Application Security

Application Security allows you to create security policies to govern the use of network and web applications. You can apply the policies that you create to specific interfaces, clone an existing policy to leverage the settings for a new policy, and remove policies from the router.

This chapter contains the following sections:

- Application Security Windows
- No Application Security Policy
- E-mail
- Instant Messaging
- Peer-to-Peer Applications
- URL Filtering
- HTTP
- Applications/Protocols
- Timeouts and Thresholds for Inspect Parameter Maps and CBAC

Application Security Windows

The controls in the Application Security windows allow you to associate policies with interfaces, make global settings, and add, delete and clone application security policies. The application security drawers enable you to quickly navigate to the application security area in which you need to make changes.
Policy Name List

Select the policy that you want to modify from this list. If no policies are configured, this list is empty, and the Application Security window displays a message that indicates no policies are available on the router. To create a policy, click the **Action** button, and choose **Add**.

Application Security Buttons

- **Action** button—Click to add a policy, delete the chosen policy, or clone the chosen policy. If no policies are configured on the router, **Add** is the only action available.
- **Associate** button—Click to display a dialog that allows you to associate the policy with an interface. The dialog enables you to choose the interface, and to specify the traffic direction to which the policy is to apply.
- **Global Settings** button—Click to make settings to timeout and threshold values that apply to all policies. Click Global Settings for more information.

E-mail Drawer

Click to make changes to e-mail application security settings. Click **E-mail** for more information.

Instant Messaging Drawer

Click to make changes to security settings for Yahoo Messenger, MSN Messenger, and other instant messaging applications. Click **Instant Messaging** for more information.

Peer-to-Peer Drawer

Click to make changes to security settings for KaZa A, eDonkey, and other peer-to-peer applications. Click **Applications/Protocols** for more information.

URL Filtering Drawer

Click to add a list of URLs that you want the application security policy to filter. You can also add filtering servers.
HTTP Drawer

Click to make changes to HTTP security settings. Click HTTP for more information.

Applications/Protocols Drawer

Click to make changes to the security settings of other applications and protocols. Click Applications/Protocols for more information.

No Application Security Policy

Cisco SDM displays this window when you click the Application Security tab, but no Application Security policy is configured on the router. You can create a policy from this window, and view the global settings that provide default values for the parameters that you can set when you create policies.

Policy Name

Empty when no policy is configured for the router. Choosing Add from the Action context menu enables you to create a policy name and to begin to make settings for the policy.

Action

If no policy is configured on the router, you can choose Add from the context menu to create a policy. Once a policy is configured, the other actions, Edit and Delete, are available.

Associate

If no policy is configured this button is disabled. When a policy is created, you can click this button to associate the policy with an interface. See Associate Policy with an Interface for more information.
Global Settings

Global settings provide the default timeouts, thresholds, and other values for policy parameters. Cisco SDM provides defaults for each parameter, and you can change each value to define a new default that will apply unless overridden for a specific application or protocol. When you are creating a policy, you can accept the default value for a particular parameter, or choose another setting. Because the Application Security configuration windows do not display the default values you must click this button to view them in the Global Timeouts and Thresholds window. See Timeouts and Thresholds for Inspect Parameter Maps and CBAC for more information.

E-mail

Specify the e-mail applications that you want to inspect in this window. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Edit Button

Click to edit the settings for the chosen application. Settings that you create override the global settings configured on the router.

Applications Column

The name of the e-mail application, for example bliff, esmtp, and smtp. To edit the settings for an application, check the box to the left of the application name, and click Edit.

Alerts, Audit, and Timeout Columns

These columns display values that have been explicitly set for an application. If a setting is not changed for an application, the column is empty. For example, if auditing has been enabled for the bliff application, but no changes have been made to the alert or to the timeout settings, the value on is displayed in the Audit column, and the Alert and Timeout columns are blank.
Options Column

This column can contain fields if other settings for the chosen application exist.

MAX Data Field
Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure login Checkbox
Causes a user at a nonsecure location to use encryption for authentication.

Reset
Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic
Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Instant Messaging

Use this window to control the traffic for Instant Messaging (IM) applications such as Yahoo Messenger, and MSN Messenger. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action the router takes if it encounters traffic with the characteristics that you specify in this window.

The following example shows traffic blocked for Yahoo Messenger traffic, and alarms generated when traffic for that application arrives:

<table>
<thead>
<tr>
<th>App</th>
<th>Block</th>
<th>Send Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo Messenger</td>
<td></td>
<td>(checked)</td>
</tr>
</tbody>
</table>

The SDM_HIGH profile blocks IM applications. If the router uses the SDM_HIGH profile, and it does not block IM applications, those applications may have connected to a new server that is not specified in the profile. To enable
the router to block these applications, check the **Send Alarm** checkbox next to the IM applications to reveal the names of the servers to which the applications connect. Then, use the CLI to block traffic from these servers. The following example uses the server name newserver.yahoo.com:

```bash
Router(config)# appfw policy-name SDM_HIGH
Router(config-appfw-policy)# application im yahoo
Router(config-appfw-policy-ymsgr)# server deny name newserver.yahoo.com
Router(config-appfw-policy-ymsgr)# exit
Router(config-appfw-policy)# exit
Router(config)#
```

**Note**

- IM applications are able to communicate over nonnative protocol ports, such as HTTP, and through their native TCP and UDP ports. Cisco SDM configures block and permit actions based on the native port for the application, and always blocks communication conducted over HTTP ports.

- Some IM applications, such as MSN Messenger 7.0, use HTTP ports by default. To permit these applications, configure the IM application to use its native port.

---

**Peer-to-Peer Applications**

This page allows you to create policy settings for peer-to-peer applications such as Gnutella, BitTorrent, and eDonkey. To learn about the buttons and drawers available in the Application Security tab, click **Application Security Windows**.

Click **Permit, Block, and Alarm Controls** to learn how to specify the action that the router takes if it encounters traffic with the characteristics that you specify in this window.

The following example shows traffic blocked for BitTorrent traffic, and alarms generated when traffic for that application arrives:

**Example 8-1  Blocking BitTorrent Traffic**

```text
BitTorrent  Block
```
Note

- Peer-to-peer applications are able to communicate over nonnative protocol ports, such as HTTP, and through their native TCP and UDP ports. Cisco SDM configures block and permit actions based on the native port for the application, and always blocks communication conducted over HTTP ports.

- Application security policies will not block files if they are being provided by a paid service such as altnet.com. Files downloaded from peer-to-peer networks are blocked.

URL Filtering

URL filtering allows you to control user access to Internet websites by using URL lists. In these lists, you can specify whether a URL is to be permitted or denied. Include URL filtering capabilities in the Application Security policy by clicking Enable URL filtering in this window.

You can configure one local URL list on the router that is used for all Application Security policies. URL lists can also be stored on URL filter servers that the router can connect to. Information for these servers is stored in a URL filter server list. You can configure one URL filter server list on the router that is used for all Application Security policies.

The local URL list can be maintained in this window by using the Add URL, Edit URL, and Import URL list buttons. Because Cisco IOS software can maintain these lists with or without a configured Application Security policy, you can also maintain these lists in the Additional Tasks window.

To learn how to maintain a local URL list, click Local URL List.
To learn how to maintain the URL filter server list, click URL Filter Servers.
For information on how the router uses a local URL list in combination with URL lists on URL filter servers, click URL Filtering Precedence.
For general information about URL filtering, click URL Filtering Window.
HTTP

Specify general settings for HTTP traffic inspection in this window. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action that the router takes when it encounters traffic with the characteristics that you specify in this window.

For more detailed information about how the router can inspect HTTP traffic, see HTTP Inspection Engine at the following link:


Detect noncompliant HTTP traffic Checkbox

Check if you want Cisco SDM to examine HTTP traffic for packets that do not comply with the HTTP protocol. Use the Permit, Block, and Alarm controls to specify the action that the router takes when this type of traffic is encountered.

Note

Blocking noncompliant HTTP traffic can cause the router to drop traffic from popular websites that might not be blocked on the basis of content, if those websites do not conform to the HTTP protocol.

Detect tunneling applications Checkbox

Check if you want Cisco SDM to examine HTTP traffic for packets that are generated by tunneling applications. Use the Permit, Block, and Alarm controls to specify the action that you want Cisco SDM to take when it encounters this type of traffic.

Set maximum URI length inspection Checkbox

Check if you want to define a maximum length for Universal Resource Indicators (URIs). Specify the maximum length in bytes, and then use the Permit, Block, and Alarm controls to specify the action that the router takes if it encounters an URL that is longer than this value.
Enable HTTP inspection Checkbox

Check if you want the router to inspect HTTP traffic. If you want to block traffic from Java applications, you can specify a Java blocking filter by clicking the ... button and either specifying an existing ACL, or creating a new ACL for Java inspection.

Enable HTTPS inspection checkbox

Check if you want the router to inspect HTTPS traffic.

Set time out value checkbox

Check if you want to set a time out for HTTP sessions, and enter the number of seconds in the Time-Out field. Sessions will be dropped that exceed this amount of time.

Enable audit trail

You can make CBAC audit trail settings for HTTP traffic that will override the setting in the Global Timeouts and Thresholds window. Default means that the current global setting will be used. On explicitly enables the CBAC audit trail for HTTP traffic and for HTTPS traffic if HTTPS inspection is enabled, and overrides the global audit trail setting. Off explicitly disables the CBAC audit trail for HTTP traffic and for HTTPS traffic if HTTPS inspection is enabled, and overrides the global audit trail setting.

Header Options

You can have the router permit or deny traffic based on HTTP header length and the request method contained in the header. Request methods are the commands sent to HTTP servers to fetch URLs, web pages, and perform other actions. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.
Set maximum header length checkbox

Check if you want the router to permit or deny traffic based on HTTP header length, and specify the maximum Request and maximum Response header length. Use the Permit, Block, and Alarm controls to specify the action the router takes if header length exceeds these lengths.

Configure Extension Request Method checkboxes

If you want the router to permit or deny HTTP traffic based on an extension request method, check the box next to that request method. Use the Permit, Block, and Alarm controls to specify the action the router takes if it encounters traffic using that request method.

Configure RFC Request Method checkboxes

If you want the router to permit or deny HTTP traffic based on one of the HTTP request methods specified in RFC 2616, Hypertext Transfer Protocol—HTTP/1.1, check the box next to that request method. Use the Permit, Block, and Alarm controls to specify the action the router takes if it encounters traffic using that request method.

Content Options

You can have the router examine the content of HTTP traffic and permit or block traffic, and generate alarms based on what things that you make the router check. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action that the router takes if it encounters traffic with the characteristics that you specify in this window.

Verify Content Type checkbox

Check if you want the router to verify the content of HTTP packets by matching the response with the request, by enabling an alarm for unknown content types, or by using both of these methods. Use the permit, block, and alarm controls to specify the action the router takes if requests cannot be matched with responses, and when it encounters an unknown content type.
Set Content Length checkbox

Check this box to set a minimum and maximum length for the data in an HTTP packet, and enter the values in the fields provided. Use the permit, block, and alarm controls to specify the action the router takes if the amount of data falls below the minimum length or when it exceeds the maximum length.

Configure Transfer Encoding Checkbox

Check this box to have the router verify how the data in the packet is encoded, and use the permit, block, and alarm controls to specify the action the router takes if it encounters the transfer encodings that you choose.

Chunk checkbox

The Encoding format specified in RFC 2616, Hypertext Transfer Protocol—HTTP/1. The body of the message is transferred in a series of chunks; each chunk contains its own size indicator.

Compress checkbox

The encoding format produced by the UNIX "compress" utility.

Deflate checkbox

The "ZLIB" format defined in RFC 1950, ZLIB Compressed Data Format Specification version 3.3, combined with the "deflate" compression mechanism described in RFC 1951, DEFLATE Compressed Data Format Specification version 1.3.

gzip checkbox

The encoding format produced by the GNU zip ("gzip") program.

Identity checkbox

Default encoding, which indicates that no encoding has been performed.
Applications/Protocols

This window allows you to create policy settings for applications and protocols that are not found in the other windows. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Applications/Protocols Tree

The Applications/Protocols tree enables you to filter the list on the right according to the type of applications and protocols that you want to view. First choose the branch for the general type that you want to display. The frame on the right displays the available items for the type that you chose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click on the + sign to expand the branch and then select the subcategory that you want to display. If the list on the right is empty, there are no applications or protocols available for that type. To choose an application, you can check the box next to it in the tree, or you can check the box next to it in the list.

Example: If you want to display all Cisco applications, click the Applications branch folder, and then click the Cisco folder. You will see applications like clp, cisco-net-mgmt, and cisco-sys.

Edit Button

Click this button to edit the settings for the chosen application. Settings that you make override the global settings configured on the router.

Applications Column

The name of the application or protocol, for example tcp, smtp, or ms-sna. To edit the settings for an item, check the box to the left of the item name, and click Edit.

Alerts, Audit, and Timeout Columns

These columns display explicitly-set values for an item. If a setting is not changed for an item, the column is empty. For example, if auditing has been enabled for the ms-sna application, but no changes have been made to the alert or to the timeout settings, the value on is displayed in the Audit column, but the Alert and Timeout columns are blank.
Options Column

This column can contain fields if other settings were made for the chosen item.

MAX Data
Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure login
Causes a user at a nonsecure location to use encryption for authentication.

Reset
Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic
Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Timeouts and Thresholds for Inspect Parameter Maps and CBAC

Use this information to help you create or edit a parameter map for inspection purposes, or to set Context-Based Access Control (CBAC) global timeouts and thresholds. CBAC uses timeouts and thresholds to determine how long to manage state information for a session and to determine when to drop sessions that do not become fully established. These timeouts and thresholds apply to all sessions. Global Timer values can be specified in seconds, minutes, or hours.

TCP Connection Timeout Value
Amount of time to wait for a TCP connection to be established. The default value is 30 seconds.
TCP FIN Wait Timeout Value

Amount of time that a TCP session will still be managed after the firewall detects a FIN exchange. The default value is 5 seconds.

TCP Idle Timeout Value

Amount of time that a TCP session will still be managed after no activity has been detected. The default value is 3600 seconds.

UDP Idle Timeout Value

Amount of time that a User Datagram Protocol (UDP) session will still be managed after no activity has been detected. The default value is 30 seconds.

DNS Timeout Value

Amount of time that a Domain Name System (DNS) name lookup session will be managed after no activity has been detected. The default value is 5 seconds.

SYN Flooding DoS Attack Thresholds

An unusually high number of half-open sessions may indicate that a Denial of Service (DoS) attack is under way. DoS attack thresholds allow the router to start deleting half-open sessions after the total number of them has reached a maximum threshold. By defining thresholds, you can specify when the router should start deleting half-open sessions and when it can stop deleting them.

One-minute session thresholds. These fields let you specify the threshold values for new connection attempts.

Low Stop deleting new connections after the number of new connections drops below this value. The default value is 400 sessions.

High Start deleting new connections when the number of new connections exceeds this value. The default value is 500 sessions.
Maximum incomplete session thresholds. These fields let you specify the threshold values for the total number of existing half-open sessions.

Low
Stop deleting new connections after the number of new connections drops below this value. The default value is 400 sessions for Cisco IOS releases older than 12.4(11)T. When a Low value is not explicitly set, Cisco IOS will stop deleting new sessions when the number of sessions drops to 400.

For Cisco IOS release 12.4(11)T and later, the default value is unlimited. When a Low value is not explicitly set, Cisco IOS will not stop deleting new connections.

High
Start deleting new connections when the number of new connections exceeds this value. The default value is 500 sessions for Cisco IOS releases older than 12.4(11)T. When a High value is not explicitly set, Cisco IOS starts deleting sessions when more than 500 new sessions have been established.

For Cisco IOS release 12.4(11)T and later, the default value is unlimited. When a High value is not explicitly set, Cisco IOS will not start deleting new connections.

TCP Maximum Incomplete Sessions per Host:
The router starts deleting half-open sessions for the same host when the total number for that host exceeds this number. The default number of sessions is 50. If you check the Blocking Time field and enter a value, the router will continue to block new connections to that host for the number of minutes that you specify.

Enable audit globally
Check if you want to turn on CBAC audit trail messages for all types of traffic.

Enable alert globally
Check if you want to turn on CBAC alert messages for all types of traffic.
Associate Policy with an Interface

In this window, select the interface to which you want to apply the selected policy. Also specify whether the policy is to apply to incoming traffic, to outgoing traffic, or to traffic in both directions.

For example, if the router has FastEthernet 0/0 and FastEthernet 0/1 interfaces, and you want to apply the policy to the FastEthernet 0/1 interface, on traffic flowing in both directions, check the box next to FastEthernet 0/1, and check the boxes in both the Incoming and the Outgoing columns. To have only incoming traffic inspected, only check the box in the Incoming column.

Edit Inspection Rule

Use this window to specify custom inspection rule settings for an application. Settings made here and applied to the router’s configuration override the global settings.

Click the Global Settings button in the Application Security window to display the global settings for the parameters that you can set in this window. See Timeouts and Thresholds for Inspect Parameter Maps and CBAC for more information.

Alert Field

Choose one of the following values:

- **default**—Use the global setting for alerts.
- **on**—Generate an alert when traffic of this type is encountered.
- **off**—Do not generate an alert when traffic of this type is encountered.

Audit Field

Choose one of the following values:

- **default**—Use the global setting for audit trails.
- **on**—Generate an audit trail when traffic of this type is encountered.
- **off**—Do not generate an audit trail when traffic of this type is encountered.
Timeout Field

Enter the number of seconds that a session for this application should be managed after no activity has been detected. The timeout value that you enter sets the TCP Idle Timeout value if this is a TCP application, or the UDP timeout value if this is a UDP application.

Other Options

Certain applications can have additional options set. Depending on the application, you may see the options described next.

MAX Data field

Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure Login Checkbox

Causes a user at a nonsecure location to use encryption for authentication.

Reset Checkbox

Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic Checkbox

Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Permit, Block, and Alarm Controls

Use the Permit, Block, and Alarm controls to specify what the router is to do when it encounters traffic with the characteristics that you specify. To make a policy setting for an option with these controls, check the box next to it. Then, in the Action column, choose Permit to allow traffic related to that option, or choose Block to deny traffic. If you want an alarm to be sent to the log when this type of traffic is encountered, check Send Alarm. The Send Alarm control is not used in all windows.
Logging must be enabled for Application Security to send alarms to the log. For more information go to this link: Application Security Log.