



# ESMTP Support for Cisco IOS Firewall

---

The ESMTP Support for Cisco IOS Firewall feature enhances the Cisco IOS Firewall to support Extended Simple Mail Transport Protocol (ESMTP), allowing customers who install mail servers behind Cisco IOS firewalls to install their servers on the basis of ESMTP (instead of Simple Mail Transport Protocol [SMTP]).

## Feature History for ESMTP Support for Cisco IOS Firewall

Release	Modification
12.3(7)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

- [Prerequisites for ESMTP Support for Cisco IOS Firewall, page 1](#)
- [Information About ESMTP Support for Cisco IOS Firewall, page 2](#)
- [How to Configure a Firewall to Support ESMTP, page 6](#)
- [Configuration Examples for Firewall ESMTP Support, page 8](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)

## Prerequisites for ESMTP Support for Cisco IOS Firewall

To enable this feature, your Cisco IOS image must contain the Cisco IOS firewall.



---

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

# Information About ESMTP Support for Cisco IOS Firewall

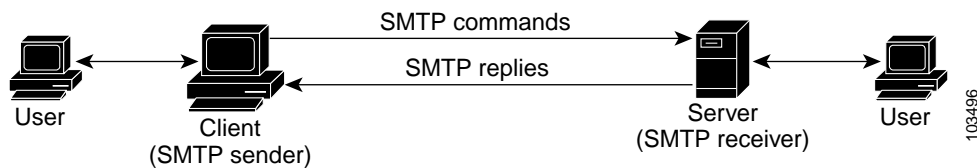
To configure a Cisco IOS firewall to inspect an ESMTP session and command sequence, you should understand the following concepts:

- [SMTP Functionality Overview, page 2](#)
- [ESMTP Overview, page 2](#)
- [SMTP Firewall and ESMTP Firewall Comparison, page 3](#)

## SMTP Functionality Overview

SMTP inspection provides a basic method for exchanging e-mail messages. [Figure 1](#) and the following steps outline a basic SMTP session.

**Figure 1** Sample SMTP Exchange Topology



After a user sends an e-mail request to the client (the “SMTP sender”), the client established a TCP channel with the server (the “SMTP receiver”). Thereafter, the client and the server exchange SMTP commands and responses until the mail transaction is complete. The steps of typical SMTP transaction are as follows:

1. The client establishes a TCP connection with the server.
2. The client sends a HELO command with its domain name. If the server can accept mail from that domain name, it responds with a 250 reply code, which allows the client to continue with the mail transaction. (If the server does not respond with a 250 reply code, the client will send a QUIT command and terminate the TCP session.)
3. The client sends the MAIL command, indicating who initiated the mail. If the server accepts the mail, it responds with an OK reply. Then, the client sends the RCPT command, identifying the recipient of the mail. If the server accepts mail for the specified recipient, it responds with an OK reply; if the server cannot accept mail for the specified recipient, it rejects the recipient but not the entire transaction. (Several recipients can be negotiated.)
4. After the list of recipients has been negotiated between the client and the server, the client sends a DATA command. If the server is ready to receive data, it responds with a 354 reply code. If the server is not ready to receive data, it responds with an error reply, and the client terminates the transaction.
5. The client sends mail data ending with a special sequence. When the server sees the end of the message, it sends a 250 code reply.
6. The client sends a QUIT command, waits for the server to respond, then terminates the session.

## ESMTP Overview

Like SMTP, ESMTP inspection provides a basic method for exchanging e-mail messages. Although an ESMTP session is similar to SMTP, there is one difference—the EHLO command.

After the TCP connection has been established between the client (the ESMTP sender) and the server (the ESMTP receiver), the client sends the EHLO command (instead of the HELO command that is used for SMTP). If the server does not support ESMTP, it sends a failure reply to the client because it did not recognize the EHLO command. If it supports ESMTP, the server responds with the code 250 and a list of extensions that the server supports. (Refer to RFC 1869 for an explanation of the extensions that your server may support.)

The server may send any of the following error codes if it supports ESMTP but is unable to function as normal:

- Error code 501—The server recognizes the EHLO command but is unable to accept it.
- Error code 502—The server recognizes the EHLO command but does not implement it.
- Error code 554—The server is unable to list the service extensions it supports.

If the client receives any of these error codes, it should issue the HELO command to revert to SMTP mode or issue the QUIT command to end the session.

After the client receives a successful response to the EHLO command, it will work the same way as SMTP, except that the client may issue new extended commands, and it may add a few parameters to the MAIL FROM and REPT TO commands.

## SMTP Firewall and ESMTP Firewall Comparison

Although a SMTP firewall and an ESMTP firewall support the same functionality—command inspection, session conversion, and Intrusion Detection System (IDS) detection—slight variations exist between the protocols. [Table 1](#) explains the firewall functionality and protocol-specific differences.

**Table 1 SMTP and ESMTP Firewalls Functionality Comparison**

Functionality	SMTP Firewall Description	ESMTP Firewall Description
Command Inspection	<p>The SMTP firewall inspects commands for illegal commands. Illegal commands found in a packet are modified to an “xxxx” pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command.</p> <p>An illegal SMTP command is any command except the following: DATA, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY.</p> <p><b>Note</b> Prior to Cisco IOS Release 12.3(7)T, an SMTP firewall will reset the TCP connection upon detection of an illegal command. That is, an SMTP firewall no longer resets the TCP connection upon detecting an illegal command.</p>	<p>ESMTP command inspection is the same as SMTP command inspection, except that ESMTP supports three additional commands—AUTH, EHLO, and ETRN.</p> <p>An illegal ESMTP command is any command except the following: AUTH, DATA, EHLO, ETRN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY.</p>
Parameter Inspection	Not applicable.	<p>The ESMTP firewall inspects the following extensions by performing deeper command inspection:</p> <ul style="list-style-type: none"> <li>• Message Size Declaration (SIZE)</li> <li>• Remote Queue Processing Declaration (ETRN)</li> <li>• Binary MIME (BINARYMIME)</li> <li>• Command Pipelining</li> <li>• Authentication</li> <li>• Delivery Status Notification (DSN)</li> <li>• Enhanced Status Code (ENHANCEDSTATUSCODE)</li> <li>• 8bit-MIMEtransport (8BITMIME)</li> </ul> <p><b>Note</b> All other extensions, including private extensions, are not supported.</p>

**Table 1 SMTP and ESMTP Firewalls Functionality Comparison (continued)**

Functionality	SMTP Firewall Description	ESMTP Firewall Description
EHLO Reply Inspection	Not applicable.	The ESMTP firewall inspects the EHLO reply, which contains a list of SMTP extensions that the server supports. Any unsupported extension that is found in the server's reply will be replaced with the "XXXX" pattern, which labels that extension "private." Thus, the client will no longer use the unsupported extension.
ESMTP to SMTP Session Conversion	<p>The SMTP firewall forces a client that initiates an ESMTP session to use SMTP. When a client attempts to initiate an ESMTP session by sending the ELHO command, the firewall treats the EHLO command as an illegal command and modified it to the "xxxx" pattern. This response causes the server to send a 5xx code reply, forcing the client to revert to SMTP mode.</p> <p><b>Note</b> Prior to Cisco IOS Release 12.3(7)T, the firewall intercepts the EHLO command and changes it to the NOOP command. The server responds with a 250 code reply. The firewall intercepts the response and modifies it to 502 code reply, which tells the client that the EHLO command is not supported.</p>	Not applicable (because EHLO is supported in ESMTP).
IDS Signature Detection	The SMTP and ESMTP firewalls scan for a set of hard-coded IDS signatures. There are 11 signatures—6 are hard coded in the firewall and are enabled by default. The other 5 signatures remain in the IDS code and are disabled by default.	

**Table 1 SMTP and ESMTP Firewalls Functionality Comparison (continued)**

Functionality	SMTP Firewall Description	ESMTP Firewall Description
Command Pipelining	Not available. (The client sends a command to the server and must wait for a reply before sending another command.)	An ESMTP firewall can inspect commands that are in the pipeline. That is, commands that are sent before a response is received are inspected.
Resetting a Connection	<p>Both SMTP and ESMTP firewalls will always send a “5xx” error code and close the connection upon detection of an unsupported parameter or an IDS signature in a command. That is, the firewall sends an appropriate reply code and closes the connection with proper TCP closing sequence packets (such as FIN or FIN+ACK) so the client does not continually attempt to send the same message.</p> <p><b>Note</b> Prior to Cisco IOS Release 12.3(7)T, an SMTP firewall will reset the TCP connection upon detection of an illegal command or IDs signature. This behavior causes the client to keep trying to send the same message for up to 4 days (which is when the original message is bounced back to the user).</p>	

## How to Configure a Firewall to Support ESMTP

This section contains the following procedures:

- [Configuring a Firewall for ESMTP Inspection, page 6](#)

### Configuring a Firewall for ESMTP Inspection

Use this task to configure a Cisco IOS Firewall to inspect an ESMTP session and command sequence.

#### Restrictions

SMTP and ESMTP cannot exist simultaneously. If SMTP is already configured, an attempt to configure ESMTP will result in the error message, “%ESMTP cannot coexist with SMTP, please unconfigure SMTP and try again...” If ESMTP is already configured, an attempt to configure SMTP will result in the error message, “%SMTP cannot coexist with ESMTP, please unconfigure ESMTP and try again...”

The following example illustrates how the router will react if you attempt to configure both protocols:

```
Router(config)# ip inspect name mail-guard smtp
Router(config)# ip inspect name mail-guard esmtp
ESMTP cannot coexist with SMTP, please unconfigure SMTP and try again...
Router(config)# end
Router# show running-config
.
.
.
ip inspect name mail-guard smtp
.
.
.
```

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* {**smtp** | **esmtplib**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**max-data** *number*] [**timeout** *seconds*]
4. **interface** *type number*
5. **ip inspect** *inspection-name* {**in** | **out**}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip inspect name</b> <i>inspection-name</i> { <b>smtp</b>   <b>esmtplib</b> } [ <b>alert</b> { <b>on</b>   <b>off</b> }] [ <b>audit-trail</b> { <b>on</b>   <b>off</b> }] [ <b>max-data</b> <i>number</i> ] [ <b>timeout</b> <i>seconds</i> ]  <b>Example:</b> Router(config)# ip inspect name test esmtplib	Configures inspection of a SMTP or an ESMTP session.
Step 4	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface ethernet0	Configures an interface type and enters interface configuration mode.
Step 5	<b>ip inspect</b> <i>inspection-name</i> { <b>in</b>   <b>out</b> }	Applies an inspection rule to an interface.
	<b>Example:</b> Router(config-if)# ip inspect test in	

## Troubleshooting Tips

To view and verify the inspection configuration, status, or session information, you can use any of the following EXEC commands:

- **show ip inspect name** *inspection-name*—Shows a particular configured inspection rule.
- **show ip inspect session**—Shows existing sessions that are currently being tracked and inspected by the firewall.
- **show ip inspect all**—Shows all inspection configuration and all existing sessions that are currently being tracked and inspected by the firewall.

### Alert Messages

The existing SMTP-related alert message will not change. This message is logged every time the firewall detects an illegal or unsupported command. The message format is as follows:

```
FW-3-SMTP_INVALID_COMMAND: Invalid SMTP command (%s) (total %d chars) from initiator (%i:%d)
```

A new alert message is added. This message is logged whenever the firewall detects an illegal parameter in an SMTP command. The message includes the address and port of the sender as well as the illegal parameter. The message format is as follows:

```
FW-3-SMTP_INVALID_PARAMETER: Invalid SMTP parameter (%s) from initiator (%i:%d)
```

## What to Do Next

To provide a record of network access through the firewall, including illegitimate access attempts, and inbound and outbound services, you should turn on logging and audit trail. For information on completing this task, refer to the section “Configuring Logging and Audit Trail” in the chapter “Configuring Context-Based Access Control” in the *Cisco IOS Security Configuration Guide*.

