PIX-to-PIX volledig gemonteerd in PIX IPSec configureren

Inhoud

Inleiding

Deze configuratie maakt het mogelijk dat particuliere netwerken achter drie Cisco Secure PIX-firewallboxen door VPN-tunnels via het internet of een openbaar netwerk dat IPsec gebruikt, worden aangesloten. Elk van de drie netwerken heeft connectiviteit op de andere twee netwerken. In dit scenario is NAT (Network Address Translation) vereist voor verbindingen met het openbare internet. NAT is echter niet vereist voor verkeer tussen de drie intranets, die kunnen worden doorgegeven met behulp van een VPN-tunnel via het openbare internet.

Voorwaarden

Vereisten

Voor IPsec om te werken moet u connectiviteit hebben van tunneleindpunt tot tunneleindpunt voordat u deze configuratie begint.

Gebruikte componenten

Deze configuratie is ontwikkeld en getest met PIX-firewall versie 6.1(2).

Opmerking: de opdracht **Show versie** moet tonen dat encryptie is ingeschakeld.

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.

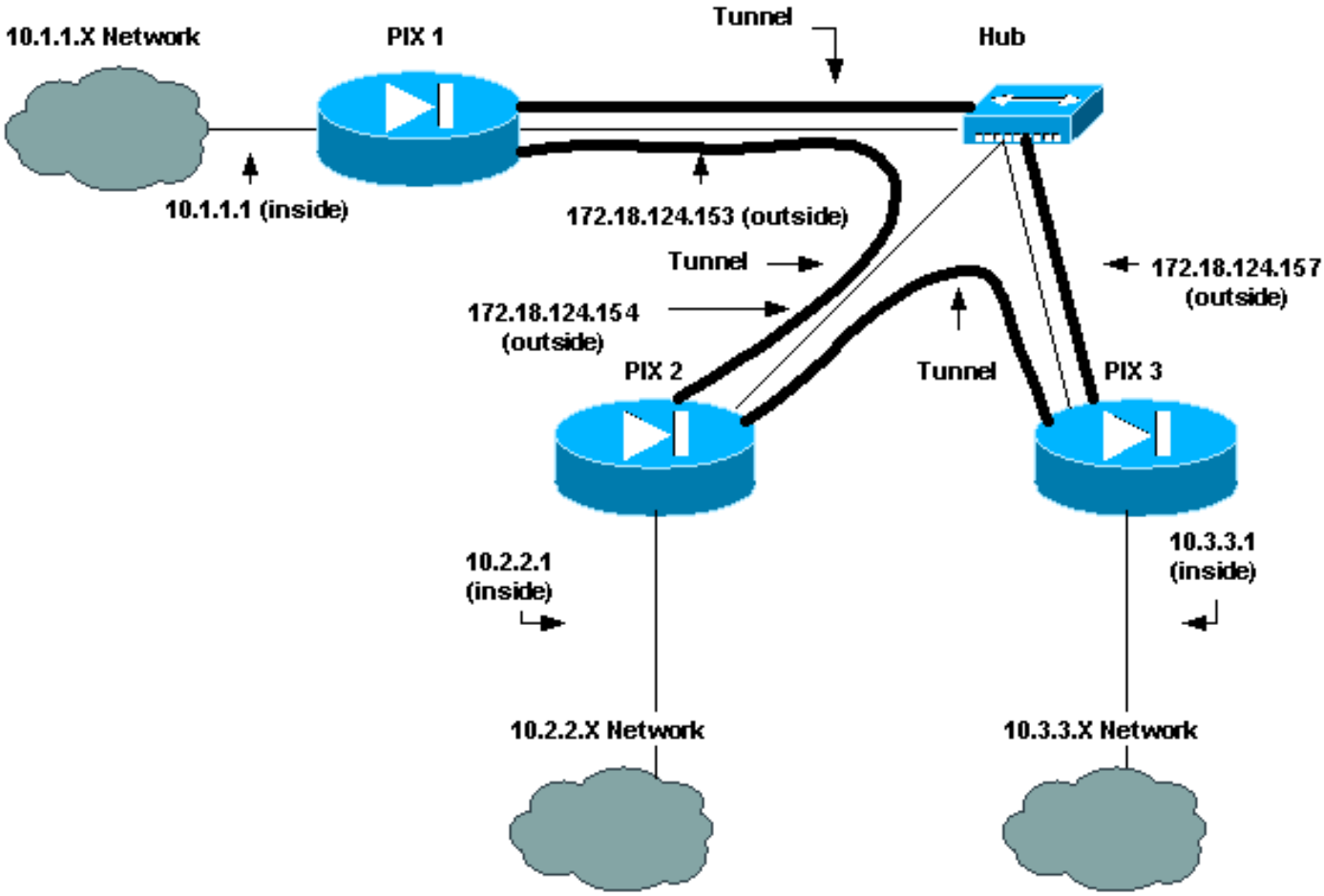
Configureren

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

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- PIX 1
- PIX 2

- PIX 3

PIX 1-configuratie

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_1
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- Traffic to PIX 2 private network: access-list 120
permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!--- Traffic to PIX 3 private network: access-list 130
permit ip 10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
!--- Do not perform NAT for traffic to !--- other PIX
Firewall private networks: access-list 100 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
access-list 100 permit ip 10.1.1.0 255.255.255.0
10.3.3.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.153 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
!--- Do not perform NAT for traffic to other PIX
Firewalls: nat (inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
   0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
```

```
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- IPsec configuration for tunnel to PIX 2: crypto map
newmap 20 ipsec-isakmp
crypto map newmap 20 match address 120
crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset
!--- IPsec configuration for tunnel to PIX 3: crypto map
newmap 30 ipsec-isakmp
crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157
crypto map newmap 30 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
isakmp key ******** address 172.18.124.154 netmask
255.255.255.255
   no-xauth no-config-mode
isakmp key ******** address 172.18.124.157 netmask
255.255.255.255
   no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:436c96500052d0276324b9ef33221b2d
: end
[OK]
```

PIX 2-configuratie

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_2
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- Traffic to PIX 1: access-list 110 permit ip
10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
!--- Traffic to PIX 3: access-list 130 permit ip
10.2.2.0 255.255.255.0 10.3.3.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewalls: access-list 100 permit ip 10.2.2.0
255.255.255.0 10.1.1.0 255.255.255.0
access-list 100 permit ip 10.2.2.0 255.255.255.0
```

```
10.3.3.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.154 255.255.255.0
ip address inside 10.2.2.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
!--- Do not perform NAT for traffic to other PIX
Firewalls: nat (inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
   0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- IPsec configuration for tunnel to PIX 1: crypto map
newmap 10 ipsec-isakmp
crypto map newmap 10 match address 110
crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset
!--- IPsec configuration for tunnel to PIX 3: crypto map
newmap 30 ipsec-isakmp
crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157
crypto map newmap 30 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
isakmp key ******** address 172.18.124.153 netmask
255.255.255.255
   no-xauth no-config-mode
isakmp key ******** address 172.18.124.157 netmask
255.255.255.255
   no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
```

```
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:aef12453a0ea29b592dd0d395de881f5
: end
```

PIX 3-configuratie

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_3
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- IPsec configuration for tunnel to PIX 1: access-
list 110 permit ip 10.3.3.0 255.255.255.0 10.1.1.0
255.255.255.0
!--- IPsec configuration for tunnel to PIX 2: access-
list 120 permit ip 10.3.3.0 255.255.255.0 10.2.2.0
255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewalls: access-list 100 permit ip 10.3.3.0
255.255.255.0 10.2.2.0 255.255.255.0
access-list 100 permit ip 10.3.3.0 255.255.255.0
10.1.1.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.3.3.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
!--- Do not perform NAT for traffic to other PIX
```

```
Firewalls: nat (inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
   0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- IPsec configuration for tunnel to PIX 1: crypto map
newmap 10 ipsec-isakmp
crypto map newmap 10 match address 110
crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset
!--- IPsec configuration for tunnel to PIX 2: crypto map
newmap 20 ipsec-isakmp
crypto map newmap 20 match address 120
crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
isakmp key ******** address 172.18.124.153 netmask
255.255.255.255
   no-xauth no-config-mode
isakmp key ******** address 172.18.124.154 netmask
255.255.255.255
   no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:e6ad75852dff21efdb2d24cc95ffbe1c
: end
[OK]
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. Raadpleeg Problemen oplossen bij de PIX om gegevensverkeer via een ingesteld IPsec-tunnelbestand uit te voeren voor meer informatie.

Opdrachten voor troubleshooting

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

Opdrachten debug

Gebruik deze opdrachten in de PIX, met de opdrachten **voor het** fouilleren van de **houtkapmonitor** of het **registreren van** de **console**.

- **debug van crypto ipsec**: debugs verwerking van IPsec.
- **debug van crypto isakmp**-Debugs: Internet Security Association en Key Management Protocol (ISAKMP)-verwerking.
- **debug van crypto motor**-displays debug-berichten over crypto motoren, die encryptie en decryptie uitvoeren.

duidelijke opdrachten

Om veiligheidsassociaties (SAs) te ontruimen, gebruik deze opdrachten in de configuratiewijze van de PIX.

- **Schakel [crypto] ipsec sa**-Verwijdert de actieve IPsec SAs. Het sleutelwoord crypto is optioneel.
- **helder [crypto] isakmp sa**—Verwijdert de actieve Internet Key Exchange (IKE) SA's. Het sleutelwoord crypto is optioneel.

Opmerking: Voor IPsec moet u connectiviteit hebben van tunneleindpunt tot tunneleindpunt voordat u met deze configuratie begint.

Gerelateerde informatie

- Probleemoplossing voor de PIX om gegevensverkeer via een ingestelde IPSec-tunnelband door te geven
- Cisco PIX 500 Series security applicaties
- PIX-opdrachtreferenties
- IPsec-onderhandeling/IKE-protocollen
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems