Sonicwall 제품과 Cisco Security Appliance의 VPN 컨피그레이션 예

목차

소개

이 문서에서는 적극적인 모드와 주 모드를 모두 사용하여 두 프라이빗 네트워크 간에 통신하기 위해 사전 공유 키를 사용하여 IPsec 터널을 구성하는 방법을 설명합니다.이 예에서 통신 네트워크는 Cisco Security Appliance(PIX/ASA) 내의 192.168.1.x 프라이빗 네트워크와 SonicwallTM TZ170 방화벽 내의 172.22.1.x 프라이빗 네트워크입니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 이 컨피그레이션을 시작하기 전에 Cisco Security Appliance 내부 및 Sonicwall TZ170 내부의 트래픽이 인터넷(10.x.x.x 네트워크로 표시)으로 이동해야 합니다.
- 사용자는 IPsec 협상에 익숙해야 합니다.이 프로세스는 2개의 IKE(Internet Key Exchange) 단계를 포함하는 5단계로 나눌 수 있습니다.IPsec 터널은 흥미로운 트래픽에 의해 시작됩니다.트래픽은 IPsec 피어 간에 이동할 때 흥미로운 것으로 간주됩니다.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.IKE 2단계에서 IPsec 피어는 IPsec SA 변형을 협상하기 위해 인증되고 안전한 터널을 사용합니다

.공유 정책의 협상은 IPsec 터널의 설정 방법을 결정합니다.IPsec 터널이 생성되고 IPsec 변형 집합에 구성된 IPsec 매개변수를 기반으로 IPsec 피어 간에 데이터가 전송됩니다.IPsec 터널은 IPsec SA가 삭제되거나 수명이 만료될 때 종료됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco PIX 515E 버전 6.3(5)
- Cisco PIX 515 버전 7.0(2)
- Sonicwall TZ170, SonicOS Standard 2.2.0.1

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.

관련 제품

이 컨피그레이션은 다음 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- PIX 6.3(5) 컨피그레이션은 해당 소프트웨어 버전(PIX 501, 506 등)을 실행하는 다른 모든 Cisco PIX 방화벽 제품과 함께 사용할 수 있습니다.
- PIX/ASA 7.0(2) 컨피그레이션은 Cisco 5500 Series ASA와 함께 PIX 7.0 소프트웨어(501, 506 및 일부 이전 515s 제외)를 실행하는 디바이스에서만 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

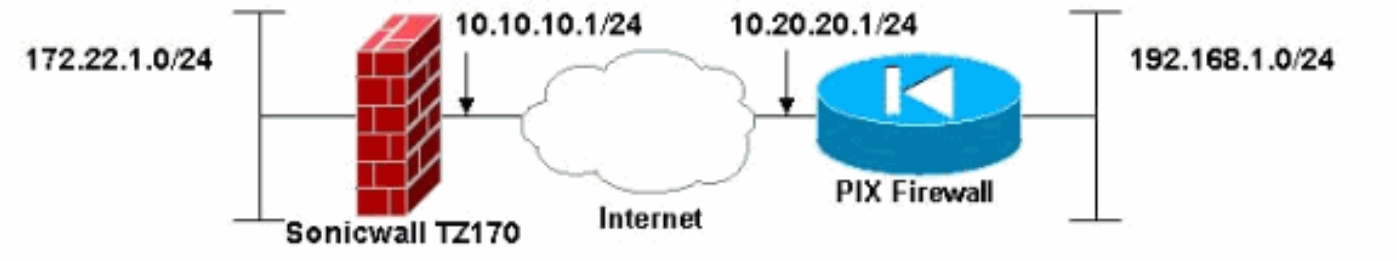
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

참고: IPsec Agressive Mode에서는 Sonicwall에서 PIX에 대한 IPsec 터널을 시작해야 합니다.이 컨피그레이션에 대한 디버그를 분석할 때 이를 확인할 수 있습니다.이는 IPsec Aggressive Mode가 작동하는 방식에 내재되어 있습니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



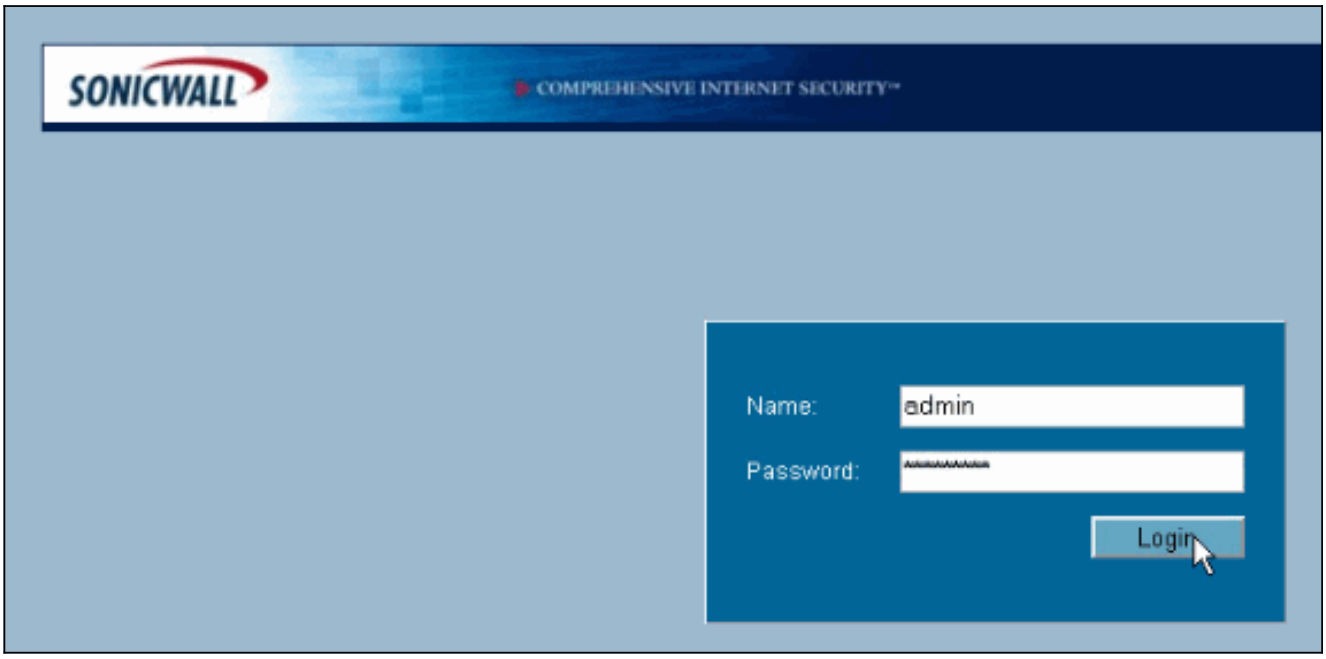
Sonicwall 컨피그레이션

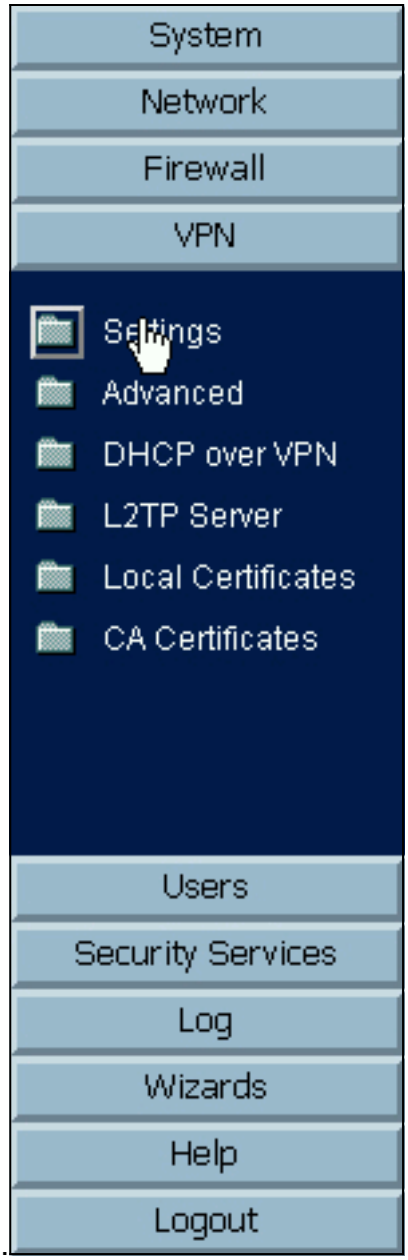
Sonicwall TZ170의 컨피그레이션은 웹 기반 인터페이스를 통해 수행됩니다.

다음 단계를 완료하십시오.

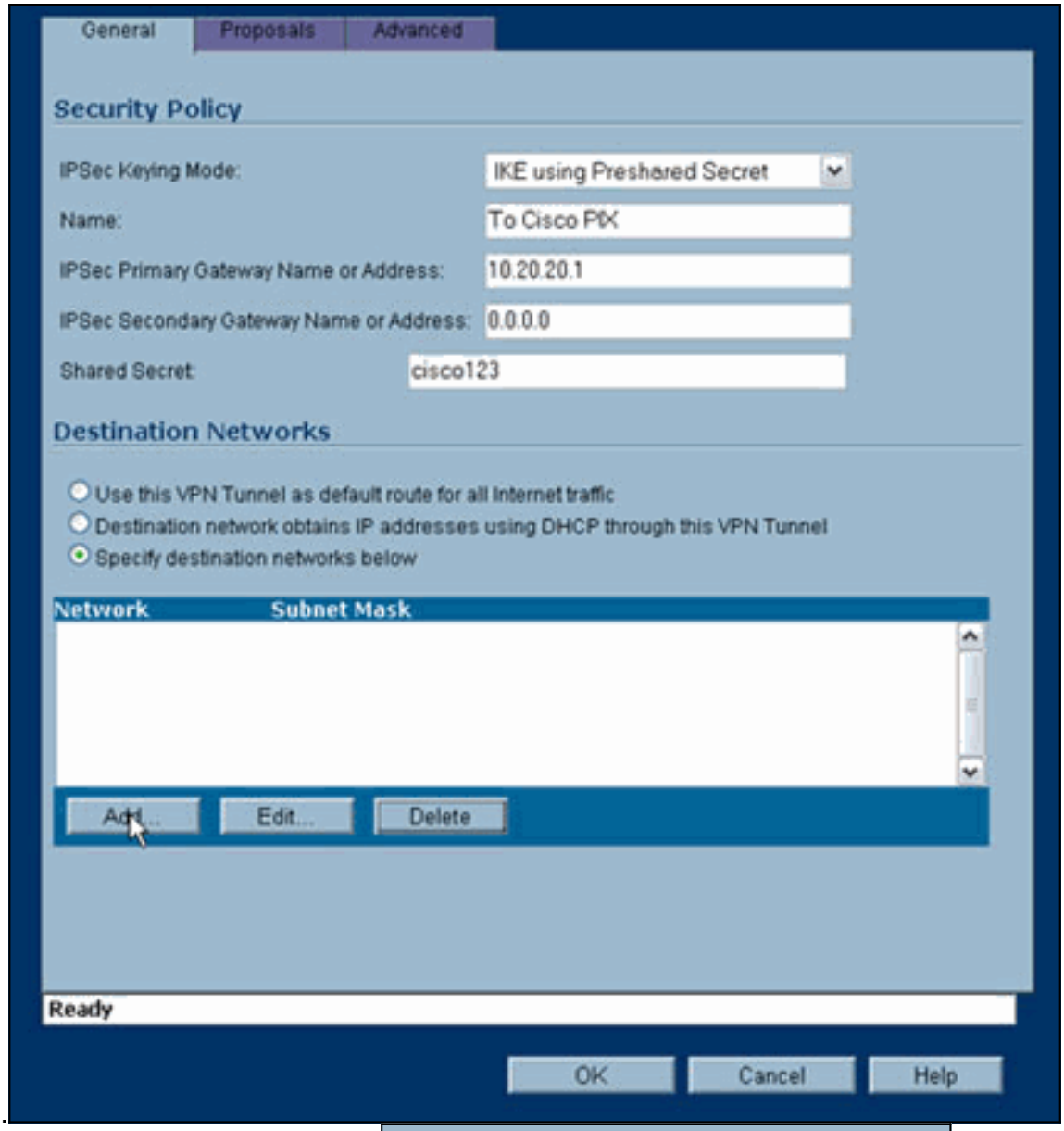
1. 표준 웹 브라우저를 사용하여 내부 인터페이스 중 하나에서 라우터의 IP 주소에 연결합니다 .로그인 창이 나타납니다

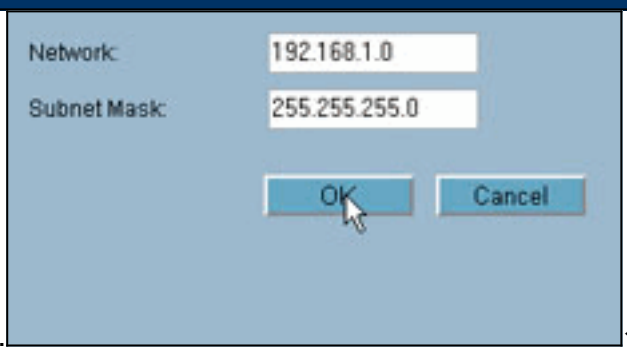
.



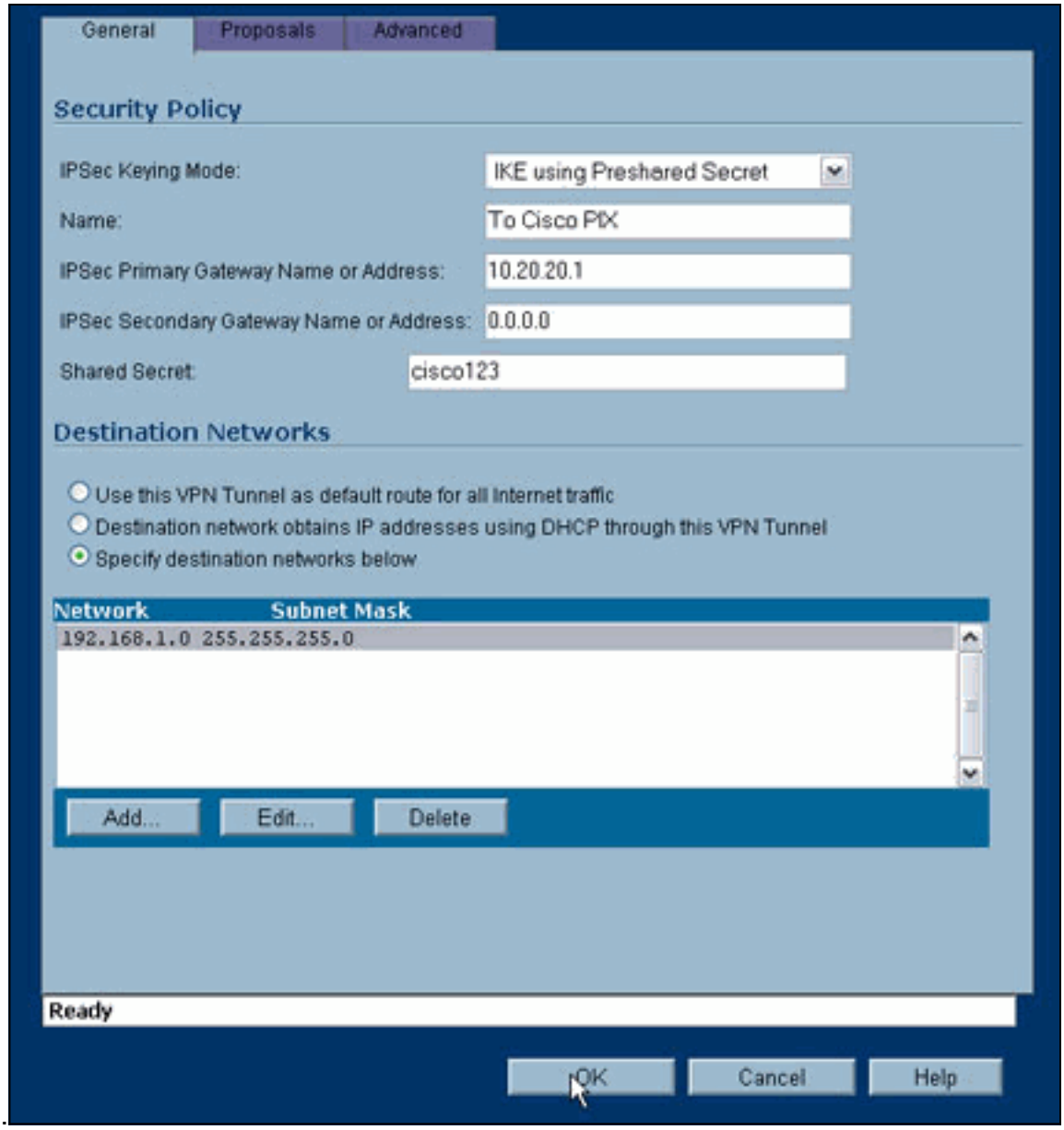


2. Sonicwall 디바이스에 로그인하고 **VPN > 설정**을 선택합니다.
3. VPN 피어의 IP 주소와 사용할 사전 공유 암호를 입력합니다.Destination Networks 아래에서 Add를 클릭합니다



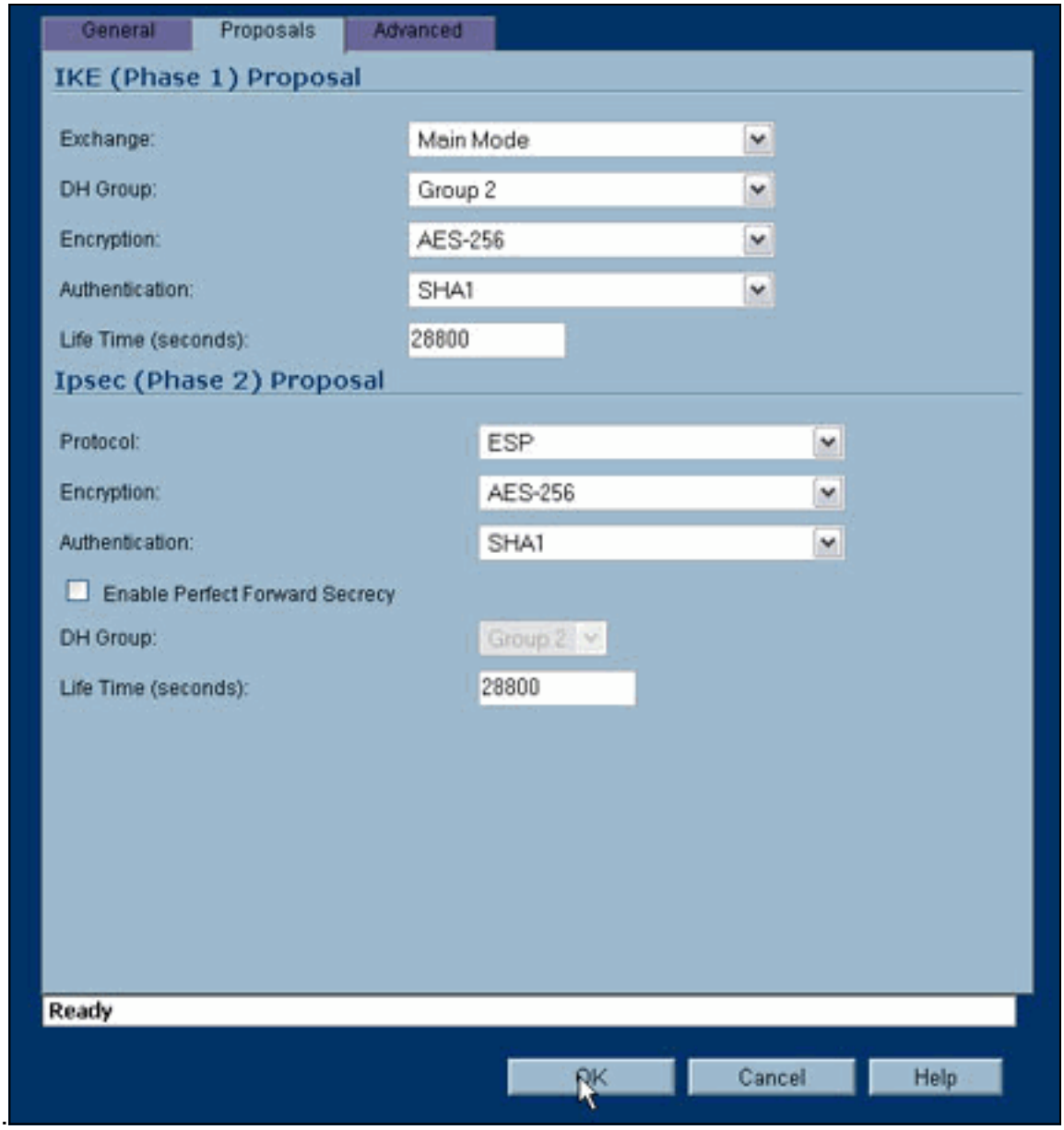
4. 대상 네트워크를 입력합니다. 

설정 창이 나타납니

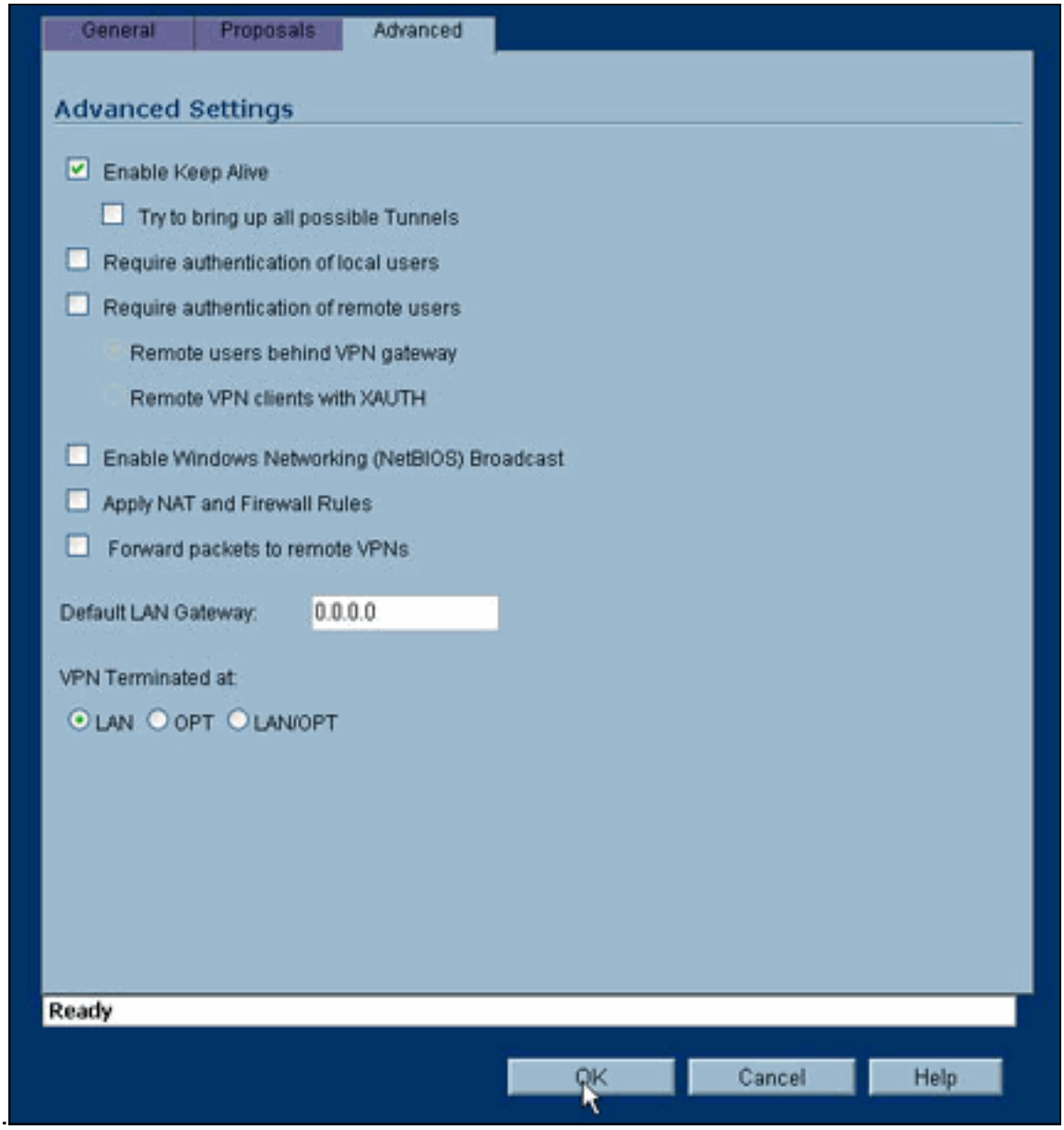


다.

5. 설정 창 상단의 제안 탭을 클릭합니다.
6. 1단계 및 2단계 설정의 나머지 설정과 함께 이 컨피그레이션(Main Mode 또는 Aggressive Mode)에 사용할 Exchange를 선택합니다.이 예제 컨피그레이션에서는 인증을 위해 SHA1 해시 알고리즘을 사용하는 두 단계 모두에 AES-256 암호화를 사용하고 IKE 정책에는 1024비트 Diffie-Hellman 그룹 2를 사용합니다



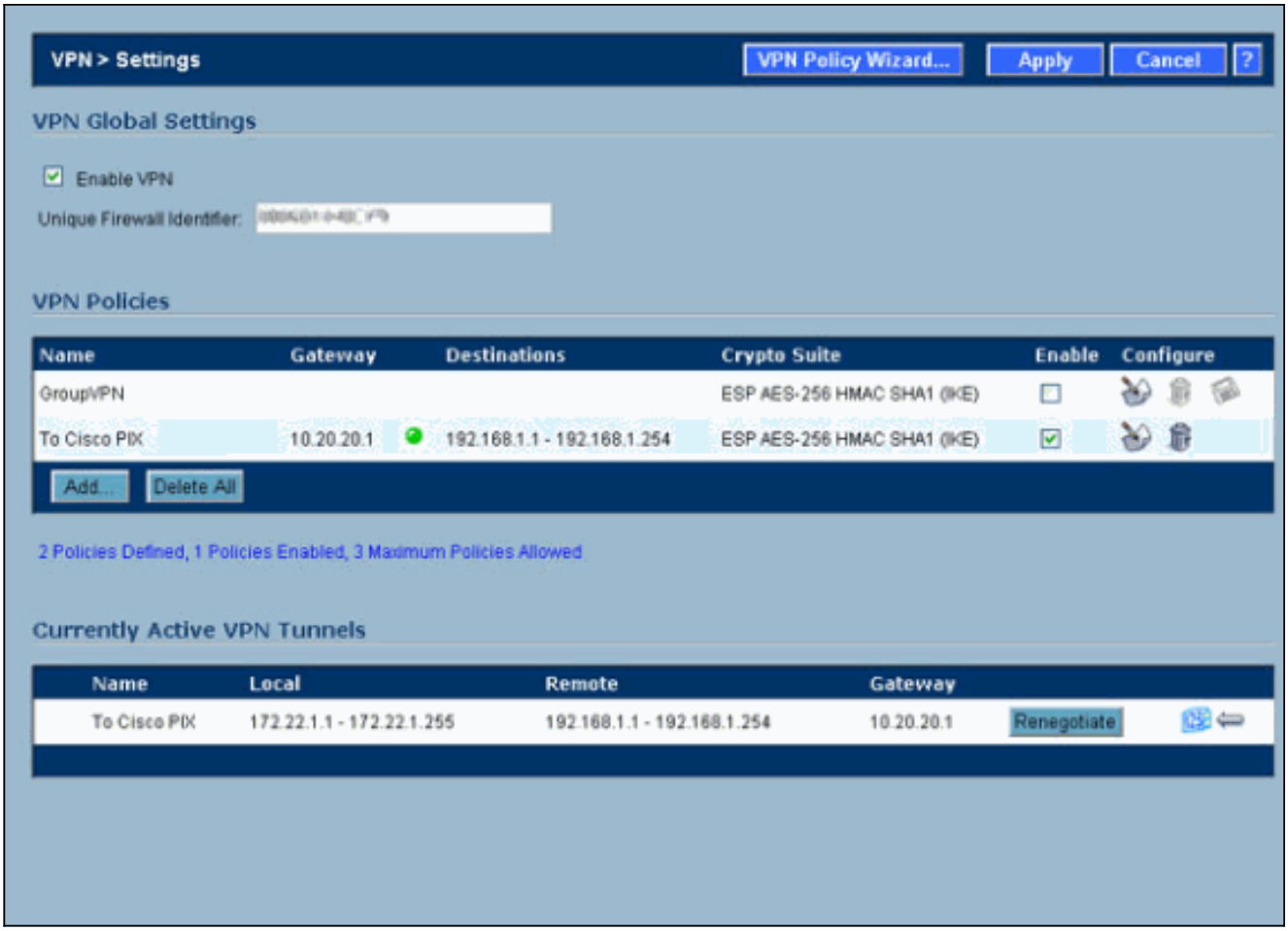
7. 고급 탭을 클릭합니다.이 탭에서 구성할 수 있는 추가 옵션이 있습니다.이 샘플 컨피그레이션에 사용되는 설정입니다



.

8. **확인을 클릭합니다**.이 컨피그레이션 및 원격 PIX의 컨피그레이션을 완료하면 Settings(설정) 창이 이 예제 Settings(설정) 창과 유사해야 합니다

.



IPsec 주 모드 컨피그레이션

이 섹션에서는 다음 컨피그레이션을 사용합니다.

- Cisco PIX 515e 버전 6.3(5)
- Cisco PIX 515 버전 7.0(2)

Cisco PIX 515e 버전 6.3(5)

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
```

```
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 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 !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION: !--- Defines the transform set
for Phase 2 encryption and authentication. !---
Austinlab is the name of the transform set that uses
aes-256 encryption !--- as well as the SHA1 hash
algorithm for authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies IKE is used to establish the IPsec SAs
for the map "maptosw". crypto map maptosw 67 ipsec-
isakmp !--- Specifies the ACL "pixtosw" to use with this
map . crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map. crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Specifies the interface
to use for the IPsec tunnel.

isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used with the preshared key cisco123. isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

Cisco PIX 515 버전 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS®. !--- This output configures the IP
address, interface name, !--- and security level for
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 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 !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies the ACL pixtosw to use with this map.
crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map . crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Defines how the PIX
```

```
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration !--- settings specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

IPsec Aggressive Mode 컨피그레이션

이 섹션에서는 다음 컨피그레이션을 사용합니다.

- Cisco PIX 515e 버전 6.3(5)
- Cisco PIX 515 버전 7.0(2)

Cisco PIX 515e 버전 6.3(5)

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
```

```
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 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 !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION !--- Defines the transform set for
Phase 2 encryption and authentication. !--- Austinlab is
the name of the transform set that uses aes-256
encryption !--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map ciscopix for the transform
set. crypto dynamic-map ciscopix 1 set transform-set
austinlab !--- Specifies the IKE that should be used to
establish SAs !--- for the dynamic map. crypto map
dynmaptosw 66 ipsec-isakmp dynamic ciscopix !--- Applies
the settings above to the outside interface. crypto map
dynmaptosw interface outside !--- PHASE 1 CONFIGURATION
!--- Specifies the interface to use for the IPsec tunnel
.
isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used as the preshared key "cisco123". isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

Cisco PIX 515 버전 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS. !--- This output configures the IP
```

```
address, interface name, and security level for !---
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 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 !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map "ciscopix" for the defined
transform set. crypto dynamic-map ciscopix 1 set
transform-set austinlab !--- Specifies that IKE should
be used to establish SAs !--- for the defined dynamic
map. crypto map dynmaptosw 66 ipsec-isakmp dynamic
ciscopix !--- Applies the settings to the outside
interface. crypto map dynmaptosw interface outside !---
PHASE 1 CONFIGURATION !--- Defines how the PIX
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration settings !--- specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
```

```
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

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 isakmp sa** - 피어의 현재 모든 IKE SA를 표시합니다.
- **show crypto ipsec sa** - 현재 SA에서 사용하는 설정을 표시합니다.

