ASA 8.3 en later: Toegang tot een e-mail (mtd) server binnen netwerkconfiguratievoorbeeld

Inhoud

Inleiding

Deze voorbeeldconfiguratie laat zien hoe u de ASA security applicatie voor toegang tot een e-mailserver (mtd) op het binnennetwerk kunt instellen.

Raadpleeg ASA 8.3 en hoger: Toegang tot een e-mail (mtd) server op het DMZ Configuration Voorbeeld voor meer informatie over het instellen van de ASA security applicatie voor toegang tot een e-mail/mtd-server op het DMZ-netwerk.

Raadpleeg ASA 8.3 en hoger: Toegang tot een e-mail (mtd) server op het Voorbeeld van de Configuratie van het Netwerk om de ASA security applicatie voor toegang tot een post/mtd-server op het Buitennetwerk in te stellen.

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

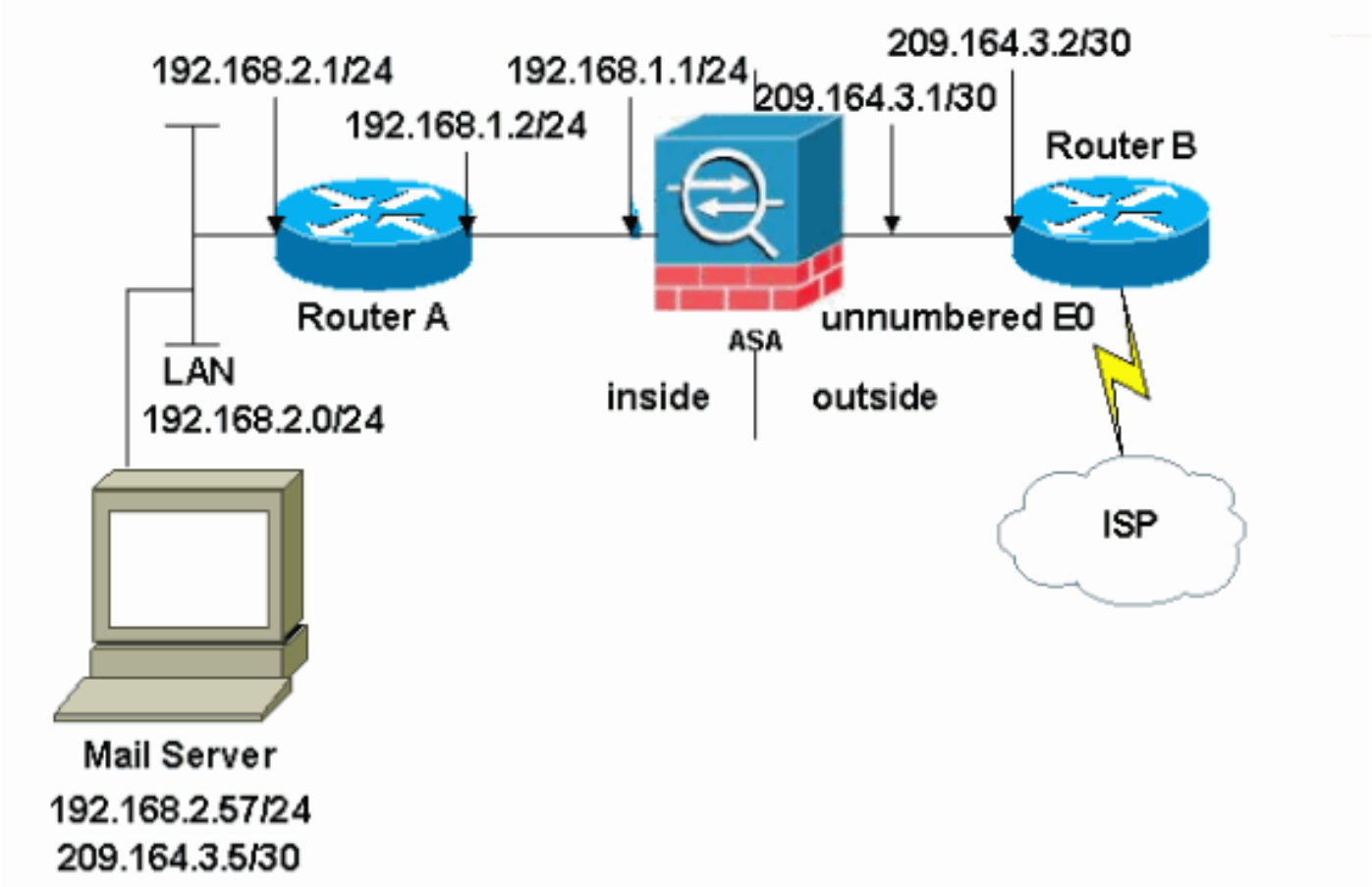
elke opdracht begrijpen.

Configureren

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

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 (192.168.1.0/24) en het externe netwerk (209.164.3.0/30). De mailserver met IP-adres 209.64.3.5 bevindt zich in het interne netwerk.

Configuraties

Dit document gebruikt deze configuraties:

- ASA
- router B

ASA

```
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
 no security-level
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
!--- Define the IP address for the inside interface. interface Ethernet3 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!

!--- Define the IP address for the outside interface. interface Ethernet4 nameif outside
 security-level 0
 ip address 209.164.3.1 255.255.255.252
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- Create an access list that permits Simple !--- Mail Transfer Protocol (SMTP) traffic from anywhere
to the host at 209.164.3.5 (our server). The name of this list is !--- smtp. Add additional lines to th
access list as required. !--- Note: There is one and only one access list allowed per !--- interface pe
direction, for example, inbound on the outside interface. !--- Because of limitation, any additional li
that need placement in !--- the access list need to be specified here. If the server !--- in question i
SMTP, replace the occurrences of SMTP with !--- www, DNS, POP3, or whatever else is required.


access-list smtp extended permit tcp any host 209.164.3.5 eq smtp

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
```

```
arp timeout 14400

!--- Specify that any traffic that originates inside from the !--- 192.168.2.x network NATs (PAT) to
209.164.3.129 if !--- such traffic passes through the outside interface. object network obj-192.168.2.0
  subnet 192.168.2.0 255.255.255.0
  nat (inside,outside) dynamic 209.164.3.129

!--- Define a static translation between 192.168.2.57 on the inside and !--- 209.164.3.5 on the outside
These are the addresses to be used by !--- the server located inside the ASA. object network obj-192.16
  host 192.168.2.57
  nat (inside,outside) static 209.164.3.5

!--- Apply the access list named smtp inbound on the outside interface. access-group smtp in interface
outside

!--- Instruct the ASA to hand any traffic destined for 192.168.x.x !--- to the router at 192.168.1.2. r
inside 192.168.0.0 255.255.0.0 192.168.1.2 1

!--- Set the default route to 209.164.3.2. !--- The ASA assumes that this address is a router address.
outside 0.0.0.0 0.0.0.0 209.164.3.2 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
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
!--- SMTP/ESMTP is inspected as "inspect esmtp" is included in the map. policy-map global_policy class
inspection_default inspect dns maximum-length 512 inspect ftp inspect h323 h225 inspect h323 ras inspec
netbios inspect rsh inspect rtsp inspect skinny inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!

!--- SMTP/ESMTP is inspected as "inspect esmtp" is included in the map. service-policy global_policy gl
Cryptochecksum:f96eaf0268573bd1af005e1db9391284 : end
```

router B

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname 2522-R5
 !
 enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
 !
 ip subnet-zero
 !
```

```
 !
 !
 !
 !
 interface Ethernet0

!--- Sets the IP address of the Ethernet interface to 209.164.3.2. ip address 209.164.3.2 255.255.255.2
interface Serial0 !--- Instructs the serial interface to use !--- the address of the Ethernet interface
the need arises. ip unnumbered ethernet 0 ! interface Serial1 no ip address no ip directed-broadcast ! 
classless !--- Instructs the router to send all traffic !--- destined for 209.164.3.x to 209.164.3.1. i
route 209.164.3.0 255.255.255.0 209.164.3.1

!--- Instructs the router to send !--- all other remote traffic out serial 0. ip route 0.0.0.0 0.0.0.0 
0
 !
 !
 line con 0
  transport input none
 line aux 0
  autoselect during-login
 line vty 0 4
  exec-timeout 5 0
  password ww
  login
 !
 end
```

Opmerking: de configuratie van de router A is niet toegevoegd. U hoeft alleen de IP-adressen op de interfaces te geven en de standaardgateway in te stellen op 192.168.1.1, de interne interface van de ASA.

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 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
```

Opmerking: In ASA versie 8.0.3 en later is de opdracht **allow-tls** beschikbaar om TLS e-mail mogelijk te maken met geïnspecteerd ESMTP ingeschakeld zoals aangegeven wordt:

```
policy-map type inspect esmtp tls-esmtp
parameters
allow-tls
inspect esmtp tls-esmtp
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

De **houtkap buffered 7** opdracht richt berichten naar de ASA console. Als de connectiviteit op de mailserver een probleem is, onderzoek de console debug berichten om de IP adressen van de verzendende en ontvangende stations te plaatsen om het probleem te bepalen.

Gerelateerde informatie

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