ASA 8.3 und höher: Beispiel für den Zugriff auf den Mail-Server (SMTP) in einem externen Netzwerk

Inhalt

Einführung

Diese Beispielkonfiguration enthält Informationen zum Einrichten der Adaptive Security Appliance (ASA) für den Zugriff auf einen Mailserver im externen Netzwerk.

Weitere Informationen finden Sie unter ASA 8.3 und höher: Mail (SMTP)-Serverzugriff im DMZ-Konfigurationsbeispiel für weitere Informationen zum Einrichten der ASA Security Appliance für den Zugriff auf einen Mail-/SMTP-Server im DMZ-Netzwerk.

Weitere Informationen finden Sie unter ASA 8.3 und höher: SMTP-Server-Zugriff auf das interne Netzwerkkonfigurationsbeispiel, um die ASA Security Appliance für den Zugriff auf einen Mail-/SMTP-Server im internen Netzwerk einzurichten.

Weitere Informationen finden Sie unter PIX/ASA 7.x und höher: Mail (SMTP) Server Access on Outside Network Configuration Example für die identische Konfiguration auf der Cisco Adaptive Security Appliance (ASA) mit Version 8.2 und 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® Software, Version 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).

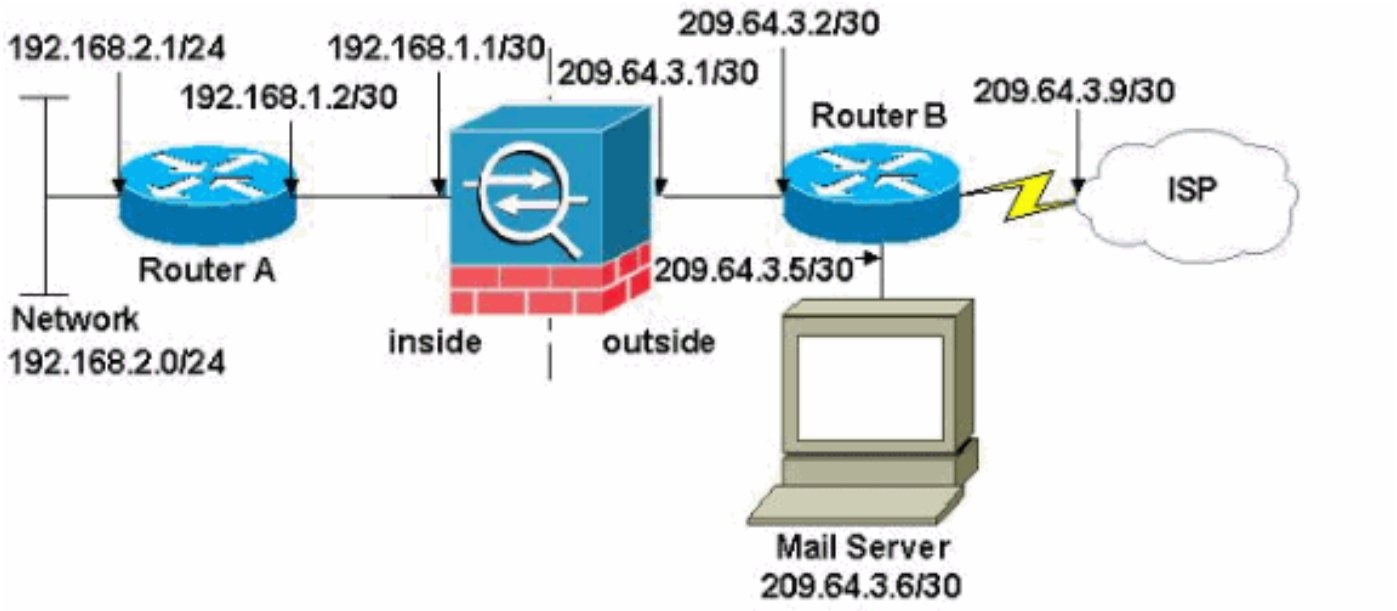
Konfigurieren

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

Hinweis: Verwenden Sie den Cisco CLI Analyzer, um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen abzurufen.

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 internem Netzwerk (192.168.1.0/30) und dem externen Netzwerk (209.64.3.0/30). Der Mailserver mit der IP-Adresse 209.64.3.6 befindet sich im externen Netzwerk. Konfigurieren Sie die NAT-Anweisung so, dass jeder Datenverkehr vom 192.168.2.x-Netzwerk, der von der internen Schnittstelle (Ethernet0) zur

externen Schnittstelle (Ethernet 1) übergeht, in eine Adresse im Bereich von 209.64.3.129 bis 209.64.3.253 umgewandelt wird. Die letzte verfügbare Adresse (209.64.3.254) ist für Port Address Translation (PAT) reserviert.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- ASA
- Router A
- 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
!

