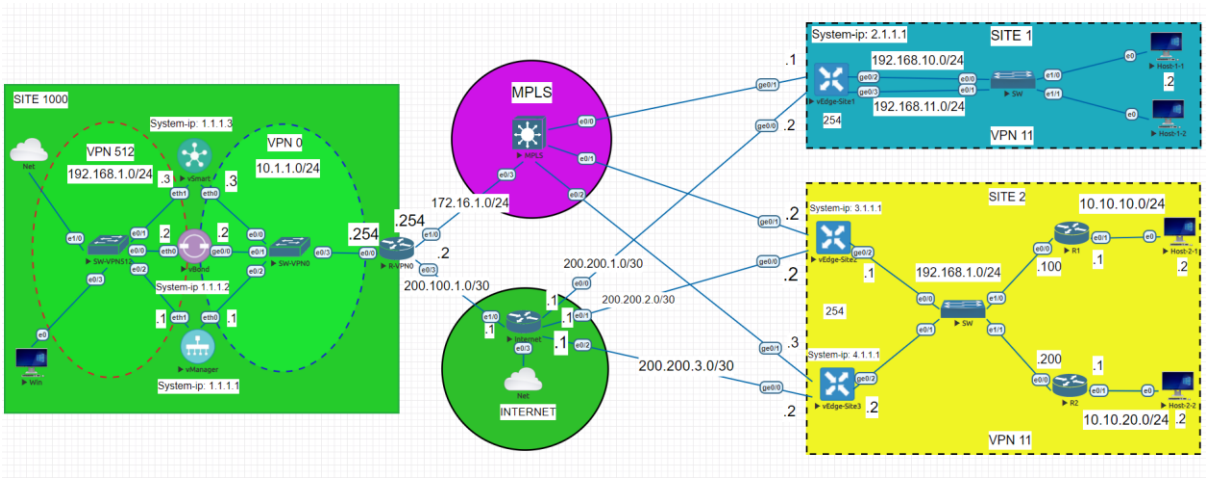
LAB - SỬ DỤNG ỨNG DỤNG TƯỜNG LỬA TRONG CISCO SD-WAN

I. Sơ đồ

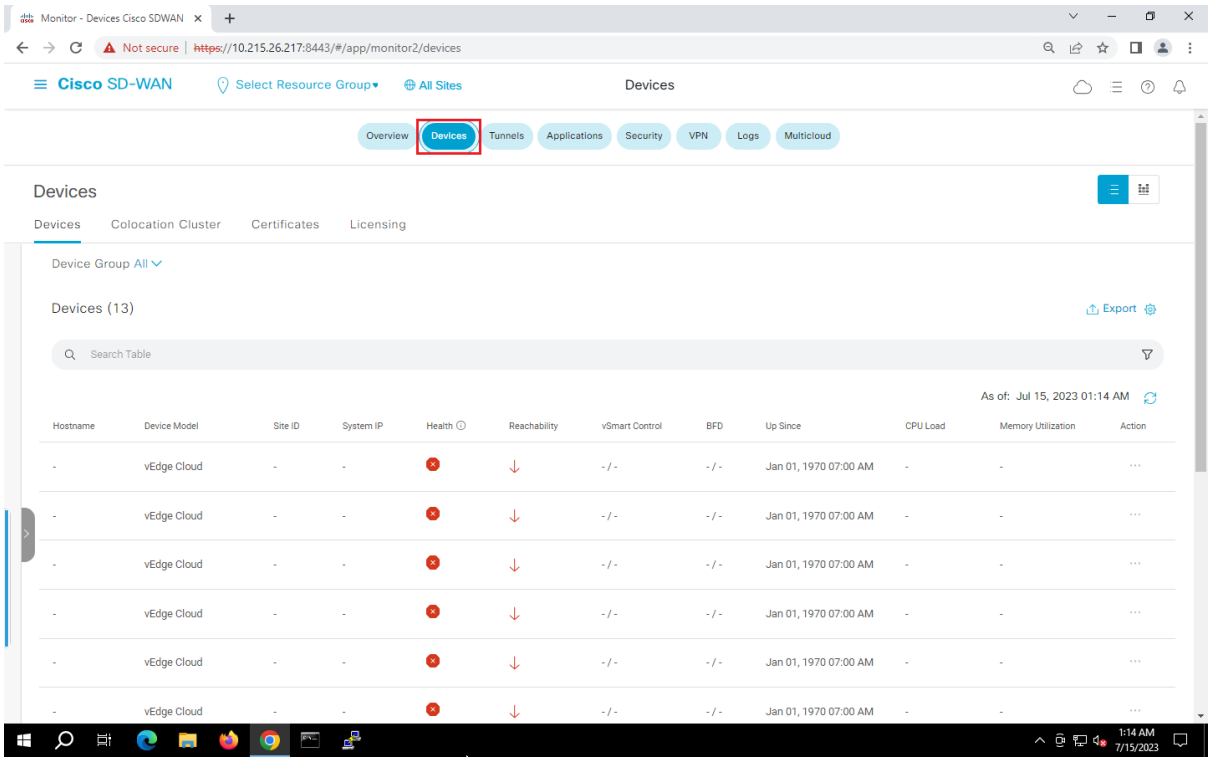


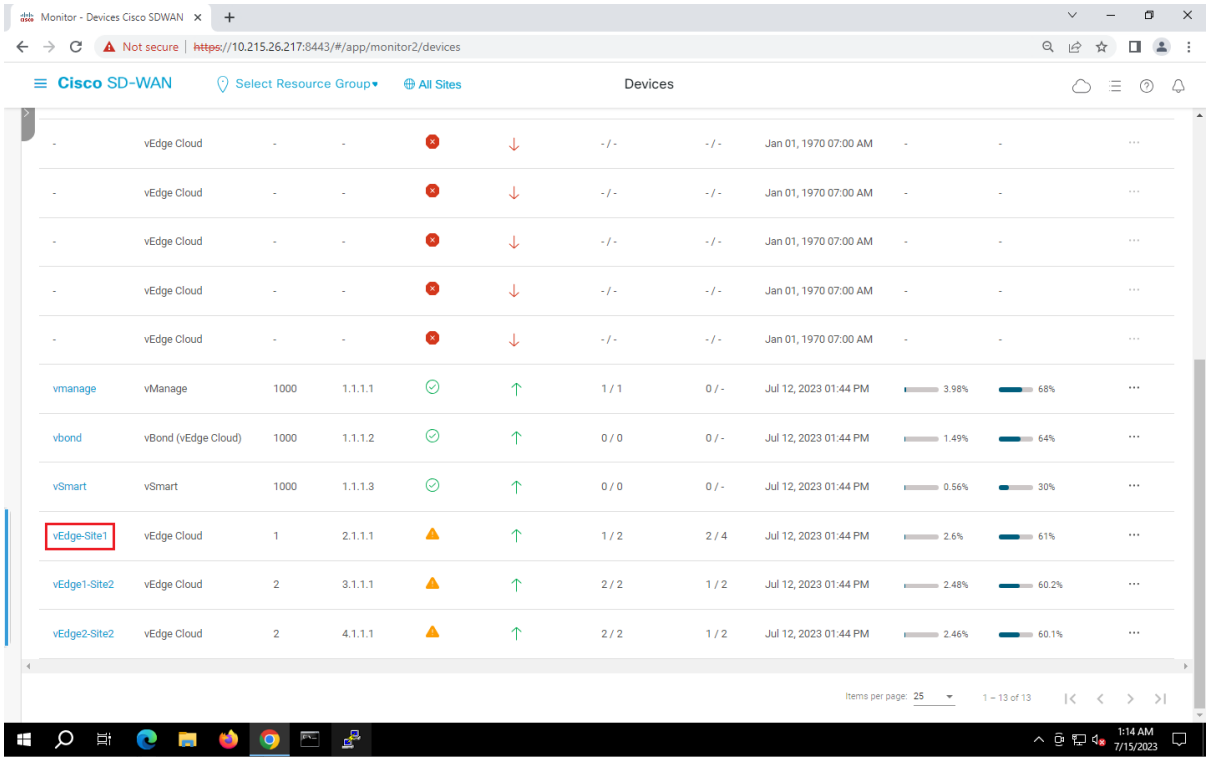
II. Yêu cầu kỹ thuật

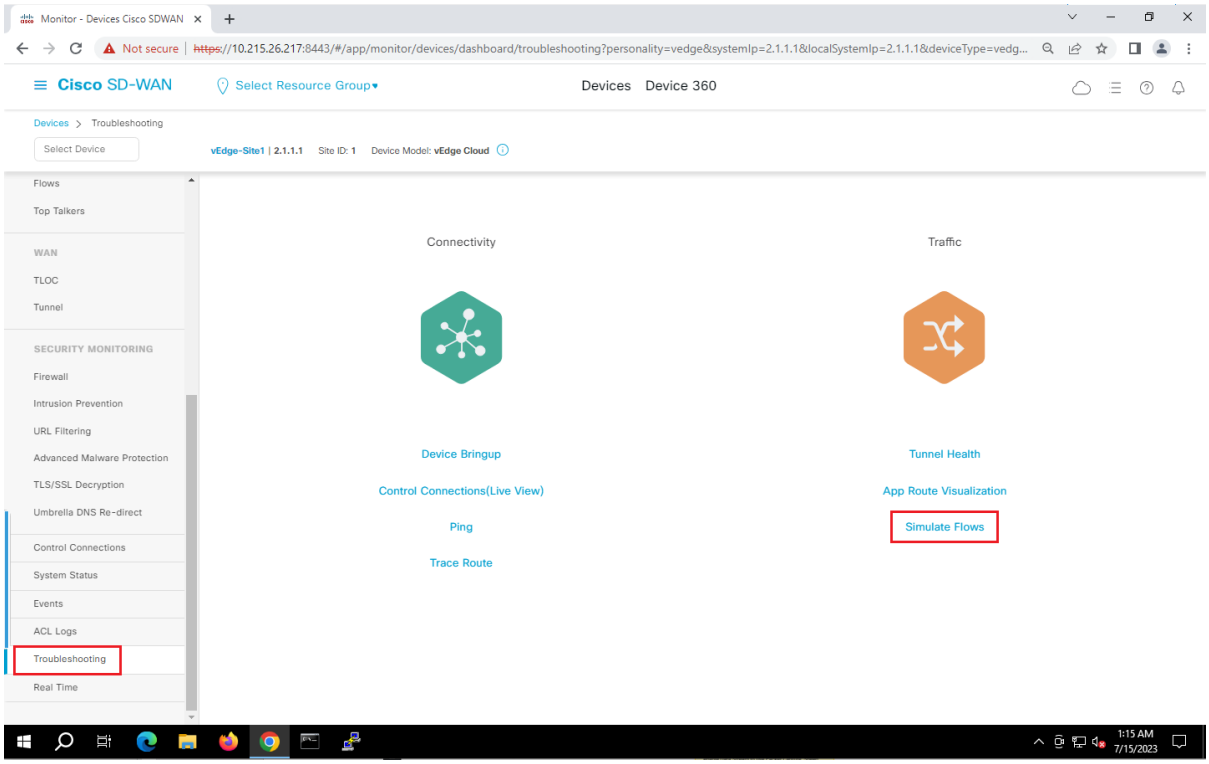
- Sử dụng ứng dụng tường lửa để Host-1-1, Host-1-2 ở site 1 không thể dùng FTP để truyền file tới R1, R2 ở site 2.
- Tiến hành kiểm tra.

