PIX-to-PIX-to-PIX IPSec 구성(허브 및 스포크)

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[구성](#)
[네트워크 다이어그램](#)
[구성](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[문제 해결 명령](#)
[보안 연결 지우기](#)
[관련 정보](#)

소개

이 컨피그레이션을 사용하면 중앙 Cisco Secure PIX Firewall이 인터넷을 통해 또는 IPsec을 사용하는 공용 네트워크를 통해 VPN 터널을 통해 다른 두 PIX Firewall 상자 뒤의 네트워크와 통신할 수 있습니다. 두 외부 네트워크는 서로 통신할 필요가 없지만 중앙 네트워크에 연결되어 있습니다. 두 외부 네트워크는 중앙 PIX를 통해 통신할 수 없습니다. PIX는 하나의 인터페이스에서 수신된 트래픽을 동일한 인터페이스로 다시 라우팅하지 않기 때문입니다. 외부 네트워크가 서로 통신해야 하는 경우 이 문서에 표시된 허브 및 스포크 컨피그레이션 대신 완전히 메시 컨피그레이션이 필요합니다. 이미 PIX에 **nat 1**, **global**, **static** 및 **전달문이** 있을 수 있습니다. 이 예에서는 암호화 추가만 보여줍니다.

사전 요구 사항

요구 사항

IPsec이 작동하려면 이 컨피그레이션을 시작하기 전에 터널 엔드포인트 간 연결을 설정해야 *합니다*.

사용되는 구성 요소

이 문서의 정보는 PIX Firewall 버전 5.1.x, 5.2.x 및 6.3.3을 기반으로 합니다.

참고: show **version** 명령은 암호화가 활성화되어 있음을 나타내야 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 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.

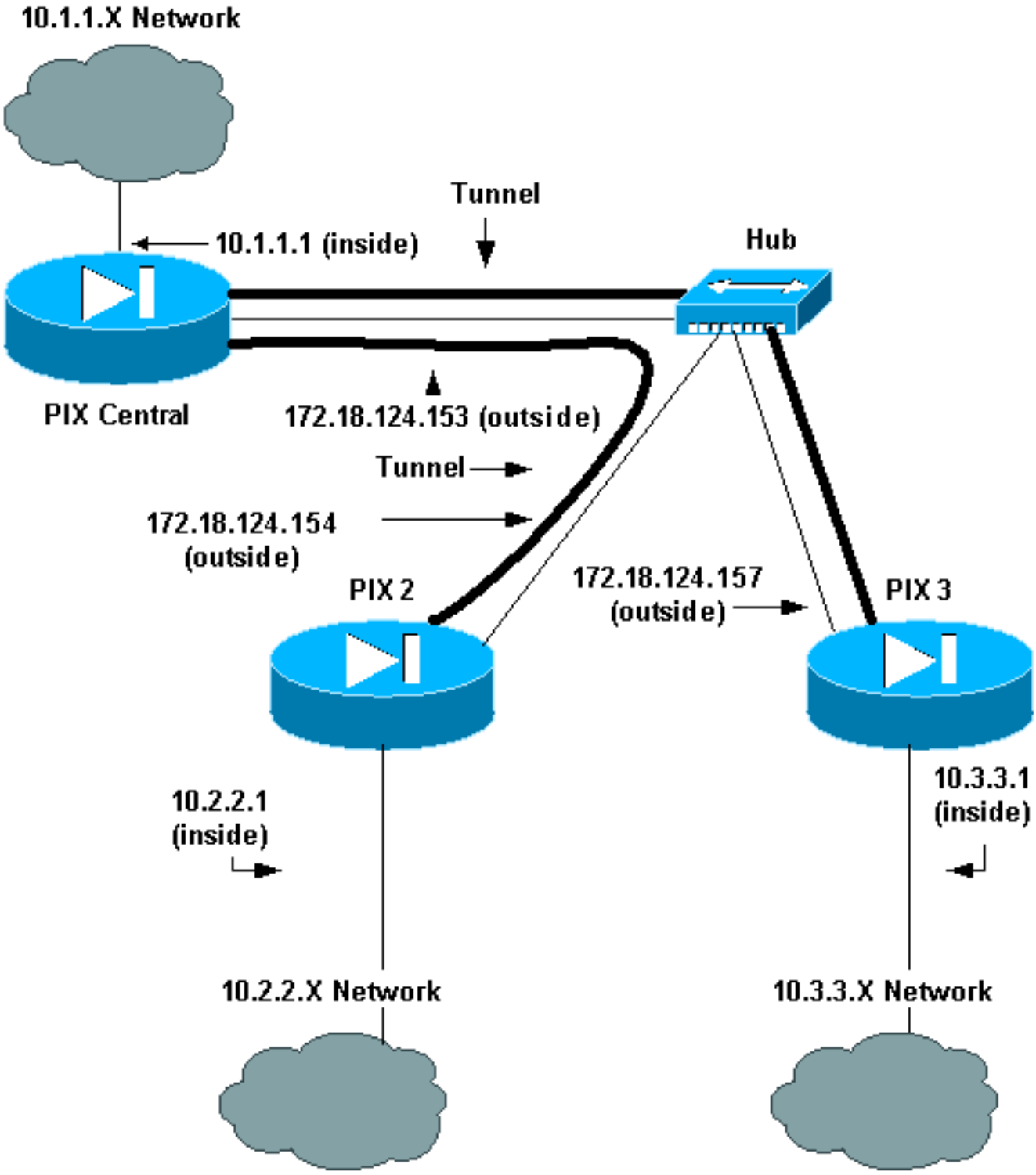
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- PIX 센트럴
- PIX 2
- PIX 3

PIX 센트럴
`Building configuration...` `: Saved`

```
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix-central
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- This is traffic to PIX 2. access-list 120 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!--- This is traffic to PIX 3. access-list 130 permit ip
10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
!--- Do not do Network Address Translation (NAT) on
traffic to other PIXes. 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
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
pdm history enable
arp timeout 14400
!--- Do not do NAT on traffic to other PIXes. 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 h225 1:00:00
timeout h323 0:05:00 mgcp 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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic 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
!--- This is traffic 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
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX 2

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix2
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- This is traffic to PIX Central. access-list 110
permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not do NAT on traffic to PIX Central. access-
list 100 permit ip 10.2.2.0 255.255.255.0 10.1.1.0
255.255.255.0
pager lines 24
logging on
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
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
!--- Do not do NAT on traffic to PIX Central. 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 h225 1:00:00
timeout h323 0:05:00 mgcp 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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic to PIX Central. 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
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 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
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX 3

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
```

```
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- This is traffic to PIX Central. access-list 110
permit ip 10.3.3.0 255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not do NAT on traffic to PIX Central. 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
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
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
!--- Do not do NAT on traffic to PIX Central. 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 h225 1:00:00
timeout h323 0:05:00 mgcp 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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic to PIX Central. 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
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 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
console timeout 0
terminal width 80
Cryptochecksum:aa3bbd8c6275d214b153e1e0bc0173e4
: end
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show crypto ipsec sa** - IPsec SA(보안 연결)의 현재 상태를 표시하며, 트래픽이 암호화되었는지 확인하는 데 유용합니다.

```
pix-central#show crypto ipsec sa

interface: outside
    Crypto map tag: newmap, local addr. 172.18.124.153

   local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157:500
     PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are sent !--- and received without any errors.
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0,
     #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 172.18.124.153,
     remote crypto endpt.: 172.18.124.157
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 3bcb6913
!--- Shows inbound SAs that are established. inbound esp sas:
      spi: 0x3efbe540(1056695616)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3, crypto map: newmap
        sa timing: remaining key lifetime (k/sec): (4607999/27330)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
     inbound pcp sas:
!--- Shows outbound SAs that are established. outbound esp sas:
       spi: 0x3bcb6913(1003186451)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel, }
```

```
          slot: 0, conn id: 4, crypto map: newmap
          sa timing: remaining key lifetime (k/sec): (4607999/27321)
          IV size: 8 bytes
          replay detection support: Y

       outbound ah sas:

       outbound pcp sas:

local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
current_peer: 172.18.124.154:500
  PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are sent !--- and received without any errors.
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0, #send errors 0, #recv errors 0

  local crypto endpt.: 172.18.124.153,
  remote crypto endpt.: 172.18.124.154
  path mtu 1500, ipsec overhead 56, media mtu 1500
  current outbound spi: da8d556
!--- Shows inbound SAs that are established. inbound esp sas: spi: 0x53835c96(1401117846)
transform: esp-des esp-md5-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 1, crypto map: newmap
       sa timing: remaining key lifetime (k/sec): (4607999/27319)
       IV size: 8 bytes
       replay detection support: Y

    inbound ah sas:

    inbound pcp sas:
!--- Shows outbound SAs that are established. outbound esp sas: spi: 0xda8d556c(3666695532)
transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: newmap
        sa timing: remaining key lifetime (k/sec): (4607999/27319)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto isakmp sa** - IKE(Internet Key Exchange) SA의 현재 상태를 표시합니다.

```
pix-central#show crypto isakmp sa
Total     : 2
Embryonic : 0
        dst               src       state     pending   created

  172.18.124.153   172.18.124.154   QM_IDLE          0         0
  172.18.124.153   172.18.124.157   QM_IDLE          0         0
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

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

PIX에서(**logging monitor 디버깅** 또는 **logging console 디버깅** 명령 실행):

- **debug crypto ipsec** - IPsec 처리를 디버깅합니다.
- **debug crypto isakmp** - ISAKMP(Internet Security Association and Key Management Protocol) 처리를 디버깅합니다.
- **debug crypto engine** - 암호화 및 해독을 수행하는 암호화 엔진에 대한 디버그 메시지를 표시합니다.

보안 연결 지우기

PIX의 컨피그레이션 모드에서 다음 명령을 사용합니다.

- **clear [crypto] ipsec sa** - 활성 IPsec SA를 삭제합니다. crypto 키워드는 선택 사항입니다.
- **clear [crypto] isakmp sa** - 활성 IKE SA를 삭제합니다. crypto 키워드는 선택 사항입니다.

관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems