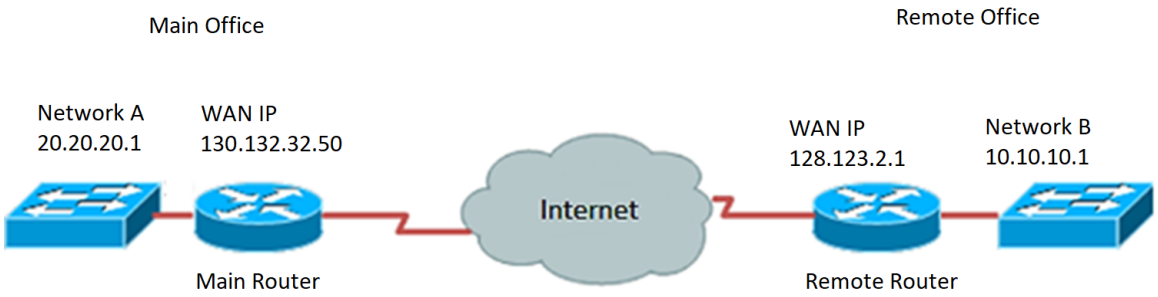
RV34x Series 라우터의 설정 마법사를 사용하여 VPN(Virtual Private Network) 연결 구성

목표

VPN(Virtual Private Network) 연결을 통해 사용자는 인터넷과 같은 공용 또는 공유 네트워크를 통해 데이터를 액세스, 전송 및 수신하고 사설 네트워크와 해당 리소스를 보호하기 위해 기본 네트워크 인프라에 안전하게 연결할 수 있습니다.

VPN 터널은 암호화 및 인증을 사용하여 데이터를 안전하게 전송할 수 있는 사설 네트워크를 설정합니다.회사 사무실은 직원들이 사무실 외부에 있더라도 개인 네트워크에 액세스할 수 있도록 하는 것이 유용하고 필요하기 때문에 VPN 연결을 주로 사용합니다.

VPN을 사용하면 원격 호스트가 동일한 로컬 네트워크에 있는 것처럼 작동할 수 있습니다.라우터는 50개의 터널을 지원합니다.VPN 설정 마법사를 사용하면 사이트 간 IPSec 터널에 대한 보안 연결을 구성할 수 있습니다.이 기능은 구성을 단순화하고 복잡한 설정 및 선택적 매개변수를 방지합니다.이렇게 하면 누구든지 빠르고 효율적인 방식으로 IPSec 터널을 설정할 수 있습니다.



VPN 연결 사용의 이점:

1. VPN 연결을 사용하면 기밀 네트워크 데이터 및 리소스를 보호할 수 있습니다.
2. 원격 근무자나 기업 직원은 물리적으로 현장에 없어도 본사에 쉽게 액세스할 수 있으며 사설 네트워크와 그 리소스의 보안을 유지할 수 있으므로 편리하고 접근성을 제공합니다.
3. VPN 연결을 사용하는 통신은 다른 원격 통신 방법에 비해 더 높은 수준의 보안을 제공합니다.오늘날의 고급 기술 수준을 통해 이를 실현할 수 있으므로 사설 네트워크를 무단 액세스로부터 보호할 수 있습니다.
4. 사용자의 실제 지리적 위치는 보호되며 인터넷과 같은 공용 또는 공유 네트워크에 노출되지 않습니다.
5. VPN은 매우 조절 가능하므로 네트워크에 새 사용자 또는 사용자 그룹을 쉽게 추가할 수 있습니다.새로운 구성 요소나 복잡한 구성 없이 네트워크를 확장할 수 있습니다.

VPN 연결 사용 위험:

1. 컨피그레이션 오류로 인한 보안 위험.VPN의 설계 및 구현이 복잡할 수 있으므로, 개인 네트워크의 보안이 침해되지 않도록 하려면 숙련된 전문가에게 연결을 구성하는 작업을 위탁해야 합니다.
2. 신뢰성.VPN 연결에는 인터넷 연결이 필요하므로, 뛰어난 인터넷 서비스를 제공하고 다운타임을 최소화하면서 보장하도록 검증되고 테스트된 제공자를 선택하는 것이 중요합

니다.

3. 확장성.새로운 인프라를 추가하거나 새 컨피그레이션을 설정해야 하는 경우, 특히 이미 사용 중인 제품이 아닌 다른 제품이나 공급업체와 관련된 경우 비호환성으로 인해 기술 문제가 발생할 수 있습니다.
4. 모바일 장치의 보안 문제.VPN 연결을 시작할 때 모바일 장치를 사용할 때 특히 무선 연결을 사용할 때 보안 문제가 발생할 수 있습니다.일부 검증되지 않은 제공자는 "무료 VPN 공급자"로 보이며 컴퓨터에 악성코드를 설치할 수도 있습니다.이 때문에 모바일 장치를 사용할 때 이러한 문제를 방지하기 위해 보안 조치를 더 추가할 수 있습니다.
5. 느린 연결 속도.무료 VPN 서비스를 제공하는 VPN 클라이언트를 사용하는 경우, 이러한 제공자가 연결 속도의 우선 순위를 지정하지 않으므로 연결 속도가 느려질 수 있습니다.

이 문서의 목적은 설정 마법사를 사용하여 RV34x Series 라우터에서 VPN 연결을 구성하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스

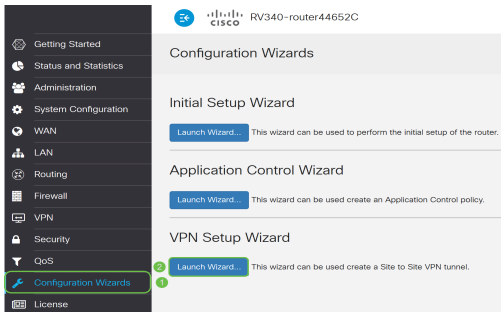
- RV34x 시리즈

소프트웨어 버전

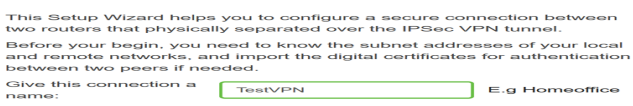
- 1.0.01.16

설정 마법사를 사용하여 VPN 연결 구성

1단계. 라우터 웹 기반 유틸리티에 로그인하고 **구성 마법사**를 선택합니다.그런 다음 *VPN Setup Wizard* 섹션에서 **Launch Wizard(마법사 시작)를** 클릭합니다.



2단계. 제공된 필드에 이 연결을 식별할 이름을 입력합니다.



참고:이 예에서는 TestVPN이 사용됩니다.

3단계. Interface(인터페이스) 영역에서 드롭다운 메뉴를 클릭하고 이 연결을 활성화할 인터페이스를 선택합니다.옵션은 다음과 같습니다.

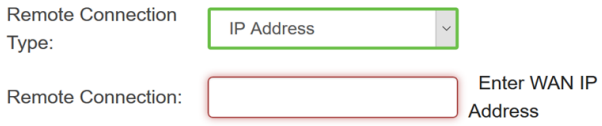
- WAN1
- WAN2
- USB1
- USB2

참고:이 예에서는 WAN1이 사용됩니다.

4단계. **다음**을 클릭합니다.

5단계. 드롭다운 화살표를 클릭하여 원격 연결 유형을 선택합니다.옵션은 다음과 같습니다.

- IP Address(IP 주소) — VPN 터널의 반대쪽 끝에 있는 원격 라우터의 IP 주소를 사용하려면 이 옵션을 선택합니다.
- FQDN — (Fully Qualified Domain Name) VPN 터널의 다른 끝에서 원격 라우터의 도메인 이름을 사용하려면 이 옵션을 선택합니다.



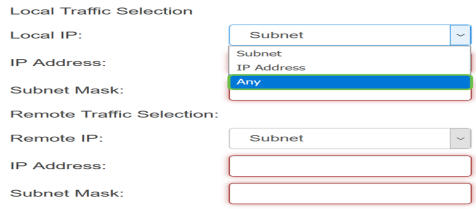
참고:이 예에서는 IP 주소가 선택됩니다.

6단계. 제공된 필드에 원격 연결의 WAN IP 주소를 입력한 다음 **Next**를 클릭합니다.

참고:이 예에서는 128.123.2.1이 사용됩니다.

7단계. Local Traffic Selection(로컬 트래픽 선택) 영역에서 드롭다운을 클릭하여 Local IP를 선택합니다.옵션은 다음과 같습니다.

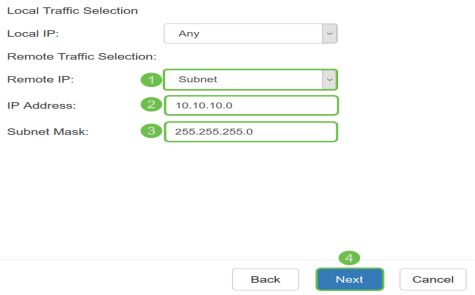
- 서브넷 — 로컬 네트워크의 IP 주소와 서브넷 마스크를 모두 입력하려면 선택합니다.
- IP Address — 로컬 네트워크의 IP 주소만 입력하려면 선택합니다.
- Any(모두) - 둘 중 하나를 원하는 경우 선택합니다.



참고:이 예에서는 Any가 선택됩니다.

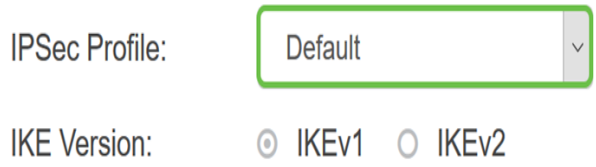
8단계. Remote Traffic Selection(원격 트래픽 선택) 영역에서 드롭다운 화살표를 클릭하여 Remote IP를 선택합니다.제공된 필드에 원격 IP 주소와 서브넷 마스크를 입력한 다음 **Next(다음)**를 클릭합니다.옵션은 다음과 같습니다.

- 서브넷 — 원격 네트워크의 IP 주소와 서브넷 마스크를 모두 입력하려면 선택합니다.
- IP Address — 원격 네트워크의 IP 주소만 입력하려면 선택합니다.



참고:이 예에서는 서브넷이 선택됩니다.10.10.10.0이(가) IP 주소로 입력되었고 255.255.255.0이 서브넷 마스크로 입력되었습니다.

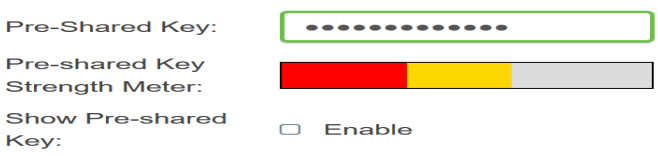
9단계. IPSec Profile(IPSec 프로필) 영역에서 드롭다운 화살표를 클릭하여 사용할 프로필을 선택합니다.



참고:이 예에서는 Default(기본값)가 선택됩니다.

10단계. Phase 1 Options(1단계 옵션) 영역의 제공된 필드에 이 연결에 대한 사전 공유 키를 입력합니다.원격 IKE(Internet Key Exchange) 피어를 인증하는 데 사용할 사전 공유 키입니다.VPN 터널의 양쪽 끝은 동일한 사전 공유 키를 사용해야 합니다.이 키에 최대 30자 또는 16진수 값을 사용할 수 있습니다.

참고:VPN 연결의 보안을 유지하려면 사전 공유 키를 정기적으로 변경하는 것이 좋습니다.

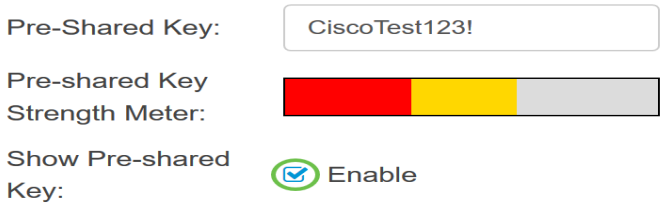


참고: Preshared Key Strength Meter는 다음을 기반으로 입력한 키의 강도를 나타냅니다.

- 빨간색 — 암호가 약합니다.

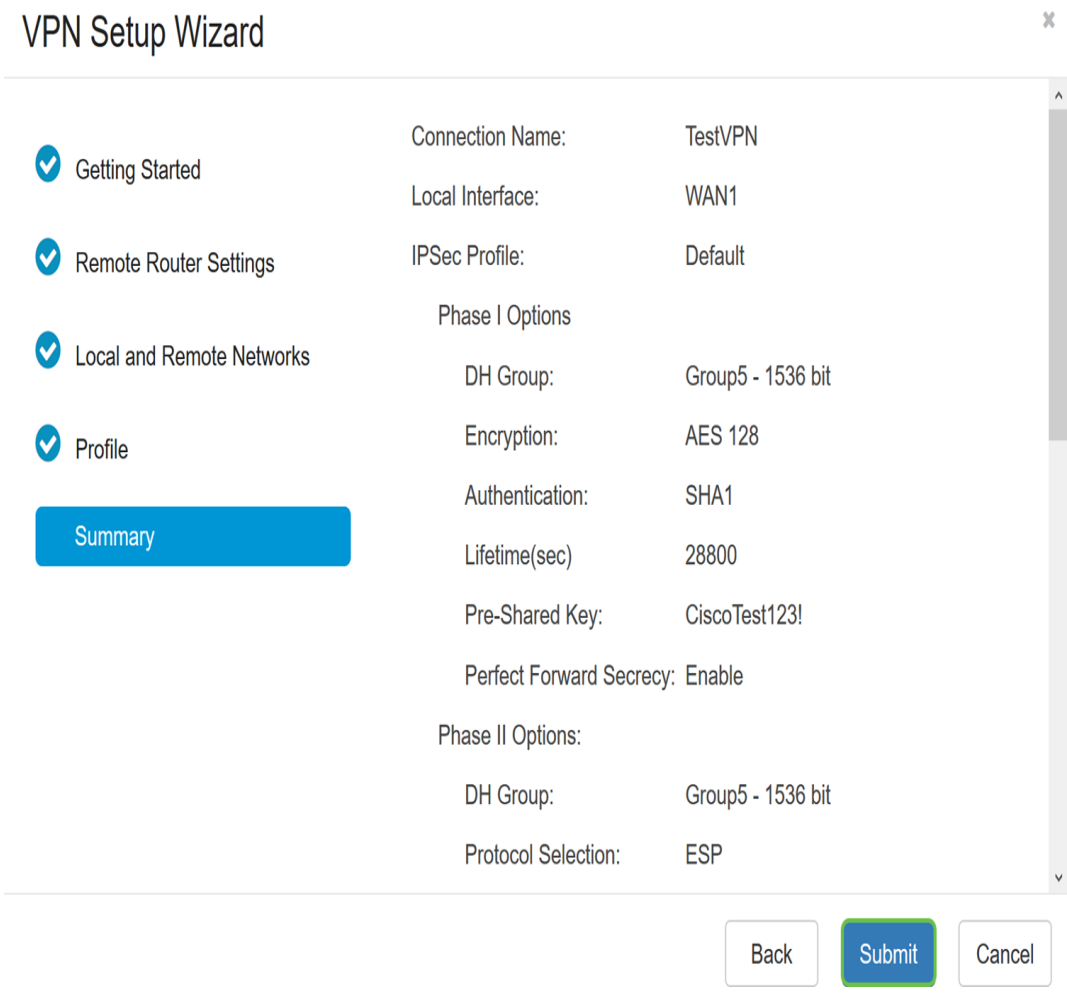
- 황색 — 비밀번호가 상당히 강력합니다.
- 녹색 — 암호가 강력합니다.

11단계(선택 사항) 편집할 때 일반 텍스트 **표시** 확인란을 선택하여 일반 텍스트로 암호를 표시할 수도 있습니다.



12단계. **다음**.

13단계. 그러면 VPN 연결의 모든 컨피그레이션 세부사항이 페이지에 표시됩니다.Submit(제출)**을 클릭합니다**.



이제 설치 마법사를 사용하여 RV34x Series Router에서 VPN 연결을 성공적으로 구성해야 합니다.사이트 대 사이트 VPN을 성공적으로 연결하려면 원격 라우터에서 설정 마법사를 구성해야 합니다.