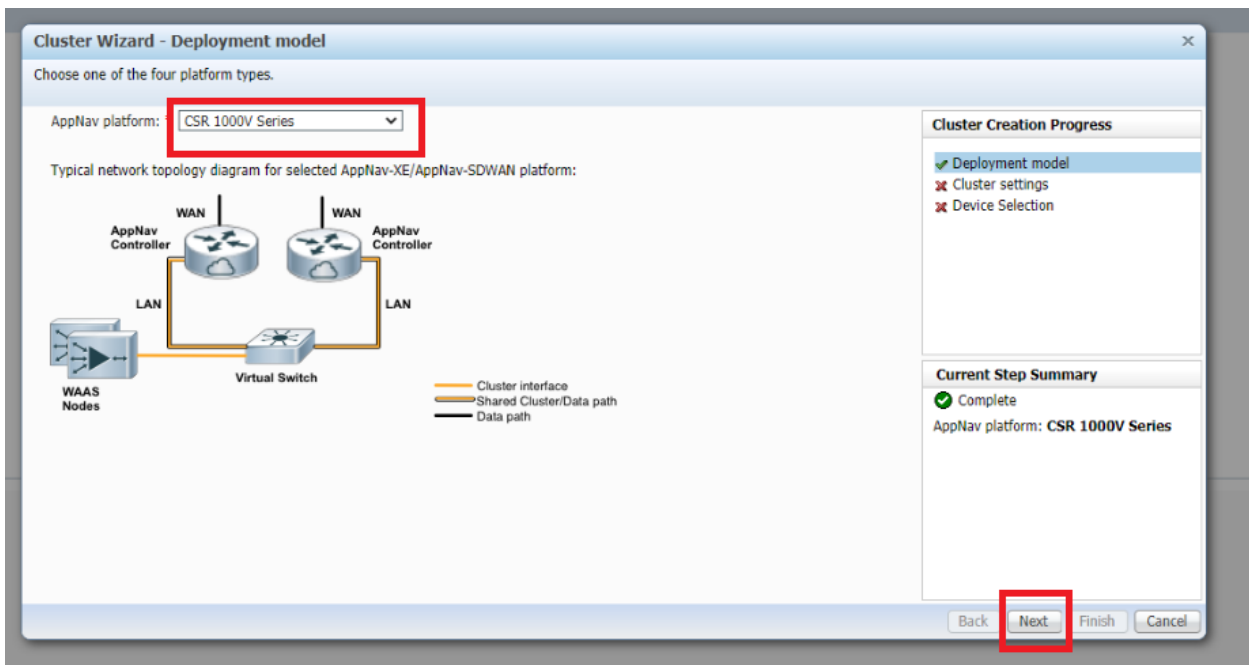
1. On the WCM GUI, make sure you're at the Home tab and click on **AppNav Clusters**. Choose **All AppNav Clusters**



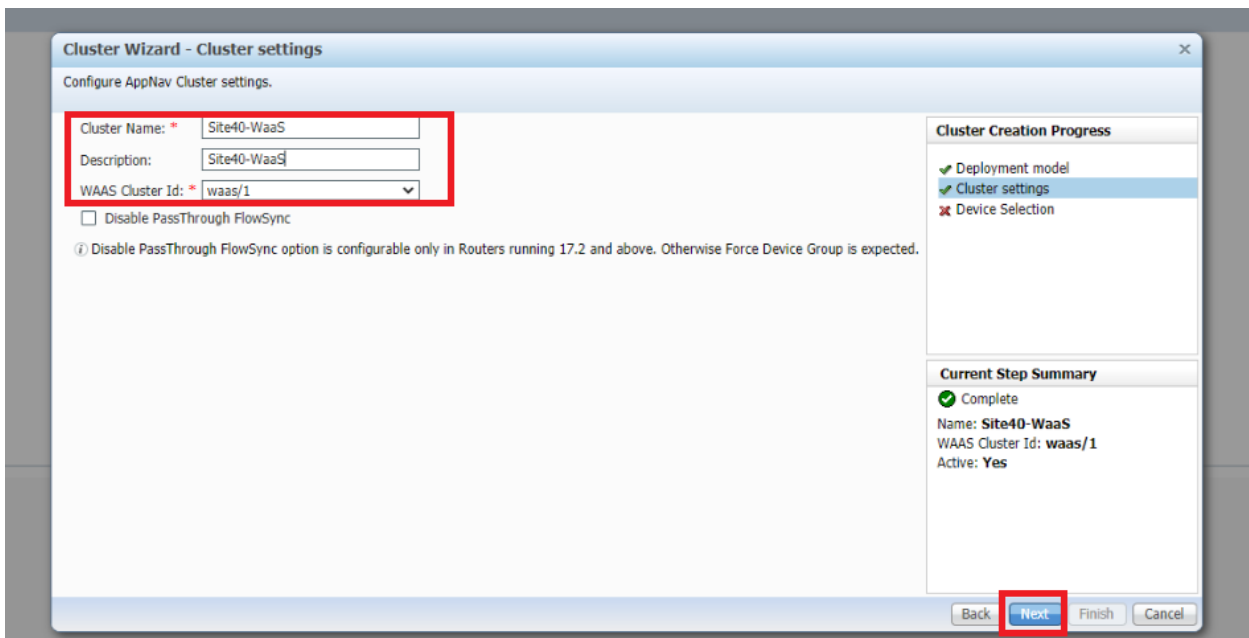
2. Click on **AppNav Cluster Wizard** to start setting up our AppNav clusters



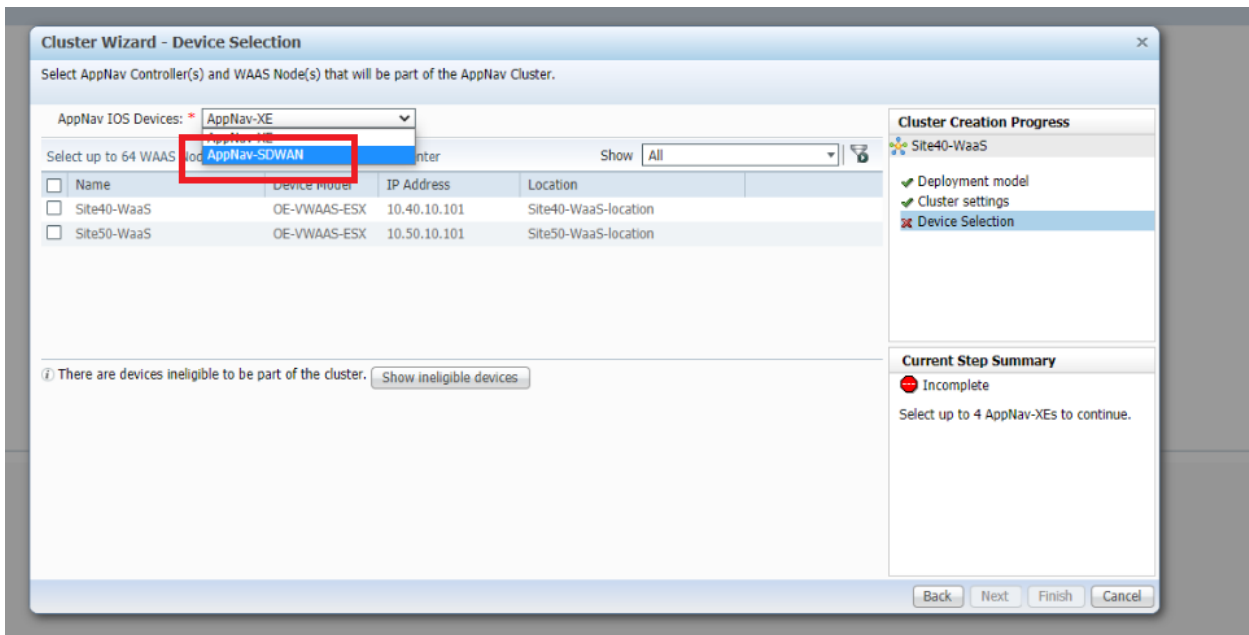
3. Choose **CSR 1000V Series** for the AppNav Platform since we will be using the CSRs at Site 40 and Site 50 as the AppNav-XE controllers. Click on **Next**



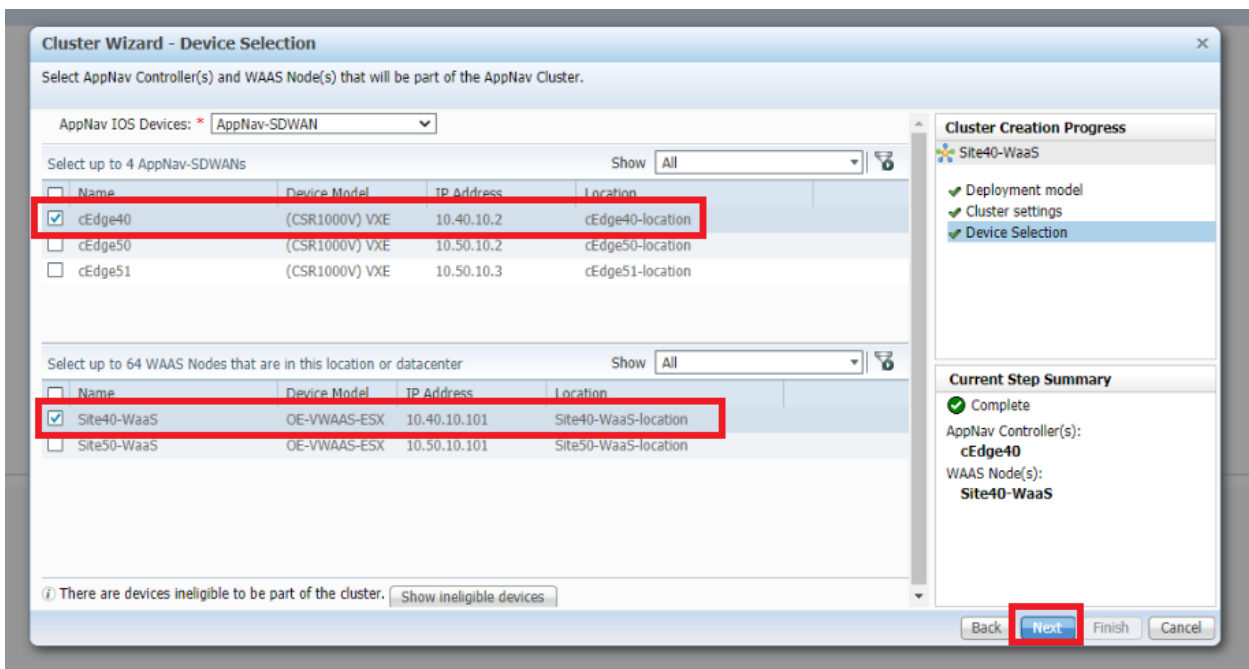
4. Enter a **Cluster Name** and **Description** of *Site40-WaaS*, select the **WAAS Cluster ID** as *waas/1* and click on **Next**



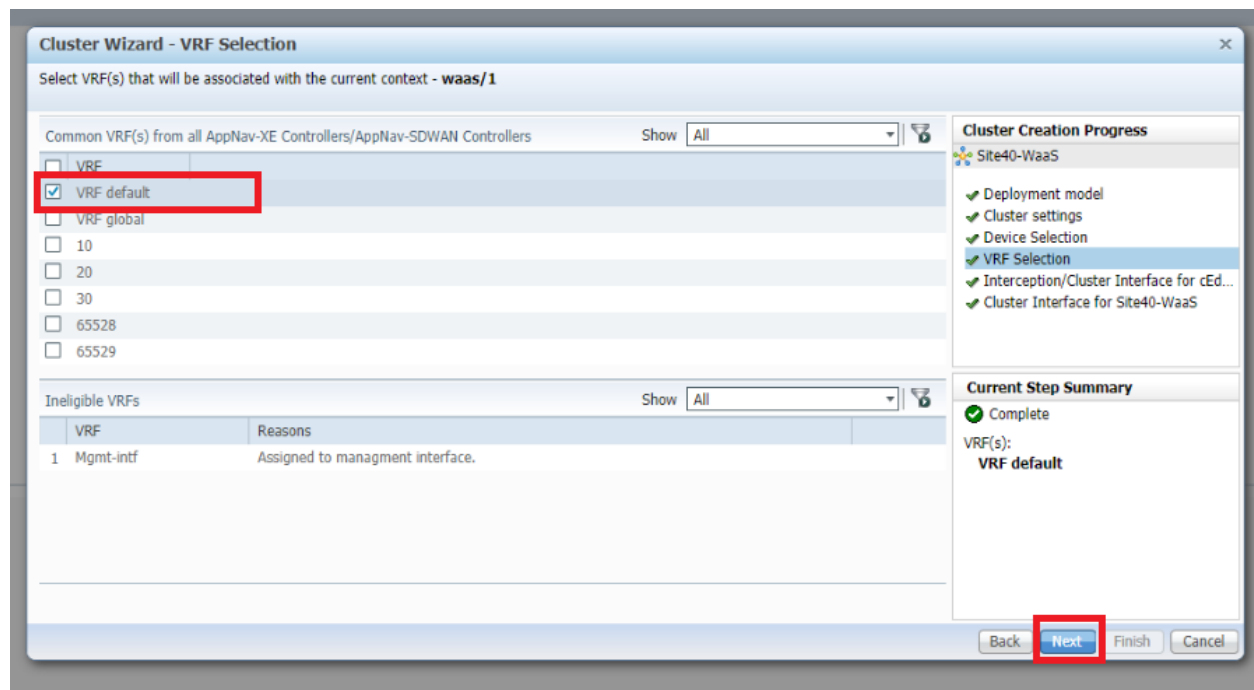
5. Select the **AppNav IOS Devices** as *AppNav-SDWAN*



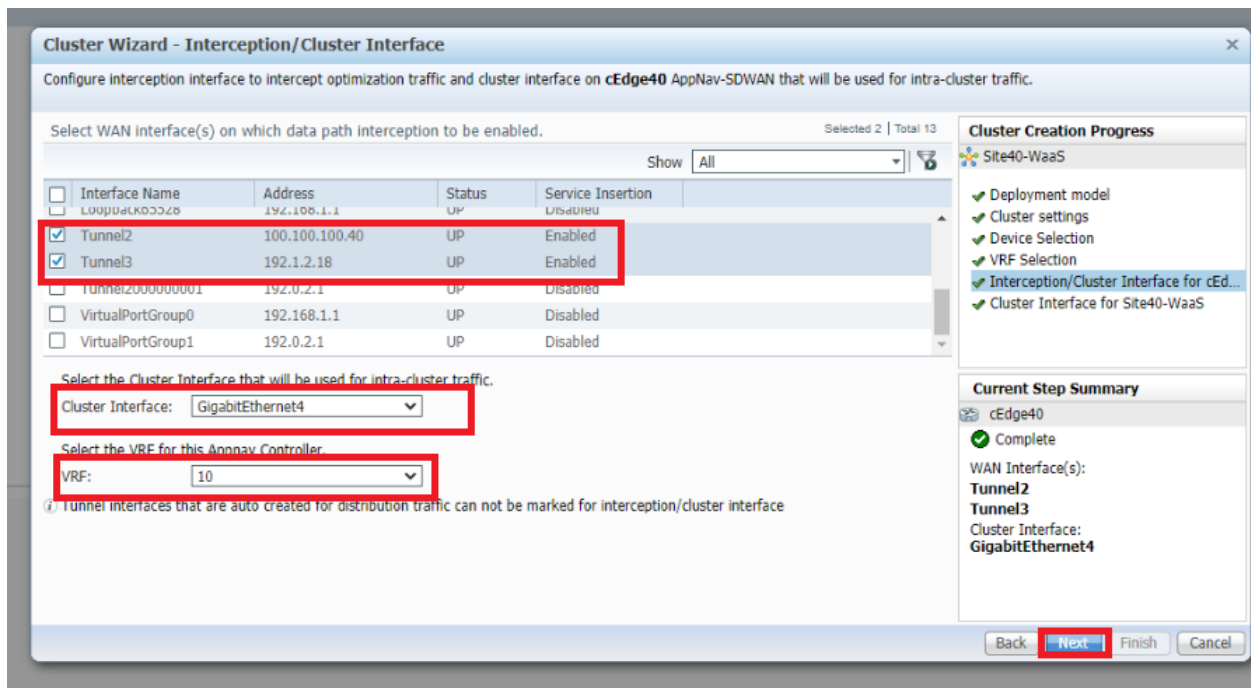
6. Select *cEdge40* in the upper half of the window and *Site40-WaaS* in the lower half. We're choosing the components of our cluster over here. Click on **Next**



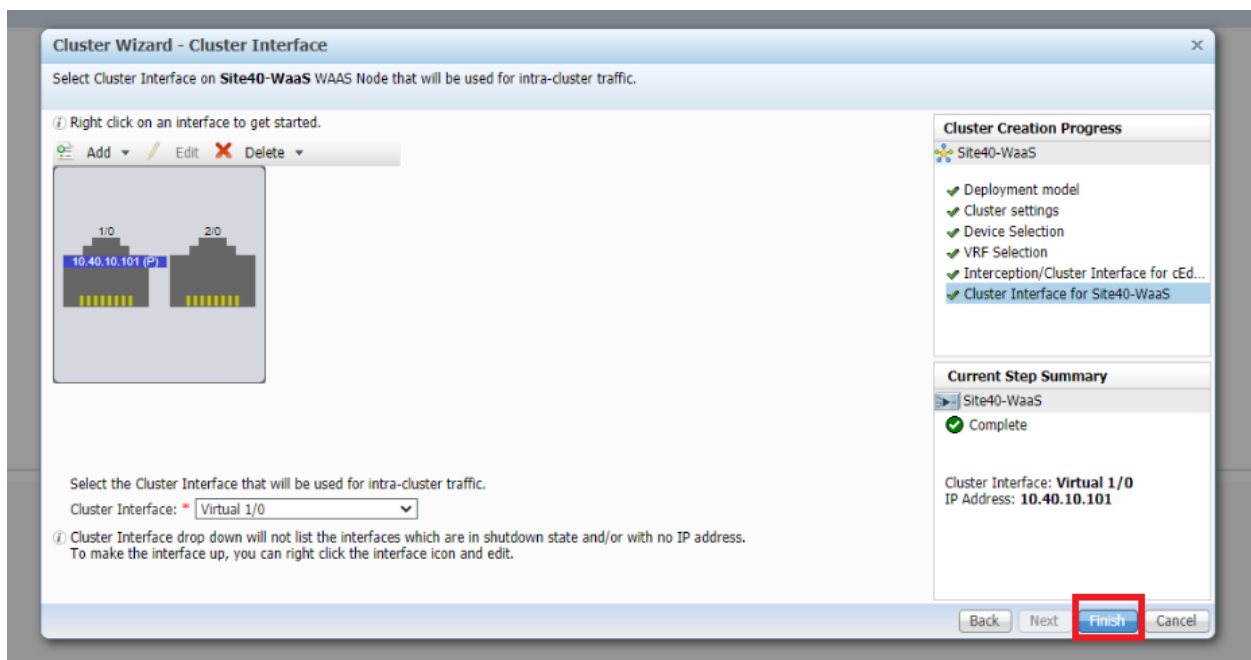
7. Select *VRF default* and click on **Next**. This associates all VRFs with the context *waas/1*



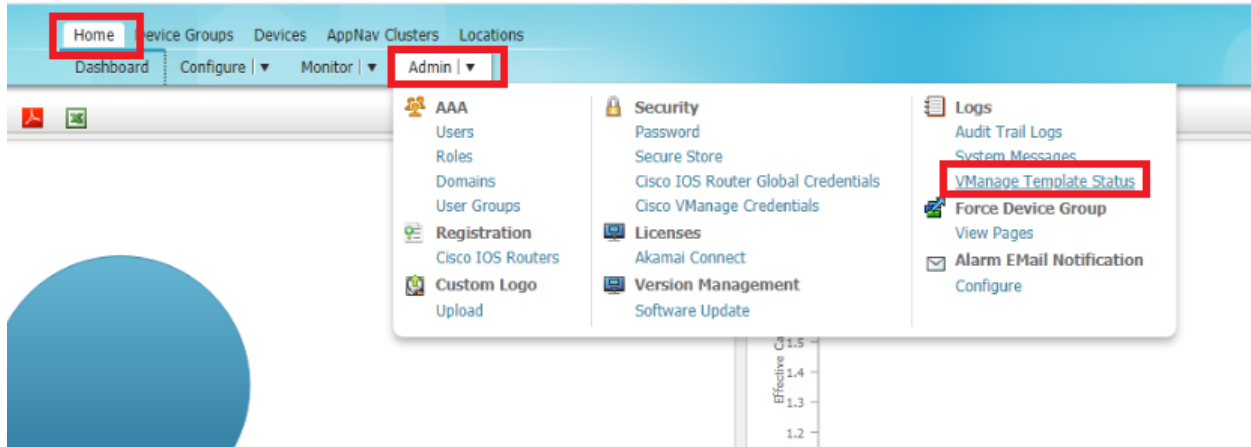
8. Select *Tunnel2* and *Tunnel3* as the WAN interfaces on which data path interception should be enabled. Make sure the **Cluster Interface** is set to *GigabitEthernet4* and the VRF is *10*. Click on **Next*



9. Click on **Finish**, making sure the cluster interface is set to **Virtual 1/0**



10. Templates are pushed to vManage which in turn configures the AppNav-XE Controllers. The status of the template push can be checked on vManage or on WCM. On WCM, make sure you're on the Home tab and click on **vManage Template Status** under **Admin**. Wait for the templates to get deployed before proceeding



This screenshot shows the 'vManage Template Status' page. The breadcrumb trail is 'Home > Admin > Logs > vManage Template Status'. Below the breadcrumb is a 'Print' button. The main content area is titled 'vManage Template Status' and contains a table with the following data:

Device	Latest Template	Status
cEdge40	push_template_configuration-98130ef1-aa56-4fdb-ae4-c670e8b0f1ea	In progress
cEdge51	push_template_configuration-9ba51b40-f52b-4f8f-844b-a026c3fe669d	Success
cEdge50	push_template_configuration-16a6dfd2-3871-4d84-ba18-0af4ba661adf	Success

Home Device Groups Devices AppNav Clusters Locations
Dashboard Configure Monitor Admin

Home > Admin > Logs > VManage Template Status

Print

vManage Template Status

Device	Latest Template	Status
cEdge40	push_template_configuration-98130ef1-ea56-4fdb-ae4-c670e8b0f1ea	Success
cEdge51	push_template_configuration-9ba51b40-f52b-4f8f-844b-a026c3fe669d	Success
cEdge50	push_template_configuration-16a6dfd2-3871-4d84-ba18-0af4ba661adf	Success

11. We have built our AppNav Cluster at Site 40. A similar procedure will need to be followed for the Site 50 AppNav Cluster. Open the AppNav Cluster Wizard and select the **AppNav Platform** as *CSR 1000V Series*. Click on **Next**

AppNav Clusters > All AppNav Clusters

Print Refresh

Manage AppNav Clusters

AppNav Cluster Wizard Delete

Name	Type	Description	AppNav Cluster Status
Site40-WaaS	AppNav-SDWAN Cluster		

Cluster Wizard - Deployment model

Choose one of the four platform types.

AppNav platform: **CSR 1000V Series**

Typical network topology diagram for selected AppNav-XE/AppNav-SDWAN platform:

Legend:
— Cluster interface
— Shared Cluster/Data path
— Data path

Cluster Creation Progress

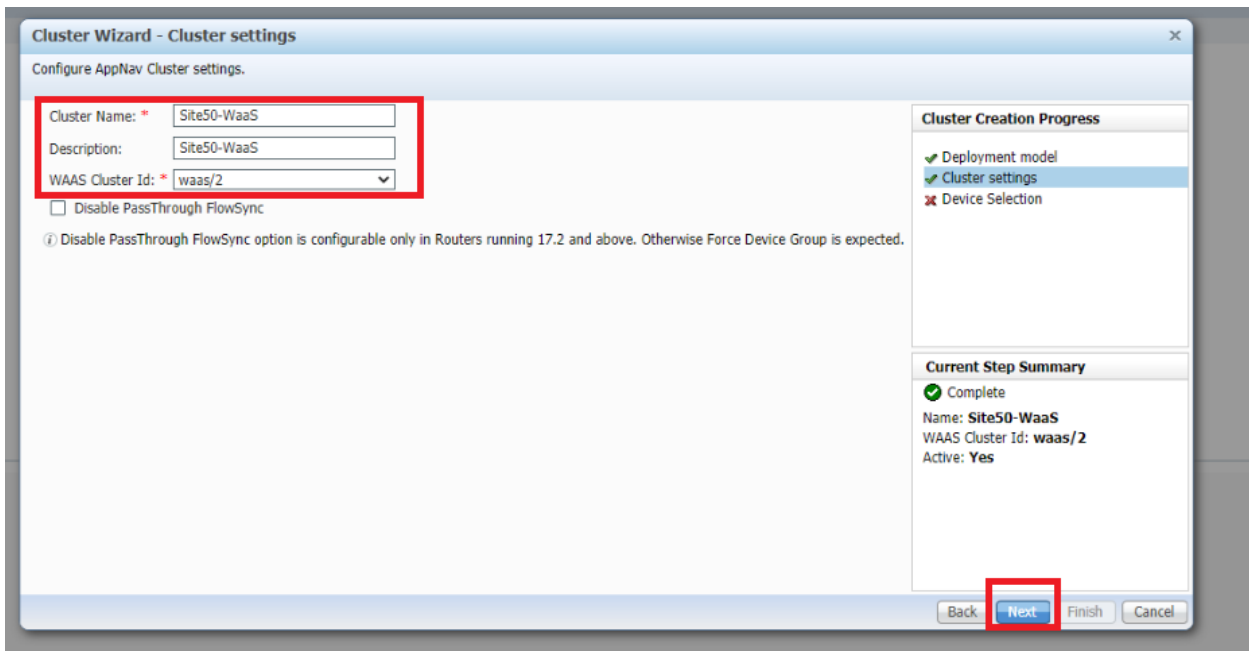
- Deployment model
- Cluster settings
- Device Selection

Current Step Summary

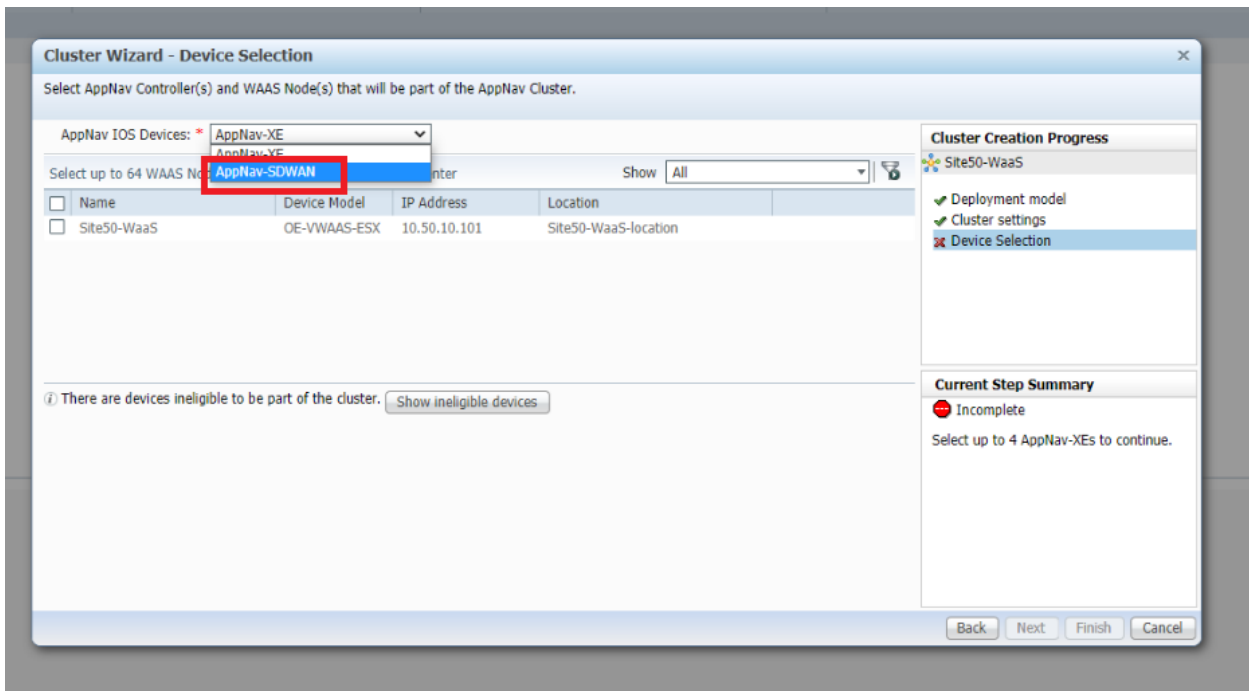
- Complete
- AppNav platform: CSR 1000V Series

Back **Next** Finish Cancel

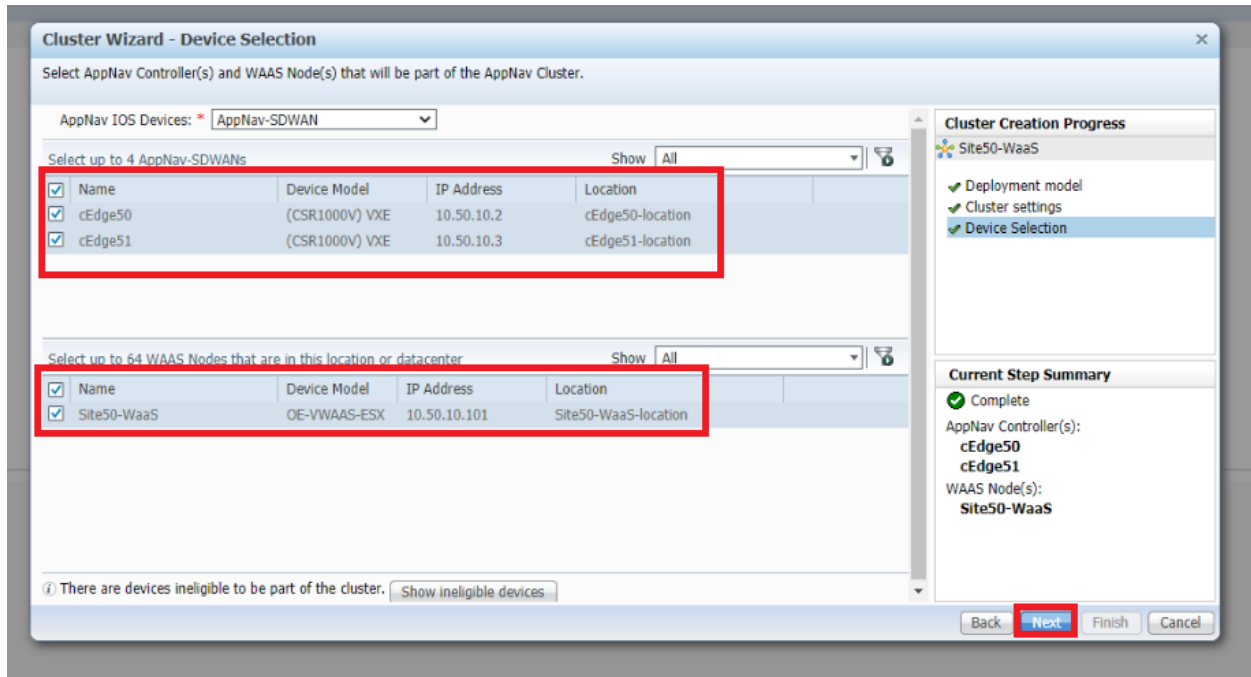
12. Enter a **Cluster Name** and **Description** of *Site50-WaaS*, select the **WAAS Cluster ID** as *waas/2* and click on **Next**



