

PIX에서 PIX로 PIX IPsec로 풀 메시 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[관련 정보](#)

[소개](#)

이 컨피그레이션을 사용하면 3개의 Cisco Secure PIX Firewall 상자 뒤의 프라이빗 네트워크를 인터넷 또는 IPsec을 사용하는 공용 네트워크를 통해 VPN 터널로 연결할 수 있습니다. 3개의 각 네트워크는 다른 2개의 네트워크에 연결되어 있습니다. 이 시나리오에서는 공용 인터넷 연결에 NAT(Network Address Translation)가 필요합니다. 그러나 NAT는 공용 인터넷을 통해 VPN 터널을 사용하여 전송할 수 있는 세 인트라넷 간의 트래픽에 필요하지 않습니다.

[사전 요구 사항](#)

[요구 사항](#)

IPsec이 작동하려면 이 컨피그레이션을 시작하기 전에 터널 엔드포인트에서 터널 엔드포인트로의 연결이 있어야 합니다.

[사용되는 구성 요소](#)

이 컨피그레이션은 PIX Firewall 버전 6.1(2)에서 개발 및 테스트되었습니다.

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

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.

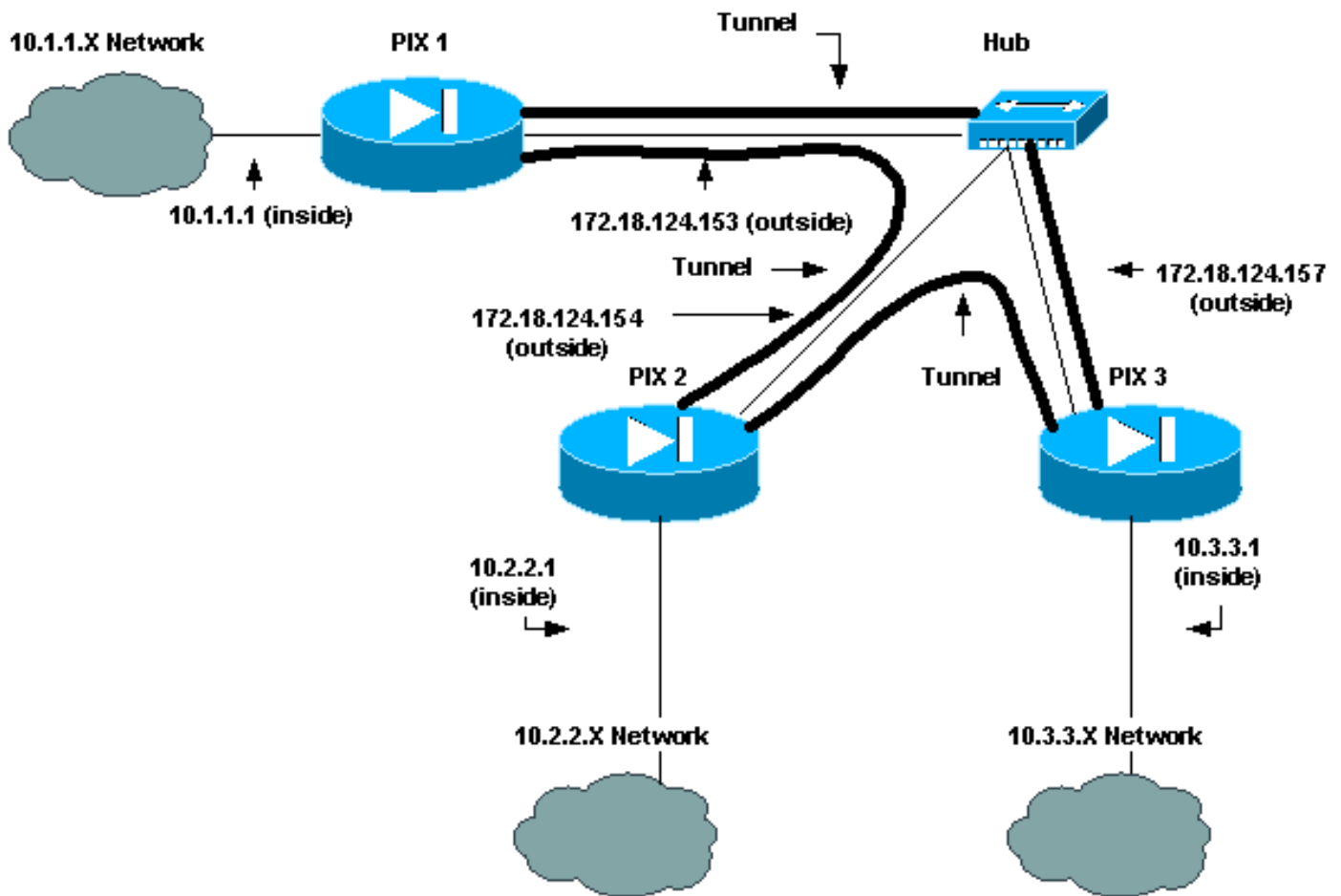
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: [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 1](#)
- [PIX 2](#)
- [PIX 3](#)

PIX 1 컨피그레이션

```
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 dnats
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 컨피그레이션

```
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 컨피그레이션

```
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 dnats
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]

```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다. 자세한 내용은 [Troubleshooting the PIX to Pass Data Traffic on an Established IPsec Tunnel\(설정된 IPsec 터널에서 데이터 트래픽을 전달하려면 PIX 트러블슈팅을 참조하십시오\)](#).

문제 해결 명령

참고: debug 명령을 사용하기 전에 디버그 [명령에 대한 중요 정보](#)를 참조하십시오.

debug 명령

logging monitor 디버깅 또는 logging console 디버깅 명령이 실행 중인 경우 PIX에서 이 명령을 사

용합니다.

- **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.

clear 명령

SA(보안 연결)를 지우려면 PIX의 컨피그레이션 모드에서 이 명령을 사용합니다.

- **clear [crypto] ipsec sa** - 활성 IPsec SA를 삭제합니다. crypto 키워드는 선택 사항입니다.
- **clear [crypto] isakmp sa** - 활성 IKE(Internet Key Exchange) SA를 삭제합니다. crypto 키워드는 선택 사항입니다.

참고: IPsec이 작동하려면 이 컨피그레이션을 시작하기 전에 터널 엔드포인트에서 터널 엔드포인트로의 연결이 있어야 합니다.

관련 정보

- [설정된 IPsec 터널에서 데이터 트래픽을 전달하기 위한 PIX 트러블슈팅](#)
- [Cisco PIX 500 Series 보안 어플라이언스](#)
- [PIX 명령 참조](#)
- [IPsec 협상/IKE 프로토콜](#)
- [RFC\(Request for Comments\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)