7

Security Services

This chapter describes how to configure Unified Threat Management (UTM) security services to provide protection from Internet threats. It includes the following sections:

To access the Security Services pages, click **Security Services** in the left hand navigation pane.

About Security Services

The security appliance supports a variety of UTM security services to provide the Internet threat protection for your network. By default, all security services except Network Reputation are disabled.

The following table lists all available security services on the security appliance.

Security Service	Description
Anti-Virus	Anti-Virus prevents network threats over a multitude of protocols, including HTTP, FTP, POP3, SMTP, CIFS, NETBIOS, and IMAP. See **Configuring Anti-Virus, page 302**.
Application Control	Application Control monitors and controls the use of applications on your network. See **Configuring Application Control, page 309**.
Spam Filter	Spam Filter detects the email sender's reputation score. If the reputation score is below the threshold, then the email is blocked or tagged as spam or suspected spam. See **Configuring Spam Filter, page 319**.
Intrusion Prevention (IPS)	IPS monitors network traffic for malicious or unwanted behaviors and can react, in real-time, to block or prevent those activities. See **Configuring Intrusion Prevention, page 321**.
Network Reputation	Network Reputation blocks incoming traffic from IP addresses that are known to initiate attacks throughout the Internet. See **Network Reputation, page 332**.
Web Reputation Filtering	Web Reputation Filtering prevents client devices from accessing dangerous websites containing viruses, spyware, malware, or phishing links. See **Configuring Web Reputation Filtering, page 325**.
Web URL Filtering	Web URL Filtering allows you to block HTTP access to malicious websites based on URL categories. See **Configuring Web URL Filtering, page 327**.

Anti-Virus, Application Control, and IPS are signature-based security services. You must update the signatures frequently to ensure that these security services can give you the best protection.

Spam Filter, Network Reputation, Web Reputation Filtering, and Web URL Filtering are reputation-based security services. They obtain the security data from the SecApps servers and determine which traffic is allowed or blocked. Make sure that the SecApps servers are online after you enable these security services, otherwise they will not be available.

Activating Security Services

The security services are licensable. You must install a valid security license on the security appliance to activate security services. A valid security license is also required for support of SSLVPN with mobile devices such as smart phones and tablets.The Product Authorization Key (PAK) is required to validate the security license. You can find the license code from the Software License Claim Certificate that Cisco provides upon purchase of the security appliance.

Make sure that the security license is installed and does not expire before you configure security services. Go to the Device Management > License Management page to validate the security license or to renew the security license before it expires. See Installing or Renewing Security License, page 441.

Priority of Security Services

Multiple security services can work simultaneously to protect your network. Web Reputation Filtering has a higher priority than Web URL Filtering. You can add the website exceptions in the website access control list when you configure a Web URL Filtering policy profile. The website exceptions can override the profile's URL category settings, but cannot override the Web Reputation Filtering settings.

For example, a website as an exception is allowed to access by Web URL Filtering, but it has reputation score lower than the web reputation threshold specified in Web Reputation Filtering. Web Reputation Filtering will block access to this website even if it is an exception in the website access control list, unless you change the web reputation threshold.

Security Services Dashboard

Use the Dashboard page to view the status of the security license, enable or disable security services, and check for signature updates for all signature-based security services.

STEP 1 Click **Security Services > Dashboard**.

The Dashboard window opens.

STEP 2 In the **License Status** area, the security license status is displayed. If the security license expires, go to the Device Management > License Management page to renew the license. See Installing or Renewing Security License, page 441.

STEP 3 In the **Settings Summary** area, you can perform the following tasks:

- To enable a security service, check the box in the **Enable** column. By default, only Network Reputation is enabled.
- To configure the settings for a security service, click **Configure**.
- To immediately check for new updates for security services, click **Check for Updates Now**.
  - For signature-based security services such as Anti-Virus, Application Control, and IPS, clicking this button will check for signature updates from Cisco's signature server. Anti-Virus and IPS use different signature database but IPS and Application Control use the same signature database. This operation will check for signature updates for all of them at a time. If a newer signature file than your current one is available on the server, the new signature file will be downloaded to your device.

    NOTE: A valid Cisco.com account is required to check for signature updates from Cisco's signature server. Go to the Device Management > Cisco.com Account page to configure your Cisco.com account credentials on the security appliance. See Configuring Cisco.com Account, page 424.
  - For reputation-based security services such as Spam Filter, Web URL Filtering, Web Reputation Filtering, and Network Reputation, clicking this button will only check for new updates for Network Reputation. This operation will not check for new updates for Spam Filter, Web URL Filtering, and Web Reputation Filtering.

The date and time of your last check are displayed in the **Last Check** column. When a signature file is updated successfully, the date and time of the last successful update are displayed in the **Last Update** column.

- Spam Filter, Web URL Filtering, Web Reputation Filtering, and Network Reputation obtain the security data from the SecApps servers and determine which traffic is allowed or blocked. The **Server Status** column displays the status of SecApps servers. Make sure that the SecApps servers are online after you enable these security services; otherwise they will not be available.

STEP 4 In the **External Web Proxy Settings** area, specify an external web proxy used to redirect HTTP traffic if needed:

- **External Web Proxy:** Click **On** to support such as Scansafe and third party outbound web proxies, or click **Off** to disable it.

  NOTE: When the external web proxy feature is enabled, the Firewall, QoS, Web URL Filtering, and Web Reputation Filtering settings will not work or be skipped for HTTP traffic.

- **Redirected Web Proxy IP Address:** Enter the IP address of the external web proxy used to redirect HTTP traffic.

- **Redirected HTTP Ports:** Specify the proxy ports. To add an entry, click **Add**. To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

STEP 5 Click **Save** to apply your settings.

Viewing Security Services Reports

Use the Security Services Reports page to view the reports for all security services. To open the page, click **Security Services > Security Services Reports**. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Refer to the following topics:

- **Viewing Web Security Report, page 296**
- **Viewing Anti-Virus Report, page 297**
- **Viewing Email Security Report, page 298**
- **Viewing Network Reputation Report, page 299**

- Viewing IPS Report, page 300
- Viewing Application Control Report, page 301

NOTE The security services reports are only active after the security license is installed. Before you choose a report to view, make sure that the corresponding security service is enabled.

Viewing Web Security Report

This report displays the number of web access requests logged and the number of websites blocked by Web URL Filtering, Web Reputation Filtering, or both.

STEP 1 In the **Web Security** tab, specify the following information:

- **Enable:** Check this box to enable the web security report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of websites blocked by Web URL Filtering and/or Web Reputation Filtering in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and the time, the IP address and the MAC address of the host that initiated the request, the web site, the blocked URL, the filter that blocked the request, and the number of times that the connection was blocked.
- **Processed Requests:** Check this box to display the number of web access requests logged by Web URL Filtering and/or Web Reputation Filtering in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of web access requests processed and total number of websites blocked since Web URL Filtering and Web Reputation Filtering were activated.

Field	Description
Total Last 7 Days	Total number of web access requests processed and total number of websites blocked in last seven days.
Total Today	Total number of web access requests processed and total number of websites blocked in one day.
Graph	Total number of web access requests processed and total number of websites blocked per day in last seven days.

Viewing Anti-Virus Report

This report displays the number of files checked and the number of viruses detected by the Anti-Virus service.

STEP 1 In the **Anti-Virus** tab, specify the following information:

- **Enable:** Check this box to enable the Anti-Virus report, or uncheck this box to disable it.
- **Detected Requests:** Check this box to display the number of viruses detected by the Anti-Virus service in the graph. To view more information about detected requests, click the red bar in the graph. A pop-up window displays the following information for each detected request: the date and the time, the IP address and the MAC address of the source and of the destination, the protocol used for the connection, the action taken, and the number of times a virus was found.
- **Processed Requests:** Check this box to display the number of files checked by the Anti-Virus service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.

Field	Description
Total Since Activated	Total number of files checked and total number of viruses detected since the Anti-Virus service was activated.
Total Last 7 Days	Total number of files checked and total number of viruses detected in last seven days.
Total Today	Total number of files checked and total number of viruses detected in one day.
Graph	Total number of files checked and total number of viruses detected per day in last seven days.

Viewing Email Security Report

This report displays the number of emails checked and the number of spam or suspected spam emails detected by the Spam Filter service.

STEP 1 In the **Email Security** tab, specify the following information:

- **Enable:** Check this box to enable the email security report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of spam or suspected spam emails detected by the Spam Filter service in the graph.
- **Processed Requests:** Check this box to display the number of emails checked by the Spam Filter service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of emails checked and total number of spam or suspected spam emails detected since the Spam Filter service was activated.

Field	Description
Total Last 7 Days	Total number of emails checked and total number of spam or suspected spam emails detected in last seven days.
Total Today	Total number of emails checked and total number of spam or suspected spam emails detected in one day.
Graph	Total number of emails checked and total number of spam or suspected spam emails detected per day in last seven days.

Viewing Network Reputation Report

This report displays the number of packets checked and the number of packets blocked by the Network Reputation service.

STEP 1 In the **Network Reputation** tab, specify the following information:

- **Enable:** Check this box to enable the network reputation report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets blocked by the Network Reputation service in the graph.
- **Processed Requests:** Check this box to display the number of packets checked by the Network Reputation service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets checked and total number of packets blocked since the Network Reputation service was activated.
Total Last 7 Days	Total number of packets checked and total number of packets blocked in last seven days.

Field	Description
Total Today	Total number of packets checked and total number of packets blocked in one day.
Graph	Total number of packets checked and total number of packets blocked per day in last seven days.

Viewing IPS Report

This report displays the number of packets detected and the number of packets dropped by the IPS service.

STEP 1 In the **IPS** tab, specify the following information:

- **Enable:** Check this box to enable the IPS report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets dropped by the IPS service in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and time, the IP address and the MAC address of the source and of the destination, the action taken, and the number of times that this event was detected.
- **Processed Requests:** Check this box to display the number of packets detected by the IPS service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets detected and total number of packets dropped since the IPS service was activated.
Total Last 7 Days	Total number of packets detected and total number of packets dropped in last seven days.
Total Today	Total number of packets detected and total number of packets dropped in one day.

Field	Description
Graph	Total number of packets detected and total number of packets dropped per day in last seven days.

Viewing Application Control Report

This report displays the number of packets detected and the number of packets blocked by the Application Control service.

STEP 1 In the **Application Control** tab, specify the following information:

- **Enable:** Check this box to enable the application control report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets dropped by the Application Control service in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and time, the IP address and the MAC address of the host that initiated the request, the blocked application, and the number of times that the application was blocked.
- **Processed Requests:** Check this box to display the number of packets detected by the Application Control service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets detected and total number of packets blocked since the Application Control service was activated.
Total Last 7 Days	Total number of packets detected and total number of packets blocked in last seven days.
Total Today	Total number of packets detected and total number of packets blocked in one day.

Field	Description
Graph	Total number of packets detected and total number of packets blocked per day in last seven days.

Configuring Anti-Virus

Anti-Virus helps protect your network from viruses and malware. Anti-Virus scans for viruses over a multitude of protocols, including HTTP, FTP, POP3, SMTP, CIFS, NETBIOS, and IMAP.

NOTE Anti-Virus covers the most recent and widespread threats but cannot detect all known viruses (including rare samples). It delivers “first layer defense,” efficiently handles malware outbreaks, and catches the most widespread and the most dangerous malware (commonly known as “in-the-wild” malware). Currently, the most widespread types of malware are worms, trojans, exploits, viruses, and rootkits. As new, widespread threats emerge, Anti-Virus will expand to include the most dangerous types of threats.

You can apply the Anti-Virus service to the zones. Anti-Virus examines all incoming and outgoing traffic for the selected zones and performs the action that you specify for different types of traffic. You can choose to drop the connection, delete the infected files, and/or send an alert email to the email receiver if viruses are detected.

Because files containing malicious code and viruses can be compressed, Anti-Virus can automatically decompress the compressed files and then scan the viruses. Anti-Virus supports scanning single level compressed files for these file types: zip, gzip, tar, rar 2.0, and bz2 (Bzip).

Anti-Virus uses signatures to identify the infected files. You must update the signatures frequently to keep the protection current. See **Updating Anti-Virus Signatures, page 308**.

You can enable the Anti-Virus report from the Security Services > Security Services Reports page or from the Status > Security Services Reports page to see the number of files checked and the number of viruses detected by the Anti-Virus service. See **Viewing Anti-Virus Report, page 297**.

You can enable the Anti-Virus Alert feature to send an alert email for virus events at a specified interval to a specified email address. See Configuring Email Alert Settings, page 408.

Refer to the following topics:

- General Anti-Virus Settings, page 303
- Configuring Advanced Anti-Virus Settings
- Configuring HTTP Notification, page 307
- Configuring Email Notification, page 307
- Updating Anti-Virus Signatures, page 308

General Anti-Virus Settings

Use the General Settings page to enable or disable Anti-Virus, specify the zones to scan for viruses, and configure the preventive actions for different types of traffic, and set the maximum file size to scan.

STEP 1 Click **Security Services > Anti-Virus > General Settings**.

STEP 2 Click **On** to enable Anti-Virus, or click **Off** to disable it.

STEP 3 In the **Zone to Scan** area, specify the zones to scan the viruses:

- **WAN Zone:** Choose this option to scan the viruses for all incoming and outgoing traffic for the WAN zone.
- **WAN+VPN Zone:** Choose this option to scan the viruses for all incoming and outgoing traffic for both WAN and VPN zones.
- **All Zone:** Choose this option to scan the viruses for all incoming and outgoing traffic for all zones.

STEP 4 In the **Applications to Scan** area, perform the following tasks to scan for viruses on your network:

- **Enable:** Check the box in this column to scan for viruses over a protocol.
- **Logging:** Check the box in this column to log the events when viruses are detected.

  To log Anti-Virus events, you must first check the **Logging** box for the protocols, and then go to the Device Management > Logs pages to configure the log settings and log facilities. See Log Management, page 442.

  - To save Anti-Virus logs to the local syslog daemon, you must enable the Log feature, set the log buffer size and the severity level for local logs, and then enable the Local Log settings for the Anti-Virus facility.

- To save Anti-Virus logs to the remote syslog server if you have a remote syslog server support, you must enable the Log feature, specify the Remote Log settings, and enable the Remote Log settings for the Anti-Virus facility.

- **Action:** Specify the preventive action for different types of traffic when viruses are detected. The following table lists all available actions for each protocol.

Protocol	Action
HTTP	**None:** No action is required when viruses are detected. **Notify:** Send an alert message to the user when viruses are detected in web pages or in files that the user tries to access. **Notify + Drop Connection:** Drop the connection and send an alert message to the user when viruses are detected in web pages or in files that the user tries to access. **Disable HTTP Resume:** Optionally, check this box to disable resuming web-based file transfer by using the HTTP protocol when viruses are detected. **NOTE:** If you choose Notify or Notify + Drop Connection, go to the HTTP Notification page to configure the notification message. See **Configuring HTTP Notification, page 307**.
FTP	**None:** No action is required when viruses are detected. **Drop Connection:** Drop the connection when viruses are detected. **Disable FTP Resume:** Optionally, check this box to disable resuming file transfer by using the FTP protocol when viruses are detected.

Protocol	Action
SMTP Email Attachments	**None:** No action is required when viruses are detected. **Notify:** Send the original email and an alert email to the email receiver when viruses are detected in email attachments. **Notify + Destruct File:** Delete the infected files and send the original email and an alert email to the email receiver when viruses are detected in email attachments. **NOTE:** If you choose Notify or Notify + Destruct File, go to the Email Notification page to configure the email notification settings. See **Configuring Email Notification, page 307**.
POP3 Email Attachments	**None:** No action is required when viruses are detected. **Notify:** Send the original email and an alert email to the email receiver when viruses are detected in email attachments. **Notify + Destruct File:** Delete the infected files and send the original email and an alert email to the email receiver when viruses are detected in email attachments. **NOTE:** If you choose Notify or Notify + Destruct File, go to the Email Notification page to configure the email notification settings. See **Configuring Email Notification, page 307**.
IMAP Email Attachments	**None:** No action is required when viruses are detected. **Destruct File:** Delete the infected files when viruses are detected in email attachments.
NETBIOS/ CIFS	**None:** No action is required when viruses are detected. **Drop Connection:** Drop the connection when viruses are detected.

STEP 5 In the **Update Virus Database** area, specify how to update the Anti-Virus signatures. You can automatically check for signature updates from Cisco's signature server every 24 hours or manually check for signature updates at any time by clicking **Update**. See **Updating Anti-Virus Signatures, page 308**.

STEP 6 Click **Save** to apply your settings.

Configuring Advanced Anti-Virus Settings

Use the Advanced Settings page to configure the scan settings.

STEP 1 Click **Security Services > Anti-Virus > Advanced Settings**.

STEP 2 **Maximum File Size to Scan:** Enter the maximum file size, from 0 to 10240 kilobytes. Files larger than this size are passed without scanning. Use the default setting, 0, to indicate that there is no limit on the file size.

NOTE: For compressed files, Anti-Virus will scan each file after decompression and bypass virus scanning for the files larger than the maximum file size.

STEP 3 For each protocol, make the desired selections:

- **HTTP:**
  - Check the **Optimize Performance** box to suspend the Anti-Virus scan for websites with a good reputation. Uncheck the box to scan all sites. This option is available only when Web Reputation Filtering is enabled. For more information, see **Configuring Web Reputation Filtering, page 325**.
  - Check the **Disable HTTP Resume** box to disable resuming web-based file transfer by using the HTTP protocol when viruses are detected. Uncheck the box to allow resuming web-based file transfers in this situation.
- **FTP:** Check the **Disable FTP Resume** box to disable resuming file transfer by using the FTP protocol when viruses are detected. Uncheck the box to enable resuming file transfers in this situation.

STEP 4 Click **Save** to apply your settings.

Configuring HTTP Notification

HTTP Notification informs users that viruses are detected in web pages or in files that they try to access. Use the HTTP Notification page to customize the notification message that will be sent to the user when viruses are detected.

STEP 1 Click **Security Services > Anti-Virus > HTTP Notification**.

STEP 2 Enter the alert message in the **Notification Content** field.

- If you select Notify as the action for the HTTP protocol, the alert message is sent to the user.
- If you select Notify + Drop Connection as the action for the HTTP protocol, the connection is dropped and the alert message is sent to the user.

STEP 3 Click **Save** to apply your settings.

Configuring Email Notification

Email Notification allows you to send an alert email to the email receiver when viruses are detected in email attachments. Use the Email Notification page to customize the tag and notification message that are displayed in the alert email.

STEP 1 Click **Security Services > Anti-Virus > Email Notification**.

The Email Notification window opens. The following information is displayed:

- **Email Notification Status:** Shows if the Notify or Notify + Destruct File action is enabled or disabled for the SMTP or POP3 protocol.
  - If you choose Notify as the preventive action, the original email and an alert email are sent to the email receiver.
  - If you choose Notify + Destruct File as the preventive action, the infected files are deleted and the original email and an alert email are sent to the email receiver.
- **From Email Address:** The email address used to send the alert email.
- **SMTP Server:** The IP address or Internet name of the SMTP server.
- **SMTP Authentication:** Shows if the SMTP authentication is enabled or disabled.

NOTE: The above email server settings are read only. They are used to send the alert email to the original email receiver. You can click the **Edit** link to configure the email server settings, but save your settings on this page first. See Configuring Email Alert Settings, page 408.

STEP 2 If the Email Notification feature is enabled and the email server settings are configured, enter the following information:

- **Mail Tag:** Enter the tag that shows in the alert email's subject. The tag will insert to the alert email subject in the **[Tag] Email Subject** format.
- **Mail Content:** Enter the notification content that appears in the alert email.

STEP 3 Click **Save** to apply your settings.

Updating Anti-Virus Signatures

You can automatically check for Anti-Virus signature updates from Cisco's signature server every 24 hours or to manually check for Anti-Virus signature updates at any time by clicking **Update**. When a newer signature file is available on the server, the new signature file will be downloaded to your device.

NOTE A valid Cisco.com account is required to check for signature updates from Cisco's signature server. Go to the Device Management > Cisco Services & Support > Cisco.com Account page or click the **Edit Cisco.com Account Settings** link to configure your Cisco.com account credentials on the security appliance. See Configuring Cisco.com Account, page 424.

STEP 1 Click **Security Services > Anti-Virus > General Settings**.

STEP 2 In the **Update Virus Database** area, you can view the status of the Anti-Virus signature file. The following information is displayed:

- **Last Check:** The date and time of your last check.
- **Last Update:** The date and time of the last successful update.
- **Version:** The version number of the Anti-Virus signature file.
- **Virus Pattern Number:** The total amount of virus patterns in the Anti-Virus signature file.

STEP 3 To automatically update the Anti-Virus signatures, perform the following steps:

a. In the **Auto Update Virus Database** area, click **On** to automatically check for signature updates from Cisco's signature server every 24 hours.

b. Click **Save** to apply your settings.

STEP 4 To manually update the Anti-Virus signatures at any time, click **Update** to check for signature updates from Cisco's signature server immediately.

You can also click **Check for Updates Now** from the Security Services > Dashboard page to manually update the Anti-Virus signatures.

Configuring Application Control

Application Control monitors traffic through the Cisco ISA500 to permit or block traffic for individual applications and categories of applications. For some applications, you can permit or block certain features or functions of the application.

Important: Read the information in this guide to understand the features, required tasks, and recommendations before you implement this service.

To configure Application Control, refer to the following topics:

- **Configuring Application Control Policies, page 310**
- **General Application Control Settings, page 314**
- **Advanced Application Control Settings, page 318**

To configure reporting and email alerts, see these topics:

- **Viewing Application Control Report, page 301**
- **Configuring Email Alert Settings, page 408**

To ensure that Application Control can identify the latest applications, see **Updating Application Signature Database, page 317**.

Configuring Application Control Policies

Use the Application Control Policies page to configure the application control policies. An application control policy allows you to permit or block traffic for the applications by schedule.

Important Tips:

- Be aware that the Cisco ISA500 can control access only for the traffic that it handles. For example, if a PC and a server are directly connected to the LAN ports of the Cisco ISA500, Application Control policies apply to the traffic between these devices. However, if a switch is uplinked to the Cisco ISA500, the security appliance does not handle the traffic through the ports of that switch and therefore the Application Control policies do not apply.
- Application Control uses signatures to identify and block the applications. You must update the application signatures frequently so that Application Control can identify the latest applications. See **Updating Application Signature Database, page 317**.

Refer to the following topics:

- **General Application Control Policy Settings, page 310**
- **Adding an Application Control Policy, page 311**
- **Permitting or Blocking Traffic for all Applications in a Category, page 312**
- **Permitting or Blocking Traffic for an Application, page 313**

General Application Control Policy Settings

STEP 1 Click **Security Services > Application Control > Application Control Policies**.

STEP 2 You can perform the following actions:

- Click **Add Policy** to add a new application control policy. See **Adding an Application Control Policy, page 311**.
- Click the **Edit** (pencil) icon to edit an existing application control policy.
- Click the **Duplicate** icon to create a copy of an existing application control policy. This feature allows you to make a minor change for an existing application control policy to create a new policy.

- Click the **Delete** (x) icon to delete an existing application control policy. The default application control policy cannot be deleted.

STEP 3 Click **Save** to apply your settings.

Adding an Application Control Policy

An application control policy is used to permit or block traffic for the applications by schedule.

NOTE Up to 80 custom application control policies can be configured on the security appliance. Up to 8 application control policies can be applied to each zone.

STEP 1 Click **Add Policy** to create a new application control policy.

The Policy Profile - Add/Edit window opens.

STEP 2 Enter the following information:

- **Policy Name:** Enter the name for the application control policy.
- **Schedule:** Choose **Always on** to keep the application control policy always active or choose a schedule to permit or block the applications at a specific time of a day or at the specified days of a week. If the schedule that you want is not in the list, choose **Create a new schedule** to add a new schedule object. To maintain the schedules, go to the Device Management > Schedules page. See Configuring Schedules, page 449.

STEP 3 The security appliance supports a long list of applications. You can use the table filter settings to filter the applications and then specify the settings for the selected applications.

- **Category:** Allows you to filter the applications by category. Choose **All** to display all categories in the table or choose a category to only display the applications that belong to the selected category. You can click the triangle next to a category to expand or contract all applications in the category.
- **Application:** Allows you to filter the application by application name. Enter the name of the application in the field. Only the application that you specified is displayed in the table.
- **Current Action:** Allows you to filter the applications by action. Choose **Deny** to display all applications that are blocked or choose **Permit** to display all applications that are permitted.

NOTE: By default, the table filter settings are hidden. You can click the triangle next to **Hide Table Filter Settings** to display or hide the table filter settings.

STEP 4 After you set the table filter settings, click **Refresh Table** to refresh the data in the table. Only the applications that you specified are displayed in the table.

STEP 5 Specify the preventive action for a single application or for all applications in a category:

- To permit or block traffic for all applications in a category, click the **Edit** (pencil) icon in the **Configure** column for the category. For complete details, see **Permitting or Blocking Traffic for all Applications in a Category, page 312**.
- If the action, schedule, or logging settings vary among the applications in a category, you can configure the settings for each application in the category. You must first choose **keep application-level settings** for the Action and Logging options of the category, and then click the **Edit** (pencil) icon in the **Configure** column for the application. For complete details, see **Permitting or Blocking Traffic for an Application, page 313**.

STEP 6 Click **OK** to save your settings.

Permitting or Blocking Traffic for all Applications in a Category

This section describes how to configure the category default settings. The category default settings are applied to all applications in a category.

STEP 1 Click the **Edit** (pencil) icon in the **Configure** column for a category.

The Policy Profile - Add/Edit window opens.

STEP 2 Specify the category default settings:

- **Category:** The name of the category.
- **Action:** Choose **Permit** to permit traffic, or choose **Deny** to block traffic. If the action settings vary among the applications in the category, you must first choose the **keep application-level settings** option, and then configure the action for each application in the category. See **Permitting or Blocking Traffic for an Application, page 313**.

- **Logging:** Choose **Enable** to log the event when an application is blocked, or choose **Disable** to disable the logging feature. If the logging settings vary among the applications in a category, you must first choose the **keep application-level settings** option, and then configure the logging settings for each application in the category. See **Permitting or Blocking Traffic for an Application, page 313**.

  To log application blocking events, you must enable the logging settings for the applications, and then go to the Device Management > Logs pages to configure the log settings and the log facilities. See Log Management, page 442.

  - To save application blocking logs to the local syslog daemon, you must enable the Log feature, set the log buffer size and the severity for local logs, and enable the Local Log settings for the Application Control facility.
  - To save application blocking logs to the remote syslog server if you have a remote syslog server support, you must enable the Log feature, specify the Remote Log settings, and enable the Remote Log settings for the Application Control facility.

  NOTE: Changing the category default settings will override the application-level settings for all applications in the category.

STEP 3 Click **OK** to save your settings.

Permitting or Blocking Traffic for an Application

If the action, schedule, or logging settings vary among the applications in a category, you can configure the action and logging settings for each application in the category. The application-level settings are applied to a single application in a category.

NOTE To edit the settings for an application with detection disabled, you must first enable the detection from the Advanced Settings page.

NOTE Before you configure the application-level settings for each application in a category, make sure that you choose **keep application-level settings** for the Action and Logging options of the category.

STEP 1 Click the **Edit** (pencil) icon in the **Configure** column for an application.

The Policy Profile - Add/Edit window opens.

STEP 2 Specify the application-level control settings:

- **Application:** The name of the application.
- **Action:** Choose **Permit** to permit traffic for the application or choose **Deny** to block traffic for the application.
- **Logging:** Choose **Enable** to log the event when an application is blocked, or choose **Disable** to disable the logging function.

  To log application blocking events, you must first enable the logging settings for the applications, and then go to the Device Management > Logs pages to configure the log settings and the log facilities. See Log Management, page 442.
- **Configure feature-specific access control:** For some applications, you can permit or block certain features or functions of the application. For example, for Google Talk application, you can permit the chat function but block the media transfer function. Check this box and then specify the action for each feature or function of the application.

  NOTE: When the action for a specified feature or function is set to “Deny,” it will no longer function.

STEP 3 Click **OK** to save your settings.

General Application Control Settings

Use the Application Control Settings page to enable the Application Control feature, apply the application control policies to different zones, and update the application signature database.

Important Tips:

- Be aware that the Cisco ISA500 can control access only for the traffic that it handles. For example, if a PC and a server are directly connected to the LAN ports of the Cisco ISA500, Application Control policies apply to the traffic between these devices. However, if a switch is uplinked to the Cisco ISA500, the security appliance does not handle the traffic through the ports of that switch and therefore the Application Control policies do not apply.
- You must update the application signatures frequently so that Application Control can identify the latest applications.

Refer to the following topics:

Enabling Application Control Service

STEP 1 Click **Security Services > Application Control > Application Control Settings**.

STEP 2 Click **On** to enable the Application Control feature, or click **Off** to disable it. If you enable Application Control, by default all applications are allowed unless specifically blocked by an application control policy.

STEP 3 Click **Save** to apply your settings.

Mapping Application Control Policies to Zones

You can apply different application control policies to different zones. You can have multiple policies within a given zone for a different set of users. By default, the default application control policy that permits traffic for all applications is selected to all zones.

STEP 1 Click **Security Services > Application Control > Application Control Settings**.

STEP 2 In the **Zone Mapping** area, you can perform the following actions:

- Click the triangle next to a zone to expand or contract the application control policy mapping rules of the selected zone.
- Click **Add Mapping Rule** to add a new application control policy mapping rule. See **Configuring Application Control Policy Mapping Rules, page 316**.
- Click the **Edit** (pencil) icon to edit an existing application control policy mapping rule.
- Click the **Delete** (x) icon to delete an application control policy mapping rule. The default application control policy mapping rule for each zone cannot be deleted.

- Re-order the priorities of multiple application control policy mapping rules within a given zone. To move the rule up one position, click the **Move up** icon. To move the rule down one position, click the **Move down** icon. The default application control policy mapping rule must be the last policy with the lowest priority for a zone.

STEP 3 Click **Save** to apply your settings.

Configuring Application Control Policy Mapping Rules

An application control policy mapping rule applies a specific application control policy to a given zone to control application traffic from and to the zone. You can also apply a selected application control policy to a different set of users.

For example, you can control outgoing and incoming traffic to a given zone for a specific host or for the hosts within a specific IP range.

NOTE Make sure that you have configured the application control policies before you configure the policy mapping rules. See **Configuring Application Control Policies, page 310**.

STEP 1 Click **Add Mapping Rule** to add a new application control policy mapping rule.

The Application Control Policy Mapping - Add/Edit window opens.

STEP 2 Enter the following information:

- **Zone:** Choose an existing zone to control application traffic from and to the selected zone. This mapping rule will be listed under the selected zone.
- **Policy:** Choose an existing application control policy to apply the selected policy to the zone.
- **Matching Condition:** You can apply the selected application control policy to all users, a specific host, or the hosts within a specific IP range. Choose one of the following options:
  - **All IP Addresses and Users:** Applies the selected application control policy to all users.
  - **Specific IP Address Object:** Applies the selected application control policy to a specific host or to the hosts within a specific IP range. Traffic for the specific host or for the hosts within the IP range will be detected. Traffic for other users will be bypassed. The IP address object can be a host or a range of IP addresses. If the address object that you want is not

in the list, choose **Create a new address** to create a new address object. To maintain the address objects, go to Networking > Address Management page. See **Address Management, page 175**.

STEP 3 Click **OK** to save your settings.

Updating Application Signature Database

Application Control uses signatures to identify and block the applications. You must update the application signatures frequently so that Application Control can identify the latest applications. You can automatically check for signature updates from Cisco's signature server on a weekly basis or manually check for signature updates at any time by clicking **Check for Update Now**. If a newer signature file is available on the server, the new signature file will be automatically downloaded to your device.

You can also first download the latest signature file from Cisco's signature server to your local PC, and then manually update the application signatures through the Configuration Utility.

A valid Cisco.com account is required to check for signature updates from Cisco's signature server. Go to the Device Management > Cisco Services & Support > Cisco.com Account page to configure your Cisco.com account credentials on the security appliance. See Configuring Cisco.com Account, page 424.

NOTE Application Control and IPS use the same signature database. Updating the application signatures will also update the IPS signatures at the same time.

STEP 1 Click **Security Services > Application Control > Application Control Settings**.

STEP 2 In the **Update Signature Database** area, the following information is displayed:

- **Last Check:** The date and time of the last check.
- **Last Update:** The date and time of the last successful update when the signature file is updated successfully.
- **Version:** The version number of the application signature file that is currently used on the security appliance.

STEP 3 To automatically update the application signatures, perform the following steps:

a. In the **Auto Update** area, click **On** to automatically check for signature updates from Cisco's signature server every Monday at 00:00.

b. Click **Save** to apply your settings.

STEP 4 To manually update the application signatures at any time, click **Check for Update Now** to check for signature updates from Cisco's signature server immediately.

You can also click **Check for Updates Now** from the Security Services > Dashboard page to manually update the application signatures.

STEP 5 To manually update the application signatures from your local PC, perform the following steps:

a. You must first download the application signature file from Cisco's signature server to your local PC.

b. In the **Manually Update Signature Database** area, click **Browse** to locate and select the signature file from your local PC.

c. Click **Update Database**.

Advanced Application Control Settings

Use the Application Control Advanced Settings page to enable or disable the detection for each application.

STEP 1 Click **Security Services > Application Control > Application Control Advanced Settings**.

The Application Control Advanced Settings window opens.

STEP 2 The security appliance supports a long list of applications. You can use the table filter settings to filter the applications in the table and then specify the detection settings for all selected applications:

- **Category:** Allows you to filter the applications by category. Choose the category that you want from the drop-down list. Only the applications that belong to the selected category are displayed. You can click the triangle next to a category to expand or contract all applications under the category.
- **Application:** Allows you to filter the application by application name. Enter the name of the application in the field. Only the application that you specified is displayed in the table.
- **Detection:** Allows you to filter the applications by detection status. Choose **Enable** to display all applications with detection enabled or choose **Disable** to display all applications with detection disabled.

NOTE: By default, the table filter settings are hidden. You can click the triangle next to **Show Table Filter Settings** to display or hide the table filter settings.

STEP 3 After you set the table filter settings, click **Refresh Table** to refresh the data in the table.

STEP 4 You can enable or disable the detection for the selected applications in the table. In the **Detection** column, choose **Enable** to enable the detection for an application or choose **Disable** to disable the detection for an application.

STEP 5 Click **Save** to apply your settings.

Configuring Spam Filter

Spam Filter detects the email sender's reputation score. The reputation scores range from -10 (bad) to +10 (good). An email is classified as spam if the sender's reputation is below the spam threshold, or is classified as suspected spam if the sender's reputation is between the spam threshold and suspected spam threshold. An email is not classified as spam if the sender's reputation is above the suspected spam threshold.

Spam Filter detects spam emails based on the reputation score of the sender's IP address. The sender's address is the address of the host that connects to the SMTP server to deliver an email message, not an address within the email header.

STEP 1 Click **Security Services > Spam Filter**.

STEP 2 Click **On** to enable Spam Filter, or check **Off** to disable it.

STEP 3 If you enable Spam Filter, enter the following information:

- **SMTP Server Address/Domain:** Enter the IP address or domain name of your internal SMTP server. The SMTP server must have its Internet traffic routed through the security appliance. The SMTP server or the clients that use this SMTP server can be configured to respond to the spam and suspected spam tags that the security appliance applies to the email.
- **Action when Spam Detected:** Choose **Block Email** to block the email, or choose **Tag Email with [Spam]** to get the email tagged with [Spam].

- **Action when Suspect Spam Detected:** Choose **Block Email** to block the email, or choose **Tag Email with [Suspect Spam]** to get the email tagged with [Suspect Spam].
- **Reputation Threshold:** Specify the block sensitivity as Low, Medium, or High, or as a numerical threshold (Custom).
  - **Low:** Blocks less spam with lowest risk of false positives. The threshold value for spam is -4 and the threshold value for suspected spam is -2.
  - **Medium:** Blocks more spam with moderate risk of false positives. The threshold value for spam is -3 and the threshold value for suspected spam is -1.
  - **High:** Blocks most spam with increased risk of false positives. The threshold value for spam is -2 and the threshold value for suspected spam is -0.5.
  - **Custom:** Manually set the spam reputation threshold. When the Custom radio button is selected, choose the threshold values for spam and suspected spam. The allowable values for the threshold are integers from -10 to -1 and the value -0.5.

STEP 4 In the **Allowed Senders** area, you can specify the email sender exceptions against your Spam Filter settings. Traffic from the specified hostnames or IP addresses will not be examined by Spam Filter.

- To add an exception, enter the hostname or IP address of the sender in the **Hostname/IP Address** field and click **Add**.
- To remove an exception, select it from the list of **Allowed Senders** and click **Remove**.

STEP 5 In the **Service Outage** area, choose one of the following actions when Spam Filter is unavailable:

- **Do Not Accept Emails when spam reputation services are not available:** All emails are delayed until Spam Filter is available.
- **Accept Emails even when spam reputation services are not available:** All emails are delivered without checking for spam.

STEP 6 Click **Save** to apply your settings.

Configuring Intrusion Prevention

Intrusion Prevention System (IPS) is a network-based platform that inspects network traffic for malicious or unwanted activity such as worms, spyware, and policy violations. When IPS detects a threat, it reacts in real-time by taking actions such as blocking or dropping connections, logging the detected activities, and sending notifications about these activities. You can use the default actions for each signature or customize the actions to suit your requirements.

IMPORTANT: IPS uses signatures to identify the attacks in progress. You must update the IPS signatures frequently to keep the protection current. See **Updating IPS Signature Database, page 324**.

After setting up IPS, you have these options for monitoring the activity:

- Enable the IPS report from the Security Services > Security Services Reports page or from the Status > Security Services Reports page to see the number of packets detected and the number of packets dropped by IPS. See **Viewing IPS Report, page 300**.
- Enable the IPS Alert feature to send an alert email to a specified email address if an attack is detected by IPS. See Configuring Email Alert Settings, page 408.

NOTE You must install licenses on the License Management page before you can configure IPS.

STEP 1 Click **Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection**.

The IPS Policy and Protocol Inspection window opens.

STEP 2 At the top of the page, enable or disable IPS by clicking **On** or **Off**.

STEP 3 In the **Zone** area, chose the zones to be inspected. IPS inspects inter-zone traffic only.

- **To add a zone:** In the Zones Available list, click a zone, and then click **Add** to move it to the Selected Zones list. All incoming and outgoing traffic for the selected zones is inspected.
- **To remove a zone:** In the Selected Zones list, click a zone, and then click **Remove** to move it to the Zones Available list.

NOTE: You can block an intrusion based on the source zones or based on the destination zones. For example, if you select the LAN and DMZ zones, IPS inspects all traffic for the LAN and DMZ zones regardless of its source. Traffic between LAN and DMZ is inspected once, not twice. If you select the WAN zone, IPS inspects all traffic for the WAN zone regardless of its destination.

STEP 4 In the **IPS Signature** area, use the options below to filter the list of signatures in the Selected Signature table. The unfiltered list includes thousands of IPS signatures that are used to identify attacks. After selecting filters, click **Refresh** to redisplay the Selected Signature table showing only the matching signatures.

- **Severity Level:** Choose a severity level, from highest to lowest: Critical, High, Medium, Low, and Information.
- **Operating System Type:** Choose **All** to include all signatures regardless of the type of operating system, or choose **Selected OS Types Only** to include only the signatures that match the specified types of operation systems.
- **Host Type:** Choose a host type.
- **Category:** Choose **All** to include all signatures regardless of the category, or choose **Selected Categories Only** to include only the signatures that match the specified categories.

The Selected Signature table displays this information:

- **Name:** The name of the signature.
- **ID:** The unique identifier of the signature. To view complete details for a signature, click the link in the ID column.
- **Severity:** The severity level of the threat that the signature can identify.
- **Category:** The category that the signature belongs to.
- **Default Action:** The default preventive action for the signature.
  - **Block and Log:** Deny the request, drop the connection, and log the event when a signature is detected by the IPS engine.
  - **Log Only:** Only log the event when a signature is detected by the IPS engine.
- **Current Action:** The current preventive action for the signature.
- **Edit Action:** Click the pencil icon to enable, disable, or set the preventive actions for a signature. For more information, see **Configuring Signature Actions, page 323**.

NOTE: For ease of use, you can edit the preventive actions for a group of signatures. Check the box for each signature that you want to change, or select all signatures by checking the box in the top left corner of the table. To edit the settings for the selected signatures, click the **Edit** (pencil) icon at the top of the table.

- **Block Threshold:** Specify a threshold at which blocking occurs; whether the Current Action is to block and log or to log only, traffic is blocked after the specified number of occurrences. Enter 0 to apply the Current Action immediately upon detection.

  NOTE: The counter is reset to 0 whenever IPS settings are saved in the configuration utility or the security appliance is rebooted.

STEP 5 Click **Save** to apply your settings.

Configuring Signature Actions

After selecting one or more signatures on the Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection page, use the Edit Selected Signature Actions page to enable or disable the selected signatures and to configure the actions.

STEP 1 Enter the following information:

- **Enable detection of selected signatures:** Check this box to enable the intrusion detection for this signature, or uncheck this box to disable it.
- **Name:** The name of the signature.
- **ID:** The unique identifier of the signature.
- **Severity:** The severity level of the threat that the signature can identify.
- **Default Action:** The default preventive action for the signature.
- **Action on Detect:** Choose one of the following actions for the signature:
  - **Block and Log:** Deny the request, drop the connection, and log the event when the security signature is detected by the IPS engine.
  - **Log only:** Only log the event when the security signature is detected by the IPS engine. This option is mostly used for troubleshooting purposes.

To log IPS events, you must first specify the action for the signatures, and then go to the Device Management > Logs pages to configure the log settings and log facilities. See Log Management, page 442.

To save IPS logs to the local syslog daemon, you must enable the Log feature, set the log buffer size and the severity for local logs, and then enable the Local Log settings for the Intrusion Prevention (IPS) facility.

To save IPS logs to a remote syslog server, you must enable the Log feature, specify the Remote Log settings, and enable the Remote Log settings for the Intrusion Prevention (IPS) facility.

STEP 2 Click **OK** to save your settings.

STEP 3 Click **Save** to apply your settings.

Updating IPS Signature Database

You can automatically check for signature updates from Cisco's signature server on a weekly basis or manually check for signature updates at any time by clicking **Check for Update Now**. If a newer signature file is available, the new signature file will be automatically downloaded to your device.

You can also first download the latest signature file from Cisco's signature server to your local PC, and then manually update the IPS signatures through the Configuration Utility.

A valid Cisco.com account is required to check for signature updates and download the IPS signature file from Cisco's signature server. Go to the Device Management > Cisco Services & Support > Cisco.com Account page to configure your Cisco.com account credentials on the security appliance. See **Configuring Cisco.com Account, page 424**.

NOTE IPS and Application Control use the same signature database. Updating the IPS signatures will also update the application signatures at the same time.

STEP 1 Click **Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection**.

The IPS Policy and Protocol Inspection window opens.

STEP 2 In the **Automatic Update Signature Database** area, the following information is displayed:

- **Last Check:** The date and time of the last check.
- **Last Update:** The date and time of the last successful update when the signature file is updated successfully.
- **Version:** The version number of the IPS signature file that is currently used on the security appliance.

STEP 3 To automatically update the IPS signatures, perform the following steps:

a. In the **Auto Update** area, click **On** to automatically check for signature updates from Cisco's signature server every Monday at 00:00.

b. Click **Save** to apply your settings.

STEP 4 To manually update the IPS signatures at any time, click **Check for Update Now** to check for signature updates from Cisco's signature server immediately.

You can also click **Check for Updates Now** from the Security Services > Dashboard page to manually update the IPS signatures.

STEP 5 To manually update the IPS signatures from your local PC, perform the following steps:

a. You must first download the signature file from Cisco's signature server to your local PC.

b. In the **Manually Update Signature Database** area, click **Browse** to locate and select the signature file from your local PC.

c. Click **Update Database**.

Configuring Web Reputation Filtering

Web Reputation Filtering prevents client devices from accessing dangerous websites containing viruses, spyware, malware, or phishing links. Web Reputation Filtering detects the web threats based on the reputation score of a web page. Reputation scores range from -10 (bad) to +10 (good). Web pages with reputation scores below a specific threshold are considered threats and blocked.

Web Reputation Filtering only monitors and controls the website visits through the specified HTTP port. Go to the Security Services > Web URL Filtering > Advanced Settings page to view or specify the HTTP port. See **Configuring Advanced Web URL Filtering Settings, page 330**.

You can create a “white list” of trusted sites by adding up to 256 Allowed Web Sites. The specified websites will not be examined by Web Reputation Filtering.

STEP 1 Click **Security Services > Web Reputation Filtering**.

STEP 2 Click **On** to enable Web Reputation Filtering, or click **Off** to disable it.

STEP 3 Specify the block sensitivity as Low, Medium, or High, or as a numerical threshold (Custom). The threshold values for Low, Medium, or High are predefined and cannot be edited.

- **Low:** Blocks fewer web threats. The threshold value is -6.
- **Medium:** Blocks more web threats. The threshold value is 5.
- **High:** Blocks most web threats. The threshold value is -4.
- **Custom:** Manually set the web reputation threshold. After selecting this option, choose a threshold value from -10 to -0.5.

Note: The rate of false positives increases as the threshold approaches 0.

STEP 4 In the **Allowed Web Sites** area, you can specify the website exceptions against your Web Reputation Filtering settings. The specified websites will not be examined by Web Reputation Filtering. You can include up to 16 websites on this list.

- To add a website exception, enter the following information:
  - **Matching Domain:** Allows you to permit the HTTP access of a website that fully matches a specific domain name. If you choose this option, enter the domain name, not including http://, in the **Site URL** field and then click **Add**.
  - **Containing Keyword:** Allows you to permit the HTTP access of a website that contains a specific keyword. If you choose this option, enter the URL keyword, not including http://, in the **Site URL** field and then click **Add**.
- To remove a website exception, select it from the list of **Allowed Sites** and click **Remove**.

STEP 5 In the **Service Outage** area, you can specify how to deal with web traffic when Web Reputation Filtering is unavailable. Choose one of the following actions:

- **Block Web Traffic when web reputation filter services are not available:** All web traffic is blocked until Web Reputation Filtering is available. The default block page will be displayed when a web page is blocked. The message that you specify in the **Blocked Web Filter Message** field will show on the default block page.
- **Allow Web Traffic even when web reputation filter services are not available:** All web traffic is allowed until Web Reputation Filtering is available.

STEP 6 Click **Save** to apply your settings.

Configuring Web URL Filtering

Web URL Filtering allows you to block HTTP access to malicious websites based on URL categories. You can allow or block an entire URL category to make configuration simpler. You can also specify the website exceptions against the URL category settings. For example, you can block the websites that Web URL Filtering usually allows, or allow the websites that Web URL Filtering usually blocks.

You can enable Web URL Filtering Alert to send email alerts to a specific email address when web URL categories have any changes. See Configuring Email Alert Settings, page 408.

Web URL Filtering only monitors and controls the website visits through the HTTP port specified on the Web URL Filtering > Advanced Settings page.

Refer to the following topics:

- **Configuring Web URL Filtering Policy Profiles, page 328**
- **Configuring Website Access Control List, page 329**
- **Mapping Web URL Filtering Policy Profiles to Zones, page 330**
- **Configuring Advanced Web URL Filtering Settings, page 330**

Configuring Web URL Filtering Policy Profiles

A Web URL Filtering policy profile is used to specify which URL categories are blocked or allowed.

NOTE Up to 256 Web URL Filtering policy profiles can be configured on the security appliance.

STEP 1 Click **Security Services > Web URL Filtering > Policy Profile**.

STEP 2 To add a new Web URL Filtering policy profile, click **Add**.

Other Options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. The default profile cannot be deleted.

The Policy Profile - Add/Edit window opens.

STEP 3 Enter the following information:

- **Policy Name:** Enter the name for the policy profile.
- **Description:** Enter a brief description for the policy profile.
- **Select URL Categories to Block:** Check an URL category to block it, or uncheck this box to permit it. If an URL category is blocked (or permitted), all websites that belong to this category are blocked (or permitted).

STEP 4 Specify the website exceptions if needed. The website exceptions allow you to permit or block specific websites against the URL category settings. All website exceptions can be added to the website access control list. The website access control list has higher priority than the URL category settings. See **Configuring Website Access Control List, page 329**.

For example, if the Sports and Recreation category is blocked, but you want to permit the website: www.espn.com, you can add it to the website access control list as an exception.

STEP 5 Click **Save** to apply your settings.

Configuring Website Access Control List

Blocking an URL category will block all websites that belong to this category. You can specify the website exceptions in the website access control list. The website exceptions will override the URL category settings in the same profile.

NOTE Up to 32 website exceptions can be configured for each Web URL Filtering policy profile.

STEP 1 In the **Specify URLs or URL keywords you want to permit or deny** area, click **Edit**.

The Policy Profile - Add/Edit window opens.

STEP 2 To add a website access rule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete all entries, click **Delete All**.

The Website Access Control Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Enable Content Filter URL:** Click **On** to enable the website access rule, or click **Off** to create only the website access rule.
- **URL:** Enter the domain name or URL keyword of a website that you want to permit or block.
- **Match Type:** Specify the method for applying this rule:
  - **Domain:** Permit or deny the HTTP access of a website that fully matches the domain name that you entered in the **URL** field.

    For example, if you enter yahoo.com in the URL field, then it can match the website http://yahoo.com/*, but cannot match the website http://*.yahoo.com.uk/*.
  - **URL Keyword:** Permit or deny the HTTP access of a website that contains the keyword that you entered in the **URL** field.

    For example, if you enter yahoo in the URL field, then it can match the websites such as www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk, and www.yahoo.co.jp.
- **Action:** Choose **Permit** to permit access, or choose **Block** to block access.

STEP 4 Click **OK** to save your settings.

Mapping Web URL Filtering Policy Profiles to Zones

Use the Policy to Zone Mapping page to apply the Web URL Filtering policy profile to each zone. The Web URL Filtering policy assigned to each zone determines whether to block or forward the HTTP requests from the hosts in the zone. By default, Default Profile that permits all URL categories is assigned to all predefined zones and new zones.

STEP 1 Click **Security Services > Web URL Filtering > Policy to Zone Mapping**.

The Policy to Zone Mapping window opens.

STEP 2 Click **On** to enable Web URL Filtering, or click **Off** to disable it.

NOTE: Enabling Web URL Filtering will disable Firewall Content Filtering and vice-versa.

STEP 3 In the **Zone Policy Map** area, choose a Web URL Filtering policy for each zone.

STEP 4 Click **Save** to apply your settings.

Configuring Advanced Web URL Filtering Settings

STEP 1 Click **Security Services > Web URL Filtering > Advanced Settings**.

STEP 2 Enter the following information:

- **Filter Traffic on HTTP port:** Enter the port number that is used for filtering HTTP traffic. Web URL Filtering only monitors and controls the website visits through this HTTP port. The default value is 80.
- **Filter Traffic on HTTPS port:** Enter the port number that is used for filtering HTTPS traffic. Web URL Filtering only monitors and controls the website visits through this HTTPS port. The default value is 443.
- **Blocked Web Components:** You can block or permit the web components like Proxy, Java, ActiveX, and Cookies. By default, all of them are permitted.

- **Proxy:** Check this box to block proxy servers, which can be used to circumvent certain firewall rules and thus present a potential security gap.
- **Java:** Check this box to block Java applets that can be downloaded from pages that contain them.
- **ActiveX:** Check this box to prevent ActiveX applets from being downloaded through Internet Explorer.
- **Cookies:** Check this box to block cookies, which typically contain sessions.

STEP 3 Choose one of the following actions when Web URL Filtering is unavailable:

- **Block Web Traffic when web URL filter services are not available:** All web traffic is blocked until Web URL Filtering is available.
- **Allow Web Traffic even when web URL filter services are not available:** All web traffic is allowed until Web URL Filtering is available.

STEP 4 Choose one of the following actions when a web page is blocked:

- **Display Blocked URL Message when the requested page is blocked:** Displays the default block page when a web page is blocked. If you choose this option, the message that you specify in the **Blocked URL Message** field will show on the default block page.
- **Redirect URL:** Redirects to a specified web page when a web page is blocked. If you choose this option, enter a desired URL to be redirected. Make sure that the specified URL is allowed by the Website Access Control List.

STEP 5 Click **Save** to apply your settings.

Network Reputation

Network Reputation blocks incoming traffic from IP addresses that are known to initiate attacks throughout the Internet. Network Reputation checks the source and destination addresses of each packet against the address blacklist to determine whether to proceed or to drop the packet. The blacklist data is automatically updated every six hours. You can click **Check for Updates Now** on the Security Services > Dashboard page to immediately check for new updates for Network Reputation.

NOTE No configuration is needed for Network Reputation. You only need to enable or disable this feature from the Security Services > Dashboard page.