

PIX/ASA 7.x en later: Toegang tot een e-mail (mtd) server buiten Network Configuration Voorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Verwante producten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[ESMTP-TLS-configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Deze voorbeeldconfiguratie laat zien hoe u de PIX-firewall kunt instellen voor toegang tot een mailserver op het externe netwerk.

Raadpleeg [PIX/ASA 7.x en hoger: Toegang tot mailservers op de binnennetwerkconfiguratie Voorbeeld](#) om de PIX/ASA security applicatie in te stellen voor toegang tot een mail/MTP server die zich op het binnennetwerk bevindt.

Raadpleeg [PIX/ASA 7.x met Mail Server Access op DMZ Network Configuration Voorbeeld](#) om de PIX/ASA security applicatie in te stellen voor toegang tot een e-mail/MTP server op het DMZ-netwerk.

Raadpleeg [ASA 8.3 en hoger: Toegang tot een e-mail-server \(mtd\) op buitennetwerkconfiguratie Voorbeeld](#) voor meer informatie over de identieke configuratie op Cisco adaptieve security applicatie (ASA) met versie 8.3 en hoger.

Raadpleeg de [documentatie bij Cisco Secure PIX-firewall](#) voor meer informatie over het instellen van Microsoft Exchange. Kies uw softwareversie, ga dan naar de configuratiehandleiding en lees het hoofdstuk over hoe u voor Microsoft Exchange moet configureren.

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:

- PIX-firewall 535
- PIX-firewall-software release 7.1(1)E
- Cisco 2500 routers

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.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Verwante producten

Deze configuratie kan ook worden gebruikt met een adaptieve security applicatie (ASA) die versie 7.x en hoger uitvoert.

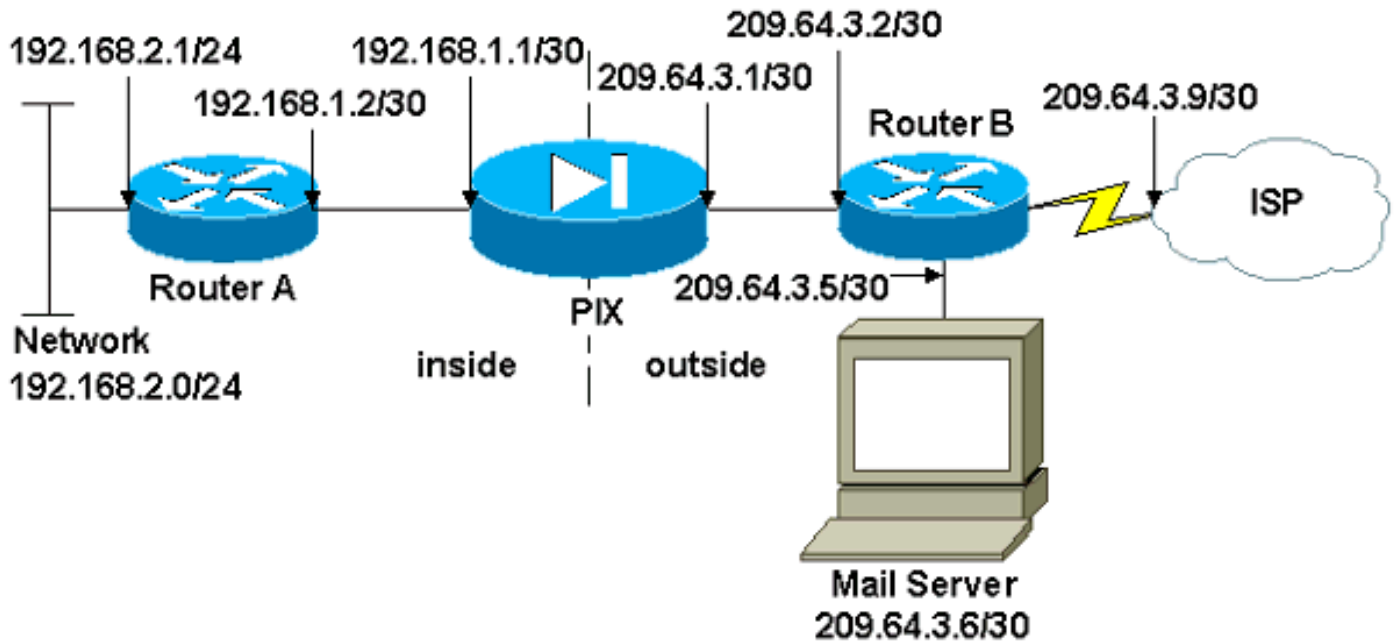
Configureren

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

Opmerking: Gebruik de [Cisco CLI Analyzer](#) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- [PIX-firewall](#)
- [router A](#)
- [router B](#)

PIX-firewall

```

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  
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  
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  
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  
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  
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 12.0
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
```

router 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$XE2aJhJlCbLWY1oDwNvcV.  
!  
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-configuratie

N.B.: Als u TLS-encryptie (Transport Layer Security) voor e-mailcommunicatie gebruikt, dan druppelt de ESMTP-inspectiemogelijkheid (standaard ingeschakeld) in PIX de pakketten af. Om de e-mails met TLS in staat te stellen, schakelt u de ESMTP-inspectiefunctie uit zoals in deze uitvoer wordt weergegeven.

```
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
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

De [Cisco CLI Analyzer](#) ondersteunt bepaalde opdrachten voor tonen. Gebruik CLI Analyzer om een analyse van de opdrachtoutput te bekijken.

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u debug-opdrachten gebruikt.

De opdracht **het** foutoptreden van de **houtkapconsole** richt berichten naar de PIX-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

- [Het bereiken van connectiviteit door de Firewalls van Cisco PIX](#)
- [Cisco PIX-firewallsoftware](#)
- [Opdrachtreferenties van Cisco Secure PIX-firewall](#)
- [Cisco ASA 5500-X Series Next-Generation Firewalls](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)