!--- Configure the inside interface. ? interface
Ethernet3 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.252
!

!--- Configure the outside interface. interface
Ethernet4 nameif outside
 security-level 0
 ip address 209.64.3.1 255.255.255.252
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
```

```
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa831-k8.bin
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400

!--- This command states that any traffic !--- from the
192.168.2.x network that passes from the inside
interface (Ethernet0) !--- to the outside interface
(Ethernet 1) translates into an address !--- in the
range of 209.64.3.129 through 209.64.3.253 and contains
a subnet !--- mask of 255.255.255.128.   object network
obj-209.64.3.129_209.64.3.253
   range 209.64.3.129-209.64.3.253


!--- This command reserves the last available address
(209.64.3.254) for !--- for Port Address Translation
(PAT). In the previous statement, !--- each address
inside that requests a connection uses one !--- of the
addresses specified. If all of these addresses are in
use, !--- this statement provides a failsafe to allow
additional inside stations !--- to establish
connections. object network obj-209.64.3.254
   host 209.64.3.254

!--- This command indicates that all addresses in the
192.168.2.x range !--- that pass from the inside
(Ethernet0) to a corresponding global !--- designation
are done with NAT. !--- As outbound traffic is permitted
by default on the ASA, no !--- static commands are
needed. object-group network nat-pat-group
   network-object object obj-209.64.3.129_209.64.3.253
   network-object object obj-209.64.3.254

 object network obj-192.168.2.0
   subnet 192.168.2.0 255.255.255.0
   nat (inside,outside) dynamic nat-pat-group

!--- Creates a static route for the 192.168.2.x network
with 192.168.1.2. !--- The ASA forwards packets with
these addresses to the router !--- at 192.168.1.2. route
inside 192.168.2.0 255.255.255.0 192.168.1.2 1

!--- Sets the default route for the ASA Firewall at
209.64.3.2. route outside 0.0.0.0 0.0.0.0 209.64.3.2 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 since "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 inspect
rsh inspect rtsp inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
Cryptochecksum:8a63de5ae2643c541a397c2de7901041
: end
```

Router A

```
Current configuration:
  !
  version 12.4
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
  !
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  !
  interface Ethernet0

!--- Assigns an IP address to the inside Ethernet
interface. ip address 192.168.2.1 255.255.255.0 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the ASA-facing interface. ip address
192.168.1.2 255.255.255.252 no ip directed-broadcast !
interface Serial0 no ip address no ip directed-broadcast
shutdown ! interface Serial1 no ip address no ip
directed-broadcast shutdown ! ip classless !--- This
route instructs the inside router to forward all !---
non-local packets to the ASA. ip route 0.0.0.0 0.0.0.0
192.168.1.1
  !
  !
  line con 0
   transport input none
   line aux 0
   autoselect during-login
   line vty 0 4
```

```
 exec-timeout 5 0
 password ww
 login
!
end
```

Router B

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2522-R4
!
enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
!
ip subnet-zero
!
!
!
!
interface Ethernet0

!--- Assigns an IP address to the ASA-facing Ethernet
interface. ip address 209.64.3.2 255.255.255.252 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the server-facing Ethernet interface. ip
address 209.64.3.5 255.255.255.252 no ip directed-
broadcast ! interface Serial0 !--- Assigns an IP address
to the Internet-facing interface. ip address 209.64.3.9
255.255.255.252 no ip directed-broadcast no ip mroute-
cache ! interface Serial1 no ip address no ip directed-
broadcast ! ip classless !--- All non-local packets are
to be sent out serial 0. In this case, !--- the IP
address on the other end of the serial interface is not
known, !--- or you can specify it here. ip route 0.0.0.0
0.0.0.0 serial 0
!

!--- This statement is required to direct traffic
destined to the !--- 209.64.3.128 network (the ASA
global pool) to the ASA to be translated !--- back to
the inside addresses. ip route 209.64.3.128
255.255.255.128 209.64.3.1
!
!
line con 0
 transport input none
line aux 0
 autoselect during-login
line vty 0 4
 exec-timeout 5 0
 password ww
 login
!
end
```

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.

```
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

Der Cisco CLI Analyzer unterstützt bestimmte **show**-Befehle. Verwenden Sie den CLI Analyzer, um eine Analyse der **Ausgabe** des **Befehls show** anzuzeigen.

Der Befehl **logging puffered 7 leitet Meldungen an die ASA-Konsole weiter.** Wenn die Verbindung zum Mailserver ein Problem darstellt, überprüfen Sie die Debug-Meldungen der Konsole, um die IP-Adressen der sendenden und empfangenden Stationen zu ermitteln, um das Problem zu ermitteln.

Zugehörige Informationen

- Cisco Firewalls der Serie ASA 5500-X
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems