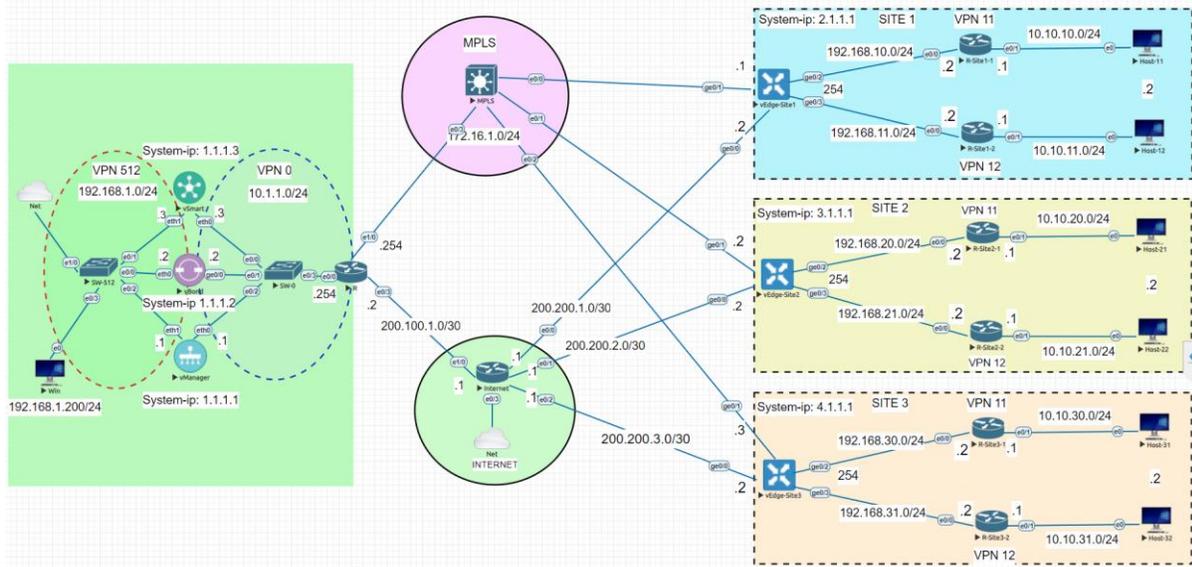


LAB - VIẾT CENTRALIZED POLICY ĐỂ CÔ LẬP GUEST USER GIỮA CÁC CHI NHÁNH

I. Sơ đồ



II. Yêu cầu kỹ thuật

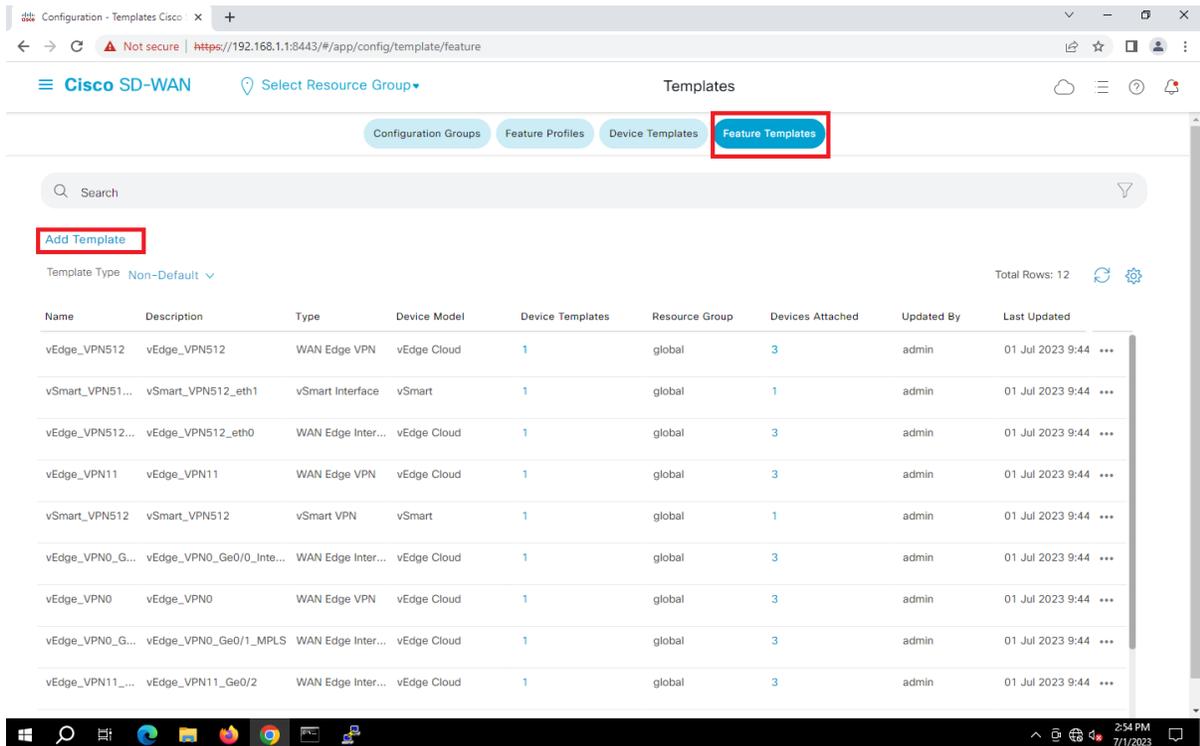
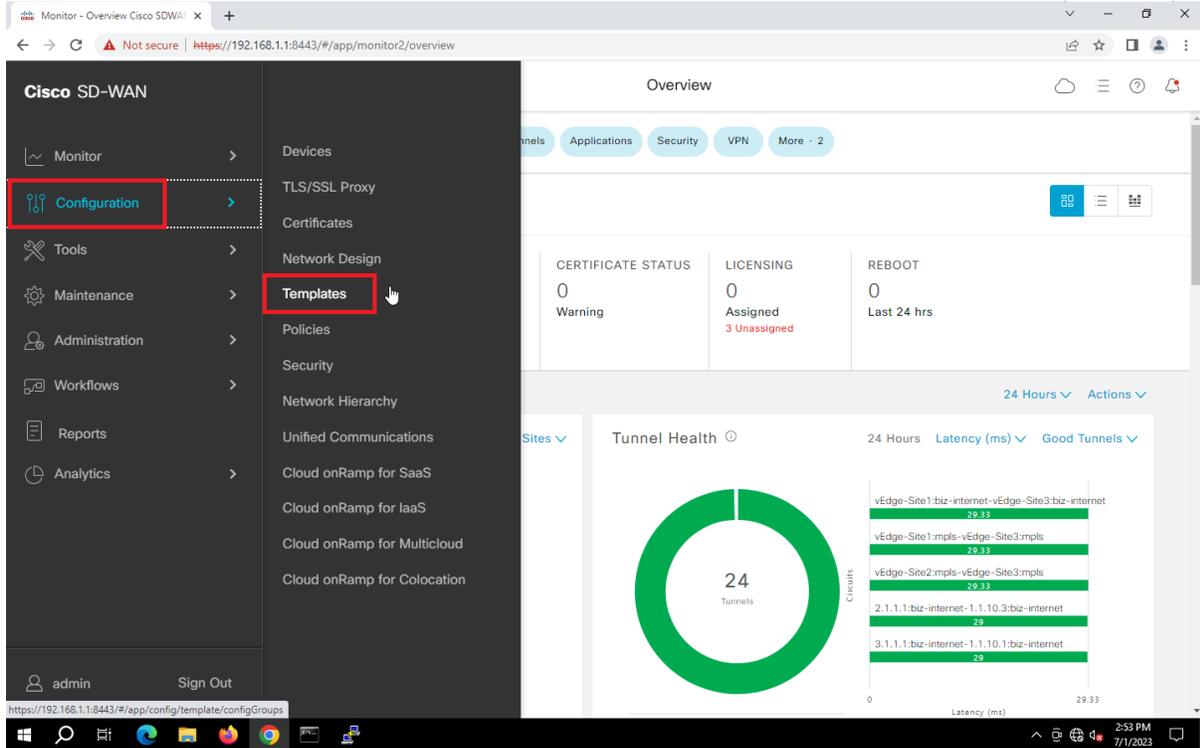
- Viết ba Feature Template có tên là *vEdge_VPN12*, *vEdge_VPN12_GE0/3* và *vEdge_VPN12*.
- Viết một Device Template từ ba Feature Template trên và dùng lại các Feature Template cũ (*vEdge_VPN0*, *vEdge_VPN0_GE0/0*, *vEdge_VPN0_GE0/1*, *vEdge_VPN512*, *vEdge_VPN512_eth0*, *vEdge_VPN11*, *vEdge_OSPF*) để tạo thêm một VPN12 dành cho khách ở các site.
- Đẩy cấu hình Device Template vừa viết xong.
- Viết Centralized Policy để cô lập VPN12 không cho giao tiếp được giữa các site.

III. Các bước thực hiện

3.1. Viết ba Feature Template cho VPN12 dành cho khách hàng

Tạo Feature Template: *vEdge_VPN12*

Đầu tiên ta vào giao diện **vManage > Configuration > Template > Feature > Add Template**.



Ở phần **Select Devices** ta chọn thiết bị **vEdge cloud** rồi chọn mục **VPN**

Configuration - Templates Cisco x +

Not secure | https://192.168.1.1:8443/#/app/config/template/feature?display=add

Cisco SD-WAN Select Resource Group Templates

Configuration Groups Feature Profiles Device Templates Feature Templates

Feature Template > Add Template

Select Devices

Search by device name

- ISRV
- vEdge 100
- vEdge 100 B
- vEdge 100 M
- vEdge 100 WM
- vEdge 1000
- vEdge 2000
- vEdge 5000
- vEdge Cloud
- vManage
- vSmart

VPN

- Secure Internet Gateway (SIG) WAN
- VPN Interface Bridge LAN
- VPN Interface Cellular WAN
- VPN Interface Ethernet Management WAN LAN
- VPN Interface GRE WAN
- VPN Interface IPsec WAN
- VPN Interface NATPool WAN
- VPN Interface PPP WAN

Tiếp theo vào mục VPN ta cấu hình như sau:

Template Name: *vEdge_VPN12*

Description: *vEdge_VPN12*

VPN: 12

Configuration - Templates Cisco x +

Not secure | https://192.168.1.1:8443/#/app/config/template/feature?display=add&deviceType=vedge-cloud&templateType=vpn-vedge

Cisco SD-WAN Select Resource Group Templates

Configuration Groups Feature Profiles Device Templates Feature Templates

Feature Template > Add Template > VPN

Device Type vEdge Cloud

Template Name* vEdge_VPN12

Description* vEdge_VPN12

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

Route Leak

BASIC CONFIGURATION

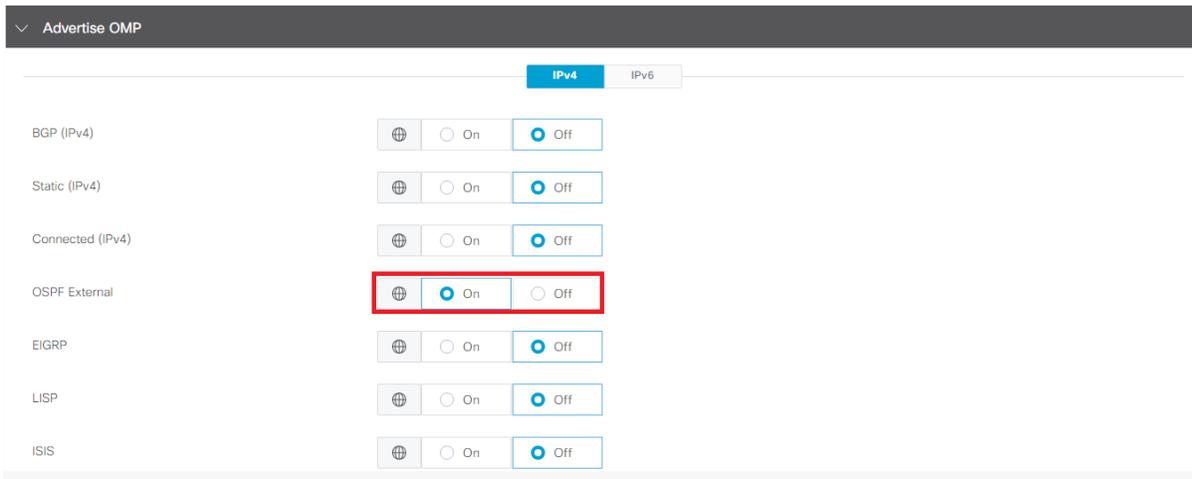
VPN 12

Name

Enhance ECMP Keying On Off

Cancel Save

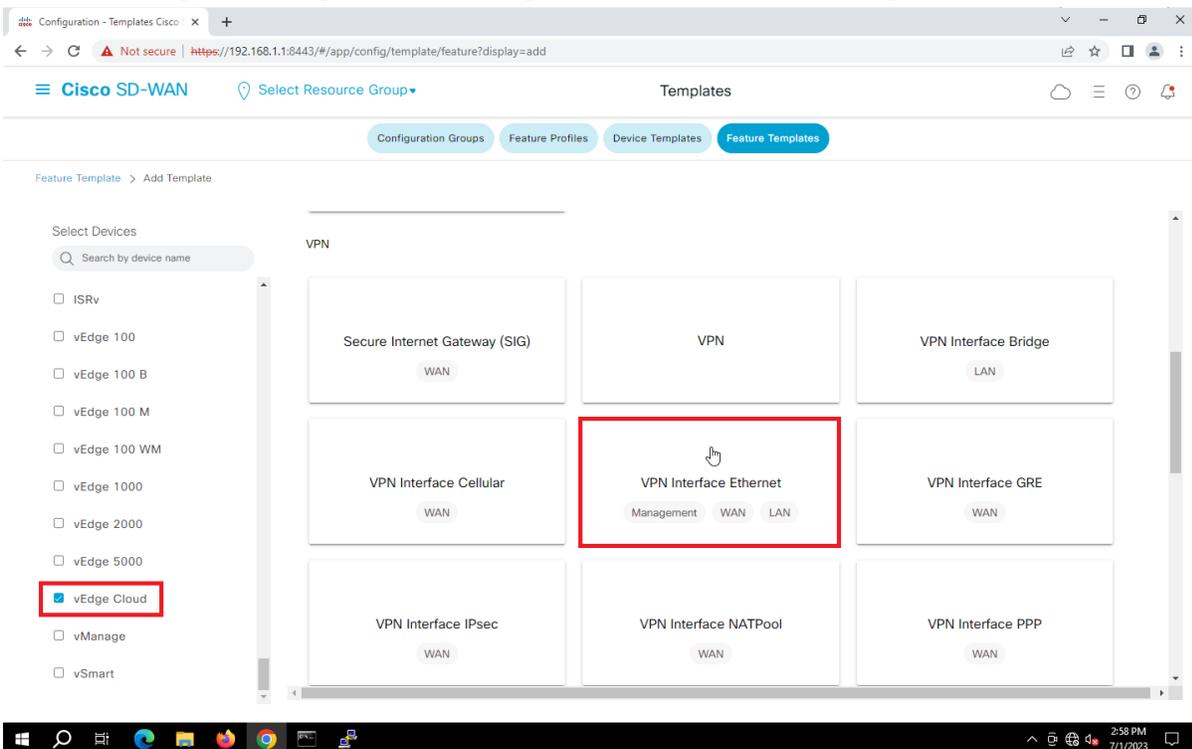
Sau đó, ở **Advertise OMP** thì ta chỉnh như sau:



Cuối cùng chọn **Save** để tạo được cái Feature Template đầu tiên

Tạo Feature Template: *vEdge_VPN12_GEO/3* (để cấu hình cổng ge0/3 cho VPN12)

Chọn **vManage** > **Configuration** > **Template** > **Feature** > **Add Template**.



Tạo template cho VPN 11 interface như bên dưới:

Select Devices: vEdge Cloud

Template: VPN/VPN Interface Ethernet

Template Name: *vEdge_VPN12_Ge0/3*

Description: *vEdge_VPN12_Ge0/3*

Configuration - Templates Cisco

Configuration Groups Feature Profiles Device Templates Feature Templates

Feature Template > Add Template > VPN Interface Ethernet

Device Type vEdge Cloud

Template Name* vEdge_VPN12_Ge0/3

Description* vEdge_VPN12_Ge0/3

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

BASIC CONFIGURATION

Shutdown Yes No

Interface Name

Description

IPv4 IPv6

Cancel Save

Configuration - Templates Cisco

Configuration Groups Feature Profiles Device Templates Feature Templates

Feature Template > Add Template > VPN Interface Ethernet

IPv4 IPv6

Dynamic Static

IPv4 Address

Secondary IP Address (Maximum: 4)

DHCP Helper

Block Non Source IP Yes No

Bandwidth Upstream

Bandwidth Downstream

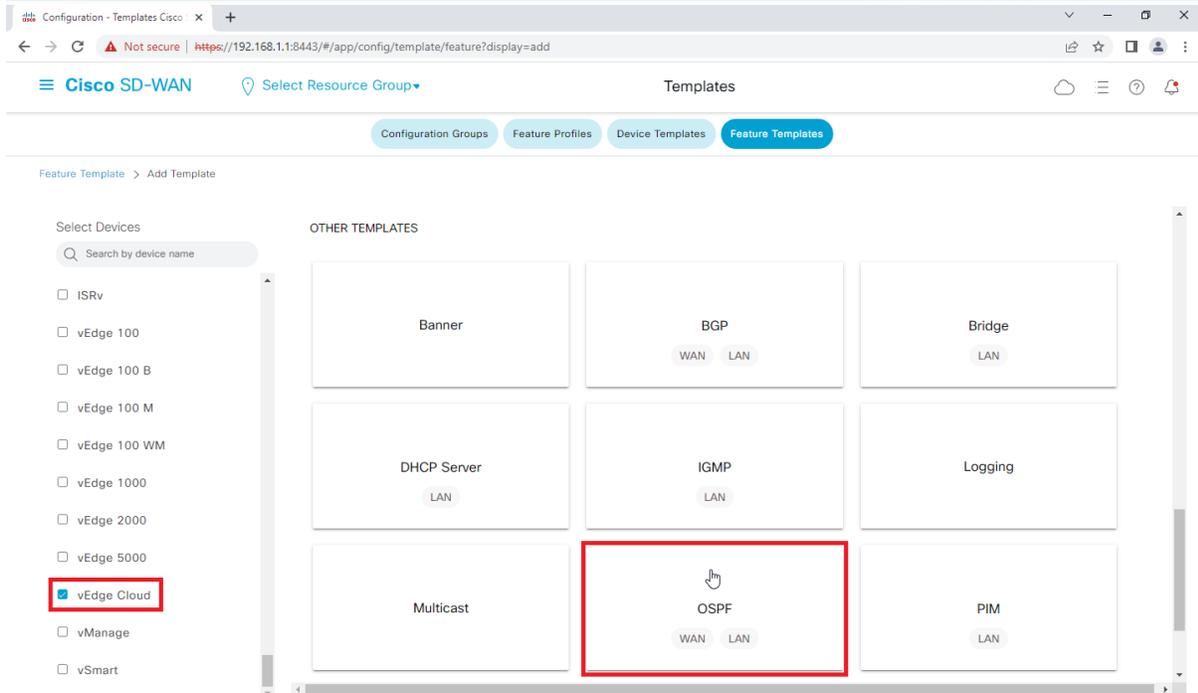
TUNNEL

Cancel Save

Chọn **Save** để tạo Template

Tạo Feature Template: vEdge_OSPF_VPN12 (để định tuyến cho VPN12)

Chọn **vManage > Configuration > Template > Feature > Add Template.**

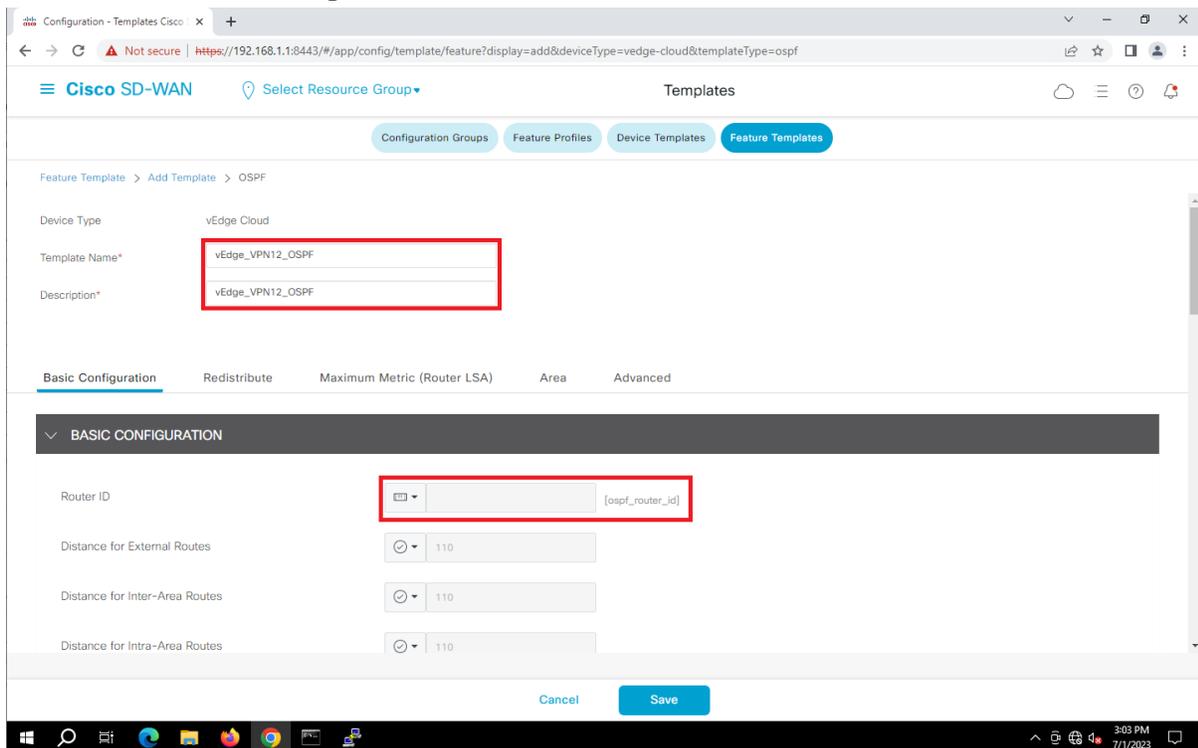


Sau đó cấu hình các thông số như hình sau:

Template Name: *vEdge_OSPF_VPN12*

Description: *vEdge_OSPF_VPN12*

Router ID chọn **Device Specific**



Tiếp theo đến phần REDISTRIBUTE ta chọn OMP

The screenshot shows the Cisco SD-WAN configuration interface. The breadcrumb trail is "Feature Template > Add Template > OSPF". Under the "REDISTRIBUTE" section, the "New Redistribute" button is highlighted with a red box. Below this, there is a table with columns "Optional", "Protocol", "Route Policy", and "Action", which currently contains no data. At the bottom of the page, there are "Cancel" and "Save" buttons.

The screenshot shows the Cisco SD-WAN configuration interface. The breadcrumb trail is "Feature Template > Add Template > OSPF". Under the "REDISTRIBUTE" section, the "New Redistribute" button is visible. The "Protocol" dropdown menu is set to "omp" and is highlighted with a red box. To the right, there is a checkbox labeled "Mark as Optional Row" which is unchecked. Below the "Protocol" field, there is a "Route Policy" dropdown menu. At the bottom right, the "Add" button is highlighted with a red box. Below the table, there are "Cancel" and "Save" buttons.

Tiếp tục đến phần AREA ta chọn number là 0 sau đó ta add interface

AREA

New Area

Optional	Number	Area Type	No Summary	Translate	Interface	Action
No data available						

AREA

New Area

Mark as Optional Row ⓘ

Area Number

Set the area type

Interface

Range

Interface

No OSPF Interfaces added, add your first OSPF Interface

Một cửa sổ hiện ra, ta chỉnh thông số như sau:

Interface Name: *ge0/3*

Và chọn add để thêm interface

Interface

Add Interface

ge0/3

Interface Name	<input type="text" value="ge0/3"/>
Hello Interval (seconds)	<input type="text" value="10"/>
Dead Interval (seconds)	<input type="text" value="40"/>
LSA Retransmission Interval (seconds)	<input type="text" value="5"/>
Interface Cost	<input type="text"/>
Advanced Options	>

Add Cancel

AREA

New Area

Mark as Optional Row

Area Number	<input type="text" value="0"/>
Set the area type	<input type="text"/>
Interface	1 Interface
Range	Add Range

Add Cancel

Cuối cùng ta chọn **Save** để tạo Template

3.2. Tạo một Device Template

Ở giao diện vManage, **Configuration > Templates** (tab Device).

Chọn **Create Template > From Feature Template**.

Chọn Device Model (vEdge Cloud).

Configuration - Templates Cisco

Not secure | https://192.168.1.1:8443/#/app/config/template/device

Cisco SD-WAN Select Resource Group Templates

Configuration Groups Feature Profiles **Device Templates** Feature Templates

Search

Create Template

- From Feature Template
- CLI Template

Total Rows: 2

Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated
vSmar...	vSmart_Template	Feature	vSmart	SDWAN Edge	global	9	Disabled	1	admin	01 Jul 2023 10:0...
vEdge...	vEdge_OSPF	Feature	vEdge Cloud	SDWAN Edge	global	14	Disabled	3	admin	01 Jul 2023 11:0...

Nhập Template Name (vEdge_VPN12), Description (vEdge_VPN12).

Configuration - Templates Cisco

Not secure | https://192.168.1.1:8443/#/app/config/template/device/feature

Cisco SD-WAN Select Resource Group Templates

Configuration Groups Feature Profiles **Device Templates** Feature Templates

Device Model* vEdge Cloud

Device Role* SDWAN Edge

Template Name* vEdge_VPN12

Description* vEdge_VPN12

Basic Information Transport & Management VPN Service VPN Additional Templates

Basic Information

System * Factory_Default_vEdge_System_Templ...

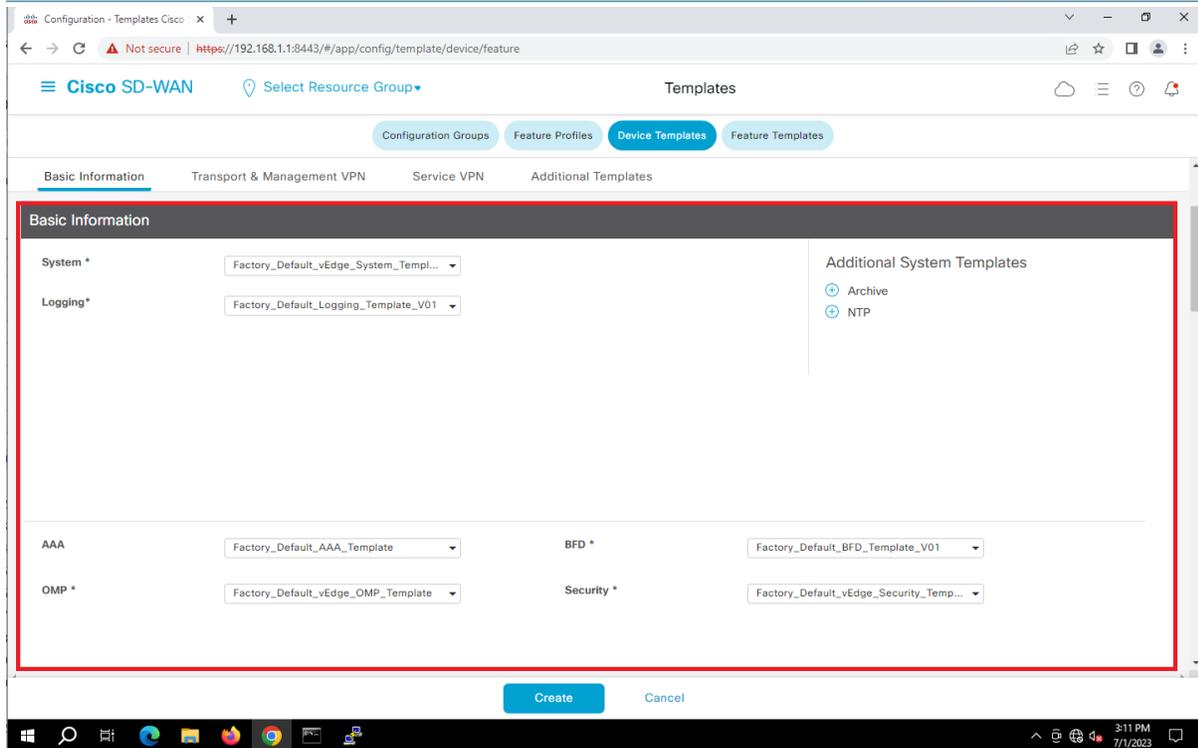
Logging * Factory_Default_Logging_Template_V01

Additional System Templates

- Archive
- NTP

Create Cancel

Trong phần Basic Information thì để mặc định nếu có những template tương ứng thì có thể chọn vào.



The screenshot shows the Cisco SD-WAN configuration interface. The browser address bar indicates the URL is <https://192.168.1.1:8443/#/app/config/template/device/feature>. The interface includes a navigation menu with 'Cisco SD-WAN' and 'Select Resource Group'. The main content area is titled 'Templates' and has tabs for 'Configuration Groups', 'Feature Profiles', 'Device Templates', and 'Feature Templates'. The 'Device Templates' tab is selected, and the 'Basic Information' sub-tab is active. The 'Basic Information' section contains several dropdown menus for selecting templates: 'System *' (Factory_Default_vEdge_System_Templ...), 'Logging*' (Factory_Default_Logging_Template_V01), 'AAA' (Factory_Default_AAA_Template), 'OMP *' (Factory_Default_vEdge_OMP_Template), 'BFD *' (Factory_Default_BFD_Template_V01), and 'Security *' (Factory_Default_vEdge_Security_Temp...). An 'Additional System Templates' section on the right lists 'Archive' and 'NTP'. At the bottom of the form are 'Create' and 'Cancel' buttons. The Windows taskbar at the bottom shows the time as 3:11 PM on 7/1/2023.

Đối với phần Transport & Management VPN, ta chọn lần lượt các Feature Template cũ sau:

VPN0: *vEdge_VPN0*

VPN Interface: *vEdge_VPN0_GE0/0*

VPN Interface: *vEdge_VPN0_GE0/1*

VPN512: *vEdge_VPN512*

VPN Interface: *vEdge_VPN_eth0*

Configuration - Templates Cisco

Not secure | <https://192.168.1.1:8443/#/app/config/template/device/feature>

Cisco SD-WAN Select Resource Group

Templates

Configuration Groups Feature Profiles Device Templates Feature Templates

Transport & Management VPN

VPN 0 *
vEdge_VPN0

VPN Interface
vEdge_VPN0_Ge0/0_Internet

VPN Interface
vEdge_VPN0_Ge0/1_MPLS

Additional VPN 0 Templates

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

VPN 512 *
vEdge_VPN512

VPN Interface
vEdge_VPN512_eth0

Additional VPN 512 Templates

- VPN Interface**

Service VPN

Create Cancel

Ở Service VPN, ta lần lượt chọn các template tương ứng với các mục như sau:

VPN: *vEdge_VPN11*

OSPF: *vEdge_OSPF*

VPN Interface: *vEdge_VPN11_GE0/2*

Configuration - Templates Cisco

Not secure | <https://192.168.1.1:8443/#/app/config/template/device/feature>

Cisco SD-WAN Select Resource Group

Templates

Configuration Groups Feature Profiles Device Templates Feature Templates

Service VPN

Search

0 Rows Selected Add VPN Remove VPN

Total Rows: 0

ID	Template Name	Sub-Templates
No data available		

Additional Templates

Banner Choose...

Create Cancel

Add VPN

Select VPNs Select Sub-Templates

Select one or more Service VPNs to add: 0 Items Selected

Available VPN Templates Select All

Search

ID	Template Name
743fa765-96e4-4de1-86bb-e1759... vEdge_VPN11	
cf833a8-0eb7-45da-a26b-ef8093... vEdge_VPN12	

Selected VPN Templates

Search

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

Next

Add VPN

Select VPNs Select Sub-Templates

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

Additional VPN Templates

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

Add

Add VPN

Select VPNs Select Sub-Templates

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

OSPF	<input type="text" value="vEdge_OSPF"/>	
VPN Interface	<input type="text" value="vEdge_VPN11_Ge0/2"/>	<input type="button" value="+ Sub-Templates"/>

Additional VPN Templates

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

Tương tự cho cổng GE0/3

VPN: *vEdge_VPN12*

OSPF: *vEdge_OSPF_VPN12*

VPN Interface: *vEdge_VPN12_GE0/3*

Add VPN

Select VPNs Select Sub-Templates

Select one or more Service VPNs to add: 0 Items Selected

Available VPN Templates		Selected VPN Templates	
ID	Template Name	ID	Template Name
<input type="text" value="Search"/> <input type="button" value="Filter"/>		<input type="text" value="Search"/> <input type="button" value="Filter"/>	
cff833a8-0eb7-45da-a26b-ef8093... vEdge_VPN12			

Add VPN

Select VPNs Select Sub-Templates

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

Additional VPN Templates	
<input type="button" value="+"/>	BGP
<input type="button" value="+"/>	IGMP
<input type="button" value="+"/>	Multicast
<input checked="" type="button" value="+"/>	OSPF
<input type="button" value="+"/>	PIM
<input checked="" type="button" value="+"/>	VPN Interface
<input type="button" value="+"/>	VPN Interface Bridge
<input type="button" value="+"/>	VPN Interface GRE
<input type="button" value="+"/>	VPN Interface IPsec
<input type="button" value="+"/>	VPN Interface Natpool

Add VPN

Select VPNs Select Sub-Templates

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

OSPF

VPN Interface

Additional VPN Templates

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

Configuration - Templates Cisco

Not secure | https://192.168.1.18443/#/app/config/template/device/feature

Cisco SD-WAN Select Resource Group Templates

Configuration Groups Feature Profiles **Device Templates** Feature Templates

Service VPN

Search

0 Rows Selected Total Rows: 2

ID	Template Name	Sub-Templates
<input type="checkbox"/> 743fa765-96e4-4de1-86bb-e1759aa4a0cf	vEdge_VPN11	OSPF, VPN Interface
<input type="checkbox"/> cff833a8-0eb7-45da-a26b-ef8093a7b05f	vEdge_VPN12	OSPF, VPN Interface

Additional Templates

Banner

Policy

Chọn **Create** để hoàn thành **Device Template**

Tiến hành cấu hình thiết bị vEdge bằng cách **Attach Devices**

The screenshot shows the Cisco SD-WAN configuration interface. The 'Device Templates' tab is active. A table lists templates, with 'vEdge_VPN12' highlighted. A context menu is open over this row, with 'Attach Devices' selected.

Name	Description	Type	Device Mode	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated
vSmar...	vSmart_Template	Feature	vSmart	SDWAN Edge	global	9	Disabled	1	admin	01 Jul 2023 1
vEdge...	vEdge_OSPF	Feature	vEdge Cloud	SDWAN Edge	global	14	Disabled	3	admin	01 Jul 2023 1
vEdge...	vEdge_VPN12	Feature	vEdge Cloud	SDWAN Edge	global	17	Disabled	0	admin	01 Jul 2023 4

Chọn thiết bị vEdge ở ba site: SITE1, SITE2, SITE3.

The 'Attach Devices' dialog box is shown. It has two panes: 'Available Devices' and 'Selected Devices'. In the 'Available Devices' pane, three devices are selected: vEdge-Site1 (2.1.1.1), vEdge-Site2 (3.1.1.1), and vEdge-Site3 (4.1.1.1). The 'Attach' button is highlighted.

Name	Device IP
be5ba729-6684-943c-1e91-7d6ff296e97b	
ecf8966f-55f0-b701-b9df-717fe3ca0fd0	
f121e275-5c29-cbce-71c1-783ee2126db4	
80060207-b2bd-a5fa-691f-72386930a34e	
84c6527e-45e6-c5a8-c33c-fff9d8ad42a4	
vEdge-Site1	2.1.1.1
vEdge-Site2	3.1.1.1
vEdge-Site3	4.1.1.1
vbond	1.1.1.2

Chọn **Attach**

Các thông số cấu hình cho thiết bị vEdge ở Site1 như sau:

S...	Chassis Number	System IP	Hostname	IPv4 Address(vpn12_ge0/3_if_ipv4_address)	Router ID(ospf_router_id)	IPv4 Address(v
0	0b0f3c75-47c5-5e73-a557-9cf97c754274	2.1.1.1	vEdge-Site1			192.168.10.254 ...
5	5316bef9-7742-d0c9-1048-df6288bb4e...	4.1.1.1	vEdge-Site3			192.168.30.254 ...
1	168a2add-2c4f-fcb1-6139-1d99df86e22e	3.1.1.1	vEdge-Site2			192.168.20.254 ...

Update Device Template

Variable List (Hover over each field for more information)

Status	in_complete
Chassis Number	0b0f3c75-47c5-5e73-a557-9cf97c754274
System IP	2.1.1.1
Hostname	vEdge-Site1
IPv4 Address(vpn12_ge0/3_if_ipv4_address)	192.168.11.254/24
Router ID(ospf_router_id)	2.1.1.1
IPv4 Address(vpn11_ge0/2_if_ipv4_address)	192.168.10.254/24
Router ID(ospf_router_id)	2.1.1.1
Address(vpn0_Internet_next_hop_ip_address_1)	200.200.1.1
IPv4 Address(vpn0_ge0/1_MPLS_if_ipv4_address)	172.16.1.1/24
IPv4 Address(vpn0_ge0/0_Internet_if_ipv4_address)	200.200.1.2/30
Hostname	vEdge-Site1
System IP	2.1.1.1

Buttons: Generate Password, Update, Cancel

Site2:

Configuration - Templates Cisco

Not secure | <https://192.168.1.1:8443/#/app/config/template/device/configure/de9192ba-ceac-4725-ac86-a5456ecc4de4>

Cisco SD-WAN | Select Resource Group | Templates

Update Device Template

Variable List (Hover over each field for more information)

Status	in_complete
Chassis Number	168a2add-2c4f-fcb1-6139-1d99df86e22e
System IP	3.1.1.1
Hostname	vEdge-Site2
IPv4 Address(vpn12_ge0/3_if_ipv4_address)	192.168.21.254/24
Router ID(ospf_router_id)	3.1.1.1
IPv4 Address(vpn11_ge0/2_if_ipv4_address)	192.168.20.254/24
Router ID(ospf_router_id)	3.1.1.1
Address(vpn0_Internet_next_hop_ip_address_1)	200.200.2.1
IPv4 Address(vpn0_ge0/1_MPLS_if_ipv4_address)	172.16.1.2/24
IPv4 Address(vpn0_ge0/0_Internet_if_ipv4_address)	200.200.2.2/30
Hostname	vEdge-Site2
System IP	3.1.1.1

Buttons: Generate Password, Update, Cancel

Site3:

Configuration - Templates Cisco

Not secure | <https://192.168.1.1:8443/#/app/config/template/device/configure/de9192ba-ceac-4725-ac86-a5456ecc4de4>

Cisco SD-WAN | Select Resource Group | Templates

Update Device Template

Variable List (Hover over each field for more information)

Status	in_complete
Chassis Number	5316bef9-7742-d0c9-1048-df6288bb4e56
System IP	4.1.1.1
Hostname	vEdge-Site3
IPv4 Address(vpn12_ge0/3_if_ipv4_address)	192.168.31.254/24
Router ID(ospf_router_id)	4.1.1.1
IPv4 Address(vpn11_ge0/2_if_ipv4_address)	192.168.30.254/24
Router ID(ospf_router_id)	4.1.1.1
Address(vpn0_Internet_next_hop_ip_address_1)	200.200.3.1
IPv4 Address(vpn0_ge0/1_MPLS_if_ipv4_address)	172.16.1.3/24
IPv4 Address(vpn0_ge0/0_Internet_if_ipv4_address)	200.200.3.2/30
Hostname	vEdge-Site3
System IP	4.1.1.1

Buttons: Generate Password, Update, Cancel

Chọn Update > Next > Configure Device

Configuration - Templates Cisco

Not secure | https://192.168.1.1:8443/#/app/config/template/device/configure/de9192ba-ceac-4725-ac86-a5456ecc4de4

Cisco SD-WAN Select Resource Group Templates

Device Template | vEdge_VPN12

Search

Total Rows: 3

S...	Chassis Number	System IP	Hostname	IPv4 Address(vpn12_ge0/3_if_ipv4_address)	Router ID(ospf_router_id)	IPv4 Address(v
✓	0b0f3c75-47c5-5e73-a557-9cf97c754274	2.1.1.1	vEdge-Site1	192.168.11.254/24	2.1.1.1	192.168.10.254 ...
✓	5316bef9-7742-d0c9-1048-df6288bb4e...	4.1.1.1	vEdge-Site3	192.168.31.254/24	4.1.1.1	192.168.30.254 ...
✓	168a2add-2c4f-fcb1-6139-1d99df86e22e	3.1.1.1	vEdge-Site2	192.168.21.254/24	3.1.1.1	192.168.20.254 ...

Next Cancel

Configuration - Templates Cisco

Not secure | https://192.168.1.1:8443/#/app/config/template/device/configure/preview/de9192ba-ceac-4725-ac86-a5456ecc4de4

Cisco SD-WAN Select Resource Group Templates

Device Template | vEdge_VPN12

Total | 1

Device list (Total: 3 devices)

Filter/Search

0b0f3c75-47c5-5e73-a557-9cf97c754274 vEdge-Site1 2.1.1.1
5316bef9-7742-d0c9-1048-df6288bb4e56 vEdge-Site3 4.1.1.1
168a2add-2c4f-fcb1-6139-1d99df86e22e vEdge-Site2 3.1.1.1

Configure Device Rollback Timer

Please select a device from the device list

Back Configure Devices Cancel

Configure Devices

Committing these changes affect the configuration on 3 devices. Are you sure you want to proceed?

Confirm configuration changes on 3 devices.

OK

Cancel

Configuration - Templates Cisco

Not secure | https://192.168.1.1:8443/#/app/device/status?activity=push_file_template_configuration&pid=push_feature_template_configuration-0ae80cc2-bcd3-4c06-a700-1a6a6...

Cisco SD-WAN Select Resource Group

Push Feature Template Configuration | Validation Success Initiated By: admin From: 192.168.1.200

Total Task: 3 | Success : 3

Search

Total Rows: 3

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature T...	0b0f3c75-47c5-5e73...	vEdge Cloud	vEdge-Site1	2.1.1.1	1	1.1.1.1
Success	Done - Push Feature T...	168a2add-2c4f-fcb1-...	vEdge Cloud	vEdge-Site2	3.1.1.1	2	1.1.1.1
Success	Done - Push Feature T...	5316bef9-7742-d0c9...	vEdge Cloud	vEdge-Site3	4.1.1.1	3	1.1.1.1

3:34 PM 7/1/2023

Tiến hành cấu hình cho thiết bị Router ở 3 site ở VPN12

R-Site1-1: ở site 1

```
ena
```

```
conf t
```

```
hostname R-Site1-1
```

```
router ospf 1
```

```
exit
```

```
int e0/0
```

```
ip add 192.168.10.2 255.255.255.0
ip ospf 1 area 0
no shut
exit
int e0/1
ip add 10.10.10.1 255.255.255.0
ip ospf 1 area 0
no shut
exit
ip route 0.0.0.0 0.0.0.0 192.168.10.254
do wr
```

R-Site1-2: ở site1

```
ena
conf t
hostname R-Site1-2
router ospf 1
exit
int e0/0
ip add 192.168.11.2 255.255.255.0
ip ospf 1 area 0
no shut
exit
int e0/1
ip add 10.10.11.1 255.255.255.0
ip ospf 1 area 0
no shut
exit
ip route 0.0.0.0 0.0.0.0 192.168.11.254
do wr
```

R-Site2-1: ở site2

```
ena
conf t
hostname R-Site2-1
router ospf 1
exit
int e0/0
```

```
ip add 192.168.20.2 255.255.255.0
ip ospf 1 area 0
no shut
exit
int e0/1
ip add 10.10.20.1 255.255.255.0
ip ospf 1 area 0
no shut
exit
ip route 0.0.0.0 0.0.0.0 192.168.20.254
do wr
```

R-Site2-2: ở site2

```
ena
conf t
hostname R-Site2-2
router ospf 1
exit
int e0/0
ip add 192.168.21.2 255.255.255.0
ip ospf 1 area 0
no shut
exit
int e0/1
ip add 10.10.21.1 255.255.255.0
ip ospf 1 area 0
no shut
exit
ip route 0.0.0.0 0.0.0.0 192.168.21.254
do wr
```

R-Site3-1: ở site3

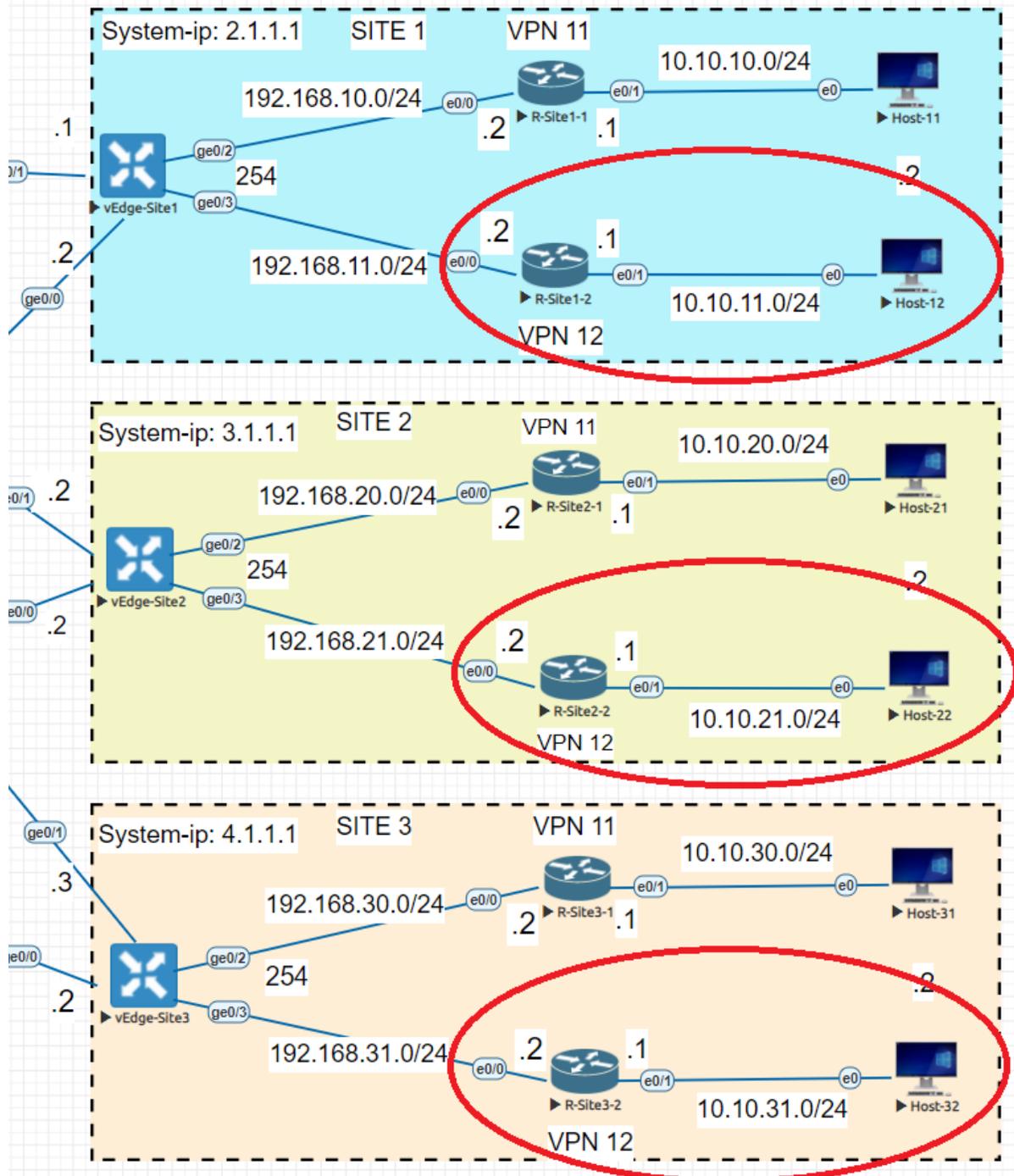
```
ena
conf t
hostname R-Site3-1
router ospf 1
exit
int e0/0
```

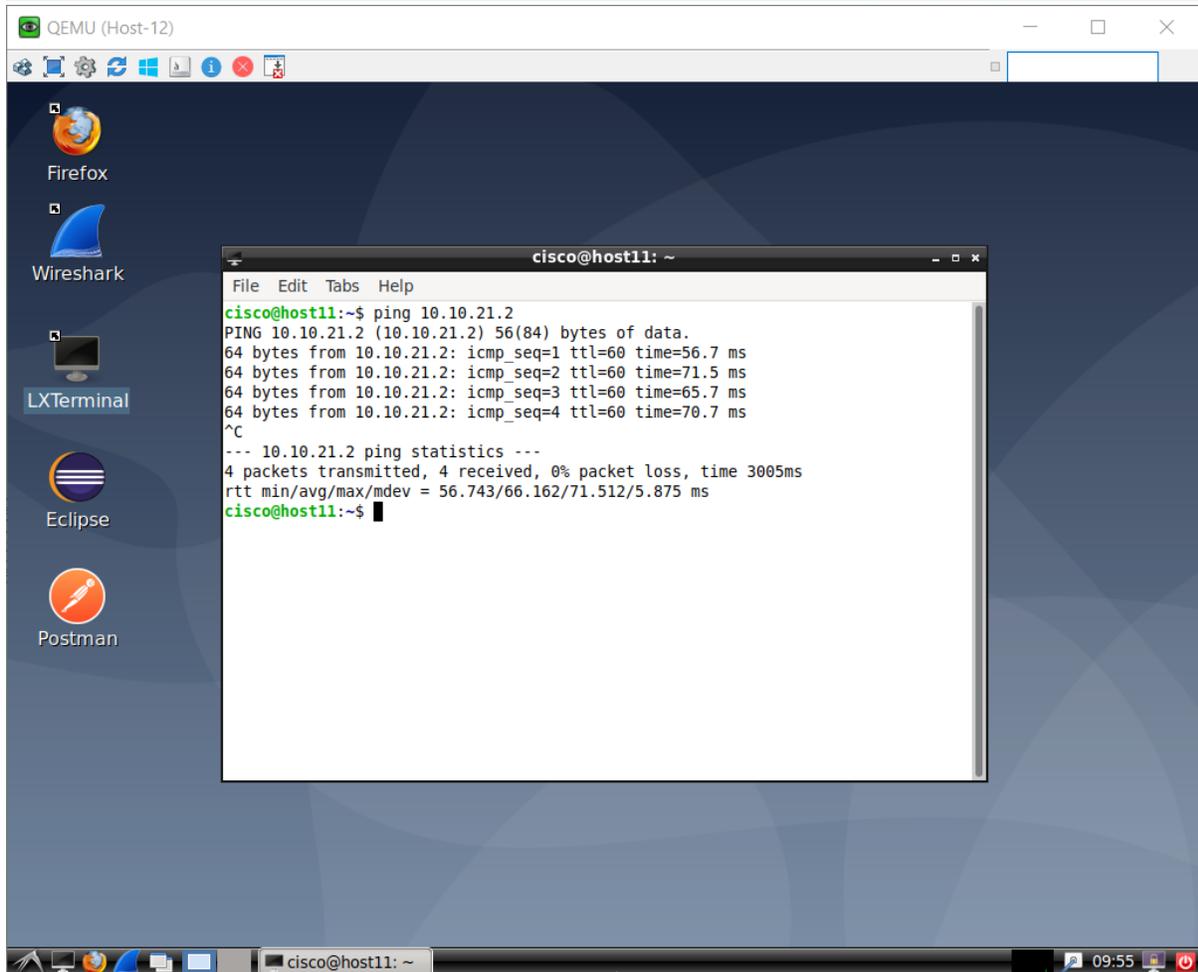
```
ip add 192.168.30.2 255.255.255.0
ip ospf 1 area 0
no shut
exit
int e0/1
ip add 10.10.30.1 255.255.255.0
ip ospf 1 area 0
no shut
exit
ip route 0.0.0.0 0.0.0.0 192.168.30.254
do wr
```

R-Site3-2: ở site3

```
ena
conf t
hostname R-Site3-2
router ospf 1
exit
int e0/0
ip add 192.168.31.2 255.255.255.0
ip ospf 1 area 0
no shut
exit
int e0/1
ip add 10.10.31.1 255.255.255.0
ip ospf 1 area 0
no shut
exit
ip route 0.0.0.0 0.0.0.0 192.168.31.254
do wr
```

Thực hiện lệnh Ping từ **Host-12** ở site1 của VPN12 sang **Host-22** ở site2 của VPN12 thì thấy ping thành công



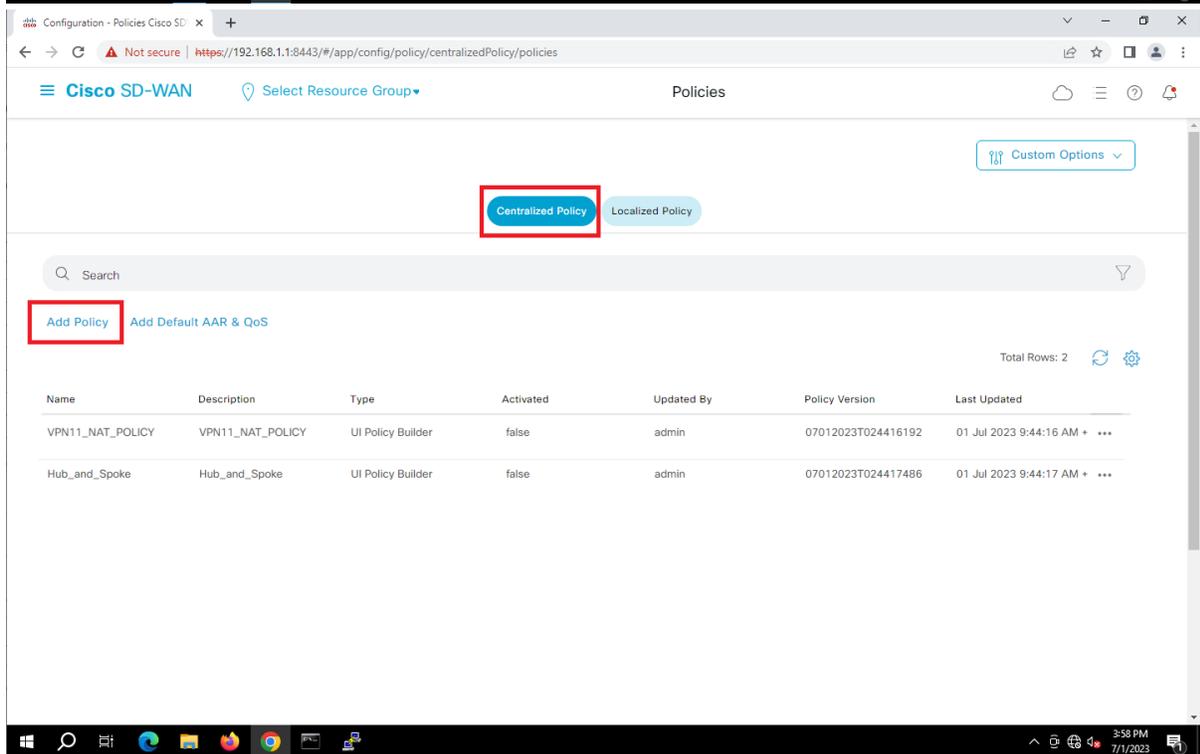
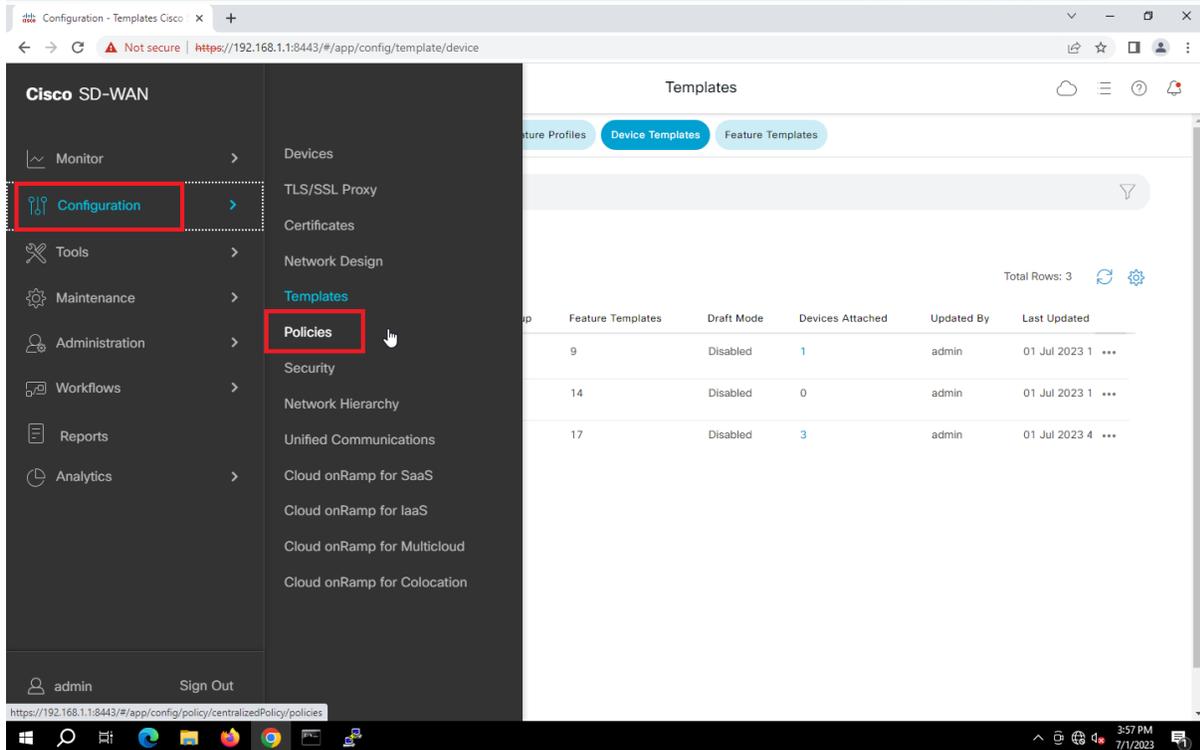


The screenshot shows a QEMU virtual machine desktop environment. The desktop background is dark blue with a grid pattern. On the left side, there is a dock with icons for Firefox, Wireshark, LXTerminal, Eclipse, and Postman. A terminal window titled 'cisco@host11: ~' is open in the center, displaying the following output:

```
cisco@host11:~$ ping 10.10.21.2
PING 10.10.21.2 (10.10.21.2) 56(84) bytes of data:
64 bytes from 10.10.21.2: icmp_seq=1 ttl=60 time=56.7 ms
64 bytes from 10.10.21.2: icmp_seq=2 ttl=60 time=71.5 ms
64 bytes from 10.10.21.2: icmp_seq=3 ttl=60 time=65.7 ms
64 bytes from 10.10.21.2: icmp_seq=4 ttl=60 time=70.7 ms
^C
--- 10.10.21.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 56.743/66.162/71.512/5.875 ms
cisco@host11:~$
```

3.3. Viết Centralized Policy để cô lập VPN12 không cho giao tiếp được giữa các site.

Vào giao diện vManage > **Configuration** > **Policies** > **Centralized Policy** > **Add Policy**



Sau đó ta vào **Site > New Site List** để thêm lần lượt ba site

Configuration - Policies Cisco SD-WAN

Centralized Policy > Add Policy

Create Groups of Interest | Configure Topology and VPN Membership | Configure Traffic Rules | Apply Policies to Sites and VPNs

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

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN
Region
Preferred Color Group

New Site List

Name	Entries	Reference Count	Updated By	Last Updated	Action
Site1	1	3	admin	01 Jul 2023 9:44:09 AM ...	
Site2	2	2	admin	01 Jul 2023 9:44:09 AM ...	
Site3	3	3	admin	01 Jul 2023 9:44:10 AM ...	

Next Cancel

3:58 PM 7/1/2023

Bước tiếp theo chọn VPN > New VPN List để tạo vpn11

Monitor - VPN Cisco SD-WAN

Centralized Policy > Add Policy

Create Groups of Interest | Configure Topology and VPN Membership | Configure Traffic Rules | Apply Policies to Sites and VPNs

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

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN
Region
Preferred Color Group

New VPN List

Name	Entries	Reference Count	Updated By	Last Updated	Action
VPN11	11	3	admin	01 Jul 2023 9:44:10 AM ...	

Next Cancel

3:59 PM 7/1/2023

Sau khi đã tạo xong các Site và VPN11 thì ta chọn Next để qua bước tiếp theo
Tiếp theo xuất hiện giao diện sau, ta chọn VPN Membership > Add VPN Membership

The screenshot shows the Cisco SD-WAN configuration page for adding a policy. The breadcrumb is "Centralized Policy > Add Policy". The progress bar indicates the current step is "Configure Topology and VPN Membership". Under "Specify your network topology", the "Topology" dropdown is set to "VPN Membership". A search bar is present. Below it, a dropdown menu "Add VPN Membership Policy" is open, showing options "Create New" and "Import Existing VPN Membership". A table with columns "Name", "Type", "Description", "Mode", "Reference Count", "Updated By", and "Last Updated" is shown below, with "Total Rows: 0". At the bottom, there are "Back", "Next", and "Cancel" buttons.

Cấu hình lần lượt các thông số như sau:

VPN Membership Name: *VPN11*

Description: *VPN11*

Site List: *site1, site2, site3*

VPN Lists: *vpn11*

Chọn **Save** để lưu policy

Centralized Policy > Add Policy

Create Groups of Interest

Specify your network topology

Topology VPN Membership

Search

Add VPN Membership Policy (Choose and add VPNs to specific site lists)

Name Type

VPN Membership Name* VPN11

Description* VPN11

Site List* VPN Lists*

Site1	VPN11 x
Site2	VPN11 x
Site3	VPN11 x

Add List

Cancel Save

Chọn Next > Next để tới bước cuối cùng là tạo tên cho policy

Centralized Policy > Add Policy

Create Groups of Interest

Configure Topology and VPN Membership

Specify your network topology

Topology VPN Membership

Search

Add VPN Membership Policy (Choose and add VPNs to specific site lists)

Total Rows: 1

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
VPN11	VPN Membership	VPN11	created	0	admin	01 Jul 2023 5:02:43 PM +...

Back

Next Cancel

Monitor - VPN Cisco SDWAN

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*

Policy Description*

VPN11

Site List	VPN List
Site1	VPN11
Site2	VPN11
Site3	VPN11

Back Preview **Save Policy** Cancel

Chọn Save Policy

Bước cuối cùng ta kích hoạt policy vừa tạo đến các vEdge ở ba site

Tìm policy vừa tạo *User_Guest_VPN12*, chọn **Activate** để kích hoạt

Monitor - VPN Cisco SDWAN

Centralized Policy Localized Policy

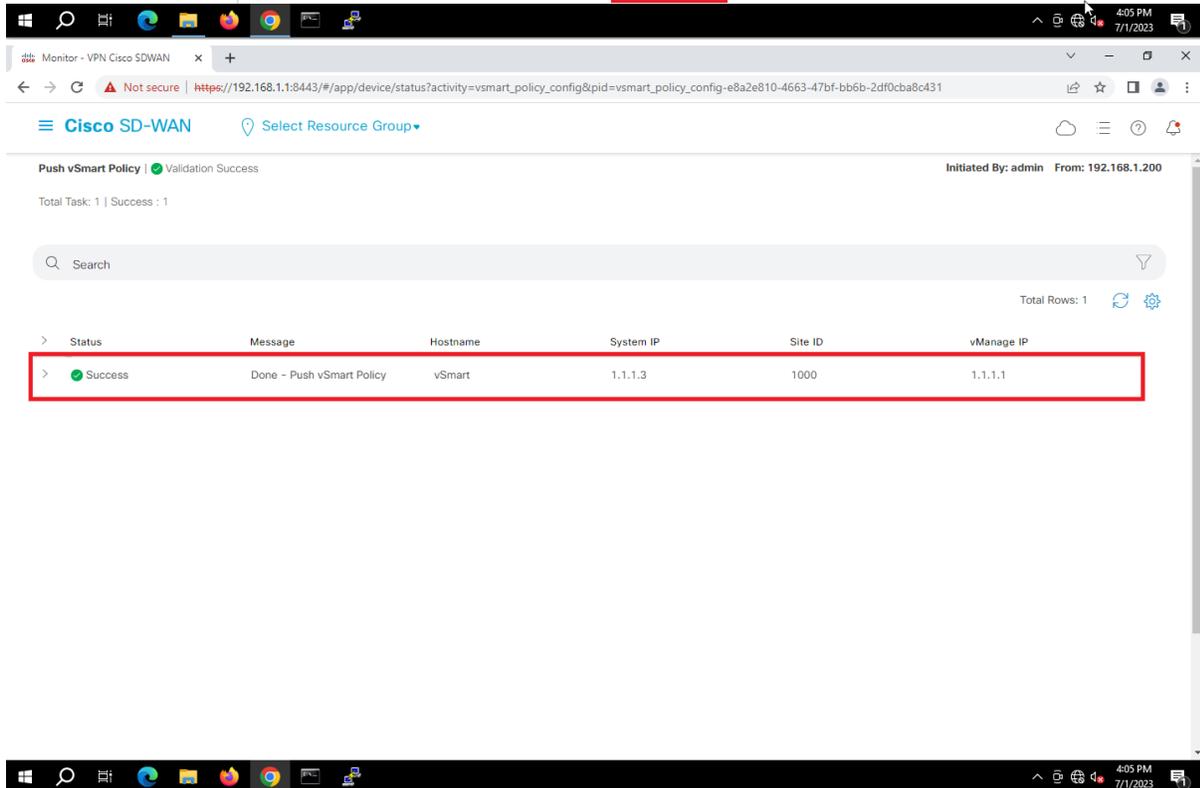
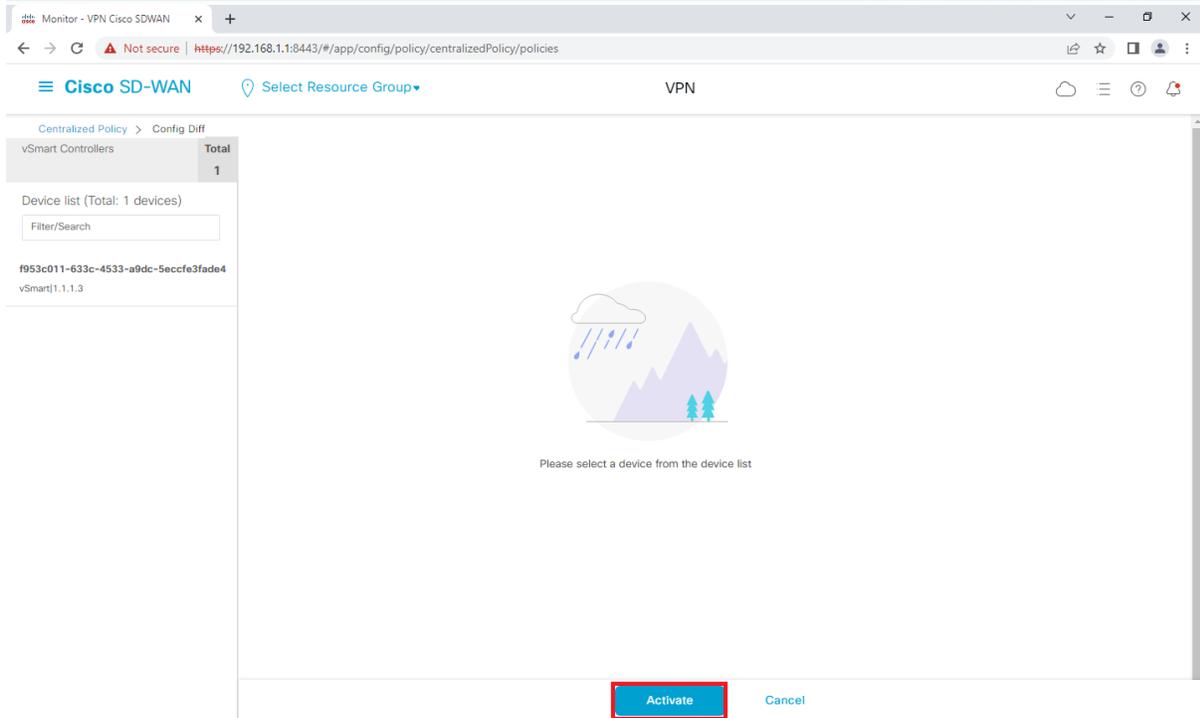
Search

Add Policy Add Default AAR & QoS

Total Rows: 3

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
User_Guest_VPN12	User_Guest_VPN12	UI Policy Builder	false	admin	07012023T100427198	01 Jul 2023 5:04:27 PM + ⋮
VPN11_NAT_POLICY	VPN11_NAT_POLICY	UI Policy Builder	false	admin	07012023T024416192	01 Jul 2023 9:44:1
Hub_and_Spoke	Hub_and_Spoke	UI Policy Builder	false	admin	07012023T024417486	01 Jul 2023 9:44:1

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



IV. Kiểm tra

Kiểm tra trên thiết bị vEdge ở ba site bằng lệnh **show ip routes**

vEdge SITE1 thì ta không thấy các route của VPN12 từ SITE2 và SITE3

```
vEdge-Site1# show ip routes
Codes Proto-sub-Type:
  IA -> ospf-intra-area, IE -> ospf-internal-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nsa-external1, N2 -> ospf-nsa-external2,
  S -> bgp-external, I -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

VPN	PREFIX	PROTOCOL	SUB TYPE	IF NAME	NEXTHOP ADDR	VPN	TLOC IP	COLOR	ENCAP	S
0	0.0.0.0/0	static	-	ge0/0	200.200.1.1	-	-	-	-	F
0	2.1.1.1/32	connected	-	system	-	-	-	-	-	F
0	10.1.1.0/24	static	-	ge0/1	172.16.1.254	-	-	-	-	F
0	172.16.1.0/24	connected	-	ge0/1	-	-	-	-	-	F
0	200.200.1.0/30	connected	-	ge0/0	-	-	-	-	-	F
11	10.10.10.0/24	ospf	IA	ge0/2	192.168.10.2	-	-	-	-	F
11	10.10.20.0/24	omp	-	-	-	-	3.1.1.1	mpls	ipsec	F
11	10.10.20.0/24	omp	-	-	-	-	3.1.1.1	biz-internet	ipsec	F
11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	mpls	ipsec	F
11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	biz-internet	ipsec	F

```
vEdge-Site1#
```

11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	mpls	ipsec	F
11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	biz-internet	ipsec	F
11	192.168.10.0/24	ospf	IA	ge0/2	-	-	-	-	-	-
11	192.168.10.0/24	connected	-	ge0/2	-	-	-	-	-	F
11	192.168.20.0/24	omp	-	-	-	-	3.1.1.1	mpls	ipsec	F
11	192.168.20.0/24	omp	-	-	-	-	3.1.1.1	biz-internet	ipsec	F
11	192.168.30.0/24	omp	-	-	-	-	4.1.1.1	mpls	ipsec	F
11	192.168.30.0/24	omp	-	-	-	-	4.1.1.1	biz-internet	ipsec	F
12	10.10.11.0/24	ospf	IA	ge0/3	192.168.11.2	-	-	-	-	F
12	192.168.11.0/24	ospf	IA	ge0/3	-	-	-	-	-	-
12	192.168.11.0/24	connected	-	ge0/3	-	-	-	-	-	F
65528	0.0.0.0/0	nat	-	ge0/0	-	0	-	-	-	F
65528	192.168.0.0/24	connected	-	loopback65528-	-	-	-	-	-	-
65530	0.0.0.0/0	nat	-	ge0/0	-	0	-	-	-	F
65530	192.168.0.0/24	connected	-	loopback65530-	-	-	-	-	-	-
65530	192.168.1.0/24	connected	-	loopback65531-	-	-	-	-	-	-

vEdge SITE2 thì ta không thấy các route của VPN12 từ SITE1 và SITE3

```
vEdge-Site2# show ip routes
Codes Proto-sub-Type:
  IA -> ospf-intra-area, IE -> ospf-internal,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

VPN	PREFIX	PROTOCOL	SUB TYPE	IF NAME	ADDR	VPN	TLOC IP	COLOR	ENCAP	S
0	0.0.0.0/0	static	-	ge0/0	200.200.2.1	-	-	-	-	F
0	3.1.1.1/32	connected	-	system	-	-	-	-	-	F
0	10.1.1.0/24	static	-	ge0/1	172.16.1.254	-	-	-	-	F
0	172.16.1.0/24	connected	-	ge0/1	-	-	-	-	-	F
0	200.200.2.0/30	connected	-	ge0/0	-	-	-	-	-	F
11	10.10.10.0/24	omp	-	-	-	-	2.1.1.1	mpls	ipsec	F
11	10.10.10.0/24	omp	-	-	-	-	2.1.1.1	biz-internet	ipsec	F
11	10.10.20.0/24	ospf	IA	ge0/2	192.168.20.2	-	-	-	-	F
11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	mpls	ipsec	F
11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	biz-internet	ipsec	F

```
vEdge-Site2# show ip routes
Codes Proto-sub-Type:
  IA -> ospf-intra-area, IE -> ospf-internal,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

VPN	PREFIX	PROTOCOL	SUB TYPE	IF NAME	ADDR	VPN	TLOC IP	COLOR	ENCAP	S
11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	mpls	ipsec	F
11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	biz-internet	ipsec	F
11	10.10.30.0/24	omp	-	-	-	-	4.1.1.1	biz-internet	ipsec	F
11	192.168.10.0/24	omp	-	-	-	-	2.1.1.1	mpls	ipsec	F
11	192.168.10.0/24	omp	-	-	-	-	2.1.1.1	biz-internet	ipsec	F
11	192.168.20.0/24	ospf	IA	ge0/2	-	-	-	-	-	F
11	192.168.20.0/24	connected	-	ge0/2	-	-	-	-	-	F
11	192.168.30.0/24	omp	-	-	-	-	4.1.1.1	mpls	ipsec	F
11	192.168.30.0/24	omp	-	-	-	-	4.1.1.1	biz-internet	ipsec	F
12	10.10.21.0/24	ospf	IA	ge0/3	192.168.21.2	-	-	-	-	F
12	192.168.21.0/24	ospf	IA	ge0/3	-	-	-	-	-	F
12	192.168.21.0/24	connected	-	ge0/3	-	-	-	-	-	F
65528	0.0.0.0/0	nat	-	ge0/0	-	0	-	-	-	F
65528	192.168.0.0/24	connected	-	loopback65528	-	-	-	-	-	F
65530	0.0.0.0/0	nat	-	ge0/0	-	0	-	-	-	F
65530	192.168.0.0/24	connected	-	loopback65530	-	-	-	-	-	F
65530	192.168.1.0/24	connected	-	loopback65531	-	-	-	-	-	F

vEdge SITE3 thì ta không thấy các route của VPN12 từ SITE1 và SITE2

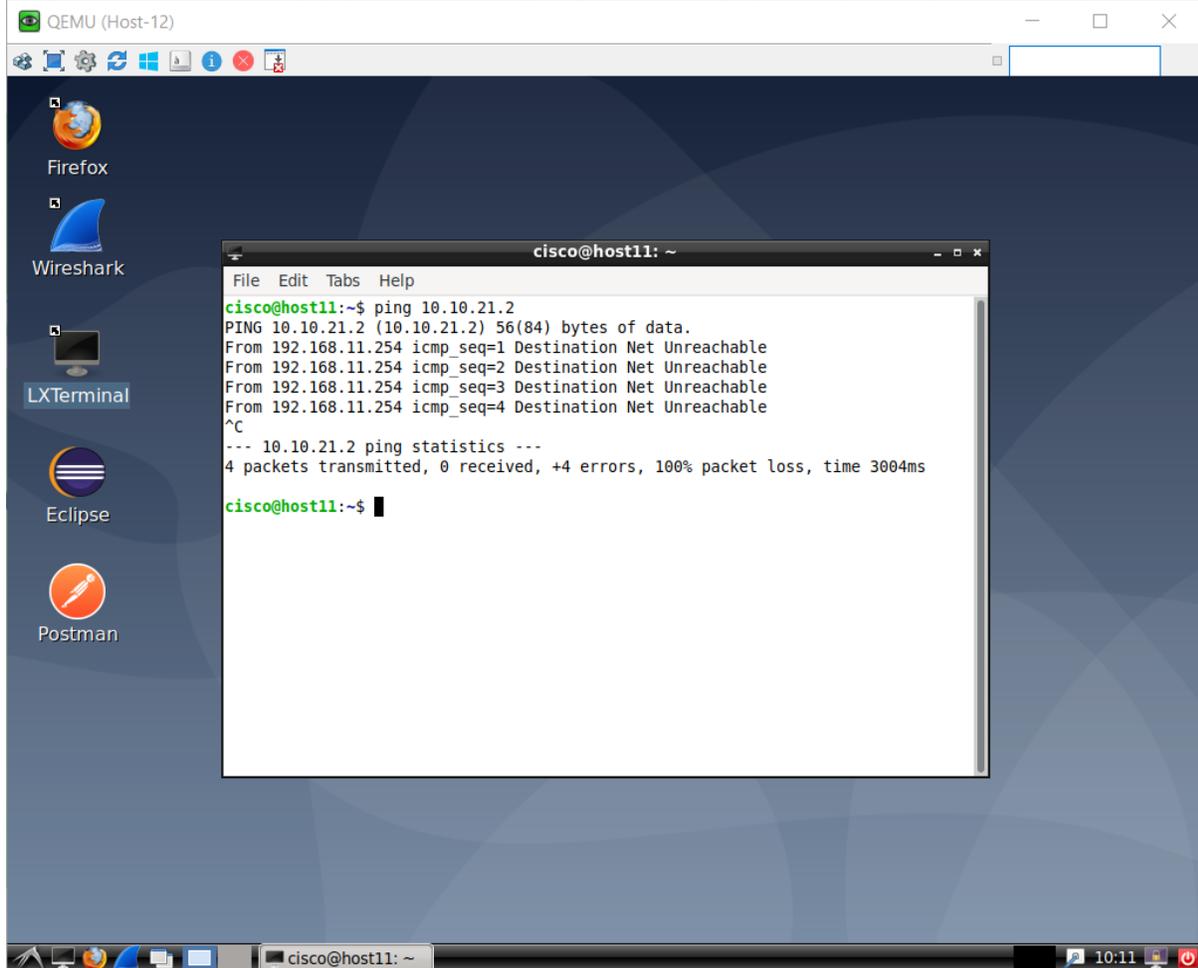
```
vEdge-Site3# show ip routes
Codes Proto-sub-Type:
  IA -> ospf-intra-area, IE -> ospf-internal,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nsa-external1, N2 -> ospf-nsa-external2,
  S -> bgp-external, I -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

VPN	PREFIX	PROTOCOL	SUB TYPE	IF NAME	NEXTHOP ADDR	VPN	TLOC IP	COLOR	ENCAP	S
0	0.0.0.0/0	static	-	ge0/0	200.200.3.1	-	-	-	-	F
0	4.1.1.1/32	connected	-	system	-	-	-	-	-	F
0	10.1.1.0/24	static	-	ge0/1	172.16.1.254	-	-	-	-	F
0	172.16.1.0/24	connected	-	ge0/1	-	-	-	-	-	F
0	200.200.3.0/30	connected	-	ge0/0	-	-	-	-	-	F
11	10.10.10.0/24	omp	-	-	-	-	2.1.1.1	mpls	ipsec	F
11	10.10.10.0/24	omp	-	-	-	-	2.1.1.1	biz-internet	ipsec	F
11	10.10.20.0/24	omp	-	-	-	-	3.1.1.1	mpls	ipsec	F
11	10.10.20.0/24	omp	-	-	-	-	3.1.1.1	biz-internet	ipsec	F
11	10.10.30.0/24	ospf	IA	ge0/2	192.168.30.2	-	-	-	-	F

```
vEdge-Site3# show ip routes
Codes Proto-sub-Type:
  IA -> ospf-intra-area, IE -> ospf-internal,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nsa-external1, N2 -> ospf-nsa-external2,
  S -> bgp-external, I -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

VPN	PREFIX	PROTOCOL	SUB TYPE	IF NAME	NEXTHOP ADDR	VPN	TLOC IP	COLOR	ENCAP	S
11	10.10.20.0/24	omp	-	-	-	-	3.1.1.1	biz-internet	ipsec	F
11	10.10.30.0/24	ospf	IA	ge0/2	192.168.30.2	-	-	-	-	F
11	192.168.10.0/24	omp	-	-	-	-	2.1.1.1	mpls	ipsec	F
11	192.168.10.0/24	omp	-	-	-	-	2.1.1.1	biz-internet	ipsec	F
11	192.168.20.0/24	omp	-	-	-	-	3.1.1.1	mpls	ipsec	F
11	192.168.20.0/24	omp	-	-	-	-	3.1.1.1	biz-internet	ipsec	F
11	192.168.30.0/24	ospf	IA	ge0/2	-	-	-	-	-	-
11	192.168.30.0/24	connected	-	ge0/2	-	-	-	-	-	F
12	10.10.31.0/24	ospf	IA	ge0/3	192.168.31.2	-	-	-	-	F
12	192.168.31.0/24	ospf	IA	ge0/3	-	-	-	-	-	-
12	192.168.31.0/24	connected	-	ge0/3	-	-	-	-	-	F
65528	0.0.0.0/0	nat	-	ge0/0	-	0	-	-	-	F
65528	192.168.0.0/24	connected	-	loopback65528-	-	-	-	-	-	-
65530	0.0.0.0/0	nat	-	ge0/0	-	0	-	-	-	F
65530	192.168.0.0/24	connected	-	loopback65530-	-	-	-	-	-	-
65530	192.168.1.0/24	connected	-	loopback65531-	-	-	-	-	-	-

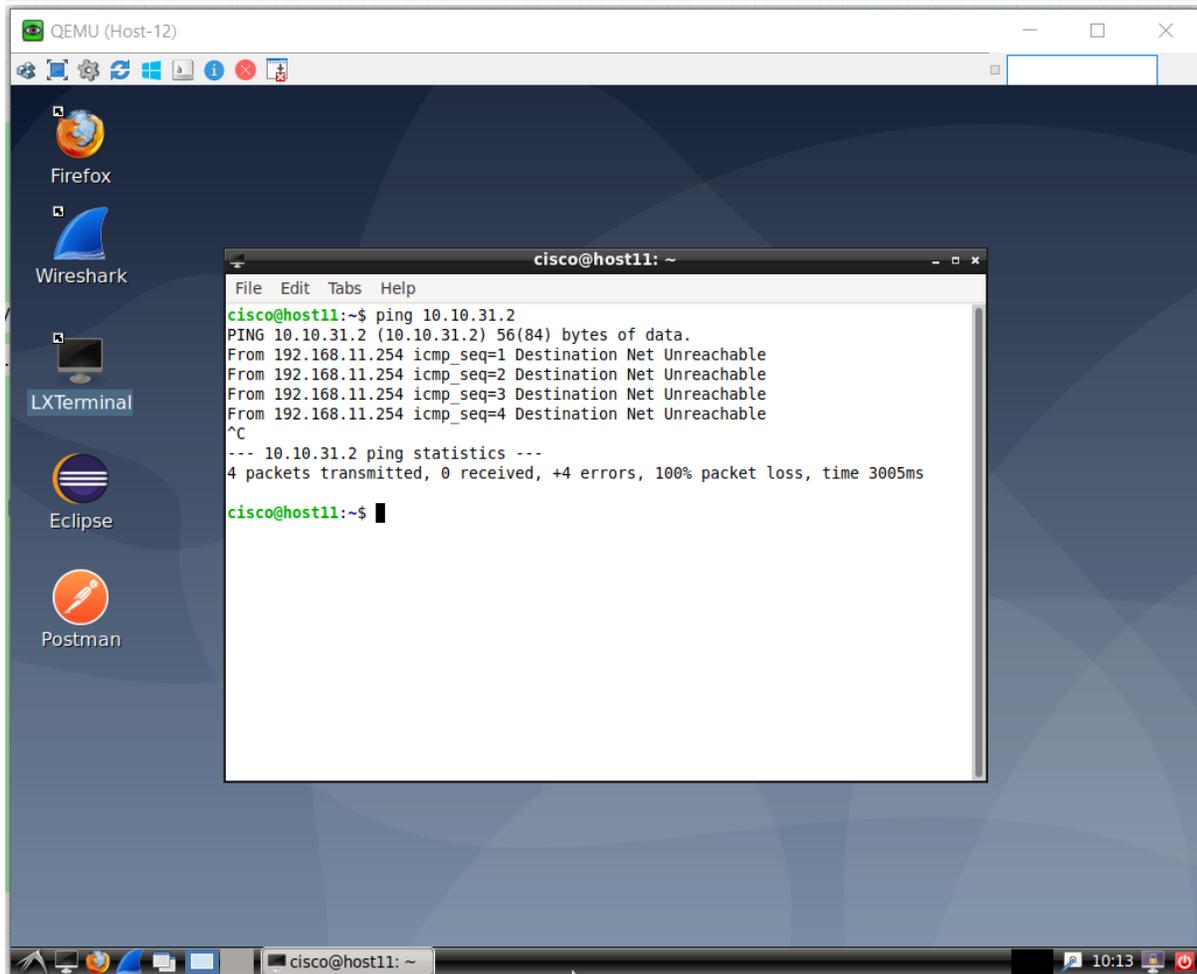
Thực hiện ping từ Host-12 của VPN12 ở site1 và Host-22 của VPN12 ở site2: thì ta thấy không biết đường đi do ta đã chặn giao tiếp giữa các site ở VPN12



The screenshot shows a QEMU virtual machine window titled "QEMU (Host-12)". The desktop environment includes icons for Firefox, Wireshark, LXTerminal, Eclipse, and Postman. A terminal window titled "cisco@host11: ~" is open, displaying the following output:

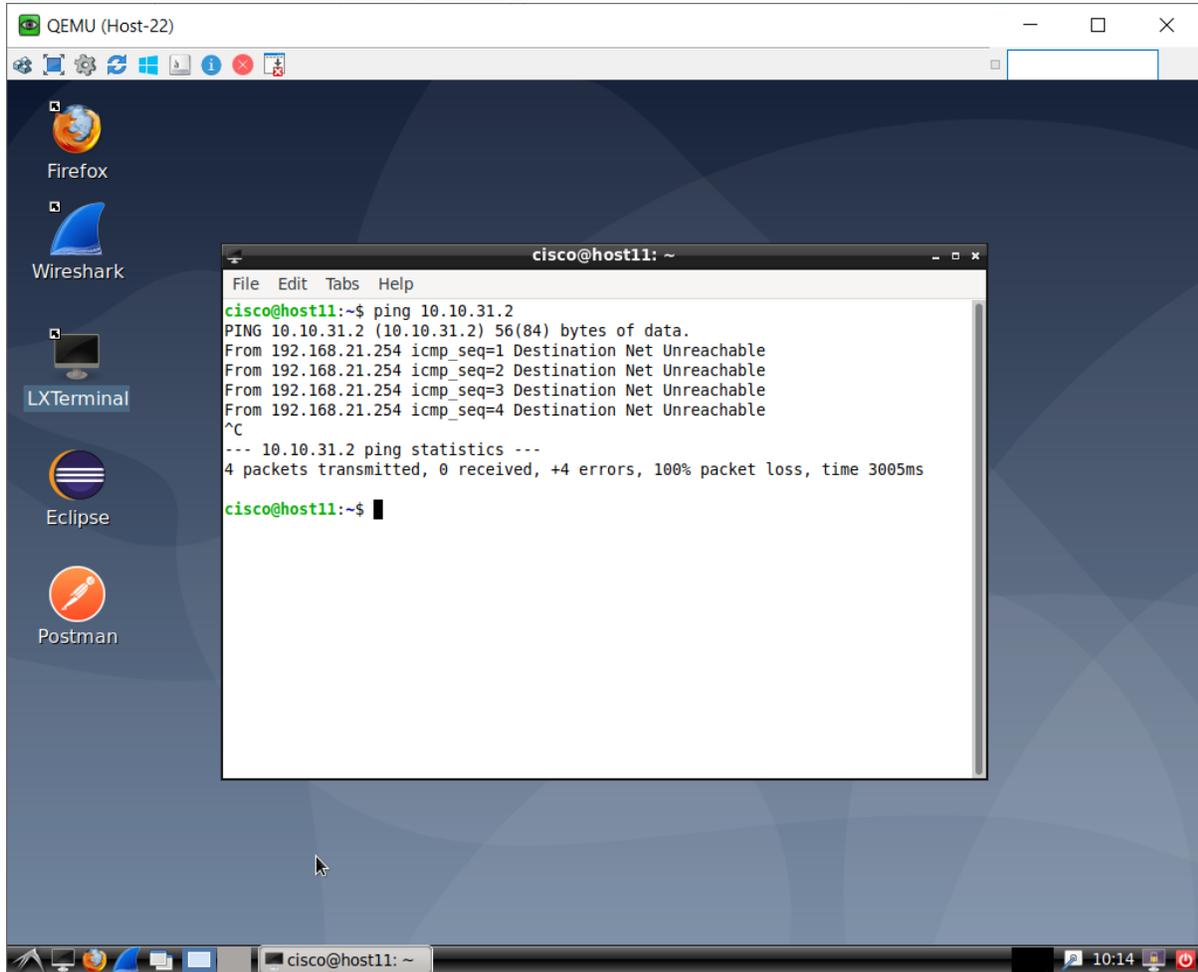
```
cisco@host11:~$ ping 10.10.21.2
PING 10.10.21.2 (10.10.21.2) 56(84) bytes of data:
From 192.168.11.254 icmp_seq=1 Destination Net Unreachable
From 192.168.11.254 icmp_seq=2 Destination Net Unreachable
From 192.168.11.254 icmp_seq=3 Destination Net Unreachable
From 192.168.11.254 icmp_seq=4 Destination Net Unreachable
^C
--- 10.10.21.2 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3004ms
cisco@host11:~$
```

Tương tự ping từ Host-12 của VPN12 ở site1 và Host-32 của VPN12 ở site3



```
cisco@host11: ~  
File Edit Tabs Help  
cisco@host11:~$ ping 10.10.31.2  
PING 10.10.31.2 (10.10.31.2) 56(84) bytes of data.  
From 192.168.11.254 icmp_seq=1 Destination Net Unreachable  
From 192.168.11.254 icmp_seq=2 Destination Net Unreachable  
From 192.168.11.254 icmp_seq=3 Destination Net Unreachable  
From 192.168.11.254 icmp_seq=4 Destination Net Unreachable  
^C  
--- 10.10.31.2 ping statistics ---  
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3005ms  
cisco@host11:~$
```

Tương tự ping từ Host-22 của VPN12 ở site2 và Host-32 của VPN12 ở site3





CÔNG TY TNHH TƯ VẤN VÀ DỊCH VỤ CHUYÊN VIỆT
TRUNG TÂM TIN HỌC VNPRO

ĐC: 276 - 278 Ung Văn Khiêm, P.25, Q. Bình Thạnh, Tp Hồ Chí Minh
ĐT: (028) 35124257 | **Hotline:** 0933427079 **Email:** vnpro@vnpro.org