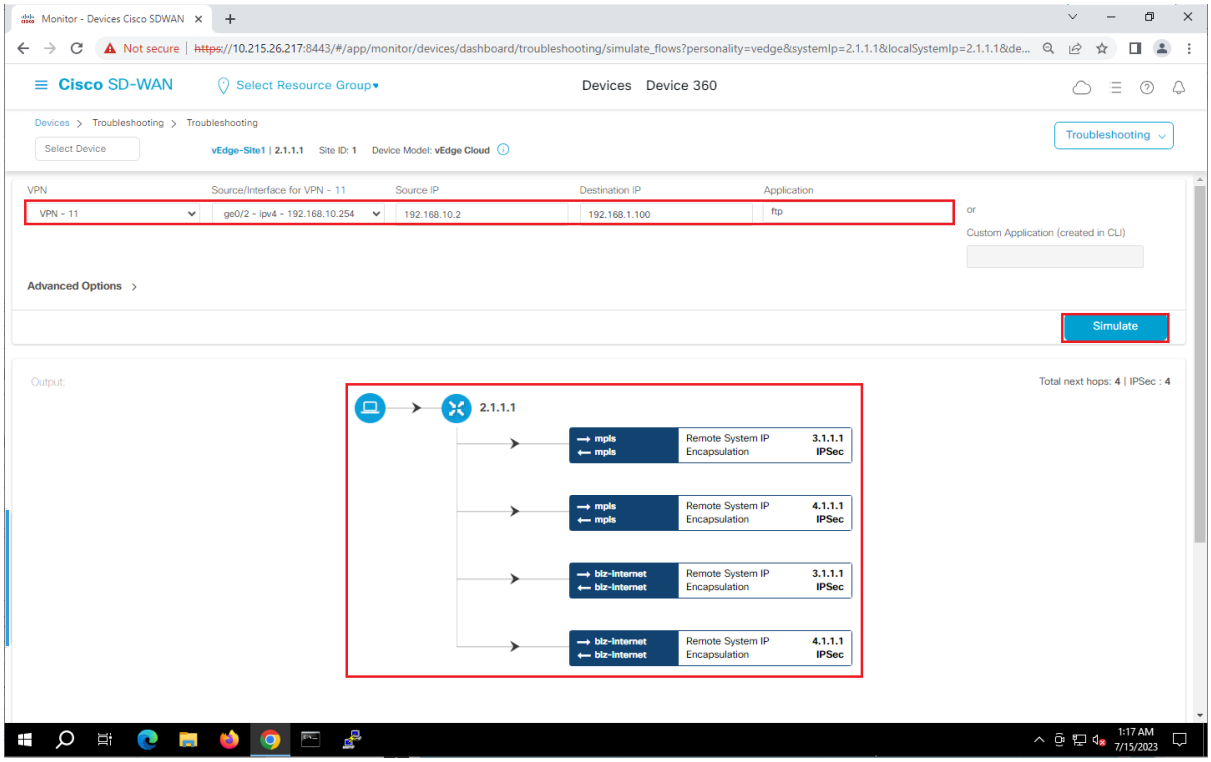
III. Các bước thực hiện

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

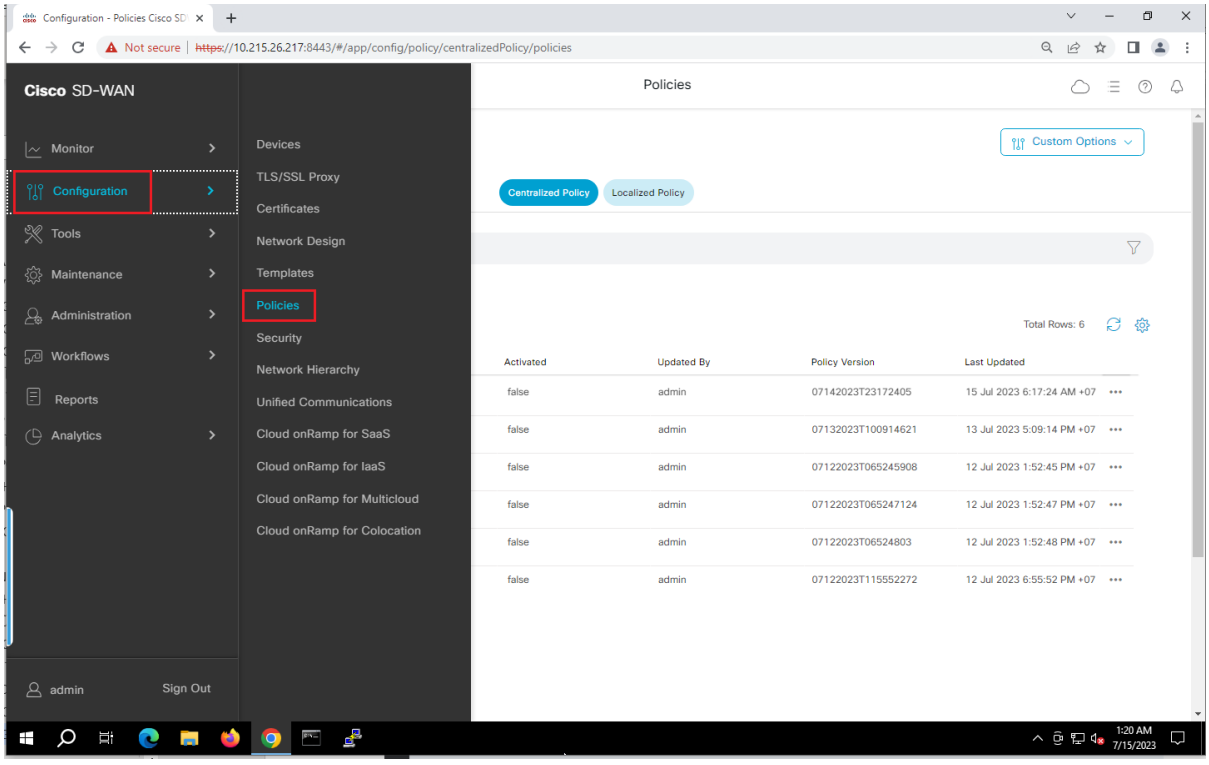


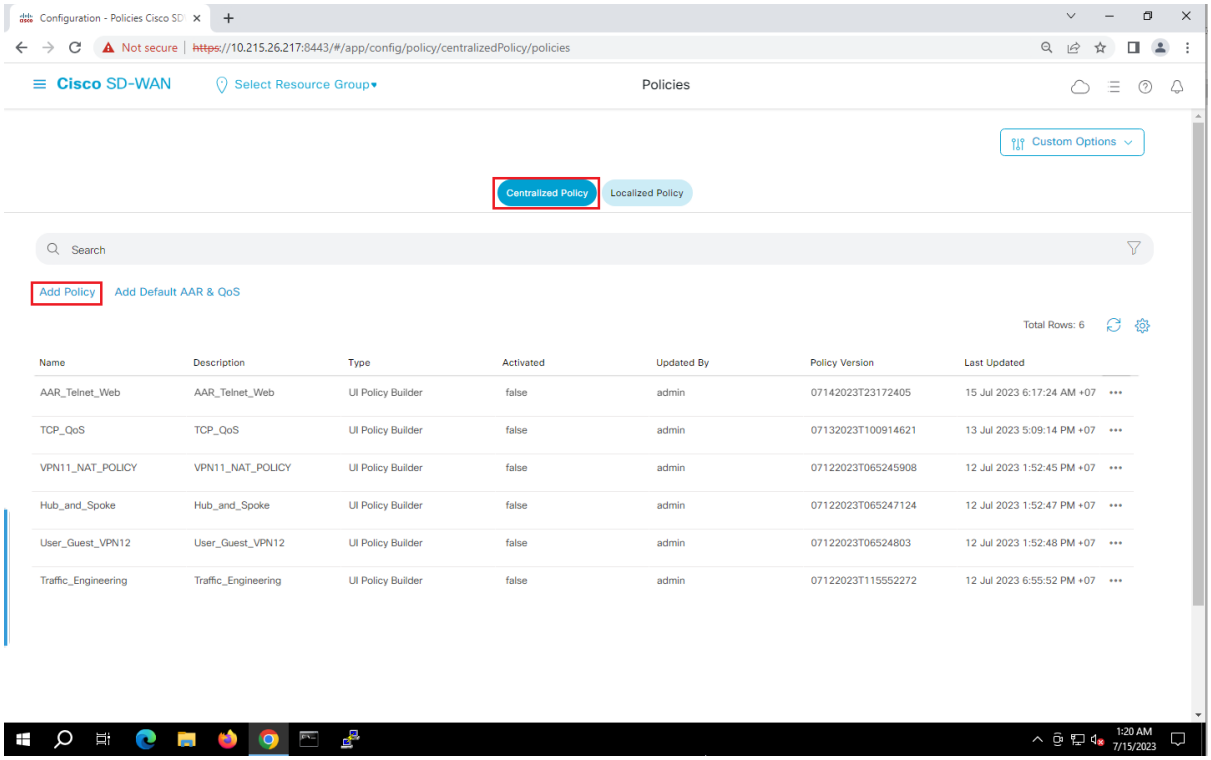

Monitor - Devices Cisco SDWAN
Not secure | https://10.215.26.217:8443/#/app/monitor2/devices
Cisco SD-WAN
Select Resource Group
All Sites
Devices
vmanage vManage 1000 1.1.1.1 1 / 1 0 / - Jul 12, 2023 01:44 PM 3.98% 68%
vbond vBond (vEdge Cloud) 1000 1.1.1.2 0 / 0 0 / - Jul 12, 2023 01:44 PM 1.49% 64%
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
1:14 AM
7/15/2023


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
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
Connectivity
Device Bringup
Control Connections(Live View)
Ping
Trace Route
Traffic
Tunnel Health
App Route Visualization
Simulate Flows
1:15 AM
7/15/2023



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

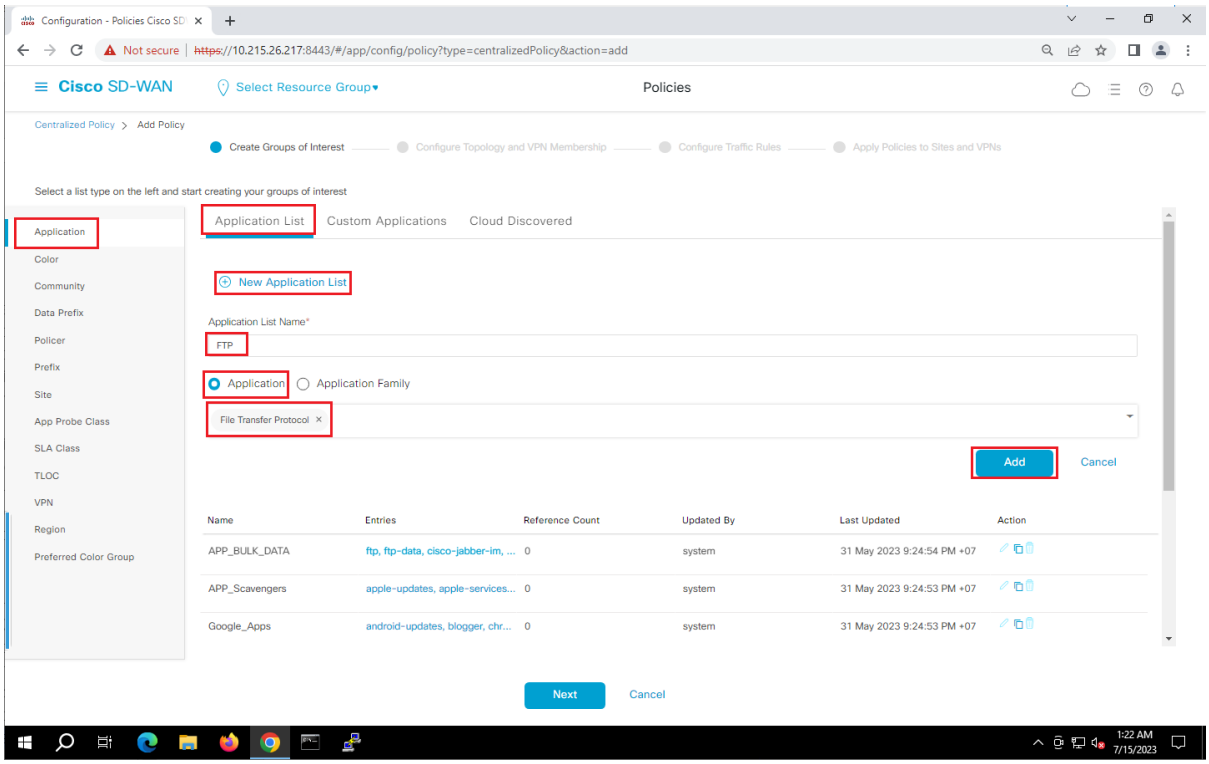




Mục **Create Groups of Internet** lần lượt tạo các thư mục sau

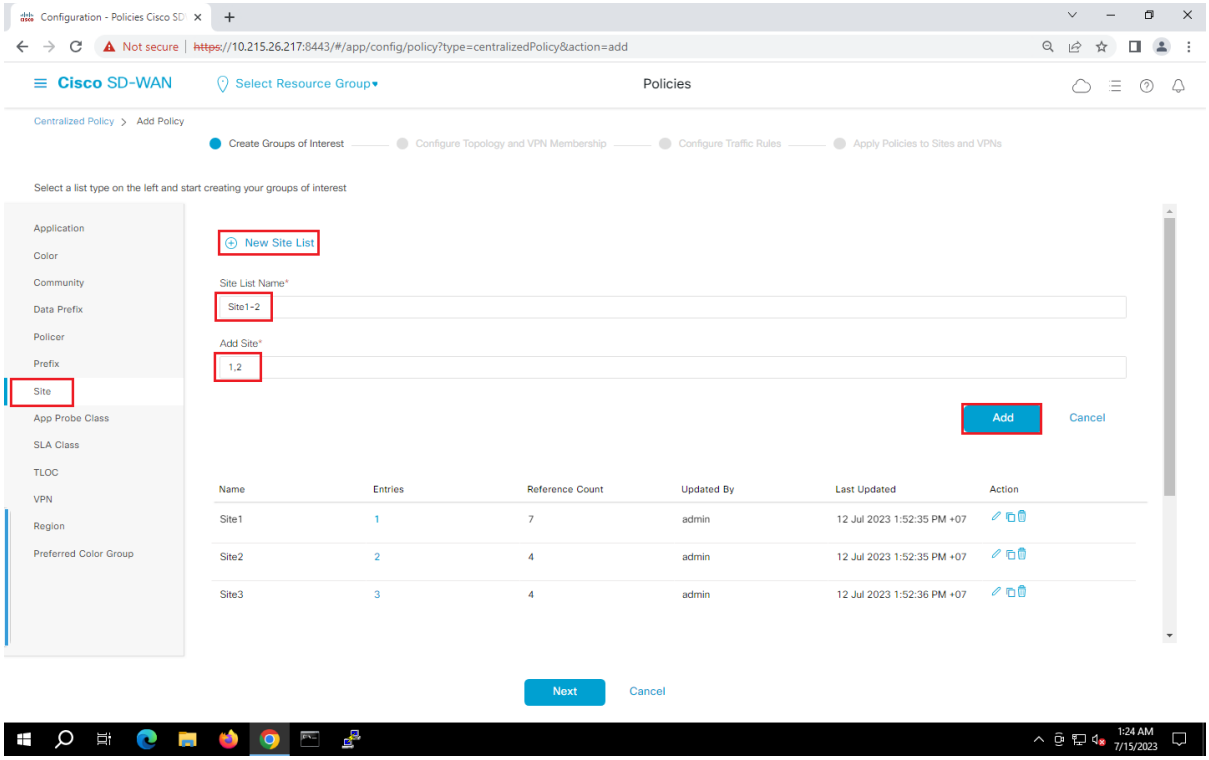
Application

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



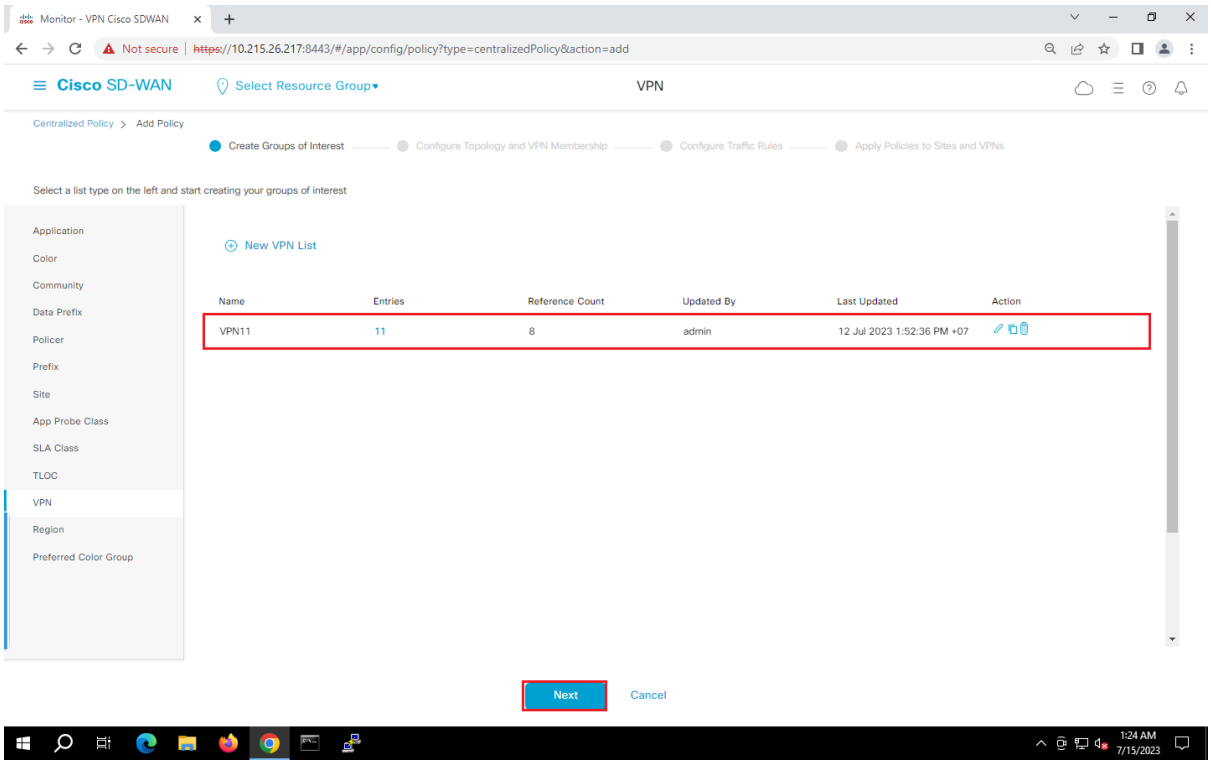
Site

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

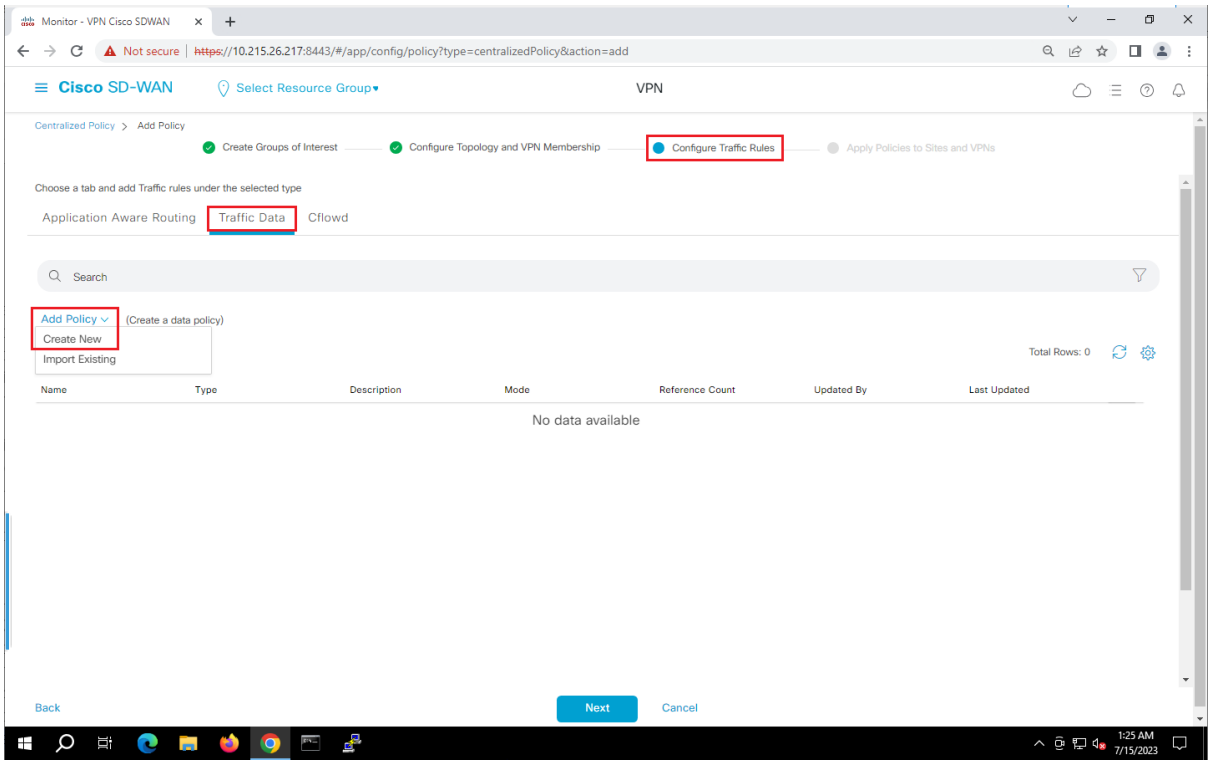


VPN:

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

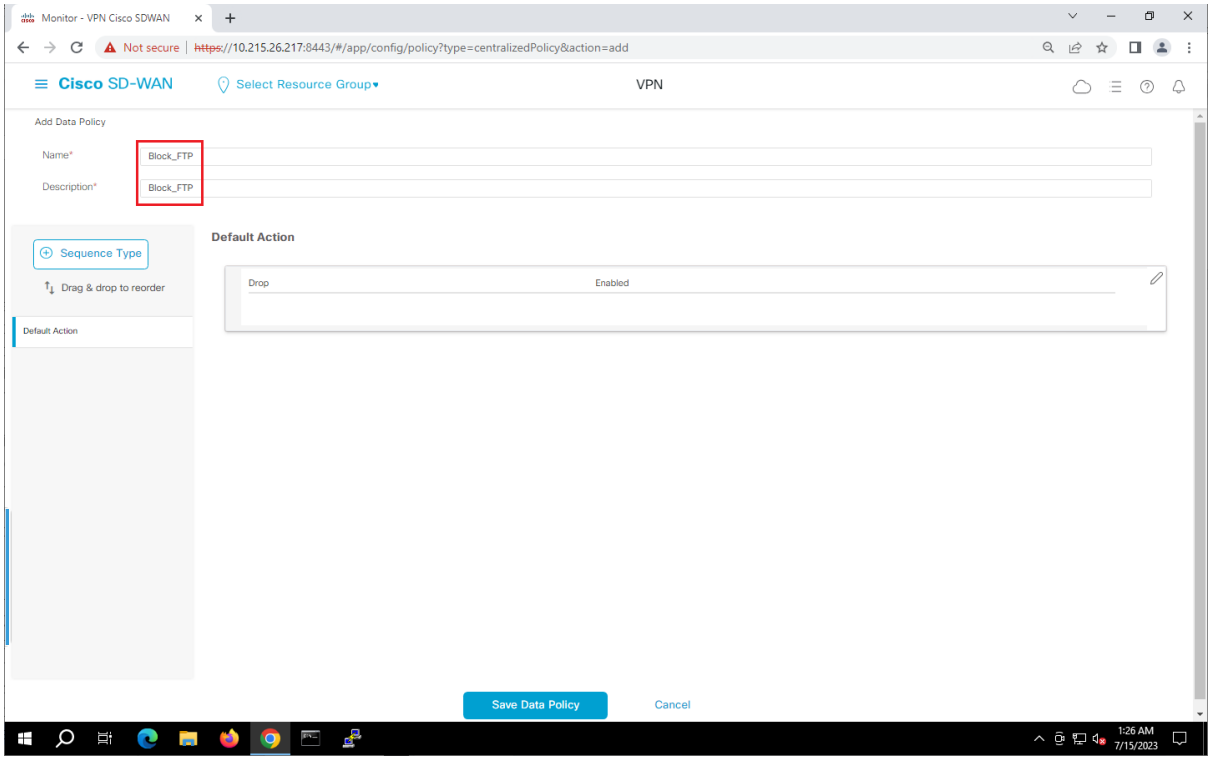


Nhấn Next tới mục **Configure Traffic Rules > Traffic Data**. Chọn **Add Policy > Create New**

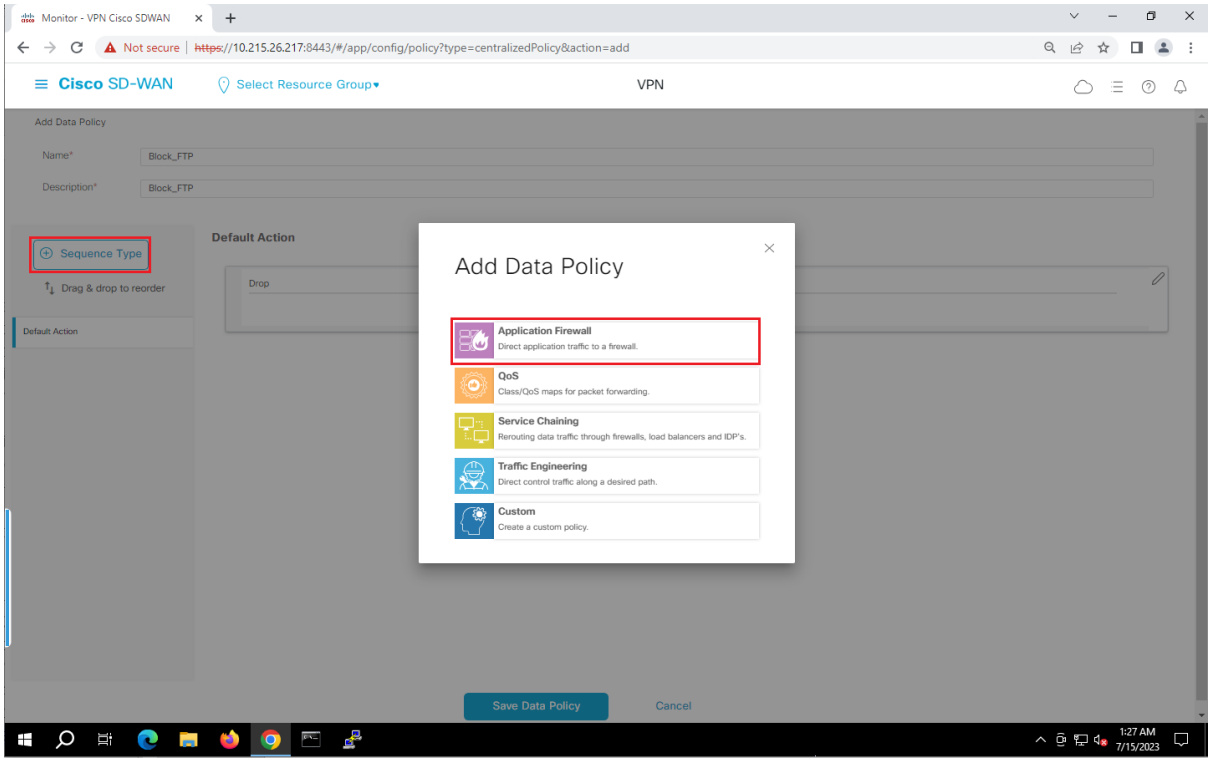


Trong phần **Add Data Policy**. Ta cấu hình lần lượt như sau:

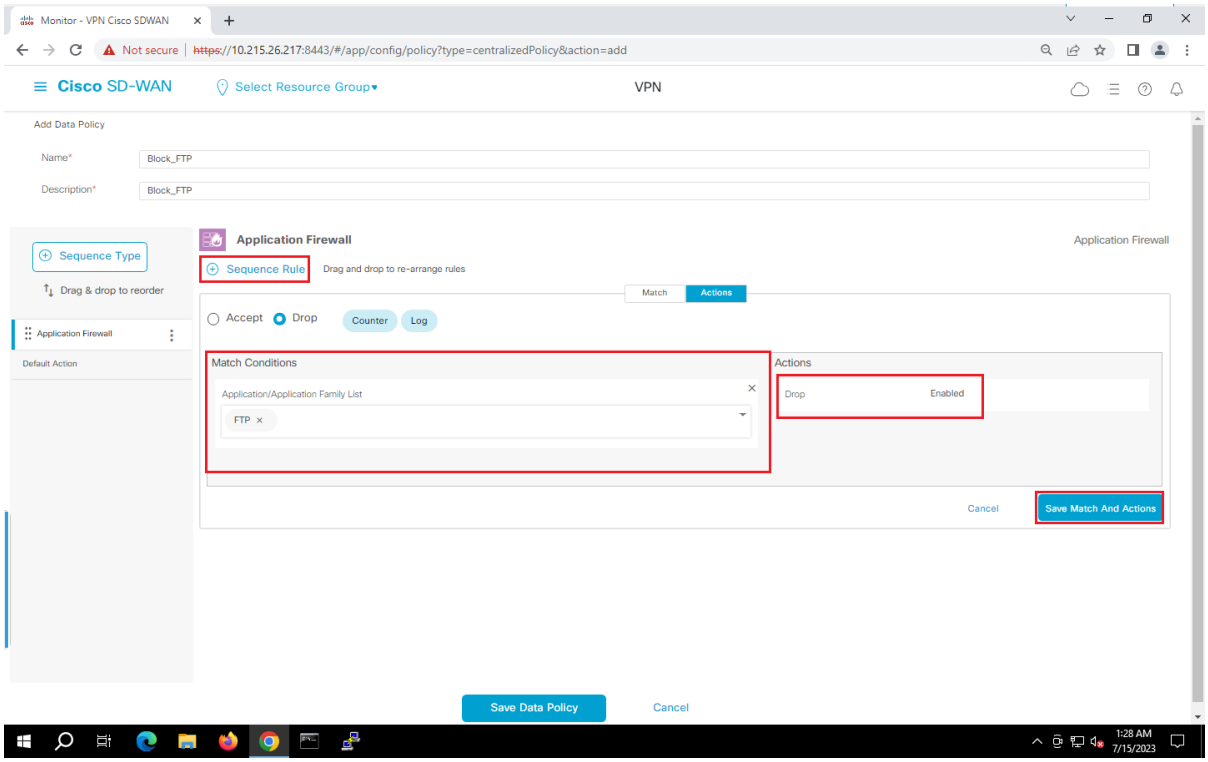
- **Name**: Block-FTP
- **Description**: Block-FTP



Chọn **Sequence Type > Application Firewall**

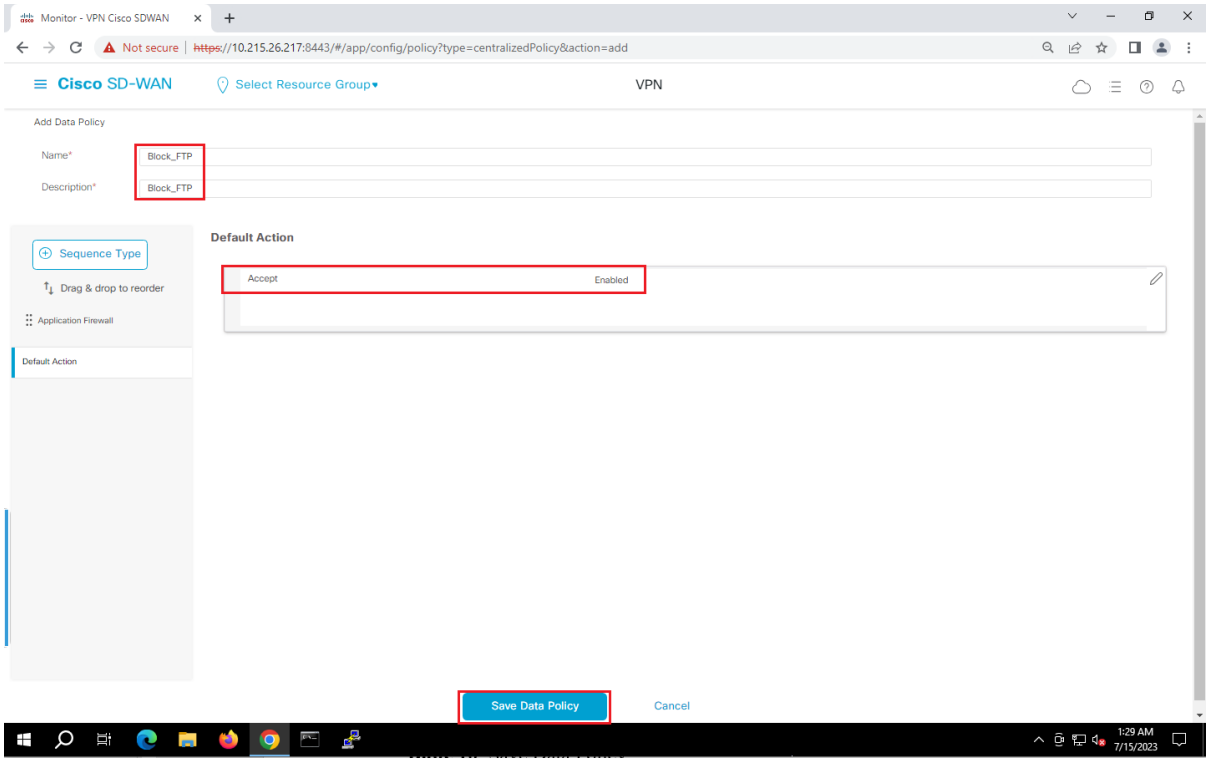


Chọn **Sequence Rule > Match > Application/ Application Family List**. Chọn **FTP**

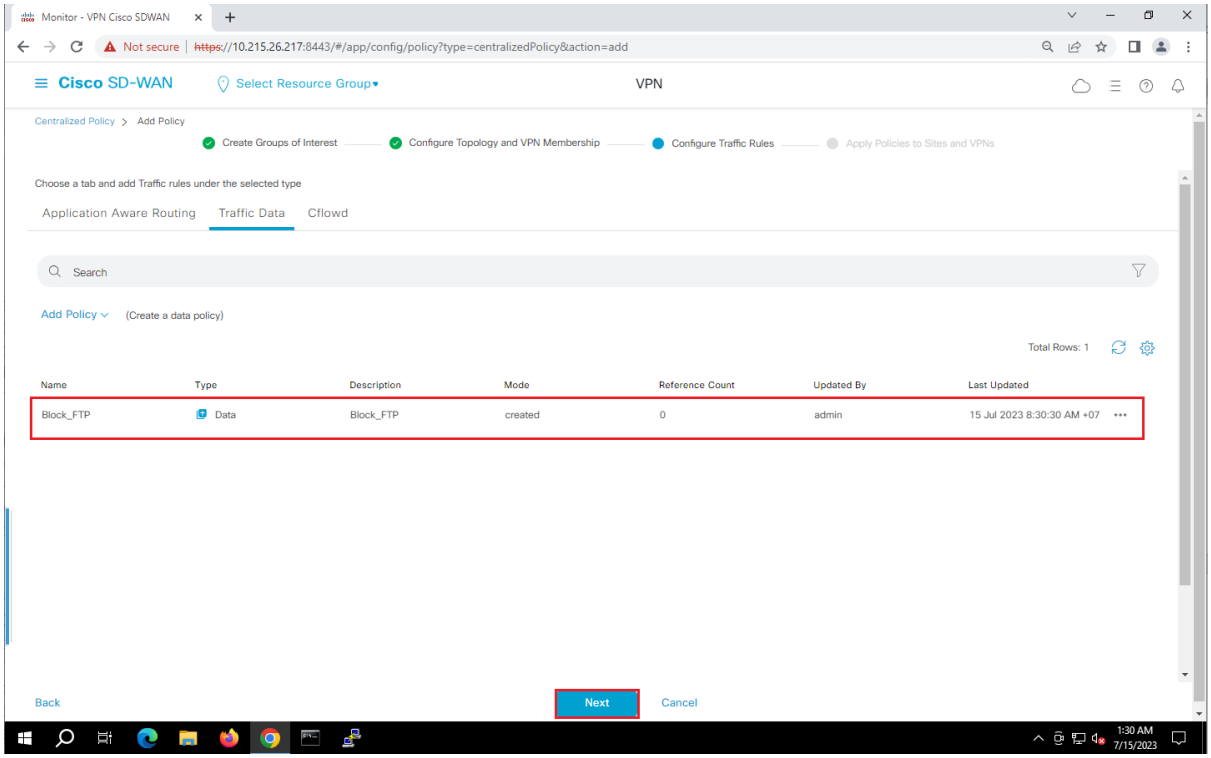


Chọn **Save Match And Actions**.

Default Action > Accept. Chọn **Save Match And Actions**.



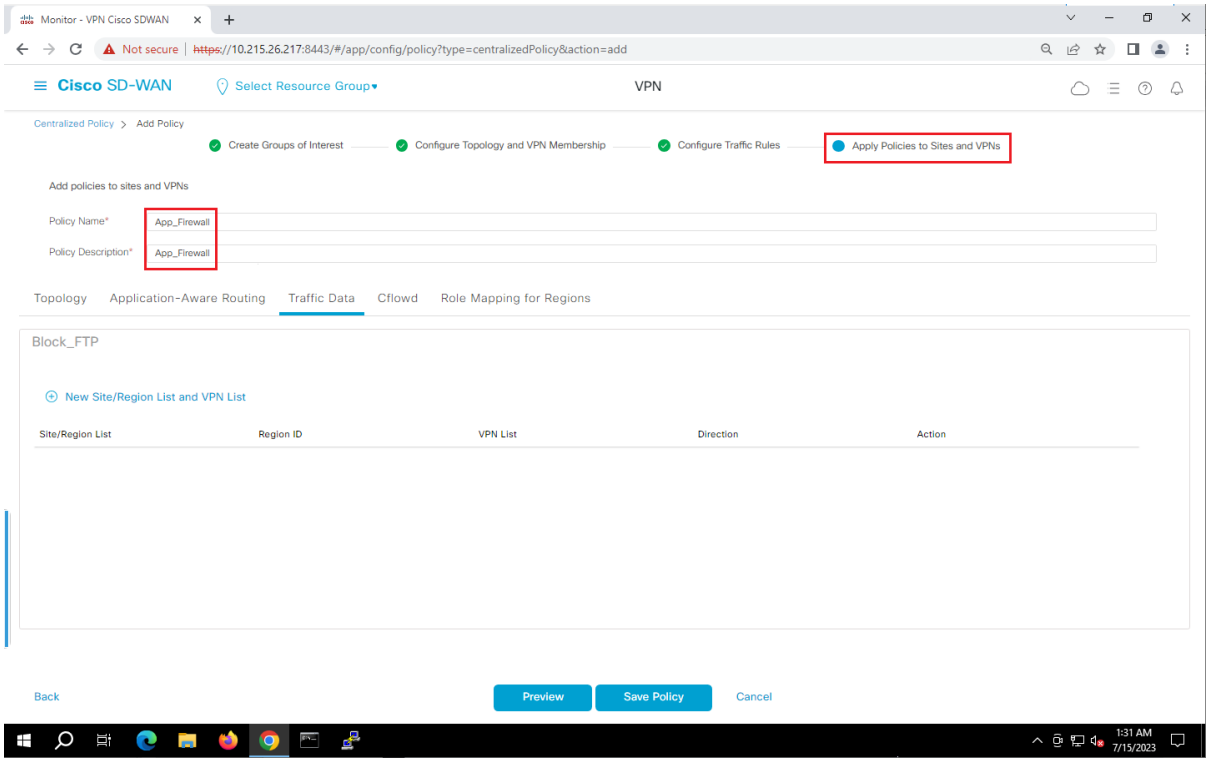
Save Data Policy.



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

Policy Name: App_Firewall

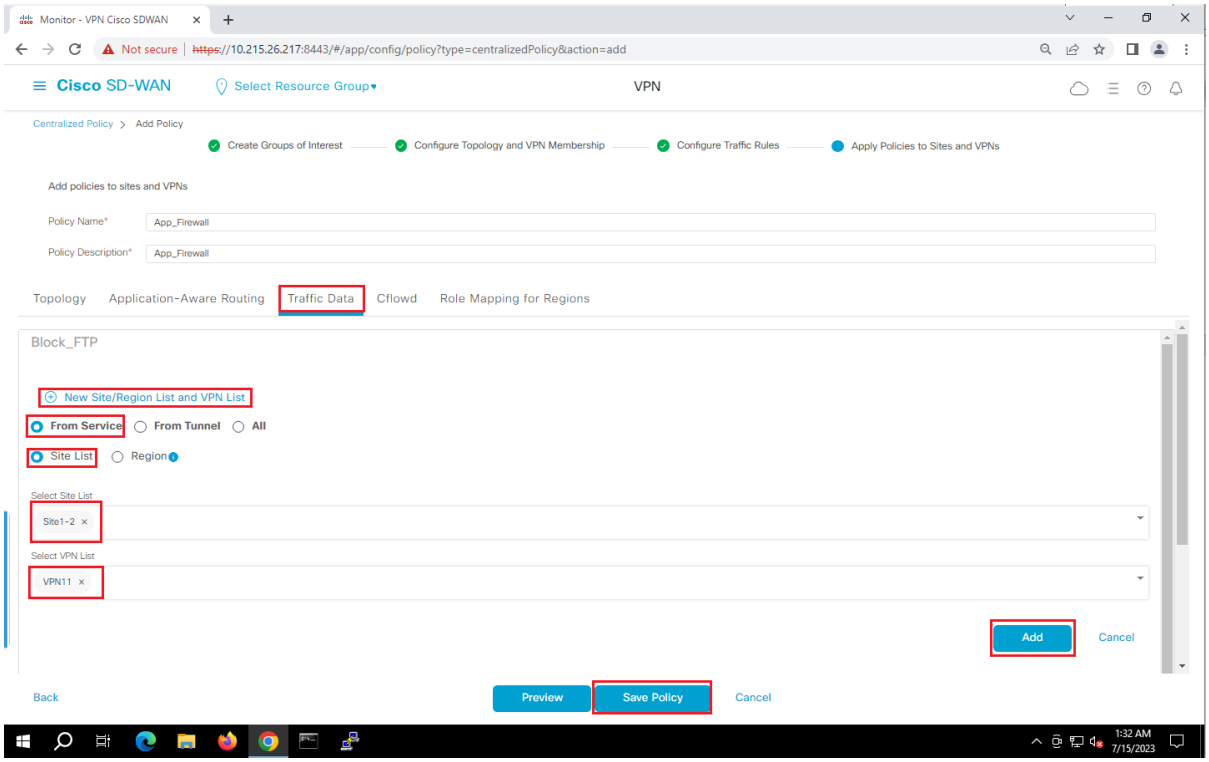
Policy Description: App_Firewall



Mục **Traffic Data > All**

Select Site List: Site1-2

Select VPN List: VPN11

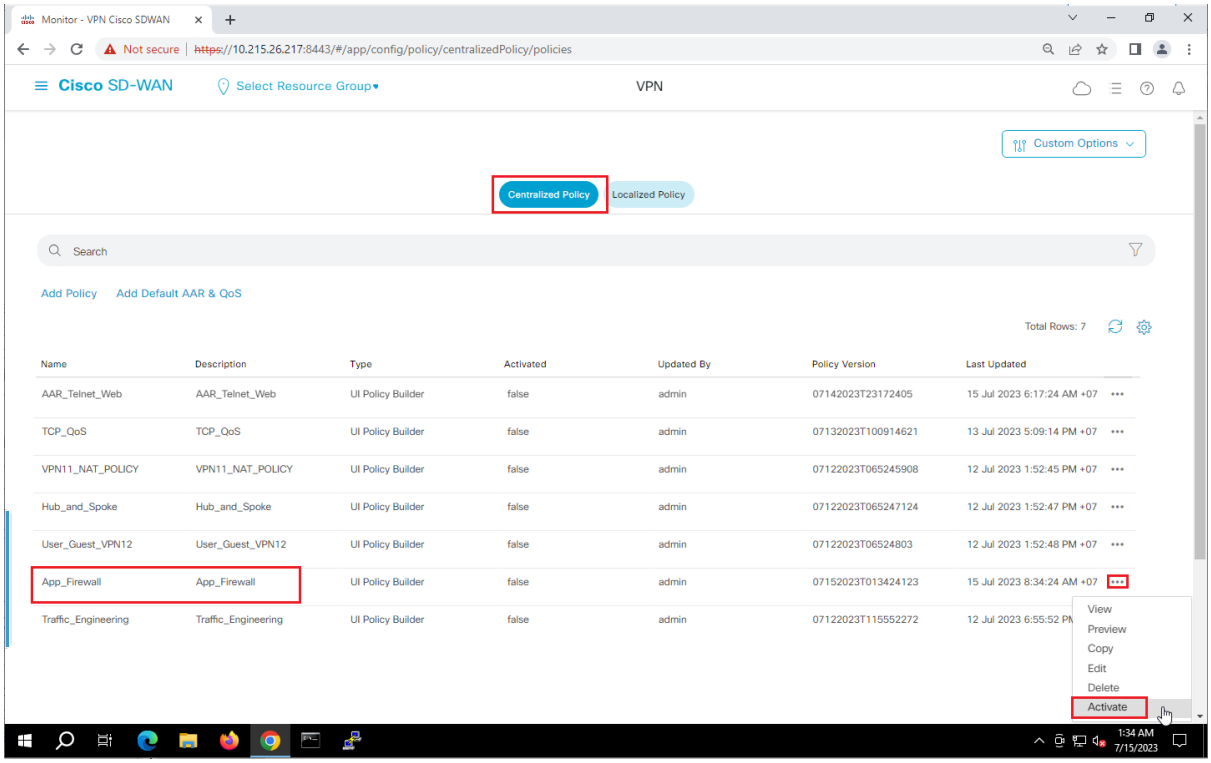


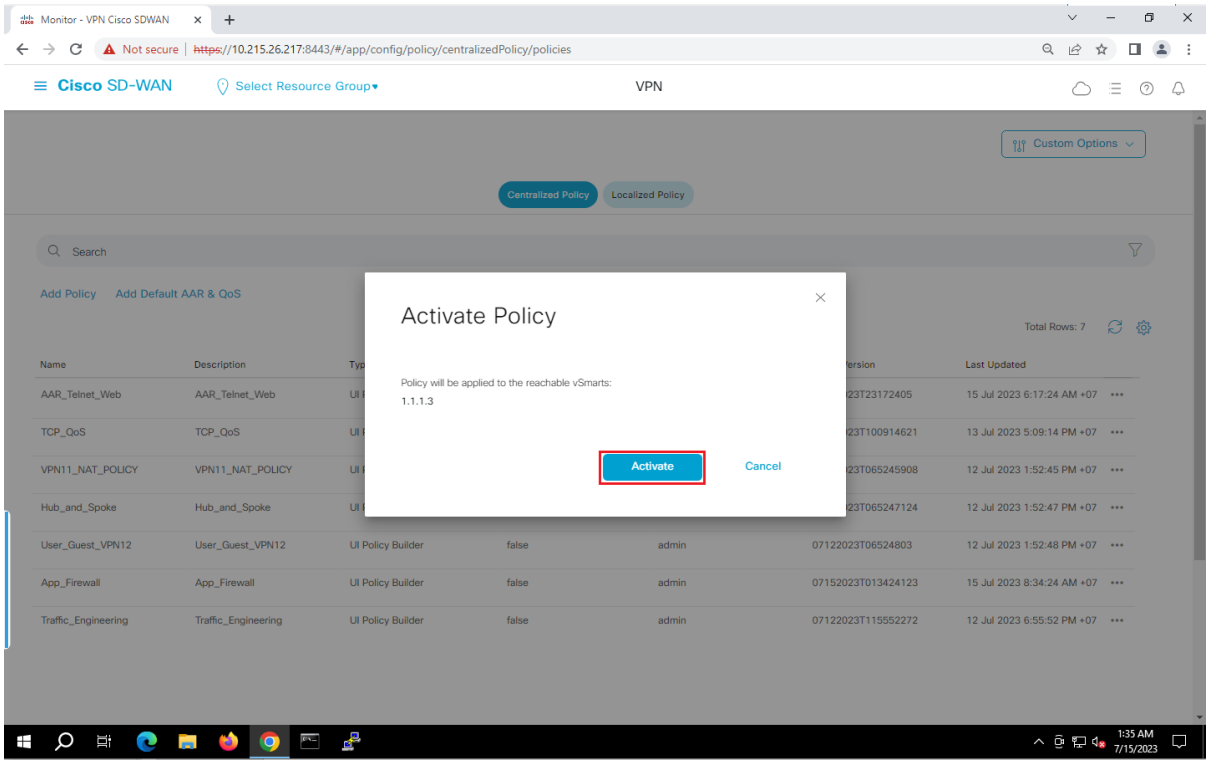
Nhấn **Add**

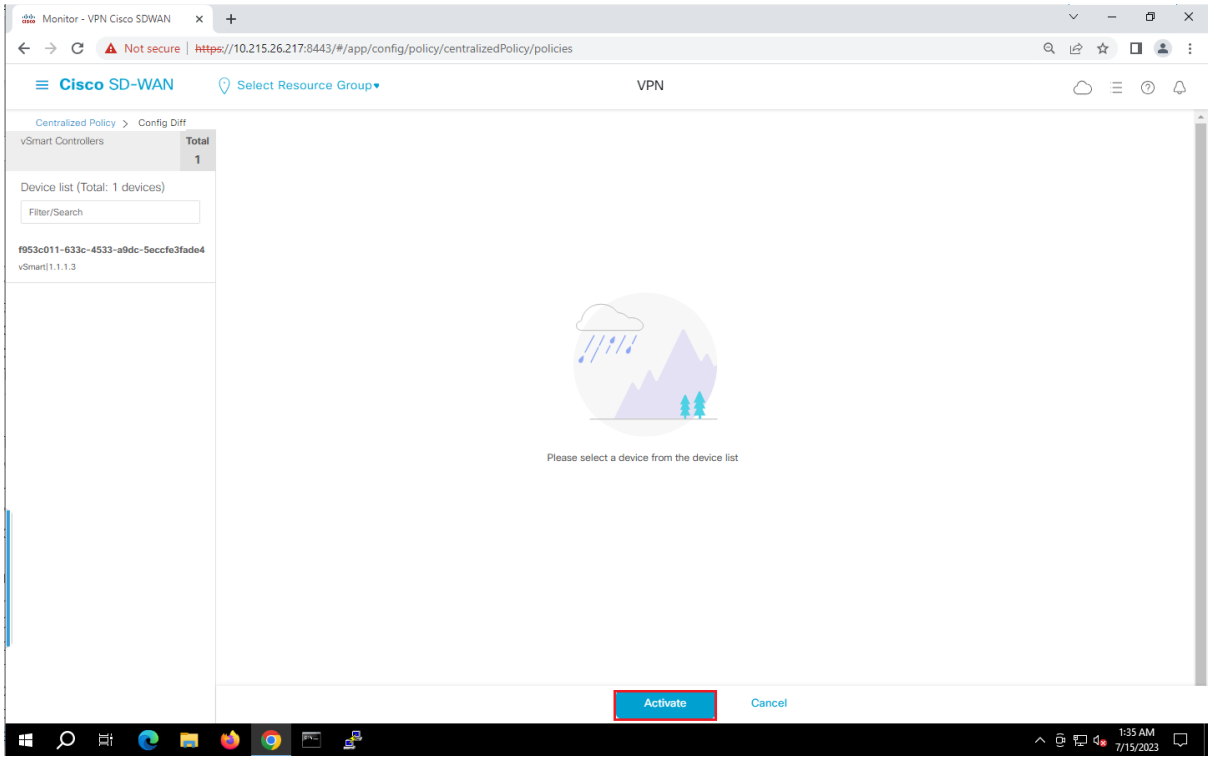
Nhấn **Save Policy**

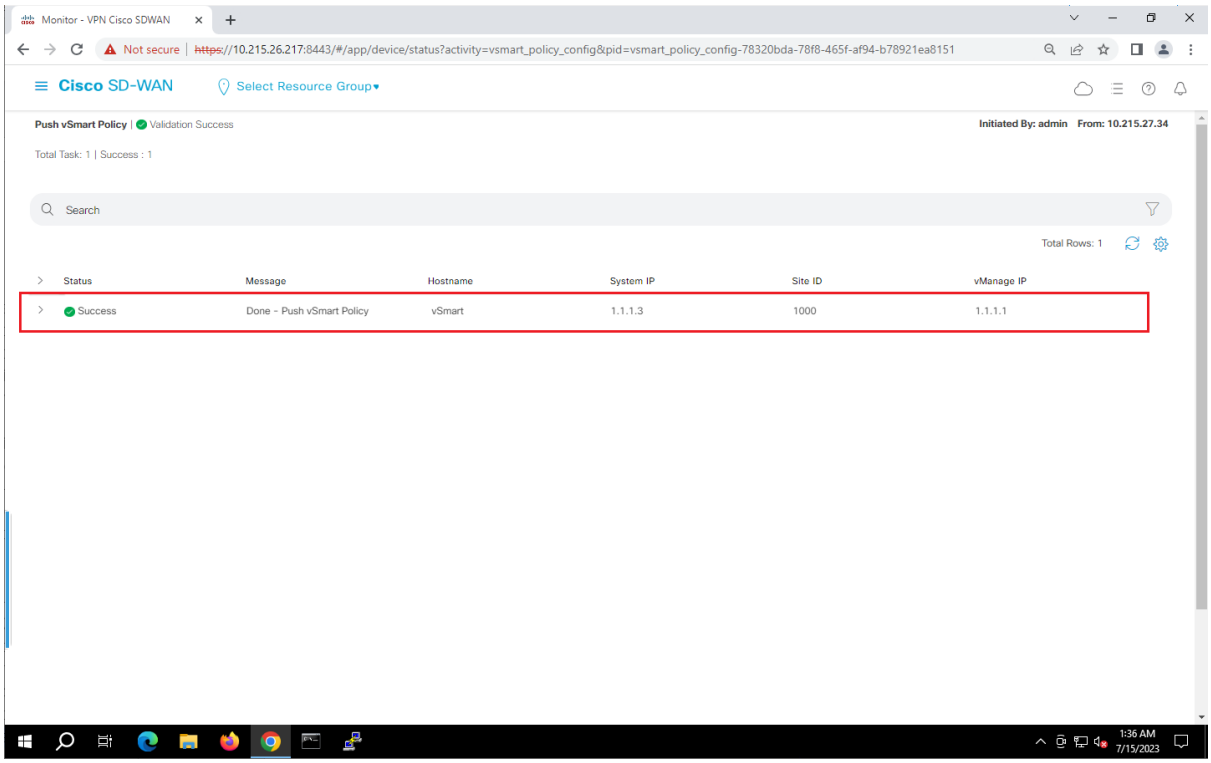
Vào lại **Configuration > Policies**. Chọn mục **Centralized Policy > App-Firewall**.

Chọn **Activale**.



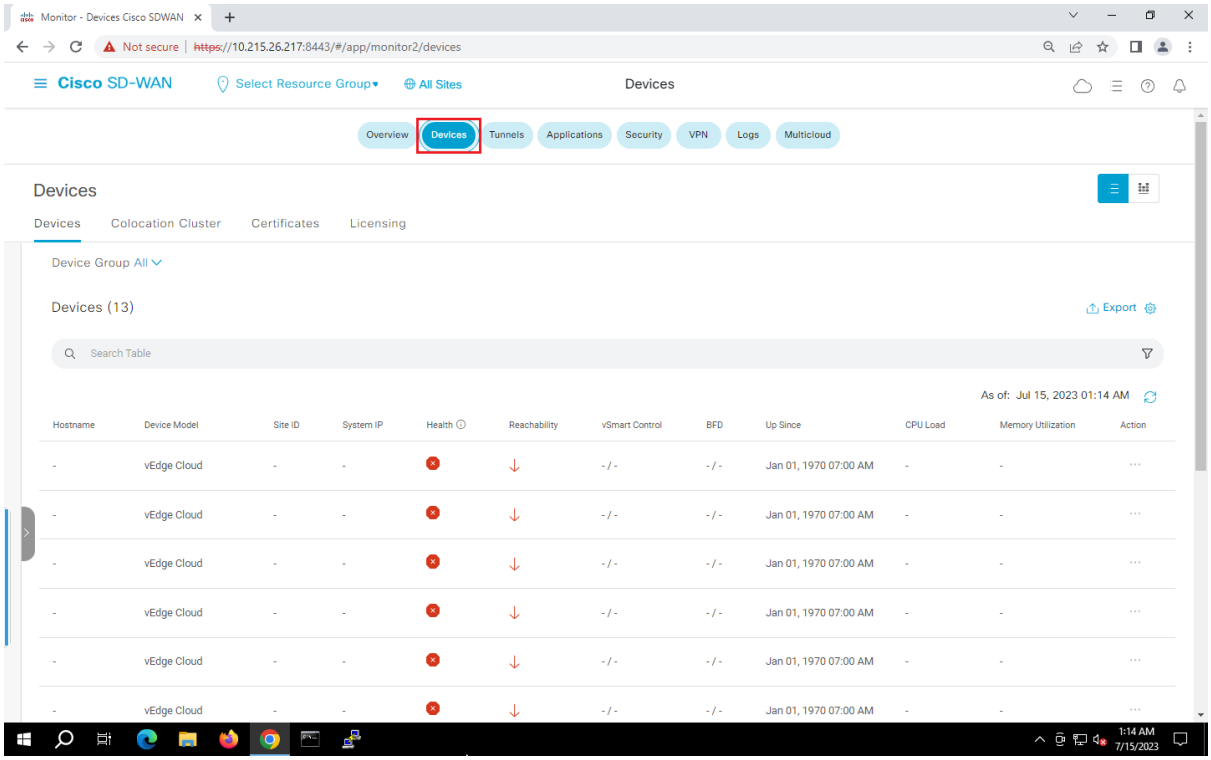


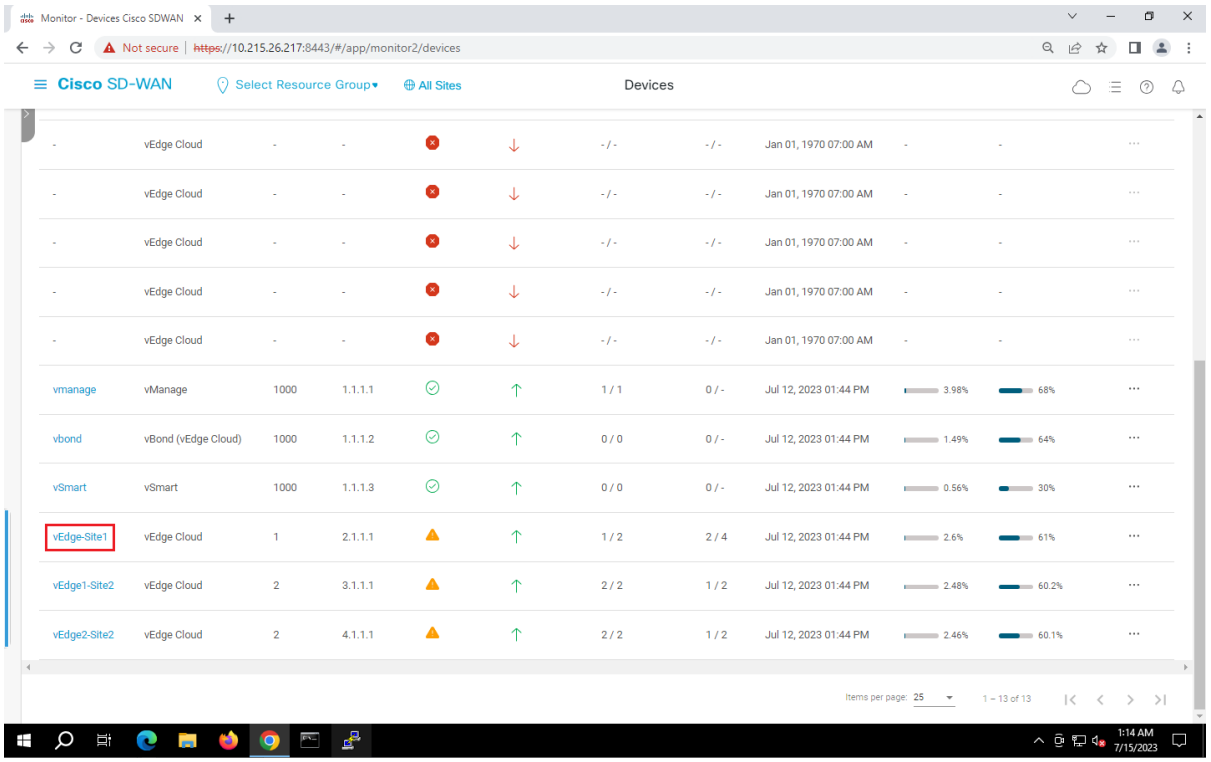


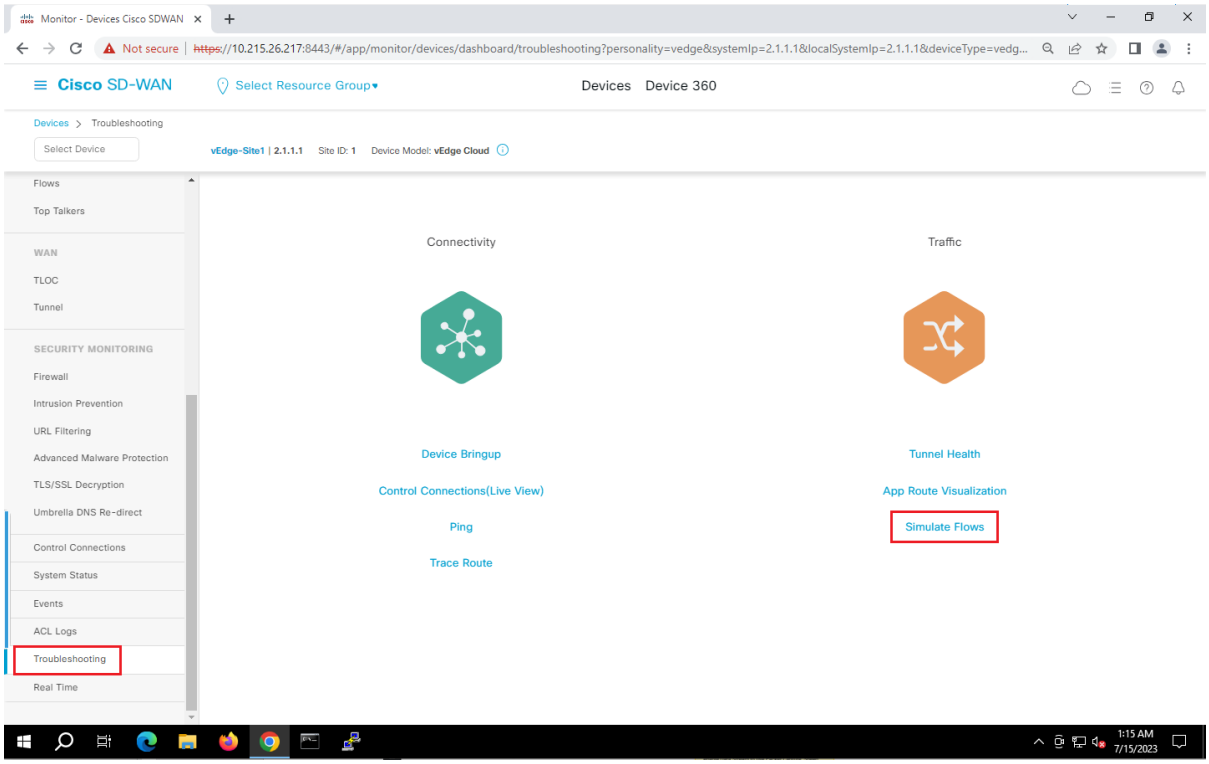


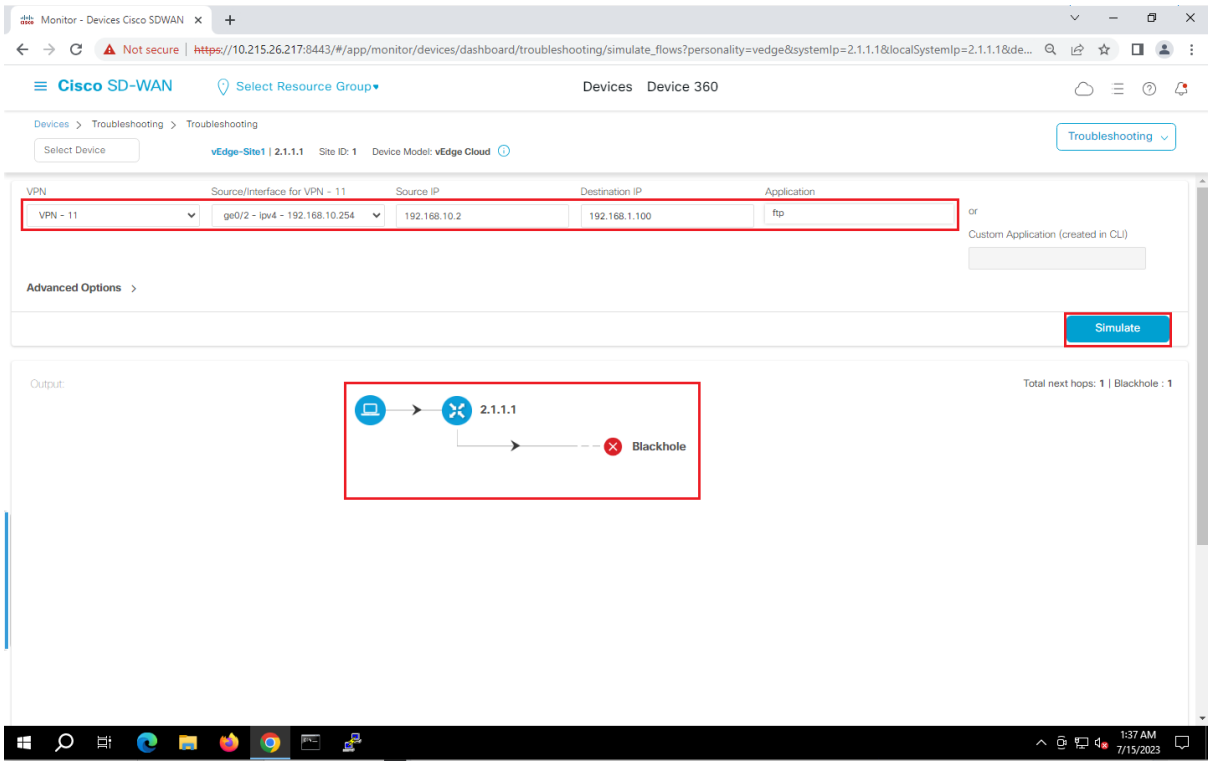
IV. Kiểm tra

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
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
1:14 AM
7/15/2023


Monitor - Devices Cisco SDWAN
Not secure | https://10.215.26.217:8443/#/app/monitor2/devices
Cisco SD-WAN
Select Resource Group
All Sites
Devices
vmanage
vManage
1000
1.1.1.1
Jul 12, 2023 01:44 PM
vbond
vBond (vEdge Cloud)
1.1.1.2
vSmart
1.1.1.3
vEdge-Site1
vEdge Cloud
2.1.1.1
vEdge1-Site2
3.1.1.1
vEdge2-Site2
4.1.1.1
Items per page: 25
1 – 13 of 13
1:14 AM
7/15/2023


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
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
Connectivity
Traffic
Device Bringup
Control Connections(Live View)
Ping
Trace Route
Tunnel Health
App Route Visualization
Simulate Flows
1:15 AM
7/15/2023


Monitor - Devices Cisco SDWAN
Not secure | https://10.215.26.217:8443/#/app/monitor/devices/dashboard/troubleshooting/simulate_flows?personality=vedge&systemIp=2.1.1.1&localSystemIp=2.1.1.1&de...
Cisco SD-WAN
Select Resource Group
Devices
Device 360
Devices > Troubleshooting > Troubleshooting
Select Device
vEdge-Site1 | 2.1.1.1 Site ID: 1 Device Model: vEdge Cloud
Troubleshooting
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
or
Custom Application (created in CLI)
Advanced Options
Simulate
Output:
Total next hops: 1 | Blackhole : 1
2.1.1.1
Blackhole
1:37 AM
7/15/2023