사전 공유 키를 사용하여 Windows 8 PC와 ASA 간에 L2TP Over IPsec 구성

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)와 Windows 8 네이티브 클라이언트 간에 사전 공유 키를 사용하여 IPsec을 통해 L2TP(Layer 2 Tunneling Protocol)를 구성하는 방법에 대해 설명합니다.

L2TP over Internet Protocol Security(IPsec)는 단일 플랫폼에서 IPsec VPN 및 방화벽 서비스와 함께 L2TP VPN(Virtual Private Network) 솔루션을 구축하고 관리하는 기능을 제공합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 클라이언트 시스템에서 ASA로의 IP 연결연결을 테스트하려면 클라이언트 엔드포인트에서 ASA의 IP 주소를 ping하거나 그 반대로 ping을 시도합니다
- UDP 포트 500 및 4500 및 ESP(Encapsulating Security Payload) 프로토콜이 연결 경로를 따라 어느 곳에서도 차단되지 않는지 확인합니다.

제한 사항

- L2TP over IPsec은 IKEv1만 지원합니다. IKEv2는 지원되지 않습니다.
- ASA에서 IPsec이 포함된 L2TP를 사용하면 LNS가 Windows, MAC OS X, Android 및 Cisco IOS와 같은 운영 체제에 통합된 네이티브 VPN 클라이언트와 상호 운용될 수 있습니다.IPsec이 있는 L2TP만 지원되며 네이티브 L2TP 자체는 ASA에서 지원되지 않습니다.
- Windows 클라이언트에서 지원되는 최소 IPsec 보안 연결 수명은 300초입니다.ASA의 수명이 300초 미만으로 설정된 경우 Windows 클라이언트가 이를 무시하고 300초 수명으로 대체합니다.
- ASA는 로컬 데이터베이스에서 PPP(Point-to-Point Protocol) 인증 PAP(Password Authentication Protocol) 및 Microsoft CHAP(Challenge-Handshake Authentication Protocol) 버전 1 및 2만 지원합니다.EAP(Extensible Authentication Protocol) 및 CHAP는 프록시 인증 서버에서 수행됩니다.따라서 원격 사용자가 **authentication eap-proxy** 또는 **인증 chap** 명령으로 구성된 터널 그룹에 속하고 ASA가 로컬 데이터베이스를 사용하도록 구성된 경우 해당 사용자는 연결할 수 없습니다.

지원되는 PPP 인증 유형

ASA의 L2TP over IPsec 연결은 표에 표시된 PPP 인증 유형만 지원합니다.

AAA 서버 지원 및 PPP 인증 유형

AAA 서버 유형	지원되는 PPP 인증 유형
로컬	PAP, MSCHAPv1, MSCHAPv2
RADIUS	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy
TACACS+	PAP, CHAP, MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

PPP 인증 유형 특성

키워드	인증 유형	특성
chap	CHAP	서버 챌린지에 대한 응답으로 클라이언트는 일반 텍스트 사용자 이름으로 암호 [challenge plus password]를 반환합니다.이 프로토콜은 PAP보다 안전하지만 데이 암호화하지 않습니다.
eap-프록시	EAP	보안 어플라이언스가 외부 RADIUS 인증 서버에 PPP 인증 프로세스를 프록시하도 용하는 EAP를 활성화합니다.
ms chap-v1	Microsoft CHAP, 버전 1	CHAP와 비슷하지만 CHAP에서와 같이 일반 텍스트 비밀번호가 아닌 암호화된 비 호만 서버에서 저장하고 비교한다는 점에서 더 안전합니다.이 프로토콜은 MPPE에
ms chap-v2	Microsoft CHAP, 버전, 2	데이터 암호화에 대한 키도 생성합니다.
pap	PAP	인증 중에 일반 텍스트 사용자 이름과 비밀번호를 전달하며 안전하지 않습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.4(1)를 실행하는 Cisco 5515 Series ASA
- L2TP/IPSec 클라이언트(Windows 8)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

관련 제품

이 컨피그레이션은 Cisco ASA 5500 Series Security Appliance 8.3(1) 이상에서도 사용할 수 있습니다.

표기 규칙

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

배경 정보

L2TP(Layer 2 Tunneling Protocol)는 원격 클라이언트가 공용 IP 네트워크를 사용하여 사설 기업 네트워크 서버와 안전하게 통신할 수 있도록 하는 VPN 터널링 프로토콜입니다.L2TP는 UDP를 통한 PPP(포트 1701)를 사용하여 데이터를 터널링합니다.

L2TP 프로토콜은 클라이언트/서버 모델을 기반으로 합니다.이 기능은 L2TP LNS(Network Server)와 L2TP LAC(Access Concentrator)로 구분됩니다. LNS는 일반적으로 ASA와 같은 네트워크 게이트웨이에서 실행되며, LAC는 Microsoft Windows, Apple iPhone 또는 Android와 같은 번들로 구성된 L2TP 클라이언트가 포함된 NAS(Dial-up Network Access Server) 또는 엔드포인트 디바이스가 될 수 있습니다.

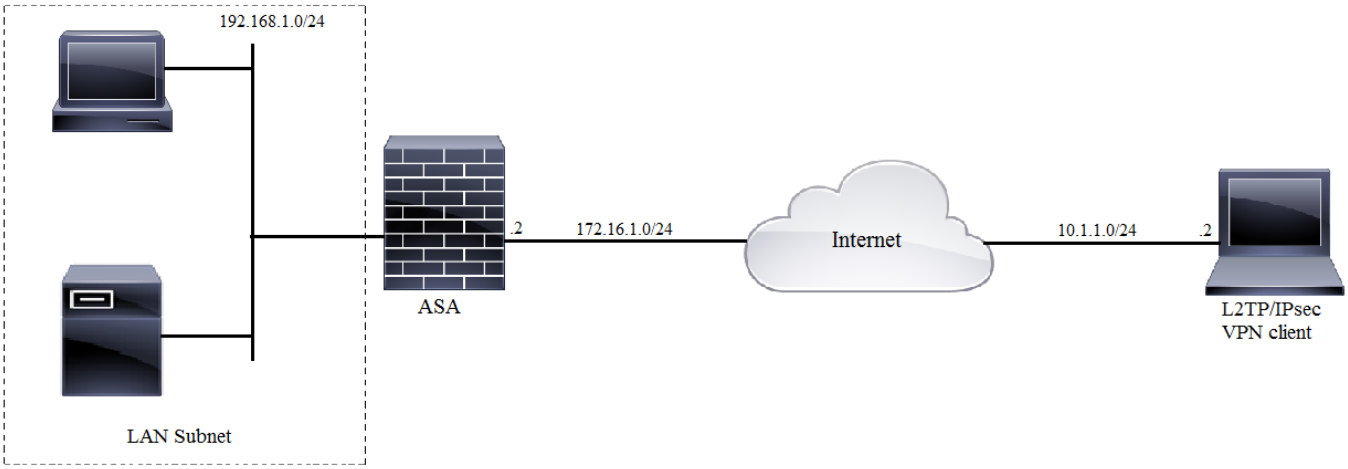
구성

이 섹션에는 이 문서에 설명된 기능을 구성하는 정보가 나와 있습니다.

> **참고:**명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 정보를 찾습니다.

> **참고:**이 컨피그레이션에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

네트워크 다이어그램

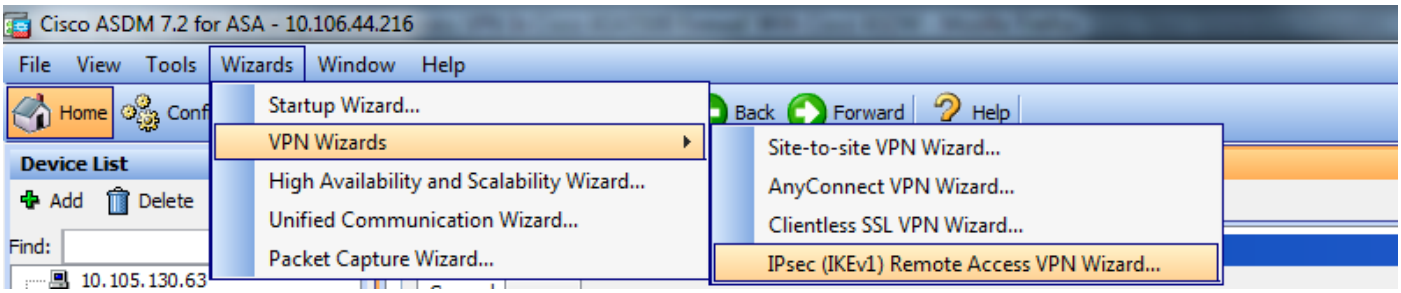


전체 터널 구성

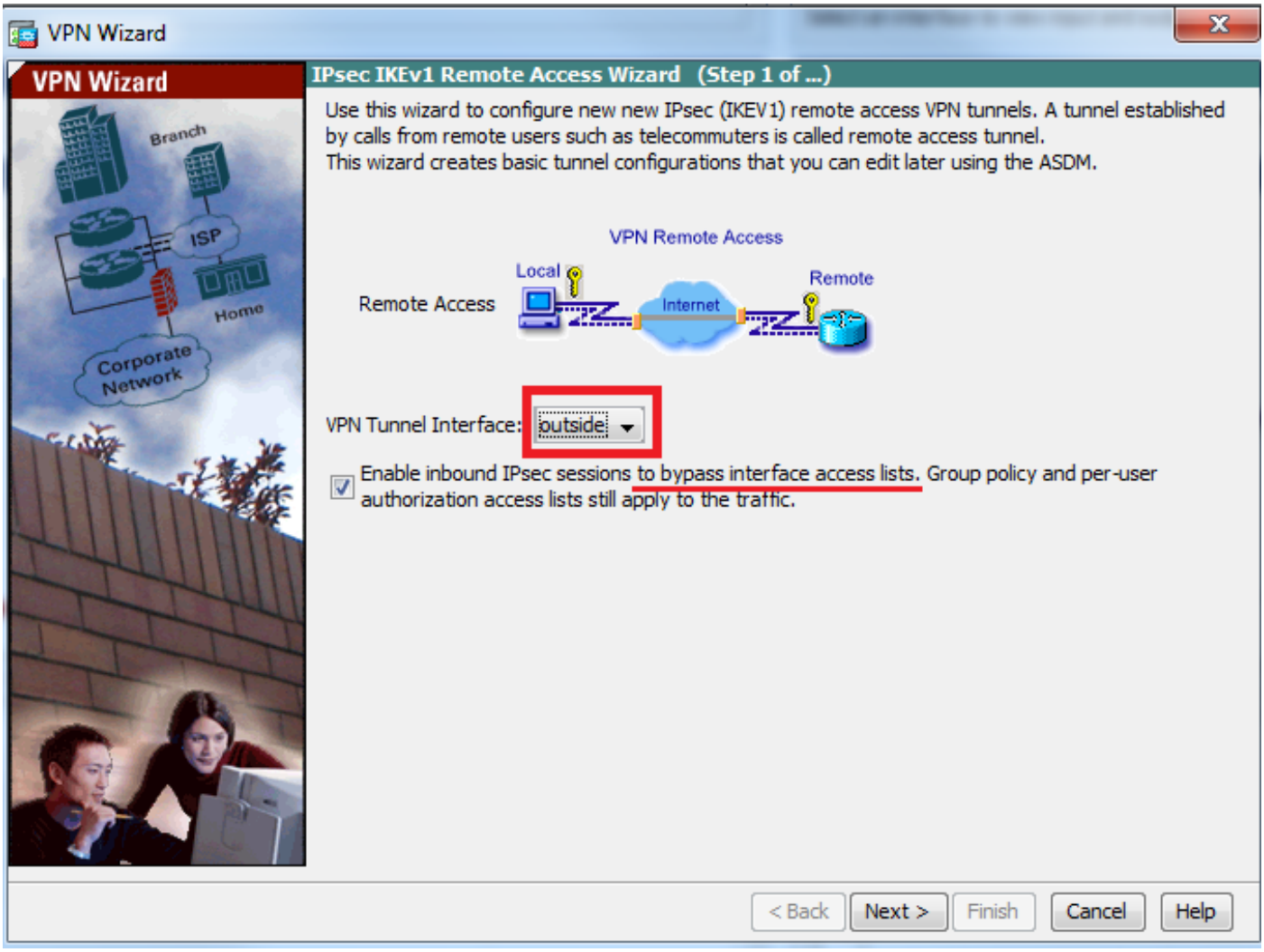
ASDM(Adaptive Security Device Manager)을 사용하는 ASA 컨피그레이션

다음 단계를 완료하십시오.

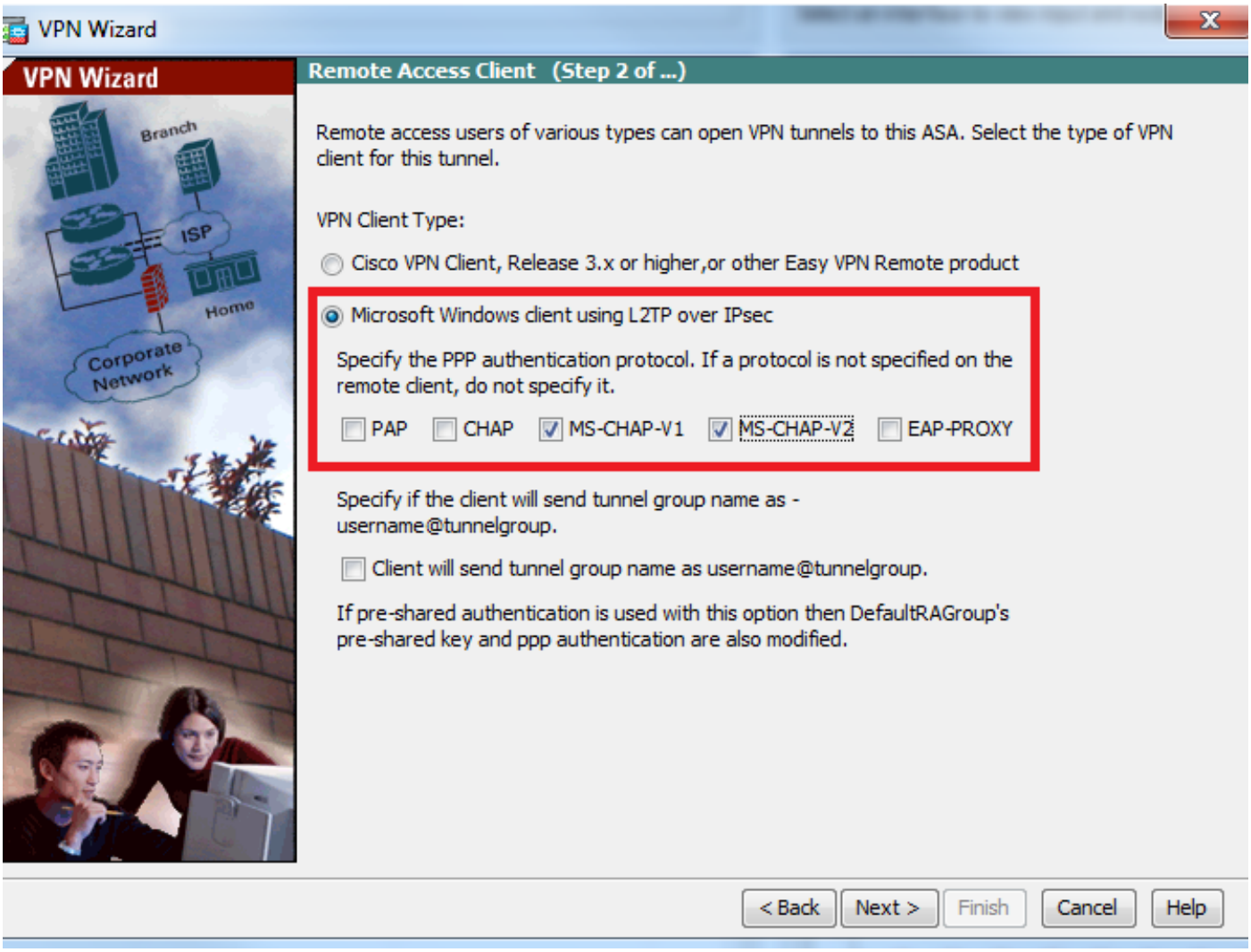
1단계. ASDM에 로그인하고 Wizards(마법사) > **VPN Wizards(VPN 마법사)** > Ipsec(IKEv1) **Remote Access VPN Wizard(IKEv1)(원격 액세스 VPN 마법사)로** 이동합니다.



