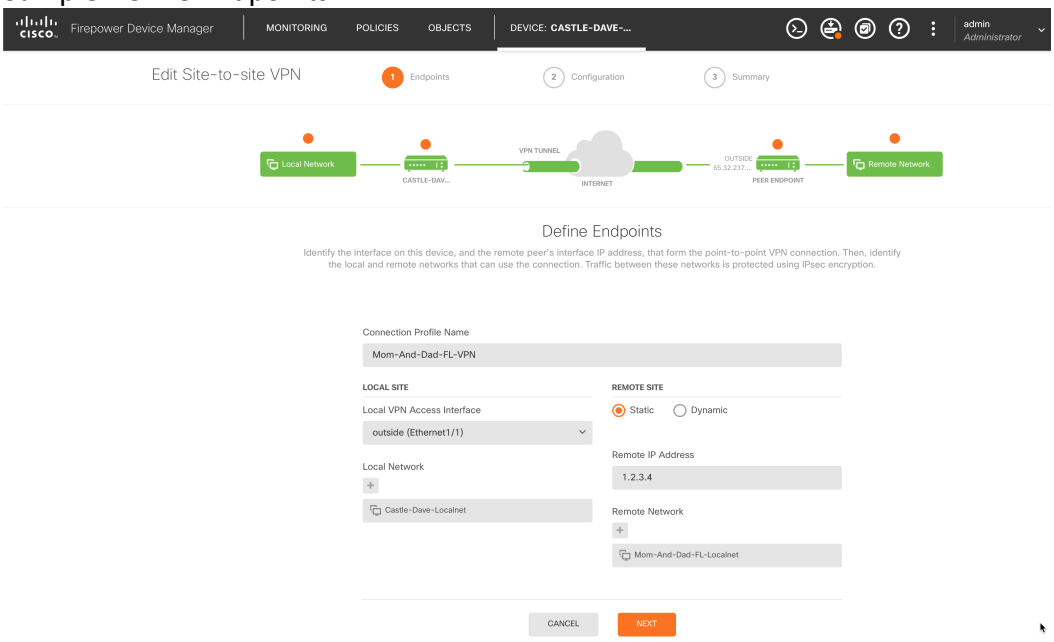
How To Configure A Site-To-Site VPN Between FirePower and Meraki Using FDM

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

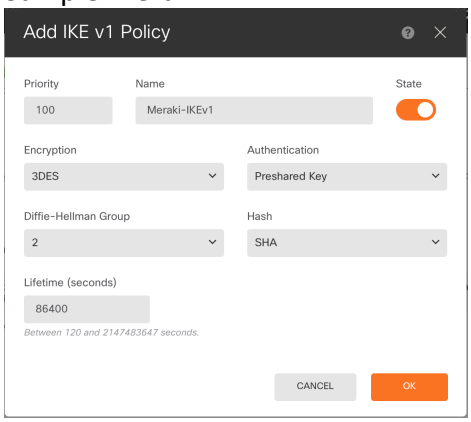
    Sample Define Endpoints:



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

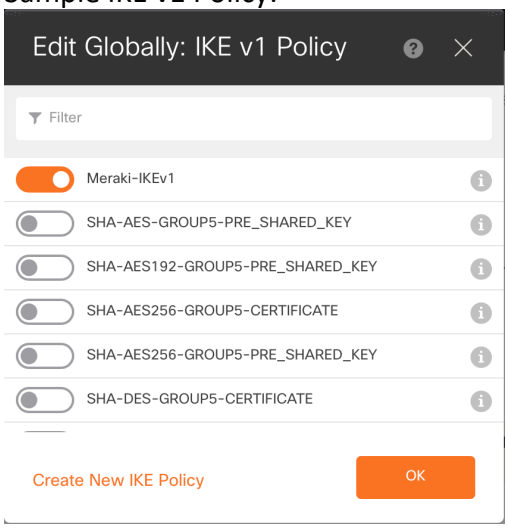
Sample Meraki-IKEv1:



9. Click OK

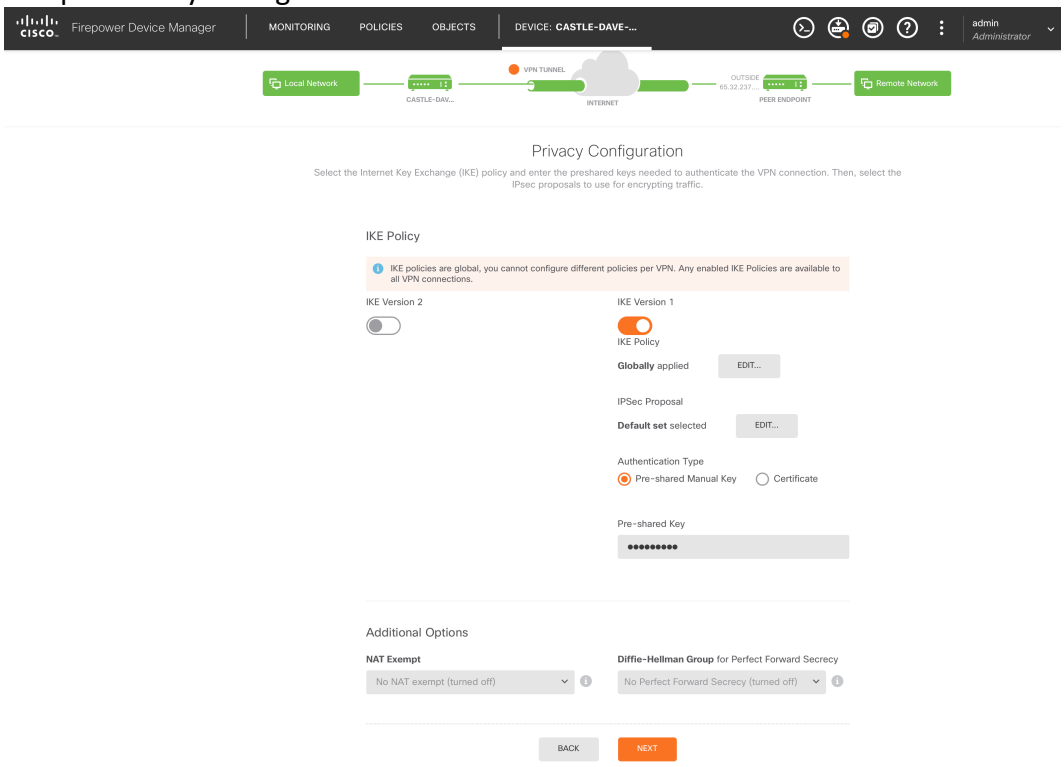
iii. Make sure the slider next to Meraki-IKEv1 is enabled and click OK

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)

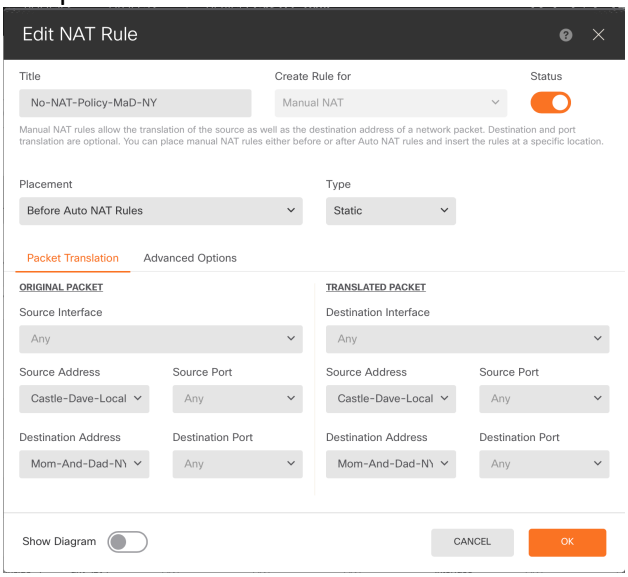
Sample Privacy Configuration:



g. Click NEXT
h. Review the information for accuracy and then click FINISH

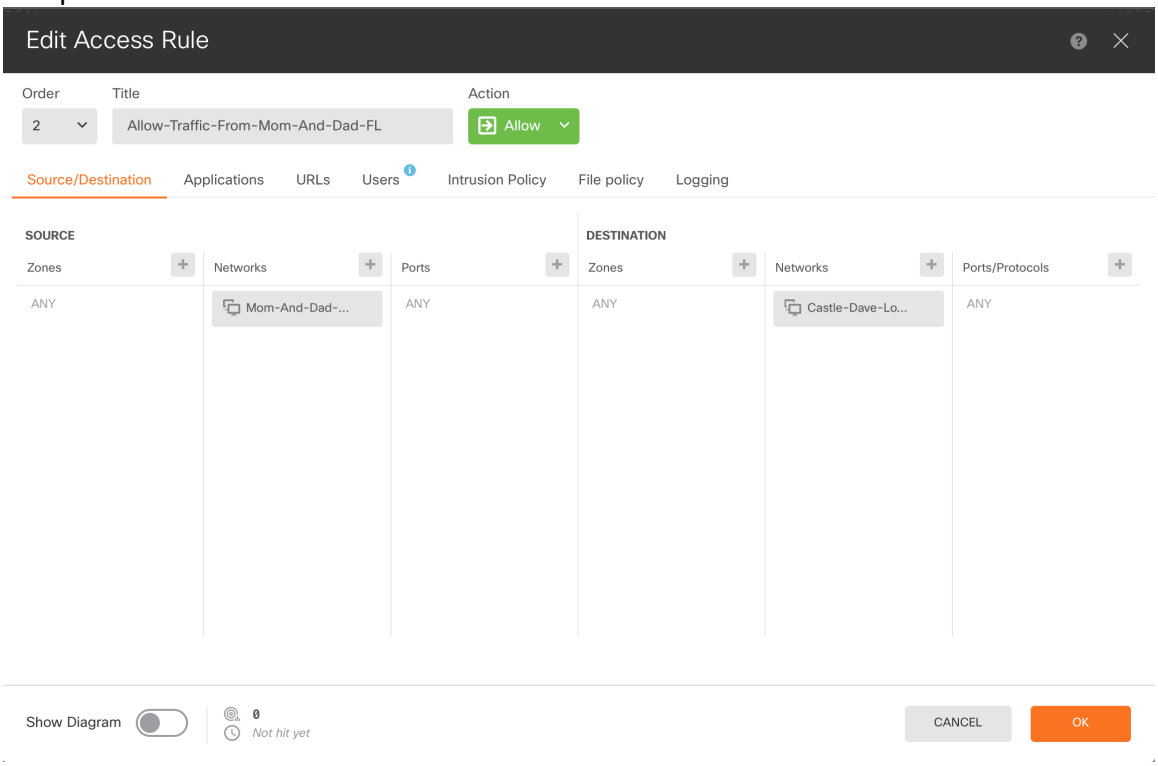
9. Click on the Policies section at the top of the page.
10. Click on NAT under Security Policies
11. Click the + on the right-hand side of the page to add a NAT rule
12. Enter a title for your NAT rule
13. Set Create Rule for to Manual NAT
14. Change Placement to Before Auto NAT Rules
15. Set type to 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:



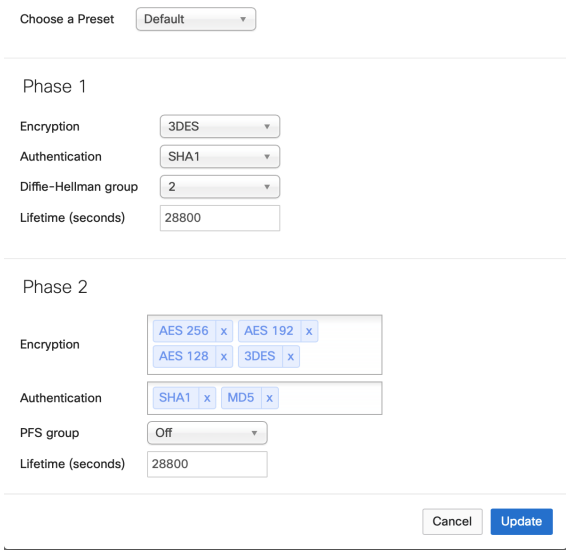
18. Click OK
19. At the top of the page, click on Access Control under Security Policies
20. Click the + on the right-hand side of the page to add an Access Control policy
21. Click the drop down under Order and select the appropriate spot. (You probably towards the top.)
22. Set and appropriate Title
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:



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

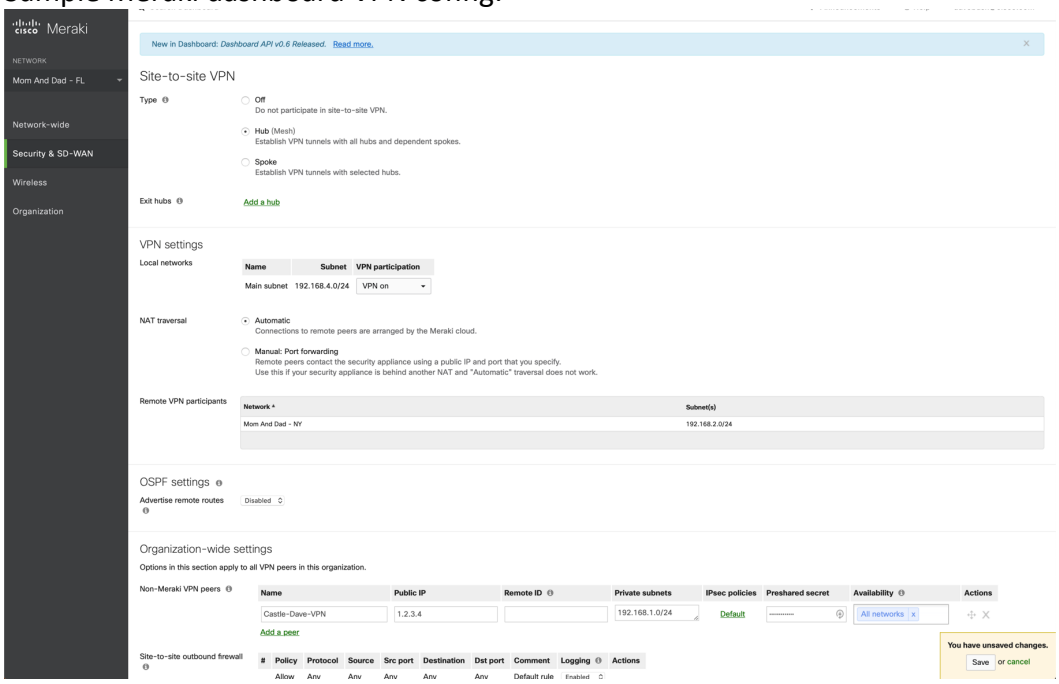
i. If you wish to click on the link to verify, they should be set to this:



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:



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.