SDM:ASA/PIX와 IOS 라우터 간 사이트 대 사이트 IPsec VPN 컨피그레이션 예

목차

소개

이 문서에서는 Cisco Security Appliance(ASA/PIX)와 Cisco IOS Router 간의 LAN-to-LAN(Site-to-Site) IPsec 터널에 대한 샘플 컨피그레이션을 제공합니다.고정 경로는 간소화를 위해 사용됩니다.

PIX/ASA Security Appliance에서 소프트웨어 버전 *7.x*를 실행하는 동일한 시나리오에 대한 자세한 내용은 IOS 라우터 LAN-to-LAN IPsec 터널 구성 예를 참조하십시오.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 이 구성을 시작하기 전에 엔드 투 엔드 IP 연결을 설정해야 합니다.
- DES(Data Encryption Standard) 암호화(최소 암호화 수준)에 대해 Security Appliance 라이센스를 활성화해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA(Adaptive Security Appliance) 버전 8.x 이상
- ASDM 버전 6.x.x 이상
- Cisco 1812 라우터(Cisco IOS® 소프트웨어 릴리스 12.3 포함)
- Cisco SDM(Security Device Manager) 버전 2.5

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

참고: SDM이 라우터를 구성하도록 허용하려면 SDM을 사용하여 기본 라우터 컨피그레이션을 참조하십시오.

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.

참고: Configuration Professional을 참조하십시오.ASA/PIX와 IOS 라우터 간 Site-to-Site IPsec VPN 라우터에서 Cisco Configuration Professional을 사용하는 유사한 구성의 예

관련 제품

이 컨피그레이션은 버전 7.x 이상을 실행하는 Cisco PIX 500 Series Security Appliance에서도 사용할 수 있습니다.

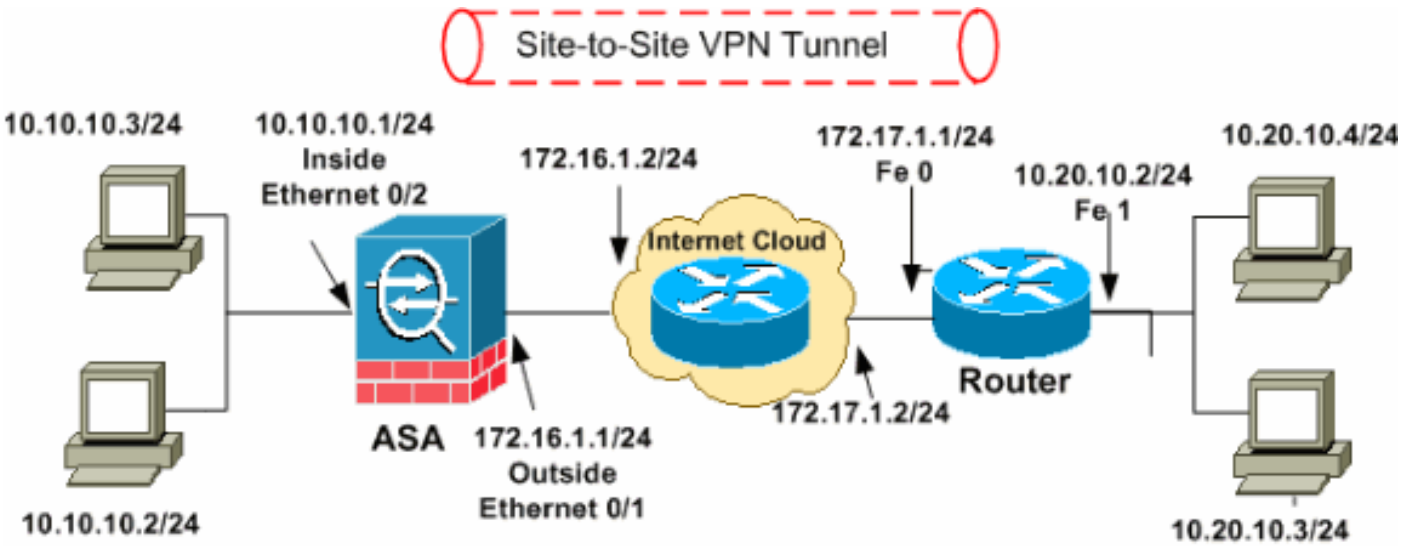
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



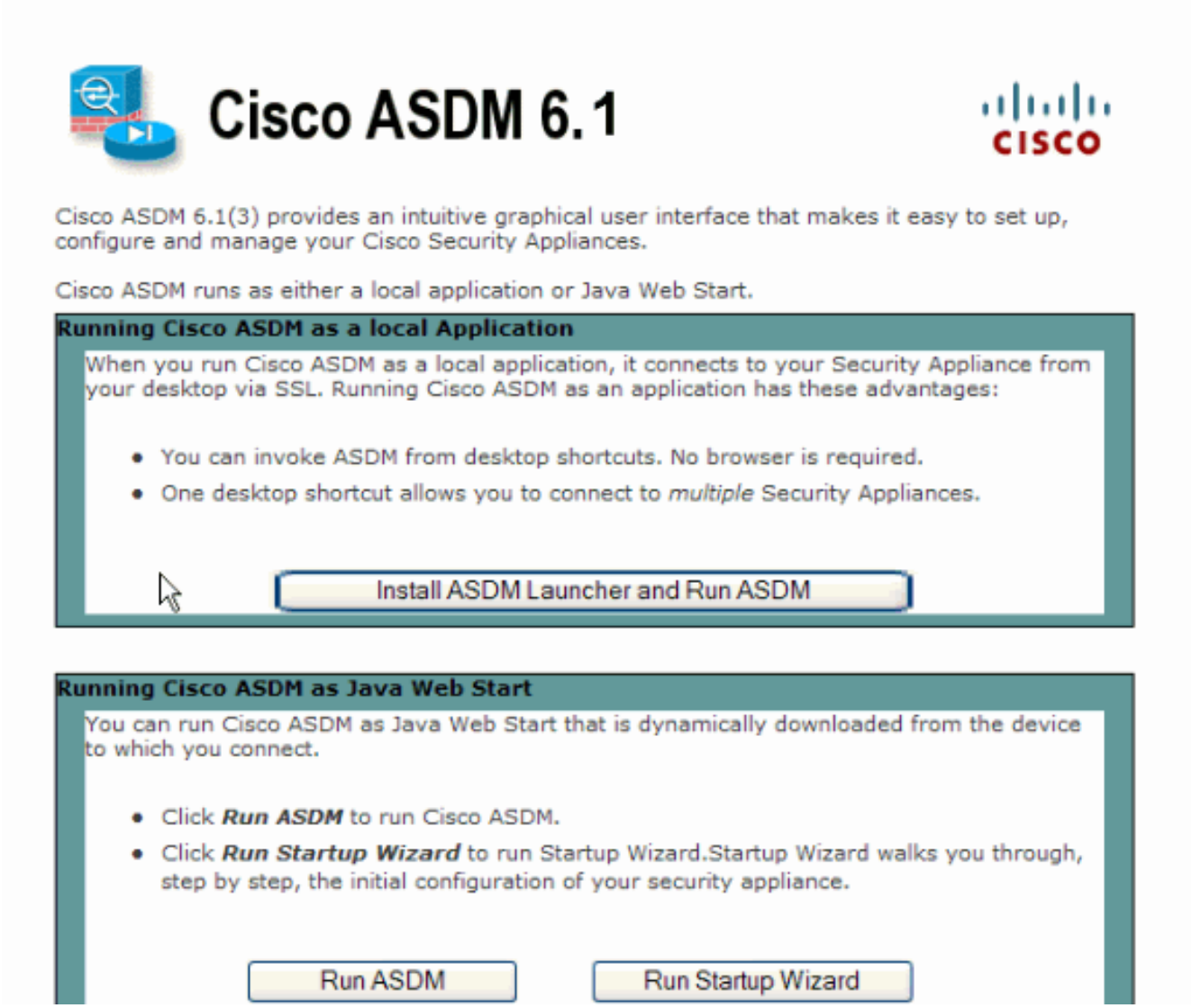
참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

- VPN 터널 ASDM 컨피그레이션
- 라우터 SDM 컨피그레이션
- ASA CLI 컨피그레이션
- 라우터 CLI 컨피그레이션

VPN 터널 ASDM 컨피그레이션

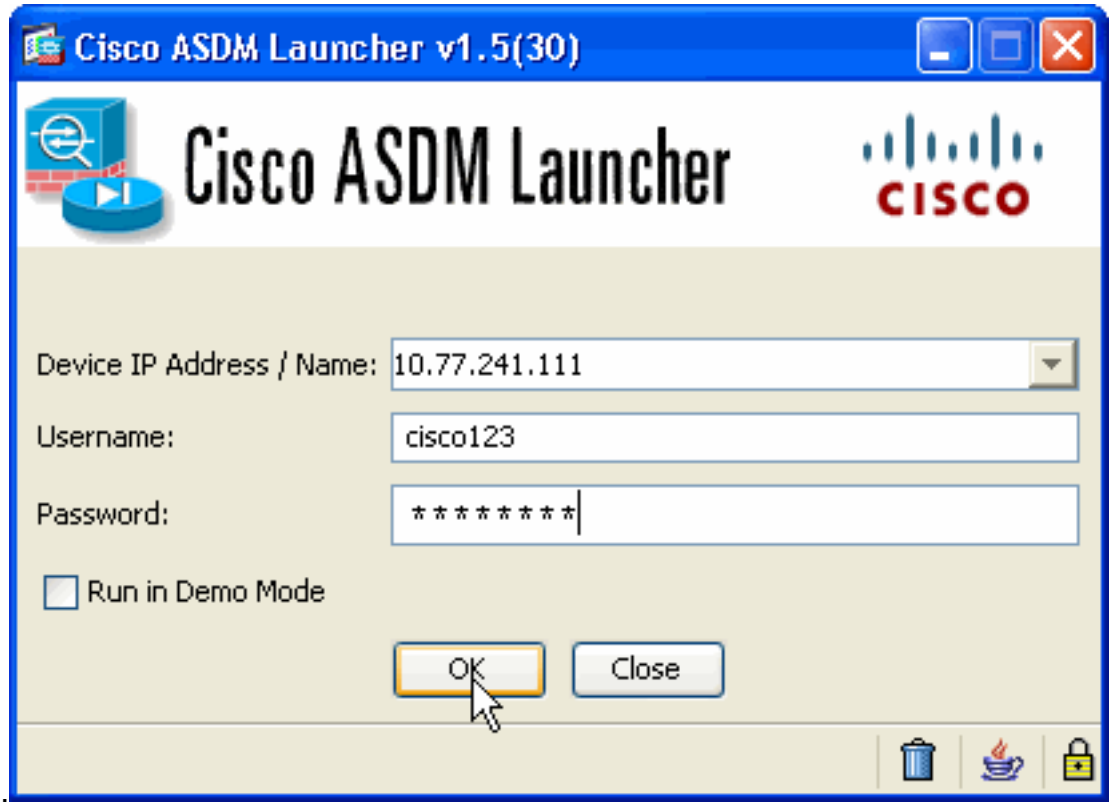
VPN 터널을 생성하려면 다음 단계를 완료합니다.

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



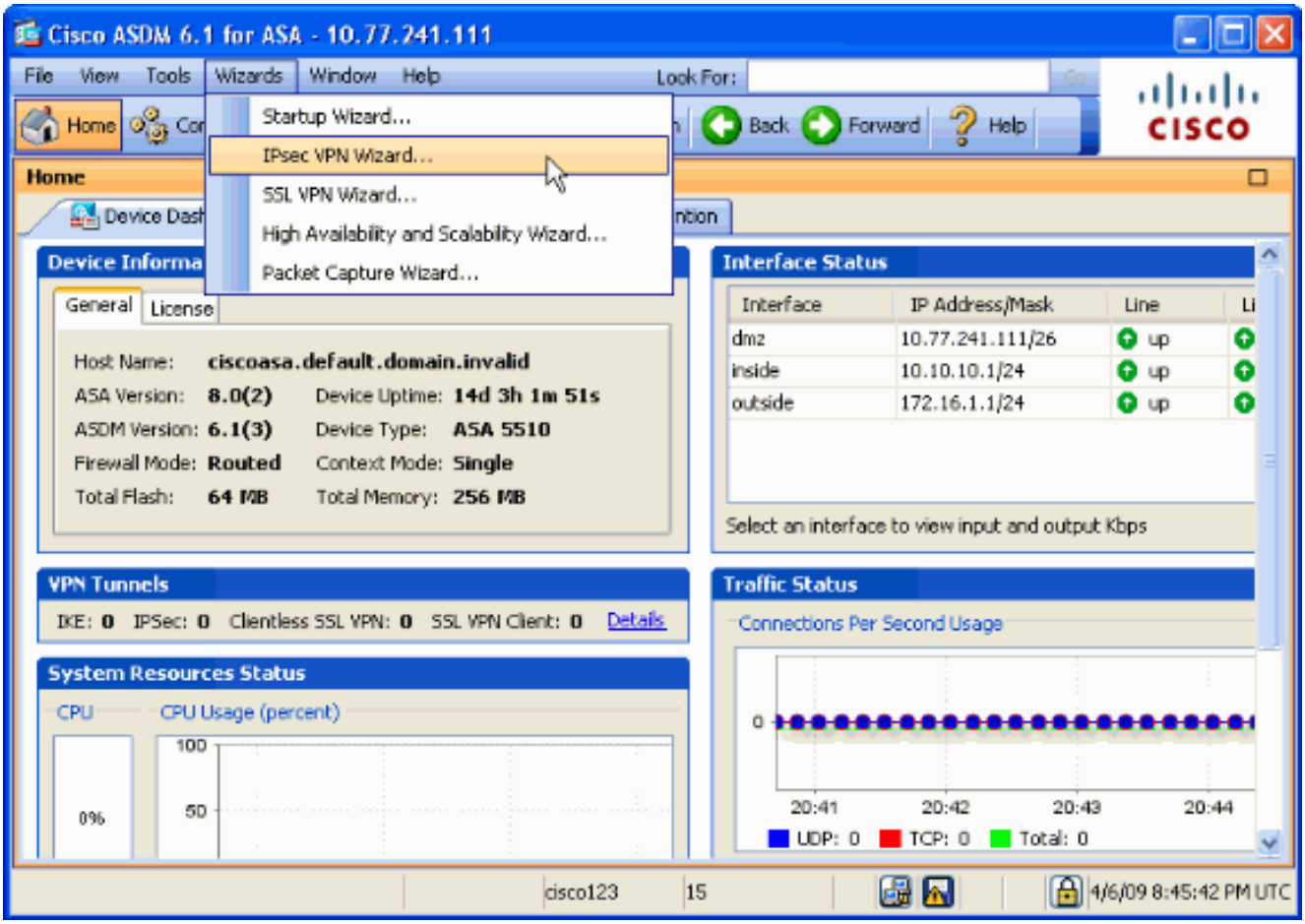
2. ASDM 애플리케이션 **설치** 프로그램을 다운로드하려면 **Download ASDM Launcher and Start ASDM(ASDM 시작** 시작 **시작**)을 클릭합니다.
3. ASDM Launcher가 다운로드되면, 소프트웨어를 설치하고 Cisco ASDM Launcher를 실행하기 위해 프롬프트에 의해 지시된 단계를 완료합니다.

