Access Control Rules: URL Filtering

The following topics describe how to configure URL filtering for your Firepower System:

- URL Conditions (URL Filtering), page 1
- Reputation-Based URL Filtering, page 2
- Manual URL Filtering, page 5
- Limitations to URL Filtering, page 6
- HTTP Response Pages, page 8

URL Conditions (URL Filtering)

URL conditions control the websites that users on your network can access. This feature is called URL filtering.

- Reputation-based URL filtering—With a URL Filtering license, you can control access to websites based on the URL’s general classification (category) and risk level (reputation).
- Manual URL filtering—With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic. SSL rules do not support manual URL filtering.

When you block unencrypted or decrypted web traffic, you can allow the user’s browser its default behavior, or you can display a generic system-provided or custom HTTP response page. Interactive blocking gives users a chance to bypass a website block by clicking through a warning page.

Rules with URL Conditions

The following rules support URL conditions:

- access control
- SSL (category and reputation only; no manual URL filtering)
Filtering HTTPS Traffic

To filter encrypted traffic, the system determines the requested URL based on information passed during the SSL handshake: the subject common name in the public key certificate used to encrypt the traffic.

HTTP filtering considers the entire host name, including subdomains. However, HTTPS filtering disregards subdomains within the subject common name, so do not include subdomain information when manually filtering HTTPS URLs in access control policies. For example, use example.com rather than www.example.com.

In an SSL policy, you can handle and decrypt traffic to specific URLs by defining a distinguished name SSL rule condition. The common name attribute in a certificate's subject distinguished name contains the site's URL. Decrypting HTTPS traffic allows access control rules to evaluate the decrypted session, which improves URL filtering.

Controlling Traffic by Encryption Protocol

The system disregards the encryption protocol (HTTP vs HTTPS) when performing URL filtering in access control policies. This occurs for both manual and reputation-based URL conditions. In other words, URL filtering treats traffic to the following websites identically:

- http://example.com/
- https://example.com/

To configure a rule that matches only HTTP or HTTPS traffic, add an application condition to the rule. For example, you could allow HTTPS access to a site while disallowing HTTP access by constructing two access control rules, each with an application and URL condition.

The first rule allows HTTPS traffic to the website:

Action: Allow
Application: HTTPS
URL: example.com

The second rule blocks HTTP access to the same website:

Action: Block
Application: HTTP
URL: example.com

Reputation-Based URL Filtering

With a URL Filtering license, you can control your users' access to websites based on the category and reputation of requested URLs:

- Category—A general classification for the URL. For example, ebay.com belongs to the Auctions category, and monster.com belongs to the Job Search category. A URL can belong to more than one category.
• Reputation—How likely the URL is to be used for purposes that might be against your organization’s security policy. Reputation range from High Risk (level 1) to Well Known (level 5).

**Note**

To see URL category and reputation information in events and application details, you must create at least one rule with a URL condition. You must also enable communications with Cisco Collective Security Intelligence (CSI) to obtain the latest threat intelligence.

**Caution**

Initially adding a category or reputation URL condition to a rule restarts the Snort process, which interrupts traffic inspection, when you deploy configuration changes. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic.

**Benefits of Reputation-Based URL Filtering**

URL categories and reputations help you quickly configure URL filtering. For example, you can use access control to block high risk URLs in the Abused Drugs category.

Using category and reputation data simplifies policy creation and administration. It grants you assurance that the system controls web traffic as expected. Because Cisco continually updates its threat intelligence with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Sites that (for example) represent security threats, or that serve undesirable content, may appear and disappear faster than you can update and deploy new policies.

Some examples of how the system can adapt include:

- If an access control rule blocks all gaming sites, as new domains get registered and classified as Gaming, the system can block those sites automatically.
- If an access control rule blocks all malware sites, and a blog page gets infected with malware, the system can recategorize the URL from Blog to Malware and block that site.
- If an access control rule blocks high-risk social networking sites, and somebody posts a link on their profile page that contains links to malicious payloads, the system can change the reputation of that page from Benign Sites to High Risk and block it.

**Performing Reputation-Based URL Filtering**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Filtering</td>
<td>URL Filtering</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>
Initially adding a category or reputation URL condition to an access control rule restarts the Snort process, which interrupts traffic inspection, when you deploy configuration changes. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic.

