Resolving NAT Mode and Site-to-site VPN conflicts

Using an MR access point, if a client connects to an SSID set for NAT Mode, it will be put on an isolated 10.0.0.0/8 network that can then be granted limited access to the local LAN. This can cause conflicts if a 10.x.x.x addressing scheme is in use elsewhere on the network.

This article describes how a conflicting subnet between NAT Mode's Meraki DHCP and a site-to-site VPN subnet is handled, as well as recommended solutions.

Overview

In the figure below, a NAT Mode client with the address of 10.44.90.223 (assigned via Meraki DHCP) is attempting to connect to the corporate network that is using a private addressing scheme of 10.0.0.0/8. A conflict occurs because there is an overlap of local and remote subnets.

*Note:* Site-to-site VPN is discussed in greater detail within this article.

Conflict

Sometimes a conflict may occur between the client’s local IP configuration and the IP configuration of the remote private network. This occurs if the client’s local network and the remote private network share overlapping subnets. In the figure above, the Site to Site VPN client has retrieved its 10.0.0.0/8 address from the MR Access Point running NAT Mode/Meraki DHCP. The last three octets of the wireless client's IP address are generated by taking the client's MAC address and running it through a hashing algorithm. If the remote VPN site is using a 10.0.0.0/n (of arbitrary size) private addressing scheme, this may cause a conflict.
where a wireless client has the same IP address as a client on the remote site. This would prevent the VPN client from connecting to the remote site entirely.

Note: The conflict of overlapping subnets will persist with either "full tunnel" or "split tunnel" Site-to-site VPN.

Solution

When working with site-to-site VPN, it is recommended that a less common client address range is configured to mitigate any chance of addressing conflicts (172.16.0.0/14, 172.16.20.0/24, 172.16.25.0/24, etc.). This means that if the remote site is using a 10.0.0.0/n network, VPN clients cannot associate with a NAT Mode SSID, and a non 10.0.0.0/n addressing scheme must be created/served to clients attempting to communicate with the remote site. In this circumstance, it may be beneficial to use a Bridge Mode SSID, configured to put clients on an isolated VLAN that can be secured as necessary with firewall rules.

Note: In the event that you are not using Meraki DHCP and you are still having a conflict regarding overlapping subnets with the remote site, Cisco Meraki Devices can support VPN translation. Please contact Cisco Meraki Support if you have any inquiries regarding the VPN translation feature.

Additional Resources

- Troubleshooting 3rd paty Site-to-site VPN
- Split-tunneling on a client VPN with Windows