ESMTP Support for Cisco IOS Firewall

Last Updated: March 26, 2012

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]).

Finding Feature Information

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

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

Prerequisites for ESMTP Support for Cisco IOS Firewall

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

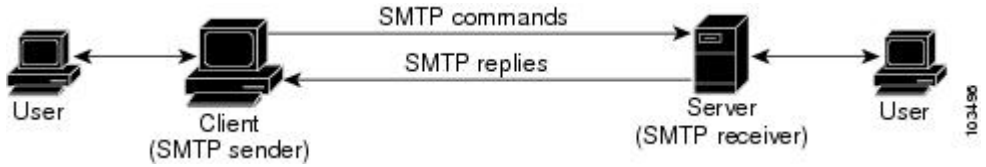
Information About ESMTP Support for Cisco IOS Firewall

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

SMTP Functionality Overview

SMTP inspection provides a basic method for exchanging e-mail messages. The figure below 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 a 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. The table below 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	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. An illegal SMTP command is any command except the following: DATA, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY. **Note** 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.	ESMTP command inspection is the same as SMTP command inspection, except that ESMTP supports three additional commands--AUTH, EHLO, and ETRN. 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.

Functionality	SMTP Firewall Description	ESMTP Firewall Description
Parameter Inspection	Not applicable.	The ESMTP firewall inspects the following extensions by performing 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** All other extensions, including private extensions, are not supported.
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.

Functionality	SMTP Firewall Description	ESMTP Firewall Description
ESMTP to SMTP Session Conversion	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. **Note** 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.	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.	
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.

Functionality	SMTP Firewall Description	ESMTP Firewall Description
Resetting a Connection	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. **Note** 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).	

How to Configure a Firewall to Support ESMTP

Configuring a Firewall for ESMTP Inspection

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

Note 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 | esmtp} [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	**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.

	Command or Action	Purpose
Step 3	ip inspect name inspection-name {smtp | esmtp} [alert {on | off}] [audit-trail {on | off}] [max-data number] [timeout seconds] **Example:** `Router(config)# ip inspect name test esmtp`	Configures inspection of a SMTP or an ESMTP session.
Step 4	**interface** *type number* **Example:** `Router(config)# interface ethernet0`	Configures an interface type and enters interface configuration mode.

Step 5	**ip inspect** *inspection-name* {**in** | **out**}
	
	Example:
	
	`Router(config-if)#`
	`ip inspect test in`
		Applies an inspection rule to an interface.

- Troubleshooting Tips, page 8
- What to Do Next, page 9

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 cha pter “Configuring Context-Based Access Control ” in the *Cisco IOS Security Configuration Guide*

Configuration Examples for Firewall ESMTP Support

Example ESMTP Inspection Configuration

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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*

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: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for ESMTP Support for Cisco IOS Firewall

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

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

Table 2 Feature Information for ESMTP Support for Cisco IOS Firewall

Feature Name	Releases	Feature Information
ESMTP Support for Cisco IOS Firewall	12.3(7)T	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]). The following commands were introduced or modified: **ip inspect name**.