Caution

Procedure

**Step 1**
In the access control rule editor, click the **URLs** tab.

**Step 2**
Click the **Category** tab in the **Categories and URLs** list.

**Step 3**
Find and select the categories of URL you want to add from the **Category** list. To match web traffic regardless of category, select **Any** category. To search for categories to add, click the **Search for a category** prompt above the **Category** list, then type the category name. The list updates as you type to display matching categories.

**Tip**
You can add a maximum of 50 items to the **Selected URLs** to match in a single URL condition. Each URL category, optionally qualified by reputation, counts as a single item. Note that you can also use literal URLs and URL objects in URL conditions, but you cannot qualify these items with a reputation.

**Step 4**
If you want to qualify your category selections, you must click a reputation level from the **Reputations** list. If you do not specify a reputation level, the system defaults to **Any**, meaning all levels. You can only select one reputation level.

- If the rule blocks or monitors web access (the rule action is **Block**, **Block with reset**, **Interactive Block**, **Interactive Block with reset**, or **Monitor**) selecting a reputation level also selects all reputations more severe than that level. For example, if you configure a rule to block or monitor **Suspicious sites** (level 2), it also automatically blocks or monitors **High risk** (level 1) sites.

- If the rule allows web access, whether to trust or further inspect it (the rule action is **Allow** or **Trust**), selecting a reputation level also selects all reputations less severe than that level. For example, if you configure a rule to allow **Benign sites** (level 4), it also automatically allows **Well known** (level 5) sites.

- If you change the rule action for a rule, the system automatically changes the reputation levels in URL conditions according to the above points.

**Step 5**
Click **Add to Rule** to add the selected items to the **Selected URLs** list.

**Step 6**
Save or continue editing the rule.

Example

The following graphic shows the URL condition for an access control rule that blocks: all malware sites, all high-risk sites, and all non-benign social networking sites. It also blocks a single site, example.com, which is represented by a URL object.
The following table summarizes how you build the condition shown above. Note that you cannot qualify a literal URL or URL object with a reputation.

**Table 1: Building A URL Condition**

<table>
<thead>
<tr>
<th>To block...</th>
<th>Select this Category or URL Object...</th>
<th>And this Reputation...</th>
</tr>
</thead>
<tbody>
<tr>
<td>malware sites, regardless of reputation</td>
<td>Malware Sites</td>
<td>Any</td>
</tr>
<tr>
<td>any URL with a high risk (level 1)</td>
<td>Any</td>
<td>1 - High Risk</td>
</tr>
<tr>
<td>social networking sites with a risk greater than benign (levels 1 through 3)</td>
<td>Social Network</td>
<td>3 - Benign sites with security risks</td>
</tr>
<tr>
<td>example.com</td>
<td>the URL object named example.com</td>
<td>none</td>
</tr>
</tbody>
</table>

**What to Do Next**

- Deploy configuration changes; see Deploying Configuration Changes.

**Manual URL Filtering**

In access control rules, you can supplement or selectively override category and reputation-based URL filtering by manually filtering individual URLs, groups of URLs, or URL lists and feeds. You can perform this type of URL filtering without a special license. Manual URL filtering is not supported in SSL rules; instead, use distinguished name conditions.

For example, you might use access control to block a category of websites that are not appropriate for your organization. However, if the category contains a website that is appropriate, and to which you want to provide access, you can create a manual Allow rule for that site and place it before the Block rule for the category.

When manually filtering specific URLs, carefully consider other traffic that might be affected. To determine whether network traffic matches a URL condition, the system performs a simple substring match. If the requested URL matches any part of the string, the URLs are considered to match.

For example, if you allow all traffic to example.com, your users could browse to URLs including:

- http://example.com/
- http://example.com/newexample

---

Selected URLs (4)

- Any (Reputation 1)
- example.com
- Malware Sites (Any Reputation)
- Social Network (Reputations 1-3)
Performing Manual URL Blocking

As another example, consider a scenario where you want to explicitly block ign.com (a gaming site). However, substring matching means that blocking ign.com also blocks verisign.com, which might not be your intent.

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 In the access control rule editor, click the URLs tab.
Step 2 Click the URLs tab in the Categories and URLs list.
Step 3 Find and select the URLs you want to add from the URLs list:

- To add a URL object on the fly, which you can then add to the condition, click the add icon ( ) above the URLs list.
- To search for URL objects, groups, global lists, custom lists and feeds, or URL categories to add, click the Search for a URL prompt above the URLs list, then type either the name of the object, or the value of a URL or IP address in the object. The list updates as you type to display matching objects.
- To select an object, click it. Although you can right-click and select All URL objects, adding URLs this way exceeds the 50-item maximum for an access control rule.