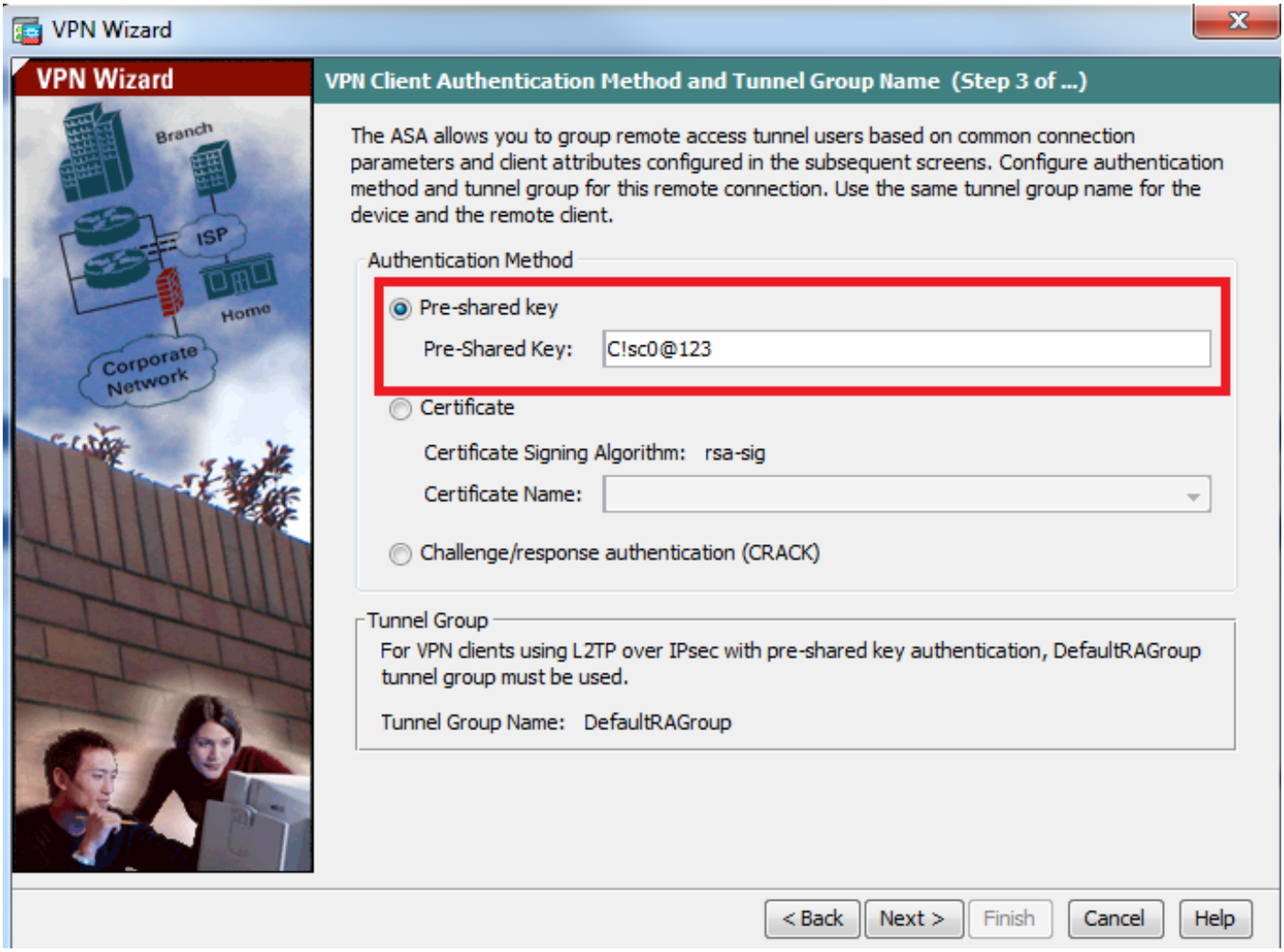
2단계. Remote Access VPN 설정 창이 나타납니다.드롭다운 목록에서 VPN 터널을 종료해야 하는 인터페이스를 선택합니다.이 예에서는 외부 인터페이스가 WAN에 연결되므로 이 인터페이스에서 VPN 터널을 종료합니다.Enable inbound **IPSec sessions to bypass interface access lists(인터페이스 액세스 목록을 우회하기 위해 인바운드 IPSec 세션 활성화) 상자를 유지합니다.그룹 정책 및 사용자별 권한 부여 액세스 목록은 여전히** 선택된 **트래픽에 적용되므로** 클라이언트가 내부 리소스에 액세스할 수 있도록 외부 인터페이스에서 새 액세스 목록을 구성할 필요가 없습니다.Next(**다음)를 클릭합니다**.



3단계. 이 이미지에 표시된 대로 PAP가 안전하지 않으며 LOCAL 데이터베이스에서 인증 서버로 다른 인증 유형이 지원되지 않으므로 클라이언트 유형을 **L2TP over IPSec** 및 **MS-CHAP-V1** 및 **MS-CHAP-V2**를 PPP 인증 프로토콜로 **사용하여 Microsoft Windows 클라이언트로** 선택합니다.

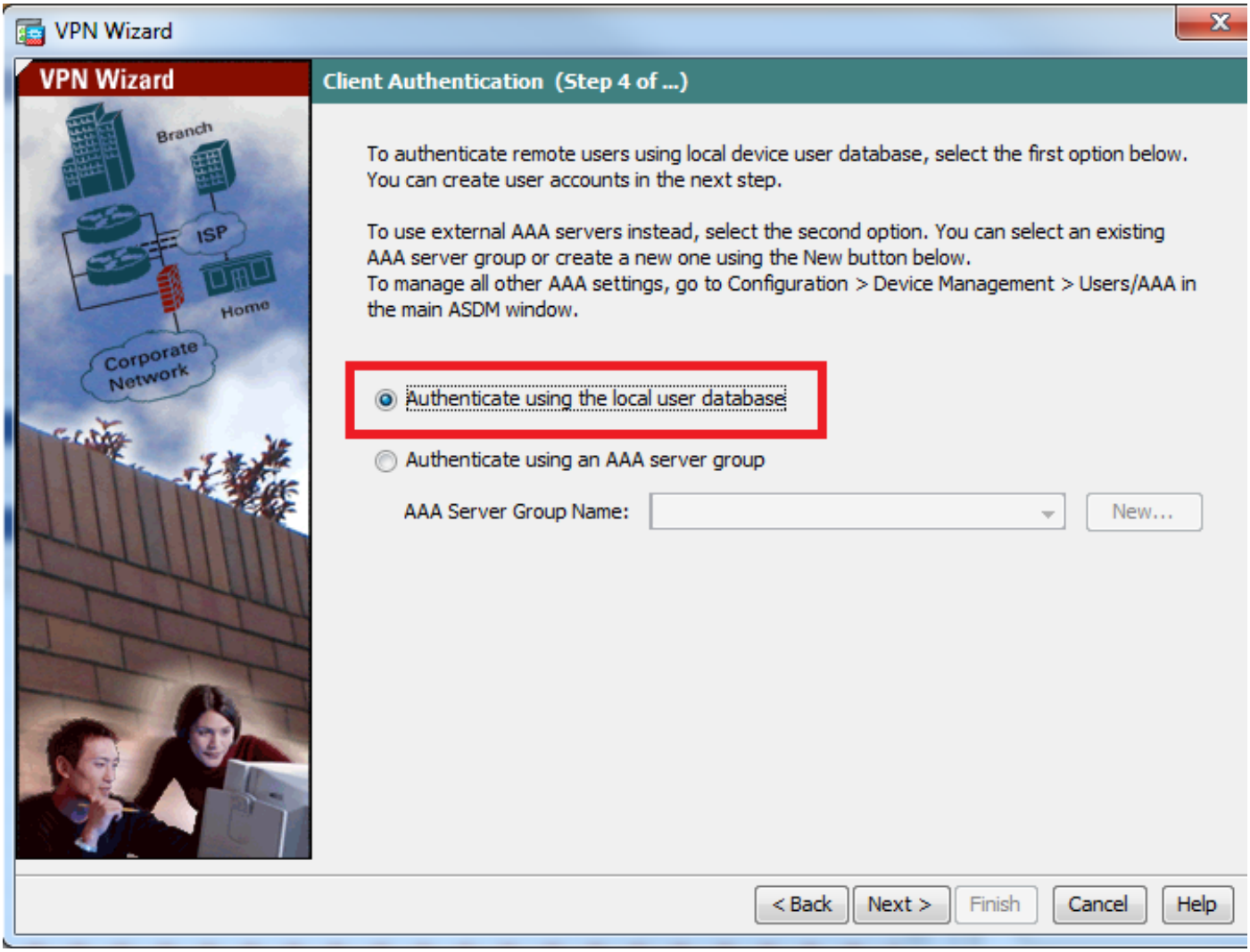


4단계. 인증 방법을 **사전 공유 키로** 선택하고 클라이언트측에서 동일해야 하는 사전 공유 키를 입력한 다음 이 이미지에 표시된 대로 **다음**을 클릭합니다.

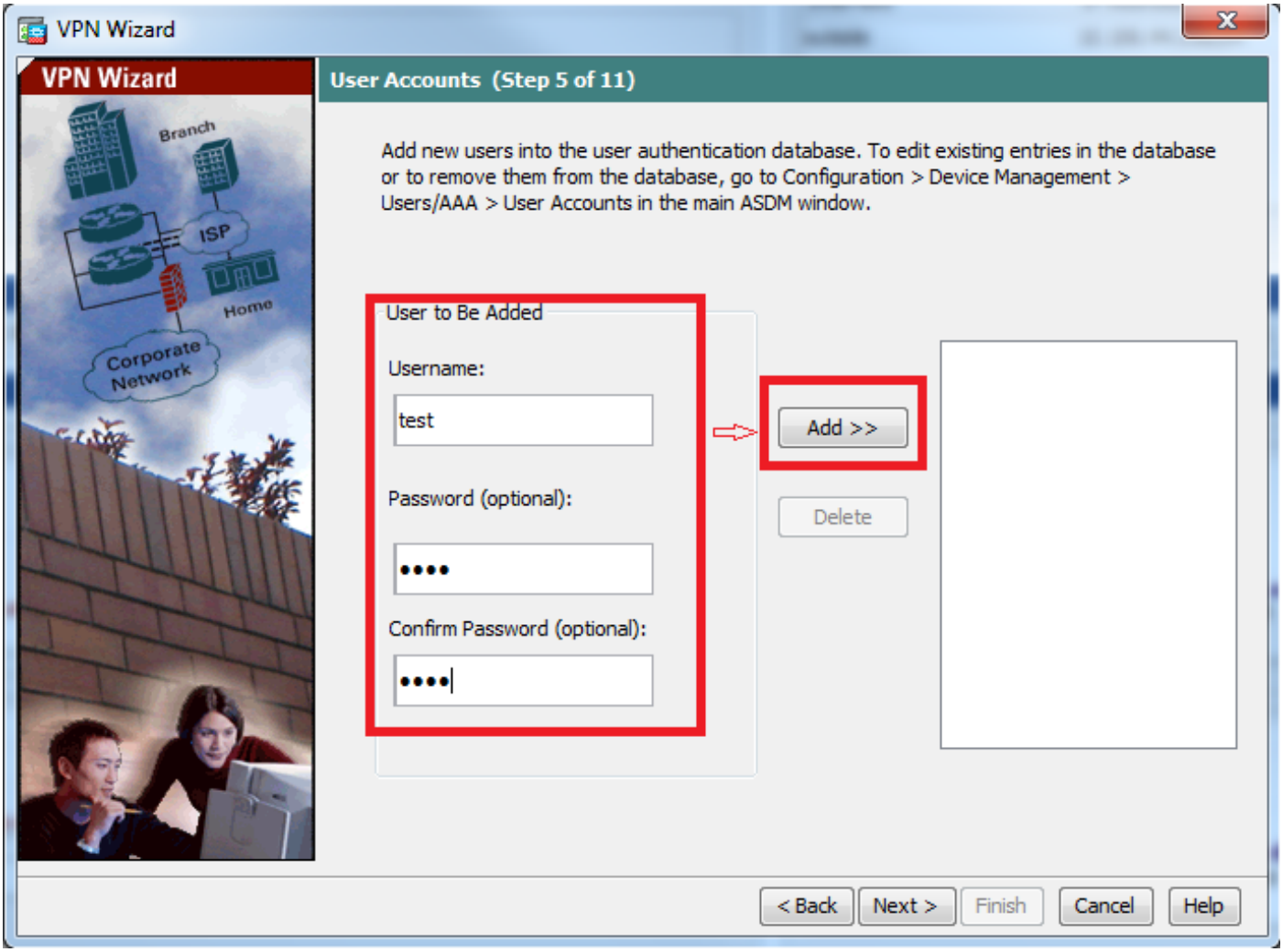


5단계. L2TP over IPsec 연결을 시도하는 사용자를 인증하는 방법을 지정합니다.외부 AAA 인증 서버 또는 자체 로컬 데이터베이스를 사용할 수 있습니다.ASA**의** 로컬 데이터베이스에 대해 클라이언트를 인증하려면 Authenticate using the local user database(**로컬 사용자 데이터베이스**를 사용하여 인증)를 선택하고 Next(다음)를 **클릭합니다.**

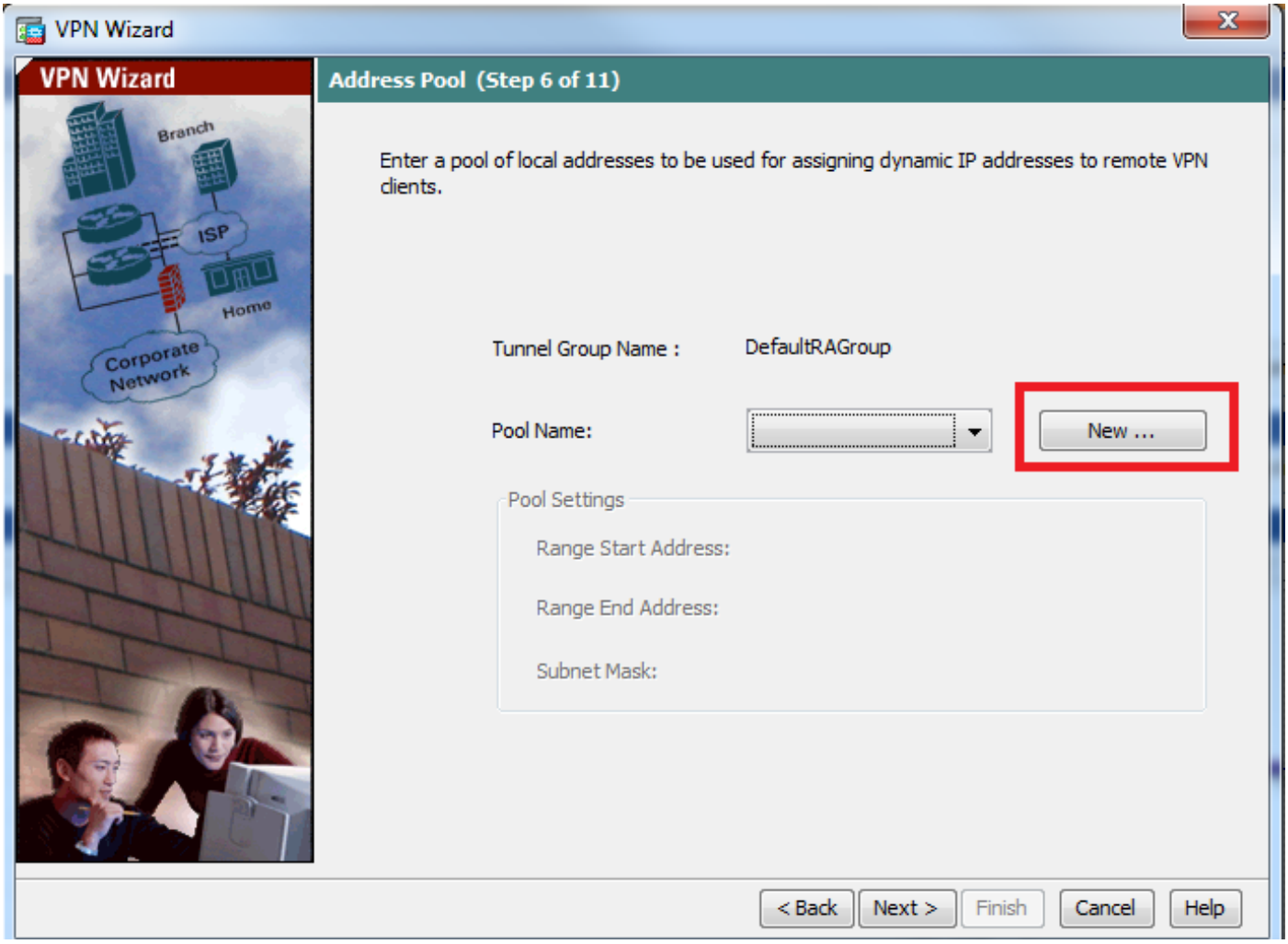
참고:외부 AAA 서버[를](#) 사용하여 사용자를 인증하려면 [VPN 사용자](#)에 대한 RADIUS 인증 구성을 참조하십시오.



6단계. 사용자 인증을 위해 로컬 데이터베이스에 새 사용자를 추가하려면 사용자 이름과 암호를 입력한 다음 **ADD(추가)**를 클릭합니다. 그렇지 않으면 이 이미지에 표시된 대로 데이터베이스의 기존 사용자 계정을 사용할 수 있습니다.Next(**다음)를 클릭합니다.**

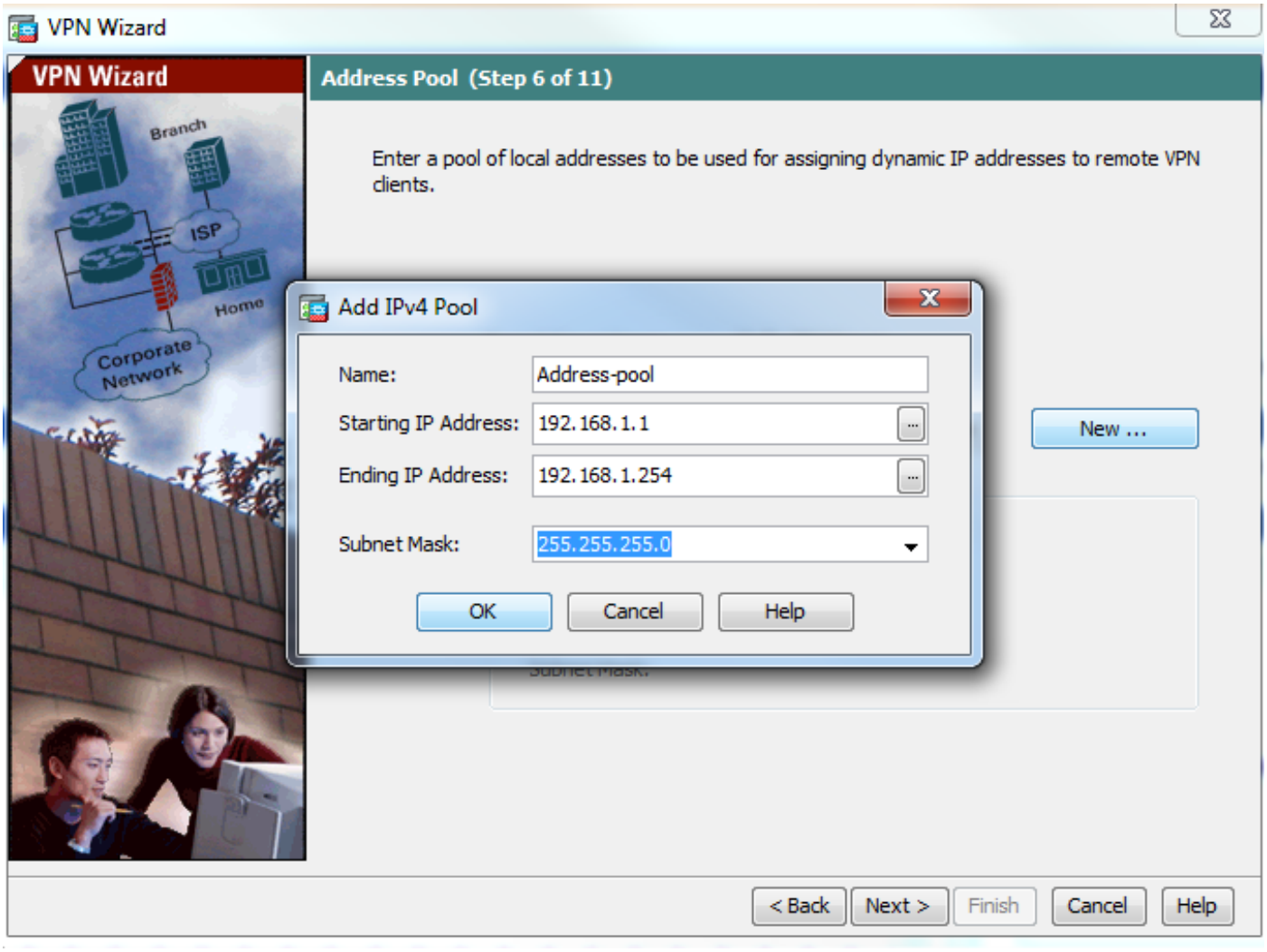


7단계. 드롭다운 목록에서 클라이언트에 IP 주소를 할당하는 데 사용할 주소 풀을 선택합니다.새 주소 풀을 생성하려면 이 이미지에 표시된 대로 New를 클릭합니다.

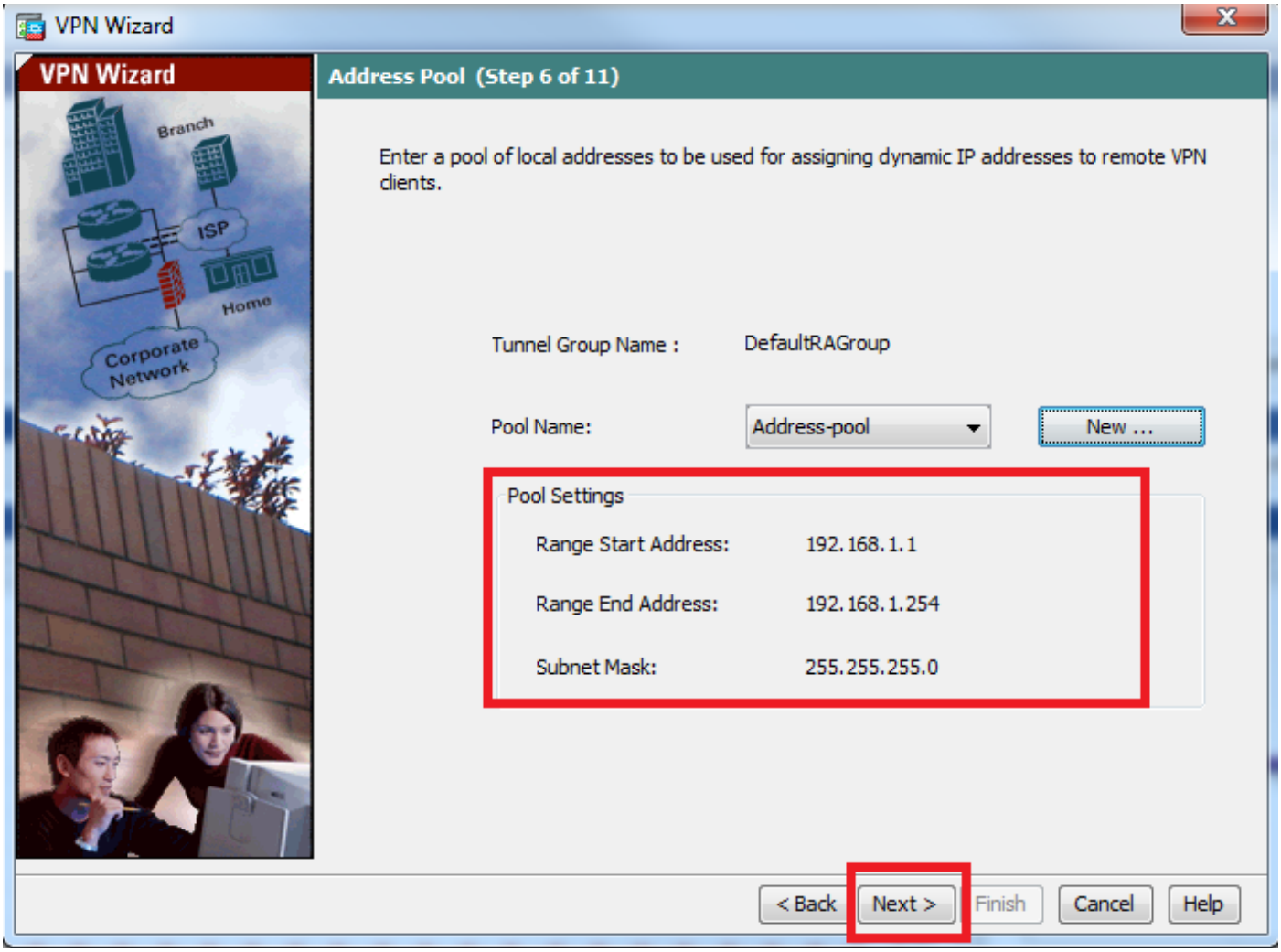


8단계. Add **IPv4 Pool(IPv4 풀 추가)** 대화 상자가 나타납니다.

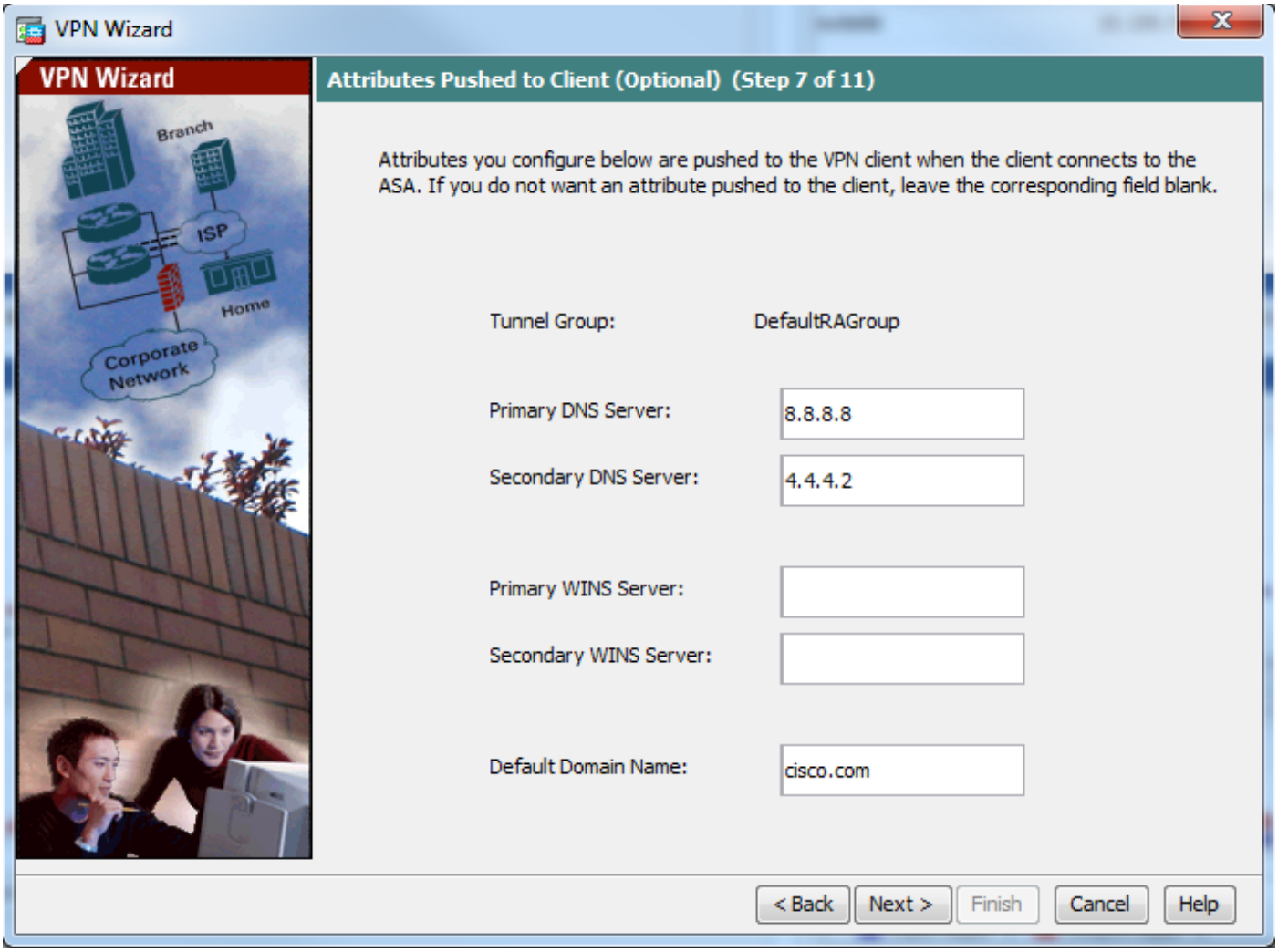
1. 새 IP 주소 풀의 이름을 입력합니다.
2. 시작 및 종료 IP 주소를 입력합니다.
3. 서브넷 마스크를 입력하고 **확인**.



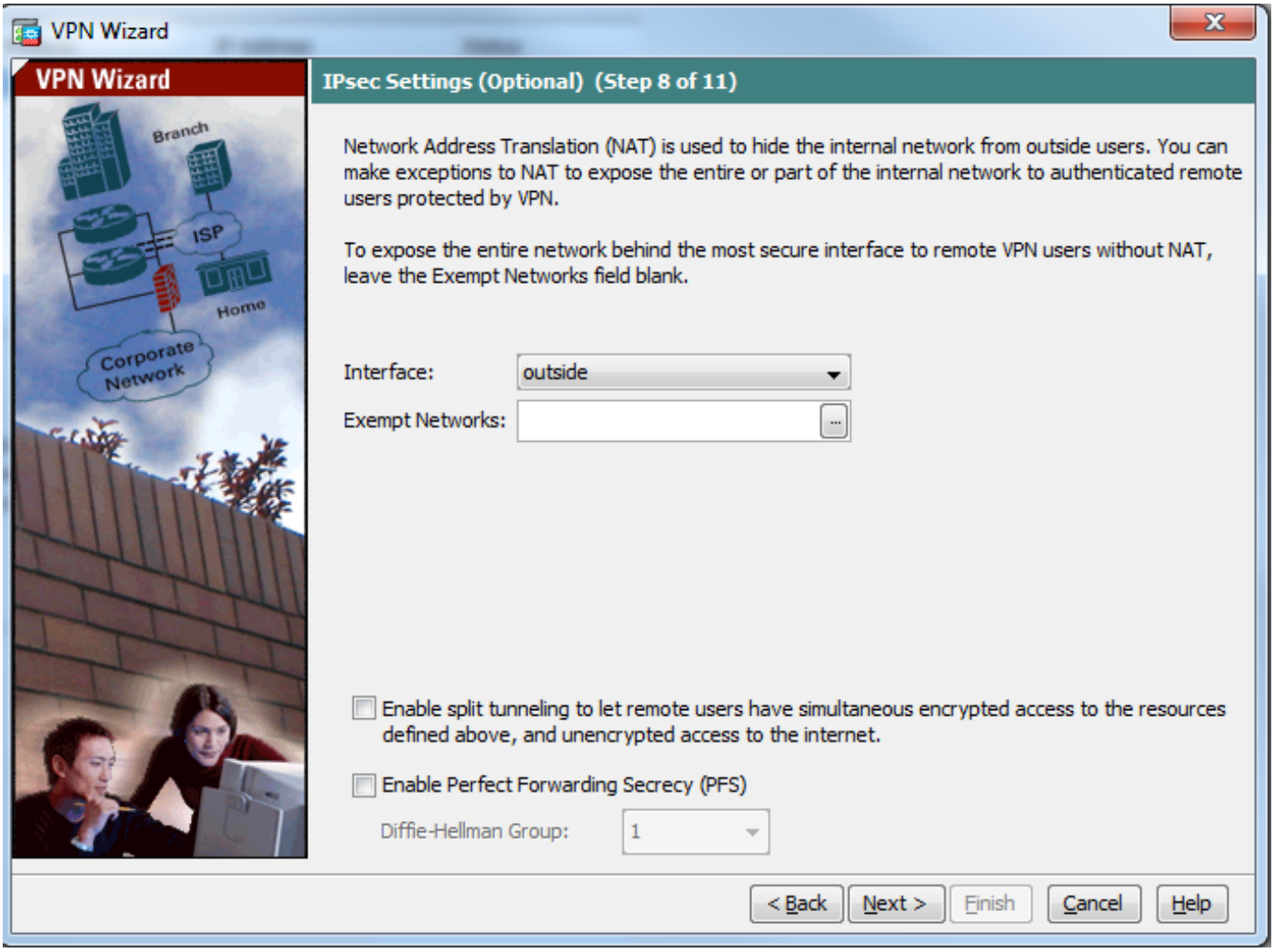
9단계. 풀 설정을 확인하고 **다음**을 클릭합니다.



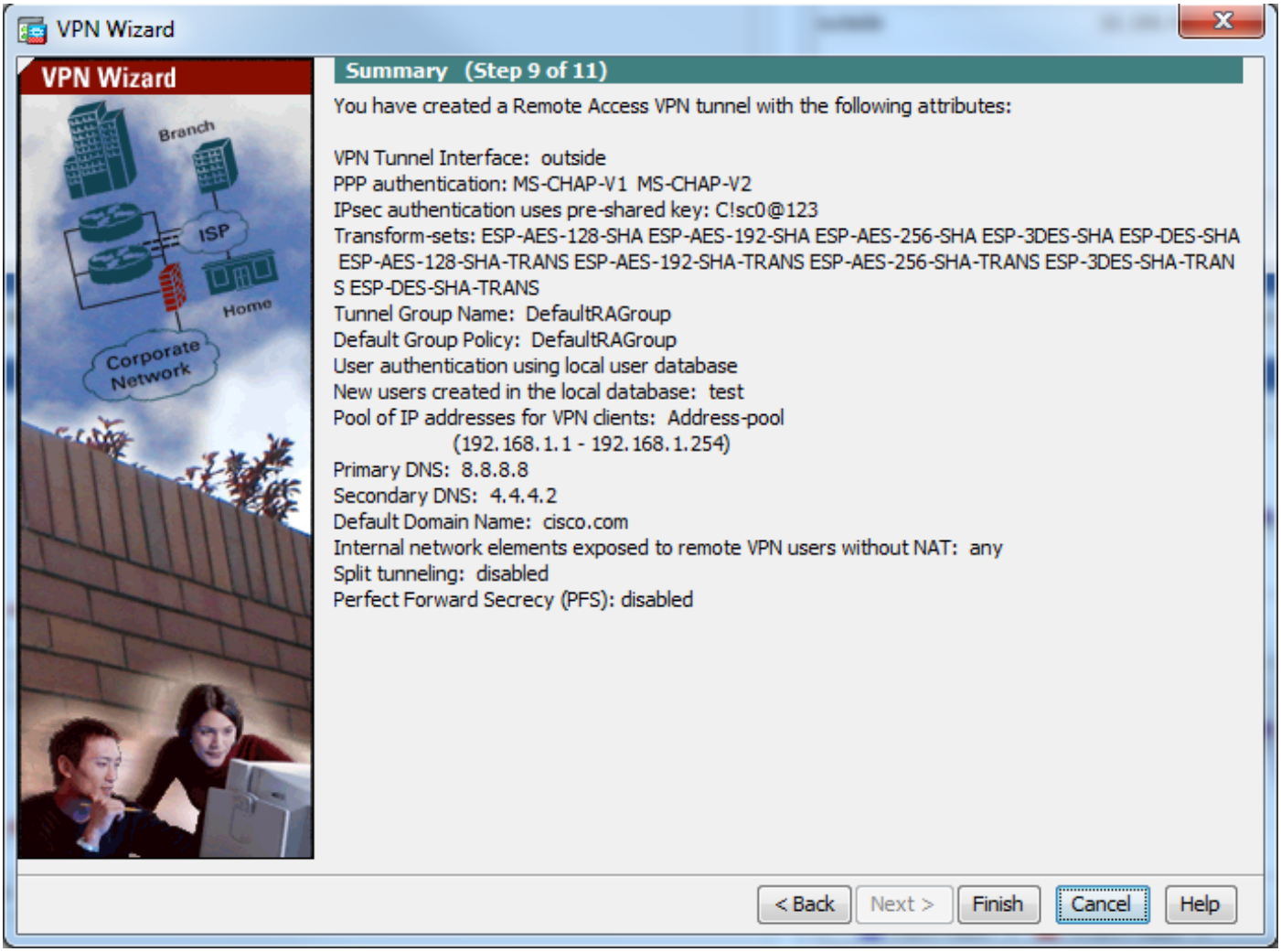
10단계. 클라이언트에 푸시될 특성을 구성하거나 비워 두고 [다음]을 **클릭합니다.**



11단계:일부 클라이언트 플랫폼은 이 기능을 지원하지 않으므로 **Enable Perfect Forwarding Secrecy (PFS)(PFS(Perfect Forwarding Secrecy) 활성화)** 상자가 선택되지 않았는지 확인합니다 .**스플릿 터널링을 활성화하여 원격 사용자가 위에서 정의한 리소스에 대해 동시에 암호화된 액세스를 허용하고 인터넷** 상자**에 대한 암호화되지 않은 액세스는** 선택 취소되므로 클라이언트 시스템의 모든 트래픽(인터넷 트래픽 포함)이 VPN 터널을 통해 ASA로 전송될 수 있습니다.Next(**다음)를 클릭합니다.**



12단계. 요약 정보를 검토한 다음 완료를 **클릭합니다.**



CLI를 사용한 ASA 컨피그레이션

1단계. IKE 1단계 정책 매개변수를 구성합니다.

이 정책은 피어 간의 제어 트래픽을 보호하는 데 사용됩니다(즉, 사전 공유 키 및 2단계 협상 보호).

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
```

2단계. 변형 집합을 구성합니다.

데이터 트래픽을 보호하는 데 사용되는 IKE Phase 2 정책 매개변수가 포함되어 있습니다.Windows L2TP/IPsec 클라이언트는 IPsec 전송 모드를 사용하므로 모드를 전송으로 설정합니다.기본값은 터널 모드입니다.

```
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport
```

3단계. 동적 맵을 구성합니다.

Windows 클라이언트가 ISP 또는 로컬 DHCP 서버(예: 모뎀)에서 동적 IP 주소를 가져오므로 ASA는 피어 IP 주소를 인식하지 못하며 이로 인해 ASA 끝의 고정 피어 구성에 문제가 발생합니다

.따라서 동적 암호화 컨피그레이션에 접근해야 합니다. 이 경우 모든 매개변수가 반드시 정의되지 않으며 누락된 매개변수가 나중에 클라이언트에서 IPSec 협상을 통해 동적으로 학습됩니다.

```
ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-
SHA
```

4단계. 동적 맵을 고정 암호화 맵에 바인딩하고 암호화 맵을 적용하고 외부 인터페이스에서 IKEv1을 활성화합니다.

동적 암호화 맵은 인터페이스에 적용할 수 없으므로 고정 암호화 맵에 바인딩합니다.동적 암호화 세트는 암호화 맵 세트에서 가장 낮은 우선순위 암호화 맵이어야 합니다(즉, 가장 높은 시퀀스 번호가 있어야 함). 그러면 ASA가 다른 암호화 맵을 먼저 평가해야 합니다.다른(정적) 맵 엔트리가 일치하지 않는 경우에만 동적 암호화 맵 집합을 검사합니다.

```
ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
ciscoasa(config)#crypto map outside_map interface outside
ciscoasa(config)#crypto ikev1 enable outside
```

5단계. IP 주소 풀 생성

IP 주소가 원격 VPN 클라이언트에 동적으로 할당되는 주소 풀을 생성합니다.ASA에서 기존 풀을 사용하려면 이 단계를 무시합니다.

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
```

6단계. 그룹 정책 구성

그룹 정책을 internal로 식별합니다. 즉, 로컬 데이터베이스에서 특성을 가져옵니다.

```
ciscoasa(config)#group-policy L2TP-VPN internal
```

> **참고:**L2TP/IPsec 연결은 기본 그룹 정책(DfltGrpPolicy) 또는 사용자 정의 그룹 정책으로 구성할 수 있습니다.두 경우 모두 L2TP/IPsec 터널링 프로토콜을 사용하도록 그룹 정책을 구성해야 합니다.vpn-protocol 특성이 구성되어 있지 않은 경우 사용자 정의 그룹 정책에 상속되는 기본 group-policy의 VPN 프로토콜 특성에 l2tp-ipsec을 구성합니다.

vpn 터널 프로토콜(이 경우 l2tp-ipsec), 도메인 이름, DNS 및 WINS 서버 IP 주소, 새 사용자 계정 등의 특성을 구성합니다.

```
ciscoasa(config)#group-policy L2TP-VPN attributes
ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2
ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
ciscoasa(config-group-policy)#default-domain value cisco.com
```

AAA를 사용하는 것 외에도 디바이스에서 사용자 이름과 비밀번호를 구성합니다.사용자가 Microsoft CHAP 버전 1 또는 버전 2를 사용하는 L2TP 클라이언트이고 ASA가 로컬 데이터베이스에 대해 인증하도록 구성된 경우 mschap 키워드를 포함해야 합니다.예를 들어 username <username> password <password> mschap를 입력합니다.

```
ciscoasa(config-group-policy)# username test password test mschap
```

7단계. tunnel-group 구성

tunnel-group 명령을 사용하여 터널 그룹을 생성하고 IP 주소를 클라이언트에 할당하는 데 사용되는 로컬 주소 풀 이름을 지정합니다.인증 방법이 pre-shared-key인 경우 터널 그룹을 지정할 수 있는 옵션이 클라이언트에 없으므로 터널 그룹 이름은 DefaultRAGroup이어야 합니다. 따라서 터널

그룹이 기본 터널 그룹에만 속합니다.default-group-policy 명령을 사용하여 그룹 정책을 터널 그룹에 바인딩

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

> **참고:**사전 공유 키 기반 인증을 수행하는 경우 기본 연결 프로파일(터널 그룹)인 DefaultRAGroup을 구성해야 합니다.인증서 기반 인증이 수행되는 경우 인증서 식별자를 기반으로 사용자 정의 연결 프로파일을 선택할 수 있습니다

tunnel-group ipsec-attributes 명령을 사용하여 ipsec-attribute 컨피그레이션 모드를 시작하여 사전 공유 키를 설정합니다.

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)#  ikev1 pre-shared-key C!sc0@123
ciscoasa(config-tunnel-ipsec)#exit
```

터널 그룹 ppp-attributes 모드에서 **authentication type** 명령을 사용하여 PPP 인증 프로토콜을 구성합니다.AAA 서버가 로컬 데이터베이스로 구성된 경우 기본적으로 지원되지 않으므로 CHAP를 비활성화합니다.

```
ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)#no authentication chap
ciscoasa(config-ppp)#authentication ms-chap-v2
ciscoasa(config-ppp)#exit
```

8단계. NAT 면제 구성

클라이언트가 내부 인터페이스에 연결된 내부 리소스에 액세스할 수 있도록 NAT 면제를 구성합니다(이 예에서는 내부 리소스가 내부 인터페이스에 연결됨).

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp route-lookup
```

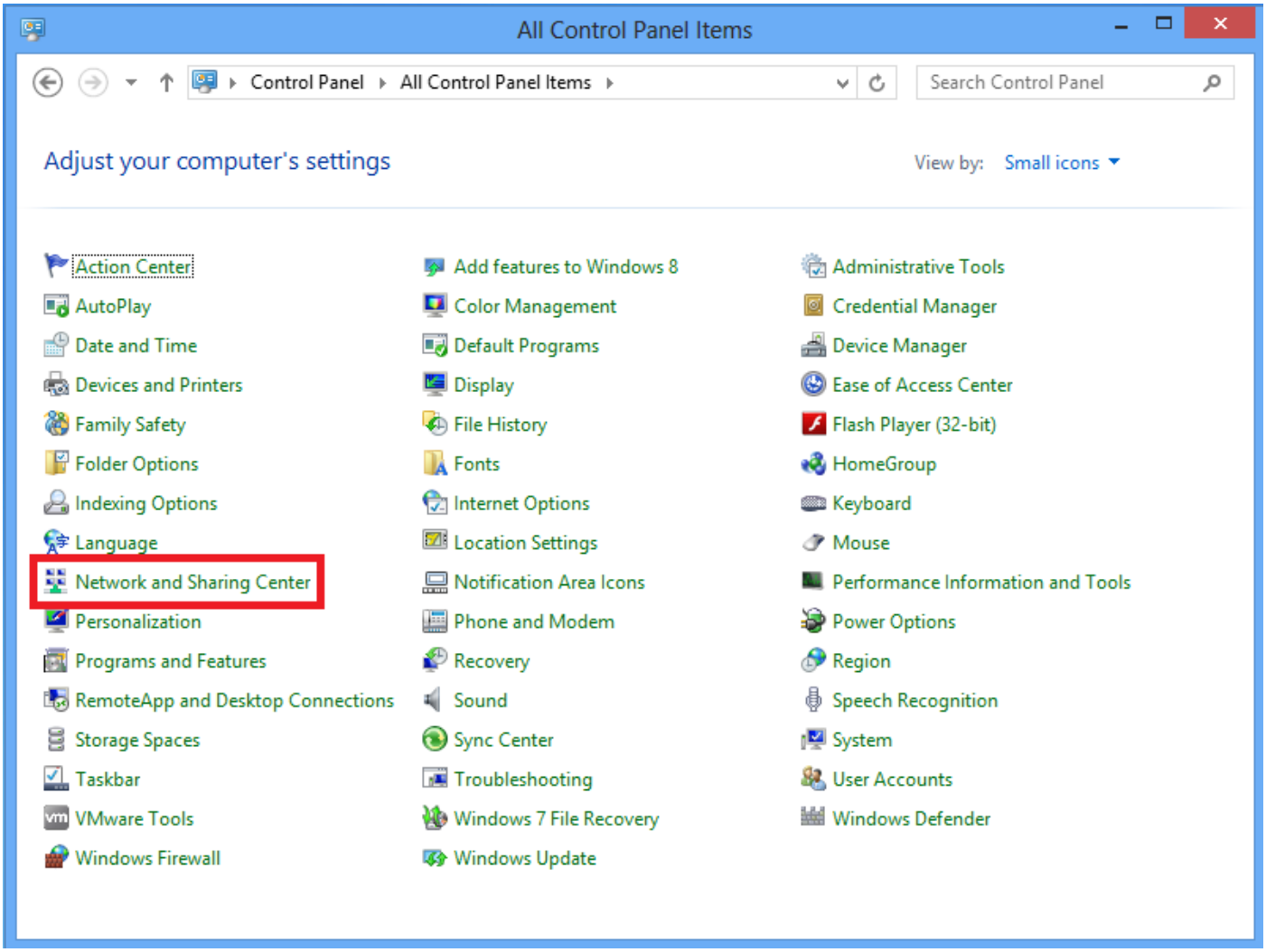
전체 샘플 구성

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit

crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport

crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ikev1 enable outside
```

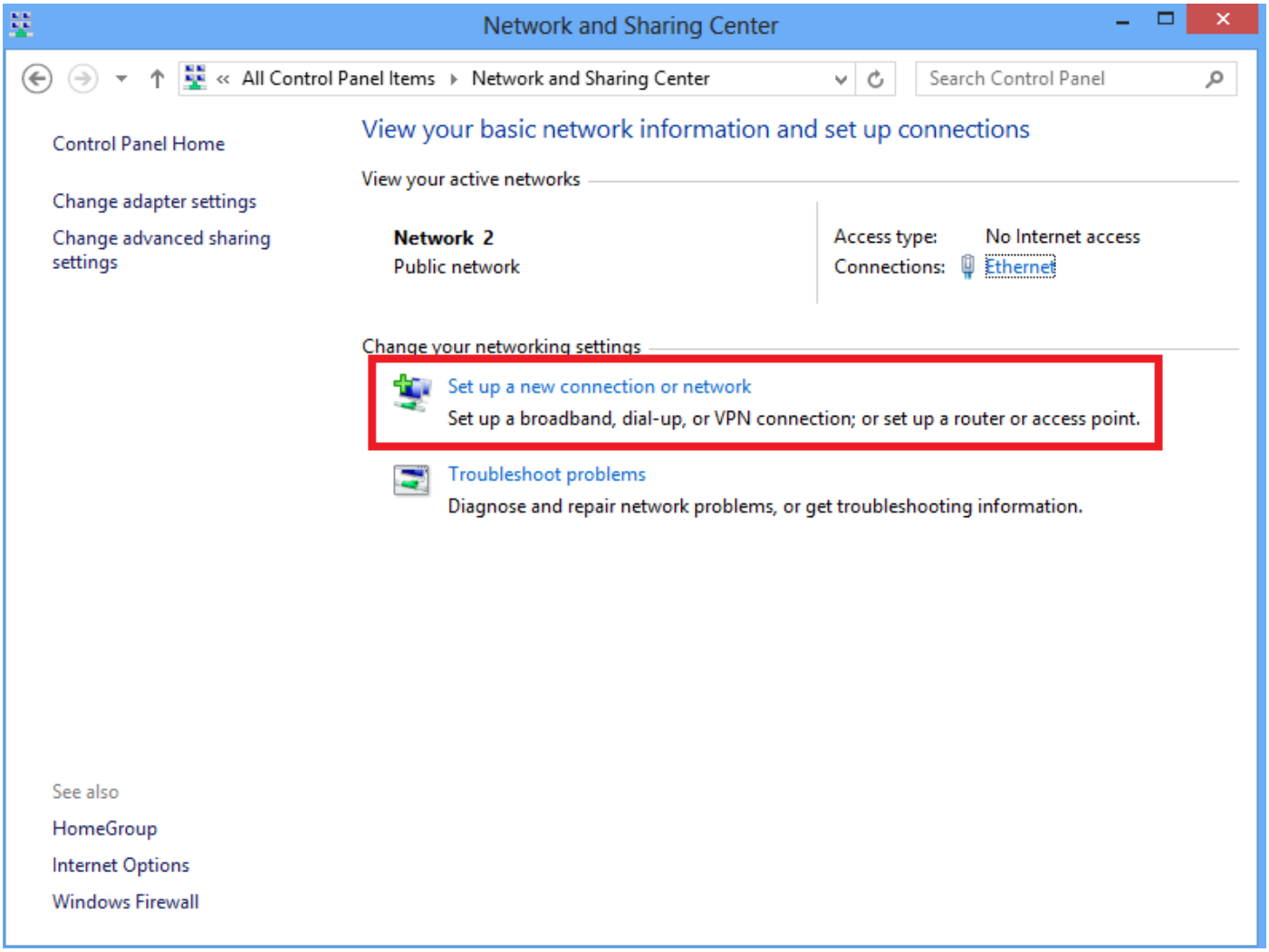
```
ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
vpn-tunnel-protocol l2tp-ipsec
default-domain value cisco.com
username test password test mschap
exit

tunnel-group DefaultRAGroup general-attributes
address-pool Address-pool
default-group-policy L2TP-VPN
exit

tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
exit

object network L2TP-Pool
subnet 192.168.1.0 255.255.255.0
exit
nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup
```

Windows 8 L2TP/IPsec 클라이언트 구성

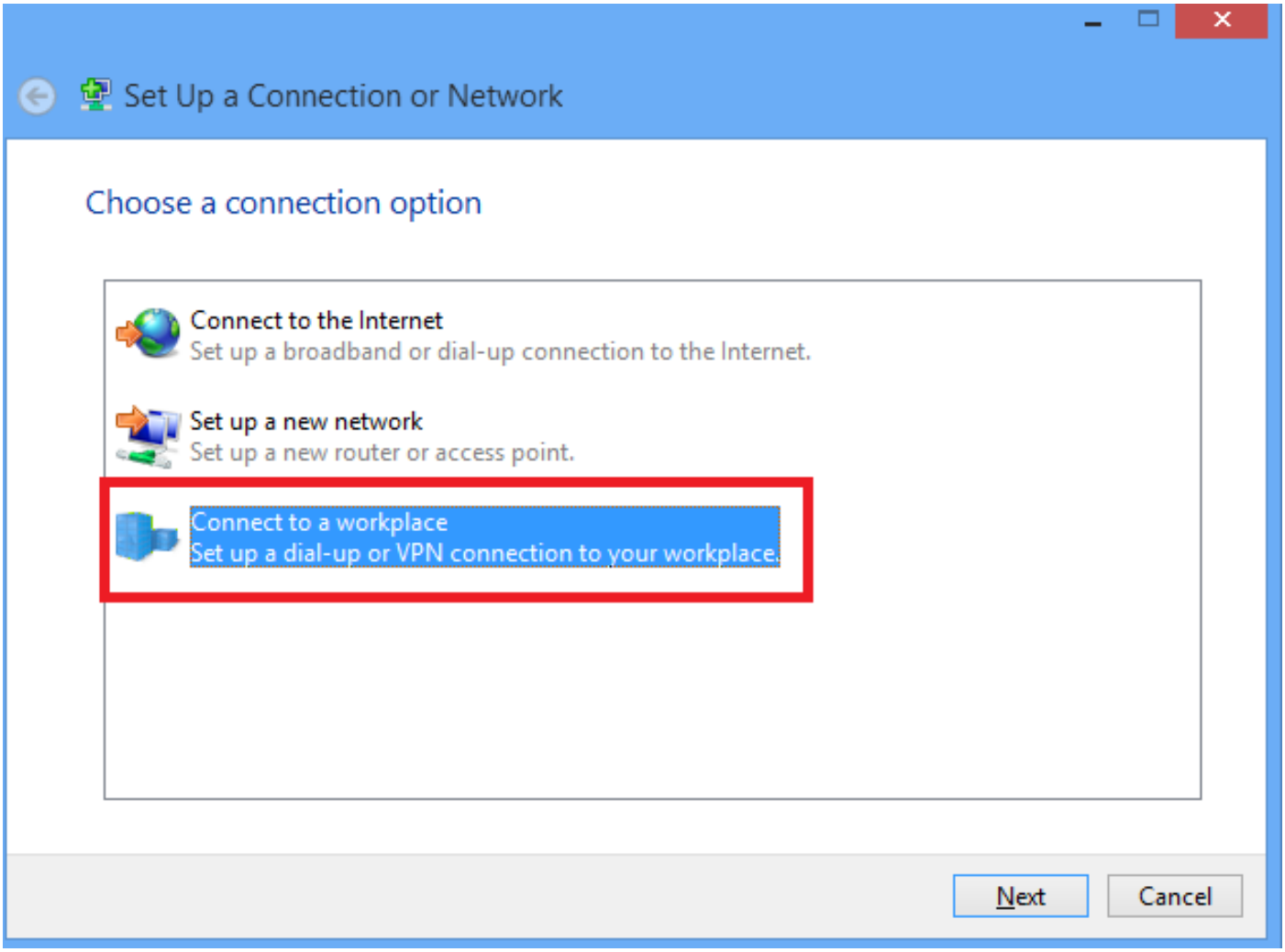
1. 제어판을 열고 네트워크 및 공유 센터를 선택합니다.



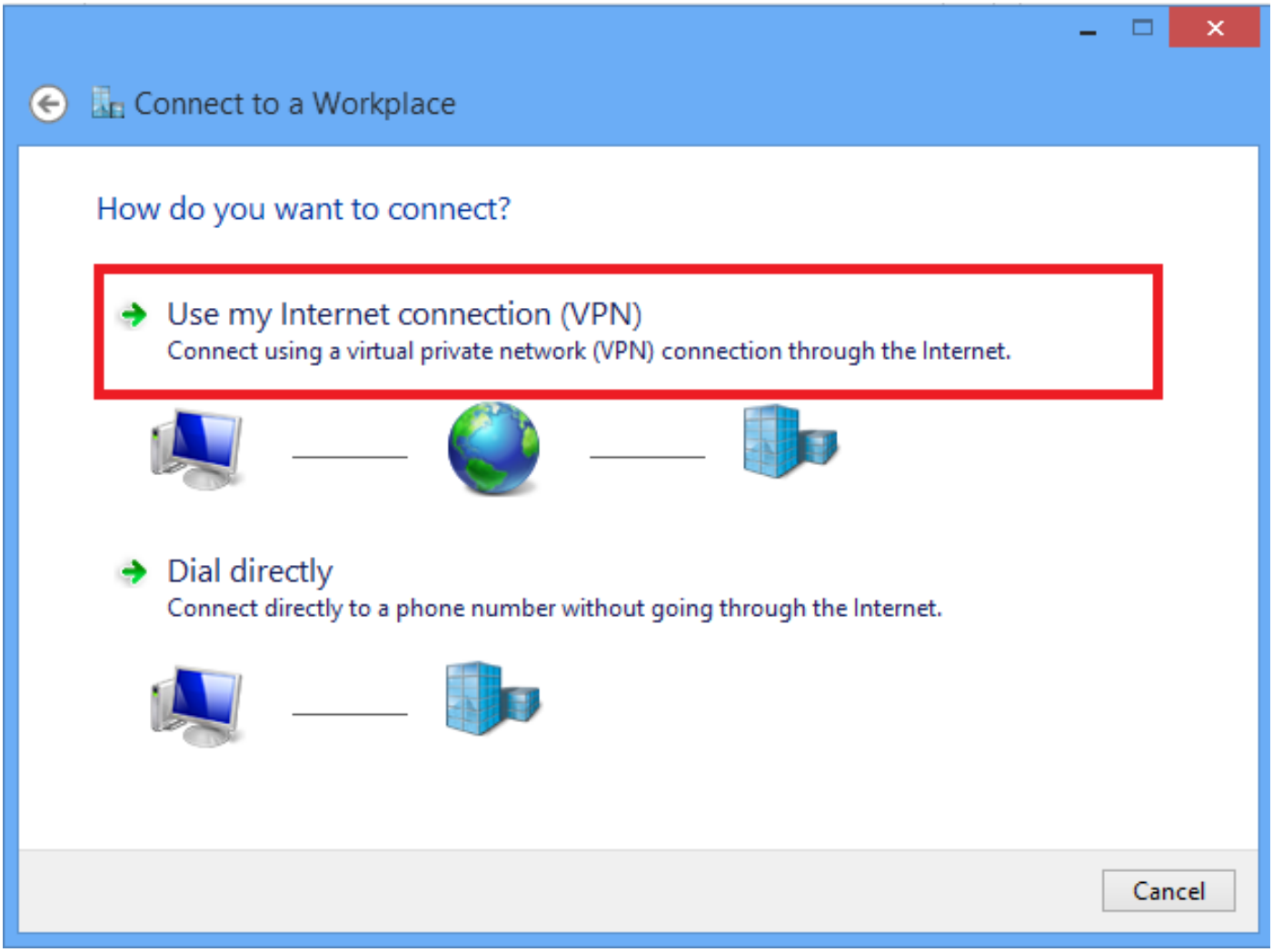
2. **신규 연결 또는 네트워크** 옵션 **설정을** 선택합니다.



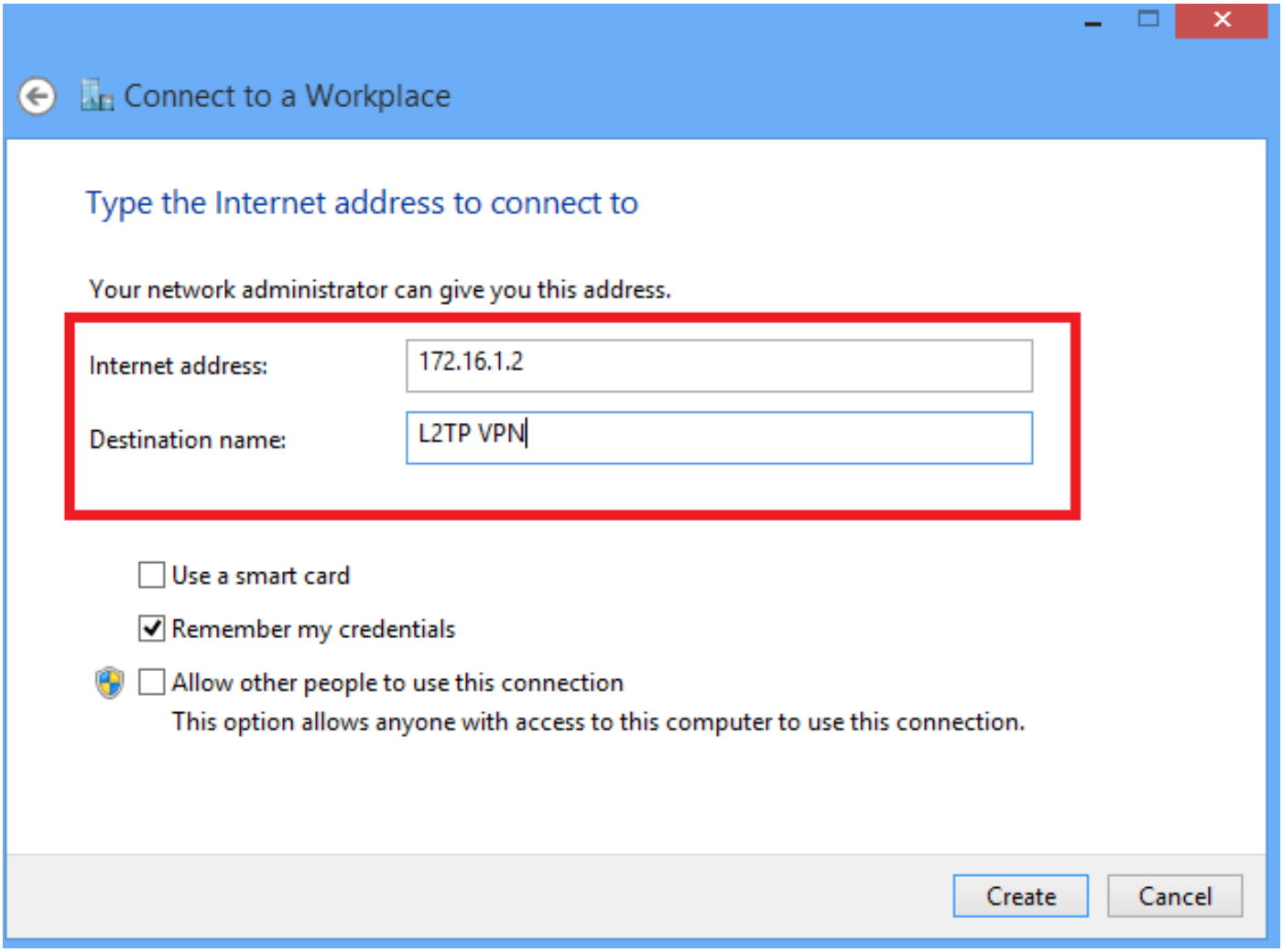
3. **작업 공간에 연결** 옵션**을 선택하고 다음**을 클릭합니다.



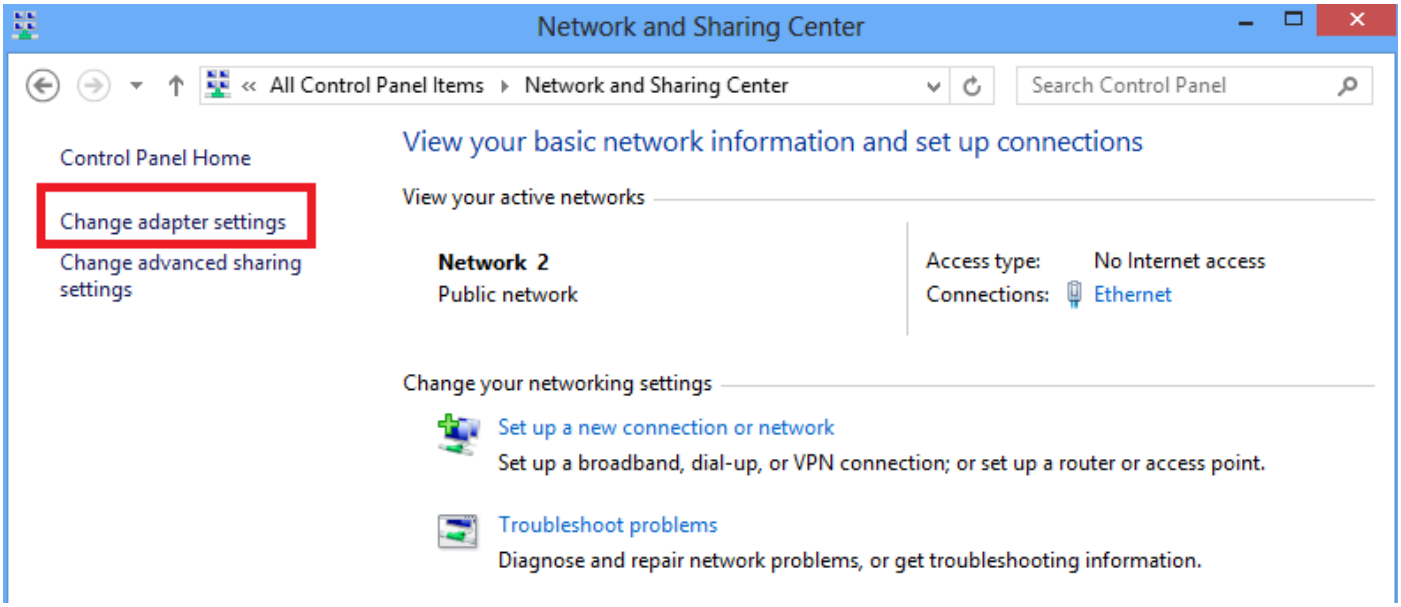
4.**Use my Internet connection (VPN)(내 인터넷 연결(VPN) 사용)** 옵션을 클릭합니다.



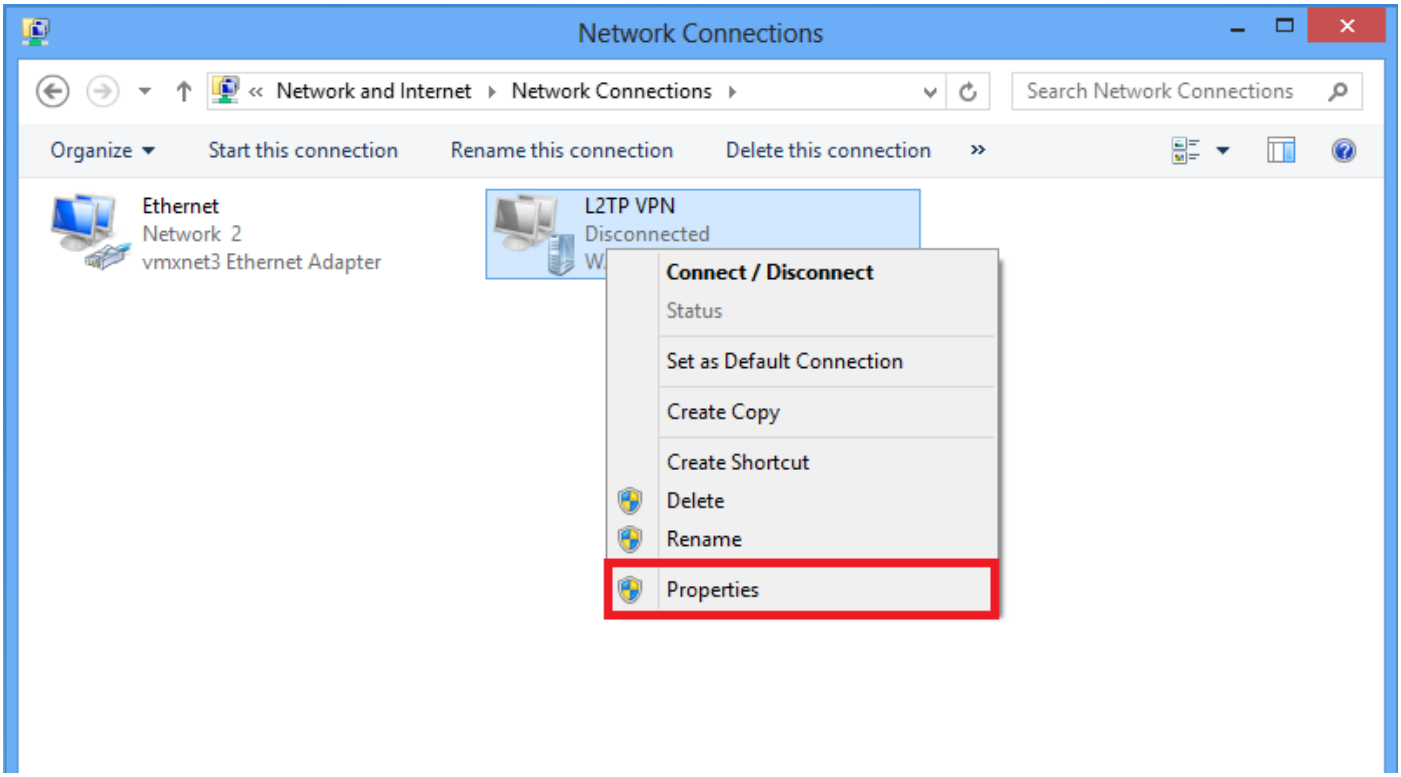
5. ASA의 WAN 인터페이스 또는 FQDN의 IP 주소 및 로컬에서 중요한 VPN 어댑터의 이름을 입력하고 Create(생성)를 **클릭합니다.**



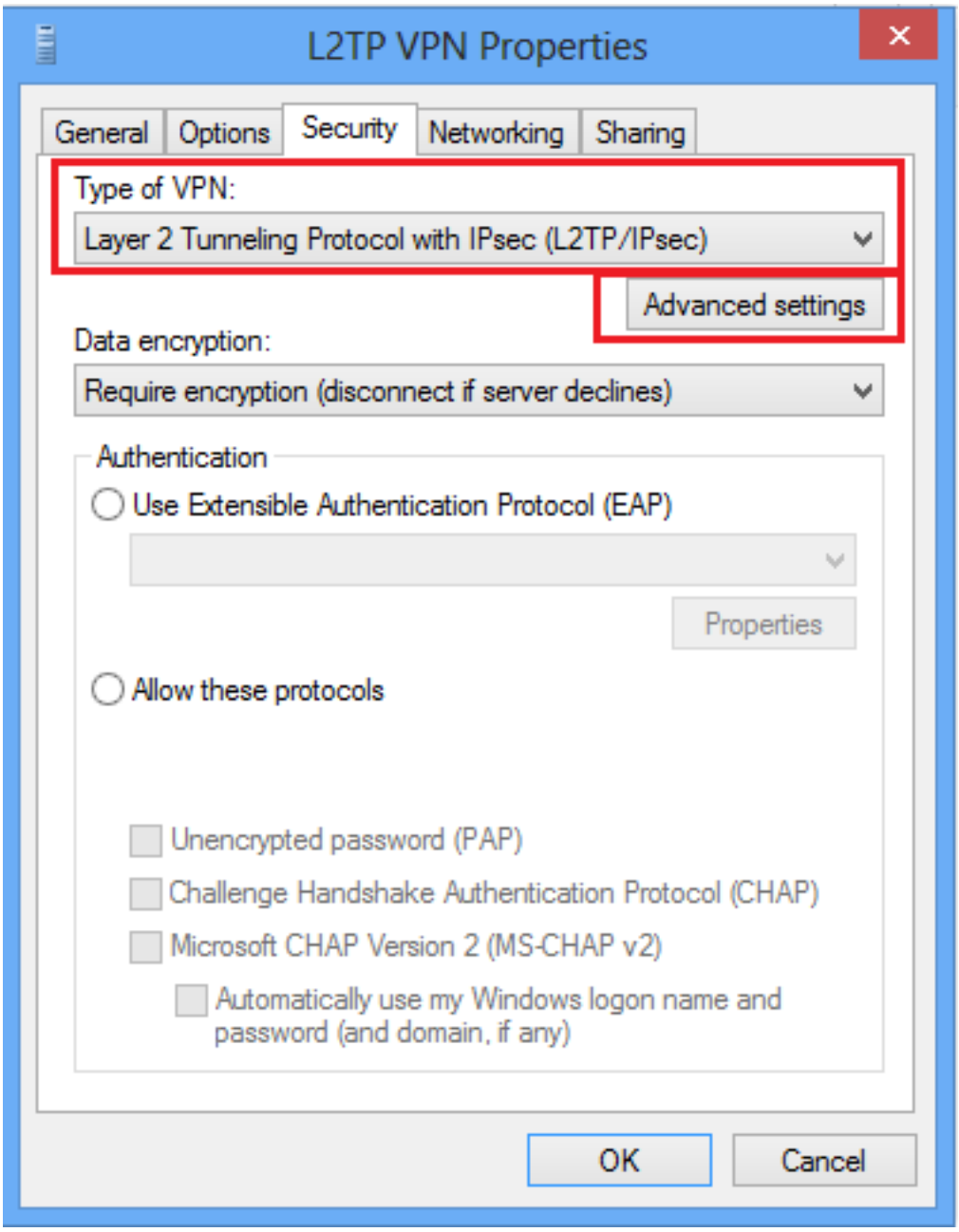
6. Network and Sharing Center(네트워크 및 공유 센터)에서 창 왼쪽 창의 **어댑터 설정 변경** 옵션을 선택합니다.



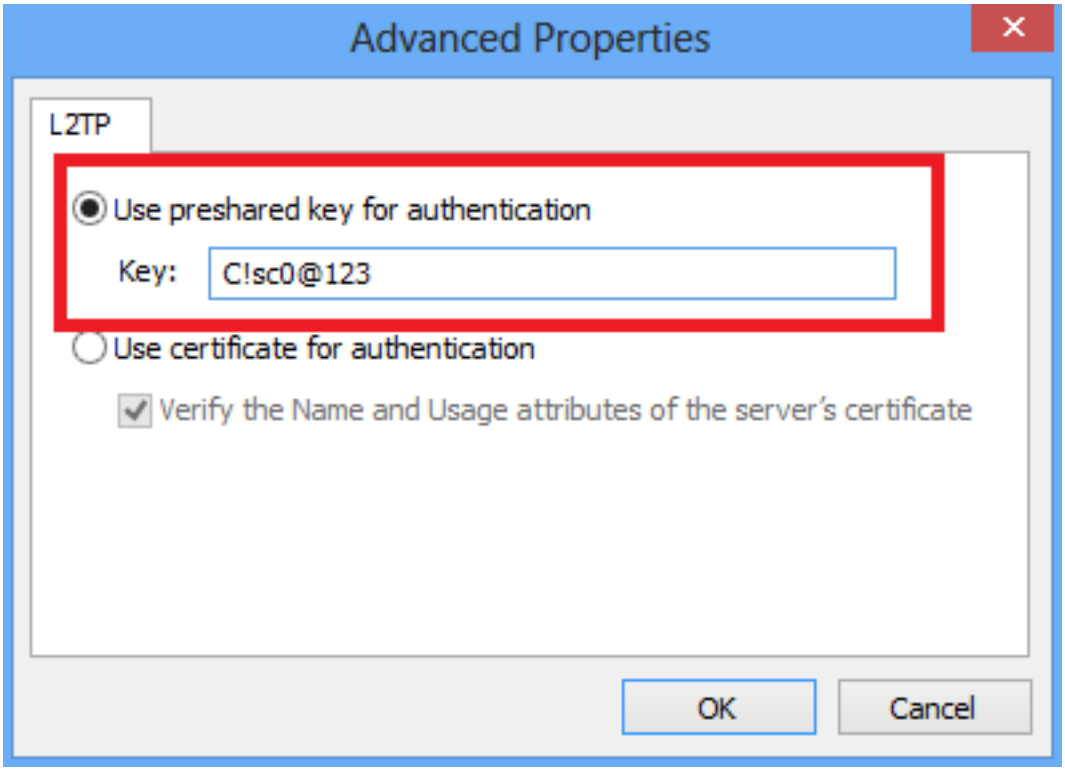
7. 최근에 생성된 L2TP VPN 어댑터를 마우스 오른쪽 버튼으로 클릭하고 Properties(속성)를 **선택합니다.**



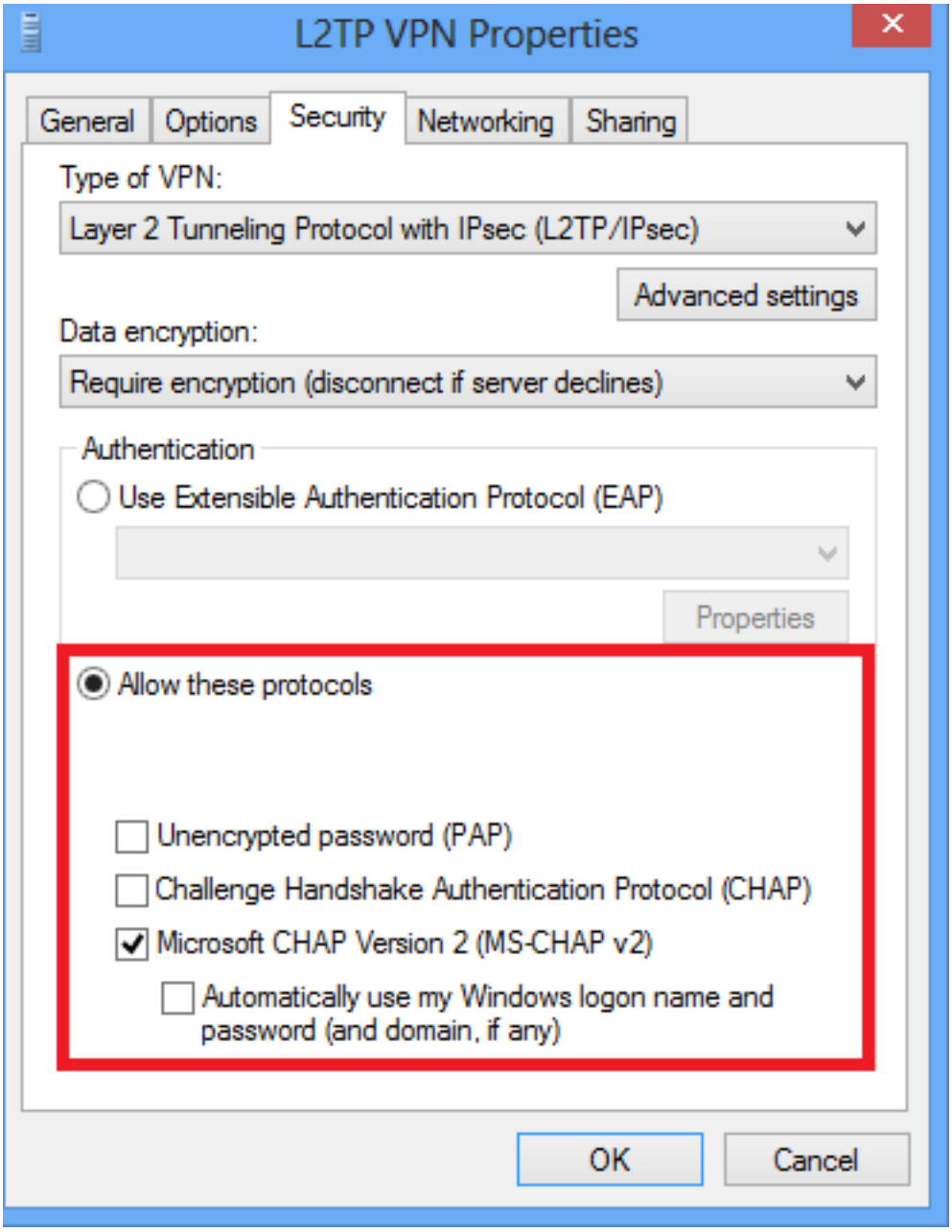
8. **Security(보안)** 탭으로 이동하여 Type of VPN as **Layer 2 Tunneling Protocol with IPsec(L2TP/IPsec)**(IPsec**(L2TP/IPsec)**을 선택하고 **Advanced settings(고급 설정)**를 클릭합니다.



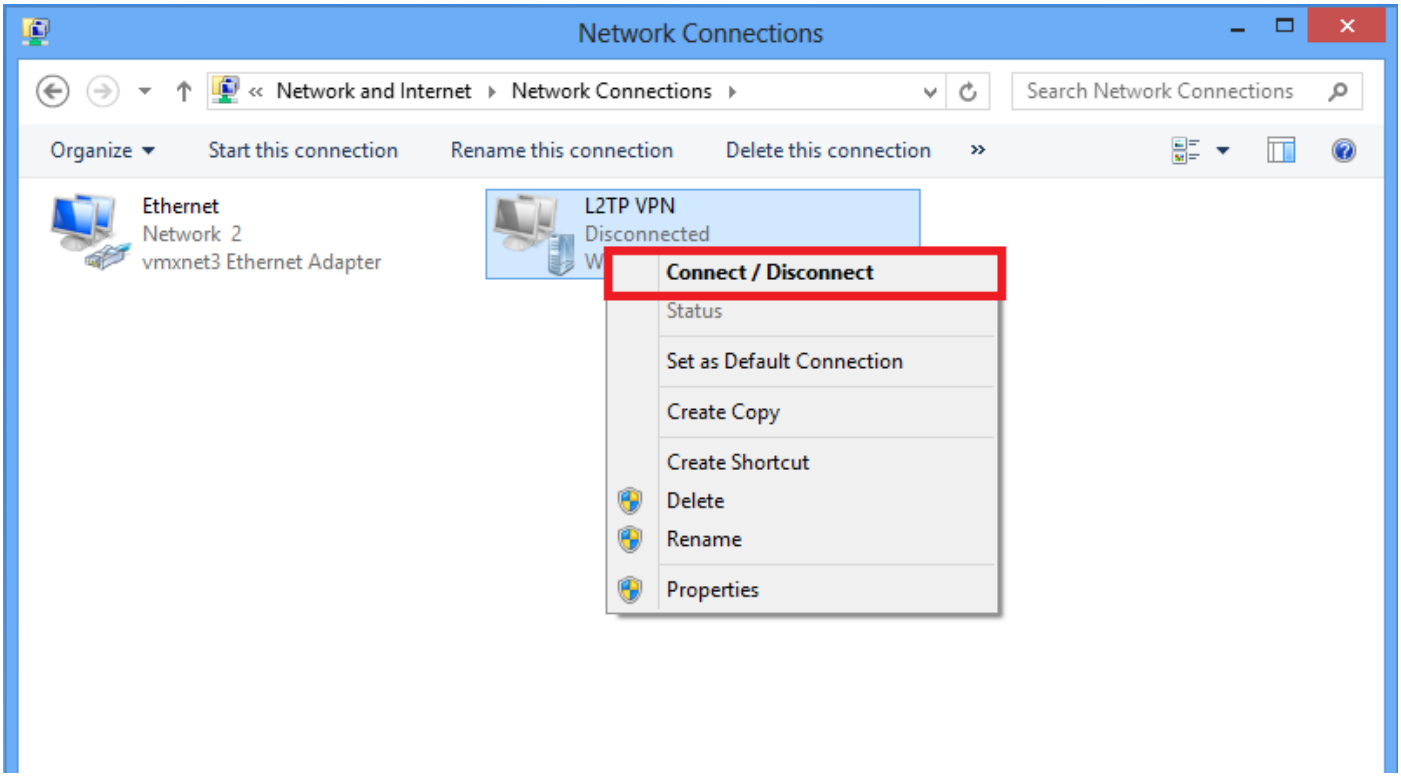
9. tunnel-group DefaultRAGroup에 언급된 것과 동일한 사전 공유 키**를 입력하고 OK**를 클릭합니다 .이 예에서는 C!sc0@123이 사전 공유 키로 사용됩니다.



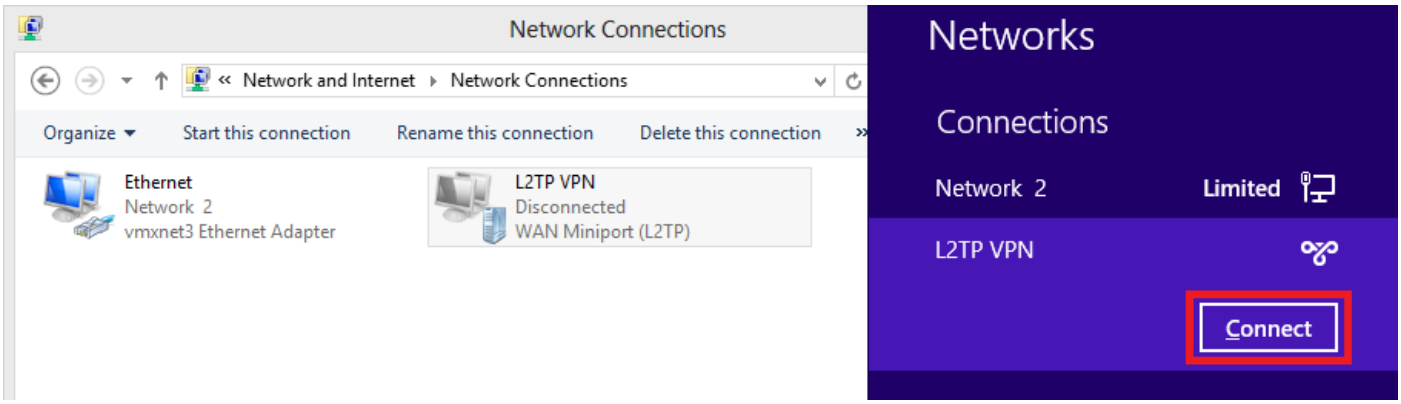
10. 인증 방법을 Allow these protocols(다음 프로토콜 허용)로 선택하고 "**Microsoft CHAP Version 2(MS-CHAP v2)(Microsoft CHAP 버전 2(MS-CHAP v2))** 확인란만 선택했는지 확인하고 **OK(확인)**를 클릭합니다.



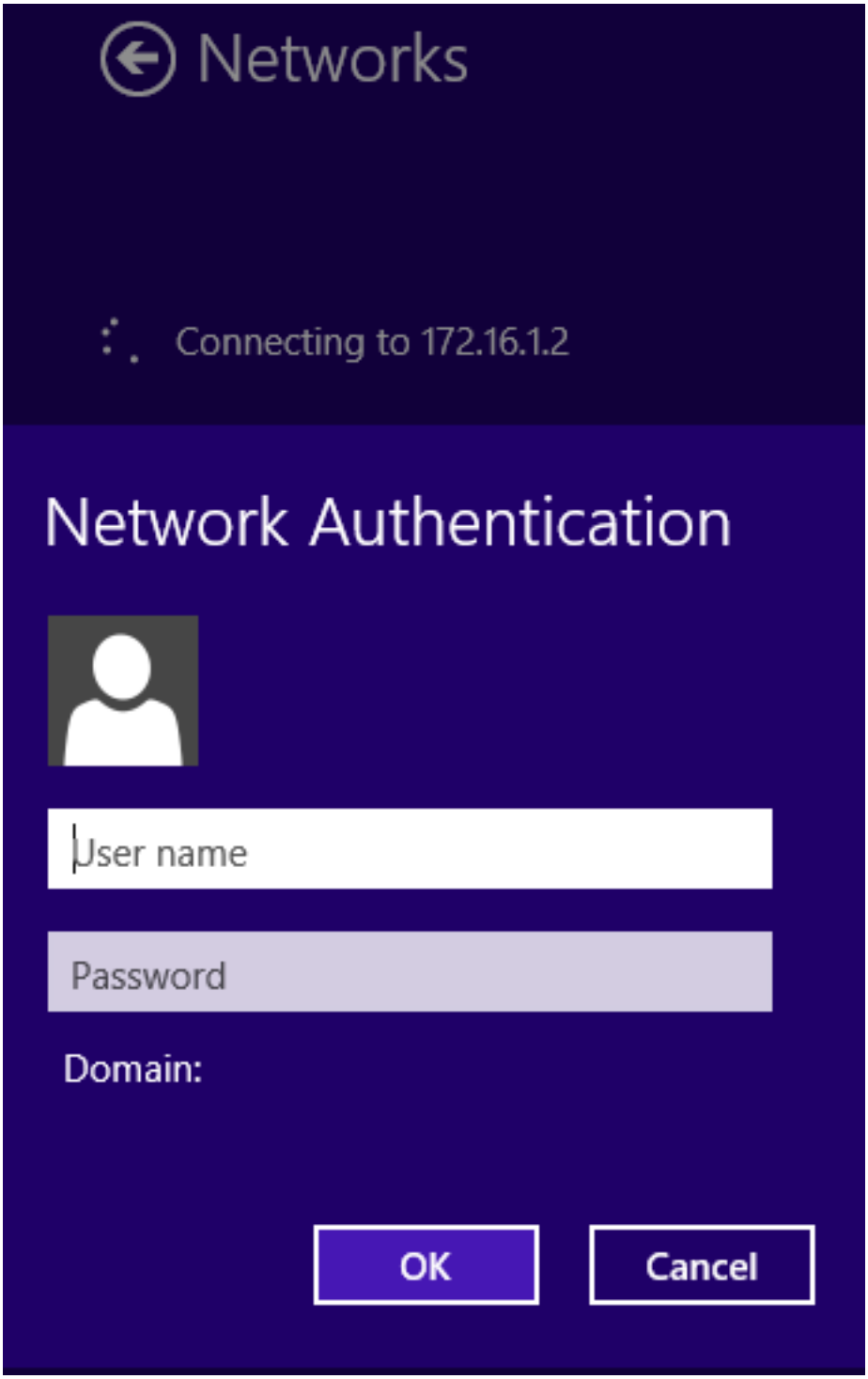
11. 네트워크 연결에서 L2TP VPN 어댑터를 마우스 오른쪽 버튼으로 클릭하고 Connect/**Disconnect(연결/연결 끊기)**를 선택합니다.



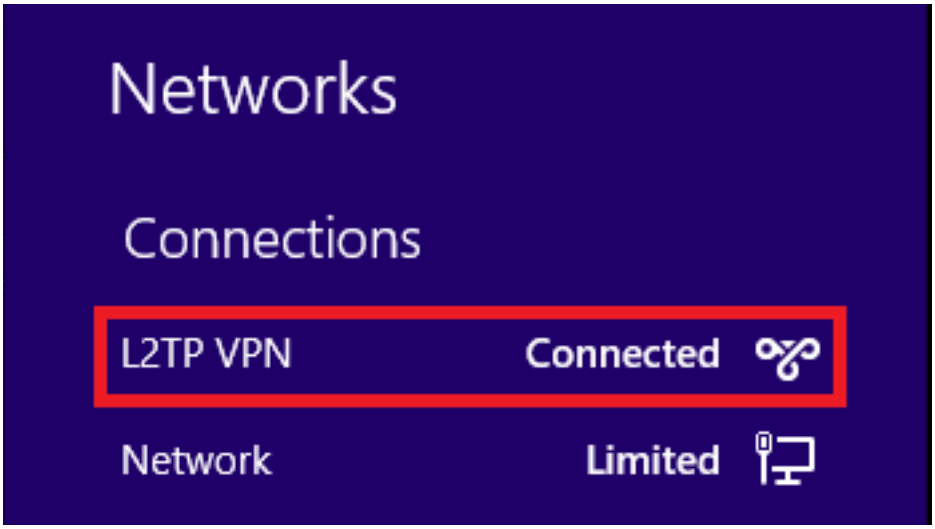
12. 네트워크 아이콘이 팝업되고 L2TP VPN 연결에서 연결을 클릭합니다.



13. 사용자 자격 증명을 입력하고 확인을 클릭합니다.



필요한 매개변수가 양쪽 끝에서 일치하면 L2TP/IPsec 연결이 설정됩니다.



스플릿 터널 컨피그레이션

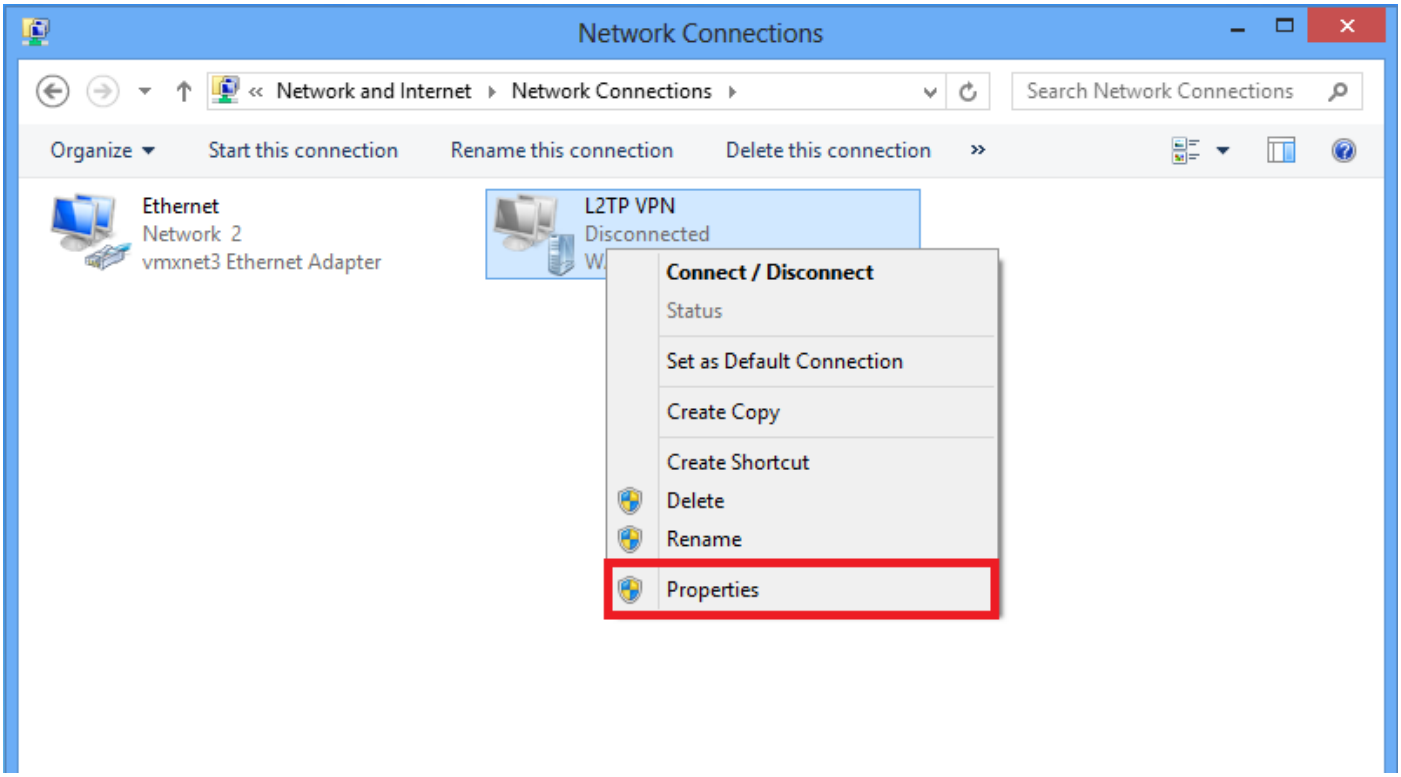
스플릿 터널링은 암호화되어야 하는 서브넷 또는 호스트의 트래픽을 정의하기 위해 사용할 수 있는 기능입니다.여기에는 이 기능과 연결된 ACL(Access Control List)의 컨피그레이션이 포함됩니다.이 ACL에 정의된 서브넷 또는 호스트에 대한 트래픽은 클라이언트 끝으로부터 터널을 통해 암호화되며, 이러한 서브넷에 대한 경로가 PC 라우팅 테이블에 설치됩니다.ASA는 클라이언트에서 DHCPINFORM 메시지를 인터셉트하고 서브넷 마스크, 도메인 이름 및 클래스 없는 고정 경로로 응답합니다.

ASA의 컨피그레이션

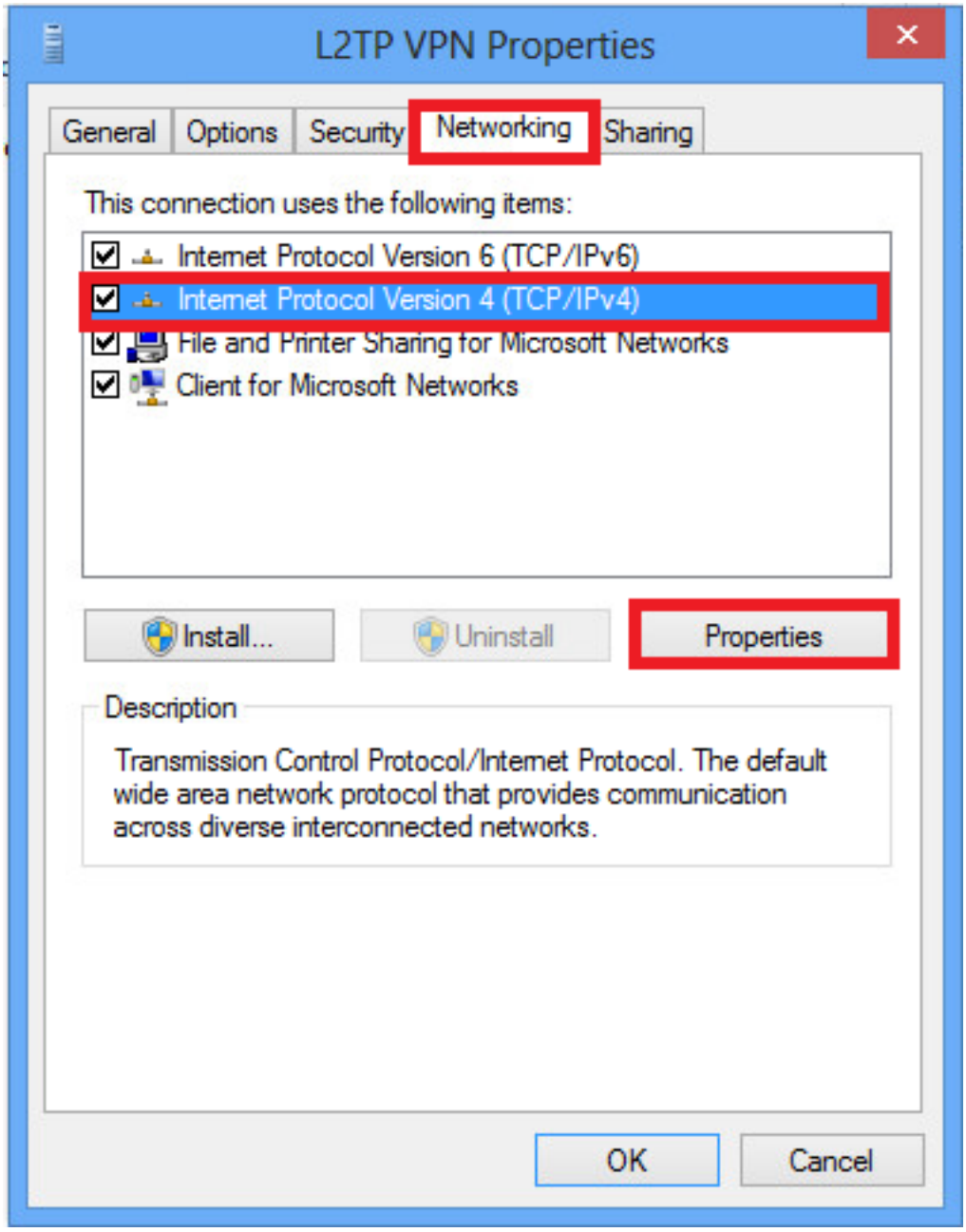
```
ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0

ciscoasa(config)# group-policy DefaultRAGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable
```

L2TP/IPsec 클라이언트의 컨피그레이션

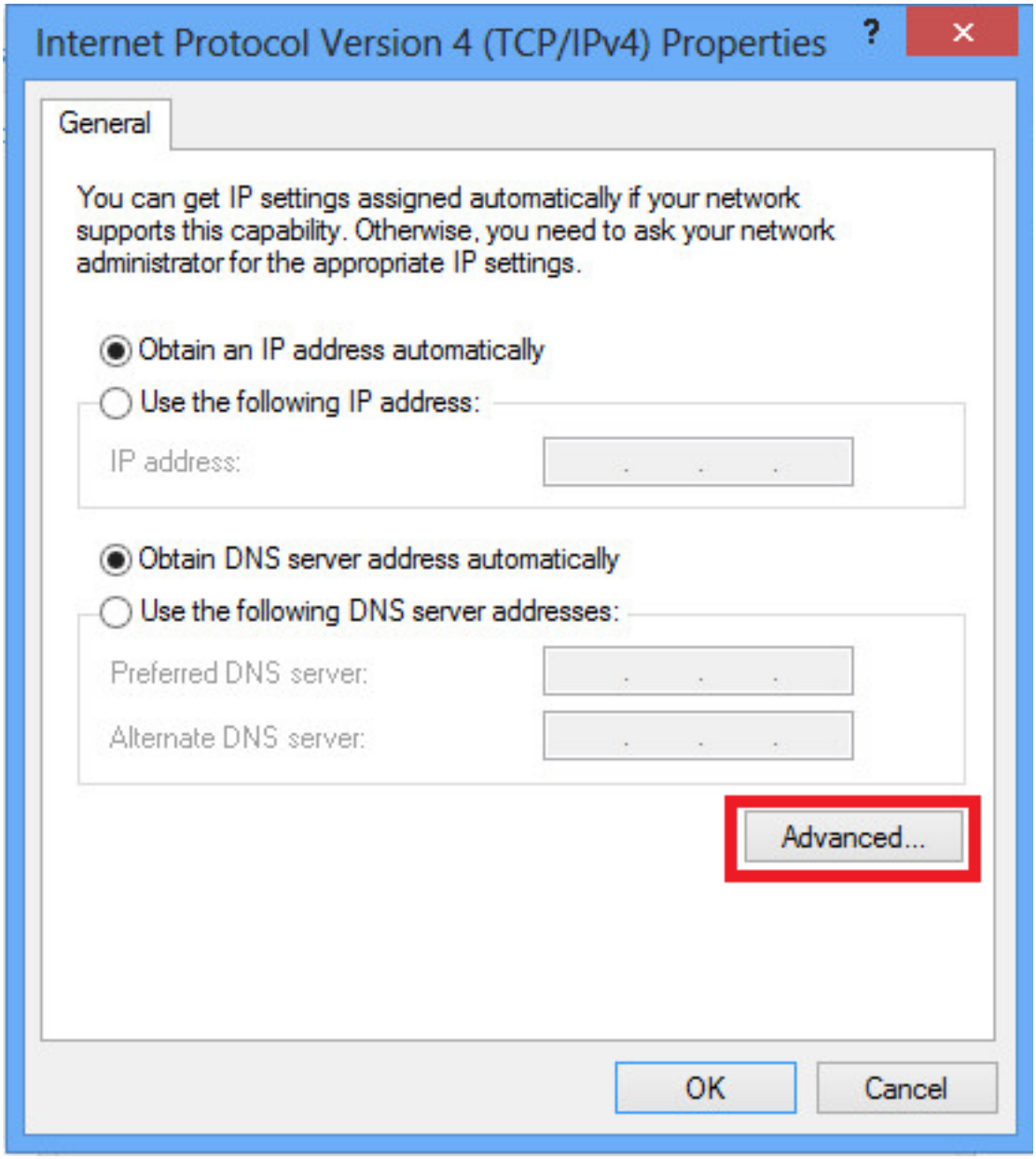
1. L2TP VPN 어댑터를 마우스 오른쪽 버튼으로 클릭하고 Properties(속성)를 **선택합니다.**



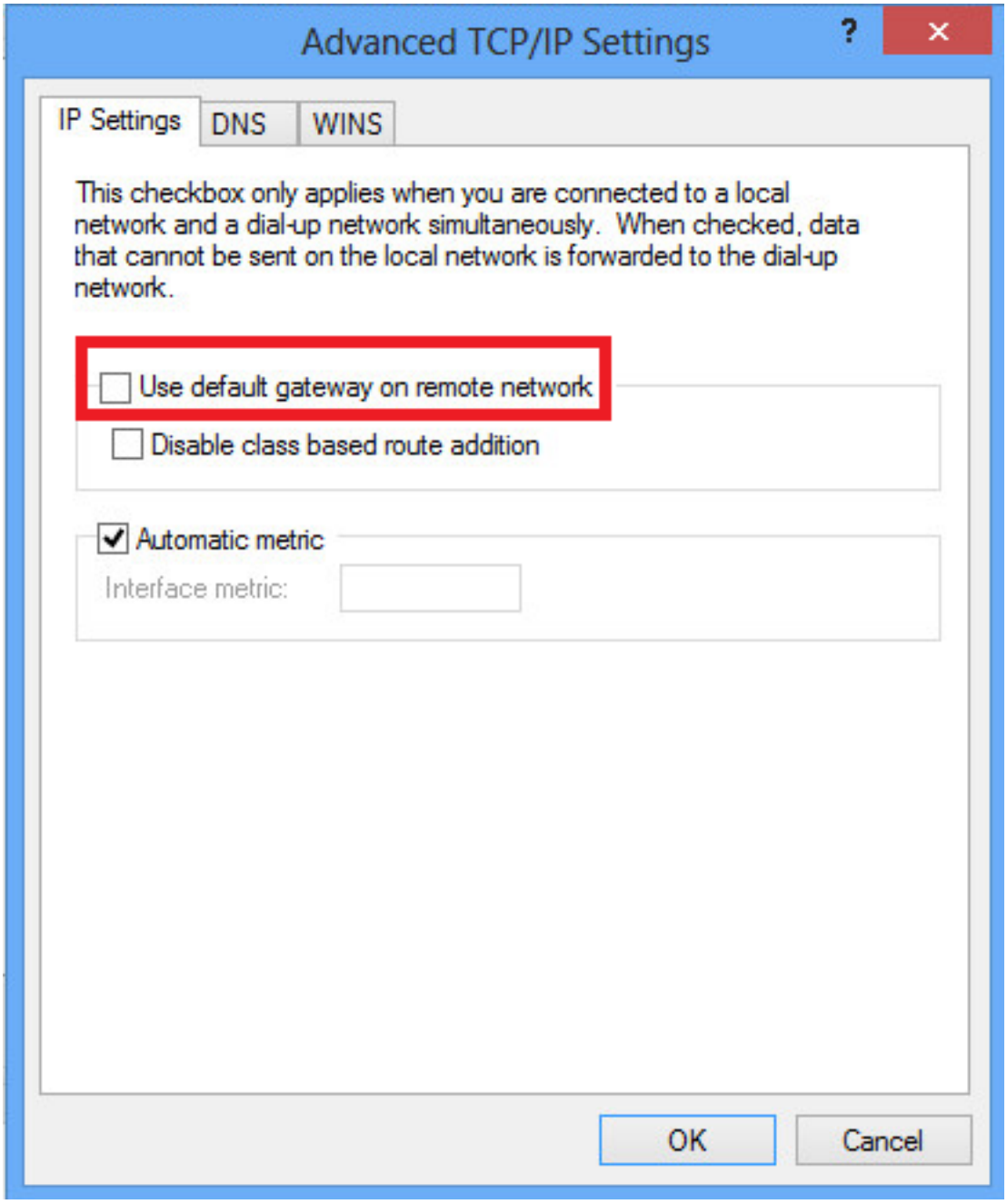
2. Networking(네트워킹) 탭으로 이동하여 Internet Protocol Version 4(TCP/IPv4)를 선택한 다음 Properties(속성)를 **클릭합니다.**



3. **고급** 옵션을 클릭합니다.



4. **Use default gateway on remote network** 옵션을 **선택 취소하고 OK**를 클릭합니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

> **참고:**Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

- **show crypto ikev1 sa** - 피어의 현재 IKE SA를 모두 표시합니다.

```
ciscoasa# show crypto ikev1 sa

IKEv1 SAs:

  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:
```

10.1.1.2

```
   Type    : user            Role    : responder
   Rekey   : no
```

State   : MM_ACTIVE

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

```
ciscoasa# show crypto ipsec sa
interface: outside
   Crypto map tag:
```

outside_dyn_map

```
, seq num: 10, local addr: 172.16.1.2

     local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/
```

17/1701

```
)
     remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/
```

17/1701

```
)
```

current_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

```
     dynamic allocated peer ip(ipv6): 0.0.0.0
```

#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

```
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
     #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
     path mtu 1500, ipsec overhead 58(36), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: E8AF927A
     current inbound spi : 71F346AB

   inbound esp sas:
     spi: 0x71F346AB (1911768747)
        transform: esp-3des esp-sha-hmac no compression
        in use settings ={RA, Transport, IKEv1, }
        slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (237303/3541)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000003
   outbound esp sas:
     spi: 0xE8AF927A (3903820410)
        transform: esp-3des esp-sha-hmac no compression
        in use settings ={RA, Transport, IKEv1, }
        slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (237303/3541)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

- **show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec - L2TP over IPsec 연결에 대한 자세한 정보를 표시합니다.**

```
ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed


Username     : test

                  Index        : 1


Assigned IP  : 192.168.1.1           Public IP    : 10.1.1.2


Protocol     : IKEv1 IPsec L2TPOverIPsec
License      : Other VPN
Encryption   : IKEv1: (1)3DES  IPsec: (1)3DES  L2TPOverIPsec: (1)none
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1  L2TPOverIPsec: (1)none
Bytes Tx     : 1574                  Bytes Rx     : 12752
Pkts Tx      : 29                    Pkts Rx      : 118
Pkts Tx Drop : 0                     Pkts Rx Drop : 0


Group Policy : L2TP-VPN              Tunnel Group : DefaultRAGroup


Login Time   : 23:32:48 UTC Sat May 16 2015
Duration     : 0h:04m:05s
Inactivity   : 0h:00m:00s
```

```
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2577000010005557d3a0
Security Grp : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1
L2TPOverIPsec Tunnels: 1
```

IKEv1:

```
 Tunnel ID    : 1.1
 UDP Src Port : 500                    UDP Dst Port : 500
 IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
 Encryption   : 3DES                   Hashing      : SHA1
 Rekey Int (T): 28800 Seconds          Rekey Left(T): 28555 Seconds
 D/H Group    : 2
 Filter Name  :
```

IPsec:

```
 Tunnel ID    : 1.2
 Local Addr   : 172.16.1.2/255.255.255.255/17/1701
 Remote Addr  : 10.1.1.2/255.255.255.255/17/1701
 Encryption   : 3DES                   Hashing      : SHA1
 Encapsulation: Transport
 Rekey Int (T): 3600 Seconds           Rekey Left(T): 3576 Seconds
 Rekey Int (D): 250000 K-Bytes         Rekey Left(D): 250000 K-Bytes
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Bytes Tx     : 1574                   Bytes Rx     : 12752
 Pkts Tx      : 29                     Pkts Rx      : 118
```

L2TPOverIPsec:

```
 Tunnel ID    : 1.3
```

Username : test

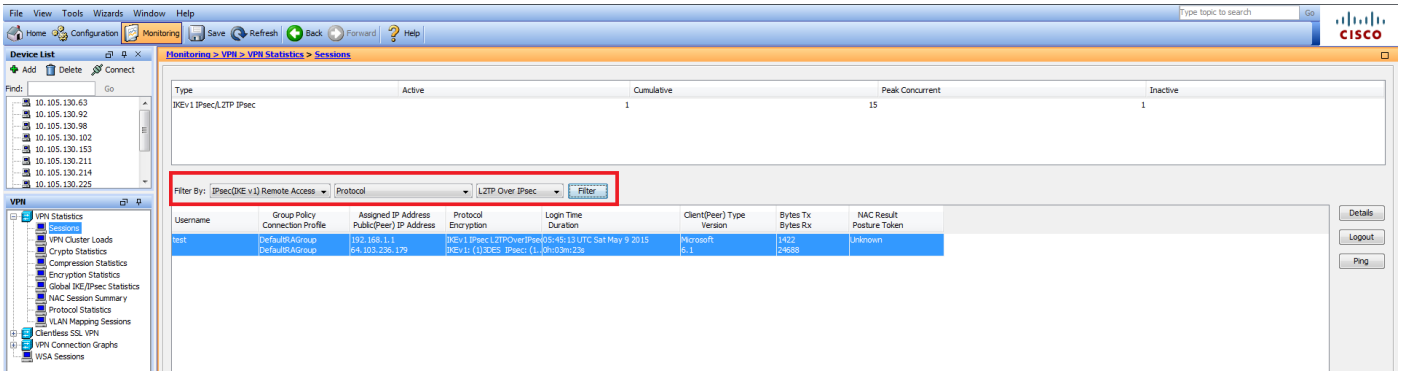
Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

```
 Encryption   : none                   Hashing      : none
```

```
Auth Mode     : msCHAPV2

Idle Time Out: 30 Minutes            Idle TO Left : 27 Minutes
Client OS     : Microsoft
Client OS Ver: 6.2
Bytes Tx      : 475                  Bytes Rx     : 9093
Pkts Tx       : 18                   Pkts Rx      : 105
```

ASDM에서 Monitoring(모니터링) **> VPN > VPN Statistics(VPN 통계) > Sessions(세션)**에서 VPN 세션에 대한 일반 정보를 볼 수 있습니다.L2TP over IPsec 세션은 **IPsec(IKEv1) Remote Access(IPsec) > Protocol(프로토콜) > L2TP Over IPsec을** 통해 필터링할 수 있습니다.



문제 해결

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

> **참고:debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

> **주의:**ASA에서는 다양한 디버그 레벨을 설정할 수 있습니다.기본적으로 level 1이 사용됩니다.디버그 수준을 변경하면 디버그의 세부 정보가 증가할 수 있습니다.특히 프로덕션 환경에서 이 작업을 신중하게 수행합니다!

VPN 터널 문제를 해결하려면 다음 **debug 명령**을 **주의**와 함께 사용하십시오.

- **debug crypto ikev1** - IKE에 대한 디버그 정보를 표시합니다.
- **debug crypto ipsec** - IPsec에 대한 디버그 정보를 표시합니다.

다음은 성공적인 L2TP over IPSec 연결을 위한 디버그 출력입니다.

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NONE (0) total length : 408
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID
```

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,
```

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended
capabilities payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,
```

Connection landed on tunnel_group DefaultRAGroup

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for
Responder...
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D
(20) + NONE (0) total length : 304
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received
10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
```

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-alives (type = None)
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds.
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I
```

PSec SA Proposal # 2, Transform # 1 acceptable

```
  Matches global IPSec SA entry # 10
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI      : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine:
SPI = 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick
mode
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,
```

Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

Local host: 172.16.1.2 Protocol 17 Port 1701

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd
QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR
+ HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x00007fffe1c75c00,
   SCB: 0xE13ABD20,
   Direction: outbound
   SPI      : 0x8C14FD70
   Session ID: 0x00001000
```

```
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x8C14FD70
IPSEC: Creating outbound VPN context, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
   Peer : 0x00000000
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: New outbound encrypt rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   Dst mask: 255.255.255.255
```

Src ports

Upper: 1701

Lower: 1701

Op   : equal

Dst ports

Upper: 1701

Lower: 1701

Op   : equal

Protocol: 17

```
   Use protocol: true
   SPI: 0x00000000
```

```
   Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   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: 0x8C14FD70
   Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User ()  Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI      : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
   Flags: 0x00000206
   SA   : 0x00007fffe13ab260
   SPI  : 0x7AD72E0D
   MTU  : 0 bytes
   VCID : 0x00000000
   Peer : 0x000028D4
   SCB  : 0x0AC5BD5B
   Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
   VPN handle: 0x0000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
   Peer : 0x00004174
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
```

```
   Rule ID: 0x00007fffe1c76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 1701
     Lower: 1701
     Op   : equal
   Dst ports
     Upper: 1701
     Lower: 1701
     Op   : equal
   Protocol: 17
   Use protocol: true
   SPI: 0x00000000
   Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   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: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   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: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

PHASE 2 COMPLETED

```
 (msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,
```

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1

이 표에는 Windows 클라이언트에서 일반적으로 나타나는 VPN 관련 오류 중 일부가 나와 있습니다

오류 코드	가능한 솔루션
691	입력한 사용자 이름과 암호가 올바른지 확인합니다.
789,835	클라이언트 컴퓨터에 구성된 사전 공유 키가 ASA와 동일한지 확인합니다.
800	1. VPN 유형이 "L2TP(Layer 2 Tunneling Protocol)"로 설정되어 있는지 확인합니다. 2. 사전 공유 키가 올바르게 구성되었는지 확인합니다.
809	UDP 포트 500, 4500(클라이언트 또는 서버가 NAT 장치 뒤에 있는 경우) 및 ESP 트래픽이 차단되지 않았는지 확인합니다.

관련 정보

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