PIX/ASA 7.x 이상: 외부 네트워크 구성의 메일 (SMTP) 서버 액세스 예

목차

소개

이 샘플 컨피그레이션에서는 외부 네트워크에 있는 메일 서버에 액세스하기 위해 PIX 방화벽을 설정하는 방법을 보여 줍니다.

PIX/ASA 7.x 이상을 참조하십시오. 내부 네트워크에 있는 메일/SMTP 서버에 액세스하기 위해 PIX/ASA Security Appliance를 설정하기 위한 Mail Server Access on Inside Network Configuration의 예

DMZ 네트워크에 있는 메일/SMTP 서버에 액세스하기 위해 PIX/ASA Security Appliance를 설정하려면 DMZ 네트워크에서 Mail Server Access가 있는 PIX/ASA 7.x를 참조하십시오.

ASA 8.3 이상을 참조하십시오. 버전 8.3 이상의 Cisco ASA(Adaptive Security Appliance)에서 동일한 컨피그레이션에 대한 자세한 내용은 외부 네트워크의 메일(SMTP) 서버 액세스 컨피그레이션 예를 참조하십시오.

Microsoft Exchange 설정 방법에 대한 자세한 내용은 Cisco Secure PIX Firewall 문서를 참조하십시오. 소프트웨어 버전을 선택한 다음 구성 가이드로 이동하여 Microsoft Exchange 구성 방법에 대한 장을 읽습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX Firewall 535
- PIX Firewall 소프트웨어 릴리스 7.1(1)
- Cisco 2500 라우터

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 규칙을 참조하십시오.

관련 제품

이 컨피그레이션은 버전 7.x 이상을 실행하는 ASA(Adaptive Security Appliance)와 함께 사용할 수도 있습니다.

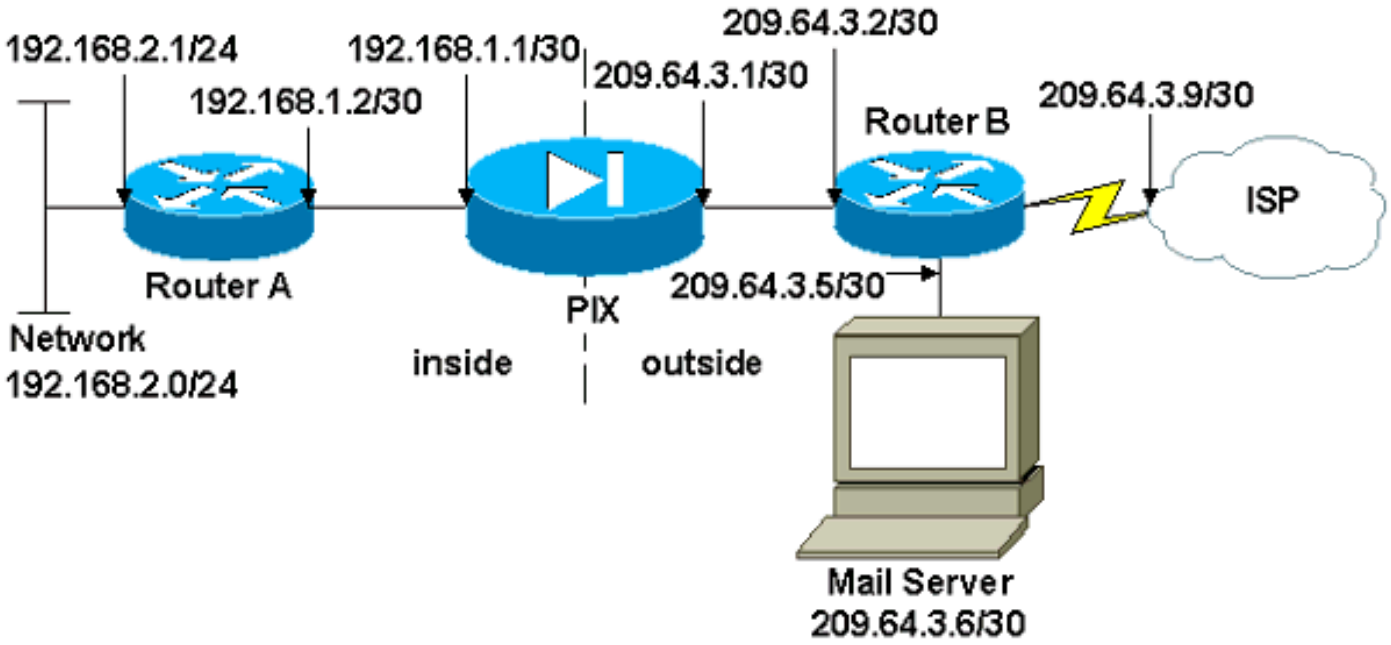
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: Cisco CLI Analyzer를 사용하여 이 섹션에서 사용하는 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- PIX 방화벽
- 라우터 A
- 라우터 B

PIX 방화벽

```
PIX Version 7.1(1)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 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 192.168.1.1 255.255.255.252
!

!--- Define the IP address for 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
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400
```

```
!--- This command defines the global for the Network
Address Translation !--- (NAT) statement. In this case,
the two commands state 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. global (outside)
1 209.64.3.129-209.64.3.253 netmask 255.255.255.128

!--- 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. global (outside) 1 209.64.3.254

!--- 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 PIX, no !--- static commands are
needed. nat (inside) 1 192.168.2.0 255.255.255.0

!--- Creates a static route for the 192.168.2.x network
with 192.168.1.2. !--- The PIX 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 PIX 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 12.0
  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 PIX-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 PIX. 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 12.0
  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 PIX-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 PIX
global pool) to the PIX 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 PIX의 ESMTP 검사 기능(기본적으로 활성화됨)이 패킷을 삭제합니다. TLS가 활성화된 이메일을 허용하려면 이 출력에 표시된 대로 ESMTP 검사 기능을 비활성화합니다.

```
pix(config)#policy-map global_policy
pix(config-pmap)#class inspection_default
pix(config-pmap-c)#no inspect esmtp
pix(config-pmap-c)#exit
pix(config-pmap)#exit
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

Cisco CLI Analyzer는 특정 **show** 명령을 지원합니다. CLI Analyzer를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

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

관련 정보

- Cisco PIX 방화벽을 통한 연결 설정
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- Cisco ASA 5500-X Series 방화벽
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems