Classify URLs for Policy Application

This chapter contains the following sections:

- Overview of Categorizing URL Transactions, on page 1
- Configuring the URL Filtering Engine , on page 4
- Managing Updates to the Set of URL Categories , on page 4
- Filtering Transactions Using URL Categories, on page 9
- Creating and Editing Custom URL Categories, on page 15
- Filtering Adult Content, on page 20
- Redirecting Traffic in the Access Policies, on page 22
- Warning Users and Allowing Them to Continue, on page 23
- Creating Time Based URL Filters, on page 24
- Viewing URL Filtering Activity, on page 25
- Regular Expressions, on page 25
- URL Category Descriptions, on page 29

Overview of Categorizing URL Transactions

Using policy groups, you can create secure policies that control access to web sites containing questionable content. The sites that are blocked, allowed, or decrypted depend on the categories you select when setting up category blocking for each policy group. To control user access based on a URL category, you must enable Cisco Web Usage Controls. This is a multi-layered URL filtering engine that uses domain prefixes and keyword analysis to categorize URLs.

You can use URL categories when performing the following tasks:

Option	Method
Define policy group membership	Matching URLs to URL Categories, on page 3
Control access to HTTP, HTTPS, and FTP requests	Filtering Transactions Using URL Categories, on page 9
Create user defined custom URL categories that specify specific hostnames and IP addresses	Creating and Editing Custom URL Categories, on page 15

Categorization of Failed URL Transactions

The Dynamic Content Analysis engine categorizes URLs when controlling access to websites in Access Policies only. It does not categorize URLs when determining policy group membership or when controlling access to websites using Decryption or Cisco Data Security Policies. This is because the engine works by analyzing the response content from the destination server, so it cannot be used on decisions that must be made at request time before any response is downloaded from the server.

If the web reputation score for an uncategorized URL is within the WBRS ALLOW range, AsyncOS allows the request without performing Dynamic Content Analysis.

After the Dynamic Content Analysis engine categorizes a URL, it stores the category verdict and URL in a temporary cache. This allows future transactions to benefit from the earlier response scan and be categorized at request time instead of at response time.

Enabling the Dynamic Content Analysis engine can impact transaction performance. However, most transactions are categorized using the Cisco Web Usage Controls URL categories database, so the Dynamic Content Analysis engine is usually only called for a small percentage of transactions.

Enabling the Dynamic Content Analysis Engine

Note It is possible for an Access Policy, or an Identity used in an Access Policy, to define policy membership by a predefined URL category and for the Access Policy to perform an action on the same URL category. The URL in the request can be uncategorized when determining Identity and Access Policy group membership, but must be categorized by the Dynamic Content Analysis engine after receiving the server response. Cisco Web Usage Controls ignores the category verdict from the Dynamic Content Analysis engine and the URL retains the "uncategorized" verdict for the remainder of the transaction. Future transactions will still benefit from the new category verdict.

Step 1 Choose **Security Services > Acceptable Use Controls**.

Step 2 Enable the Cisco Web Usage Controls.

Step 3 **Click** to enable the Dynamic Content Analysis engine.

Step 4 Submit and Commit Changes.

Uncategorized URLs

An uncategorized URL is a URL that does not match any pre-defined URL category or *included* custom URL category.

Note When determining policy group membership, a custom URL category is considered included, only when it is selected for policy group membership.

All transactions resulting in unmatched categories are reported on the Reporting > URL Categories page as "Uncategorized URLs." A large number of uncategorized URLs are generated from requests to web sites

within the internal network. Cisco recommends using custom URL categories to group internal URLs and allow all requests to internal web sites. This decreases the number of web transactions reported as "Uncategorized URLs" and instead reports internal transactions as part of "URL Filtering Bypassed" statistics.

Related Topics

- Understanding Unfiltered and Uncategorized Data, on page 25.
- Creating and Editing Custom URL Categories, on page 15.

Matching URLs to URL Categories

When the URL filtering engine matches a URL category to the URL in a client request, it first evaluates the URL against the custom URL categories *included* in the policy group. If the URL in the request does not match an included custom category, the URL filtering engine compares it to the predefined URL categories. If the URL does not match any included custom or predefined URL categories, the request is uncategorized.

Note When determining policy group membership, a custom URL category is considered included only when it is selected for policy group membership.

To see what category a particular web site is assigned to, go to the URL in Reporting Uncategorized and Misclassified URLs, on page 3.

Related Topics

- Uncategorized URLs, on page 2.

Reporting Uncategorized and Misclassified URLs

You can report uncategorized and misclassified URLs to Cisco. Cisco provides a URL submission tool on its website that allows you to submit multiple URLs simultaneously:

- https://securityhub.cisco.com/web/submit_urls
  - To check the status of submitted URLs, click the Status on Submitted URLs tab on this page.
  - You can also use the URL submission tool to look up the assigned URL category for any URL.
- https://www.talosintelligence.com/reputation_center/support
  - To submit a dispute, you must be logged into your Cisco account. Disputes can be filed for URLs, IPs, or domains.
  - Use the Reputation Center Search box to look up web reputation information.

URL Categories Database

The category that a URL falls into is determined by a filtering categories database. The Web Security appliance collects information and maintains a separate database for each URL filtering engine. The filtering categories databases periodically receive updates from the Cisco update server.

The URL categories database includes many different factors and sources of data internal to Cisco and from the Internet. One of the factors occasionally considered, heavily modified from the original, is information from the Open Directory Project.

To see what category a particular web site is assigned to, go to the URL in Reporting Uncategorized and Misclassified URLs, on page 3.

Related Topics

- Manually Updating Security Service Components.

Configuring the URL Filtering Engine

By default, the Cisco Web Usage Controls URL filtering engine is enabled in the System Setup Wizard.

Step 1 Choose **Security Services > Acceptable Use Controls**.

Step 2 Click **Edit Global Settings**.

Step 3 Verify the Enable Acceptable Use Controls property is enabled.

Step 4 Choose whether to enable the Dynamic Content Analysis Engine.

Step 5 Choose the default action the Web Proxy should use when the URL filtering engine is unavailable, either Monitor or Block. Default is Monitor.

Step 6 Submit and Commit Changes.

Managing Updates to the Set of URL Categories

The set of predefined URL categories may occasionally be updated in order to accommodate new web trends and evolving usage patterns. Updates to the URL category set are distinct from the changes that add new URLs and re-map misclassified URLs. Category set updates may change configurations in your existing policies and therefore require action. URL category set updates may occur between product releases; an AsyncOS upgrade is not required.

Information is available from: http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html.

Take the following actions:

When to Act	Method
Before updates occur (Do these tasks as part of your initial setup)	Understanding the Impacts of URL Category Set Updates , on page 5 Controlling Updates to the URL Category Set , on page 7 Default Settings for New and Changed Categories , on page 8 Receiving Alerts About Category and Policy Changes , on page 9
After updates occur	Responding to Alerts about URL Category Set Updates , on page 9

Understanding the Impacts of URL Category Set Updates

URL category set updates can have the following impacts on existing Access Policies, Decryption Policies, and Cisco Data Security policies, and on Identities:

- Effects of URL Category Set Changes on Policy Group Membership , on page 5
- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 5

Effects of URL Category Set Changes on Policy Group Membership

This section applies to all policy types with membership that can be defined by URL category, and to Identities. When policy group membership is defined by URL category, changes to the category set may have the following effects:

- If the sole criterion for membership is a deleted category, the policy or identity is disabled.

If membership in any policy is defined by a URL category that changes, and if this causes ACL list changes, the web proxy will restart.

Effects of URL Category Set Updates on Filtering Actions in Policies

URL category set updates can change policy behavior in the following ways:

Change	Effect on Policies and Identities
A new category can be added	For each policy, the default action for newly-added categories is the action specified for Uncategorized URLs for that policy.
A category can be deleted	The action associated with the deleted category is deleted. If the policy depended exclusively on the deleted category, the policy is disabled. If a policy depends on an identity that depended exclusively on a deleted category, the policy will be disabled.
A category can be renamed	No change to the behavior of the existing policy.
A category can split	A single category can become multiple new categories. Both new categories have the action associated with the original category.

Change	Effect on Policies and Identities
Two or more existing categories can merge	If all original categories in a policy had the same action assigned, the merged category has the same action as the original categories. If all original categories were set to "Use Global Setting" then the merged category is also set to "Use Global Setting." If the policy had different actions assigned to the original categories, the action assigned to the merged category depends on the Uncategorized URLs setting in that policy: • If Uncategorized URLs is set to Block (or "Use Global Setting" when the global setting is Block), then the most restrictive action among the original categories is applied to the merged category. • If Uncategorized URLs is set to any action other than Block (or "Use Global Setting" when the global setting is anything other than Block), then the least restrictive action among the original categories is applied to the merged category. In this case, sites that were previously blocked may now be accessible to users. If policy membership is defined by URL category, and some of the categories involved in the merge, or the Uncategorized URLs action, are not included in the policy membership definition, then the values in the Global Policy are used for the missing items. The order of restrictiveness is as follows (not all actions are available for all policy types): • Block • Drop • Decrypt • Warn • Time-based • Monitor • Pass Through **Note** Time-based policies that are based on merged categories adopt the action associated with any one of the original categories. (In time-based policies, there may be no obviously most- or least-restrictive action.)

Related Topics

• Merged Categories - Examples , on page 7.

Merged Categories - Examples

Some examples of merged categories, based on settings on the URL Filtering page for the policy:

Original Category 1	Original Category 2	Uncategorized URLs	Merged Category
Monitor	Monitor	(Not Applicable)	Monitor
Block	Block	(Not Applicable)	Block
Use Global Settings	Use Global Settings	(Not Applicable)	Use Global Settings
Warn	Block	Monitor Use the least restrictive among the original categories.	Warn
Monitor	• Block or • Use Global Settings,when Global is set to Block	• Block or • Use Global Setting, when Global is set to Block Use the most restrictive among the original categories.	Block
Block	• Monitor or • Use Global Settings, when Global is set to Monitor	• Monitor or • Use Global Setting, when Global is set to Monitor Use the least restrictive among the original categories.	Monitor
For policies in which membership is defined by URL category: Monitor	An action for this category is not specified in this policy, but the value in the Global Policy for this category is Block	An action for Uncategorized URLs is not specified in this policy, but the value in the Global Policy for Uncategorized URLs is Monitor	Monitor

Controlling Updates to the URL Category Set

By default, URL category set updates to occur automatically. These updates may change existing policy configurations, so you may prefer to disable all automatic updates.

Option	Method
If you disable updates, you will need to manually update all services listed in the Update Servers (list) section of the System Administration > Upgrade and Update Settings page	Manually Updating the URL Category Set , on page 8 and Manually Updating Security Service Components
Disabling all automatic updates	Configuring Upgrade and Service Update Settings.

Note If you use the CLI, disable updates by setting the update interval to zero (0)

Manually Updating the URL Category Set

Note

- Do not interrupt an update in progress.
- If you have disabled automatic updates, you can manually update the set of URL categories at your convenience.

Step 1 Choose **Security Services > Acceptable Use Controls**.

Step 2 Determine whether an update is available:

Look at the "Cisco Web Usage Controls - Web Categorization Categories List" item in the Acceptable Use Controls Engine Updates table.

Step 3 To update, click **Update Now**.

Default Settings for New and Changed Categories

URL category set updates may change the behavior of your existing policies. You should specify default settings for certain changes when you configure your policies, so that they are ready when URL category set updates occur. When new categories are added, or existing categories merge into a new category, the default action for these categories for each policy are affected by the Uncategorized URLs setting in that policy.

Verifying Existing Settings and/or Making Changes

Step 1 Choose **Web Security Manager**.

Step 2 For each Access Policy, Decryption Policy, and Cisco Data Security policy click the **URL Filtering** link.

Step 3 Check the selected setting for Uncategorized URLs.

What to do next

Related Topics

- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 5.

Receiving Alerts About Category and Policy Changes

Category set updates trigger two types of alerts:

- Alerts about category changes
- Alerts about policies that have changed or been disabled as a result of category set changes.

Step 1 Choose **System Administration > Alerts**.

Step 2 Click **Add Recipient** and add email address (or multiple email addresses).

Step 3 Decide which **Alert Types** and **Alert Severities** to receive.

Step 4 Submit and Commit Changes.

Responding to Alerts about URL Category Set Updates

When you receive an alert about category set changes, you should do the following:

- Check policies and identities to be sure that they still meet your policy goals after category merges, additions, and deletions, and
- Consider modifying policies and identities to benefit from new categories and the added granularity of split categories.

Related Topics

- Understanding the Impacts of URL Category Set Updates , on page 5

Filtering Transactions Using URL Categories

The URL filtering engine lets you filter transactions in Access, Decryption, and Data Security Policies. When you configure URL categories for policy groups, you can configure actions for custom URL categories, if any are defined, and predefined URL categories.

The URL filtering actions you can configure depends on the type of policy group:

Option	Method
Access Policies	Configuring URL Filters for Access Policy Groups, on page 10
Decryption Policies	Configuring URL Filters for Decryption Policy Groups, on page 12
Cisco Data Security Policies	Configuring URL Filters for Data Security Policy Groups, on page 13

Related Topics

- Redirecting Traffic in the Access Policies, on page 22
- Warning Users and Allowing Them to Continue, on page 23
- Creating and Editing Custom URL Categories, on page 15
- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 5

Configuring URL Filters for Access Policy Groups

You can configure URL filtering for user-defined Access Policy groups and the Global Policy Group.

Step 1 Choose **Web Security Manager > Access Policies**.

Step 2 Click the link in the policies table under the URL Filtering column for the policy group you want to edit.

Step 3 (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:

a) Click **Select Custom Categories**.

b) Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 4 In the Custom URL Category Filtering section, choose an action for each included custom URL category.

Action	Description
Use Global Settings	Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups. Applies to user defined policy groups only. **Note** When a custom URL category is excluded in the global Access Policy, then the default action for included custom URL categories in user defined Access Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Access Policy.
Block	The Web Proxy denies transactions that match this setting.
Redirect	Redirects traffic originally destined for a URL in this category to a location you specify. When you choose this action, the Redirect To field appears. Enter a URL to which to redirect all traffic.
Allow	Always allows client requests for web sites in this category. Allowed requests bypass all further filtering and malware scanning. Only use this setting for trusted web sites. You might want to use this setting for internal sites.
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.

Action	Description
Warn	The Web Proxy initially blocks the request and displays a warning page, but allows the user to continue by clicking a hypertext link in the warning page.
Quota-Based	As a individual user approaches either the volume or time quotas you have specified, a warning is displayed. When a quota is met, a block page is displayed. See Time Ranges and Quotas.
Time-Based	The Web Proxy blocks or monitors the request during the time ranges you specify. See Time Ranges and Quotas.

Step 5 In the Predefined URL Category Filtering section, choose one of the following actions for each category:

- Use Global Settings
- Monitor
- Warn
- Block
- Time-Based
- Quota-Based

Step 6 In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category. This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 7 Submit and Commit Changes.

What to do next

- Exceptions to Blocking for Embedded and Referred Content, on page 11

Exceptions to Blocking for Embedded and Referred Content

A Website may embed or refer to content that is categorized differently than the source page, or that is considered an application. By default, embedded/referred content is blocked or monitored based on the action selected for its assigned category or application, regardless of how the source Website is categorized. For example, a *News* site could contain content, or a link to content, that categorized as *Streaming Video* and identified as being the application YouTube. According to your policy, *Streaming Video* and YouTube are both blocked, while *News* sites are not.

Note Requests for embedded content usually include the address of the site from which the request originated (this is known as the “referer” field in the request’s HTTP header). This header information is used to determine categorization of the referred content.

You can use this feature to define exceptions to the default actions for embedded/referred content; for example, to permit all content embedded in or referred to from *News* Websites, or from a custom category representing your intranet.

Note Referer-based exceptions are supported only in Access policies. To use this feature with HTTPS traffic, before defining exceptions in Access policies, you must configure HTTPS decryption of the URL Categories that you will select for exception. See Configuring URL Filters for Decryption Policy Groups, on page 12 for information about configuring HTTPS decryption. See Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content for additional information about using this feature with HTTPS decryption.

Step 1 On the URL Filtering page for a particular Access Policy (see Configuring URL Filters for Access Policy Groups, on page 10), click **Enable Exceptions** in the Exceptions to Blocking for Embedded/Referred Content section.

Step 2 Click the **Click to select categories** link in the Set Exception for Content Referred by These Categories column, opening the URL filtering category referral-exception selection page.

Step 3 From the Predefined and Custom URL Categories lists, select the categories for which you wish to define this referral exception, then click **Done** to return to the URL Filtering page for this Access Policy.

Step 4 Choose an exception type from the Set Exception for this Referred Content drop-down list:

- **All embedded/referred content** – All content embedded in and referred from sites of the specified category types is not blocked, regardless of the categorization of that content.
- **Selected embedded/referred content** – After choosing this option, select specific Categories and Applications that are not blocked when originating from the specified URL categories.
- **All embedded/referred content except** – After choosing this option, all content embedded in and referred from sites of the specified category types is not blocked, except those URL categories and applications you now specify here. In other words, these types will remain blocked.

Step 5 Submit and Commit Changes.

What to do next

You can elect to display “Permitted by Referrer” transaction data in the tables and charts provided on the following Reporting pages: URL Categories, Users and Web Sites, as well as related charts on the Overview page. See Choosing Which Data to Chart for more information about selecting chart-display options.

Configuring URL Filters for Decryption Policy Groups

You can configure URL filtering for user defined Decryption Policy groups and the global Decryption Policy group.

Step 1 Choose **Web Security Manager > Decryption Policies**.

Step 2 Click the link in the policies table under the URL Filtering column for the policy group you want to edit.

Step 3 (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:

a) Click **Select Custom Categories**.

b) Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL

categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 4 Choose an action for each custom and predefined URL category.

Action	Description
Use Global Setting	Uses the action for this category in the global Decryption Policy group. This is the default action for user defined policy groups. Applies to user defined policy groups only. When a custom URL category is excluded in the global Decryption Policy, then the default action for included custom URL categories in user defined Decryption Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Decryption Policy.
Pass Through	Passes through the connection between the client and the server without inspecting the traffic content.
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.
Decrypt	Allows the connection, but inspects the traffic content. The appliance decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plain text HTTP connection. By decrypting the connection and applying Access Policies, you can scan the traffic for malware.
Drop	Drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.

Note If you want to *block* a particular URL category for HTTPS requests, choose to decrypt that URL category in the Decryption Policy group and then choose to block the same URL category in the Access Policy group.

Step 5 In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category.

This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 6 Submit and Commit Changes.

Configuring URL Filters for Data Security Policy Groups

You can configure URL filtering for user defined Data Security Policy groups and the Global Policy Group.

Step 1 Choose **Web Security Manager > Cisco Data Security**.

Step 2 Click the link in the policies table under the URL Filtering column for the policy group you want to edit.

Step 3 (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:

a) Click **Select Custom Categories**.
b) Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 4 In the Custom URL Category Filtering section, choose an action for each custom URL category.

Action	Description
Use Global Setting	Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups. Applies to user defined policy groups only. When a custom URL category is excluded in the global Cisco Data Security Policy, then the default action for included custom URL categories in user defined Cisco Data Security Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Cisco Data Security Policy.
Allow	Always allows upload requests for web sites in this category. Applies to custom URL categories only. Allowed requests bypass all further data security scanning and the request is evaluated against Access Policies. Only use this setting for trusted web sites. You might want to use this setting for internal sites.
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the upload request against other policy group control settings, such as web reputation filtering.
Block	The Web Proxy denies transactions that match this setting.

Step 5 In the Predefined URL Category Filtering section, choose one of the following actions for each category:

- Use Global Settings
- Monitor
- Block

Step 6 In the Uncategorized URLs section, choose the action to take for upload requests to web sites that do not fall into a predefined or custom URL category. This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 7 Submit and Commit Changes.

What to do next

Related Topics

- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 5.

Creating and Editing Custom URL Categories

You can create custom and external live-feed URL categories that describe specific host names and IP addresses. In addition, you can edit and delete existing URL categories. When you include these custom URL categories in the same Access, Decryption, or Cisco Data Security Policy group and assign different actions to each category, the action of the higher included custom URL category takes precedence.

Note You can use no more than five External Live Feed files in these URL category definitions, and each file should contain no more than 1000 entries. Increasing the number of external feed entries causes performance degradation.

The Web Security appliance uses the first four characters of custom URL category names preceded by "c_" in the access logs. Consider the custom URL category name if you use Sawmill to parse the access logs. If the first four characters of the custom URL category include a space, Sawmill cannot properly parse the access log entry. Instead, only use supported characters in the first four characters. If you want to include the full name of a custom URL category in the access logs, add the %XF format specifier to the access logs.

Before you begin

Go to **Security Services** > **Acceptable Use Controls** to enable Acceptable Use Controls.

Step 1 Choose **Web Security Manager > Custom and External URL Categories**.

Step 2 To create a custom URL category, click **Add Category**. To edit an existing custom URL category, click the name of the URL category.

Step 3 Provide the following information.

Setting	Description
Category Name	Enter an identifier for this URL category. This name appears when you configure URL filtering for policy groups.
List Order	Specify the order of this category in the list of custom URL categories. Enter "1" for the first URL category in the list. The URL filtering engine evaluates a client request against the custom URL categories in the order specified.
Category Type	Choose **Local Custom Category** or **External Live Feed Category**.
Routing Table	Choose **Management** or **Data**. This choice is available only if "split routing" is enabled; that is, it is not available with local custom categories. See Enabling or Changing Network Interfaces for information about enabling split routing.

Setting	Description

Sites / Feed File Location	If you choose **Local Custom Category** for the **Category Type**, provide the custom **Sites**:
	• Enter one or more Site addresses for this custom category. You can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats:
	  • IPv4 address, such as 10.1.1.0
	  • IPv6 address, such as 2001:0db8::
	  • IPv4 CIDR address, such as 10.1.1.0/24
	  • IPv6 CIDR address, such as 2001:0db8::/32
	  • Domain name, such as example.com
	  • Hostname, such as crm.example.com
	  • Partial hostname, such as .example.com; this will also match www.example.com
	  • Regular expressions can be entered in the **Advanced** section, as described below.
	Note It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed is relevant. If you include these categories in the same policy, and define different actions for each, the action defined for the category listed highest in the custom URL categories table will be the one applied.
	• (Optional) Click **Sort URLs** to sort all addresses in the Sites field.
	Note Once you sort the addresses, you cannot retrieve their original order.

Setting	Description
Feed Location (cont.)	If you choose **External Live Feed Category** for the **Category Type**, provide the **Feed File Location** information; that is, locate and download the file containing the addresses for this custom category: **1.** Select either **Cisco Feed Format**, or **Office 365 Feed Format**, or **Office 365 Web Service**, and provide the appropriate feed-file information. • **Cisco Feed Format**: • Choose the transport protocol to be used—either HTTPS or HTTP—and then enter the URL of the live-feed file. This file must be a comma-separated values (.csv)-formatted file. See External Feed-file Formats, on page 19 for more information about this file. • Optionally, provide **Authentication** credentials in the **Advanced** section. Provide a Username and Passphrase to be used for connection to the specified feed server. • **Office 365 Feed Format**: • Enter the **Office 365 Feed Location** (URL) of the live-feed file. This file must be an XML-formatted file; see External Feed-file Formats, on page 19 for more information about this file. • **Office 365 Web Service** Enter the web service URL. It must not contain a ClientRequestId, and have JSON as the format. **2.** For Cisco Feed Format and Office 365 Feed formats, click **Get File** to test the connection to the feed server, and then parse and download the feed file from the server. Progress is displayed in the text box below the **Get File** button. If an error occurs, the problem is indicated and must be rectified before trying again. Refer to Issues Downloading An External Live Feed File for additional information about possible errors. For the Office 365 Web Service, click **Start Test** to initiate the service and download URLs and IPs. **Note** You can use no more than five External Live Feed files in these URL category definitions, and each file should contain no more than 1000 entries. Increasing the number of external feed entries causes performance degradation. **Tip** After you save your changes to this live-feed category, you can click **View** in the **Feed Content** column for this entry on the Custom and External URL Categories page (**Web Security Manager** > **Custom and External URL Categories**) to open a window that displays the addresses contained in the Cisco Feed Format or Office 365 Feed Format feed file you downloaded here.

Setting	Description
Advanced	If you choose **Local Custom Category** for the Category Type, you can enter regular expressions in this section to specify additional sets of addresses. You can use regular expressions to specify multiple addresses that match the patterns you enter. **Note** The URL filtering engine compares URLs with addresses entered in the Sites field first. If the URL of a transaction matches an entry in the Sites field, it is not compared to any expression entered here. See Regular Expressions, on page 25 for more information about using regular expressions.
Auto Update the Feed	Choose a feed update option: • **Do not auto update** • **Every *n* HH:MM**; for example, enter 00:05 for five minutes. However, note that updating frequently can affect WSA performance. **Note** If the available feed file is different than the currently downloaded file, the newer file will be downloaded and the download time updated. Otherwise, the file is not fetched, and a "304 not modified" entry is logged.

Step 4 Submit and Commit Changes.

What to do next

Related Topics

- Regular Expressions, on page 25.
- Customizing Access Logs.
- Problems with Custom and External URL Categories

Address Formats and Feed-file Formats for Custom and External URL Categories

When Creating and Editing Custom and External URL Categories, you must provide one or more network addresses, whether for a **Local Custom Category**, or in an **External Live Feed Category** feed file. In each instance, you can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats:

- IPv4 address, such as 10.1.1.0
- IPv6 address, such as 2001:0db8::
- IPv4 CIDR address, such as 10.1.1.0/24
- IPv6 CIDR address, such as 2001:0db8::/32
- Domain name, such as example.com
- Hostname, such as crm.example.com

- Partial hostname, such as .example.com; this will also match www.example.com
- Regular expressions to specify multiple addresses that match the provided patterns (see Regular Expressions, on page 25 for more information about using regular expressions)

Note It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed is relevant. If you include these categories in the same policy, and define different actions for each, the action defined for the category listed highest in the custom URL categories table will be the one applied.

External Feed-file Formats

If you select **External Live Feed Category** for the **Category Type** when Creating and Editing Custom and External URL Categories, you must select the feed format (**Cisco Feed Format** or **Office 365 Feed Format**) and then provide a URL to the appropriate feed-file server.

The expected format for each feed file is as follows:

- **Cisco Feed Format** – This must be a comma-separated values (.csv) file; that is, a text file with a .csv extension. Each entry in the .csv file must be on a separate line, formatted as address/comma/addresstype (for example: `www.cisco.com,site` or `ad2.*\.com,`regex). Valid addresstypes are `site` and `regex`. Here is an excerpt from a Cisco Feed Format .csv file:

```
www.cisco.com,site

\.xyz,regex

ad2.*\.com,regex

www.trafficholder.com,site

2000:1:1:11:1:1::200,site
```

Note Do not include `http://` or `https://` as part of any `site` entry in the file, or an error will occur. In other words, `www.example.com` is parsed correctly, while `http://www.example.com` produces an error.

- **Office 365 Feed Format** – This is an XML file located on a Microsoft Office 365 server, or a local server to which you saved the file. It is provided by the Office 365 service and cannot be modified. The network addresses in the file are enclosed by XML tags, following this structure: `products` > `product` > `addresslist` > `address`. In the current implementation, an `addresslist` type can be IPv6, IPv4, or URL (which can include domains and regex patterns). Here is a snippet of an Office 365 feed file:

```
<products updated="4/15/2016">

   <product name="o365">

      <addresslist type="IPv6">

         <address>2603:1040:401::d:80</address>

         <address>2603:1040:401::a</address>
```

```
            <address>2603:1040:401::9</address>
         </addresslist>
         <addresslist type="IPv4">
            <address>13.71.145.72</address>
            <address>13.71.148.74</address>
            <address>13.71.145.114</address>
         </addresslist>
         <addresslist type="URL">
            <address>*.aadrm.com</address>
            <address>*.azurerms.com</address>
            <address>*.cloudapp.net2</address>
         </addresslist>
      </product>
      <product name="LYO">
         <addresslist type="URL">
            <address>*.broadcast.skype.com</address>
            <address>*.Lync.com</address>
         </addresslist>
      </product>
   </products>
```

Filtering Adult Content

You can configure the Web Security appliance to filter adult content from some web searches and websites. To enforce safe search and site content ratings, the AVC engine takes advantage of the safe mode feature implemented at a particular website by rewriting URLs and/or web cookies to force the safety mode to be on.

The following features filter adult content:

Option	Description
Enforce safe searches	You can configure the Web Security appliance so that outgoing search requests appear to search engines as safe search requests. This can prevent users from bypassing acceptable use policies using search engines.

Option	Description
Enforce site content ratings	Some content sharing sites allow users to restrict their own access to the adult content on these sites by either enforcing their own safe search feature or blocking access to adult content, or both. This classification feature is commonly called content ratings.

Note Any Access Policy that has either the safe search or site content ratings feature enabled is considered a safe browsing Access Policy.

Enforcing Safe Searches and Site Content Ratings

Note When you enable Safe Search or Site Content Rating, the AVC Engine is tasked with identifying applications for safe browsing. As one of the criteria, the AVC engine will scan the response body to detect a search application. As a result, the appliance will not forward range headers.

Step 1 Choose **Web Security Manager > Access Policies**.

Step 2 Click the link under the URL Filtering column for an Access Policy group or the Global Policy Group.

Step 3 When editing a user-defined Access Policy, choose Define Content Filtering Custom Settings in the Content Filtering section.

Step 4 Click the **Enable Safe Search** check box to enable the safe search feature.

Step 5 Choose whether to block users from search engines that are not currently supported by the Web Security appliance safe search feature.

Step 6 Click the **Enable Site Content Rating** check box to enable the site content ratings feature.

Step 7 Choose whether to block all adult content from the supported content ratings websites or to display the end-user URL filtering warning page.

Note When the URL of one of the supported search engines or supported content ratings websites is included in a custom URL category with the Allow action applied, no search results are blocked and all content is visible.

Step 8 Submit and Commit Changes.

What to do next

Related Topics

- Warning Users and Allowing Them to Continue, on page 23.

Logging Adult Content Access

By default, the access logs include a safe browsing scanning verdict inside the angled brackets of each entry. The safe browsing scanning verdict indicates whether or not either the safe search or site content ratings feature was applied to the transaction. You can also add the safe browsing scanning verdict variable to the access logs or W3C access logs:

- Access logs: %XS
- W3C access logs: x-request-rewrite

Value	Description
ensrch	The original client request was unsafe and the safe search feature was applied.
encrt	The original client request was unsafe and the site content ratings feature was applied.
unsupp	The original client request was to an unsupported search engine.
err	The original client request was unsafe, but neither the safe search nor the site content ratings feature could be applied due to an error.
-	Neither the safe search nor the site content ratings feature was applied to the client request because the features were bypassed (for example, the transaction was allowed in a custom URL category) or the request was made from an unsupported application.

Requests blocked due to either the safe search or site content rating features, use one of the following ACL decision tags in the access logs:

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

Related Topics

- ACL Decision Tags.

Redirecting Traffic in the Access Policies

You can configure the Web Security appliance to redirect traffic originally destined for a URL in a custom URL category to a location you specify. This allows you to redirect traffic at the appliance instead of at the destination server. You can redirect traffic for a custom Access Policy group or the Global Policy Group

Before you begin

To redirect traffic you must define at least one custom URL category.

Step 1 Choose **Web Security Manager > Access Policies**.

Step 2 Click the link under the URL Filtering column for an Access Policy group or the Global Policy Group.

Step 3 In the Custom URL Category Filtering section, click **Select Custom Categories**.

Step 4 In the **Select Custom Categories for this Policy** dialog box, choose **Include in policy** for the custom URL category you want to redirect.

Step 5 Click **Apply**.

Step 6 Click the Redirect column for the custom category you want to redirect.

Step 7 Enter the URL to which you want to redirect traffic in the **Redirect To** field for the custom category.

Step 8 Submit and Commit Changes.

Note Beware of infinite loops when you configure the appliance to redirect traffic.

What to do next

Related Topics

- Creating and Editing Custom URL Categories, on page 15

Logging and Reporting

When you redirect traffic, the access log entry for the originally requested website has an ACL tag that starts with REDIRECT_CUSTOMCAT. Later in the access log (typically the next line) appears the entry for the website to which the user was redirected.

The reports displayed on the Reporting tab display redirected transactions as "Allowed."

Warning Users and Allowing Them to Continue

You can warn users that a site does not meet the organization's acceptable use policies. Users are tracked in the access log by user name if authentication has made a user name available, and tracked by IP address if no user name is available.

You can warn and allow users to continue using one of the following methods:

- Choose the Warn action for a URL category in an Access Policy group or
- Enable the site content ratings feature and warn users that access adult content instead of blocking them.

Configuring Settings for the End-User Filtering Warning Page

Note

- The warn and continue feature only works for HTTP and decrypted HTTPS transactions. It does not work with native FTP transactions.
- When the URL filtering engine warns users for a particular request, it provides a warning page that the Web Proxy sends to the end user. However, not all websites display the warning page to the end user. When this happens, users are blocked from the URL that is assigned the Warn option without being given the chance to continue accessing the site anyway.

Step 1 Choose **Security Services > End-User Notification**.

Step 2 Click **Edit Settings**.

Step 3 Configure the following settings on the **End-User Filtering Warning** page:

Option	Method
Time Between Warning	The Time Between Warning determines how often the Web Proxy displays the end-user URL filtering warning page for each URL category per user. This setting applies to users tracked by username and users tracked by IP address. Specify any value from 30 to 2678400 seconds (one month). Default is 1 hour (3600 seconds).
Custom Message	The custom message is text you enter that appears on every end-user URL filtering warning page. Include some simple HTML tags to format the text.

Step 4 Click Submit.

What to do next

Related Topics

- Filtering Adult Content, on page 20
- Custom Messages on Notification Pages
- Configuring the End-User URL Filtering Warning Page

Creating Time Based URL Filters

You can configure how the Web Security appliance to handles requests for URLs in particular categories differently based on time and day.

Before you begin

Go to the **Web Security Manager > Defined Time Range** page to define at least one time range.

Step 1 Choose **Web Security Manager > Access Policies**.

Step 2 Click the link in the policies table under the URL Filtering column for the policy group you want to edit.

Step 3 Select **Time-Based** for the custom or predefined URL category you want to configure based on time range.

Step 4 In the **In Time Range** field, choose the defined time range to use for the URL category.

Step 5 In the **Action** field, choose the action to enact on transactions in this URL category during the defined time range.

Step 6 In the **Otherwise** field, choose the action to enact on transactions in this URL category *outside* the defined time range.

Step 7 Submit and Commit Changes.

What to do next

Related Topics

- Time Ranges and Quotas

Viewing URL Filtering Activity

The **Reporting > URL Categories** page provides a collective display of URL statistics that includes information about top URL categories matched and top URL categories blocked. This page displays category-specific data for bandwidth savings and web transactions.

Related Topics

- Generate Reports to Monitor End-user Activity

Understanding Unfiltered and Uncategorized Data

When viewing URL statistics on the Reporting > URL Categories page, it is important to understand how to interpret the following data:

Data Type	Description
URL Filtering Bypassed	Represents policy, port, and admin user agent blocking that occurs before URL filtering.
Uncategorized URL	Represents all transactions for which the URL filtering engine is queried, but no category is matched.

URL Category Logging in Access Logs

The access log file records the URL category for each transaction in the scanning verdict information section of each entry.

Related Topics

- Monitor System Activity Through Logs.
- URL Category Descriptions, on page 29.

Regular Expressions

The Web Security appliance uses a regular expression syntax that differs slightly from the regular expression syntax used by other Velocity pattern-matching engine implementations. Further, the appliance does not support using a backward slash to escape a forward slash. If you need to use a forward slash in a regular expression, simply type the forward slash without a backward slash.

Note Technically, AsyncOS for Web uses the Flex regular expression analyzer.

You can use regular expressions in the following locations:

- **Custom URL categories for Access Policies.** When you create a custom URL category to use with Access Policy groups, you can use regular expressions to specify multiple web servers that match the pattern you enter.
- **Custom user agents to block.** When you edit the applications to block for an Access Policy group, you can use regular expressions to enter specific user agents to block.

Note Regular expressions that perform extensive character matching consume resources and can affect system performance. For this reason, regular expressions should be cautiously applied.

Related Topics

- Creating and Editing Custom URL Categories, on page 15

Forming Regular Expressions

Regular expressions are rules that typically use the word "matches" in the expressions. They can be applied to match specific URL destinations or web servers. For example, the following regular expression matches any pattern containing "`blocksite.com`":

```
\.blocksite\.com
```

Consider the following regular expression example:

```
server[0-9]\.example\.com
```

In this example, `server[0-9]` matches `server0`, `server1`, `server2`, ..., `server9` in the domain `example.com`.

In the following example, the regular expression matches files ending in `.exe`, `.zip` and `.bin` in the downloads directory.

```
/downloads/.*\.(exe|zip|bin)
```

Note You must enclose regular expressions that contain blank spaces or non-alphanumeric characters in ASCII quotation marks.

Guidelines for Avoiding Validation Failures

Important: Regular expressions that return more that 63 characters will fail and produce an invalid-entry error. Please be sure to form regular expressions that do not have the potential to return more than 63 characters.

Follow these guidelines to minimize validation failures:

- Use literal expressions rather than wildcards and bracketed expressions whenever possible. A literal expression is essentially just straight text such as "`It's as easy as ABC123`". This is less likely to fail

than using "`It's as easy as [A-C]{3}[1-3]{3}`". The latter expression results in the creation of non-deterministic finite automatons (NFA) entries, which can dramatically increase processing time.

- Avoid the use of an unescaped dot whenever possible. The dot is a special regular-expression character that means match any character except for a newline. If you want to match an actual dot, for example, as in "`url.com`", then escape the dot using the \ character, as in "`url\.com`". Escaped dots are treated as literal entries and therefore do not cause issues.
- Any unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the pattern-matching engine, and an alert to that effect will be sent to you, and you will continue to receive an alert following each update until you correct or replace the pattern.

  Similarly, use more specific matches rather than unescaped dots wherever possible. For example, if you want to match a URL that is followed by a single digit, use "`url[0-9]`" rather than "`url.`".
- Unescaped dots in a larger regular expression can be especially problematic and should be avoided. For example, "`Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created .qual`" may cause a failure. Replacing the dot in "`.qual`" with the literal "`equal`" should resolve the problem.

  Also, an unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the pattern-matching engine. Correct or replace the pattern.
- You cannot use "`.*`" to begin or end a regular expression. You also cannot use "`./`" in a regular expression intended to match a URL, nor can you end such an expression with a dot.
- Combinations of wildcards and bracket expressions can cause problems. Eliminate as many combinations as possible. For example, "`id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\) Gecko/20100101 Firefox/9\.0\.1\$`" may cause a failure, while "`Gecko/20100101 Firefox/9\.0\.1\$`" will not. The latter expression does not include any wildcards or bracketed expressions, and both expressions use only escaped dots.

  When wildcards and bracketed expressions cannot be eliminated, try to reduce the expression's size and complexity. For example, "`[0-9a-z]{64}`" may cause a failure. Changing it to something smaller or less complex, such as "`[0-9]{64}`" or "`[0-9a-z]{40}`" may resolve the problem.

If a failure occurs, try to resolve it by applying the previous rules to the wildcard (such as *, + and .) and bracketed expressions.

Note You can use the CLI option `advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex?` to enable or disable default regex conversion to lower case for case-insensitive matching. Use if you are experiencing issues with case sensitivity. See Web Security Appliance CLI Commands for more information about this option.

Regular Expression Character Table

Meta-character	Description
.	Matches any single character, except the newline character (0x0A). For example, the regular expression r.t matches the strings rat, rut, r t, but not root. Be wary of using unescaped dots in long patterns, and especially in the middle of longer patterns. See Guidelines for Avoiding Validation Failures, on page 26 for more information.
*	Matches zero or more occurrences of the character immediately preceding. For example, the regular expression .* means match any string of characters, and [0-9]* matches any string of digits. Be wary of using this meta-character, especially in conjunction with the dot character. Any pattern containing an unescaped dot that returns more than 63 characters after the dot will be disabled. See Guidelines for Avoiding Validation Failures, on page 26 for more information.
\	The escape character; it means treat the following meta-character as an ordinary character. For example, \^ is used to match the caret character (^) rather than the beginning of a line. Similarly, the expression \. is used to match an actual dot rather than any single character.
^	Matches the beginning of a line. For example, the regular expression ^When in matches the beginning of the string “When in the course of human events” but not the string “What and when in the”.
$	Matches the end of a line or string. For example, b$\. matches any line or string that ends with “b.”
+	Matches one or more occurrences of the character or regular expression immediately preceding. For example, the regular expression 9+ matches 9, 99, and 999.
?	Matches zero or one occurrence of the preceding pattern element. For example, colou?r matches both “colour” and “color” since the “u” is optional.
( )	Treat the expression between the left and right parens as a group, limiting the scope of other meta-characters. For example, (abc)+ matches one or more occurrences of the string “abc”; such as, “abcabcabc” or “abc123” but not “abab” or “ab123”.
|	Logical OR: matches the preceding pattern or the following pattern. For example (him|her) matches the line “it belongs to him” and the line “it belongs to her” but does not match the line “it belongs to them.”

Meta-character	Description
[ ]	Matches any one of the characters between the brackets. For example, the regular expression r[aou]t matches “rat”, “rot”, and “rut”, but not “ret”. Ranges of characters are specified by a beginning character, a hyphen, and an ending character. For example, the pattern [0-9] means match any digit. Multiple ranges can be specified as well. The pattern [A-Za-z] means match any upper- or lower-case letter. To match any character except those in the range (that is, the complementary range), use a caret as the first character after the opening bracket. For example, the expression [^269A-Z] matches any characters except 2, 6, 9, and uppercase letters.
{ }	Specifies the number of times to match the previous pattern. For example: D{1,3} matches one to three occurrences of the letter D Matches a specific number {**n**} or a minimum number {**n**,} of instances of the preceding pattern. For example, the expression A[0-9]{3} matches “A” followed by exactly three digits. That is, it matches “A123” but not “A1234”. The expression [0-9]{4,} matches any sequence of four or more digits.
“...”	Literally interpret any characters enclosed within the quotation marks.

URL Category Descriptions

This section lists the URL categories for Cisco Web Usage Controls. The tables also include the abbreviated URL category names that may appear in the Web Reputation filtering and anti-malware scanning section of an access log file entry.

Note In the access logs, the URL category abbreviations for Cisco Web Usage Controls include the prefix “IW_” before each abbreviation so that the “art” category becomes “IW_art.”

URL Category	Abbreviation	Code	Description	Example URLs
Adult	adlt	1006	Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers); general information about sex, non-pornographic in nature; genital piercing; adult products or greeting cards; information about sex not in the context of health or disease.	www.adultentertainmentexpo.com www.adultnetline.com

URL Category	Abbreviation	Code	Description	Example URLs
Advertisements	adv	1027	Banner and pop-up advertisements that often accompany a web page; other advertising websites that provide advertisement content. Advertising services and sales are classified as "Business and Industry."	www.adforce.com www.doubleclick.com
Alcohol	alc	1077	Alcohol as a pleasurable activity; beer and wine making, cocktail recipes; liquor sellers, wineries, vineyards, breweries, alcohol distributors. Alcohol addiction is classified as "Health and Nutrition." Bars and restaurants are classified as "Dining and Drinking."	www.samueladams.com www.whisky.com
Arts	art	1002	Galleries and exhibitions; artists and art; photography; literature and books; performing arts and theater; musicals; ballet; museums; design; architecture. Cinema and television are classified as "Entertainment."	www.moma.org www.nga.gov
Astrology	astr	1074	Astrology; horoscope; fortune telling; numerology; psychic advice; tarot.	www.astro.com www.astrology.com
Auctions	auct	1088	Online and offline auctions, auction houses, and classified advertisements.	www.craigslist.com www.ebay.com

URL Category	Abbreviation	Code	Description	Example URLs
Business and Industry	busi	1019	Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital; office supplies; industrial equipment (process equipment), machines and mechanical systems; heating equipment, cooling equipment; materials handling equipment; packaging equipment; manufacturing: solids handling, metal fabrication, construction and building; passenger transportation; commerce; industrial design; construction, building materials; shipping and freight (freight services, trucking, freight forwarders, truckload carriers, freight and transportation brokers, expedited services, load and freight matching, track and trace, rail shipping, ocean shipping, road feeder services, moving and storage).	www.freightcenter.com www.staples.com
Chat and Instant Messaging	chat	1040	Web-based instant messaging and chat rooms.	www.icq.com www.meebo.com
Cheating and Plagiarism	plag	1051	Promoting cheating and selling written work, such as term papers, for plagiarism.	www.bestessays.com www.superiorpapers.com
Child Abuse Content	cprn	1064	Worldwide illegal child sexual abuse content.	—
Computer Security	csec	1065	Offering security products and services for corporate and home users.	www.computersecurity.com www.symantec.com
Computers and Internet	comp	1003	Information about computers and software, such as hardware, software, software support; information for software engineers, programming and networking; website design; the web and Internet in general; computer science; computer graphics and clipart. “Freeware and Shareware” is a separate category.	www.xml.com www.w3.org
Dating	date	1055	Dating, online personals, matrimonial agencies.	www.eharmony.com www.match.com

URL Category	Abbreviation	Code	Description	Example URLs
Digital Postcards	card	1082	Enabling sending of digital postcards and e-cards.	www.all-yours.net www.delivr.net
Dining and Drinking	food	1061	Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews.	www.hideawaybrewpub.com www.restaurantrow.com
Dynamic and Residential	dyn	1091	IP addresses of broadband links that usually indicates users attempting to access their home network, for example for a remote session to a home computer.	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
Education	edu	1001	Education-related, such as schools, colleges, universities, teaching materials, and teachers' resources; technical and vocational training; online training; education issues and policies; financial aid; school funding; standards and testing.	www.education.com www.greatschools.org
Entertainment	ent	1093	Details or discussion of films; music and bands; television; celebrities and fan websites; entertainment news; celebrity gossip; entertainment venues. Compare with the "Arts" category.	www.eonline.com www.ew.com
Extreme	extr	1075	Material of a sexually violent or criminal nature; violence and violent behavior; tasteless, often gory photographs, such as autopsy photos; photos of crime scenes, crime and accident victims; excessive obscene material; shock websites.	www.car-accidents.com www.crime-scene-photos.com
Fashion	fash	1076	Clothing and fashion; hair salons; cosmetics; accessories; jewelry; perfume; pictures and text relating to body modification; tattoos and piercing; modeling agencies. Dermatological products are classified as "Health and Nutrition."	www.fashion.net www.findabeautysalon.com
File Transfer Services	fts	1071	File transfer services with the primary purpose of providing download services and hosted file sharing	www.rapidshare.com www.yousendit.com

URL Category	Abbreviation	Code	Description	Example URLs
Filter Avoidance	filt	1025	Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services.	www.bypassschoolfilter.com www.filterbypass.com
Finance	fnnc	1015	Primarily financial in nature, such as accounting practices and accountants, taxation, taxes, banking, insurance, investing, the national economy, personal finance involving insurance of all types, credit cards, retirement and estate planning, loans, mortgages. Stock and shares are classified as "Online Trading."	finance.yahoo.com www.bankofamerica.com
Freeware and Shareware	free	1068	Providing downloads of free and shareware software.	www.freewarehome.com www.shareware.com
Gambling	gamb	1049	Casinos and online gambling; bookmakers and odds; gambling advice; competitive racing in a gambling context; sports booking; sports gambling; services for spread betting on stocks and shares. Websites dealing with gambling addiction are classified as "Health and Nutrition." Government-run lotteries are classified as "Lotteries".	www.888.com www.gambling.com
Games	game	1007	Various card games, board games, word games, and video games; combat games; sports games; downloadable games; game reviews; cheat sheets; computer games and Internet games, such as role-playing games.	www.games.com www.shockwave.com

URL Category	Abbreviation	Code	Description	Example URLs
Government and Law	gov	1011	Government websites; foreign relations; news and information relating to government and elections; information relating to the field of law, such as attorneys, law firms, law publications, legal reference material, courts, dockets, and legal associations; legislation and court decisions; civil rights issues; immigration; patents and copyrights; information relating to law enforcement and correctional systems; crime reporting, law enforcement, and crime statistics; military, such as the armed forces, military bases, military organizations; anti-terrorism.	www.usa.gov www.law.com
Hacking	hack	1050	Discussing ways to bypass the security of websites, software, and computers.	www.hackthissite.org www.gohacking.com
Hate Speech	hate	1016	Websites promoting hatred, intolerance, or discrimination on the basis of social group, color, religion, sexual orientation, disability, class, ethnicity, nationality, age, gender, gender identity; sites promoting racism; sexism; racist theology; hate music; neo-Nazi organizations; supremacism; Holocaust denial.	www.kkk.com www.nazi.org
Health and Nutrition	hlth	1009	Health care; diseases and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in the context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in the context of health (disease and health care); food in general; food and beverage; cooking and recipes; food and nutrition, health, and dieting; cooking, including recipe and culinary websites; alternative medicine.	www.health.com www.webmd.com
Humor	lol	1079	Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as “Adult.”	www.humor.com www.jokes.com

URL Category	Abbreviation	Code	Description	Example URLs
Illegal Activities	ilac	1022	Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.	www.ekran.no www.thedisease.net
Illegal Downloads	ildl	1084	Providing the ability to download software or other materials, serial numbers, key generators, and tools for bypassing software protection in violation of copyright agreements. Torrents are classified as "Peer File Transfer."	www.keygenguru.com www.zcrack.com
Illegal Drugs	drug	1047	Information about recreational drugs, drug paraphernalia, drug purchase and manufacture.	www.cocaine.org www.hightimes.com
Infrastructure and Content Delivery Networks	infr	1018	Content delivery infrastructure and dynamically generated content; websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.	www.akamai.net www.webstat.net
Internet Telephony	voip	1067	Telephonic services using the Internet.	www.evaphone.com www.skype.com
Job Search	job	1004	Career advice; resume writing and interviewing skills; job placement services; job databanks; permanent and temporary employment agencies; employer websites.	www.careerbuilder.com www.monster.com
Lingerie and Swimsuits	ling	1031	Intimate apparel and swimwear, especially when modeled.	www.swimsuits.com www.victoriassecret.com
Lotteries	lotr	1034	Sweepstakes, contests and state-sponsored lotteries.	www.calottery.com www.flalottery.com
Mobile Phones	cell	1070	Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the "Business and Industry" category.	www.cbfsms.com www.zedge.net

URL Category	Abbreviation	Code	Description	Example URLs
Nature	natr	1013	Natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation, forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry); animals, pets, livestock, and zoology; biology; botany.	www.enature.com www.nature.org
News	news	1058	News; headlines; newspapers; television stations; magazines; weather; ski conditions.	www.cnn.com news.bbc.co.uk
Non-Governmental Organizations	ngo	1087	Non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.	www.panda.org www.unions.org
Non-Sexual Nudity	nsn	1060	Nudism and nudity; naturism; nudist camps; artistic nudes.	www.artenuda.com www.naturistsociety.com
Online Communities	comm	1024	Affinity groups; special interest groups; web newsgroups; message boards. Excludes websites classified as “Professional Networking” or “Social Networking.”	www.igda.org www.ieee.org
Online Storage and Backup	osb	1066	Offsite and peer-to-peer storage for backup, sharing, and hosting.	www.adrive.com www.dropbox.com

URL Category	Abbreviation	Code	Description	Example URLs
Online Trading	trad	1028	Online brokerages; websites that enable the user to trade stocks online; information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock splits. Services for spread betting on stocks and shares are classified as "Gambling." Other financial services are classified as "Finance."	www.tdameritrade.com www.scottrade.com
Organizational Email	pem	1085	Websites used to access business email (often via Outlook Web Access).	—
Parked Domains	park	1092	Websites that monetize traffic from the domain using paid listings from an ad network, or are owned by "squatters" hoping to sell the domain name for a profit. These also include fake search websites which return paid ad links.	www.domainzaar.com www.parked.com
Peer File Transfer	p2p	1056	Peer-to-peer file request websites. This does not track the file transfers themselves.	www.bittorrent.com www.limewire.com
Personal Sites	pers	1081	Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme.	www.karymullis.com www.stallman.org
Photo Searches and Images	img	1090	Facilitating the storing and searching for, images, photographs, and clip-art.	www.flickr.com www.photobucket.com
Politics	pol	1083	Websites of politicians; political parties; news and information on politics, elections, democracy, and voting.	www.politics.com www.thisnation.com
Pornography	porn	1054	Sexually explicit text or depictions. Includes explicit anime and cartoons; general explicit depictions; other fetish material; explicit chat rooms; sex simulators; strip poker; adult movies; lewd art; web-based explicit email.	www.redtube.com www.youporn.com
Professional Networking	pnet	1089	Social networking for the purpose of career or professional development. See also "Social Networking."	www.linkedin.com www.europeanpwn.net

URL Category	Abbreviation	Code	Description	Example URLs
Real Estate	rest	1045	Information that would support the search for real estate; office and commercial space; real estate listings, such as rentals, apartments, and homes; house building.	www.realtor.com www.zillow.com
Reference	ref	1017	City and state guides; maps, time; reference sources; dictionaries; libraries.	www.wikipedia.org www.yellowpages.com
Religion	rel	1086	Religious content, information about religions; religious communities.	www.religionfacts.com www.religioustolerance.org
and B2B	saas	1080	Web portals for online business services; online meetings.	www.netsuite.com www.salesforce.com
Safe for Kids	kids	1057	Directed at, and specifically approved for, young children.	kids.discovery.com www.nickjr.com
Science and Technology	sci	1012	Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar subjects; space exploration; meteorology; geography; environment; energy (fossil, nuclear, renewable); communications (telephones, telecommunications).	www.physorg.com www.science.gov
Search Engines and Portals	srch	1020	Search engines and other initial points of access to information on the Internet.	www.bing.com www.google.com
Sex Education	sxed	1052	Factual websites dealing with sex; sexual health; contraception; pregnancy.	www.avert.org www.scarleteen.com
Shopping	shop	1005	Bartering; online purchasing; coupons and free offers; general office supplies; online catalogs; online malls.	www.amazon.com www.shopping.com
Social Networking	snet	1069	Social networking. See also “Professional Networking.”	www.facebook.com www.twitter.com
Social Science	socs	1014	Sciences and history related to society; archaeology; anthropology; cultural studies; history; linguistics; geography; philosophy; psychology; women's studies.	www.archaeology.org www.anthropology.net

URL Category	Abbreviation	Code	Description	Example URLs
Society and Culture	scty	1010	Family and relationships; ethnicity; social organizations; genealogy; seniors; child-care.	www.childcare.gov www.familysearch.org
Software Updates	swup	1053	Websites that host updates for software packages.	www.softwarepatch.com www.versiontracker.com
Sports and Recreation	sprt	1008	All sports, professional and amateur; recreational activities; fishing; fantasy sports; public parks; amusement parks; water parks; theme parks; zoos and aquariums; spas.	www.espn.com www.recreation.gov
Streaming Audio	aud	1073	Real-time streaming audio content including Internet radio and audio feeds.	www.live-radio.net www.shoutcast.com
Streaming Video	vid	1072	Real-time streaming video including Internet television, web casts, and video sharing.	www.hulu.com www.youtube.com
Tobacco	tob	1078	Pro-tobacco websites; tobacco manufacturers; pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as “Health and Nutrition.”	www.bat.com www.tobacco.org
Transportation	trns	1044	Personal transportation; information about cars and motorcycles; shopping for new and used cars and motorcycles; car clubs; boats, airplanes, recreational vehicles (RVs), and other similar items. Note, car and motorcycle racing is classified as “Sports and Recreation.”	www.cars.com www.motorcycles.com
Travel	trvl	1046	Business and personal travel; travel information; travel resources; travel agents; vacation packages; cruises; lodging and accommodation; travel transportation; flight booking; airfares; car rental; vacation homes.	www.expedia.com www.lonelyplanet.com
Unclassified	—	—	Websites which are not in the Cisco database are recorded as unclassified for reporting purposes. This may include mistyped URLs.	—

URL Category	Abbreviation	Code	Description	Example URLs
Weapons	weap	1036	Information relating to the purchase or use of conventional weapons such as gun sellers, gun auctions, gun classified ads, gun accessories, gun shows, and gun training; general information about guns; other weapons and graphic hunting sites may be included. Government military websites are classified as "Government and Law."	www.coldsteel.com www.gunbroker.com
Web Hosting	whst	1037	Website hosting; bandwidth services.	www.bluehost.com www.godaddy.com
Web Page Translation	tran	1063	Translation of web pages between languages.	babelfish.yahoo.com translate.google.com
Web-Based Email	mail	1038	Public web-based email services. Websites enabling individuals to access their company or organization's email service are classified as "Organizational Email."	mail.yahoo.com www.hotmail.com

Related Topics

- Managing Updates to the Set of URL Categories , on page 4
- Reporting Uncategorized and Misclassified URLs, on page 3