PIX 6.x: 간단한 PIX-to-PIX VPN 터널 컨피그레이션 예

목차

소개

이 컨피그레이션을 통해 두 Cisco Secure PIX Firewalls에서 인터넷을 통해 또는 IP 보안(IPSec)을 사용하는 공용 네트워크를 통해 PIX에서 PIX로 연결되는 간단한 VPN(Virtual Private Network) 터널을 실행할 수 있습니다. IPSec은 IPSec 피어 간에 데이터 기밀성, 데이터 무결성 및 데이터 출처 인증을 제공하는 개방형 표준의 조합입니다.

PIX/ASA 7.x 참조: Simple PIX-to-PIX VPN Tunnel Configuration Example에서 Cisco Security Appliance가 소프트웨어 버전 7.x를 실행하는 동일한 시나리오에 대한 자세한 내용을 확인할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure PIX 515E Firewall 소프트웨어 버전 6.3(5)
- Cisco Secure PIX 515E Firewall 소프트웨어 버전 6.3(5)

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

IPSec 협상은 두 개의 IKE(Internet Key Exchange) 단계를 포함하는 5단계로 나눌 수 있습니다.

1. IPSec 터널은 흥미로운 트래픽에 의해 시작됩니다. 트래픽은 IPSec 피어 간에 이동할 때 흥미로운 것으로 간주됩니다.
2. IKE 1단계에서 IPSec 피어는 설정된 IKE SA(Security Association) 정책을 협상합니다. 피어가 인증되면 ISAKMP(Internet Security Association and Key Management Protocol)를 사용하여 보안 터널이 생성됩니다.
3. IKE 2단계에서 IPSec 피어는 IPSec SA 변형을 협상하기 위해 인증되고 안전한 터널을 사용합니다. 공유 정책의 협상은 IPSec 터널의 설정 방법을 결정합니다.
4. IPSec 터널이 생성되고 IPSec 변형 집합에 구성된 IPSec 매개변수를 기반으로 IPSec 피어 간에 데이터가 전송됩니다.
5. IPSec 터널은 IPSec SA가 삭제되거나 수명이 만료될 때 종료됩니다.

참고: 두 IKE 단계의 SA가 피어에서 일치하지 않으면 두 PIX 간의 IPSec 협상이 실패합니다.

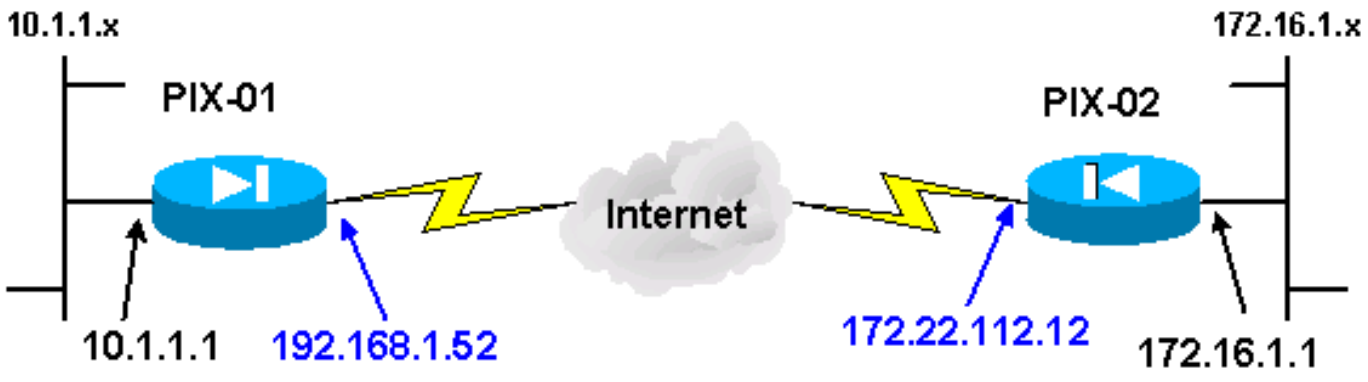
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 자세한 내용은 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 다이어그램을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 이는 실

습 환경에서 사용된 RFC 1918 주소입니다.

IKE 및 IPSec 컨피그레이션

각 PIX의 IPSec 컨피그레이션은 암호화 맵 및 변형 집합에 대해 선택한 이름 지정 규칙과 피어 정보를 삽입할 때만 달라집니다. **쓰기 터미널** 또는 **show** 명령으로 컨피그레이션을 확인할 수 있습니다. 관련 명령은 **show isakmp**, **show isakmp policy**, **show access-list**, **show crypto IPSec transform-set** 및 show crypto **map입니다.** 이러한 명령에 대한 자세한 내용은 Cisco Secure PIX Firewall Command Reference를 참조하십시오.

IPSec을 구성하려면 다음 단계를 완료하십시오.

1. 사전 공유 키에 대한 IKE 구성
2. IPSec 구성
3. NAT(Network Address Translation) 구성
4. PIX 시스템 옵션 구성

사전 공유 키에 대한 IKE 구성

IPSec **종료** 인터페이스에서 IKE를 활성화하려면 isakmp enable 명령을 실행합니다. 이 시나리오에서 외부 인터페이스는 두 PIX의 IPSec 종료 인터페이스입니다. IKE는 두 PIX에 모두 구성됩니다. 이 명령은 PIX-01만 표시합니다.

```
isakmp enable outside
```

또한 IKE 협상 중에 사용되는 IKE 정책을 정의해야 합니다. 이 작업을 **수행하려면 isakmp policy** 명령을 실행합니다. 이 명령을 실행할 때 정책이 고유하게 식별되도록 우선 순위 수준을 할당해야 합니다. 이 경우 가장 높은 우선 순위 1이 정책에 할당됩니다. 또한 이 정책은 사전 공유 키, 데이터 인증을 위한 MD5 해싱 알고리즘, ESP(Encapsulating Security Payload)를 위한 DES 및 Diffie-Hellman group1을 사용하도록 설정됩니다. 또한 SA 수명을 사용하도록 정책이 설정됩니다.

```
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

IKE 컨피그레이션은 show isakmp **policy** 명령으로 확인할 수 있습니다.

```
PIX-01#show isakmp policy
Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 1000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
```

```
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

마지막으로, 사전 공유 키를 구성하고 피어 주소를 할당하려면 isakmp key 명령을 실행합니다. 사전 공유 키를 사용할 때는 IPSec 피어에서 동일한 사전 공유 키가 일치해야 합니다. 원격 피어의 IP 주소에 따라 주소가 다릅니다.

```
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
PIX-01#
```

write terminal 또는 show isakmp 명령으로 정책을 확인할 수 있습니다.

```
PIX-01#show isakmp
isakmp enable outside
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
isakmp identity address
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

IPSec 구성

IPSec은 PIX 중 하나가 다른 PIX 내부 네트워크로 향하는 트래픽을 수신할 때 시작됩니다. 이 트래픽은 IPSec을 통해 보호해야 하는 흥미로운 트래픽으로 간주됩니다. 액세스 목록은 어떤 트래픽이 IKE 및 IPSec 협상을 시작할지를 결정하는 데 사용됩니다. 이 액세스 목록을 사용하면 10.1.1.x 네트워크에서 IPSec 터널을 통해 172.16.1.x 네트워크로 트래픽을 전송할 수 있습니다. 반대 PIX 구성의 액세스 목록은 이 액세스 목록을 미러링합니다. 이는 PIX-01에 적합합니다.

```
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

IPSec 변형 집합은 피어가 데이터 흐름을 보호하기 위해 사용하는 보안 정책을 정의합니다. IPSec 변환은 crypto IPSec transform-**set** 명령**을** 사용하여 정의됩니다. 변형 집합에 대해 고유한 이름을 선택해야 하며 IPSec 보안 프로토콜을 정의하기 위해 최대 3개의 변형을 선택할 수 있습니다. 이 컨피그레이션에서는 두 가지 변형만 사용합니다. **esp-hmac-md5** 및 **esp-des**.

```
crypto IPSec transform-set chevelle esp-des esp-md5-hmac
```

암호화 맵은 암호화된 트래픽에 대해 IPSec SA를 설정합니다. 암호화 맵을 만들려면 맵 이름과 시퀀스 번호를 할당해야 합니다. 그런 다음 암호화 맵 매개변수를 정의합니다. 표시된 암호화 맵 트랜잭션은 IKE를 사용하여 IPSec SA를 설정하고, 액세스 목록 101과 일치하는 모든 항목을 암호화하고, set peer를 가지며, **chevelle** transform-set를 사용하여 트래픽에 대한 보안 정책을 적용합니다.

```
crypto map transam 1 IPSec-isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform-set chevelle
```

암호화 맵을 정의한 후 암호화 맵을 인터페이스에 적용합니다. 선택하는 인터페이스는 IPSec 종료 인터페이스여야 합니다.

```
crypto map transam interface outside
```

show crypto **map** 명령을 실행하여 암호화 맵 특성을 확인합니다.

```
PIX-01#show crypto map

Crypto Map: "transam" interfaces: { outside }

Crypto Map "transam" 1 IPSec-isakmp
Peer = 172.22.112.12
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255
Current peer: 172.22.112.12
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ chevelle, }
```

NAT 구성

이 명령은 IPSec에 대해 흥미롭게 간주되는 트래픽을 NAT에 알리지 않습니다. 따라서 **access-list** 명령문과 일치하는 모든 트래픽은 NAT 서비스에서 제외됩니다.

```
access-list NoNAT permit ip 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0
nat (inside) 0 access-list NoNAT
```

PIX 시스템 옵션 구성

모든 인바운드 세션은 액세스 목록 또는 도관에 의해 명시적으로 허용되어야 하므로 sysopt **connection permit-IPSec** 명령은 모든 인바운드 IPSec 인증 암호 세션을 허용하는 데 사용됩니다. IPSec 보호 트래픽을 사용할 경우 보조 도관 검사는 이중화되어 터널 생성에 실패할 수 있습니다. sysopt 명령은 다양한 PIX 방화벽 보안 및 컨피그레이션 기능을 튜닝합니다.

```
sysopt connection permit-IPSec
```

구성

Cisco 디바이스에서 **write terminal** 명령의 출력이 있는 경우 Output Interpreter (등록된 고객만)를 사용하여 잠재적인 문제 및 수정 사항을 표시할 수 있습니다. Output Interpreter를 사용하려면 로그인되어 있고 JavaScript가 활성화되어 있어야 (등록된 고객만 해당) 합니다.

PIX-01(192.68.1.52)
PIX Version 6.3(5) interface ethernet0 auto

```
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-01
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
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewall. access-list NoNAT permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
!--- Sets the outside address on the PIX Firewall. ip
address outside 192.168.1.52 255.255.255.0
!--- Sets the inside address on the PIX Firewall. 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
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
route outside 0.0.0.0 0.0.0.0 192.168.1.1 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 sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
```

```
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2: !--- The IPSec transform-set
"chevelle" uses esp-md5-hmac to provide !--- data
authentication.

crypto IPSec transform-set chevelle esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map transam 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 172.22.112.12.
crypto map transam 1 match address 101
!--- Sets the IPSec peer. crypto map transam 1 set peer
172.22.112.12
!--- Sets the IPSec transform set "chevelle" !--- to be
used with the crypto map entry "transam". crypto map
transam 1 set transform-set chevelle
!--- Assigns the crypto map transam to the interface.
crypto map transam interface outside
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate the IPSec tunnel

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the pre-shared key between the IPSec peers. !--- The
same preshared key must be configured on the !--- IPSec
peers for IKE authentication. isakmp key ********
address 172.22.112.12 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
!--- The show isakmp policy command shows the
differences in !--- the default and configured policy.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX-02(172.22.112.12)

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
```

```
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-02
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
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewall. access-list NoNAT permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
!--- Sets the outside address on the PIX Firewall. ip
address outside 172.22.112.12 255.255.255.0
!--- Sets the inside address on the PIX Firewall. ip
address inside 172.16.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
route outside 0.0.0.0 0.0.0.0 172.22.112.1 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 sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
```

```
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2:  !--- The IPSec transform set defines
the negotiated security policy !--- that the peers use
to protect the data flow. !--- The IPSec transform-set
"toyota" uses hmac-md5 authentication header !--- and
encapsulates the payload with des.

crypto IPSec transform-set toyota esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map bmw 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 192.168.1.52.
crypto map bmw 1 match address 101
!--- Sets IPSec peer. crypto map bmw 1 set peer
192.168.1.52
!--- Sets the IPSec transform set "toyota" !--- to be
used with the crypto map entry "bmw". crypto map bmw 1
set transform-set toyota
!--- Assigns the crypto map bmw to the interface. crypto
map bmw interface outside
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate IPSec tunnel.

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the preshared key between the IPSec peers. !--- The same
preshared key must be configured on the !--- IPSec peers
for IKE authentication. isakmp key ******** address
192.168.1.52 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 show 명령 출력의 분석 결과를 볼 수 있습니다.

- **show crypto IPSec sa** - 이 명령은 IPSec SA의 현재 상태를 표시하며, 트래픽이 암호화 중인지 확인하는 데 유용합니다.
- **show crypto isakmp sa** - 이 명령은 IKE SA의 현재 상태를 표시합니다.

PIX-01 show 명령

PIX-01 show 명령

```
PIX-01#show crypto IPSec sa
interface: outside
Crypto map tag: transam, local addr. 192.168.1.52

local ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
current_peer: 172.22.112.12
PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are being sent
!--- and received without any errors. #pkts encaps: 3,
#pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 192.168.1.52, remote crypto endpt.:
172.22.112.12
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 6f09cbf1
!--- Shows inbound SAs that are established. inbound esp
sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: transam
sa timing: remaining key lifetime (k/sec):
(4607999/28430)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:
!--- Shows outbound SAs that are established. outbound
ESP sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: transam
sa timing: remaining key lifetime (k/sec):
(4607999/28430)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
```

```
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. PIX-01#show
crypto isakmp sa
     dst             src          state      pending
created
172.22.112.12    192.168.1.52    QM_IDLE         0
1Maui-PIX-01#
```

PIX-02 show 명령

PIX-02 show 명령

```
PIX-02#show crypto IPSec sa

interface: outside
Crypto map tag: bmw, local addr. 172.22.112.12

local ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.52
PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are !--- being
sent and recede without any errors. #pkts encaps: 3,
#pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#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.: 172.22.112.12, remote crypto
endpt.: 192.168.1.52
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 70be0c04
!--- Shows inbound SAs that are established. Inbound ESP
sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: bmw
sa timing: remaining key lifetime (k/sec):
(4607999/28097)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:
!--- Shows outbound SAs that are established. Outbound
ESP sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: bmw
sa timing: remaining key lifetime (k/sec):
(4607999/28097)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:

outbound PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. PIX-02#show
crypto isakmp sa
     dst             src           state      pending
created
172.22.112.12    192.168.1.52    QM_IDLE          0
PIX-02#
```

PIX의 내부 인터페이스는 management-access 명령이 전역 컨피그레이션 모드에서 구성되어 있지 않으면 터널의 형성을 위해 ping을 수행할 수 없습니다.

```
PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside
```

문제 해결

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

문제 해결 명령

참고: clear 명령은 컨피그레이션 모드에서 수행해야 합니다.

- **clear crypto IPSec sa** - 이 명령은 VPN 터널 협상을 실패한 후 IPSec SA를 재설정합니다.
- **clear crypto isakmp sa** - 이 명령은 VPN 터널 협상을 실패한 후 ISAKMP SA를 재설정합니다.

참고: 디버그 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto IPSec** - 이 명령은 클라이언트가 VPN 연결의 IPSec 부분을 협상하고 있는지 여부를 표시합니다.
- **debug crypto isakmp**—이 명령은 피어가 VPN 연결의 ISAKMP 부분을 협상하는지 여부를 표시합니다.

연결이 완료되면 **show** 명령을 사용하여 확인할 수 있습니다.

관련 정보

- PIX 지원 페이지
- PIX 명령 참조
- RFC(Request for Comments)
- IPSec 협상/IKE 프로토콜 지원 페이지
- 기술 지원 및 문서 – Cisco Systems