

shrew 소프트웨어 VPN 클라이언트를 사용하여 RV130 및 RV130W에서 IPSec VPN 서버에 연결

목표

IPSec VPN(Virtual Private Network)을 사용하면 인터넷을 통해 암호화된 터널을 설정하여 원격 리소스를 안전하게 가져올 수 있습니다.

RV130 및 RV130W는 IPSec VPN 서버로 작동하며 Shrew Soft VPN 클라이언트를 지원합니다.

클라이언트 소프트웨어의 최신 릴리스를 다운로드해야 합니다.

·Shrew 소프트웨어(<https://www.shrew.net/download/vpn>)

참고: IPSec VPN 서버를 사용하여 Shrew Soft VPN 클라이언트를 성공적으로 설정 및 구성하려면 먼저 IPSec VPN 서버를 구성해야 합니다. 이 방법에 대한 자세한 내용은 [RV130 및 RV130W에서 IPSec VPN Server의 구성 문서를 참조하십시오.](#)

이 문서의 목적은 Shrew Soft VPN 클라이언트를 사용하여 RV130 및 RV130W에서 IPSec VPN Server에 연결하는 방법을 설명하는 것입니다.

적용 가능한 장치

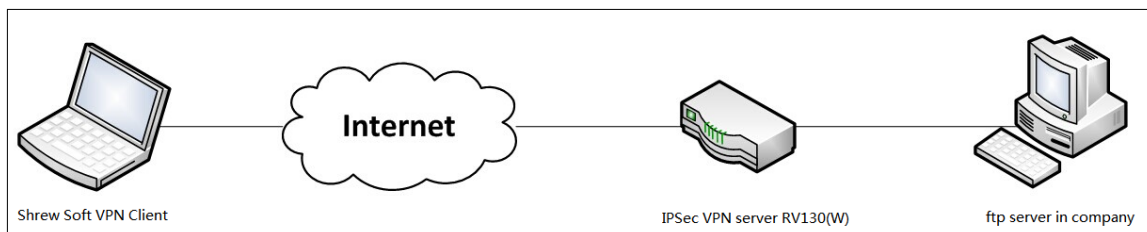
- RV130W Wireless-N VPN Firewall
- RV130 VPN Firewall

시스템 요구 사항

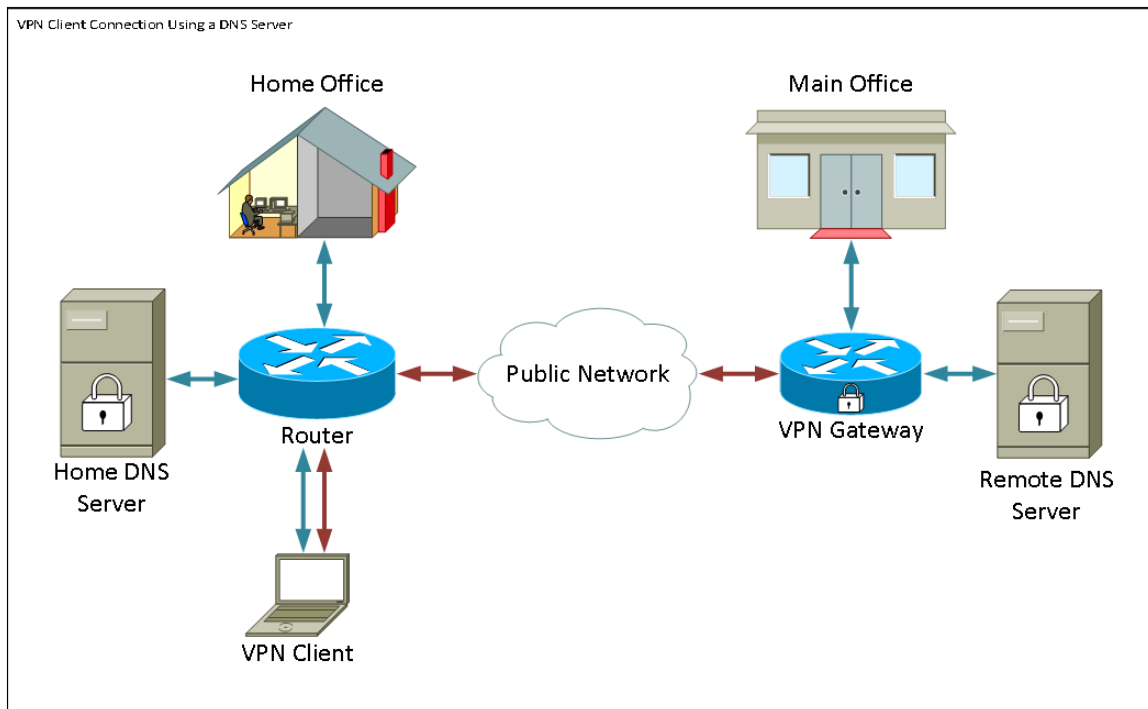
- 32비트 또는 64비트 시스템
- Windows 2000, XP, Vista 또는 Windows 7/8

토폴로지

다음은 Shrewsoft 클라이언트와 사이트 간 컨피그레이션과 관련된 디바이스를 보여주는 최상위 토폴로지입니다.



소규모 비즈니스 네트워크 환경에서 DNS 서버의 역할을 좀 더 자세히 설명하는 흐름도는 다음과 같습니다.



소프트웨어 버전

•1.0.1.3

shrew 소프트 VPN 클라이언트 설정

IPSec VPN 설정 및 사용자 구성

1단계. 웹 구성 유틸리티에 로그인하고 VPN > IPSec VPN Server > Setup을 선택합니다. 설정 페이지가 열립니다.

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:


Authentication Algorithm:

PFS Key Group: Enable

DH Group:

2단계. RV130용 IPSec VPN 서버가 올바르게 구성되었는지 확인합니다. IPSec VPN 서버가 구성되지 않았거나 잘못 구성된 경우 RV130 및 [RV130W에서 IPSec VPN 서버 구성을](#) 참조하고 **Save(저장)**를 클릭합니다.

Setup

 Configuration settings have been saved successfully

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group: Enable

DH Group:

참고: 위 설정은 RV130/RV130W IPSec VPN Server 구성의 예입니다. 이 설정은 문서의 [RV130 및 RV130W에서 IPSec VPN Server의 구성을 기반으로 하며](#) 후속 단계에서 참조합니다.

3단계. VPN > IPSec VPN Server > User로 이동합니다. User 페이지가 나타납니다.

User

User Account Table

<input type="checkbox"/>	UserName	Password
<input type="checkbox"/>	No data to display	

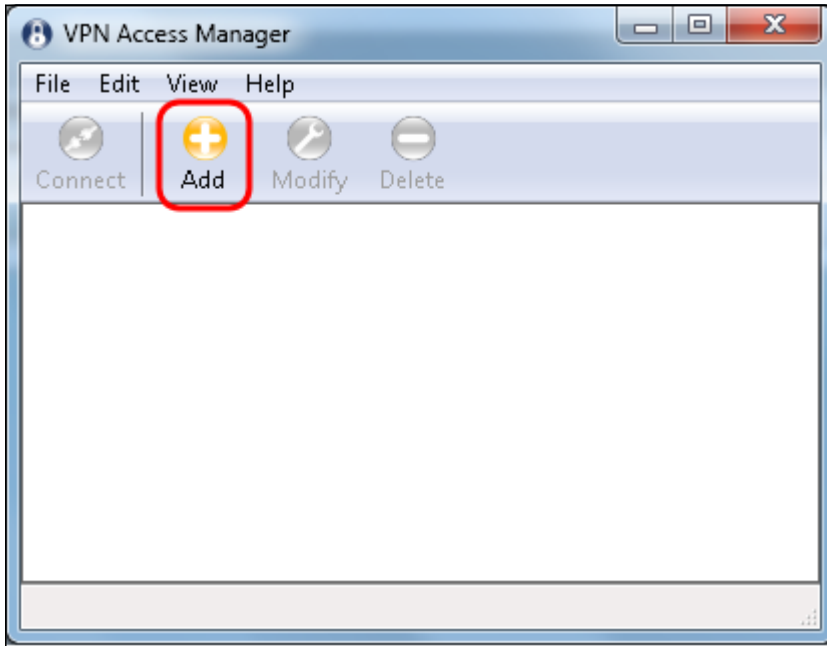
4단계. Add Row(행 추가)를 클릭하여 VPN 클라이언트를 인증하는 데 사용되는 사용자 계정을 추가하고(확장 인증) 제공된 필드에 원하는 사용자 이름과 비밀번호를 입력합니다.



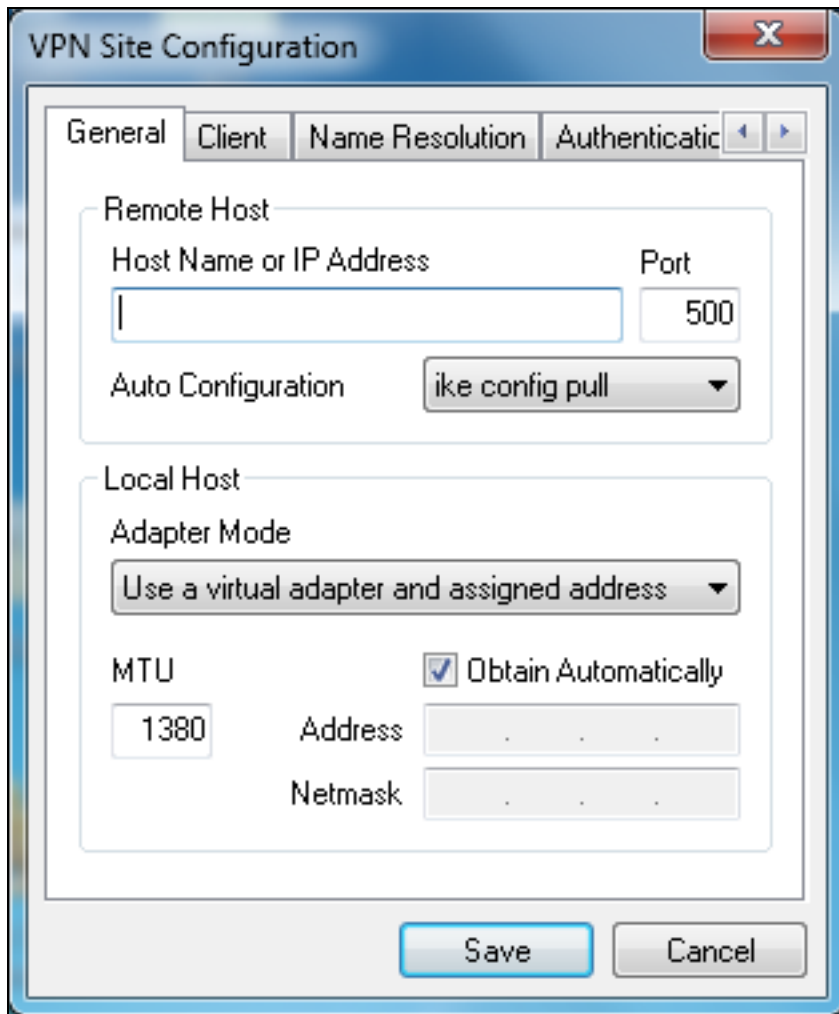
5단계. **저장**을 클릭하여 설정을 저장합니다.

VPN 클라이언트 컨피그레이션

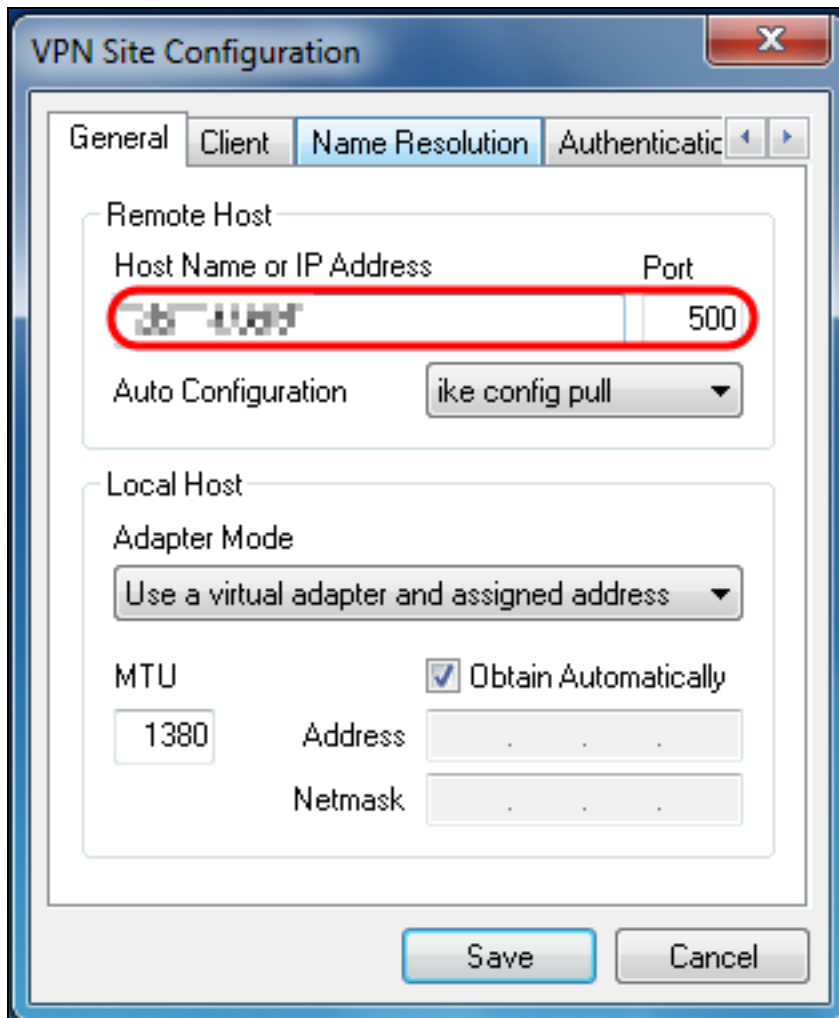
1단계. Shrew VPN Access Manager를 열고 Add(추가)를 클릭하여 **프로필**을 추가합니다.



VPN Site Configuration(VPN 사이트 컨피그레이션) 창이 나타납니다.

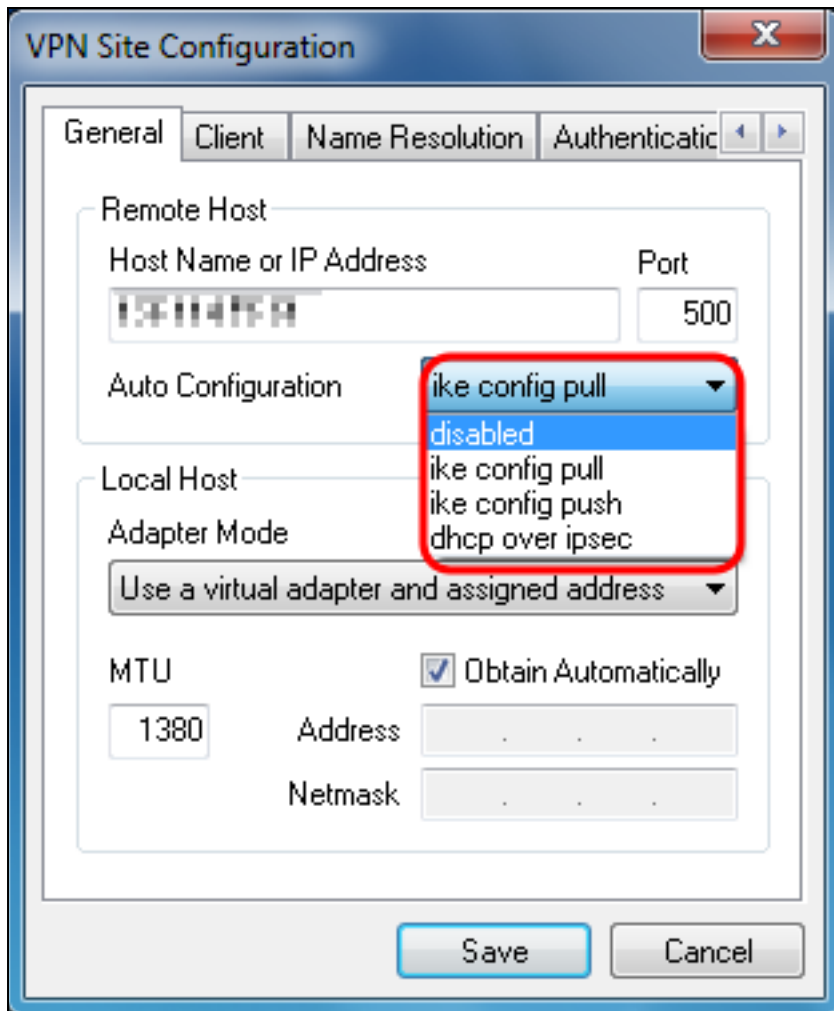


2단계. *Remote Host*(원격 호스트) 섹션의 *General*(일반) 탭 아래에 연결하려는 네트워크의 공용 호스트 이름 또는 IP 주소를 입력합니다.



참고: 포트 번호가 기본값 500으로 설정되어 있는지 확인합니다. VPN이 작동하려면 터널에서 ISAKMP 트래픽이 방화벽에서 전달되도록 설정해야 하는 UDP 포트 500을 사용합니다.

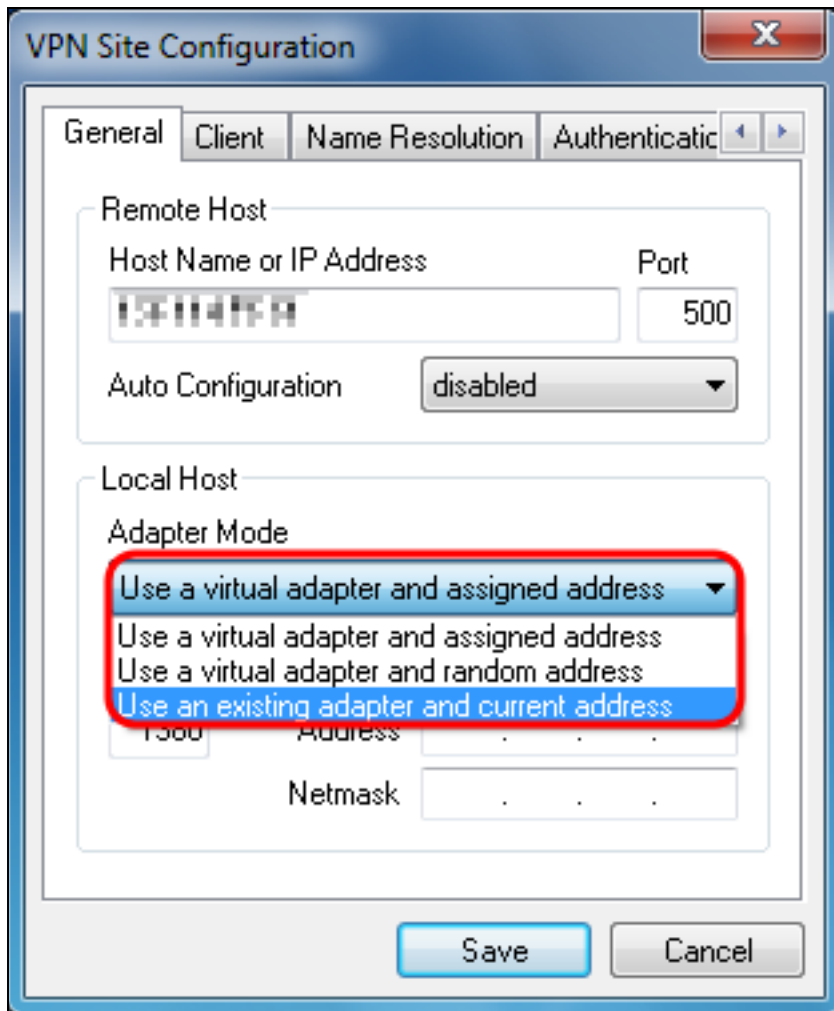
3단계. *Auto Configuration* 드롭다운 목록에서 disabled를 선택합니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

- Disabled — 자동 클라이언트 컨피그레이션을 비활성화합니다.
- IKE Config Pull — 클라이언트에서 컴퓨터의 요청을 설정할 수 있습니다. 컴퓨터에서 Pull 메서드를 지원하면 클라이언트에서 지원하는 설정 목록이 반환됩니다.
- IKE Config Push — 컴퓨터에 컨피그레이션 프로세스를 통해 클라이언트에 설정을 제공할 수 있는 기회를 제공합니다. 컴퓨터에서 Push 메서드를 지원하면 클라이언트에서 지원하는 설정 목록이 반환됩니다.
- DHCP Over IPsec — 클라이언트에서 DHCP over IPsec을 통해 컴퓨터의 설정을 요청할 수 있습니다.

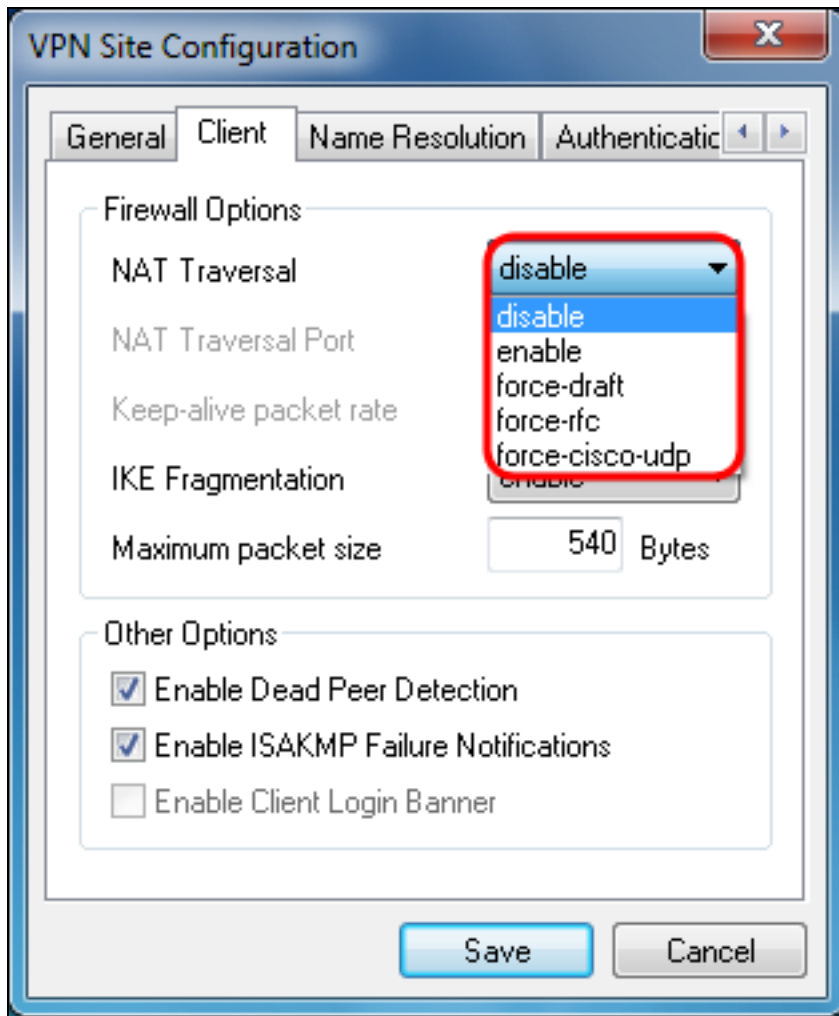
4단계. *Local Host*(로컬 호스트) 섹션의 *Adapter Mode*(어댑터 모드) 드롭다운 목록에서 **Use an existing adapter and current address**(기존 어댑터 및 현재 주소 사용)를 선택합니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

- 가상 어댑터 및 할당된 주소 사용 — 클라이언트가 지정된 주소의 가상 어댑터를 IPsec 통신의 소스로 사용할 수 있습니다.
- 가상 어댑터 및 임의 주소 사용 — 클라이언트가 임의 주소를 가진 가상 어댑터를 IPsec 통신의 소스로 사용할 수 있습니다.
- 기존 어댑터 및 현재 주소 사용 — 클라이언트가 현재 주소를 IPsec 통신의 소스로 사용하는 기존 물리적 어댑터만 사용할 수 있습니다.

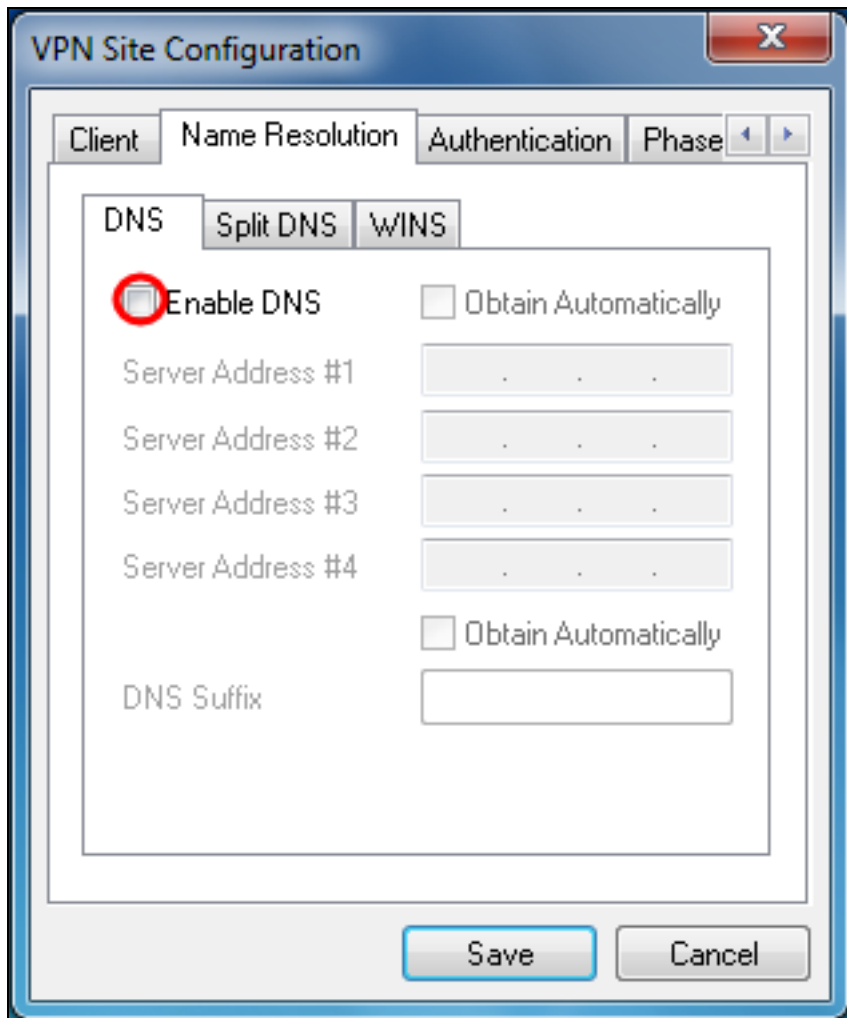
5단계. Client(클라이언트) 탭을 클릭합니다. NAT Traversal 드롭다운 목록에서 RV130/RV130W의 IPsec [VPN Server](#) 기사 컨피그레이션에서 NAT Traversal에 대해 RV130/RV130W [에서 구성한 것과](#) 동일한 설정을 [선택합니다.](#)



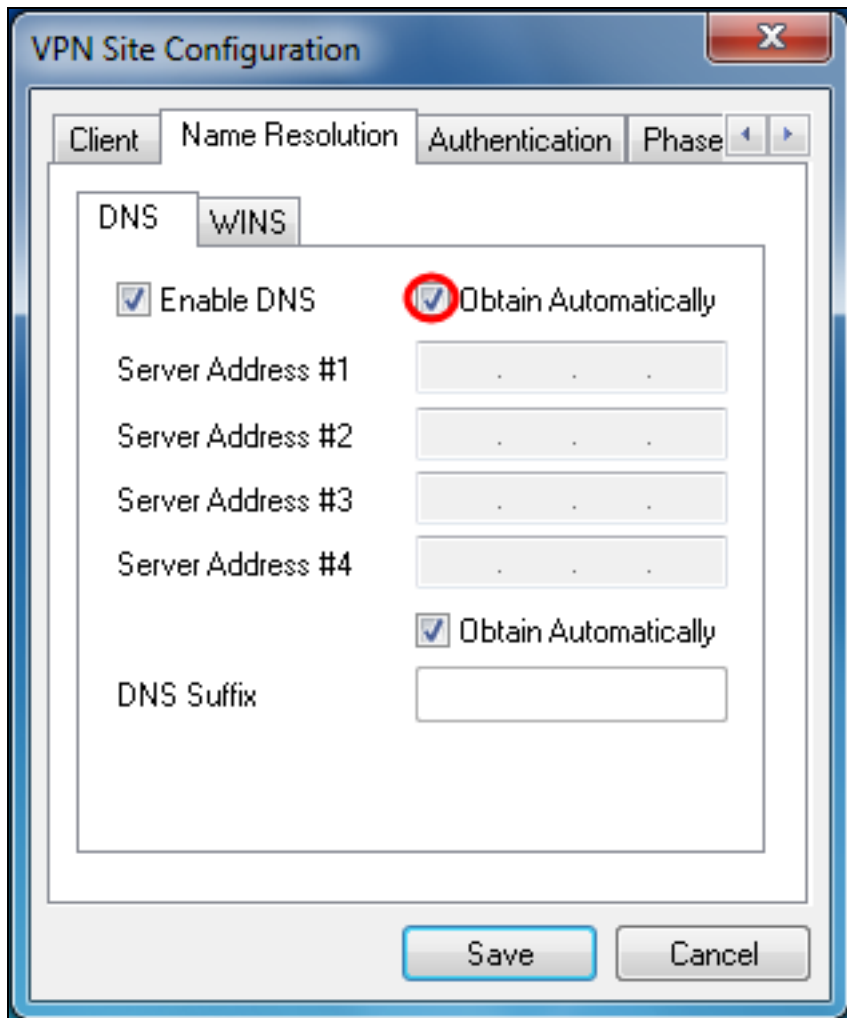
사용 가능한 NAT(Network Address Translation Traversal) 메뉴 옵션은 다음과 같이 정의됩니다.

- Disable — NAT 프로토콜 확장이 사용되지 않습니다.
- Enable — NAT 프로토콜 확장은 협상 중에 VPN 게이트웨이가 지원을 표시하고 NAT가 탐지된 경우에만 사용됩니다.
- Force-Draft — VPN 게이트웨이가 협상 중 지원을 나타내거나 NAT가 탐지되는지 여부에 관계없이 NAT 프로토콜 확장의 초안 버전이 사용됩니다.
- Force-RFC — VPN 게이트웨이가 협상 중 지원을 나타내는지 또는 NAT가 탐지되는지 여부와 상관없이 NAT 프로토콜의 RFC 버전이 사용됩니다.
- Force-Cisco-UDP — NAT가 없는 VPN 클라이언트에 대해 UDP 캡슐화를 강제로 적용합니다.

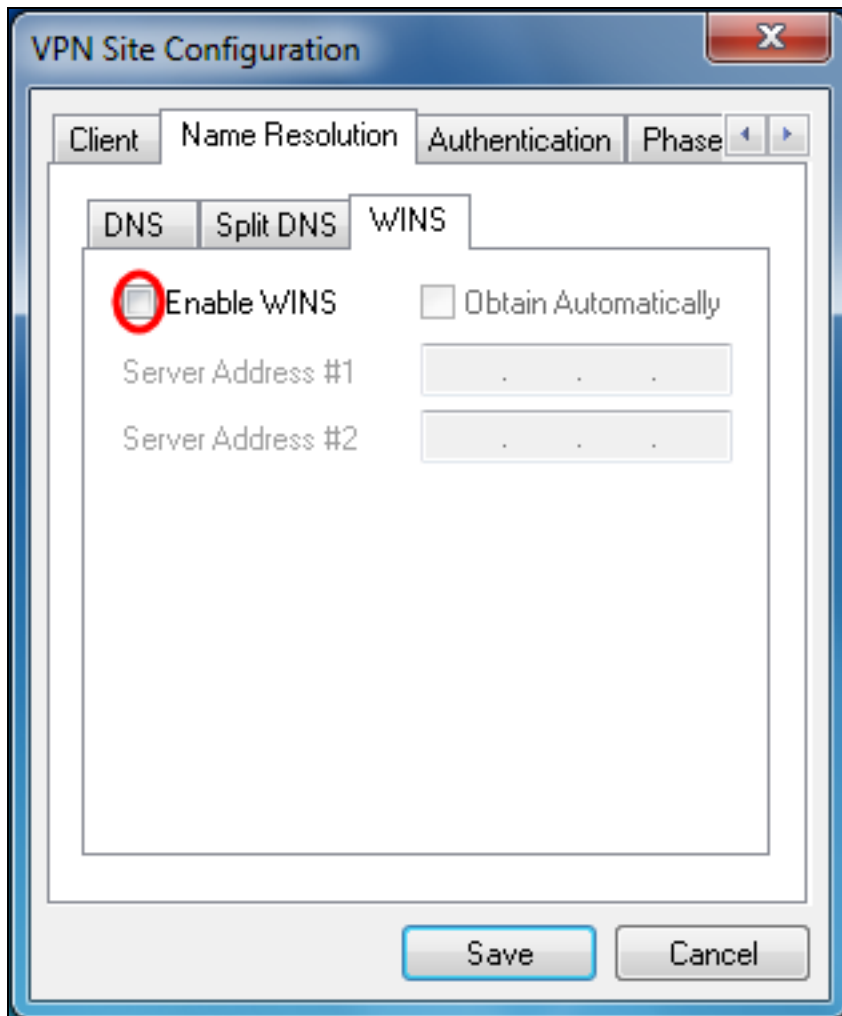
6단계. *Name Resolution(이름 확인)* 탭을 클릭하고 DNS를 **활성화**하려면 Enable DNS(DNS 활성화) 확인란을 선택합니다. 특정 DNS 설정이 사이트 구성에 필요하지 않은 경우 Enable DNS(DNS 활성화) 확인란의 선택을 취소합니다.



7단계. (선택 사항) 원격 게이트웨이가 Configuration Exchange를 지원하도록 구성된 경우 게이트웨이가 DNS 설정을 자동으로 제공할 수 있습니다. 그렇지 않은 경우 Obtain Automatically(자동으로 가져오기) 확인란이 선택되지 않았는지 확인하고 유효한 DNS 서버 주소를 수동으로 입력합니다.

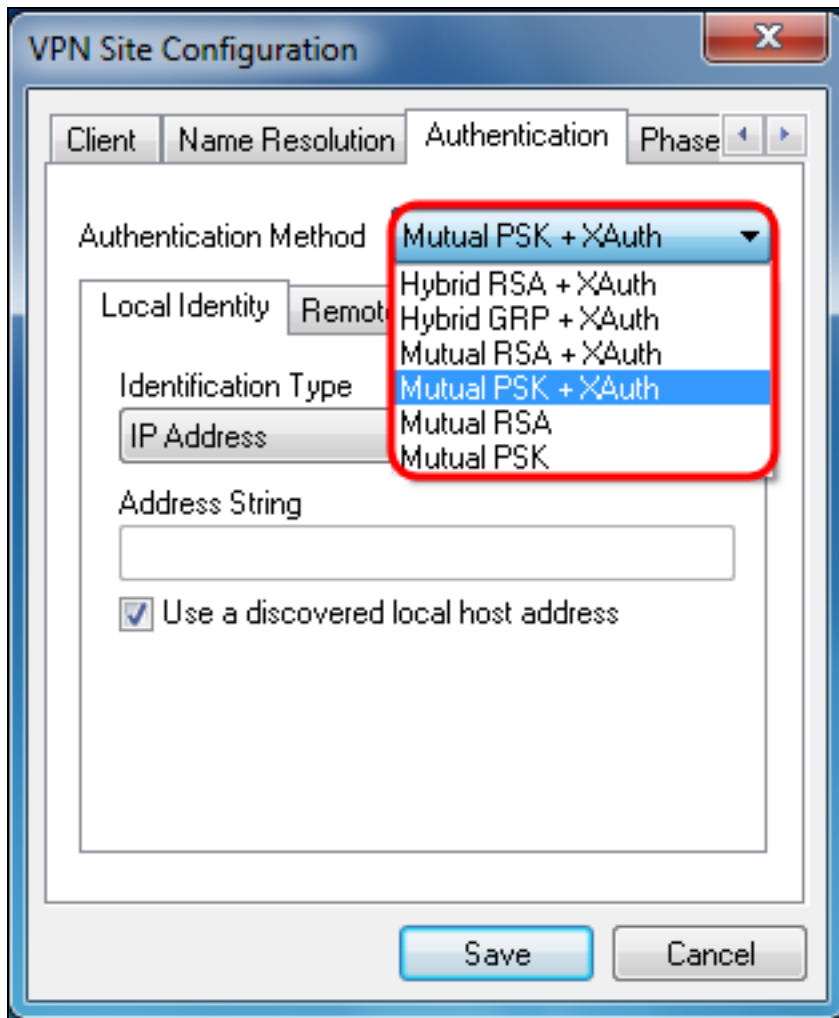


8단계. (선택 사항) WINS(Windows Internet Name Server)를 활성화하려면 *Name Resolution*(이름 확인) 탭을 클릭하고 **Enable WINS**(WINS 활성화) 확인란을 선택합니다. 원격 게이트웨이가 구성 교환을 지원하도록 구성된 경우 게이트웨이는 WINS 설정을 자동으로 제공할 수 있습니다. 그렇지 않은 경우 Obtain Automatically(자동으로 가져오기) **확인란**이 선택되지 않았는지 확인하고 유효한 WINS 서버 주소를 수동으로 입력합니다.



참고: WINS 구성 정보를 제공하면 클라이언트는 원격 개인 네트워크에 있는 서버를 사용하여 WINS 이름을 확인할 수 있습니다. 이 기능은 UNIFORM Naming Convention 경로 이름을 사용하여 원격 Windows 네트워크 리소스에 액세스하려고 시도할 때 유용합니다. WINS 서버는 일반적으로 Windows 도메인 컨트롤러 또는 Samba 서버에 속합니다.

9단계. Authentication(인증) 탭을 클릭하고 Authentication Method(인증 방법) 드롭다운 목록에서 Mutual PSK + XAuth를 선택합니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

·하이브리드 RSA + XAuth — 클라이언트 자격 증명이 필요하지 않습니다. 클라이언트가 게이트웨이를 인증합니다. 자격 증명은 PEM 또는 PKCS12 인증서 파일 또는 키 파일 형식의 형태로 제공됩니다.

·하이브리드 GRP + XAuth — 클라이언트 자격 증명이 필요하지 않습니다. 클라이언트가 게이트웨이를 인증합니다. 자격 증명은 PEM 또는 PKCS12 인증서 파일 및 공유 암호 문자열 형식입니다.

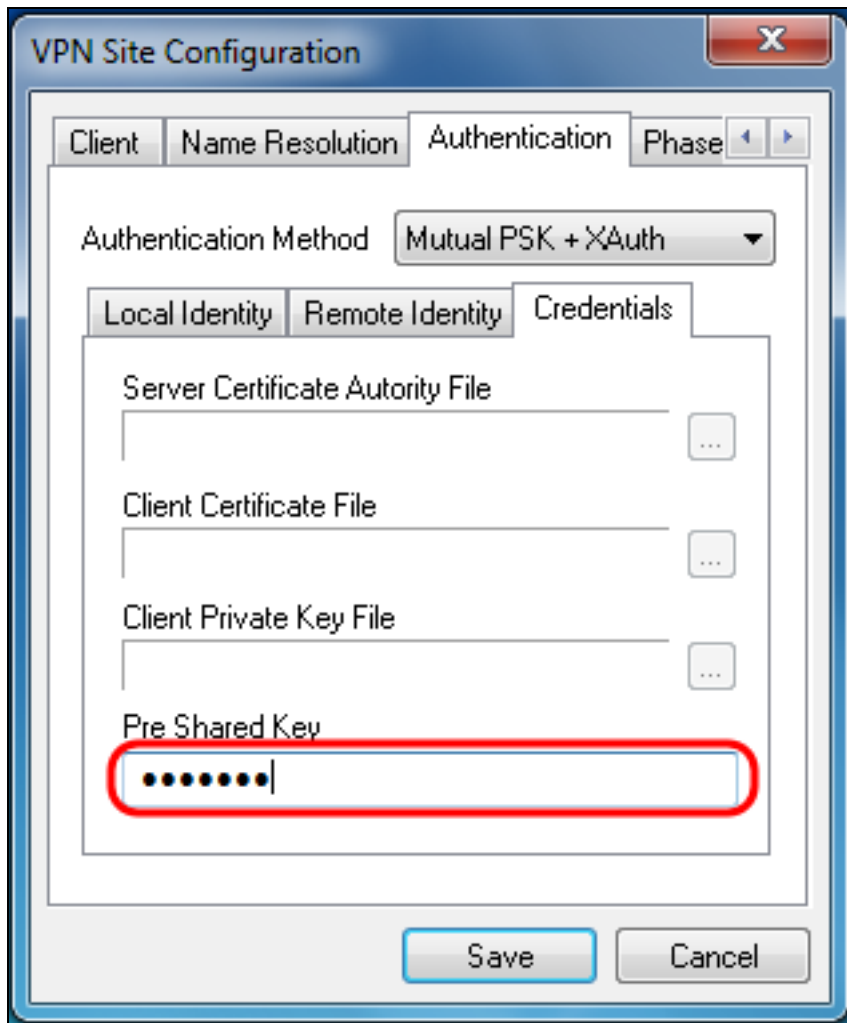
·상호 RSA + XAuth — 클라이언트와 게이트웨이는 모두 인증을 위해 자격 증명이 필요합니다. 자격 증명은 PEM 또는 PKCS12 인증서 파일 또는 키 유형 형식입니다.

·상호 PSK + XAuth — 인증하려면 클라이언트와 게이트웨이 모두에 자격 증명이 필요합니다. 자격 증명은 공유 암호 문자열 형식입니다.

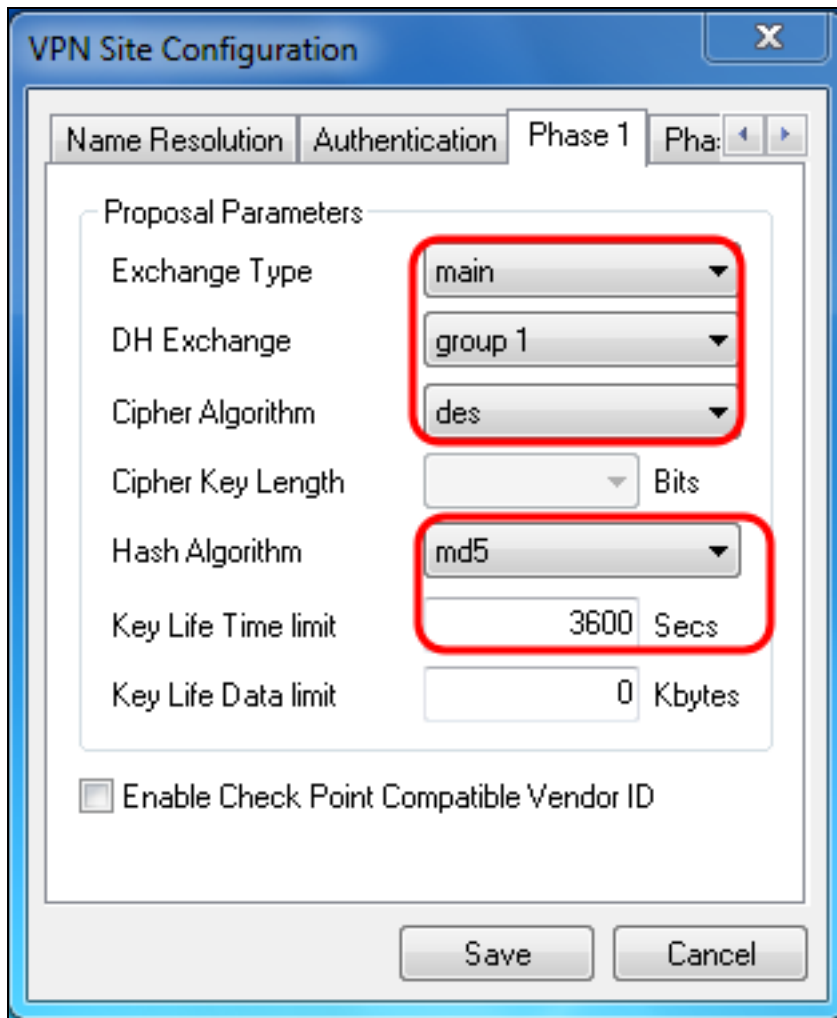
·상호 RSA — 클라이언트와 게이트웨이 모두 인증을 위해 자격 증명이 필요합니다. 자격 증명은 PEM 또는 PKCS12 인증서 파일 또는 키 유형 형식입니다.

·상호 PSK — 인증하려면 클라이언트와 게이트웨이 모두 자격 증명이 필요합니다. 자격 증명은 공유 암호 문자열 형식입니다.

10단계. *Authentication(인증)* 섹션에서 *Credentials(자격 증명)* 하위 탭을 클릭하고 Pre Shared Key(사전 공유 키) 필드의 *IPsec VPN Server Setup(IPsec VPN 서버 설정) 페이지*에서 구성한 것과 동일한 사전 공유 키를 입력합니다.



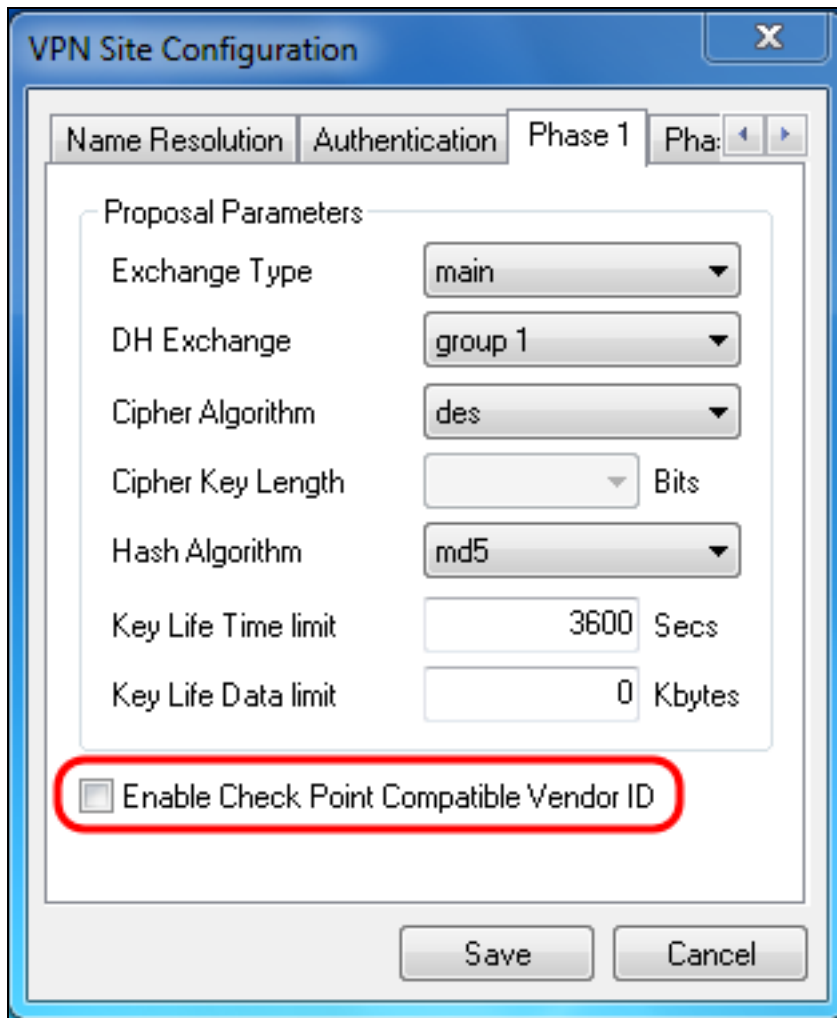
11단계. 1단계 탭을 클릭합니다. 이 문서의 IPsec [VPN Server User Configuration\(IPsec VPN 서버 사용자 컨피그레이션\)](#) 섹션의 2단계에서 RV130/RV130W에 대해 구성한 것과 동일한 설정을 갖도록 다음 매개변수를 구성합니다.



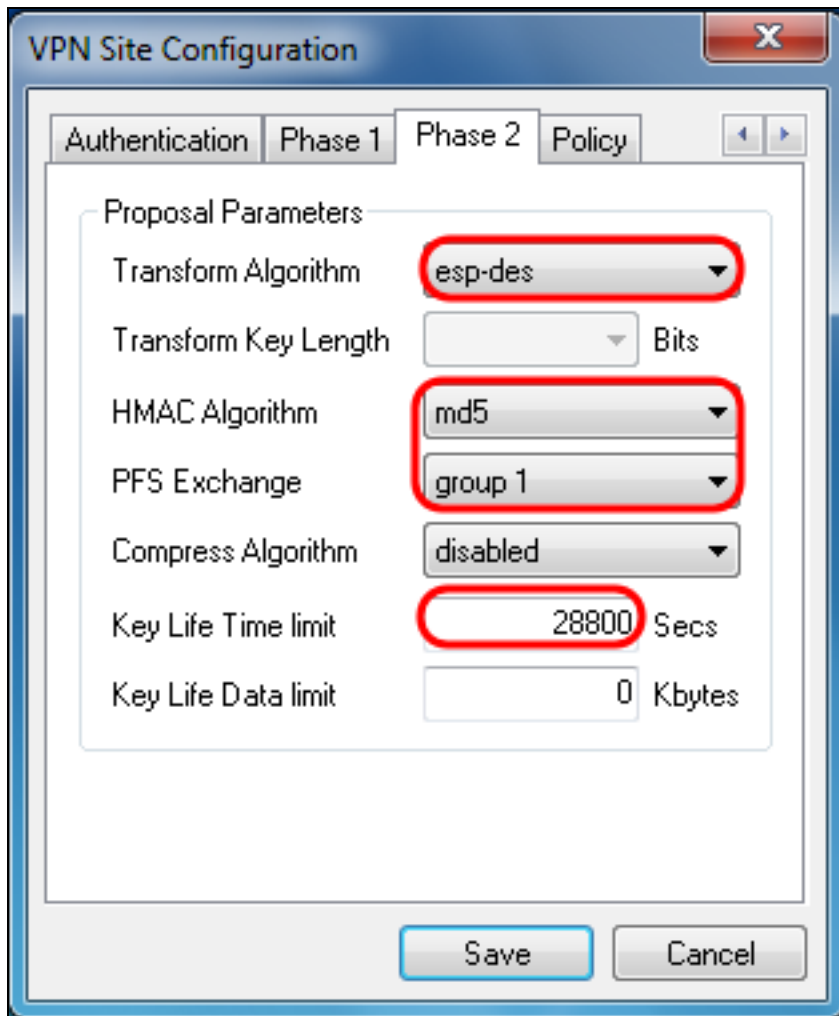
shrew Soft의 매개변수는 다음과 같이 1단계의 RV130/RV130W 구성과 일치해야 합니다.

- "Exchange Type"은 "Exchange Mode"와 일치해야 합니다.
- "DH Exchange"는 "DH Group"과 일치해야 합니다.
- "암호 알고리즘"은 "암호화 알고리즘"과 일치해야 합니다.
- "해시 알고리즘"은 "인증 알고리즘"과 일치해야 합니다.

12단계. (선택 사항) 1단계 협상 중에 게이트웨이에서 Cisco Compatible Vendor ID를 제공하는 경우 **Enable Check Point Compatible Vendor ID(Check Point Compatible Vendor ID 활성화)** 확인란을 선택합니다. 게이트웨이가 없거나 확실하지 않은 경우 확인란을 선택하지 않은 상태로 둡니다.



13단계. 2단계 탭을 클릭합니다. 이 문서의 IPsec [VPN Server User Configuration\(IPsec VPN 서버 사용자 컨피그레이션\)](#) 섹션의 2단계에서 RV130/RV130W에 대해 구성한 것과 동일한 설정을 갖도록 다음 매개변수를 구성합니다.



shrew Soft의 매개변수는 다음과 같이 2단계의 RV130/RV130W 구성과 일치해야 합니다.

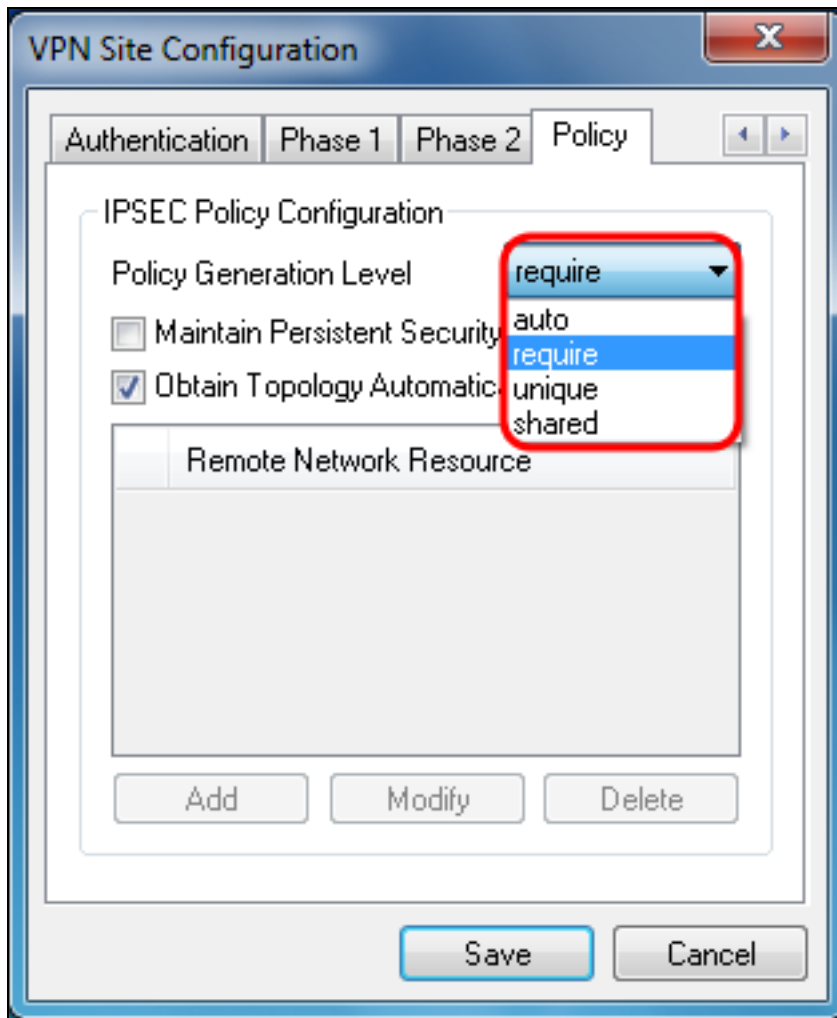
- "Transform Algorithm"은 "Encryption Algorithm"과 일치해야 합니다.

- "HMAC 알고리즘"은 "인증 알고리즘"과 일치해야 합니다.

- RV130/RV130W에서 PFS 키 그룹이 활성화된 경우 PFS Exchange"는 "DH 그룹"과 일치해야 합니다. 그렇지 않으면 disabled를 선택합니다.

- "Key Life Time limit"은 "IPSec SA Lifetime"과 일치해야 합니다.

14단계. *Policy*(정책) 탭을 클릭하고 *Policy Generation Level*(정책 생성 레벨) 드롭다운 목록에서 *require*(필요)를 선택합니다. *Policy Generation Level* 옵션은 IPsec 정책이 생성되는 수준을 수정합니다. 드롭다운 목록에 제공된 여러 레벨은 여러 공급업체 구현으로 구현된 IPsec SA 협상 동작에 매핑됩니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

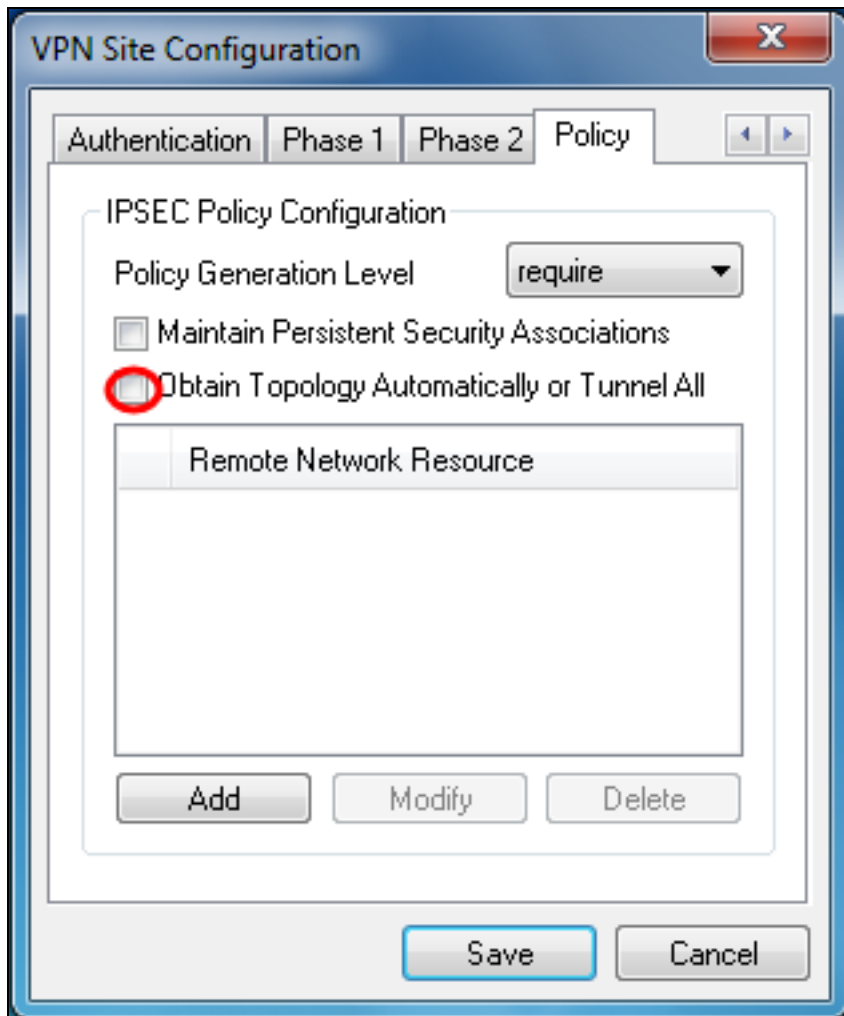
·자동 — 클라이언트가 자동으로 적절한 IPsec 정책 수준을 결정합니다.

·필요 — 클라이언트가 각 정책에 대해 고유한 SA(Security Association)를 협상하지 않습니다. 로컬 공용 주소를 로컬 정책 ID로 사용하고 원격 네트워크 리소스를 원격 정책 ID로 사용하여 정책이 생성됩니다. 2단계 제안에서는 협상 중에 정책 ID를 사용합니다.

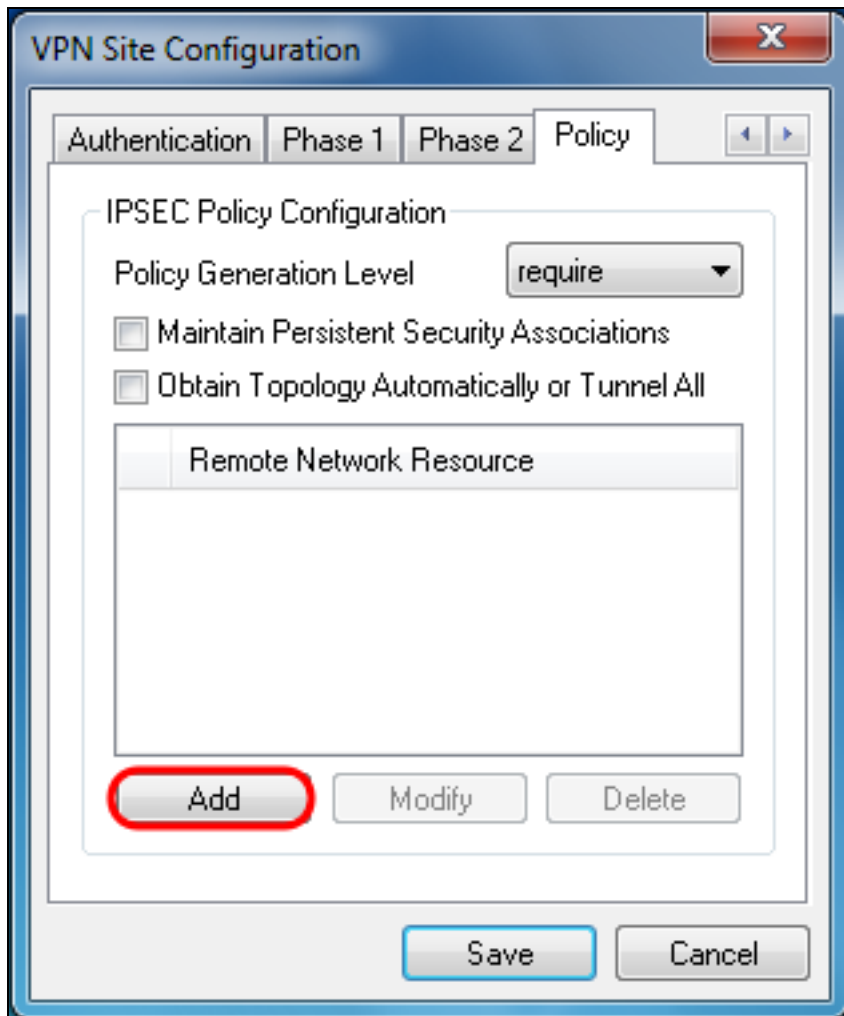
·Unique — 클라이언트가 각 정책에 대해 고유한 SA를 협상합니다.

·공유 - 필요한 수준에서 정책이 생성됩니다. 2단계 제안에서는 협상 중에 로컬 정책 ID를 로컬 ID로 사용하고 Any(0.0.0.0/0)를 원격 ID로 사용합니다.

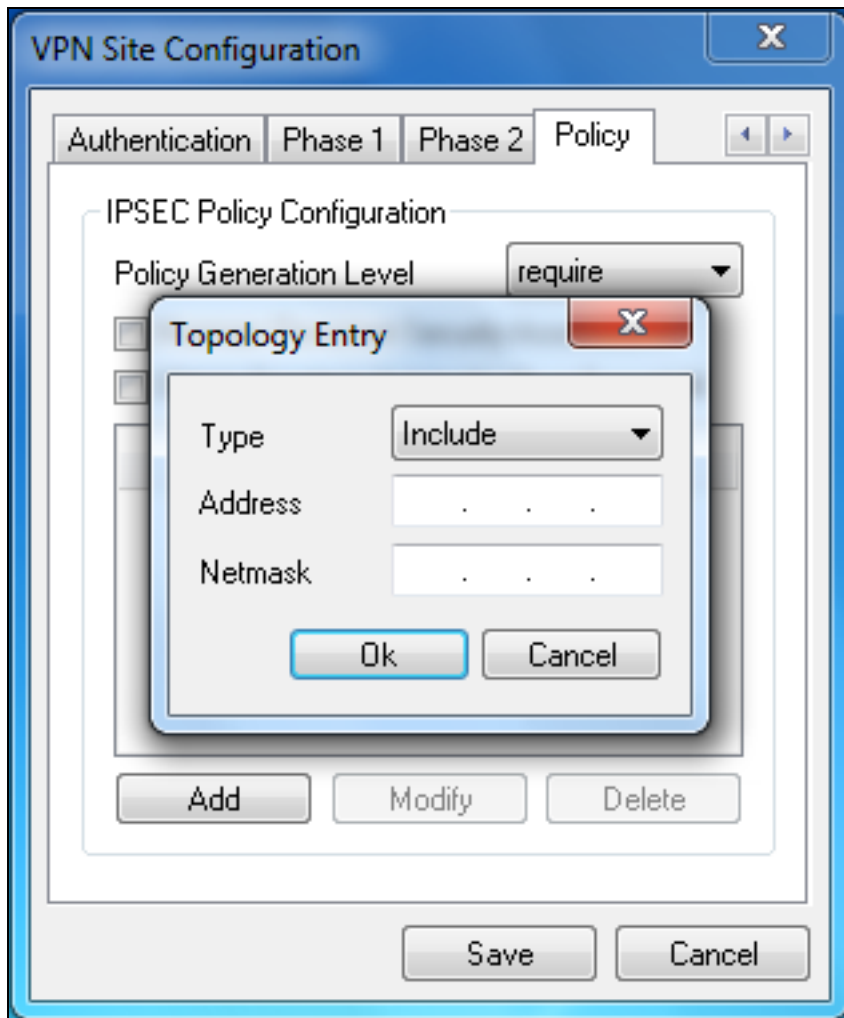
15단계. Obtain Topology Automatically or Tunnel All **확인란**의 선택을 취소합니다. 이 옵션은 연결에 대해 보안 정책을 구성하는 방법을 수정합니다. 비활성화하면 수동 컨피그레이션을 수행해야 합니다. 활성화되면 자동 컨피그레이션이 수행됩니다.



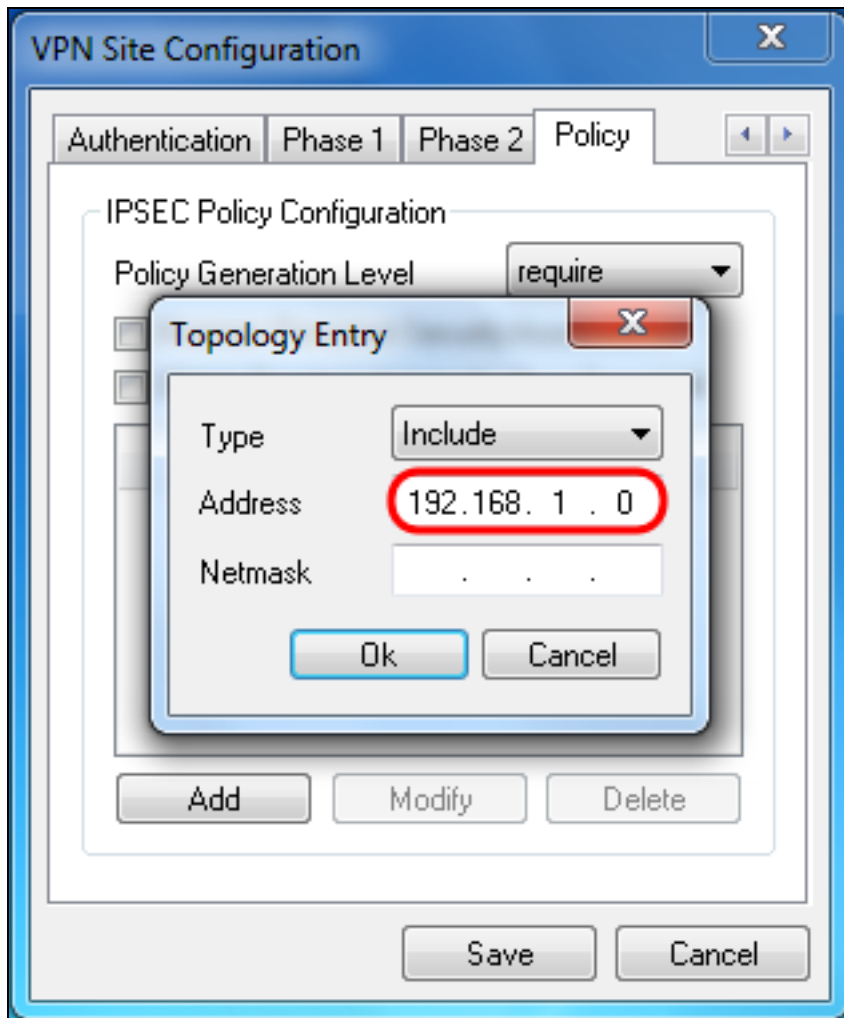
16단계. 연결할 원격 네트워크 리소스를 추가하려면 Add를 클릭합니다. 원격 네트워크 리소스는 원격 데스크톱 액세스, 부서별 리소스, 네트워크 드라이브, 보안 전자 메일 등이 있습니다.



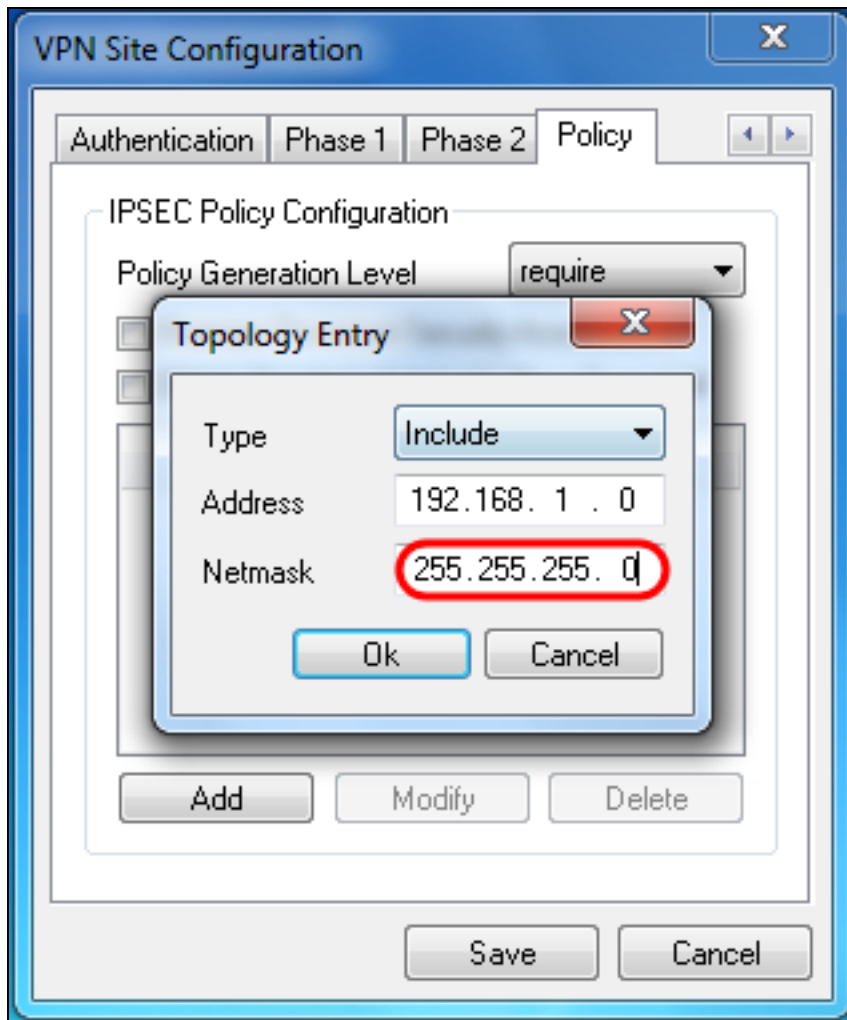
Topology *Entry* 창이 나타납니다.



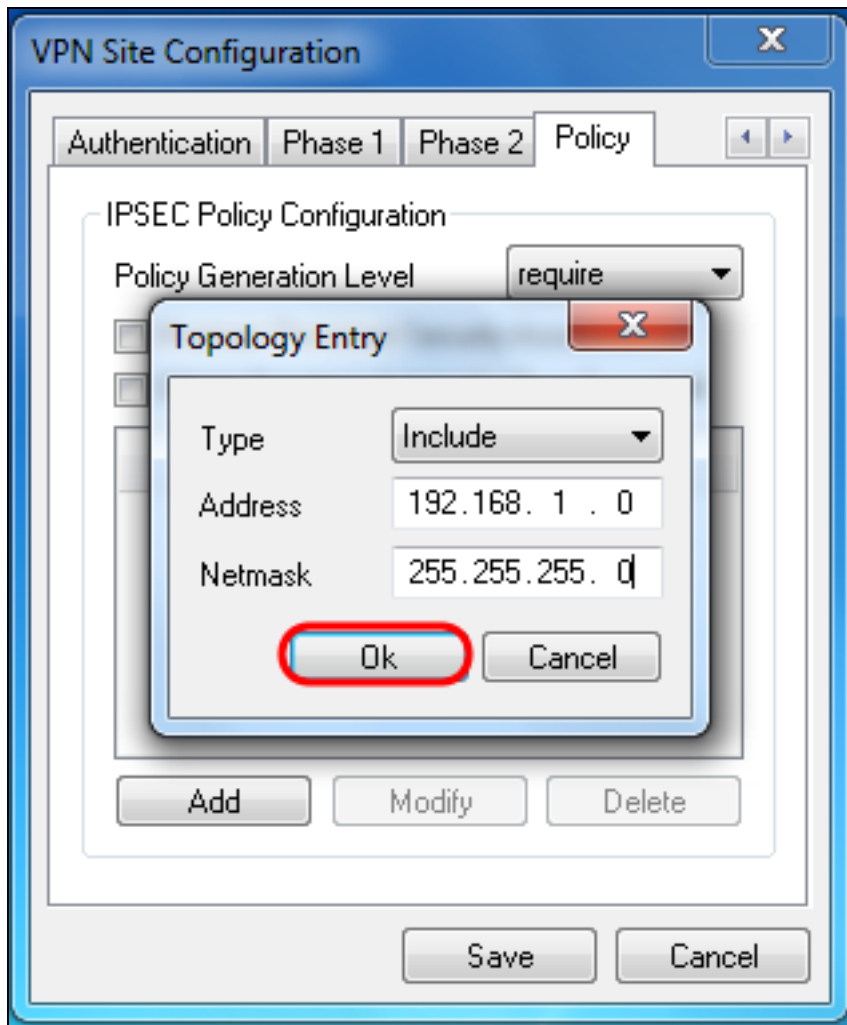
17단계. 주소 필드에 RV130/RV130W의 서브넷 ID를 입력합니다. 주소는 이 문서의 IPsec [VPN Server Setup and User Configuration\(IPsec VPN 서버 설정 및 사용자 컨피그레이션\) 섹션의 2단계](#)에서 IP Address(IP 주소) 필드와 일치해야 합니다.



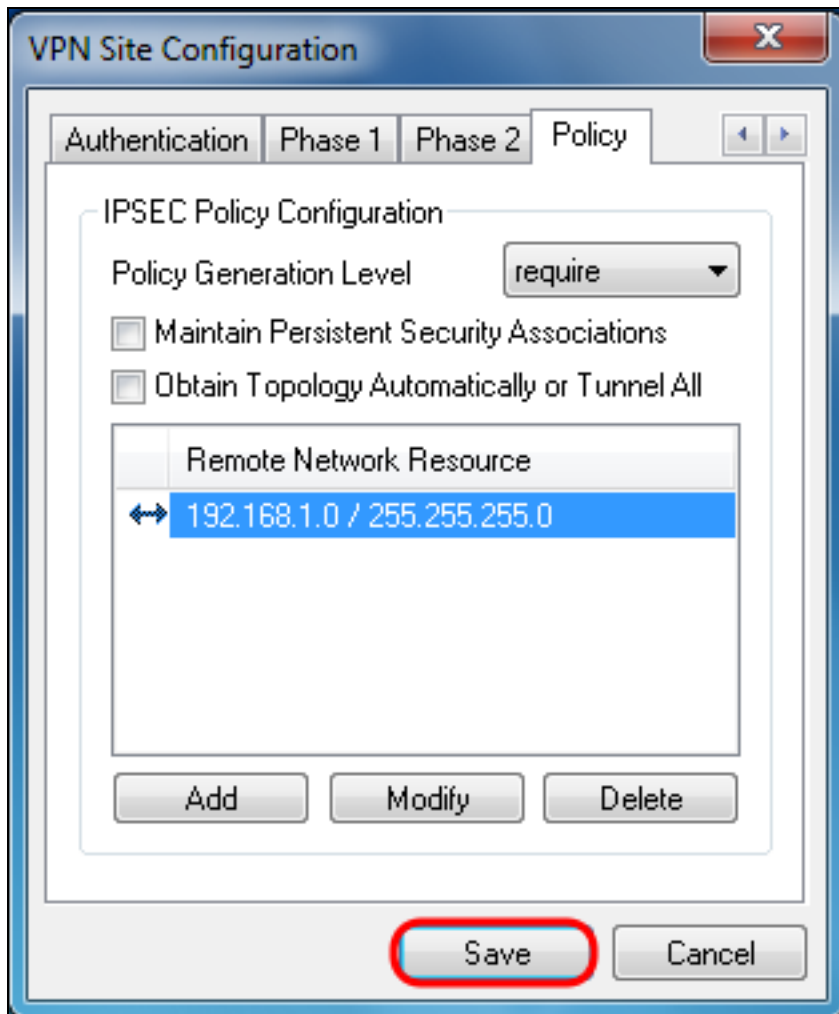
18단계. Netmask(넷마스크) 필드에 RV130/RV130W의 로컬 네트워크에 대한 서브넷 마스크를 입력합니다. 넷마스크는 이 문서의 IPsec [VPN 서버 사용자 구성 섹션의 2단계](#)에서 [서브넷 마스크 필드](#)와 일치해야 합니다.



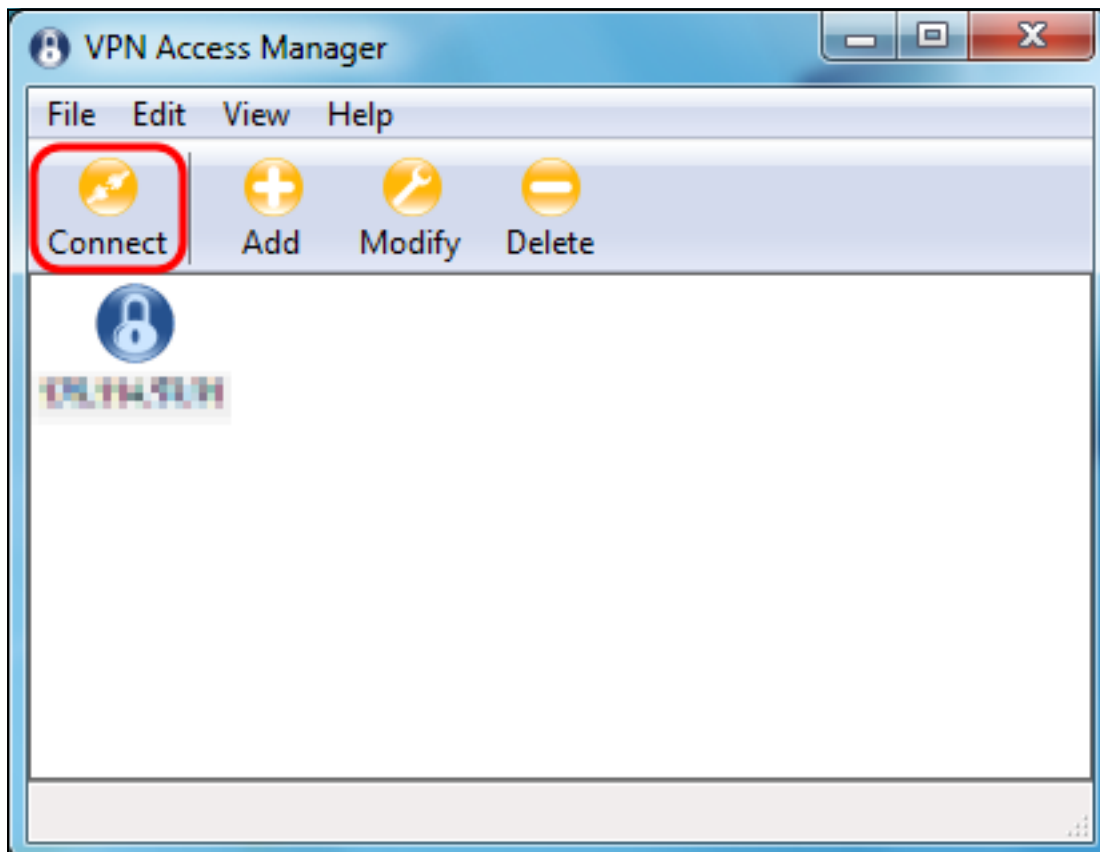
19단계. **확인**을 클릭하여 원격 네트워크 리소스 추가를 완료합니다.



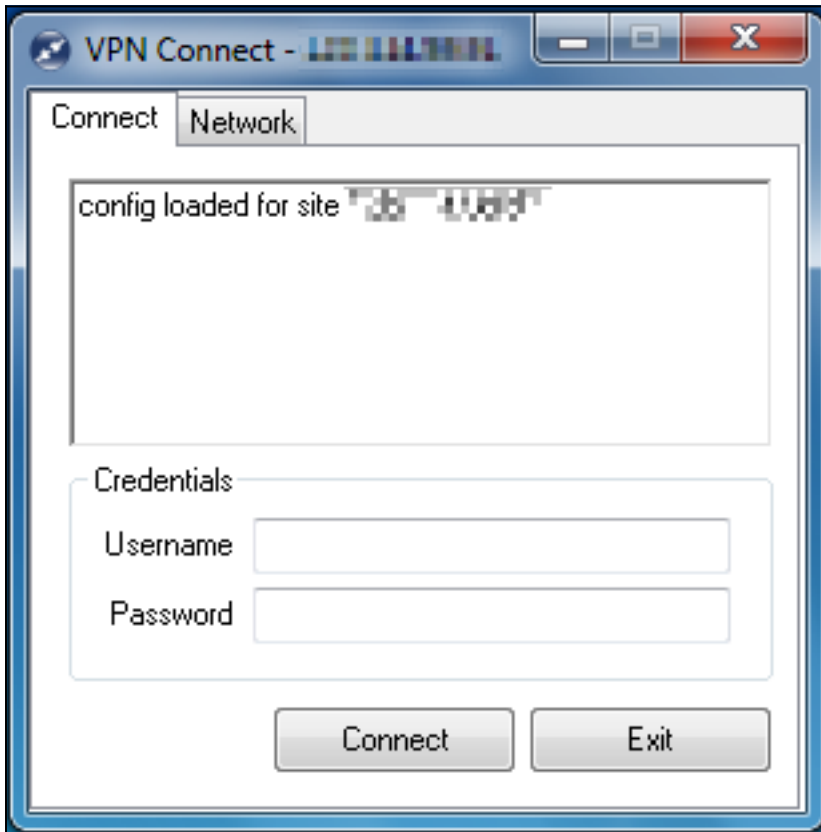
20단계. **Save(저장)**를 클릭하여 VPN 사이트에 연결하기 위한 구성을 저장합니다.



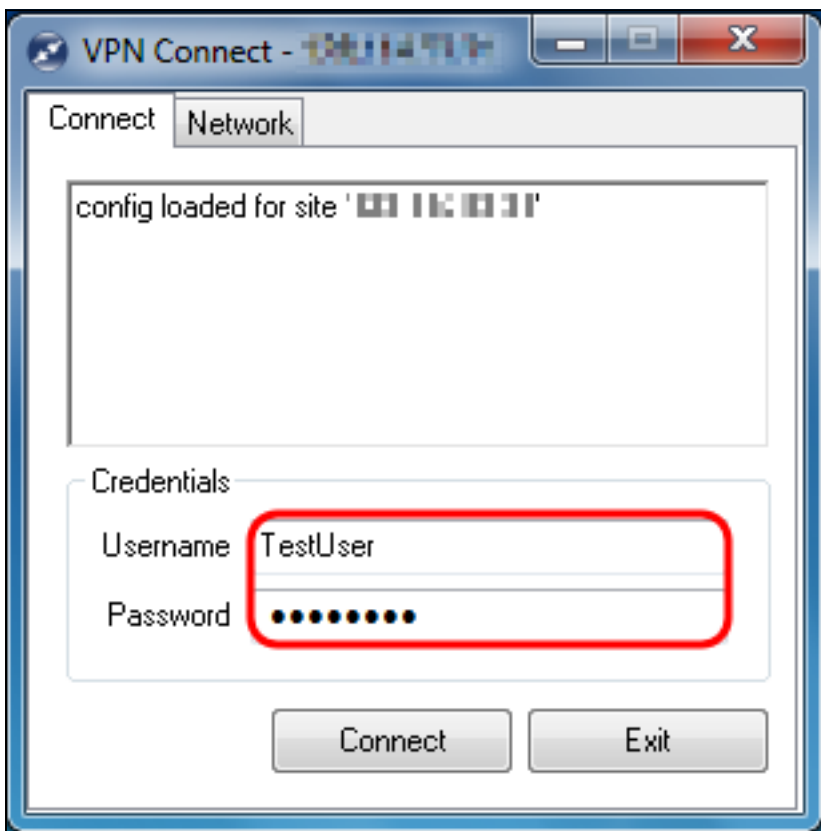
21단계. VPN Access Manager 창으로 돌아가서 구성한 VPN 사이트를 선택하고 Connect(연결) 버튼을 클릭합니다.



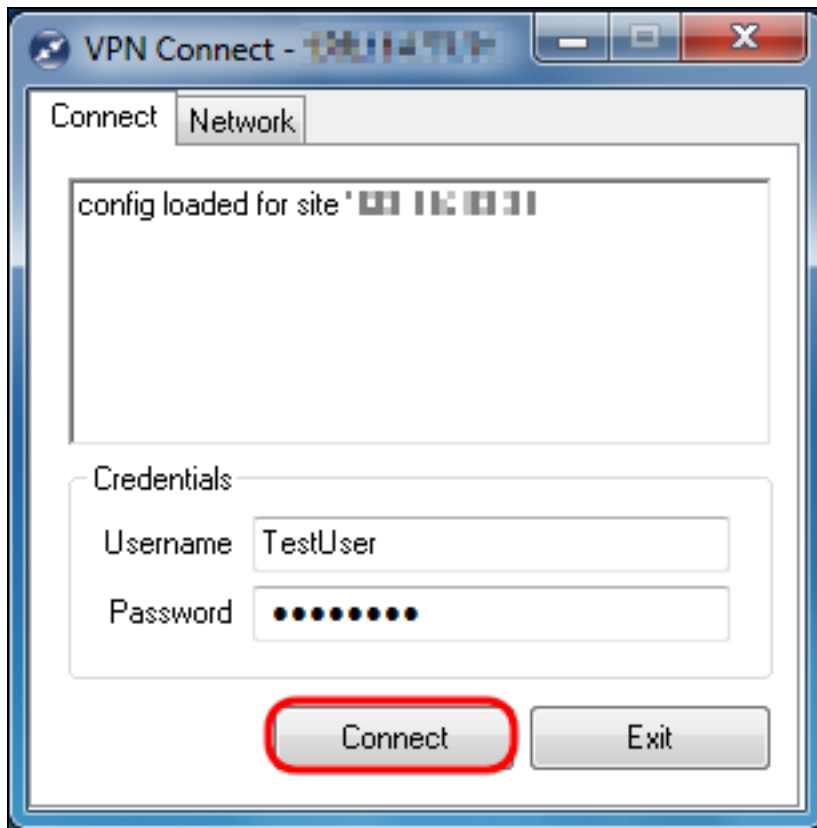
VPN Connect(VPN 연결) 창이 나타납니다.



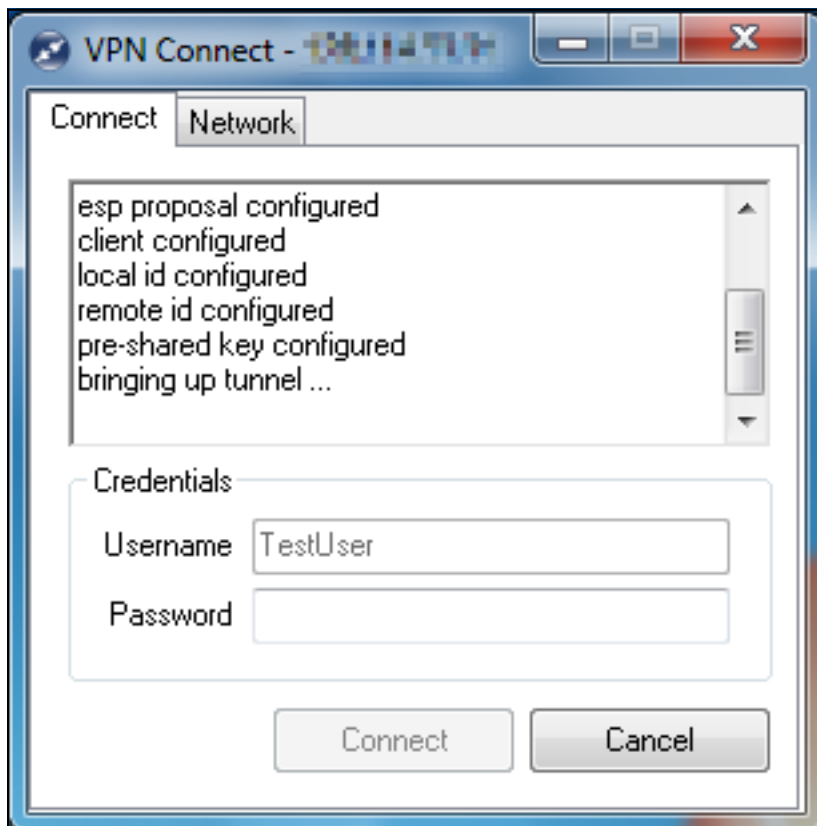
22단계. Credentials(자격 증명) 섹션에서 이 문서의 IPsec [VPN Server User Configuration\(IPsec VPN 서버 사용자 컨피그레이션\) 섹션의 4단계](#)에서 설정한 계정의 사용자 이름 및 비밀번호를 입력합니다.

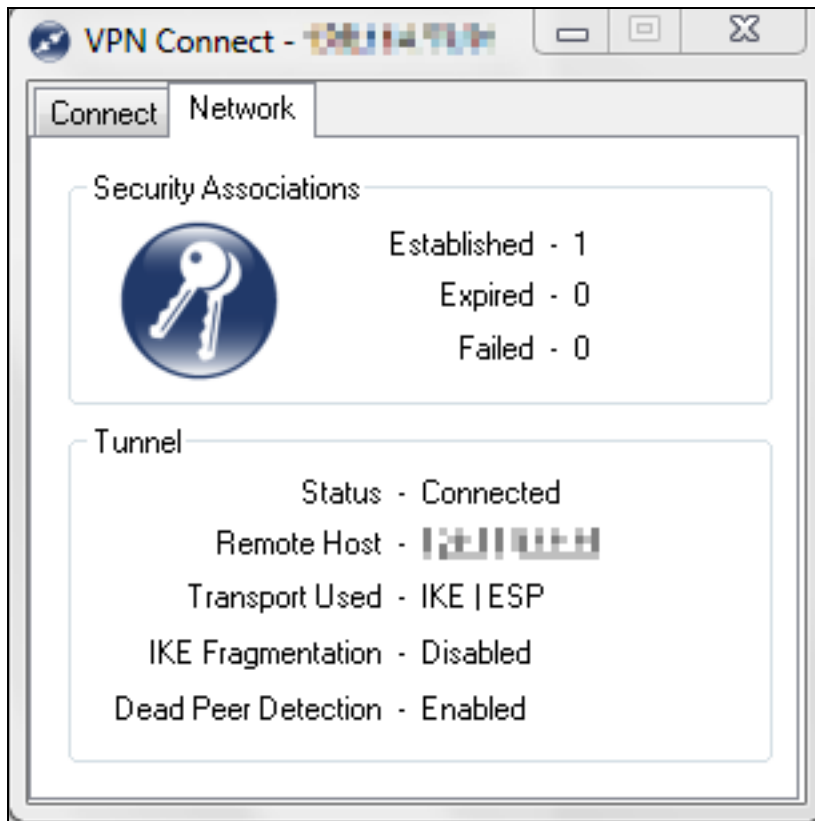


23단계. RV130/RV130W에 VPN에 **연결** 을 클릭합니다.



IPSec VPN 터널이 설정되고 VPN 클라이언트는 RV130/RV130W LAN 뒤의 리소스에 액세스할 수 있습니다.





[이 문서 관련 비디오 보기...](#)

[Cisco의 다른 기술 상답을 보려면 여기를 클릭하십시오.](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.