



E-mail Inspection Engine

The E-mail Inspection Engine feature allows the Cisco IOS Firewall to inspect Post Office Protocol 3 (POP3) and Internet Message Access Protocol (IMAP) e-mail, in addition to Simple Mail Transfer Protocol (SMTP) and Extended Simple Mail Transfer Protocol (ESMTP) e-mail which were previously supported.

The **secure-login** enhancement allows people to download external POP3 e-mail only if authentication methods are secure.

Feature History for E-mail Inspection Engine

Release	Modification
12.3(14)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 E-mail Inspection Engine, page 544](#)
- [Restrictions for E-mail Inspection Engine, page 544](#)
- [Information About E-mail Inspection Engine, page 544](#)
- [How to Configure E-mail Inspection Engine, page 546](#)
- [Configuration Examples for E-mail Inspection Engine, page 549](#)
- [Additional References, page 550](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 551](#)
- [Glossary, page 552](#)

Prerequisites for E-mail Inspection Engine

- Configure CBAC.
- Enable SSL VPN tunnels.

Restrictions for E-mail Inspection Engine

None.

Information About E-mail Inspection Engine

To configure E-mail Inspection Engine, you need to understand the following concepts:

- [E-mail Inspection Engine Operation, page 544](#)
- [Inspection, page 545](#)
- [POP3, page 545](#)
- [IMAP Protocol, page 545](#)
- [Client Command Validation, page 546](#)
- [SMTP, page 546](#)
- [SSL, page 546](#)

E-mail Inspection Engine Operation

The client/server communication is validated from the time the TCP connection is initialized until the client is authenticated. The Cisco IOS Firewall uses a state router to track each stage of authentication. After the client is authenticated, the Cisco IOS Firewall allows all the client/server commands without further L7 inspection. TCP L4 inspection continues until the connection is closed. At the end of the e-mail session when the client host quits and before the TCP connection is closed, no further client/server interaction is allowed unless the client is reauthenticated.

During the authentication, any unrecognized command causes the Cisco IOS Firewall to drop the packet and close the connection.

If encryption is negotiated between the client and server control channel, no further validation occurs.

An e-mail client logging in from a nonsecure location may need to use encryption for authentication. For information about secure logins, see the description of the **secure-login** keyword of the **ip inspect name** command.

Inspection

Context Based Access Control (CBAC) inspects traffic that travels through the firewall to discover and manage state information for TCP and User Datagram Protocol (UDP) sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions.

Inspecting packets at the application layer and maintaining TCP and UDP session information provides CBAC with the ability to detect and prevent certain types of network attacks such as SYN-flooding. A SYN-flood attack occurs when a network attacker floods a server with a barrage of requests for connection and does not complete the connection. The resulting volume of half-open connections can overwhelm the server, causing it to deny service to valid requests. Network attacks that deny access to a network device are called denial-of-service (DoS) attacks.

POP3

The Post Office Protocol, Version 3 (POP3) is used to receive e-mail that is stored on a mail server. Unlike IMAP, POP only retrieves mail from a remote host.

POP3 works best when there is only one computer because it supports “offline” message access where messages are downloaded and then deleted from the mail server. This mode of access is not compatible with access from multiple computers because it tends to sprinkle messages across all the computers used for mail access.

With POP3-based e-mail clients, messages are downloaded to the user's local message store and can also be deleted from the mail server. Deletion is optional in most clients. When a new voice message arrives, the subscriber's only immediate notification is the activation of the MWI on the phone. New messages are displayed in the Inbox only after the client's local message store is updated with the Exchange message store. After the subscriber downloads new messages, the message state automatically changes from “new” to “read” on the server, even though the subscriber has not actually listened to the voice messages. MWIs on the subscriber's phone are extinguished, and the message state between the TUI and the subscriber's Inbox are not synchronized.

IMAP Protocol

The Internet Message Access Protocol (IMAP) is a method of accessing electronic mail or bulletin board messages that are kept on a mail server that may be shared. It permits a “client” e-mail program to access remote messages as though they were local. For example, e-mail stored on an IMAP server can be retrieved, sent, and managed from a desktop computer at home, from a workstation at the office, or from a laptop without transferring messages or files back and forth between the computers.

Only the message header and sender information are displayed in the Inbox until the user downloads the entire message, including attachments, from the server. When a new voice message arrives, the subscriber's only immediate notification is the activation of the Message Waiting Indication (MWI) on the phone. New messages are displayed in the Inbox only after the client's local message store is updated with the Exchange message store. When the subscriber listens to a new message by using the telephone user interface (TUI), the MWI is extinguished. In this case again, the message state is not updated in the Inbox until the client's message store is refreshed. However, if the subscriber uses an installed multimedia player to listen to the WaveForm Audio (WAV) attachment from the e-mail client's Inbox, message state changes are automatically synchronized with the TUI.

How message state changes are conveyed to the Cisco Unity subscriber, and how these changes are synchronized with the TUI, depend on whether the subscriber's e-mail client is configured to use POP3 or IMAP4 to access Exchange.

Client Command Validation

The Cisco IOS Firewall authenticates an e-mail client accessing an IMAP or POP3 server before allowing complete access into the server. The firewall searches the IMAP/POP3 TCP stream for valid protocol commands. If the client's commands are outside the protocol's definition, the Cisco IOS Firewall drops the packets and resets the connection.

Client command validation is typically needed in a DeMilitarized Zone (DMZ). Client access is allowed into the DMZ only if the e-mail server validates the user authentication. After the client is authenticated, the client becomes a trusted user and access is permitted.

SMTP

The Simple Mail Transfer Protocol (SMTP) is used to transfer e-mail between servers and clients on the Internet. E-mail clients and mail servers that use protocols other than Message Application Programming Interface (MAPI) can use the SMTP protocol to transfer a message from a client to the server, and then forward it to a message recipient's server. To retrieve, send, and manage these messages from the e-mail client use POP3 or IMAP4.

Cisco Unity uses SMTP to route voice messages via the Internet Voice Connector (IVC) gateway between other Exchange servers that are not connected by using a Site Message Connector. There is an IVC gateway on either end of the SMTP connection between Exchange servers. This ensures that MAPI message attributes survive the outbound transit between SMTP connections. It also ensures that the MIME-encoded attributes survive the inbound transit, and are included with the message stored in the Exchange message store.

SSL

The Secure Socket Layer (SSL) protocol is the standard protocol that delivers secure content over the Internet. It is a point-to-point security protocol that secures communication between a client and a server. SSL usually does not require a special client (that is, a Web browser often will suffice) and it does not require any additional operating system software.

SSL includes client and server authentication and data encryption for a limited set of applications (for example, the Web, e-mail, news, and file transfer). SSL is useful for securing e-commerce transactions over the Internet, and the protocol is well suited for extranets and remote access because it is relatively simple to deploy.

How to Configure E-mail Inspection Engine

This section contains the following procedures:

- [Configuring Firewall Inspection of POP3 or IMAP E-mail, page 547](#) (required)
- [Verifying the E-mail Inspection Engine Configuration, page 548](#) (optional)

Configuring Firewall Inspection of POP3 or IMAP E-mail

To allow the Cisco IOS Firewall to inspect POP3 or IMAP e-mail, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name protocol* [**alert {on | off}**] [**audit-trail {on | off}**][**reset**]
[**secure-login**] [**timeout seconds**]
4. **interface** *type slot/port*
5. **ip inspect name** *inspection-name* {**in** | **out**}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>ip inspect name inspection-name protocol [alert {on off}] [audit-trail {on off}][reset] [secure-login] [timeout seconds]</pre> <p>Example: Router(config)# ip inspect name mail-guard pop3 </p>	Defines a set of inspection rules.
Step 4	<pre>interface type slot/port</pre> <p>Example: Router(config-if)# interface 1/0 </p>	Configures an interface type.
Step 5	<pre>ip inspect name inspection-name {in out}</pre> <p>Example: Router(config-if)# ip inspect name mail-guard in </p>	Enables the Cisco IOS Firewall on an interface.
Step 6	<pre>exit</pre> <p>Example: Router(config-if)# exit </p>	Exits interface configuration mode and returns to global configuration mode.

Verifying the E-mail Inspection Engine Configuration

To verify the E-mail Inspection Engine configuration, perform the following steps.

SUMMARY STEPS

1. **debug ip inspect imap**
2. **debug ip inspect pop3**
3. **show ip inspect {name inspection-name | config | interfaces | session [detail] | all}**

DETAILED STEPS

Step 1 **debug ip inspect imap**

Use this command to display messages about Cisco IOS Firewall events related to IMAP protocol e-mail messages.

```
Router# debug ip inspect imap
```

Step 2 **debug ip inspect pop3**

Use this command to display messages about Cisco IOS Firewall events related to POP3 protocol e-mail messages.

```
Router# debug ip inspect pop3
```

Step 3 **show ip inspect {name *inspection-name* | config | interfaces | session [detail] | all}**

Use this command to view CBAC configuration and session information.

```
Router# show ip inspect
```

```
Session audit trail is disabled
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 mail-guard
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

Configuration Examples for E-mail Inspection Engine

- [Configuring IMAP and POP3 Protocol E-mail: Example, page 549](#)

Configuring IMAP and POP3 Protocol E-mail: Example

The following example configures the Cisco IOS Firewall inspection of IMAP and POP3 protocol e-mail:

```
configure terminal
ip inspect name mail-guard pop3
ip inspect name mail-guard imap
exit
```

The following commands enable this functionality on an interface:

```
configure terminal
interface 1/0
ip inspect name mail-guard in
exit
```

Additional References

The following sections provide references related to E-Mail Inspection Engine.

Related Documents

Related Topic	Document Title
IMAP and POP3	White Paper: <i>Deploying Cisco Unity in Diverse Messaging Environments (All Versions with Microsoft Exchange)</i>
CBAC	<i>Cisco IOS Security Configuration Guide</i> , Release 12.3 <i>Cisco IOS Security Command Reference</i> , Release 12.3T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFCs	Title
RFC 1939	J Myers and M. Rose, "Post Office Protocol, Version 3 (POP3)," May 1996.
RFC 3501	M. Crispin, " <i>Internet Message Access Protocol (IMAP4rev1)</i> ," March 2003.

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.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **debug ip inspect**
- **ip inspect name**
- **show ip inspect**

Glossary

authentication—Process during which any unrecognized command causes the Cisco IOS Firewall to drop the packet and close the connection.

CBAC—Context-Based Access Control. A Cisco IOS Firewall set feature that scrutinizes source and destination addresses to enhance security for TCP and UDP applications that use well-known ports, such as FTP and e-mail traffic.

ESMTP—Extended Simple Mail Transfer Protocol. An extended version of the Simple Mail Transfer Protocol (SMTP), which includes additional functionality, such as delivery notification and session delivery.

IMAP—Internet Message Access Protocol. A method of accessing e-mail or bulletin board messages kept on a mail server that can be shared. IMAP permits client e-mail applications to access remote message stores as if they were local without actually transferring the message.

POP—Post Office Protocol. A protocol that client e-mail applications use to retrieve mail from a mail server.

SMTP—Simple Mail Transfer Protocol. An Internet protocol providing e-mail services.

SSL—Secure Socket Layer Protocol. This protocol is used to deliver secure information over the Internet.

state router—A router that tracks the client/server commands until the client is authenticated.

TCP—Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

UDP—User Datagram Protocol. A connectionless transport-layer protocol for exchanging datagrams without acknowledgments or guaranteed delivery.

VPN—Virtual Private Network. A network that enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN network uses “tunneling” to encrypt all information at the IP level.



Note

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

© 2005 Cisco Systems, Inc. All rights reserved.