Controlling Network Access with Context-Aware Access Policies

The following topics explain how to use context-aware access policies on CX devices to control access to the network.

- Overview of Context-Aware Access Policies, page 1
- Configuring Context-Aware Access Policies, page 2
- Notifying Users of Blocking Policies, page 11
- URL and Application Filtering, page 17
- Web Reputation Filtering (Malware Protection), page 39
- Next Generation IPS Filtering, page 42
- Configuring Signature and Engine Updates, page 44

Overview of Context-Aware Access Policies

The context-aware access policy is the primary policy for implementing acceptable use policies through a CX device. Use context-aware access policies to supply the following services:

- Traditional access control based on the source and destination IP addresses, protocols, and ports for a traffic flow.
- Identity-based access control to allow or deny access based on the user requesting the access, regardless of which IP address the user is currently using. You can enforce identity-based access control by specifying user groups rather than individual users, so that a user is provided access based on group membership.
- Application-based access control to allow or deny specific applications or general types of application. Because some undesirable applications can change port usage, using traditional service definitions of protocol and port is not always effective. Through inspection, the application used in a traffic flow can frequently be determined. Thus, you can write policies based on application names such as Facebook or LinkedIn, making your policies easier to understand and evaluate.

Some applications have multiple behaviors that you can selectively allow or deny. For example, you could allow Facebook but deny posting to Facebook.
• Client-based access control to allow selective access based on the HTTP user agent being used to initiate a traffic flow (for example, web browsers) or for remote access VPN users, the operating system of their client.

• URL filtering to prevent access to undesirable web sites. You can control access to specific URLs or to entire web site categories, such as Gambling web sites.

• Warning policies to notify users that access to certain sites is against policy, without overtly denying access to those sites. Users can click a link to continue to the site. (Works with HTTP and decrypted HTTPS only; all other traffic is simply allowed.)

• Web reputation filtering to prevent access to web sites that have low public reputation scores. By filtering on reputation, you can allow access to an otherwise high-reputation web site while preventing advertisements or other material on the site hosted from external low-reputation sites. Thus, users might see pages with empty boxes where the low-reputation information would have appeared.

• File transport control to selectively deny the uploading or downloading of files based on MIME type. For example, if you have a high-security zone in your network, you might want to prohibit all file uploads from that zone.

• Next Generation IPS filtering to compare the traffic contents against attack threats. If a connection matches a threat, you can drop the connection to block the threat. You can also choose to monitor but allow, or completely ignore, threats that you decide are benign.

• Rate limiting (also called policing) to ensure that no traffic exceeds the maximum rate that you configure, thus ensuring that bandwidth-intensive traffic flows cannot take over all resources.

• Safe Search enforcement to prevent users from relaxing search engine controls to include inappropriate or explicit results for searches.

Default Context-Aware Access Policy Behavior

If a traffic flow does not match any of your access policies, an implicit action is applied to the flow. All non-matching traffic flows are allowed without condition by default. This default policy is named Implicit Allow when it appears in dashboards or events.

Note

The default context-aware access policy behavior is the exact opposite of traditional firewall access policies. For example, the ASA denies any traffic flows that do not match an allow rule in the global or interface-specific access policies.

It is best practice to create an explicit rule that defines the action to apply to non-matching traffic flows. Place the policy last in the access policy set. If desired, you can apply the Deny action instead of the Allow action. For traffic matching conditions, use the default Any for source, destination, and application.

Configuring Context-Aware Access Policies

Use context-aware access policies to control access to network resources. You can control access based on:

• Traditional 5-tuple characteristics such as source and destination IP addresses, protocol, and ports.

• The user who is making the request, or the user groups in which the user is a member.
• The application that is being used. You can also control access for generalized application types.

• The HTTP client type being used to make a request (such as the browser type), or the operating system of a VPN client.

• The destination URL of a web request, including the generalized category of the URL.

When you create an access policy that allows network access, you can limit the allowed activity by applying Next Generation IPS filtering, by selectively prohibiting the uploading or downloading of certain types of files, or by disallowing access to web sites that have poor public reputations.

**Procedure**

**Step 1** Select Configurations > Policies/Settings and open the Access Policies tab.

(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

**Tip** In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Click Context-Aware Policies to ensure that you are working in the CX access policy section.

**Step 2** Do any of the following:

- To add a new policy, use one of the Add Policy buttons. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.

- To edit an existing policy, select the policy and click the Edit Policy button.

- To base a new policy on a similar existing policy, select the policy and click the Duplicate Policy button.

A form opens with the policy properties.

**Step 3** Select the policy action to apply to matching traffic.

- Allow—Allow the traffic subject to the profile and application behavior settings in the policy.

- Warn—For HTTP and decrypted HTTPS connections, display a warning notification to advise the user that access to the site is not recommended. The user can click a link to continue with the connection. Thus, the connection is initially denied, but potentially allowed. Any non-HTTP/decrypted HTTPS traffic is simply allowed.

- Deny—Drop the traffic unconditionally.

**Step 4** Define the traffic matching criteria using the Source, Destination, and Application fields.

You can leave any field blank to not restrict traffic based on that criteria. See the reference topic for detailed information about each field, but consider the following tips:

- If you need to create very complex source or destination criteria, use the source and destination object groups. These objects allow complex combinations of other objects to precisely define traffic flows.

- To implement URL filtering, use URL objects in the destination criteria. You can use URL categories to control access to all web sites that provide a particular type of service. For example, you could disallow all gambling web sites by using the Gambling category without needing to know the URLs for every gambling site. You could also set up a URL object to disallow a category, but exclude specific web sites within the category that you do want to allow.

- To implement application control, specify criteria in the Application field. You can control entire application types (which apply the same policies to all specific applications that are of that type), or you
can control specific applications, including application services that you define yourself. When you specify applications or types, you can control access without limiting the control to specific ports.

Note Some applications, such as Facebook and LinkedIn, allow granular control of specific application behaviors. These behaviors appear when you select an item that includes applications with controllable behaviors.

Step 5 (Optional) Unless the policy action is Deny, you can also configure the following profiles to selectively disallow actions:

- **Bandwidth Limit**—The maximum bandwidth to allow each traffic flow that matches this policy, from 1 Kbps to 4000 Mbps. You can specify the limit in Mbps or Kbps, select the appropriate measure.

- **Safe Search: On/Off**—Whether to enforce Safe Search for search engine or other supported content search requests. By enforcing Safe Search, you prevent users from relaxing search engine settings, ensuring that you filter out inappropriate or explicit content from search results. The default is Off, which allows users to configure the search engine as desired.

- **File filtering**—You can select a profile object that defines file MIME types that should not be downloaded or uploaded.

- **Web reputation**—You can select a profile object that defines the public reputation score range that should be blocked. Use this to protect against malware. To use the device level profile, select Device Level Profile (name); the name of the profile configured is shown in the option. The pre-defined system object Default web reputation profile implements the recommended blocking of sites with reputation scores from -10 to -6.

- **NG IPS**—You can select a profile object that defines the Next Generation IPS filtering policy to apply. If you do not select a profile, no filtering is applied. To use the device level profile, select Device Level Profile (name); the name of the profile configured is shown in the option. The pre-defined system object Default NG IPS profile implements the recommended policy.

Tip You can see whether intrusion prevention (Next Generation IPS filtering) and malware protection (web reputation) are on or off for the device by looking at the status information above the access policy list. Mouse over the On/Off indication to see details about the device-level profile for each feature. There is an Edit Settings link in the popup to open the settings tab for the feature, where you can change the status and profile.

Step 6 If you want to limit the policy to traffic on specific interfaces on the parent device, select the Source Interface Role or the Destination Interface Role, or both, that identify the interfaces. The default is to apply the policy to traffic between any interfaces on the device. If you select interfaces that do not exist on the device, the policy is never applied to traffic.

Step 7 Click Save Policy.

Step 8 If necessary, move the policy so that it is in priority order. Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.
What to Do Next

Analyze the activity of the policy. When viewing the policies list, each policy includes hit count information, which is linked to the detailed Policy Hits dashboard for the policy. You can also access the Policy Hits dashboards directly by selecting Dashboard > Policies.

Context-Aware Access Policy Properties

Use context-aware access policies on CX devices to control access to the network.

Access policies have the following properties:

Policy Name

The name of the policy. This name appears in dashboards and Event Viewer for data and events generated by traffic that matches this policy, so choose a name that will help you analyze dashboard and event data.

Enable Policy: On/Off

Whether the policy is enabled. You can turn a policy off to temporarily disable it without deleting the policy. Disabled policies are never applied to traffic.

Policy Action

One of the following:

- **Allow**—Allow the traffic subject to the profile and application behavior settings in the policy.
- **Warn**—For HTTP and decrypted HTTPS connections, display a warning notification to advise the user that access to the site is not recommended. The user can click a link to continue with the connection. Thus, the connection is initially denied, but potentially allowed. Any non-HTTP/decrypted HTTPS traffic is simply allowed.
- **Deny**—Drop the traffic unconditionally.

