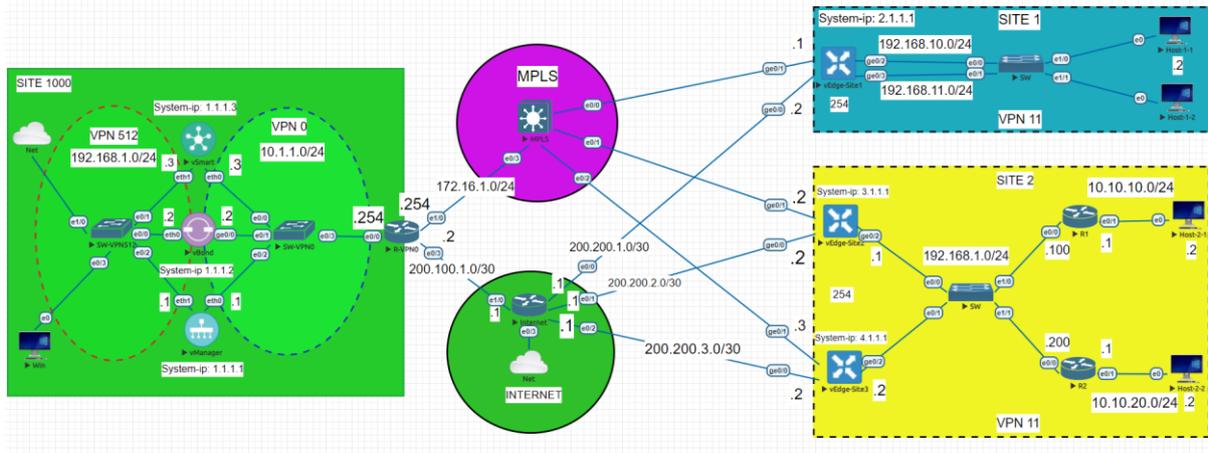


LAB - SỬ DỤNG ỨNG DỤNG TƯỜNG LỬA TRONG CISCO SD-WAN

I. Sơ đồ

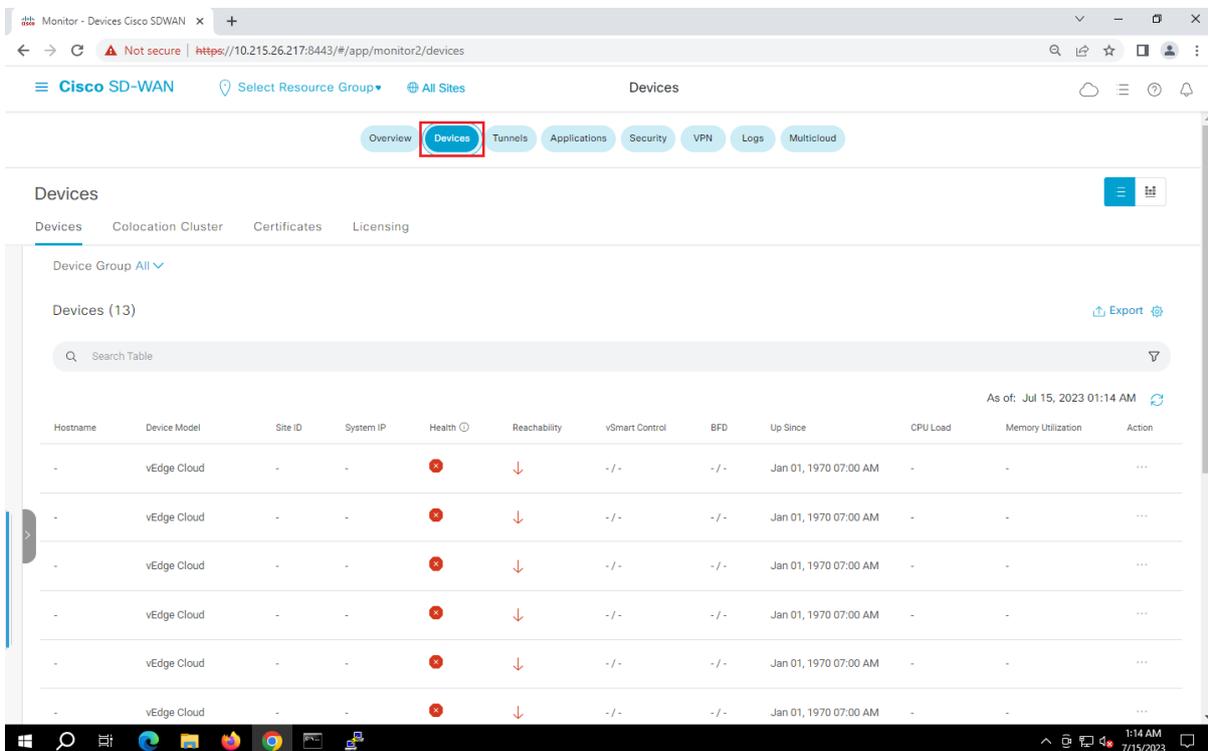


II. Yêu cầu kỹ thuật

- Sử dụng ứng dụng tường lửa để Host-1-1, Host-1-2 ở site 1 không thể dùng FTP để truyền file tới R1, R2 ở site 2.
- Tiến hành kiểm tra.

III. Các bước thực hiện

Vào **Monitor > Network** và chọn **vEdge-Site1**. Vào **Troubleshooting** và chọn công cụ **Simulated Flows**. Thiết lập các thông số như hình:



Monitor - Devices Cisco SDWAN

Not secure | https://10.215.26.217:8443/#/app/monitor2/devices

Cisco SD-WAN | Select Resource Group | All Sites | Devices

Device Name	Model	Serial	IP	Status	Direction	Uptime	Version	Config	Health	...
vEdge Cloud	-	-	-	Down	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-
vEdge Cloud	-	-	-	Down	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-
vEdge Cloud	-	-	-	Down	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-
vEdge Cloud	-	-	-	Down	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-
vEdge Cloud	-	-	-	Down	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-
vmanage	vManage	1000	1.1.1.1	Up	↑	1 / 1	0 / -	Jul 12, 2023 01:44 PM	3.98%	68%
vbond	vBond (vEdge Cloud)	1000	1.1.1.2	Up	↑	0 / 0	0 / -	Jul 12, 2023 01:44 PM	1.49%	64%
vSmart	vSmart	1000	1.1.1.3	Up	↑	0 / 0	0 / -	Jul 12, 2023 01:44 PM	0.56%	30%
vEdge-Site1	vEdge Cloud	1	2.1.1.1	Warning	↑	1 / 2	2 / 4	Jul 12, 2023 01:44 PM	2.6%	61%
vEdge1-Site2	vEdge Cloud	2	3.1.1.1	Warning	↑	2 / 2	1 / 2	Jul 12, 2023 01:44 PM	2.48%	60.2%
vEdge2-Site2	vEdge Cloud	2	4.1.1.1	Warning	↑	2 / 2	1 / 2	Jul 12, 2023 01:44 PM	2.46%	60.1%

Items per page: 25 | 1 - 13 of 13

Monitor - Devices Cisco SDWAN

Not secure | https://10.215.26.217:8443/#/app/monitor/devices/dashboard/troubleshooting?personality=vedge&systemIp=2.1.1.1&localSystemIp=2.1.1.1&deviceType=vedg...

Cisco SD-WAN | Select Resource Group | Devices | Device 360

Devices > Troubleshooting

Select Device: vEdge-Site1 | 2.1.1.1 | Site ID: 1 | Device Model: vEdge Cloud

Connectivity

Device Bringup

Control Connections(Live View)

Ping

Trace Route

Traffic

Tunnel Health

App Route Visualization

Simulate Flows

Flows

Top Talkers

WAN

TLOC

Tunnel

SECURITY MONITORING

Firewall

Intrusion Prevention

URL Filtering

Advanced Malware Protection

TLS/SSL Decryption

Umbrella DNS Re-direct

Control Connections

System Status

Events

ACL Logs

Troubleshooting

Real Time

VPN: VPN - 11
Source/Interface for VPN - 11: ge0/2 - ipv4 - 192.168.10.254
Source IP: 192.168.10.2
Destination IP: 192.168.1.100
Application: ftp

Advanced Options >

Simulate

Output:

Total next hops: 4 | IPsec : 4

Diagram showing traffic flow from source 2.1.1.1 through various tunnels (mpls, biz-Internet) to remote system IPs (3.1.1.1, 4.1.1.1) with IPsec encapsulation.

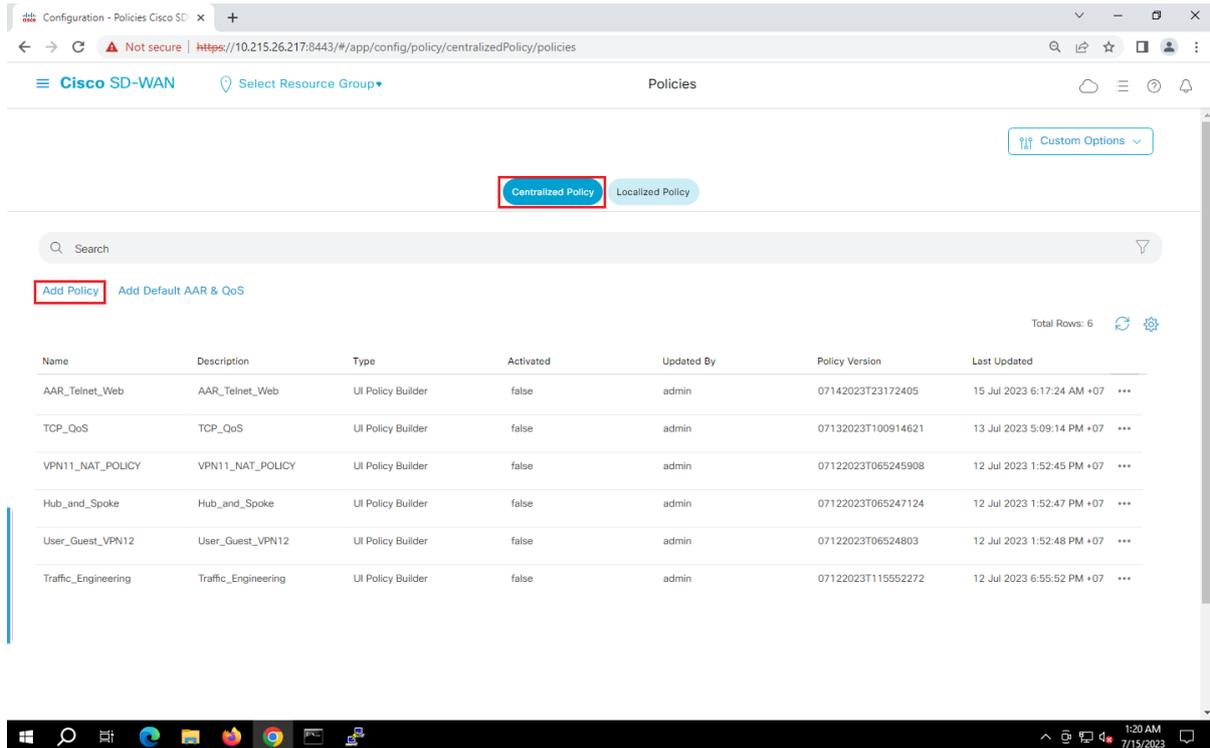
Vào Configuration>Policies. Vào mục Centralized Policy > Add Policy

Configuration - Policies Cisco SD-WAN

Configuration > Policies

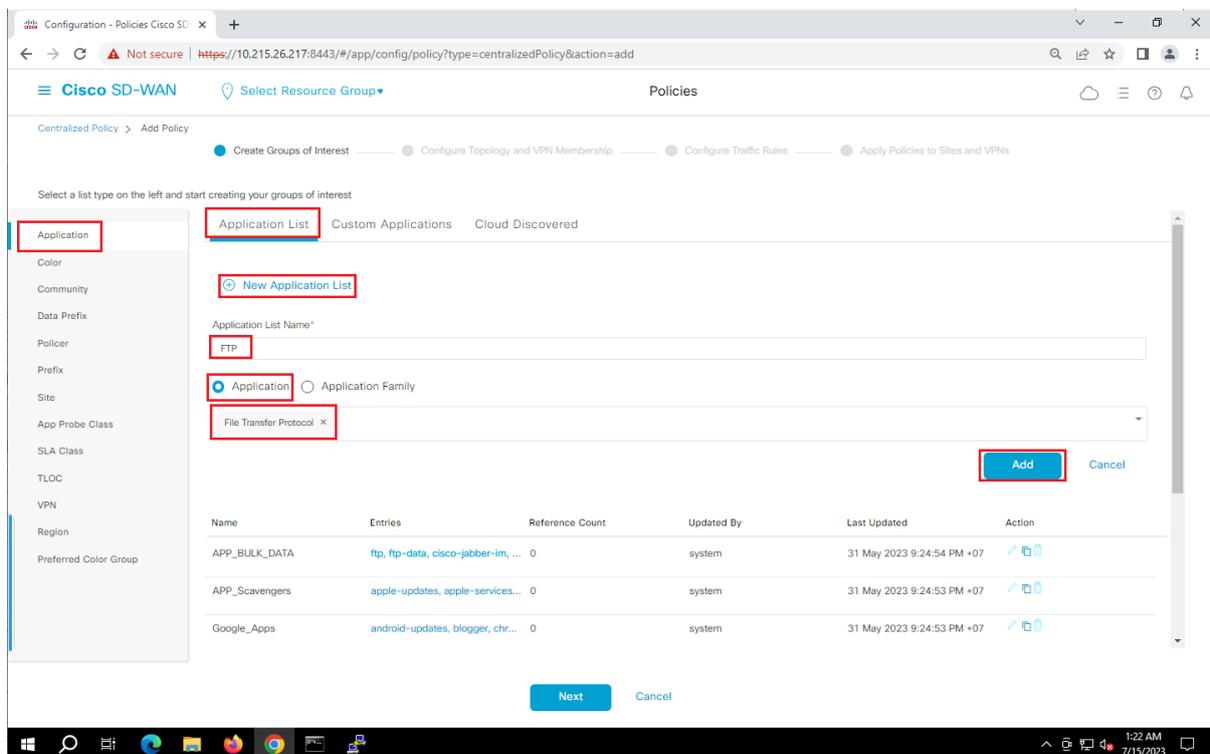
Centralized Policy Localized Policy

Activated	Updated By	Policy Version	Last Updated
false	admin	07142023T23172405	15 Jul 2023 6:17:24 AM +07 ...
false	admin	07132023T100914621	13 Jul 2023 5:09:14 PM +07 ...
false	admin	07122023T065245908	12 Jul 2023 1:52:45 PM +07 ...
false	admin	07122023T065247124	12 Jul 2023 1:52:47 PM +07 ...
false	admin	07122023T06524803	12 Jul 2023 1:52:48 PM +07 ...
false	admin	07122023T11552272	12 Jul 2023 6:55:22 PM +07 ...



Mục Create Groups of Internet lần lượt tạo các thư mục sau Application

- **Application List Name:** FTP
- **Application:** File Transfer Protocol
- **Chọn Add**



Site

- Site list Name: Site1-2
- Add Site: 1,2
- Chọn Add

The screenshot shows the Cisco SD-WAN configuration interface for adding a site list. The breadcrumb is "Centralized Policy > Add Policy". The page has four progress steps: "Create Groups of Interest" (active), "Configure Topology and VPN Membership", "Configure Traffic Rules", and "Apply Policies to Sites and VPNs". A sidebar on the left lists various configuration categories, with "Site" selected. The main area contains a "New Site List" form with the following fields: "Site List Name*" (Site1-2), "Add Site*" (1,2), and an "Add" button. Below the form is a table of existing site lists:

Name	Entries	Reference Count	Updated By	Last Updated	Action
Site1	1	7	admin	12 Jul 2023 1:52:35 PM +07	
Site2	2	4	admin	12 Jul 2023 1:52:35 PM +07	
Site3	3	4	admin	12 Jul 2023 1:52:36 PM +07	

At the bottom of the form, there are "Next" and "Cancel" buttons.

VPN:

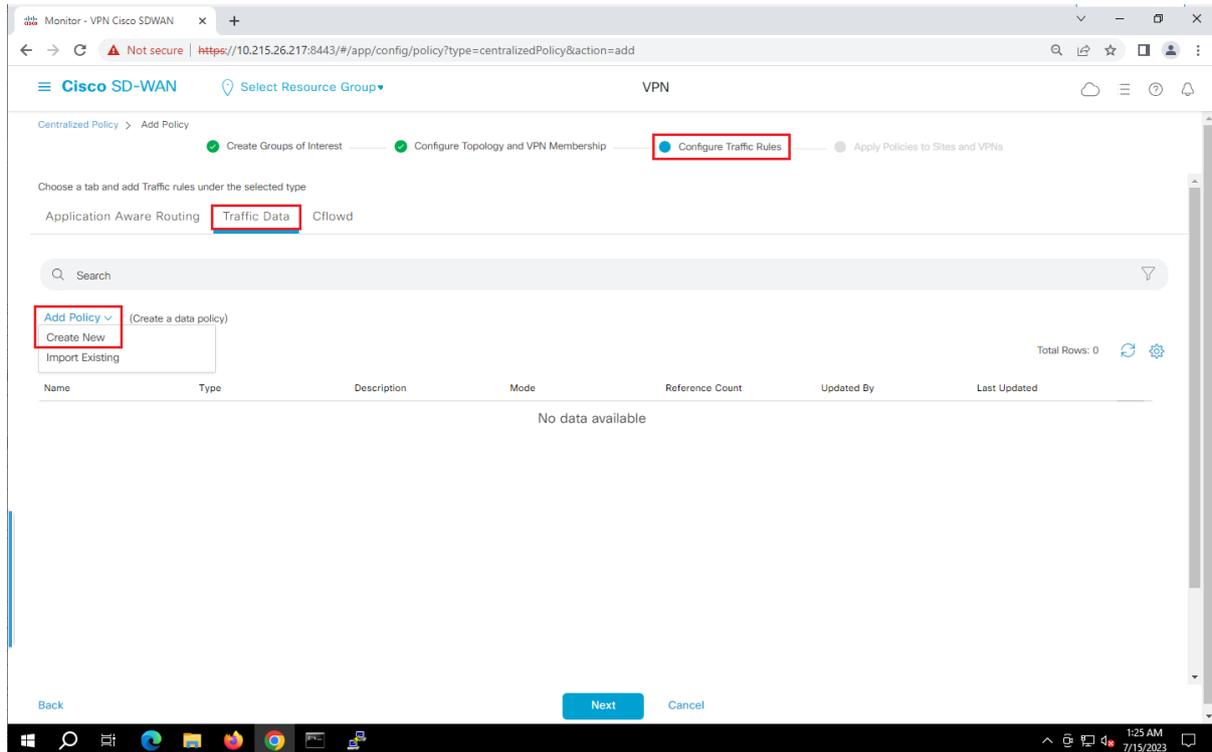
- Site list VPN: VPN11
- Add VPN: 11
- Chọn Add

The screenshot shows the Cisco SD-WAN configuration interface for adding a VPN list. The breadcrumb is "Centralized Policy > Add Policy". The page has four progress steps: "Create Groups of Interest" (active), "Configure Topology and VPN Membership", "Configure Traffic Rules", and "Apply Policies to Sites and VPNs". A sidebar on the left lists various configuration categories, with "VPN" selected. The main area contains a "New VPN List" table with the following entry highlighted in red:

Name	Entries	Reference Count	Updated By	Last Updated	Action
VPN11	11	8	admin	12 Jul 2023 1:52:36 PM +07	

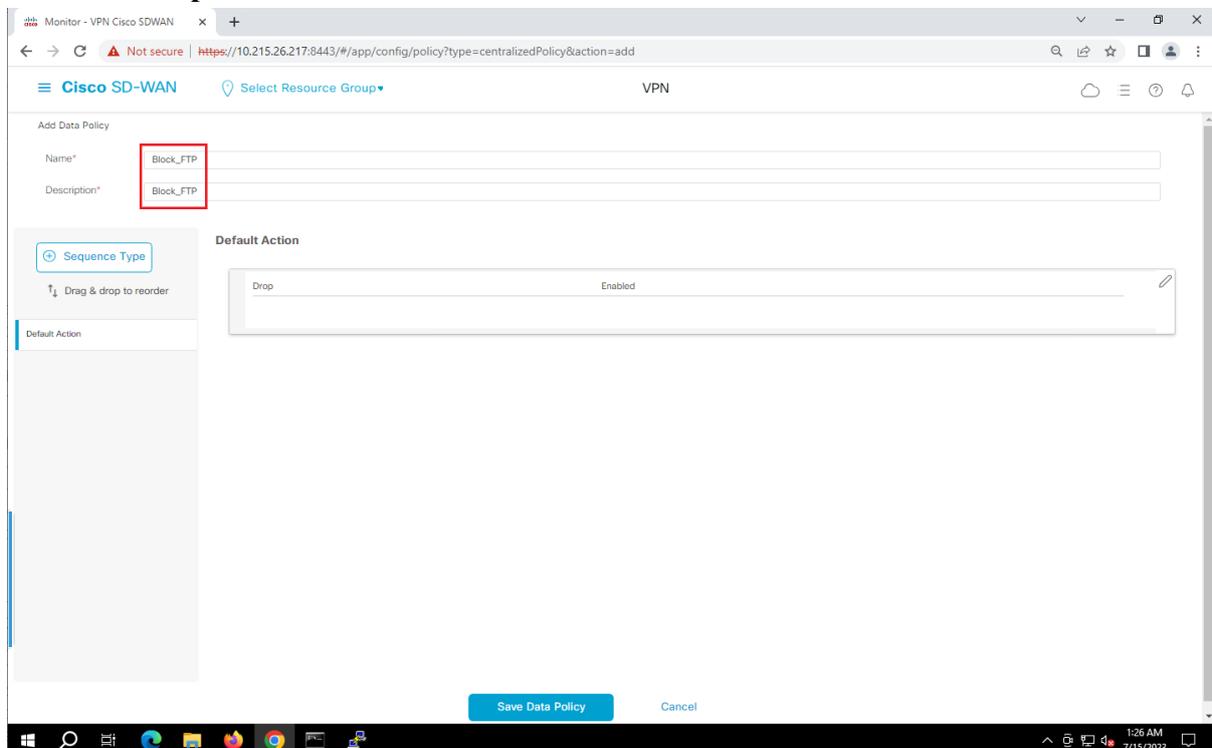
At the bottom of the form, there are "Next" and "Cancel" buttons.

Nhấn Next tới mục **Configure Traffic Rules > Traffic Data**. Chọn **Add Policy > Create New**

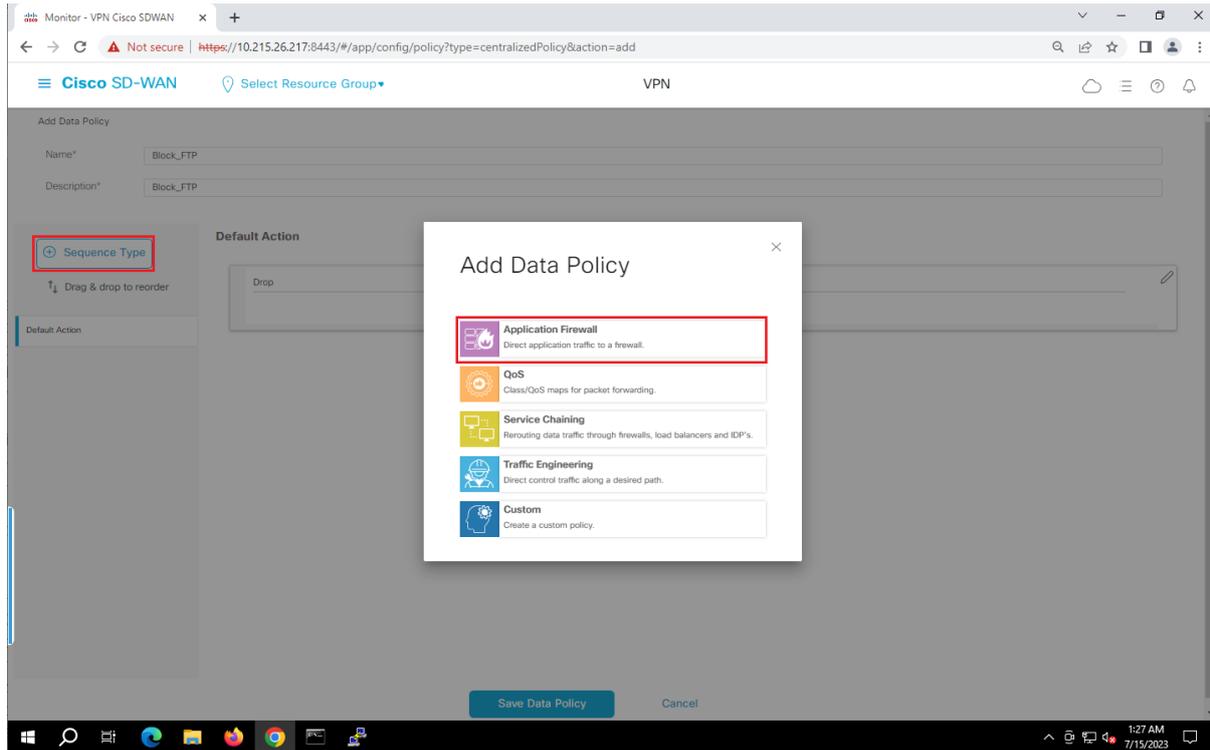


Trong phần **Add Data Policy**. Ta cấu hình lần lượt như sau:

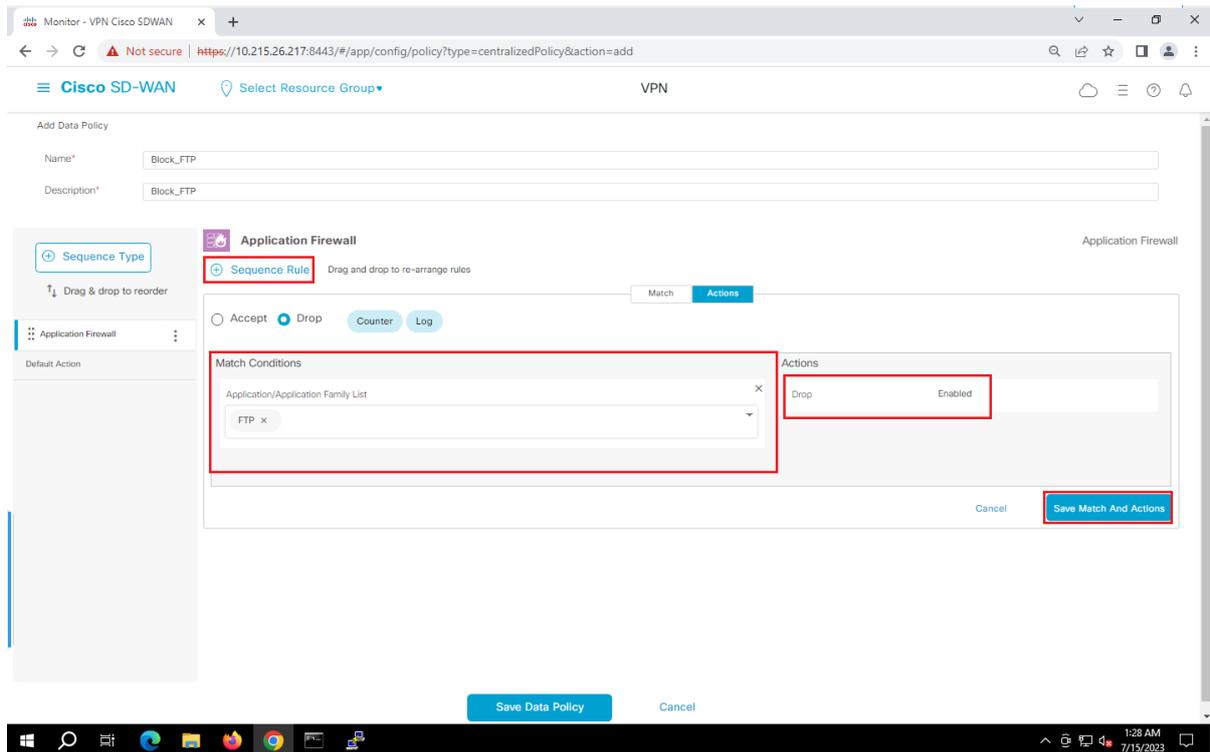
- **Name:** Block-FTP
- **Description:** Block-FTP



Chọn **Sequence Type > Application Firewall**

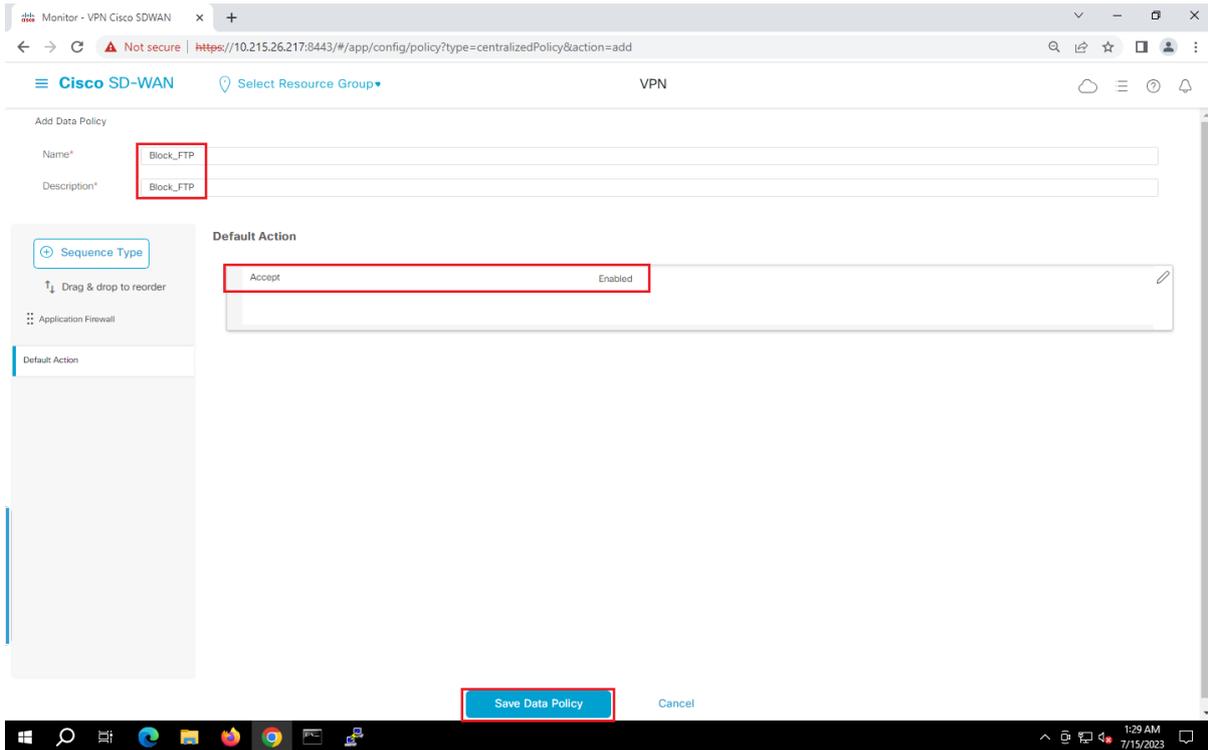


Chọn Sequence Rule > Match > Application/ Application Family List. Chọn FTP

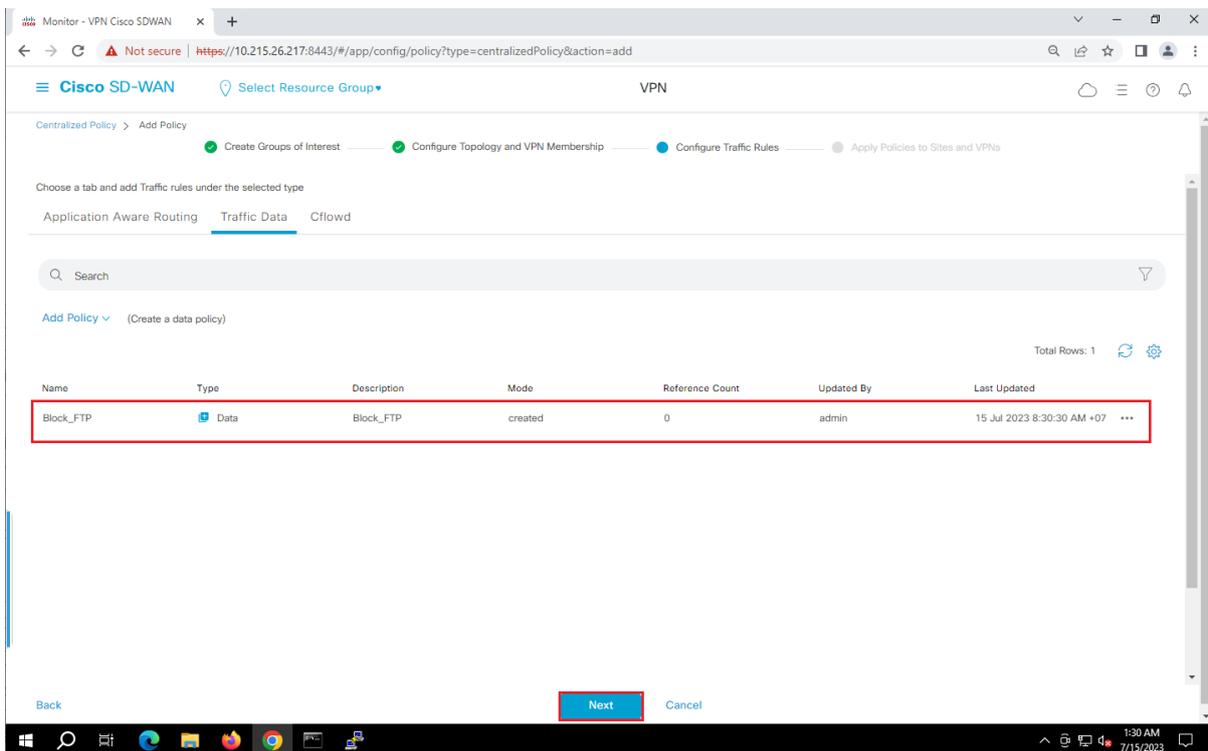


Chọn Save Match And Actions.

Default Action > Accept. Chọn Save Match And Actions.



Save Data Policy.



Nhấn Next đến mục **Apply Policies to Sites and VPNs.**

Policy Name: App_Firewall

Policy Description: App_Firewall

Mục **Traffic Data** > **All**

Select **Site List**: Site1-2

Select **VPN List**: VPN11

Nhấn **Add**

Nhấn **Save Policy**

Vào lại **Configuration** > **Policies**. Chọn mục **Centralized Policy** > **App-Firewall**.

Chọn Activale.

Centralized Policy Localized Policy

Search

Add Policy Add Default AAR & QoS

Total Rows: 7

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
AAR_Telnet_Web	AAR_Telnet_Web	UI Policy Builder	false	admin	07142023T23172405	15 Jul 2023 6:17:24 AM +07
TCP_QoS	TCP_QoS	UI Policy Builder	false	admin	07132023T100914621	13 Jul 2023 5:09:14 PM +07
VPN11_NAT_POLICY	VPN11_NAT_POLICY	UI Policy Builder	false	admin	07122023T065245908	12 Jul 2023 1:52:45 PM +07
Hub_and_Spoke	Hub_and_Spoke	UI Policy Builder	false	admin	07122023T065247124	12 Jul 2023 1:52:47 PM +07
User_Guest_VPN12	User_Guest_VPN12	UI Policy Builder	false	admin	07122023T06524803	12 Jul 2023 1:52:48 PM +07
App_Firewall	App_Firewall	UI Policy Builder	false	admin	07152023T013424123	15 Jul 2023 8:34:24 AM +07
Traffic_Engineering	Traffic_Engineering	UI Policy Builder	false	admin	07122023T115552272	12 Jul 2023 6:55:52 PM +07

View
Preview
Copy
Edit
Delete
Activate

Centralized Policy Localized Policy

Search

Add Policy Add Default AAR & QoS

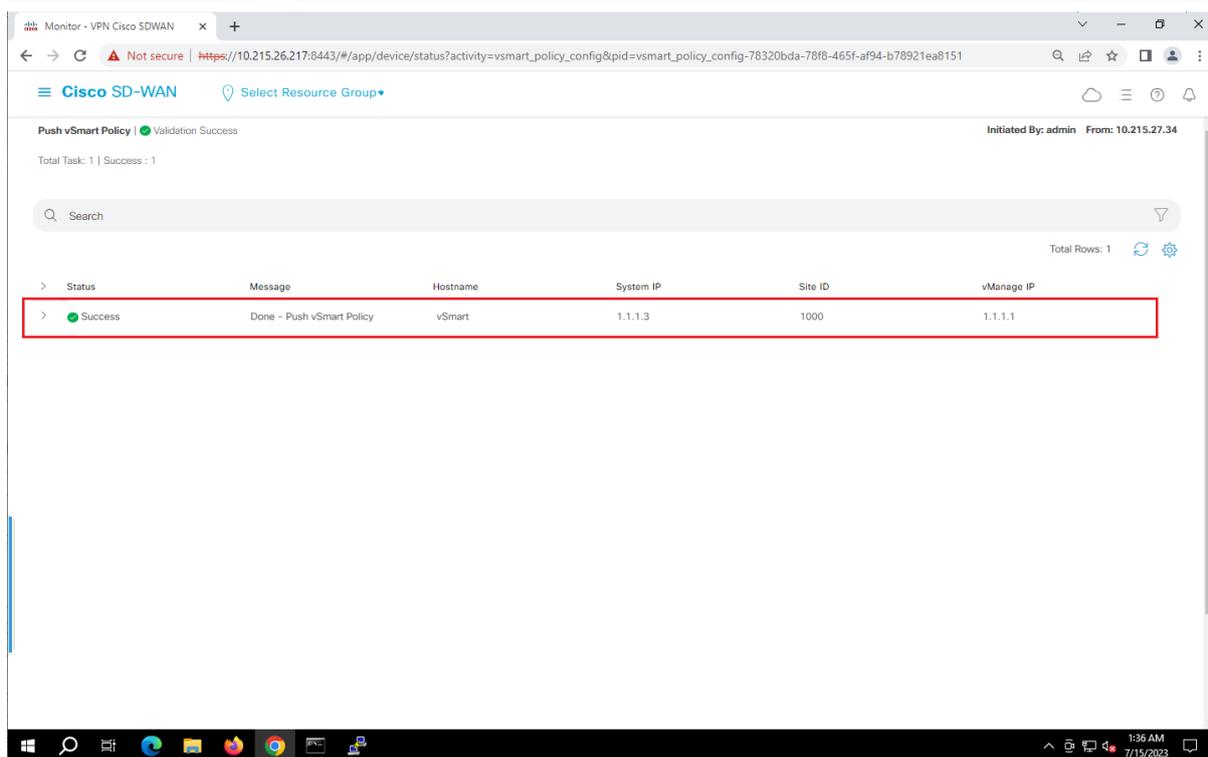
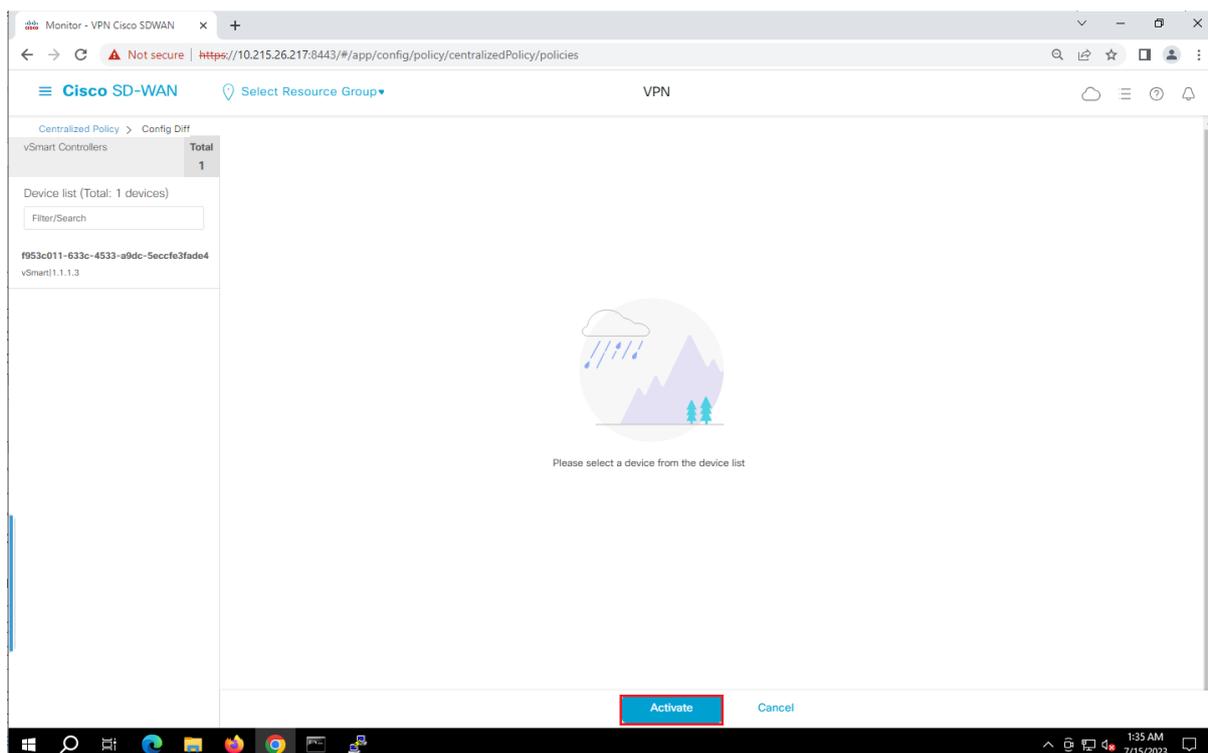
Total Rows: 7

Activate Policy

Policy will be applied to the reachable vSmarts:
1.1.1.3

Activate Cancel

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
AAR_Telnet_Web	AAR_Telnet_Web	UI Policy Builder	false	admin	07142023T23172405	15 Jul 2023 6:17:24 AM +07
TCP_QoS	TCP_QoS	UI Policy Builder	false	admin	07132023T100914621	13 Jul 2023 5:09:14 PM +07
VPN11_NAT_POLICY	VPN11_NAT_POLICY	UI Policy Builder	false	admin	07122023T065245908	12 Jul 2023 1:52:45 PM +07
Hub_and_Spoke	Hub_and_Spoke	UI Policy Builder	false	admin	07122023T065247124	12 Jul 2023 1:52:47 PM +07
User_Guest_VPN12	User_Guest_VPN12	UI Policy Builder	false	admin	07122023T06524803	12 Jul 2023 1:52:48 PM +07
App_Firewall	App_Firewall	UI Policy Builder	false	admin	07152023T013424123	15 Jul 2023 8:34:24 AM +07
Traffic_Engineering	Traffic_Engineering	UI Policy Builder	false	admin	07122023T115552272	12 Jul 2023 6:55:52 PM +07



IV. Kiểm tra

Kiểm tra bằng cách vào lại Monitor > Network và chọn vEdge-Site1. Vào Troubleshooting và chọn công cụ the Simulated Flows. Thiết lập các thông số như bước 1.

Monitor - Devices Cisco SDWAN x +
 Not secure | https://10.215.26.217:8443/#/app/monitor2/devices

Cisco SD-WAN Select Resource Group All Sites Devices

Overview **Devices** Tunnels Applications Security VPN Logs Multicloud

Devices

Devices Colocation Cluster Certificates Licensing

Device Group All

Devices (13) Export

Search Table

As of: Jul 15, 2023 01:14 AM

Hostname	Device Model	Site ID	System IP	Health	Reachability	vSmart Control	BFD	Up Since	CPU Load	Memory Utilization	Action
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...

Monitor - Devices Cisco SDWAN x +
 Not secure | https://10.215.26.217:8443/#/app/monitor2/devices

Cisco SD-WAN Select Resource Group All Sites Devices

-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
-	vEdge Cloud	-	-	✖	↓	-/-	-/-	Jan 01, 1970 07:00 AM	-	-	...
vmanage	vManage	1000	1.1.1.1	✔	↑	1 / 1	0 / -	Jul 12, 2023 01:44 PM	3.98%	68%	...
vbond	vBond (vEdge Cloud)	1000	1.1.1.2	✔	↑	0 / 0	0 / -	Jul 12, 2023 01:44 PM	1.49%	64%	...
vSmart	vSmart	1000	1.1.1.3	✔	↑	0 / 0	0 / -	Jul 12, 2023 01:44 PM	0.56%	30%	...
vEdge-Site1	vEdge Cloud	1	2.1.1.1	⚠	↑	1 / 2	2 / 4	Jul 12, 2023 01:44 PM	2.6%	61%	...
vEdge1-Site2	vEdge Cloud	2	3.1.1.1	⚠	↑	2 / 2	1 / 2	Jul 12, 2023 01:44 PM	2.48%	60.2%	...
vEdge2-Site2	vEdge Cloud	2	4.1.1.1	⚠	↑	2 / 2	1 / 2	Jul 12, 2023 01:44 PM	2.46%	60.1%	...

Items per page: 25 1 - 13 of 13

The screenshot shows the Cisco SD-WAN Troubleshooting dashboard for Device 360. The left sidebar contains a navigation menu with 'Troubleshooting' highlighted. The main area is divided into two sections: 'Connectivity' and 'Traffic'. Under 'Connectivity', there are links for 'Device Bringup', 'Control Connections(Live View)', 'Ping', and 'Trace Route'. Under 'Traffic', there are links for 'Tunnel Health', 'App Route Visualization', and 'Simulate Flows' (which is highlighted with a red box).

The screenshot shows the 'Simulate Flows' configuration page. A table defines the flow parameters:

VPN	Source/Interface for VPN - 11	Source IP	Destination IP	Application
VPN - 11	ge0/2 - ipv4 - 192.168.10.254	192.168.10.2	192.168.1.100	ftp

Below the table, there is an 'Advanced Options' section and a 'Simulate' button (highlighted with a red box). The 'Output' section shows a network diagram with a source node, a router node labeled '2.1.1.1', and a destination node labeled 'Blackhole' with a red 'X' icon. The text 'Total next hops: 1 | Blackhole : 1' is displayed to the right of the diagram.