Managing Access to Web Applications

This topic contains the following sections:

Overview of Managing Access to Web Applications

The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

Using Access Policies you can:

- Control application behaviors
- Control the amount of bandwidth used for particular application types
- Notify end-users when they are blocked
- Assign controls to Instant Messaging, Blogging and Social Media applications
- Specify Range Request settings

To control applications using the AVC engine, perform the following tasks:

Task	Link to Task
Enable the AVC engine	Enabling the AVC Engine, on page 2
Set Controls in an Access Policy Group	Configuring Application Control Settings in an Access Policy Group, on page 5
Limit bandwidth consumed by some application types to control congestion	Controlling Bandwidth, on page 6

Task	Link to Task
Allow instant messaging traffic, but disallow file sharing using instant messenger	Controlling Instant Messaging Traffic, on page 8

Enabling the AVC Engine

Enable the AVC engine when you enable the Acceptable Use Controls.

Note You can view the AVC engine scanning activity in the Application Visibility report on the Reporting > Application Visibility page.

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

Step 2 Click **Enable** or **Edit Global Settings**, depending on the current status of the Acceptable Use Controls.

Step 3 Be sure Enable Cisco Web Usage Controls is checked.

Step 4 In the Acceptable Use Controls Service panel, select **Cisco Web Usage Controls**, and then select **Enable Application Visibility and Control**.

Step 5 Select the **Default Action for Unreachable Service**: **Monitor** or **Block**.

Step 6 Submit and Commit Changes.

What to do next

Related Topics

- AVC Engine Updates and Default Actions , on page 2
- User Experience When Requests Are Blocked by the AVC Engine, on page 3

AVC Engine Updates and Default Actions

AsyncOS periodically queries the update servers for new updates to all security service components, including the AVC engine. AVC engine updates can include support for new application types and applications, as well as updated support for existing applications if any application behaviors change. By updating the AVC engine between AsyncOS version updates, the Secure Web Appliance remains flexible without requiring a server upgrade.

AsyncOS for Web assigns the following default actions for the Global Access Policy:

- New Application Types default to **Monitor**.
- New application behaviors, such as block file transfer within a particular application; defaults to **Monitor**.
- New applications for an existing application type default to the Application Type's default.

Note In the Global Access Policy, you can set the default action for each Application Type, so new applications introduced in an AVC engine update automatically inherit the specified default action. See Configuring Application Control Settings in an Access Policy Group, on page 5.

User Experience When Requests Are Blocked by the AVC Engine

When the AVC engine blocks a transaction, the Web Proxy sends a block page to the end user. However, not all Websites display the block page to the end user; many Websites display dynamic content using JavaScript instead of a static Web page and are not likely to display the block page. Users are still properly blocked from downloading malicious data, but they may not always be informed of this by the Website.

Note When the HTTPS proxy is disabled and Webroot is:

- Enabled - The AVC engine may or may not be launched and return the verdict. The transaction will be processed according to scanner's verdict.
- Disabled - The AVC engine will be launched and return the verdict. The transaction will be processed according to AVC's verdict.

Policy Application Control Settings

Controlling applications involves configuring the following elements:

Option	Description
Application Types	A category that contains one or more applications.
Applications	Particular applications within an Application Type.
Application behaviors	Particular actions or behaviors that users can do within an application that administrators can control. Not all applications include behaviors you can configure.

You can configure application control settings in Access Policy groups. On the **Web Security Manager** > **Access Policies** page, click the **Applications** link for the policy group you want to configure. When configuring applications, you can choose the following actions:

Option	Description
Block	This action is a final action. Users are prevented from viewing a webpage and instead an end-user notification page displays
Monitor	This action is an intermediary action. The Web Proxy continues comparing the transaction to the other control settings to determine which final action to apply

Option	Description
Restrict	This action indicates that an application behavior is blocked. For example, when you block file transfers for a particular instant messaging application, the action for that application is Restrict.
Bandwidth Limit	For certain applications, such as Media and Facebook, you can limit the bandwidth available for Web traffic. You can limit bandwidth for the application itself, and for its users.

Related Topics

- Range Request Settings, on page 4
- Rules and Guidelines for Configuring Application Control , on page 5

Range Request Settings

When HTTP range requests are disabled and a large file is downloaded over multiple streams, the consolidated package is scanned. This disables the performance advantages of download-management utilities and applications that are used to download large objects.

Alternatively, when Range Request Forwarding is enabled (see Configuring Web Proxy Settings), you can control how incoming range requests are handled on a per-policy basis. This process is known as "byte serving" and is a means of bandwidth optimization when requesting large files.

However, enabling range request forwarding can interfere with policy-based Application Visibility and Control (AVC) efficiency, and can compromise security. Please exercise caution and enable HTTP Range Request Forwarding only if the advantages outweigh the security implications.

Note The Range Request Settings are available only when Range Request Forwarding is enabled, and at least one application is set to Block, Restrict, or Throttle.

Range Request Settings for Policy	
Range Request Settings	• **Do not forward range requests**—The client sends a request for a particular range. But, the Secure Web Appliance removes the range header from the request before sending it to the target server. The Secure Web Appliance then scans the entire file and sends the range of bytes to the client. **Note** When the client sends the range request for the first time, Secure Web Appliance, expecting subsequent range requests from the client, sends the entire file. For any successive request from the same or another client, Secure Web Appliance delivers only the partial content to the client. • **Forward range requests**—The client sends a request for a particular range. The Secure Web Appliance sends the same request to the target server and receives a partial content which is then returned to the client. The Secure Web Appliance scans only the partial content for which the scan results may not be accurate.

Exception list	You can specify traffic destinations which are exempt from the current forwarding selection. That is, when **Do not forward range requests** is selected, you can specify destinations for which requests are forwarded. Similarly, when **Forward range requests** is selected, you can specify destinations for which requests are not forwarded.

Rules and Guidelines for Configuring Application Control

Consider the following rules and guidelines when configuring application control settings:

- The supported Application Types, applications, and application behaviors may change between AsyncOS for Web upgrades, or after AVC engine updates.
- If you enable Safe Search or Site Content Rating, the AVC Engine is tasked with identifying applications for safe browsing. As one of the criteria, the AVC engine will scan the response body to detect a search application. As a result, the appliance will not forward range headers.
- In Application Type listings, the summary for each Application Type lists the final actions for its applications, but does not indicate whether these actions are inherited from the global policy or configured in the current Access Policy. To learn more about the action for a particular application, expand the application type.
- In the Global Access Policy, you can set the default action for each Application Type, so new applications introduced in an AVC engine update automatically inherit the default action.
- You can quickly configure the same action for all applications in an application type by clicking the “edit all” link for the Application Type in Browse view. However, you can only configure the application action, not application behavior actions. To configure application behaviors, you must edit the application individually.
- In Search view, when you sort the table by the action column, the sort order is by the final action. For example, “Use Global (Block)” comes after “Block” in the sort order.
- Decryption may cause some applications to fail unless the root certificate for signing is installed on the client.

Related Topics

- Configuring Application Control Settings in an Access Policy Group, on page 5
- Configuring Overall Bandwidth Limits, on page 7
- Viewing AVC Activity, on page 9

Configuring Application Control Settings in an Access Policy Group

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

Step 2 Click the link in the Policies table under the Applications column for the policy group you want to edit.

Step 3 When configuring the Global Access Policy:

a) Define the default action for each Application Type in the **Default Actions for Application Types** section.

b) You can edit the default actions for each Application Type's individual members, as a group or individually, in the **Edit Applications Settings** section of the page. Editing the default action for individual applications is described in the following steps.

Step 4 When configuring a user defined Access Policy, choose **Define Applications Custom Settings** in the **Edit Applications Settings** section.

Step 5 In the Application Settings area, choose **Browse view** or **Search view** from the drop-down menu:

- **Browse view.** You can browse Application Types. You can use Browse view to configure all applications of a particular type at the same time. When an Application Type is collapsed in Browse view, the summary for the Application Type lists the final actions for its applications; however it does not indicate whether the actions are inherited from the global policy, or configured in the current Access Policy.
- **Search view.** You can search for applications by name. You might use Search view when the total list of applications is long and you need to quickly find and configure a particular application.

Step 6 Configure the action for each application and application behavior.

Step 7 Configure the bandwidth controls for each applicable application.

Step 8 Submit and Commit Changes.

What to do next

Related Topics

- Controlling Bandwidth, on page 6

Controlling Bandwidth

When both the overall limit and user limit applies to a transaction, the most restrictive option applies. You can define bandwidth limits for particular URL categories by defining an Identity group for a URL category and using it in an Access Policy that restricts the bandwidth.

You can define the following bandwidth limits:

Bandwidth limit	Description	Link to Task
Overall	Define an overall limit for all users on the network for the supported application types. The overall bandwidth limit affects the traffic between the Secure Web Appliance and application servers. It does not limit traffic served from the web cache.	Configuring Overall Bandwidth Limits, on page 7
User	Define a limit for particular users on the network per application type. User bandwidth limits traffic from web servers as well as traffic served from the web cache.	Configuring User Bandwidth Limits, on page 7

Note Defining bandwidth limits only throttles the data going to users. It does not block data based on reaching a quota. The Web Proxy introduces latency into each application transaction to mimic a slower link to the server.

Configuring Overall Bandwidth Limits

Step 1 Choose **Web Security Manager > Overall Bandwidth Limits**

Step 2 Click **Edit Settings**.

Step 3 Select the **Limit to** option.

Step 4 Enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps).

Step 5 Submit and Commit Changes.

Configuring User Bandwidth Limits

You can define user bandwidth limits by configuring bandwidth control settings on the Applications Visibility and Control page of Access Policies. You can define the following types of bandwidth controls for users in Access Policies:

Option	Description	Link to task
Default bandwidth limit for an application type	In the Global Access Policy, you can define the default bandwidth limit for all applications of an application type.	Configuring the Default Bandwidth Limit for an Application Type, on page 7
Bandwidth limit for an application type	In a user defined Access Policy, you can override the default bandwidth limit for the application type defined in the Global Access Policy.	Overriding the Default Bandwidth Limit for an Application Type, on page 8
Bandwidth limit for an application	In a user defined or Global Access Policy, you can choose to apply the application type bandwidth limit or no limit (exempt the application type limit).	Configuring Bandwidth Controls for an Application, on page 8

Configuring the Default Bandwidth Limit for an Application Type

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

Step 2 Click the link in the policies table under the Applications column for the Global Access Policy.

Step 3 In the **Default Actions for Application Types** section, click the link next to “Bandwidth Limit” for the application type you want to edit.

Step 4 Select **Set Bandwidth Limit** and enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps).

Step 5 Click **Apply**.

Step 6 Submit and Commit Changes.

Overriding the Default Bandwidth Limit for an Application Type

You can override the default bandwidth limit defined at the Global Access Policy group in the user defined Access Policies. You can only do this in Browse view.

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

Step 2 Click the link in the policies table under the Applications column for the user defined policy group you want to edit.

Step 3 Choose **Define Applications Custom Settings** in the **Edit Applications Settings** section.

Step 4 Click the link next to "Bandwidth Limit" for the application type you want to edit.

Step 5 To choose a different bandwidth limit value, select **Set Bandwidth Limit** and enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps). To specify no bandwidth limit, select **No Bandwidth Limit for Application Type**.

Step 6 Click **Apply**.

Step 7 Submit and Commit Changes.

Configuring Bandwidth Controls for an Application

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

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

Step 3 Expand the application type that contains the application you want to define.

Step 4 Click the link for the application you want to configure.

Step 5 Select **Monitor**, and then choose to use either the bandwidth limit defined for the application type or no limit.

Note The bandwidth limit setting is not applicable when the application is blocked or when no bandwidth limit is defined for the application type.

Step 6 Click **Done**.

Step 7 Submit and Commit Changes.

Controlling Instant Messaging Traffic

You can block or monitor the IM traffic, and depending on the IM service, you can block particular activities (also known as application behaviors) in an IM session.

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

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

Step 3 Click **Define Applications Custom Setting**.

Step 4 Expand the Instant Messaging application type.

Step 5 Click the link next to the IM application you want to configure.

Step 6 To block all traffic for this IM application, select **Block**.

Step 7 To monitor the IM application, but block particular activities within the application, select **Monitor**, and then select the application behavior to **Block**.

Step 8 Click **Done**.

Step 9 Submit and Commit Changes.

Viewing AVC Activity

The **Reporting > Application Visibility** page displays information about the top applications and application types used. It also displays the top applications and application types blocked.

AVC Information in Access Log File

The access log file records the information returned by the AVC engine for each transaction. The scanning verdict information section in the access logs includes the fields listed below:

Description	Custom Field in Access Logs	Custom Field in W3C Logs
Application name	%XO	x-avc-app
Application type	%Xu	x-avc-type
Application behavior	%Xb	x-avc-behavior