4. **http -** 명령으로 구성한 인터페이스의 IP 주소를 입력하고 사용자 이름과 비밀번호를 지정한 경우 입력합니다.이 예에서는 **cisco123**을 사용자 이름에 사용하고 **cisco123**을 비밀번호로 사용합니다.



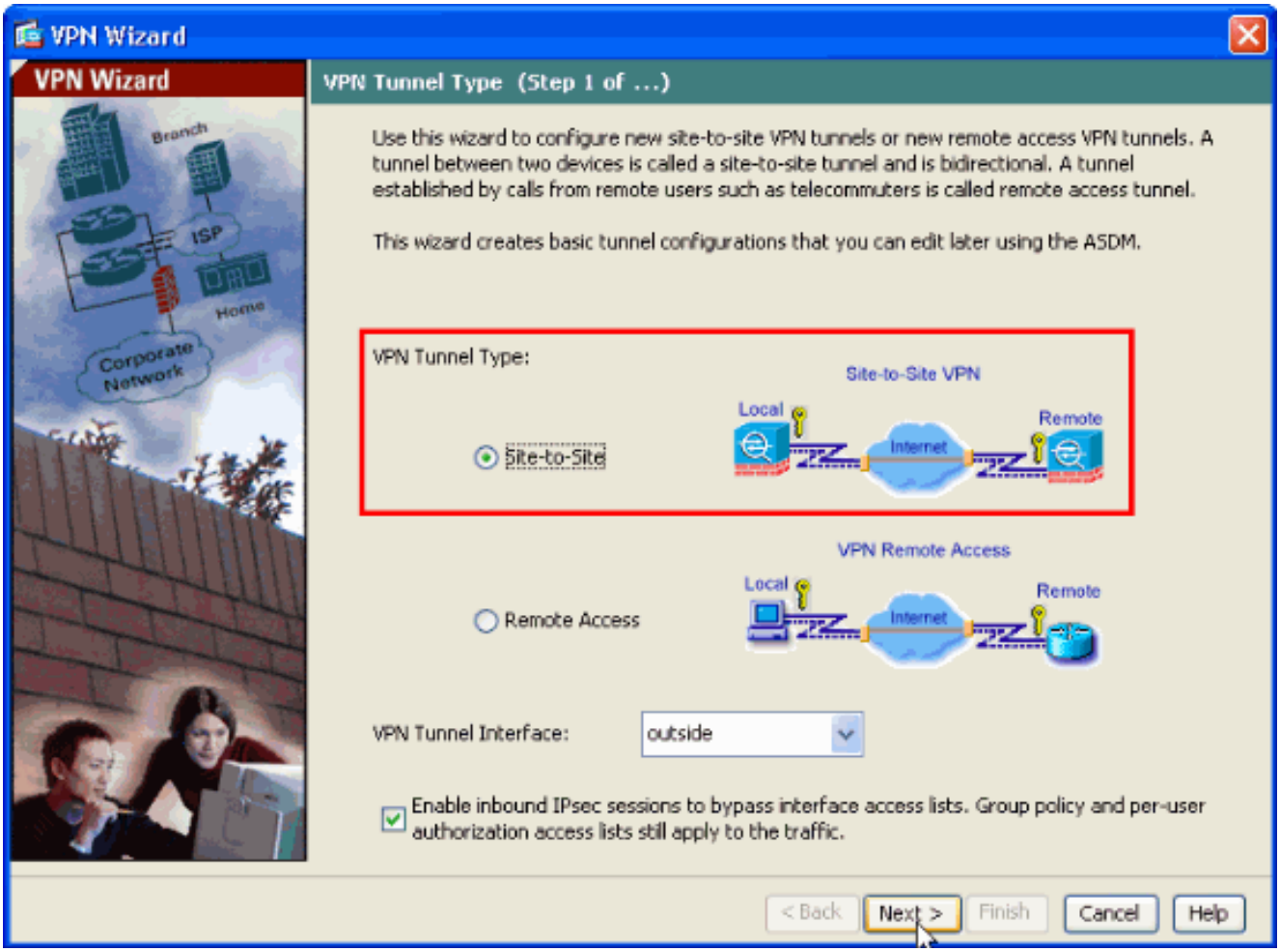
5. ASDM 애플리케이션이 ASA에 연결되면 IPsec VPN **마법사**를 실행합니다

.



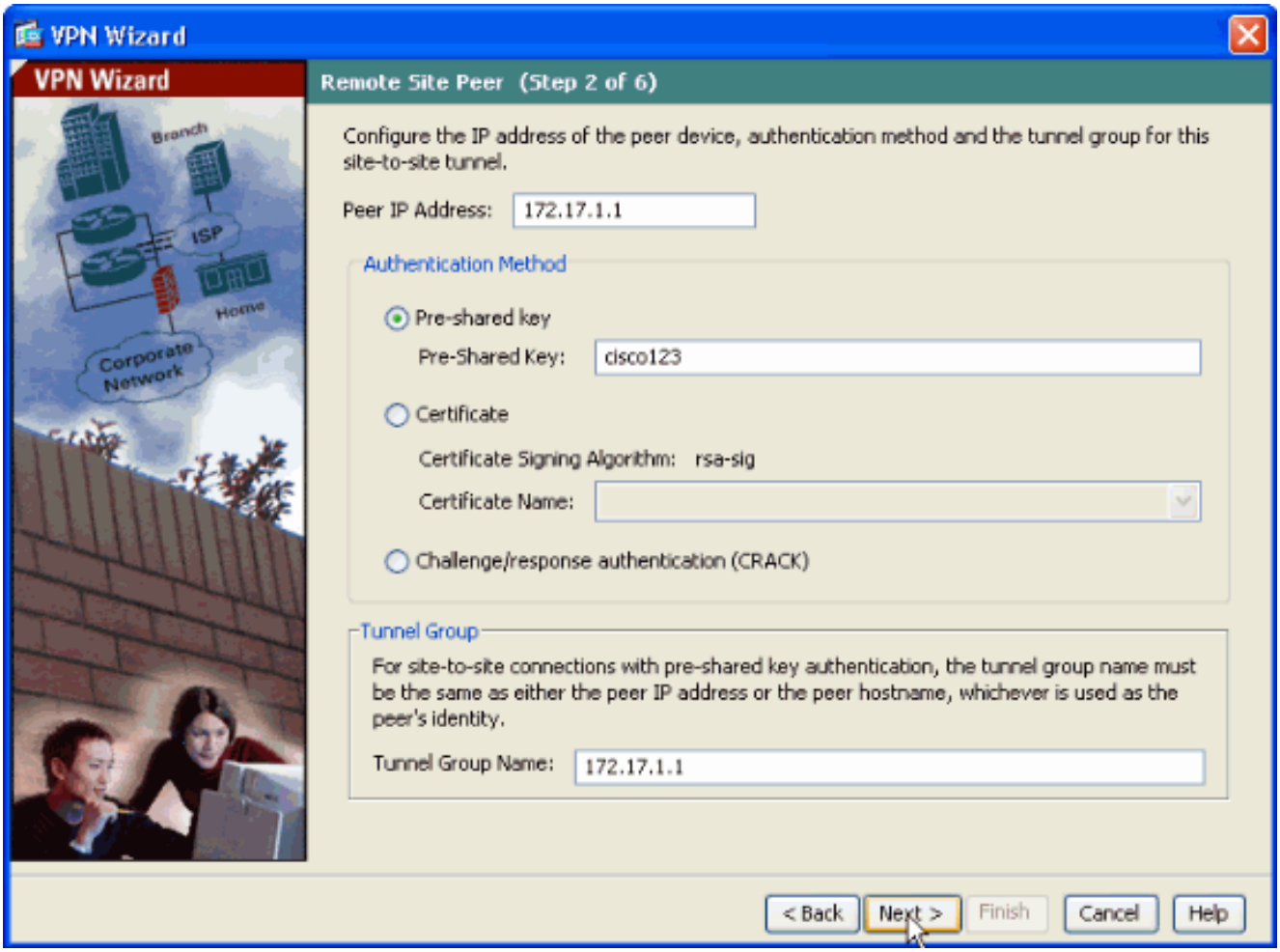
6. Site-**to-Site** IPsec VPN 터널 유형을 선택하고 여기**와** 같이 **Next(다음)**를 클릭합니다

.



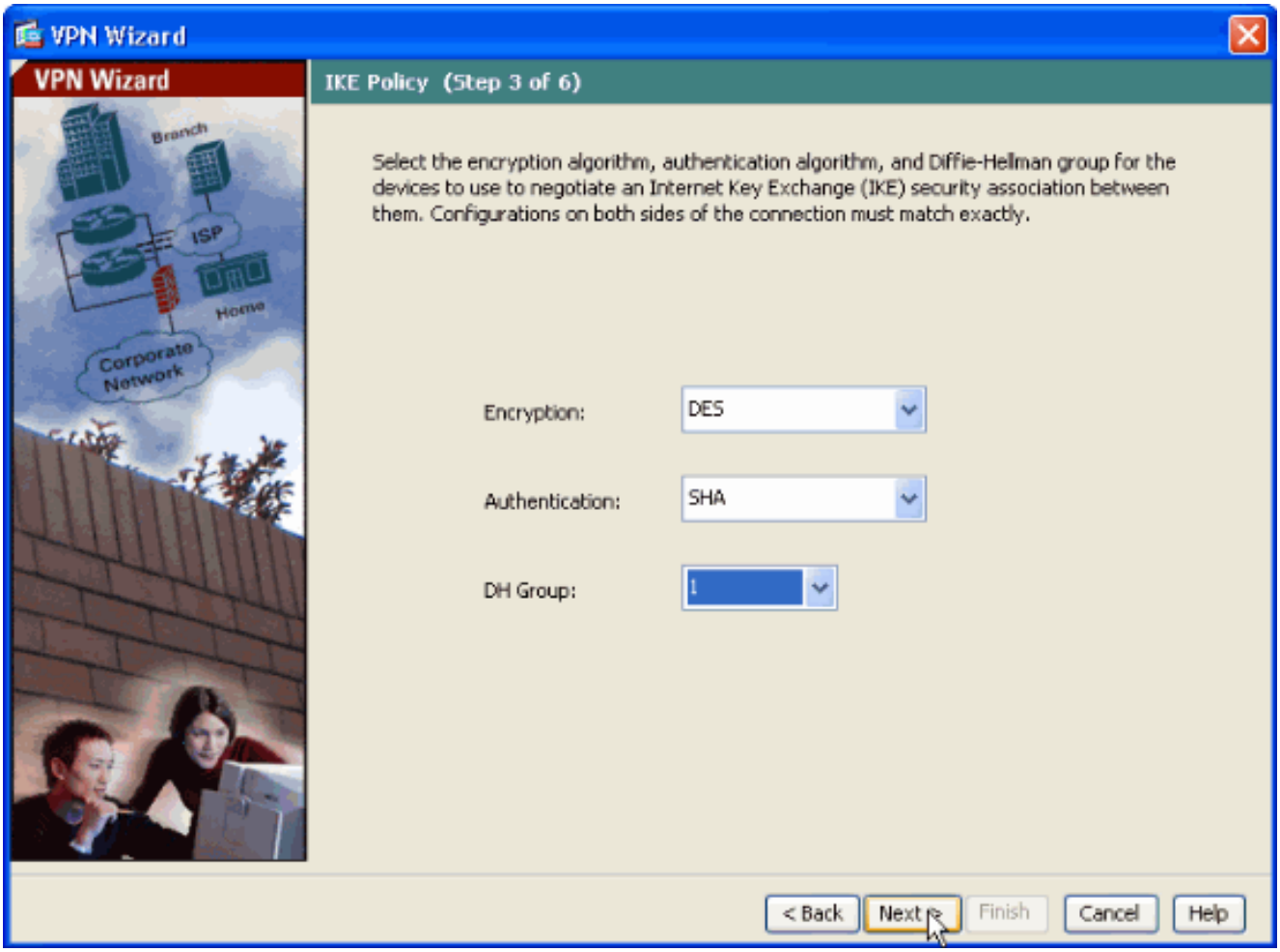
7. 원격 피어의 외부 IP 주소를 지정합니다.이 예에서 사전 공유 키인 사용할 인증 정보를 입력합니다.이 예에서 사용된 사전 공유 키는 **cisco123**입니다. L2L VPN을 구성하는 경우 기본적으로 **터널 그룹 이름**은 외부 IP 주소가 됩니다.Next(**다음)를 클릭합니다**

.



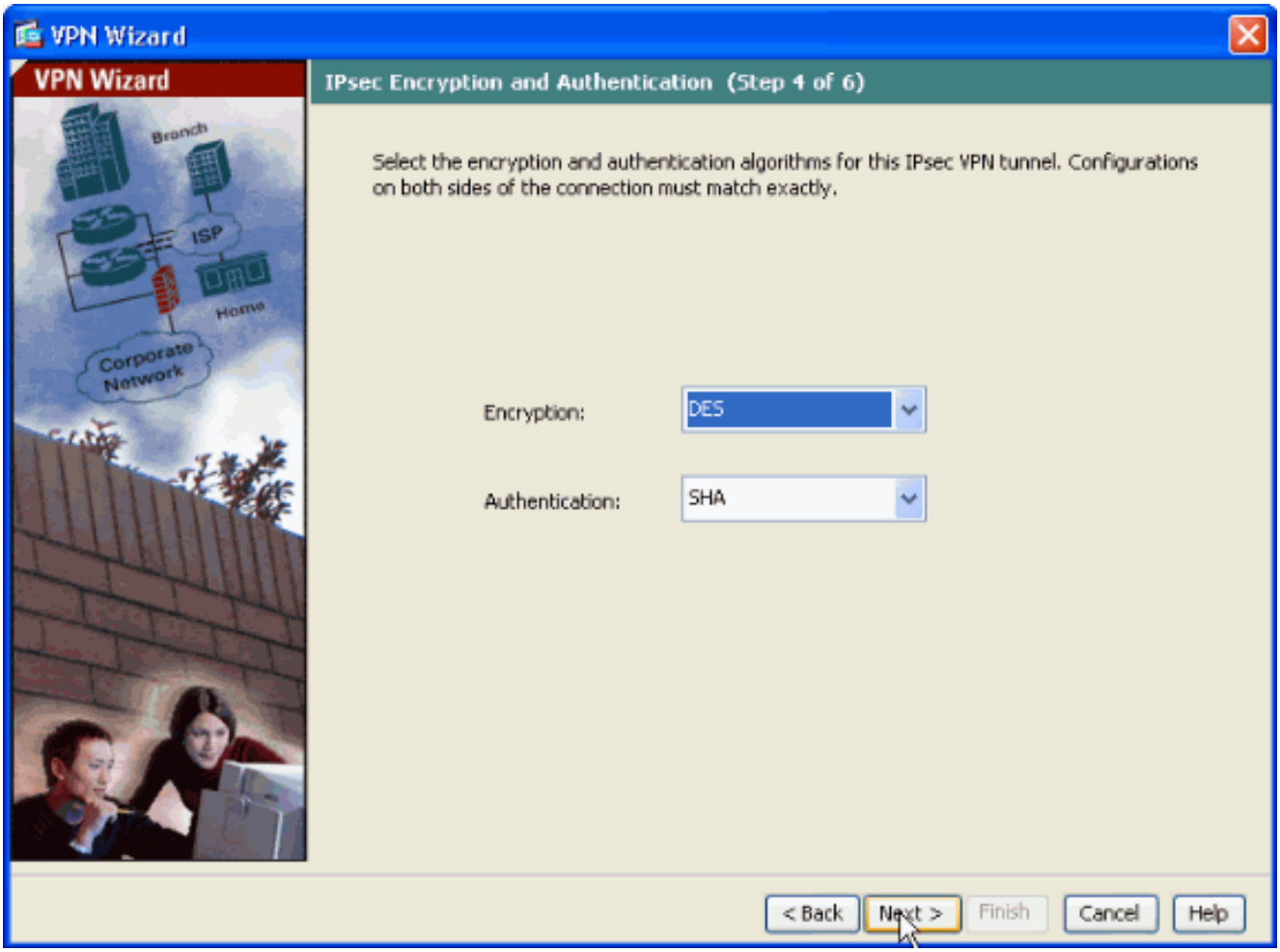
8. 1단계라고도 하는 IKE에 사용할 특성을 지정합니다. 이러한 특성은 ASA와 IOS 라우터 모두에서 동일해야 합니다.Next(**다음)를 클릭합니다**

.

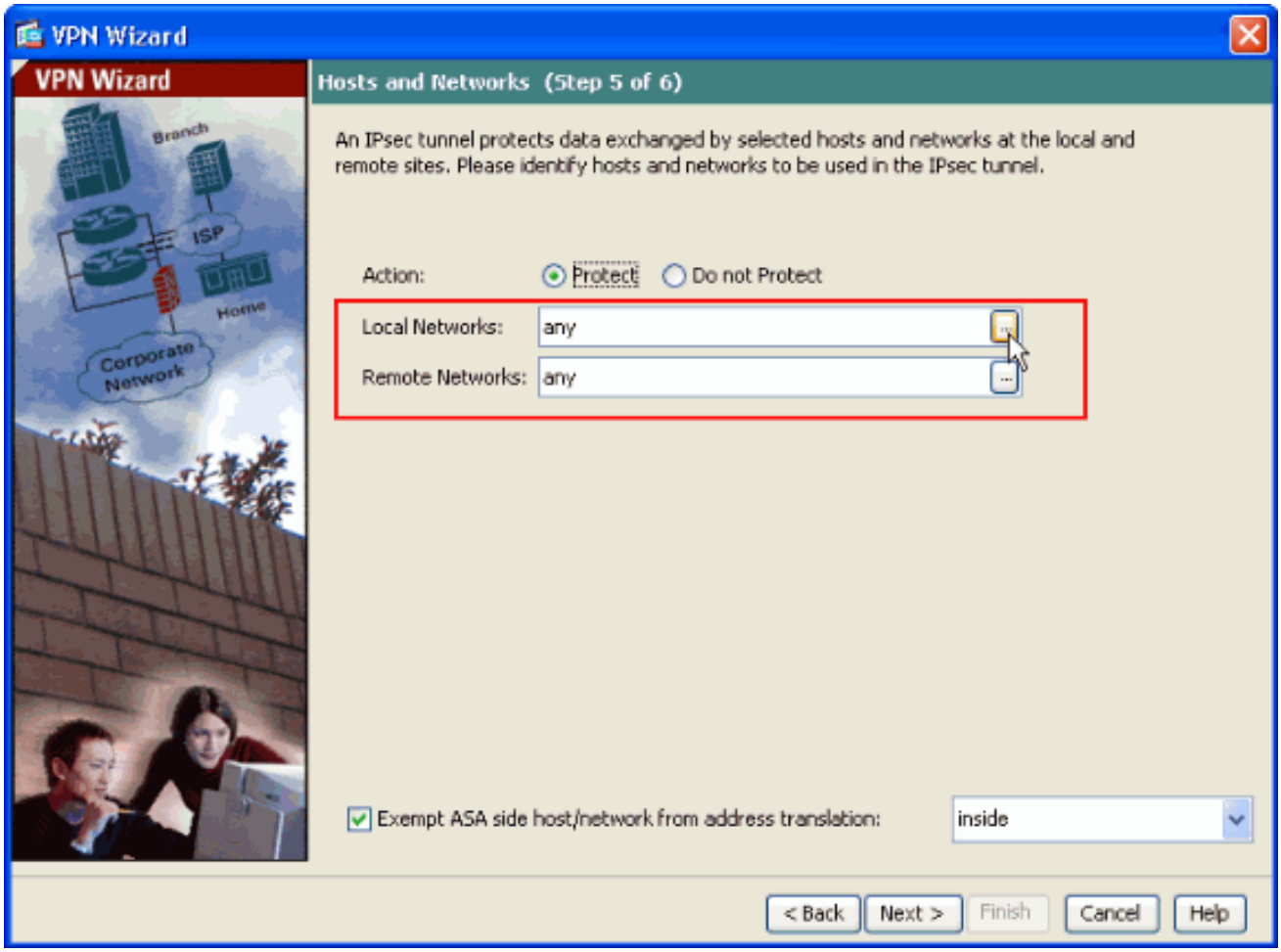


9. IPsec(2단계라고도 함)에 사용할 특성을 지정합니다. 이러한 특성은 ASA와 IOS 라우터 모두에서 일치해야 합니다.Next(**다음)를 클릭합니다**

.

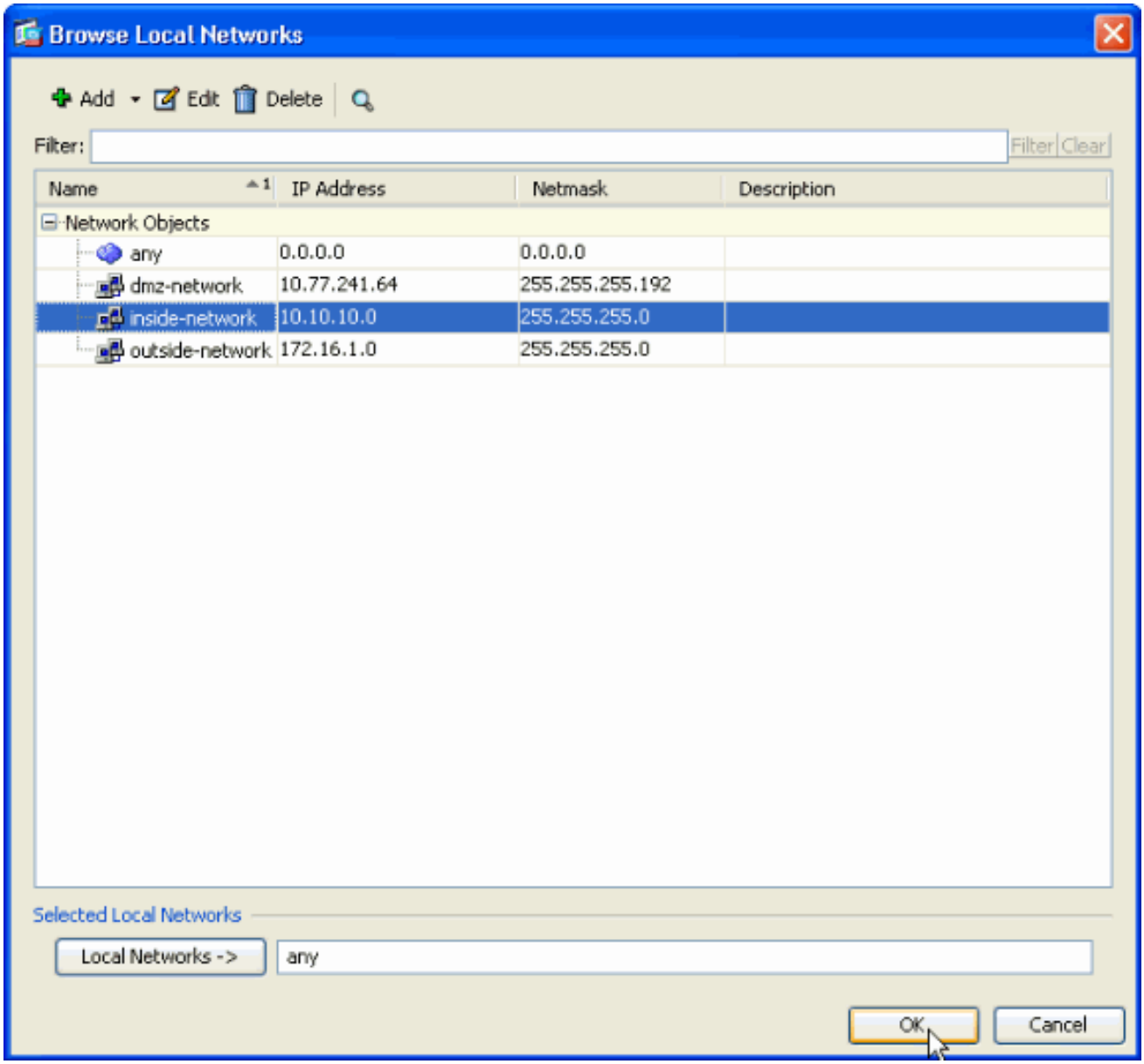


10. VPN 터널을 통과하도록 트래픽을 허용할 호스트를 지정합니다.이 단계에서는 VPN 터널에 **로컬** 및 **원격 네트워크**를 제공해야 합니다.드롭다운 목록에서 로컬 네트워크 주소를 선택하려면 여기 표시된 대로 **Local Networks(로컬 네트워크)** 옆에 있는 버튼을 클릭합니다
.



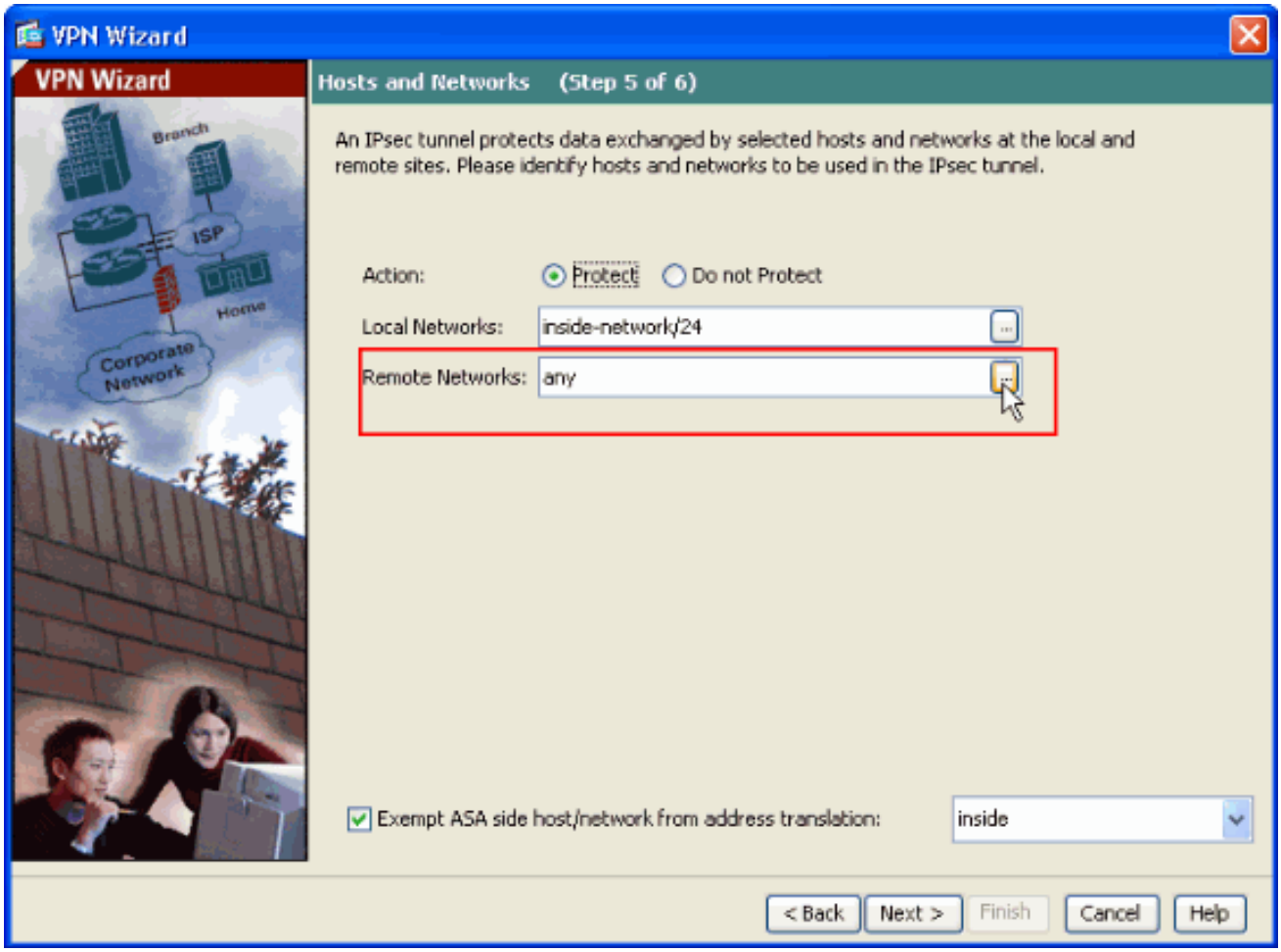
11. 로컬 **네트워크** 주소를 선택한 다음 **OK(확인)를** 클릭합니다

.



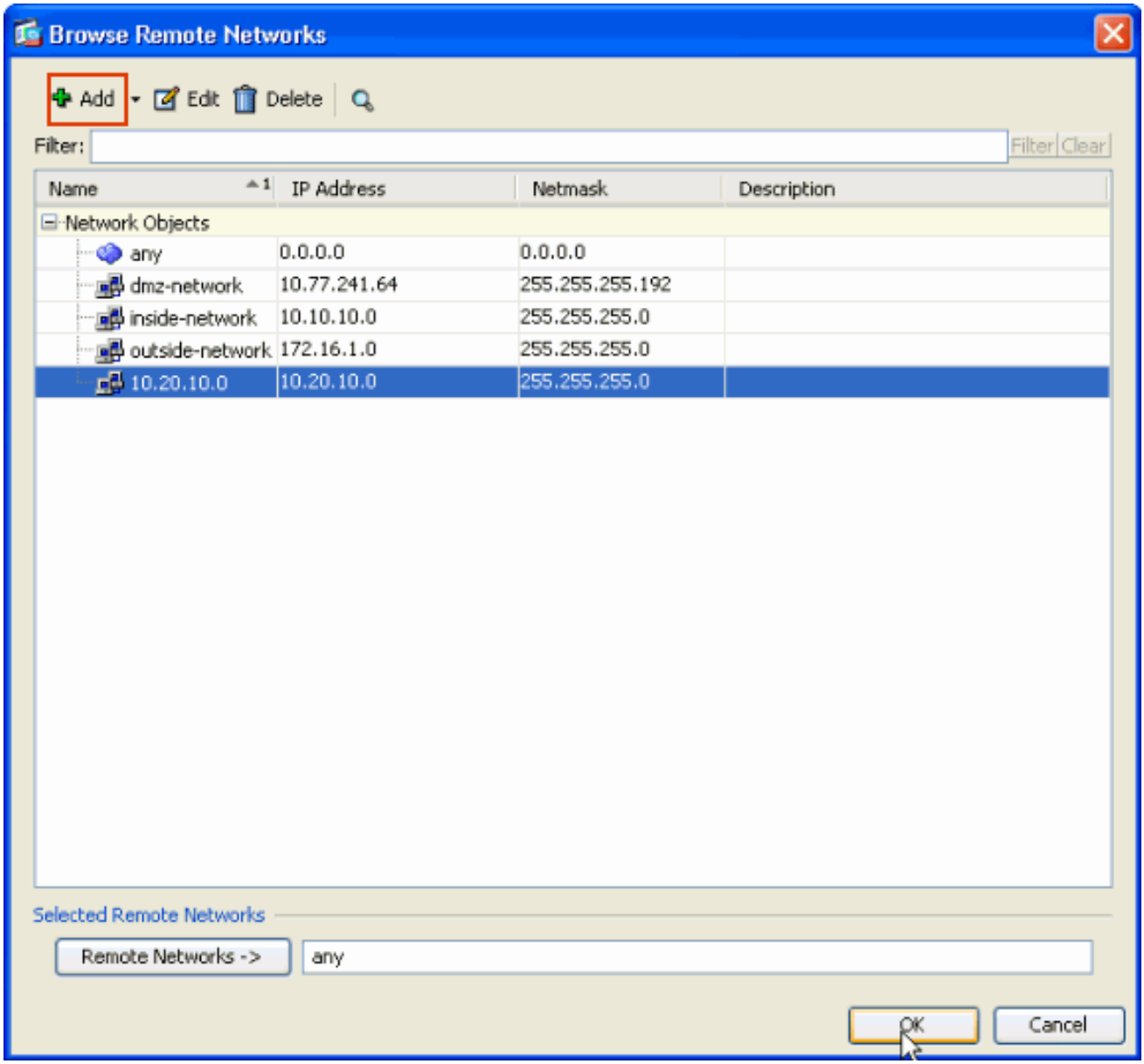
12. 드롭다운 목록에서 원격 네트워크 주소를 선택하려면 여기 표시된 **Remote Networks** 옆에 있는 버튼을 클릭합니다

.

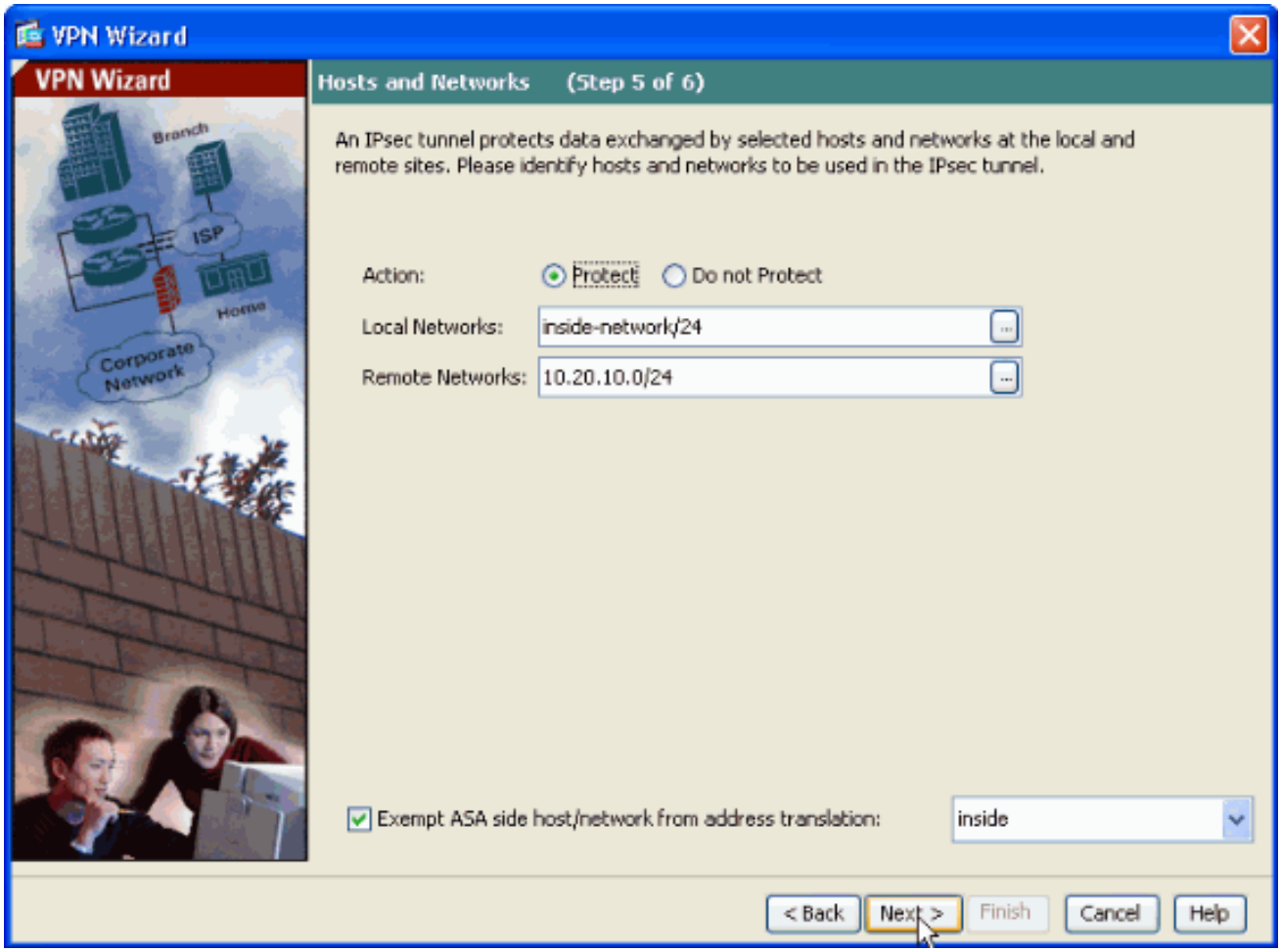


13. **원격 네트워크** 주소를 선택한 다음 여기**와** 같이 **확인**을 클릭합니다.**참고:** 목록에 Remote Network(원격 네트워크)가 없는 경우 Add(추가)를 클릭하여 네트워크를 목록에 추가해야 **합니다**

.

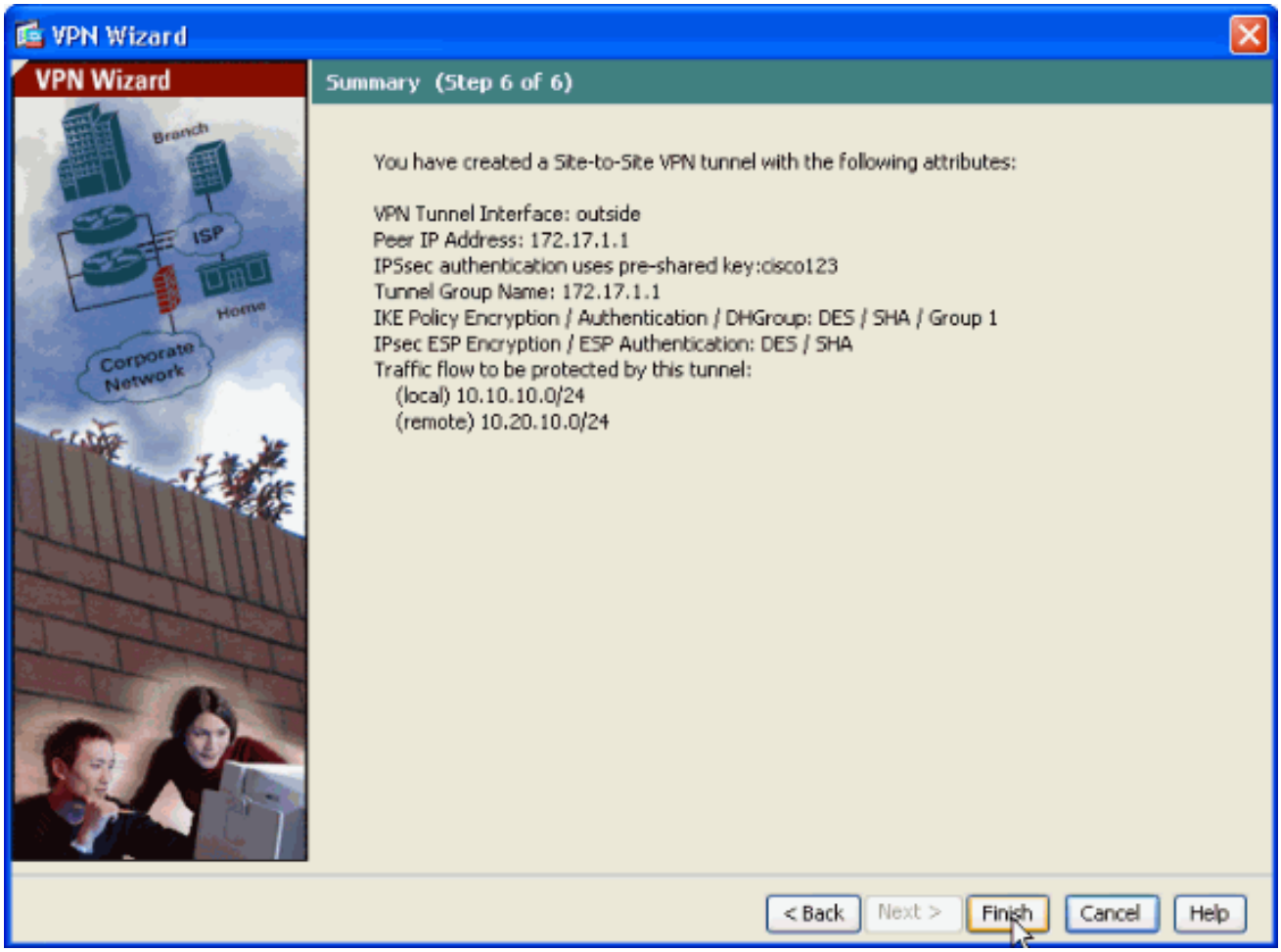


14. 터널 트래픽이 Network Address Translation(**네트워크 주소 변환)을** 통과하지 못하도록 하려면 Exempt ASA side host/network from address translation(**주소 변환에서 ASA 측 호스트/네트워크 제외**) 확인란을 **선택합니다**.그런 다음 **다음**을 클릭합니다
.



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

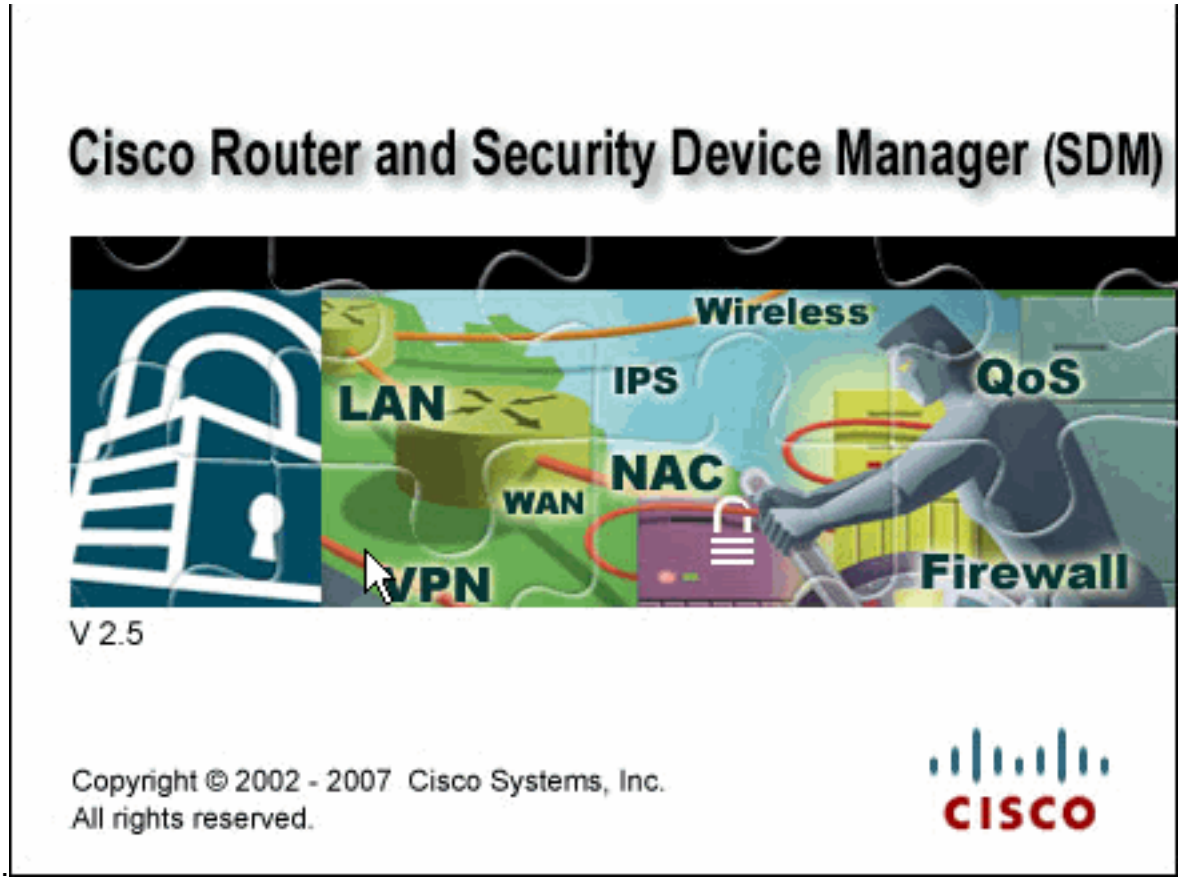
.



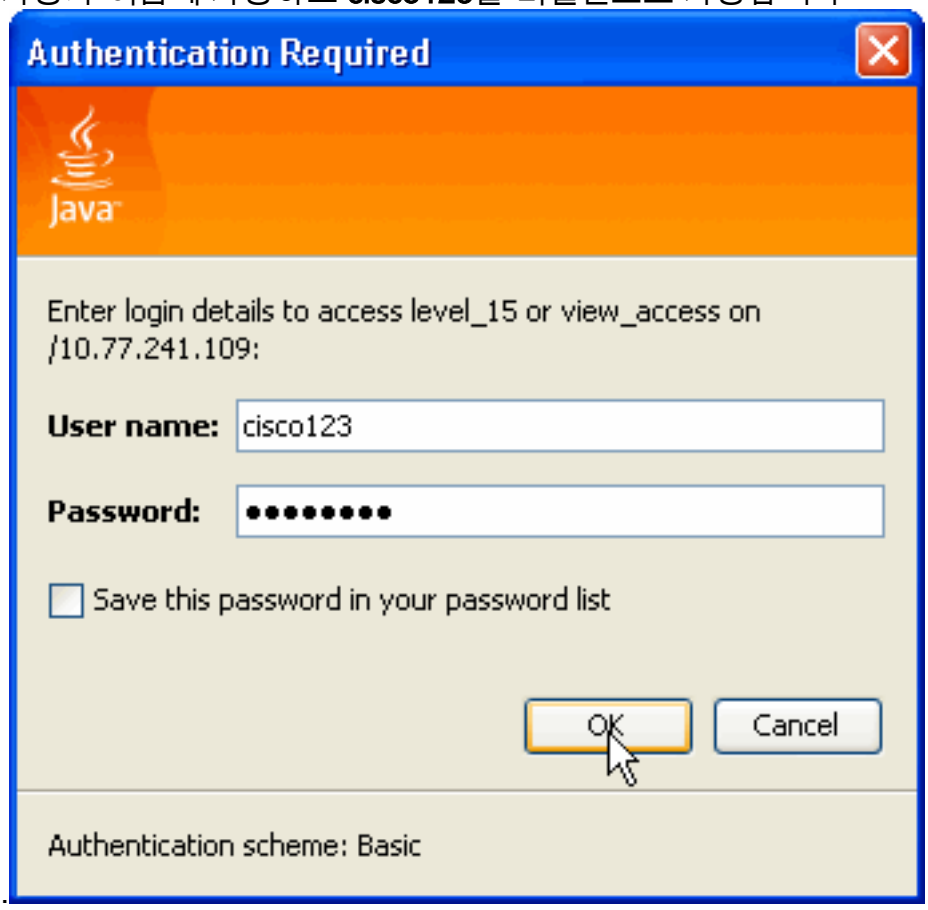
라우터 SDM 컨피그레이션

Cisco IOS 라우터에서 Site-to-Site VPN 터널을 구성하려면 다음 단계를 완료하십시오.

1. 브라우저를 열고 SDM **Access에 대해 구성된 라우터 인터페이스의 https://<IP_Address>를 입력하여** 라우터의 SDM에 액세스합니다.브라우저에서 SSL 인증서 신뢰성과 관련된 경고를 승인해야 합니다.기본 사용자 이름과 비밀번호는 모두 비어 있습니다.라우터는 SDM 응용 프로그램을 다운로드할 수 있도록 이 창을 표시합니다.이 예에서는 응용 프로그램을 로컬 컴퓨터에 로드하며 Java 애플릿에서 실행되지 않습니다



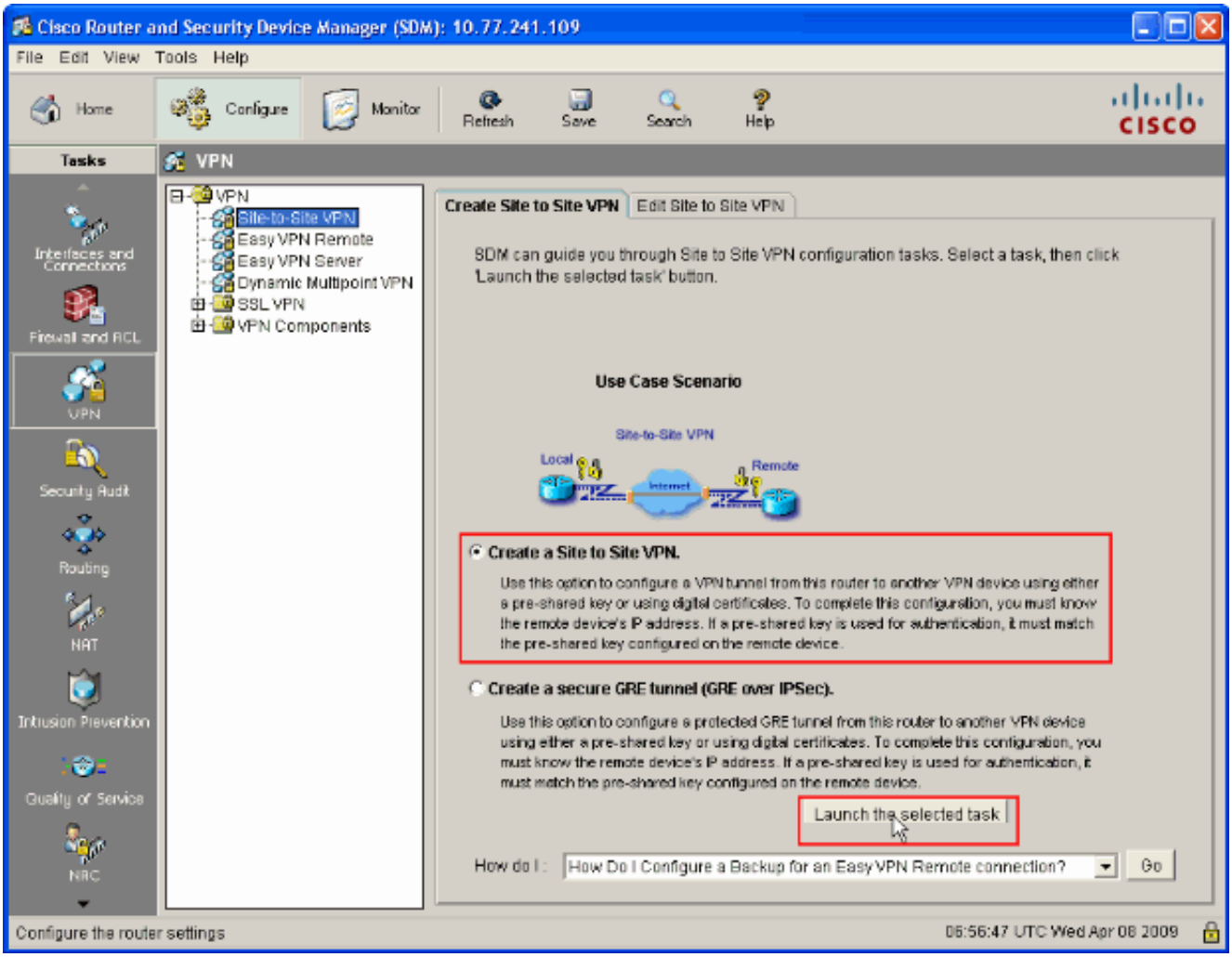
2. SDM 다운로드가 지금 시작됩니다.SDM Launcher가 다운로드되면, 소프트웨어를 설치하고 Cisco SDM Launcher를 실행하기 위해 프롬프트에 의해 지시된 단계를 완료합니다.
3. 사용자 **이름** 및 **비밀번호**를 지정한 경우 입력하고 **확인**을 클릭합니다.이 예에서는 **cisco123**을 사용자 이름에 사용하고 **cisco123**을 비밀번호로 사용합니다



4. Configuration(**컨피그레이션**)->**VPN**->**Site-to-Site VPN**을 선택하고 SDM 홈 페이지**에서 Create a Site-to-Site VPN(사이트 대 사이트 VPN 생성)** 옆의 라디오 버튼을 클릭합니다.그런

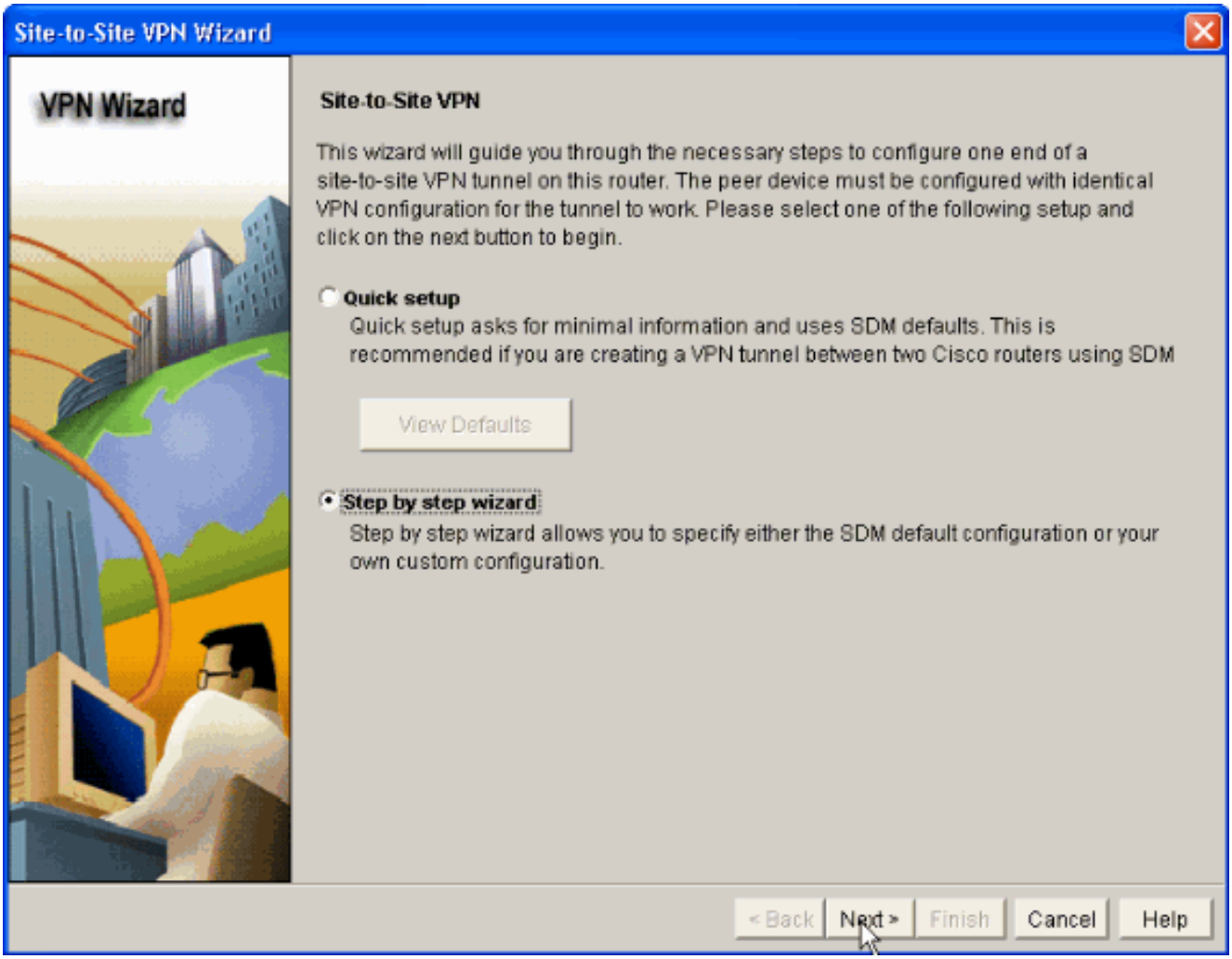
다음 여기와 같이 **선택한 작업 시작**을 클릭합니다

.

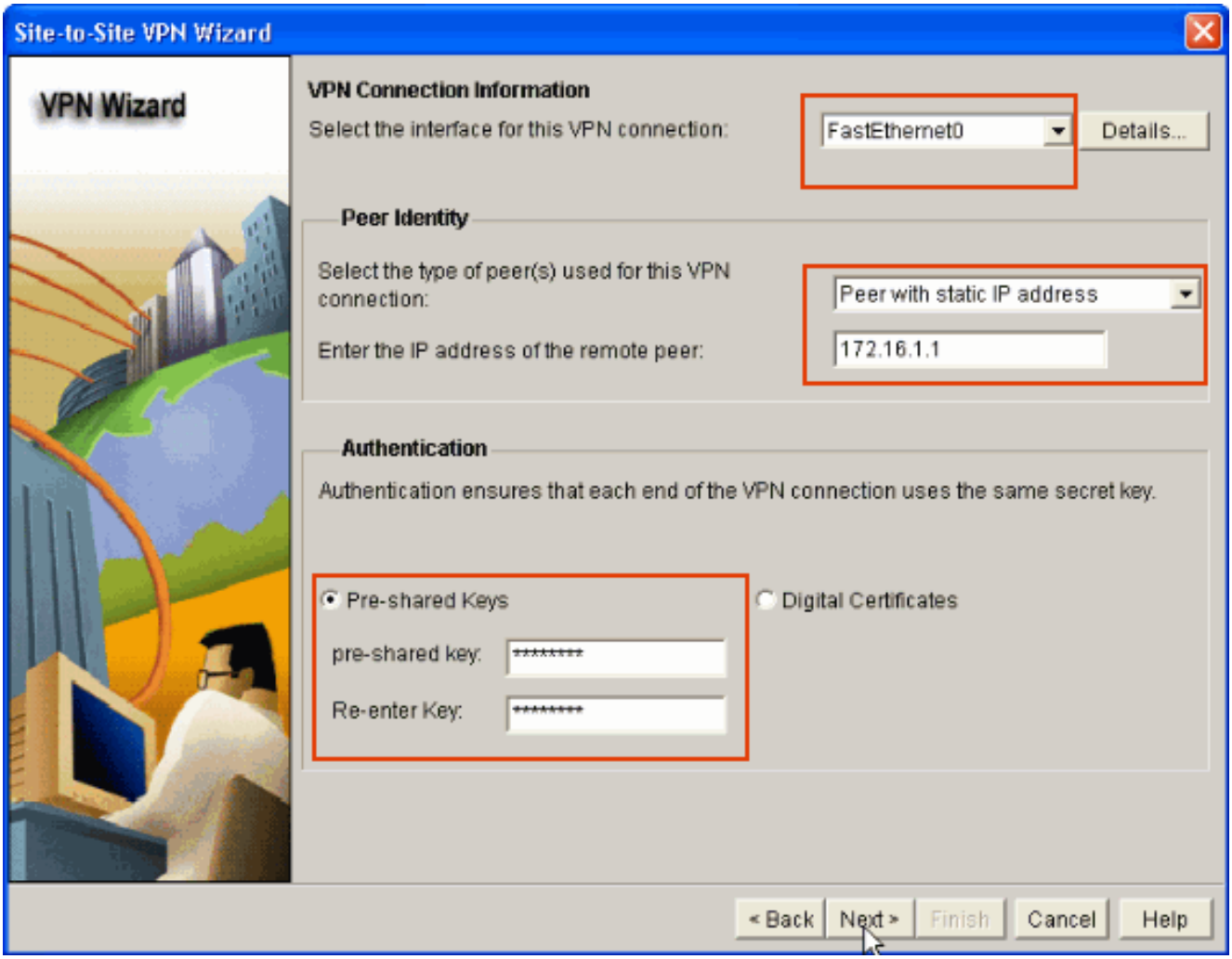


5. Step **by step wizard(단계별 마법사)**를 선택하여 컨피그레이션을 진행합니다

.

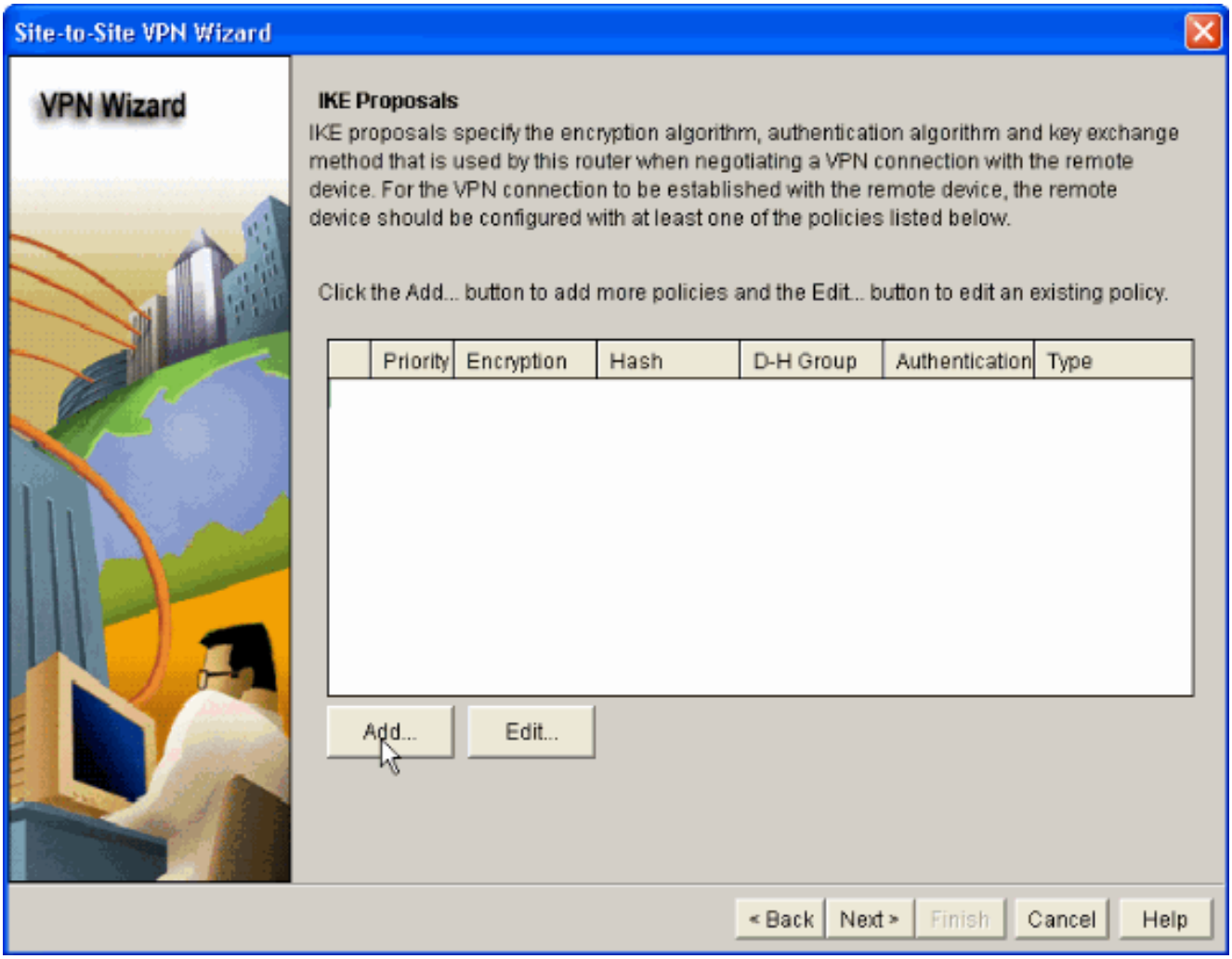


6. 다음 창에서 각 공간에 **VPN 연결 정보**를 제공합니다.드롭다운 목록에서 VPN 터널의 인터페이스를 선택합니다.여기서 **FastEthernet0**을 선택합니다.Peer **Identity** 섹션에서 **Peer with static IP address**를 선택하고 원격 피어 IP 주소를 제공합니다.그런 다음 Authentication 섹션에서 **사전 공유 키**(이 예제의 **cisco123**)를 제공합니다.그런 다음 **다음**을 클릭합니다
.

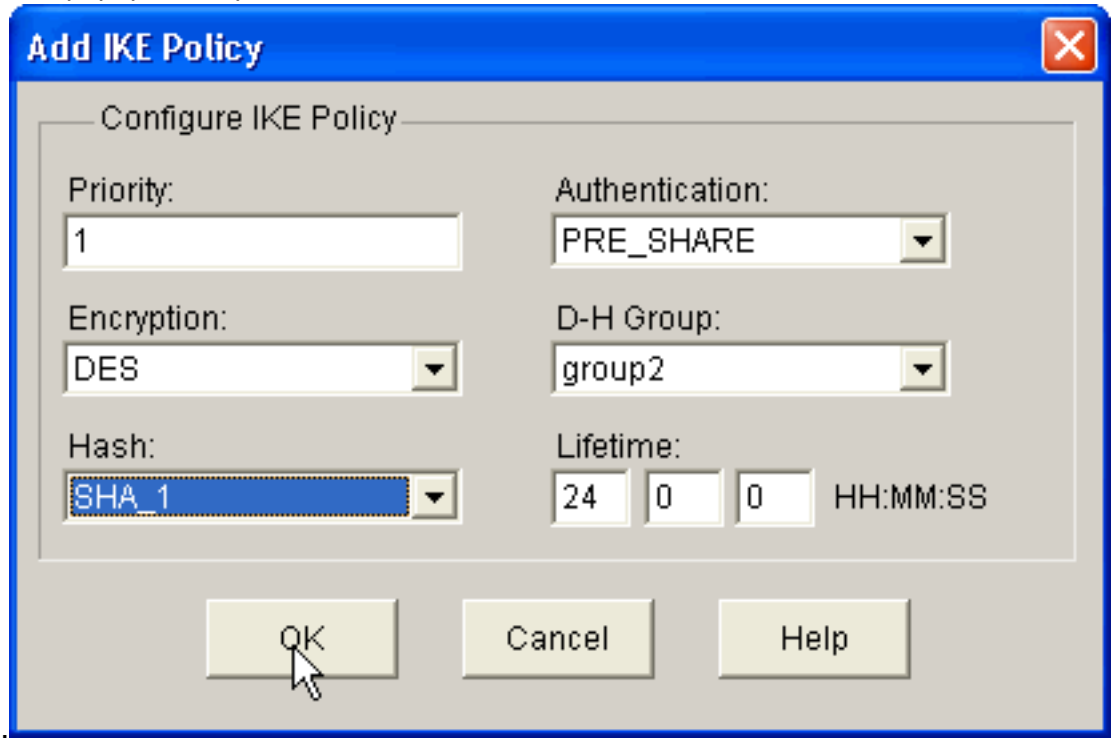


7. Add(**추가**)를 클릭하여 **암호화 알고리즘, 인증 알고리즘** 및 **키 교환 방법**을 지정하는 IKE 제안서를 **추가합니다**

.



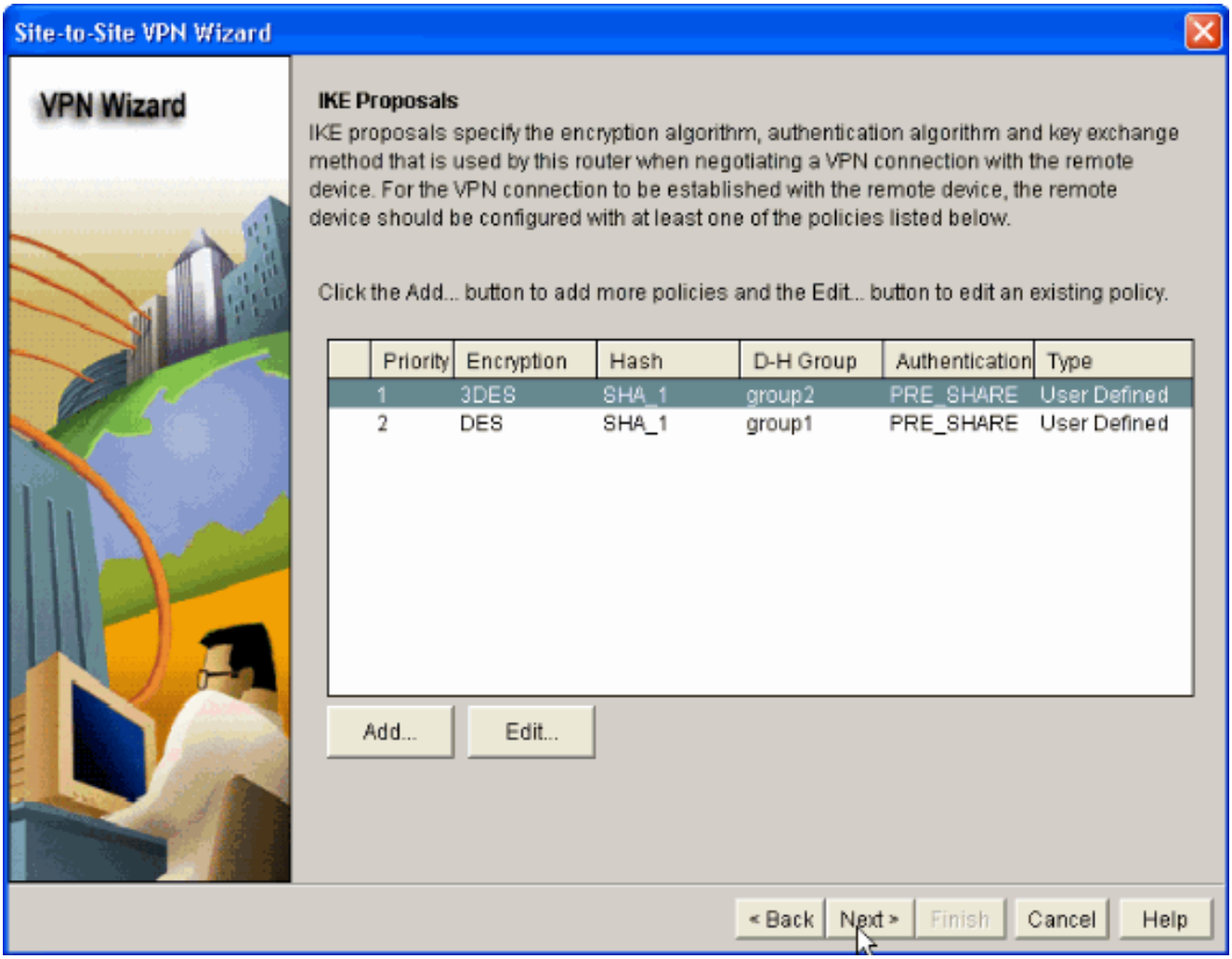
8. **암호화 알고리즘**, **인증 알고리즘** 및 **키 교환 방법**을 여기와 같이 제공한 다음 **확인 을 클릭합니다**.Encryption **Algorithm**, **Authentication Algorithm** 및 **Key Exchange 메서드** 값은 ASA에 제공된 데이터와 일치해야 합니다



.

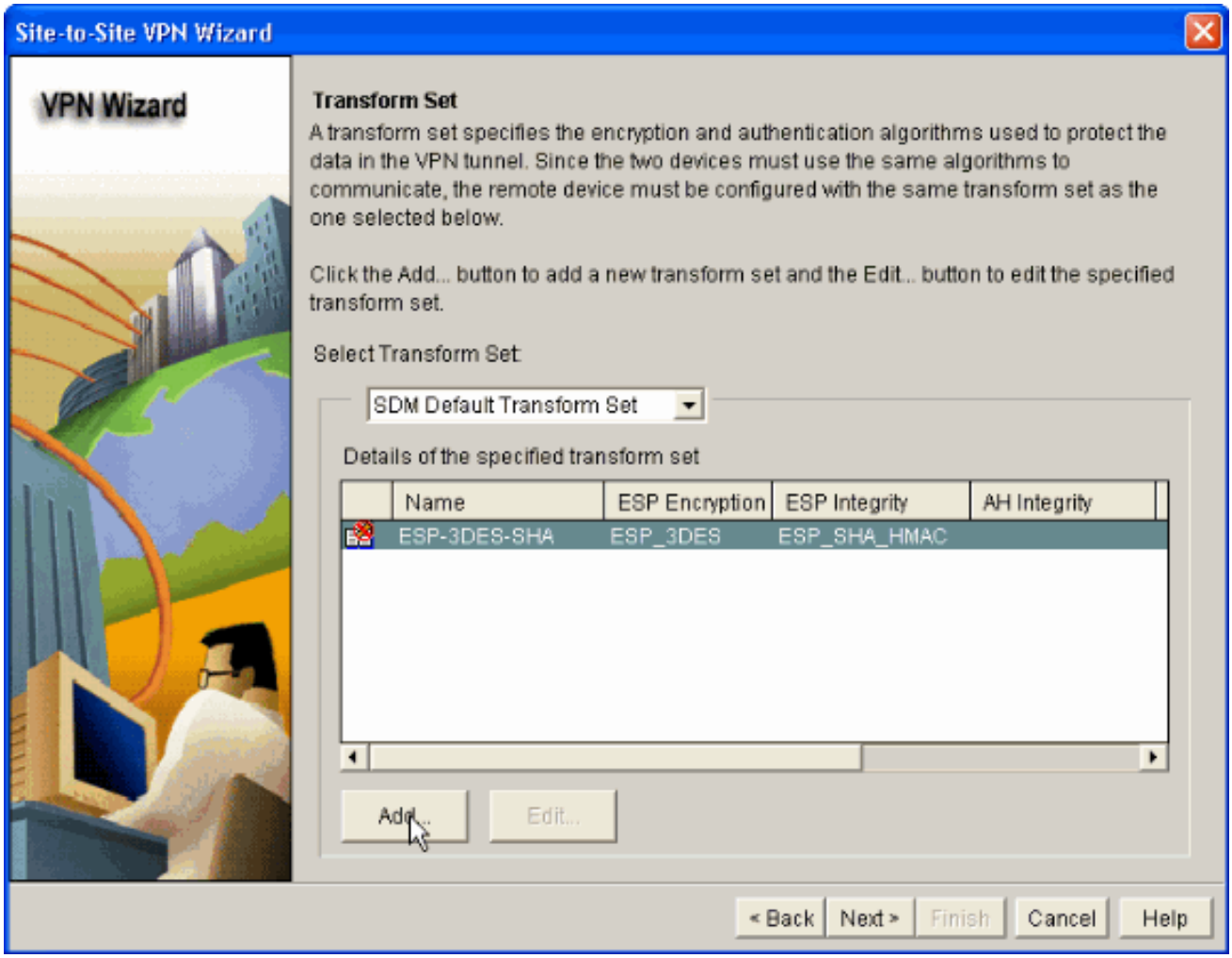
9. 여기와 같이 Next를 클릭합니다

.

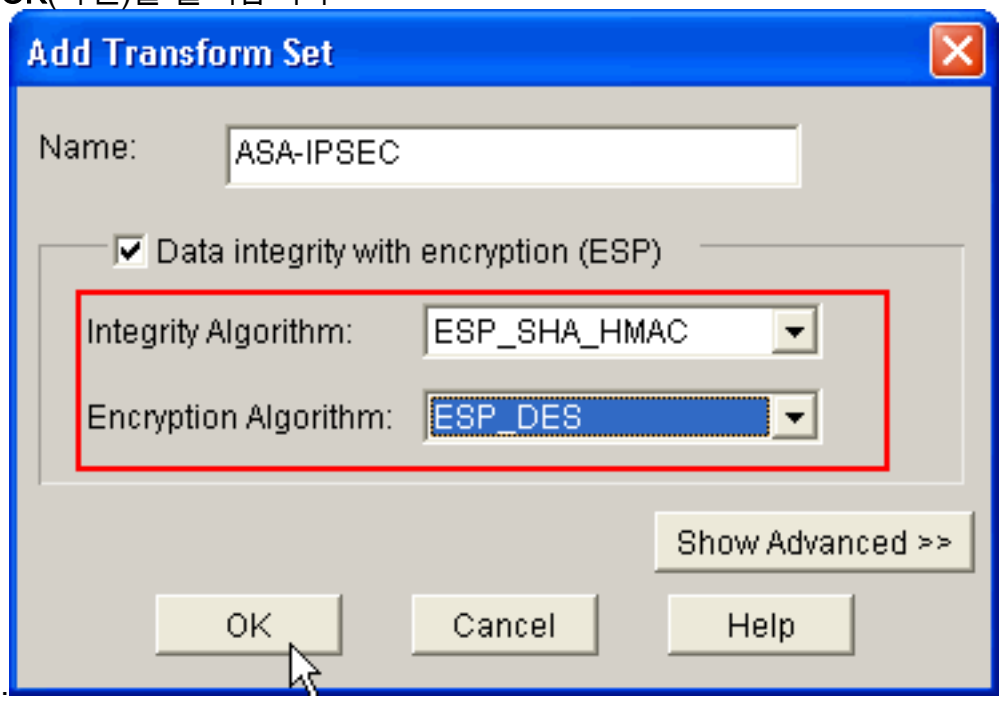


10. 이 새 창에서 **변형 집합** 세부사항을 제공해야 합니다.Transform Set는 **VPN 터널**에서 **데이터를** 보호하는 데 사용되는 **암호화** 및 **인증 알고리즘을 지정합니다**.그런 다음 **Add(추가)를** 클릭하여 이러한 세부 정보를 제공합니다.필요에 따라 Add(추가)를 클릭하고 **세부** 정보를 제공하여 원하는 수의 변형 집합을 추가할 수 있습니다

.



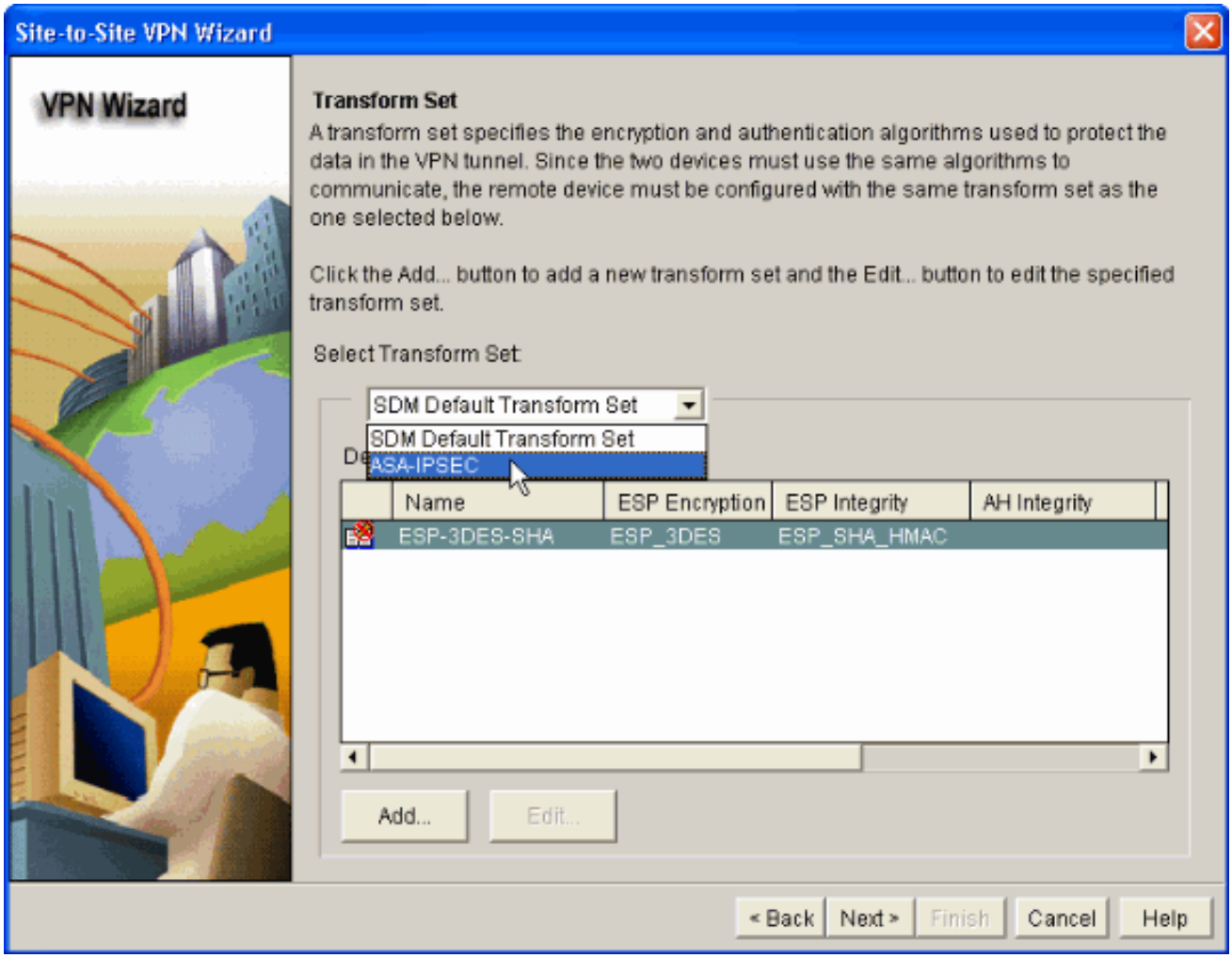
11. Transform **Set** 세부 정보(**Encryption and Authentication Algorithm**)를 제공하고 표시된 대로 **OK**(확인)를 클릭합니다



.

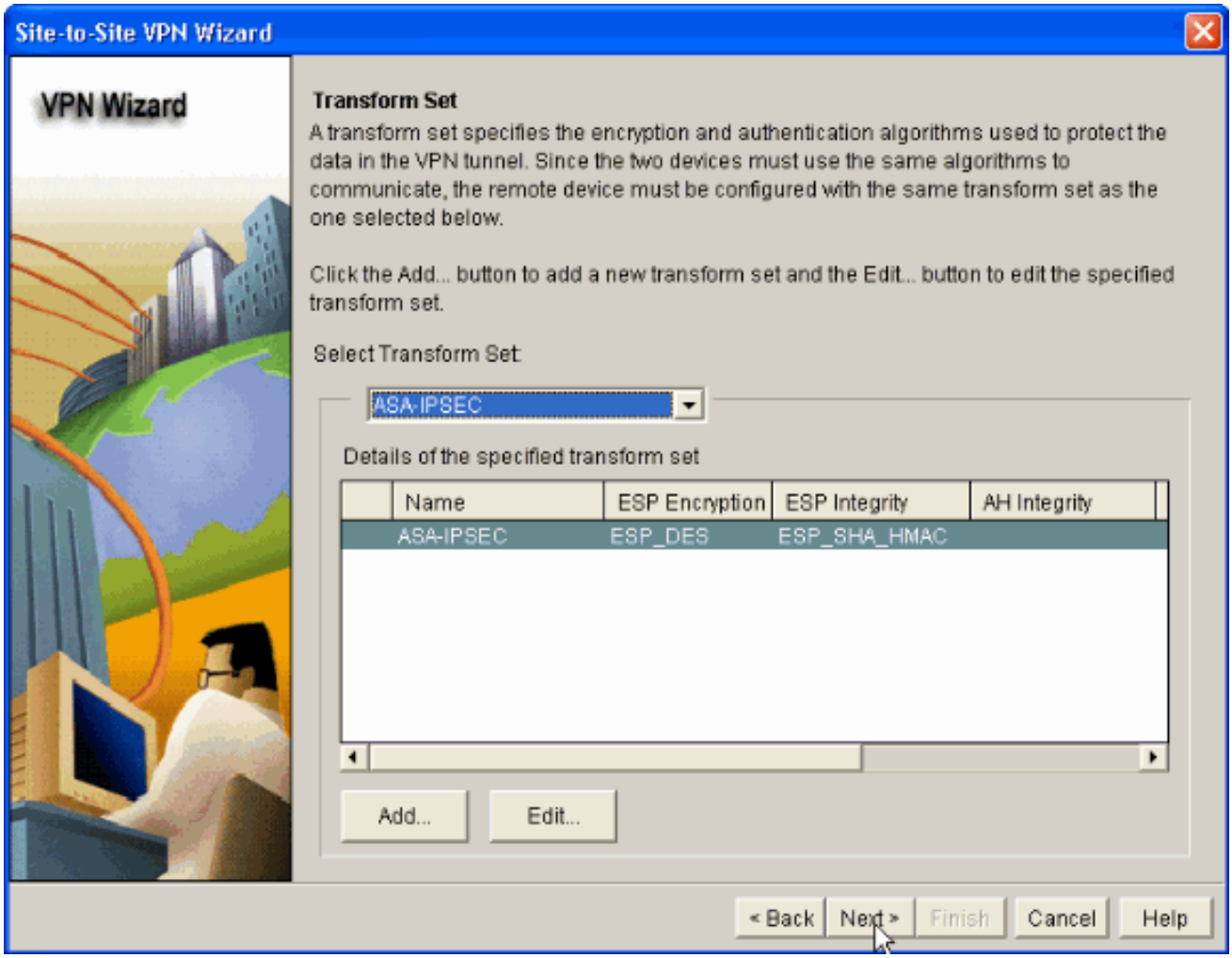
12. 드롭다운 목록에서 사용할 **변형 집합**을 선택합니다

.

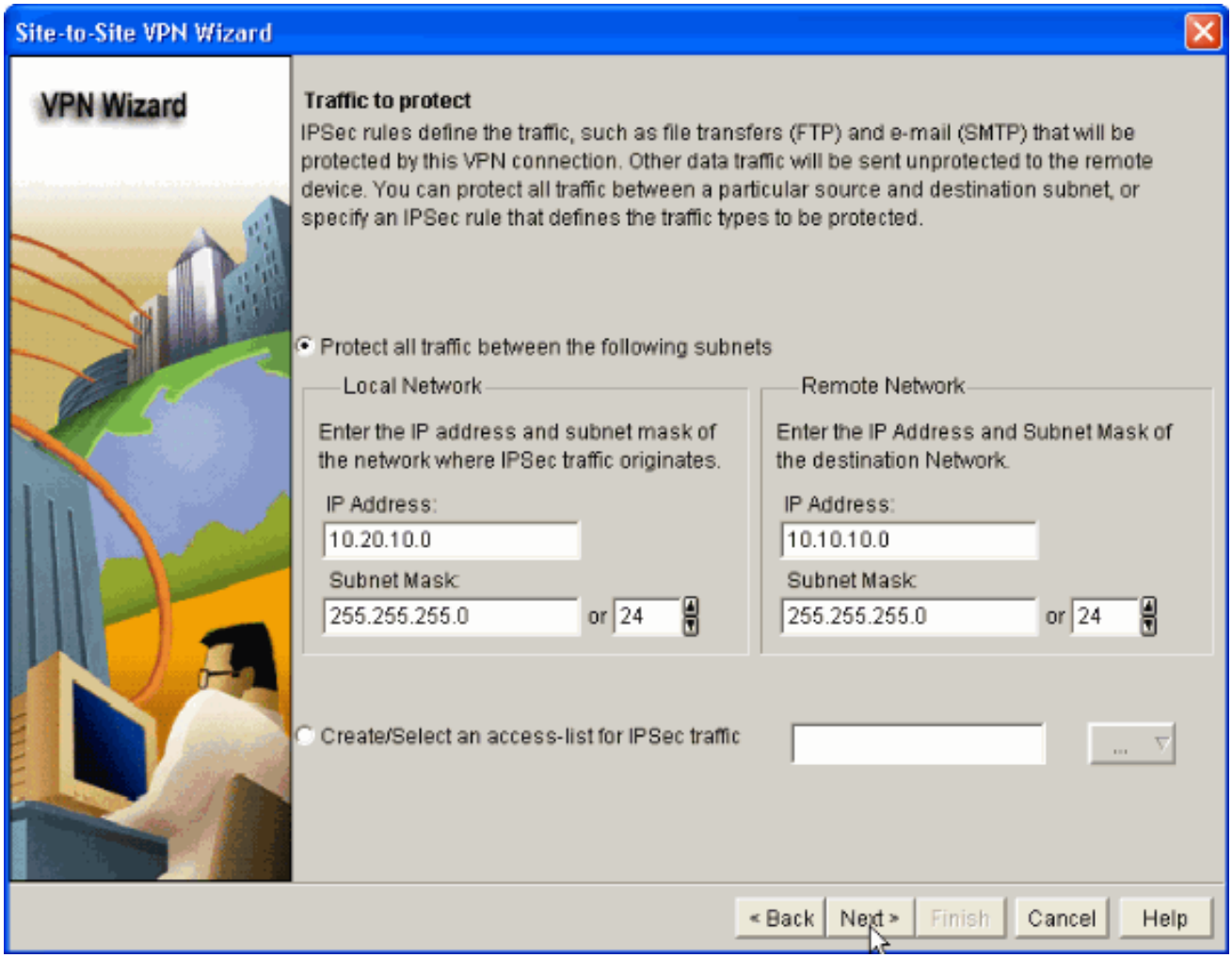


13. Next(다음)를 클릭합니다

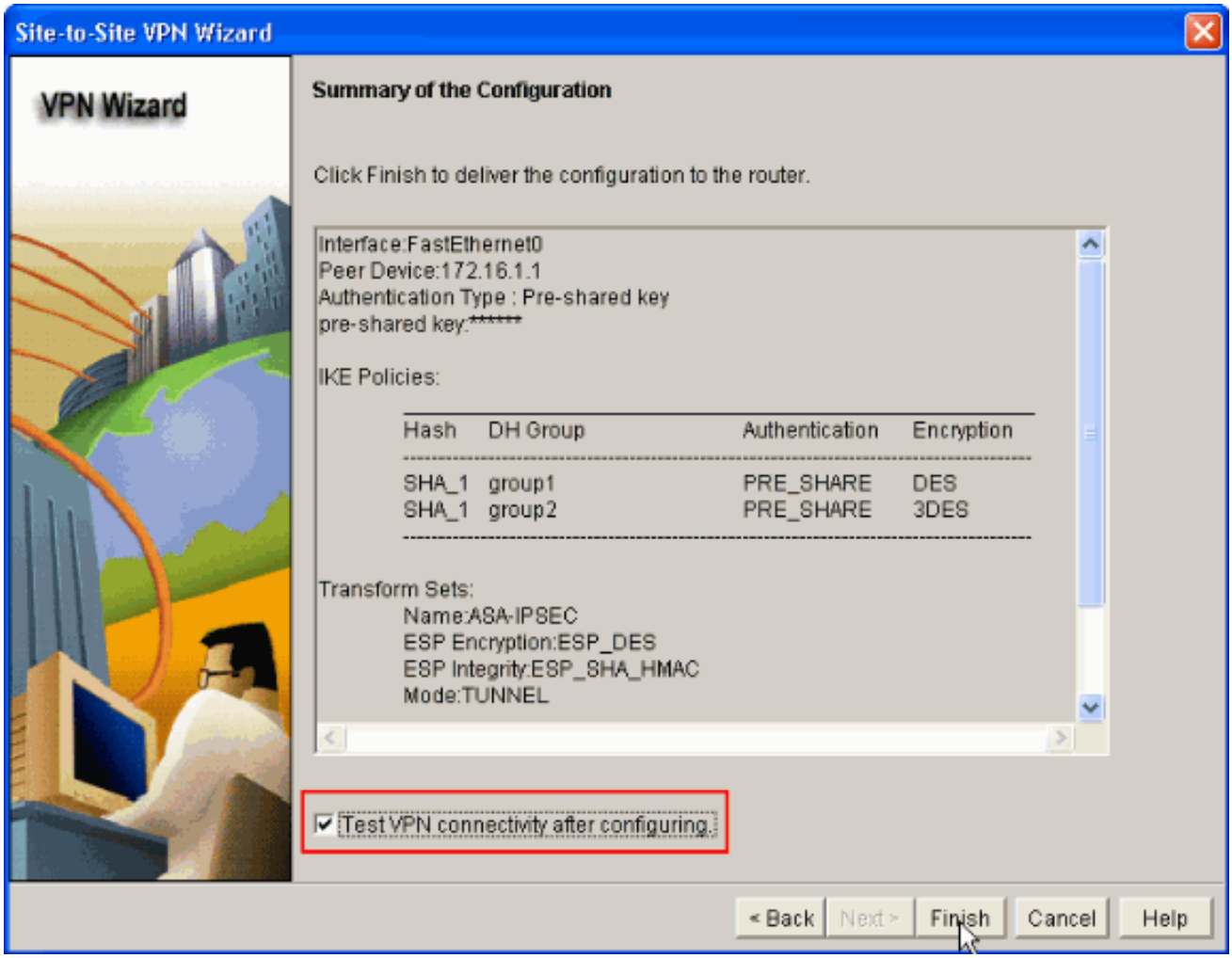
.



14. 다음 창에서 VPN 터널을 통해 **보호할 트래픽**에 대한 세부 정보를 제공합니다.지정된 소스 **및** 대상 네트워크 간의 트래픽이 보호되도록 보호할 트래픽의 소스 및 대상 네트워크를 제공하십시오.이 예에서 소스 네트워크는 10.20.10.0이고 대상 네트워크는 10.10.10.0입니다. 그런 다음 **다음**을 클릭합니다
.

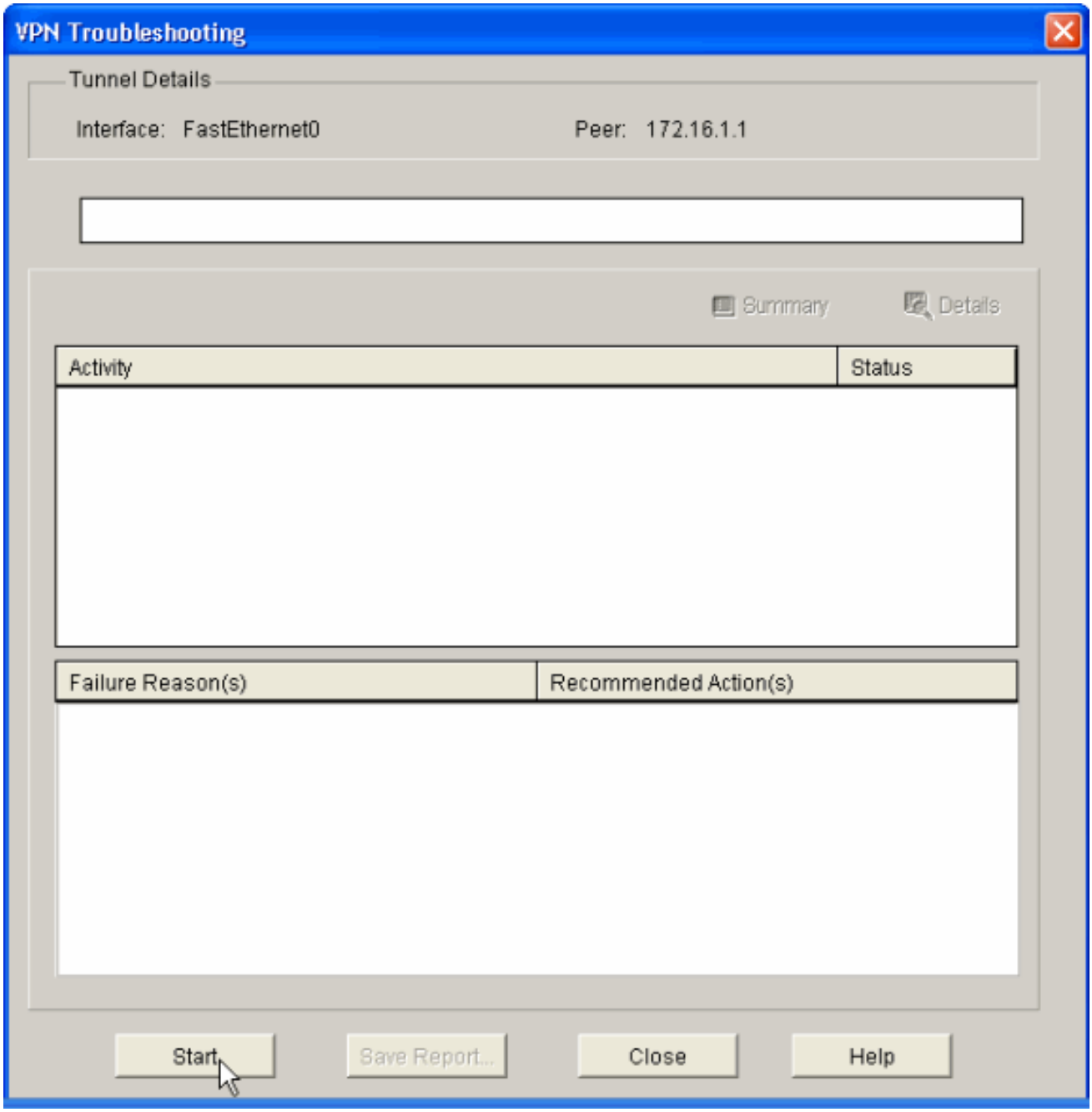


15. 이 창에는 완료된 Site-to-Site VPN 컨피그레이션의 요약이 표시됩니다.VPN 연결을 테스트하려면 **Test VPN Connectivity after configuring(구성 후 VPN 연결** 테스트) 확인란을 선택합니다.여기서는 연결을 선택해야 하므로 확인란이 선택됩니다.그런 다음 **마침**을 클릭합니다.



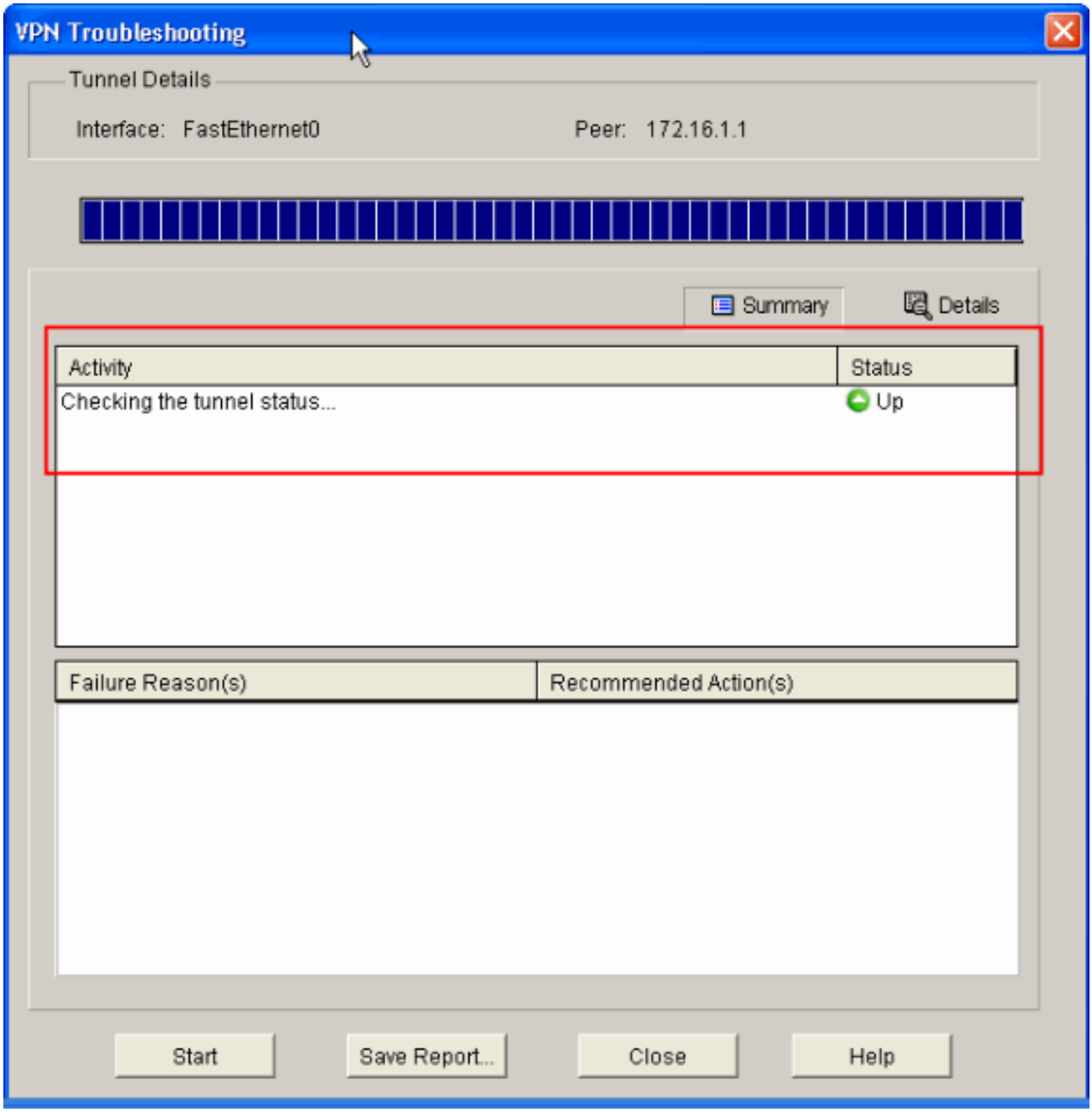
16. 표시된 대로 **시작**을 클릭하여 VPN 연결을 확인합니다

.



17. 다음 창에서 **VPN 연결 테스트** 결과가 제공됩니다.여기서 터널이 **Up** 또는 **Down**인지 확인할 수 있습니다.이 컨피그레이션에서는 녹색과 같이 터널이 작동 중입니다

.



이렇게 하면 Cisco IOS 라우터에서 컨피그레이션이 완료됩니다.

ASA CLI 컨피그레이션

ASA

```
ASA#show run
: Saved
ASA Version 8.0(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configure the outside interface. ! interface
Ethernet0/1 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 !--- Configure the inside
interface. ! interface Ethernet0/2 nameif inside
security-level 100 ip address 10.10.10.1 255.255.255.0
!-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU
```

```
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid access-list 100
extended permit ip any any access-list
inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0
10.20.10.0 255.255.255.0
!--- 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_1_cryptomap). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_1_cryptomap extended permit ip
10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
!--- This access list (outside_cryptomap) 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 disk0:/asdm-613.bin
asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 10.10.10.0 255.255.255.0

nat (inside) 0 access-list inside_nat0_outbound
!--- NAT 0 prevents NAT for networks specified in !---
the ACL inside_nat0_outbound.


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
http 0.0.0.0 0.0.0.0 dmz
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-DES-SHA esp-des esp-sha-hmac
!--- Define the transform set for Phase 2. crypto map
outside_map 1 match address outside_1_cryptomap
!--- Define which traffic should be sent to the IPsec
peer. crypto map outside_map 1 set peer 172.17.1.1
!--- Sets the IPsec peer crypto map outside_map 1 set
```

```
transform-set ESP-DES-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. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. crypto
isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 1
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!



tunnel-group 172.17.1.1 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 command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 172.17.1.1 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 threat-detection basic-threat
threat-detection statistics access-list ! class-map
inspection_default match default-inspection-traffic ! !
!-- Output suppressed! username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

라우터 CLI 컨피그레이션

라우터

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
```

```
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
crypto isakmp policy 2
 authentication pre-share

!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
!
!
!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ASA-IPSEC
esp-des esp-sha-hmac
!

!--- !--- Indicates that IKE is used to establish !---
the IPsec Security Association for protecting the !---
traffic specified by this crypto map entry. crypto map
SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1

!--- !--- Sets the IP address of the remote end. set
peer 172.16.1.1

!--- !--- Configures IPsec to use the transform-set !---
"ASA-IPSEC" defined earlier in this configuration. set
transform-set ASA-IPSEC

!--- !--- Specifies the interesting traffic to be
encrypted. match address 100
!
!
!
!--- Configures the interface to use the !--- crypto map
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface
FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
!
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
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.

- PIX Security Appliance - **show** 명령
- 원격 IOS 라우터 - **show** 명령

ASA/PIX Security Appliance - show 명령

- **show crypto isakmp sa** - 피어의 현재 IKE SA를 모두 표시합니다.

```
ASA#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: 172.17.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

- **show crypto ipsec sa** - 피어에 있는 모든 현재 IPsec SA를 표시합니다.

```
ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

     #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 434C4A7F

    inbound esp sas:
      spi: 0xB7C1948E (3082917006)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x434C4A7F (1129073279)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
```

원격 IOS 라우터 - show 명령

- **show crypto isakmp sa** - 피어의 현재 IKE SA를 모두 표시합니다.

```
Router#show crypto isakmp sa

dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1      QM_IDLE              3    0 ACTIVE
```

- **show crypto ipsec sa** - 피어에 있는 모든 현재 IPsec SA를 표시합니다.

```
Router#show crypto ipsec sa
interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto engine connections active(암호화 엔진 연결 활성** 표시) - 현재 연결 및 암호화 및 암호 해독된 패킷에 대한 정보를 표시합니다(라우터에만 해당).

```
Router#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   3 FastEthernet0        172.17.1.1      set    HMAC_SHA+DES_56_CB        0        0
2001 FastEthernet0        172.17.1.1      set    DES+SHA                   0       59
2002 FastEthernet0        172.17.1.1      set    DES+SHA                  59        0
```

문제 해결

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

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

참고: debug **명령**을 사용하기 전에 Debug 명령 및 IP 보안 문제 해결 - Understanding and Using debug Commands(디버그 명령 이해 및 사용)에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec 7** - 2단계의 IPsec 협상을 표시합니다.**debug crypto isakmp 7** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.**debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.

사이트 사이트 VPN 문제 해결에 대한 자세한 내용은 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션을 참조하십시오.

관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliance
- Configuration Professional:ASA/PIX와 IOS 라우터 컨피그레이션 간의 사이트 대 사이트 IPsec VPN 예
- Cisco Secure PIX Firewall 명령 참조
- Cisco 라우터 및 보안 장치 관리자
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems