SSID Tunneling and Layer 3 Roaming - VPN Concentration Configuration Guide

Meraki access points may be configured to concentrate traffic to a single point either for layer 3 roaming or teleworker use cases. Teleworker VPN and Layer 3 roaming with a concentrator both use the same Meraki Auto VPN technology. Wireless access points should concentrate to a Meraki MX security appliance.

It is recommended that a separate network be created in dashboard for each remote site location for purposes of manageability and usage tracking. Remote site networks should be created and access points added to the networks using the Quick Start guide. Get started by selecting “Create a network” from the network selector in dashboard.

SSID Configuration

Configuring a SSID to concentrate to a MX security appliance or the VPN concentrator is simple for both Layer 3 Roaming and VPN Concentrator.

1) Configure the SSID on the Access Control Page to either Layer 3 Roaming or VPN Concentration.

- Layer 3 roaming with a concentrator
  Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.

- VPN: tunnel data to a concentrator
  Meraki devices send traffic over a secure tunnel to an MX concentrator.

2) Select the MX security appliance concentrator that exists within the same Dashboard organization

3) Optional: Configure a specific VLAN to terminate the SSID on at the VPN concentrator. A list of available VLANs will be displayed if a MX security appliance is selected for concentration.

VPN Traffic Handling

An SSID that is configured for teleworker VPN can be configured in two different traffic handling modes Full Tunnel and Split Tunnel. The split tunnel feature can
route selected traffic over the VPN and route all other traffic to the local network upstream (and to the Internet).

WPA2-Enterprise RADIUS Authenticator

WPA2-Enterprise uses 802.1x to secure the wireless network. There are three pieces to 802.1x authentication; a supplicant, an authenticator, and an authentication server. Other operating modes like Bridge Mode and NAT Mode, the AP assumes the authenticator. SSID configured for VPN Concentrator and concentrated Layer 3 roaming SSIDs will pass the authenticator role to the VPN Concentrator.

If CoA on an enterprised SSID is required, this is only supported in MX tracking clients by MAC address. For more information click here.

In many cases each RADIUS authenticator must be added to the RADIUS authentication server such as Microsoft NPS or Cisco ISE. For VPN concentration and concentrated Layer 3 roaming SSIDs, just concentrators would need to be added to the RADIUS authentication server.

SSID Tunneling to an MX VPN Concentrator

The MX security appliance is the ideal solution for SSID Tunneling using VPN concentration as it is custom built for mission critical networks. Choose the MX security appliance that is best fit for your needs based on the Sizing Guide.

The MX security appliance is ready to concentrate SSIDs out of the box without any additional configuration beyond what is outlined in the quick start guide. VPN Concentrator tunneling is only officially supported for passthrough/concentrator mode MX devices so it is important to ensure your MX is in passthrough/concentrator mode for this feature to work correctly.

For additional information on how to set this up, please refer to this section.

To increase reliability, a second MX security appliance can be paired in HA mode. In the case that the primary MX becomes unreachable from the Meraki Cloud, the Access Points will failover to the HA standby MX.

How SSID Tunneling Works
Expected Packet Flow
After an SSID is configured to tunnel traffic to an MX concentrator, both the MR and MX send Register-Request packets to Meraki VPN registries.

**Register-Request** message is always a packet sent from node to the VPN Registry server. Registry-Request packets do the following:

- Port ranges used to contact VPN registry:
  - Source: UDP port range 32768-61000
  - Destination: UDP port 9350

**Note:** VPN Concentrator tunneling is only officially supported for passthrough/concentrator mode MX devices and is **NOT** officially supported for routed mode MX devices.

A **Register-Request message** is always a packet sent from node to the VPN Registry server. Registry-Request packets do the following:
• Provides the contact information of node's source IP and UDP port the node can be reached at to form tunnels, so this information can be shared with other registered peers.

• Request IP address of peer node's uplink and port the peer is using to form tunnels.

In an example, MR dynamically chooses UDP source port 39199 with source IP 192.168.2.3. MR then sends a Registry-Request packet to the VPN registries. The source IP gets of packet gets rewritten to the upstream NAT firewall's outside IP which is 76.126.47.131.

In an example, MR dynamically chooses UDP source port 39199 with source IP 192.168.2.3. MR then sends a Registry-Request packet to the VPN registries. The source IP gets of packet gets rewritten to the upstream NAT firewall's outside IP which is 76.126.47.131.

Similarly, the MX dynamically chooses UDP source port 49069 with source IP 192.168.10.17. The MX then sends a Registry-Request packet to the VPN registries. The source IP of the packet gets rewritten to the upstream NAT firewall's outside IP which is 128.107.241.175.

2. The VPN Registry servers reply back with Register-Response message. The Register-Response packets do the following:
• Informs the MR that the MX can be reached at IP address 128.107.241.175 and UDP port 49069.

3. When the MR receives connection information about the MX, it attempts to punch a hole in its local upstream firewall by sending packets to the outside IP address of the NAT firewall that the MX concentrator sits behind with the following parameters:

• Source IP: 192.168.2.3 (NATs to 76.126.47.131)
• Source Port: 39199
• Destination IP: 128.107.241.175
• Destination Port: 49069

4. When the first UDP packet sent by the MR reaches the MX, the stateful nature of upstream firewall drops it because the NAT table doesn't contain a session.

• Informs the MR that the MX can be reached at IP address 76.126.47.131 and UDP port 39199.
that allows inbound traffic from the MR firewall's outside IP.

5. When the MX receives connection information about the MR, it attempts to punch a hole in its local upstream firewall by sending packets to outside the IP address of the NAT firewall that the MR sits behind with the following parameters:

- **Source IP**: 192.168.0.17 (NATs to 128.107.241.175)
- **Source Port**: 49069
- **Destination IP**: 76.126.47.131
- **Destination Port**: 39199

6. When this first UDP packet sent by the MX reaches the MR's NAT firewall, it is allowed because it matches a previously established outbound session (established in #3) in the NAT table, so it is forwarded to the MR on the LAN.

7. The MR sends a second UDP packet to the MX.

8. The MX's upstream firewall allows this packet because it matches a previously established outbound session (established in #5) in the NAT table, so it is forwarded to the MX on the LAN.

9. Now an active UDP session is created in the NAT tables of both firewalls.

MR communication with the NAT firewall IP of MX:

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Bytes in Flight</th>
<th>Info</th>
</tr>
</thead>
</table>

* Frame 80080: 218 bytes on wire (1680 bits), 218 bytes captured (1680 bits)
  * Ethernet II, Src: 00:0b:0e:00:00:00, Dst: 00:0b:0e:00:00:00
  * User Datagram Protocol, Src Port: 49069, Dst Port: 39199
* Source Port: 49069
* Destination Port: 39199
* Length: 178
* [Checksum [missing]]
* [Checksum Status: Not present]
* [Stream index: 24]
* [Time since first frame: 5.8729510000 seconds]
* [Time since previous frame: 2.1890230000 seconds]

MX communication with the NAT firewall IP of MR:
10. Both Meraki appliances can now exchange the required UDP encapsulated IPsec packets to complete the IPsec negotiation and build a tunnel.

11. Once a tunnel is built, traffic from the concentrated SSID from the MRs will be tunneled to the MX concentrator.

**Note:** IPsec tunnels between peers never traverse the Cloud. The VPN registry simply acts as a broker allowing peers to exchange connection specific information. The actual IPsec tunnel is always peer-to-peer.

The above example does not consider upstream NAT firewalls doing PAT (NAT overload). If the upstream firewalls are doing PAT, source ports will change when Register-Request packets are sent out. Rewritten ports will be provided to the VPN registry and will be shared to other registered peers as such.