ASA 8.3 und höher: SMTP-Serverzugriff (Mail) im DMZ-Konfigurationsbeispiel

Inhalt

Einführung

Diese Beispielkonfiguration veranschaulicht, wie die ASA Security Appliance für den Zugriff auf einen SMTP-Server (Simple Mail Transfer Protocol) im DMZ-Netzwerk (Demilitarized Zone) eingerichtet wird.

Weitere Informationen finden Sie unter ASA 8.3 und höher: SMTP-Serverzugriff (Mail Server Access on Inside Network Configuration Example für weitere Informationen zum Einrichten der ASA Security Appliance für den Zugriff auf einen Mail-/SMTP-Server im Inside-Netzwerk.

Weitere Informationen finden Sie unter ASA 8.3 und höher: SMTP-Serverzugriff (Mail Server Access on Outside Network Configuration Example für weitere Informationen zum Einrichten der ASA Security Appliance für den Zugriff auf einen Mail-/SMTP-Server im externen Netzwerk.

Weitere Informationen finden Sie unter PIX/ASA 7.x und höher: Mail (SMTP)-Serverzugriff im DMZ-Konfigurationsbeispiel für eine identische Konfiguration auf der Cisco Adaptive Security Appliance (ASA) mit Version 8.2 oder früher.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance (ASA) mit Version 8.3 und höher
- Cisco 1841 Router mit Cisco IOS® Softwareversion 12.4(20)T

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

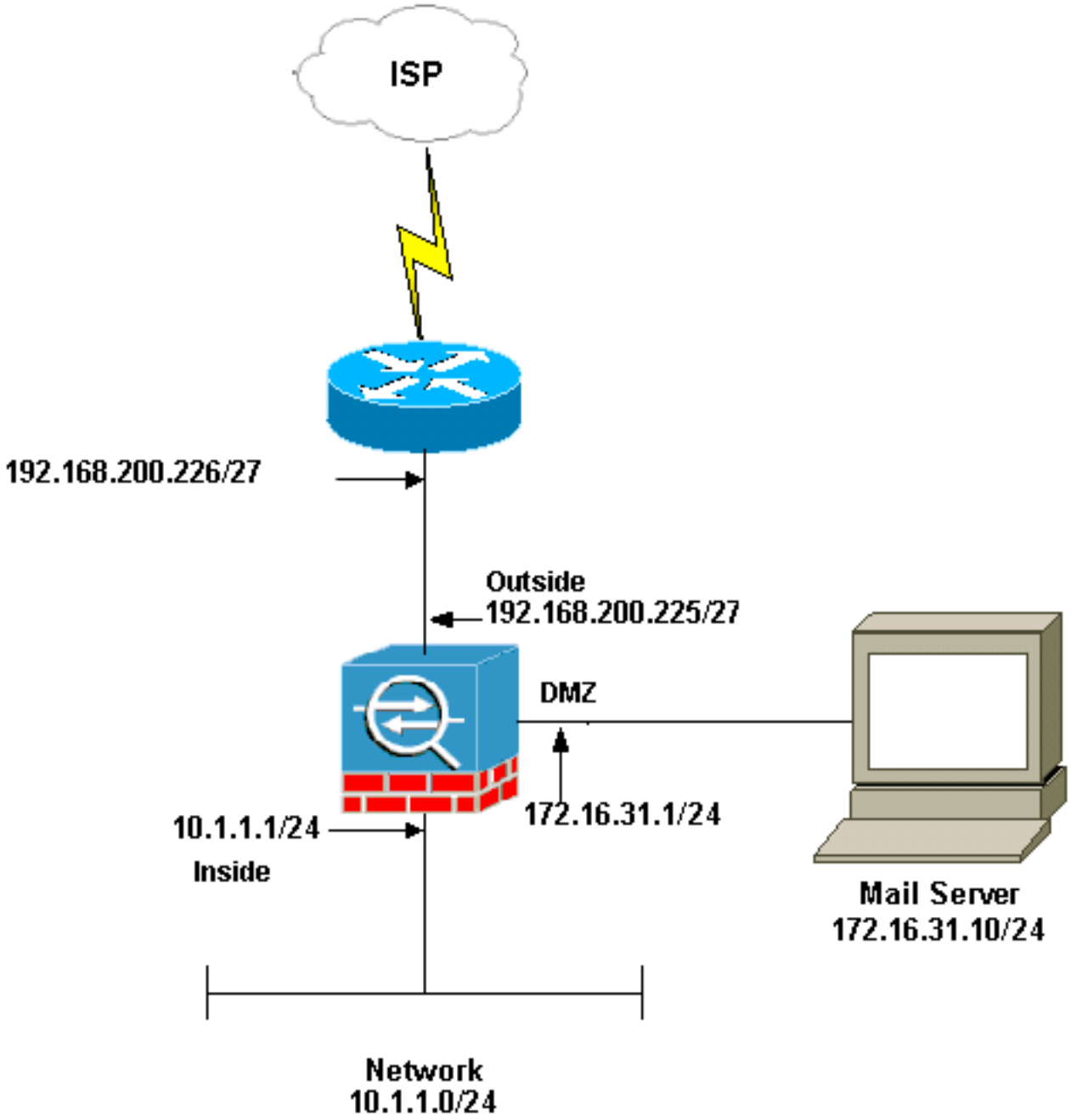
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