이 표에서는 터널이 완전히 설정된 후 PIX 6.3(5) 및 PIX 7.0(2) 모두에서 Main 및 Aggressive 모드에 대한 일부 디버그의 출력을 보여 줍니다.

참고: 이 정보는 이 두 하드웨어 유형 간에 설정된 IPsec 터널을 가져오는 데 충분한 정보여야 합니다.의견이 있는 경우 이 문서의 왼쪽에 있는 피드백 양식을 사용하십시오.

- Cisco PIX 515e 버전 6.3(5) - 기본 모드
- Cisco PIX 515 버전 7.0(2)- 기본 모드
- Cisco PIX 515e 버전 6.3(5) - 적극적인 모드
- Cisco PIX 515 버전 7.0(2) - 적극적인 모드

Cisco PIX 515e 버전 6.3(5) - 기본 모드

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src         state     pending
created
      10.10.10.1       10.20.20.1    QM_IDLE          0
1
pix515e-635#



pix515e-635#show crypto ipsec sa


           interface: outside
           Crypto map tag: maptosw, local addr.
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1:500
           PERMIT, flags={origin_is_acl,}
           #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 1, #recv errors 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
           path mtu 1500, ipsec overhead 72, media mtu
1500
           current outbound spi: ed0afa33

 inbound esp sas:
           spi: 0xac624692(2892121746)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 1, crypto map: maptosw
           sa timing: remaining key lifetime (k/sec):
(4607999/28718)
           IV size: 16 bytes
           replay detection support: Y


           inbound ah sas:


           inbound pcp sas:


           outbound esp sas:
           spi: 0xed0afa33(3976919603)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 2, crypto map: maptosw
           sa timing: remaining key lifetime (k/sec):
(4607999/28718)
           IV size: 16 bytes
           replay detection support: Y


           outbound ah sas:


           outbound pcp sas:

pix515e-635#
```

Cisco PIX 515 버전 7.0(2)- 기본 모드

```
pix515-702#show crypto isakmp sa

 Active SA: 1
           Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
           Total IKE SA: 1

1 IKE Peer: 10.10.10.1
           Type : L2L Role : initiator
           Rekey : no State : MM_ACTIVE
           pix515-702#
```

```
pix515-702#show crypto ipsec sa
interface: outside
    Crypto map tag: maptosw, local addr: 10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: 2D006547

 inbound esp sas:
           spi: 0x309F7A33 (815757875)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28739)
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0x2D006547 (755000647)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28737)
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

Cisco PIX 515e 버전 6.3(5) - 적극적인 모드

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending
created
      10.20.20.1       10.10.10.1    QM_IDLE         0
1

pix515e-635#show crypto ipsec sa


           interface: outside
           Crypto map tag: dynmaptosw, local addr.
10.20.20.1

 local ident (addr/mask/prot/port):
```

```
(192.168.1.0/255.255.255.0/0/0)
          remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
          current_peer: 10.10.10.1:500
          PERMIT, flags={}
          #pkts encaps: 0, #pkts encrypt: 0, #pkts
digest 0
          #pkts decaps: 0, #pkts decrypt: 0, #pkts
verify 0
          #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.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
          path mtu 1500, ipsec overhead 72, media mtu
1500
          current outbound spi: efb1149d

 inbound esp sas:
          spi: 0x2ad2c13c(718455100)
          transform: esp-aes-256 esp-sha-hmac ,
          in use settings ={Tunnel, }
          slot: 0, conn id: 2, crypto map: dynmaptosw
          sa timing: remaining key lifetime (k/sec):
(4608000/28736)
          IV size: 16 bytes
          replay detection support: Y


          inbound ah sas:


          inbound pcp sas:


          outbound esp sas:
          spi: 0xefb1149d(4021359773)
          transform: esp-aes-256 esp-sha-hmac ,
          in use settings ={Tunnel, }
          slot: 0, conn id: 1, crypto map: dynmaptosw
          sa timing: remaining key lifetime (k/sec):
(4608000/28727)
          IV size: 16 bytes
          replay detection support: Y


          outbound ah sas:


          outbound pcp sas:

pix515e-635#
```

Cisco PIX 515 버전 7.0(2) - 적극적인 모드

```
pix515-702#show crypto isakmp sa

 Active SA: 1
          Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
          Total IKE SA: 1
```

```
1 IKE Peer: 10.10.10.1
           Type : L2L Role : responder
           Rekey : no State : AM_ACTIVE
           pix515-702#

pix515-702#show crypto ipsec sa
           interface: outside
           Crypto map tag: ciscopix, local addr:
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: D7E2F5FD

 inbound esp sas:
           spi: 0xDCBF6AD3 (3703532243)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28703
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0xD7E2F5FD (3621975549)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28701
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco PIX 방화벽 소프트웨어

- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems