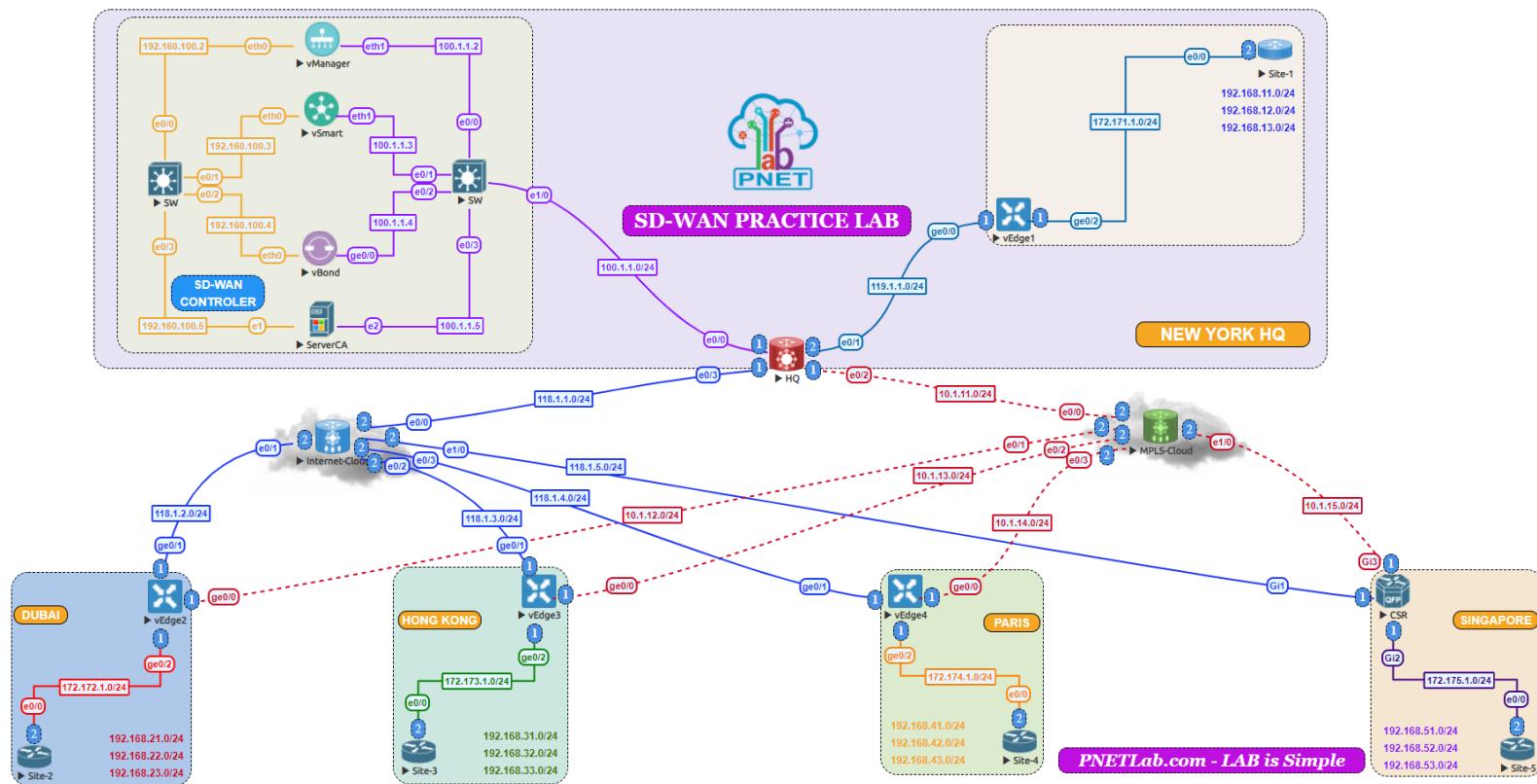




# SD-WAN Practice LAB 1 – PNETLab.com



## Lab Topology





## Table of Contents

VERSION HISTORY .....	7
HOW TO SETUP LAB .....	8
Hardware Requirement .....	8
Link to download lab and Setup .....	10
Account login to the devices in the SD-WAN LAB.....	22
Lab 1: Configuring the WAN Components .....	24
Task 1 – HQ Router Configuration .....	24
Task 2 – MPLS Cloud Router Configuration .....	25
Task 3- Internet Cloud Router Configuration.....	26
Lab 2: Installing the Enterprise Certificate Server .....	27
Task 1- Configure the interface.....	27
Task 2- Installing the Enterprise Root Certificate Server .....	28
Task 2 Install WinSCP .....	34
Lab 3- Initializing vManage -CLI .....	35
Task 1- Configuring the System Component.....	35
Task 2- Configured the VPN parameters.....	35
Lab 4- Initializing vManage – GUI.....	37
Task 1- Organization name & vBond Address.....	37
Task 2 – Configure Controller Authorization as Enterprise Root and Download the Root Certificate... <td>37</td>	37
Task 3- Generate a CSR for vManage.....	44
Task 4 – Request a Certificate from the CA Server .....	46
Task 5 – Issue the Certificate from the CA Server.....	49
Task 6- Downloading the Issued Certificate.....	50
Task 7- Installing the Identity Certificate for vManage.....	55
Lab 5- Initializing vBond – CLI .....	58
Task 1- Configuring the System component.....	58
Task 2 – Configure the vpn parameters.....	58
Lab 6- Initializing vBond -GUI.....	60
Task 1 – Add vBond to vManage.....	60
Task 2 – View the generated CSR for vBond and copy it .....	61
Task 3- Request a certificate from the CA Server .....	63
Task 4 – Issue the Certificate from the CA Server.....	66





Task 5- Downloading the Issued Certificate.....	67
Task 6- Installing the Identity Certificate for vManage.....	72
Lab 7 – Initializing vSmart – CLI.....	75
Task 1 - Configuring the System Component.....	75
Task 2 – Configured the vpn parameters.....	75
Lab 8 – Initializing vSmart – GUI .....	77
Task 1- Add vSmart to vManage .....	77
Task 2 – View the generated CSR for vSmart and Copy it .....	78
Task 3 – Request a Certificate from the CA Server .....	80
Task 4 – Issue the Certificate from the CA Server.....	83
Task 5- Downloading the Issued Certificate.....	84
Task 6- Installing the Identity Certificate for vManage.....	89
Lab 9 – initializing vEdge – CLI .....	92
Task 1 – Upload the WAN Edge List .....	92
Task 1 – Configuring the System Component.....	95
Task 2 – Configure the vpn parameters.....	96
Task 1 – Configuring the System Component.....	97
Task 2 – Configure the vpn parameters.....	97
Task 1 – Configuring the System Component.....	98
Task 2 – Configure the vpn parameters.....	98
Task 1 – Configuring the System Component.....	99
Task 2 – Configure the vpn parameters.....	100
Lab 10 – Registering vEdges in vManage .....	101
Task 1- Upload the Root Certificate to the vEdge.....	101
Task 2- Install the Root Certificate on vEdge1 .....	102
Task 3- Active vEdge on vManage.....	103
Task 1 – Upload the Root Certificate to the vEdge .....	104
Task 2- Install the Root Certificate on vEdge2 .....	106
Task 3- Active vEdge on vManage.....	107
Task 1 – Upload the Root Certificate to the vEdge .....	108
Task 2- Install the Root Certificate on vEdge3 .....	110
Task 3- Active vEdge on vManage.....	111
Task 1 – Upload the Root Certificate to the vEdge .....	112





Task 2- Install the Root Certificate on vEdge4 .....	114
Task 3- Active vEdge on vManage.....	115
Lab 11 – Initializing cEdge – CLI .....	117
Task 1 – Configuring the System Component.....	117
Task 2 – Configure the Interface and Tunnel Parameters .....	117
Lab 12 – Registering cEdges in vManage .....	119
Task 1 – Upload the Root Certificate to the cEdge .....	119
Task 2 – Install the Root Certificate on cEdge1.....	120
Task 3 - Activate cEdge on vManage.....	121
Lab 13 – Configuring Feature Template –System .....	123
Task 1 – Configure the System Template to be used by all vEdgeCloud Devices .....	123
Task 2 – Configure the System Template to be used by all cEdgeCloud Devices .....	124
Task 3 – Configure the System Template to be used by all vSmart Device .....	126
Lab 14 – Configuring Feature Template –Banner .....	128
Task 1 – Configure the Banner Template to be used by all vEdgeCloud Devices .....	128
Task 2 – Configure the Banner Template to be used by all cEdgeCloud Devices .....	129
Lab 15 - Configuring Feature Templates -VPN & VPN Interfaces for VPN 0 & 512 —Branch Site(vEdges) .....	131
Task 1 – Configure a VPN Template to be used by all Branch vEdgeCloud Devices for VPN 0.....	131
Task 2 – Configure a VPN Template to be used by all Branch vEdgeCloud Devices for VPN 512.....	133
Task 3 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 0 for Interface G0/0 .....	135
Task 4 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 0 for Interface G0/1 .....	137
Task 5 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 512 for Interface Eth0.....	140
Lab 16 - Configuring Feature Templates –External Routing - OSPF for VPN 0 –Branch Site (vEdges).....	143
Task 1 – Configure a OSPF Template to be used by all Branch vEdgeCloud Devices for VPN 0 .....	143
Lab 17 - Configuring and Deploying Device Templates for vEdge – Branch Site(vEdge2) .....	146
Task 1 – Configure a Device Template for Branch vEdge Devices. ....	146
Task 2 – Attach vEdge2 to the Device Template.....	149
Task 3 – Configure the Variable Parameters for the Feature Templates .....	150
Lab 18 - Configuring Internal Routing Protocols on the Internal Routing Devices – HQ & All Branches..	155
Task 1 – Internal Site Router Configurations .....	156





Lab 19 - Configuring Feature Templates –Service VPN – VPN, VPN Interface and Internal Routing – Branch Site (vEdges).....	160
Task 1 - Configure a VPN Template to be used by all Branch vEdgeCloud Devices for VPN 1 .....	160
Task 2 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud devices for VPN 1 for Interface G0/2 .....	161
Task 3 – Configure a OSPF Template to be used by all Branch vEdgeCloud Devices for VPN 1 .....	163
Lab 20 - Implementing a Service VPN using Templates – Branch Site (vEdge2).....	165
Task 1 – Edit the BR-VE-TEMP Device Template for Branch vEdge Devices.....	165
Task 2 – Configure the Variable Parameters for the Feature Templates .....	165
Lab 21 - Pushing Template to configure other Branch Sites – Branch Site(vEdge3 & vEdge4) .....	168
Task 1 – Attach the BR-VE-TEMP Device Template for Branch vEdge Devices.....	168
Lab 22 – Configuring Feature Templates for HQ-Site(vEdge1) – VPNs, VPN Interfaces, External & Internal Routing.....	172
Task 1 – Configure a VPN Template for HQ vEdge-Cloud Devices for VPN 0 .....	172
Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 0 for Interface G0/0.....	174
Task 3 – Configure a BGP Template to be used by HQ vEdge-Cloud Devices for VPN 0 .....	175
Task 1 – Configure a VPN Template to be used by HQ vEdge-Cloud Devices for VPN 512 .....	178
Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 512 for Interface Eth0.....	180
Task 1 – Configure a VPN Template for HQ vEdge-Cloud Devices for VPN 1 .....	182
Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 1 for Interface G0/2.....	184
Task 3 – Configure a OSPF Template to be used by HQ vEdge-Cloud Devices for VPN 1.....	186
Lab 23 - Configuring Device Templates for HQ-Site(vEdge1) to deploy VPN 0, 1 and 512.....	188
Task 1 – Configure a Device Template for HQ vEdge Devices. ....	188
Task 2 – Attach vEdge1 to the Device Template.....	190
Task 3 – Configure the Variable Parameters for the Feature Templates .....	191
Lab 24 – Configuring Feature Templates for CSR – VPNs, VPN Interfaces, External & Internal Routing .	198
Task 1 – Configure a VPN Template by CSR for VPN 0.....	198
Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 0 for Interface GigabitEthernet1.....	199
Task 3 – Configure a VPN Interface Template to be used by CSR for VPN 0 for Interface GigabitEthernet3.....	201
Task 4 – Configure a OSPF Template to be used by CSR for VPN 0 .....	203





Task 1 – Configure a VPN Template to be used by CSR for VPN 512.....	204
Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 512 for Interface GigabitEthernet4.....	206
Task 1 – Configure a VPN Template for CSR for VPN 1 .....	208
Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 1 for Interface G2.....	210
Task 3 – Configure a OSPF Template to be used by CSR for VPN 1 .....	212
Lab 25 - Configuring Device Templates for CSR to deploy VPN 0, 1 and 512 .....	214
Task 1 – Configure a Device Template for CSR Branch Devices.....	214
Task 2 – Attach cEdge1 to the Device Template.....	218
Task 3 – Configure the Variable Parameters for the Feature Templates .....	219
Lab 26 - Configuring and Deploying Feature and Device Templates for vSmart Controllers .....	225
Task 1 – Configure a VPN Template to be used by vSmart Controllers for VPN 0.....	225
Task 2 – Configure a VPN Template to be used by vSmart Controllers for VPN 512.....	226
Task 3 – Configure a VPN Interface Template to be used by vSmart Controllers for VPN 0 for Interface Eth1 .....	228
Task 4 – Configure a VPN Interface Template to be used vSmart Controllers for VPN 512 for Interface Eth0 .....	229
Task 5 – Configure a Device Template for vSmart Controllers. ....	231
Task 6 – Attach vSmart to the Device Template.....	233
Task 7 – Configure the Variable Parameters for the Feature Templates .....	233
Lab 27 - Configuring Application Aware Policies using Telnet and Web .....	236
Task 1 – Configure Groups of Interests/List that will be used for Telnet & Web Application Aware Routing (AAR) Policy .....	236
Task 2 – Configure an AAR policy based on the Requirements .....	239
Task 3 – Create a Centralized Policy and call the Traffic Policy .....	242
Lab 28 - Manipulating Traffic flow using TLOCs .....	249
Task 1 – Configure Groups of Interests/List that will be used for Traffic Engineering Policy for DUBAI .....	249
Task 2 – Configure Control/Topology policy based on the Requirements .....	251
Task 3 – Modify the existing Centralized Policy “Main-CentralPolicy” and call the Topology Policy... ..	252
Lab 29 - Configuring Route Filtering .....	256
Task 1 – Configure Groups of Interests/List that will be used for Route Filtering Policy for Newyork ..	256
Task 2 – Configure Control/Topology policy based on the Requirements .....	257
Task 3 – Modify the existing Centralized Policy “Main-CentralPolicy” and call the Topology Policy... ..	258





## VERSION HISTORY

No	Version	Comment
1	1	Released workbook
2	1.1	Fixed: + Organization-name from "SDWAN" to "viptela sdwan" + Timer mismatched between Certificate and Controller + Correct ip address on E0/1 of HQ Router



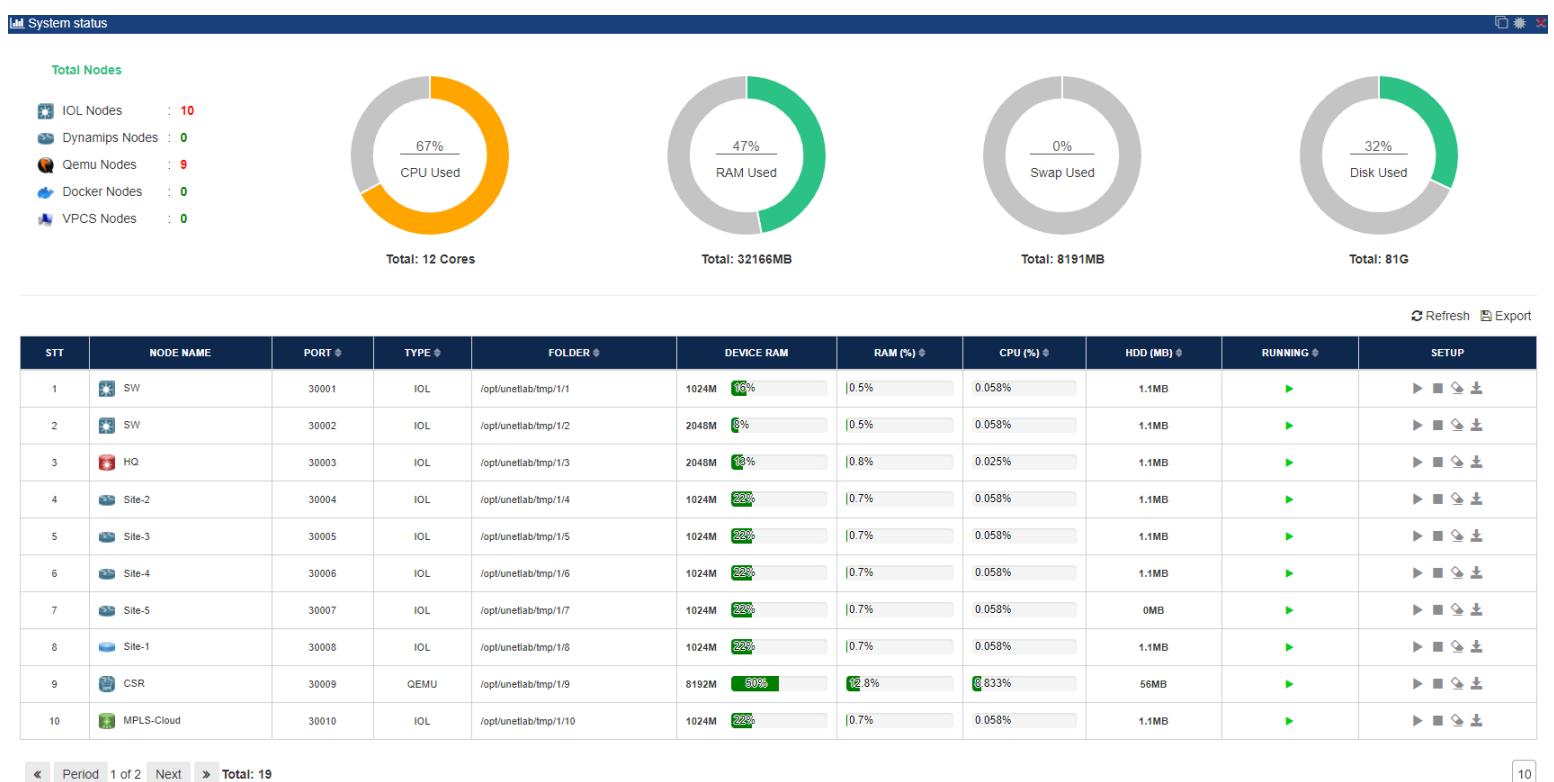
## HOW TO SETUP LAB

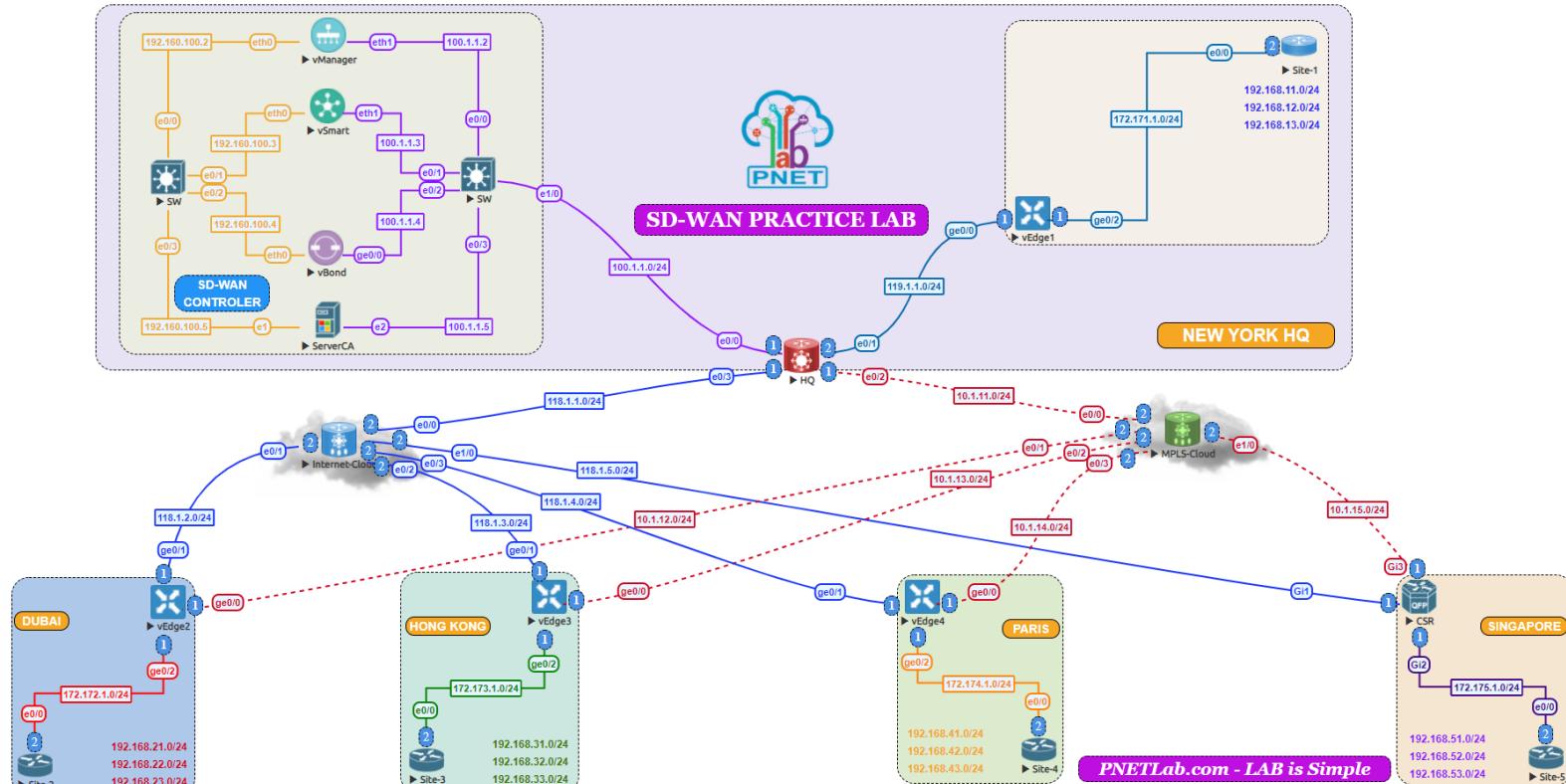
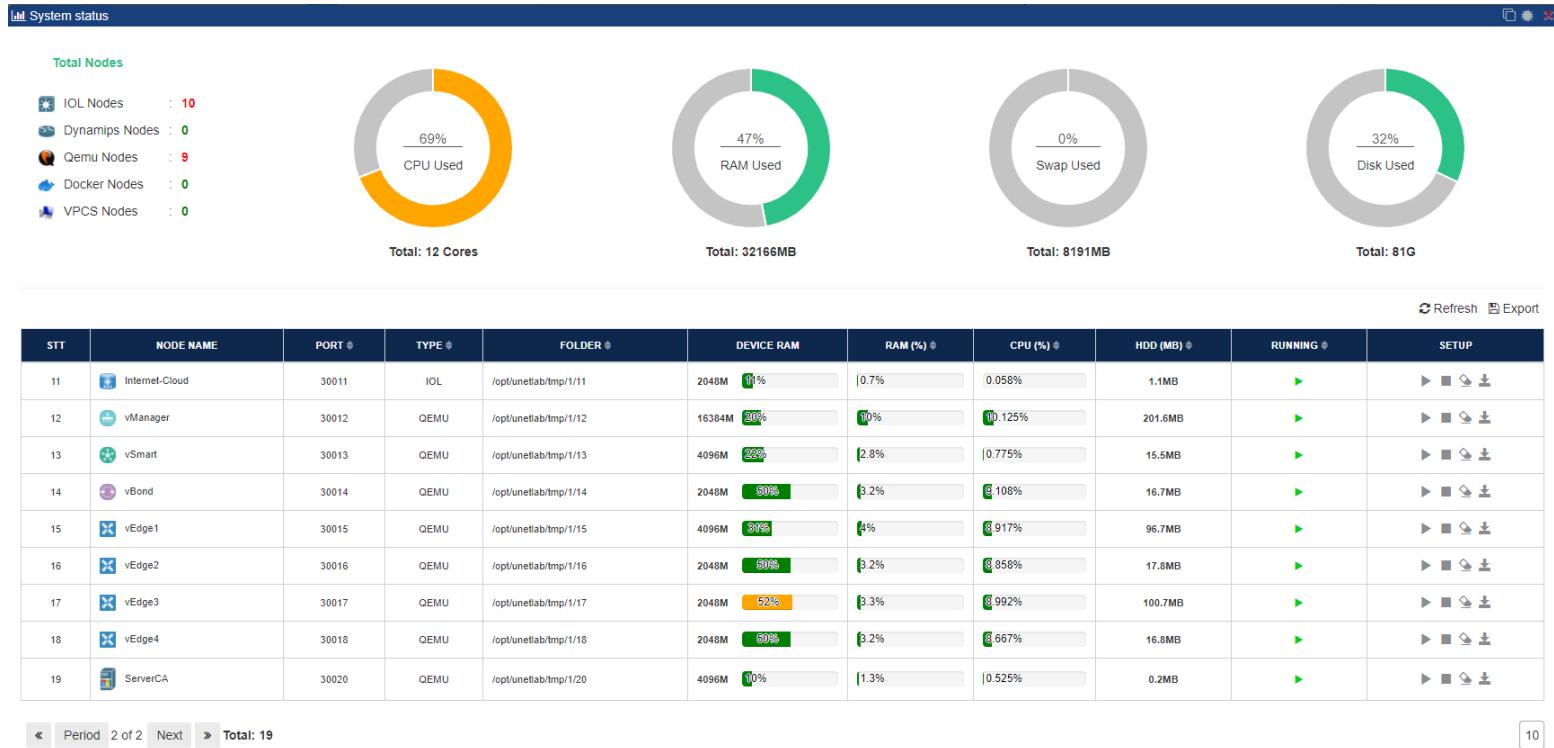
### Hardware Requirement

- CPU: 12v CPU
- RAM: 32GB
- HDD: 100GB

Note: Recommended Rack Rental (if you do not have a PC or server to practice).

- Join the Telegram group support: <https://t.me/rackrental>
- Pricing: **25 USD/1 week**
  - o Dedicated IP, Server for practice SD-WAN LAB.
  - o Included: all in one (IOS, Licensed, Workbook...) just practice only.
  - o Support: 24/7







## Link to download lab and Setup

### Note: Lab devices

- VIPTELA 20.3.1: vManager, vBond, vSmart, vEdge.
- Layer 2 Switches: L2-Advan-15.2-IRON
- Layer 3 Router: L3-Advan-15.4
- CRS: CRS1000vng-SDWAN
- ServerCA: Winserver-2008R2

### 1. [How to upload images into PNETLab](#)

#### a. Prerequisite:

- Download PNETLab platform and lab in the link:
  - o Link to download PNETLab Platform and setup: <https://pnetlab.com/pages/download>
  - o Link to download Lab from Store:  
<https://user.pnetlab.com/store/labs/detail?id=16052623645692>
  - o Download WINSSCP in the link then setup: <https://winscp.net/eng/download.php>
- Download all images in the link:  
<magnet:?xt=urn:btih:F1BD30B97284C7ABF46B5DEAC28E415676E0FCEB&dn=viptela>

Name
asav-981
csr1000vng-ucmk9.16.12.3
vtbond-20.3.1
vtedge-20.3.1
vtmgmt-20.3.1
vtsmart-20.3.1
winserver-2008R2
winserver-ServerCA
L2-ADVENTERPRISEK9-M-15.2-IRON-20151103.bin
L3-AdvEnterpriseK9-M2_157_3_May_2018.bin

#### b. Upload Images into PNETLab:

- **Step 1:** Start PNETLab then login with WinSCP (using your ip address, username and password as root and pnet respectively)



```
PNETLab (default root password is 'pnet')
Use https or http://192.168.17.135/
pnetlab login: _
```

WinSCP

Local Mark Files Commands Session Options Remote Help

New Session

My documents

C:\Users\Eagle\Documents\

Name

- ..
- ViberDownloads
- My Videos
- My Pictures
- My Music
- Virtual Machines
- Axure
- My Maps
- Zalo Received Files
- Navicat
- My Data Sources
- Outlook Files
- OneNote Notebooks
- cache
- Snagit
- Snagit Stamps
- Custom Office Templates
- My Shapes
- My ISO Files
- desktop.ini

0 B of 402 B in 0 of 19  
Not connected.

Login

Session

File protocol: SFTP

Host name: 192.168.17.135 Port number: 22

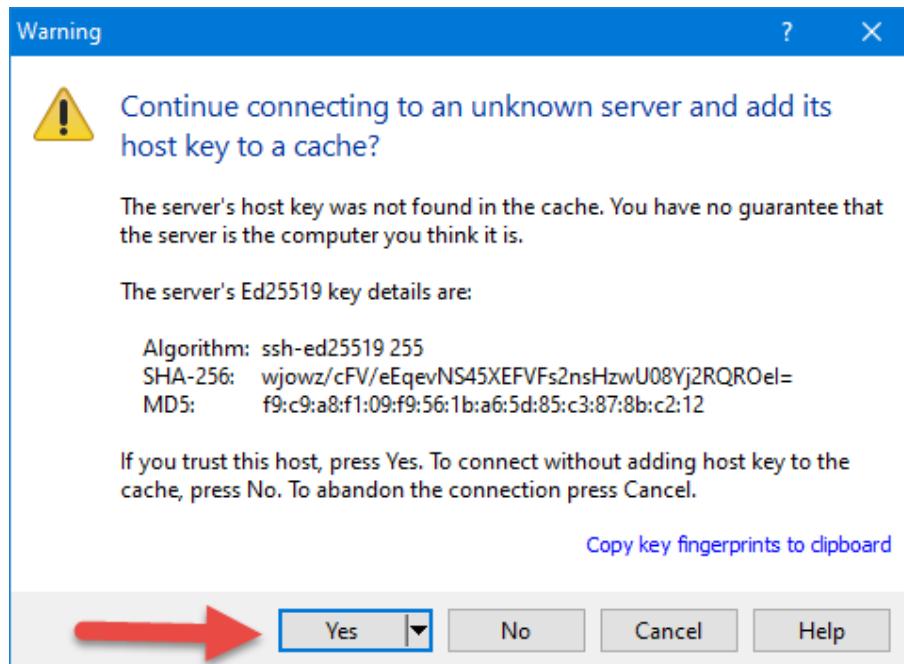
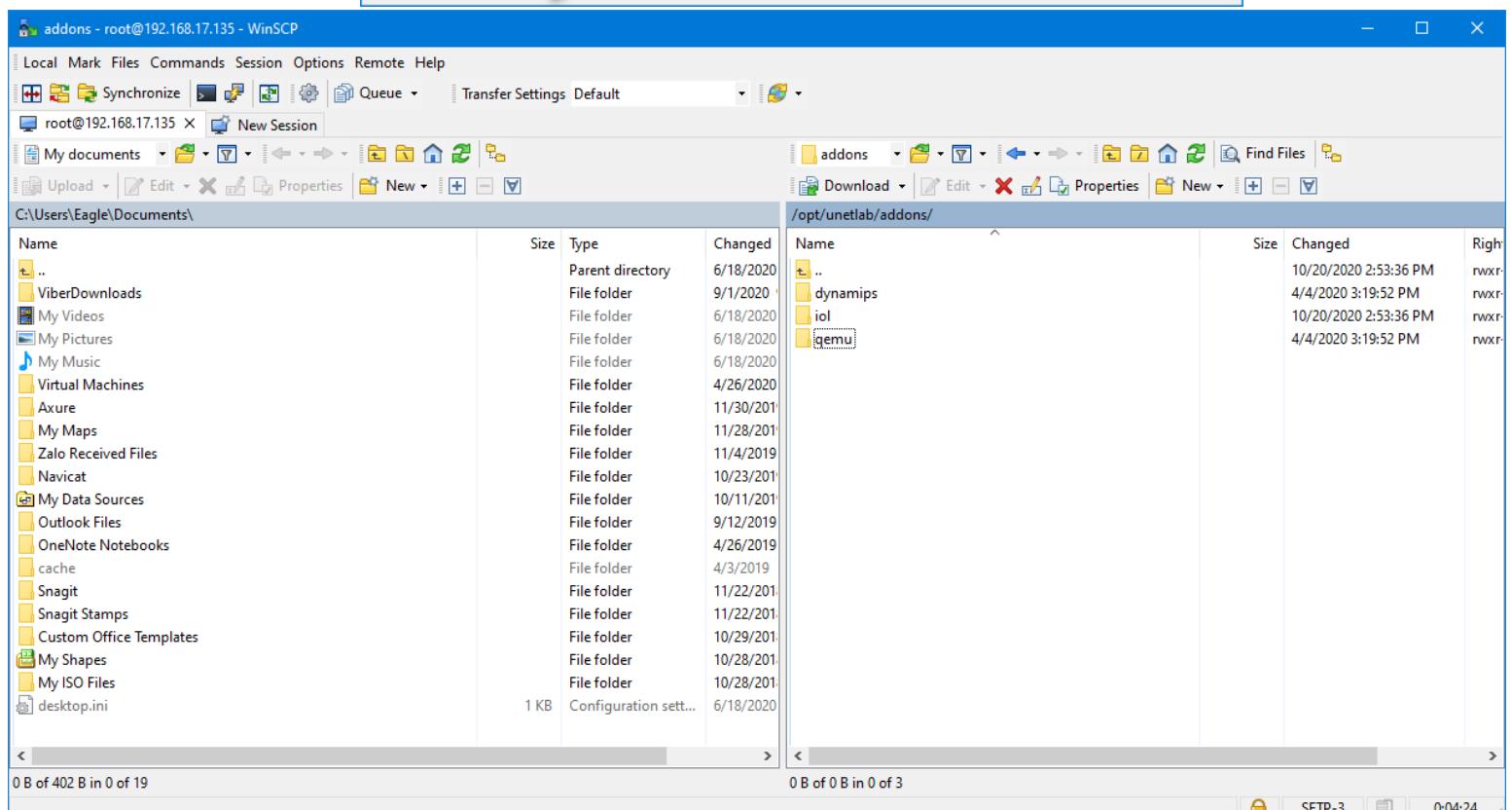
User name: root Password: \*\*\*\*

Save Advanced...

Tools Manage Login Close Help

Show Login dialog on startup and when the last session is closed

File folder	1 KB	Configuration sett...	10/28/2018 1:43:44 AM	6/18/2020 2:34:55 PM

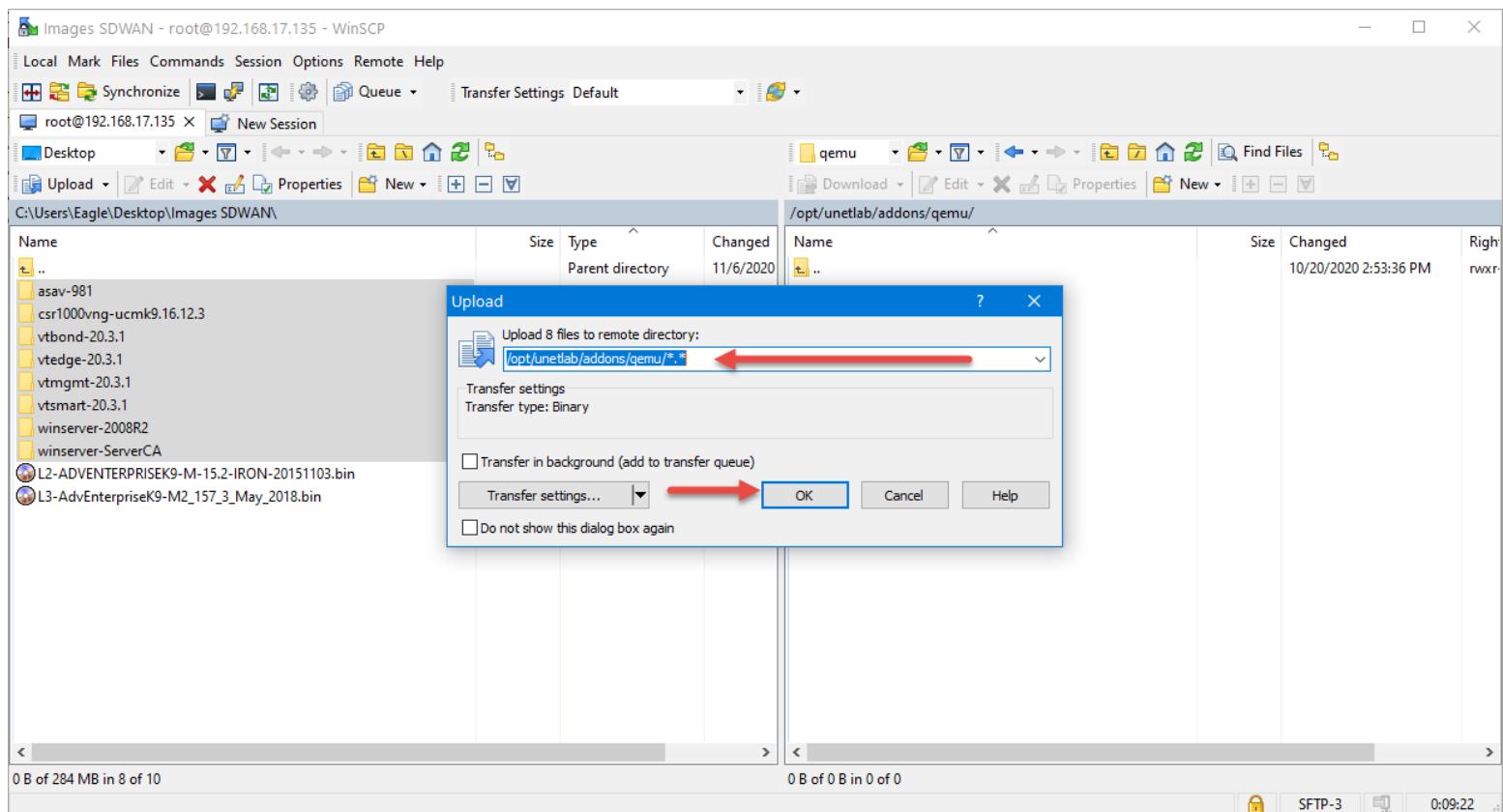
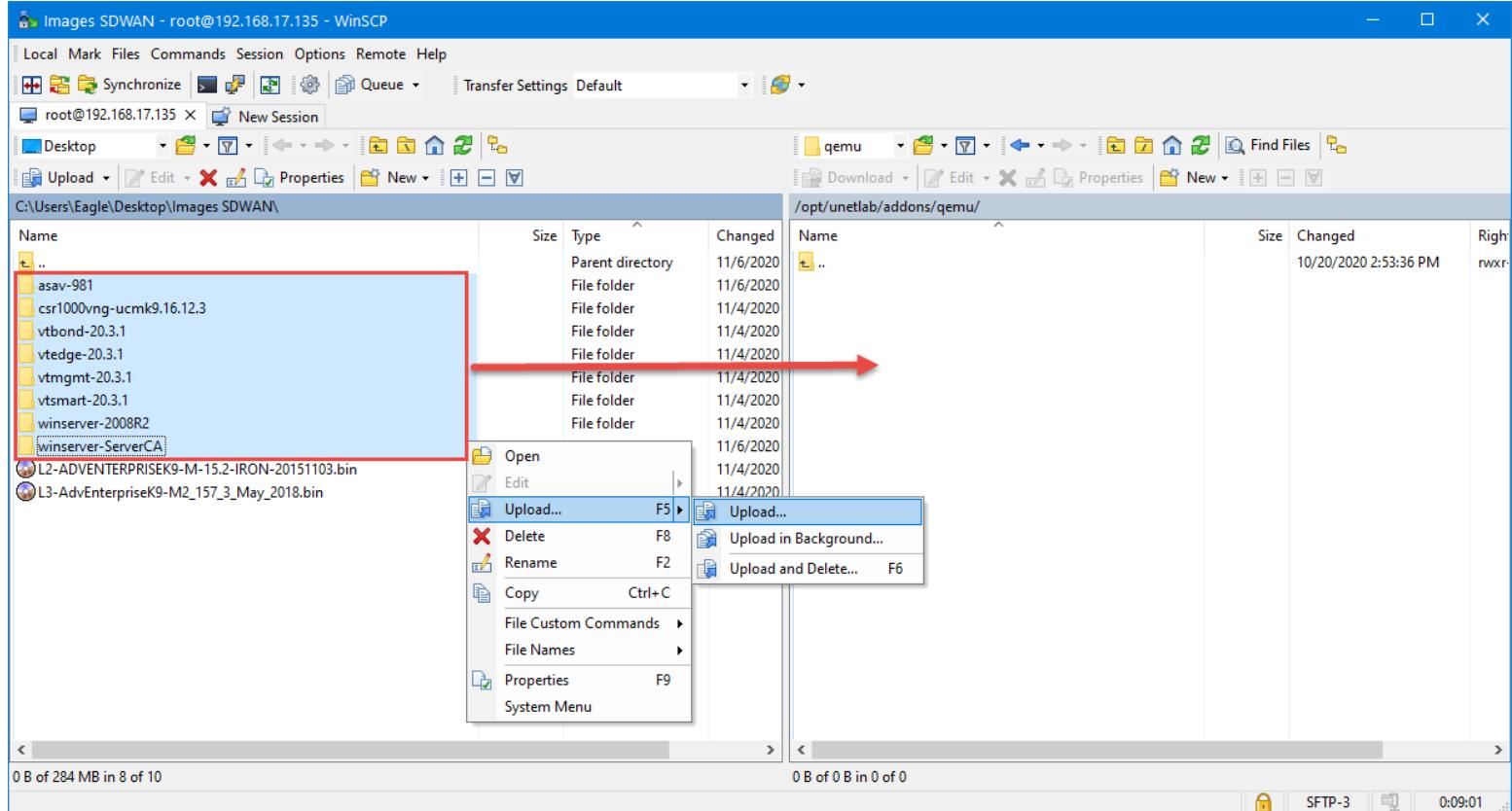



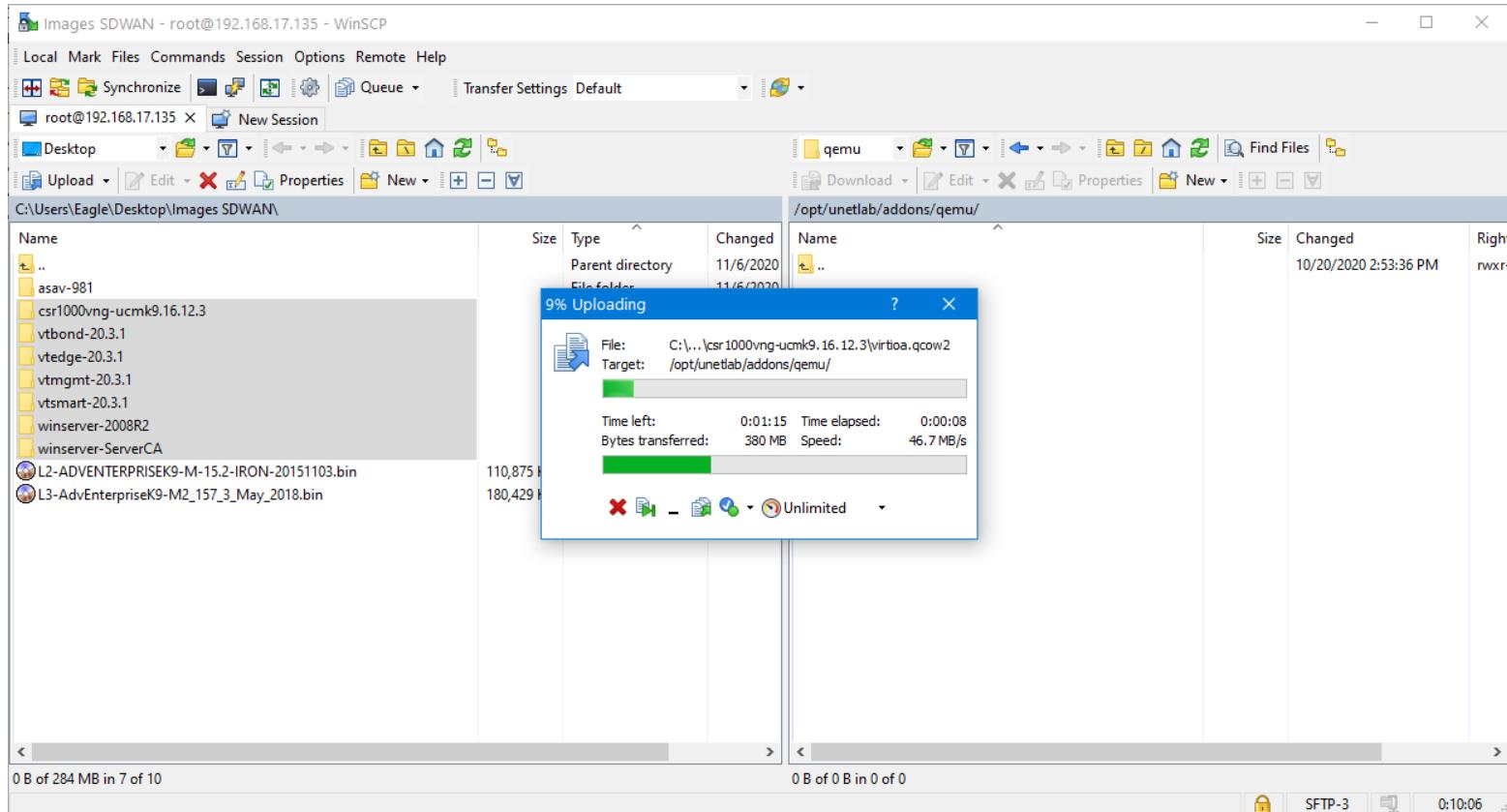
Name	Type	Size	Changed	Right
..	Parent directory		6/18/2020	
ViberDownloads	File folder		9/1/2020	
My Videos	File folder		6/18/2020	
My Pictures	File folder		6/18/2020	
My Music	File folder		6/18/2020	
Virtual Machines	File folder		4/26/2020	
Axure	File folder		11/30/2019	
My Maps	File folder		11/28/2019	
Zalo Received Files	File folder		11/4/2019	
Navicat	File folder		10/23/2019	
My Data Sources	File folder		10/11/2019	
Outlook Files	File folder		9/12/2019	
OneNote Notebooks	File folder		4/26/2019	
cache	File folder		4/3/2019	
Snagit	File folder		11/22/2019	
Snagit Stamps	File folder		11/22/2019	
Custom Office Templates	File folder		10/29/2019	
My Shapes	File folder		10/28/2019	
My ISO Files	File folder		10/28/2019	
desktop.ini	Configuration sett...	1 KB	6/18/2020	

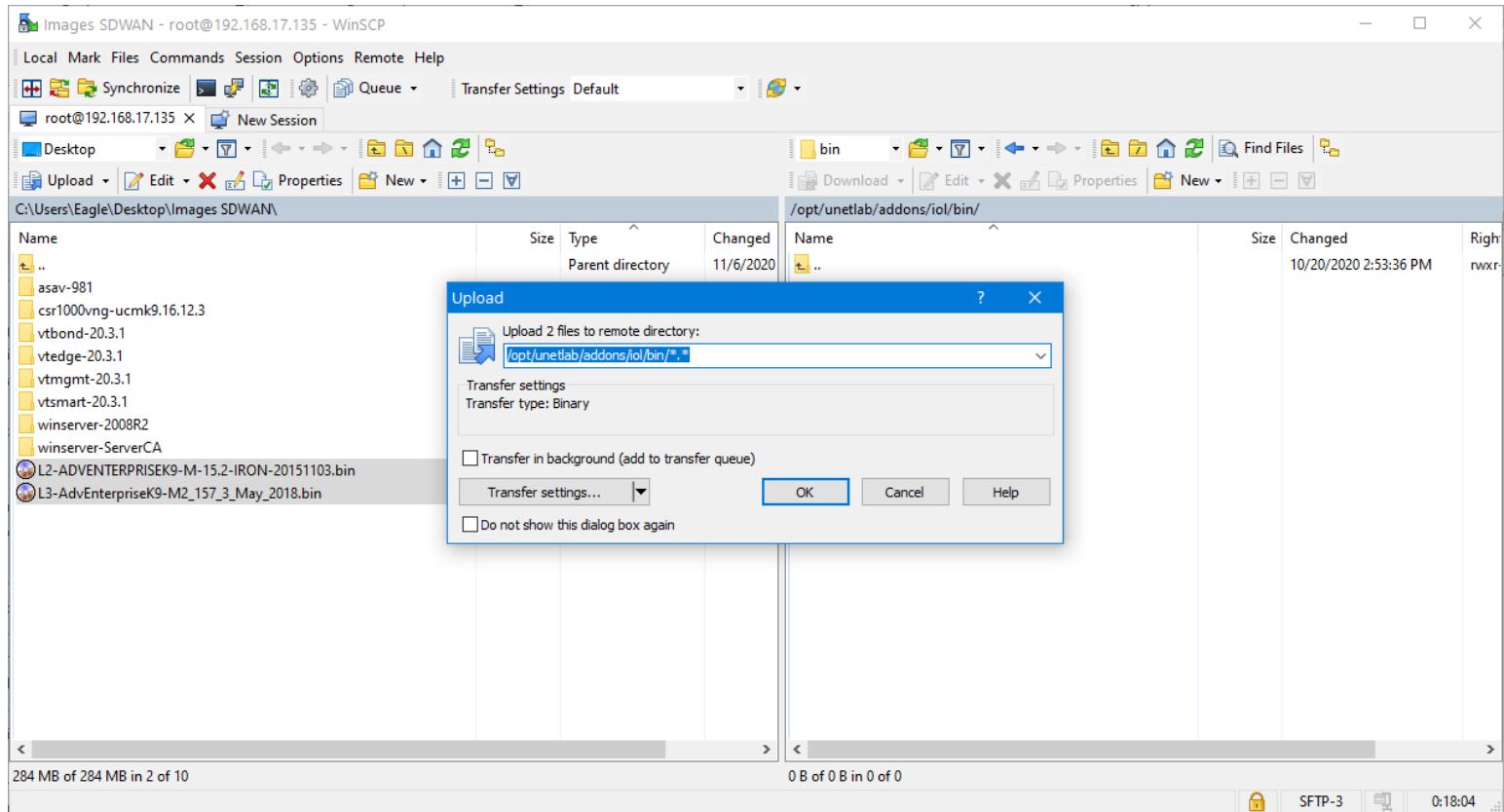
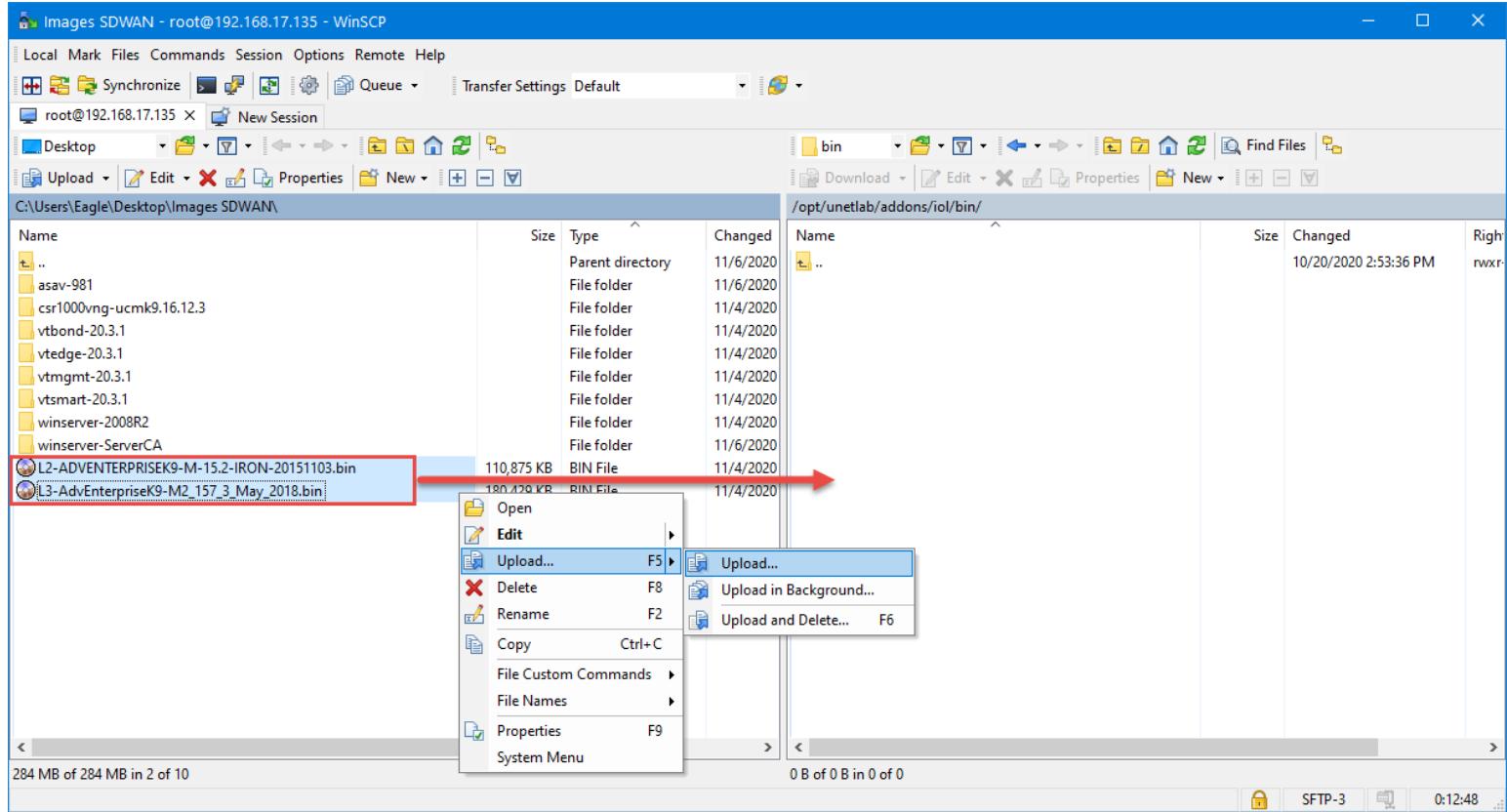
Name	Type	Size	Changed	Right
..	Parent directory		10/20/2020 2:53:36 PM	
dynamips	File folder		4/4/2020 3:19:52 PM	
iol	File folder		10/20/2020 2:53:36 PM	
qemu	File folder		4/4/2020 3:19:52 PM	

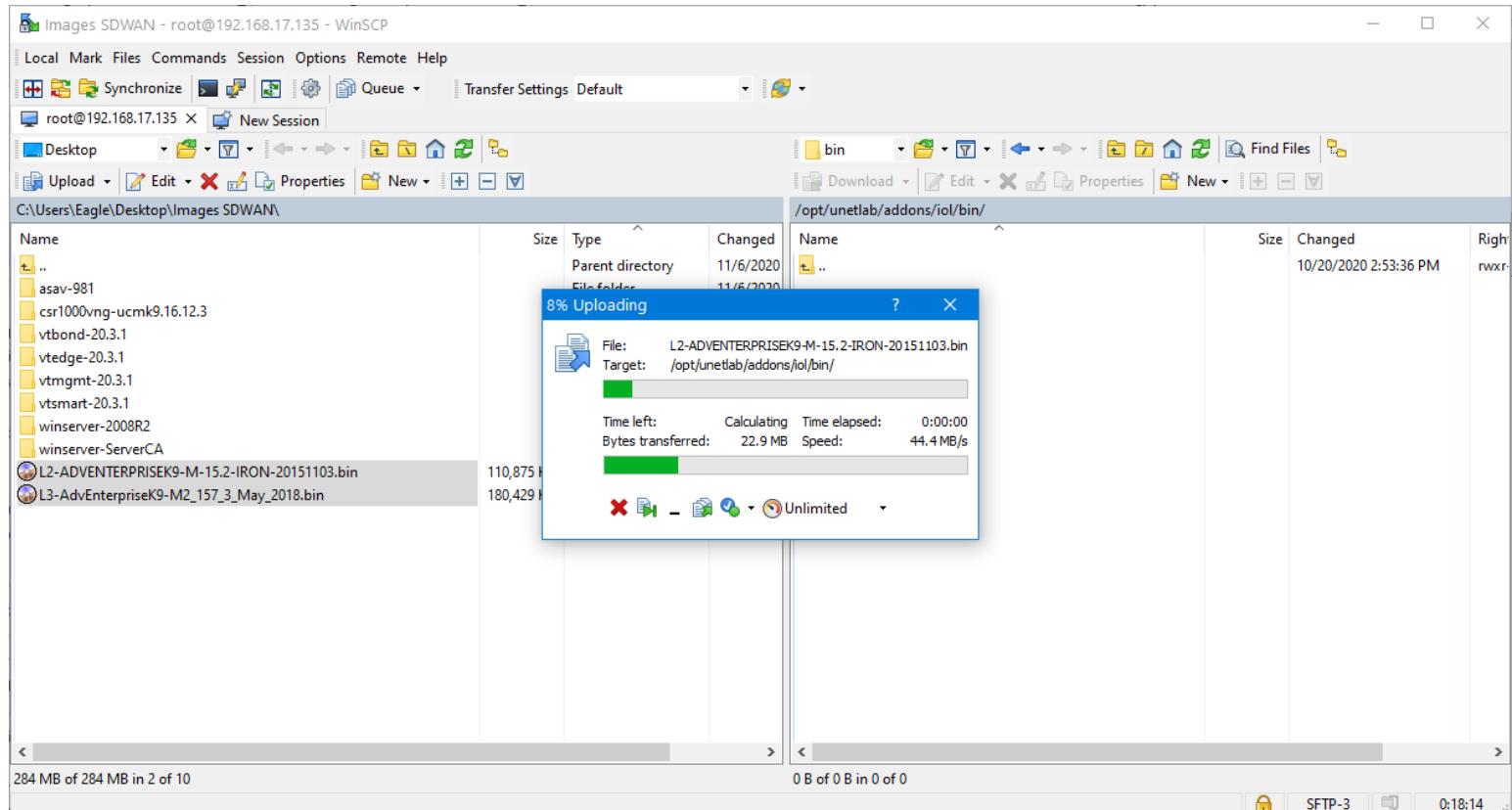
- **Step 2:** Upload Qemu Images and IOS as shown below:
  - **Upload All Qemu Images to folder: /opt/unetlab addons/qemu**





- Upload All IOS Images to folder: /opt/unetlab/addons/iol/bin





o Upload template file for SD-WAN devices to Folder: /opt/unetlab/html/templates

If you skip this step, SD-WAN devices cannot start properly

Link to download Template file:

<https://drive.google.com/file/d/1CZqoBv27HBJH3aUTwVDIfPXBr6KX3N5p/view?usp=sharing>

Backup Link: [https://mega.nz/file/uzxEEKLK#LvfeYdKR\\_SFj-msYcJgDHQ2vdRrpBltEKqcLChcCiRs](https://mega.nz/file/uzxEEKLK#LvfeYdKR_SFj-msYcJgDHQ2vdRrpBltEKqcLChcCiRs)

Unzip and copy to folder **/opt/unetlab/html/templates** in PNETLab

**Note:** If you are using **PNETLab Version from 4.2.0**, You do not need to do this step

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



sdwan-templates - Admin PNETLAB - WinSCP

Local Mark Files Commands Session Options Remote Help

Synchronize Queue Transfer Settings Default

Admin PNETLAB New Session

Desktop Upload Edit Properties New

C:\Users\Eagle\Desktop\Images SDWAN\sdwan-templates\

Name	Size	Type	Changed
..		Parent directory	10/18/2020 5:10:11 PM
cedge1.txt	2 KB	Text Document	10/18/2020 5:12:51 PM
csr1000vng.yml	2 KB	YML File	10/18/2020 5:08:23 PM
vtbond.yml	2 KB	YML File	5/8/2020 8:15:53 PM
vtedge.yml	2 KB	YML File	4/19/2020 1:54:50 AM
vtmgmt.yml	2 KB	YML File	9/25/2020 8:47:30 PM
vtsmart.yml	2 KB	YML File	4/19/2020 1:54:50 AM

Open Edit F5 Upload... F5 Upload... Upload in Background... Upload and Delete... F6

.. \*.yml .htaccess a10.yml acsyu.. alteon.yml ampcloud.yml apicem.yml aruba.yml asayml asav.yml barracuda.yml bigip.yml brocadeadvx.yml c1710.yml c3725.yml c7200.yml cdayml cips.yml clearpass.yml coeus.yml

0.7 KB of 10.7 KB in 6 of 6

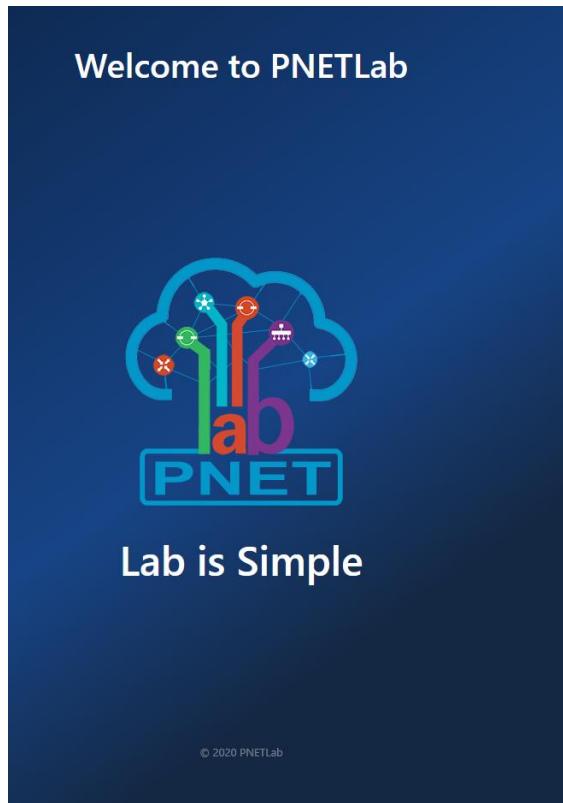
0 B of 160 KB in 0 of 87

SFTP-3 0:07:32

The screenshot shows a WinSCP session comparing local files on the left and remote files on the right. A red box highlights the local directory 'C:\Users\Eagle\Desktop\Images SDWAN\sdwan-templates\' containing several configuration files. A red arrow points from the 'Upload...' option in the context menu of a selected file ('cedge1.txt') to the 'Upload...' option in the context menu of the remote directory '/opt/unetlab/html/templates/'. Both menus are open, showing the 'Upload...' command.

- Step 3: Fix permissions

- o Login to PNETLab platform (note: logging with online account)



Login

Algernon

.....

Console

[Forgot password?](#)

0C 0C

[Login](#)

[Login by Offline Account](#)





- Go to: System → System Setting

The screenshot shows the PNETLab Platform interface. At the top, there's a navigation bar with links like Main, Running Labs, Accounts, System, Download Labs, Sell Your Labs, and Devices. Below the navigation bar is a sidebar titled 'Workspace' with a 'root' folder. A red arrow points from the 'Search Labs' input field towards the 'System' menu. The 'System' menu is open, showing options: System Mode, System status, System Setting (which is highlighted with a blue background), and Versions. To the right of the menu is a 'Lab Preview' section containing a grid pattern.

- Click to Fix permission button

The screenshot shows the 'Controller' settings page. At the top, there are several buttons: 'Stop All Nodes' (blue), 'Fix Permission' (blue, with a red arrow pointing to it), 'Reboot' (red), and 'Shutdown' (red). Below these buttons are sections for 'Docker Wireshark Only' (with a red circle around the checkbox), 'Default Console' (Auto is selected), and 'Default Language'. The bottom half of the screen contains two main sections: 'Share Folders' (with a list of 'Selected Folders' including 'labs' and 'Your labs from PNETLab Store') and 'Share Folders permissions' (a list of checkboxes for various lab management actions).





The screenshot shows the PNETLab Platform's Controller settings. A modal window is centered, indicating that permissions have been fixed successfully. The background displays various configuration options such as Docker Wireshark Only, Default Console (set to Auto), and Share Folders (selected 'labs'). At the bottom right, there is a list of lab-related actions: Add New Lab, Import Lab, Export Lab, Move Lab, Clone Lab, Join Lab Session, and Open New Lab Session.

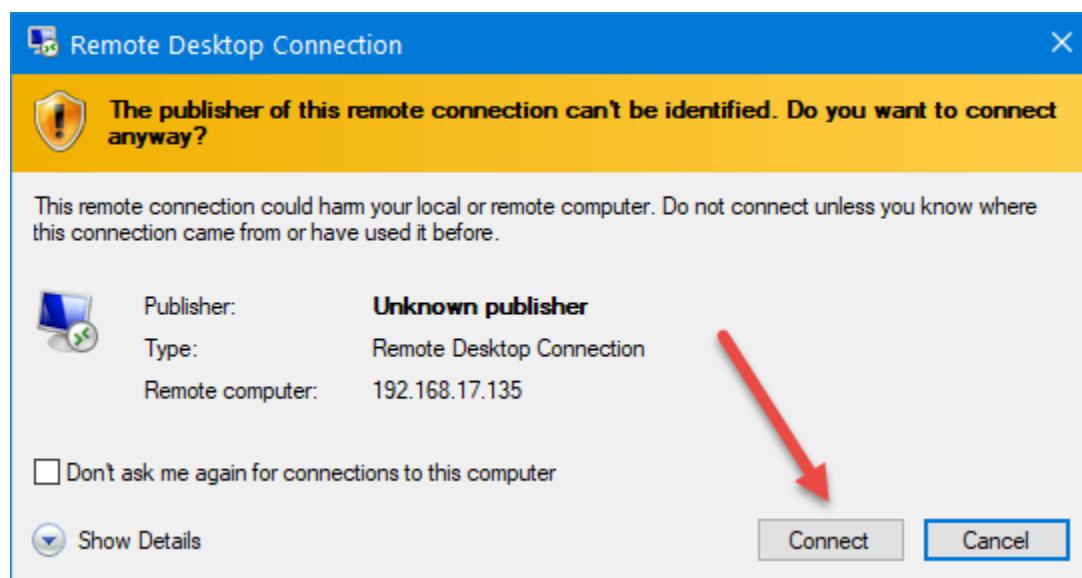
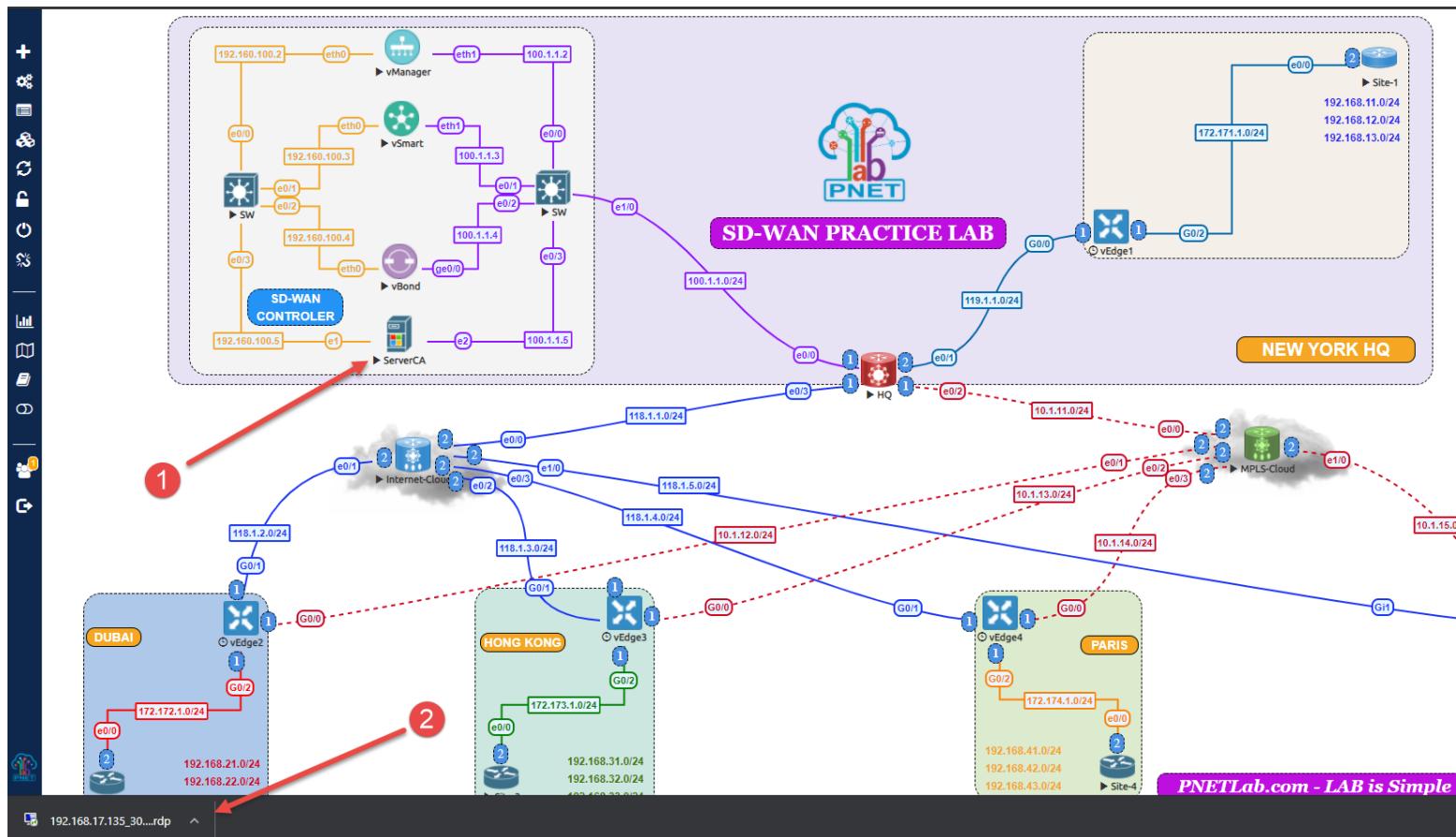
## 2. **How to setup and practice Lab**

### a. Licensing on SD-WAN devices

- Link to download file serial licence: <https://drive.google.com/file/d/1KFqwBLHz-xB7DXgTWudryedKIEK0lfKy/view?usp=sharing>
  - o Backup Link:  
[https://mega.nz/file/jyZnSlhJ#rSprYR4z9XY\\_o2Ryyw3CCBdto5JxEU5AUvzRXRruX-Y](https://mega.nz/file/jyZnSlhJ#rSprYR4z9XY_o2Ryyw3CCBdto5JxEU5AUvzRXRruX-Y)
- Save that file to your PC then using this license file for Lab 9

### b. ServerCA – Windows Server 2008

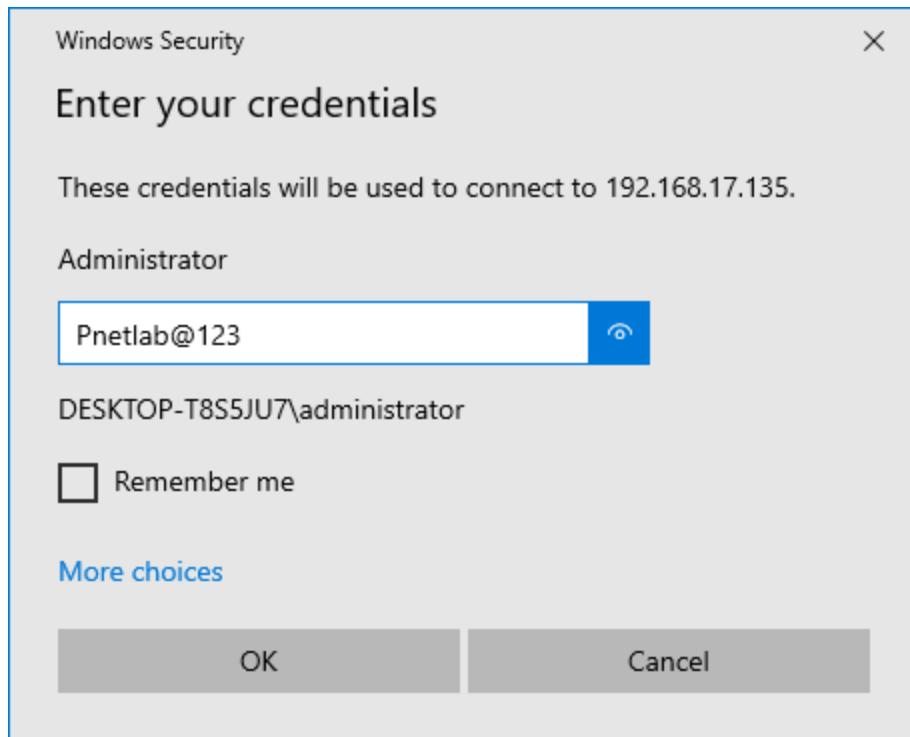
- We already set up all tools for SD-WAN Lab in serverCA, just download in the link above (we shared in session: Link to download Lab and Setup).
- How to login to ServerCA:
  - o Click to ServerCA then download RDP file and Open, Login with account:  
**administrator/Pnetlab@123**



[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)

A screenshot of a Windows Server 2008 R2 desktop. On the left, a browser window shows the Google homepage. On the right, the "Initial Configuration Tasks" window is open, listing tasks such as "Provide Computer Information", "Update This Server", and "Customize This Server". Two red arrows point from the bottom of the screen towards the "Initial Configuration Tasks" window.

Initial Configuration Tasks

Perform the following tasks to configure this server

Windows Server 2008 R2 Standard

Provide Computer Information

- Activate Windows
- Set time zone
- Configure networking
- Provide computer name and domain

Product ID: 00477-001-0000421-84589 (Activated)  
Time Zone: (UTC-04:00) Atlantic Time (Canada)  
Network Adapters: Multiple detected  
Full Computer Name: WIN-AJCU16BUBLG  
Workgroup: WORKGROUP

Update This Server

- Enable automatic updating and feedback
- Download and install updates

Updates: Not configured  
Feedback: Windows Error Reporting off  
Checked for Updates: Never  
Installed Updates: Never

Customize This Server

- Add roles
- Add features
- Enable Remote Desktop
- Configure Windows Firewall

Roles: Active Directory Certificate Services, Web Server (IIS)  
Features: Remote Server Administration Tools  
Remote Desktop: Enabled  
Firewall: Public: Off

Print, e-mail, or save this information

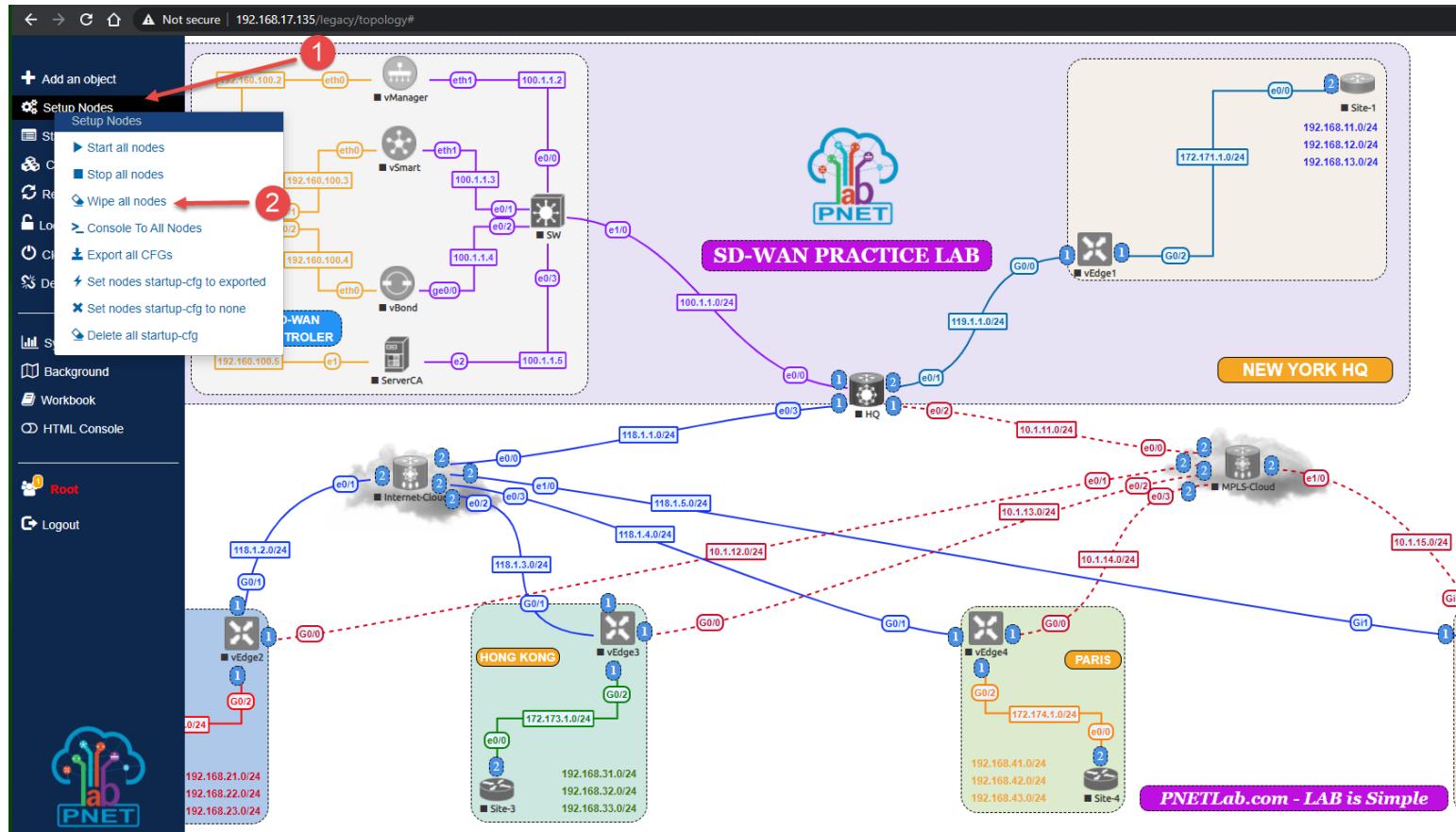
Do not show this window at logon



## Account login to the devices in the SD-WAN LAB

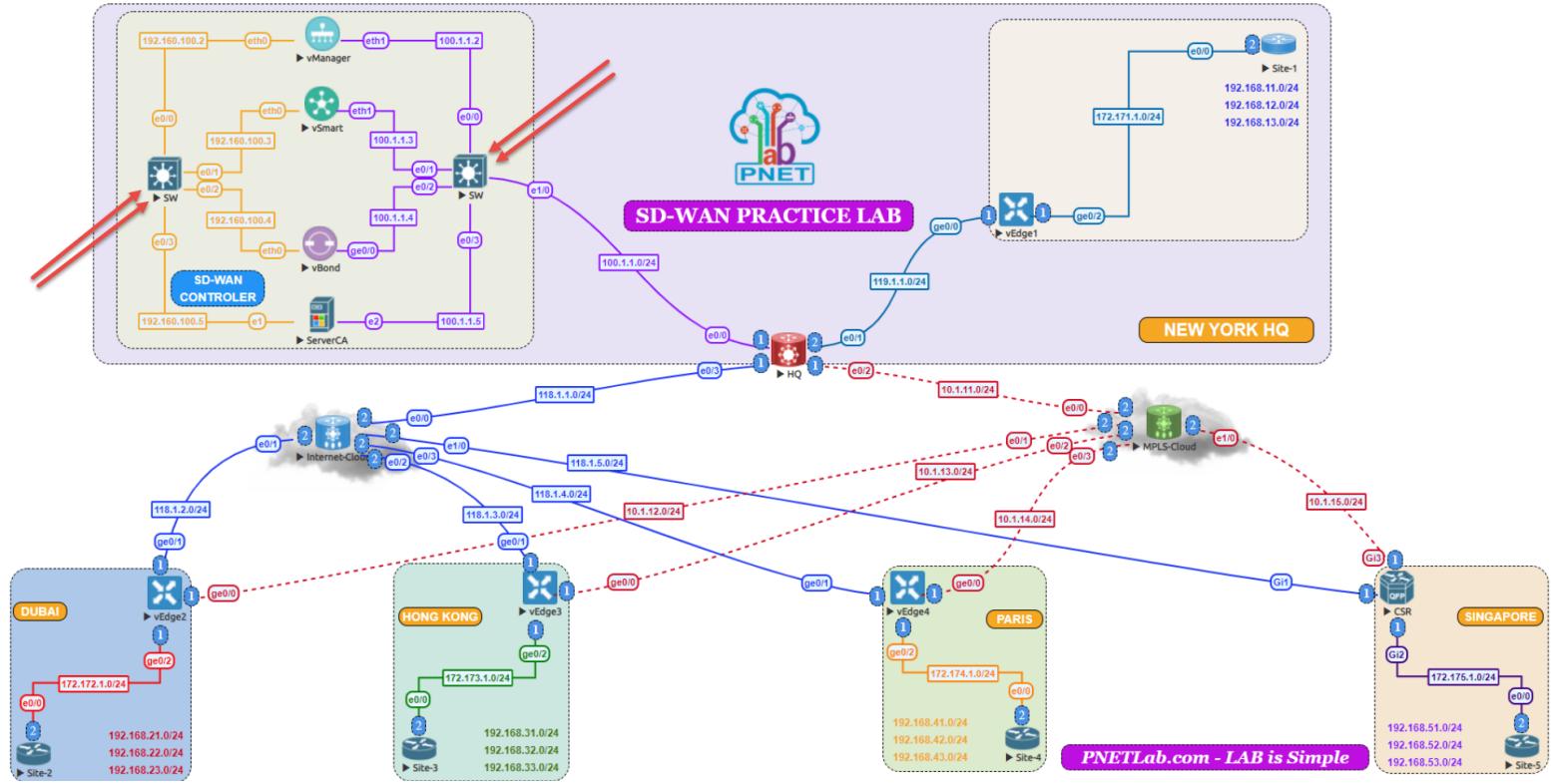
- Default username and password to login vManager, vSmart, vBond, vEdge is: **admin/admin**
- Default username and password to login to ServerCA: **administrator/Pnetlab@123**

**Note: Remember before you start the lab, wipe all nodes:**



**=====Some key notes for practicing this lab=====**

- If you see all 4 vEdge and cEdge down in Vmanage, almost problem by Switch, you should stop and start those switch**



- If only 4 vEdge down but cEdge are okay then you can start/stop 4 vEdges. Sometime they are not stable in lab.**



## Lab 1: Configuring the WAN Components

### Interface Configuration

#### HQ

Interface	IP address	Subnet Mask
E0/0	100.1.1.1	255.255.255.0
E0/1	119.1.1.2	255.255.255.0
E0/2	10.1.11.1	255.255.255.0
E0/3	118.1.6.1	255.255.255.0

#### MPLS-Cloud

Interface	IP address	Subnet Mask
E0/0	10.1.11.2	255.255.255.0
E0/1	10.1.12.2	255.255.255.0
E0/2	10.1.13.2	255.255.255.0
E0/3	10.1.14.2	255.255.255.0
E1/0	10.1.15.2	255.255.255.0

#### Interface-Cloud

Interface	IP address	Subnet Mask
E0/0	118.1.6.2	255.255.255.0
E0/1	118.1.2.2	255.255.255.0
E0/2	118.1.3.2	255.255.255.0
E0/3	118.1.4.2	255.255.255.0
E1/0	118.1.5.2	255.255.255.0

#### Task 1 – HQ Router Configuration

- Configure the Interfaces based on the Logical Diagram
- Configure OSPF as the IGP to communicate with the MPLS Cloud. Enable all the interfaces.
- Make sure OSPF only sends and receives OSPF packets on the link towards the MPLS Cloud using the Passive-interface command.
- Configure a default route on the router towards the Internet. The IP Address of the Internet Router is 192.1.101.254
- Configure BGP between vEdge1 (199.1.1.17) in 65001 and HQ router. Redistribute OPSF into BGP.

#### HQ Router

```
hostname HQ
!
interface Ethernet0/0
  ip address 100.1.1.1 255.255.255.0
!
interface Ethernet0/1
```



```
ip address 119.1.1.2 255.255.255.0
!
interface Ethernet0/2
  ip address 10.1.11.1 255.255.255.0
!
interface Ethernet0/3
  ip address 118.1.6.1 255.255.255.0
!
router ospf 1
  passive-interface default
  no passive-interface Ethernet0/2
  network 10.1.11.0 0.0.0.255 area 0
  network 100.1.1.0 0.0.0.255 area 0
  network 118.1.1.0 0.0.0.255 area 0
  network 119.1.1.0 0.0.0.255 area 0
!
router bgp 65001
  bgp log-neighbor-changes
  redistribute ospf 1
  neighbor 199.1.1.17 remote-as 65001
!
ip route 0.0.0.0 0.0.0.0 118.1.1.2
```

## Task 2 – MPLS Cloud Router Configuration

- Configure the Interfaces based on the Logical Diagram.
- Configure OSPF as the IGP on all the interfaces.

### MPLS Cloud Router

```
hostname MPLS
!
interface Ethernet0/0
  ip address 10.1.11.2 255.255.255.0
!
interface Ethernet0/1
  ip address 10.1.12.2 255.255.255.0
  ip ospf network point-to-point
!
interface Ethernet0/2
  ip address 10.1.13.2 255.255.255.0
  ip ospf network point-to-point
!
interface Ethernet0/3
  ip address 10.1.14.2 255.255.255.0
  ip ospf network point-to-point
!
interface Ethernet1/0
  ip address 10.1.15.2 255.255.255.0
  ip ospf network point-to-point
```



```
!
router ospf 1
  network 10.1.11.0 0.0.0.255 area 0
  network 10.1.12.0 0.0.0.255 area 0
  network 10.1.13.0 0.0.0.255 area 0
  network 10.1.14.0 0.0.0.255 area 0
  network 10.1.15.0 0.0.0.255 area 0
```

### Task 3- Internet Cloud Router Configuration

- Configure the Interfaces based on the Logical Diagram
- Configure a static route on the Router for the 100.1.1.0/24 network. The Next-hop should point towards the Internet IP of the HQ Router

#### Internet Cloud Router

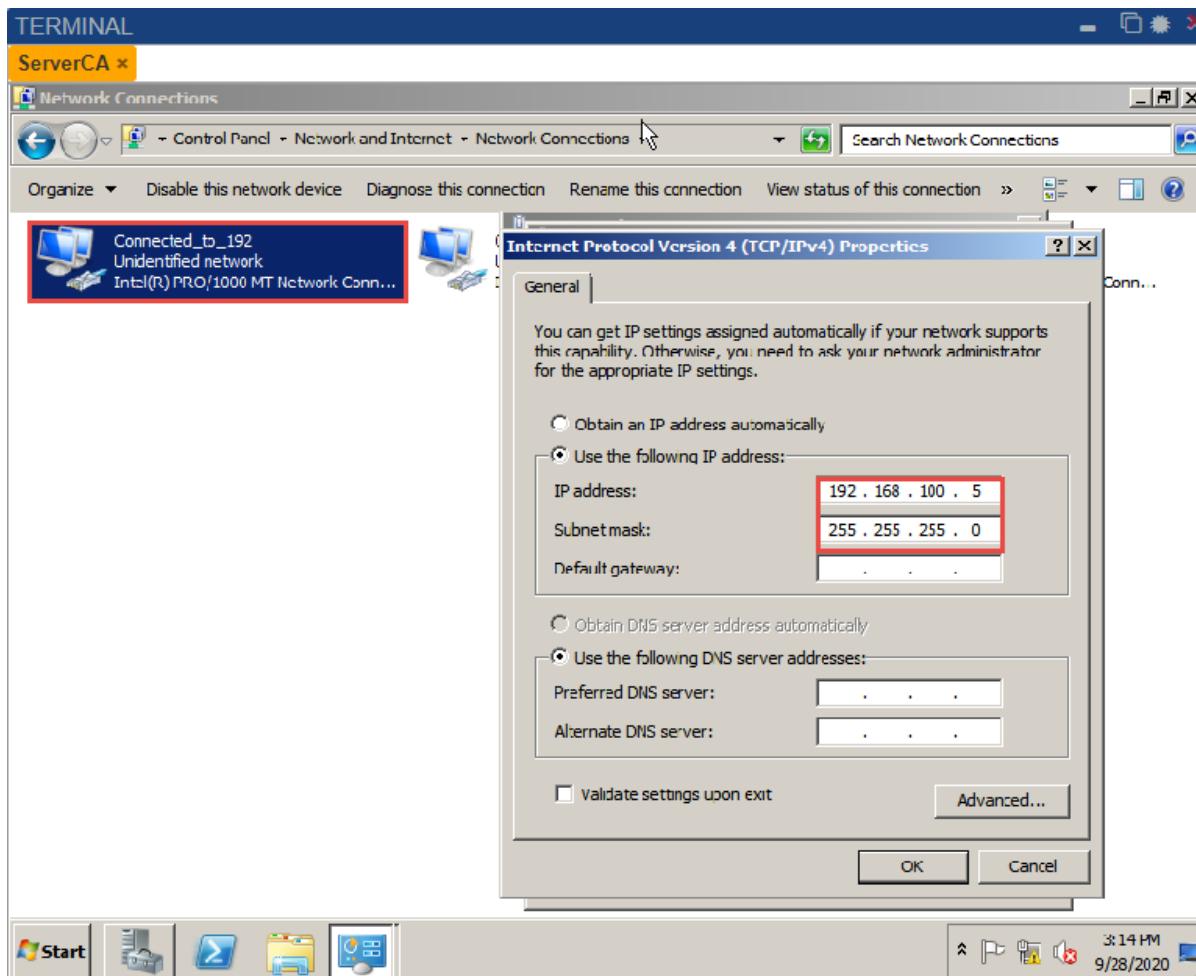
```
hostname Internet
!
no ip domain lookup
ip cef
!
interface Ethernet0/0
  ip address 118.1.1.2 255.255.255.0
!
interface Ethernet0/1
  ip address 118.1.2.1 255.255.255.0
!
interface Ethernet0/2
  ip address 118.1.3.2 255.255.255.0
!
interface Ethernet0/3
  ip address 118.1.4.2 255.255.255.0
!
interface Ethernet1/0
  ip address 118.1.5.2 255.255.255.0
!
ip route 100.1.1.0 255.255.255.0 118.1.1.1
```



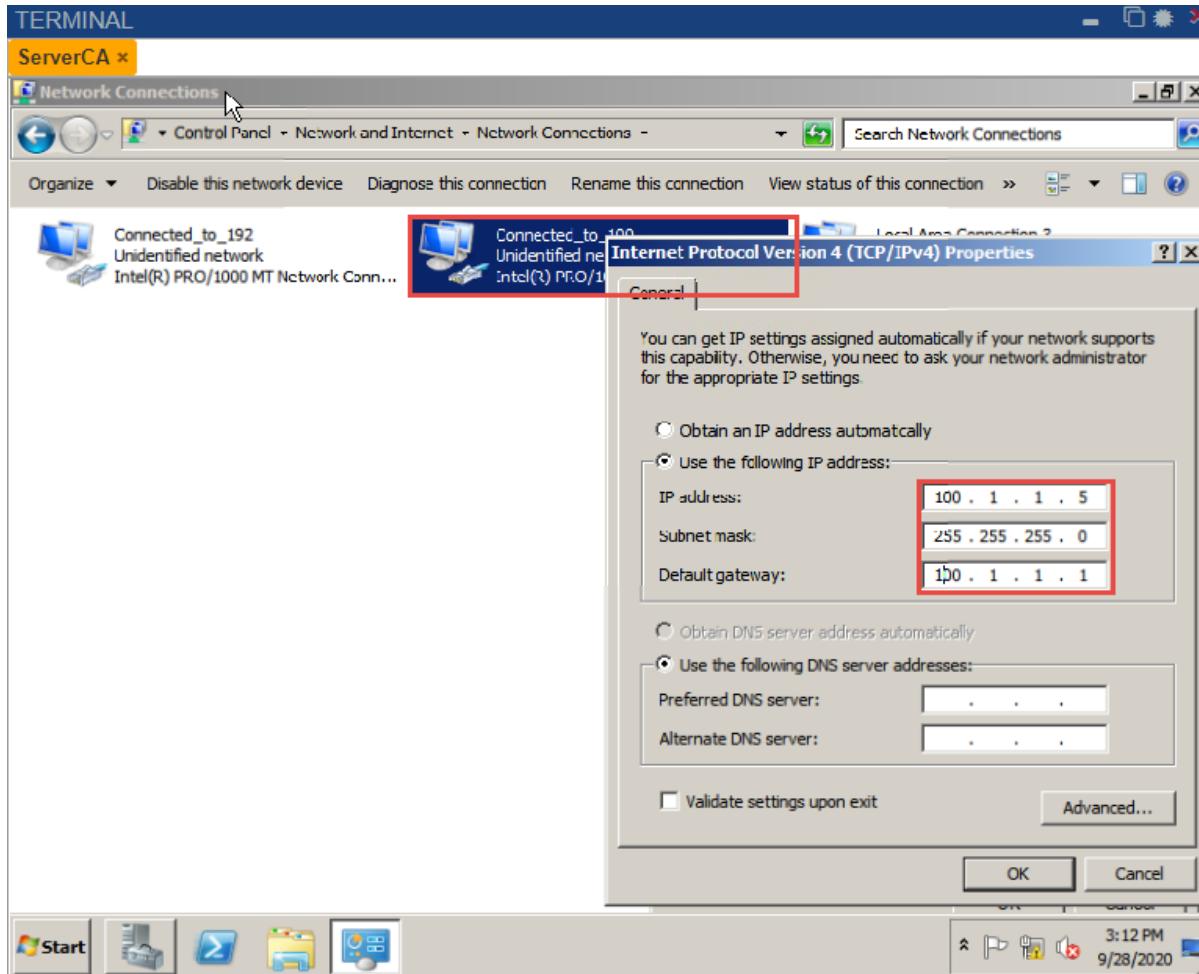
## Lab 2: Installing the Enterprise Certificate Server

### Task 1- Configure the interface

- First Ethernet Interface: Connected\_to\_192
- Ip address: 192.168.100.4
- Subnet: 255.255.255.0

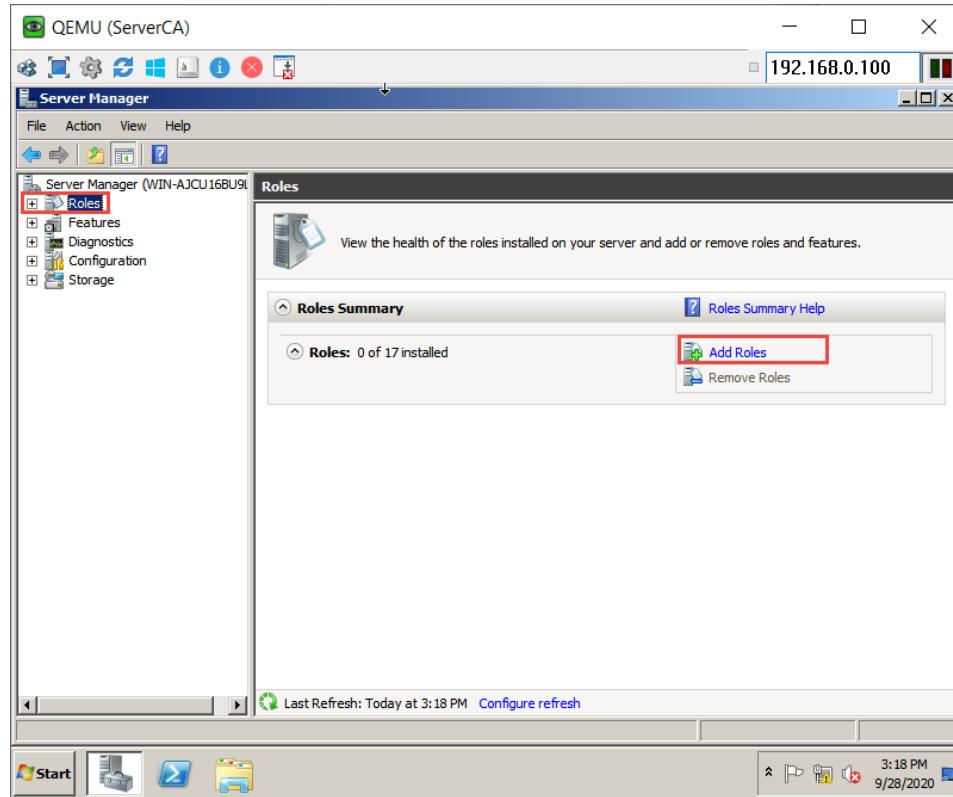


- Third Ethernet Interface: Connected\_to\_100
- Ip address: 100.1.1.5
- Netmask: 255.255.255.0
- Gateway: 100.1.1.1

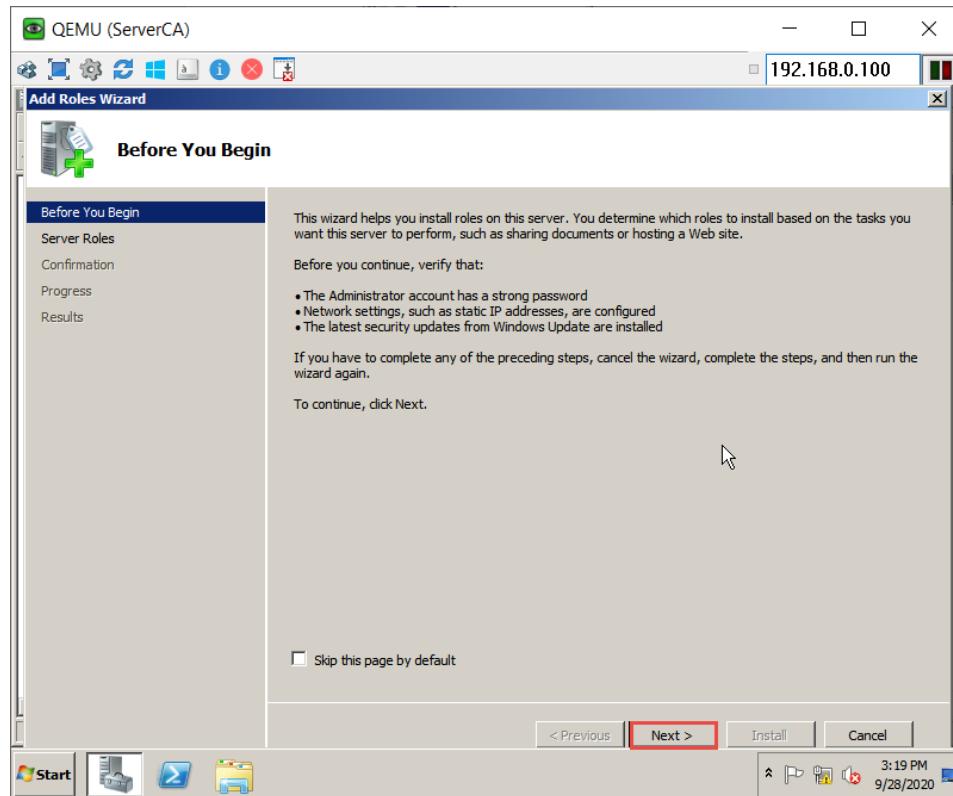


## Task 2- Installing the Enterprise Root Certificate Server

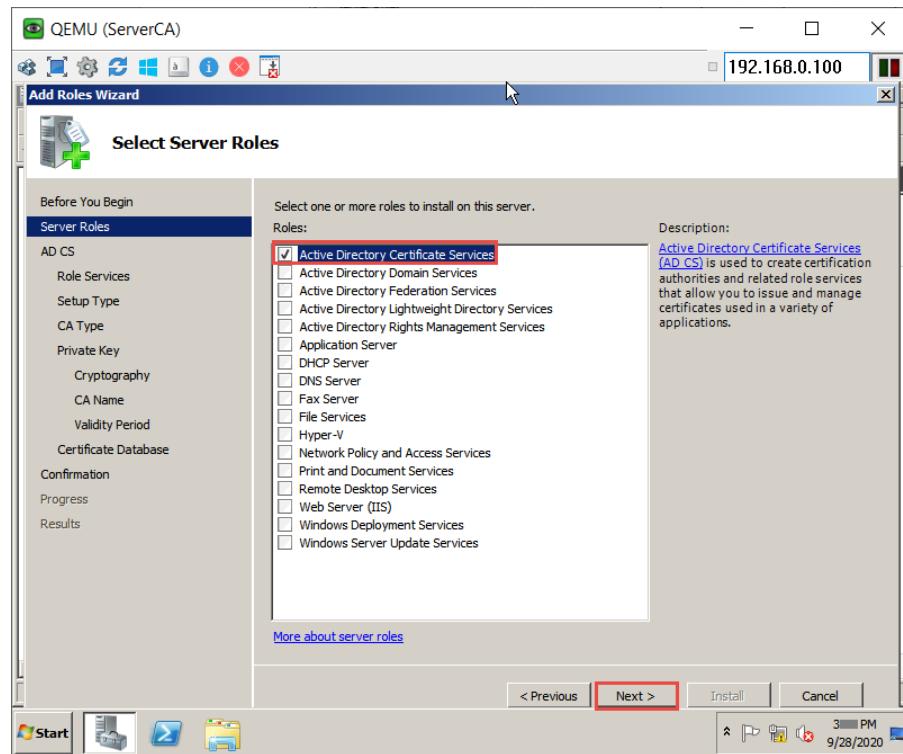
- Open Server Manager -> click Roles-> Next



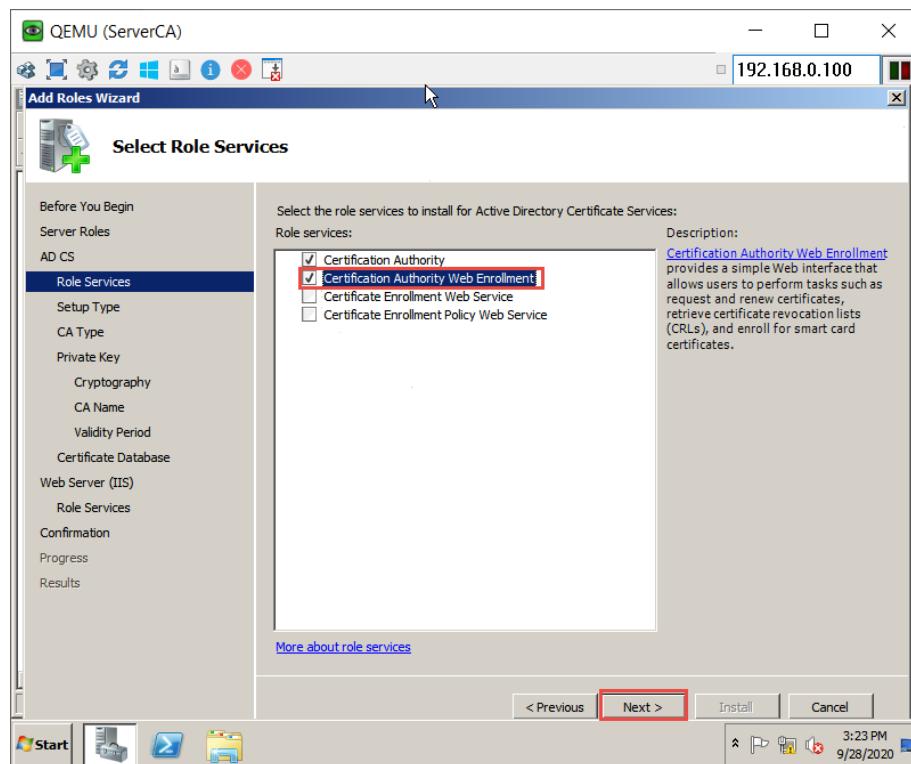
- Click Next



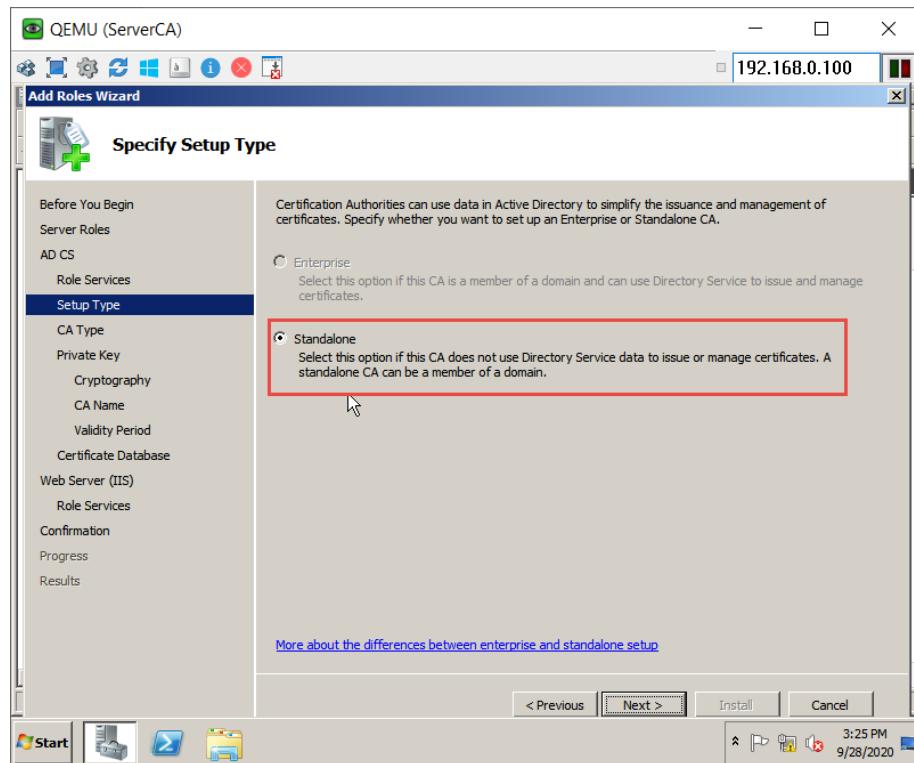
- Select the “**Active Directory Certificate Services**” and click **Next**



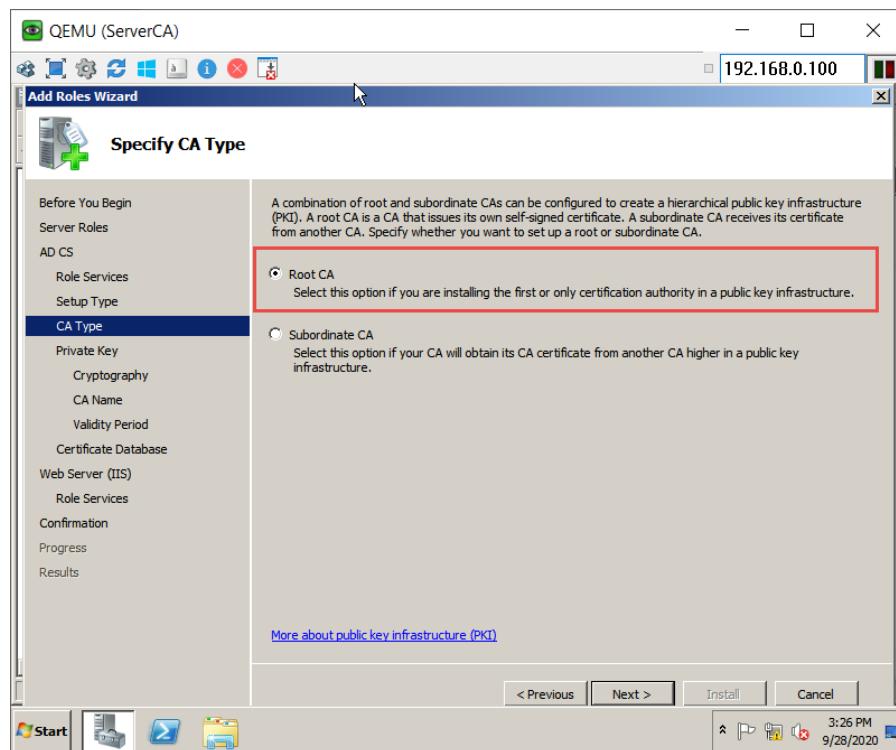
- Click **Next**
- Select “**Certification authority Web enrollment**” and click **Next**



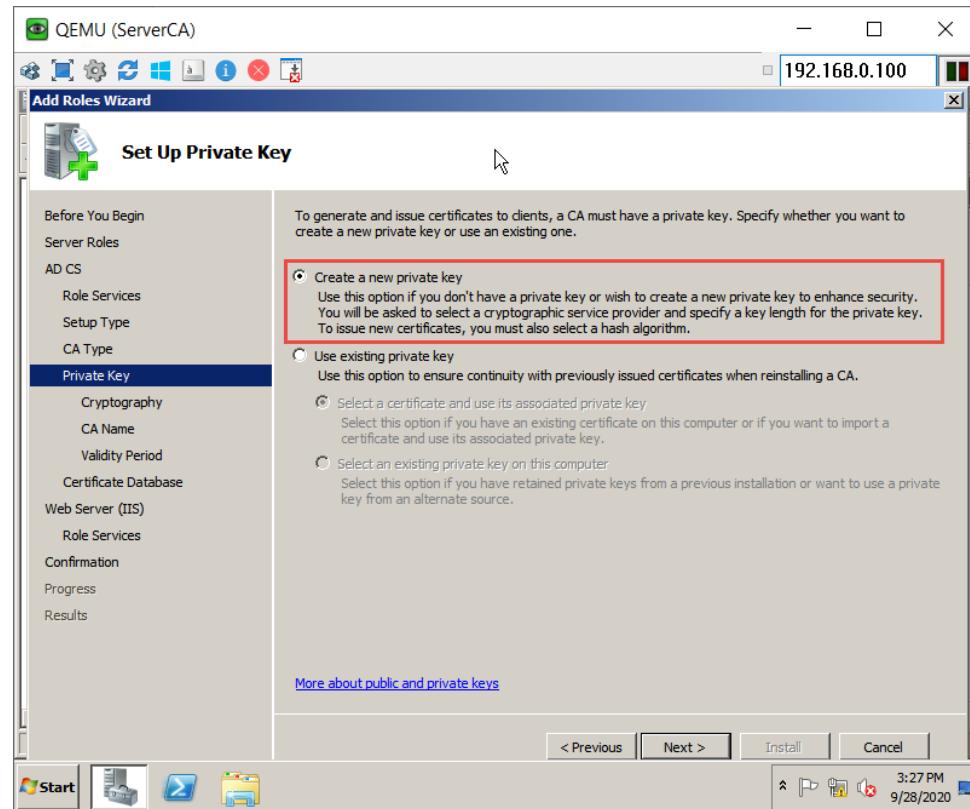
- Leave it as **Standalone** and click **Next**



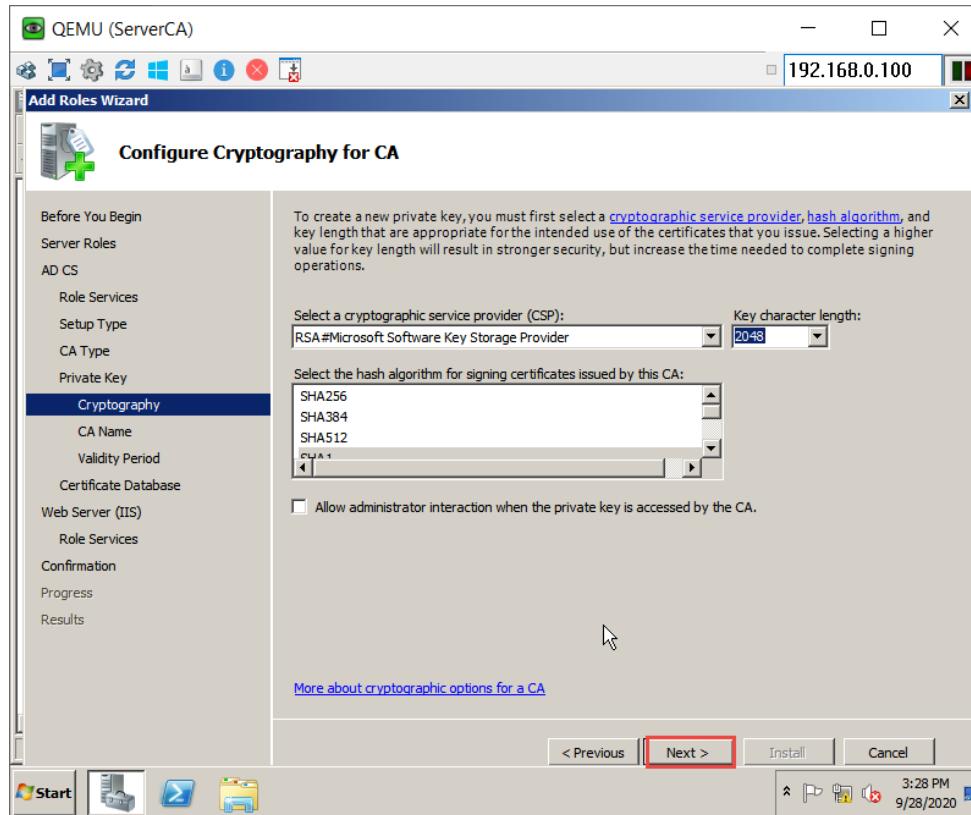
- Leave it as **Root CA** and click **Next**



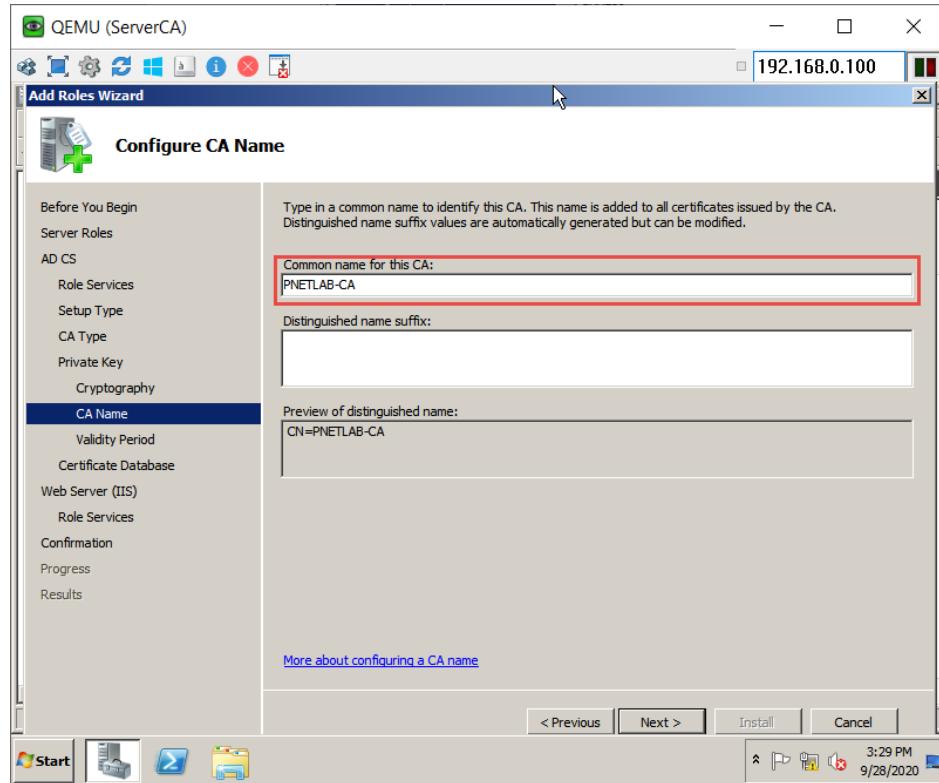
- Leave "Create a new private key" and click **Next**



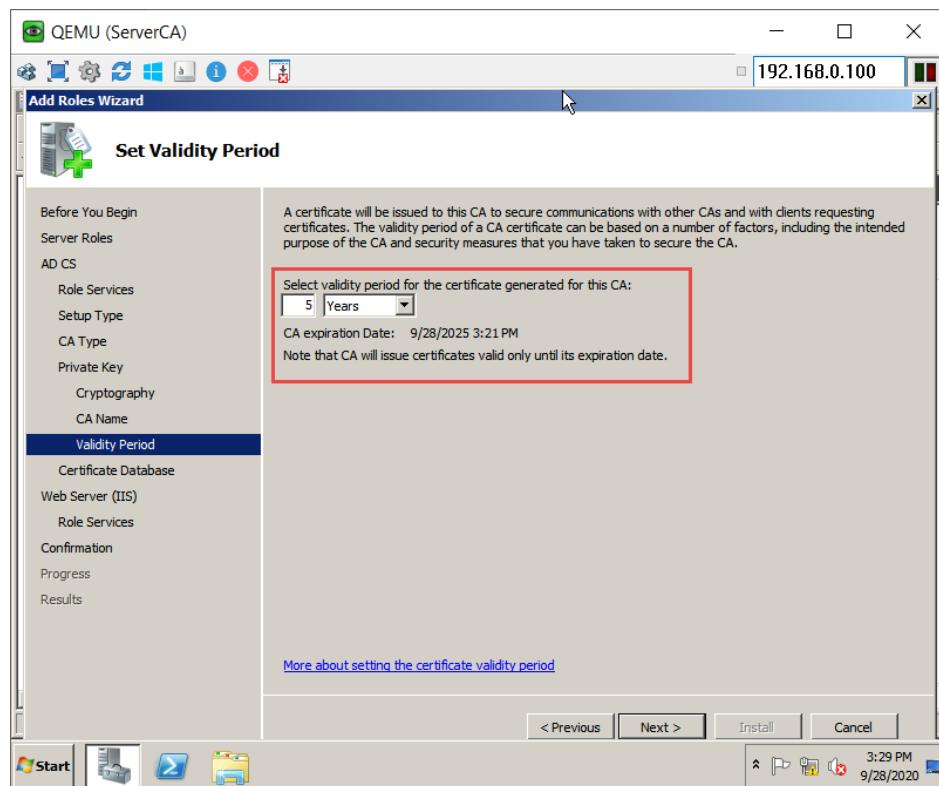
- Leave the default for the Cryptography for CA and click **Next**



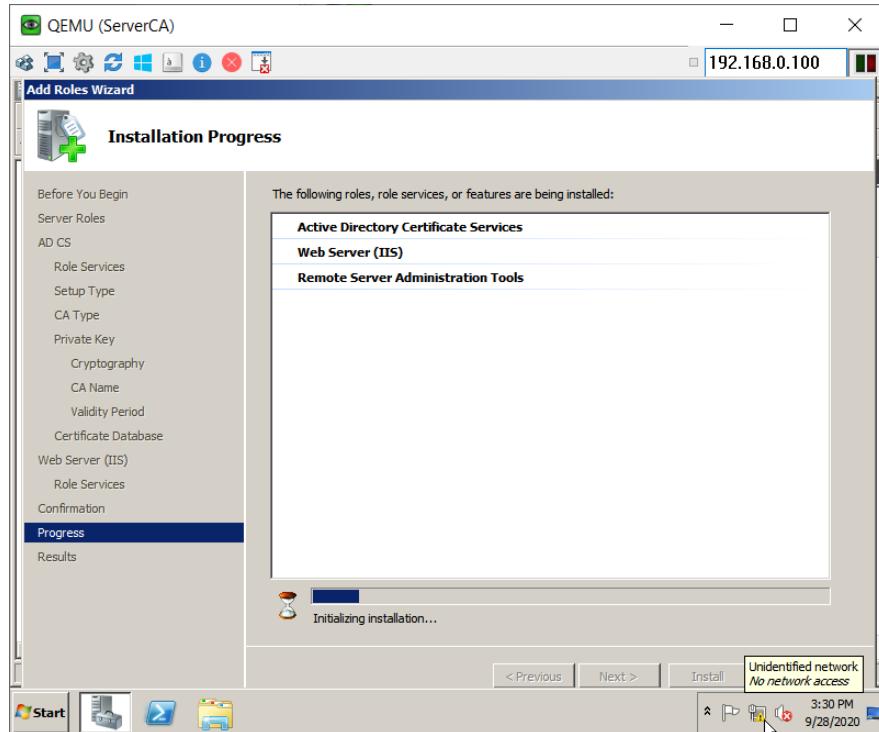
- Set the Common name as **PNETLAB-CA** and click **Next**



- Leave the default for the **Validity Period** and click **Next**



- Click Next ➔ Install



## Task 2 Install WinSCP

- Download WinSCP in this link: <https://winscp.net/eng/download.php>
- Double-click the WinSCP installation file
- Do a Default installation



## Lab 3- Initializing vManage -CLI

### Task 1- Configuring the System Component

- Configure the System parameters based on the following:
  - o Hostname: **vManage1**
  - o Organization: "**viptela sdwan**"
  - o System-IP: **100.1.1.12**
  - o SiteID: **1**
  - o Vbond Address: **100.1.1.4**
  - o Timezone: based on the appropriate Timezone

#### Note:

- Default username: **admin**, default password:**admin**

Then log in with **admin/admin**

#### vManage

```
config
!
system
host-name vManage1
system-ip 100.1.1.12
site-id 1
organization-name "viptela sdwan"
clock timezone America/Antigua
vbond 100.1.1.4
!
commit
```

### Task 2- Configured the VPN parameters

- Configure the VPN parameters based on the following:
  - o Vpn0
    - Interface eth1
    - IP address: **100.1.1.2/24**
    - Tunnel Interface
    - Tunel Services (All, NetConf, SSHD)
    - Default route: **100.1.1.1**
  - o Vpn 512
    - Interface eth0
    - Ip address: **192.168.100.2/24**



**vManage**

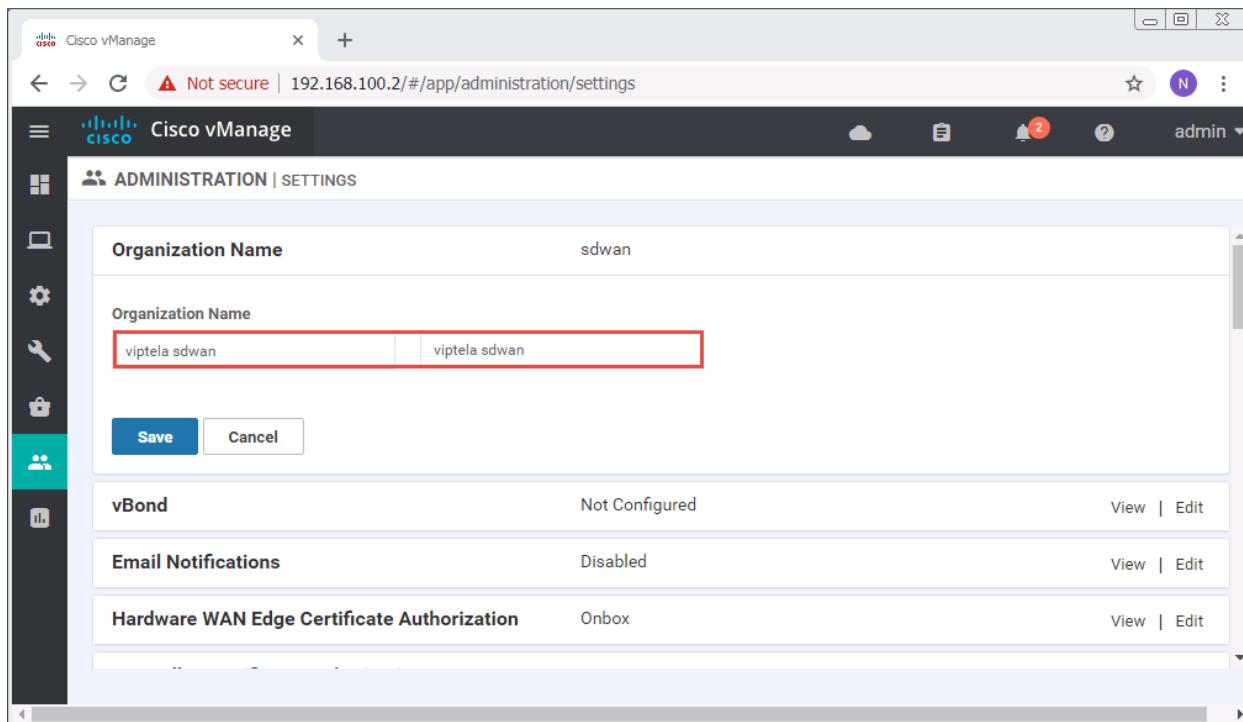
```
config
!
vpn 0
no interface eth0
interface eth1
ip address 100.1.1.2/24
tunnel-interface
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 100.1.1.1
!
vpn 512
interface eth0
ip address 192.168.100.2/24
no shut
!
commit
```



## Lab 4- Initializing vManage – GUI

### Task 1- Organization name & vBond Address

- Login into the vManage from the Server by browsing to <https://192.168.100.2:8443> using username of admin and password of admin
- Navigate to **Administration -> Settings**
- Click **Edit** on the Organization name and set it to "viptela sdwan". Confirm the Organization name. Click OK.
- Click **Edit** on the vBond address and change it to 100.1.1.4. Confirm and click **OK**.



The screenshot shows the Cisco vManage interface. The left sidebar has icons for Home, Devices, Network, Security, Applications, and Admin. The main navigation bar says "Cisco vManage" and "ADMINISTRATION | SETTINGS". The "Organization Name" field is set to "sdwan". A modal dialog is open over the main content, showing the current value "viptela sdwan" in the "Organization Name" input field, which is highlighted with a red border. Below the input fields are "Save" and "Cancel" buttons. The main content area shows other settings: "vBond" is listed as "Not Configured" with "View" and "Edit" links. "Email Notifications" is set to "Disabled" with "View" and "Edit" links. "Hardware WAN Edge Certificate Authorization" is set to "Onbox" with "View" and "Edit" links.

### Task 2 – Configure Controller Authorization as Enterprise Root and Download the Root Certificate.

- Browse to <http://100.1.1.5/certsrv>
- Click “Download Root Certificate”.



QEMU (ServerCA) Microsoft Active Directory Certificate Services – PNETLAB-CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

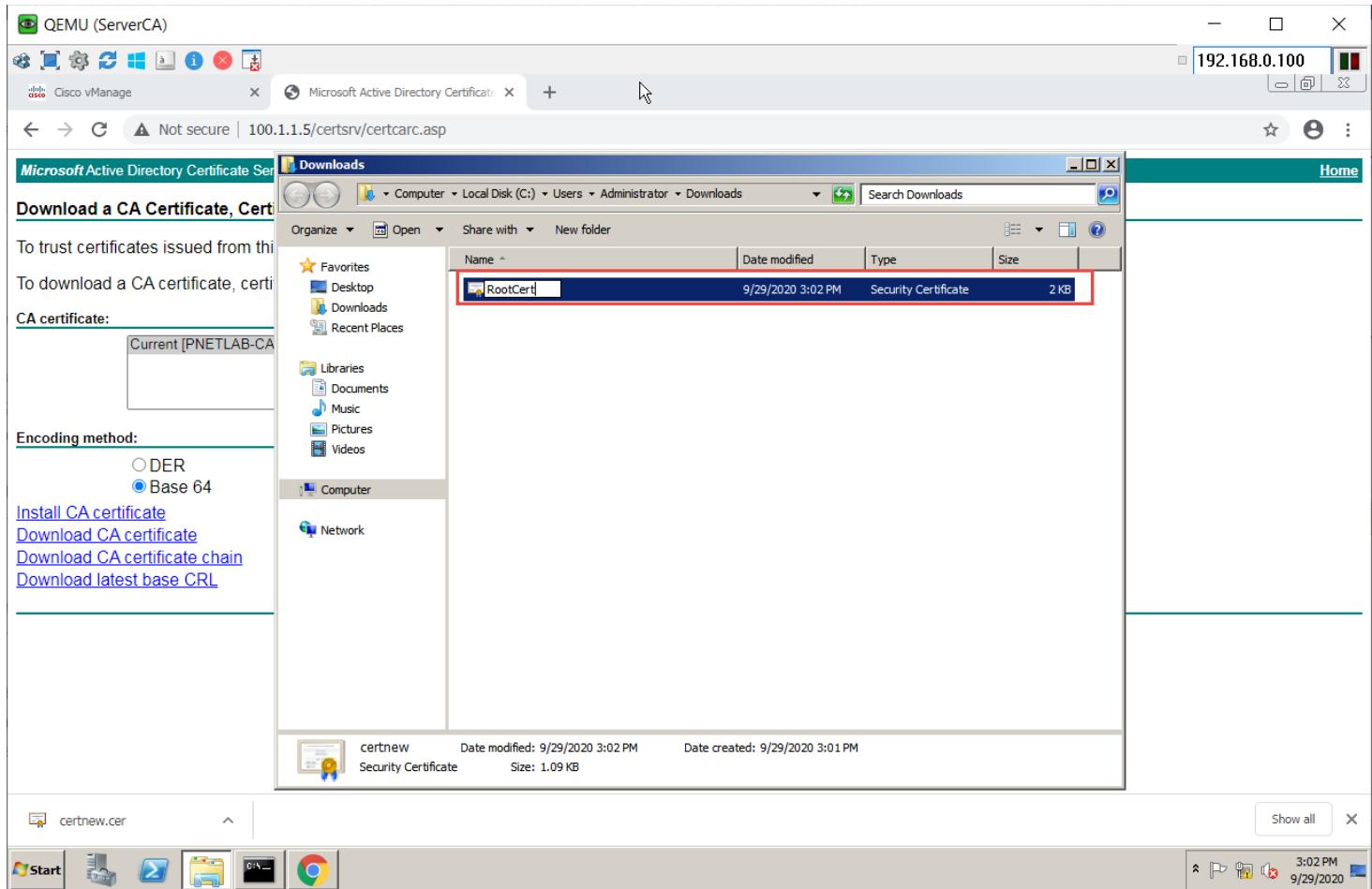
Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

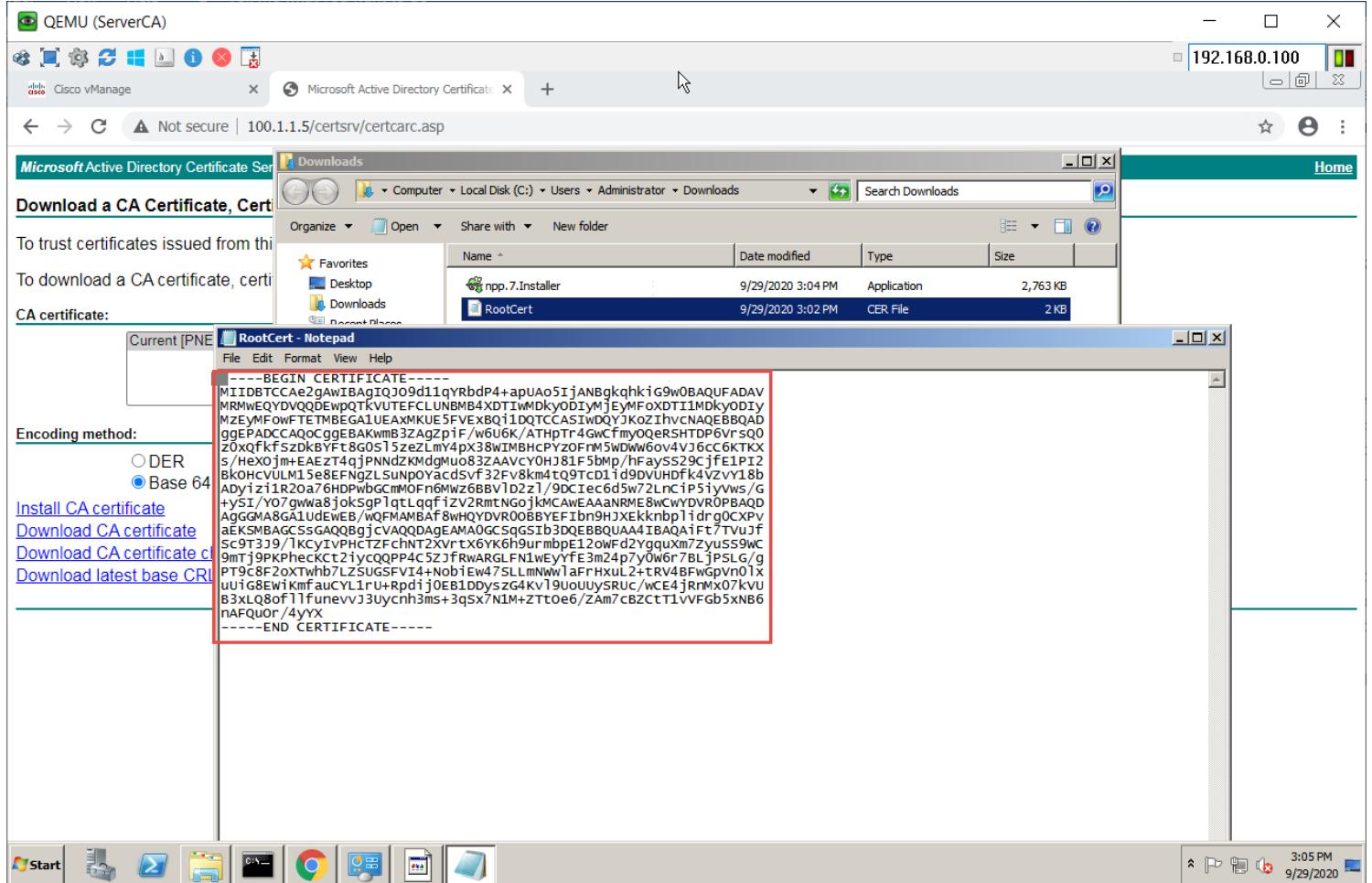
- Select “**Base 64**”.
- Click “**Download CA Certificate**”.



- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file “**Certnew**” to “**RootCert**”.



- Open the “RootCert.cer” file using Notepad.
- Copy using **CTRL-A** and **CTRL-C**.



- In vManage, Navigate to **Administration → Settings → Controller Certificate Authorization**.
- Change the “**Certificate Signing by:**” to “**Enterprise Root Certificate**”.
- Paste the **RootCert.cer** that you had copied by using **CTRL-V**.

QEMU (ServerCA)

192.168.0.100

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.2/Index.html#/app/administration/settings

admin

ADMINISTRATION | SETTINGS

Email Notifications Disabled

Controller Certificate Authorization Manual

Certificate Signing by:  Symantec Automated (Recommended)  Symantec Manual  Enterprise Root Certificate

Certificate

-----BEGIN CERTIFICATE-----  
MIIDBTCCAc2gAwIBAgIQJ09d11qYRbdP4+apUAo5ljANBgkqhkiG9w0BAQUFADAY  
MRMvE0QDVQDDEwpOTkvUTEFLUNBMB4XDThwMDkyODiyMjEyMfoXDTT1MDkyODly  
MzEvMFowfTEtMBEGA1UEAxMKUE5FVExB0I1DQTCCASiwDQYJKoZIhvNAQEBBQAD  
ggEPADCCAQoCggEBAKwmB3ZAqZpIF/w6U6K/ATHpTr4GwCfmyOQeRSHTDP6VrsQ0  
z0x0fk5zDkBYF18GOSl5zeLmV4px38WIMBHCvzOFnM5WDWW6ov4VJ6cC6KTKX  
s/HeX0jm+EAEzT4qPNNdZKMdgMu083ZAAvY0HJ81F5bMp/hFaySS29CifE1P12  
BkOHcvULM15e8EFNgZLSuNpOyacdSvf32Fv8km4tQ9TcD1id9DVUHDfk4VzvY18b  
ADyiz1R20a76HPwbGCmMOFn6MWz6BBViD2zI/9DClecd5w72LnCIP5jvVs/G  
+ySI/Y07gwWa8jokSpPqlLqgfzV2rmTNgojkMCawEAAnRMEBwCwYDVR0PBAQD  
AgGGMA8GA1UdEwEB/wQFAMB Af8wHQYDVROOBByEFlbn9HJXEkknbpldrg0CXPv  
aEKSMBA GCSeGAQOBjicVAQDDAgEAMAOGCSqGSlb3DQEBCQAA4iBAQAfI77Vujf  
Sc9T3J9/KCylvPHcTZfchNT2XVrtX6K6h9urmbeE12oWFd2YgguKm72yuSS9WC  
9mTjPKFheekCt2ivcQOPP4C5ZJRwARGLfNT1wEyFE3m24p7y0W6r7BLPSLG/g  
PT9c8F2oXTwhb7LZSUGSFV14+NobiEw47SLlMnNWwlaFrhxuL2+RV4BFwGpVn0lx  
uIG8EWiKmfauCYL1rU+Rpdi0EB1DDyszG4Kv19UoUUySRUc/wCE4RnMx07kVU  
B3xL08eflfunevJ3Uycnh3ms+3qSx7N1M+ZTt0e6/ZAm7cBZCtT1vF6b5xNB6

Select a file

3:07 PM 9/29/2020

- Set the CSR Parameters with the Organization name, City, State, Country. Set the Time to 3 Years and save.



The screenshot shows the Cisco vManage Administration Settings page. A red box highlights the 'Set CSR Properties' checkbox. Another red box highlights the 'Domain Name' field containing 'PNETLAB.COM'. A third red box highlights the 'Organizational Unit' field containing 'PNETLAB'. A fourth red box highlights the 'Organization' field containing 'PNETLAB'. A fifth red box highlights the 'City' field containing 'PNETLAB'. A sixth red box highlights the 'State' field containing 'PNETLAB'. A seventh red box highlights the 'Email' field containing 'pnetlab@gmail.com'. A eighth red box highlights the '2-Letter Country Code' field containing 'US'. A ninth red box highlights the 'Validity' dropdown menu showing '3 Years'.

**Note:** with sdwan version 20, **You must uncheck "Set CSR Properties"** due to the bug on the version

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvp75927>



### Task 3- Generate a CSR for vManage

- Navigate to Configuration -> Certificates -> Controllers -> vManage -> Generate CSR

The screenshot shows the Cisco vManage web interface. The user is navigating through the 'Configuration' > 'Certificates' > 'Controllers' > 'vManage' path. In the 'vManage' section, there is a table with one row. The last column of the table has a three-dot menu icon. A red arrow points to this icon. A context menu is displayed, listing several options: 'View CSR', 'View Certificate', 'Generate CSR' (which is highlighted with a red box), 'Reset RSA', and 'Invalidate'. The table data is as follows:

Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date	uuid
CSR Generated	vManage	vManage1	10.1.1.101	1	No certificate installed	-	f79d5... ***

- It will open a windows with CSR. Copy by using **CTRL-A** and **CTRL-C**

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Screenshot of a Cisco vManage interface showing the generation of a CSR (Certificate Signing Request). The CSR content is displayed in a modal window:

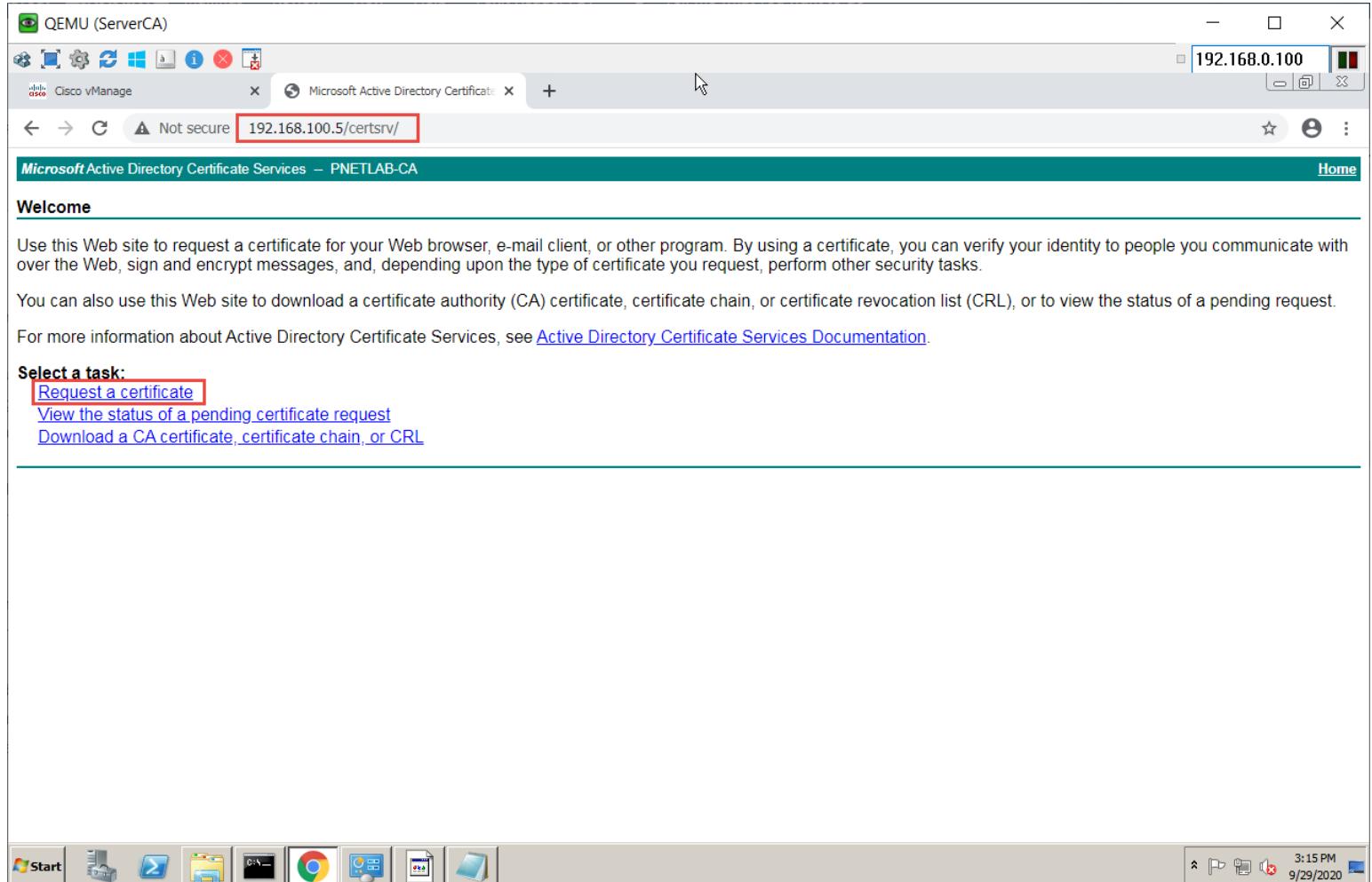
```
--BEGIN CERTIFICATE REQUEST--  
MIIDOTCCAjECAQAwgbqxCzAJBgNVBAYTAjVTMRAwDgYDVQQIEwdQTkVUTEFC  
MRaw  
DgYDVQQHEwdQTkVUTEFCMRAwDgYDVQQLEwdQTkVUTEFCMRAwDgYDVQQK  
EwdQTkVU  
TEFCMT8wPQYDVQQDEzZ2bWFuYWdlLWY30WQ1MzAyLWJhNTUtNDIyMC05M  
GM0LWFh  
MjIjMWMxNDJMS0wLIBORVRMQUxDAeBgkqhkiG9w0BCQEWEXBuZXRsYWJA  
Z21h  
eWwuY29tMIIBjANBgkqhkiG9w0BAQEAAQ8AMIIIBCgKCAQEAvw/4iSYv1/u  
o  
KaHgC/f8fGkmFOOWLz+MJH0db5eL4T6UEIEIFXL8Z57t6/H//VgnJ/3Q9XAdq  
TRxL0gtu0fTUgcmB8Hwb1m03sxDr5qY8H2wavkwRRTFDAUvYS38gsViQDoX1SL  
-----
```

The interface shows a WAN Edge List and a Controllers tab. The Controllers tab is active, showing one entry: "CSR Generated" (Operation Status) and "vManage" (Controller Type). A progress bar at the bottom indicates the task is complete.



## Task 4 – Request a Certificate from the CA Server

- Browser to <http://192.168.1.5/certsrv>
- Click “Request a Certificate”



QEMU (ServerCA)

192.168.0.100

Not secure 192.168.100.5/certsrv/

Microsoft Active Directory Certificate Services – PNETLAB-CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#) (highlighted with a red box)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

- Select “Advanced”

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Screenshot of a web browser window showing the Microsoft Active Directory Certificate Services - PNETLAB-CA interface. The URL is 192.168.0.100/certsrv/certrqus.asp. The page displays options for requesting a certificate, including "Web Browser Certificate" and "E-Mail Protection Certificate". A link to "advanced certificate request" is highlighted with a red box. The browser toolbar at the top shows tabs for "Cisco vManage" and "Microsoft Active Directory Certificate". The taskbar at the bottom includes icons for Start, File Explorer, Task View, File Explorer, Task View, File Explorer, Task View, and Task View.

- Paste the CSR in the box by using **CTRL-V** and click submit



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.5/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services – PNELAB-CA Home

**Submit a Certificate Request or Renewal Request**

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
1e+80r9YIor5Fwu29+MPABzzNVG2L6EZ1BJwzo^
UvzgtPCSmNDACHq7gFeRtu9VKkSLxRaGL1zc1a
FjmuyRzx7bgA7yxXl1Jhd0ZQNGSYuwTupvs2Gv
WrVDMuFtJzY6w1Y/Pg==
-----END CERTIFICATE REQUEST-----
```

**Additional Attributes:**

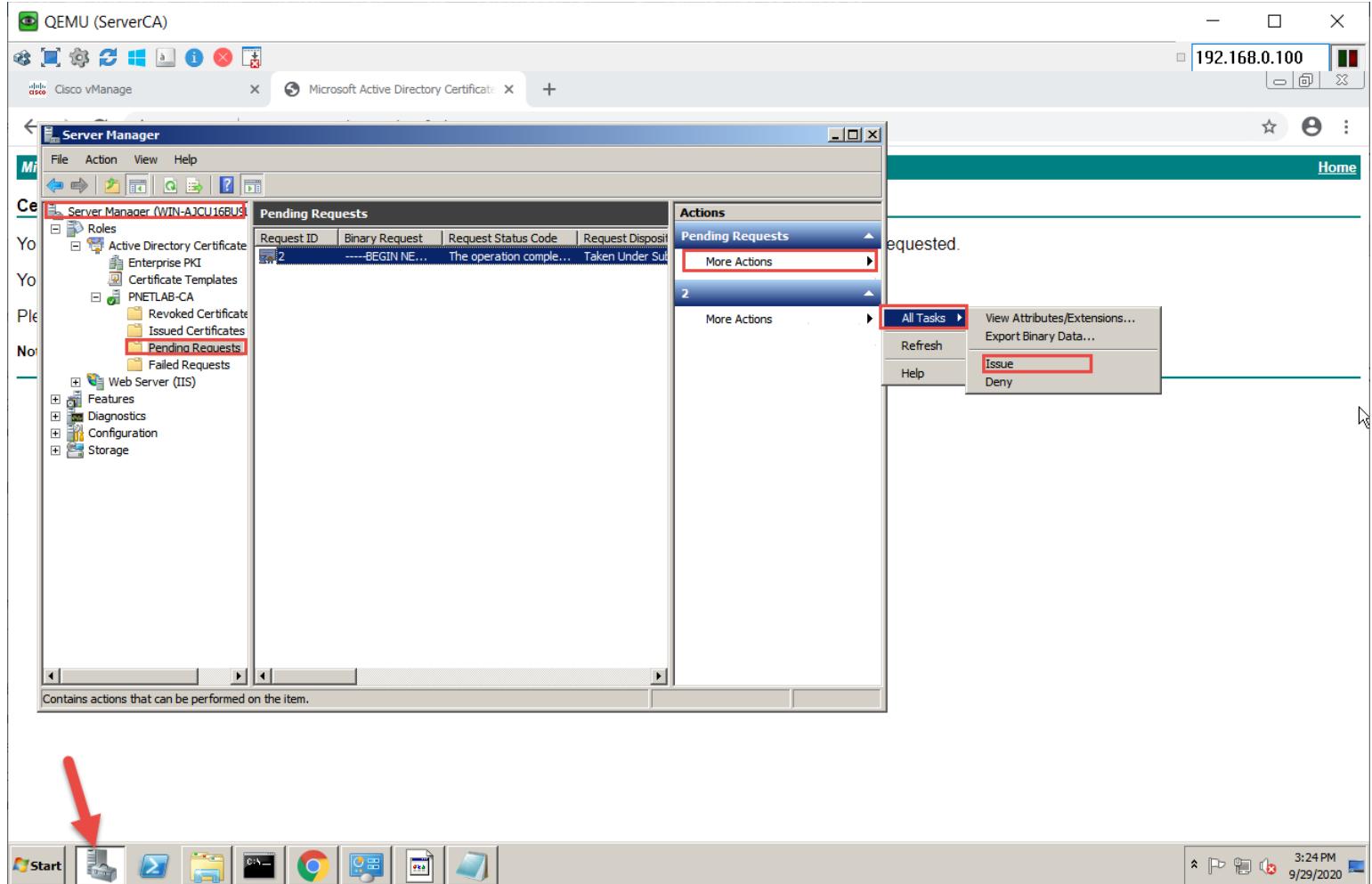
Attributes:

**Submit >**

Start | Taskbar icons | Date/Time: 3:18 PM 9/29/2020

## Task 5 – Issue the Certificate from the CA Server

- Open Server Manager → Roles → Active Directory Certificate Server → PNETLAB-CA → Pending Request.
- Right-click the request → more action → all tasks and click “Issue”





## Task 6- Downloading the Issued Certificate

- Browser to <http://192.168.100.5/certsrv>
- Click “Check on Pending Certificate Request”

Microsoft Active Directory Certificate Services – PNETLAB-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

- The issued certificate link will show up. Click on the link

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate Services – PNETLAB-CA Home

View the Status of a Pending Certificate Request

Select the certificate request you want to view:  
[Saved-Request Certificate \(9/29/2020 3:18:49 PM\)](#)

Start File Internet Explorer Google Chrome File View Insert Tools Help 3:27 PM 9/29/2020

The screenshot shows a Windows desktop environment with a browser window open to the Microsoft Active Directory Certificate Services interface. The URL in the address bar is 192.168.0.100. The page displays a pending certificate request titled 'Saved-Request Certificate (9/29/2020 3:18:49 PM)'. The taskbar at the bottom shows various pinned icons and the current date and time as 3:27 PM on 9/29/2020.

- Select “Base 64” and click “Download”



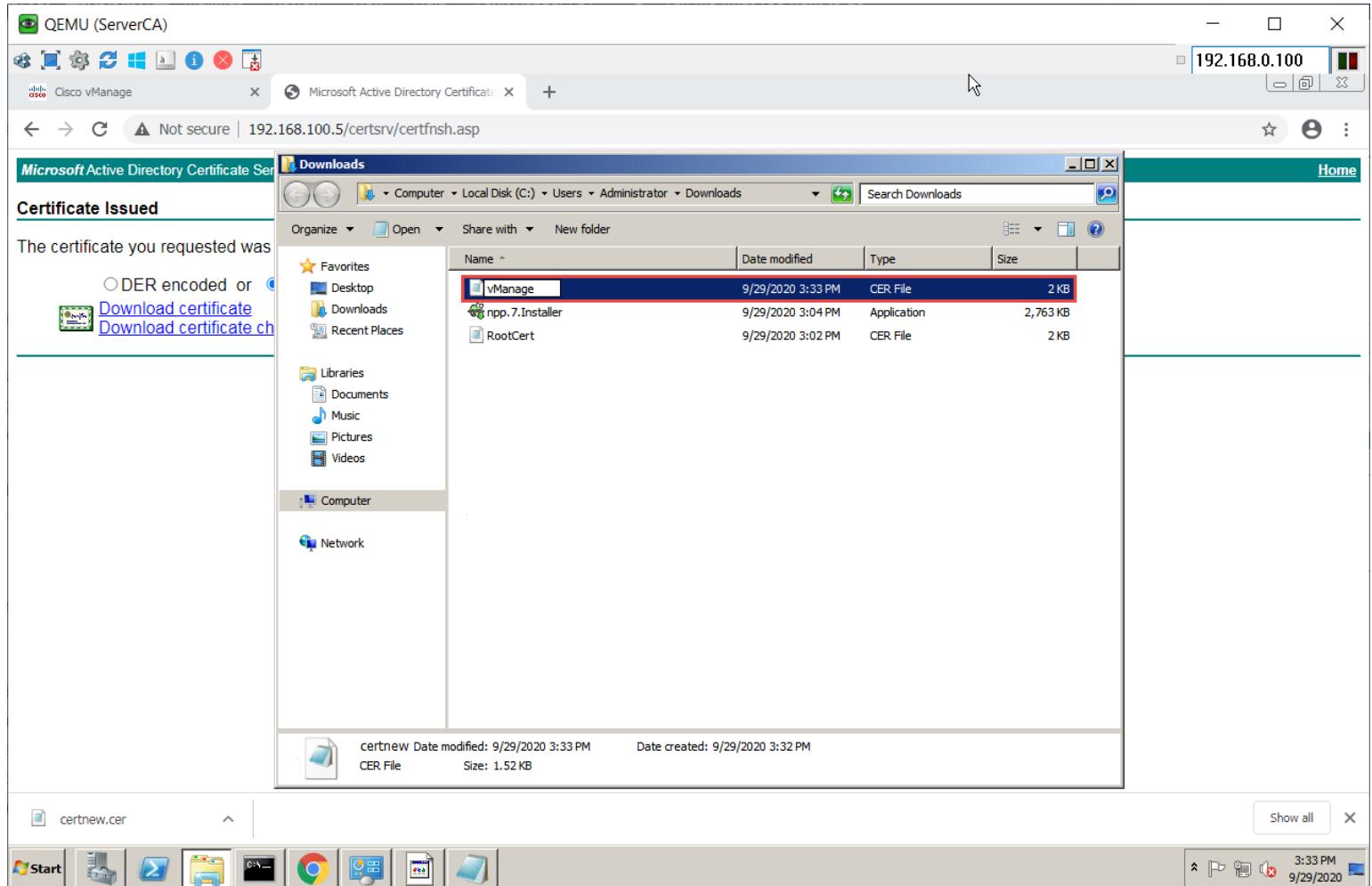
The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

[Download certificate](#) [Download certificate chain](#)

- Open explorer and navigate to the downloads folder.
- Change the name of the Downloaded file “**Certnew**” to “**vManage**”





The screenshot shows a Windows desktop environment. In the center, a Microsoft Edge browser window is open, displaying a certificate issuance page from a QEMU-based ServerCA. The URL is 192.168.0.100. The page shows a certificate named 'vManage' has been issued. Below the browser is a standard Windows file explorer window titled 'Downloads'. It lists three files: 'vManage.cer' (selected and highlighted in red), 'npp.7.Installer', and 'RootCert'. The 'vManage.cer' file was created on 9/29/2020 at 3:32 PM and is a 1.52 KB CER File. The taskbar at the bottom shows the 'certnew.cer' file is currently active. The system tray in the bottom right corner shows the date and time as 3:33 PM on 9/29/2020.

- Open the “vManage.cer” file using Notepad
- Copy using **CTRL-A** and **CTRL-C**



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.5/certsrv/certfnsh.asp

Microsoft Active Directory Certificate Server

Certificate Issued

The certificate you requested was

DER encoded or  Base64 encoded

[Download certificate](#) [Download certificate \(.crt\)](#)

Downloads

Name	Date modified	Type	Size
npp.7.Installer	9/29/2020 3:04 PM	Application	2,763 KB
RootCert	9/29/2020 3:02 PM	CER File	2 KB
vManage	9/29/2020 3:33 PM	CER File	2 KB

vManage - Notepad

```
-----BEGIN CERTIFICATE-----
MIIEERTCCAYzGAWIBAQIKGBVZXwAAAAAAjANBgkqhkiG9w0BAQUFADAVMRMwEQYD
VQQDEwp0TkVUTEFLUNBMB4XDIIwMDkyOTIyMTYwN10xdTIXmDkyOTIyMjYwN1ow
gbgXCzA2BgnVBAYTA1VTMRawDgYDVQqIEwd0tKvUTEFCMRawDgYDVQqHEwd0tKvU
TEFCMRawDgYDVQqKEwd0tKvUTEFCMRawDgYDVQqLEwd0tKvUTEFCMT8wPOYDVQOD
Ezz2bwFluywld1LWY30wQ1mZayLwJhNTUTNDIMC05MG0LwFhmjljMWWXNDj1MS0x
L1B0RVRMQuixIDAeBgkqhkiG9w0BCQEWExBuZXRSYwJAZ21haiwuY29tMIIBiJAN
BgkqhkiG9w0BAQEFAOCAQ8AMIIIBCgKCAQEAwg/4iSYv1/uokaffgc/f8fGknFOO
WLz+MjH0db5eL4T6UE1EFXL8257t6/H/Vgnrj/3Q9XAdqjTRXLogtu0FTugcmb
8Hwblm03sxb5qY8H2zwavkwRTFDAUVYS3BgsV1Qb0x1SLMy1Bqho+yZ+12Vwv3
8j0kw4Oaaok7b5jM1hxJwYkmgoYosR1pkMTB6HbchTZHfkHCGLA2S2jzdndq75Tu
Yiwa2i45c+8za5fd1seod4d1H3T2c16ps+bc3Pc1M6prCFUwcdnp0168uoCr
NFET63ZFEEwz5bchgfomxt9v9ffJB5dfi0ymGRZENSK5M0oyRX87yg8oIDAQAB
04HYMIHVMAGA1udEweb/wQCMAAwHOYDVRO0BBYEF17bkcy0yLDub7nmpMI7kxa
ohzvMB8GA1udIwQYMaAFIbn9HjxeEkknbplidrg0CXpvaeKSMEEGA1udHwQ6MDgw
NoA00DGmGzpbGu6ly9XSU4tQupdvTE2Q1U5TEcv02Q1U5TEdfUE5FVEXBQ11D
QS5jcnqwDQYJkozIhvNAQEFBQAQdgGEBAEGxxf1KHsJJacWPOMAkwearejzh02/I
M8uxAtS1575upqHcd69qw8NCXLBTTThalY/4bk5ML10ng5fffeezjLk1Ln1nqovP
FRTfmQSS1exONV2LxpCm58+k96xrc5rblkdsqyezzhgXkjkpmFZjnwh9ACN3
ofrcjpxfliu6wkvGgl1/2ppbe90MZ624NUxNyNnh+65v7vrksIM1fgM7Axfx
wuy980G+HTZQMyupFYKKDIwC3EK3mkmtE20ucG1L07Z16TF15TOrZLEMTCmch5x
nA0v5QAR16/pZxtql27YX8+yAqjFOOsMyvac8hwviM8Lf1c-h91fh+g=
-----END CERTIFICATE-----
```

certnew.cer

Start

3:34 PM 9/29/2020



## Task 7- Installing the Identity Certificate for vManage

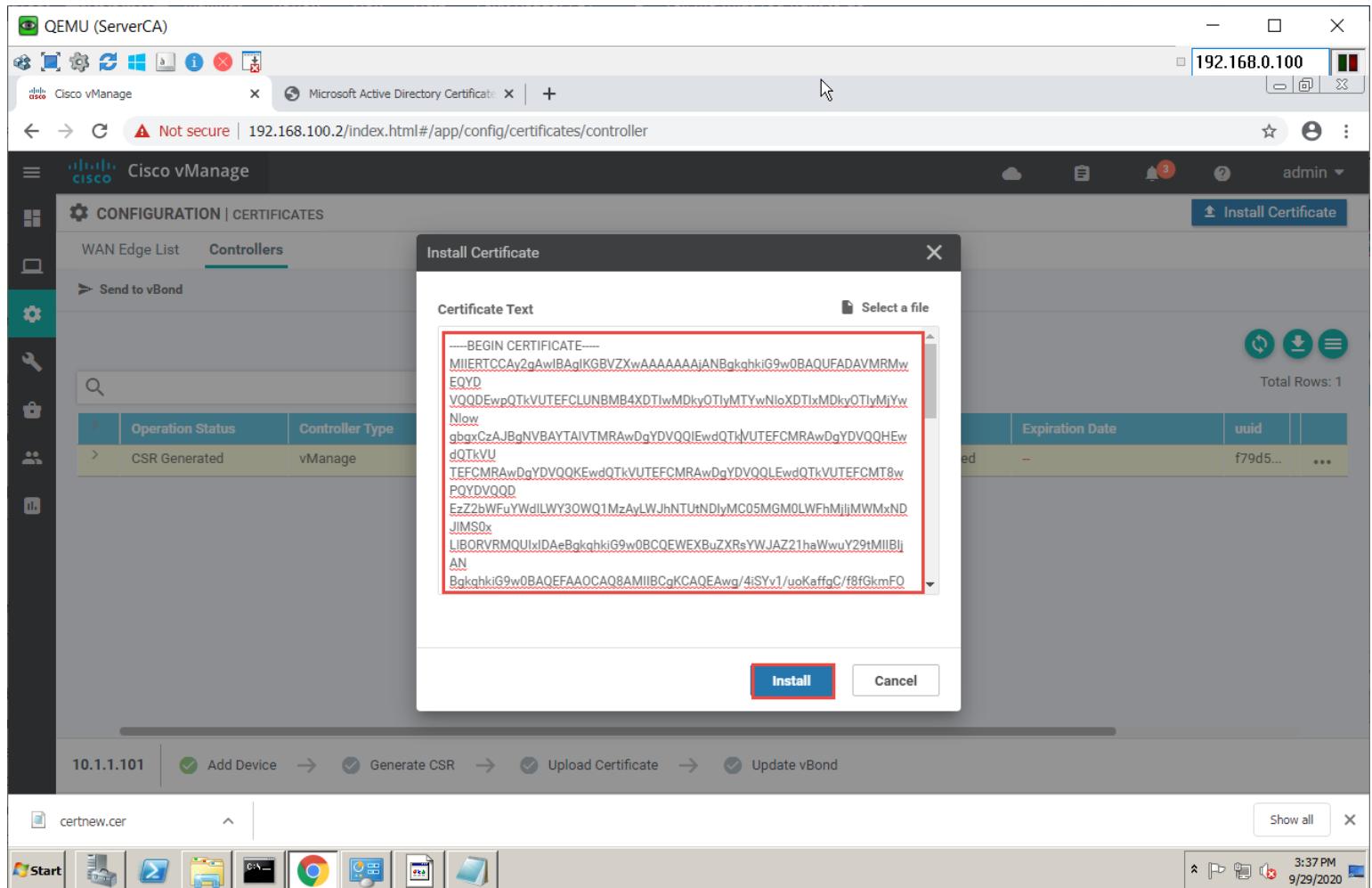
- In vManage, Navigate to Configuration → Certificate → Controller
- Click on the “install” button at the top right corner

The screenshot shows the Cisco vManage web interface. The URL in the browser is [192.168.100.2/index.html#/app/config/certificates/controller](http://192.168.100.2/index.html#/app/config/certificates/controller). The page title is "Cisco vManage". On the right side, there is a red box highlighting the "Install Certificate" button. The main content area shows a table with one row of data:

Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date	uuid
CSR Generated	vManage	vManage1	10.1.1.101	1	No certificate installed	-	f79d5...

At the bottom of the interface, there is a navigation bar with steps: 10.1.1.101 → Add Device → Generate CSR → Upload Certificate → Update vBond. Below the interface, a taskbar shows icons for Start, File Explorer, Task View, File Explorer, Google Chrome, File Explorer, and File Explorer. The system tray shows the date and time as 3:37 PM 9/29/2020.

- Paste the Certificate (**CTRL-V**) and **Install**



The screenshot shows the Cisco vManage web interface. In the center, a modal window titled "Install Certificate" is open. Inside the modal, there is a text area labeled "Certificate Text" containing a long string of certificate data. This data is highlighted with a red rectangular selection. At the bottom of the modal are two buttons: "Install" (highlighted with a blue border) and "Cancel". The background of the main interface shows a table with columns "Operation Status" and "Controller Type", and a search bar. The status for one row is listed as "CSR Generated". The top right corner of the screen shows the IP address "192.168.0.100".

- The identity certificate should be installed on vManage



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.0.100

Cisco vManage

TASK VIEW

Install Certificate

Total Task: 1 | Success : 1

Initiated By: admin From: 169.254.0.253

Search Options

Status Message Device Type Device IP vManage IP

Status	Message	Device Type	Device IP	vManage IP
Success	Successfully synced vEdge list on v... vManage	f79d5302-ba55-4220-90c4-aa29c1c...	10.1.1.101	
	[30-Sep-2020 17:59:17 AST] Install Certificate, on device f79d5302-ba55-4220-90c4-aa29c1c142e1, started by user "admin" from IP address "169.254.0.253" [30-Sep-2020 17:59:18 AST] Pushing serial list to vManage-f79d5302-ba55-4220-90c4-aa29c1c142e1 (vManage1) [30-Sep-2020 17:59:18 AST] Started processing serial list file on vManage-f79d5302-ba55-4220-90c4-aa29c1c142e1 (vManage1) [30-Sep-2020 17:59:19 AST] Completed processing serial list file on vManage-f79d5302-ba55-4220-90c4-aa29c1c142e1 (vManage1) [30-Sep-2020 17:59:20 AST] Done - Push vSmart List for vManage-f79d5302-ba55-4220-90c4-aa29c1c142e1 (vManage1) [30-Sep-2020 17:59:20 AST] Pushed serial list to vManage-f79d5302-ba55-4220-90c4-aa29c1c142e1 (vManage1) [30-Sep-2020 17:59:20 AST] Updated controllers with new certificate serial number of vManage-f79d5302-ba55-4220-90c4-aa29c1c142e1			

Total Rows: 1

Start

7:59 PM 9/30/2020



## Lab 5- Initializing vBond – CLI

### Task 1- Configuring the System component

- Configure the System parameters based on the following:
  - o Hostname: **vBond1**
  - o Organization: "viptela sdwan"
  - o System-IP: **100.1.1.14**
  - o Site ID: 1
  - o vbond Address: **100.1.1.4**
  - o Timezone: based on the appropriate timezone

#### Note:

Default username: admin, default password: admin

#### vBond

```
config
!
system
host-name vBond1
system-ip 100.1.1.14
site-id 1
organization-name "viptela sdwan"
clock timezone America/Antigua
vbond 100.1.1.4 local
!
commit
```

### Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:
  - o Vpn 0
    - Interface ge0/0
    - Ip address: 100.1.1.4/24
    - Tunnel interface
    - Tunnel Services (all, Netconf, sshhd)
    - Encapsulation: IPSec
    - Default route: 100.1.1.1
  - o Vpn 512
    - Interface eth0
    - Ip address: 192.168.100.4

#### vBond

```
config
!
vpn 0
no interface eth0
```





```
interface ge0/0
ip address 100.1.1.4/24
tunnel-interface
encapsulation ipsec
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 100.1.1.1
!
vpn 512
interface eth0
ip address 192.168.100.4/24
no shut
!
commit
```



## Lab 6- Initializing vBond -GUI

### Task 1 – Add vBond to vManage

- Navigate to Configuration → Devices → Controllers → Add Controllers – vBond and specify the following to add the vBond in vManage.
  - IP Address: **100.1.1.4**
  - Username: **admin**
  - Password: **admin**
  - Check Generate CSR
  - Click OK

The screenshot shows the Cisco vManage web interface. The URL in the address bar is <http://192.168.100.2/index.html#/app/config/devices/controller>. The page title is "Cisco vManage". On the left, there's a sidebar with various icons. The main content area shows a table for "WAN Edge List" and a "Controllers" tab. A modal dialog box titled "Add vBond" is open in the center. The "vBond Management IP Address" field contains "100.1.1.4". The "Username" field contains "admin". The "Password" field contains "\*\*\*\*". The "Generate CSR" checkbox is checked. At the bottom of the dialog are "Add" and "Cancel" buttons.



## Task 2 – View the generated CSR for vBond and copy it

- Navigate to Configuration → Certificates → Controllers → vBond → view CSR

The screenshot shows the Cisco vManage web interface. The URL in the address bar is <https://192.168.100.2/index.html#/app/config/certificates/controller>. The page title is "Cisco vManage". On the left, there's a sidebar with icons for QEMU (ServerCA), Cisco vManage, Microsoft Active Directory Certificate, and a search bar. The main content area has a title "CONFIGURATION | CERTIFICATES" and tabs for "WAN Edge List" and "Controllers". The "Controllers" tab is selected. A table lists two entries:

	Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate Serial
>	vBond	--	--	--	3ab17...	CSR Generated	--	No certificate installed
>	vManage	vManage1	10.1.1.101	30 Sep 2021 3:08:22 PM PDT	f79d5...	vBond Updated	1	1D2A8C7B000000000004

A red arrow points from the "vBond" row to a context menu. The menu options are: View CSR (highlighted with a red box), View Certificate, Generate CSR, Reset RSA, and Invalidate.

At the bottom of the interface, there are buttons for "Add Device", "Generate CSR", and "Upload Certificate". The status bar at the bottom right shows the IP address 100.1.1.4, the date 9/30/2020, and the time 8:18 PM.

- It will open a windows with CSR. Copy by using **CTRL-A** and **CTRL-C**

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.2/index.html#/app/config/certificates/controller

Cisco vManage

CONFIGURATION | CERTIFICATES

WAN Edge List Controllers

Send to vBond

CSR

IP Address: 100.1.1.4

Download

BEGIN CERTIFICATE REQUEST—  
MIIDNzCCAh8CAQAwgbYxCzAJBgNVBAYTAiVTMRAwDgYDVQQIEwdQTkVUTEF  
CMRAwDgYDVQQHEwdQTkVUTEFCMRAwDgYDVQQLEwdQTkVUTEFCMRAwDgYDVQQ  
EwdQTkVU  
TEFCMT0wOwYDVQQDEzR2Ym9uZC0zYWlxNzAyZi1mN2ILTQ1NTctOTk0Ni01Y  
mly  
Mn04ZTRjMjgtMC5QTkVUTEFCMSAwHgYJKoZIhvcNAQkBFhFwbnV0bGFiQGdt  
YWls  
LmNvbTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK31KmkoJYR  
L9IN  
oye2J5IxmtTZcTnk96c0k/v8x4dMk1Syy/FMhLNII TOU4FKk99gLxmovzoChrIn  
VUFga3Y2T4qLn1Sr1YPlupVvJkwjyhSeqfOS+1tq+uGs2YbzZeTnhWqWHo4gb5V  
T...  
Close

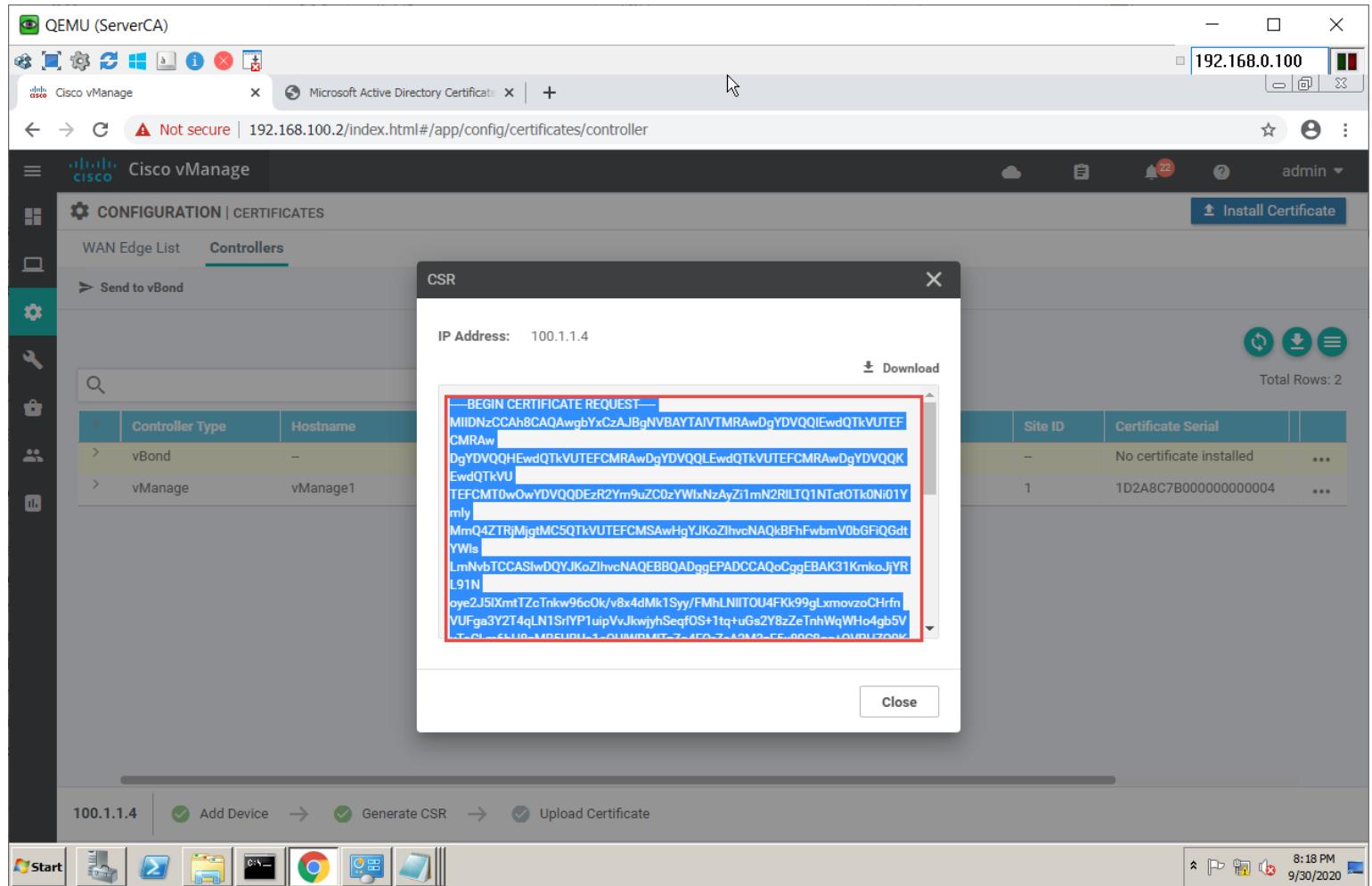
Site ID Certificate Serial

— No certificate installed ...  
1 1D2A8C7B000000000004 ...

100.1.1.4 Add Device Generate CSR Upload Certificate

Start

8:18 PM 9/30/2020





### Task 3- Request a certificate from the CA Server

- Browser to <http://192.168.100.5/certsrv>
- Click “Request a Certificate”

- Select “Advanced”

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)

A screenshot of a web browser window titled "QEMU (ServerCA)". The address bar shows "192.168.0.100". The page content is the "Microsoft Active Directory Certificate Services – PNETLAB-CA" interface. It displays a section titled "Request a Certificate" with instructions to "Select the certificate type:" followed by links to "Web Browser Certificate" and "E-Mail Protection Certificate". Below this, a note says "Or, submit an [advanced certificate request](#).", which is highlighted with a red box. The browser's taskbar at the bottom shows various icons, and the system tray on the right indicates the date as 9/30/2020 and the time as 8:20 PM.

- Paste the CSR in the box by using **CTRL-V** and click **Submit**



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate Services – PNETLAB-CA 192.168.0.100

Not secure | 192.168.100.5/certsrv/certrqxt.asp

Home

**Submit a Certificate Request or Renewal Request**

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
MIS8GWTw7xnqyuQG99Mc4r6IX91doDjh1jTYLP
Zr7yEoxy9yNwB6bn3NcxNjYnut5rh0WkbFad7
ySMUzcfSNpx+558vyKA04vH13i/mizi4brf
IhZxJvHhQabhmw=
-----END CERTIFICATE REQUEST-----
```

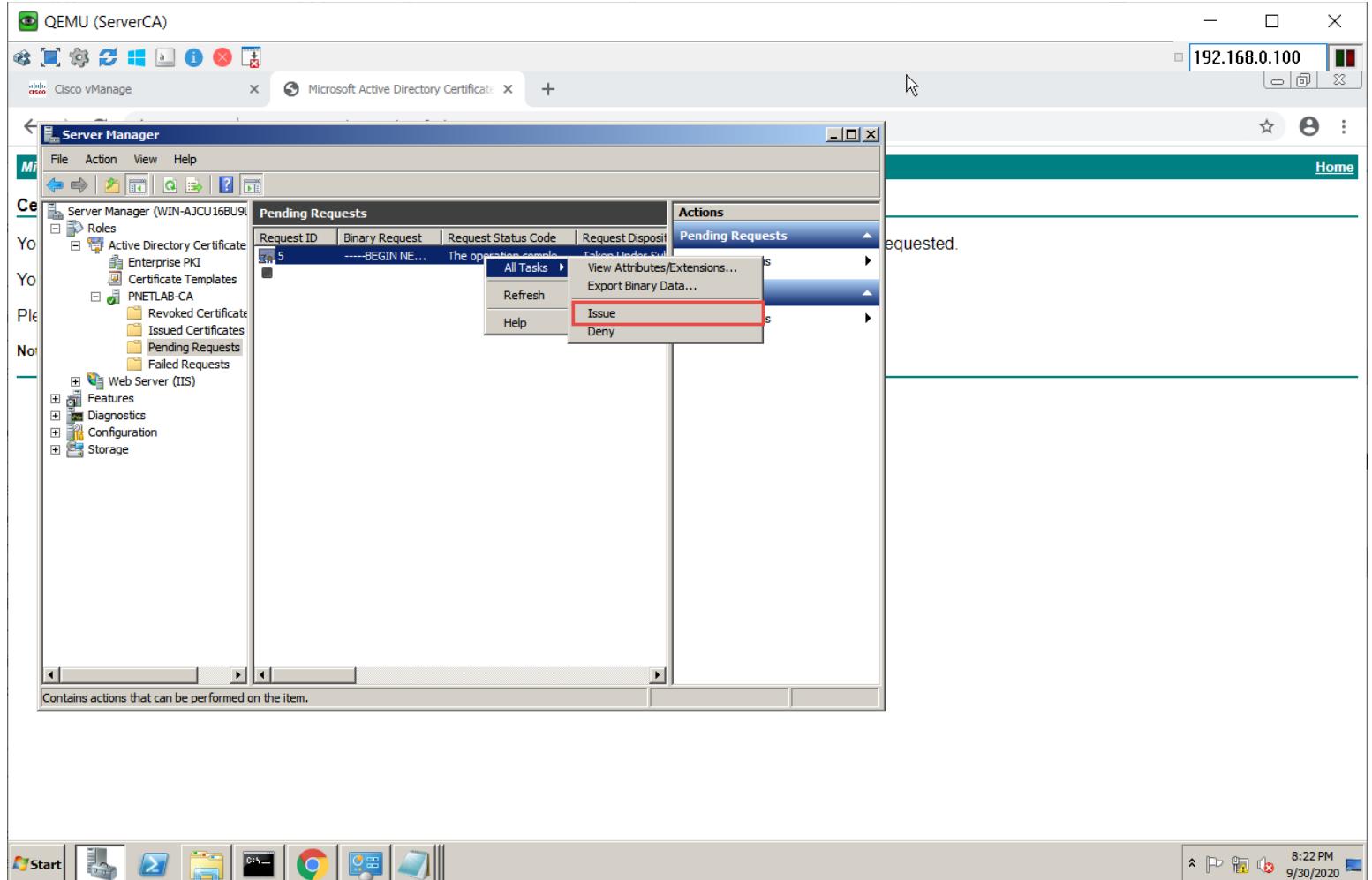
**Additional Attributes:**

Attributes:

8:21 PM 9/30/2020

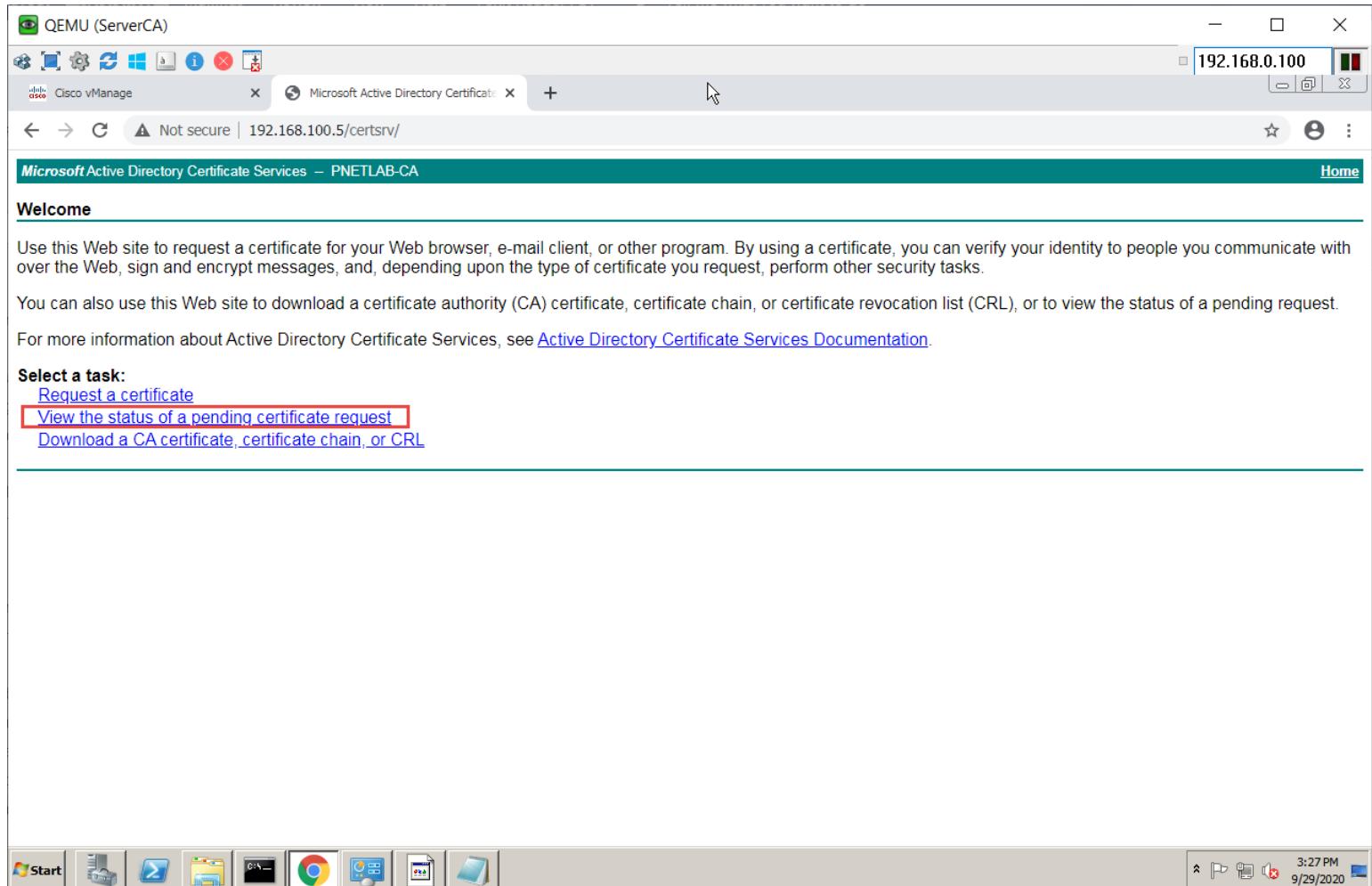
## Task 4 – Issue the Certificate from the CA Server

- Open Server Manager → Roles → Active Directory Certificate Server → PNETLAB-CA → Pending Request.
- Right-click the request → more action → all tasks and click “Issue”



## Task 5- Downloading the Issued Certificate

- Browser to <http://192.168.100.5/certsrv>
- Click “Check on Pending Certificate Request”



QEMU (ServerCA)

192.168.0.100

Cisco vManage

Microsoft Active Directory Certificate Services – PNETLAB-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

- The issued certificate link will show up. Click on the link

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



A screenshot of a Windows desktop environment showing a web browser window. The browser title bar says "QEMU (ServerCA)". The address bar shows "192.168.100.100". The page content is titled "Microsoft Active Directory Certificate Services – PNETLAB-CA" and displays a section for "View the Status of a Pending Certificate Request". A specific link, "Saved-Request Certificate (9/29/2020 3:18:49 PM)", is highlighted with a red rectangular box. The taskbar at the bottom shows various pinned icons and the date/time as 3:27 PM on 9/29/2020.

- Select “Base 64” and click “Download”

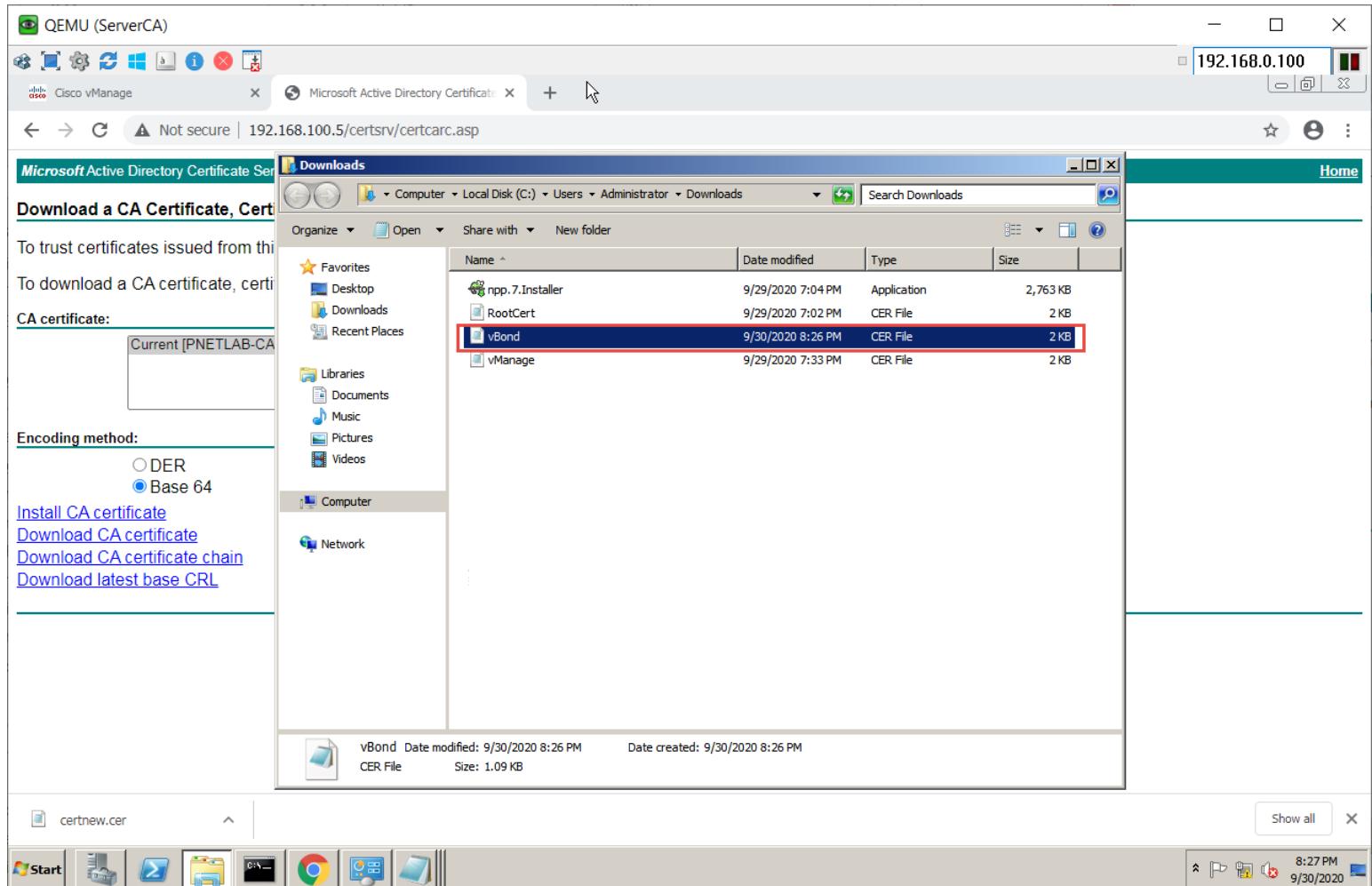


The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

[Download certificate](#) [Download certificate chain](#)

- Open explorer and navigate to the downloads folder.
- Change the name of the Downloaded file “**Certnew**” to “**vBond**”



The screenshot shows a Windows desktop environment. In the center, a Microsoft Edge browser window is open to the URL <https://192.168.100.5/certsrv/certarc.asp>. The page displays instructions for downloading a CA certificate, with the 'vBond' file highlighted in red. Below the browser, a Windows File Explorer window is open to the 'Downloads' folder at [Computer > Local Disk \(C:\) > Users > Administrator > Downloads](file:///C:/Users/Administrator/Downloads). The 'vBond' file is listed in the file list, showing it was modified on 9/30/2020 at 8:26 PM and is a CER File (2 KB). The taskbar at the bottom shows various pinned icons and the date/time as 8:27 PM on 9/30/2020.

Name	Date modified	Type	Size
npp.7.Installer	9/29/2020 7:04 PM	Application	2,763 KB
RootCert	9/29/2020 7:02 PM	CER File	2 KB
<b>vBond</b>	<b>9/30/2020 8:26 PM</b>	<b>CER File</b>	<b>2 KB</b>
vManage	9/29/2020 7:33 PM	CER File	2 KB

- Open the vBond.cer file using Notepad
- Copy using **CTRL-A** and **CTRL-C**



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.5/certsrv/certcarr.asp

Microsoft Active Directory Certificate Server

Download a CA Certificate, Cert

To trust certificates issued from this CA, download the CA certificate.

To download a CA certificate, cert

CA certificate:

Current [PNE]

Encoding method:

DER

Base 64

Install CA certificate

Download CA certificate

Download CA certificate

Download latest base CRL

vbond - Notepad

```
-----BEGIN CERTIFICATE-----
MIIDBTCCAc2gAwIBAgIQJ09d11qYRbdP4+apUo5IjANBgkqhkJG9w0BAQUFADAV
MRMwEQQDVQDewp0TkvUTEfCLUNBMB4XDTiWMDkyODiYMjEYMF0xDTi1MDkyODiY
MZEyMFowFTETMBEGA1UEAXMKUE5FVEXBQiJDQTCASiWQYIKoZIhvCNQEBBQAD
ggEPADCCAQOCggEBAKwmB32AgzpiF/wGU6K/ATHTr4GwCfmyqqersHTDP6vns00
z0xfkfszdKByFt8G0S15zezLmY4px38wIMBHCpyzoFm5Wdw6oV4Vj6c6KTKX
s/Hex0j+EAEZt4qjPNndZKmdMu83zAAVcyOHJ81F5bMp/hFayss29cjfe1PT2
BkOHCvULM15e8eFngZLsunpoYacdsvf32Fv8km4tq9TcdId9dvuhfk4vzvY18b
Ady1zi1r2oA76HPwbGcmMOFnGMw26BBV1D2z1/9dc1ec6d5w72lncip5iyws/G
+y51/Y07gwwa8joksgP1gtLqqtifZv2RmtNGojKMCwAEAAAARME8wCwYDVR0PAQD
AgGMArGA1UdEwEB/wQFMAMBAf8wHQYDVR0OBByEFEbn9HJXEkknbplidrg0CXpV
aEKSMBaGCSsGAAQ8Q8jCVAAQDAEAMAOGCCS1b3DQE8BQUAA4IBAQAIff7TVuf
SC9T3j9/1KcyIVPHCTZFCNT2Xvrtx6YK6h9urmbpe12owfd2Yqqxm7zyuSS9wC
9mTj9PKPhecKct21ycQQPP4C52JfrwARGLFN1wEyfE3m24p7y0w6r7BLjPSLG/g
PT9c8F2oXTwhb7LZSUGSFVi4+Nob1ew47SLLmnNwlAFRHxUL2+TR4BFWGPvn01x
uuig8EW1KmfaucYL1ru+Rpdi1jOEBlDDyzg4KV19u0uUySRUC/wCE4jRMx07kvU
B3xlQ8of1funevvJ3Uycnh3ms+3qsx/N1M+zT0e6/ZAm7cbZctT1VVFGb5xNB6
nAFQuor/4yyX
-----END CERTIFICATE-----
```

Downloads Computer Local Disk (C:) Users Administrator Downloads Search Downloads

Name Date modified Type Size

npp.7.Installer 9/29/2020 7:04 PM Application 2,763 KB

RootCert 9/29/2020 7:02 PM CER File 2 KB

certnew.cer

Start 8:36 PM 9/30/2020



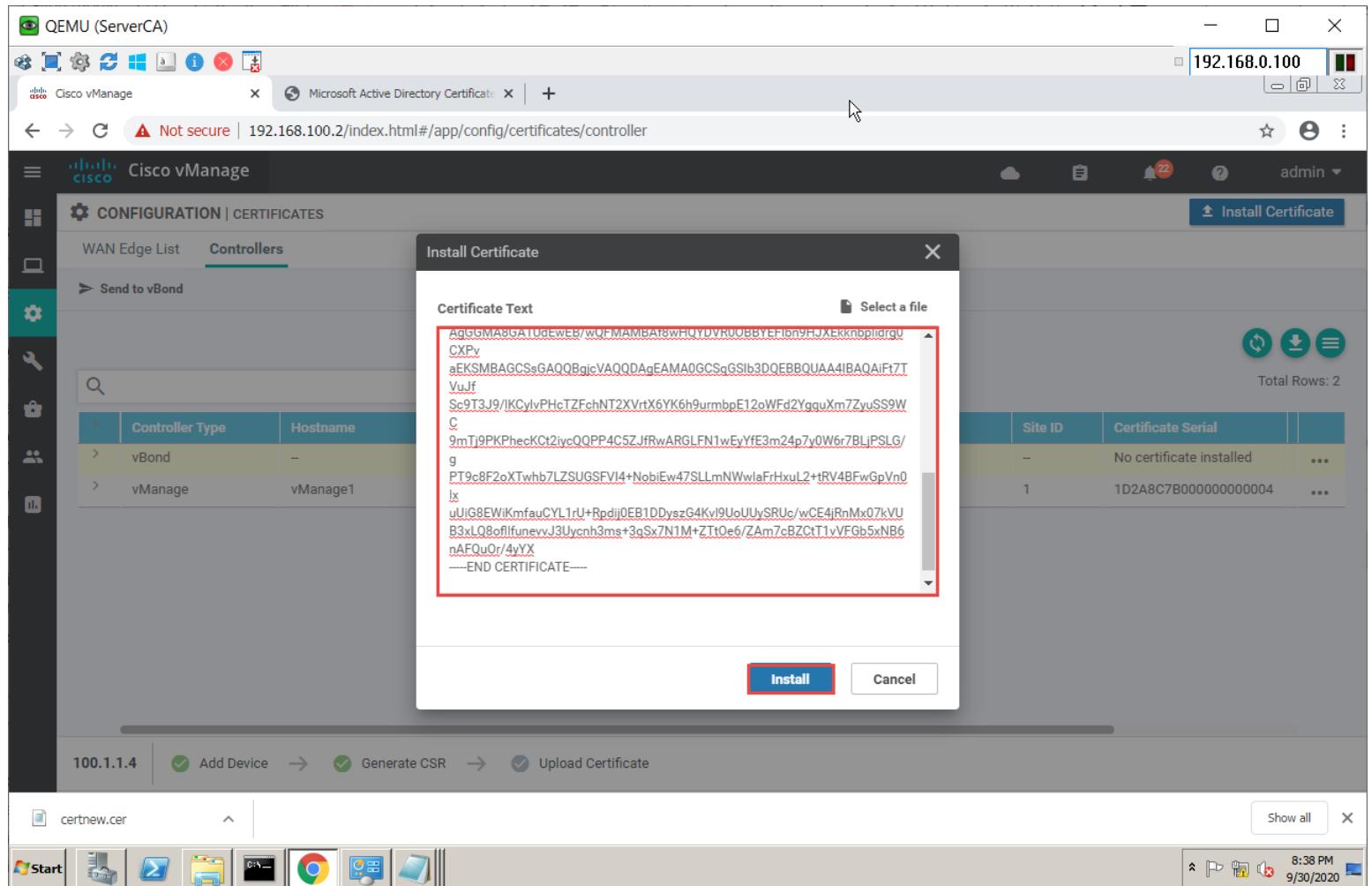


## Task 6- Installing the Identity Certificate for vManage

- In vManage, Navigate to **Configuration → Certificates → Controllers**
- Click on the “**Install Certificate**” button at the top right corner

The screenshot shows the Cisco vManage web interface. The URL in the address bar is [192.168.0.100/index.html#/app/config/certificates/controller](http://192.168.0.100/index.html#/app/config/certificates/controller). The page title is "Cisco vManage". On the left, there's a sidebar with various icons. The main content area has a header "CONFIGURATION | CERTIFICATES" with a sub-header "Controllers". Below that, there's a search bar and a table with two rows. The table columns are: Controller Type, Hostname, System IP, Expiration Date, uuid, Operation Status, Site ID, and Certificate Serial. The first row (vBond) shows "vBond" as the Controller Type, an empty hostname field, an empty system IP field, an empty expiration date field, a UUID, "CSR Generated" status, an empty site ID, and "No certificate installed" in the serial field. The second row (vManage) shows "vManage" as the Controller Type, "vManage1" as the Hostname, "10.1.1.101" as the System IP, "30 Sep 2021 3:08:22 PM PDT" as the Expiration Date, a UUID, "vBond Updated" status, "1" as the Site ID, and the serial number "1D2A8C7B000000000004". At the bottom of the table, there are three icons: a magnifying glass, a download arrow, and a list icon. Below the table, there's a progress bar and some navigation links: "Add Device", "Generate CSR", and "Upload Certificate". The status bar at the bottom shows the IP "100.1.1.4", a file named "certnew.cer", and the date/time "8:38 PM 9/30/2020".

- Paste the **Certificate (CTRL-V)**.



The screenshot shows the Cisco vManage web interface. In the center, a modal dialog box titled "Install Certificate" is open. It contains a text area labeled "Certificate Text" which displays a long string of certificate data. Below the text area are two buttons: "Install" (highlighted with a red border) and "Cancel". In the background, the main vManage interface shows a table of controllers, with one entry for "vManage" named "vManage1". At the bottom of the screen, a taskbar is visible with icons for Start, File Explorer, Task View, Taskbar settings, Google Chrome, File Explorer, and Taskbar settings, along with a system tray showing the date and time.

- The Identity certificate should be installed for vBond and pushed to it.



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.2/index.html#/app/device/status?activity=install\_certificate&pid=caabe15e-06af-469b-a136-23106167bc4c

Cisco vManage

TASK VIEW

Install Certificate

Total Task: 1 | Success : 1

Initiated By: admin From: 169.254.0.253

Status Message Device Type Device IP vManage IP

Success Successfully synced vEdge list on v... vBond 3ab1702f-f7de-4557-9946-5bb22d8e4c28 10.1.1.101

[30-Sep-2020 19:29:51 AST] Install Certificate, on device 3ab1702f-f7de-4557-9946-5bb22d8e4c28, started by user "admin" from IP address "169.254.0.253"  
[30-Sep-2020 19:29:53 AST] Certificate Installed for vBond-3ab1702f-f7de-4557-9946-5bb22d8e4c28  
[30-Sep-2020 19:29:54 AST] Pushing serial list to vBond-3ab1702f-f7de-4557-9946-5bb22d8e4c28  
[30-Sep-2020 19:29:54 AST] Started processing serial list file on vBond-3ab1702f-f7de-4557-9946-5bb22d8e4c28  
[30-Sep-2020 19:29:55 AST] Completed processing serial list file on vBond-3ab1702f-f7de-4557-9946-5bb22d8e4c28  
[30-Sep-2020 19:29:56 AST] Done - Push vSmart List for vBond-3ab1702f-f7de-4557-9946-5bb22d8e4c28  
[30-Sep-2020 19:29:56 AST] Pushed serial list to vBond-3ab1702f-f7de-4557-9946-5bb22d8e4c28 ()

Start

9:29 PM 9/30/2020



## Lab 7 – Initializing vSmart – CLI

### Task 1 - Configuring the System Component

- Configure the System parameters based on the following:
  - o Host-name : vSmart1
  - o Organization: "viptela sdwan"
  - o System-IP: 100.1.1.13
  - o Site ID: 1
  - o vbond Address: 100.1.1.4
  - o Timezone: Based on the appropriate Timezone

**Note:** Default username: admin Default password: admin

#### vSmart

```
config
!
system
host-name vSmart1
system-ip 100.1.1.13
site-id 1
organization-name "viptela sdwan"
clock timezone America/Antigua
vbond 100.1.1.4
!
commit
```

### Task 2 – Configured the vpn parameters

- Configure the VPN parameters based on the following:
  - o vpn 0
    - Interface Eth1
    - IP Address: 100.1.1.3/24
    - Tunnel Interface
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 100.1.1.1
  - o vpn 512
    - Interface eth0
    - IP Address: 192.168.100.3/24

#### vSmart

```
config
!
vpn 0
no interface eth0
interface eth1
ip address 100.1.1.3/24
tunnel-interface
```





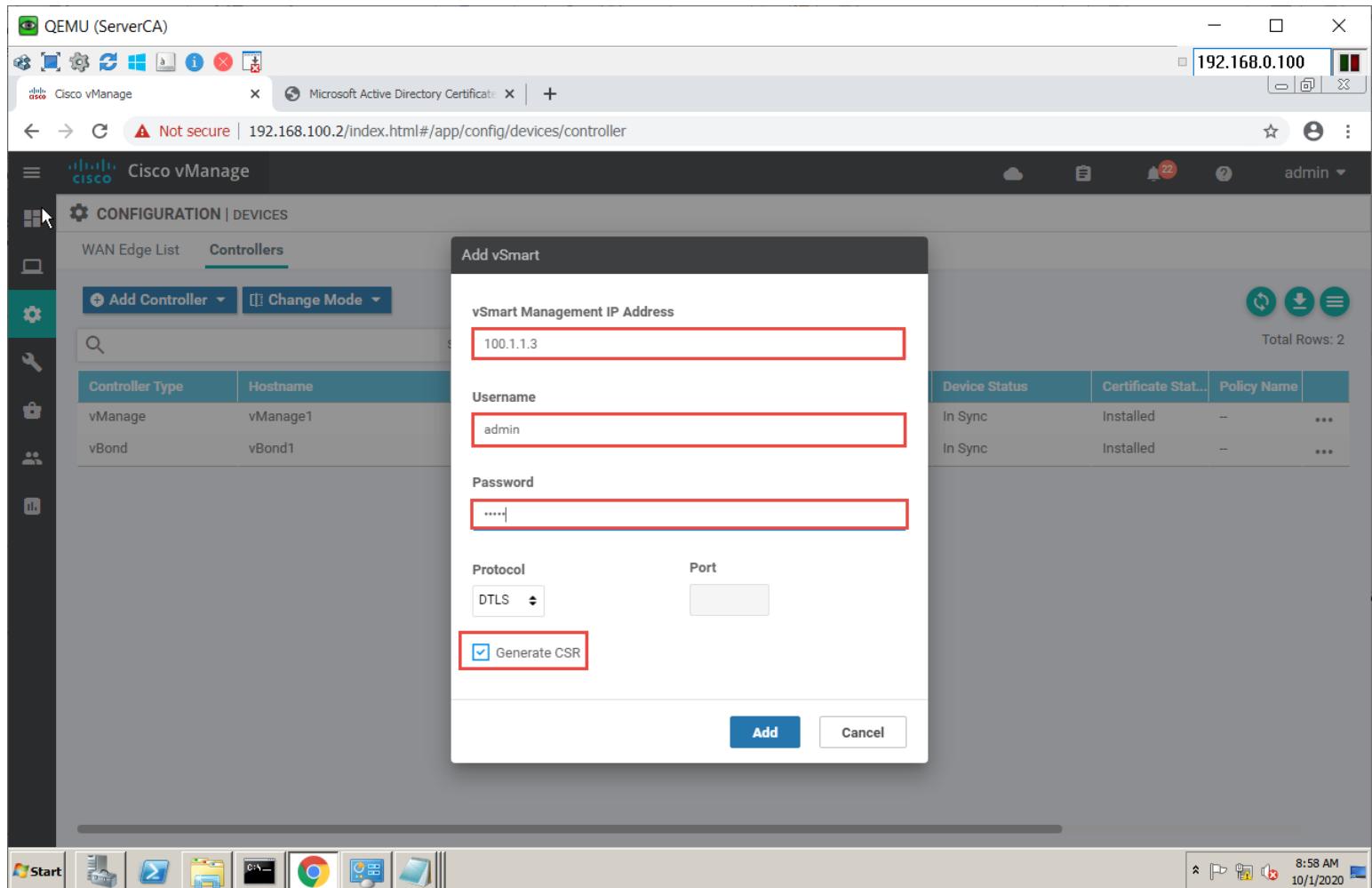
```
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 100.1.1.1
!
vpn 512
interface eth0
ip address 192.168.100.3/24
no shut
!
commit
```



## Lab 8 – Initializing vSmart – GUI

### Task 1- Add vSmart to vManage

- Navigate to **Configuration** → **Devices** → **Controllers** → **Add Controllers** → **vSmart** and specify the following to add the vBond in vManage.
  - IP Address: **100.1.1.3**
  - Username: **Admin**
  - Password: **Admin**
  - Check Generate CSR
  - Click **OK**



The screenshot shows the Cisco vManage web interface. In the center, a modal dialog box titled "Add vSmart" is open. It contains fields for "vSmart Management IP Address" (set to 100.1.1.3), "Username" (set to admin), "Password" (redacted), "Protocol" (set to DTLS), and "Port" (set to 443). A checkbox for "Generate CSR" is checked and highlighted with a red border. At the bottom of the dialog are "Add" and "Cancel" buttons. The background shows the main vManage dashboard with a table of device status and certificates. The browser address bar at the top shows the URL 192.168.100.2/index.html#/app/config/devices/controller.



## Task 2 – View the generated CSR for vSmart and Copy it

- Navigate to Configuration → Certificates → Controllers → vSmart → View CSR

The screenshot shows the Cisco vManage web interface. The URL in the address bar is <https://192.168.100.2/index.html#/app/config/certificates/controller>. The page title is "Cisco vManage". The left sidebar has icons for QEMU (ServerCA), Cisco vManage, Microsoft Active Directory Certificate, and admin. The main content area is titled "CONFIGURATION | CERTIFICATES" and shows a table for "Controllers". The table has columns: Controller Type, Hostname, System IP, Expiration Date, uuid, Operation Status, Site ID, and Certificate. There are three rows: 1. vBond, vBond1, 10.10.10.3, 30 Sep 2021 9:19:57 PM ADT, 3ab17..., Installed, 1, 1DA304E7. 2. vSmart, -, -, -, a9c68..., CSR Generated, -, No certificate installed. 3. vManage, vManage1, 10.10.10.1, 30 Sep 2021 7:08:22 PM ADT, f79d5..., vBond Updated, 1, 1D2A8C7B000000000000000000000000. A red arrow points to the "vSmart" row, specifically to the "..." button in the "Certificate" column. A red box highlights the "View CSR" option in the context menu that appears when clicking the "...".

Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate
vBond	vBond1	10.10.10.3	30 Sep 2021 9:19:57 PM ADT	3ab17...	Installed	1	1DA304E7
vSmart	-	-	-	a9c68...	CSR Generated	-	No certificate installed
vManage	vManage1	10.10.10.1	30 Sep 2021 7:08:22 PM ADT	f79d5...	vBond Updated	1	1D2A8C7B000000000000000000000000

- It will open a window with CSR. Copy by using CTRL-A and CTRL-C



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.2/Index.html#/app/config/certificates/controller

Cisco vManage

CONFIGURATION | CERTIFICATES

WAN Edge List Controllers

Send to vBond

CSR

IP Address: 100.1.1.3

BEGIN CERTIFICATE REQUEST

```
-----  
MIIDODCCAiACAQAwgbcxCzAJBgNVBAYTAiVTMRAwDgYDVQQIEwdQTkVUTEFC  
MRaw  
DgYDVQQHEwdQTkVUTEFCMRAwDgYDVQQLEwdQTkVUTEFCMRAwDgYDVQQK  
EwdQTkVU  
TEFCMT4wPAYDVQQDEzV2c21hcnaTqYTjNjhjZTEtZDA4My00ZWM5LWI5njEtMD  
F1  
NTNIYjwMTMyLTauUE5FVExBQjEgMB4GCSqGSib3DQEJARYRcG5ldGxhYkBnbW  
Fp  
bC5jb20vvgjEiMA0GCSqGSib3DQEBAQUAA4IBDwAwggEKAoIBAQDqEKMRxEy5M  
+Fm2  
iPaNyPnfjUpkoIQqx+vDy9P9wezBTLvsKk4Y9rcifH2SM8NoZrh/juSJ2iZiC  
5XMAjUCVq6gpC7FTxLu/WyaXrmaTLUG/Y4VeWR+e8laT+ipcC7aEo7Pjly5fxws
```

Total Rows: 3

Site ID	Certificate Serial	Actions
1	1DA304E7000000000006	...
--	No certificate installed	...
1	1D2A8C7B000000000004	...

100.1.1.3 Add Device Generate CSR Upload Certificate Update vBond

Start

10:57 AM 10/1/2020

### Task 3 – Request a Certificate from the CA Server

- Browser to <http://192.168.100.5/certsrv>
- Click “Request a Certificate”

Active Directory Certificate Services Documentation.' A red box highlights the 'Request a certificate' link under 'Select a task:'. The browser toolbar at the bottom shows icons for Start, File, Print, Copy, Paste, and others, along with the date and time (8:20 PM, 9/30/2020)."/&gt;

- Select “Advanced”

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)

A screenshot of a Microsoft Edge browser window. The address bar shows the URL 192.168.0.100/certsrv/certrqus.asp. The page title is "Microsoft Active Directory Certificate Services – PNETLAB-CA". The main content area is titled "Request a Certificate" and asks to "Select the certificate type:" with options for "Web Browser Certificate" and "E-Mail Protection Certificate". Below this, it says "Or, submit an [advanced certificate request](#)". The browser's taskbar at the bottom shows various pinned icons and the date/time 8:20 PM 9/30/2020.

- Paste the CSR in the box by using **CTRL-V** and click Submit



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate 192.168.0.100

Not secure | 192.168.100.5/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services – PNELAB-CA Home

**Submit a Certificate Request or Renewal Request**

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
MIS8GTw7xnqyuQG99Mc4r6IX91doDjh1jTYLP
Zr7yEOxy9yNwB6bn3NcxNJYnut5rhu0WkbFad7
ySUMZcFSWpx+55ByyaKKAO4vH13i/mizI4brf
Ih2xJvHhQabhMnw=
-----END CERTIFICATE REQUEST-----
```

**Additional Attributes:**

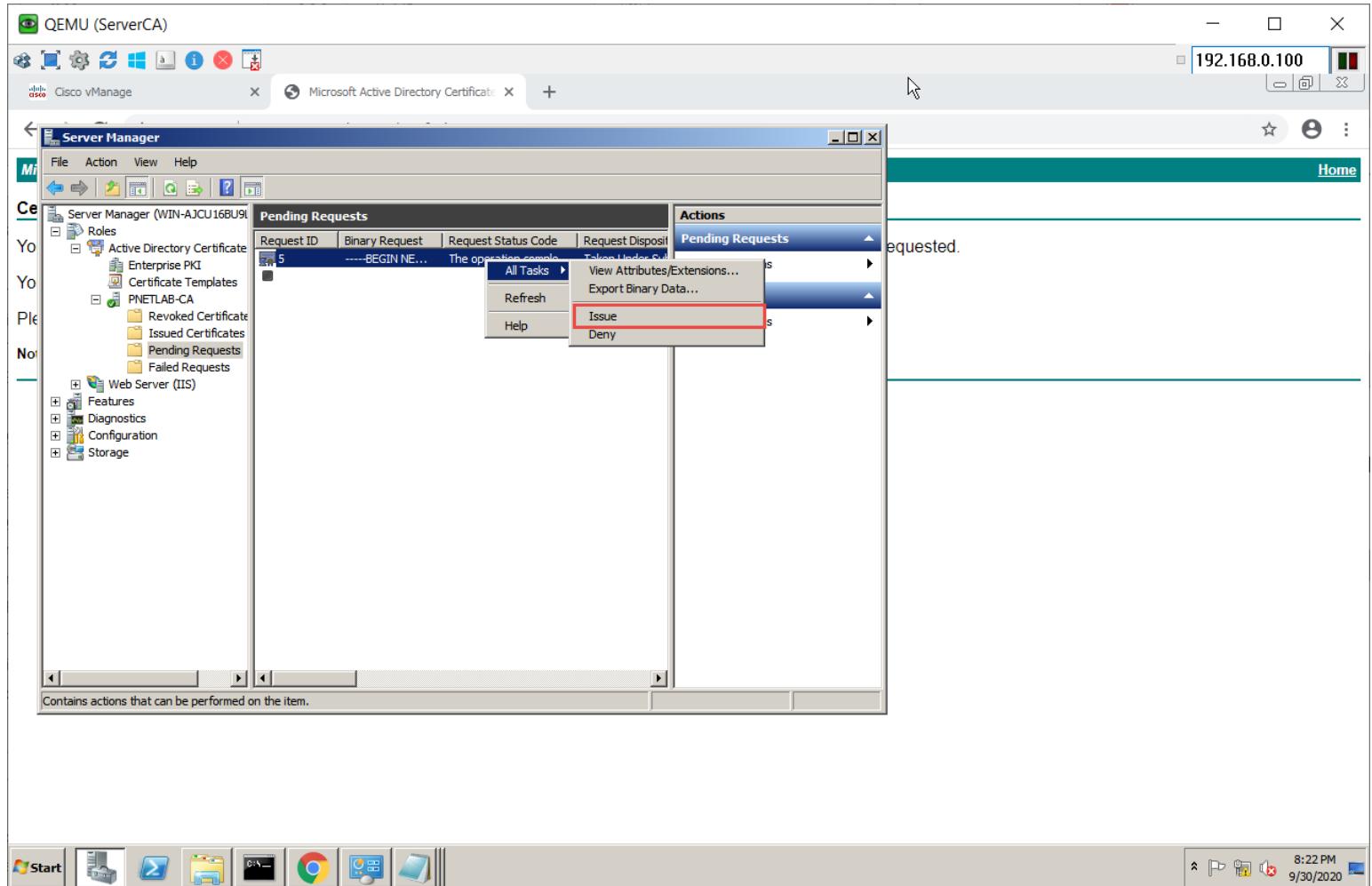
Attributes:

**Submit >**

Start | Taskbar | Icons | Task View | File Explorer | Google Chrome | Control Panel | Device Manager | Help and Support | 8:21 PM | 9/30/2020

#### Task 4 – Issue the Certificate from the CA Server

- Open Server Manager → Roles → Active Directory Certificate Server → PNETLAB-CA → Pending Request.
- Right-click the request → more action → all tasks and click “Issue”





## Task 5- Downloading the Issued Certificate

- Browser to <http://192.168.100.5/certsrv>
- Click “Check on Pending Certificate Request”

QEMU (ServerCA)

Microsoft Active Directory Certificate Services – PNETLAB-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

3:27 PM 9/29/2020

- The issued certificate link will show up. Click on the link

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



QEMU (ServerCA)

Cisco vManage Microsoft Active Directory Certificate Services - PNETLAB-CA

View the Status of a Pending Certificate Request

Select the certificate request you want to view:

[Saved-Request Certificate \(9/29/2020 3:18:49 PM\)](#)

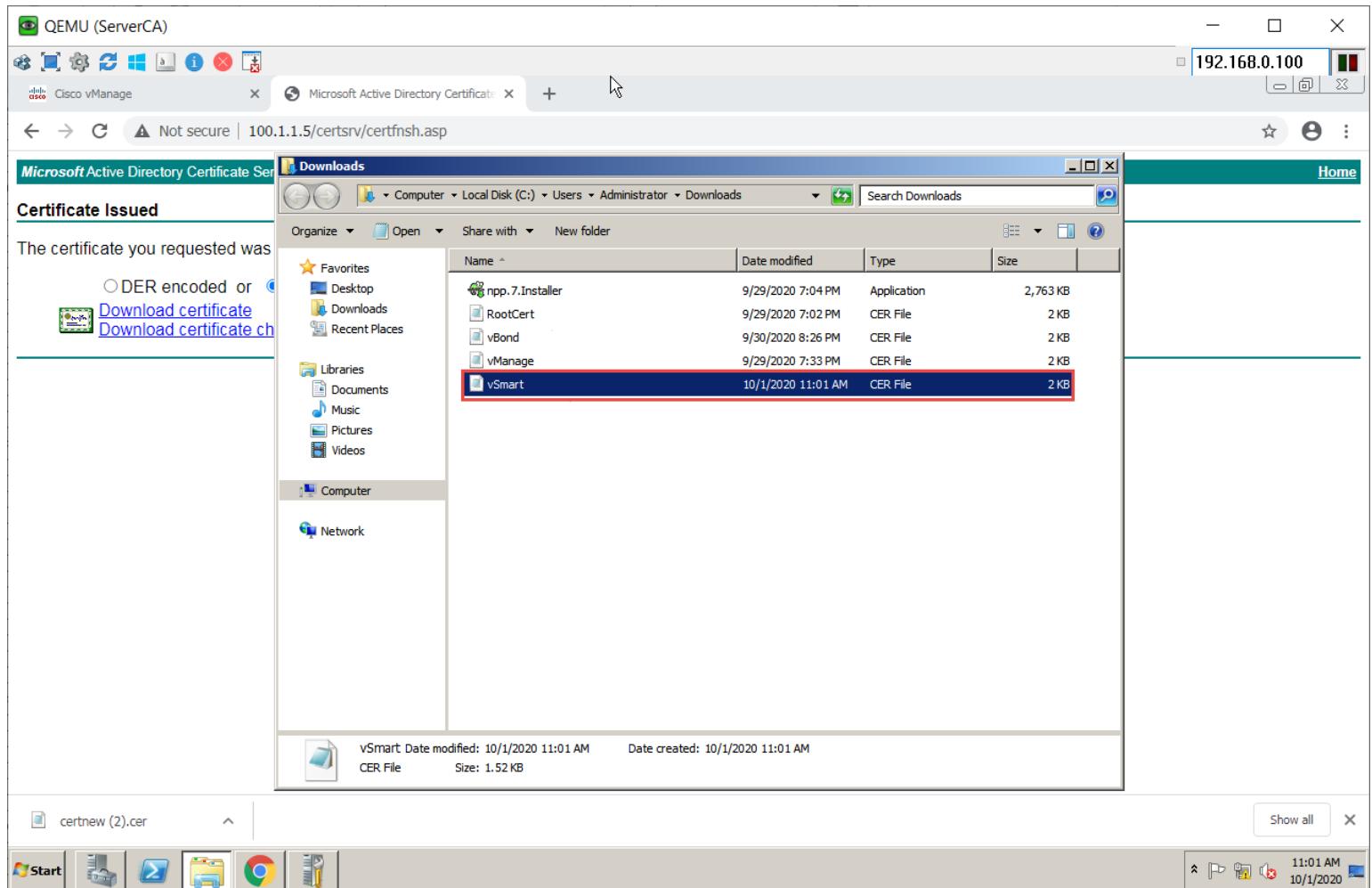
Start button

3:27 PM 9/29/2020

- Select “**Base 64**” and click “**Download**”



- Open explorer and navigate to the downloads folder.
- Change the name of the Downloaded file “**Certnew**” to “**vSmart**”



The certificate you requested was issued.

DER encoded or CER encoded

[Download certificate](#) [Download certificate.cer](#)

Downloads

Name	Date modified	Type	Size
npp.7.Installer	9/29/2020 7:04 PM	Application	2,763 KB
RootCert	9/29/2020 7:02 PM	CER File	2 KB
vBond	9/30/2020 8:26 PM	CER File	2 KB
vManage	9/29/2020 7:33 PM	CER File	2 KB
<b>vSmart</b>	<b>10/1/2020 11:01 AM</b>	<b>CER File</b>	<b>2 KB</b>

vSmart Date modified: 10/1/2020 11:01 AM Date created: 10/1/2020 11:01 AM  
CER File Size: 1.52 KB

certnew (2).cer

Start | File Explorer | Google Chrome | Task View | Taskbar

- Open the vBond.cer file using Notepad
- Copy using **CTRL-A** and **CTRL-C**



QEMU (ServerCA)

192.168.0.100

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.2/index.html#/app/config/certificates/controller

admin

CONFIGURATION | CERTIFICATES

WAN Edge List Controllers

Send to vBond

CSR

IP Address: 100.1.1.3

vSmart - Notepad

File Edit Format View Help

Controller Type

vBond

vSmart

vManage

-----BEGIN CERTIFICATE-----  
MIIERDCCAYggAwIBAgIKYaiYwWAQAAAABZANBgkqhkiG9w0BAQUFADAVMRMwEQYD  
VQQDEwp0TKVUTEFLUNBMB4XDTE1wMTAwMTEzNTAyVOXOXTIXMTAwMTE0MDAyOVow  
gbCXCZAjBgNvBAYTA1VTMRRawDgYDVQOIEwd0TkvUTEFCMRAwDgYDVQOHEwd0TkvU  
TEFCMRAwDgYDVQKEwd0TkvUTEFCMRAwDgYDVQLEwd0TkvU1Ef-CM14WPAYDVQD  
EZV2c21hcncqYT1jnjhjZTETzDA4My00ZWM5LW15NjETMDtNTNT1Y1mMTMyLTAU  
UE5FVExbQJegmB4GCSqGSib3DQEJARYRCG51dgxhykBnbwFpb5jb20wgge1mAOG  
CsqGSib3DQEBAQAA4IBDwawggeKaoIBAQDgEKMREy5M+FM2jPanypnfjupko1qd  
x+vDy9PwezBTLTvskk4Y9rycifH2zM8Nozrh/jus52l1z1tC5xMaJUcv6gpc77f  
TxLU/waxrmaTLUG/Y4vewr+e8iat+ipcc7AE07Pjly5fxwsjomkThb/AyBVbu3  
kxLghuzvsB2gi6o2e9bm8Dd+JGX2jmFrhw1vuyGudsTY01NukumzTL0o011xvp  
zm28dh1lieg95M9ow0tk0UDz9gy7h9mBxz25z7yUEm7r3/JxP7ly8Q92GOKqlu  
RZbl3oZazw9LTQZQHmA3j3Bq10wr14uinDzNo5DKE05sKRMUEfLSa64fAgMBAAG  
gfIwge8wDAYDVROTAQH/BAlwADAbgNVHQ4EFgQUs6aq21BzHOASKEKdgtstQz2/W  
rZowHwDVROjBBgwfoahufofc1cssdumwJ2u0QJc+9oqpiQYDVRofBdow0DA2  
ODSGMoYWzm1sZTovl1dTi1BSKNMVTZCVTlMRy9dzXJ0Rw5yb2xsLlBORVRMQuIt  
Q0EUY3jsMfwGCCsGAQUFbwEBBFawtjBMBggrBqeFBQcwaoAZm1sZTovl1d3Tii1B  
SkNMVTZCVTlMRy9dzXJ0Rw5yb2xsLl1d3Tii1BSKNMVTZCVTlMR19QtKVUTEFLUNB  
LmNydnDAnBgkqhkiG9w0BAQF0AAQEA186pkporqRPAczdT1CqgKxJHD+g7u9y9  
z8swkAVFN/8Lcqtp+gszhtPn2v0I6y6Ahraku+Lkb1szysm6xtZREXcfxqar934g  
edf4vypm/eeSww8sgTf1Fnbiu89qrNrwl0YB24y2hyQnkQwb1/+6HK6kMz8TyA  
RT6duvgMF/RKjsuWE9730Ho20iu0x8ka07t82qdGh16Vs4j59bhMIPr+EtP4PUgg  
IwjorK1jGo/Jxgo9goQhoc1i4o1sfpA8R8dvHd5F6Xj+3yN6MF4B7A4+s1lPmp9i  
wy4D0z9tCHsnzSwr9xDN1pkf1u+oQz6PSjtewohvn7058wZNxw9rw==  
-----END CERTIFICATE-----

certnew (2).cer

100.1.1.3 Ad

11:02 AM 10/1/2020





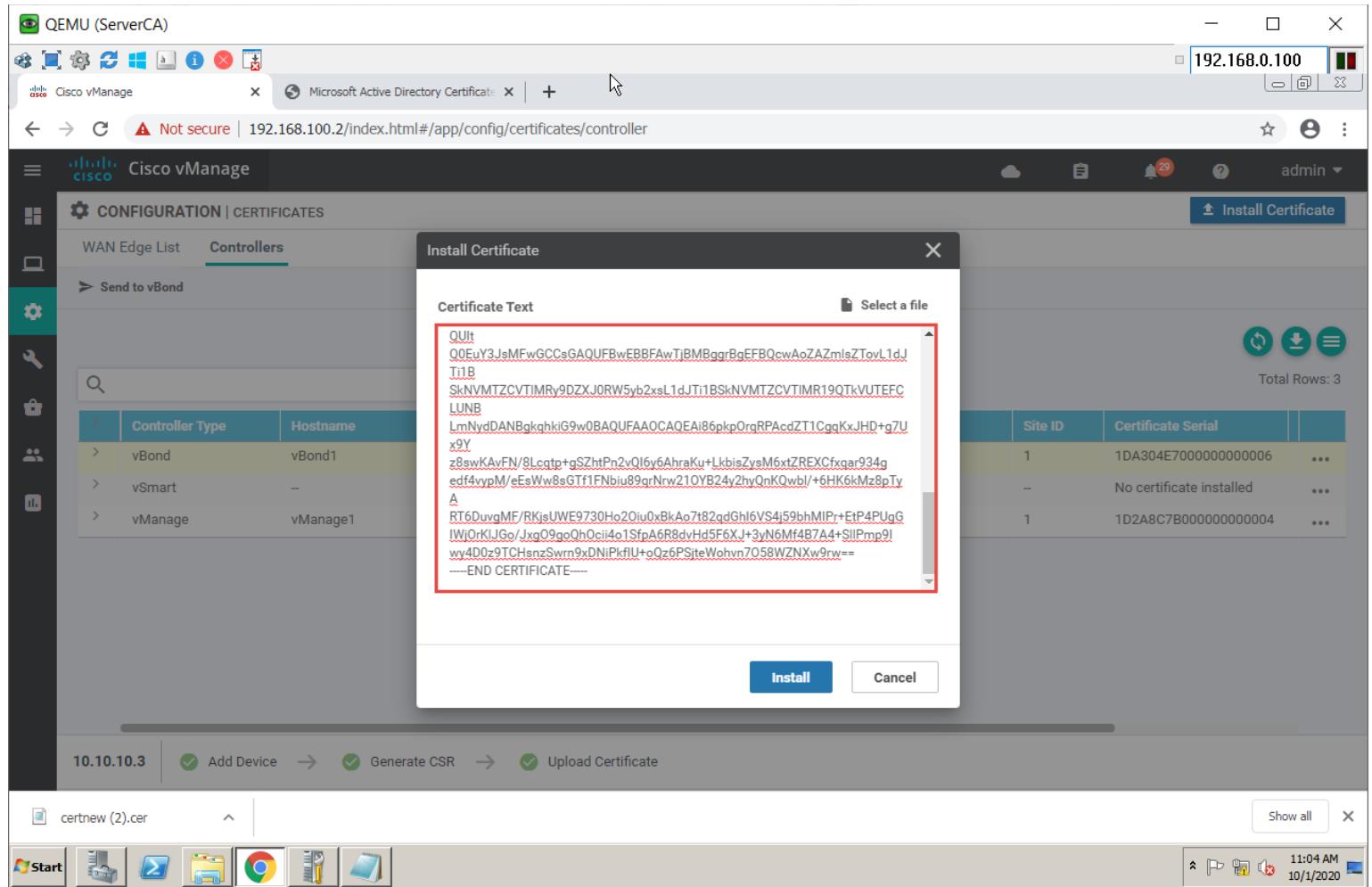
## Task 6- Installing the Identity Certificate for vManage

- In vManage, Navigate to **Configuration → Certificates → Controllers**
- Click on the “Install Certificate” button at the top right corner

The screenshot shows the Cisco vManage web interface. The URL in the address bar is [192.168.100.2/index.html#/app/config/certificates/controller](http://192.168.100.2/index.html#/app/config/certificates/controller). The page title is "Cisco vManage". On the left, there's a sidebar with various icons. The main content area has a header "CONFIGURATION | CERTIFICATES" with tabs for "WAN Edge List" and "Controllers". The "Controllers" tab is selected. A table lists three controllers: vBond1, vSmart, and vManage1. The vManage1 row shows "CSR Generated" under Operation Status and "No certificate installed" under Certificate Serial. At the top right of the table is a red-bordered "Install Certificate" button. Below the table, there's a navigation bar with steps: "Add Device", "Generate CSR", "Upload Certificate", and "Update vBond". At the bottom, there's a file browser window showing "certnew (2).cer" and a taskbar with icons.

Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate Serial	Actions
vBond	vBond1	10.10.10.3	30 Sep 2021 9:19:57 PM ADT	3ab17...	Installed	1	1DA304E7000000000006	...
vSmart	--	--	--	a9c68...	CSR Generated	--	No certificate installed	...
vManage	vManage1	10.10.10.1	30 Sep 2021 7:08:22 PM ADT	f79d5...	vBond Updated	1	1D2A8C7B000000000004	...

- Paste the Certificate (CTRL-V).



The screenshot shows the Cisco vManage interface. A modal dialog box titled "Install Certificate" is open, displaying a large block of certificate text. The text is highlighted with a red rectangle. At the bottom of the dialog are two buttons: "Install" (blue) and "Cancel" (white). In the background, the main configuration page is visible, showing a table of controllers (vBond, vSmart, vManage) with their respective types and hostnames. The URL in the browser bar is 192.168.100.2/index.html#/app/config/certificates/controller.

- The Identity certificate should be installed for vSmart and pushed to it.

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



QEMU (ServerCA)

192.168.0.100

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.2/index.html#/app/device/status?activity=install\_certificate&pid=4b370838-5924-4336-8e25-accc5bc169ed

Cisco vManage

TASK VIEW

Install Certificate

Initiated By: admin From: 169.254.0.253

Total Task: 1 | Success : 1

Search Options

Total Rows: 1

Status	Message	Device Type	Device IP	vManage IP
Success	Successfully synced vEdge list on v... vSmart		a9c68ce1-d083-4ec9-b961-01e53e...	10.10.10.1

certnew (2).cer

Show all

Start

11:10 AM 10/1/2020

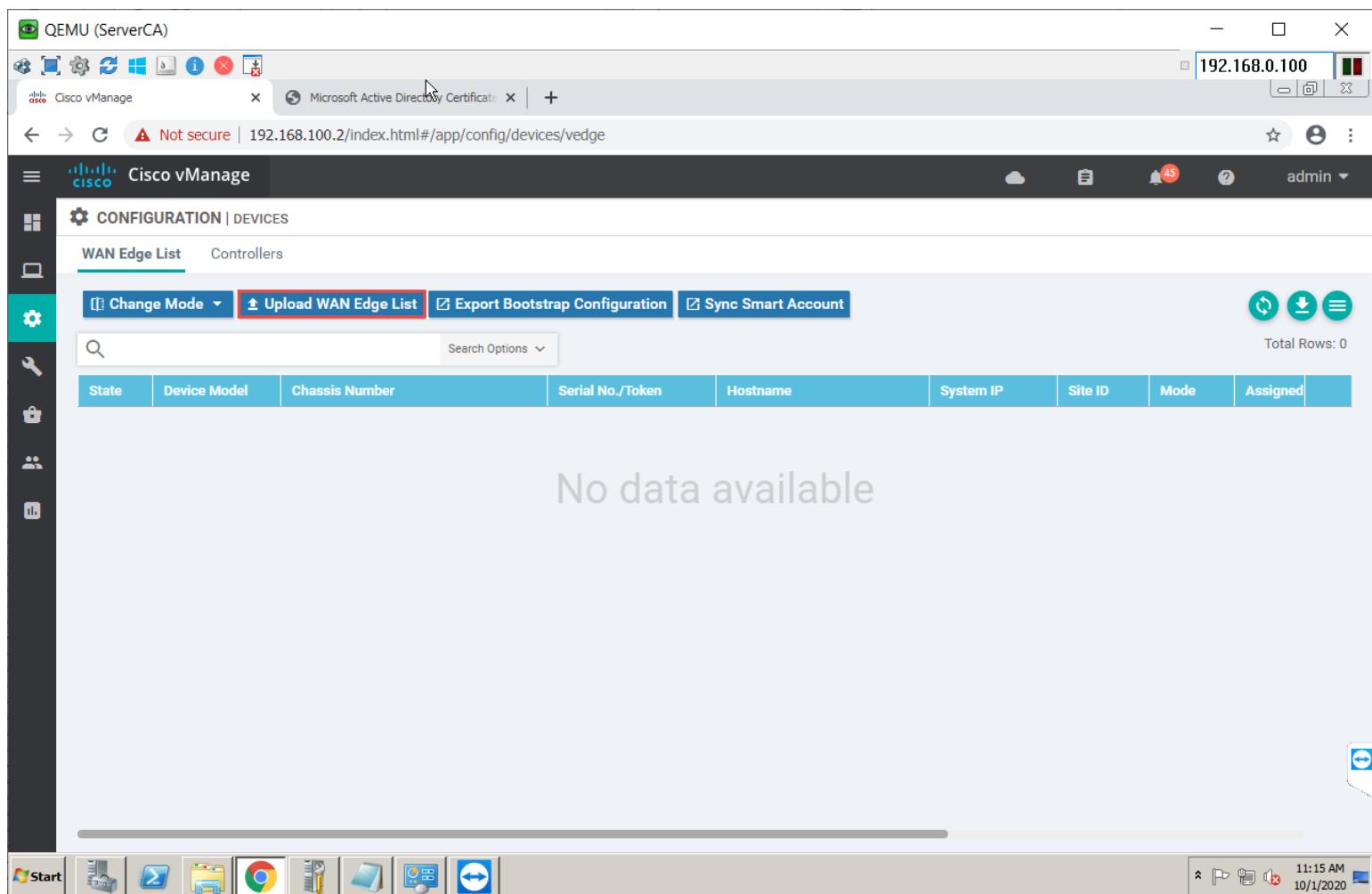
## Lab 9 – initializing vEdge – CLI

### Note:

Before doing this lab, please note that vedge have **bug related to resolve the next-hop on vpn0**. So sometime, **vmanage cant reach to vedge** → You must flap Ge0/0 or Ge0/1 interface.

### Task 1 – Upload the WAN Edge List

- On the vManage Main windows, Navigte to **Configuration → Devices**. Click on “**Upload WAN Edge List**”.



The screenshot shows the Cisco vManage web interface. The top navigation bar includes links for QEMU (ServerCA), Cisco vManage, Microsoft Active Directory Certificate, and a connection to 192.168.100.100. The main header says "Cisco vManage". The left sidebar has icons for Home, Configuration, Devices, Network, Security, and Analytics. The main content area is titled "CONFIGURATION | DEVICES" and "WAN Edge List". It features a toolbar with "Change Mode", "Upload WAN Edge List" (which is red), "Export Bootstrap Configuration", and "Sync Smart Account". Below the toolbar is a search bar and a table header with columns: State, Device Model, Chassis Number, Serial No./Token, Hostname, System IP, Site ID, Mode, and Assigned. A message "No data available" is displayed in the center. The bottom of the screen shows a Windows taskbar with icons for Start, File Explorer, Google Chrome, Task View, Taskbar settings, and a system tray showing the date and time (11:15 AM, 10/1/2020).

- Select the file you downloaded from Section: **HOW TO SETUP LAB > Link to download lab and Setup > 2. How to setup and practice lab > licensing on SD-WAN Devices**. Upload it and check the **Validate** option.



Screenshot of a Cisco vManage interface showing the "WAN Edge List" configuration screen. A modal dialog box titled "Upload WAN Edge List" is open, prompting the user to choose a file named "serialFile.viptela". A checkbox labeled "Validate the uploaded vEdge List and send to controllers" is checked and highlighted with a red box. A yellow confirmation message at the bottom asks "Are you sure you want to upload serialFile.viptela ?" with "OK" and "Cancel" buttons.

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Screenshot of a Cisco vManage interface showing the "WAN Edge List" configuration screen. A modal dialog box titled "Upload WAN Edge List" is open, prompting the user to choose a file named "serialFile.viptela". The "Upload" button is highlighted with a red border.

The main interface shows a table with columns: State, Device Model, Chassis Number, Item IP, Site ID, Mode, and Assigned. The status bar at the bottom indicates "Total Rows: 0".

At the bottom of the screen, a Windows taskbar is visible with icons for Start, File Explorer, Task View, File Explorer, Google Chrome, File Explorer, Task View, and a blue circular icon. The system tray shows the date and time as "11:16 AM 10/1/2020".



QEMU (ServerCA)

192.168.0.100

Cisco vManage Microsoft Active Directory Certificate

Not secure | 192.168.100.2/index.html#/app/config/devices/vedge

Cisco vManage

CONFIGURATION | DEVICES

WAN Edge List Controllers

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

Search Options Total Rows: 20

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	Assigned
Green	CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C93...	Token - 74360338b195...	--	--	--	CLI	--
Green	CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD...	Token - 0ba7e5da97b7f...	--	--	--	CLI	--
Green	vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	Token - 3af218a1836cb...	--	--	--	CLI	--
Green	vEdge Cloud	2eb9da66-7afd-04fd-6f49-fba8e745554c	Token - 7132efe986193...	--	--	--	CLI	--
Green	vEdge Cloud	d6d98a35-f70c-9955-0106-86192f2377...	Token - 45762da037dff...	--	--	--	CLI	--
Green	vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737...	Token - 89854fac6a002...	--	--	--	CLI	--
Green	vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924...	Token - 898afb6f2a52f...	--	--	--	CLI	--
Green	vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e850561...	Token - 7b2f4c767fd25...	--	--	--	CLI	--
Green	CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6E...	Token - 9fc4540ef1d38...	--	--	--	CLI	--
Green	CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542...	Token - eb4aa30174b1f...	--	--	--	CLI	--
Green	CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E...	Token - 6a7dd54f7eb7f...	--	--	--	CLI	--
Green	CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A...	Token - c1159ba3bc25f...	--	--	--	CLI	--
Green	CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A...	Token - bd4a897a56ebf...	--	--	--	CLI	--

Start

11:19 AM 10/1/2020

## vEDGE-1

### Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - o Host-name : vEdge1
  - o Organization: "viptela sdwan"
  - o System-IP: 119.1.1.21
  - o Site ID: 1
  - o vbond Address: 100.1.1.4
  - o Timezone: clock timezone America/Antigua

Note: Default username: **admin** Default password: **admin**

**vEdge1**

```
config
system
host-name vEdge1
system-ip 119.1.1.21
site-id 1
organization-name "viptela sdwan"
clock timezone America/Antigua
vbond 100.1.1.4

commit
```

**Task 2 – Configure the vpn parameters**

- Configure the VPN parameters based on the following:
  - o vpn 0
    - Interface ge0/0
    - IP Address: 119.1.1.1/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 119.1.1.2
  - o vpn 512
    - Interface eth0
    - IP Address: DHCP Client

**vEdge1**

```
config
vpn 0
no interface eth0
interface ge0/0
ip address 119.1.1.1/24
tunnel-interface
encapsulation ipsec
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 119.1.1.2
vpn 512
interface eth0
ip dhcp-client
no shutdown
commit
```



## vEDGE-2

### Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - o Host-name : vEdge2
  - o Organization: "viptela sdwan"
  - o System-IP: 118.1.2.22
  - o Site ID: 2
  - o vbond Address: 100.1.1.4
  - o Timezone: Based on the appropriate Timezone

**Note:** Default username: **admin** Default password: **admin**

**vEdge2**

```
config
system
host-name vEdge2
system-ip 118.1.2.22
site-id 2
organization-name "viptela sdwan"
clock timezone America/Antigua
vbond 100.1.1.4
commit
```

### Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:
  - o vpn 0
    - Interface ge0/0
    - IP Address: 118.1.2.1/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 118.1.2.2
  - o vpn 512
    - Interface eth0
    - IP Address: DHCP Client

**vEdge2**

```
config
vpn 0
no interface eth0
interface ge0/1
ip address 118.1.2.1/24
tunnel-interface
encapsulation ipsec
```





```
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 118.1.2.2
vpn 512
interface eth0
ip dhcp-client
no shutdown
!
commit
```

## vEDGE-3

### Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - o Host-name : vEdge3
  - o Organization: "viptela sdwan"
  - o System-IP: 118.1.3.23
  - o Site ID: 3
  - o vbond Address: 100.1.1.4
  - o Timezone: Based on the appropriate Timezone
  - o Note: Default username: admin Default password: admin

#### vEdge3

```
config
!
system
host-name vEdge3
system-ip 118.1.3.23
site-id 3
organization-name "viptela sdwan"
clock timezone America/Antigua
vbond 100.1.1.4
!
commit
```

### Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:
- vpn 0
  - o Interface ge0/1
  - o IP Address: 118.1.3.1/24
  - o Tunnel Interface
  - o Encapsulation IPSec
  - o Tunnel Services (All, NetConf, SSHD)





- Default Route: 118.1.3.2
- vpn 512
  - Interface eth0
  - IP Address: DHCP Client

### vEdge3

```
config
vpn 0
no interface ge0/0
interface ge0/1
ip address 118.1.3.1/24
tunnel-interface
encapsulation ipsec
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 118.1.3.2
vpn 512
interface eth0
ip dhcp-client
no shutdown
commit
```

## vEDGE-4

### Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge4
  - Organization: "**viptela sdwan**"
  - System-IP: 118.1.5.25
  - Site ID: 4
  - vbond Address: 100.1.1.4
  - Timezone: Based on the appropriate Timezone

Note: Default username: **admin** Default password: **admin**

### vEdge4

```
config
system
host-name vEdge4
system-ip 118.1.5.25
site-id 4
organization-name "viptela sdwan"
clock timezone America/Antigua
vbond 100.1.1.4
```





```
commit
```

## Task 2 – Configure the vpn parameters

- Configure the VPN parameters based on the following:
  - o vpn 0
    - Interface ge0/0
    - IP Address: 118.1.4.1/24
    - Tunnel Interface
    - Encapsulation IPSec
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 118.1.4.2
  - o vpn 512
    - Interface eth0
    - IP Address: DHCP Client

vEdge4

```
config
vpn 0
no interface ge0/0
interface ge0/1
ip address 118.1.4.1/24
tunnel-interface
encapsulation ipsec
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 118.1.4.2
vpn 512
interface eth0
ip dhcp-client
no shutdown
commit
```

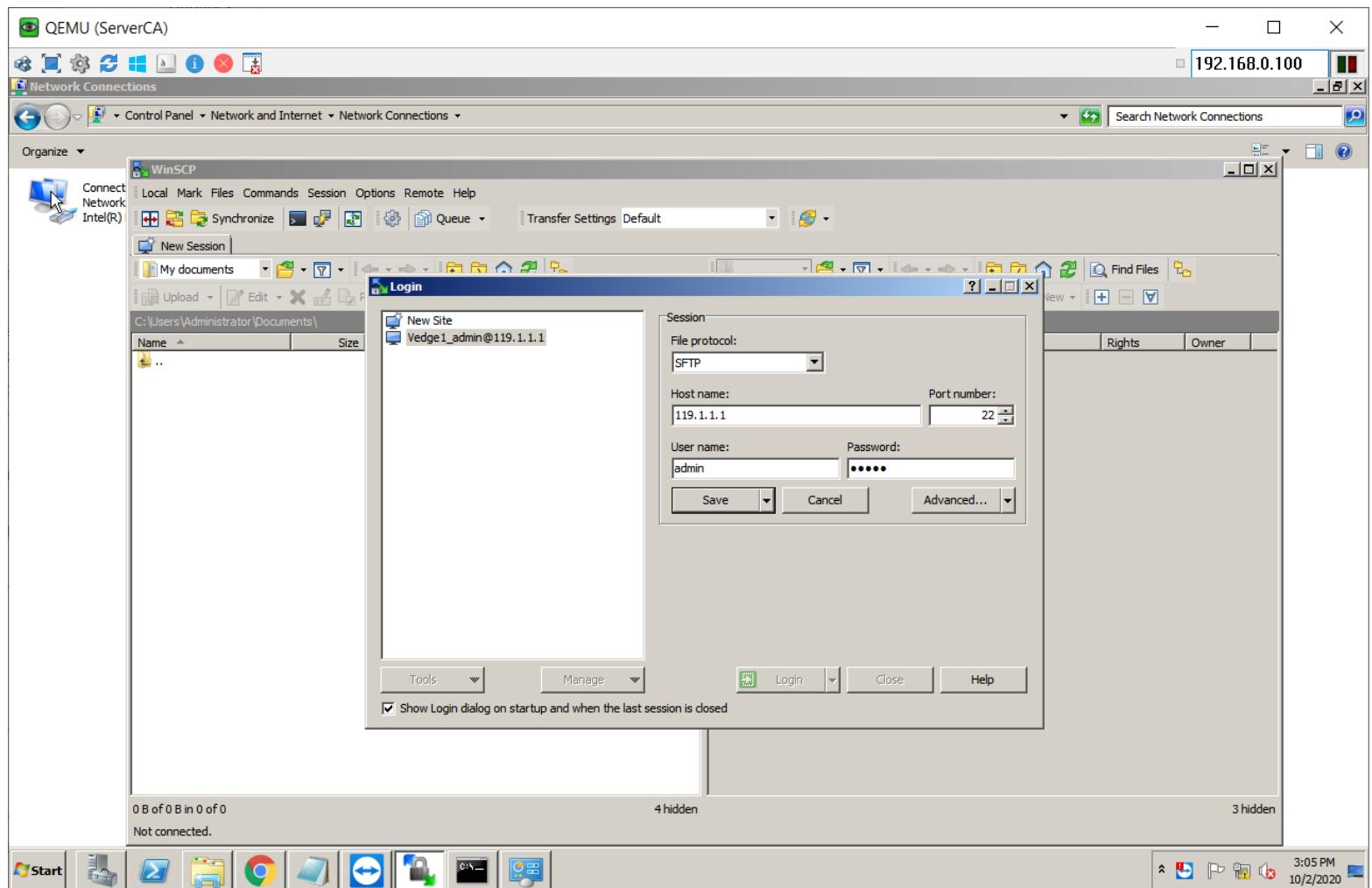


## Lab 10 – Registering vEdges in vManage

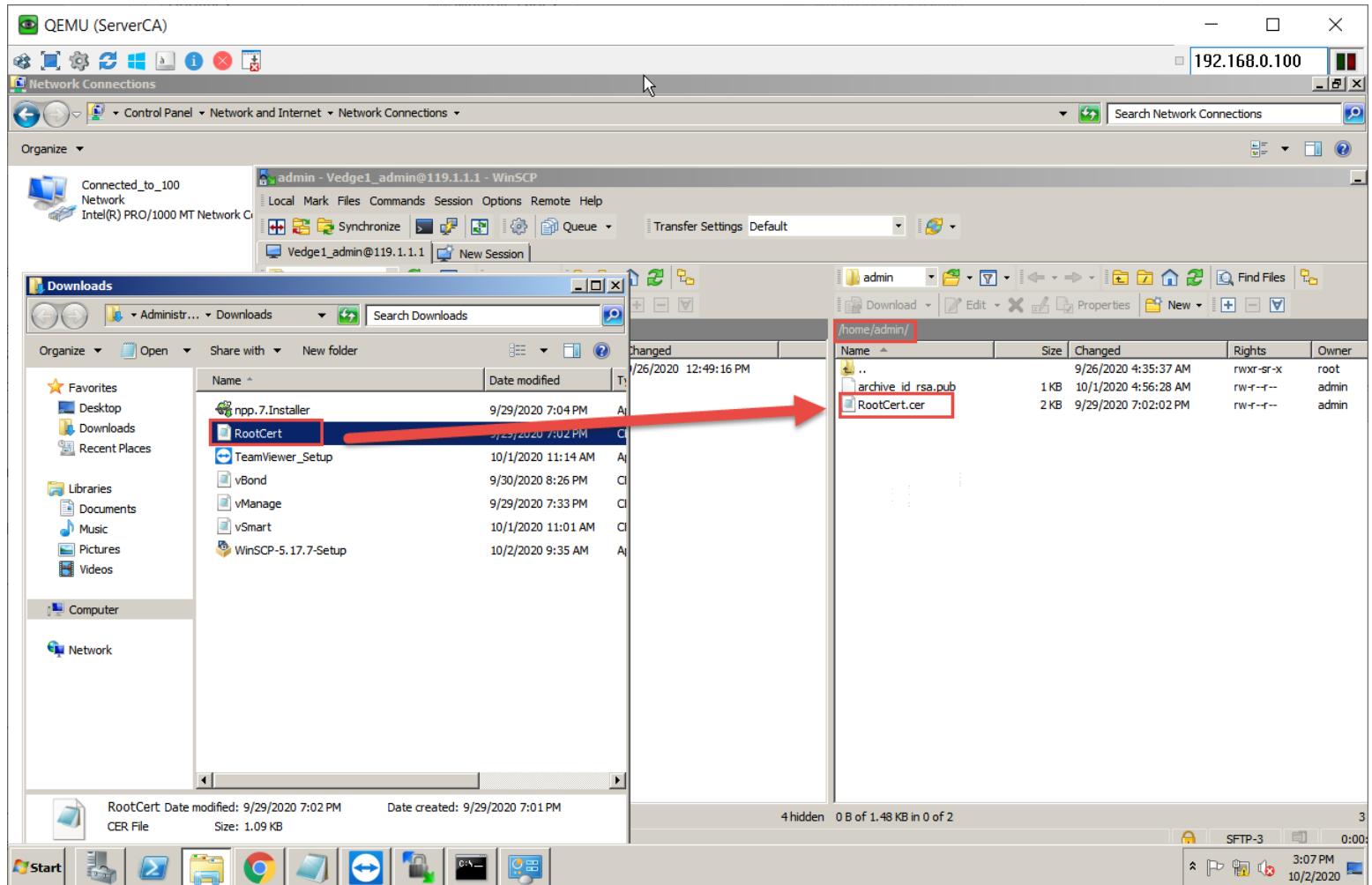
### vEDGE-1

#### Task 1- Upload the Root Certificate to the vEdge

- On the Windows Server, open WINSSCP application.
- Connect to vEdge1 using the following information:
  - o IP Address : 119.1.1.1
  - o Protocol - SFTP
  - o Username : admin
  - o Password : admin



- Copy the RootCert.cer file from the Downloads folder to the: /home/admin folder on the vEdge1



## Task 2- Install the Root Certificate on vEdge1

- Connect to the console of vEdge1 and issue the following command:

vEdge1:

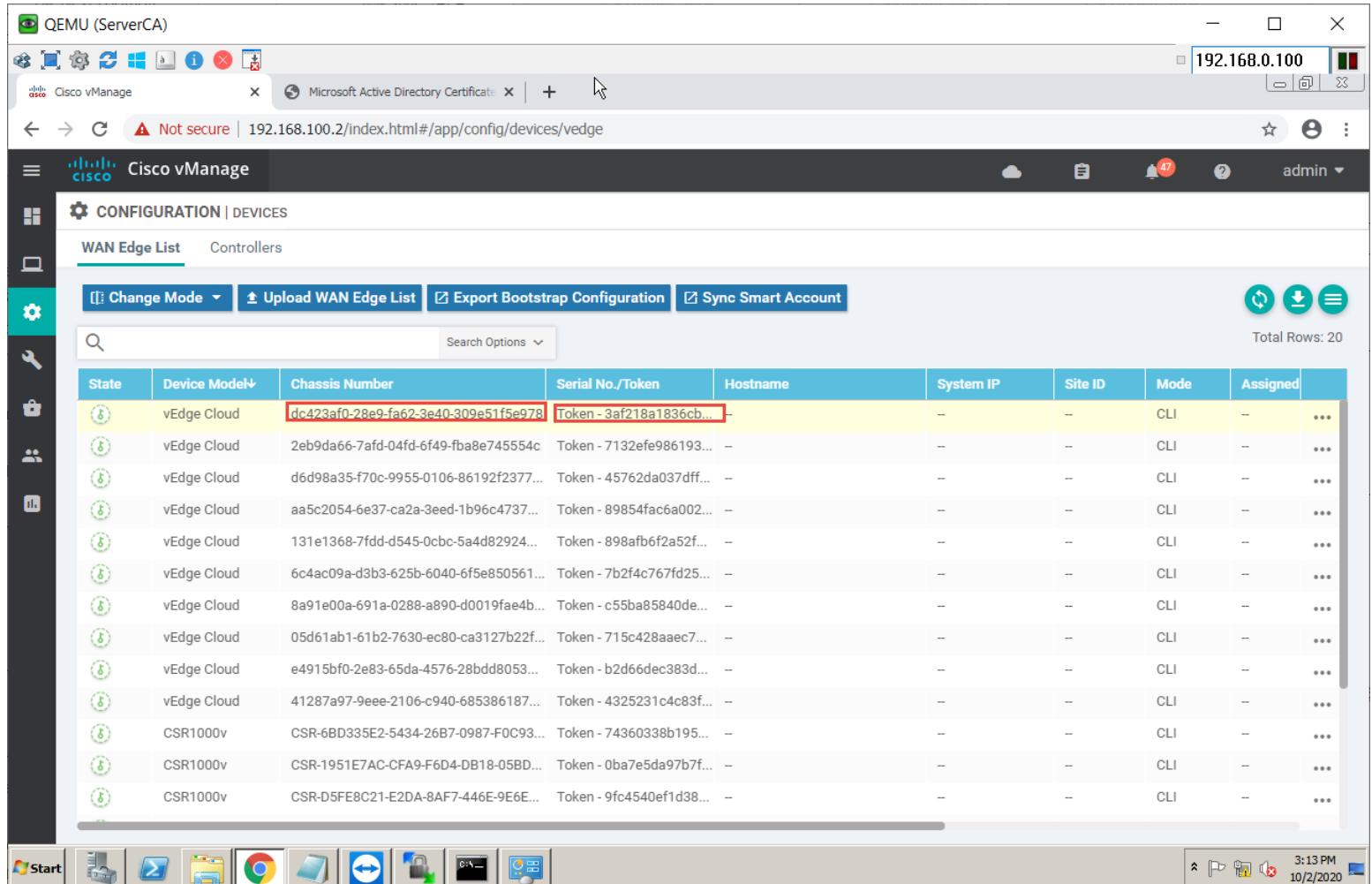
```
request root-cert-chain install /home/admin/RootCert.cer
```

Log install successfully as bellow:

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

### Task 3- Active vEdge on vManage

- Navigate to Configuration ➔ Devices



The screenshot shows the Cisco vManage interface with the title bar "QEMU (ServerCA)" and the URL "192.168.100.2/index.html#/app/config/devices/vedge". The left sidebar has icons for Home, Devices, Network, Security, and Analytics. The main menu bar includes Cisco vManage, Microsoft Active Directory Certificate, and admin. The configuration menu is open, showing "CONFIGURATION | DEVICES" and "WAN Edge List". The "WAN Edge List" tab is selected, displaying a table with columns: State, Device Model, Chassis Number, Serial No./Token, Hostname, System IP, Site ID, Mode, and Assigned. There are 20 total rows. The first row's Chassis Number and Token are highlighted with red boxes.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mode	Assigned	
vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	Token - 3af218a1836cb...	--	--	--	--	CLI	--	...
vEdge Cloud	2eb9da66-7afdf-04fd-6f49-fba8e745554c	Token - 7132efe986193...	--	--	--	--	CLI	--	...
vEdge Cloud	d6d98a35-f70c-9955-0106-86192f2377...	Token - 45762da037dff...	--	--	--	--	CLI	--	...
vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737...	Token - 89854fac6a002...	--	--	--	--	CLI	--	...
vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924...	Token - 898afb6f2a52f...	--	--	--	--	CLI	--	...
vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e850561...	Token - 7b2f4c767fd25...	--	--	--	--	CLI	--	...
vEdge Cloud	8a91e00a-691a-0288-a890-d0019fae4b...	Token - c55ba85840de...	--	--	--	--	CLI	--	...
vEdge Cloud	05d61ab1-61b2-7630-ec80-ca3127b22f...	Token - 715c428aaec7...	--	--	--	--	CLI	--	...
vEdge Cloud	e4915bf0-2e83-65da-4576-28bdd8053...	Token - b2d66dec383d...	--	--	--	--	CLI	--	...
vEdge Cloud	41287a97-9eee-2106-c940-685386187...	Token - 4325231c4c83f...	--	--	--	--	CLI	--	...
CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C93...	Token - 74360338b195...	--	--	--	--	CLI	--	...
CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD...	Token - 0ba7e5da97b7f...	--	--	--	--	CLI	--	...
CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6E...	Token - 9fc4540ef1d38...	--	--	--	--	CLI	--	...

- Note and use the Chassis Number and Token Number for the list vEdge from vManage
- Use the information from the previous step in the following command on the vEdge1 console.

**vEdge1**

```
Request vedge-cloud activate chassis-number <chassis number> <token>
```

- We can check after adding finish



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/devices/vedge

Cisco vManage

CONFIGURATION | DEVICES

WAN Edge List Controllers

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

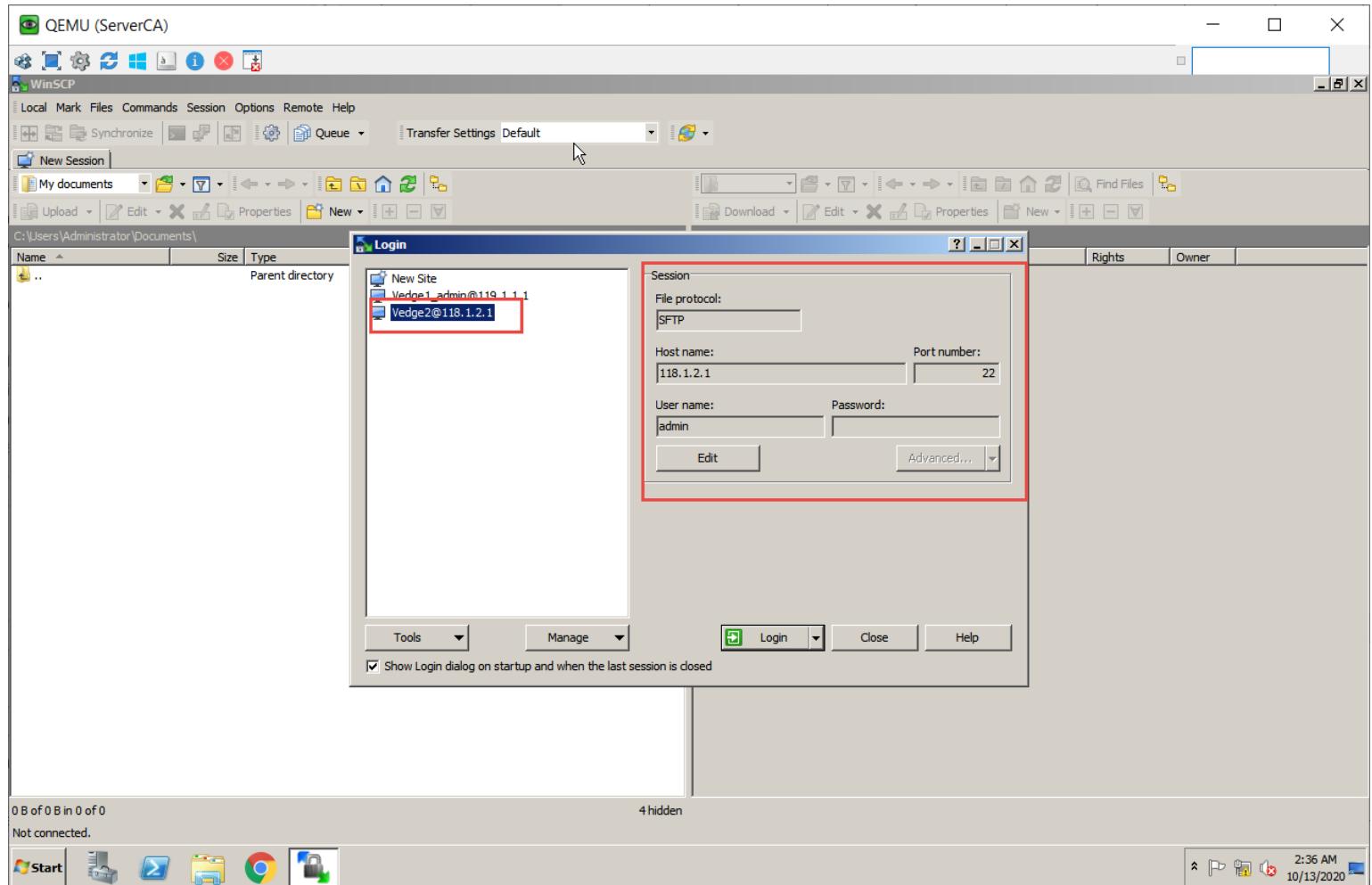
Search Options Total Rows: 20

State	Device Model	Chassis Number	Serial No./Token	Hostname↑	System IP	Site ID	Mode	Assigned	
	vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	A61F6406	vEdge1	119.1.1.21	1	CLI	—	...
	CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C93...	Token - 74360338b195...	—	—	—	CLI	—	...
	CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD...	Token - 0ba7e5da97b7f...	—	—	—	CLI	—	...
	vEdge Cloud	2eb9da66-7af0-04fd-6f49-fba8e745554c	Token - 7132efe986193...	—	—	—	CLI	—	...
	vEdge Cloud	d6d98a35-f70c-9955-0106-86192f237f...	Token - 45762da037dff...	—	—	—	CLI	—	...
	vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737...	Token - 89854fac6a002...	—	—	—	CLI	—	...
	vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924...	Token - 898afb6f2a52f...	—	—	—	CLI	—	...
	vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e850561...	Token - 7b2f4c767fd25...	—	—	—	CLI	—	...
	CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6E...	Token - 9fc4540ef1d38...	—	—	—	CLI	—	...
	CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542...	Token - eb4aa30174b1f...	—	—	—	CLI	—	...
	CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E...	Token - 6a7dd54f7eb7f...	—	—	—	CLI	—	...
	CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A...	Token - c1159ba3bc25f...	—	—	—	CLI	—	...
	CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A...	Token - bd4a897a56ebf...	—	—	—	CLI	—	...

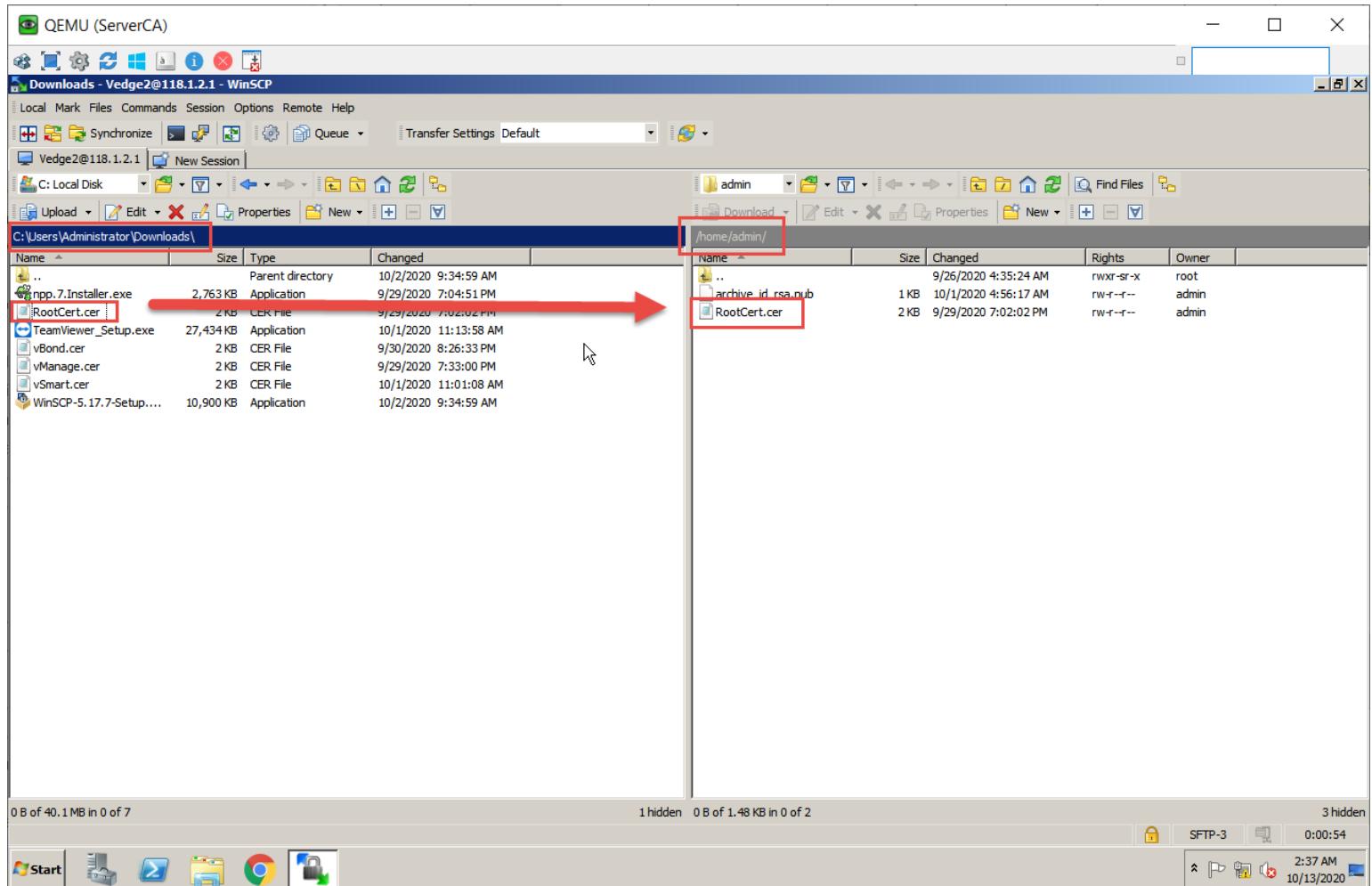
## vEDGE-2

### Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open WINSOCK application.
- Connect to vEdge2 using the following information:
  - o IP Address : **118.1.2.1**
  - o Protocol - SFTP
  - o Username : **admin**
  - o Password : **admin**



- Copy the RootCert.cer file from the Downloads folder to the: **/home/admin folder on the vEdge2**



## Task 2- Install the Root Certificate on vEdge2

- Connect to the console of vEdge2 and issue the following command:

**vEdge2:**

```
request root-cert-chain install /home/admin/RootCert.cer
```

Log install successfully as bellow:

```
vEdge2# request root-cert-chain install /home/admin/RootCert.cer
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/RootCert.cer via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```



### Task 3- Active vEdge on vManage

- Navigate to Configuration ➔ Devices

The screenshot shows the Cisco vManage web interface. The title bar says "Cisco vManage" and the address bar shows "Not secure 192.168.100.2 index.html#/app/config/devices/vedge". The main menu on the left has "CONFIGURATION | DEVICES" selected. Under "WAN Edge List", there are two tabs: "Controllers" and "WAN Edge List" (which is selected). Below the tabs are buttons for "Change Mode", "Upload WAN Edge List", "Export Bootstrap Configuration", and "Sync Smart Account". A search bar and a "Search Options" dropdown are also present. The main area displays a table of devices. The columns are: State, Device Model, Chassis Number, Serial No./Token, Hostname, System IP, Site ID, and Mod. There are 20 total rows. The 2nd row from the top, which is highlighted with a red border, represents a vEdge Cloud device with the following details:

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Mod
	CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C9...	Token - 74360338b195951a386b47a75ef...	-	--	-	CLI ...
	CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD...	Token - 0ba7e5da97b7f3f67f28a86d3a75...	-	--	-	CLI ...
	vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	A61F6406	vEdge1	119.1.1.21	1	CLI ...
	vEdge Cloud	2eb9da66-7af... (highlighted)	Token - 7132e...	-	--	-	CLI ...
	vEdge Cloud	d6d98a35-f70c-9955-0106-86192f2377...	Token - 45762da037dff0b5df1897a9e03...	-	--	-	CLI ...
	vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737...	Token - 89854fac6a002d1e39b697eabdd...	-	--	-	CLI ...
	vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924...	Token - 898afb6f2a52f4089c03b7cf521cf...	-	--	-	CLI ...
	vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e850561...	Token - 7b2f4c767fd25af5b3431e444218...	-	--	-	CLI ...
	CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6E...	Token - 9fc4540ef1d3866620ff03395f288...	-	--	-	CLI ...
	CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542...	Token - eb4aa30174b1f84e0612cba127c...	-	--	-	CLI ...
	CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E...	Token - 6a7dd54f7eb7fcf9ad3a2c009fab6...	-	--	-	CLI ...
	CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A...	Token - c1159ba3bc25f6cdeb3aed98598...	-	--	-	CLI ...
	CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A...	Token - bd4a897a56ebfa96028f5c4b67ad...	-	--	-	CLI ...

- Note and use the Chassis Number and Token number for the 2<sup>nd</sup> vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge2 console

```
Request vedge-cloud activate chassis-number <chassis number> <token>
```

```
request vedge-cloud activate chassis-number XXXXXXXX-XXXXXXX-XXXX-XXXXXXXXXXXX token
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

- You should see the vEdge in the vManage console with a Certificate issued.



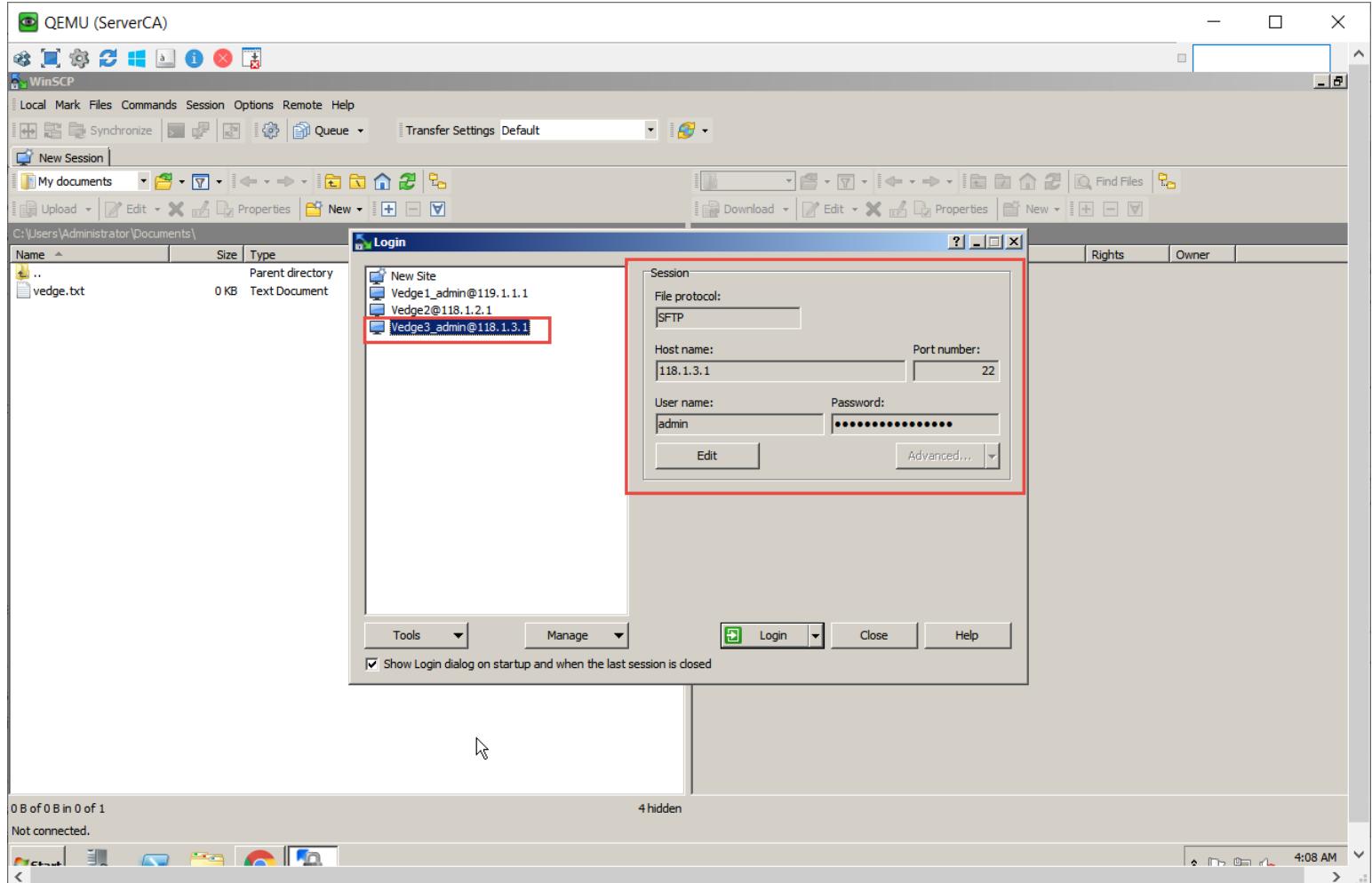
The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Configuration' and has a 'Devices' section with various options like Certificates, Network Design, Templates, Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area is titled 'CONFIGURATION | DEVICES' and 'WAN Edge List'. It displays a table of devices with columns: State, Device Model, Chassis Number, Serial No./Token, Hostname, System IP, Site ID, and Actions. There are 20 total rows. The row for 'vEdge Cloud' with ID 2 is selected and highlighted with a red border. The table data is as follows:

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Actions
CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C93...	CSR-6BD335E2-5434-26B7-0987-F0C93...	Token - 74360338b195...	--	--	--	...
CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD...	CSR-1951E7AC-CFA9-F6D4-DB18-05BD...	Token - 0ba7e5da97b7f...	--	--	--	...
vEdge Cloud	dc423af0-28e9-fa62-3e40-309e1f5e978	dc423af0-28e9-fa62-3e40-309e1f5e978	A61F6406	vEdge1	119.1.1.21	1	...
<b>vEdge Cloud</b>	<b>2eb9da66-7af0-04fd-6f49-fba8e745554c</b>	<b>2eb9da66-7af0-04fd-6f49-fba8e745554c</b>	<b>440303C9</b>	<b>vEdge2</b>	<b>118.1.2.22</b>	<b>2</b>	<b>...</b>
vEdge Cloud	d6d98a35-f70c-9955-0106-86192f2377...	d6d98a35-f70c-9955-0106-86192f2377...	Token - 45762da037dff...	--	--	--	...
vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737...	aa5c2054-6e37-ca2a-3eed-1b96c4737...	Token - 89854fac6a002...	--	--	--	...
vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924...	131e1368-7fdd-d545-0cbc-5a4d82924...	Token - 898afb6f2a52f...	--	--	--	...
vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e850561...	6c4ac09a-d3b3-625b-6040-6f5e850561...	Token - 7b2f4c767fd25...	--	--	--	...
CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6E...	CSR-D5FE8C21-E2DA-8AF7-446E-9E6E...	Token - 9fc4540ef1d38...	--	--	--	...
CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542...	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542...	Token - eb4aa30174b1f...	--	--	--	...
CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E...	CSR-B038DB62-2CA9-E2AA-5427-377E...	Token - 6a7dd54f7eb7f...	--	--	--	...
CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A...	CSR-1C2E4075-F30D-1729-2C56-A74A...	Token - c1159ba3bc25f...	--	--	--	...
CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A...	CSR-E583C473-393D-2FAD-9A84-7D2A...	Token - bd4a897a56ebf...	--	--	--	...

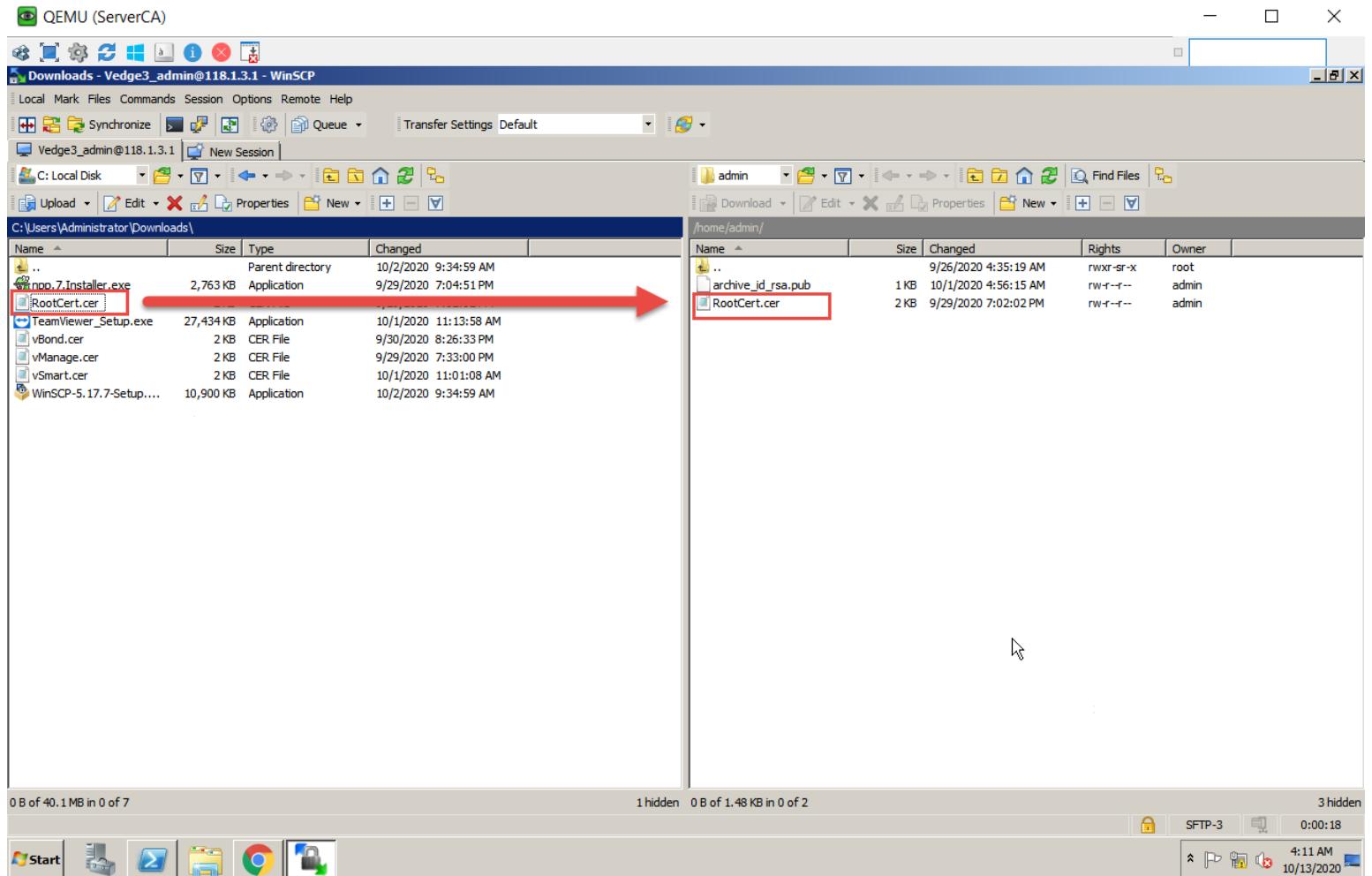
## vEDGE-3

### Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open WINSCP application.
- Connect to vEdge3 using the following information:
  - o IP Address : 118.1.3.1
  - o Protocol - SFTP
  - o Username : admin
  - o Password : admin



- Copy the RootCert.cer file from the Downloads folder to the: **/home/admin** folder on the **vEdge3**



## Task 2- Install the Root Certificate on vEdge3

- Connect to the console of vEdge3 and issue the following command:

**vEdge3:**

```
request root-cert-chain install /home/admin/RootCert.cer
```

Log install successfully as bellow:

```
vEdge3# request root-cert-chain install /home/admin/RootCert.cer
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/RootCert.cer via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```



### Task 3- Active vEdge on vManage

- Navigate to Configuration ➔ Devices

The screenshot shows the Cisco vManage interface. The left sidebar is titled 'Configuration' and has a 'Devices' section. The main pane is titled 'CONFIGURATION | DEVICES' and shows a 'WAN Edge List'. The table contains 20 rows of vEdge devices. The third row, which is highlighted with a red border, represents a vEdge Cloud device with the following details:

State	Device Model	Chassis Number	Serial No./Token	Hostname	System
Green	CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C93...	Token - 74360338b195951a386b47a75efe4bb4	--	--
Green	CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD...	Token - 0ba7e5da97b7f3f67f28a86d3a7575ec	--	--
Green	vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	A61F6406	vEdge1	119.1.1
Green	vEdge Cloud	2eb9da66-7afd-04fd-6f49-fba8e745554c	440303C9	vEdge2	118.1.2
Green	vEdge Cloud	d6d98a35-f70c-9955-0106-86192f2377...	Token - 45762da037dff0b5df1897a9e033508	--	--
Green	vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737...	Token - 89854fac6a002d1e39b697eabdd9c970	--	--
Green	vEdge Cloud	131e1368-7fd-d545-0cbc-5a4d82924...	Token - 898afb6f2a52f4089c03b7cf521cf9ee	--	--
Green	vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e850561...	Token - 7b2f4c767fd25af5b3431e4442181d6d	--	--
Green	CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6E...	Token - 9fc4540ef1d3866620ff03395f2885fe	--	--
Green	CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542...	Token - eb4aa30174b1f84e0612cba127c67033	--	--
Green	CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E...	Token - 6a7dd54f7eb7fcf9ad3a2c009fab6d1f	--	--
Green	CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A...	Token - c1159ba3bc25f6cdeb3aed9859807550	--	--
Green	CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A...	Token - bd4a897a56ebfa96028f5c4b67ad7abc	--	--

- Note and use the Chassis Number and Token number for the 3rd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge3 console

```
Request vedge-cloud activate chassis-number <chassis number> <token>
```

```
request vedge-cloud activate chassis-number XXXXXXXX-XXXXXXX-XXXX-XXXXXXXXXXXX token  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

- You should see the vEdge in the vManage console with a Certificate issued.



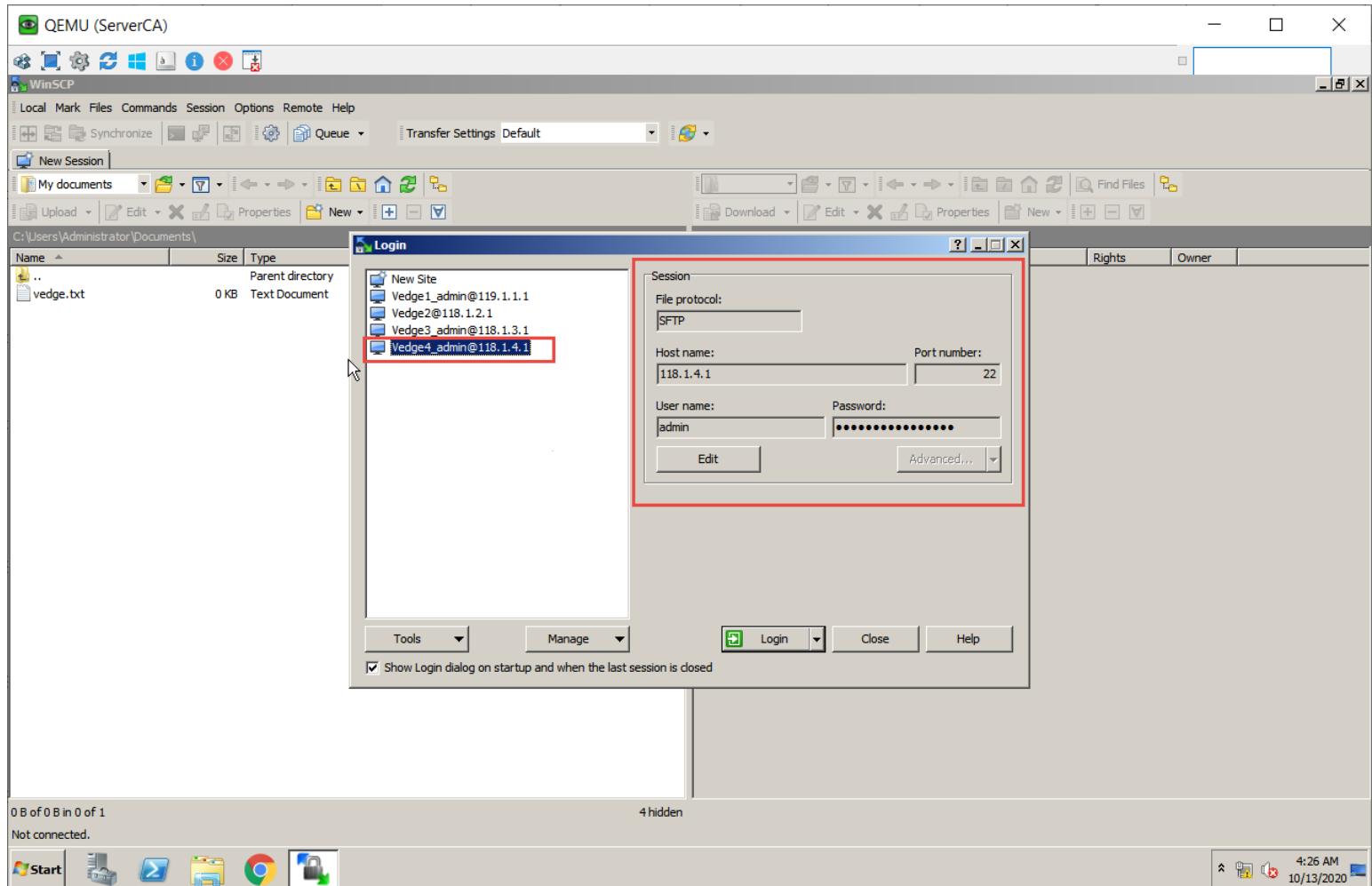
The screenshot shows the Cisco vManage interface with the title "Cisco vManage". The left sidebar is titled "Configuration" and has a "Devices" section. Under "Devices", there are links for Certificates, Network Design, Templates, Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area is titled "CONFIGURATION | DEVICES" and "WAN Edge List". It includes buttons for "Change Mode", "Upload WAN Edge List", "Export Bootstrap Configuration", and "Sync Smart Account". A search bar and a "Search Options" dropdown are also present. The table displays the following data:

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Actions
CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C93...	Token - 74360338b195...	-	-	-	-	...
CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD...	Token - 0ba7e5da97b7f...	-	-	-	-	...
vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	A61F6406	vEdge1	119.1.1.21	1	...	...
vEdge Cloud	2eb9da66-7afd-04fd-6f49-fba8e745554c	440303C9	vEdge2	118.1.2.22	2	...	...
vEdge Cloud	d6d98a35-f70c-9955-0106-86192f2377...	28B158E3	vEdge3	118.1.3.23	3	...	...
vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737...	Token - 89854fac6a002...	-	-	-	-	...
vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924...	Token - 898afb6f2a52f...	-	-	-	-	...
vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e850561...	Token - 7b2f4c767fd25...	-	-	-	-	...
CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6E...	Token - 9fc4540ef1d38...	-	-	-	-	...
CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542...	Token - eb4aa30174b1f...	-	-	-	-	...
CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E...	Token - 6a7dd54f7eb7f...	-	-	-	-	...
CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A...	Token - c1159ba3bc25f...	-	-	-	-	...
CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A...	Token - bd4a897a56ebf...	-	-	-	-	...

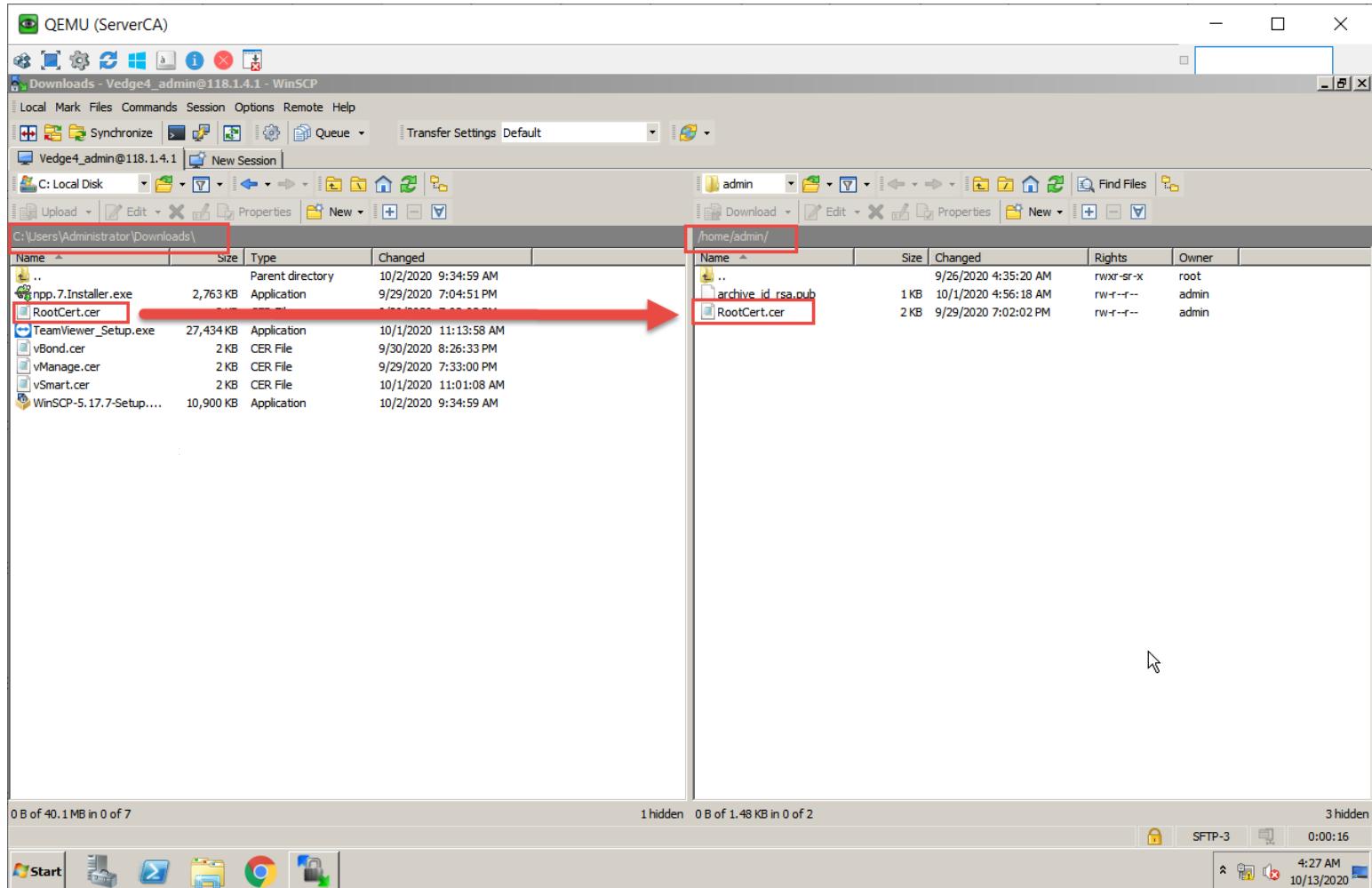
## vEDGE-4

### Task 1 – Upload the Root Certificate to the vEdge

- On the Windows Server, open WINSSCP application.
- Connect to vEdge4 using the following information:
  - o IP Address : 118.1.4.1
  - o Protocol - SFTP
  - o Username : admin
  - o Password : admin



- Copy the RootCert.cer file from the Downloads folder to the: /home/admin folder on the vEdge4



## Task 2- Install the Root Certificate on vEdge4

- Connect to the console of vEdge4 and issue the following command:

**vEdge4:**

```
request root-cert-chain install /home/admin/RootCert.cer
```

Log install successfully as bellow:

```
vEdge4# request root-cert-chain install /home/admin/RootCert.cer
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/RootCert.cer via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```



### Task 3- Active vEdge on vManage

- Navigate to Configuration ➔ Devices

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site	
Green	CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C9355262CE	Token - 74360338b195951a386b47a75efe4bb4	-	-	-	***
Green	CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD394455...	Token - 0ba7e5da97b7f3f67f28a86d3a7575ec	-	-	-	***
Green	vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	A61F6406	vEdge1	119.1.1.21	1	***
Green	vEdge Cloud	2eb9da66-7afd-04fd-6f49-fba8e745554c	440303C9	vEdge2	118.1.2.22	2	***
Green	vEdge Cloud	d6d98a35-f70c-9955-0106-86192f237703	28B158E3	vEdge3	118.1.3.23	3	***
Yellow	vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737bc0	Token - 89854fac6a002d1e39b697eabdd9c970	-	-	-	***
Green	vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924d94	Token - 898afb6f2a52f4089c03b7cf521cf9ee	-	-	-	***
Green	vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e8505617a	Token - 7b2f4c767fd25af5b3431e4442181d6d	-	-	-	***
Green	CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6EDDF28A...	Token - 9fc4540ef1d3866620ff03395f2885fe	-	-	-	***
Green	CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542260A230	Token - eb4aa30174b1f84e0612cba127c67033	-	-	-	***
Green	CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E2A3B6...	Token - 6a7dd54f7eb7fcf9ad3a2c009fab6d1f	-	-	-	***
Green	CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A690577...	Token - c1159ba3bc25f6cdeb3aed9859807550	-	-	-	***
Green	CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A9275E3...	Token - bd4a897a56eba96028f5c4b67ad7abc	-	-	-	***

- Note and use the Chassis Number and Token number for the 3rd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge3 console

```
Request vedge-cloud activate chassis-number <chassis number> <token>
```

```
request vedge-cloud activate chassis-number XXXXXXXX-XXXXXXX-XXXX-XXXXXXXXXXXX token
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

- You should see the vEdge in the vManage console with a Certificate issued.

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/devices/vedge

Cisco vManage

CONFIGURATION | DEVICES

WAN Edge List Controllers

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

Total Rows: 20

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site	Actions
Green	CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C9355262CE	Token - 74360338b195951a386b47a75efe4bb4	--	--	--	...
Green	CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD394455...	Token - 0ba7e5da97b7f3f67f28a86d3a7575ec	--	--	--	...
Green	vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	A6156406	vEdge1	119.1.1.21	1	...
Green	vEdge Cloud	2eb9da66-7af6-04fd-6f49-fba8e745554c	440303C9	vEdge2	118.1.2.22	2	...
Green	vEdge Cloud	d6d98a35-f70c-9955-0106-86192f237703	28B158E3	vEdge3	118.1.3.23	3	...
Green	vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737bc0	2EEF75FE	vEdge4	118.1.4.24	--	...
Green	vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924d94	Token - 898afb6f2a52f4089c03b7cf521cf9ee	--	--	--	...
Green	vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e8505617a	Token - 7b2f4c767fd25af5b3431e4442181d6d	--	--	--	...
Green	CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6EDDF28A...	Token - 9fc4540ef1d3866620ff03395f2885fe	--	--	--	...
Green	CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542260A230	Token - eb4aa30174b1f84e0612cba127c67033	--	--	--	...
Green	CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E2A3B6...	Token - 6a7dd54f7eb7fcf9ad3a2c009fab6d1f	--	--	--	...
Green	CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A690577...	Token - c1159ba3bc25f6cdeb3aed9859807550	--	--	--	...
Green	CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A9275E3...	Token - bd4a897a56ebfa96028f5c4b67ad7abc	--	--	--	...

Start

4:35 AM 10/13/2020



## Lab 11 – Initializing cEdge – CLI

### cEDGE-1

#### Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - o Host-name : **cEdge5**
  - o Organization: "**viptela sdwan**"
  - o System-IP: **118.1.5.25**
  - o Site ID: **5**
  - o vbond Address: **100.1.1.4**
  - o Timezone: Based on the appropriate Timezone

Note: Default username: **admin** Default password: **admin**

#### **cEdge1**

```
config-transaction
hostname cEdge1
system
system-ip 118.1.5.25
site-id 5
organization-name "viptela sdwan"
vbond 100.1.1.4
exit
clock timezone America/Antigua
commit
```

#### Task 2 – Configure the Interface and Tunnel Parameters

- Configure the Interface parameters based on the following:
  - o GigabitEthernet1 Parameters
    - IP Address: 118.1.5.1/24
    - Default Route: 118.1.5.2
  - o Tunnel Parameters Parameters
    - Tunnel Interface: Tunnel1
    - Tunnel Source: GigabitEthernet1
    - Tunnel Mode: SDWAN
  - o SDWAN Interface Parameters
    - Interface: GigabitEthernet1
    - Encapsulation: IPSec
    - Color: default
    - Tunnel Services (All, NetConf, SSHD)



**cEdge1:**

```
cEdge1
config-transaction
interface GigabitEthernet1
no shutdown
ip address 118.1.5.1 255.255.255.0
exit
ip route 0.0.0.0 0.0.0.0 118.1.5.2

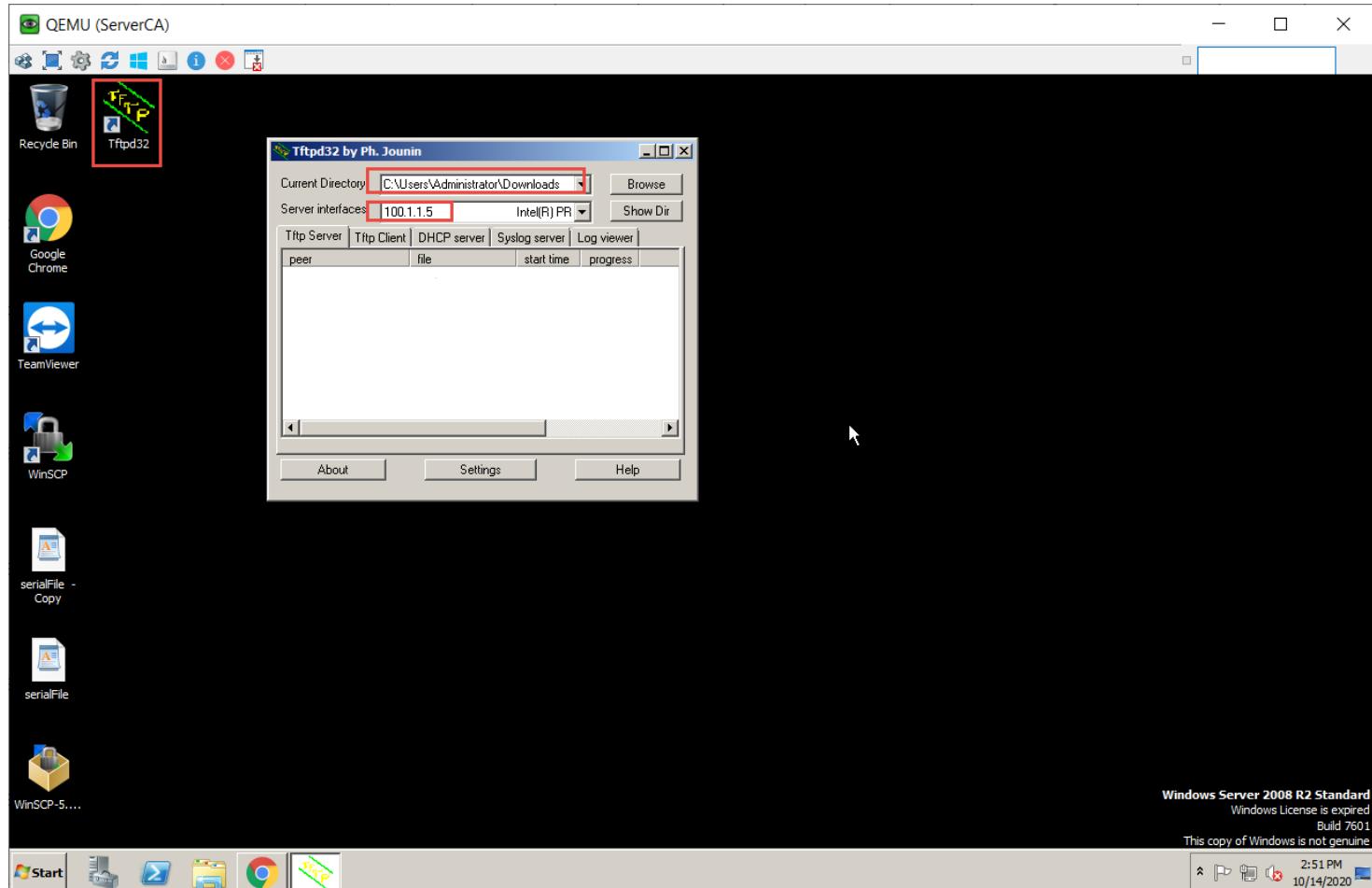
interface Tunnel1
no shutdown
ip unnumbered GigabitEthernet1
tunnel source GigabitEthernet1
tunnel mode sdwan
exit
sdwan
interface GigabitEthernet1
tunnel-interface
encapsulation ipsec
color default
allow-service all
allow-service sshd
allow-service netconf
exit
exit
commit
```

## Lab 12 – Registering cEdges in vManage

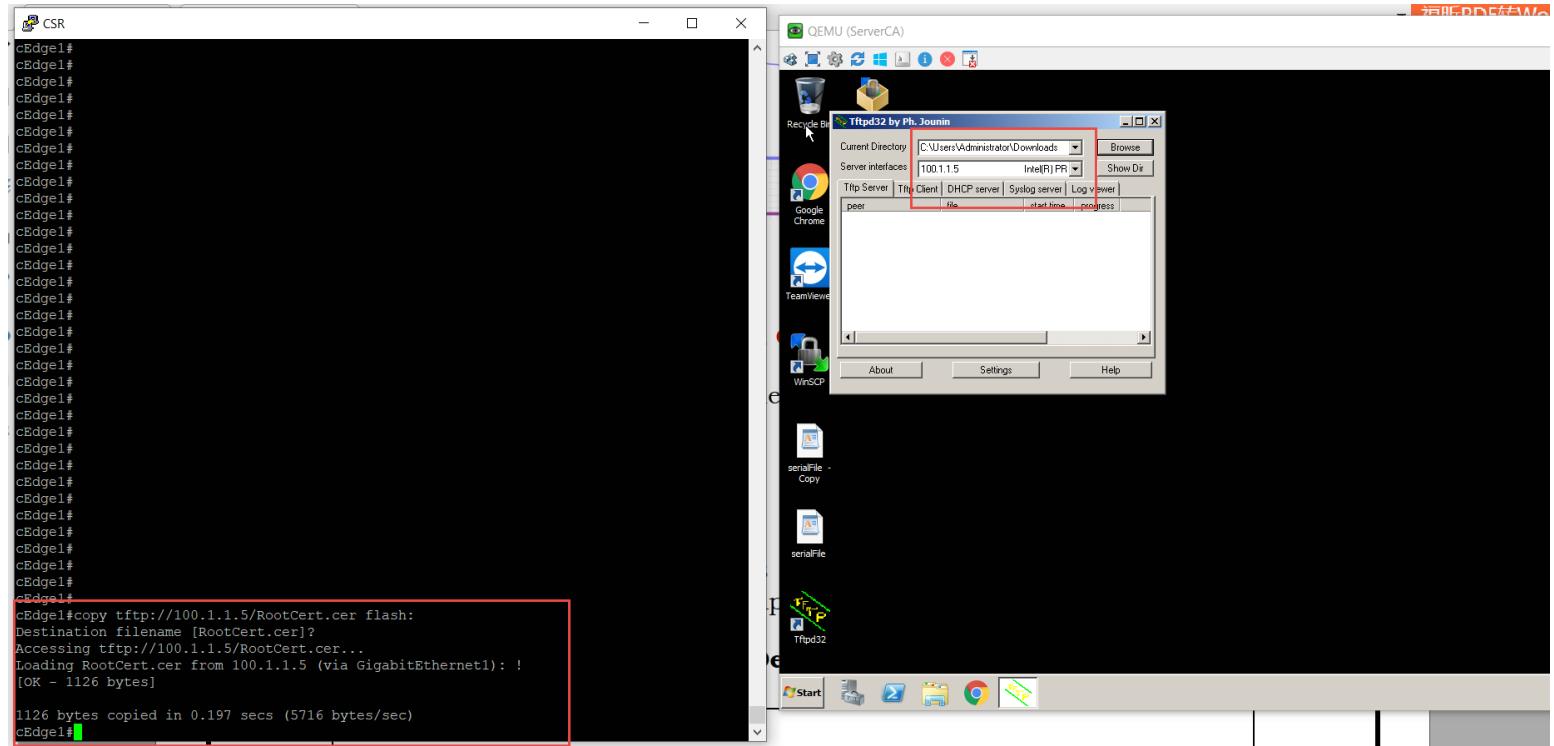
### cEDGE-1

#### Task 1 – Upload the Root Certificate to the cEdge

- Open the TFTP Application on the Windows Server.
- Configure the Default Folder as the Downloads Folder and using the 100.1.1.5 as the TFTP Interface.

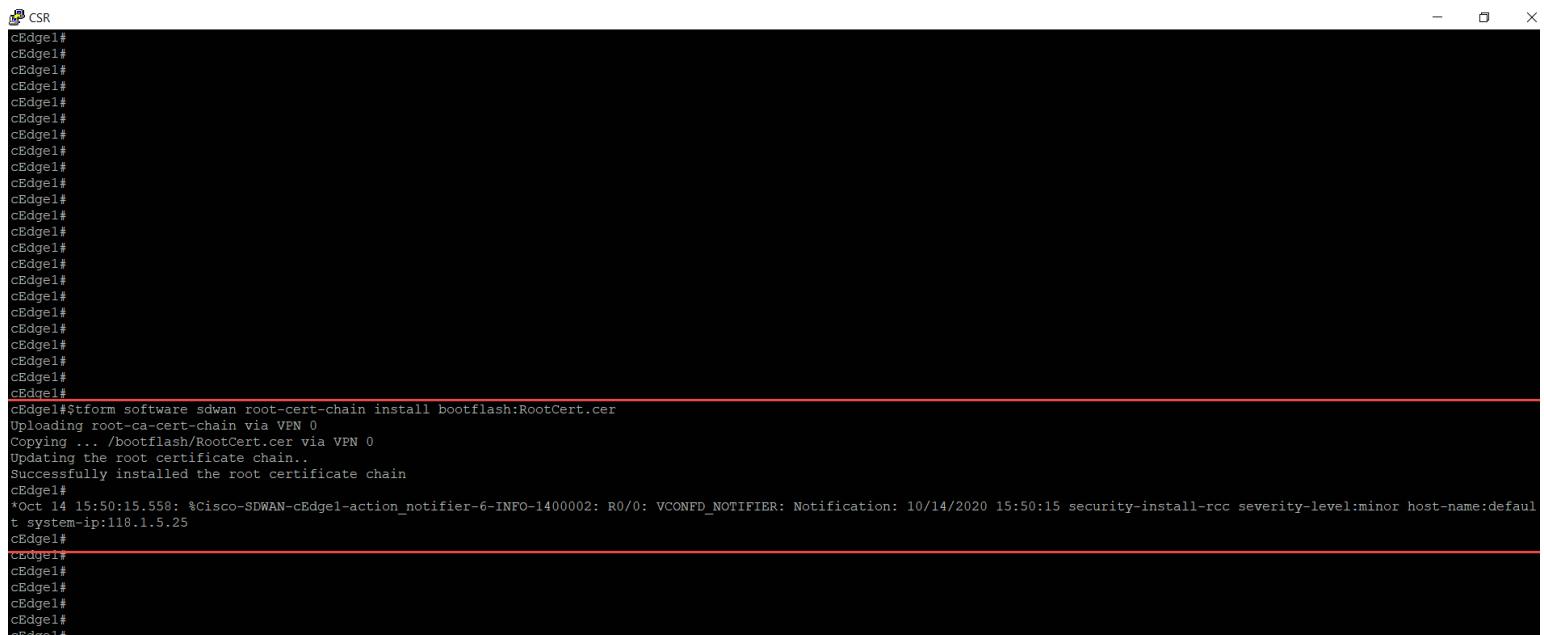


- Connect to the console of cEdge1 and copy the RootCert.cer file to flash: using the following command: **copy tftp://100.1.1.5/RootCert.cer flash:**



## Task 2 – Install the Root Certificate on cEdge1

Connect to the console of cEdge1 and issue the following command: request platform software sdwan root-cert-chain install bootflash:RootCert.cer





### Task 3 - Activate cEdge on vManage

- Navigate to Configuration -> Devices
- Note and use the Chassis Number and Token number for the 1<sup>st</sup> CSR Device from vManage.

State	Device Model	Chassis Number	Serial No./Token	Hostname	S
Up	CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C9355262CE	Token - 74360338b195951a386b47a75efe4bb4	--	...
Up	CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD394455A5	Token - 0ba7e5da97b7f3f67f28a86d3a7575ec	--	...
Up	vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	A61F6406	vEdge1	1
Up	vEdge Cloud	2eb9da66-7af0-04fd-6f49-fba8e745554c	440303C9	vEdge2	1
Up	vEdge Cloud	d6d98a35-f70c-9955-0106-86192f237703	28B158E3	vEdge3	1
Up	vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737bc0	2EEF75FE	vEdge4	1
Up	vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924d94	Token - 898afb6f2a52f4089c03b7cf521cf9ee	--	...
Up	vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e8505617a	Token - 7b2f4c767fd25af5b3431e4442181d6d	--	...
Up	CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6EDDF28A41	Token - 9fc4540ef1d3866620ff03395f2885fe	--	...
Up	CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF542260A230	Token - eb4aa30174b1f84e0612cba127c67033	--	...
Up	CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E2A3B60E0	Token - 6a7dd54f7eb7fcf9ad3a2c009fab6d1f	--	...
Up	CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A6905770C	Token - c1159ba3bc25f6cdeb3aed9859807550	--	...
Up	CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A9275E3F0	Token - bd4a897a56ebfa96028f5c4b67ad7abc	--	...

- Use the information from the previous step in the following command on the cEdge1 console.

```
request platform software sdwan vedge_cloud activate chassis-number CSR-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXX token XXXXXXXXXXXXXXXXXXXXXXXXX
```

- You should see the vEdge in the vManage console with a Certificate issued

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/devices/vedge

Cisco vManage

CONFIGURATION | DEVICES

WAN Edge List Controllers

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

Search Options

Total Rows: 20

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	Actions
Green	CSR1000v	CSR-6BD335E2-5434-26B7-0987-F0C9355...	75BCF9D6	cEdge1	118.1.5.25	-	...
Green	CSR1000v	CSR-1951E7AC-CFA9-F6D4-DB18-05BD39...	Token - 0ba7e5da97b7f3f67f28a86d3a7575ec	--	--	--	...
Green	vEdge Cloud	dc423af0-28e9-fa62-3e40-309e51f5e978	A61F6406	vEdge1	119.1.1.21	1	...
Green	vEdge Cloud	2eb9da66-7af0-04fd-6f49-fba8e745554c	440303C9	vEdge2	118.1.2.22	2	...
Green	vEdge Cloud	d6d98a35-f70c-9955-0106-86192f237703	28B158E3	vEdge3	118.1.3.23	3	...
Green	vEdge Cloud	aa5c2054-6e37-ca2a-3eed-1b96c4737bc0	2EEF75FE	vEdge4	118.1.4.24	4	...
Green	vEdge Cloud	131e1368-7fdd-d545-0cbc-5a4d82924d94	Token - 898afb6f2a52f4089c03b7cf521cf9ee	--	--	--	...
Green	vEdge Cloud	6c4ac09a-d3b3-625b-6040-6f5e8505617a	Token - 7b2f4c767fd25af5b3431e4442181d6d	--	--	--	...
Green	CSR1000v	CSR-D5FE8C21-E2DA-8AF7-446E-9E6EDD...	Token - 9fc4540ef1d3866620ff03395f2885fe	--	--	--	...
Green	CSR1000v	CSR-4E5E13F6-56D8-FFE9-F2A3-BF54226...	Token - eb4aa30174b1f84e0612cba127c67033	--	--	--	...
Green	CSR1000v	CSR-B038DB62-2CA9-E2AA-5427-377E2A...	Token - 6a7dd54f7eb7fcf9ad3a2c009fab6d1f	--	--	--	...
Green	CSR1000v	CSR-1C2E4075-F30D-1729-2C56-A74A690...	Token - c1159ba3bc25f6cdeb3aed9859807550	--	--	--	...
Green	CSR1000v	CSR-E583C473-393D-2FAD-9A84-7D2A92...	Token - bd4a897a56ebfa96028f5c4b67ad7abc	--	--	--	...

Start

3:12 AM  
10/15/2020



## Lab 13 – Configuring Feature Template –System

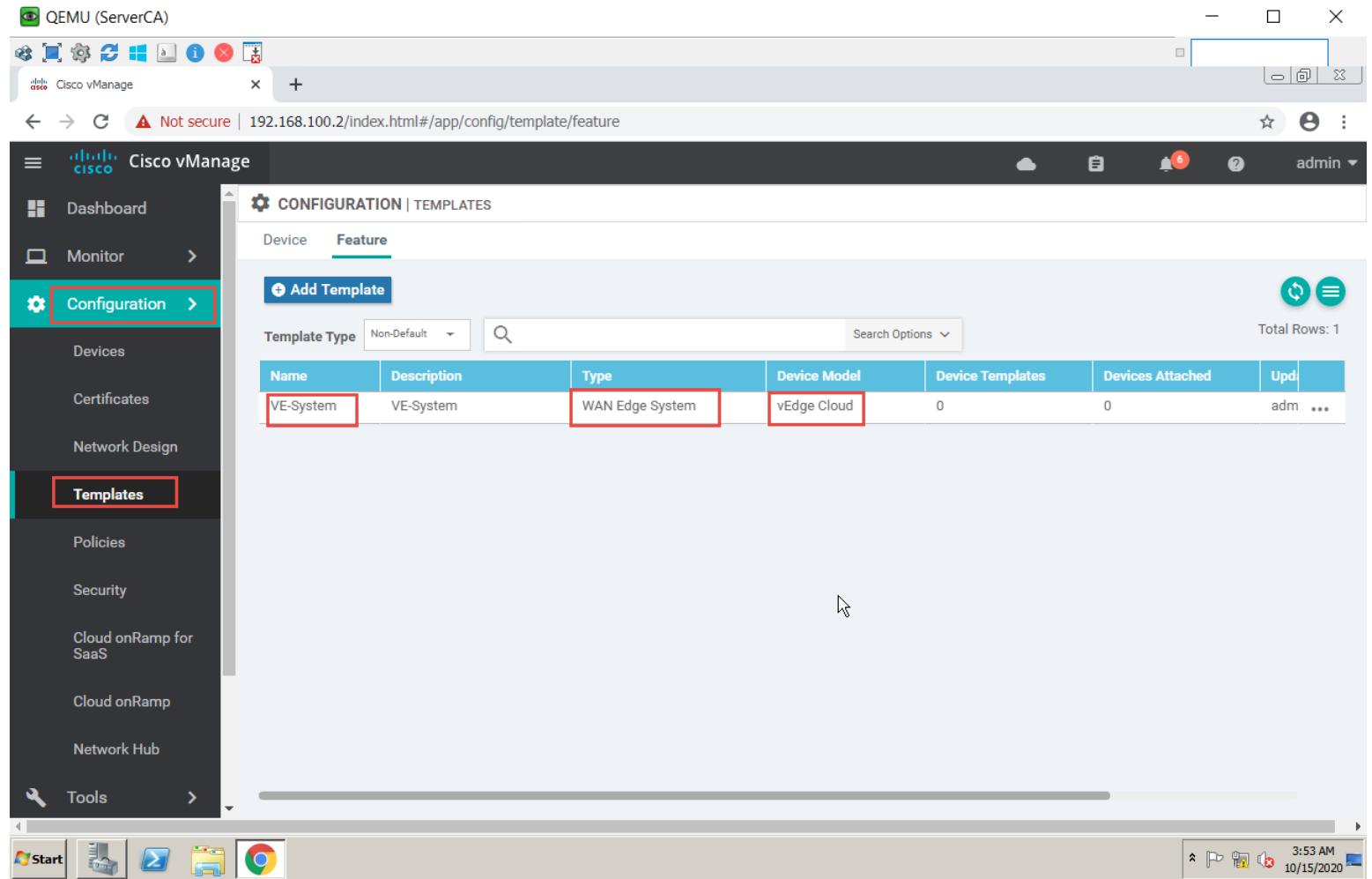
### Task 1 – Configure the System Template to be used by all vEdgeCloud Devices

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → Basic Information → System
- Configure the System parameters based on the following:
  - o Template Name: VE-System
  - o Description: VE-System
  - o Site ID → Device Specific
  - o System IP → Device Specific
  - o Hostname → Device Specific
  - o Timezone → Global: America/Antigua
  - o Console Baud Rate → 9600
- Click Save to save the Template.

The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing the 'Configuration' section selected. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows 'Feature' selected under 'Device'. A sub-section titled 'Feature Template > Add Template' is shown with 'System' selected. The 'Basic Configuration' tab is active. The configuration fields are as follows:

- Device Type: vEdge Cloud
- Template Name: VE-System
- Description: VE-System
- Basic Configuration:
  - Site ID: Global (selected from a dropdown menu)
  - System IP: Device Specific (selected from a dropdown menu)
  - Overlay ID: 1

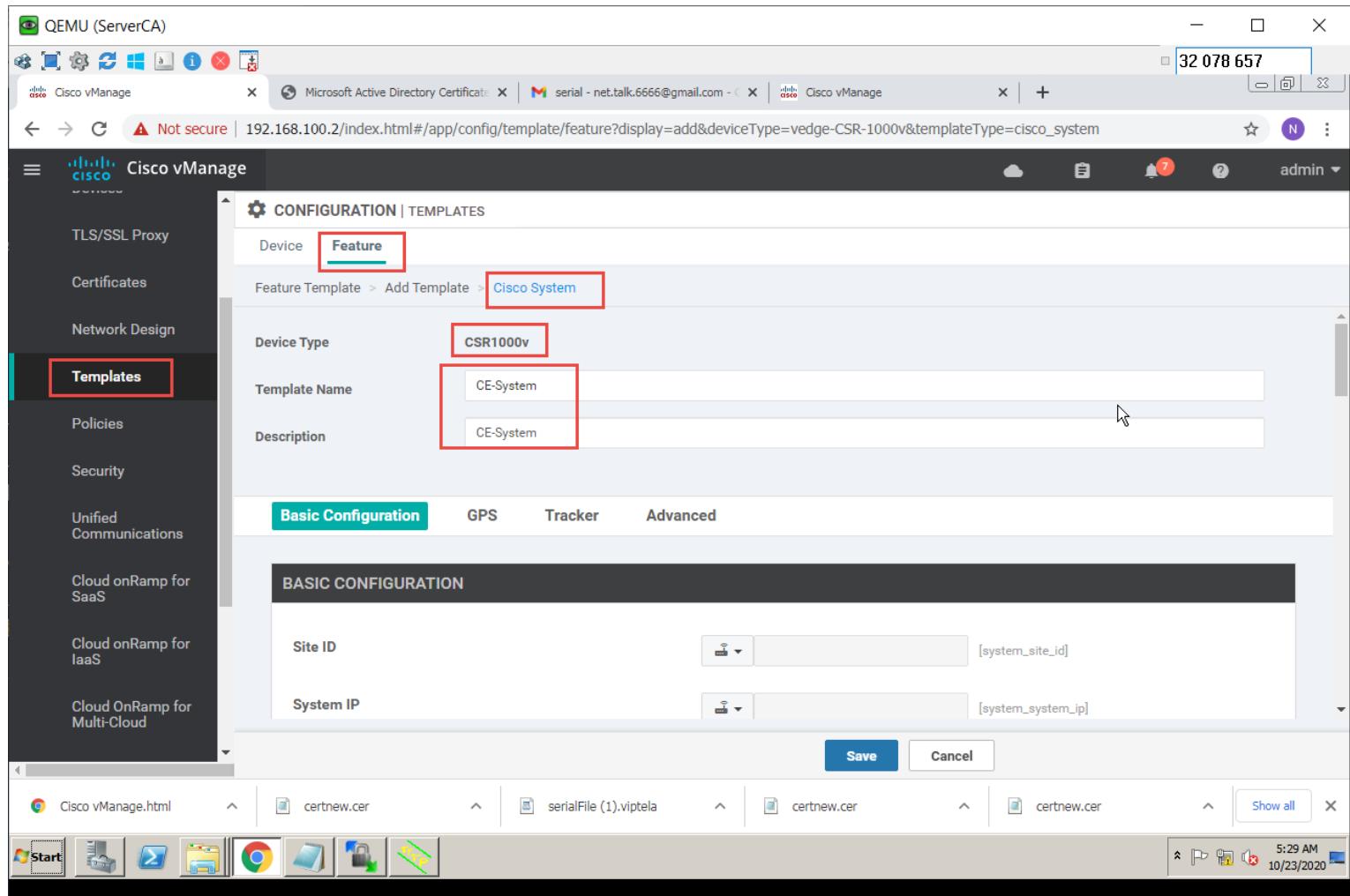
At the bottom right of the configuration form are 'Save' and 'Cancel' buttons. The status bar at the bottom right shows the date and time: 3:47 AM 10/15/2020.



Name	Description	Type	Device Model	Device Templates	Devices Attached	Upd.
VE-System	VE-System	WAN Edge System	vEdge Cloud	0	0	adm ...

## Task 2 – Configure the System Template to be used by all cEdgeCloud Devices

- In vManage, Navigate to Configuration → Templates → Feature → CSR 1000v → Basic Information → Cisco System
- Configure the System parameters based on the following:
  - o Template Name : CE-System
  - o Description: CE-System
  - o Site ID → Device Specific
  - o System IP → Device Specific
  - o Hostname → Device Specific
  - o Timezone → Global : America/Antigua
  - o Console Baud Rate → 9600
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar has a 'Templates' section highlighted with a red box. The main area shows a 'CONFIGURATION | TEMPLATES' screen with a 'Feature' tab selected (also highlighted with a red box). A breadcrumb path 'Feature Template > Add Template > Cisco System' is visible. The configuration form includes fields for 'Device Type' (CSR1000v), 'Template Name' (CE-System), and 'Description' (CE-System). Below the form are tabs for 'Basic Configuration', 'GPS', 'Tracker', and 'Advanced'. Under 'Basic Configuration', there are fields for 'Site ID' and 'System IP', both with dropdown menus. At the bottom right are 'Save' and 'Cancel' buttons. The browser's address bar shows the URL: 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-CSR-1000v&templateType=cisco\_system. The status bar at the bottom shows the date and time: 5:29 AM 10/23/2020.



The screenshot shows the Cisco vManage web interface. The left sidebar is dark-themed and includes sections for Dashboard, Monitor, Configuration (which is selected), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area has a light background and displays the 'CONFIGURATION | TEMPLATES' section under 'Feature'. A table lists system templates:

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Total Rows: 2
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	admin ***	
VE-System	VE-System	WAN Edge System	vEdge Cloud	0	0	admin ***	

### Task 3 – Configure the System Template to be used by all vSmart Device

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → Basic Information → System
- Configure the System parameters based on the following:
  - o Template Name : Vsmartrt-System
  - o Description : Vsmartrt-System
  - o Site ID → Device Specific
  - o System IP → Device Specific
  - o Hostname → Device Specific
  - o Timezone → Global : America/Antigua
- Click Save to save the Template.

[Download PNETLab Platform](#)[PNETLAB Store](#)[PNETLab.com](#)

Cisco vManage

**CONFIGURATION | TEMPLATES**

Device **Feature**

Feature Template > Add Template > System

Device Type **vSmart**

Template Name **Vsmart-System**

Description **Vsmart-System**

**Basic Configuration** GPS Advanced

**BASIC CONFIGURATION**

Site ID **[system\_site\_id]**

System IP **[system\_system\_ip]**

Overlay ID **1**

Hostname **[system\_host\_name]**

Location

Device Groups

Timezone **America/Antigua**

Description

Save Cancel

Cisco vManage

**CONFIGURATION | TEMPLATES**

Device **Feature**

**Add Template**

Template Type Non-Default

Search Options Total Rows: 35

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:49:25 PM ADT
BR-VE-VPNINT-VPN12-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:51:24 PM ADT
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	admin	29 Oct 2020 11:00:30 PM ADT
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	admin	30 Oct 2020 5:27:27 AM ADT
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3	admin	30 Oct 2020 5:28:24 AM ADT
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	admin	30 Oct 2020 5:31:07 AM ADT
vSmart-VPN-VPN0	vSmart-VPN-VPN0	vSmart VPN	vSmart	0	0	admin	01 Nov 2020 4:13:42 AM AST
HQ-VE-VPNINT-VPN512-E0	HQ-VE-VPNINT-VPN512-E0	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:17:24 PM ADT
HQ-VE-VPNINT-VPN0-G0	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:11:01 PM ADT
HQ-VE-BGP-VPN0	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	1	1	admin	30 Oct 2020 1:13:14 PM ADT
HQ-VE-VPN-VPN1	HQ-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:18:27 PM ADT
HQ-VE-VPN-VPN512	HQ-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:13:56 PM ADT
<b>Vsmart-System</b>	<b>Vsmart-System</b>	<b>vSmart System</b>	<b>vSmart</b>	<b>0</b>	<b>0</b>	<b>admin</b>	<b>01 Nov 2020 4:47:35 AM AST</b>
HQ-VE-VPN-VPN0	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:09:25 PM ADT
BR-CSR-VPN-VPN1	BR-CSR-VPN-VPN1	Cisco VPN	CSR1000v	1	1	admin	01 Nov 2020 12:37:33 AM ADT
BR-CSR-OSPF-VPN1	BR-CSR-OSPF-VPN1	Cisco OSPF	CSR1000v	1	1	admin	01 Nov 2020 12:41:28 AM ADT
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	Cisco VPN	CSR1000v	1	1	admin	31 Oct 2020 11:53:32 PM ADT
BR-CSR-OSPF-VPN0	BR-CSR-OSPF-VPN0	Cisco OSPF	CSR1000v	1	1	admin	01 Nov 2020 12:00:47 AM ADT
BR-CSR-VPNINT-VPN1-G2	BR-CSR-VPNINT-VPN1-G2	Cisco VPN Interface Ethernet	CSR1000v	1	1	admin	01 Nov 2020 12:39:57 AM ADT
vSmart-VPN-VPN512	vSmart-VPN-VPN512	vSmart VPN	vSmart	0	0	admin	01 Nov 2020 4:17:07 AM AST
vSmart-VPNINT-VPN0-E1	vSmart-VPNINT-VPN0-E1	vSmart Interface	vSmart	0	0	admin	01 Nov 2020 4:27:07 AM AST
BR-CSR-VPNINT-VPN0-G1	BR-CSR-VPNINT-VPN0-G1	Cisco VPN Interface Ethernet	CSR1000v	1	1	admin	31 Oct 2020 11:56:31 PM ADT
BR-CSR-VPNINT-VPN0-G3	BR-CSR-VPNINT-VPN0-G3	Cisco VPN Interface Ethernet	CSR1000v	1	1	admin	31 Oct 2020 11:58:29 PM ADT



## Lab 14 – Configuring Feature Template –Banner

### Task 1 – Configure the Banner Template to be used by all vEdgeCloud Devices

- In vManage, Navigate to **Configuration** → **Templates** → **Feature** → **vEdge Cloud** → **OTHER TEMPLATES** → **Banner**
- Configure the Banner parameters based on the following:
  - Template Name : VE-Banner
  - Description : VE-Banner
  - Login Banner: PNETLAB Authorized Users Only !!!
  - MOTD: Welcome To SD-PNETLAB !!!
- Click Save to save the Template.

The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing the 'Configuration' section with 'Templates' selected. The main content area is titled 'CONFIGURATION | TEMPLATES' and has the 'Feature' tab selected. A sub-section titled 'OTHER TEMPLATES' is displayed, containing several templates: Banner, BGP, Bridge, DHCP Server, IGMP, Logging, Multicast, OSPF, PIM, and SNMP. The 'Banner' template is highlighted with a red box. On the left, under 'Select Devices', 'vEdge 100 M' is selected, and 'vEdge Cloud' is checked. The bottom right corner of the screen shows the date and time: 10/15/2020 and 4:05 AM.



The screenshot shows the Cisco vManage web interface. The left sidebar is titled "Cisco vManage" and includes links for Dashboard, Monitor, Configuration (which is selected and highlighted in teal), Templates, Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area is titled "CONFIGURATION | TEMPLATES" and has tabs for "Device" and "Feature" (which is selected). A button "+ Add Template" is visible. Below it is a search bar and a "Search Options" dropdown. A table lists templates with columns: Name, Description, Type, Device Model, Device Templates, Devices Attached, Updated By, and Last Modified. The first row, "VE-Banner", is highlighted with a red border. The table shows three total rows.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Modified
VE-Ba...	VE-Banner	Banner	vEdge Cloud	0	0	admin	15 ...
CE-Sys...	CE-System	WAN Edge System	CSR1000v	0	0	admin	15 ...
VE-Sys...	VE-System	WAN Edge System	vEdge Cloud	0	0	admin	15 ...

## Task 2 – Configure the Banner Template to be used by all cEdgeCloud Devices

- In vManage, **Navigate to Configuration → Templates → Feature → CSR 1000v → OTHER TEMPLATES → Cisco Banner**
- Configure the Banner parameters based on the following:
  - o Template Name: CE-Banner
  - o Description: CE-Banner
  - o Banner: PNETLAB Authorized Users Only !!!
  - o MOTD: Welcome To SD-PNETLAB !!!
- Click Save to save the Template.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/template/feature

Cisco vManage

Dashboard

Monitor

Configuration >

Devices

Certificates

Network Design

**Templates**

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools >

CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type Non-Default

Search Options Total Rows: 4

Name	Description	Type	Device Model	Device Templates	Devices Attached	Up
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	adl ...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	adl ...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	adl ...
VE-System	VE-System	WAN Edge System	vEdge Cloud	0	0	adl ...

Start

4:13 AM  
10/15/2020

## Lab 15 - Configuring Feature Templates -VPN & VPN Interfaces for VPN 0 & 512 —Branch Site(vEdges)

### Task 1 – Configure a VPN Template to be used by all Branch vEdgeCloud Devices for VPN 0

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN
- Configure the VPN parameters based on the following:
  - o Template Name: BR-VE-VPN-VPNO
  - o Description: BR-VE-VPN-VPNO

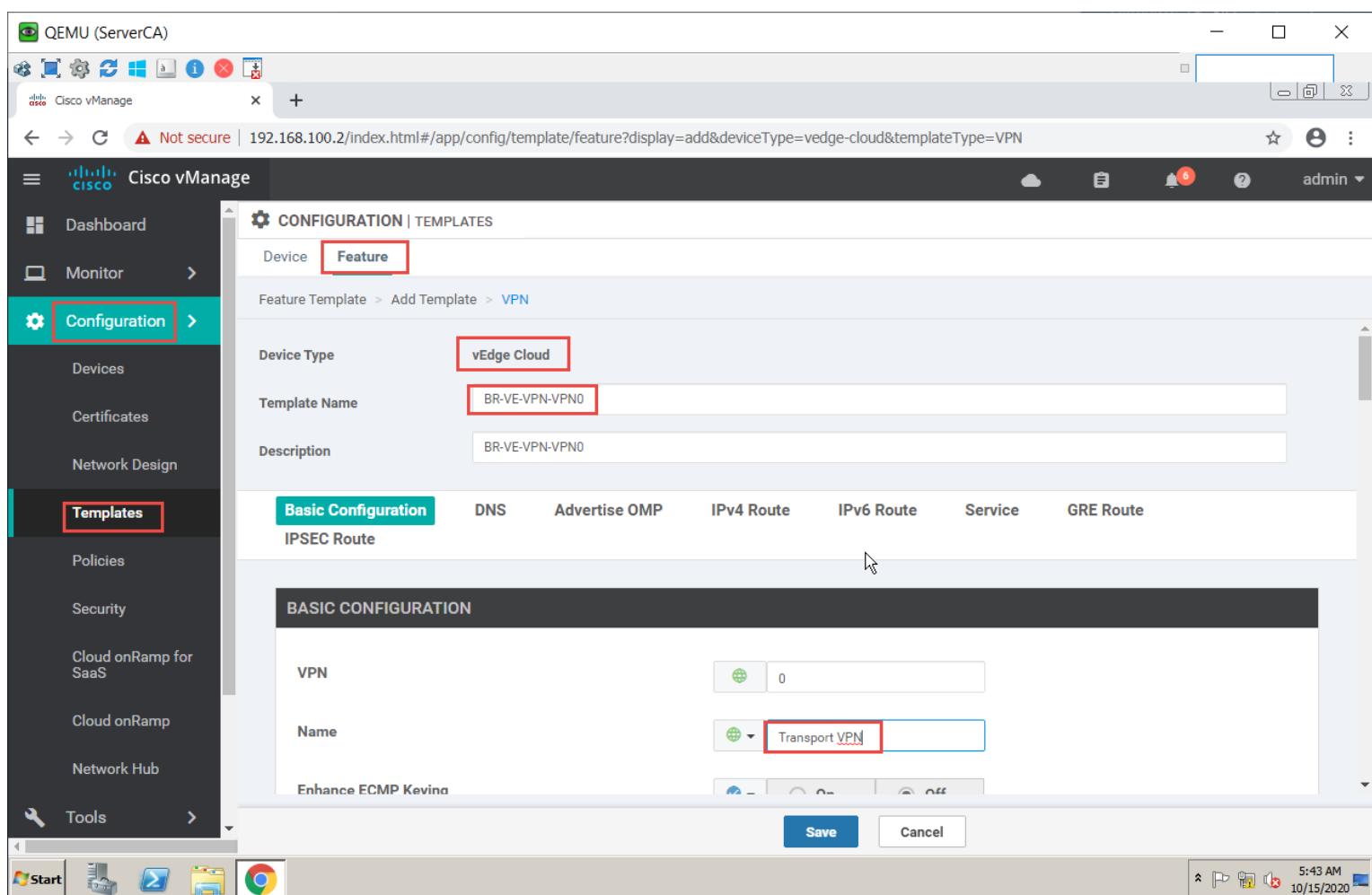
#### Basic Configuration

- o VPN → Global: 0
- o Name → Global: Transport VPN

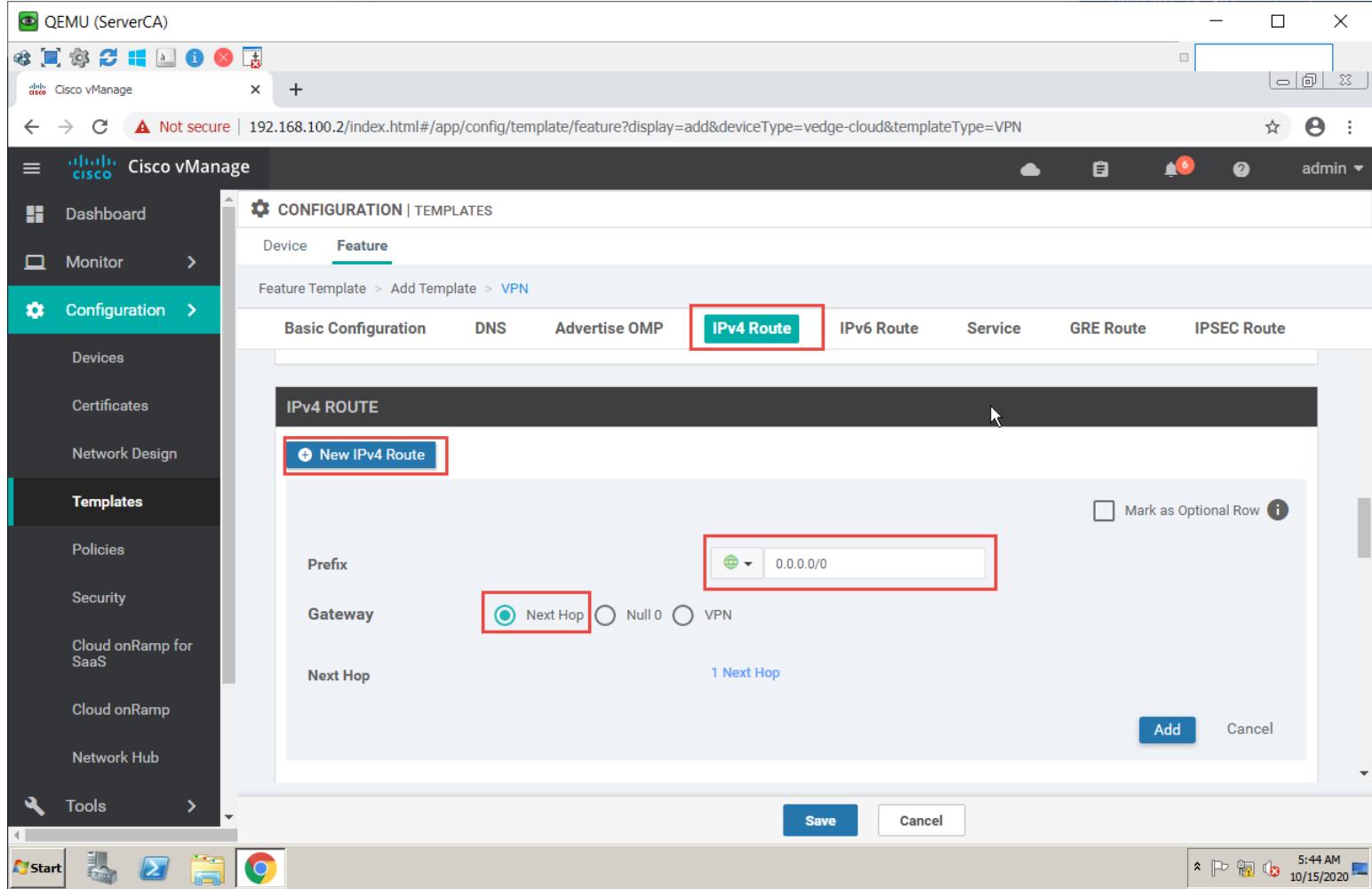
#### IPv4 Route

- o Prefix → Global: 0.0.0.0/0
- o Next Hop → Device Specific

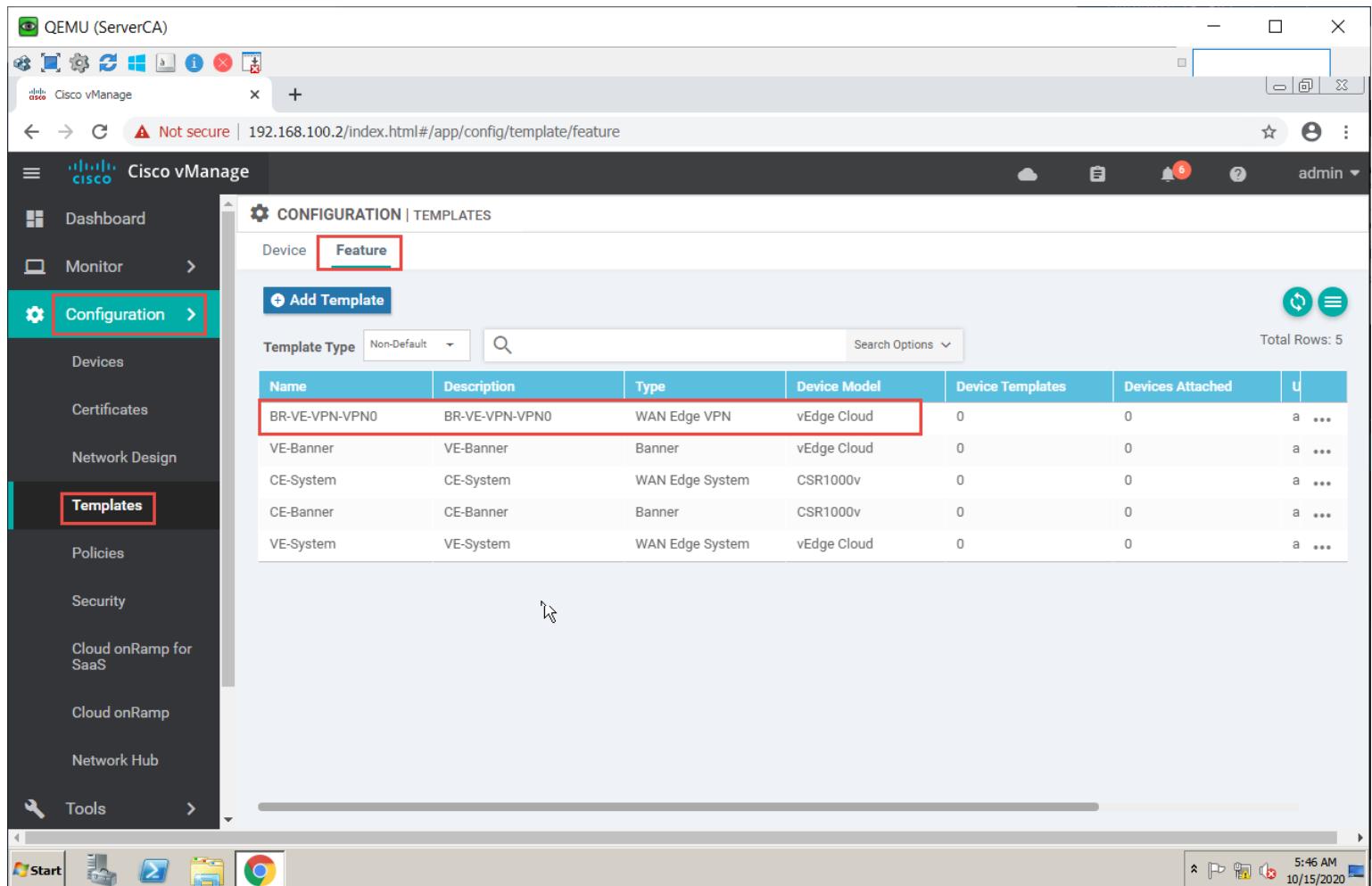
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is open with the 'Configuration' tab selected. Under 'TEMPLATES', the 'Feature' tab is highlighted. The main content area shows the 'CONFIGURATION | TEMPLATES' screen for adding a new template. The 'Device Type' is set to 'vEdge Cloud'. The 'Template Name' field contains 'BR-VE-VPN-VPNO'. The 'Description' field contains 'BR-VE-VPN-VPNO'. Below this, there are tabs for 'Basic Configuration', 'DNS', 'Advertise OMP', 'IPv4 Route', 'IPv6 Route', 'Service', and 'GRE Route'. The 'IPSEC Route' tab is currently inactive. Under the 'Basic Configuration' tab, there is a 'BASIC CONFIGURATION' section. It shows 'VPN' set to '0' and 'Name' set to 'Transport VPN'. There is also an 'Enhance ECMP Keypad' section. At the bottom right of the configuration window are 'Save' and 'Cancel' buttons. The status bar at the bottom of the browser window shows the date and time as '5:43 AM 10/15/2020'.



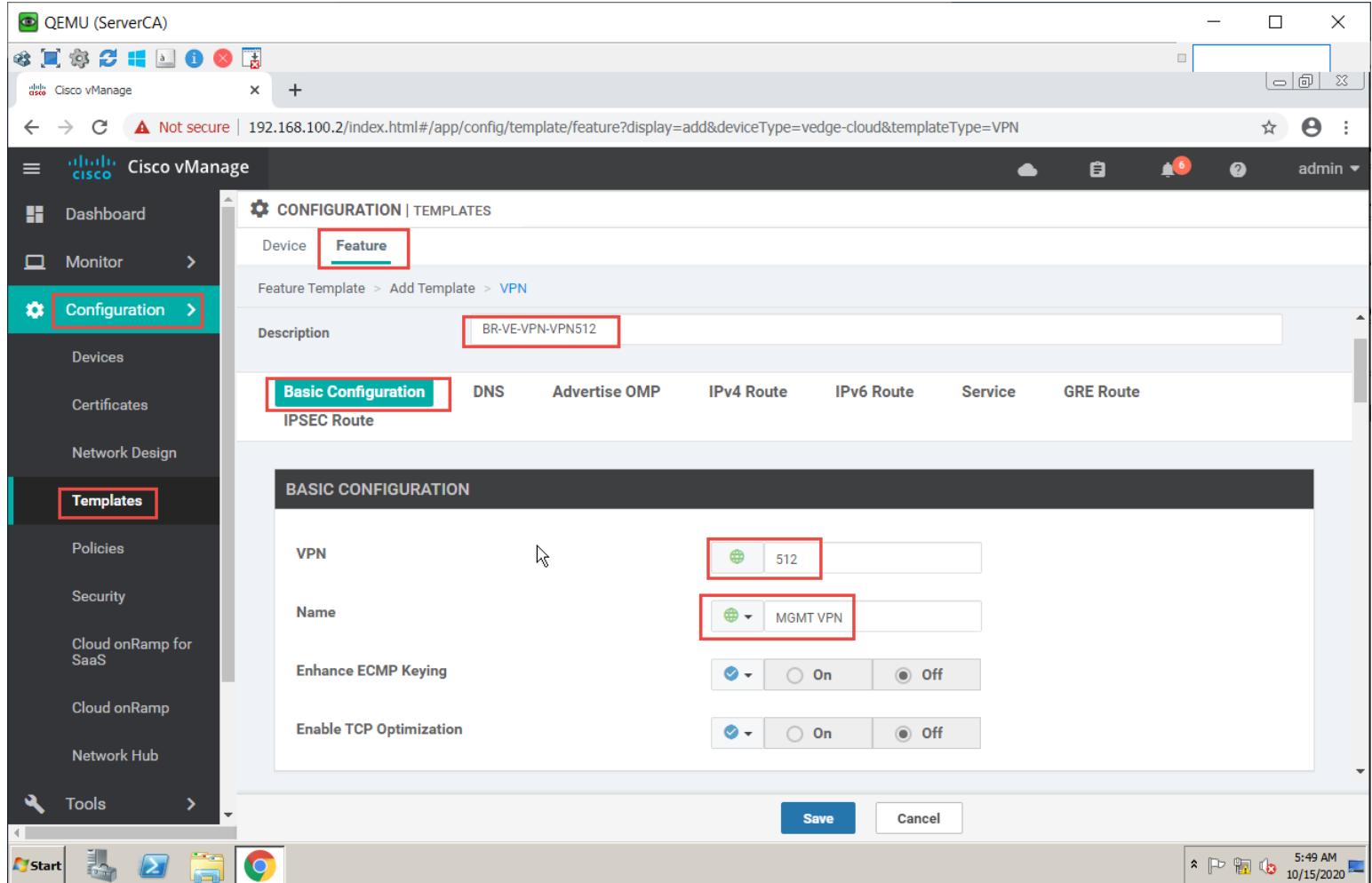
The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Configuration' and includes sections for Devices, Certificates, Network Design, Templates (which is currently selected), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. The top navigation bar shows 'Cisco vManage' and the URL '192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN'. The main content area is titled 'CONFIGURATION | TEMPLATES' under 'Feature'. It shows a 'Feature Template > Add Template > VPN' path. A tab bar at the top of the content area includes 'Basic Configuration', 'DNS', 'Advertise OMP', 'IPv4 Route' (which is highlighted with a red box), 'IPv6 Route', 'Service', 'GRE Route', and 'IPSEC Route'. Below this, a sub-section titled 'IPv4 ROUTE' has a button '+ New IPv4 Route' (also highlighted with a red box). The configuration form includes fields for 'Prefix' (with a dropdown menu and a value '0.0.0.0/0' highlighted with a red box), 'Gateway' (with radio buttons for 'Next Hop' (selected), 'Null 0', and 'VPN'), and 'Next Hop' (with a link '1 Next Hop'). At the bottom of the form are 'Save' and 'Cancel' buttons.



Name	Description	Type	Device Model	Device Templates	Devices Attached	Actions
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	<a href="#">a</a> <a href="#">...</a>
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	<a href="#">a</a> <a href="#">...</a>
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	<a href="#">a</a> <a href="#">...</a>
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	<a href="#">a</a> <a href="#">...</a>
VE-System	VE-System	WAN Edge System	vEdge Cloud	0	0	<a href="#">a</a> <a href="#">...</a>

## Task 2 – Configure a VPN Template to be used by all Branch vEdgeCloud Devices for VPN 512

- In vManage, **Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN**
- Configure the VPN parameters based on the following:
  - o Template Name: BR-VE-VPN-VPN512
  - o Description: BR-VE-VPN-VPN512
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is titled "Cisco vManage" and includes sections for Dashboard, Monitor, Configuration (which is selected and highlighted with a red box), Templates (also highlighted with a red box), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area is titled "CONFIGURATION | TEMPLATES" and shows "Feature" selected under "Device". A breadcrumb navigation path indicates "Feature Template > Add Template > VPN". The "Description" field contains "BR-VE-VPN-VPN512". Below this, the "Basic Configuration" tab is selected (highlighted with a red box) among other tabs: DNS, Advertise OMP, IPv4 Route, IPv6 Route, Service, and GRE Route. Under "IPSEC Route", there is a "BASIC CONFIGURATION" section with the following settings:

- VPN: A dropdown menu set to "512" (highlighted with a red box).
- Name: A dropdown menu set to "MGMT VPN" (highlighted with a red box).
- Enhance ECMP Keying: A group of three radio buttons with the first one checked.
- Enable TCP Optimization: A group of three radio buttons with the first one checked.

At the bottom right of the configuration window are "Save" and "Cancel" buttons. The bottom of the screen shows a Windows taskbar with icons for Start, File Explorer, Task View, and Google Chrome, along with system status icons on the right.



The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Configuration' and includes options like Devices, Certificates, Network Design, Templates (which is selected), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. The main content area is titled 'CONFIGURATION | TEMPLATES' and has tabs for 'Device' and 'Feature'. It shows a table of templates with columns: Name, Description, Type, Device Model, Device Templates, Devices Attached, and Updated. One row, 'BR-VE-VPN-VPN512', is highlighted with a red border.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	admir ...
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	admir ...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	admir ...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	admir ...
VE-System	VE-System	WAN Edge System	vEdge Cloud	0	0	admir ...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	0	0	admir ...

### Task 3 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - Template Name: BR-VE-VPNINT-VPNO-G0
  - Description: BR-VE-VPNINT-VPNO-G0

#### Basic Configuration

- Shutdown → Global: No
- Interface Name → Global: Ge0/0
- IPv4 Address → Static → Device Specific

#### Tunnel

- Tunnel Inteface → Global: On
- Color → Global: MPLS

#### Allow Service

- All → Global: On





- NETCONF → Global: On
- SSH → Global: On
- Click Save to save the Template.

The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Cisco vManage' and includes 'Dashboard', 'Monitor', 'Configuration' (which is selected and highlighted with a red box), 'Templates' (which is also highlighted with a red box), 'Devices', 'Certificates', 'Network Design', 'Policies', 'Security', 'Cloud onRamp for SaaS', 'Cloud onRamp', and 'Network Hub'. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows 'Feature' selected. It displays a 'Feature Template > Add Template > VPN Interface Ethernet' path. The 'Device Type' is set to 'vEdge Cloud'. The 'Template Name' is 'BR-VE-VPNINT-VPN0-G0'. The 'Description' is 'BR-VE-VPNINT-VPN0-G0'. The 'Basic Configuration' tab is active, showing the 'BASIC CONFIGURATION' section. Under 'Shutdown', the 'Yes' radio button is unselected and 'No' is selected (highlighted with a red box). Under 'Interface Name', the dropdown shows 'ge0/0' (highlighted with a red box). Under 'Description', there is a checkbox and a text input field. At the bottom of the configuration window are 'Save' and 'Cancel' buttons. The status bar at the bottom shows '5:56 AM 10/15/2020'.



The screenshot shows the Cisco vManage web interface. The left sidebar is dark grey with white text, showing navigation options like Dashboard, Monitor, Configuration (which is selected), Templates, Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. Below the sidebar is a toolbar with icons for Start, Task View, File Explorer, and Google Chrome. The main content area has a light grey header with the Cisco logo and the title "Cisco vManage". Below the header is a search bar with the URL "192.168.100.2/index.html#/app/config/template/feature". The main content is titled "CONFIGURATION | TEMPLATES" and has tabs for "Device" and "Feature" (which is selected). There is a button "+ Add Template" and a search bar. A table below shows template details:

Name	Description	Type	Device Model	Device Templates	Devices Attached	Actions
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	0	0	...
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	...
VE-System	VE-System	WAN Edge System	vEdge Cloud	0	0	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	0	0	...

## Task 4 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 0 for Interface G0/1

- In vManage, **Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN Interface Ethernet**
- Configure the VPN parameters based on the following:
  - o Template Name: BR-VE-VPNINT-VPN0-G1
  - o Description: BR-VE-VPNINT-VPN0-G1

### Basic Configuration

- o Shutdown → Global: No
- o Interface Name → Global: Ge0/1
- o IPv4 Address → Static → Device Specific

### Tunnel

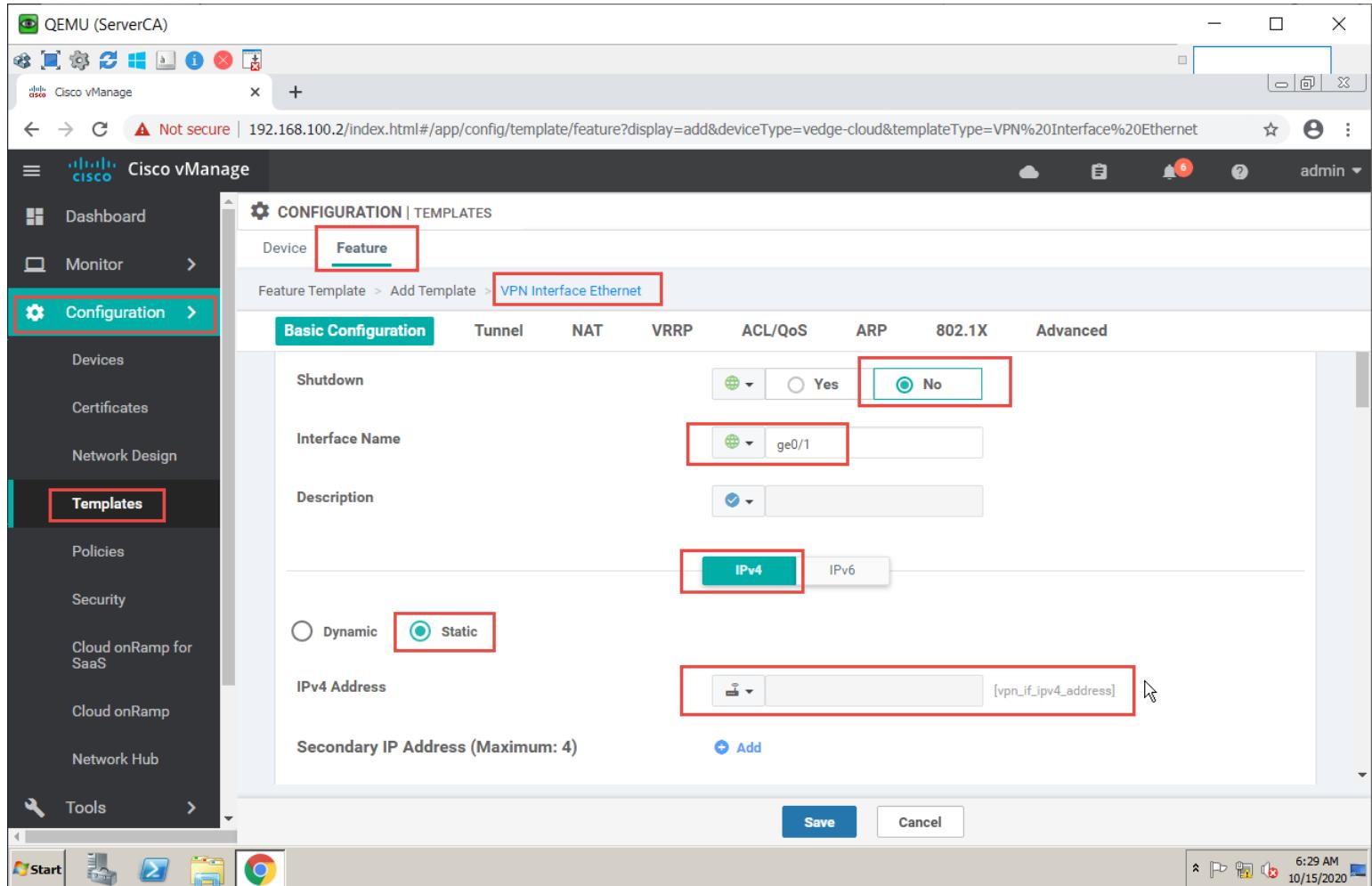
- o Tunnel Interface → Global: On
- o Color → Global: BIZ-Internet

### Allow Service

- o All → Global: On



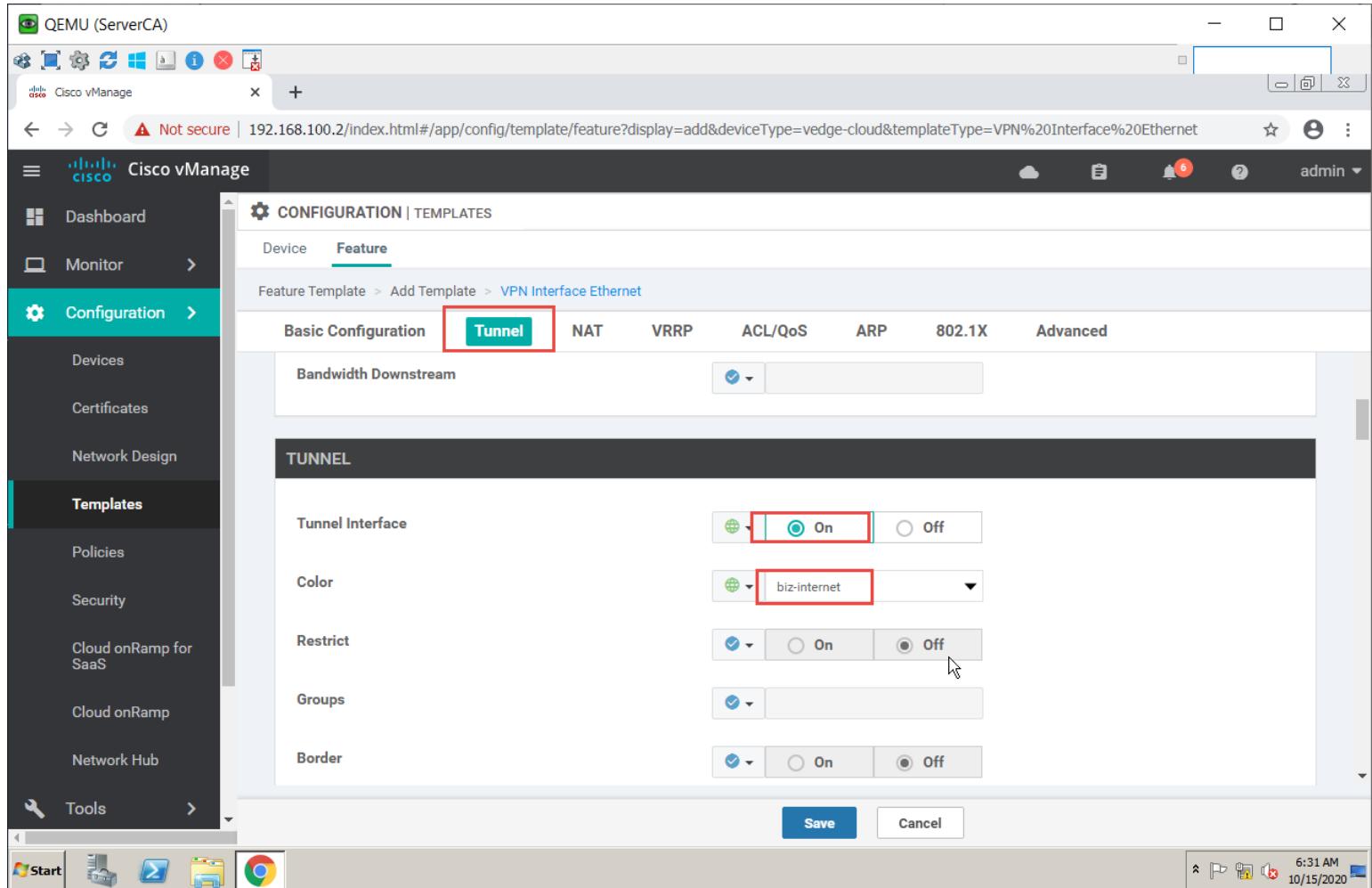
- NETCONF → Global: On
- SSH → Global: On
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing the 'Configuration' section with 'Templates' selected. The main content area is titled 'CONFIGURATION | TEMPLATES' under 'Feature'. A breadcrumb navigation bar indicates the path: Feature Template > Add Template > VPN Interface Ethernet. The 'Basic Configuration' tab is active. Several fields are highlighted with red boxes:

- 'Shutdown' dropdown set to 'No'.
- 'Interface Name' dropdown set to 'ge0/1'.
- 'Description' dropdown.
- 'IPv4' tab selected in the 'IP Version' dropdown.
- 'Static' radio button selected for 'Dynamic/Static' selection.
- 'IPv4 Address' input field containing '[vpn\_if\_ipv4\_address]'.

The bottom right of the configuration window has 'Save' and 'Cancel' buttons. The status bar at the bottom shows the date and time: 6:29 AM 10/15/2020.



The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Cisco vManage' and includes 'Dashboard', 'Monitor', 'Configuration' (which is selected and highlighted in teal), 'Templates' (selected), 'Policies', 'Security', 'Cloud onRamp for SaaS', 'Cloud onRamp', and 'Network Hub'. Below the sidebar is a toolbar with icons for Start, File, Edit, View, Insert, Tools, and Help, along with a search bar and date/time information (6:31 AM, 10/15/2020).

The main content area is titled 'CONFIGURATION | TEMPLATES' under 'Feature'. It shows 'Basic Configuration' and 'Tunnel' tabs, with 'Tunnel' selected and highlighted in red. The URL in the browser bar is '192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN%20Interface%20Ethernet'.

The 'TUNNEL' configuration page contains several sections:

- Tunnel Interface:** A dropdown menu set to 'biz-internet' is highlighted with a red box.
- Color:** A color swatch is highlighted with a red box.
- Restrict:** A dropdown menu with 'On' and 'Off' options is highlighted with a red box.
- Groups:** A dropdown menu is highlighted with a red box.
- Border:** A dropdown menu with 'On' and 'Off' options is highlighted with a red box.

At the bottom right of the configuration page are 'Save' and 'Cancel' buttons.



The screenshot shows the Cisco vManage web interface. The left sidebar has a 'Configuration' section with 'Templates' selected. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows a table of templates under the 'Feature' tab. One template, 'BR-VE-... BR-VE-VPNINT-VPN0-G1', is highlighted with a red border.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated
BR-VE...	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	admini ...
BR-VE...	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	0	0	admini ...
VE-Ba...	VE-Banner	Banner	vEdge Cloud	0	0	admini ...
CE-Sys...	CE-System	WAN Edge System	CSR1000v	0	0	admini ...
CE-Ba...	CE-Banner	Banner	CSR1000v	0	0	admini ...
VE-Sys...	VE-System	WAN Edge System	vEdge Cloud	0	0	admini ...
BR-VE...	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	0	0	admini ...
BR-VE...	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	0	0	admini ...

## Task 5 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - o Template Name: BR-VE-VPNINT-VPN512-Eth0
  - o Description: BR-VE-VPNINT-VPN512-Eth02
- Basic Configuration
  - o Shutdown -> Global: No
  - o Interface Name -> Global: Eth0
  - o IPv4 Address -> Dynamic
- Click Save to save the Template





Screenshot of Cisco vManage interface showing the configuration of a Feature Template (VPN Interface Ethernet). The template is named "BR-VE-VPNINT-VPN512-Eth0". The "Basic Configuration" tab is selected.

**Device Type:** vEdge Cloud

**Template Name:** BR-VE-VPNINT-VPN512-Eth0

**Description:** BR-VE-VPNINT-VPN512-Eth0

**Basic Configuration:**

- Shutdown:** Yes (radio button)
- Interface Name:** eth0
- Description:** (checkbox checked)

Buttons at the bottom: Update, Cancel

Bottom status bar: Start, Task View, File Explorer, Google Chrome, 4:31 PM, 10/15/2020



Screenshot of the Cisco vManage web interface showing the configuration of a Feature Template for a VPN Interface Ethernet.

The left sidebar shows the navigation menu under Configuration, with Templates selected. The main content area displays the "CONFIGURATION | TEMPLATES" screen for "Feature".

The "Basic Configuration" tab is active. Under "Description", there is a dropdown menu with "IPv4" highlighted by a red box. Below it, the "Dynamic" radio button is selected, also highlighted by a red box.

Other tabs include Tunnel, NAT, VRRP, ACL/QoS, ARP, 802.1X, and Advanced.

At the bottom right of the configuration window are "Save" and "Cancel" buttons.

The browser address bar shows the URL: 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN%20Interface%20Ethernet

The taskbar at the bottom shows the Windows Start button, File Explorer, Task View, and Google Chrome icons. The system tray indicates the date and time as 6:43 AM, 10/15/2020.

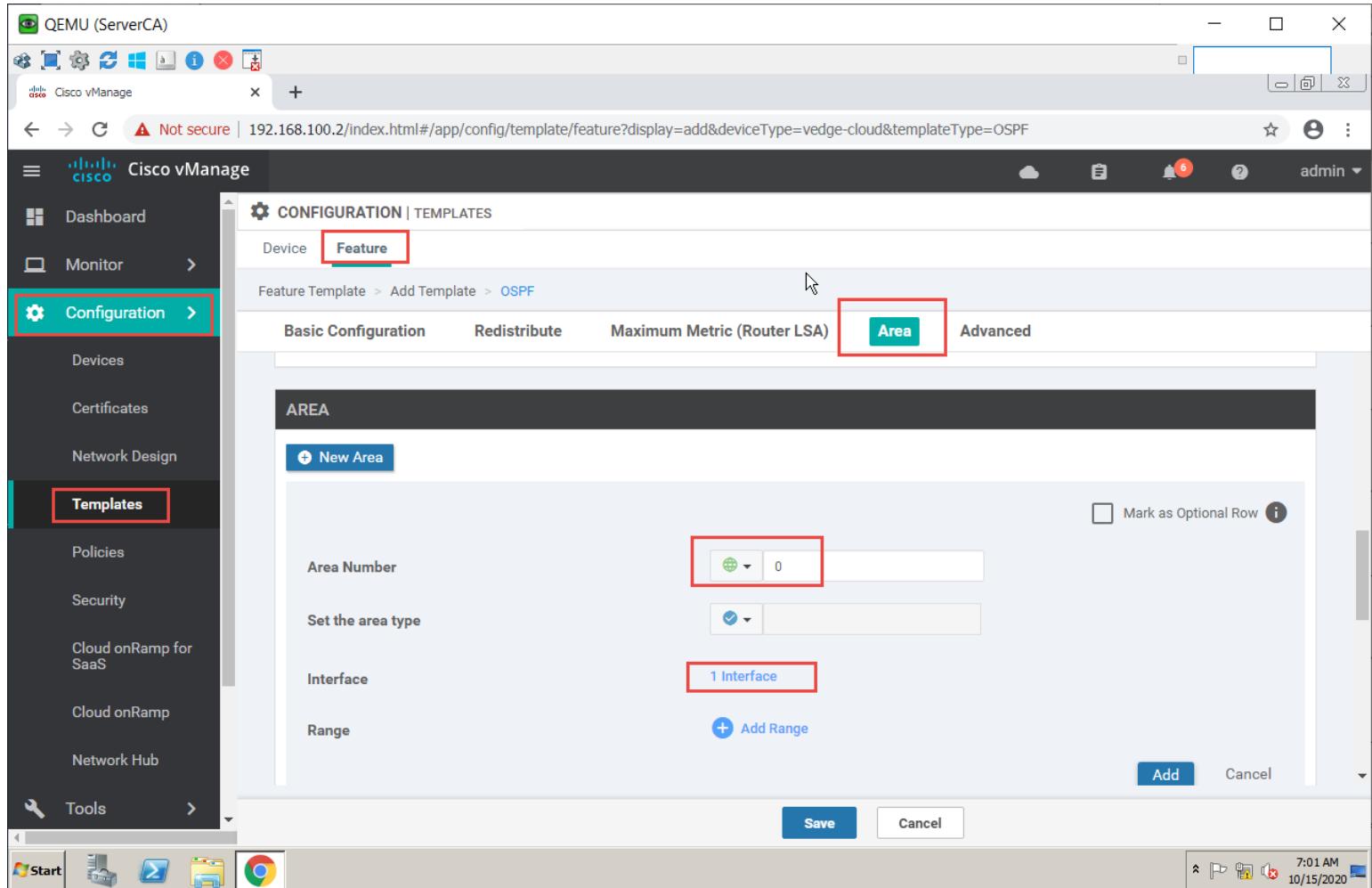


## Lab 16 - Configuring Feature Templates –External Routing - OSPF for VPN 0 –Branch Site (vEdges)

Task 1 – Configure a OSPF Template to be used by all Branch vEdgeCloud Devices for VPN 0

- In vManage, **Navigate to Configuration → Templates → Feature → vEdge Cloud → Other Templates → OSPF**
- Configure the OSPF parameters based on the following:
  - o Template Name: BR-VE-OSPF-VPNO
  - o Description: BR-VE-OSPF-VPNO
- Area Configuration
  - o Area Number → Global: 0
  - o Area Type → Default
- Interface Configuration
  - o Interface Name: Ge0/0
- Advanced
  - o OSPF Network Type: Point-to-Point
- Click Add to add the Interface and Click Add to add OSPF.
- Click Save to save the Template.





The screenshot shows the Cisco vManage web interface for configuring OSPF areas. The left sidebar is titled 'Cisco vManage' and includes sections for Dashboard, Monitor, Configuration (which is selected and highlighted in red), Templates (also highlighted in red), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The top navigation bar shows the URL '192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=OSPF'. The main content area is titled 'CONFIGURATION | TEMPLATES' under 'Feature'. It shows tabs for Basic Configuration, Redistribute, Maximum Metric (Router LSA), and Area (which is selected and highlighted in red). Below these tabs is a section titled 'AREA' with a 'New Area' button. The configuration fields include 'Area Number' (set to 0), 'Set the area type' (checkbox checked), 'Interface' (set to 1 Interface), and 'Range' (button for 'Add Range'). At the bottom right of the configuration form are 'Save' and 'Cancel' buttons.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/template/feature

Cisco vManage

Dashboard

Monitor

Configuration

Devices

Certificates

Network Design

**Templates**

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type Non-Default

Search Options

Total Rows: 10

Name	Description	Type	Device Model	Device Templates	Devices Attached	Actions
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	0	0	...
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	...
<b>BR-VE-OSPF-VPN0</b>	<b>BR-VE-OSPF-VPN0</b>	<b>OSPF</b>	<b>vEdge Cloud</b>	<b>0</b>	<b>0</b>	<b>...</b>
VE-System	VE-System	WAN Edge System	vEdge Cloud	0	0	...
BR-VE-VPNINT-VPN512-G2	BR-VE-VPNINT-VPN512-G2	WAN Edge Interface	vEdge Cloud	0	0	...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	0	0	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	0	0	...

Start

7:03 AM  
10/15/2020

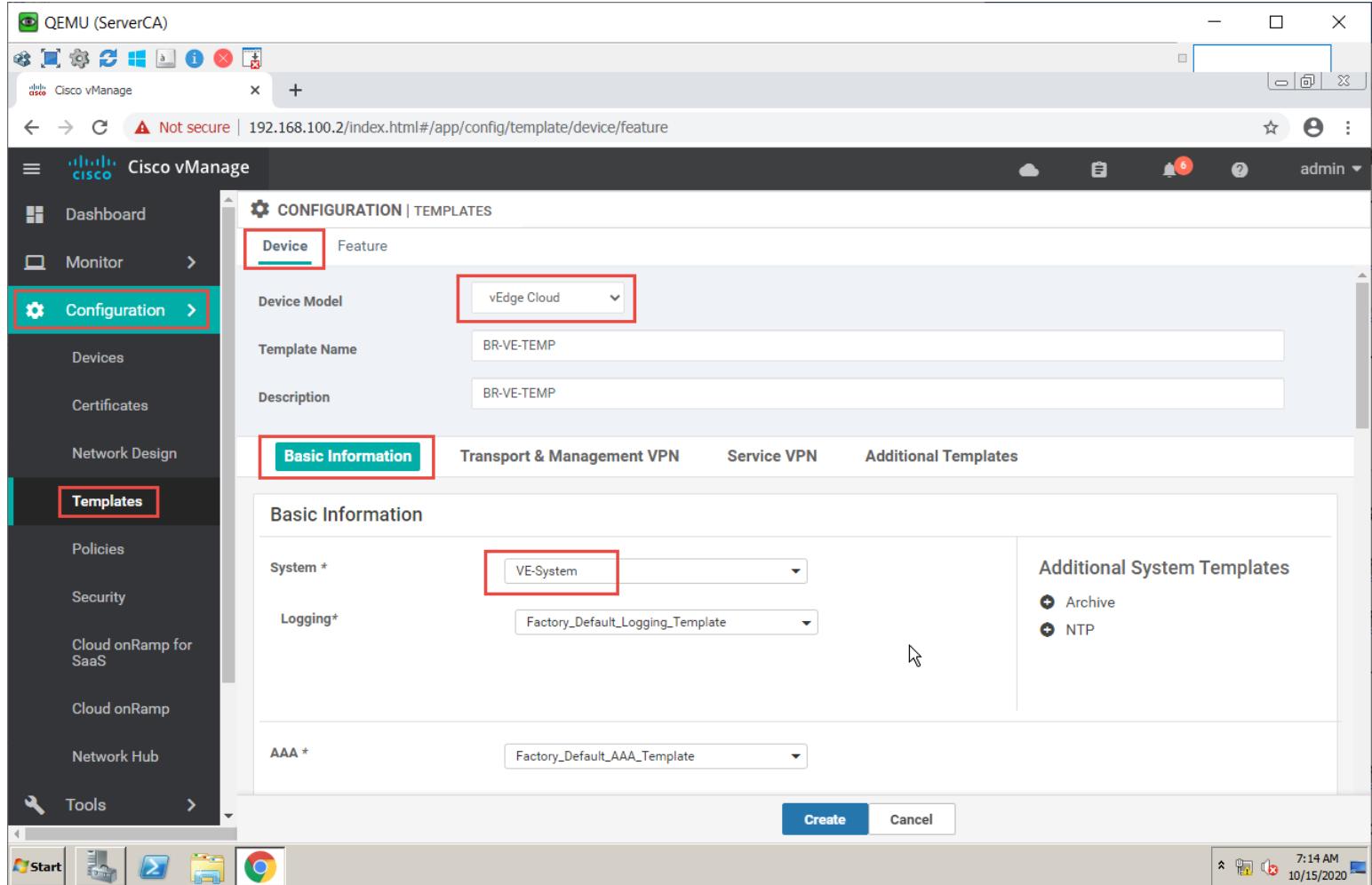


## Lab 17 - Configuring and Deploying Device Templates for vEdge – Branch Site(vEdge2)

### Task 1 – Configure a Device Template for Branch vEdge Devices.

- In vManage, Navigate to Configuration → Templates → Device → Create Template → vEdge Cloud
- Configure the Device Template based on the following:
  - o Template Name: BR-VE-TEMP
  - o Description: BR-VE-TEMP
- Basic Information
  - o System → VE-System
- Transport & Management
  - o VPN 0: BR-VE-VPN-VPNO
  - o VPN Interface: BR-VE-VPNINT-VPNO-G0
  - o VPN Interface: BR-VE-VPNINT-VPNO-G1
  - o OSPF: BR-VE-OSPF-VPNO
  - o VPN 512: BR-VE-VPN-VPN512
  - o VPN Interface: BR-VE-VPNINT-VPN512-Eth0
- Click Create to save the Template.





The screenshot shows the Cisco vManage web interface. The left sidebar is titled "Cisco vManage" and includes sections for Dashboard, Monitor, Configuration (which is selected and highlighted in red), Templates (also highlighted in red), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area is titled "CONFIGURATION | TEMPLATES" and has tabs for Device (selected) and Feature. Under Device, the "Device Model" dropdown is set to "vEdge Cloud". The "Template Name" is "BR-VE-TEMP" and the "Description" is also "BR-VE-TEMP". Below these fields are three tabs: "Basic Information" (selected and highlighted in red), "Transport & Management VPN", "Service VPN", and "Additional Templates". The "Basic Information" tab contains fields for "System \*", "Logging \*", and "AAA \*". The "System \*" dropdown is set to "VE-System" (highlighted in red). The "Logging \*" dropdown is set to "Factory\_Default\_Logging\_Template". The "AAA \*" dropdown is set to "Factory\_Default\_AAA\_Template". On the right side of the "Basic Information" section, there is a panel titled "Additional System Templates" with options for "Archive" and "NTP". At the bottom of the configuration dialog are "Create" and "Cancel" buttons.

Screenshot of Cisco vManage interface showing Configuration | Templates > Transport & Management VPN.

The Transport & Management VPN tab is selected. The configuration details are as follows:

Category	Value	Additional Options
VPN 0 *	BR-VE-VPN-VPN0	
OSPF	BR-VE-OSPF-VPN0	
VPN Interface	BR-VE-VPNINT-VPN0-G0	
VPN Interface	BR-VE-VPNINT-VPN0-G1	
VPN 512 *	BR-VE-VPN-VPN512	
VPN Interface	BR-VE-VPNINT-VPN512-G2	
VPN Interface	BR-VE-VPNINT-VPN512-Eth0	

Buttons at the bottom: Update, Cancel.

Right sidebar: Additional VPN 0 Templates (BGP, OSPF, VPN Interface, VPN Interface GRE, VPN Interface IPsec, VPN Interface PPP) and Additional VPN 512 Templates (VPN Interface).

Bottom status bar: Start button, taskbar icons, system tray with date/time (8:31 AM, 10/15/2020).

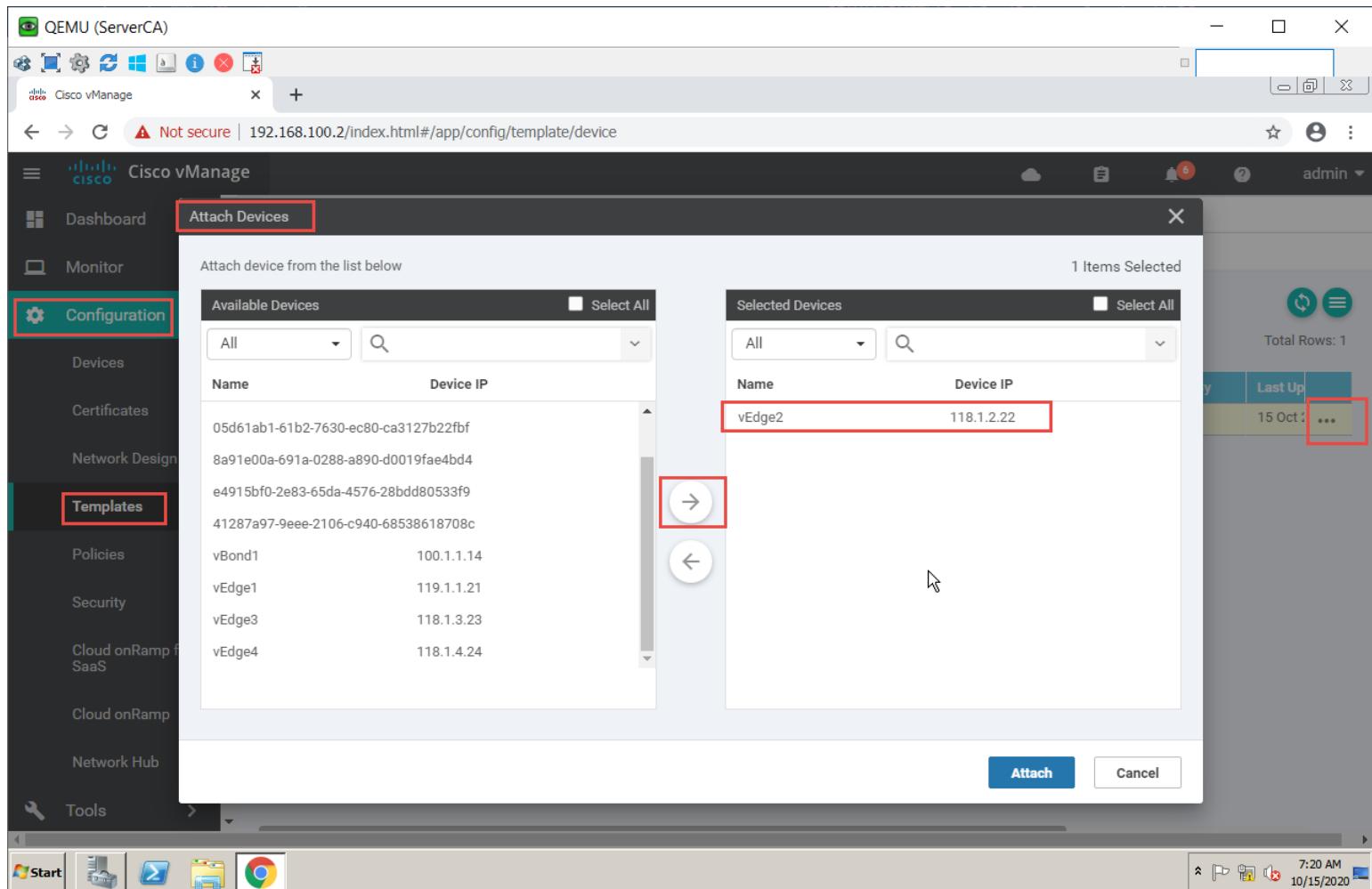


The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Cisco vManage' and includes sections for Dashboard, Monitor, Configuration (which is selected and highlighted with a red box), Templates (also highlighted with a red box), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. Below the sidebar is a toolbar with icons for Start, Task View, File Explorer, and Google Chrome. The main content area is titled 'CONFIGURATION | TEMPLATES' and has tabs for 'Device' (highlighted with a red box) and 'Feature'. A sub-header 'Create Template' with a plus sign is visible. A search bar and search options are at the top of the list table. The table has columns: Name, Description, Type, Device Model, Feature Templates, Devices Attached, Updated By, and Last Up. One row is highlighted with a red box: BR-VE-TEMP, BR-VE-TEMP, Feature, vEdge Cloud, 12, 0, admin, 15 Oct. The bottom right corner of the table row contains three dots (...). The status bar at the bottom right shows the date and time: 7:18 AM 10/15/2020.

## Task 2 – Attach vEdge2 to the Device Template

- In vManage, **Navigate to Configuration → Templates → Device → BRVE-TEMP.**
- Click on “...” towards the right-hand side.
- Click Attach Devices.
- Select vEdge2 and click the “→” button.
- Click Attach.

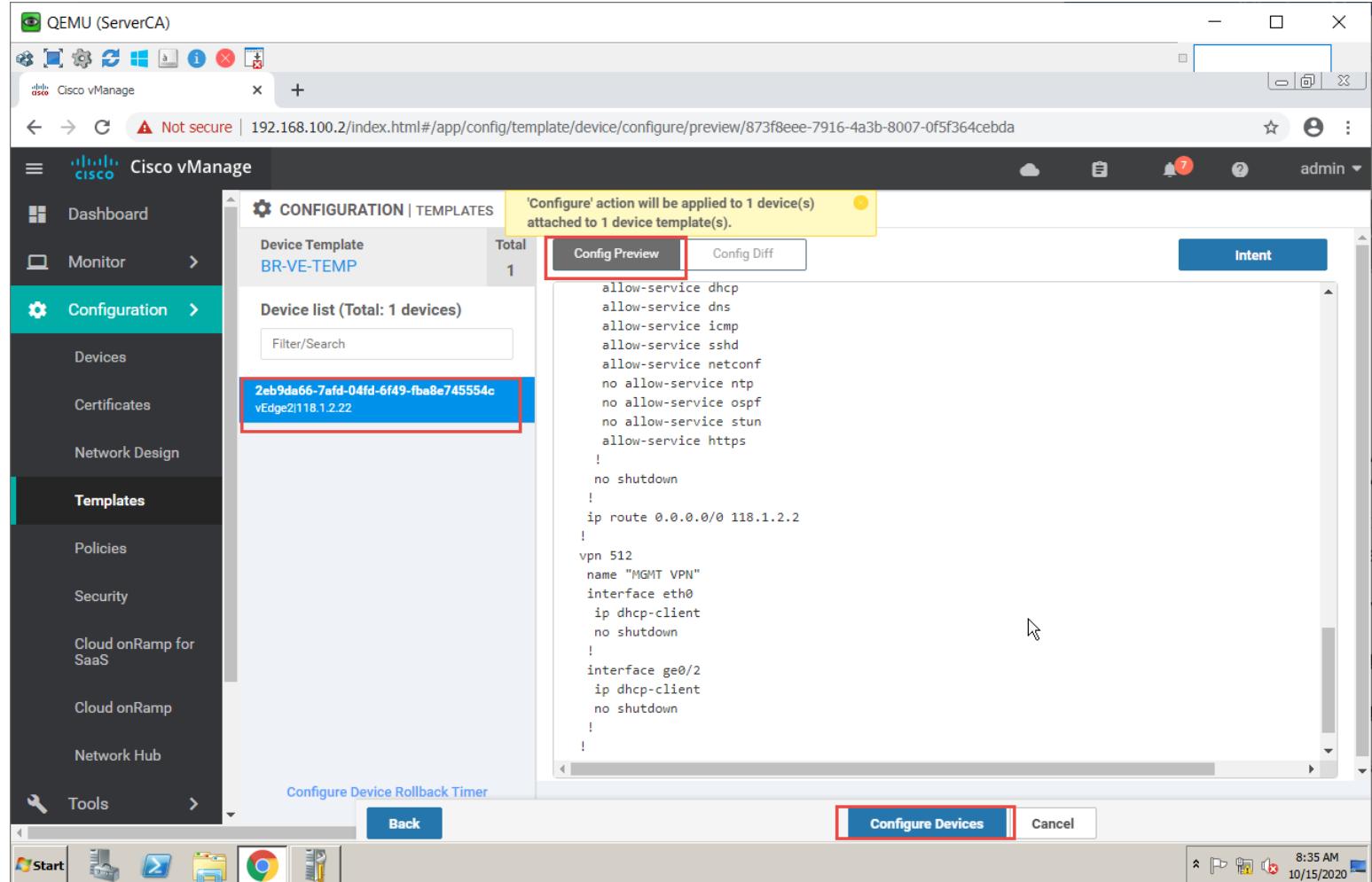




### Task 3 – Configure the Variable Parameters for the Feature Templates

- vEdge2 will appear in the window.
- Click on “...” towards the right-hand side.
- Click Edit Device Template.
- Configure the variables based on the following:
  - o Default Gateway for VPNO: 118.1.2.2
  - o Interface IP for Ge0/1: 118.1.2.1/24
  - o Interface IP for Ge0/0: 10.1.12.1/24
  - o Hostname: vEdge-2
  - o System IP: 118.1.2.22
  - o Site ID: 2
- Click Update.
- Verify the Configuration & Click Configure Devices.
- Wait for it to update the device. It should come back with Status of Success.
- Verify the configuration on vEdge2. You can do that by verify OSPF Neighbor relationship with the MPLS Router by issuing the Show ospf neighbor command on vEdge2.

- Type Show Ip route on vEdge2 to verify that you are receiving OSPF routes from the MPLS Router.



The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Configuration' and has a 'Templates' section selected. In the main content area, the 'CONFIGURATION | TEMPLATES' tab is active, showing a device template named 'BR-VE-TEMP' with a total of 1 device. A device named '2eb9da66-7af0-04fd-6f49-fba8e745554c vEdge2|118.1.2.22' is selected and highlighted with a red box. A yellow banner at the top right states: "'Configure' action will be applied to 1 device(s) attached to 1 device template(s.)". Below the banner, there are two tabs: 'Config Preview' (which is highlighted with a red box) and 'Config Diff'. The 'Config Preview' tab displays the configuration script:

```
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
no shutdown
!
ip route 0.0.0.0/0 118.1.2.2
!
vpn 512
name "MGMT VPN"
interface eth0
ip dhcp-client
no shutdown
!
interface ge0/2
ip dhcp-client
no shutdown
!
```

At the bottom right of the configuration preview window, there are 'Configure Devices' and 'Cancel' buttons, with 'Configure Devices' also highlighted with a red box. The status bar at the bottom right shows the date and time: '8:35 AM 10/15/2020'.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/device/status?activity=push\_file\_template\_configuration&pid=push\_feature\_template\_configuration-2afca0fe-8b3b...

Cisco vManage

Dashboard

Monitor

Configuration

Devices

Certificates

Network Design

Templates

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

TASK VIEW

Push Feature Template Configuration | Validation Success

Total Task: 1 | Success : 1

Initiated By: admin From: 169.254.0.253

Search Options

Search

Status Message Chassis Number Device Model Hostname System IP Site ID vManage IP

Success Done - Push Fea... 2eb9da66-7afd-04fd... vEdge Cloud vEdge2 118.1.2.22 2 100.1.1.12

[15-Oct-2020 4:35:48 AST] Configuring device with feature template: BR-VE-TEMP  
[15-Oct-2020 4:35:48 AST] Generating configuration from template  
[15-Oct-2020 4:35:50 AST] Checking and creating device in vManage  
[15-Oct-2020 4:35:51 AST] Device is online  
[15-Oct-2020 4:35:51 AST] Updating device configuration in vManage  
[15-Oct-2020 4:35:52 AST] Pushing configuration to device  
[15-Oct-2020 4:36:03 AST] Template successfully attached to device

8:37 AM 10/15/2020

The screenshot shows the Cisco vManage interface with a task log for pushing a feature template configuration. The task was initiated by 'admin' from '169.254.0.253'. The log details the process of generating configuration from a template, checking and creating the device in vManage, updating the device configuration, and finally pushing the configuration to the device. The task status is 'Success'.





vEdge2

```
usergroup operator
task system read
task interface read
task policy read
task routing read
task security read
!
user admin
password $6$siwKBQ==$wT2lUa9BSreDPI6gB8s14E6PAJoVXgMbqv/whJ8F1C6sWdRazdxorYYTLrL6syiG6qnLABTnrE96HJiKF6QRql
!
!
logging
disk
enable
!
!
!
!
omp
no shutdown
graceful-restart
advertise connected
advertise static
!
security
ipsec
authentication-type sha1-hmac ah-sha1-hmac
!
!
vpn 0
name "Transport VPN"
router
ospf
timers spf 200 1000 10000
area 0
interface ge0/0
network point-to-point
exit
exit
!
!
interface ge0/0
ip address 10.1.12.1/24
tunnei-terrace
encapsulation ipsec
color mpls
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
--More--
```





vEdge2

```
ip address 10.1.12.1/24
tunnel-interface
encapsulation ipsec
color mpls
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
Aborted: by user
vEdge2#
vEdge2#
vEdge2# show ospf nei
```

```
vEdge2# show ospf int
ospf interface vpn 0 10.1.12.1/24 0
```

```
if-name          ge0/0
mtu             1500
bandwidth       0
area-addr       0
mtu-mismatch   true
router-id      118.1.2.22
if-type         point-to-point
cost            10
delay           1
ospf-if-state  if-point-to-point
priority        1
members         all
hello-timer     10
dead-interval   40
retransmit-timer 5
neighbor-count  0
adj-neighbor-count 0
hello-due-time  7
oper-state     true
```

```
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
```

```
vEdge2# show ospf nei
```

```
DBsmL -> Database Summary List
RqstL -> Link State Request List
RXmtL -> Link State Retransmission List
```

VPN	IP ADDRESS	INTERFACE	ROUTER ID	STATE	PRIORITY	DEAD			
						TIMER	DBsmL	RqstL	RXmtL
0	10.1.12.2	ge0/0	192.168.105.254	full	1	38	0	0	0

```
vEdge2#
```



## Lab 18 - Configuring Internal Routing Protocols on the Internal Routing Devices – HQ & All Branches

### Interface Configuration

#### Site-1

Interface	IP address	Mask
E 0/0	172.171.1.2	255.255.255.0
Loopback1	192.168.11.1	255.255.255.0
Loopback2	192.168.12.1	255.255.255.0
Loopback3	192.168.13.1	255.255.255.0

#### Site-2

Interface	IP Address	Subnet Mask
E 0/0	172.172.1.2	255.255.255.0
Loopback1	192.168.21.1	255.255.255.0
Loopback2	192.168.22.1	255.255.255.0
Loopback3	192.168.23.1	255.255.255.0
Loopback4	192.168.234.2	255.255.255.255

#### Site-3

Interface	IP Address	Subnet Mask
E 0/0	172.173.1.2	255.255.255.0
Loopback1	192.168.31.1	255.255.255.0
Loopback2	192.168.32.1	255.255.255.0
Loopback3	192.168.33.1	255.255.255.0
Loopback4	192.168.234.3	255.255.255.255

#### Site-4

Interface	IP Address	Subnet Mask
E 0/0	172.174.1.2	255.255.255.0
Loopback1	192.168.41.1	255.255.255.0
Loopback2	192.168.42.1	255.255.255.0
Loopback3	192.168.43.1	255.255.255.0
Loopback4	192.168.234.4	255.255.255.255

#### Site-5

Interface	IP Address	Subnet Mask
E 0/0	172.175.1.2	255.255.255.0
Loopback1	192.168.51.1	255.255.255.0
Loopback2	192.168.52.1	255.255.255.0
Loopback3	192.168.53.1	255.255.255.0



## Task 1 – Internal Site Router Configurations

- Configure the Interfaces based on the Logical Diagram
- Configure OSPF as the IGP to communicate with the vEdge/cEdge devices. Enable all the interfaces under OSPF.
- Configure the Loopback Interfaces as OSPF Network Point-to-point Interfaces.

### Site-1

```
no ip domain-loo
line con 0
logg sync
no exec-timeout
!
Hostname Site-1
!
Interface E 0/0
ip address 172.171.1.2 255.255.255.0
no shut
!
Interface Loopback1
ip address 192.168.11.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback2
ip address 192.168.12.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback3
ip address 192.168.13.1 255.255.255.0
ip ospf network point-to-point
!
router ospf 1
network 172.171.1.0 0.0.0.255 area 0
network 192.168.0.0 0.0.255.255 area 0
```

### Site-2

```
no ip domain-loo
line con 0
logg sync
no exec-timeout
!
Hostname Site-2
!
Interface E 0/0
ip address 172.172.1.2 255.255.255.0
no shut
!
Interface Loopback1
ip address 192.168.21.1 255.255.255.0
```



```
ip ospf network point-to-point
!
Interface Loopback2
ip address 192.168.22.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback3
ip address 192.168.23.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback4
ip address 192.168.234.2 255.255.255.255
ip ospf network point-to-point
!
router ospf 1
network 172.174.1.0 0.0.0.255 area 0
network 192.168.0.0 0.0.255.255 area 0
```

**Site-3**

```
no ip domain-loo
line con 0
logg sync
no exec-timeout
!
Hostname Site-3
!
Interface E 0/0
ip address 172.173.1.2 255.255.255.0
no shut
!
Interface Loopback1
ip address 192.168.31.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback2
ip address 192.168.32.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback3
ip address 192.168.33.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback4
ip address 192.168.234.3 255.255.255.255
ip ospf network point-to-point
!
router ospf 1
network 172.173.1.0 0.0.0.255 area 0
network 192.168.0.0 0.0.255.255 area 0
```

**Site-4**

```
no ip domain-loo
line con 0
logg sync
no exec-timeout
!
Hostname Site-4
!
Interface E 0/0
ip address 172.174.1.2 255.255.255.0
no shut

Interface Loopback1
ip address 192.168.41.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback2
ip address 192.168.42.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback3
ip address 192.168.43.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback4
ip address 192.168.234.4 255.255.255.255
ip ospf network point-to-point
!
router ospf 1
network 172.174.1.0 0.0.0.255 area 0
network 192.168.0.0 0.0.255.255 area 0
```

**Site-5**

```
no ip domain-loo
line con 0
logg sync
no exec-timeout
!
Hostname Site-5
!
Interface E0/0
ip address 172.175.1.2 255.255.255.0
ip ospf network point-to-point
no shut
!
Interface Loopback1
ip address 192.168.51.1 255.255.255.0
```





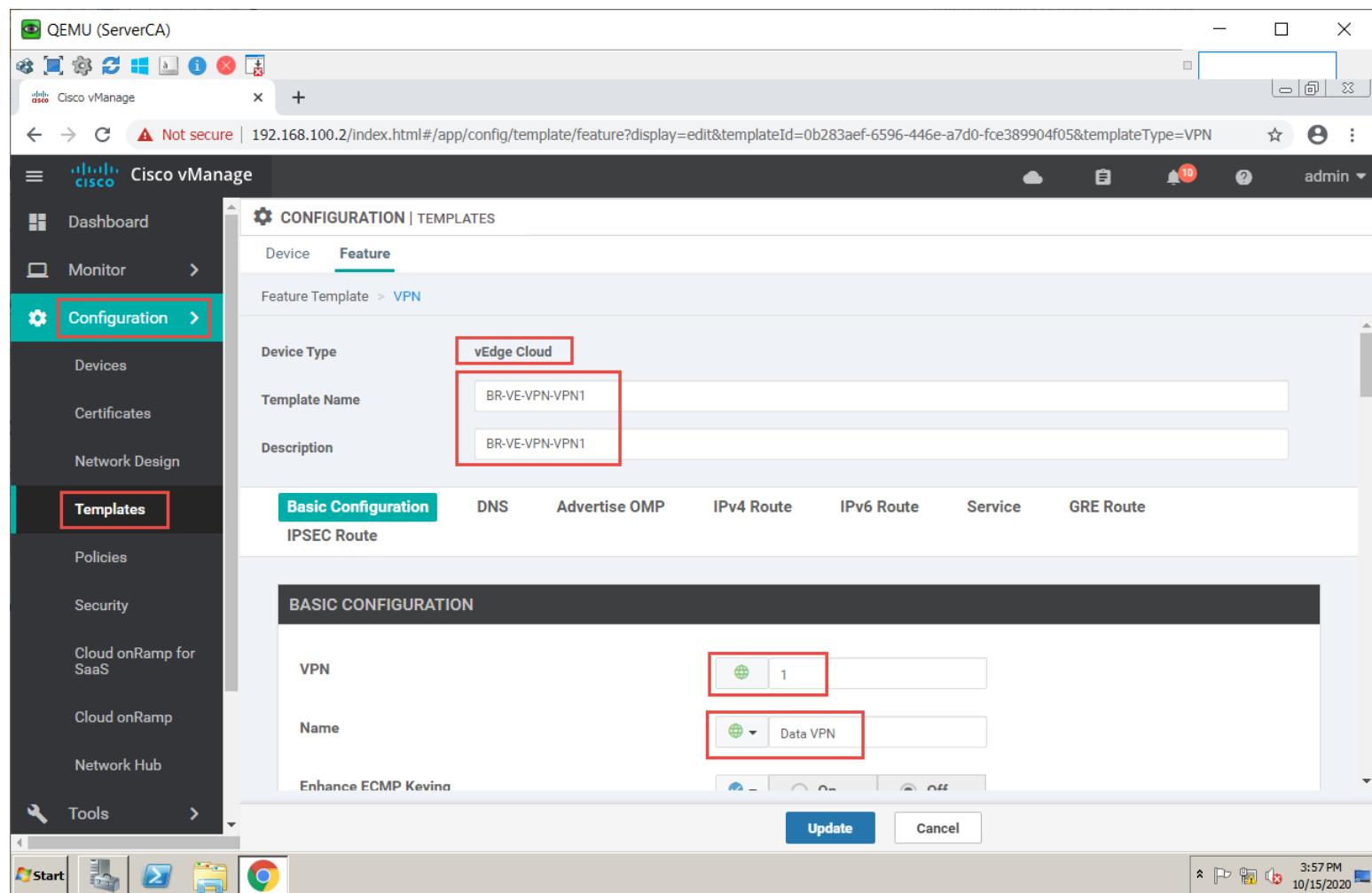
```
ip ospf network point-to-point
!
Interface Loopback2
ip address 192.168.52.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback3
ip address 192.168.53.1 255.255.255.0
ip ospf network point-to-point
!
router ospf 1
network 172.175.1.0 0.0.0.255 area 0
network 192.168.0.0 0.0.255.255 area 0
```



## Lab 19 - Configuring Feature Templates –Service VPN – VPN, VPN Interface and Internal Routing – Branch Site (vEdges)

### Task 1 - Configure a VPN Template to be used by all Branch vEdgeCloud Devices for VPN 1

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN
- Configure the VPN parameters based on the following:
  - o Template Name: BR-VE-VPN-VPN1
  - o Description: BR-VE-VPN-VPN1
- Basic Configuration
  - o VPN → Global: 1
  - o Name → Global: Data VPN
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing the 'Configuration' tab selected (highlighted with a red box). Under 'Templates', the 'VPN' option is also highlighted with a red box. The main content area shows the 'CONFIGURATION | TEMPLATES' screen for 'Feature'. A 'Device Type' dropdown is set to 'vEdge Cloud' (highlighted with a red box). The 'Template Name' field contains 'BR-VE-VPN-VPN1' (highlighted with a red box), and the 'Description' field contains 'BR-VE-VPN-VPN1'. Below this, the 'Basic Configuration' tab is selected (highlighted with a red box), showing the 'VPN' setting (Global: 1) and 'Name' setting (Data VPN, with a dropdown icon highlighted with a red box). At the bottom right are 'Update' and 'Cancel' buttons.



The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Configuration' and has a 'Templates' section selected. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows a table of templates. One template, 'BR-VE-VPN-VPN1', is highlighted with a red border. The table columns are: Name, Description, Type, Device Model, Device Templates, Devices Attached, and Actions (ellipsis). The 'Device Templates' column for 'BR-VE-VPN-VPN1' shows a value of 0, while other rows show values like 1 or 1.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Actions
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	1	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	1	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	0	0	...
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	...
BR-VE-VPNINT-VPN512-...	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	1	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	1	...
VE-System	VE-System	WAN Edge System	vEdge Cloud	1	1	...
BR-VE-VPNINT-VPN512-...	BR-VE-VPNINT-VPN512-G2	WAN Edge Interface	vEdge Cloud	1	1	...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	1	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	1	...

## Task 2 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud devices for VPN 1 for Interface G0/2

- In vManage, **Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN Interface Ethernet**
- Configure the VPN parameters based on the following:
  - o Template Name: BR-VE-VPNINT-VPN1-G2
  - o Description: BR-VE-VPNINT-VPN1-G2
- Basic Configuration
  - o Shutdown → Global: No
  - o Interface Name → Global: Ge0/2
  - o IPv4 Address → Static → Device Specific
- Click Save to save the Template.



Screenshot of Cisco vManage interface showing the configuration of a VPN Interface Ethernet template.

The left sidebar shows the navigation menu with the "Templates" option selected. The main content area shows the "CONFIGURATION | TEMPLATES" screen under the "Feature" tab. A red box highlights the "VPN Interface Ethernet" link in the breadcrumb trail.

The configuration details are as follows:

- Device Type:** vEdge Cloud (highlighted by a red box)
- Template Name:** BR-VE-VPNINT-VPN1-G2 (highlighted by a red box)
- Description:** BR-VE-VPNINT-VPN1-G2

The "Basic Configuration" tab is selected. The configuration fields are:

- Shutdown:** No (highlighted by a red box)
- Interface Name:** ge0/2 (highlighted by a red box)
- Description:** (empty)

At the bottom right of the configuration window are the "Save" and "Cancel" buttons.

The bottom of the screen shows the Windows taskbar with icons for Start, File Explorer, Task View, and Google Chrome, along with system status indicators.



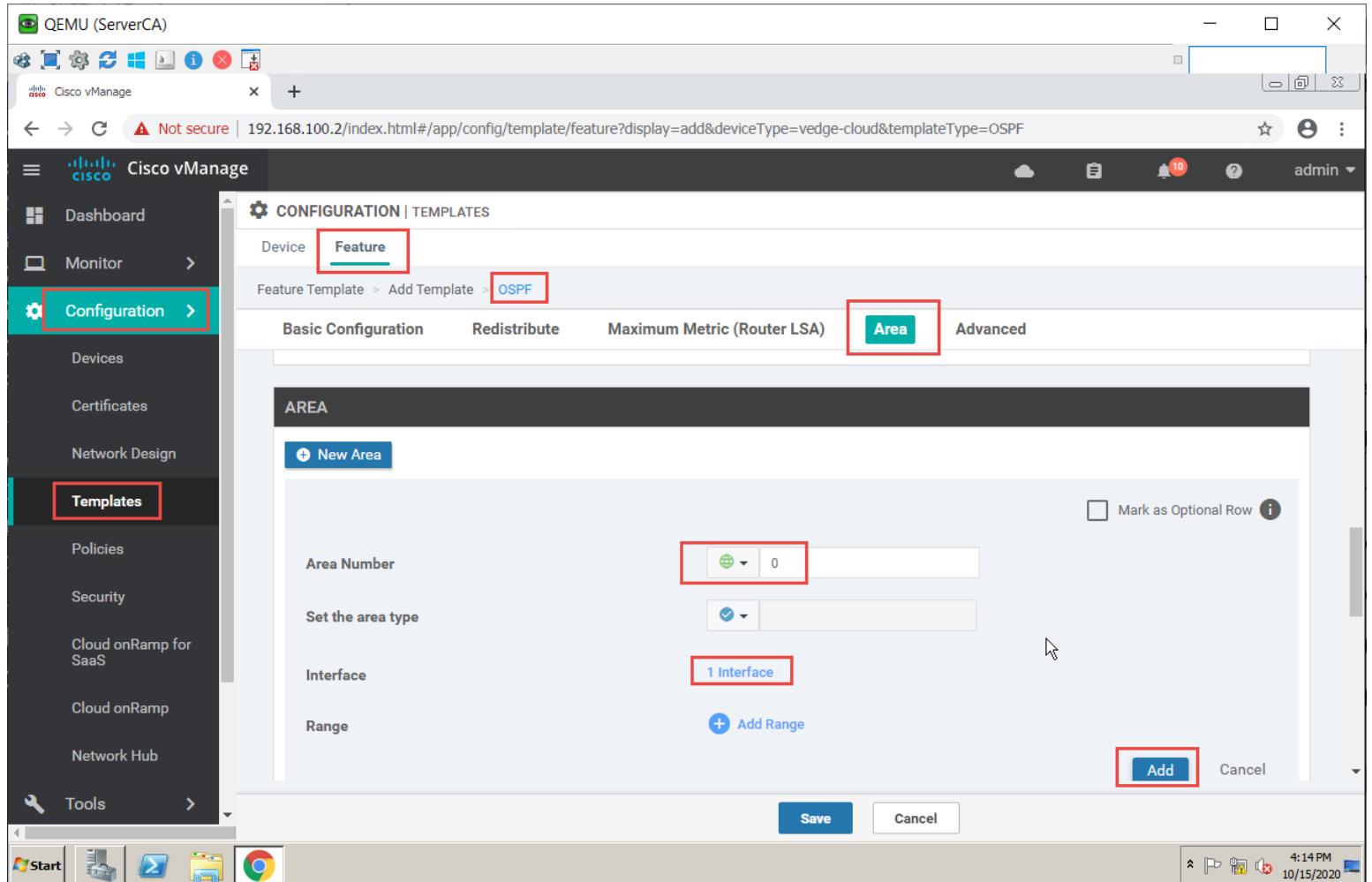
Name	Description	Type↑	Device Model	Device Templates	Devices Attached	⋮
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	1	...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	...
VE-System	VE-System	WAN Edge System	vEdge Cloud	1	1	...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	1	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	0	0	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	1	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	1	...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	0	0	...
BR-VE-VPNINT-VPN512-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	1	...
BR-VE-VPNINT-VPN512-G2	BR-VE-VPNINT-VPN512-G2	WAN Edge Interface	vEdge Cloud	1	1	...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	1	...

### Task 3 – Configure a OSPF Template to be used by all Branch vEdgeCloud Devices for VPN

1

- In vManage, **Navigate to Configuration → Templates → Feature → vEdge Cloud → Other Templates → OSPF**
- Configure the OSPF parameters based on the following:
  - o Template Name: BR-VE-OSPF-VPN1
  - o Description: BR-VE-OSPF-VPN1
- **Redistribution**
  - o Protocol: OMP
- **Area Configuration**
  - o Area Number → Global : 0
  - o Area Type → Default
- **Interface Configuration**
  - o Interface Name: Ge0/2
- Click Add to add the Interface and Click Add to add OSPF.
- Click Save to save the Template.





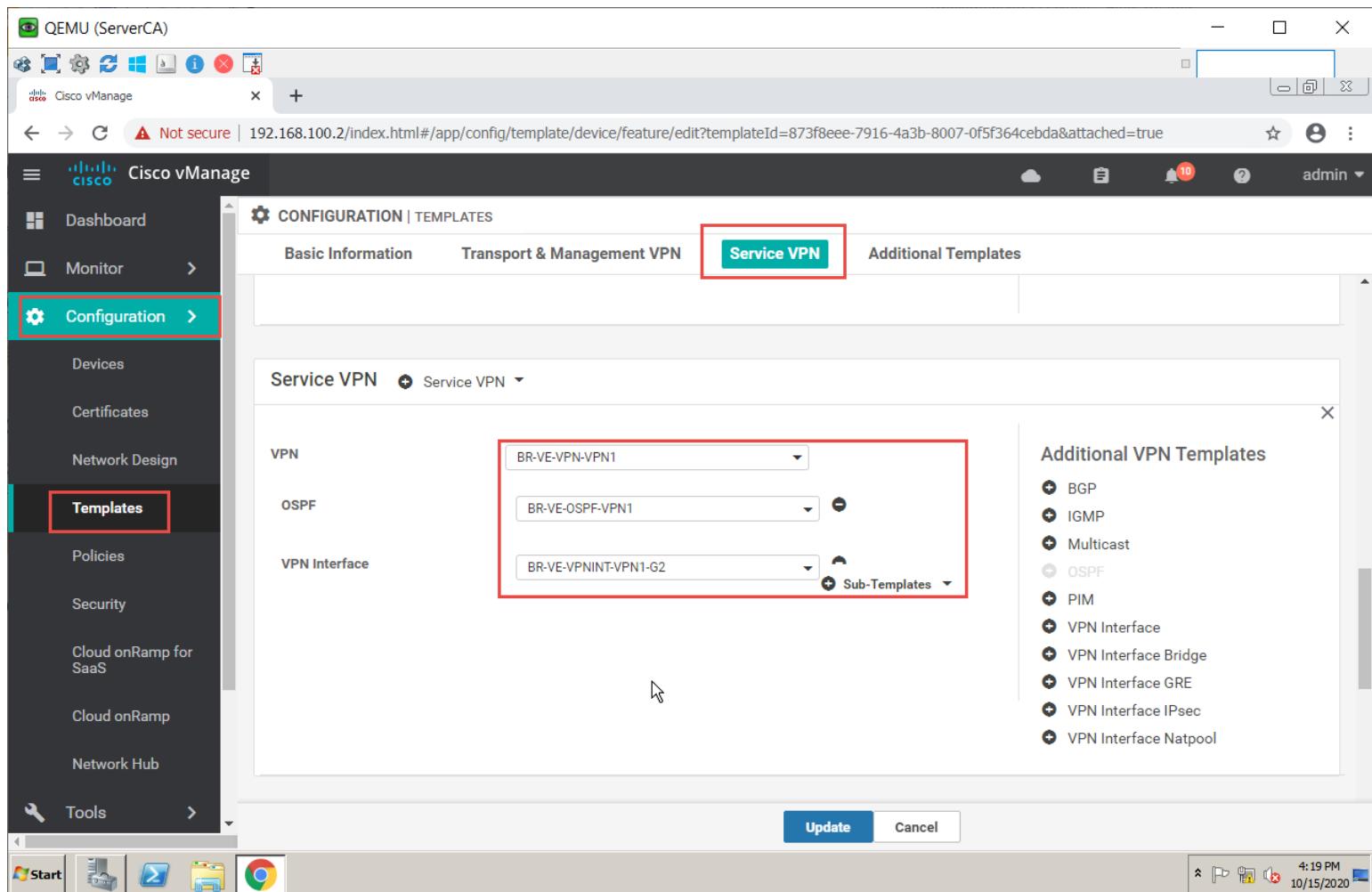
The screenshot shows the Cisco vManage web interface for managing network templates. The left sidebar is titled 'QEMU (ServerCA)' and contains navigation links for Dashboard, Monitor, Configuration (which is selected and highlighted in teal), Templates (also highlighted in red), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. Below the sidebar is a Windows taskbar with icons for Start, File Explorer, Task View, and Google Chrome.

The main content area has a title 'CONFIGURATION | TEMPLATES' and a breadcrumb path 'Feature Template > Add Template > OSPF'. The 'Feature' tab is selected. The 'Area' tab is also highlighted with a red box. The configuration page is titled 'AREA' and includes fields for 'Area Number' (set to 0), 'Set the area type' (checkbox checked), 'Interface' (set to 1 Interface), and 'Range' (button to 'Add Range'). At the bottom right are 'Save' and 'Cancel' buttons, and a large red box highlights the 'Add' button.

## Lab 20 - Implementing a Service VPN using Templates – Branch Site (vEdge2)

### Task 1 – Edit the BR-VE-TEMP Device Template for Branch vEdge Devices.

- In vManage, **Navigate to Configuration → Templates → Device → BRVE-TEMP → “...” → Edit**
- Edit the BR-VE-TEMP Device Template based on the following:
  - Service VPN
    - VPN 1: BR-VE-VPN-VPN1
    - VPN Interface: BR-VE-VPNINT-VPN1-G2
    - OSPF: BR-VE-OSPF-VPN1
- Click Save to save the Template



The screenshot shows the Cisco vManage web interface. The left sidebar is expanded, showing the 'Configuration' section with 'Templates' selected. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows the 'Service VPN' tab selected. Under the 'Service VPN' section, there are three dropdown menus: 'VPN' (set to 'BR-VE-VPN-VPN1'), 'OSPF' (set to 'BR-VE-OSPF-VPN1'), and 'VPN Interface' (set to 'BR-VE-VPNINT-VPN1-G2'). To the right, a sidebar titled 'Additional VPN Templates' lists various options like BGP, IGMP, Multicast, OSPF, PIM, and different types of VPN interfaces, each preceded by a plus sign. At the bottom of the configuration window are 'Update' and 'Cancel' buttons. The browser address bar shows the URL: 192.168.100.2/index.html#/app/config/template/device/feature/edit?templateId=873f8eee-7916-4a3b-8007-0f5f364cebda&attached=true.

### Task 2 – Configure the Variable Parameters for the Feature Templates

- vEdge2 will appear in the window.
- Click on “...” towards the right-hand side & click Edit Device Template.
- Configure the variables based on the following:



- Interface IP for Ge0/2: 172.172.1.1/24
- Click Update.
- Verify the Configuration & Click Configure Devices.
- Wait for it to update the device. It should come back with Status of Success.
- Verify the configuration on vEdge2. You can do that by verify OSPF Neighbor relationship with the Site-2 Router by issuing the Show ospf neighbor command on vEdge2.
- Type Show Ip route on vEdge2 to verify that you are receiving OSPF routes from the Internal Site Router.

The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing various management options like Dashboard, Monitor, Configuration, Templates, Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. The 'Configuration' section is currently selected. In the center, there's a modal dialog titled 'Update Device Template'. This dialog contains a 'Variable List' with several fields:

- Chassis Number: 2eb9da66-7af0-04fd-6f49-fba8e745554c
- System IP: 118.1.2.22
- Hostname: vEdge2
- Address(vpn\_next\_hop\_ip\_address\_0): 118.1.2.2
- IPv4 Address(vpn\_if\_ipv4\_address): 118.1.2.1/24
- IPv4 Address(vpn\_if\_ipv4\_address): 10.1.12.1/24
- Hostname(system\_host\_name): vEdge2
- System IP(system\_system\_ip): 118.1.2.22
- Site ID(system\_site\_id): 2
- IPv4 Address(vpn\_if\_ipv4\_address): 172.172.1.1/24

The 'IPv4 Address(vpn\_if\_ipv4\_address)' field at the bottom is highlighted with a red border. At the bottom right of the dialog are 'Update' and 'Cancel' buttons. The background shows a table with one row of data, and the status bar at the bottom right indicates the date and time: 4:24 PM 10/15/2020.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/template/device/configure/preview/873f8eee-7916-4a3b-8007-0f5f364cebda

Cisco vManage

Dashboard

Monitor

Configuration

Devices

Certificates

Network Design

Templates

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

CONFIGURATION | TEMPLATES

Device Template BR-VE-TEMP Total 1

Device list (Total: 1 devices)

Filter/Search

2eb9da66-7af0-04fd-6f49-fbe8e745554c vEdge2|118.1.2.22

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

Config Preview Config Diff Intent

```
allow-service netcom  
no allow-service ntp  
no allow-service ospf  
no allow-service stun  
allow-service https  
!  
no shutdown  
!  
ip route 0.0.0.0/0 118.1.2.2  
  
vpn 1  
name "Data VPN"  
router  
ospf  
timers spf 200 1000 10000  
redistribute ospf  
!  
!  
interface ge0/2  
ip address 172.172.1.1/24  
no shutdown  
  
!  
vpn 512  
name "MGMT VPN"  
router ospf 512
```

Configure Device Rollback Timer

Back Configure Devices Cancel

4:25 PM 10/15/2020

vEdge2# show ospf nei

DBsmL -> Database Summary List

RqstL -> Link State Request List

RXmtL -> Link State Retransmission List

VPN	IP ADDRESS	INTERFACE	ROUTER ID	STATE	PRIORITY	DEAD			
						DBsmL	RqstL	RXmtL	
0	10.1.12.2	ge0/0	192.168.105.254	full	1	30	0	0	0
1	172.172.1.2	ge0/2	172.16.234.2	full	1	32	0	0	0

vEdge2#



## Lab 21 - Pushing Template to configure other Branch Sites -- Branch Site(vEdge3 & vEdge4)

### Task 1 – Attach the BR-VE-TEMP Device Template for Branch vEdge Devices

- In vManage, Navigate to Configuration → Templates → Device → BRVE-TEMP → “...” → Attach Devices.
- Click Attach Devices.
- Select vEdge3 & vEdge4 and click the “→” button.
- Click Attach.
- vEdge3 & vEdge4 will appear in the window.
- Click on “...” towards the right-hand side for both devices, one at a time click Edit Device Template.
- Configure the variables based on the following:
  - vEdge-3
    - Interface IP for ge0/2: 172.173.1.1/24
    - Default Gateway for VPNO: 118.1.3.2
    - Interface IP for ge0/1: 118.1.3.1/24
    - Interface IP for ge0/0: 10.1.13.1/24
    - Hostname: vEdge-3
    - System IP: 118.1.3.23
    - Site ID: 3
  - Click Update.
  - vEdge-4
    - Interface IP for ge0/2: 172.174.1.1/24
    - Default Gateway for VPNO: 118.1.4.2
    - Interface IP for ge0/1: 118.1.4.1/24
    - Interface IP for ge0/0: 10.1.14.1/24
    - Hostname: vEdge-4
    - System IP: 118.1.4.24
    - Site ID: 4
  - Click Update.
  - Verify the Configuration & Click Configure Devices.
  - Wait for it to update the device. It should come back with Status of Success.
  - Verify the configuration on vEdge3 & vEdge4. You can do that by verify OSPF Neighbor relationship with the Internal Site Router by issuing the Show ospf neighbor command on the vEdges.
  - Type Show Ip route on Internal Site Routers to verify that you are receiving OSPF routes from the other Sites.
  - Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks.



Screenshot of Cisco vManage interface showing the "Attach Devices" dialog.

The left sidebar shows the navigation menu with "Configuration" and "Templates" highlighted.

The "Available Devices" list contains several device entries:

Name	Device IP
41287a97-9eee-2106-c940-68538618708c	
e4915bf0-2e83-65da-4576-28bdd80533f9	
8a91e00a-691a-0288-a890-d0019fae4bd4	
05d61ab1-61b2-7630-ec80-ca3127b22fbf	
6c4ac09a-d3b3-625b-6040-6f5e8505617a	
131e1368-7fd-d545-0cbc-5a4d82924d94	
vBond1	100.1.1.14
vEdge1	119.1.1.21

The "Selected Devices" list contains two devices selected (highlighted with a red box):

Name	Device IP
vEdge3	118.1.3.23
vEdge4	118.1.4.24

Buttons at the bottom right of the dialog are "Attach" and "Cancel".

The status bar at the bottom shows the Windows taskbar with icons for Start, File Explorer, Task View, and Google Chrome, along with system information: 4:54 PM, 10/15/2020.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/device/status?activity=push\_file\_template\_configuration&pid=push\_feature\_template\_configuration-7eda7bee-53ba...

TASK VIEW

Push Feature Template Configuration | Validation Success

Initiated By: admin From: 169.254.0.253

Total Task: 2 | Success : 2

Search Options

Total Rows: 2

	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
▼	Success	Done - Push Fea...	d6d98a35-f70c-9955...	vEdge Cloud	vEdge3	118.1.3.23	3	100.1.1.12
▼	Success	Done - Push Fea...	aa5c2054-6e37-ca2...	vEdge Cloud	vEdge4	118.1.4.24	4	100.1.1.12

[15-Oct-2020 13:00:32 AST] Configuring device with feature template: BR-VE-TEMP  
[15-Oct-2020 13:00:32 AST] Generating configuration from template  
[15-Oct-2020 13:00:35 AST] Checking and creating device in vManage  
[15-Oct-2020 13:00:37 AST] Device is online  
[15-Oct-2020 13:00:37 AST] Updating device configuration in vManage  
[15-Oct-2020 13:00:39 AST] Pushing configuration to device  
[15-Oct-2020 13:00:52 AST] Template successfully attached to device

[15-Oct-2020 13:00:32 AST] Configuring device with feature template: BR-VE-TEMP  
[15-Oct-2020 13:00:32 AST] Generating configuration from template  
[15-Oct-2020 13:00:35 AST] Checking and creating device in vManage  
[15-Oct-2020 13:00:37 AST] Device is online  
[15-Oct-2020 13:00:37 AST] Updating device configuration in vManage  
[15-Oct-2020 13:00:39 AST] Pushing configuration to device  
[15-Oct-2020 13:02:43 AST] Template successfully attached to device

Start | File | Edit | View | Favorites | Help | 5:03 PM | 10/15/2020





```
vEdge3
info ID 0
area-id 0
cost 11
path-type intra-area
dest-type network
next-hop 172.173.1.2
if-name ge0/2
ospf routes-table vpn 1 network 192.168.32.0/24
info ID 0
area-id 0
cost 11
path-type intra-area
dest-type network
next-hop 172.173.1.2
if-name ge0/2
ospf routes-table vpn 1 network 192.168.33.0/24
info ID 0
area-id 0
cost 11
path-type intra-area
dest-type network
next-hop 172.173.1.2
if-name ge0/2
ospf routes-table vpn 1 network 192.168.234.3/32
Info ID 0
area-id 0
cost 11
path-type intra-area
dest-type network
next-hop 172.173.1.2
if-name ge0/2
vEdge3# show ospf nei
DBsmL -> Database Summary List
RgstL -> Link State Request List
RXmtL -> Link State Retransmission List
      SOURCE
VPN   IP ADDRESS     INTERFACE    ROUTER ID      STATE      PRIORITY      DEAD
1     172.173.1.2    ge0/2       172.16.234.3  full       1           37          0           0           0
vEdge3# ping 192.168.234.3 vpn 1
PING in VEN 1
PING 192.168.234.3 (192.168.234.3) 56(84) bytes of data.
64 bytes from 192.168.234.3: icmp_seq=1 ttl=255 time=0.905 ms
64 bytes from 192.168.234.3: icmp_seq=2 ttl=255 time=0.421 ms
^C
--- 192.168.234.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.421/0.663/0.905/0.242 ms
vEdge3#
```



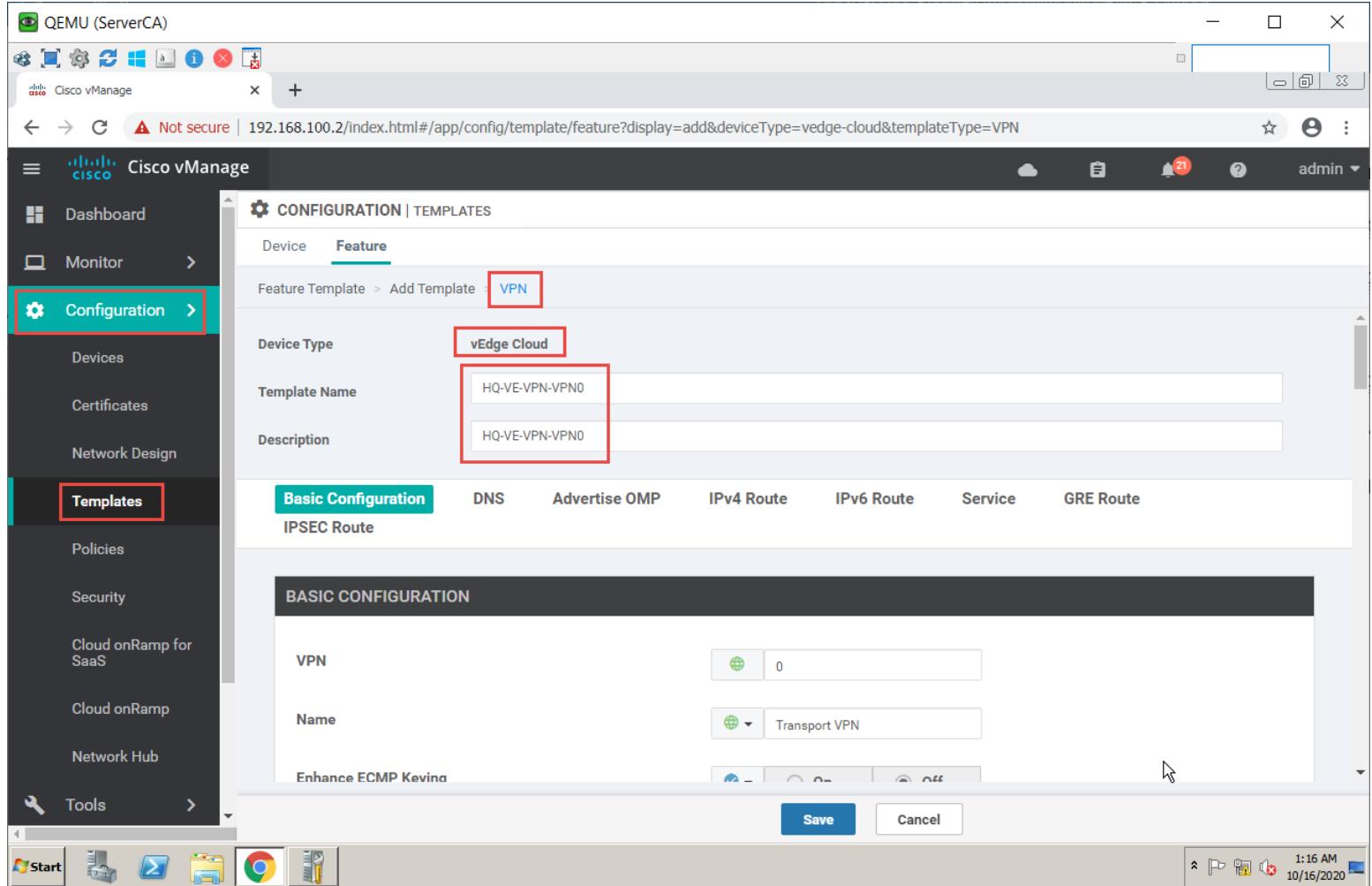


## Lab 22 – Configuring Feature Templates for HQ-Site(vEdge1) – VPNs, VPN Interfaces, External & Internal Routing

### VPN 0

#### Task 1 – Configure a VPN Template for HQ vEdge-Cloud Devices for VPN 0

- In vManage, **Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ VPN ➔ VPN**
- Configure the VPN parameters based on the following:
  - o Template Name: HQ-VE-VPN-VPNO
  - o Description: HQ-VE-VPN-VPNO
- Basic Configuration
  - o VPN ➔ Global: 0
  - o Name ➔ Global: Transport VPN
- IPv4 Route
  - o Prefix ➔ Global: 0.0.0.0/0
  - o Next Hop ➔ Device Specific
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing various management sections like Dashboard, Monitor, Configuration, Templates (which is selected and highlighted in red), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. Below the sidebar is a toolbar with icons for Start, Task View, File Explorer, Google Chrome, and others.

The main content area is titled "CONFIGURATION | TEMPLATES". It has tabs for "Device" and "Feature", with "Feature" selected. A breadcrumb navigation shows "Feature Template > Add Template". The "Feature Template" field contains "VPN".

The configuration form includes fields for "Device Type" (set to "vEdge Cloud"), "Template Name" (set to "HQ-VE-VPN-VPN0"), and "Description" (set to "HQ-VE-VPN-VPN0"). Below the form are tabs for "Basic Configuration" (selected), DNS, Advertise OMP, IPv4 Route, IPv6 Route, Service, and GRE Route. Under "Basic Configuration", there's a section for "VPN" with a "Name" field set to "Transport VPN". At the bottom right of the configuration form are "Save" and "Cancel" buttons.



The screenshot shows the Cisco vManage web interface. The left sidebar has a 'Configuration' section with 'Templates' selected. The main area is titled 'CONFIGURATION | TEMPLATES' and shows a table of templates. One template, 'HQ-VE-VPN-VPN0', is highlighted with a red border.

Name	Description	Type	Device Model	Device Templates	Devices	Actions
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	...
VE-System	VE-System	WAN Edge System	vEdge Cloud	1	3	...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	...
HQ-VE-VPN-VPN0	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	...
BR-VE-VPNINT-VPN0...	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN1...	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VF-VPNINT-VPN5...	BR-VF-VPNINT-VPN512-Fth0	WAN Edge Interface	vEdge Cloud	1	3	...

## Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 0 for Interface G0/0

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - o Template Name: HQ-VE-VPNINT-VPN0-G0
  - o Description: HQ-VE-VPNINT-VPN0-G0

### Basic Configuration

- o Shutdown → Global : No
- o Interface Name → Global: ge0/0
- o IPv4 Address → Static → Device Specific

### Tunnel

- o Tunnel Interface → Global: On
- o Color → Default

### Allow Service

- o All → Global: On





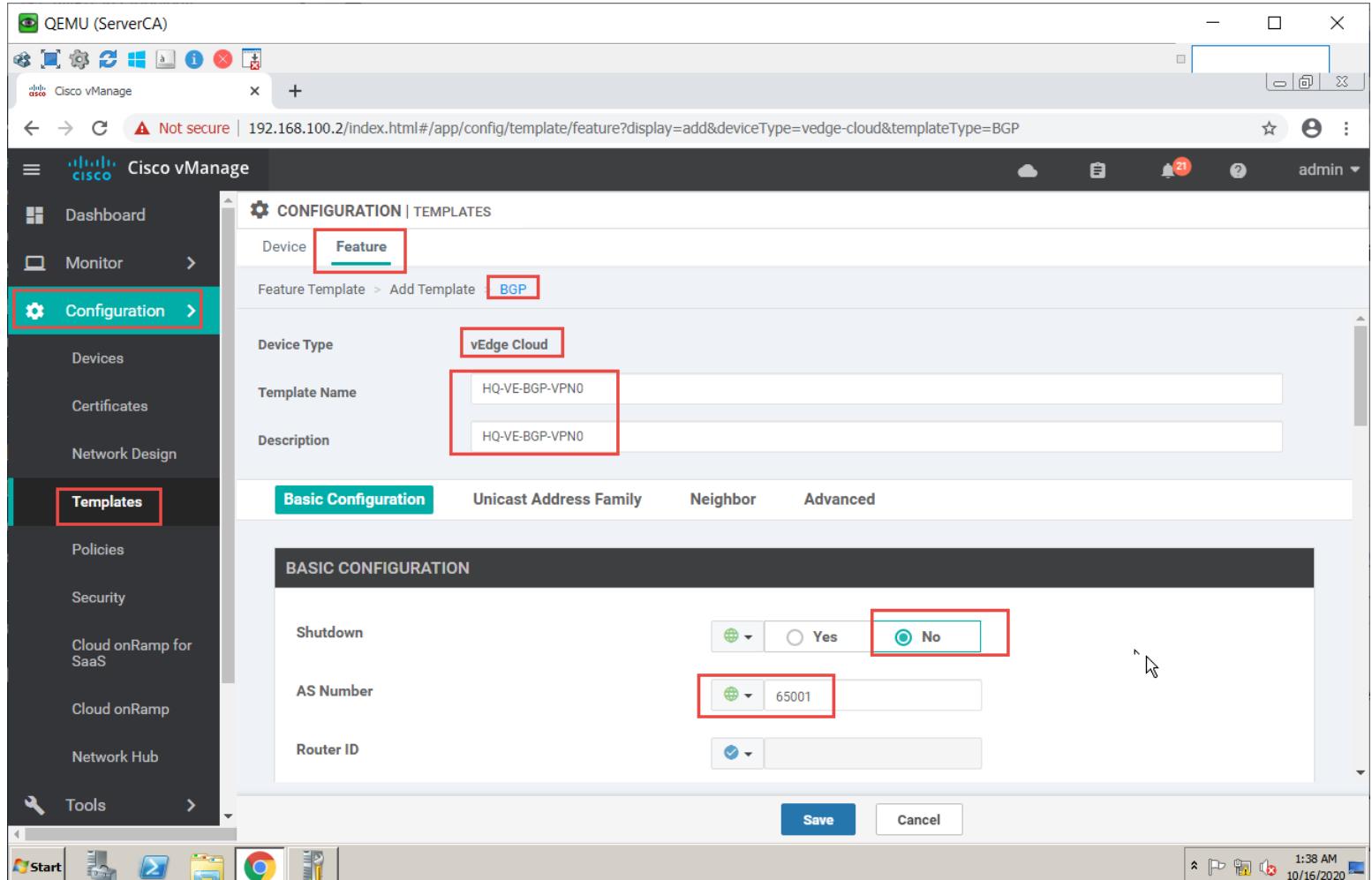
- NETCONF → Global: On
- SSH → Global: On
- Click Save to save the Template.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Actions
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	...
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN512-E...	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	...
VE-System	VE-System	WAN Edge System	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN512-G2	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	...
HQ-VE-VPN-VPN0	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE-VPNINT-VPN0-G0	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	0	0	...

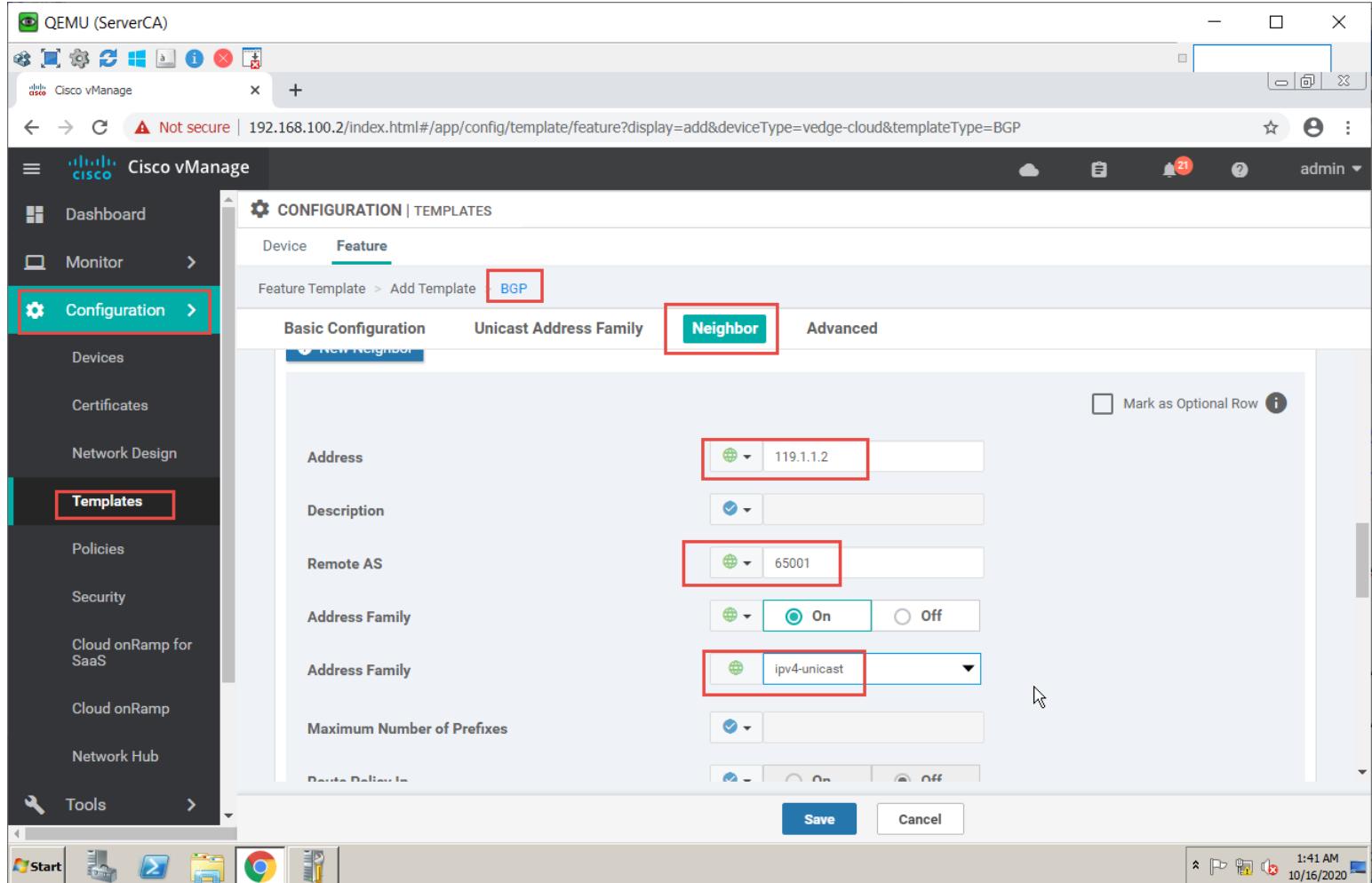
### Task 3 – Configure a BGP Template to be used by HQ vEdge-Cloud Devices for VPN 0

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → Other Templates → BGP
- Configure the BGP parameters based on the following:
  - Template Name: HQ-VE-BGP-VPN0
  - Description: HQ-VE-BGP-VPN0
- Basic Configuration
  - Shutdown → Global: No
  - AS Number → Global: 65001
- Neighbor
  - Address → Global: 119.1.1.2
  - Remote AS → Global: 65001
  - Address Family → Global: On
  - Address Family → Global: IPv4-Unicast

- Click Add to add the Interface and Click Add to add BGP Neighbor.
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing various management options like Dashboard, Monitor, Configuration, Templates (which is selected and highlighted with a red box), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. Below the sidebar is a toolbar with icons for Start, Task View, File Explorer, Google Chrome, and others. The main content area has a title bar "QEMU (ServerCA)" and a browser header "Cisco vManage" with a warning about "Not secure" and the URL "192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=BGP". The user is in the "Configuration | Templates" section under the "Feature" tab (also highlighted with a red box). A sub-menu "Add Template" is open, showing "BGP" selected. The configuration form includes fields for "Device Type" (vEdge Cloud), "Template Name" (HQ-VE-BGP-VPN0), and "Description" (HQ-VE-BGP-VPN0). Below the form are tabs for "Basic Configuration" (selected), "Unicast Address Family", "Neighbor", and "Advanced". Under "Basic Configuration", there are sections for "Shutdown" (radio button set to "No" and highlighted with a red box), "AS Number" (set to 65001 and highlighted with a red box), and "Router ID". At the bottom are "Save" and "Cancel" buttons. The status bar at the bottom right shows the date and time: "10/16/2020 1:38 AM".



The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing the 'Configuration' section with 'Templates' selected. The main content area is titled 'CONFIGURATION | TEMPLATES' under the 'Feature' tab. A 'BGP' feature template is selected. The 'Neighbor' tab is active. The configuration form includes fields for 'Address' (119.1.1.2), 'Description' (checkbox checked), 'Remote AS' (65001), 'Address Family' (radio button set to 'On', dropdown selected 'ipv4-unicast'), and 'Maximum Number of Prefixes' (checkbox checked). Buttons for 'Save' and 'Cancel' are at the bottom.



## VPN 512

### Task 1 – Configure a VPN Template to be used by HQ vEdge-Cloud Devices for VPN 512

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN
- Configure the VPN parameters based on the following:
  - o Template Name: HQ-VE-VPN-VPN512
  - o Description: HQ-VE-VPN-VPN512
- Basic Configuration
  - o VPN → Global: 512
  - o Name → Global: MGMT VPN
- Click Save to save the Template.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN

Cisco vManage

Dashboard

Monitor >

Configuration >

Devices

Certificates

Network Design

Templates

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools >

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template > **VPN**

Device Type **vEdge Cloud**

Template Name **HQ-VE-VPN-VPN512**

Description **HQ-VE-VPN-VPN512**

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

IPSEC Route

BASIC CONFIGURATION

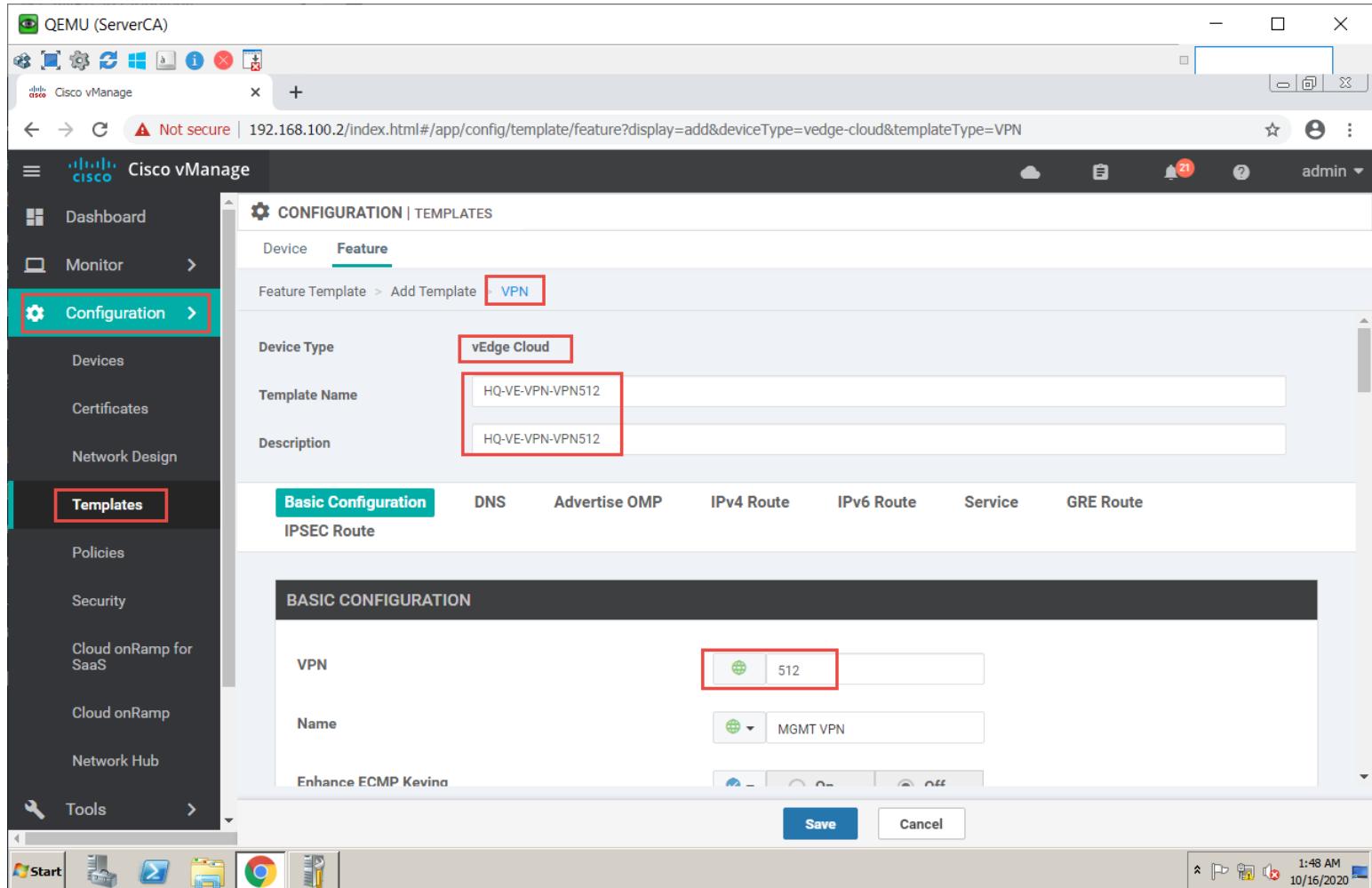
VPN **512**

Name **MGMT VPN**

Enhance ECMP Keving

Save Cancel

1:48 AM 10/16/2020



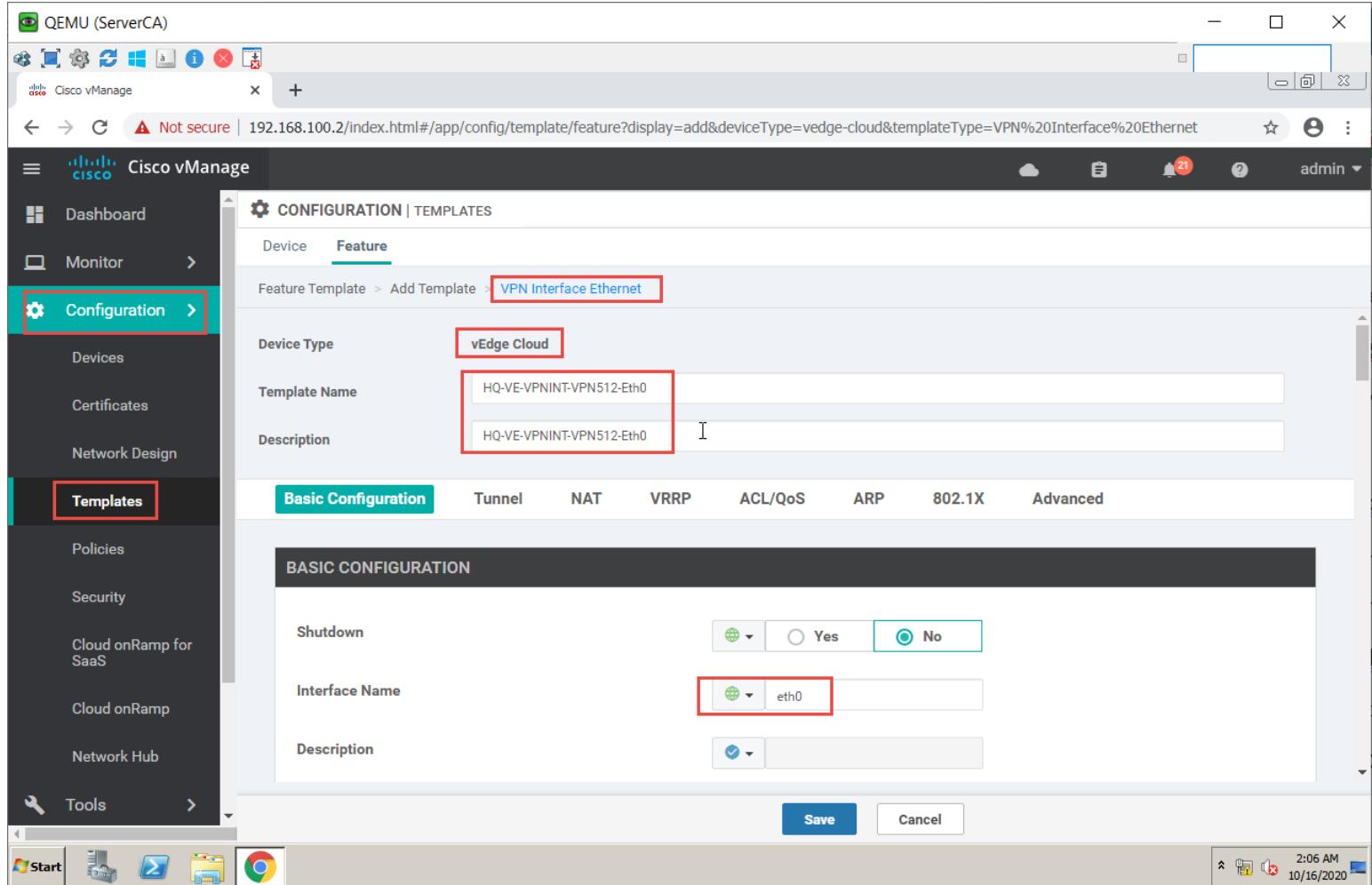


The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing various configuration tabs like Devices, Certificates, Network Design, Templates (which is currently selected), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area is titled 'CONFIGURATION | TEMPLATES' and has a sub-tab 'Feature' selected. It displays a table of templates with columns: Name, Description, Type, Device Model, Device Templates, and Devices Attached. There are 18 total rows. One row, 'HQ-VE-VPN-VPN512', is highlighted with a red box. The table data is as follows:

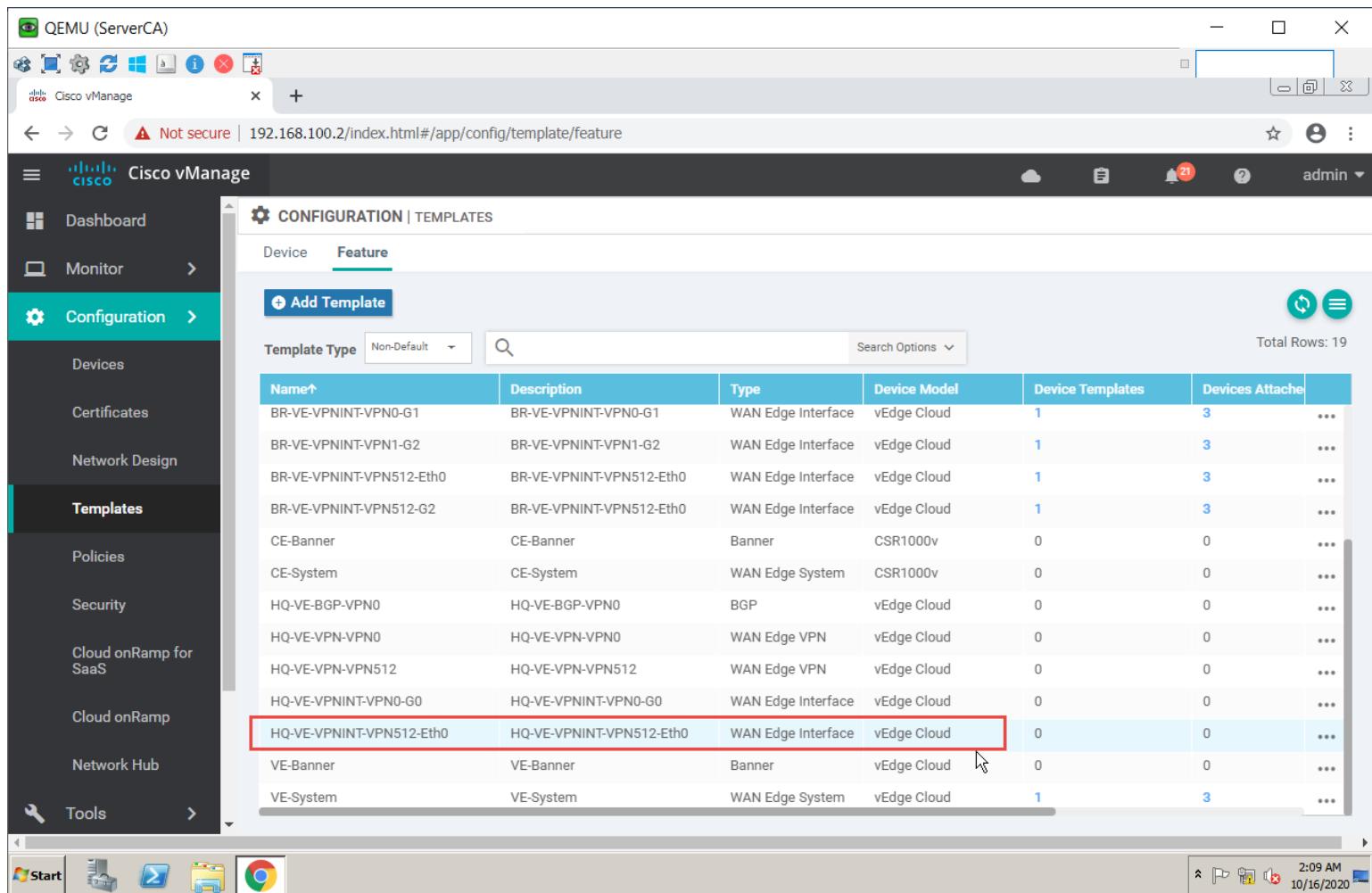
Name	Description	Type	Device Model	Device Templates	Devices Attached
HQ-VE-BGP-VPN0	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	0	0
CE-System	CE-System	WAN Edge System	CSR1000v	0	0
CE-Banner	CE-Banner	Banner	CSR1000v	0	0
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3
BR-VE-VPNINT-VPN512-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3
VE-System	VE-System	WAN Edge System	vEdge Cloud	1	3
BR-VE-VPNINT-VPN512-G2	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3
HQ-VE-VPN-VPN0	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0
HQ-VE-VPNINT-VPN0-G0	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	0	0
<b>HQ-VE-VPN-VPN512</b>	<b>HQ-VE-VPN-VPN512</b>	<b>WAN Edge VPN</b>	<b>vEdge Cloud</b>	<b>0</b>	<b>0</b>

## Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN Interface Ethernet
  - Configure the VPN parameters based on the following:
    - o Template Name: HQ-VE-VPNINT-VPN512-E0
    - o Description: HQ-VE-VPNINT-VPN512-E0
- Basic Configuration**
- o Shutdown → Global: No
  - o Interface Name → Global: eth0
  - o IPv4 Address → Dynamic
- Click Save to save the Template



The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing various configuration tabs like Configuration, Templates (which is selected and highlighted in red), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. The main content area is titled "CONFIGURATION | TEMPLATES" under the "Feature" tab. It shows a breadcrumb path: Feature Template > Add Template > **VPN Interface Ethernet**. The "Device Type" is set to "vEdge Cloud". The "Template Name" is "HQ-VE-VPNINT-VPN512-Eth0", and the "Description" is "HQ-VE-VPNINT-VPN512-Eth0". Below this, there are tabs for Basic Configuration, Tunnel, NAT, VRRP, ACL/QoS, ARP, 802.1X, and Advanced. The "Basic Configuration" tab is active. Under "BASIC CONFIGURATION", there are fields for "Shutdown" (set to "No") and "Interface Name" (set to "eth0"). At the bottom right of the configuration window are "Save" and "Cancel" buttons. The browser address bar shows the URL <https://192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN%20Interface%20Ethernet>. The status bar at the bottom indicates the date and time as 10/16/2020 and 2:06 AM.



The screenshot shows the Cisco vManage web interface. The left sidebar is open with the 'Configuration' tab selected. In the main content area, the 'TEMPLATES' section is active, and the 'Feature' tab is selected. A table lists various templates, including 'BR-VE-VPNINT-VPN0-G1', 'BR-VE-VPNINT-VPN1-G2', 'BR-VE-VPNINT-VPN512-Eth0', 'BR-VE-VPNINT-VPN512-G2', 'CE-Banner', 'CE-System', 'HQ-VE-BGP-VPN0', 'HQ-VE-VPN-VPN0', 'HQ-VE-VPN-VPN512', 'HQ-VE-VPNINT-VPN0-G0', 'HQ-VE-VPNINT-VPN512-Eth0', 'VE-Banner', and 'VE-System'. The row for 'HQ-VE-VPNINT-VPN512-Eth0' is highlighted with a red border. The table has columns for Name, Description, Type, Device Model, Device Templates, Devices Attached, and Actions.

Name	Description	Type	Device Model	Device Templates	Devices Attached	Actions
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN512-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN512-G2	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	...
CE-System	CE-System	WAN Edge System	CSR1000v	0	0	...
HQ-VE-BGP-VPN0	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	0	0	...
HQ-VE-VPN-VPN0	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE-VPN-VPN512	HQ-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE-VPNINT-VPN0-G0	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	0	0	...
HQ-VE-VPNINT-VPN512-Eth0	HQ-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	0	0	...
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	...
VE-System	VE-System	WAN Edge System	vEdge Cloud	1	3	...

## VPN 1

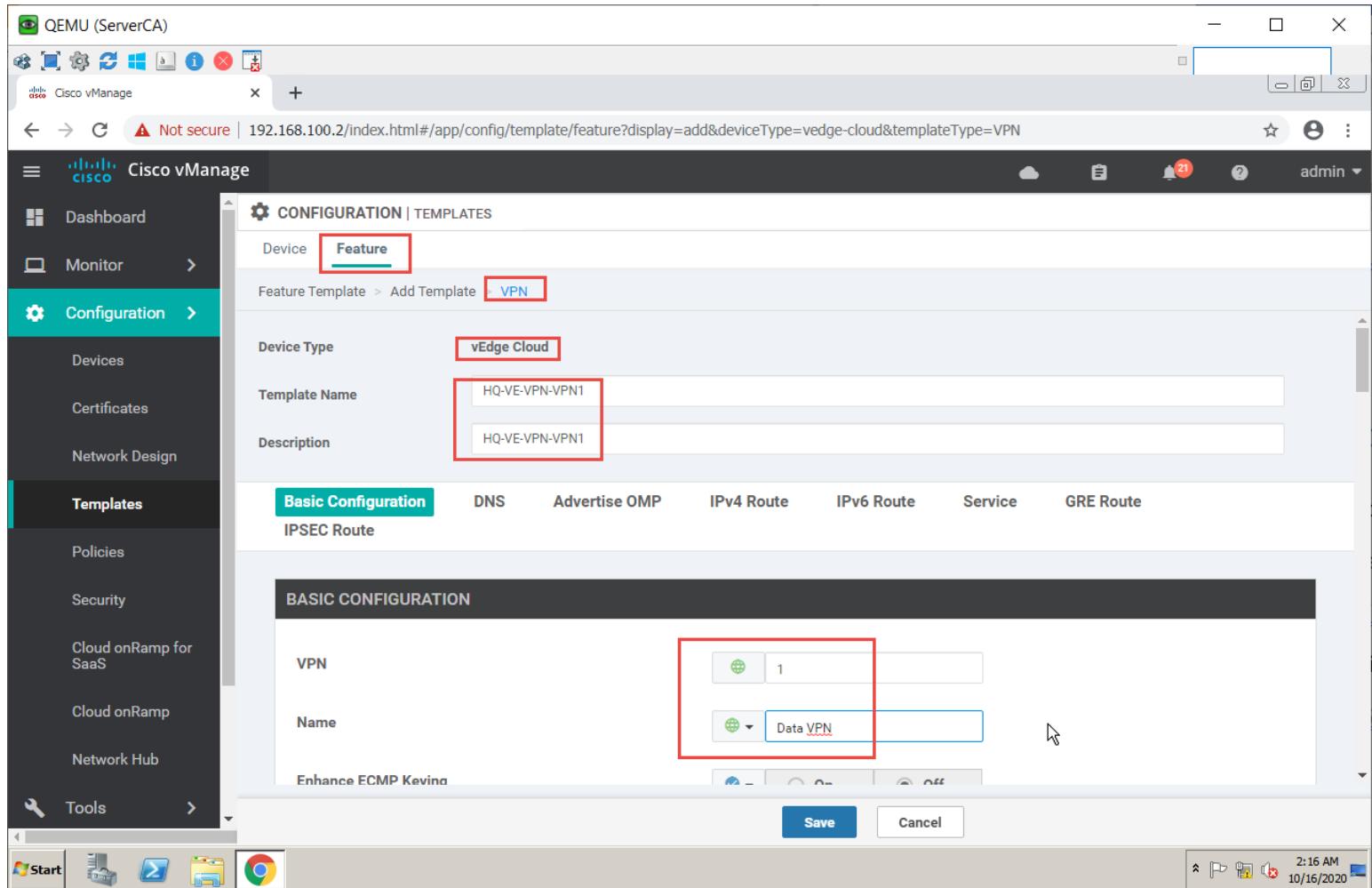
### Task 1 – Configure a VPN Template for HQ vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN
- Configure the VPN parameters based on the following:
  - o Template Name: HQ-VE-VPN-VPN1
  - o Description: HQ-VE-VPN-VPN1

#### Basic Configuration

- o VPN → Global: 1
- o Name → Global: Data VPN

- Click Save to save the Template.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN

admin

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Add Template **VPN**

Device Type **vEdge Cloud**

Template Name **HQ-VE-VPN-VPN1**

Description **HQ-VE-VPN-VPN1**

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

IPSEC Route

BASIC CONFIGURATION

VPN

Name **Data VPN**

Enhance ECMP Keving

Save Cancel



Cisco vManage Not secure | 192.168.100.2/index.html#/app/config/template/feature admin

Cisco vManage

Dashboard Monitor Configuration > Templates Policies Security Cloud onRamp for SaaS Cloud onRamp Network Hub Tools

CONFIGURATION | TEMPLATES

Device Feature + Add Template

Template Type Non-Default Search Options Total Rows: 20

Name↑	Description	Type	Device Model	Device Templates	Devices	...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Inter...	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN51...	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Inter...	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN51...	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Inter...	vEdge Cloud	1	3	...
CE-Banner	CE-Banner	Banner	CSR1000v	0	0	...
CE-System	CE-System	WAN Edge Syst...	CSR1000v	0	0	...
HQ-VE-BGP-VPN0	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	0	0	...
HQ-VE-VPN-VPN0	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE-VPN-VPN1	HQ-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE-VPN-VPN512	HQ-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE-VPNINT-VPN0-...	HQ-VE-VPNINT-VPN0-G0	WAN Edge Inter...	vEdge Cloud	0	0	...
HQ-VE-VPNINT-VPN51...	HQ-VE-VPNINT-VPN512-Eth0	WAN Edge Inter...	vEdge Cloud	0	0	...
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	...
VE-System	VE-System	WAN Edge Syst...	vEdge Cloud	1	3	...

Start Google Chrome 2:17 AM 10/16/2020

## Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 1 for Interface G0/2

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → VPN → VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - Template Name: HQ-VE-VPNINT-VPN1-G2
  - Description: HQ-VE-VPNINT-VPN1-G2
- Basic Configuration
  - Shutdown → Global: No
  - Interface Name → Global: ge0/2
  - IPv4 Address → Static → Device Specific
- Click Save to save the Template.



Screenshot of Cisco vManage interface showing the configuration of a VPN Interface Ethernet template.

The left sidebar shows the navigation menu with the "Templates" option selected. The main configuration screen is titled "CONFIGURATION | TEMPLATES" under the "Device" tab. A red box highlights the "Feature" tab. The feature template being edited is "VPN Interface Ethernet".

The "Basic Configuration" tab is selected. The "Shutdown" field is set to "No" (radio button selected), and the "Interface Name" dropdown is set to "ge0/2".

At the bottom right of the configuration window, there are "Save" and "Cancel" buttons.

The browser address bar shows the URL: 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN%20Interface%20Ethernet

The taskbar at the bottom shows icons for Start, File, Task View, File Explorer, and Google Chrome, along with system status indicators.



The screenshot shows the Cisco vManage web interface. The left sidebar is open with the 'Configuration' tab selected. Under 'Templates', the 'Feature' tab is active. A table lists various templates, with one row highlighted by a red box: 'HQ-VE-VPNINT-VPN1-G2'. This row has a 'WAN Edge Interface' type, 'vEdge Cloud' device model, and 0 device templates. The table includes columns for Name, Description, Type, Device Model, Device Templates, and Device.

Name	Description	Type	Device Model	Device Templates	Device
BR-VE-VPNINT-VPN0...	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3 ***
BR-VE-VPNINT-VPN5...	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3 ***
CE-Banner	CE-Banner	Banner	CSR1000v	0	0 ***
CE-System	CE-System	WAN Edge System	CSR1000v	0	0 ***
HQ-VE-BGP-VPN0	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	0	0 ***
HQ-VE-VPN-VPN0	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0 ***
HQ-VE-VPN-VPN1	HQ-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	0	0 ***
HQ-VE-VPN-VPN512	HQ-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	0	0 ***
HQ-VE-VPNINT-VPN0...	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	0	0 ***
HQ-VE-VPNINT-VPN1...	HQ-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	0	0 ***
HQ-VE-VPNINT-VPN5...	HQ-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	0	0 ***
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0 ***
VE-System	VE-System	WAN Edge System	vEdge Cloud	1	3 ***

### Task 3 – Configure a OSPF Template to be used by HQ vEdge-Cloud Devices for VPN 1

- In vManage, Navigate to Configuration → Templates → Feature → vEdge Cloud → Other Templates → OSPF
- Configure the OSPF parameters based on the following
  - o Template Name: HQ-VE-OSPF-VPN1
  - o Description: HQ-VE-OSPF-VPN1
- Redistribution
  - o Protocol: OMP
- Area Configuration
  - o Area Number → Global: 0
  - o Area Type → Default
- Interface Configuration
  - o Interface Name: ge0/2
- Click Add to add the Interface and Click Add to add OSPF.
- Click Save to save the Template.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/template/feature

Cisco vManage

Dashboard

Monitor

Configuration

Devices

Certificates

Network Design

**Templates**

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type Non-Default

Search Options Total Rows: 22

Name	Description	Type	Device Model	Device Templates	Devices Attached	Actions
BR-VE...	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	...
CE-Ba...	CE-Banner	Banner	CSR1000v	0	0	...
CE-Sys...	CE-System	WAN Edge System	CSR1000v	0	0	...
HQ-VE...	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	0	0	...
<b>HQ-VE...</b>	<b>HQ-VE-OSPF-VPN1</b>	<b>OSPF</b>	<b>vEdge Cloud</b>	0	0	...
HQ-VE...	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE...	HQ-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE...	HQ-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	0	0	...
HQ-VE...	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	0	0	...
HQ-VE...	HQ-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	0	0	...
HQ-VE...	HQ-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	0	0	...
VE-Ba...	VE-Banner	Banner	vEdge Cloud	0	0	...
VE-Sys...	VE-System	WAN Edge System	vEdge Cloud	1	3	...

Start

2:31 AM 10/16/2020



## Lab 23 - Configuring Device Templates for HQ-Site(vEdge1) to deploy VPN 0, 1 and 512.

### Task 1 – Configure a Device Template for HQ vEdge Devices.

- In vManage, Navigate to Configuration ➔ Templates ➔ Device ➔ Create Template ➔ vEdge Cloud
- Configure the Device Template based on the following:
  - o Template Name: HQ-VE-TEMP
  - o Description: HQ-VE-TEMP
- Basic Information
  - o System ➔ VE-System
- Transport & Management
  - o VPN 0: HQ-VE-VPN-VPNO
  - o VPN Interface: HQ-VE-VPNINT-VPNO-G0
  - o BGP: HQ-VE-BGP-VPNO
  - o VPN 512: HQ-VE-VPN-VPN512
  - o VPN Interface: HQ-VE-VPNINT-VPN512-E0
- Service VPN
  - o VPN 1: HQ-VE-VPN-VPN1
  - o VPN Interface: HQ-VE-VPNINT-VPN1-G2
  - o OSPF: HQ-VE-OSPF-VPN1
- Click Save to save the Template.





QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/template/device

Cisco vManage

Dashboard

Monitor

Configuration

Devices

Certificates

Network Design

**Templates**

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

CONFIGURATION | TEMPLATES

Device Feature

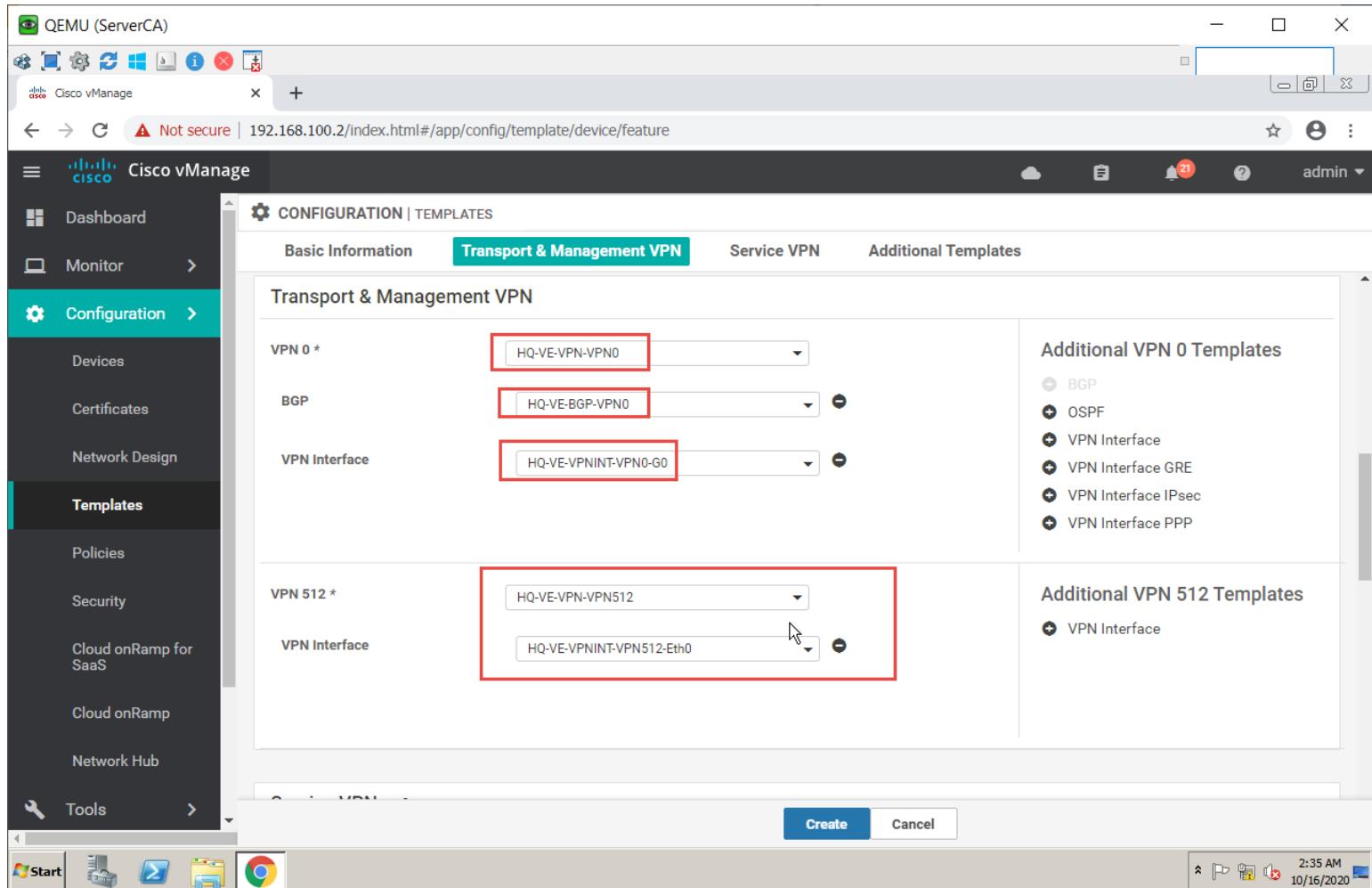
Create Template

Search Options

Total Rows: 2

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Up
BR-VE-TEMP	BR-VE-TEMP	Feature	vEdge Cloud	16	3	admin	15 Oct 2020
HQ-VE-TEMP	HQ-VE-TEMP	Feature	vEdge Cloud	14	0	admin	15 Oct 2020

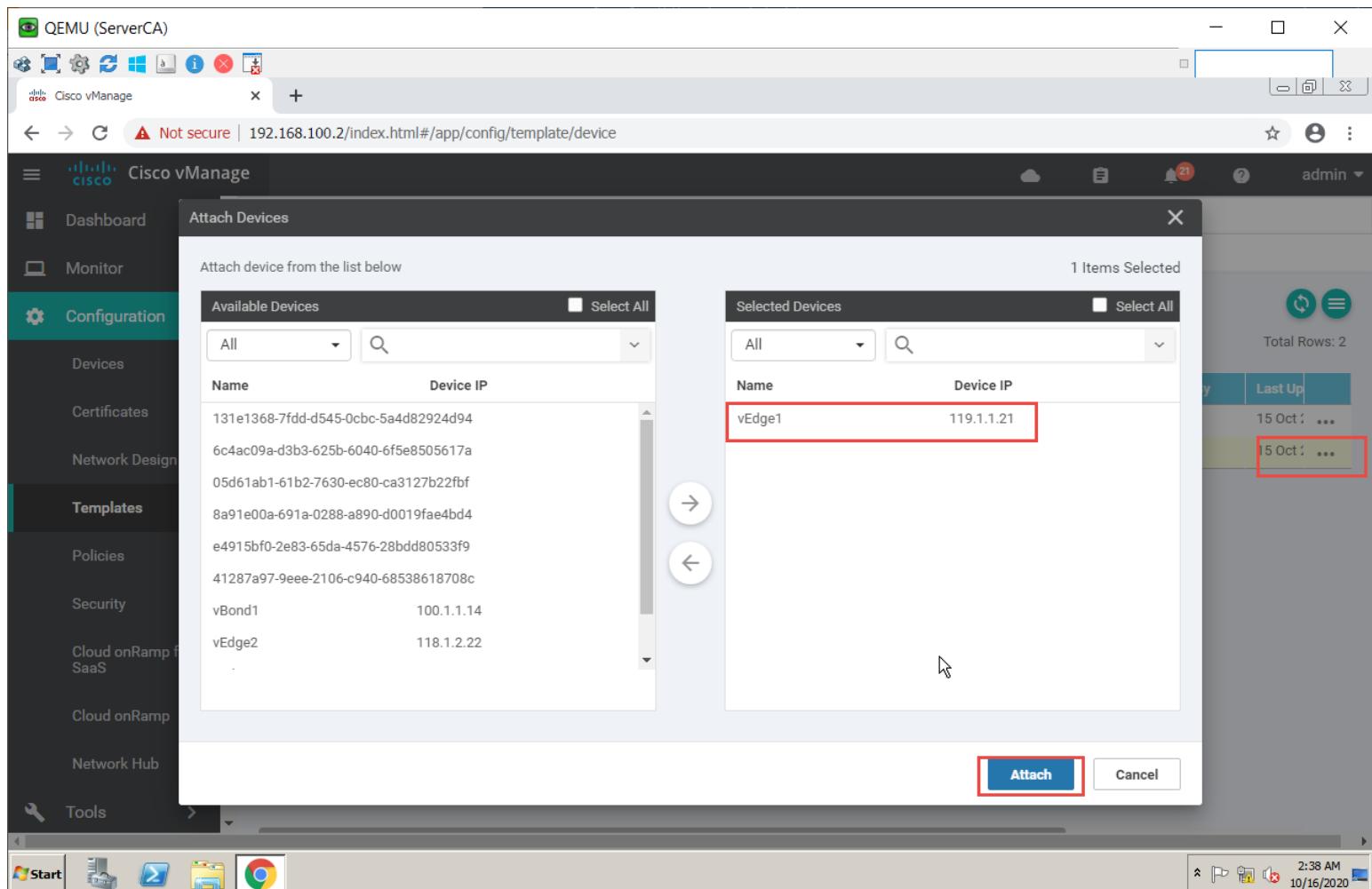
2:36 AM 10/16/2020



The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Configuration' and includes options like Devices, Certificates, Network Design, Templates (which is currently selected), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. The top navigation bar shows 'Cisco vManage' and the URL '192.168.100.2/index.html#/app/config/template/device/feature'. The main content area is titled 'CONFIGURATION | TEMPLATES' and has tabs for Basic Information, Transport & Management VPN (which is active), Service VPN, and Additional Templates. Under 'Transport & Management VPN', there are two sections: 'VPN 0 \*' and 'VPN 512 \*'. Each section has a 'VPN Interface' dropdown menu. The 'VPN Interface' dropdown for both sections is highlighted with a red box. To the right of each section, there is a list of 'Additional VPN 0 Templates' and 'Additional VPN 512 Templates' respectively. The 'Create' and 'Cancel' buttons are at the bottom of the template configuration area.

## Task 2 – Attach vEdge1 to the Device Template

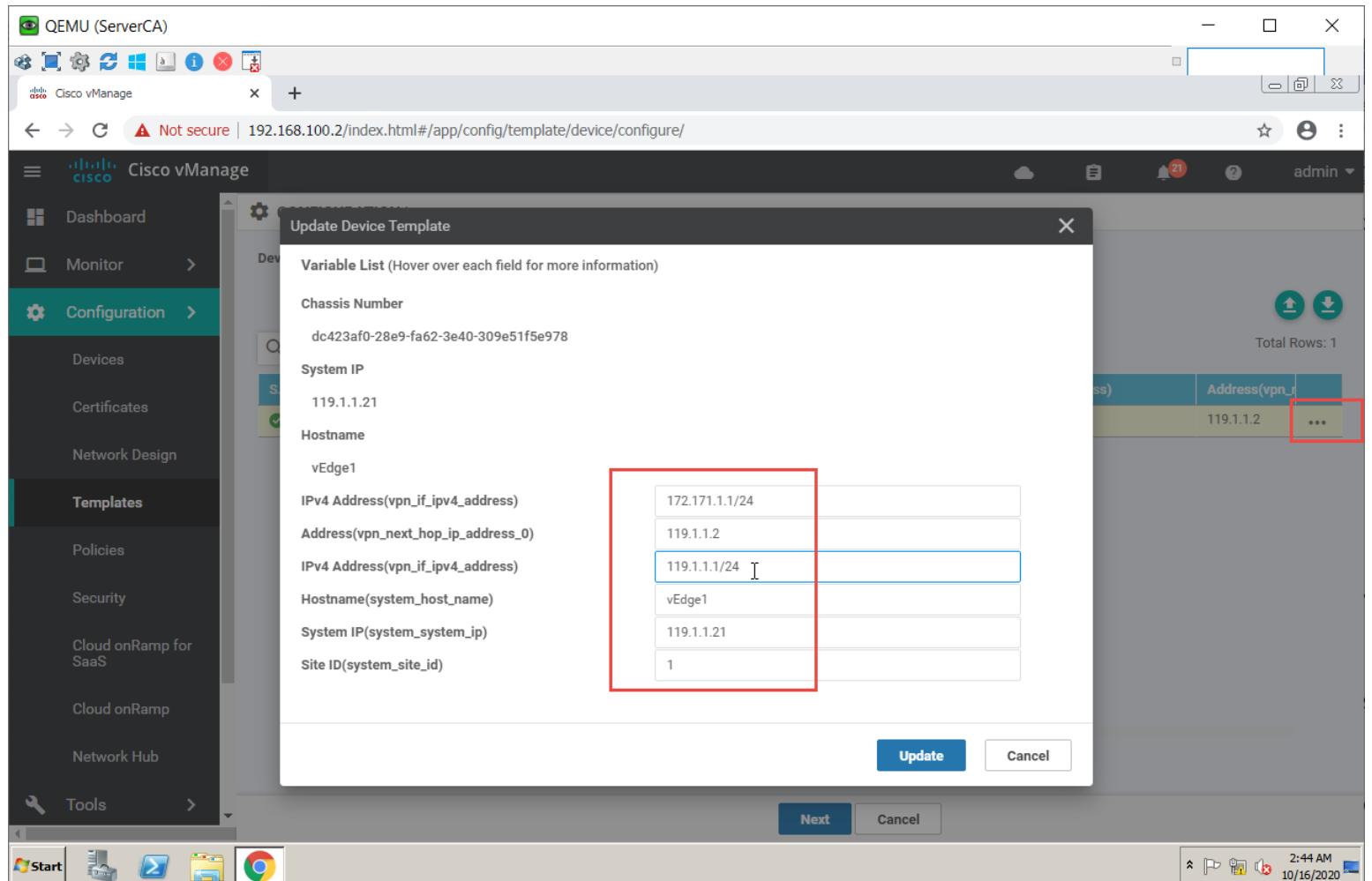
- In vManage, Navigate to Configuration → Templates → Device → HQ-VE-TEMP.
- Click on “...” towards the right-hand side.
- Click Attach Devices.
- Select vEdge1 and click the “→” button.
- Click Attach.

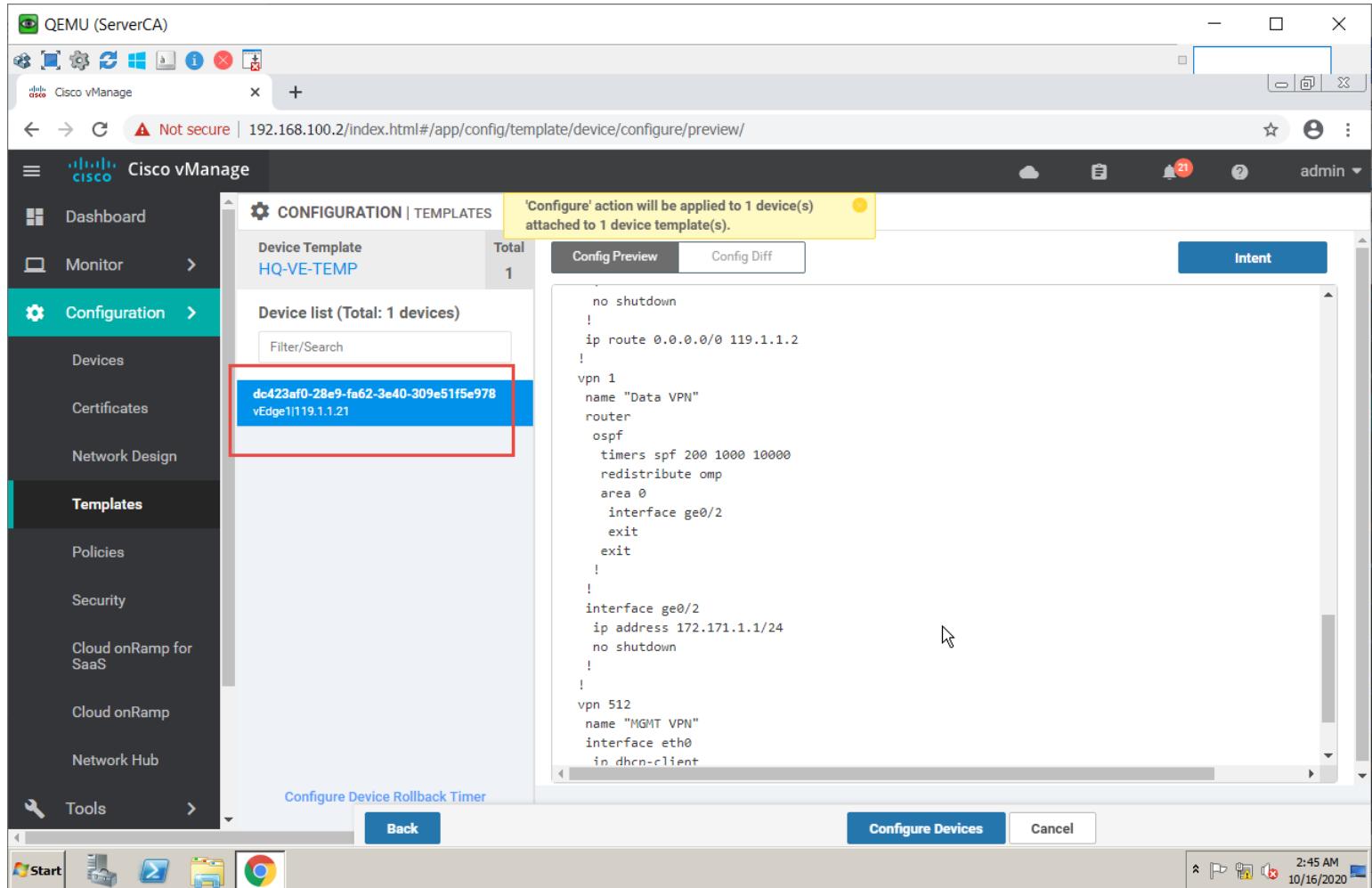


### Task 3 – Configure the Variable Parameters for the Feature Templates

- vEdge1 will appear in the window.
- Click on “...” towards the right-hand side.
- Click Edit Device Template.
- Configure the variables based on the following:
  - o Interface IP for ge0/2:172.171.1.1/24
  - o Default Gateway for VPNO: 119.1.1.2
  - o Interface IP for ge0/0:119.1.1.1/24
  - o Hostname: vEdge-1
  - o System IP: 119.1.1.21
  - o Site ID: 1
- Click Update.
- Verify the Configuration & Click Configure Devices.
- Wait for it to update the device. It should come back with Status of Success.
- Verify the configuration on vEdge1. You can do that by verify OSPF Neighbor relationship with the Internal Router by issuing the Show ospf neighbor command on vEdge1.

- Type Show Ip route on vEdge2 to verify that you are receiving OSPF routes from the MPLS Router.
- Type Show Ip route on Internal Site Routers to verify that you are receiving OSPF routes from the other Sites.
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks.





The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Cisco vManage' and includes 'Dashboard', 'Monitor', 'Configuration' (selected), 'Devices', 'Certificates', 'Network Design', 'Templates' (selected), 'Policies', 'Security', 'Cloud onRamp for SaaS', 'Cloud onRamp', and 'Network Hub'. Below the sidebar is a toolbar with icons for Start, File, Edit, View, Insert, Tools, and Help, along with a date/time stamp of 2:45 AM 10/16/2020.

The main content area has a title 'CONFIGURATION | TEMPLATES' and a sub-section 'Device Template HQ-VE-TEMP Total 1'. A yellow message bar at the top right says "'Configure' action will be applied to 1 device(s) attached to 1 device template(s.)".

The 'Device list (Total: 1 devices)' section shows one entry: 'dc423af0-28e9-fa62-3e40-309e51f5e978 vEdge1|119.1.1.21'. This entry is highlighted with a red box.

The 'Config Preview' tab is selected, displaying the following configuration script:

```
no shutdown
!
ip route 0.0.0.0/0 119.1.1.2
!
vpn 1
name "Data VPN"
router
ospf
timers spf 200 1000 10000
redistribute ospf
area 0
interface ge0/2
exit
exit
!
!
interface ge0/2
ip address 172.171.1.1/24
no shutdown
!
!
vpn 512
name "MGMT VPN"
interface eth0
in dhcpc-client
```

At the bottom of the configuration preview are 'Configure Devices' and 'Cancel' buttons.

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/device/status?activity=push\_file\_template\_configuration&pid=push\_feature\_template\_configuration-87615f69-f78a-...

Cisco vManage

Dashboard

Monitor

Configuration

Devices

Certificates

Network Design

Templates

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

TASK VIEW

Push Feature Template Configuration | Validation Success

Total Task: 1 | Success : 1

Initiated By: admin From: 169.254.0.253

Search Options

Total Rows: 1

	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
>	Success	Done - Push Fea...	dc423af0-28e9-fa62-...	vEdge Cloud	vEdge1	119.1.1.21	1	100.1.1.12

2:46 AM 10/16/2020



```
vEdge1#
vEdge1#
vEdge1#
vEdge1#
vEdge1# show ospf nei
DBsmL -> Database Summary List
RqstL -> Link State Request List
RXmtL -> Link State Retransmission List
      SOURCE          VPN    IP ADDRESS     INTERFACE   ROUTER ID      STATE      PRIORITY      DEAD
                                         DBsmL   RqstL   RXmtL
1    172.171.1.2      ge0/2        192.168.13.1    full       1           39      0      0      0
vEdge1# show ospf routes
ospf routes-table vpn 1 network 172.171.1.0/24
  info ID 0
    area-id 0
    cost 10
    path-type intra-area
    dest-type network
    next-hop 0.0.0.0
    if-name ge0/2
ospf routes-table vpn 1 network 192.168.11.0/24
  info ID 0
    area-id 0
    cost 11
    path-type intra-area
    dest-type network
    next-hop 172.171.1.2
    if-name ge0/2
ospf routes-table vpn 1 network 192.168.12.0/24
  info ID 0
    area-id 0
    cost 11
    path-type intra-area
    dest-type network
    next-hop 172.171.1.2
Aborted: by user
^CvEdge1# ping 192.168.12.1 vpn1
syntax error: unknown element
vEdge1# ping 192.168.12.1 vpn 1
Ping in VPN 1
PING 192.168.12.1 (192.168.12.1) 56(84) bytes of data.
64 bytes from 192.168.12.1: icmp_seq=1 ttl=255 time=1.31 ms
64 bytes from 192.168.12.1: icmp_seq=2 ttl=255 time=0.460 ms
^C
--- 192.168.12.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.460/0.885/1.311/0.426 ms
vEdge1#
```



PuTTY (inactive)

```
ip dhcp-client
no shutdown
!
vEdge2# show ip route
Codes: F -> fib, S -> selected, I -> inactive,
       B -> blackhole, R -> recursive
Codes Status flags:
F -> fib, S -> selected, I -> inactive,
B -> blackhole, R -> recursive
```

VPN	PREFIX	PROTOCOL	SUB	TYPE	IF NAME	NEXTHOP	ADDR	NEXTHOP	VPN	TLOC	IP	COLOR	ENCAP	STATUS
0	0.0.0.0/0	static	-		ge0/1	118.1.2.2	-	-	-	-	-	-	F,S	
0	10.1.11.0/24	ospf	IA		ge0/0	10.1.12.2	-	-	-	-	-	-	F,S	
0	10.1.12.0/24	ospf	IA		ge0/0	-	-	-	-	-	-	-	-	
0	10.1.12.0/24	connected	-		ge0/0	-	-	-	-	-	-	-	F,S	
0	10.1.13.0/24	ospf	IA		ge0/0	10.1.12.2	-	-	-	-	-	-	F,S	
0	10.1.14.0/24	ospf	IA		ge0/0	10.1.12.2	-	-	-	-	-	-	F,S	
0	10.1.15.0/24	ospf	IA		ge0/0	10.1.12.2	-	-	-	-	-	-	F,S	
0	100.1.1.0/24	ospf	IA		ge0/0	10.1.12.2	-	-	-	-	-	-	F,S	
0	118.1.2.0/24	connected	-		ge0/1	-	-	-	-	-	-	-	F,S	
0	118.1.2.22/32	connected	-	system	-	-	-	-	-	-	-	-	F,S	
0	119.1.1.0/24	ospf	IA		ge0/0	10.1.12.2	-	-	-	-	-	-	F,S	
1	172.16.234.4/32	omp	-		-	-	-	118.1.3.24	mpls			ipsec	F,S	
1	172.16.234.4/32	omp	-		-	-	-	118.1.3.24	biz-internet			ipsec	F,S	
1	172.171.1.0/24	omp	-		-	-	-	119.1.1.21	default			ipsec	F,S	
1	172.172.1.0/24	ospf	IA		ge0/2	-	-	-	-	-	-	-	-	
1	172.172.1.0/24	connected	-		ge0/2	-	-	-	-	-	-	-	F,S	
1	172.173.1.0/24	omp	-		-	-	-	118.1.3.23	mpls			ipsec	F,S	
1	172.173.1.0/24	omp	-		-	-	-	118.1.3.23	biz-internet			ipsec	F,S	
1	172.174.1.0/24	omp	-		-	-	-	118.1.3.24	mpls			ipsec	F,S	
1	172.174.1.0/24	omp	-		-	-	-	118.1.3.24	biz-internet			ipsec	F,S	
1	192.168.11.1/32	omp	-		-	-	-	119.1.1.21	default			ipsec	F,S	
1	192.168.12.1/32	omp	-		-	-	-	119.1.1.21	default			ipsec	F,S	
1	192.168.13.1/32	omp	-		-	-	-	119.1.1.21	default			ipsec	F,S	
1	192.168.21.0/24	ospf	IA		ge0/2	172.172.1.2	-	-	-	-	-	-	F,S	
1	192.168.22.0/24	ospf	IA		ge0/2	172.172.1.2	-	-	-	-	-	-	F,S	
1	192.168.23.0/24	ospf	IA		ge0/2	172.172.1.2	-	-	-	-	-	-	F,S	
1	192.168.31.0/24	omp	-		-	-	-	118.1.3.23	mpls			ipsec	F,S	
1	192.168.31.0/24	omp	-		-	-	-	118.1.3.23	biz-internet			ipsec	F,S	
1	192.168.32.0/24	omp	-		-	-	-	118.1.3.23	mpls			ipsec	F,S	
1	192.168.32.0/24	omp	-		-	-	-	118.1.3.23	biz-internet			ipsec	F,S	
1	192.168.33.0/24	omp	-		-	-	-	118.1.3.23	mpls			ipsec	F,S	
1	192.168.33.0/24	omp	-		-	-	-	118.1.3.23	biz-internet			ipsec	F,S	





## Site-2

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2  
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  
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP  
a - application route  
+ - replicated route, % - next hop override

Gateway of last resort is not set

```
    172.16.0.0/32 is subnetted, 1 subnets
O E2      172.16.234.4 [110/16777214] via 172.172.1.1, 00:18:26, Ethernet0/0
    172.171.0.0/24 is subnetted, 1 subnets
O E2      172.171.1.0 [110/16777214] via 172.172.1.1, 00:18:26, Ethernet0/0
    172.172.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.172.1.0/24 is directly connected, Ethernet0/0
L        172.172.1.2/32 is directly connected, Ethernet0/0
    172.173.0.0/24 is subnetted, 1 subnets
O E2      172.173.1.0 [110/16777214] via 172.172.1.1, 12:40:45, Ethernet0/0
    172.174.0.0/24 is subnetted, 1 subnets
O E2      172.174.1.0 [110/16777214] via 172.172.1.1, 00:18:26, Ethernet0/0
O E2      192.168.11.0/24 [110/16777214] via 172.172.1.1, 00:00:29, Ethernet0/0
O E2      192.168.12.0/24 [110/16777214] via 172.172.1.1, 00:00:29, Ethernet0/0
O E2      192.168.13.0/24 [110/16777214] via 172.172.1.1, 00:00:24, Ethernet0/0
    192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.21.0/24 is directly connected, Loopback1
L        192.168.21.1/32 is directly connected, Loopback1
    192.168.22.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.22.0/24 is directly connected, Loopback2
L        192.168.22.1/32 is directly connected, Loopback2
    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.23.0/24 is directly connected, Loopback3
L        192.168.23.1/32 is directly connected, Loopback3
O E2      192.168.31.0/24 [110/16777214] via 172.172.1.1, 12:40:45, Ethernet0/0
O E2      192.168.32.0/24 [110/16777214] via 172.172.1.1, 12:40:45, Ethernet0/0
O E2      192.168.33.0/24 [110/16777214] via 172.172.1.1, 12:40:45, Ethernet0/0
O E2      192.168.41.0/24 [110/16777214] via 172.172.1.1, 00:18:26, Ethernet0/0
O E2      192.168.42.0/24 [110/16777214] via 172.172.1.1, 00:18:26, Ethernet0/0
O E2      192.168.43.0/24 [110/16777214] via 172.172.1.1, 00:18:26, Ethernet0/0
    192.168.234.0/32 is subnetted, 3 subnets
C        192.168.234.2 is directly connected, Loopback4
O E2      192.168.234.3 [110/16777214] via 172.172.1.1, 12:40:45, Ethernet0/0
O E2      192.168.234.4 [110/16777214] via 172.172.1.1, 00:18:26, Ethernet0/0
```

Site-2#

Site-2#ping 192.168.11.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

Site-2#

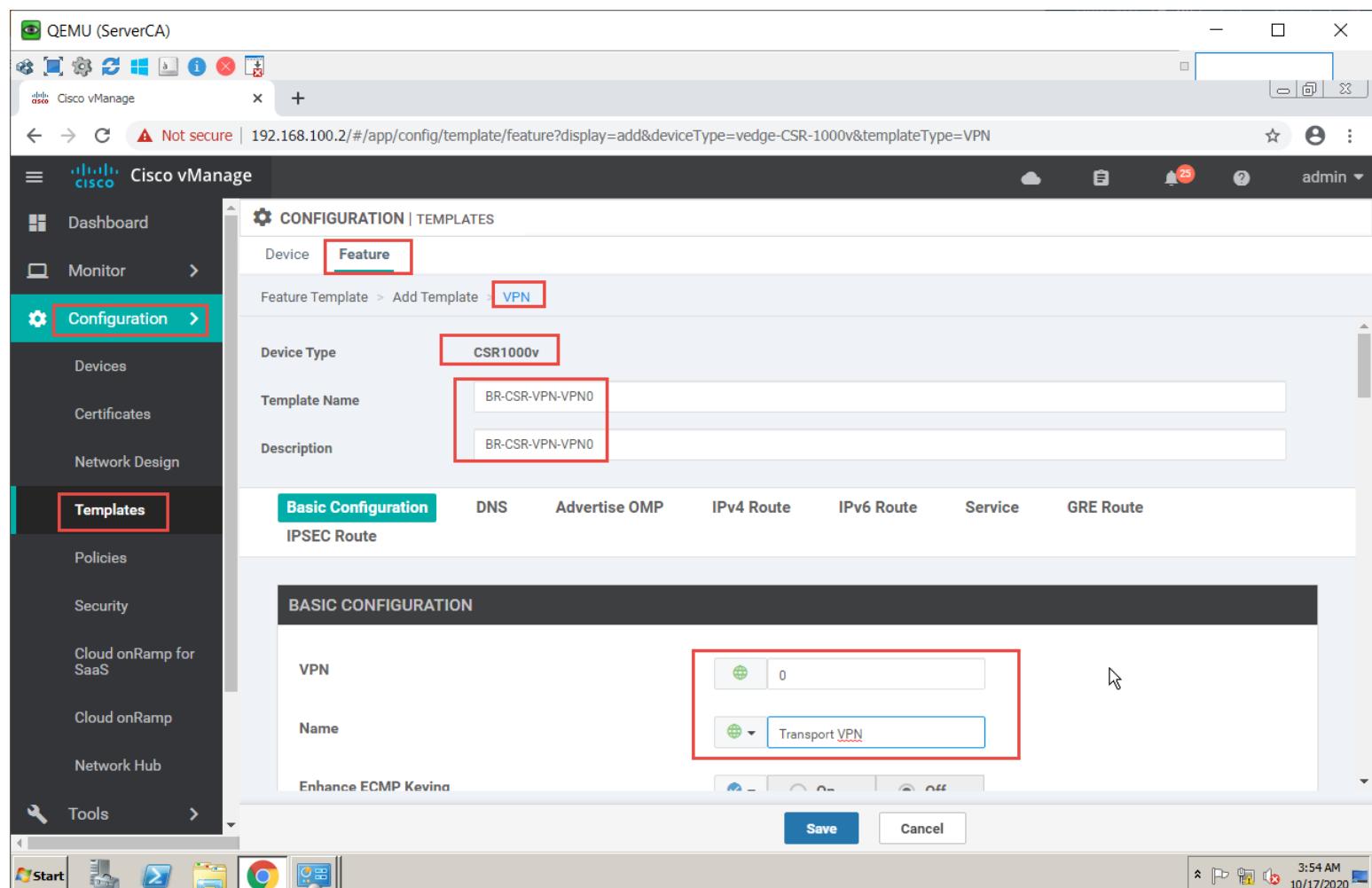


## Lab 24 – Configuring Feature Templates for CSR – VPNs, VPN Interfaces, External & Internal Routing

### VPN 0

#### Task 1 – Configure a VPN Template by CSR for VPN 0

- In vManage, Navigate to Configuration → Templates → Feature → CSR1000v → VPN → Cisco VPN
- Configure the VPN parameters based on the following:
  - o Template Name: BR-CSR-VPN-VPNO
  - o Description: BR-CSR -VPN-VPNO
- Basic Configuration
  - o VPN → Global: 0
  - o Name → Global: Transport VPN
- IPv4 Route
  - o Prefix → Global: 0.0.0.0/0
  - o Next Hop → Device Specific
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing the 'Configuration' tab selected under 'Templates'. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows the 'Feature' tab selected. A sub-menu 'Feature Template > Add Template > VPN' is visible. The 'Device Type' is set to 'CSR1000v'. The 'Template Name' is 'BR-CSR-VPN-VPNO' and the 'Description' is also 'BR-CSR-VPN-VPNO'. Below this, the 'Basic Configuration' tab is selected, showing the 'VPN' configuration section. It has a 'Name' field set to 'Transport VPN'. At the bottom right of the configuration window are 'Save' and 'Cancel' buttons. The status bar at the bottom right shows the date and time: '3:54 AM 10/17/2020'.



## Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 0 for Interface GigabitEthernet1

- In vManage, Navigate to Configuration → Templates → Feature → CSR1000v → VPN → VPN Interface Ethernet

- Configure the VPN parameters based on the following:

- Template Name: BR-CSR-VPNINT-VPN0-G1
  - Description: BR-CSR-VPNINT-VPN0-G1

### Basic Configuration

- Shutdown → Global: No
  - Interface Name → Global: GigabitEthernet1
  - IPv4 Address → Static → Device Specific

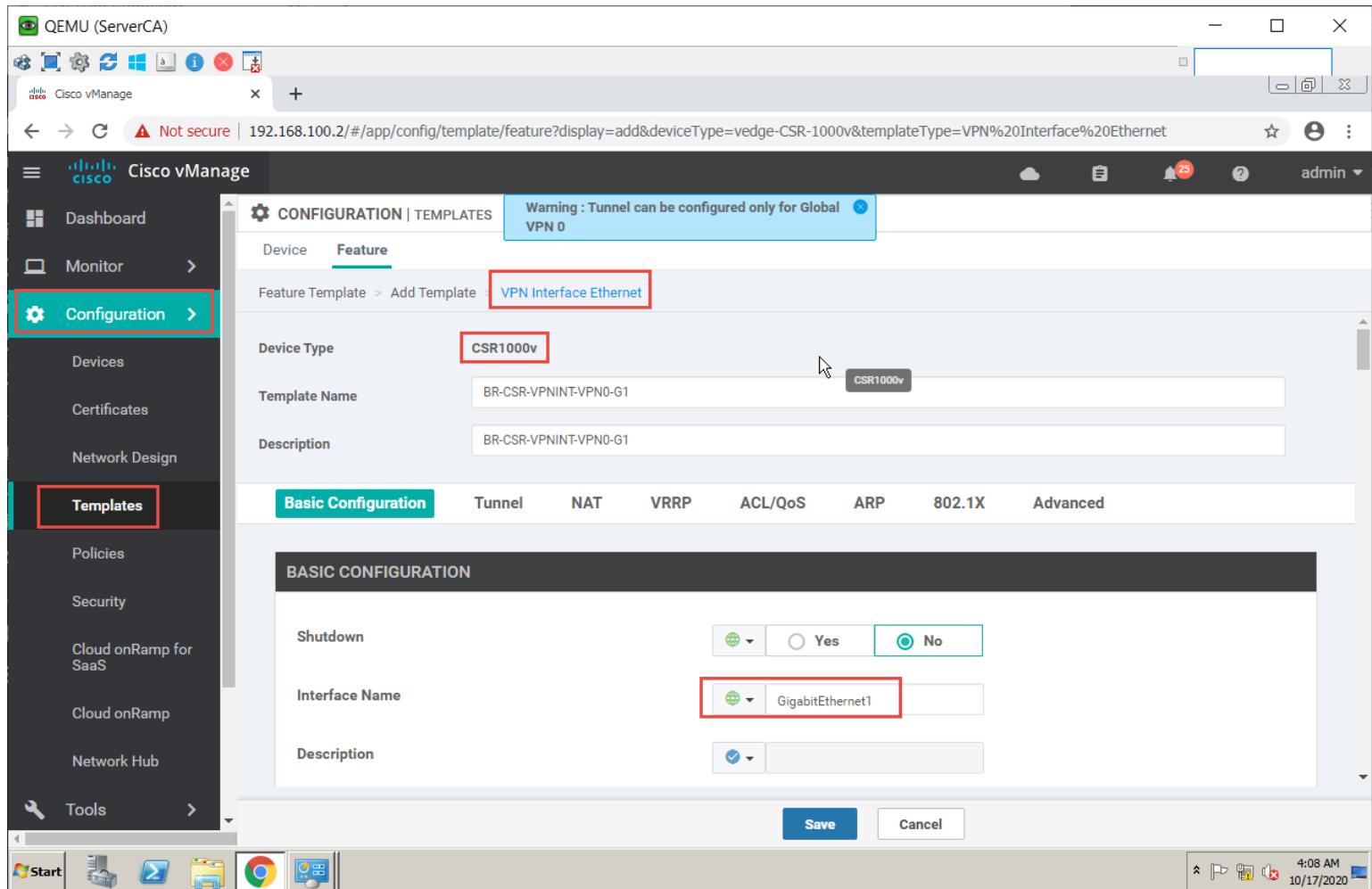
### Tunnel

- Tunnel Inteface → Global: On
  - Color → Default

### Allow Service

- All → Global: On
  - NETCONF → Global: On
  - SSH → Global: On

- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing various management options like Dashboard, Monitor, Configuration, Templates (which is selected and highlighted with a red border), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. The main content area is titled "CONFIGURATION | TEMPLATES". It shows a "Feature" tab selected, with a "Warning" message: "Tunnel can be configured only for Global VPN 0". Below this, it says "Feature Template > Add Template > **VPN Interface Ethernet**". Under "Device Type", "CSR1000v" is selected. The "Template Name" is "BR-CSR-VPNINT-VPN0-G1" and the "Description" is "BR-CSR-VPNINT-VPN0-G1". A navigation bar at the bottom includes tabs for Basic Configuration, Tunnel, NAT, VRRP, ACL/QoS, ARP, 802.1X, and Advanced. The "Basic Configuration" tab is active. In the "BASIC CONFIGURATION" section, there are fields for "Shutdown" (radio buttons for Yes or No, with No selected) and "Interface Name" (dropdown menu showing "GigabitEthernet1" which is also highlighted with a red border). There is also a "Description" field with a dropdown arrow. At the bottom right of the configuration window are "Save" and "Cancel" buttons. The status bar at the bottom of the browser window shows the URL "192.168.100.2/#/app/config/template/feature?display=add&deviceType=vedge-CSR-1000v&templateType=VPN%20Interface%20Ethernet", the date "10/17/2020", and the time "4:08 AM".



Name↑	Description	Type	Device Model	Device Templates	Devices Attached	Actions
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	WAN Edge VPN	CSR1000v	0	0	a ...
BR-CSR-VPNINT-VPN0-G1	BR-CSR-VPNINT-VPN0-G1	WAN Edge Interf...	CSR1000v	0	0	a ...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	a ...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	a ...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3	a ...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	a ...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	a ...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interf...	vEdge Cloud	1	3	a ...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interf...	vEdge Cloud	1	3	a ...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interf...	vEdge Cloud	1	3	a ...
BR-VE-VPNINT-VPN512-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interf...	vEdge Cloud	1	3	a ...
BR-VE-VPNINT-VPN512-G2	BR-VE-VPNINT-VPN512-G2	WAN Edge Interf...	vEdge Cloud	1	3	a ...
CF-Banner	CF-Banner	Banner	CSR1000v	0	0	a ...

### Task 3 – Configure a VPN Interface Template to be used by CSR for VPN 0 for Interface GigabitEthernet3

- In vManage, Navigate to Configuration → Templates → Feature → CSR1000v → VPN → VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - o Template Name: BR-CSR-VPNINT-VPN0-G3
  - o Description: BR-CSR-VPNINT-VPN0-G3
- Basic Configuration
  - o Shutdown → Global : No
  - o Interface Name → Global: GigabitEthernet3
  - o IPv4 Address → Static → Device Specific
- Tunnel
  - o Tunnel Interface → Global: On
  - o Color → MPLS
- Allow Service
  - o All → Global : On





- NETCONF → Global : On
- SSH → Global : On
- Click Save to save the Template.

The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing the 'Configuration' section with 'Templates' selected. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows a 'Feature' tab selected. A warning message 'Warning : Tunnel can be configured only for Global VPN 0' is displayed. The 'Device Type' is set to 'CSR1000v'. The 'Template Name' is 'BR-CSR-VPNINT-VPN0-G3' and the 'Description' is also 'BR-CSR-VPNINT-VPN0-G3'. The 'Basic Configuration' tab is selected, showing fields for 'Shutdown' (set to 'Yes') and 'Interface Name' (set to 'GigabitEthernet3'). The 'Save' button is visible at the bottom right of the configuration panel.



Name↑	Description	Type	Device Model	Device Templates	Devices At	...
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	WAN Edge VPN	CSR1000v	0	0	...
BR-CSR-VPNINT-VPN0-G1	BR-CSR-VPNINT-VPN0-G1	WAN Edge Interface	CSR1000v	0	0	...
BR-CSR-VPNINT-VPN0-G3	BR-CSR-VPNINT-VPN0-G3	WAN Edge Interface	CSR1000v	0	0	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN512-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VF-VPNINT-VPN512-G2	BR-VF-VPNINT-VPN512-G2	WAN Edge Interface	vEdge Cloud	1	3	...

#### Task 4 – Configure a OSPF Template to be used by CSR for VPN 0

- In vManage, Navigate to Configuration → Templates → Feature → CSR1000v → Other Templates → Cisco OSPF
- Configure the OSPF parameters based on the following:
  - o Template Name: BR-CSR-OSPF-VPNO
  - o Description: BR-CSR-OSPF-VPNO
- Area Configuration
  - o Area Number → Global: 0
  - o Area Type → Default
- Interface Configuration
  - o Interface Name: GigabitEthernet3
  - o OSPF Network Type: Point-to-Point
- Click Add to add the Interface and Click Add to add OSPF.
- Click Save to save the Template.





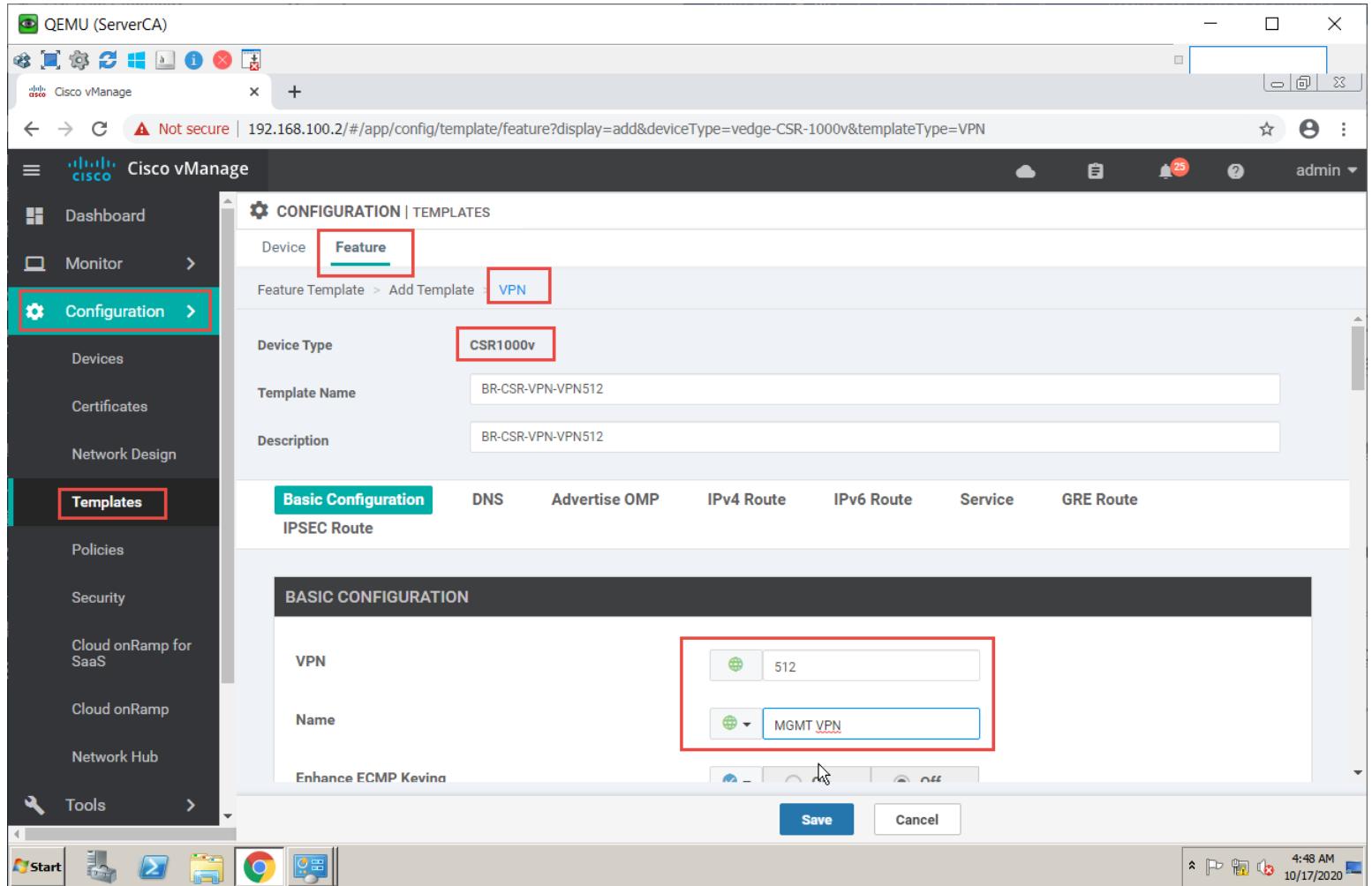
Name↑	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Action
BR-CSR-OSPF-VPN0	BR-CSR-OSPF-VPN0	OSPF	CSR1000v	0	0	admin	...
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	WAN Edge V...	CSR1000v	0	0	admin	...
BR-CSR-VPNINT-VPN0-G1	BR-CSR-VPNINT-VPN0-G1	WAN Edge In...	CSR1000v	0	0	admin	...
BR-CSR-VPNINT-VPN0-G3	BR-CSR-VPNINT-VPN0-G3	WAN Edge In...	CSR1000v	0	0	admin	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	admin	...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	admin	...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge V...	vEdge Cloud	1	3	admin	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge V...	vEdge Cloud	1	3	admin	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge V...	vEdge Cloud	1	3	admin	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge In...	vEdge Cloud	1	3	admin	...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge In...	vEdge Cloud	1	3	admin	...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge In...	vEdge Cloud	1	3	admin	...
BR-VF-VPNINT-VPN512-	BR-VF-VPNINT-VPN512-Fth0	WAN Edge In...	vEdge Cloud	1	3	admin	...

## VPN 512

### Task 1 – Configure a VPN Template to be used by CSR for VPN 512

- In vManage, Navigate to Configuration → Templates → Feature → CSR1000v → VPN → Cisco VPN
- Configure the VPN parameters based on the following:
  - o Template Name : BR-CSR-VPN-VPN512
  - o Description : BR-CSR-VPN-VPN512
  - o Basic Configuration
  - o VPN → Global : 512
  - o Name → Global : MGMT VPN
- Click Save to save the Template.





QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/#/app/config/template/feature?display=add&deviceType=vedge-CSR-1000v&templateType=VPN

admin

Configuration >

Templates

Devices

Certificates

Network Design

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Add Template **VPN**

Device Type **CSR1000v**

Template Name **BR-CSR-VPN-VPN512**

Description **BR-CSR-VPN-VPN512**

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

IPSEC Route

BASIC CONFIGURATION

VPN

Name **MGMT VPN**

Enhance ECMP Keiana

Save Cancel

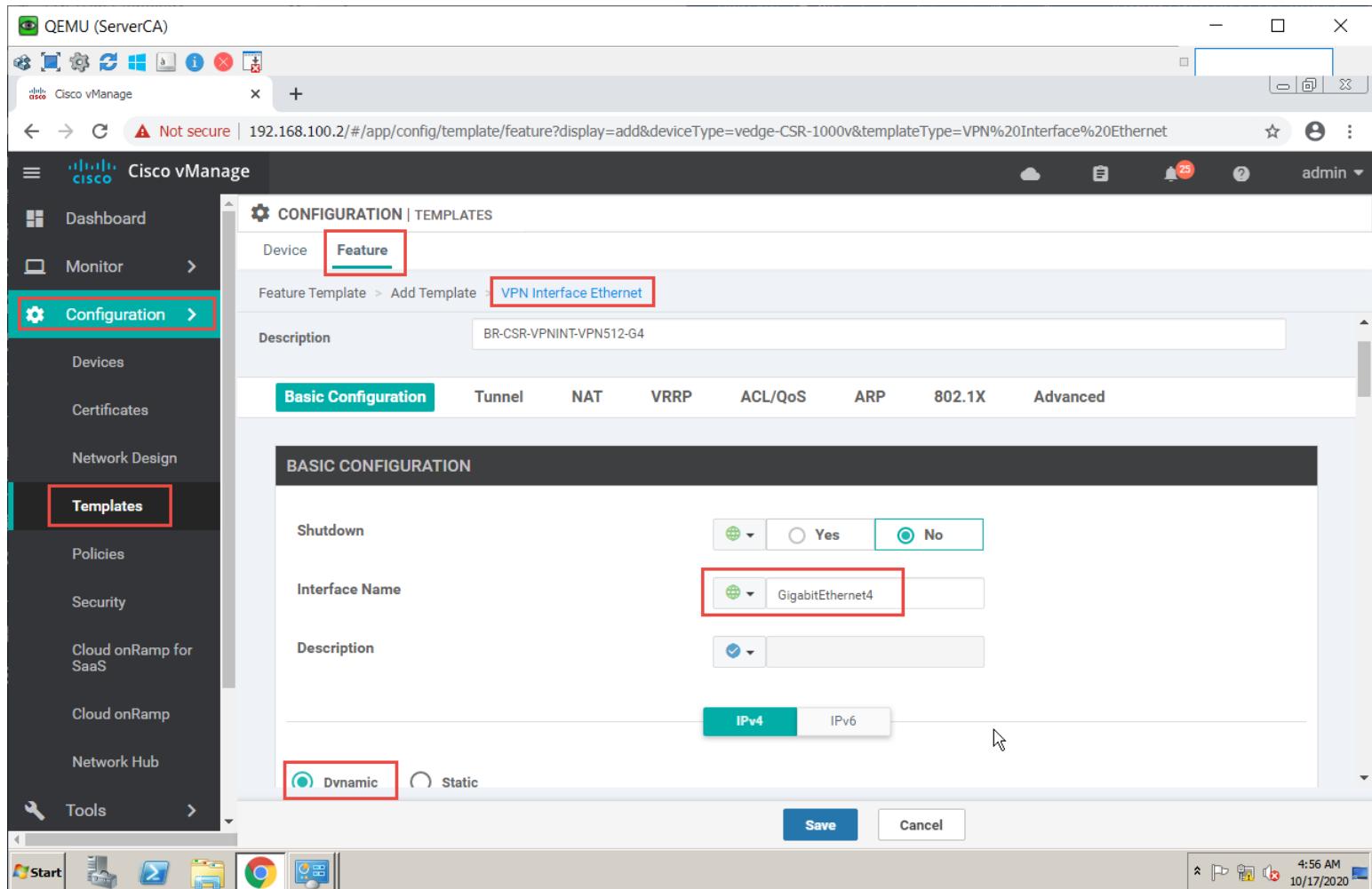
4:48 AM 10/17/2020



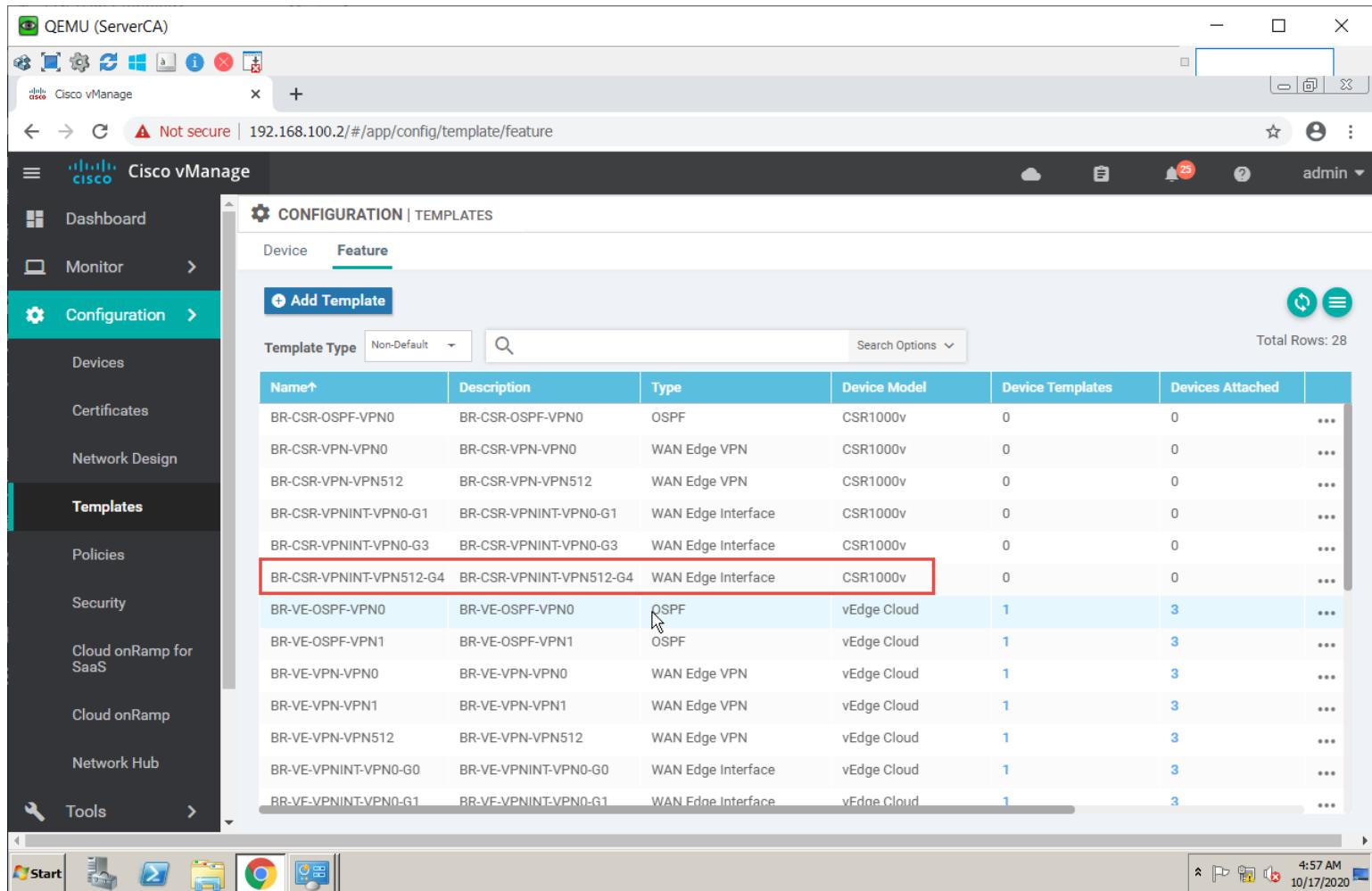
Name↑	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Actions
BR-CSR-OSPF-VPN0	BR-CSR-OSPF-VPN0	OSPF	CSR1000v	0	0	admin	...
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	WAN Edge VPN	CSR1000v	0	0	admin	...
BR-CSR-VPN-VPN512	BR-CSR-VPN-VPN512	WAN Edge VPN	CSR1000v	0	0	admin	...
BR-CSR-VPNINT-VP...	BR-CSR-VPNINT-VPN0-G1	WAN Edge Interf...	CSR1000v	0	0	admin	...
BR-CSR-VPNINT-VP...	BR-CSR-VPNINT-VPN0-G3	WAN Edge Interf...	CSR1000v	0	0	admin	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	admin	...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	admin	...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3	admin	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	admin	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	admin	...
BR-VE-VPNINT-VPN...	BR-VE-VPNINT-VPN0-G0	WAN Edge Interf...	vEdge Cloud	1	3	admin	...
BR-VE-VPNINT-VPN...	BR-VE-VPNINT-VPN0-G1	WAN Edge Interf...	vEdge Cloud	1	3	admin	...
BR-VF-VPNINT-VPN...	BR-VF-VPNINT-VPN1-G2	WAN Edge Interf...	vEdge Cloud	1	3	admin	...

## Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 512 for Interface GigabitEthernet4

- In vManage, Navigate to Configuration → Templates → Feature → CSR1000v → VPN → Cisco VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - o Template Name : BR-CSR-VPNINT-VPN512-G4
  - o Description : BR-CSR-VPNINT-VPN512-G4
- Basic Configuration
  - o Shutdown → Global: No
  - o Interface Name → Global: GigabitEthernet4
  - o IPv4 Address → Dynamic
- Click Save to save the Template



The screenshot shows the Cisco vManage web interface. The left sidebar is titled "Cisco vManage" and includes sections for Dashboard, Monitor, Configuration (which is selected and highlighted in red), Templates (also highlighted in red), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area is titled "CONFIGURATION | TEMPLATES" under "Device" and "Feature". A breadcrumb navigation bar indicates the path: Feature Template > Add Template > VPN Interface Ethernet. The "Basic Configuration" tab is selected. In the "BASIC CONFIGURATION" section, the "Interface Name" field is set to "GigabitEthernet4" and is highlighted with a red box. Below the interface name, there are tabs for "IPv4" and "IPv6", with "IPv4" selected. At the bottom of the configuration form, there are "Save" and "Cancel" buttons. The status bar at the bottom of the browser window shows the time as 4:56 AM and the date as 10/17/2020.

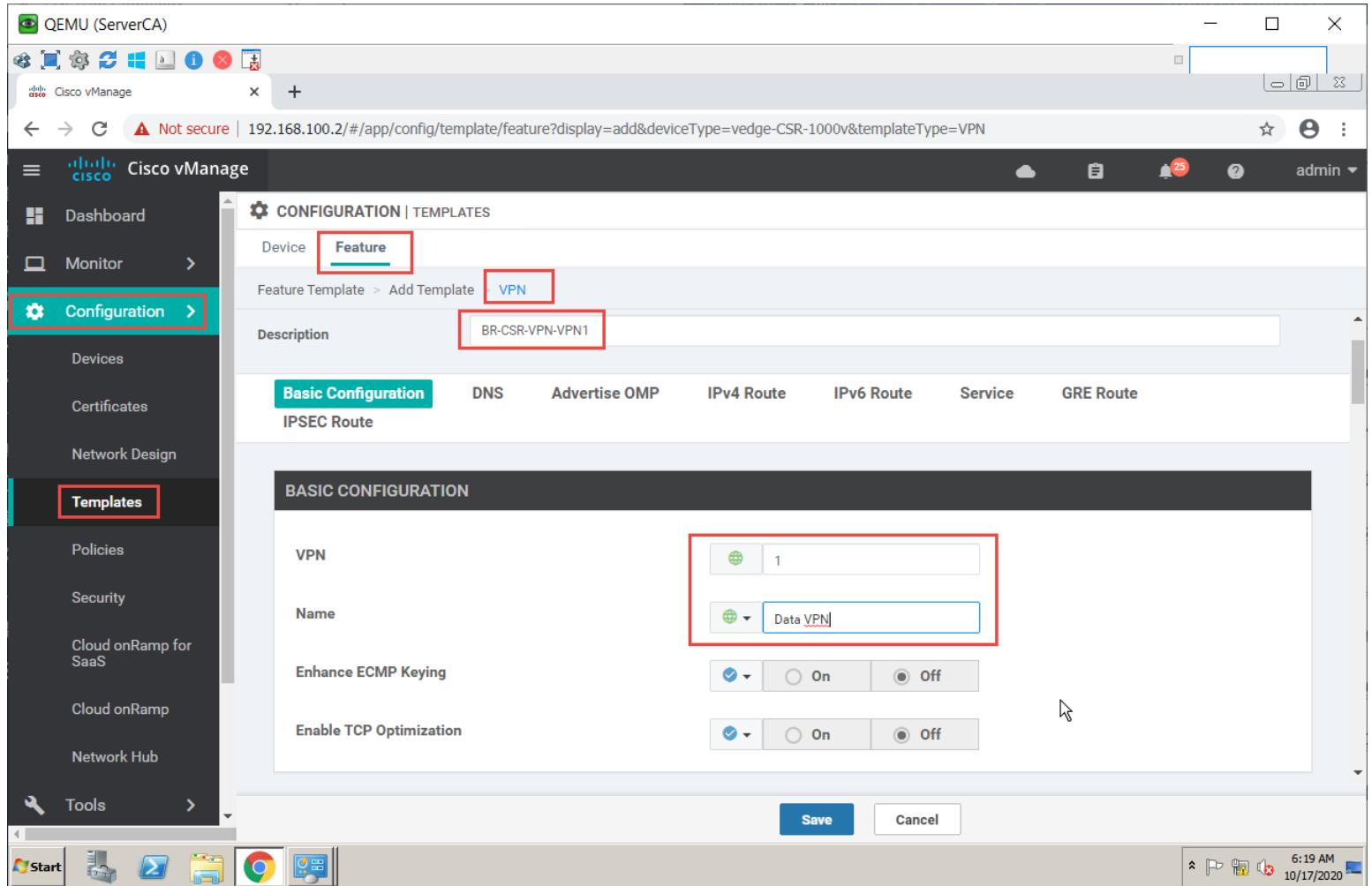


Name↑	Description	Type	Device Model	Device Templates	Devices Attached	...
BR-CSR-OSPF-VPN0	BR-CSR-OSPF-VPN0	OSPF	CSR1000v	0	0	...
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	WAN Edge VPN	CSR1000v	0	0	...
BR-CSR-VPN-VPN512	BR-CSR-VPN-VPN512	WAN Edge VPN	CSR1000v	0	0	...
BR-CSR-VPNINT-VPN0-G1	BR-CSR-VPNINT-VPN0-G1	WAN Edge Interface	CSR1000v	0	0	...
BR-CSR-VPNINT-VPN0-G3	BR-CSR-VPNINT-VPN0-G3	WAN Edge Interface	CSR1000v	0	0	...
BR-CSR-VPNINT-VPN512-G4	BR-CSR-VPNINT-VPN512-G4	WAN Edge Interface	CSR1000v	0	0	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	3	...
BR-VF-VPNINT-VPN0-G1	BR-VF-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3	...

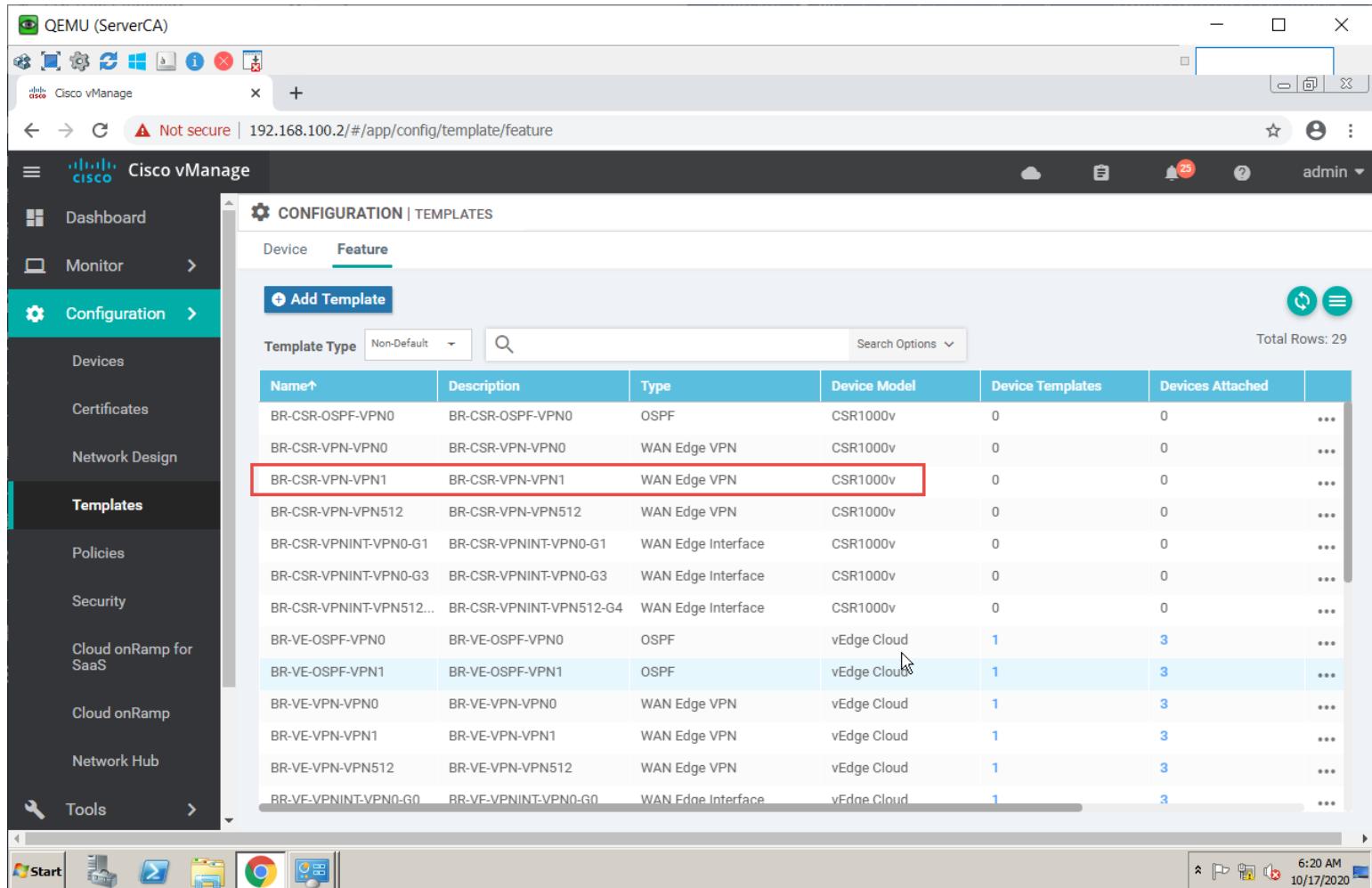
## VPN 1

### Task 1 – Configure a VPN Template for CSR for VPN 1

- In vManage, Navigate to Configuration → Templates → Feature → CSR1000v → VPN → Cisco VPN
- Configure the VPN parameters based on the following:
  - o Template Name : BR-CSR-VPN-VPN1
  - o Description : BR-CSR-VPN-VPN1
- Basic Configuration
  - o VPN → Global : 1
  - o Name → Global : Data VPN
- Click Save to save the Template.



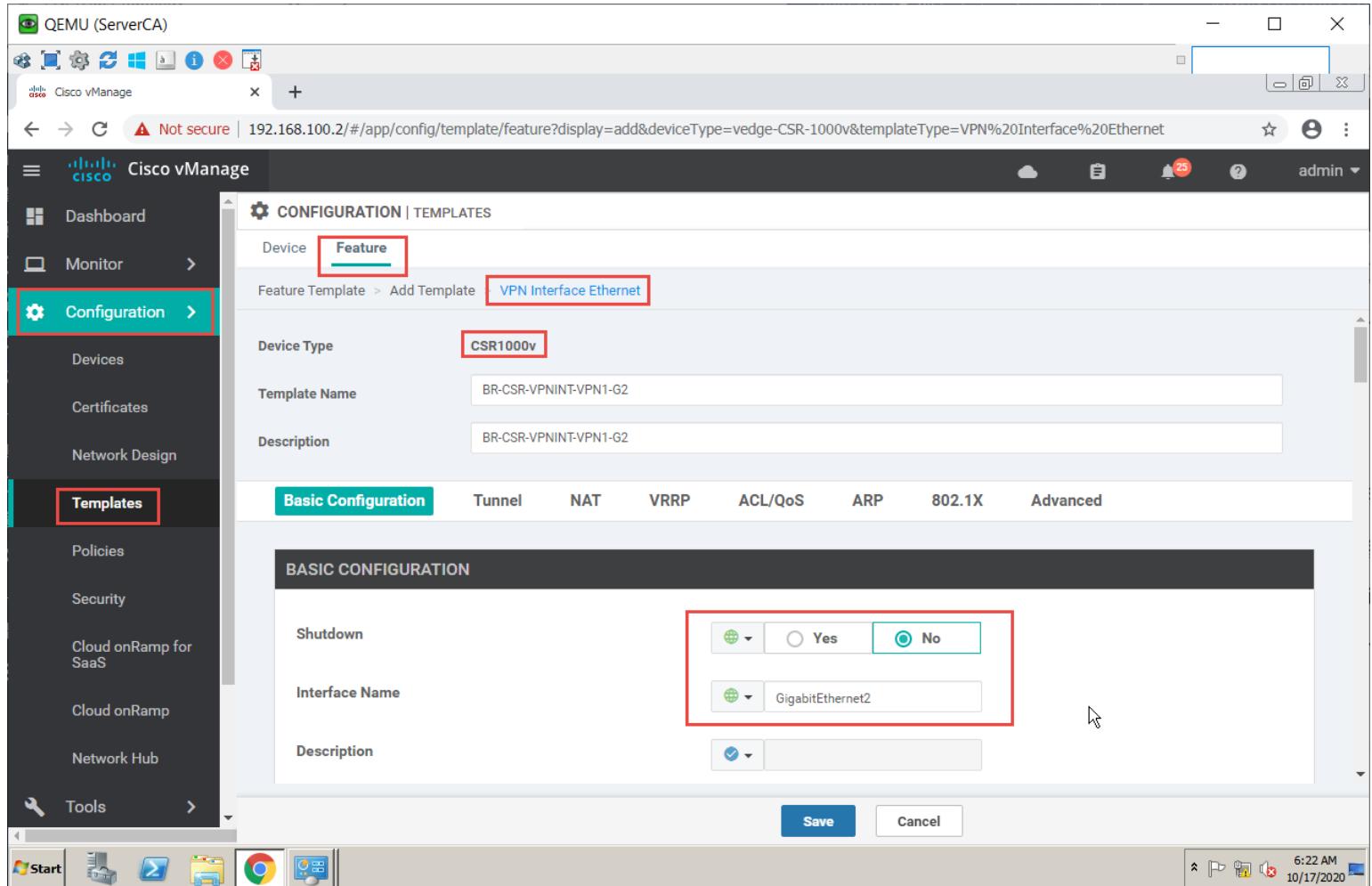
The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing various management categories like Dashboard, Monitor, Configuration, Templates (which is selected), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. The main content area is titled "CONFIGURATION | TEMPLATES". It shows a breadcrumb path: Feature Template > Add Template > VPN. A new template is being created with the description "BR-CSR-VPN-VPN1". The "Basic Configuration" tab is active, displaying settings for a VPN connection. The "Name" field contains "Data VPN" and is highlighted with a red box. Other visible tabs include DNS, Advertise OMP, IPv4 Route, IPv6 Route, Service, and GRE Route. At the bottom right of the configuration window are "Save" and "Cancel" buttons.



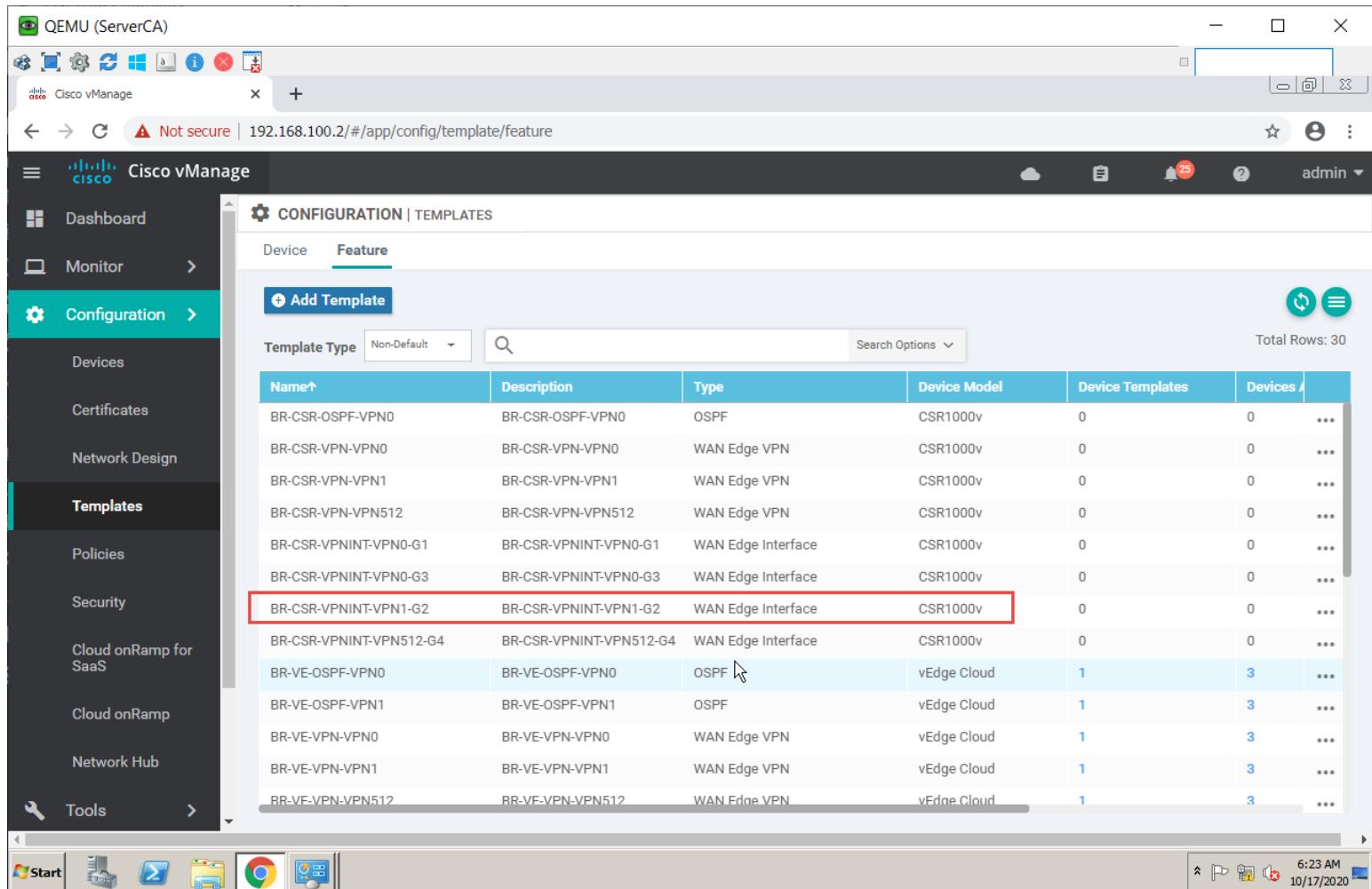
Name↑	Description	Type	Device Model	Device Templates	Devices Attached	...
BR-CSR-OSPF-VPN0	BR-CSR-OSPF-VPN0	OSPF	CSR1000v	0	0	...
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	WAN Edge VPN	CSR1000v	0	0	...
BR-CSR-VPN-VPN1	BR-CSR-VPN-VPN1	WAN Edge VPN	CSR1000v	0	0	...
BR-CSR-VPN-VPN512	BR-CSR-VPN-VPN512	WAN Edge VPN	CSR1000v	0	0	...
BR-CSR-VPNINT-VPN0-G1	BR-CSR-VPNINT-VPN0-G1	WAN Edge Interface	CSR1000v	0	0	...
BR-CSR-VPNINT-VPN0-G3	BR-CSR-VPNINT-VPN0-G3	WAN Edge Interface	CSR1000v	0	0	...
BR-CSR-VPNINT-VPN512-G4	BR-CSR-VPNINT-VPN512-G4	WAN Edge Interface	CSR1000v	0	0	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	...
BR-VF-VPNINT-VPN0-G0	BR-VF-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	3	...

## Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 1 for Interface G2

- In vManage, Navigate to Configuration → Templates → Feature → CSR → VPN → Cisco VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - o Template Name : BR-CSR-VPNINT-VPN1-G2
  - o Description : BR-CSR-VPNINT-VPN1-G2
- Basic Configuration
  - o Shutdown → Global : No
  - o Interface Name → Global : GigabitEthernet2
  - o IPv4 Address → Static -> Device Specific
- Click Save to save the Template.



The screenshot shows the Cisco vManage web interface. The left sidebar is open, revealing sections like Dashboard, Monitor, Configuration (which is selected and highlighted in red), Templates (also highlighted in red), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, and Tools. The main content area is titled "CONFIGURATION | TEMPLATES" under "Feature". A sub-tutorial bar at the top says "Feature Template > Add Template" with "VPN Interface Ethernet" highlighted in red. The "Device Type" is set to "CSR1000v". The "Template Name" is "BR-CSR-VPNINT-VPN1-G2" and the "Description" is "BR-CSR-VPNINT-VPN1-G2". The "Basic Configuration" tab is active, showing fields for "Shutdown" (radio button set to "No") and "Interface Name" (set to "GigabitEthernet2"). The "Save" and "Cancel" buttons are at the bottom right of the configuration panel.



Name↑	Description	Type	Device Model	Device Templates	Devices
BR-CSR-OSPF-VPN0	BR-CSR-OSPF-VPN0	OSPF	CSR1000v	0	0
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	WAN Edge VPN	CSR1000v	0	0
BR-CSR-VPN-VPN1	BR-CSR-VPN-VPN1	WAN Edge VPN	CSR1000v	0	0
BR-CSR-VPN-VPN512	BR-CSR-VPN-VPN512	WAN Edge VPN	CSR1000v	0	0
BR-CSR-VPNINT-VPN0-G1	BR-CSR-VPNINT-VPN0-G1	WAN Edge Interface	CSR1000v	0	0
BR-CSR-VPNINT-VPN0-G3	BR-CSR-VPNINT-VPN0-G3	WAN Edge Interface	CSR1000v	0	0
BR-CSR-VPNINT-VPN1-G2	BR-CSR-VPNINT-VPN1-G2	WAN Edge Interface	CSR1000v	0	0
BR-CSR-VPNINT-VPN512-G4	BR-CSR-VPNINT-VPN512-G4	WAN Edge Interface	CSR1000v	0	0
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3
BR-VF-VPN-VPN512	BR-VF-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3

### Task 3 – Configure a OSPF Template to be used by CSR for VPN 1

- In vManage, Navigate to Configuration → Templates → Feature → CSR1000v → Other Templates → Cisco OSPF
- Configure the OSPF parameters based on the following:
  - o Template Name : BR-CSR-OSPF-VPN1
  - o Description : BR-CSR-OSPF-VPN1
- Redistribution
  - o Protocol : OMP
- Area Configuration
  - o Area Number → Global : 0
  - o Area Type → Default
- Interface Configuration
  - o Interface Name: GigabitEthernet2
- Click Add to add the Interface and Click Add to add OSPF.
- Click Save to save the Template.

QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/#/app/config/template/feature?display=add&deviceType=vedge-CS1000v&templateType=OSPF

admin

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Add Template : OSPF

Basic Configuration    Redistribution    Maximum Metric (Router LSA)    Area    Advanced

Distance for Inter-Area Routes: 110

Distance for Intra-Area Routes: 110

REDISTRIBUTE

+ New Redistribute

Optional	Protocol	Route Policy	Action
<input type="checkbox"/>	 ospf	<input checked="" type="checkbox"/>	 

Save    Cancel

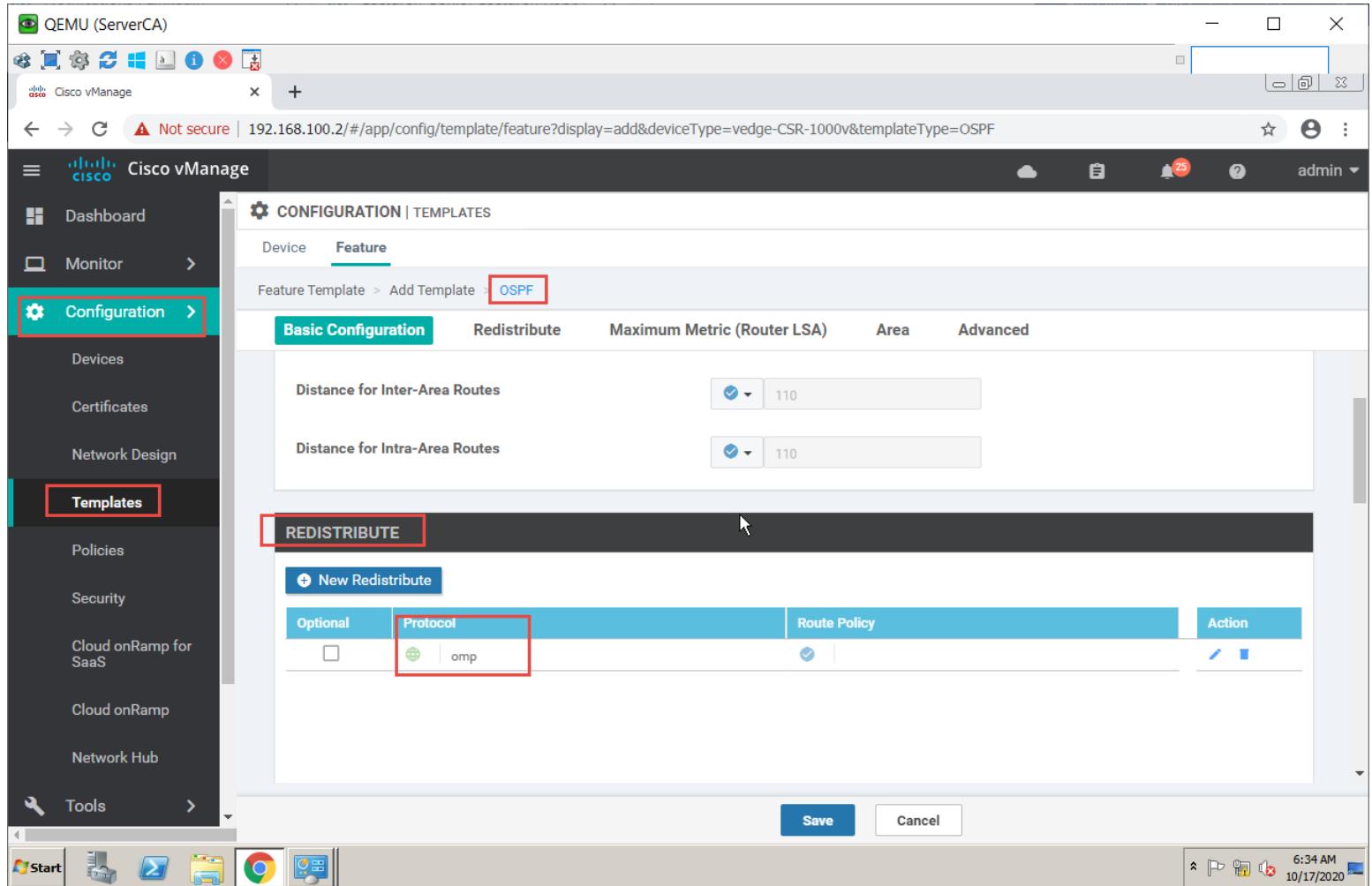
6:34 AM 10/17/2020

Templates

Devices  
Certificates  
Network Design  
Policies  
Security  
Cloud onRamp for SaaS  
Cloud onRamp  
Network Hub

Tools

Start

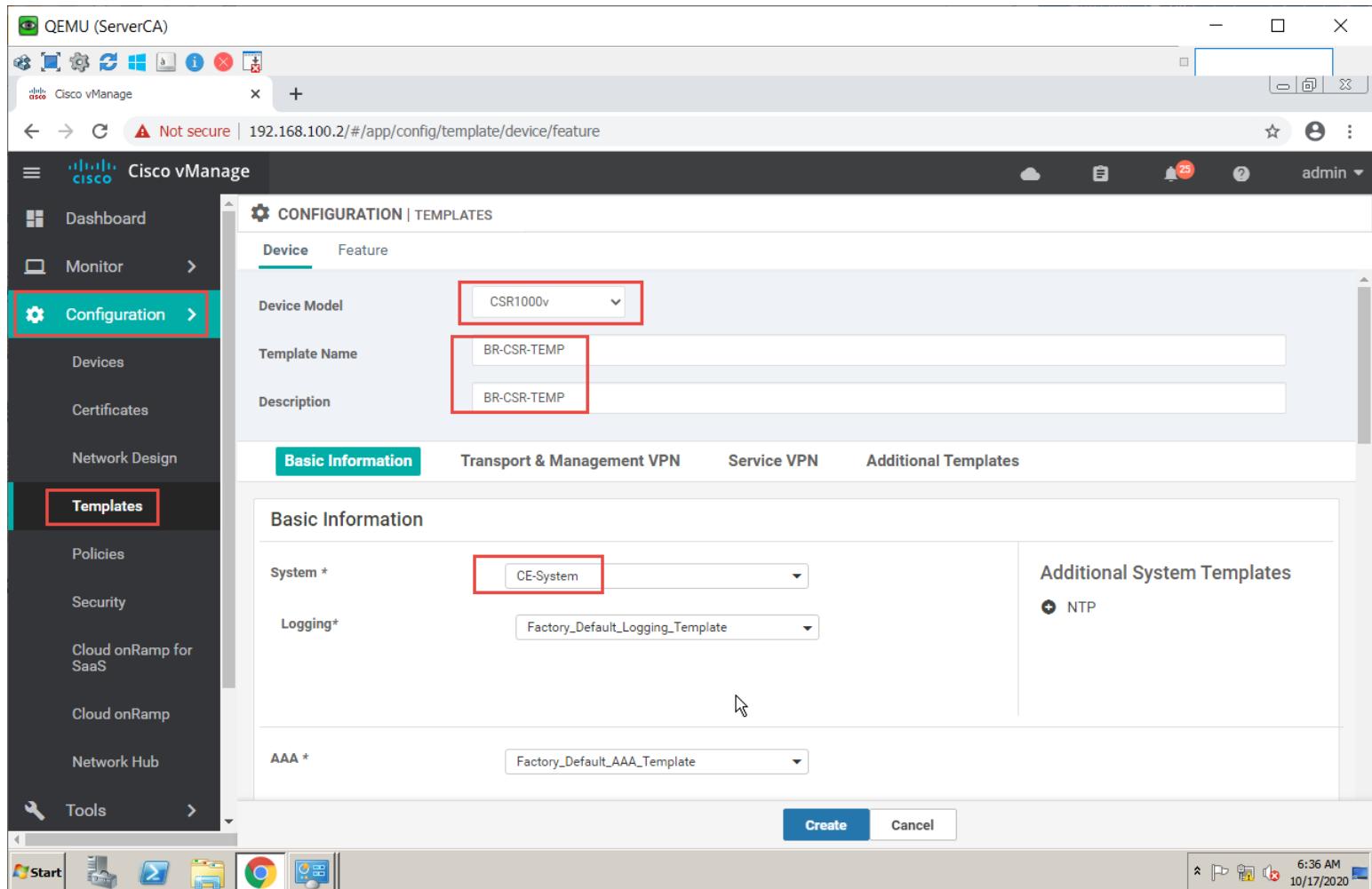




## Lab 25 - Configuring Device Templates for CSR to deploy VPN 0, 1 and 512

### Task 1 – Configure a Device Template for CSR Branch Devices.

- In vManage, Navigate to Configuration → Templates → Device → Create Template → CSR1000v
  - Configure the Device Template based on the following:
    - o Template Name : BR-CSR-TEMP
    - o Description : BR-CSR-TEMP
- Basic Information
- o System → CE-System
- Transport & Management
- o VPN 0 : BR-CSR-VPN-VPNO
  - o VPN Interface : BR-CSR-VPNINT-VPN0-G1
  - o VPN Interface : BR-CSR-VPNINT-VPN0-G3
  - o OSPF : BR-CSR-OSPF-VPNO
  - o VPN 512 : BR-CSR-VPN-VPN512
  - o VPN Interface : BR-CSR-VPNINT-VPN512-G4
- Service VPN
- o VPN 1 : BR-CSR-VPN-VPN1
  - o VPN Interface : BR-CSR-VPNINT-VPN1-G2
  - o OSPF : BR-CSR-OSPF-VPN1
- Click Save to save the Template.

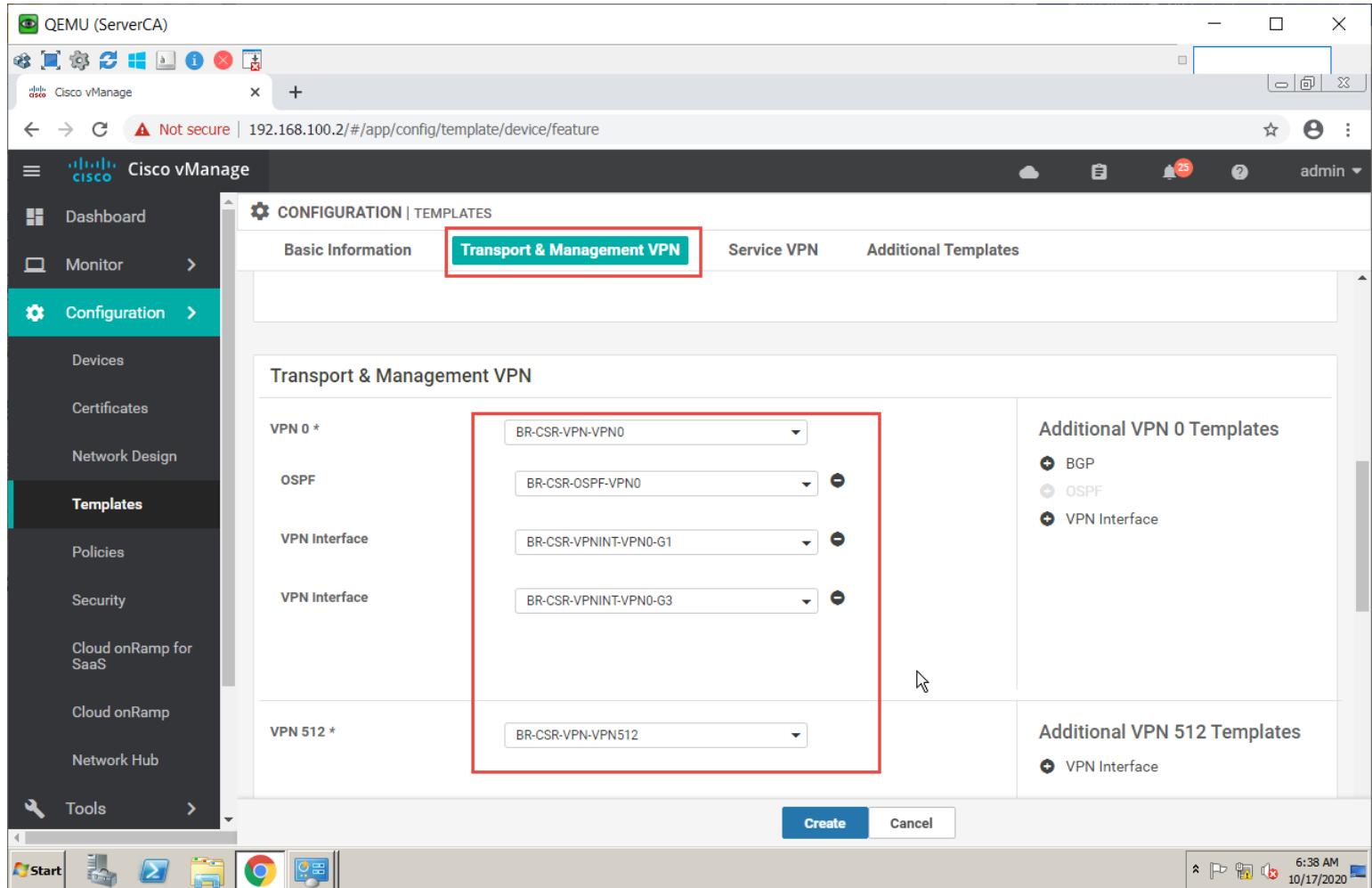


The screenshot shows the Cisco vManage web interface. The left sidebar is open, showing various management tabs like Dashboard, Monitor, Configuration, Templates (which is selected and highlighted with a red border), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. Below the sidebar is a Windows taskbar with icons for Start, File Explorer, Task View, and Google Chrome.

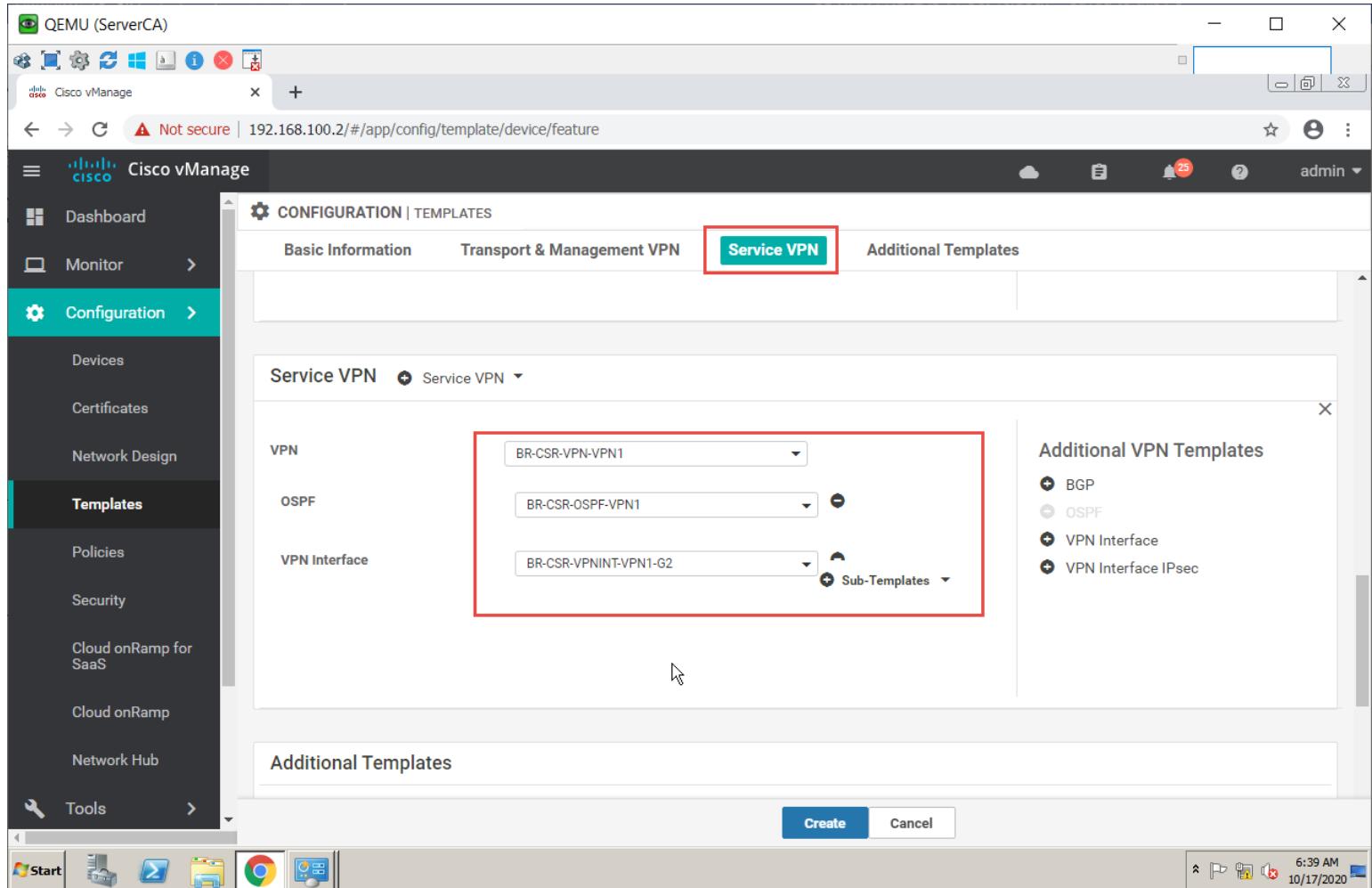
The main content area is titled "CONFIGURATION | TEMPLATES". It has two tabs: "Device" (selected) and "Feature". Under "Device", there are fields for "Device Model" (set to "CSR1000v"), "Template Name" (set to "BR-CSR-TEMP"), and "Description" (also set to "BR-CSR-TEMP"). Below these are four tabs: "Basic Information" (selected), "Transport & Management VPN", "Service VPN", and "Additional Templates".

In the "Basic Information" section, there are three dropdown menus: "System \*" (set to "CE-System"), "Logging\*" (set to "Factory\_Default\_Logging\_Template"), and "AAA \*" (set to "Factory\_Default\_AAA\_Template"). To the right of these dropdowns is a panel titled "Additional System Templates" which includes a "+ NTP" button.

At the bottom of the configuration window are "Create" and "Cancel" buttons.



The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Configuration' and includes options like 'Devices', 'Certificates', 'Network Design', 'Templates' (which is selected), 'Policies', 'Security', 'Cloud onRamp for SaaS', 'Cloud onRamp', and 'Network Hub'. The top navigation bar shows 'Cisco vManage' and the URL '192.168.100.2/#/app/config/template/device/feature'. The main content area is titled 'CONFIGURATION | TEMPLATES' and has tabs for 'Basic Information', 'Transport & Management VPN' (which is highlighted with a red box), 'Service VPN', and 'Additional Templates'. The 'Transport & Management VPN' tab displays a form with sections for 'VPN 0 \*', 'OSPF', 'VPN Interface', and 'VPN 512 \*'. Each section contains dropdown menus with specific template names. To the right of the form are two columns: 'Additional VPN 0 Templates' and 'Additional VPN 512 Templates', each with a '+' icon to add more templates. At the bottom of the form are 'Create' and 'Cancel' buttons.



The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Configuration' and includes options like 'Devices', 'Certificates', 'Network Design', 'Templates' (which is selected), 'Policies', 'Security', 'Cloud onRamp for SaaS', 'Cloud onRamp', 'Network Hub', and 'Tools'. The main content area has a title 'CONFIGURATION | TEMPLATES' and tabs for 'Basic Information', 'Transport & Management VPN', and 'Service VPN' (which is highlighted with a red box). Below these tabs, there's a section for 'Service VPN' with dropdown menus for 'VPN' (set to 'BR-CSR-VPN-VPN1'), 'OSPF' (set to 'BR-CSR-OSPF-VPN1'), and 'VPN Interface' (set to 'BR-CSR-VPNINT-VPN1-G2'). To the right, there's a sidebar titled 'Additional VPN Templates' with icons for BGP, OSPF, VPN Interface, and VPN Interface IPsec. At the bottom of the configuration window are 'Create' and 'Cancel' buttons.



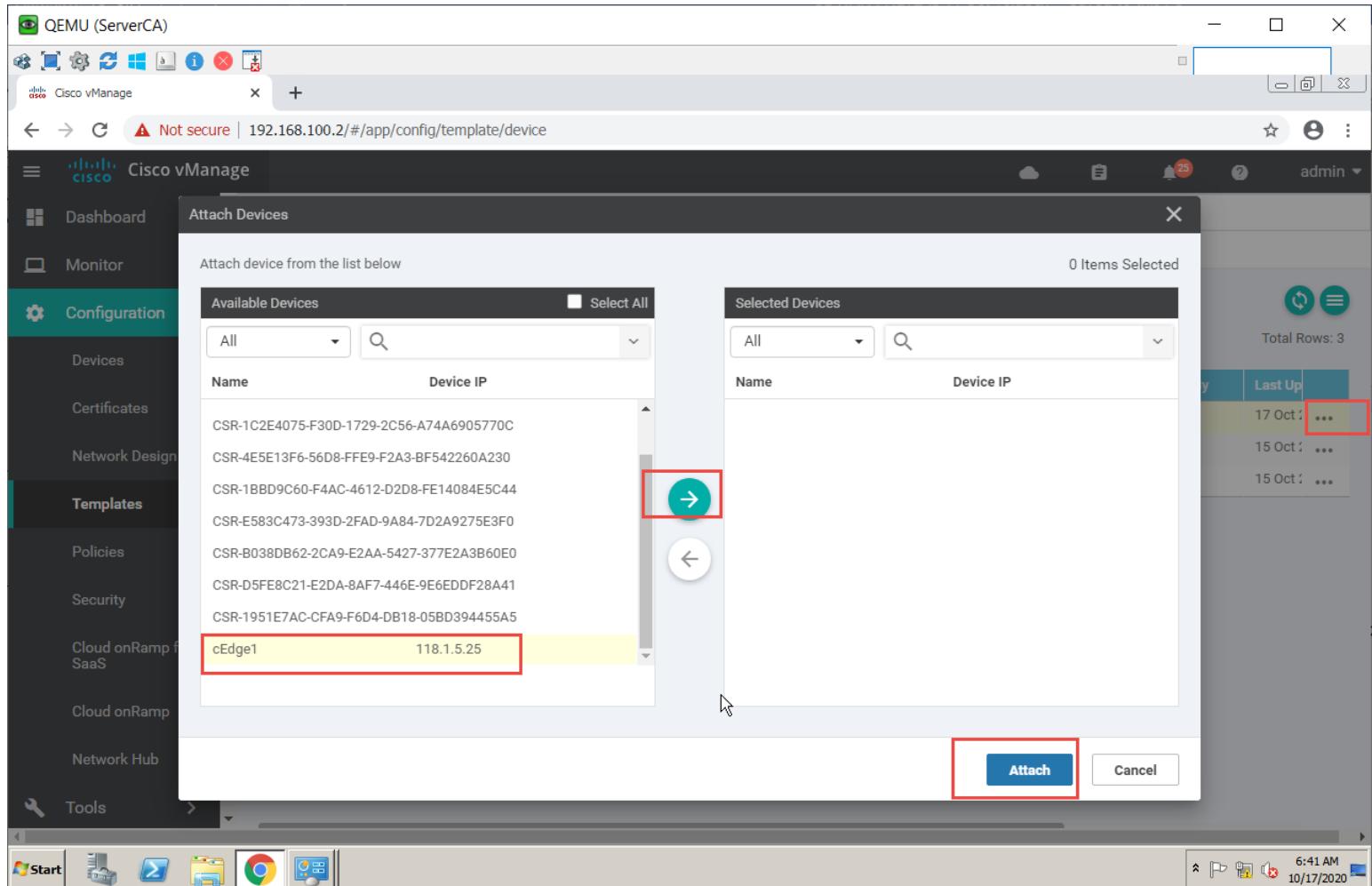
The screenshot shows the Cisco vManage web interface. The URL in the address bar is <https://192.168.100.2/#/app/config/template/device>. The left sidebar has a 'Configuration' section with several options: Devices, Certificates, Network Design, **Templates**, Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, and Network Hub. The 'Templates' option is highlighted with a red box. The main content area is titled 'CONFIGURATION | TEMPLATES' and has a 'Device' tab selected, indicated by a red box. Below it is a 'Feature' tab. A 'Create Template' button is visible. A search bar and search options are present. A table lists three templates:

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Up
BR-CSR-TEMP	BR-CSR-TEMP	Feature	CSR1000v	15	0	admin	17 Oct 1 ...
BR-VE-TEMP	BR-VE-TEMP	Feature	vEdge Cloud	16	3	admin	15 Oct 1 ...
HQ-VE-TEMP	HQ-VE-TEMP	Feature	vEdge Cloud	14	1	admin	15 Oct 1 ...

Total Rows: 3

## Task 2 – Attach cEdge1 to the Device Template

- In vManage, Navigate to Configuration → Templates → Device → BRCSR-TEMP.
- Click on “...” towards the right-hand side.
- Click Attach Devices.
- Select cEdge1 and click the “➔” button.
- Click Attach.



### Task 3 – Configure the Variable Parameters for the Feature Templates

- cEdge1 will appear in the window.
- Click on “...” towards the right-hand side.
- Click Edit Device Template.
- Configure the variables based on the following:
  - o Interface IP for GigabitEthernet3: 10.1.15.1/24
  - o Default Gateway for VPNO: 118.1.5.2
  - o Interface IP for GigabitEthernet2: 172.175.1.1/24
  - o Interface IP for GigabitEthernet1: 118.1.5.1/24
  - o Hostname: cEdge-1
  - o System IP: 118.1.5.25
  - o Site ID: 5
- Click Update.
- Verify the Configuration & Click Configure Devices.
- Wait for it to update the device. It should come back with Status of Success.



- Verify the configuration on cEdge1. You can do that by verify OSPF Neighbor relationship with the Internal Router by issuing the Show ip ospf neighbor command on cEdge1.
- Type Show Ip route on cEdge1 to verify that you are receiving OSPF routes from the MPLS Router.
- Type Show Ip route on Internal Site Routers to verify that you are receiving OSPF routes from the other Sites.
- Verify reachability between the sites by Pinging the Internal Loopback to Loopback networks.

The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Cisco vManage' and includes 'Dashboard', 'Monitor', 'Configuration' (which is selected), 'Devices', 'Certificates', 'Network Design', 'Templates' (selected), 'Policies', 'Security', 'Cloud onRamp for SaaS', 'Cloud onRamp', and 'Network Hub'. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows a table for 'Device Template'. The table has columns: S..., Chassis Number, System IP, Hostname, IPv4 Address(vpn\_if\_ipv4\_address), and Address(vpn\_i...). A single row is visible: CSR-6BD335E2-5434-26B7-0987-F0C935526... (Chassis Number), 118.1.5.25 (System IP), cEdge1 (Hostname). The entire row is highlighted with a red box. At the bottom right of the table are 'Next' and 'Cancel' buttons, with 'Next' also highlighted with a red box. The top status bar shows 'QEMU (ServerCA)' and the URL '192.168.100.2/#/app/config/template/device/configure/0beadd36-9575-4603-bb8f-930acf1cdf3b'. The top right corner shows the user 'admin'.

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/#/app/config/template/device/configure/0beadd36-9575-4603-bb8f-930acf1cdf3b

Cisco vManage

Dashboard

Monitor

Configuration

Devices

Certificates

Network Design

**Templates**

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

CONFIGURATION | TEMPLATES

Device Template | BR-CSR-TEMP

Search Options

Total Rows: 1

S...	Chassis Number	System IP	Hostname	IPv4 Address(vpn_if.ipv4_address)	Address(vpn_if.ipv4_address)
CSR-6BD335E2-5434-26B7-0987-F0C935526...	118.1.5.25	cEdge1			

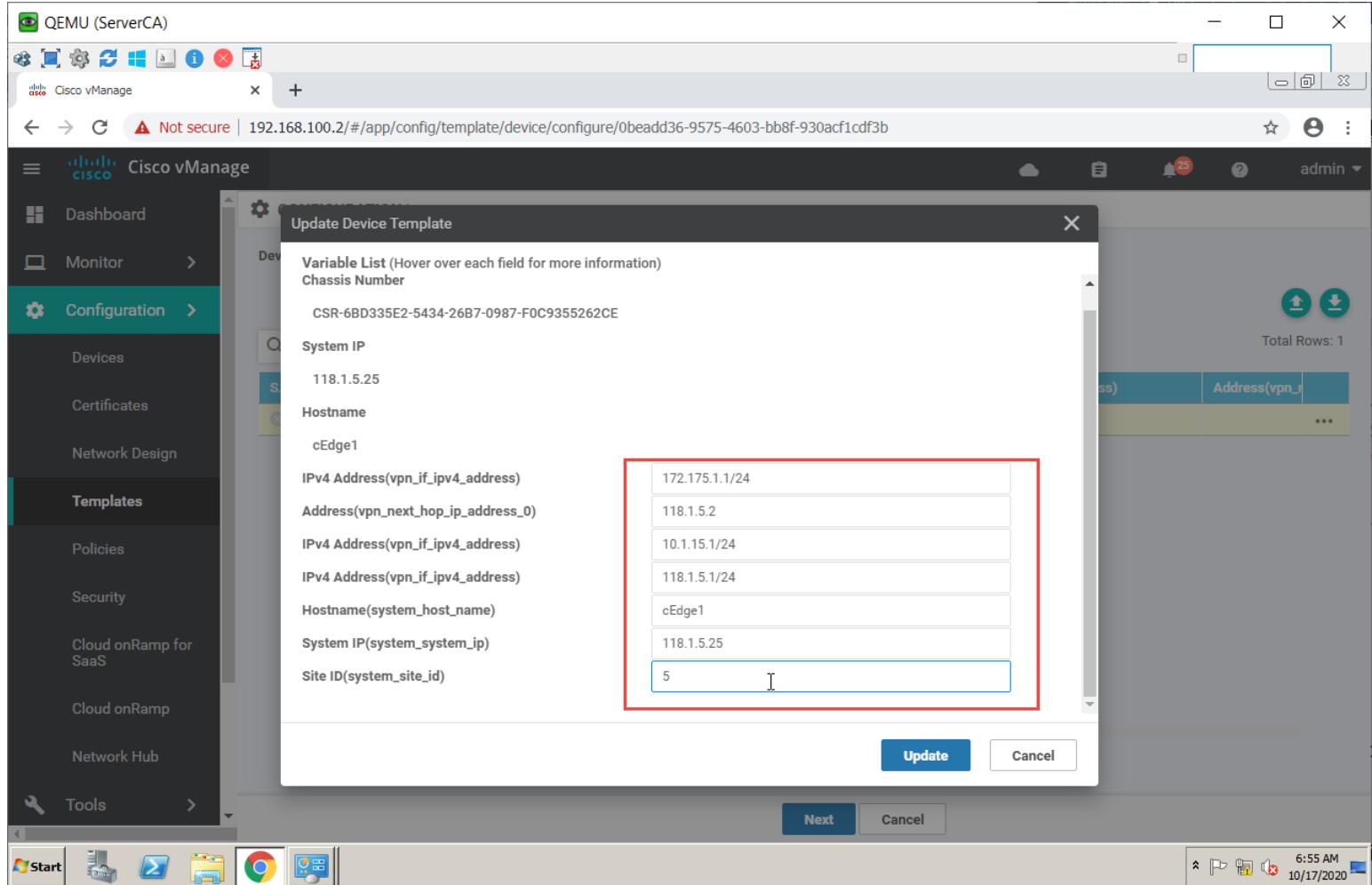
Edit Device Template

Next Cancel

Start

6:53 AM 10/17/2020

A screenshot of the Cisco vManage web interface. The left sidebar shows navigation links like Configuration, Templates (which is selected), Policies, and Security. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows a table for a 'Device Template' named 'BR-CSR-TEMP'. The table has columns for Chassis Number, System IP, Hostname, IPv4 Address, and Address. One row is visible with the chassis number 'CSR-6BD335E2-5434-26B7-0987-F0C935526...', system IP '118.1.5.25', hostname 'cEdge1', and empty address fields. To the right of the table is a 'Total Rows: 1' message. At the bottom right of the table is a red box around a button labeled 'Edit Device Template'. Below the table are 'Next' and 'Cancel' buttons. The bottom of the screen shows a Windows taskbar with icons for Start, File Explorer, Task View, and Google Chrome, along with system status icons like battery level and date/time.



QEMU (ServerCA)

Cisco vManage

Not secure | 192.168.100.2/#/app/config/template/device/configure/0beadd36-9575-4603-bb8f-930acf1cdf3b

admin

Dashboard

Monitor

Configuration

Devices

Certificates

Network Design

Templates

Policies

Security

Cloud onRamp for SaaS

Cloud onRamp

Network Hub

Tools

Update Device Template

Variable List (Hover over each field for more information)

Chassis Number

CSR-6BD335E2-5434-26B7-0987-F0C9355262CE

System IP

118.1.5.25

Hostname

cEdge1

IPv4 Address(vpn\_if\_ipv4\_address)

Address(vpn\_next\_hop\_ip\_address\_0)

IPv4 Address(vpn\_if\_ipv4\_address)

IPv4 Address(vpn\_if\_ipv4\_address)

Hostname(system\_host\_name)

System IP(system\_system\_ip)

Site ID(system\_site\_id)

172.175.1.1/24

118.1.5.2

10.1.15.1/24

118.1.5.1/24

cEdge1

118.1.5.25

5

Total Rows: 1

Update Cancel

Next Cancel

6:55 AM 10/17/2020



cEdge-1#

cEdge-1#show ip route vrf 1

Routing Table: 1

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

```
172.172.0.0/24 is subnetted, 1 subnets
m      172.172.1.0 [251/0] via 118.1.2.22, 00:04:51
172.175.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.175.1.0/24 is directly connected, GigabitEthernet2
L      172.175.1.1/32 is directly connected, GigabitEthernet2
m      192.168.21.0/24 [251/0] via 118.1.2.22, 00:04:51
m      192.168.22.0/24 [251/0] via 118.1.2.22, 00:04:51
m      192.168.23.0/24 [251/0] via 118.1.2.22, 00:04:51
      192.168.234.0/32 is subnetted, 1 subnets
m      192.168.234.2 [251/0] via 118.1.2.22, 00:04:51
```

cEdge-1#

cEdge-1#

cEdge-1#

cEdge-1#ping vrf 1 192.168.21.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/3 ms

cEdge-1#





Site-5

```
*Nov 1 04:03:24.772: %SYS-5-CONFIG_I: Configured from console by console
Site-5#show ip route
Codes: L - local, C - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      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
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override

Gateway of last resort is not set

      172.172.0.0/24 is subnetted, 1 subnets
O E2    172.172.1.0 [110/16777214] via 172.175.1.1, 00:00:00, Ethernet0/0
      172.175.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.175.1.0/24 is directly connected, Ethernet0/0
L       172.175.1.2/32 is directly connected, Ethernet0/0
O E2    192.168.21.0/24 [110/16777214] via 172.175.1.1, 00:00:00, Ethernet0/0
O E2    192.168.22.0/24 [110/16777214] via 172.175.1.1, 00:00:00, Ethernet0/0
O E2    192.168.23.0/24 [110/16777214] via 172.175.1.1, 00:00:00, Ethernet0/0
      192.168.51.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.51.0/24 is directly connected, Loopback1
L       192.168.51.1/32 is directly connected, Loopback1
      192.168.52.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.52.0/24 is directly connected, Loopback2
L       192.168.52.1/32 is directly connected, Loopback2
      192.168.53.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.53.0/24 is directly connected, Loopback3
L       192.168.53.1/32 is directly connected, Loopback3
      192.168.234.0/32 is subnetted, 1 subnets
O E2    192.168.234.2 [110/16777214] via 172.175.1.1, 00:00:00, Ethernet0/0
Site-5#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Site-5#
```





## Lab 26 - Configuring and Deploying Feature and Device Templates for vSmart Controllers

### Task 1 – Configure a VPN Template to be used by vSmart Controllers for VPN 0

- In vManage, Navigate to Configuration → Templates → Feature → vSmart → VPN → VPN
- Configure the VPN parameters based on the following:
  - o Template Name: vSmart-VPN-VPN0
  - o Description: vSmart-VPN-VPN0

#### Basic Configuration

- o VPN → Global: 0
- o Name → Global : Transport VPN

#### IPv4 Route

- o Prefix → Global: 0.0.0.0/0
- o Next Hop → Global: 100.1.1.1

- Click Save to save the Template.

The screenshot shows the Cisco vManage web interface. The left sidebar is collapsed. The main navigation bar has 'Cisco vManage' at the top, followed by 'Not secure | 192.168.100.2/#/app/config/template/feature?display=edit&templateId=86279100-0176-4eea-b92c-5276435decf0&templateType=vpn-vsmar'. The 'Configuration' tab is selected. Under 'TEMPLATES', 'Feature' is selected. A red box highlights the 'Feature Template > VPN - vSmart-VPN-VPN0' path. The 'Device Type' is set to 'vSmart'. The 'Template Name' is 'vSmart-VPN-VPN0' and the 'Description' is 'vSmart-VPN-VPN0'. The 'Basic Configuration' tab is active, showing the 'BASIC CONFIGURATION' section with 'VPN' set to 'VPN 0' and 'Name' set to 'Transport VPN'. The 'DNS' section shows 'Primary DNS Address' and a 'New Host Mapping' button. The 'Optional' tab is selected in the host mapping table, which is currently empty. At the bottom right are 'Update' and 'Cancel' buttons. The status bar at the bottom shows '8:14 AM 11/1/2020'.



Not secure | 192.168.100.2/#/app/config/template/feature

Cisco vManage

Dashboard >

Monitor >

Configuration > 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

Tools >

Maintenance >

Administration >

vAnalytics >

CONFIGURATION | TEMPLATES

Device Feature

Add Template

Template Type Non-Default

Search Options

Total Rows: 31

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	...
HQ-VE-OSPF-VPN1	HQ-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	1	admin	30 Oct 2020 1:21:10 PM ADT	...
BR-CSR-VPN-VPN512	BR-CSR-VPN-VPN512	Cisco VPN	CSR1000v	1	1	admin	01 Nov 2020 12:01:51 AM ADT	...
VE-System	VE-System	WAN Edge System	vEdge Cloud	2	4	admin	29 Oct 2020 10:30:04 PM ADT	...
CE-Banner	CE-Banner	Cisco Banner	CSR1000v	0	0	admin	29 Oct 2020 10:37:53 PM ADT	...
HQ-VE-VPNINT-VPN1-02	HQ-VE-VPNINT-VPN1-02	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:47:58 PM ADT	...
BR-CSR-VPNINT-VPN512-G4	BR-CSR-VPNINT-VPN512-G4	Cisco VPN Interface Ethernet	CSR1000v	1	1	admin	01 Nov 2020 12:03:08 AM ADT	...
CE-System	CE-System	Cisco System	CSR1000v	1	1	admin	29 Oct 2020 10:31:56 PM ADT	...
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	admin	29 Oct 2020 10:36:50 PM ADT	...
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3	admin	29 Oct 2020 10:39:55 PM ADT	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	admin	29 Oct 2020 10:40:53 PM ADT	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:45:51 PM ADT	...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:49:25 PM ADT	...
BR-VE-VPNINT-VPN512-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:51:24 PM ADT	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	admin	29 Oct 2020 11:00:30 PM ADT	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	admin	30 Oct 2020 5:27:27 AM ADT	...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3	admin	30 Oct 2020 5:28:24 AM ADT	...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	admin	30 Oct 2020 5:31:07 AM ADT	...
<b>vSmart-VPN-VPN0</b>	<b>vSmart-VPN-VPN0</b>	<b>vSmart VPN</b>	<b>vSmart</b>	0	0	admin	01 Nov 2020 4:13:42 AM AST	...
HQ-VE-VPNINT-VPN512-E0	HQ-VE-VPNINT-VPN512-E0	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:17:24 PM ADT	...
HQ-VE-VPNINT-VPN0-G0	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:11:01 PM ADT	...
HQ-VE-BGP-VPN0	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	1	1	admin	30 Oct 2020 1:13:14 PM ADT	...
HQ-VE-VPN-VPN1	HQ-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:18:27 PM ADT	...
HQ-VE-VPN-VPN512	HQ-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:13:56 PM ADT	...

Start

8:14 AM  
11/1/2020

## Task 2 – Configure a VPN Template to be used by vSmart Controllers for VPN 512

- In vManage, Navigate to Configuration → Templates → Feature → vSmart → VPN → VPN
- Configure the VPN parameters based on the following:
  - o Template Name: vSmart -VPN-VPN512
  - o Description: vSmart -VPN-VPN512
- Basic Configuration
  - o VPN → Global : 512
  - o Name → Global : MGMT VPN
- Click Save to save the Template.

[Download PNETLab Platform](#)[PNETLAB Store](#)[PNETLab.com](#)

Not secure | 192.168.100.2/#/app/config/template/feature?display=edit&templateId=33b21506-e570-422e-a54c-c734233a7ebb&templateType=vpn-vsmart

Cisco vManage

Dashboard >

Monitor >

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

Tools >

Maintenance >

Administration >

vAnalytics >

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > VPN > vSmart-VPN-VPN512

Device Type vSmart

Template Name vSmart-VPN-VPN512

Description vSmart-VPN-VPN512

Basic Configuration DNS IPv4 Route IPv6 Route

BASIC CONFIGURATION

VPN

Name

Primary DNS Address

New Host Mapping

Optional Hostname List of IP Addresses (Maximum: 8) Action

No data available

Not secure | 192.168.100.2/#/app/config/template/feature

Cisco vManage

Dashboard >

Monitor >

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

Tools >

Maintenance >

Administration >

vAnalytics >

CONFIGURATION | TEMPLATES

Add Template

Template Type Non-Default Search Options Total Rows: 32

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated	...
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	admin	29 Oct 2020 10:40:53 PM ADT	...
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:45:51 PM ADT	...
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:49:25 PM ADT	...
BR-VE-VPNINT-VPN512-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:51:24 PM ADT	...
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	admin	29 Oct 2020 11:00:30 PM ADT	...
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	admin	30 Oct 2020 5:27:27 AM ADT	...
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3	admin	30 Oct 2020 5:28:24 AM ADT	...
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	admin	30 Oct 2020 5:31:07 AM ADT	...
vSmart-VPN-VPN0	vSmart-VPN-VPN0	vSmart VPN	vSmart	0	0	admin	01 Nov 2020 4:13:42 AM AST	...
HQ-VE-VPNINT-VPN512-E0	HQ-VE-VPNINT-VPN512-E0	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:17:24 PM ADT	...
HQ-VE-VPNINT-VPN0-G0	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:11:01 PM ADT	...
HQ-VE-BGP-VPN0	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	1	1	admin	30 Oct 2020 1:13:44 PM ADT	...
HQ-VE-VPN-VPN1	HQ-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:18:27 PM ADT	...
HQ-VE-VPN-VPN512	HQ-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:18:56 PM ADT	...
HQ-VE-VPN-VPN0	HQ-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:09:25 PM ADT	...
BR-CSR-VPN-VPN1	BR-CSR-VPN-VPN1	Cisco VPN	CSR1000v	1	1	admin	01 Nov 2020 12:37:33 AM ADT	...
BR-CSR-OSPF-VPN1	BR-CSR-OSPF-VPN1	Cisco OSPF	CSR1000v	1	1	admin	01 Nov 2020 12:41:28 AM ADT	...
BR-CSR-VPN-VPN0	BR-CSR-VPN-VPN0	Cisco VPN	CSR1000v	1	1	admin	31 Oct 2020 11:53:32 PM ADT	...
BR-CSR-OSPF-VPN0	BR-CSR-OSPF-VPN0	Cisco OSPF	CSR1000v	1	1	admin	01 Nov 2020 12:00:47 AM ADT	...
BR-CSR-VPNINT-VPN1-G2	BR-CSR-VPNINT-VPN1-G2	Cisco VPN Interface Ethernet	CSR1000v	1	1	admin	01 Nov 2020 12:39:57 PM ADT	...
vSmart-VPN-VPN512	vSmart-VPN-VPN512	vSmart VPN	vSmart	0	0	admin	01 Nov 2020 4:17:07 AM AST	...
BR-CSR-VPNINT-VPN0-G1	BR-CSR-VPNINT-VPN0-G1	Cisco VPN Interface Ethernet	CSR1000v	1	1	admin	31 Oct 2020 11:56:31 PM ADT	...
BR-CSR-VPNINT-VPN0-G3	BR-CSR-VPNINT-VPN0-G3	Cisco VPN Interface Ethernet	CSR1000v	1	1	admin	31 Oct 2020 11:58:29 PM ADT	...



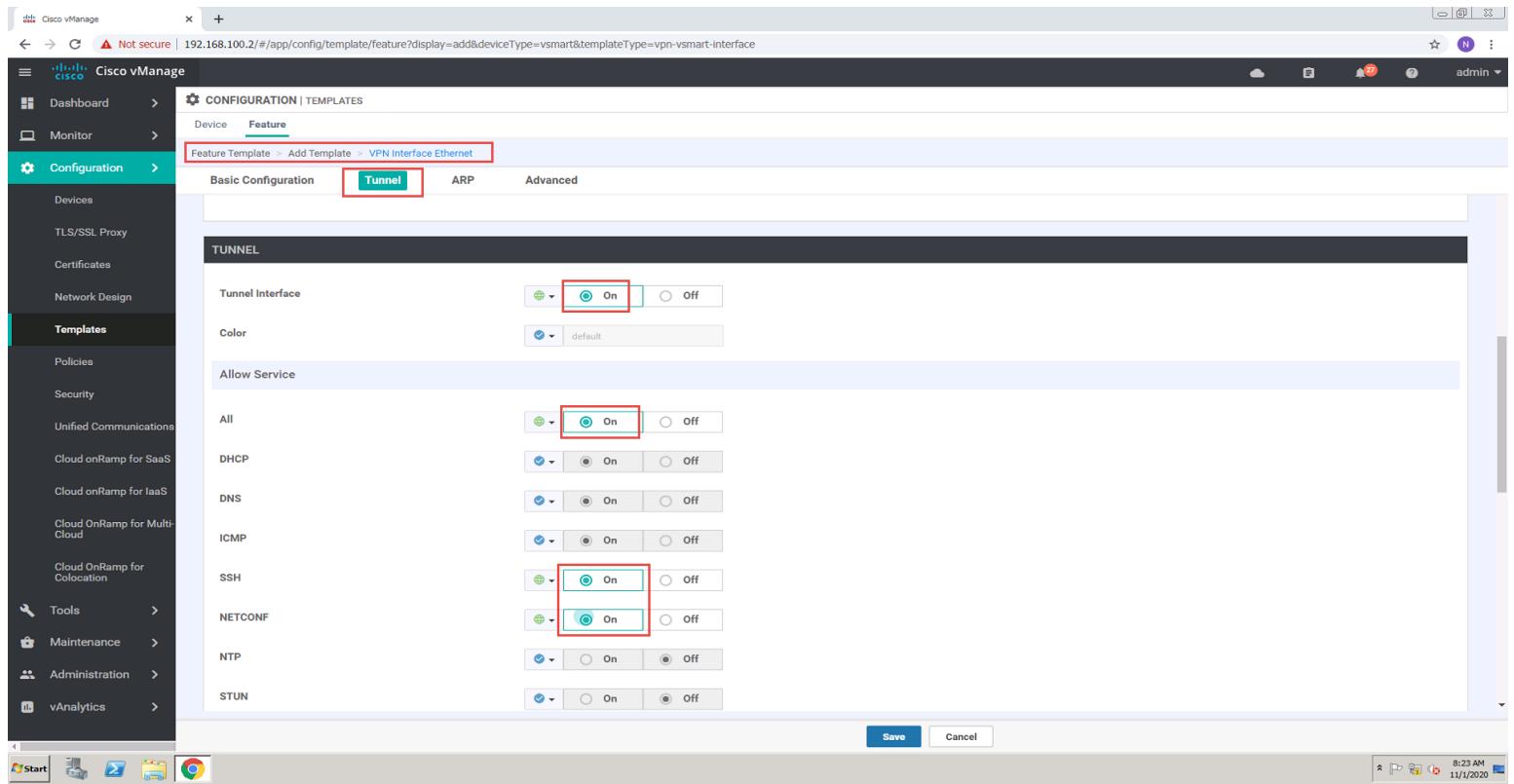
## Task 3 – Configure a VPN Interface Template to be used by vSmart Controllers for VPN 0 for Interface Eth1

- In vManage, Navigate to Configuration → Templates → Feature → vSmart → VPN → VPN Interface Ethernet
  - Configure the VPN parameters based on the following:
    - o Template Name: vSmart-VPNINT-VPN0-E1
    - o Description: vSmart-VPNINT-VPN0-E1
- Basic Configuration
- o Shutdown → Global : No
  - o Interface Name → Global : eth1
  - o IPv4 Address → Static → Device Specific
- Tunnel
- o Tunnel Interface → Global : On
  - o Color → default
- Allow Service
- o All → Global: On
  - o NETCONF → Global: On
  - o SSH → Global: On
- Click Save to save the Template.

The screenshot shows the Cisco vManage interface under the Configuration tab. In the Templates section, a new Feature Template is being created for 'vSmart'. The 'Device Type' is set to 'vSmart'. The 'Template Name' is 'vSmart-VPNINT-VPN0-E1' and the 'Description' is also 'vSmart-VPNINT-VPN0-E1'. The 'Basic Configuration' tab is selected, showing the following settings:

- Shutdown:** The 'Yes' radio button is selected, while 'No' is highlighted with a red box.
- Interface Name:** The value 'eth1' is entered in the dropdown field, which is also highlighted with a red box.
- Description:** A dropdown menu is open.
- IP Configuration:** The 'Static' radio button is selected, while 'Dynamic' is highlighted with a red box.
- IPv4 Address:** A placeholder '[vpn\_if\_ip\_address]' is shown in the input field.

At the bottom right of the configuration window are 'Save' and 'Cancel' buttons.



The screenshot shows the Cisco vManage web interface. The URL is 192.168.100.2/#/app/config/template/feature?display=add&deviceType=vsmart&templateType=vpn-vsmart-interface. The left sidebar is open with 'Templates' selected. The main area shows the 'CONFIGURATION | TEMPLATES' screen under 'Feature'. The 'Tunnel' tab is active. A red box highlights the 'Tunnel Interface' section where the 'On' radio button is selected. Another red box highlights the 'Allow Service' section, specifically the checkboxes for 'All', 'SSH', and 'NETCONF', all of which are also selected.

## Task 4 – Configure a VPN Interface Template to be used vSmart Controllers for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration → Templates → Feature → vSmart → VPN → VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - o Template Name: vSmart-VPNINT-VPN512-E0
  - o Description: vSmart-VPNINT-VPN512-E0
- Basic Configuration
  - o Shutdown → Global: No
  - o Interface Name → Global: eth0
  - o IPv4 Address → Static → Device-Specific
- Click Save to save the Template

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Cisco vManage

Not secure | 192.168.100.2/#/app/config/template/feature?display=edit&templateId=2831e77b-b623-4d83-bc87-4198c4a236f2&templateType=vpn-vsmart-interface

admin

Configuration | TEMPLATES

Device Feature

Feature Template > VPN Interface Ethernet - vSmart-VPNINT-VPN512-E0

Device Type vSmart

Template Name vSmart-VPNINT-VPN512-E0

Description vSmart-VPNINT-VPN512-E0

Basic Configuration Tunnel ARP Advanced

BASIC CONFIGURATION

Shutdown Yes No

Interface Name eth0

Description

IP Configuration

Dynamic Static

IPv4 Address [vpn\_(ip\_address)]

IPv6 Configuration

Update Cancel

8:36 AM 11/1/2020

Cisco vManage

Not secure | 192.168.100.2/#/app/config/template/feature

admin

Configuration | TEMPLATES

Add Template

Template Type Non-Default

Name Description Type Device Model Device Templates Devices Attached Updated By Last Updated

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
HQ-VE-OSPF-VPN1	HQ-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	1	admin	30 Oct 2020 1:21:10 PM ADT
vSmart-VPNINT-VPN512-E0	vSmart-VPNINT-VPN512-E0	vSmart Interface	vSmart	0	0	admin	01 Nov 2020 4:36:40 AM AST
BR-CSR-VPN-VPN512	BR-CSR-VPN-VPN512	Cisco VPN	CSR1000v	1	1	admin	01 Nov 2020 12:01:51 AM ADT
VE-System	VE-System	WAN Edge System	vEdge Cloud	2	4	admin	29 Oct 2020 10:30:04 PM ADT
CE-Banner	CE-Banner	Cisco Banner	CSR1000v	0	0	admin	29 Oct 2020 10:37:53 PM ADT
HQ-VE-VPNINT-VPN1-G2	HQ-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:47:58 PM ADT
BR-CSR-VPNINT-VPN512-G4	BR-CSR-VPNINT-VPN512-G4	Cisco VPN Interface Ethernet	CSR1000v	1	1	admin	01 Nov 2020 12:03:08 AM ADT
CE-System	CE-System	Cisco System	CSR1000v	1	1	admin	29 Oct 2020 10:31:56 PM ADT
VE-Banner	VE-Banner	Banner	vEdge Cloud	0	0	admin	29 Oct 2020 10:36:50 PM ADT
BR-VE-VPN-VPN0	BR-VE-VPN-VPN0	WAN Edge VPN	vEdge Cloud	1	3	admin	29 Oct 2020 10:39:55 PM ADT
BR-VE-VPN-VPN512	BR-VE-VPN-VPN512	WAN Edge VPN	vEdge Cloud	1	3	admin	29 Oct 2020 10:40:53 PM ADT
BR-VE-VPN-VPN512-G0	BR-VE-VPN-VPN512-G0	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:45:51 PM ADT
BR-VE-VPNINT-VPN0-G0	BR-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:49:25 PM ADT
BR-VE-VPNINT-VPN0-G1	BR-VE-VPNINT-VPN0-G1	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 10:51:24 PM ADT
BR-VE-VPNINT-VPN512-Eth0	BR-VE-VPNINT-VPN512-Eth0	WAN Edge Interface	vEdge Cloud	1	3	admin	29 Oct 2020 11:00:30 PM ADT
BR-VE-OSPF-VPN0	BR-VE-OSPF-VPN0	OSPF	vEdge Cloud	1	3	admin	30 Oct 2020 1:27:27 AM ADT
BR-VE-VPN-VPN1	BR-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	3	admin	30 Oct 2020 4:13:42 AM AST
BR-VE-VPNINT-VPN1-G2	BR-VE-VPNINT-VPN1-G2	WAN Edge Interface	vEdge Cloud	1	3	admin	30 Oct 2020 5:28:24 AM ADT
BR-VE-OSPF-VPN1	BR-VE-OSPF-VPN1	OSPF	vEdge Cloud	1	3	admin	30 Oct 2020 5:31:07 AM ADT
vSmart-VPN-VPN0	vSmart-VPN-VPN0	vSmart VPN	vSmart	0	0	admin	01 Nov 2020 4:13:42 AM AST
HQ-VE-VPNINT-VPN512-E0	HQ-VE-VPNINT-VPN512-E0	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:17:24 PM ADT
HQ-VE-VPNINT-VPN0-G0	HQ-VE-VPNINT-VPN0-G0	WAN Edge Interface	vEdge Cloud	1	1	admin	30 Oct 2020 1:11:01 PM ADT
HQ-VE-BGP-VPN0	HQ-VE-BGP-VPN0	BGP	vEdge Cloud	1	1	admin	30 Oct 2020 1:13:14 PM ADT
HQ-VE-VPN-VPN1	HQ-VE-VPN-VPN1	WAN Edge VPN	vEdge Cloud	1	1	admin	30 Oct 2020 1:18:27 PM ADT

Total Rows: 34

8:37 AM 11/1/2020



## Task 5 – Configure a Device Template for vSmart Controllers.

- In vManage, Navigate to Configuration → Templates → Device → Create Template → vSmart
- Configure the Device Template based on the following:
  - o Template Name: vSmart-TEMP
  - o Description: vSmart-TEMP
- Basic Information
  - o System → Vsmart-System
- Transport & Management
  - o VPN 0: vSmart-VPN-VPNO
  - o VPN Interface: vSmart-VPNINT-VPNO-E1
  - o VPN 512: vSmart-VPN-VPN512
  - o VPN Interface: vSmart-VPNINT-VPN512-E0
- Click Save to save the Template.

The screenshot shows the Cisco vManage web interface. The left sidebar is open with the 'Templates' section selected. The main content area is titled 'CONFIGURATION | TEMPLATES' and shows the 'Device' tab is active. A search bar contains 'vSmart-TEMP'. Below it, there are tabs for 'Basic Information', 'Transport & Management VPN', and 'Additional Templates'. Under 'Basic Information', the 'System' dropdown is set to 'Vsmart-System'. Under 'Transport & Management VPN', the 'VPN 0' dropdown is set to 'vSmart-VPN-VPNO' and the 'VPN Interface' dropdown is set to 'vSmart-VPNINT-VPNO-E1'. Both of these dropdowns are highlighted with red boxes. On the right side, there are sections for 'Additional System Templates' (Archive, NTP) and 'Additional VPN 0 Templates' (VPN Interface). At the bottom right are 'Create' and 'Cancel' buttons.

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Cisco vManage | Not secure | 192.168.100.2/#/app/config/template/device/feature/edit?templateId=96d1f408-f76b-4cf8-8d47-ebd5d68f0a10&attached=false | admin

**CONFIGURATION | TEMPLATES**

**Basic Information**

System \*: Vsmart-System  
Logging+: Factory\_Default\_Logging\_Template\_V01

**Additional System Templates**

- Archive
- NTP

**Transport & Management VPN**

VPN 0 \*: vSmart-VPN-VPN0  
VPN Interface: vSmart-VPNINT-VPN0-E1

**Additional VPN 0 Templates**

- VPN Interface

**VPN 512 \*** (highlighted with a red box)  
VPN Interface: vSmart-VPNINT-VPN512-E0

**Additional VPN 512 Templates**

- VPN Interface

**Update** **Cancel**

Cisco vManage | Not secure | 192.168.100.2/#/app/config/template/device | admin

**CONFIGURATION | TEMPLATES**

**Create Template**

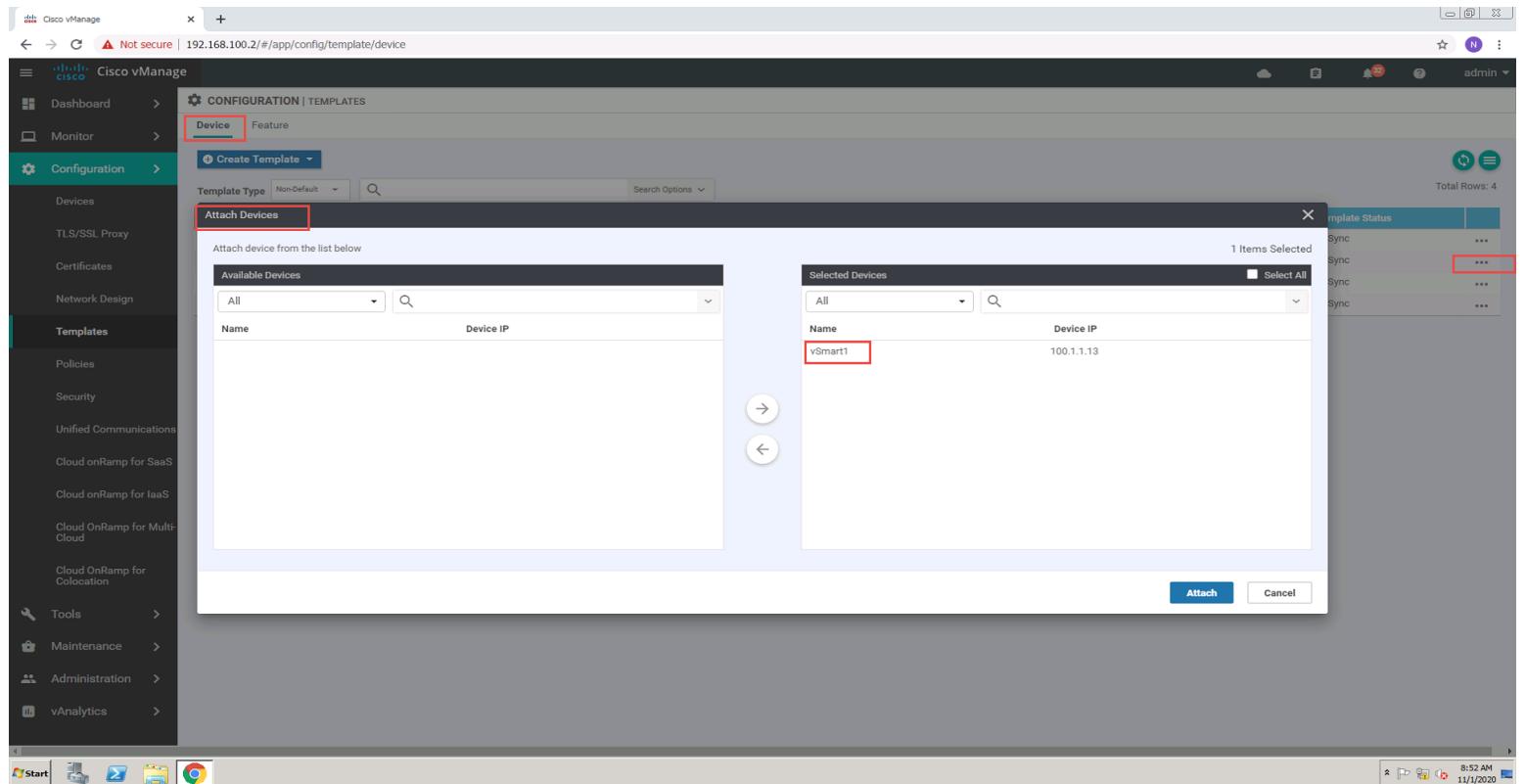
Template Type: Non-default

Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	Action
BR-VE-TEMP	BR-VE-TEMP	Feature	vEdge Cloud	15	3	admin	30 Oct 2020 5:42:00 AM A...	In Sync	...
vSmart-TEMP	vSmart-TEMP	Feature	vSmart	9	0	admin	01 Nov 2020 4:50:31 AM A...	In Sync	...
HQ-VE-TEMP	HQ-VE-TEMP	Feature	vEdge Cloud	14	1	admin	30 Oct 2020 1:23:57 PM ADT	In Sync	...
BR-CSR-TEMP	BR-CSR-TEMP	Feature	CSR1000v	16	1	admin	01 Nov 2020 12:47:16 AM ...	In Sync	...

Total Rows: 4

## Task 6 – Attach vSmart to the Device Template

- In vManage, Navigate to Configuration → Templates → Device → vSmart-TEMP
- Click on “...” towards the right-hand side.
- Click Attach Devices.
- Select vSmart and click the “→” button.
- Click Attach.



## Task 7 – Configure the Variable Parameters for the Feature Templates

- vSmart will appear in the window.
- Click on “...” towards the right-hand side.
- Click Edit Device Template.
- Configure the variables based on the following:
  - Interface IP for Eth1: 100.1.1.3/24
  - Interface IP for Eth0: 192.168.1.2/24
  - Hostname: vSmart-1
  - System IP: 100.1.1.12
  - Site ID: 1
- Click Update.
- Verify the Configuration & Click Configure Devices.
- Wait for it to update the device. It should come back with Status of Success.



Cisco vManage | Not secure | 192.168.100.2/#/app/config/template/device/configure/96d1f408-f76b-4cf8-8d47-ebd5d68f0a10 | admin | 9:03 AM 11/1/2020

**CONFIGURATION | Device Template**

**Update Device Template**

**Variable List (Hover over each field for more information)**

Chassis Number	15cc1f84-2ba7-4a9b-839c-4daf4d96489f
System IP	100.1.1.13
Hostname	vSmart1
IPv4 Address(vpn_if_ip_address)	192.168.100.3/24
IPv4 Address(vpn_if_ip_address)	100.1.3/24
Hostname(system_host_name)	vSmart1
System IP(system_system_ip)	100.1.1.13
Site ID(system_site_id)	1

**Generate Password** **Update** **Cancel**

**CONFIGURATION | TEMPLATES**

**Device Template** **Total 1**

**Config Preview** **Config Diff**

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

**Device list (Total: 1 devices)**

15cc1f84-2ba7-4a9b-839c-4daf4d96489f  
vSmart1|100.1.1.13

```

system
device-model          vSmart
host-name             vSmart-1
system-ip              100.1.1.13
domain-id              1
site-id                1
admin-tech-on-failure
sp-organization-name  PNETLAB
organization-name      PNETLAB
clock timezone         America/Antigua
vbond 100.1.1.4 port 12346
aaa
auth-order local radius tacacs
usergroup basic
task system read write
task interface read write
!
usergroup netadmin
!
usergroup operator
task system read
task interface read
task policy read
task routing read
task security read
!
user admin
password $6$ivKBQ==uT2lUa9B5reDPI6g8s14E6PAJ0vXg!bgv/whJ8F1C6sldRazdxorYYTLrL6sy106qnLABTnrE96HjIKF6QRq1
!
logging
disk enable
!
!
omp no shutdown graceful-restart
!
vpn 0
name "Transport VPN"
interface eth1

```

**Configure Device Rollback Timer**

**Back** **Configure Devices** **Cancel**



[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Cisco vManage Not secure | 192.168.100.2/#/app/device/status?activity=push\_file\_template\_configuration&pid=push\_feature\_template\_configuration-14568f1b-ac25-4afa-a91e-bf74a1bd8bb8 admin

**TASK VIEW**  
Push Feature Template Configuration | Validation Success  
Initiated By: admin From: 192.168.100.5  
Total Task: 1 | Success : 1

Total Rows: 1

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template ... 15cc1fb4-2ba7-4a9b-839c-4da... vSmart	vSmart1	100.1.1.13	1	100.1.1.12		

Search Options ▾

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

Tools  
Maintenance  
Administration  
vAnalytics

Start | Google Chrome | 9:07 AM 11/1/2020





## Lab 27 - Configuring Application Aware Policies using Telnet and Web

### Requirements:

- Dubai (Site-2) & Hongkong (Site-3) Sites should use the MPLS Transport for Telnet
- Traffic and the Biz-Internet Transport for Web Traffic.
- Telnet Should have a SLA based on the following:
  - o Loss – 5%
  - o Latency – 200
  - o Jitter – 100ms
- Web Should have a SLA based on the following:
  - o Loss – 10%
  - o Latency – 500
  - o Jitter – 100ms
- Create the Sites for Dubai and Hongkong.
- Create the VPN for VPN ID 1.

### Task 1 – Configure Groups of Interests/List that will be used for Telnet & Web Application Aware Routing (AAR) Policy

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Lists.
- Click SLA Class and select New SLA Class list. Create 2 policies based on the following:
  - o Name: SLA-Telnet
  - o Loss: 30% (because in lab, packet lost is high)
  - o Latency: 200
  - o Jitter: 100ms
  - o Name: SLA-Web
  - o Loss: 40% (because in lab, packet lost is high)
  - o Latency: 500
  - o Jitter: 100ms
- Click VPN and select New VPN list. Create 1 policy based on the following:
  - o Name: VPN1
  - o ID: 1
- Click Site and select New Site list. Create 2 policies based on the following:
  - o Name: Dubai
  - o Site ID: 2
  - o Name: Hongkong
  - o Site ID: 3





Cisco vManage

Not secure | 192.168.100.2/#/app/config/policy/centralizedPolicy/policies

admin

**CONFIGURATION | POLICIES**

**Centralized Policy** Localized Policy

**Centralized Policy**

- CLI Policy
- Lists**
- Topology
- Traffic Policy

**Localized Policy**

- CLI Policy
- Lists
- Forwarding Class/QoS
- Access Control Lists
- Route Policy

No Centralized Policies added, add your first Policy

Add Policy

Cisco vManage

Not secure | 192.168.100.2/#/app/config/policy/custom/centralizedPolicy/define\_lists/sla\_class

admin

**CONFIGURATION | POLICIES** **Centralized Policy** > Define Lists

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

**SLA Class**

Name	Loss (%)	Latency (ms)	Jitter (ms)
Voice-And-Video	2	45	30
Transactional-Data	5	50	100
Bulk-Data	10	300	100
Default	25	300	100

**New SLA Class List**

**SLA Class List Name**: SLA-Telnet

**Loss (%)**: 5

**Latency (ms)**: 200

**Jitter (ms)**: 100

Add Cancel



[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Cisco vManage | Not secure | 192.168.100.2/#/app/config/policy/custom/centralizedPolicy/define\_lists/sla\_class

Cisco vManage

CONFIGURATION | POLICIES Centralized Policy > Define Lists

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

Application **New SLA Class List**

SLA Class List Name: SLA-Web

Loss (%): 10

Latency (ms): 500

Jitter (ms): 100

Add Cancel

Name	Loss (%)	Latency (ms)	Jitter (ms)	Reference Count	Updated By	Last Updated	Action
Voice-And-Video	2	45	30	0	system	27 Oct 2020 9:16:51 AM A...	
Transactional-Data	5	50	100	0	system	27 Oct 2020 9:16:53 AM A...	
Bulk-Data	10	300	100	0	system	27 Oct 2020 9:16:53 AM A...	
Default	25	300	100	0	system	27 Oct 2020 9:16:51 AM A...	
SLA-Telnet	5	200	100	0	admin	01 Nov 2020 5:30:19 AM A...	

Cisco vManage | Not secure | 192.168.100.2/#/app/config/policy/custom/centralizedPolicy/define\_lists/vpn

Cisco vManage

CONFIGURATION | POLICIES Centralized Policy > Define Lists

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

Application **New VPN List**

VPN List Name: VPN1

Add VPN: 1

Add Cancel

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



The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Cisco vManage' and includes sections for Dashboard, Monitor, Configuration (selected), Policies (selected), Security, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, Cloud OnRamp for Multi-Cloud, Cloud OnRamp for Colocation, Tools, Maintenance, Administration, and vAnalytics. The main content area is titled 'CONFIGURATION | POLICIES > Centralized Policy > Define Lists'. It displays a form for creating a new site list. The 'Site' section is highlighted with a red box. Inside, the 'Site List Name' field contains 'Dubai' and the 'Add Site' button has the value '2'. A large red box surrounds the entire input area. Below the form is a table with the following columns: Name, Entries, Reference Count, Updated By, Last Updated, and Action. The message 'No data available' is centered in the table area.

## Task 2 – Configure an AAR policy based on the Requirements

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Traffic Policy.
- Configure 2 App Routes based on the following:
  - o Policy Name: TELNET-WEB-Policy
  - o Description: TELNET-WEB-Policy

Telnet Sequence

Match Conditions:

- o Protocol: 6
- o Port: 23

Action

- o SLA Class List: SLA-Telnet
- o Color: mpls
- o Backup Preferred Color: biz-internet
- o Click Save Match and Actions to save the Sequence.

Web Sequence

Match Conditions:

- o Protocol: 6
- o Port: 80

Action

- o SLA Class List: SLA-Web



[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



- Color : biz-internet
- Backup Preferred Color: mpls
- Click Save Match and Actions to save the Sequence.
- Save the Policy.

The screenshot shows the Cisco vManage web interface. The URL is 192.168.100.2/#/app/config/policy/centralizedPolicy/policies. The left sidebar is open under 'Configuration' and 'Policies'. The 'Centralized Policy' tab is selected. A modal window titled 'Centralized Policy' is open, showing a list of policy types: CLI Policy, Lists, Topology, Forwarding Class/QoS, Access Control Lists, and Route Policy. The 'Traffic Policy' option is highlighted with a red box. The main content area displays a green hexagonal icon with three horizontal lines and a plus sign, indicating no policies have been added. Below it is the text 'No Centralized Policies added, add your first Policy' and a blue 'Add Policy' button. The top right corner shows the user is logged in as 'admin'.

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Screenshot of Cisco vManage interface showing the configuration of an Application Aware Routing Policy. The policy is named "TELNET-WEB-Policy". The "Sequence Type" is set to "Telnet Sequence". A "Default Action" is defined as "None" and is enabled. The "Save Application Aware Routing Policy" button is visible at the bottom.

Screenshot of Cisco vManage interface showing the detailed configuration of the "TELNET-WEB-Policy". The "Sequence Type" is set to "Telnet Sequence". Under "Match Conditions", "Protocol" is set to "6" and "Destination Port" is set to "23". Under "Actions", "SLA Class" is set to "SLA-Telnet", "Preferred Color" is set to "mpls", and "Backup SLA Preferred Color" is set to "biz-internet". The "Save Match And Actions" button is highlighted with a red box.



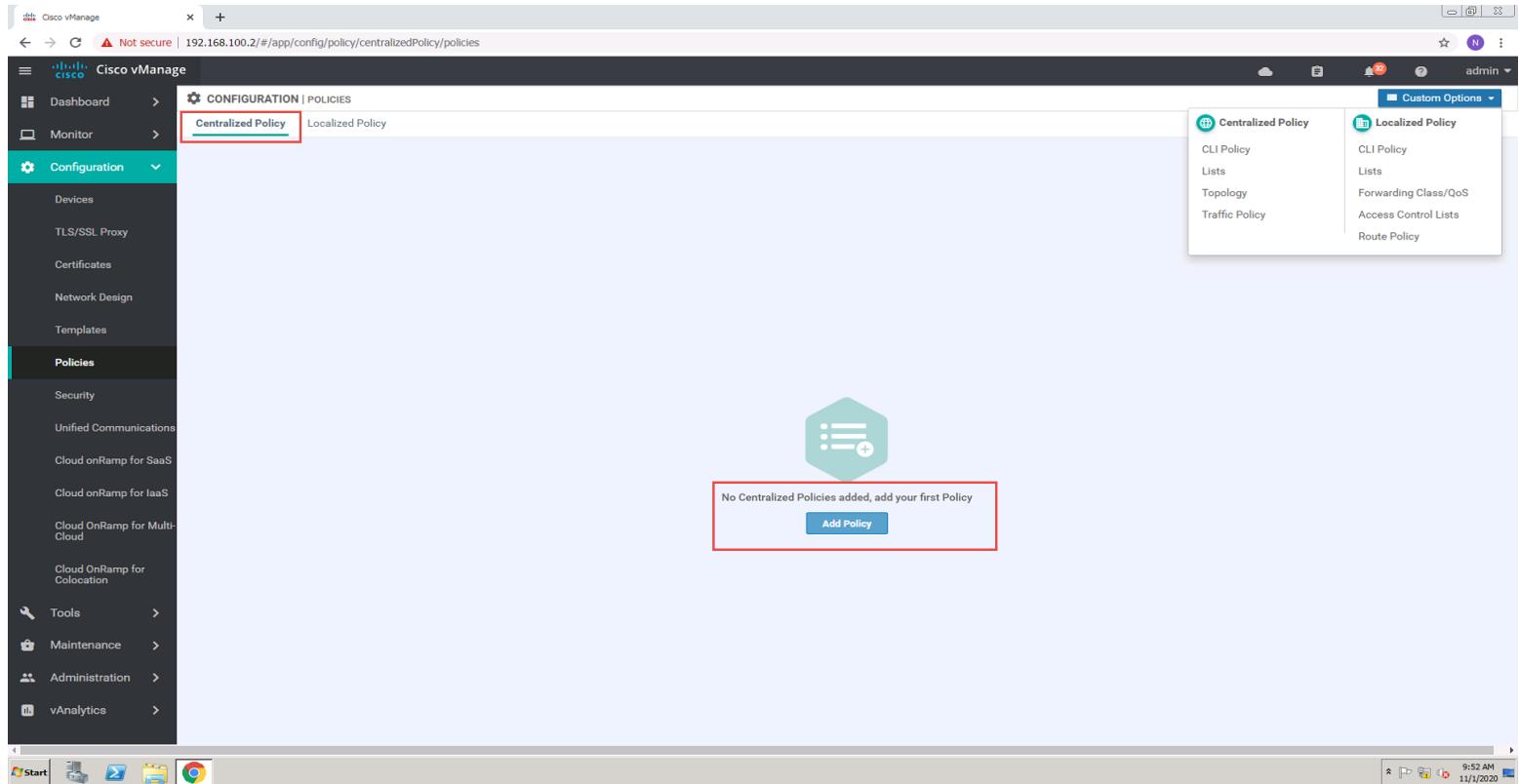
The screenshot shows the Cisco vManage web interface. The left sidebar is titled "Cisco vManage" and includes sections for Dashboard, Monitor, Configuration (Devices, TLS/SSL Proxy, Certificates, Network Design, Templates), Policies (Security, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, Cloud OnRamp for Multi-Cloud, Cloud OnRamp for Colocation), Tools, Maintenance, Administration, and vAnalytics. The main content area is titled "CONFIGURATION | POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy". It shows a form with "Name" set to "TELNET-WEB-Policy" and "Description" also set to "TELNET-WEB-Policy". Under "Sequence Type", "Web Sequence" is selected. The "Match" tab is active, showing "Protocol" (IPv4) and "Destination Port" (80). The "Actions" tab is also active, containing "SLA Class" (SLA-Web), "Preferred Color" (biz-internet), and "Backup SLA Preferred Color" (mpls). A red box highlights the "Actions" tab. A red box also highlights the "Save Match And Actions" button at the bottom right. The status bar at the bottom indicates "PREVIEW", "Save Application Aware Routing Policy", and "CANCEL".

### Task 3 – Create a Centralized Policy and call the Traffic Policy

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Add Centralized Policy
- Click Next on the “Group of Interests” page as we have already created the required lists.
- Click Next on the “Topology and VPN Membership” page as we are not using any Control Policies.
- Click Add Policy on the “Configure Traffic Rules” page.
- Click “Import Existing” and select the TELNET-WEB-POLICY from the drop-down list and click Import.
- Click Next to move to the “Apply Policy to Sites and VPNs” Page.
- Click the “Appliacation-Aware Policy” tab.
- The TELNET-WEB-Policy will be there. Click “New Site List and VPN List” button.
- Select Dubai and Hongkong in the Site List.
- Select VPN1 in the Site List.
- Click Add.
- Assign the Policy a name and Desription based on the following:
  - o Policy Name: Main-Central-Policy
  - o Description: Main-Central-Policy
- Click the Save Policy button towards the button.
- Activate the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).



- Verify the policy by using the Monitor → Network → vEdge3 → Troubleshooting → Simulate Flows Tool.
- Telnet from Dubai or Hongkong should only use the mpls transport.
- Web from Dubai or Hongkong should only use the biz-internet transport.
- Normal Ping from Dubai or Hongkong should use both the Transports.



The screenshot shows the Cisco vManage web interface. The URL in the address bar is 192.168.100.2/#/app/config/policy/centralizedPolicy/policies. The left sidebar is open under 'Configuration' and shows the 'Polices' section. Under 'Centralized Policy', there is a red box around the 'Centralized Policy' tab. A modal window titled 'CONFIGURATION | POLICIES' is displayed, with 'Centralized Policy' selected. The main content area says 'No Centralized Policies added, add your first Policy' and has a blue 'Add Policy' button. On the right side, there is a sidebar with 'Custom Options' and two tabs: 'Centralized Policy' and 'Localized Policy'. Under 'Centralized Policy', there are links for CLI Policy, Lists, Topology, Traffic Policy, and others. Under 'Localized Policy', there are links for CLI Policy, Lists, Forwarding Class/QoS, Access Control Lists, and Route Policy. The bottom status bar shows the date and time as 9:52 AM 11/1/2020.

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Cisco vManage Cisco vManage

Not secure | 192.168.100.2/#/app/config/policy?type=centralizedPolicy&action=add

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest

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

**Application**

Application List Custom Applications

New Application List

Name	Entries	Reference Count	Updated By	Last Updated	Action
Microsoft_Apps	bing, hockeyapp, live, hotmail, lync, ly...	0	system	27 Oct 2020 9:16:52 AM ADT	
Google_Apps	android-updates, blogger, chrome_up...	0	system	27 Oct 2020 9:16:53 AM ADT	

Next CANCEL

Start Google Chrome Taskbar

9:53 AM 11/1/2020

Cisco vManage Cisco vManage

Not secure | 192.168.100.2/#/app/config/policy?type=centralizedPolicy&action=add

CONFIGURATION | POLICIES Centralized Policy > Add Policy

Create Groups of Interest

Configure Topology and VPN Membership

Specify your network topology

**Topology** VPN Membership

Add Topology

Search Options

Name	Type	Description	Reference Count	Updated By	Last Updated
No data available					

Total Rows: 0

BACK Next CANCEL

Start Google Chrome Taskbar

9:55 AM 11/1/2020

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Screenshot of Cisco vManage interface showing the import of an Application Aware Routing Policy.

The main window displays the "CONFIGURATION | POLICIES | Centralized Policy > Add Policy" screen. A red box highlights the "Configure Traffic Rules" button in the top right corner. Another red box highlights the "Add Policy" button in the "Application Aware Routing" tab.

A modal dialog titled "Import Existing Application Aware Routing Policy" is open. It shows a dropdown menu with "TELNET-WEB-Policy" selected, and a red box highlights the "Import" button at the bottom right of the dialog.

Screenshot of Cisco vManage interface showing the configuration of a new centralized policy.

The main window displays the "CONFIGURATION | POLICIES | Centralized Policy > Add Policy" screen. A red box highlights the "Apply Policies to Sites and VPNs" button in the top right corner.

The "Add policies to sites and VPNs" section includes fields for "Policy Name" (Main-Central-Policy) and "Policy Description" (Main-Central-Policy). A red box highlights the "Topology" dropdown set to "Application-Aware Routing".

The "TELNET-WEB-Policy" section contains a "New Site List and VPN List" button, which is highlighted with a red box. Below it are "Select Site List" and "Select VPN List" dropdowns, each containing "Dubai" and "Hongkong" respectively, with a red box highlighting the "Hongkong" entry in the site list.

At the bottom right of the configuration area, a red box highlights the "Add" button.



Cisco vManage | Not secure | 192.168.100.2/#/app/config/policy/centralizedPolicy/policies

**CONFIGURATION | POLICIES**

**Centralized Policy**   Localized Policy

**Add Policy**

Search Options

Name Description Type Activated Updated By Policy Version Last Updated

Main-Central-Policy	Main-Central-Policy	UI Policy Builder	false	admin	11012020T055914188	01 Nov 2020 5:59:14 AM AST	...
---------------------	---------------------	-------------------	-------	-------	--------------------	----------------------------	-----

Total Rows: 1

View  
Preview  
Copy  
Edit  
Delete  
**Activate**

Cisco vManage | Not secure | 192.168.100.2/#/app/device/status?activity=vsmart\_policy\_config&pid=vsmart\_policy\_config-88d09de9-7f43-4e4d-be7e-dab0d3939f79

**TASK VIEW**

Push vSmart Policy | Validation Success

Total Task: 1 | Success : 1

Initiated By: admin From: 192.168.100.5

Search Options

Status	Message	Hostname	System IP	Site ID	vManage IP
Success	Done - Push vSmart Policy	vSmart-1	100.1.1.13	1	100.1.1.12

Total Rows: 1



Screenshot of Cisco vManage interface showing flow simulation results.

Selected Device: vEdge-3 | 118.1.3.23 Site ID: 3 Device Model: vEdge Cloud

Protocol: 6 (highlighted with a red box)

Source Port: 172.173.1.1

Destination Port: 23

DSCP: 0

All Paths: checked

Simulate button

Output:



Total next hops: 1 | IPSec : 1

[Download PNETLab Platform](#)

[PNETLAB Store](#)

[PNETLab.com](#)



Cisco vManage Cisco vManage

Not secure | 192.168.100.2/index.html#/app/monitor/dashboard/troubleshooting/simulate\_flows?personality=vedge&systemIp=118.1.3.23&localSystemIp=118.1.3.23&deviceType=vedge&deviceModel=vEdge-Cloud&uuid=d6d98a35-f70c-9955-0106-86192f37703... admin

MONITOR Network > Troubleshooting > Simulate Flows

Select Device: vEdge-3 | 118.1.3.23 Site ID: 3 Device Model: vEdge Cloud

Advanced Options

Protocol: ICMP Source Port: 172.173.1.1 Destination Port: 192.168.51.1 DSCP: All Paths

Output:

Simulate Total next hops: 2 | IPSec: 2

11:21 AM 11/1/2020

vEdge3

```
access-list-policers          ACL policer
app-route-policy-filter       Application-aware routing policy filters
data-policy-filter            Data policy filters
device-access-policy-counters Device Access Policy counters
device-access-policy-names   Device access policy names
filter-memory-usage          Show memory usage statistics
from-vsmart                  Display policy from vsmart
ipv6                         IPv6 policy configuration
qos-map-info                 QoS map information
qos-scheduler-info           Scheduler information
rewrite-associations         Rewrite rule to interface bindings
service-path                 Display next-hop information for packet coming from service side
tunnel-path                  Display next-hop information for packet coming over the WAN tunnel
zbfw                         Zone pair inspect sessions information

vEdge-3# show policy from-vsmart
from-vsmart sla-class SLA-Telnet
loss 30
latency 200
jitter 100
from-vsmart sla-class SLA-Web
loss 10
latency 500
jitter 100
from-vsmart app-route-policy _VPN1_TELNET-WEB-Policy
vpn-list VPN1
sequence 1
  match
    source-ip      0.0.0.0/0
    destination-port 23
    protocol      6
  action
    backup-sla-preferred-color biz-internet
    sla-class      SLA-Telnet
    no sla-class strict
    sla-class preferred-color mpls
sequence 11
  match
    source-ip      0.0.0.0/0
    destination-port 80
    protocol      6
  action
    backup-sla-preferred-color mpls
    sla-class      SLA-Web
    no sla-class strict
    sla-class preferred-color biz-internet
from-vsmart lists vpn-list VPN1
vpn 1
```





## Lab 28 - Manipulating Traffic flow using TLOCs

### Requirements:

- Paris should only use the MPLS TLOC as the preferred color while communicating to Dubai. The Internet TLOC should be backup TLOC.

### Task 1 – Configure Groups of Interests/List that will be used for Traffic Engineering Policy for DUBAI

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Lists.
- Click TLOCs and select New TLOC list. Create a policy based on the following:
  - o Name: DB-TLOC-MPLS-INT
  - o TLOC#1:
    - IP Address: 118.1.2.22
    - Color: MPLS
    - Encapsulation: IPSec
    - Preference: 300
  - o TLOC#2:
    - IP Address: 118.1.2.22
    - Color: Biz-internet
    - Encapsulation: IPSec
    - Preference: 200





vEdge2

```
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vEdge-2
vEdge-2# show omp tlocs advertised
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
-----
ipv4        118.1.2.22    mpls          ipsec
              118.1.2.22    biz-internet  ipsec

vEdge-2#
vEdge-2#
vEdge-2#
```

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/policy/custom\_lists/tloc

Custom Options

New TLOC List

Name	TLOC	Color	Encap	Preference	Reference Co.	Updated By	Last Updated	Action
DB-TLOC-MPLS-INT	118.1.2.22	mpls	ipsec	300	0	admin	01 Nov 2020 11:07:47 AM A	
	118.1.2.22	biz-internet	ipsec	200				

TLOC

## Task 2 – Configure Control/Topology policy based on the Requirements

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Topology.

- Configure 1 Route Policy based on the following:
  - o Policy Name : DB-MPLS-INT
  - o Description : DB-MPLS-INT

### Route Sequence

#### Match Conditions:

- o Site List: Dubai
- o VPN List: VPN1

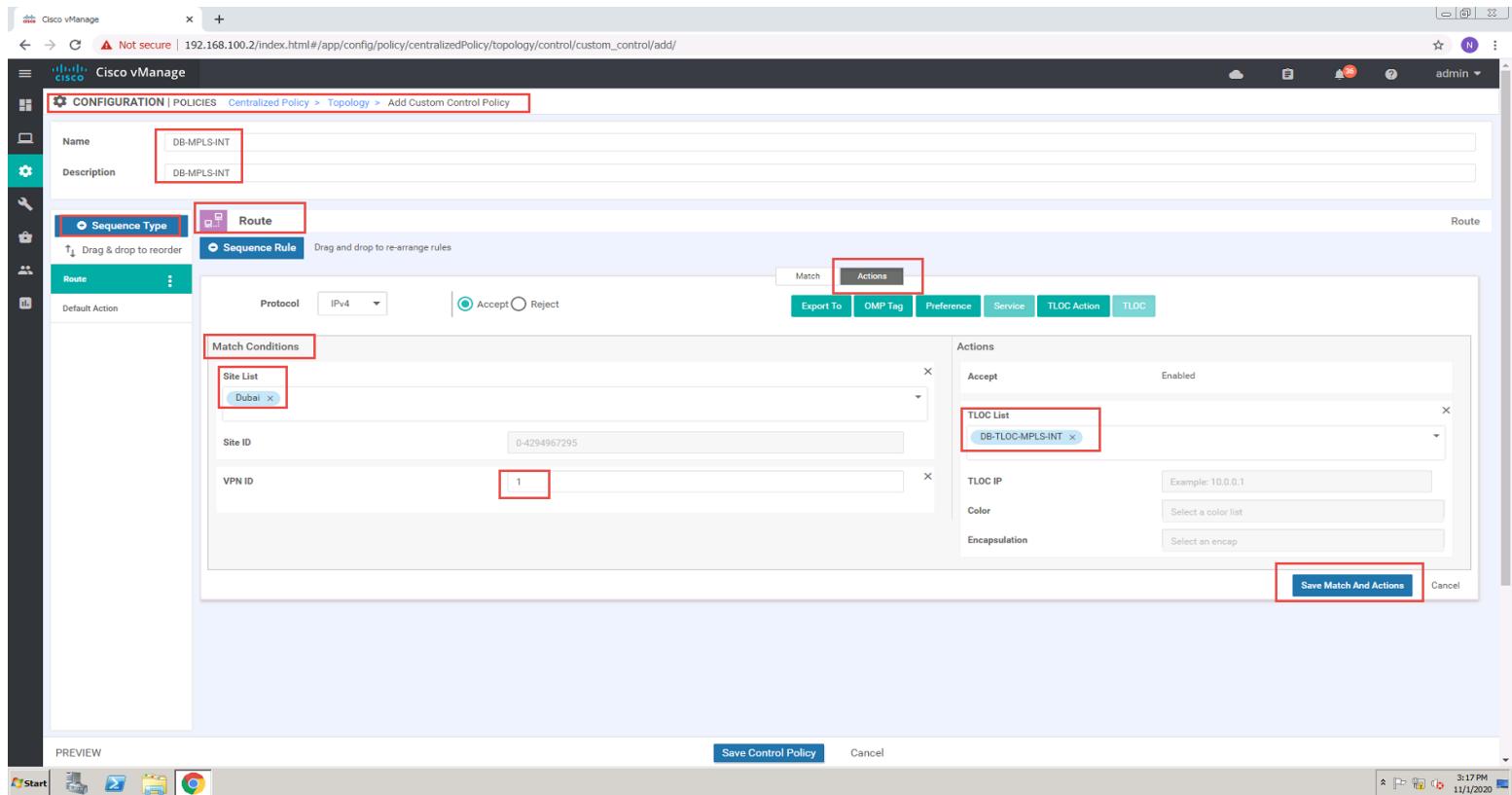
#### Action

- o TLOC/TLOC List: DB-MPLS-INT
- o Click Save Match and Actions to save the Sequence.

#### Default Sequence

#### Action

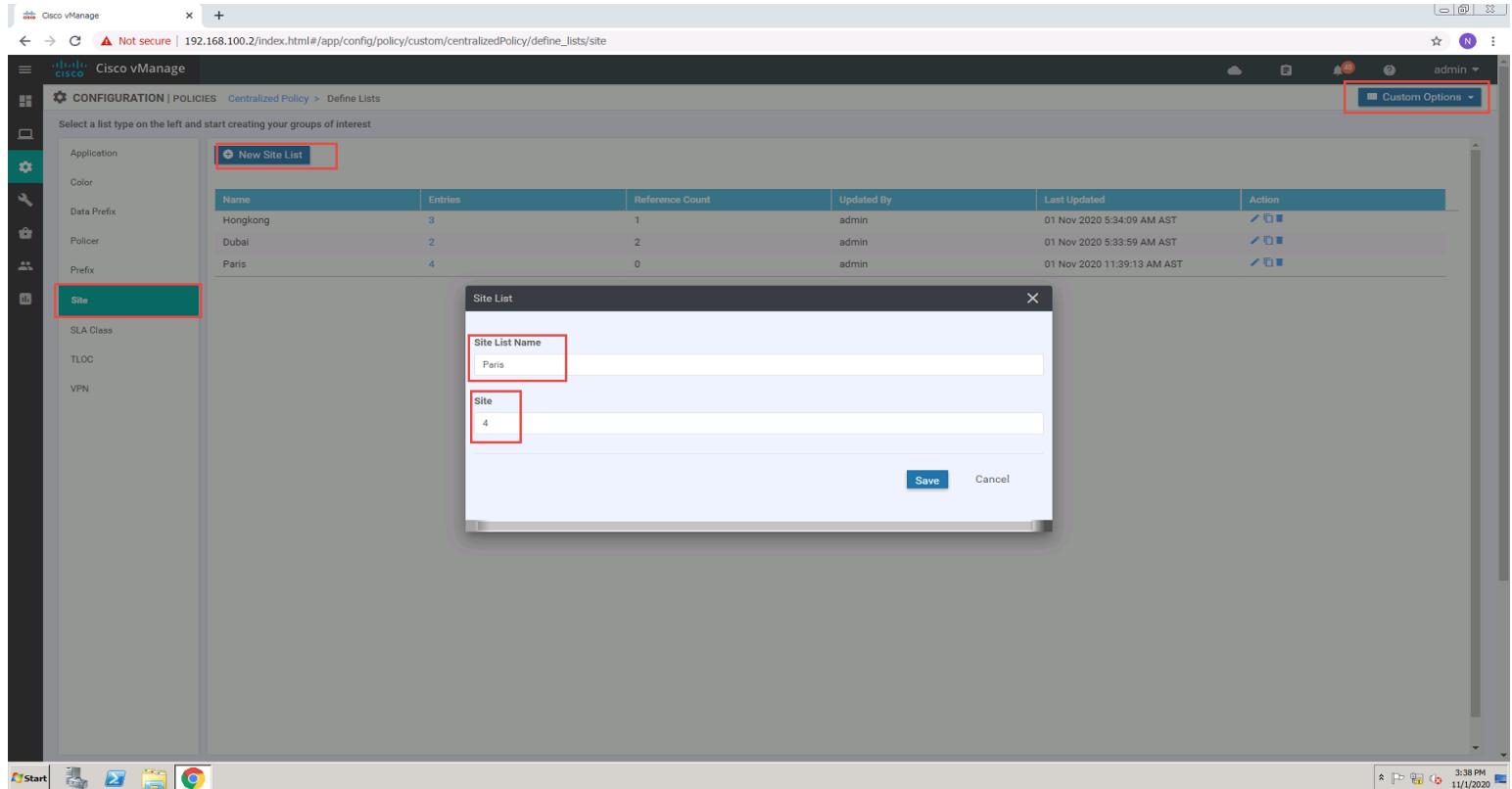
- o Accept
- o Click Save Match and Actions to save the Sequence.
- o Save the Policy



The screenshot shows the Cisco vManage web interface for configuring a Centralized Policy. The policy is named "DB-MPLS-INT" and is of type "Route". The "Match" section is configured to accept traffic from the "Dubai" site list and has a Site ID of 0-4294967295. The "Actions" section specifies an "Accept" action and a "TLOC List" of "DB-TLOC-MPLS-INT". The "Save Match And Actions" button is highlighted with a red box.

## Task 3 – Modify the existing Centralized Policy “Main-CentralPolicy” and call the Topology Policy

- In vManage, Navigate to Configuration → Policies → Custom Options → Lists → Site
- Create new site list Paris with site id 4.



The screenshot shows the Cisco vManage web interface. The left sidebar has a 'Site' button highlighted in red. The main content area shows a table of existing site lists: Hongkong (3 entries), Dubal (2 entries), and Paris (4 entries). A modal window titled 'Site List' is open, also with its title bar and 'Save' button highlighted in red. Inside the modal, the 'Site List Name' field contains 'Paris' and the 'Site' field contains '4'. The URL in the browser's address bar is 192.168.100.2/index.html#/app/config/policy/custom/centralizedPolicy/define\_lists/site.



The screenshot shows the Cisco vManage web interface. At the top, it displays a message: "Push vSmart Policy | Validation Success". Below this, a table titled "Total Task: 1 | Success : 1" shows one task row:

Status	Message	Hostname	System IP	Site ID	vManage IP
Success	Done - Push vSmart Policy	vSmart-1	100.1.1.13	1	100.1.1.12

At the bottom right of the table, it says "Total Rows: 1". The entire table row is highlighted with a red border.

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Main-Central-Policy → Click “...” → Edit.
- Click Topology on the Top of the page.
- Click Add Topology.
- Click “Import Existing” and select the DB-MPLS-INT from the dropdown list and click Import.
- Click Policy Application on the Top of the page.
- Click the “Topology” tab.
- The DB-MPLS-INT -Policy will be there. Click “New Site” button.
- Select Paris in the Outbound Site List.
- Click Add.
- Click the Save Policy button towards the button.
- Activate the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).
- Verify by using the Show IP route vpn 1 command on the Paris vEdge (vEdge4).
- It should only have 1 TLOC for Dubai routes (118.1.2.22– MPLS), whereas it will have 2 TLOCs for Hongkong (118.1.3.23-MPLS, 118.1.3.23-Biz-Internet).





Cisco vManage Not secure | 192.168.100.2/index.html#/app/config/policy?type=centralizedPolicy&action=edit&policyId=4d173a13-01f2-4786-a8e8-5c73a3fb427d admin

**CONFIGURATION | POLICIES Centralized Policy > Edit Policy**

Specify your network topology  
Topology VPN Membership

Add Topology

Name Type Description Reference Count Updated By Last Updated

Import Existing Topology

Policy Type: Hub And Spoke, Mesh, Custom Control (Route and TLOC) (selected)

Policy: DB-MPLS-INT

Import Cancel

Preview Save Policy Changes CANCEL

Start 3:21 PM 11/1/2020

Cisco vManage Not secure | 192.168.100.2/index.html#/app/device/status?activity=vsmart\_policy\_config&pid=vsmart\_policy\_config-fbfbe8b8-79e9-4524-8786-8f97ea9a4c37 admin

**TASK VIEW**

Push vSmart Policy Validation Success Initiated By: admin From: 192.168.100.5

Total Task: 1 | Success : 1

Search Options

Status	Message	Hostname	System IP	Site ID	vManage IP
Success	Done - Push vSmart Policy	vSmart-1	100.1.1.13	1	100.1.1.12

Start 3:45 PM 11/1/2020



```
vEdge4
l 192.168.43.0/24 ospf IA ge0/2 172.174.1.2 - - - - F,S
l 192.168.234.4/32 ospf IA ge0/2 172.174.1.2 - - - - F,S

vEdge-4# show omp tloc-paths
tloc-paths entries 118.1.2.22 mpls ipsec
tloc-paths entries 118.1.2.22 biz-internet ipsec
tloc-paths entries 118.1.3.23 mpls ipsec
tloc-paths entries 118.1.3.23 biz-internet ipsec
tloc-paths entries 118.1.4.24 mpls ipsec
tloc-paths entries 118.1.4.24 biz-internet ipsec
tloc-paths entries 118.1.5.25 default ipsec
tloc-paths entries 119.1.1.21 default ipsec
vEdge-4# show ip route vpn 1
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, L -> import

VPN  PREFIX      PROTOCOL   SUB TYPE  NEXTHOP  NEXTHOP  NEXTHOP  TLOC IP  COLOR  ENCAP  STATUS
      PREIF      PROTO     ADDR    VEN      IFNAME    ADDR    VEN      TLOCIP  COLOR   ENCP   STATUS
l 172.16.234.4/32 ospf IA ge0/2 172.174.1.2 - - - - F,S
l 172.172.1.0/24 omp - - - - 118.1.2.22 mpls ipsec F,S
l 172.173.1.0/24 omp - - - - 118.1.3.23 mpls ipsec F,S
l 172.173.1.0/24 omp - - - - 118.1.3.23 biz-internet ipsec F,S
l 172.174.1.0/24 ospf IA ge0/2 - - - - - - - - F,S
l 172.174.1.0/24 connected - - - - - - - - F,S
l 192.168.21.0/24 omp - - - - 118.1.2.22 mpls ipsec F,S
l 192.168.22.0/24 omp - - - - 118.1.2.22 mpls ipsec F,S
l 192.168.23.0/24 omp - - - - 118.1.2.22 mpls ipsec F,S
l 192.168.31.0/24 omp - - - - 118.1.3.23 mpls ipsec F,S
l 192.168.31.0/24 omp - - - - 118.1.3.23 biz-internet ipsec F,S
l 192.168.32.0/24 omp - - - - 118.1.3.23 mpls ipsec F,S
l 192.168.32.0/24 omp - - - - 118.1.3.23 biz-internet ipsec F,S
l 192.168.33.0/24 omp - - - - 118.1.3.23 mpls ipsec F,S
l 192.168.33.0/24 omp - - - - 118.1.3.23 biz-internet ipsec F,S
l 192.168.41.0/24 ospf IA ge0/2 172.174.1.2 - - - - F,S
l 192.168.42.0/24 ospf IA ge0/2 172.174.1.2 - - - - F,S
l 192.168.43.0/24 ospf IA ge0/2 172.174.1.2 - - - - F,S
l 192.168.234.2/32 omp - - - - 118.1.2.22 mpls ipsec F,S
l 192.168.234.3/32 omp - - - - 118.1.3.23 mpls ipsec F,S
l 192.168.234.3/32 omp - - - - 118.1.3.23 biz-internet ipsec F,S
l 192.168.234.4/32 ospf IA ge0/2 172.174.1.2 - - - - F,S

vEdge-4#
```



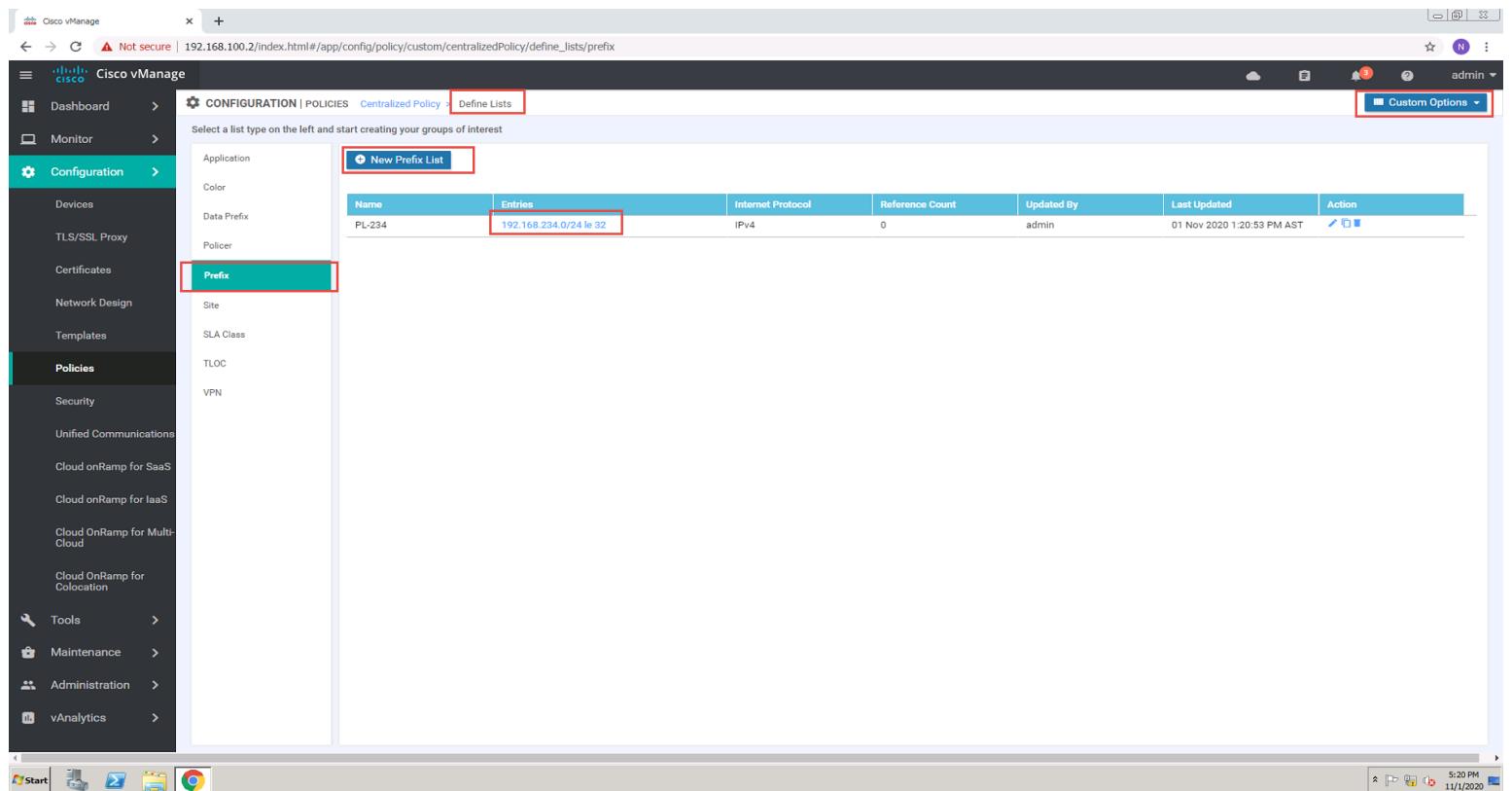
## Lab 29 - Configuring Route Filtering

### Requirements:

- The 172.16.234.2/32, 172.16.234.3/24 & 172.16.234.4/24 should not be propagated to the Newyork Site (Site 1).

### Task 1 – Configure Groups of Interests/List that will be used for Route Filtering Policy for Newyork

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Lists.
- Click Prefix and select New Prefix list. Create a policy based on the following:
  - o Name: PL-234
  - o Prefix List Entry: 192.168.234.0/24 le 32
- Click Site and select New Site list. Create a policy based on the following:
  - o Name : Newyork
  - o Site ID : 1



The screenshot shows the Cisco vManage web interface. The left sidebar is titled "Cisco vManage" and includes links for Dashboard, Monitor, Configuration (which is selected), Policies, Security, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, Cloud OnRamp for Multi-Cloud, Cloud OnRamp for Colocation, Tools, Maintenance, Administration, and vAnalytics. The main content area has a header "CONFIGURATION | POLICIES Centralized Policy Define Lists". A red box highlights the "Custom Options" button in the top right corner. Below it, a red box highlights the "Prefix" link in the sidebar under the "Policies" section. The central pane shows a table for a "New Prefix List" named "PL-234" with one entry: "192.168.234.0/24 le 32". The table columns are Name, Entries, Internet Protocol, Reference Count, Updated By, Last Updated, and Action.

Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated	Action
PL-234	192.168.234.0/24 le 32	IPv4	0	admin	01 Nov 2020 1:20:53 PM AST	



The screenshot shows the Cisco vManage web interface. The URL is 192.168.100.2/index.html#/app/config/policy/custom/centralizedPolicy/define\_lists/site. The left sidebar is titled 'Cisco vManage' and includes sections for Dashboard, Monitor, Configuration (with Site selected), Policies, Tools, Maintenance, Administration, and vAnalytics. The main content area is titled 'CONFIGURATION | POLICIES Centralized Policy > Define Lists'. It shows a 'Site List Name' input field with 'Newyork1' and an 'Add Site' button with '1' next to it. Below this is a table listing sites: Hongkong (3 entries, last updated 01 Nov 2020 5:34:09 AM AST), Dubai (2 entries, last updated 01 Nov 2020 5:33:59 AM AST), and Paris (4 entries, last updated 01 Nov 2020 11:42:15 AM AST). The 'Add' button at the bottom right of the list table is also highlighted with a red box.

## Task 2 – Configure Control/Topology policy based on the Requirements

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Topology.
- Configure 1 Route Policy based on the following:
  - o Policy Name : PREF-234-NOT-2-NY
  - o Description : PREF-234-NOT-2-NY

Route Sequence

Match Conditions:

- o Prefix List: PL-234

Action: Reject

- o Click Save Match and Actions to save the Sequence.

Default Sequence

Action

- o Accept
- o Click Save Match and Actions to save the Sequence.
- o Save the Policy





The screenshot shows the Cisco vManage web interface. The left sidebar is titled 'Cisco vManage' and includes sections for Dashboard, Monitor, Configuration (selected), Devices, TLS/SSL Proxy, Certificates, Network Design, Templates, Policies (selected), Security, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, Cloud OnRamp for Multi-Cloud, Cloud OnRamp for Colocation, Tools, Maintenance, Administration, and vAnalytics. The main content area is titled 'CONFIGURATION | POLICIES' and shows 'Centralized Policy > Topology > Edit Custom Control Policy'. The policy is named 'PREF-234-NOT-2-NY' and has a 'Route' sequence type. It contains one rule with match conditions 'PL-234' and action 'Reject'. The policy is enabled. At the bottom right of the main area, there are 'Save Control Policy' and 'Cancel' buttons. The status bar at the bottom right shows the date and time: 5:28 PM 11/1/2020.

### Task 3 – Modify the existing Centralized Policy “Main-CentralPolicy” and call the Topology Policy

- In vManage, Navigate to Configuration → Policies → Custom Options → Centralized Policy → Main-Central-Policy → Click “...” → Edit.
- Click Topology on the Top of the page.
- Click Add Topology.
- Click “Import Existing” and select the PREF-234-NOT-2-NY from the drop-down list and click Import.
- Click Policy Application on the Top of the page.
- Click the “Topology” tab.
- The PREF-234-NOT-2-NY will be there. Click “New Site” button.
- Select Newyork in the Outbound Site List.
- Click Add.
- Click the Save Policy button towards the button.
- Activate the policy.
- Wait for it to push the policy to the reachable vSmart Controller(s).
- Verify by using the Show IP route vpn 1 command on the Newyork vEdge (vEdge1).
- It should all the routes from the Branches except the 192.168.234.X/32routes.
- These routes should be present in the vEdge2, vEdge3 and vEdge4 routers. You can use the Show IP route vpn 1 command to verify.





Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/policy?type=centralizedPolicy&action=edit&policyId=4d173a13-01f2-4786-a8e8-5c73a3fb427d

**CONFIGURATION | POLICIES** Centralized Policy > Edit Policy

Topology Traffic Rules

Specify your network topology

Add Topology

Import Existing Topology

Name	Type	Description	Reference Count	Updated By	Last Updated
DB-MPLS-INT	Custom		0	min	01 Nov 2020 12:10:03 PM AST

Policy Type: Custom Control (Route and TLOC)

Policy: PREF-234-NOT-2-NY

Import

Preview Save Policy Changes CANCEL

Cisco vManage

Not secure | 192.168.100.2/index.html#/app/config/policy?type=centralizedPolicy&action=edit&policyId=4d173a13-01f2-4786-a8e8-5c73a3fb427d

**CONFIGURATION | POLICIES** Centralized Policy > Edit Policy

Policy Application

Add policies to sites and VPNs

Policy Name: Main-Central-Policy

Policy Description: Main-Central-Policy

Topology

PREF-234-NOT-2-NY

New Site List

Direction: out

Site List: Newyork

Action

DB-MPLS-INT

New Site List

Direction: out

Site List: Paris

Action

Preview Save Policy Changes CANCEL





vEdge1

```
vEdge-1# show ip route
Codes Proto-sub-type:
 IA -> ospf-intia-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, L -> import
```

VPN	PREFIX	PROTOCOL	PROTOCOL	SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	NEXTHOP VPN	TLOC IP	COLOR	ENCAP	STATUS
0	0.0.0.0/0	static	-	ge0/0	119.1.1.2	-	-	-	-	-	F,S
0	10.1.11.0/24	bgp	i	ge0/0	119.1.1.2	-	-	-	-	-	F,S
0	10.1.12.0/24	bgp	i	-	10.1.11.2	-	-	-	-	-	I
0	10.1.13.0/24	bgp	i	-	10.1.11.2	-	-	-	-	-	I
0	10.1.14.0/24	bgp	i	-	10.1.11.2	-	-	-	-	-	I
0	10.1.15.0/24	bgp	i	-	10.1.11.2	-	-	-	-	-	I
0	100.1.1.0/24	bgp	i	ge0/0	119.1.1.2	-	-	-	-	-	F,S
0	119.1.1.0/24	bgp	i	-	119.1.1.2	-	-	-	-	-	I
0	119.1.1.0/24	connected	-	ge0/0	-	-	-	-	-	-	F,S
0	119.1.1.21/32	connected	-	system	-	-	-	-	-	-	F,S
1	172.16.234.4/32	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	172.171.1.0/24	ospf	IA	ge0/2	-	-	-	-	-	-	-
1	172.171.1.0/24	connected	-	ge0/2	-	-	-	-	-	-	F,S
1	172.172.1.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	172.173.1.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	ipsec	F,S
1	172.174.1.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	172.175.1.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	ipsec	F,S
1	192.168.11.0/24	ospf	IA	ge0/2	172.171.1.2	-	-	-	-	-	F,S
1	192.168.12.0/24	ospf	IA	ge0/2	172.171.1.2	-	-	-	-	-	F,S
1	192.168.13.0/24	ospf	IA	ge0/2	172.171.1.2	-	-	-	-	-	F,S
1	192.168.21.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	192.168.22.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	192.168.23.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	192.168.31.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	ipsec	F,S
1	192.168.33.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	ipsec	F,S
1	192.168.41.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	192.168.42.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	192.168.43.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	192.168.51.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	ipsec	F,S
1	192.168.52.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	ipsec	F,S
1	192.168.53.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	ipsec	F,S
1	192.168.234.2/32	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	192.168.234.3/32	omp	-	-	-	-	118.1.3.23	mpls	ipsec	ipsec	F,S
1	192.168.234.4/32	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S

Before apply policy

vEdge1

```
vEdge-1# show ip route
Codes Proto-sub-type:
 IA -> ospf-intia-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, L -> import
```

VPN	PREFIX	PROTOCOL	PROTOCOL	SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	NEXTHOP VPN	TLOC IP	COLOR	ENCAP	STATUS
0	0.0.0.0/0	static	-	ge0/0	119.1.1.2	-	-	-	-	-	F,S
0	10.1.11.0/24	bgp	i	ge0/0	119.1.1.2	-	-	-	-	-	F,S
0	10.1.12.0/24	bgp	i	-	10.1.11.2	-	-	-	-	-	I
0	10.1.13.0/24	bgp	i	-	10.1.11.2	-	-	-	-	-	I
0	10.1.14.0/24	bgp	i	-	10.1.11.2	-	-	-	-	-	I
0	10.1.15.0/24	bgp	i	-	10.1.11.2	-	-	-	-	-	I
0	100.1.1.0/24	bgp	i	ge0/0	119.1.1.2	-	-	-	-	-	F,S
0	119.1.1.0/24	bgp	i	-	119.1.1.2	-	-	-	-	-	I
0	119.1.1.21/32	connected	-	ge0/0	-	-	-	-	-	-	F,S
1	172.16.234.4/32	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	172.171.1.0/24	ospf	IA	ge0/2	-	-	-	-	-	-	-
1	172.171.1.0/24	connected	-	ge0/2	-	-	-	-	-	-	F,S
1	172.172.1.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	172.173.1.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	ipsec	F,S
1	172.174.1.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	172.175.1.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	ipsec	F,S
1	192.168.11.0/24	ospf	IA	ge0/2	172.171.1.2	-	-	-	-	-	F,S
1	192.168.12.0/24	ospf	IA	ge0/2	172.171.1.2	-	-	-	-	-	F,S
1	192.168.13.0/24	ospf	IA	ge0/2	172.171.1.2	-	-	-	-	-	F,S
1	192.168.21.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	192.168.22.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	192.168.23.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	192.168.31.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	ipsec	F,S
1	192.168.33.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	ipsec	F,S
1	192.168.41.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	192.168.42.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	192.168.43.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S
1	192.168.51.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	ipsec	F,S
1	192.168.52.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	ipsec	F,S
1	192.168.53.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	ipsec	F,S
1	192.168.234.2/32	omp	-	-	-	-	118.1.2.22	mpls	ipsec	ipsec	F,S
1	192.168.234.3/32	omp	-	-	-	-	118.1.3.23	mpls	ipsec	ipsec	F,S
1	192.168.234.4/32	omp	-	-	-	-	118.1.4.24	mpls	ipsec	ipsec	F,S

Before apply policy





```
vEdge4#
vEdge-4#
vEdge-4# show ip route vpn 1
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-external-area,
  E1 -> ospf-external1, E2 -> ospf-external12,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external12,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import

VPN  PREFIX          PROTOCOL      NEXTHOP     NEXTHOP      NEXTHOP      TLOC IP      COLOR      ENCAP      STATUS
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1    172.16.234.4/32  ospf          IA           ge0/2       172.174.1.2   -           118.1.3.23  biz-internet  ipsec      F,S
1    192.168.41.0/24   ospf          IA           ge0/2       172.174.1.2   -           -           -           -           -           F,S
1    192.168.42.0/24   ospf          IA           ge0/2       172.174.1.2   -           -           -           -           -           F,S
1    192.168.43.0/24   ospf          IA           ge0/2       172.174.1.2   -           -           -           -           -           F,S
1    192.168.234.2/32  ospf          -            -           -           -           118.1.2.22  mpls        ipsec      F,S
1    192.168.234.3/32  ospf          -            -           -           -           118.1.3.23  mpls        ipsec      F,S
1    192.168.234.3/32  ospf          -            -           -           -           118.1.3.23  biz-internet  ipsec      F,S
1    192.168.234.4/32  ospf          IA           ge0/2       172.174.1.2   -           -           -           -           -           F,S

vEdge-4#
vEdge-4#
```

