



Application Firewall-Instant Message Traffic Enforcement

Last Updated: January 19, 2012

The Application Firewall--Instant Message Traffic Enforcement feature enables users to define and enforce a policy that specifies which instant messenger traffic types are allowed into the network. Thus, the following additional functionality can also be enforced:

- Configuration of firewall inspection rules
- Deep packet inspection of the payload, looking for services such as text chat
- [Finding Feature Information, page 1](#)
- [Restrictions for Application Firewall-Instant Message Traffic Enforcement, page 1](#)
- [Information About Application Firewall-Instant Message Traffic Enforcement, page 2](#)
- [How to Define and Apply an Application Policy to a Firewall for Inspection, page 2](#)
- [Configuration Examples for Setting Up an Instant Messenger Traffic Inspection Engine, page 8](#)
- [Additional References, page 8](#)
- [Feature Information for Application Firewall-Instant Message Traffic Enforcement, page 10](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Application Firewall-Instant Message Traffic Enforcement

If an instant messenger traffic enforcement policy is configured on a Cisco IOS router with a server command, traffic destined to other services (such as Telnet, FTP, SMTP) that is running on the instant



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

message server's IP address will also be treated as IM traffic by the Cisco IOS router. Thus, access to the other services is prevented through the Cisco IOS firewall; however, this limitation is not a problem for most IM application users who are connecting from a user's network.

Information About Application Firewall-Instant Message Traffic Enforcement

- [What Is an Application Policy, page 2](#)
- [Instant Messenger Application Policy Overview, page 2](#)

What Is an Application Policy

The application firewall uses an application policy, which consists of a collection of static signatures, to detect security violations. A static signature is a collection of parameters that specify protocol conditions that must be met before an action is taken. These protocol conditions and reactions are defined by the end user via the command-line interface (CLI) to form an application policy.

Instant Messenger Application Policy Overview

Cisco IOS application firewall has been enhanced to support instant native messenger application policies. Thus, the Cisco IOS firewall can now detect and prohibit user connections to instant messenger servers for the AOL Instant Messenger (AIM), Yahoo! Messenger, and MSN Messenger instant messaging services. This functionality controls all connections for supported services, including text, voice, video, and file-transfer capabilities. The three applications can be individually denied or permitted. Each service may be individually controlled so that text-chat service is allowed, and voice, file transfer, video, and other services are restricted. This functionality augments existing Application Inspection capability to control IM application traffic that has been disguised as HTTP (web) traffic.

**Note**

If an instant messenger application is blocked, the connection will be reset and a syslog message will be generated, as appropriate.

How to Define and Apply an Application Policy to a Firewall for Inspection

- [Defining an Application Policy to Permit or Deny Instant Messenger Traffic, page 2](#)
- [Applying an Instant Messenger Traffic Application Policy to a Firewall for Inspection, page 6](#)

Defining an Application Policy to Permit or Deny Instant Messenger Traffic

Use this task to create an instant messenger application firewall policy.

**Note**

If at least one DNS name was not specified for resolution under any of the application policies for IM protocols (AOL, Yahoo, or MSN), you do not need to configure the DNS server IP address in the Cisco IOS router.

Before defining and enabling an application policy for instant messenger traffic, you must have already properly configured your router with a Domain Name System (DNS) server IP address via the **ip domain lookup** command and the **ip name-server** command.

The IP address of the DNS server configured on the Cisco IOS router must be the same as that configured on all PCs connecting to the IM servers from behind the Cisco IOS firewall.

**Note**

Although application firewall policies are defined in global configuration mode, only one global policy for a given protocol is allowed per interface.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **appfw policy-name policy-name**
4. **application protocol**
5. **audit-trail {on | off}**
6. **server {permit | deny} {name string | ip-address {ip-address | range ip-address-start ip-address-end}}**
7. **timeout seconds**
8. **service {default | text-chat} action {allow [alarm] | reset [alarm] | alarm}**
9. **alert {on | off}**
10. **exit**
11. **show appfw {configuration | dns cache} [policy policy-name]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<p>appfw policy-name policy-name</p> <p>Example:</p> <pre>Router(config)# appfw policy-name my_policy</pre>	<p>Defines an application firewall policy and enters application firewall policy configuration mode.</p>
Step 4	<p>application protocol</p> <p>Example:</p> <pre>Router(cfg-appfw-policy)# application im aol</pre>	<p>Allows you to configure inspection parameters for a given protocol.</p> <ul style="list-style-type: none"> <i>protocol</i> -- One of the following options: <ul style="list-style-type: none"> http (HTTP traffic will be inspected) im {aol yahoo msn} (Traffic for the specified instant messenger application will be inspected) <p>This command puts the router in appfw-policy-protocol configuration mode, where “protocol” is dependent upon the specified protocol.</p>
Step 5	<p>audit-trail {on off}</p> <p>Example:</p> <pre>Router(cfg-appfw-policy-aim)# audit- trail on</pre>	<p>(Optional) Enables message logging for established or torn-down connections.</p> <p>If this command is not issued, the default value specified via the ip inspect audit-trail command will be used.</p>
Step 6	<p>server {permit deny} {name string ip-address {ip-address range ip-address-start ip-address-end}}</p> <p>Example:</p> <pre>Router(cfg-appfw-policy-aim)# server permit name login.cat.aol.com</pre>	<p>Controls access to instant messenger servers.</p> <p>Note The server command helps the instant messenger application engine to recognize the port-hopping instant messenger traffic and to enforce the security policy for that instant messenger application; thus, if this command is not issued, the security policy cannot be enforced if IM applications use port-hopping techniques. To deploy IM traffic enforcement policies effectively, it is recommended that you issue the appropriate server command.</p>
Step 7	<p>timeout <i>seconds</i></p> <p>Example:</p> <pre>Router(cfg-appfw-policy-aim)# timeout 30</pre>	<p>(Optional) Specifies the elapsed length of time before an inactive connection is torn down.</p> <ul style="list-style-type: none"> <i>seconds</i> -- Available timeout range: 5 to 43200 (12 hours). <p>If this command is not issued, the default value specified via the ip inspect tcp idle-time command will be used.</p> <p>Note Some IM applications continue to send “keepalive-like” packets that effectively prevent timeout even when the user is idle.</p>

	Command or Action	Purpose
Step 8	<p>service {default text-chat} action {allow [alarm] reset [alarm] alarm}</p> <p>Example:</p> <pre>Router(cfg-appfw-policy-aim)# service default action reset</pre>	<p>(Optional) Specifies an action when a specific service is detected in the instant messenger traffic.</p> <ul style="list-style-type: none"> If a specific action is not specified for a service, the service default command will be performed. If the service default command is not specified for an application, the action is considered “reset” by the system.
Step 9	<p>alert {on off}</p> <p>Example:</p> <pre>Router(cfg-appfw-policy-aim)# alert on</pre>	<p>(Optional) Enables message logging when events, such as the start of a text-chat, begin.</p> <p>If this parameter is not configured, the global setting for the ip inspect alert-off command will take effect.</p>
Step 10	<p>exit</p> <p>Example:</p> <pre>Router(cfg-appfw-policy-aim)# exit</pre> <p>Example:</p> <pre>Router(cfg-appfw-policy)# exit</pre> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>(Optional) Exits application firewall policy <i>protocol</i> configuration mode, application firewall policy configuration mode, and global configuration mode.</p>
Step 11	<p>show appfw {configuration dns cache} [policy policy-name]</p> <p>Example:</p> <pre>Router# show appfw dns cache policy abc</pre>	<p>(Optional) Displays the IP addresses that have been resolved by the DNS server and stored in the DNS cache of the IM traffic policy enforcement component of the Cisco IOS router.</p> <ul style="list-style-type: none"> If you don’t indicate a specific policy via the policy policy-name option, IP addresses gathered for all DNS names for all policies are displayed.

- [Troubleshooting Tips, page 5](#)
- [What to Do Next, page 6](#)

Troubleshooting Tips

Resolved IP addresses are never “timed out” and not automatically removed from the DNS cache. Thus, if you find an obsolete IP address in the instant messenger database (DNS cache), you can issue the **clear appfw dns cache** command to remove the IP address and prevent the address from being interpreted by the router as that of an IM server.

Always allow a couple of minutes for the DNS cache to populate after configuring the **server** command (with the **name string** option) in an application firewall policy for IM applications.

If you do not want the DNS resolver to send periodic queries, do not use the **server** command (with the **name string** option); instead, use the **server** command (with the **ip address** option).

If you issue the **server** command (with the **name string** option), ensure that you specify the name of every DNS server for an IM application in your policy. Always be alert to new names.

What to Do Next

After you have successfully defined an application policy for instant message traffic inspection, you must apply the policy to an inspection rule. Thereafter, the inspection rule must be applied to an interface. For information on completing this task, see the section “Applying an Instant Messenger Traffic Application Policy to a Firewall for Inspection.”

Applying an Instant Messenger Traffic Application Policy to a Firewall for Inspection

Use this task to apply an IM application policy to an inspection rule, followed by applying the inspection rule to an interface.

You must have already defined an application policy (as shown in the section “Defining an Application Policy to Permit or Deny Instant Messenger Traffic”).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* **appfw** *policy-name*
4. **interface** *type number*
5. **ip inspect** *inspection-name* **in | out**
6. **exit**
7. **exit**
8. **show appfw** configuration [name]

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name <i>inspection-name</i> appfw <i>policy-name</i> Example: Router(config)# ip inspect name firewall appfw mypolicy	Defines a set of inspection rules for the application policy. <ul style="list-style-type: none"> • <i>policy-name</i> --Must match the policy name specified via the appfw <i>policy-name</i> command.
Step 4	interface <i>type number</i> Example: Router#(config)# interface FastEthernet0/0	Configures an interface type and enters interface configuration mode.
Step 5	ip inspect <i>inspection-name</i> in out} Example: Router#(config-if)# ip inspect firewall in	Applies the inspection rules (defined in Step 3) to all traffic entering the specified interface. <ul style="list-style-type: none"> • The <i>inspection-name</i> argument must match the inspection name defined via the ip inspect name command.
Step 6	exit Example: Router#(config-if)# exit	Exits interface configuration mode.
Step 7	exit Example: Router(config)# exit	Exits global configuration mode.
Step 8	show appfw configuration [name] Example: Router# show appfw configuration	(Optional) Displays application firewall policy configuration information.

Configuration Examples for Setting Up an Instant Messenger Traffic Inspection Engine

- [Example Instant Messenger Application Policy Configuration, page 8](#)

Example Instant Messenger Application Policy Configuration

The following example shows to configure application policy “my-im-policy,” which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
application http
  port-misuse im reset
!
application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
application im aol
  server deny name login.oscar.aol.com
!
application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy
interface FastEthernet0/0
  description Inside interface
  ip inspect test in
```

The **port-misuse im** command blocks all the three IM applications going through the HTTP protocol. It is always recommended that you block IM activity through HTTP and allow IM traffic to pass, if at all, through its native port.

The **server permit** commands help to identify all the servers for Yahoo! messenger services. A connection to any one of the specified servers will be recognized by the firewall as a Yahoo! IM session—even if the Yahoo! client uses port-hopping techniques (which can be accomplished by using server port-numbers such as 25 instead of the standard 5050.)

If a **server permit** command is not issued within the **application im yahoo** command, the Cisco IOS firewall will classify only the traffic going to server port 5050 as Yahoo! messenger traffic. Because the port classification scheme breaks if any of the Yahoo! clients are configured to use a port other than 5050, it is more reliable to have **server permit** command entries instead of relying on the port classification method.

The **server deny** commands under other IM applications deny connection to respective servers. This action operates at the network layer connection level—not at the application session level. When traffic is denied, the TCP connection to the server is denied, no data traffic is allowed, and all packets are dropped in the firewall.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Firewall commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i>
Application firewall: configure a firewall to detect and prohibit HTTP connections	"HTTP Inspection Engine"

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Application Firewall-Instant Message Traffic Enforcement

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 *Feature Information for Application Firewall-Instant Message Traffic Enforcement*

Feature Name	Releases	Feature Information
Application Firewall--Instant Message Traffic Enforcement	12.4(4)T	<p>The Application Firewall--Instant Message Traffic Enforcement feature enables users to define and enforce a policy that specifies which instant messenger traffic types are allowed into the network.</p> <p>The following commands were introduced or modified: alert, application (application firewall policy), audit-trail, clear appfw dns cache, server (application firewall policy), service, show appfw, timeout.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.