MX Routing Behavior

Overview

This article discusses route configuration and the interaction of differing routes on the MX. This article is intended to serve as a reference for deeper understanding of how routing decisions are made on MX Security Appliances.

This article may be especially useful for:

- Understanding the underlying mechanics of MPLS failover to AutoVPN
- Learning how VPN routing decisions in a DC-DC Failover configuration are made
- Understanding how the MX will behave in more complex routing configurations that leverage multiple types of routes or overlapping routes

Please note that this article assumes familiarity with configuring MX Security Appliances.

Types of Routes

MX Security Appliances support the configuration of several different types of routes, as detailed below.

Directly Connected

Directly connected routes are subnets defined in the Security & SD-WAN > Configure > Addressing & VLANs page of Dashboard. This is true of configurations leveraging a number of VLANs defined on an MX, or those that utilize a single subnet configuration with VLANs disabled.

Static routes are not directly connected.

Client VPN

The client VPN subnet is configured under the Security & SD-WAN > Configure > Client VPN page of Dashboard. There is only ever a single client VPN subnet on an individual MX network.

While client VPN utilizes the IPsec protocol to form a secure tunnel with the end device, the client VPN subnet is treated differently from routes to non-Meraki VPN peers.

Static Routes

Static routes are configured on the Security & SD-WAN > Configure > Addressing & VLANs page of Dashboard. Configuration of static routes is only possible while the MX is operating in Routed mode.
Static routes are used to communicate with subnets or VLANs that are not defined or "owned" by the MX, but are reachable through another layer 3 device on the network. Static routes require a next hop IP address be specified within the scope of a configured VLAN or subnet to be able to successfully route traffic to another layer 3 device.

Static routes are used to define subnets accessible through the LAN of the MX.

**AutoVPN**

Cisco Meraki’s AutoVPN can be configured on the Security & SD-WAN > Configure > Site-to-site VPN page of Dashboard. AutoVPN is a layer 3, IPsec-based site-to-site VPN. The mechanics are outlined in this white paper.

An MX Security Appliance configured to participate in an AutoVPN topology will automatically create routes for subnets included in the AutoVPN topology.

**Non-Meraki VPN Peers (Other IPsec)**

Non-Meraki VPN peers are configured on the Security & SD-WAN > Configure > Site-to-site VPN page of Dashboard. These VPN peers are connected to using IPsec. If an MX is configured to establish a VPN with a non-Meraki VPN peer, the MX will also have routes to the private subnets defined for that VPN peer.

**NAT**

The MX Security Appliance can be configured to operate in Routed mode, from the Security & SD-WAN > Configure > Addressing & VLANs page of Dashboard. When in Routed mode, the MX can be configured with multiple LAN subnets and static routes. If a route for a particular subnet does not exist on the MX then in this mode, the traffic is NATED and sent out across an Ethernet connection into one of the Internet interfaces, or out a cellular connection.

**Route Priority**

Each type of route configured on the MX has a specific priority in comparison with other types of routes. The priority is as follows:

1. Directly Connected
2. Client VPN
3. Static Routes
4. AutoVPN Routes
5. Non-Meraki VPN Peers
6. BGP learned Routes
7. NAT*

NOTE: For BGP route selection please refer to: [https://documentation.meraki.com/MX/Networks_and_Routing/BGP](https://documentation.meraki.com/MX/Networks_and_Routing/BGP)

*If no routes are defined, then the traffic is NATED and sent out an active Internet interface. This only occurs while the MX is configured in Routed mode.
When routing decisions are made, traffic destined for an address for which multiple routes exist will be routed in the order of priority above. For example, if a route for 10.0.0.0/8 is defined as both a static route and as an AutoVPN route, traffic destined for that subnet is routed using the static route, as static routes take precedence over AutoVPN routes.

**Overlapping Routes**

Route priority dictates how traffic is routed when multiple routes exist to the same subnet. However, overlapping routes that are not identical are also present in many deployments. In this case, the most specific route will be used.

**Advanced Configurations**

**Static Route Tracking**

Static routes can be configured with three different availability settings:

- always active,
- active while the next hop responds to ping, and
- active while host responds to ping

If the static route is always active, the configured static route will always be maintained in the routing table.

When a route is configured as active while the next hop responds to ping, or active while a host responds to ping, the MX tracks the route. If the MX stops receiving ping responses for a period of time, the route will be removed from the routing table. The route is re-added when responses are received again.

**Datacenter Redundancy (DC-DC Failover)**

A DC-DC failover configuration is defined by the following characteristics:

- Multiple MXs are configured in VPN concentrator mode on the Security & SD-WAN > Configure > Addressing & VLANs page of Dashboard
- The VPN concentrator mode MXs are configured to advertise the same upstream subnet(s) via the Security & SD-WAN > Configure > Site-to-site VPN page in Dashboard
- The VPN concentrator mode MXs are configured as AutoVPN hubs for spoke MXs if a hub & spoke topology is being used

In this configuration, multiple routes exist to the same subnet and the routes are the same type (AutoVPN). Since route priority and matching on the most specific route cannot be used to determine which AutoVPN route should be used, the concentrator priority is used as a tie breaker.

In a DC-DC failover configuration, AutoVPN traffic to subnets advertised from multiple concentrators is routed to the highest priority VPN concentrator that is reachable. VPN Concentrator priority is defined on the Security & SD-WAN > Configure > Site-to-site VPN page in Dashboard.
When an MX Security Appliance is configured to connect to multiple VPN concentrators advertising identical subnets, the routes to those subnets become tracked. Hello messages are periodically sent across the tunnel to monitor connectivity. If the tunnel to the highest priority hub goes down, the route is removed from the route table and traffic is routed to the next highest priority hub that is reachable.

## Failover Times

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Failover Time</th>
<th>Failback Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoVPN Tunnels</td>
<td>30-40 seconds</td>
<td>30-40 seconds</td>
</tr>
<tr>
<td>DC-DC Failover</td>
<td>20-30 seconds</td>
<td>20-30 seconds</td>
</tr>
<tr>
<td>Static Route Tracking</td>
<td>15-20 seconds</td>
<td>9-12 seconds</td>
</tr>
<tr>
<td>WAN connectivity</td>
<td>300 seconds or less</td>
<td>15-30 seconds</td>
</tr>
</tbody>
</table>

## Example Scenarios and Traffic Flow Details

### MPLS Failover to AutoVPN

This article describes the configuration and failover behavior for a configuration that leverages MPLS failover to AutoVPN tunnels.

### DC-DC Failover

The following section provides an explanation of how VPN routing functions in a configuration where multiple VPN hubs are configured in a DC-DC failover topology.

Consider the following example:

- One branch location
- The branch acting as a spoke to 4 VPN hubs
- One VPN hub, DC1 hosting a /8 subnet, and a unique /24
- One VPN hub, DC2, is hosting a unique /16 that overlaps with DC1
- Two VPN hubs, DC3 and DC4, are configured to advertise the same /24. DC3 has a higher hub priority than DC4.
In this configuration, the branch MX will receive routes for all subnets at each of the 4 datacenters, even those that overlap. The following table represents the routes presented to the branch MX in this configuration:

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Next Hop Concentrator</th>
<th>Hub Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>DC1</td>
<td>1</td>
</tr>
<tr>
<td>192.168.100.0/24</td>
<td>DC1</td>
<td>1</td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>DC2</td>
<td>2</td>
</tr>
<tr>
<td>172.16.1.0/24</td>
<td>DC3</td>
<td>3</td>
</tr>
<tr>
<td>172.16.1.0/24</td>
<td>DC4</td>
<td>4</td>
</tr>
</tbody>
</table>

How is traffic routed given the above configuration?

**If traffic is sent to 10.100.12.44**

The branch MX sends this traffic to DC1. This subnet is only contained within the 10.0.0.0/8 subnet advertised via this DC.

**If traffic is sent to 192.168.100.30**

The branch MX sends this traffic to DC1. This subnet is only advertised by DC1.
If traffic is sent to 10.1.0.98
The branch MX sends this traffic to DC2. This subnet matches on both the 10.0.0.0/8 subnet advertised by DC1 and the 10.1.0.0/16 subnet advertised by DC2. While DC1 has a higher hub priority, the MX prefers the most specific route and sends the traffic to DC2. If the branch MX does not have connectivity to DC2, traffic will not be routed to DC1. This is because only identical subnets are tracked for failover.

If traffic is sent to 172.16.1.214
The branch MX sends this traffic to DC3. DC3 has a higher priority than DC4, so traffic for the subnet advertised from both concentrators is sent to DC3. If a VPN connection cannot be established to DC3, then this traffic is routed to DC4.

**If you require the spoke MX to be able to failover to a hub with a less specific subnet, please contact Cisco Meraki Support.**

Multiple Overlapping Routes
Consider the following example:

- One branch
- A static route for the 172.16.0.0/12 subnet to MPLS
- Static routes to other downstream subnets of 172.16.30.0/24, 192.68.20.0/25
- AutoVPN tunnels to two Datacenters, DC1 and DC2
- DC1 is configured to advertise subnets of 10.1.10.0/24 and 172.16.10.0/24
- DC2 is configured to advertise subnets of 10.1.10.0/24 and 172.16.0.0/12
- An IPsec VPN connection to a non-Meraki VPN peer is also present
- The non-Meraki VPN peer has 172.16.45.0/24, 192.168.20.0/25, and 192.168.0.0/16
The following table represents the routes presented to the branch MX in this configuration:

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Route Type</th>
<th>Hub Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.10.0/24 (DC1)</td>
<td>AutoVPN</td>
<td>1</td>
</tr>
<tr>
<td>10.1.10.0/24 (DC2)</td>
<td>AutoVPN</td>
<td>2</td>
</tr>
<tr>
<td>172.16.0.0/12</td>
<td>Static</td>
<td>N/A - Not an AutoVPN route</td>
</tr>
<tr>
<td>172.16.0.0/12 (DC2)</td>
<td>AutoVPN</td>
<td>2</td>
</tr>
<tr>
<td>172.16.10.0/24 (DC1)</td>
<td>AutoVPN</td>
<td>1</td>
</tr>
<tr>
<td>172.16.30.0/24</td>
<td>Static</td>
<td>N/A - Not an AutoVPN route</td>
</tr>
<tr>
<td>172.16.45.0/24</td>
<td>Non-Meraki VPN Peer</td>
<td>N/A - Not an AutoVPN route</td>
</tr>
<tr>
<td>192.168.0.0/16</td>
<td>Non-Meraki VPN Peer</td>
<td>N/A - Not an AutoVPN route</td>
</tr>
<tr>
<td>192.168.20.0/25</td>
<td>Static</td>
<td>N/A - Not an AutoVPN route</td>
</tr>
<tr>
<td>192.168.20.0/25</td>
<td>Non-Meraki VPN Peer</td>
<td>N/A - Not an AutoVPN route</td>
</tr>
</tbody>
</table>

How is traffic routed given the above configuration?
If traffic is sent to 10.1.10.1
The MX sends this traffic to DC1. DC1 has a higher priority than DC2, so traffic for the subnet advertised from both concentrators is sent to DC1. If a VPN connection cannot be established to DC1, then this traffic is routed to DC2.

If traffic is sent to 172.16.0.1
The MX has both a static and AutoVPN route for this subnet. Since static routes have a higher priority than AutoVPN routes, traffic will be sent using the static route.

If route tracking has been configured on the static route, when the MX stops receiving ping responses for the static route it will be removed from the routing table. In this scenario, the only remaining route is the AutoVPN route and traffic will be sent to DC2.

If traffic is sent to 172.16.10.1
The MX has multiple routes for 172.16.0.0/12, but a more specific AutoVPN route for the 172.16.10.0/24 subnet is available. Traffic will be sent to DC1 using the more specific route.

If traffic is sent to 172.16.30.1
The MX has multiple routes for 172.16.0.0/12, but a more specific static route for the 172.16.30.0/24 subnet is available. Traffic will be sent using the more specific static route.

If route tracking has been configured on the static route, when the MX stops receiving ping responses for the static route it will be removed from the routing table. In this scenario, traffic will be routed using the available 172.16.0.0/12 routes. As static routes have a higher priority than AutoVPN routes, traffic will be sent using the static route.

If the static route for 172.16.0.0/12 has also been removed via route tracking, then the AutoVPN route will be used and traffic is sent to DC2.

If traffic is sent to 172.16.45.1
The MX has multiple routes for 172.16.0.0/12, but a more specific route for the 172.16.45.0/24 subnet is available via the non-Meraki VPN peer. Traffic will be sent using the more specific route from the non-Meraki VPN peer.

If traffic is sent to 192.168.0.1
The MX has a route available for 192.168.0.0/16 via a non-Meraki VPN peer. Traffic will be sent to the non-Meraki VPN peer.

If traffic is sent to 192.168.0.1
The MX has a route available for 192.168.20.0/25, as well as a route for 192.168.0.0/16. The more specific 192.168.20.0/25 routes will be used over the /16 route available from the non-Meraki VPN peer. As static routes have a higher priority than routes from non-Meraki VPN peers, traffic will be sent using the static route.

If route tracking has been configured on the static route, when the MX stops receiving ping responses for the static route it will be removed from the routing table. In this scenario, traffic would be sent to the remaining 192.168.20.0/25 route available via the non-Meraki VPN peer.
Additional Considerations

When configuring routing on an MX Security Appliance it is important to take note of the following considerations.

AutoVPN and Non-Meraki VPN peers

An MX Security Appliance can establish tunnels to both AutoVPN and Non-Meraki VPN peers. The MX will send traffic to those VPN peers using the principles discussed above. However, an MX that builds tunnels to both AutoVPN and Non-Meraki VPN peers, will not route traffic between the non-Meraki VPN peers and other AutoVPN peers.

Spoke-to-Spoke Communication

All MX Security Appliances joined to an AutoVPN topology will receive routes for all other subnets joined to the AutoVPN topology. In a hub and spoke topology, a spoke MX will receive routes to communicate with other spoke sites with a next hop of their configured VPN hub(s). The VPN hubs will then route between spoke sites.

To prevent certain traffic from entering the VPN, site-to-site VPN firewall rules can be configured on the Security & SD-WAN > Configure > Site-to-site VPN page in Dashboard.

Routed Mode and AutoVPN

You can only advertise the same subnet from more than one appliance if all appliances advertising that subnet are in Passthrough or VPN Concentrator mode. All subnets advertised from an appliance in Routed mode must be unique within the AutoVPN topology.

Private Subnet Configuration on Multiple Non-Meraki VPN Peers

When two or more non-Meraki VPN peers are configured identical or overlapping private subnets, you will be prompted with a message alerting you of the overlapping or identical subnets that must be confirmed before saving changes. The messages describe the following routing behavior:

- When two subnets overlap, IP traffic will be routed to the most specific subnet.
- When two subnets directly conflict, IP routing behavior will be undefined. This can be avoided by configuring the Availability column with different network tags to ensure that no security appliances have peers with conflicting IP subnets.

An example screenshot and confirmation message can be found below:

<table>
<thead>
<tr>
<th>Non-Meraki VPN peers</th>
<th>Name</th>
<th>Public IP</th>
<th>Private subnets</th>
<th>IPsec policies</th>
<th>Preshared secret</th>
<th>Availability</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer1</td>
<td></td>
<td>1.2.3.4</td>
<td>10.0.0.0/8</td>
<td>Default</td>
<td></td>
<td>All networks</td>
<td>✗ ✗</td>
</tr>
<tr>
<td>peer2</td>
<td></td>
<td>5.6.7.8</td>
<td>10.0.0.0/8</td>
<td>Default</td>
<td></td>
<td>All networks</td>
<td>✗ ✗</td>
</tr>
<tr>
<td>peer3</td>
<td></td>
<td>1.1.1.1</td>
<td>10.0.0.0/7</td>
<td>Default</td>
<td></td>
<td>All networks</td>
<td>✗ ✗</td>
</tr>
</tbody>
</table>

Add a peer
Behavior of Management Traffic

The following services and features have their traffic always ingress or egress the primary WAN/Internet uplink:

• Meraki IPsec tunnel - management connection to the Meraki Cloud
• AMP - File disposition lookups used for Advanced Malware Protection
• Security Lists - lists used for IDS/IPS signatures
• Content Filtering - Top Sites lists and Full Lists lookups
• Meraki AutoVPN tunnel termination - AutoVPN may terminate one or both uplinks if configured. Note: Client traffic inside of these VPN tunnels follow normal routing behavior
• Teleworker SSID tunnel termination - Note: Client traffic inside of these VPN tunnels follow normal routing behavior
• Non-Meraki and Client VPN tunnel termination - Note: Client traffic inside of these VPN tunnels follow normal routing behavior

The following services/tools will specifically adhere to the route priority and not necessarily ingress or egress the primary WAN/Internet uplink:

• Advanced Malware Protection registration
• Meraki Cloud Authentication
• Meraki Cloud Communication on TCP ports 80,443 and 7734
• Ping and Dashboard Throughput Live Tools
• List Updates for the following services: Content Filtering, IDS/IPS Rule Updates and Geo-IP Lists for Layer 7 Country-Based Firewall rules