URL Filtering

URL Filtering Overview

Use the URL filtering feature to control the websites that users on your network can access:

- Category and 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). This is the recommended option.
- 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. For more information, see Manual URL Filtering, on page 14.

See also Blocking Traffic with Security Intelligence, a similar but different feature for blocking malicious URLs, domains, and IP addresses.

About URL Filtering with Category and Reputation

With a URL Filtering license, you can control 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. Reputations range from Unknown risk (level 0) or Untrusted (level 1) to Trusted (level 5).

Benefits of Category and Reputation-Based URL Filtering

URL categories and reputations help you quickly configure URL filtering. For example, you can use access control to block untrusted URLs in the Hacking category. Or, you can use QoS to rate limit traffic from sites in the Streaming Video category. There are also categories for types of threats, such as a Spyware and Adware 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, 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 Games, the system can block those sites automatically. Similarly, if a QoS rule rate limits all streaming video sites, the system can automatically limit traffic to new Streaming Video sites.
- If an access control rule blocks all malware sites and a shopping page gets infected with malware, the system can recategorize the URL from Shopping to Malware Sites and block that site.
- If an access control rule blocks untrusted 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 Favorable to Untrusted and block it.

Related Topics

Snort® Restart Scenarios

URL Category and Reputation Descriptions

Category Descriptions

A description of each URL category is available from https://www.talosintelligence.com/categories.

Be sure to click **Threat Categories** to see those categories.

Reputation Level Descriptions

Go to https://talosintelligence.com/reputation_center/support and look in the Common Questions section.

URL Filtering Data from the Cisco Cloud

URL filtering based on category and reputation requires a data set provided by the Cisco cloud.

Generally, by default, when a valid URL Filtering license is applied to an active device, the URL category and reputation data set is downloaded from the Cisco cloud to the Firepower Management Center and pushed to devices. This locally stored data set is updated periodically.

When a user on the network accesses a URL, the system looks for a match in the local (downloaded) data set. If there is no match, the system checks a cache of results that the system previously looked up in the Cisco

cloud. If there is still no match, the system looks up the URL in the Cisco cloud and adds the result to the cache.

The set of URL categories may change periodically. When you receive notification of such changes, you should review the URL rules in your policies to see if you need to make changes. For more information, see If the URL Category Set Changes, Take Action, on page 17.

Best Practices for URL Filtering

Keep in mind the following guidelines and limitations for URL filtering:

Filter by Category and Reputation

Follow the instructions in How to Configure URL Filtering with Category and Reputation, on page 7.

Configure Your Policy to Inspect Packets That Must Pass Before a URL Can Be Identified

The system cannot filter URLs before:

- A monitored connection is established between a client and server.
- The system identifies the DNS, HTTP or HTTPS application in the session.
- The system identifies the requested domain or URL (for encrypted sessions, from a non-encrypted domain name, the ClientHello message or the server certificate).

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

Important! To ensure that your system examines these initial packets that would otherwise pass, see Inspection of Packets That Pass Before Traffic Is Identified and subtopics.

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 TLS/SSL handshake to complete). After the system completes its identification, the system applies the appropriate rule action to the remaining session traffic.

Block Threat Categories

Be sure that your policies specifically address Threat categories, which identify known malicious sites. Do this in addition to blocking sites with poor reputations.

For example, to protect your network from malicious sites, you must block all Threat categories in addition to blocking sites with poor or questionable reputations.

For specifics, see **Threat Categories** at the URL in URL Category and Reputation Descriptions, on page 2.

URL Conditions and Rule Order

- Position URL rules after all other rules that *must* be hit.
- URLs can belong to more than one category. It is possible to want to allow one category of websites and block another—whether explicitly or by relying on the default action. In this case, make sure you create and order URL rules so you get the desired effect, depending on whether the allow or the block should take precedence.

For additional guidelines for rules, see the following topics: Best Practices for Access Control Rules and Rule Condition Mechanics.

Uncategorized or Reputationless URLs

When you build a URL rule, you first choose the category you want to match. If you explicitly choose **Uncategorized** URLs, you cannot further constrain by reputation.

Uncategorized URLs with Untrusted reputation are handled by the **Malicious Sites** category. If you want to block uncategorized sites with any other reputation level (such as Questionable), you must block all uncategorized sites.

After selecting a category and a reputation level, you can optionally select **Apply to unknown reputation**. For example, you can create a rule that applies to sites with Untrusted, Questionable, and unknown reputations.

You cannot manually assign categories and reputations to URLs, but in access control and QoS policies, you can manually block specific URLs. See Manual URL Filtering, on page 14. See also Dispute URL Category and Reputation, on page 16.

URL Filtering for Encrypted Web Traffic

When performing URL filtering on encrypted web traffic, the system:

- (If DNS filtering is enabled) Checks to see if the system has previously seen the originating domain or the domain is in the local reputation database, and if so, takes action based on the reputation and category of the domain. Otherwise, the system processes the traffic based on your configurations for encrypted traffic, even if **Retry URL cache miss lookup** is enabled in the access control policy's advanced settings.
- 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.
- Does not use URL lists. You must use URL objects and groups instead.
- Matches HTTPS traffic based on the subject common name in the public key certificate used to encrypt the traffic, and also evaluates the reputation of any other URLs presented at any time during the transaction, including the post-decryption HTTP URL.
- Disregards subdomains within the subject common name.
- Does not display an HTTP response page for encrypted connections blocked by access control rules (or any other configuration); see Limitations to HTTP Response Pages.

URL Filtering and TLS Server Identity Discovery

The latest version of the Transport Layer Security (TLS) protocol 1.3, defined by RFC 8446, is the preferred protocol for many web servers to provide secure communications. Because the TLS 1.3 protocol encrypts the server's certificate for additional security, and the certificate is needed to match application and URL filtering criteria in access control rules, the Firepower System provides a way to extract the server certificate *without* decrypting the entire packet.

Access control policy advanced settings offer an **Early application detection and URL categorization** option for TLS Server Identity Discovery.

We strongly recommend enabling it for any traffic you want to match on application or URL criteria, especially if you want to perform deep inspection of that traffic. An SSL policy is not required because *traffic is not decrypted* in the process of extracting the server certificate.

Note

- Because the certificate is decrypted, TLS server identity discovery can reduce performance depending on the hardware platform.
- TLS server identity discovery is not supported in inline tap mode or passive mode deployments.

For more information, see Access Control Policy Advanced Settings.

HTTP/2

The system can extract HTTP/2 URLs from TLS certificates, but not from a payload.

Manual URL Filtering

- Specify URLs using a custom Security Intelligence list or feed object. Do not use a URL object or directly enter a URL into the rule. For details, see Manual URL Filtering Options, on page 14.
- If you manually filter specific URLs using URL objects or by entering URLs directly into the rule, 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.
- If you use manual URL filtering to create exceptions to other rules, position the specific rule with the exceptions above the general rule that would otherwise apply.

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.

URL Filtering in High Availability Deployments

For guidelines for URL filtering with Firepower Management Centers in high availability, see URL Filtering and Security Intelligence.

Memory Limitations for Selected Device Models

- If you are using NGIPSv, see the Cisco Firepower NGIPSv Quick Start Guide for VMware for information on allocating the correct amount of memory to perform category and reputation-based URL filtering.
- Device models with less memory store less URL data locally, and the system may therefore check the cloud more frequently to determine category and reputation for sites that are not in the local database.

  Lower-memory devices include:

  - FTD 1010
  - Virtual FTD (FTDv) with 8 GB of RAM
  - ASA 5508-X and ASA 5516-X

Related Topics

Inspection of Packets That Pass Before Traffic Is Identified

Filtering HTTPS Traffic

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

HTTPS filtering, unlike HTTP filtering, disregards subdomains within the subject common name. Do not include subdomain information when manually filtering HTTPS URLs in access control or QoS policies. For example, use example.com rather than www.example.com.

Tip 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 or QoS 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

License Requirements for URL Filtering

FTD License

- Category and reputation filtering—URL Filtering
- Manual filtering—No additional license.

Classic License

- Category and reputation filtering—URL Filtering
- Manual filtering—No additional license.

Requirements and Prerequisites for URL Filtering

Model Support

Any

Supported Domains

Any

User Roles

- Admin
- Access Admin
- Network Admin

How to Configure URL Filtering with Category and Reputation

	Do This	More Information
Step	If you will use category and reputation-based URL filtering on an NGIPSv device, allocate the required amount of memory.	Cisco Firepower NGIPSv Quick Start Guide for VMware
Step	Ensure that you have the correct licenses.	Licensing the Firepower System, including: . • URL Filtering Licenses for Firepower Threat Defense Devices • URL Filtering Licenses for Classic Devices Assign the URL Filtering license to each managed device that will filter URLs. In order to enable the feature, at least one managed device must have a URL Filtering license assigned to it.
Step	Ensure that your Firepower Management Center can communicate with the cloud to obtain URL filtering data.	Internet Access Requirements and Communication Port Requirements.

	Do This	More Information
Step	Understand limitations and guidelines and take any necessary actions.	Best Practices for URL Filtering, on page 3
Step	Enable the URL Filtering feature.	Enable URL Filtering Using Category and Reputation, on page 9
Step	Configure rules to filter URLs by category and reputation.	Configuring URL Conditions, on page 10 For the best protection against malicious sites, you must block sites by reputation AND block URLs in all Threat categories. (Optional) Supplement or Selectively Override Category and Reputation-Based URL Filtering, on page 15
Step	(Optional) Allow users to bypass a website block by clicking through a warning page.	HTTP Response Pages and Interactive Blocking
Step	Order your rules so that traffic hits key rules first.	URL Rule Order
Step	**Beta feature:** Use DNS filtering to improve URL filtering efficacy.	See: • DNS Filtering: Identify URL Reputation and Category During DNS Lookup (Beta), on page 12 • Enable DNS Filtering to Identify URLs During Domain Lookup (Beta), on page 12.
Step	(Optional) Modify advanced options related to URL filtering.	Generally, use the defaults unless you have a specific reason to change them. For information about advanced options, including the following, see Access Control Policy Advanced Settings. • **Maximum URL characters to store in connection events** • **Allow an Interactive Block to bypass blocking for (seconds)** • **Retry URL cache miss lookup**
Step	Deploy your changes.	Deploy Configuration Changes
Step	Ensure that your system receives future URL data updates as expected	Configure URL Filtering Health Monitors, on page 16
Step	Be sure you have enabled other Firepower features that protect your network from malicious sites	See Blocking Traffic with Security Intelligence.

Enable URL Filtering Using Category and Reputation

You must be an Admin user to perform this task.

Before you begin

Complete prerequisites described in How to Configure URL Filtering with Category and Reputation, on page 7.

Procedure

Step 1 Choose **System** > **Integration**.

Step 2 Click **Cloud Services**.

Step 3 Configure URL Filtering Options, on page 9.

Step 4 Click **Save**.

URL Filtering Options

The following options are on the **System > Integration** page:

Enable URL Filtering

Allows traffic filtering based on a website's general classification, or category, and risk level, or reputation. Adding a URL Filtering license automatically enables **Enable URL Filtering**. URL filtering must be enabled before you can choose other URL filtering options.

When you enable URL filtering, depending on how long since URL filtering was last enabled, or if this is the first time you are enabling URL filtering, the Firepower Management Center downloads URL data from the Cisco cloud. This process may take some time.

Enable Automatic Updates

Options for updating URL filtering threat data:

- If you enable the **Enable Automatic Updates** option on the **System > Integration** page, the Firepower Management Center checks the cloud every 30 minutes for updates. This option is enabled by default when you add a URL filtering license.
- If you need strict control over when the system contacts external resources, disable automatic updates on this page and instead create a recurring task using the scheduler. See Automating URL Filtering Updates Using a Scheduled Task.

Update Now

You can perform a one-time, on-demand update by clicking the **Update Now** button at the top of this dialog box, but you should also either enable automatic updates or create a recurring task using the scheduler. You cannot start an on-demand update if an update is already in progress.

Although daily updates tend to be small, if it has been more than five days since your last update, new URL data may take up to 20 minutes to download, depending on your bandwidth. Then, it may take up to 30 minutes to perform the update itself.

Query Cisco Cloud for Unknown URLs

Allows the system to submit URLs to the cloud for threat intelligence evaluation when users browse to a website whose category and reputation are not in the local dataset. Disable this option if you do not want to submit your uncategorized URLs, for example, for privacy reasons.

This option is enabled by default if at least one managed device has a valid URL Filtering license.

Connections to uncategorized URLs do **not** match rules with category or reputation-based URL conditions. You cannot assign categories or reputations to URLs manually.

If you use SSL rules to handle encrypted traffic, see also TLS/SSL Rule Guidelines and Limitations.

Cached URLs Expire

This setting is relevant only if **Query Cisco Cloud for Unknown URLs** is enabled.

Caching category and reputation data makes web browsing faster. By default, cached data for URLs never expires, for fastest performance.

To minimize instances of URLs matching on stale data, you can set URLs in the cache to expire. For greater accuracy and currency of threat data, choose a shorter expiration time.

