

How To Configure A Site-To-Site VPN Between FirePower and Meraki Using FDM

1. Log into FDM and then click on the Device section at the top of the page.
2. Click on View Configuration under Site-to-Site VPN at the bottom of the page.
3. Click + in the top right of the page to add a new Site-to-Site VPN
4. Set a name under Connection Profile Name
5. Under Local Site
 - a. Choose your outside interface under Local VPN Access Interface
 - b. Click + under Local Network and choose your local network object
6. Under Remote Site
 - a. Select the radio button for Static
 - b. Enter the Remote IP Address
 - c. Click + under Remote Network and choose the remote network object

Sample Define Endpoints:

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name
Mom-And-Dad-FL-VPN

LOCAL SITE

Local VPN Access Interface
outside (Ethernet1/1)

Local Network
+
Castle-Dave-Localnet

REMOTE SITE

Static Dynamic

Remote IP Address
1.2.3.4

Remote Network
+
Mom-And-Dad-FL-Localnet

CANCEL NEXT

7. Click the slider to turn off IKE Version 2
8. Under IKE Version 1
 - a. Click EDIT under IKE Policy
 - i. Disable all existing options
 - ii. Click Create New IKE Policy
 1. Set Priority to 100
 2. Set Name to Meraki-IKE-v1
 3. Move the slider for State to the right to enable it
 4. Set Encryption to 3DES
 5. Set Authentication to Preshared Key
 6. Set Diffie-Hellman Group to 2

7. Set Hash to SHA
8. Set Lifetime to 86400

Sample Meraki-IKEv1:

9. Click OK
- iii. Make sure the slider next to Meraki-IKEv1 is enabled and click OK

Sample IKE v1 Policy:

- b. Click EDIT under IPSec Proposal
 - i. Make sure ESP_SHA_HMAC-ESP_AES256-TUNNEL is enabled
 1. If ESP_SHA_HMAC-ESP_AES256-TUNNEL is not present, click + to add it
 - ii. Remove any other options
 - iii. Click OK
- c. Under Authentication Type, check the radio button for Pre-shared Manual Key
- d. Enter the Pre-shared key in the box
- e. Set NAT Exempt to No NAT exempt (turned off)
- f. Set Diffie-Hellman Group for Perfect Forward Secrecy to No Perfect Forward Secrecy (turned off)

Sample Privacy Configuration:

Local Network — VPN TUNNEL (CASTLE-DAVE...) — INTERNET — OUTSIDE (65.32.237...) — PEER ENDPOINT — Remote Network

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE Version 2

IKE Version 1

IKE Policy
Globally applied

IPSec Proposal
Default set selected

Authentication Type
 Pre-shared Manual Key Certificate

Pre-shared Key

Additional Options

NAT Exempt
No NAT exempt (turned off)

Diffie-Hellman Group for Perfect Forward Secrecy
No Perfect Forward Secrecy (turned off)

- g. Click NEXT
 - h. Review the information for accuracy and then click FINISH
9. Click on the Policies section at the top of the page.
10. Click on NAT under Security Policies
11. Click the + on the right-hand side of the page to add a NAT rule
12. Enter a title for your NAT rule
13. Set Create Rule for to Manual NAT
14. Change Placement to Before Auto NAT Rules
15. Set type to Static
16. Under Original Packet
 - a. Leave Source Interface set to Any
 - b. Change Source Address to be the local subnet on the device
 - c. Change Destination Address to be the remove subnet on the Meraki device
17. Under Translated Packet
 - a. Leave Source Interface set to Any
 - b. Change Source Address to be the local subnet on the device
 - c. Change Destination Address to be the remove subnet on the Meraki device

Sample NAT Rule:

Edit NAT Rule

Title: No-NAT-Policy-MaD-NY Create Rule for: Manual NAT Status:

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules Type: Static

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	Any	Destination Interface	Any
Source Address	Castle-Dave-Local	Source Address	Castle-Dave-Local
Source Port	Any	Source Port	Any
Destination Address	Mom-And-Dad-N\	Destination Address	Mom-And-Dad-N\
Destination Port	Any	Destination Port	Any

Show Diagram: CANCEL OK

18. Click OK
19. At the top of the page, click on Access Control under Security Policies
20. Click the + on the right-hand side of the page to add an Access Control policy
21. Click the drop down under Order and select the appropriate spot. (You probably towards the top.)
22. Set and appropriate Title
23. Under Source, click the + next to Networks and select your remote network
24. Under Destination, click the + next to Networks and select your local network

Sample Access Rule:

Edit Access Rule

Order	Title	Action
2	Allow-Traffic-From-Mom-And-Dad-FL	Allow

Source/Destination Applications URLs Users Intrusion Policy File policy Logging

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	Mom-And-Dad-...	ANY	ANY	Castle-Dave-Lo...	ANY

Show Diagram 0 Not hit yet

CANCEL OK

25. Click OK

26. Click the icon at the top of the screen, and deploy your changes.

27. Log into your Meraki dashboard and go to Security & SD-WAN and then select Site-to-site VPN

28. Set the Type to Hub (Mesh)

29. Under Organizational-wide settings, click Add a peer under Non-Meraki VPN peers

- Set a name for your VPN
- Enter the public IP of the FirePower device in the box for Public IP
- Leave the box for Remote ID blank
- Enter the network on the FirePower side under Private subnets
- Leave IPsec policies set at Default.

i. If you wish to click on the link to verify, they should be set to this:

Choose a Preset Default

Phase 1

Encryption 3DES

Authentication SHA1

Diffie-Hellman group 2

Lifetime (seconds) 28800

Phase 2

Encryption AES 256 AES 192 AES 128 3DES

Authentication SHA1 MD5

PFS group Off

Lifetime (seconds) 28800

Cancel Update

- f. Under Preshared secret, enter the same pre-shared key you configured on the FirePower device
- g. Leave Availability set to All networks

Sample Meraki dashboard VPN config:

New in Dashboard: Dashboard API v3.6 Released. [Read more.](#)

Site-to-site VPN

Type Off
Do not participate in site-to-site VPN.

Hub (Mesh)
Establish VPN tunnels with all hubs and dependent spokes.

Spoke
Establish VPN tunnels with selected hubs.

Exit hubs [Add a hub](#)

VPN settings

Name	Subnet	VPN participation
Main subnet	192.168.4.0/24	VPN on

NAT traversal Automatic
Connections to remote peers are arranged by the Meraki cloud.

Manual: Port forwarding
Remote peers contact the security appliance using a public IP and port that you specify. Use this if your security appliance is behind another NAT and "Automatic" traversal does not work.

Remote VPN participants

Network	Subnet(s)
Mom And Dad - NY	192.168.2.0/24

OSPF settings

Advertise remote routes Disabled

Organization-wide settings

Options in this section apply to all VPN peers in this organization.

Name	Public IP	Remote ID	Private subnets	IPsec policies	Preshared secret	Availability	Actions
Castle-Clave-VPN	1.2.3.4		192.168.1.0/24	Default		All networks	

[Add a peer](#)

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Logging	Actions
	Allow	Any	Any	Any	Any	Any	Default rule	Enabled	

You have unsaved changes.
Save or cancel

30. Click Save

Once the changes are pushed to the Meraki device, you should be able to ping from the local network of one device to remote network on the other device.