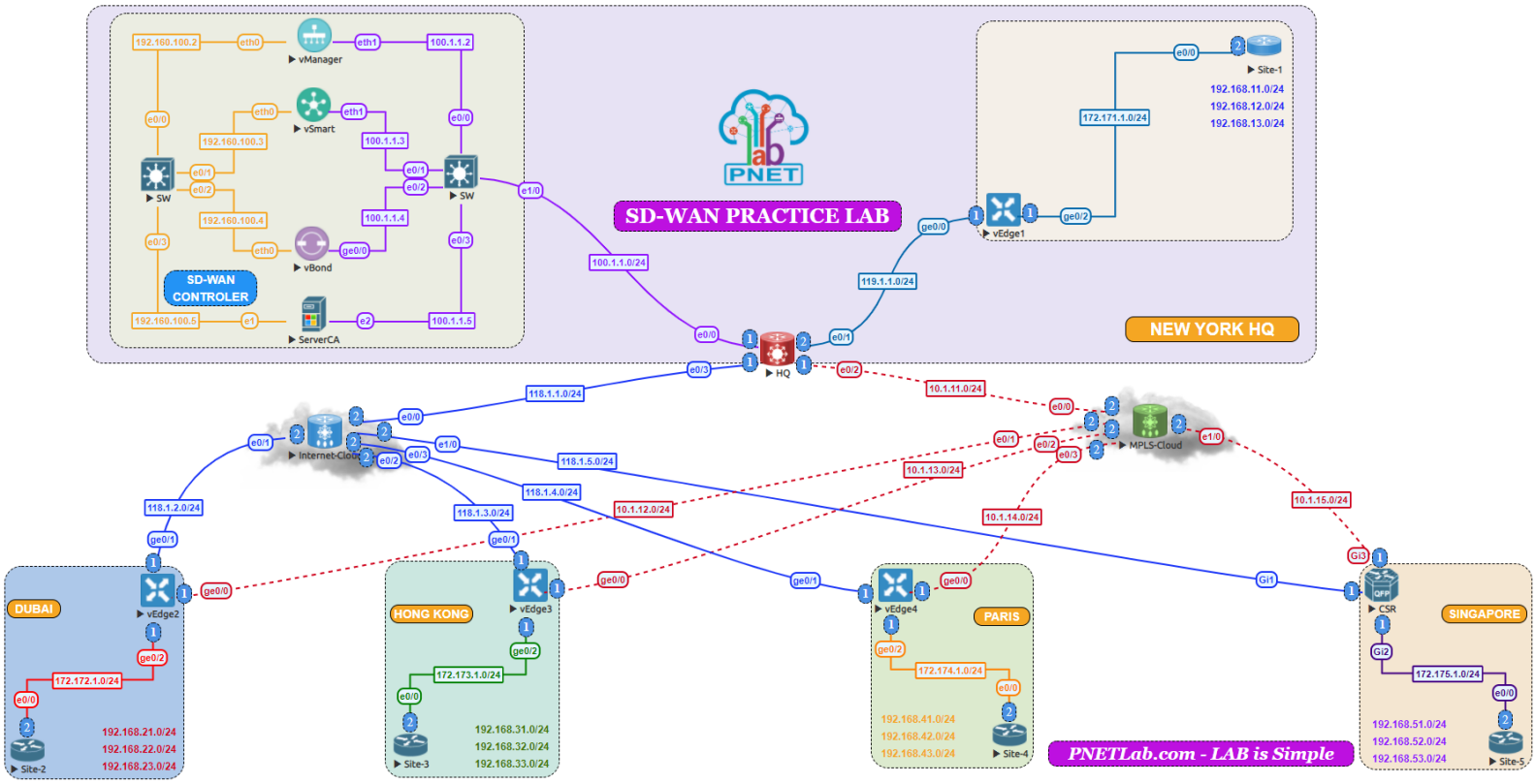
SD-WAN Practice LAB 1 – PNETLab.com



Lab Topology

Table of Contents

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

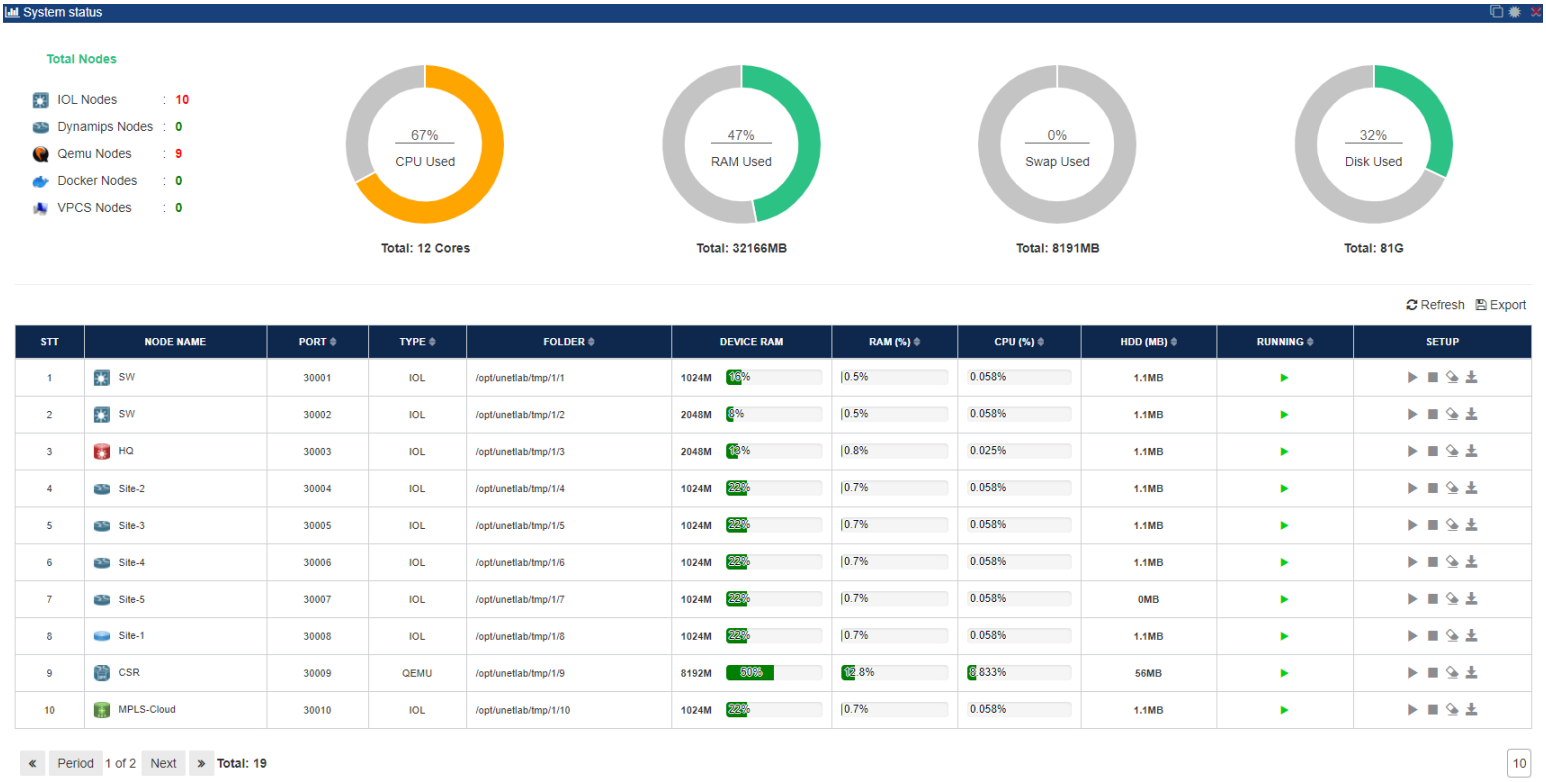
HOW TO SETUP LAB

Hardware Requirement

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

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

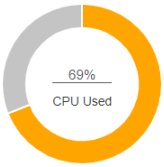
- Join the Telegram group support: https://t.me/rackrental
- Pricing: **25 USD/1 week**
  - Dedicated IP, Server for pactice SD-WAN LAB.
  - Included: all in one (IOS, Licensed, Workbook…) just practice only.
  - Support: 24/7



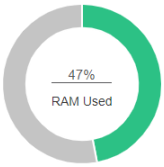
System status

Total Nodes

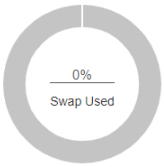
- IOL Nodes : 10
- Dynamips Nodes : 0
- Qemu Nodes : 9
- Docker Nodes : 0
- VPCS Nodes : 0



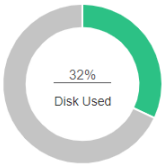
Total: 12 Cores



Total: 32166MB



Total: 8191MB



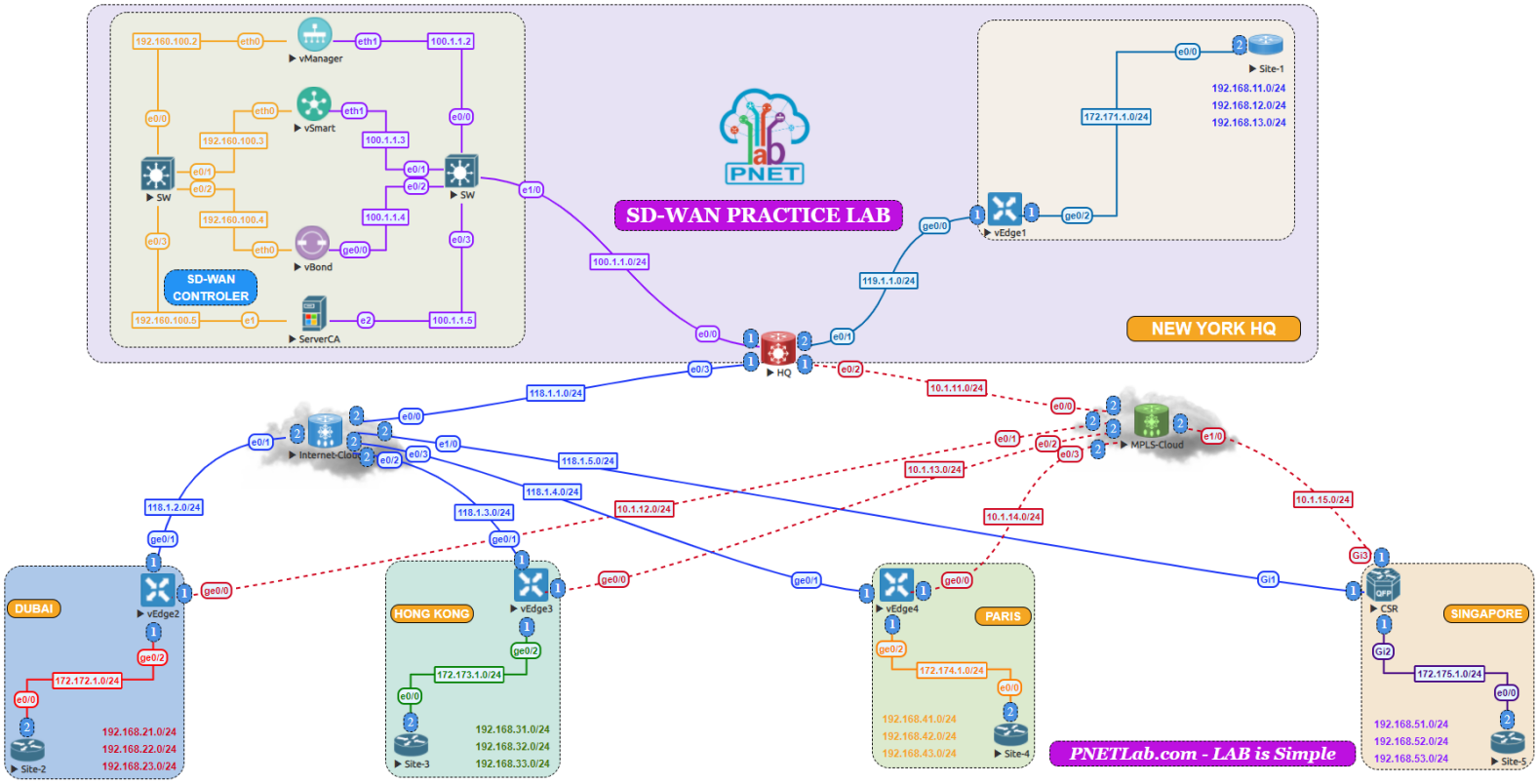
Total: 81G

Refresh Export

STT	NODE NAME	PORT	TYPE	FOLDER	DEVICE RAM	RAM (%)	CPU (%)	HDD (MB)	RUNNING	SETUP
11	Internet-Cloud	30011	IOL	/opt/unetlab/tmp/1/11	2048M 1%	0.7%	0.058%	1.1MB	▶	
12	vManager	30012	QEMU	/opt/unetlab/tmp/1/12	16384M 20%	10%	0.125%	201.6MB	▶	
13	vSmart	30013	QEMU	/opt/unetlab/tmp/1/13	4096M 22%	2.8%	0.775%	15.5MB	▶	
14	vBond	30014	QEMU	/opt/unetlab/tmp/1/14	2048M 50%	3.2%	0.108%	16.7MB	▶	
15	vEdge1	30015	QEMU	/opt/unetlab/tmp/1/15	4096M 31%	4%	0.917%	96.7MB	▶	
16	vEdge2	30016	QEMU	/opt/unetlab/tmp/1/16	2048M 50%	3.2%	0.858%	17.8MB	▶	
17	vEdge3	30017	QEMU	/opt/unetlab/tmp/1/17	2048M 52%	3.3%	0.992%	100.7MB	▶	
18	vEdge4	30018	QEMU	/opt/unetlab/tmp/1/18	2048M 50%	3.2%	0.667%	16.8MB	▶	
19	ServerCA	30020	QEMU	/opt/unetlab/tmp/1/20	4096M 10%	1.3%	0.525%	0.2MB	▶	

« Period 2 of 2 Next » Total: 19

10



Link to download lab and Setup

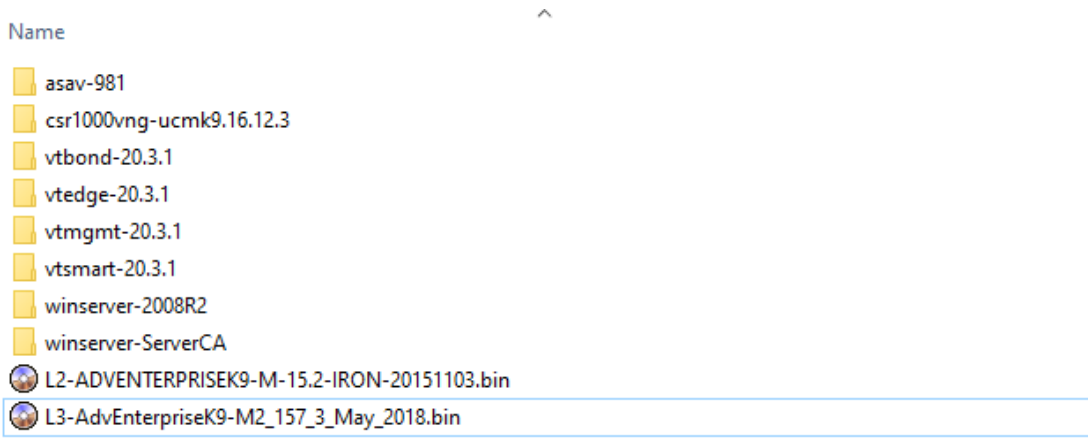
Note: Lab devices

- 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. Prerequirement:

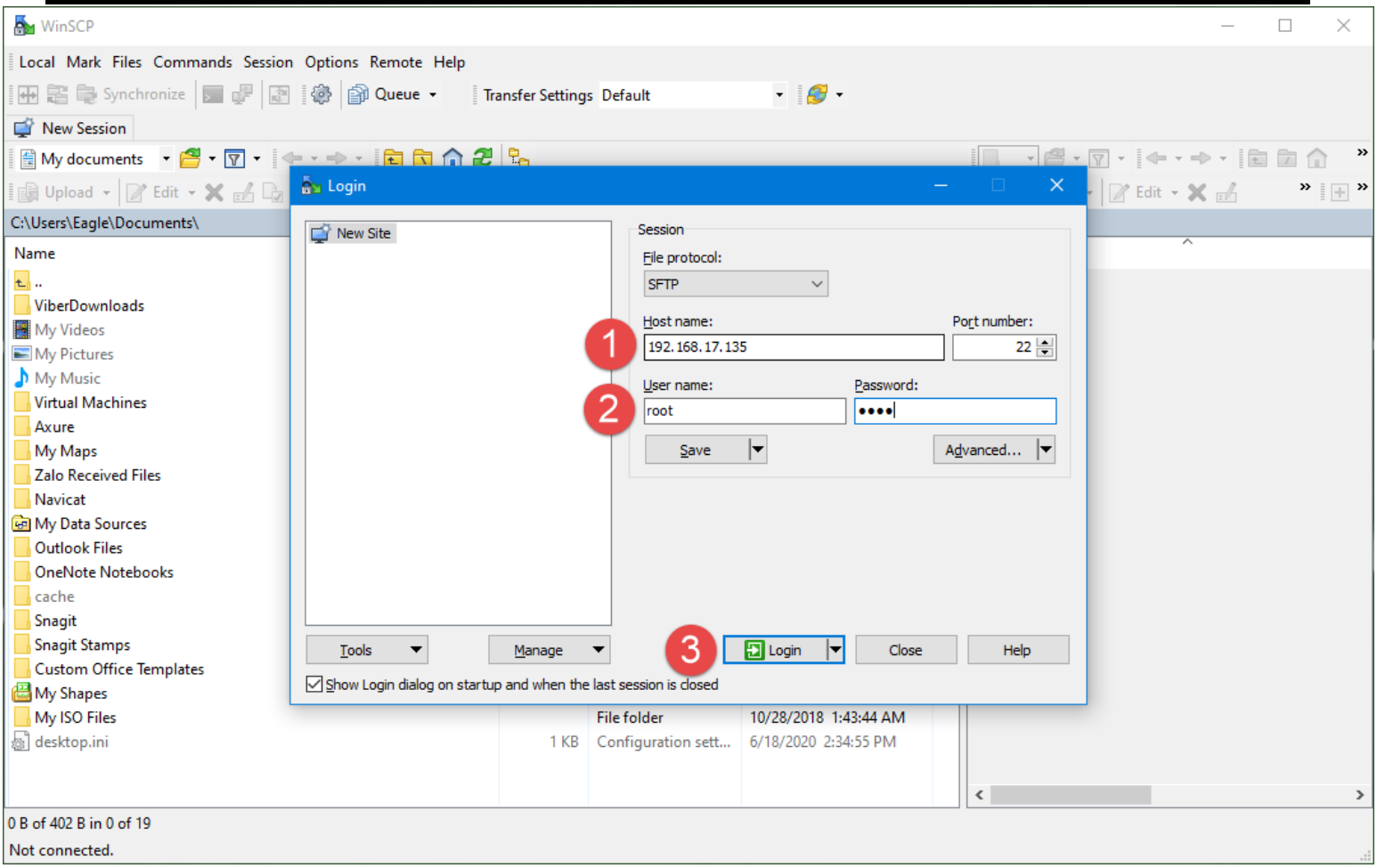
- Download PNETLab platform and lab in the link:
  - Link to download PNETLab Platform and setup: https://pnetlab.com/pages/download
  - Link to download Lab from Store: https://user.pnetlab.com/store/labs/detail?id=16052623645692
  - Download WINSCP in the link then setup: https://winscp.net/eng/download.php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

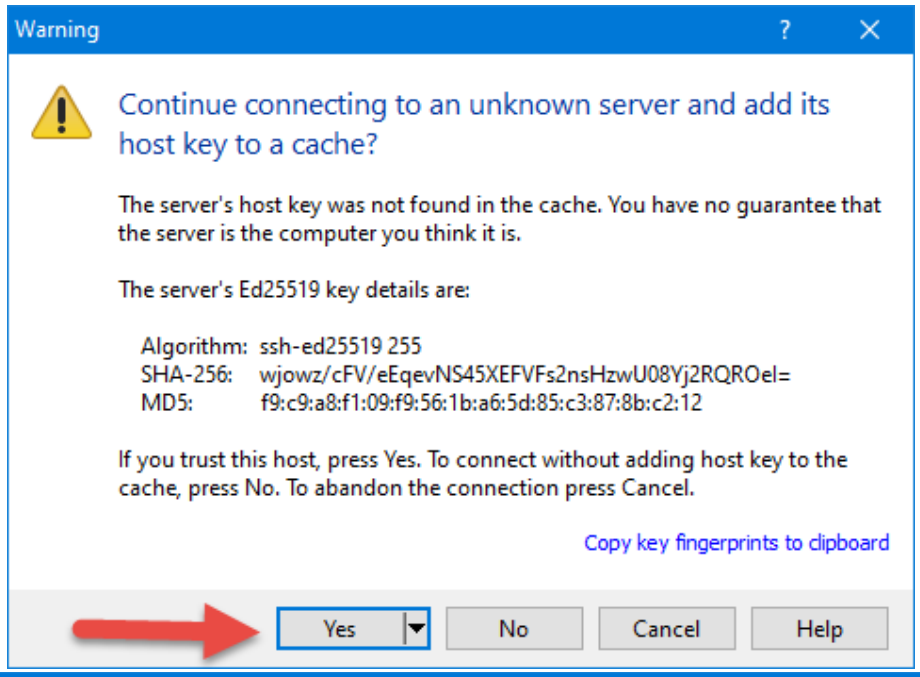


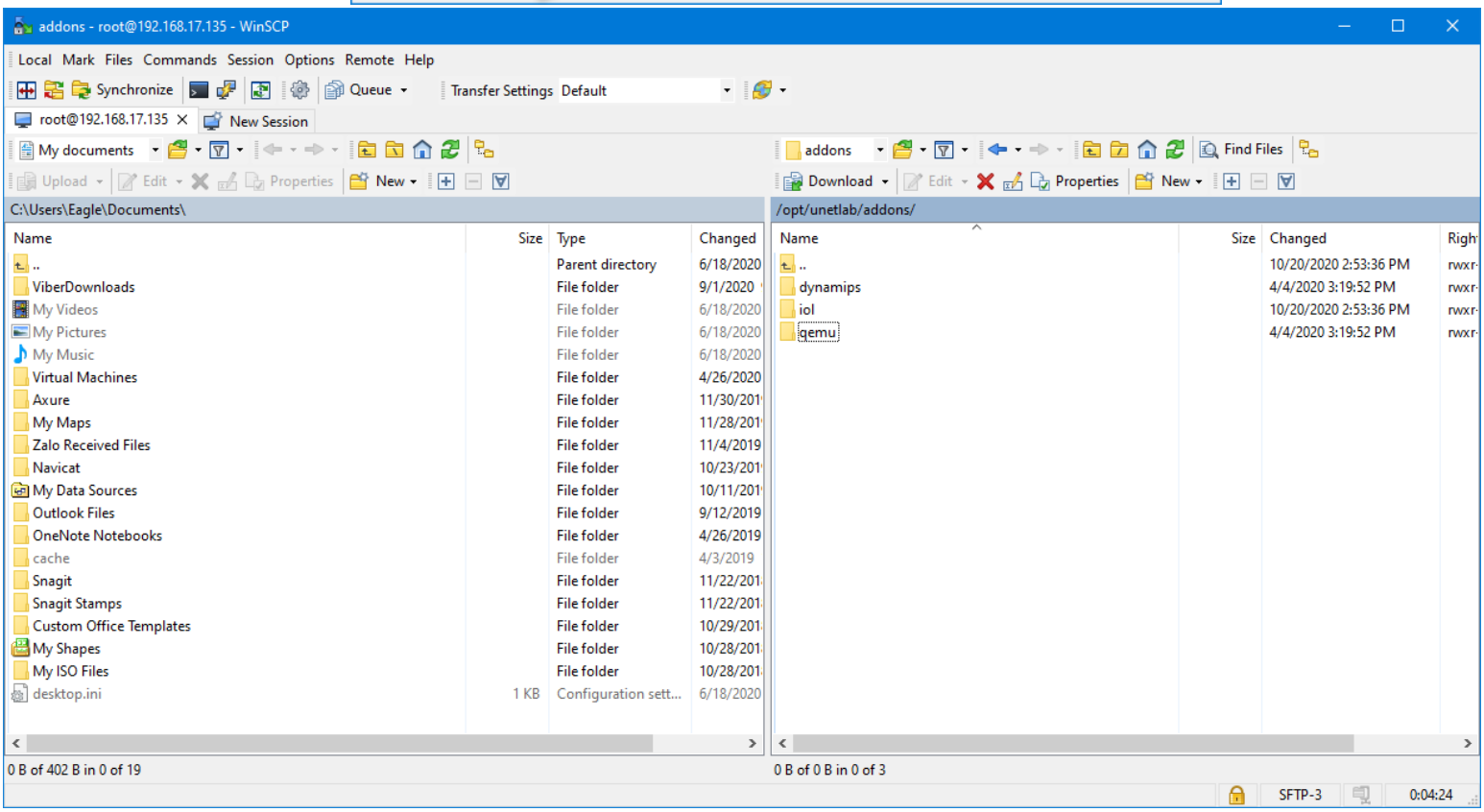
b. Upload Images into PNETLab:

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

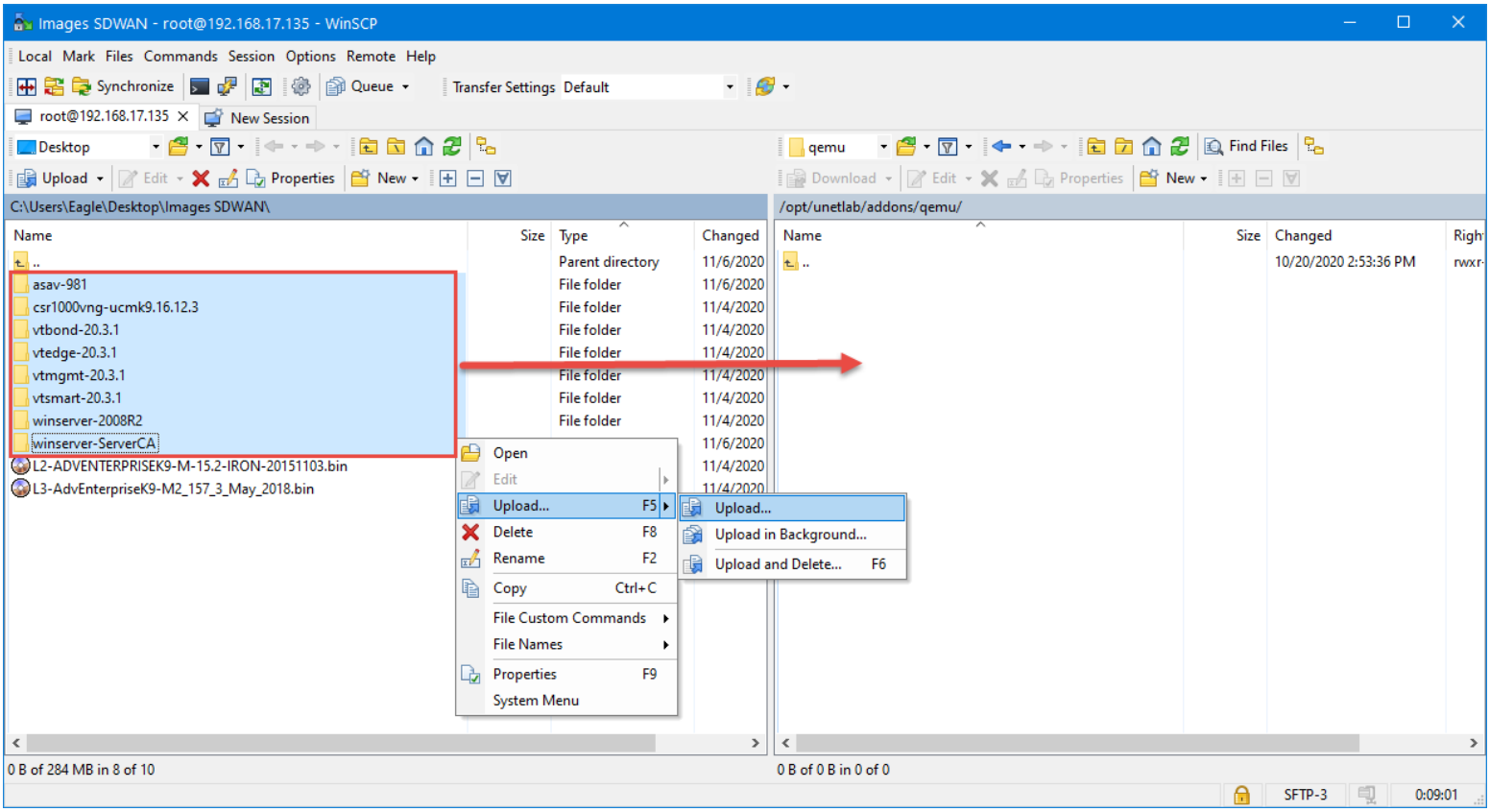

PNETLab (default root password is 'pnet')
Use https or http://192.168.17.135/
pnetlab login: _

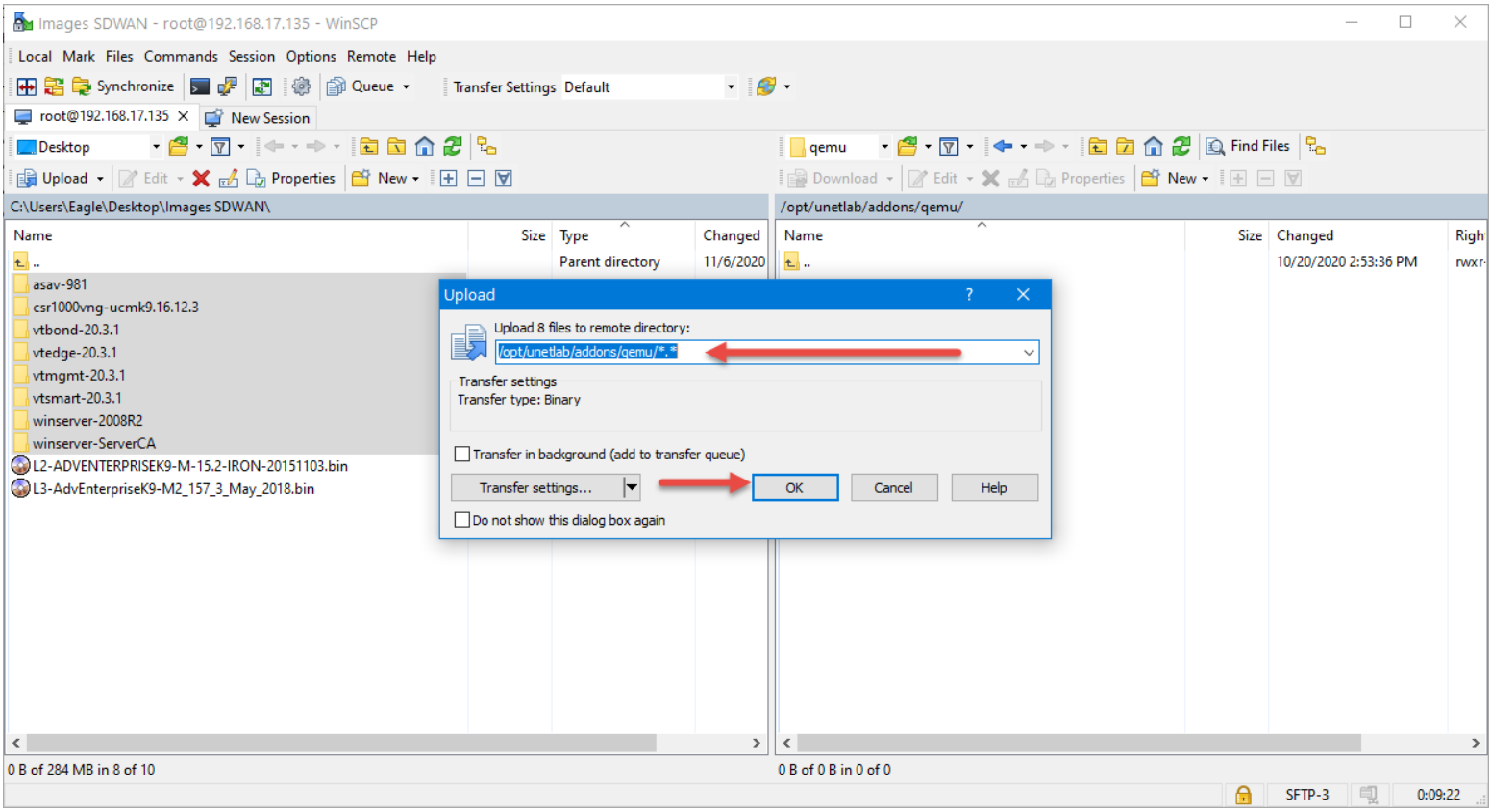

WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
New Session
My documents
Upload
Edit
C:\Users\Eagle\Documents\
Name
ViberDownloads
My Videos
My Pictures
My Music
Virtual Machines
Axure
My Maps
Zalo Received Files
Navicat
My Data Sources
Outlook Files
OneNote Notebooks
cache
Snagit
Snagit Stamps
Custom Office Templates
My Shapes
My ISO Files
desktop.ini
File folder
10/28/2018 1:43:44 AM
1 KB
Configuration sett...
6/18/2020 2:34:55 PM
0 B of 402 B in 0 of 19
Not connected.
Login
New Site
Session
File protocol:
SFTP
Host name:
Port number:
192.168.17.135
22
User name:
Password:
root
Save
Advanced...
Tools
Manage
Login
Close
Help
Show Login dialog on startup and when the last session is closed
1
2
3

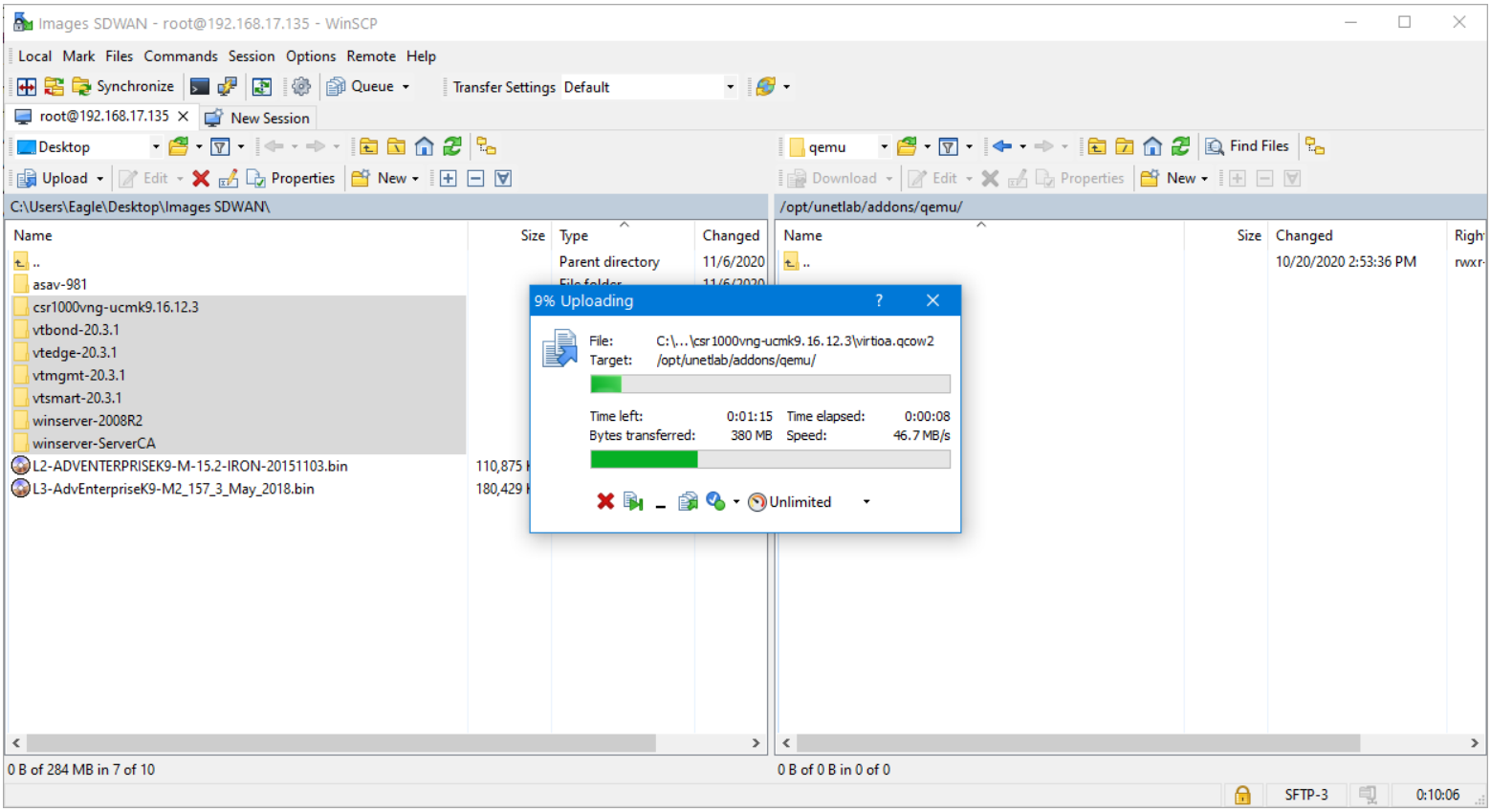




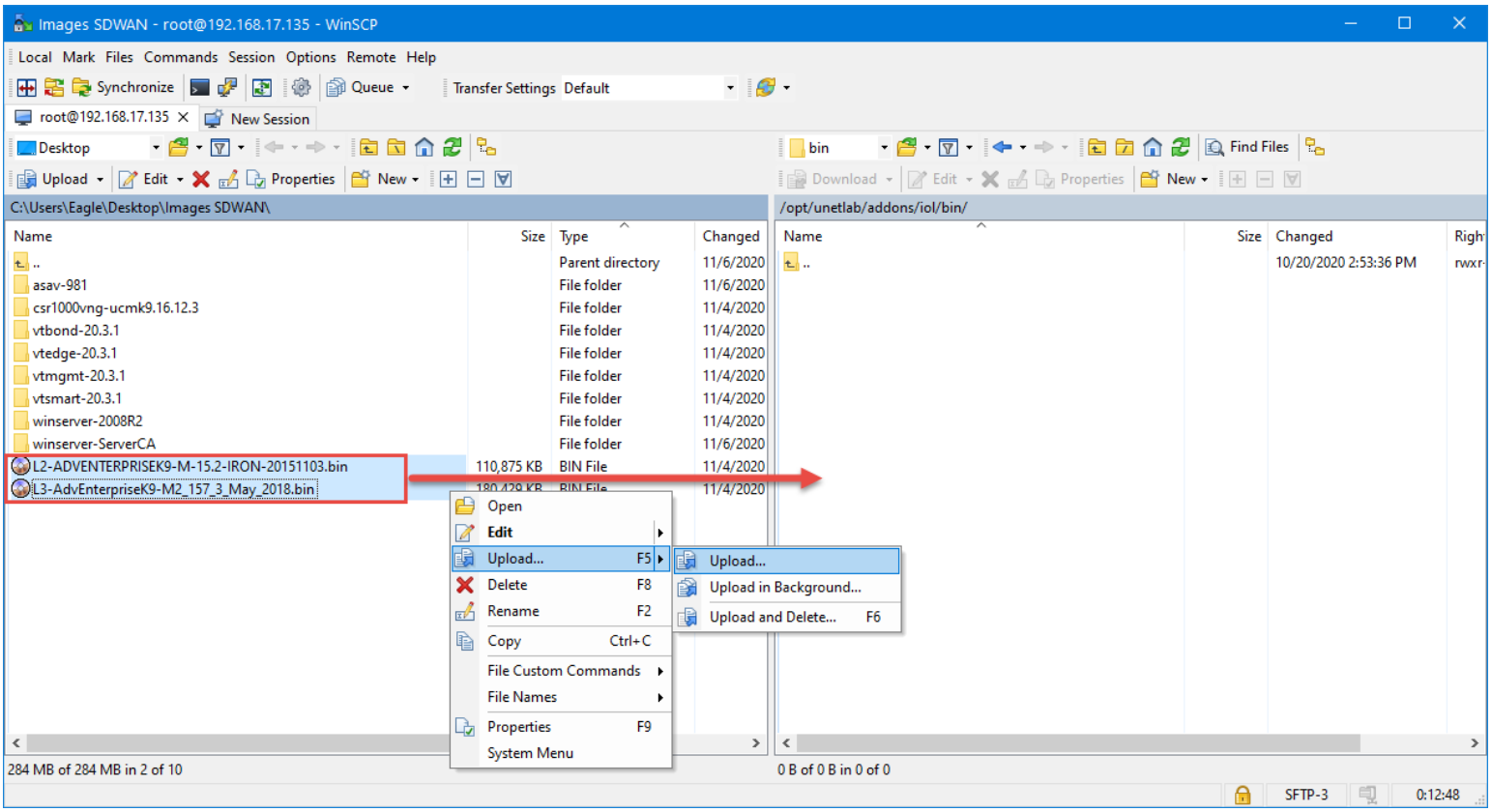
- **Step 2:** Upload Qemu Images and IOS as shown below:
  - **Upload All Qemu Images to folder: /opt/unetlab/addons/qemu**

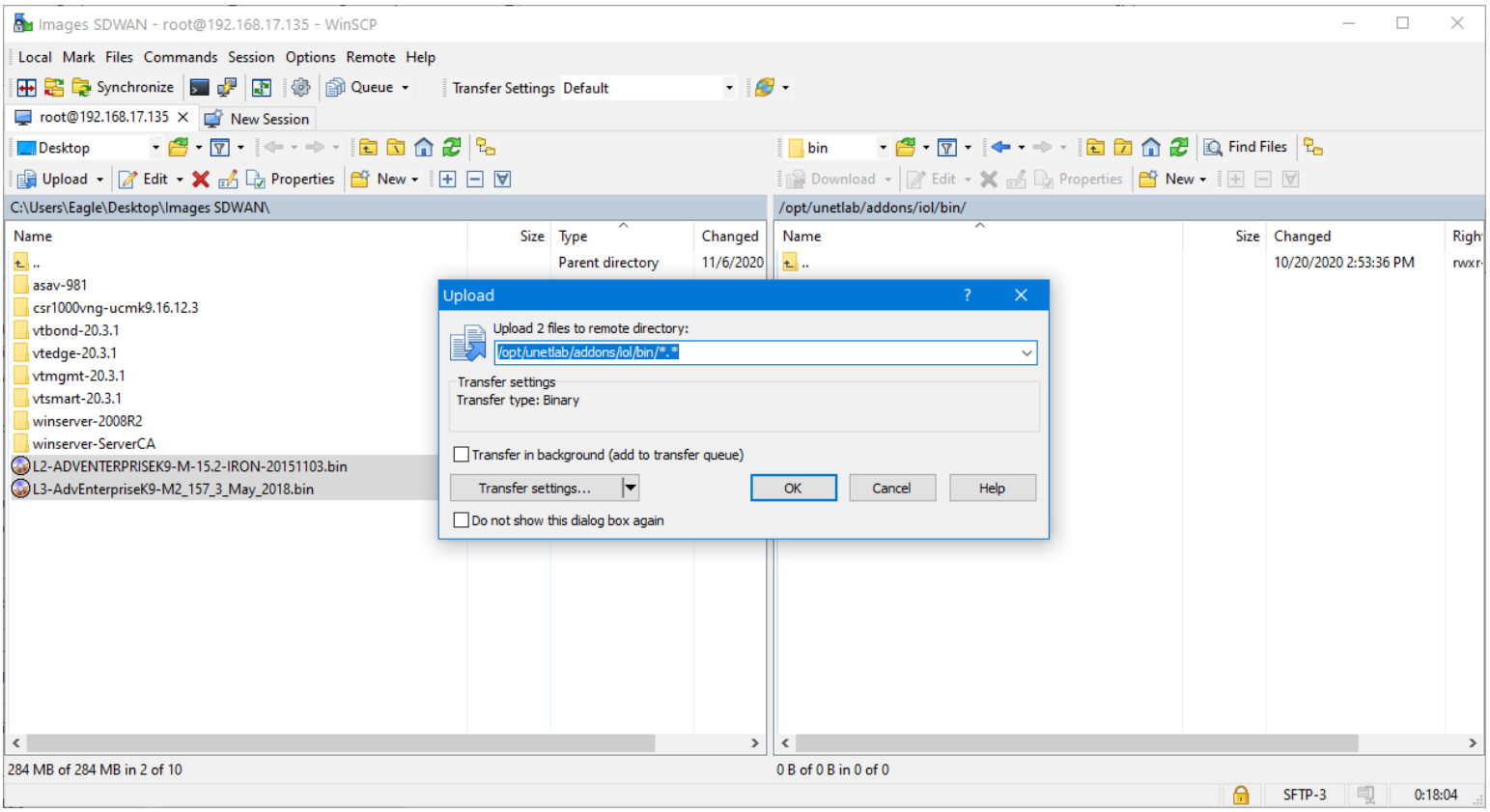

Images SDWAN - root@192.168.17.135 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
root@192.168.17.135
New Session
Desktop
Upload
Edit
Properties
New
qemu
Find Files
Download
C:\Users\Eagle\Desktop\Images SDWAN\
/opt/unetlab/addons/qemu/
Name
Size
Type
Changed
Parent directory
11/6/2020
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
Open
Edit
Upload... F5
Delete F8
Rename F2
Copy Ctrl+C
File Custom Commands
File Names
Properties F9
System Menu
Upload...
Upload in Background...
Upload and Delete... F6
10/20/2020 2:53:36 PM
0 B of 284 MB in 8 of 10
0 B of 0 B in 0 of 0
SFTP-3
0:09:01

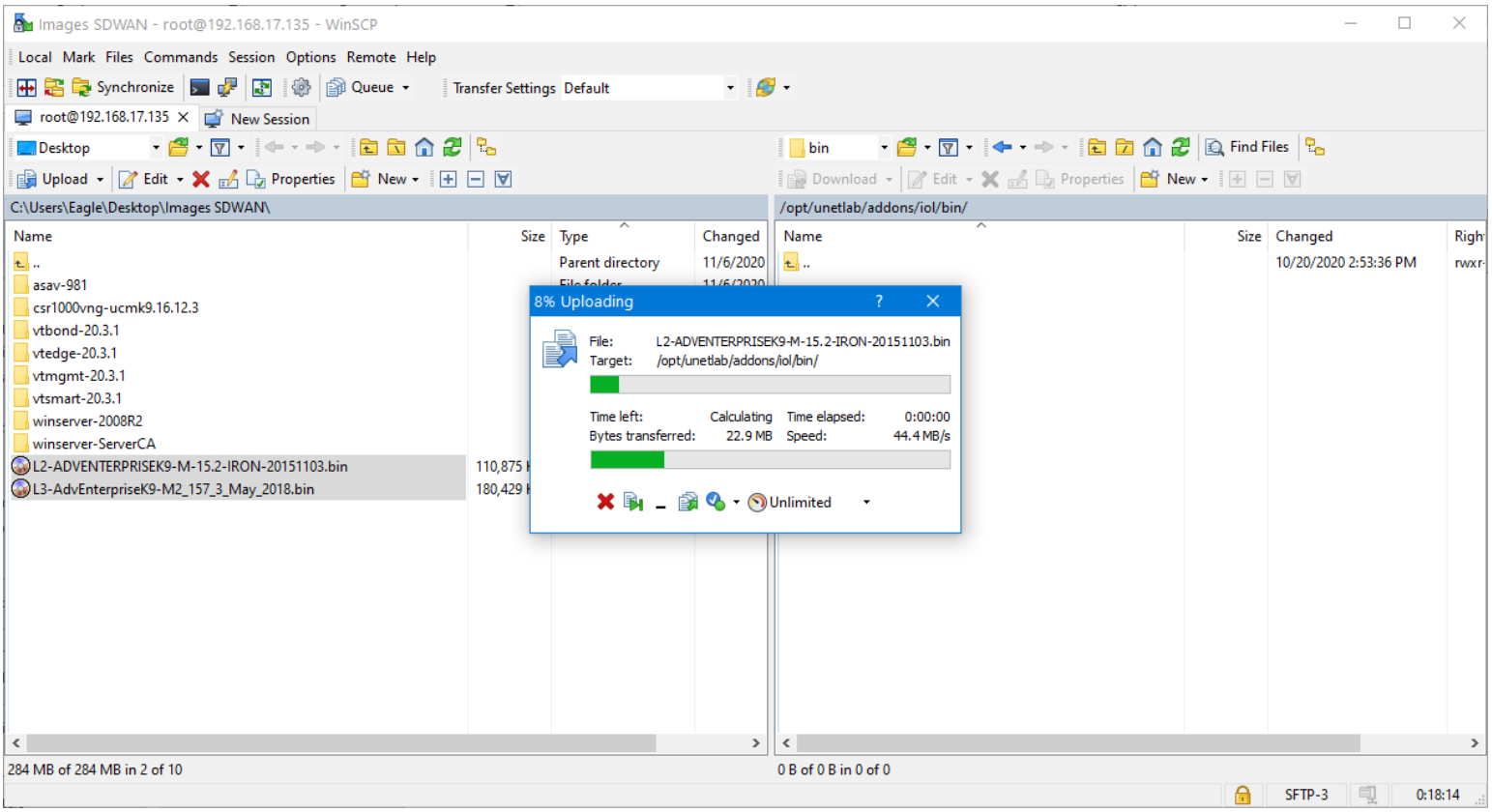

Images SDWAN - root@192.168.17.135 - WinSCP
Upload
Upload 8 files to remote directory:
/opt/unetlab/addons/qemu/*.*
Transfer settings
Transfer type: Binary
Transfer in background (add to transfer queue)
Transfer settings...
OK
Cancel
Help
Do not show this dialog box again
0 B of 284 MB in 8 of 10
0 B of 0 B in 0 of 0
SFTP-3
0:09:22



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


Images SDWAN - root@192.168.17.135 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
root@192.168.17.135
New Session
Desktop
Upload
Edit
Properties
New
C:\Users\Eagle\Desktop\Images SDWAN\
bin
Find Files
Download
/opt/unetlab/addons/iol/bin/
Name
Size
Type
Changed
Parent directory
11/6/2020
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
110,875 KB
BIN File
11/4/2020
L3-AdvEnterpriseK9-M2_157_3_May_2018.bin
Open
Edit
Upload... F5
Delete F8
Rename F2
Copy Ctrl+C
File Custom Commands
File Names
Properties F9
System Menu
Upload...
Upload in Background...
Upload and Delete... F6
10/20/2020 2:53:36 PM
284 MB of 284 MB in 2 of 10
0 B of 0 B in 0 of 0
SFTP-3
0:12:48


Images SDWAN - root@192.168.17.135 - WinSCP
Upload
Upload 2 files to remote directory:
/opt/unetlab/addons/iol/bin/*.*
Transfer settings
Transfer type: Binary
Transfer in background (add to transfer queue)
Transfer settings...
OK
Cancel
Help
Do not show this dialog box again
284 MB of 284 MB in 2 of 10
0 B of 0 B in 0 of 0
SFTP-3
0:18:04



- **Upload tempalte file for SD-WAN devices to Folder: /opt/unetlab/html/templates**

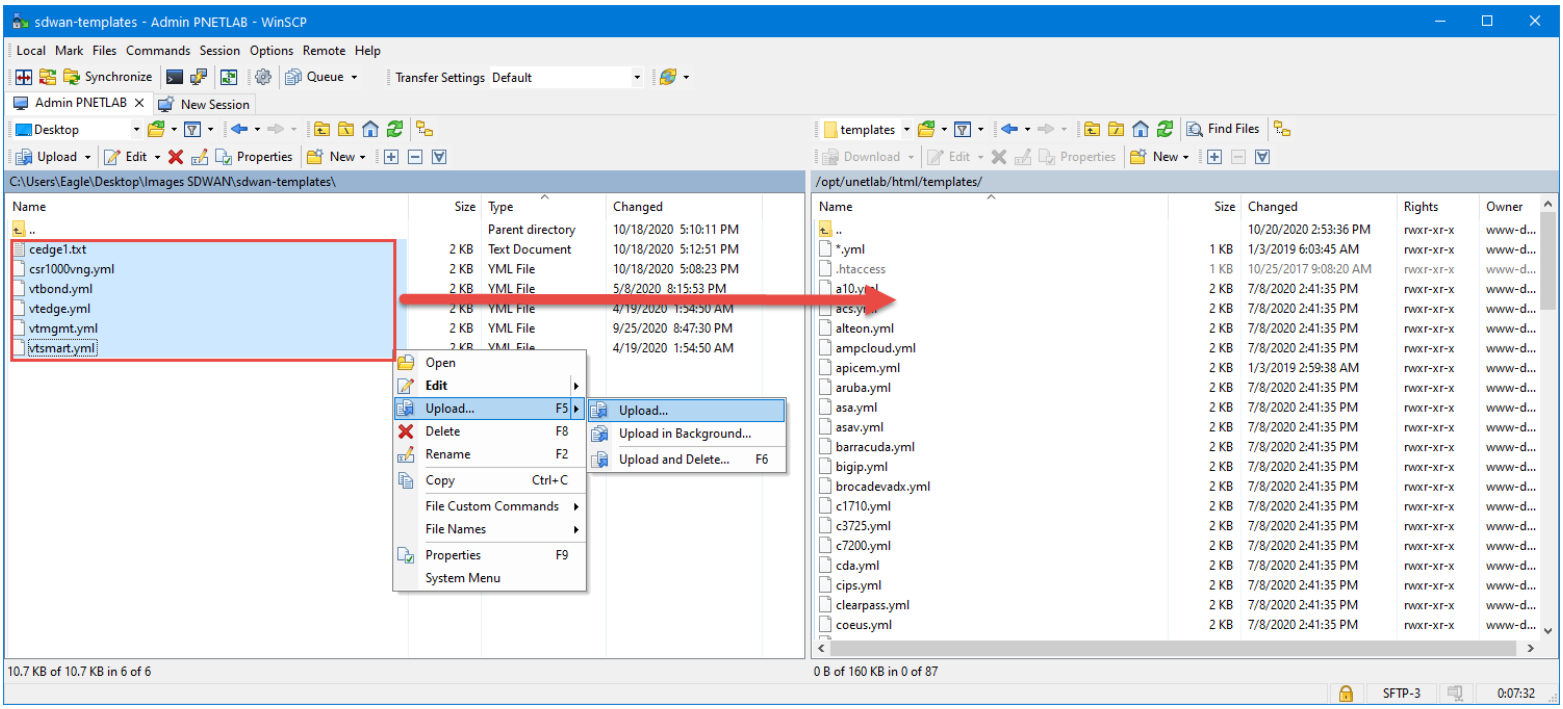
If you skip this step, SD-WAN devices cannot start properly

Link to download Template file:
https://drive.google.com/file/d/1CZqoBv27HBJH3aUTwVDlfPXBr6KX3N5p/view?usp=sharing

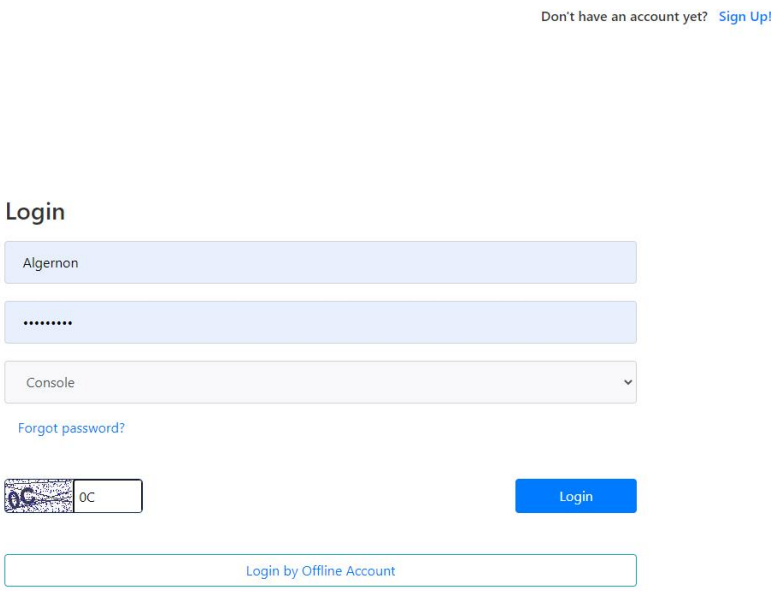
Backup Link: https://mega.nz/file/uzxEEKLK#LvfeYdKR_SFi-msYcJgDHQ2vdRrpBltEKqcLChcCiRs

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

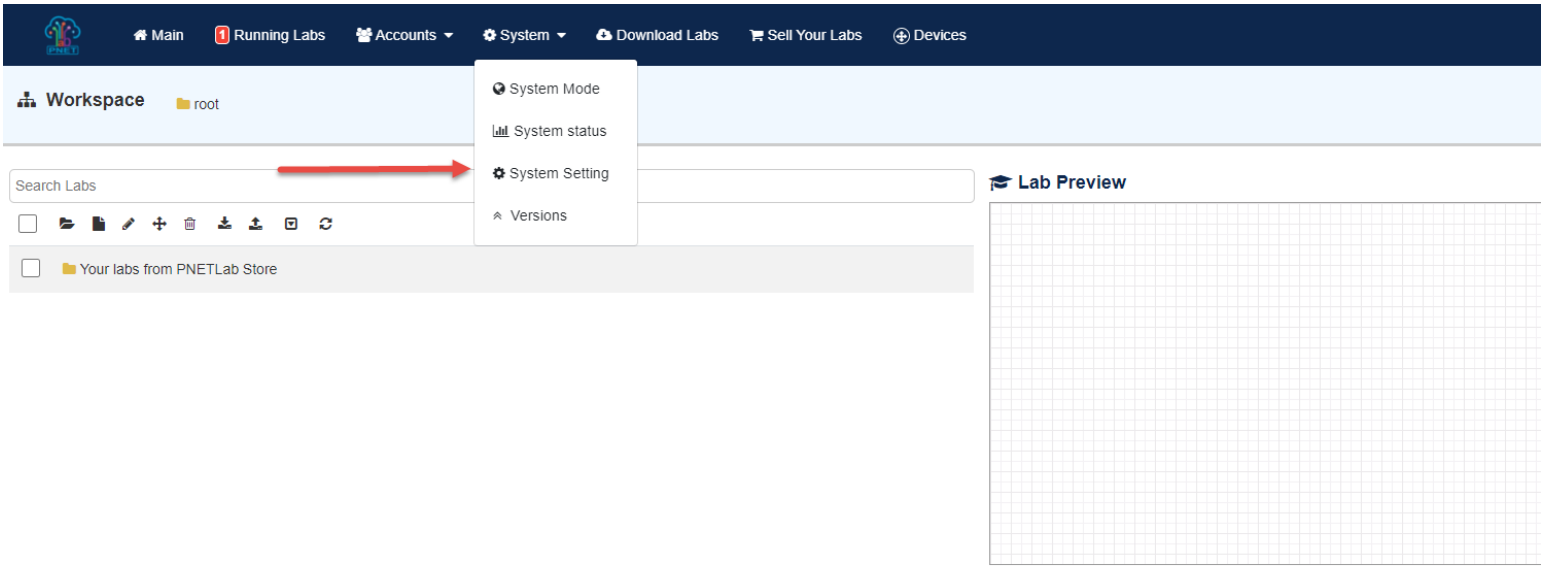
Note: If you are using **PNETLab Version from 4.2.0**, You do not need to do this step



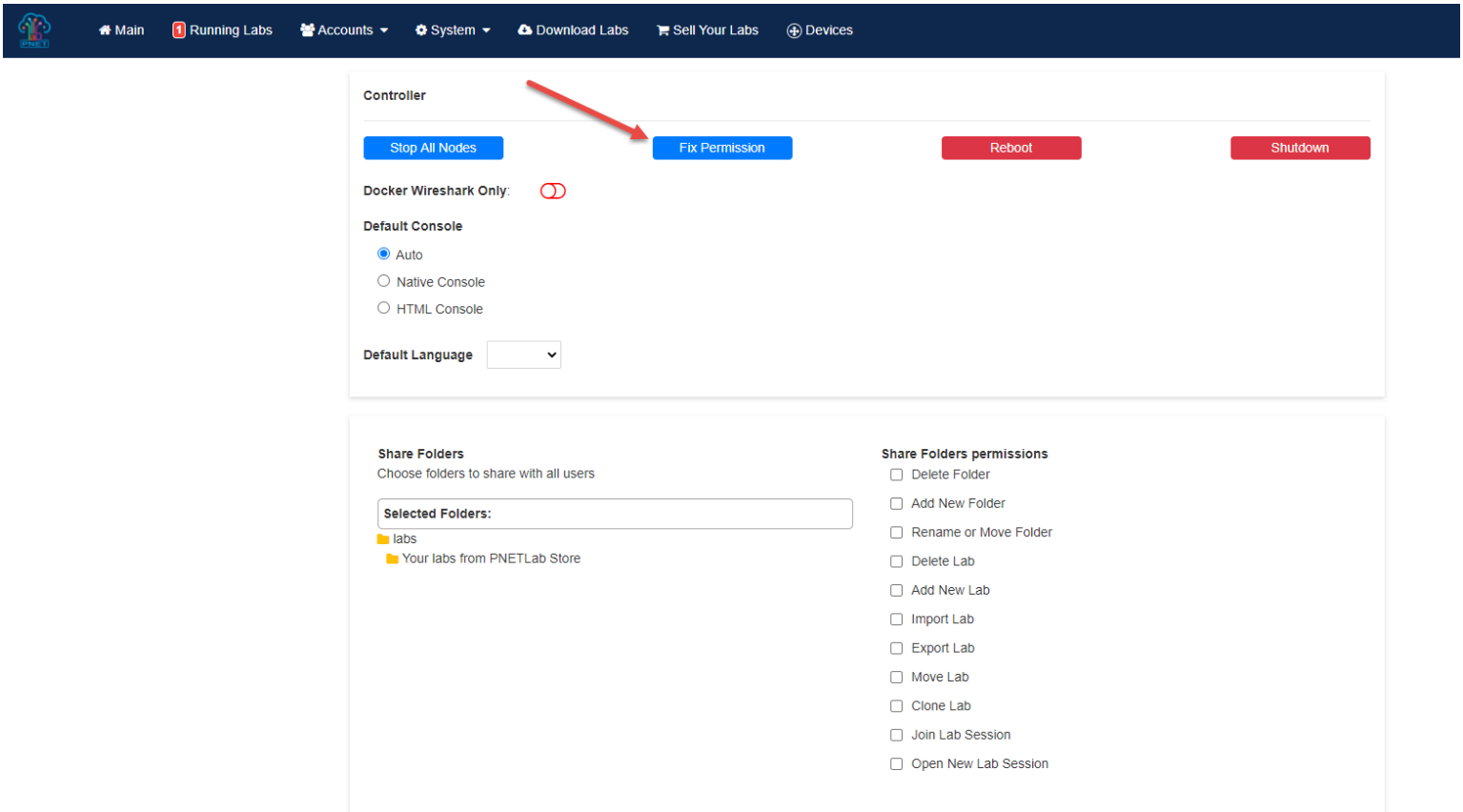
- **Step 3**: **Fixpermissions**
  - **Login to PNETLab platform (note: logging with online account)**

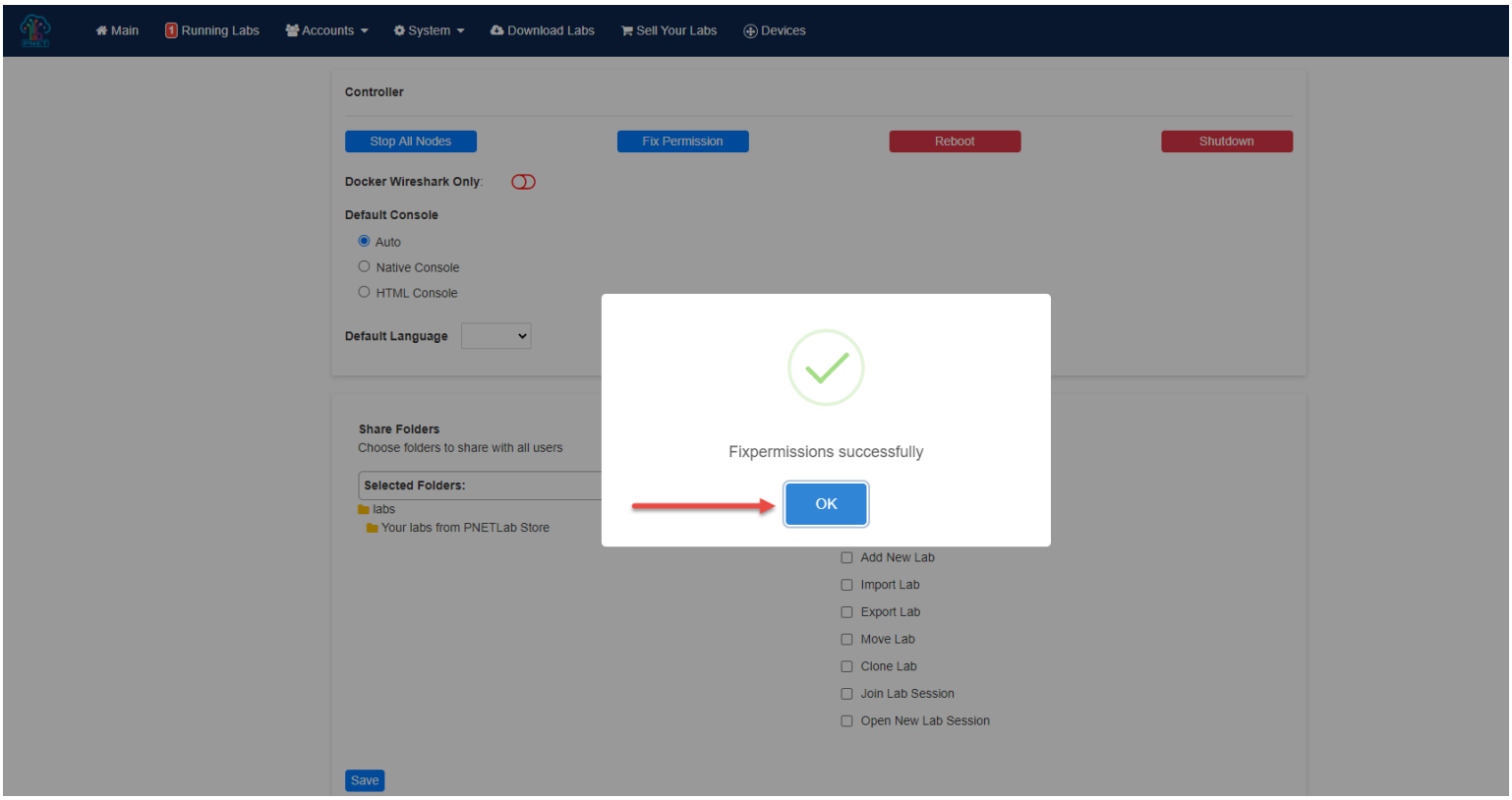


- Go to: System ➔ System Setting



- **Click to Fix permission button**





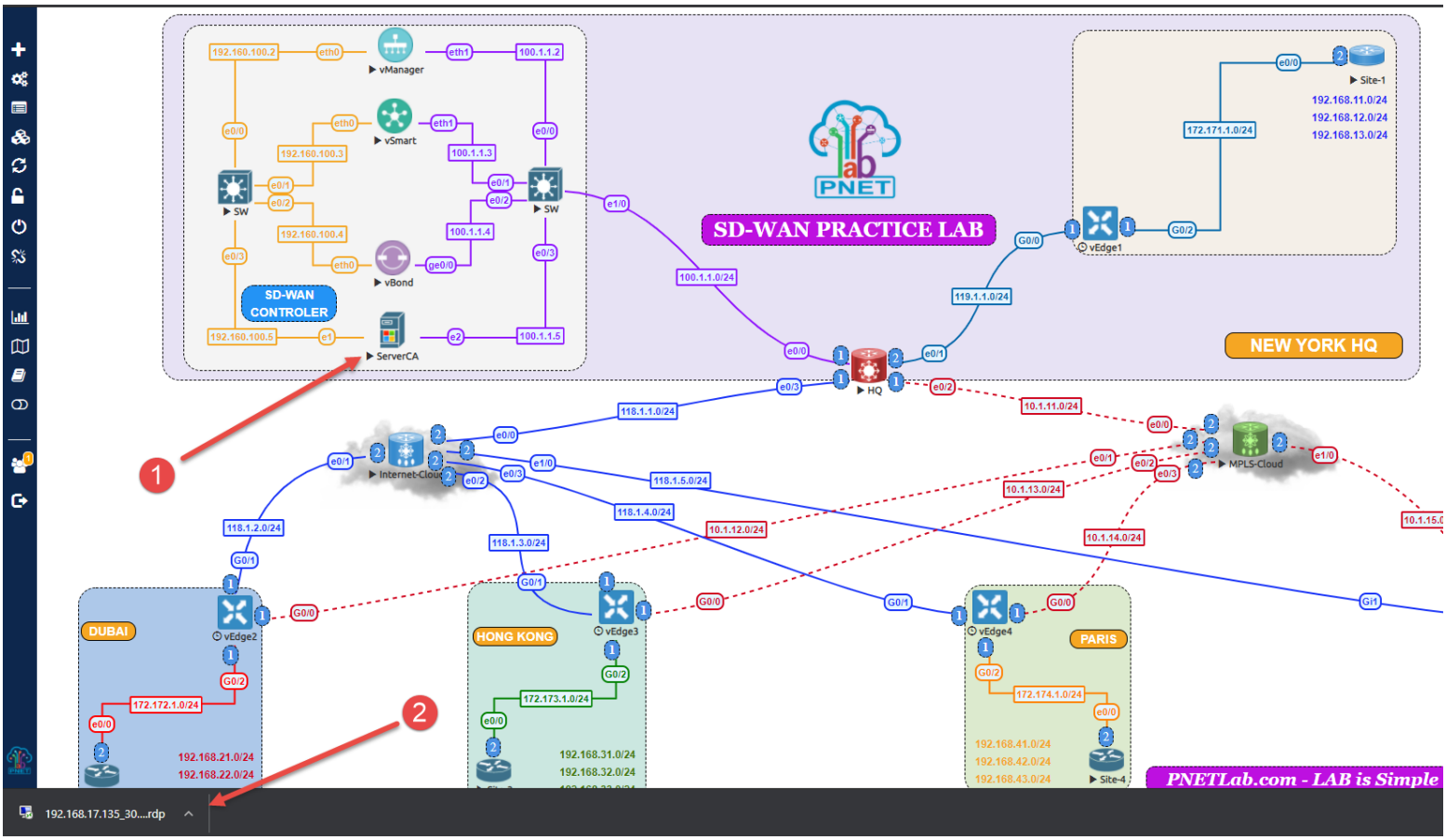
2. How to setup and practice Lab

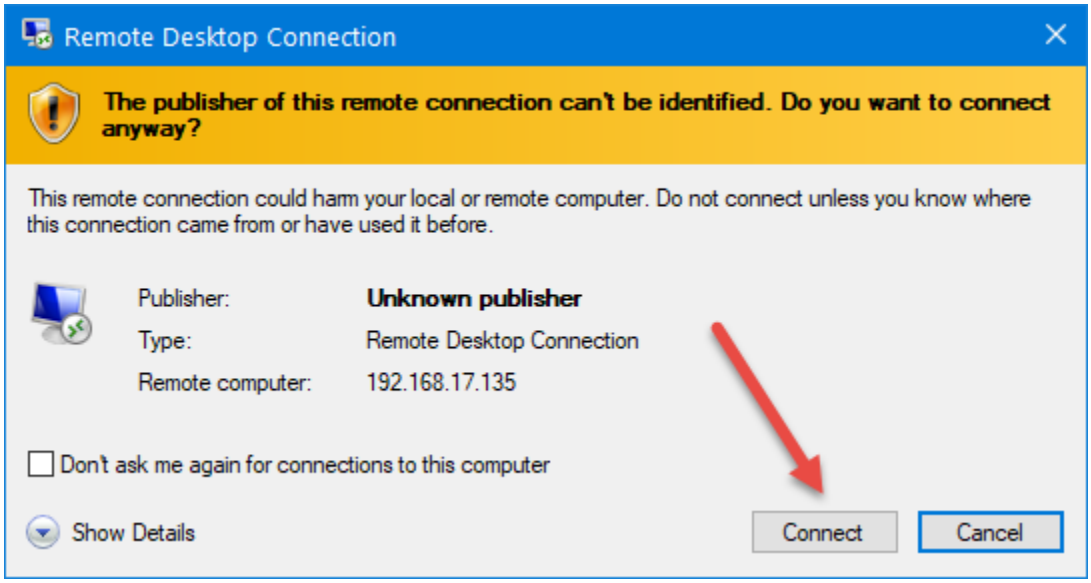
a. Licensing on SD-WAN devices

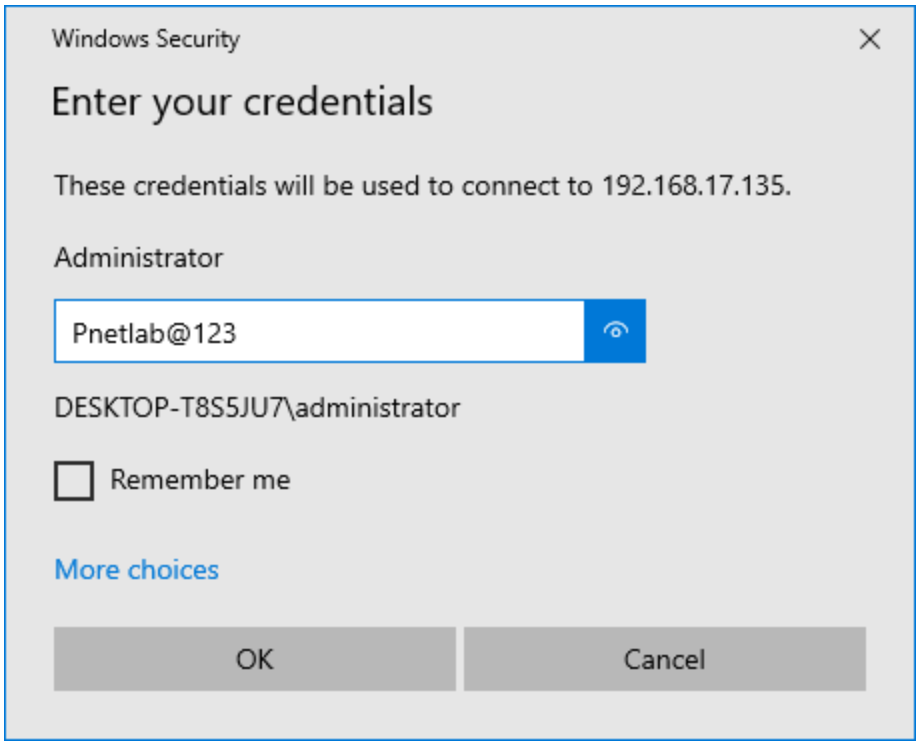
- Link to download file serial licence: https://drive.google.com/file/d/1KFqwBLHz-xB7DXgTWudryedKlEK0lfKy/view?usp=sharing
    - Backup Link: https://mega.nz/file/jyZnSIhJ#rSprYR4z9XY_o2Ryyw3CCBdto5JxEU5AUVzRXRruX-Y
- Save that file to your PC then using this license file for Lab 9

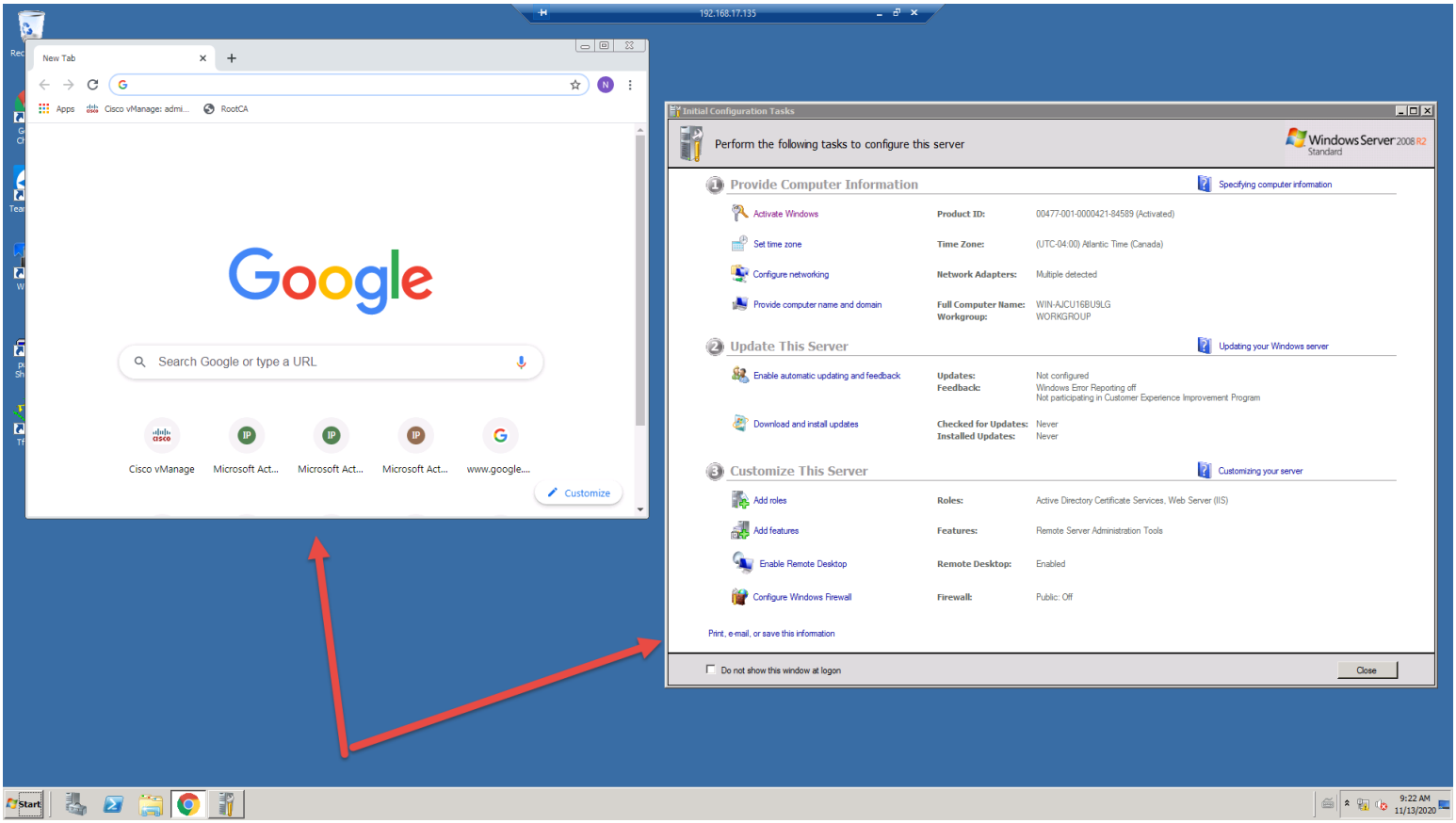
b. ServerCA – Windows Server 2008

- 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:
    - Click to ServerCA then download RDP file and Open, Login with account: **administrator/Pnetlab@123**


SD-WAN PRACTICE LAB
NEW YORK HQ
SD-WAN CONTROLER
vManager
vSmart
vBond
ServerCA
SW
HQ
Internet-Cloud
MPLS-Cloud
vEdge1
Site-1
DUBAI
vEdge2
HONG KONG
vEdge3
PARIS
vEdge4
Site-4
1
2
192.168.17.135_30....rdp
PNETLab.com - LAB is Simple


Remote Desktop Connection
The publisher of this remote connection can't be identified. Do you want to connect anyway?
This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.
Publisher: Unknown publisher
Type: Remote Desktop Connection
Remote computer: 192.168.17.135
Don't ask me again for connections to this computer
Show Details
Connect
Cancel

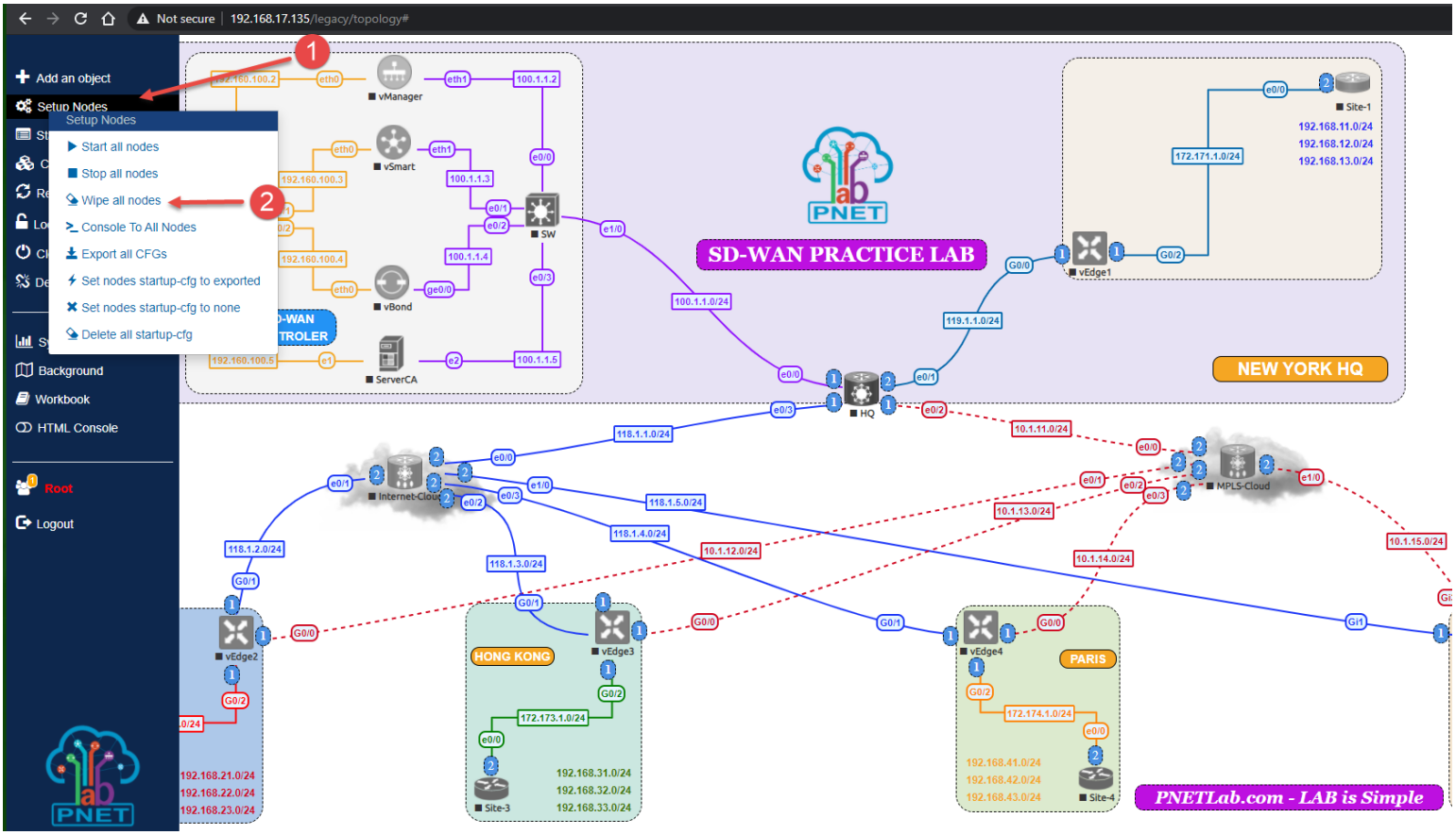

Windows Security
Enter your credentials
These credentials will be used to connect to 192.168.17.135.
Administrator
Pnetlab@123
DESKTOP-T8S5JU7\administrator
Remember me
More choices
OK
Cancel


192.168.17.135
New Tab
Apps
Cisco vManage: admi...
RootCA
Google
Search Google or type a URL
Cisco vManage
Microsoft Act...
Microsoft Act...
Microsoft Act...
www.google....
Customize
Initial Configuration Tasks
Perform the following tasks to configure this server
Windows Server 2008 R2 Standard
Provide Computer Information
Specifying computer information
Activate Windows
Product ID: 00477-001-0000421-84589 (Activated)
Set time zone
Time Zone: (UTC-04:00) Atlantic Time (Canada)
Configure networking
Network Adapters: Multiple detected
Provide computer name and domain
Full Computer Name: WIN-AJCU16BU9LG
Workgroup: WORKGROUP
Update This Server
Updating your Windows server
Enable automatic updating and feedback
Updates: Not configured
Feedback: Windows Error Reporting off
Not participating in Customer Experience Improvement Program
Download and install updates
Checked for Updates: Never
Installed Updates: Never
Customize This Server
Customizing your server
Add roles
Roles: Active Directory Certificate Services, Web Server (IIS)
Add features
Features: Remote Server Administration Tools
Enable Remote Desktop
Remote Desktop: Enabled
Configure Windows Firewall
Firewall: Public: Off
Print, e-mail, or save this information
Do not show this window at logon
Close
Start
9:22 AM
11/13/2020

Account login to the devices in the SD-WAN LAB

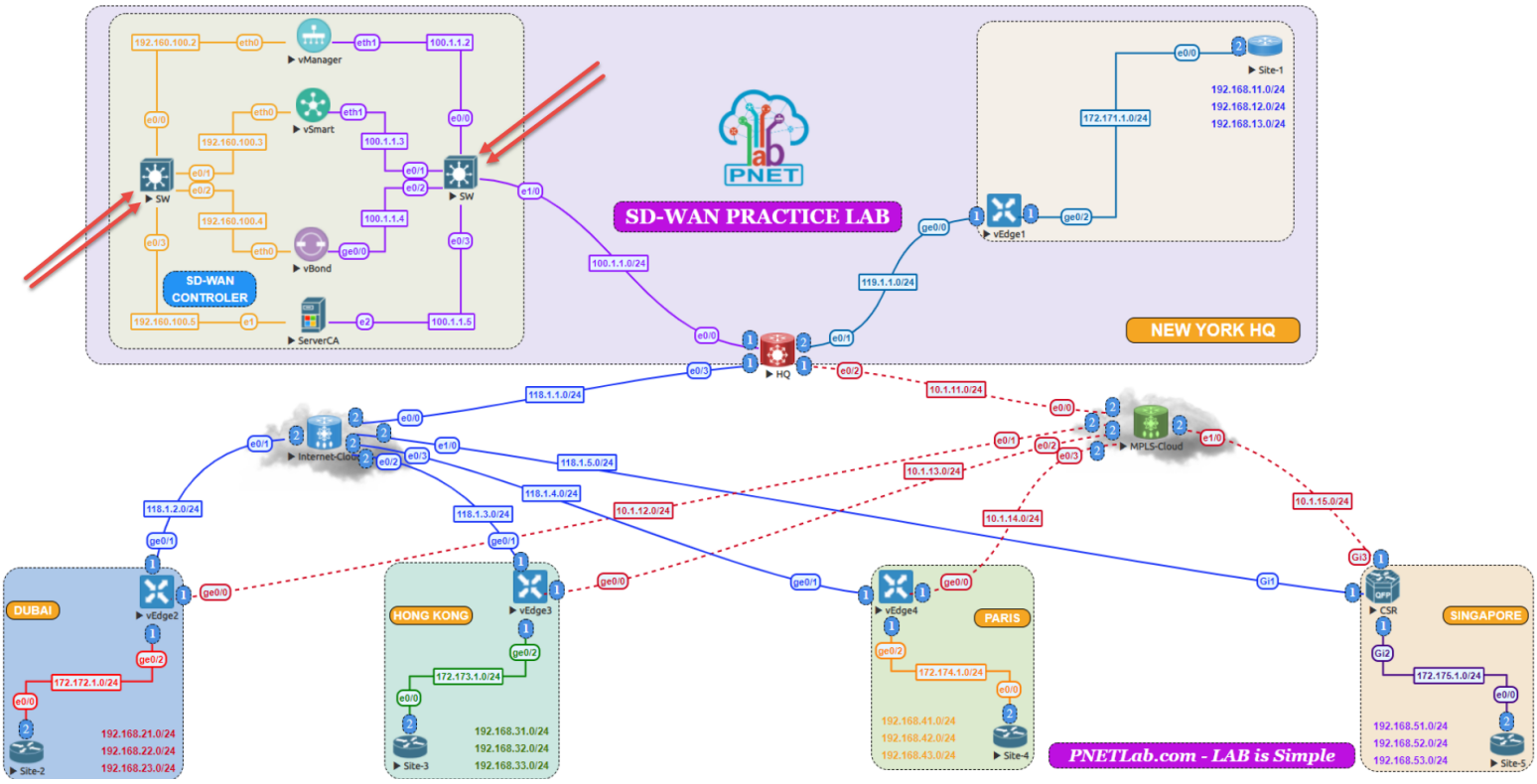
- Default username and password to login **vManager, vSmart, vBond, vEdge** is: **admin/admin**
- Default username and password to login to **ServerCA**: **administrator/Pnetlab@123**

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



========Some key notes for practing this lab========

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



2. **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

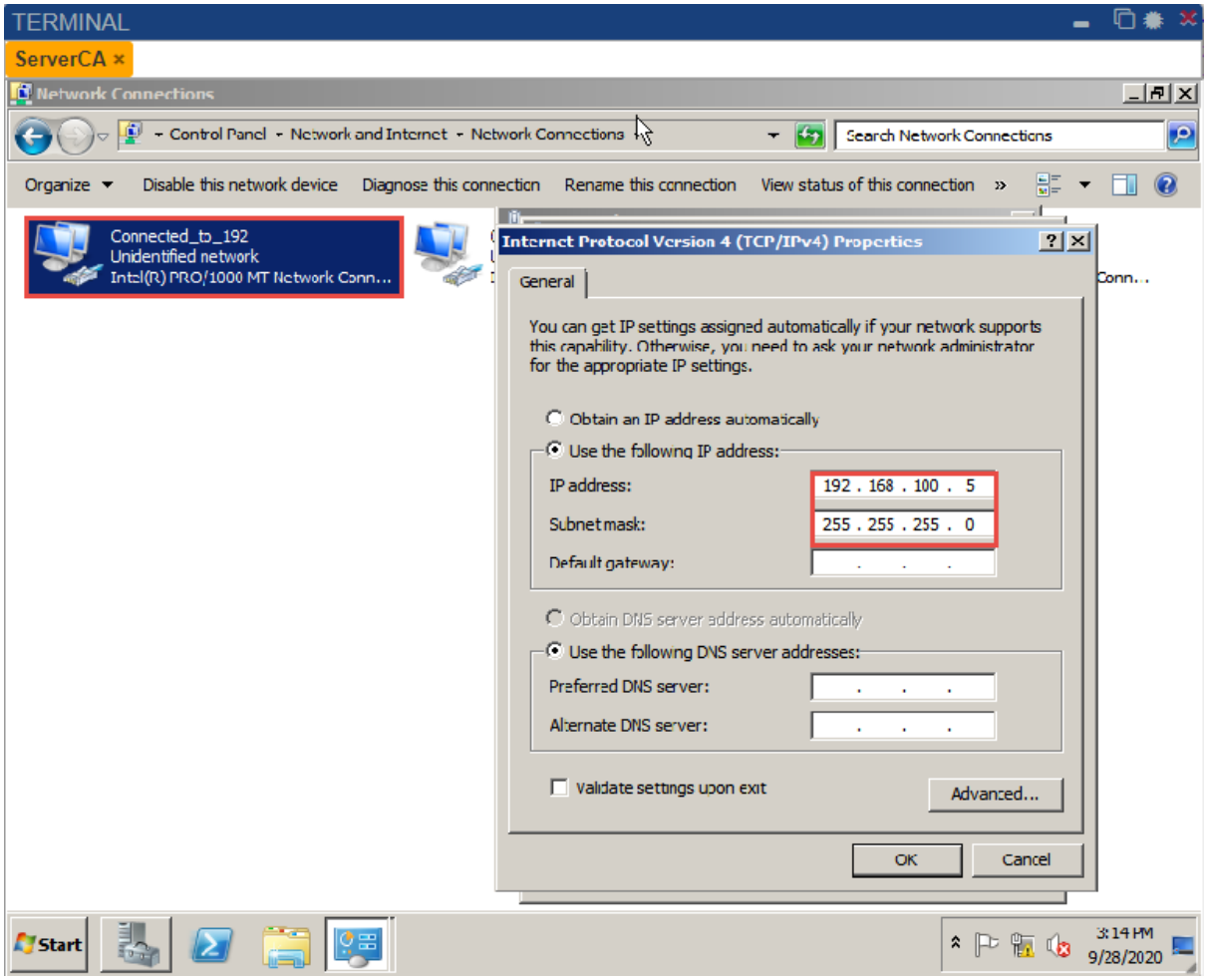
Internet Cloud Router

```
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
```

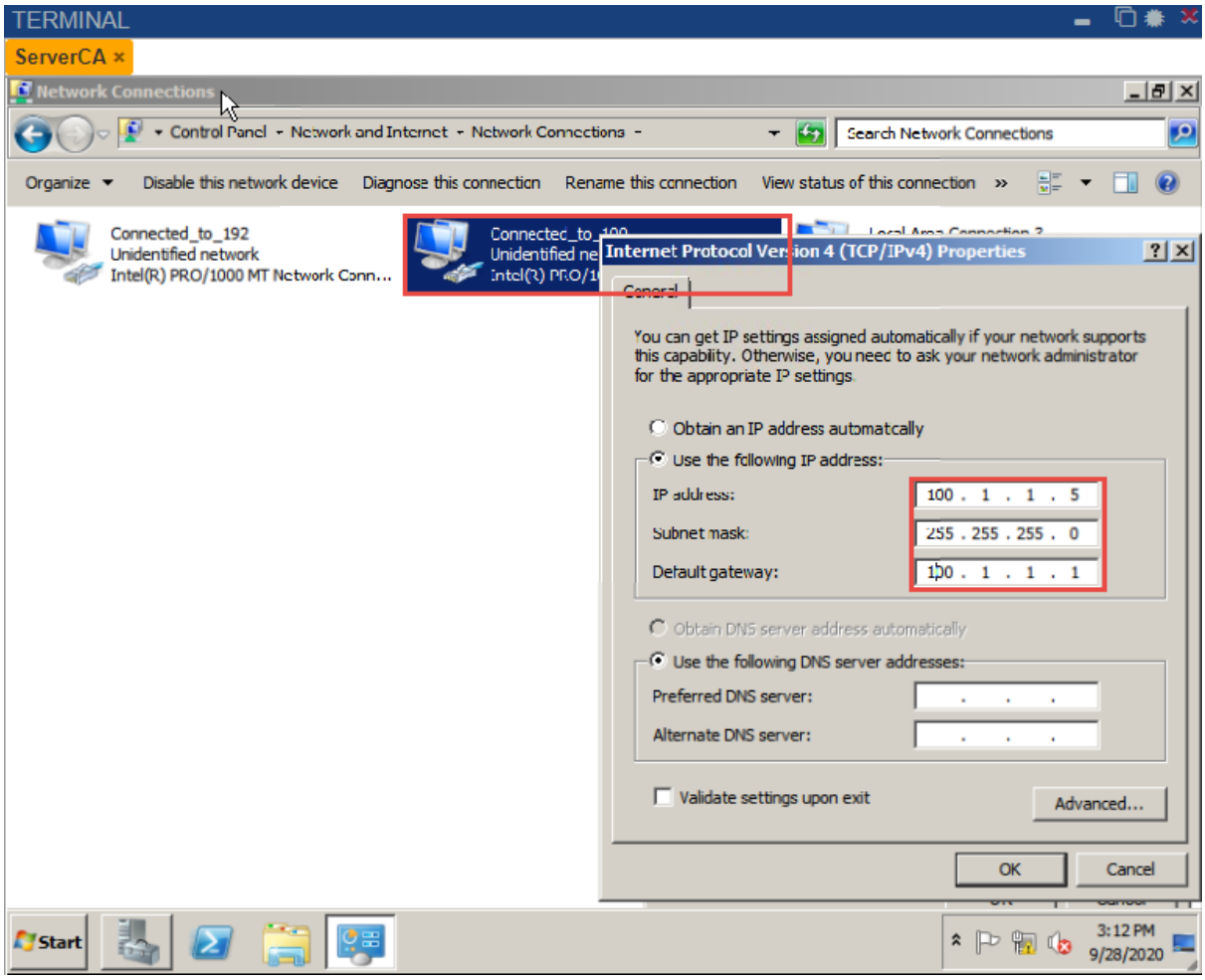
Lab 2: Installing the Enterprise Certificate Server

Task 1- Configure the interface

- First Ethernet Interface: Connected_to_192
- Ip address: 192.168.100.4
- Subnet: 255.255.255.0

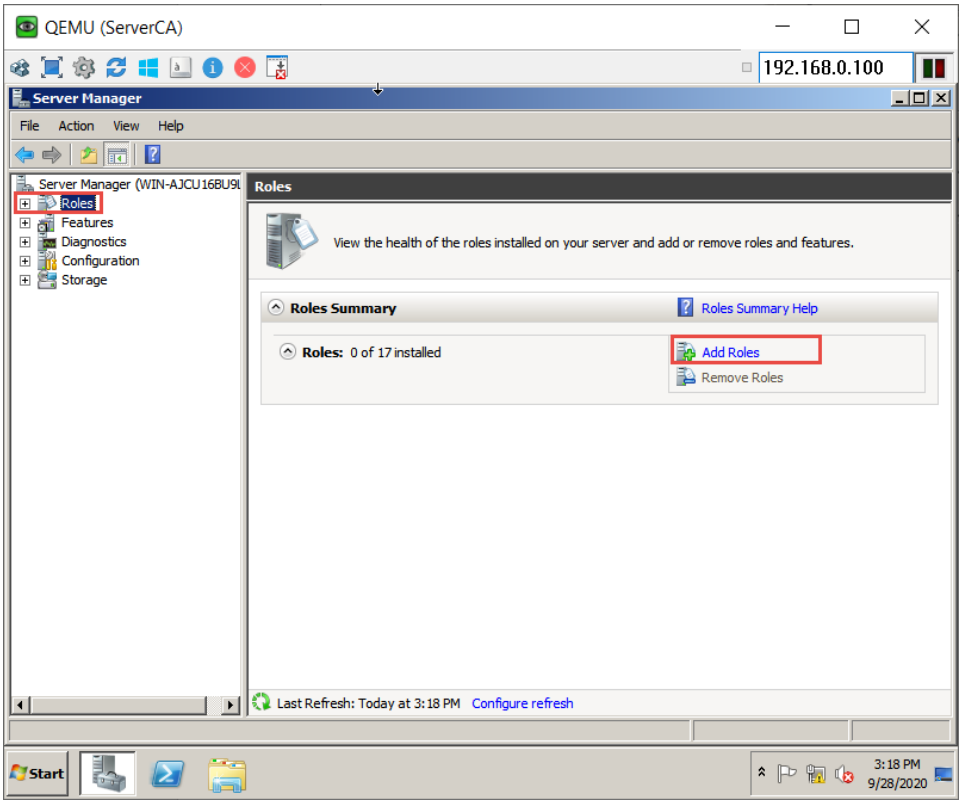


- Third Ethernet Interface: Connected_to_100
- Ip address: 100.1.1.5
- Netmask: 255.255.255.0
- Gateway: 100.1.1.1

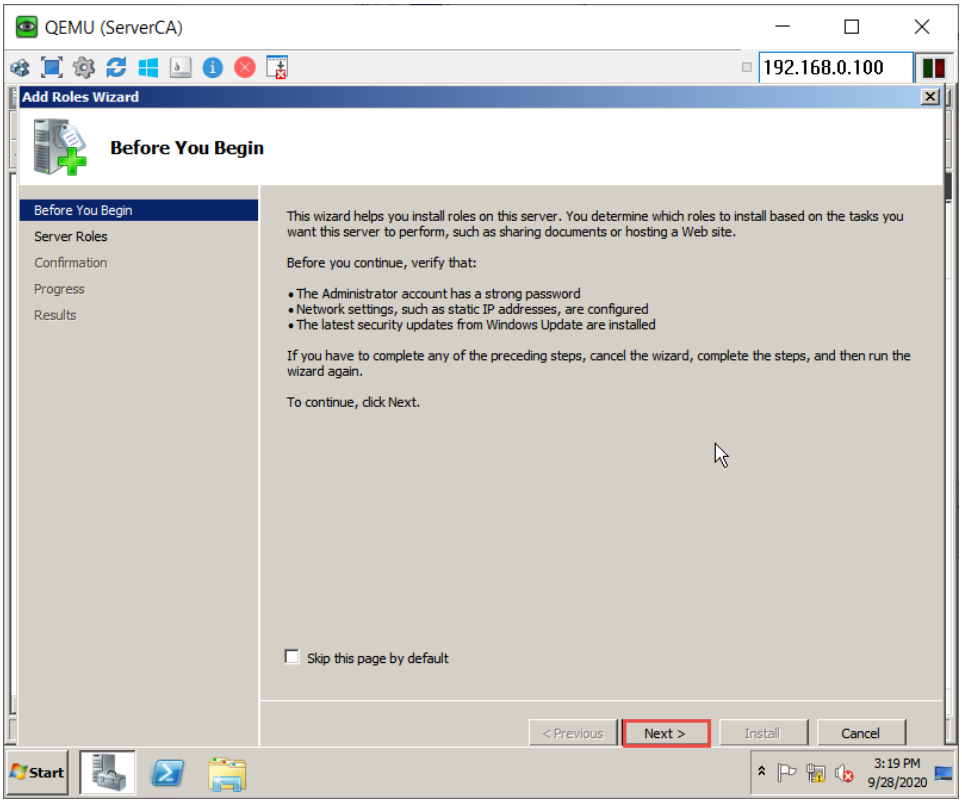


Task 2- Installing the Enterprise Root Certificate Server

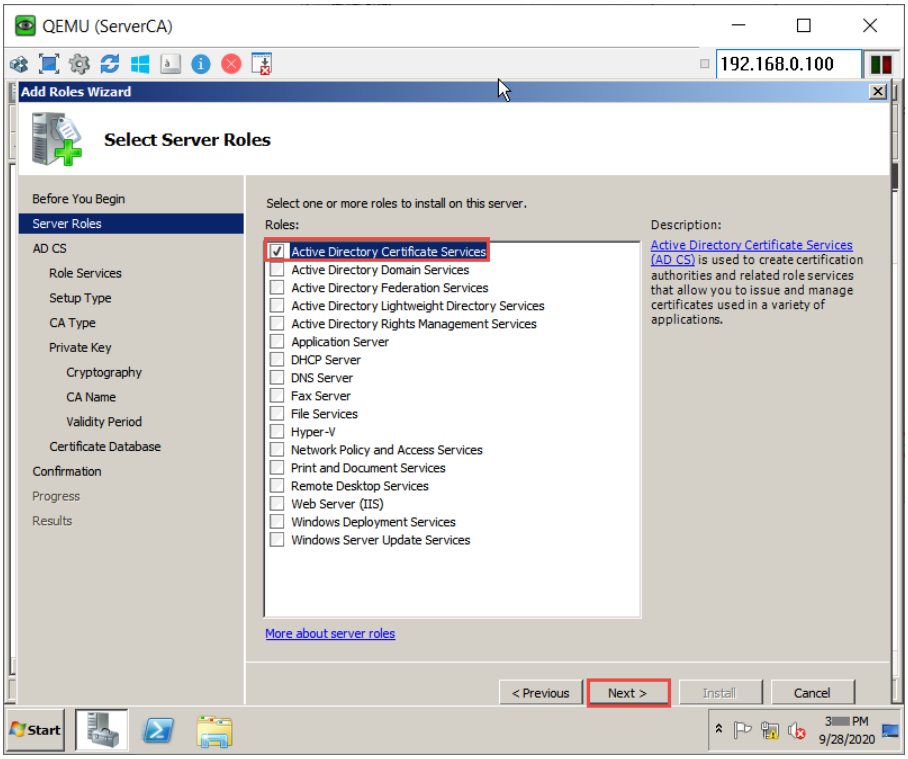
- Open Server **Manager -> click Roles-> Next**


QEMU (ServerCA)
192.168.0.100
Server Manager
File Action View Help
Server Manager (WIN-AJCU16BU9L
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 0 of 17 installed
Add Roles
Remove Roles
Last Refresh: Today at 3:18 PM Configure refresh
Start
3:18 PM
9/28/2020

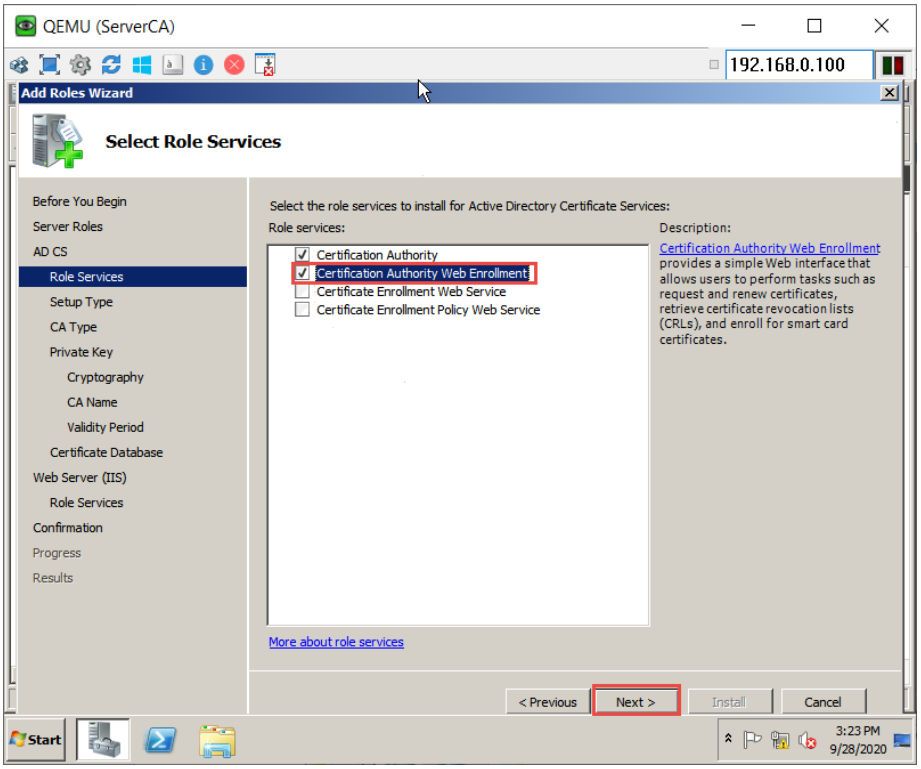
- Click Next


QEMU (ServerCA)
192.168.0.100
Add Roles Wizard
Before You Begin
Before You Begin
Server Roles
Confirmation
Progress
Results
This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.
Before you continue, verify that:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The latest security updates from Windows Update are installed
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
Start
3:19 PM
9/28/2020

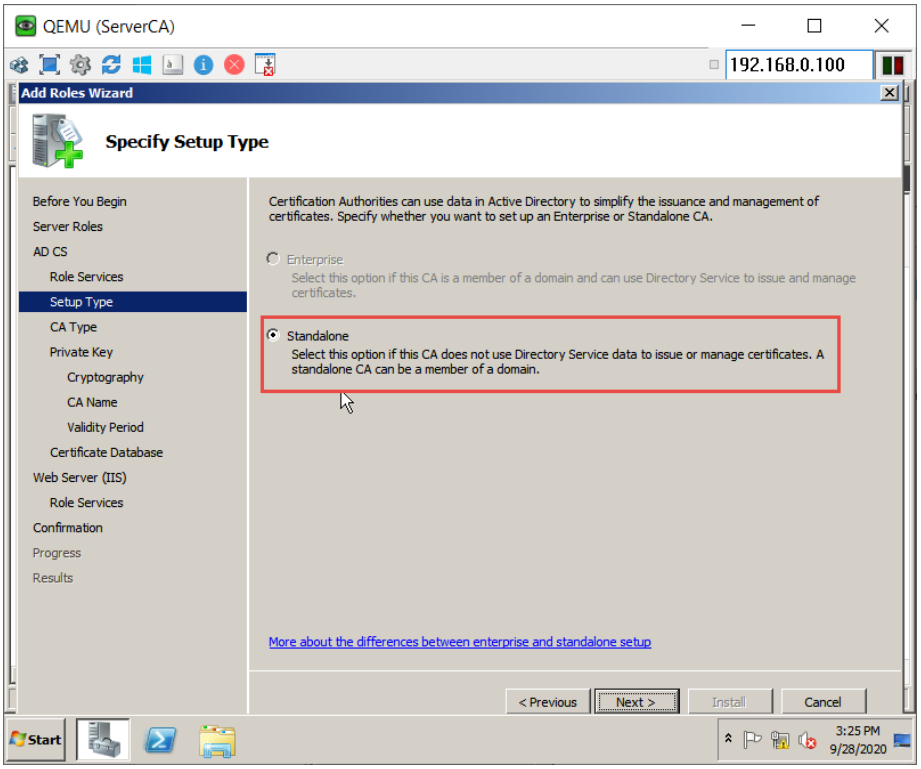
- Select the "**Active Directory Certificate Services**" and click Next



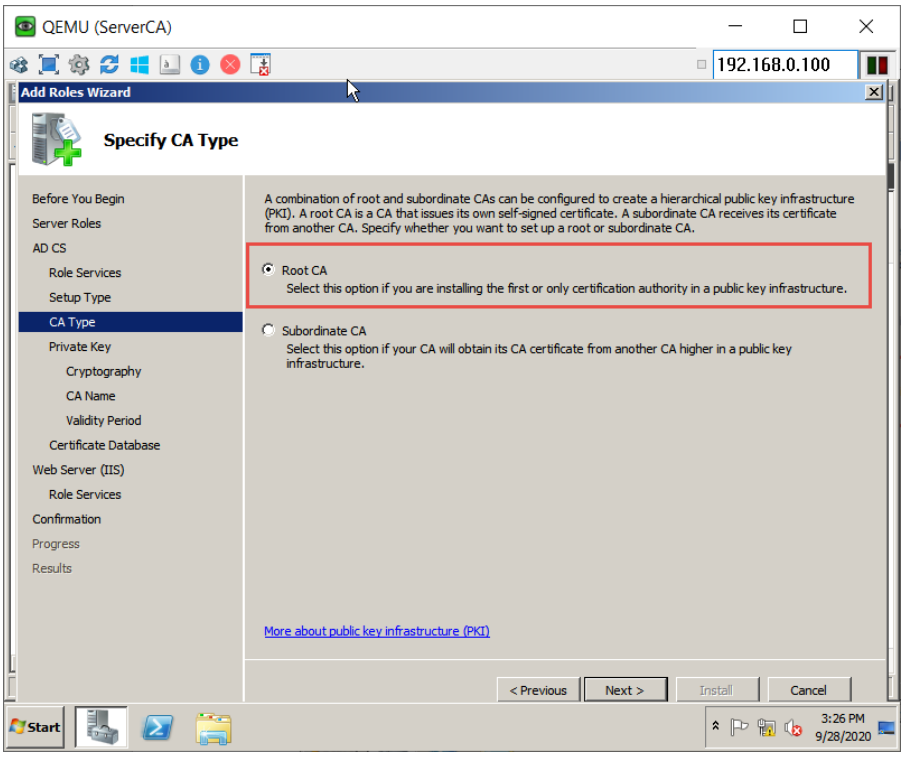
- Click **Next**
- Select "**Certification authority Web enrollment**" and click **Next**



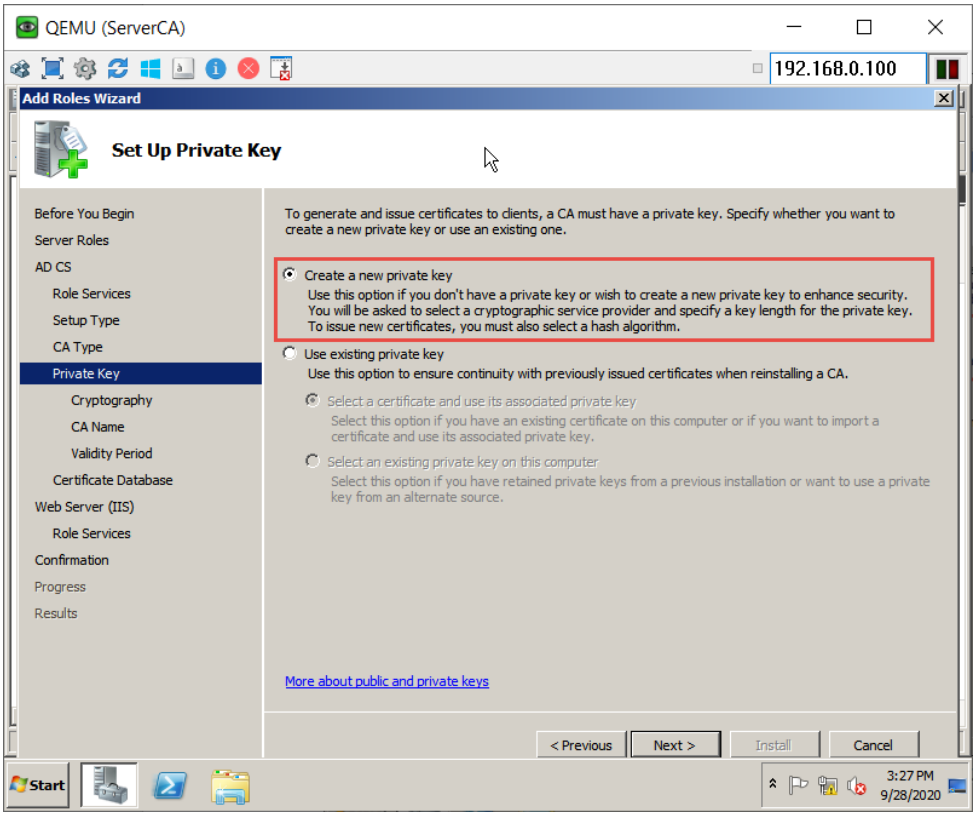
- Leave it as **Standalone** and click **Next**



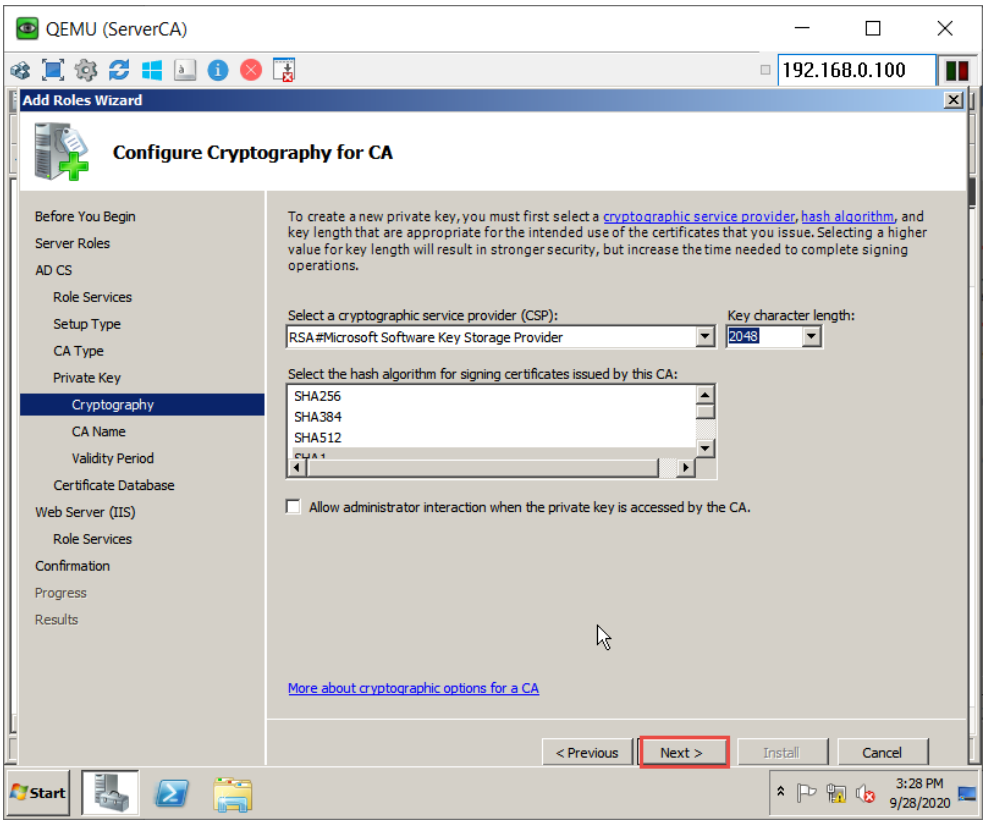
- Leave it as **Root CA** and click **Next**



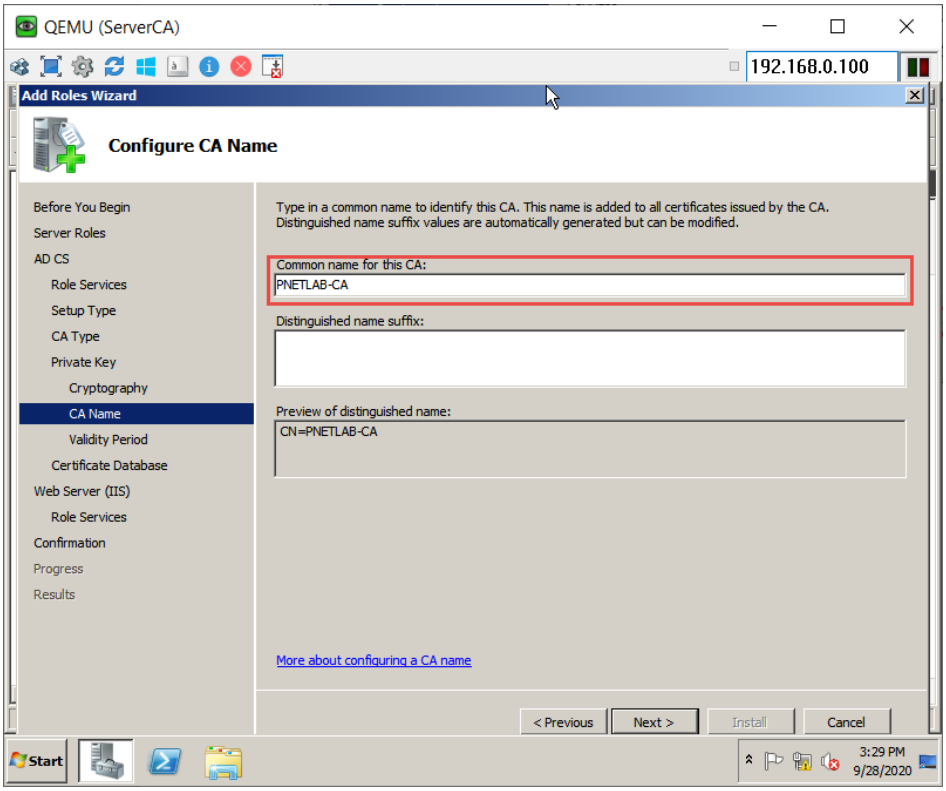
- Leave "**Create a new private key**" and click **Next**



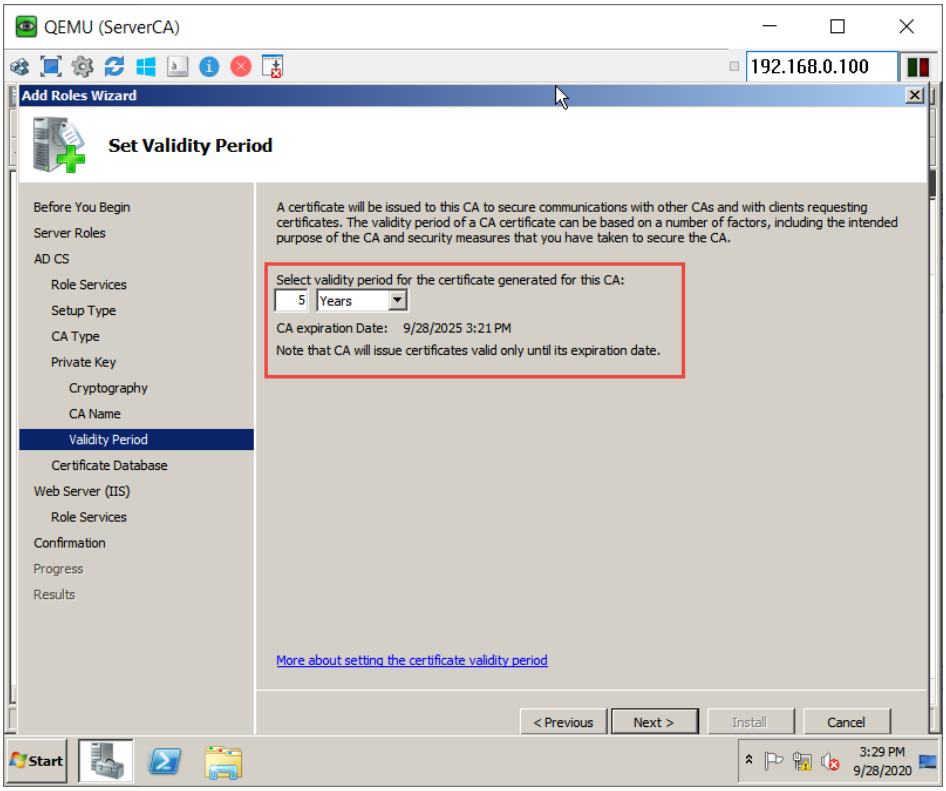
- Leave the default for the Cryptography for CA and click **Next**



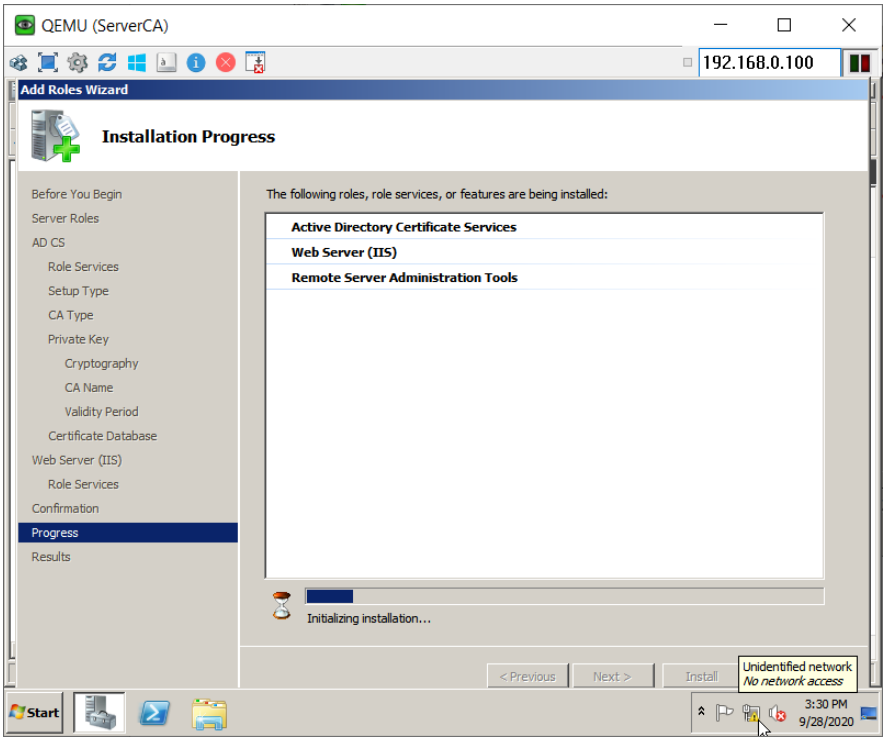
- Set the Common name as **PNETLAB-CA** and click **Next**



- 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:
  - Hostname: **vManage1**
  - Organization: **"viptela sdwan"**
  - System-IP: **100.1.1.12**
  - SiteID: **1**
  - Vbond Address: **100.1.1.4**
  - 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:
  - Vpn0
    - Interface eth1
    - IP address: **100.1.1.2/24**
    - Tunnel Interface
    - Tunel Services (All, NetConf, SSHD)
    - Default route: **100.1.1.1**
  - Vpn 512
    - Interface eth0
    - Ip address: **192.168.100.2/24**

vManage

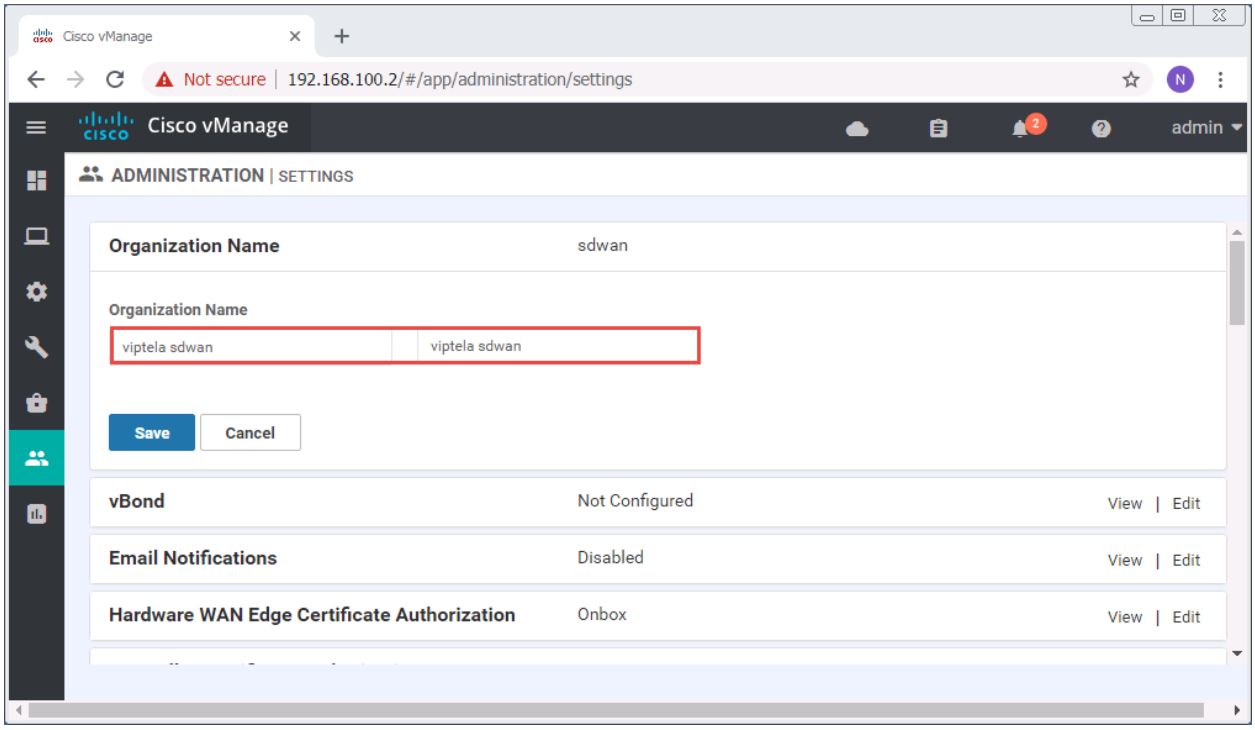
```
config
!
vpn 0
no interface eth0
interface eth1
ip address 100.1.1.2/24
tunnel-interface
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 100.1.1.1
!
vpn 512
interface eth0
ip address 192.168.100.2/24
no shut
!
commit
```

Lab 4- Initializing vManage – GUI

Task 1- Organization name & vBond Address

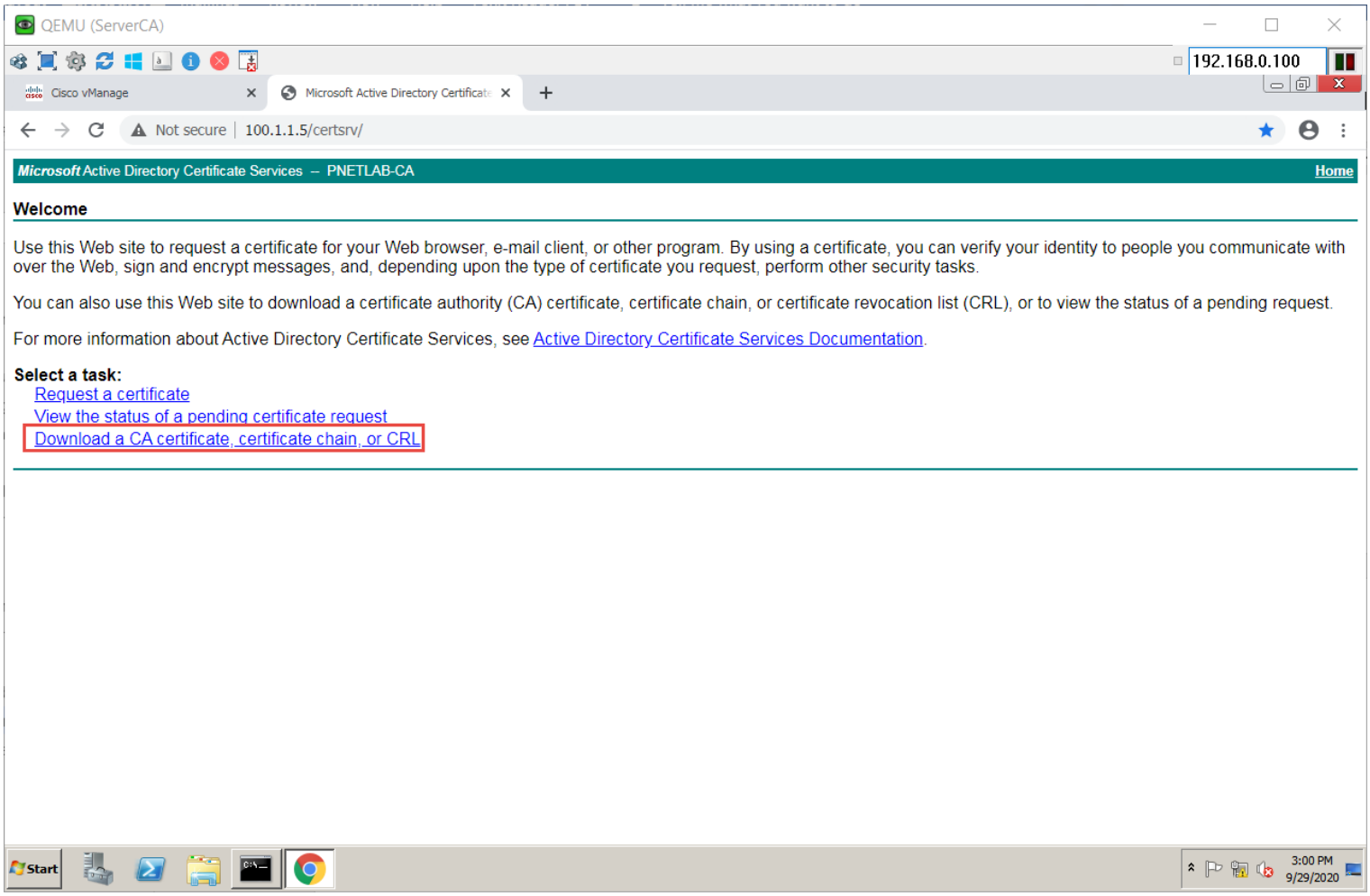
- Login into the vManage from the Server by browsing to https://192.168.100.2:8443 using username of admin and password of admin

- 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**.

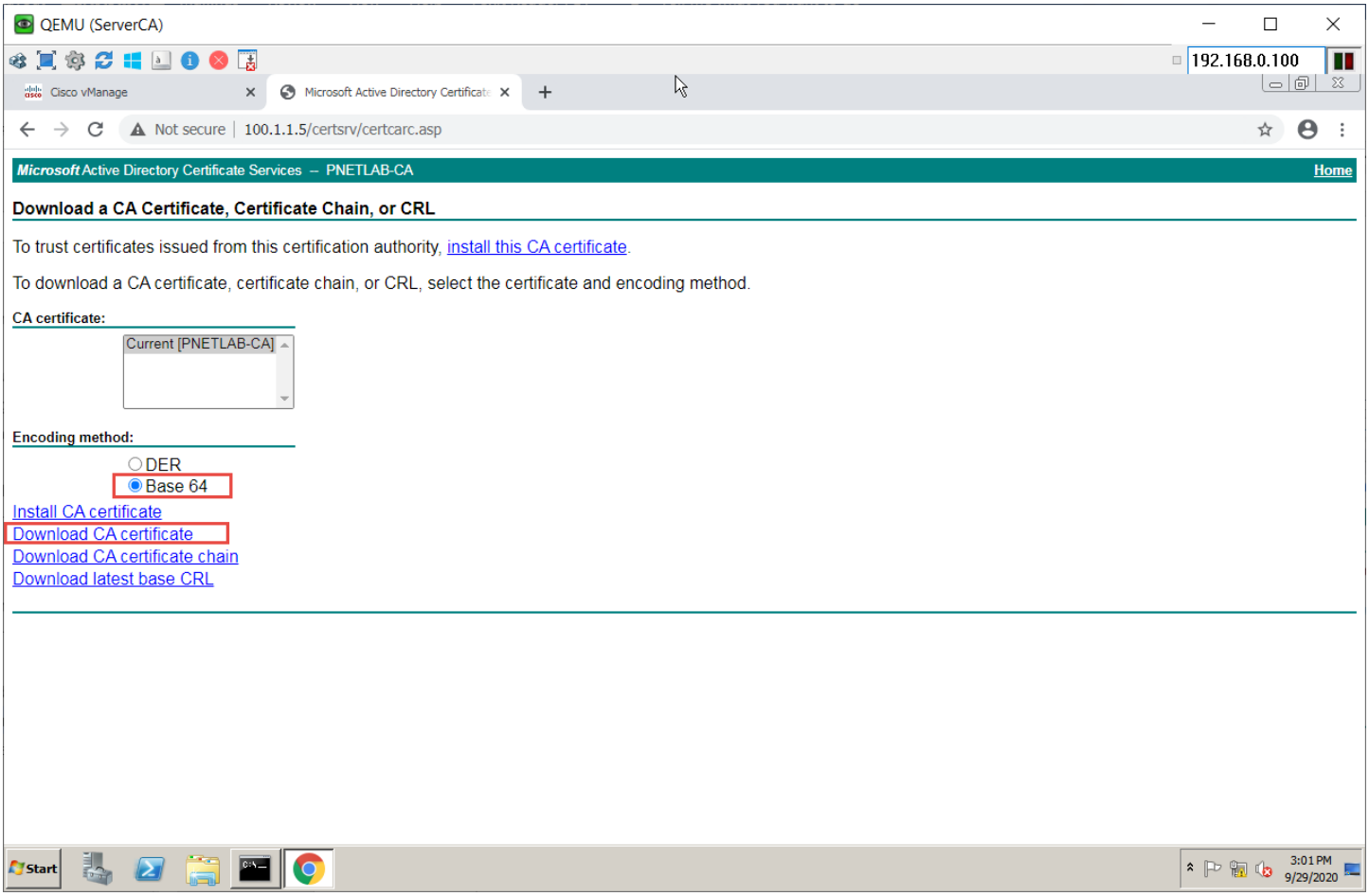


Task 2 – Configure Controller Authorization as Enterprise Root and Download the Root Certificate.

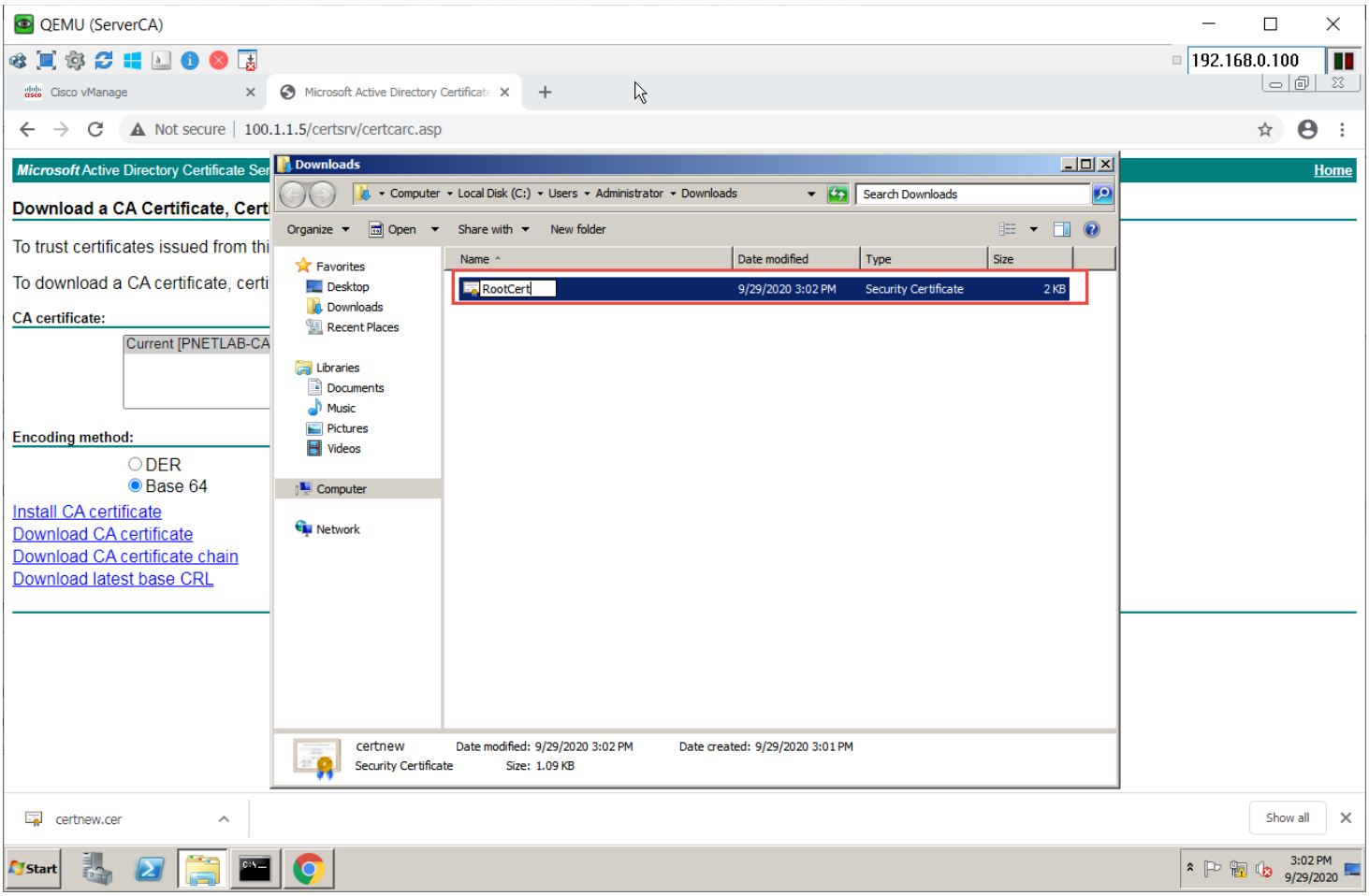
- Browse to http://100.1.1.5/certsrv
- Click "**Download Root Certificate**".



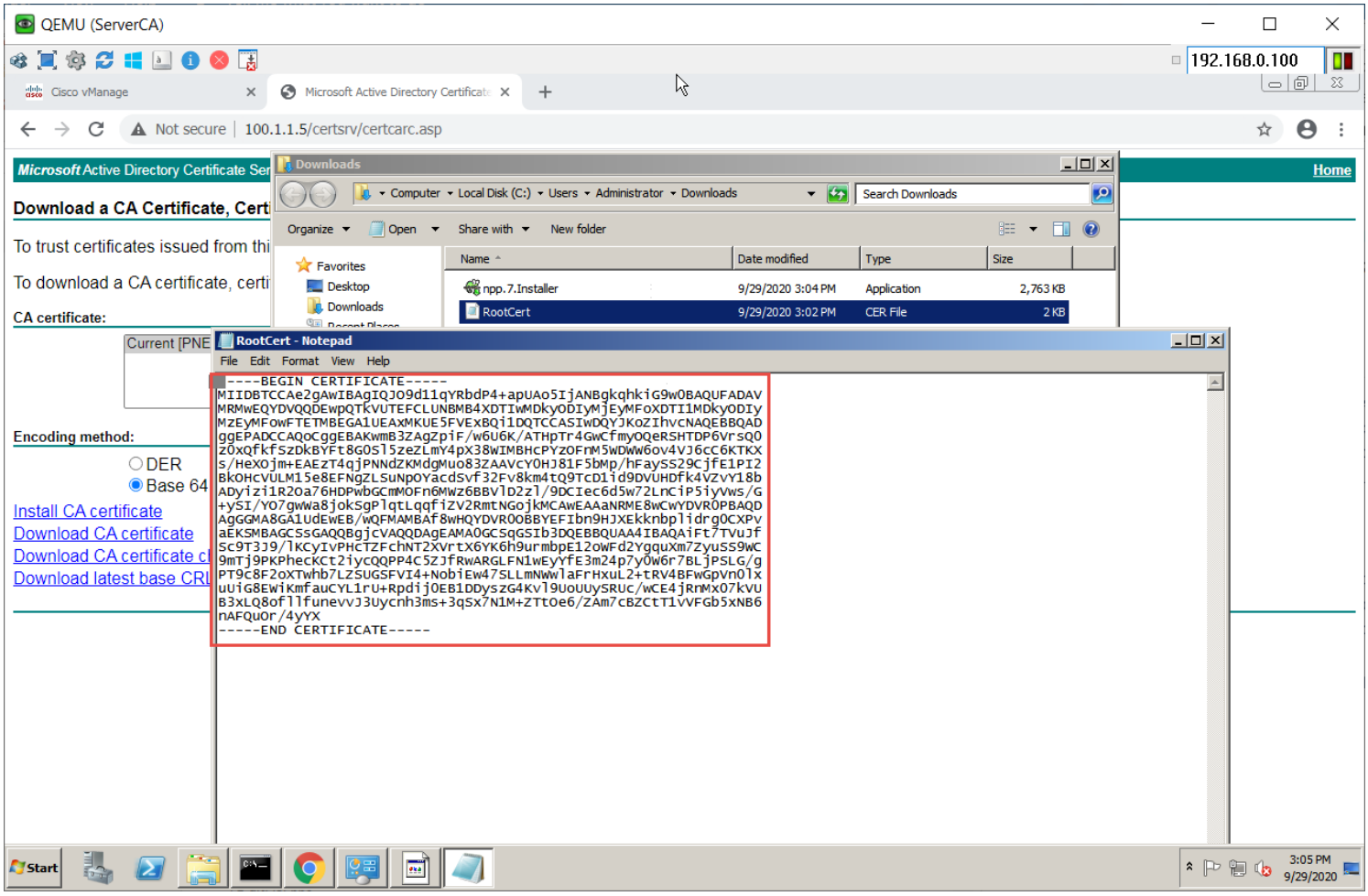
- Select "**Base 64**".
- Click "**Download CA Certificate**".



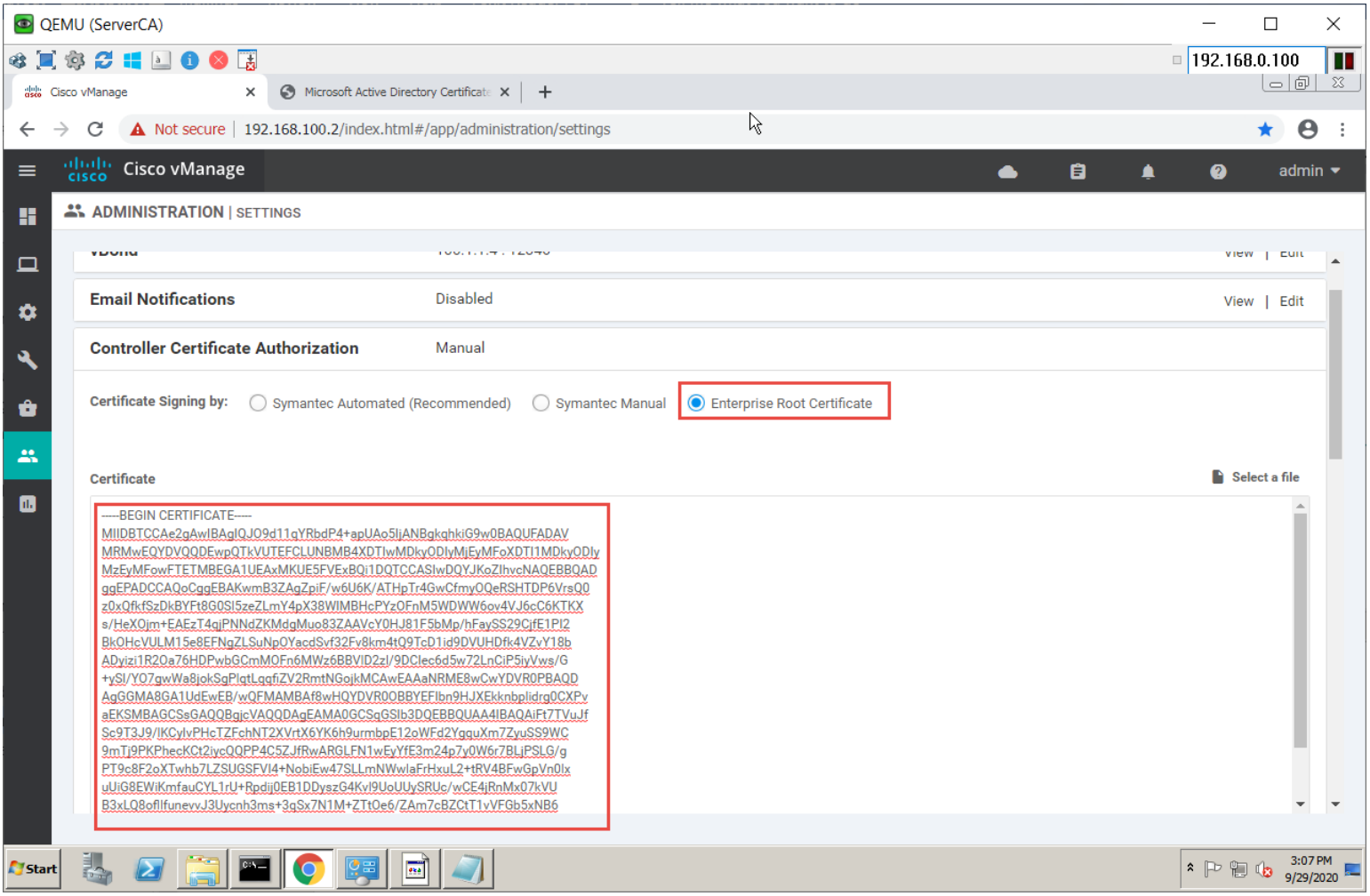
- Open Explorer and navigate to the downloads folder.
- Change the name of the Downloaded file "**Certnew" to "RootCert**".



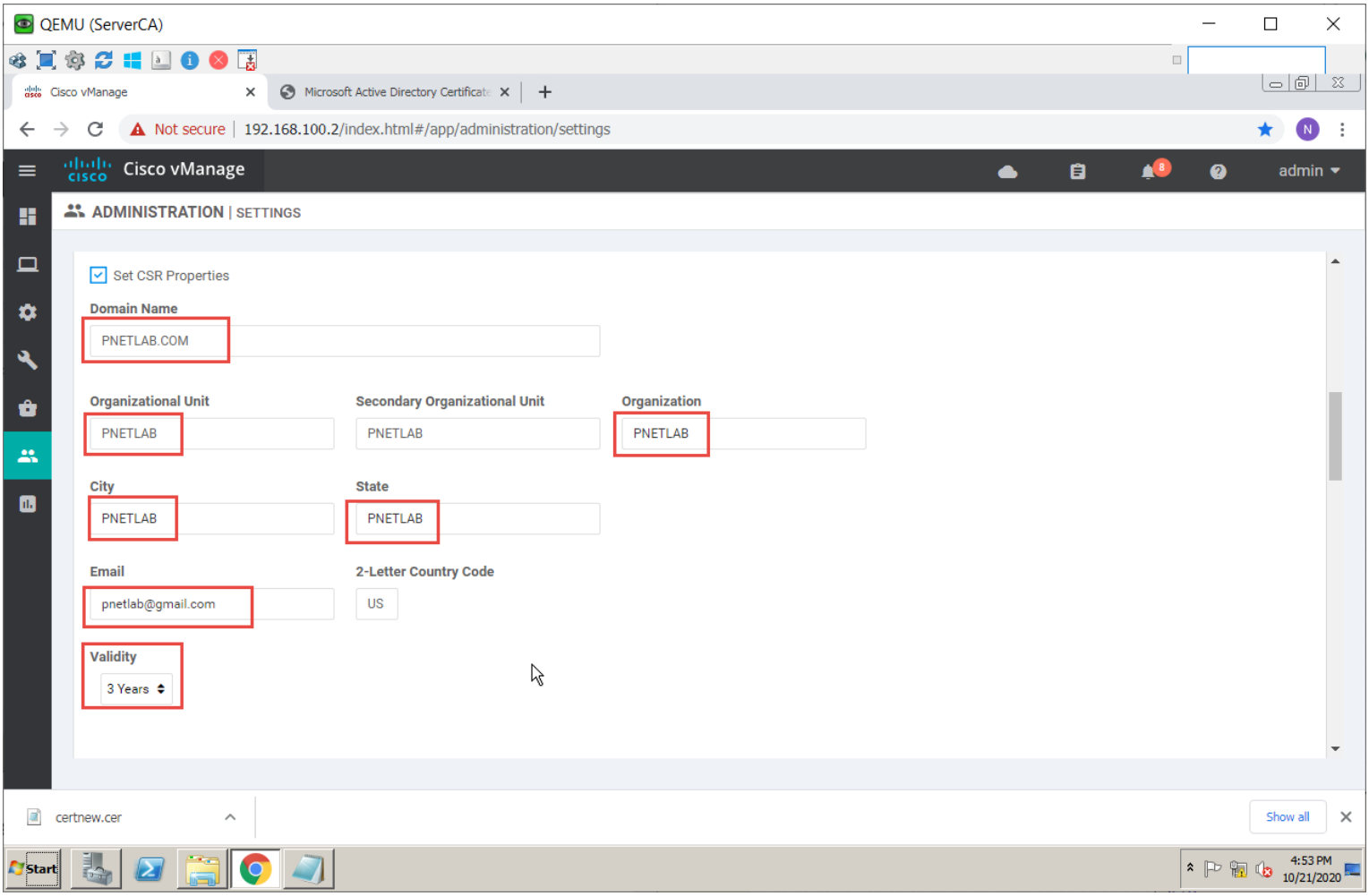
- Open the "**RootCert.cer**" file using Notepad.
- Copy using **CTRL-A and CTRL-C**.



- 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**.



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

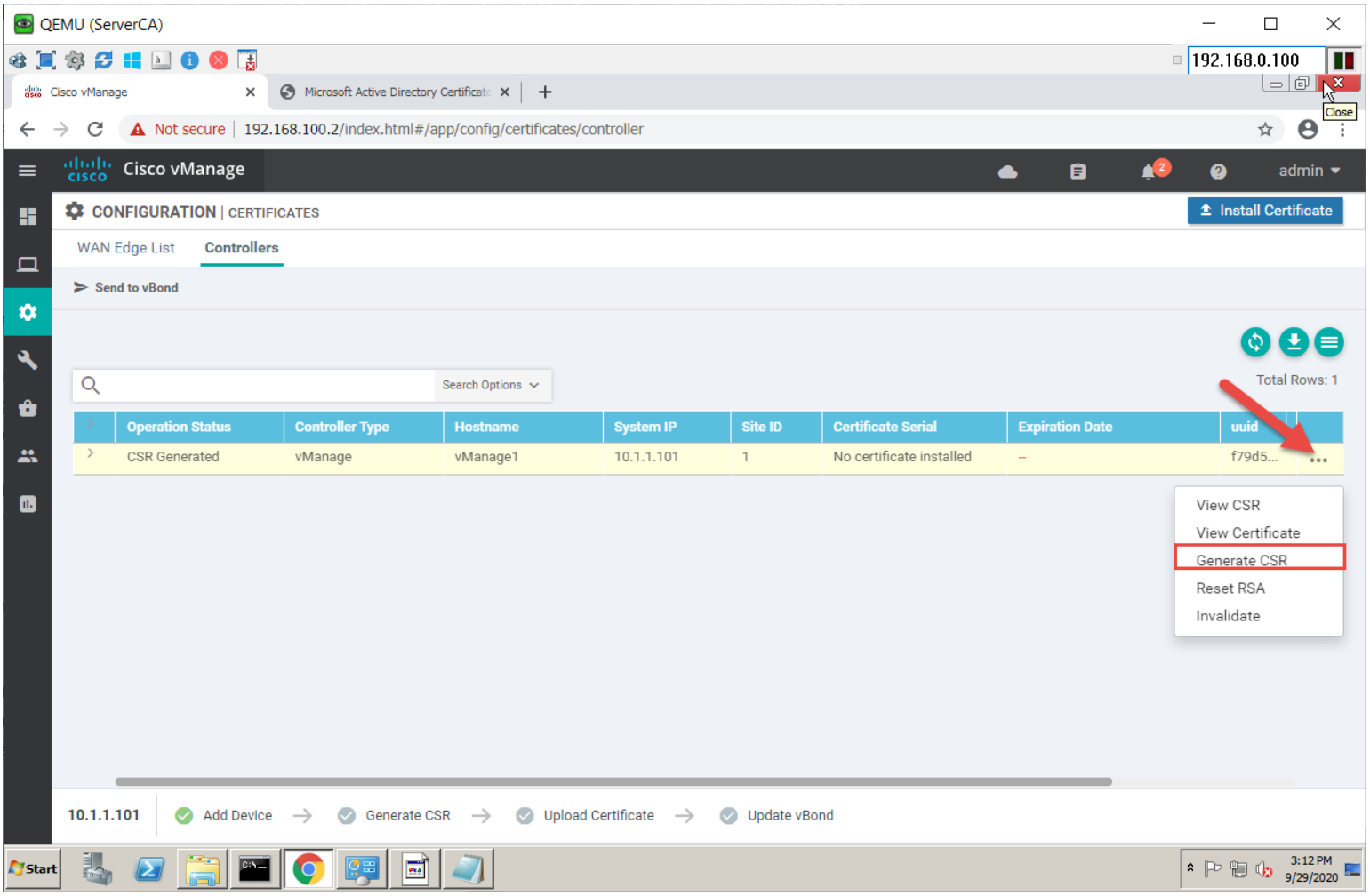


Note: with sdwan version 20, **You must uncheck** "**Set CSR Properties**" due to the bug on the version

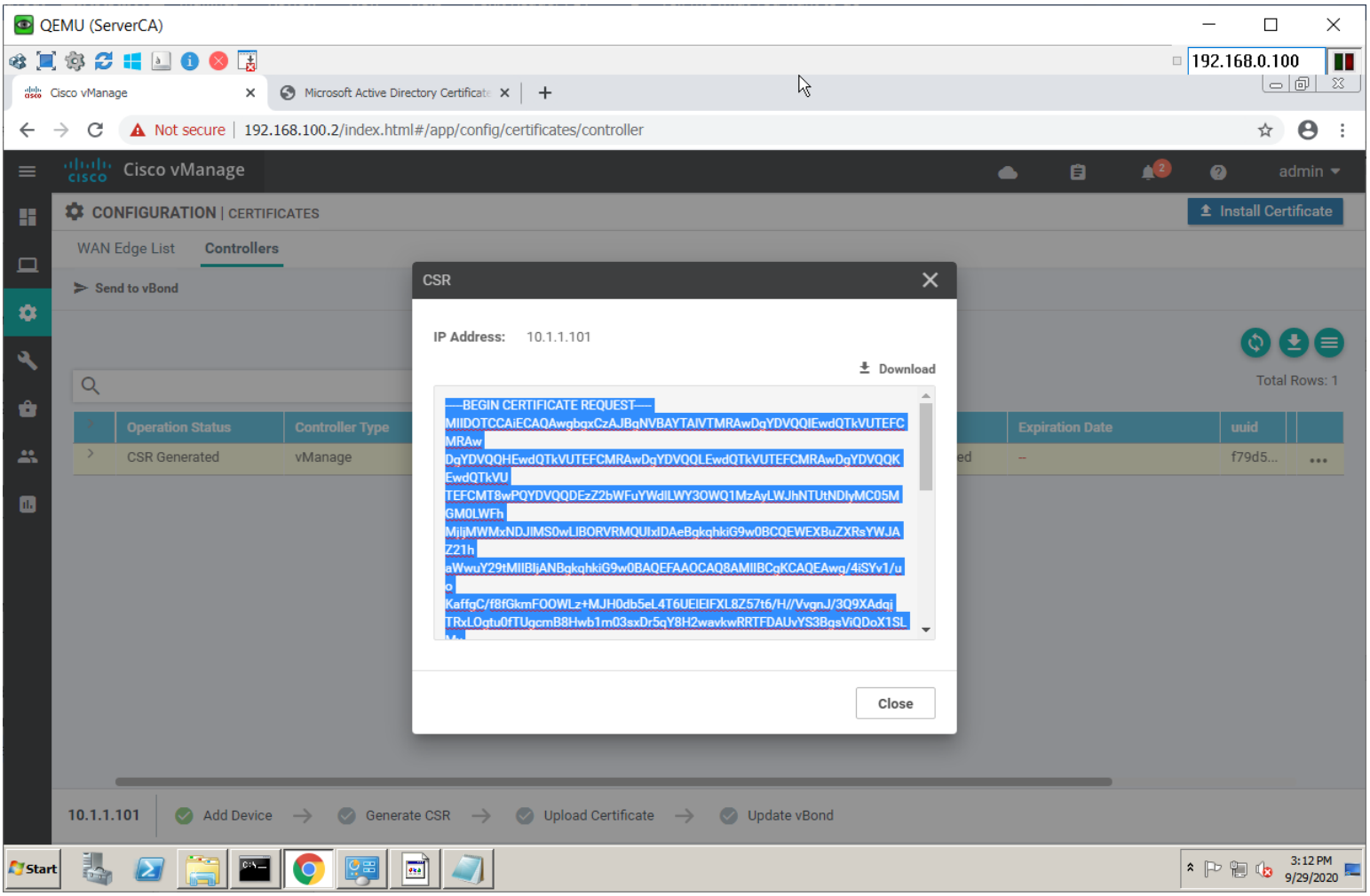
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvp75927

Task 3- Generate a CSR for vManage

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

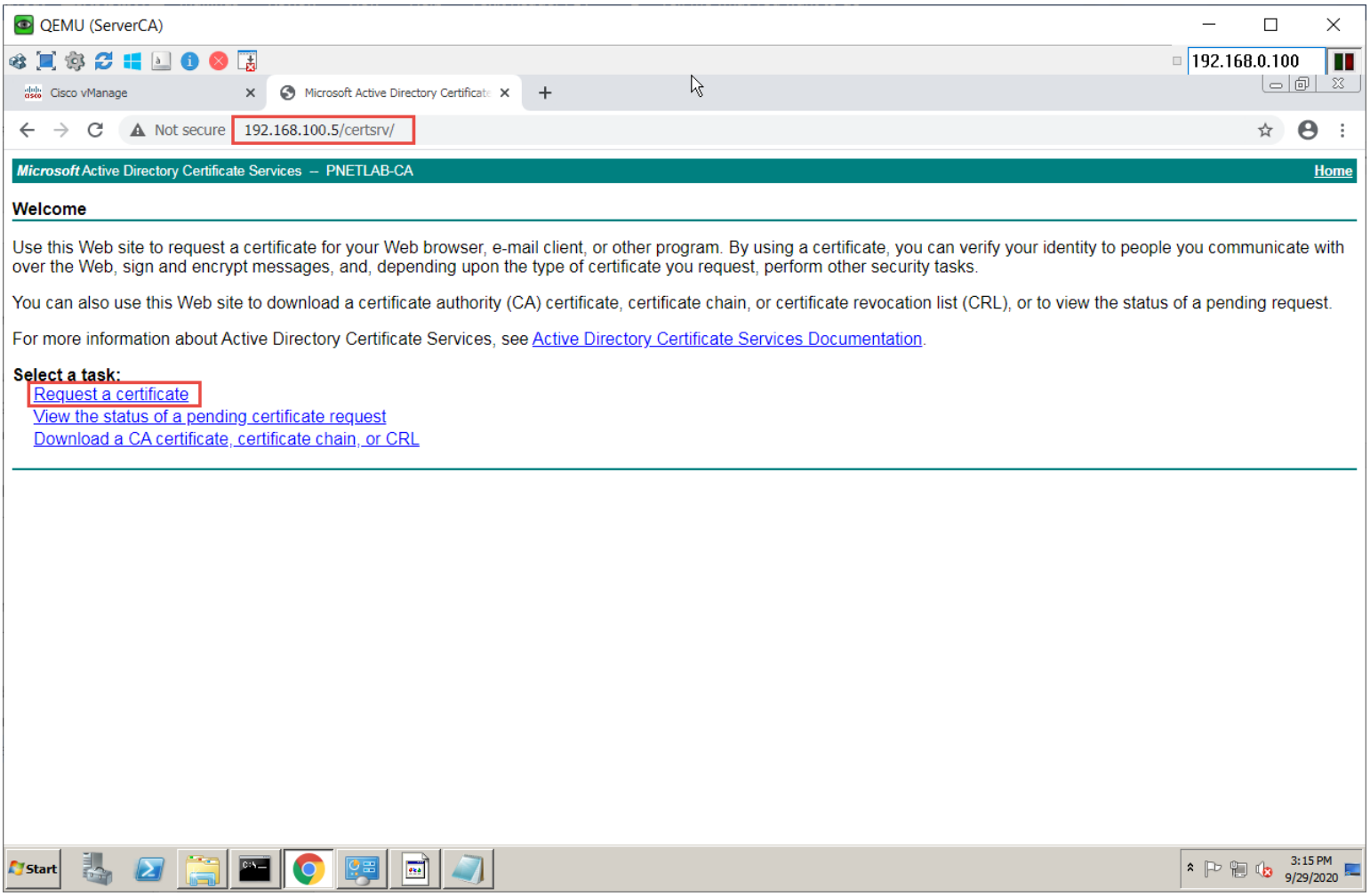


- It will open a windows with CSR. Copy by using **CTRL-A** and **CTRL-C**

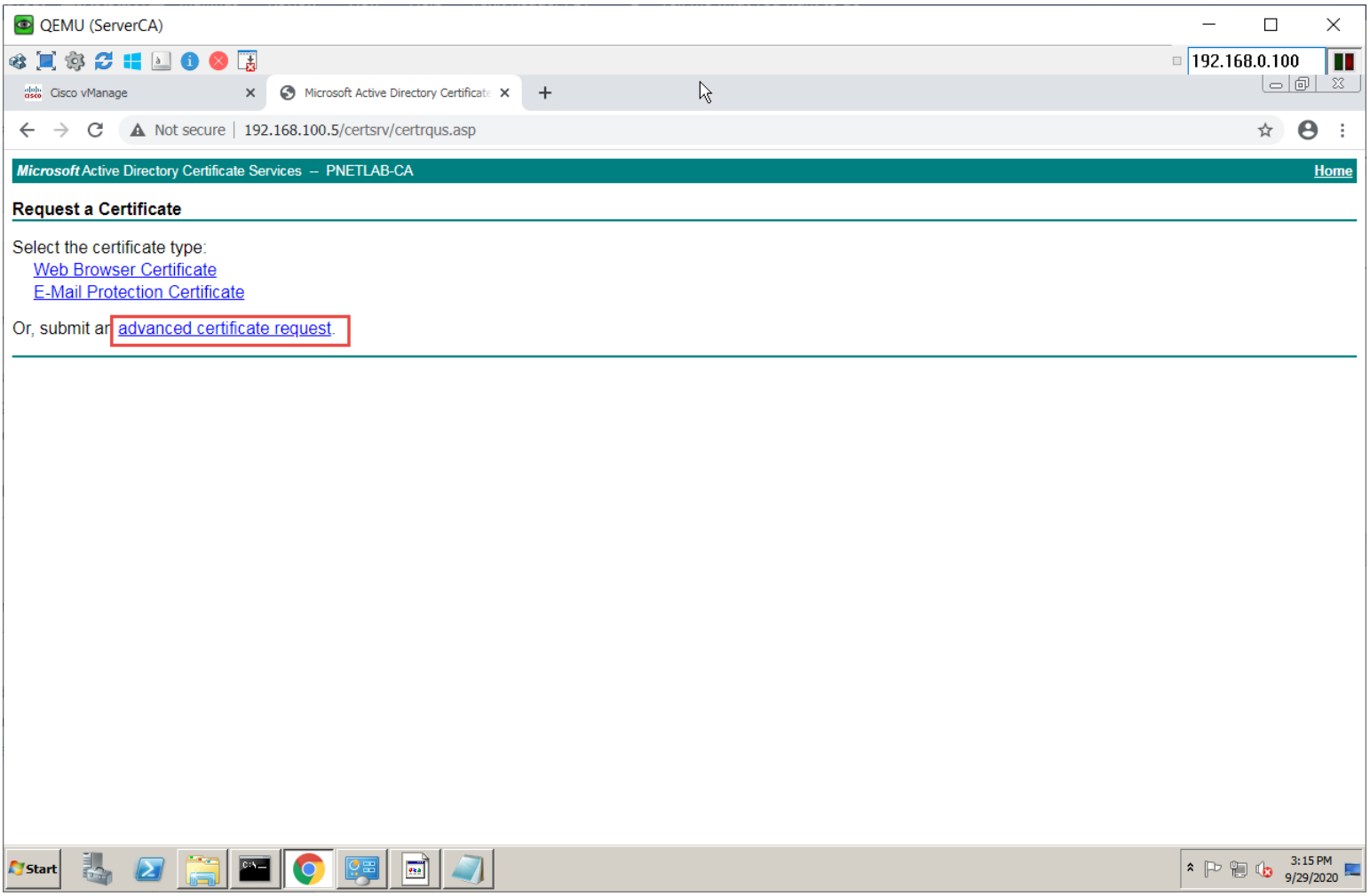

QEMU (ServerCA)
192.168.0.100
Cisco vManage
Microsoft Active Directory Certificate
Not secure | 192.168.100.2/index.html#/app/config/certificates/controller
Cisco vManage
admin
CONFIGURATION | CERTIFICATES
Install Certificate
WAN Edge List
Controllers
Send to vBond
Total Rows: 1
Operation Status
Controller Type
Expiration Date
uuid
CSR Generated
vManage
f79d5...
CSR
IP Address: 10.1.1.101
Download
-----BEGIN CERTIFICATE REQUEST-----
MIIDOTCCAiECAQAwgbqxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdQTkVUTEFCMRAw
DgYDVQQHEwdQTkVUTEFCMRAwDgYDVQQLEwdQTkVUTEFCMRAwDgYDVQQKEwdQTkVU
TEFCMT8wPQYDVQQDEzZ2bWFuYWdlLWY3OWQ1MzAyLWJhNTUtNDIyMC05MGM0LWFh
MjIjMWMxNDJlMS0wLIBORVRMQUIxIDAeBgkqhkiG9w0BCQEWEXBuZXRsYWJA
Z21h
aWwuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwq/4iSYv1/u
o
KaffgC/f8fGkmFOOWLz+MJH0db5eL4T6UEIEIFXL8Z57t6/H//VvgnJ/3Q9XAdqi
TRxLOqtu0fTUqcmB8Hwb1m03sxDr5qY8H2wavkwRRTFDAUvYS3BqsViQDoX1SL
Close
10.1.1.101
Add Device
Generate CSR
Upload Certificate
Update vBond
Start
3:12 PM
9/29/2020

Task 4 – Request a Certificate from the CA Server

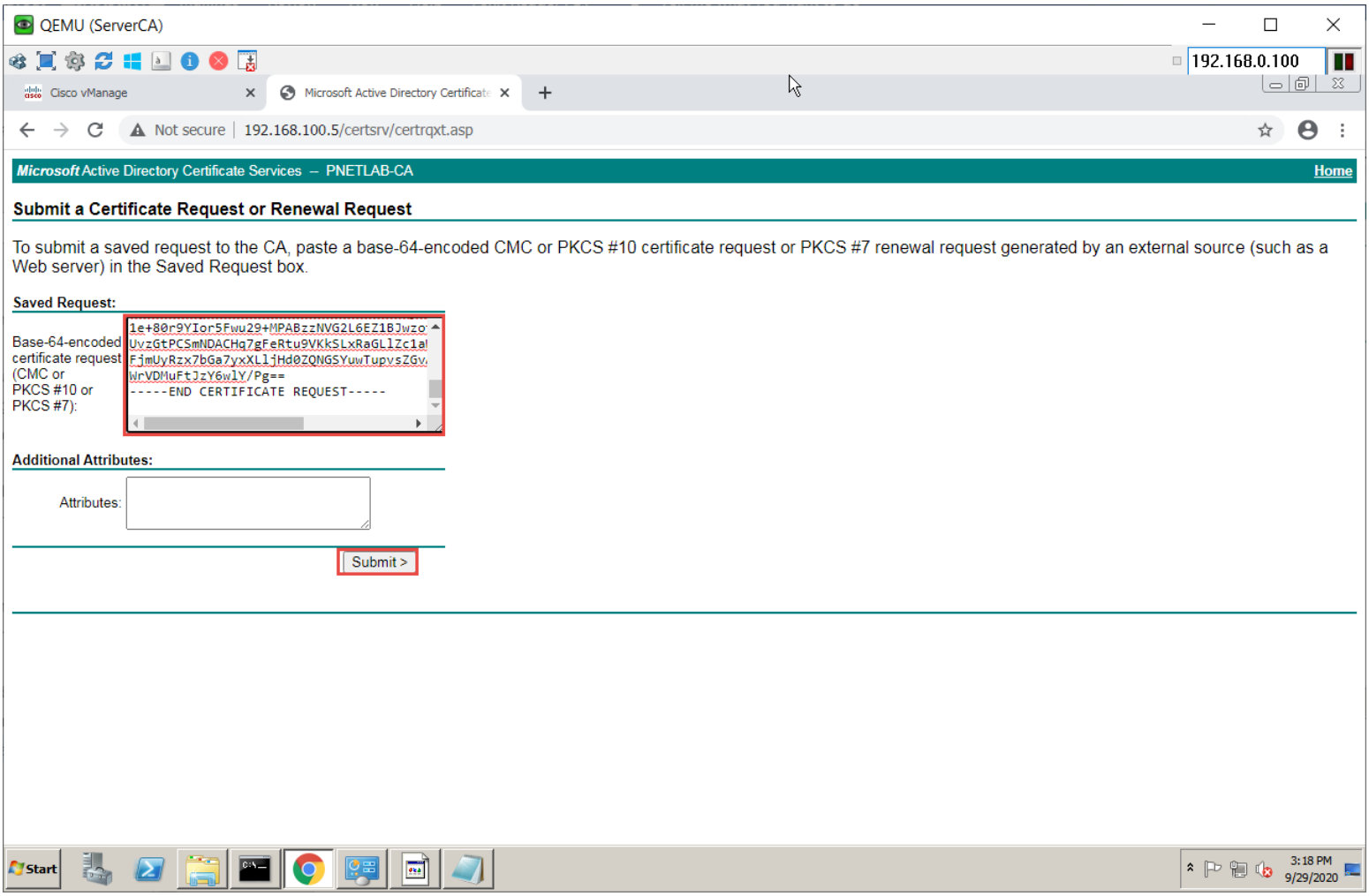
- Browser to http://192.168.1.5/certsrv
- Click "**Request a Certificate**"



- Select "**Advanced**"

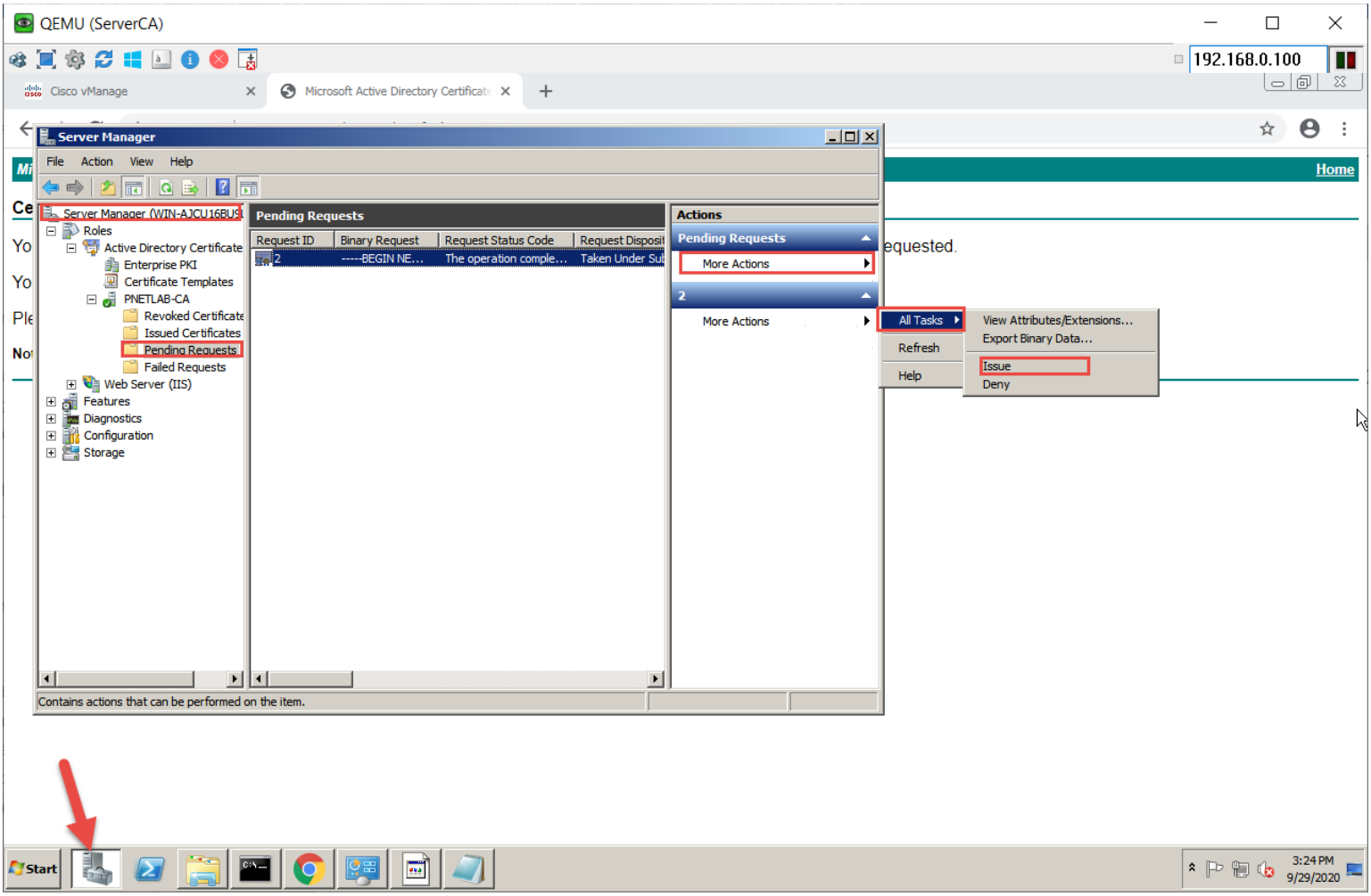


- Paste the CSR in the box by using **CTRL-V** and click submit


QEMU (ServerCA)
192.168.0.100
Cisco vManage
Microsoft Active Directory Certificate
Not secure | 192.168.100.5/certsrv/certrqxt.asp
Microsoft Active Directory Certificate Services -- PNETLAB-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
UvzGtPCSmNDACHq7gFeRtu9VKkSLxRaGLlZc1a
FjmUyRzx7bGa7yxXLljHd0ZQNGSYuwTupvsZGv
WrVDMuFtJzY6wlY/Pg==
-----END CERTIFICATE REQUEST-----
Additional Attributes:
Attributes:
Submit >
Start
3:18 PM
9/29/2020

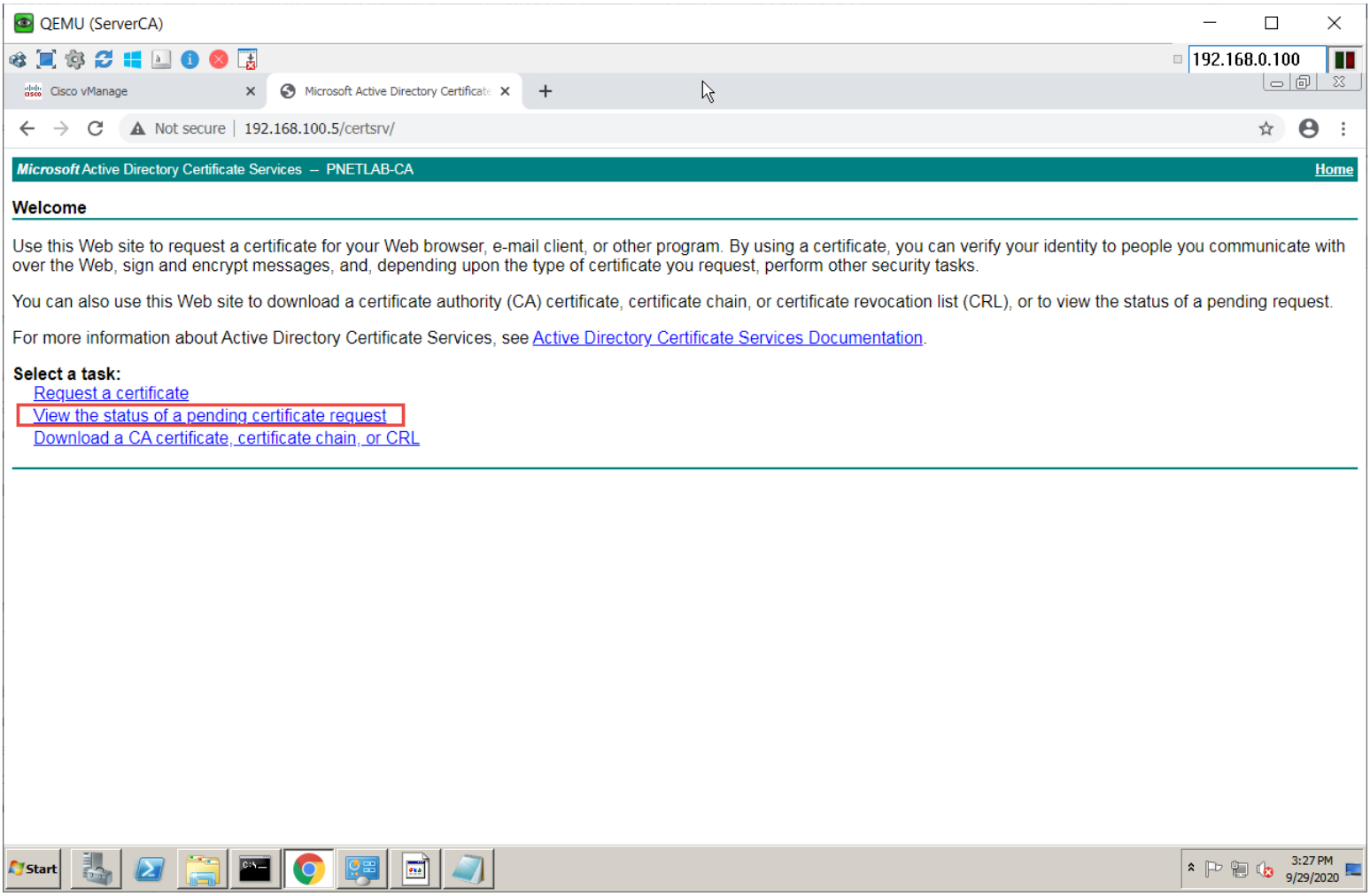
Task 5 – Issue the Certificate from the CA Server

- Open **Server Manager ➔ Roles ➔ Active Directory Certificate Server ➔ PNETLAB-CA ➔ Pending Request**.
- Right-click the request ➔ **more action ➔ all tasks and click "Issue"**

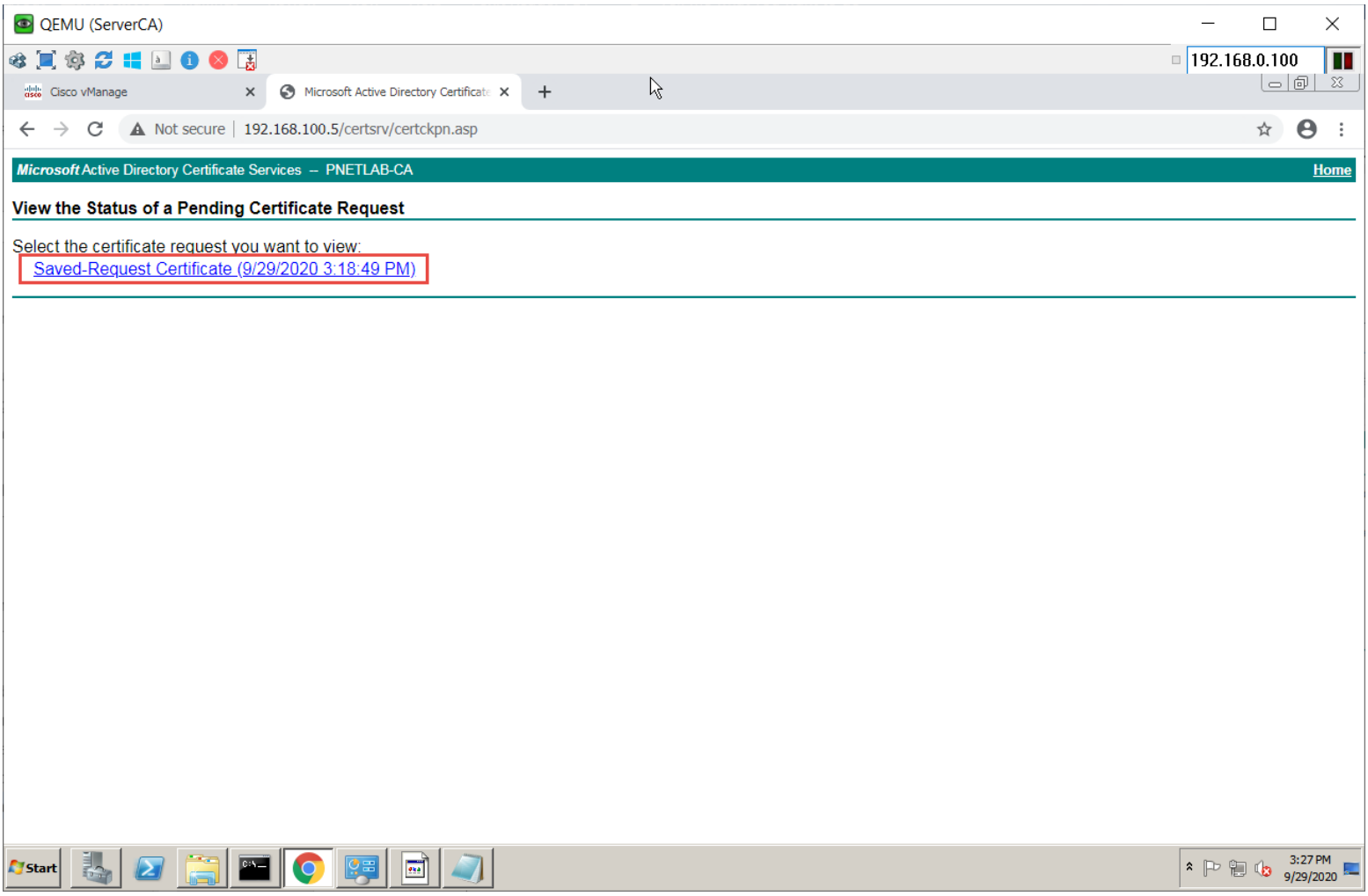


Task 6- Downloading the Issueed Certificate

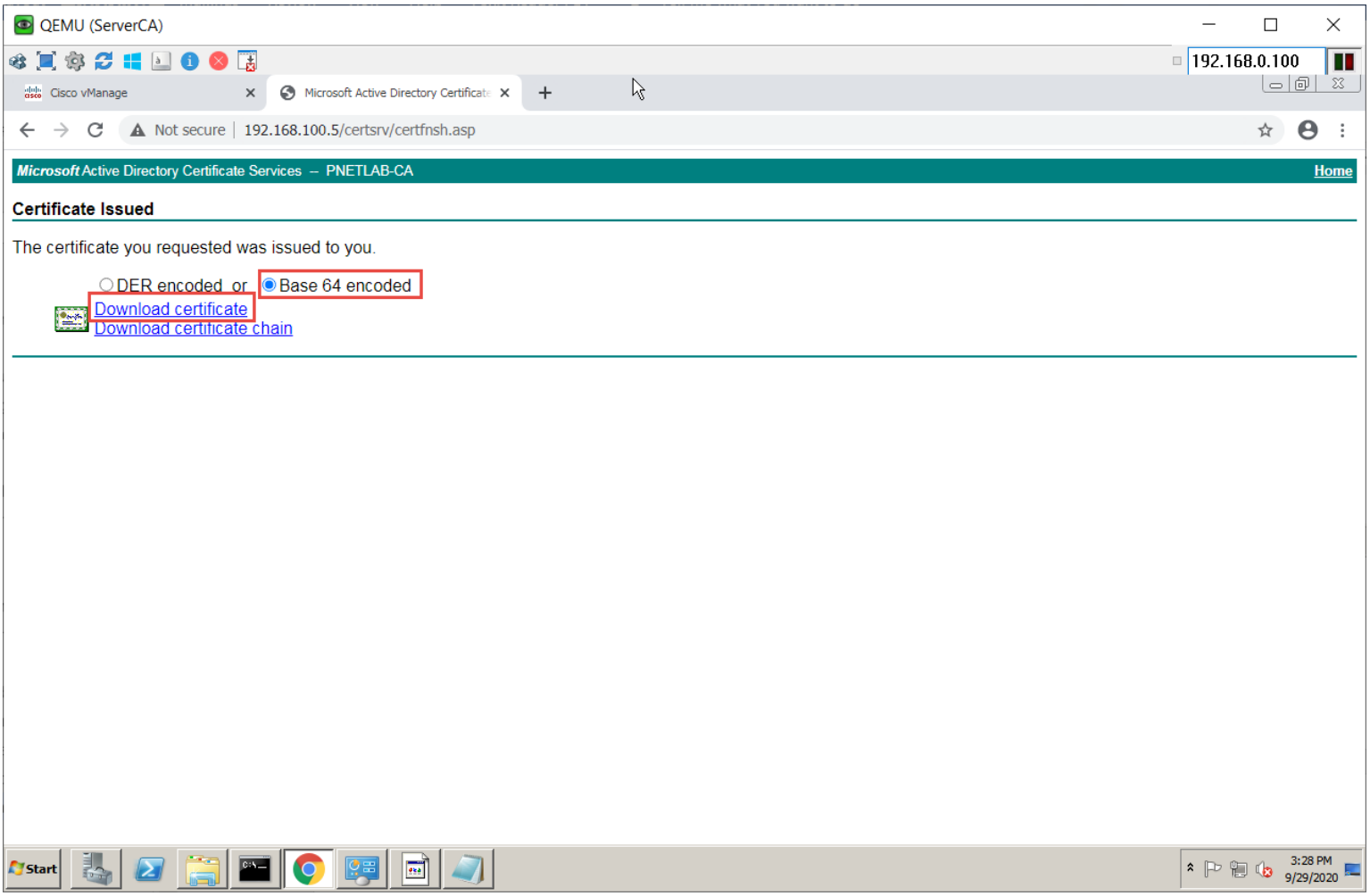
- Browser to http://192.168.100.5/certsrv
- Click "**Check on Pending Certificate Request**"



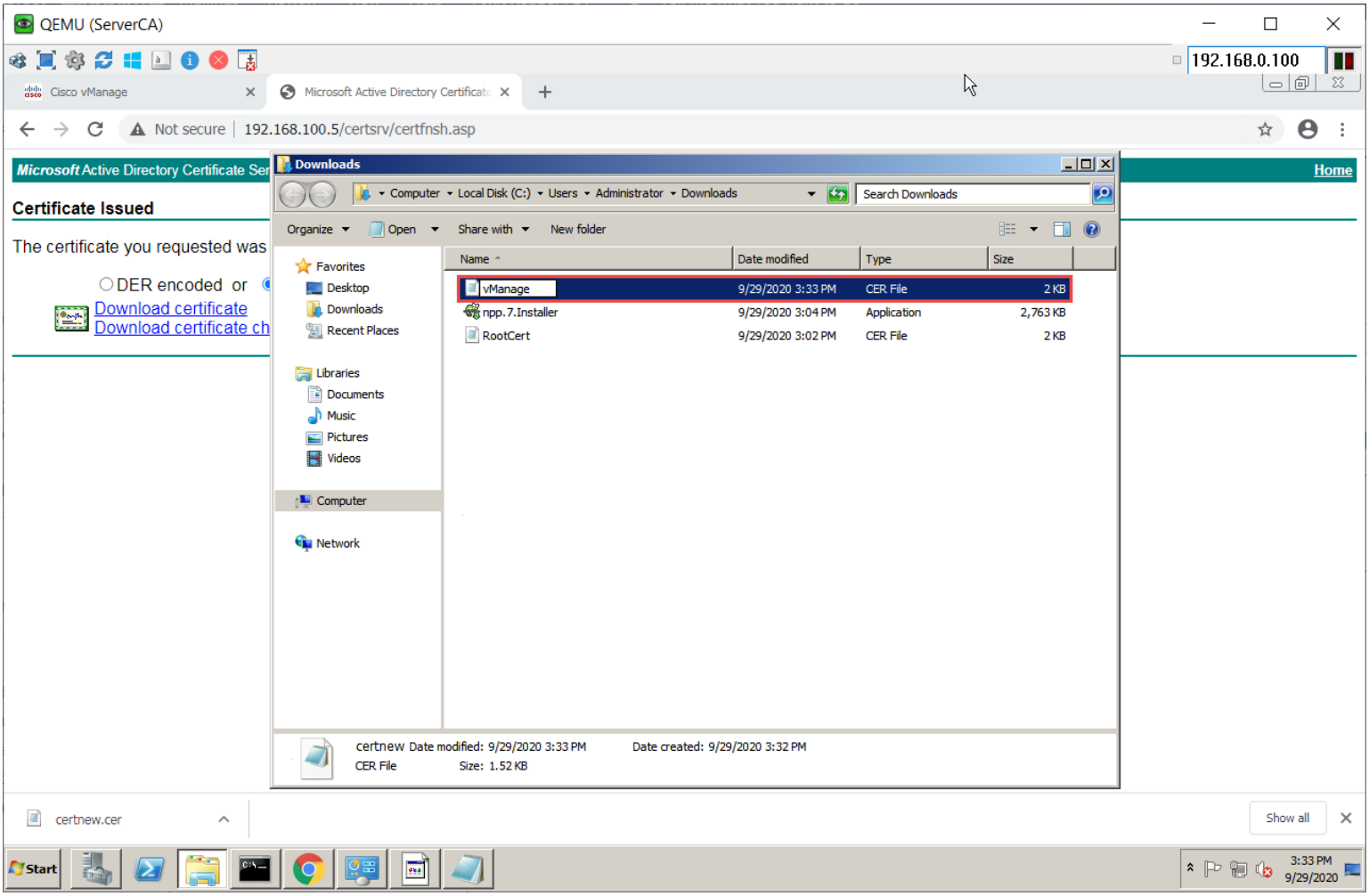
- The issued certificate link will show up. Click on the link



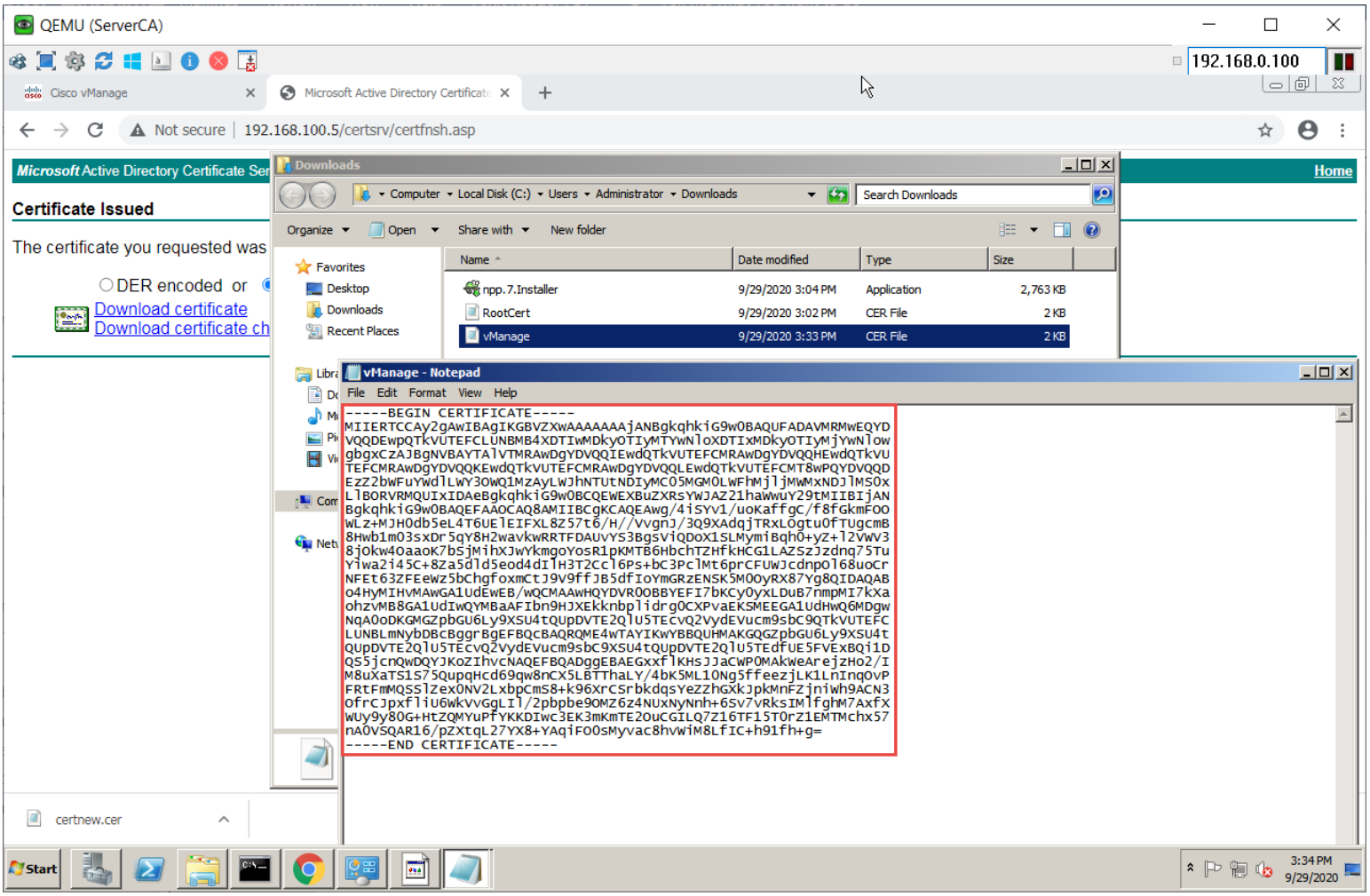
- Select "**Base 64**" and click "**Download**"



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

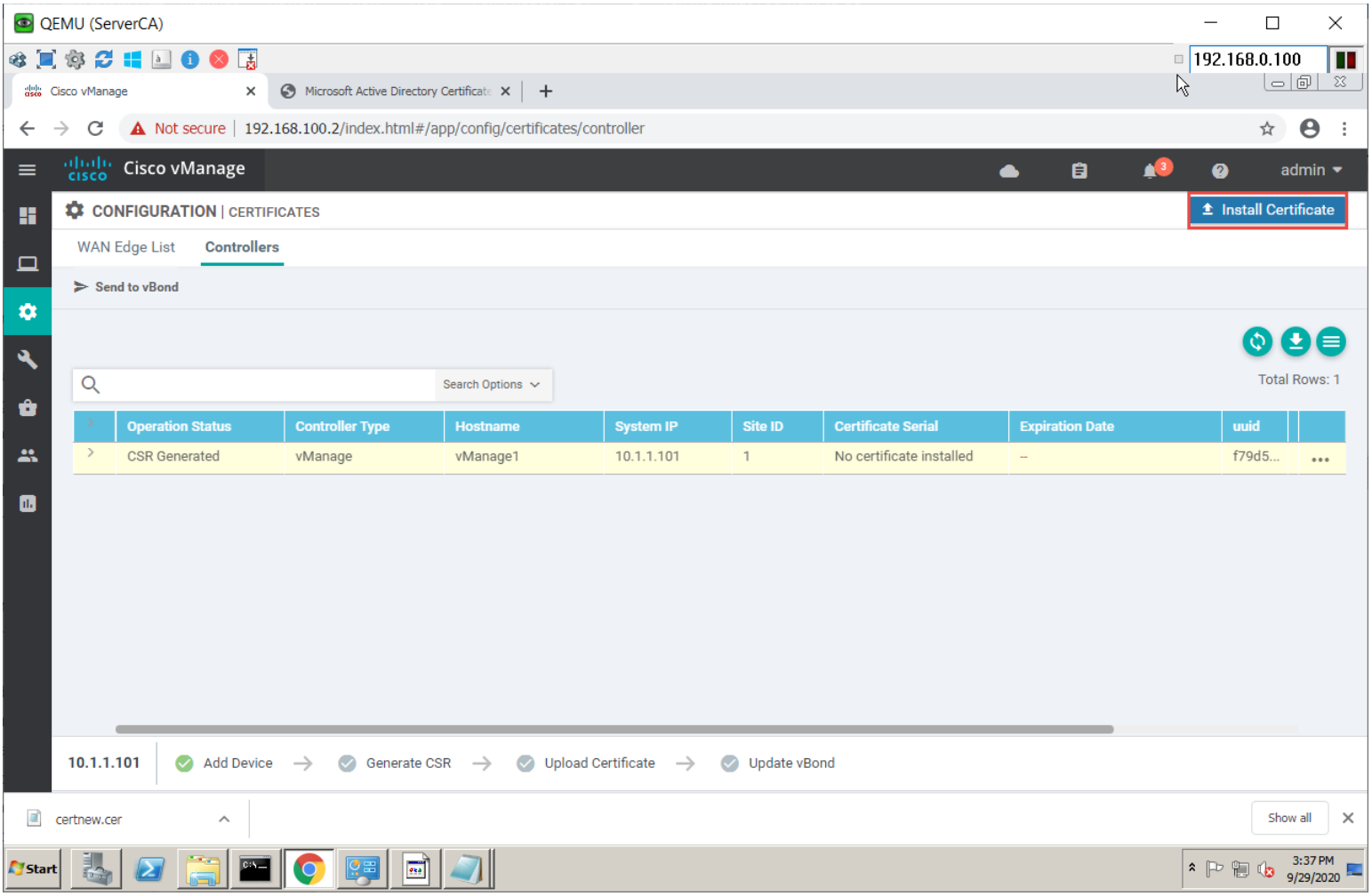


- Open the "**vManage.cer**" file using Notepad
- Copy using **CTRL-A** and **CTRL-C**

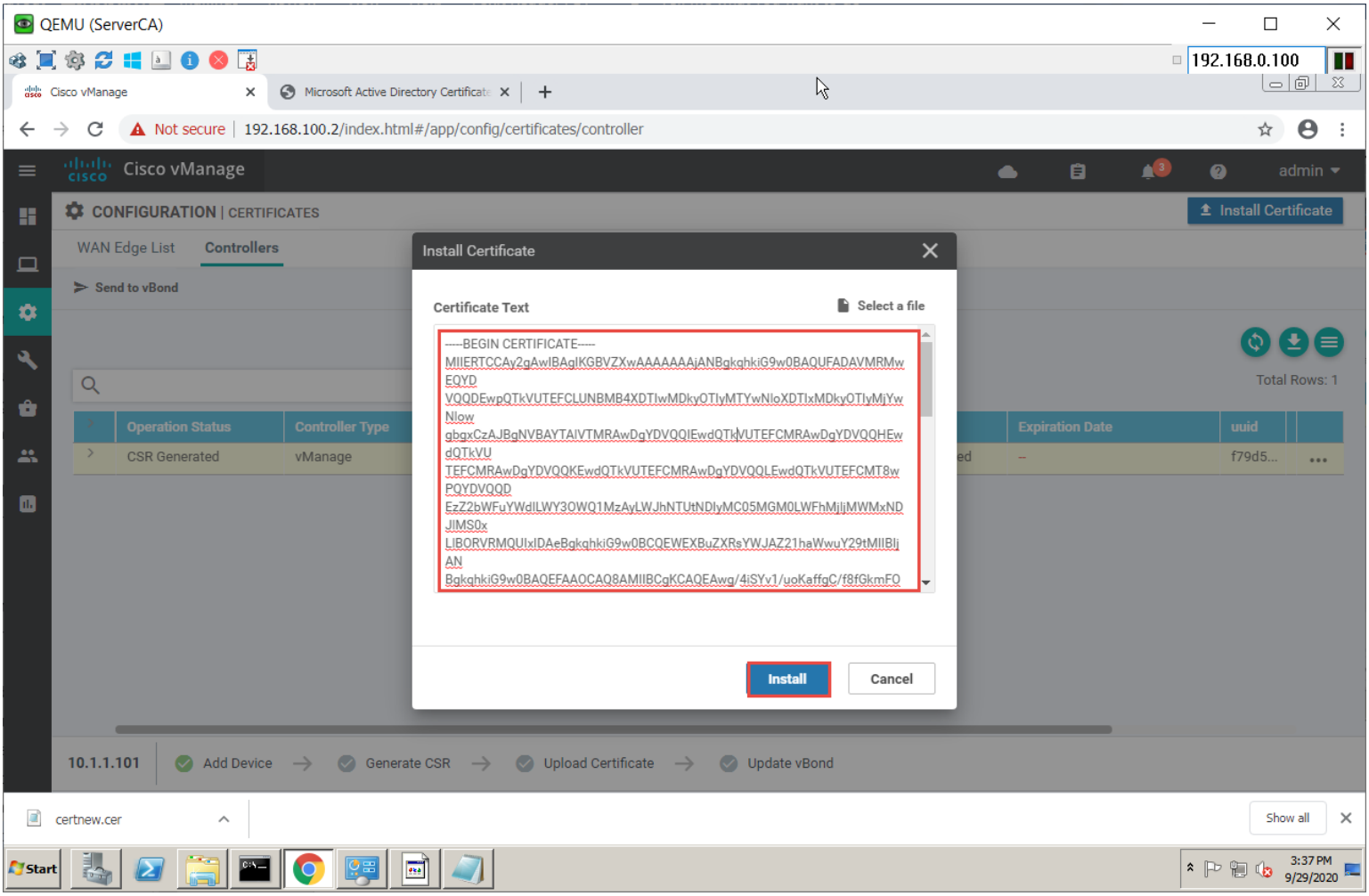

QEMU (ServerCA)
192.168.0.100
Cisco vManage
Microsoft Active Directory Certificate
Not secure | 192.168.100.5/certsrv/certfnsh.asp
Microsoft Active Directory Certificate Ser
Home
Certificate Issued
The certificate you requested was
DER encoded or
Download certificate
Download certificate ch
Downloads
Computer ▸ Local Disk (C:) ▸ Users ▸ Administrator ▸ Downloads
Search Downloads
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
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
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIERTCCAy2gAwIBAgIKGBVZXwAAAAAAAjANBgkqhkiG9w0BAQUFADAVMRMwEQYD
VQQDEwpQTkVUTEFCLUNBMB4XDTIwMDkyOTIyMTYwNloXDTIxMDkyOTIyMjYwNlow
gbgxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdQTkVUTEFCMRAwDgYDVQQHEwdQTkVU
TEFCMRAwDgYDVQQKEwdQTkVUTEFCMRAwDgYDVQQLEwdQTkVUTEFCMT8wPQYDVQQD
EzZ2bWFuYWdlLWY3OWQ1MzAyLWJhNTUtNDIyMC05MGM0LWFhMjljMWMxNDJlMS0x
LlBORVRMQUIxIDAeBgkqhkiG9w0BCQEWEXBuZXRsYWJAZ21haWwuY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwg/4iSYv1/uoKaffgC/f8fGkmFOO
WLz+MJHOdb5eL4T6UElEIFXL8Z57t6/H//VvgnJ/3Q9XAdqjTRxLOgtuOfTUgcmB
8Hwb1m03sxDr5qY8H2wavkwRRTFDAUvYS3BgsViQDoX1SLMymiBqhO+yZ+l2VwV3
8jOkw4OaaoK7bSjMihXJwYkmgoYosR1pKMTB6HbchTZHfkHCG1LAZSzJzdnq75Tu
Yiwa2i45C+8Za5dld5eod4dIlH3T2Ccl6Ps+bC3PclMt6prCFUWJcdnpOl68uoCr
NFEt63ZFEeWz5bChgfoxmCtJ9V9ffJB5dfIoYmGRzENSK5M0OyRX87Yg8QIDAQAB
o4HyMIHvMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFI7bKCy0yxLDuB7nmpMI7kXa
ohzvMB8GA1UdIwQYMBaAFIbn9HJXEkknbplidrg0CXPvaEK5MEEGA1UdHwQ6MDgw
NqA0oDKGMGZpbGU6Ly9XSU4tQUpDVTE2QlU5TEcvQ2VydEVucm9sbC9QTkVUTEFC
LUNBLmNybDBcBggrBgEFBQcBAQRQME4wTAYIKwYBBQUHMAKGQGZpbGU6Ly9XSU4t
QUpDVTE2QlU5TEcvQ2VydEVucm9sbC9XSU4tQUpDVTE2QlU5TEdfUE5FVExBQi1D
QS5jcnQwDQYJKoZIhvcNAQEFBQADggEBAEGxxflKHsJJaCWP0MAkWeArejzHo2/I
M8uXaTS1S75QupqHcd69qw8nCX5LBTThaLY/4bK5ML1ONg5ffeezjLK1LnInqOvP
FRtFmMQSSlZex0NV2LxbpCmS8+k96XrCSrbkdqsYeZZhGXkJpkMnFZjniWh9ACN3
OfrCJpxfliU6WkVvGgLIl/2pbpbe9OMZ6z4NUxNyNnh+6Sv7vRksIMlfgHM7AxfX
WUy9y8OG+HtZQMYuPfYKKDIwc3EK3mKmTE2OuCGILQ7Z16TF15TOrZ1EMTMchx57
nA0VSQAR16/pZXtqL27YX8+YAqiFO0sMyvac8hvwiM8LfIC+h91fh+g=
-----END CERTIFICATE-----
certnew.cer
Start
3:34 PM
9/29/2020

Task 7- Installing the Identity Certificate for vManage

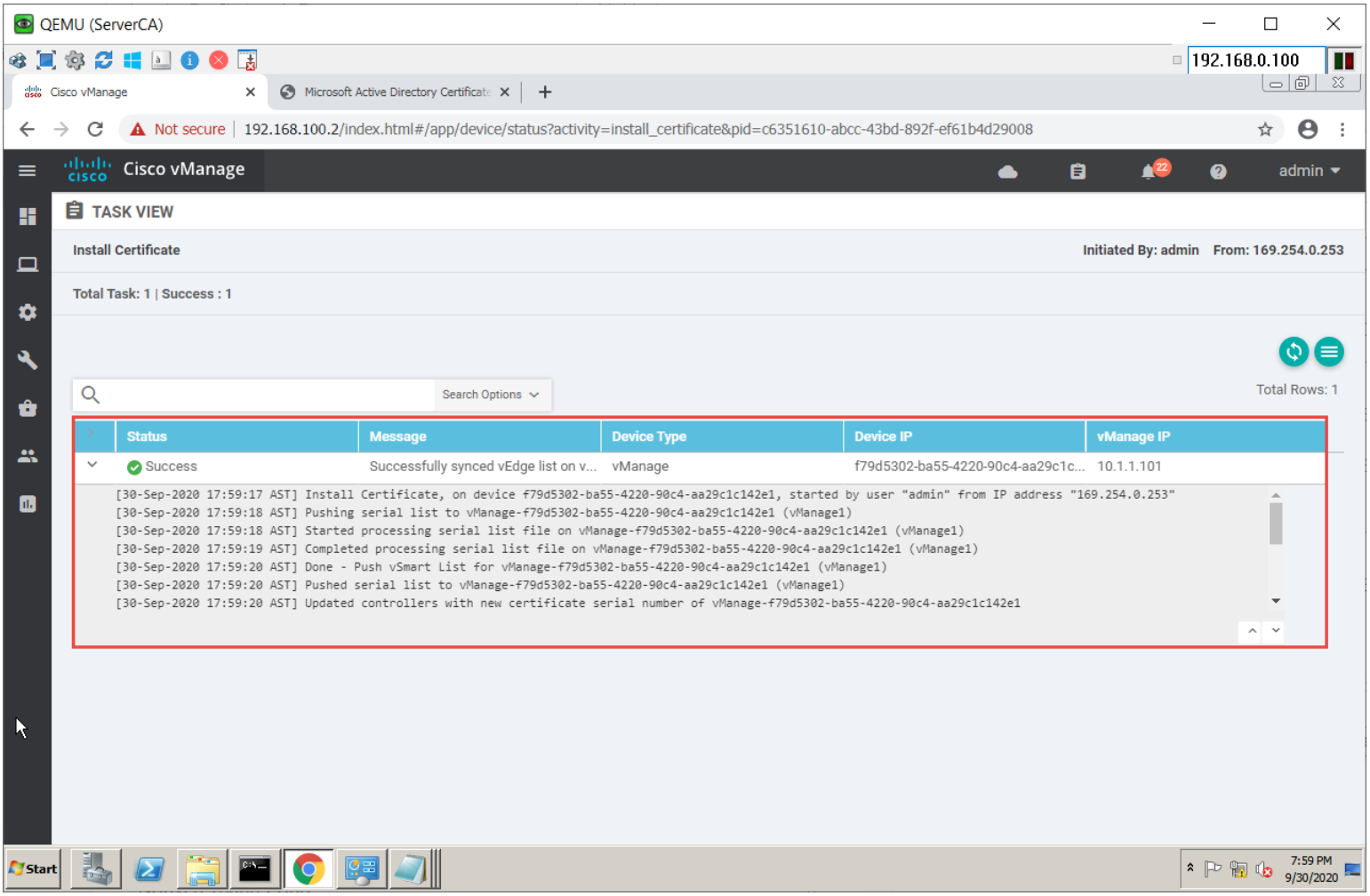
- In vManage, **Navigate to Configuration ➔ Certificate ➔ Controller**
- Click on the "**install**" button at the top right corner



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



- The identity certificate should be installed on vManage


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=c6351610-abcc-43bd-892f-ef61b4d29008
Cisco vManage
admin
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...
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
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:
  - Hostname: **vBond1**
  - Organization: **"viptela sdwan"**
  - System-IP: **100.1.1.14**
  - Site ID: 1
  - vbond Address: **100.1.1.4**
  - 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:
  - 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
  - Vpn 512
    - Interface eth0
    - Ip address: 192.168.100.4

vBond

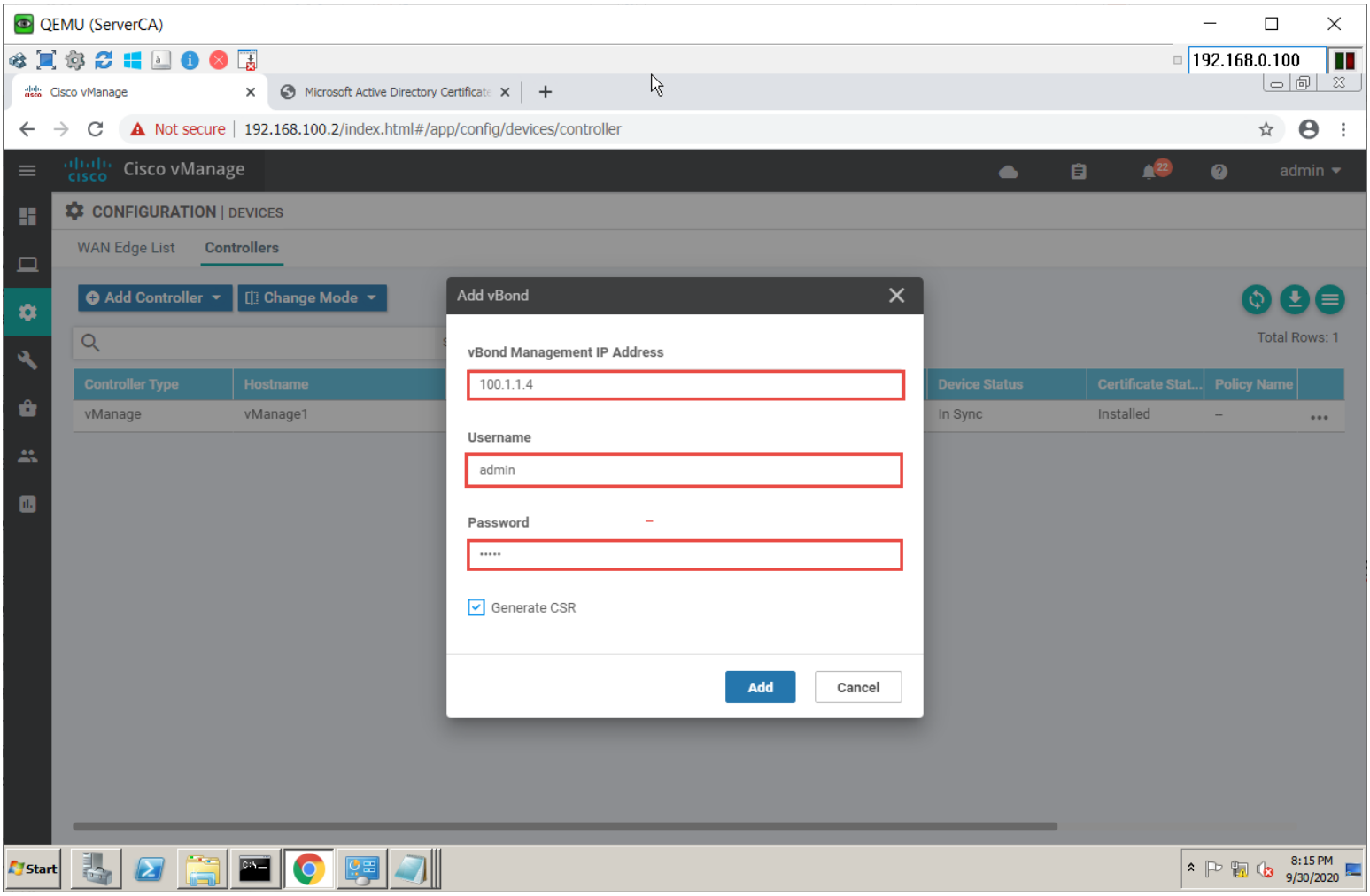
```
config
!
vpn 0
no interface eth0
```

```
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

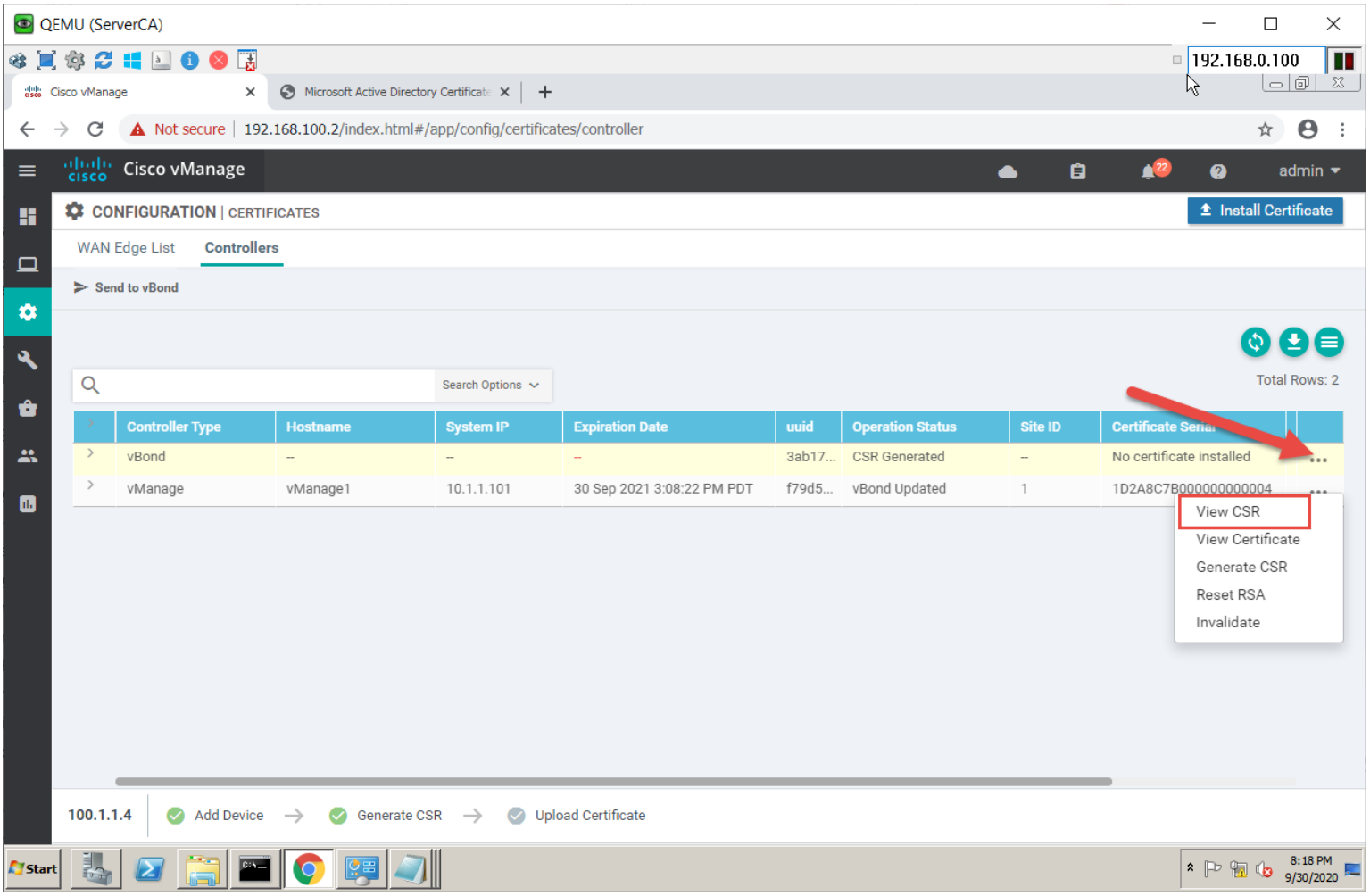
Task 1 – Add vBond to vManage

- 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

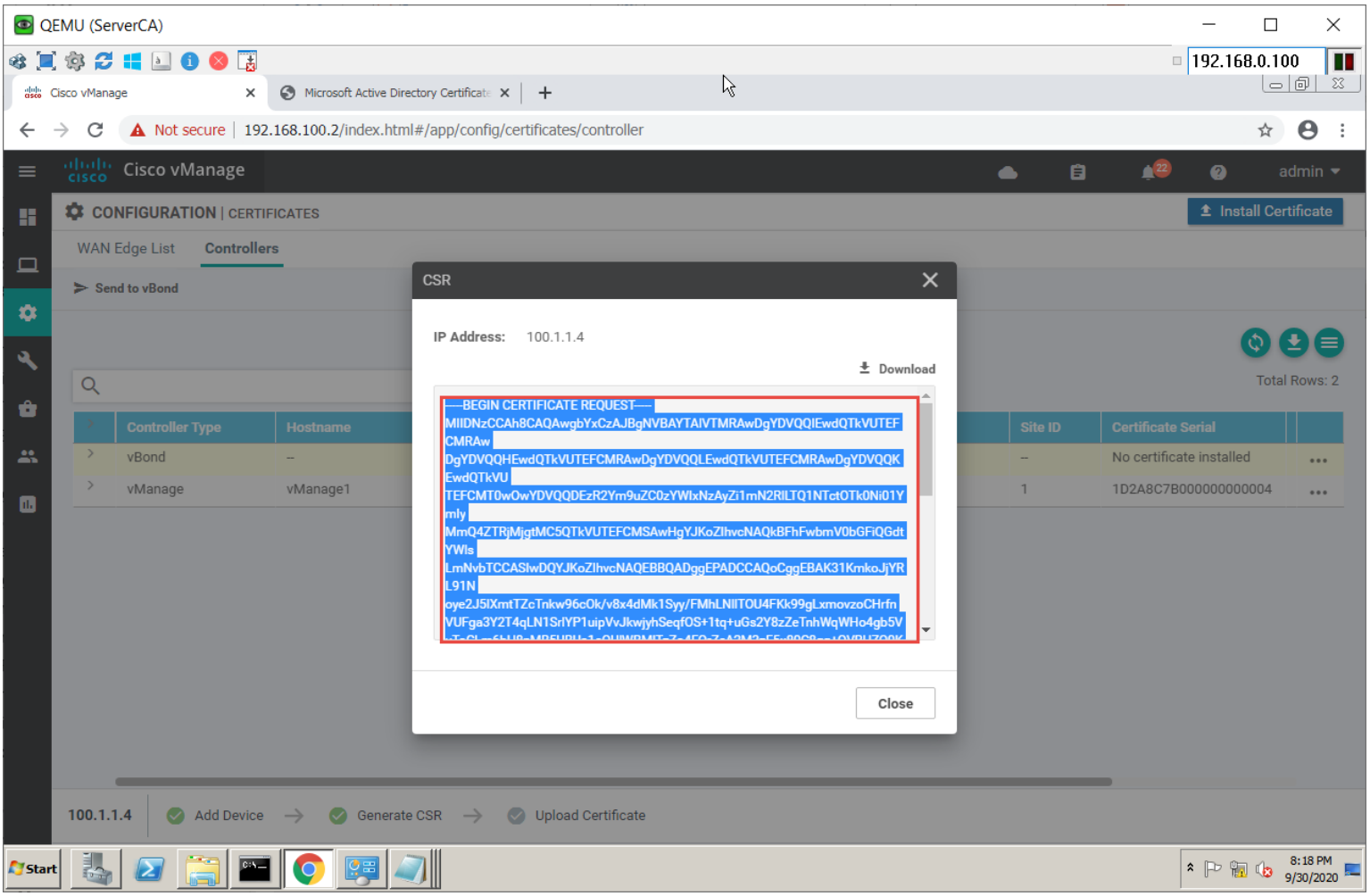


Task 2 – View the generated CSR for vBond and copy it

- Navigate to **Configuration** ➔ **Certificates** ➔ **Controllers** ➔ **vBond** ➔ **view CSR**

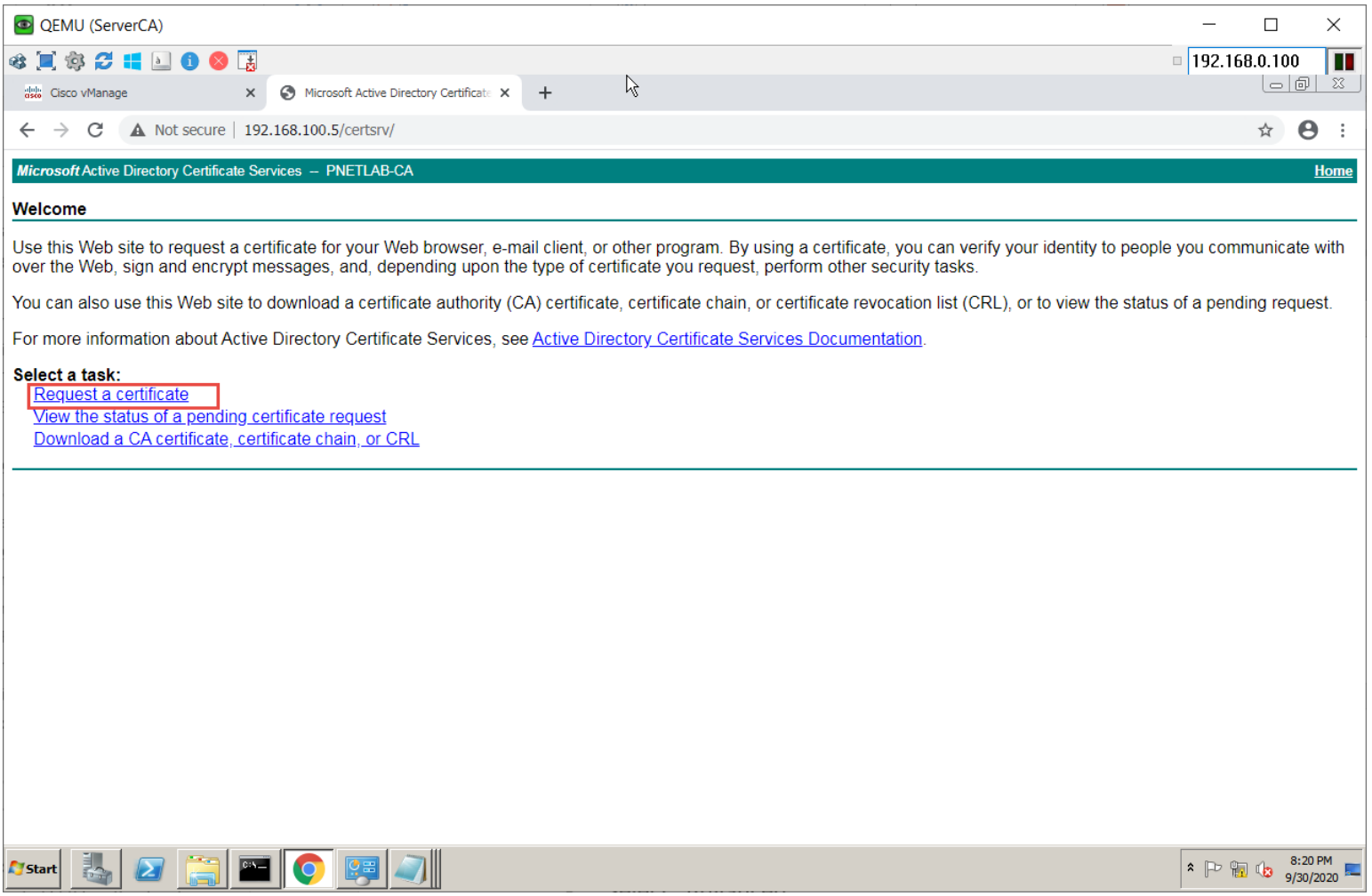


- It will open a windows with CSR. Copy by using **CTRL-A** and **CTRL-C**

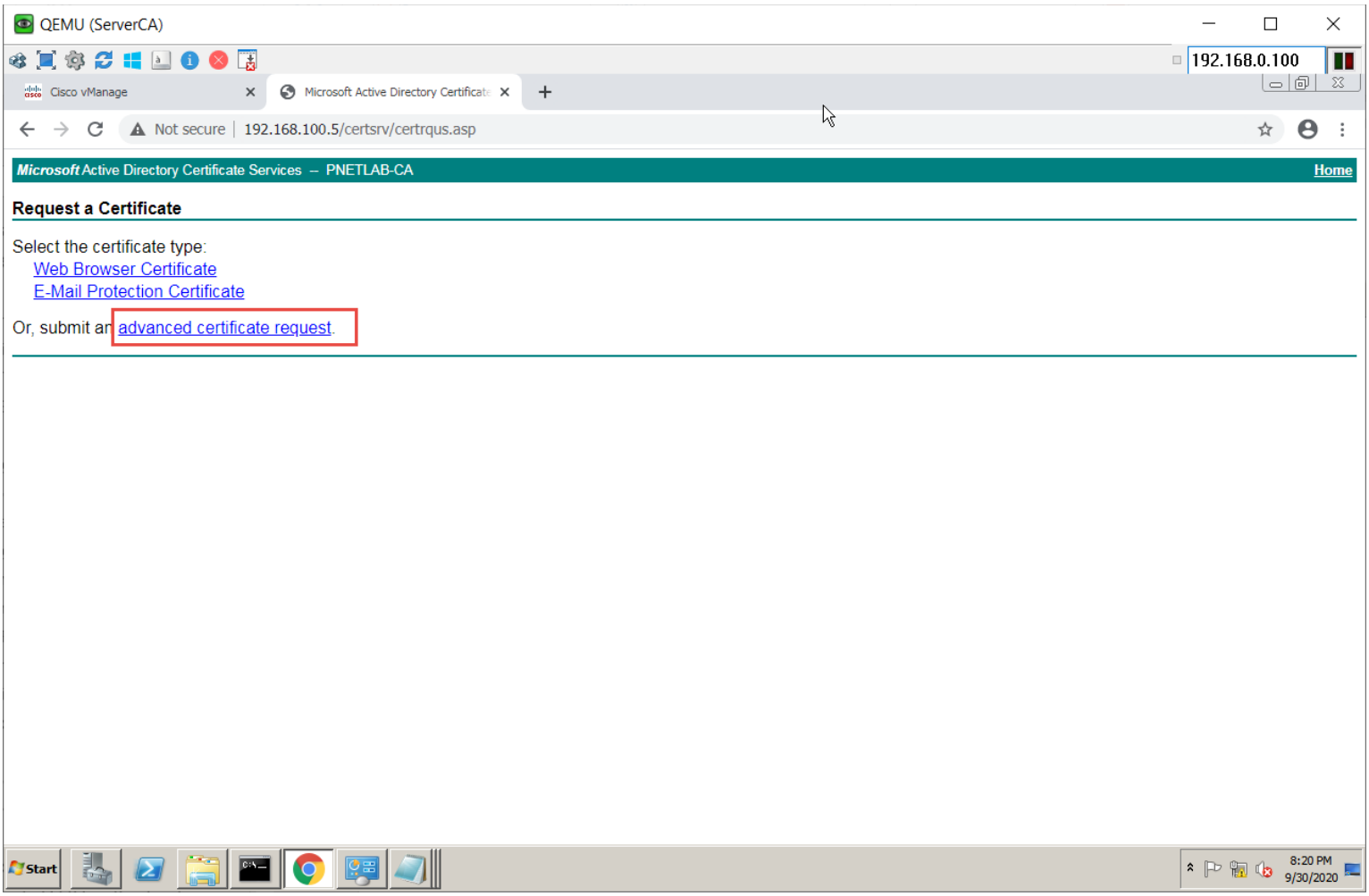

QEMU (ServerCA)
192.168.0.100
Cisco vManage
Microsoft Active Directory Certificate
Not secure
192.168.100.2/index.html#/app/config/certificates/controller
Cisco vManage
admin
CONFIGURATION | CERTIFICATES
Install Certificate
WAN Edge List
Controllers
Send to vBond
Total Rows: 2
Controller Type
Hostname
Site ID
Certificate Serial
vBond
No certificate installed
vManage
vManage1
1
1D2A8C7B000000000004
CSR
IP Address: 100.1.1.4
Download
-----BEGIN CERTIFICATE REQUEST-----
MIIDNzCCAh8CAQAwgbYxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdQTkVUTEFCMRAw
DgYDVQQHEwdQTkVUTEFCMRAwDgYDVQQLEwdQTkVUTEFCMRAwDgYDVQQKEwdQTkVU
TEFCMT0wOwYDVQQDEzR2Ym9uZC0zYWIxNzAyZi1mN2RlLTQ1NTctOTk0Ni01YmIy
MmQ4ZTRjMjgtMC5QTkVUTEFCMSAwHgYJKoZIhvcNAQkBFhFwbmV0bGFiQGdtYWls
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK31KmkoJjYRL91N
oye2J5lXmtTZcTnkw96c0k/v8x4dMk1Syy/FMhLNIITOU4FKk99gLxmovzoCHrfn
VUFga3Y2T4qLN1SrlYP1uipVvJkwjyhSeqfOS+1tq+uGs2Y8zZeTnhWqWHo4gb5V
Close
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

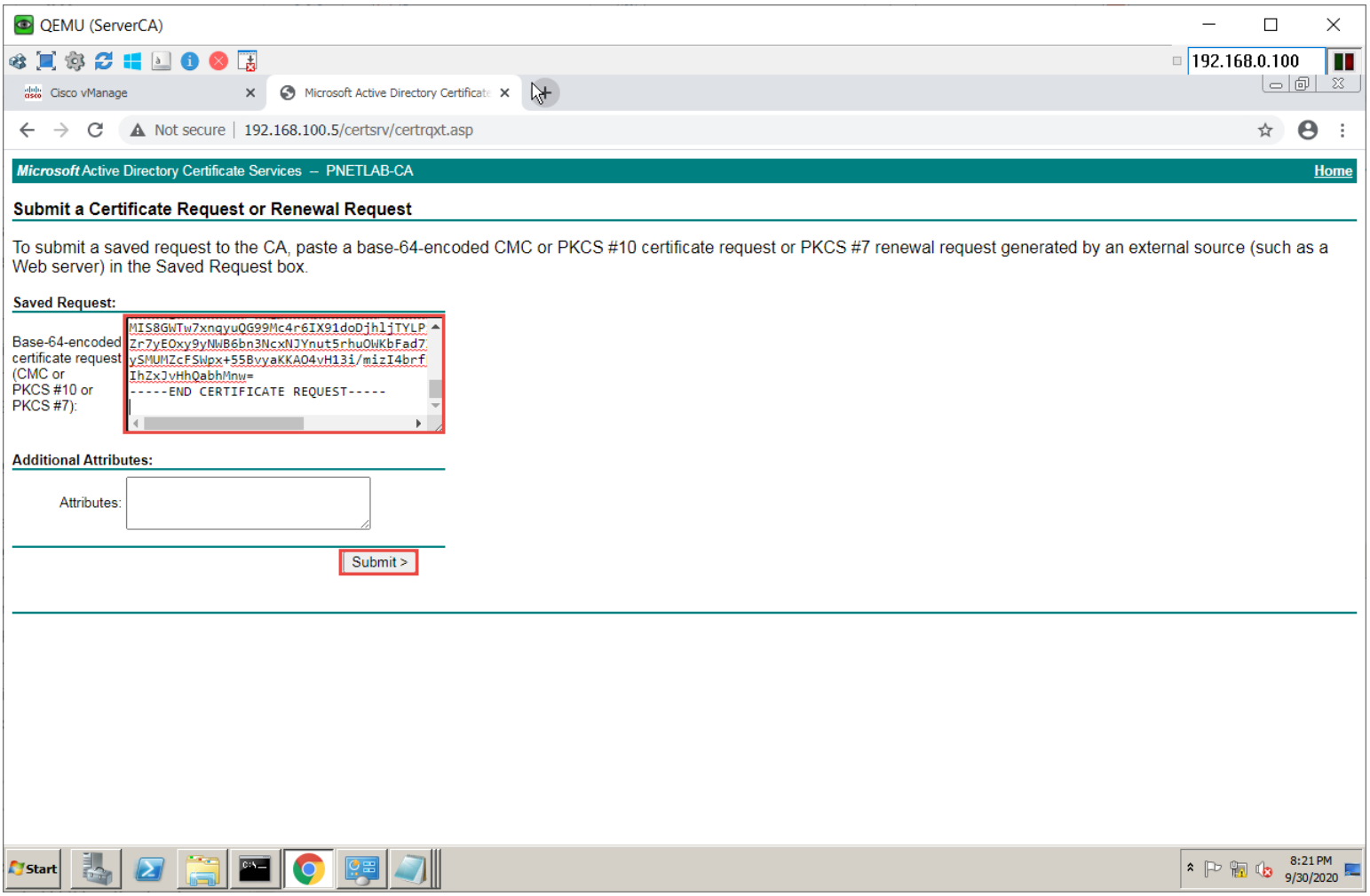
- Browser to http://192.168.100.5/certsrv
- Click "**Request a Certificate**"



- Select "**Advanced**"

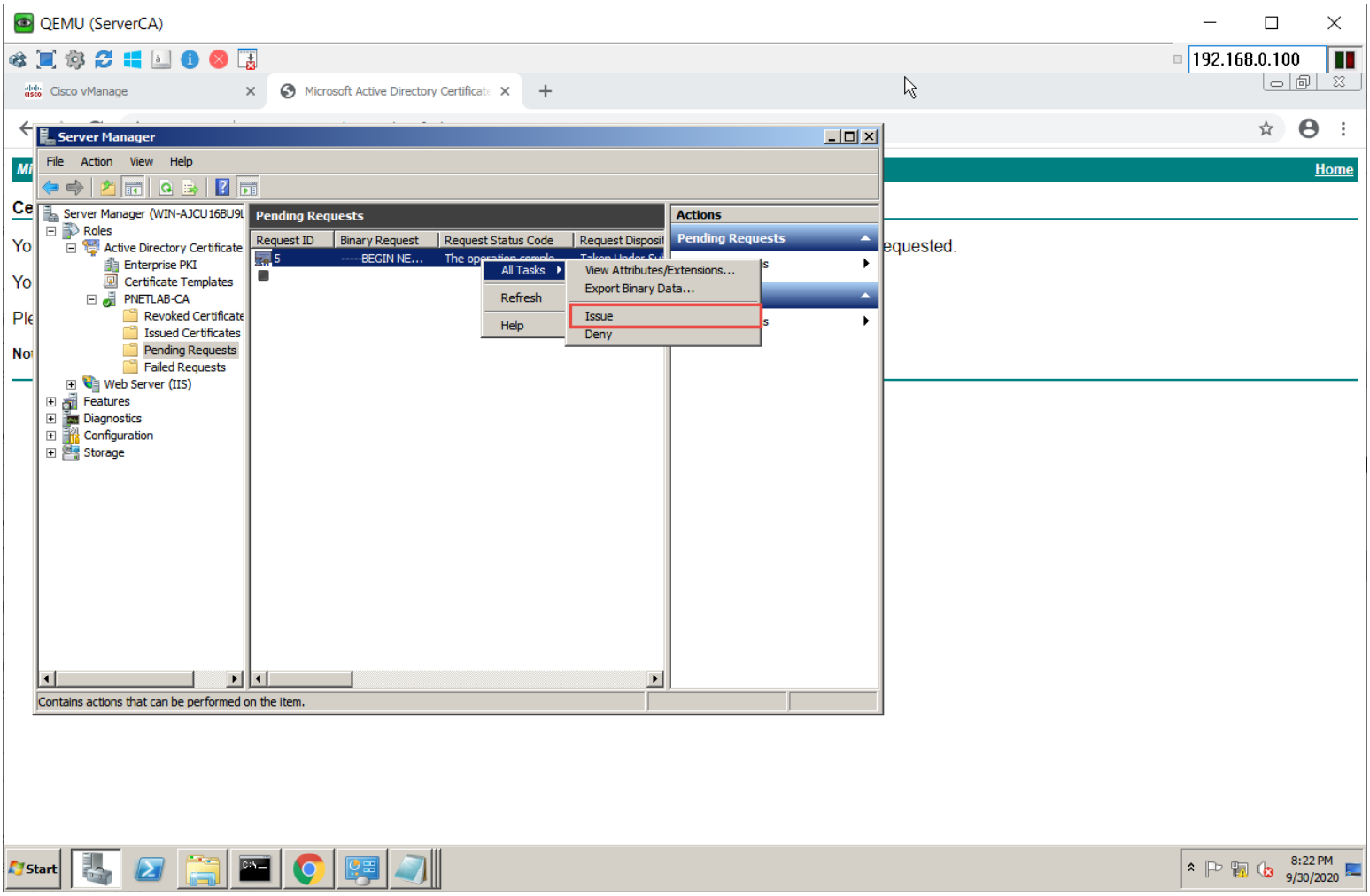


- Paste the CSR in the box by using **CTRL-V** and click **Submit**



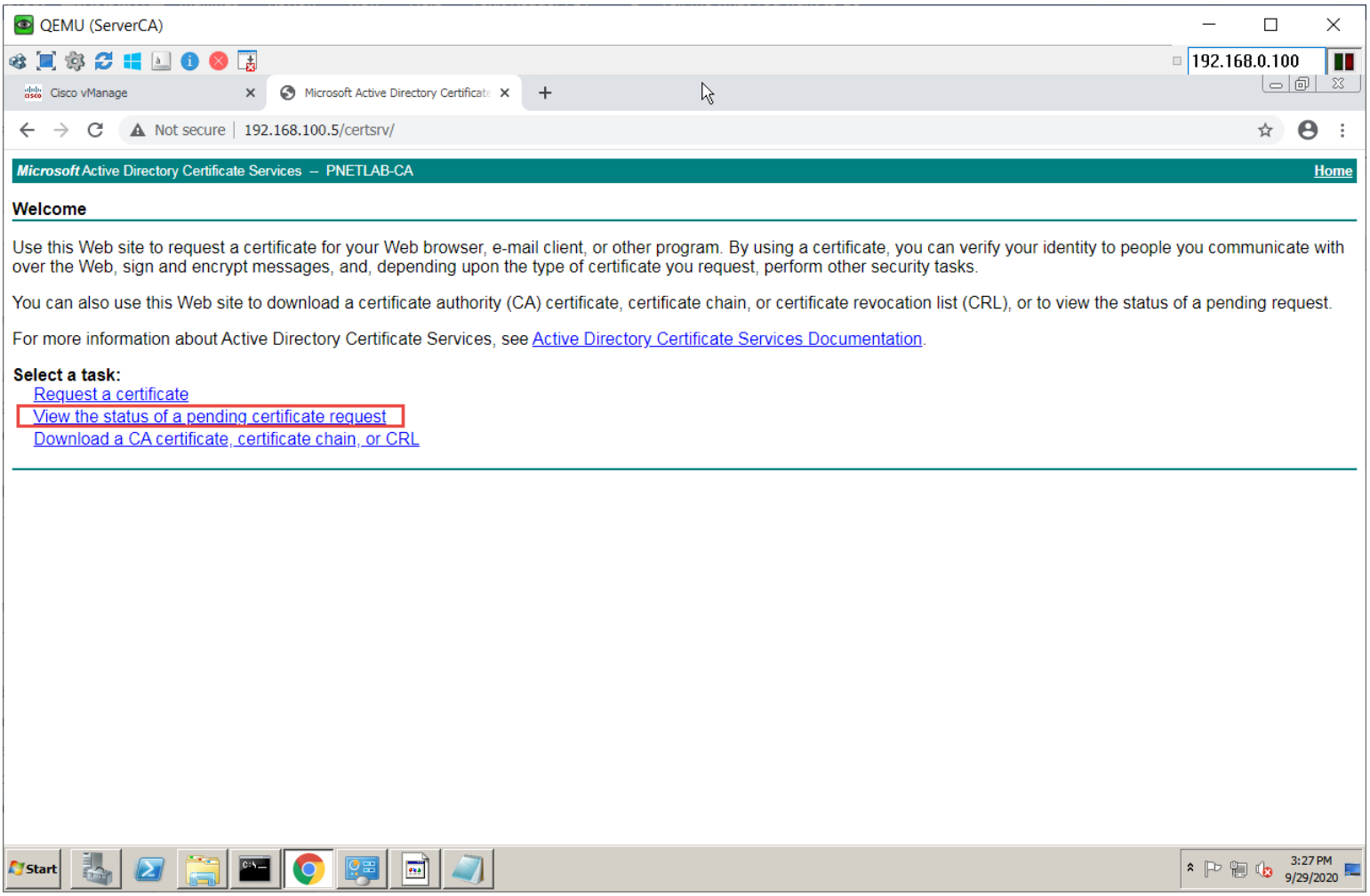
Task 4 – Issue the Certificate from the CA Server

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

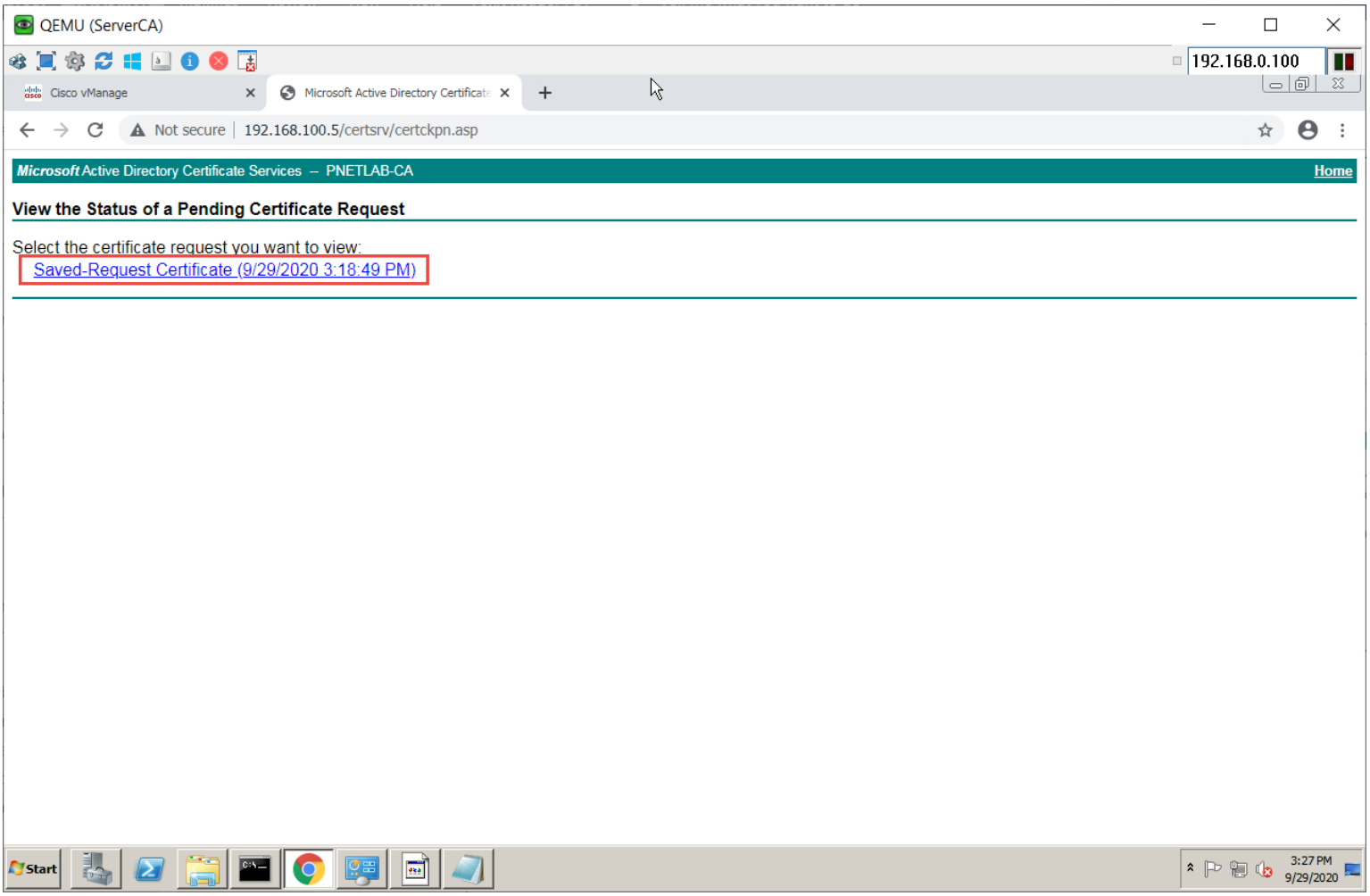


Task 5- Downloading the Issued Certificate

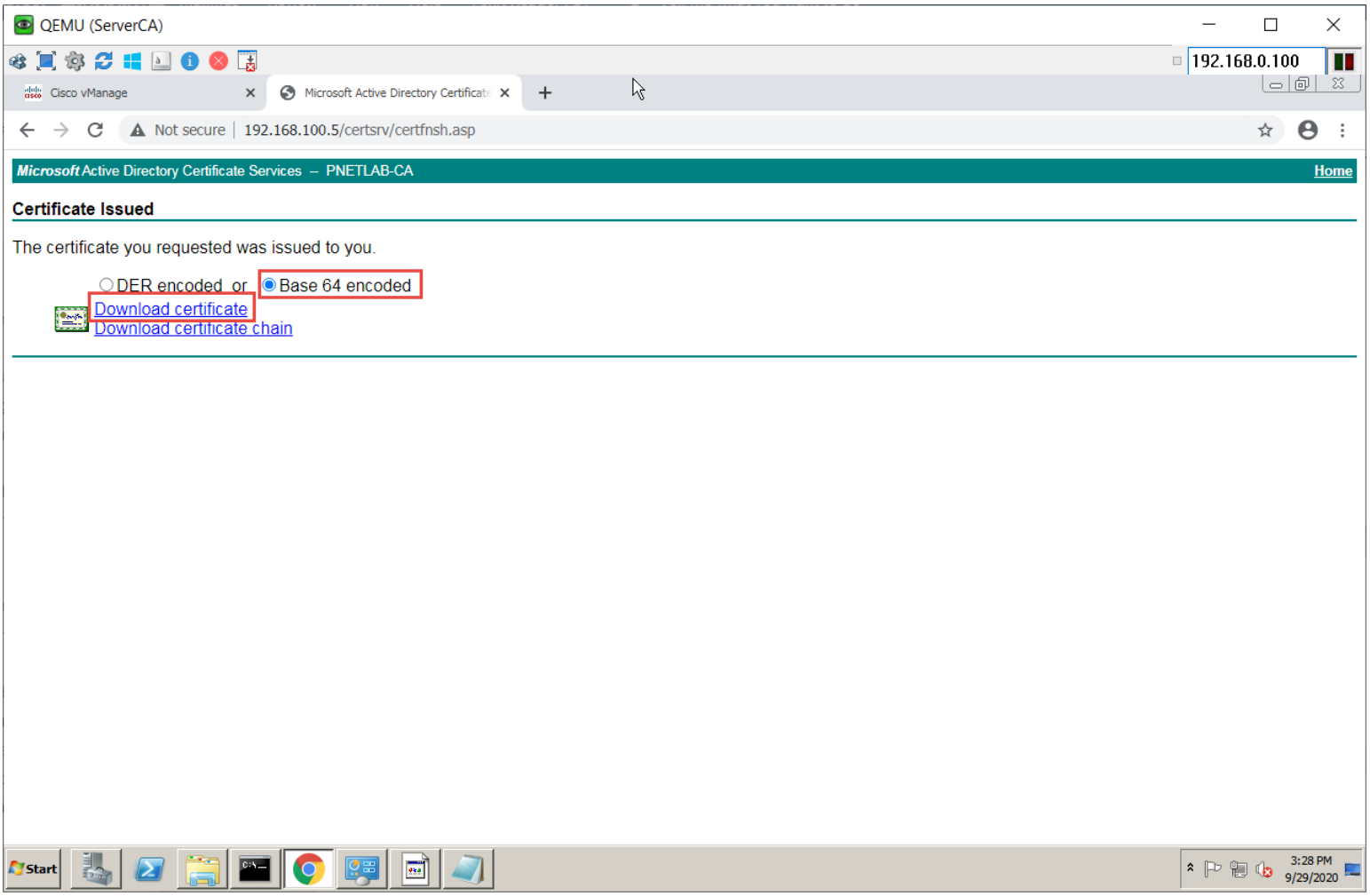
- Browser to http://192.168.100.5/certsrv
- Click "**Check on Pending Certificate Request**"



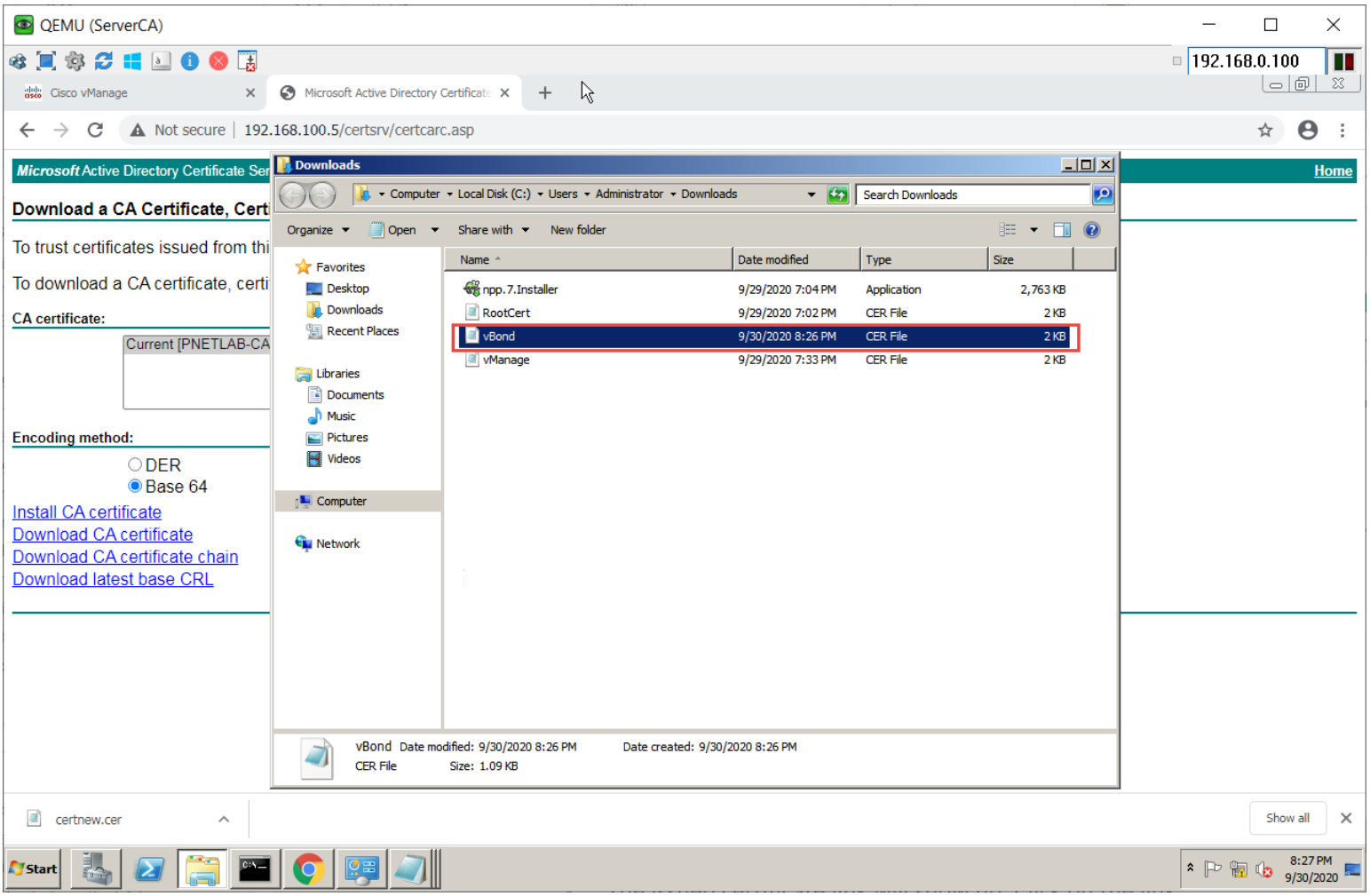
- The issued certificate link will show up. Click on the link



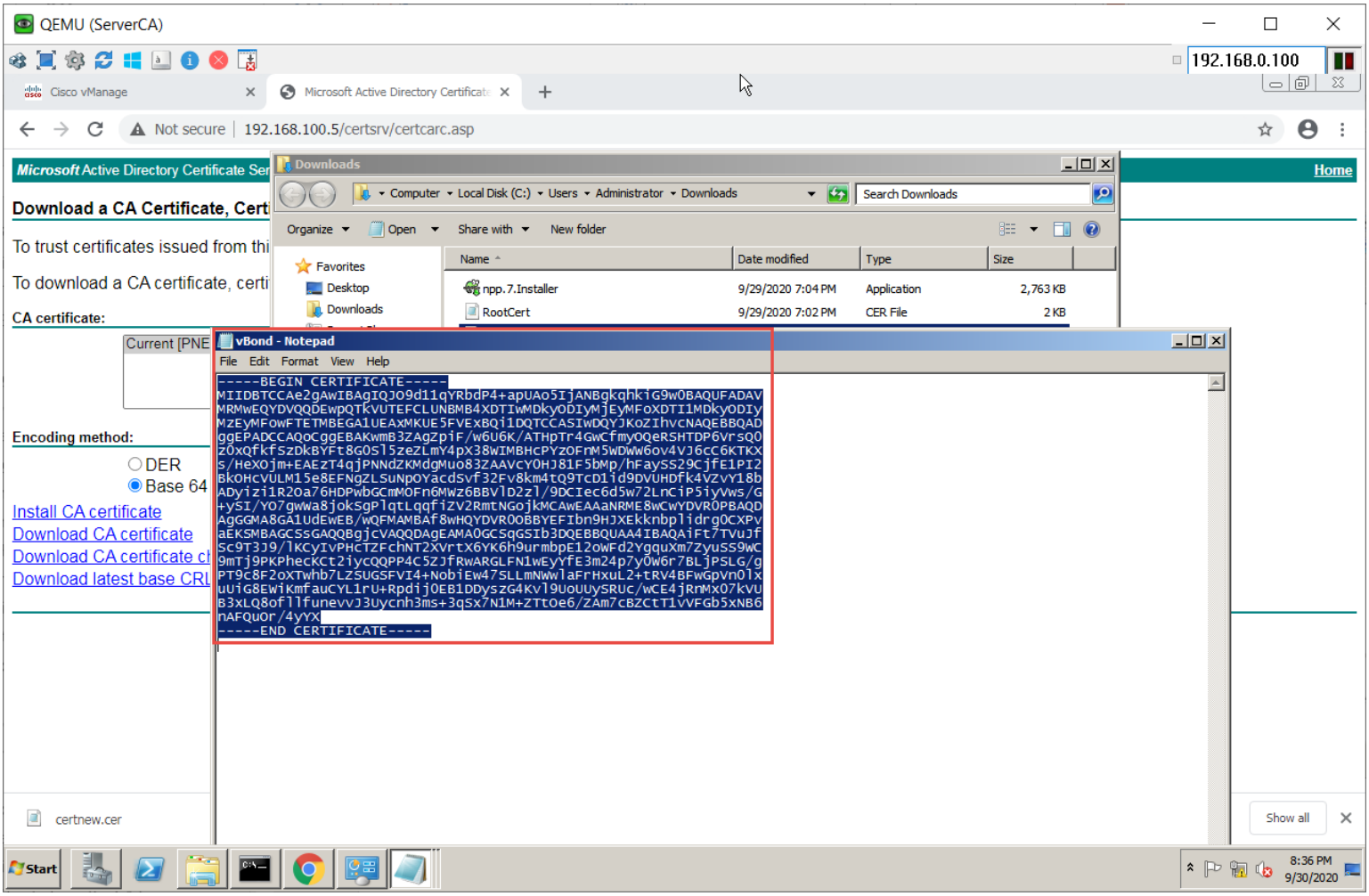
- Select "**Base 64**" and click "**Download**"



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

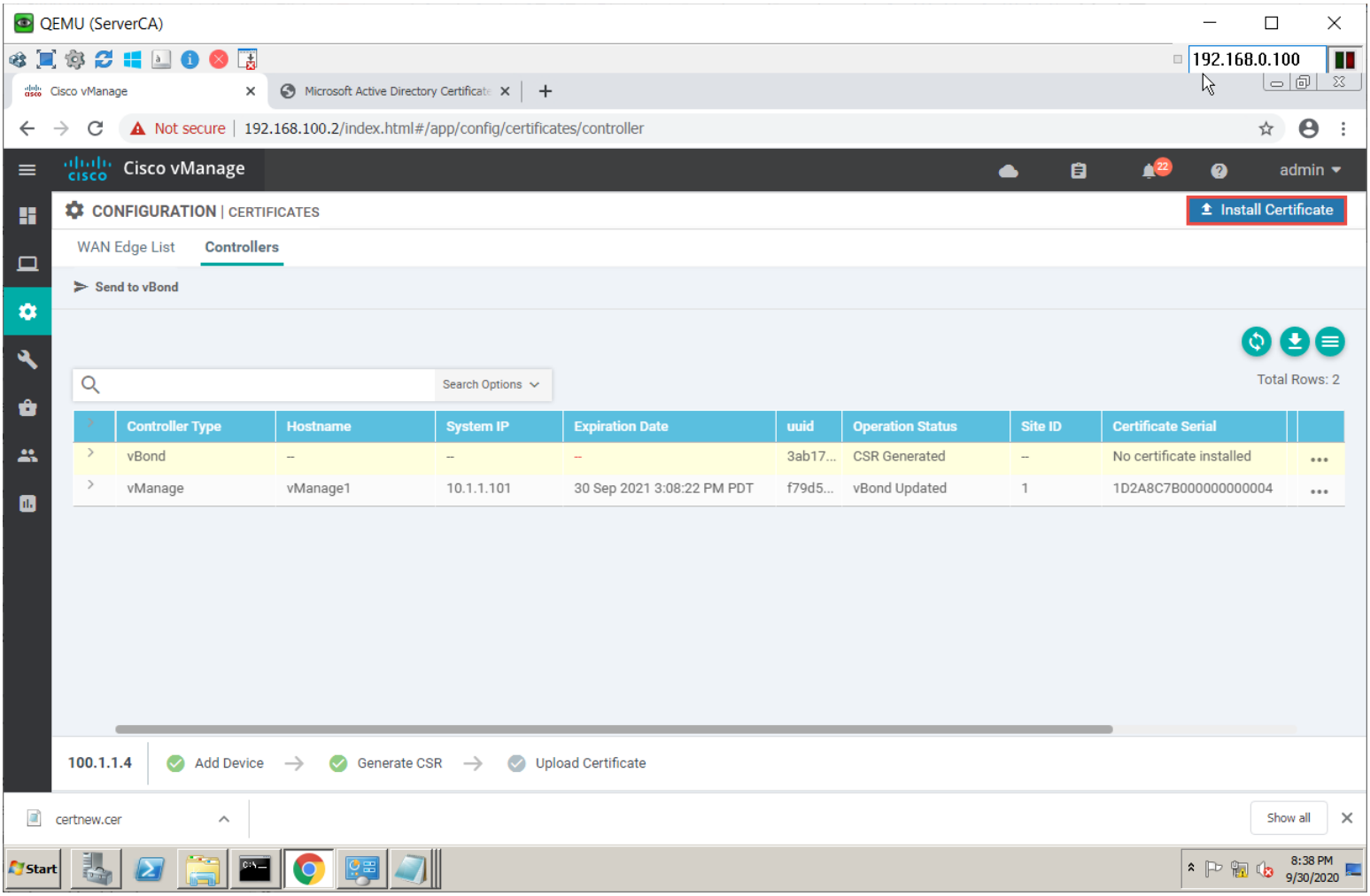


- Open the vBond.cer file using Notepad
- Copy using **CTRL-A and CTRL-C**

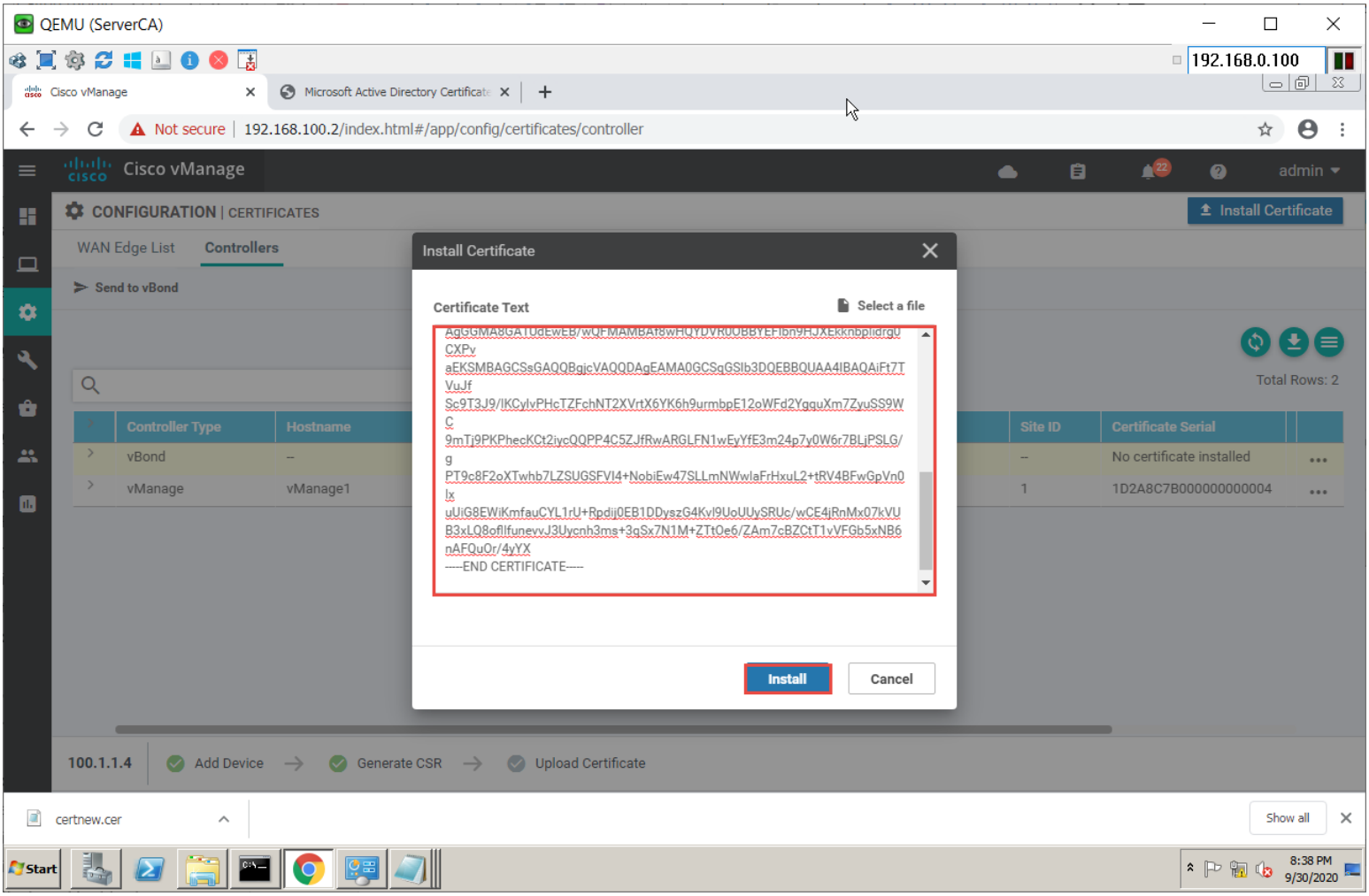

QEMU (ServerCA)
192.168.0.100
Cisco vManage
Microsoft Active Directory Certificate
Not secure | 192.168.100.5/certsrv/certcarc.asp
Microsoft Active Directory Certificate Ser
Home
Download a CA Certificate, Certi
To trust certificates issued from thi
To download a CA certificate, certi
CA certificate:
Current [PNE
Encoding method:
DER
Base 64
Install CA certificate
Download CA certificate
Download CA certificate cl
Download latest base CRL
Downloads
Computer ▸ Local Disk (C:) ▸ Users ▸ Administrator ▸ Downloads
Search Downloads
Organize
Open
Share with
New folder
Favorites
Desktop
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 - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDBTCCAe2gAwIBAgIQJO9d11qYRbdP4+apUAo5IjANBgkqhkiG9w0BAQUFADAV
MRMwEQYDVQQDEwpQTkVUTEFCLUNBMB4XDTIwMDkyODIyMjEyMFoXDTI1MDkyODIy
MzEyMFowFTETMBEGA1UEAxMKUE5FVExBQi1DQTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKwmB3ZAgZpiF/w6U6K/ATHpTr4GwCfmyOQeRSHTDP6VrsQO
zOxQfkfSzDkBYFt8GOSl5zeZLmY4pX38WIMBHcPYzOFnM5WDWW6ov4VJ6cC6KTKX
s/HeXOjm+EAEzT4qjPNNdZKMdgMuo83ZAAVcYOHJ81F5bMp/hFaySS29CjfE1PI2
BkOHcVULM15e8EFNgZLSuNpOYacdSvf32Fv8km4tQ9TcD1id9DvUHDfk4VZvY18b
ADyizi1R2Oa76HDPWbGCmMOFn6MWz6BBVlD2zl/9DCIec6d5w72LnCiP5iyVws/G
+ySI/YO7gwWa8jokSgPlqtLqqfiZV2RmtNGojkMCAwEAAaNRME8wCwYDVR0PBAQD
AgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFIbn9HJXEkknbplidrg0CXPv
aEKSMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBBQUAA4IBAQAiFt7TVuJf
Sc9T3J9/lKCyIvPHcTZFchNT2XVrtX6YK6h9urmbpE12oWFd2YgquXm7ZyuSS9WC
9mTj9PKPhecKCt2iycQQPP4C5ZJfRwARGLFN1wEyYfE3m24p7yOW6r7BLjPSLG/g
PT9c8F2oXTwhb7LzSUGSFVI4+NobiEw47SLLmNWwlaFrHxuL2+tRV4BFwGpVnOlx
uUiG8EWiKmfauCYL1rU+RpdijOEB1DDyszG4Kvl9UoUUySRUc/wCE4jRnMxO7kVu
B3xLQ8ofllfunevvJ3Uycnh3ms+3qSx7N1M+ZTtOe6/ZAm7cBZCtT1vVFGb5xNB6
nAFQuOr/4yYX
-----END CERTIFICATE-----
certnew.cer
Show all
Start
8:36 PM
9/30/2020

Task 6- Installing the Identity Certificate for vManage

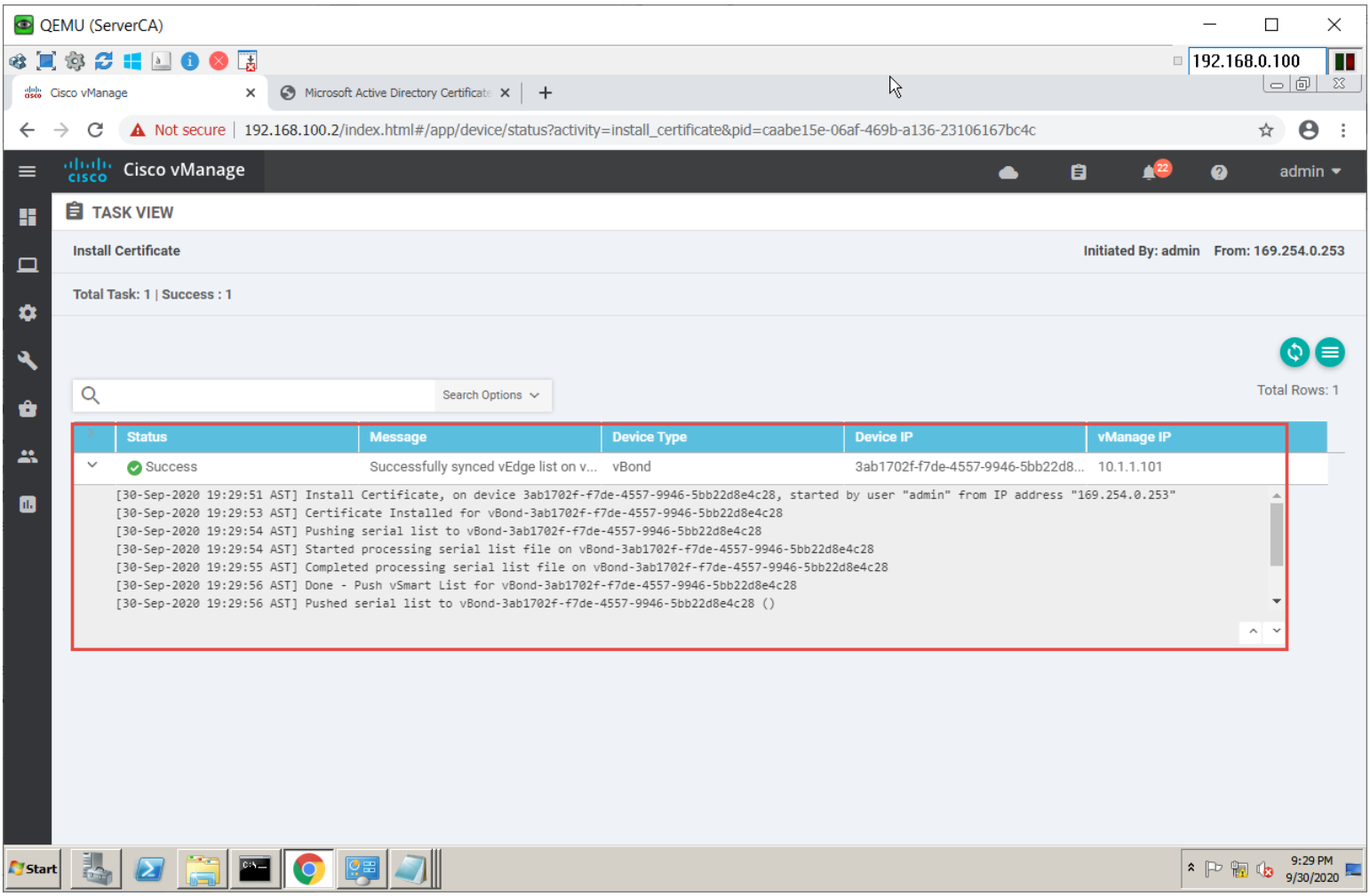
- In vManage, Navigate to **Configuration** ➔ **Certificates** ➔ **Controllers**
- Click on the **"Install Certificate"** button at the top right corner



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



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


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=caabe15e-06af-469b-a136-23106167bc4c
Cisco vManage
admin
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...
vBond
3ab1702f-f7de-4557-9946-5bb22d8...
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:
  - Host-name : vSmart1
  - Organization: **"viptela sdwan"**
  - System-IP: `100.1.1.13`
  - Site ID: 1
  - vbond Address: `100.1.1.4`
  - 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:
  - vpn 0
    - Interface Eth1
    - IP Address: 100.1.1.3/24
    - Tunnel Interface
    - Tunnel Services (All, NetConf, SSHD)
    - Default Route: 100.1.1.1
  - vpn 512
    - Interface eth0
    - IP Address: 192.168.100.3/24

vSmart

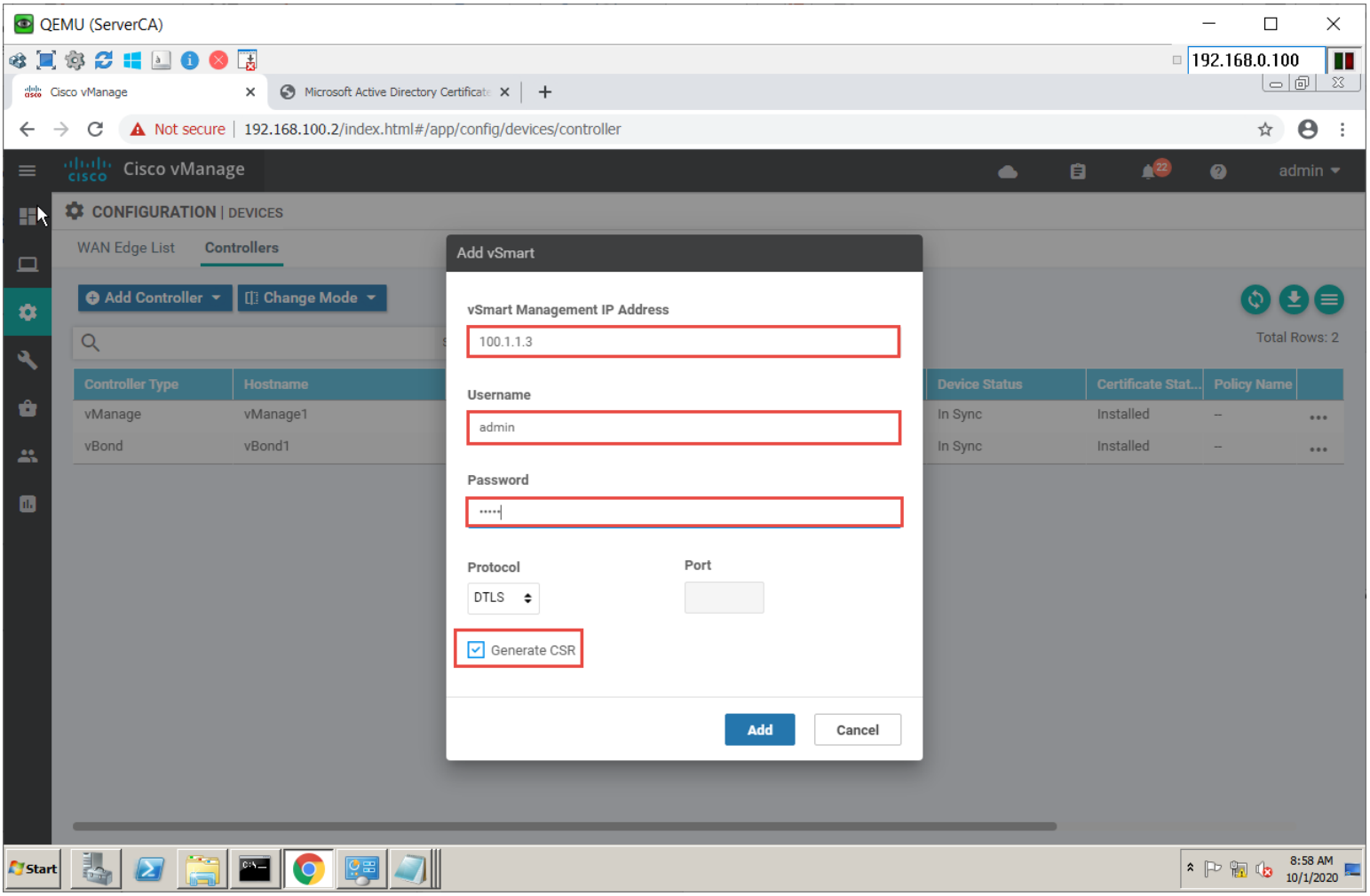
```
config
!
vpn 0
no interface eth0
interface eth1
ip address 100.1.1.3/24
tunnel-interface
```

```
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

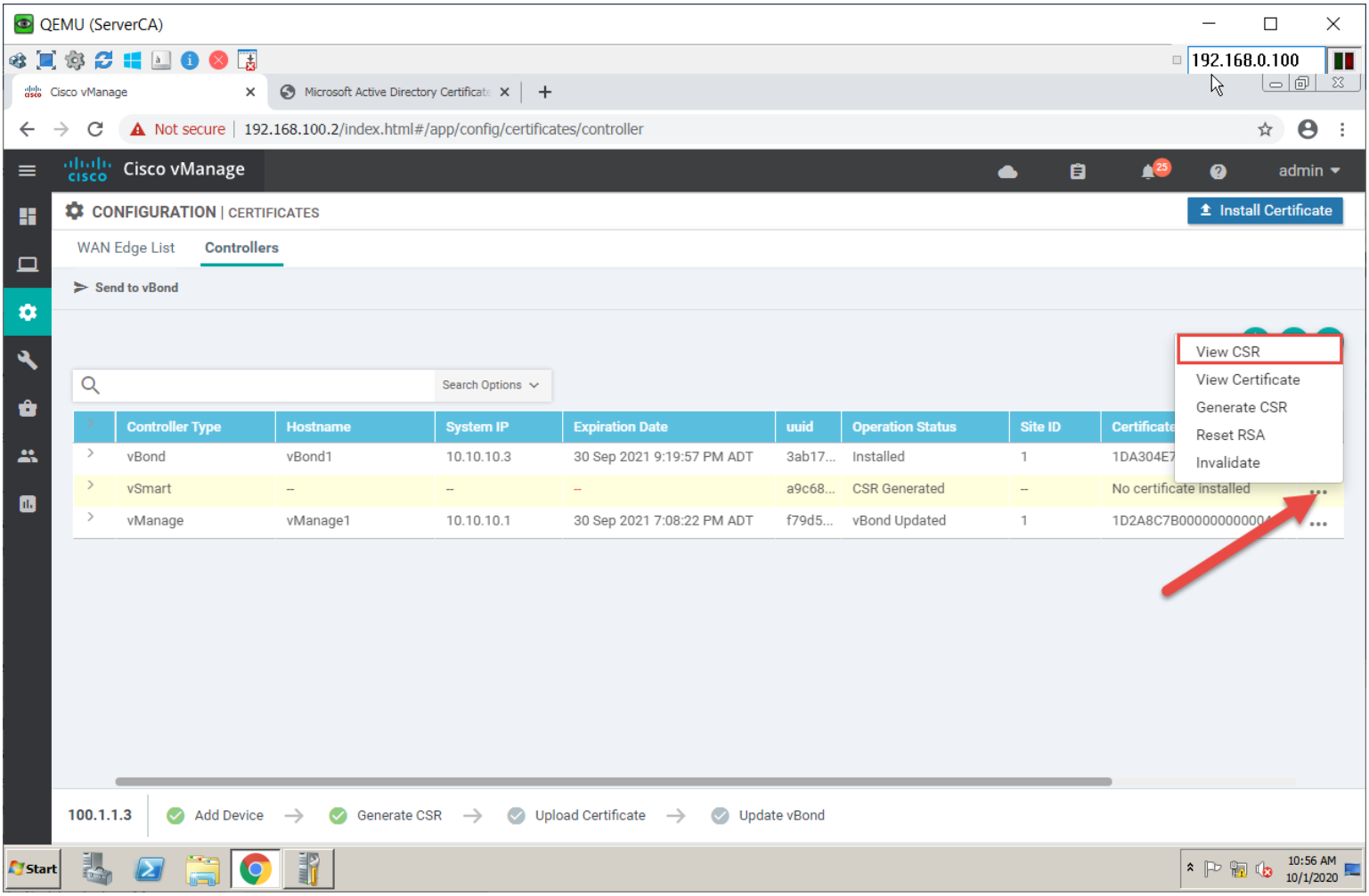
Task 1- Add vSmart to vManage

- 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**

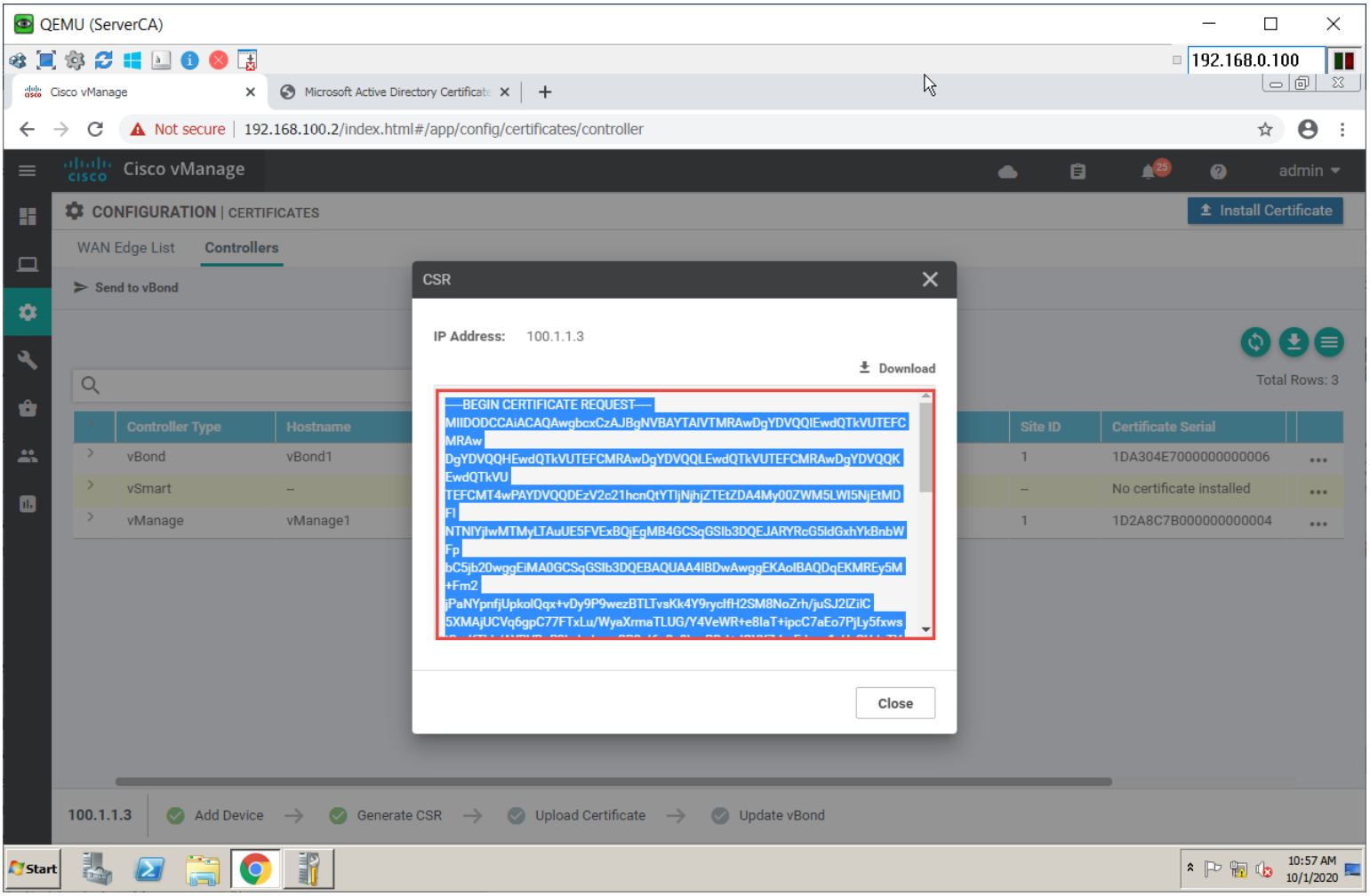


Task 2 – View the generated CSR for vSmart and Copy it

- Navigate to Configuration ➔ **Certificates** ➔ **Controllers** ➔ **vSmart** ➔ **View CSR**

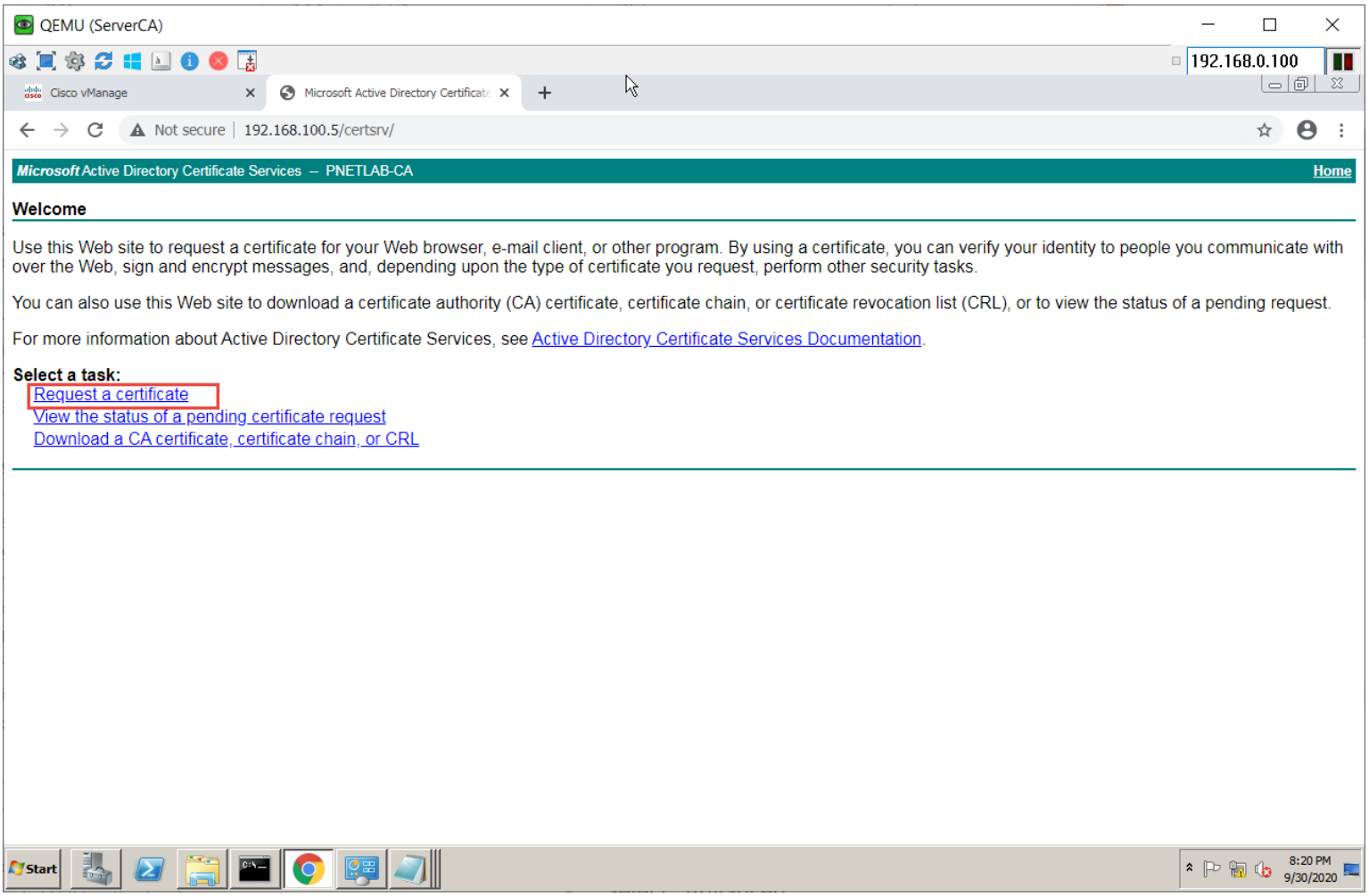


- It will open a window with CSR. Copy by using CTRL-A and CTRL-C

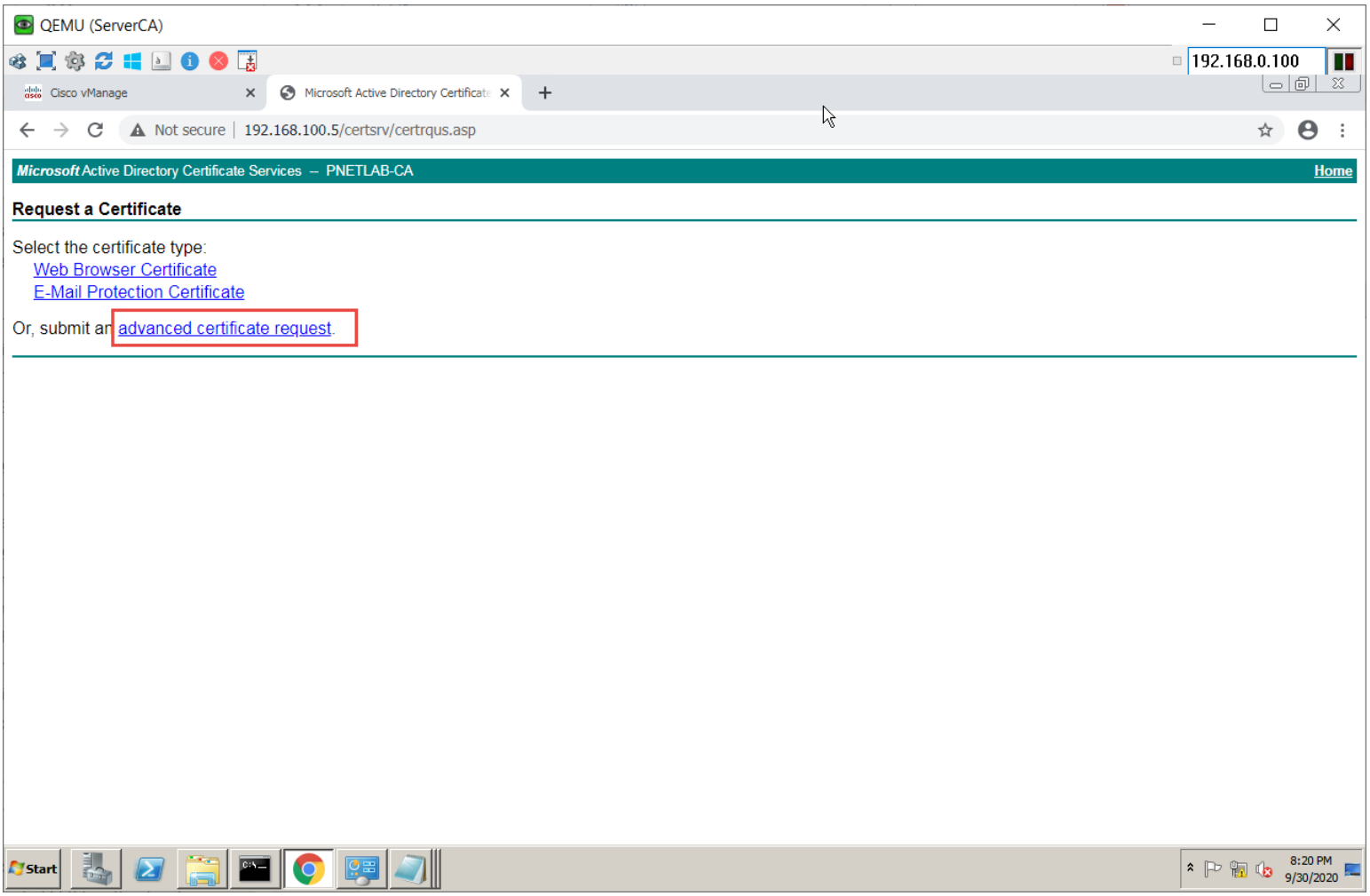

QEMU (ServerCA)
192.168.0.100
Cisco vManage
Microsoft Active Directory Certificate
Not secure | 192.168.100.2/index.html#/app/config/certificates/controller
Cisco vManage
admin
CONFIGURATION | CERTIFICATES
Install Certificate
WAN Edge List
Controllers
Send to vBond
Total Rows: 3
Controller Type
Hostname
Site ID
Certificate Serial
vBond
vBond1
1
1DA304E7000000000006
vSmart
--
No certificate installed
vManage
vManage1
1
1D2A8C7B000000000004
CSR
IP Address: 100.1.1.3
Download
-----BEGIN CERTIFICATE REQUEST-----
MIIDODCCAiACAQAwgbcxCzAJBgNVBAYTAIVTMRAwDgYDVQQIEwdQTkVUTEFC
MRAw
DgYDVQQHEwdQTkVUTEFCMRAwDgYDVQQLEwdQTkVUTEFCMRAwDgYDVQQK
EwdQTkVU
TEFCMT4wPAYDVQQDEzV2c21hcnQtYTIjNjhjZTEtZDA4My00ZWM5LWI5NjEtMD
FI
NTNlYjIwMTMyLTAuUE5FVExBQjEgMB4GCSqGSIb3DQEJARYRcG5ldGxhYkBnbW
Fp
bC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDqEKMREy5M
+Fm2
jPaNYpnfjUpkolQqx+vDy9P9wezBTLTvsKk4Y9ryclfH2SM8NoZrh/juSJ2IZiiC
5XMAjUCVq6gpC77FTxLu/WyaXrmaTLUG/Y4VeWR+e8laT+ipcC7aEo7PjLy5fxws
Close
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

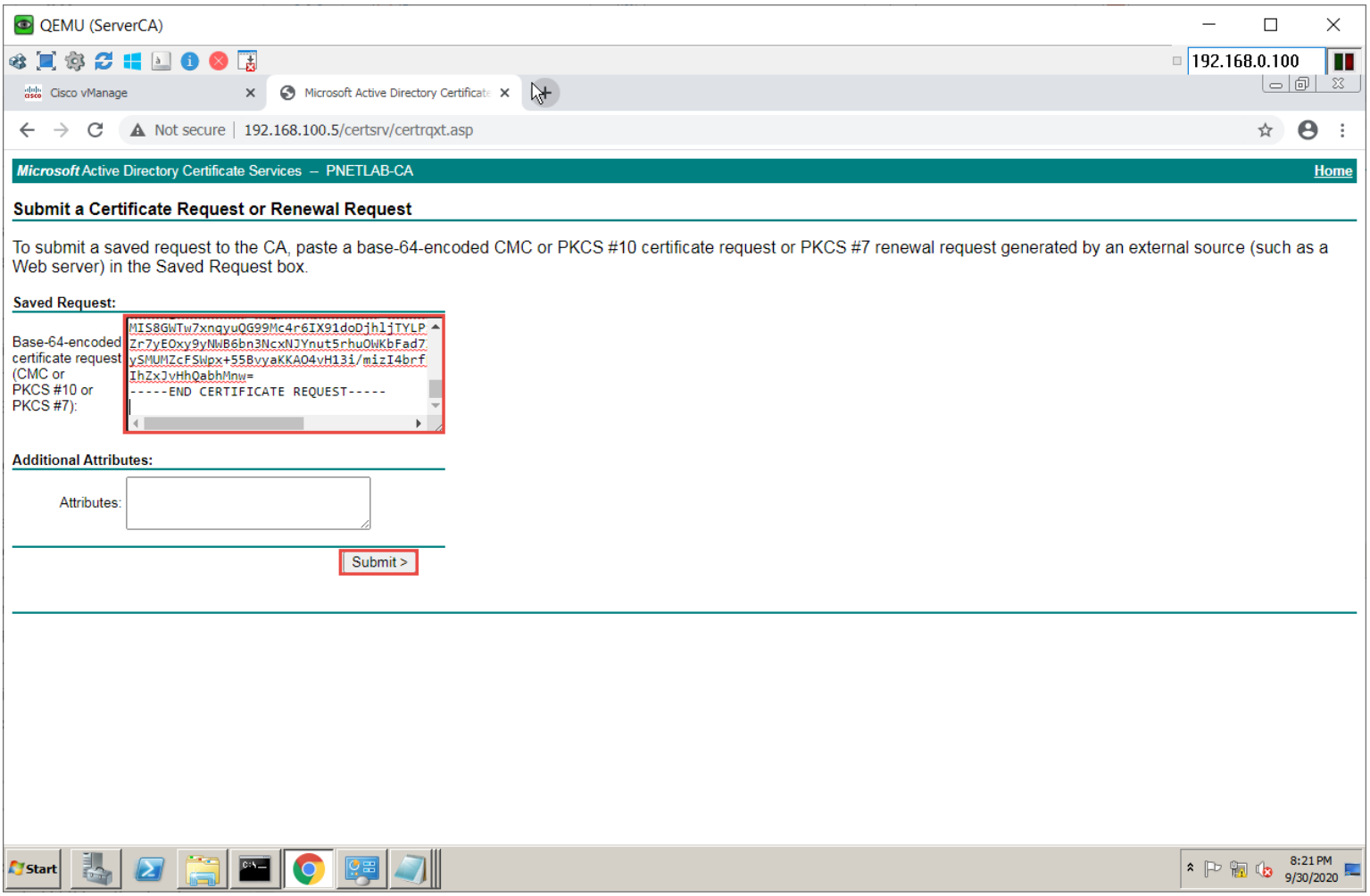
- Browser to http://192.168.100.5/certsrv
- Click "**Request a Certificate**"



- Select "**Advanced**"

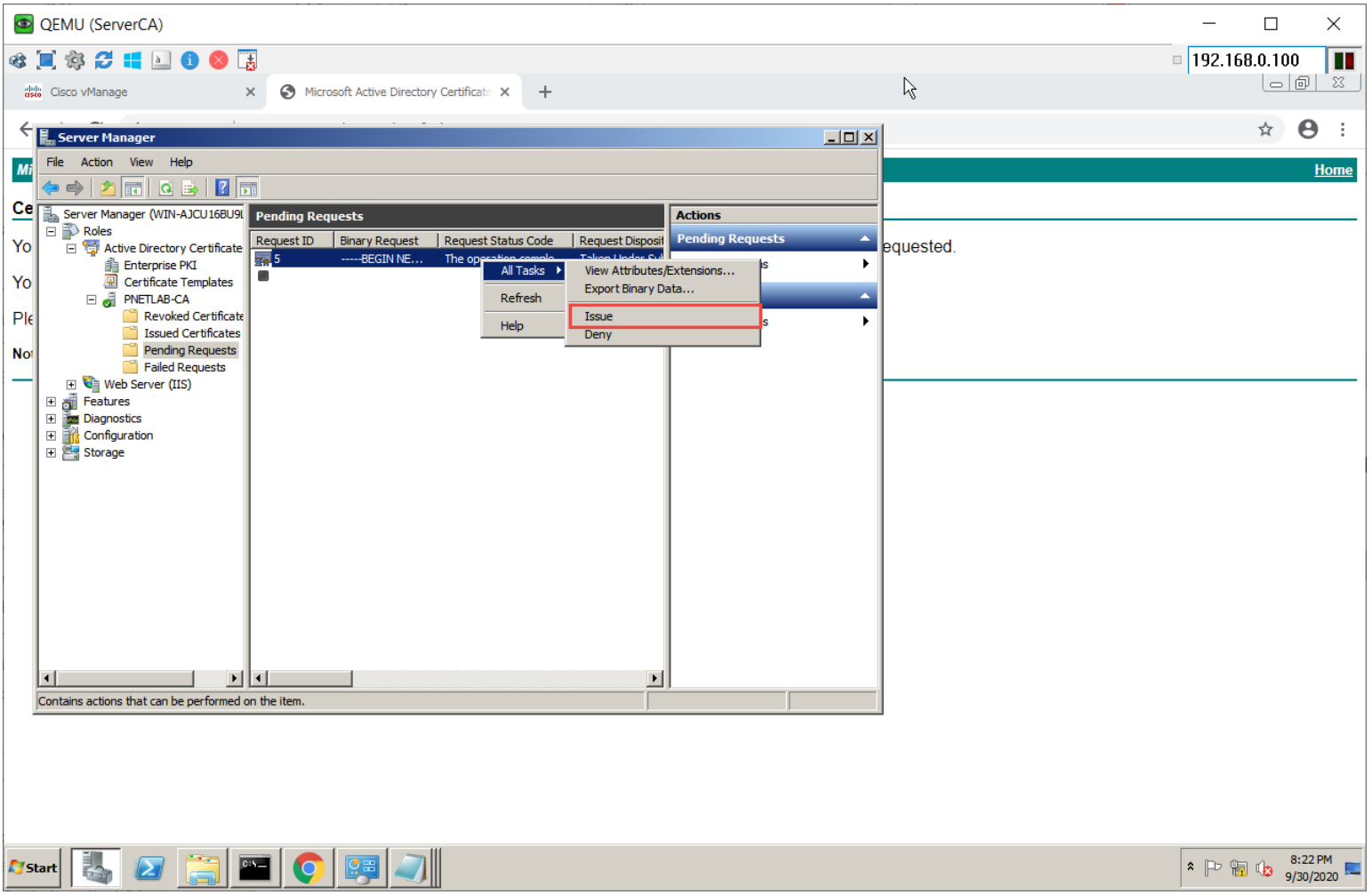


- Paste the CSR in the box by using **CTRL-V** and click Submit



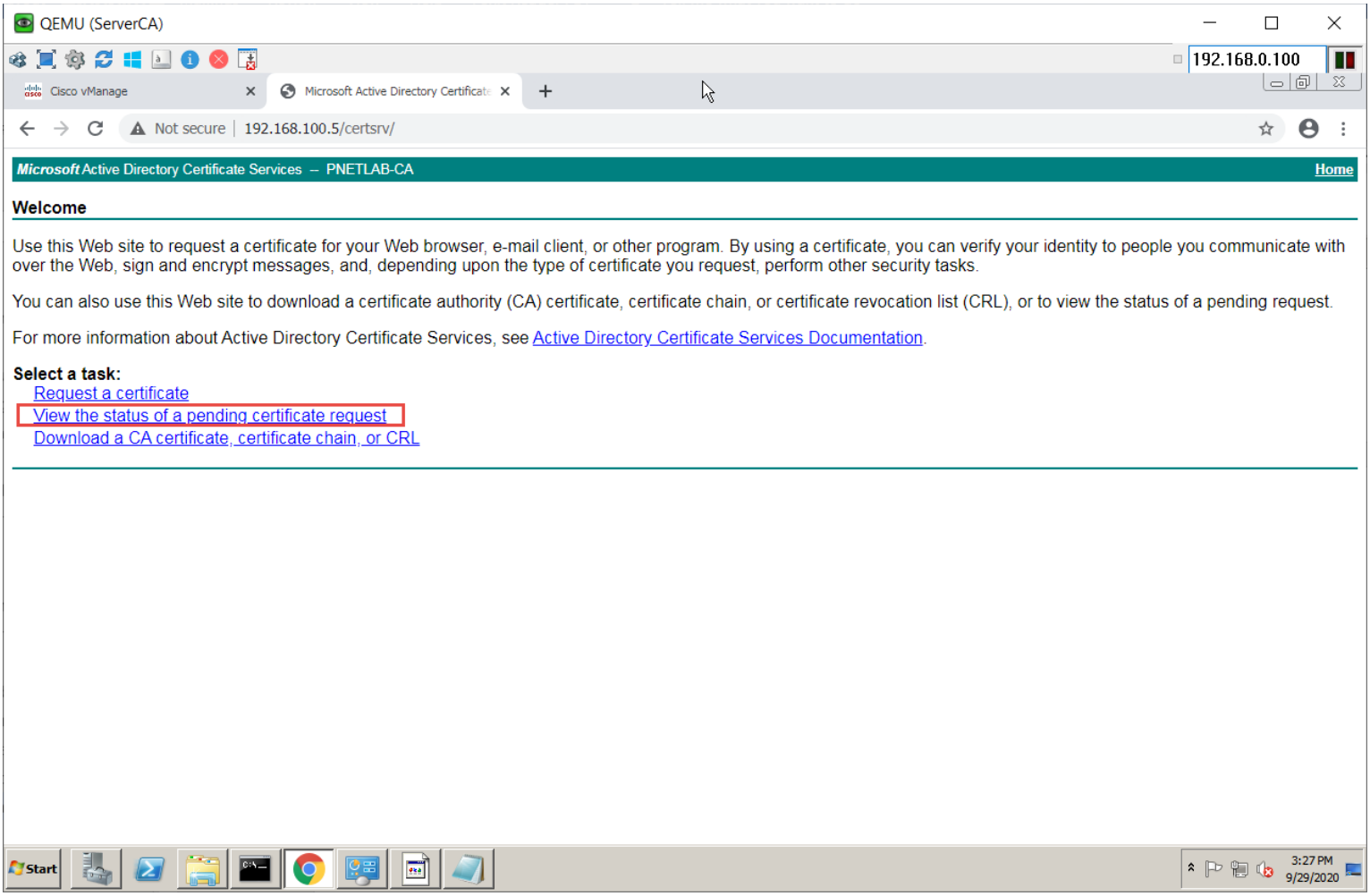
Task 4 – Issue the Certificate from the CA Server

- Open **Server Manager ➔ Roles ➔ Active Directory Certificate Server ➔ PNETLAB-CA ➔ Pending Request**.
- Right-click the **request ➔ more action ➔** all tasks and click "**Issue**"

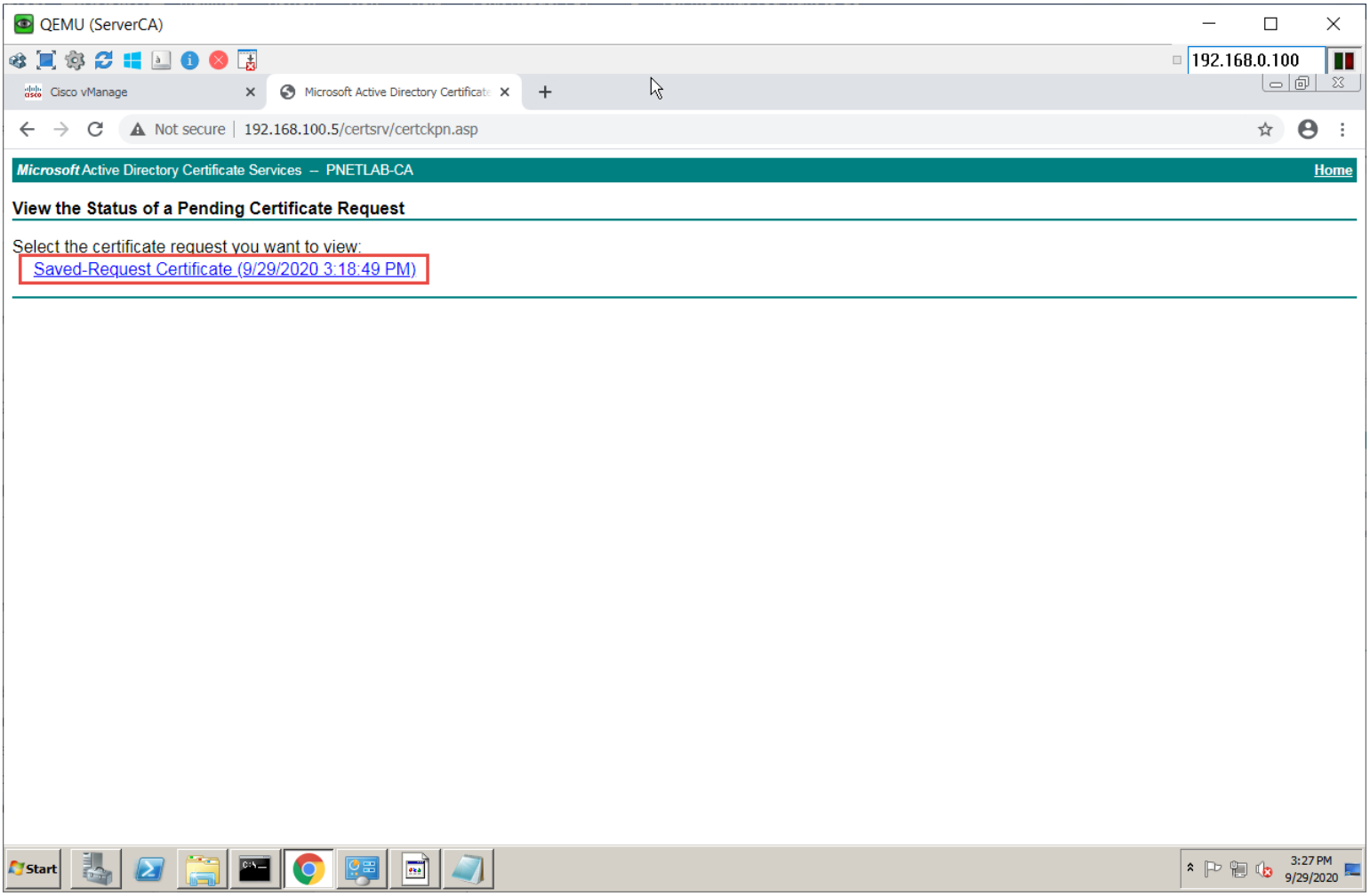


Task 5- Downloading the Issued Certificate

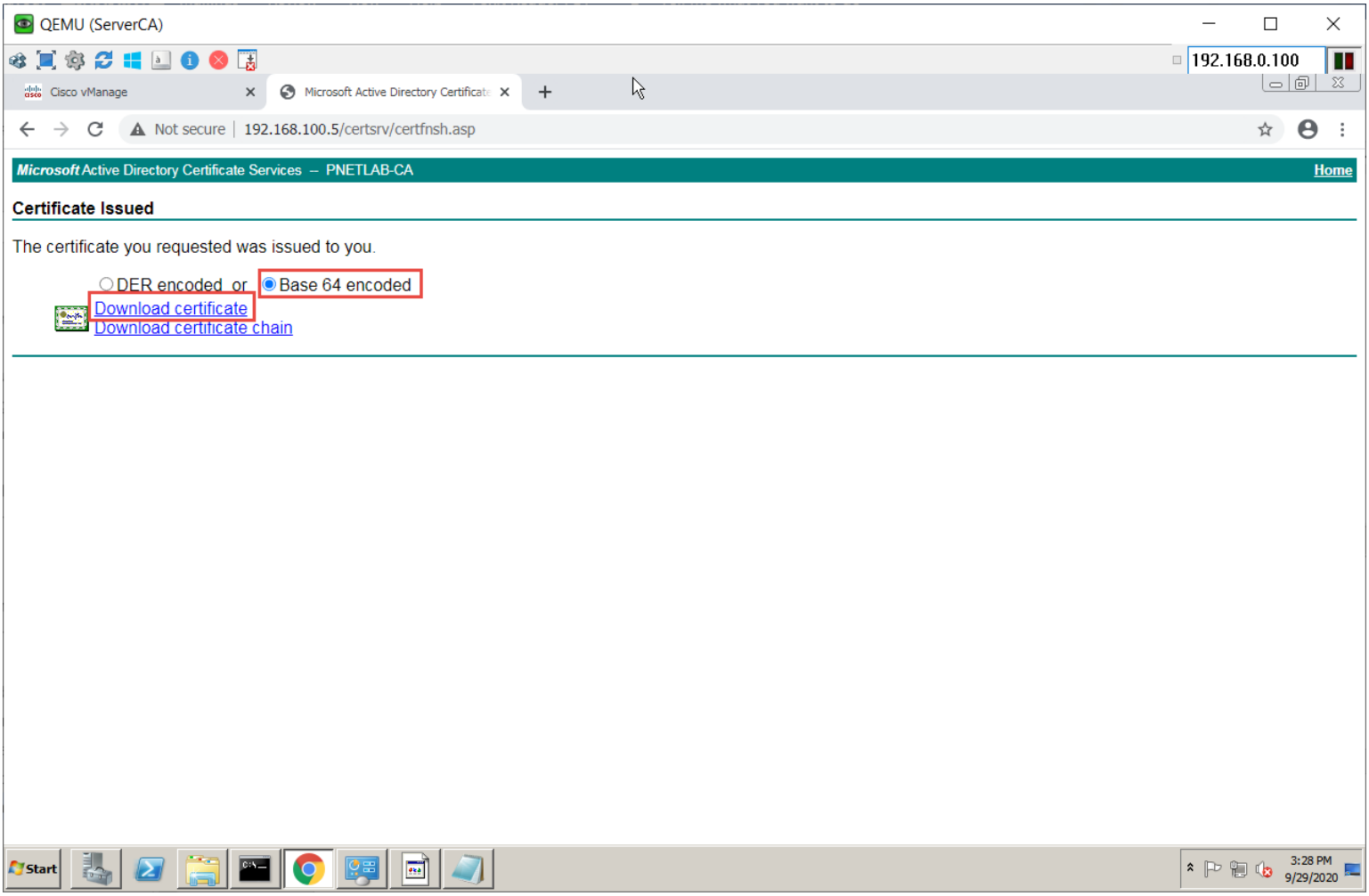
- Browser to http://192.168.100.5/certsrv
- Click "**Check on Pending Certificate Request**"



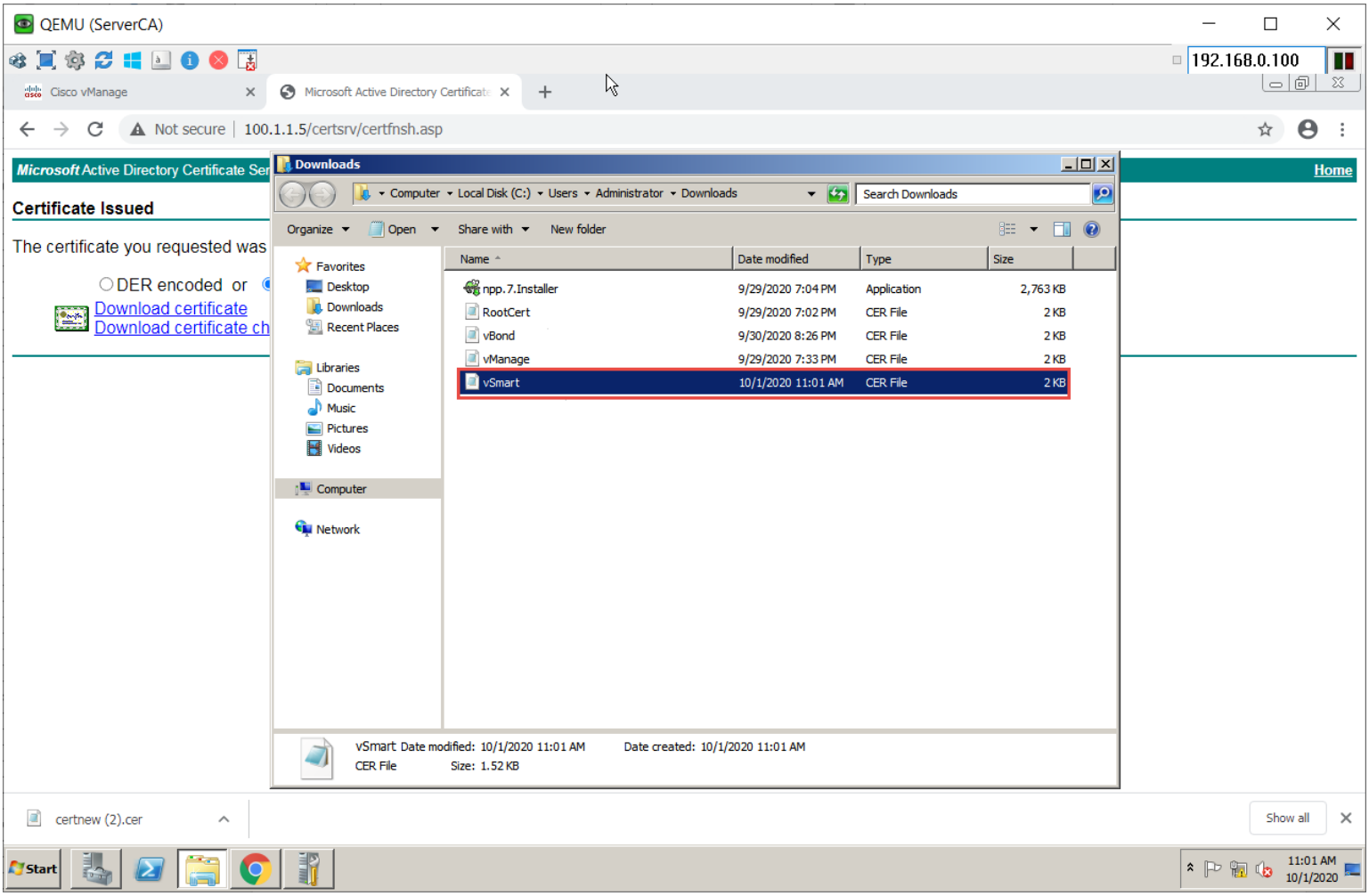
- The issued certificate link will show up. Click on the link



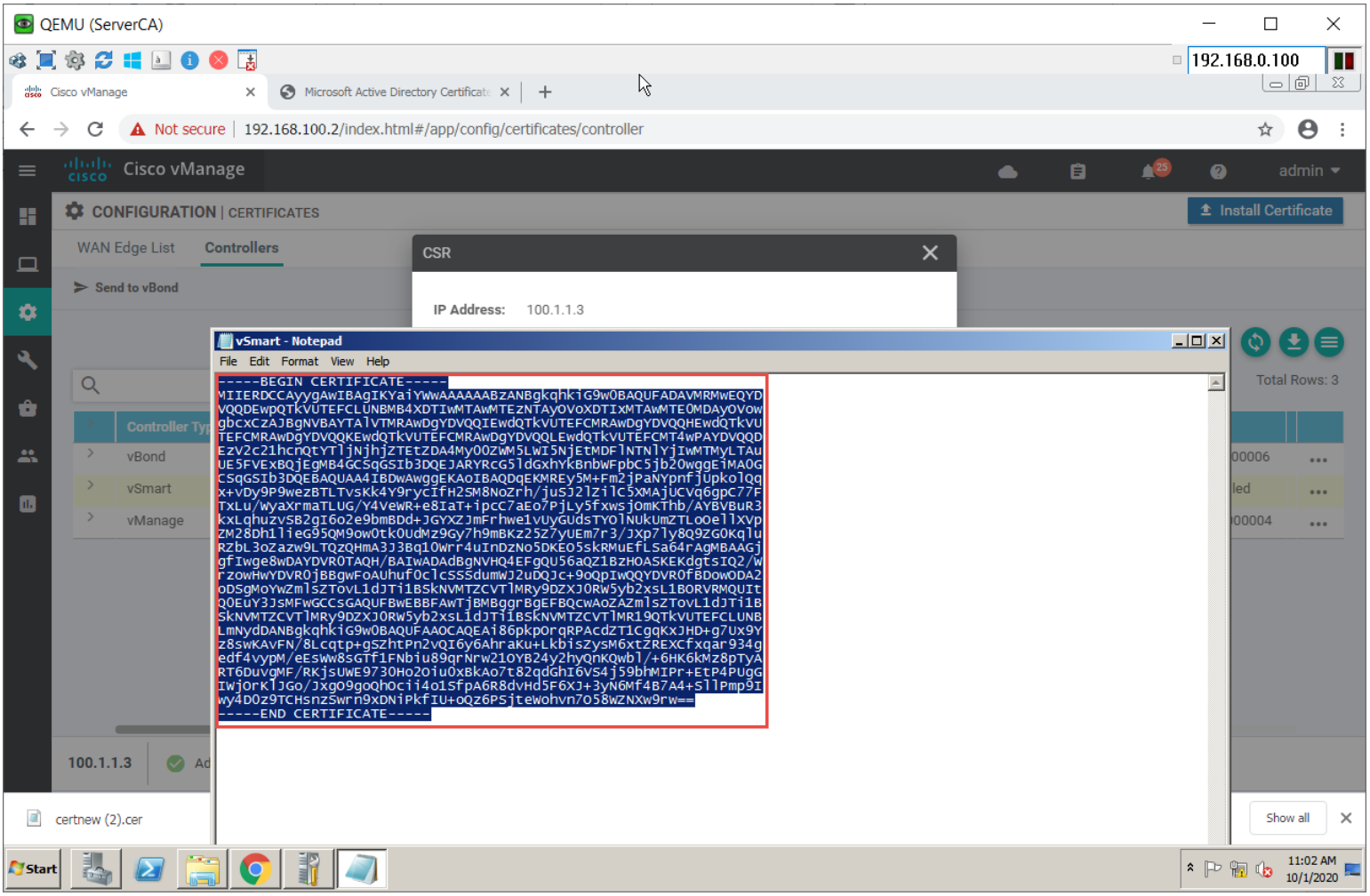
- Select "**Base 64**" and click "**Download**"



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

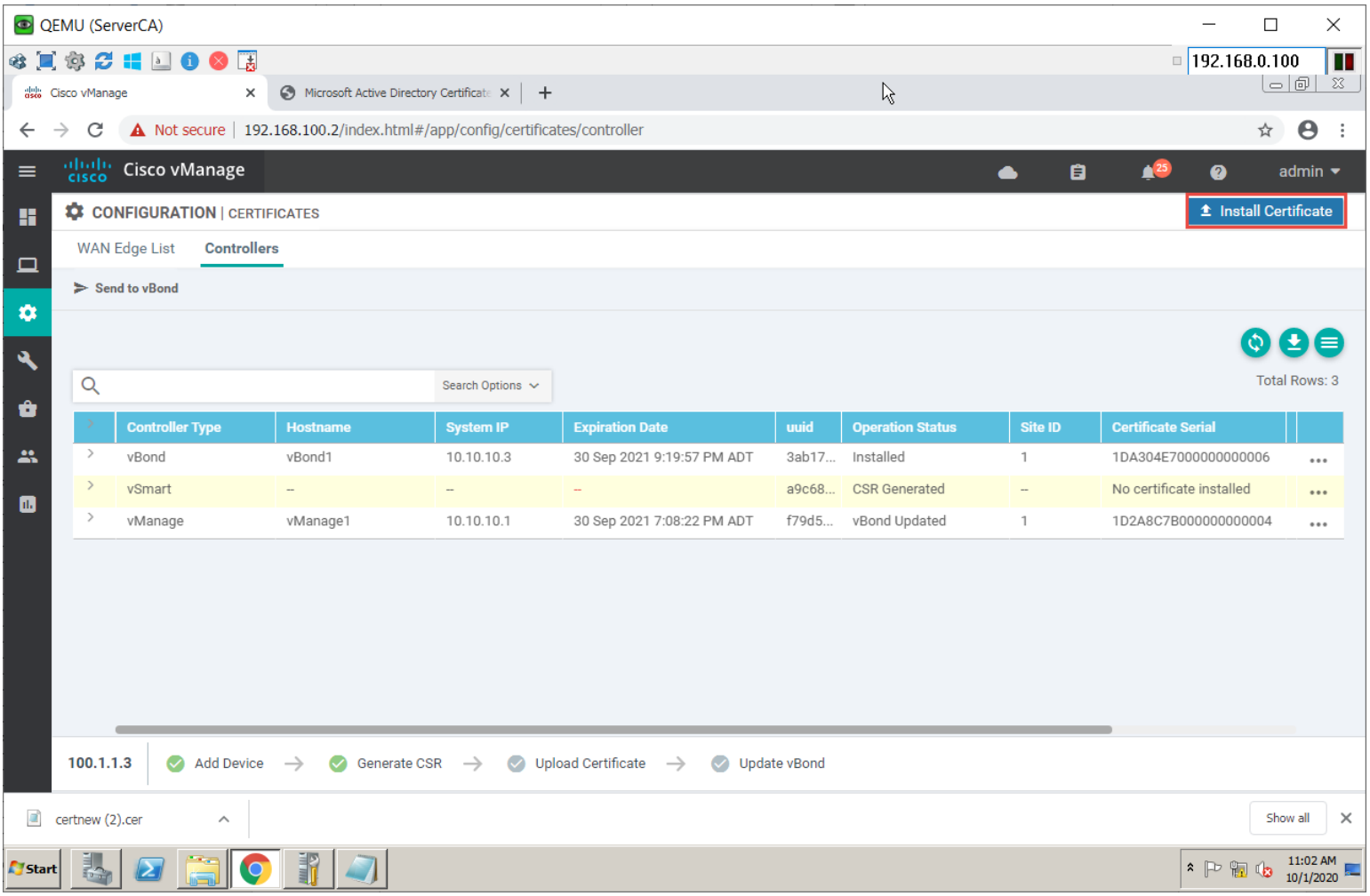


- Open the vBond.cer file using Notepad
- Copy using **CTRL-A and CTRL-C**

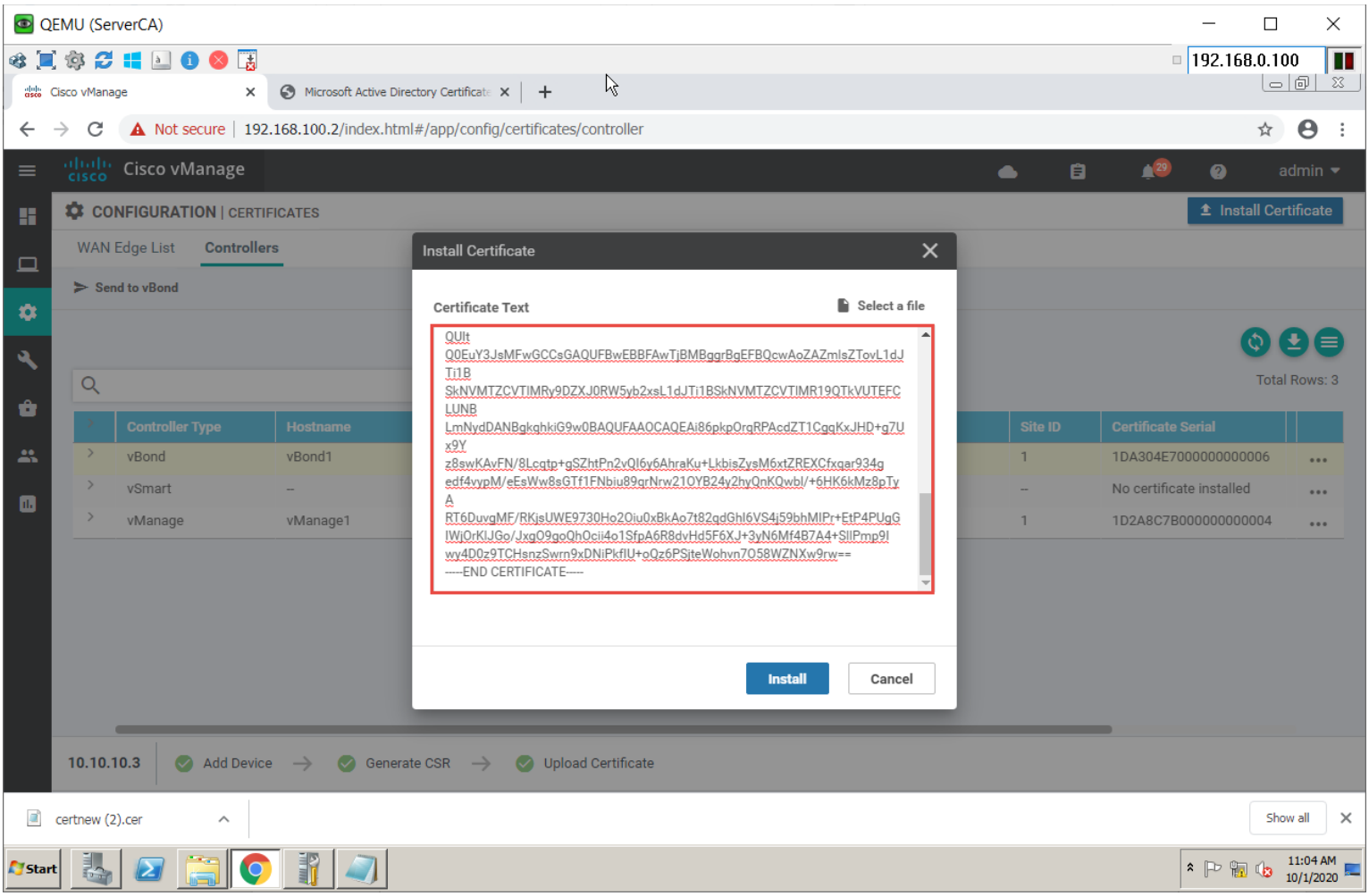

QEMU (ServerCA)
192.168.0.100
Cisco vManage
Microsoft Active Directory Certificate
Not secure
192.168.100.2/index.html#/app/config/certificates/controller
Cisco vManage
admin
CONFIGURATION | CERTIFICATES
Install Certificate
WAN Edge List
Controllers
Send to vBond
CSR
IP Address: 100.1.1.3
vSmart - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIERDCCAyygAwIBAgIKYaiYwwAAAAAABzANBgkqhkiG9w0BAQUFADAVMRMwEQYD
VQQDEwpQTkVUTEFCLUNBMB4XDTIwMTAwMTEzNTAyOVoXDTIxMTAwMTE0MDAyOVow
gbcxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdQTkVUTEFCMRAwDgYDVQQHEwdQTkVU
TEFCMRAwDgYDVQQKEwdQTkVUTEFCMRAwDgYDVQQLEwdQTkVUTEFCMT4wPAYDVQQD
EzV2c21hcnQtYTljNjhjZTEtZDA4MyO0ZWM5LWI5NjEtMDFlNTNlYjIwMTMyLTAu
UE5FVExBQjEgMB4GCSqGSIb3DQEJARYRcG5ldGxhYkBnbWFpbC5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDqEKMREy5M+Fm2jPaNYpnfjUpkolQg
x+vDy9P9wezBTLTvsKk4Y9rycIfH2SM8NoZrh/jusJ2lZilC5XMAjUCVq6gpC77F
TXLu/WyaXrmaTLUG/Y4VeWR+e8IaT+ipcC7aEo7PjLy5fxwsjOmKThb/AYBVBuR3
kxLqhuzvSB2gI6o2e9bmBDd+JGYXZJmFrhwe1vUyGUdsTYOlNUkUmZTLoOellXVp
ZM28Dh1lieG95QM9owOtkOUdMz9Gy7h9mBKz25Z7yUEm7r3/JXp7ly8Q9ZG0Kqlu
RZbL3oZazw9LTQzQHmA3J3Bq1OWrr4uInDzNo5DKEO5skRMuEfLSa64rAgMBAAGj
gfIwge8wDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU56aQZ1BzHOASKEKdgtsIQ2/W
rzowHwYDVR0jBBgwFoAUhuf0clcSS5dumWJ2uDQJc+9oQpIwQQYDVR0fBDowODA2
oDSgMoYwZmlsZTovL1dJTi1BSkNVMTZCVTlMRy9DZXJ0RW5yb2xsL1BORVRMQUIt
QOEuY3JsMFwGCCsGAQUFBwEBBFAwTjBMBggrBgEFBQcwAoZAZmlsZTovL1dJTi1B
SkNVMTZCVTlMRy9DZXJ0RW5yb2xsL1dJTi1BSkNVMTZCVTlMR19QTkVUTEFCLUNB
LmNydDANBgkqhkiG9w0BAQUFAAOCAQEAi86pkpOrqRPAcdZTICgqKxJHD+g7Ux9Y
z8swKAvFN/8Lcqtp+gSzhtPn2vQI6y6AhraKu+LkbisZysM6xtZREXCfxqar934g
edf4vypM/eEsWw8sGTf1FNbiu89qrNrw21OYB24y2hyQnKQwbl/+6HK6kMz8pTyA
RT6DuvgMF/RKjSUwE973OHo2Oiu0xBkAo7t82qdGhI6VS4j59bhMIPr+EtP4PUgG
IwjOrKlJGo/JxgO9goQhOcii4o1SfpA6R8dvHd5F6XJ+3yN6Mf4B7A4+SllPmp9I
wy4DOz9TCHsnz5wrn9xDNiPkfIU+oQz6PSjteWohvn7O58WZNXw9rw==
-----END CERTIFICATE-----
Total Rows: 3
100.1.1.3
certnew (2).cer
Show all
Start
11:02 AM
10/1/2020

Task 6- Installing the Identity Certificate for vManage

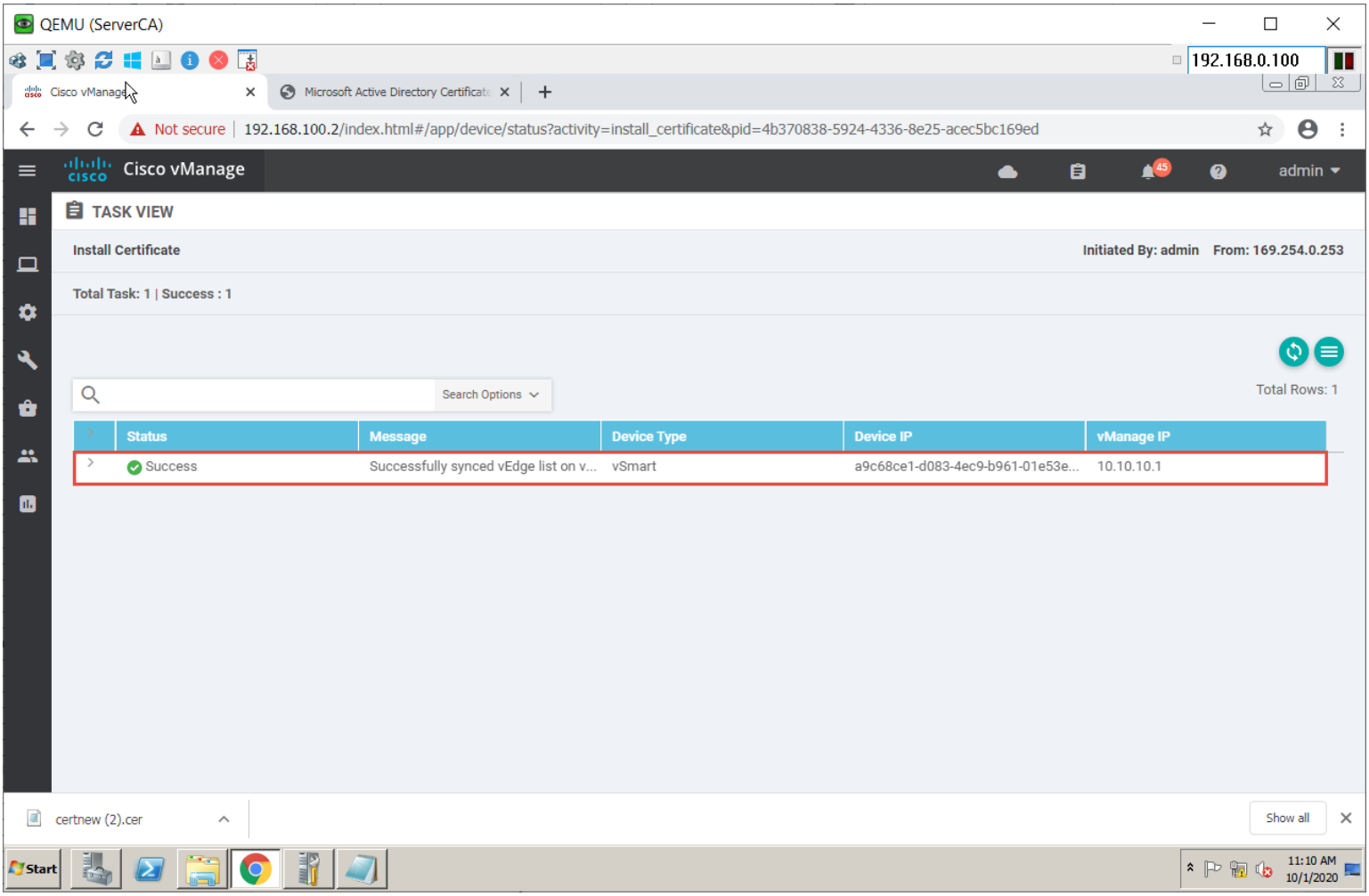
- In vManage, Navigate to **Configuration ➔ Certificates ➔ Controllers**
- Click on the **"Install Certificate"** button at the top right corner



- Paste the Certificate (CTRL-V).



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


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-acec5bc169ed
Cisco vManage
admin
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

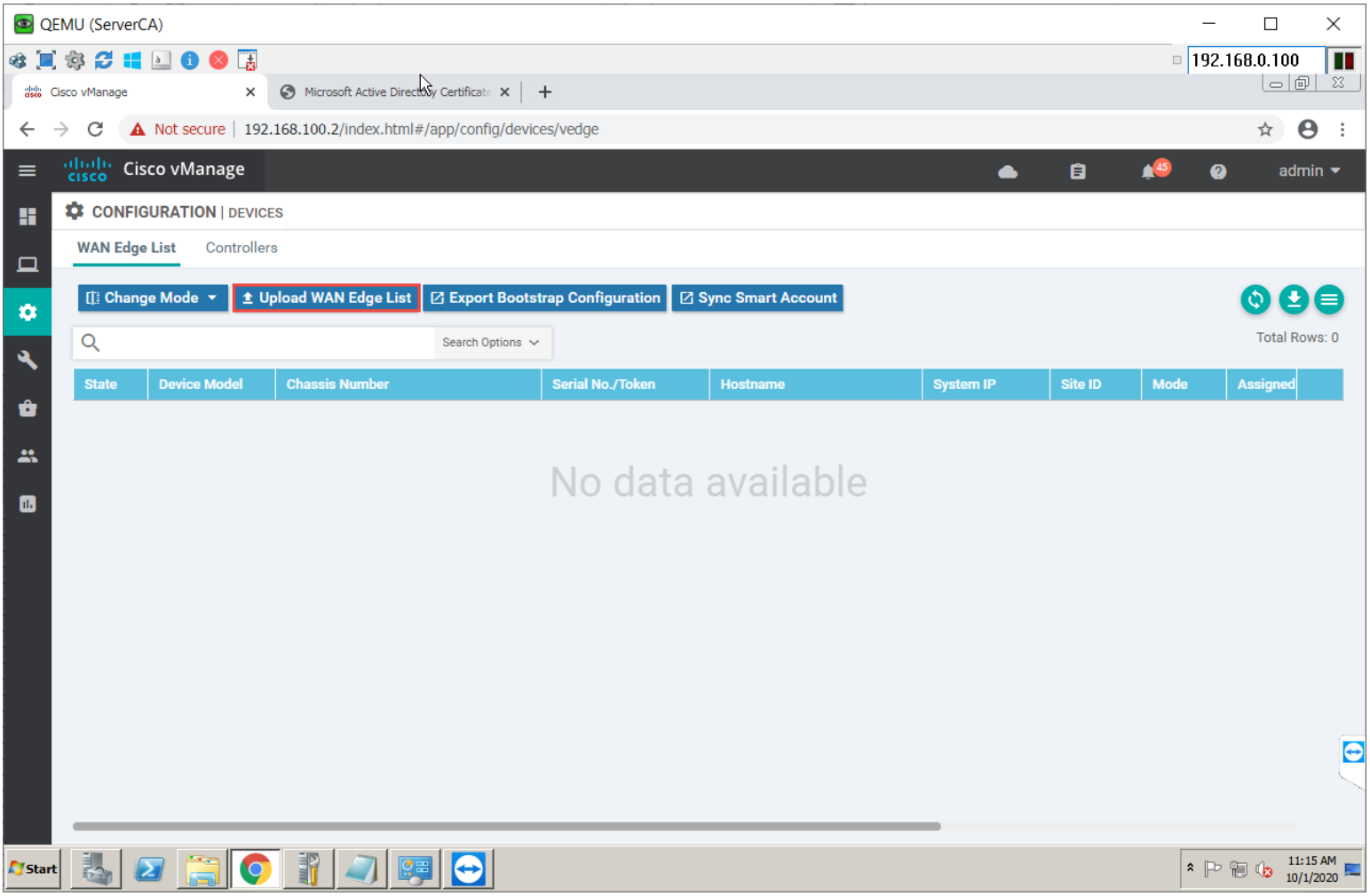
Lab 9 – initializing vEdge – CLI

Note:

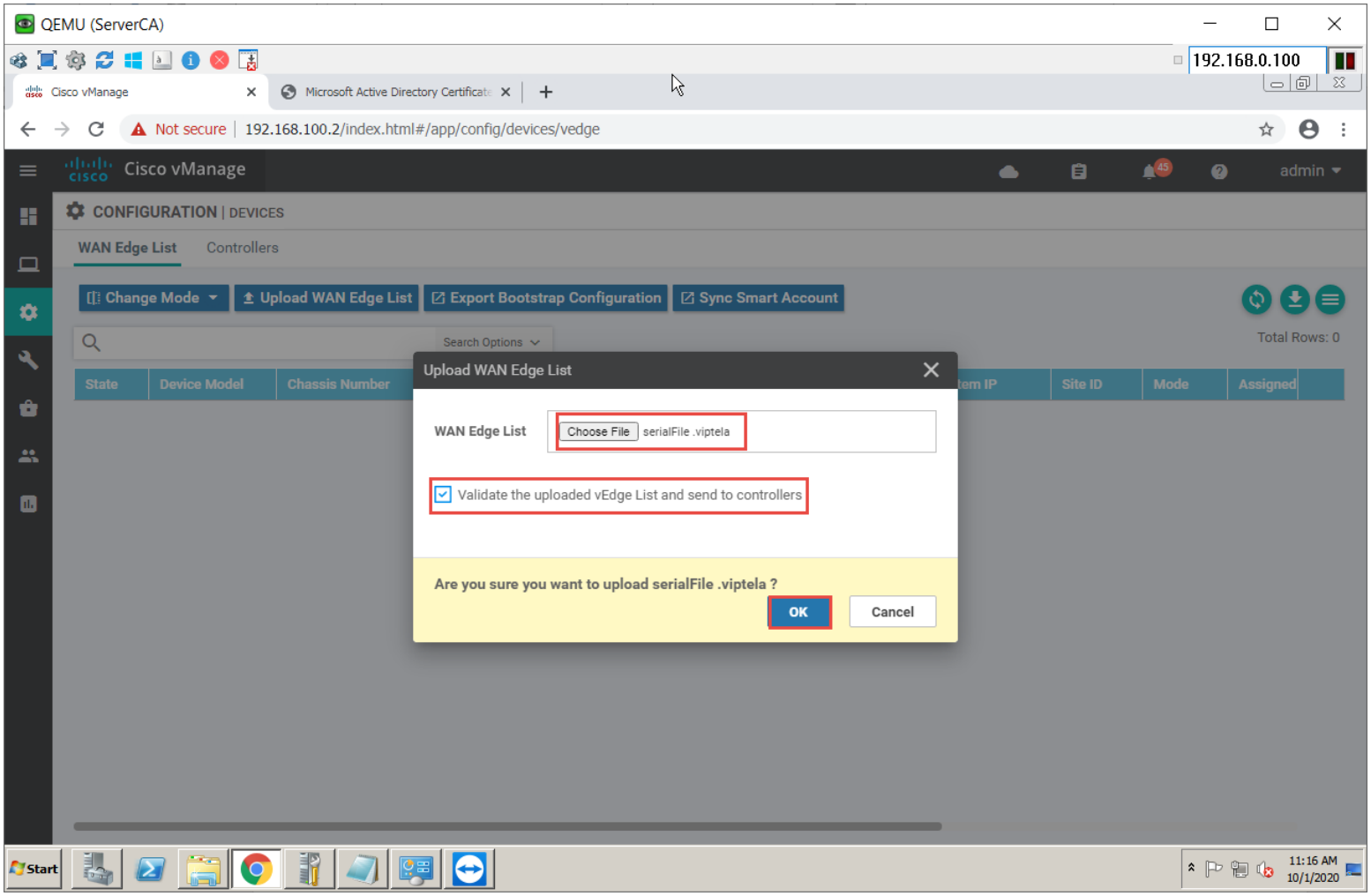
Before doing this lab, please note that vedge have **bug related to resolve the next-hop on vpn0**. So sometime, **vmanage cant reach to vedge** ➔ You **must flap Ge0/0 or Ge0/1 interface**.

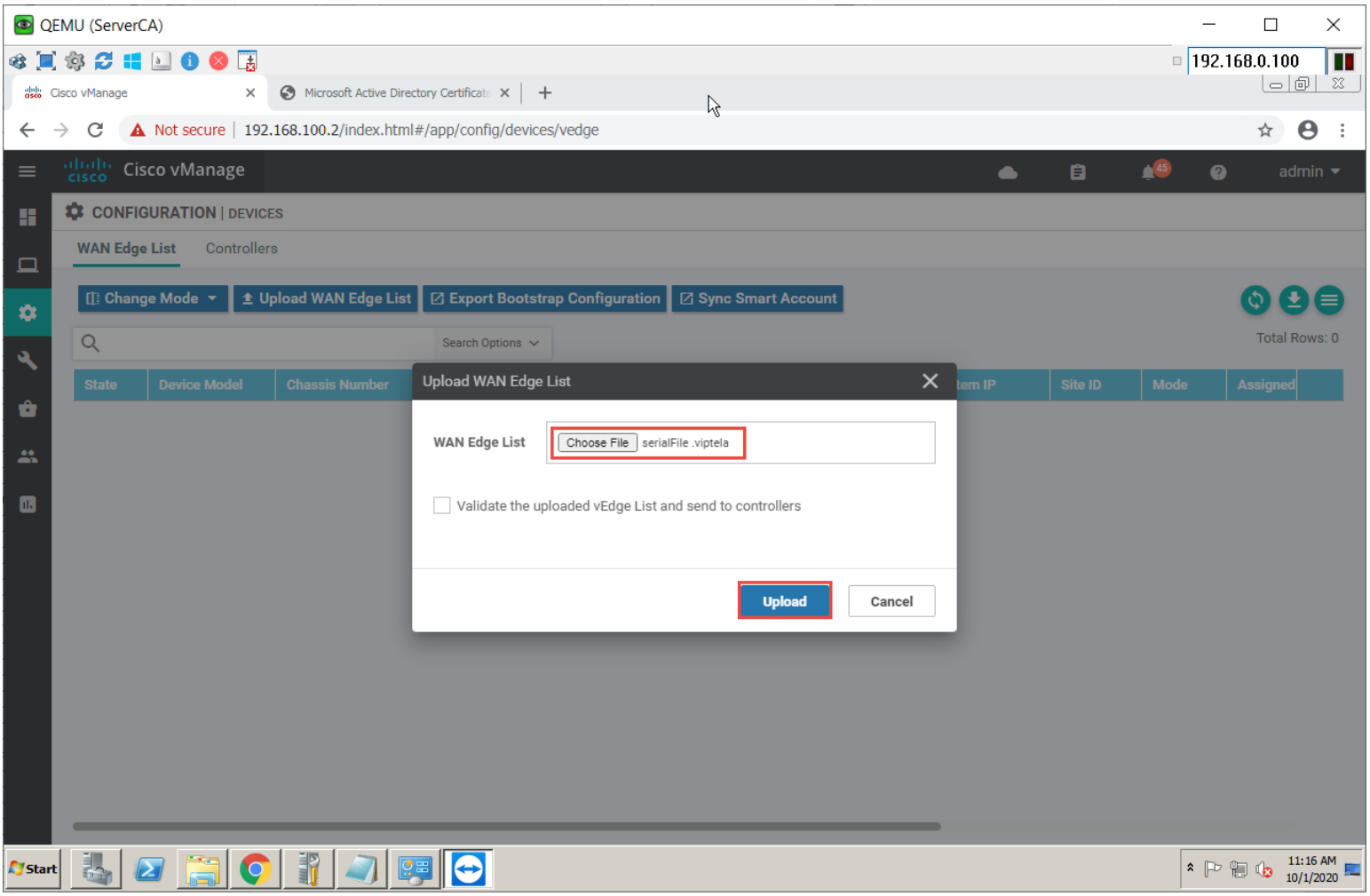
Task 1 – Upload the WAN Edge List

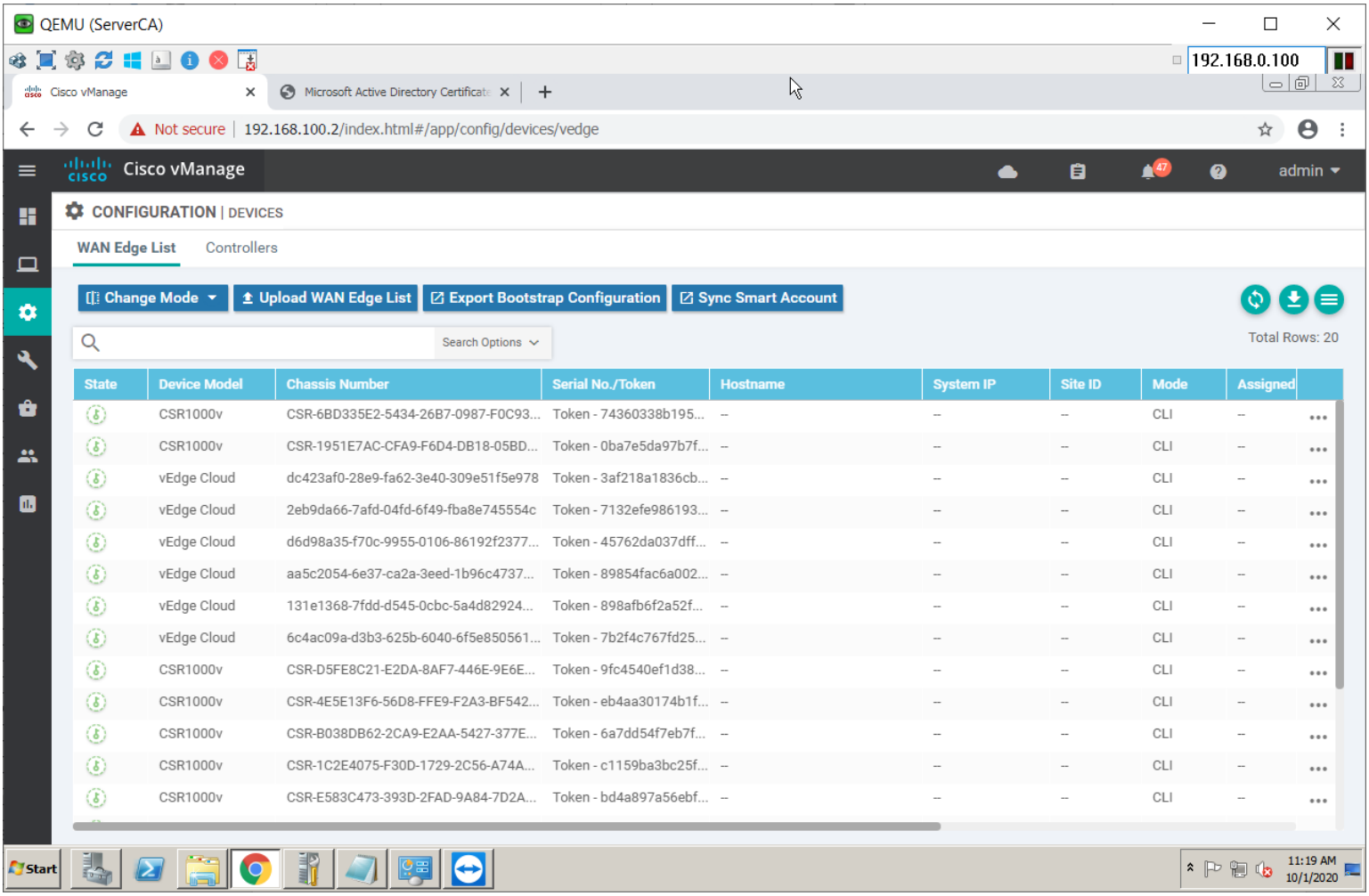
- On the vManage Main windows, Naviagte to **Configuration** ➔ **Devices**. Click on "**Upload WAN Edge List**".



- 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.


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
admin
CONFIGURATION | DEVICES
WAN Edge List
Controllers
Change Mode
Upload WAN Edge List
Export Bootstrap Configuration
Sync Smart Account
Search Options
Total Rows: 0
State
Device Model
Chassis Number
Site ID
Mode
Assigned
Upload WAN Edge List
WAN Edge List
Choose File
serialFile .viptela
Validate the uploaded vEdge List and send to controllers
Are you sure you want to upload serialFile .viptela ?
OK
Cancel
Start
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
admin
CONFIGURATION | DEVICES
WAN Edge List
Controllers
Change Mode
Upload WAN Edge List
Export Bootstrap Configuration
Sync Smart Account
Search Options
Total Rows: 0
State
Device Model
Chassis Number
Site ID
Mode
Assigned
Upload WAN Edge List
WAN Edge List
Choose File
serialFile .viptela
Validate the uploaded vEdge List and send to controllers
Upload
Cancel
Start
11:16 AM
10/1/2020



vEDGE-1

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : vEdge1
  - Organization: **"viptela sdwan"**
  - System-IP: 119.1.1.21
  - Site ID: 1
  - vbond Address: 100.1.1.4
  - 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:
    - 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
    - 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:
  - Host-name : vEdge2
  - Organization: **"viptela sdwan"**
  - System-IP: 118.1.2.22
  - Site ID: 2
  - vbond Address: 100.1.1.4
  - 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:
  - 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
  - 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:
  - Host-name : vEdge3
  - Organization: **"viptela sdwan"**
  - System-IP: 118.1.3.23
  - Site ID: 3
  - vbond Address: 100.1.1.4
  - Timezone: Based on the appropriate Timezone
  - 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
  - Interface ge0/1
  - IP Address: 118.1.3.1/24
  - Tunnel Interface
  - Encapsulation IPSec
  - 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:
    - 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
    - vpn 512
        - Interface eth0
        - IP Address: DHCP Client

vEdge4

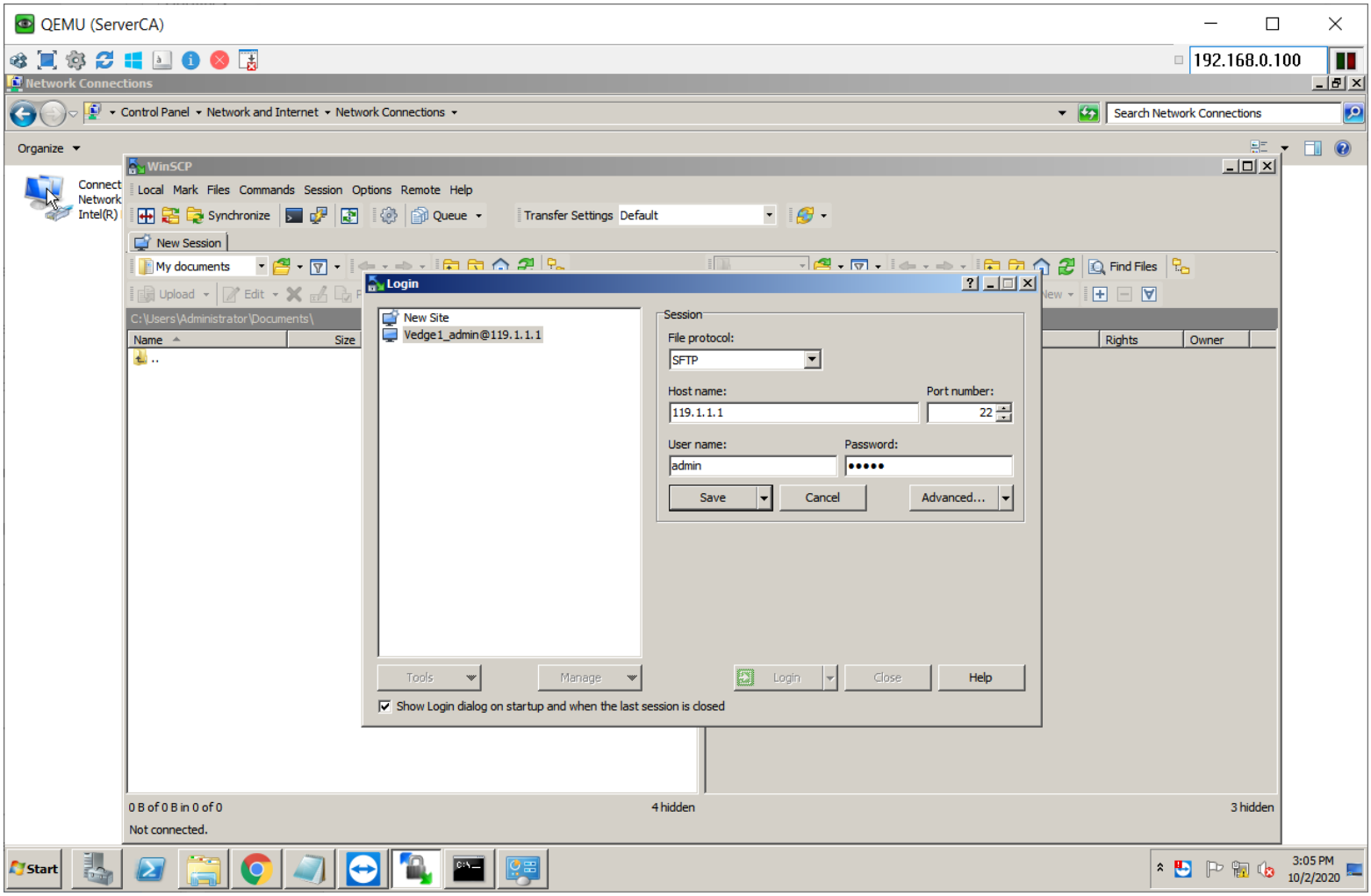
```
config
vpn 0
no interface ge0/0
interface ge0/1
ip address 118.1.4.1/24
tunnel-interface
encapsulation ipsec
allow-service all
allow-service netconf
allow-service sshd
no shut
ip route 0.0.0.0/0 118.1.4.2
vpn 512
interface eth0
ip dhcp-client
no shutdown
commit
```

Lab 10 – Registering vEdges in vManage

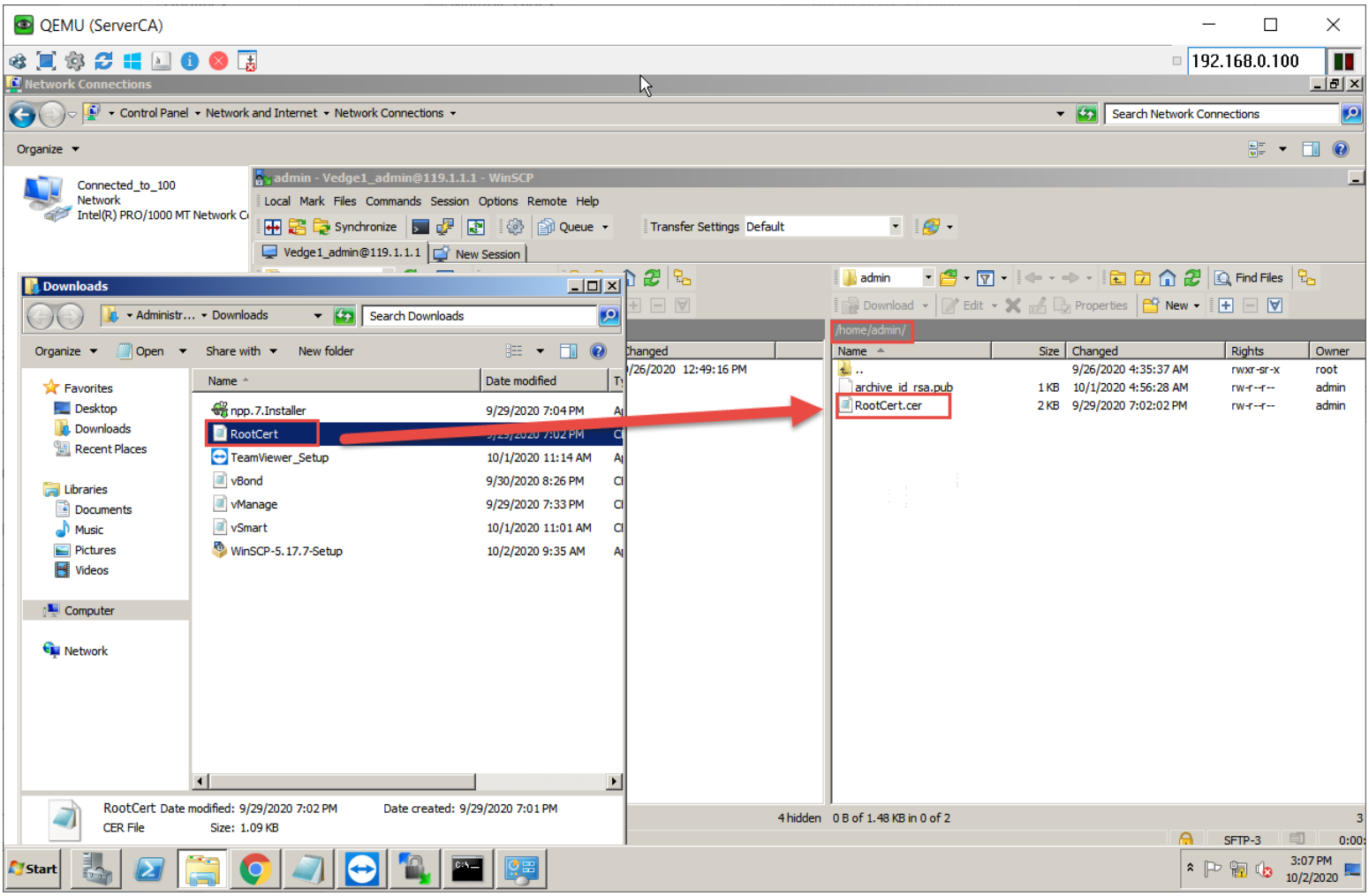
vEDGE-1

Task 1- Upload the Root Certificate to the vEdge

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

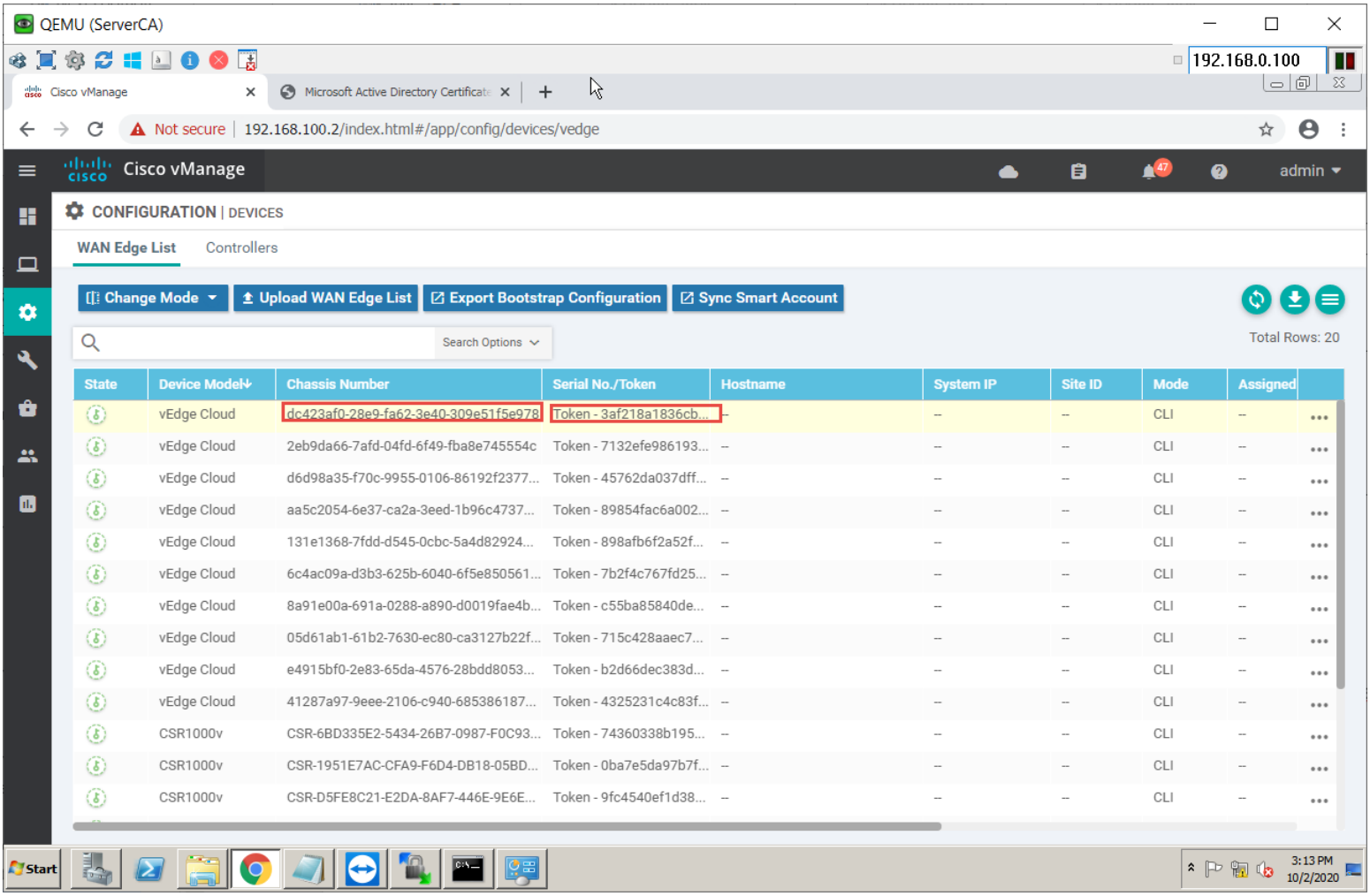
```
request root-cert-chain install /home/admin/RootCert.cer
```

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**

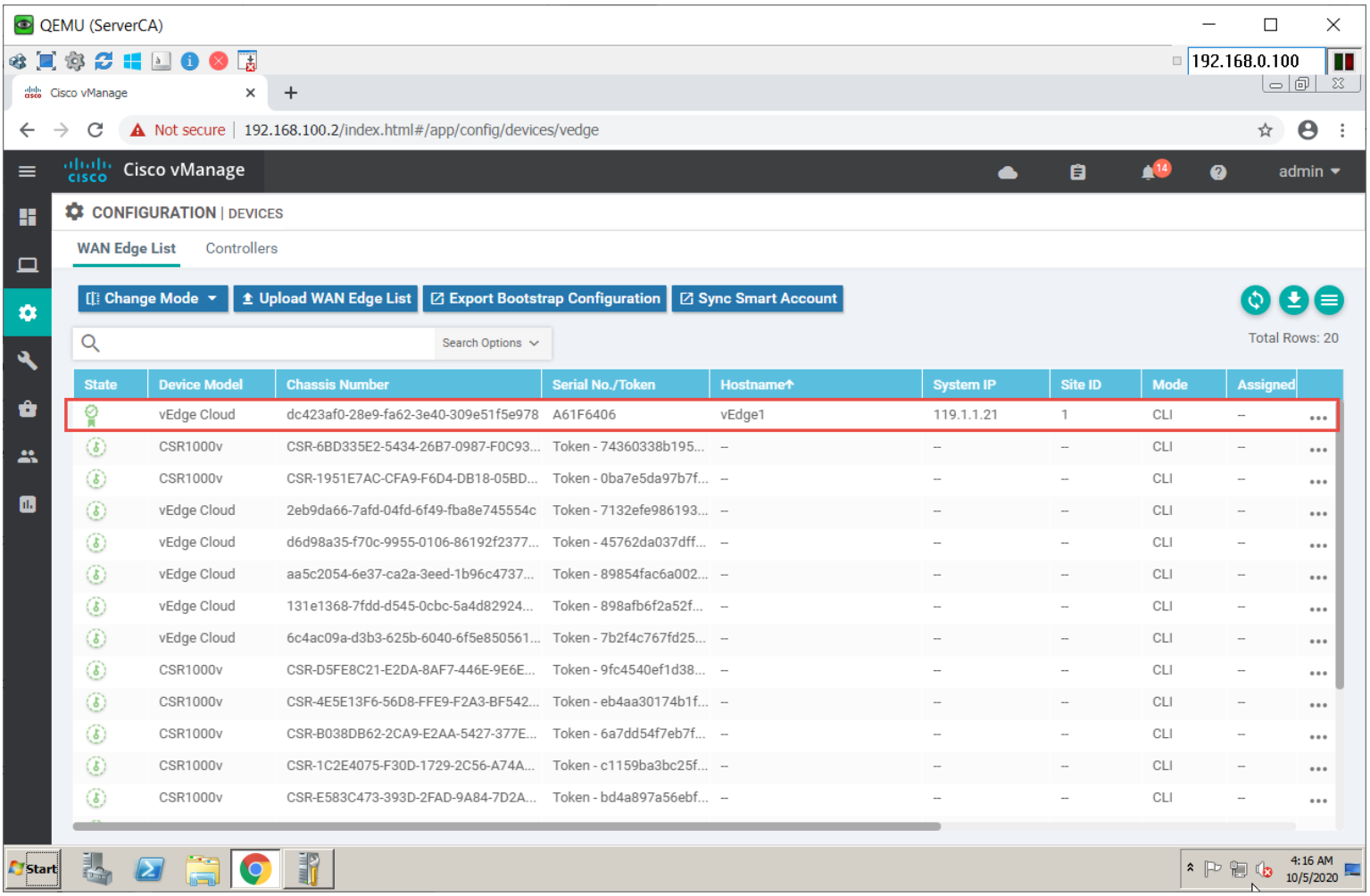


- Note and use the Chassis Number and Token Number for the list vEdge from vManage
- Use the information from the previous step in the following command on the vEdge1 console.

vEdge1

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

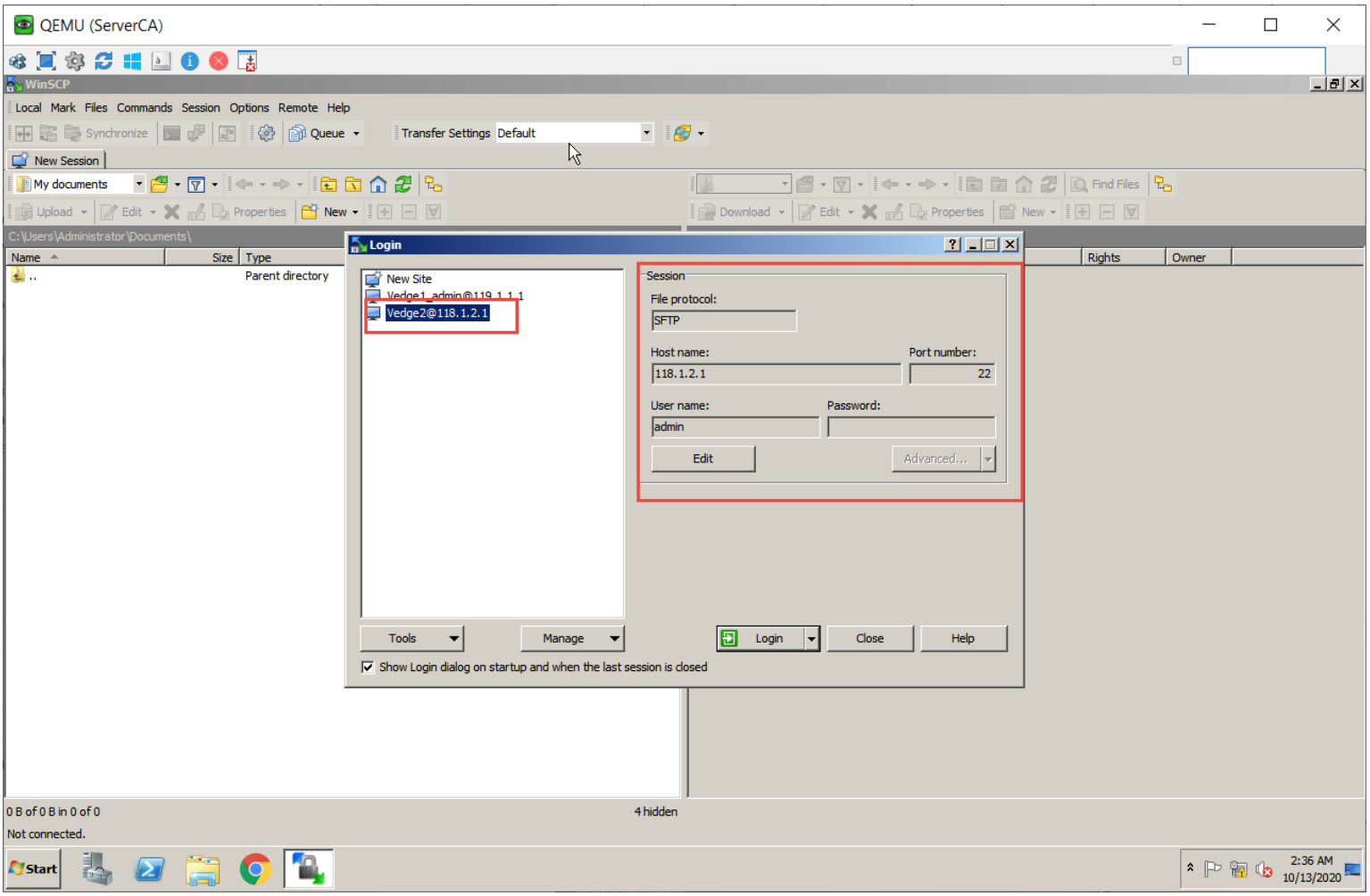
- We can check after adding finish



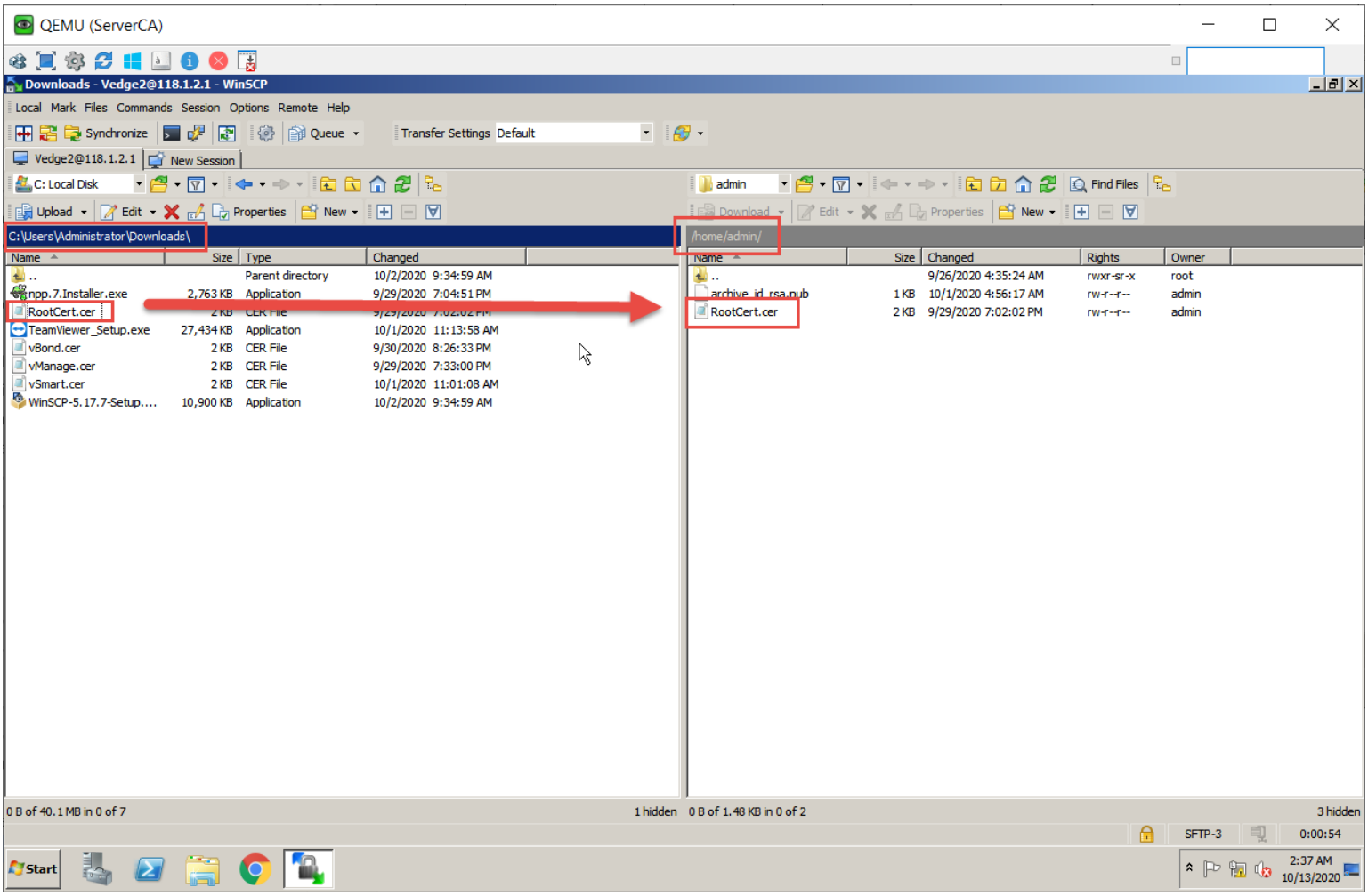
vEDGE-2

Task 1 – Upload the Root Certificate to the vEdge

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

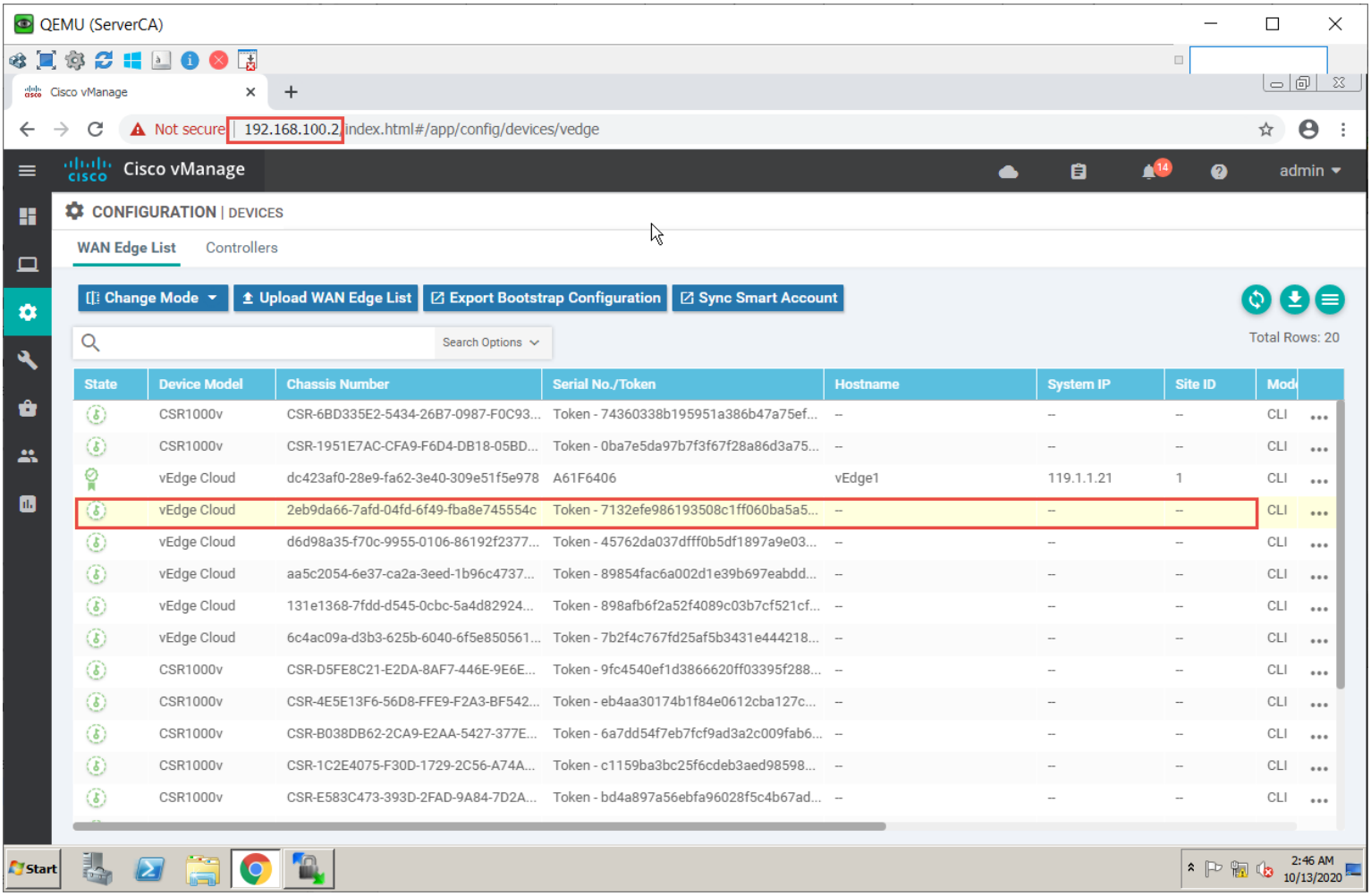
```
request root-cert-chain install /home/admin/RootCert.cer
```

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**



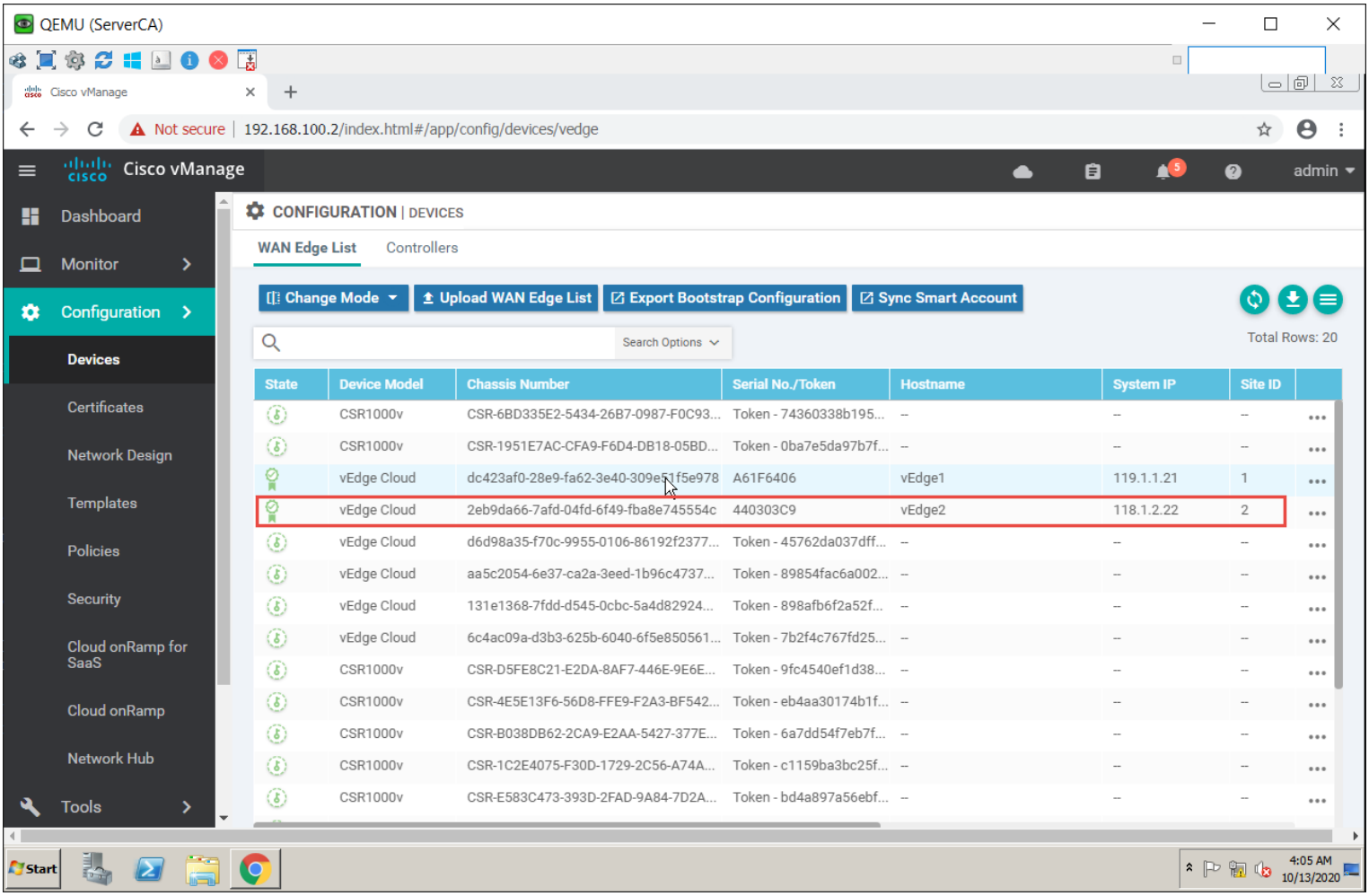
- Note and use the Chassis Number and Token number for the 2nd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge2 console

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

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

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

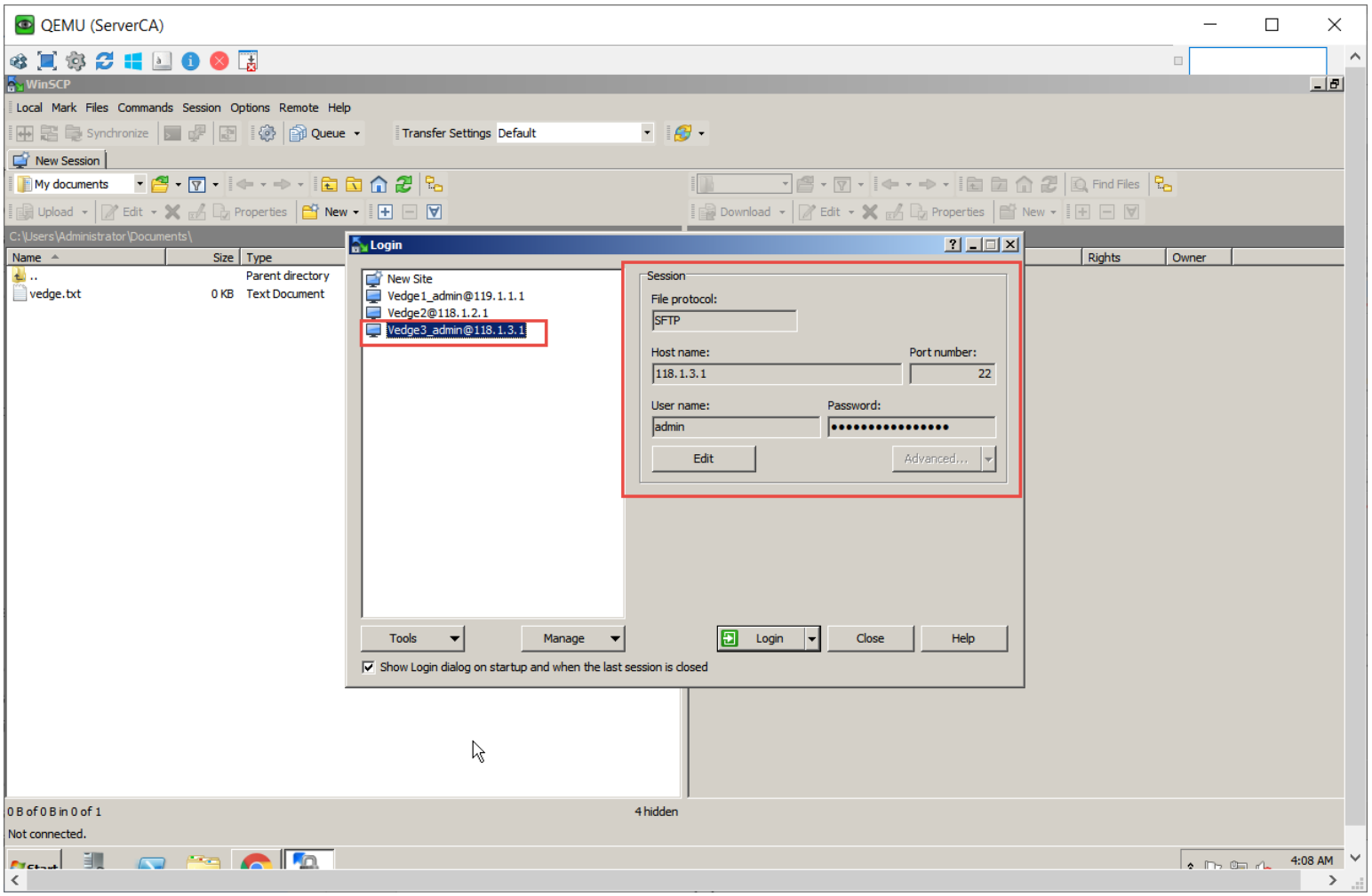
- You should see the vEdge in the vManage console with a Certificate issued.



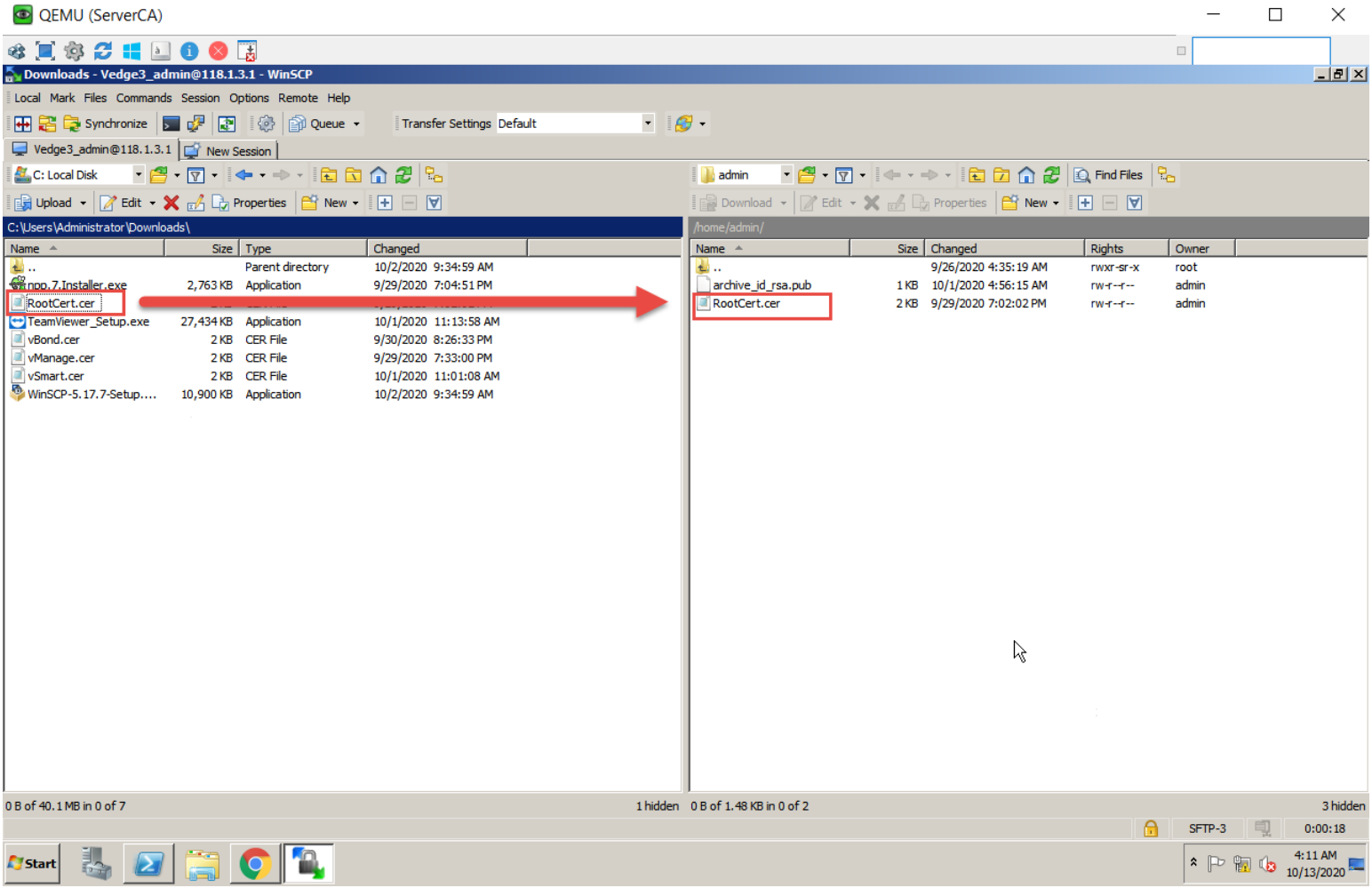
vEDGE-3

Task 1 – Upload the Root Certificate to the vEdge

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

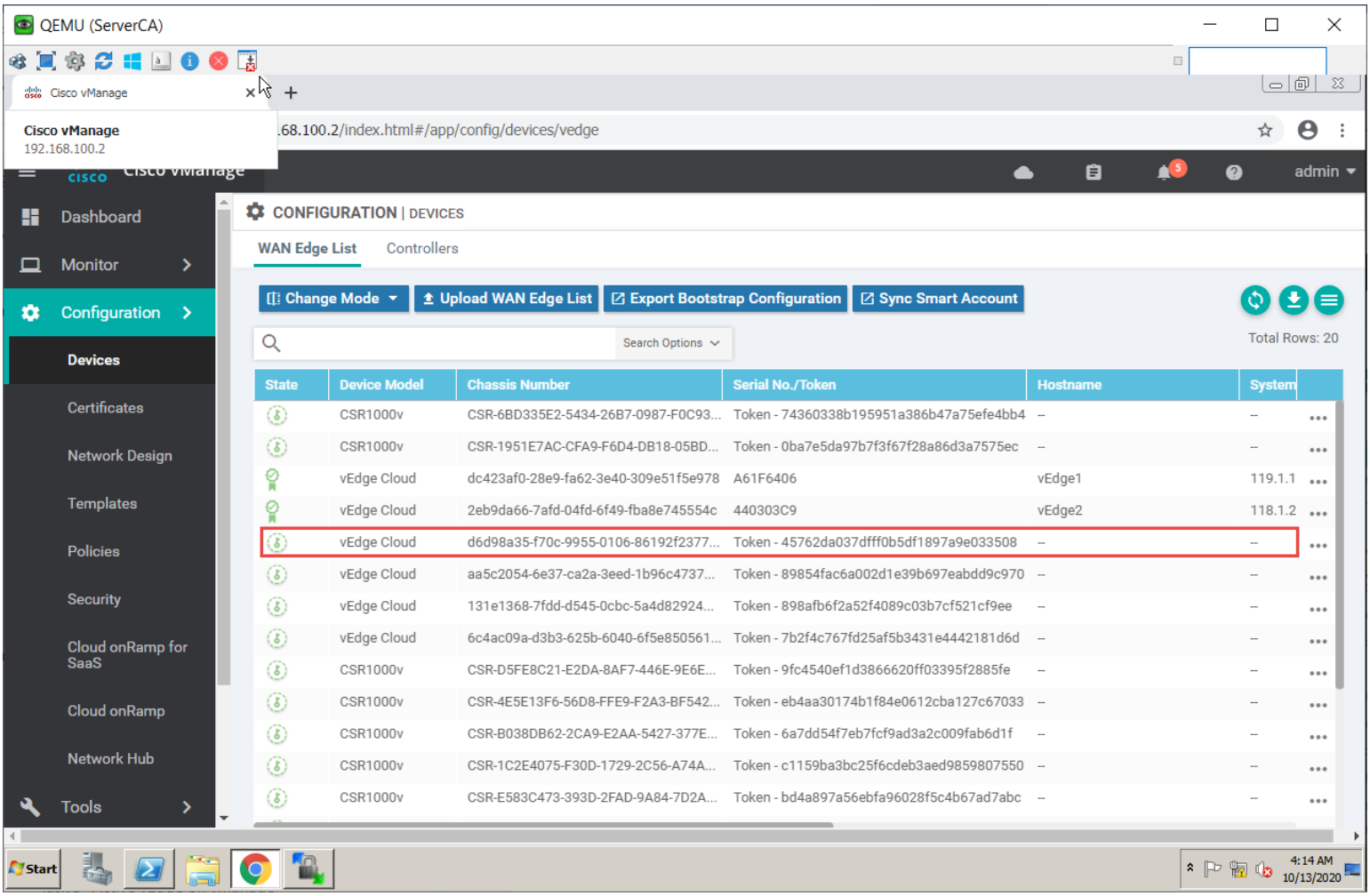
```
request root-cert-chain install /home/admin/RootCert.cer
```

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**



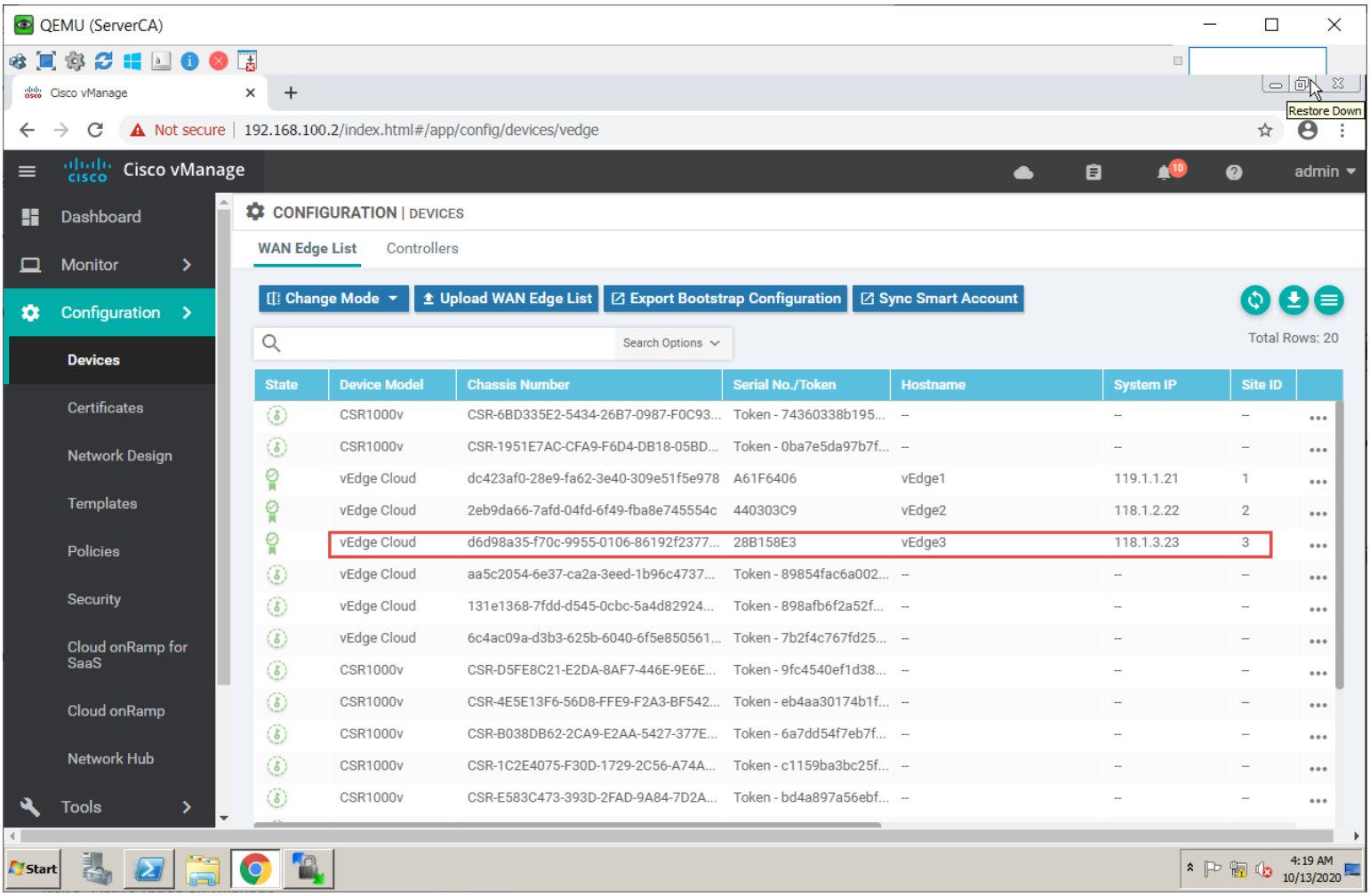
- Note and use the Chassis Number and Token number for the 3nd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge3 console

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

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

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

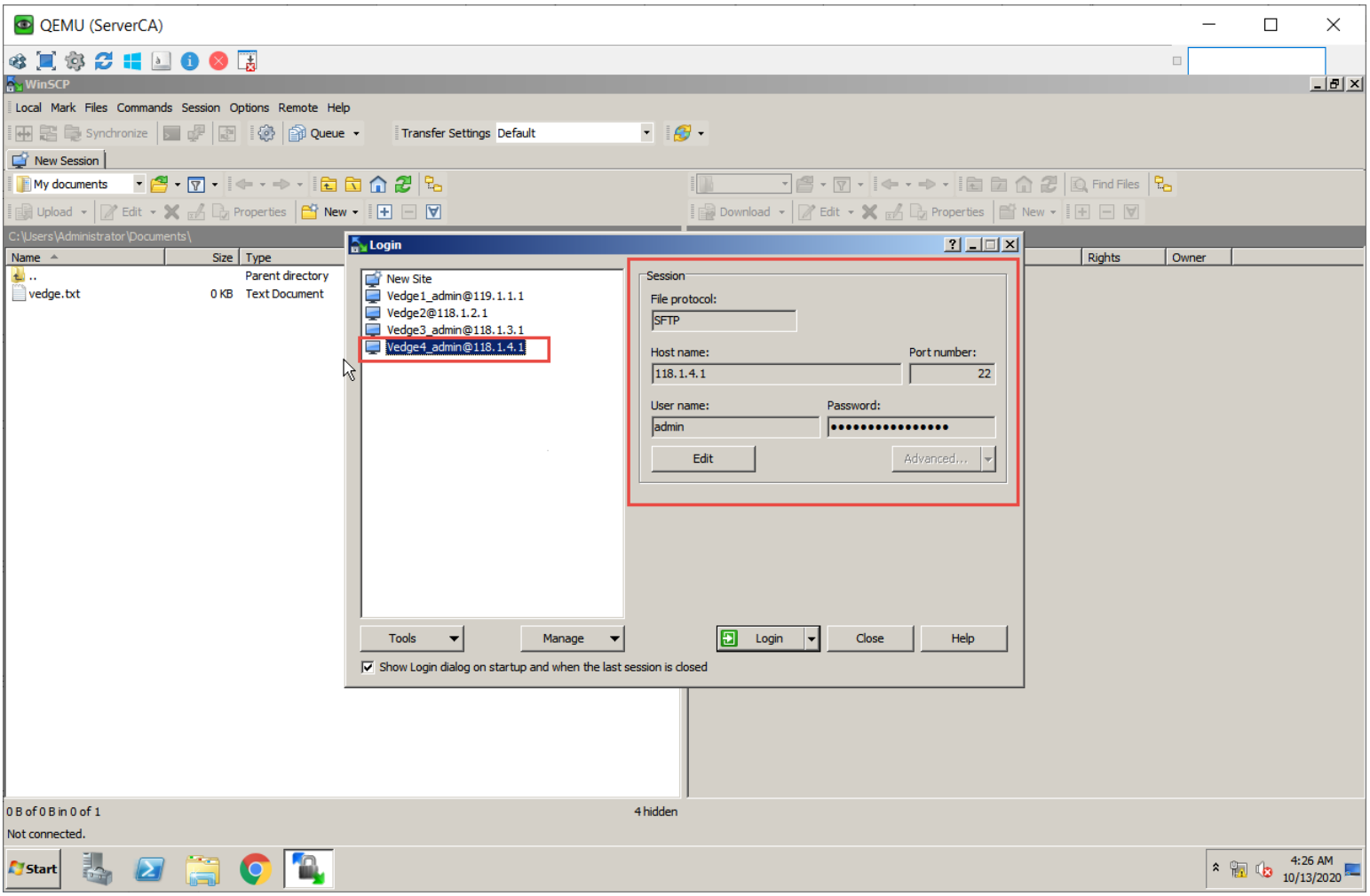
- You should see the vEdge in the vManage console with a Certificate issued.



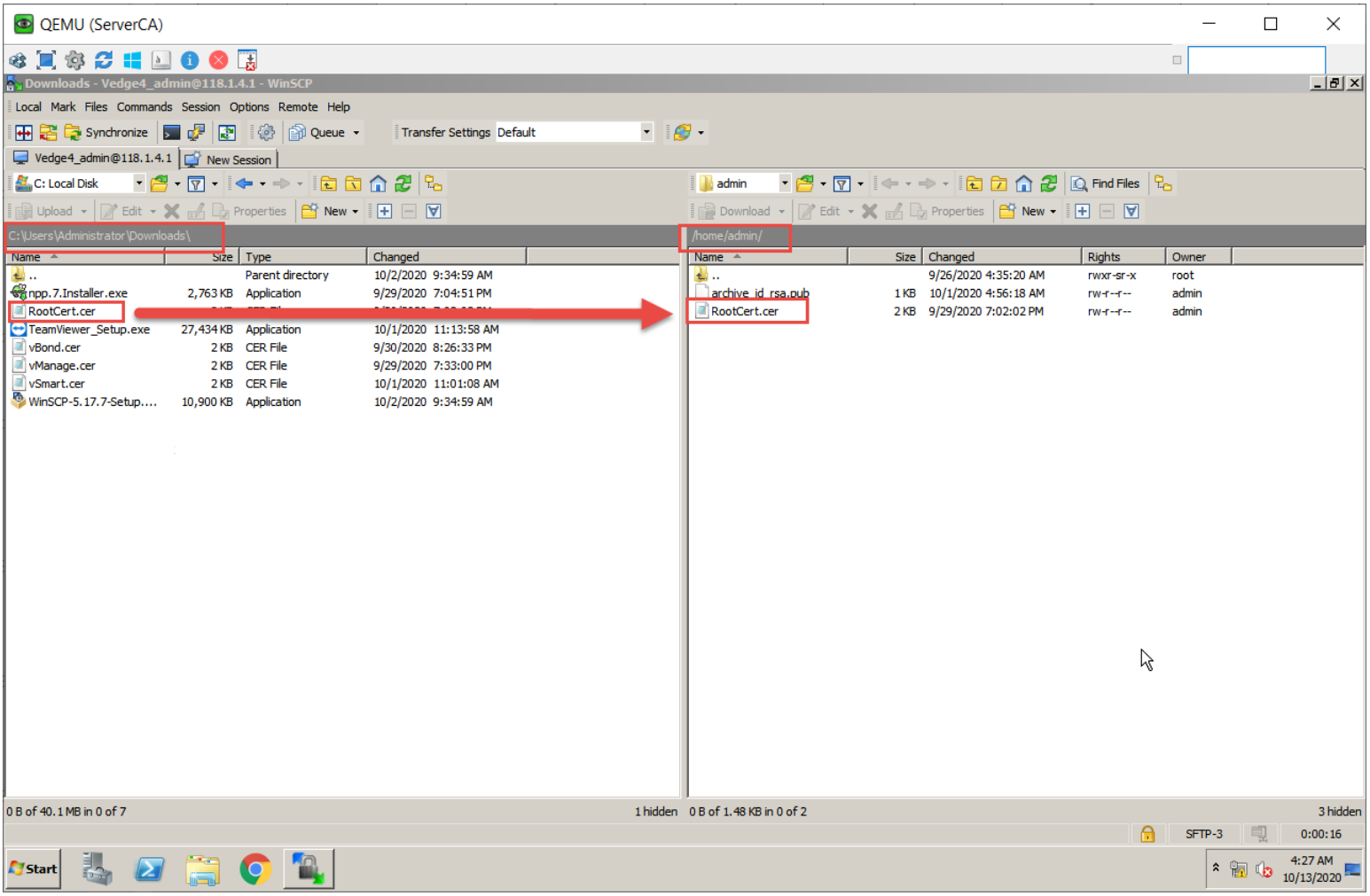
vEDGE-4

Task 1 – Upload the Root Certificate to the vEdge

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

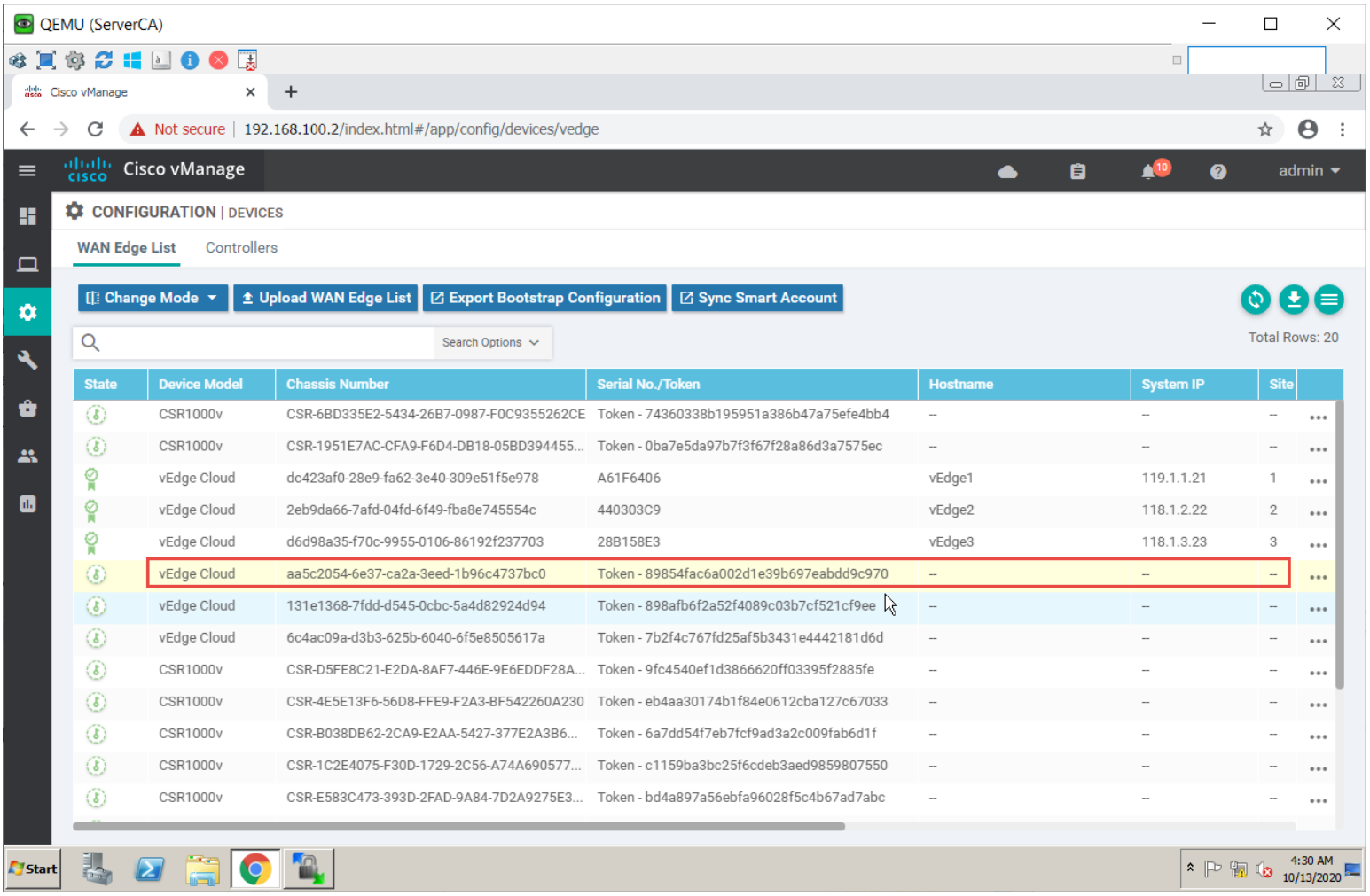
```
request root-cert-chain install /home/admin/RootCert.cer
```

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**



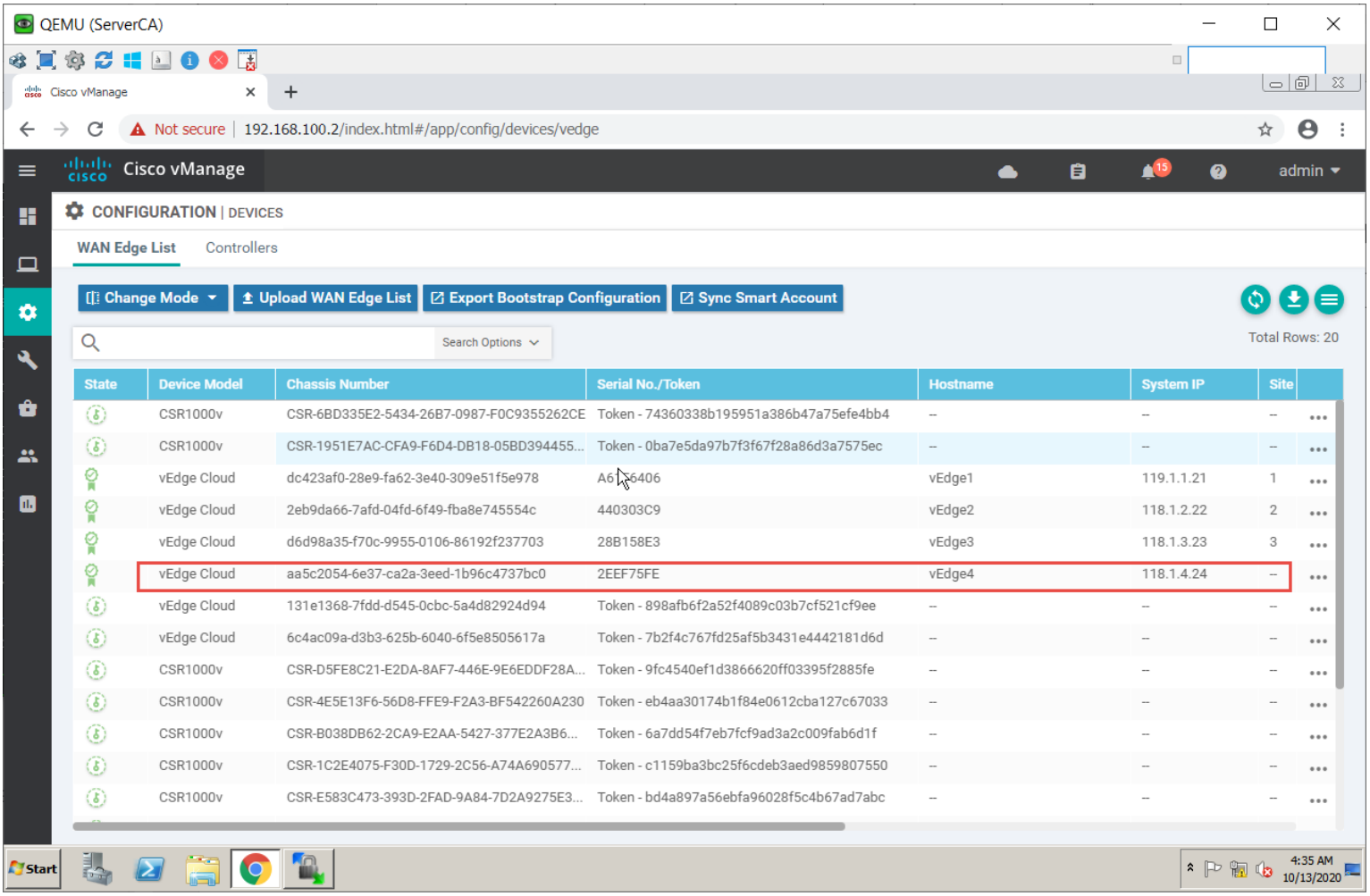
- Note and use the Chassis Number and Token number for the 3nd vEdge from vManage.
- Use the information from the previous step in the following command on the vEdge3 console

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

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

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

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



Lab 11 – Initializing cEdge – CLI

cEDGE-1

Task 1 – Configuring the System Component

- Configure the System parameters based on the following:
  - Host-name : **cEdge5**
  - Organization: **"viptela sdwan"**
  - System-IP: **118.1.5.25**
  - Site ID: **5**
  - vbond Address: **100.1.1.4**
  - 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:
  - GigabitEthernet1 Parameters
    - IP Address: 118.1.5.1/24
    - Default Route: 118.1.5.2
  - Tunnel Parameters Parameters
    - Tunnel Interface: Tunnel1
    - Tunnel Source: GigabitEthernet1
    - Tunnel Mode: SDWAN
  - SDWAN Interface Parameters
    - Interface: GigabitEthernet1
    - Encapsulation: IPSec
    - Color: default
    - Tunnel Services (All, NetConf, SSHD)

cEdge1:

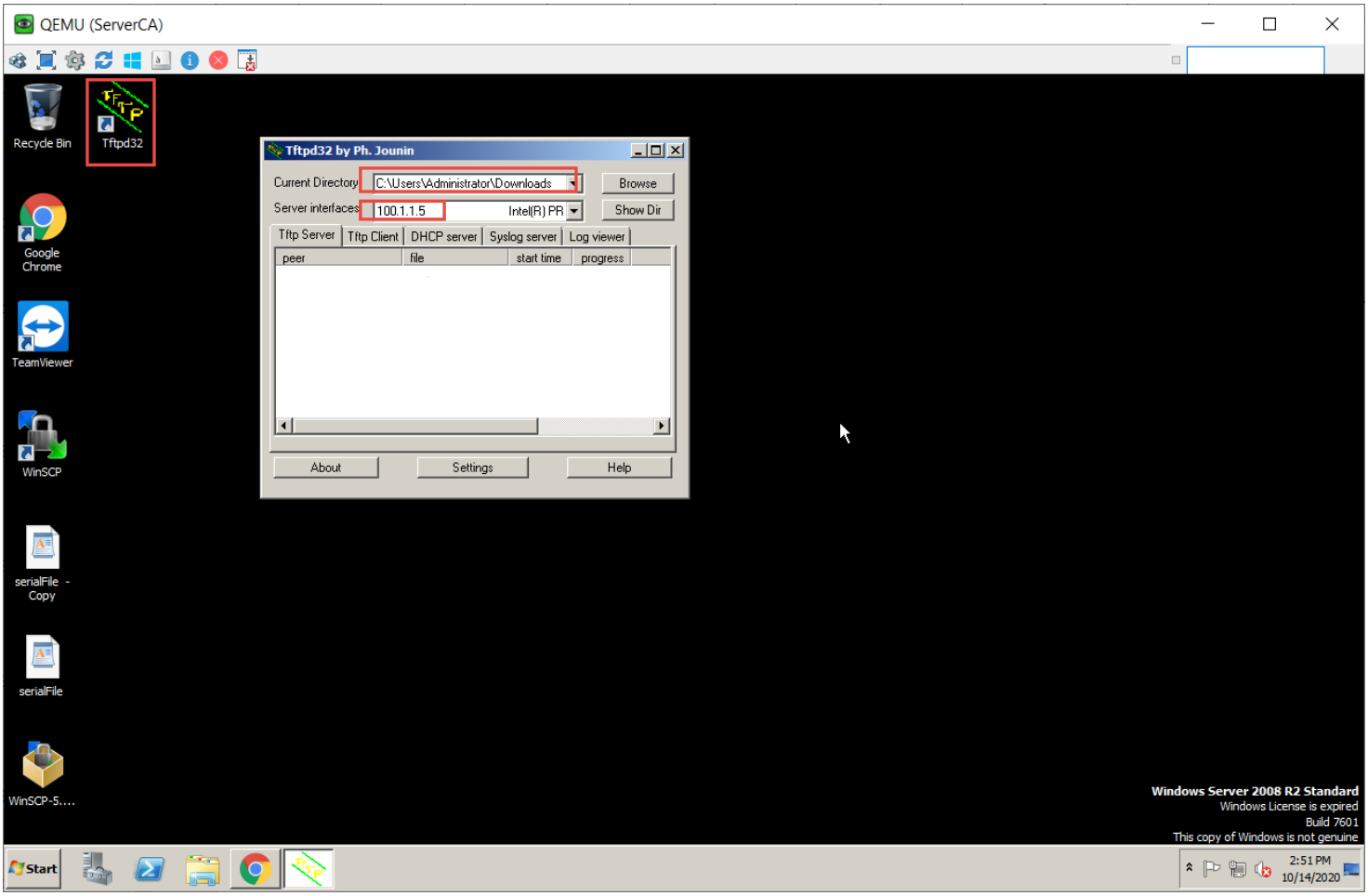
```
cEdge1
config-transaction
interface GigabitEthernet1
no shutdown
ip address 118.1.5.1 255.255.255.0
exit
ip route 0.0.0.0 0.0.0.0 118.1.5.2

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

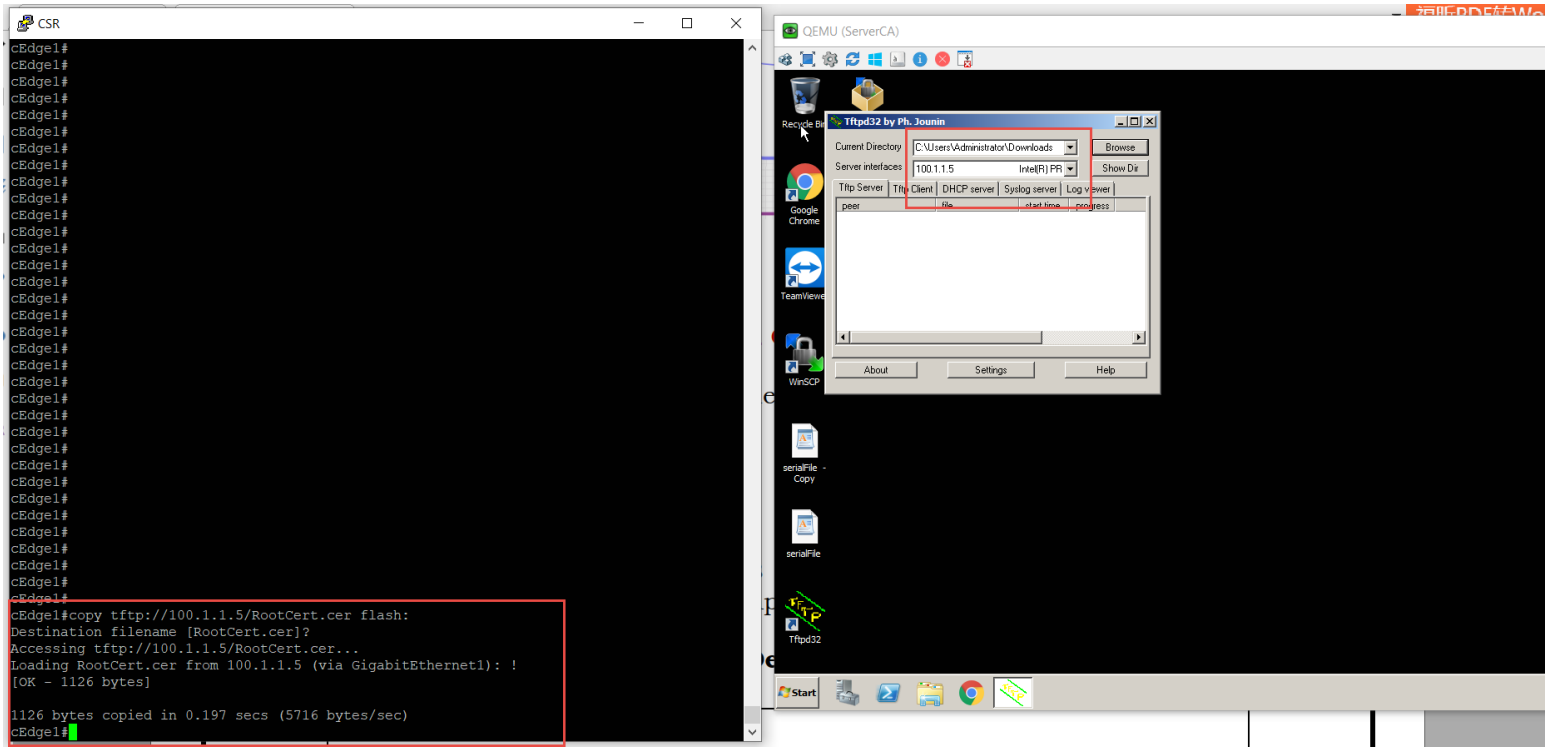
cEDGE-1

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.

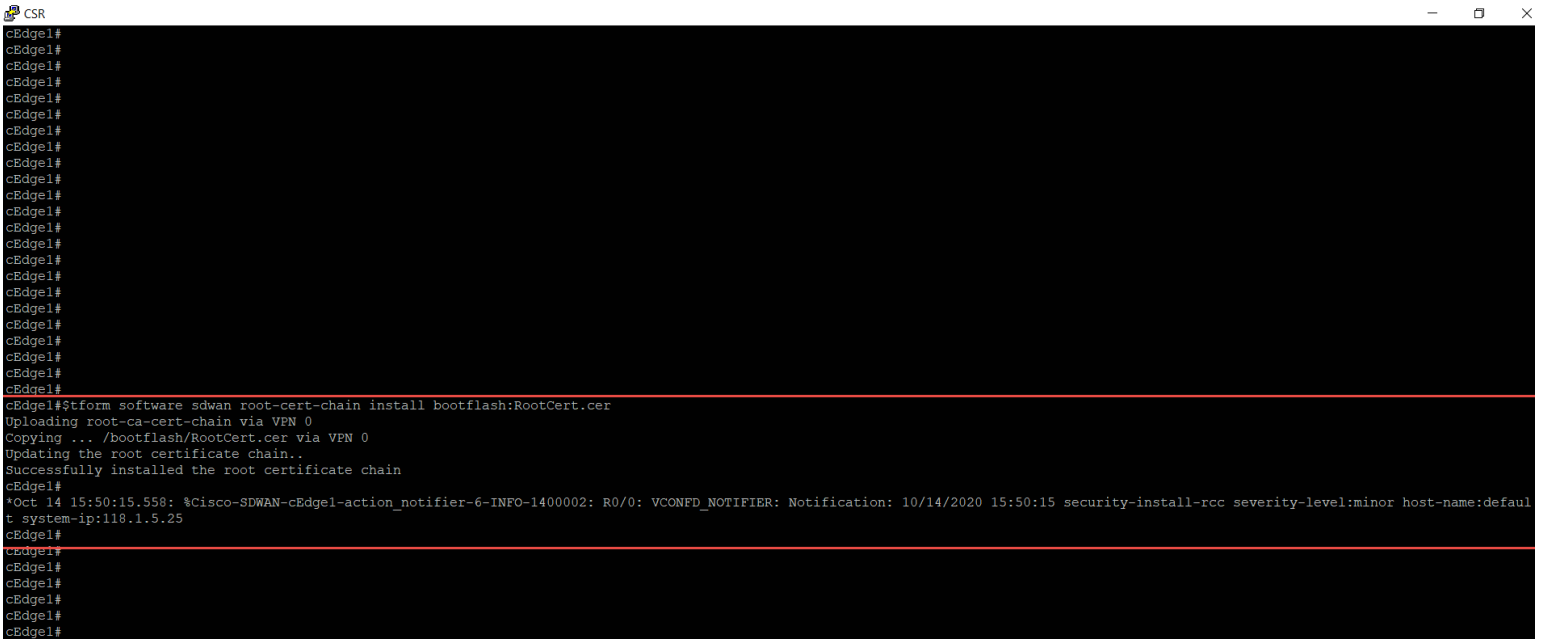


- Connect to the console of cEdge1 and copy the RootCert.cer file to flash: using the following command: **copy tftp://100.1.1.5/RootCert.cer flash:**



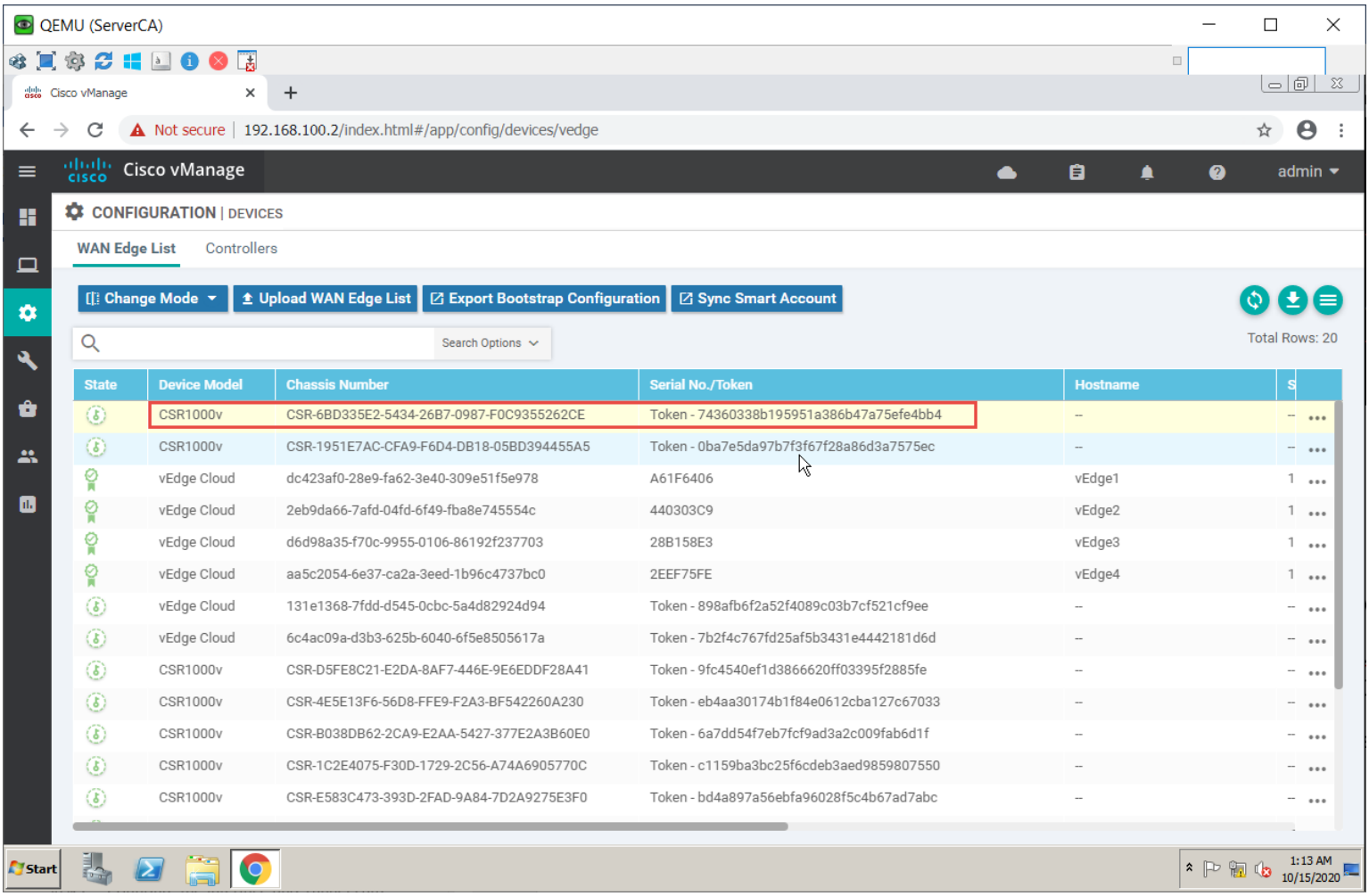
Task 2 – Install the Root Certificate on cEdge1

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

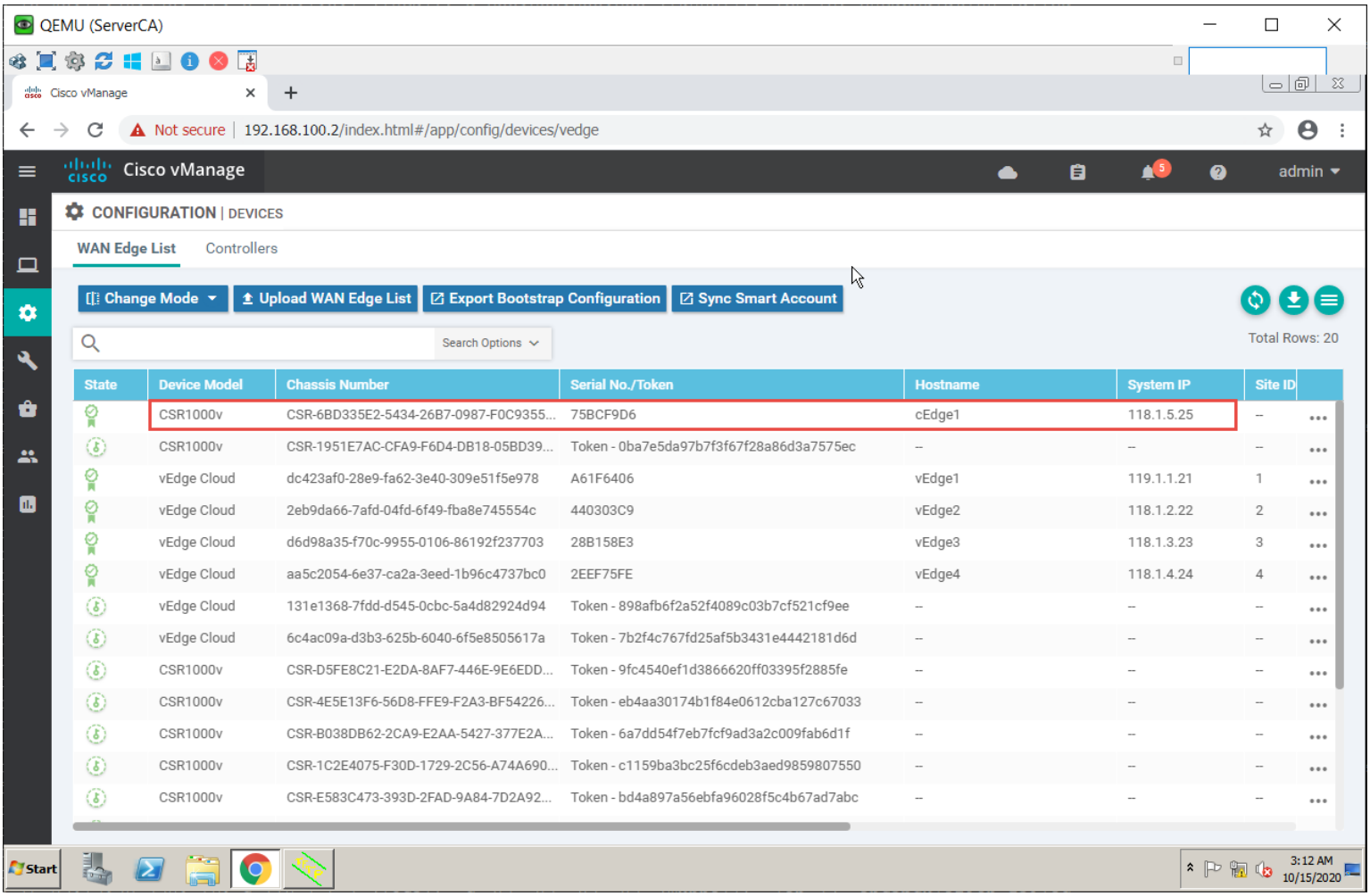
- Navigate to **Configuration -> Devices**
- Note and use the Chassis Number and Token number for the 1st CSR Device from vManage.



- 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-XXXXXXXXXXXXXXXX token XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

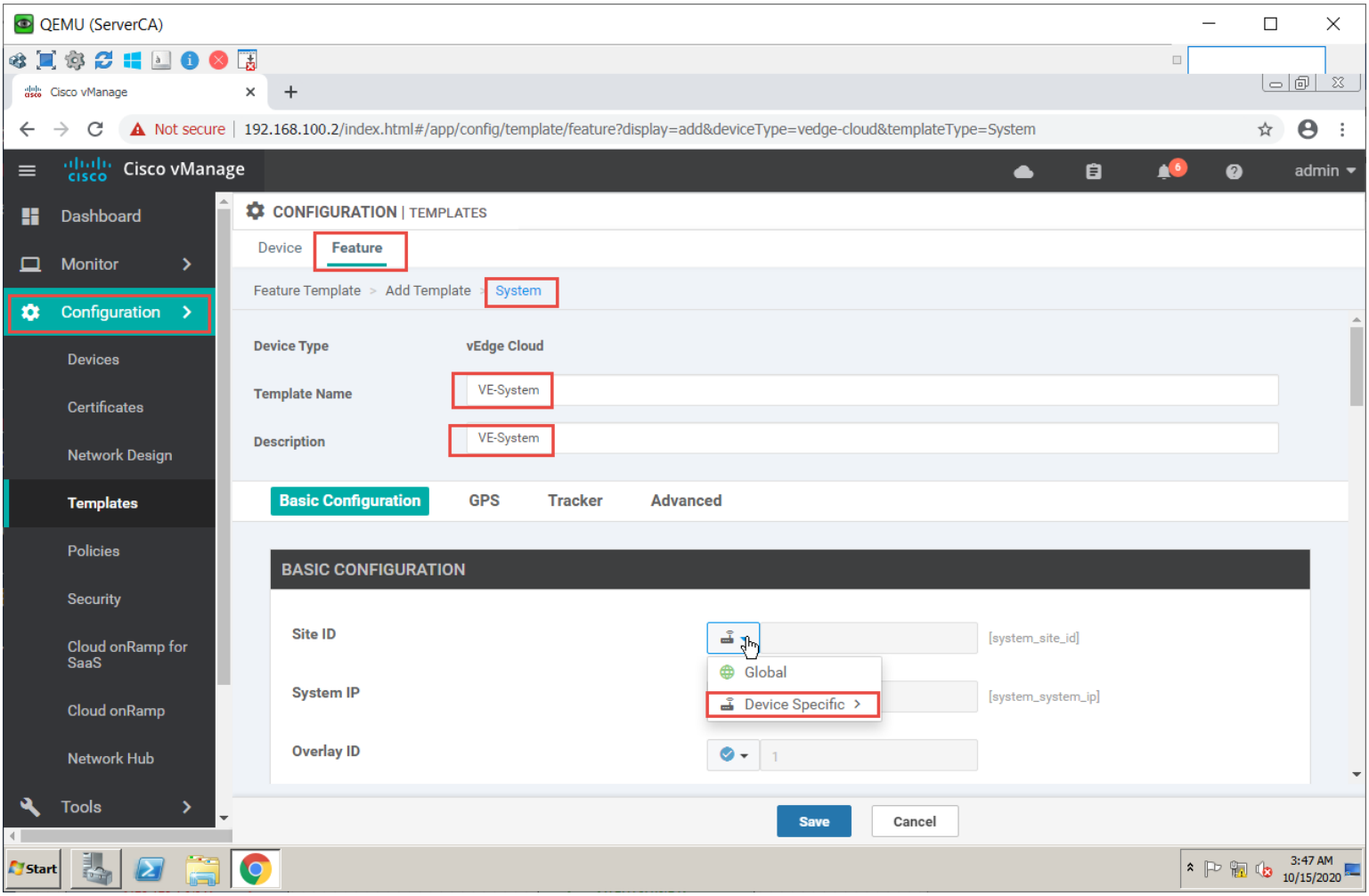
- You should see the vEdge in the vManage console with a Certificate issued

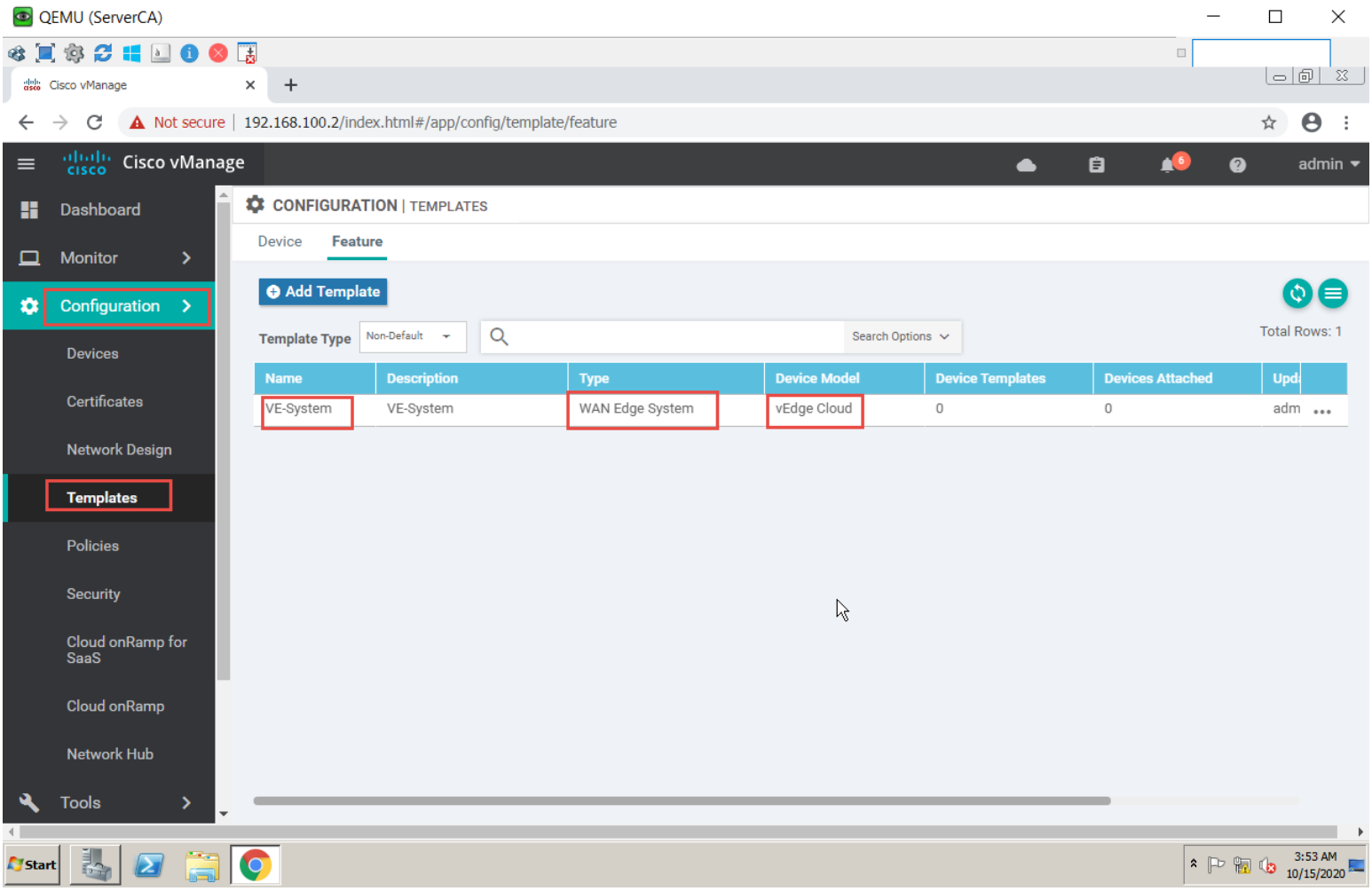

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/devices/vedge
Cisco vManage
admin
CONFIGURATION | DEVICES
WAN Edge List
Controllers
Change Mode
Upload WAN Edge List
Export Bootstrap Configuration
Sync Smart Account
Search Options
Total Rows: 20
State | Device Model | Chassis Number | Serial No./Token | Hostname | System IP | Site ID
CSR1000v | CSR-6BD335E2-5434-26B7-0987-F0C9355... | 75BCF9D6 | cEdge1 | 118.1.5.25 | --
CSR1000v | CSR-1951E7AC-CFA9-F6D4-DB18-05BD39... | Token - 0ba7e5da97b7f3f67f28a86d3a7575ec | -- | -- | --
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-9955-0106-86192f237703 | 28B158E3 | vEdge3 | 118.1.3.23 | 3
vEdge Cloud | aa5c2054-6e37-ca2a-3eed-1b96c4737bc0 | 2EEF75FE | vEdge4 | 118.1.4.24 | 4
vEdge Cloud | 131e1368-7fdd-d545-0cbc-5a4d82924d94 | Token - 898afb6f2a52f4089c03b7cf521cf9ee | -- | -- | --
vEdge Cloud | 6c4ac09a-d3b3-625b-6040-6f5e8505617a | Token - 7b2f4c767fd25af5b3431e4442181d6d | -- | -- | --
CSR1000v | CSR-D5FE8C21-E2DA-8AF7-446E-9E6EDD... | Token - 9fc4540ef1d3866620ff03395f2885fe | -- | -- | --
CSR1000v | CSR-4E5E13F6-56D8-FFE9-F2A3-BF54226... | Token - eb4aa30174b1f84e0612cba127c67033 | -- | -- | --
CSR1000v | CSR-B038DB62-2CA9-E2AA-5427-377E2A... | Token - 6a7dd54f7eb7fcf9ad3a2c009fab6d1f | -- | -- | --
CSR1000v | CSR-1C2E4075-F30D-1729-2C56-A74A690... | Token - c1159ba3bc25f6cdeb3aed9859807550 | -- | -- | --
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

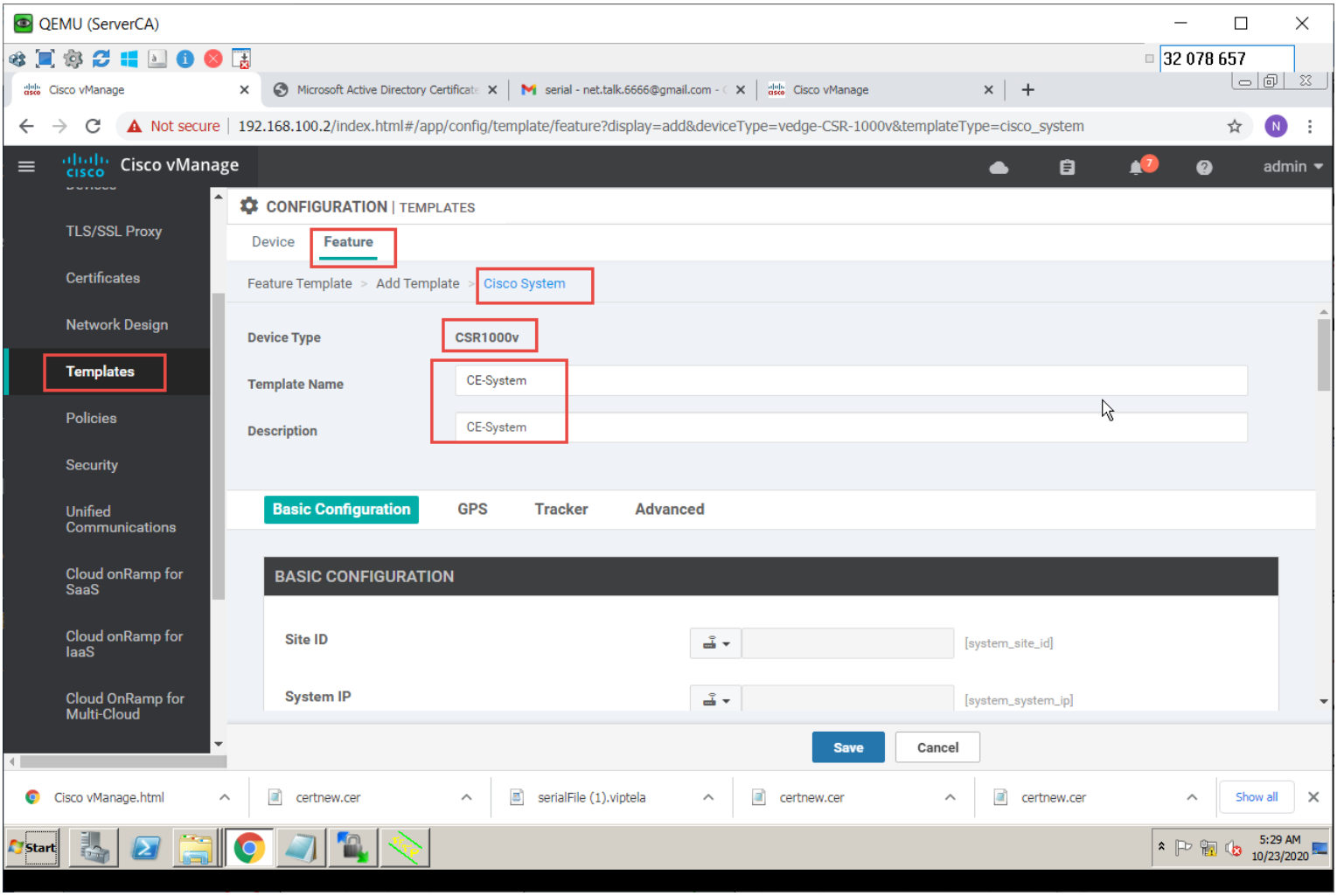
- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ Basic Information ➔ System
- Configure the System parameters based on the following:
  - Template Name: VE-System
  - Description: VE-System
  - Site ID ➔ Device Specific
  - System IP ➔ Device Specific
  - Hostname ➔ Device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

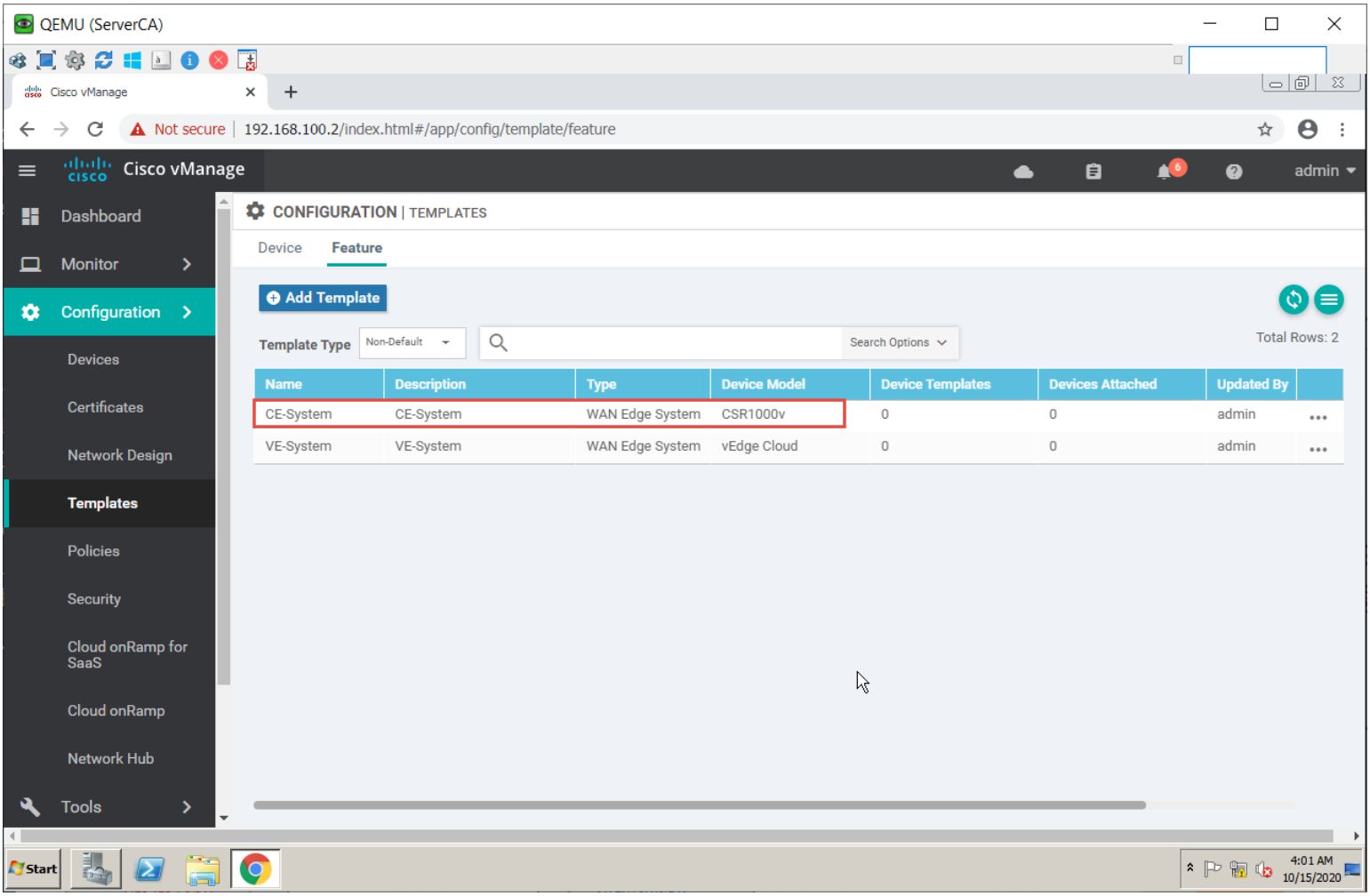




Task 2 – Configure the System Template to be used by all cEdgeCloud Devices

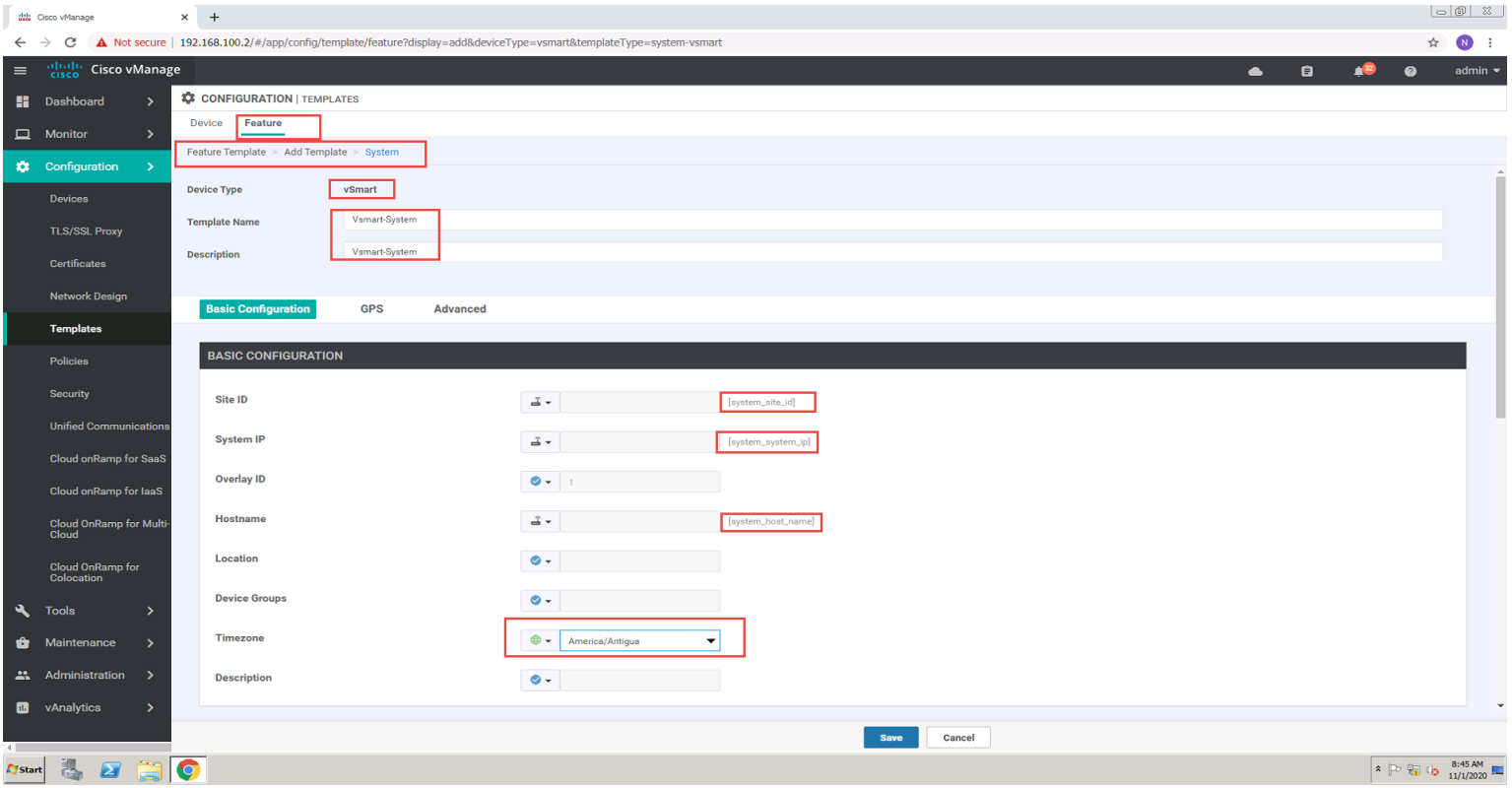
- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ CSR 1000v ➔ Basic Information ➔ Cisco System
- Configure the System parameters based on the following:
  - Template Name : CE-System
  - Description: CE-System
  - Site ID ➔ Device Specific
  - System IP ➔ Device Specific
  - Hostname ➔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

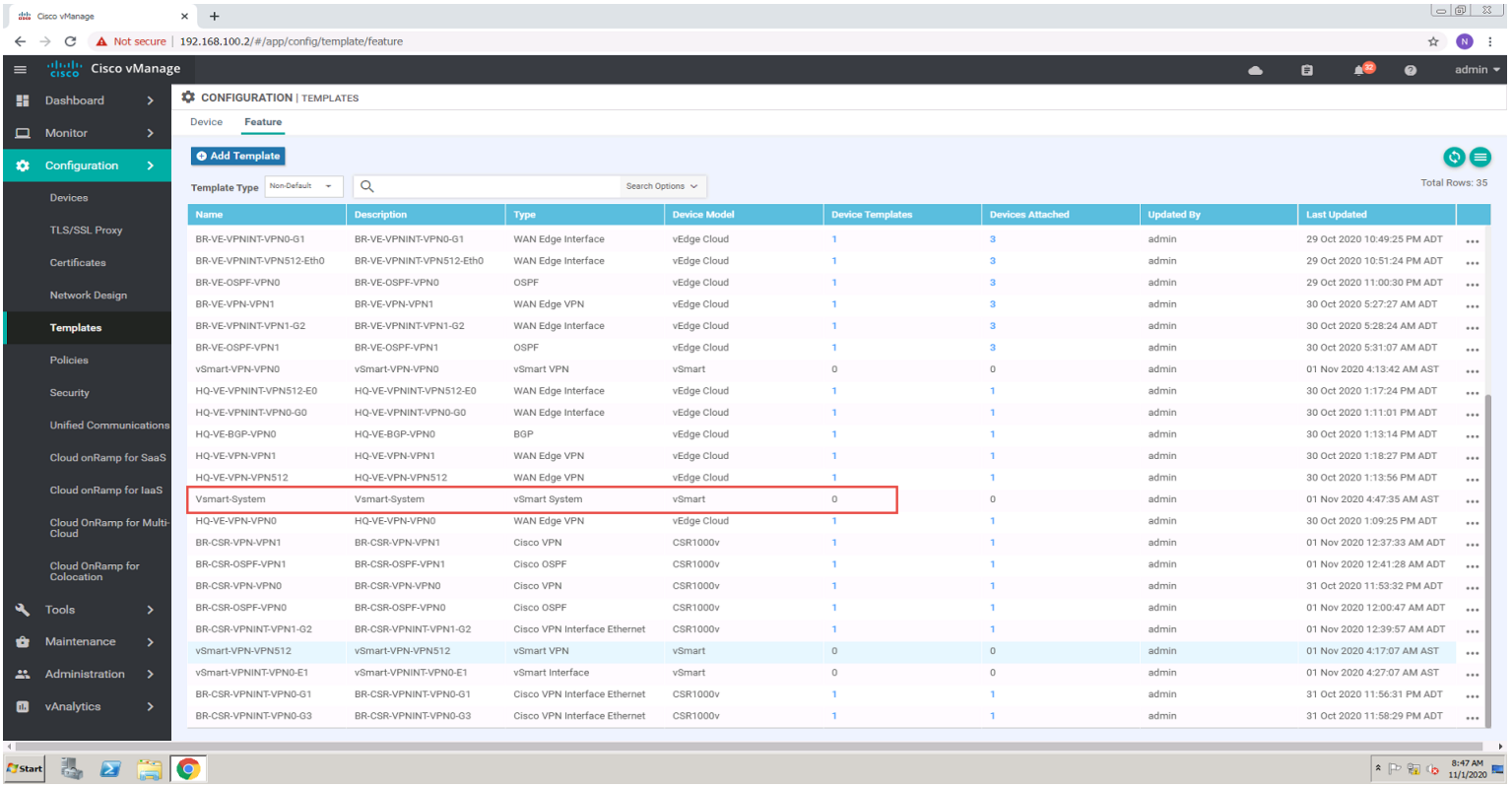

QEMU (ServerCA)
32 078 657
Cisco vManage
Microsoft Active Directory Certificate
serial - net.talk.6666@gmail.com -
Cisco vManage
Not secure
192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-CSR-1000v&templateType=cisco_system
Cisco vManage
admin
TLS/SSL Proxy
Certificates
Network Design
Templates
Policies
Security
Unified Communications
Cloud onRamp for SaaS
Cloud onRamp for IaaS
Cloud OnRamp for Multi-Cloud
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > Cisco System
Device Type
CSR1000v
Template Name
CE-System
Description
CE-System
Basic Configuration
GPS
Tracker
Advanced
BASIC CONFIGURATION
Site ID
[system_site_id]
System IP
[system_system_ip]
Save
Cancel
Cisco vManage.html
certnew.cer
serialFile (1).viptela
certnew.cer
certnew.cer
Show all
Start
5:29 AM
10/23/2020



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:
  - Template Name : Vsmart-System
  - Description : Vsmart-System
  - Site ID ➔ Device Specific
  - System IP ➔ Device Specific
  - Hostname ➔ Device Specific
  - Timezone ➔ Global : America/Antigua
- Click Save to save the Template.

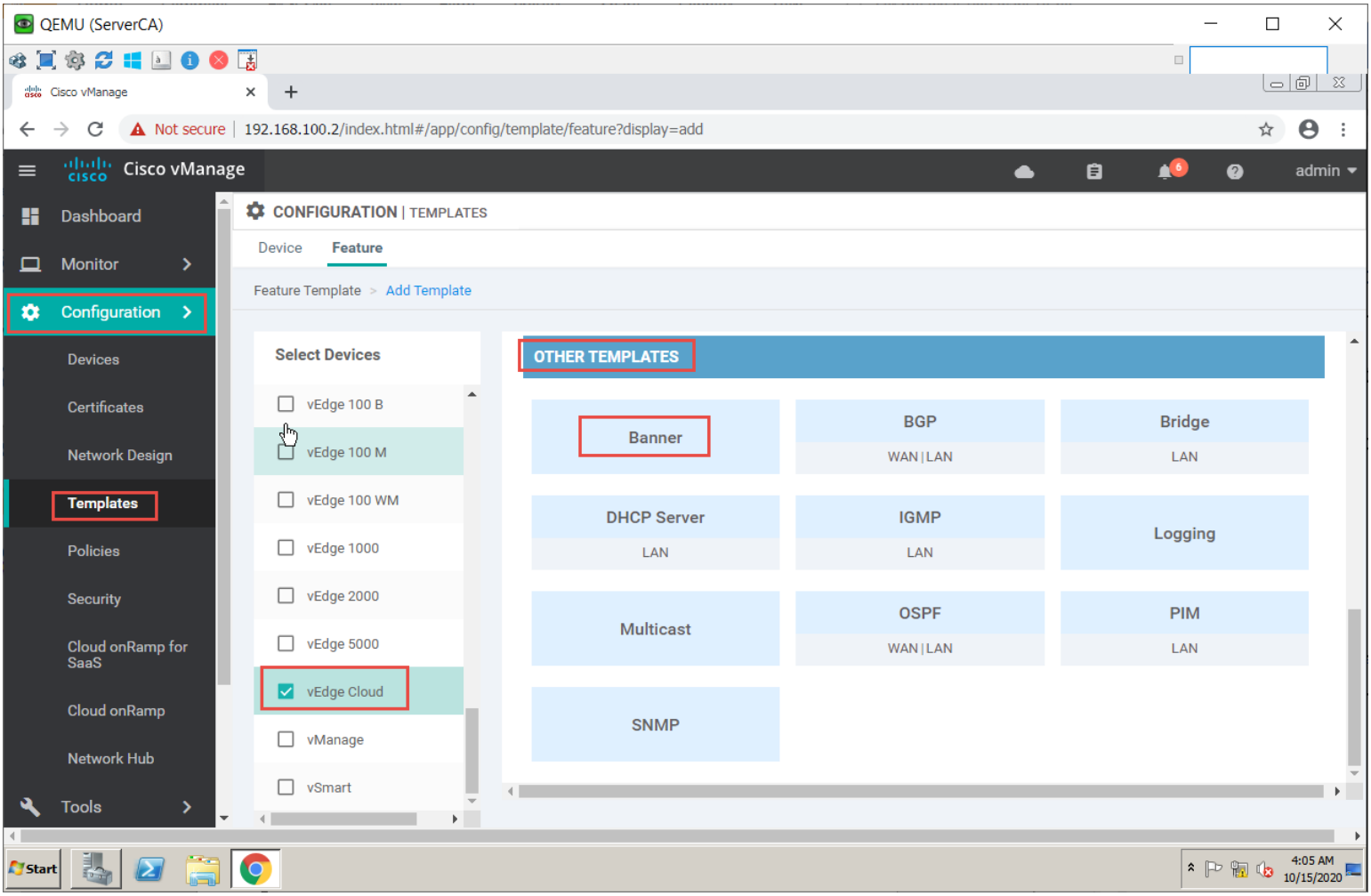


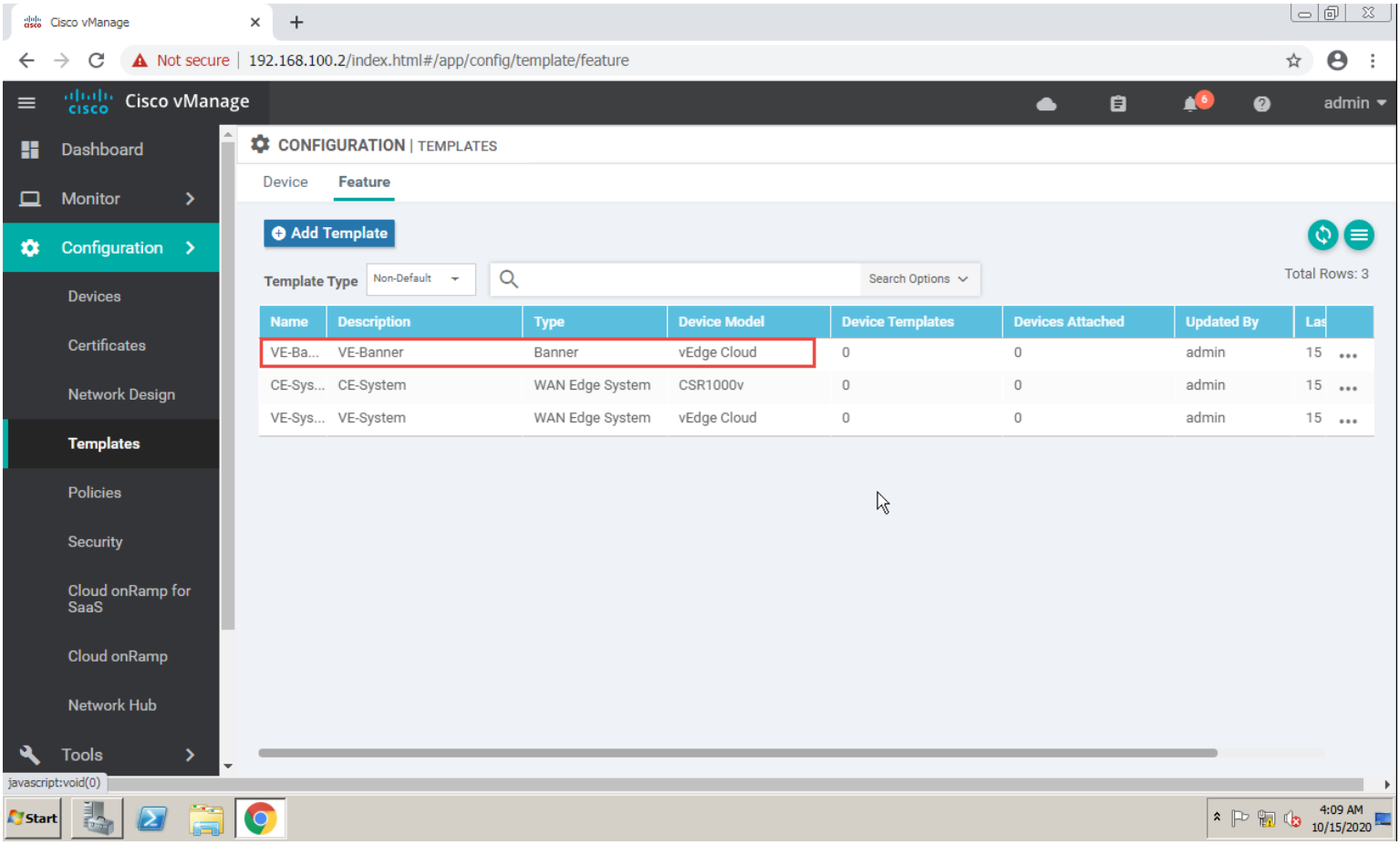


Lab 14 – Configuring Feature Template –Banner

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

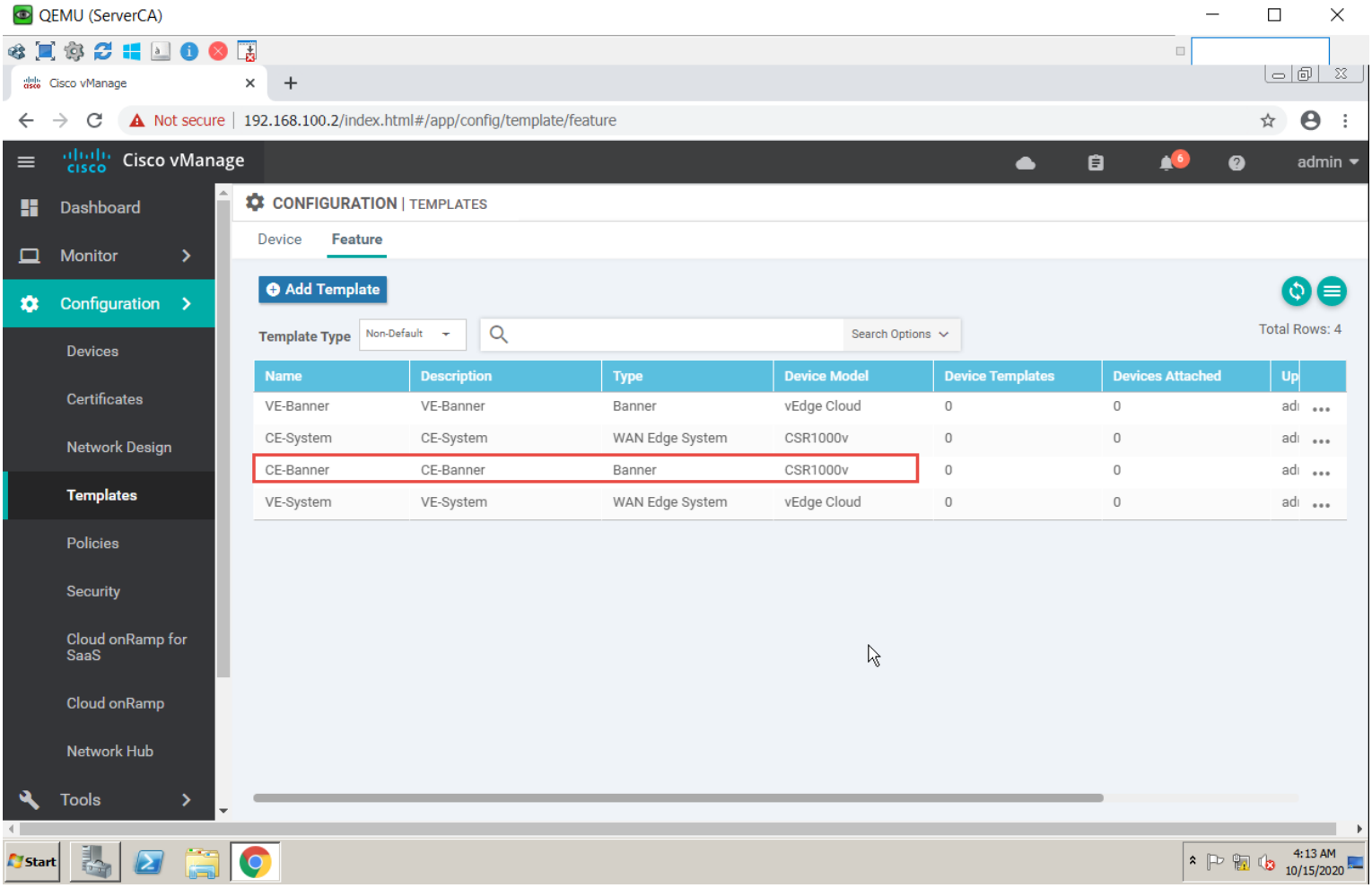
- In vManage, Navigate to **Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ OTHER TEMPLETES ➔ Banner**
- Configure the Banner parameters based on the following:
  - Template Name : VE-Banner
  - Description : VE-Banner
  - Login Banner: PNETLAB Authorized Users Only !!!
  - MOTD: Welcome To SD-PNETLAB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





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

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



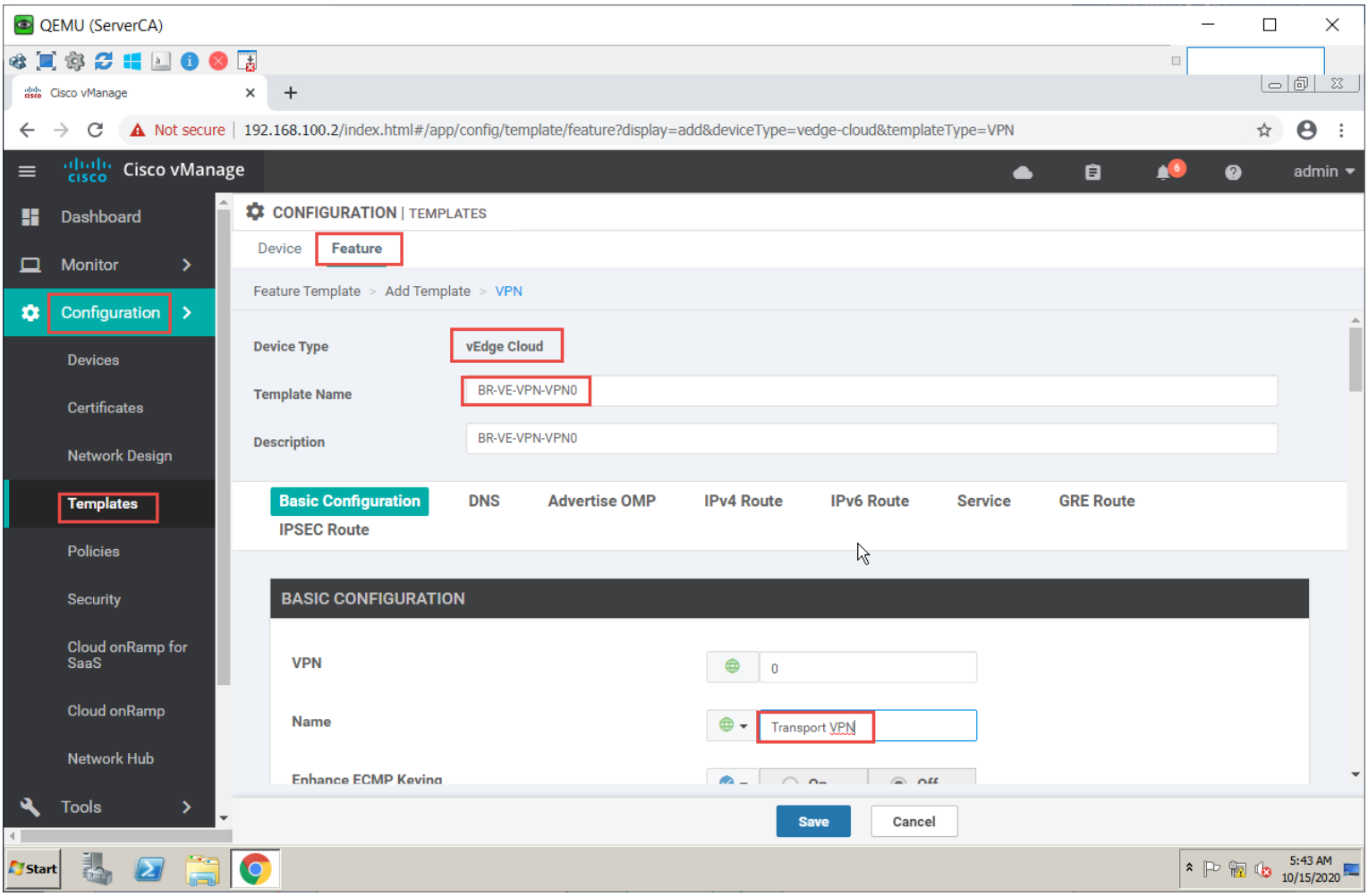
Lab 15 - Configuring Feature Templates -VPN & VPN Interfaces for VPN 0 & 512 —Branch Site(vEdges)

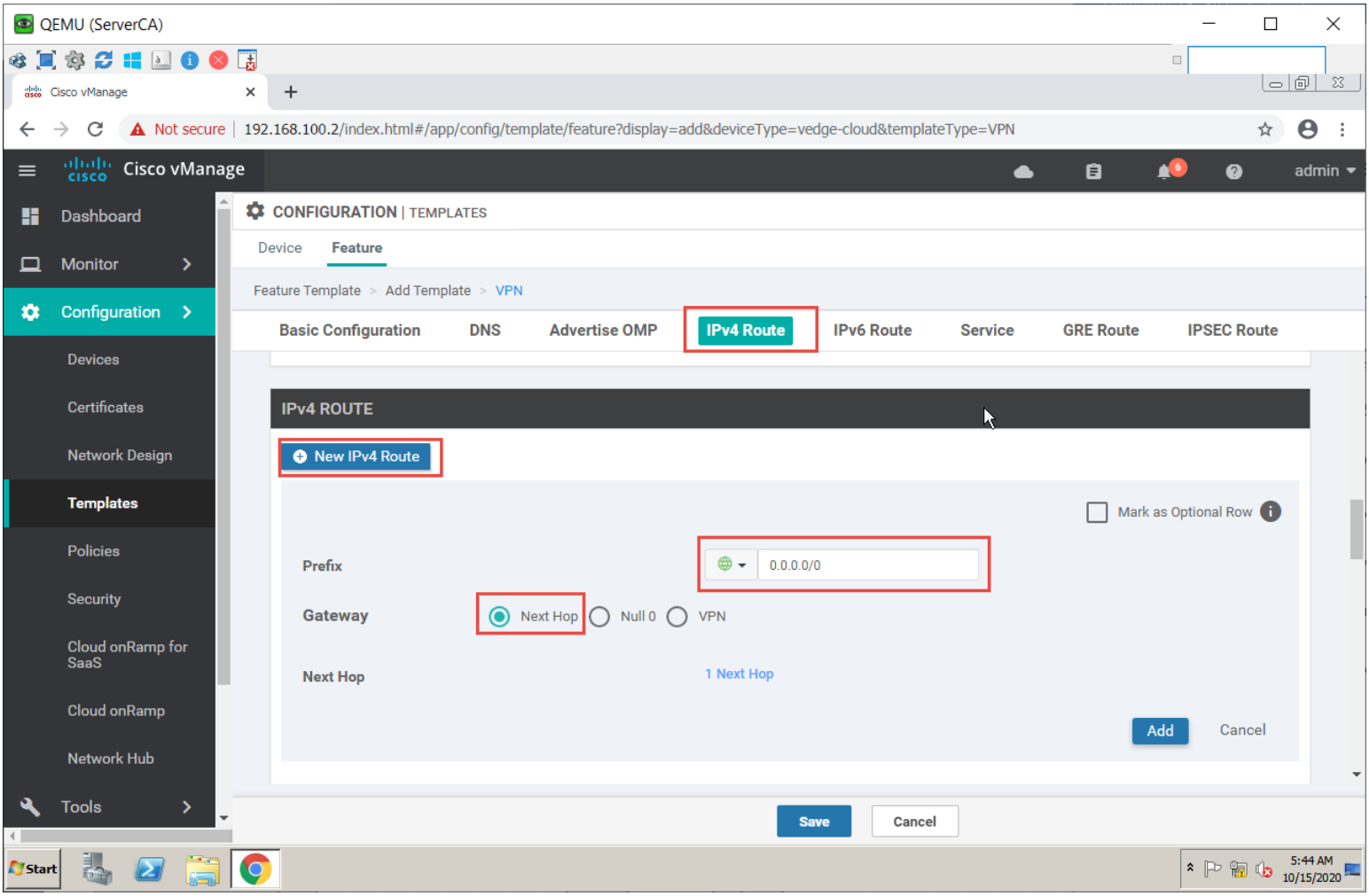
Task 1 – Configure a VPN Template to be used by all Branch vEdgeCloud Devices for VPN 0

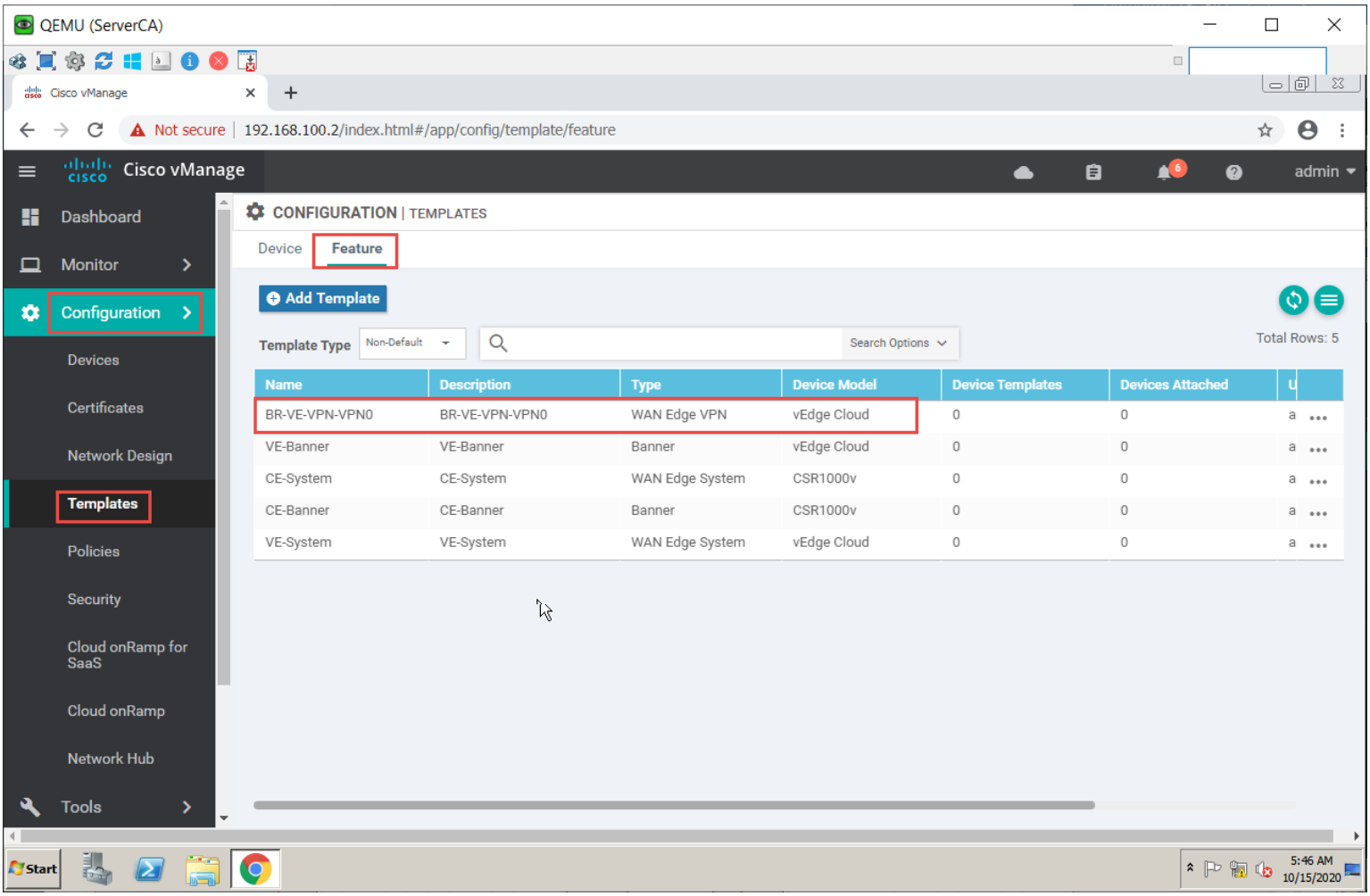
- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ VPN ➔ VPN
- Configure the VPN parameters based on the following:
  - Template Name: BR-VE-VPN-VPN0
  - Description: BR-VE-VPN-VPN0

  Basic Configuration
  - VPN ➔ Global: 0
  - Name ➔ Global: Transport VPN

  IPv4 Route
  - Prefix ➔ Global: 0.0.0.0/0
  - Next Hop ➔ Device Specific
- Click Save to save the Template.



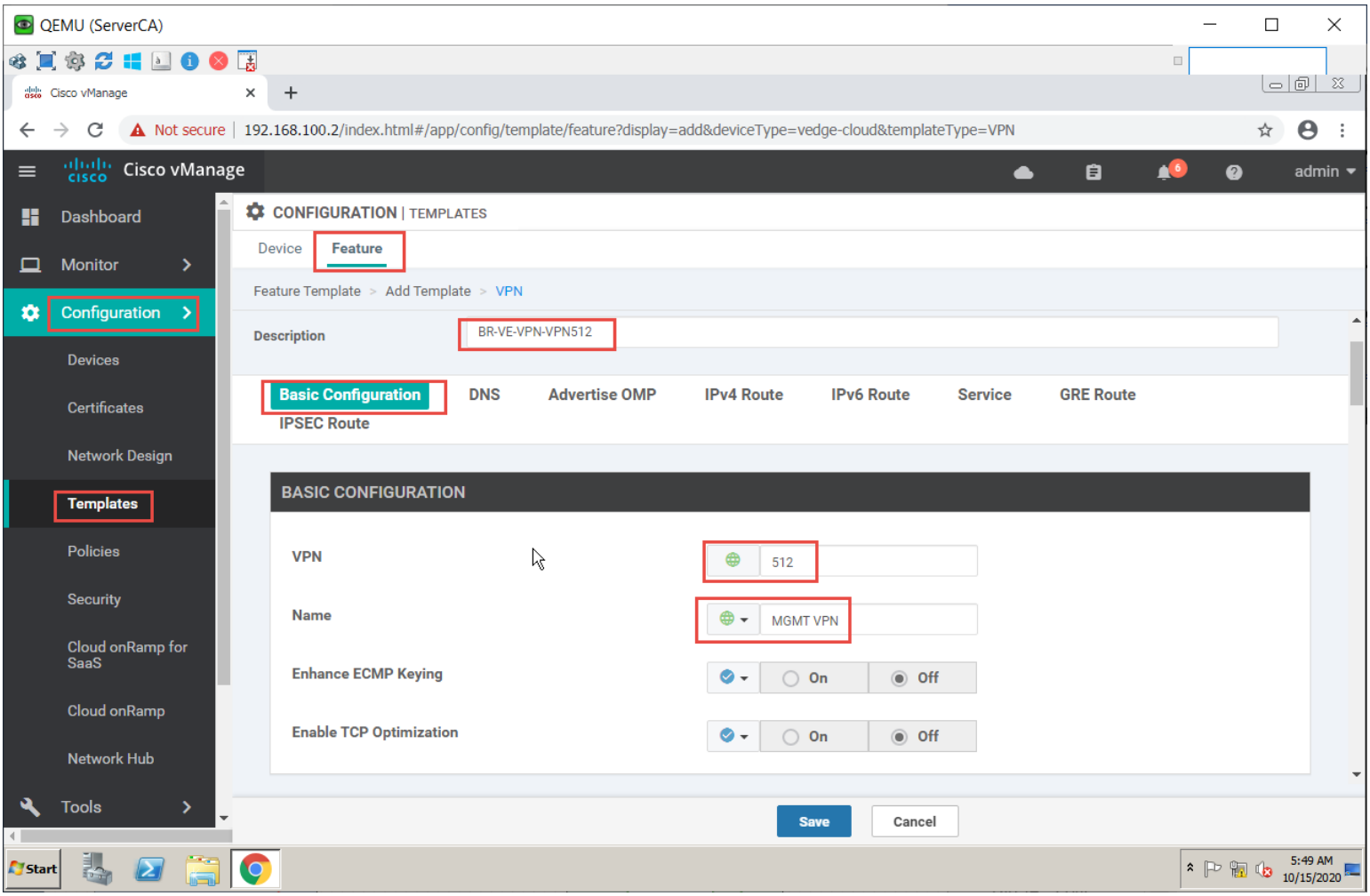

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > VPN
Basic Configuration
DNS
Advertise OMP
IPv4 Route
IPv6 Route
Service
GRE Route
IPSEC Route
IPv4 ROUTE
New IPv4 Route
Mark as Optional Row
Prefix
0.0.0.0/0
Gateway
Next Hop
Null 0
VPN
Next Hop
1 Next Hop
Add
Cancel
Save
Cancel
Start
5:44 AM
10/15/2020

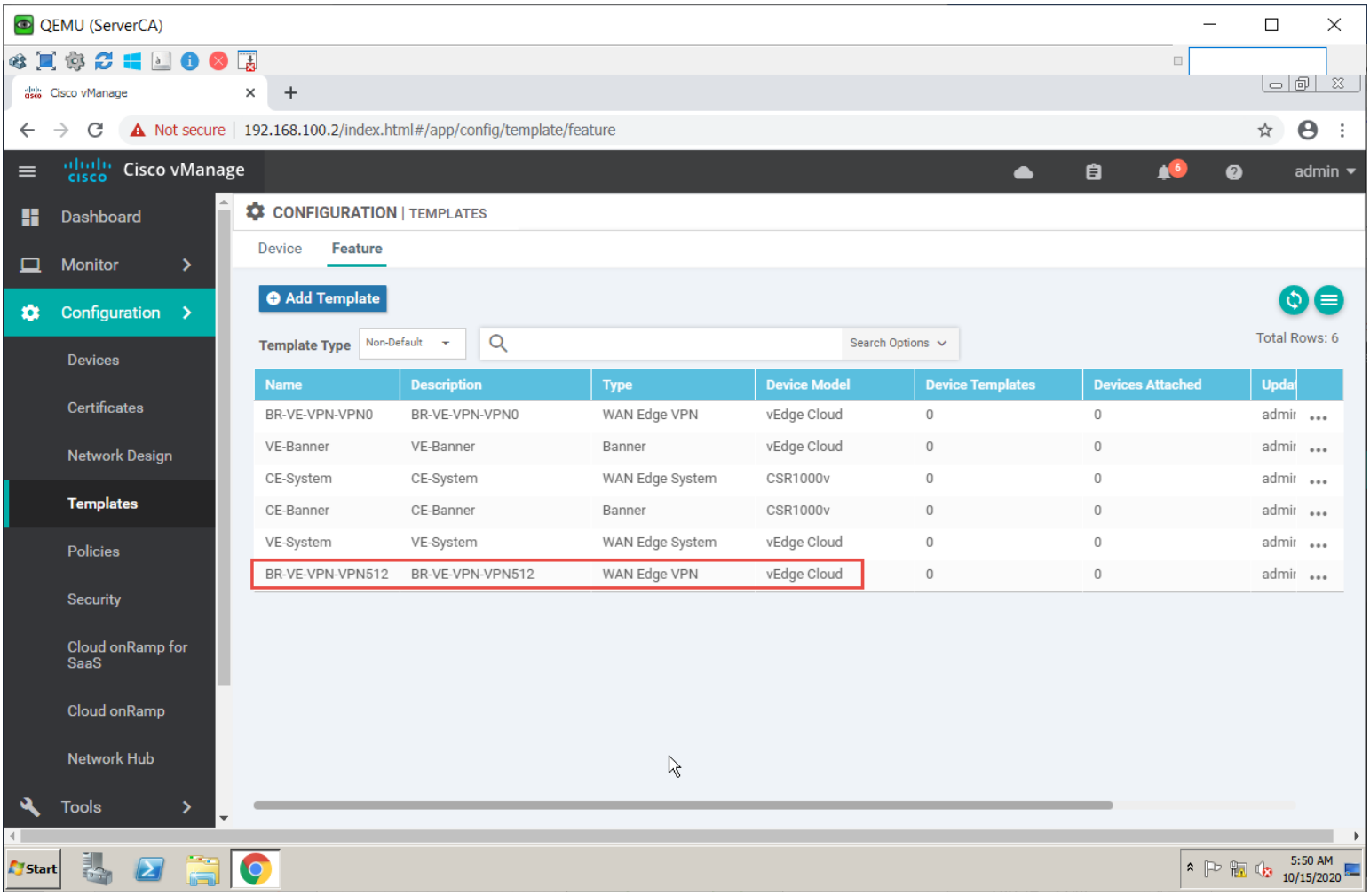


Task 2 – Configure a VPN Template to be used by all Branch vEdgeCloud Devices for VPN 512

- In vManage, **Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ VPN ➔ VPN**
- Configure the VPN parameters based on the following:
  - Template Name: BR-VE-VPN-VPN512
  - Description: BR-VE-VPN-VPN512

  Basic Configuration
  - VPN ➔ Global: 512
  - Name ➔ Global: MGMT VPN
- Click Save to save the Template.





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-VPN0-G0
    - Description: BR-VE-VPNINT-VPN0-G0

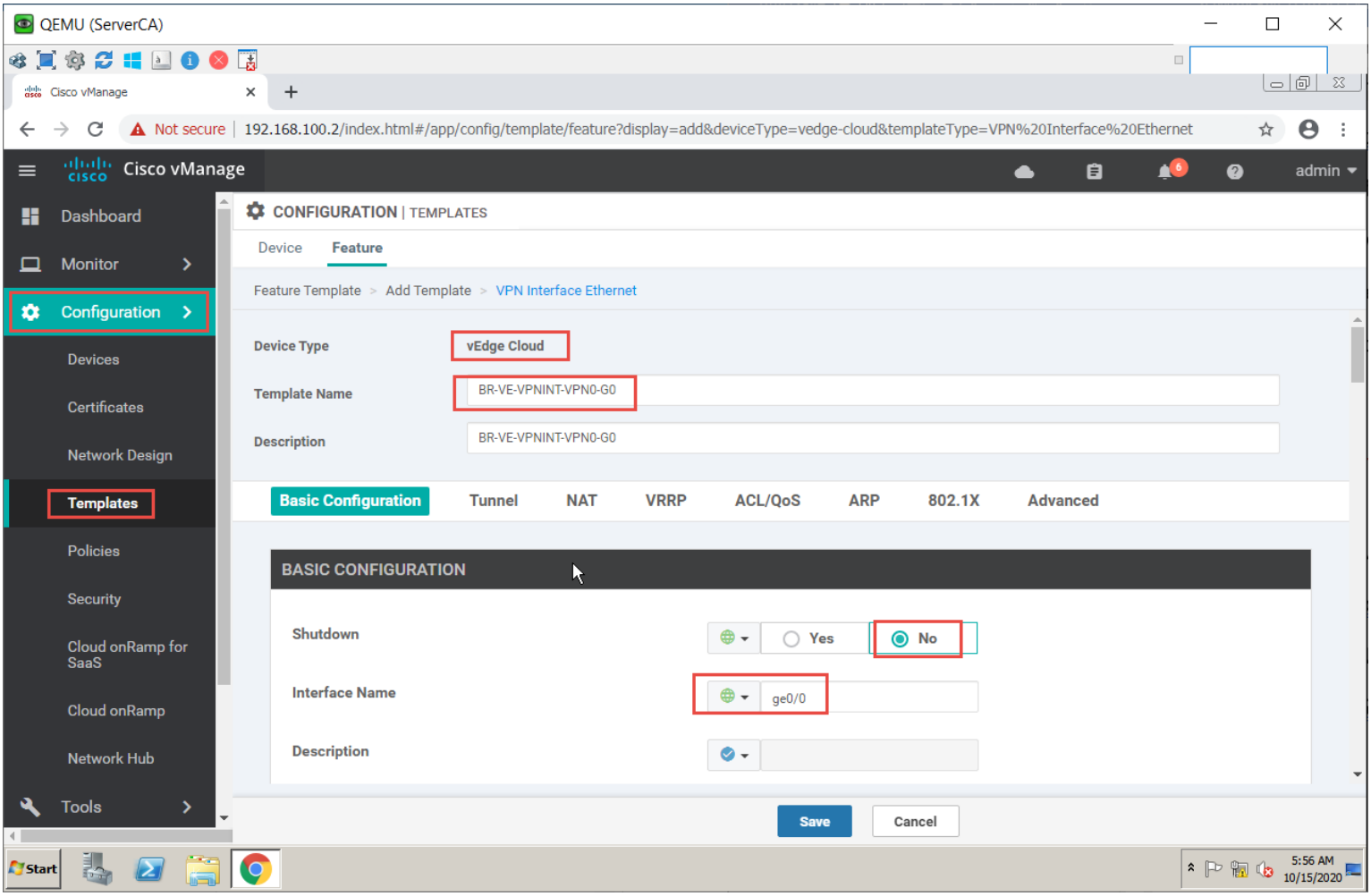
  Basic Configuration
    - Shutdown ➔ Global: No
    - Interface Name ➔ Global: Ge0/0
    - IPv4 Address ➔ Static ➔ Device Specific

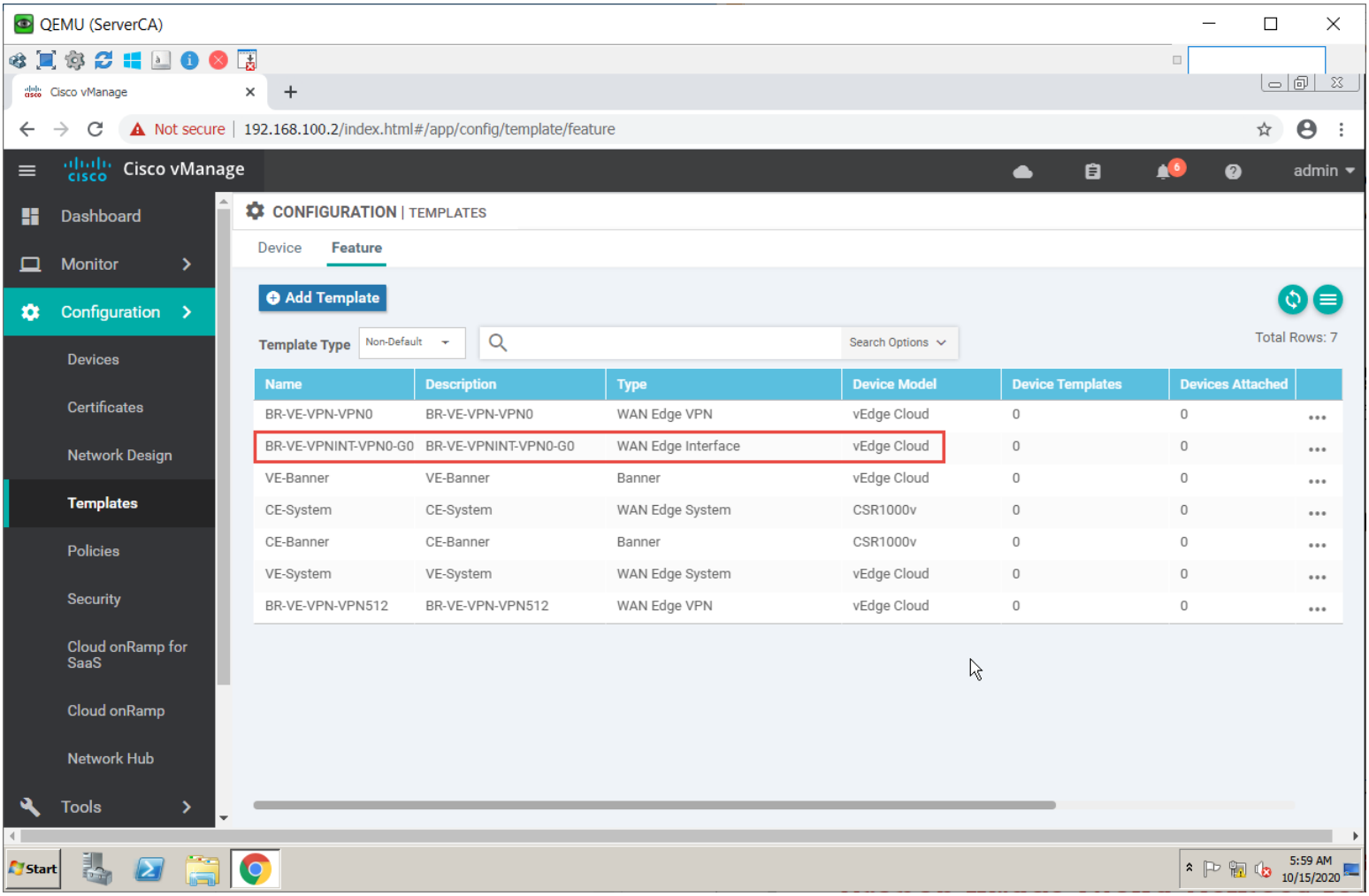
  Tunnel
    - Tunnel Inteface ➔ Global: On
    - Color ➔ Global: MPLS

  Allow Service
    - All ➔ Global: On

- NETCONF ➔ Global: On
- SSH ➔ Global: On

- Click Save to save the Template.





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

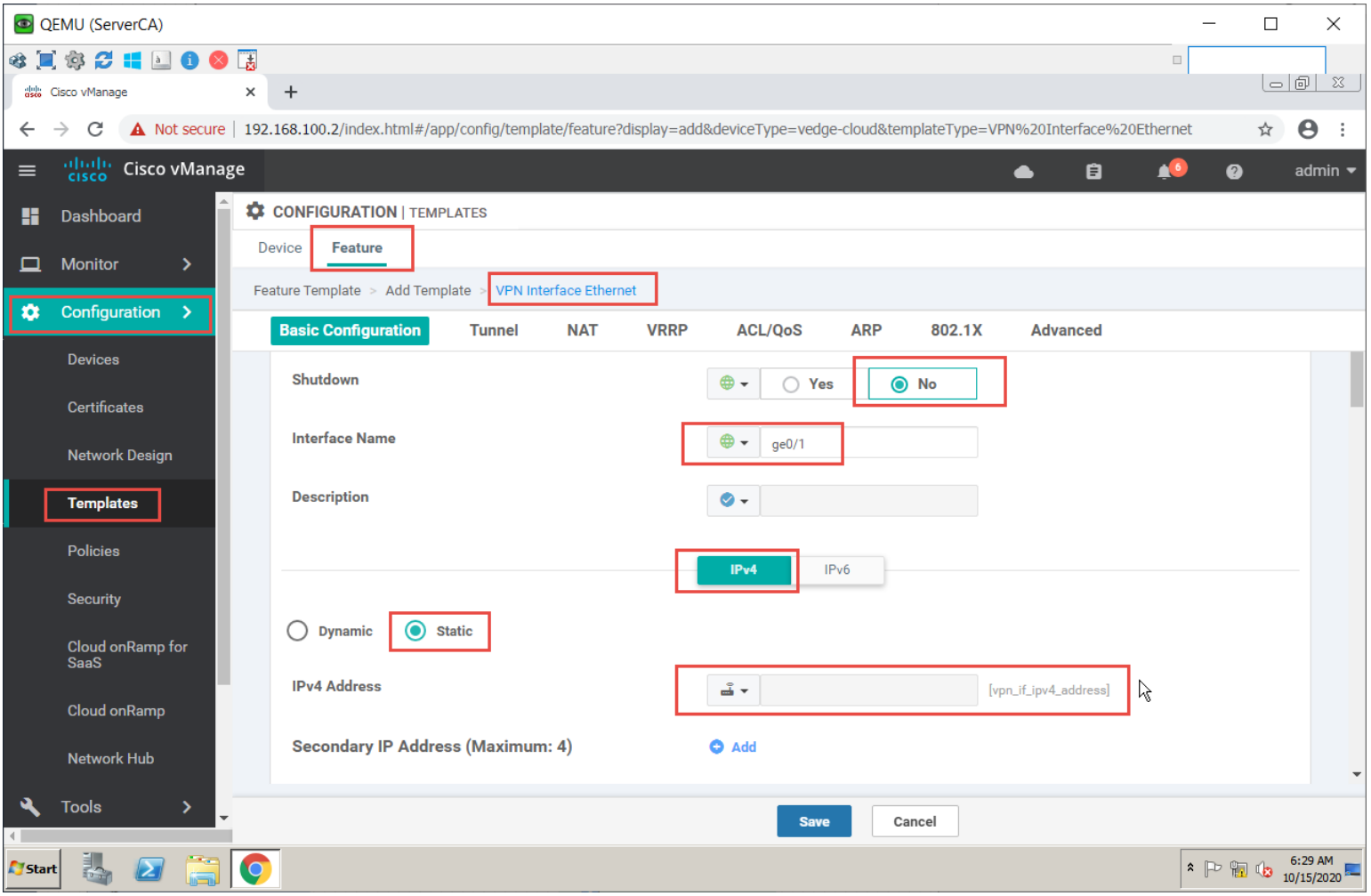
  Basic Configuration
    - Shutdown ➔ Global: No
    - Interface Name ➔ Global: Ge0/1
    - IPv4 Address ➔ Static ➔ Device Specific

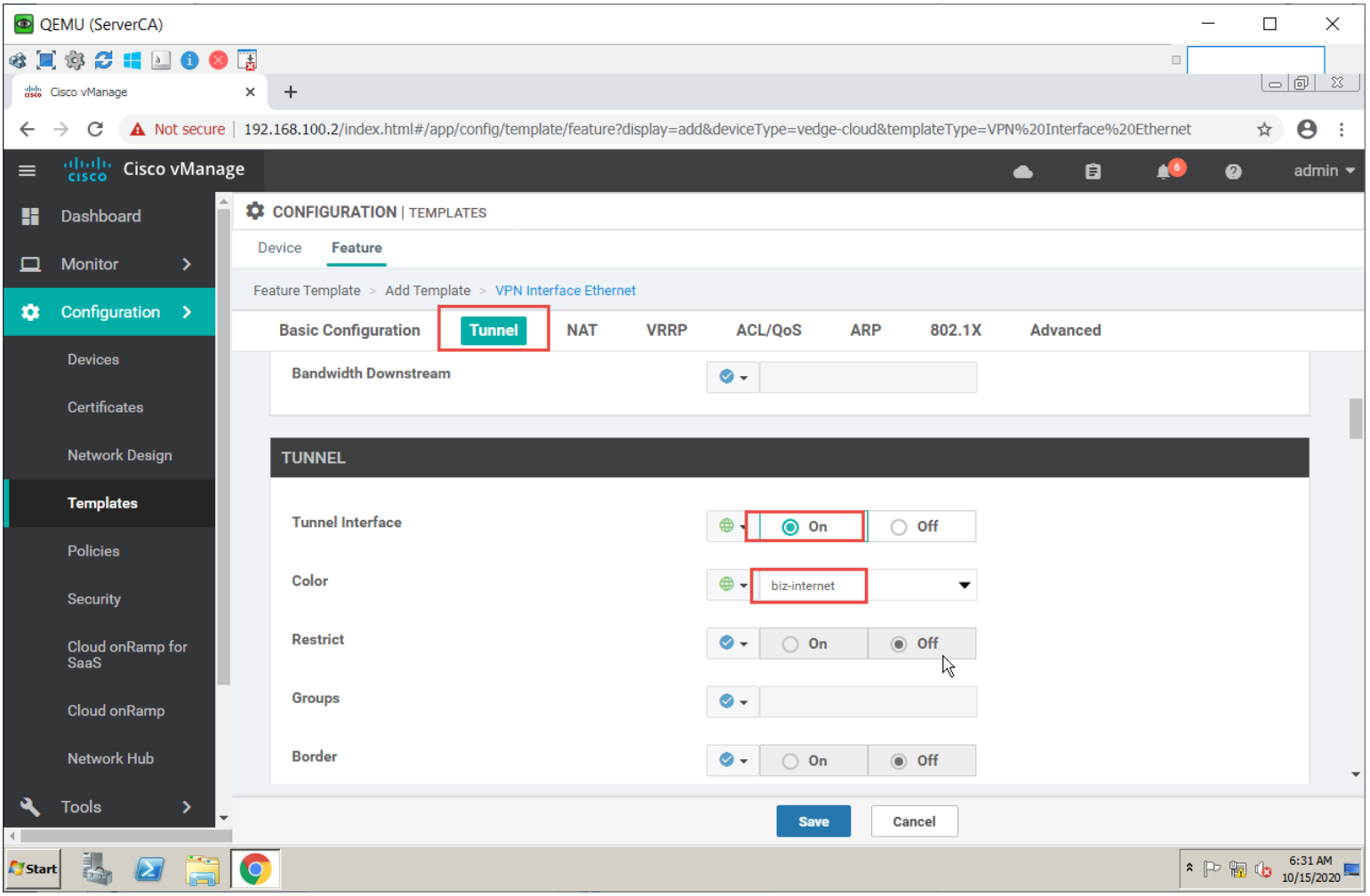
  Tunnel
    - Tunnel Inteface ➔ Global: On
    - Color ➔ Global: BIZ-Internet

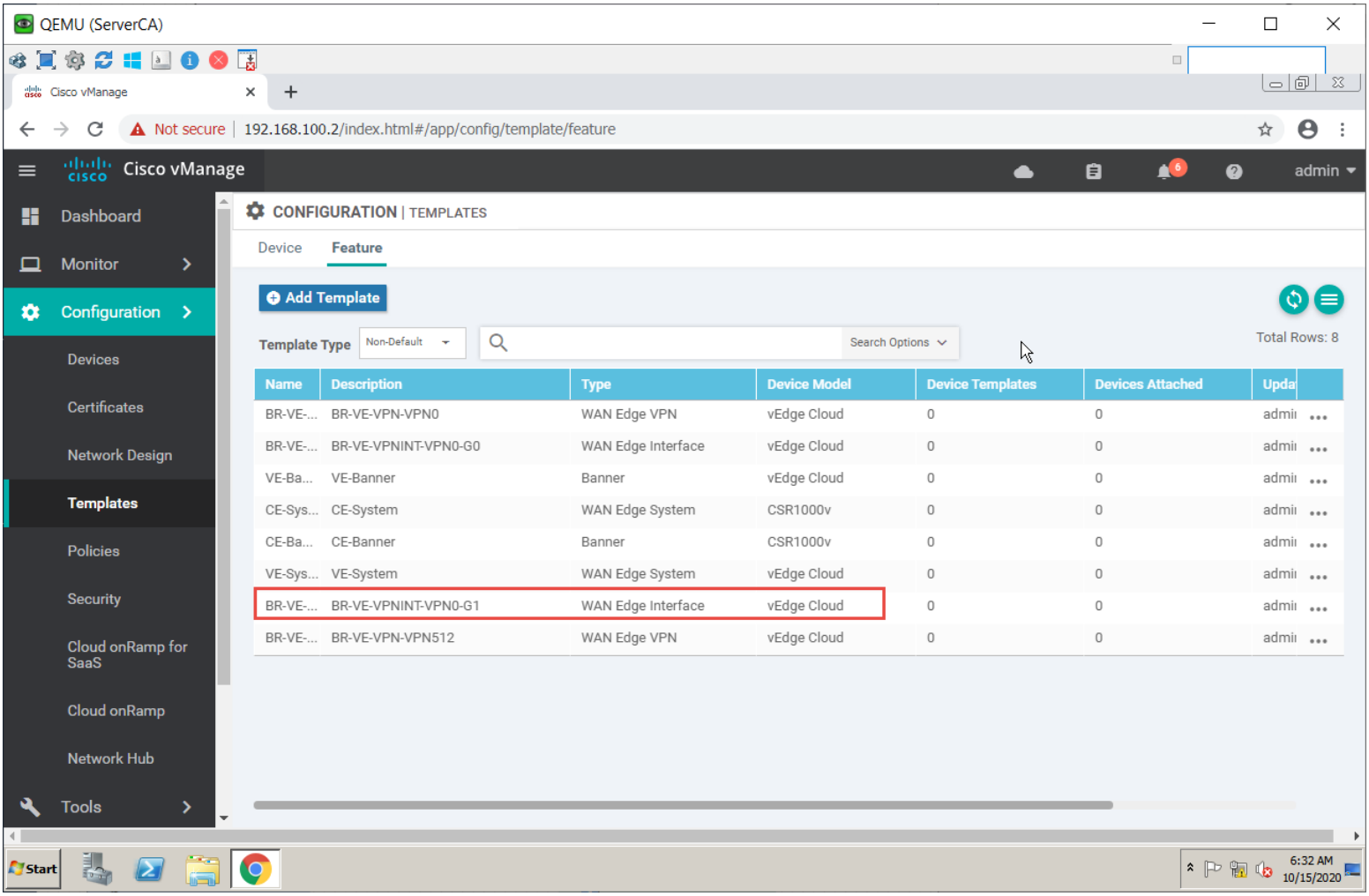
  Allow Service
    - All ➔ Global: On

- NETCONF ➔ Global: On
- SSH ➔ Global: On

- Click Save to save the Template.



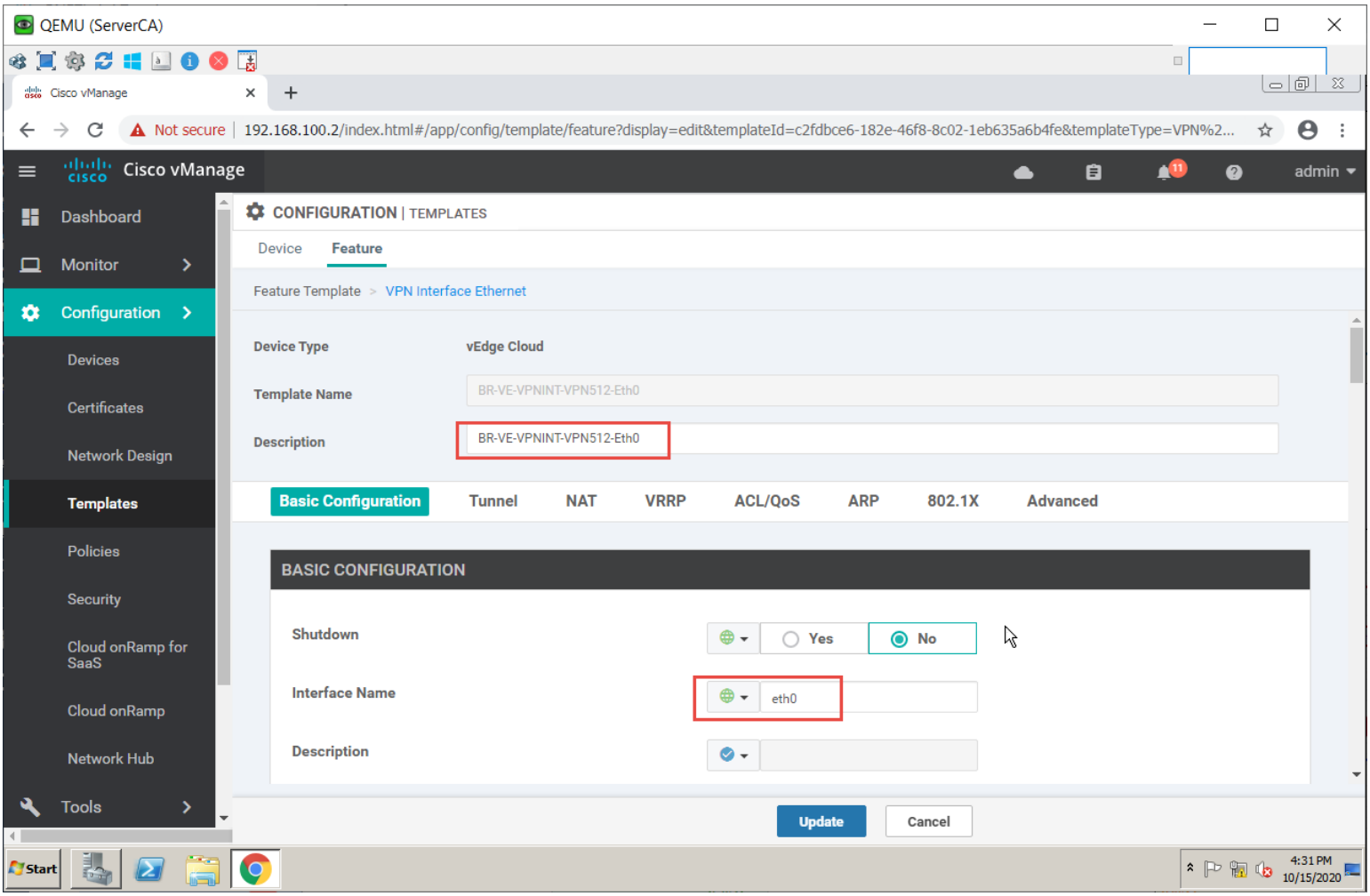

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN%20Interface%20Ethernet
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > VPN Interface Ethernet
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
Bandwidth Downstream
TUNNEL
Tunnel Interface
On
Off
Color
biz-internet
Restrict
On
Off
Groups
Border
On
Off
Save
Cancel
Start
6:31 AM
10/15/2020

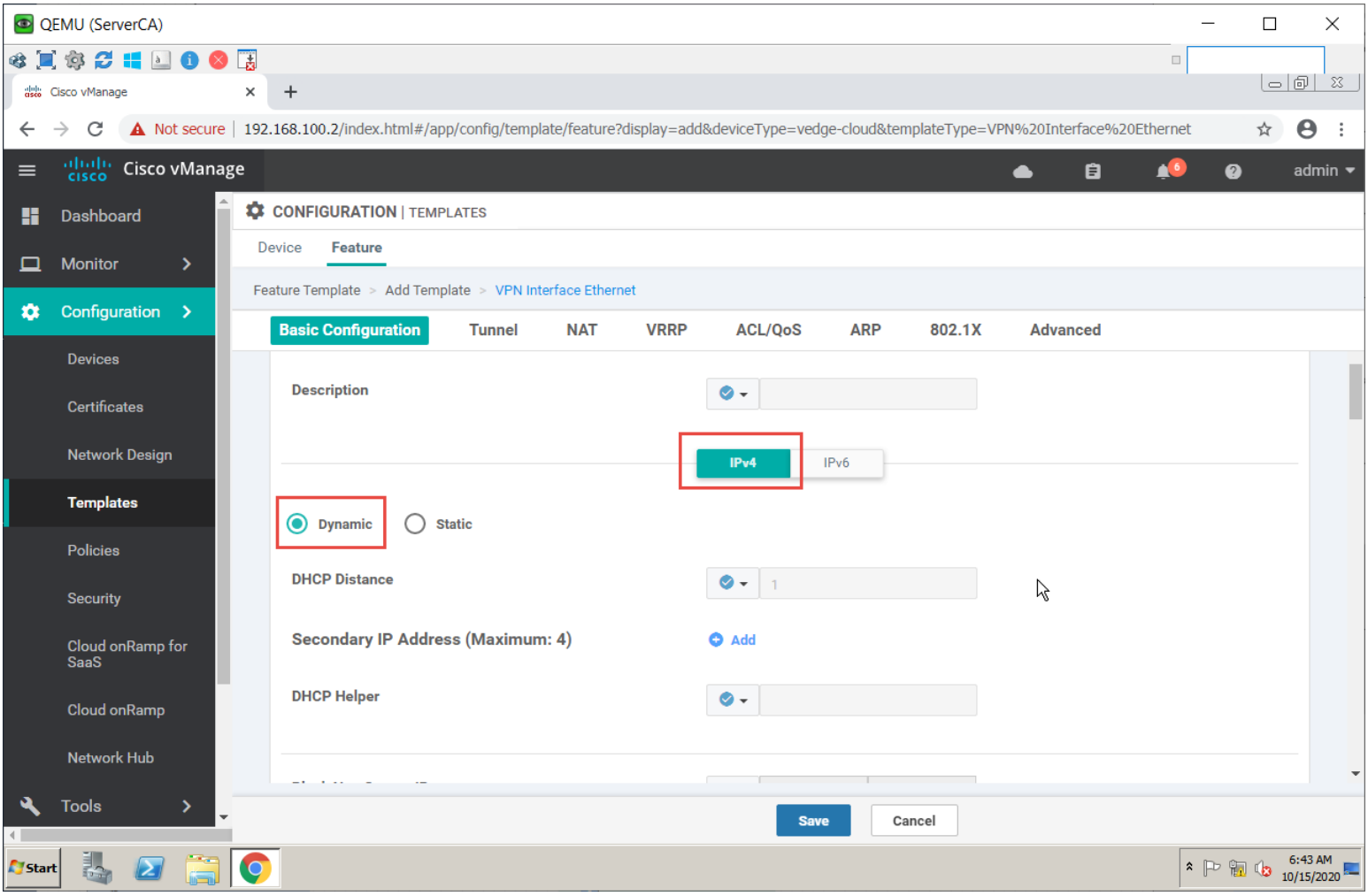


Task 5 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud Devices for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ VPN ➔ VPN Interface Ethernet
- Configure the VPN parameters based on the following:
  - Template Name: BR-VE-VPNINT-VPN512-Eth0
  - Description: BR-VE-VPNINT-VPN512-Eth02

  Basic Configuration
  - Shutdown -> Global: No
  - Interface Name -> Global: Eth0
  - IPv4 Address -> Dynamic
- Click Save to save the Template


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=edit&templateId=c2fdbce6-182e-46f8-8c02-1eb635a6b4fe&templateType=VPN%2...
Cisco vManage
admin
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 > VPN Interface Ethernet
Device Type
vEdge Cloud
Template Name
BR-VE-VPNINT-VPN512-Eth0
Description
BR-VE-VPNINT-VPN512-Eth0
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
BASIC CONFIGURATION
Shutdown
Yes
No
Interface Name
eth0
Description
Update
Cancel
Start
4:31 PM
10/15/2020


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN%20Interface%20Ethernet
Cisco vManage
admin
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 Interface Ethernet
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
Description
IPv4
IPv6
Dynamic
Static
DHCP Distance
1
Secondary IP Address (Maximum: 4)
Add
DHCP Helper
Save
Cancel
Start
6:43 AM
10/15/2020

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

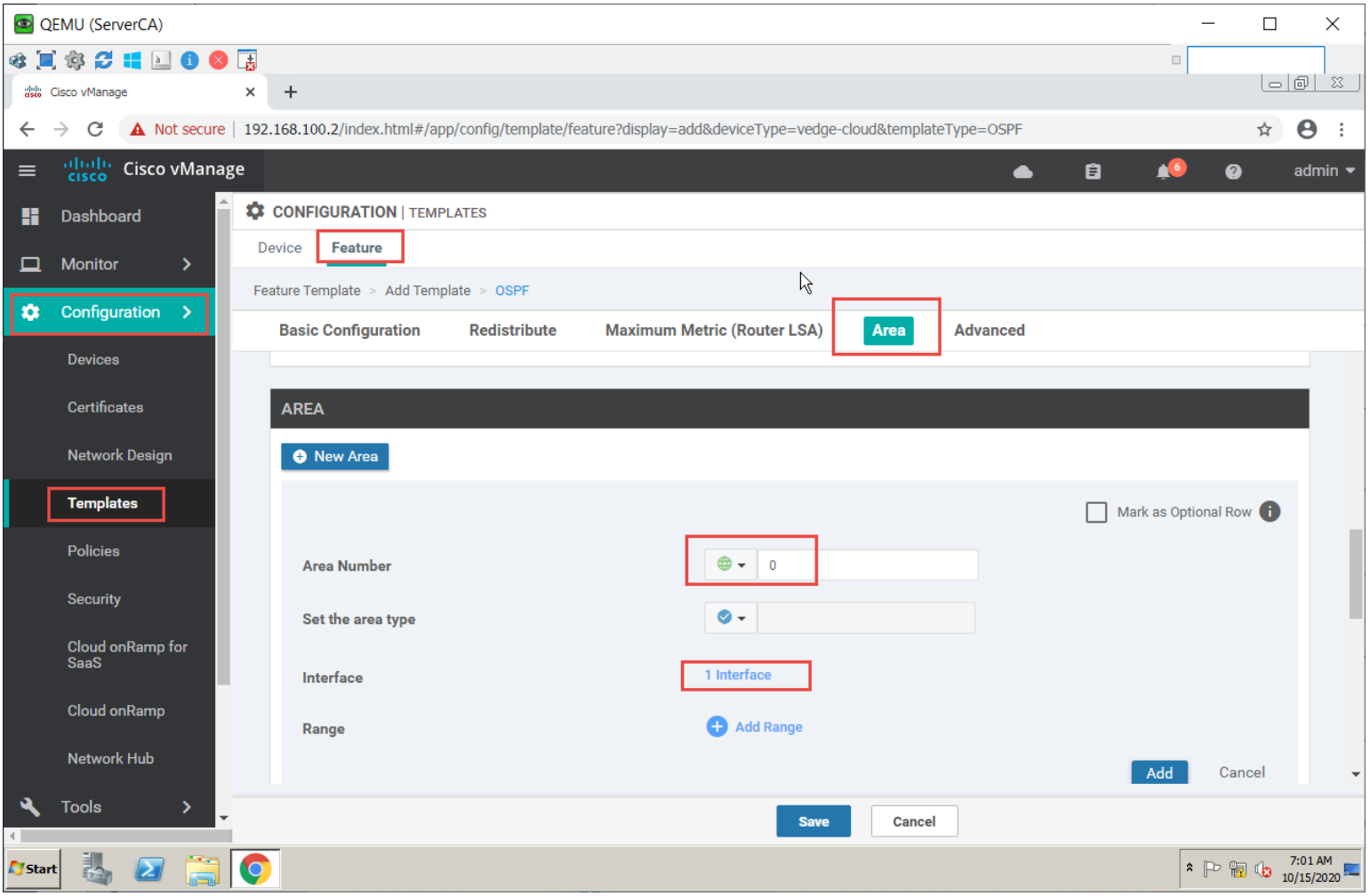
Task 1 – Configure a OSPF Template to be used by all Branch vEdgeCloud Devices for VPN 0

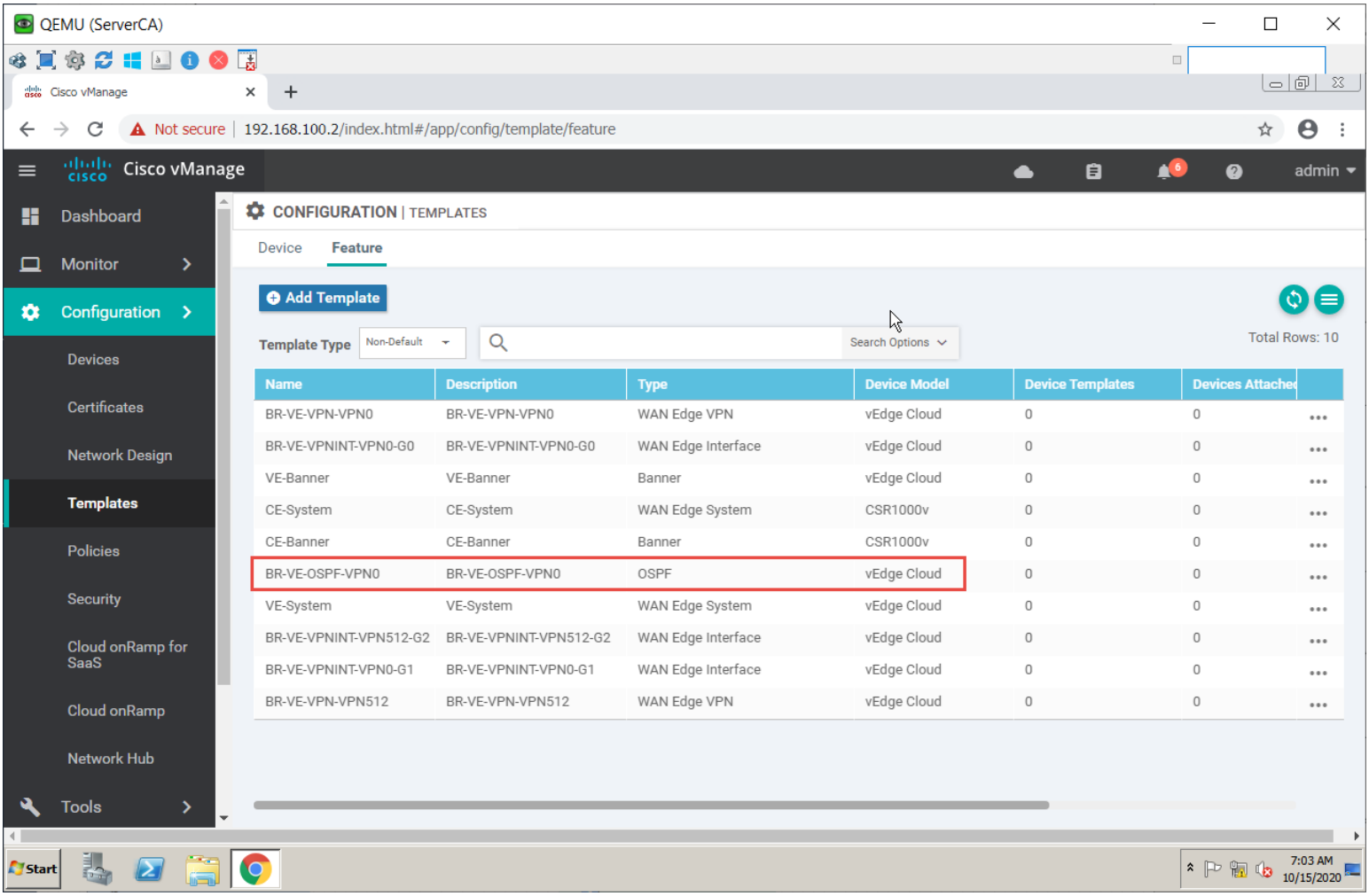
- In vManage, **Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ Other Templates ➔ OSPF**
- Configure the OSPF parameters based on the following:
    - Template Name: BR-VE-OSPF-VPN0
    - Description: BR-VE-OSPF-VPN0

  Area Configuration
    - Area Number ➔ Global: 0
    - Area Type ➔ Default

  Interface Configuration
    - Interface Name: Ge0/0

  Advanced
    - OSPF Network Type: Point-to-Point
- 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?display=add&deviceType=vedge-cloud&templateType=OSPF
Cisco vManage
admin
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 > OSPF
Basic Configuration
Redistribute
Maximum Metric (Router LSA)
Area
Advanced
AREA
New Area
Mark as Optional Row
Area Number
0
Set the area type
Interface
1 Interface
Range
Add Range
Add
Cancel
Save
Cancel
Start
7:01 AM
10/15/2020



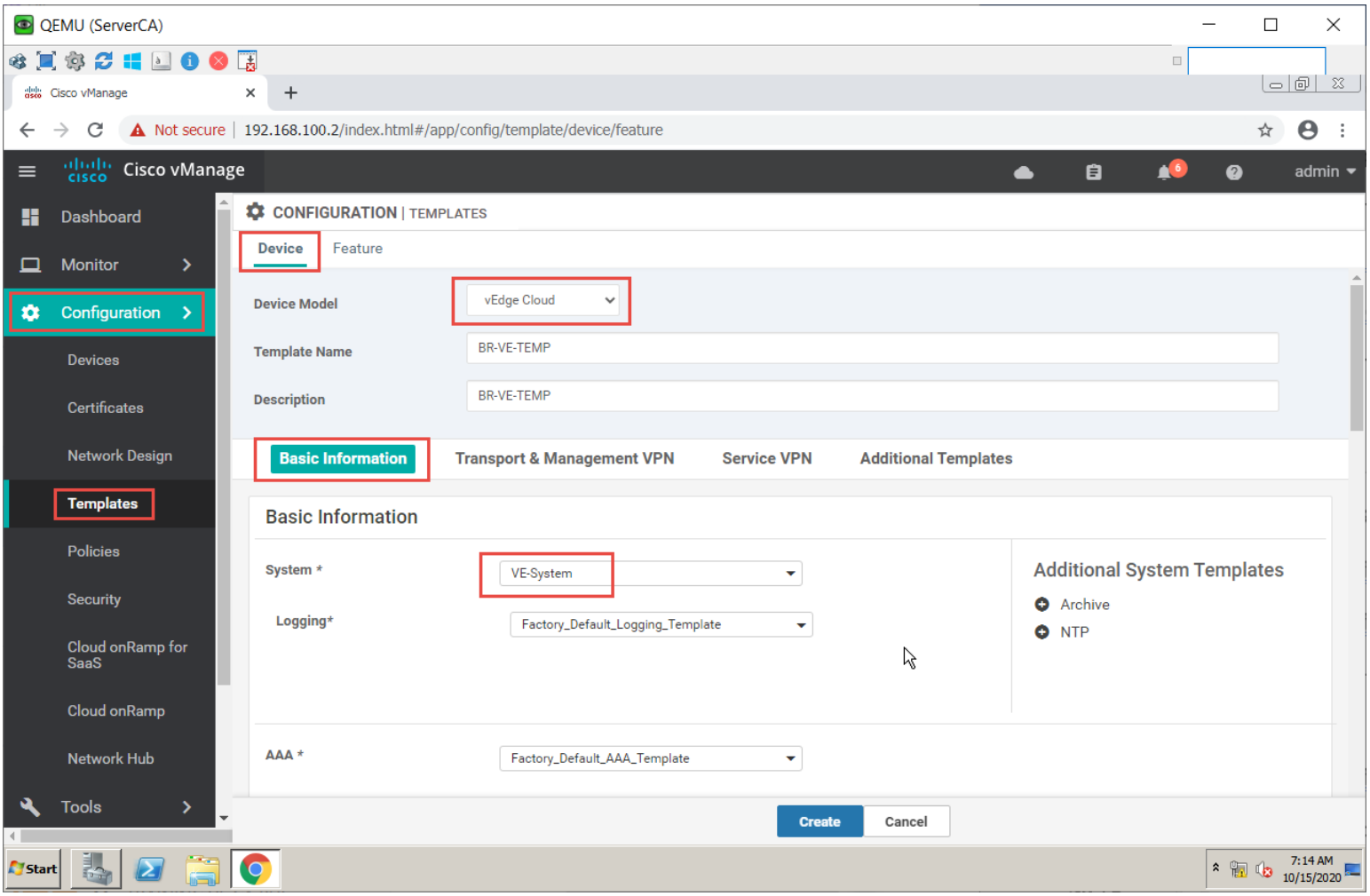
Lab 17 - Configuring and Deploying Device Templates for vEdge – Branch Site(vEdge2)

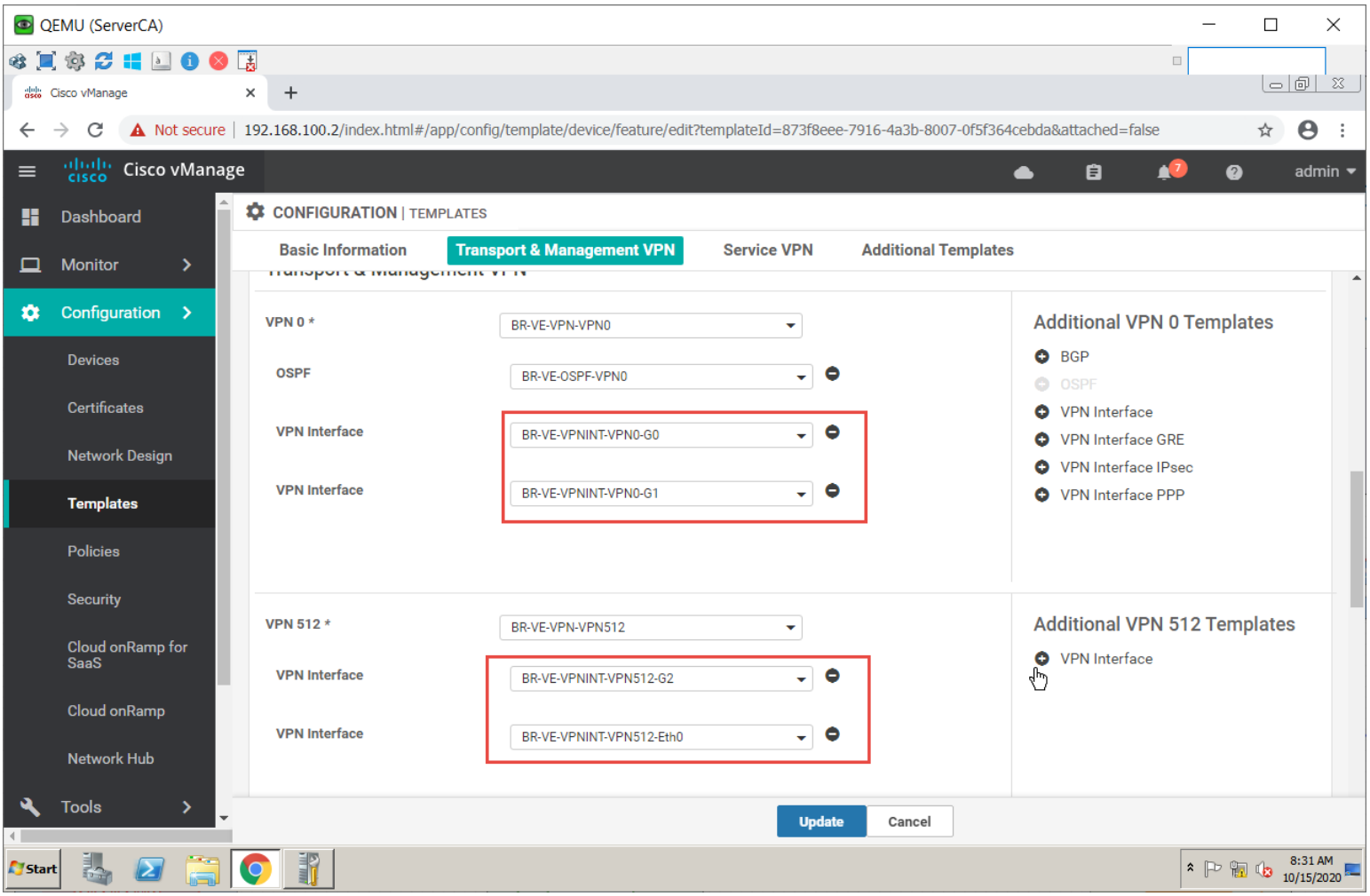
Task 1 – Configure a Device Template for Branch vEdge Devices.

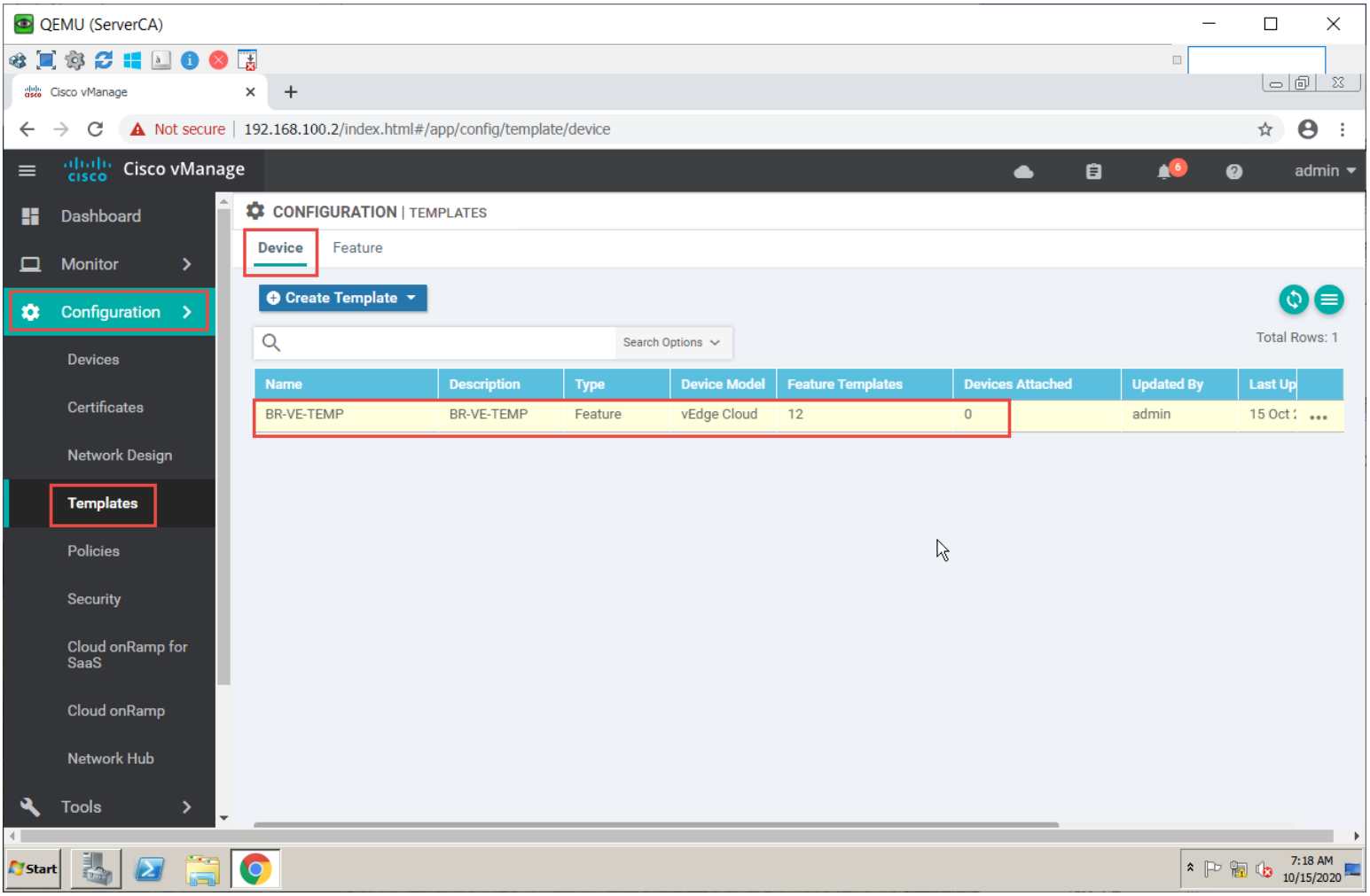
- In vManage, Navigate to Configuration ➔ Templates ➔ Device ➔ Create Template ➔ vEdge Cloud
- Configure the Device Template based on the following:
    - Template Name: BR-VE-TEMP
    - Description: BR-VE-TEMP

  Basic Information
    - System ➔ VE-System

  Transport & Management
    - VPN 0: BR-VE-VPN-VPN0
    - VPN Interface: BR-VE-VPNINT-VPN0-G0
    - VPN Interface: BR-VE-VPNINT-VPN0-G1
    - OSPF: BR-VE-OSPF-VPN0
    - VPN 512: BR-VE-VPN-VPN512
    - VPN Interface: BR-VE-VPNINT-VPN512-Eth0
- Click Create to save the Template.

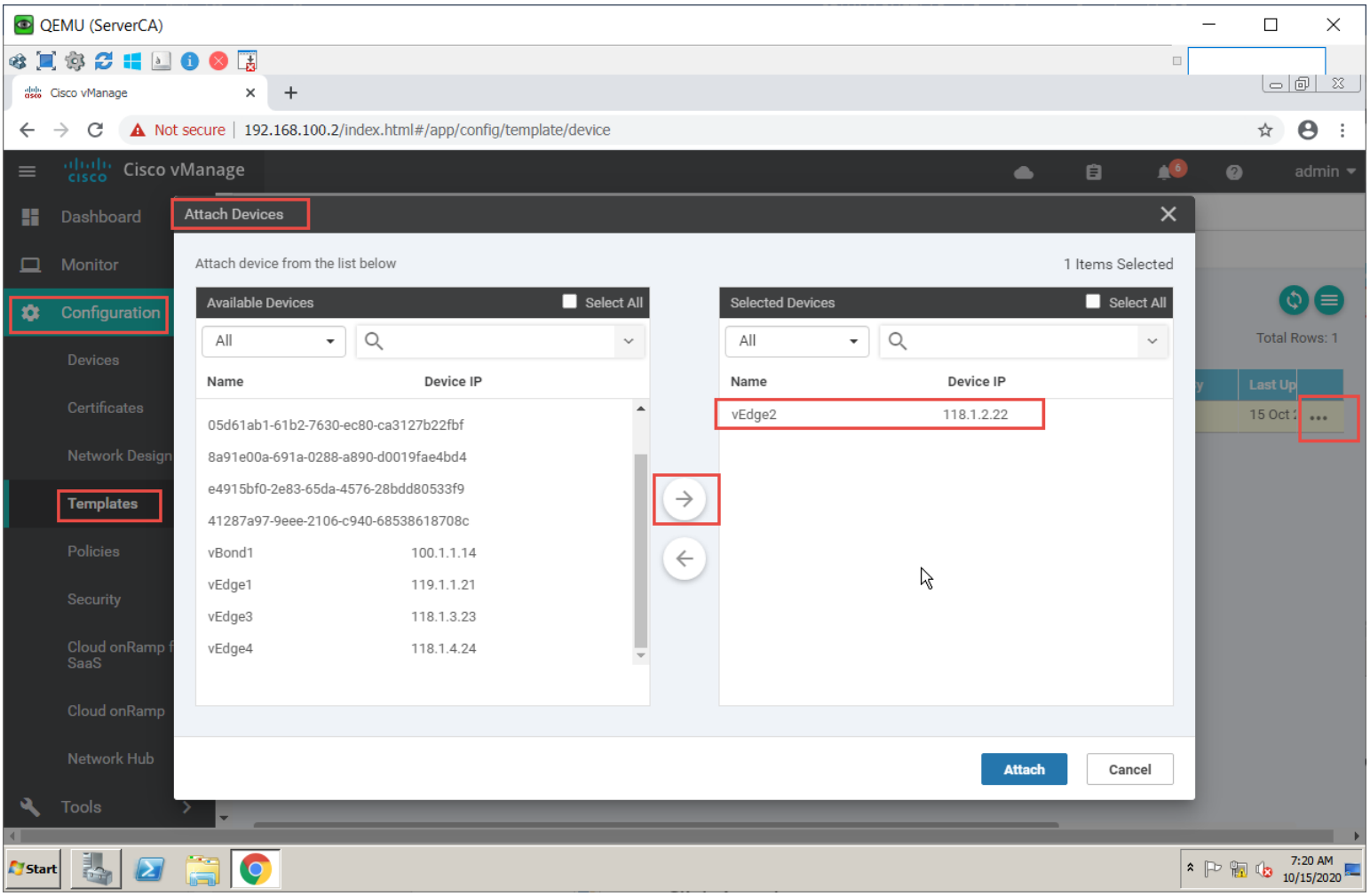

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/device/feature
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Device
Feature
Device Model
vEdge Cloud
Template Name
BR-VE-TEMP
Description
BR-VE-TEMP
Basic Information
Transport & Management VPN
Service VPN
Additional Templates
Basic Information
System *
VE-System
Logging*
Factory_Default_Logging_Template
Additional System Templates
Archive
NTP
AAA *
Factory_Default_AAA_Template
Create
Cancel
Start
7:14 AM
10/15/2020


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/device/feature/edit?templateId=873f8eee-7916-4a3b-8007-0f5f364cebda&attached=false
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Basic Information
Transport & Management VPN
Service VPN
Additional Templates
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
Additional VPN 0 Templates
BGP
OSPF
VPN Interface
VPN Interface GRE
VPN Interface IPsec
VPN Interface PPP
VPN 512 *
BR-VE-VPN-VPN512
VPN Interface
BR-VE-VPNINT-VPN512-G2
VPN Interface
BR-VE-VPNINT-VPN512-Eth0
Additional VPN 512 Templates
VPN Interface
Update
Cancel
Start
8:31 AM
10/15/2020



Task 2 – Attach vEdge2 to the Device Template

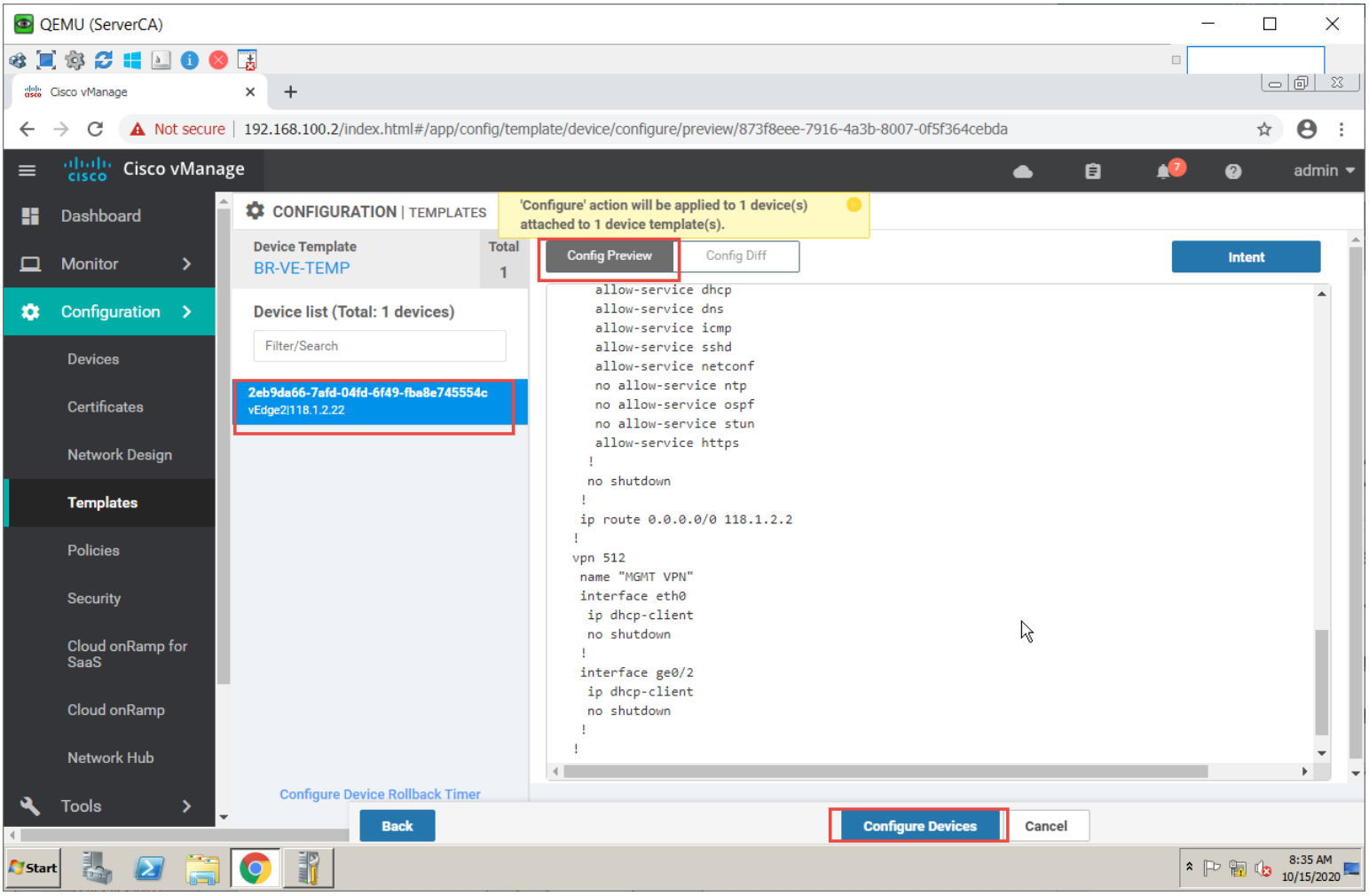
- In vManage, **Navigate to Configuration ➔ Templates ➔ Device ➔ BRVE-TEMP**.
- Click on "…" towards the right-hand side.
- Click Attach Devices.
- Select vEdge2 and click the "➔" button.
- Click Attach.

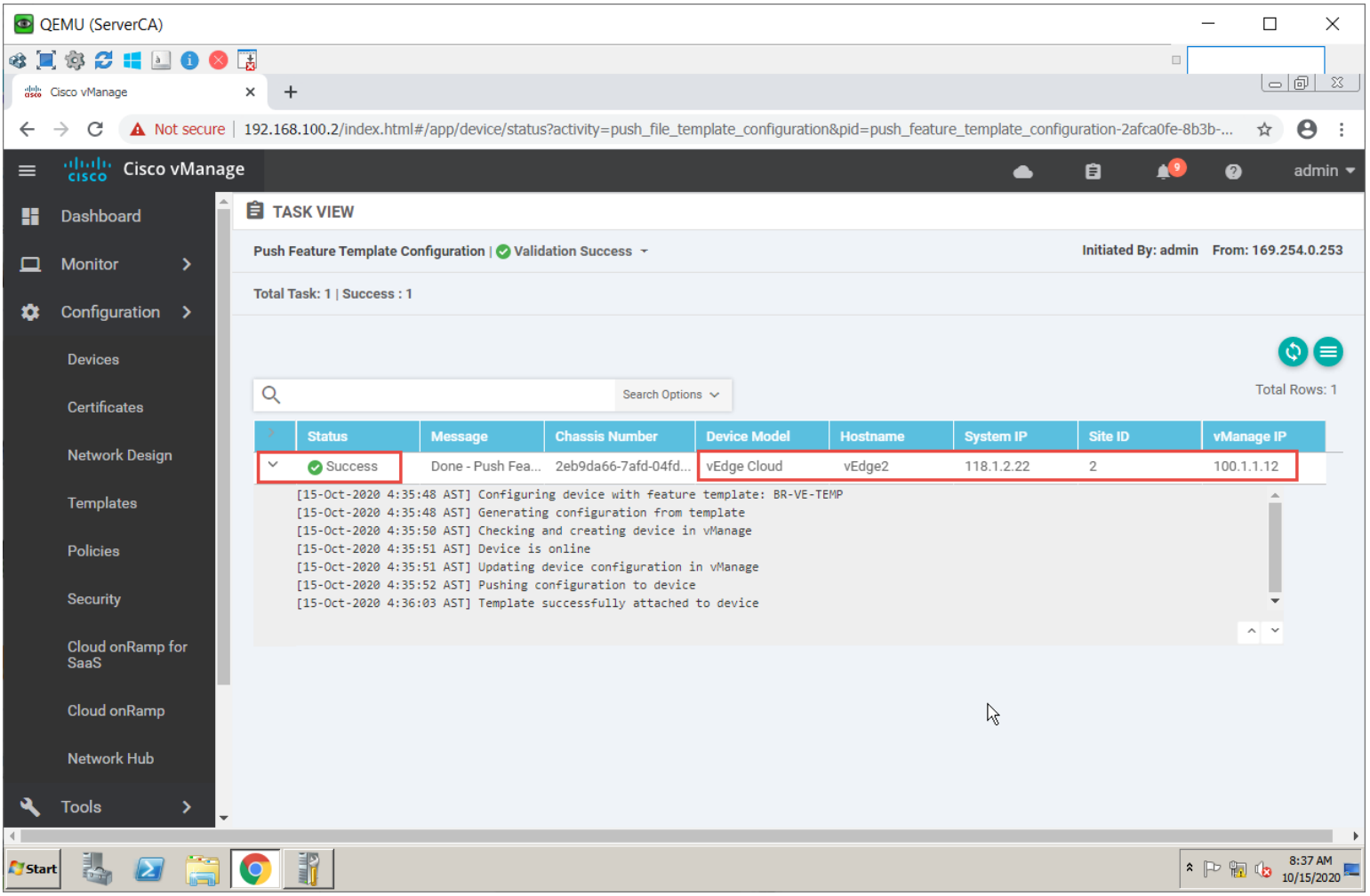


Task 3 – Configure the Variable Parameters for the Feature Templates

- vEdge2 will appear in the window.
- Click on "…" towards the right-hand side.
- Click Edit Device Template.
- Configure the variables based on the following:
    - Default Gateway for VPN0: 118.1.2.2
    - Interface IP for Ge0/1: 118.1.2.1/24
    - Interface IP for Ge0/0: 10.1.12.1/24
    - Hostname: vEdge-2
    - System IP: 118.1.2.22
    - 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.




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
admin
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
Initiated By: admin From: 169.254.0.253
Total Task: 1 | Success : 1
Search Options
Total Rows: 1
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
Start
8:37 AM
10/15/2020

vEdge2

```
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password $6$siwKBQ==$wT2lUa9BSreDPI6gB8sl4E6PAJoVXgMbgv/whJ8F1C6sWdRazdxorYYTLrL6syiG6qnLABTnrE96HJiKF6QRq1
  !
 !
 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
  tunnel-interface
   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
       SOURCE                                                                DEAD
VPN    IP ADDRESS       INTERFACE        ROUTER ID        STATE        PRIORITY  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
```

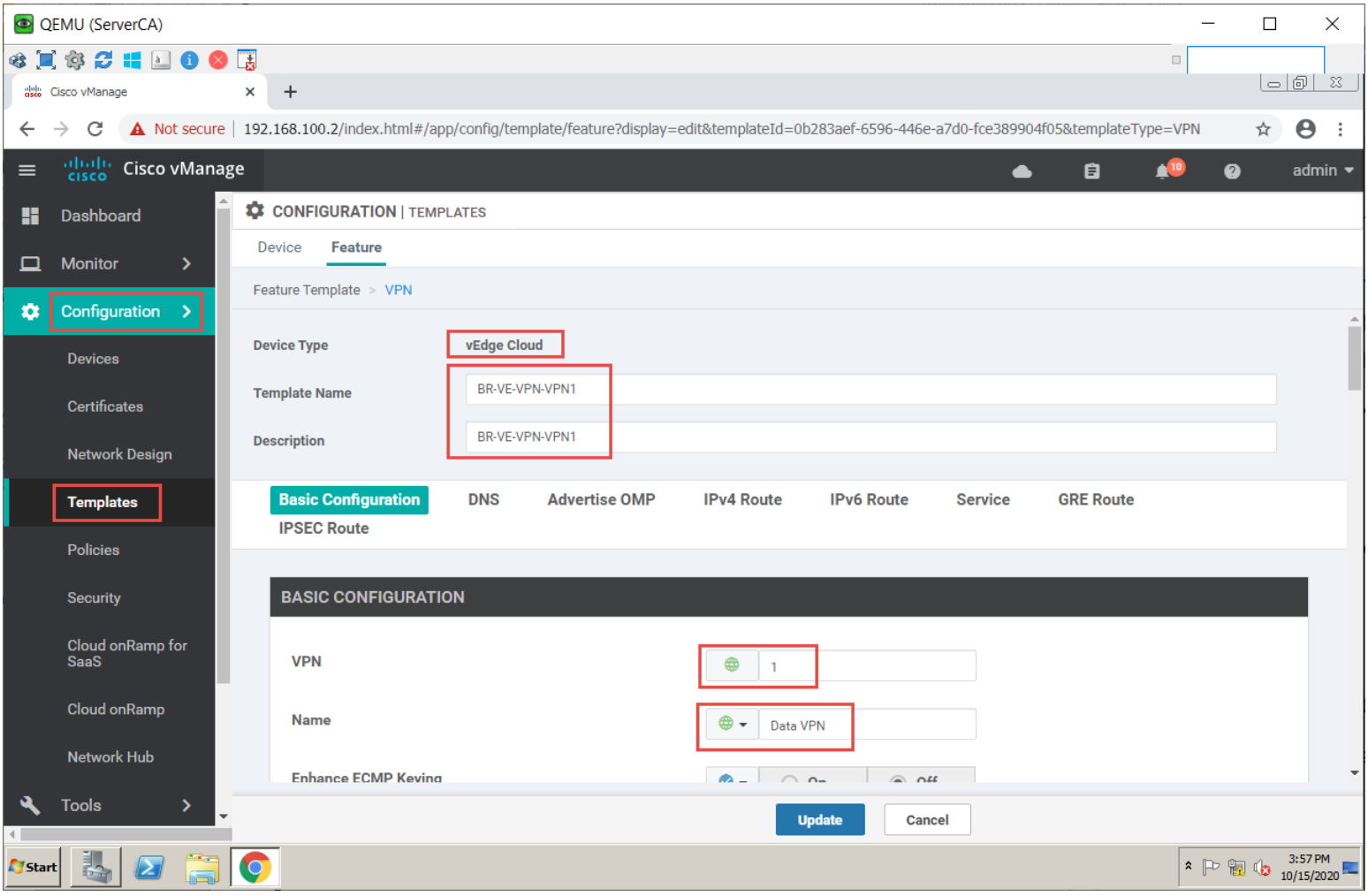
```
ip ospf network point-to-point
!
Interface Loopback2
ip address 192.168.52.1 255.255.255.0
ip ospf network point-to-point
!
Interface Loopback3
ip address 192.168.53.1  255.255.255.0
ip ospf network point-to-point
!
router ospf 1
network 172.175.1.0 0.0.0.255 area 0
network 192.168.0.0 0.0.255.255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

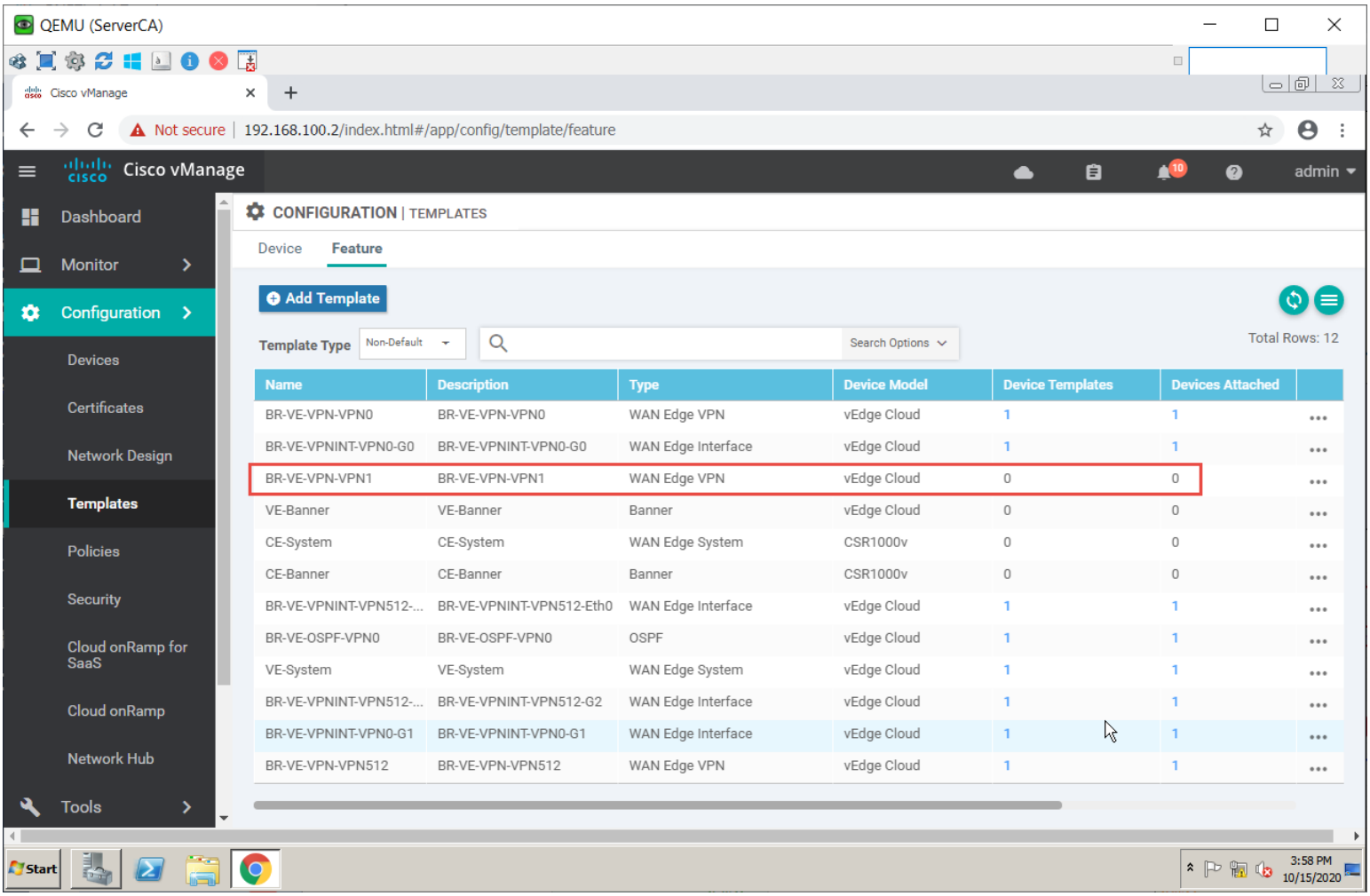
Lab 19 - Configuring Feature Templates –Service VPN – VPN, VPN Interface and Internal Routing – Branch Site (vEdges)

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:
  - Template Name: BR-VE-VPN-VPN1
  - Description: BR-VE-VPN-VPN1

  Basic Configuration
  - VPN ➔ Global: 1
  - Name ➔ Global: Data VPN
- Click Save to save the Template.

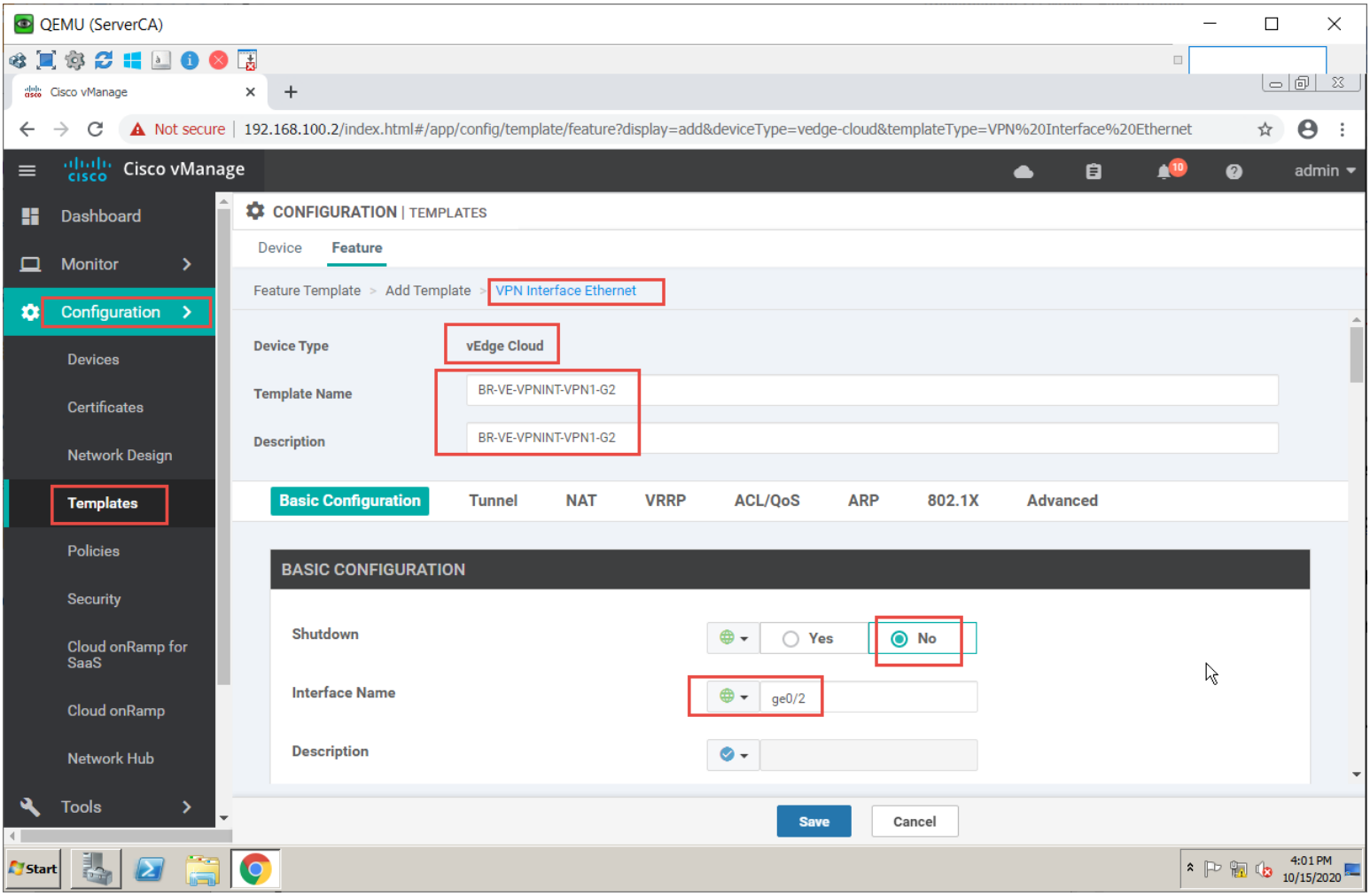


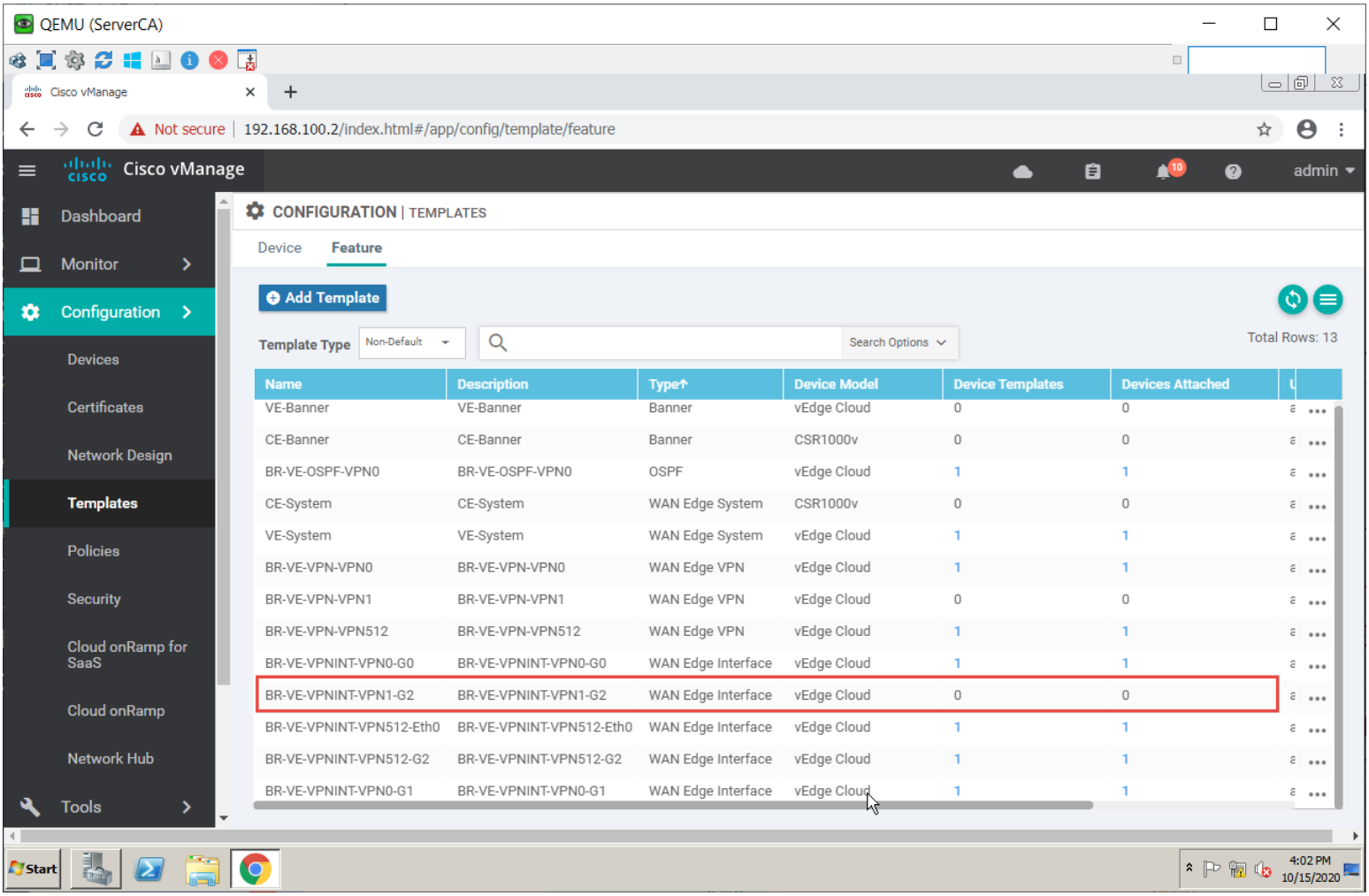


Task 2 – Configure a VPN Interface Template to be used by all Branch vEdge-Cloud devices for VPN 1 for Interface G0/2

- In vManage, **Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ VPN ➔ VPN Interface Ethernet**
- Configure the VPN parameters based on the following:
    - Template Name: BR-VE-VPNINT-VPN1-G2
    - Description: BR-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.


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN%20Interface%20Ethernet
Cisco vManage
admin
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 Interface Ethernet
Device Type
vEdge Cloud
Template Name
BR-VE-VPNINT-VPN1-G2
Description
BR-VE-VPNINT-VPN1-G2
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
BASIC CONFIGURATION
Shutdown
Yes
No
Interface Name
ge0/2
Description
Save
Cancel
Start
4:01 PM
10/15/2020

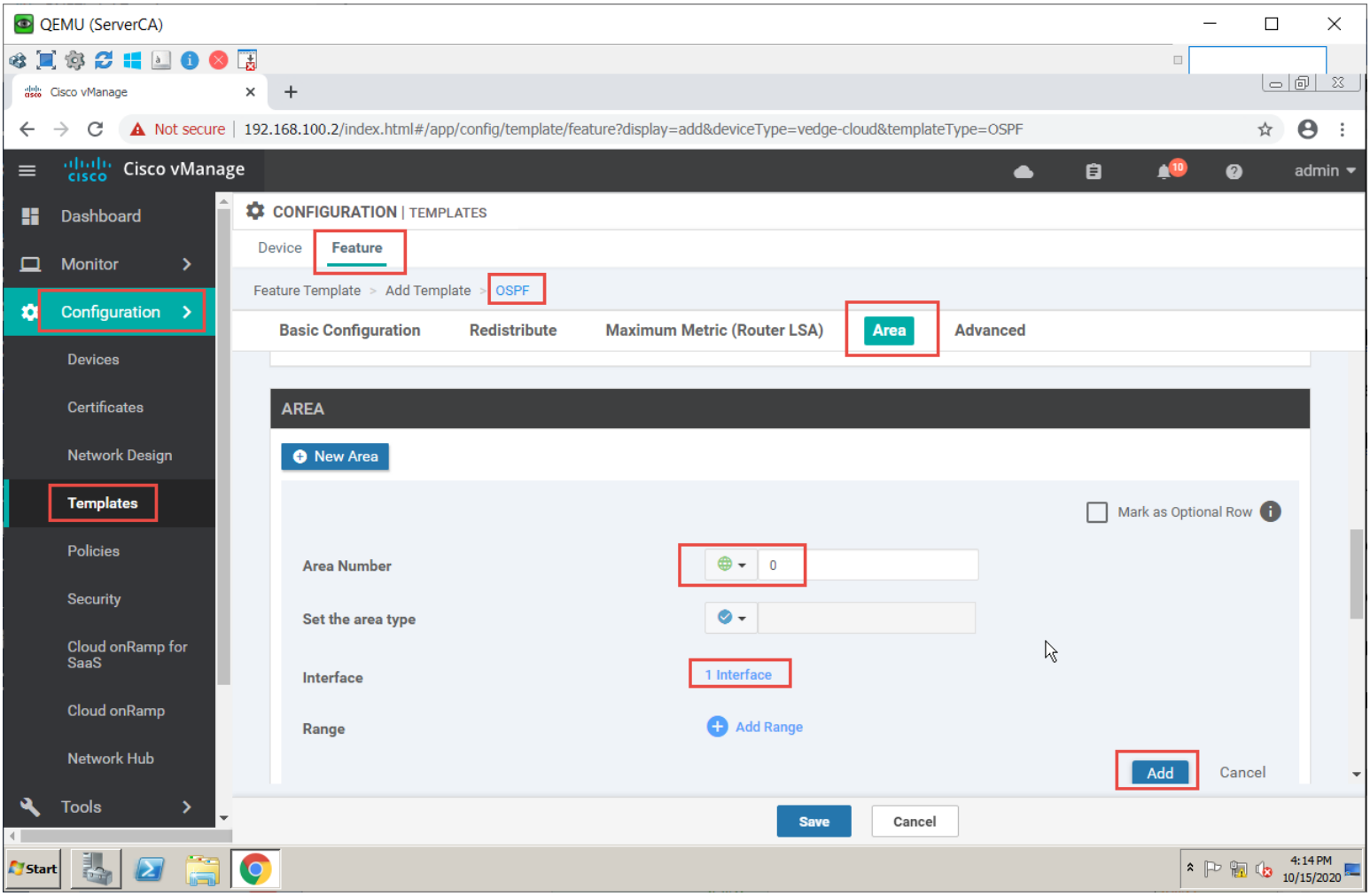


Task 3 – Configure a OSPF Template to be used by all Branch vEdgeCloud Devices for VPN 1

- In vManage, **Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ Other Templates ➔ OSPF**
- Configure the OSPF parameters based on the following:
  - Template Name: BR-VE-OSPF-VPN1
  - Description: BR-VE-OSPF-VPN1

  Redistribution
  - Protocol: OMP
- Area Configuration
  - Area Number ➔ Global : 0
  - Area Type ➔ Default

  Interface Configuration
  - Interface Name: Ge0/2
- Click Add to add the Interface and Click Add to add OSPF.
- Click Save to save the Template.

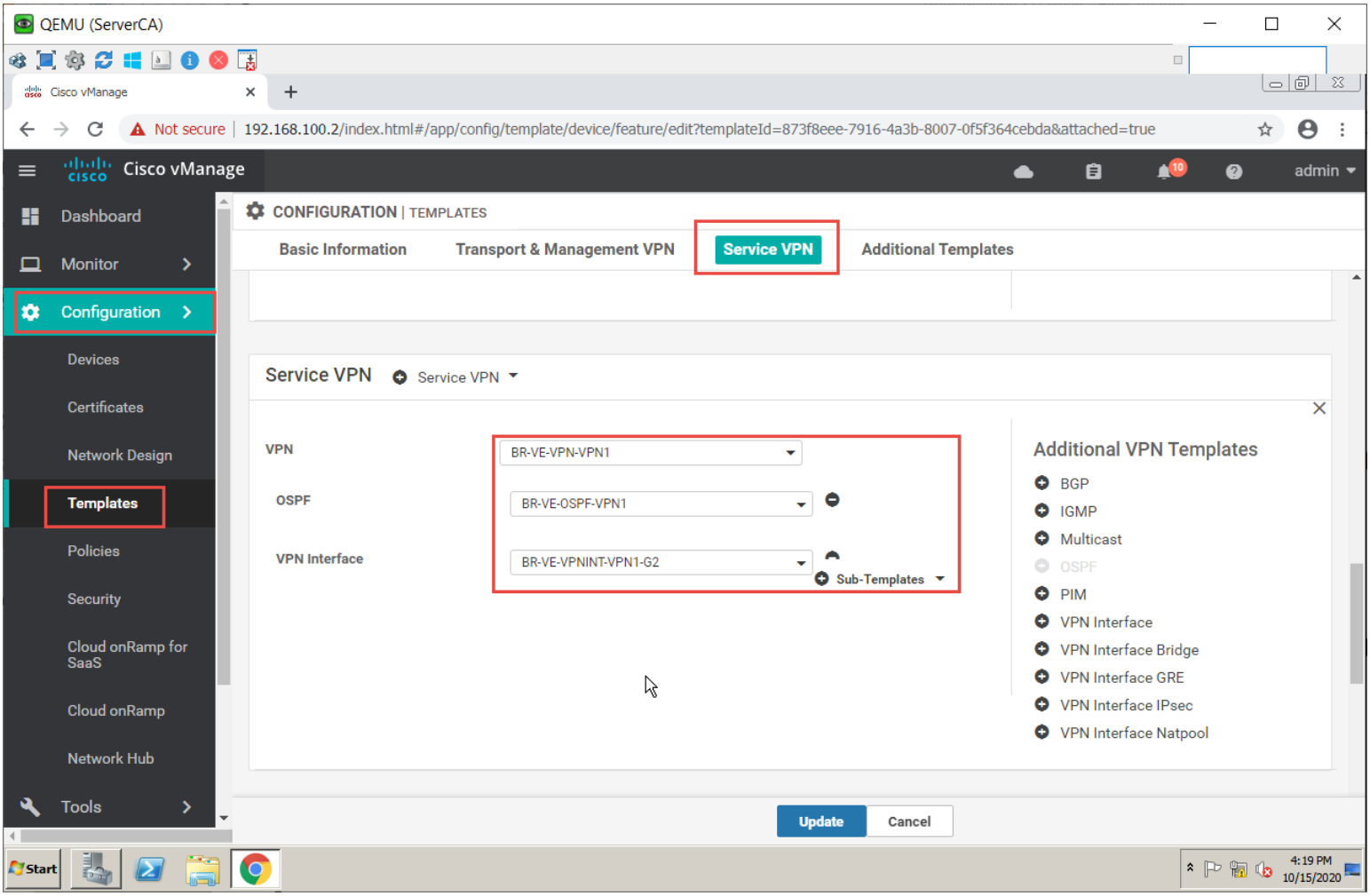

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=OSPF
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > OSPF
Basic Configuration
Redistribute
Maximum Metric (Router LSA)
Area
Advanced
AREA
New Area
Mark as Optional Row
Area Number
0
Set the area type
Interface
1 Interface
Range
Add Range
Add
Cancel
Save
Cancel
Start
4:14 PM
10/15/2020

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

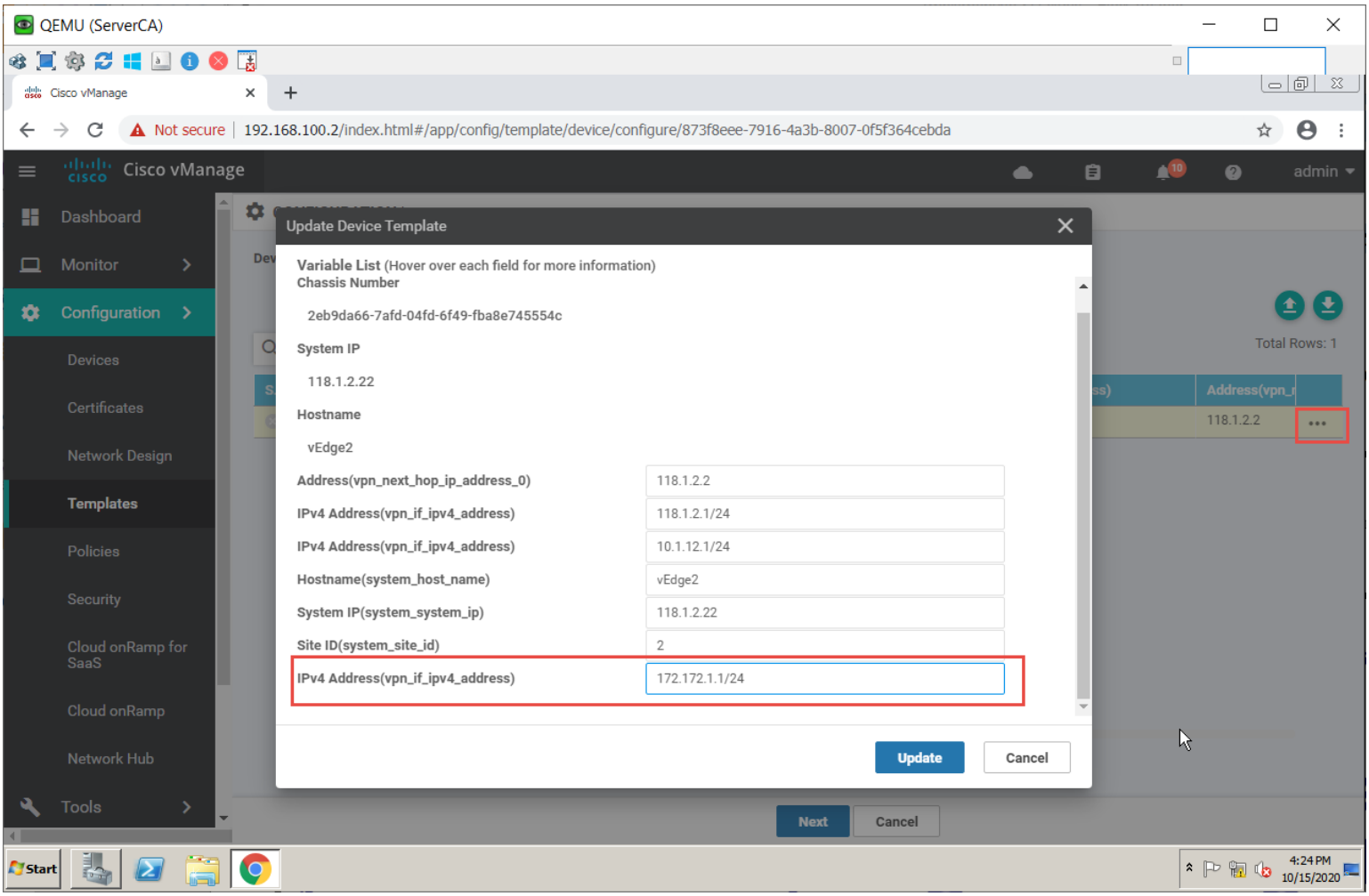


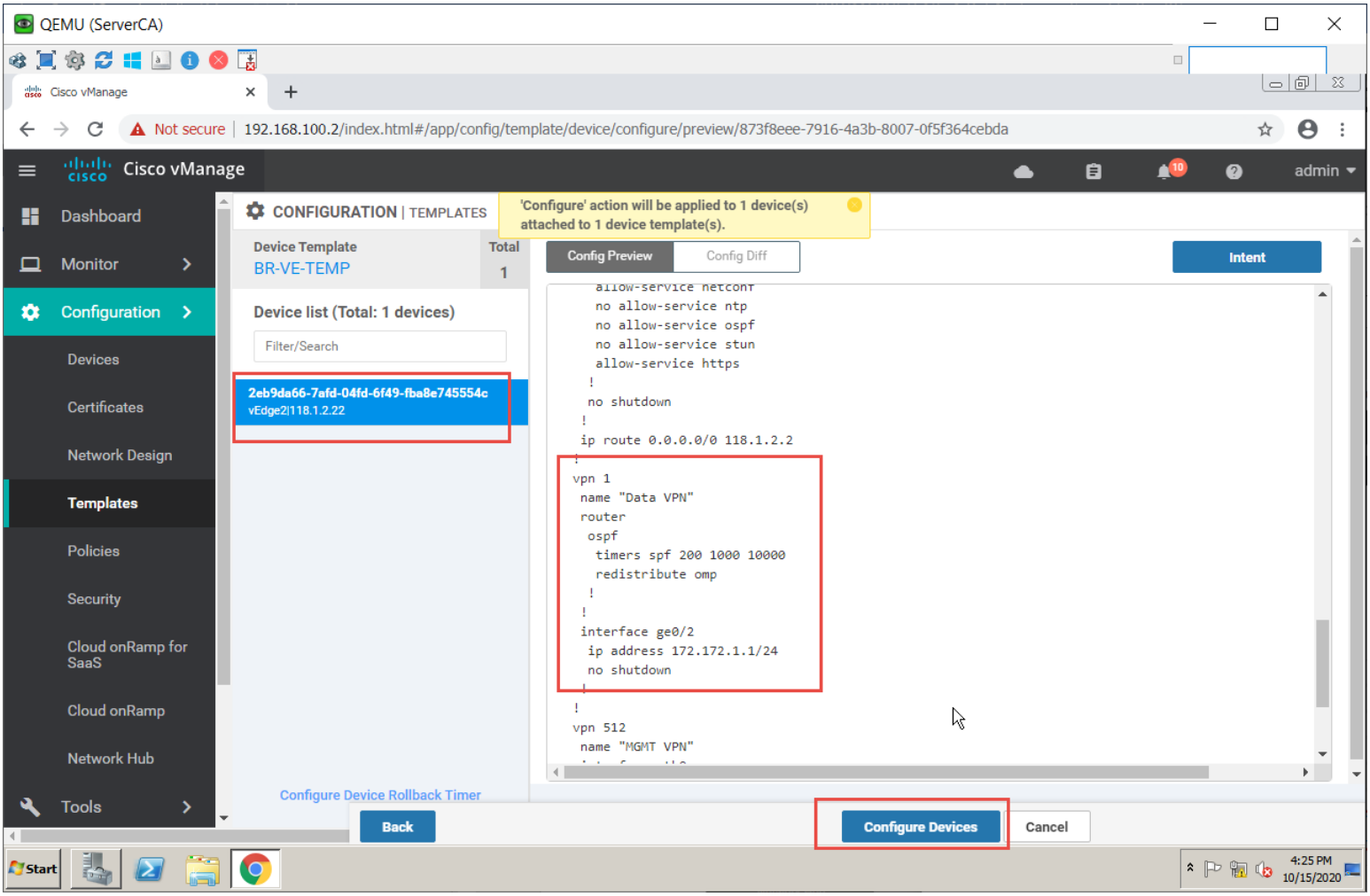
Task 2 – Configure the Variable Parameters for the Feature Templates

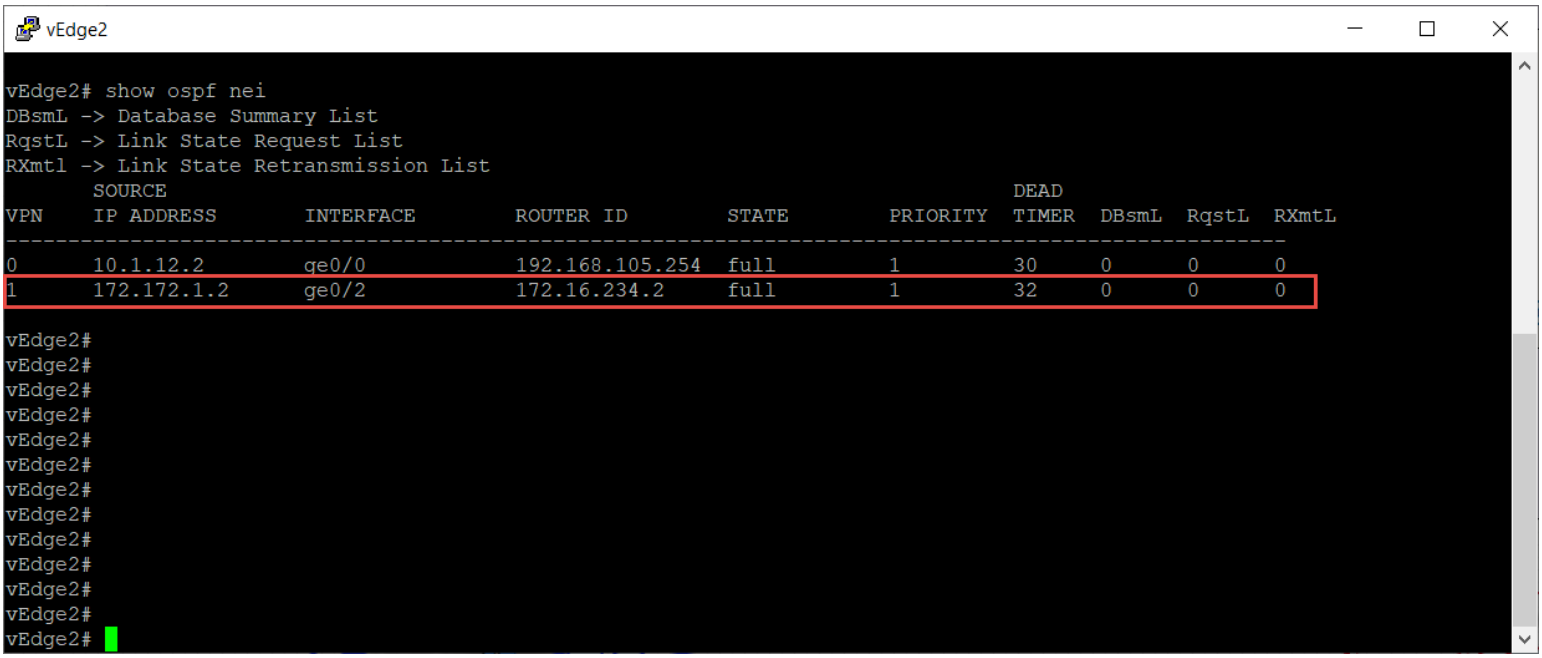
- vEdge2 will appear in the window.
- Click on "…" towards the right-hand side & click Edit Device Template.
- Configure the variables based on the following:

- 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.



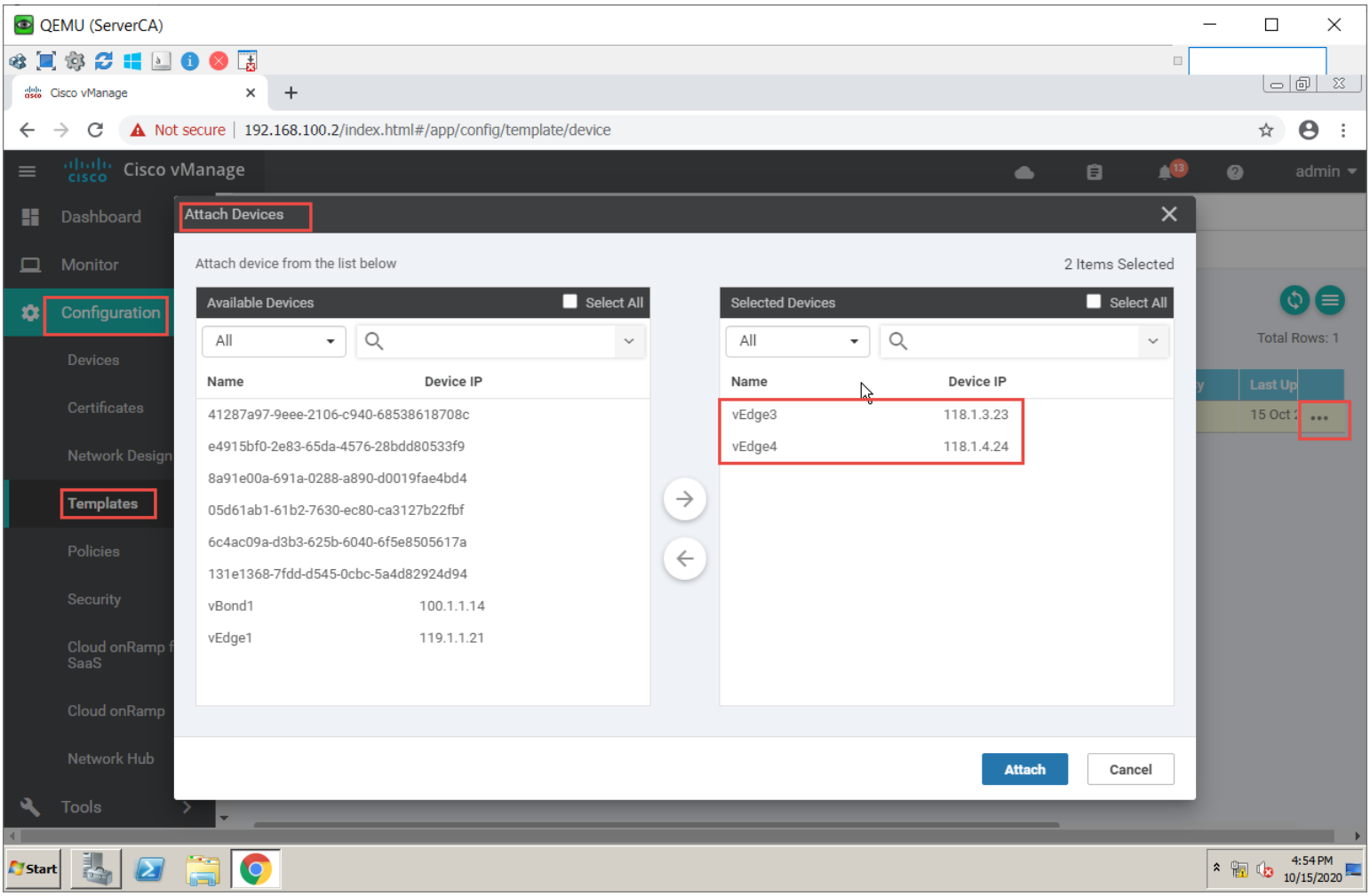

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/device/configure/preview/873f8eee-7916-4a3b-8007-0f5f364cebda
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
'Configure' action will be applied to 1 device(s) attached to 1 device template(s).
Device Template
BR-VE-TEMP
Total
1
Device list (Total: 1 devices)
Filter/Search
2eb9da66-7afd-04fd-6f49-fba8e745554c
vEdge2|118.1.2.22
Config Preview
Config Diff
Intent
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 omp
interface ge0/2
ip address 172.172.1.1/24
no shutdown
vpn 512
name "MGMT VPN"
Configure Device Rollback Timer
Back
Configure Devices
Cancel
Start
4:25 PM
10/15/2020

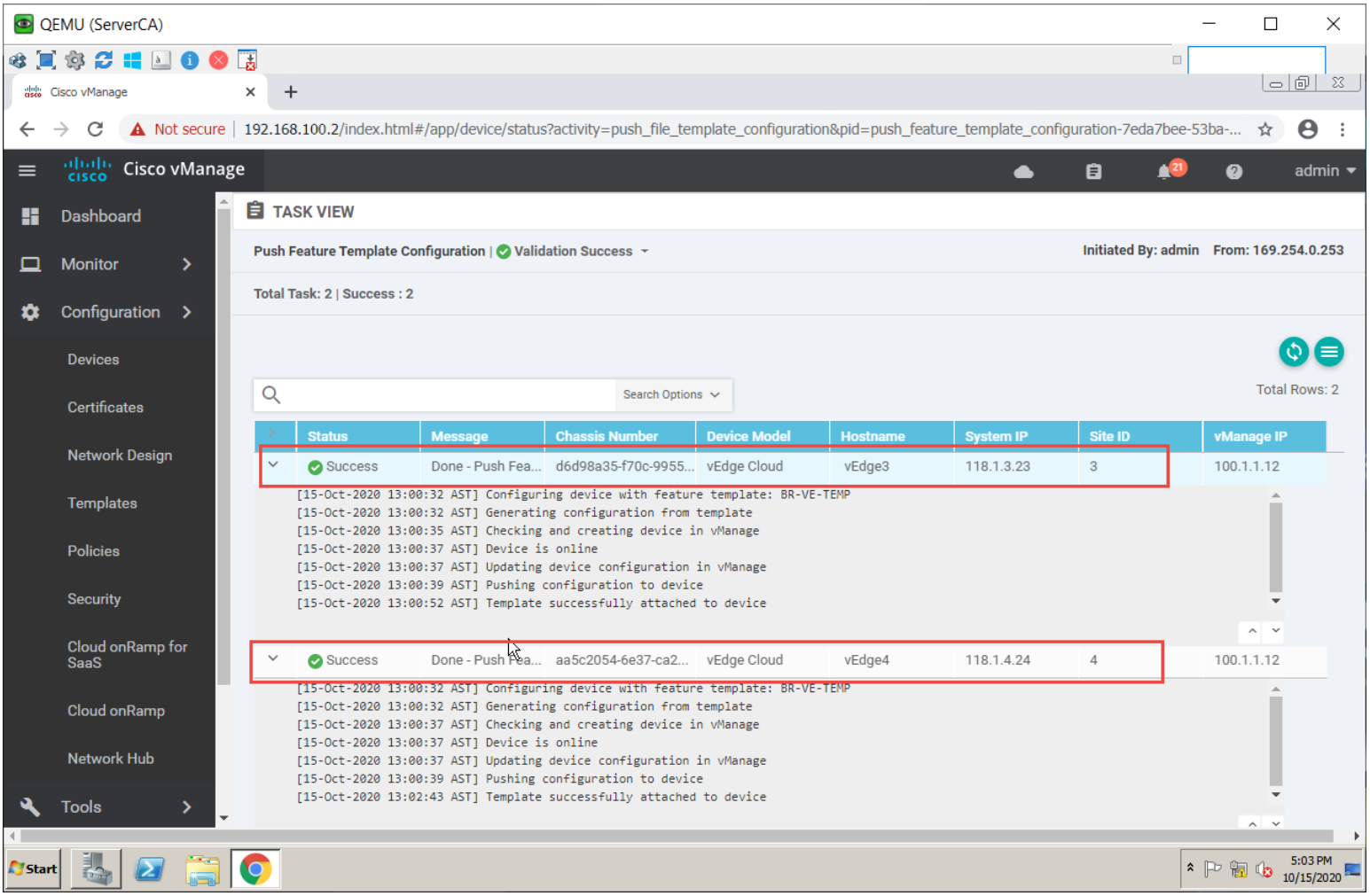

vEdge2
vEdge2# show ospf nei
DBsmL -> Database Summary List
RqstL -> Link State Request List
RXmtl -> Link State Retransmission List
VPN SOURCE IP ADDRESS INTERFACE ROUTER ID STATE PRIORITY DEAD TIMER DBsmL RqstL RXmtL
0 10.1.12.2 ge0/0 192.168.105.254 full 1 30 0 0 0
1 172.172.1.2 ge0/2 172.16.234.2 full 1 32 0 0 0
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#
vEdge2#

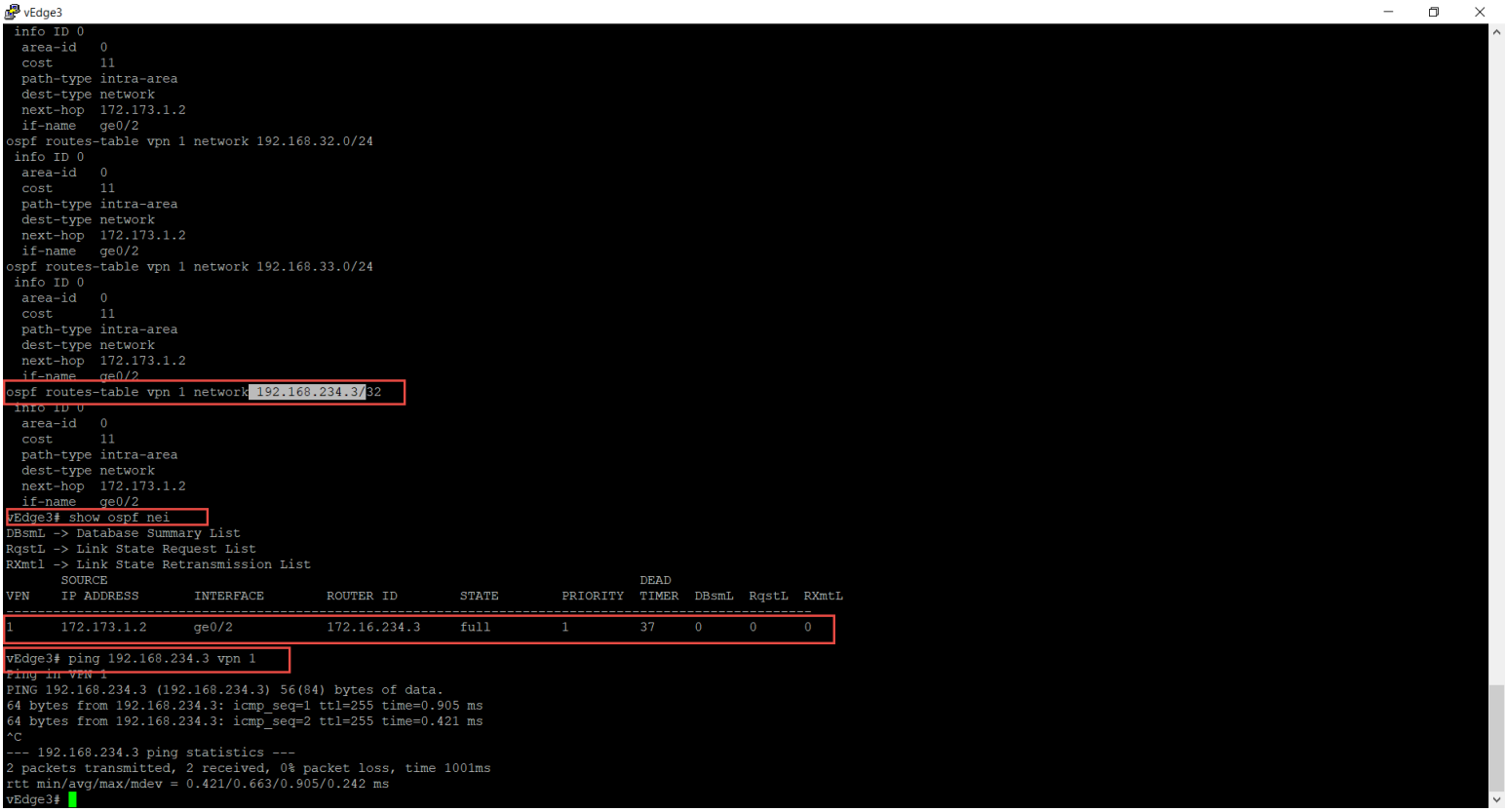
Lab 21 - Pushing Template to configure other Branch Sites - – Branch Site(vEdge3 & vEdge4)

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 VPN0: 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 VPN0: 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.




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-...
Cisco vManage
admin
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
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
[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
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 13:00:37 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
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
RqstL -> Link State Request List
RXmtl -> Link State Retransmission List
VPN SOURCE IP ADDRESS INTERFACE ROUTER ID STATE PRIORITY DEAD TIMER DBsmL RqstL RXmtL
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 VPN 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

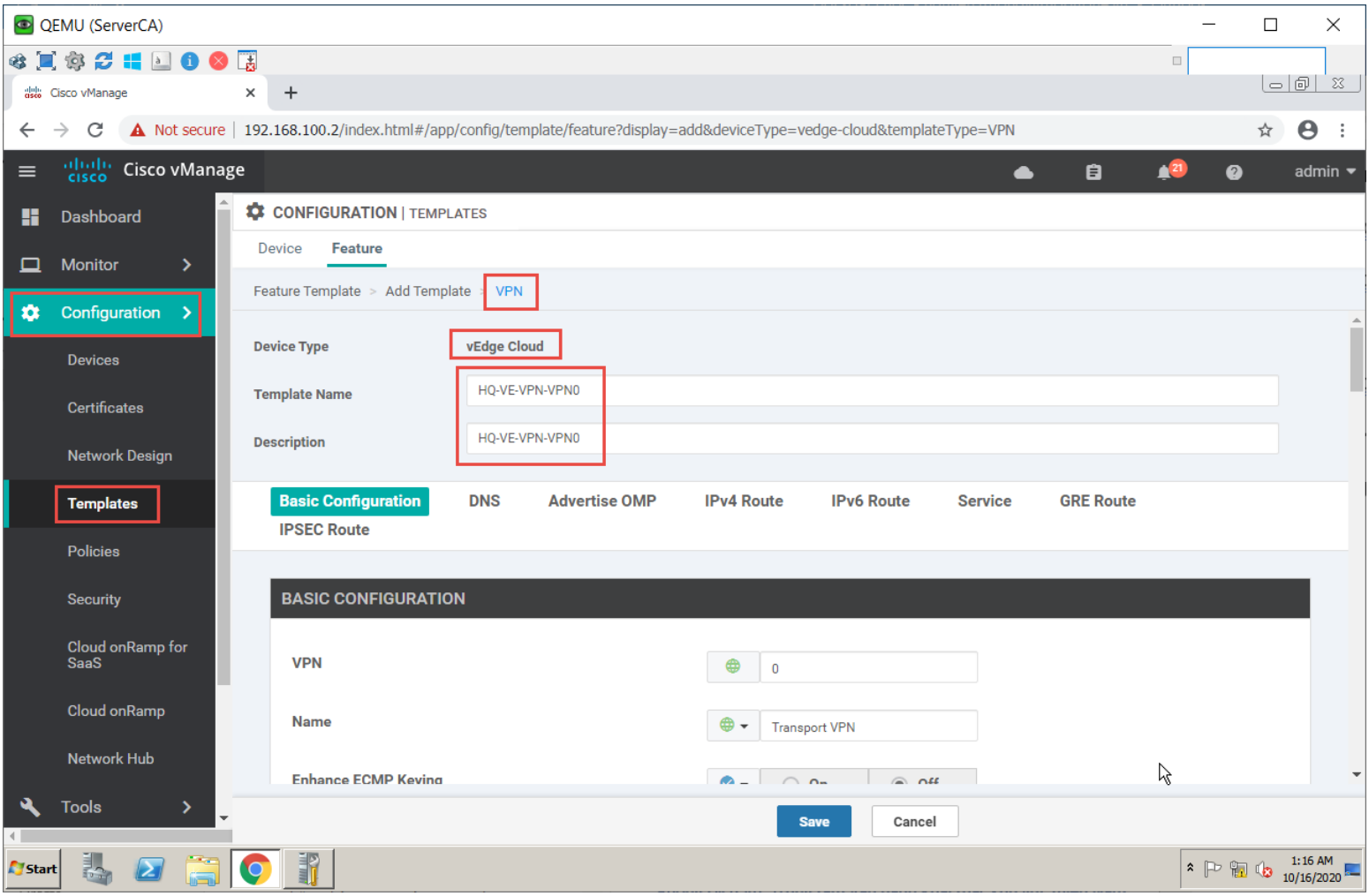
VPN 0

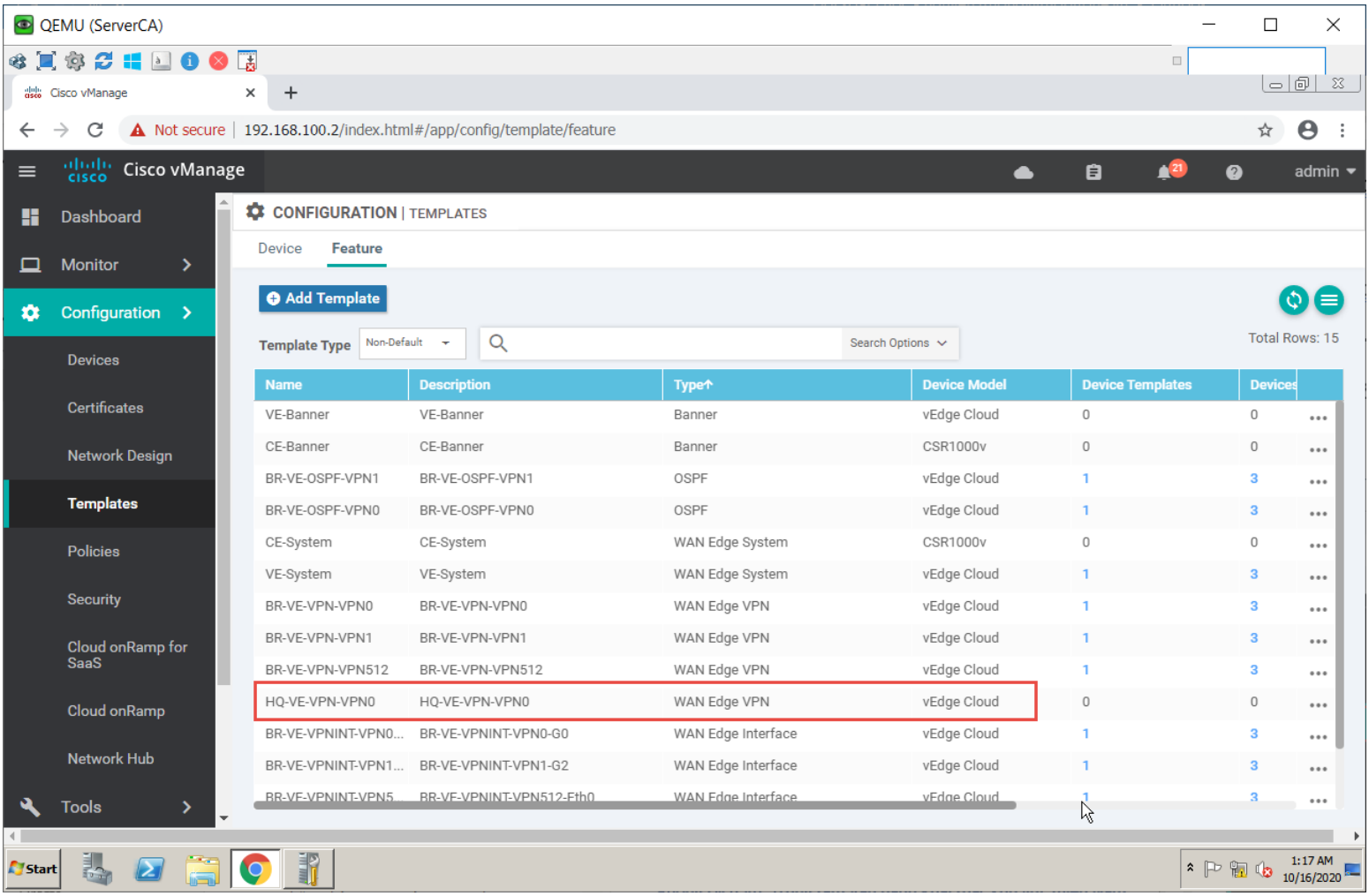
Task 1 – Configure a VPN Template for HQ vEdge-Cloud Devices for VPN 0

- In vManage, **Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ VPN ➔ VPN**
- Configure the VPN parameters based on the following:
    - Template Name: HQ-VE-VPN-VPN0
    - Description: HQ-VE-VPN-VPN0

  Basic Configuration
    - VPN ➔ Global: 0
    - Name ➔ Global: Transport VPN

  IPv4 Route
    - Prefix ➔ Global: 0.0.0.0/0
    - Next Hop ➔ Device Specific
- 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
admin
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-VPN0
Description
HQ-VE-VPN-VPN0
Basic Configuration
DNS
Advertise OMP
IPv4 Route
IPv6 Route
Service
GRE Route
IPSEC Route
BASIC CONFIGURATION
VPN
0
Name
Transport VPN
Enhance ECMP Keying
Save
Cancel
Start
1:16 AM
10/16/2020



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:
    - Template Name: HQ-VE-VPNINT-VPN0-G0
    - Description: HQ-VE-VPNINT-VPN0-G0

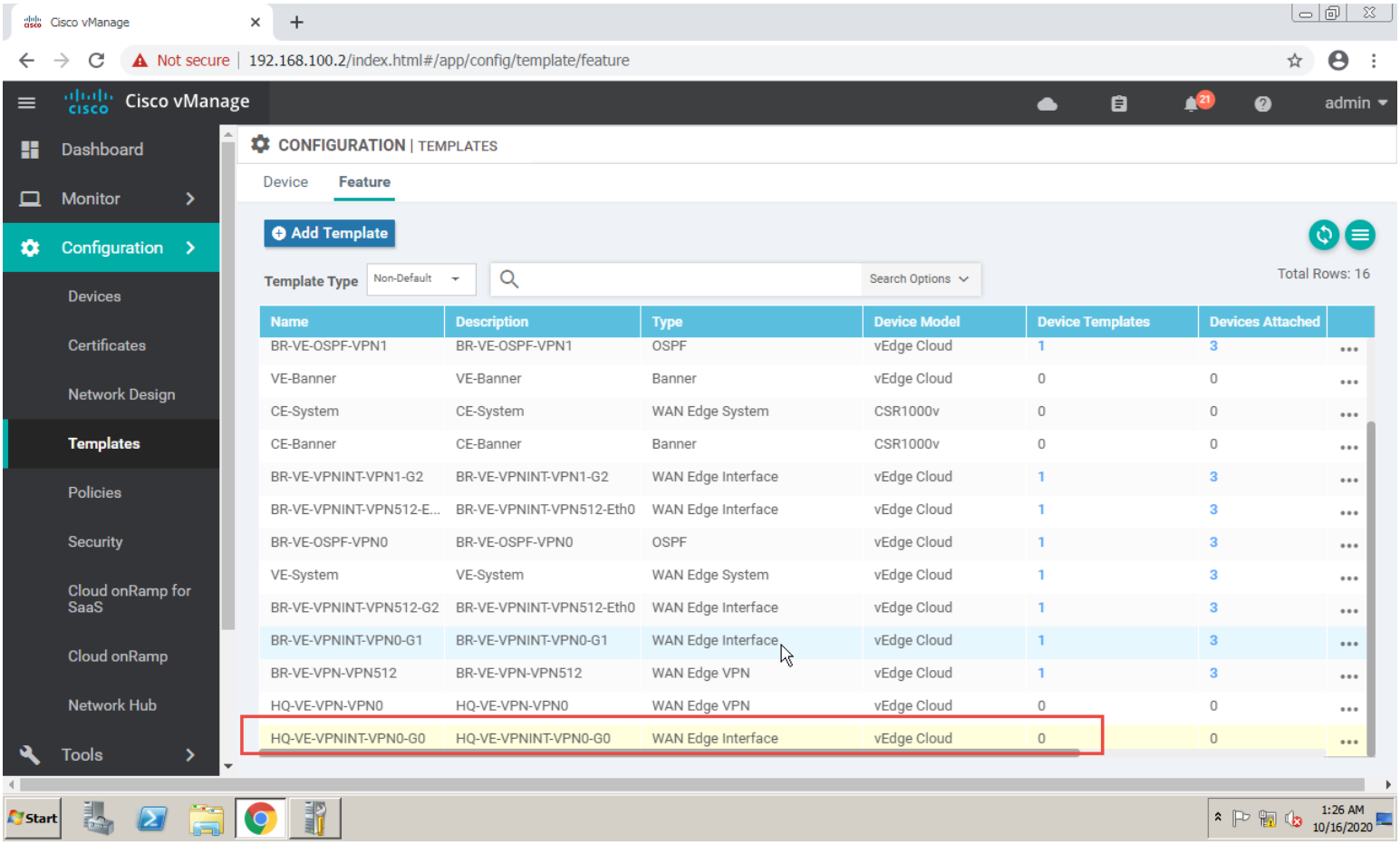
  Basic Configuration
    - Shutdown ➔ Global : No
    - Interface Name ➔ Global: ge0/0
    - IPv4 Address ➔ Static ➔ Device Specific

  Tunnel
    - Tunnel Interface ➔ Global: On
    - Color ➔ Default

  Allow Service
    - All ➔ Global: On

- NETCONF ➔ Global: On
- SSH ➔ Global: On

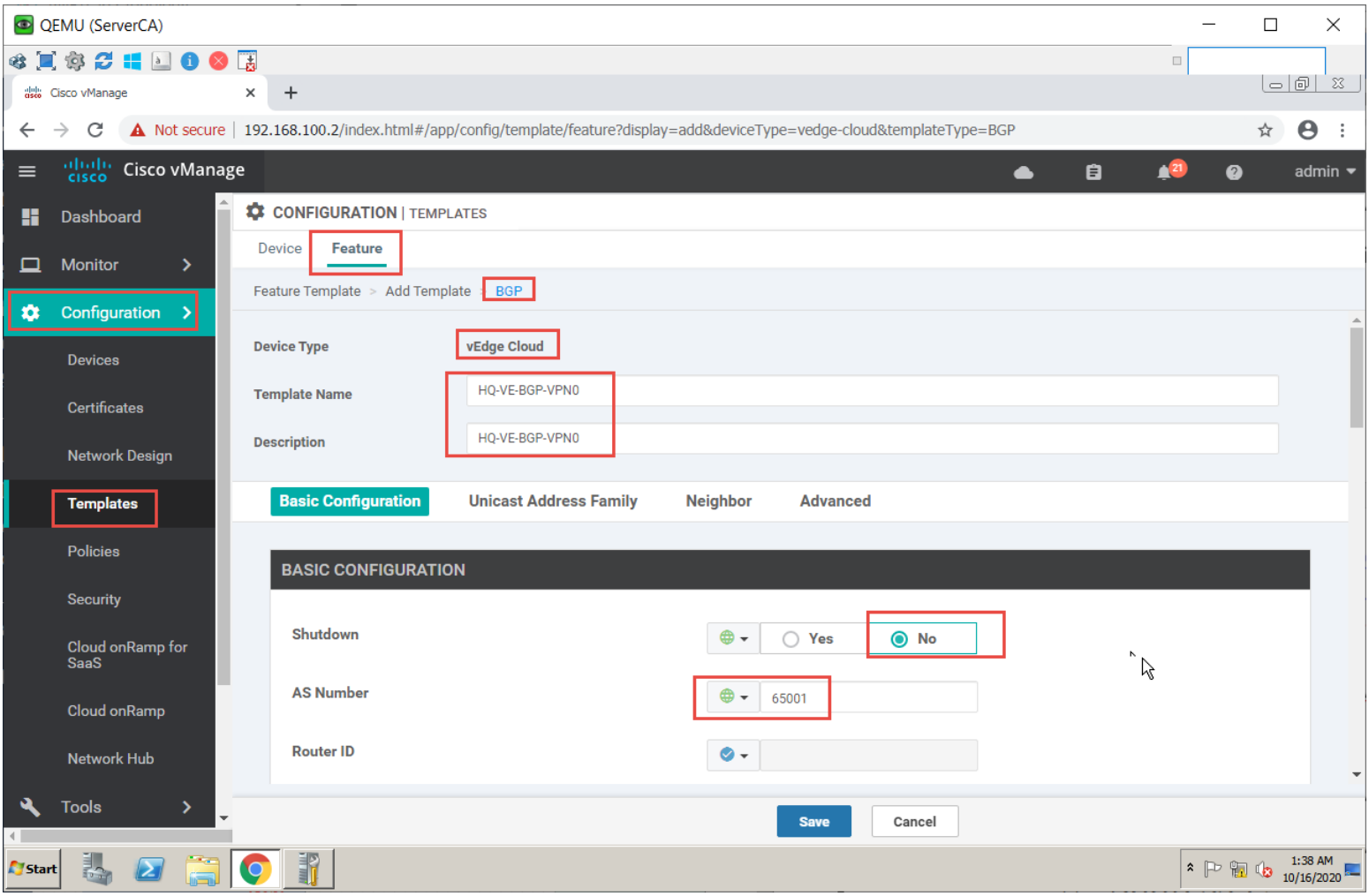
- Click Save to save the Template.

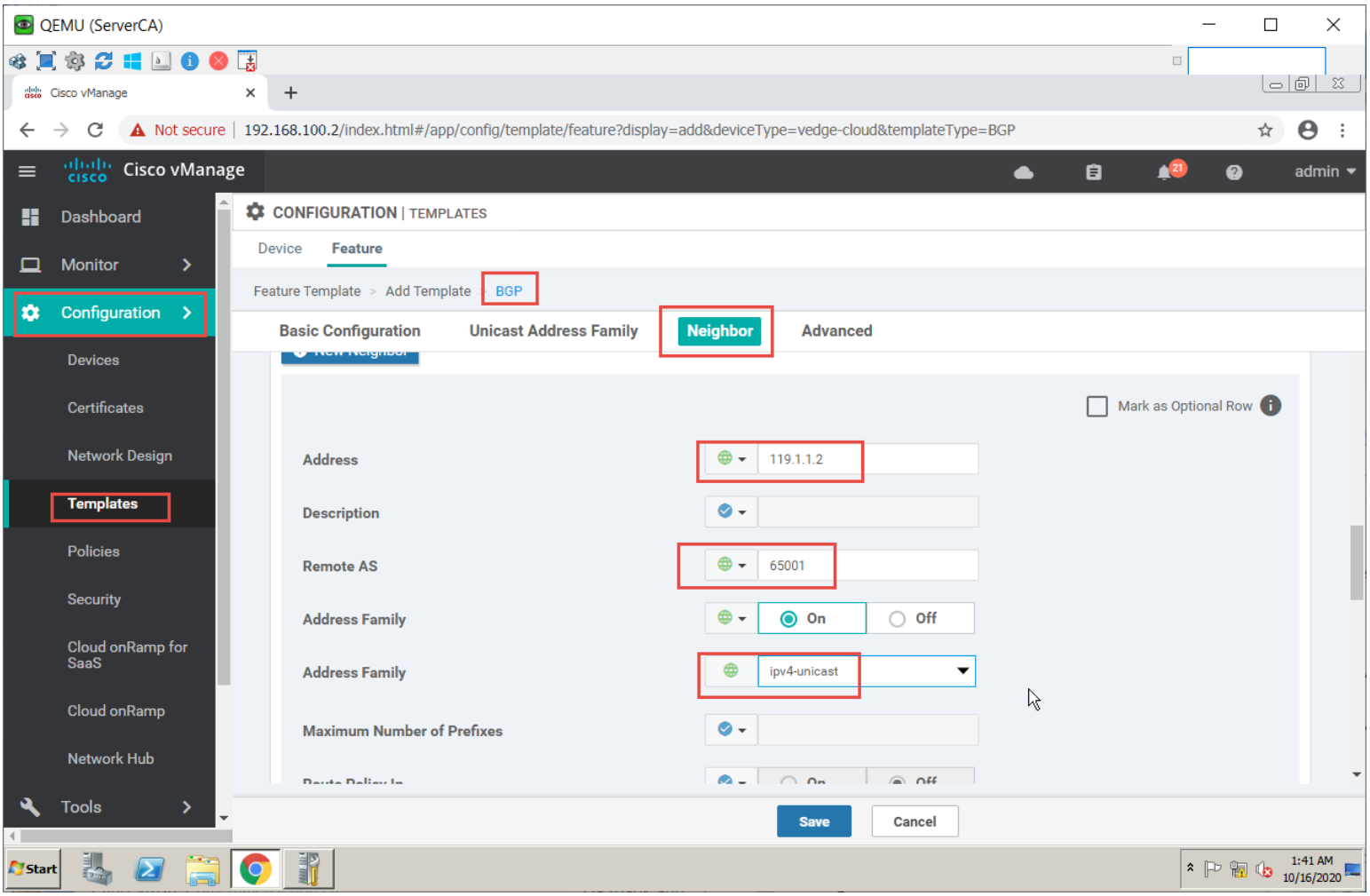


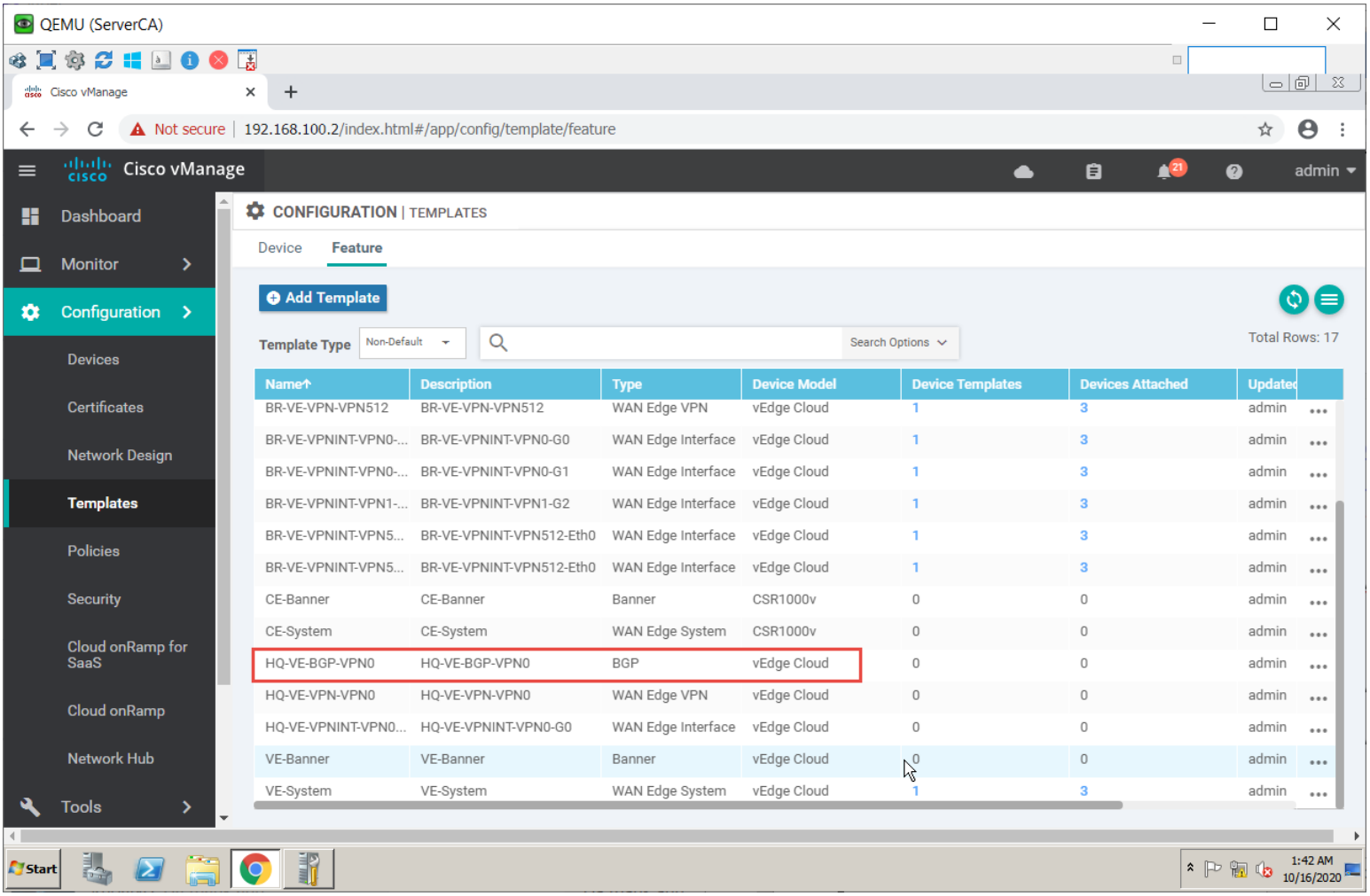
Task 3 – Configure a BGP Template to be used by HQ vEdge-Cloud Devices for VPN 0

- 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.




QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=BGP
Cisco vManage
admin
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 BGP
Basic Configuration
Unicast Address Family
Neighbor
Advanced
Mark as Optional Row
Address
119.1.1.2
Description
Remote AS
65001
Address Family
On
Off
Address Family
ipv4-unicast
Maximum Number of Prefixes
Save
Cancel
Start
1:41 AM
10/16/2020

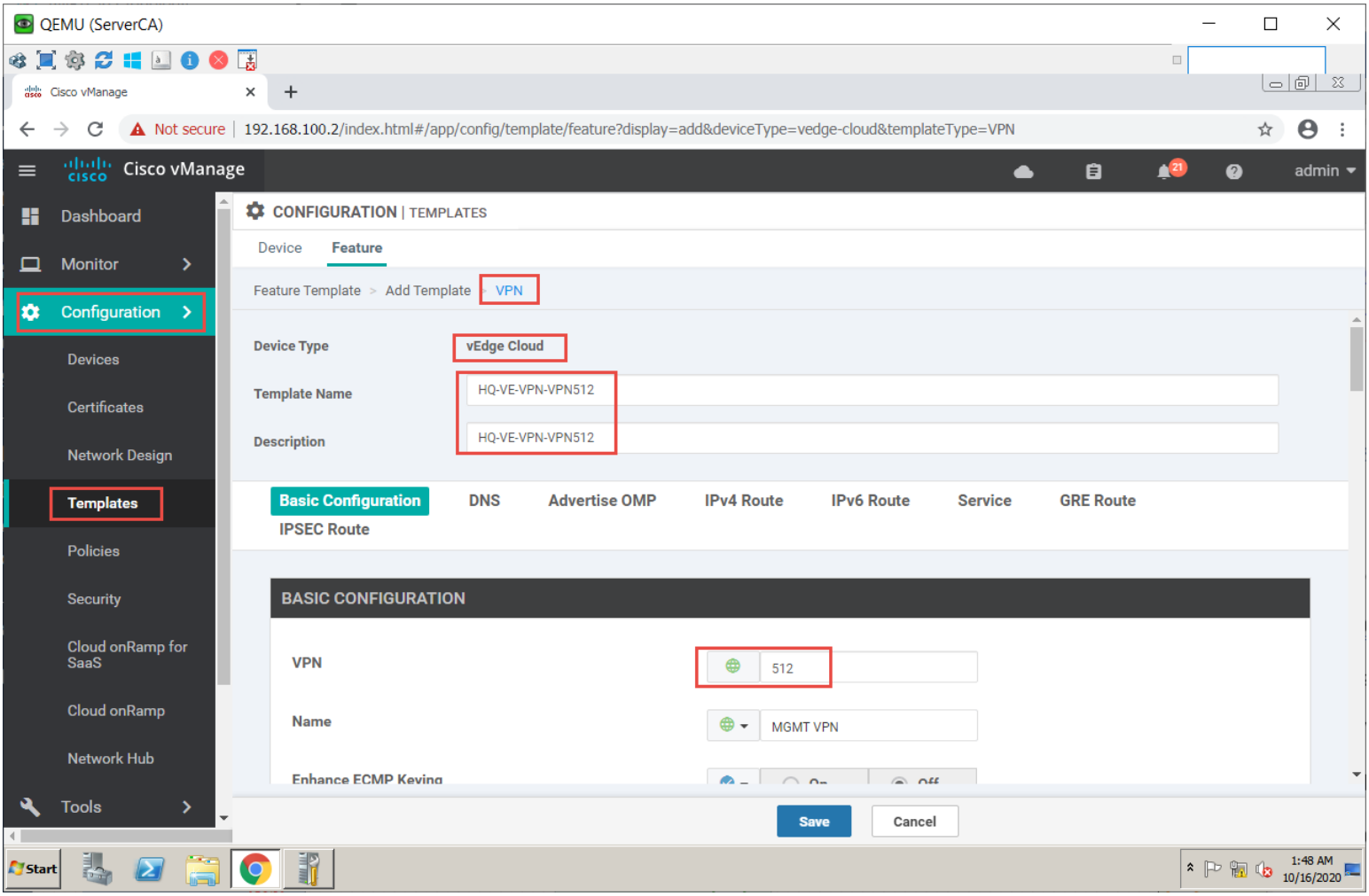


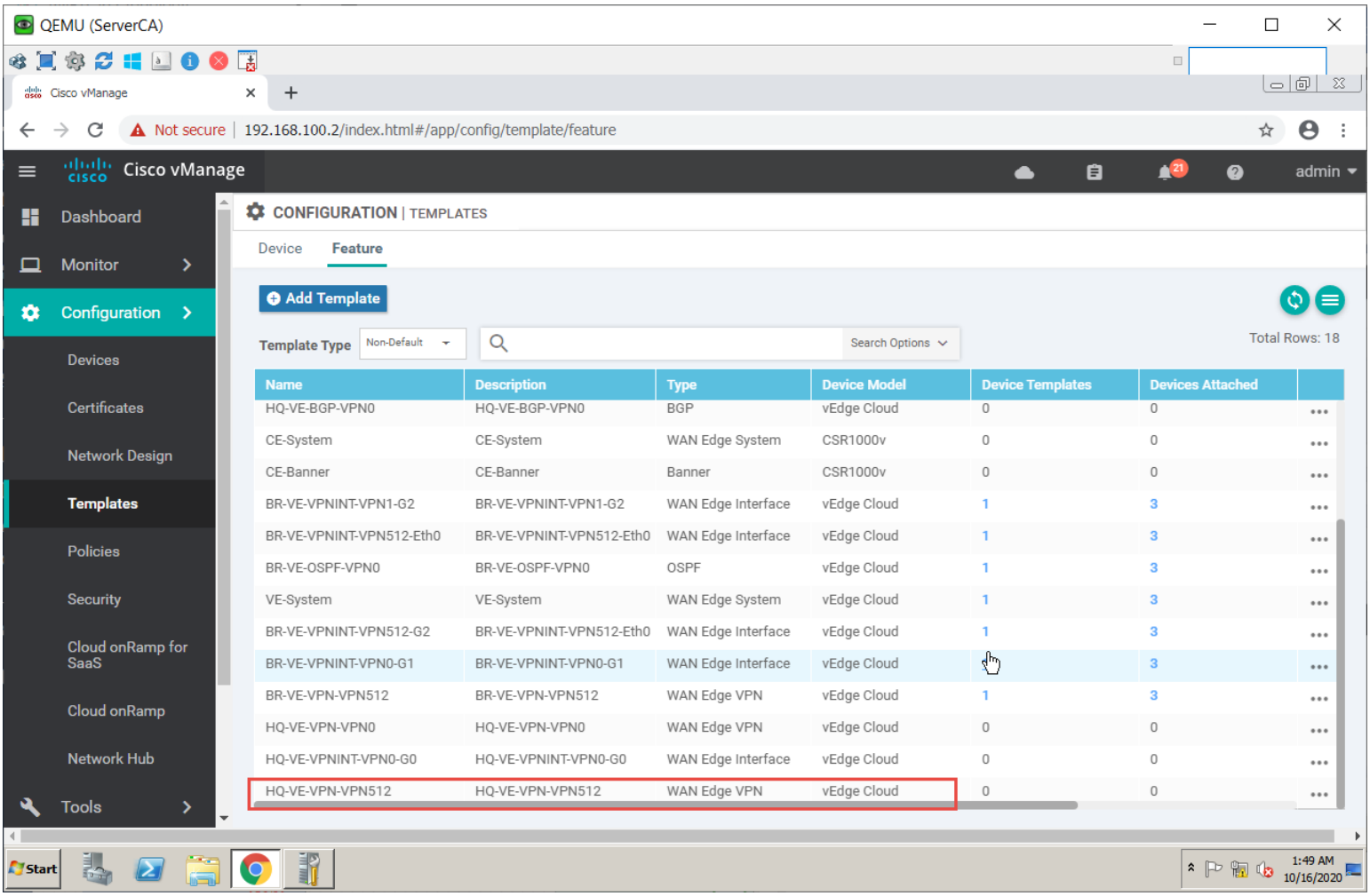
VPN 512

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:
    - Template Name: HQ-VE-VPN-VPN512
    - Description: HQ-VE-VPN-VPN512

  Basic Configuration
    - VPN ➔ Global: 512
    - Name ➔ Global: MGMT VPN
- Click Save to save the Template.

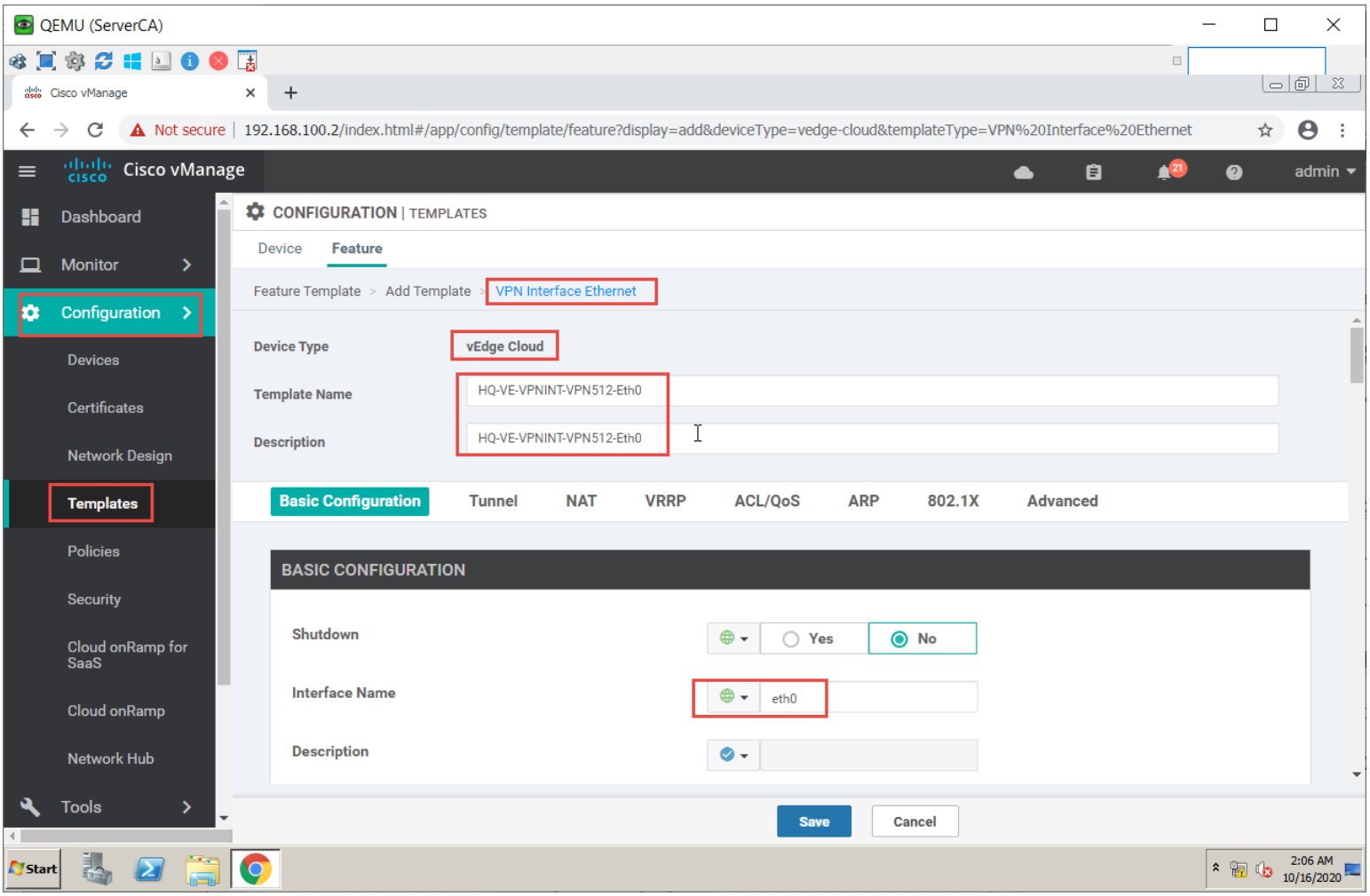

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network 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
Save
Cancel
Start
1:48 AM
10/16/2020

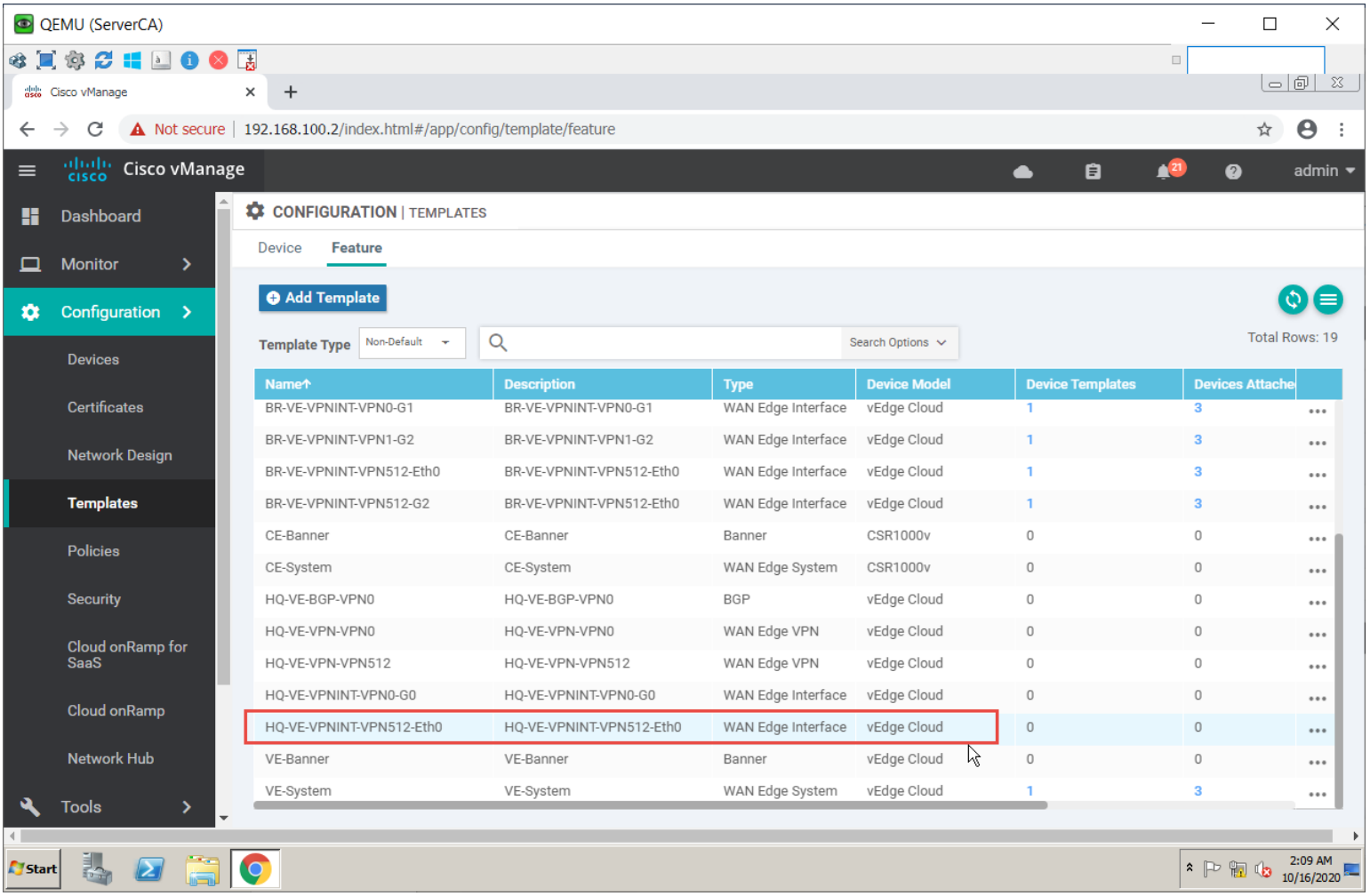


Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ vEdge Cloud ➔ VPN ➔ VPN Interface Ethernet
- Configure the VPN parameters based on the following:
    - Template Name: HQ-VE-VPNINT-VPN512-E0
    - Description: HQ-VE-VPNINT-VPN512-E0

  Basic Configuration
    - Shutdown ➔ Global: No
    - Interface Name ➔ Global: eth0
    - IPv4 Address ➔ Dynamic
- 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%20Interface%20Ethernet
Cisco vManage
admin
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 Interface Ethernet
Device Type
vEdge Cloud
Template Name
HQ-VE-VPNINT-VPN512-Eth0
Description
HQ-VE-VPNINT-VPN512-Eth0
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
BASIC CONFIGURATION
Shutdown
Yes
No
Interface Name
eth0
Description
Save
Cancel
Start
2:06 AM
10/16/2020

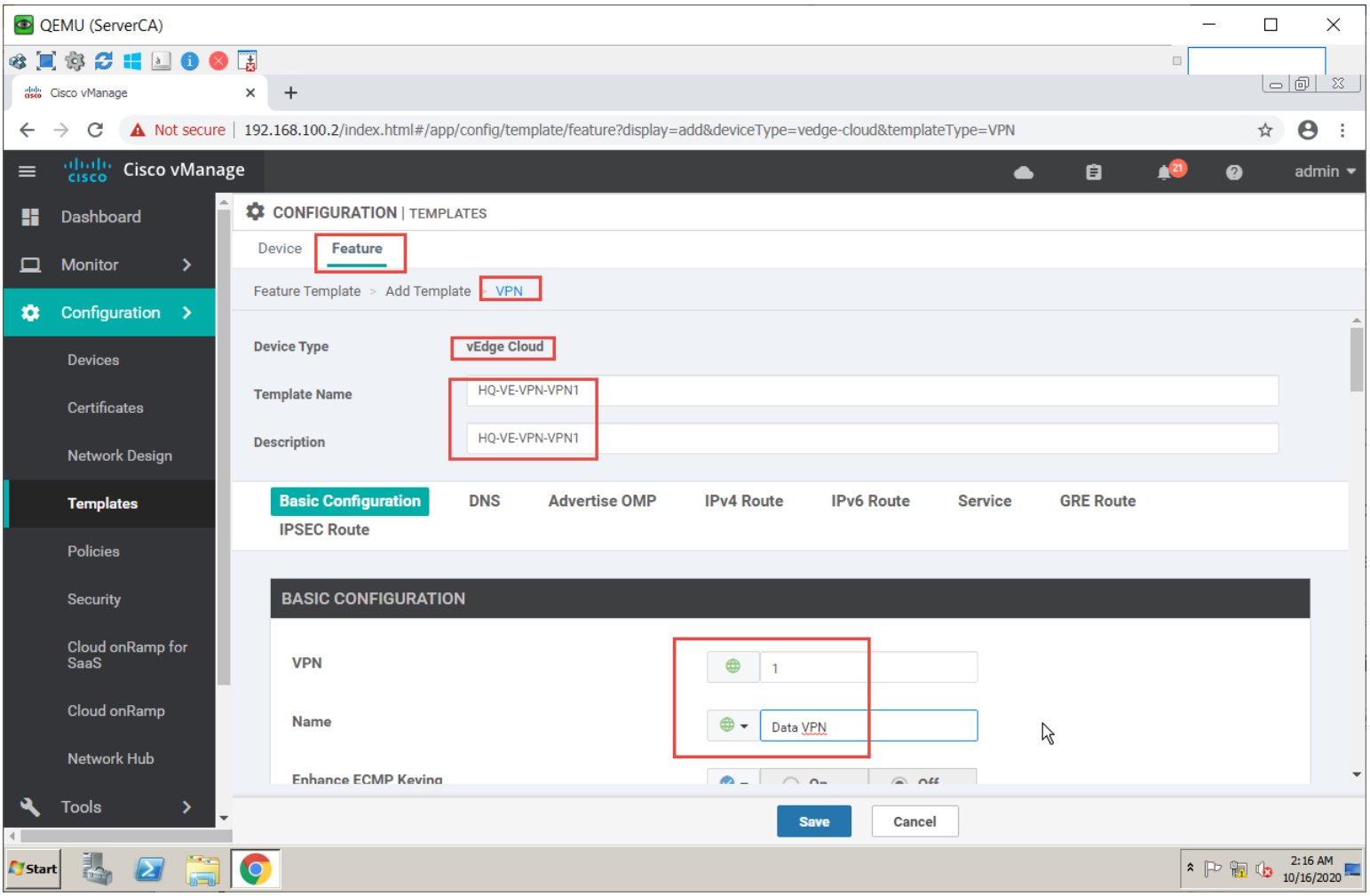


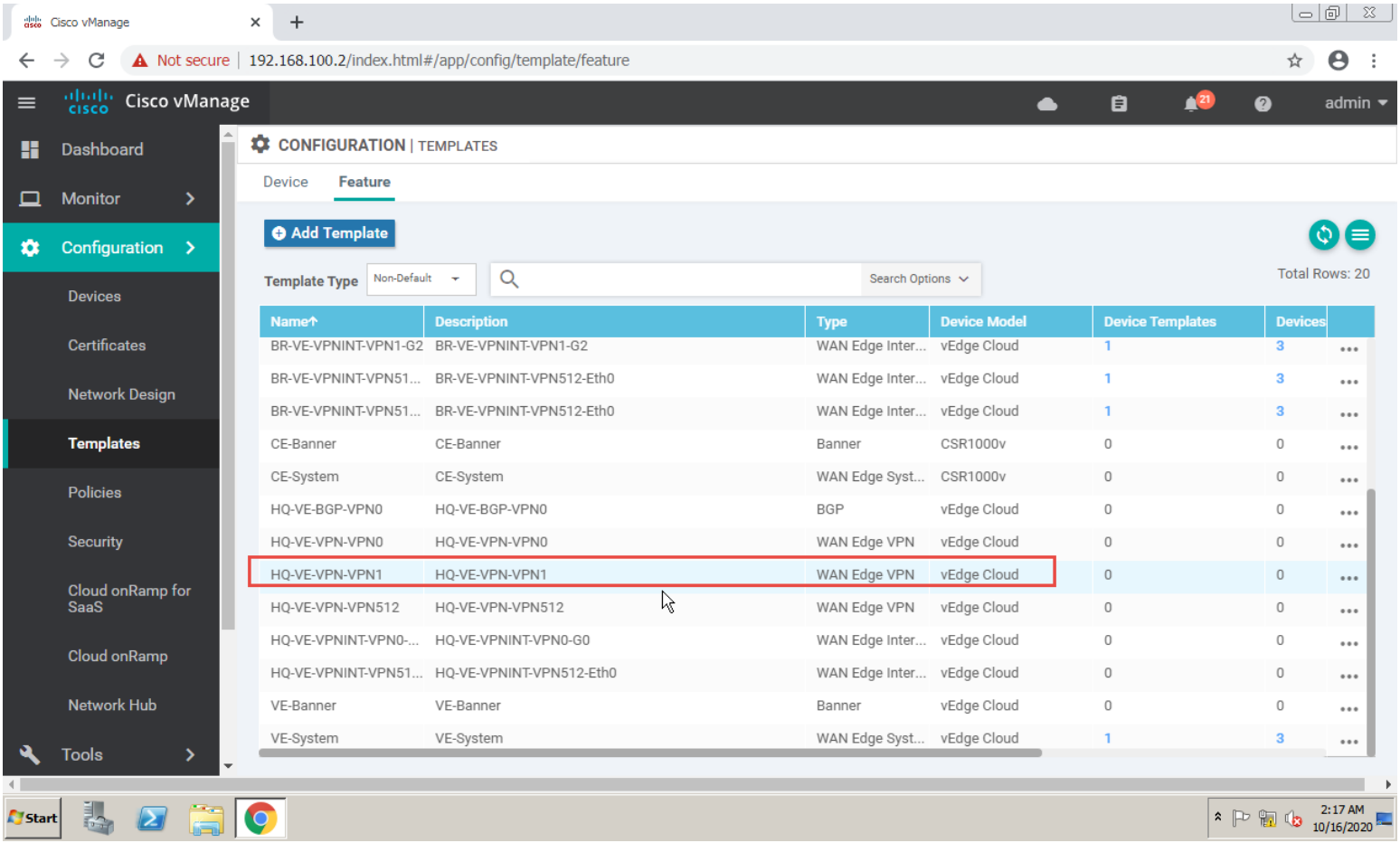
VPN 1

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:
    - Template Name: HQ-VE-VPN-VPN1
    - Description: HQ-VE-VPN-VPN1

  Basic Configuration
    - VPN ➔ Global: 1
    - Name ➔ Global: Data VPN
- Click Save to save the Template.

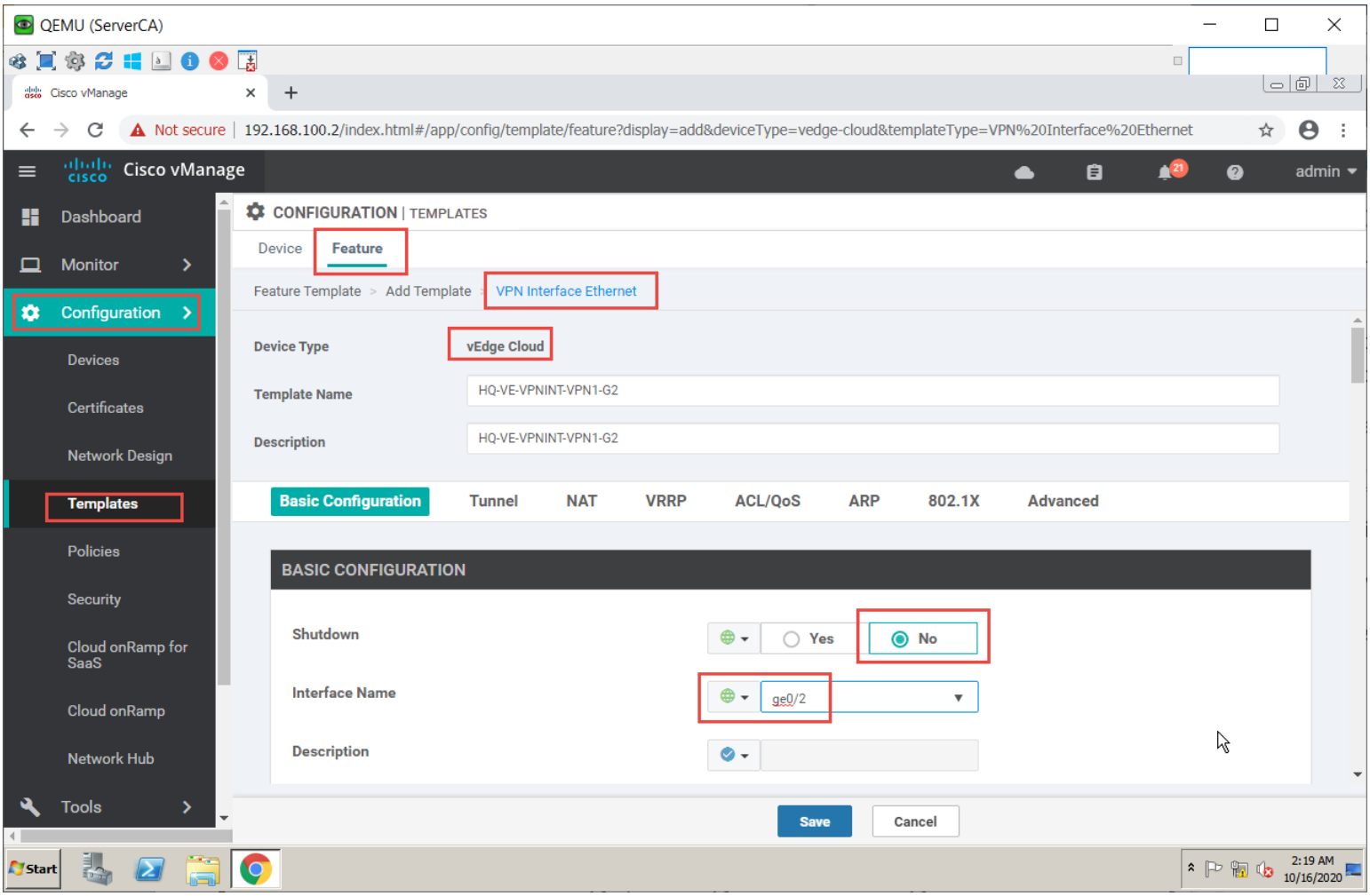

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > VPN
Device Type
vEdge Cloud
Template Name
HQ-VE-VPN-VPN1
Description
HQ-VE-VPN-VPN1
Basic Configuration
DNS
Advertise OMP
IPv4 Route
IPv6 Route
Service
GRE Route
IPSEC Route
BASIC CONFIGURATION
VPN
1
Name
Data VPN
Save
Cancel
Start
2:16 AM
10/16/2020

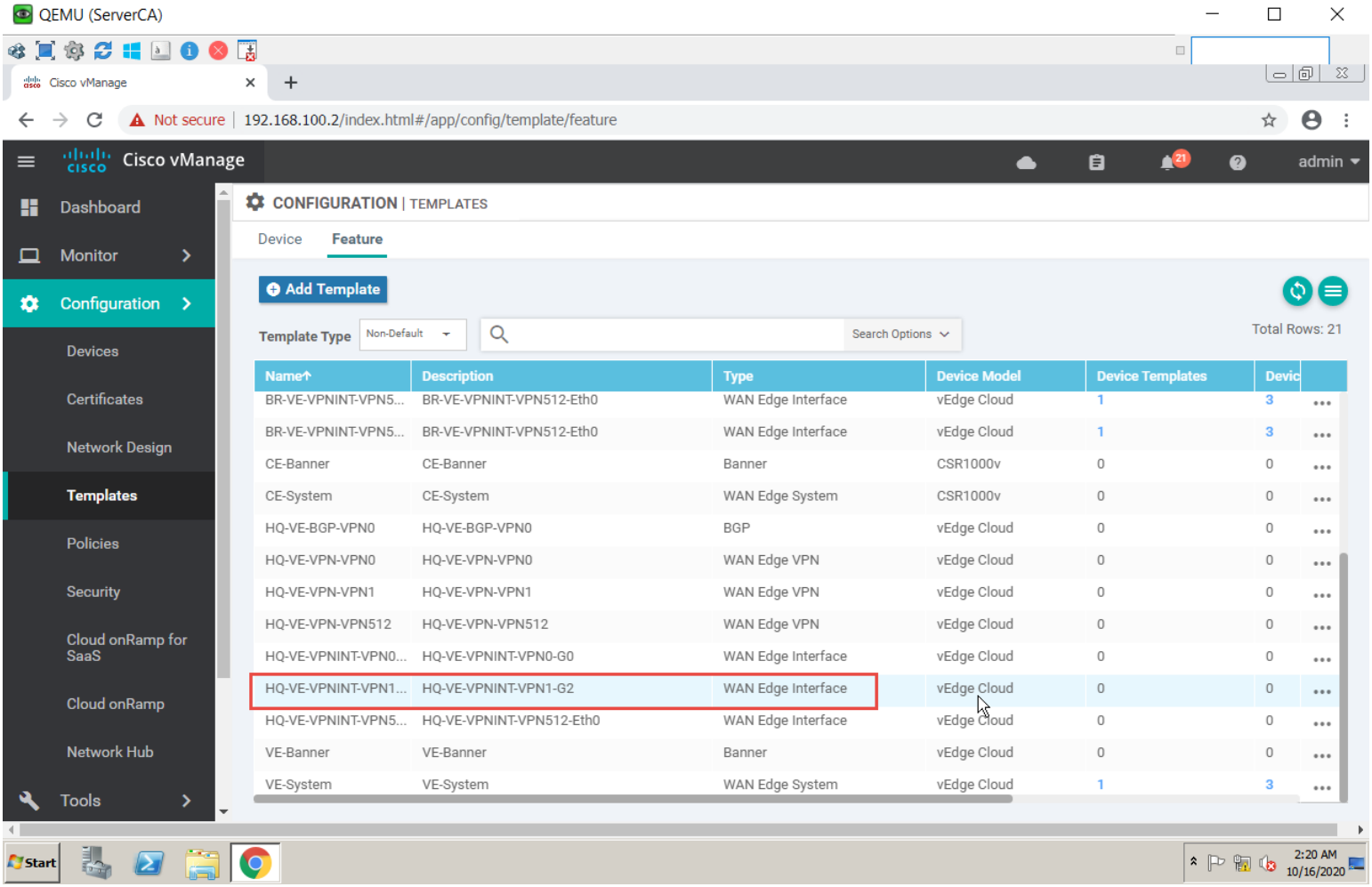


Task 2 – Configure a VPN Interface Template to be used by HQ vEdge-Cloud Devices for VPN 1 for Interface G0/2

- 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.


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=VPN%20Interface%20Ethernet
Cisco vManage
admin
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 Interface Ethernet
Device Type
vEdge Cloud
Template Name
HQ-VE-VPNINT-VPN1-G2
Description
HQ-VE-VPNINT-VPN1-G2
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
BASIC CONFIGURATION
Shutdown
Yes
No
Interface Name
ge0/2
Description
Save
Cancel
Start
2:19 AM
10/16/2020

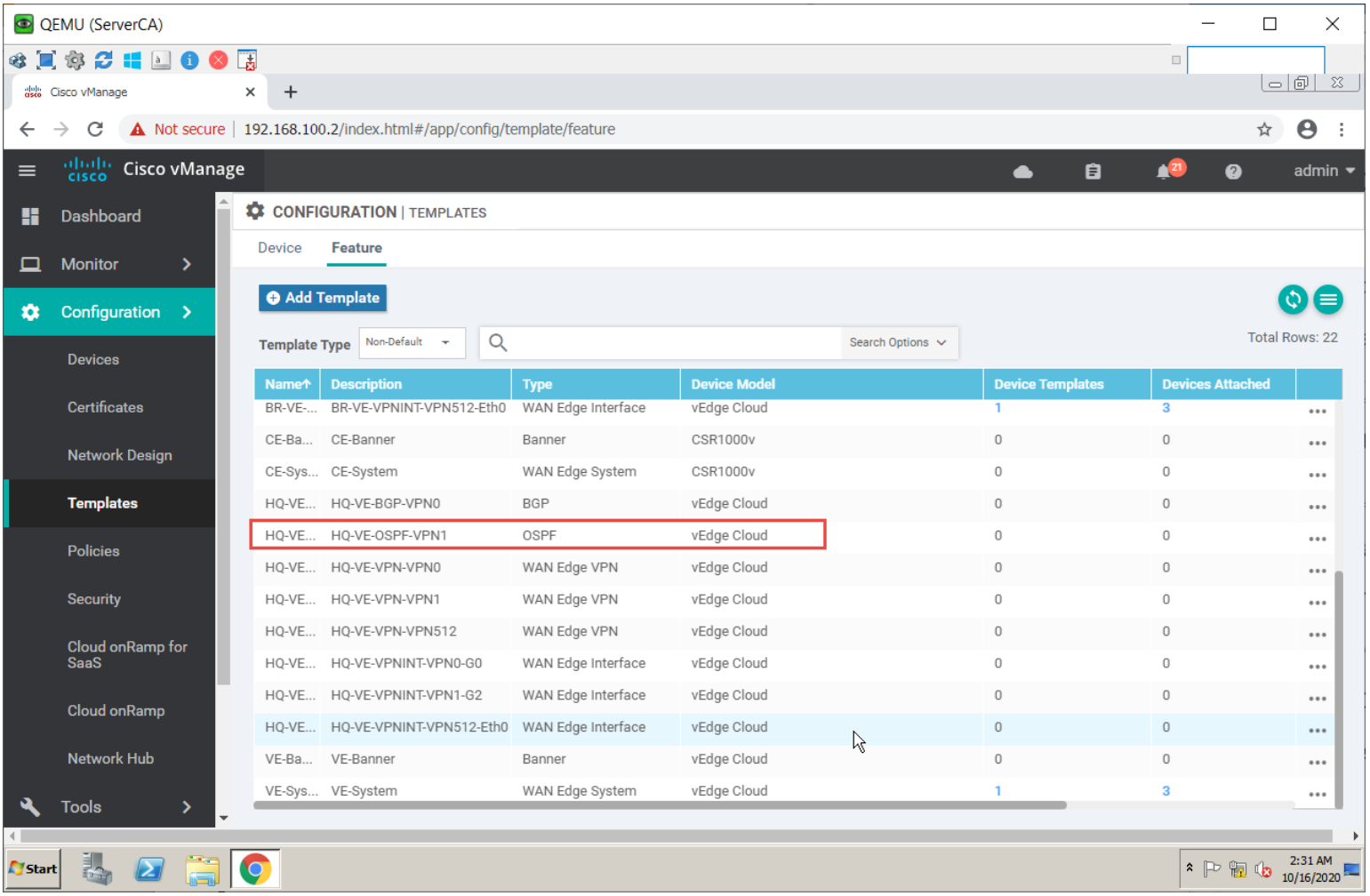


Task 3 – Configure a OSPF Template to be used by HQ vEdge-Cloud Devices for VPN 1

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

  Redistribution
    - Protocol: OMP
- Area Configuration
    - Area Number ➔ Global: 0
    - Area Type ➔ Default

  Interface Configuration
    - Interface Name: ge0/2
- Click Add to add the Interface and Click Add to add OSPF.
- Click Save to save the Template.



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

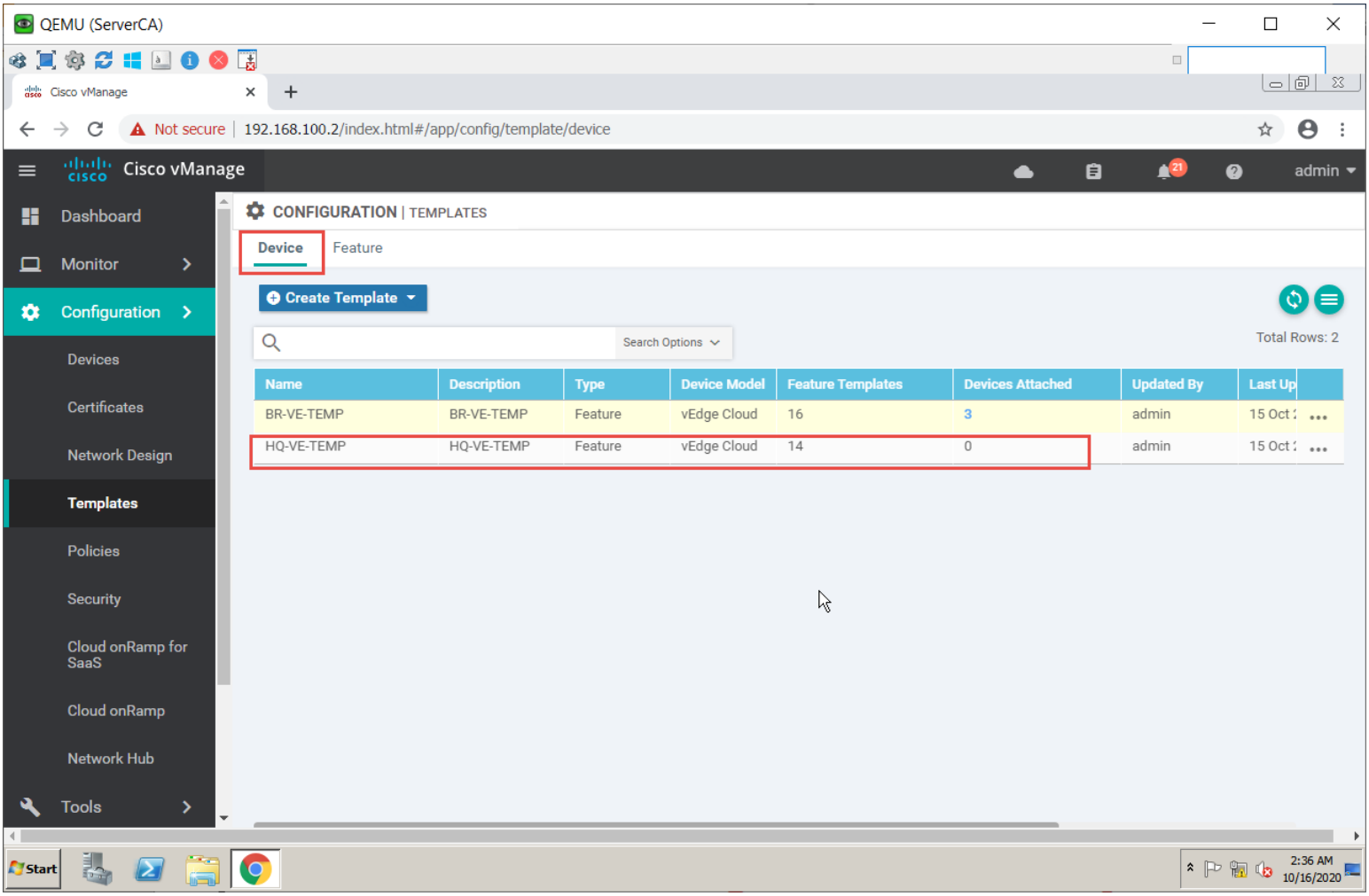
Task 1 – Configure a Device Template for HQ vEdge Devices.

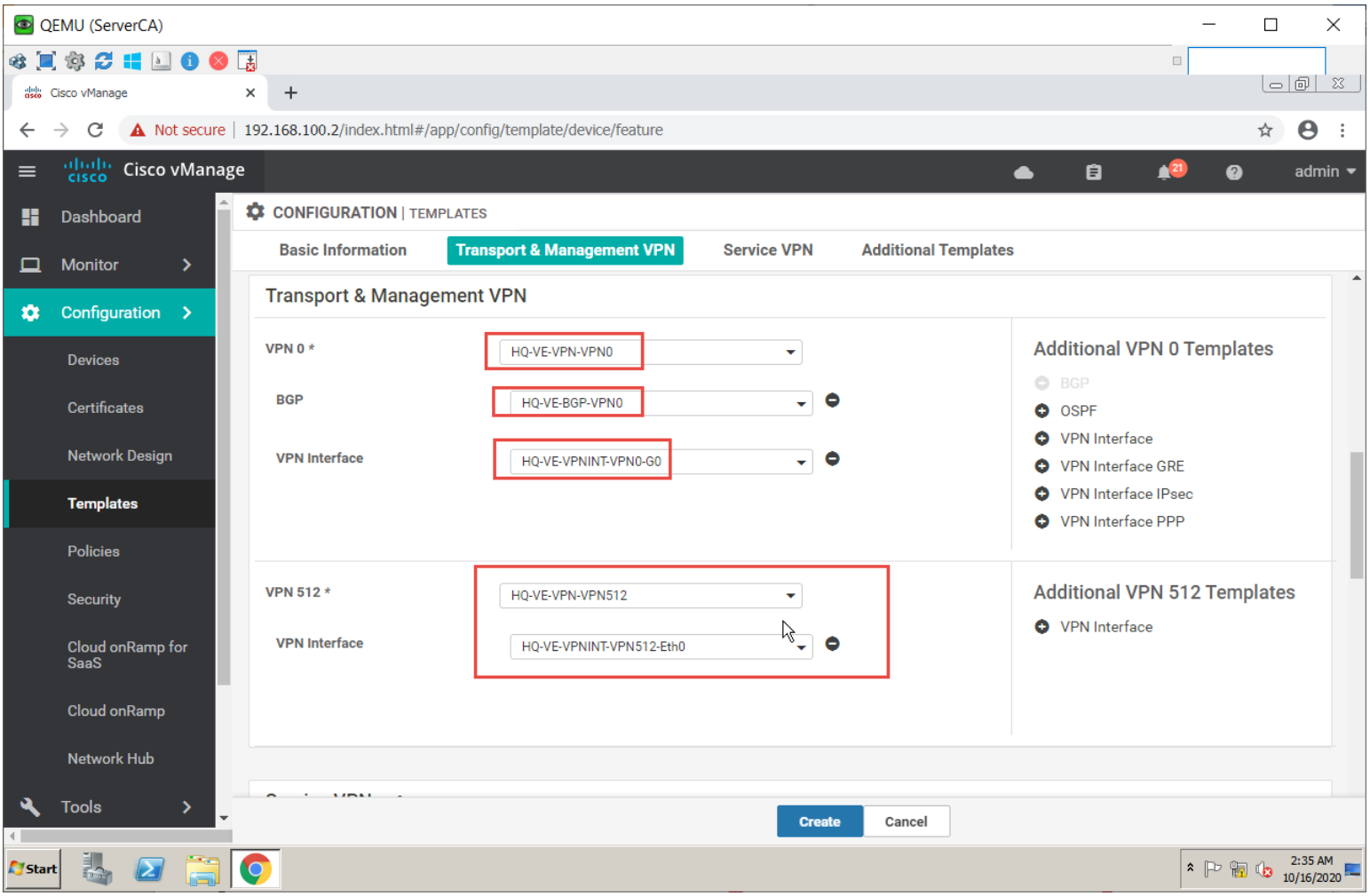
- In vManage, Navigate to Configuration ➔ Templates ➔ Device ➔ Create Template ➔ vEdge Cloud
- Configure the Device Template based on the following:
    - Template Name: HQ-VE-TEMP
    - Description: HQ-VE-TEMP

  Basic Information
    - System ➔ VE-System

  Transport & Management
    - VPN 0: HQ-VE-VPN-VPN0
    - VPN Interface: HQ-VE-VPNINT-VPN0-G0
    - BGP: HQ-VE-BGP-VPN0
    - VPN 512: HQ-VE-VPN-VPN512
    - VPN Interface: HQ-VE-VPNINT-VPN512-E0

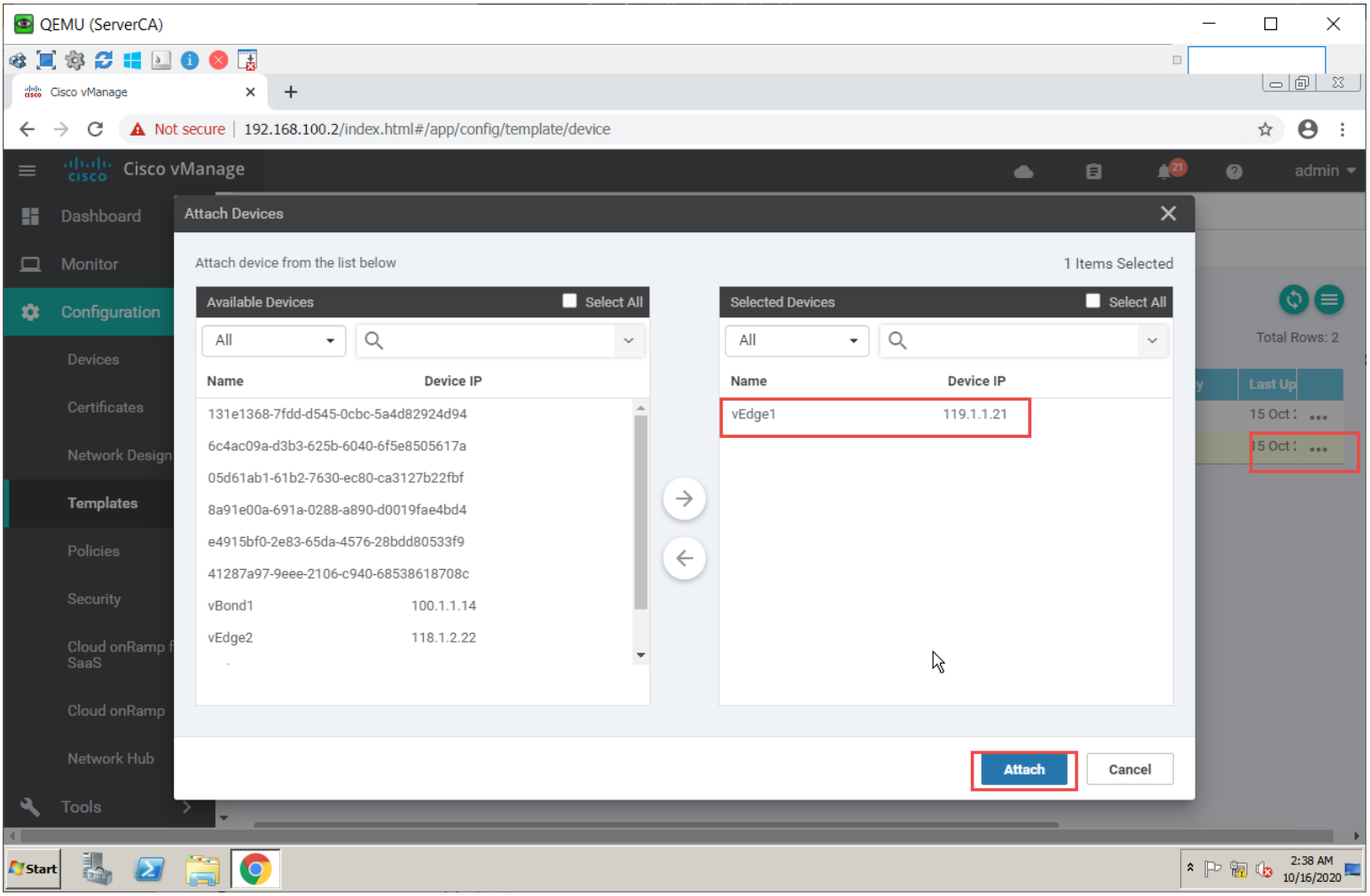
  Service VPN
    - VPN 1: HQ-VE-VPN-VPN1
    - VPN Interface: HQ-VE-VPNINT-VPN1-G2
    - OSPF: HQ-VE-OSPF-VPN1
- Click Save to save the Template.


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/device
Cisco vManage
admin
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
HQ-VE-TEMP
HQ-VE-TEMP
Feature
vEdge Cloud
14
0
admin
15 Oct
Start
2:36 AM
10/16/2020



Task 2 – Attach vEdge1 to the Device Template

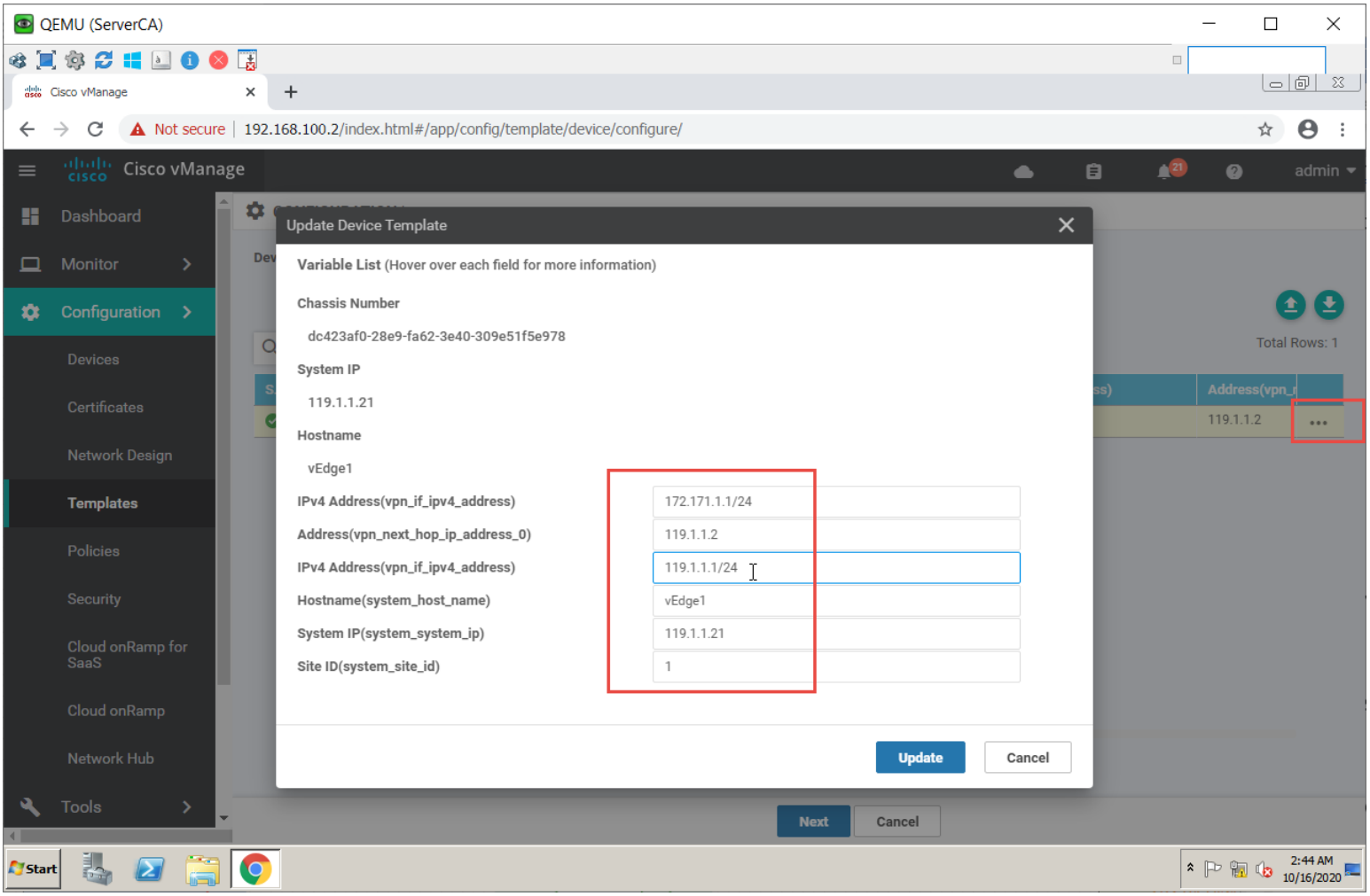
- In vManage, Navigate to Configuration ➔ Templates ➔ Device ➔ HQ-VE-TEMP.
- Click on "…" towards the right-hand side.
- Click Attach Devices.
- Select vEdge1 and click the "➔" button.
- Click Attach.

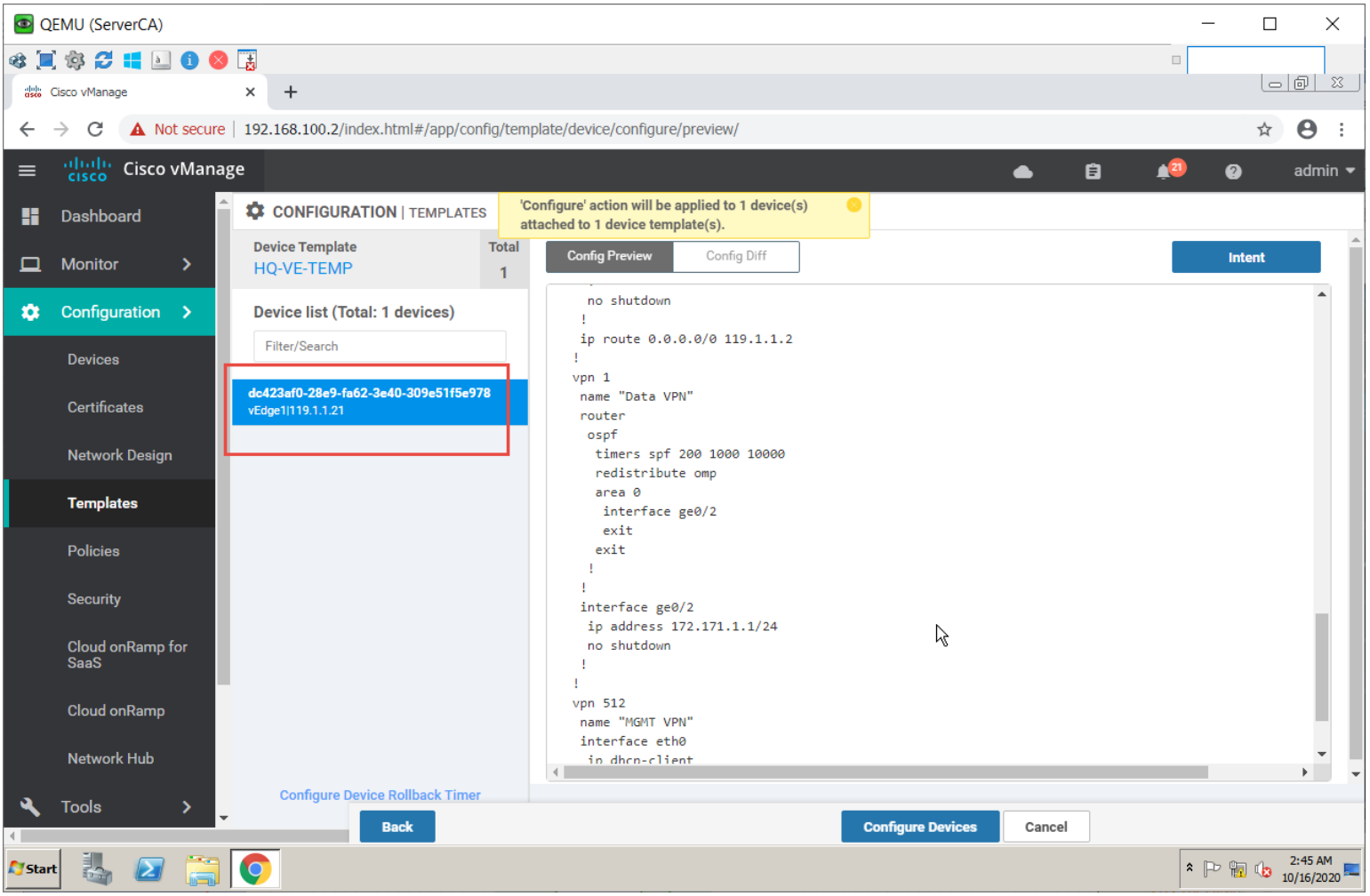


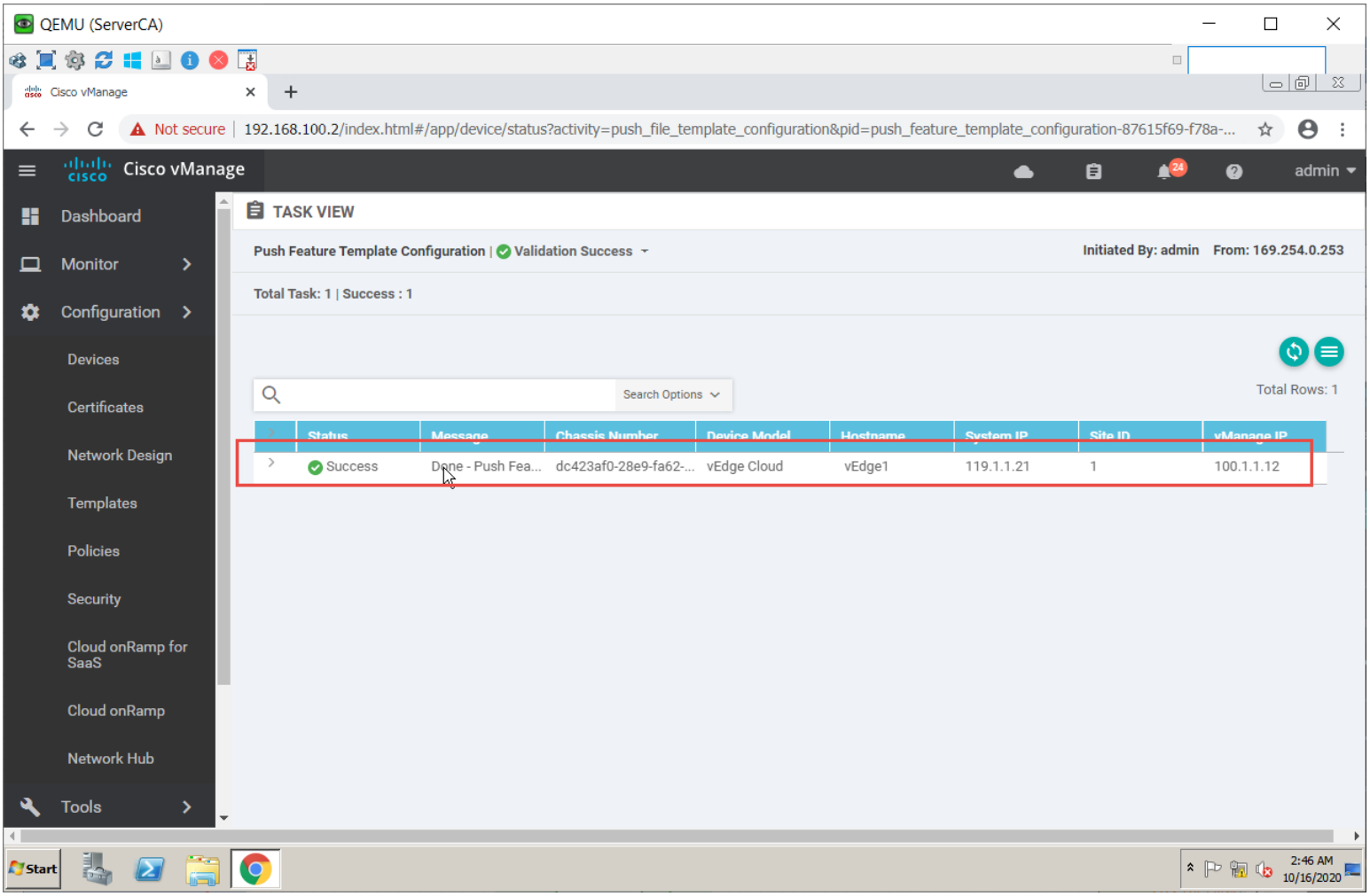
Task 3 – Configure the Variable Parameters for the Feature Templates

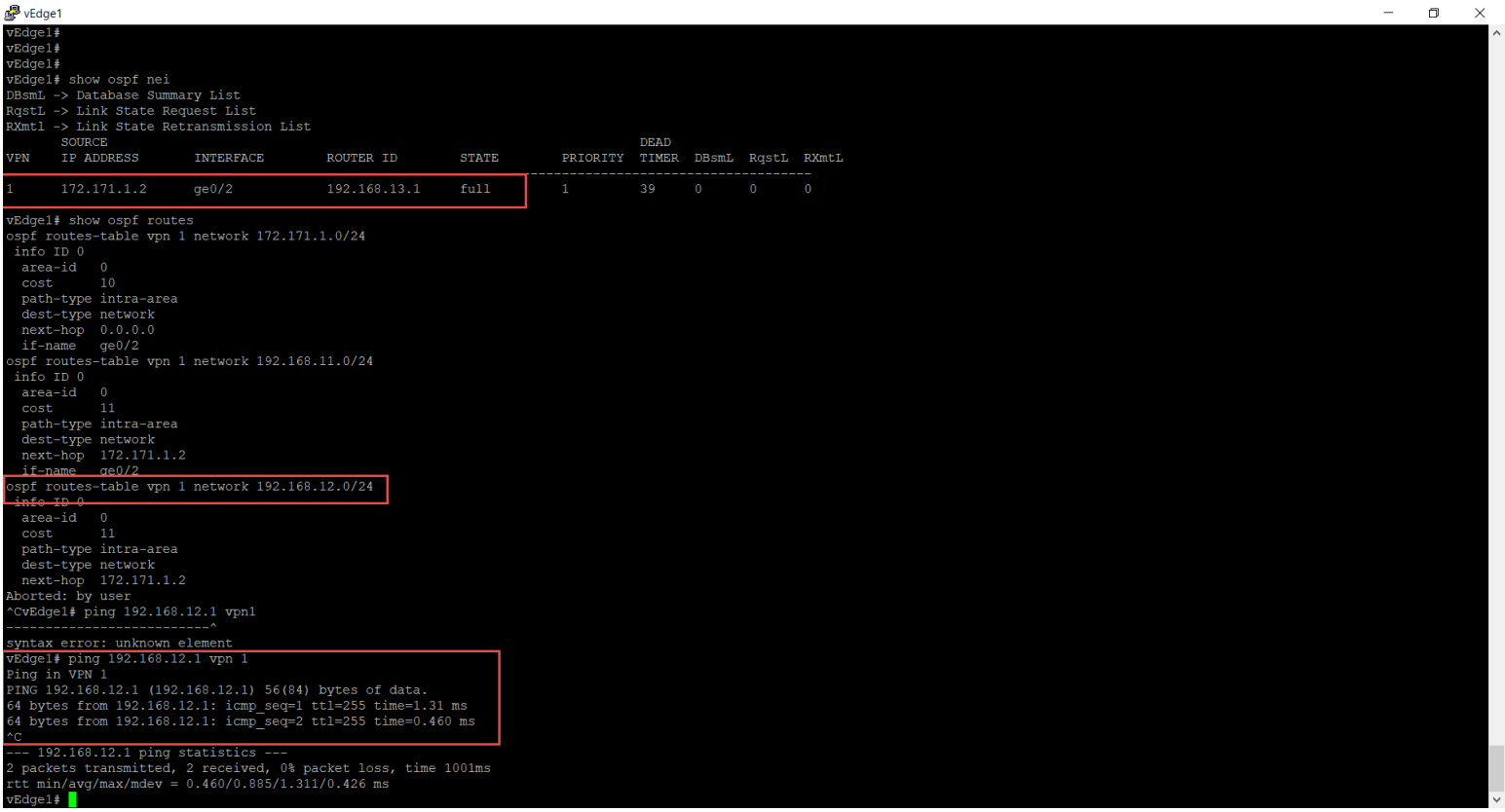
- vEdge1 will appear in the window.
- Click on "…" towards the right-hand side.
- Click Edit Device Template.
- Configure the variables based on the following:
    - Interface IP for ge0/2:172.171.1.1/24
    - Default Gateway for VPN0: 119.1.1.2
    - Interface IP for ge0/0:119.1.1.1/24
    - Hostname: vEdge-1
    - System IP: 119.1.1.21
    - 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.




QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/index.html#/app/config/template/device/configure/preview/
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
'Configure' action will be applied to 1 device(s) attached to 1 device template(s).
Device Template
HQ-VE-TEMP
Total
1
Device list (Total: 1 devices)
Filter/Search
dc423af0-28e9-fa62-3e40-309e51f5e978
vEdge1|119.1.1.21
Config Preview
Config Diff
Intent
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 omp
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
ip dhcp-client
Configure Device Rollback Timer
Back
Configure Devices
Cancel
Start
2:45 AM
10/16/2020


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-87615f69-f78a-...
Cisco vManage
admin
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
Initiated By: admin From: 169.254.0.253
Total Task: 1 | Success : 1
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
Start
2:46 AM
10/16/2020



PuTTY (inactive)

```
  ip dhcp-client
  no shutdown
 !
!
vEdge2# show ip route
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive

                                      PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP
VPN     PREFIX              PROTOCOL  SUB TYPE  IF NAME     ADDR             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

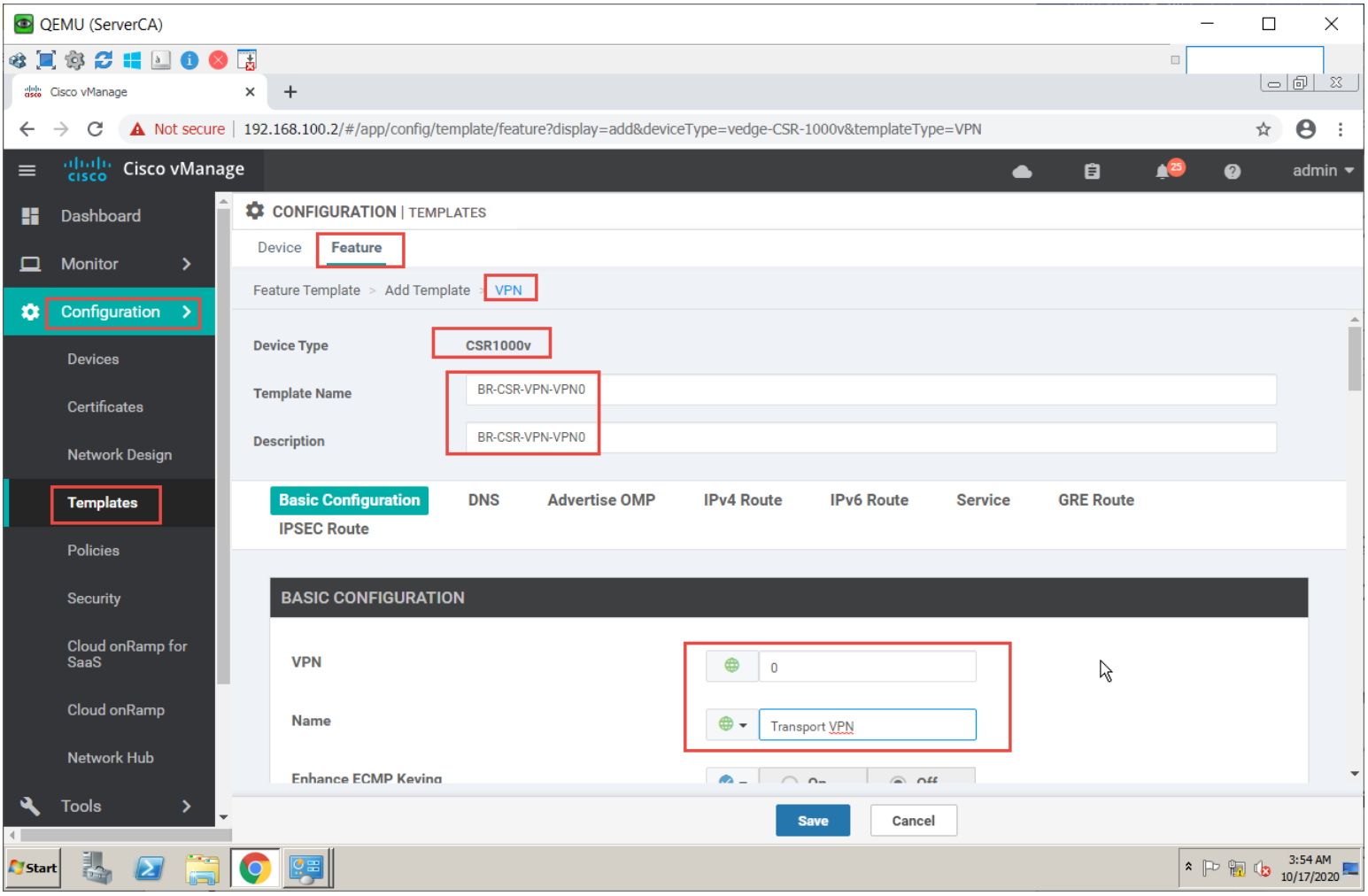
VPN 0

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:
  - Template Name: BR-CSR-VPN-VPN0
  - Description: BR-CSR -VPN-VPN0

  Basic Configuration
  - VPN ➔ Global: 0
  - Name ➔ Global: Transport VPN

  IPv4 Route
  - Prefix ➔ Global: 0.0.0.0/0
  - Next Hop ➔ Device Specific
- Click Save to save the Template.



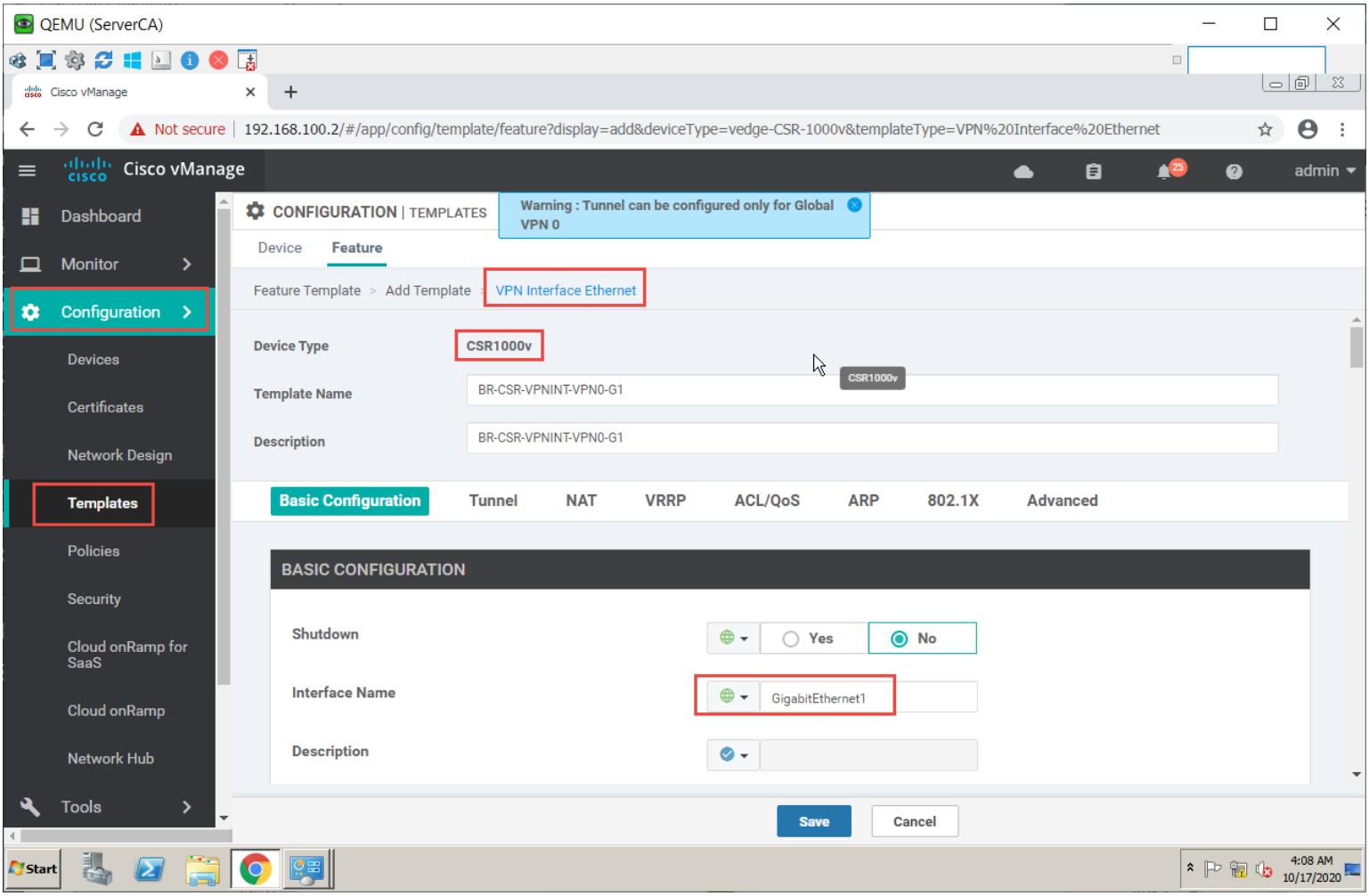
Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 0 for Interface GigabitEthernet1

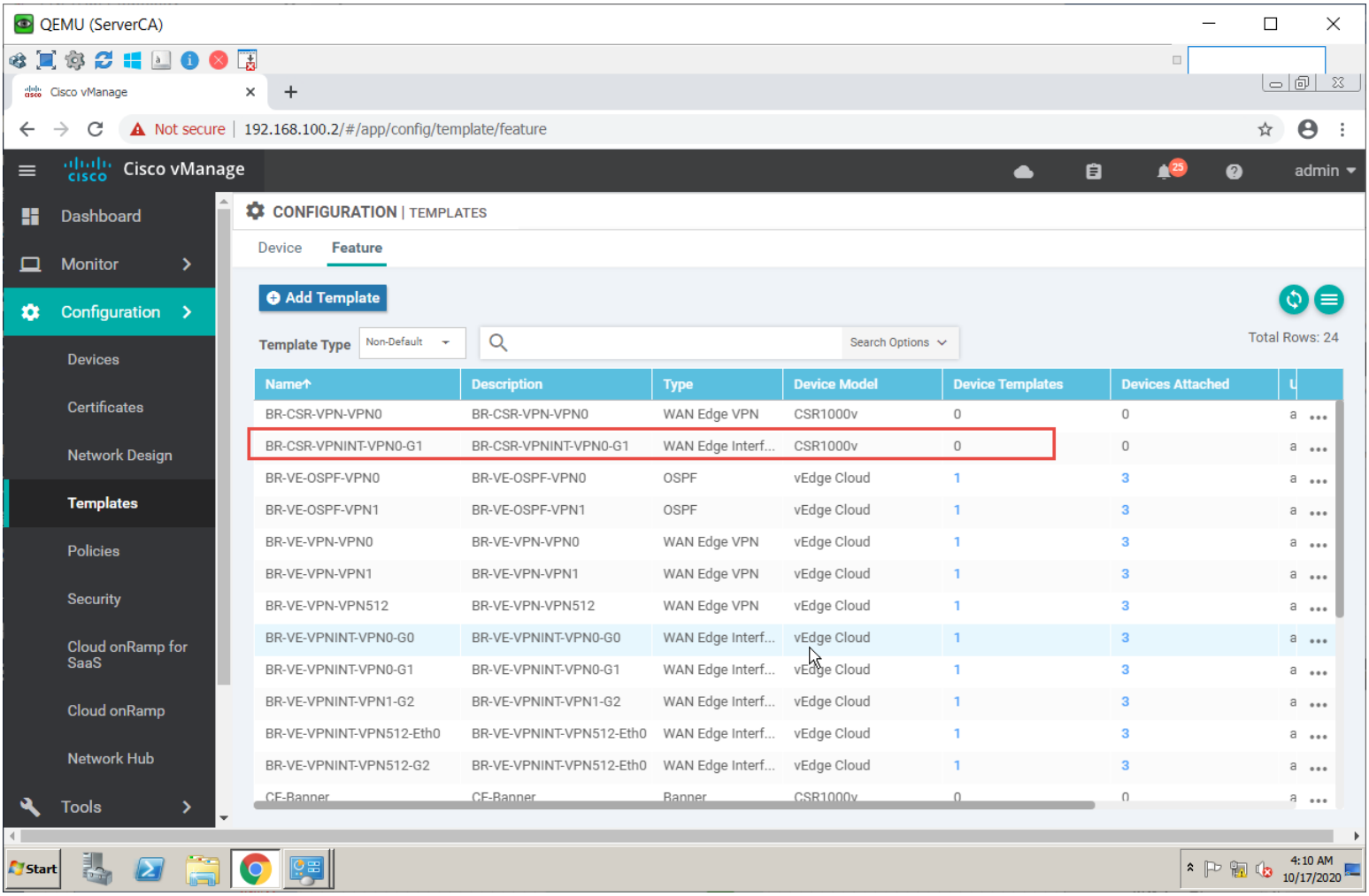
- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ CSR1000v ➔ VPN ➔ VPN Interface Ethernet
- Configure the VPN parameters based on the following:
    - Template Name: BR-CSR-VPNINT-VPN0-G1
    - Description: BR-CSR-VPNINT-VPN0-G1

  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.


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/feature?display=add&deviceType=vedge-CSR-1000v&templateType=VPN%20Interface%20Ethernet
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Warning : Tunnel can be configured only for Global VPN 0
Device
Feature
Feature Template > Add Template > VPN Interface Ethernet
Device Type
CSR1000v
Template Name
BR-CSR-VPNINT-VPN0-G1
Description
BR-CSR-VPNINT-VPN0-G1
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
BASIC CONFIGURATION
Shutdown
Yes
No
Interface Name
GigabitEthernet1
Description
Save
Cancel
Start
4:08 AM
10/17/2020

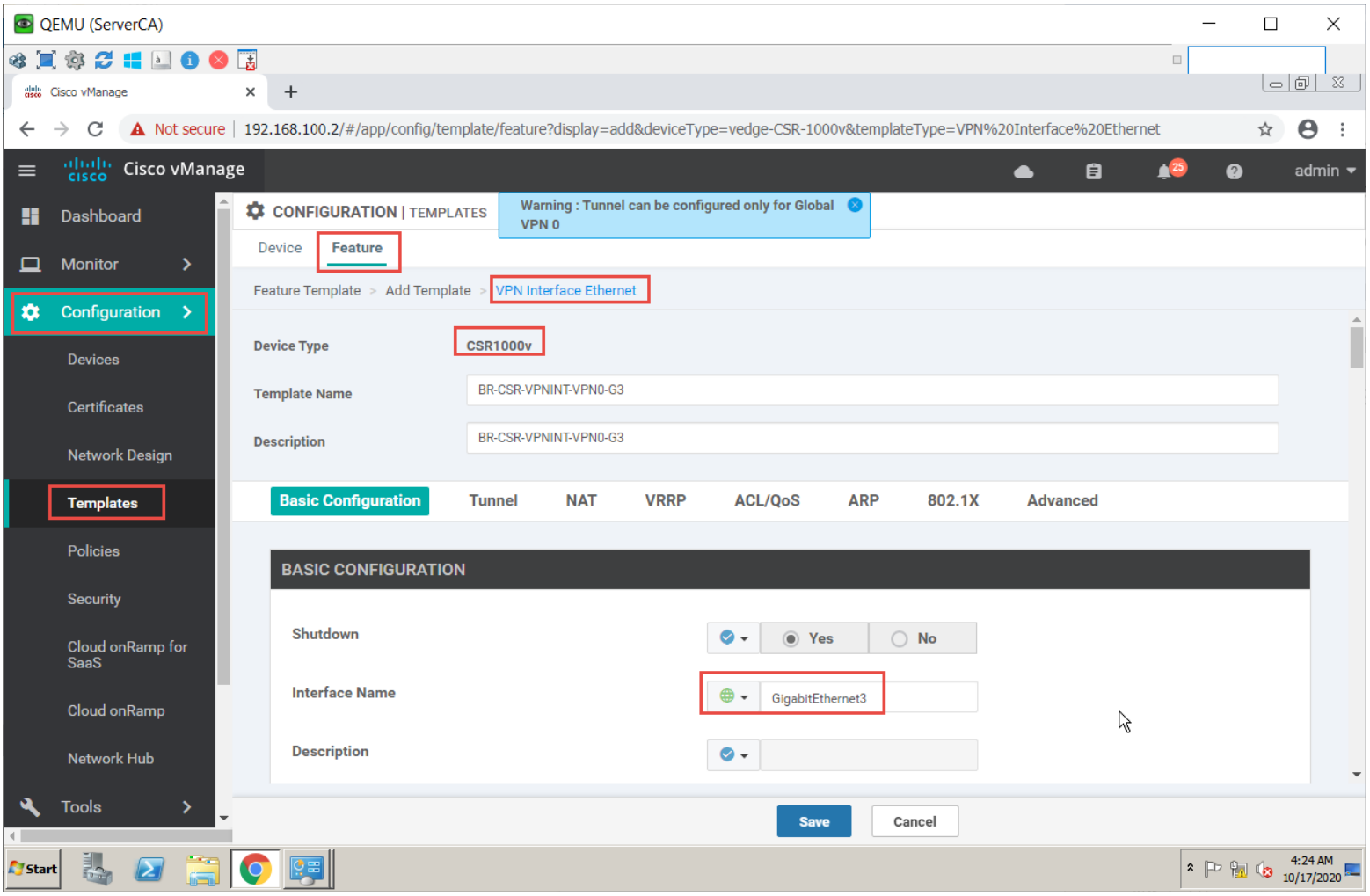


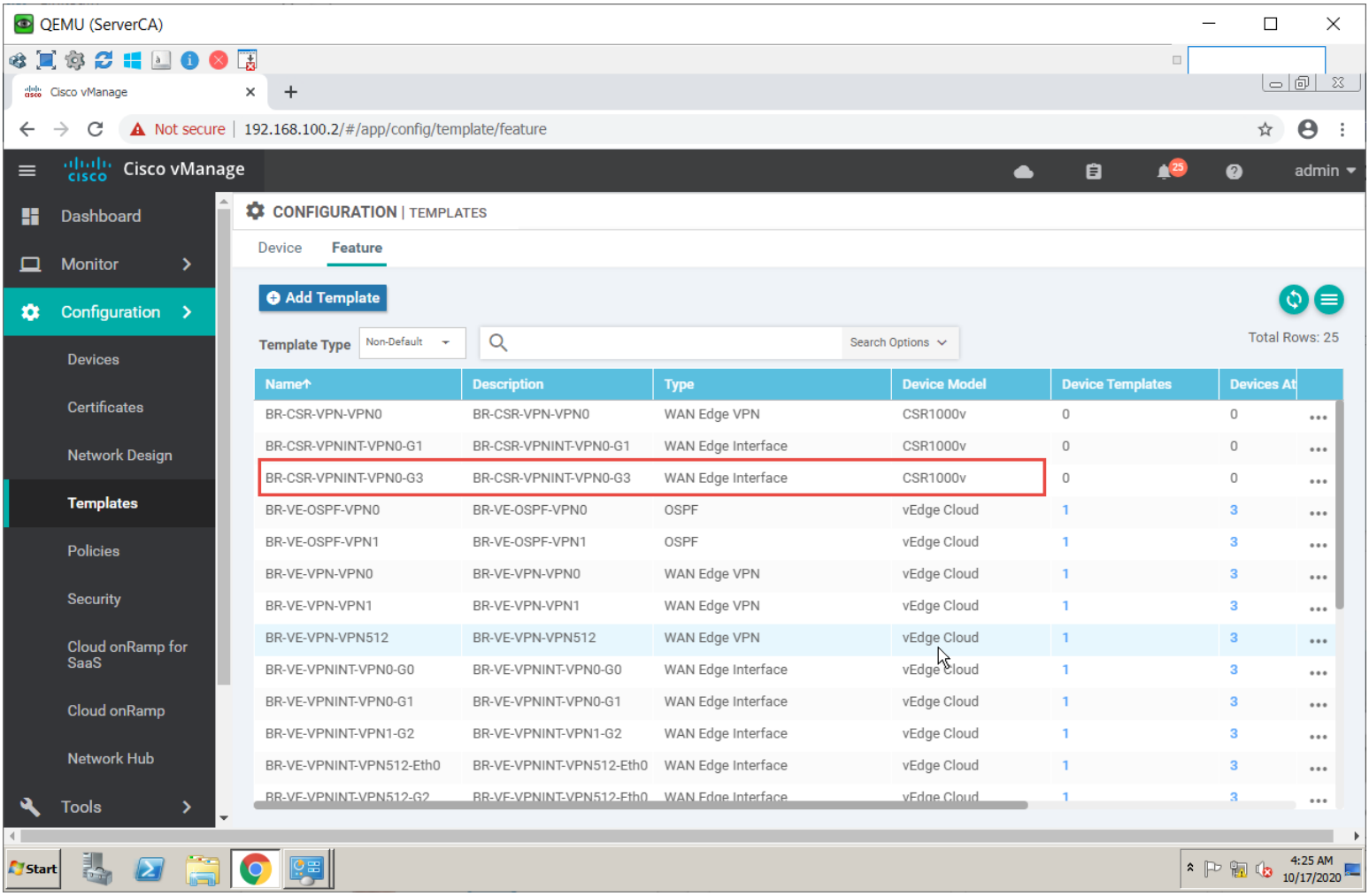
Task 3 – Configure a VPN Interface Template to be used by CSR for VPN 0 for Interface GigabitEthernet3

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

- NETCONF ➔ Global : On
- SSH ➔ Global : On

- Click Save to save the Template.



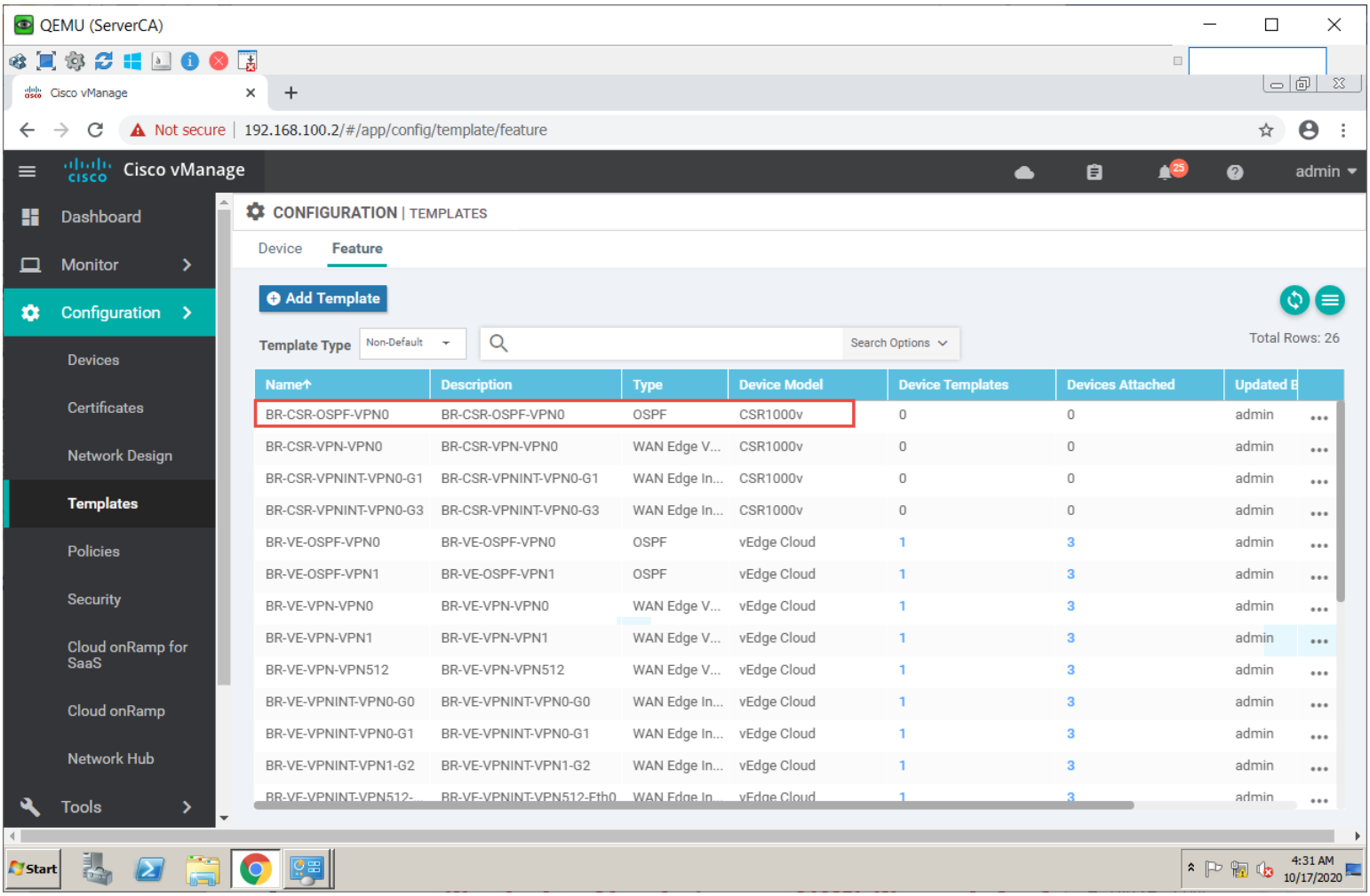


Task 4 – Configure a OSPF Template to be used by CSR for VPN 0

- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ CSR1000v ➔ Other Templates ➔ Cisco OSPF
- Configure the OSPF parameters based on the following:
    - Template Name: BR-CSR-OSPF-VPN0
    - Description: BR-CSR-OSPF-VPN0

  Area Configuration
    - Area Number ➔ Global: 0
    - Area Type ➔ Default

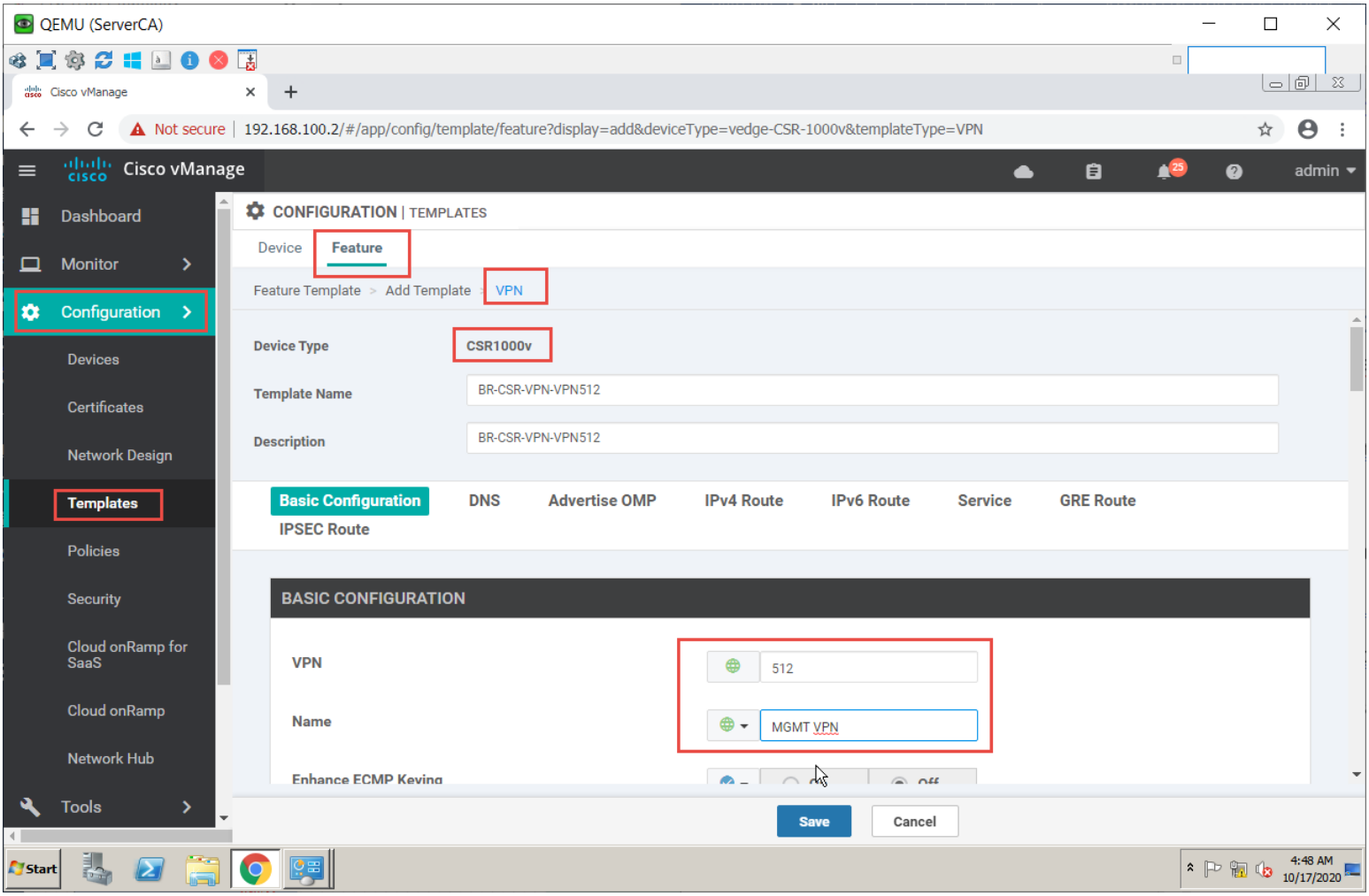
  Interface Configuration
    - Interface Name: GigabitEthernet3
    - OSPF Network Type: Point-to-Point
- Click Add to add the Interface and Click Add to add OSPF.
- Click Save to save the Template.

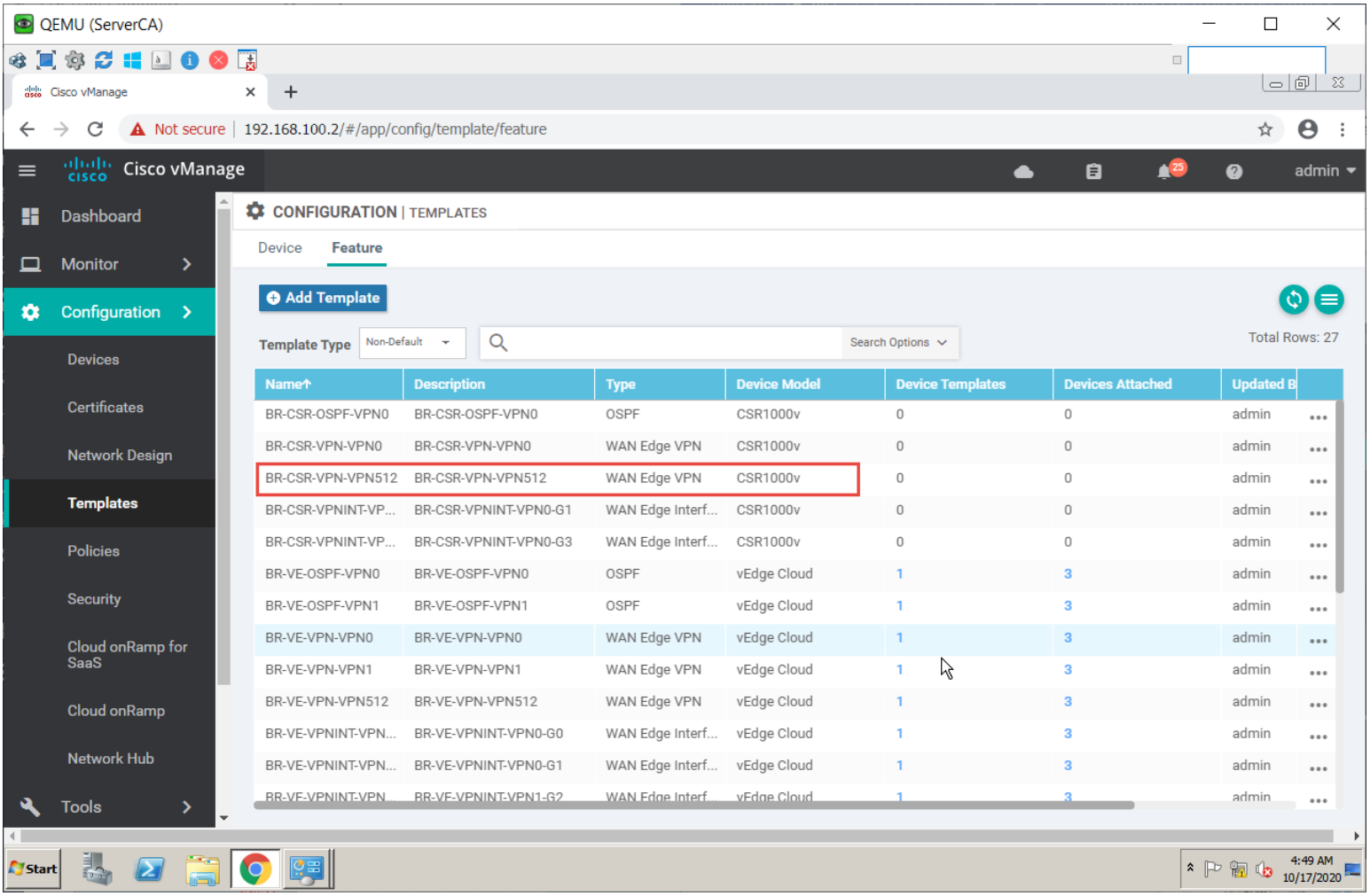


VPN 512

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
- Basic Configuration
- o VPN ➔ Global : 512
- o Name ➔ Global : MGMT VPN
- Click Save to save the Template.

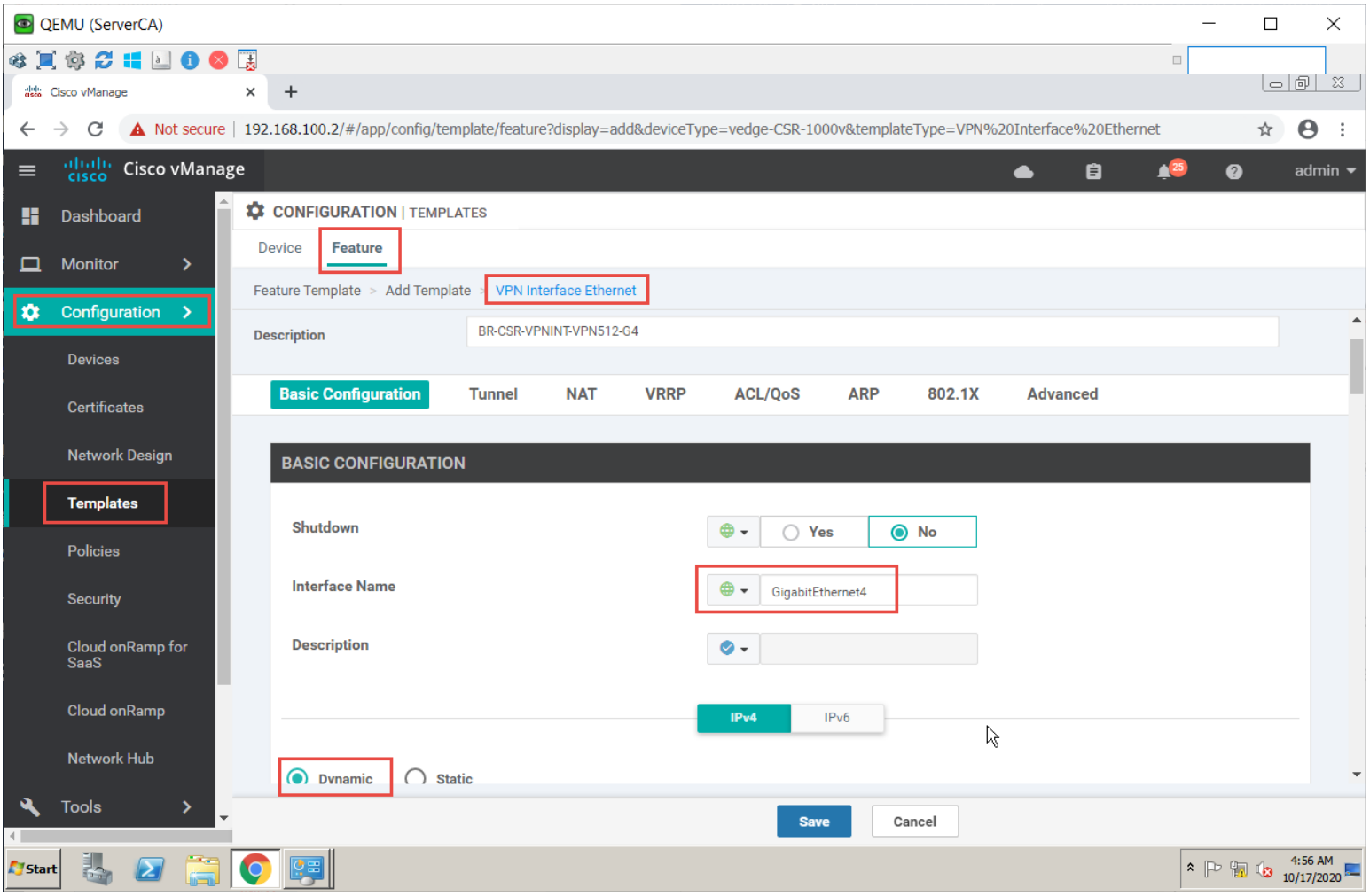

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/feature?display=add&deviceType=vedge-CSR-1000v&templateType=VPN
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template | VPN
Device Type
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
512
Name
MGMT VPN
Save
Cancel
Start
4:48 AM
10/17/2020

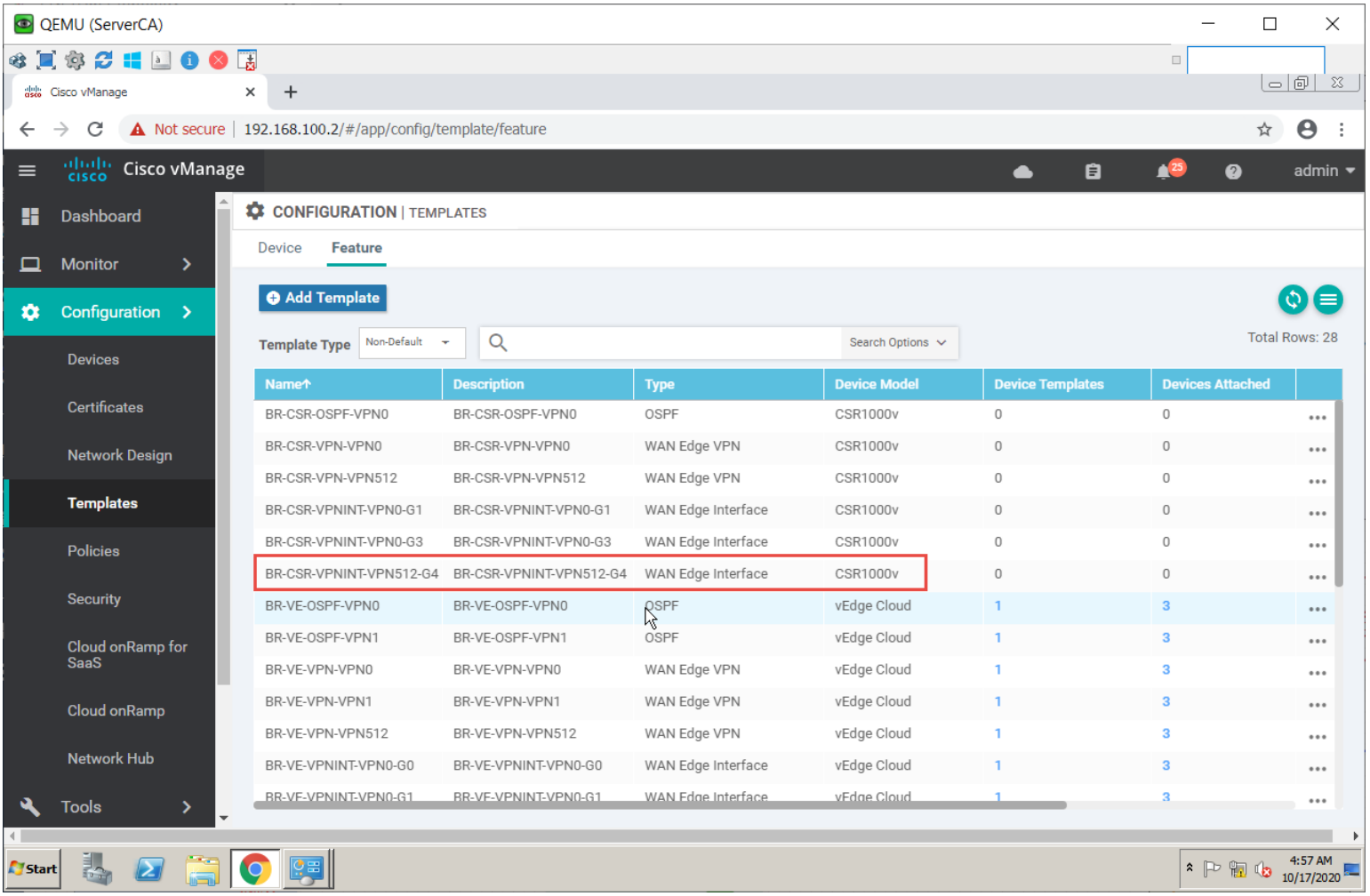


Task 2 – Configure a VPN Interface Template to be used by CSR for VPN 512 for Interface GigabitEthernet4

- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ CSR1000v ➔ VPN ➔ Cisco VPN Interface Ethernet
- Configure the VPN parameters based on the following:
    - Template Name : BR-CSR-VPNINT-VPN512-G4
    - Description : BR-CSR-VPNINT-VPN512-G4

  Basic Configuration
    - Shutdown ➔ Global: No
    - Interface Name ➔ Global: GigabitEthernet4
    - IPv4 Address ➔ Dynamic
- 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%20Interface%20Ethernet
Cisco vManage
admin
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 Interface Ethernet
Description
BR-CSR-VPNINT-VPN512-G4
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
BASIC CONFIGURATION
Shutdown
Yes
No
Interface Name
GigabitEthernet4
Description
IPv4
IPv6
Dynamic
Static
Save
Cancel
Start
4:56 AM
10/17/2020

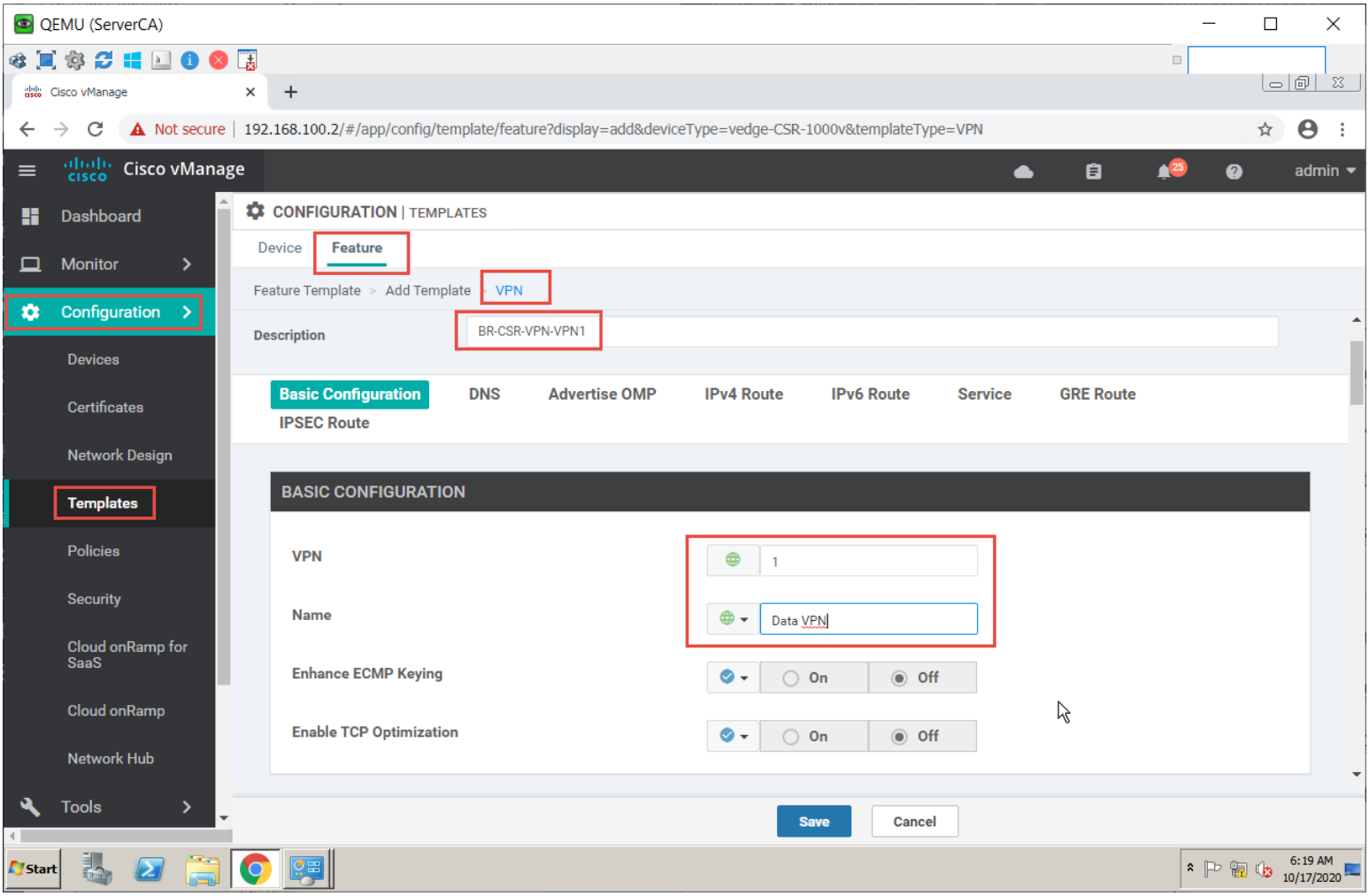


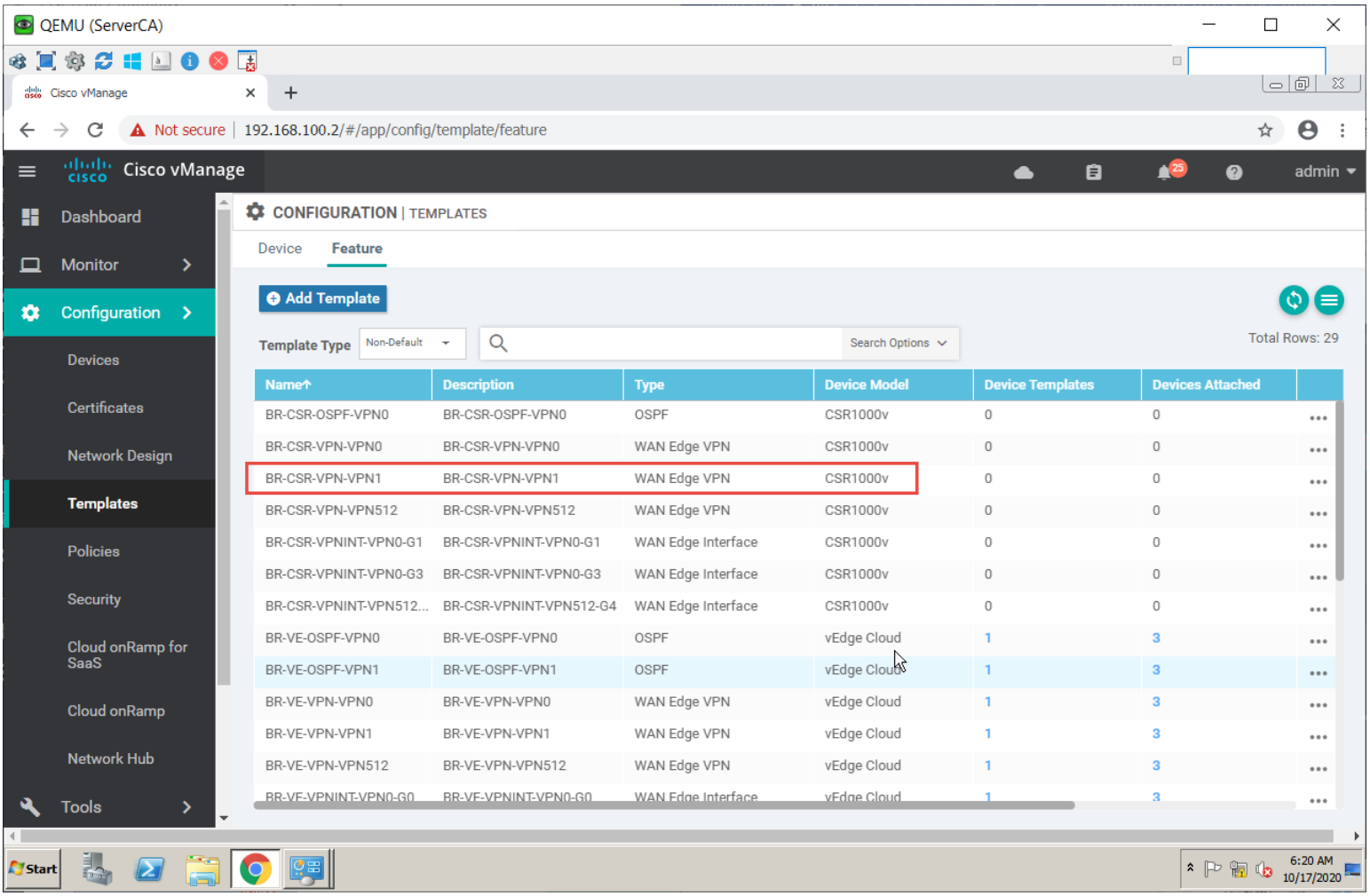
VPN 1

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:
    - Template Name : BR-CSR-VPN-VPN1
    - Description : BR-CSR-VPN-VPN1

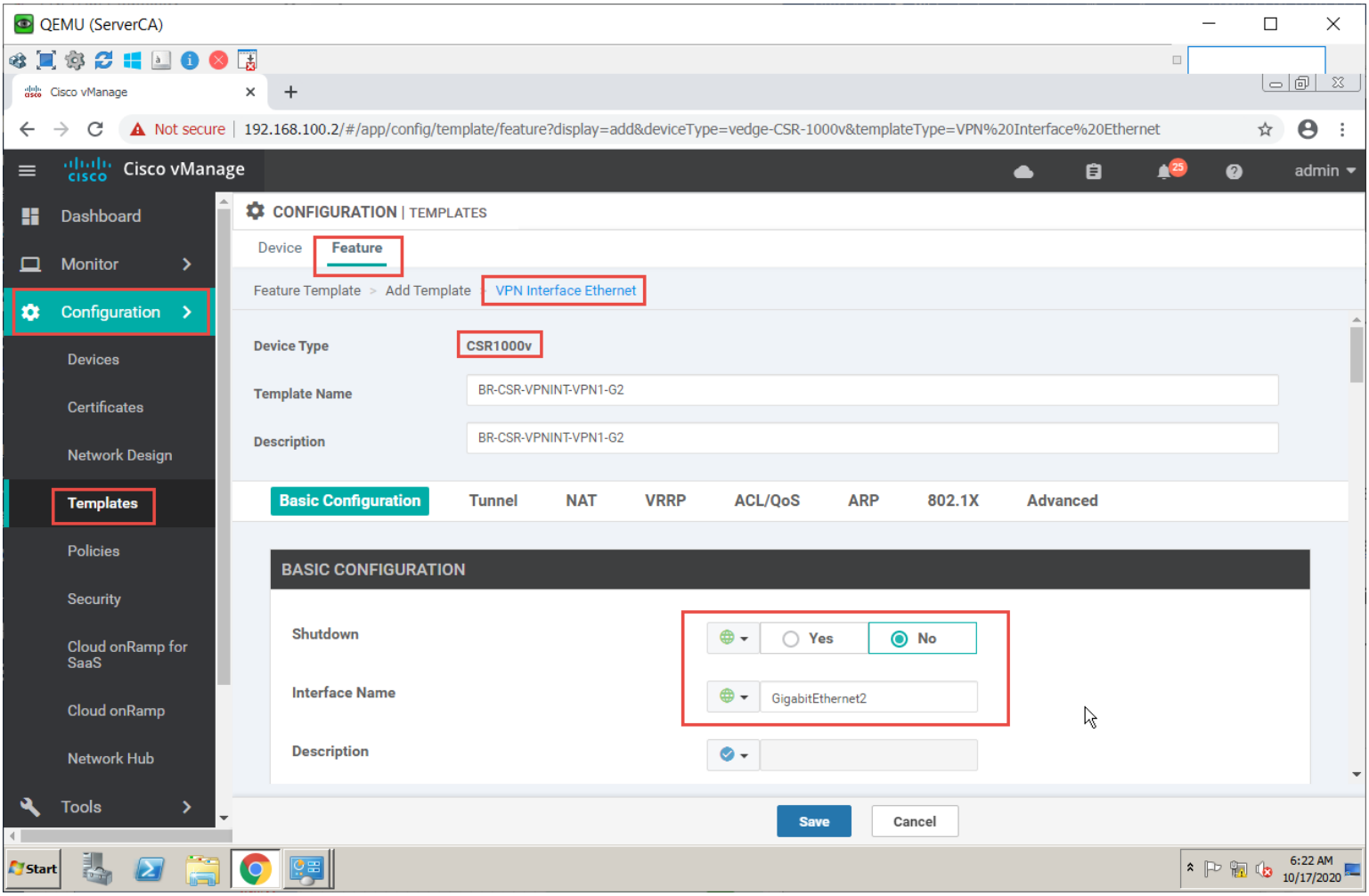
  Basic Configuration
    - VPN ➔ Global : 1
    - Name ➔ Global : Data VPN
- Click Save to save the Template.

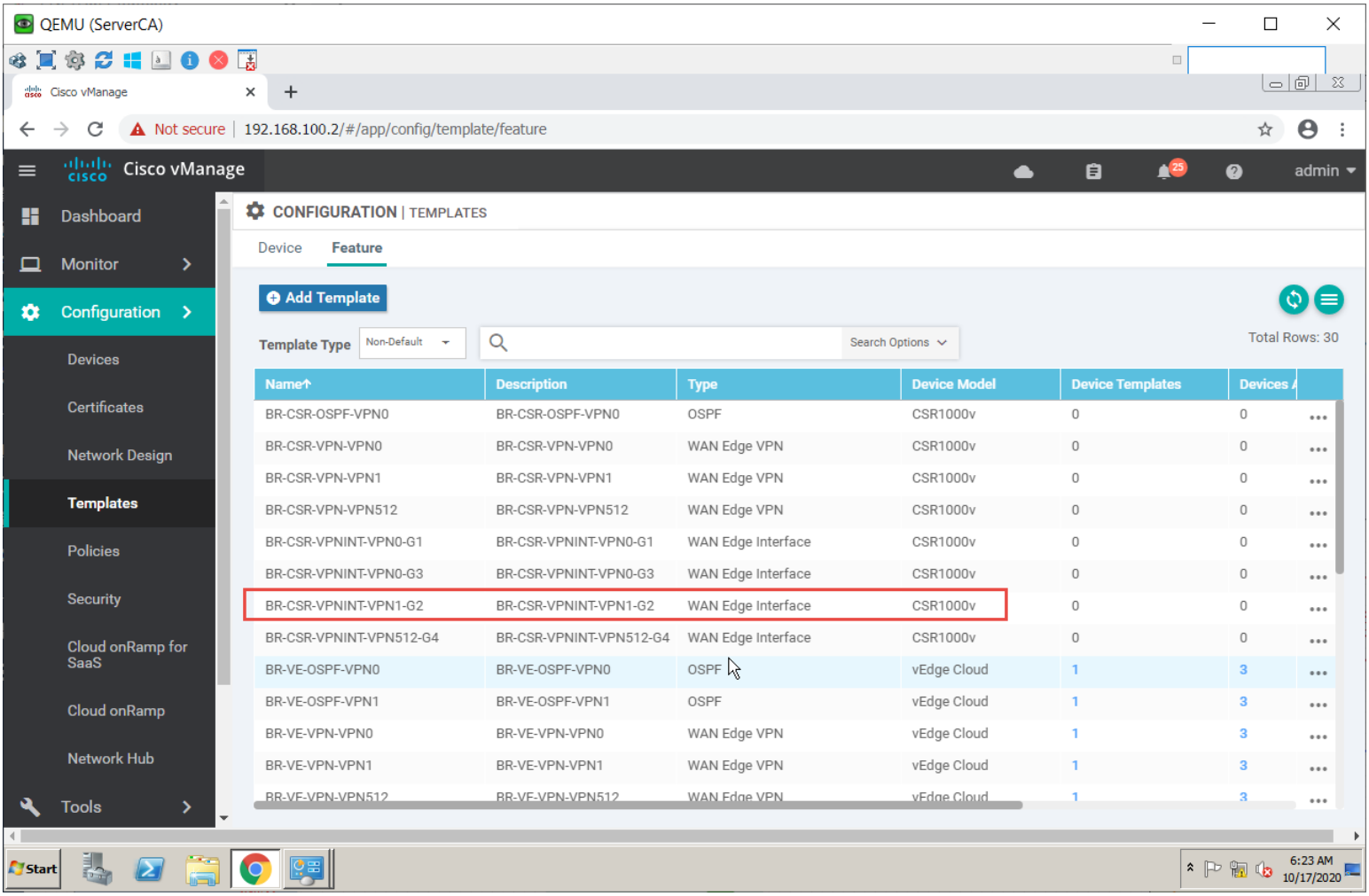

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/feature?display=add&deviceType=vedge-CSR-1000v&templateType=VPN
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > VPN
Description
BR-CSR-VPN-VPN1
Basic Configuration
DNS
Advertise OMP
IPv4 Route
IPv6 Route
Service
GRE Route
IPSEC Route
BASIC CONFIGURATION
VPN
1
Name
Data VPN
Enhance ECMP Keying
On
Off
Enable TCP Optimization
On
Off
Save
Cancel
Start
6:19 AM
10/17/2020



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:
  - Template Name : BR-CSR-VPNINT-VPN1-G2
  - Description : BR-CSR-VPNINT-VPN1-G2
- Basic Configuration
  - Shutdown ➔ Global : No
  - Interface Name ➔ Global : GigabitEthernet2
  - IPv4 Address ➔ Static -> Device Specific
- 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%20Interface%20Ethernet
Cisco vManage
admin
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 Interface Ethernet
Device Type
CSR1000v
Template Name
BR-CSR-VPNINT-VPN1-G2
Description
BR-CSR-VPNINT-VPN1-G2
Basic Configuration
Tunnel
NAT
VRRP
ACL/QoS
ARP
802.1X
Advanced
BASIC CONFIGURATION
Shutdown
Yes
No
Interface Name
GigabitEthernet2
Description
Save
Cancel
Start
6:22 AM
10/17/2020



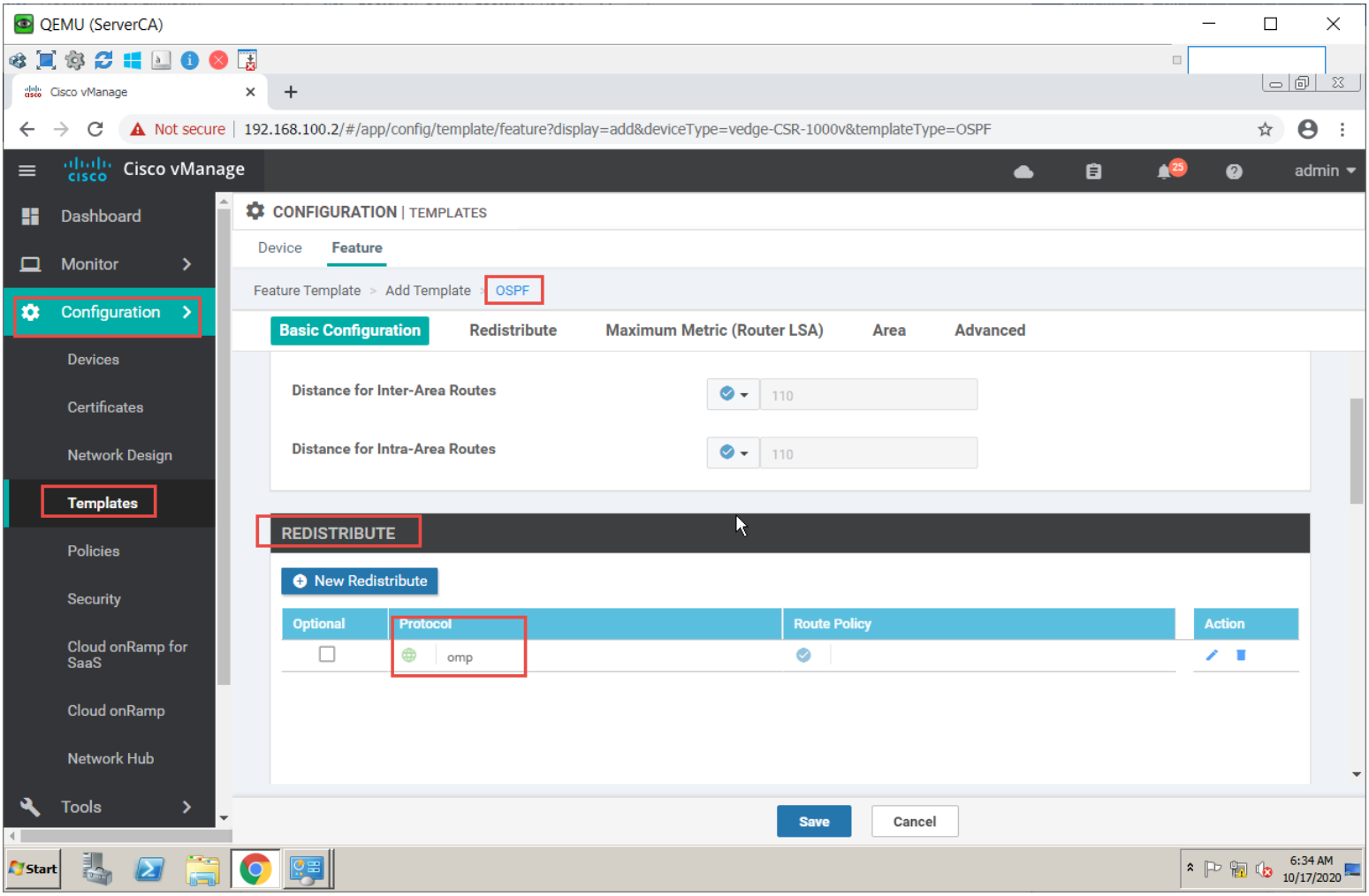
Task 3 – Configure a OSPF Template to be used by CSR for VPN 1

- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ CSR1000v ➔ Other Templates ➔ Cisco OSPF
- Configure the OSPF parameters based on the following:
    - Template Name : BR-CSR-OSPF-VPN1
    - Description : BR-CSR-OSPF-VPN1

  Redistribution
    - Protocol : OMP

  Area Configuration
    - Area Number ➔ Global : 0
    - Area Type ➔ Default

  Interface Configuration
    - 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-CSR-1000v&templateType=OSPF
Cisco vManage
admin
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 > OSPF
Basic Configuration
Redistribute
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
omp
Save
Cancel
Start
6:34 AM
10/17/2020

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

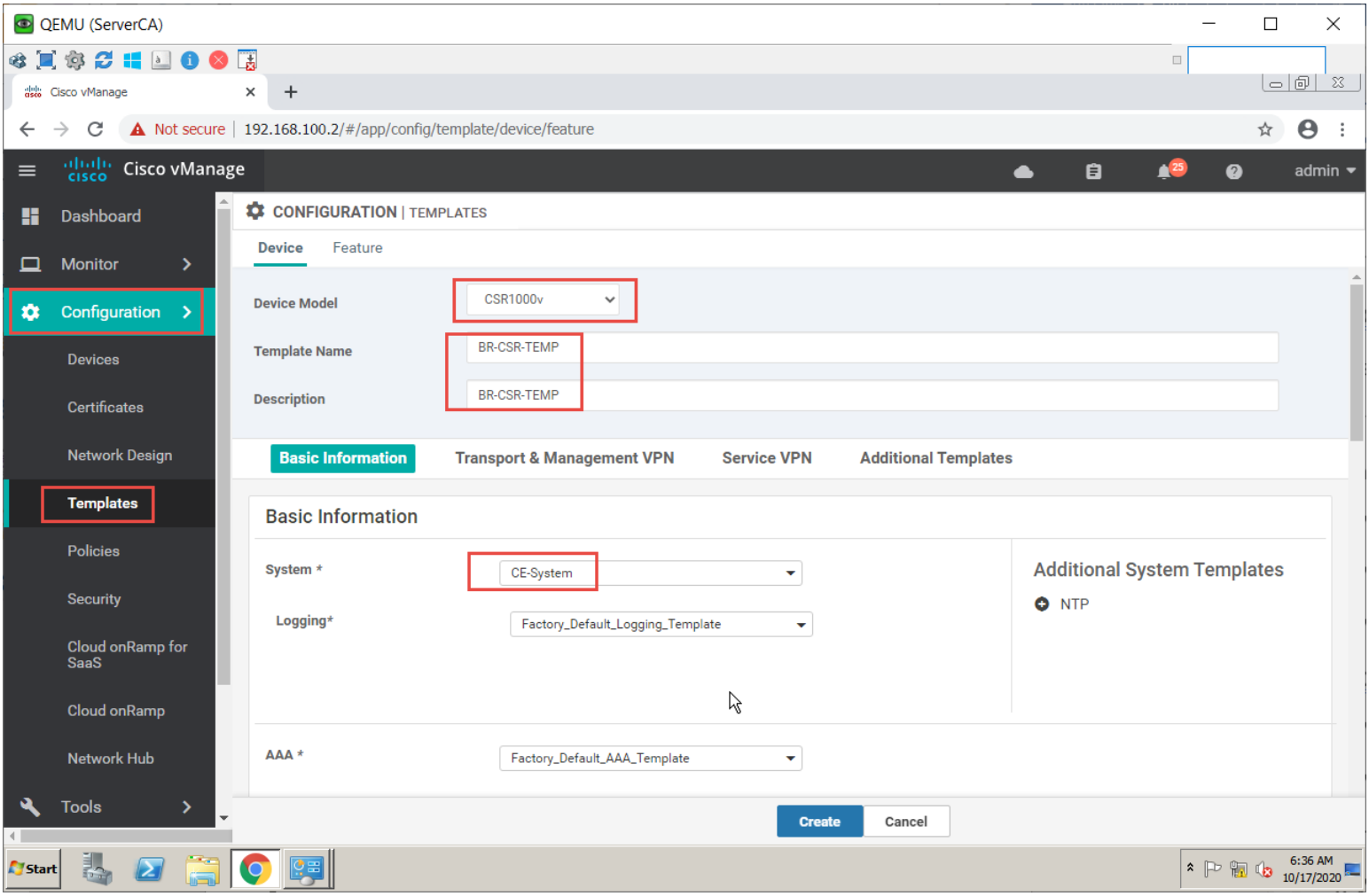
Task 1 – Configure a Device Template for CSR Branch Devices.

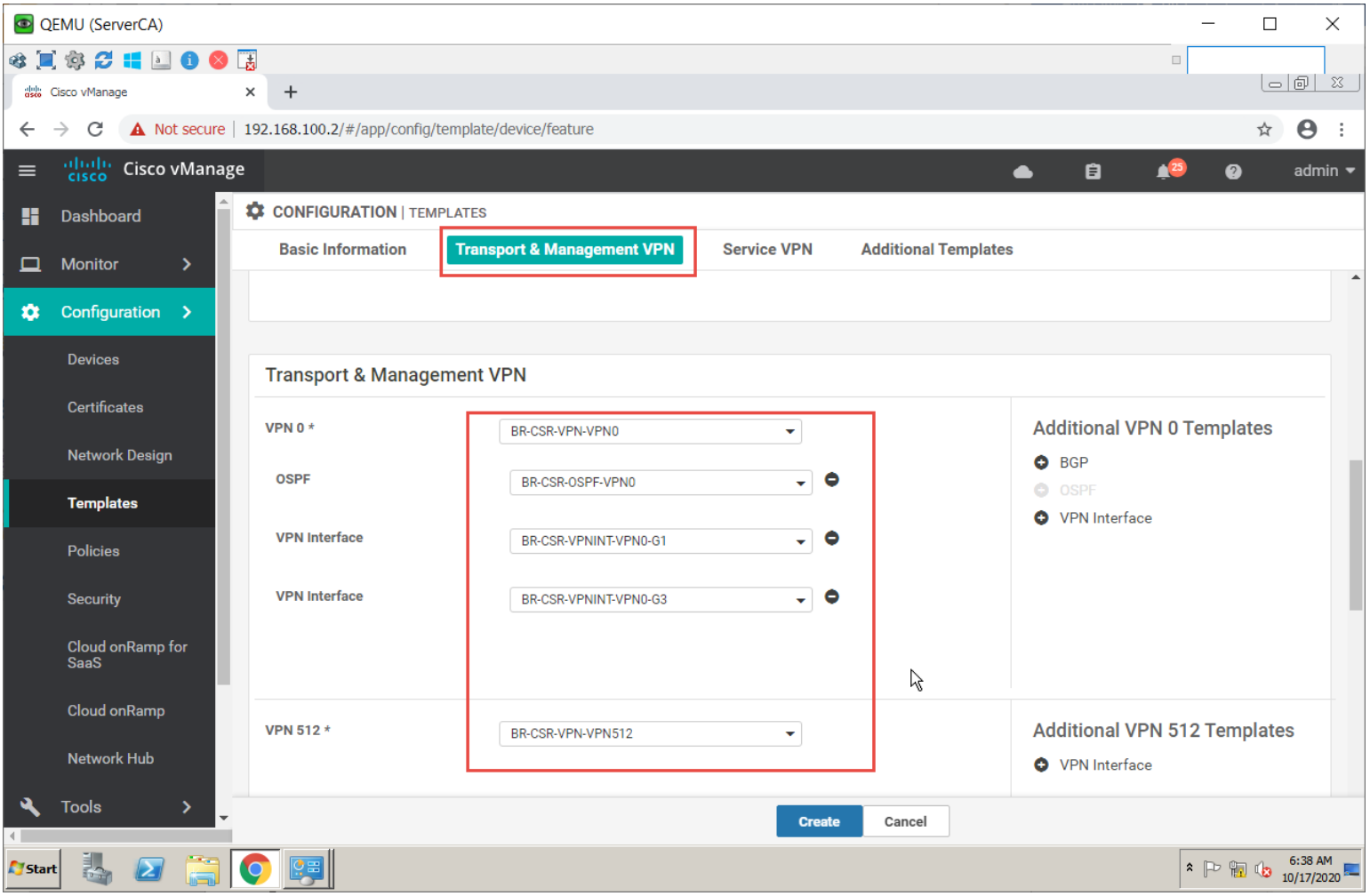
- In vManage, Navigate to Configuration ➔ Templates ➔ Device ➔ Create Template ➔ CSR1000v
- Configure the Device Template based on the following:
    - Template Name : BR-CSR-TEMP
    - Description : BR-CSR-TEMP

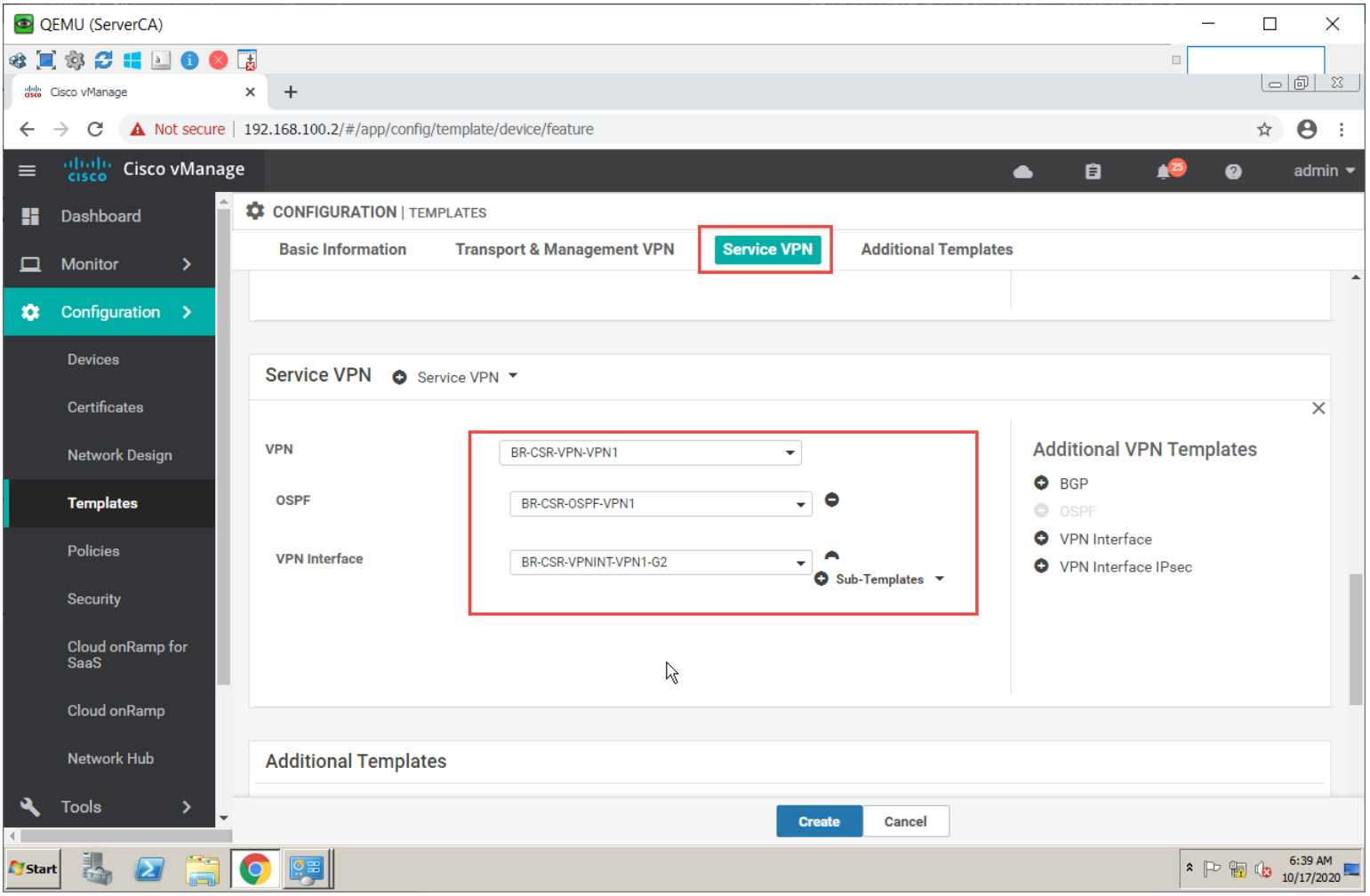
  Basic Information
    - System ➔ CE-System

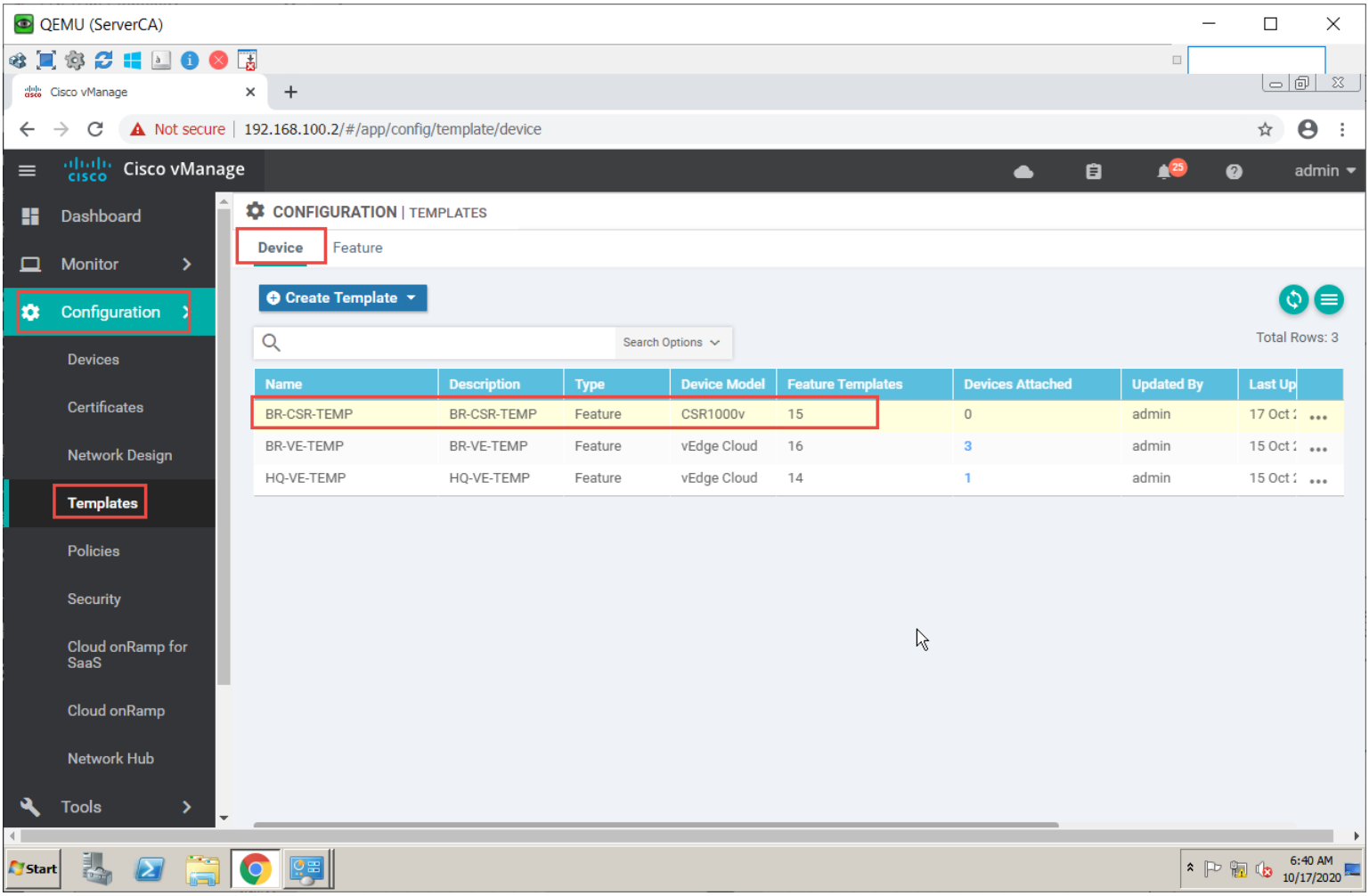
  Transport & Management
    - VPN 0 : BR-CSR-VPN-VPN0
    - VPN Interface : BR-CSR-VPNINT-VPN0-G1
    - VPN Interface : BR-CSR-VPNINT-VPN0-G3
    - OSPF : BR-CSR-OSPF-VPN0
    - VPN 512 : BR-CSR-VPN-VPN512
    - VPN Interface : BR-CSR-VPNINT-VPN512-G4

  Service VPN
    - VPN 1 : BR-CSR-VPN-VPN1
    - VPN Interface : BR-CSR-VPNINT-VPN1-G2
    - OSPF : BR-CSR-OSPF-VPN1
- Click Save to save the Template.


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/device/feature
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Device
Feature
Device Model
CSR1000v
Template Name
BR-CSR-TEMP
Description
BR-CSR-TEMP
Basic Information
Transport & Management VPN
Service VPN
Additional Templates
Basic Information
System *
CE-System
Logging*
Factory_Default_Logging_Template
AAA *
Factory_Default_AAA_Template
Additional System Templates
NTP
Create
Cancel
Start
6:36 AM
10/17/2020

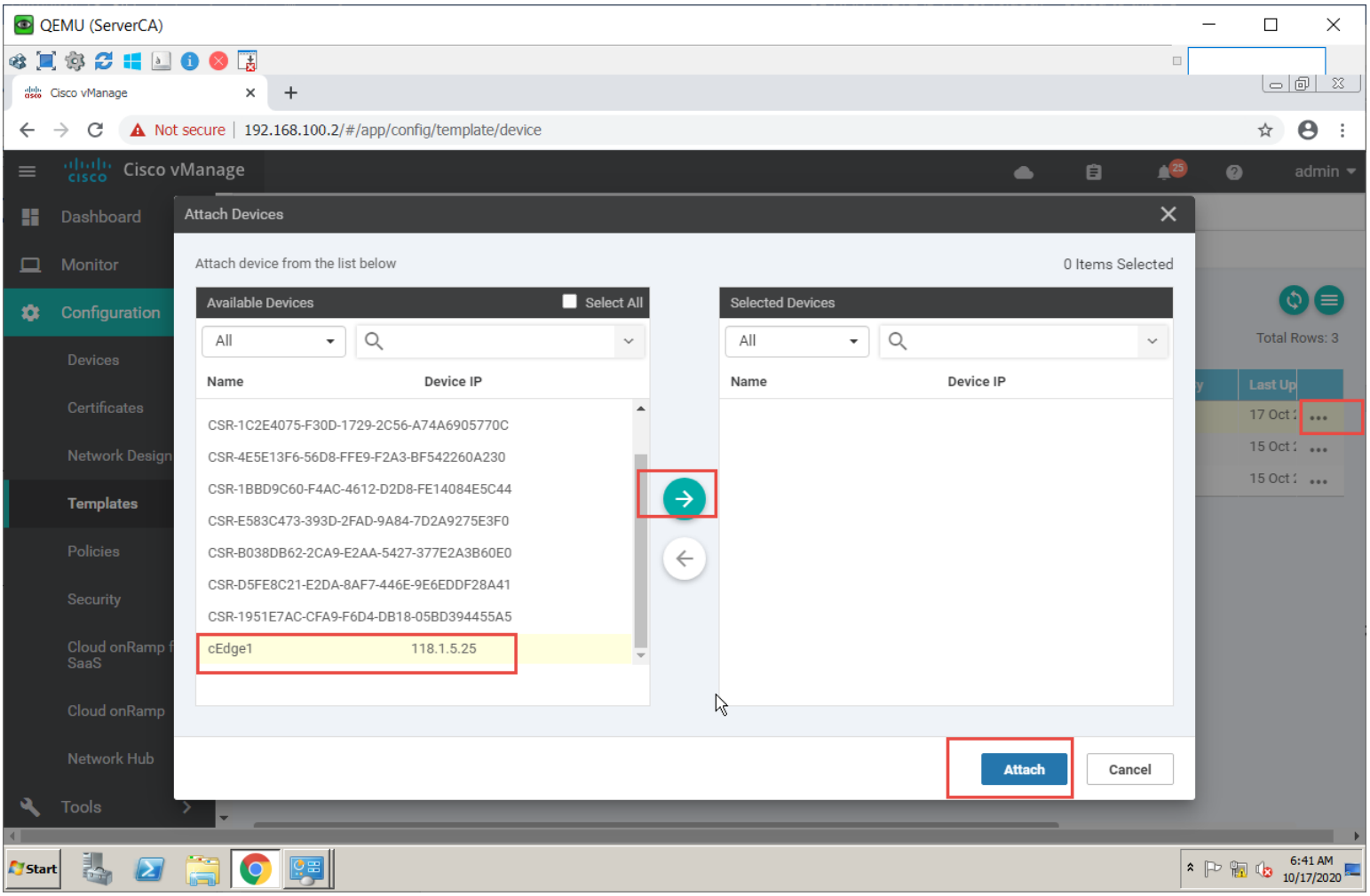

QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/device/feature
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Basic Information
Transport & Management VPN
Service VPN
Additional Templates
Transport & Management VPN
VPN 0 *
BR-CSR-VPN-VPN0
OSPF
BR-CSR-OSPF-VPN0
VPN Interface
BR-CSR-VPNINT-VPN0-G1
VPN Interface
BR-CSR-VPNINT-VPN0-G3
Additional VPN 0 Templates
BGP
OSPF
VPN Interface
VPN 512 *
BR-CSR-VPN-VPN512
Additional VPN 512 Templates
VPN Interface
Create
Cancel
Start
6:38 AM
10/17/2020


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/device/feature
Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Network Design
Templates
Policies
Security
Cloud onRamp for SaaS
Cloud onRamp
Network Hub
Tools
CONFIGURATION | TEMPLATES
Basic Information
Transport & Management VPN
Service VPN
Additional Templates
Service VPN
Service VPN
VPN
BR-CSR-VPN-VPN1
OSPF
BR-CSR-OSPF-VPN1
VPN Interface
BR-CSR-VPNINT-VPN1-G2
Sub-Templates
Additional VPN Templates
BGP
OSPF
VPN Interface
VPN Interface IPsec
Additional Templates
Create
Cancel
Start
6:39 AM
10/17/2020



Task 2 – Attach cEdge1 to the Device Template

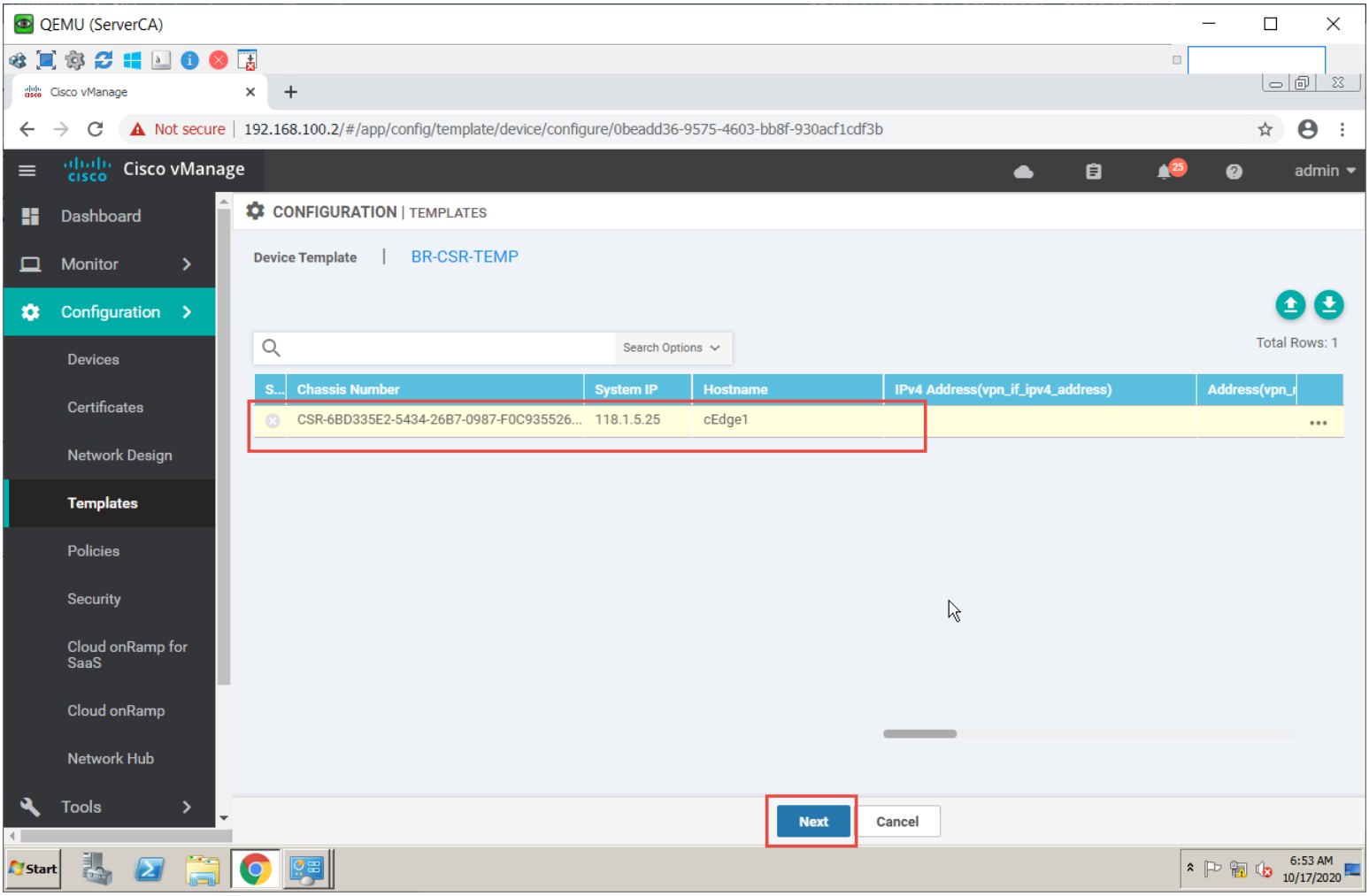
- In vManage, Navigate to Configuration ➔ Templates ➔ Device ➔ BRCSR-TEMP.
- Click on "…" towards the right-hand side.
- Click Attach Devices.
- Select cEdge1 and click the "➔" button.
- Click Attach.

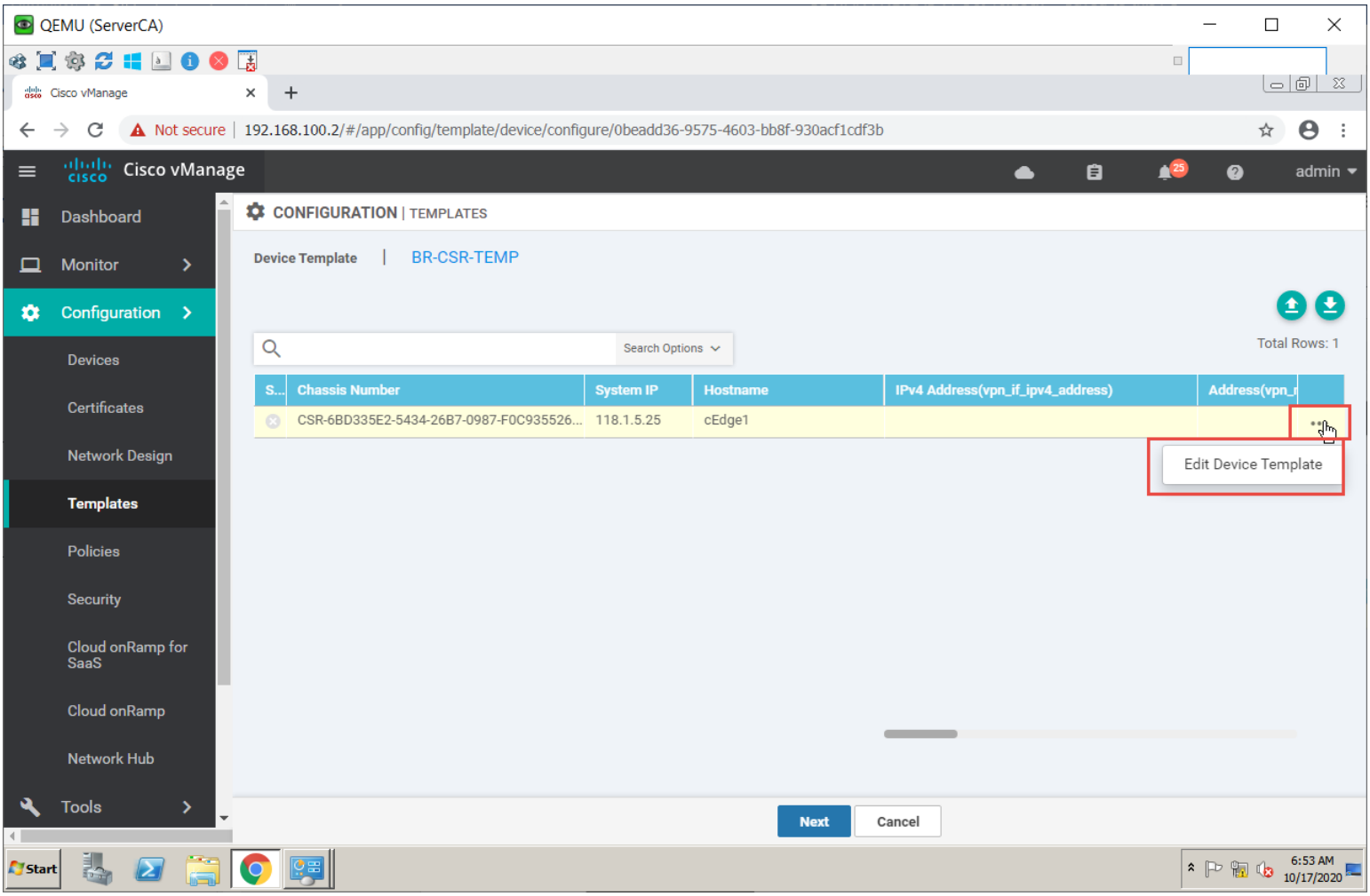


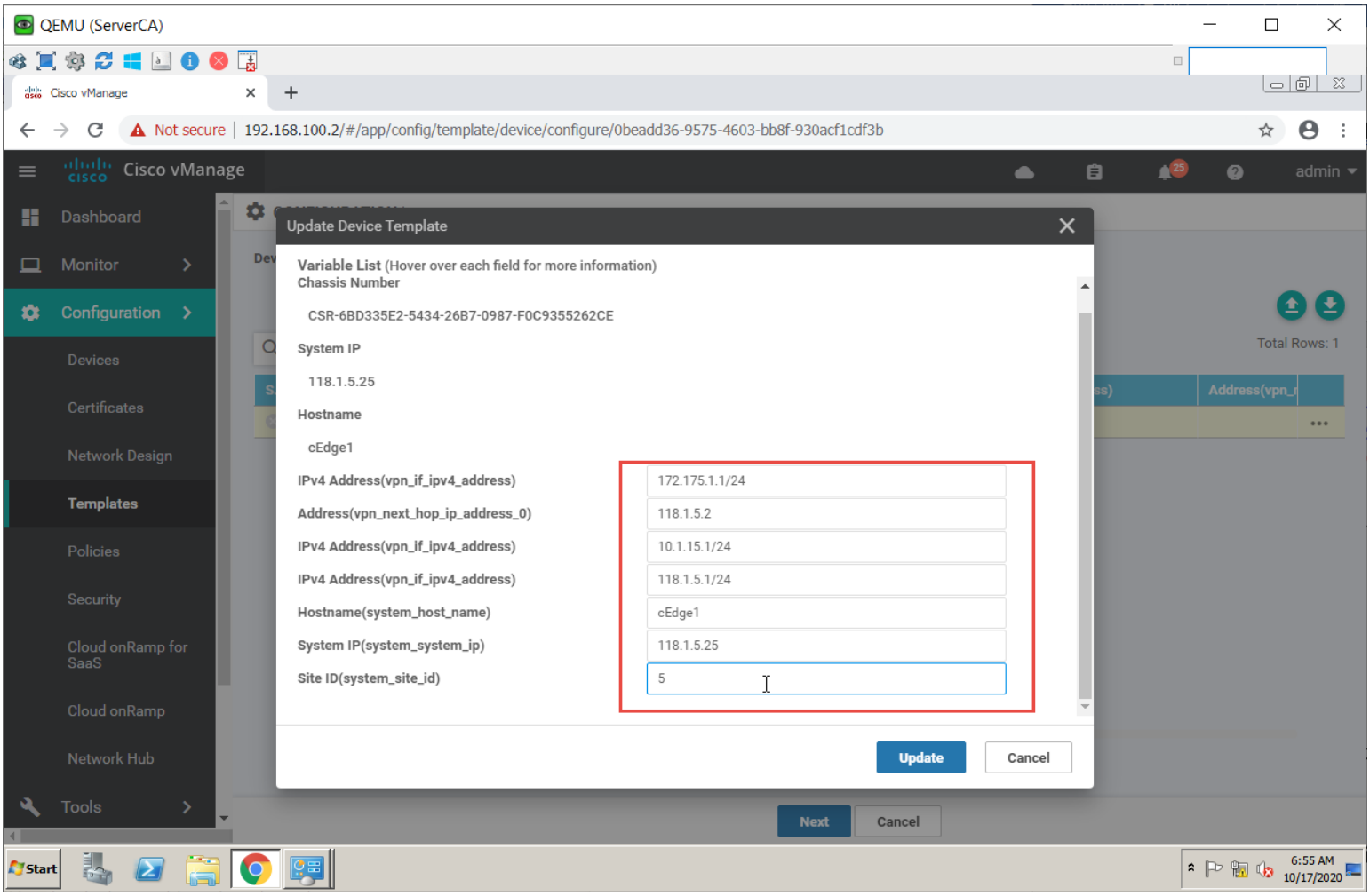
Task 3 – Configure the Variable Parameters for the Feature Templates

- cEdge1 will appear in the window.
- Click on "…" towards the right-hand side.
- Click Edit Device Template.
- Configure the variables based on the following:
    - Interface IP for GigabitEthernet3: 10.1.15.1/24
    - Default Gateway for VPN0: 118.1.5.2
    - Interface IP for GigabitEthernet2: 172.175.1.1/24
    - Interface IP for GigabitEthernet1: 118.1.5.1/24
    - Hostname: cEdge-1
    - System IP: 118.1.5.25
    - 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.




QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/device/configure/0beadd36-9575-4603-bb8f-930acf1cdf3b
Cisco vManage
admin
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_
CSR-6BD335E2-5434-26B7-0987-F0C935526...
118.1.5.25
cEdge1
Edit Device Template
Next
Cancel
Start
6:53 AM
10/17/2020


QEMU (ServerCA)
Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/device/configure/0beadd36-9575-4603-bb8f-930acf1cdf3b
Cisco vManage
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)
172.175.1.1/24
Address(vpn_next_hop_ip_address_0)
118.1.5.2
IPv4 Address(vpn_if_ipv4_address)
10.1.15.1/24
IPv4 Address(vpn_if_ipv4_address)
118.1.5.1/24
Hostname(system_host_name)
cEdge1
System IP(system_system_ip)
118.1.5.25
Site ID(system_site_id)
5
Update
Cancel
Total Rows: 1
Address(vpn_
Next
Cancel
Start
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 - 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
       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#
```

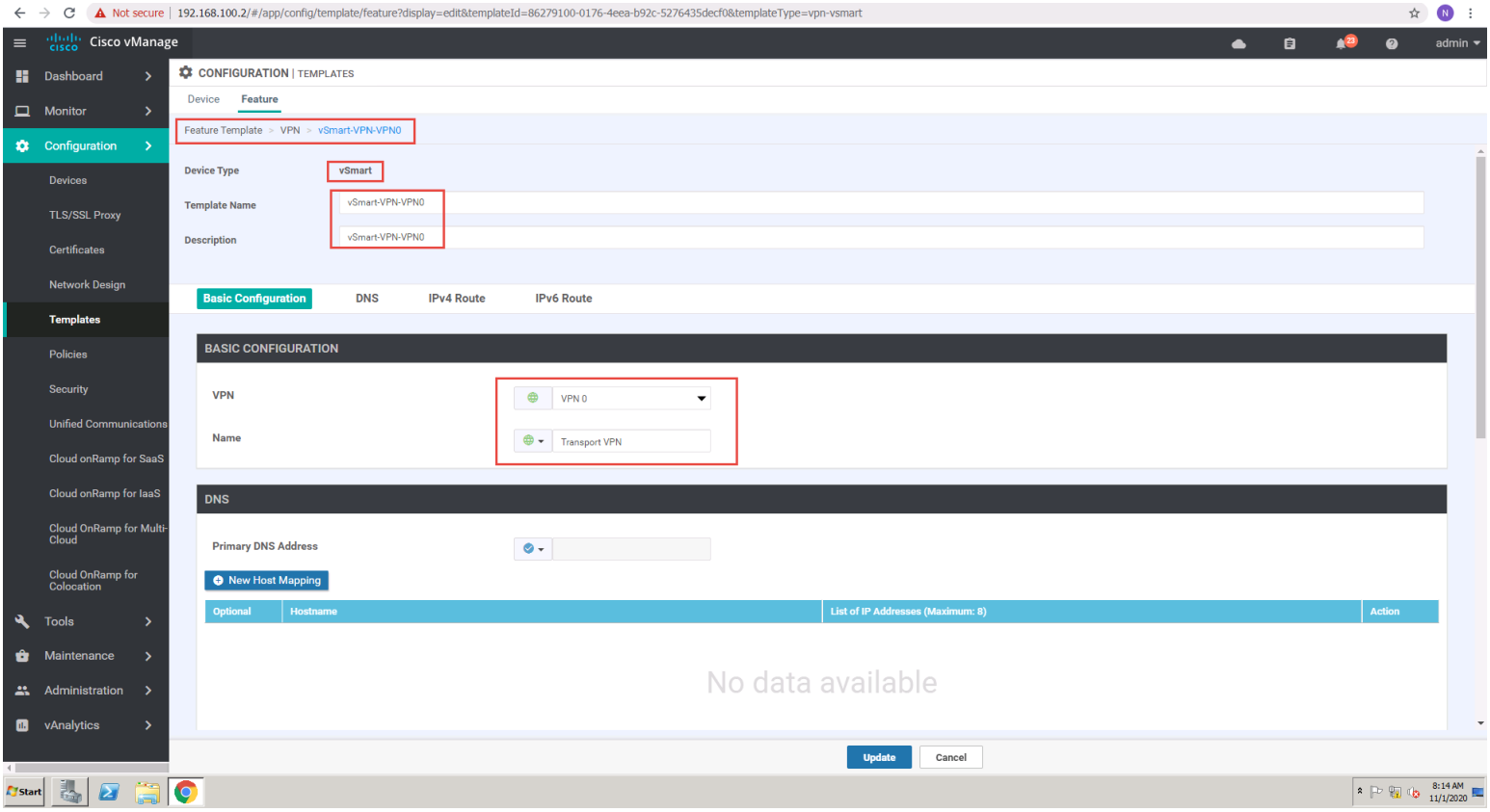
Lab 26 - Configuring and Deploying Feature and Device Templates for vSmart Controllers

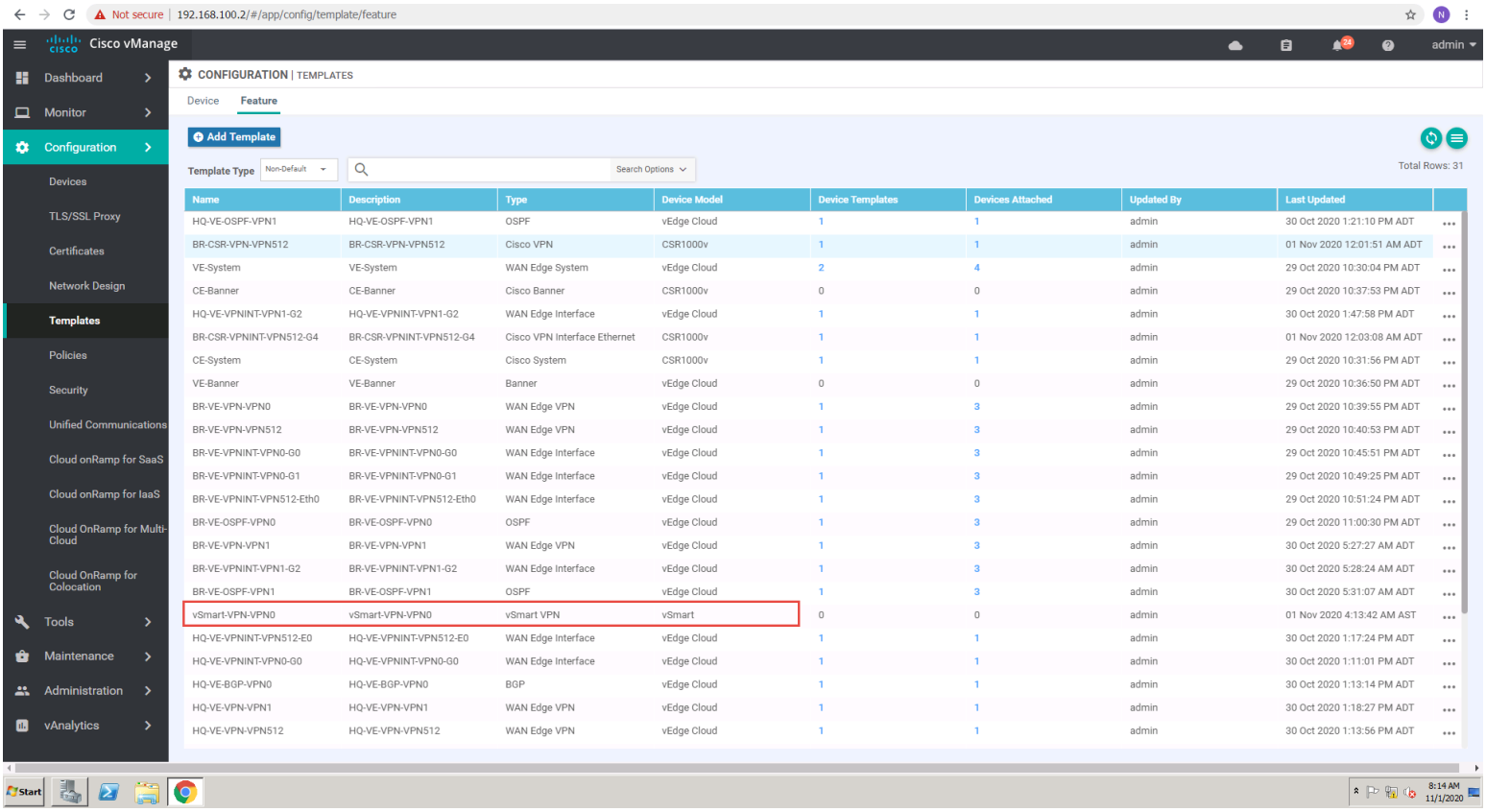
Task 1 – Configure a VPN Template to be used by vSmart Controllers for VPN 0

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

  Basic Configuration
    - VPN ➔ Global: 0
    - Name ➔ Global : Transport VPN

  IPv4 Route
    - Prefix ➔ Global: 0.0.0.0/0
    - Next Hop ➔ Global: 100.1.1.1
- Click Save to save the Template.

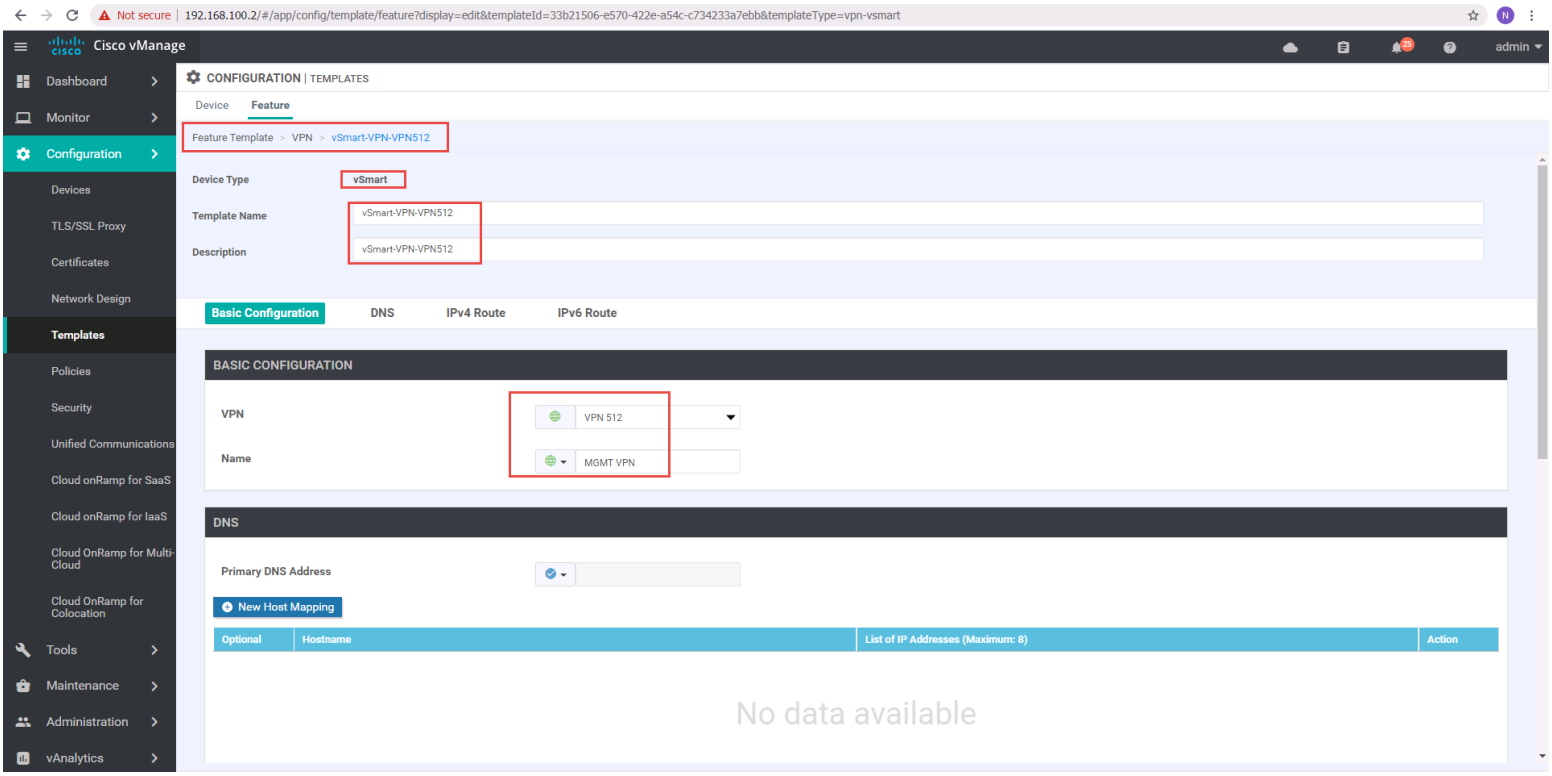


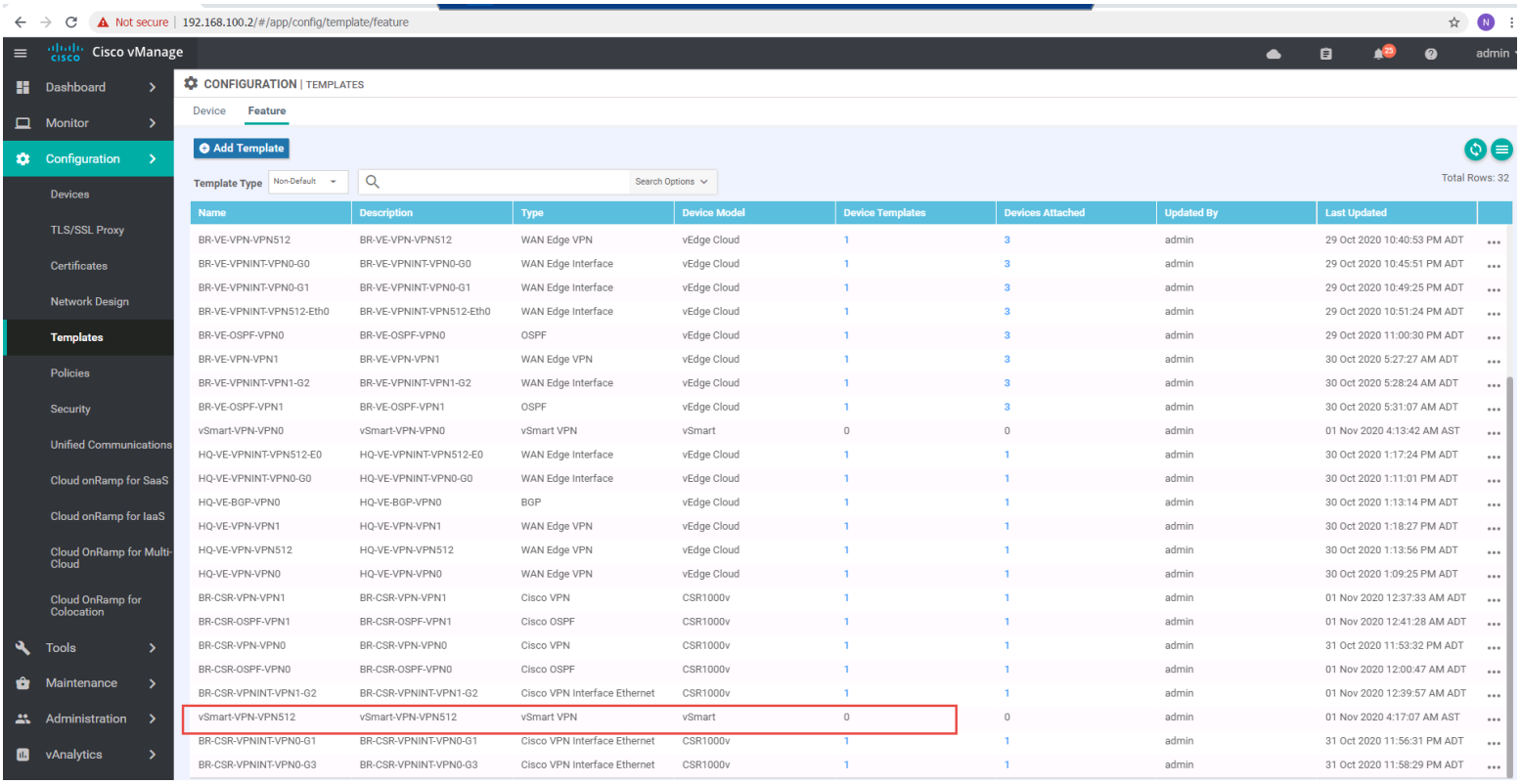


Task 2 – Configure a VPN Template to be used by vSmart Controllers for VPN 512

- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ vSmart ➔ VPN ➔ VPN
- Configure the VPN parameters based on the following:
    - Template Name: vSmart -VPN-VPN512
    - Description: vSmart -VPN-VPN512

  Basic Configuration
    - VPN ➔ Global : 512
    - Name ➔ Global : MGMT VPN
- Click Save to save the Template.





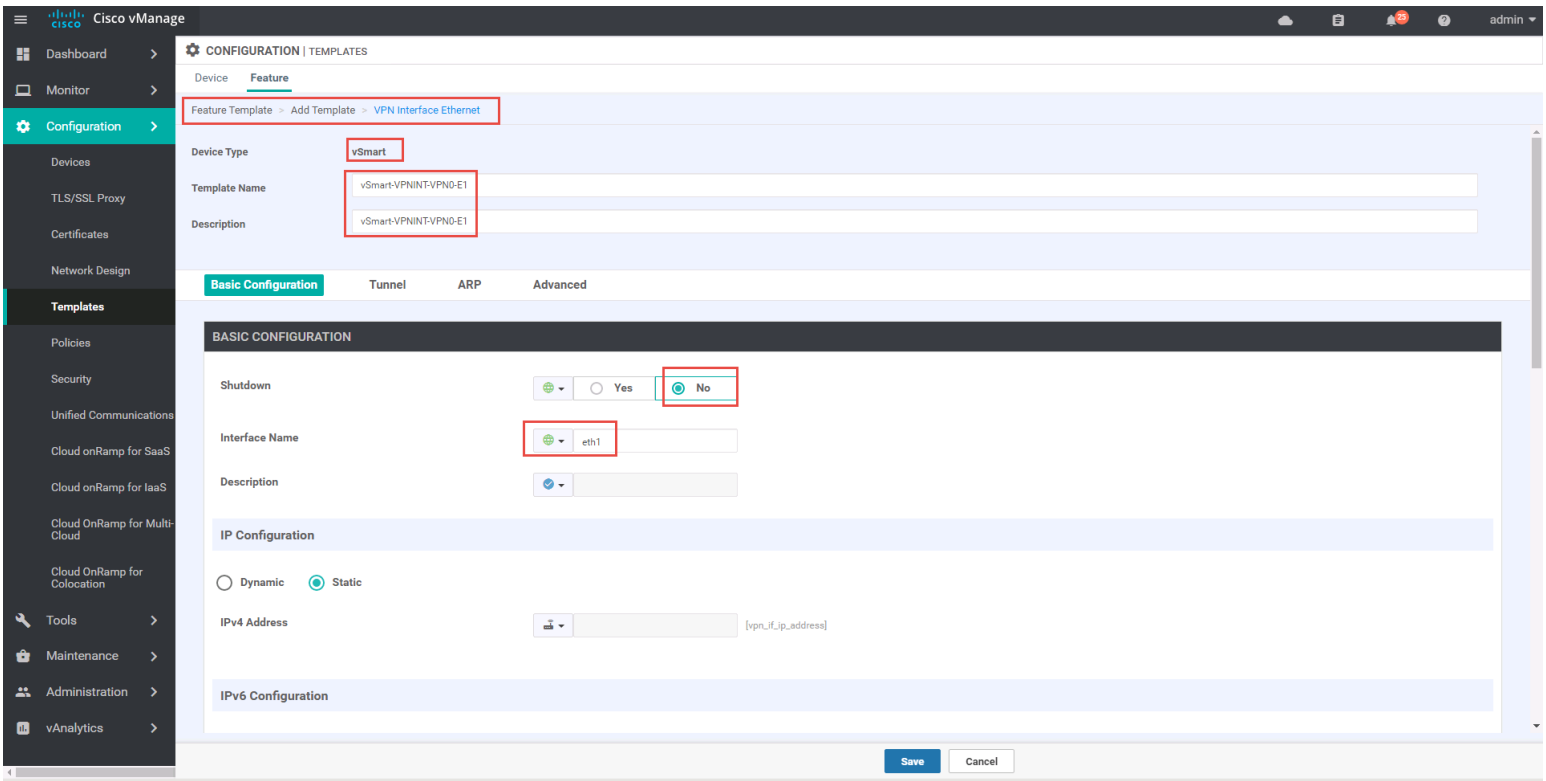
Task 3 – Configure a VPN Interface Template to be used by vSmart Controllers for VPN 0 for Interface Eth1

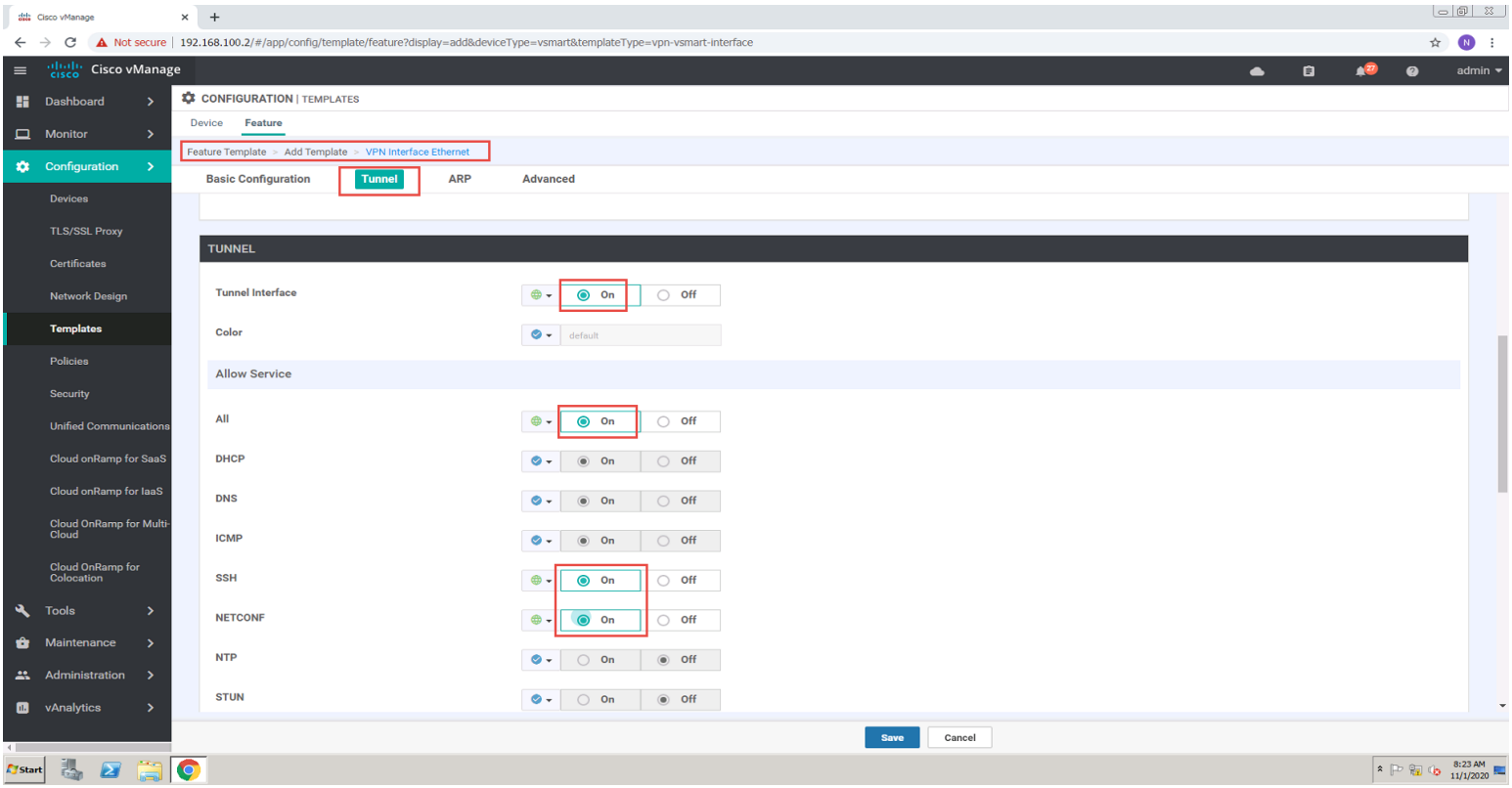
- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ vSmart ➔ VPN ➔ VPN Interface Ethernet
- Configure the VPN parameters based on the following:
    - Template Name: vSmart-VPNINT-VPN0-E1
    - Description: vSmart-VPNINT-VPN0-E1

  Basic Configuration
    - Shutdown ➔ Global : No
    - Interface Name ➔ Global : eth1
    - 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.

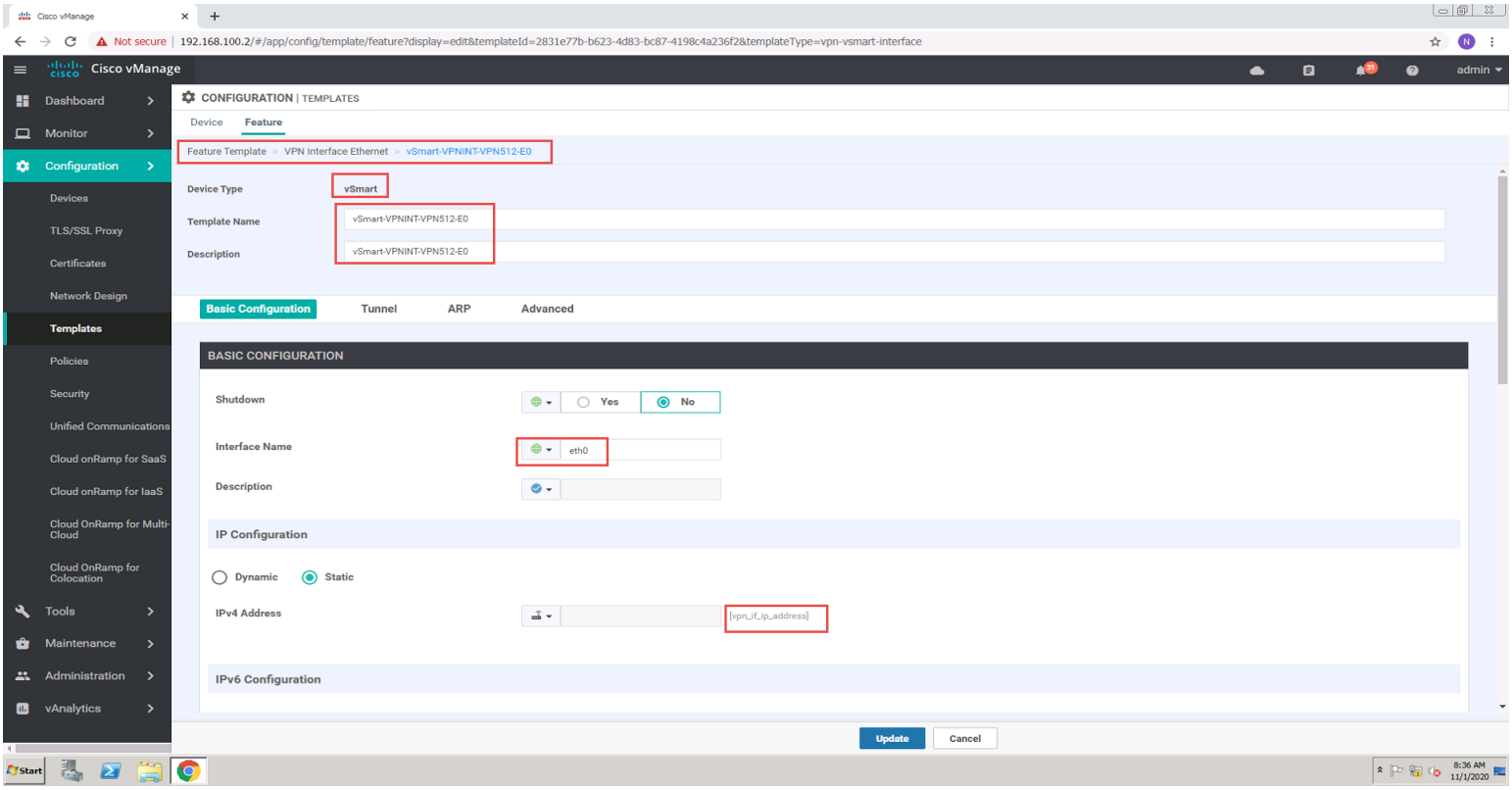


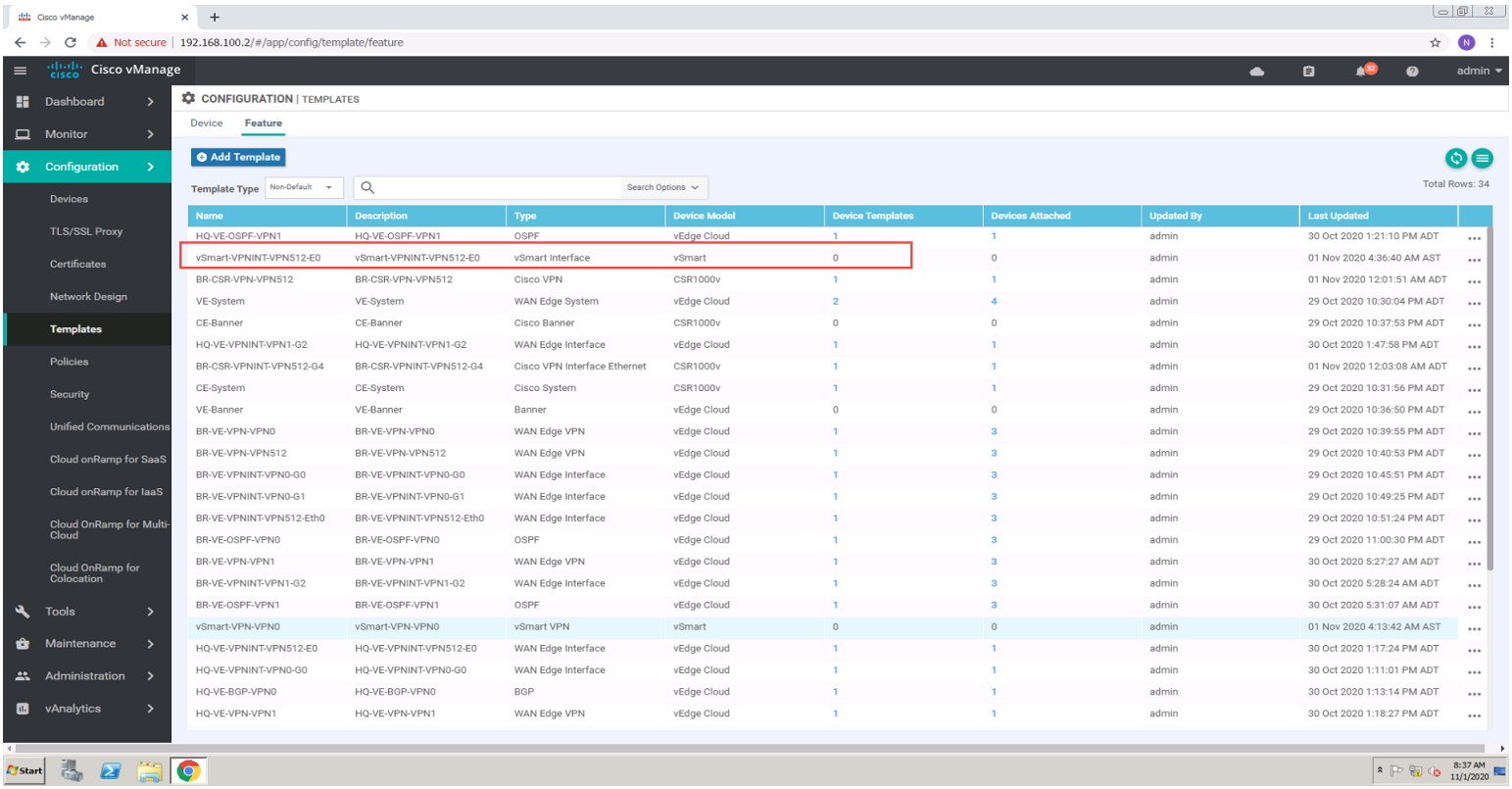


Task 4 – Configure a VPN Interface Template to be used vSmart Controllers for VPN 512 for Interface Eth0

- In vManage, Navigate to Configuration ➔ Templates ➔ Feature ➔ vSmart ➔ VPN ➔ VPN Interface Ethernet
- Configure the VPN parameters based on the following:
    - Template Name: vSmart-VPNINT-VPN512-E0
    - Description: vSmart-VPNINT-VPN512-E0

  Basic Configuration
    - Shutdown ➔ Global: No
    - Interface Name ➔ Global: eth0
    - IPv4 Address ➔ Static ➔ Device-Specific
- Click Save to save the Template



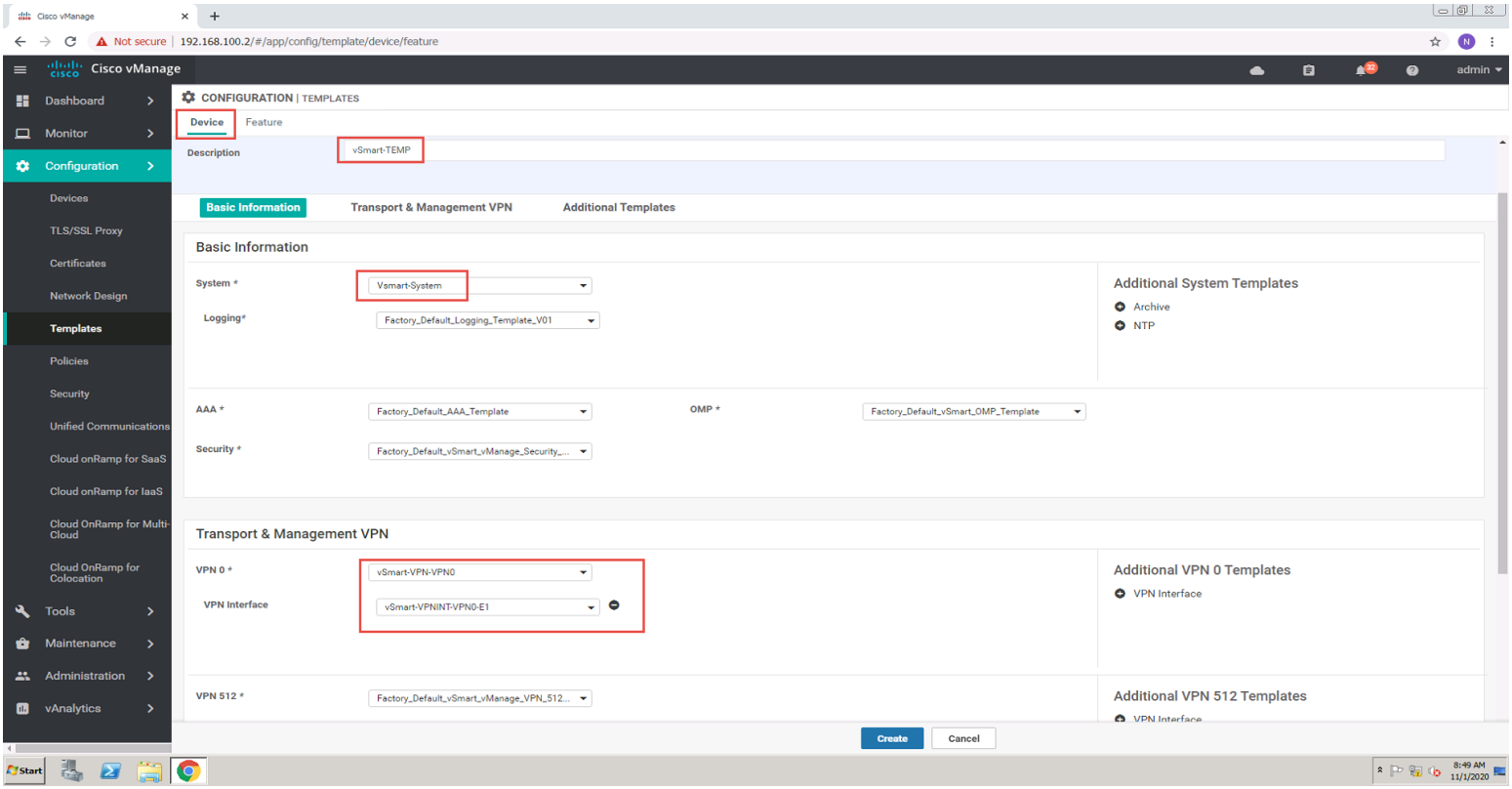


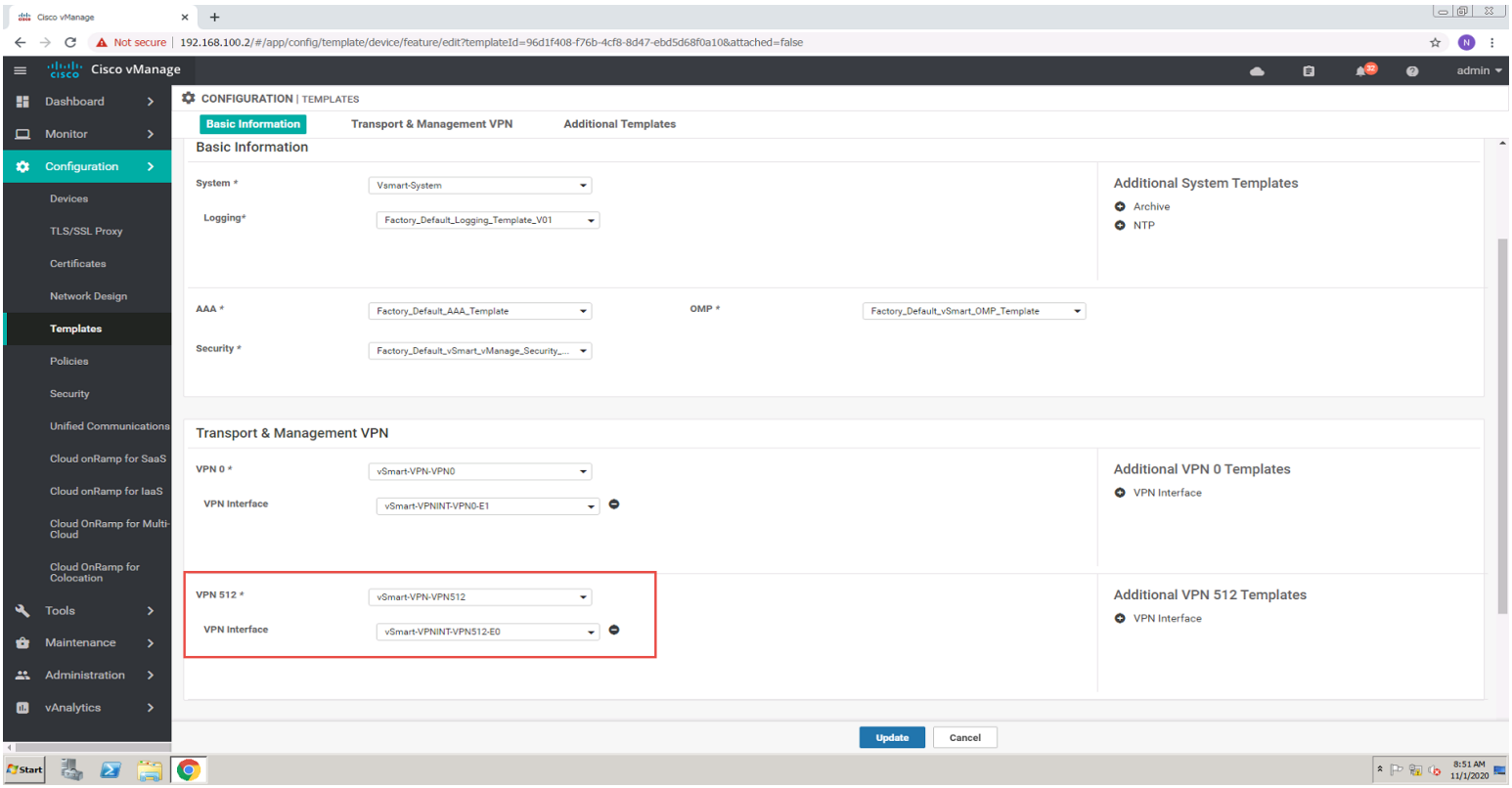
Task 5 – Configure a Device Template for vSmart Controllers.

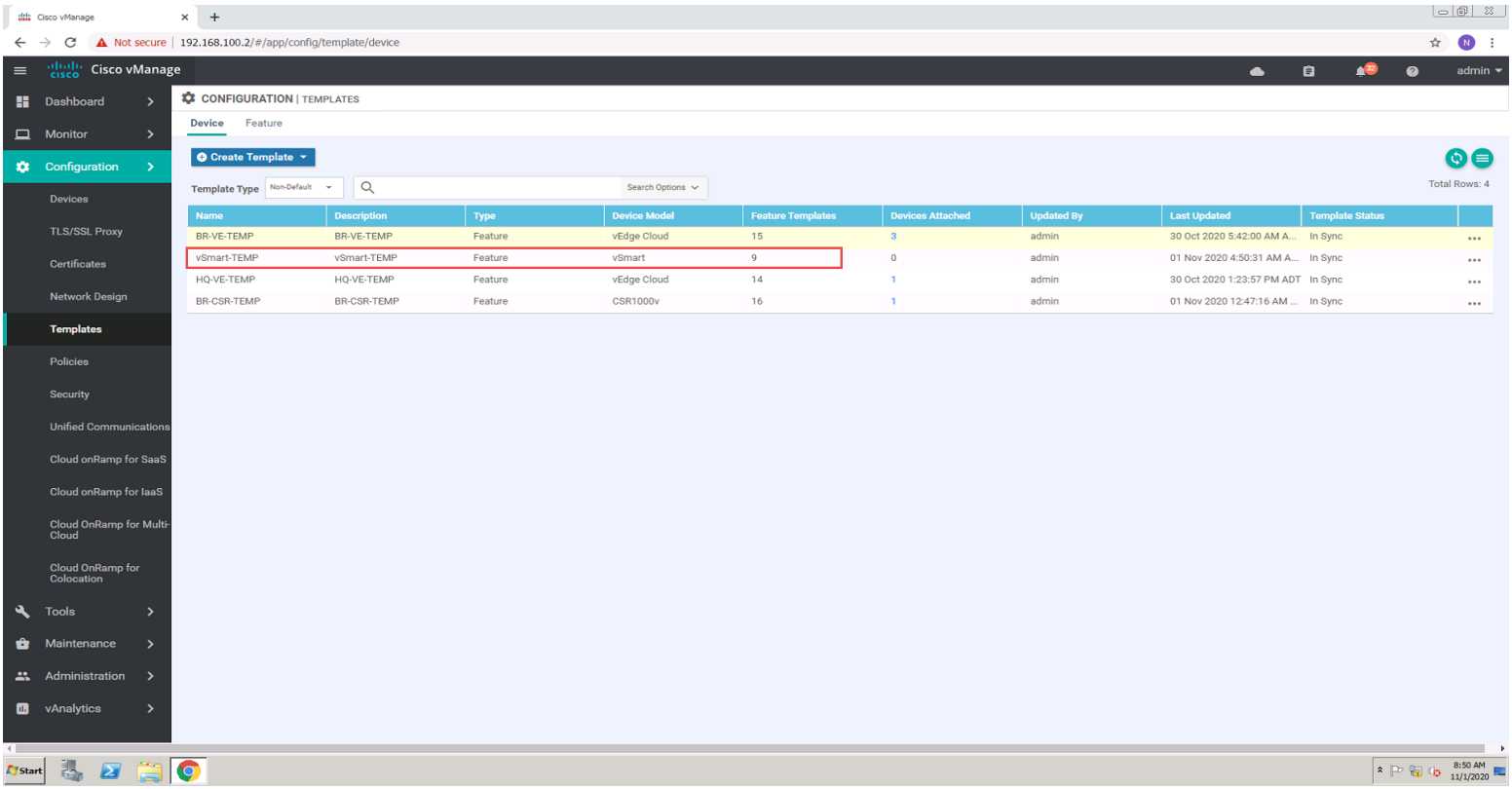
- In vManage, Navigate to Configuration ➔ Templates ➔ Device ➔ Create Template ➔ vSmart
- Configure the Device Template based on the following:
    - Template Name: vSmart-TEMP
    - Description: vSmart-TEMP

  Basic Information
    - System ➔ Vsmart-System

  Transport & Management
    - VPN 0: vSmart-VPN-VPN0
    - VPN Interface: vSmart-VPNINT-VPN0-E1
    - VPN 512: vSmart-VPN-VPN512
    - VPN Interface: vSmart-VPNINT-VPN512-E0
- Click Save to save the Template.

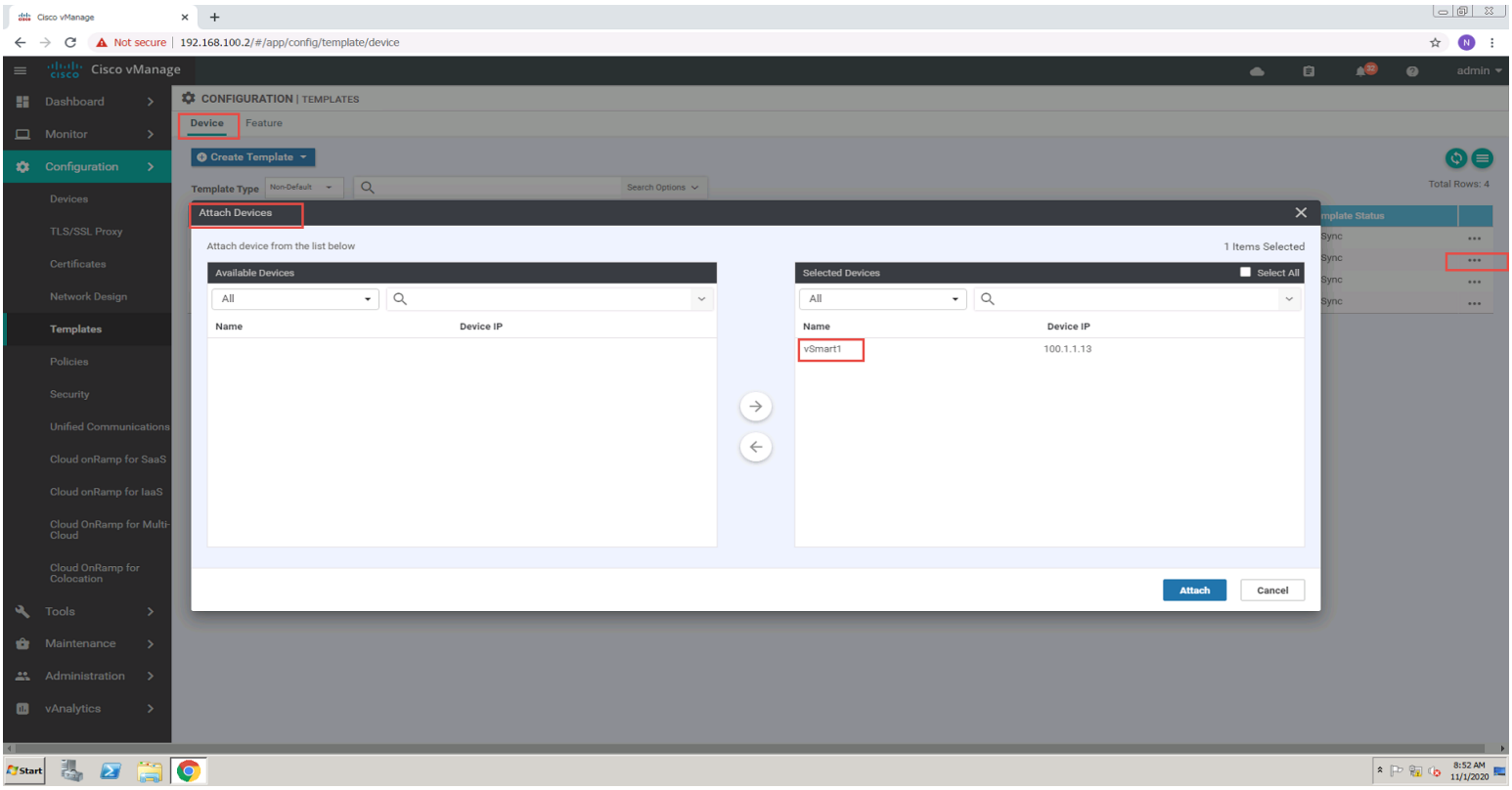



Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/device/feature/edit?templateId=96d1f408-f76b-4cf8-8d47-ebd5d68f0a10&attached=false
CONFIGURATION | TEMPLATES
Basic Information
Transport & Management VPN
Additional Templates
Basic Information
System *
Vsmart-System
Logging*
Factory_Default_Logging_Template_V01
AAA *
Factory_Default_AAA_Template
OMP *
Factory_Default_vSmart_OMP_Template
Security *
Factory_Default_vSmart_vManage_Security_...
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 *
vSmart-VPN-VPN512
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
CONFIGURATION | TEMPLATES
Device
Feature
Create Template
Template Type
Non-Default
Search Options
Total Rows: 4
Name | Description | Type | Device Model | Feature Templates | Devices Attached | Updated By | Last Updated | Template Status
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

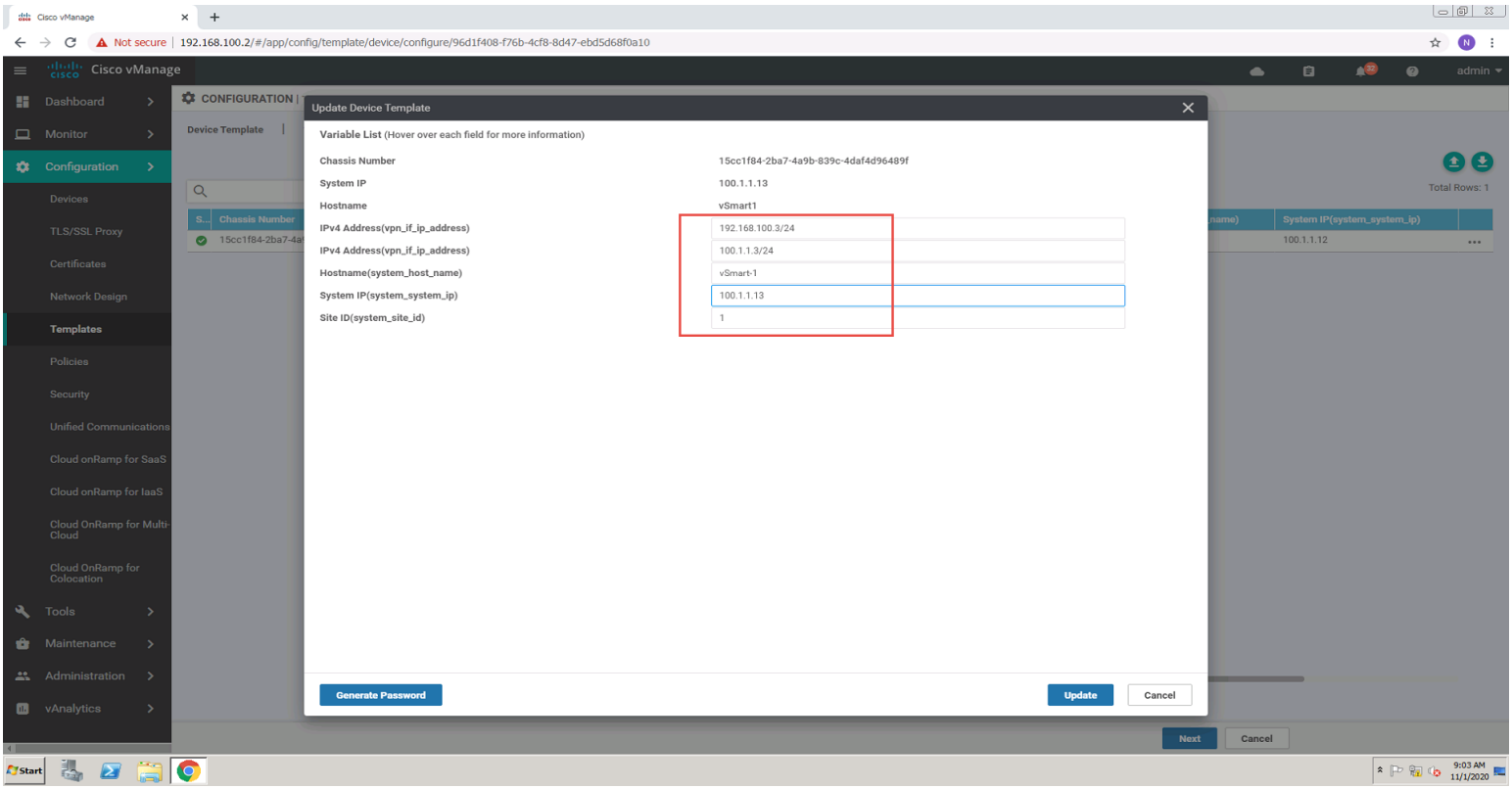
Task 6 – Attach vSmart to the Device Template

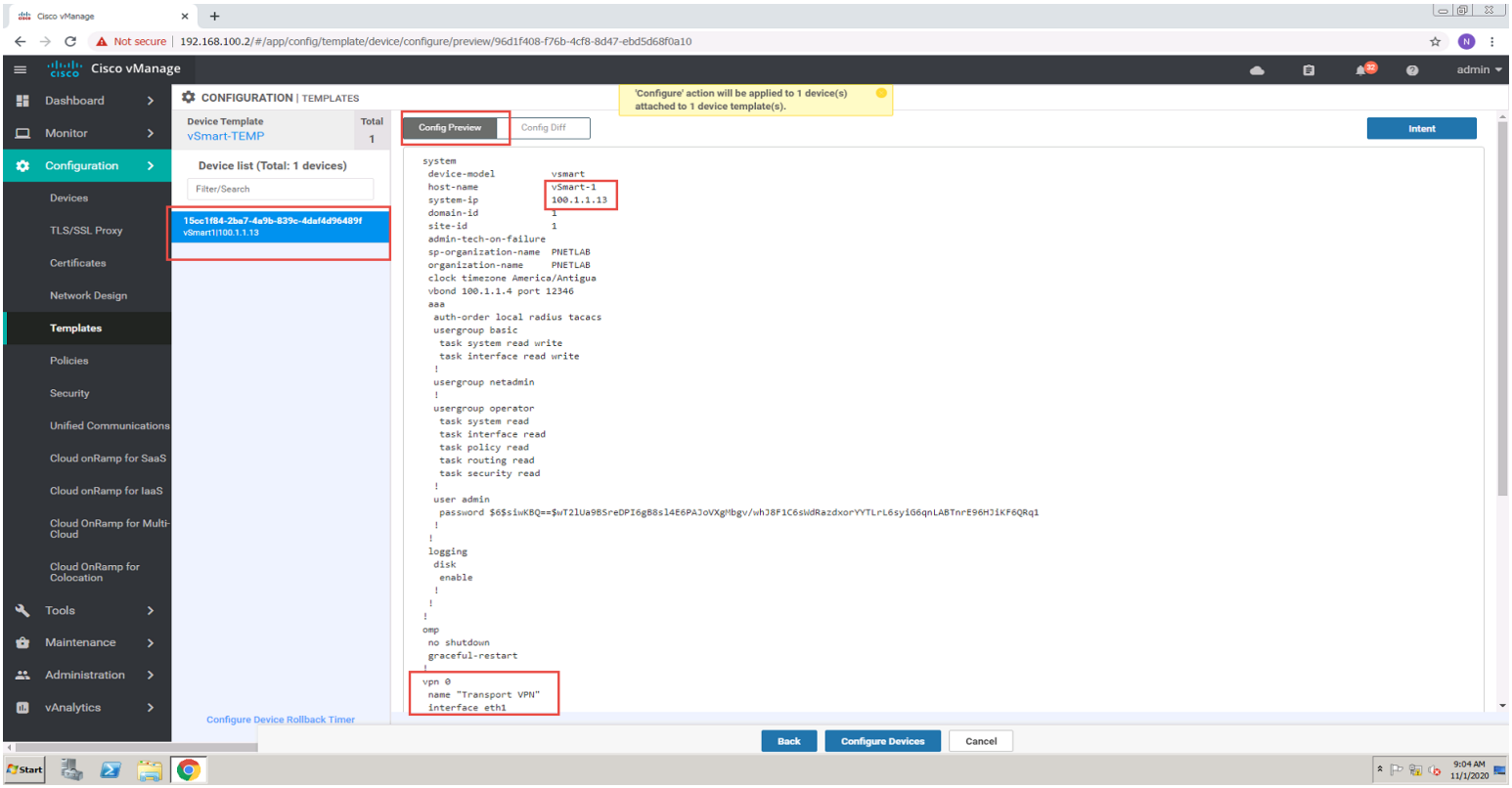
- In vManage, Navigate to Configuration ➔ Templates ➔ Device ➔ vSmart-TEMP
- Click on "…" towards the right-hand side.
- Click Attach Devices.
- Select vSmart and click the "➔" button.
- Click Attach.

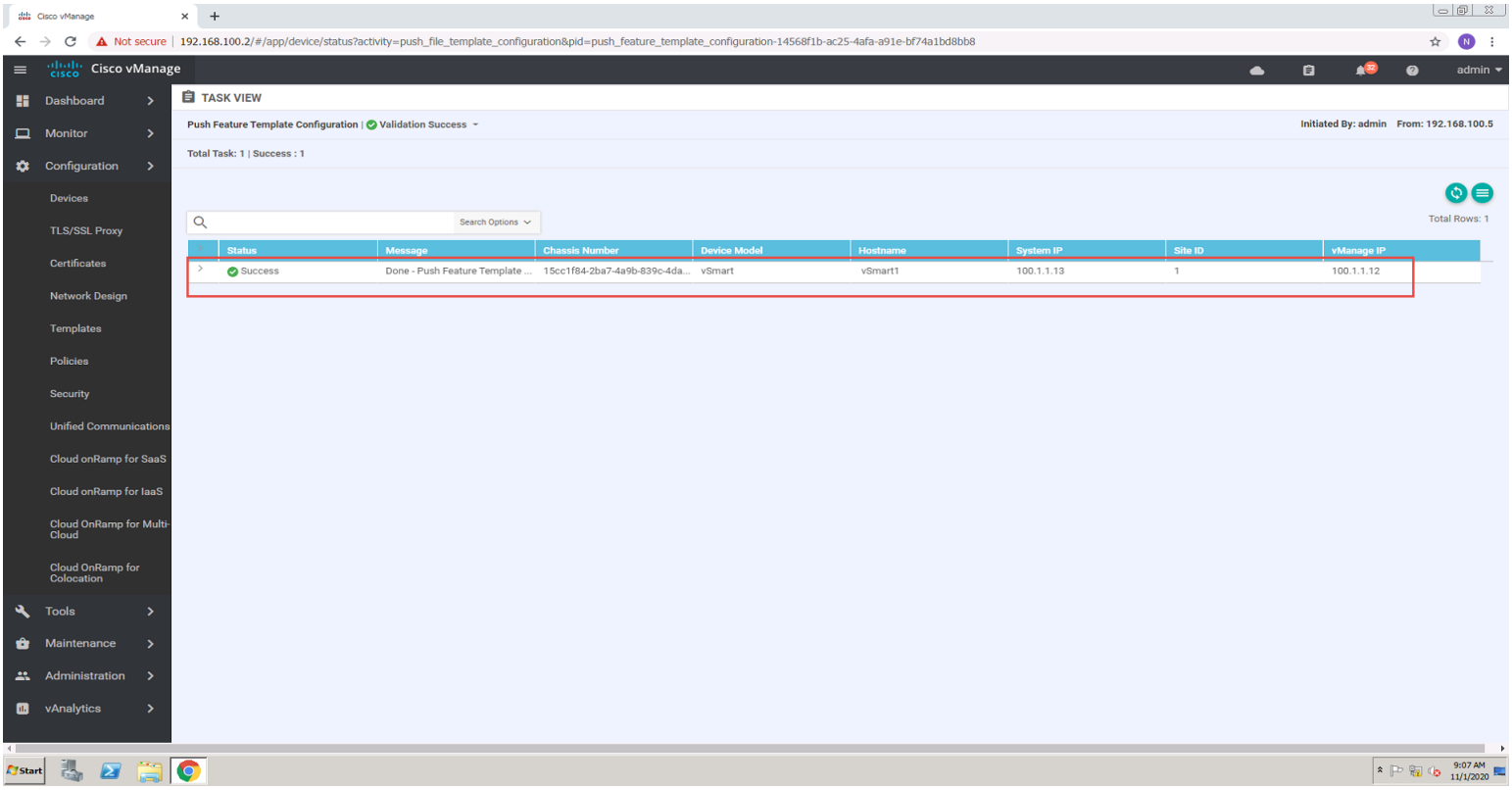


Task 7 – Configure the Variable Parameters for the Feature Templates

- 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
CONFIGURATION
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)
100.1.1.3/24
Hostname(system_host_name)
vSmart-1
System IP(system_system_ip)
100.1.1.13
Site ID(system_site_id)
1
Generate Password
Update
Cancel
Next
Cancel


Cisco vManage
Not secure | 192.168.100.2/#/app/config/template/device/configure/preview/96d1f408-f76b-4cf8-8d47-ebd5d68f0a10
CONFIGURATION | TEMPLATES
'Configure' action will be applied to 1 device(s) attached to 1 device template(s).
Device Template
vSmart-TEMP
Total 1
Device list (Total: 1 devices)
Filter/Search
15cc1f84-2ba7-4a9b-839c-4daf4d96489f
vSmart1|100.1.1.13
Config Preview
Config Diff
Intent
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 6siwKBQ==$wT2lUa9BSreDPI6gB8sl4E6PAJoVXgMbgv/whJ8F1C6sWdRazdxorYYTLrL6syiG6qnLABTnrE96HJlKF6QRq1
!
!
logging
disk
enable
!
!
!
omp
no shutdown
graceful-restart
!
vpn 0
name "Transport VPN"
interface eth1
Configure Device Rollback Timer
Back
Configure Devices
Cancel


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
Cisco vManage
admin
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
TASK VIEW
Push Feature Template Configuration | Validation Success
Initiated By: admin From: 192.168.100.5
Total Task: 1 | Success : 1
Search Options
Total Rows: 1
Status
Message
Chassis Number
Device Model
Hostname
System IP
Site ID
vManage IP
Success
Done - Push Feature Template ...
15cc1f84-2ba7-4a9b-839c-4da...
vSmart
vSmart1
100.1.1.13
1
100.1.1.12
Start
9:07 AM
11/1/2020

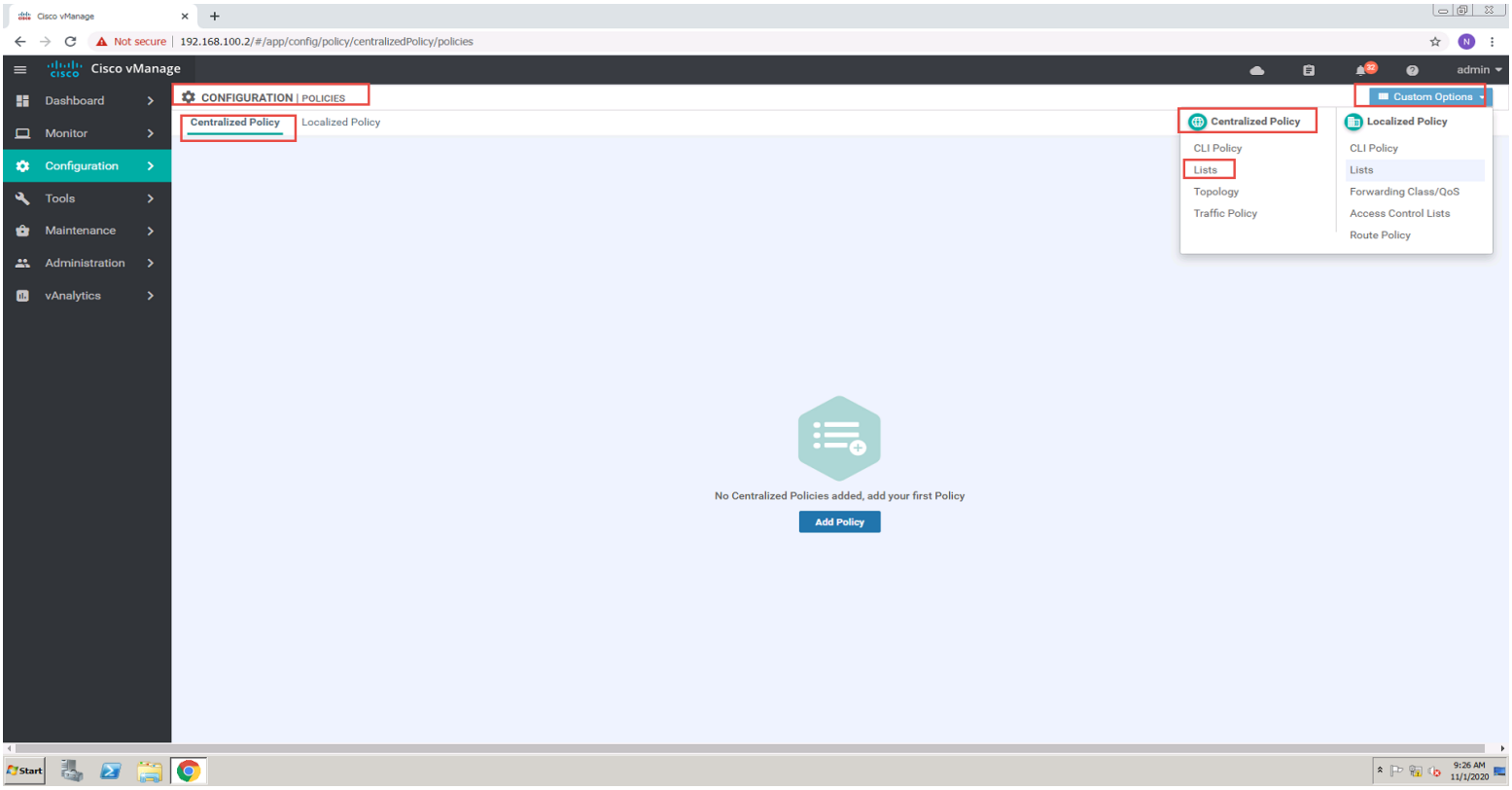
Lab 27 - Configuring Application Aware Policies using Telnet and Web

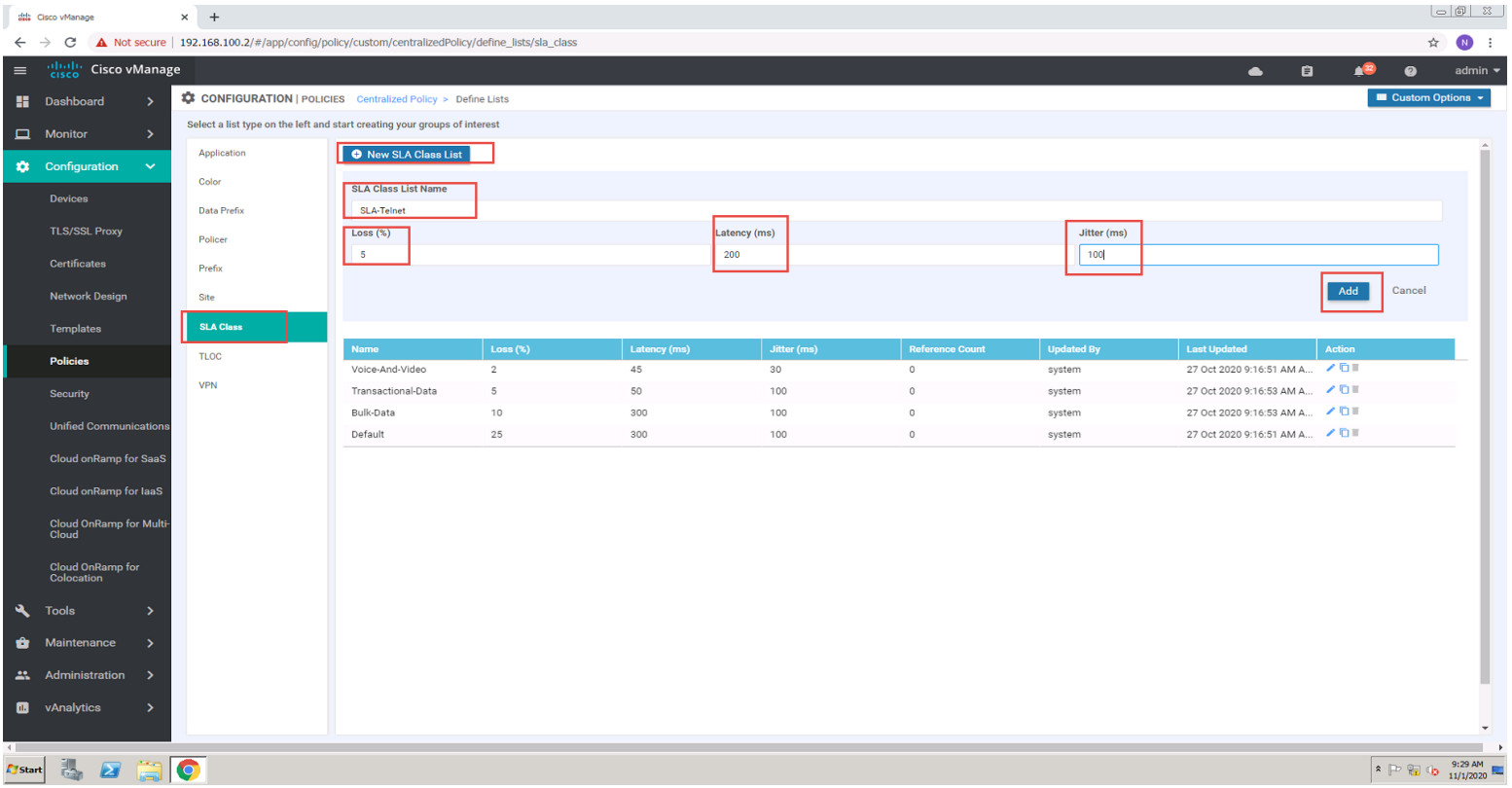
Requirements:

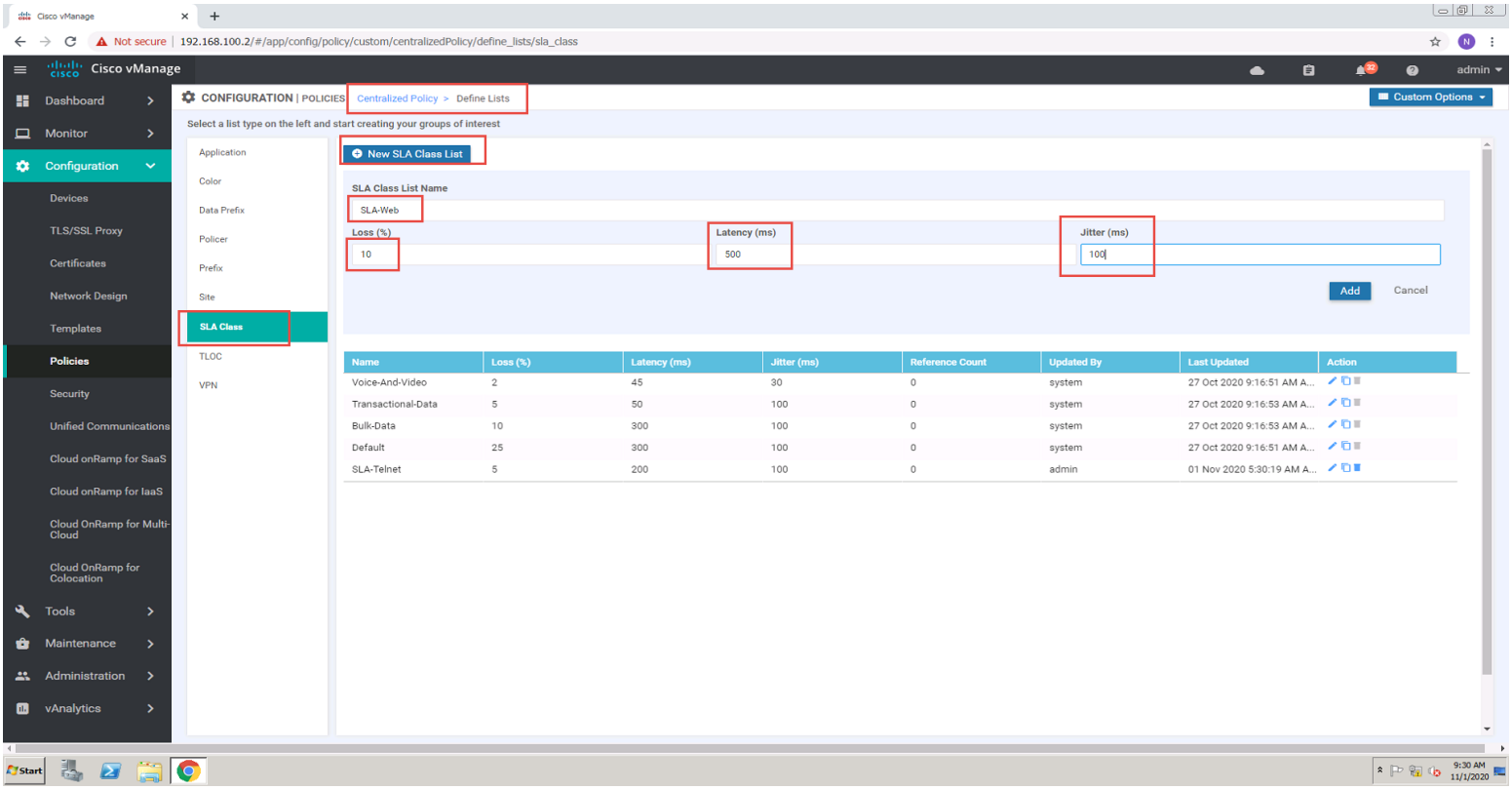
- Dubai (Site-2) & Hongkong (Site-3) Sites should use the MPLS Transport for Telnet
- Traffic and the Biz-Internet Transport for Web Traffic.
- Telnet Should have a SLA based on the following:
    - Loss – 5%
    - Latency – 200
    - Jitter – 100ms
- Web Should have a SLA based on the following:
  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

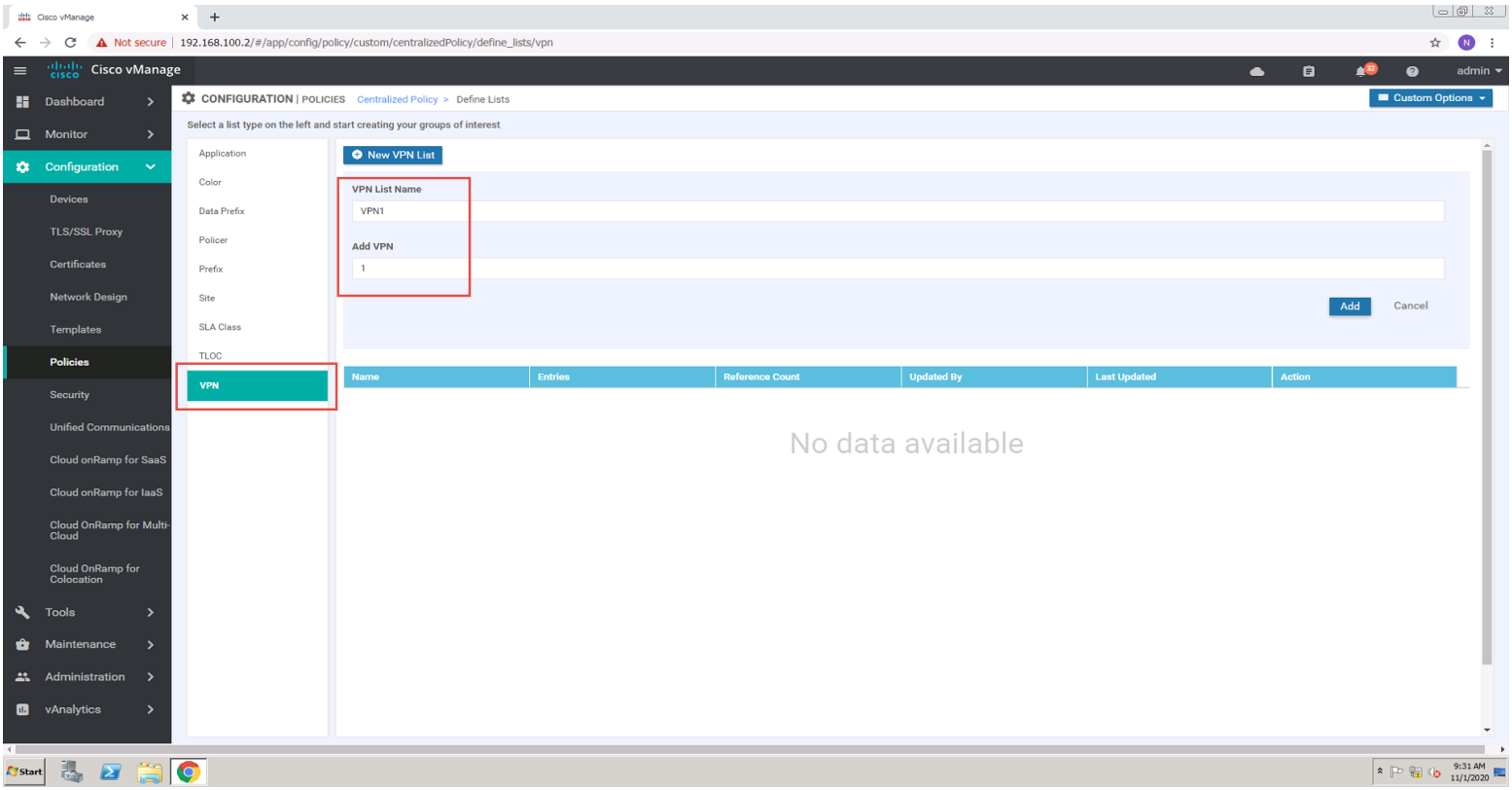
Task 1 – Configure Groups of Interests/List that will be used for Telnet & Web Application Aware Routing (AAR) Policy

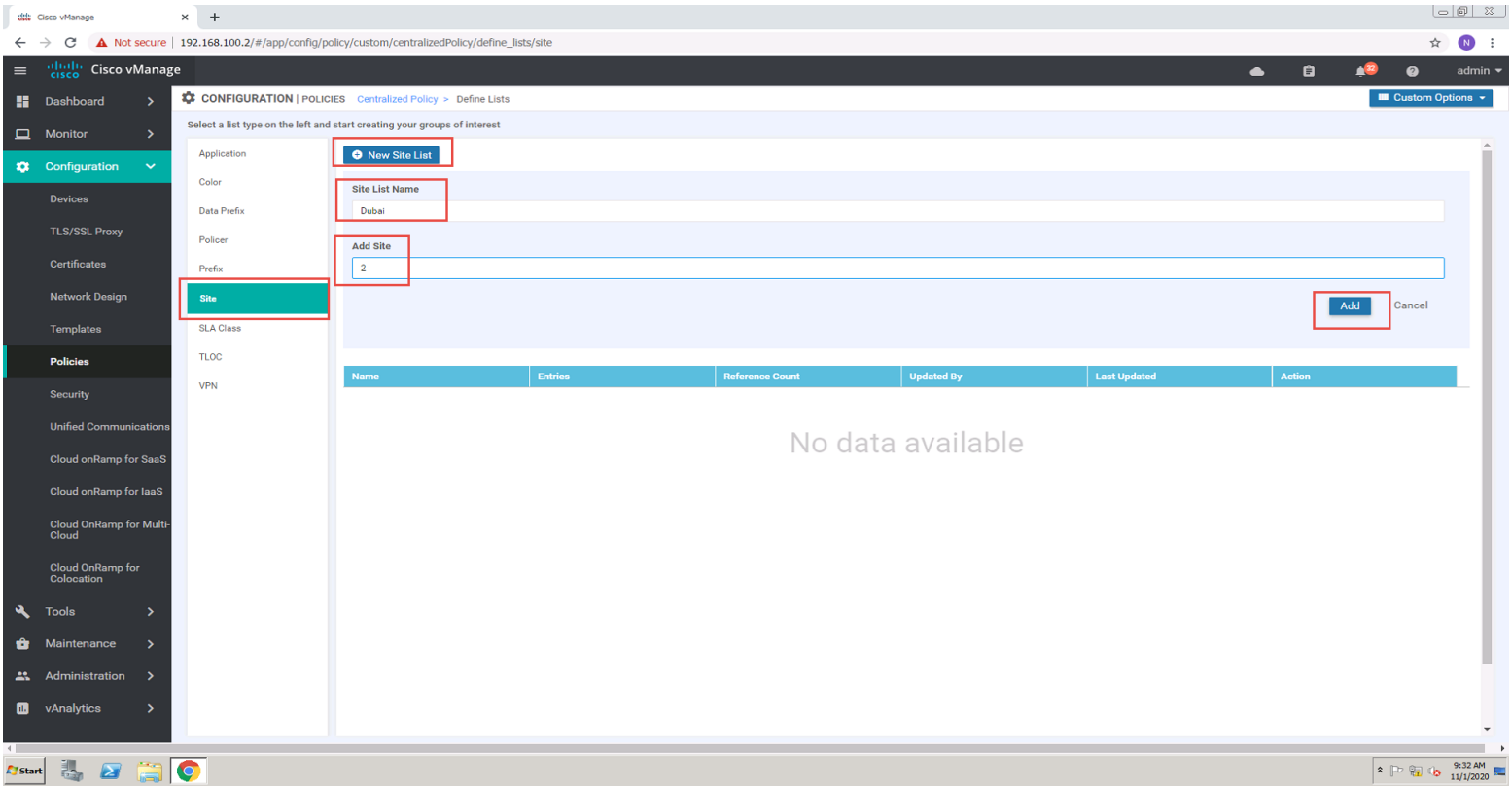
- In vManage, Navigate to Configuration ➔ Policies ➔ Custom Options ➔ Centralized Policy ➔ Lists.
- Click SLA Class and select New SLA Class list. Create 2 policies based on the following:
    - Name: SLA-Telnet
    - Loss: 30% (because in lab, packet lost is high)
    - Latency: 200
    - Jitter: 100ms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






Cisco vManage
Not secure | 192.168.100.2/#/app/config/policy/custom/centralizedPolicy/define_lists/sla_class
CONFIGURATION | POLICIES
Centralized Policy > Define Lists
Custom Options
Select a list type on the left and start creating your groups of interest
Application
Color
Data Prefix
Policer
Prefix
Site
SLA Class
TLOC
VPN
New 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
CONFIGURATION | POLICIES
Centralized Policy > Define Lists
Custom Options
Select a list type on the left and start creating your groups of interest
Application
Color
Data Prefix
Policer
Prefix
Site
SLA Class
TLOC
VPN
New VPN List
VPN List Name
VPN1
Add VPN
1
Add
Cancel
Name
Entries
Reference Count
Updated By
Last Updated
Action
No data available



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:
    - Policy Name: TELNET-WEB-Policy
    - Description: TELNET-WEB-Policy

  Telnet Sequence

  Match Conditions:
    - Protocol: 6
    - Port: 23

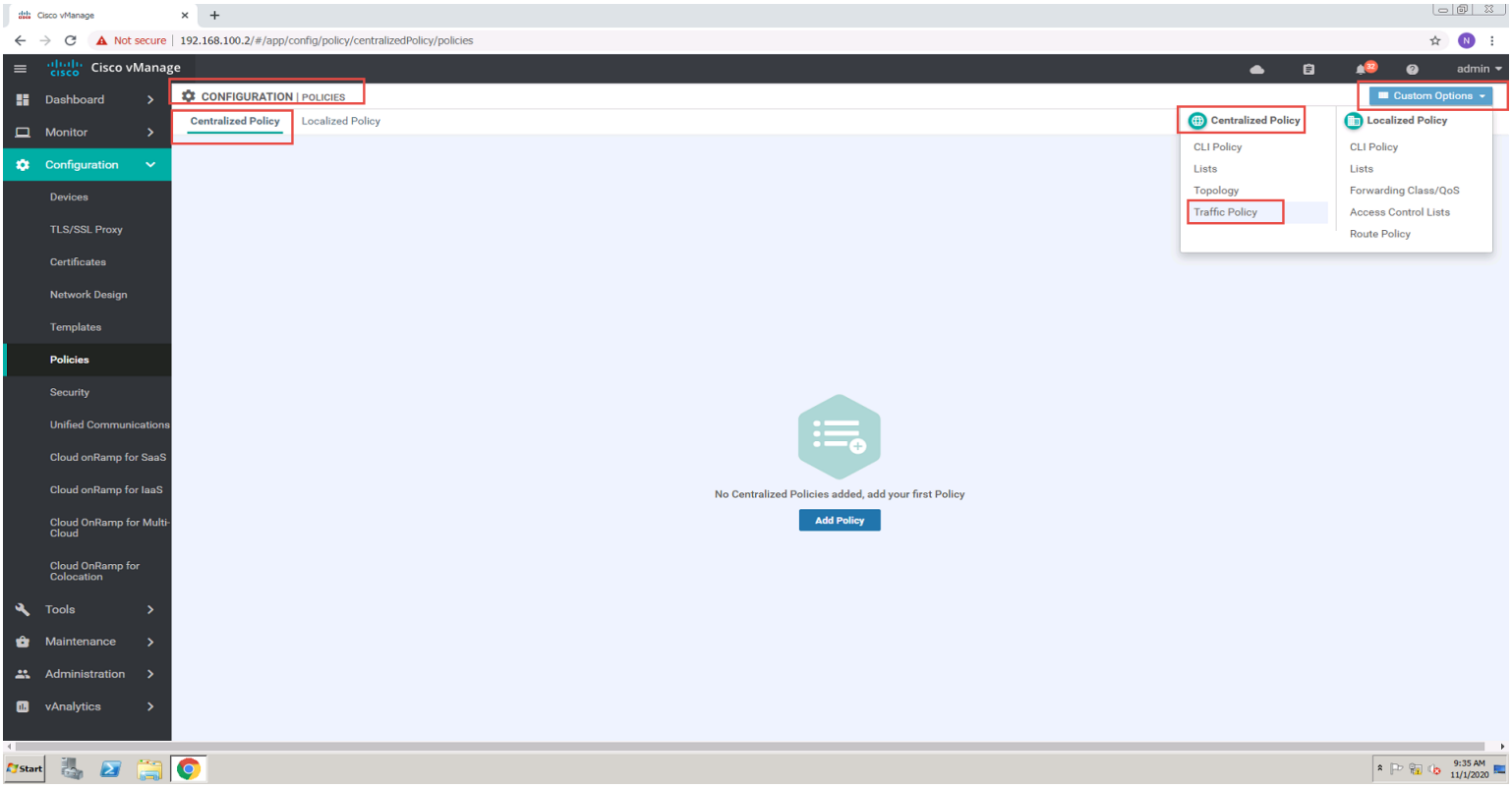
  Action
    - SLA Class List: SLA-Telnet
    - Color: mpls
    - Backup Preferred Color: biz-internet
    - Click Save Match and Actions to save the Sequence.

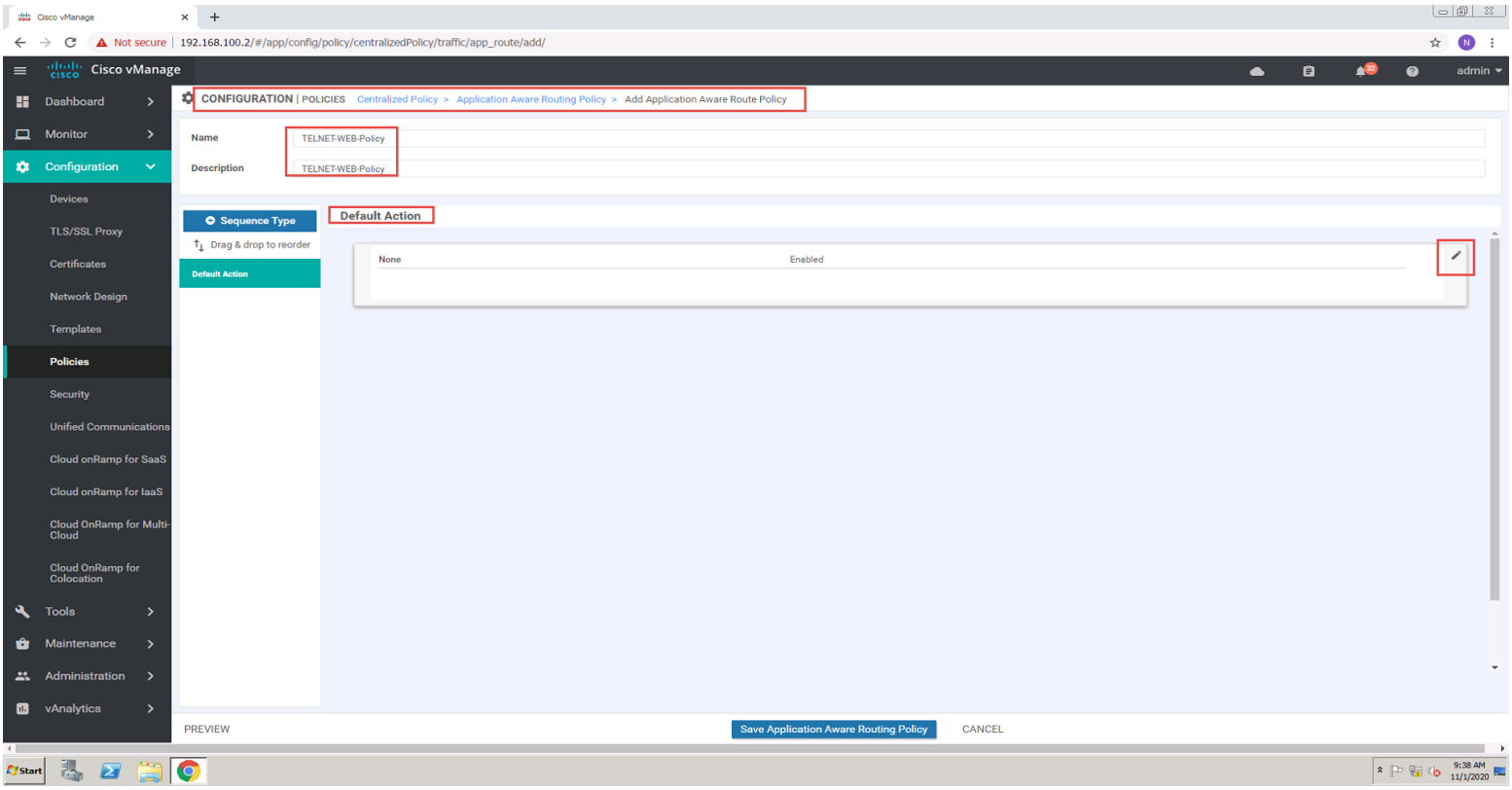
  Web Sequence

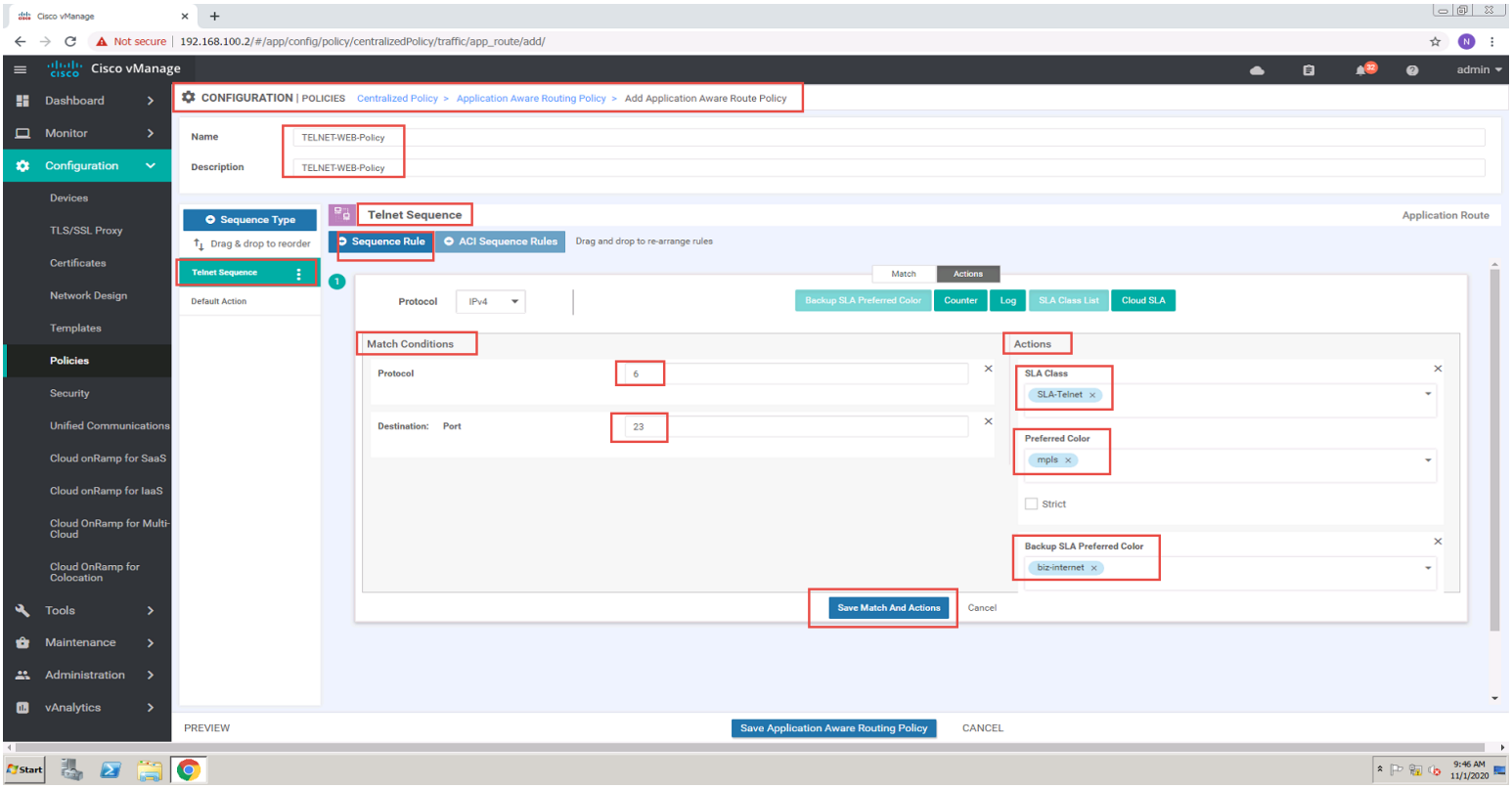
  Match Conditions:
    - Protocol: 6
    - Port: 80

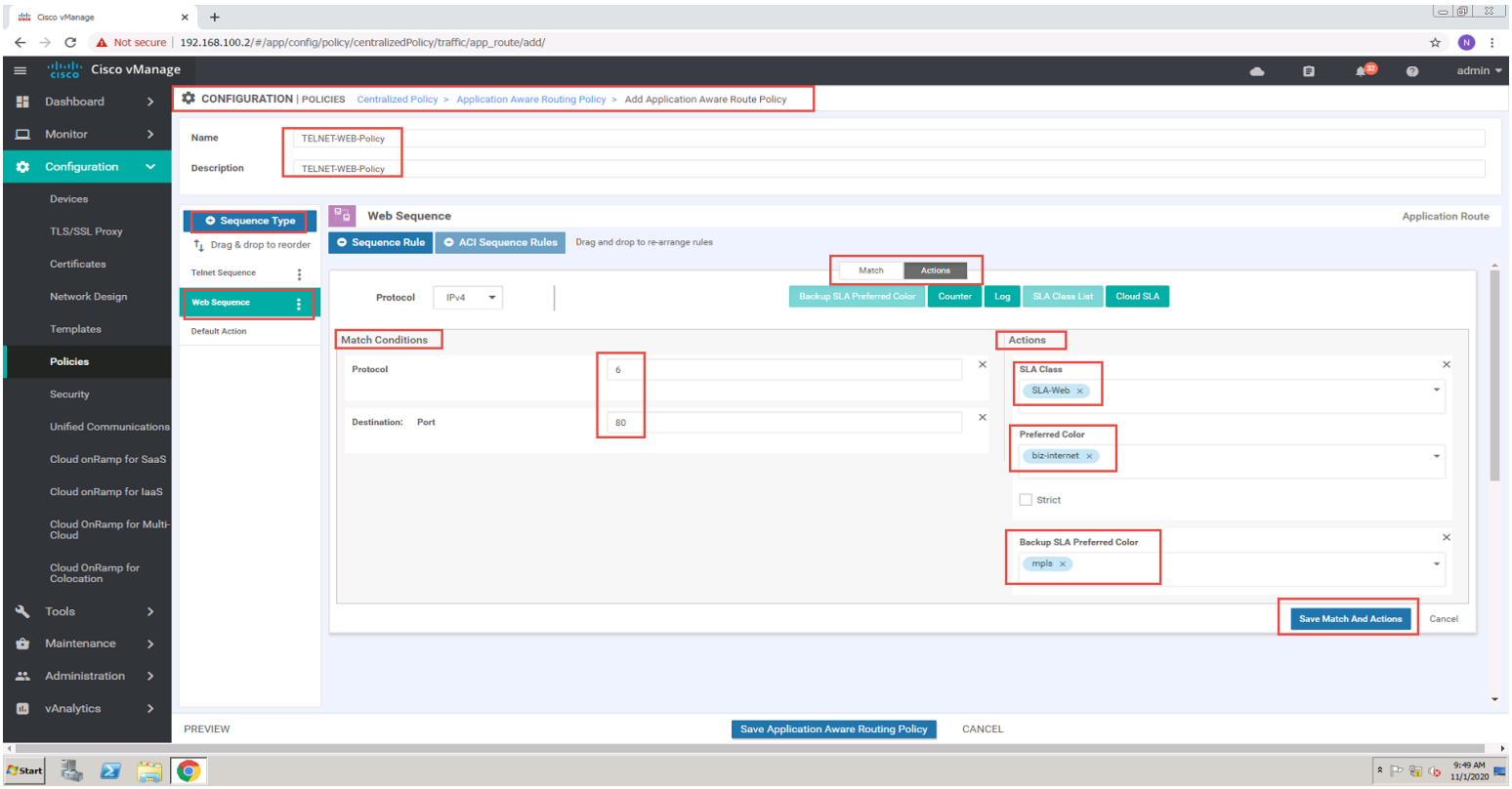
  Action
    - SLA Class List: SLA-Web

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




Cisco vManage
192.168.100.2/#/app/config/policy/centralizedPolicy/traffic/app_route/add/
CONFIGURATION | POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy
Name
TELNET-WEB-Policy
Description
TELNET-WEB-Policy
Sequence Type
Drag & drop to reorder
Default Action
Default Action
None
Enabled
PREVIEW
Save Application Aware Routing Policy
CANCEL

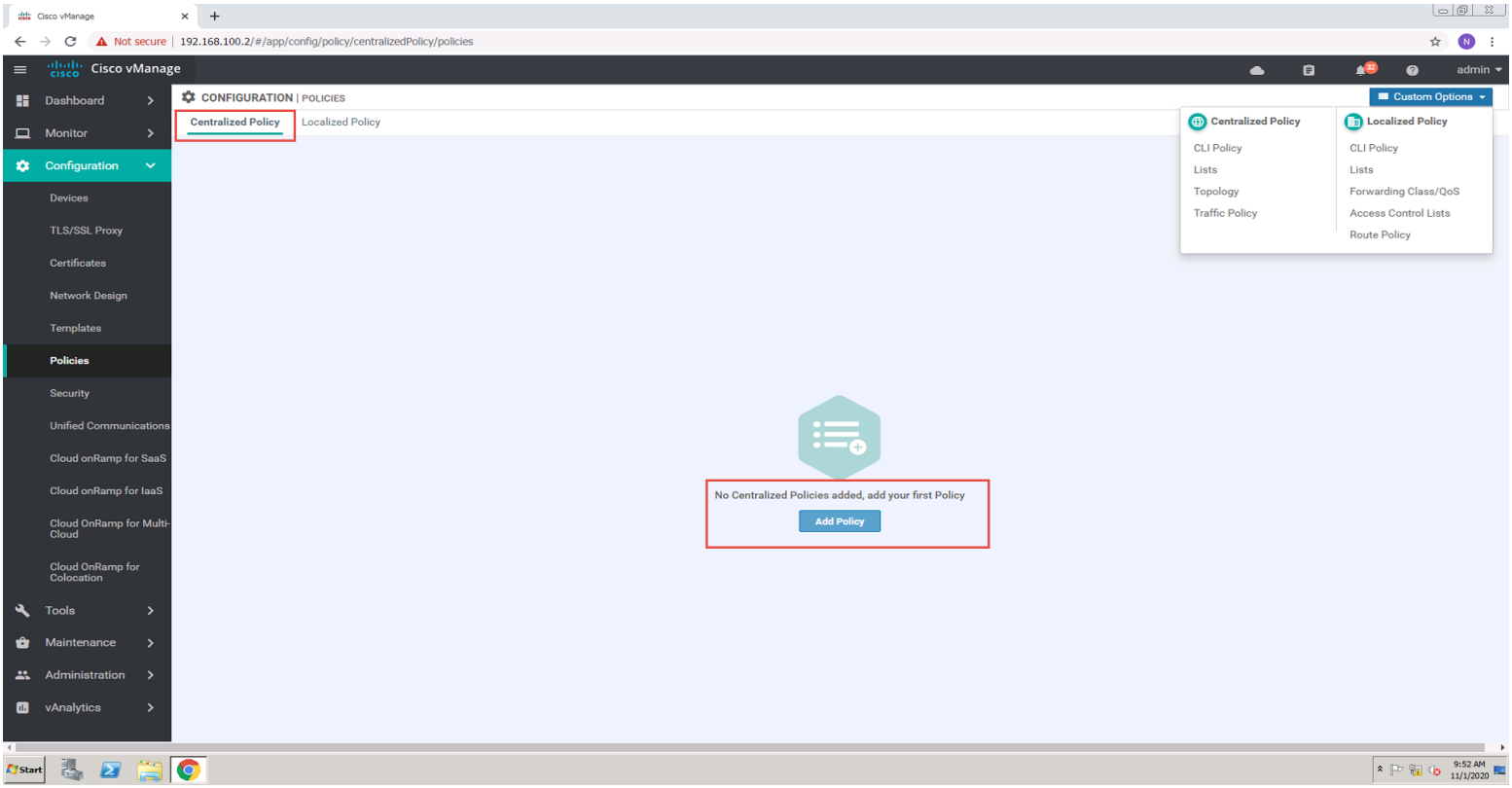

Cisco vManage
192.168.100.2/#/app/config/policy/centralizedPolicy/traffic/app_route/add/
CONFIGURATION | POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy
Name
TELNET-WEB-Policy
Description
TELNET-WEB-Policy
Sequence Type
Drag & drop to reorder
Telnet Sequence
Default Action
Telnet Sequence
Application Route
Sequence Rule
ACI Sequence Rules
Drag and drop to re-arrange rules
Match
Actions
Protocol
IPv4
Backup SLA Preferred Color
Counter
Log
SLA Class List
Cloud SLA
Match Conditions
Actions
Protocol
6
Destination: Port
23
SLA Class
SLA-Telnet
Preferred Color
mpls
Strict
Backup SLA Preferred Color
biz-internet
Save Match And Actions
Cancel
PREVIEW
Save Application Aware Routing Policy
CANCEL

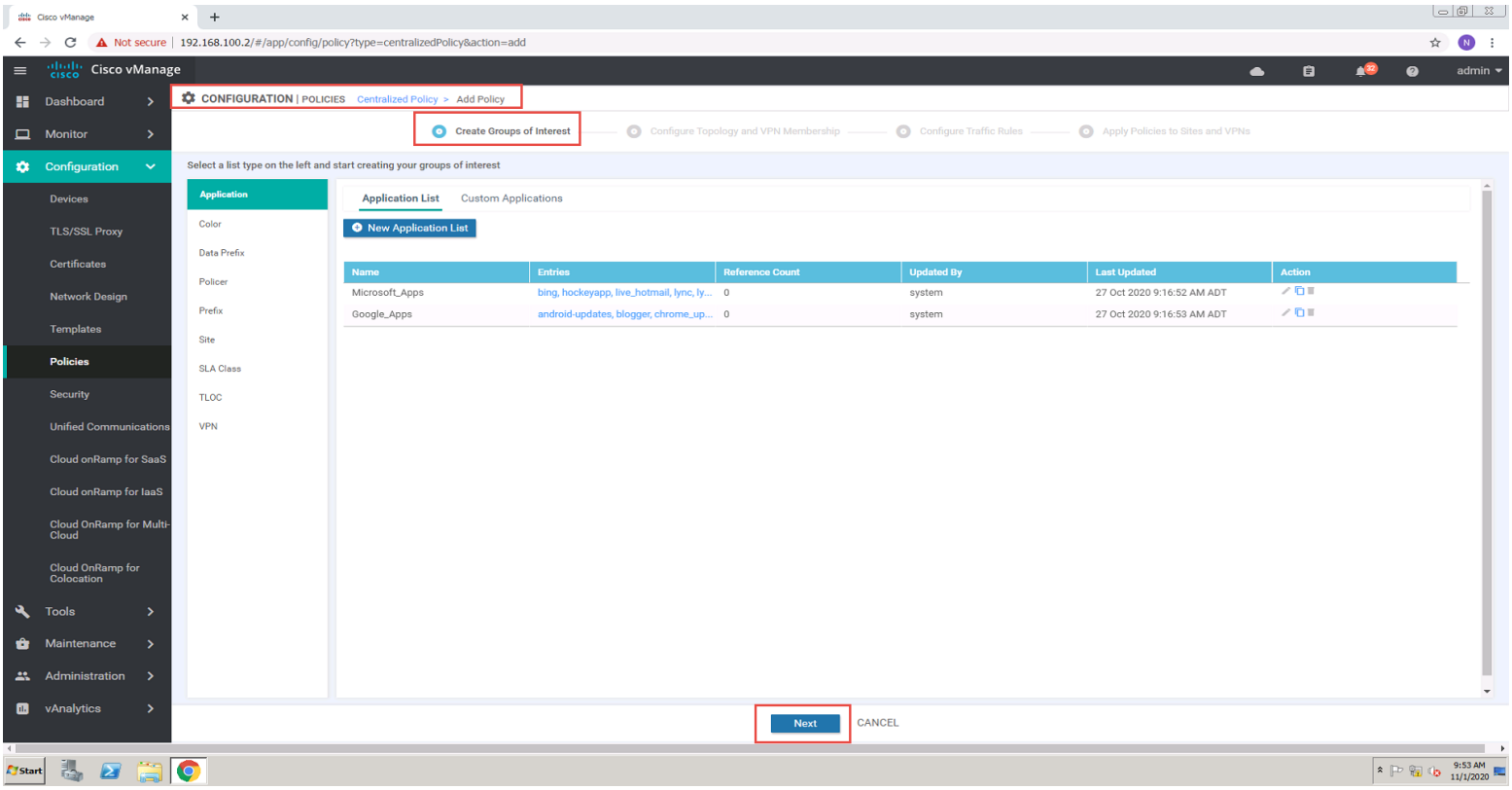


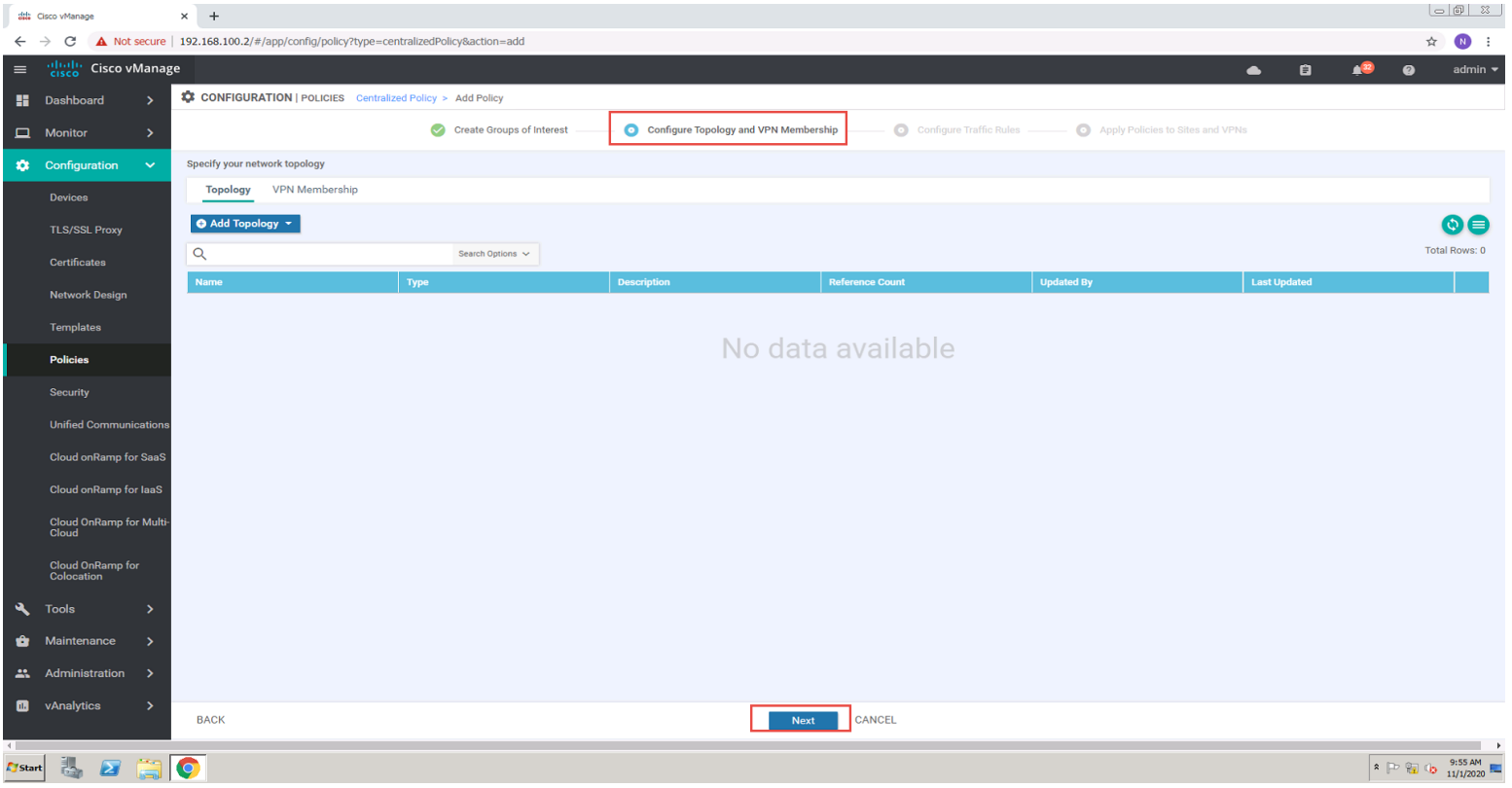
Task 3 – Create a Centralized Policy and call the Traffic Policy

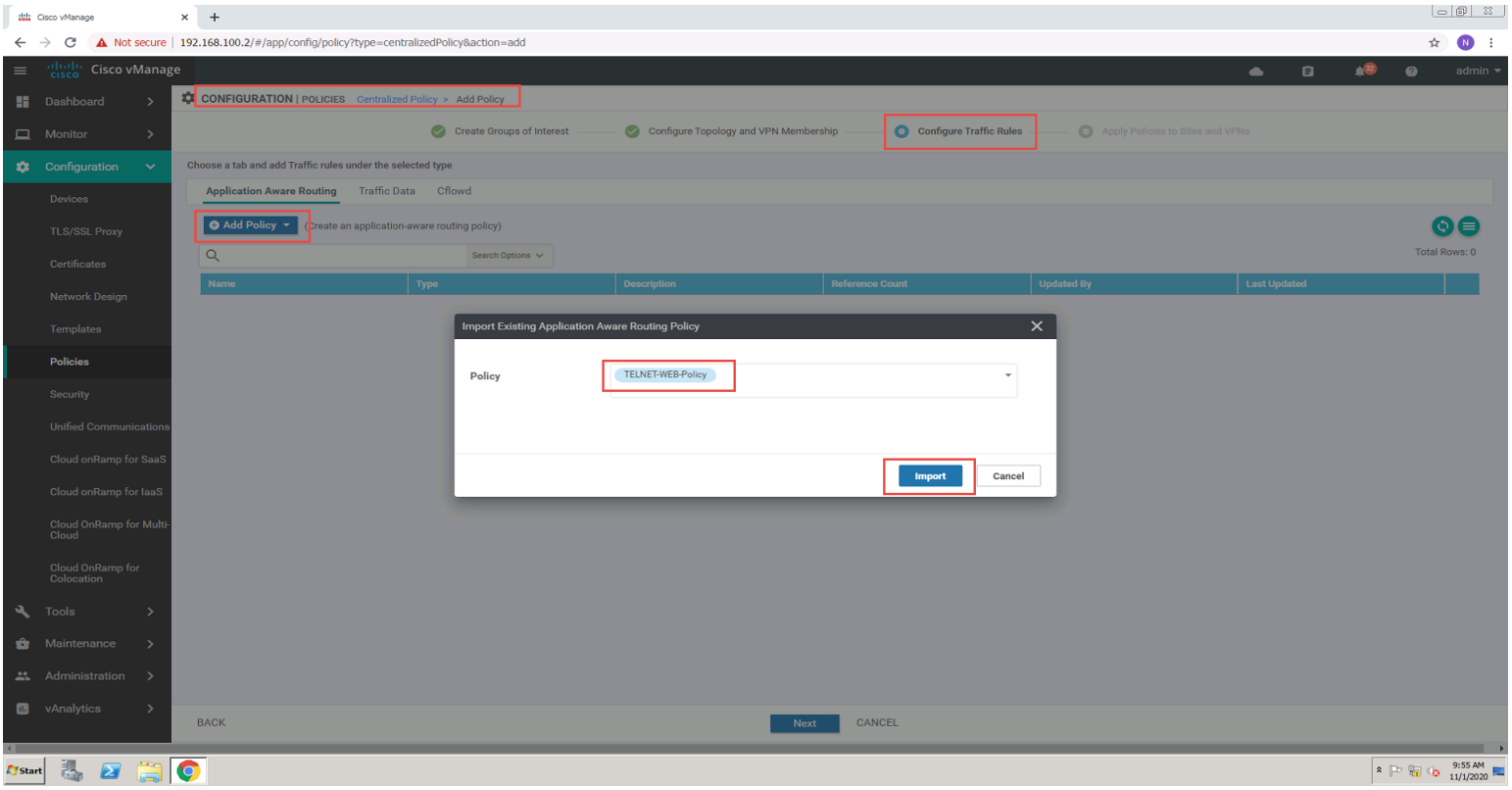
- In vManage, Navigate to Configuration ➔ Policies ➔ Custom Options ➔ Centralized Policy ➔ Add Centralized Policy
- Click Next on the “Group of Interests” page as we have already created the required lists.
- Click Next on the “Topology and VPN Membership” page as we are not using any Control Policies.
- 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:
    - Policy Name: Main-Central-Policy
    - 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).

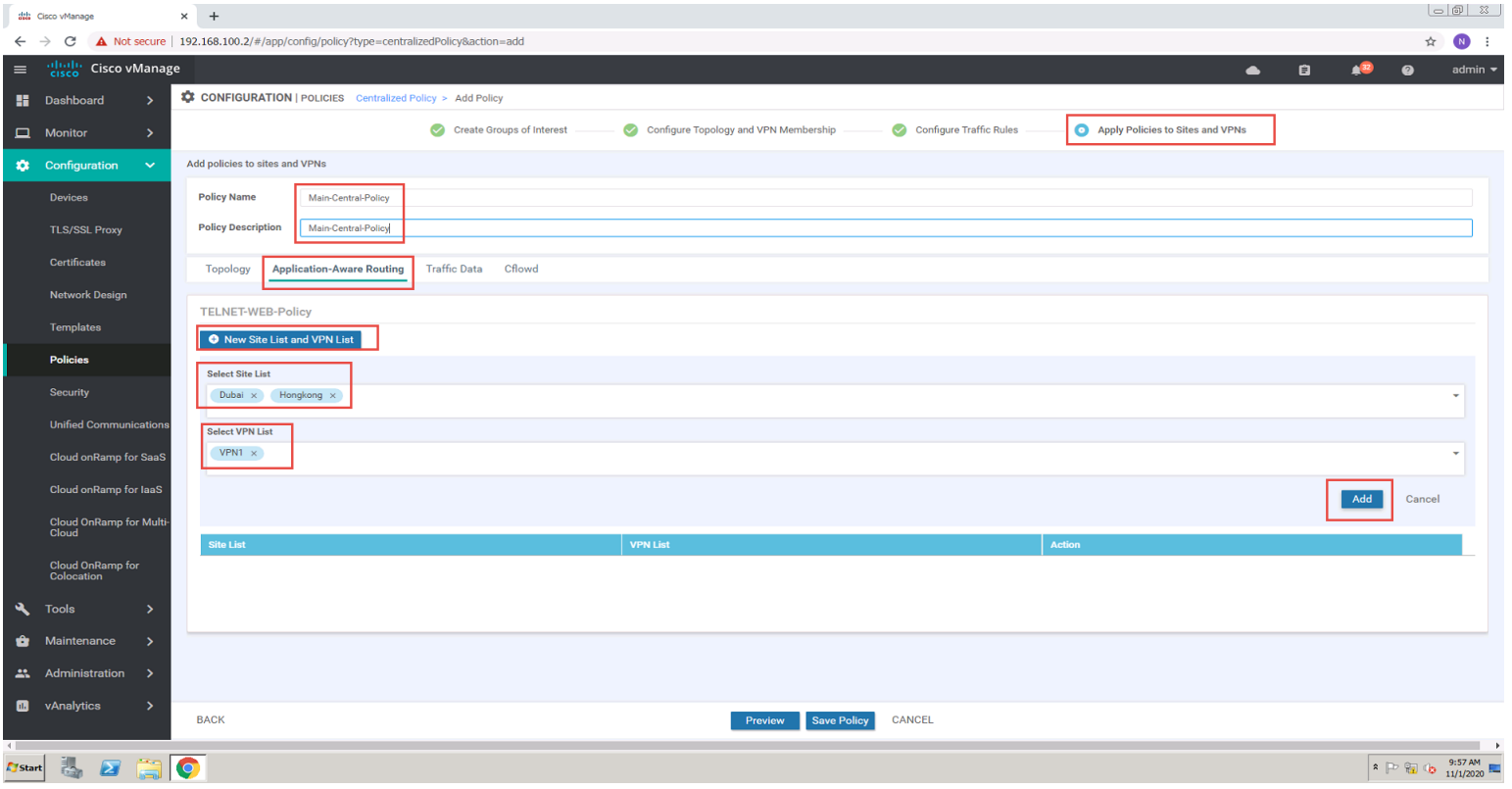
- Verify the policy by using the Monitor ➔ Network ➔ vEdge3 ➔ Troubleshooting ➔ Simulate Flows Tool.
- Telnet from Dubai or Hongkong should only use the mpls transport.
- Web from Dubai or Hongkong should only use the biz-internet transport.
- Normal Ping from Dubai or Hongkong should use both the Transports.

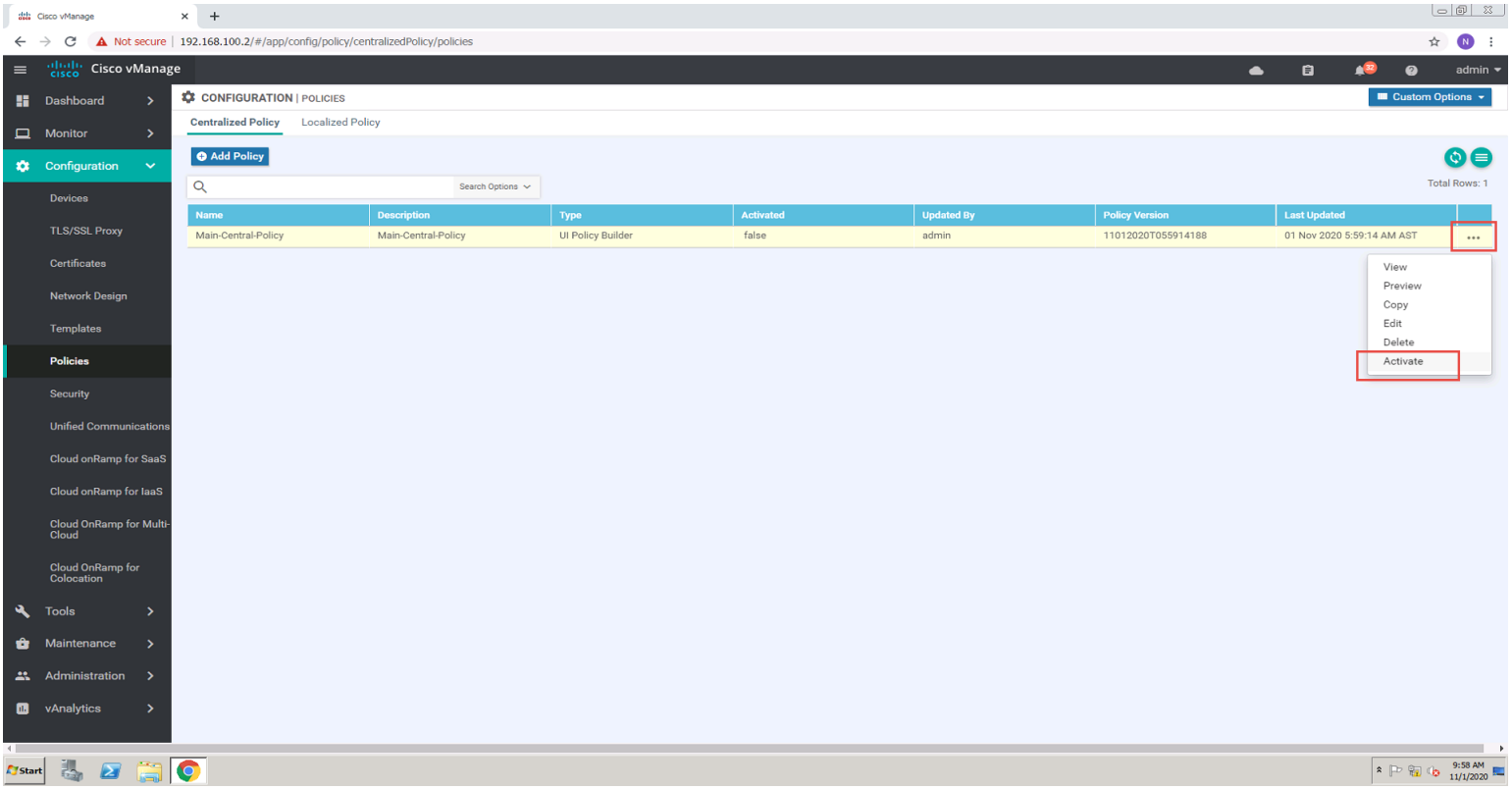


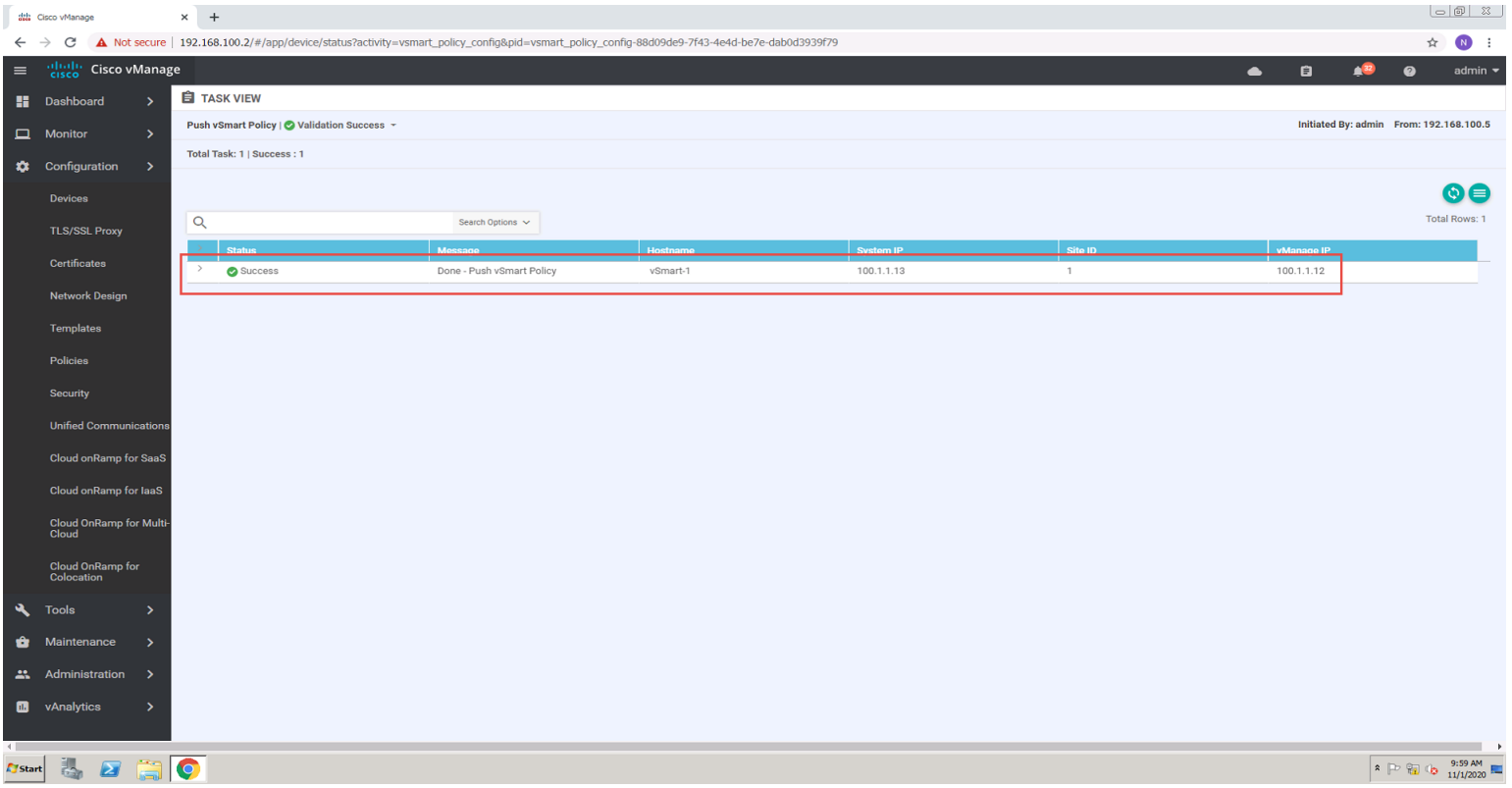


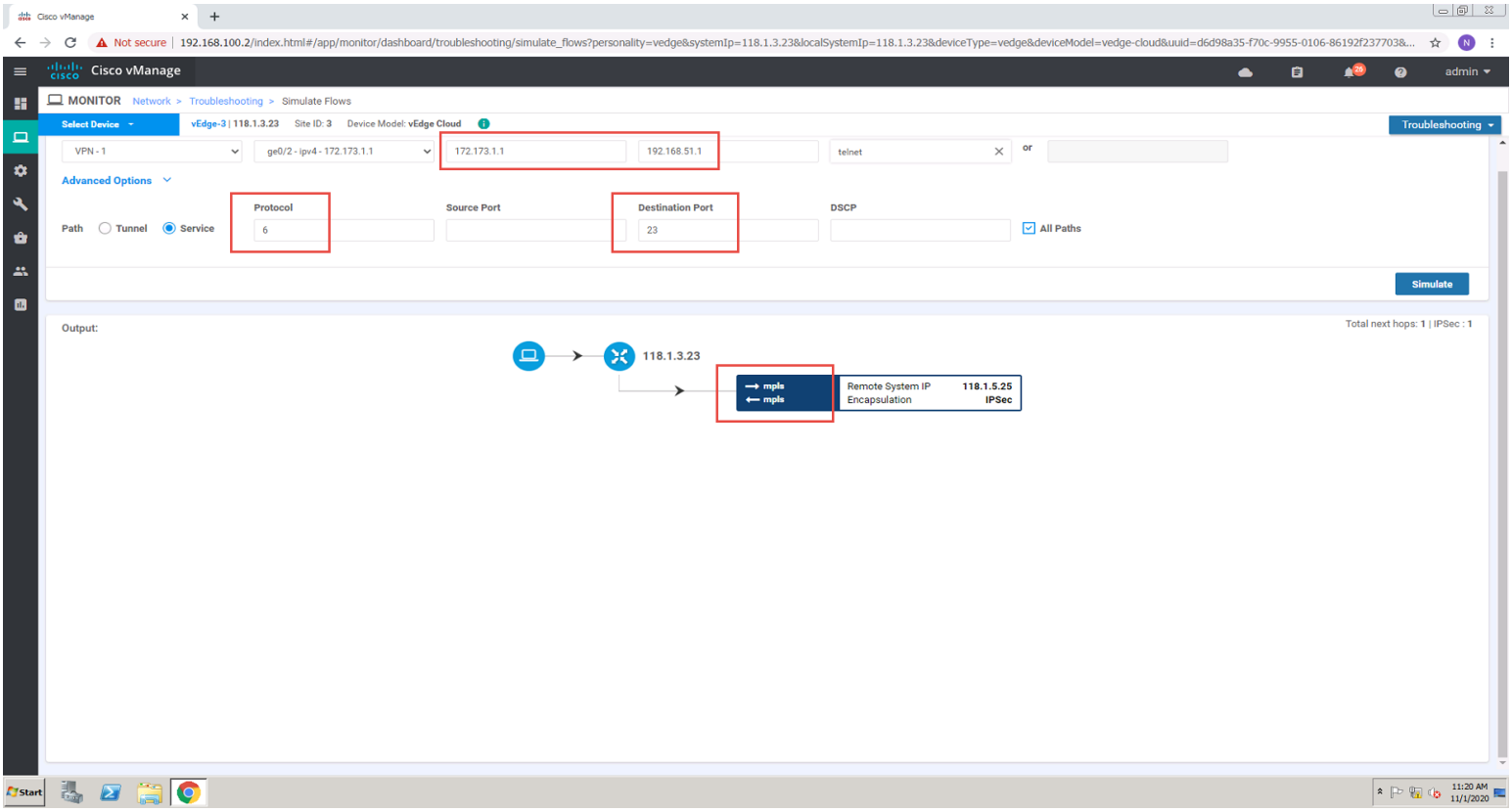


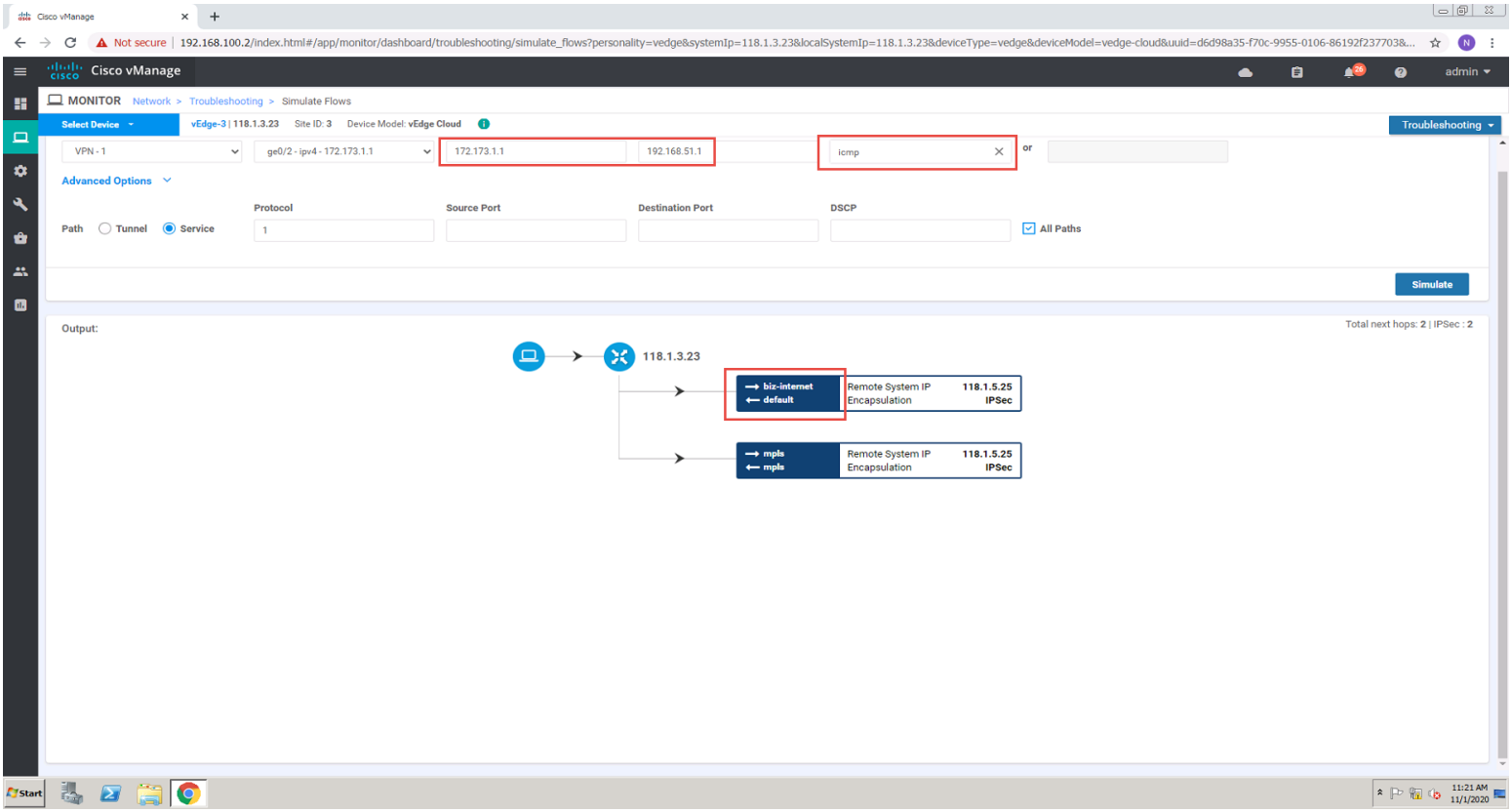

Cisco vManage
Not secure | 192.168.100.2/#/app/config/policy?type=centralizedPolicy&action=add
CONFIGURATION | POLICIES Centralized Policy > Add Policy
Create Groups of Interest
Configure Topology and VPN Membership
Configure Traffic Rules
Apply Policies to Sites and VPNs
Choose a tab and add Traffic rules under the selected type
Application Aware Routing
Traffic Data
Cflowd
Add Policy
Create an application-aware routing policy)
Import Existing Application Aware Routing Policy
Policy
TELNET-WEB-Policy
Import
Cancel
BACK
Next
CANCEL

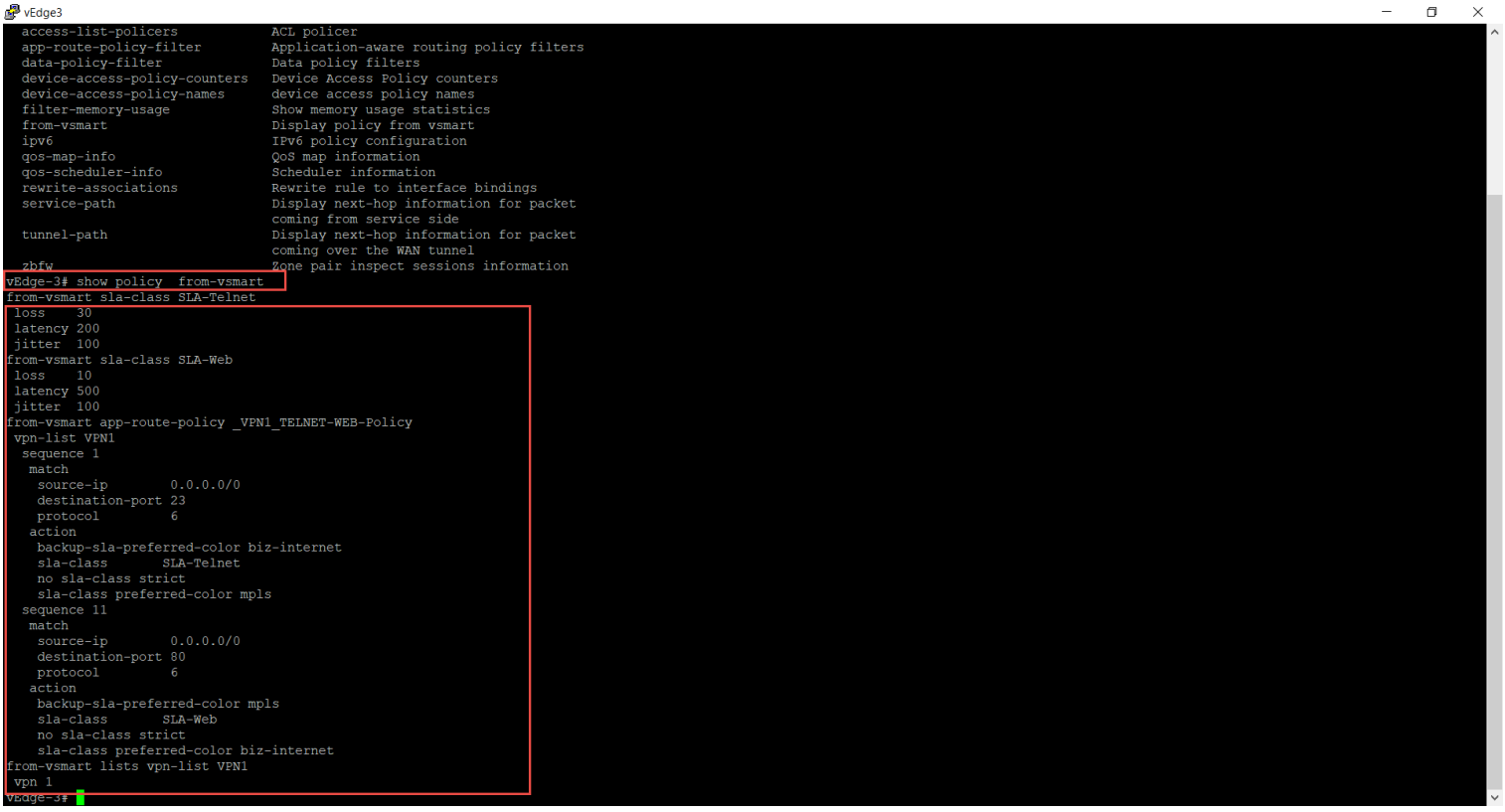

Cisco vManage
Not secure | 192.168.100.2/#/app/config/policy?type=centralizedPolicy&action=add
CONFIGURATION | POLICIES Centralized Policy > Add Policy
Create Groups of Interest
Configure Topology and VPN Membership
Configure Traffic Rules
Apply Policies to Sites and VPNs
Add policies to sites and VPNs
Policy Name
Main-Central-Policy
Policy Description
Main-Central-Policy
Topology
Application-Aware Routing
Traffic Data
Cflowd
TELNET-WEB-Policy
New Site List and VPN List
Select Site List
Dubai
Hongkong
Select VPN List
VPN1
Add
Cancel
Site List
VPN List
Action
BACK
Preview
Save Policy
CANCEL








Cisco vManage
MONITOR Network > Troubleshooting > Simulate Flows
Select Device
vEdge-3 | 118.1.3.23 Site ID: 3 Device Model: vEdge Cloud
Troubleshooting
VPN - 1
ge0/2 - ipv4 - 172.173.1.1
172.173.1.1
192.168.51.1
icmp
or
Advanced Options
Protocol
Source Port
Destination Port
DSCP
Path Tunnel Service
1
All Paths
Simulate
Output:
Total next hops: 2 | IPSec : 2
118.1.3.23
biz-internet
default
Remote System IP 118.1.5.25
Encapsulation IPSec
mpls
mpls
Remote System IP 118.1.5.25
Encapsulation IPSec


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
vEdge-3#

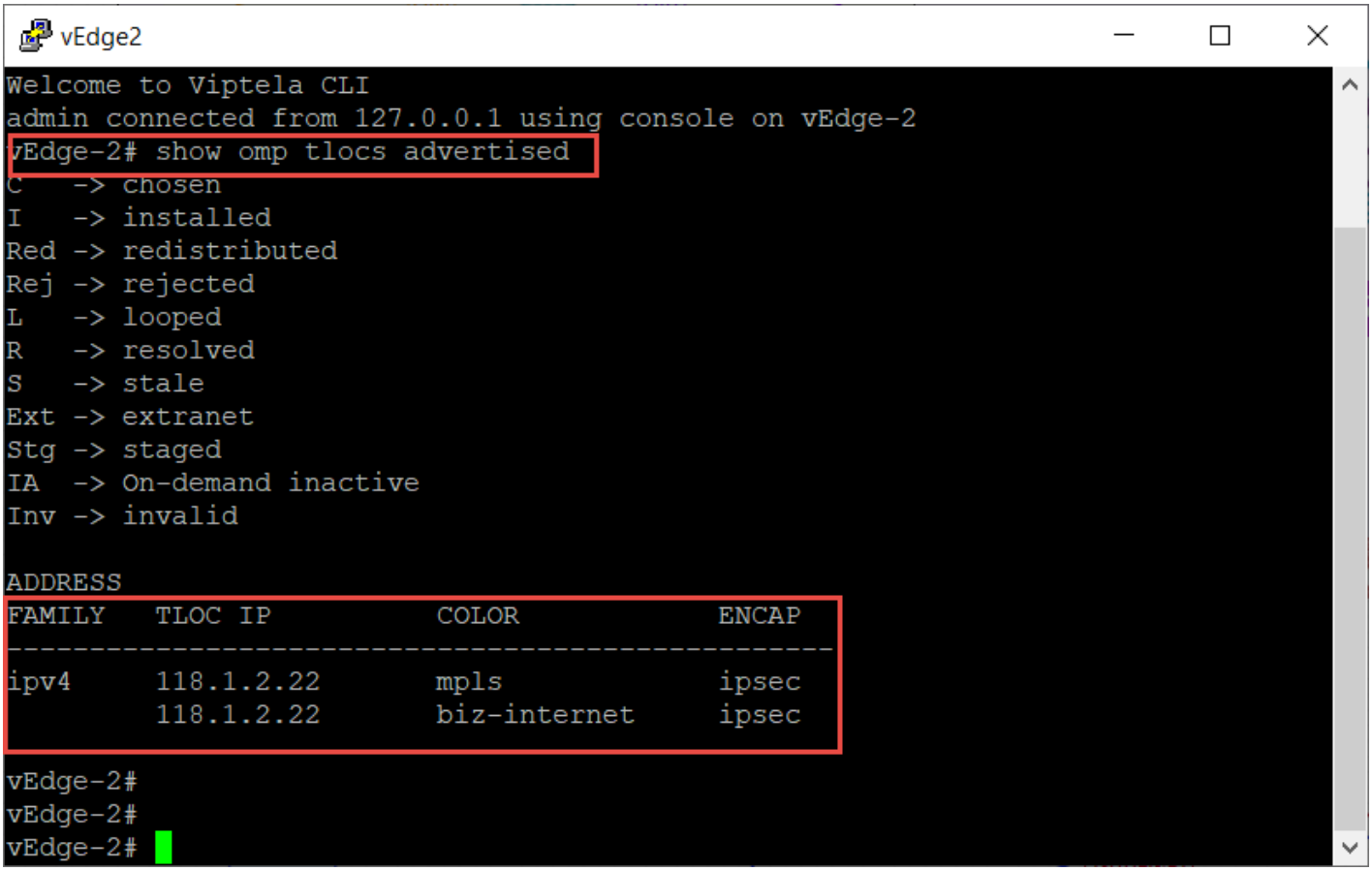
Lab 28 - Manipulating Traffic flow using TLOCs

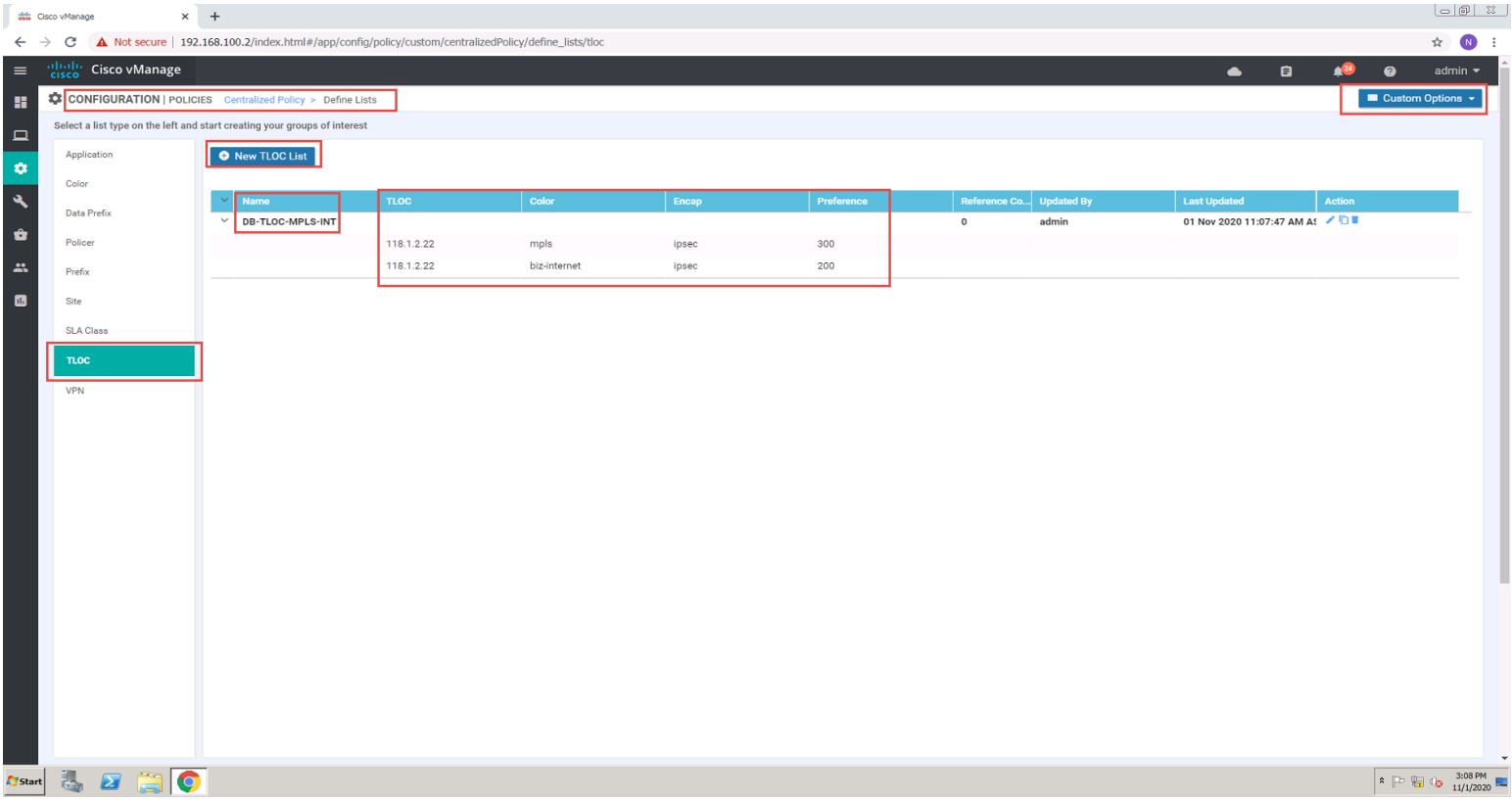
Requirements:

- Paris should only 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:
    - Name: DB-TLOC-MPLS-INT
    - TLOC#1:
        - IP Address: 118.1.2.22
        - Color: MPLS
        - Encapsulation: IPSec
        - Preference: 300
    - 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/centralizedPolicy/define_lists/tloc
Cisco vManage
admin
CONFIGURATION | POLICIES Centralized Policy > Define Lists
Custom Options
Select a list type on the left and start creating your groups of interest
Application
Color
Data Prefix
Policer
Prefix
Site
SLA Class
TLOC
VPN
New TLOC List
Name
TLOC
Color
Encap
Preference
Reference Co...
Updated By
Last Updated
Action
DB-TLOC-MPLS-INT
0
admin
01 Nov 2020 11:07:47 AM A
118.1.2.22 mpls ipsec 300
118.1.2.22 biz-internet ipsec 200

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:

- Site List: Dubai
- VPN List: VPN1

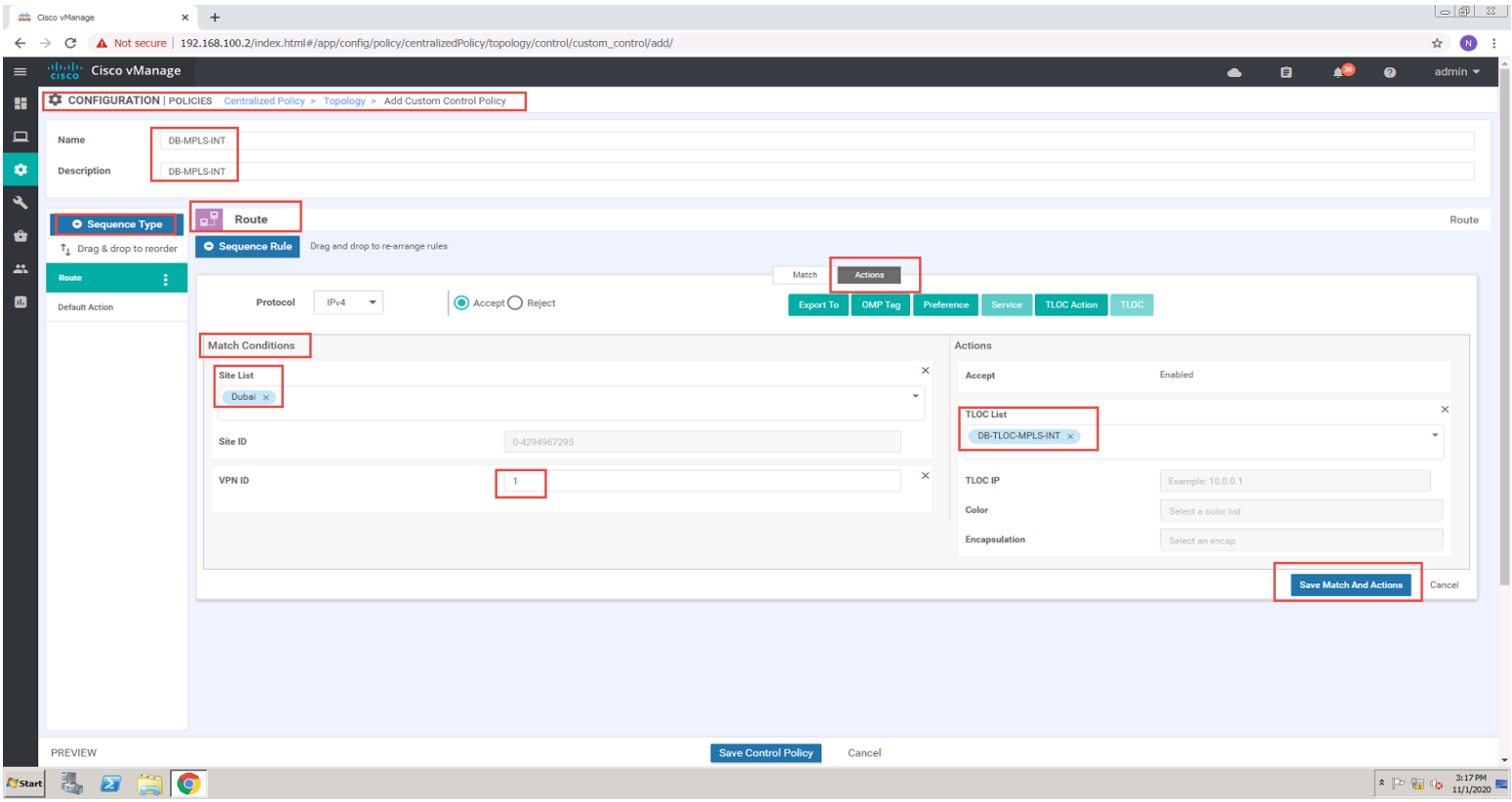
Action

- TLOC/TLOC List: DB-MPLS-INT
- Click Save Match and Actions to save the Sequence.

Default Sequence

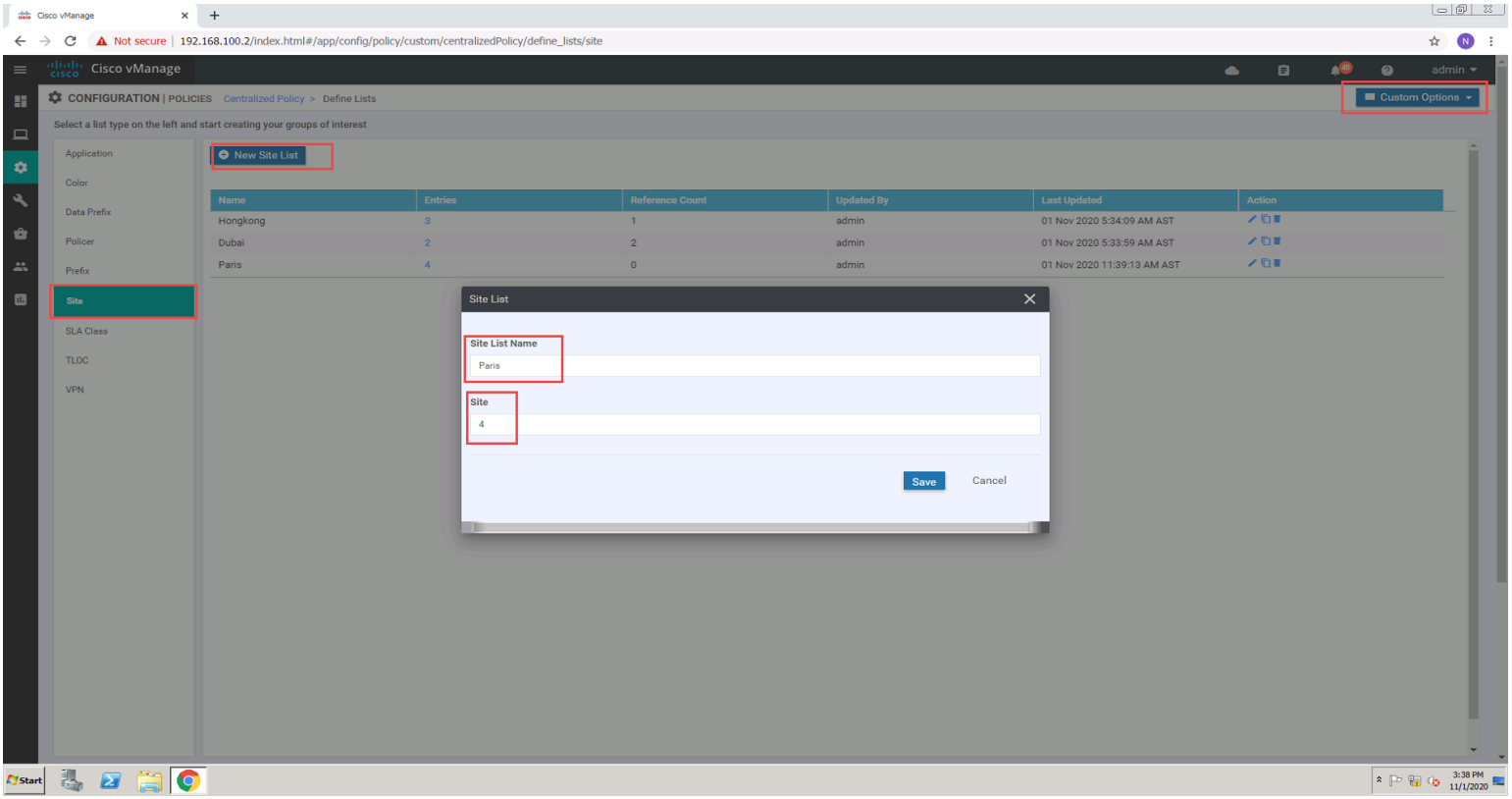
Action

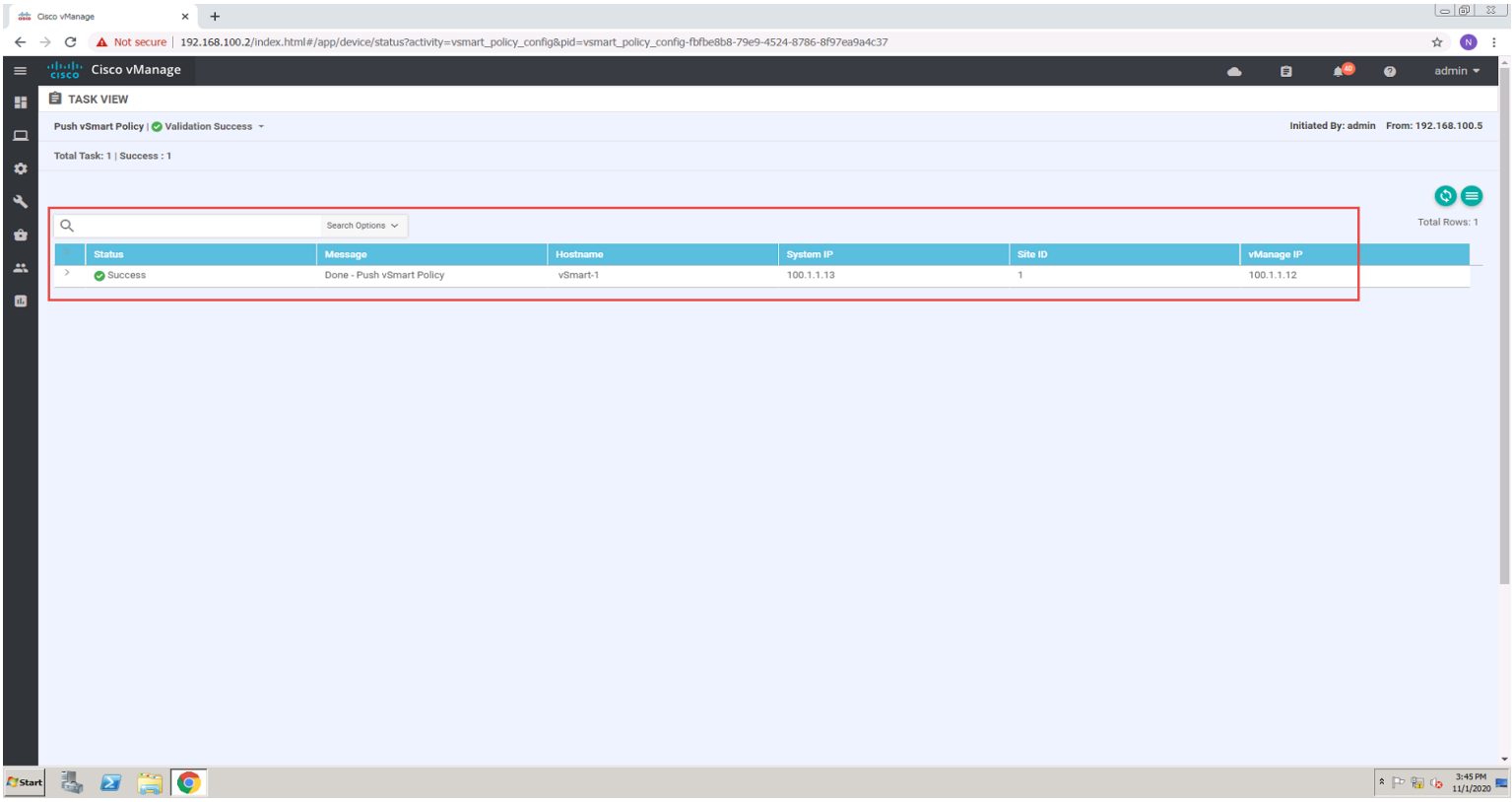
- Accept
- Click Save Match and Actions to save the Sequence.
- Save the Policy



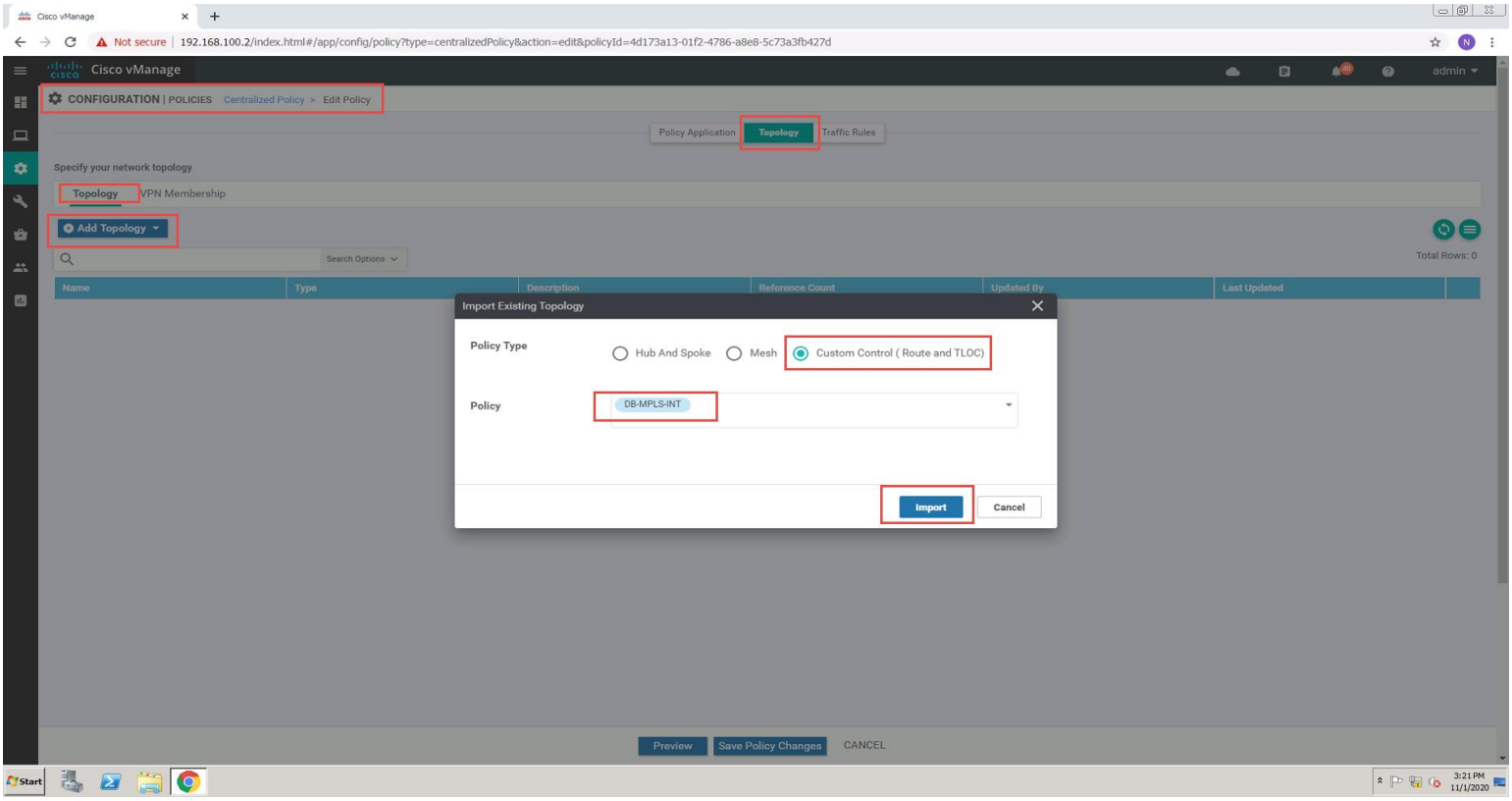
Task 3 – Modify the existing Centralized Policy "Main-CentralPolicy" and call the Topology Policy

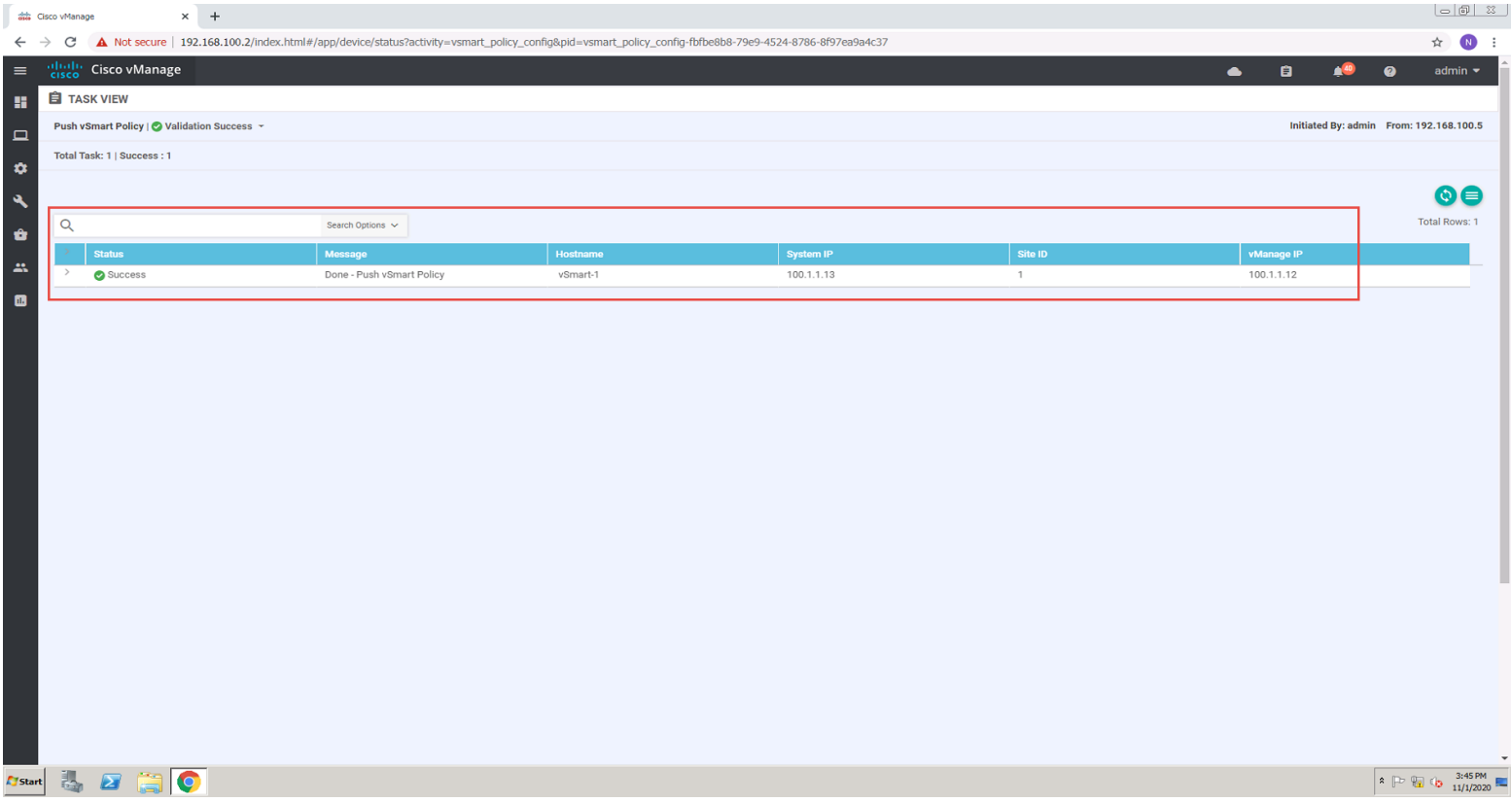
- In vManage, Navigate to Configuration ➔ Policies ➔ Custom Options ➔ Lists ➔ Site
- Create new site list Paris with site id 4.





- 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
Cisco vManage
admin
CONFIGURATION | POLICIES Centralized Policy > Edit Policy
Policy Application
Topology
Traffic Rules
Specify your network topology
Topology
VPN Membership
Add Topology
Search Options
Total Rows: 0
Name
Type
Description
Reference Count
Updated By
Last Updated
Import Existing Topology
Policy Type
Hub And Spoke
Mesh
Custom Control (Route and TLOC)
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
Cisco vManage
admin
TASK VIEW
Push vSmart Policy | Validation Success
Initiated By: admin From: 192.168.100.5
Total Task: 1 | Success : 1
Search Options
Total Rows: 1
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

```
1      192.168.43.0/24     ospf            IA       ge0/2       172.174.1.2     -       -               -              -      F,S
1      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 118.1.5.25 mpls 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

                                    PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP
VPN    PREFIX              PROTOCOL  SUB TYPE  IF NAME     ADDR             VPN      TLOC IP          COLOR           ENCAP  STATUS
-------------------------------------------------------------------------------------------------------------------------------------
1      172.16.234.4/32     ospf            IA       ge0/2       172.174.1.2     -       -               -              -      F,S
1      172.172.1.0/24      omp             -        -           -               -       118.1.2.22      mpls           ipsec  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      ospf            IA       ge0/2       -               -       -               -              -      -
1      172.174.1.0/24      connected       -        ge0/2       -               -       -               -              -      F,S
1      192.168.21.0/24     omp             -        -           -               -       118.1.2.22      mpls           ipsec  F,S
1      192.168.22.0/24     omp             -        -           -               -       118.1.2.22      mpls           ipsec  F,S
1      192.168.23.0/24     omp             -        -           -               -       118.1.2.22      mpls           ipsec  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
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    omp             -        -           -               -       118.1.2.22      mpls           ipsec  F,S
1      192.168.234.3/32    omp             -        -           -               -       118.1.3.23      mpls           ipsec  F,S
1      192.168.234.3/32    omp             -        -           -               -       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#
```

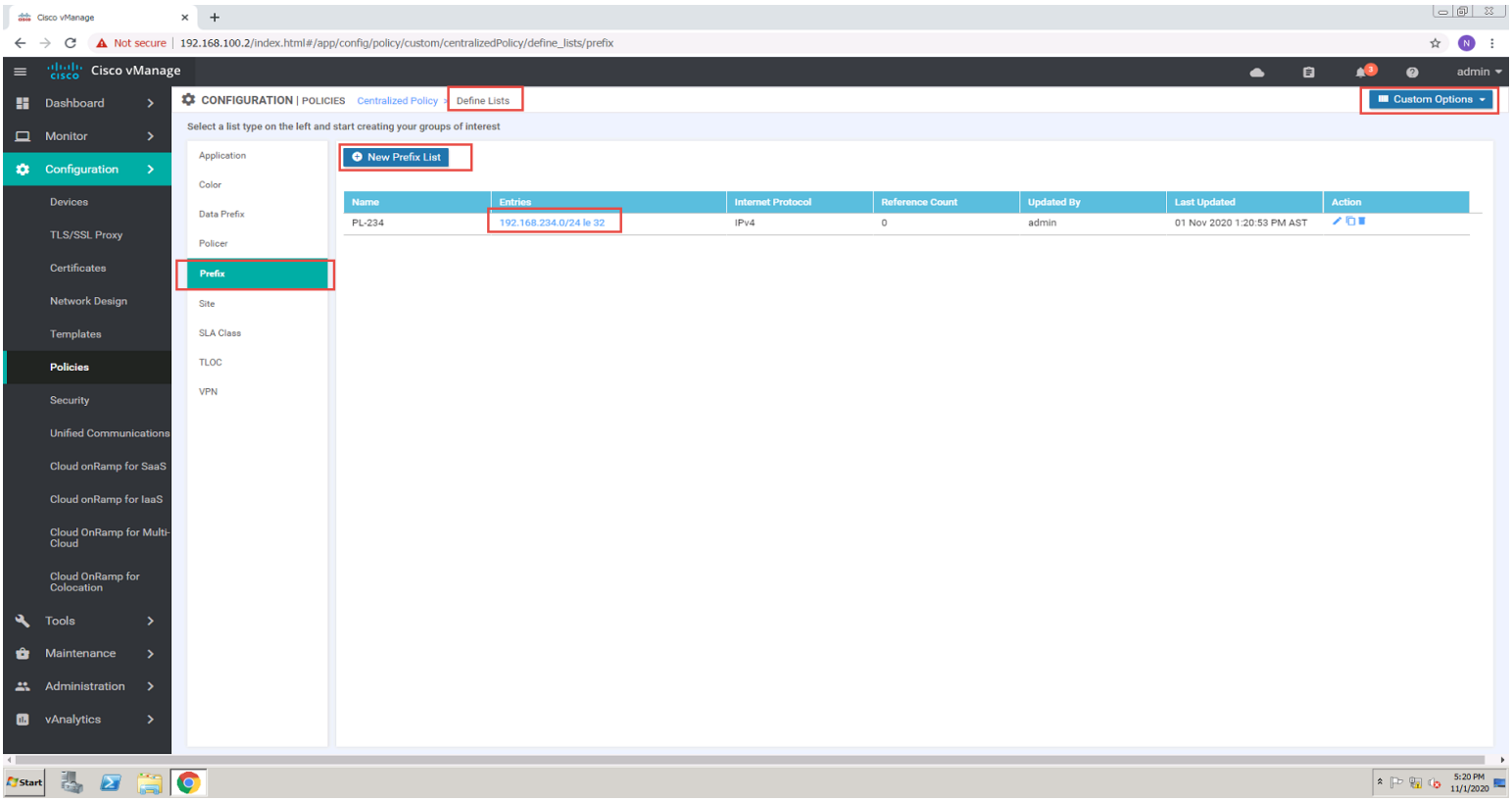
Lab 29 - Configuring Route Filtering

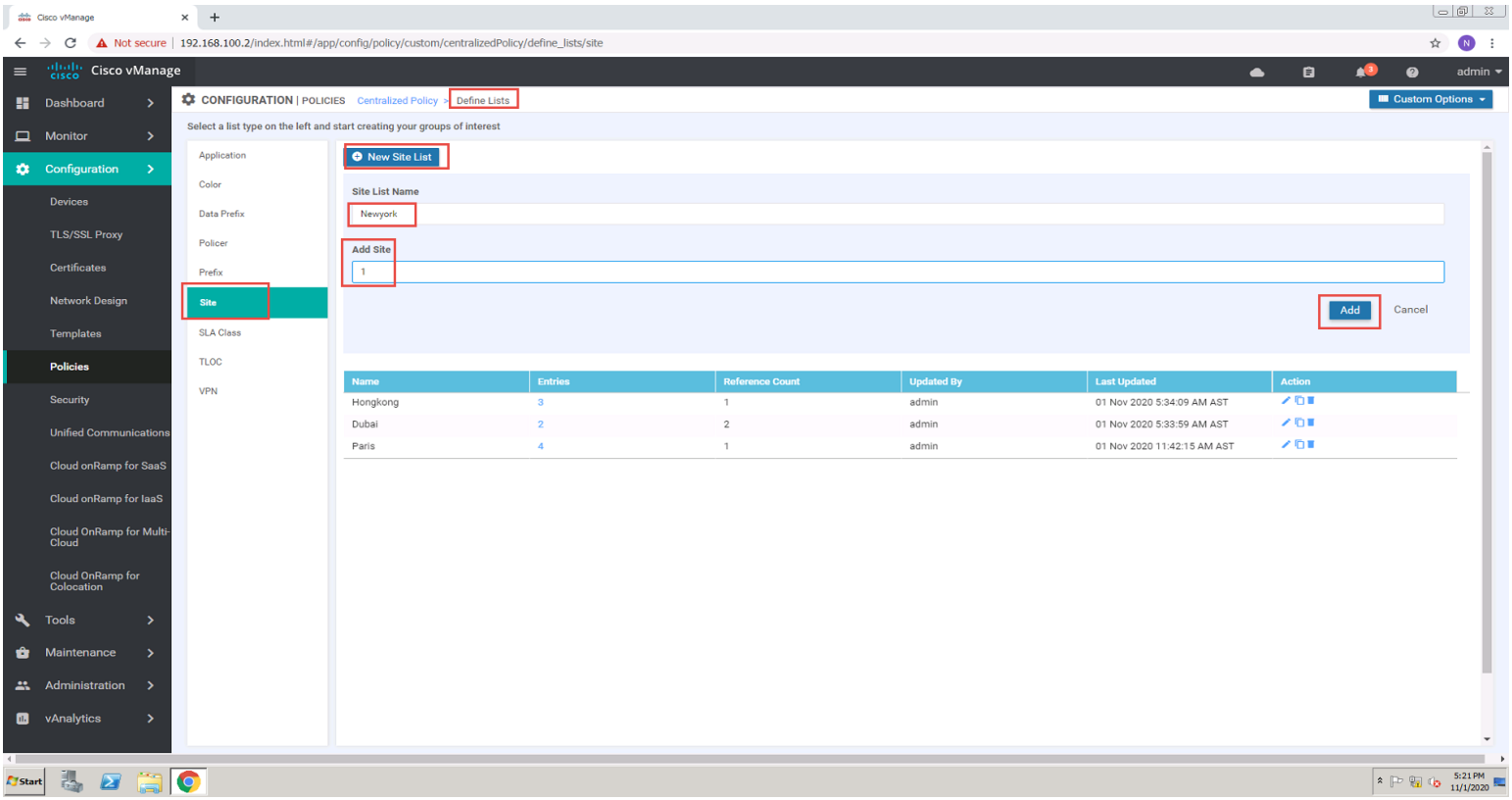
Requirements:

- 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:
  - Name: PL-234
  - Prefix List Entry: 192.168.234.0/24 le 32
- Click Site and select New Site list. Create a policy based on the following:
  - Name : Newyork
  - Site ID : 1





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:
    - Policy Name : PREF-234-NOT-2-NY
    - Description : PREF-234-NOT-2-NY

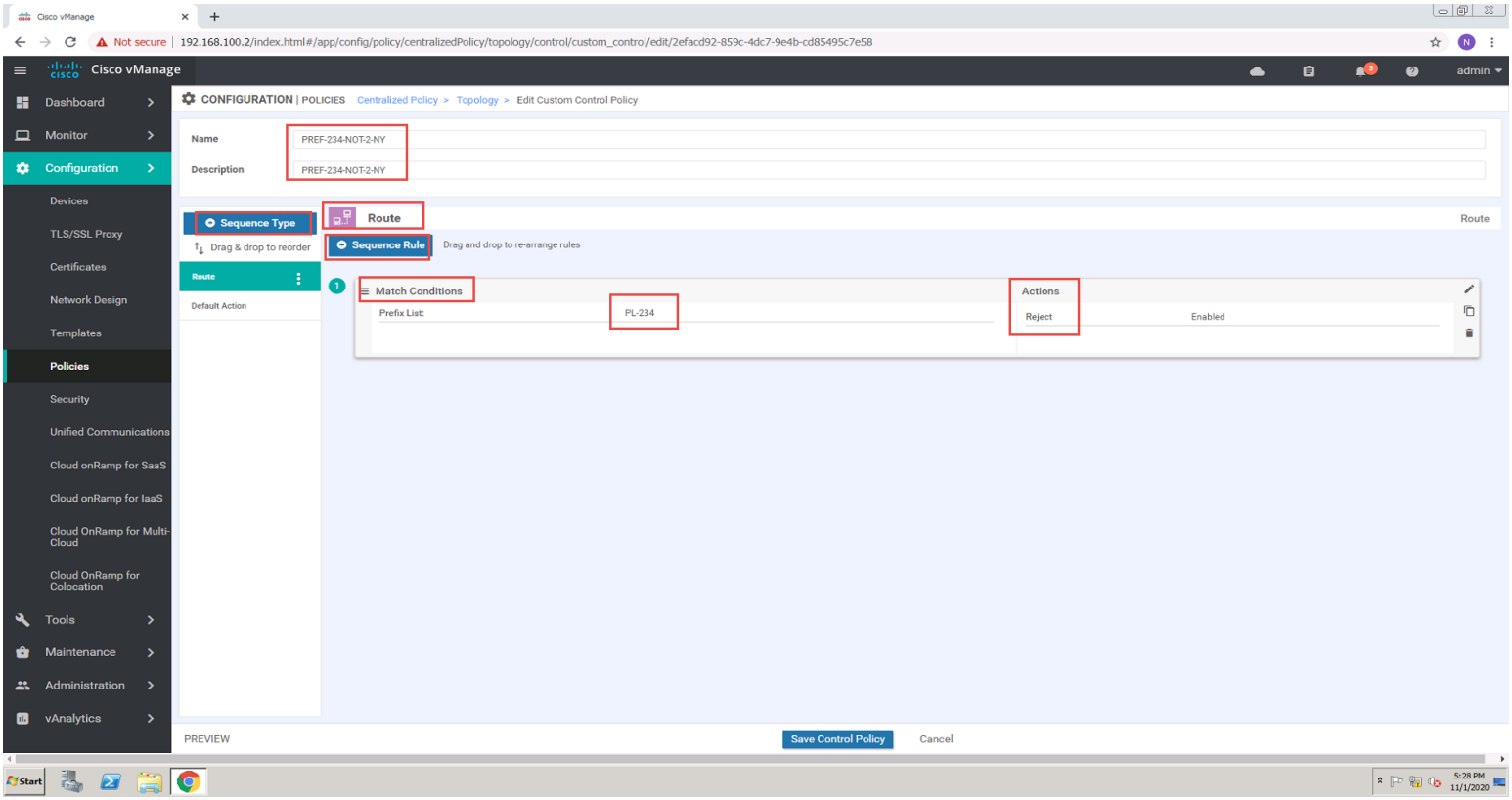
  Route Sequence

  Match Conditions:
    - Prefix List: PL-234

  Action: Reject
    - Click Save Match and Actions to save the Sequence.

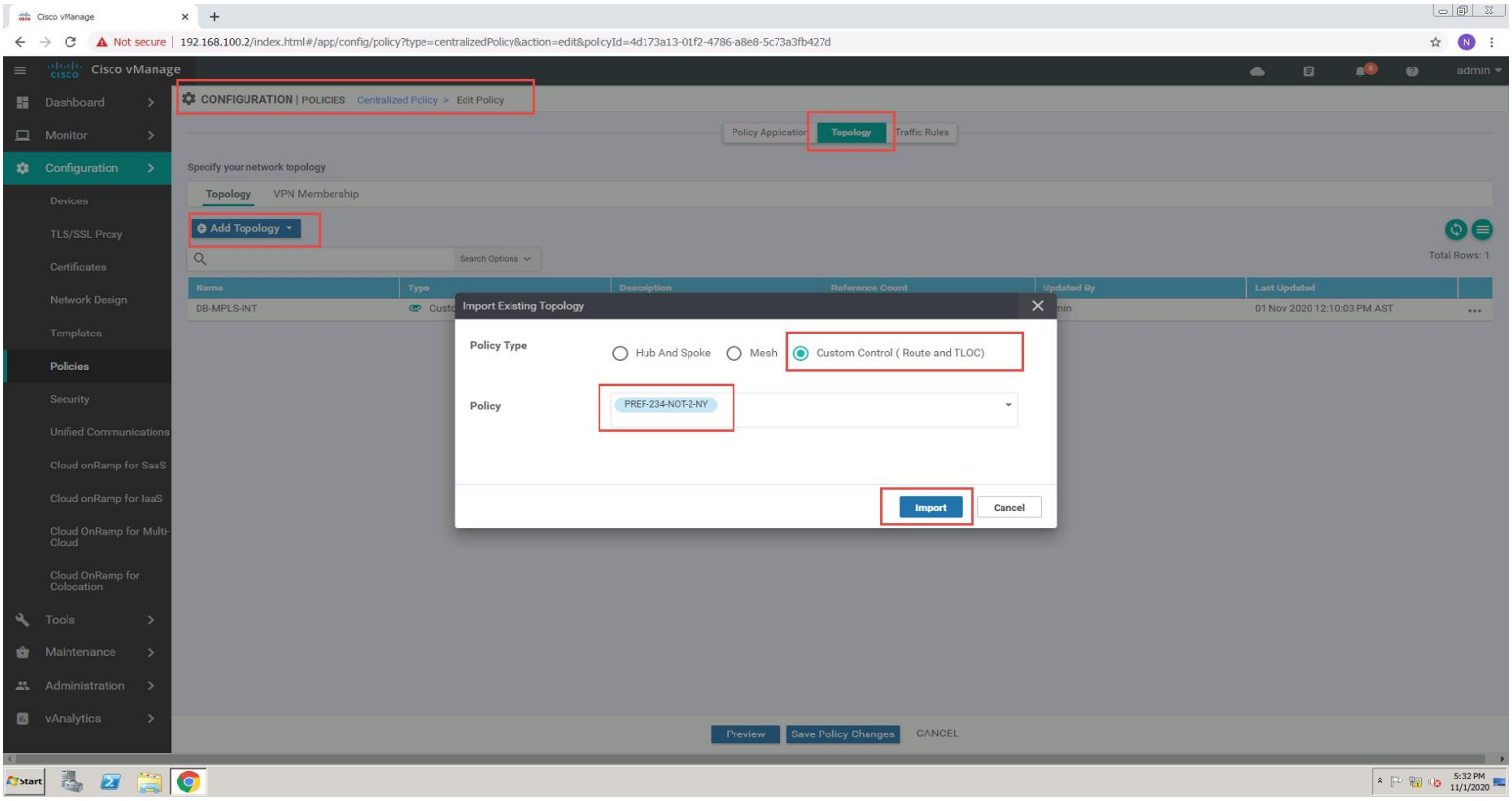
  Default Sequence

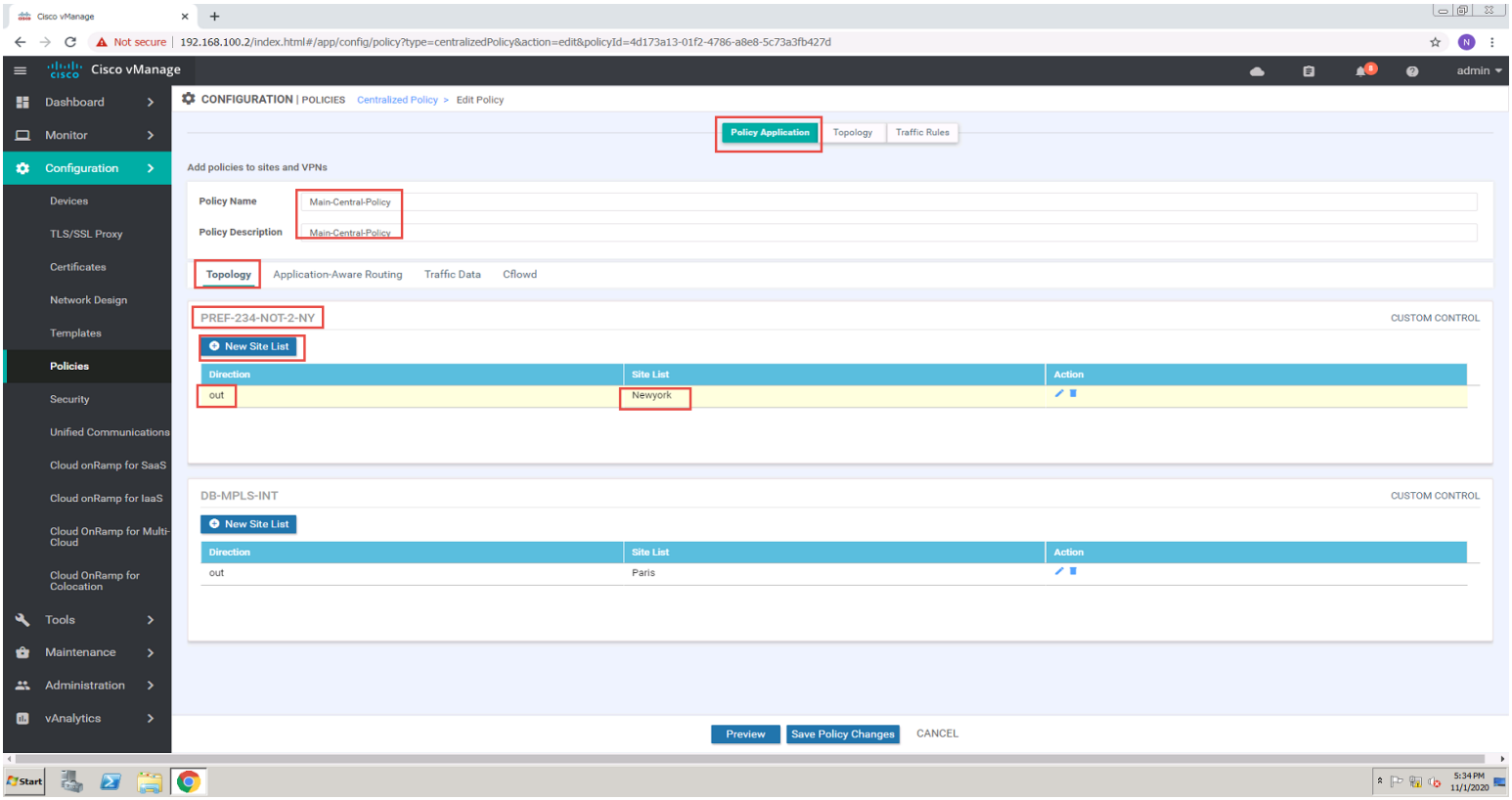
  Action
    - Accept
    - Click Save Match and Actions to save the Sequence.
    - Save the Policy



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
Policy Application Topology Traffic Rules
Specify your network topology
Topology VPN Membership
Add Topology
Import Existing Topology
Policy Type
Hub And Spoke
Mesh
Custom Control (Route and TLOC)
Policy
PREF-234-NOT-2-NY
Import
Cancel
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 Topology Traffic Rules
Add policies to sites and VPNs
Policy Name Main-Central-Policy
Policy Description Main-Central-Policy
Topology Application-Aware Routing Traffic Data Cflowd
PREF-234-NOT-2-NY
CUSTOM CONTROL
New Site List
Direction Site List Action
out Newyork
DB-MPLS-INT
CUSTOM CONTROL
New Site List
Direction Site List Action
out Paris
Preview
Save Policy Changes
CANCEL

vEdge1

```
vEdge-1# show ip route
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

Before apply policy

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	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	F,S
1	172.173.1.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	172.174.1.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S
1	172.175.1.0/24	omp	-	-	-	-	118.1.5.25	mpls	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	F,S
1	192.168.22.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	F,S
1	192.168.23.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	F,S
1	192.168.31.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	192.168.32.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	192.168.33.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	192.168.41.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S
1	192.168.42.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S
1	192.168.43.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S
1	192.168.51.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	F,S
1	192.168.52.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	F,S
1	192.168.53.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	F,S
1	192.168.234.2/32	omp	-	-	-	-	118.1.2.22	mpls	ipsec	F,S
1	192.168.234.3/32	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	192.168.234.4/32	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S

vEdge1

```
vEdge-1# show ip route
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

Before apply policy

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	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	F,S
1	172.173.1.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	172.174.1.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S
1	172.175.1.0/24	omp	-	-	-	-	118.1.5.25	mpls	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	F,S
1	192.168.22.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	F,S
1	192.168.23.0/24	omp	-	-	-	-	118.1.2.22	mpls	ipsec	F,S
1	192.168.31.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	192.168.32.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	192.168.33.0/24	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	192.168.41.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S
1	192.168.42.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S
1	192.168.43.0/24	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S
1	192.168.51.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	F,S
1	192.168.52.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	F,S
1	192.168.53.0/24	omp	-	-	-	-	118.1.5.25	mpls	ipsec	F,S
1	192.168.234.2/32	omp	-	-	-	-	118.1.2.22	mpls	ipsec	F,S
1	192.168.234.3/32	omp	-	-	-	-	118.1.3.23	mpls	ipsec	F,S
1	192.168.234.4/32	omp	-	-	-	-	118.1.4.24	mpls	ipsec	F,S