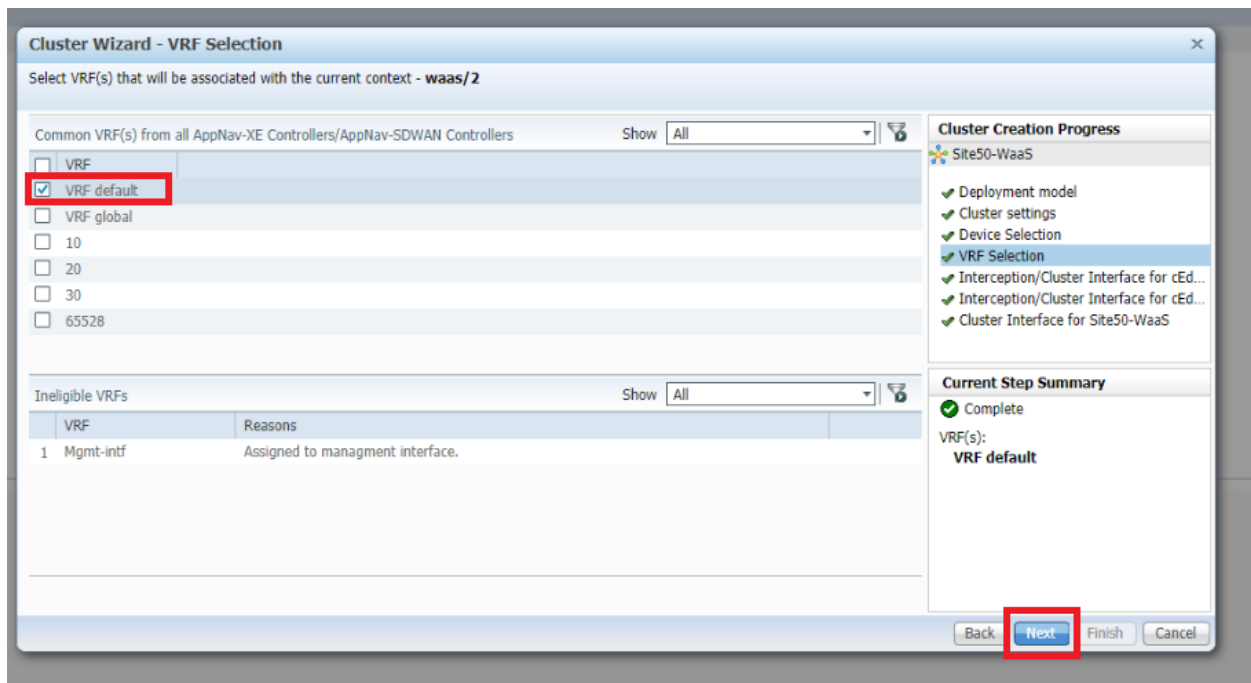
13. Select the **AppNav IOS Devices** as *AppNav-SDWAN*



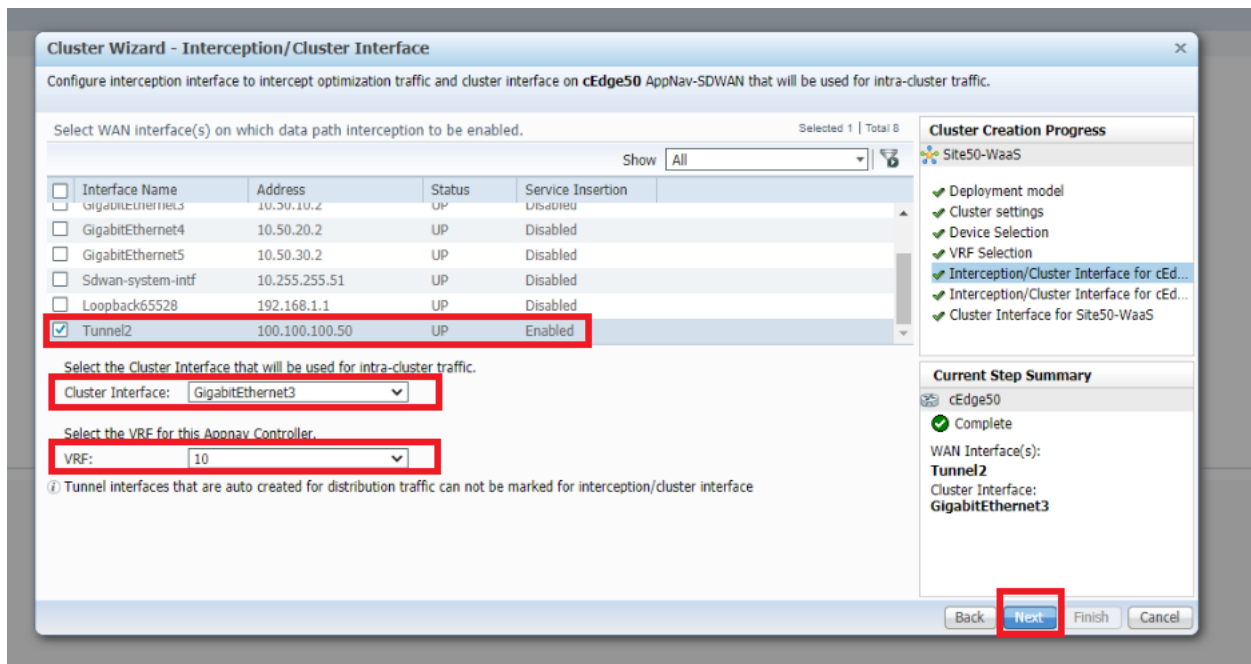
14. Select *cEdge50* and *cEdge51* in the upper half of the window and *Site50-WaaS* in the lower half. We're choosing the components of our cluster over here. Click on **Next**



15. Select *VRF default* and click on **Next**. This associates all VRFs with the context *waas/2*



16. Select *Tunnel2* as the WAN interfaces on which data path interception should be enabled. Make sure the **Cluster Interface** is set to *GigabitEthernet3* and the VRF is *10*. Click on **Next**. This is for *cEdge50*



17. Select *Tunnel2* as the WAN interfaces on which data path interception should be enabled. Make sure the **Cluster Interface** is set to *GigabitEthernet3* and the VRF is *10*. Click on **Next**. This is for *cEdge51*

Cluster Wizard - Interception/Cluster Interface

Configure interception interface to intercept optimization traffic and cluster interface on **cEdge51** AppNav-SDWAN that will be used for intra-cluster traffic.

Select WAN interface(s) on which data path interception to be enabled. Selected 1 | Total 8

Interface Name	Address	Status	Service Insertion
GigabitEthernet3	10.50.10.3	UP	Disabled
GigabitEthernet4	10.50.20.3	UP	Disabled
GigabitEthernet5	10.50.30.3	UP	Disabled
Sdwan-system-intf	10.255.255.52	UP	Disabled
Loopback65528	192.168.1.1	UP	Disabled
<input checked="" type="checkbox"/> Tunnel2	192.1.2.22	UP	Enabled

Select the Cluster Interface that will be used for intra-cluster traffic.

Cluster Interface: GigabitEthernet3

Select the VRF for this Appnav Controller.

VRF: 10

Tunnel interfaces that are auto created for distribution traffic can not be marked for interception/cluster interface

Cluster Creation Progress

- Site50-WaaS
- Deployment model
- Cluster settings
- Device Selection
- VRF Selection
- Interception/Cluster Interface for cEd...
- Interception/Cluster Interface for cEd...
- Cluster Interface for Site50-WaaS

Current Step Summary

cEdge51

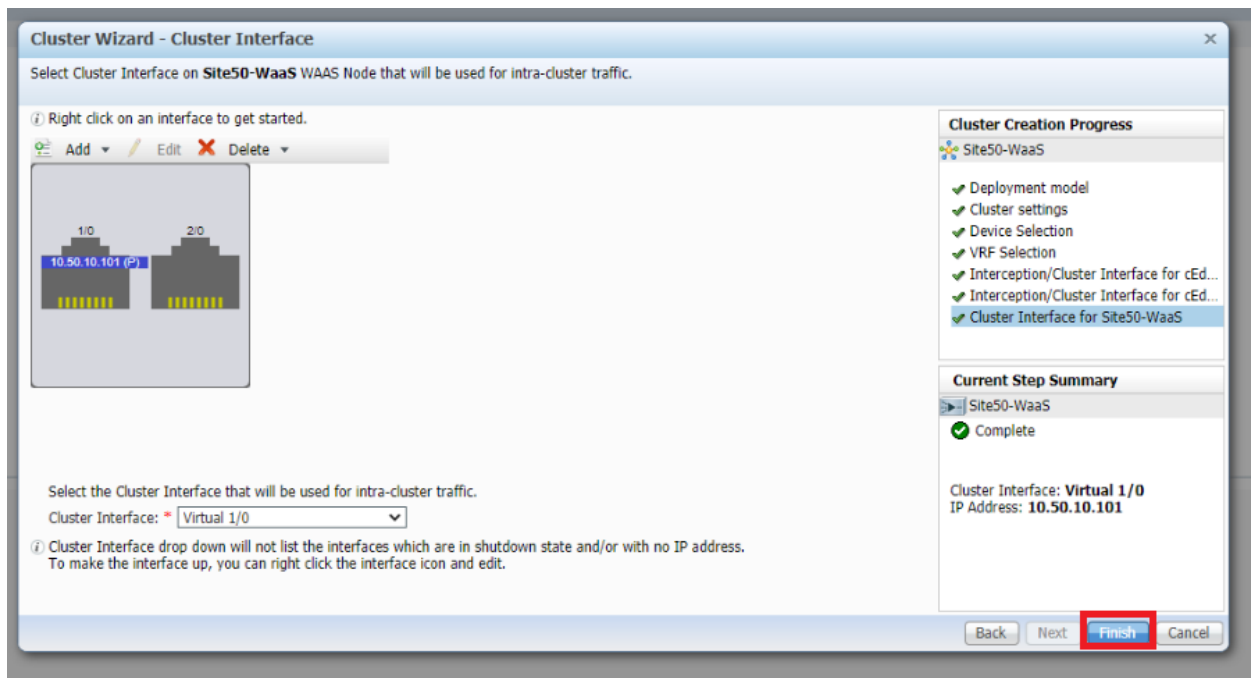
- Complete

WAN Interface(s):
Tunnel2

Cluster Interface:
GigabitEthernet3

Back Next Finish Cancel

18. Click on **Finish**, making sure the cluster interface is set to **Virtual 1/0**



19. Wait for approximately 8 minutes and head over to the AppNav Cluster section on WCM, clicking on **All AppNav Clusters**. Both clusters we just created should be operational

Manage AppNav Clusters

AppNav Cluster Wizard ✖ Delete

Name	Type	Description	AppNav Cluster Status
<input checked="" type="radio"/> Site50-WaaS	AppNav-SDWAN Cluster	Site50-WaaS	<input checked="" type="checkbox"/> AppNav Cluster is operational
<input type="radio"/> Site40-WaaS	AppNav-SDWAN Cluster	Site40-WaaS	<input checked="" type="checkbox"/> AppNav Cluster is operational

We have created the AppNav Clusters and applied some default policies. Traffic optimization should be in effect. This will be verified in the next section.

Task List

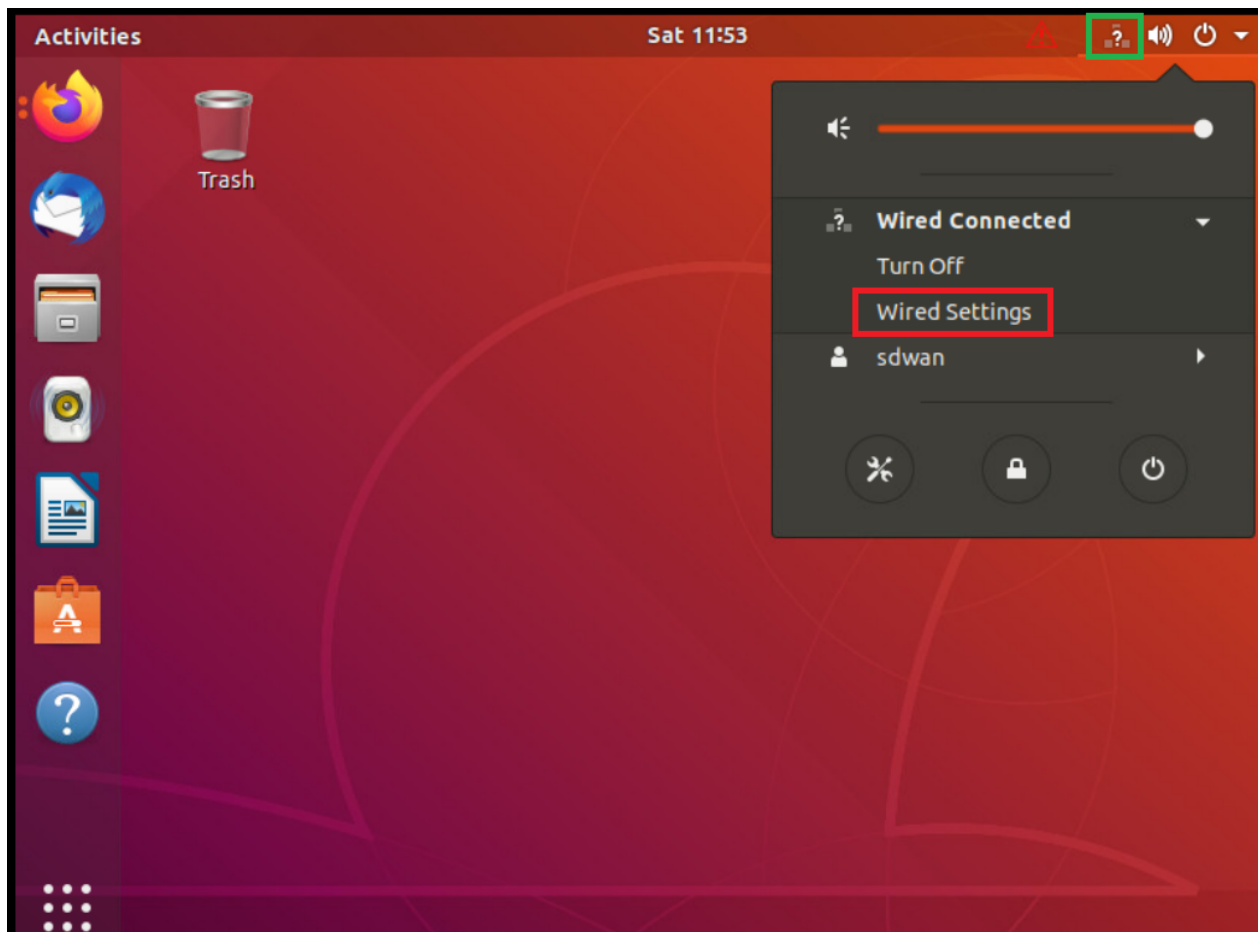
- [Overview](#)
- [Adding WAAS Nodes to WCM](#)

- [Downloading vManage certs and Enabling DIA at Site DC](#)
- [Integrating vManage and WCM](#)
- [Discovering the AppNav XE Controllers](#)
- [Setting up the AppNav Clusters](#)
- Verification and Testing

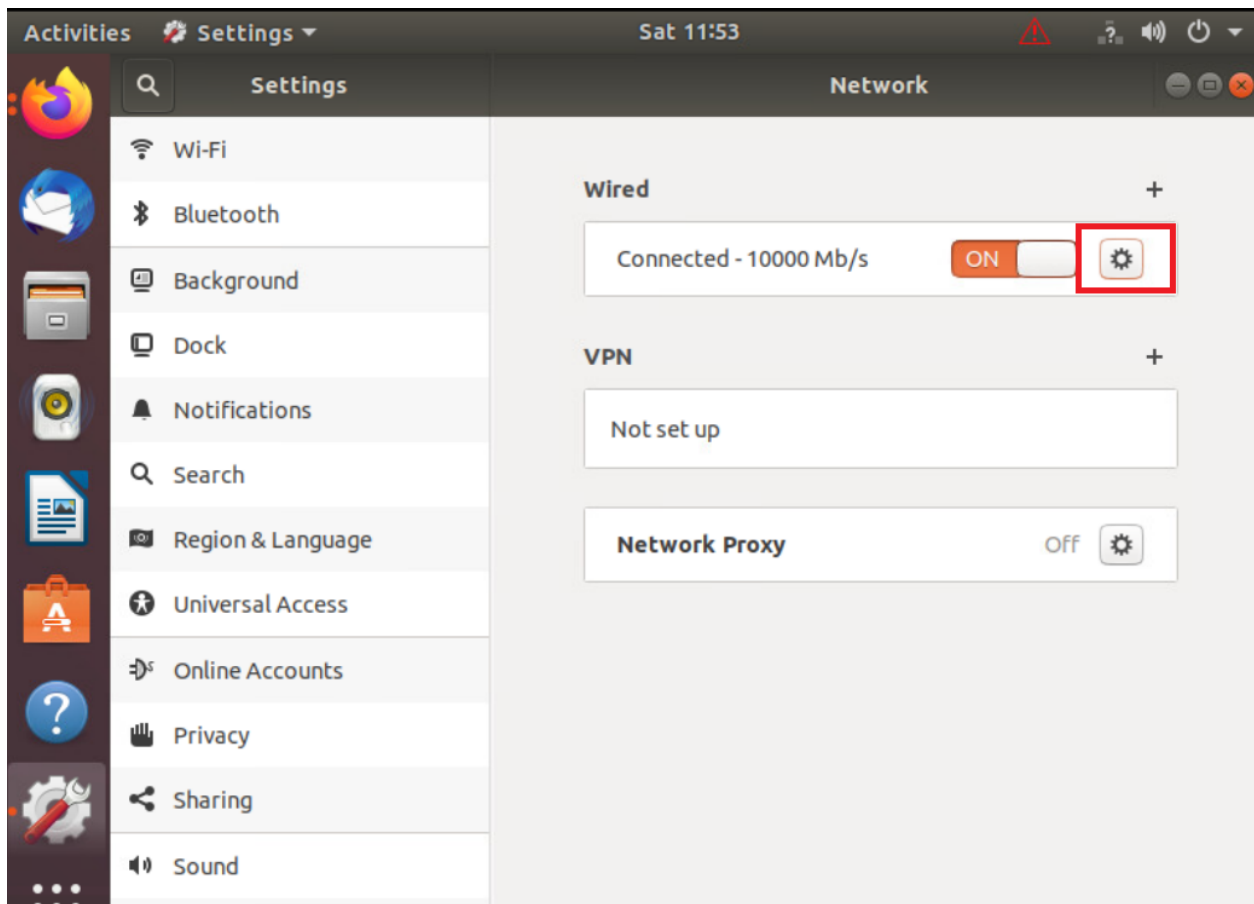
Verification and Testing

We will be testing things out in VPN 10 and generating HTTP traffic in that VPN from Site 40 to Site 50. A few changes will need to be made on the workstations available at Site 40 and Site 50, post which we can begin verification.

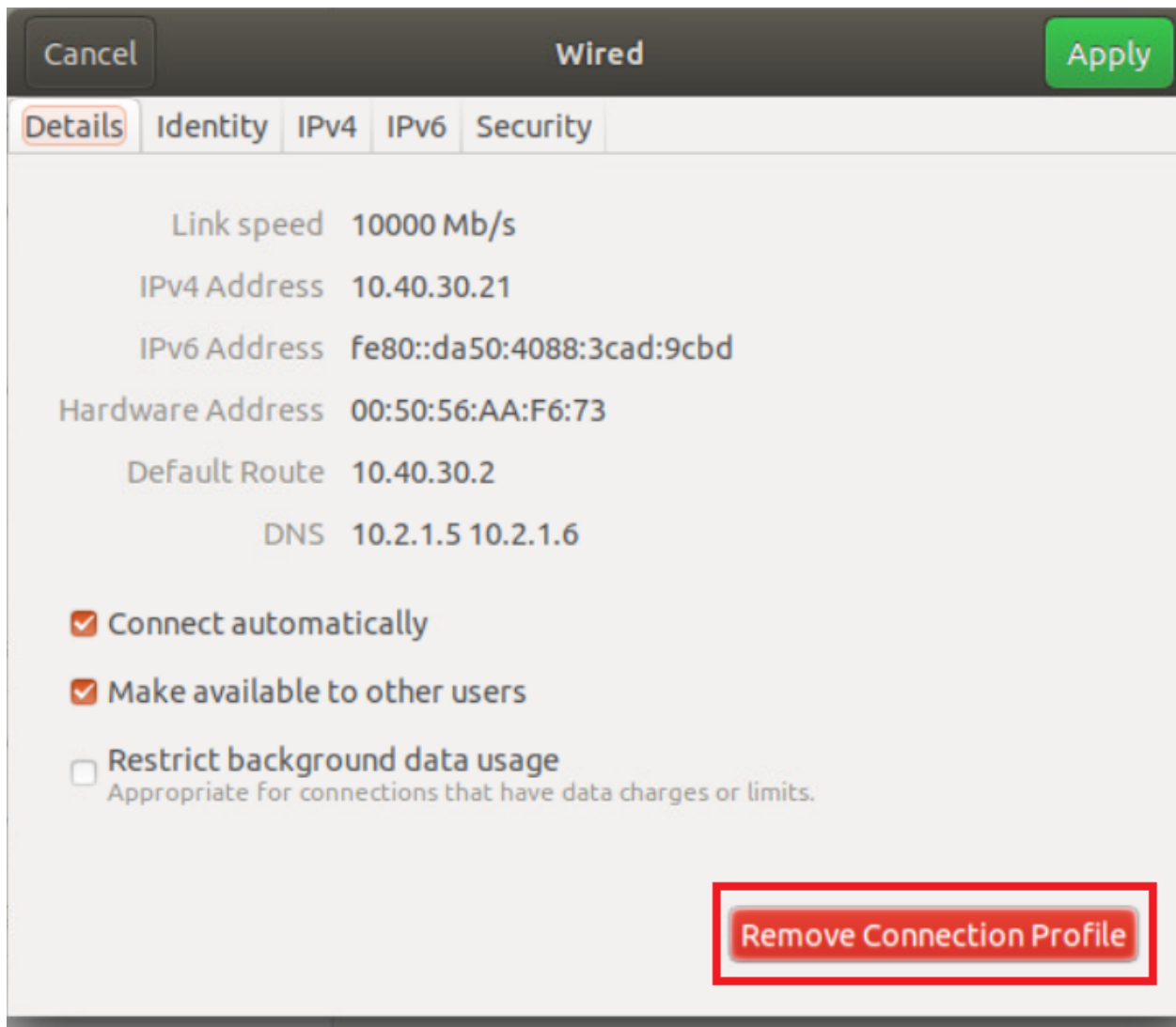
1. Log in to vCenter (use the bookmark or go to 10.2.1.50/ui) using the credentials provided to you. Locate the *sdwan-slc/ghi-site40pc-podX* VM and click on it. Open the Web Console to the Site 40 PC VM and log in. The Username is sdwan and the password is C1sco12345. Click the network icon in the top-right corner and go to Wired Settings



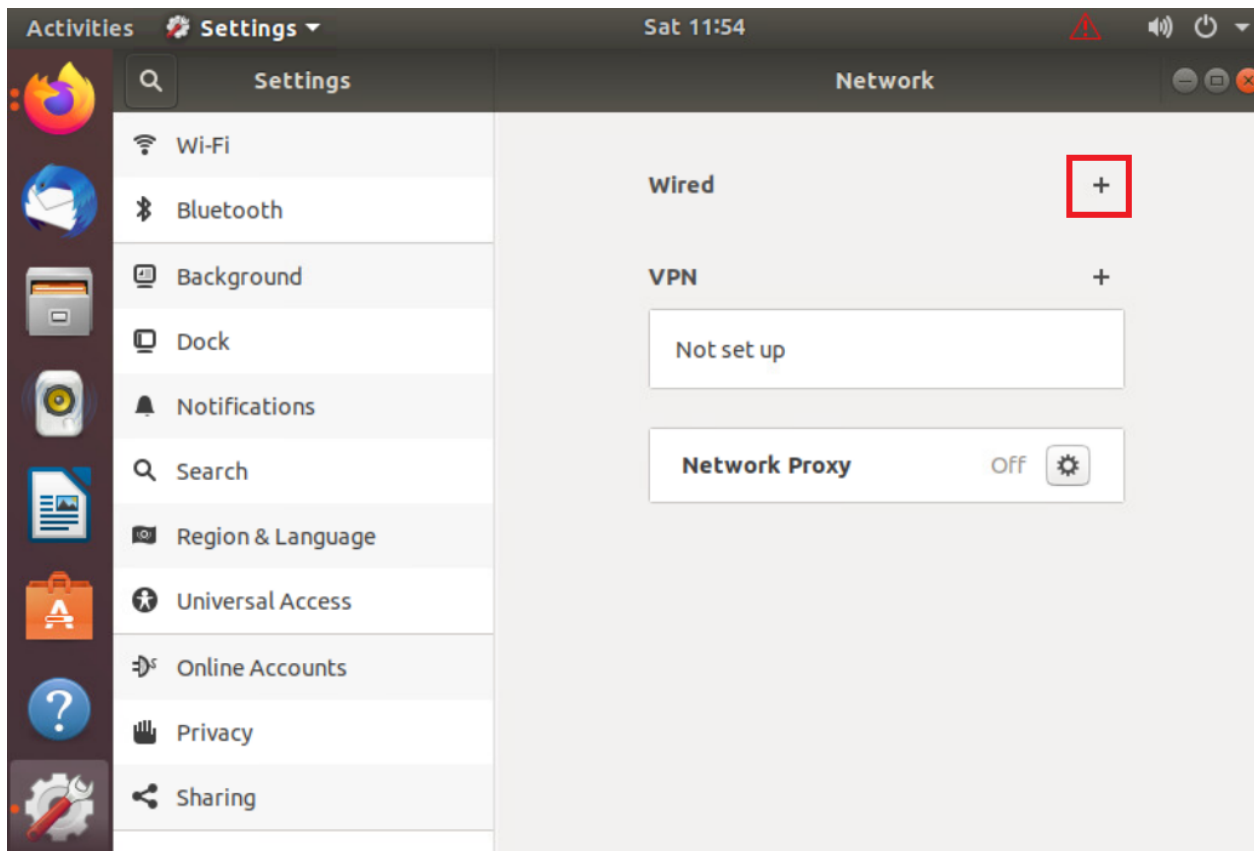
2. Click on the cog wheel/gear icon



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).

Cancel **New Profile** Add

Identity IPv4 IPv6 Security

IPv4 Method Automatic (DHCP) Link-Local Only
 Manual Disable

Addresses

Address	Netmask	Gateway	
10.40.10.21	255.255.255.0	10.40.10.2	✕
			✕

DNS Automatic OFF

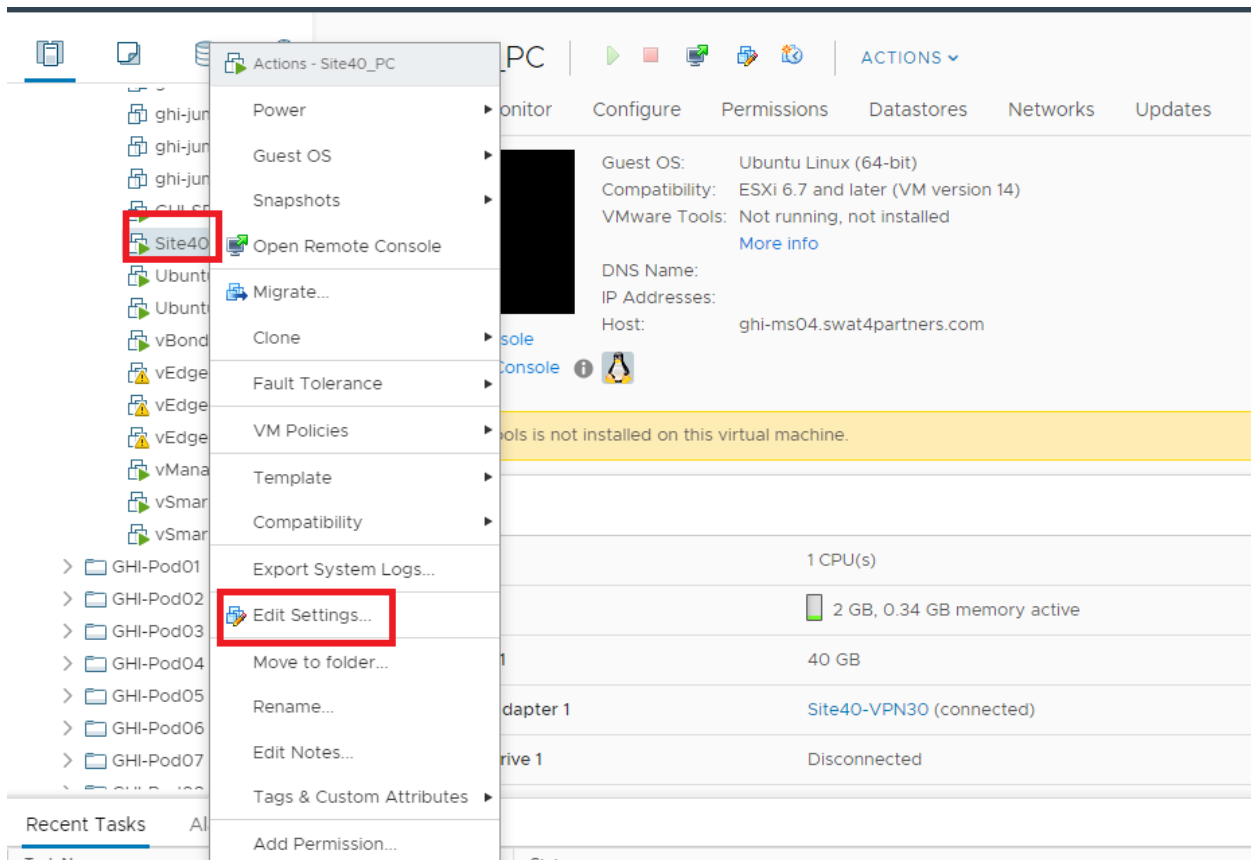
10.2.1.5, 10.2.1.6

Separate IP addresses with commas

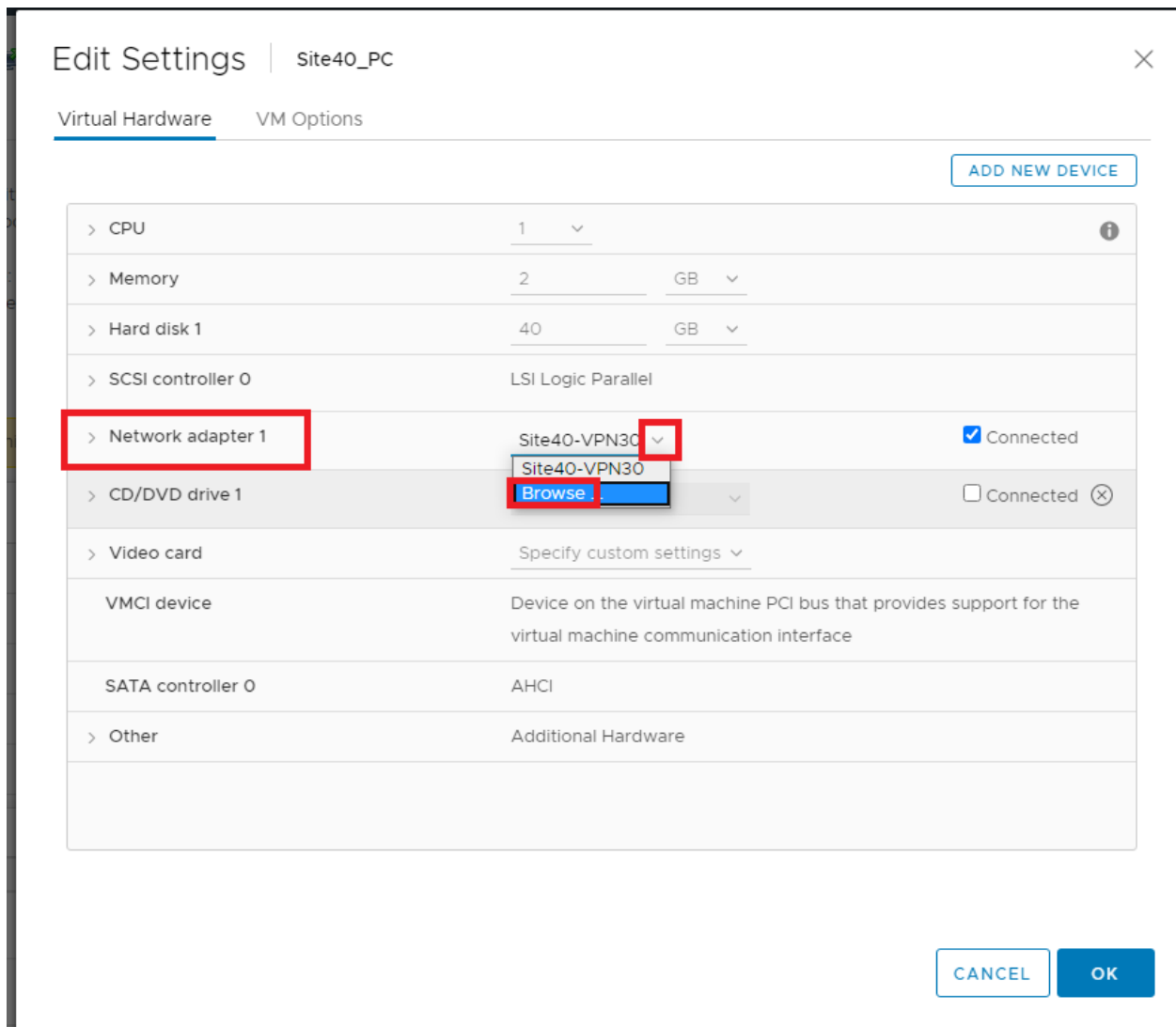
Routes Automatic ON

Address	Netmask	Gateway	Metric	
				✕

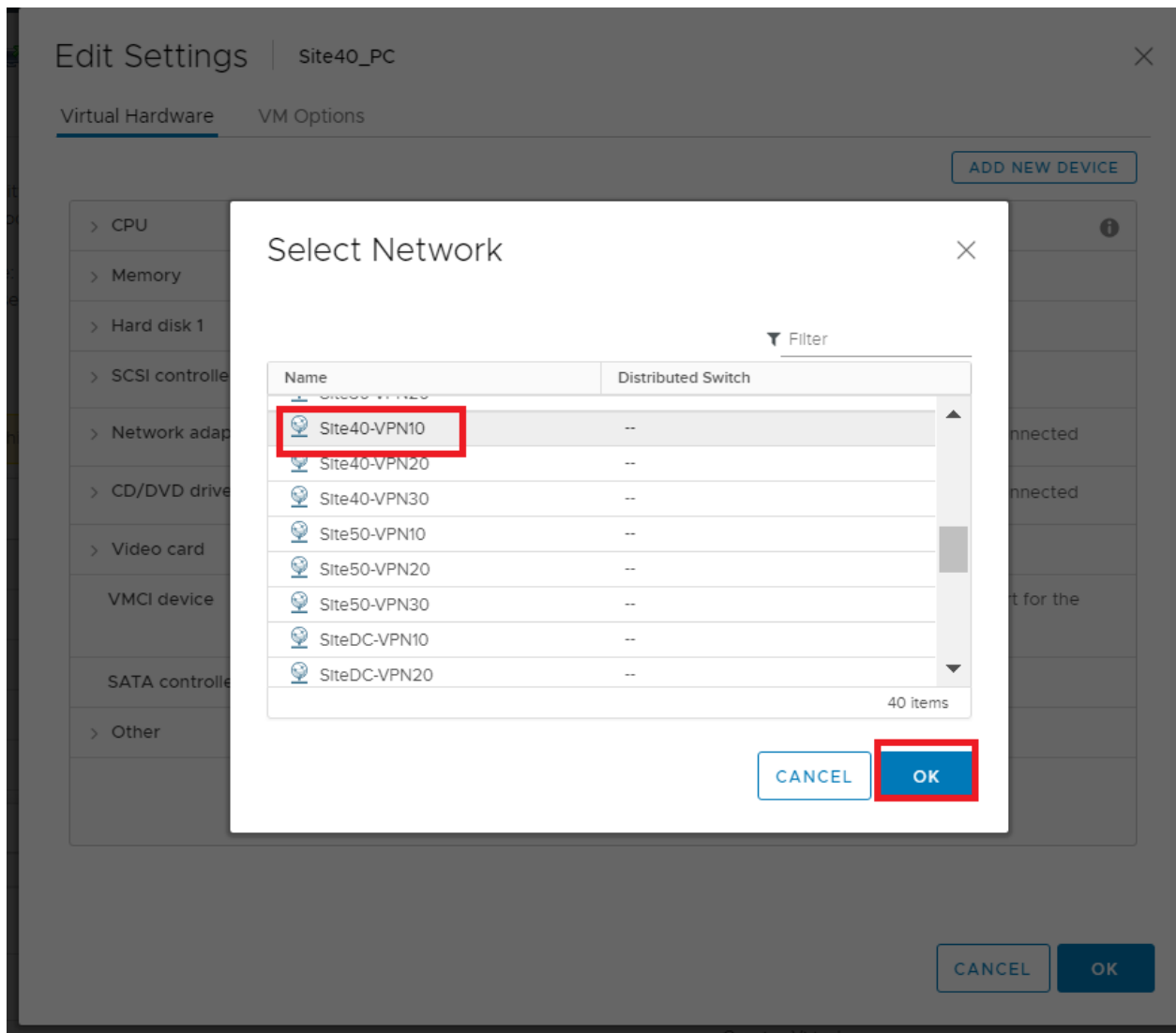
6. Back at the vCenter screen, right click on the Site40PC (named sdwan-slc/ghi-site40pc-podX) for your POD and click on **Edit Settings** (image as an example only)



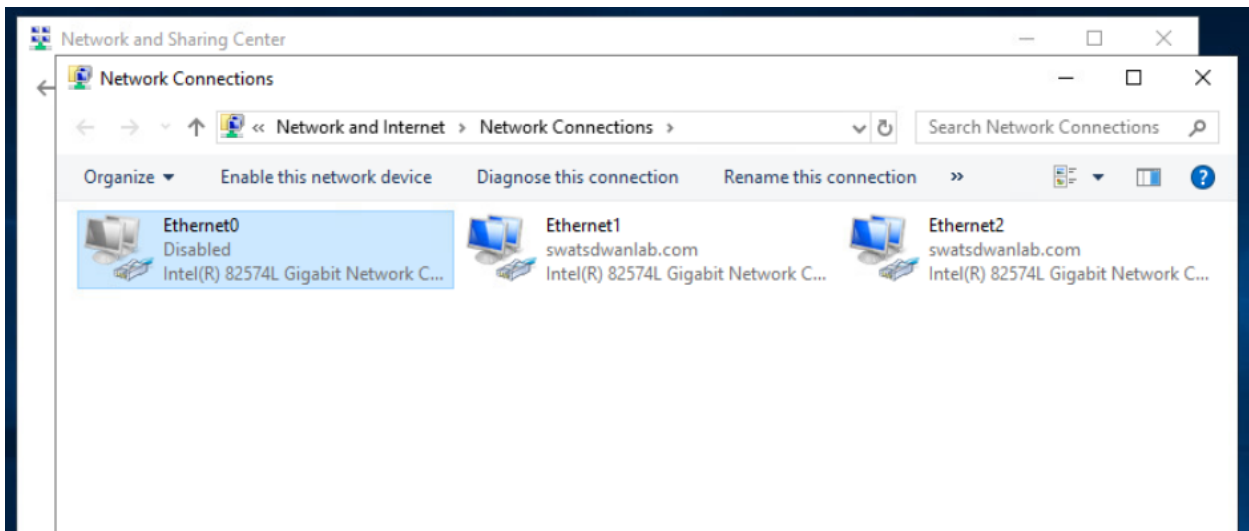
7. Under **Network Adapter 1** click on the drop down and click **Browse**



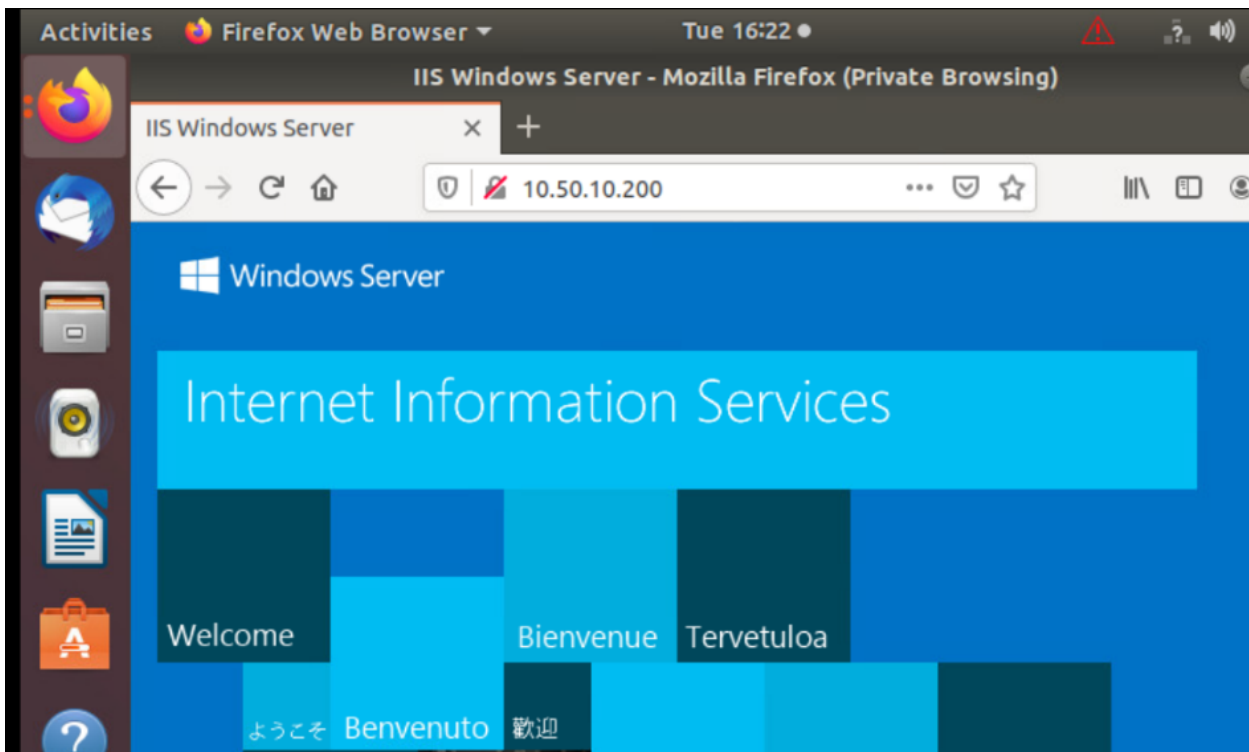
8. Select *Site40-VPN10* from the list of Networks and click on **OK**. Click on **OK** again. The Site 40 PC is now in VPN 10



9. Back at vCenter, console in to *sdwan-ghi/slc-ad-podX*. The username is administrator and the password is C1sco12345. Click on **Start** and type *ncpa.cpl* to open the Network Connections. Right click on Ethernet0 and **Disable** it. Right click on Ethernet2 and **Enable** the adapter



10. Go to the Site 40 PC console session and open Firefox. Access 10.50.10.200 via the browser - it should open an IIS page. Open multiple tabs to the same IP so as to generate some web traffic



11. SSH to the Site40-WaaS Node (IP of 10.40.10.101) or console in via vCenter (VM name is *sdwan-ghi/slc-site40waas-podX*). Log in via the username of admin and a password of default and enter the command `show statistics connection`

The screenshot displays the vSphere Client interface. The left sidebar shows a tree view of the environment, with the VM 'sdwan-ghi-site40waas-podx' selected. The main pane shows the VM's summary and hardware configuration.

VM Summary:

- Guest OS: Other 2.6.x Linux (64-bit)
- Compatibility: ESXi 5.5 and later (VM version 10)
- VMware Tools: Running, version:2147483647 (Guest Managed)
- DNS Name: Site40-WaaS
- IP Addresses: 10.40.10.101
- Host: ghi-ms03.swat4partners.com

VM Hardware:

Component	Configuration
CPU	1 CPU(s)
Memory	3.02 GB, 0.18 GB memory active
Hard disk 1	4 GB
Hard disk 2	160 GB
Network adapter 1	Site40-VPN10 (connected)
Network adapter 2	Site40-VPN10 (connected)
CD/DVD drive 1	Connected
Floppy drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual communication interface
Other	Additional Hardware

```

Site40-WaaS#
Site40-WaaS#show statistics connection

Current Active Optimized Flows: 1
  Current Active Optimized TCP Plus Flows: 1
  Current Active Optimized TCP Only Flows: 0
  Current Active Optimized Single Sided Flows: 0
  Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows: 0
Current Reserved Flows: 10
Current Active Pass-Through Flows: 1
Historical Flows: 1

D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOLM,C:SMB,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN SECURE,s:SSL
Interposer

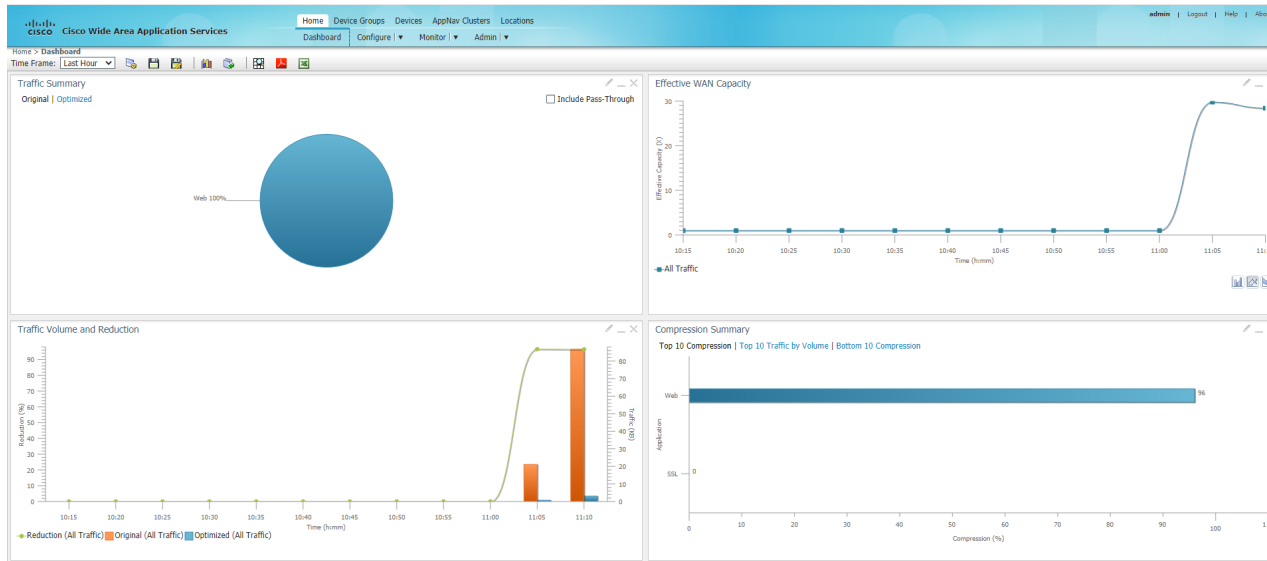
ConnID      Source IP:Port      Dest IP:Port      PeerID Accel RR
 2819      10.40.10.21:48912   10.50.10.200:80  00:50:56:aa:39:f7 THDL 98.0%

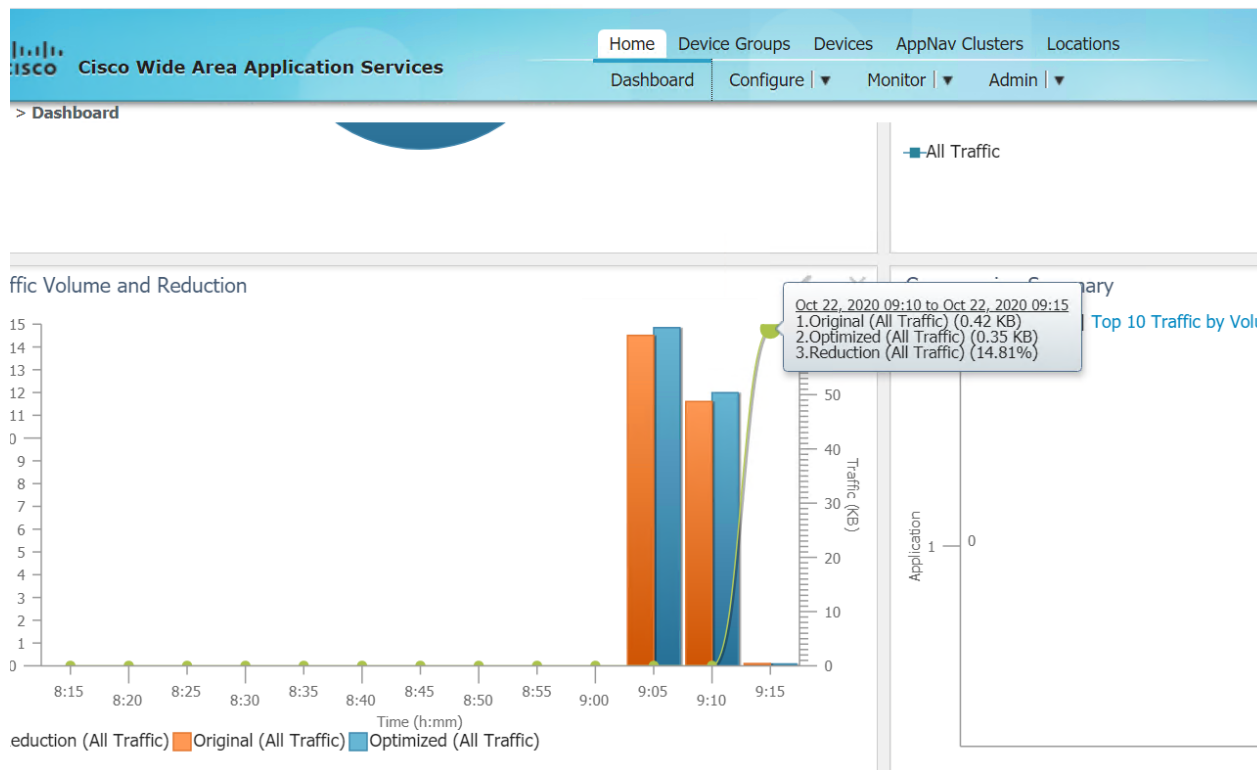
Local IP:Port      Remote IP:Port      Peer ID      ConnType
10.40.10.101:49238 10.100.10.100:443   N/A          Internal Client

```

We can see that the web traffic is showing up in the output and it has a Reduction Ratio (RR) of 98% in this example. The RR will vary.

12. On the WCM GUI, navigate to the main dashboard by clicking on **Home**. You should see traffic being optimized





This completes the integration of WAAS with Cisco SD-WAN.

Task List

- [Overview](#)
- [Adding WAAS Nodes to WCM](#)
- [Downloading vManage certs and Enabling DIA at Site DG](#)
- [Integrating vManage and WCM](#)
- [Discovering the AppNav XE Controllers](#)
- [Setting up the AppNav Clusters](#)
- [Verification and Testing](#)



-->

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.

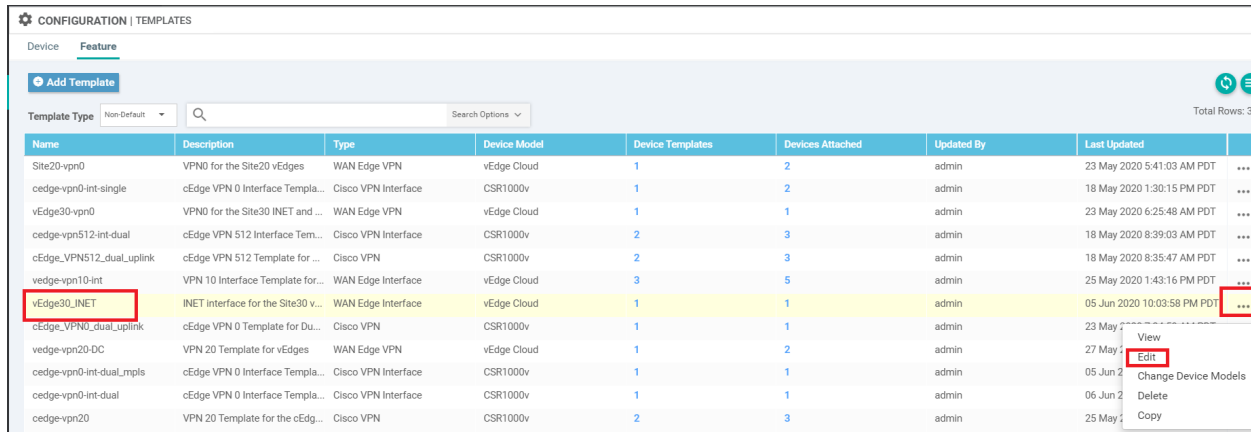
Cloud OnRamp for SaaS monitors widely used Cloud Applications and arrives at a vQoE score (Viptela Quality of Experience). Loss and latency are used to calculate the vQoE score and based on this, the solution routes traffic to the Cloud Application via the optimal path. The vQoE value is calculated periodically 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



CONFIGURATION | TEMPLATES

Device Feature

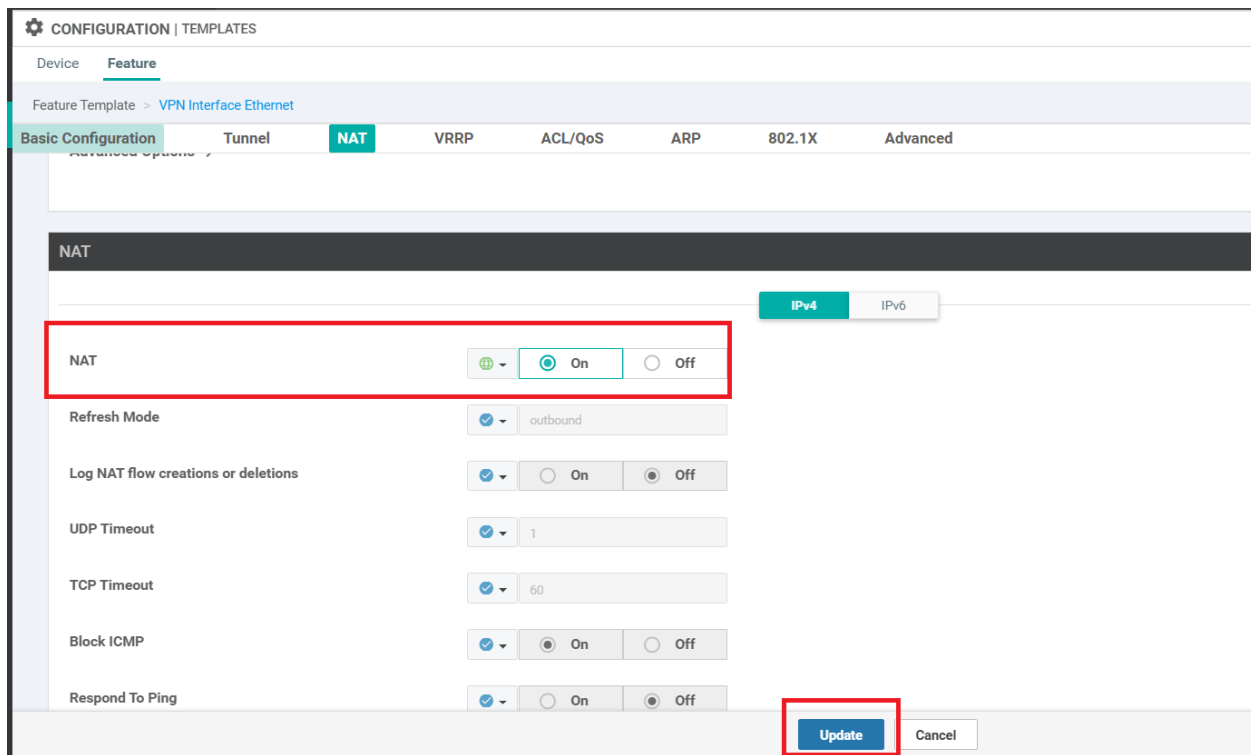
Add Template

Template Type: Non-Default

Total Rows: 37

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	...
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 6:25:48 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 2020 10:03:58 PM PDT	View
vedge-vpn20-DC	VPN 20 Template for vEdges	WAN Edge VPN	vEdge Cloud	1	2	admin	27 May 2020 10:03:58 PM PDT	Edit
cedge-vpn0-int-dual_mpls	cEdge VPN 0 Interface Templa...	Cisco VPN Interface	CSR1000v	1	1	admin	05 Jun 2020 10:03:58 PM PDT	Change Device Models
cedge-vpn0-int-dual	cEdge VPN 0 Interface Templa...	Cisco VPN Interface	CSR1000v	1	1	admin	06 Jun 2020 10:03:58 PM PDT	Delete
cedge-vpn20	VPN 20 Template for the cEdg...	Cisco VPN	CSR1000v	2	3	admin	25 May 2020 10:03:58 PM PDT	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

Note: This step is not required if you have gone through the WAAS Integration. Please skip to the next section if WAAS integration has been done.

CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type: Non-Default Search Options

Total Rows: 7 of 37

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	
vedge-vpn20-DC	VPN 20 Template for vEdges	WAN Edge VPN	vEdge Cloud	1	2	admin	27 May 2020 2:43:36 PM PDT	...
DC-vEdge_mgmt_int	MGMT interface for the DC-vE...	WAN Edge Interface	vEdge Cloud	3	5	admin	23 May 2020 1:49:11 AM PDT	...
DC-vEdge_MPLS	MPLS interface for the DC-vEd...	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 1:43:22 AM PDT	...
DC-vEdge_INET	INET interface for the DC-vEdg...	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 1:43:22 AM PDT	View
DCvEdge-vpn512	VPN512 for the DC-vEdges	WAN Edge VPN	vEdge Cloud	3	5	admin	23 May 2020 1:43:22 AM PDT	Edit
DCvEdge-vpn0	VPN0 for the DC-vEdges INET...	WAN Edge VPN	vEdge Cloud	1	2	admin	23 May 2020 1:43:22 AM PDT	Change Device Models Delete Copy

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**

Note: This step is not required if you have gone through the WAAS Integration. Please skip to the next section if WAAS integration has been done.

Basic Configuration Tunnel **NAT** VRRP ACL/QoS ARP 802.1X Advanced

NAT

IPv4 IPv6

NAT On Off

Refresh Mode outbound

Log NAT flow creations or deletions On Off

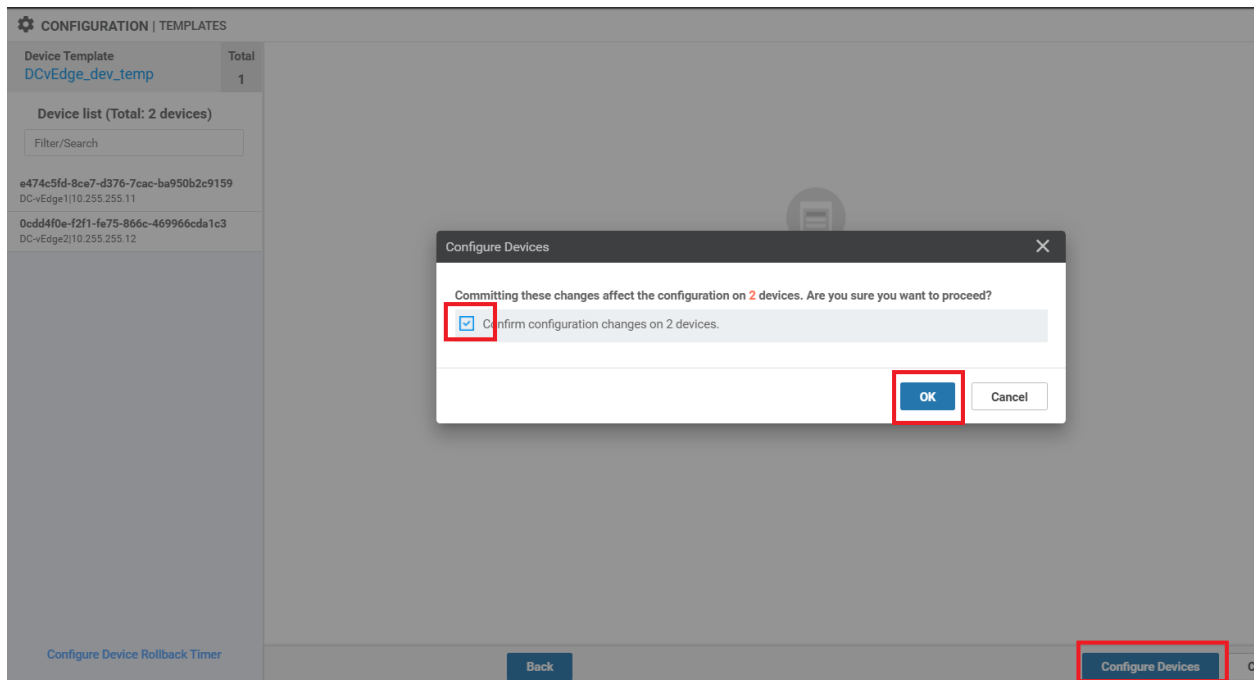
UDP Timeout 1

TCP Timeout 60

Block ICMP On Off

Respond To Ping On Off

Update Cancel



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.

