CLI 및 ASDM 컨피그레이션을 사용하여 확장된 인증을 사용하는 원격 VPN 서버로서의 PIX/ASA 예

목차

소개

이 문서에서는 ASDM(Adaptive Security Device Manager) 또는 CLI를 사용하여 원격 VPN 서버로 작동하도록 Cisco 5500 Series ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.ASDM은 직관적이고 사용하기 쉬운 웹 기반 관리 인터페이스를 통해 세계적인 수준의 보안 관리 및 모니터링을 제공합니다.Cisco ASA 컨피그레이션이 완료되면 Cisco VPN 클라이언트를 사용하여 확인할 수 있습니다.

Cisco VPN Client(4.x for Windows)와 PIX 500 Series Security Appliance 7.x 간의 원격 액세스 VPN 연결을 설정하려면 Windows 2003 IAS RADIUS를 사용하는 PIX/ASA 7.x 및 Cisco VPN Client 4.x(Active Directory에 대해) 인증 컨피그레이션 예를 참조하십시오.원격 VPN 클라이언트 사용자는 Microsoft Windows 2003 IAS(Internet Authentication Service) RADIUS 서버를 사용하여 Active Directory에 대해 인증합니다.

확장 인증(Xauth)을 위해 Cisco VPN Client(4.x for Windows)와 PIX 500 Series Security Appliance 7.x(ACS 버전 3.2)를 사용하여 Cisco VPN Client(4.x for Windows) 간 원격 액세스 VPN 연결을 설정하려면 PIX/ASA 7.x 및 Cisco VPN Client 4.x를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에서는 ASA가 완전히 작동 중이고 Cisco ASDM 또는 CLI에서 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

참고: ASDM 또는 PIX/ASA 7.x에 대한 HTTPS 액세스 허용을 참조하십시오.ASDM 또는 SSH(Secure Shell)에서 디바이스를 원격으로 구성할 수 있도록 하려면 Inside 및 Outside Interface Configuration Example의 SSH를 사용합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance Software 버전 7.x 이상
- Adaptive Security Device Manager 버전 5.x 이상
- Cisco VPN Client Version 4.x 이상

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.x 이상에서도 사용할 수 있습니다.

표기 규칙

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

배경 정보

원격 액세스 컨피그레이션은 모바일 사용자와 같은 Cisco VPN 클라이언트에 안전한 원격 액세스를 제공합니다.원격 액세스 VPN을 사용하면 원격 사용자가 중앙 집중식 네트워크 리소스에 안전하게 액세스할 수 있습니다.Cisco VPN Client는 IPSec 프로토콜을 준수하며 보안 어플라이언스와 작동하도록 특별히 설계되었습니다.그러나 보안 어플라이언스는 많은 프로토콜 호환 클라이언트와의 IPSec 연결을 설정할 수 있습니다.IPSec에 대한 자세한 내용은 ASA 컨피그레이션 가이드를 참조하십시오.

그룹과 사용자는 VPN 보안 관리 및 보안 어플라이언스 컨피그레이션의 핵심 개념입니다.VPN에 대한 사용자 액세스 및 VPN 사용을 결정하는 특성을 지정합니다.그룹은 단일 엔티티로 처리되는 사용자 모음입니다.사용자는 그룹 정책에서 특성을 가져옵니다.터널 그룹은 특정 연결에 대한 그룹 정책을 식별합니다.사용자에게 특정 그룹 정책을 할당하지 않으면 연결에 대한 기본 그룹 정책이 적용됩니다.

터널 그룹은 터널 연결 정책을 결정하는 레코드 집합으로 구성됩니다.이러한 레코드는 터널 사용자가 인증되는 서버와 연결 정보가 전송되는 어카운팅 서버(있는 경우)를 식별합니다.또한 연결에 대한 기본 그룹 정책을 식별하고 프로토콜별 연결 매개변수를 포함합니다.터널 그룹에는 터널 자체 생성과 관련된 소수의 특성이 포함됩니다.터널 그룹에는 사용자 지향 특성을 정의하는 그룹 정책에 대한 포인터가 포함됩니다.

참고: 이 문서의 샘플 컨피그레이션에서는 로컬 사용자 계정이 인증에 사용됩니다.LDAP 및

RADIUS와 같은 다른 서비스를 사용하려면 권한 부여 및 인증을 위해 외부 RADIUS 서버 구성을 참조하십시오.

IKE라고도 하는 ISAKMP(Internet Security Association and Key Management Protocol)는 호스트가 IPSec 보안 연결을 구축하는 방법에 동의하는 협상 프로토콜입니다.각 ISAKMP 협상은 Phase1과 Phase2라는 두 섹션으로 구분됩니다. Phase1은 이후 ISAKMP 협상 메시지를 보호하기 위해 첫 번째 터널을 생성합니다.2단계에서는 보안 연결을 통과하는 데이터를 보호하는 터널을 생성합니다 .ISAKMP에 대한 자세한 내용은 CLI 명령에 대한 ISAKMP 정책 키워드를 참조하십시오.

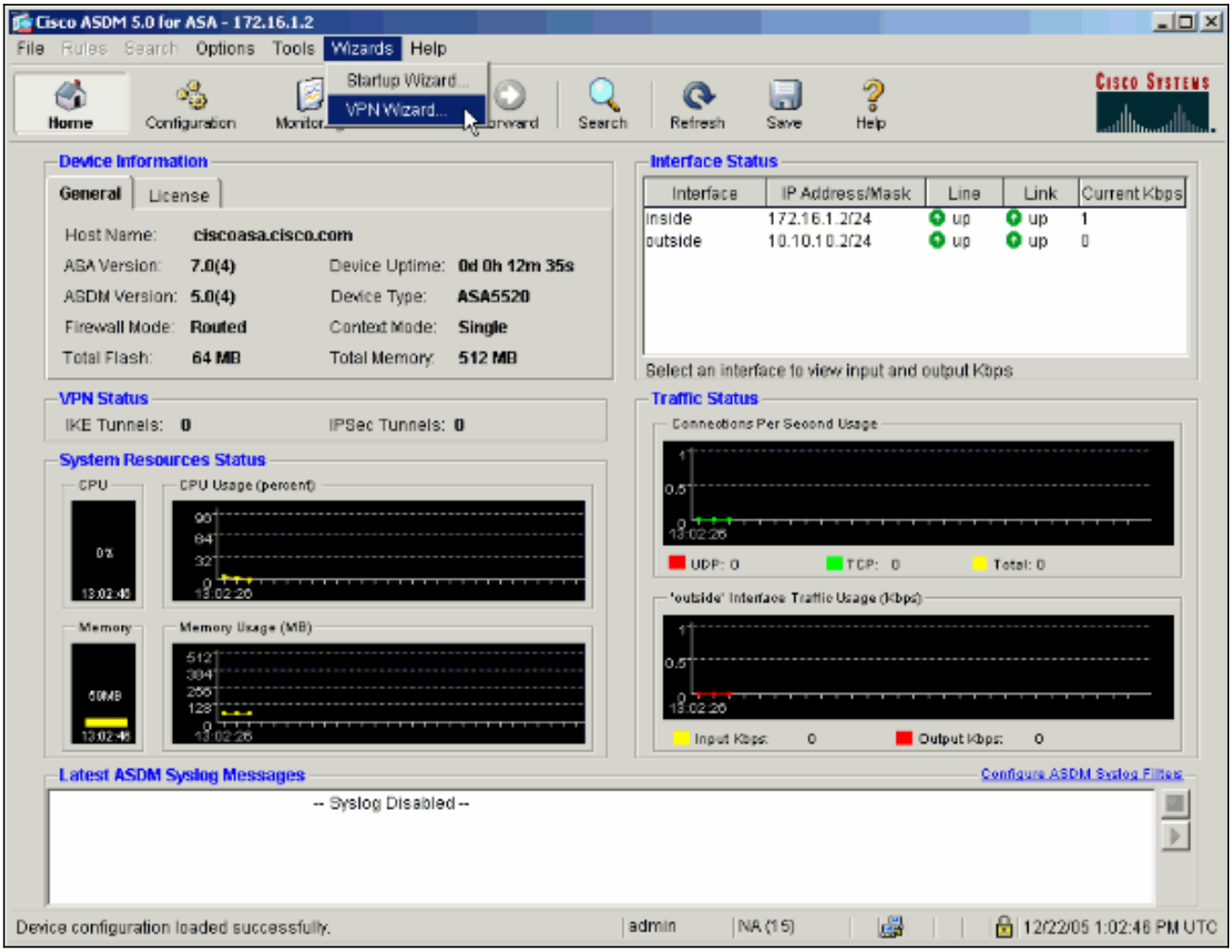
구성

ASDM을 사용하여 ASA/PIX를 원격 VPN 서버로 구성

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

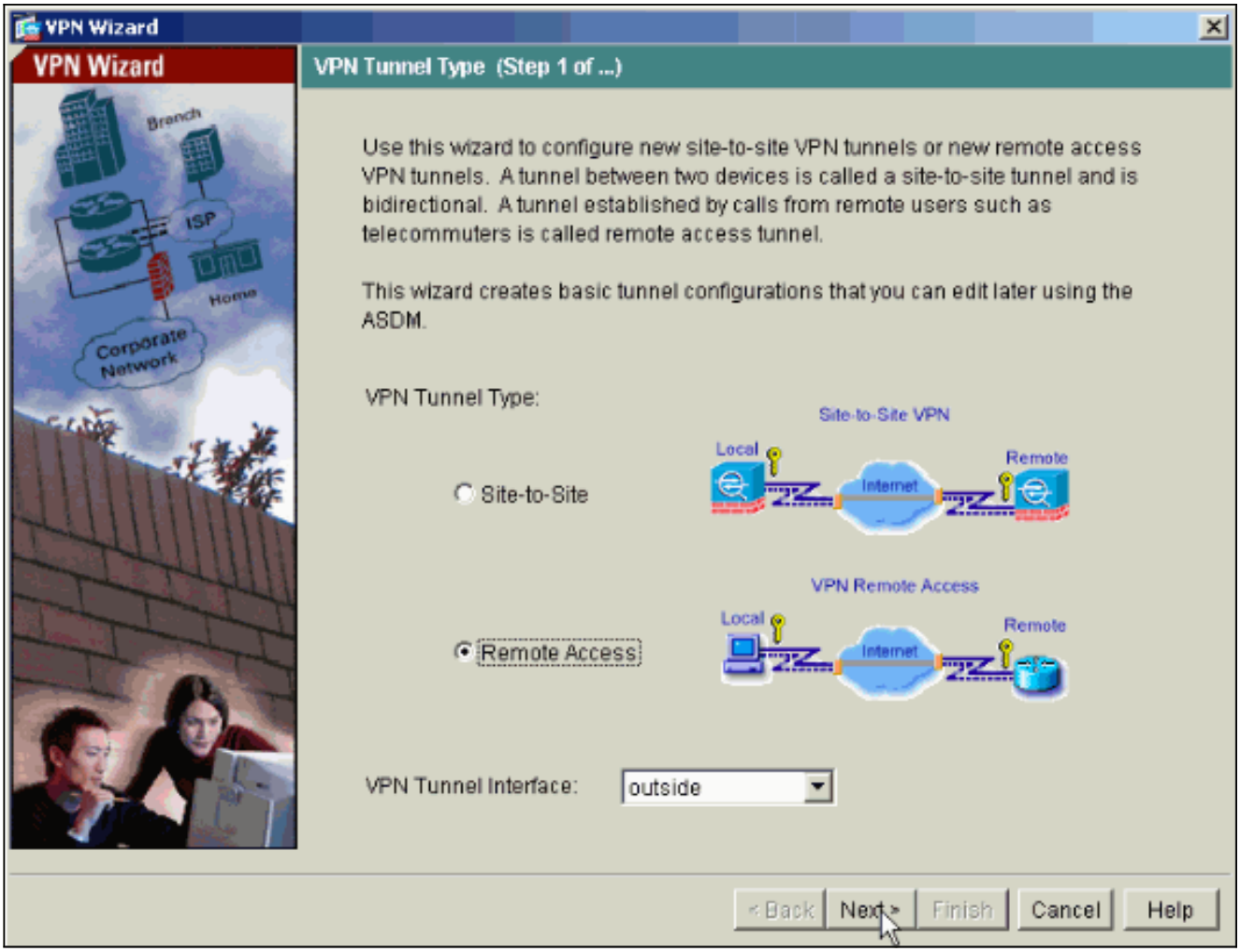
1. 홈 창에서 **Wizards > VPN Wizard**를 선택합니다

.



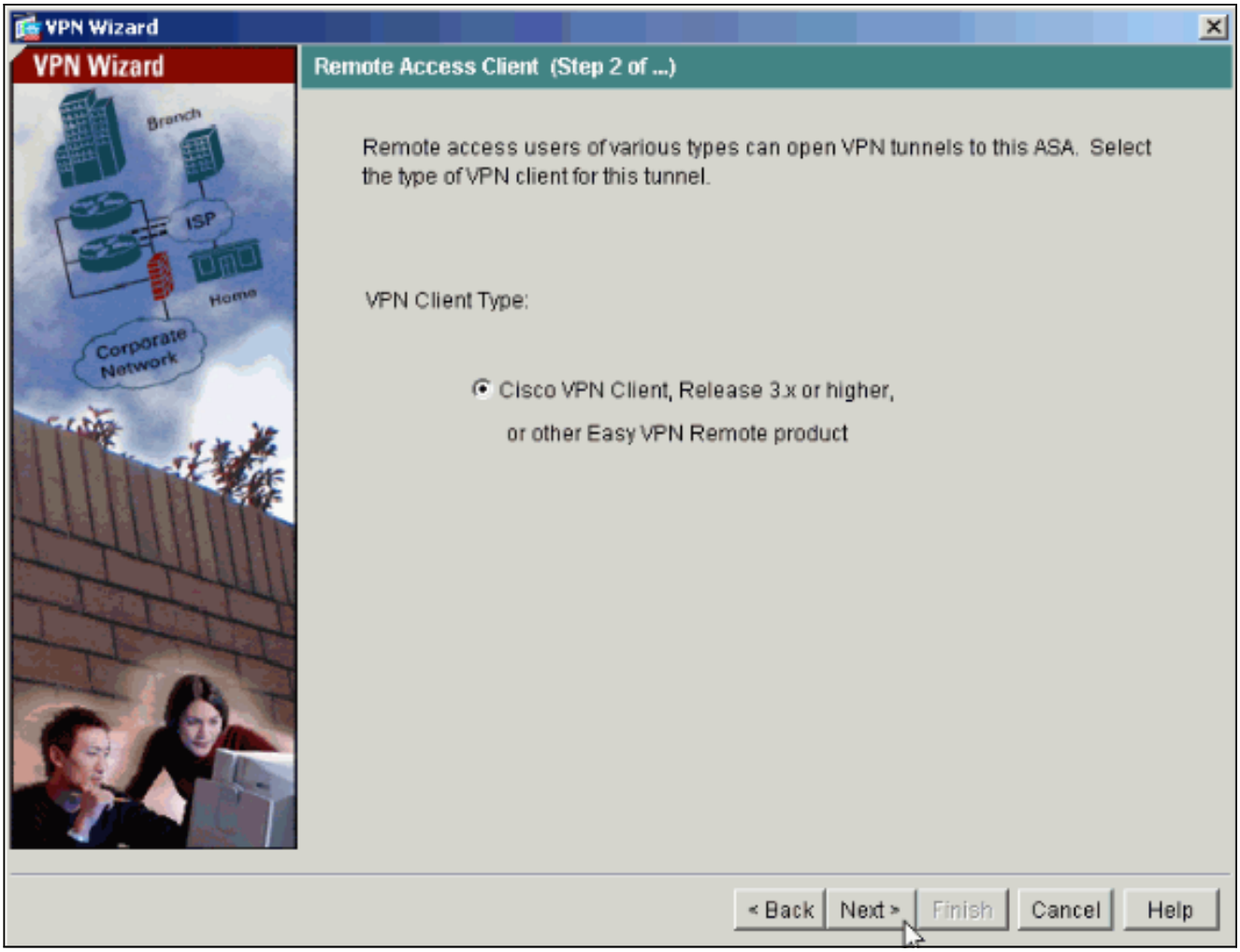
2. Remote **Access** VPN 터널 유형을 선택하고 VPN 터널 인터페이스가 원하는 대로 설정되었는지 확인합니다

.



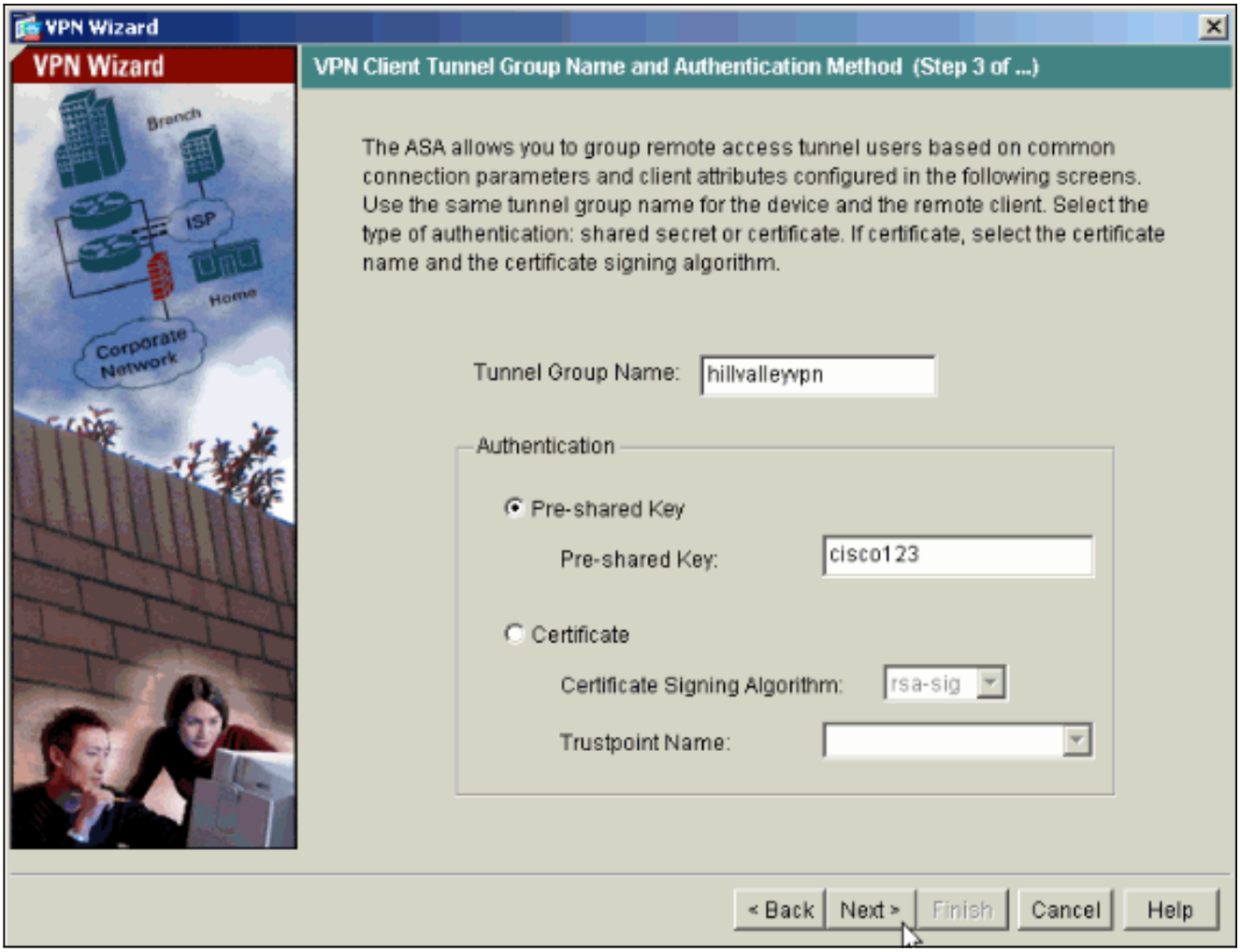
3. 사용 가능한 유일한 VPN 클라이언트 유형이 이미 선택되어 있습니다.Next(**다음)를 클릭합니다**

.



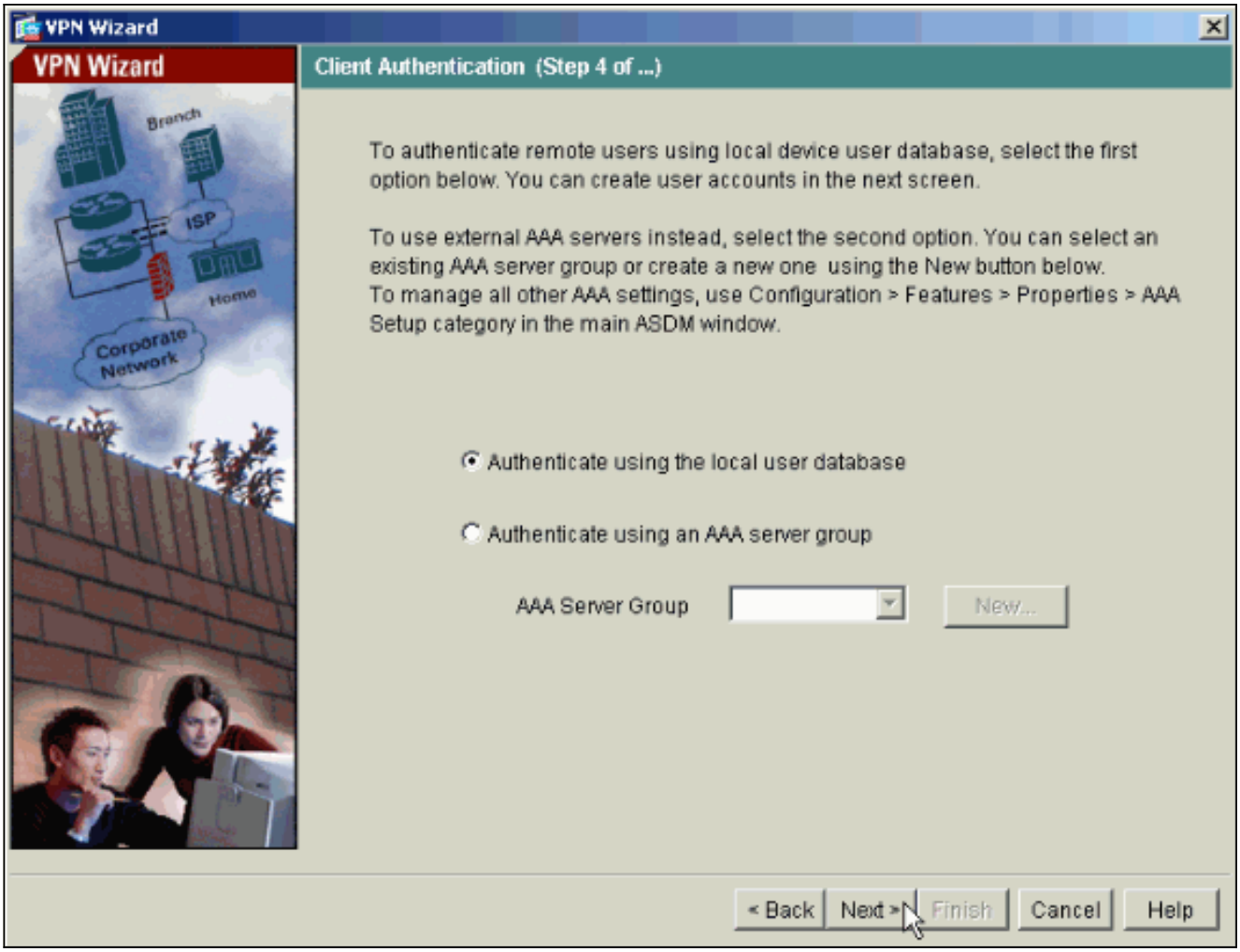
4. 터널 그룹 이름의 이름을 입력합니다.사용할 인증 정보를 입력합니다.**이 예에서 사전 공유 키**가 선택됩니다

.



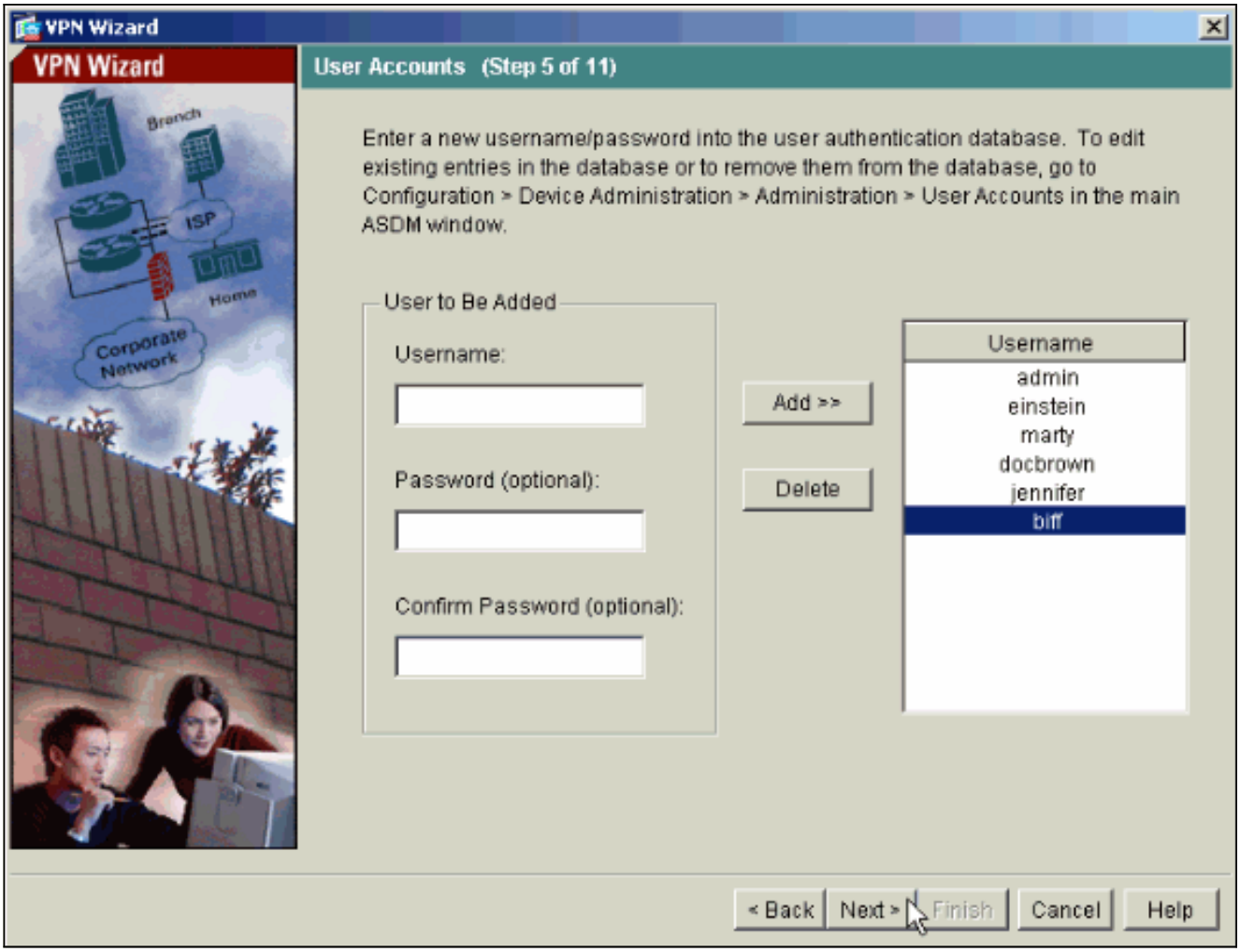
참고: ASDM에서 사전 공유 키를 숨기거나 암호화하는 방법은 없습니다.이유는 ASDM은 ASA를 구성하는 사람 또는 이 컨피그레이션을 고객에게 지원하는 사람만이 사용해야 하기 때문입니다.

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
.

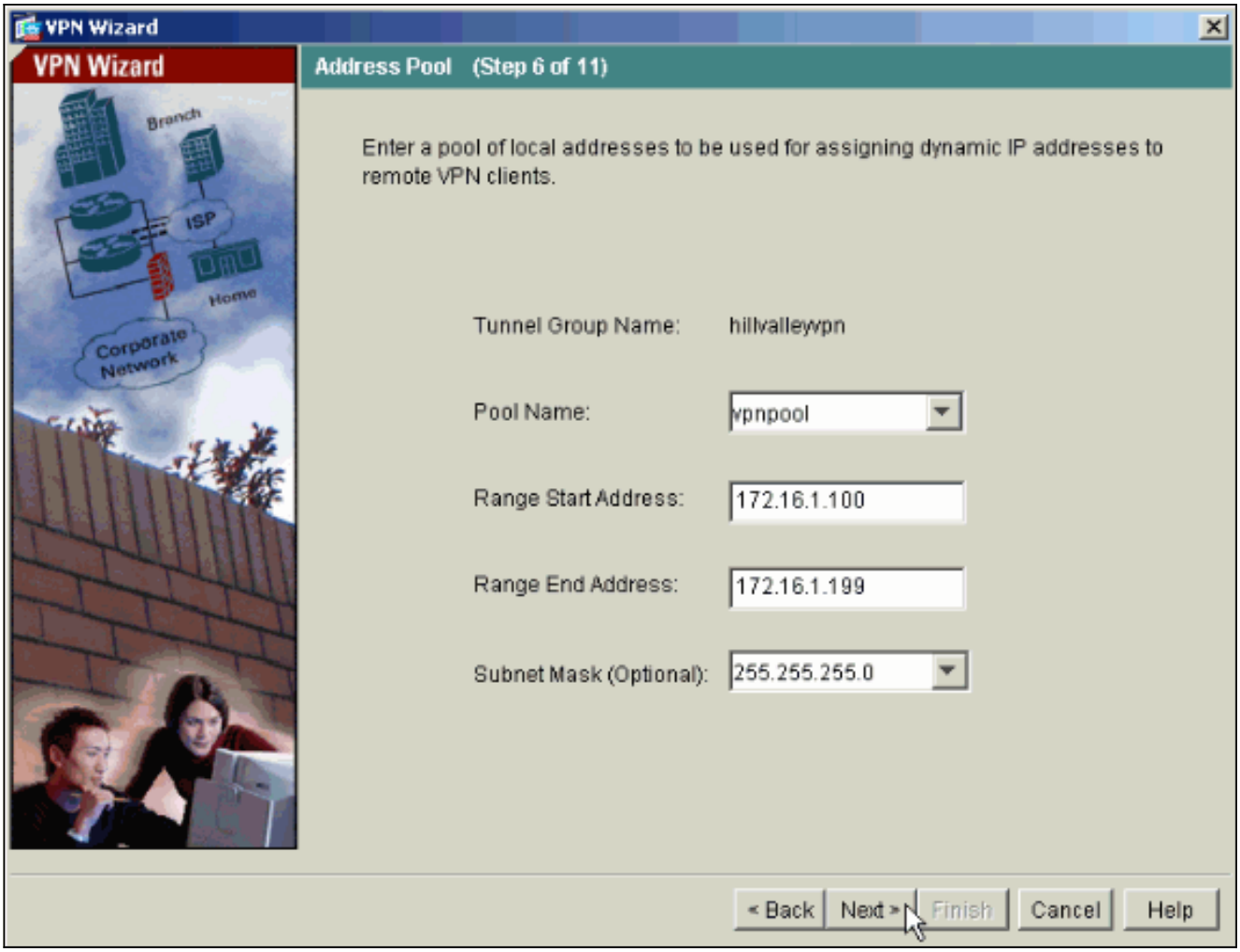


6. 필요한 경우 로컬 데이터베이스에 사용자를 추가합니다.**참고:** 이 창에서 기존 사용자를 제거하지 마십시오.기본 ASDM **창에서 Configuration > Device Administration > Administration > User Accounts를 선택하여** 데이터베이스의 기존 항목을 편집하거나 데이터베이스에서 제거합니다

.

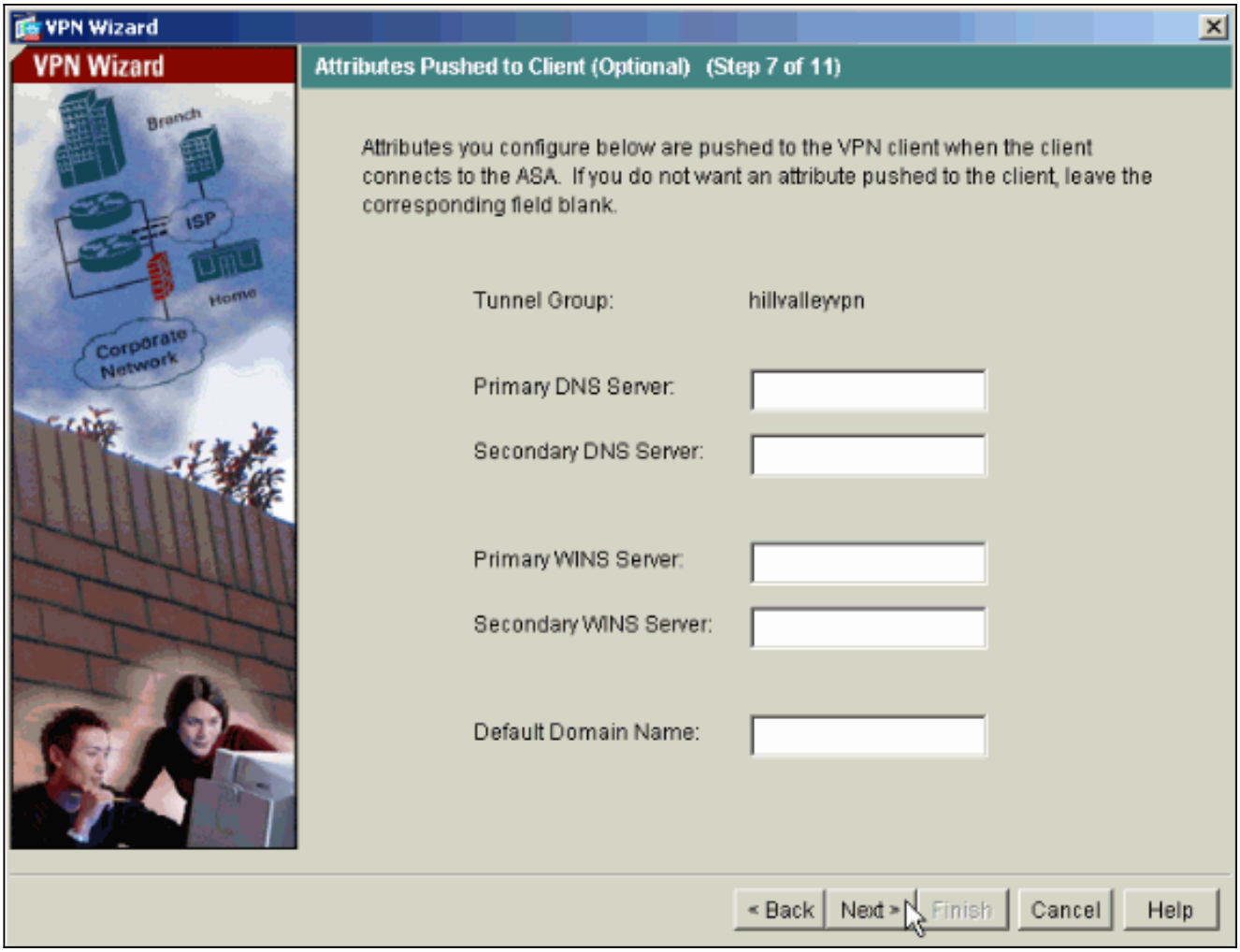


7. 연결할 때 원격 VPN 클라이언트에 동적으로 할당할 로컬 주소 풀을 정의합니다
.

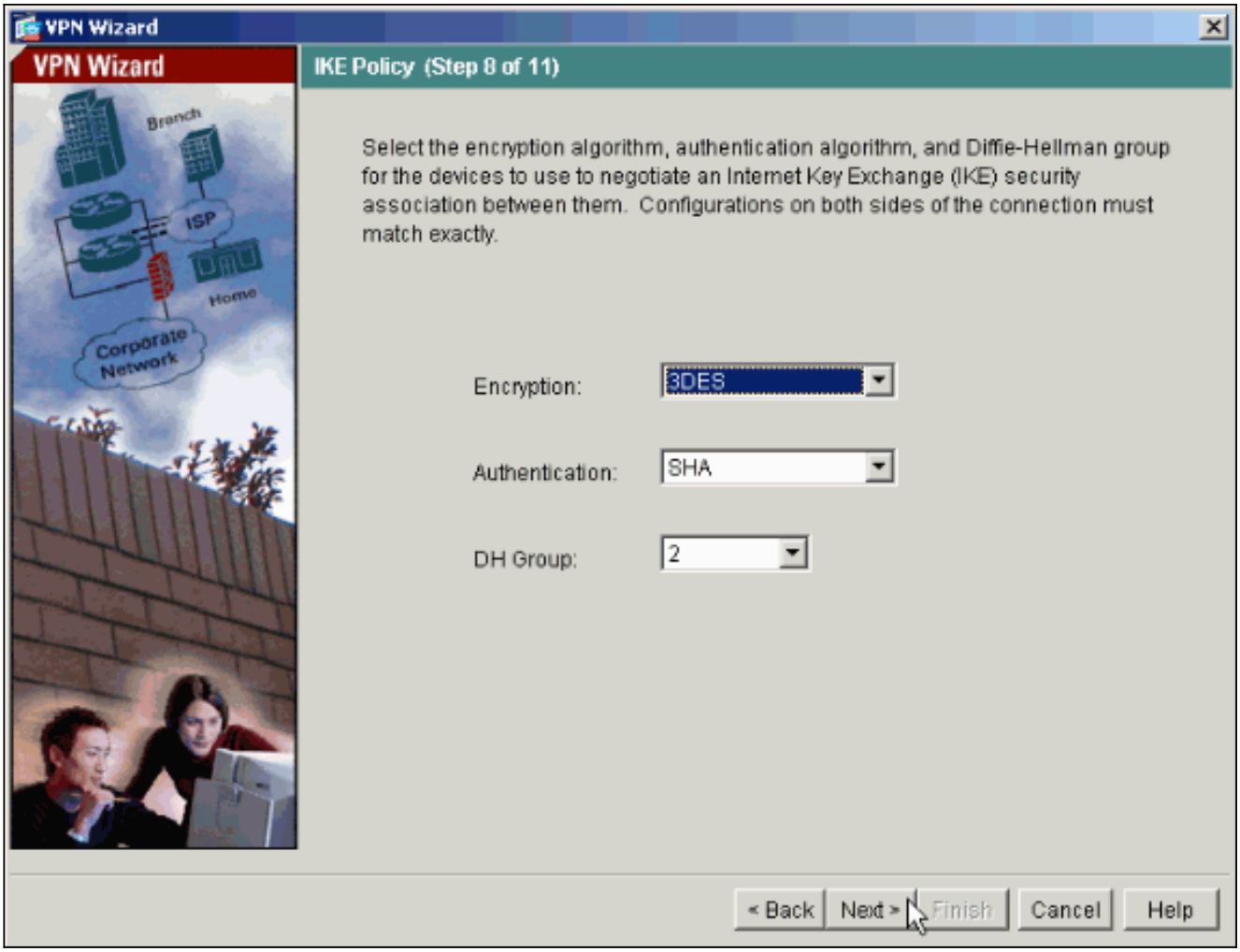


8. *선택 사항:*원격 VPN 클라이언트에 푸시할 DNS 및 WINS 서버 정보 및 기본 도메인 이름을 지정합니다

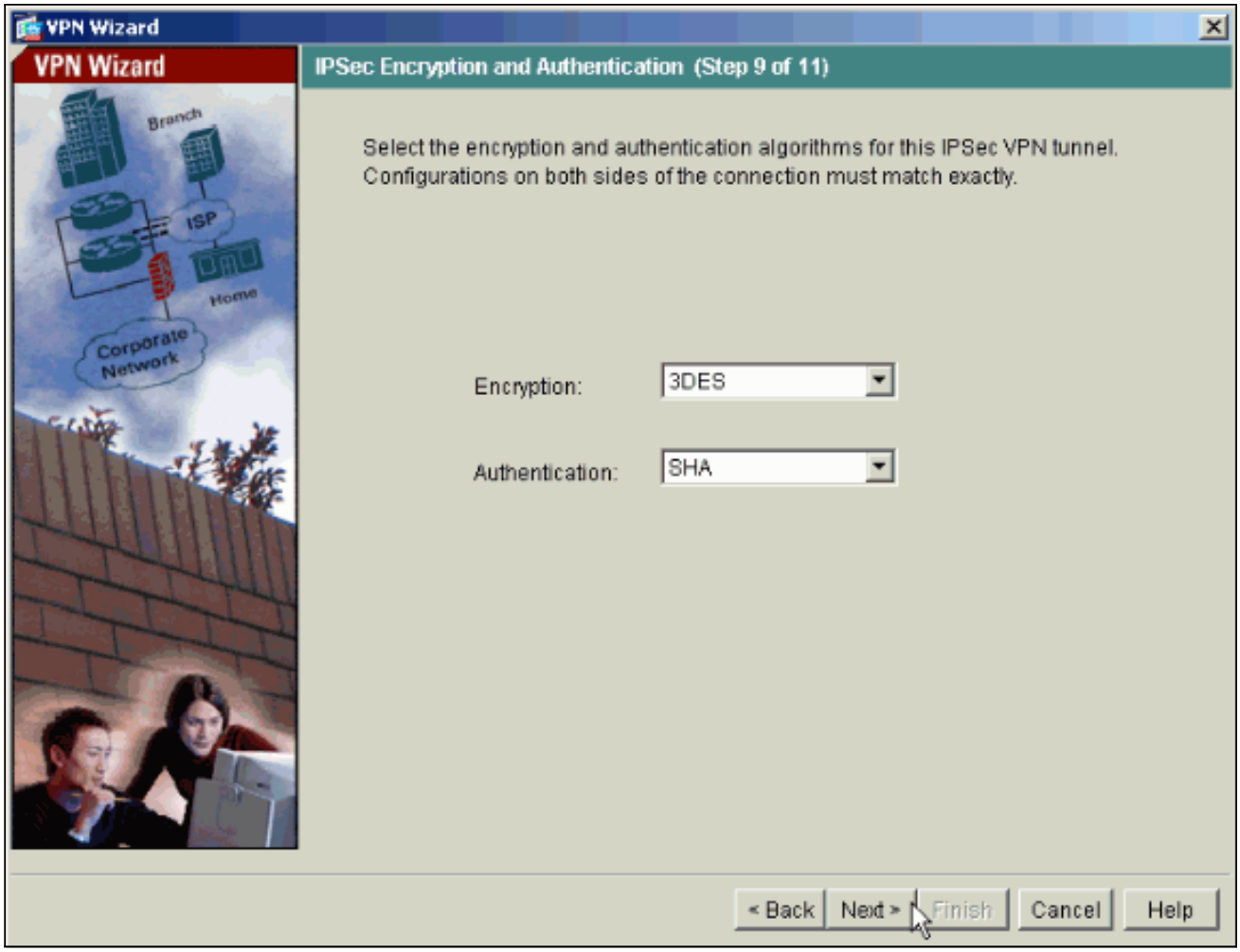
.



9. IKE 1단계라고도 하는 IKE의 매개변수를 지정합니다.터널의 양쪽에 있는 컨피그레이션은 정확히 일치해야 합니다.그러나 Cisco VPN Client는 자동으로 자신에게 적합한 컨피그레이션을 선택합니다.따라서 클라이언트 PC에는 IKE 컨피그레이션이 필요하지 않습니다
.

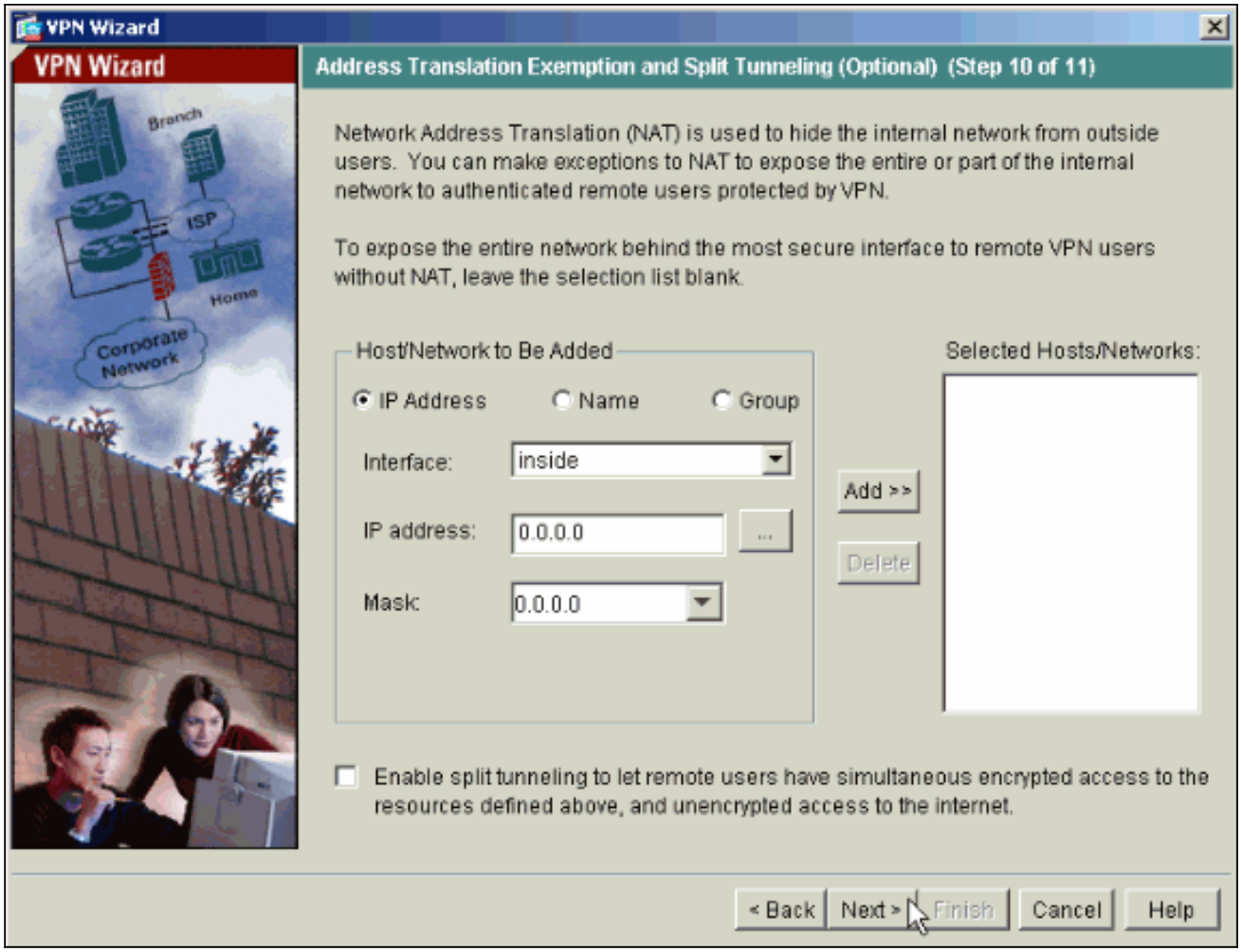


10. IKE Phase 2라고도 하는 IPSec의 매개변수를 지정합니다.터널의 양쪽에 있는 컨피그레이션은 정확히 일치해야 합니다.그러나 Cisco VPN Client는 자동으로 자신에게 적합한 컨피그레이션을 선택합니다.따라서 클라이언트 PC에는 IKE 컨피그레이션이 필요하지 않습니다
.

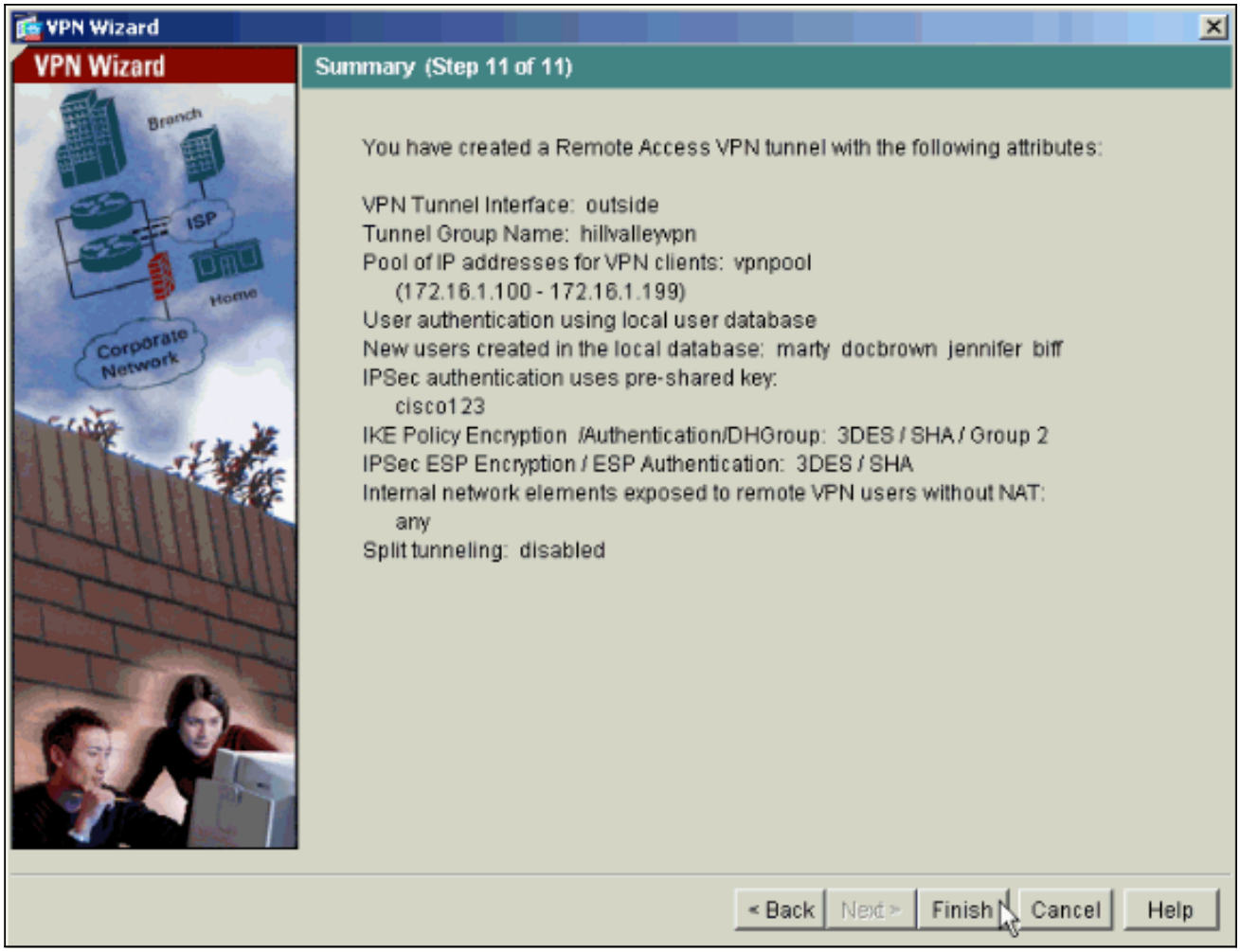


11. 내부 호스트 또는 네트워크가 원격 VPN 사용자에게 노출되어야 하는 경우 지정합니다.이 목록을 비워 두면 원격 VPN 사용자가 ASA의 전체 내부 네트워크에 액세스할 수 있습니다.이 창에서 스플릿 터널링을 활성화할 수도 있습니다.스플릿 터널링은 이 절차의 앞부분에서 정의한 리소스로 트래픽을 암호화하고 해당 트래픽을 터널링하지 않음으로써 인터넷에 대한 암호화되지 않은 액세스를 제공합니다.스플릿 터널링이 *활성화되지 않으면* 원격 VPN 사용자의 모든 트래픽이 ASA로 터널링됩니다.이는 컨피그레이션에 따라 대역폭과 프로세서 집약적인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

.



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



CLI를 사용하여 ASA/PIX를 원격 VPN 서버로 구성

명령줄에서 원격 VPN 액세스 서버를 구성하려면 다음 단계를 완료합니다.사용되는 각 명령에 대한 자세한 내용은 원격 액세스 VPN 구성 또는 Cisco ASA 5500 Series Adaptive Security Appliances-Command Reference를 참조하십시오.

1. VPN 원격 액세스 터널에 사용할 IP 주소 풀을 구성하려면 전역 컨피그레이션 모드에서 **ip local pool** 명령을 입력합니다.주소 풀을 삭제하려면 이 명령의 no 형식을 입력합니다.보안 어플라이언스는 연결에 터널 그룹을 기반으로 주소 풀을 사용합니다.터널 그룹에 대해 둘 이상의 주소 풀을 구성할 경우 보안 어플라이언스는 구성된 순서대로 주소 풀을 사용합니다.원격 액세스 VPN 클라이언트에 동적 주소를 할당하는 데 사용할 수 있는 로컬 주소 풀을 생성하려면 이 명령을 실행합니다.
```
ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
  255.255.255.0
```

2. 다음 명령을 실행합니다.
```
ASA-AIP-CLI(config)#username marty password 12345678
```

3. 특정 터널을 구성하려면 다음 명령 집합을 실행합니다.ASA-AIP-CLI(config)#**isakmp 정책 1 인증 사전 공유**ASA-AIP-CLI(config)#**isakmp policy 1 encryption 3des**ASA-AIP-CLI(config)#**isakmp policy 1 hash sha**ASA-AIP-CLI(config)#**isakmp policy 1 group 2**ASA-AIP-CLI(config)#**isakmp policy 1 lifetime 43200**ASA-AIP-CLI(config)#**isakmp 외부에서 활성화**ASA-AIP-CLI(config)#**crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHA**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set reverse-route**

설정ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000**ASA-AIP-CLI(config)#**crypto map outside_map 10 ipsec-isakmp dynamic outside_dyn_map**ASA-AIP-CLI(config)#**crypto map outside_map 인터페이스 외부**
ASA-AIP-CLI(config)#**crypto isakmp nat-traversal**

4. *선택 사항:*연결에 인터페이스에 적용되는 액세스 목록을 우회하려면 다음 명령을 실행합니다.
   ASA-AIP-CLI(config)#**sysopt connection permit-ipsec**

   참고: 이 명령은 7.2(2) 이전의 7.x 이미지에서 작동합니다. image 7.2(2)를 사용하는 경우 ASA-AIP-CLI(config)#sysopt connection permit-vpn 명령을 실행합니다.
5. 다음 명령을 실행합니다.
   ASA-AIP-CLI(config)#**group-policy hillvalleyvpn internal**

6. 클라이언트 연결 설정을 구성하려면 다음 명령을 실행합니다.ASA-AIP-CLI(config)#**group-policy hilllevpn 특성**ASA-AIP-CLI(config)#(config-group-policy)#**dns-server 값 172.16.1.11**ASA-AIP-CLI(config)#(config-group-policy)#**vpn-tunnel-protocol IPSec**ASA-AIP-CLI(config)#(config-group-policy)#**default-domain value test.com**
7. 다음 명령을 실행합니다.
   ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-ra**

8. 다음 명령을 실행합니다.
   ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-attributes**

9. 다음 명령을 실행합니다.
   ASA-AIP-CLI(config-tunnel-ipsec)#**pre-shared-key cisco123**

10. 다음 명령을 실행합니다.
    ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn general-attributes**

11. 인증을 위해 로컬 사용자 데이터베이스를 참조하려면 이 명령을 실행합니다.
    ASA-AIP-CLI(config-tunnel-general)#**authentication-server-group LOCAL**

12. 그룹 정책을 터널 그룹과 연결
    ASA-AIP-CLI(config-tunnel-ipsec)# **default-group-policy hillvalleyvpn**

13. 1단계에서 생성한 vpnpool을 힐vallleyvpn 그룹에 할당하려면, hillleyvpn tunnel-group의 general-attributes 모드에서 이 명령을 실행합니다.
    ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

ASA 디바이스에서 컨피그레이션 실행

```
ASA-AIP-CLI(config)#show running-config
ASA Version 7.2(2)
!
hostname ASAwAIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
!
```

```
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
pager lines 24
mtu outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
 dns-server value 172.16.1.11
 vpn-tunnel-protocol IPSec
 default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
crypto dynamic-map outside_dyn_map 10 set transform-set
ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-
association lifetime seconds 288000
crypto map outside_map 10 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map interface outside
crypto isakmp enable outside
```

```
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
 address-pool vpnpool
 default-group-policy hillvalleyvpn
tunnel-group hillvalleyvpn ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

Cisco VPN 클라이언트 비밀번호 스토리지 컨피그레이션

여러 Cisco VPN 클라이언트가 있는 경우 모든 VPN 클라이언트 사용자 이름과 비밀번호를 기억하기가 매우 어렵습니다.VPN 클라이언트 시스템에 비밀번호를 저장하려면 이 섹션에서 설명하는 대로 ASA/PIX 및 VPN 클라이언트를 구성합니다.

ASA/PIX

글로벌 컨피그레이션 모드에서 **group-policy attributes** 명령을 사용합니다.

```
group-policy VPNusers attributes
  password-storage enable
```

Cisco VPN 클라이언트

.pcf **파일**을 **편집하고** 다음 매개변수를 수정합니다.

```
SaveUserPassword=1
UserPassword=
```

확장 인증 비활성화

터널 그룹 모드에서 PIX/ASA 7.x에서 기본적으로 활성화된 확장 인증을 비활성화하려면 이 명령을 입력합니다.

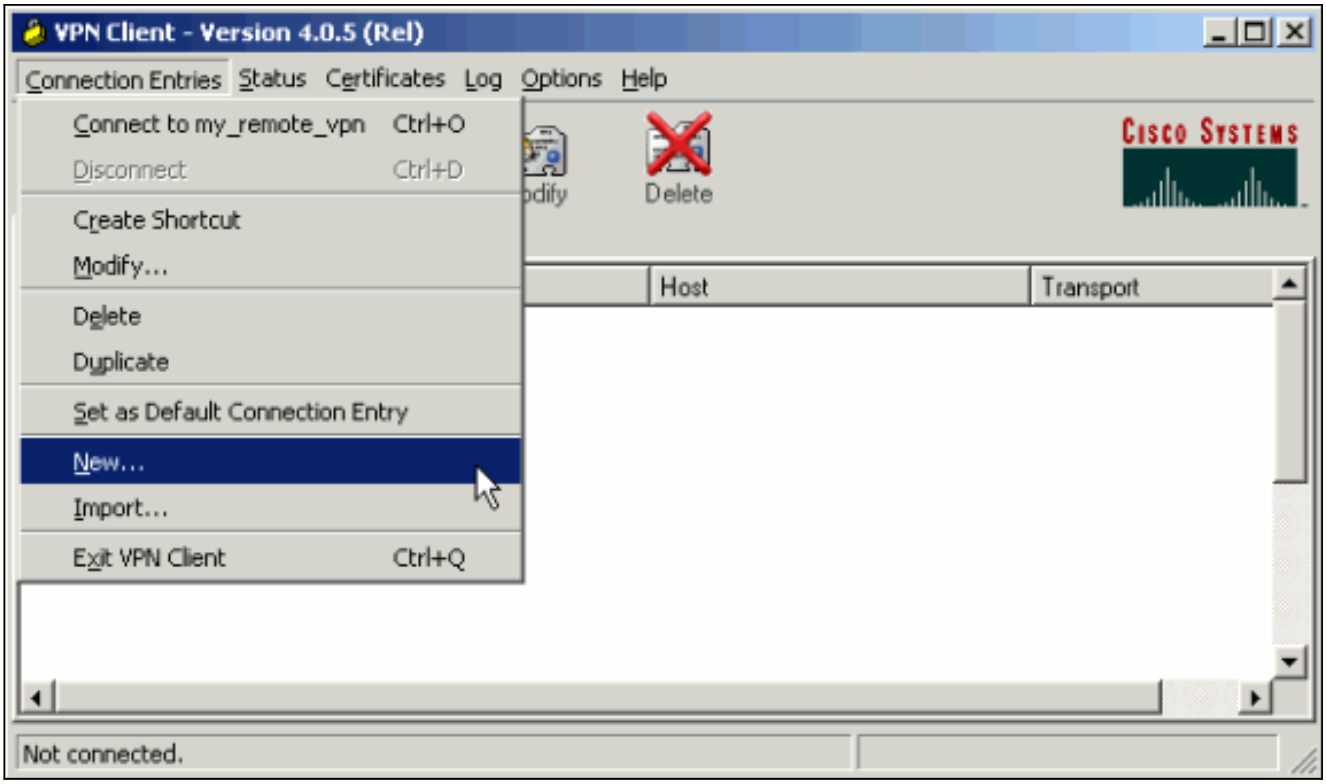
```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

확장 인증을 비활성화한 후 VPN 클라이언트는 인증(Xauth)에 대한 사용자 이름/비밀번호를 팝업하지 않습니다. 따라서 ASA/PIX는 VPN 클라이언트를 인증하기 위해 사용자 이름 및 비밀번호 컨피그레이션이 필요하지 않습니다.

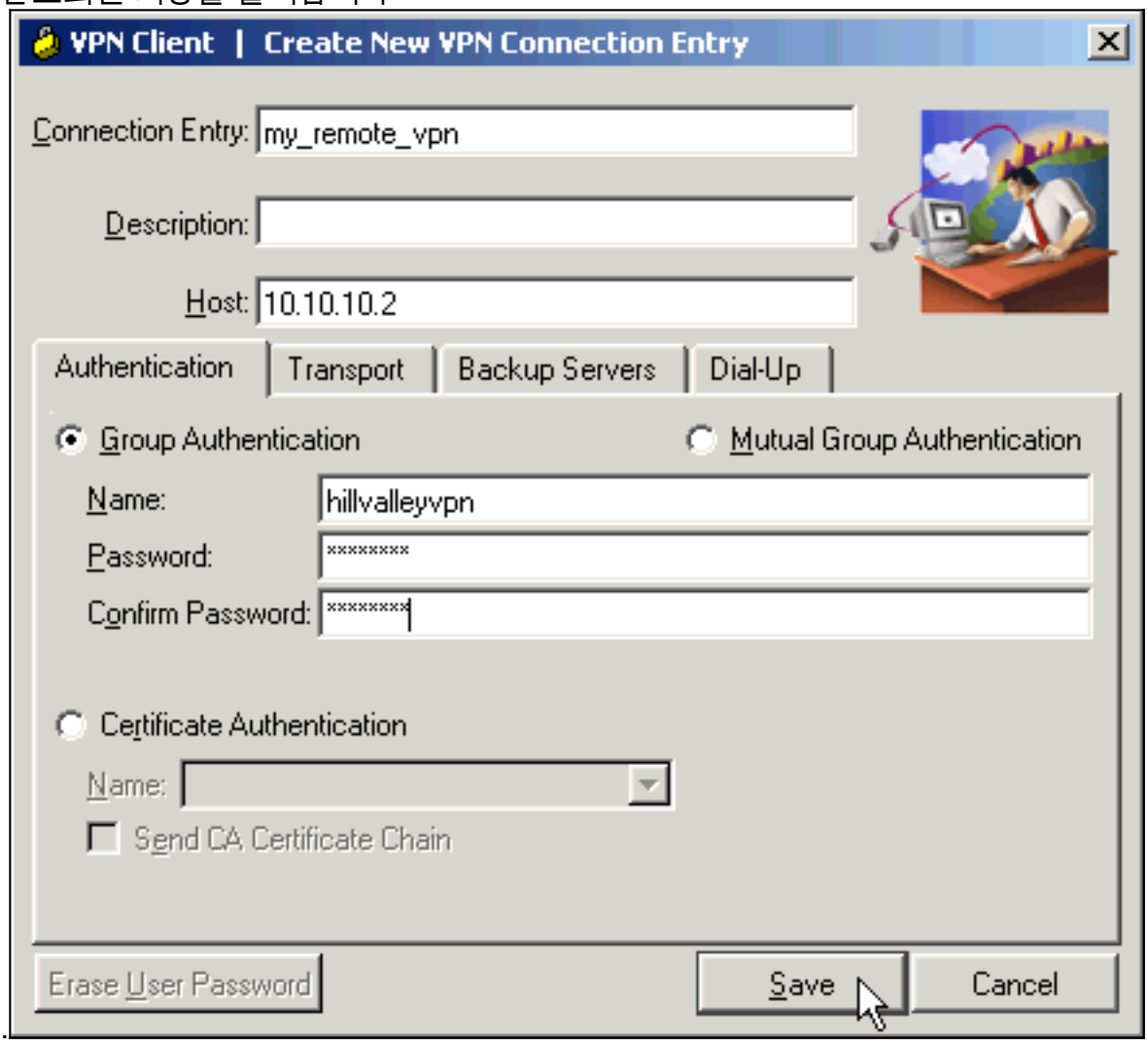
다음을 확인합니다.

ASA가 성공적으로 구성되었는지 확인하기 위해 Cisco VPN Client를 사용하여 Cisco ASA에 연결하려고 시도합니다.

1. Connection **Entries(연결 항목) > New(새로 만들기)를 선택합니다**
   .

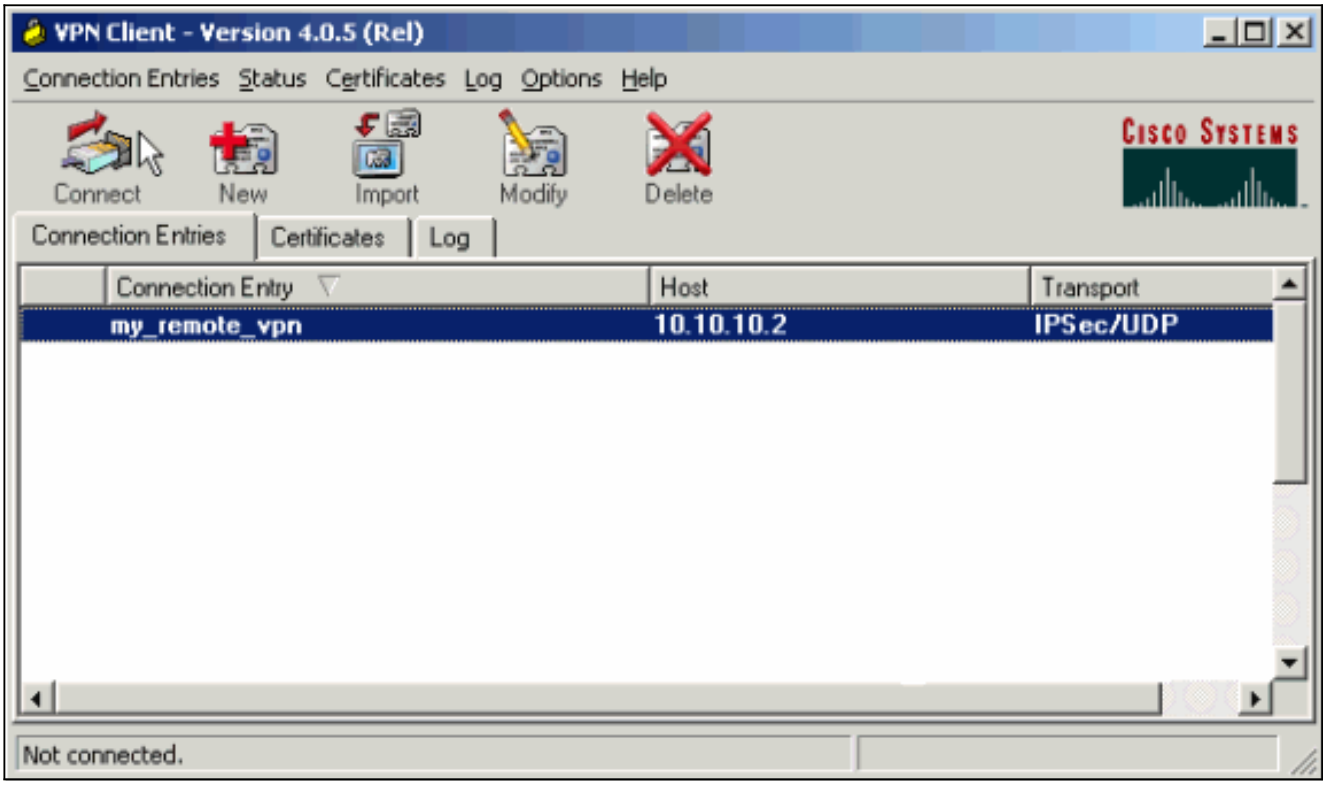


2. 새 연결의 세부 정보를 입력합니다.Host 필드에는 이전에 구성한 Cisco ASA의 IP 주소 또는 호스트 이름이 포함되어야 합니다.그룹 인증 정보는 4단계에서 사용된 것과 일치해야 합니다. 완료되면 저장을 클릭합니다



3. 새로 생성된 연결을 선택하고 **연결**을 클릭합니다

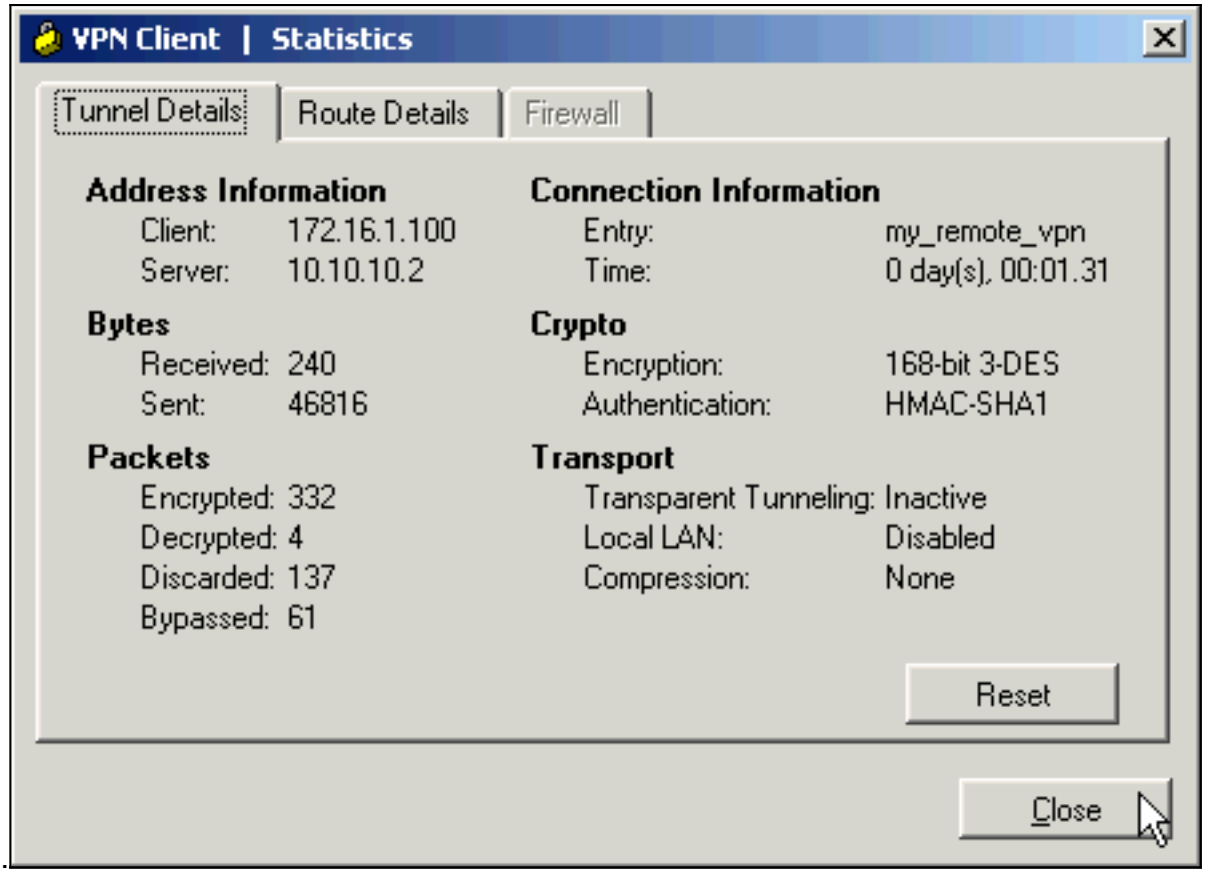
.



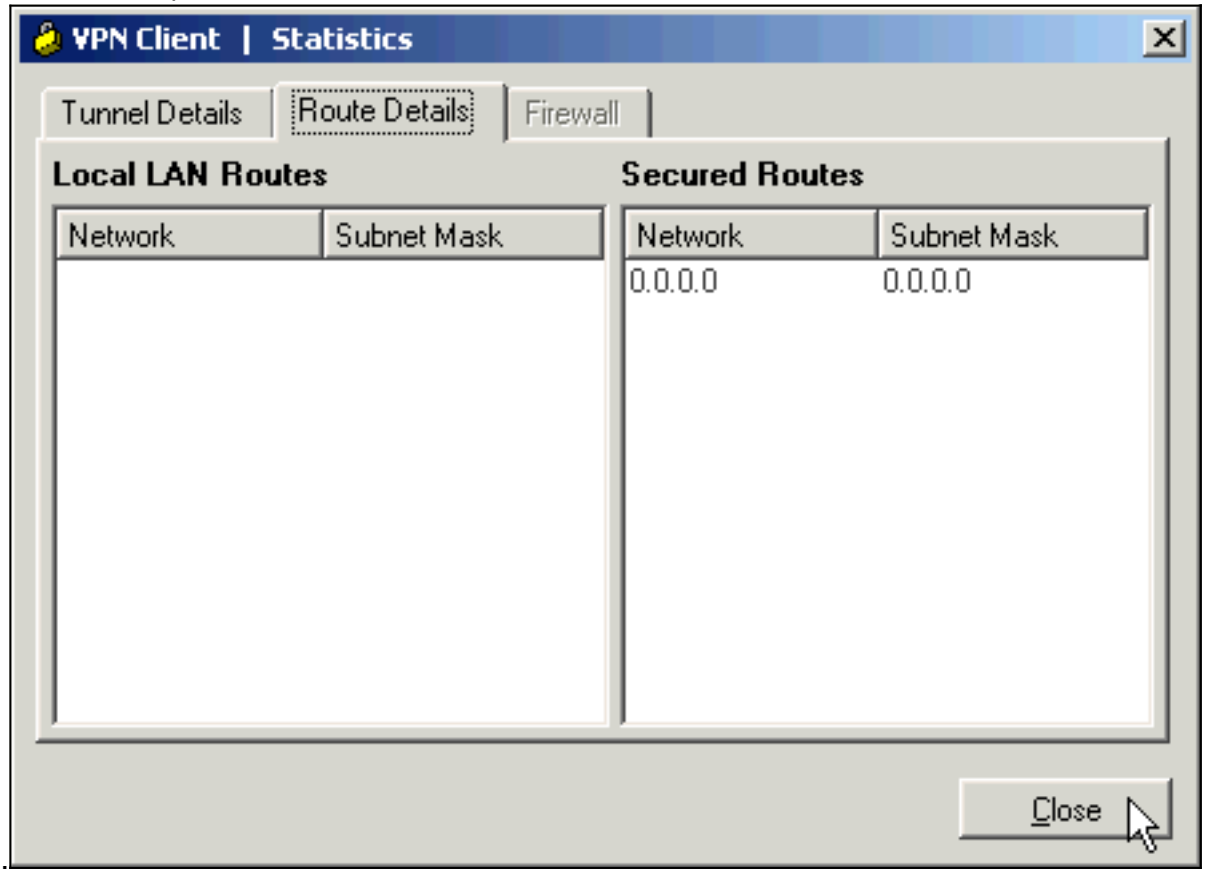
4. 확장 인증을 위한 사용자 이름 및 비밀번호를 입력합니다.이 정보는 5단계 및 6단계에 지정된 것과 일치해야 합니다

.

5. 연결이 성공적으로 설정되면 Status 메뉴에서 Statistics를 선택하여 터널의 세부 정보를 확인합니다.이 창에는 트래픽 및 암호화 정보가 표시됩니다



이 창에는 스플릿 터널링 정보가 표시됩니다



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

잘못된 암호화 ACL

ASDM 5.0(2)은 스플릿 터널링을 사용하는 VPN 클라이언트 및 네트워크 확장 모드의 하드웨어 클라이언트에 문제를 일으킬 수 있는 암호화 ACL(Access Control List)을 생성하고 적용하는 것으로 알려져 있습니다.이 문제를 방지하려면 ASDM 버전 5.0(4.3) 이상을 사용하십시오.자세한 내용은 Cisco 버그 ID CSCsc10806(등록된 고객만 해당)을 참조하십시오.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- 가장 일반적인 L2L 및 원격 액세스 IPsec VPN 문제 해결 솔루션
- Cisco ASA 5500 Series Adaptive Security Appliances 트러블슈팅 및 알림
- 기술 지원 및 문서 – Cisco Systems