ASA 8.3 이상: DMZ 구성의 메일(SMTP) 서버 액세스 예

목차

소개

이 샘플 컨피그레이션에서는 DMZ(Demilitarized Zone) 네트워크에 있는 SMTP(Simple Mail Transfer Protocol) 서버에 액세스하기 위해 ASA Security Appliance를 설정하는 방법을 보여 줍니다.

ASA 8.3 이상을 참조하십시오. 내부 네트워크 컨피그레이션의 메일(SMTP) 서버 액세스 내부 네트워크에 위치한 메일/SMTP 서버에 액세스하기 위해 ASA Security Appliance를 설정하는 방법에 대한 자세한 내용은 Example을 참조하십시오.

ASA 8.3 이상을 참조하십시오. 외부 네트워크에 있는 메일/SMTP 서버에 액세스하기 위해 ASA Security Appliance를 설정하는 방법에 대한 자세한 내용은 Mail(SMTP) Server Access on Outside Network Configuration Example을 참조하십시오.

PIX/ASA 7.x 이상을 참조하십시오. 버전 8.2 이하의 Cisco ASA(Adaptive Security Appliance)에서 동일한 컨피그레이션을 위한 DMZ 컨피그레이션의 메일(SMTP) 서버 액세스 예

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 8.3 이상을 실행하는 Cisco ASA(Adaptive Security Appliance)
- Cisco 1841 Router with Cisco IOS® Software 릴리스 12.4(20)T

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.

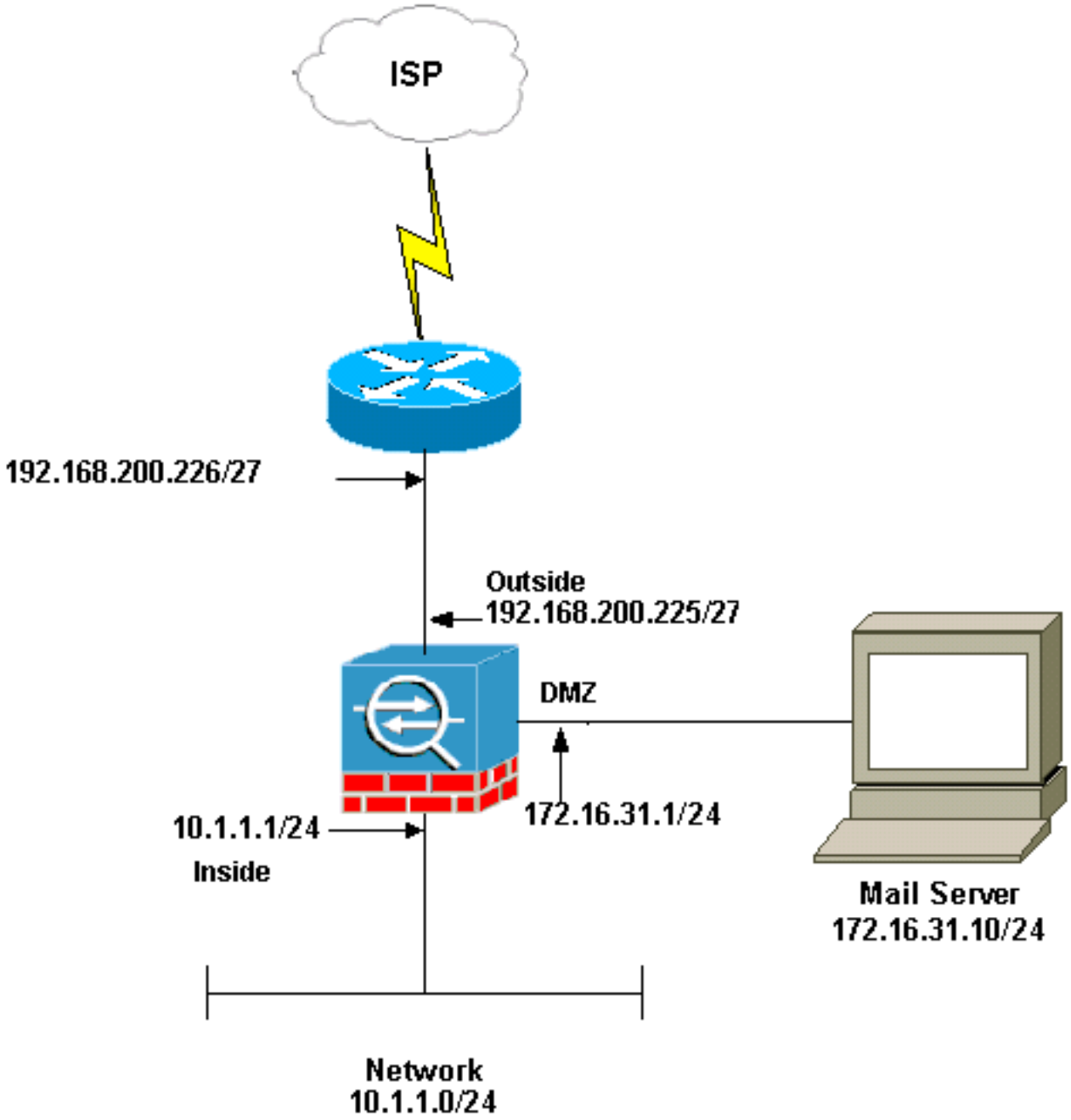
구성

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.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 이는 실습 환경에서 사용된 RFC 1918 주소입니다.

이 예에서 사용된 네트워크 설정에는 내부 네트워크(10.1.1.0/24)과 외부 네트워크(192.168.200.0/27)이 있는 ASA가 있습니다. IP 주소가 172.16.31.10인 메일 서버는 DMZ 네트워크에 있습니다. 내부에서 Mailserver에 액세스하려는 경우 사용자는 ID NAT를 구성합니다. 이 예에서 **dmz_int** 액세스 목록을 구성하여 Mailserver에서 내부 네트워크의 호스트로 나가는 SMTP 연결을 허용하고 이를 DMZ 인터페이스에 바인딩합니다.

마찬가지로, 외부 사용자가 Mailserver에 액세스하도록 하려면 정적 NAT 및 액세스 목록(이 예에서 **outside_int**)을 구성하여 외부 사용자가 Mailserver에 액세스하도록 하고 이 액세스 목록을 외부 인터페이스에 바인딩합니다.

ASA 컨피그레이션

이 문서에서는 다음 구성을 사용합니다.

ASA 컨피그레이션

```
ASA#show run
: Saved
:
ASA Version 8.3(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 no nameif
 no security-level
 no ip address
!
!--- Configure the inside interface. interface Ethernet3
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 192.168.200.225 255.255.255.224 ! !--- Configure
dmz interface. interface Ethernet5 nameif dmz security-
level 10 ip address 172.16.31.1 255.255.255.0 ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa831-
k8.bin ftp mode passive !--- This access list allows
hosts to access !--- IP address 192.168.200.227 for the
SMTP port. access-list outside_int extended permit tcp
any host  192.168.200.227 eq smtp
!--- Allows outgoing SMTP connections. !--- This access
list allows host IP 172.16.31.10 !--- sourcing the SMTP
port to access any host. access-list dmz_int extended
permit tcp host 172.16.31.10 eq smtp any

pager lines 24
mtu BB 1500
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
no asdm history enable
arp timeout 14400


  object network obj-192.168.200.228-192.168.200.253
   range 192.168.200.228-192.168.200.253
 object network obj-192.168.200.254
   host 192.168.200.254

 object-group network nat-pat-group
   network-object object obj-192.168.200.228-
```

```
192.168.200.253
   network-object object obj-192.168.200.254

 object network obj-10.1.1.0
   subnet 10.1.1.0 255.255.255.0
   nat (inside,outside) dynamic nat-pat-group

!--- This network static does not use address
translation. !--- Inside hosts appear on the DMZ with
their own addresses. object network obj-10.1.1.0
   subnet 10.1.1.0 255.255.255.0
   nat (inside,dmz) static obj-10.1.1.0

!--- This network static uses address translation. !---
Hosts that access the mail server from the outside !---
use the 192.168.200.227 address. object network obj-
172.16.31.10
   host 172.16.31.10
   nat (dmz,outside) static 192.168.200.227
access-group outside_int in interface outside
access-group dmz_int in interface dmz
route outside 0.0.0.0 0.0.0.0  192.168.200.226 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
!--- The inspect esmtp command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.


policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
!--- The  inspect esmtp  command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.

service-policy global_policy global
```

```
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda
: end
[OK]
```

ESMTP TLS 컨피그레이션

참고: 이메일 통신에 TLS(Transport Layer Security) 암호화를 사용하는 경우 ASA의 ESMTP 검사 기능(기본적으로 활성화됨)이 패킷을 삭제합니다. TLS가 활성화된 이메일을 허용하려면 이 출력에 표시된 대로 ESMTP 검사 기능을 비활성화합니다. 자세한 내용은 Cisco 버그 ID CSCtn08326(등록된 고객만 해당)을 참조하십시오.

```
ciscoasa(config)#
policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#no inspect esmtp
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

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

- **debug icmp trace** - 호스트의 ICMP(Internet Control Message Protocol) 요청이 ASA에 도달하는지 여부를 표시합니다. 이 디버그를 실행하기 위해 컨피그레이션에서 ICMP를 허용하려면 **access-list** 명령을 추가해야 합니다.**참고:** 이 디버그를 사용하려면 다음 출력에 표시된 대로 `access-list outside_int`에서 ICMP를 허용해야 합니다.
  ```
  access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp
  access-list outside_int extended permit icmp any any
  ```
- **logging buffered 7** - Adaptive Security Appliance가 syslog 메시지를 로그 버퍼로 전송할 수 있도록 전역 컨피그레이션 모드에서 사용됩니다. ASA 로그 버퍼의 내용은 show logging **명령**을 사용하여 확인할 수 있습니다.

로깅을 설정하는 방법에 대한 자세한 내용은 ASDM을 사용하여 Syslog 구성을 참조하십시오.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems