Blocking Websites with Content Filtering and Layer 7 Firewall Rules

Cisco Meraki appliances and access points can be configured with Layer 7 firewall rules to block traffic by application or destination hostname. The MX can also perform "Content Filtering," which blocks access to websites based on their content. The MX can also redirect users to a "This website has been blocked by your network administrator" page, so a user understands why they cannot access a blocked site.

This article covers the process of creating content filtering and layer 7 firewall rules on the MX Security Appliance, as well as troubleshooting the block page.

**Note:** While MR Access Points can be configured with Layer 7 firewall rules, they will not redirect users to a block page. To read about how to configure a Layer 7 firewall rule on an MR Access Point, please consult the following article - [Creating a Layer 7 Firewall Rule](#)

### Configuring Content Filtering

To block user access to groups of websites or individual sites, follow the below instructions for creating a Content Filtering rule:

1. In Dashboard, navigate to **Security appliance > Configure > Content Filtering**.
2. To block a specific website or page, add the URL pattern for the webpage under **URL Blocking > Blocked URL Patterns**. For more information on writing a URL Pattern, click the "Learn how URL blocking works" link in Dashboard, on the **Content Filtering** page.
3. To block a category of websites, select the website category under **Category Filtering > Blocked Website Categories**. An example configuration with a blocked category can be seen below:
Content filtering

These settings will apply to all clients that are not whitelisted.

Set identity-based policies by configuring this network to authenticate clients with Active Directory.

Category filtering

Blocked website categories

Launch the URL category lookup tool

URL category list size

Full list (better coverage)

Search Filtering

Web search filtering
Disabled

YouTube for Schools
Disabled

URL blocking

Learn how URL blocking works

Blocked URL patterns

(Enter one pattern per line)

Whitelisted URL patterns

(Enter one pattern per line)

Configuring Layer 7 Firewall Rules

To prevent a user from using a certain port/application, accessing a range of IP addresses, or using a certain category of web services, the network admin should configure a Layer 7 Firewall rule. Instructions for doing so are available on the following KB Article - Creating a Layer 7 Firewall Rule.
Testing a Blocking Rule

**Note:** It may take several minutes for a new block rule to take effect. If the website remains available after this time, reference the Troubleshooting the Block Page section of this article. Please note that HTTPS requests will not result in a block page, refer to the Troubleshooting section for more details.

1. Use a non-whitelisted device to test the block rule. This device must be connected to the network behind a LAN port on the MX Security Appliance.
2. Open a browser on the device and clear the browsing cache. If the blocked website has been cached, the cached page will be displayed in the browser.
3. Try to access the blocked website in this browser. If a block page loads, similar to the image below, the block is successful. If the blocked site still loads or no block page appears, refer to the Troubleshooting section for next steps.

![Block Page Image](https://example.com/block.png)

Troubleshooting

The following instructions outline troubleshooting steps for a number of common issues regarding the block page:

**Blocked Site is Still Accessible**

1. Make sure to clear the browser cache. If the blocked page has been cached by the browser, the cached page may still appear even though the block is working.
2. Verify that the client device is not whitelisted; a whitelisted device will not be affected by filtering rules on the MX. To check if the device has been whitelisted on the MX, consult the following article - [Viewing Blocked and/or Whitelisted Devices on Meraki Dashboard](#)
3. If the website should be blocked by a **Blocked Website Category**, it is possible that this particular site is not included under that category. Try including the site under **Blocked URL Patterns** to block that specific website.
4. If the website is listed as a **Blocked URL Pattern**, make sure the specific syntax of that rule matches the URL in the browser. For more information about the syntax of a URL pattern, click the "Learn how URL blocking works" link in Dashboard, on the **Content Filtering** page.
5. If the website is listed as a **Blocked URL Pattern**, verify the website does not perform a redirect to another URL.
1. If your browser/the website is using HTTPS/SSL, the browser will not be forwarded to the block page. Due to the encrypted nature of SSL requests, the MX cannot decrypt and redirect HTTPS traffic. Instead, the MX will force the request to timeout (an example of which can be seen in Fig. 3, below).

2. If the device is connected to a Cisco Meraki MR that has its own Layer 7 Firewall rules, the MR's firewall rules will apply before the Content Filtering/Layer 7 Firewall rules on the MX. Since the MR does not forward to a block page, the request will timeout instead of reaching a block page.