Manually Integrating Cisco Umbrella with Meraki Networks

Overview

Integrating the Meraki dashboard and Umbrella DNS allows clients connected behind Meraki security appliances or access points to have their DNS traffic filtered through Cisco's Umbrella DNS service.

This integration allows administrators to easily apply and modify DNS-based filtering rules to multiple groups of clients on their network by simply assigning a filtering policy to a specific Meraki group policy or SSID. Once assigned, all DNS requests from clients included under that policy will be automatically redirected to Cisco's Umbrella DNS service where it will be checked against the appropriate policy configured for the Network Device in the Umbrella dashboard.

For MX integration this feature requires MX 15.10+ beta firmware. This can be enabled per-network via the dashboard Organization > Firmware upgrades page. MR integration requires MR 26.1+ beta firmware. This can also be enabled per-network via the dashboard Organization > Firmware upgrades page.

This feature is only available on MX devices with an Advanced Security license.

Configuring Umbrella DNS Integration

Linking the Meraki and Umbrella Dashboards

Integrating Umbrella DNS with a Meraki network is a simple process that requires only a few steps to get set up. For Umbrella filtering policies to be applied successfully, the Meraki and Umbrella dashboards must first be linked via the Umbrella Network Devices API Key. Once the dashboards have been linked, then Umbrella policies can be properly assigned to the appropriate Meraki SSID or group policy.

Generate the Umbrella API Key

Before linking the two dashboards, the Umbrella API Key and associated Secret must first be created on the Umbrella dashboard. This can be done from the Umbrella dashboard by selecting Admin > API Keys.
If there is no existing key available for the Umbrella Network Devices, select the blue and white plus sign (+) labeled ‘Create’ at the top right of the page. (Highlighted in the picture below) ‘Umbrella Network Devices’ should be selected by default. If not, select it and click ‘Create.’ Once the key has been generated, copy both the Key and the Secret so they can be entered on the Meraki dashboard. Be sure to save the Secret in a safe location as it will only ever be shown once.

If the ‘Umbrella Network Devices’ API Key and Secret have already been generated, use the existing API Key and Secret.

NOTE: Make sure when generating and copying the API Key that the ‘Umbrella Network Devices’ key is used, not the ‘Legacy Network Devices’ key.

WARNING: The Umbrella dashboard will only display the API Secret when it is first generated, make sure that you’ve saved both the Key and Secret before closing the page.

Apply the Umbrella API Key to a Meraki Network

Once the Umbrella API Key and secret have been generated, they need to be added to the Meraki dashboard to properly link the Meraki network and the Umbrella dashboard. This is done by going to the Network-wide > Configure > General page. Once there, scroll down to the bottom of the page and click ‘New credentials’ under the ‘Cisco Umbrella account’ header. Then paste the Umbrella API Key and Secret in the appropriate fields and click ‘Save Changes.’

Once this information has been saved the Meraki and Umbrella dashboards should now be properly linked, allowing Umbrella policies to be applied to Meraki SSIDs or group policies within the current Meraki network.
**Unlinking a Meraki Network and Cisco Umbrella**

Once the Meraki and Umbrella dashboards have been linked successfully the currently linked API Key will be displayed at the bottom of the Network-wide > Configure > General page. There is also a checkbox to delete the link between the selected Meraki network and the Umbrella dashboard.

To unlink a Meraki network from Umbrella simply check the ‘Delete linked account’ box and select ‘Save Changes’ on the Meraki dashboard. Deleting this link between accounts will clear any objects in the Umbrella dashboard that were sourced from this network in addition to any Umbrella Policies applied to SSIDs or group policies in the network.

**Linking and Applying an Umbrella Policy**

Linking an SSID or group policy to an Umbrella Policy is straightforward once the dashboards have been linked. When a Meraki SSID or group policy is linked to Umbrella, a unique Device ID is generated for that Meraki object. An Umbrella policy is then linked to that device ID on the Umbrella dashboard. This device ID is included in any DNS traffic sent to Umbrella and used to specify which Umbrella Policy that traffic should be checked against.

**NOTE:** These Meraki objects can be viewed on the Umbrella dashboard by going to Deployments > Core Identities > Network Devices. Umbrella Network Devices are automatically created when linking a Meraki SSID or group policy and use the following naming format: '<SSID/Group_Policy_name>__<Network name>_wireless'
Linking a Meraki Group Policy to an Umbrella Policy (MX & MR)

Create the Group Policy

Before linking an Umbrella policy to a Meraki group policy, the group policy must first exist in the Meraki dashboard. Group policies can be created by going to Network-wide > Configure > Group policies. Ensure the group policy is set to use ‘Custom network firewall & shaping rules’. For more guidance in creating a group policy on the Meraki dashboard, feel free to check out our more detailed documentation specifically for creating group policies.

NOTE: Before attempting to link the group policy with Umbrella, ensure that the group policy is completely saved on the Meraki dashboard first.

Link the Meraki Group Policy with Umbrella

From the Network-wide > Configure > Group policies page, select the group policy that should be linked, then select the 'Link Umbrella policies' button located under the Layer 7 firewall rules. The Meraki dashboard will then automatically create the appropriate Network Device on the Umbrella dashboard and apply the Default Policy to the group policy.

NOTE: Group policies must be set to use ‘Custom network firewall & shaping rules’ to link an Umbrella policy.

WARNING: If creating a new group policy then the policy must first be saved before it can be linked to Umbrella.

Apply an Umbrella Policy to the Group Policy

When first linking a group policy to Umbrella the Default Policy is automatically applied. To apply a different Umbrella policy to the Meraki group policy, simply select the appropriate Umbrella policy from the dropdown on the group policy details page for the appropriate group policy, then select ‘Save’ at the bottom of the page.

If the Umbrella policy does not yet exist then it must first be created from the Umbrella dashboard. This can be done by navigating to Policies > Management > All Policies on the Cisco Umbrella dashboard, then clicking ‘Add’ at the top right corner and following through with the necessary policy creation steps. Once the Umbrella policy has been created it can now be applied to the appropriate Meraki group policy from the Meraki dashboard.
Apply the Group Policy to Clients

Apply the Group Policy to Specific Clients (MX & MR)

To apply the Umbrella filtering policy to specific end clients, assign the Meraki group policy to the client from the Meraki dashboard. Group policies can be applied to clients in various ways, including utilizing an Active Directory integration, or to simply manually assign a policy from the Network-wide > Monitor > Clients page. Filter the client list down to the intended client, select the checkbox to the left for that client, then use the Policy dropdown menu to apply the appropriate group policy containing the Umbrella policy to the client. For a more detailed overview of applying a group policy to a specific client, check out our dedicated group policy documentation.

Apply the Group Policy to a Whole Subnet (MX Only)

When MX Umbrella integration is available, an Umbrella enabled Meraki group policy can be applied to an entire subnet of clients. In this configuration, any traffic that passes through the MX with a source IP contained within that subnet will be subject to Umbrella filtering for the Umbrella policy selected in the relevant Meraki group policy.

To do so, first go to Security & SD-WAN > Configure > Addressing & VLANS. Then, select the appropriate subnet from the Subnets list. In the accompanying dialog box, use the group policy drop-down menu to select the appropriate group policy and associated Umbrella Policy to apply. Finally, select Update, then
Save to apply the changes. For more information about applying a group policy to an entire subnet, feel free to check out our dedicated group policy documentation.

Linking an SSID to an Umbrella Policy (MR Only)

Create the SSID

Before linking an Umbrella policy to a Meraki SSID, the SSID must first exist in the Meraki dashboard. SSIDs can be enabled by going to Wireless > Configure > SSIDs. For more guidance in creating and configuring an SSID on the Meraki dashboard, feel free to check out our more detailed documentation on Enabling and Naming SSIDs, and also on Client IP Assignment modes for SSIDs.

NOTE: Ensure that the SSID is completely saved in the Meraki dashboard before attempting to link an SSID with Umbrella.

Link the SSID to Umbrella

Linking an SSID to Umbrella is done from the Wireless > Configure > Firewall & traffic shaping page, under the Block Applications and Content Categories header for the appropriate SSID. Simply select ‘Link Umbrella Policies’ on the appropriate SSID and the Meraki dashboard will automatically create the appropriate Network Device on the Umbrella dashboard and apply the Default Policy to the SSID.

Umbrella integration with MR is currently supported for all client addressing types found under the Access Control page.

Apply an Umbrella Policy to the SSID

After linking an SSID to Umbrella the Default policy is automatically applied. To apply a different Umbrella Policy, simply select the appropriate Umbrella Policy from the dropdown on the Firewall & traffic shaping page, then select ‘Save’ at the bottom of the page.

If the Umbrella policy does not yet exist then it must first be created from the Umbrella dashboard. This can be done by navigating to Policies > Management > All Policies on the Cisco Umbrella dashboard, then clicking ‘Add’ at the top right corner and following through with the necessary policy creation steps. Once the policy has been created it can now be applied to the appropriate Meraki SSID from the Meraki dashboard.
Removing an Umbrella Policy from an SSID or group policy

To remove an Umbrella Policy from an SSID or group policy navigate to the Wireless > Configure > Firewall & traffic shaping page for SSIDs or the Network-wide > Group policies > Group policy details page for the appropriate group policy. Under the currently applied Umbrella policy click 'Disconnect from Cisco Umbrella' followed by 'Yes' in the confirmation popup.

**WARNING:** Disconnecting an SSID or group policy from Umbrella will delete the associated Object from the Umbrella dashboard and unlink any policies applied to that SSID or group policy in the Meraki dashboard.
This section of the article describes in detail the expected traffic flow of DNS traffic from clients after an SSID or group policy has been successfully linked to an Umbrella filtering policy.

1. Client sends a DNS Query
2. Meraki intercepts the DNS query and attaches an identifier to the DNS query to identify what Umbrella policy this request should be checked against.
3. Meraki then encrypts the DNS query using DNSCrypt, source NAT's the packet to the MR management IP and redirects it to the appropriate Umbrella endpoint
4. After arriving at the Umbrella endpoint the DNS query is decrypted and checked against the appropriate Umbrella policy (based on the attached identifier) to determine if it should be allowed or not.
5. If the request is allowed then Umbrella will return an encrypted DNS response with the appropriate IP.
6. If the request should be blocked then Umbrella will return an encrypted DNS response pointing to the Umbrella block page.

7. The client is sent the requested web page based on applied policy.

NOTE: DNSCrypt Compatibility

Access points that do not support 802.11ac, such as the MR18, will still be able to utilize Umbrella DNS services but do not support the use of DNSCrypt when communicating back to the Umbrella servers. All access points that are capable of 802.11ac or newer fully support the use of DNSCrypt with Umbrella DNS.

NOTE: HTTPS Blocking

Just like Meraki's content filtering, blocked requests for HTTPS content will not load the Umbrella blocked page correctly. Instead, users will simply be presented with a generic 'Webpage is not available' error.

NOTE: Cisco Umbrella has 2 potential endpoints that Meraki will send DNS traffic to: 208.67.222.222/32 and 208.67.220.220/32. Make sure that bi-directional UDP 443 to both of these addresses is allowed on any upstream devices.

**DNS Exclusion**

When an SSID is configured in 'Bridge mode' the option to configure DNS Exclusion will be available under the Policy selection dropdown menu. This allows administrators to specify domains that should be excluded from Umbrella filtering. DNS requests for excluded domains will not be redirected to Umbrella and will instead be forwarded to the DNS server specified by the client. This is extremely useful for preventing DNS requests for local resources from being redirected to Umbrella and instead allowing them to reach internal DNS servers to resolve correctly. MRs automatically add the '.local' and 'in-addr.arpa' domains to be excluded from Umbrella redirection by default.

NOTE: DNS Exclusion is only available for SSIDs configured in Bridge mode.

NOTE: DNS Exclusion is not available for configuration on group policies that are linked to Umbrella policies. The domain exclusions for group policies will adhere to the configuration of the SSID. For example, if the 'Employee' SSID is excluding 'meraki.com' from Umbrella lookups, and a client with an assigned group policy linked to a different Umbrella policy connects, then 'meraki.com' will still be excluded from DNS lookups sourced from that client.

**Troubleshooting**

**General Troubleshooting Steps**

- Ensure that the Umbrella and Meraki dashboards are properly linked via API from **Network-wide > General** (Section 2.1)
- Ensure that the SSID/group policy has been linked to Umbrella in the Meraki dashboard and has an Umbrella Policy applied from either **Network-wide > Group polices** or **Wireless > Firewall & traffic shaping** respectively. (Section 3.1 & 3.2)
• Ensure that the appropriate Identity exists under **Deployments > Core Identities > Network Devices** on the Umbrella dashboard (Section 3)

• Ensure that the correct Policy is assigned to the correct Network Device in the Umbrella dashboard from **Policies > Policy List**

• Ensure that bi-directional UDP 443 traffic is allowed to the Umbrella endpoints - 208.67.222.222/32 and 208.67.220.220/32 (Section 4)