Die in diesem Beispiel verwendete Netzwerkeinrichtung hat die ASA mit dem internen Netzwerk (10.1.1.0/24) und dem externen Netzwerk (192.168.200.0/27). Der Mailserver mit der IP-Adresse 172.16.31.10 befindet sich im DMZ-Netzwerk (Demilitarized Zone). Damit auf den Mailserver von innen zugegriffen werden kann, konfigurieren Benutzer die Identität-NAT. Konfigurieren Sie eine Zugriffsliste, die in diesem Beispiel **dmz_int** lautet, um die ausgehenden SMTP-Verbindungen vom Mailserver zu den Hosts im internen Netzwerk zuzulassen und an die DMZ-Schnittstelle zu binden.

Ebenso konfigurieren die externen Benutzer für den Zugriff auf den Mailserver eine statische NAT sowie eine Zugriffsliste, die **außerhalb_int** in diesem Beispiel ist, um externen Benutzern den Zugriff auf den Mailserver zu ermöglichen und diese Zugriffsliste an die externe Schnittstelle zu binden.

ASA-Konfiguration

In diesem Dokument wird diese Konfiguration verwendet:

ASA-Konfiguration

```
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-Konfiguration

Hinweis: Wenn Sie die TLS-Verschlüsselung (Transport Layer Security) für die E-Mail-Kommunikation verwenden, werden die Pakete von der ESMTP-Überprüfungsfunktion (standardmäßig aktiviert) in der ASA verworfen. Um E-Mails mit aktiviertem TLS zuzulassen, deaktivieren Sie die ESMTP-Überprüfungsfunktion, wie in dieser Ausgabe dargestellt. Weitere Informationen finden Sie unter Cisco Bug ID CSCtn08326 (nur registrierte Kunden).

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- debug icmp trace - Zeigt an, ob ICMP-Anfragen (Internet Control Message Protocol) von den Hosts die ASA erreichen. Sie müssen den Befehl **access-list** hinzufügen, um ICMP in Ihrer Konfiguration zuzulassen, damit dieses Debuggen ausgeführt werden kann.**Hinweis:** Um dieses Debuggen zu verwenden, stellen Sie sicher, dass Sie ICMP in der `Zugriffsliste "outside_int"` zulassen, wie diese Ausgabe Folgendes zeigt:
  ```
  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 puffered 7 - Wird im globalen Konfigurationsmodus verwendet, um der adaptiven Sicherheits-Appliance das Senden von Syslog-Meldungen an den Protokollpuffer zu ermöglichen. Der Inhalt des ASA-Protokollpuffers wird mit dem **Befehl show logging** angezeigt.

Weitere Informationen zum Einrichten der Protokollierung finden Sie unter Konfigurieren von Syslog mithilfe von ASDM.

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems