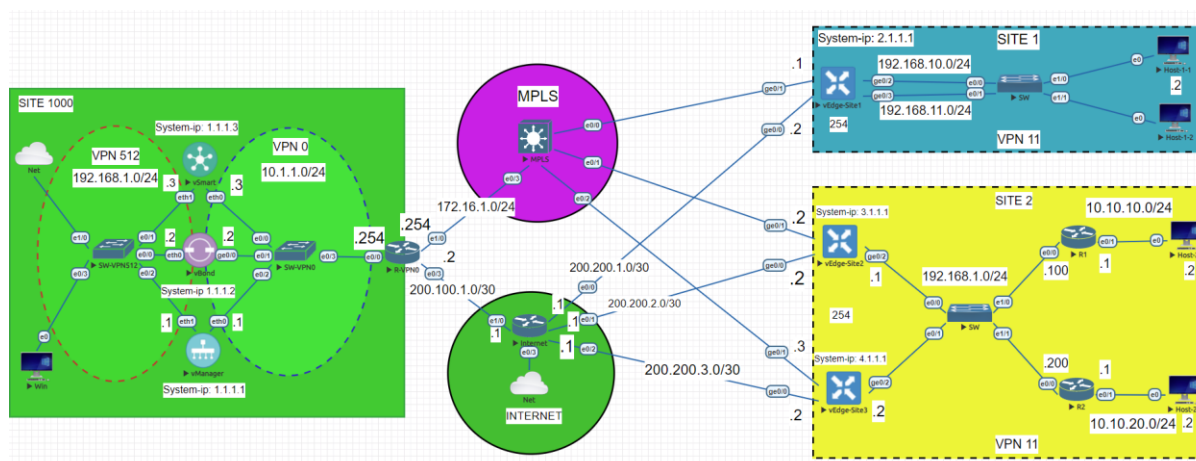


LAB - VIẾT ACCESS-CONTROL LIST (ACL) POLICY TRONG CISCO SD-WAN

I. Sơ đồ



II. Yêu cầu kỹ thuật

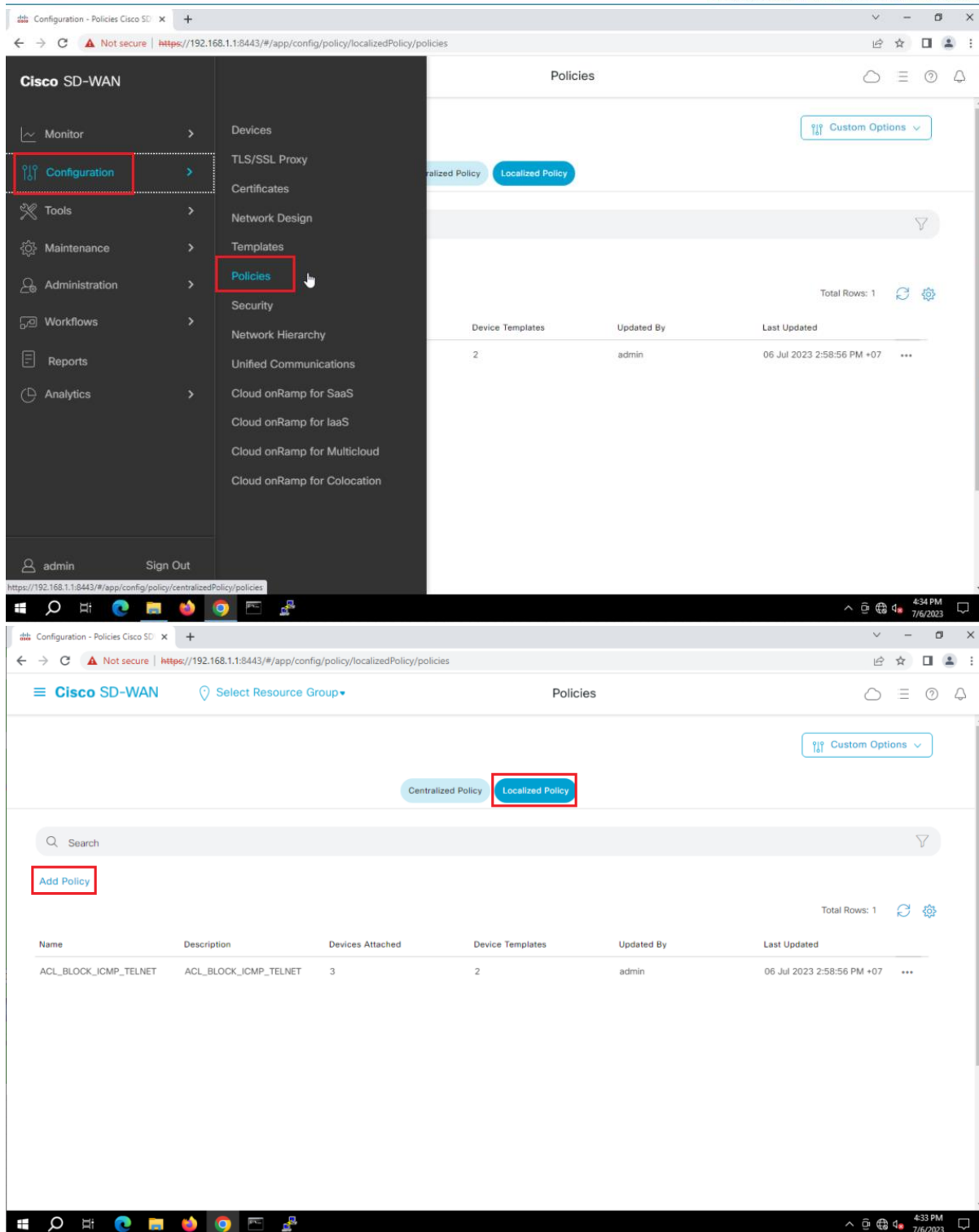
- Viết 1 chính sách Localized Data Policies: *ACL_BLOCK_ICMP_TELNET* nhằm mục đích chặn ping từ router R1, R2 đến thiết bị Host-1-1, và Host-1-2 không thể telnet đến các thiết bị router R1, R2 ở Site 2.
- Đẩy cấu hình chính sách Policy xuống các thiết bị vEdge-Site1, vEdge1-Site2, vEdge2-Site2.
- Kiểm tra ping từ router R1, R2 đến thiết bị Host-1-1, và thiết bị Host-1-2 telnet đến router R1, R2 sau khi áp dụng policy.

III. Các bước thực hiện

3.1. Cấu hình ACLs thông qua vManage và Localized Data Policies

- Tạo localized Policy: *ACL_BLOCK_ICMP_TELNET*

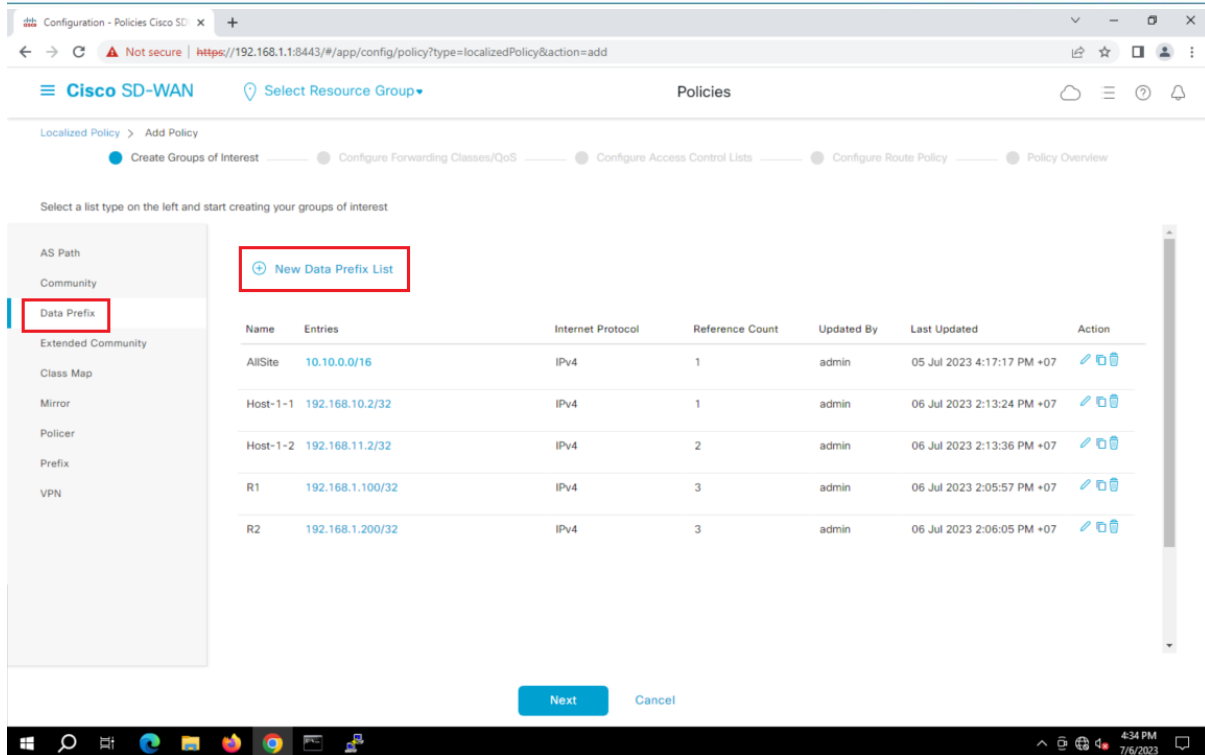
Đầu tiên ta vào giao diện **vManage > Configuration > Policies > Localized Policy > Add Policy**



The screenshot shows the Cisco SD-WAN configuration interface. The left sidebar contains a menu with options: Monitor, Configuration (highlighted), Tools, Maintenance, Administration, Workflows, Reports, and Analytics. The 'Configuration' menu is expanded, showing sub-options: Devices, TLS/SSL Proxy, Certificates, Network Design, Templates, Policies (highlighted), Security, Network Hierarchy, Unified Communications, Cloud onRamp for SaaS, Cloud onRamp for IaaS, Cloud onRamp for Multicloud, and Cloud onRamp for Colocation. The main area displays the 'Policies' section with tabs for 'Centralized Policy' and 'Localized Policy' (highlighted). A search bar and an 'Add Policy' button (highlighted) are visible. Below the search bar, a table lists existing policies.

Name	Description	Devices Attached	Device Templates	Updated By	Last Updated
ACL_BLOCK_ICMP_TELNET	ACL_BLOCK_ICMP_TELNET	3	2	admin	06 Jul 2023 2:58:56 PM +07

Ở phần **Create Groups of Internet**, ta chọn phần **Data Prefix** > **New Data Prefix List** để tạo các data prefix list như sau:



Configuration - Policies Cisco SD-WAN

Localized Policy > Add Policy

Create Groups of Interest | Configure Forwarding Classes/QoS | Configure Access Control Lists | Configure Route Policy | Policy Overview

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

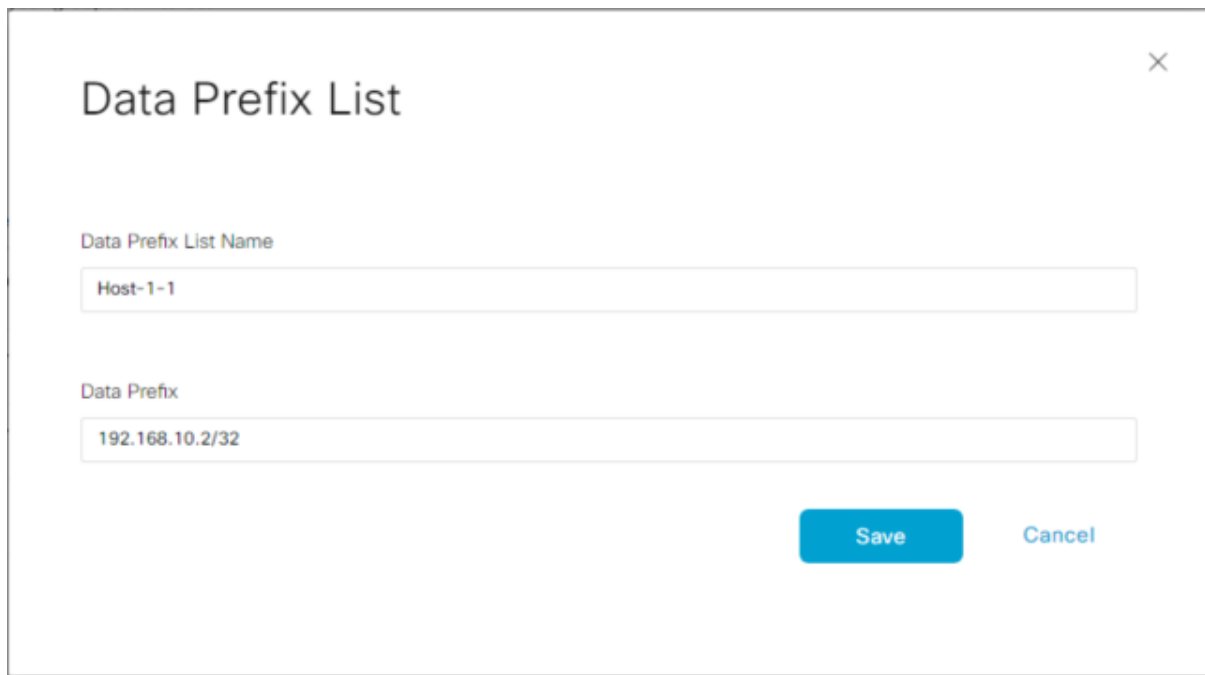
AS Path
Community
Data Prefix
Extended Community
Class Map
Mirror
Policer
Prefix
VPN

New Data Prefix List

Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated	Action
AllSite	10.10.0.0/16	IPv4	1	admin	05 Jul 2023 4:17:17 PM +07	 
Host-1-1	192.168.10.2/32	IPv4	1	admin	06 Jul 2023 2:13:24 PM +07	 
Host-1-2	192.168.11.2/32	IPv4	2	admin	06 Jul 2023 2:13:36 PM +07	 
R1	192.168.1.100/32	IPv4	3	admin	06 Jul 2023 2:05:57 PM +07	 
R2	192.168.1.200/32	IPv4	3	admin	06 Jul 2023 2:06:05 PM +07	 

Next Cancel

Dải ip của thiết bị **Host-1-1**:



Data Prefix List

Data Prefix List Name

Host-1-1

Data Prefix

192.168.10.2/32

Save Cancel

Dải ip của thiết bị **Host-1-2**:

×

Data Prefix List

Data Prefix List Name

Host-1-2

Data Prefix

192.168.11.2/32

Save

Cancel

R1 và R2

×

Data Prefix List

Data Prefix List Name

R1

Data Prefix

192.168.1.100/32

Save

Cancel

Data Prefix List

Data Prefix List Name

Data Prefix

SaveCancel

Configuration - Policies Cisco SD-WAN

Select Resource Group

Policies

Localized Policy > Add Policy

Create Groups of Interest

Configure Forwarding Classes/QoS

Configure Access Control Lists

Configure Route Policy

Policy Overview

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

AS Path

Community

Data Prefix

Extended Community

Class Map

Mirror

Policer

Prefix

VPN

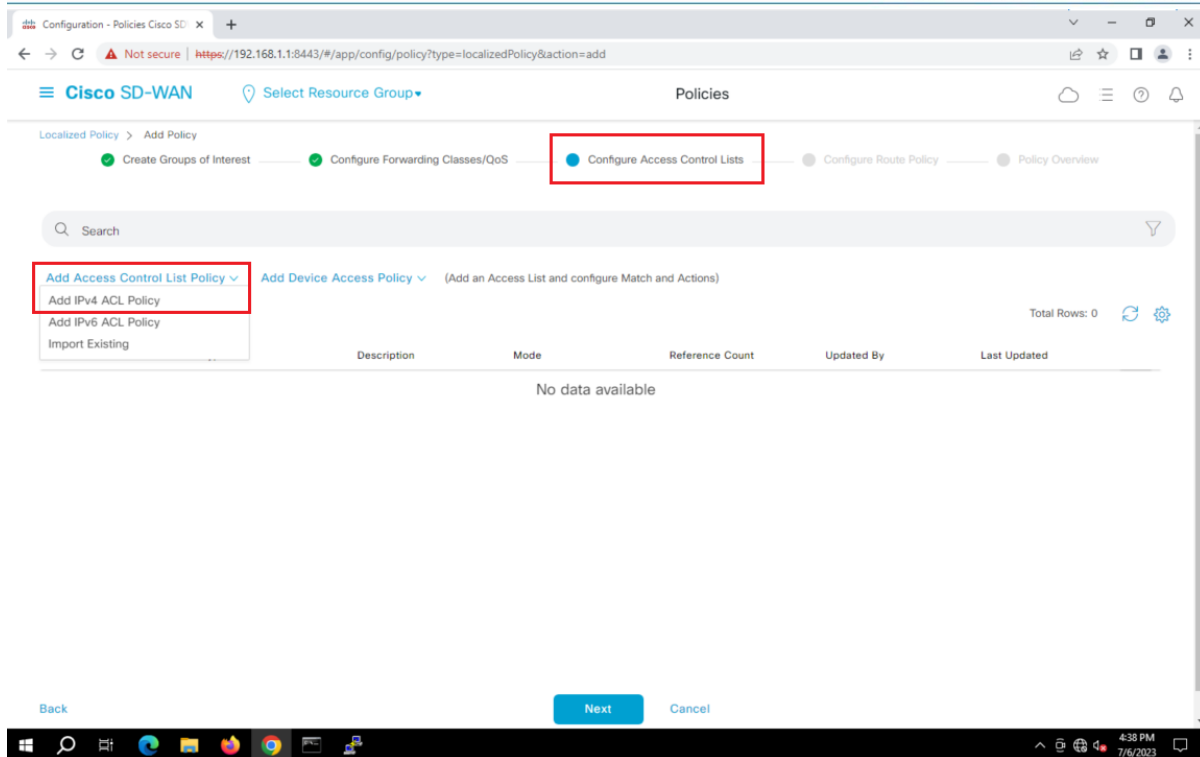
New Data Prefix List

Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated	Action
AllSite	10.10.0.0/16	IPv4	1	admin	05 Jul 2023 4:17:17 PM +07	 
Host-1-1	192.168.10.2/32	IPv4	1	admin	06 Jul 2023 2:13:24 PM +07	 
Host-1-2	192.168.11.2/32	IPv4	2	admin	06 Jul 2023 2:13:36 PM +07	 
R1	192.168.1.100/32	IPv4	3	admin	06 Jul 2023 2:05:57 PM +07	 
R2	192.168.1.200/32	IPv4	3	admin	06 Jul 2023 2:06:05 PM +07	 

Next

Cancel

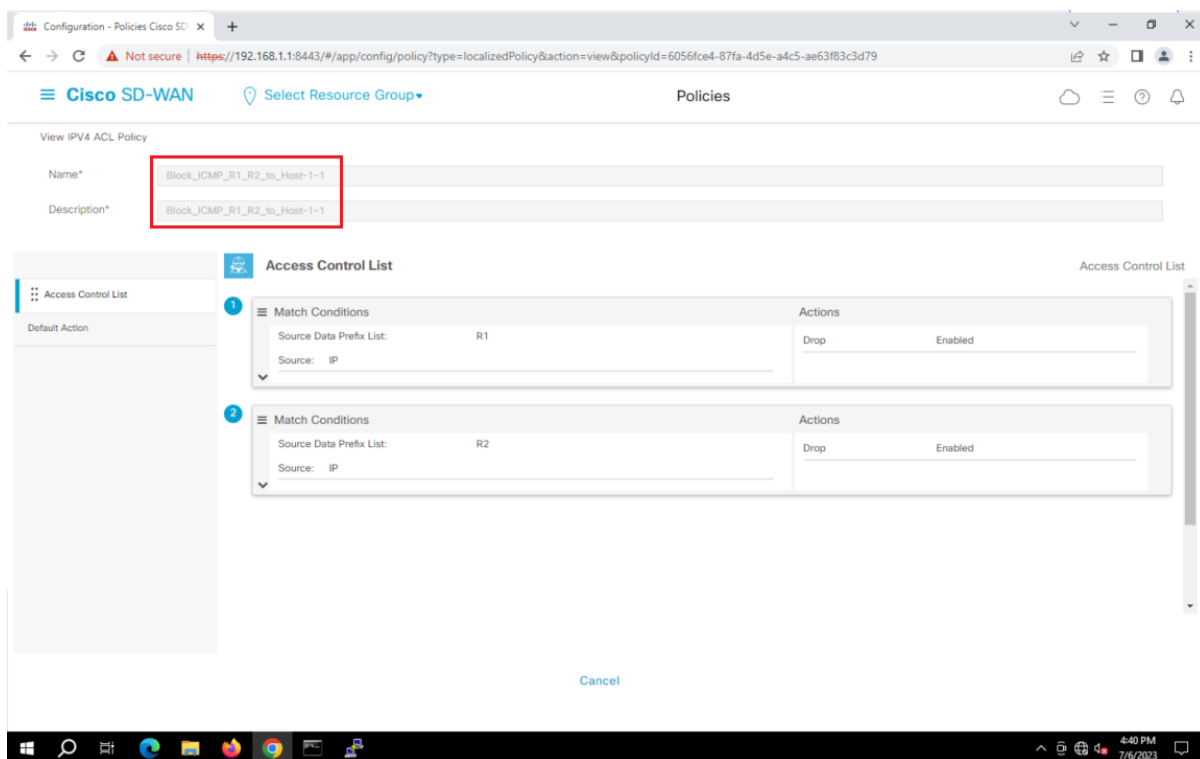
Ở phần **Configure Access Control Lists > Add Access Control List Policy > Add IPv4 ACL Policy** để tạo ACL Policy:



Trong phần **Add IPv4 ACL Policy**, ta lần lượt cấu hình như sau:

Name: *Block_ICMP_R1_R1_to_Host-1-1*

Description: *Block_ICMP_R1_R1_to_Host-1-1*



Sau đó chọn **Add ACL Sequence** để tạo ACL như sau:

1

Match Conditions	Actions
Source Data Prefix List: R1	Drop Enabled
Source: IP	
Destination Data Prefix List: Host-1-1	
Destination: IP	
Protocol: 1	
ICMP Message	

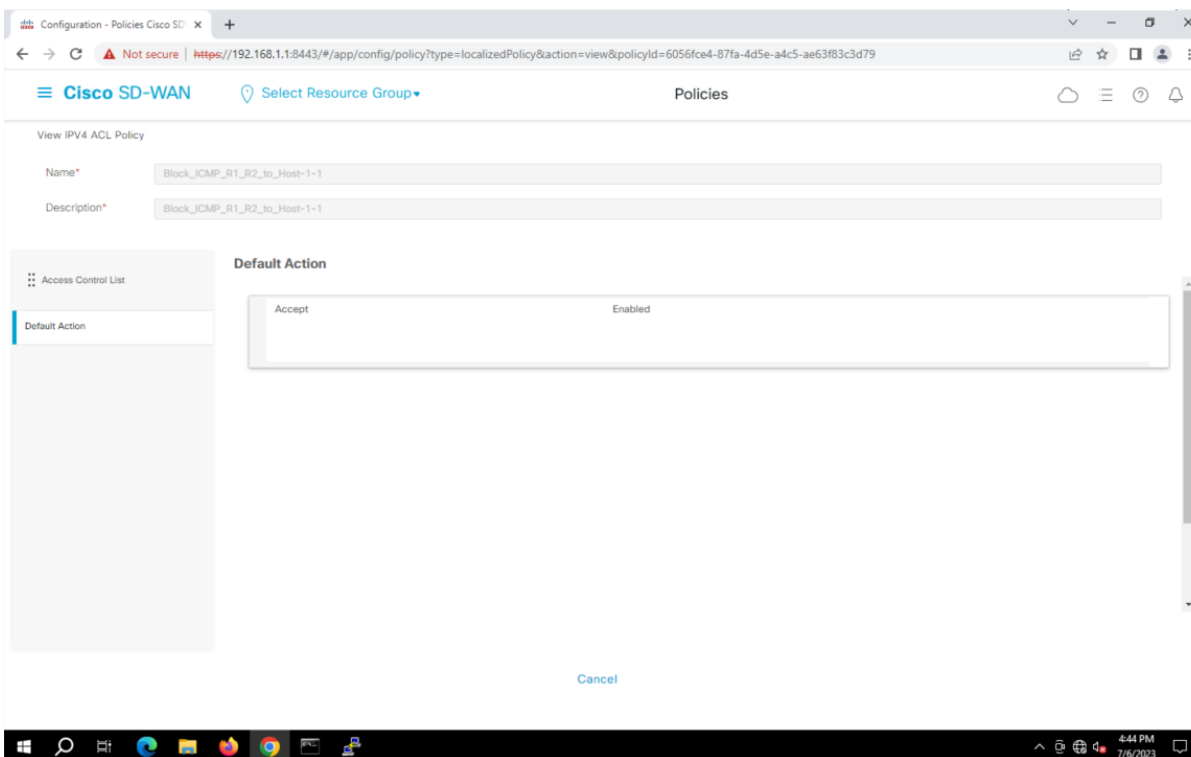
Cấu hình xong tiến hành chọn **Save Match And Actions**

2

Match Conditions	Actions
Source Data Prefix List: R2	Drop Enabled
Source: IP	
Destination Data Prefix List: Host-1-1	
Destination: IP	
Protocol: 1	
ICMP Message	

Cấu hình xong tiến hành chọn **Save Match And Actions**

Ở mục **Default Action > Accept**



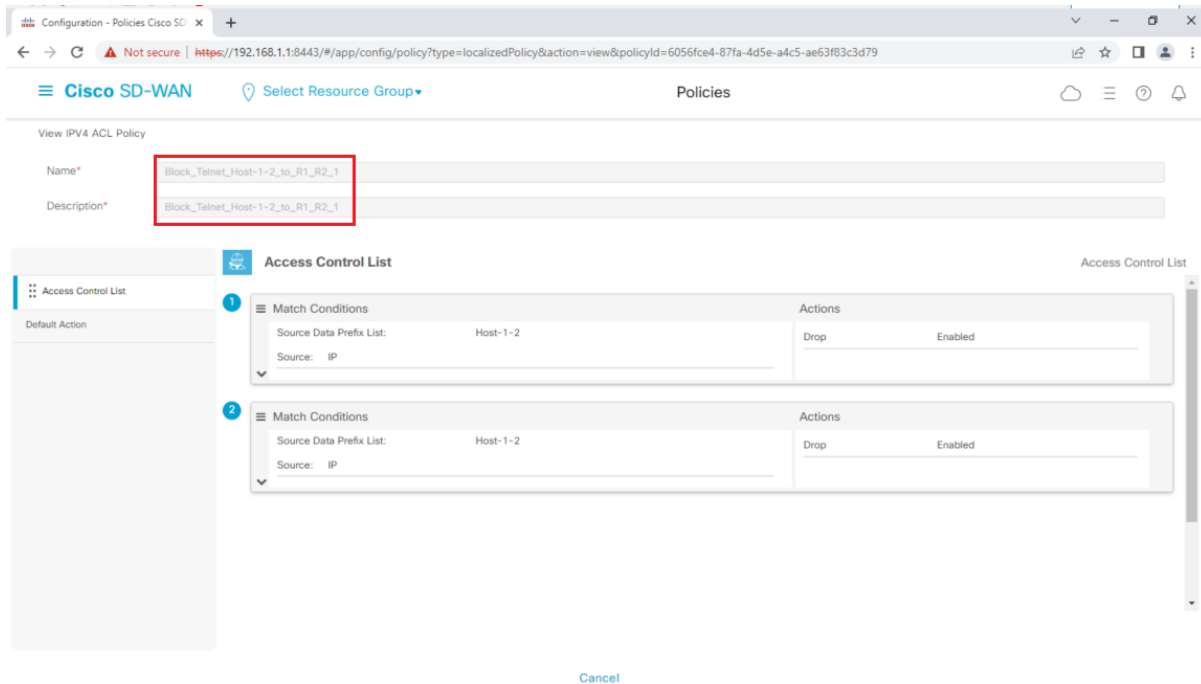
The screenshot shows the Cisco SD-WAN configuration interface. The 'Default Action' section is visible, showing 'Accept' as the selected action and 'Enabled' as its status. The interface includes a sidebar with 'Access Control List' and 'Default Action' options, and a main area for configuring the policy. The URL in the browser address bar is <https://192.168.1.1:8443/#/app/config/policy?type=localizedPolicy&action=view&policyId=6056fce4-87fa-4d5e-a4c5-ae63f83c3d79>.

Sau đó **Save Match And Actions > Save ACL Policy**

Tiếp theo ta chọn **Add IPv4 ACL Policy**, ta lần lượt cấu hình như sau:

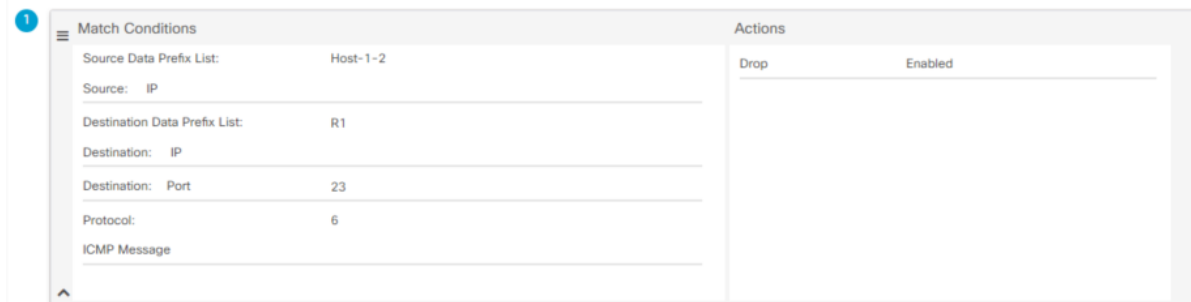
Name: Block_Telnet_Host-1-2_to_R1_R2

Description: Block_Telnet_Host-1-2_to_R1_R2



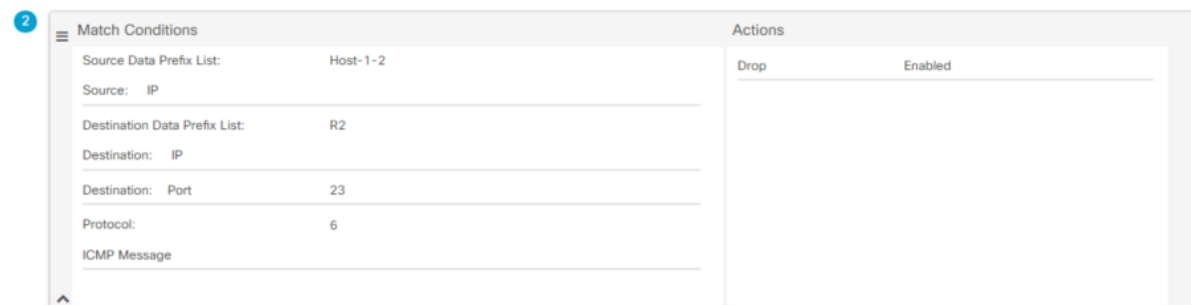
The screenshot shows the Cisco SD-WAN configuration interface. The 'Policies' tab is selected. Under 'View IPv4 ACL Policy', the 'Name*' field is set to 'Block_Telnet_Host-1-2_to_R1_R2_1' and the 'Description*' field is also set to 'Block_Telnet_Host-1-2_to_R1_R2_1'. Below this, the 'Access Control List' section is visible, showing two match conditions. Each condition has 'Source Data Prefix List' set to 'Host-1-2' and 'Source' set to 'IP'. The 'Actions' column shows 'Drop' and 'Enabled'.

Sau đó chọn **Add ACL Sequence** để tạo ACL như sau:



The screenshot shows the 'Match Conditions' and 'Actions' configuration for the first ACL sequence. The 'Match Conditions' section includes: 'Source Data Prefix List' set to 'Host-1-2', 'Source' set to 'IP', 'Destination Data Prefix List' set to 'R1', 'Destination' set to 'IP', 'Destination: Port' set to '23', 'Protocol' set to '6', and 'ICMP Message'. The 'Actions' section shows 'Drop' and 'Enabled'.

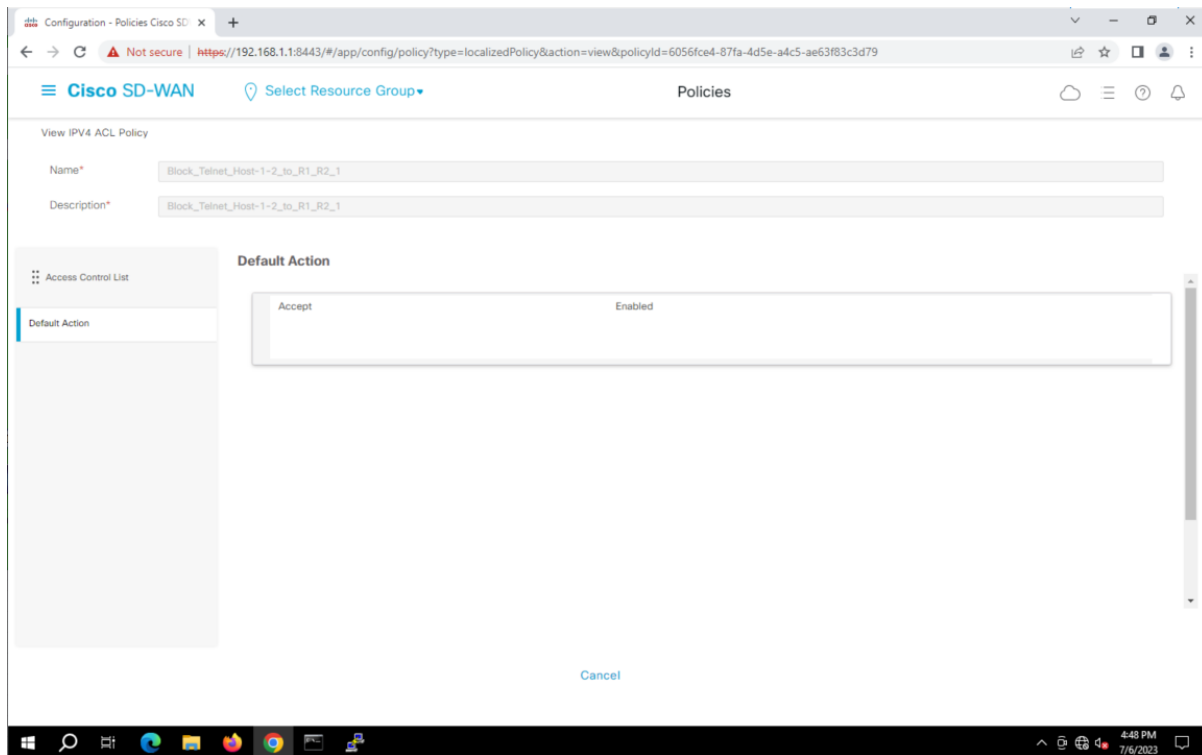
Cấu hình xong tiến hành chọn **Save Match And Actions**



The screenshot shows the 'Match Conditions' and 'Actions' configuration for the second ACL sequence. The 'Match Conditions' section includes: 'Source Data Prefix List' set to 'Host-1-2', 'Source' set to 'IP', 'Destination Data Prefix List' set to 'R2', 'Destination' set to 'IP', 'Destination: Port' set to '23', 'Protocol' set to '6', and 'ICMP Message'. The 'Actions' section shows 'Drop' and 'Enabled'.

Cấu hình xong tiến hành chọn **Save Match And Actions**

Ở mục Default Action > Accept

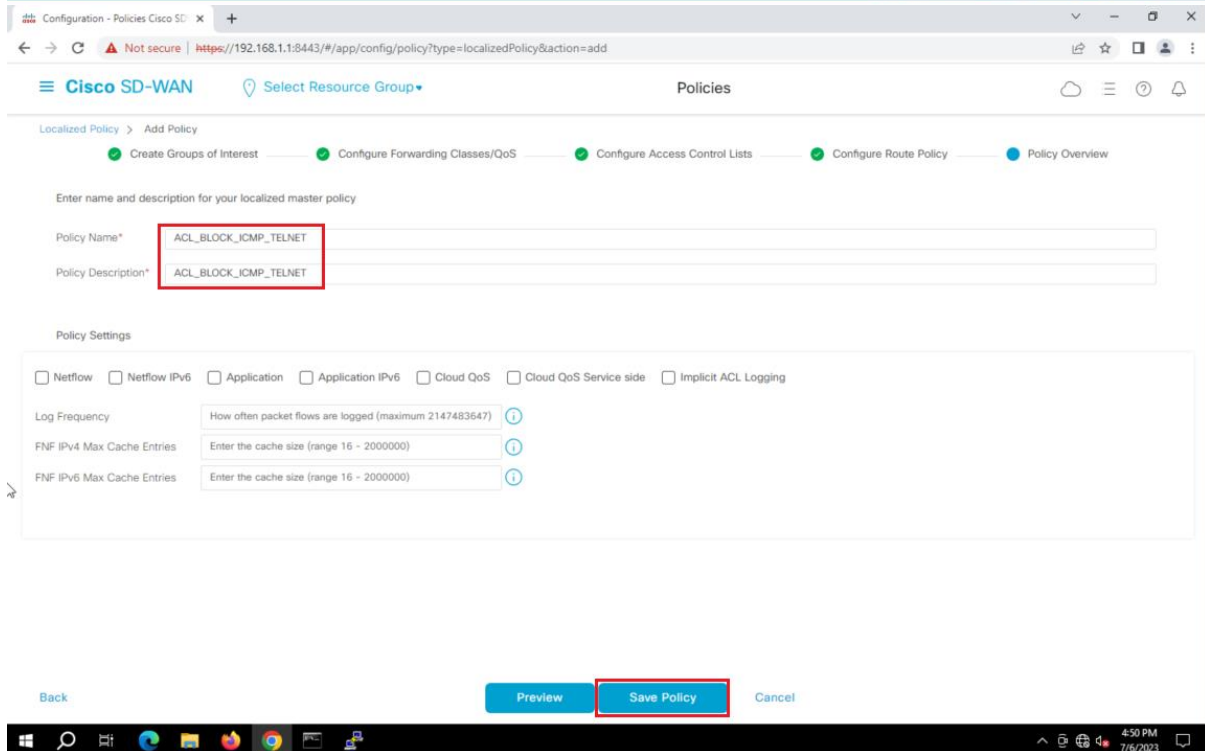


Sau đó **Save Match And Actions > Save ACL Policy**

Ở phần **Policy Overview**

Policy Name: ACL_BLOCK_ICMP_TELNET

Policy Description: ACL_BLOCK_ICMP_TELNET



Configuration - Policies Cisco SD-WAN

Localized Policy > Add Policy

Create Groups of Interest ☒ Configure Forwarding Classes/QoS ☒ Configure Access Control Lists ☒ Configure Route Policy ☒ Policy Overview ☒

Enter name and description for your localized master policy

Policy Name*

Policy Description*

Policy Settings

☐ Netflow ☐ Netflow IPv6 ☐ Application ☐ Application IPv6 ☐ Cloud QoS ☐ Cloud QoS Service side ☐ Implicit ACL Logging

Log Frequency

FNF IPv4 Max Cache Entries

FNF IPv6 Max Cache Entries

Back Preview **Save Policy** Cancel

Cuối cùng tiến hành **Save Policy**

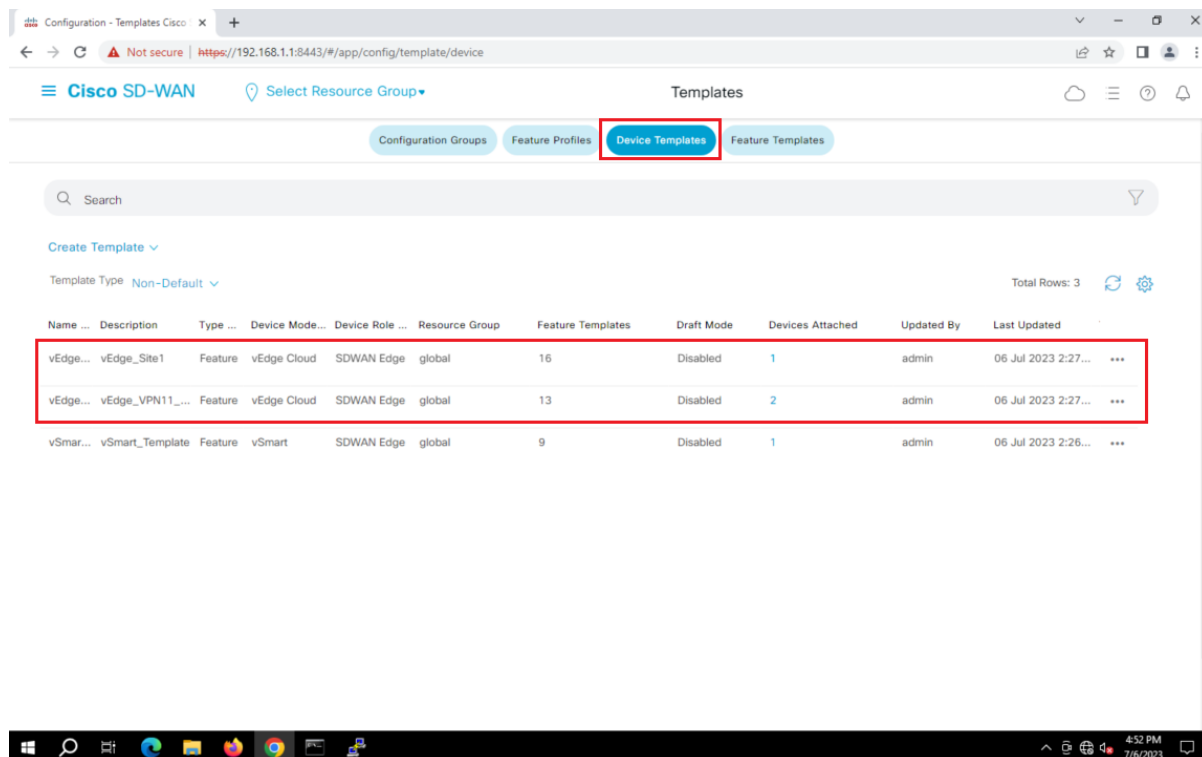
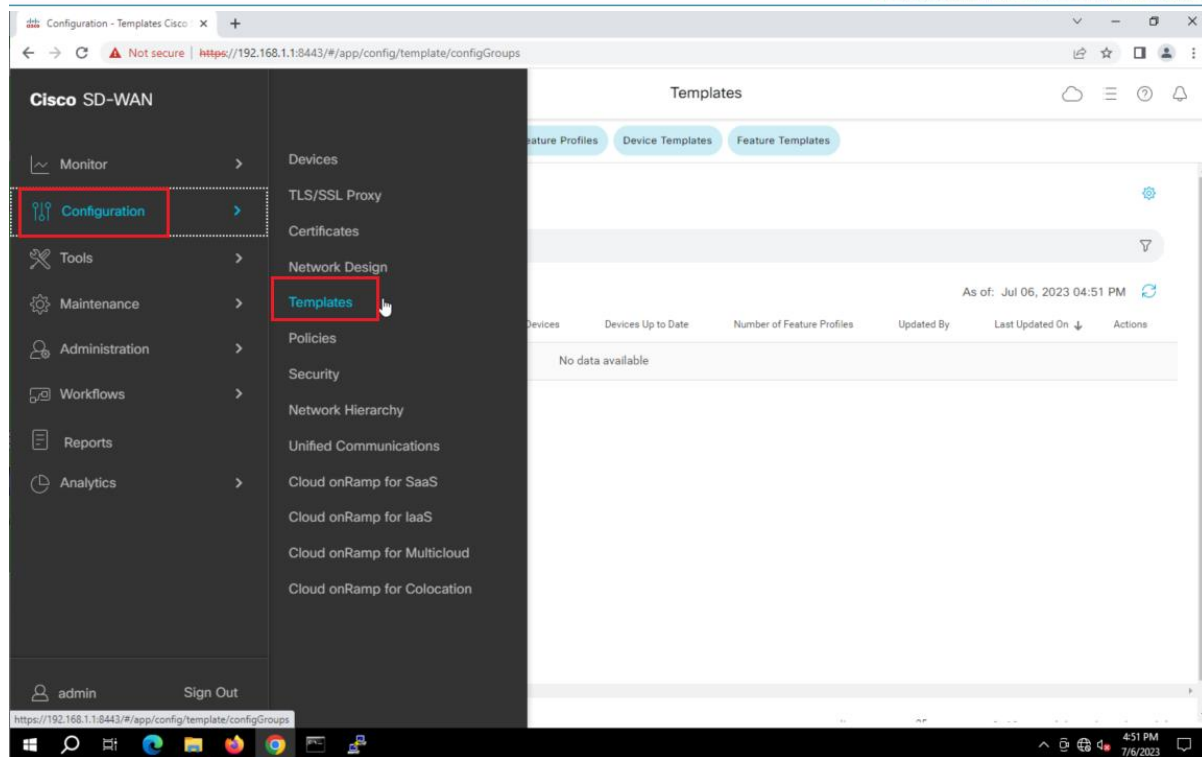
3.2. Thêm ACL Policy vào thiết bị và Port.

Add policy vào thiết bị

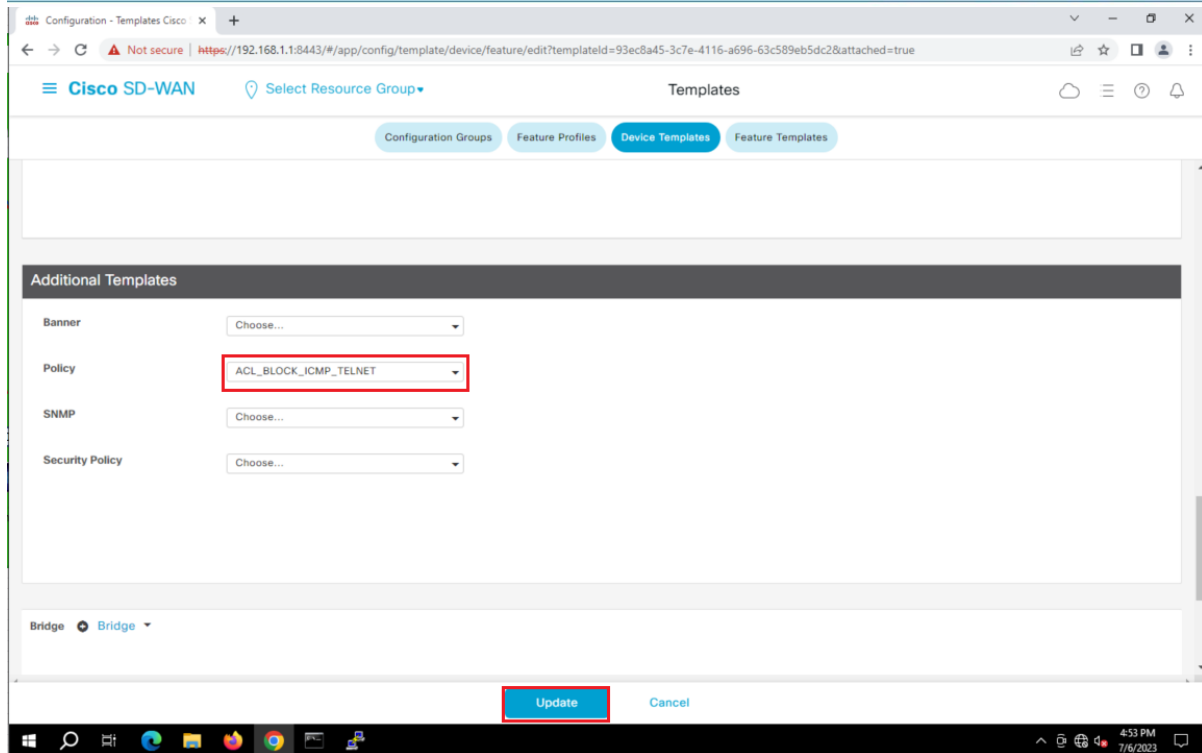
Ở giao diện vManage, **Configuration > Templates** (tab Device).

Ta lần lượt chọn lần lượt các **Device Template > Edit** như sau:

Device Template: vEdge_VPN11_Ge0/2_VRRP

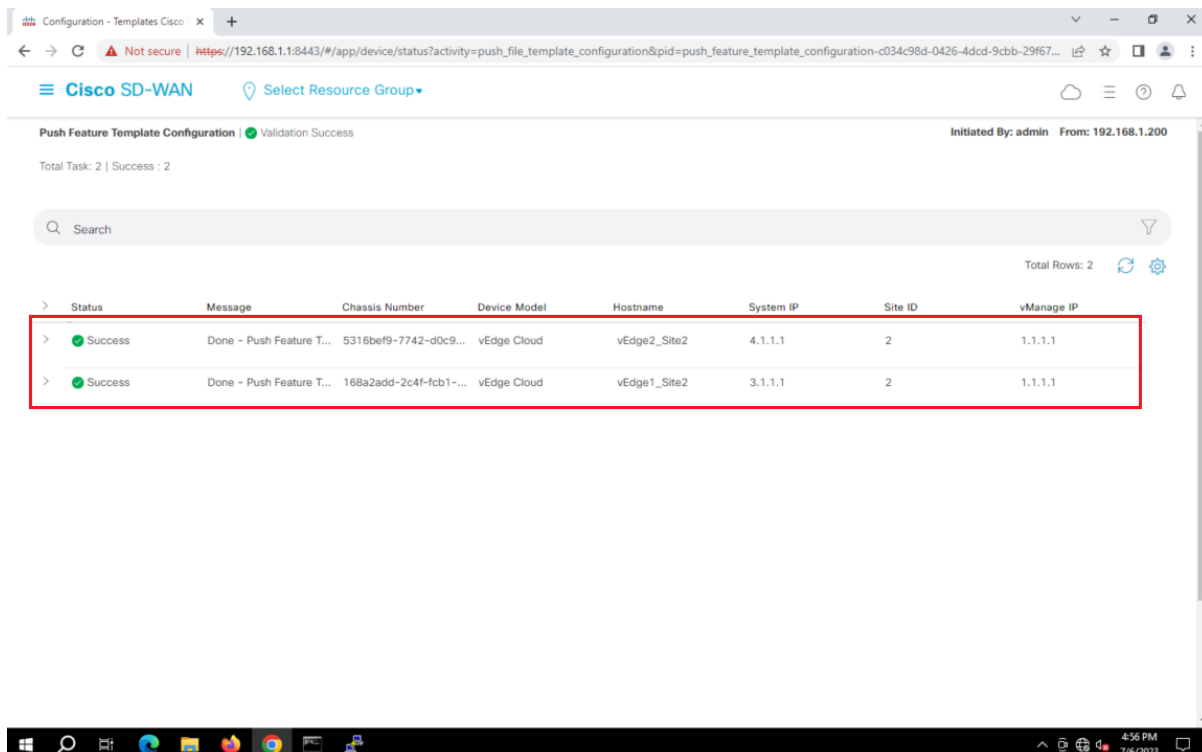


Ở mục Additional Templates, ta vào mục **Policy** và chọn **ACL_BLOCK_ICMP_TELNET** (đã tạo trước đó)

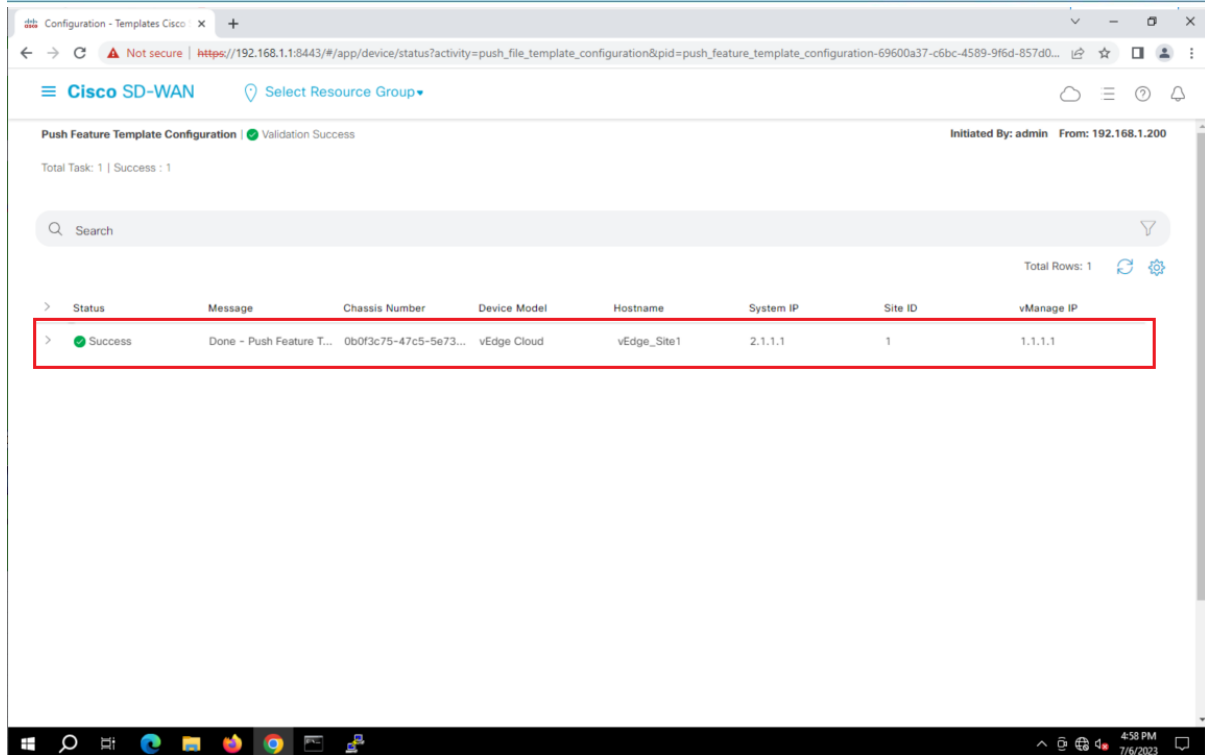


Sau đó tiến hành **Update**

Thiết bị vEdge1-Site2, vEdge2-Site2 đã được áp cấu hình Policy xuống thành công.



Trương tự cho vEdge-Site1 ở site 1



The screenshot shows the Cisco SD-WAN vManage interface. The top navigation bar includes 'Cisco SD-WAN' and 'Select Resource Group'. The main content area displays 'Push Feature Template Configuration' with a 'Validation Success' status. Below this, a table lists the configuration details for a single task.

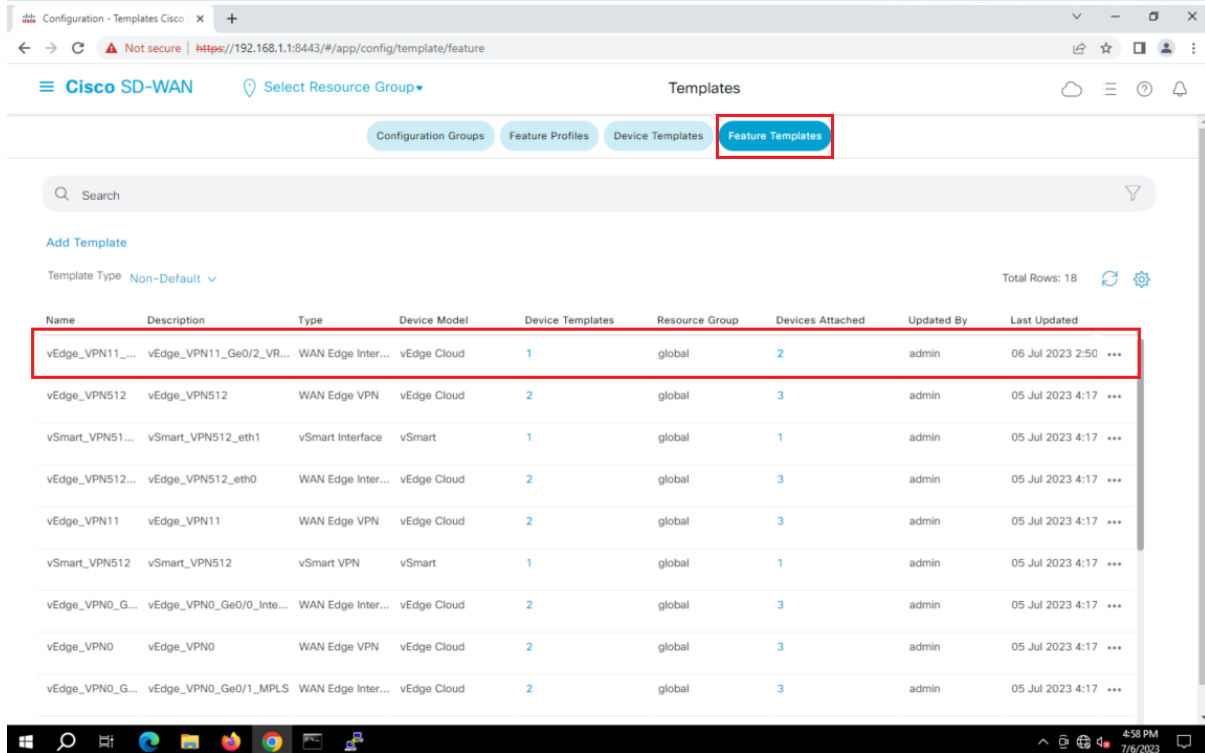
Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature T...	0b0f3c75-47c5-5e73...	vEdge Cloud	vEdge_Site1	2.1.1.1	1	1.1.1.1

Add Policy vào Port Ge0/2 ở site 2

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

Và Edit các Template của các port sau

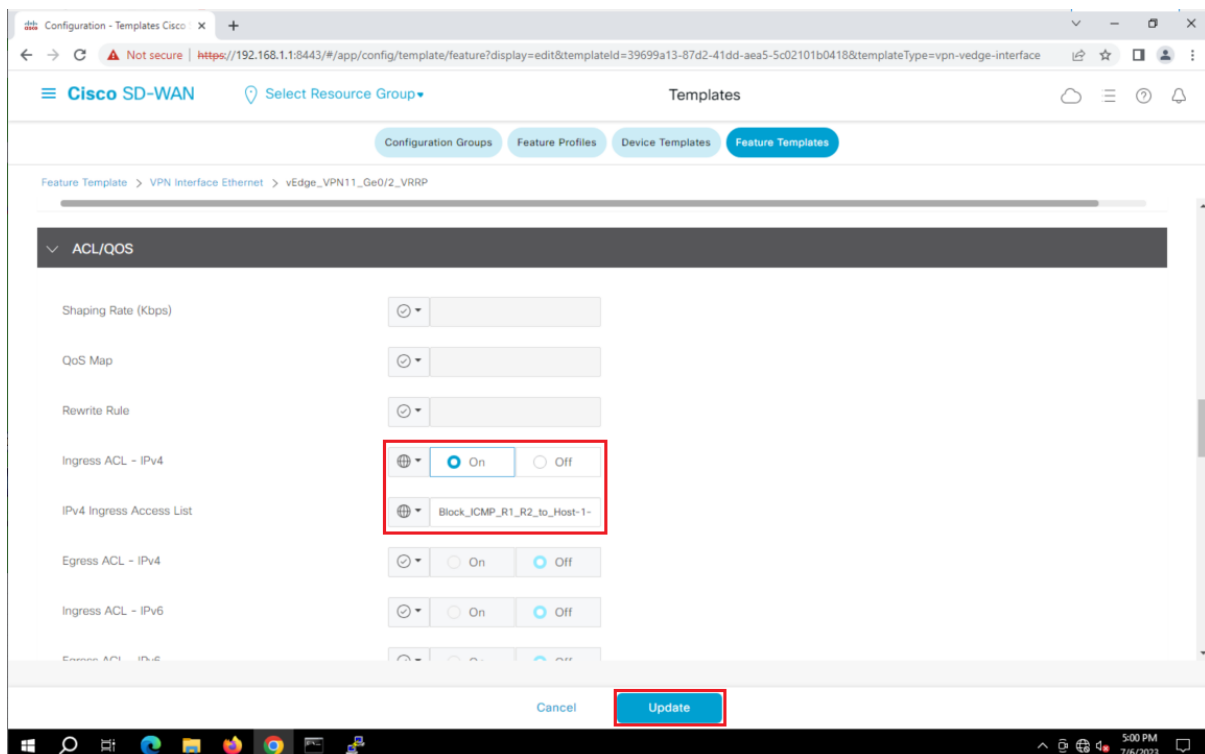
vEdge_VPN11_Ge0/2_VRRP



Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
vEdge_VPN11_...	vEdge_VPN11_Ge0/2_VR...	WAN Edge Inter...	vEdge Cloud	1	global	2	admin	06 Jul 2023 2:50
vEdge_VPN512	vEdge_VPN512	WAN Edge VPN	vEdge Cloud	2	global	3	admin	05 Jul 2023 4:17
vSmart_VPN51...	vSmart_VPN512_eth1	vSmart Interface	vSmart	1	global	1	admin	05 Jul 2023 4:17
vEdge_VPN512...	vEdge_VPN512_eth0	WAN Edge Inter...	vEdge Cloud	2	global	3	admin	05 Jul 2023 4:17
vEdge_VPN11	vEdge_VPN11	WAN Edge VPN	vEdge Cloud	2	global	3	admin	05 Jul 2023 4:17
vSmart_VPN512	vSmart_VPN512	vSmart VPN	vSmart	1	global	1	admin	05 Jul 2023 4:17
vEdge_VPN0_G...	vEdge_VPN0_Ge0/0_Inte...	WAN Edge Inter...	vEdge Cloud	2	global	3	admin	05 Jul 2023 4:17
vEdge_VPN0	vEdge_VPN0	WAN Edge VPN	vEdge Cloud	2	global	3	admin	05 Jul 2023 4:17
vEdge_VPN0_G...	vEdge_VPN0_Ge0/1_MPLS	WAN Edge Inter...	vEdge Cloud	2	global	3	admin	05 Jul 2023 4:17

Ở phần mục ACL/QoS ta edit các thông số như sau:

Block_ICMP_R1_R2_to_Host-1-1 (đã tạo ACL ở trên)



Feature Template > VPN Interface Ethernet > vEdge_VPN11_Ge0/2_VRRP

ACL/QoS

Shaping Rate (Kbps)

QoS Map

Rewrite Rule

Ingress ACL - IPv4 ☒ On ☐ Off

IPv4 Ingress Access List

Egress ACL - IPv4 ☐ On ☒ Off

Ingress ACL - IPv6 ☐ On ☒ Off

Egress ACL - IPv6 ☐ On ☒ Off

Cancel

Sau đó chọn Update > Next để update template xuống hai vEdge:

Configuration - Templates Cisco x

Not secure | https://192.168.1.1:8443/#/app/config/template/device/configure/af54c6fe-9221-463a-9d7c-b5354f3164b1

Cisco SD-WAN Select Resource Group Templates

Device Template | vEdge_VPN11_Geo/2_VRRP

Search

Total Rows: 2

S...	Chassis Number	System IP	Hostname	IPv4 Address(vpn11_ge0/2_if_ipv4_address)	Group ID(vpn_if_vrrp_grpid)	Priority(vpn_
✓	5316bef9-7742-d0c9-1048-df6288bb4e...	4.1.1.1	vEdge2_Site2	192.168.1.1/24	100	150 ***
✓	168a2add-2c4f-fcb1-6139-1d99df86e22e	3.1.1.1	vEdge1_Site2	192.168.1.1/24	100	120 ***

Next Cancel

Windows taskbar: 5:01 PM 7/6/2023

Configure Devices

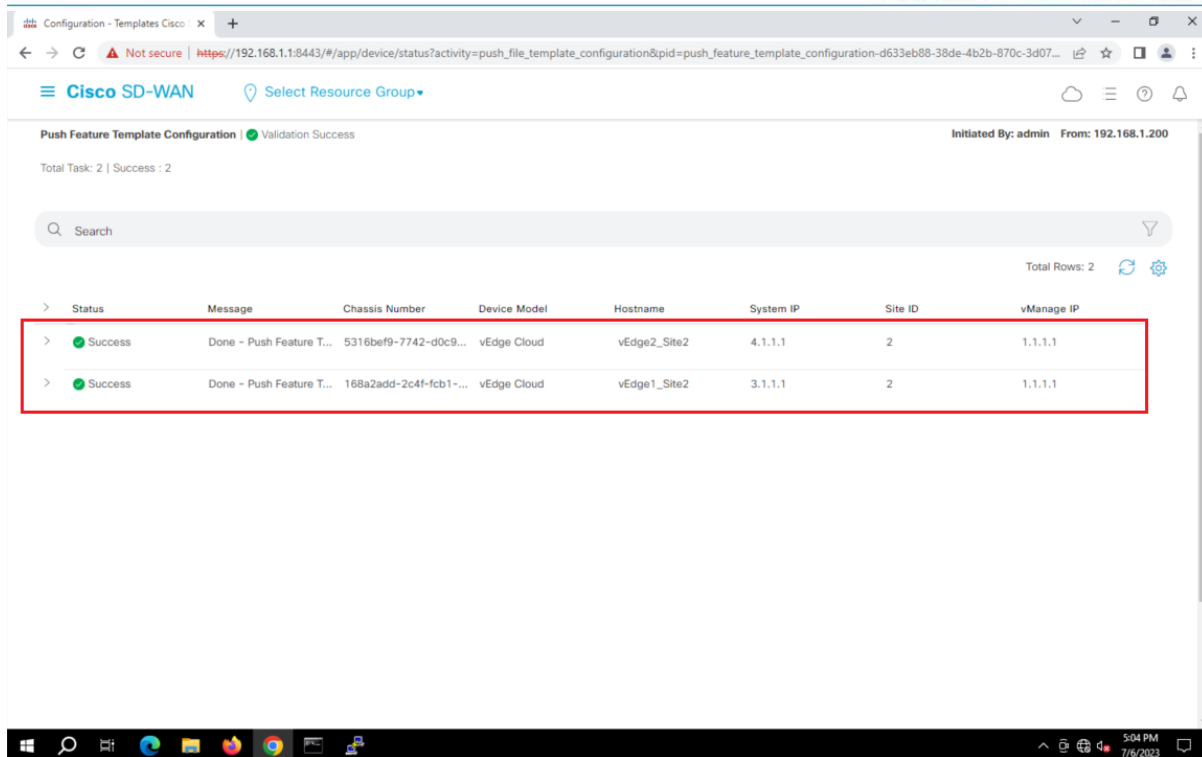
Committing these changes affect the configuration on 2 devices. Are you sure you want to proceed?

☒ Confirm configuration changes on 2 devices.

OK

Cancel

Sau đó áp dụng cấu hình thành công xuống cho vEdge1-Site2, vEdge2-Site2



Configuration - Templates Cisco

Push Feature Template Configuration | Validation Success

Initiated By: admin From: 192.168.1.200

Total Task: 2 | Success: 2

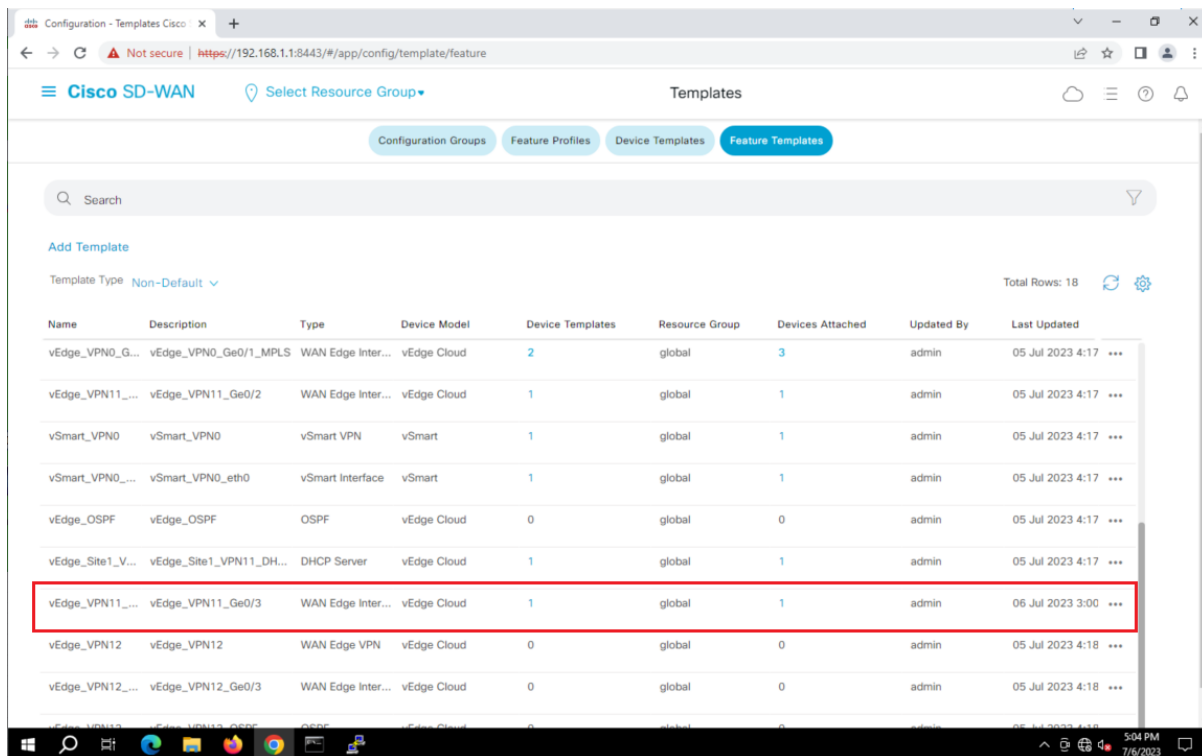
Search

Total Rows: 2

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature T...	5316bef9-7742-d0c9...	vEdge Cloud	vEdge2_Site2	4.1.1.1	2	1.1.1.1
Success	Done - Push Feature T...	168a2add-2c4f-fcb1-...	vEdge Cloud	vEdge1_Site2	3.1.1.1	2	1.1.1.1

Đối với vEdge1 ở site 1

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



Configuration - Templates Cisco

Templates

Configuration Groups Feature Profiles Device Templates Feature Templates

Search

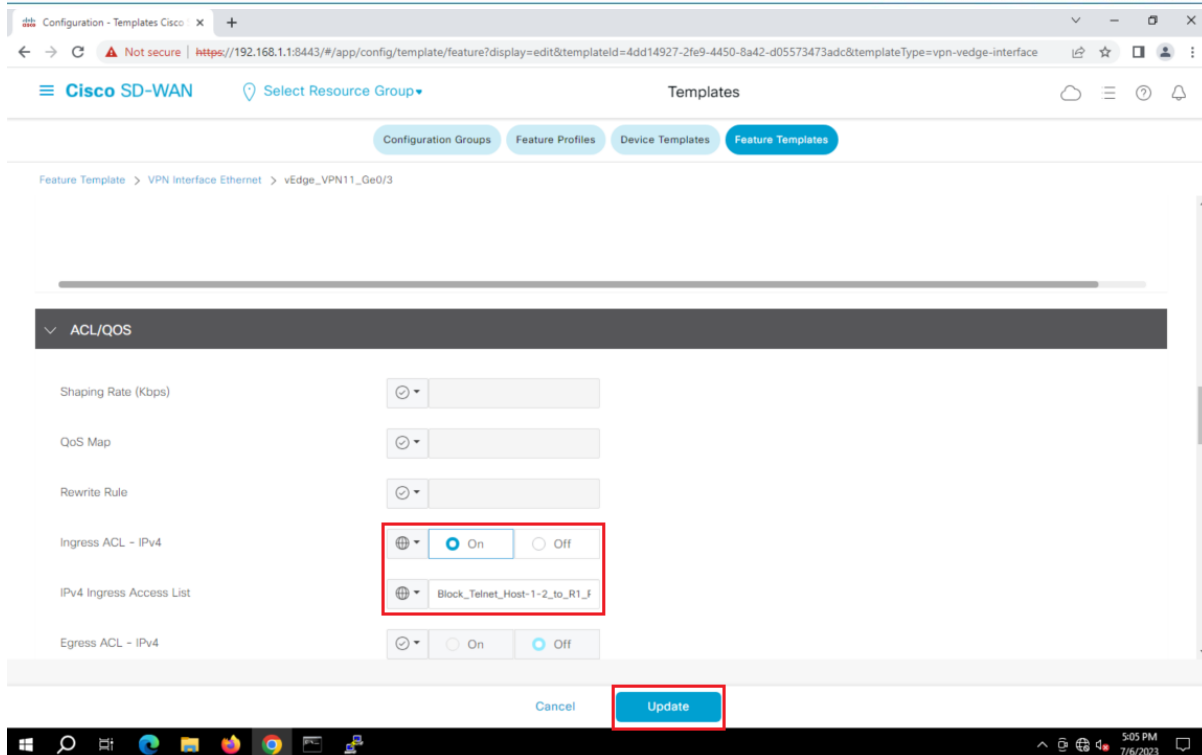
Add Template

Template Type Non-Default

Total Rows: 18

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
vEdge_VPN0_G...	vEdge_VPN0_Ge0/1_MPLS	WAN Edge Inter...	vEdge Cloud	2	global	3	admin	05 Jul 2023 4:17
vEdge_VPN11_...	vEdge_VPN11_Ge0/2	WAN Edge Inter...	vEdge Cloud	1	global	1	admin	05 Jul 2023 4:17
vSmart_VPN0	vSmart_VPN0	vSmart VPN	vSmart	1	global	1	admin	05 Jul 2023 4:17
vSmart_VPN0_...	vSmart_VPN0_eth0	vSmart Interface	vSmart	1	global	1	admin	05 Jul 2023 4:17
vEdge_OSPF	vEdge_OSPF	OSPF	vEdge Cloud	0	global	0	admin	05 Jul 2023 4:17
vEdge_Site1_V...	vEdge_Site1_VPN11_DH...	DHCP Server	vEdge Cloud	1	global	1	admin	05 Jul 2023 4:17
vEdge_VPN11_...	vEdge_VPN11_Ge0/3	WAN Edge Inter...	vEdge Cloud	1	global	1	admin	06 Jul 2023 3:00
vEdge_VPN12	vEdge_VPN12	WAN Edge VPN	vEdge Cloud	0	global	0	admin	05 Jul 2023 4:18
vEdge_VPN12_...	vEdge_VPN12_Ge0/3	WAN Edge Inter...	vEdge Cloud	0	global	0	admin	05 Jul 2023 4:18

Ở phần mục **ACL/QoS** ta edit các thông số như sau:



Configuration - Templates Cisco

Not secure | https://192.168.1.1:8443/#/app/config/template/feature?display=edit&templateId=4dd14927-2fe9-4450-8a42-d05573473adc&templateType=vpn-vedge-interface

Cisco SD-WAN Select Resource Group

Templates

Configuration Groups Feature Profiles Device Templates Feature Templates

Feature Template > VPN Interface Ethernet > vEdge_VPN11_Ge0/3

ACL/QoS

Shaping Rate (Kbps)

QoS Map

Rewrite Rule

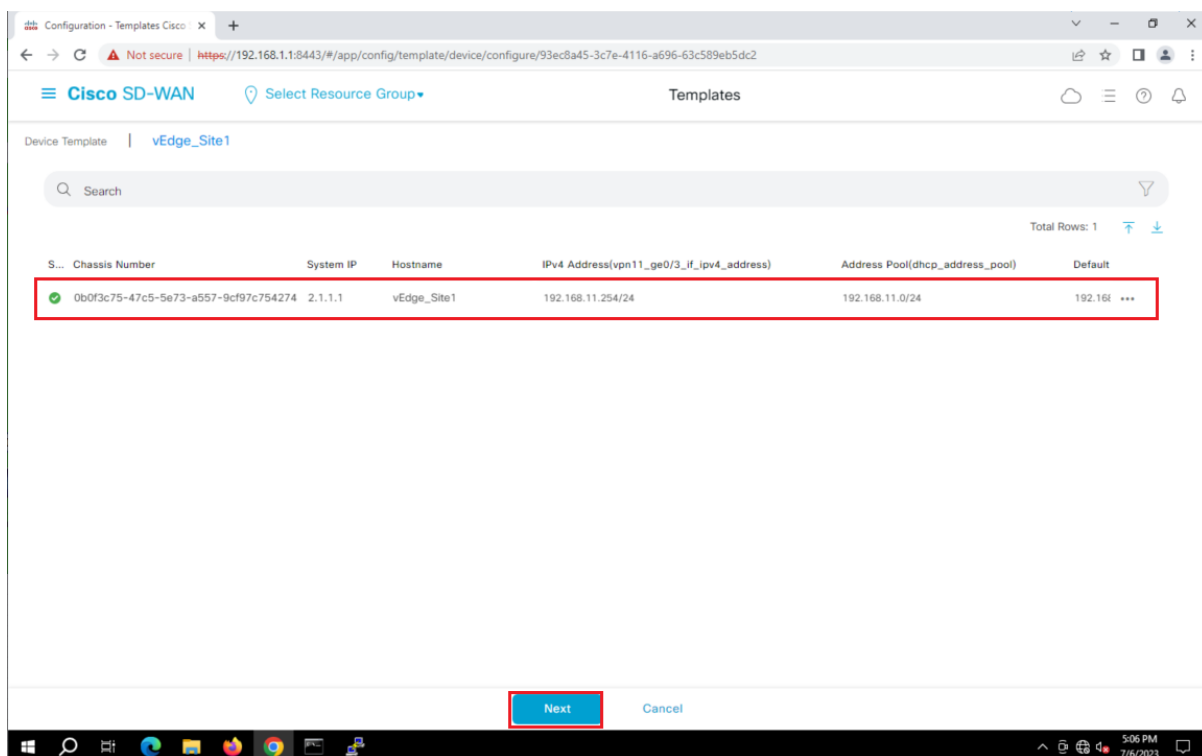
Ingress ACL - IPv4 ☒ On ☐ Off

IPv4 Ingress Access List

Egress ACL - IPv4 ☐ On ☒ Off

Cancel Update

Sau đó chọn **Update** > **Next** để update template xuống vEdge:



Configuration - Templates Cisco

Not secure | https://192.168.1.1:8443/#/app/config/template/device/configure/93ec8a45-3c7e-4116-a696-63c589eb5dc2

Cisco SD-WAN Select Resource Group

Templates

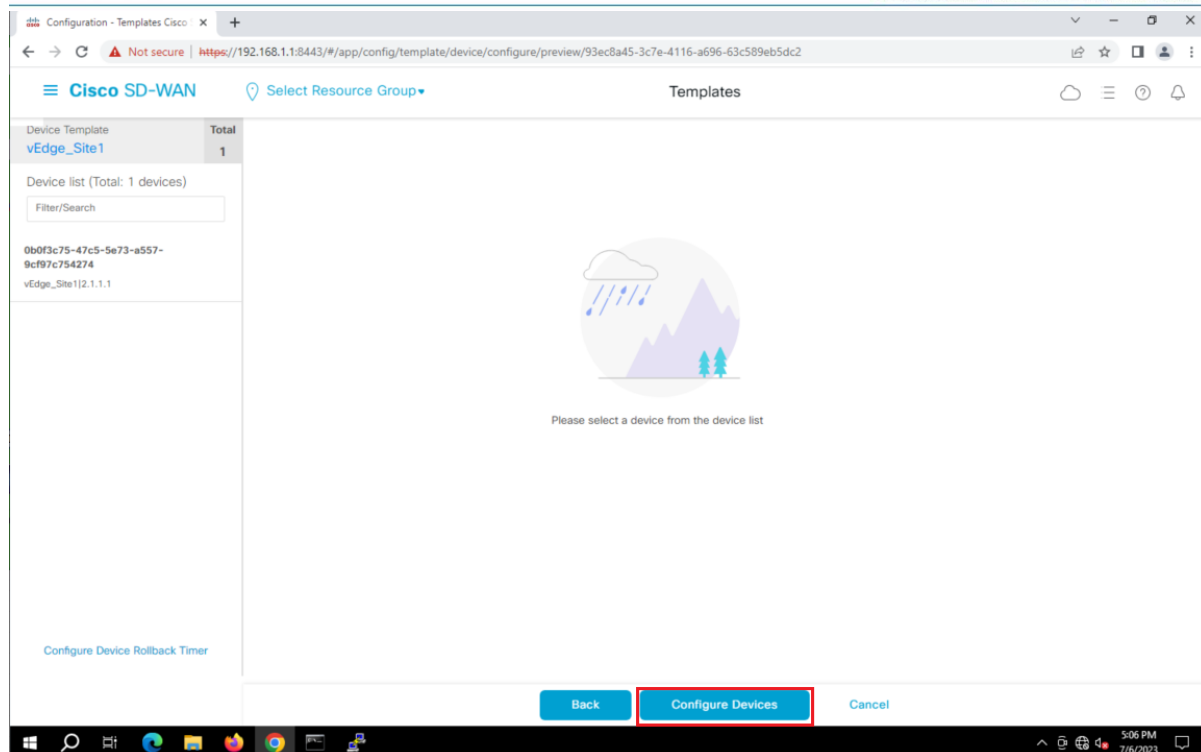
Device Template | vEdge_Site1

Search

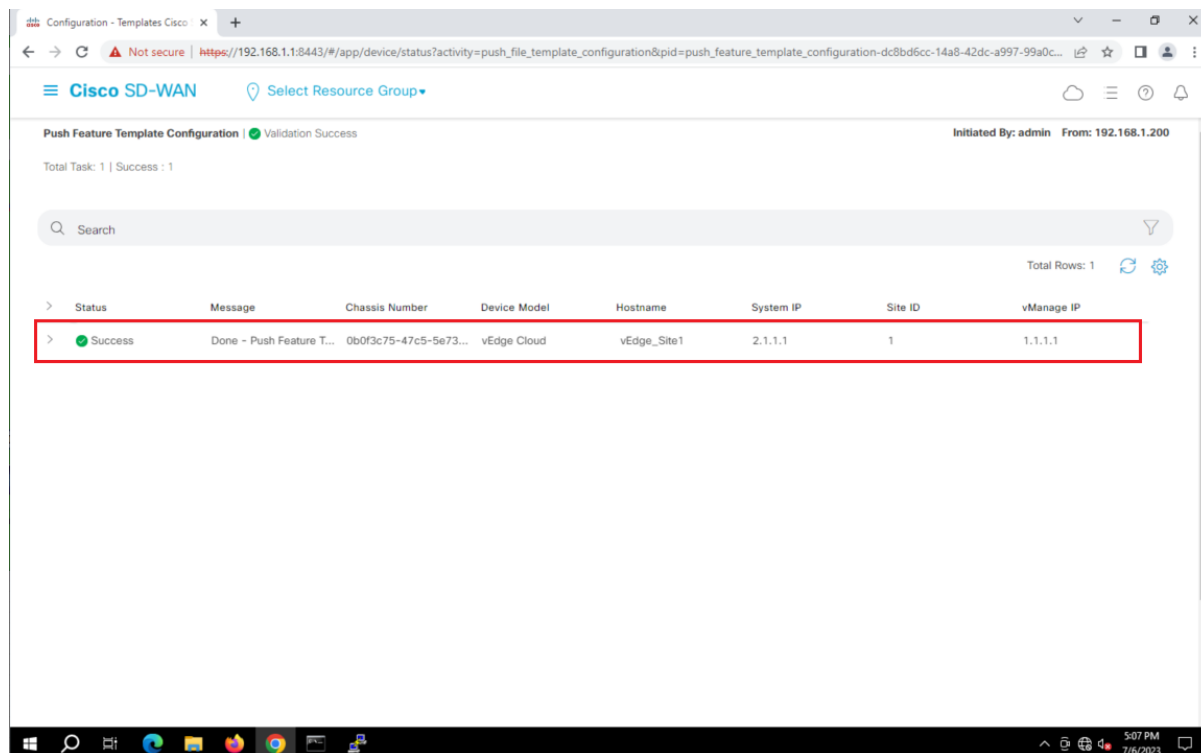
Total Rows: 1

S...	Chassis Number	System IP	Hostname	IPv4 Address(vpn11_ge0/3_if_ipv4_address)	Address Pool(dhcp_address_pool)	Default
✓	0b0f3c75-47c5-5e73-a557-9cf97c754274	2.1.1.1	vEdge_Site1	192.168.11.254/24	192.168.11.0/24	192.168.11.1

Next Cancel



Sau đó áp dụng cấu hình thành công xuống cho vEdge-Site1



Cấu hình Telnet cho router R1, R2

R1

username admin password admin

```
line vty 0 4
transport input telnet
login local
exit
```

R2

```
username admin password admin
line vty 0 4
transport input telnet
login local
exit
```

IV. Kiểm tra

Kiểm tra Ping

R1, R2 ping sang các thiết bị ở Site 1, **Host-1-1** và **Host-1-2**

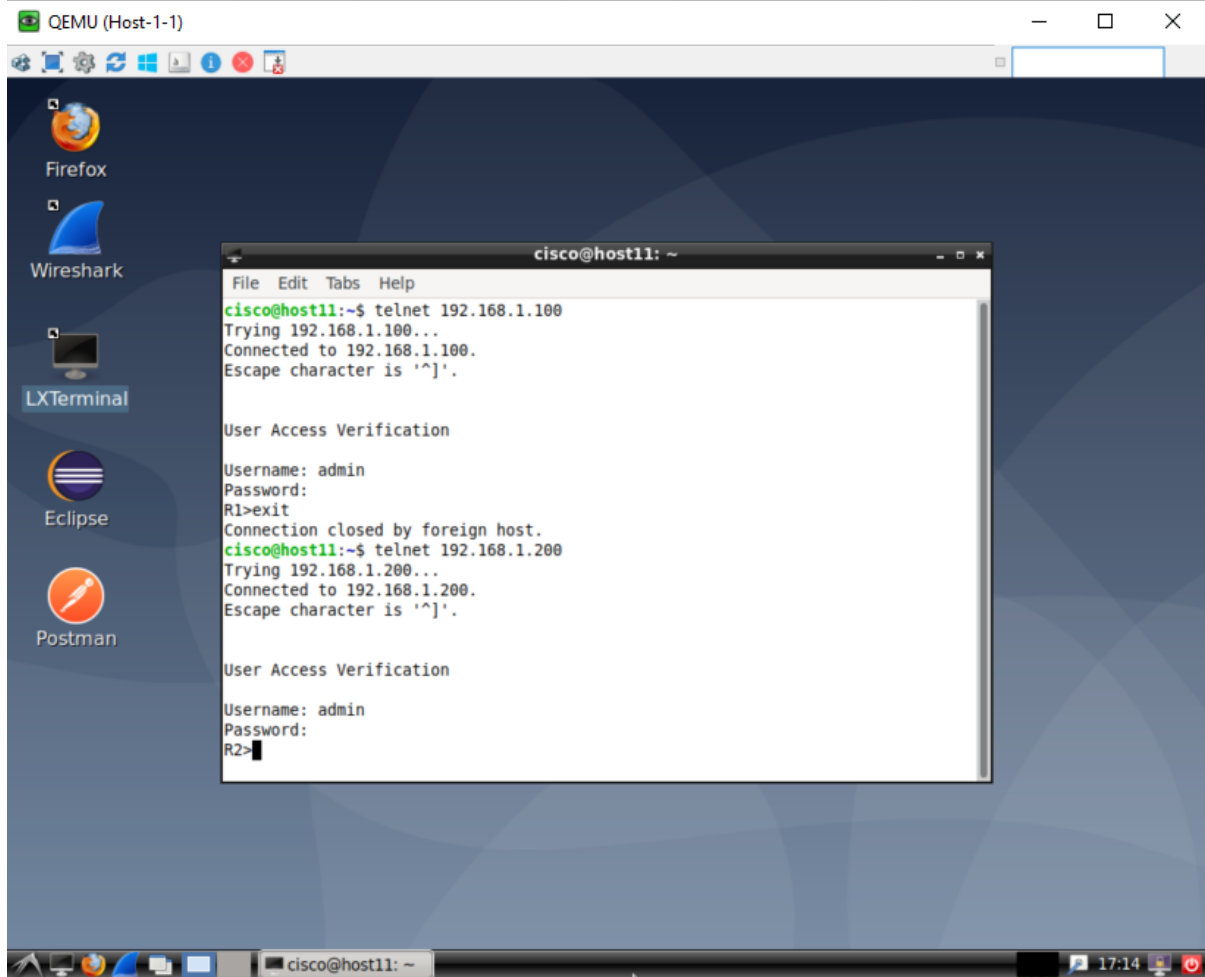
```
R1>ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
R1>ping 192.168.11.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 61/66/72 ms
R1>ping 192.168.10.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/58/61 ms
R1>ping 192.168.11.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 51/55/62 ms
R1>
```

```
R2>ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
R2>ping 192.168.11.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 63/69/71 ms
R2>ping 192.168.10.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.254, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 50/51/56 ms
R2>ping 192.168.11.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.254, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 46/57/62 ms
R2>■
```

Kiểm tra telnet

Trên **Host-1-1** ta tiến hành telnet tới **R1, R2**

Telnet tới thiết bị **R1, R2**



Trên **Host-1-2** ta tiến hành telnet tới **R1, R2**

Telnet tới thiết bị R1, R2

