ASA 8.3 이상: 내부 네트워크 구성의 메일(SMTP) 서버 액세스 예

목차

소개

이 샘플 컨피그레이션에서는 내부 네트워크에 있는 메일(SMTP) 서버에 액세스하기 위해 ASA Security Appliance를 설정하는 방법을 보여 줍니다.

ASA 8.3 이상을 참조하십시오. DMZ 네트워크에 있는 메일/SMTP 서버에 액세스하기 위해 ASA Security Appliance를 설정하는 방법에 대한 자세한 내용은 DMZ 구성의 메일(SMTP) 서버 액세스 예를 참조하십시오.

ASA 8.3 이상을 참조하십시오. 외부 네트워크 컨피그레이션의 메일(SMTP) 서버 액세스 외부 네트워크에 위치한 메일/SMTP 서버에 액세스하기 위해 ASA 보안 어플라이언스를 설정하는 예입니다.

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

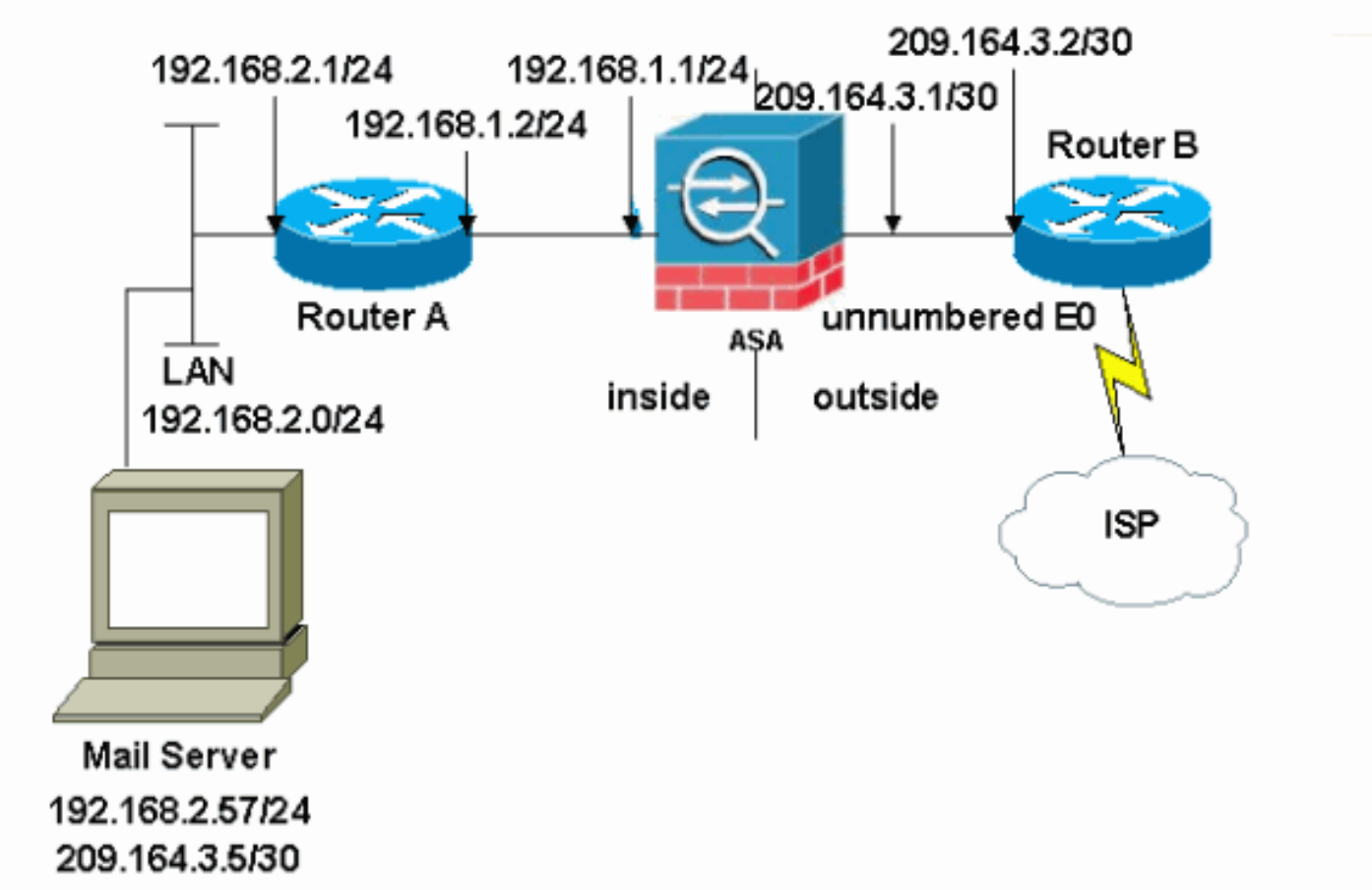
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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(192.168.1.0/24)과 외부 네트워크(209.164.3.0/30)이 있는 ASA가 있습니다. IP 주소가 209.64.3.5인 메일 서버는 내부 네트워크에 있습니다.

구성

이 문서에서는 다음 구성을 사용합니다.

- ASA
- 라우터 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
```

라우터 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
```

참고: 라우터 A 컨피그레이션은 추가되지 않습니다. 인터페이스의 IP 주소를 지정하고 기본 게이트웨이를 192.168.1.1으로 설정하기만 하면 됩니다. 이는 ASA의 내부 인터페이스입니다.

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 CSCtn08326을 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
```

참고: ASA 버전 8.0.3 이상에서는 다음과 같이 **allow-tls** 명령을 사용하여 inspect esmtp가 활성화된 TLS 이메일을 허용할 수 있습니다.

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

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

logging buffered **7** 명령은 메시지를 ASA 콘솔로 전달합니다. 메일 서버와의 연결에 문제가 있는 경

우 콘솔 디버그 메시지를 검사하여 전송 및 수신 스테이션의 IP 주소를 찾아 문제를 확인합니다.

관련 정보

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