

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

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[ESMTP TLS 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 샘플 컨피그레이션은 외부 네트워크에 있는 메일 서버에 액세스하기 위해 ASA(Adaptive Security Appliance)를 설정하는 방법에 대한 정보를 제공합니다.

[ASA 8.3 이상](#)을 참조하십시오. [DMZ 네트워크](#)에 있는 메일/SMTP 서버에 액세스하기 위해 ASA Security Appliance를 설정하는 방법에 대한 자세한 내용은 DMZ [구성의 메일\(SMTP\) 서버 액세스 예](#)를 참조하십시오.

[ASA 8.3 이상](#)을 참조하십시오. [내부 네트워크](#)에 있는 메일/SMTP 서버에 액세스하기 위해 ASA Security Appliance를 설정하기 위한 SMTP(Mail) Server Access on Inside Network Configuration 예시입니다.

[PIX/ASA 7.x 이상](#)을 참조하십시오. Cisco ASA(Adaptive Security Appliance) 버전 8.2 이하의 동일한 컨피그레이션에 대한 [외부 네트워크의 메일\(SMTP\) 서버 액세스](#) 컨피그레이션 예

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

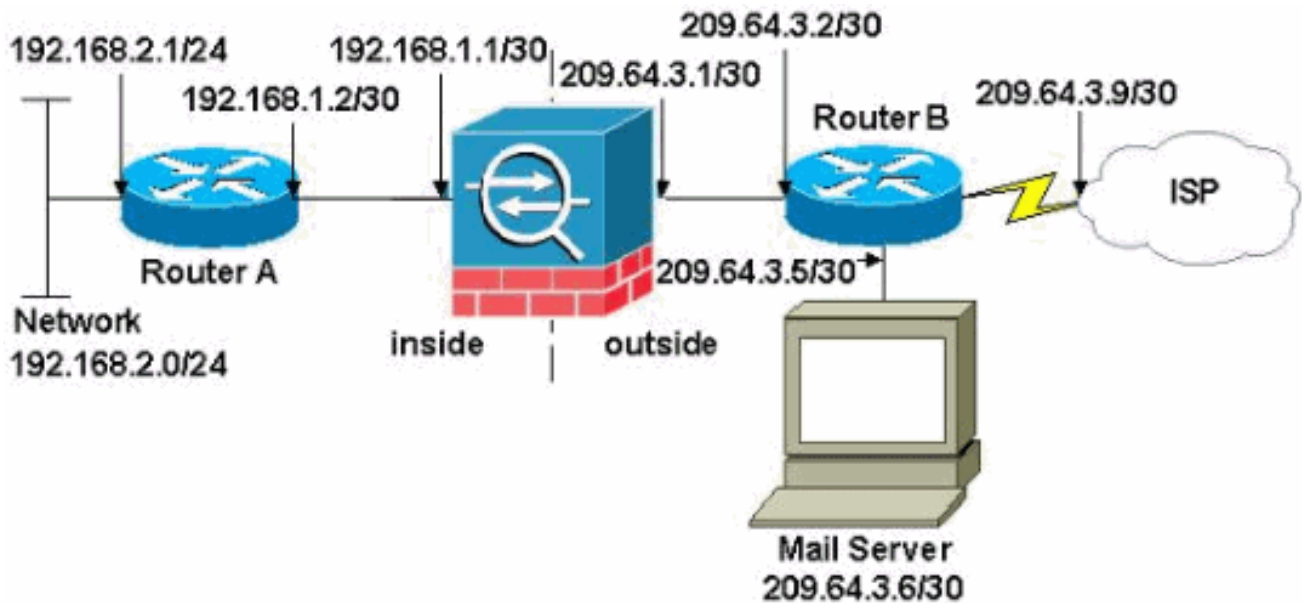
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: [Cisco CLI Analyzer](#)를 사용하여 이 섹션에서 사용하는 명령에 대한 자세한 내용을 확인하십시오.

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(192.168.1.0/30)와 외부 네트워크(209.64.3.0/30)가 있는 ASA가 있습니다. IP 주소가 209.64.3.6인 메일 서버는 외부 네트워크에 있습니다. 내부 인터페이스(Ethernet0)에서 외부 인터페이스(이더넷 1)로 전달되는 192.168.2.x 네트워크의 모든 트래픽이 209.64.3.129 ~ 209.64.3.253 범위의 주소로 변환되도록 NAT 문을 구성합니다. 마지막 사용 가능한 주소(209.64.3.254)은 PAT(Port Address Translation)용으로 예약됩니다.

구성

이 문서에서는 다음 구성을 사용합니다.

- [ASA](#)
- [라우터 A](#)
- [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
!
!--- 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
```

라우터 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
```

라우터 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 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
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

[Cisco CLI Analyzer](#)는 특정 **show** 명령을 지원합니다. CLI Analyzer를 사용하여 **show** 명령 출력의 분석을 봅니다.

logging buffered **7** 명령은 메시지를 ASA 콘솔로 전달합니다. 메일 서버와의 연결에 문제가 있는 경우 콘솔 디버그 메시지를 검사하여 전송 및 수신 스테이션의 IP 주소를 찾아 문제를 확인합니다.

관련 정보

- [Cisco ASA 5500-X Series 방화벽](#)
- [RFC\(Request for Comments\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)