# 스틱 컨피그레이션의 공용 인터넷 VPN용 PIX/ASA 및 VPN 클라이언트 예

## 목차



## 소개

이 문서에서는 ASA Security Appliance 7.2 이상을 설정하여 스틱에서 IPsec을 수행하는 방법에 대해 설명합니다.이 설정은 ASA에서 스플릿 터널링을 허용하지 않고 사용자가 인터넷으로 이동하기 전에 ASA에 직접 연결하는 특정 경우에 적용됩니다.

**참고:** PIX/ASA 버전 7.2 이상에서 intra-interface 키워드는 IPsec 트래픽뿐만 아니라 모든 트래픽이 동일한 인터페이스로 들어오고 나갈 수 있도록 합니다.

중앙 사이트 라우터에서 유사한 컨피그레이션을 완료하려면 Stick 컨피그레이션 예에서 Router 및 VPN Client for Public Internet을 참조하십시오.

허브 PIX가 VPN 클라이언트에서 스포크 PIX로 트래픽을 리디렉션하는 시나리오에 대한 자세한 내용은 PIX/ASA 7.x Enhanced Spoke-to-Client VPN with TACACS+ Authentication Configuration 예를 참조하십시오.

**참고:** 네트워크에서 IP 주소가 중복되지 않도록 하려면 완전히 다른 IP 주소 풀을 VPN 클라이언트(예: 10.x.x.x, 172.16.x.x 및 192.168.x.x)에 할당합니다. 이 IP 주소 지정 체계는 네트워크 문제를 해결하는 데 유용합니다.

# 사전 요구 사항

## 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 허브 PIX/ASA Security Appliance는 버전 7.2 이상을 실행해야 합니다.
- Cisco VPN Client 버전 5.x

## 사용되는 구성 요소

이 문서의 정보는 PIX 또는 ASA 보안 어플라이언스 버전 8.0.2 및 Cisco VPN Client 버전 5.0을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 관련 제품

이 컨피그레이션은 Cisco PIX Security Appliance 버전 7.2 이상에서도 사용할 수 있습니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

# 배경 정보

## 헤어핀 또는 U-턴

이 기능은 인터페이스로 들어가지만 동일한 인터페이스에서 라우팅되는 VPN 트래픽에 유용합니다.예를 들어 보안 어플라이언스가 허브이고 원격 VPN 네트워크가 스포크인 허브-스포크 VPN 네트워크가 있는 경우 한 스포크가 다른 스포크와 통신하기 위해서는 트래픽이 보안 어플라이언스로 이동한 다음 다른 스포크로 다시 나가야 합니다.

트래픽이 동일한 인터페이스로 들어오고 나가도록 허용하려면 same-**security-traffic** 명령을 사용합니다.

```
securityappliance(config)#same-security-traffic permit intra-interface
```

**참고:** 헤어피닝 또는 U-turn은 VPN 클라이언트에서 VPN 클라이언트 간 통신에도 적용됩니다.

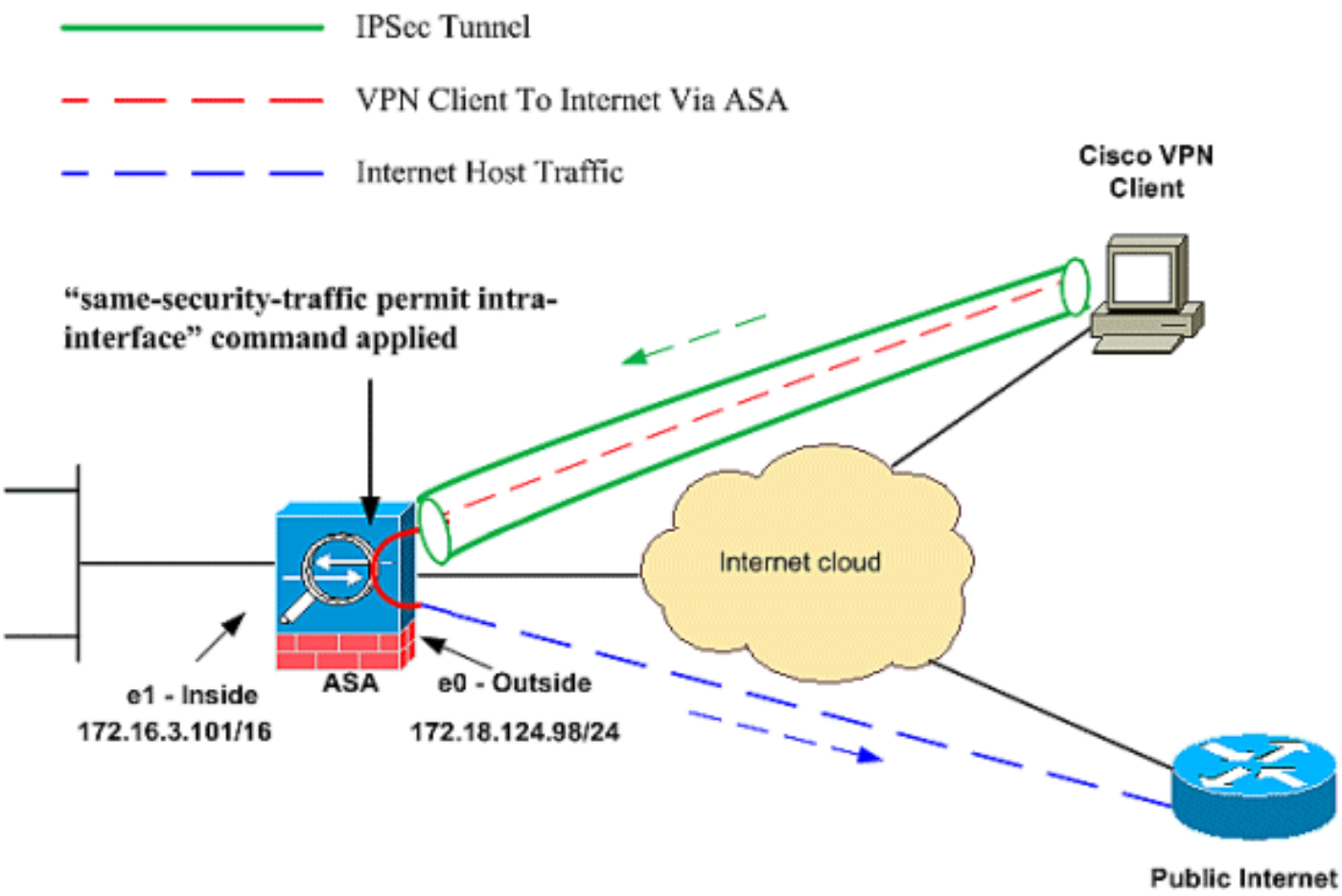
# 구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

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

## 네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.




## PIX/ASA의 CLI 컨피그레이션

- PIX/ASA

**PIX/ASA에서 컨피그레이션 실행**

```
PIX Version 8.0(2)
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
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 pixfirewall
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface
access-list 100 extended permit icmp any any echo-reply
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500

ip local pool vpnpool
   192.168.10.1-192.168.10.254 mask 255.255.255.0

no failover
monitor-interface outside
monitor-interface inside
icmp permit any outside
no asdm history enable
arp timeout 14400
nat-control!--- The address pool for the VPN Clients. !-
-- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP.

global (outside) 1 172.18.124.166

!--- The NAT statement to define what to encrypt (the
addresses from the vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 172.16.3.102 172.16.3.102
   netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.124.98 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

!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal
group-policy clientgroup attributes
vpn-idle-timeout 20

!--- Forces VPN Clients over the tunnel for Internet
access. split-tunnel-policy tunnelall


no snmp-server location
no snmp-server contact
snmp-server enable traps snmp

!--- Configuration of IPsec Phase 2. crypto ipsec
transform-set myset esp-3des esp-sha-hmac

!--- Crypto map configuration for VPN Clients that
connect to this PIX. crypto dynamic-map rtpdynmap 20 set
transform-set myset

!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap

!--- Crypto map applied to the outside interface. crypto
map mymap interface outside

!--- Enable ISAKMP on the outside interface. isakmp
identity address
isakmp enable outside

!--- Configuration of ISAKMP policy. isakmp policy 10
authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
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
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Configuration of tunnel-group with group
information for VPN Clients. tunnel-group rtptacvpn type
ipsec-ra

!--- Configuration of group parameters for the VPN
Clients. tunnel-group rtptacvpn general-attributes
address-pool vpnpool

!--- Disable user authentication. authentication-server-
group none


!--- Bind group-policy parameters to the tunnel-group
for VPN Clients. default-group-policy clientgroup
```

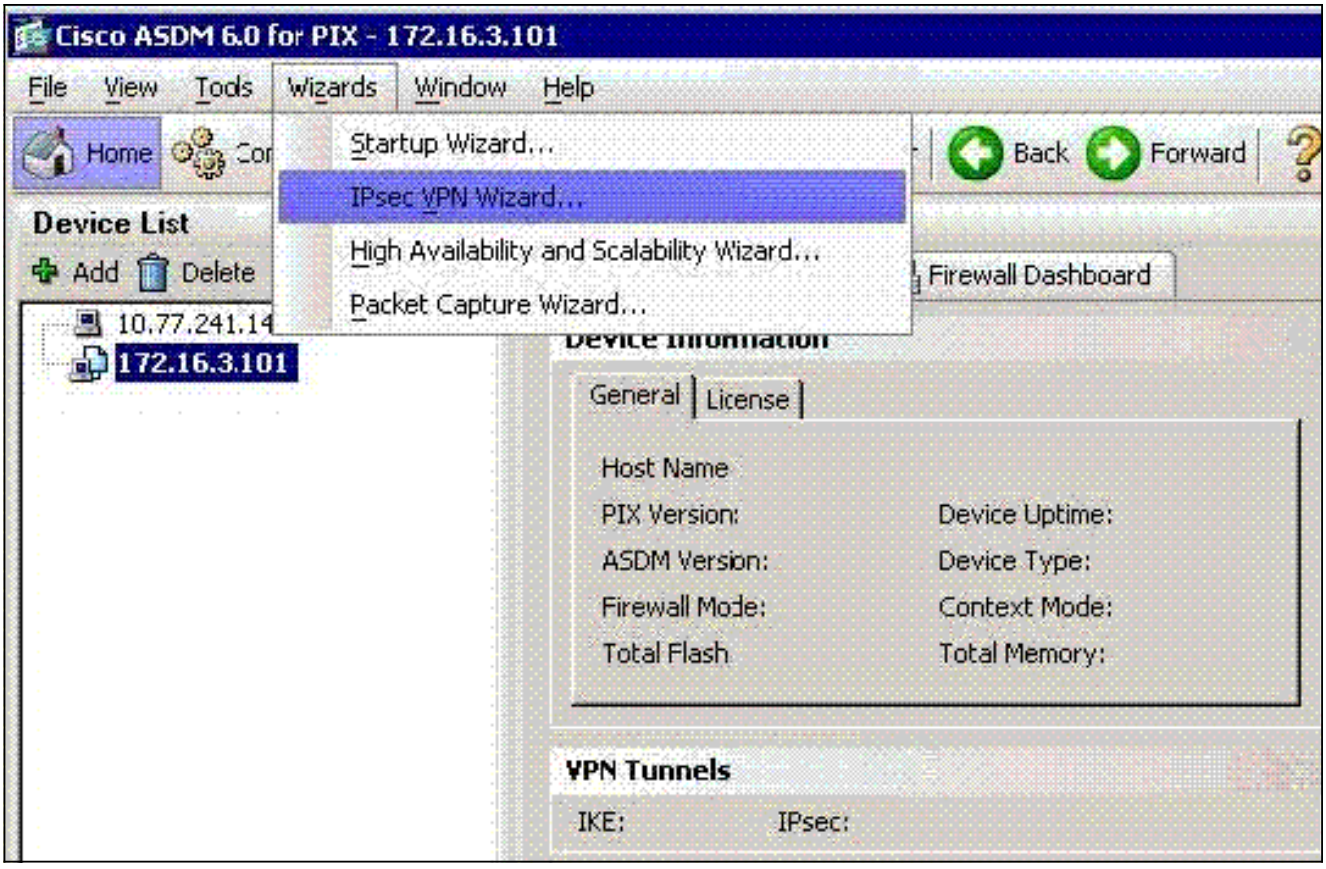
```
tunnel-group rtptacvpn ipsec-attributes
pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
 inspect dns maximum-length 512
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0
: end
```

## ASDM을 사용하여 ASA/PIX 구성

ASDM을 사용하여 Cisco ASA를 원격 VPN 서버로 구성하려면 다음 단계를 완료합니다.

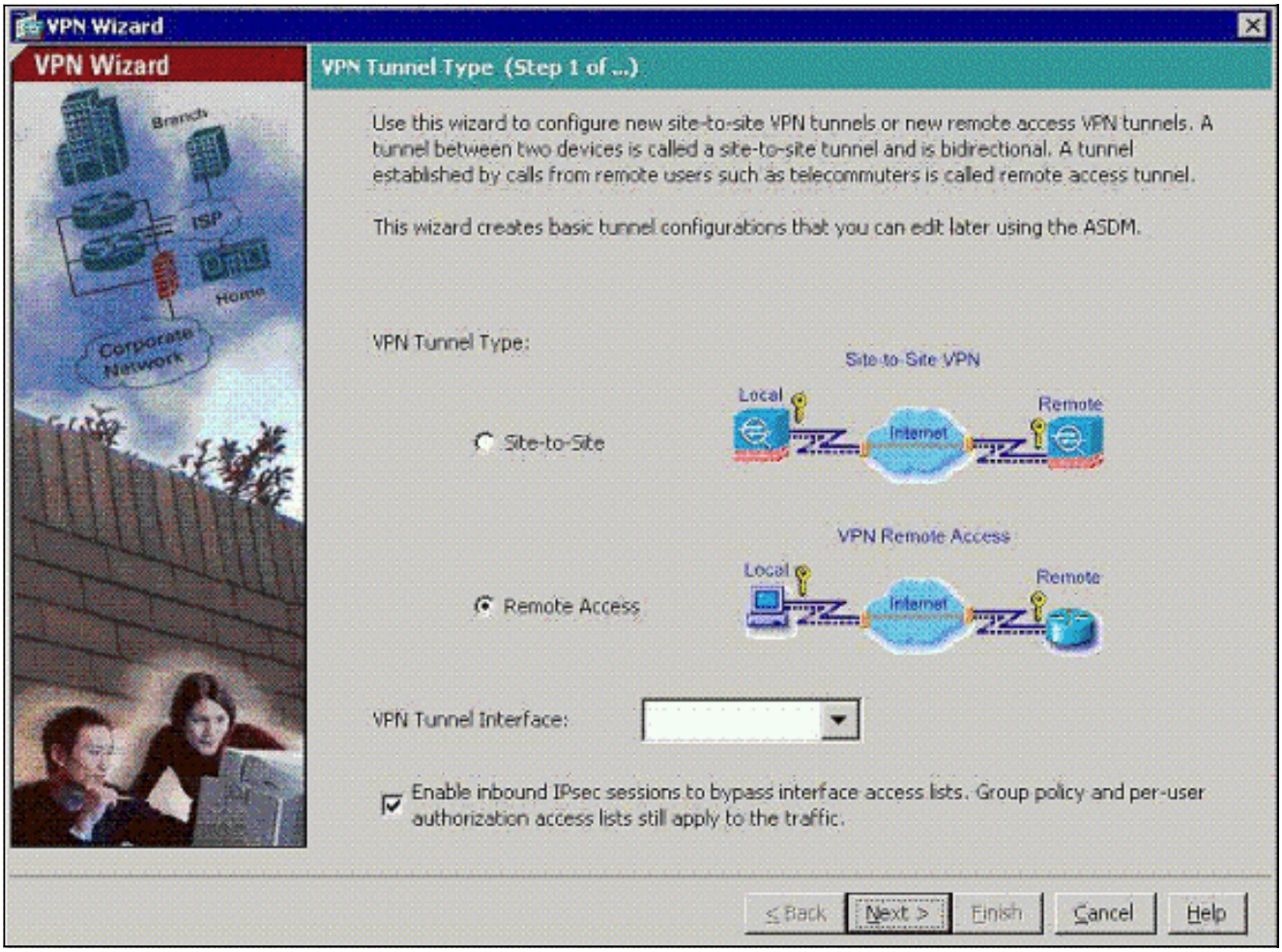
1. 홈 창에서 **Wizards > IPsec VPN Wizard**를 선택합니다

.



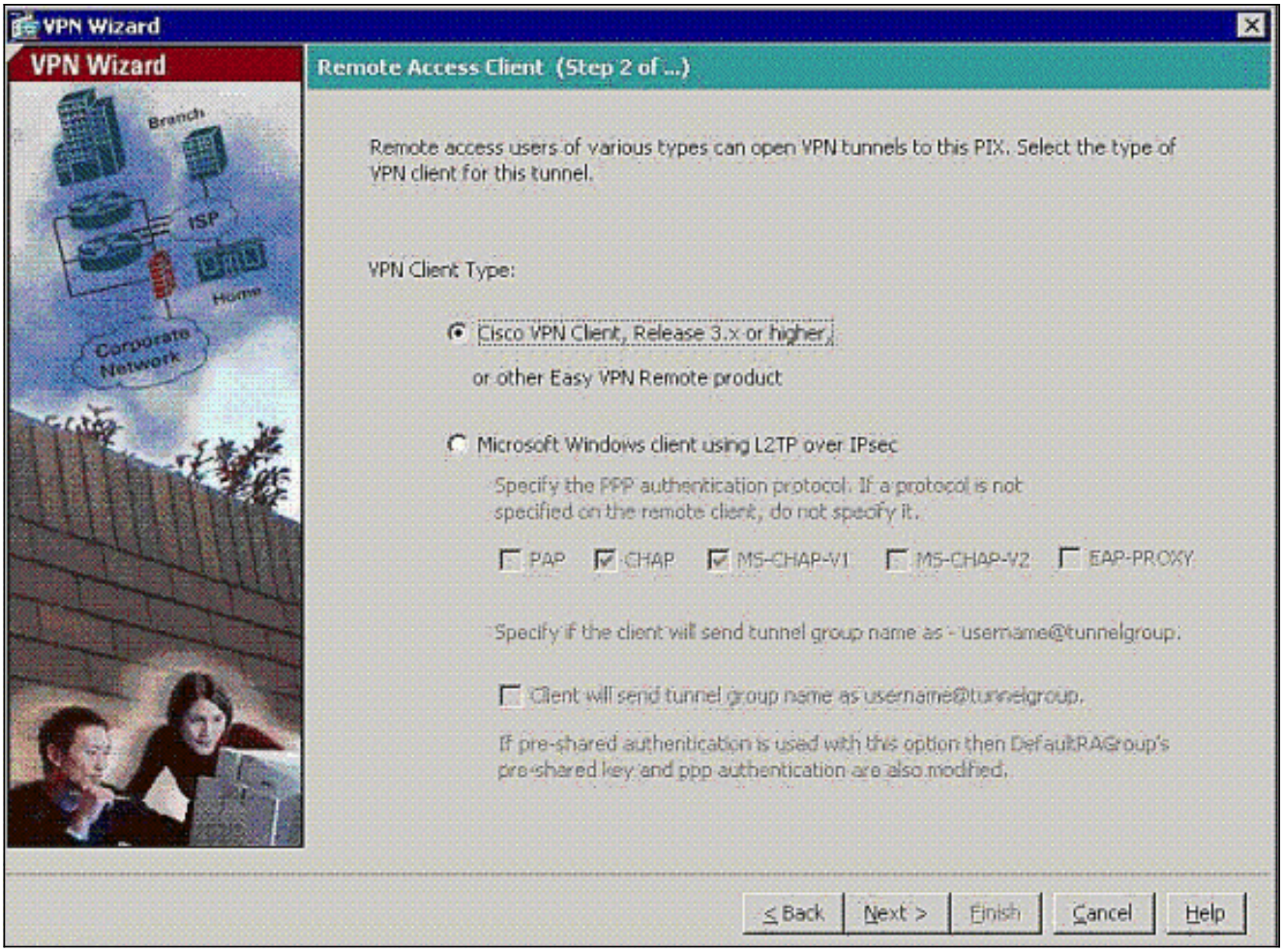
2. Remote **Access** VPN 터널 유형을 선택하고 VPN 터널 인터페이스가 원하는 대로 설정되었는지 확인합니다

.



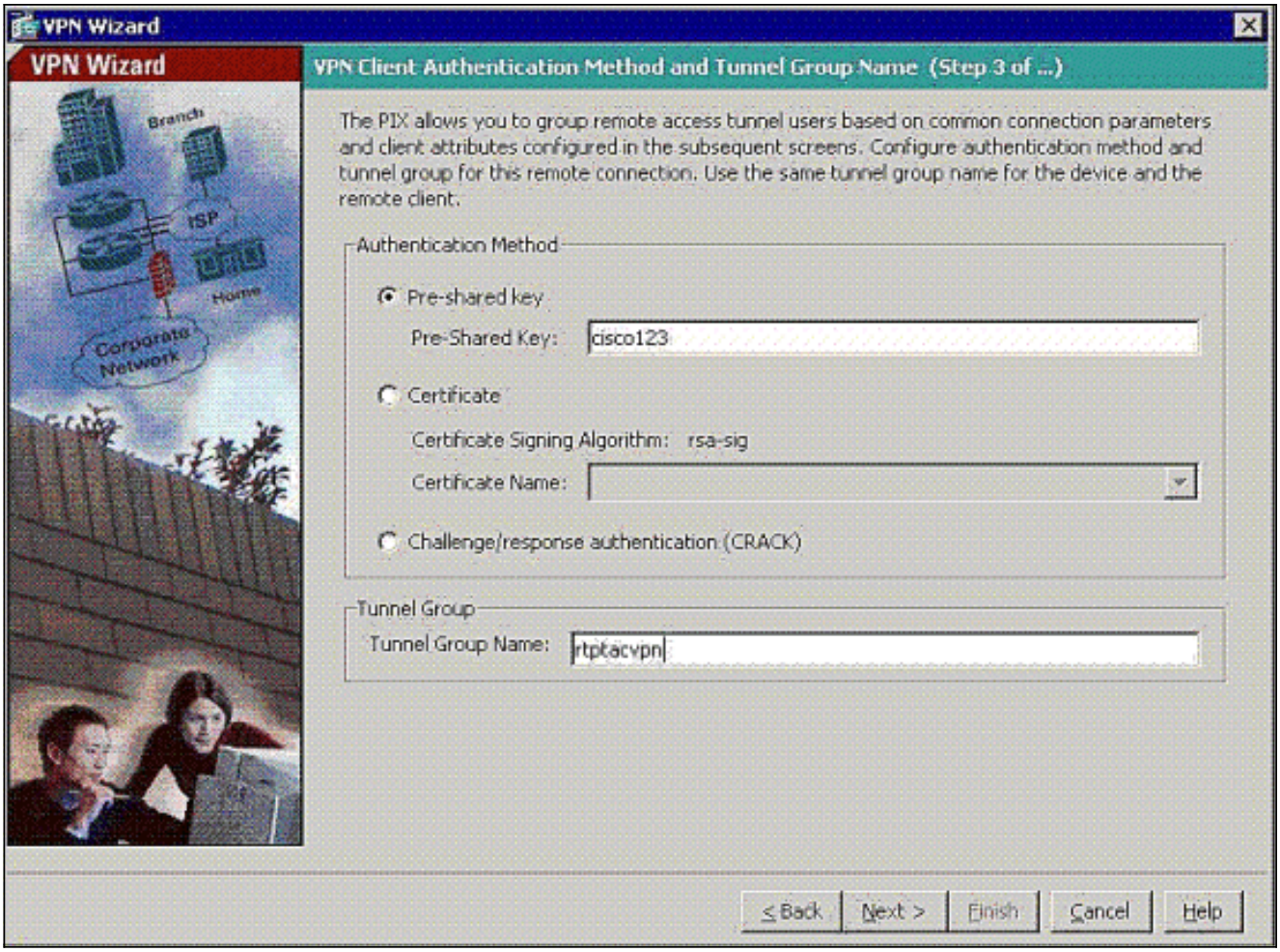

3. 사용 가능한 유일한 VPN 클라이언트 유형이 이미 선택되어 있습니다.Next(**다음)를 클릭합니다**

.



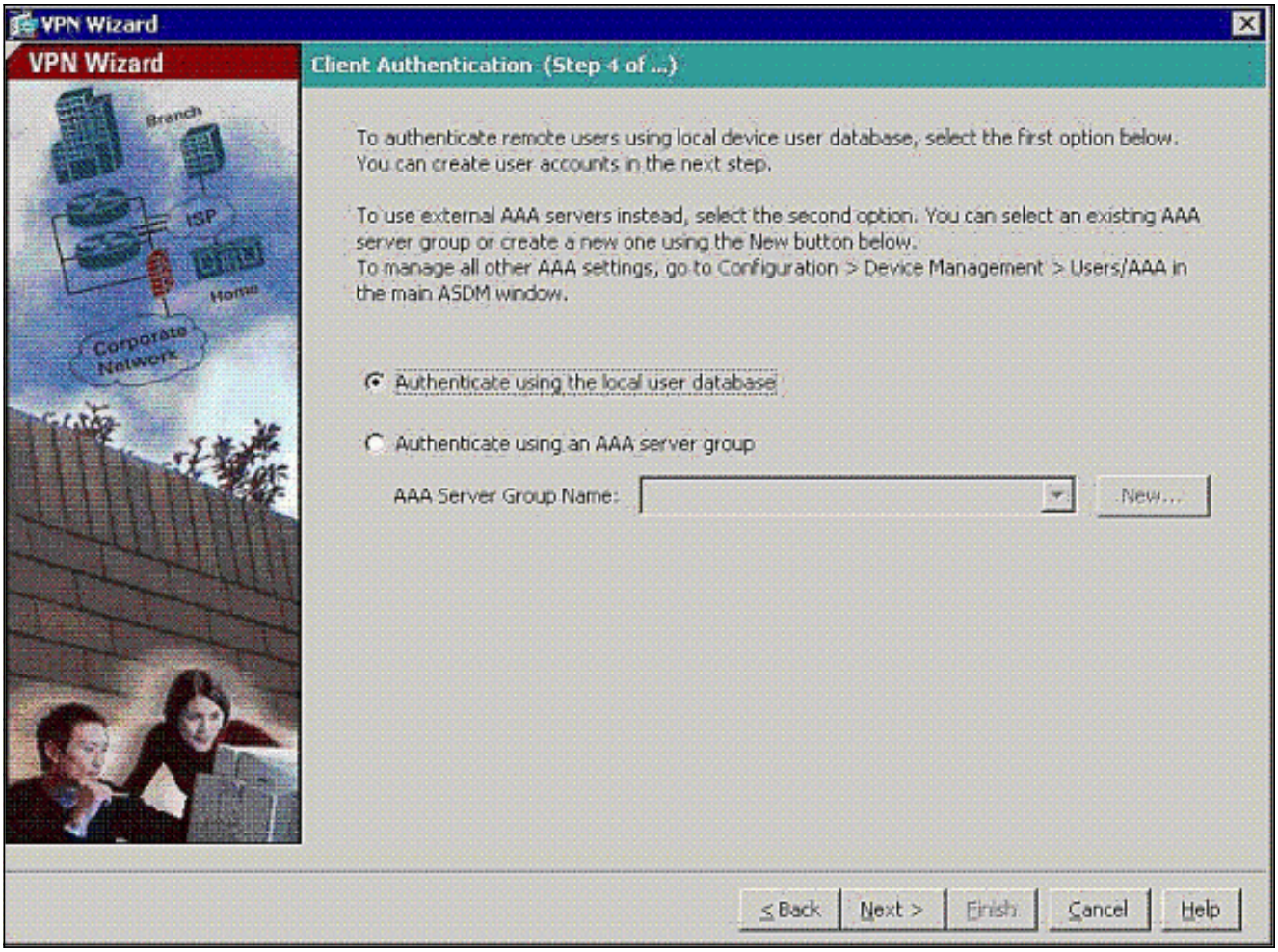

4. 터널 그룹 이름의 이름을 입력합니다.사용할 인증 정보를 입력합니다.**이 예에서 사전 공유 키**가 선택됩니다

.



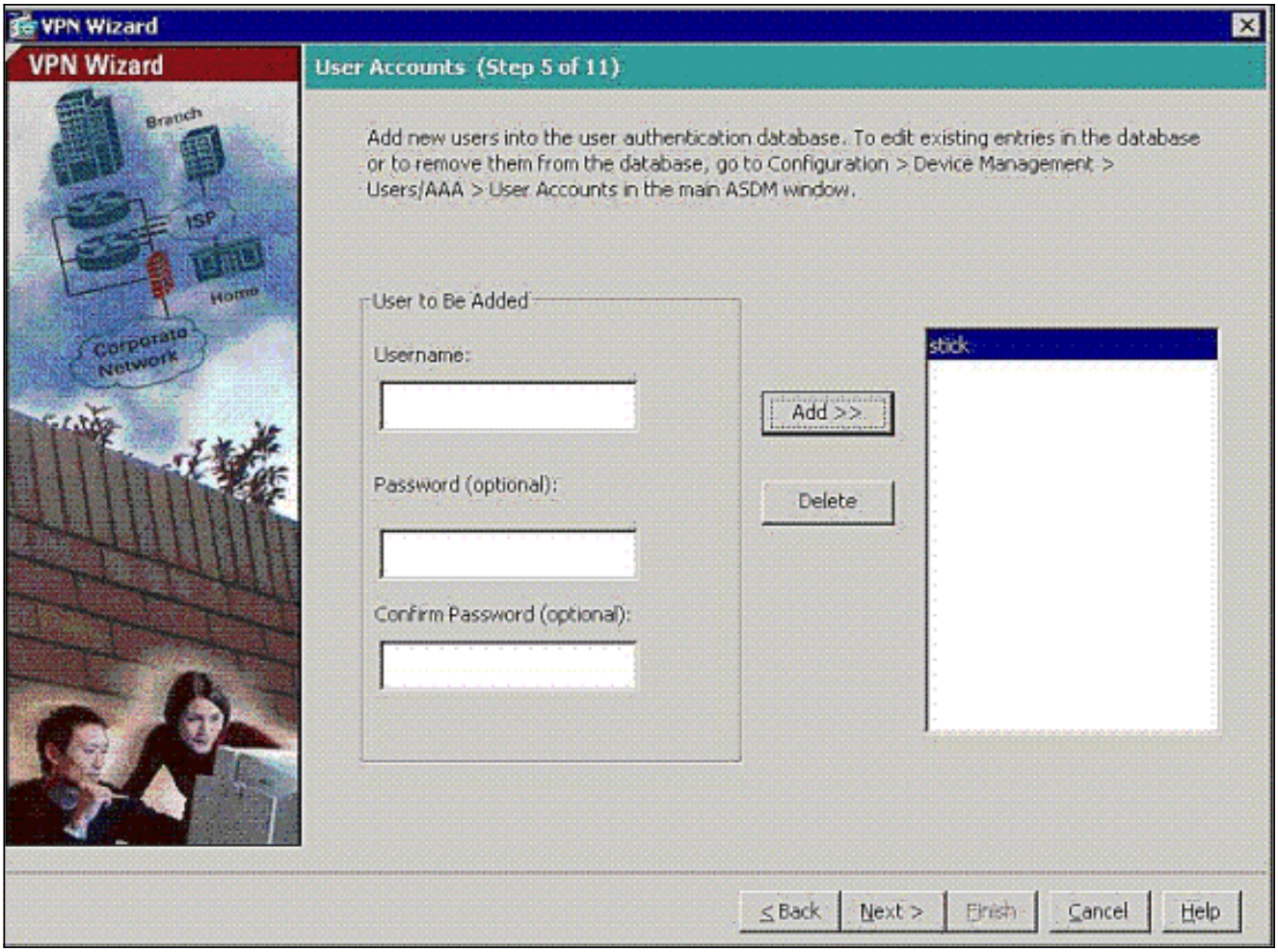

**참고:** ASDM에서 사전 공유 키를 숨기거나 암호화하는 방법은 없습니다.그 이유는 ASDM은 ASA를 구성하는 사람 또는 이 컨피그레이션을 지원하는 사람만이 사용해야 하기 때문입니다.

5. 원격 사용자를 로컬 사용자 데이터베이스에 인증할지 아니면 외부 AAA 서버 그룹에 인증할지를 선택합니다.**참고:** 6단계에서 사용자를 로컬 사용자 데이터베이스에 추가합니다.**참고:** ASDM을 통해 외부 AAA 서버 그룹을 구성하는 방법에 대한 자세한 내용은 ASDM 컨피그레이션을 통해 VPN 사용자용 PIX/ASA 7.x 인증 및 권한 부여 서버 그룹을 참조하십시오
.



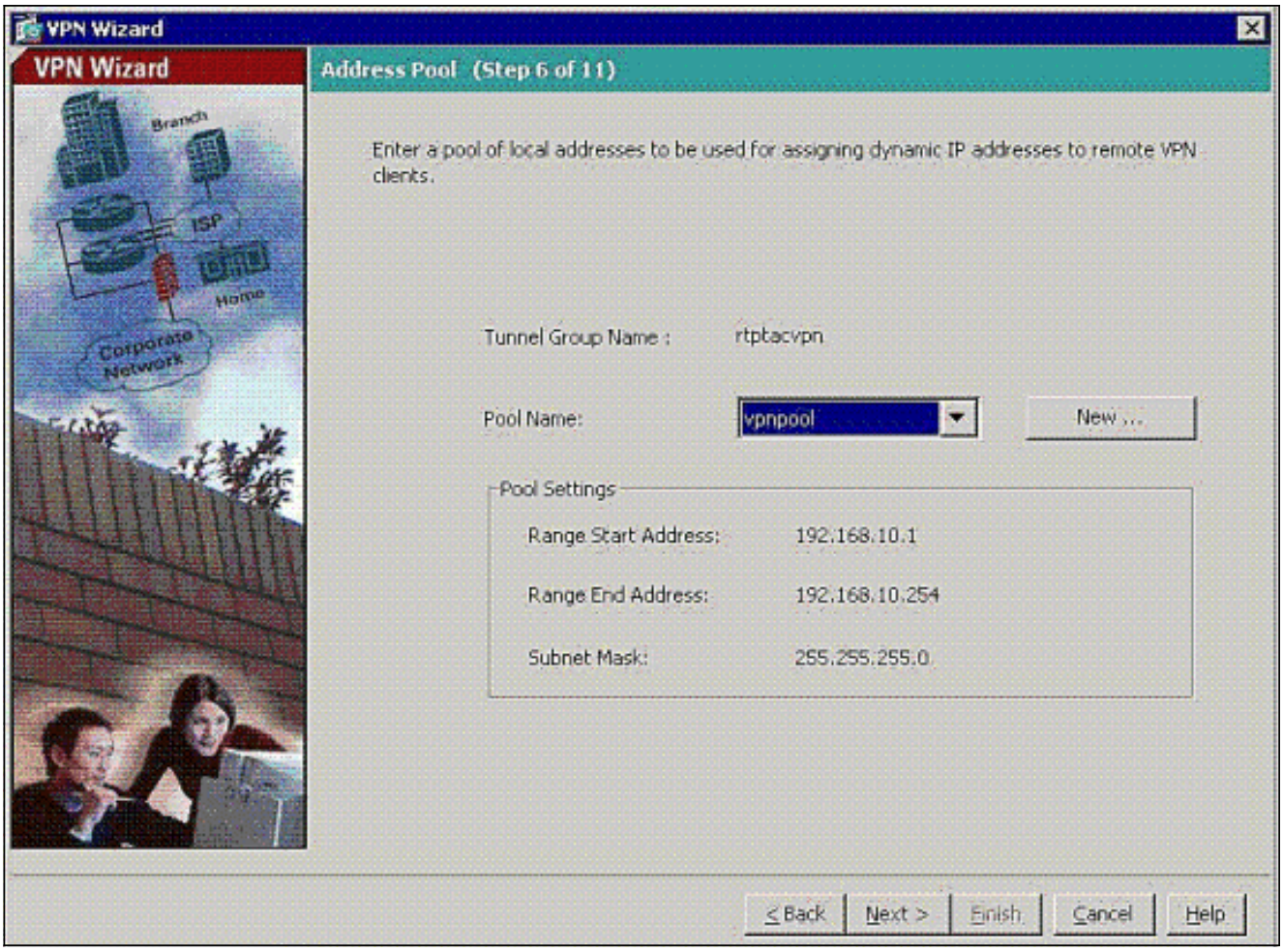

6. 필요한 경우 로컬 데이터베이스에 사용자를 추가합니다.**참고:** 이 창에서 현재 사용자를 제거하지 마십시오.데이터베이스**에서** 기존 항목을 편집하거나 데이터베이스에서 제거하려면 **기본 ASDM 창에서 Configuration > Device Administration > Administration > User Accounts**를 선택합니다

.



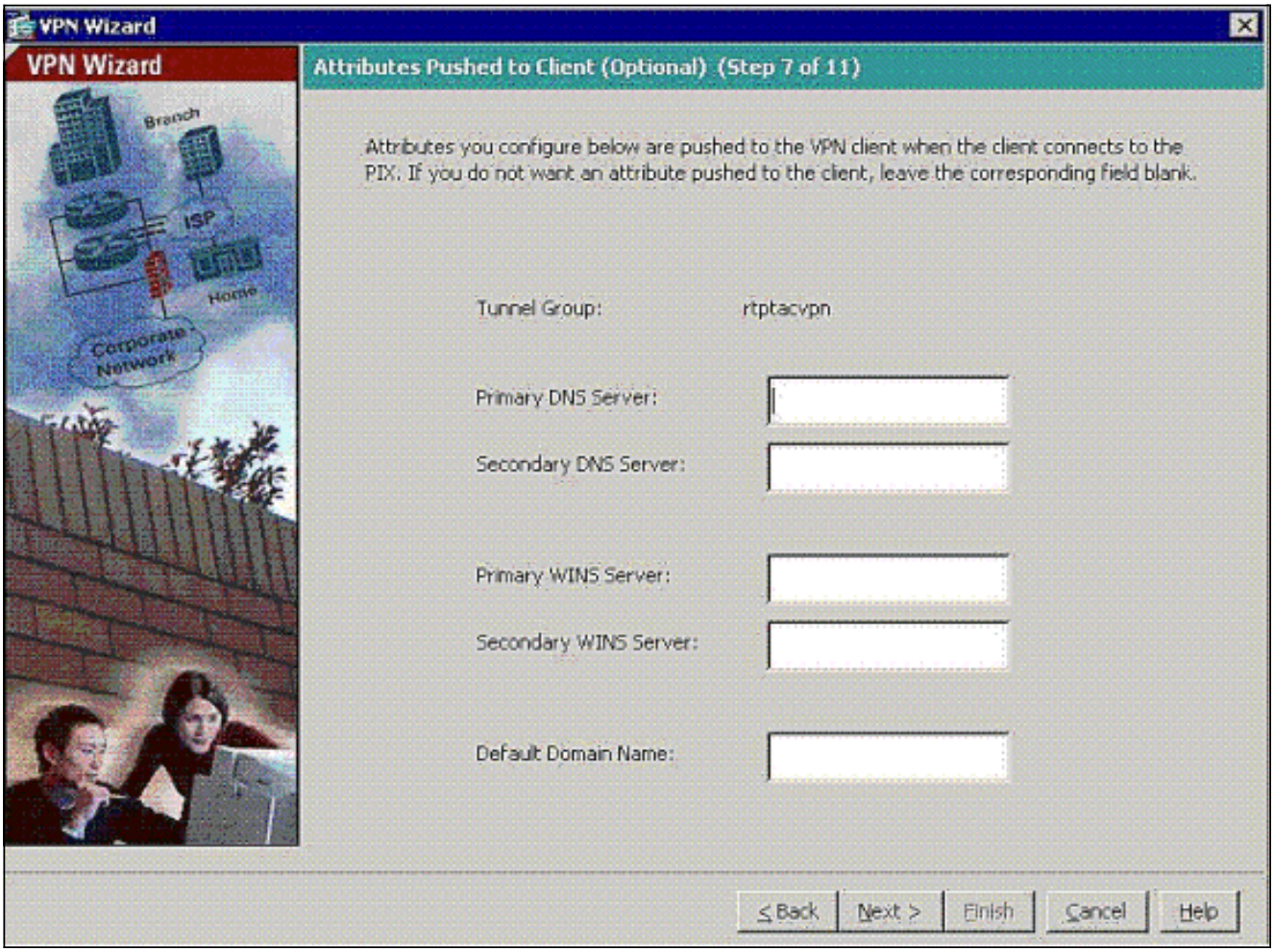

7. 연결할 때 원격 VPN 클라이언트에 동적으로 할당할 로컬 주소 풀을 정의합니다

.



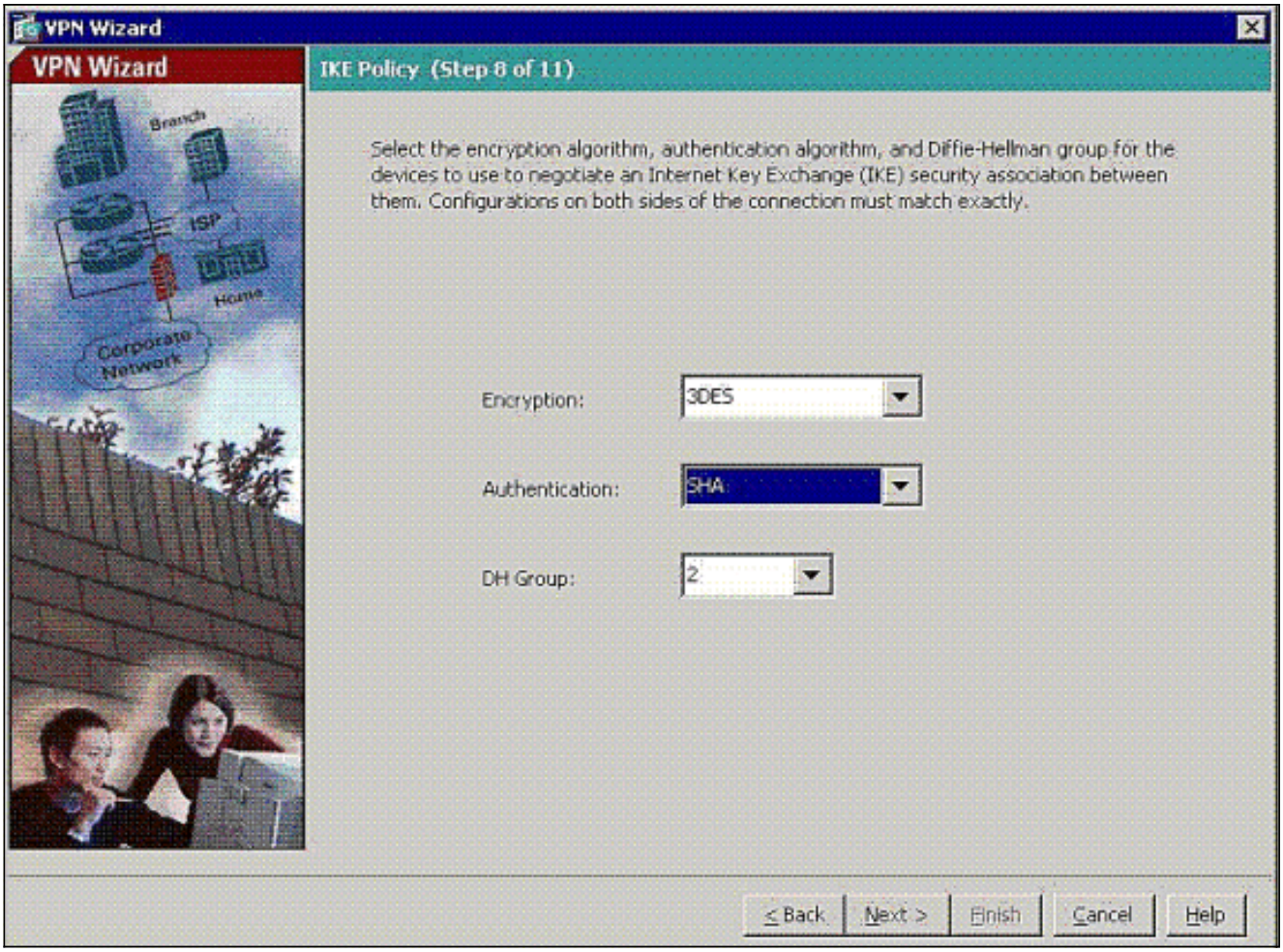
8. *선택 사항:*원격 VPN 클라이언트에 푸시할 DNS 및 WINS 서버 정보 및 기본 도메인 이름을 지정합니다

.



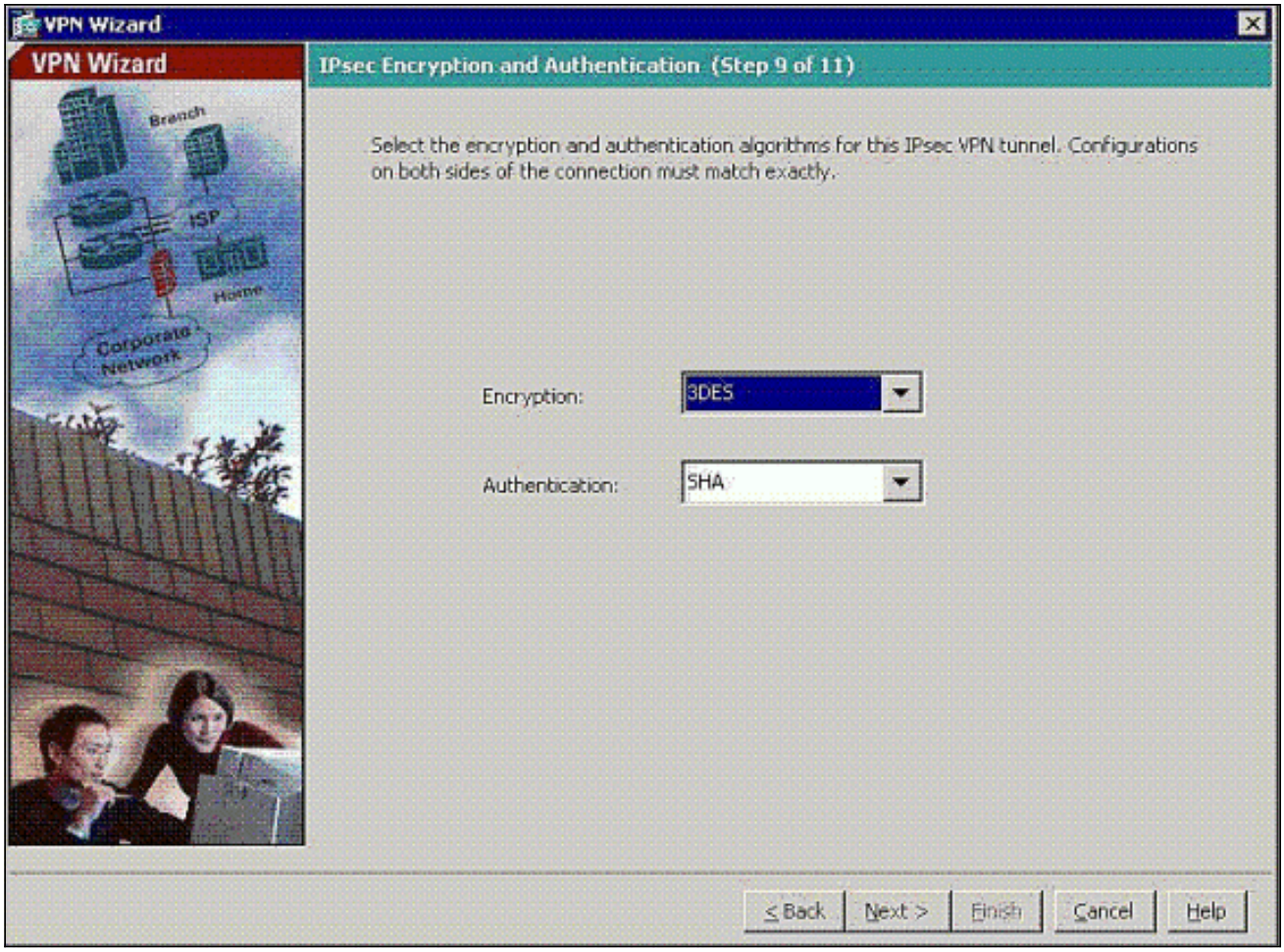

9. IKE 1단계라고도 하는 IKE의 매개변수를 지정합니다.터널의 양쪽에 있는 컨피그레이션은 정확히 일치해야 하지만 Cisco VPN Client는 자동으로 적절한 컨피그레이션을 선택합니다.클라이언트 PC에는 IKE 컨피그레이션이 필요하지 않습니다

.



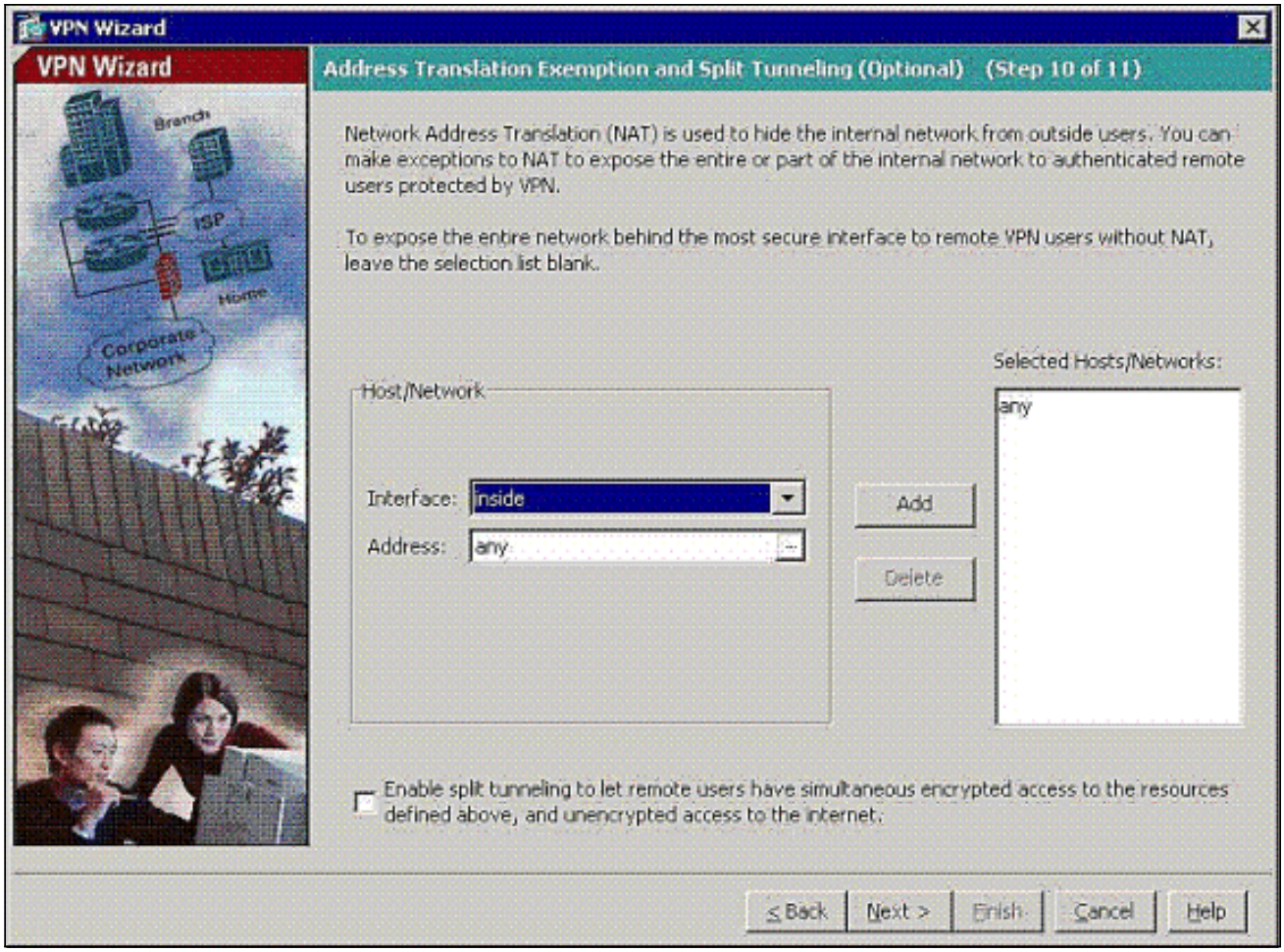

10. IKE Phase 2라고도 하는 IPSec의 매개변수를 지정합니다.터널의 양쪽에 있는 컨피그레이션은 정확히 일치해야 하지만 Cisco VPN Client는 자동으로 적절한 컨피그레이션을 선택합니다.클라이언트 PC에는 IKE 컨피그레이션이 필요하지 않습니다

.



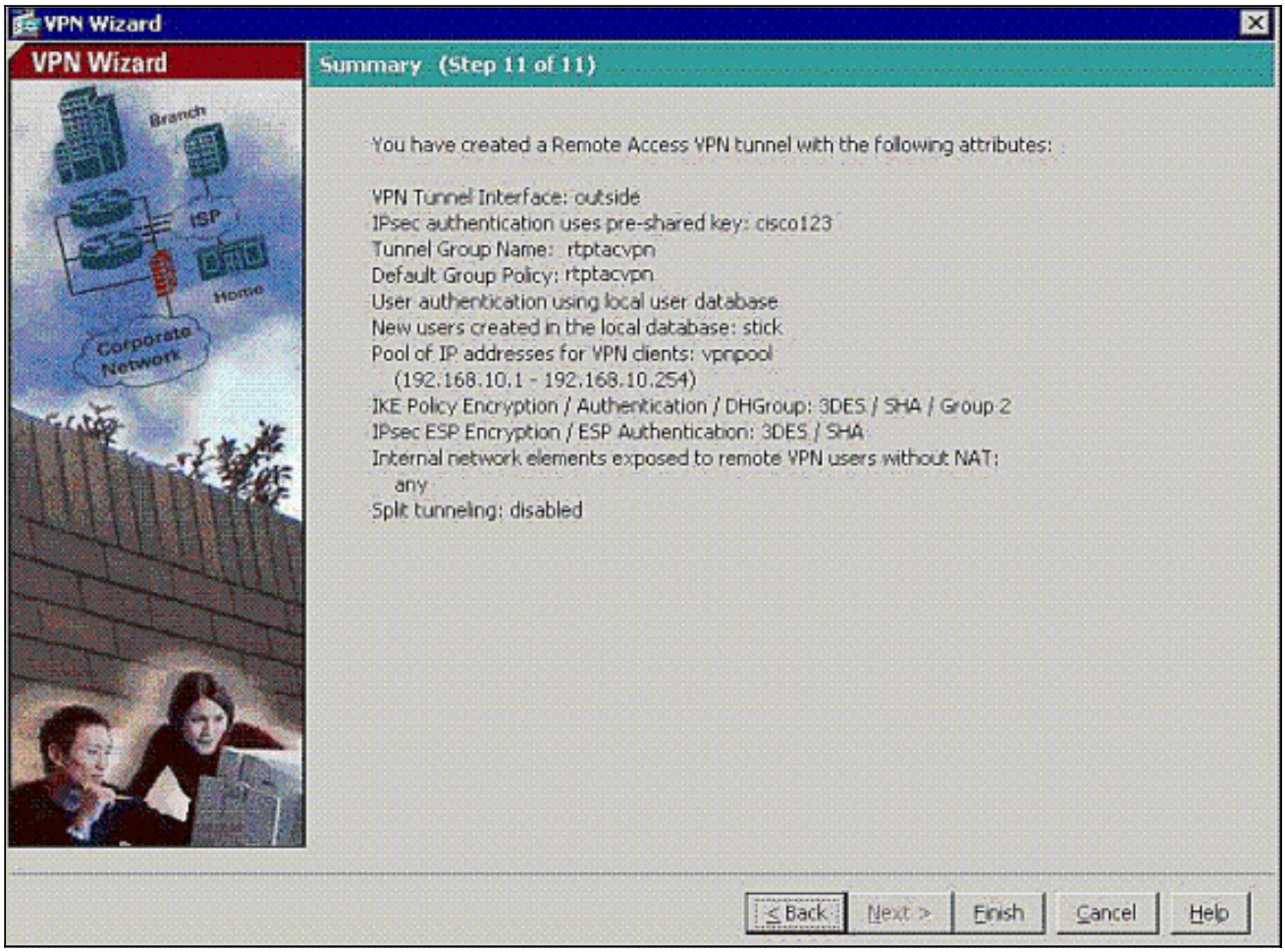

11. 내부 호스트 또는 네트워크가 원격 VPN 사용자에게 노출될 수 있는 경우 지정합니다.이 목록을 비워 두면 원격 VPN 사용자가 ASA의 전체 내부 네트워크에 액세스할 수 있습니다.이 창에서 스플릿 터널링을 활성화할 수도 있습니다.스플릿 터널링은 이 절차의 앞부분에서 정의한 리소스로 트래픽을 암호화하고 해당 트래픽을 터널링하지 않음으로써 인터넷에 대한 암호화되지 않은 액세스를 제공합니다.스플릿 터널링이 *활성화되지 않으면* 원격 VPN 사용자의 모든 트래픽이 ASA로 터널링됩니다.이는 컨피그레이션에 따라 대역폭과 프로세서 집약적인 문제가 될 수 있습니다

.



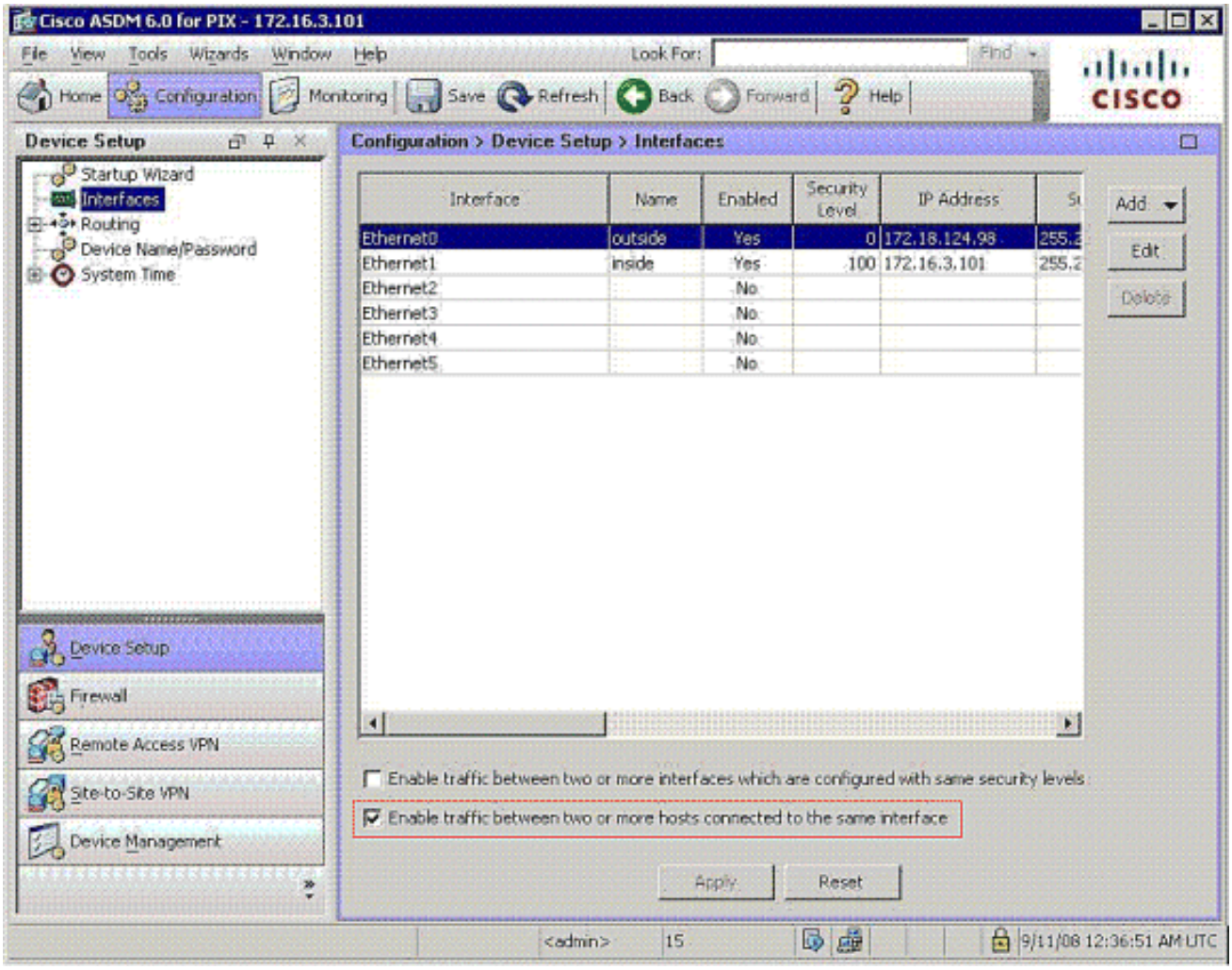

12. 이 창에는 수행한 작업의 요약이 표시됩니다.구성에 만족하면 마침을 클릭합니다

.



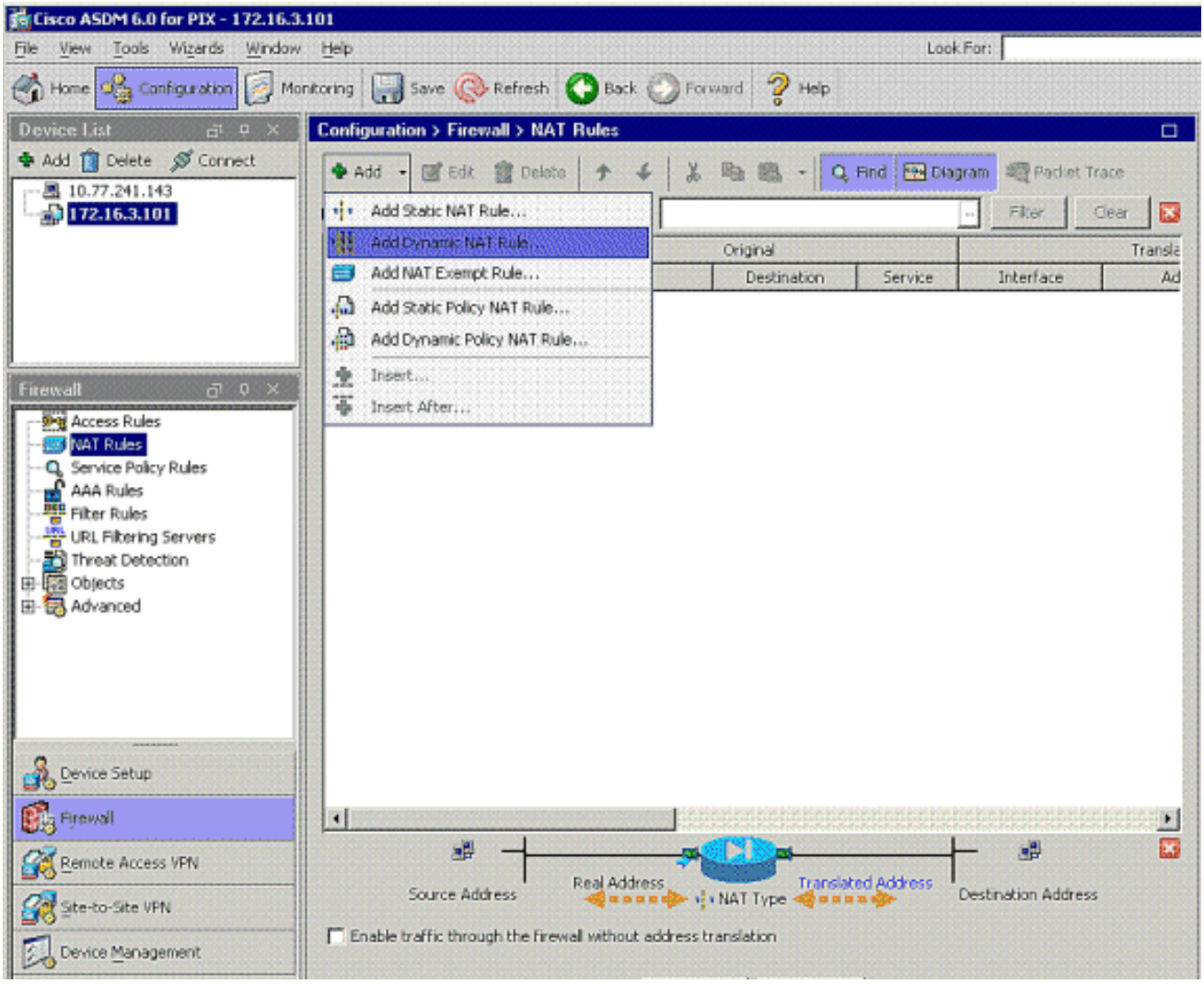
13. 명령 same-**security-traffic을 구성하여** 다음과 같이 확인란을 클릭할 때 동일한 인터페이스에 연결된 둘 이상의 호스트 간 트래픽을 활성화합니다

.

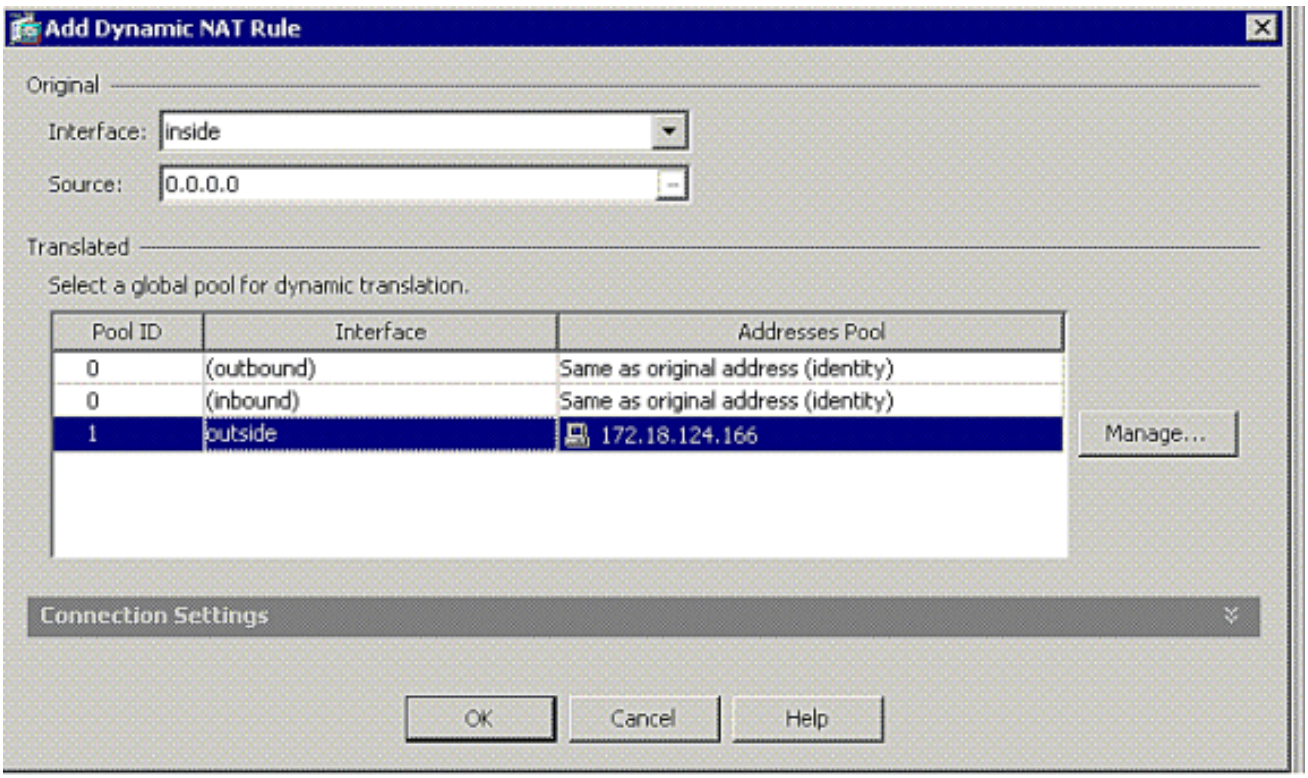



14. Configuration(**컨피그레이션) > Firewall(방화벽) > NAT Rules(NAT 규칙)**를 선택하고 **Add Dynamic NAT Rule(동적 NAT 규칙 추가)을** 클릭하여 ASDM을 사용하여 이 동적 변환을 생성합니다

.

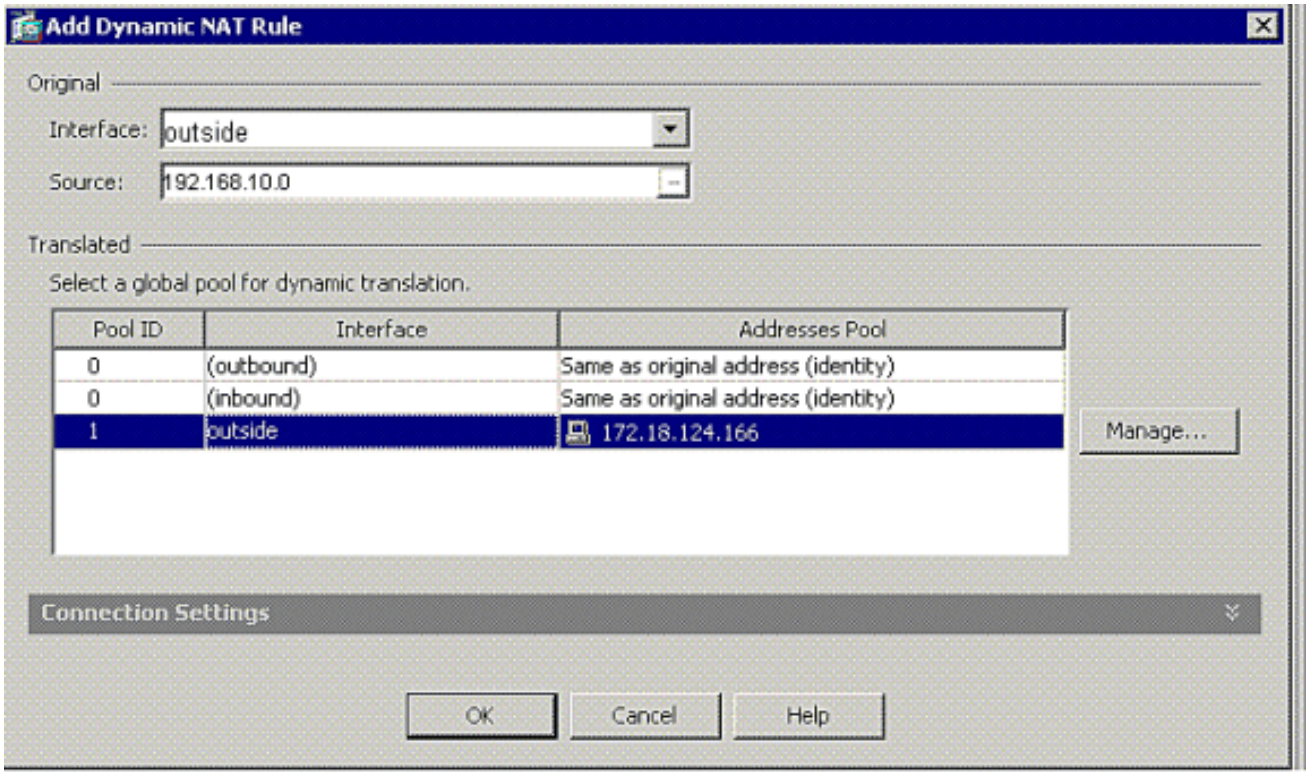



15. **내부**를 소스 인터페이스로 선택하고 NAT할 주소를 입력합니다.Translate Address on Interface(인터페이스에서 주소 변환)에서 **outside(외부)**를 선택하고 **OK(확인)**를 클릭합니다
.



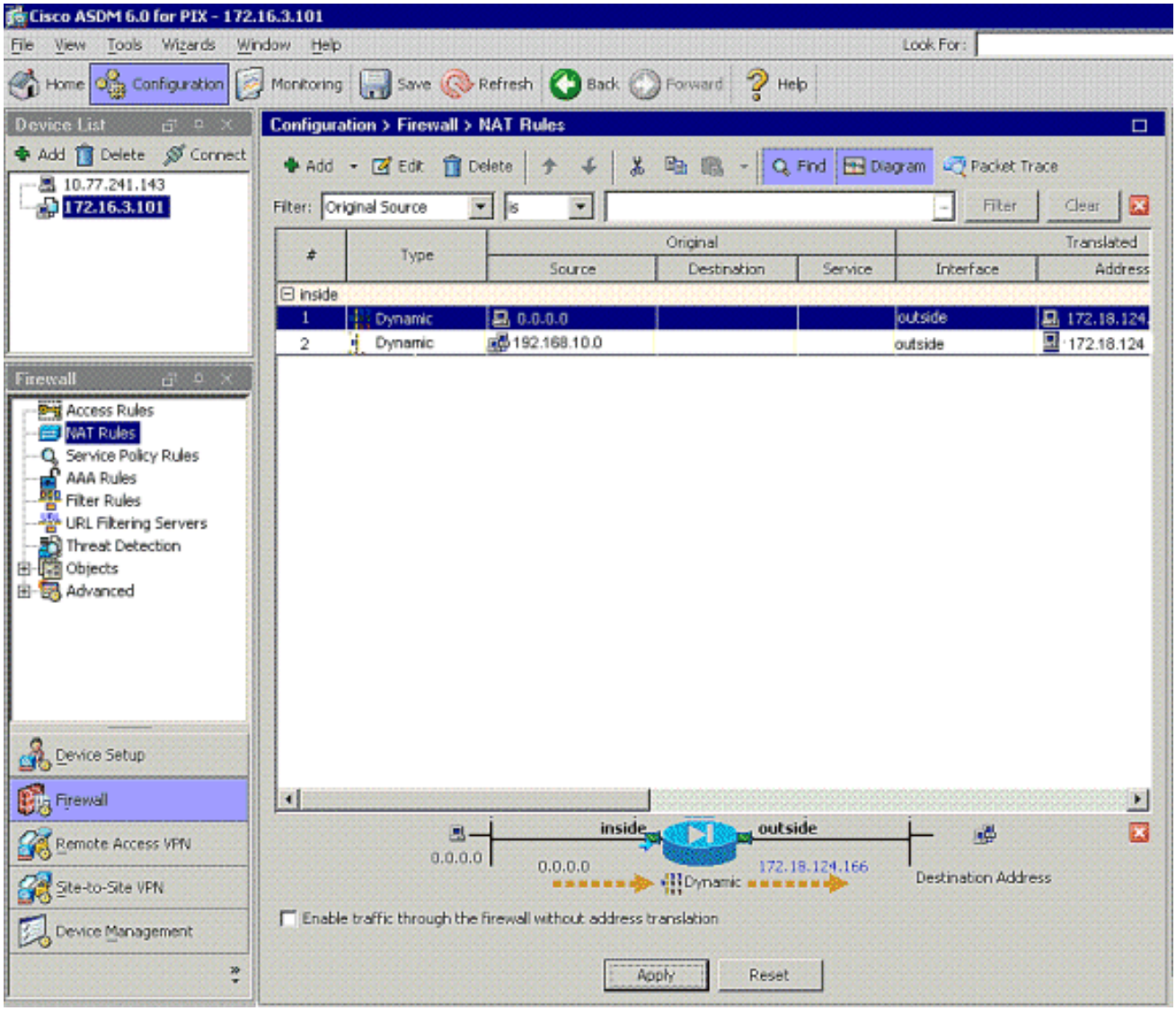

16. **outside**를 소스 인터페이스로 선택하고 NAT할 주소를 입력합니다.Translate Address on Interface(인터페이스에서 주소 변환)에서 **outside(외부)**를 선택하고 **OK(확인)**를 클릭합니다

.




17. 변환은 Translation Rules at Configuration(컨피그레이션) > Firewall(방화벽) > NAT Rules(NAT 규칙**의 변환 규칙)에** 나타납니다

.




**참고 1:**sysopt connection permit-vpn 명령을 구성해야 합니다.show running-config sysopt 명령은 구성되었는지 확인합니다.

**참고 2:**선택적 UDP 전송에 대해 다음 출력을 추가합니다.

```
group-policy clientgroup attributes vpn-idle-timeout 20
ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

**참고 3:**VPN 클라이언트가 IPsec over TCP를 통해 연결할 수 있도록 PIX 어플라이언스의 전역 컨피그레이션에서 이 명령을 구성합니다.

```
isakmp ipsec-over-tcp port 10000
```

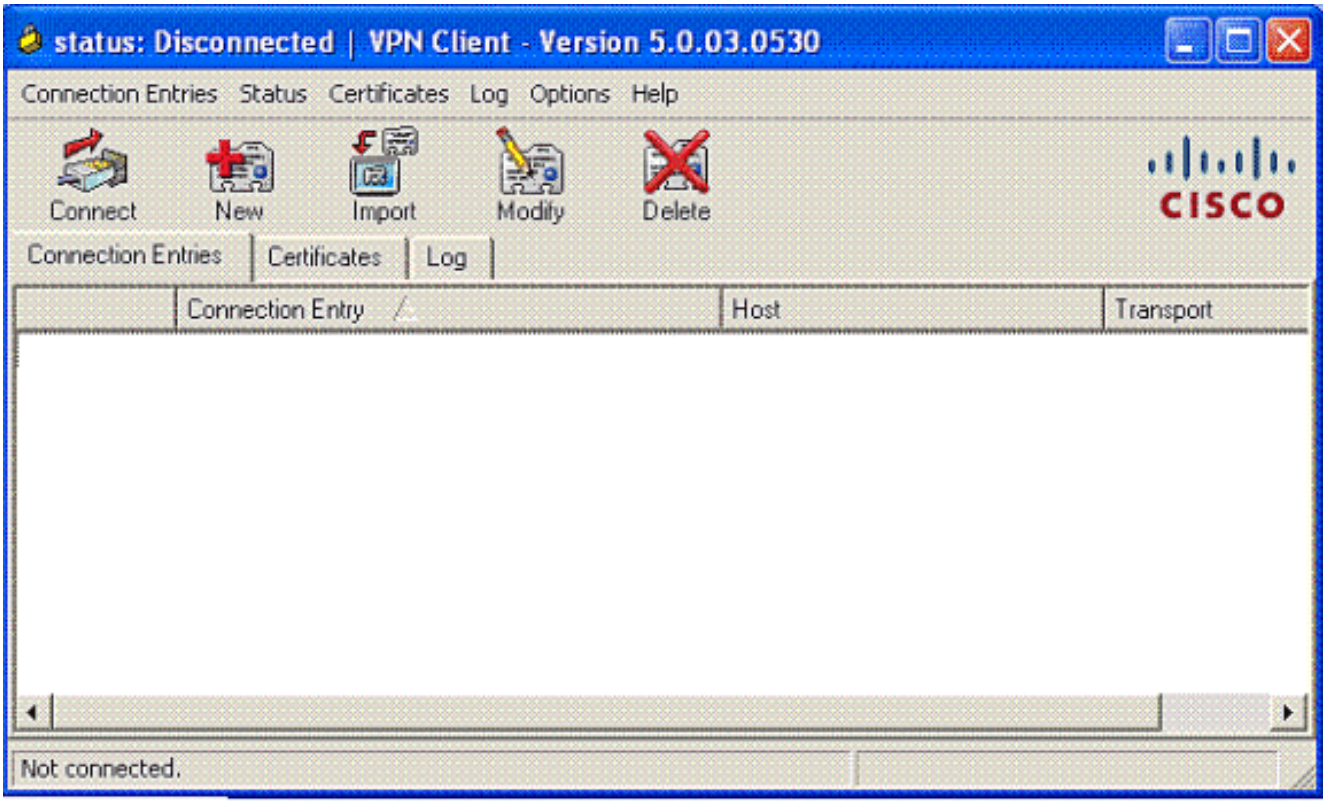
**참고:** Cisco ASA 의 헤어핀을 사용할 수 있는 다양한 시나리오에 대한 자세한 내용은 Hair-Pinning 비디오를 참조하십시오.

## VPN 클라이언트 컨피그레이션

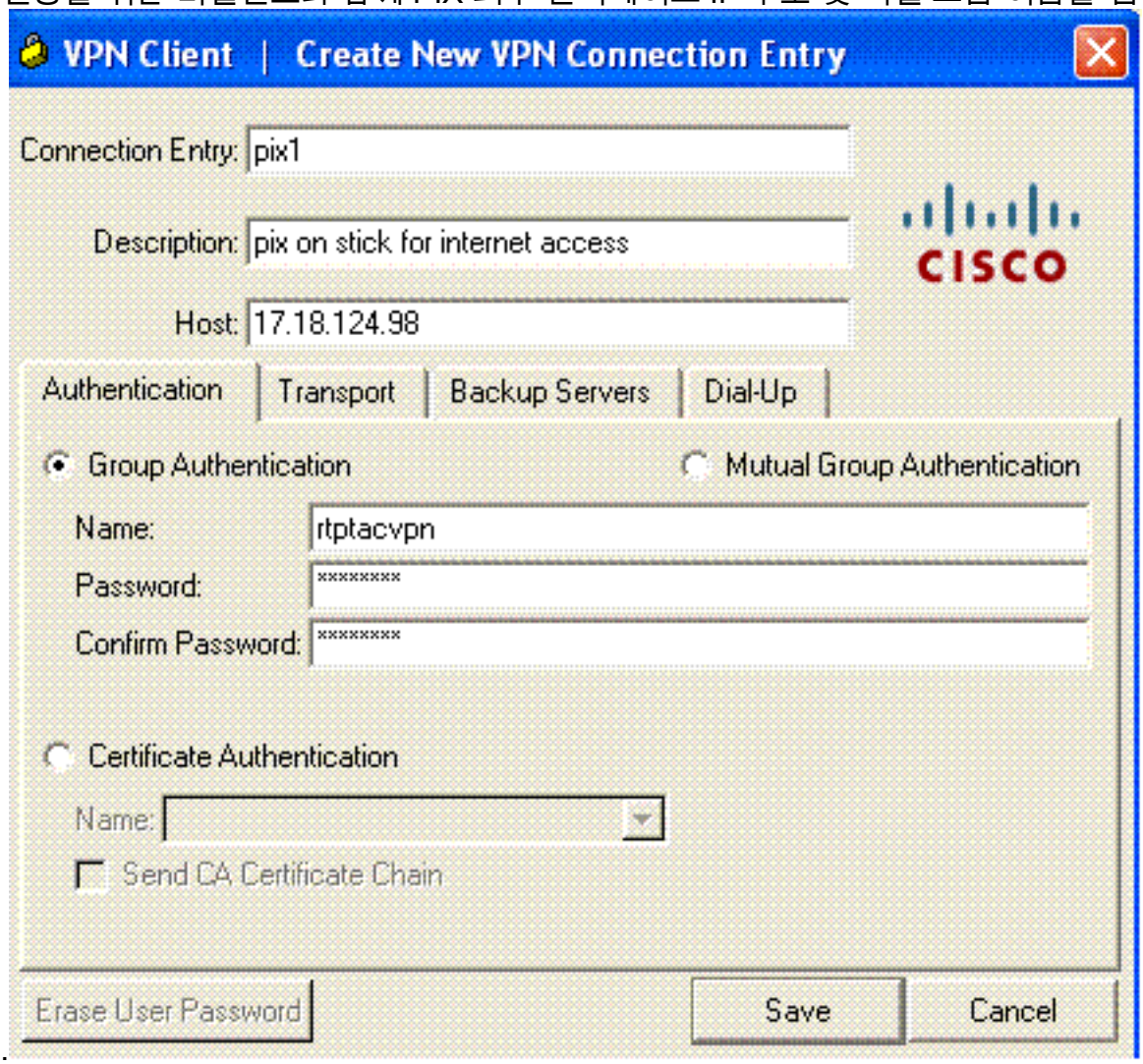
VPN 클라이언트를 구성하려면 다음 단계를 완료합니다.

1. 새로 **만들기를 선택합니다**

.



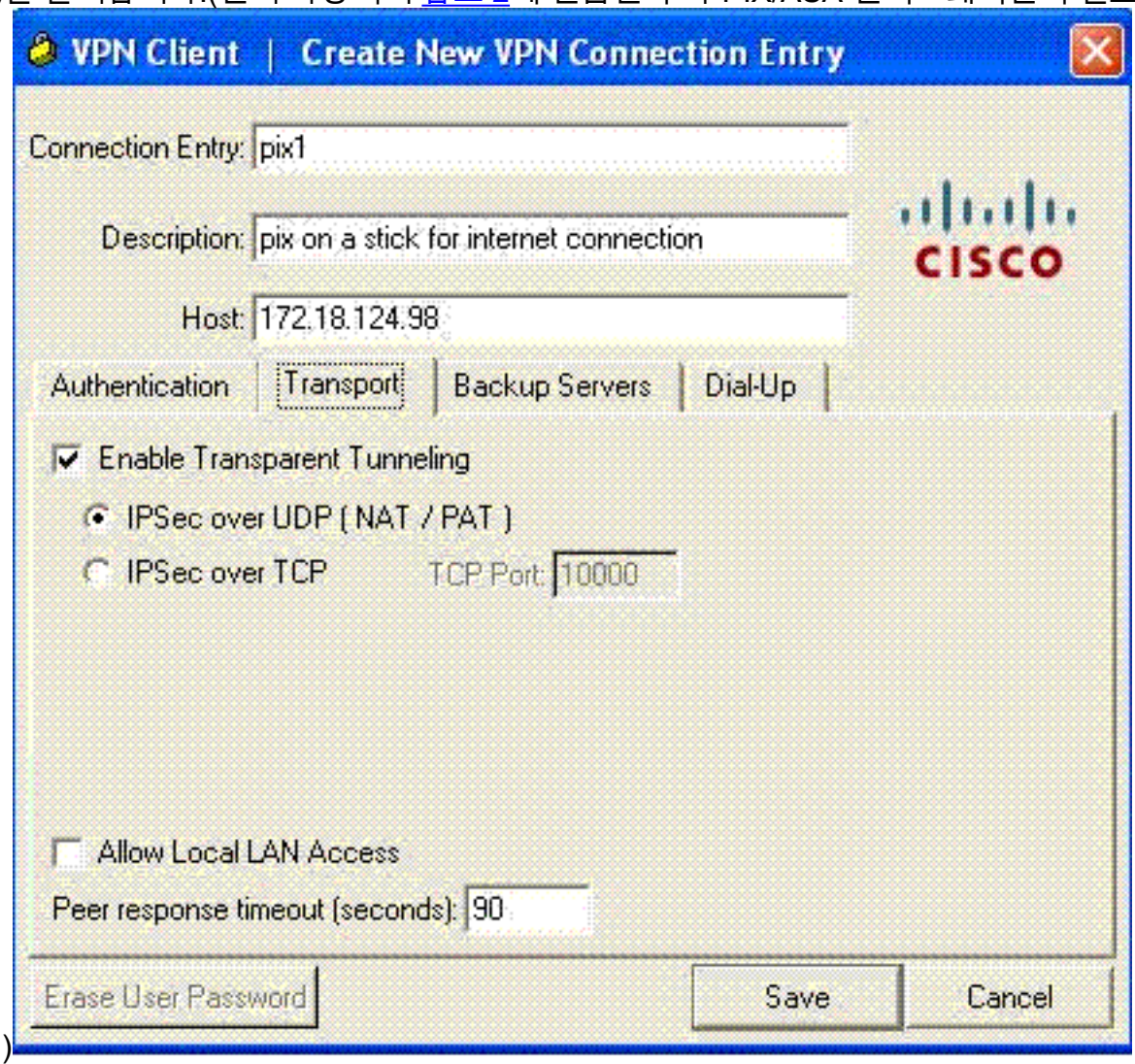

2. 인증을 위한 비밀번호와 함께 PIX 외부 인터페이스 IP 주소 및 터널 그룹 이름을 입력합니다




.

3. (*선택* 사항) Transport(전송) 탭 아래에서 Enable Transparent Tunneling(투명 터널링 활성화

)을 클릭합니다.(선택 사항이며 참고 2에 언급된 추가 PIX/ASA 컨피그레이션이 필요합니다




.)

4. 프로파일을 저장합니다.

# 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** - 피어에 있는 현재 IKE SA(보안 연결)를 모두 표시합니다.
- **show crypto ipsec sa** - 현재 모든 SA를 표시합니다.VPN 클라이언트 트래픽을 정의하는 SA에서 패킷을 암호화하고 해독합니다.

클라이언트에서 퍼블릭 IP 주소를 ping하거나 찾아봅니다(예: www.cisco.com).

**참고:** management-access 명령이 전역 확인 모드에서 구성되지 않는 한 PIX의 내부 인터페이스에서 터널을 생성할 수 없습니다.

```
PIX1(config)#management-access inside
PIX1(config)#show management-access

management-access inside
```

## VPN 클라이언트 확인

VPN 클라이언트를 확인하려면 다음 단계를 완료하십시오.

1. 연결 성공 후 시스템 트레이에 있는 VPN Client Lock(VPN 클라이언트 잠금) 아이콘을 마우스 오른쪽 버튼으로 클릭하고 암호화 및 암호 해독을 볼 **통계** 옵션을 선택합니다.
2. Route Details(경로 세부사항) 탭을 클릭하여 어플라이언스에서 전달된 스플릿 터널 없음 목록을 확인합니다.

# 문제 해결

**참고:** VPN 문제 해결 방법에 대한 자세한 내용은 VPN 문제 해결 **솔루션**을 참조하십시오.

# 관련 정보

- PIX Security Appliance 버전 7.0의 향상된 Spoke-to-Client VPN 컨피그레이션 예
- Cisco VPN 클라이언트
- IPsec 협상/IKE 프로토콜
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- Cisco ASA의 헤어핀
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems