Cisco IOS 방화벽 컨피그레이션을 사용한 SMTP 및 ESMTP 연결 검사 예

목차

소개

이 문서는 Cisco IOS에서 Cisco IOS® Firewall을 사용하는 인바운드 SMTP(Simple Mail Transfer Protocol) 또는 ESMTP(Extended Simple Mail Transfer Protocol) 연결 검사를 위한 샘플 컨피그레이션을 제공합니다. 이러한 검사는 Cisco PIX 500 Series Security Appliance에 있는 MailGuard 기능과 유사합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.3(4)T 이상
- Cisco 3640 Router

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

SMTP 검사로 인해 SMTP 명령이 잘못된 명령에 대해 검사됩니다. 잘못된 명령이 있는 패킷은 "xxxx" 패턴으로 수정되고 서버로 전달됩니다. 이 프로세스에서는 서버가 부정적인 회신을 보냅니다. 그러면 클라이언트가 올바른 명령을 실행해야 합니다. 잘못된 SMTP 명령은 다음 명령을 제외한 모든 명령입니다.

• 데이터 • 헬로 • 도움말 • 메일 • NOOP • 종료	• RCPT • RSET • SAML • 전송 • SOML • VRFY

ESMTP 검사는 SMTP 검사가 수행하는 것과 동일하게 작동합니다. 잘못된 명령이 있는 패킷은 "xxxx" 패턴으로 수정되고 서버로 전달되며, 이 경우 음의 회신이 트리거됩니다. 잘못된 ESMTP 명령은 다음 명령을 제외한 모든 명령입니다.

• 인증 • 데이터 • EHLO • ETRN • 헬로 • 도움말 • 도움말 • 메일	• NOOP • 종료 • RCPT • RSET • SAML • 전송 • SOML • VRFY

ESMTP 검사는 심층 명령 검사를 통해 이러한 확장을 검사합니다.

- 메시지 크기 선언(SIZE)
- ETRN(원격 대기열 처리 선언)
- 이진 MIME(BINARYMIME)
- 명령 파이프라인
- 인증
- 배달 상태 알림(DSN)
- 향상된 상태 코드(ENHANCEDSTATUSCODE)
- 8비트 MIMEtransport(8BITMIME)

참고: SMTP 및 ESMTP 검사는 동시에 구성할 수 없습니다. 두 구성 모두 구성하면 오류 메시지가 표시됩니다.

참고: Cisco IOS Software Release 12.3(4)T 이상에서는 Cisco IOS Firewall에서 트래픽을 허용하는 동적 액세스 목록 항목을 더 이상 생성하지 않습니다. Cisco IOS Firewall은 이제 검사된 연결의 보안을 제어하는 세션 상태 테이블을 유지 관리합니다.

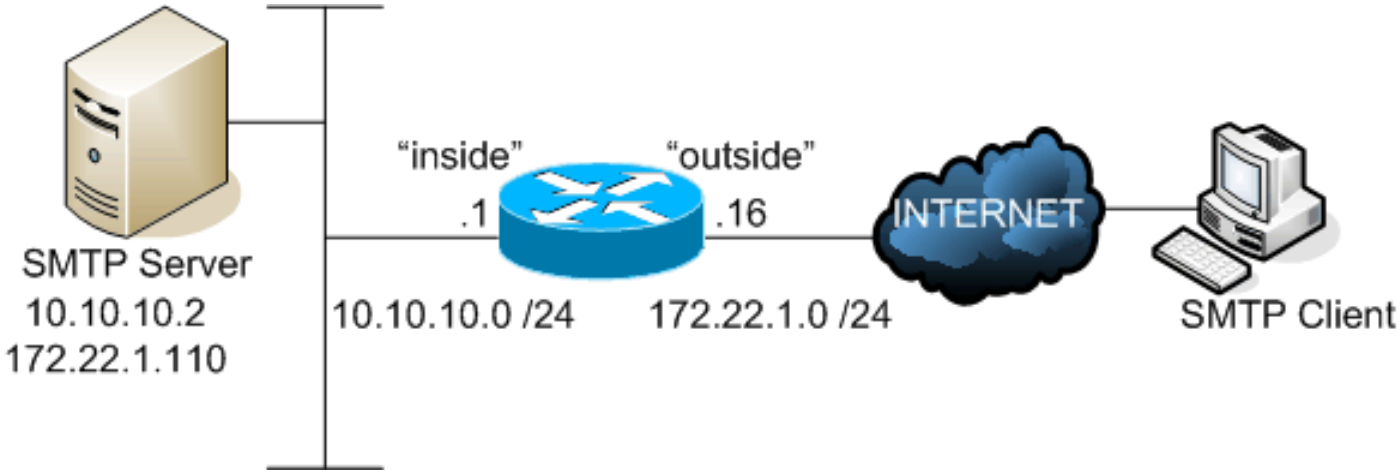
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

3640 라우터

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show ip inspect all** - Cisco IOS Firewall 검사 규칙 및 해당 애플리케이션의 인터페이스를 확인합니다.

```
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** - Cisco IOS Firewall SMTP 검사 이벤트에 대한 메시지를 표시합니다.**참고:** debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

```
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_state:18
*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_state:18 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:3 *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_state:18 *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
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco IOS 방화벽 기능 세트 FAQ
- IOS 방화벽 지원 페이지
- 기술 지원 및 문서 – Cisco Systems