Eventing: On/Off

Whether traffic flows that match the policy will generate events and dashboard data. The default is On. If you turn off eventing, traffic that matches this policy will not be reflected in dashboards, and you will not see events for the flows in Event Viewer.

Capture Packets: On/Off

Whether to capture packets for flows that match this policy, if, and only if, the match criteria for the policy are limited to Layer 3/Layer 4 (L3/L4) criteria (network objects, service objects) or they use the default Any. The packet capture default is Off. All packets are captured, so carefully consider traffic volumes for matching flows before enabling packet capture.

Packets are not captured for policies that use any criteria other than L3/L4 criteria, even if you enable packet capture.

The packet capture file is not written to disk until you turn off packet capture. To upload packet captures to a server, log into the system CLI and use the **support diagnostic** command.

For more detailed information on how to capture packets, see Capturing Packets.
Traffic Matching Criteria

You can create complex traffic matching criteria to define precise policies. To match the access policy, the flow must match every specified property, that is, there is an AND relationship between the properties. Use the default Any selection if you do not want to restrict the policy based on that condition. Leave all fields with the default Any to match every possible traffic flow.

The **Source**, **Destination**, and **Application/Service** criteria are used to determine the traffic to which a policy applies. For information on how to select items, including how to add, edit, or remove them, filter the selection list, create or edit objects, or view object contents, see Selecting Items.

Source

A list of policy objects of the following types: network group (IP addresses), identity (user or user group names), user agent (the type of client application that is making a web request), Secure Mobility (type of remote access VPN client), or source object group (a collection of objects in complex AND/OR relationships that you cannot define directly in a policy). If a packet matches any selected object, it is considered to satisfy the source condition.

Note

(Multiple Device mode.) When using PRSM in Multiple Device mode, you can also use network objects or groups defined on the device that contains the CX device for source or destination criteria, or ASA service objects for the service criteria. The network group objects come in two types: one that can be used on both ASA and CX devices, and one that can be used on CX devices only, which is explicitly called CX network group.

Destination

A list of policy objects of the following types: network group, URL (URLs or web categories), or destination object group (a collection of objects in complex AND/OR relationships that you cannot define directly in a policy). If a packet matches any selected object, it is considered to satisfy the destination condition.

If you disable the URL filtering feature, or you do not have a valid Web Security Essentials license, you cannot use URL objects in this field or in a destination object group.

Tip

When configuring URL objects for access policies, be aware that paths cannot be matched for encrypted traffic (where a decryption policy did not decrypt the flow) or for any decrypted flow that is not HTTPS; in these cases, the access policy matches URLs that specify a domain name only.
Application/Service

A list of applications, application types, application objects, service groups (protocol and port combinations), or application service objects (which define an application based on a combination of service and application specifications). Because traffic is inspected, the application for a traffic flow can often be determined regardless of the port used by the flow; you can create rules directed to a specific application or application type by name rather than trying to predict the ports used. If a packet matches any selected application specification, it is considered to satisfy the application condition.

Tip

If you disable the Application Services feature, or you do not have a valid Application Visibility and Control license, this field is named Services and you are limited to using service objects and groups.

Some applications have multiple application behaviors. For example, Facebook includes behaviors such as Post and Tag, categorized by Facebook areas or features, such as Events, General, Messages, Notes, Photos, and Places. If you specify an application type that has multiple behaviors in an access policy whose action is not Deny, you have granular control over these behaviors, so that you can in general allow the application type, but deny specific behaviors. For example, you could allow Facebook posting, but not allow the upload of photos or message attachments.

If you select applications that include multiple behaviors, the Set Application Behaviors control appears beneath the Application box. Each behavior is listed separately. You can do the following to control the specific behaviors:

• To change the settings for all behaviors at once, select Allow All or Deny All for Set Global Behavior To. These options provide a shortcut for changing the Allow/Deny setting throughout the behaviors list. For example, if your intention is to deny most behaviors, but allow a few, you can select Deny All initially, then change the desired behaviors to Allow. The default is to allow all application behaviors.

• To change the setting for an individual behavior, click the Allow/Deny field to show the desired option. The Allow/Deny field appears only if you change the overall policy action to Allow.

Shared/Local

(Multiple Device mode only.) The devices on which to configure this policy. If you leave this field blank, the policy is configured on all devices that share the policy set that contains the policy. If you want to limit this policy to a subset of the devices that share the policy set, select those devices here; the policy will not be configured on any unlisted devices that otherwise share the policy set. The devices available for selection are constrained to those that currently share the policy set.

For example, you can use this setting to create a handful of policies specific to a device that otherwise should use the same policies as a group of devices.
Profile

Unless you select Deny for Policy Action, you can optionally select profile options to implement acceptable use policies. Using profiles, you can drop certain types of traffic that is otherwise allowed:

- **Bandwidth Limit**—The maximum bandwidth to allow traffic that matches this policy, from 1 Kbps to 4000 Mbps. You can specify the limit in **Mbps** or **Kbps**, select the appropriate measure.

- **Safe Search: On/Off**—Whether to enforce Safe Search for search engine or other supported content search requests. By enforcing Safe Search, you prevent users from relaxing search engine settings, ensuring that you filter out inappropriate or explicit content from search results. The default is **Off**, which allows users to configure the search engine as desired.

- **File Filtering**—A profile object that determines which types of files users can upload or download.

- **Web Reputation**—A profile object that determines which traffic is dropped based on the web reputation of the traffic. If you do not select a profile, no filtering is applied. To use the device level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. The pre-defined system object **Default web reputation profile** implements the recommended blocking of sites with reputation scores from -10 to -6.

- **NG IPS**—A profile object that defines the Next Generation IPS filtering policy to apply. If you do not select a profile, no filtering is applied. To use the device level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. The pre-defined system object **Default NG IPS profile** implements the recommended policy.

Interface Roles

The criteria that identifies the parent device’s interfaces to which the policy applies. To match the policy, the traffic must enter the device on one of the source interfaces and leave the device on one of the destination interfaces. The default is any interface for both source and destination, meaning the policy is not restricted to specific interfaces.

To limit the policy to specific interfaces, select the appropriate interface role objects in either the **Source Interface Role** or **Destination Interface Role** fields, or both. The interface role objects define the interface names or naming patterns for the interfaces.

**Tip**

If you specify interface roles, and no interfaces on the device match the interface names defined in the role, the policy will never apply to any traffic on the device.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.
Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

Warning Users of Undesirable Sites

You can use Warning access policies to notify users when they try to access sites that you deem undesirable. For HTTP, or decrypted HTTPS, connections that match a warning policy, the connection is initially denied, and the Warning end-user notification page is shown. After reading your message, the user can elect to click a link that will continue to the site. Thus, Warning policies initially result in a deny action, but can be coupled with an allow action. In Event Viewer, the deny reason indicates that a user acceptance to a warning is pending in these cases. An HTTP Complete message with Yes in the User Accepted Warning field indicates that the user continued to the site.

Because the user must be shown an HTML warning page, warning policies make sense for browser-hosted HTTP/HTTPS traffic only. Thus, a warning policy should use a URL object in the destination. It would make no sense, for example, to apply the Warn action to a rule for GRE traffic. Specifically:

- HTTP/HTTPS traffic that cannot be shown a warning is dropped. That is, traffic for web-based applications that are not hosted in a browser will typically be dropped. Thus, Warning policies are not good choices for application filtering.
- All non-HTTP or non-decrypted HTTPS traffic that matches a Warning policy is simply allowed.

You can modify the Warning end-user notification page to explain your organization's acceptable use policies.

Limitations for Warning Policies

If a user clicks the link to continue to a site, the system tracks the acceptance based on the user’s IP address and the warning policy, but not the destination. Subsequent traffic from that IP address that matches the policy will be allowed without warning until the acceptance times out after 8 hours. This method of tracking has the following implications when the user accepts the warning:

- If you use NAT to map multiple addresses to a single IP address, the first user who accepts a warning will accept it for all users. Subsequent users who try to access a site you are warning against will not see the warning.
- If you use web categories in the warning policy, the user accepts the warning for all sites in that category. Thus, if the user goes to Gambling Site A and accepts the warning, the user will not see a warning for Gambling Site B.
- If you specify more than one web category in the warning policy, the user accepts the warning for all categories at once. Thus, if you create a warning policy for Gambling and Games, if the user goes to Gambling Site A and accepts the warning, the user will not see a warning for Gaming Site B.

Recommendations for Warning Policies

There is a single Warning end-user notification page that you can customize. You can use this page to list all web categories and applications that you are warning against.
When configuring the warning policies, you have two main strategies that you can employ:

1. Create a single policy that includes all border-line sites. This is the simplest method, but if you specify more than a single site or category, if the user accepts the warning for one, the user accepts it for all. The user might not be warned for every border-line access attempt.

2. Create a separate warning policy for each site or category. Depending on how many sites and categories fall in your border-line area, this can bloat your policy list. However, it will increase the chances that the user will be warned for every questionable access attempt. You will also be able to track the volume of access attempts for each category based on policy hit counts.

**Applying Rate Limits (Policing)**

Rate limiting, also called policing, is a way of ensuring that no traffic exceeds the maximum rate (in bits/second) that you configure, thus ensuring that bandwidth-intensive applications cannot take over all resources. When traffic exceeds the maximum rate, CX drops the excess traffic.

To apply a rate limit, you enter a value in the **Bandwidth Limit** field, under **Profile**, in a CX Context-Aware access policy. You can specify the limit in **Mbps** or **Kbps**; ensure that you select the right measure.

For example, you could create access policies to apply a 50 Kbps rate limit for any of the following:

- In **Application/Service**, select the File Sharing, iTunes, and Social Networking application types.
- In **Destination**, select a URL object that specifies high bandwidth categories, such as Entertainment, Games, Streaming Audio, and Streaming Video.
- In **Source**, select an identity object that specifies user groups whose access should be constrained.

All concurrent traffic flows that match the policy will have the limit applied collectively. The limit does not affect flows that match other access policies. Events for matching flows will indicate that a limit was applied.

Be aware that you can also configure policing rate limits and other Quality of Service (QoS) settings on the ASA. If you apply rate limits in both devices, the actual maximum limit might be lower than the limit you configure in the access policy. Additionally, the ASA rate limit might apply to traffic that you are not trying to limit in CX.

**Enforcing Safe Search**

Many search engines and other content-heavy web sites, such as Google and Yahoo, provide a feature called **Safe Search**. With Safe Search, you can configure the site to filter out inappropriate or explicit results from a search request. Each site uses different terminology for this search option, such as Google’s "Filter Explicit Results" or Yahoo’s "Filter out adult Web, video, and image search results."

Because Safe Search is optional, a user can turn it off and get unfiltered results. This might be undesirable in your organization, especially when the search results contain images that could easily be seen by other people. Thus, you might want to use your CX Context-Aware access policies to enforce Safe Search.

To enforce Safe Search, you simply select **Safe Search: On** in the Profile section of a CX Context-Aware access policy. Use the Source and Destination fields to tailor the policy to the users and networks that need Safe Search enforcement.

When enforcing Safe Search, CX implements strict blocking, not moderate blocking. The HTTP inspector will modify search URLs to include the required string, or modify the HTTP header, based on the
implementation used by the targeted search engine. If CX does not support a particular search engine, all user access to that engine will be denied for traffic flows that match a Safe Search-enabled policy.

Keep the following tips in mind when enforcing Safe Search:

- If CX must rewrite the user’s search URL, the Safe Search column in traffic events will say Yes.
- If CX does not support a search engine, users will see a notification that the site is blocked, and you will see an HTTP Deny event.
- Safe search enforcement will apply to an HTTPS site only if you have a decryption policy that decrypts the traffic. If the traffic is not decrypted, the search URL cannot be rewritten.

Notifying Users of Blocking Policies

When you create access policies that deny traffic flows, end users are blocked from the destination. You might want to make public your general policies, especially if you implement URL filtering or selective blocking of applications or application behaviors. For example, if users know beforehand that you are blocking access to all gambling web sites, or to Facebook, they will not try to access those sites and will not be surprised if they are blocked if they do try.

The following topics explain end user notification and how to configure your own notification pages.

When Are Notifications Sent?

In many situations, the CX device will show an end user notification page when blocking web destinations in the user’s browser. This notification indicates that your organization’s policies block access to the resource. Showing an end user notification page is not always possible. Users should typically see the notification if they are trying to open a standard URL to a web destination, and you are broadly applying blocking to the web site. However, notification is not always possible. The following list explains some of the situations in which users will be blocked from a resource without getting a notification:

- Notifications are never sent for non-web traffic, that is, users might see notifications only if they are accessing an HTTP or HTTPS resource.
- Notifications are never sent if the destination is denied because the transaction matches a Next Generation IPS threat that you are blocking.
- If you deny access based on IP address, user name, or user group membership, no notifications are sent.
- For warning policies, notifications are shown regardless of what elements the traffic matches, including IP address, username, user group membership, URLs, applications, and so forth. HTTP/HTTPS traffic for which notifications cannot be displayed is blocked, but non-HTTP/HTTPS traffic is simply allowed.
- If you deny access to a site that is a Web 2.0-style application, where the site gives the appearance of a self-contained application rather than a standard web page, it is very likely that users will not see notifications. This occurs because the web site is using Javascript to control the user experience, and instead of loading new pages, often uses AJAX calls to update content without changing the URL. The device can recognize requests for application behaviors that you have denied, but cannot insert a user notification into the site’s Javascript.
Some policies result in "late" verdicts on whether the flow will be allowed or denied. To ensure good network performance, the device might send some of a traffic flow to the destination before determining that the flow should be denied. This can happen when you have policies that block file uploads or downloads, or that block flows based on application specifications. If the flow is eventually denied after an initial response from the destination has been received, the flow is dropped mid-stream and no notification is possible.

The order of your access policies matter. If a traffic flow matches a deny policy that is low in the access policy set, and policies higher in the policy set require additional analysis to determine if a flow matches (for example, policies that specify application criteria), the deny verdict might come late, after part of the flow has already been sent and an initial response received. Because policy sets are analyzed on a first match basis, you should always put more specific policies above more general policies. You should also put simpler policies, such as URL filtering, above more complex application filtering policies.

**End User Notifications Page**

Use the end user notification feature to customize the pages shown to users when you deny, or warn against, access to a site. You can create different notifications for the different types of reasons you might be blocking access. The following image and text explains the basics of using this page.

**Figure 1: End User Notification Page**

The following points explain the image call-outs.
(1) Notification Type

You can configure different notifications based on the reason for denying access to a resource. If more than one deny reason applies to a traffic flow, the notification used is based on the following priority. (The Warning notification is always shown for warning policies.)

- Web reputation—The traffic violated the allowed reputation range defined in the web reputation profile attached to policy.
- File type—A file in the traffic flow was not allowed based on the file filtering profile attached to the access policy.
- URL filtering—The destination web site was not allowed. This might happen based on URL or based on the web category of the site.
- Application—The traffic flow was for an application or application behavior that is not allowed.
- Destination—The traffic flow was for a site that is not allowed for some other reason. This might include denying site access based on source criteria, such as user identity, user group membership, and so forth. This message is shown if no other message fits the deny reason.
- Warning—The traffic matched a policy with the Warn action. The notification page will include a link that allows the user to continue to the undesirable site.

(2) Import

Click this button to import your own HTML file for the selected notification type.

(3) Preview Draft

Click this button to see how the message you are editing will appear to users. Sample values are used for variables.

(4) Restore Default

Click this button to return the message you are editing to the system default. You are shown the default message and asked to confirm your decision; click Restore to complete the action.

(5) Background Color

The hexadecimal number that represents the background color for the notification panel. Click in the box to open a color palette and click the color you want, or edit the number directly if you know the desired value. If you edit the number, click outside the box to complete your change.

(6) Left Pane of Message

From top to bottom, the left pane of the end user notification message contains the following items:

- Logo image—Click Upload Logo to add your own organization’s logo. The page explains the image limits. You can click Remove Logo if you do not want a graphic.
- Action image—An image that indicates action you are taking. Click Upload Graphic to add your own image, or click Remove Graphic if you do not want one.
- Message headline—A text message that indicates the action you are taking.
(7) Right Pane of Message

The detailed part of the message. Editing controls across the top let you manipulate the message. The controls and elements of the pane are:

- **Undo, Redo buttons**—You can cycle through your changes to undo and redo them when necessary.
- **B, I, U**—Bold, italicize, or underline text.
- **Right, left, center, or justify text alignment.**
- **Chain link**—Enter a hyperlinked URL. You are prompted for the URL and the text for the link. Click **Set** to add the link at the cursor position.
- **Insert variable**—Insert a system variable at the cursor position. The value assigned to the variable for the denied traffic flow will be presented to the end user. Variables are enclosed in double braces, `{variable_name}`).
- **Message body**—Type in the message body box. Use the Tab/Reverse Tab key to add or remove indents.

### Customizing End User Notifications

You can change the notifications shown to end users when they are denied access to a web page, or warned against accessing the site. You can customize the pages by editing the pre-defined notifications, or you can import your own HTML to use as the notification page.

The following topics explain how to change the notification pages.

### Editing End User Notifications

You can edit the pages shown to users when you deny, or warn against, access to a site. There are different pages for each denial reason.

#### Procedure

**Step 1** Select **Administration > End User Notification**.
For detailed information about this page, including the available notification types, see **End User Notifications Page** on page 12.

**Step 2** Select the type of notification you want to edit from the **Notification Type** list.

**Step 3** Make your edits.
Following are some tips for editing the notification messages:

- The toolbar above the right pane lets you manipulate some characteristics of the text. You can also use the Tab/Reverse Tab key to manage text indentation.
- You can upload your own images for the logo and action image shown on the notification. The web interface explains the size and file type limitations for the images.
- Use the hypertext link button to build links to your internal help or acceptable use policy pages.
**Importing End User Notifications**

Instead of editing the pre-defined notification pages, you can create your own page and import it into the application. By importing pages, you can create more complex pages than possible using the editor.

You cannot edit the imported file. If you need to make changes, edit your original file and import it again.

**Before You Begin**

Create a separate HTML page for each notification type you intend to replace. Although you can import plain text, the application expects HTML, and you probably will not get good results unless you insert the desired markup tags.

Following are some tips about how to configure the HTML file for a notification page:

- The file should include complete, valid HTML markup, including the <html> container tag. We suggest that you use an HTML editor to generate the appropriate markup. Test the file in a browser before importing it to ensure that you get the desired presentation.

- Insert whatever CSS styles you require directly into the HTML file.

- Although you can use an <img> tag to refer to an image that resides on a web server, it is possible your policies will prevent access to the server for some users. If you want to include images, and ensure that the image is always available for all users, you can generate the base64 encoding for the image and insert it in the following markup. This example assumes a PNG graphic, but you can use JPEG or other graphic types supported by browsers if you adjust the image media type declaration.

```html
<div
   class="class_name"
   style="background-image: url(data:image/png;base64,insert-string-here)"
>
</div>
```

**Procedure**

**Step 1** Select **Administration > End User Notification**.

For detailed information about this page, including the available notification types, see **End User Notifications Page**, on page 12.
Step 2  Select the type of notification you want to import from the Notification Type list.
Step 3  Click Import.
Step 4  In the Import EUN File popup, click Browse and select your HTML file.
Step 5  Click Upload.

If the file includes acceptable content, it is uploaded and shown, and the message “Upload Successful” appears at the bottom of the page. You can click Preview Draft to verify it will appear to end users as expected.

If the results are not acceptable, click Do Not Use Imported Version to return to the pre-defined page.

If the file cannot be uploaded, you should see an error message at the bottom of the page. Following are some common problems:

• **File not composed of valid text**—The file contents are not recognized as HTML. For example, you might have selected an RTF file. Ensure that you save the file as HTML before trying to import it.

• **Error: Invalid variable name** {{var_name}}—The var_name is not a recognized variable name. Any text that appears between two sets of braces must be a recognized variable. The message mentions the first wrong variable name encountered, but there might be more than one incorrect variable in the file. Correct all variable names and try again.

### End User Notification Variables

Any text within double braces, such as {{variable_name}}, is considered a system variable. Variables are replaced with values from the flow when the end user notification message is presented to the user. Use variables to help users understand the reasons for the action you are taking and to aid your help desk staff if users ask for an explanation.

The available variables differ based on the notification type. Many variables are available for all types of messages whereas others are limited to one type, as explained in the following table.

If the variable name does not match a name listed in the following table, users will see an empty space in place of your variable name.

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Example</th>
<th>Description</th>
<th>Notification Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>application_behavior</td>
<td>Tweet</td>
<td>The application behavior, which is not available for all applications.</td>
<td>Application</td>
</tr>
<tr>
<td>application_name</td>
<td>Twitter</td>
<td>The name of the application.</td>
<td>Application</td>
</tr>
<tr>
<td>application_type</td>
<td>Social Networking</td>
<td>The general type of application.</td>
<td>Application</td>
</tr>
<tr>
<td>blocking_reason</td>
<td>Application</td>
<td>The reason access was blocked.</td>
<td>All</td>
</tr>
<tr>
<td>continue_url</td>
<td><a href="http://server.com?redirect=http://www.example.com/index/">http://server.com?redirect=http://www.example.com/index/</a></td>
<td>The URL that will be used if the user clicks the link to continue.</td>
<td>Warning</td>
</tr>
<tr>
<td>destination_ip</td>
<td>10.100.10.10</td>
<td>The IP address of the destination site.</td>
<td>All</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Example</td>
<td>Description</td>
<td>Notification Types</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>destination_port</td>
<td>80</td>
<td>The TCP/UDP port on the destination site.</td>
<td>All</td>
</tr>
<tr>
<td>file_type</td>
<td>audio</td>
<td>The media, or MIME, type for the file.</td>
<td>File type</td>
</tr>
<tr>
<td>flow_id</td>
<td>384</td>
<td>The identifier given to the traffic flow by the firewall.</td>
<td>All</td>
</tr>
<tr>
<td>full_url</td>
<td><a href="http://www.example.com/index/">http://www.example.com/index/</a></td>
<td>The URL of the destination, including the full path.</td>
<td>All</td>
</tr>
<tr>
<td>source_ip</td>
<td>10.100.10.10</td>
<td>The IP address of the traffic source.</td>
<td>All</td>
</tr>
<tr>
<td>source_port</td>
<td>80</td>
<td>The TCP/UDP port of the traffic source.</td>
<td>All</td>
</tr>
<tr>
<td>time</td>
<td>02:50:55pm UTC</td>
<td>When the traffic flow occurred.</td>
<td>All</td>
</tr>
<tr>
<td>threat_type</td>
<td>Phishing</td>
<td>The threat type associated with the low reputation site. The reputation must be -6 or below to have a threat type.</td>
<td>Web reputation</td>
</tr>
<tr>
<td>uploads_or_downloads</td>
<td>upload</td>
<td>Whether the file transfer was an upload (source to destination) or download (destination to source).</td>
<td>File type</td>
</tr>
<tr>
<td>web_category</td>
<td>Social Networking</td>
<td>The general web category to which the destination URL belongs.</td>
<td>URL filtering</td>
</tr>
<tr>
<td>web_reputation</td>
<td>-6.7</td>
<td>The web reputation of the destination site, from -10 (worst) to 10 (best).</td>
<td>Web reputation</td>
</tr>
</tbody>
</table>

**URL and Application Filtering**

Context-Aware Security access rules allow you to control network access based on individual URLs or URL categories (called URL filtering) and application criteria, a combination of applications and traditional port-based service specifications, and even different behaviors for individual applications (called application filtering). These features can make it easier for you to define and deploy a policy without having to determine the exact characteristics of the traffic you are trying to prevent or allow, especially for traffic that intentionally changes ports to avoid firewall blocking.

Although you can define similar policies using URL filtering and application filtering, these types of filtering are not equivalent. For example, you do not get the same results if you create an access rule denying the Games URL category as you do creating an access rule denying the Games application type.

The following topics explain URL and application filtering in more detail.
Comparing URL and Application Filtering

URL and application filtering serve two different purposes:

**URL Filtering**

URL filtering denies or allows traffic based on the URL of the destination site and works for HTTP or HTTPS traffic only.

The purpose of URL filtering is primarily to completely block or allow access to a web site. Although you can target individual pages, you typically specify a host name (such as www.example.com) or a URL category, which defines a list of host names that provide a particular type of service (such as Gambling).

Thus, URL filtering rules are broad in their application and can be easily applied, so there is no delay in the device allowing or denying traffic.

You can also use URL filtering in decryption policies to help identify traffic flows that should receive specific types of decryption handling. For example, you could target the Finance category and apply the Do Not Decrypt action, so that you do not spend device resources decrypting traffic to sites that are generally trustworthy. Application filtering is not available in decryption policies.

To configure URL filtering, you specify URL objects in the Destination field of access or decryption policies. You can also include URL objects in destination object groups, which you can then use to specify the destination in these policies.

**Application Filtering**

Application filtering denies or allows traffic based on more subtle characteristics of the traffic flow. For some applications, you can specify different actions based on the behaviors available with the application; for example, you could allow Facebook access but prevent users from posting photographs.

Additionally, there are applications and application types for many non-HTTP/HTTPS traffic flows. There are even applications and application types for non-TCP/UDP flows, such as ICMP and various routing protocols. Thus, you can define policies at an application level for traffic flows unrelated to web browsing.

**Note**

Applications that use protocols other than HTTP or HTTPS typically must use their default ports to be recognized.

Also note that the applications included in an application type do not necessarily include all and only the same web sites included in the equivalent URL category.

Because it might not be obvious at the start of a traffic flow which application or behavior is included in the flow, part of a flow might be allowed before a decision is reached on the content of the flow. A deny access policy might be applied in the middle of a flow rather than at the start of the flow.

When trying to decide whether to use URL filtering or application filtering for HTTP/HTTPS traffic flows, consider whether your intention is to create a policy that applies to all traffic directed at a web site. If your intention is to treat all such traffic the same way (denying it or allowing it), use URL filtering. If your intention is to selectively block or allow traffic to the site, use application filtering.

Also keep in mind that URL and application filtering require special licenses.
Controlling Applications

The Application Visibility and Control (AVC) engine inspects traffic to determine the application associated with a traffic flow. Inspection can determine, for example, the specific application being carried over an HTTP traffic flow, differentiating between Facebook and LinkedIn, for example.

Because there are a wide variety of web-based applications, AVC makes it possible to control specific web-based applications rather than forcing you to apply a blanket policy to all web traffic, or use URL filtering to attempt to control an application associated with a specific web site. Application control gives you more granular control over web traffic than just URL filtering.

AVC also can identity non-web traffic, so that you can create application-based policies rather than protocol/port based policies. For example, you could create an application-based policy for Border Gateway Protocol traffic rather than the TCP/179 service. The AVC engine allows you to create policies to control application activity on the network without having to fully understand the underlying technology of each application.

To control traffic flows based on applications, you create context-aware access policies that specify any combination of the following in the Application field:

- Application type, to control the use of a group of related applications. For example, you can write a policy for Instant Messaging applications to cover AOL Instant Messenger, Google Talk, ICQ, and many other IM applications, if your intention is to treat them all the same. An application will map to a single type.
- Application, to control the use of a specific application.
- Application object, to control a group of applications based solely on application criteria that you define in an application policy object.
- Application-Service object, to control applications that you define based on application criteria and traditional service group objects that specify protocol and port.

Decryption Requirements for Application Filtering

Some application information might be available for encrypted traffic flows. However, in many cases, the application or behavior used in a traffic flow can be determined only if the traffic flow is not encrypted. In addition, the identified application might not be as specific as it could be, for example, Facebook, but not Facebook Games.

Thus, if an application typically uses the HTTPS (encrypted) protocol, you must ensure that any access policy you write for the application is paired with a decryption policy that applies an action that decrypts the traffic for the application.

For example, if you write an access policy for any source to any destination and specify an application that uses encryption, your decryption policy must also apply to any source and any destination, or the application might not be decrypted in all cases, meaning that the application will not always be identified.

Tips for Application Filtering

If you want to create traffic matching criteria in access policies using the application criterion, you typically just select the desired application specifications. You can do this directly or by creating reusable application or application service objects.
However, there are occasionally tricks to getting the results that you expect. The following table provides some tips on using application filtering for certain applications.

<table>
<thead>
<tr>
<th>Application</th>
<th>Filtering Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL Instant Messenger (AIM)</td>
<td>To target all AIM traffic, you must select two applications: <strong>AOL Instant Messenger</strong> and <strong>AOL protocol</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> AOL protocol is also used with ICQ, so if you want to allow one of ICQ or AIM, and disallow the other, you must allow AOL protocol.</td>
</tr>
<tr>
<td>BitTorrent</td>
<td>There is more than one application that relates to BitTorrent. You can get unexpected results if you allow one but deny another, particularly when dealing with the <strong>BitTorrent</strong> and <strong>BitTorrent Networking</strong> applications. There is also an <strong>Encrypted BitTorrent</strong> application. Best practice is to select all of these applications if you intend to write a policy on any one of them. Either allow or deny them as a group.</td>
</tr>
<tr>
<td>ICMP</td>
<td>There are many ways to target Internet Control Message Protocol (ICMP) traffic:</td>
</tr>
<tr>
<td></td>
<td>• Service objects—You can use service objects instead of application filtering. You can use the pre-defined <strong>protocol-icmp</strong> or <strong>protocol-icmp6</strong> to target all ICMP traffic (IPv4 or IPv6), or there are pre-defined objects that target each ICMP message type (named <strong>icmp-</strong>* and <strong>icmp6-</strong>*). You can also create objects to define any combination of message types.</td>
</tr>
<tr>
<td></td>
<td>• Applications—There are several applications such as <strong>internet control message protocol</strong>, <strong>internet control message protocol version 4</strong>, and <strong>ipv6-icmp</strong>. However, these applications do not match <strong>ping</strong>, which has its own application. There are also applications for some other message types named <strong>ipv6-</strong>*, but not all message types have their own application.</td>
</tr>
<tr>
<td>ICQ</td>
<td>To target all ICQ (&quot;I seek you&quot;) traffic, you must select two applications: <strong>icq</strong> and <strong>AOL protocol</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> AOL protocol is also used with AIM, so if you want to allow one of ICQ or AIM, and disallow the other, you must allow AOL protocol.</td>
</tr>
<tr>
<td>eMule</td>
<td>To target eMule traffic, select the <strong>eDonkey</strong> and <strong>encrypted emule</strong> applications.</td>
</tr>
</tbody>
</table>

**Using the Application Viewer**

Use the Application Viewer to:

- Explore the applications and application types currently available for access control and reporting.
• Determine the applications that are contained within an application type, or to which type an application belongs.

• Determine the controllable behaviors available for an application, if any.

• View the current usage of an application or application type within policies or policy objects.

• View a hit count for each application, which indicates the number of times users tried to use the application. The hit count is linked to the application detail dashboard for the application.

• View a hit count for each application type, which indicates the number of times users tried to use applications of that type. The count is a summary of all application hits within the type. The hit count is linked to the application type detail dashboard.

Tip

The hit count is based on the time range currently selected in the dashboards. Mouse over the hit count to see the time range.

To open the Applications viewer, select **Components > Applications**.

The Application Viewer includes the following items:

- **I want to**—Includes the following commands:

  - **View by Application Types**—To display application types in the list, not individual applications.

  - **View by Application Names**—To display individual applications in the list, not application types.

  - **View New Applications**—To display applications that have been added in the past 30 days through new application signature downloads.

- **List of applications or application types**—Each application shows the name, description, application type, behaviors, ports, and when the application was added. If you view the list by application type, the applications are organized in application type folders. Open a folder to see which applications are contained within the type.

  The following information is also available:

  - If any traffic for the application or application type has been seen, a hit count is also shown; click the hit count link to view the detailed dashboard for the application or application type.

  - If the application or application type has been used in a policy or policy object, a summary of the usage is shown in the list. Mouse over the item and click the **View Usage Details** command to see details about the policies and objects. Also click this link to view the full description of an object it is has been truncated with an ellipsis.

### URL Filtering

URL Filtering allows you to control user access based on the web server category of a particular HTTP or HTTPS request. For example, you can block all HTTP requests for gambling web sites, or you can decrypt all HTTPS requests for web-based email web sites.

You can also allow or block access based on individual URLs. For example, you could allow access to all web servers on your internal network, or block access to a new web site that has not yet been categorized.
To implement URL filtering, you do the following:

- Create URL objects that define the categories or individual URLs, or both, that you want to treat the same way. You can put categories or URLs in the exclude list of the object to exclude sites that would otherwise match the categories or URLs in the include list. For example, you could create a URL object for the Games category with the intention of blocking most games, but put a few specific URLs for gaming sites in the exclude list to allow access to those sites.

- (Optional.) Create destination objects to define a complex combination of URL objects associated with network group objects to define access based on a combination of destination IP addresses for hosts or networks and the URLs or categories of servers with matching addresses.

- Use URL objects or destination objects in the following policies:
  - Access, to either allow or block access to the included URLs or categories.
  - Decryption, to determine whether HTTPS access to the included URLs or categories is decrypted so that the traffic can be examined for deeper characteristics, such as application content or behavior.

### Determining the Category for a URL

URL categories are powerful tools for creating rules. For example, you might want to block gambling on the corporate network if gambling is not consistent with your corporate acceptable use policies. By creating an access rule denying the Gambling category, you implement your policy without having to type in the address of every individual gambling web site, and you do not need to invest your time in scouring the Internet to determine the address of every possible gambling site.

On the other hand, you do not want to block traffic to an acceptable site by inadvertently blocking the URL category to which the site belongs.

Thus, you might want to determine the web category of a site before defining rules that might affect traffic to the site. If you determine the site belongs to a category that you otherwise want to block, you can add the acceptable site to the Exclude list in the URL object that includes the otherwise objectionable category.

You can use any of the following methods to determine the URL category of a web site:

- If traffic to the site has already gone through the device, you can look at dashboards or Event Viewer to find the site.
  - Dashboards—Look at the Web Destinations dashboard and find the web site. Click the site to see the detailed dashboard for the destination. The Top Destinations group shows the URL category as well as the application and application type.
  - Event Viewer—Find an event with the web site as the destination. For example, open the web site from a workstation whose traffic goes through the device while you are looking at events in real time. The event details include the URL category.

- You can use the following procedure to look up the category for a site, especially if you have strong reasons to believe the site hosts malware or is otherwise objectionable, meaning that you do not want to open the site directly. You must have an account on Cisco.com.

  1. Open the following URL in your web browser: https://securityhub.cisco.com/web/submit_urls. You will be prompted to log into Cisco.com if you are not already logged in.

  2. On the Lookup or Submit URLs tab, enter the URL in the URLs for Lookup box. You can enter more than one URL at a time.
3 Select ASA CX.

4 Click Lookup.

Upon successful lookup, a table lists the URLs you entered and their associated URL categories. If there is no category, the URL has not yet been categorized. If you disagree with the category, or you have a suggestion for an uncategorized URL, you can select the URL, then select the category you believe is more appropriate, and click Submit to make a request that the category be changed. You can track your requests on the Status on Submitted URLs tab.

URL Category Descriptions

The following list describes the URL categories available at the time of this release. URL category updates can add, remove, merge, or divide categories.

Adult

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.

Examples:

- www.adultentertainmentexpo.com
- www.adultnetline.com

Advertisements

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.”

Examples:

- www.adforce.com
- www.doubleclick.com

Alcohol

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.”

Examples:

- www.samueladams.com
- www.whisky.com
Arts
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.”

Examples:
• www.moma.org
• www.nga.gov

Astrology
Astrology; horoscope; fortune telling; numerology; psychic advice; tarot.

Examples:
• www.astro.com
• www.astrology.com

Auctions
Online and offline auctions, auction houses, and classified advertisements.

Examples:
• www.craigslist.org
• www.ebay.com

Business and Industry
Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital; office supplies; industrial equipment (process equipment), machinery 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).

Examples:
• www.freightcenter.com
• www.staples.com

Chat and Instant Messaging
Web-based instant messaging and chat rooms.

Examples:
• www.icq.com
• www.meebo.com
Cheating and Plagiarism
Promoting cheating and selling written work, such as term papers, for plagiarism.
Examples:
- www.bestessays.com
- www.superiorpapers.com

Child Abuse Content
Worldwide illegal child sexual abuse content.

Computer Security
Offering security products and services for corporate and home users.
Examples:
- www.computersecurity.com
- www.symantec.com

Computers and Internet
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.
Examples:
- www.xml.com
- www.w3.org

Dating
Dating, online personals, matrimonial agencies.
Examples:
- www.eharmony.com
- www.match.com

Digital Postcards
Enabling sending of digital postcards and e-cards.
Examples:
- www.all-yours.com
- www.e-cards.com
Dining and Drinking

Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews.
Examples:
• www.hideawaybrewpub.com
• www.restaurantrow.com

Dynamic and Residential

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.
Examples:
• http://109.60.192.55
• http://dynalink.co.jp
• http://ipadsl.net

Education

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.
Examples:
• www.education.com
• www.greatschools.org

Entertainment

Details or discussion of films; music and bands; television; celebrities and fan websites; entertainment news; celebrity gossip; entertainment venues. Compare with the "Arts" category.
Examples:
• www.eonline.com
• www.ew.com

Extreme

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.
Examples:
• www.car-accidents.com
• www.crime-scene-photos.com
Fashion
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.”

Examples:
- www.fashion.net
- www.findabeautysalon.com

File Transfer Services
File-transfer services with the primary purpose of providing download services and hosted file sharing.

Examples:
- www.rapidshare.com
- www.yousendit.com

Filter Avoidance
Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services.

Examples:
- www.bypassschoolfilter.com
- www.filterbypass.com

Finance
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.”

Examples:
- finance.yahoo.com
- www.bankofamerica.com

Freeware and Sharewar
Providing downloads of free and shareware software.

Examples:
- www.freewarehome.com
- www.shareware.com
Gambling
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.”
Examples:
- www.888.com
- www.gambling.com

Games
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.
Examples:
- www.games.com
- www.shockwave.com

Government and Law
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.
Examples:
- www.usa.gov
- www.law.com

Hacking
Discussing ways to bypass the security of websites, software, and computers.
Examples:
- www.hackthissite.org
- www.gohacking.com
Hate Speech

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.

Examples:

- www.kkk.com
- www.nazi.org

Health and Nutrition

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.

Examples:

- www.health.com
- www.webmd.com

Humor

Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as "Adult."

Examples:

- www.humor.com
- www.jokes.com

Illegal Activities

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.

Examples:

- www.ekran.com
- www.thedisease.net
Illegal Downloads

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."

Examples:

- www.keygenguru.com
- www.zcrack.com

Illegal Drugs

Information about recreational drugs, drug paraphernalia, drug purchase and manufacture.

Examples:

- www.cocaine.org
- www.hightimes.com

Infrastructure and Content Delivery Networks

Content delivery infrastructure and dynamically generated content; websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.

Examples:

- www.akamai.net
- www.webstat.net

Internet Telephony

Telephonic services using the Internet.

Examples:

- www.evaphone.com
- www.skype.com

Job Search

Career advice; resume writing and interviewing skills; job placement services; job databanks; permanent and temporary employment agencies; employer websites.

Examples:

- www.careerbuilder.com
- www.monster.com
Lingerie and Swimsuits
Intimate apparel and swimwear, especially when modeled.
Examples:
  • www.swimsuits.com
  • www.victoriassecret.com

Lotteries
Sweepstakes, contests and state-sponsored lotteries.
Examples:
  • www.calottery.com
  • www.flalottery.com

Mobile Phones
Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the “Business and Industry” category.
Examples:
  • www.cbfsms.com
  • www.zedge.net

Nature
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.
Examples:
  • www.enature.com
  • www.nature.org

News
News; headlines; newspapers; television stations; magazines; weather; ski conditions.
Examples:
  • www.cnn.com
  • news.bbc.co.uk
Non-governmental Organization
Non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.
Examples:
• www.panda.org
• www.unions.org

Non-sexual Nudity
Nudism and nudity; naturism; nudist camps; artistic nudes.
Examples:
• www.artenuda.com
• www.naturistsociety.com

Online Communities
Affinity groups; special interest groups; web newsgroups; message boards. Excludes websites classified as "Professional Networking" or "Social Networking."
Examples:
• www.igda.com
• www.ieee.com

Online Storage and Backup
Offsite and peer-to-peer storage for backup, sharing, and hosting.
Examples:
• www.adrive.com
• www.dropbox.com

Online Trading
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."
Examples:
• www.tdameritrade.com
• www.scottrade.com

Organizational Email
Websites used to access business email (often via Outlook Web Access).
Parked Domains
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.
Examples:
- www.domainzaar.com
- www.parked.com

Peer File Transfer
Peer-to-peer file request websites. This does not track the file transfers themselves.
Examples:
- www.bittorrent.com
- www.limewire.com

Personal Sites
Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme.
Examples:
- www.karymullis.com
- www.stallman.org

Photo Searches and Images
Facilitating the storing and searching for, images, photographs, and clip-art.
Examples:
- www.flickr.com
- www.photobucket.com

Politics
Websites of politicians; political parties; news and information on politics, elections, democracy, and voting.
Examples:
- www.politics.com
- www.thisnation.com
Pornography
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.
Examples:
- www.redtube.com
- www.youporn.com

Professional Networking
Social networking for the purpose of career or professional development. See also “Social Networking.”
Examples:
- www.linkedin.com
- www.europeanpwn.com

Real Estate
Information that would support the search for real estate; office and commercial space; real estate listings, such as rentals, apartments, and homes; house building.
Examples:
- www.realtor.com
- www.zillow.com

Reference
City and state guides; maps, time; reference sources; dictionaries; libraries.
Examples:
- www.wikipedia.org
- www.yellowpages.com

Religion
Religious content, information about religions; religious communities.
Examples:
- www.religionfacts.com
- www.religioustolerance.org
SaaS and B2B

Web portals for online business services; online meetings.

Examples:

- www.netsuite.com
- www.salesforce.com

Safe for Kids

Directed at, and specifically approved for, young children.

Examples:

- kids.discovery.com
- www.nickjr.com

Science and Technology

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).

Examples:

- www.physorg.com
- www.science.gov

Search Engines and Portals

Search engines and other initial points of access to information on the Internet.

Examples:

- www.bing.com
- www.google.com

Sex Education

Factual websites dealing with sex; sexual health; contraception; pregnancy.

Examples:

- www.avert.org
- www.scarleteen.com
Shopping

Bartering; online purchasing; coupons and free offers; general office supplies; online catalogs; online malls.
Examples:
• www.amazon.com
• www.shopping.com

Social Networking

Social networking. See also "Professional Networking."
Examples:
• www.facebook.com
• www.twitter.com

Social Science

Sciences and history related to society; archaeology; anthropology; cultural studies; history; linguistics; geography; philosophy; psychology; women's studies.
Examples:
• www.archaeology.com
• www.anthropology.com

Society and Culture

Family and relationships; ethnicity; social organizations; genealogy; seniors; child-care.
Examples:
• www.childcare.gov
• www.familysearch.org

Software Updates

Websites that host updates for software packages.
Examples:
• www.softwarepatch.com
• www.versiontracker.com
Sports and Recreation
All sports, professional and amateur; recreational activities; fishing; fantasy sports; public parks; amusement parks; water parks; theme parks; zoos and aquariums; spas.
Examples:
- www.espn.com
- www.recreation.gov

Streaming Audio
Real-time streaming audio content including Internet radio and audio feeds.
Examples:
- www.live-radio.net
- www.shoutcast.com

Streaming Video
Real-time streaming video including Internet television, web casts, and video sharing.
Examples:
- www.hulu.com
- www.youtube.com

Tobacco
Pro-tobacco websites; tobacco manufacturers; pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as "Health and Nutrition."
Examples:
- www.bat.com
- www.tobacco.org

Transportation
Personal transportation; information about cars and motorcycles; shopping for new and used cars and motorcycles; car clubs; boats, airplanes, recreational vehicles (RV's), and other similar items. Note, car and motorcycle racing is classified as "Sports and Recreation."
Examples:
- www.cars.com
- www.motorcycles.com
Travel

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.

Examples:

- www.expedia.com
- www.lonelyplanet.com

Weapons

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."

Examples:

- www.coldsteel.com
- www.gunbroker.com

Web Hosting

Website hosting; bandwidth services.

Examples:

- www.bluehost.com
- www.godaddy.com

Web Page Translation

Translation of web pages between languages.

Examples:

- babelfish.yahoo.com
- translate.google.com

Web-based Email

Public web-based email services. Websites enabling individuals to access their company or organization’s email service are classified as “Organizational Email.”

Examples:

- mail.yahoo.com
- www.hotmail.com
Web Reputation Filtering (Malware Protection)

Users are continually at risk of obtaining malware from Internet sites. Even trusted sites can be hijacked to serve malware to unsuspecting users. As illustrated below, web pages can contain objects coming from different sources. These objects can include images, executables, Javascript, advertisements, and so forth. Compromised web sites often incorporate objects hosted on external sources. Real security means looking at each object individually, not just the initial request.

The Cisco Threat Operations Center uses dynamic updates and actionable intelligence obtained from ASAs, IPSs, Email security appliances, web security appliances, and system administrators to calculate a web reputation score for web sites. Web reputation is a statistical assessment based on context and past behavior and combines many factors of varying significance into one correlated metric. Similar to a person's credit score, web reputation is a continuous value along a graduated scale from -10 to 10. By defining a low reputation zone, you can implement predictive, zero-day protection against low reputation sites, the ones that are most likely to serve malware to your users.

The following topics explain how to implement web reputation filtering.

Guide to Web Reputation Scores

Following is a general guideline to the web reputation scores:

-10 to -6
Sites in the lowest reputation zone are dedicated or hijacked sites that persistently distribute key loggers, root-kits, and other malware. Also included are phishing sites, bots, and drive-by installers. Sites in this reputation range are almost guaranteed to be malicious.

The pre-defined default web reputation profile defines this zone as the low reputation zone.

-6 to -3
Sites in this zone tend to be aggressive ad syndication and user tracking networks. These sites are suspected of being malicious, but maliciousness has not been confirmed.

-3 to 3
Sites in this zone tend to be well managed, responsible content syndication networks and user generated content sites.
Sites in this zone have some history of responsible behavior or third party validation.

Sites in this zone have a long history of responsible behavior, have significant traffic volume, and are widely accessed.

To look up the reputation of a site, you can use the tool at http://www.senderbase.org/home.

Configuring Web Reputation Filtering

To implement reputation-based processing, you apply a web reputation profile to the following types of policy:

- Access policies that allow traffic. By adding a web reputation profile, the policy will in general allow matching traffic, but drop any traffic from a low reputation site. You can apply the profile to any or all access policies that have the Allow action.

- Decryption policies whose action is Decrypt Potentially Malicious Traffic. By adding a web reputation profile, any low reputation sites that match the policy will be decrypted, so that access policies have knowledge of the content of the traffic. The access policies can then drop the traffic if configured to do so. Even if you do not have a matching access policy that drops the traffic, decrypting the low reputation traffic provides data for reports that is otherwise unavailable for encrypted TLS/SSL traffic flows.

For access policies, you can configure a device-level profile and have the policy use that profile. You can then easily change your default filtering policy by editing the Malware Protection settings.

You must have a Web Security Essentials license to implement web reputation filtering.

Procedure

Step 1 Select Components > Objects and create the web reputation profiles needed to implement your filtering policies. There is a Default Web Reputation Profile object. If this object satisfies your requirements, you do not need to create your own objects. Otherwise, select I want to > Add Web Reputation Profile and create the object. Adjust the slider to determine the low reputation zone, which is blocked (denied), and the high reputation zone, which is allowed.

Keep in mind that the reputation score for a site can change over time, so a site can move between zones as its relative danger assessment changes.

To look up the reputation of a site, you can use the tool at http://www.senderbase.org/home.

Step 2 Select Configurations > Policies/Settings, open the Malware Protection tab, and enable web reputation filtering and select a device-level profile. The device-level profile is applied to all traffic matching access policies configured to use the device-level profile. Use the option to define your default web reputation filtering policy.

(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
Step 3 Edit access policies to apply the desired profile. For each access policy that should apply a web reputation filtering profile, edit the policy and select the appropriate profile. To use the device-level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. If you select no profile (or if the device-level profile is “none”), web reputation filtering is not applied to matching traffic. You can create web reputation profiles on the Policy Objects page, or you can create them while editing the access policies.

Step 4 Configure decryption policies if you want to use reputation as a basis for decrypting encrypted traffic. If you select **Decrypt Potentially Malicious Traffic** as the action of a decryption policy, you select a web reputation profile to design the low reputation zone. Sites in that zone are decrypted, whereas sites in the high zone are not decrypted.

Step 5 Monitor the results:

- Select **Dashboard > Malware Traffic**.
- Select **Events > Events**, then select the Context Aware Security or Encrypted Traffic views.

### Configuring Malware Protection (Web Reputation) Settings

You can configure a device-level web reputation profile and apply it to CX Context-Aware access policies. By configuring a device-level profile, you can easily apply uniform reputation filtering across your policies and quickly change settings by simply changing the device-level profile or by editing it.

Although web reputation filtering is enabled by default, you can turn it off in these settings.

**Note** You cannot configure decryption policies to use the device level profile configured here, because the web reputation setting is not optional for reputation-based decryption. You must explicitly select a profile in each decryption policy that requires one.

**Procedure**

**Step 1** Select **Configurations > Policies/Settings** and open the **Malware Protection** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

**Step 2** Select **Malware Protection: On** to enable web reputation filtering. If you change this setting, filtering is enabled or disabled when you commit your changes. However, the change applies to new traffic flows; any existing traffic flows continue to be filtered or not filtered based on the previous setting.

You must have the Web Security Essentials license to enable the service.

**Step 3** Select the device-level web reputation profile object in **Web Reputation Profile**. The system-defined **Default web reputation profile** implements the recommended filtering, but you can select **Create New Profile** to create your own, or select any other already-defined profile.

If an access policy specifies **Device Level Profile (name)**, the profile defined here is used for matching traffic.
If you leave the device-level profile empty, web reputation filtering will be disabled for any access policy configured to use it.

Step 4  Click Save.

Next Generation IPS Filtering

Next Generation IPS (Intrusion Prevention System) filtering analyzes network traffic in real time, comparing the traffic contents against known threats. If a connection matches a threat, you can drop the connection to block the threat. You can also choose to monitor but allow, or completely ignore, threats that you decide are benign.

The Cisco Security Intelligence Operations Center develops signatures that identify threats. Multiple signatures can map to a single threat. New signature sets are downloaded on a regular basis unless you disable updates. You can also implement automatic blocking of blacklisted sites, which are sites considered to be always dangerous.

The following topics explain how to implement Next Generation IPS filtering.

Configuring Next Generation IPS Filtering

You can configure device-level and per-access policy settings for Next Generation IPS filtering.

You must have the Next Generation IPS license to enable filtering.

Procedure

Step 1  Select Components > Objects and create the NG IPS profiles needed to implement your filtering policies. There is a Default NG IPS profile object. If this object satisfies your requirements, you do not need to create your own objects. Otherwise, select I want to > Add NG IPS Profile and create the object. Adjust the sliders to determine the zones you will block (deny), allow and monitor (alert, that is, generate events), and allow and do not monitor (ignore, that is, do not generate events). You can also configure exceptions for these zones if you know of specific threats that fall into a zone but which you want to treat differently.

Keep in mind that the score for a threat can change over time, so a threat can move between zones as its relative danger assessment changes.

You can see descriptions of the various threats by selecting Components > Threats.

Step 2  Select Configurations > Policies/Settings, open the Intrusion Prevention tab, and enable Next Generation IPS filtering, select a device-level profile, and configure other settings.

The device-level profile is applied to all traffic matching access policies configured to use the device-level profile. Use the option to define your default Next Generation IPS filtering policy.

(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Step 3  Edit access policies to apply the desired profile.

For each access policy that should apply a Next Generation IPS filtering profile, edit the policy and select the appropriate NG IPS profile. To use the device-level profile, select Device Level Profile (name); the name of
the profile configured is shown in the option. If you select no profile (or if the device-level profile is “none”), Next Generation IPS filtering is not applied to matching traffic. You can create NG IPS profiles on the Policy Objects page, or you can create them while editing the access policies.

**Step 4** Configure decryption policies if you want the most effective Next Generation IPS filtering for encrypted traffic.
In some cases, Next Generation IPS filtering can recognize threats in encrypted traffic. However, in other cases, the traffic must be decrypted for the threat to be identified. Thus, decryption is not an absolute requirement for Next Generation IPS filtering.

**Step 5** Monitor the results:

- Select Dashboard > NG Intrusion Prevention.
- Select Events > Events, then select the NG IPS view.

### Configuring Intrusion Prevention Settings

Use the Next Generation IPS settings to enable the service, define the device-level filtering profile, and set other advanced options.

**Procedure**

**Step 1** Select Configurations > Policies/Settings and open the Intrusion Prevention tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

**Step 2** Select Intrusion Prevention: On to enable Next Generation IPS filtering. If you change this setting, filtering is enabled or disabled when you commit your changes. However, the change applies to new traffic flows; any existing traffic flows continue to be filtered or not filtered based on the previous setting.
You must have the Next Generation IPS license to enable the service.

**Step 3** Select the device-level NG IPS profile object in NG IPS Profile. The system-defined Default NG IPS profile implements the recommended filtering, but you can select Create New Profile to create your own, or select any other already-defined profile.
If an access policy specifies Device Level Profile (name), the profile defined here is used for matching traffic. If you leave the device-level profile empty, Next Generation IPS filtering will be disabled for any access policy configured to use it.

**Step 4** Configure the following advanced settings as desired:

- **Scan High Reputation Traffic : On/Off**—Whether to perform Next Generation IPS filtering for traffic flows to high reputation sites, which are defined as low risk, that is, worthy of being bypassed. Next Generation IPS can identify certain types of traffic as being highly unlikely to contain threats, and web reputation can be part of this identification. Be aware that reputation scores are updated regularly with WBRS downloads, and you need to have an active Web Security Essentials license for these downloads to occur; otherwise, the reputation scores used in this evaluation will become dated.
• **Block Blacklisted Traffic: On/Off**—Whether to block the sites on the blacklist downloaded periodically through the engine and signature updates. These sites are considered so threatening that all traffic from them or to them is dangerous. The actual sites on the list change as updates occur. If you enable this option, blacklisted traffic flows are blocked before any other access policies are considered.

• **Blacklisted Traffic Eventing: On/Off**—Whether to generate traffic events when a traffic flow is dropped because it involves a blacklisted site. If you turn this off, blacklisted flows are dropped silently. If you enable eventing, dropped traffic generates Flow Deny events where the policy name is Blacklist (Source) or Blacklist (Destination), depending on whether the blacklist site originated the traffic or was the destination.

**Step 5**  
Click **Save**.

---

**Viewing Next Generation IPS Threats**

You can view descriptions of the threats available in the system.  
Select **Components > Threats** to see the list.  
For threats with long descriptions, which are truncated, mouse over the threat and click **Read More**. You can find additional detail from external sources by clicking the **Go to Information Site** link; the link will open in a new window.

**Configuring Signature and Engine Updates**

Applications and their attributes, URL categories, and web reputation are defined by signatures and applied by Security Application Scanner (SAS) engines. Next Generation IPS also includes a signature and engine package. Updates to these and other components are made available frequently on an update server. You can configure a time window and an HTTP proxy for obtaining these updates.

If you do not change the update settings, the device checks the update server every 5 minutes throughout the day and downloads updates if any are found. Updates can result in the following changes:

• New URL categories, applications, application behaviors, application types, or Next Generation IPS threats.

• Changes to existing URL categories, applications and their attributes, or Next Generation IPS threats. Existing items might be renamed or deleted. Two or more items can be merged, or a single item can be split into one or more items.
  * If an item is simply renamed, the new name appears in any policy that used the item and your policy continues to behave as expected.
  * If an item is deleted, split, or merged, the item is replaced with an error message indicating that it is unsupported. No traffic will match the item. You must edit each affected policy to select an appropriate replacement.

• Changes in the URLs contained within a URL category.

• Changes in the web reputation of web sites.
Changes in how an application or website is categorized can alter how traffic for the application, or traffic to the website, is handled based on your existing policies. For example, if a new site is added to a category that you are blocking, traffic to that site might have been allowed prior to the update, but users will suddenly find traffic blocked after the update.

If new behaviors are added to an application for which you have written a policy, the new behaviors are initially allowed. You need to edit the appropriate policy if you want to deny the behavior. Use the Application Viewer to see which applications are new in the past 30 days to help you identify whether new access policies are desirable. To open the Applications viewer, select Components > Applications.

Tip
If you define a proxy in PRSM Multiple Device mode, the same proxy is used by all managed CX devices. Ensure that the geographical location of the proxy in relation to the managed devices makes sense. If you cannot use the same proxy for all managed devices, use multiple PRSM servers to manage groups of devices that can use the same proxy. Alternatively, alter the firewall rules for the management networks for each device to allow access to the Internet, so that a proxy is not needed.

Procedure

Step 1
Select Configurations > Updates.
The Updates page shows the various signature packages and engines that can be updated, including the date and time of the last update and the component version. In PRSM Multiple Device mode, there are separate lists for PRSM and for each managed CX device; you can compare the component versions among the systems.

Packages include the following:

• AVC—Application Visibility and Control. The components in this package define the applications and application types for which you can configure policies.

• WBRS—Metascan web reputation filters. The components in this package define web reputation scores and URL categories.

• SAS—Security Application Scanners. The SAS engines evaluate traffic to determine the application, web category, or web reputation associated with the destination.

• TP—Threat Protection, for Next Generation IPS threat filtering. There is a signature package and an engine package.

• CX Telemetry—Network participation engine. This client collects attack and usage data and sends it to Cisco for analysis if you opt into network participation.

• IBRS Drop—IPS Base Reputation System Drop list, a blacklist of high-threat sites. You can configure Next Generation IPS filtering to drop traffic flows to and from sites on this list.

Step 2
Select I want to > Edit Settings.

Step 3
Configure the following settings as desired:

• Updates—How frequently to download updates:

  • Check every 5 minutes—The update server is checked every 5 minutes throughout the day seven days a week. This is the default.

  • Check every 5 minutes within window—The update server is checked daily but only within the time window that you select. Click in the boxes to select the start and end times, which can be in
15 minute increments. For example, you could select "From 12:00 AM to 04:00 AM" to limit updates to a lower-traffic early morning period.

*Note* The time window is limited to a single day. You cannot specify a time window that straddles midnight.

*Never check*—The update server is never checked. Use this setting temporarily or if you decide to not purchase feature licenses.

**HTTP Proxy Server: Enable/Disable**—The proxy server through which updates will be downloaded. If you do not configure a proxy server, updates are obtained through the management interface, so you need to ensure there is a route to the Internet from your management network. To configure a proxy server, configure the following properties:

* HTTP Proxy Server: Enable.

* Proxy IP—The IP address or fully-qualified domain name of the proxy server. For example, 10.100.10.10 or proxy.example.com.

* Port—The port on which the proxy server is listening. Typical ports are 80, 3128, or 8080. Consult the configuration of the proxy server to determine the correct port number.

* Username, Password—The credentials required to log into the proxy server and pass traffic through it, if any are needed.

**Step 4** Click *Save*.

**What to Do Next**

* Use Event Viewer to see system events related to updates. Look at the System Events view and look for updaters connection events.

* Use the Application Viewer to see the new applications that have been installed in the past 30 days.

* Configure policies to use new items.

* View the dashboards to see statistics for new items. New items are immediately available in dashboards, assuming any traffic that goes through the system matches them.

**Troubleshooting Signature and Engine Updates**

Use Event Viewer to see system events related to updates. Look at the System Events view and look for updaters connection events.

Following are some typical issues you might encounter:

* Updates occur only if the system has active licenses for the services associated with a signature or engine update. Ensure that you have the appropriate licenses for features that you are using.

* Updates occur only if the system has a route to the Internet and can reach the Cisco update server. You have two choices: either ensure that the network to which the management interface is connected has a route to the Internet, or configure an HTTP proxy server for the Updater.
• When using PRSM Multiple Device mode, be aware that both the CX device and the PRSM server download updates.

  ◦ If you import a device that has a more recent version than the PRSM server, you might see "(Unrecognized application)" in imported access policies that include specifications for applications not available in PRSM. These policies will deploy correctly, and PRSM will show the correct application name as soon as it has the updated signatures.

  ◦ If the PRSM server has the more recent update, applications that are no longer defined in the signatures have "(deprecated)" appended to the name in the policy. However, these application names appear in dashboards and reports without this indication. You should pro-actively redefine policies that specify deprecated applications.

• If you define a proxy in PRSM Multiple Device mode, the same proxy is used by all managed CX devices. Ensure that the geographical location of the proxy in relation to the managed devices makes sense. If you cannot use the same proxy for all managed devices, use multiple PRSM servers to manage groups of devices that can use the same proxy. Alternatively, alter the firewall rules for the management networks for each CX device to allow access to the Internet, so that a proxy is not needed.

• Signatures are not updated unless the related engine is at the required version. Once the new engine is installed, new signature files that require it will be installed.

• The system can gracefully recognize bad updates, remove the update, and return to the previous good version without user intervention. The last known good version is always kept for recovery purposes.