Application Firewall—Instant Message Traffic Enforcement

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

History for the Application Firewall—Instant Message Traffic Enforcement Feature

Release	Modification
12.4(4)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

CISCO SYSTEMS

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

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 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

Before creating an application firewall policy for instant message traffic enforcement, you should understand the following concept:

- 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 servies, 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

This section contains the following procedures:

Defining an Application Policy to Permit or Deny Instant Messenger Traffic

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

Prerequisites

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 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.

Restrictions

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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**appfw policy-name** *policy-name* **Example:** `Router(config)# appfw policy-name my_policy`	Defines an application firewall policy and enters application firewall policy configuration mode.
Step 4	**application** *protocol* **Example:** `Router(cfg-appfw-policy)# application im aol`	Allows you to configure inspection parameters for a given protocol. • *protocol*— One of the following options: – **http** (HTTP traffic will be inspected) – **im** {**aol** | **yahoo** | **msn**} (Traffic for the specified instant messenger application will be inspected) This command puts the router in appfw-policy-protocol configuration mode, where "protocol" is dependent upon the specified protocol.
Step 5	**audit-trail** {**on** | **off**} **Example:** `Router(cfg-appfw-policy-aim)# audit-trail on`	(Optional) Enables message logging for established or torn-down connections. If this command is not issued, the default value specified via the **ip inspect audit-trail** command will be used.
Step 6	**server** {**permit** | **deny**} {**name** *string* | **ip-address** {*ip-address* | **range** *ip-address-start ip-address-end*} **Example:** `Router(cfg-appfw-policy-aim)# server permit name login.cat.aol.com`	Controls access to instant messenger servers. **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.

	Command or Action	Purpose
Step 7	**timeout** *seconds* **Example:** `Router(cfg-appfw-policy-aim)# timeout 30`	(Optional) Specifies the elapsed length of time before an inactive connection is torn down. • *seconds*—Available timeout range: 5 to 43200 (12 hours). If this command is not issued, the default value specified via the **ip inspect tcp idle-time** command will be used. **Note** Some IM applications continue to send "keepalive-like" packets that effectively prevent timeout even when the user is idle.
Step 8	**service** {**default** | **text-chat**} **action** {**allow** [**alarm**] | **reset** [**alarm**] | **alarm**} **Example:** `Router(cfg-appfw-policy-aim)# service default action reset`	(Optional) Specifies an action when a specific service is detected in the instant messenger traffic. • 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	**alert** {**on** | **off**} **Example:** `Router(cfg-appfw-policy-aim)# alert on`	(Optional) Enables message logging when events, such as the start of a text-chat, begin. If this parameter is not configured, the global setting for the **ip inspect alert-off** command will take effect.

Step 10	**exit**
	
	Example:
	`Router(cfg-appfw-policy-aim)# exit`
	
	Example:
	`Router(cfg-appfw-policy)# exit`
	
	Example:
	`Router(config)# exit`
		(Optional) Exits application firewall policy *protocol* configuration mode, application firewall policy configuration mode, and global configuration mode.

Step 11	**show appfw** {**configuration** | **dns cache**} [**policy** *policy-name*] **Example:** `Router# show appfw dns cache policy abc`	(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. • 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

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.

Prerequisites

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip inspect name** *inspection-name* **appfw** *policy-name* **Example:** `Router(config)# ip inspect name firewall appfw mypolicy`	Defines a set of inspection rules for the application policy. • *policy-name*—Must match the policy name specified via the **appfw policy-name** command.
Step 4	**interface** *type number* **Example:** `Router#(config)# interface FastEthernet0/0`	Configures an interface type and enters interface configuration mode.
Step 5	**ip inspect** *inspection-name* {**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. • The *inspection-name* 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

This section contains the following configuration example:

- Instant Messenger Application Policy Configuration: Example, page 8

Instant Messenger Application Policy Configuration: Example

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

The following sections provide references related to the Application Firewall—Instant Message Traffic Enforcement feature.

Related Documents

Related Topic	Document Title
Application firewall: configure a firewall to detect and prohibit HTTP connections	*HTTP Inspection Engine*, Cisco IOS Release 12.3(14)T feature module
Additional firewall configuration tasks and overview information	The section "Traffic Filtering, Firewalls, and Virus Detection" in the *Cisco IOS Security Configuration Guide*
Firewall commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*, Release 12.4T

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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

New Commands

- **alert**
- **clear appfw dns cache**
- **server (application firewall policy)**
- **service**

Modified Commands

- **application (application firewall policy)**
- **audit-trail**
- **show appfw**
- **timeout**

alert

To enable message logging when events, such as the start of a text-chat, begin, use the **alert** command in the appropriate configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

alert {**on** | **off**}

no alert

Syntax Description

on	Enables message logging for instant messenger application policy events.
off	Disables message logging for instant messenger application policy events.

Command Default

If this command is not configured, the global setting for the **ip inspect alert-off** command will take effect.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Examples

The following example shows to enable audit trail messages for all AOL instant messenger traffic:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im aol
  server deny name login.oscar.aol.com
  audit trail on
  alert on
```

Related Commands

Command	Description
ip inspect alert-off	Disables Cisco IOS firewall alert messages.

application (application firewall policy)

To put the router in appfw-policy-*protocol* configuration mode and begin configuring inspection parameters for a given protocol, use the **application** command in application firewall policy configuration mode. To remove protocol-specific rules, use the **no** form of this command.

application *protocol*

no application *protocol*

Syntax Description

protocol	Protocol-specific traffic will be inspected. One of the following protocols (keywords) can be specified: • **http** (HTTP traffic will be inspected.) • **im** {**aol** | **yahoo** | **msn**} (Traffic for the specified instant messenger application will be inspected.)

Command Default

You cannot set up protocol-specific inspection parameters.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	The **im**, **aol**, **yahoo**, and **msn** keywords were introduced to support instant message traffic detection and prohibition.

Examples

This command puts the router in appfw-policy-*protocol* configuration mode, where "*protocol*" is dependent upon the specified protocol.

HTTP-Specific Inspection Commands

After you issue the **application http** command and enter the appfw-policy-http configuration mode, begin configuring inspection parameters for HTTP traffic by issuing any of the following commands:

- **audit-trail**
- **content-length**
- **content-type-verification**
- **max-header-length**
- **max-uri-length**
- **port-misuse**

- **request-method**
- **strict-http**
- **timeout**
- **transfer-encoding**

Instant Messenger-Specific Inspection Commands

After you issue the **application im** command and specify an instant messenger application (AOL, Yahoo, or MSN), you can begin configuring inspection parameters for IM traffic by issuing any of the following commands:

- **alert**
- **audit trail**
- **server**
- **service**
- **timeout**

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

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
```

Related Commands

Command	Description
appfw policy-name	Defines an application firewall policy and puts the router in application firewall policy configuration mode.

audit-trail

To enable message logging for established or torn-down connections, use the **audit-trail** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

audit-trail {**on** | **off**}

no audit-trail {**on** | **off**}

Syntax Description

on	Audit trail messages are generated.
off	Audit trail messages are not generated.

Defaults

If this command is not issued, the default value specified via the **ip inspect audit-trail** command will be used.

Command Modes

cfg-appfw-policy-http configuration

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	Support for the inspection of instant messenger applications was introduced.

Usage Guidelines

The **audit-trail** command will override the **ip inspect audit-trail** global command.

Before you can issue the **audit-trail** command, you must enable protocol inspection via the **application** command, which allows you to specify whether you want to inspect HTTP traffic or instant messenger application traffic. The **application** command puts the router in appfw-policy-*protocol* configuration mode, where "*protocol*" is dependent upon the specified protocol.

Examples

The following example, which shows how to define the HTTP application firewall policy "mypolicy," enables audit trail messages for the given policy. This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  audit trail on
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
```

```
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
ip inspect audit-trail	Turns on audit trail messages.

clear appfw dns cache

To clear at least one IP address from the Domain Name System (DNS) cache, use the **clear appfw dns cache** command in privileged EXEC mode.

clear appfw dns cache name *dns-name* [**address** *address*]

Syntax Description

name *dns-name*	DNS name of the IM server as entered in the **server name** command in application firewall policy.
address *address*	(Optional) Deletes a specific IP address from the DNS server cache. If an IP address is not specified, all IP addresses for the *dns-name* are deleted from the DNS server cache.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

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 an IM server.

Only one IP address can be deleted at a time. If the deleted IP address appears in the subsequent DNS resolution, the IP address is added to the DNS cache again.

Examples

The following example shows how to clear the IP address "172.16.0.0" from the cache of the DNS server "logon.cat.aol.com":

```
Router# clear appfw dns cache name logon.cat.aol.com address 172.16.0.0
```

Related Commands

Command	Description
server	Configures a set of DNS servers for which the specified instant messenger application will be interacting.

server (application firewall policy)

To configure a set of Domain Name System (DNS) servers for which the specified instant messenger application will be interacting, use the **server** command in the appropriate configuration mode. To change or remove a configured set of DNS servers, use the **no** form of this command.

server {**permit** | **deny**} {**name** *string* | **ip-address** {*ip-address* | **range** *ip-address-start ip-address-end*}

no server {**permit** | **deny**} {**name** *string* | **ip-address** {*ip-address* | **range** *ip-address-start ip-address-end*}

Syntax Description

permit	Inspects all traffic destined for a specified server, and the applicable policy is enforced.
deny	Blocks all traffic destined for a specified, denied server. TCP connections are denied by dropping all packets bound to the specified server.
name *string*	Name of DNS server for which traffic will be permitted (and inspected) or denied. The same server name cannot appear under two different instant messenger applications; however, the same name can appear under two different policies within the same instant messenger application. Each entry will accept only one DNS name.
ip-address	Indicates that at least one IP address will be listed.
ip-address	IP address of the DNS server for which traffic will be permitted (and inspected) or denied.
range *ip-address-start ip-address-end*	Range of DNS server IP addresses for which traffic will be permitted (and inspected) or denied.

Command Default

If this command is not issued, instant messenger application polices cannot be enforced.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

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.

Note If a router cannot identify a packet as belonging to a particular instant messenger policy, the corresponding policy cannot be enforced.

To configure more than one set of servers, you can issue the **server** command multiple times within an instant messenger's application policy. Multiple entries are treated cumulatively.

The server name Command

The server command (with the **name** keyword) internally resolves the DNS name of the server. This command sends DNS queries multiple times to gather all possible IP addresses for the IM servers, which return different IP addresses at different times in response to DNS queries of the same names. It uses the Time to Live (TTL) field found in DNS responses to refresh its cache. After a certain period, the DNS cache in IM applications stabilize. It is recommended that you allow a couple of minutes for the DNS cache to populate with the IM server IP addresses before the IM traffic reaches the Cisco IOS firewall. All existing IM application connections are not subjected to IM policy enforcement.

Denying Access to a Particular Instant Messenger Application

You can deny traffic to a particular instant messenger application in one of the following ways:

- Issue the **server deny** command and list all the server names and IP addresses to which you want to deny access.

Note The first option is the preferred method because it performs slightly better than the second option.

- Issue the **server permit** command and list all the server names and IP addresses that you want inspected; thereafter, issue the **service default reset** command, which will deny access to all services.
- Issue **server deny** command to block access to any site given its DNS name. For example, to block all access to a gambling site, you can configure **server deny name www.noaccess.com**.

Examples

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.cat.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
```

Related Commands

Command	Description
service	Specifies an action when a specific service is detected in the instant messenger traffic.

service

To specify an action when a specific service is detected in the instant messenger traffic, use the **service** command in the appropriate configuration mode. To disable or change a specified action, use the **no** form of this command.

service {**default** | **text-chat**} **action** {**allow** [**alarm**] | **reset** [**alarm**] | **alarm**}

no service {**default** | **text-chat**} **action** {**allow** [**alarm**] | **reset** [**alarm**] | **alarm**}

Syntax Description

default	Matches all services that are not explicitly configured under the application. **Note** It is recommended that when an IM application is allowed, always specify the default option for an IM application.
text-chat	Controls the text-based chat service that is provided by instant messenger applications.
action	Indicates that a specific action is to follow.
allow	Allows a specific service.
reset	Blocks the service specified in the configuration. If the **default** option is being used, only services for which a specific action has been identified are allowed; all other services are denied.
alarm	Generates an alarm message when the specified service is encountered over the connection.

Command Default

service default action reset

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

When the **reset** keyword is used, the connection is reset if TCP is used, and the packet is dropped if UDP is used. When dropping a packet from a UDP connection, the session will not be immediately deleted; instead, the session will time out to prevent additional sessions from being immediately created.

The **alarm** keyword can be specified alone or with the **allow** or **reset** keywords; however, the **allow** or **reset** keywords are mutually exclusive.

Examples

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
```

show appfw

To display application firewall policy information, use the **show appfw** command in privileged EXEC mode.

show appfw {**configuration** | **dns cache**} [**policy** *policy-name*]

Syntax Description

configuration	Displays configuration information for configured policies.
dns cache	Displays the IP addresses resolved by the Domain Name System (DNS) server of the applicable instant messenger application.
policy *policy-name*	(Optional) Displays information only for the specified policy. If you do not indicate a specific policy via the **policy** *policy-name* option, IP addresses gathered for all DNS names for all policies are displayed.

Defaults

If no policies are specified, information for all policies is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	The **dns cache** keyword was added to support instant messenger traffic inspection.

Usage Guidelines

Use this command to display information regarding the application firewall policy configuration or the IP addresses of the DNS cache.

Examples

This sample output for the **show appfw configuration** command and the **show ip inspect configuration** command display the configuration for the inspection rule "mypolicy," which has been applied to all incoming HTTP traffic on the FastEthernet0/0 interface. In this example, you can see that all available HTTP inspection parameters have been defined.

```
Router# show appfw configuration

Application Firewall Rule configuration
  Application Policy name mypolicy
    Application http
      strict-http action allow alarm
      content-length minimum 0 maximum 1 action allow alarm
      content-type-verification match-req-rsp action allow alarm
      max-header-length request length 1 response length 1 action allow alarm
      max-uri-length 1 action allow alarm
      port-misuse default action allow alarm
      request-method rfc default action allow alarm
      request-method extension default action allow alarm
      transfer-encoding default action allow alarm
```

```
Router# show ip inspect config

Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name firewall
http alert is on audit-trail is off timeout 3600
```

Related Commands

Command	Description
show ip inspect	Displays firewall configuration and session information.

timeout

To specify the elapsed length of time before an inactive connection is torn down, use the **timeout** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description

seconds	Idle timeout value. Available range: 5 to 43200 (12 hours).

Command Default

If this command is not issued, the default value specified via the **ip inspect tcp idle-time** command will be used.

Command Modes

cfg-appfw-policy-http configuration

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	Support for the inspection of instant messenger applications was introduced.

Usage Guidelines

The **timeout** command overrides the global TCP idle timeout value for HTTP traffic or for traffic of a specified instant messenger application (AOL, Yahoo, or MSN).

Before you can issue the **timeout** command, you must enable protocol inspection via the **application** command, which allows you to specify whether you want to inspect HTTP traffic or instant messenger application traffic. The **application** command puts the router in appfw-policy-*protocol* configuration mode, where "*protocol*" is dependent upon the specified protocol.

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
```

```
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
  timeout 60
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will be managed while there is no activity).