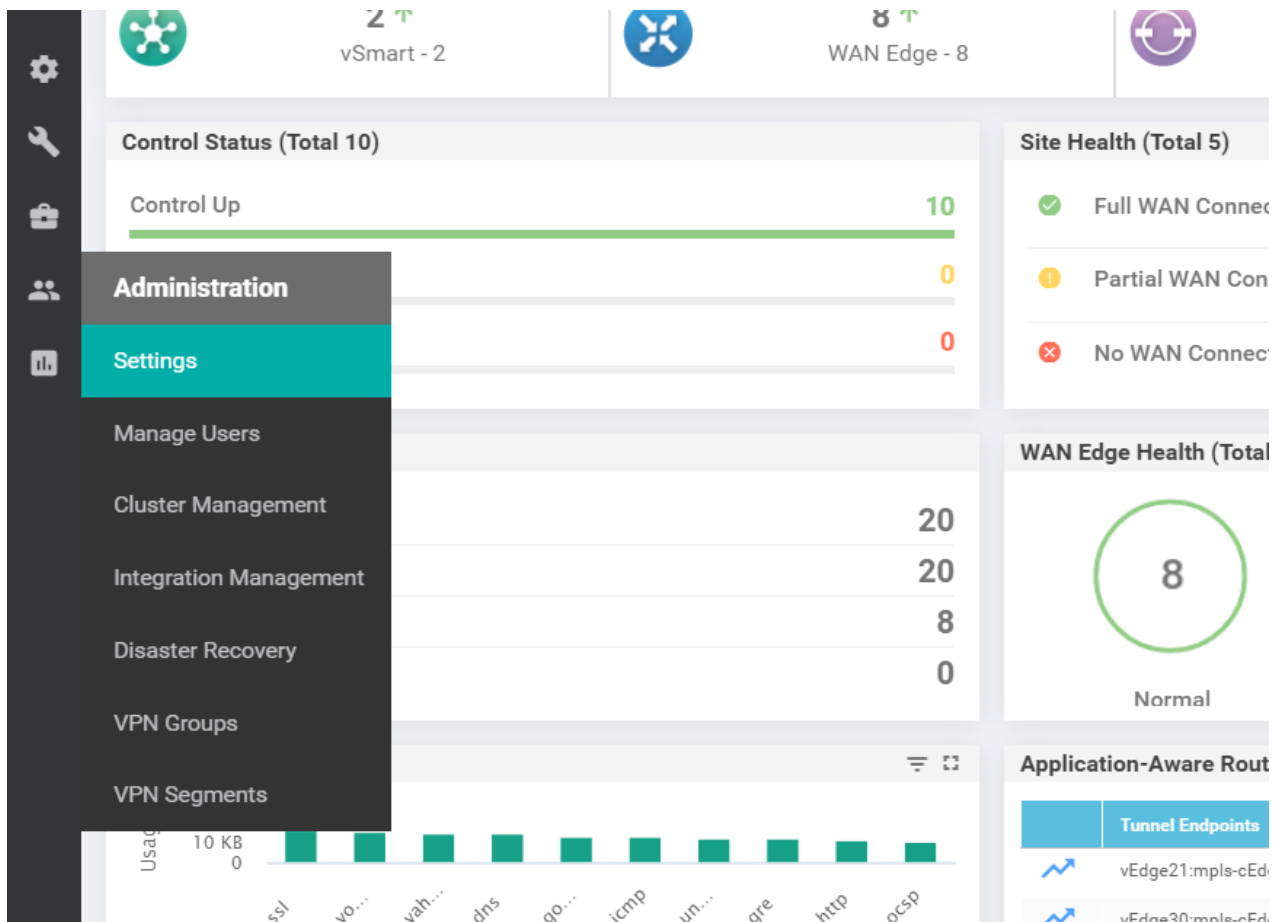
Task List

- [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**



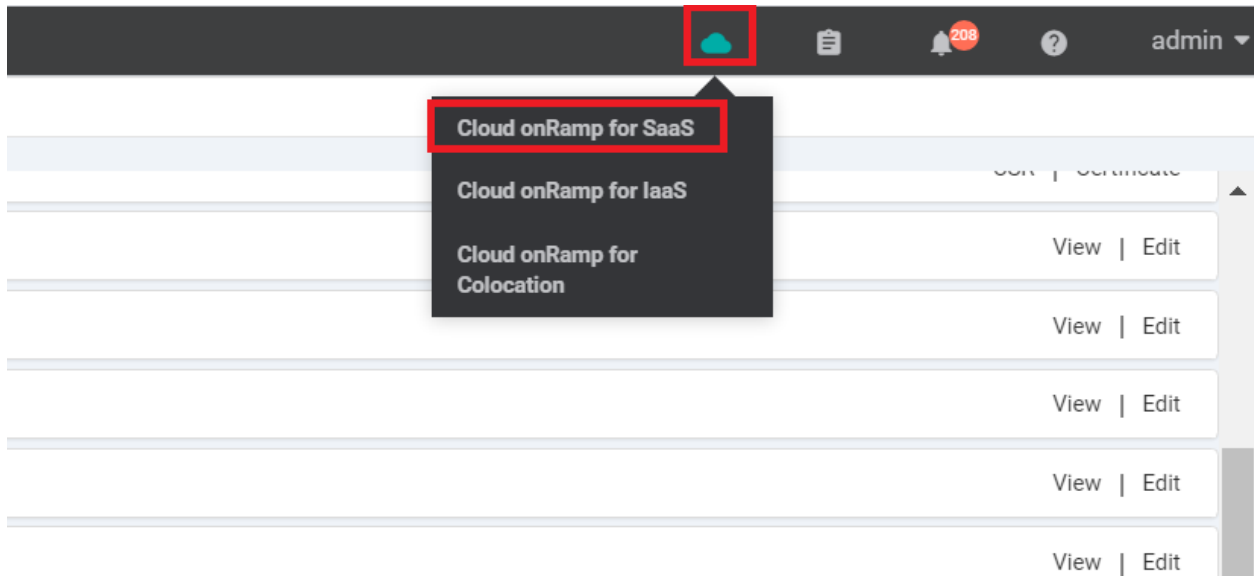
2. Locate the **Cloud onRamp for SaaS** section and click on **Edit**. Set the radio button to **Enabled** and click on **Save**. Cloud OnRamp for SaaS needs to be enabled system wide before it can be used

The **Statistics Setting** page shows the following configuration:

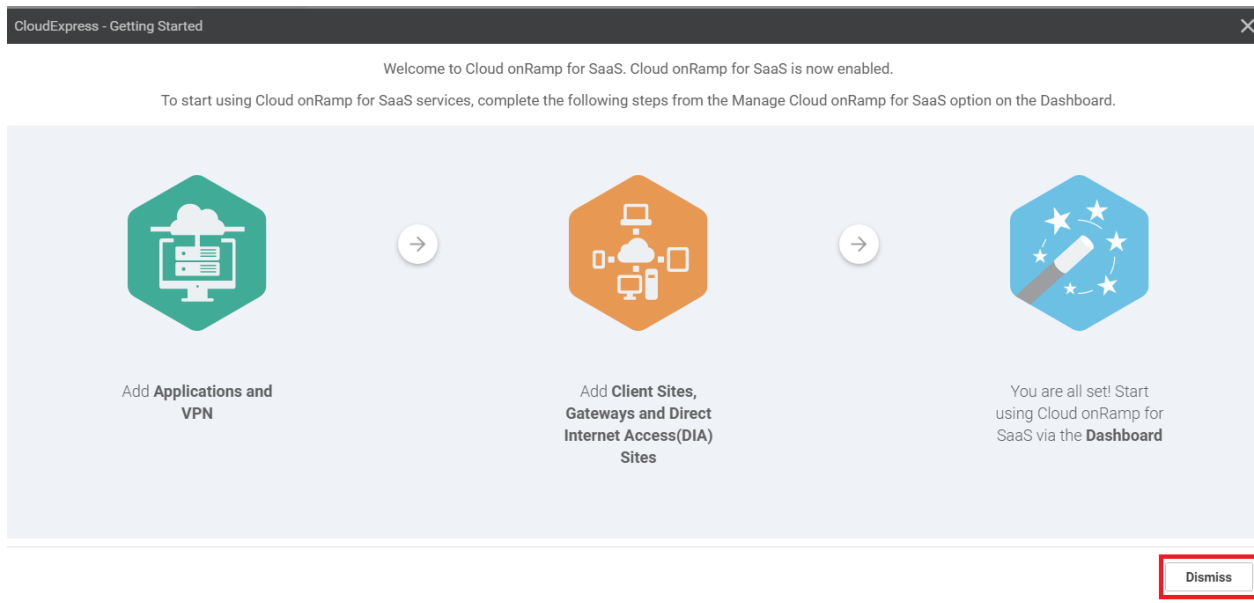
- Cloud onRamp for SaaS:** Disabled
- Enable CloudExpress:** Enabled Disabled
- Manage Encrypted Password:** Disabled
- vAnalytics:** Disabled

The **Save** button is highlighted in red.

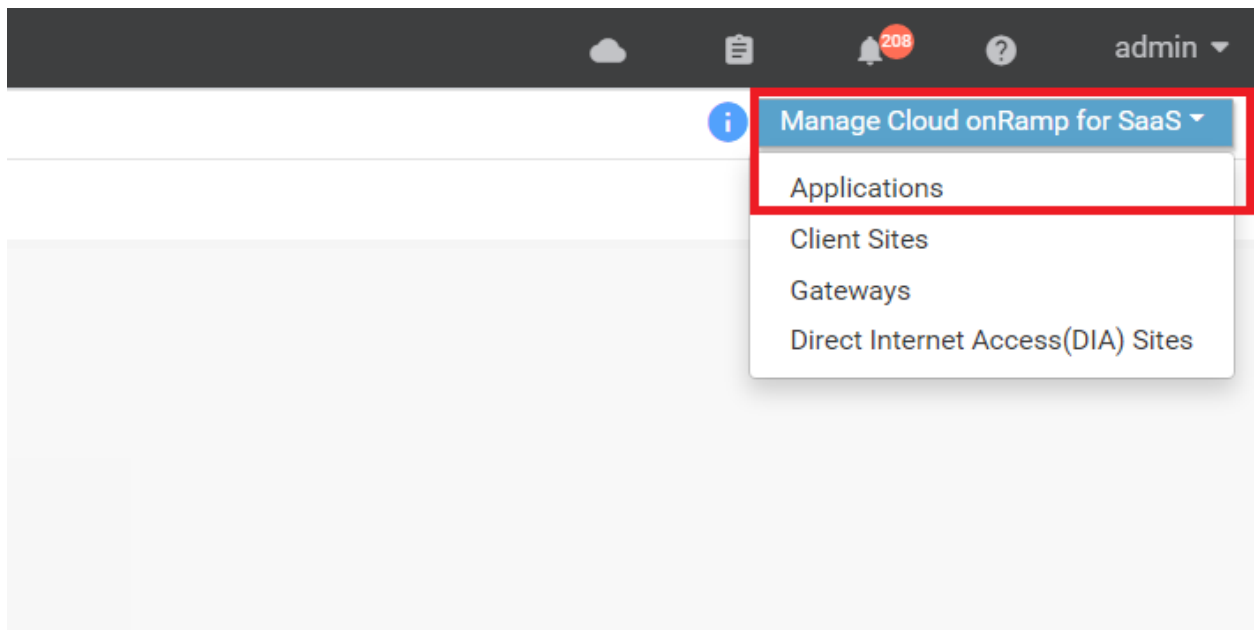
3. Once enabled, click on the **Cloud** icon in the top right-hand of the screen and click on **Cloud onRamp for SaaS**



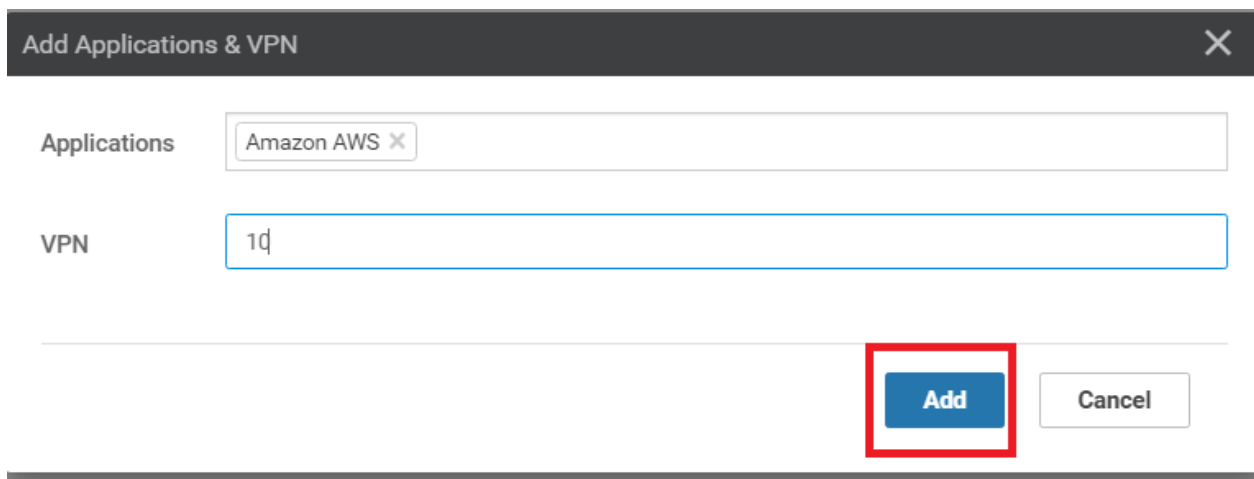
4. Click on **Dismiss**



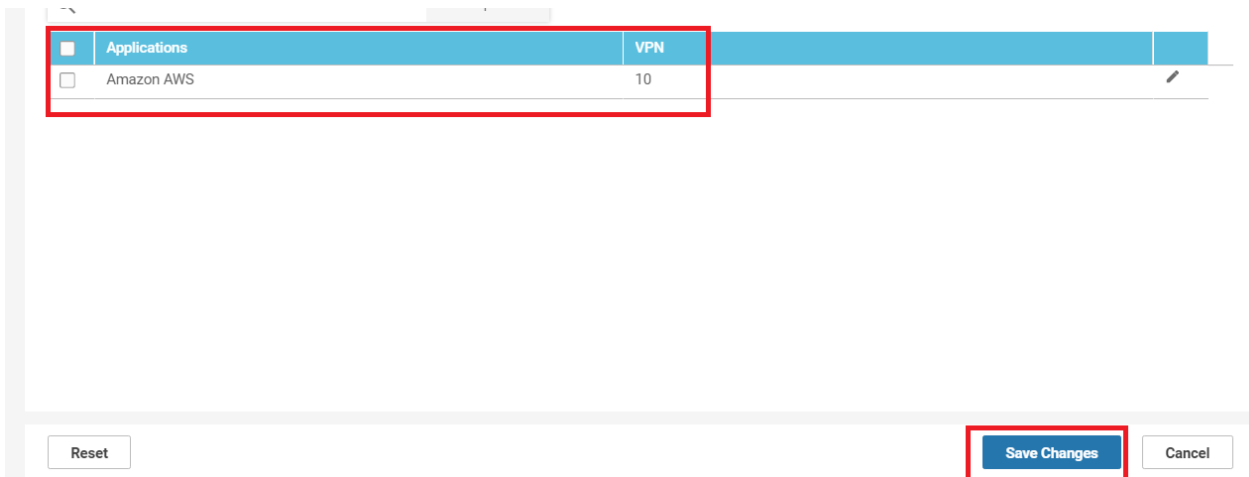
5. Click on **Manage Cloud onRamp for SaaS** (top right-hand corner) and click on **Applications**



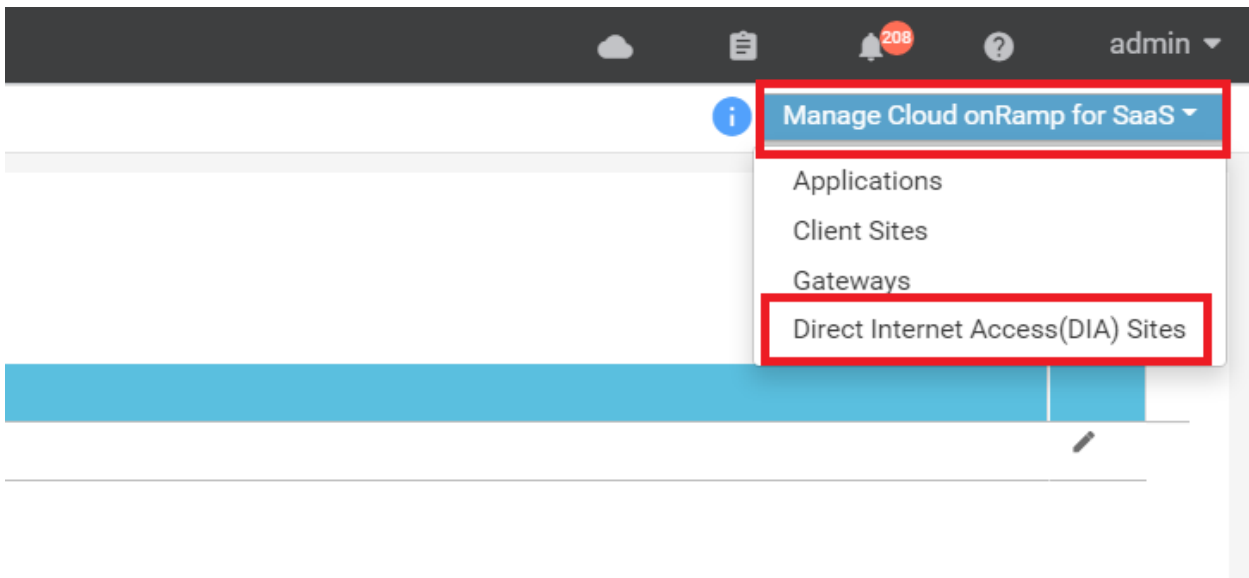
6. Specify a random application (example shows Amazon AWS, but you can choose something else like Oracle or Google Apps) and populate a **VPN** of 10



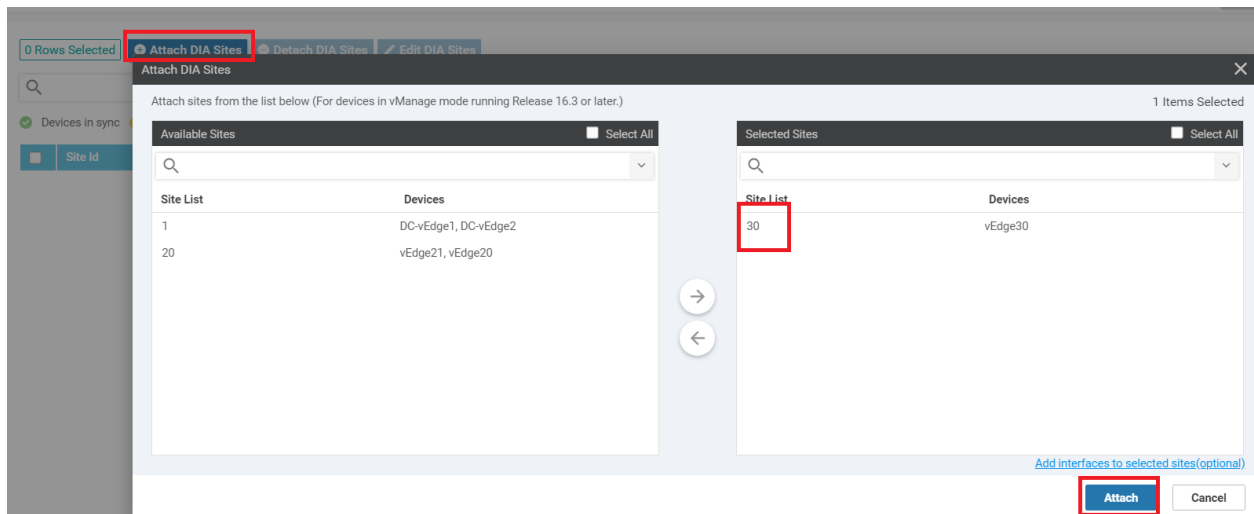
7. Make sure the chosen Application shows up and click on **Save Changes**



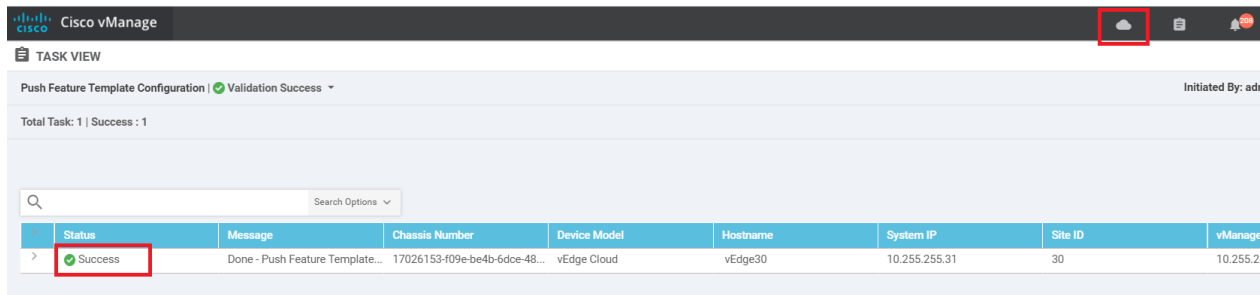
8. Click on **Cloud onRamp for SaaS** (top right-hand corner) again and click on **Direct Internet Access (DIA) Sites**



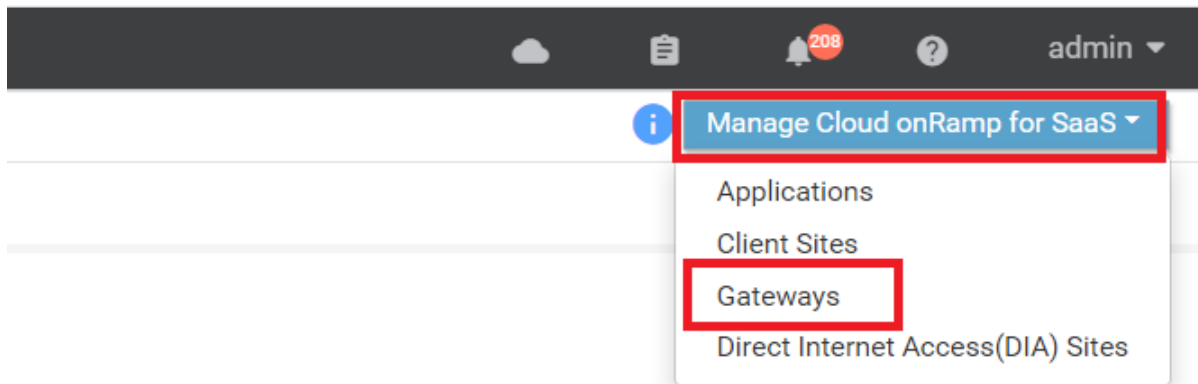
9. Click on **Attach DIA Sites** and move Site 30 to the **Selected Sites** section. Click on **Attach**



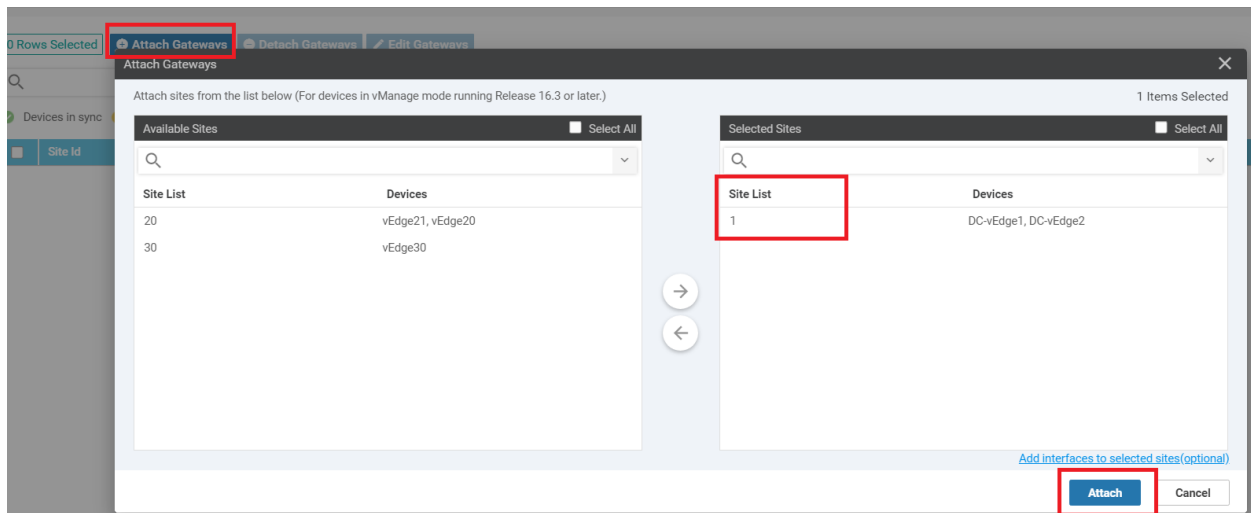
10. Wait for the task to go through successfully. Once it is done, click on the **Cloud** icon in the top right corner and click **Cloud onRamp for SaaS**



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?)

VPN List VPN-10

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

VPN List VPN-10

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

Total Rows: 3

Cisco vManage CONFIGURATION Cloud onRamp for SaaS > Amazon AWS

VPN List VPN-10

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 templates in a web interface. The table has columns for Name, Description, Type, Device Model, Device Templates, Devices Attached, Updated By, and Last Updated. The 'vEdge30_INET' template is highlighted in yellow. A context menu is open over the 'vEdge30_INET' row, with 'Edit' selected.

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	...
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_mgmtL_int	MGMT interface for the DC-vE...	WAN Edge Interface	vEdge Cloud	3	5	admin	23 May 2020 9:49:46 AM PDT	...
vedge-vpn20-int	VPN 20 Interface Template for...	WAN Edge Interface	vEdge Cloud	3	5	admin	25 May 2020 1:43:16 PM PDT	...
vedge-vpn20	VPN 20 Template for vEdges	WAN Edge VPN	vEdge Cloud	2	3	admin	25 May 2020 1:43:16 PM PDT	...
DC-vEdge_MPLS	MPLS interface for the DC-vEd...	WAN Edge Interface	vEdge Cloud	1	2	admin	23 May 2020 9:49:46 AM PDT	...
DC-OSPF	OSPF Template for the DC	OSPF	vEdge Cloud	1	2	admin	25 May 2020 1:43:16 PM PDT	...
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)	<input type="text" value="1"/>
QoS Map	<input type="text" value="WAN-QoS"/>
Rewrite Rule	<input checked="" type="checkbox"/>
Ingress ACL - IPv4	<input checked="" type="checkbox"/> <input type="radio"/> On <input checked="" type="radio"/> Off
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

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: 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 Devices

'Configure' action will be applied to 1 device(s) attached to 1 device template(s).

49	dns 10.2.1.5 primary	49	dns 10.2.1.5 primary
50	dns 10.2.1.6 secondary	50	dns 10.2.1.6 secondary
51	interface ge0/0	51	interface ge0/0
52	ip address 100.100.100.30/24	52	ip address 100.100.100.30/24
53	nat	53	nat
54	!	54	!
55	tunnel-interface	55	tunnel-interface
56	encapsulation ipsec	56	encapsulation ipsec
57	color public-internet	57	color public-internet
58	allow-service all	58	allow-service all
59	no allow-service bgp	59	no allow-service bgp
60	allow-service dhcp	60	allow-service dhcp
61	allow-service dns	61	allow-service dns
62	allow-service icmp	62	allow-service icmp
63	no allow-service sshd	63	no allow-service sshd
64	no allow-service netconf	64	no allow-service netconf
65	no allow-service ntp	65	no allow-service ntp
66	no allow-service ospf	66	no allow-service ospf
67	no allow-service stun	67	no allow-service stun
68	allow-service https	68	allow-service https
69	!	69	!
70	no shutdown	70	no shutdown
71	qos-map WAN-QoS	71	shaping-rate 1
72	!	72	qos-map WAN-QoS
73	!	73	!
74	interface ge0/1	74	interface ge0/1
75	ip address 192.0.2.14/30	75	ip address 192.0.2.14/30
76	tunnel-interface	76	tunnel-interface
77	encapsulation ipsec	77	encapsulation ipsec

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

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)

Cisco vManage

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
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)

QoS Map

Rewrite Rule

Ingress ACL - IPv4 On Off

Egress ACL - IPv4 On Off

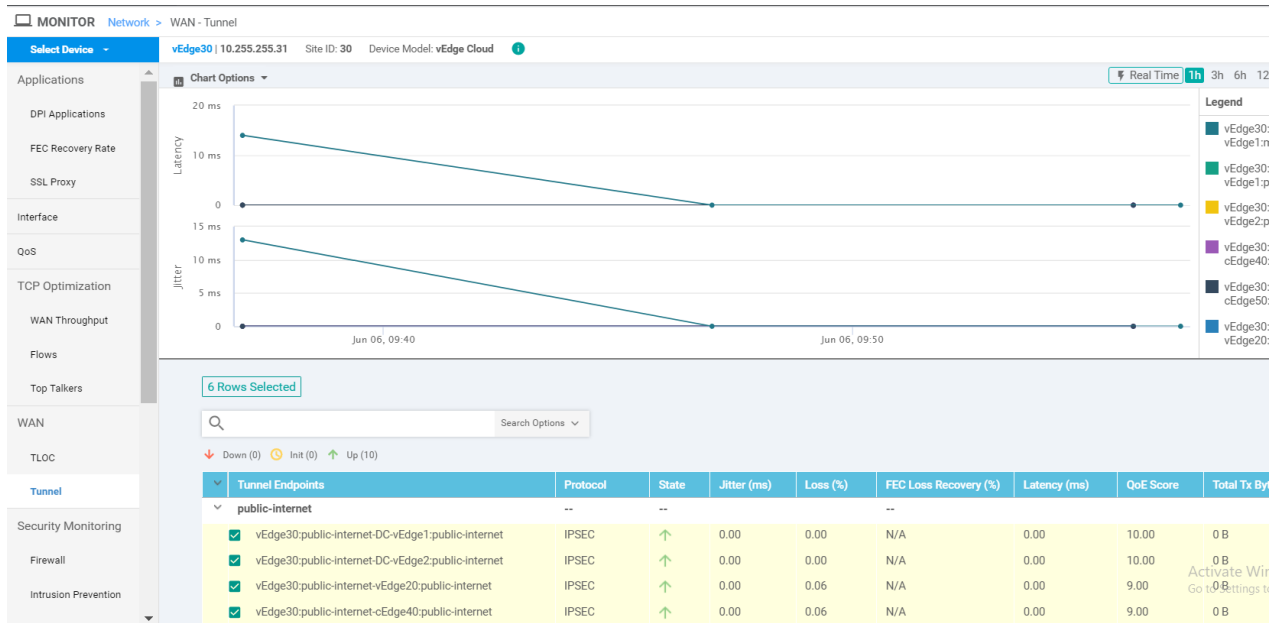
Ingress ACL - IPv6 On Off

Egress ACL - IPv6 On Off

Ingress Policer On Off

Update 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

Bad (0-5) Average (5-8)

VPN List VPN - 10

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	●	10.0	local	ge0/0	N/A	N/A	N/A
1	DC-Edge2	▲	7.0	local	ge0/0	N/A	N/A	N/A

CONFIGURATION Cloud onRamp for SaaS > Amazon AWS Manage Cloud onRamp for SaaS

Bad (0-5) Average (5-8) Good (8-10) 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: Oct 26, 2020