Step 4 Click Add to Rule to add the selected items to the Selected URLs list.

Note You can also type a literal URL or IP address in the Enter URL prompt below the Selected URLs list. You cannot use wildcards (*).

Step 5 Save or continue editing the rule.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes.

Limitations to URL Filtering

Speed of URL Identification

The system cannot filter URLs before:

- a monitored connection is established between a client and server
• the system identifies the HTTP or HTTPS application in the session
• the system identifies the requested URL (for encrypted sessions, from either the ClientHello message or the server certificate)

This identification should occur within 3 to 5 packets, or after the server certificate exchange in the SSL handshake if the traffic is encrypted.

If early traffic matches all other rule conditions but identification is incomplete, the system allows the packet to pass and the connection to be established (or the SSL handshake to complete). After the system completes its identification, the system applies the appropriate rule action to the remaining session traffic.

For access control, these passed packets are inspected by the access control policy’s default intrusion policy—not the default action intrusion policy nor the almost-matched rule’s intrusion policy.

URLs with Unknown Category or Reputation
If the system does not know the category or reputation of a URL, browsing to that website does not match rules with category or reputation-based URL conditions. You cannot assign categories or reputations to URLs manually.

Manual URL Filtering
When manually filtering specific URLs, carefully consider other traffic that might be affected. To determine whether network traffic matches a URL condition, the system performs a simple substring match. If the requested URL matches any part of the string, the URLs are considered to match.

URL Filtering for Encrypted Web Traffic
When performing URL filtering on encrypted web traffic, the system:
• disregards the encryption protocol; a rule matches both HTTPS and HTTP traffic if the rule has a URL condition but not an application condition that specifies the protocol
• matches HTTPS traffic based on the subject common name in the public key certificate used to encrypt the traffic, and disregards subdomains within the subject common name
• does not display an HTTP response page for blocked traffic, even if you configured one in an access control policy

HTTP Response Pages
HTTP response pages do not appear when web traffic is blocked:
• and the session is or was encrypted
• as a result of a promoted access control rule (an early-placed blocking rule with only simple network conditions)
• after the connection has been established and allowed to flow for a few packets so the system can identify the requested URL
Search Query Parameters in URLs

The system does not use search query parameters in the URL to match URL conditions. For example, consider a scenario where you block all shopping traffic. In that case, using a web search to search for amazon.com is not blocked, but browsing to amazon.com is.

Memory Limitations for Selected Device Models

Due to memory limitations, some device models perform URL filtering with a smaller, less granular, set of categories and reputations. For example, if a parent URL's subsites have different URL categories and reputations, some devices may use the parent URL's data for all subsites. As a specific example, the system might evaluate mail.google.com using the google.com category and reputation. Affected devices include the 7100 Family and the following ASA models: ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5512-X, ASA5515-X, ASA5516-X, and ASA5525-X. For virtual devices, see the *Firepower System Virtual Installation Guide* for information on allocating the correct amount of memory to perform category and reputation-based URL filtering.

HTTP Response Pages

Users see an HTTP response page if you block their session. You can either display a generic system-provided response page, or you can enter custom HTML.

When the system blocks a user’s HTTP web request, what the user sees in a browser depends on how you block the session, using the access control rule’s action. You should select:

- **Block** or **Block with reset** to deny the connection. A blocked session times out; the system resets Block with reset connections. However, for both blocking actions, you can override the default browser or server page with a custom page that explains that the connection was denied. The system calls this custom page an *HTTP response page*.

- **Interactive Block** or **Interactive Block with reset** if you want to display an interactive *HTTP response page* that warns users, but also allows them to click a button to continue or refresh the page to load the originally requested site. Users may have to refresh after bypassing the response page to load page elements that did not load.

In each access control policy, you configure the interactive HTTP response page separately from the response page you use to block traffic without interaction, that is, using a Block rule. For example, you could display the system-provided page to users whose sessions are blocked without interaction, but a custom page to users who can click to continue.

HTTP response pages do not appear when web traffic is blocked:

- and the session is or was encrypted
- as a result of a promoted access control rule (an early-placed blocking rule with only simple network conditions)
- after the connection has been established and allowed to flow for a few packets so the system can identify application details and any requested URL
Configuring an HTTP Response Page

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

When you enter custom text for an HTTP response page, a counter shows how many characters you have used.

Reliable display of HTTP response pages to your users depends on your network configuration, traffic loads, and size of the page. If you build a custom response page, a smaller page is more likely to display successfully.

**Procedure**

**Step 1**
In the access control policy editor, click the **HTTP Responses** tab.
If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

**Step 2**
For the **Block Response Page** and the **Interactive Block Response Page**, choose responses from the drop-down lists. For each page, you have the following choices:

- To use a generic response, choose **System-provided**. You can click the view icon (🔍) to view the HTML code for this page.
- To create a custom response, choose **Custom**. A pop-up window appears, prepopulated with system-provided code that you can replace or modify. When you are done, save your changes. You can edit a custom page by clicking the edit icon (✍).
- To prevent the system from displaying an HTTP response page, choose **None**. Selecting this option for interactively blocked sessions prevents users from clicking to continue; the session is blocked without interaction.

**Step 3**
Click **Save** to save the policy.

**What to Do Next**

- Deploy configuration changes; see Deploying Configuration Changes.

**Interactive Block HTTP Response Pages**

When you block a user’s HTTP web request using an access control rule, setting the rule action to **Interactive Block** or **Interactive Block with reset** gives that user a chance to bypass the block by clicking through a warning **HTTP response page**. You can display a generic system-provided response page or you can enter custom HTML.
You configure the interactive HTTP response page separately from the response page you configure for Block rules. For example, you could display the system-provided page to users whose sessions are blocked without interaction, but a custom page to users who can click to continue.

By default, the system allows users to bypass blocks for 10 minutes (600 seconds) without displaying the warning page on subsequent visits. You can set the duration to as long as a year, or you can force the user to bypass the block every time. This limit applies to every Interactive Block rule in the policy. You cannot set the limit per rule.

If the user does not bypass the block, matching traffic is denied without further inspection; you can also reset the connection. On the other hand, if a user bypasses the block, the system allows the traffic. Allowing this traffic means that you can continue to inspect unencrypted payloads for intrusions, malware, prohibited files, and discovery data. Note that users may have to refresh after bypassing the block to load page elements that did not load.

Logging options for interactively blocked traffic are identical to those in allowed traffic, but if a user does not bypass the interactive block, the system can log only beginning-of-connection events. When the system initially warns the user, it marks any logged beginning-of-connection event with the Interactive Block or Interactive Block with reset action. If the user bypasses the block, additional connection events logged for the session have an action of Allow.

In the following situations, the response page does not appear and traffic is blocked without interaction, even if the session matches an Interactive Block rule:

- if the session was or is encrypted; this includes sessions decrypted by the system
- after a connection has been established and allowed to flow for a few packets so the system can inspect it for requested URLs and application details.

Tip
To quickly disable interactive blocking for all rules in an access control policy, display neither the system-provided page nor a custom page. This causes the system to block all connections that match an Interactive Block rule without interaction.

Configuring Interactive Blocking of Web Traffic

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

Before You Begin
Optionally, create and use a custom page to display that allows users to bypass a block; see HTTP Response Pages, on page 8.

Procedure

Step 1 In the access control policy editor, create an access control rule that matches web traffic with a URL condition.
If a view icon (_visible) appears next to a rule instead, the rule belongs to an ancestor policy, or you do not have permission to modify the rule.

**Step 2** Make sure the access control rule action is **Interactive Block** or **Interactive Block with reset**.

**Step 3** Assume users will bypass the block and choose inspection and logging options for the rule accordingly.

**Step 4** Optionally, on the **Advanced** tab, set the amount of time that elapses after a user bypasses a block before the system displays the warning page again.

If a view icon (_visible) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

**Step 5** Optionally, on the **HTTP Responses** tab, choose a custom page to allow users to bypass a block, create and use a custom page.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

**Step 6** Click **Save** to save the policy.

---

**What to Do Next**

- Deploy configuration changes; see **Deploying Configuration Changes**.

---

**Setting the User Bypass Timeout for a Blocked Website**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

---

**Procedure**

**Step 1** In the access control policy editor, click the **Advanced** tab.

**Step 2** Click the edit icon (_visible) next to General Settings.

If a view icon (_visible) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

**Step 3** In the **Allow an Interactive Block to bypass blocking for (seconds)** field, type the number of seconds that must elapse before the user bypass expires. Specifying zero forces your users to bypass the block every time.

**Step 4** Click **OK**.

**Step 5** Click **Save** to save the policy.
What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes.