# SMTP and ESMTP Connections Inspection with Cisco IOS Firewall Configuration Example

## Document ID: 69309

## Contents

## Introduction

This document provides a sample configuration for the inspection of inbound Simple Mail Transfer Protocol (SMTP) or Extended Simple Mail Transfer Protocol (ESMTP) connections using Cisco IOS® Firewall in Cisco IOS. Such inspection is similar to the MailGuard feature found in the Cisco PIX 500 Series Security Appliances.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.3(4)T or later
- Cisco 3640 Router

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

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

| | |
|---|---|
| • DATA<br>• HELO<br>• HELP<br>• MAIL<br>• NOOP<br>• QUIT | • RCPT<br>• RSET<br>• SAML<br>• SEND<br>• SOML<br>• VRFY |

ESMTP inspection operates in the same way that SMTP inspection does. Packets with illegal commands are modified to an "xxxx" pattern and forwarded to the server, which triggers a negative reply. An illegal ESMTP command is any command except for these commands:

| | |
|---|---|
| • AUTH<br>• DATA<br>• EHLO<br>• ETRN<br>• HELO<br>• HELP<br>• HELP<br>• MAIL | • NOOP<br>• QUIT<br>• RCPT<br>• RSET<br>• SAML<br>• SEND<br>• SOML<br>• VRFY |

ESMTP inspection also examines these 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)
- 8−bit MIMEtransport (8BITMIME)

**Note:** SMTP and ESMTP inspection cannot be configured simultaneously. An attempt to configure both results in an error message.

**Note:** In Cisco IOS Software Release 12.3(4)T and later, Cisco IOS Firewall no longer creates dynamic access−list entries to permit traffic. Cisco IOS Firewall now maintains a session state table to control the security of inspected connections.

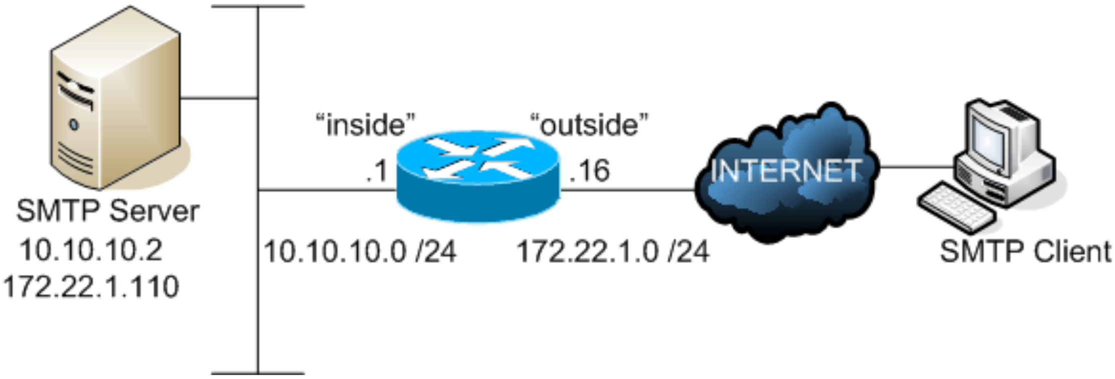
## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

## Network Diagram

This document uses this network setup:



## Configurations

This document uses this configuration:

**3640 Router**

```
3640-123#show running-config
Building configuration...

Current configuration : 1432 bytes
!
version 12.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 3640-123
!
boot-start-marker
boot-end-marker
!
enable password 7 02050D4808095E731F
!
no aaa new-model
!
resource policy
!
voice-card 3
!
ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
!
!

!--- This is the Cisco IOS Firewall configuration.


!--- IN-OUT is the inspection rule for traffic that flows
```

```
!--- from the inside interface of the router to the outside interface.

ip inspect name IN-OUT tcp
ip inspect name IN-OUT udp
ip inspect name IN-OUT ftp
ip inspect name IN-OUT http
ip inspect name IN-OUT icmp


!--- OUT-IN is the inspection rule for traffic that flows
!--- from the outside interface of the router to the inside interface.
!--- This rule is where SMTP/ESMTP inspection is specified.

ip inspect name OUT-IN smtp
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
!
!
controller T1 3/0
 framing sf
 linecode ami
!
!
!
!
!

!--- The outside interface.

interface Ethernet2/0
 ip address 172.22.1.16 255.255.255.0


!--- Apply the access list to permit SMTP/ESMTP connections
!--- to the mail server. This also allows Cisco IOS Firewall
!--- to inspect SMTP or ESMTP commands.

 ip access-group 101 in
 ip nat outside


!--- Apply the inspection rule OUT-IN inbound on this interface.  This is
!--- the rule that defines SMTP/ESMTP inspection.

 ip inspect OUT-IN in
 ip virtual-reassembly
 half-duplex
!
interface Serial2/0
 no ip address
 shutdown
!

!--- The inside interface.

interface Ethernet2/1
 ip address 10.10.10.1 255.255.255.0
 ip nat inside


!--- Apply the inspection rule IN-OUT inbound on this interface.
```

```
 ip inspect IN-OUT in
 ip virtual-reassembly
 half-duplex
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 172.22.1.1
!
!

!--- The static translation for the mail server.

ip nat inside source static 10.10.10.2 172.22.1.110
ip nat inside source static 10.10.10.5 172.22.1.111
!

!--- The access list to permit SMTP and ESMTP to the mail server.
!--- Cisco IOS Firewall inspects permitted traffic.

access-list 101 permit tcp any host 172.22.1.110 eq smtp
!
!
!
control-plane
!
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 password 7 121A0C0411045D5679
 login
!
!
end
```

# Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show ip inspect all** Verifies the configuration of Cisco IOS Firewall inspection rules and their application to interfaces.

```
3640-123#show ip inspect all
```

```
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 IN-OUT
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    ftp alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
    icmp alert is on audit-trail is off timeout 10
 Inspection name OUT-IN
    smtp max-data 20000000 alert is on audit-trail is off timeout 3600

Interface Configuration
 Interface Ethernet2/1
  Inbound inspection rule is IN-OUT
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    ftp alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
    icmp alert is on audit-trail is off timeout 10
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
 Interface Ethernet2/0
  Inbound inspection rule is OUT-IN
    smtp max-data 20000000 alert is on audit-trail is off timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is 101
  Outgoing access list is not set
```

- **debug ip inspect smtp** Displays messages about Cisco IOS Firewall SMTP inspection events.

**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

```
ausnml-3600-02#debug ip inspect smtp
INSPECT SMTP Inspection debugging is on
ausnml-3600-02#
*Oct 18 21:51:35.886: CBAC SMTP: reply_type OTHERS
*Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY - Reply len: 64, match_len:64, reply_re
*Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY match id:10
*Oct 18 21:51:35.886: CBAC SMTP: End Of Reply Line - index:0 ,len:64


!--- The client issues a command.

*Oct 18 21:51:40.810: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:9
*Oct 18 21:51:40.994: CBAC SMTP: VERB - Cmd len:2, match_len:1, cmd_re_state:24
*Oct 18 21:51:41.190: CBAC SMTP: VERB - Cmd len:3, match_len:1, cmd_re_state:40
*Oct 18 21:51:41.390: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:56
*Oct 18 21:51:41.390: CBAC SMTP: VERB - match id:5
*Oct 18 21:51:42.046: CBAC SMTP: CMD PARAM - Cmd len:5, match_len:1, cmd_re_state:7
*Oct 18 21:51:43.462: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:1, cmd_re_state:2
*Oct 18 21:51:43.594: CBAC SMTP: CMD PARAM - Cmd len:7, match_len:1, cmd_re_state:2
*Oct 18 21:51:43.794: CBAC SMTP: CMD PARAM - Cmd len:9, match_len:2, cmd_re_state:2
*Oct 18 21:51:43.994: CBAC SMTP: CMD PARAM - Cmd len:10, match_len:1, cmd_re_state:2
*Oct 18 21:51:44.194: CBAC SMTP: CMD PARAM - Cmd len:12, match_len:2, cmd_re_state:3
*Oct 18 21:51:44.194: CBAC SMTP: CMD PARAM - match id:6
*Oct 18 21:51:44.194: CBAC SMTP: End Of Command Line - index:1, len:12
```

```
!--- The server replies.

*Oct 18 21:51:44.198: CBAC SMTP: reply_type OTHERS
*Oct 18 21:51:44.198: CBAC SMTP: OTHER REPLY - Reply len: 11, match_len:11, reply_re
*Oct 18 21:51:44.198: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:51:44.198: CBAC SMTP: OTHER REPLY match id:10
*Oct 18 21:51:44.198: CBAC SMTP: End Of Reply Line - index:1 ,len:11


!--- The client issues a command.

*Oct 18 21:51:49.482: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:3
*Oct 18 21:51:50.222: CBAC SMTP: VERB - Cmd len:2, match_len:1, cmd_re_state:15
*Oct 18 21:51:50.618: CBAC SMTP: VERB - Cmd len:3, match_len:1, cmd_re_state:31
*Oct 18 21:51:50.954: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:46
*Oct 18 21:51:50.954: CBAC SMTP: VERB - match id:15
*Oct 18 21:51:51.642: CBAC SMTP: CMD PARAM - Cmd len:5, match_len:1, cmd_re_state:7
*Oct 18 21:51:51.914: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:1, cmd_re_state:2
*Oct 18 21:51:52.106: CBAC SMTP: CMD PARAM - Cmd len:7, match_len:1, cmd_re_state:2
*Oct 18 21:51:54.754: CBAC SMTP: CMD PARAM - Cmd len:8, match_len:1, cmd_re_state:4
*Oct 18 21:51:55.098: CBAC SMTP: CMD PARAM - Cmd len:9, match_len:1, cmd_re_state:2
*Oct 18 21:51:55.322: CBAC SMTP: CMD PARAM - Cmd len:11, match_len:2, cmd_re_state:3
*Oct 18 21:51:55.322: CBAC SMTP: CMD PARAM - match id:6
*Oct 18 21:51:55.322: CBAC SMTP: End Of Command Line - index:2, len:11


!--- The server replies.

*Oct 18 21:51:55.326: CBAC SMTP: reply_type OTHERS
*Oct 18 21:51:55.326: CBAC SMTP: OTHER REPLY - Reply len: 19, match_len:19, reply_re
*Oct 18 21:51:55.326: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:51:55.326: CBAC SMTP: End Of Reply Line - index:2 ,len:19

*Oct 18 21:51:57.070: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:3
*Oct 18 21:51:57.402: CBAC SMTP: VERB - Cmd len:2, match_len:1, cmd_re_state:15
*Oct 18 21:51:58.162: CBAC SMTP: VERB - Cmd len:3, match_len:1, cmd_re_state:31
*Oct 18 21:51:58.462: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:46
*Oct 18 21:51:58.466: CBAC SMTP: VERB - match id:15
*Oct 18 21:51:58.746: CBAC SMTP: CMD PARAM - Cmd len:5, match_len:1, cmd_re_state:7
*Oct 18 21:51:59.006: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:1, cmd_re_state:2
*Oct 18 21:51:59.234: CBAC SMTP: CMD PARAM - Cmd len:7, match_len:1, cmd_re_state:2
*Oct 18 21:51:59.418: CBAC SMTP: CMD PARAM - Cmd len:9, match_len:2, cmd_re_state:2
*Oct 18 21:51:59.618: CBAC SMTP: CMD PARAM - Cmd len:10, match_len:1, cmd_re_state:2
*Oct 18 21:51:59.818: CBAC SMTP: CMD PARAM - Cmd len:12, match_len:2, cmd_re_state:3
*Oct 18 21:51:59.818: CBAC SMTP: CMD PARAM - match id:6
*Oct 18 21:51:59.818: CBAC SMTP: End Of Command Line - index:3, len:12

*Oct 18 21:51:59.818: CBAC SMTP: reply_type OTHERS
*Oct 18 21:51:59.818: CBAC SMTP: OTHER REPLY - Reply len: 19, match_len:19, reply_re
*Oct 18 21:51:59.822: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:51:59.822: CBAC SMTP: End Of Reply Line - index:3 ,len:19

*Oct 18 21:52:04.974: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:9
*Oct 18 21:52:05.170: CBAC SMTP: VERB - Cmd len:2, match_len:1, cmd_re_state:24
*Oct 18 21:52:05.326: CBAC SMTP: VERB - Cmd len:3, match_len:1, cmd_re_state:40
*Oct 18 21:52:05.526: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:55
*Oct 18 21:52:05.526: CBAC SMTP: VERB - match id:6
*Oct 18 21:52:05.742: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:2, cmd_re_state:3
*Oct 18 21:52:05.742: CBAC SMTP: CMD PARAM - match id:6
*Oct 18 21:52:05.742: CBAC SMTP: End Of Command Line - index:4, len:6

*Oct 18 21:52:05.746: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY - Reply len: 54, match_len:54, reply_re
*Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:4 ,len:54
```

```
*Oct 18 21:52:05.746: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY - Reply len: 15, match_len:15, reply_re
*Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:5 ,len:15

*Oct 18 21:52:05.746: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY - Reply len: 15, match_len:15, reply_re
*Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:6 ,len:15

*Oct 18 21:52:05.746: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY - Reply len: 6, match_len:6, reply_re_s
*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:7 ,len:6

*Oct 18 21:52:05.750: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY - Reply len: 19, match_len:19, reply_re
*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:8 ,len:19

*Oct 18 21:52:05.750: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY - Reply len: 17, match_len:17, reply_re
*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:9 ,len:17

*Oct 18 21:52:05.750: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY - Reply len: 6, match_len:6, reply_re_s
*Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:10 ,len:6

*Oct 18 21:52:05.754: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY - Reply len: 6, match_len:6, reply_re_s
*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:11 ,len:6

*Oct 18 21:52:05.754: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY - Reply len: 6, match_len:6, reply_re_s
*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:12 ,len:6

*Oct 18 21:52:05.754: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY - Reply len: 3, match_len:3, reply_re_s
*Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:13 ,len:3

*Oct 18 21:52:15.646: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:6
*Oct 18 21:52:15.838: CBAC SMTP: VERB - Cmd len:3, match_len:2, cmd_re_state:37
*Oct 18 21:52:16.206: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:52
*Oct 18 21:52:16.206: CBAC SMTP: VERB - match id:9
*Oct 18 21:52:18.954: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:2, cmd_re_state:3
*Oct 18 21:52:18.958: CBAC SMTP: CMD PARAM - match id:6
*Oct 18 21:52:18.958: CBAC SMTP: End Of Command Line - index:5, len:6

*Oct 18 21:52:18.958: CBAC SMTP: reply_type OTHERS
*Oct 18 21:52:18.958: CBAC SMTP: OTHER REPLY - Reply len: 21, match_len:21, reply_re
*Oct 18 21:52:18.958: CBAC SMTP: OTHER REPLY match id:13
*Oct 18 21:52:18.958: CBAC SMTP: OTHER REPLY match id:10
*Oct 18 21:52:18.958: CBAC SMTP: End Of Reply Line - index:14 ,len:21
```

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## Related Information

- **Cisco IOS Firewall Feature Set Frequently Asked Questions**
- **IOS Firewall Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 03, 2006 Document ID: 69309