PIX/ASA 7.x 이상:PIX-to-PIX VPN 터널 컨피그레이션 예

목차

소개

이 문서에서는 Cisco ASDM(Adaptive Security Device Manager)을 사용하여 두 PIX 방화벽 간에 VPN 터널을 구성하는 절차에 대해 설명합니다.ASDM은 GUI를 통해 PIX 방화벽을 설정, 구성 및 모니터링하는 데 도움이 되도록 설계된 애플리케이션 기반 컨피그레이션 툴입니다.PIX 방화벽은 서로 다른 두 사이트에 배치됩니다.

터널은 IPsec을 사용하여 형성됩니다.IPsec은 IPsec 피어 간에 데이터 기밀성, 데이터 무결성 및 데이터 출처 인증을 제공하는 개방형 표준의 조합입니다.

참고: PIX 7.1 이상에서는 sysopt **connection permit-ipsec** 명령**이 sysopt connection permit-vpn**으로 **변경됩니다**.이 명령을 사용하면 VPN 터널을 통해 보안 어플라이언스로 진입하고 암호 해독된 트래픽이 인터페이스 액세스 목록을 우회하도록 허용합니다.그룹 정책 및 사용자별 권한 부여 액세스 목록은 여전히 트래픽에 적용됩니다.이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.이 명령은 CLI 컨피그레이션에 표시되지 않습니다.

PIX 6.x 참조:Cisco PIX Security Appliance에서 소프트웨어 버전 6.x를 실행하는 동일한 시나리오에 대해 자세히 알아보려면 간단한 PIX-to-PIX VPN 터널 구성 예

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 이 피어가 연결할 적절한 피어를 결정하기 위해 첫 번째 독점적 교환을 시작하도록 지정합니다.

- Cisco PIX 500 Series Security Appliance 버전 7.x 이상
- ASDM 버전 5.x.이상

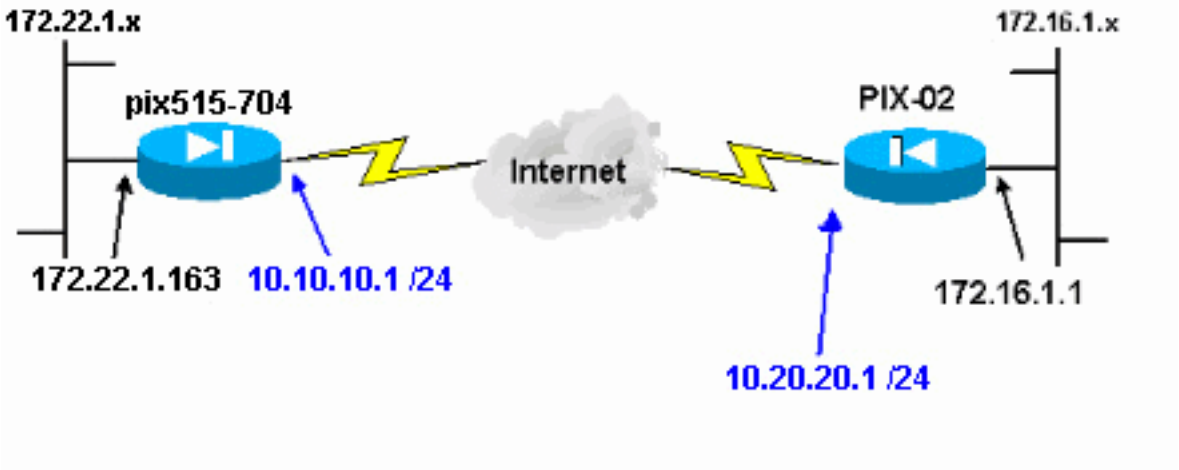
참고: ASDM에서 ASA를 구성할 수 있도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

참고: ASA 5500 Series 버전 7.x/8.x은 PIX 버전 7.x/8.x과 동일한 소프트웨어를 실행합니다.이 문서의 구성은 두 제품 라인에 모두 적용됩니다.

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.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

IPsec 협상은 5단계로 나눌 수 있으며 2개의 IKE(Internet Key Exchange) 단계를 포함합니다.

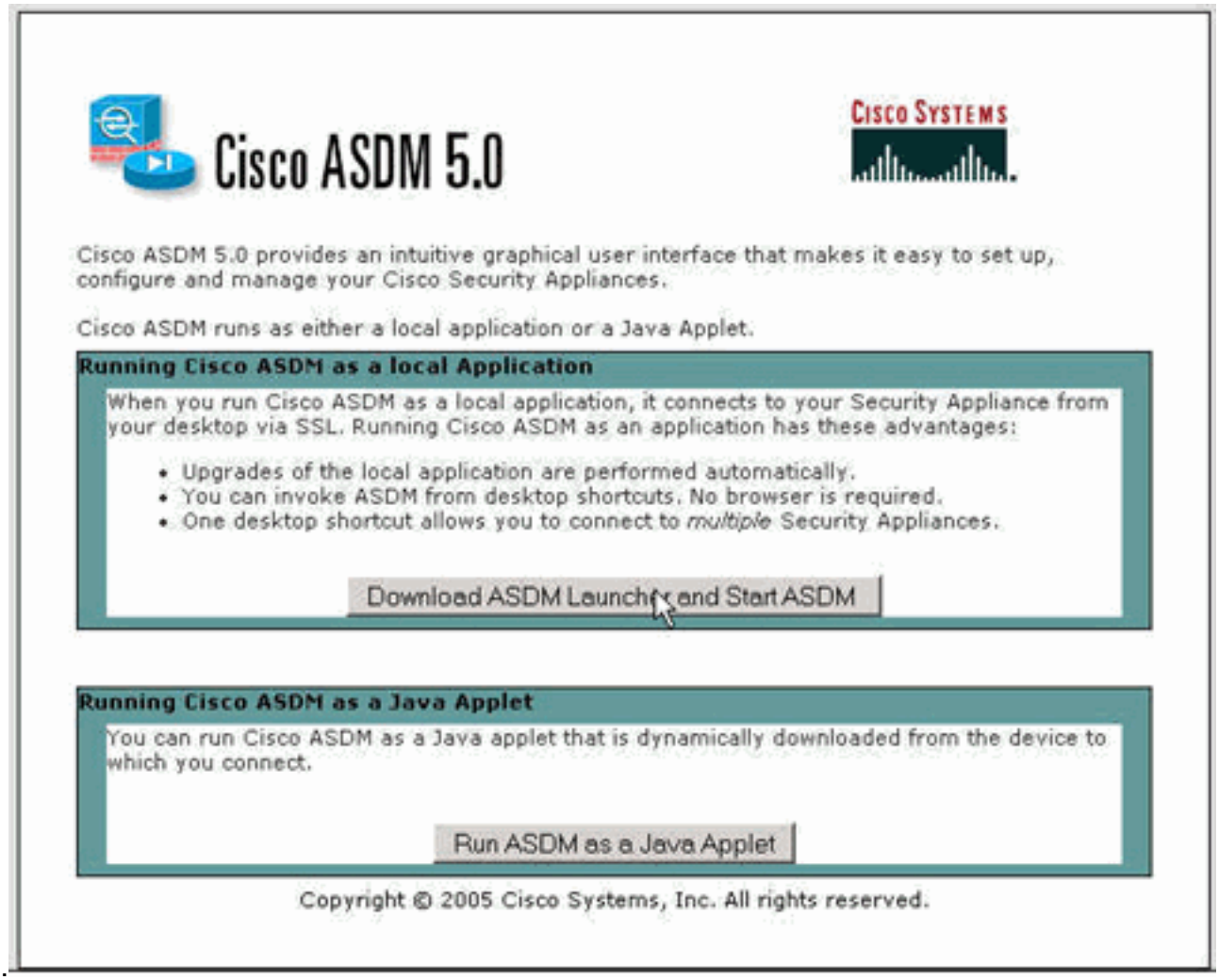
1. IPsec 터널은 흥미로운 트래픽에 의해 시작됩니다.트래픽은 IPsec 피어 간에 이동할 때 흥미로운 것으로 간주됩니다.
2. IKE 1단계에서 IPsec 피어는 설정된 IKE SA(Security Association) 정책을 협상합니다.피어가 인증되면 ISAKMP(Internet Security Association and Key Management Protocol)를 사용하여 보안 터널이 생성됩니다.
3. IKE 2단계에서 IPsec 피어는 IPsec SA 변형을 협상하기 위해 인증되고 안전한 터널을 사용합니다.공유 정책의 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

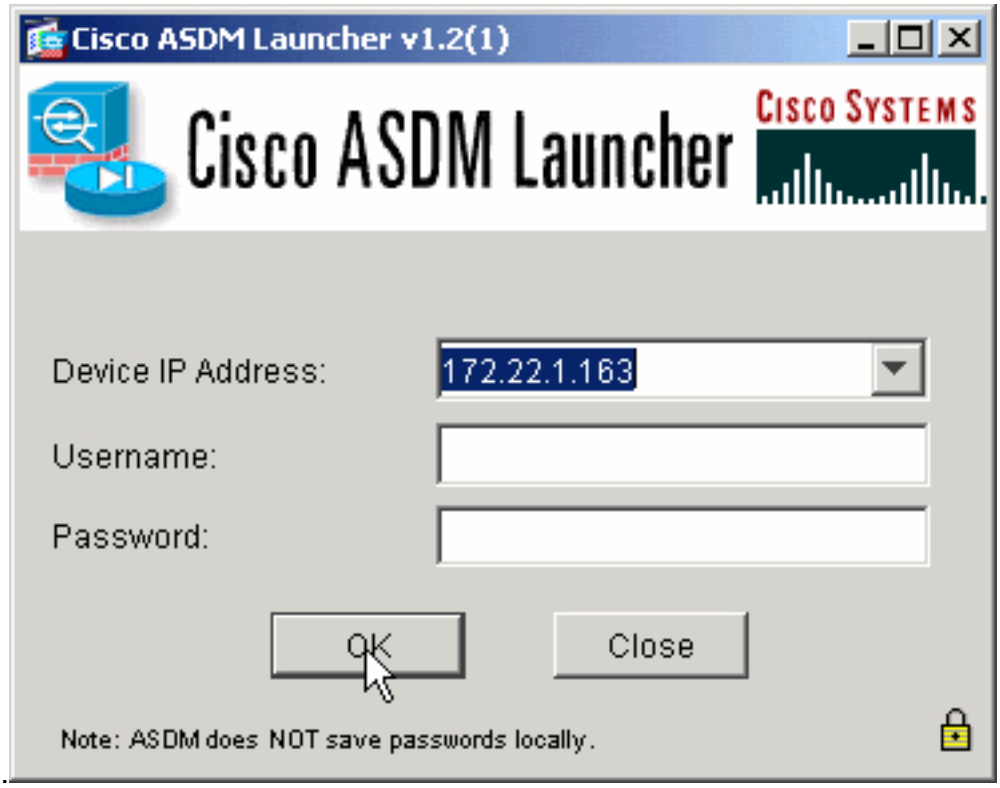
ASDM 컨피그레이션

다음 단계를 완료하십시오.

1. 브라우저를 열고 **https://<Inside_IP_Address_of_PIX>를 입력하여 PIX**의 ASDM에 액세스합니다.브라우저에서 SSL 인증서 신뢰성과 관련된 경고를 승인해야 합니다.기본 사용자 이름과 비밀번호는 모두 비어 있습니다.PIX는 ASDM 애플리케이션을 다운로드할 수 있도록 이 창을 표시합니다.이 예에서는 응용 프로그램을 로컬 컴퓨터에 로드하며 Java 애플릿에서 실행되지 않습니다



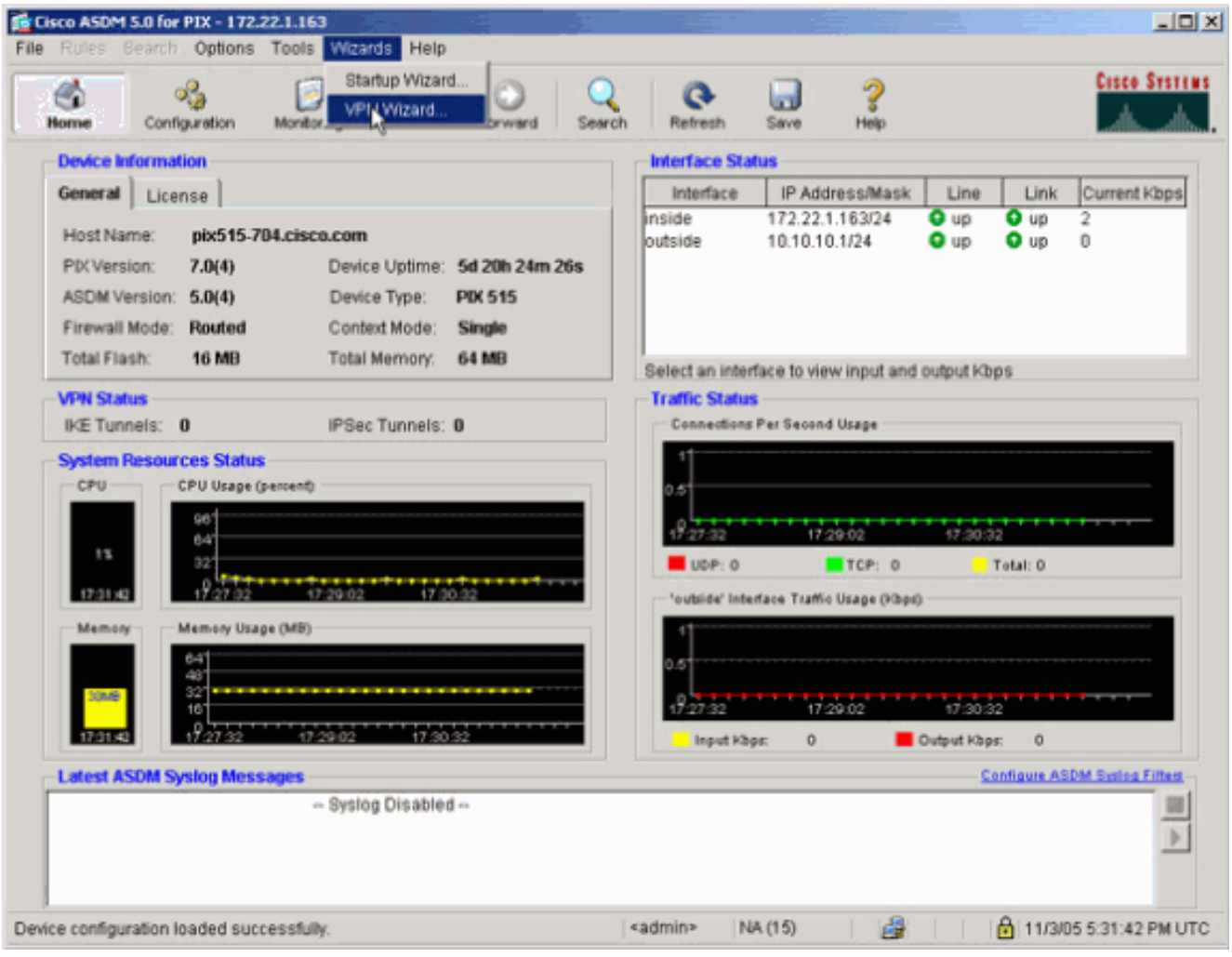
2. Download **ASDM Launcher and Start ASDM(ASDM Launcher 다운로드 및 ASDM 시작)**을 클릭하여 ASDM 애플리케이션용 설치 프로그램을 다운로드합니다.
3. ASDM Launcher가 다운로드되면 프롬프트를 따라 소프트웨어를 설치하고 Cisco ASDM Launcher를 실행합니다.
4. **http -** 명령으로 구성한 인터페이스의 IP 주소와 사용자 이름 및 비밀번호를 지정한 경우 입력합니다.이 예에서는 기본 빈 사용자 이름과 비밀번호를 사용합니다



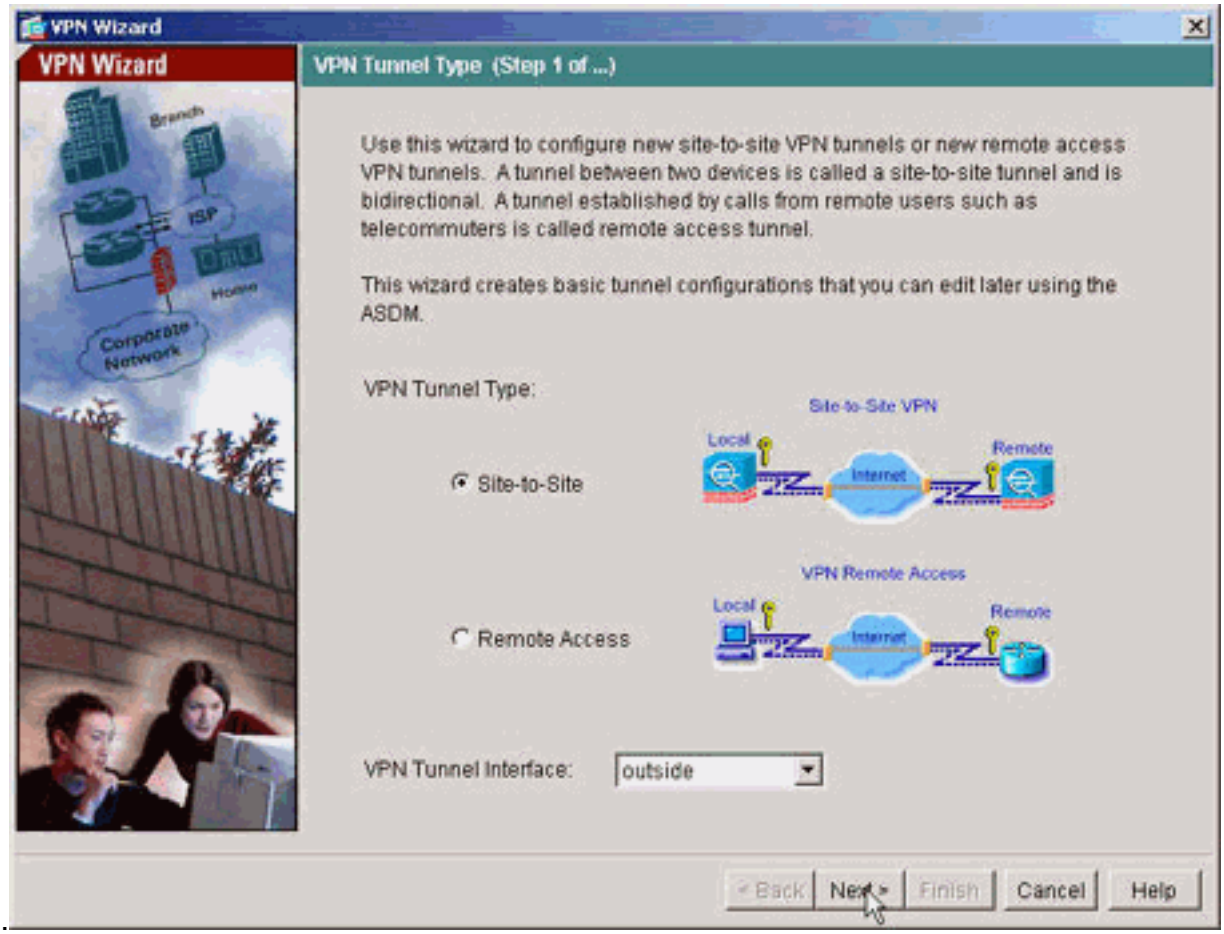
.

5. ASDM 애플리케이션이 PIX에 연결되면 VPN 마법사를 실행합니다

.

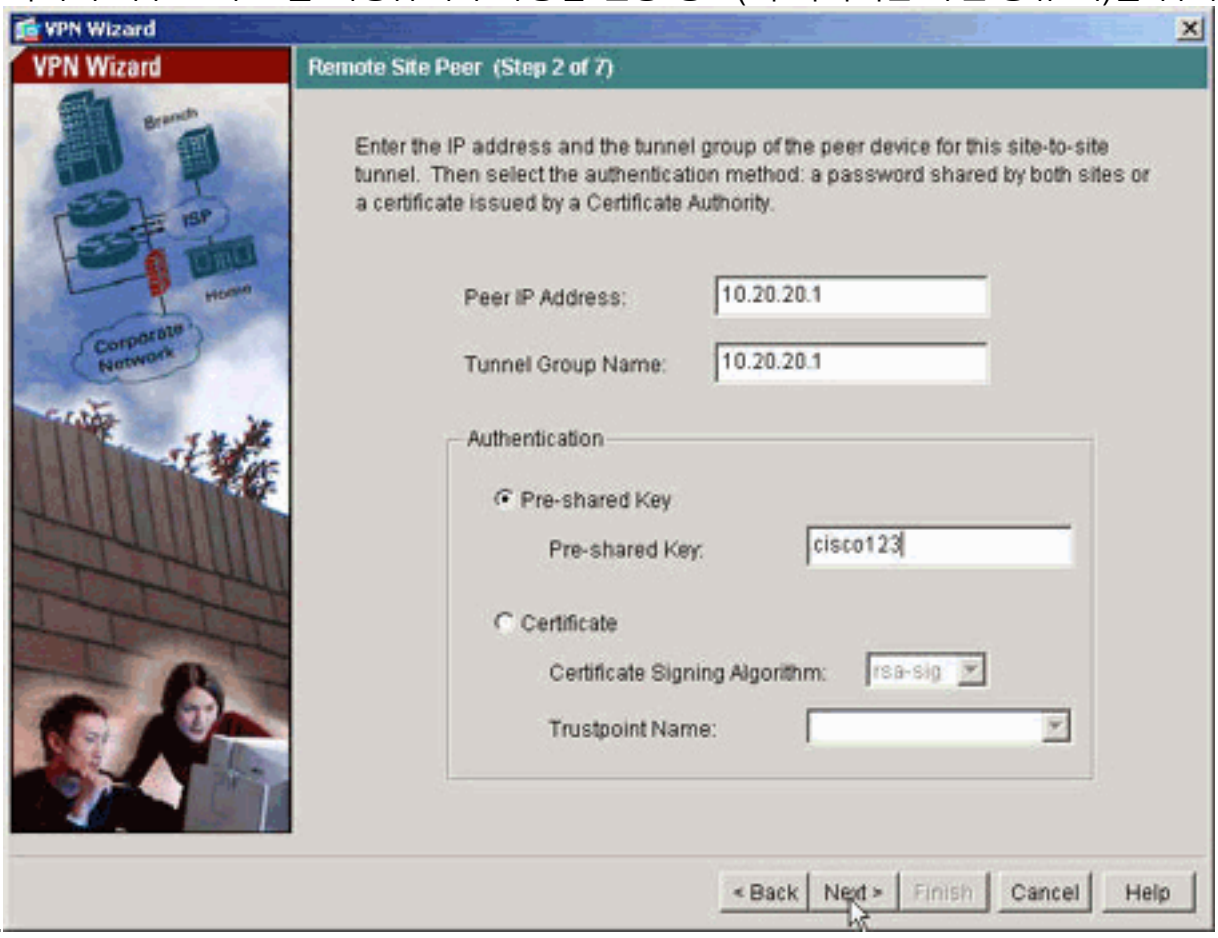


6. Site-**to-Site** VPN 터널 유형을 선택합니다



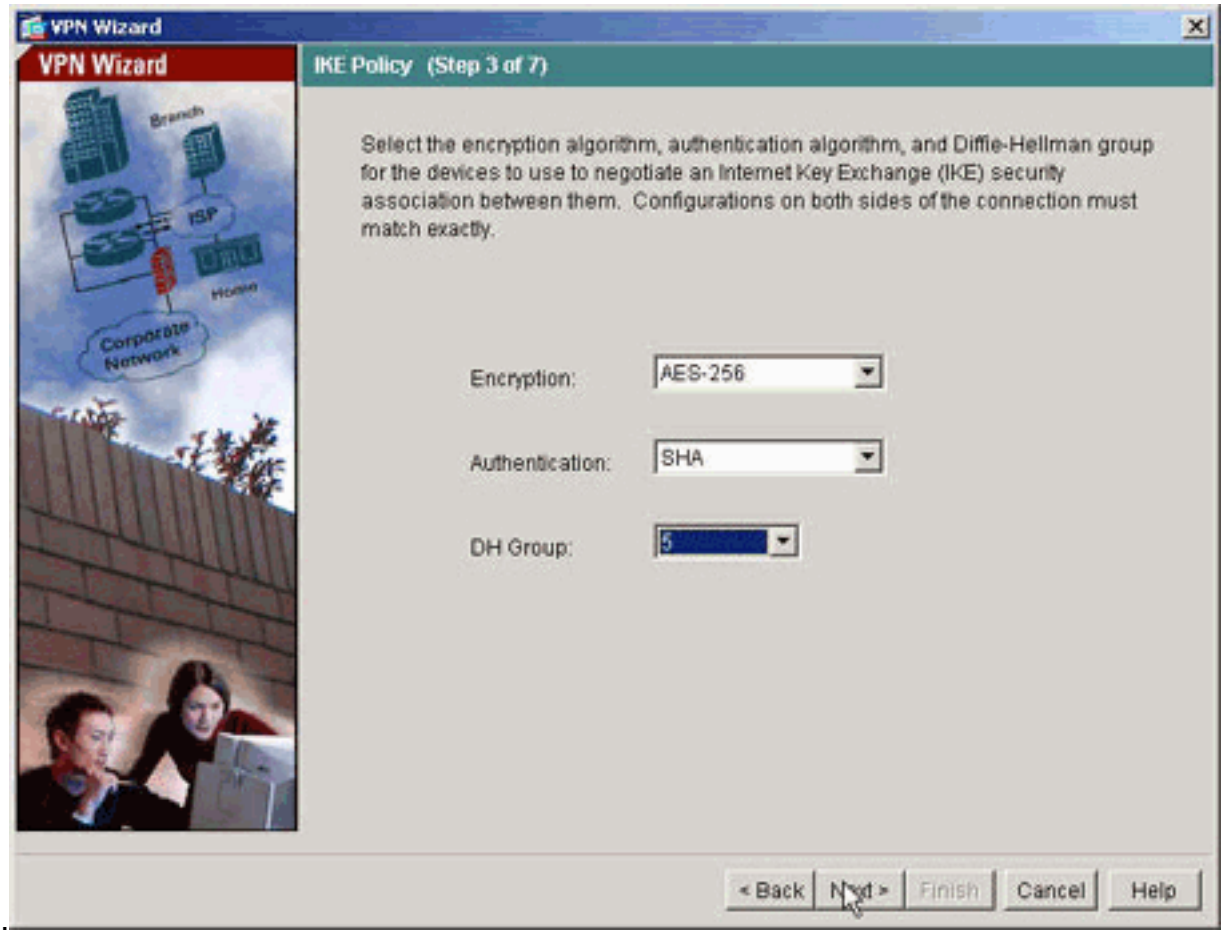
.

7. 원격 피어의 외부 IP 주소를 지정합니다.사용할 인증 정보(이 예에서는 사전 공유 키)를 입력합

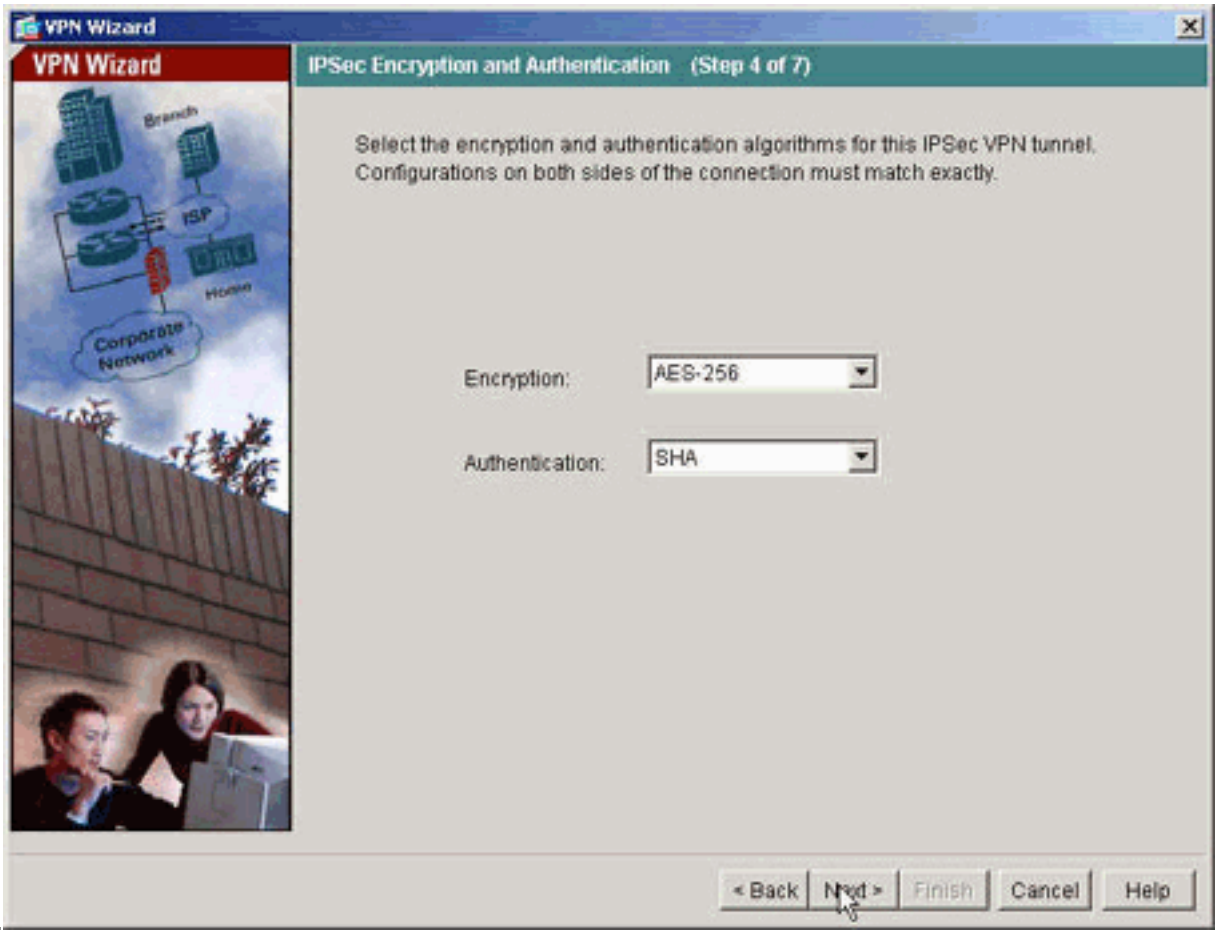


니다.

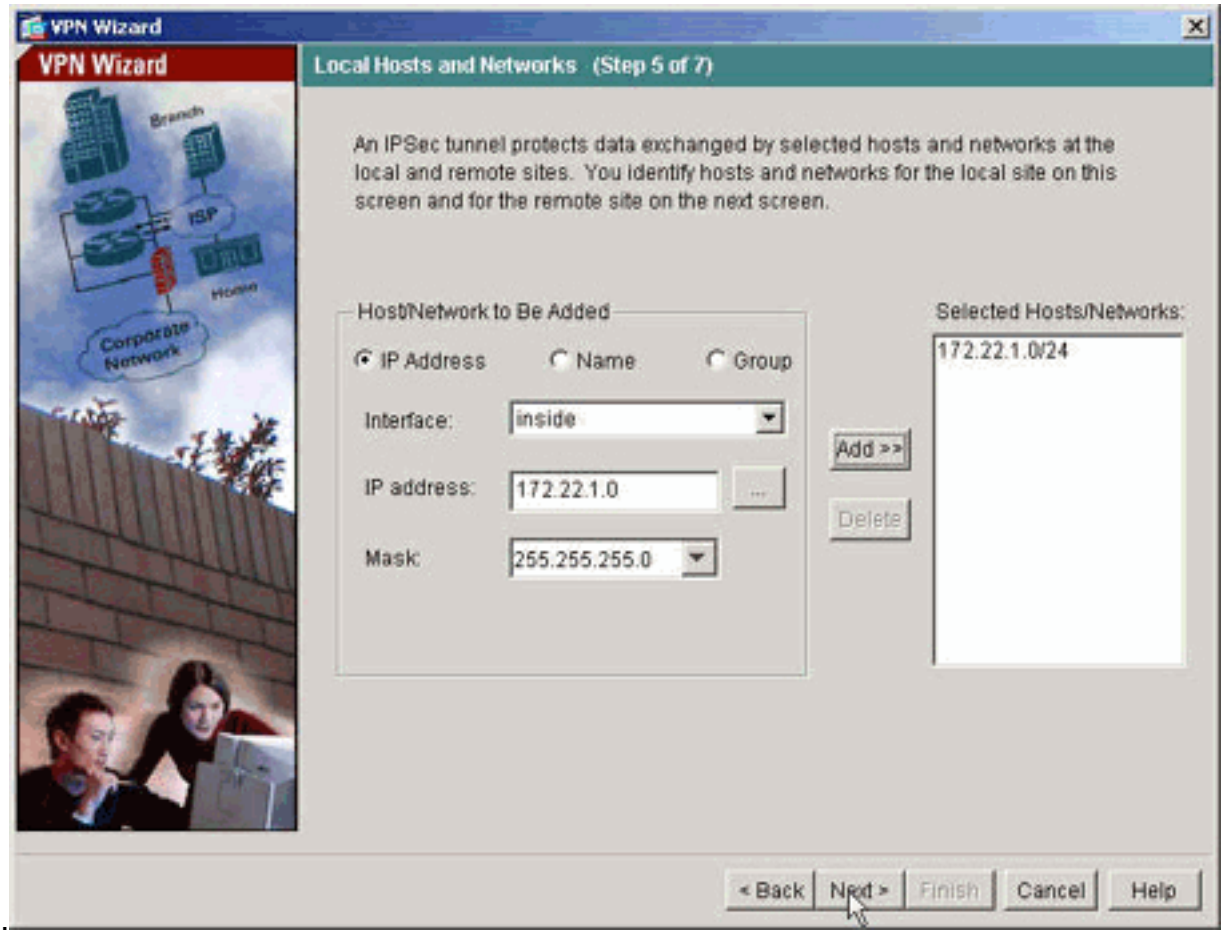
8. "1단계"라고도 하는 IKE에 사용할 특성을 지정합니다. 이러한 특성은 터널의 양쪽에서 동일해야 합니다



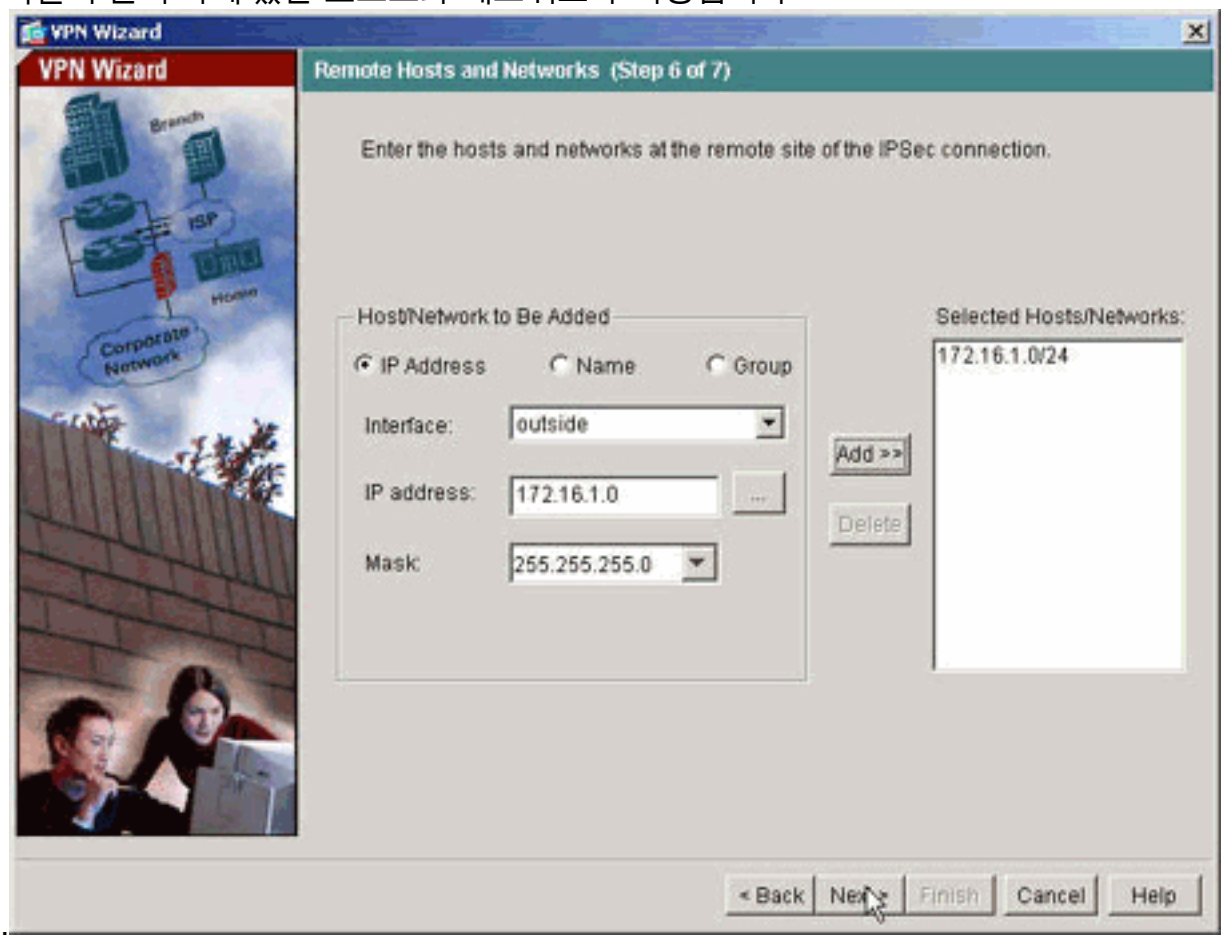
9. "2단계"라고도 하는 IPsec에 사용할 특성을 지정합니다. 이러한 특성은 양쪽에서 일치해야 합니다.



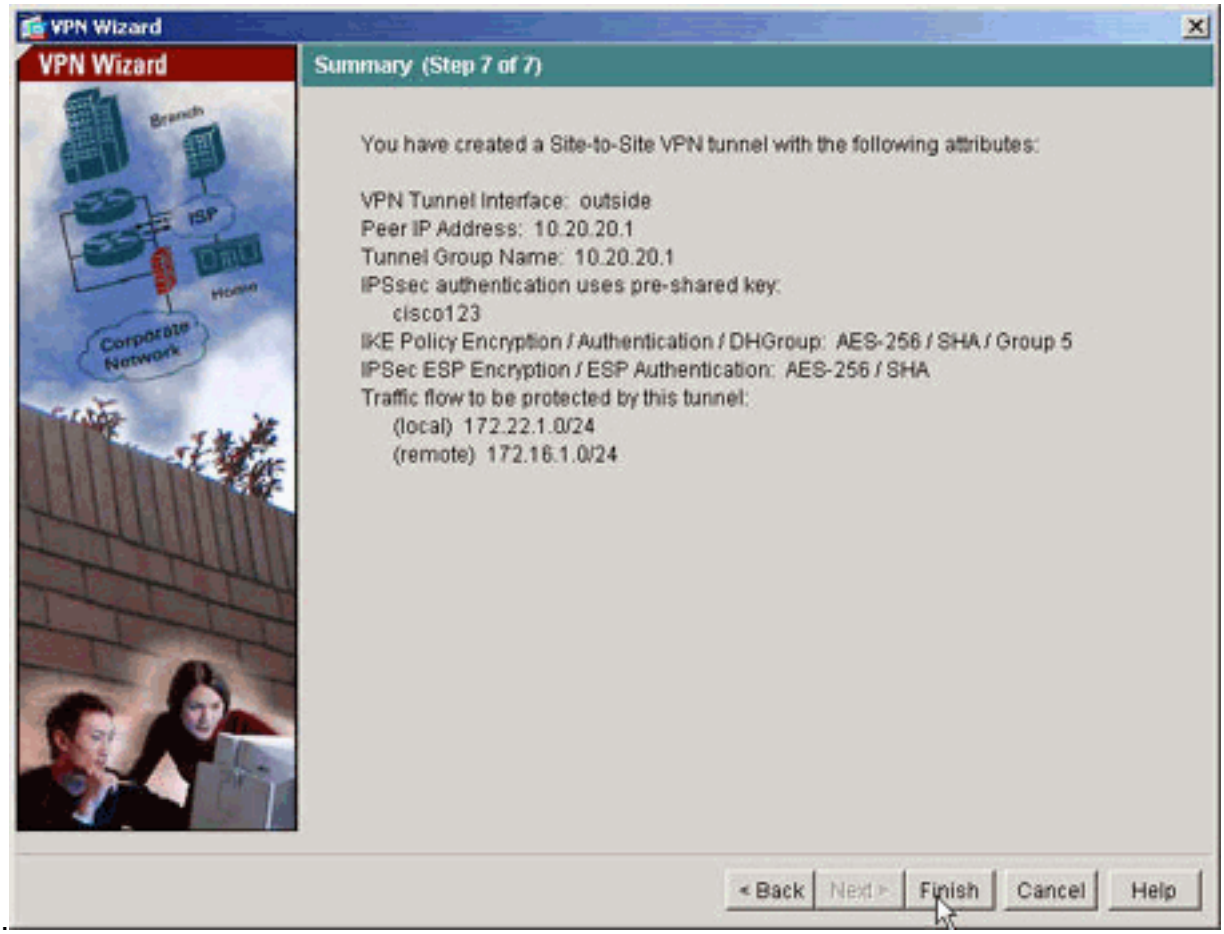
10. VPN 터널을 통과하도록 트래픽을 허용할 호스트를 지정합니다.이 단계에서는 pix515-704에 대한 로컬 호스트가 지정됩니다



11. 터널의 원격 쪽에 있는 호스트와 네트워크가 지정됩니다



12. VPN 마법사에서 정의한 특성이 이 요약에 표시됩니다.설정이 올바르면 구성을 다시 확인하고 **Finish(마침)**를 클릭합니다



PIX CLI 컨피그레이션

pix515-704

```
pixfirewall#show run
: Saved
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.10.10.1 255.255.255.0
!--- Configure the outside interface. ! interface
Ethernet1 nameif inside security-level 100 ip address
172.22.1.163 255.255.255.0 !--- Configure the inside
interface. ! !-- Output suppressed ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
group DefaultDNS domain-name default.domain.invalid
access-list inside_nat0_outbound extended permit ip
172.22.1.0 255.255.255.0 172 .16.1.0 255.255.255.0 !---
This access list (inside_nat0_outbound) is used with the
nat zero command. !--- This prevents traffic which
matches the access list from undergoing !--- network
address translation (NAT). The traffic specified by this
ACL is !--- traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
```

```
-- the same as (outside_cryptomap_20). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_cryptomap_20 extended permit ip
172.22.1.0 255.255.255.0 172
.16.1.0 255.255.255.0
!--- This access list (outside_cryptomap_20) is used
with the crypto map !--- outside_map to determine which
traffic should be encrypted and sent !--- across the
tunnel. !--- This ACL is intentionally the same as
(inside_nat0_outbound). !--- Two separate access lists
should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover

asdm image flash:/asdm-511.bin
!--- Enter this command to specify the location of the
ASDM image. asdm history enable arp timeout 14400 nat
(inside) 0 access-list inside_nat0_outbound !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound.

route outside 0.0.0.0 0.0.0.0 10.10.10.2 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


http server enable
!--- Enter this command in order to enable the HTTPS
server for ASDM. http 172.22.1.1 255.255.255.255 inside
!--- Identify the IP addresses from which the security
appliance !--- accepts HTTPS connections. no snmp-server
location no snmp-server contact !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. crypto ipsec transform-set ESP-AES-
256-SHA esp-aes-256 esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 20
match address outside_cryptomap_20 !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec
peer crypto map outside_map 20 set transform-set ESP-
AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-
256-SHA" !--- to be used with the crypto map entry
"outside_map". crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- Policy 65535 is included in the config
by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. isakmp
enable outside isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256 isakmp policy 10
hash sha isakmp policy 10 group 5 isakmp policy 10
lifetime 86400 isakmp policy 65535 authentication pre-
```

```
share isakmp policy 65535 encryption 3des isakmp policy
65535 hash sha isakmp policy 65535 group 2 isakmp policy
65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-
l2l !--- In order to create and manage the database of
connection-specific records !--- for ipsec-l2l-IPsec
(LAN-to-LAN) tunnels, use the tunnel-group !--- command
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 10.20.20.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared-key in order to configure the
authentication method. telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf : end
```

PIX-02

```
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on pix515-704.

access-list outside_cryptomap_20 extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
outside_cryptomap_20 !--- ACL on pix515-704.

pager lines 24
mtu inside 1500
```

```
mtu outside 1500
no failover
asdm image flash:/asdm-511.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
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
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256
esp-sha-hmac
crypto map outside_map 20 match address
outside_cryptomap_20
crypto map outside_map 20 set peer 10.10.10.1
crypto map outside_map 20 set transform-set ESP-AES-256-
SHA
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:677469124487070 5f858ad4e9b810874
: end
pixfirewall#
```

사이트 간 터널 백업

이 암호화 맵 엔트리에 대한 Backup Site-to-Site 기능에 대한 연결 유형을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set connection-type** 명령을 사용합니다.기본 설정으로 돌아가려면 이 명령의 `no` 형식을 사용합니다.

구문:

crypto map *map-name seq-num set* **connection-type {answer-only | originate-only | bidirectional}**

- **answer-only**—이 피어는 초기 독점 교환 중에 연결할 적절한 피어를 결정하기 위해 인바운드 IKE 연결에만 응답하도록 지정합니다.
- **bidirectional**—이 피어가 이 암호화 맵 엔트리를 기반으로 연결을 수락하고 시작할 수 있음을 지정합니다.이는 모든 사이트 간 연결에 대한 기본 연결 유형입니다.
- **originate-only**—이 피어가 연결할 적절한 피어를 결정하기 위해 첫 번째 전용 교환을 시작하도록 지정합니다.

crypto **map set connection-type** 명령은 백업 LAN-to-LAN 기능의 연결 유형을 지정합니다.연결의 한 끝에서 여러 백업 피어를 지정할 수 있습니다.이 기능은 다음 플랫폼 간에만 작동합니다.

- Cisco ASA 5500 Series 보안 어플라이언스 2개
- Cisco ASA 5500 Series 보안 어플라이언스 및 Cisco VPN 3000 Concentrator
- Cisco ASA 5500 Series Security Appliance 및 Cisco PIX Security Appliance Software 버전 7.0 이상을 실행하는 보안 어플라이언스

백업 LAN-to-LAN 연결을 구성하려면 연결의 한 쪽 끝을 originate-only 키워드로 originate-only 구성하고, 여러 백업 피어로 끝은 `answer-only` 키워드로 answer-only로 구성하는 것이 좋습니다 .originate-only end에서 **crypto map set peer** 명령을 사용하여 피어의 우선순위를 정렬합니다 .originate-only 보안 어플라이언스는 목록의 첫 번째 피어와 협상을 시도합니다.해당 피어가 응답하지 않을 경우, 보안 어플라이언스는 피어가 응답하거나 목록에 더 이상 피어가 없을 때까지 목록 아래로 작동합니다.

이러한 방식으로 구성된 경우 originate-only 피어는 처음에 전용 터널을 설정하고 피어와 협상하려고 시도합니다.그 후 두 피어가 정상적인 LAN-to-LAN 연결을 설정할 수 있으며, 두 종단 중 하나의 데이터가 터널 연결을 시작할 수 있습니다.

참고: 암호화 항목에 대해 여러 피어 IP 주소로 VPN을 구성한 경우 기본 피어가 다운되면 백업 피어 IP로 VPN이 설정됩니다.그러나 기본 피어가 돌아오면 VPN은 기본 IP 주소를 선점하지 않습니다 .VPN 협상을 다시 시작하여 기본 IP 주소로 전환하려면 기존 SA를 수동으로 삭제해야 합니다.결론에서 알 수 있듯이 VPN 선점은 사이트 간 터널에서 지원되지 않습니다.

지원되는 백업 LAN-to-LAN 연결 유형

원격 측	중앙 쪽
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

예

글로벌 컨피그레이션 모드에서 입력된 이 예에서는 **암호화 맵 mymap을 구성하고** connection-type을 originate-only로 *설정합니다*.

```
hostname(config)#crypto map outside_map 20 connection-type originate-only
```

SA(보안 연결 지우기)

PIX의 권한 모드에서 다음 명령을 사용합니다.

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

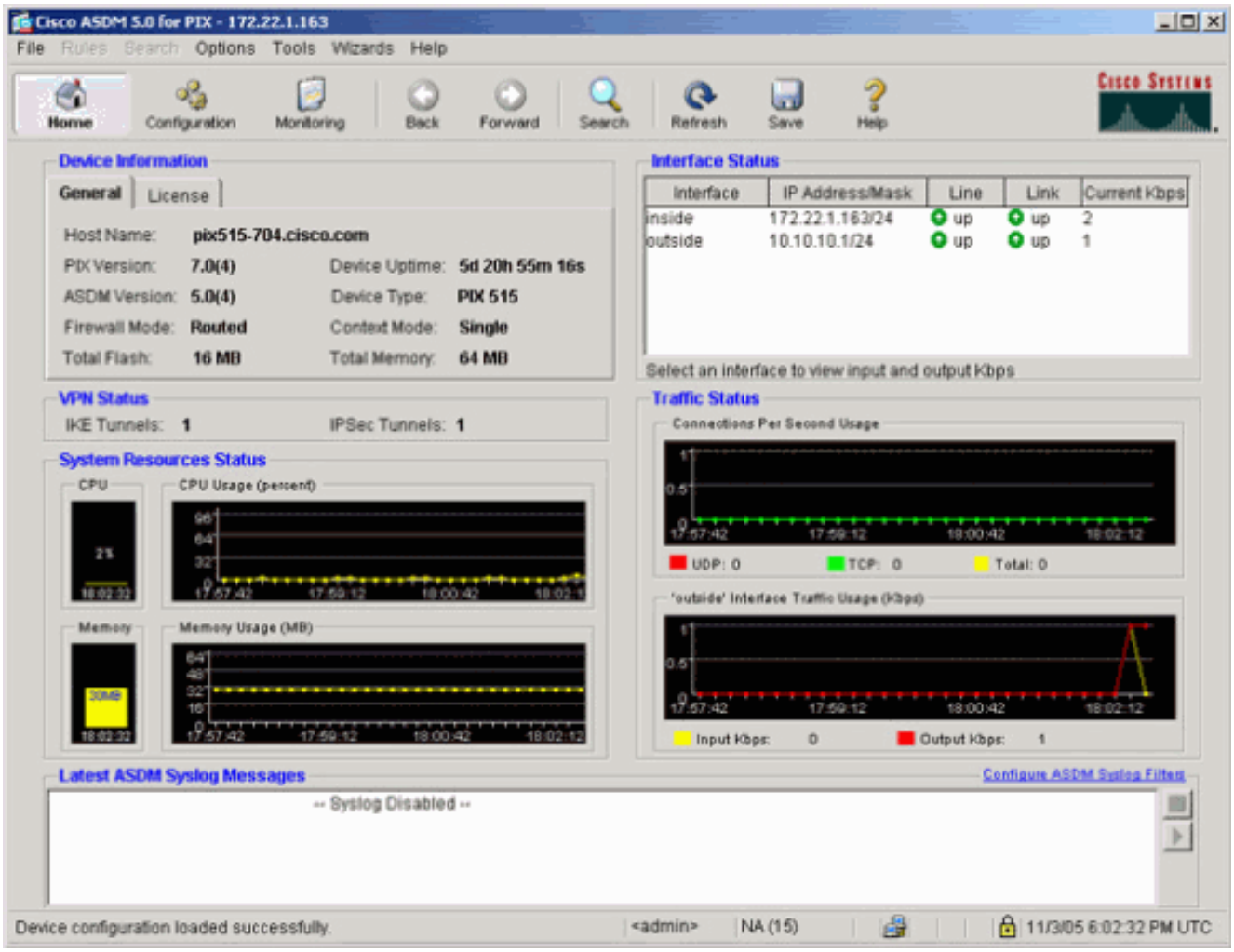
다음을 확인합니다.

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.

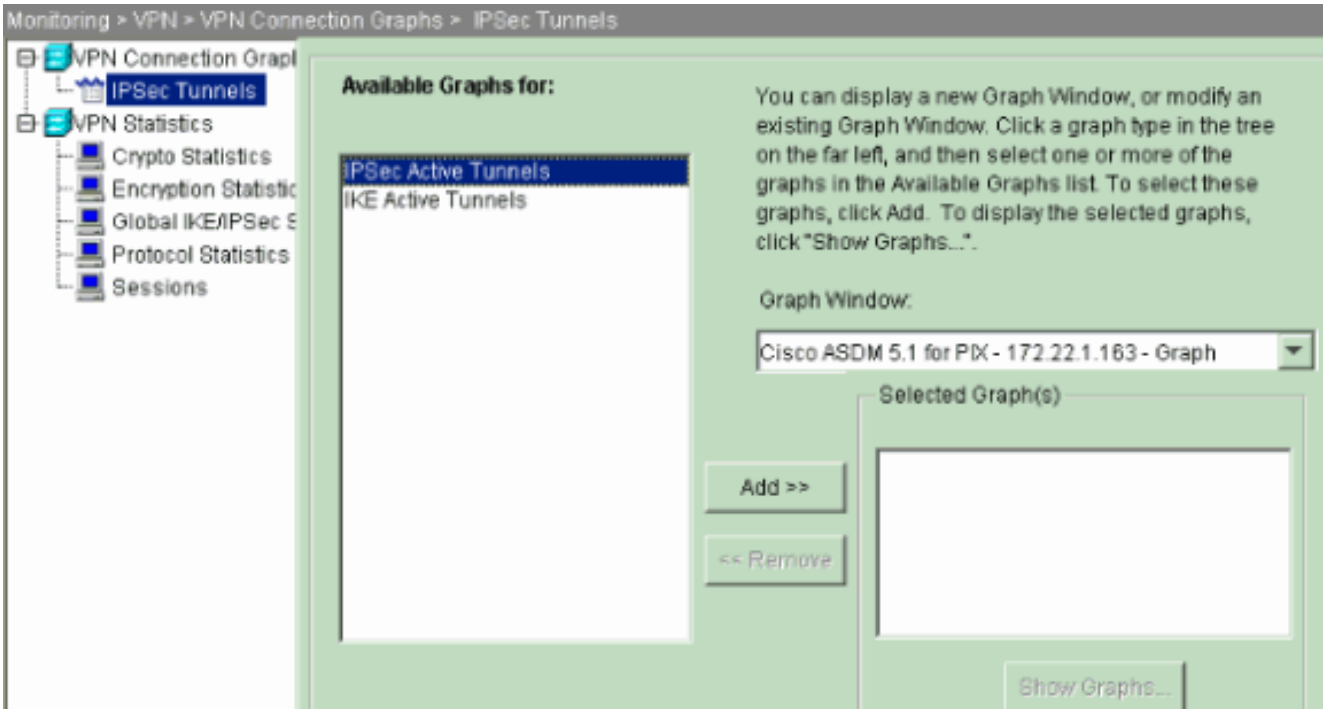
피어에 대한 흥미로운 트래픽이 있는 경우 터널은 pix515-704와 PIX-02 사이에 설정됩니다.

1. ASDM의 **Home**(홈)에서 VPN Status(VPN 상태)를 확인하여 터널의 구성을 확인합니다
   .



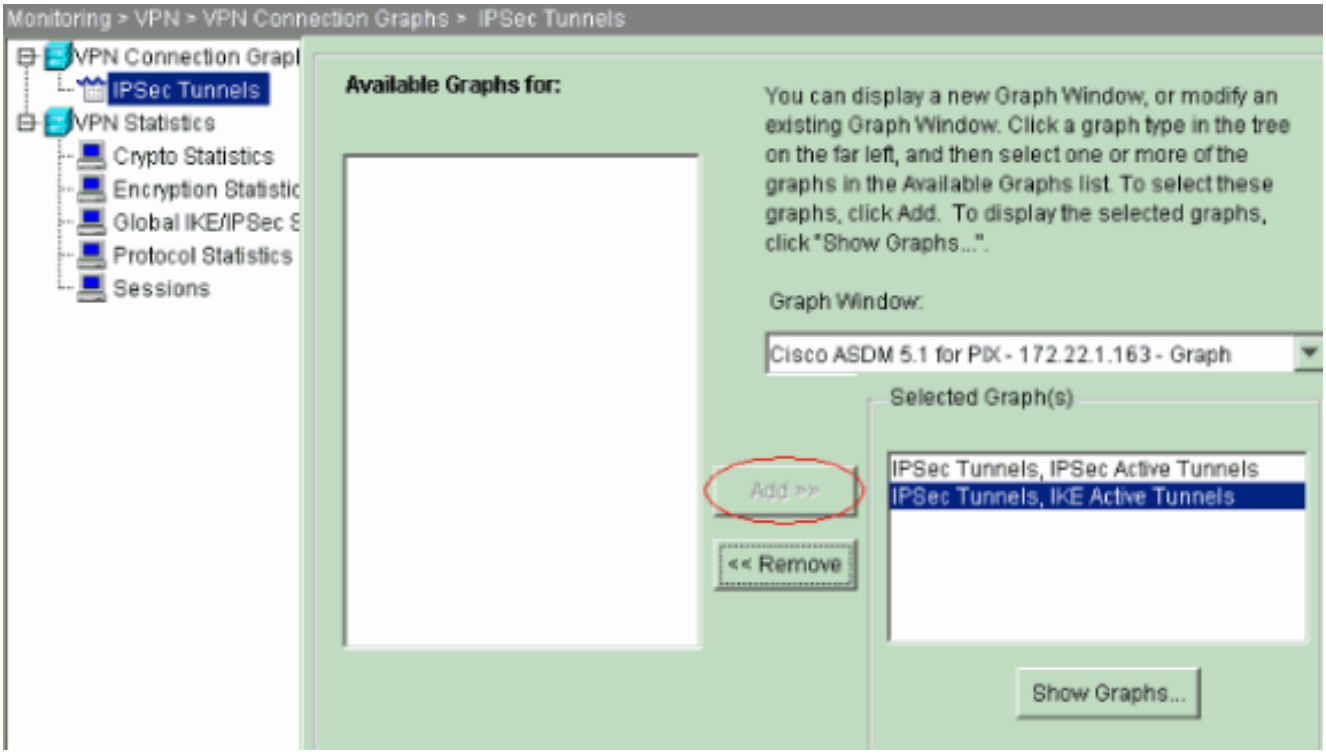
2. Monitoring(**모니터링**) > **VPN** > **VPN Connection Graphs(VPN 연결 그래프)** > **IPSec Tunnels(IPSec 터널)를 선택하여** 터널 설정에 대한 세부 정보를 확인합니다

.

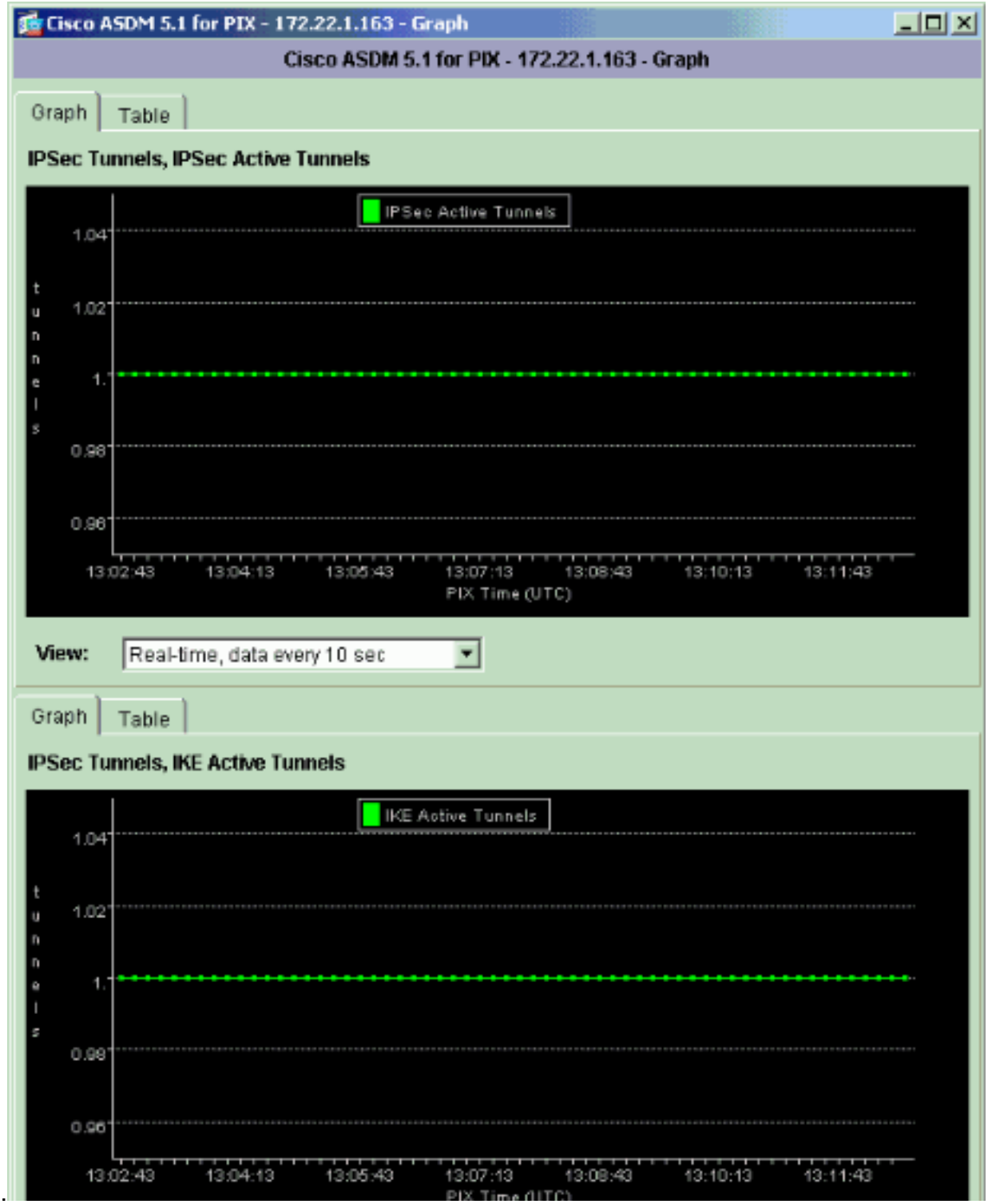


3. Add(**추가**)를 클릭하여 그래프 창에서 볼 수 있는 그래프를 선택합니다

.



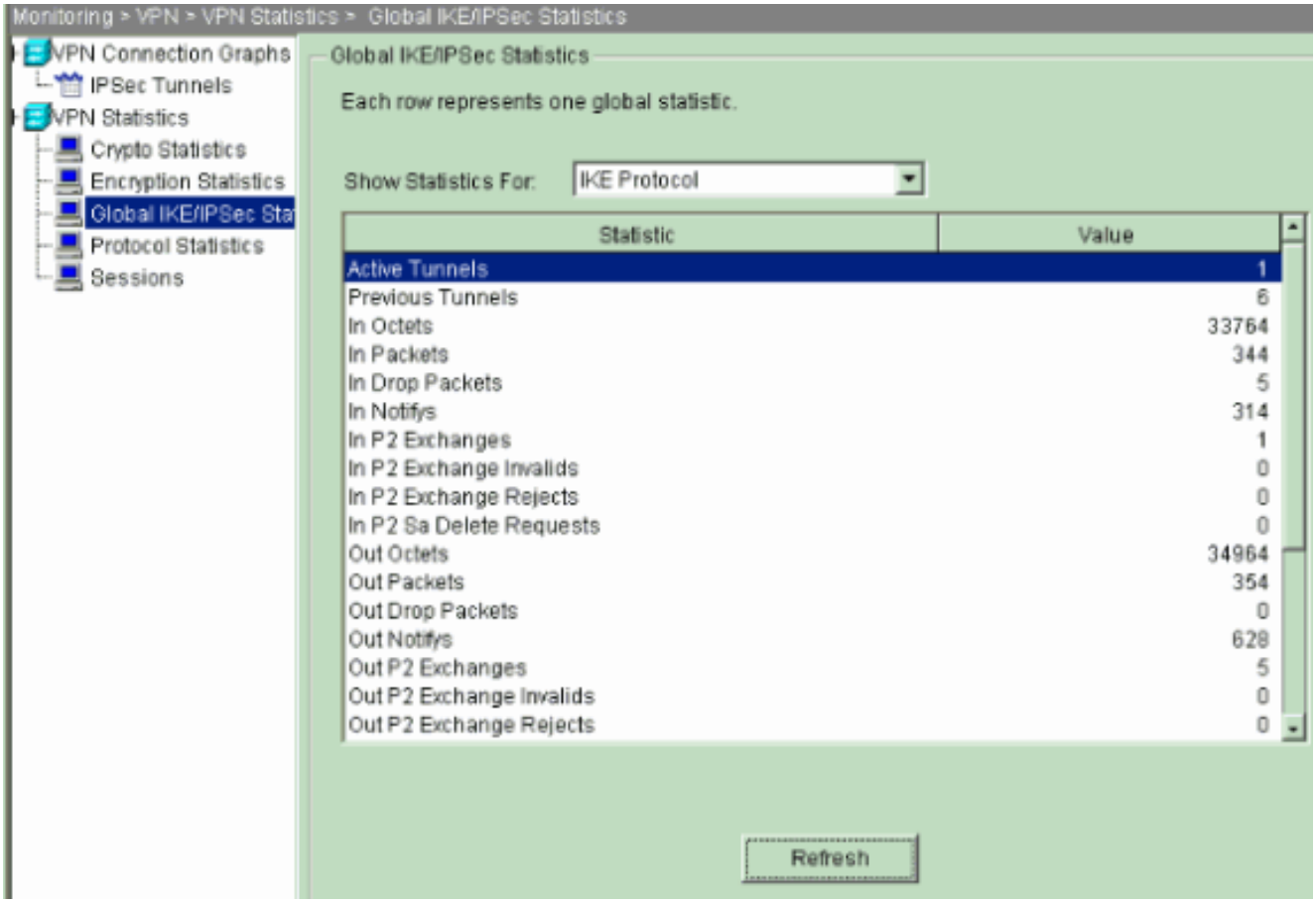
4. IKE 및 IPsec 활성 터널의 그래프를 보려면 Show Graphs를 클릭합니다



.

5. VPN 터널의 통계 정보를 확인하려면 Monitoring > VPN > VPN Statistics > Global IKE/IPSec Statistics를 선택합니다

.



CLI를 사용하여 터널 구성을 확인할 수도 있습니다.show crypto isakmp **sa** 명령을 실행하여 터널 구성을 확인하고 **show crypto ipsec sa** 명령을 실행하여 캡슐화, 암호화 등의 패킷 수를 확인합니다 .

pix515-704

```
pixfirewall(config)#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: 10.20.20.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

pix515-704

```
pixfirewall(config)#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local
addr: 10.10.10.1

     access-list outside_cryptomap_20 permit ip
172.22.1.0
       255.255.255.0 172.16.1.0 255.255.255.0
     local ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
     current_peer: 10.20.20.1

      #pkts encaps: 20, #pkts encrypt: 20, #pkts digest:
```

```
20
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify:
20
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 20, #pkts comp failed: 0,
#pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

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

      path mtu 1500, ipsec overhead 76, media mtu 1500
      current outbound spi: 44532974

    inbound esp sas:
      spi: 0xA87AD6FA (2826622714)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec):
(3824998/28246)
         IV size: 16 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x44532974 (1146300788)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec):
(3824998/28245)
         IV size: 16 bytes
         replay detection support: Y
```

문제 해결

PFS

IPsec 협상에서 PFS(Perfect Forward Secrecy)는 각 새 암호화 키가 이전 키와 관련이 없도록 합니다.두 터널 피어에서 PFS를 활성화 또는 비활성화하십시오. 그렇지 않으면 L2L IPsec 터널이 PIX/ASA에 설정되지 않습니다.

PFS는 기본적으로 비활성화되어 있습니다.PFS를 활성화하려면 그룹 정책 컨피그레이션 모드에서 enable **키워드**와 함께 pfs 명령을 사용합니다.PFS를 비활성화하려면 disable 키워드***를 입력합니다***.

```
hostname(config-group-policy)#pfs {enable | disable}
```

실행 중인 컨피그레이션에서 PFS 특성을 제거하려면 이 명령의 **no** 형식을 입력합니다.그룹 정책은 다른 그룹 정책에서 PFS에 대한 값을 상속할 수 있습니다.값 상속을 방지하려면 이 명령의 **no** 형식을 입력합니다.

```
hostname(config-group-policy)#no pfs
```

관리-액세스

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

PIX의 내부 인터페이스는 management-access 명령이 전역 컨피그레이션 모드에서 구성되지 않으면 터널의 다른 쪽 끝에서 ping할 수 없습니다.

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

디버그 명령

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

debug crypto isakmp - IPsec 연결에 대한 디버그 정보를 표시하고 양쪽 끝에서 비호환성으로 인해 거부된 첫 번째 특성 집합을 표시합니다.

디버그 암호화 isakmp

```
pixfirewall(config)#debug crypto isakmp 7
Nov 27 12:01:59 [IKEv1 DEBUG]: Pitcher: received a key
acquire message,
spi 0x0
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE Initiator:
New Phase 1,
Intf 2, IKE Peer 10.20.20.1  local Proxy Address
172.22.1.0, remote
Proxy Address 172.16.1.0,  Crypto map (outside_map)
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing ISAKMP SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing Fragmentation
VID + extended capabilities payload
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=0) with payloads : HDR +
 SA (1) + VENDOR (13) + NONE (0) total length : 148
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0)
total length : 112
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley
proposal is acceptable
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Fragmentation VID
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer
included
IKE fragmentation capability flags
:  Main Mode:        True  Aggressive Mode:  True
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing Cisco Unity VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
```

```
constructing xauth V6 VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS
VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities:
20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send
Altiga/
Cisco VPN3000/Cisco ASA GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13)
+ VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NONE (0) total length
 : 320
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message
(msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) +
NONE (0) total length : 320
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing ISA_KE payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Cisco Unity client VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
xauth V6 VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Processing VPN3000/ASA
spoofing IOS Vendor ID payload (version: 1.0.0,
capabilities: 20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Altiga/Cisco VPN3000/Cisco ASA
GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection
landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, Generating keys
for Initiator...
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
```

```
Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing dpd vid payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE
(14) + VENDOR (13) +
NONE (0) total length : 119
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE
(14) + VENDOR (13) +
NONE (0) total length : 96
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Processing IOS keep alive payload: proposal=32767/32767
sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Received DPD VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection
landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Oakley begin quick mode
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1, PHASE 1 COMPLETED
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive
type for this connection: DPD
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Starting phase 1 rekey timer: 73440000 (ms)
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, IKE got
SPI from key engine: SPI = 0x44ae0956
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
oakley constucting quick mode
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing blank hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing IPSec SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing IPSec nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing proxy ID
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
```

```
10.20.20.1,
Transmitting Proxy Id:
  Local subnet:  172.22.1.0  mask 255.255.255.0 Protocol
0  Port 0
  Remote subnet: 172.16.1.0  Mask 255.255.255.0 Protocol
0  Port 0
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing qm hash payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5)
+ NOTIFY (11) +
NONE (0) total length : 200
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message
(msgid=d723766b) with payloads
 : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID
(5) + NONE (0)
 total length : 172
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
loading all IPSEC SAs
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
Security negotiation complete for LAN-to-LAN Group
(10.20.20.1)
Initiator, Inbound SPI = 0x44ae0956, Outbound SPI =
0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
oakley constructing final quick mode
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
IKE got a KEY_ADD msg for SA: SPI = 0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Pitcher: received KEY_UPDATE, spi 0x44ae0956
```

```
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
 Starting P2 Rekey timer to expire in 24480 seconds
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
PHASE 2 COMPLETED (msgid=d723766b)
```

debug crypto ipsec - IPsec 연결에 대한 디버그 정보를 표시합니다.

디버그 암호화 ipsec

```
pix1(config)#debug crypto ipsec 7

exec mode commands/options:
  <1-255>  Specify an optional debug level (default is
1)
  <cr>
pix1(config)# debug crypto ipsec 7
pix1(config)# IPSEC: New embryonic SA created @
0x024211B0,
    SCB: 0x0240AEB0,
    Direction: inbound
    SPI      : 0x2A3E12BE
    Session ID: 0x00000001
    VPIF num  : 0x00000001
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: New embryonic SA created @ 0x0240B7A0,
    SCB: 0x0240B710,
    Direction: outbound
    SPI      : 0xB283D32F
    Session ID: 0x00000001
    VPIF num  : 0x00000001
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xB283D32F
IPSEC: Updating outbound VPN context 0x02422618, SPI
0xB283D32F
    Flags: 0x00000005
    SA   : 0x0240B7A0
    SPI  : 0xB283D32F
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x00000000
    SCB  : 0x0240B710
    Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
    VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
    Rule ID: 0x01FA0290
IPSEC: New outbound permit rule, SPI 0xB283D32F
    Src addr: 10.10.10.1
    Src mask: 255.255.255.255
    Dst addr: 10.20.20.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
```

```
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0xB283D32F
    Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xB283D32F
    Rule ID: 0x0240AF40
IPSEC: Completed host IBSA update, SPI 0x2A3E12BE
IPSEC: Creating inbound VPN context, SPI 0x2A3E12BE
    Flags: 0x00000006
    SA   : 0x024211B0
    SPI  : 0x2A3E12BE
    MTU  : 0 bytes
    VCID : 0x00000000
    Peer : 0x02422618
    SCB  : 0x0240AEB0
    Channel: 0x014A45B0
IPSEC: Completed inbound VPN context, SPI 0x2A3E12BE
    VPN handle: 0x0240BF80
IPSEC: Updating outbound VPN context 0x02422618, SPI
0xB283D32F
    Flags: 0x00000005
    SA   : 0x0240B7A0
    SPI  : 0xB283D32F
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x0240BF80
    SCB  : 0x0240B710
    Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
    VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
    Rule ID: 0x01FA0290
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
    Rule ID: 0x0240AF40
IPSEC: New inbound tunnel flow rule, SPI 0x2A3E12BE
    Src addr: 172.16.1.0
    Src mask: 255.255.255.0
    Dst addr: 172.22.1.0
    Dst mask: 255.255.255.0
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 0
    Use protocol: false
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI
0x2A3E12BE
    Rule ID: 0x0240B108
IPSEC: New inbound decrypt rule, SPI 0x2A3E12BE
    Src addr: 10.20.20.1
    Src mask: 255.255.255.255
    Dst addr: 10.10.10.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
```

```
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x2A3E12BE
    Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x2A3E12BE
    Rule ID: 0x02406E98
IPSEC: New inbound permit rule, SPI 0x2A3E12BE
    Src addr: 10.20.20.1
    Src mask: 255.255.255.255
    Dst addr: 10.10.10.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x2A3E12BE
    Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x2A3E12BE
    Rule ID: 0x02422C78
```

관련 정보

- PDM을 사용하여 방화벽 간 이중 터널 생성
- Cisco PIX 방화벽 소프트웨어
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems