ASA 8.3 en later: Toegang tot een e-mail-server op het DMZ-configuratievoorbeeld

Inhoud

Inleiding

Deze voorbeeldconfiguratie laat zien hoe u de ASA security applicatie kunt instellen voor toegang tot een Simple Mail Transfer Protocol (MTP)-server op het gedemilitariseerde Zone (DMZ) netwerk.

Raadpleeg ASA 8.3 en hoger: Toegang tot een e-mail (mtd) server op de configuratie van het binnennetwerk Voorbeeld voor meer informatie over hoe u de ASA security applicatie kunt instellen voor toegang tot een e-mail/mtd-server die zich op het binnennetwerk bevindt.

Raadpleeg ASA 8.3 en hoger: Toegang tot een e-mail (mtd) server op buitennetwerkconfiguratie Voorbeeld voor meer informatie over hoe u de ASA security applicatie kunt instellen voor toegang tot een e-mail/mtd-server die zich op het netwerk buiten bevindt.

Raadpleeg PIX/ASA 7.x en hoger: Toegang tot de Mail-server (md) op het DMZ Configuration Voorbeeld voor identieke configuratie op Cisco Adaptieve security applicatie (ASA) met versies 8.2 en eerder.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco adaptieve security applicatie (ASA) die versie 8.3 en hoger uitvoert.
- Cisco 1841 router met Cisco IOS-softwarerelease 12.4(20)T

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

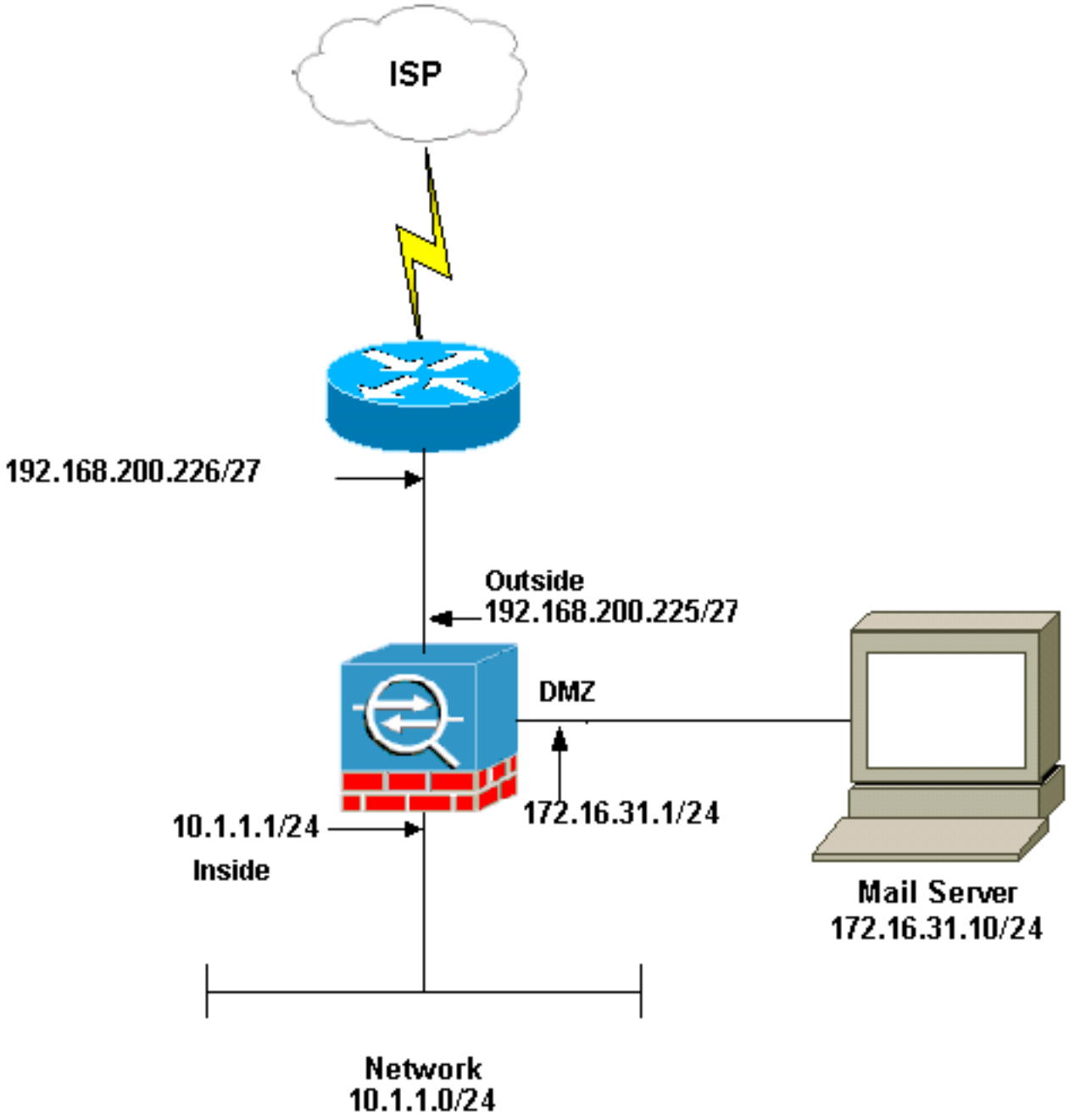
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

De netwerkinstelling die in dit voorbeeld wordt gebruikt heeft de ASA met binnennetwerk (10.1.1.0/24) en het externe netwerk (192.168.200.0/27). De mailserver met IP-adres 172.16.31.10 bevindt zich in het netwerk van gedemilitariseerde zone (DMZ). Om de toegang tot de postserver door de binnenkant te hebben, vormen de gebruikers de identiteit NAT. Configureer een toegangslijst, die **dmz_int** is in dit voorbeeld, om de uitgaande TCP-verbindingen van de postserver naar de hosts in het binnennetwerk toe te staan en verbind deze met de DMZ-interface.

Op dezelfde manier vormt een statische NAT voor de buitengebruikers om toegang te krijgen tot de Brievenserver en ook een toegangslijst, die in dit voorbeeld is **buitenkant_int**, om externe gebruikers toe te staan om tot de Brievenster toegang te hebben en bindt deze toegangslijst aan de buiteninterface.

ASA-configuratie

Dit document gebruikt deze configuratie:

ASA-configuratie

```
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-configuratie

N.B.: Als u TLS-encryptie (Transport Layer Security) voor e-mailcommunicatie gebruikt, dan laat de ESMTP-inspectiemogelijkheid (standaard ingeschakeld) in de ASA de pakketten vallen. Om de e-mails met TLS in staat te stellen, schakelt u de ESMTP-inspectiefunctie uit zoals in deze uitvoer wordt weergegeven. Raadpleeg Cisco bug-ID CSCtn08326 (alleen geregistreerde klanten) voor meer informatie.

```
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
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- debug icmp spoor-toont of de verzoeken van het Protocol van de Controle van Internet Protocol (ICMP) van de hosts de ASA bereiken. U moet de opdracht **toegangslijst** toevoegen om ICMP in uw configuratie toe te staan om dit debug uit te voeren.**Opmerking:** Als u dit debug wilt gebruiken, zorg er dan voor dat u ICMP in de `access-list` toestaat `buiten_int` zoals deze uitvoer toont:
  ```
  access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp
  access-list outside_int extended permit icmp any any
  ```
- houtkap gebufferd op 7—gebruikt in de mondiale configuratiemodus om het adaptieve security apparaat in staat te stellen syslig-berichten naar de logbuffer te sturen. De inhoud van de ASA logbuffer kan worden gezien met de **opdracht** show logging logging.

Raadpleeg het pictogram Configureren met ASDM voor meer informatie over het instellen van de vastlegging.

Gerelateerde informatie

- Adaptieve security applicaties van Cisco ASA 5500 Series
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems