

RV34X Series Router에 연결하도록 Shrew Soft VPN 클라이언트 구성

목표

이 문서의 목적은 Shrew Soft VPN 클라이언트를 사용하여 RV340 Series 라우터에 연결하는 방법을 보여 주는 것입니다.

shrew Soft VPN 클라이언트 소프트웨어의 최신 버전을 여기에서 다운로드할 수 있습니다.

<https://www.shrew.net/download/vpn>

적용 가능한 디바이스 | 소프트웨어 버전

RV340 | 1.0.3.17 ([최신 다운로드](#))

RV340W | 1.0.3.17([최신 다운로드](#))

RV345 | 1.0.3.17([최신 다운로드](#))

RV345P | 1.0.3.17([최신 다운로드](#))

소개/활용 사례

IPSec VPN(Virtual Private Network)을 사용하면 인터넷을 통해 암호화된 터널을 설정하여 원격 리소스를 안전하게 확보할 수 있습니다.RV34X 시리즈 라우터는 IPSEC VPN 서버로 작동하며 Shrew Soft VPN Client를 지원합니다.이 가이드에서는 라우터와 Shrew Soft Client를 구성하여 VPN에 대한 연결을 보호하는 방법을 보여줍니다.

이 문서는 두 부분으로 구성됩니다.

RV340 Series 라우터 구성

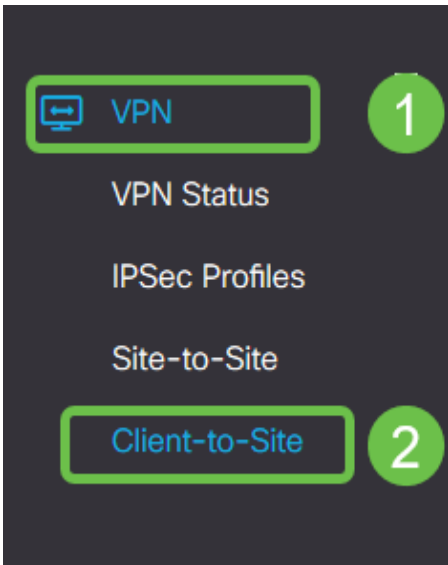
shrew Soft VPN 클라이언트 구성

RV34X Series 라우터를 구성합니다.

먼저 RV34x에서 Client-to-Site VPN을 구성합니다.

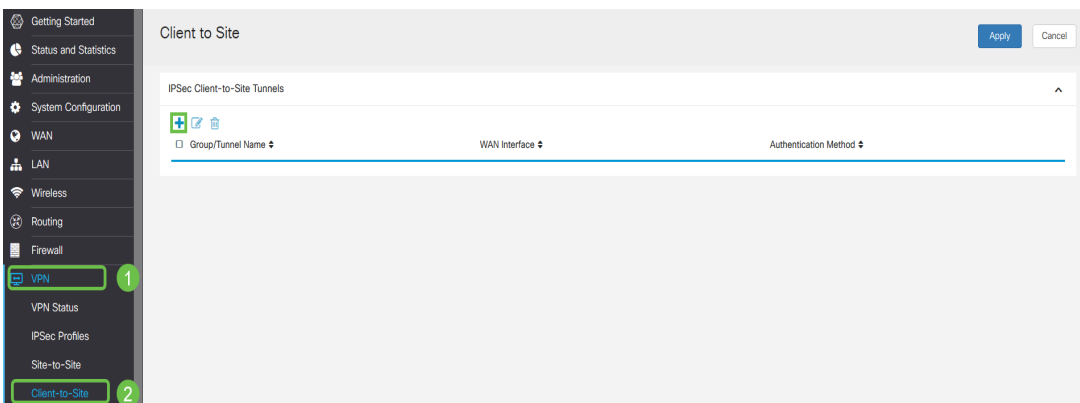
1단계

VPN > Client-to-Site에서



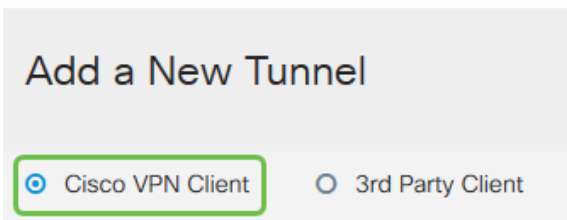
2단계

클라이언트 대 사이트 VPN 프로파일 추가



3단계

Cisco VPN Client 옵션을 선택합니다.



4단계

Enable(활성화) 확인란을 선택하여 VPN 클라이언트 프로파일을 활성화합니다. 또한 그룹 이름을 구성하고 WAN 인터페이스를 선택한 다음 사전 공유 키를 입력하겠습니다.

참고: 그룹 이름 및 사전 공유 키는 나중에 클라이언트를 구성할 때 사용되므로 주의하십시오.

Enable:

Group Name:

Interface:

IKE Authentication Method

Pre-shared Key:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

5단계

사용자 그룹 테이블을 비워둡니다. 라우터의 사용자 그룹에 대한 것이지만 아직 구성하지 않았습니다. Mode(모드)가 Client(클라이언트)로 설정되었는지 확인합니다. 클라이언트 LAN 풀 범위를 입력합니다. 172.16.10.1~172.16.10.10을 사용하겠습니다

참고: 풀 범위는 네트워크의 다른 곳에서 사용되지 않는 고유한 서브넷을 사용해야 합니다.

User Group:

User Group Table

+

Mode: Client NEM

Pool Range for Client LAN

Start IP:

End IP:

6단계

여기서 모드 컨피그레이션 설정을 구성합니다. 사용할 설정은 다음과 같습니다.

기본 DNS 서버: 내부 DNS 서버가 있거나 외부 DNS 서버를 사용하려는 경우 여기에 입력할 수 있습니다. 그렇지 않으면 기본값은 RV340 LAN IP 주소로 설정됩니다. 여기서는 기본값을 사용합니다.

스플릿 터널: 스플릿 터널링을 활성화하려면 선택합니다. VPN 터널을 통해 이동할 트래픽을 지정하는 데 사용됩니다. 여기서는 스플릿 터널을 사용합니다.

분할 터널 테이블: VPN 클라이언트가 VPN을 통해 액세스할 수 있는 네트워크를 입력합니다. 이 예에서는 RV340 LAN 네트워크를 사용합니다.

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain:

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Split Tunnel:

Split Tunnel Table

7단계

Save(저장)를 클릭한 후 IPsec Client-to-Site Groups(IPsec 클라이언트-사이트 그룹) 목록에서 Profile(프로필)을 볼 수 있습니다.

Client to Site

IPsec Client-to-Site Tunnels

Group/Tunnel Name	WAN Interface	Authentication Method
Clients	WAN1	Pre-shared Key

8단계

이제 VPN 클라이언트 사용자 인증에 사용할 사용자 그룹을 구성합니다. System Configuration(시스템 컨피그레이션) > User Groups(사용자 그룹)에서 '+'를 클릭하여 사용자 그룹을 추가합니다.

- Status and Statistics
- Administration
- System Configuration
- System
- Time
- Log
- Email
- User Accounts
- User Groups

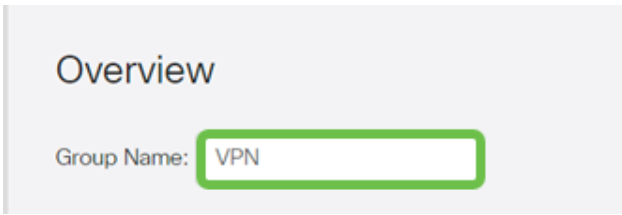
User Groups

User Groups Table

Group	Web Login/NETCONF/RESTCONF
admin	Admin
guest	Disabled

9단계

그룹 이름을 입력합니다.

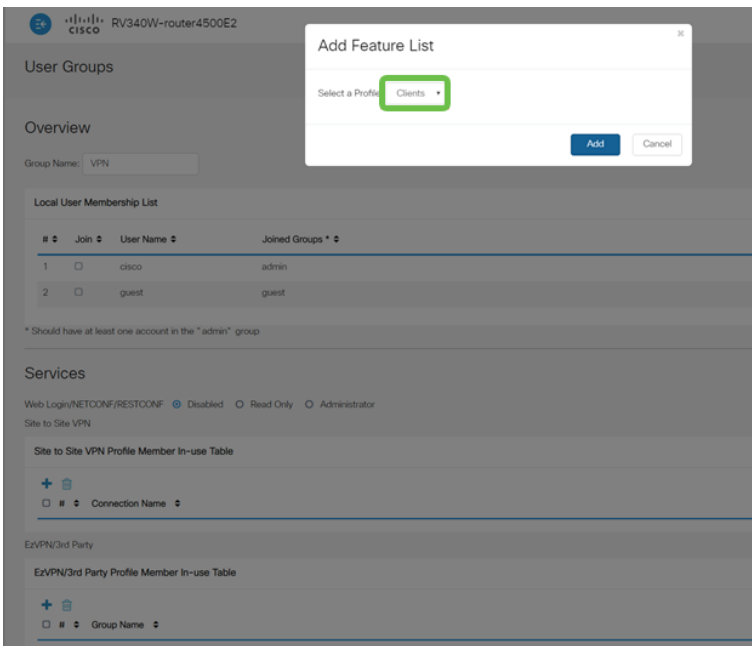


Overview

Group Name:

10단계

Services(서비스) 섹션 > EzVPN/3rd Party(EzVPN/서드파티)에서 Add(추가)를 클릭하여 이 사용자 그룹을 이전에 구성한 Client-to-Site Profile(클라이언트-사이트 간 프로필)에 연결합니다.



Add Feature List

Select a Profile:

Buttons: Add, Cancel

User Groups Overview

Group Name: VPN

Local User Membership List

#	Join	User Name	Joined Groups
1	<input type="checkbox"/>	cisco	admin
2	<input type="checkbox"/>	guest	guest

* Should have at least one account in the "admin" group

Services

Web Login/NETCONF/RESTCONF: Disabled, Read Only, Administrator

Site to Site VPN

Site to Site VPN Profile Member In-use Table

#	Connection Name
---	-----------------

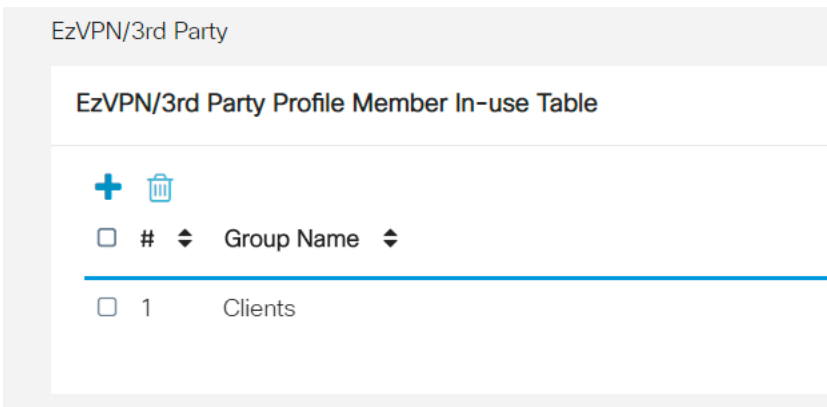
EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

#	Group Name
---	------------

11단계

이제 EzVPN/타사의 목록에 Client-to-Site Group Name이 표시되어야 합니다.



EzVPN/3rd Party

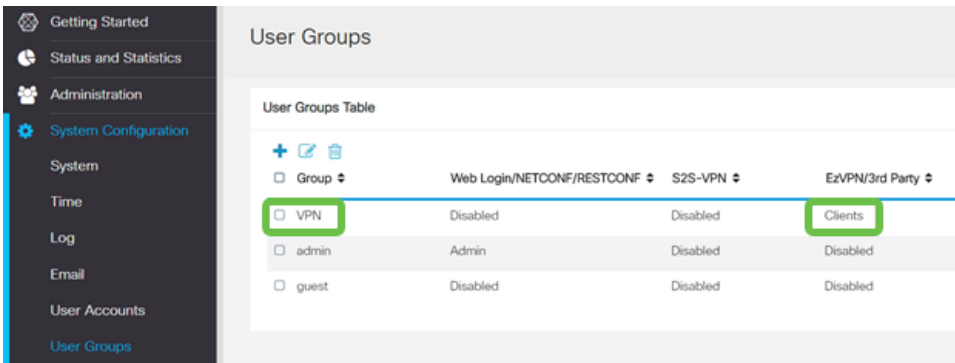
EzVPN/3rd Party Profile Member In-use Table

Buttons: +, -

#	Group Name
1	Clients

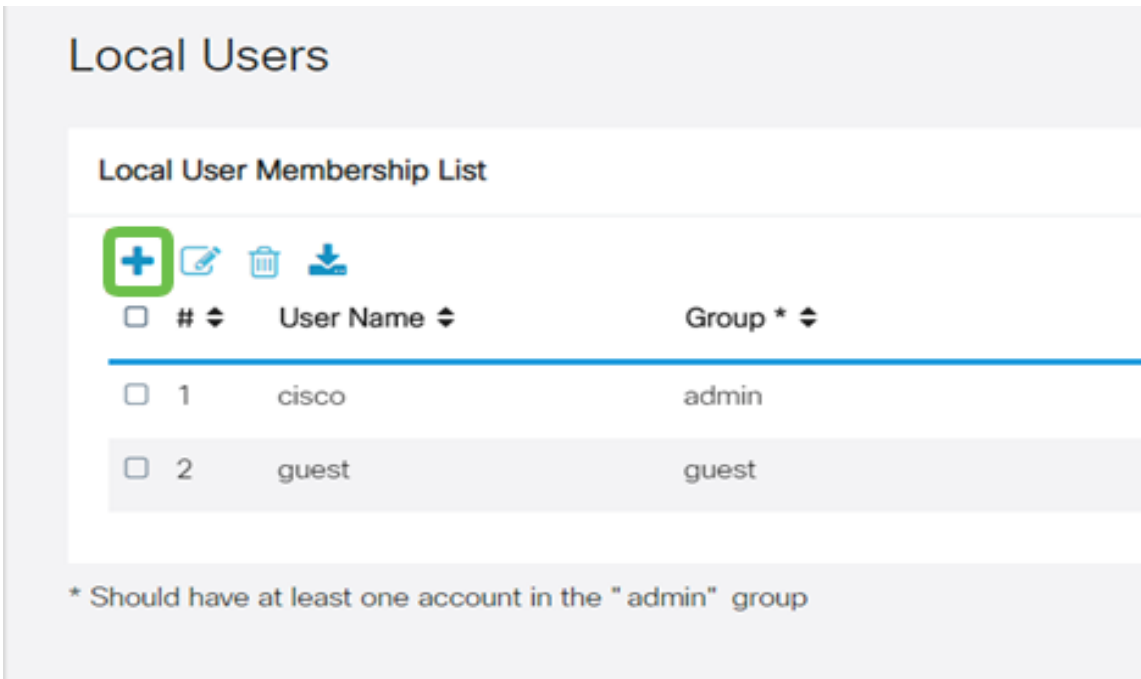
12단계

사용자 그룹 컨피그레이션을 적용한 후 사용자 그룹 목록에 해당 컨피그레이션이 표시되고 새 사용자 그룹이 이전에 생성한 클라이언트-사이트 프로필과 함께 사용됨을 표시합니다.



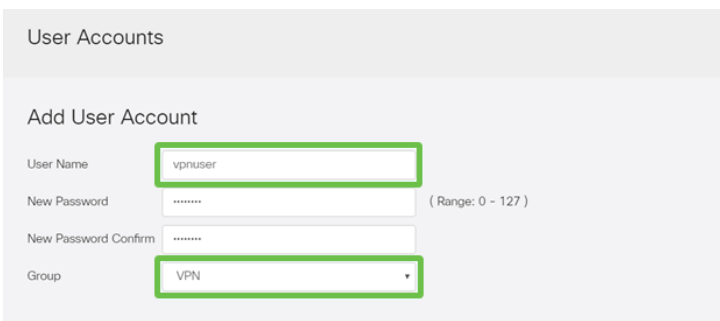
13단계

이제 System Configuration(시스템 컨피그레이션) > User Accounts(사용자 계정)에서 새 사용자를 구성합니다. '+'를 클릭하여 새 사용자를 생성합니다.



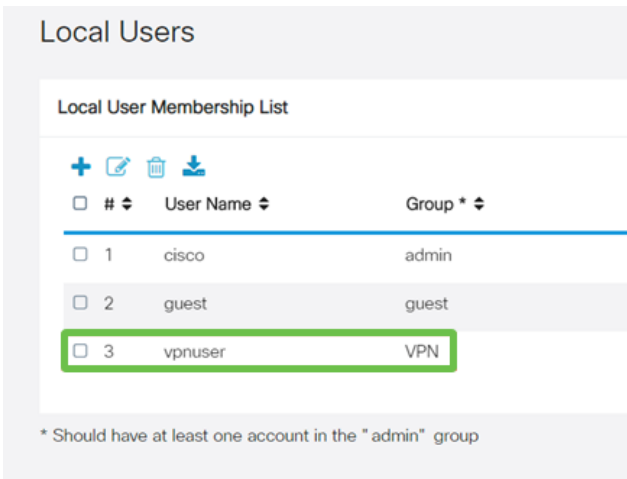
14단계

새 사용자 이름과 새 비밀번호를 입력합니다. 그룹이 방금 구성한 새 사용자 그룹으로 설정되어 있는지 확인합니다. 완료되면 Apply를 클릭합니다.



15단계

새 사용자가 로컬 사용자 목록에 표시됩니다.



이렇게 하면 RV340 Series 라우터의 컨피그레이션이 완료됩니다. 이제 Shrew Soft VPN 클라이언트를 구성합니다.

뒤쥬Soft VPN 클라이언트 구성

이제 Shrew Soft VPN 클라이언트를 구성합니다.

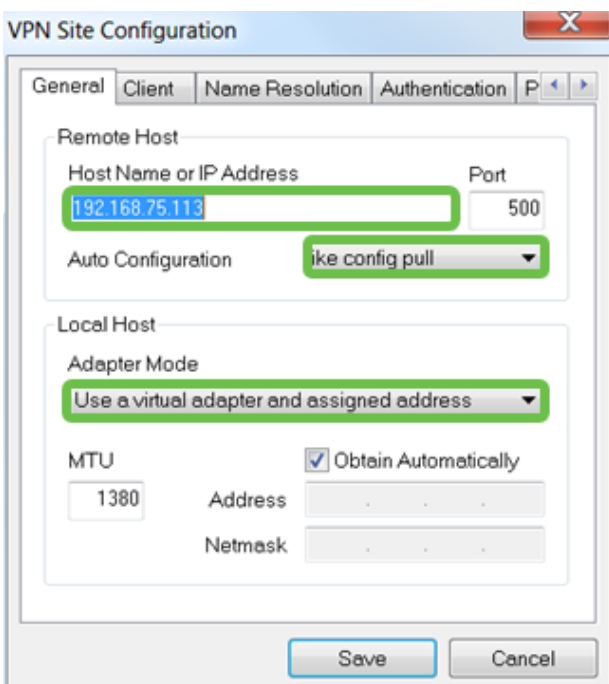
1단계

뒤쥬Soft *VPN Access Manager*를 열고 **Add**를 클릭하여 프로필을 추가합니다. 나타나는 *VPN Site Configuration*(VPN 사이트 컨피그레이션) 창에서 **General**(일반) 탭을 구성합니다.

호스트 이름 또는 IP 주소: WAN ip 주소(또는 RV340의 호스트 이름)를 사용합니다.

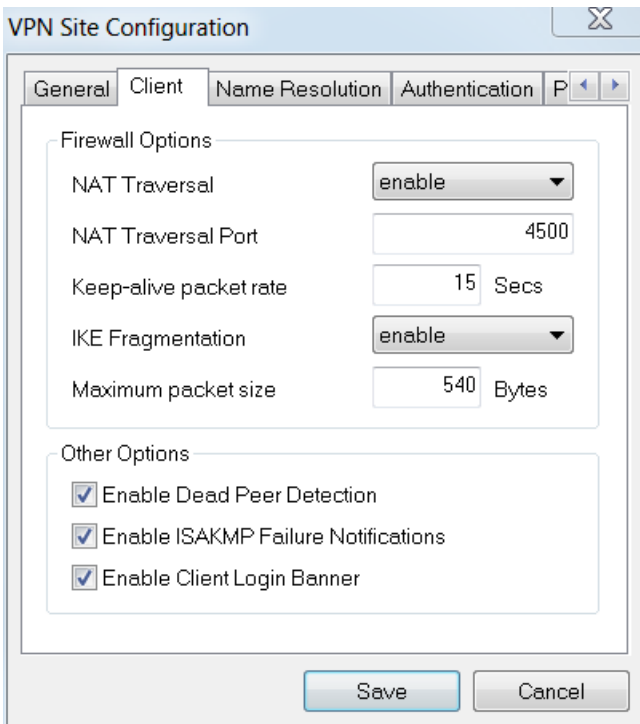
자동 구성: ike config pull 선택

어댑터 모드: 가상 어댑터 및 할당된 주소 사용을 선택합니다.



2단계

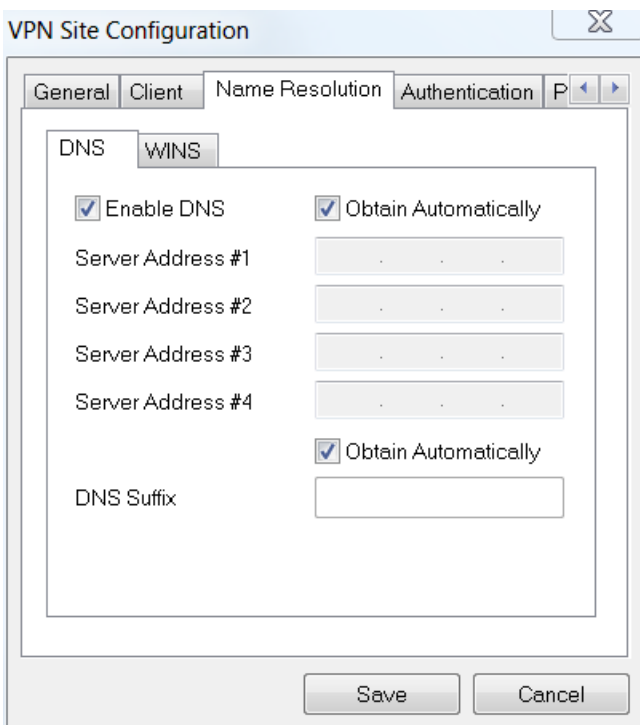
Client(클라이언트) 탭을 구성합니다.기본 설정만 사용합니다.



The image shows the 'VPN Site Configuration' dialog box with the 'Client' tab selected. The 'Firewall Options' section includes: NAT Traversal (enable), NAT Traversal Port (4500), Keep-alive packet rate (15 Secs), IKE Fragmentation (enable), and Maximum packet size (540 Bytes). The 'Other Options' section includes: Enable Dead Peer Detection (checked), Enable ISAKMP Failure Notifications (checked), and Enable Client Login Banner (checked). 'Save' and 'Cancel' buttons are at the bottom.

3단계

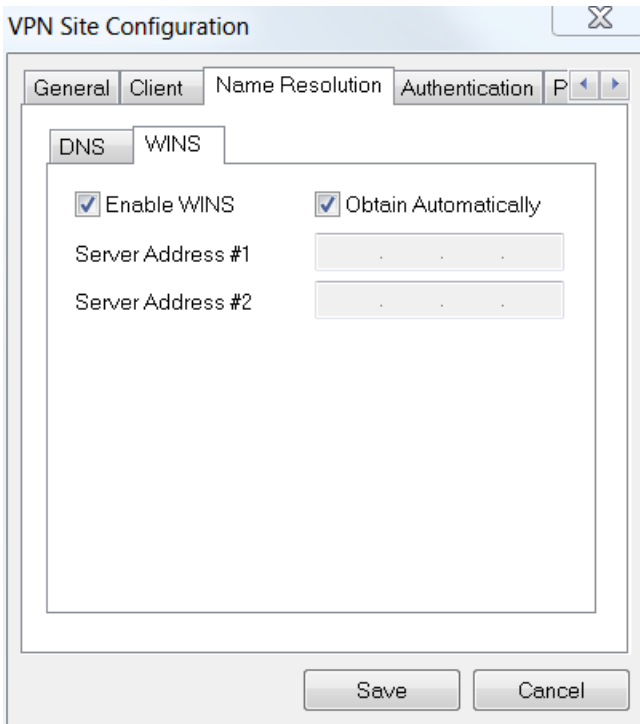
Name Resolution(이름 확인) 탭 > DNS 탭에서 Enable DNS(DNS 활성화) 확인란을 선택하고 Obtain Automatically(자동 가져오기) 확인란을 선택한 상태로 둡니다.



The image shows the 'VPN Site Configuration' dialog box with the 'Name Resolution' tab selected. The 'DNS' sub-tab is active. It includes: Enable DNS (checked), Obtain Automatically (checked), Server Address #1, #2, #3, and #4 (empty), and DNS Suffix (empty). There is also an 'Obtain Automatically' checkbox checked below the server addresses. 'Save' and 'Cancel' buttons are at the bottom.

4단계

Name Resolution(이름 확인) 탭 > WINS 탭에서 Enable WINS(WINS 활성화) 상자를 선택하고 Obtain Automatically(자동 가져오기) 확인란을 선택한 상태로 둡니다.

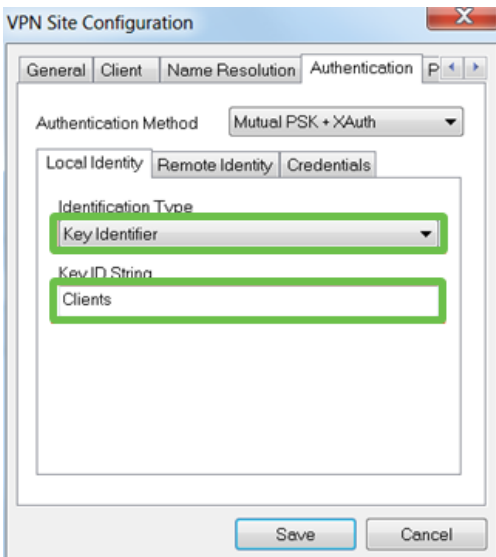


5단계

Authentication(인증) 탭 > Local Identity(로컬 ID) 탭을 구성합니다.

식별 유형: 키 식별자 선택

키 ID 문자열: RV34x에 구성된 그룹 이름을 입력합니다.



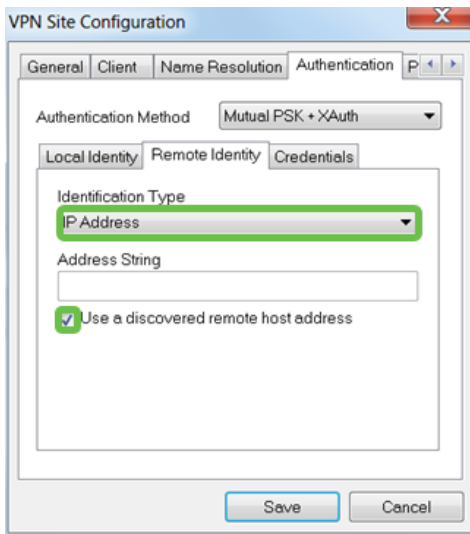
6단계

Authentication(인증) 탭 > Remote Identity(원격 ID) 탭에서 기본 설정을 그대로 둡니다.

식별 유형: IP 주소

주소 문자열:<공백>

검색된 원격 호스트 주소 상자 사용:선택

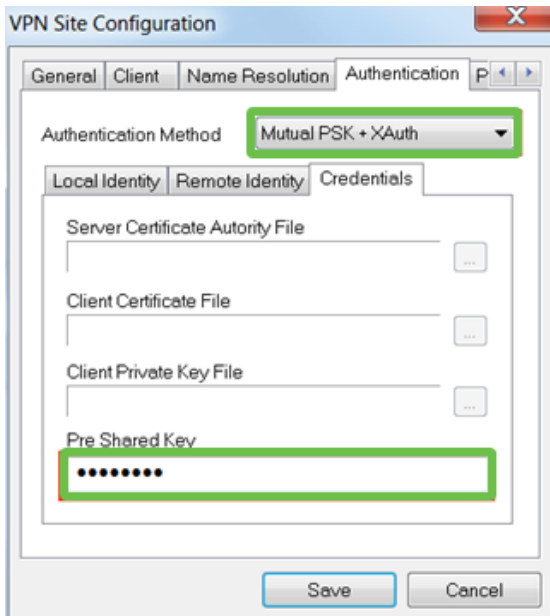


7단계

Authentication(인증) 탭 > Credentials(자격 증명) 탭에서 다음을 구성합니다.

인증 방법:상호 PSK + XAuth 선택

사전 공유 키:RV340 Client Profile에 구성된 사전 공유 키를 입력합니다.



8단계

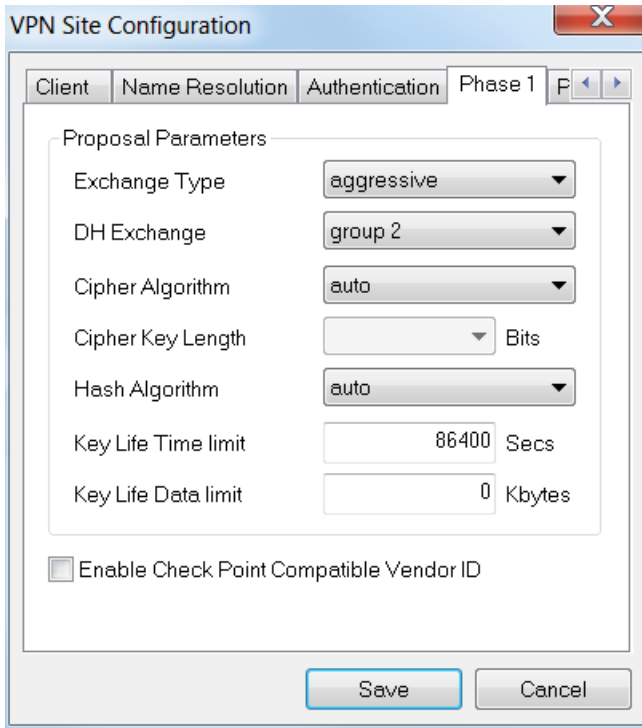
1단계 탭의 경우 기본 설정은 그대로 둡니다.

Exchange 유형:공격적

DH 교환:그룹 2

암호 알고리즘:자동

해시 알고리즘:자동



9단계

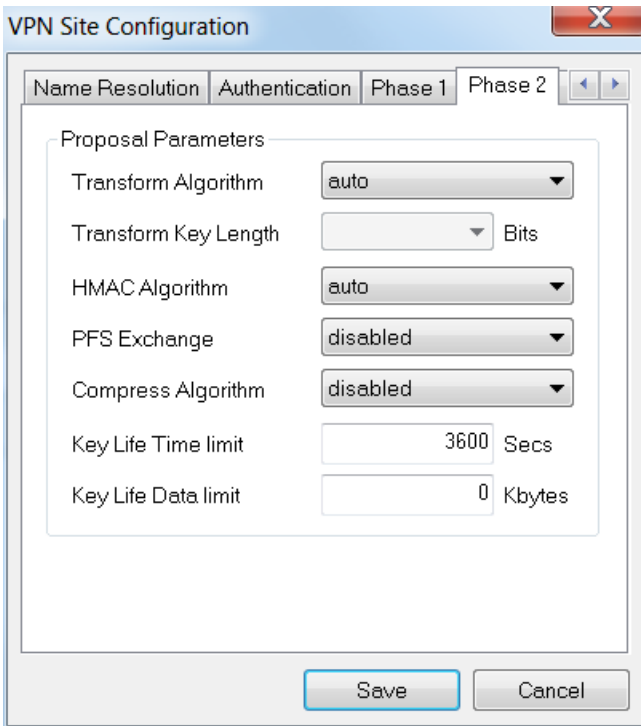
2단계 탭의 기본값도 사용합니다.

변환 알고리즘:자동

HMAC 알고리즘:자동

PFS 교환:비활성화됨

압축 알고리즘:비활성화됨



10단계

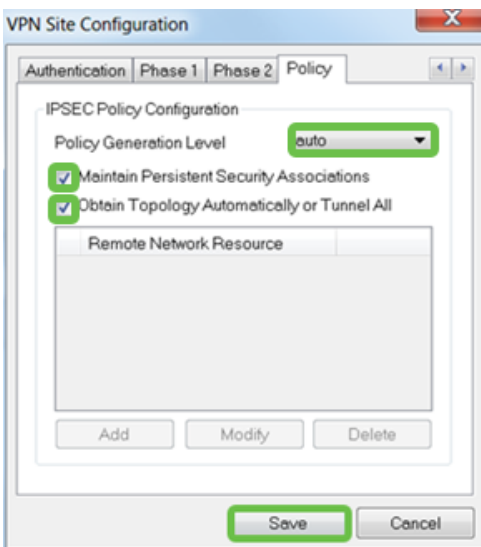
Policy 탭의 경우 다음 설정을 사용합니다.

정책 생성 레벨:자동

영구 보안 연결 유지:선택

토폴로지 자동 가져오기 또는 모두 터널:선택

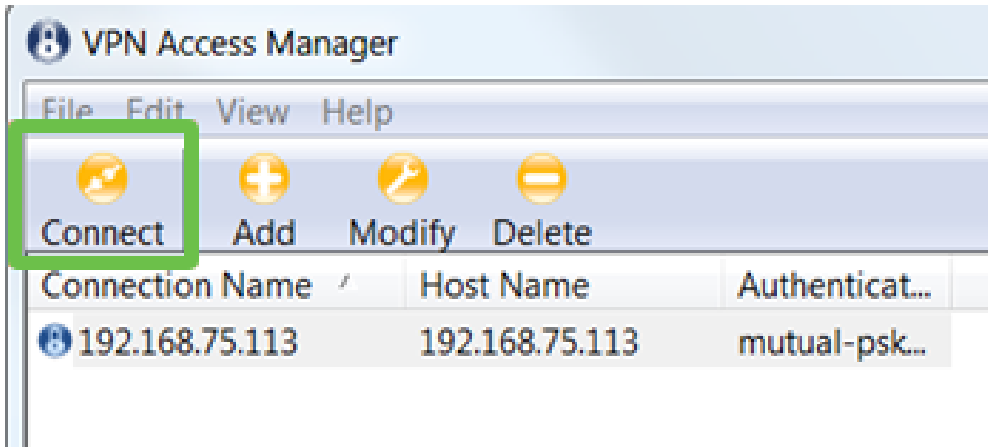
RV340에서 스플릿 터널링을 구성했으므로 여기서 구성할 필요가 없습니다.



완료되면 저장을 클릭합니다.

11단계

이제 연결을 테스트할 준비가 되었습니다. *VPN Access Manager*에서 연결 프로파일을 강조 표시하고 **Connect(연결)** 버튼을 클릭합니다.



12단계

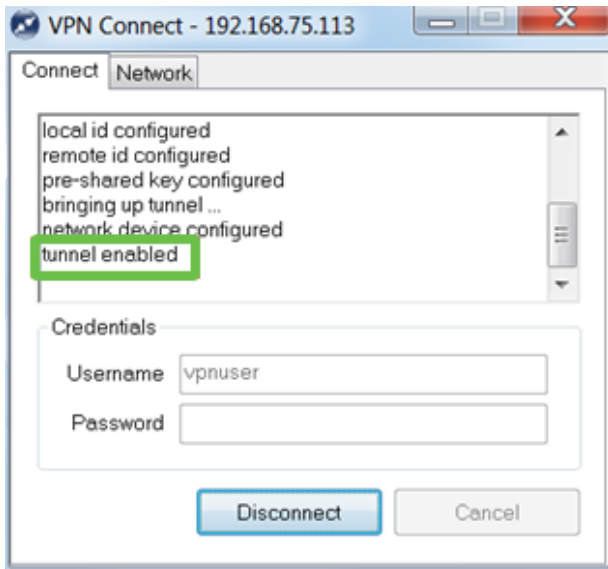
표시되는 **VPN Connect** 창에서 RV340에서 생성한 **User Account**의 자격 증명을 사용하여 **Username** 및 **Password**(13 및 14단계)를 입력합니다.



완료되면 **연결**을 클릭합니다.

13단계

터널이 연결되어 있는지 확인합니다.터널이 **활성화되었음**을 확인해야 합니다.



결론

그렇습니다. 이제 VPN을 통해 네트워크에 연결하도록 설정됩니다.