# Configuration Examples for Firewall ESMTP Support

This section contains the following configuration example:

- [ESMTP Inspection Configuration: Example, page 8](#)

## ESMTP Inspection Configuration: Example

The following example shows how to configure inspection of ESMTP traffic:

```
Router# configure terminal
Router(config)# ip inspect name mail-guard esmtp timeout 30
```

## Additional References

The following sections provide references related to ESMTP Support for Cisco IOS Firewall.

## Related Documents

Related Topic	Document Title
Cisco IOS Firewall configuration	The section “Traffic Filtering and Firewalls” in the <i>Cisco IOS Security Configuration Guide</i>
Cisco IOS Firewall commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T

## Standards

Standards	Title
None	—

## MIBs

MIBs	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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 821	<i>Simple Mail Transfer Protocol</i>
RFC 1652	<i>SMTP Service Extension for 8bit-MIMEtransport</i>
RFC 1845	<i>SMTP Service Extension for Checkpoint/Restart</i>
RFC 1869	<i>SMTP Service Extensions</i>
RFC 1870	<i>SMTP Service Extension for Message Size Declaration</i>
RFC 1891	<i>SMTP Service Extension for Delivery Status Notifications</i>
RFC 1985	<i>SMTP Service Extension for Remote Message Queue Starting</i>
RFC 2034	<i>SMTP Service Extension for Returning Enhanced Error Codes</i>
RFC 2554	<i>SMTP Service Extension for Authentication</i>
RFC 2645	<i>ON-DEMAND MAIL RELAY (ODMR) SMTP with Dynamic IP Addresses</i>
RFC 2920	<i>SMTP Service Extension for Command Pipelining</i>
RFC 3030	<i>SMTP Service Extensions for Transmission of Large and Binary MIME Messages</i>
RFC 3207	<i>SMTP Service Extension for Secure SMTP over Transport Layer Security</i>

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 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.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents the following modified command:

- **[ip inspect name](#)**

# ip inspect name

To define a set of inspection rules, use the **ip inspect name** command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

```
ip inspect name inspection-name protocol [alert {on | off}] [audit-trail {on | off}]
[timeout seconds]
```

```
no ip inspect name [inspection-name protocol]
```

## HTTP Inspection Syntax

```
ip inspect name inspection-name http [urlfilter] [java-list access-list] [alert {on | off}]
[audit-trail {on | off}] [timeout seconds]
```

```
no ip inspect name inspection-name protocol
```

## SMTP and ESMTP Inspection Syntax

```
ip inspect name inspection-name {smtp | esmtp} [alert {on | off}] [audit-trail {on | off}]
[max-data number] [timeout seconds]
```

## remote-procedure call (RPC) Inspection Syntax

```
ip inspect name inspection-name rpc program-number number [wait-time minutes] [alert {on |
off}] [audit-trail {on | off}] [timeout seconds]
```

```
no ip inspect name inspection-name protocol
```

## Fragment Inspection Syntax

```
ip inspect name inspection-name fragment [max number timeout seconds]
```

```
no ip inspect name inspection-name fragment
```

Syntax Description	
<i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same <i>inspection-name</i> as the existing set of rules.  <b>Note</b> The <i>inspection-name</i> cannot exceed 16 characters; otherwise, the name will be truncated to the 16-character limit.
<i>protocol</i>	A protocol keyword listed in <a href="#">Table 2</a> or <a href="#">Table 3</a> .
<b>alert {on   off}</b>	(Optional) For each inspected protocol, the generation of alert messages can be set be <b>on</b> or <b>off</b> . If no option is selected, alerts are generated on the basis of the setting of the <b>ip inspect alert-off</b> command.
<b>audit-trail {on   off}</b>	(Optional) For each inspected protocol, <b>audit trail</b> can be set <b>on</b> or <b>off</b> . If no option is selected, an audit trail message are generated on the basis of the setting of the <b>ip inspect audit-trail</b> command.
<b>http</b>	Specifies the HTTP protocol for Java applet blocking.

<b>urlfilter</b>	(Optional) Associates URL filtering with HTTP inspection.
<b>timeout</b> <i>seconds</i>	(Optional) To override the global TCP or User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) idle timeouts for the specified protocol, specify the number of seconds for a different idle timeout.  This timeout overrides the global TCP, UDP, or ICMP timeouts but will not override the global Domain Name System (DNS) timeout.
<b>java-list</b> <i>access-list</i>	(Optional) Specifies the numbered standard access list to use to determine “friendly” sites. This keyword is available only for the HTTP protocol, for Java applet blocking. Java blocking only works with numbered standard access lists.
<b>max-data</b> <i>number</i>	(Optional) 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 will log an alert message and close the session. Default value: 20MB
<b>rpc program-number</b> <i>number</i>	Specifies the program number to permit. This keyword is available only for the remote-procedure call protocol.
<b>wait-time</b> <i>minutes</i>	(Optional) Specifies the number of minutes to keep a small hole in the firewall to allow subsequent connections from the same source address and to the same destination address and port. The default wait-time is zero minutes. This keyword is available only for the remote-procedure call (RPC) protocol.
<b>fragment</b>	Specifies fragment inspection for the named rule.
<b>max</b> <i>number</i>	(Optional) Specifies the maximum number of unassembled packets for which state information (structures) is allocated by Cisco IOS software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. The acceptable range is 50 through 10000. The default is 256 state entries.  Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.
<b>timeout</b> <i>seconds</i> (fragmentation)	(Optional) Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default timeout value is one second.  If this number is set to a value greater than one second, it will be automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.

**Defaults**

No inspection rules are defined until you define them using this command.

**Command Modes**

Global configuration

Command History	Release	Modification
	11.2 P	This command was introduced.
	12.0(5)T	Introduced configurable alert and audit trail, IP fragmentation checking, and NetShow protocol support.
	12.2(11)YU	Support was added for ICMP and SIP protocols and the <b>urlfilter</b> keyword was added to the HTTP inspection syntax.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
	12.3(1)	Skinny protocol support was added.
	12.3(7)T	ESMTP protocol support was added.

## Usage Guidelines

To define a set of inspection rules, enter this command for each protocol that you want the Cisco IOS firewall to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*, which should not exceed the 16-character limit. Define either one or two sets of rules per interface—you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for TCP, UDP, or ICMP as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the **no** form of this command with the specified inspection name and protocol; to remove the entire set of inspection rules, use the **no** form of this command only; that is, do not list any inspection names or protocols.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

### TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session: the entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

### ICMP Inspection

An ICMP inspection session is on the basis of the source address of the inside host that originates the ICMP packet. Dynamic access control lists (ACLs) are created for return ICMP packets of the allowed types (echo-reply, time-exceeded, destination unreachable, and timestamp reply) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet

is wild-carded in the ACL. The wild-card address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

**Table 2 Protocol Keywords—Transport-Layer and Network-Layer Protocols**

Protocol	Keyword
ICMP	<b>icmp</b>
TCP	<b>tcp</b>
UDP	<b>udp</b>

### Application-Layer Protocol Inspection

In general, if you configure inspection for an application-layer protocol, packets for that protocol should be permitted to exit the firewall (by configuring the correct access control list), and packets for that protocol will only be allowed back in through the firewall if they belong to a valid existing session. Each protocol packet is inspected to maintain information about the session state.

Java, H.323, RPC, Session Initiation Protocol (SIP), and SMTP inspection have additional information, described in the next five sections. [Table 3](#) lists the supported application-layer protocols.

**Table 3 Protocol Keywords—Application-Layer Protocols**

Protocol	Keyword
CU-SeeMe	<b>cuseeme</b>
Extended Simple Mail Transfer Protocol (ESMTP)	<b>smtp</b>
FTP	<b>ftp</b>
Java	<b>http</b>
H.323	<b>h323</b>
Microsoft NetShow	<b>netshow</b>
RealAudio	<b>realaudio</b>
RPC	<b>rpc</b>
SIP	<b>sip</b>
Simple Mail Transfer Protocol (SMTP)	<b>smtp</b>
Skinny Client Control Protocol (SCCP)	<b>skinny</b>
StreamWorks	<b>streamworks</b>
Structured Query Language*Net (SQL*Net)	<b>sqlnet</b>
TFTP	<b>tftp</b>
UNIX R commands (rlogin, rexec, rsh)	<b>rcmd</b>
VDOLive	<b>vdolive</b>

### Java Inspection

Java inspection enables Java applet filtering at the firewall. Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as “friendly.” If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. Alternately, you could permit applets from all sites except sites specifically designated as “hostile.”



#### Note

Before you configure Java inspection, you must configure a numbered standard access list that defines “friendly” and “hostile” external sites. You configure this numbered standard access list to permit traffic from friendly sites, and to deny traffic from hostile sites. If you do not configure a numbered standard access list, but use a “placeholder” access list in the **ip inspect name inspection-name http** command, all Java applets will be blocked.



#### Caution

Context-Based Access Control (CBAC) does not detect or block encapsulated Java applets. Therefore, Java applets that are wrapped or encapsulated, such as applets in .zip or .jar format, are *not* blocked at the firewall. CBAC also does not detect or block applets loaded via FTP, gopher, or HTTP on a nonstandard port.

### H.323 Inspection

If you want CBAC inspection to work with NetMeeting 2.0 traffic (an H.323 application-layer protocol), you must also configure inspection for TCP, as described in the chapter “Configuring Context-Based Access Control” in the *Cisco IOS Security Configuration Guide*. This requirement exists because NetMeeting 2.0 uses an additional TCP channel not defined in the H.323 specification.

### RPC Inspection

RPC inspection allows the specification of various program numbers. You can define multiple program numbers by creating multiple entries for RPC inspection, each with a different program number. If a program number is specified, all traffic for that program number will be permitted. If a program number is not specified, all traffic for that program number will be blocked. For example, if you created an RPC entry with the NFS program number, all NFS traffic will be allowed through the firewall.

### SIP Inspection

You can configure SIP inspection to permit media sessions associated with SIP-signaled calls to traverse the firewall. Because SIP is frequently used to signal both incoming and outgoing calls, it is often necessary to configure SIP inspection in both directions on a firewall (both from the protected internal network and from the external network). Because inspection of traffic from the external network is not done with most protocols, it may be necessary to create an additional inspection rule to cause only SIP inspection to be performed on traffic coming from the external network.

### SMTP Inspection

SMTP inspection causes SMTP commands to be inspected for illegal commands. Packets with illegal commands are modified to a “xxxx” pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal SMTP command is any command except the following:

- DATA
- HELO
- HELP

- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

### ESMTP Inspection

Like SMTP, ESMTP inspection also causes the commands to be inspected for illegal commands. Packets with illegal commands are modified to a “xxxx” pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal ESMTP command is any command except the following:

- AUTH
- DATA
- EHLO
- ETRN
- HELO
- HELP
- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

In addition to inspecting commands, the ESMTP firewall also inspects the following extensions via deeper command inspection:

- Message Size Declaration (SIZE)
- Remote Queue Processing Declaration (ETRN)
- Binary MIME (BINARYMIME)
- Command Pipelining
- Authentication
- Delivery Status Notification (DSN)

- Enhanced Status Code (ENHANCEDSTATUSCODE)
- 8bit-MIMEtransport (8BITMIME)

**Note**

SMTP and ESMTP cannot exist simultaneously. An attempt to configure both protocols will result in an error message.

**Use of the `urlfilter` Keyword**

If you specify the **`urlfilter`** keyword, the Cisco IOS firewall will interact with a URL filtering software to control web traffic for a given host or user on the basis of a specified security policy.

**Note**

Enabling HTTP inspection with or without any option triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the **`java-list access-list`** option. Configuring URL filtering without enabling the **`java-list access-list`** option will severely impact performance.

**Use of the `timeout` Keyword**

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

**IP Fragmentation Inspection**

CBAC inspection rules can help protect hosts against certain denial-of-service attacks involving fragmented IP packets. Even though the firewall keeps an attacker from making actual connections to a given host, the attacker may still be able to disrupt services provided by that host. This is done by sending many non-initial IP fragments or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets.

Using fragmentation inspection, the firewall maintains an *interfragment state* (structure) for IP traffic. Non-initial fragments are discarded unless the corresponding initial fragment was permitted to pass through the firewall. Non-initial fragments received before the corresponding initial fragments are discarded.

**Note**

Fragmentation inspection can have undesirable effects in certain cases, because it can result in the firewall discarding any packet whose fragments arrive out of order. There are many circumstances that can cause out-of-order delivery of legitimate fragments. Apply fragmentation inspection in situations where legitimate fragments, which are likely to arrive out of order, might have a severe performance impact.

Because routers running Cisco IOS software are used in a very large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the fragmentation inspection feature is not enabled by default. Fragmentation detection must be explicitly enabled for an inspection rule using the **ip inspect name** command. Unfragmented traffic is never discarded because it lacks a fragment state. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall's fragment state resources, and legitimate, unfragmented traffic can flow through the firewall unimpeded.

**Examples**

The following example causes the software to inspect TCP sessions and UDP sessions, and to specifically allow CU-SeeMe, FTP, and RPC traffic back through the firewall for existing sessions only. For UDP traffic, audit-trail is on. For FTP traffic, the idle timeout is set to override the global TCP idle timeout. For RPC traffic, program numbers 100003, 100005, and 100021 are permitted.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
```

The following example adds fragment checking to software inspection of TCP and UDP sessions for the rule named "myrules." In this example, the firewall software will allocate 100 state structures, and the timeout value for dropping unassembled packets is set to 4 seconds. If 100 initial fragments for 100 different packets are sent through the router, all of the state structures will be used up. The initial fragment for packet 101 will be dropped. Additionally, if the number of free state structures (structures available for use by unassembled packets) drops below the threshold values, 32 or 16, the timeout value is automatically reduced to 2 or 1, respectively. Changing the timeout value frees up packet state structures more quickly.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
ip inspect name myrules fragment max 100 timeout 4
```

The following firewall and SIP example shows how to allow outside-initiated calls and internal calls. For outside-initiated calls, an ACL needs to be punched to allow for the traffic from the initial signaling packet from outside. Subsequent signaling and media channels will be allowed by the inspection module.

```
ip inspect name voip sip
interface FastEthernet0/0
 ip inspect voip in
!
```

```

interface FastEthernet0/1
  ip inspect voip in
  ip access-group 100 in
!
!
access-list 100 permit udp host <gw ip> any eq 5060
access-list 100 permit udp host <proxy ip> any eq 5060
access-list deny ip any any

```

The following example shows two configured inspections named “fw\_only” and “fw\_urlf”; URL filtering will work only on the traffic that is inspected by fw\_urlf. Note that the **java-list access-list** option has been enabled, which disables java scanning.

```

ip inspect name fw_only http java-list 51 timeout 30
interface e0
  ip inspect fw_only in
!
ip inspect name fw_urlf http urlfilter java-list 51 timeout 30
interface e1
  ip inspect fw_urlf in

```

#### Related Commands

Command	Description
<b>ip inspect</b>	Applies a set of inspection rules to an interface.
<b>ip inspect alert-off</b>	Disables CBAC alert messages.
<b>ip inspect audit trail</b>	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

■ ip inspect name