Wireless Client Isolation

Overview

Wireless Client Isolation is a security feature that prevents wireless clients from communicating with one another. This feature is useful for guest and BYOD SSIDs adding a level of security to limit attacks and threats between devices connected to the wireless networks. The below sections describe the feature in more detail.

Bridge Mode Client Isolation

Client Isolation is available for SSIDs configured for **Bridge mode** however is disabled by default. When a SSID is configured for bridge mode, clients are bridged through the Access Point potentially to a specific VLAN. Upon connection to the AP, clients will be permitted to make a DHCP request on the vlan they are assigned to. After DHCP is completed, the MAC address of the default gateway is tracked for the particular client. The MAC address of the default gateway is then permitted in a layer 2 firewall that restricts all other traffic to and from the wireless client. Since this feature relies on DHCP, clients with a statically assigned IP address connected to an SSID with Client Isolation enabled will not be able to pass meaningful traffic.

Configuration

When an SSID is configured for Bridge mode a configuration option becomes visible on the Firewall and Traffic Shaping page for the SSID. This configuration option is disabled by default but can be enabled on a per SSID basis.

Client Isolation does not interoperate with IPv6-only networks

Firewall

Layer 2 LAN isolation

Client Isolation also extends to Port Profiles that can be leveraged on Access Points such as the MR30H, MR52, MR53 and MR84. More information on creating Port Profiles can be found here: [https://documentation.meraki.com/MR/.../Port_Profiles](https://documentation.meraki.com/MR/.../Port_Profiles)
**Example Scenarios - MR 25.11 and Newer**

In MR 25.11 and newer, HSRP is supported. With HSRP, egress traffic uses the virtual MAC for the default gateway, but HSRP uses the physical BIA for the source MAC on ingress traffic coming back in through the gateway. With this new functionality, the AP will allow ingress traffic from upstream devices, regardless of the source MAC. This allows Client Isolation to operate in conjunction with HSRP. In the instance that ingress traffic is sourced upstream to a client (rather than return traffic) the ingress traffic will be allowed through the MR. Return traffic from the client will be filtered (since traffic is not destined for gateway).

The figure below shows that broadcast or unicast traffic sourced from the wireless client will not be sent to the other wireless clients on the SSID.
The figure below shows that broadcast or unicast traffic sourced from a wired client on the same VLAN as the client will be allowed to reach the client via the AP, but any return traffic from the client will be blocked.
The figure below shows that DHCP traffic is allowed in addition to unicast and broadcast traffic with the gateway the client obtained though DHCP process.

Bridge Mode Client Isolation is not currently supported on mesh repeaters.

Example Scenarios - Pre-MR 25.11 Version

The figure below shows that DHCP traffic is allowed in addition to unicast and broadcast traffic with the gateway the client obtained though DHCP process.

DNS and DHCP are both allowed through the MR.
The figure below shows that broadcast or unicast traffic sourced from the wireless client will not be sent to the other wireless clients on the SSID.

The figure below shows that broadcast or unicast traffic sourced from a wired client on the same VLAN as the client will be blocked by the Access Point.
NAT Mode Client Isolation

SSIDs that are configured for NAT Mode also have basic client isolation. Basic Client Isolation is enabled by default when the SSID is configured for NAT mode and cannot be disabled.

The implications of enabling NAT mode are as follows:

- Devices outside of the wireless network cannot initiate a connection to a wireless client.
- Wireless clients cannot use Layer 2 discovery protocols to find other devices on either the wired or wireless network.

For more information on NAT mode, please see NAT Mode with Meraki DHCP.