Content Filtering Troubleshooting

Cisco Meraki MX Security Appliances can be configured to block web traffic using Content Filtering. Content Filtering uses URL patterns, pre-defined categorizations and other specifications for determining what types of traffic are let through the firewall. It can be set, for example, to block all websites that are known to be categorized as 'Games' or 'Social Networking.' The MX will return a page that displays a message letting the user know their page is being blocked by their administrator so they understand why they cannot reach a blocked site.

This article covers troubleshooting steps for resolving issues that are commonly experienced when using Content Filtering. For instructions on configuring Content Filtering based on Active Directory LDAP groups, please refer to this article.

Configuring Content Filtering

Content Filtering can be used to filter content passing through your security appliance based on content known to exist on specified web pages. Content Filtering is best used for setting catch-all blocks for certain categories of traffic, or for blocking certain URL patterns.

Content Filtering settings can be found in the Dashboard by navigating to Security & SD-WAN > Configure > Content Filtering.

Instructions on setting up Content Filtering, including details about what each section of the page does (and how to block all web traffic other than whitelisted pages), can be found in this article.

The content filtering feature is available only with an Advanced Security Edition License.

Troubleshooting Content Filtering

The following sections outline troubleshooting steps for a variety of common issues experienced when using Content Filtering.

Category Filtering

Category Filtering provides a pre-made, regularly-updated list of categories that can be selected to block traffic to sites with content matching that category.

How are categories and/or reputation determined?

Category Filtering provides a list of categories than can be selected to block all web traffic destined to a URL/IP that matches with these categories on a hosted list. The list of website categories is hosted by BrightCloud. BrightCloud determines the categorization and reputation of all URLs/IPs that pass through Meraki Category Filtering. Meraki does not determine the reputation of domains directly, and requests for reclassification can be made through BrightCloud's reclassification request tool on their website.

The Meraki Dashboard has a URL category lookup tool on the Content Filtering page, below the Blocked website categories box, which can be used to check the category of a website before you decide to block that category. It is highly recommended to check for important URLs before enabling content filtering to ensure something is not accidentally blocked when it should be allowed.
How can one unblock a site that is being blocked?

If a site is being blocked because it matches a certain category you’ve blocked, but you do not want to disable that category, you can whitelist the URL pattern. This is the easiest way to whitelist a particular site that may be blocked by a content category. URL whitelisting can be found on the Content Filtering page. Examples of pattern matching and its hierarchy can be found in this article.

If you have a website that you believe is being miscategorized by your security appliance's firewall, you can submit a URL categorization change request here. If you have a website that is marked as malicious when it should not be, you can submit a URL reputation change request and/or an IP reputation change request.

Additionally, you can remove the Content Filtering category, or can leave it out of the list until Brightcloud is able to process a reputation change.

Why is a site being blocked when it should not be?

Sometimes, sites will be blocked even though their URL category is not blocked. Usually this happens when the IP has a bad reputation but the URL reputation is good. This happens commonly with very large domains like Google that own many IP addresses and sometimes purchase new IP addresses that have not yet been recategorized to take their new owner into consideration. In situations like this, these IPs sometimes have a category of 'Phishing and Other Frauds,' or various other categories that may actually be blocked:

This issue can be permanently resolved by upgrading your MX Firmware to the latest stable firmware version. In the latest firmware revision, URL reputation is prioritized over IP reputation, as opposed to IP reputation being the deciding factor on previous firmware versions. Firmware can be upgraded by navigating to Organization > Monitor > Firmware upgrades.

If you are on the latest stable firmware version and are still experiencing issues with sites being blocked that should not be, there are a few other factors that
could contribute:

- **Group Policies**: Often, a client will have a group policy applied to it that will override the default category whitelist. Group policy rules always take priority over default network rules.

- **Blocked URL Patterns**: Blocked URL patterns could match with the site you are attempting to reach. Make sure the site is not blocked here.

- **AMP**: Sometimes, downloads on a site will be blocked. This can be caused by AMP (threat protection). Make sure the site is on the whitelist on your Threat Protection page.

- **Upstream Firewall**: Try finding the client you are using by navigating to **Network-wide > Monitor > Clients**, opening their client page, and setting their 'Policy' (lower-left corner) to 'Whitelisted.' If this is done and the client is still blocked, then the MX's firewall is probably not contributing to the block, and an upstream router/firewall could be contributing to this issue. This could also be verified by connecting directly to the upstream modem/router and seeing if the issue persists.

---

**Why is a site NOT being blocked when it should be?**

There are several factors that can contribute to a website not being blocked when it should be. Consider the following factors:

- When Content Filtering rules are configured/changed, it can take a while for them to fully take effect. This goes for both blocking and unblocking content. This process can sometimes take up to 10 minutes.

- Make sure that the client you are configuring is not whitelisted. Try finding the client you are testing with by navigating to **Network-wide > Monitor > Clients**, opening their client page, and making sure their 'Policy' is not set to 'Whitelisted.'

- Additionally, clients can also be unintentionally whitelisted by having Group Policies applied to them. ALL Group Policy rules take priority over default network rules unless set to 'Use network default' settings.

- Check to make sure that the URL is not in the URL whitelist on the Content Filtering page.

- It is possible that the site does not actually have a good reputation, or may be in a different category than it should be. Be sure to check the IP/URL reputation on BrightCloud.

- In the latest stable firmware version, URL reputation is prioritized over IP reputation, as opposed to IP reputation being the deciding factor on previous firmware versions. If for some reason the IP has a different categorization then the URL, the client could be allowed through. Firmware can be upgraded by navigating to **Organization > Monitor > Firmware upgrades**.

---

**How can one tell what policy is blocking a client?**

If a client is being blocked from accessing a page, the easiest way to tell whether content filtering is blocking the traffic is to check your Event log. When looking at the Security Appliance network in the Dashboard, navigate to **Network-wide > Monitor > Event log**. To help narrow down the scope, the event type 'Content filtering blocked URL' can be included in the 'Event type include' field.
In the 'Details' section, the category will be defined if the traffic was blocked by the content filter. You will also be able to see what IP address and URL is being blocked. This can also be helpful information to use for whitelisting embedded content on a page.

Why is the Meraki block page not displayed?

If the website you are trying to reach is using HTTPS/SSL (rather than HTTP), the browser will display an error page rather than the Meraki block page. Because HTTPS/SSL traffic is encrypted, the MX cannot decrypt and redirect HTTPS traffic to the block page. Instead, the request will simply time out (as seen in the image below).

Additionally, if the website/IP is being blocked by any Layer 7 Firewall rules, these will take effect before the Content Filtering rules do.

Why is an allowed site loading, but missing images/content?

Sometimes, when a page is allowed through the firewall, the page will load, but it will be missing pictures or images. This is usually because there is content on the page that is actually hosted on another domain but displayed on the page, and that hosting domain is being blocked by URL blocking, category filtering, or firewall rules.

Example:
When Category filtering for 'Social Networking' is turned on, but 'twitter.com' is explicitly allowed in the URL whitelist, the page will sometimes load, but not all
When the Event log is checked, there are entries for 'Content filtering blocked URL' for Social Networking. While 'twitter.com' was allowed, their image/content hosting domain 'twimg.com' was not.

In order to display the full page properly, the hosting domain would also need to be whitelisted.

**Why are certain downloads (like PDFs) on a page hanging or not working correctly?**

This issue is usually not related to Content Filtering. This is usually caused by AMP (threat protection) blocking certain hosts from providing downloads. There is a whitelist that can be applied by navigating to Security & SD-WAN > Configure > Threat protection. Both URLs and specific files can be whitelisted here.
Why are pages loading slowly (especially the first time they're visited)?

When the URL category list size is set to 'Full list,' it can significantly slow down access to web pages, especially the first time they're visited. If a site is not in the list of 'Top sites,' the URL will have to be looked up and this will noticeably affect browsing speeds. This value can be changed back to 'Top sites' to improve speeds if the 'Top sites' list is sufficient. This feature is found on the Content Filtering page, next to Blocked website categories.

Web Search Filtering

Web Search Filtering is not filtering searches

Web search filtering can be enabled to encourage web searches to be relayed to Safesearch for Google, Yahoo! and Bing. When the MX sees traffic that contains a web search for these sites, it redirects the content to the Safesearch alternative for the respective site. However, any search that is made through HTTPS/SSL will not be affected by this setting. Because the content on an HTTPS/SSL page is encrypted, there is no way for the MX to inspect the traffic. More information on Web search filtering can be found in this article.

Hosted email applications are being blocked

Web search filtering can also interfere with some mail applications that go through hosted services like Office 365. If it is not essential, Web search filtering should be disabled when applications like this are having issues.

URL Blocking

Blocked URL patterns are not being blocked

Several factors can contribute to Blocked URL patterns not being blocked successfully. If this is occurring, be sure to consider each of the following factors:

- Make sure the syntax for the URL pattern is correct. The more specific/lengthy a URL block entry is, the less likely it is to block the entire website. The more vague a block pattern is, the more likely it is to block the entire domain. More information on patterns for URL blocking can be found in this article.
- Make sure that the client you are configuring is not whitelisted. Try finding the client you are testing with by navigating to Network-wide > Monitor > Clients, opening their client page, and making sure their 'Policy' is not set
to 'Whitelisted.'

- Additionally, clients can also be unintentionally whitelisted by having Group Policies applied to them. ALL Group Policy rules take priority over default network rules unless set to 'Use network default' settings.

- To ensure that the firewall rules are being applied to the client, the policy on the Clients page can be set to 'Blocked' to test to make sure that the client is actually being blocked. If this works, then it is likely that the URL pattern block simply doesn't actually match the destination.

**Whitelisted URL Patterns are not being allowed**

Several factors can contribute to whitelisted URL patterns not being allowed through the firewall. If this is occurring, be sure sure to consider each of the following factors:

- Make sure the syntax for the URL pattern is correct. The more specific/lengthy a URL whitelist entry is, the less likely it is to whitelist the intended destination. The more vague a whitelist pattern is, the more likely it is to allow the entire domain. More information on patterns for URL whitelisting can be found in this article.

- Make sure that the client you are configuring is not blocked. Try finding the client you are testing with by navigating to Network-wide > Monitor > Clients, opening their client page, and making sure their 'Policy' is not set to 'Blocked.'

- Additionally, clients can also be unintentionally blocked by having Group Policies applied to them. ALL Group Policy rules take priority over default network rules unless set to 'Use network default' settings.

- Try whitelisting a client by navigating to Network-wide > Monitor > Clients, opening the client page, and setting the 'Policy' to 'Whitelisted.' If the client is still blocked, it is likely that the MX is not contributing to the issue, and an upstream firewall or ISP is blocking the traffic. This can be verified by connecting directly to the modem/upstream router, if possible.