A cached URL refreshes *after* the first time a user on the network accesses it after the specified time has passed. The first user does not see the refreshed result, but the next user who visits this URL does see the refreshed result.

For more information about caching of URL data, see URL Filtering Data from the Cisco Cloud , on page 2.

Configuring URL Conditions

Protect your network by controlling access to sites based on URL category and reputation.

Procedure

Step 1 In the rule editor, click the following for URL conditions:

- Access control or QoS—Click **URLs**.
- SSL—Click **Category**.

Step 2 Find and choose the URL categories that you want to control:

In an access control or QoS rule, click **Category**.

For effective protection from malicious sites, you must block URLs in all Threat categories in addition to blocking URLs with poor or questionable reputation. For a list of Threat categories, see URL Category and Reputation Descriptions, on page 2.

Be sure to click the arrows at the bottom of the list to see all available categories.

Step 3 (Optional) Constrain URL categories by choosing a **Reputation**.

Note that if you explicitly match **Uncategorized** URLs, you cannot further constrain by reputation. Choosing a reputation level also includes other reputations either more or less severe than the level you choose, depending on the rule action:

- Includes less severe reputations—If the rule allows or trusts web traffic. For example, if you configure an access control rule to allow Favorable (level 4), it also automatically allows Trusted (level 5) sites.
- Includes more severe reputations—If the rule rate limits, decrypts, blocks, or monitors web traffic. For example, if you configure an access control rule to block Questionable sites (level 2), it also blocks Untrusted (level 1) sites.

If you change the rule action, the system automatically changes the reputation levels in URL conditions.

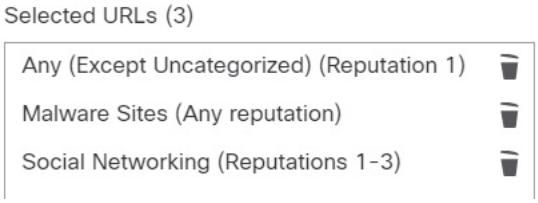
Optionally, select **Apply to unknown reputation**.

Step 4 Click **Add to Rule**, or drag and drop.

Step 5 Save or continue editing the rule.

Example: URL Condition in an Access Control Rule

The following graphic shows the URL condition for an access control rule that blocks all malware sites, all Untrusted sites, and all social networking sites with a reputation level of Neutral or worse.



The following table summarizes how you build the condition.

Blocked URL	Category	Reputation
Malware sites, regardless of reputation	Malware Sites	Any
Any untrusted URL (level 1)	Any	1 - Untrusted
Social networking sites with a reputation level of Neutral or worse (levels 1 through 3)	Social Network	3 - Neutral

What to do next

- (Optional) Supplement or Selectively Override Category and Reputation-Based URL Filtering, on page 15
- Return to How to Configure URL Filtering with Category and Reputation, on page 7.
- If you are done making changes, Deploy configuration changes; see Deploy Configuration Changes.

Rules with URL Conditions

The following table lists rules that support URL conditions, and the types of filtering that each rule type supports.

Rule Type	Supports Category and Reputation Filtering?	Supports Manual Filtering?
Access control	Yes	Yes
SSL	Yes	No; use distinguished name conditions instead
QoS	Yes	Yes

URL Rule Order

For the most effective URL matching, place rules that include URL conditions before other rules, particularly if the URL rules are block rules and the other rules meet both of the following criteria:

- They include application conditions.
- The traffic to be inspected is encrypted.

If you configure exceptions to a rule, put the exception above the other rule.

DNS Filtering: Identify URL Reputation and Category During DNS Lookup (Beta)

This feature is experimental for release 6.7. Therefore, it may not work as expected; do not use it in production environments.

This option slightly modifies URL filtering behavior and is applicable only when URL filtering is enabled and configured.

When this option is enabled:

- The system evaluates domain category and reputation early in URL transactions, when the browser looks up the domain name to get the IP address
- Category and reputation of encrypted traffic can often be determined without decryption

  If DNS filtering cannot determine the URL of encrypted traffic, that traffic is processed using your configurations for encrypted traffic.

Enable DNS Filtering to Identify URLs During Domain Lookup (Beta)

Note **This feature is experimental for release 6.7. Therefore, it may not work as expected; do not use it in production environments.**

Before you begin

- URL filtering using category and reputation must be licensed, enabled, and configured.

(DNS filtering does NOT use the following settings in the URLs tab: URL groups, URL objects, URL lists and feeds, and URLs entered into the "Enter URL" text box.)

- See limitations at DNS Filtering Limitations, on page 13.

Procedure

Step 1 In your access control policy's **Advanced** tab, select **Enable reputation enforcement on DNS traffic**.

Step 2 In the same policy, for each access control rule that has URL category and reputation blocking configured:

- In the **Applications** tab:

  If there is anything other than **any** under **Selected Applications and Filters**, add **DNS** to that list.

  (Other DNS-related options in the Available Applications list are not relevant for this purpose.)

- In the **Ports** tab:

  If there is anything other than **any** under **Selected Destination Ports**, add **DNS_over_TCP** and **DNS_over_UDP**.

Step 3 Save your changes.

What to do next

If you are done making changes: Deploy Configuration Changes.

DNS Filtering Limitations

Traffic that matches rules having action **Block with reset**, **Interactive Block**, or **Interactive Block with reset** will be treated as if the rule action were **Block**.

End users trying to access a blocked URL will experience this as an unexplained inability to connect to their page; the connection will spin and then time out.

DNS Filtering and Events

Connection events generated by DNS filtering are logged using the following fields: DNS Query, URL Category, URL Reputation, and Destination Port. The DNS Query field holds the domain name; the URL field will be blank for DNS filtering matches. The Destination Port will be 53.

Also:

- When the access control rule action is **Allow** or **Trust**, two connection events will be generated for the same traffic, one for DNS filtering (with the **DNS Query** field populated) and one for URL filtering (with the **URL** field populated).
- The first time the system encounters a particular URL, you will see two events for that single session: One event showing uncategorized/reputationless for the DNS Query, and one event showing the actual category and reputation for the URL, which were retrieved during the DNS Query and applied to the session while processing using standard URL filtering.

Manual URL Filtering

In access control and QoS 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.

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.

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.

Caution Depending on how you implement manual URL filtering, URL matching may not be what you intend. See Manual URL Filtering Options, on page 14.

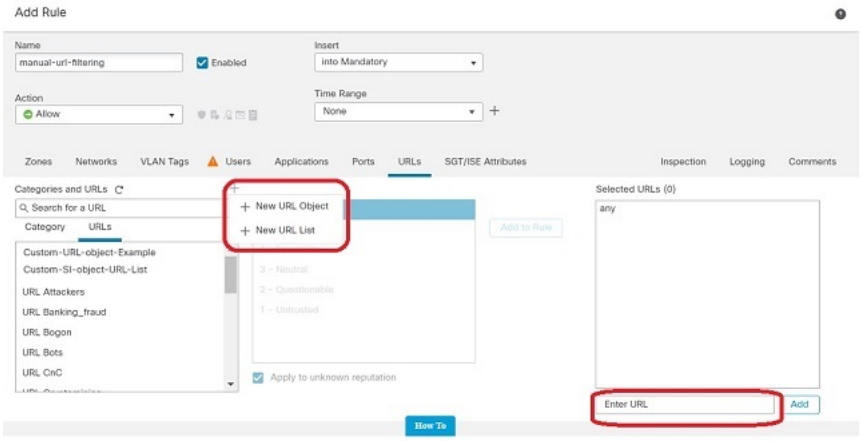
Related Topics

Security Intelligence Lists and Feeds

Manual URL Filtering Options

There are several ways to specify URLs for manual URL filtering:

Figure 1: Manual URL Filtering Options in an Access Control Rule



Option	Description
(Best practice) Use custom Security Intelligence URL list or feed objects. This is the **New URL List** option on the rule page in the web interface.	This is the recommended method for manual URL filtering. You can create a new list or feed, or choose an existing one from the URLs sub-tab of the URLs tab in an access control or QoS rule. For more information, see Custom Security Intelligence Lists and Feeds and subtopics.

Option	Description
Use URL objects, individually or as groups. (URL objects are described at URL Objects.) Or Enter URLs directly into the access control rule. (The **Enter URL** option on the rule page in the web interface.)	If you do not include a path (that is, there is no / character in the URL), the match is based on the server's hostname only. The hostname is considered a match if it comes after the :// separator, or after any dot in the hostname. For example, ign.com matches ign.com and www.ign.com, but it does not match verisign.com. If you include one or more / character, the entire URL string is used for a substring match, including the server name, path, and any query parameters. However, we recommend that you do not use manual URL filtering to block or allow individual web pages or parts of sites, as servers can be reorganized and pages moved to new paths. Substring matching can also lead to unexpected matches, where the string you include in the URL object also matches paths on unintended servers or strings within query parameters. The **Enter URL** option does not support wildcards.

Supplement or Selectively Override Category and Reputation-Based URL Filtering

In access control or QoS rules, you can use Security Intelligence URL lists and feeds to supplement, or to specify exceptions to, your category and reputation-based URL filtering rules.

(In SSL rules, use distinguished name conditions to serve this purpose.)

Before you begin

- Configure URL filtering using category and reputation. See Configuring URL Conditions, on page 10.
- Understand important best practices for manual URL filtering. See Best Practices for URL Filtering, on page 3 and Manual URL Filtering Options, on page 14.
- Configure one or more Security Intelligence objects (lists or feeds) containing the URLs that you want to use for manual filtering. See Custom Security Intelligence Lists and Feeds.

Procedure

Step 1 Navigate to the access control or QoS policy in which you will define your rule.

Step 2 Create or edit the rule in which you will add your new condition:

- If you are supplementing a category- or reputation-based URL filtering rule, edit the existing rule.
- If you are overriding or creating exceptions to a category- or reputation-based URL filtering rule, create a new rule.

Step 3 If you are creating a new rule, configure the rule name, position, action, and other options at the top of the rule.

Important! If the list or feed you are configuring in this procedure contains exceptions to category- or reputation-based rules, put this rule above those rules in the rule order.

Step 4 Click **URLs**.

Step 5 Click **URLs** (beside the **Category** tab.)

Step 6 Select the list or feed you created in the prerequisite to this task.

Step 7 Click **Add to Rule**.

Step 8 Click **Add** or continue editing the rule.

What to do next

(Optional) In SSL rules, use distinguished name conditions to configure parallel behavior.

Configure URL Filtering Health Monitors

The following health policies alert if the system has problems obtaining or updating URL category and reputation data.

- URL Filtering Monitor
- Threat Data Updates on Device

To ensure that these are configured the way you want them, see #unique_310 and Configuring Health Monitoring.

Dispute URL Category and Reputation

If you disagree with a category or reputation assigned by Talos, you can submit a request for re-evaluation.

Before you begin

You will need your Cisco account credentials.

Procedure

Step 1 In the Firepower Management Center web interface, do one of the following:

Location of Dispute Option	Path to Dispute Option
Cloud Services configuration page	a. Navigate to the **System** > **Integration** > **Cloud Services** page. b. Select **Dispute URL categories and reputations**.
Manual URL Lookup page	a. Navigate to the manual URL Lookup page: **Analysis** > **Advanced** > **URL**. b. Look up the URL in question. c. To see **Dispute** at the end of the table row, hover over the relevant entry in the list of results, then click dispute.

Location of Dispute Option	Path to Dispute Option
URL Connection Event	a. Navigate to any page under the **Analysis > Connections** menu that has a table that includes URLs. b. Right-click an item in the **URL Category** or **URL Reputation** column (show hidden columns if needed) and select an option.

The Talos web site opens in a separate browser window.

Step 2 Sign in to the Talos site with your Cisco credentials.

Step 3 Review the information and follow the instructions on the Talos page.

Step 4 Look for information on the Talos site about how submitted disputes are handled and what response to expect, if any.

The dispute process is independent of Firepower products.

If the URL Category Set Changes, Take Action

Smart License	Classic License	Supported Devices	Supported Domains	Access
URL Filtering	URL Filtering	Any	Any	Admin/Access Admin/Network Admin

The set of URL Filtering categories may occasionally change, in order to accommodate new web trends and evolving usage patterns.

These changes affect both policies and events.

Shortly before URL category changes are scheduled to occur, and after they occur, you will see alerts in the list of rules in any access control, SSL, and QoS policy that is affected by the changes, and on URL or Category in rules that you edit.

You should take action when you see these alerts.

Note Updates to the URL category set as described in this topic are distinct from the changes that simply add new URLs to existing categories or re-classify misclassified URLs. This topic does not apply to category changes for individual URLs.

Procedure

Step 1 If you see an alert beside a rule in an access control policy, hover over the alert to see details.

Step 2 If the alert mentions changes to URL categories, edit the rule to see further details.

Step 3 Hover over the URL or Category in the rule dialog to see general information about the type of changes.

Step 4 If you see an alert beside a category, click the alert to view details.

Step 5 If you see a "More information" link in the description of a change, click it to view information about the category on the Talos web site.

Alternately, see a list and descriptions all categories at the link in URL Category and Reputation Descriptions, on page 2.

Step 6 Depending on the type of change, take appropriate action:

Type of Category Change	What The System Will Do	What You Should Do
Existing category will soon be deprecated	Nothing yet. You have a few weeks to change affected rules. If you do not take action in that time, the system eventually will not be able to redeploy the policy.	Remove this category from all rules that include it. If there is a similar new category, consider using that category instead.
New category is added	By default, the system does not use newly added categories.	Consider creating new rules for the new category.
Existing category is deleted	The category will appear in the rule in strikethrough text (that is, with a line through the category name.)	You must delete the obsolete category from the rule before you can deploy the policy.

Step 7 Check your SSL rules (Category) for these changes and take action as needed.

Step 8 Check your QoS rules (URL) for these changes and take action as needed.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

URL Category and Reputation Changes: Effect on Events

- When URL categories change, events that the system processed before the category change will be associated with their original category names and will be labeled with **Legacy**. Events that the system processed after the category change will be associated with the new categories.

  Older, legacy events will age out of the system over time.

- If a URL does not have a reputation at the time it was processed, the URL Reputation column in the event viewer will be empty.

Troubleshoot URL Filtering

Expected URL Category is Missing from the Categories List

The URL filtering feature uses a different set of categories than the Security Intelligence feature; the category that you expect to see may be a Security Intelligence category. To see those categories, look at the **URLs** tab on the **Security Intelligence** tab in an access control policy.

Initial Packets Are Passing Uninspected

See Inspection of Packets That Pass Before Traffic Is Identified and subtopics.

Health alert: "URL Filtering registration failure"

Verify that your FMC and any proxies can connect to the Cisco cloud. You may need information about URL Filtering and URL categories in the following topics: Internet Access Requirements and Communication Port Requirements.

How can I find the category and reputation of a particular URL?

Do a manual lookup. See Finding URL Category and Reputation.

Error when attempting a manual lookup: "Cloud Lookup Failure for <URL>"

Make sure the feature is properly enabled. See the prerequisites in Finding URL Category and Reputation.

URL appears to be incorrectly handled based on its URL category and reputation

Problem: The system does not handle the URL correctly based on its URL category and reputation.

Solutions:

- Verify that the URL category and reputation associated with the URL are what you think they are. See Finding URL Category and Reputation.
- The following issues may be addressed by settings described in URL Filtering Options, on page 9, accessible using Enable URL Filtering Using Category and Reputation, on page 9.
  - The URL cache may hold stale information. See information about the **Cached URLs Expire** setting in URL Filtering Options, on page 9.
  - The local data set may not be updated with current information from the cloud. See information about the **Enable Automatic Updates** setting in URL Filtering Options, on page 9.
  - The system may be configured to *not* check the cloud for current data. See information about the **Query Cisco cloud for unknown URLs** setting in URL Filtering Options, on page 9.
- Your access control policy may be configured to pass traffic to the URL without checking the cloud. See information about the **Retry URL cache miss lookup** setting in Access Control Policy Advanced Settings.
- See also Best Practices for URL Filtering, on page 3.
- If the URL is processed using an SSL rule, see TLS/SSL Rule Guidelines and Limitations and SSL Rule Order

- Verify that the URL is being handled using the access control rule that you think it is being handled by, and that the rule does what you think it does. Consider rule order.
- Verify that the local URL category and reputation database on the Firepower Management Center is successfully being updated from the cloud and that managed devices are successfully being updated from the Firepower Management Center.

  Status of these processes are reported in the Health Monitor, in the **URL Filtering Monitor** module and the **Threat Data Updates on Devices** module. For details, see Health Monitoring.

If you want to immediately update the local URL category and reputation database, go to **System** > **Integration**, click **Cloud Services**, then click **Update Now**. For more information, see URL Filtering Options, on page 9.

A URL category or reputation is not correct

For access control or QoS rules: Use manual filtering, paying careful attention to rule order. See Manual URL Filtering, on page 14 and Configuring URL Conditions, on page 10.

For SSL rules: Manual filtering is not supported. Instead, use distinguished name conditions.

See also Dispute URL Category and Reputation, on page 16.

Web pages are slow to load

There is a tradeoff between security and performance. Some options:

- Consider modifying the **Cached URLs Expire** setting. Click **System** > **Integration**, then select **Cloud Services**. For information, see URL Filtering Options, on page 9.
- Consider deselecting the **Retry URL cache miss lookup** setting in Access Control Policy Advanced Settings.

Events Do Not Include URL Category and Reputation

- Make sure you have included applicable URL rules in an access control policy, the rules are active, and the policies have been deployed to the relevant devices.
- URL category and reputation do not appear in an event if the connection is processed before it matches a URL rule.
- The rule that handles the connection must be configured for URL category and reputation.
- Even if you have configured URL categories in the Categories tab in an SSL rule, you must also configure the URLs tab in a rule in your access control policy.

DNS Filtering is not working

Make sure you have completed all prerequisites and steps in Enable DNS Filtering to Identify URLs During Domain Lookup (Beta), on page 12.

An End User Tries to Access a Blocked URL and the Page Just Spins and Times Out

When DNS Filtering is enabled and end users access a URL that is blocked, the page will spin but not load. End users are not notified that the page is blocked. This is currently a limitation when DNS filtering is enabled.

See DNS Filtering Limitations, on page 13.

Events Include URL Category and Reputation but URL Field is Blank

If the DNS Query field is populated and the URL field is empty, this is expected when the DNS filtering feature is enabled.

See DNS Filtering and Events, on page 13.

Multiple Events are Generated for a Single Transaction

A single web transaction sometimes generates two connection events, one for DNS filtering and one for URL filtering. This is expected when DNS filtering is enabled and:

- the access control rule action for the traffic is Allow or Trust.
- the system encounters a URL for the first time.

See DNS Filtering and Events, on page 13.

History for URL Filtering

Feature	Version	Details
DNS filtering	6.7 (Beta)	A new option in the advanced settings for each access control policy allows earlier filtering of web traffic by category and reputation. Supported Platforms: FMC and managed devices at any supported version.
Ability to specify handling for sites with unknown reputation	6.7	You can now specify handling for URLs with unknown reputation. Modified screens: URL rules in access control policies and QoS policies, and category rules in SSL policies, include a new checkbox for this purpose below the reputation selection area. Supported Platforms: All
New and changed URL categories New names for reputation levels	6.5	The following changes apply to URL rules in access control and QoS policies and to Category rules in SSL policies: The set of URL categories has changed. There are now two "pages" of categories from which to selec when you create a URL rule. The name associated with each reputation level has changed. For descriptions of the new categories and reputation names, see URL Category and Reputation Descriptions, on page 2. For complete details specific to upgrades, see also the Release Notes and upgrade instructions for version 6.5. If there are future category set changes, your rules will display icons to alert you. Modified screens: URL rules in access control policies, SSL policies, and QoS policies; event data related to URL categories. Supported Platforms: FMC and devices running release 6.5.

Feature	Version	Details
Minor change to classic device licensing	6.5	For devices that use classic licenses, URL filtering will not be enabled until the device is registered to the FMC and a URL Filtering license is assigned to the device. Supported Platforms: NGIPSv and ASA with FirePOWER Services devices.
Addresses for retrieving URL data from the Cisco cloud have changed	6.5	See the URL Filtering row in Internet Access Requirements.
Opportunity to dispute an assigned URL Category	6.5	If you disagree with the category that the system assigns to a URL, you can submit a request to change the category. New/Modified screens: • New menu option when right-clicking a URL category or reputation in tables of connection events under the **Analysis** menu. • New button on the URL Lookups page (**Analysis > Advanced > URL**). (Hover your pointer over the URL to display the button.) • New option on the **System > Integration > Cloud Services** page Supported platforms: All
The **Cisco CSI** tab is renamed to **Cloud Services**	6.4	Modified screens and navigation:**System > Integration > Cisco CSI** is now **System > Integration > Cloud Services** Supported platforms: FMC
Moved URL Filtering information from various locations to this new URL Filtering chapter	6.3	Moved information about configuring cloud communications for URL Filtering to the new URL Filtering chapter. Moved certain other URL Filtering information from other locations to this chapter. Made related changes to the structure of the Cisco CSI topics in the chapter.
New option: Cached URLs Expire	6.3	Use this new control to balance performance with freshness of URL category and reputation data in order to minimize instances of URLs matching on stale data. Modified screens: **System > Integration > Cisco CSI**. Supported Platforms: All.
Changed menu path	6.3	The path to the manual URL Lookup page has changed from **Analysis > Lookup > URL** to **Analysis > Advanced > URL**.