RV160 및 RV260 라우터와 연결하려면 TheGreenBow IPsec VPN Client 설정 및 사용

목표

이 문서의 목적은 TheGreenBow IPsec VPN Client를 설정하고 사용하여 RV160 및 RV260 라우터에 연결하는 것입니다.

소개

VPN(Virtual Private Network) 연결을 통해 사용자는 인터넷과 같은 공용 또는 공유 네트워크를 통해 데이터를 액세스, 전송 및 수신할 수 있지만 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 사용하는 경우가 많습니다.

VPN을 사용하면 원격 호스트 또는 클라이언트가 동일한 로컬 네트워크에 있는 것처럼 작동할 수 있습니다.RV160 라우터는 최대 10개의 VPN 터널을 지원하며 RV260은 최대 20개를 지원합니다. 라우터가 인터넷 연결을 위해 구성된 후 라우터와 엔드포인트 간에 VPN 연결을 설정할 수 있습니다.VPN 클라이언트는 연결을 설정할 수 있도록 VPN 라우터의 설정에 전적으로 의존합니다.설정이 정확히 일치해야 합니다. 그렇지 않으면 통신할 수 없습니다.

GreenBow VPN Client는 RV160 및 RV260 Series 라우터를 사용하여 호스트 디바이스가 클라이언트-사이트 IPsec 터널에 대한 보안 연결을 구성할 수 있도록 하는 서드파티 VPN 클라이언트 애플리케이션입니다.

VPN 연결 사용의 이점

VPN 연결을 사용하면 기밀 네트워크 데이터 및 리소스를 보호할 수 있습니다.

원격 근무자나 기업 직원은 물리적으로 현장에 없어도 본사에 쉽게 액세스할 수 있으며 사설 네트워크와 해당 리소스의 보안을 유지할 수 있으므로 편리하고 접근성을 제공합니다.

VPN 연결을 사용하는 통신은 다른 원격 통신 방법에 비해 더 높은 수준의 보안을 제공합니다.고급 암호화 알고리즘을 사용하면 프라이빗 네트워크를 무단 액세스로부터 보호할 수 있습니다.

사용자의 실제 지리적 위치는 보호되며 인터넷과 같은 공용 또는 공유 네트워크에 노출되지 않습니다.

VPN을 사용하면 추가 구성 요소나 복잡한 구성 없이 새 사용자 또는 사용자 그룹을 추가할 수 있습니다.

VPN 연결 사용 위험

컨피그레이션 오류로 인해 보안 위험이 발생할 수 있습니다.VPN의 설계 및 구현이 복잡할 수 있으므로, 사설 네트워크의 보안이 침해되지 않도록 하려면 숙련된 전문가에게 연결을 구성하는 작업을 위탁해야 합니다.

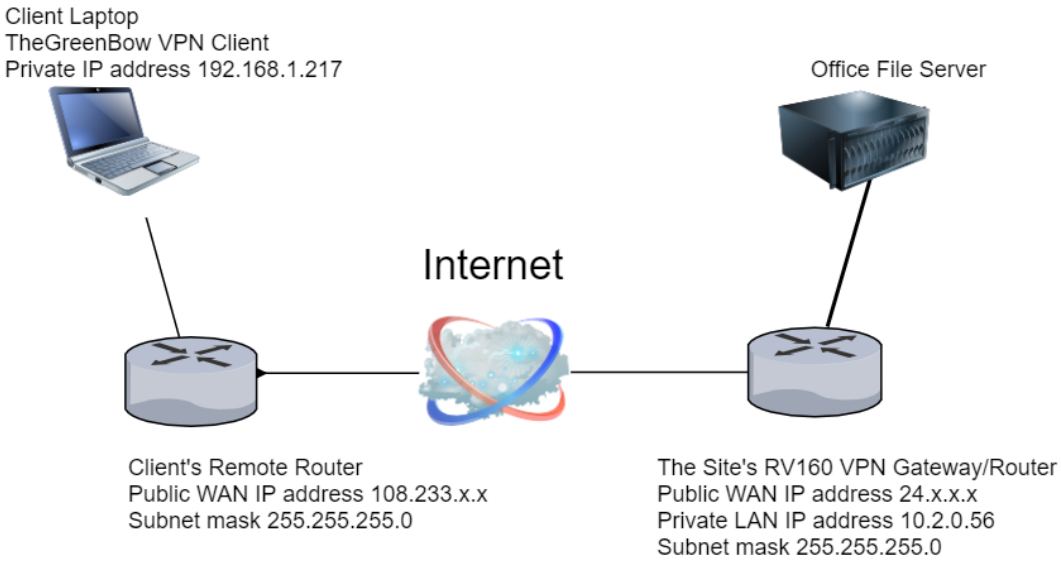
안정성이 떨어집니다.VPN 연결에는 인터넷 연결이 필요하므로, 뛰어난 인터넷 서비스를 제공하고 다운타임을 최소화하면서 중단 없이 보장하려면 검증되고 테스트된 평판을 가진 공급자를 보유하는 것이 중요합니다.

새로운 인프라 또는 새로운 구성 집합을 추가해야 하는 상황이 발생하는 경우, 특히 이미 사용 중인 제품 또는 공급업체가 아닌 다른 제품과 관련된 경우 비호환성으로 인해 기술 문제가 발생할 수 있습니다.

느린 연결 속도가 발생할 수 있습니다.무료 VPN 서비스를 제공하는 VPN 클라이언트를 사용 중인 경우 이러한 공급자가 연결 속도의 우선 순위를 지정하지 않으므로 연결 속도가 느려질 수 있습니다.이 문서에서는 이 문제를 해결해야 하는 유료 제3자를 사용할 것입니다.

클라이언트-사이트 네트워크의 기본 토폴로지

이것은 설치할 네트워크의 기본 레이아웃입니다.퍼블릭 WAN IP 주소가 부분적으로 흐리게 되었거나 실제 번호 대신 **x를** 표시하여 이 네트워크를 공격으로부터 보호합니다.



이 문서에서는 사이트에서 다음 항목에 대해 RV160 또는 RV260 라우터를 구성하는 데 필요한 단계를 살펴봅니다.

- 사용자 그룹 — **VPNUsers**
- 클라이언트로 액세스가 허용되는 사용자 계정(하나 이상의 사용자)
- IPsec 프로파일 — **GreenBow**
- 클라이언트-사이트 프로파일 — **클라이언트**
- 클라이언트가 연결되면 사이트에서 VPN 상태를 보는 방법도 표시됩니다

참고:사용자 그룹, IPsec 프로파일 및 클라이언트-사이트 프로파일의 이름을 사용할 수 있습니다.나열된 이름은 단지 예시입니다.

이 문서에서는 각 클라이언트가 컴퓨터에 TheGreenBow VPN을 구성하는 데 수행하는 단계에 대해서도 설명합니다.

- GreenBow VPN 클라이언트 소프트웨어 다운로드 및 설정
- 클라이언트에 대한 1단계 및 2 설정 구성
- 클라이언트로 VPN 연결 시작 및 확인

사이트의 라우터의 모든 설정이 클라이언트 설정과 일치해야 합니다.컨피그레이션으로 인해 VPN

연결이 성공하지 못할 경우 모든 설정을 확인하여 설정이 일치하는지 확인합니다.이 문서의 예제는 연결을 설정하는 한 가지 방법입니다.

목차

적용 가능한 디바이스

- RV160
- RV260

소프트웨어 버전

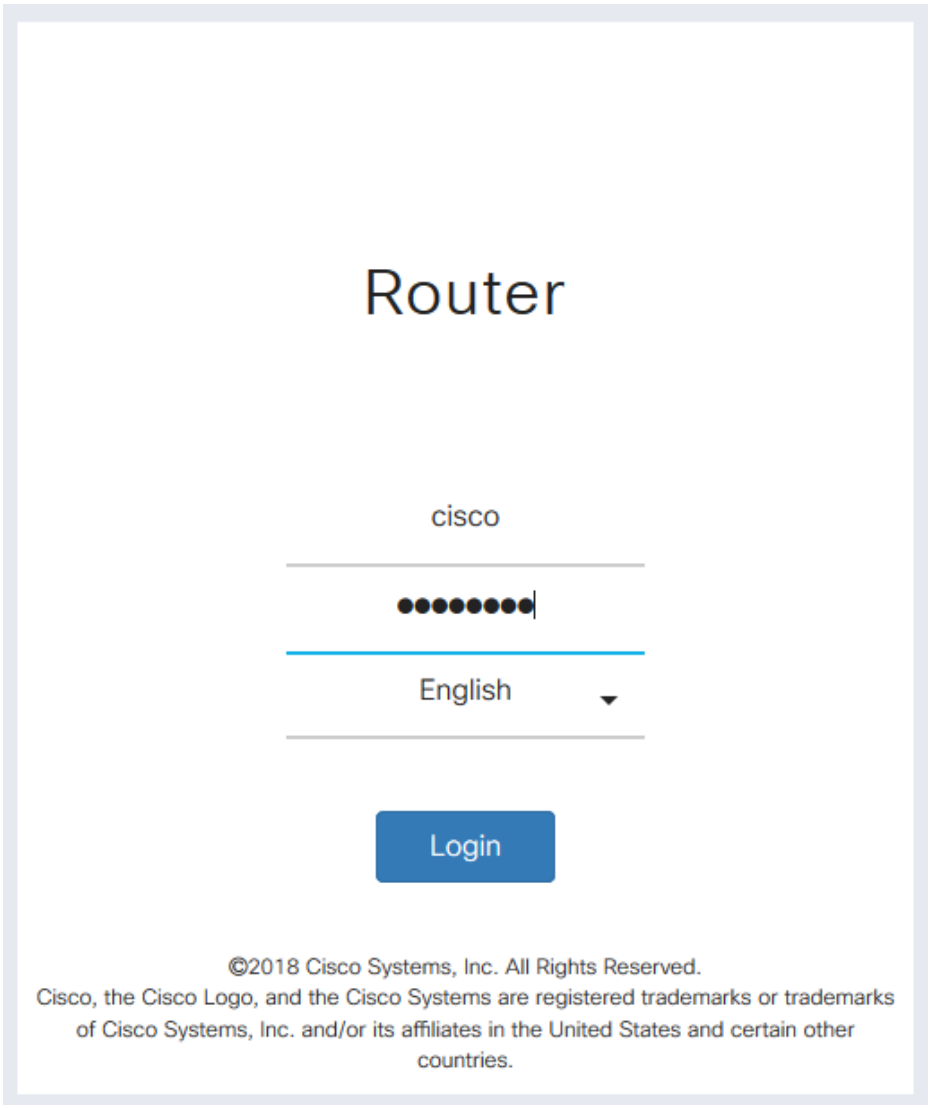
- 1.0.00.15

RV160 또는 RV260 라우터의 사이트에서 VPN 클라이언트 구성

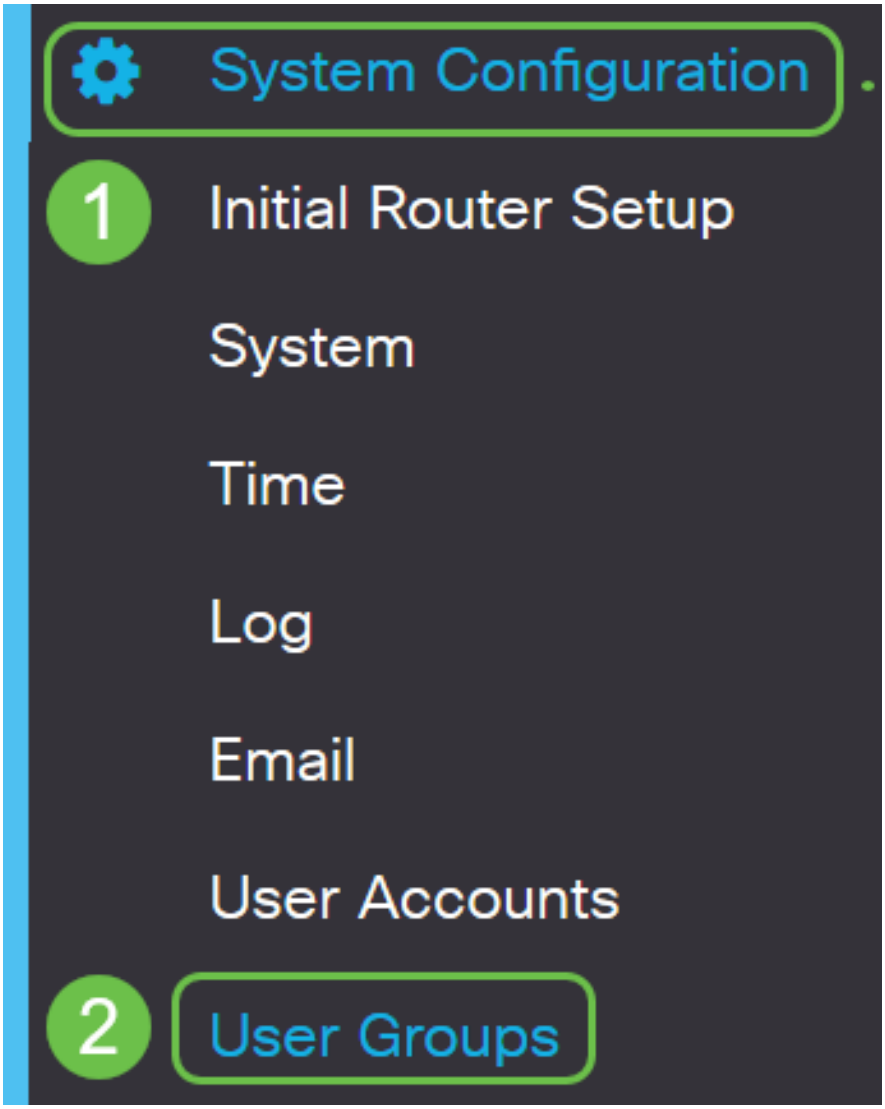
사용자 그룹 생성

중요 참고 사항:관리자 그룹에 기본 관리자 계정을 유지하고 TheGreenBow에 대한 새 사용자 계정과 사용자 그룹을 만드십시오.관리자 계정을 다른 그룹으로 이동하면 라우터에 로그인하지 못하게 됩니다.

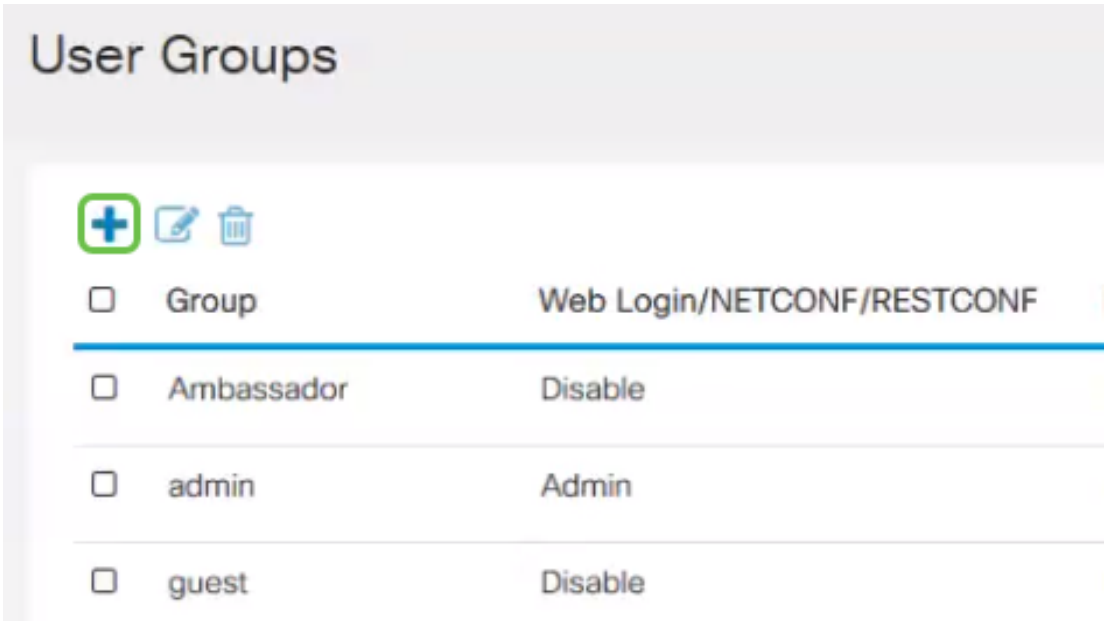
1단계. 라우터의 웹 기반 유틸리티에 로그인합니다.



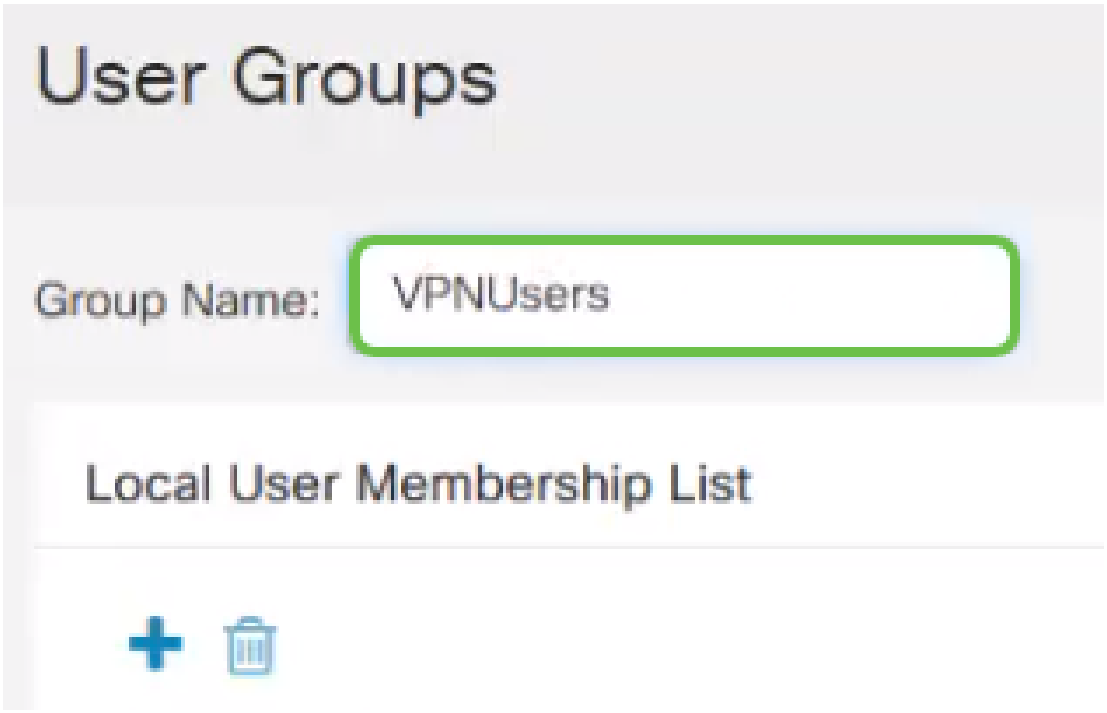
2단계. **System Configuration(시스템 컨피그레이션) > User Groups(사용자 그룹)**를 선택합니다.



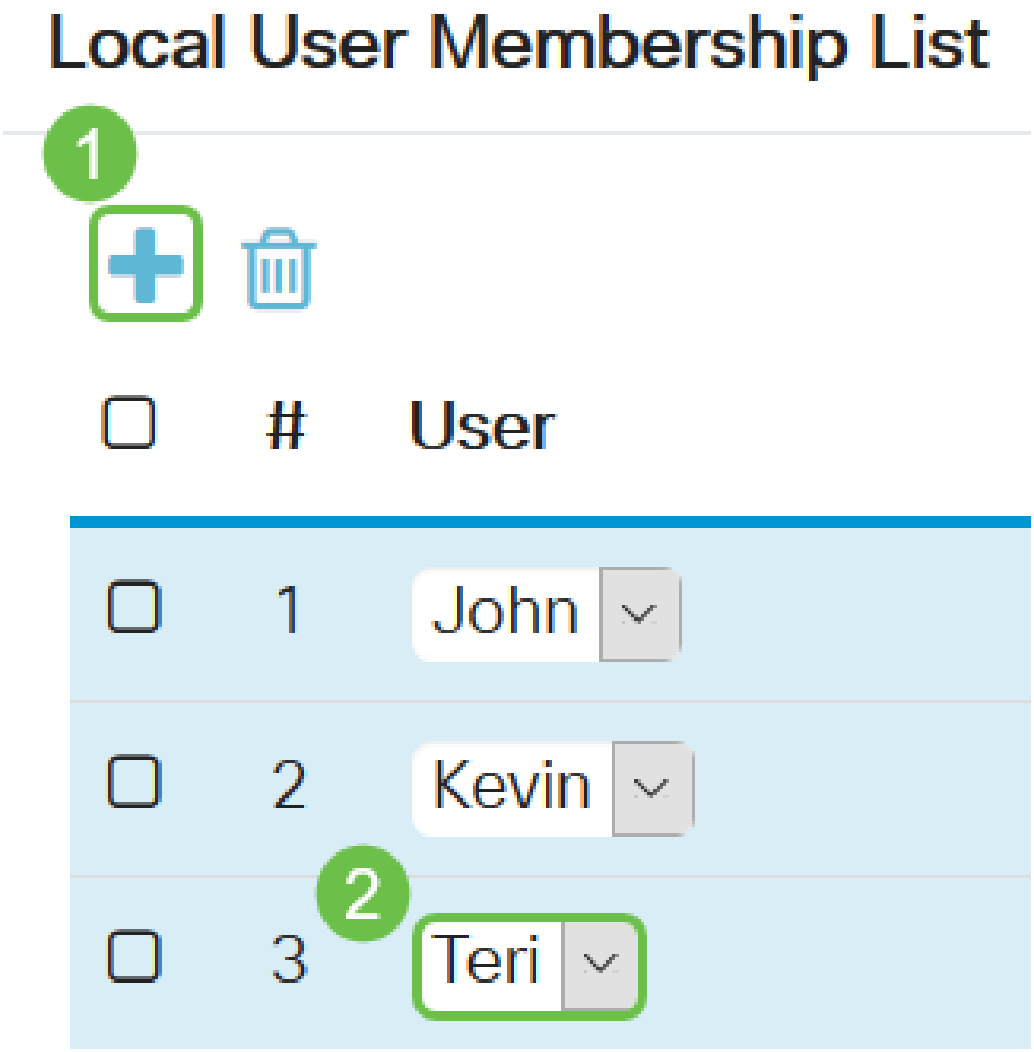
3단계. **더하기** 아이콘을 클릭하여 사용자 그룹을 추가합니다.



4단계. Overview(개요) 영역의 *Group Name(그룹 이름)* 필드에 그룹 이름을 입력합니다.

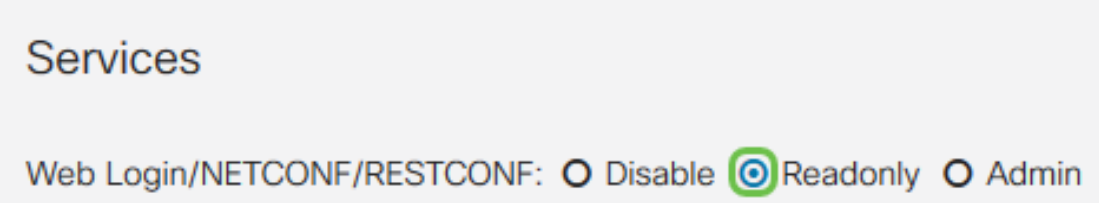


5단계. *Local User Membership List(로컬 사용자 구성원 목록)*에서 **더하기** 아이콘을 클릭하고 드롭다운 목록에서 사용자를 선택합니다.추가하려면 **더하기** 아이콘을 다시 누르고 추가할 다른 멤버를 선택합니다.구성원은 하나의 그룹에만 속할 수 있습니다.모든 사용자를 이미 입력하지 않은 경우 Create a User Account 섹션에서 더 추가할 수 있습니다.

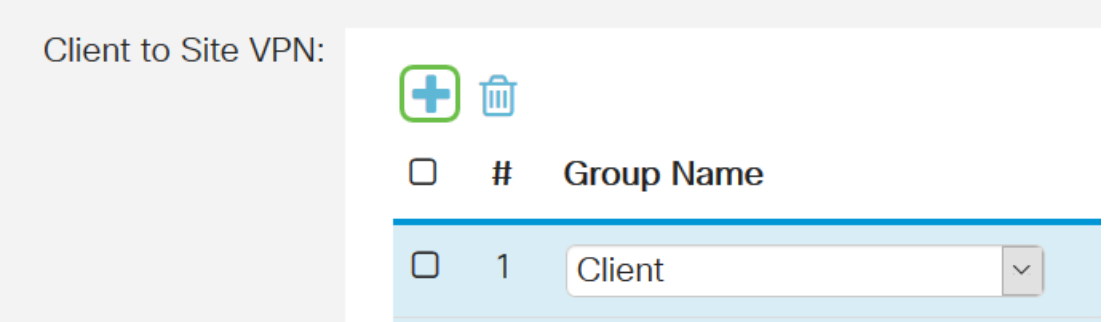


6단계. *서비스*에서 그룹의 사용자에게 부여할 권한을 선택합니다.옵션은 다음과 같습니다.

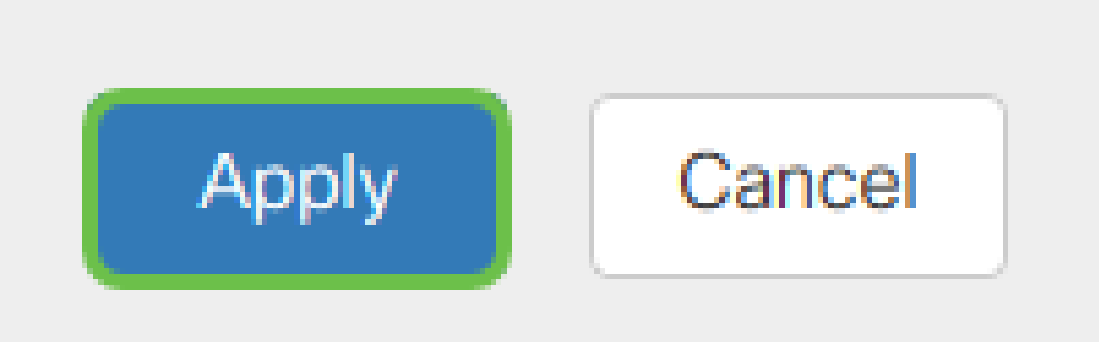
- Disabled(비활성화됨) — 이 옵션은 그룹 구성원이 브라우저를 통해 웹 기반 유틸리티에 액세스할 수 없음을 의미합니다.
- 읽기 전용 — 이 옵션은 그룹 구성원이 로그인한 후에만 시스템의 상태를 읽을 수 있음을 의미합니다.설정을 편집할 수 없습니다.
- Admin — 이 옵션은 그룹 구성원에게 읽기 및 쓰기 권한을 제공하며 시스템 상태를 구성할 수 있습니다.



7단계. **더하기** 아이콘을 클릭하여 기존 Client-to-Site VPN을 추가합니다.이 설정을 구성하지 않은 경우 Create a Client-to-Site Profile(클라이언트-사이트 프로필 생성) 섹션 아래에서 정보를 찾을 수 있습니다.

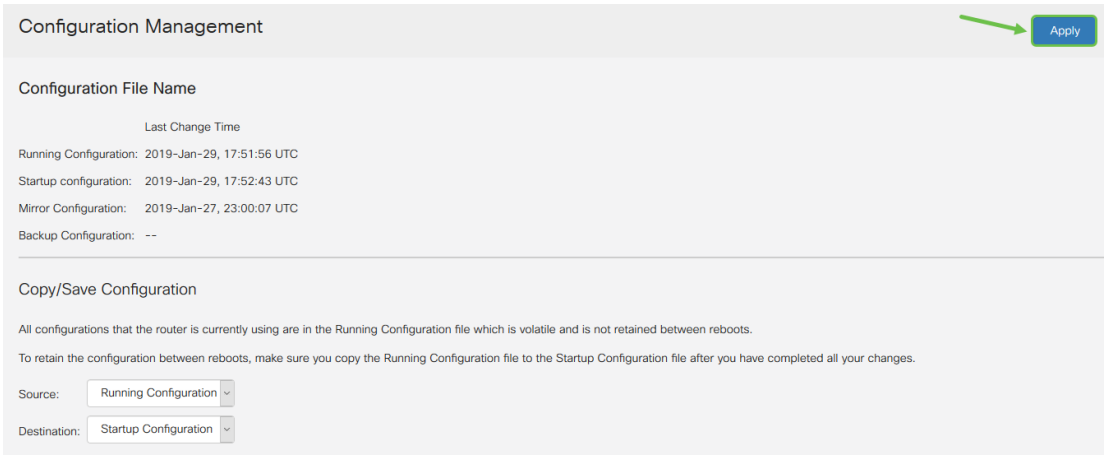


8단계. 적용을 **클릭합니다**.

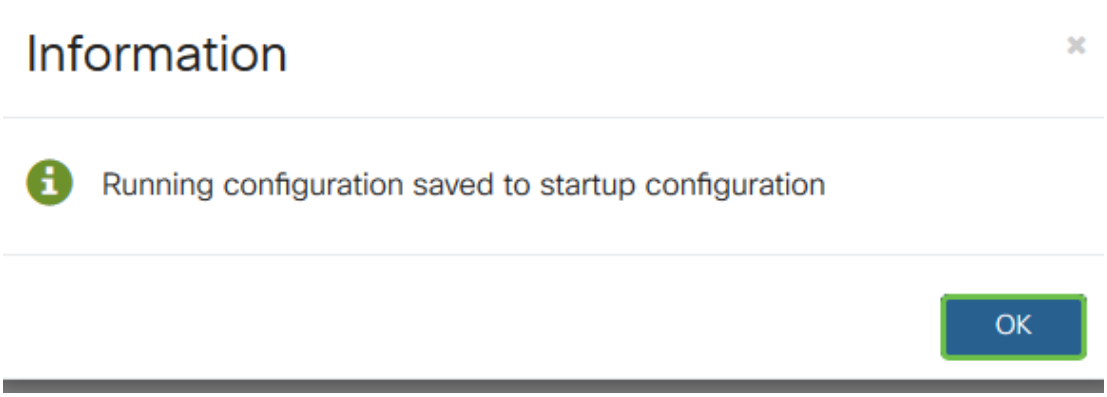


5단계. **저장**을 클릭합니다.

10단계. **Apply(적용)**를 다시 한 번 클릭하여 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.



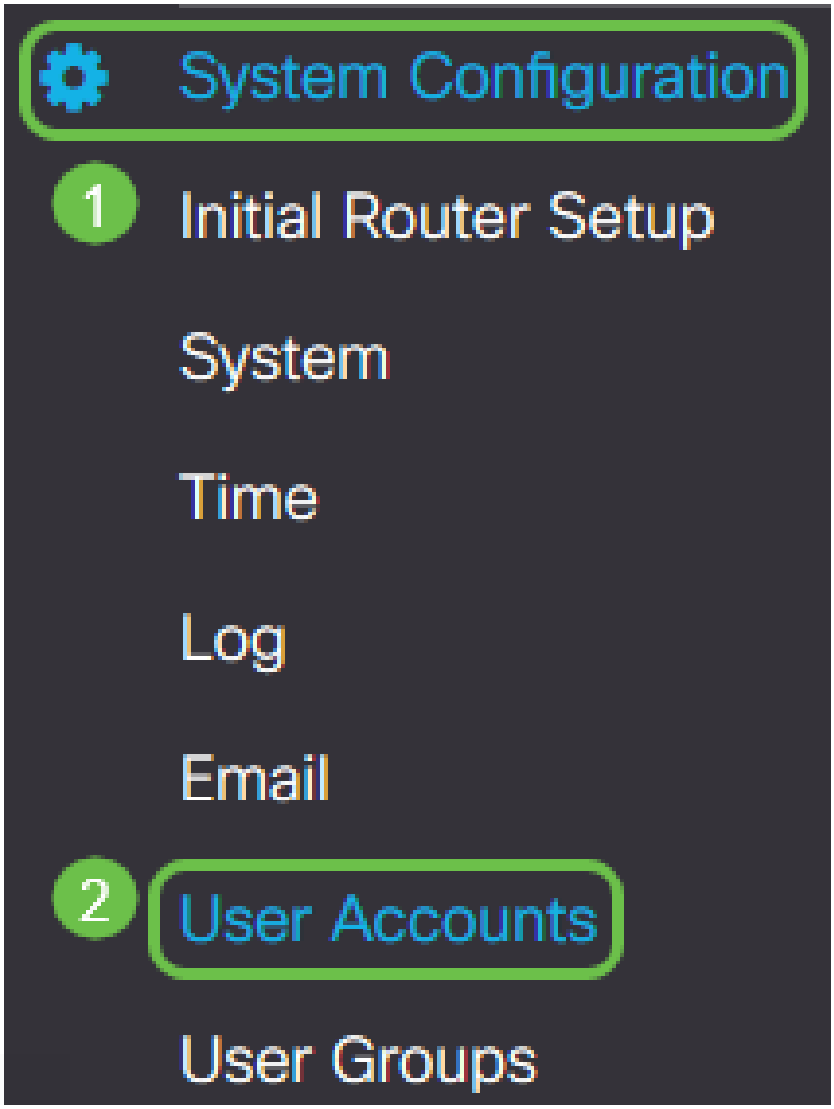
11단계. 확인 메시지가 표시되면 **확인**을 클릭합니다.



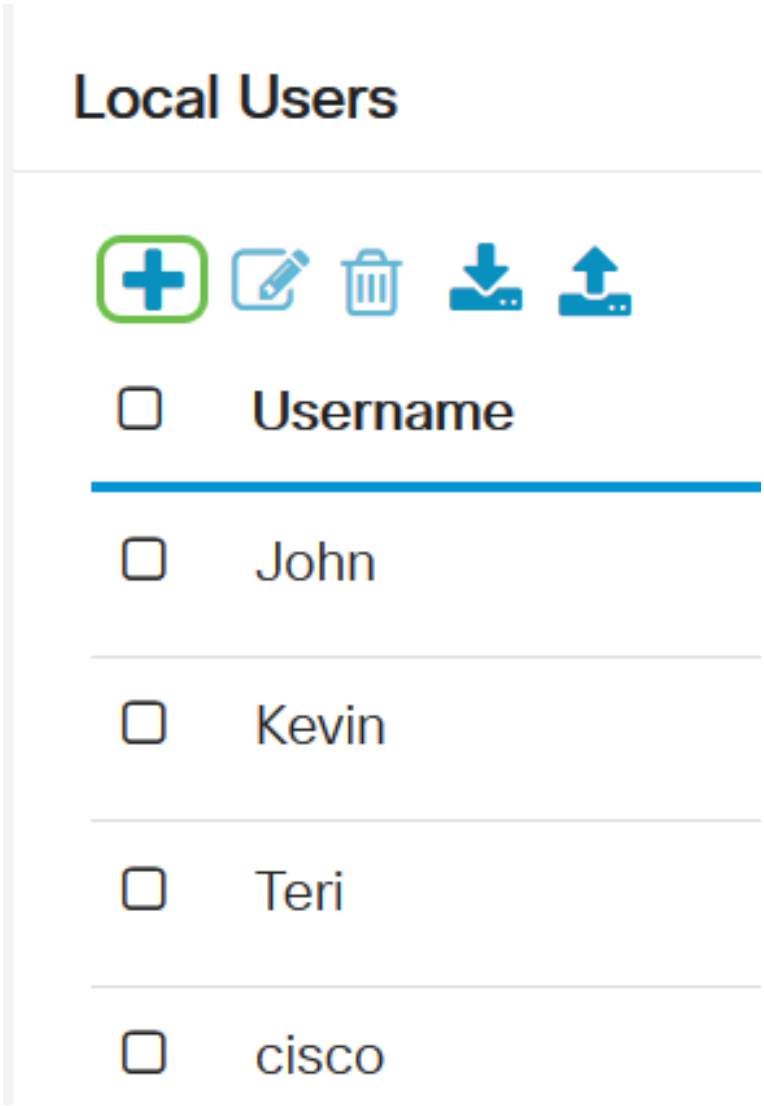
이제 RV160 또는 RV260 Series Router에서 사용자 그룹을 성공적으로 생성해야 합니다.

사용자 계정 생성

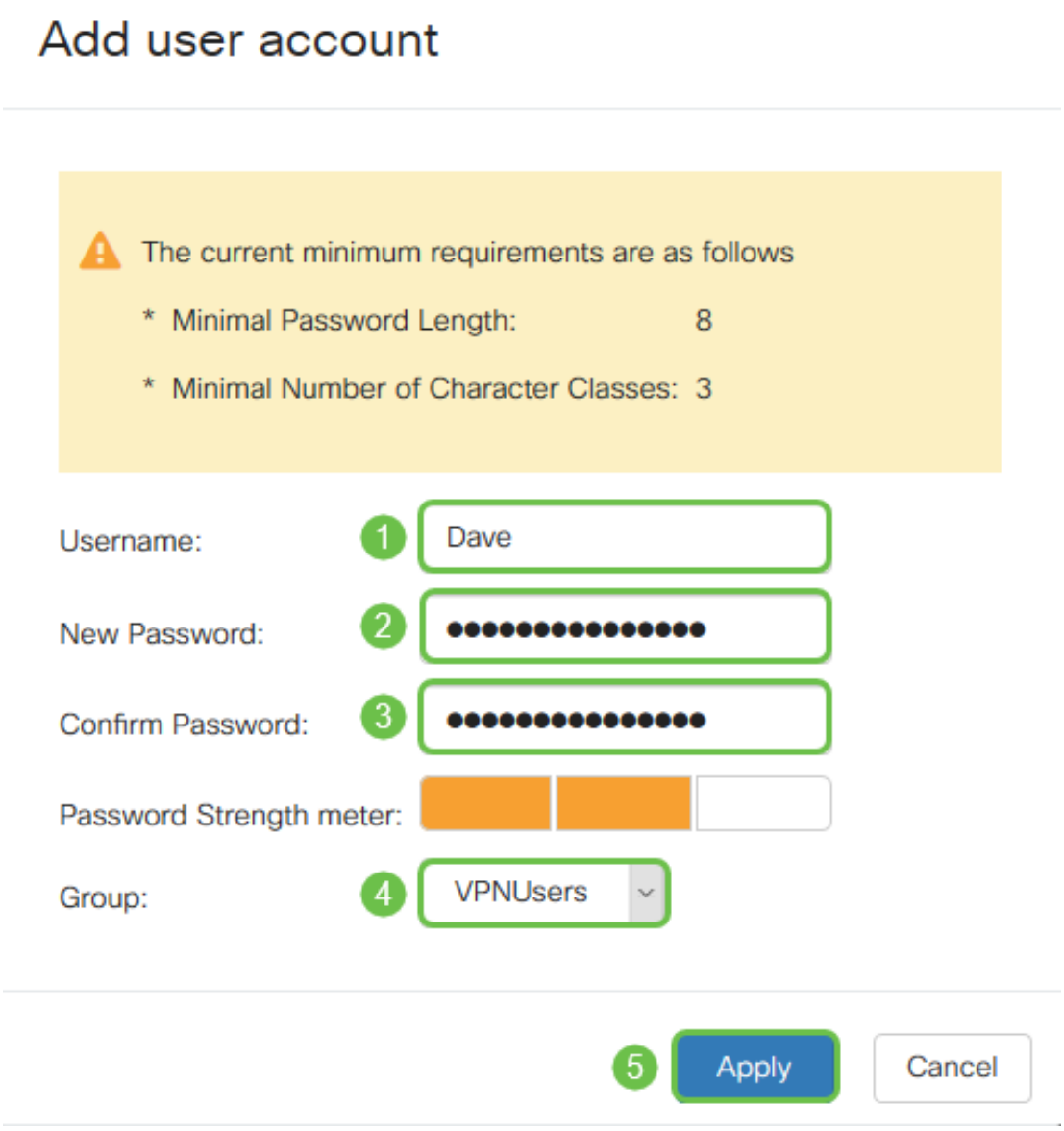
1단계. 라우터의 웹 기반 유틸리티에 로그인하고 **System Configuration(시스템 컨피그레이션) > User Accounts(사용자 계정)를** 선택합니다.



2단계. *Local Users(로컬 사용자)* 영역에서 **추가** 아이콘을 클릭합니다.



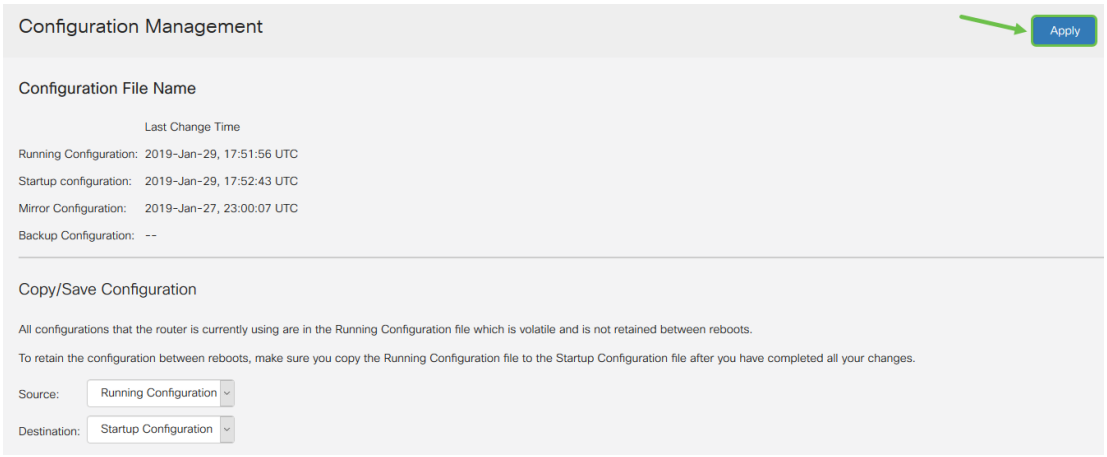
3단계. *사용자 이름* 필드, 비밀번호 및 사용자를 추가할 그룹을 드롭다운 메뉴에서 입력합니다 .Apply를 **클릭합니다**.



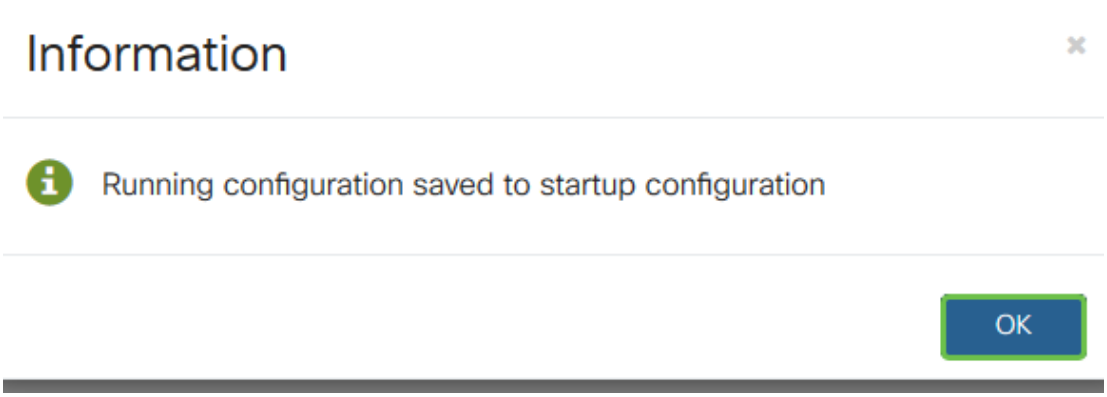
참고:클라이언트가 컴퓨터에 TheGreenBow Client를 설정하면 동일한 사용자 이름과 비밀번호로 로그인합니다.

4단계. **저장**을 클릭합니다.

5단계. Apply(**적용**)를 다시 한 번 클릭하여 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.



6단계. 확인 메시지가 표시되면 **확인**을 클릭합니다.

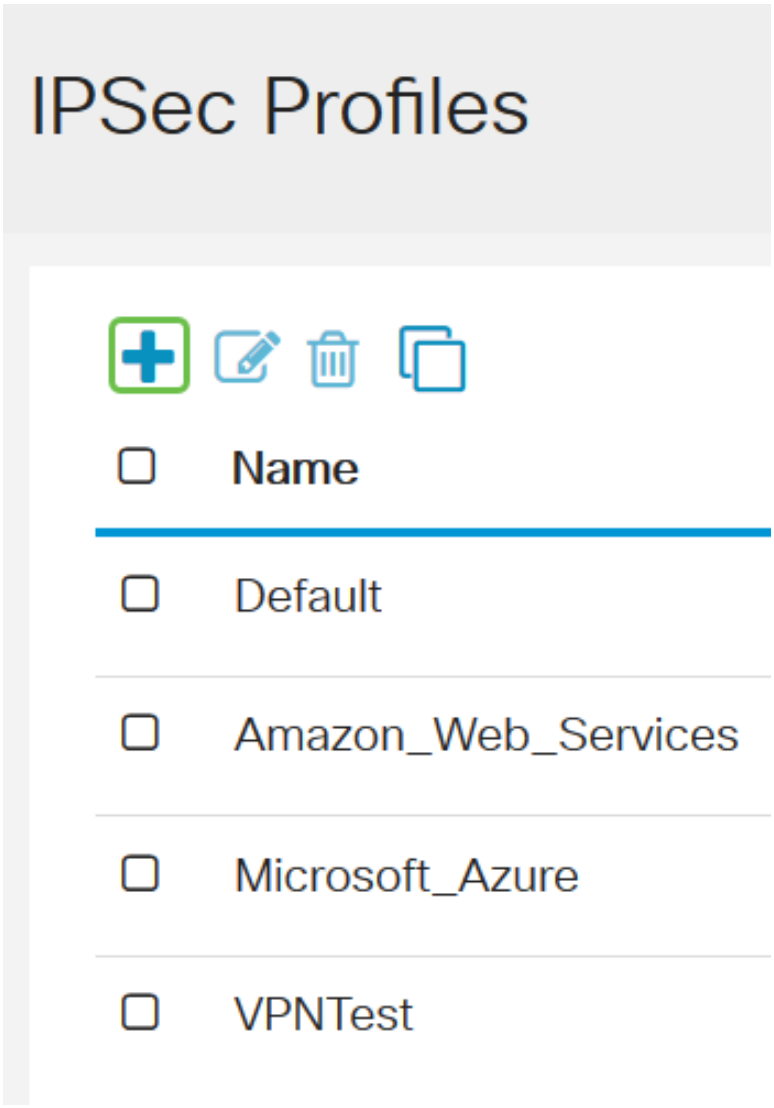


이제 RV160 또는 RV260 라우터에 사용자 계정을 생성해야 합니다.

IPsec 프로필 구성

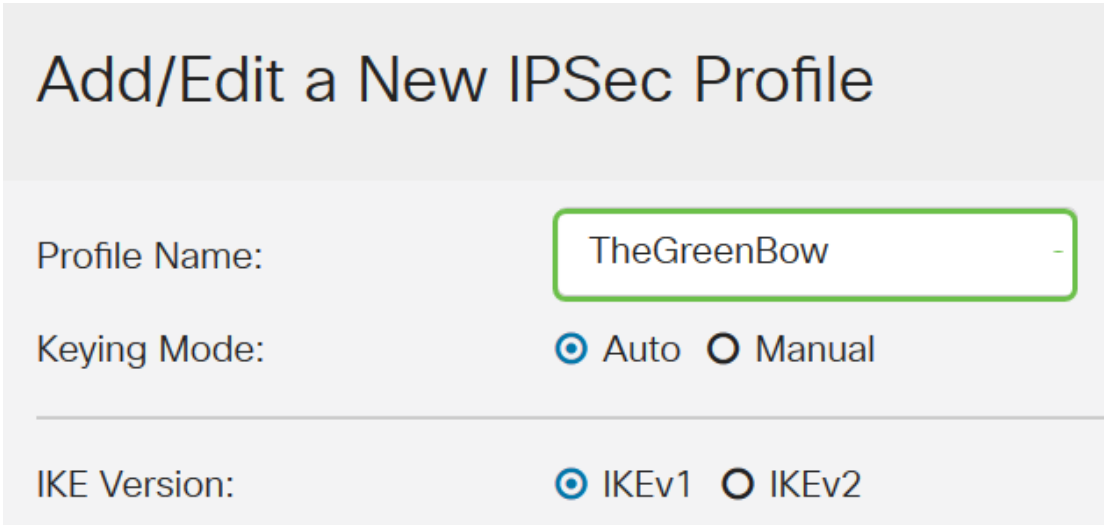
1단계. RV160 또는 RV260 라우터의 웹 기반 유틸리티에 로그인하고 **VPN** > **IPSec VPN** > IPSec **Profiles**를 선택합니다.

2단계. IPSec 프로파일 테이블에는 기존 프로파일이 표시됩니다.**더하기** 아이콘을 클릭하여 새 프로파일을 생성합니다.



참고: Amazon_Web_Services, Default 및 Microsoft_Azure는 기본 프로필입니다.

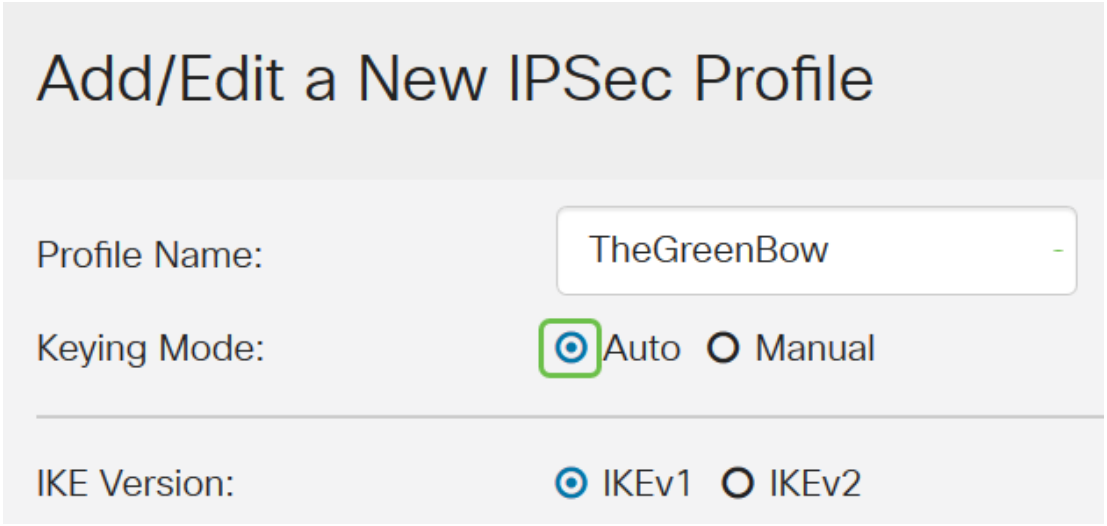
3단계. 프로파일 이름 필드에 프로파일 이름을 *생성합니다*.프로파일 이름은 특수 문자의 영숫자 문자 및 밑줄(_)만 포함해야 합니다.



4단계. 라디오 버튼을 클릭하여 프로필에서 인증에 사용할 키 교환 방법을 결정합니다.옵션은 다음과 같습니다.

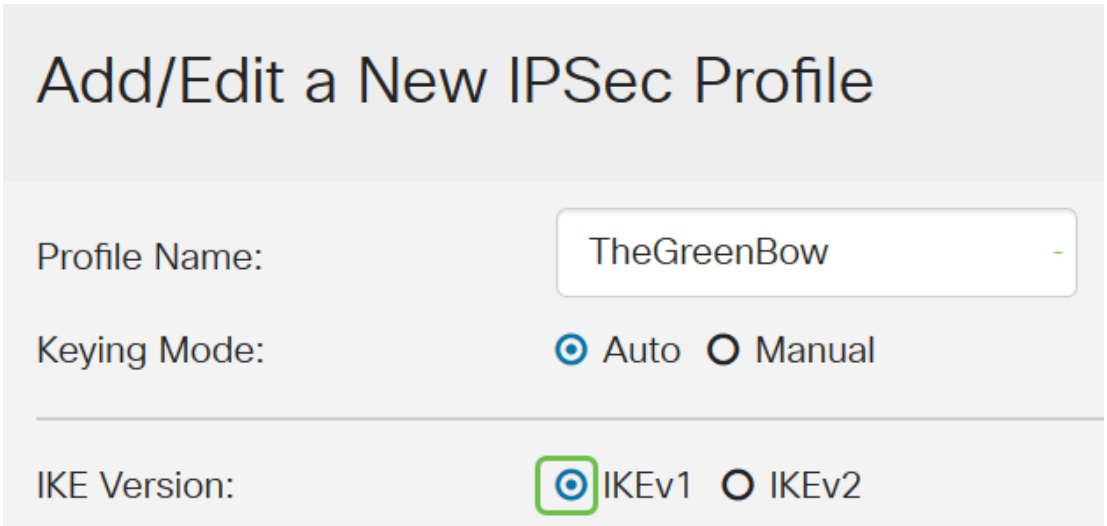
- 자동 — 정책 매개변수가 자동으로 설정됩니다.이 옵션은 데이터 무결성 및 암호화 키 교환을 위해 IKE(Internet Key Exchange) 정책을 사용합니다.이 옵션을 선택하면 Auto Policy Parameters(자동 정책 매개변수) 영역 아래의 컨피그레이션 설정이 활성화됩니다.

- 수동 — 이 옵션을 사용하면 VPN 터널의 데이터 암호화 및 무결성을 위한 키를 수동으로 구성할 수 있습니다.이 옵션을 선택하면 Manual Policy Parameters(수동 정책 매개변수) 영역 아래의 컨피그레이션 설정이 활성화됩니다.널리 사용되지 않습니다.



참고:이 예에서는 **자동**이 선택되었습니다.

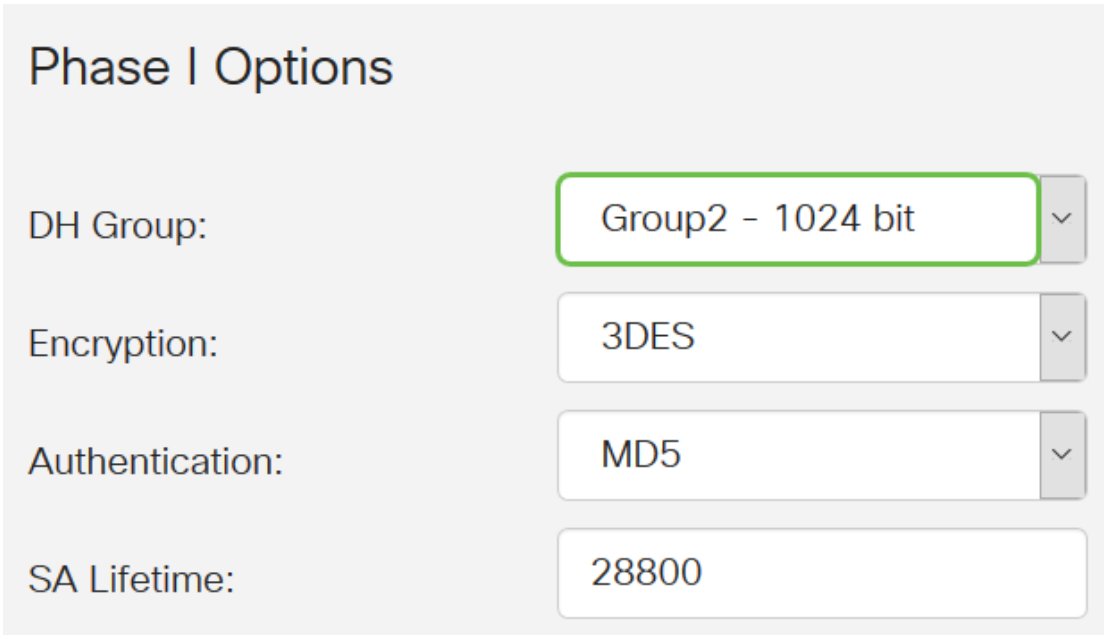
5단계. IKE 버전을 선택합니다.클라이언트 측에서 TheGreenBow를 설정할 때 동일한 버전이 선택되어 있는지 확인합니다.



1단계 및 2단계 설정 구성

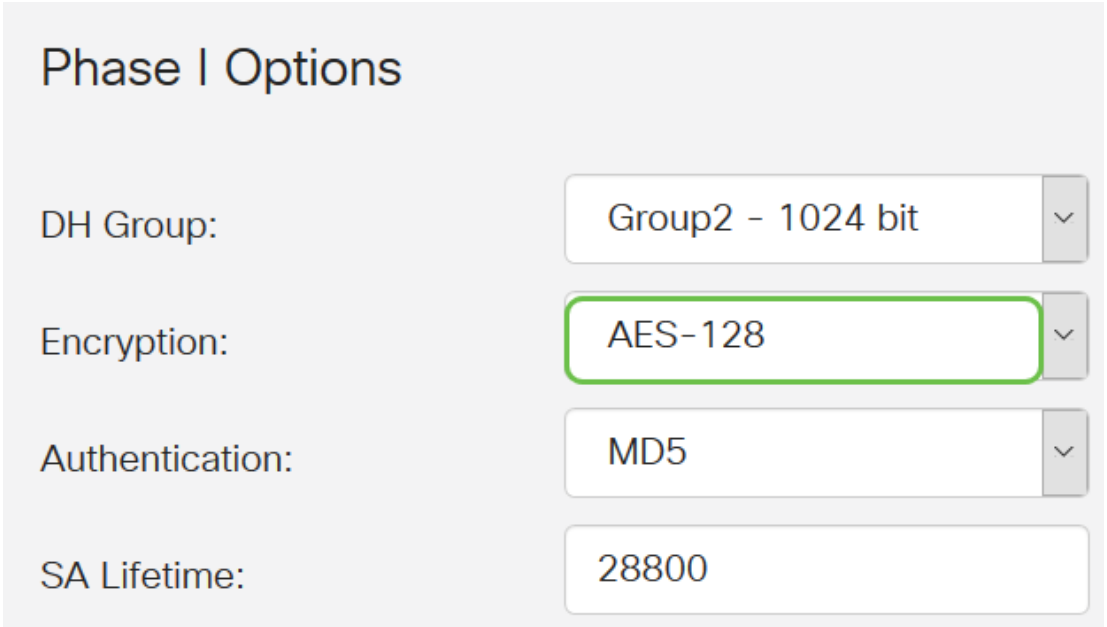
1단계. Phase 1 Options(1단계 옵션) 영역에서 *DH Group(DH 그룹)* 드롭다운 목록에서 1단계의 키와 함께 사용할 적절한 DH(Diffie-Hellman) 그룹을 선택합니다.Diffie-Hellman은 사전 공유 키 집합을 교환하기 위해 연결에 사용되는 암호화 키 교환 프로토콜입니다.알고리즘의 강도는 비트로 결정됩니다.옵션은 다음과 같습니다.

- Group2-1024비트 — 이 옵션은 키를 느리게 계산하지만 그룹 1보다 안전합니다.
- Group5-1536비트 — 이 옵션은 가장 느린 키를 계산하지만 가장 안전합니다.



2단계. *Encryption* 드롭다운 목록에서 암호화 방법을 선택하여 ESP(Encapsulating Security Payload) 및 ISAKMP(Internet Security Association and Key Management Protocol)를 암호화하고 해독합니다. 옵션은 다음과 같습니다.

- 3DES — 3중 데이터 암호화 표준권장되지 않습니다.일부 "차단 충돌" 공격에 취약하기 때문에 이전 버전과의 호환성이 필요한 경우에만 사용하십시오.
- AES-128 — 고급 암호화 표준은 128비트 키를 사용합니다.AES(Advanced Encryption Standard)는 DES보다 더 안전하도록 설계된 암호화 알고리즘입니다.AES는 더 큰 키 크기를 사용하여 메시지 해독에 알려진 유일한 방법은 침입자가 가능한 모든 키를 시도하기 위한 것입니다.
- AES-192 — 고급 암호화 표준은 192비트 키를 사용합니다.
- AES-256 — 고급 암호화 표준은 256비트 키를 사용합니다.가장 안전한 암호화 옵션입니다.

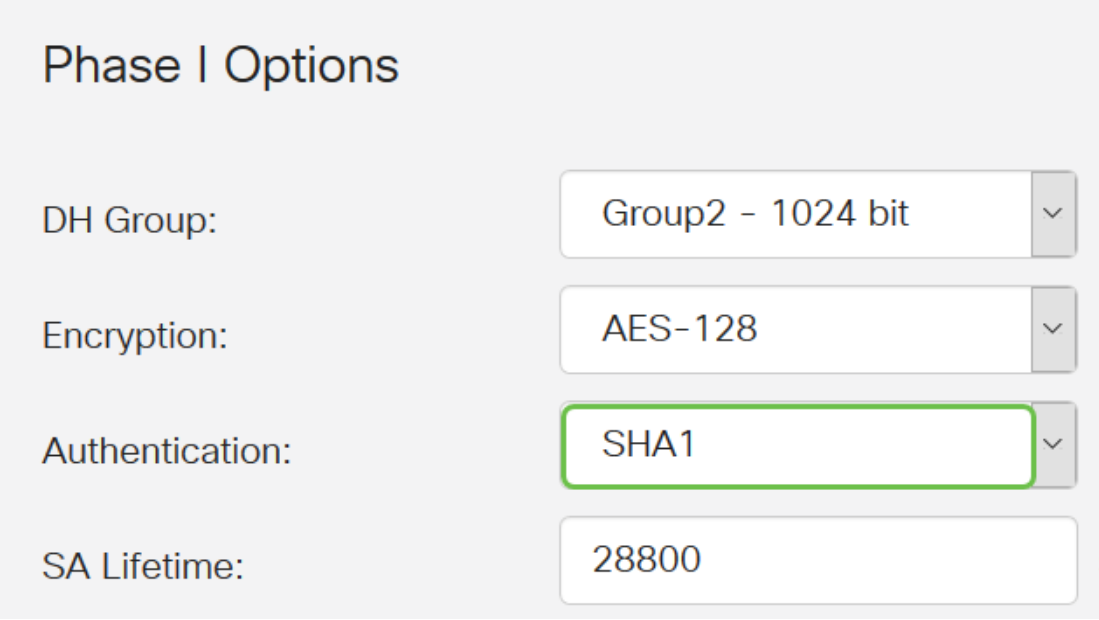


참고:AES는 DES와 3DES를 통한 암호화의 표준 방법으로 성능과 보안을 강화합니다.AES 키를 늘리면 성능이 저하되어 보안이 강화됩니다.

3단계. Authentication(*인증*) 드롭다운 목록에서 ESP 및 ISAKMP의 인증 방법을 결정하는 인증 방법을 선택합니다.옵션은 다음과 같습니다.

- MD5 — 메시지 다이제스트 알고리즘에 128비트 해시 값이 있습니다.
- SHA-1 — 보안 해시 알고리즘에는 160비트 해시 값이 있습니다.
- SHA2-256 — 256비트 해시 값을 사용하는 보안 해시 알고리즘.가장 안전하고 권장되는 알고리즘입니다.

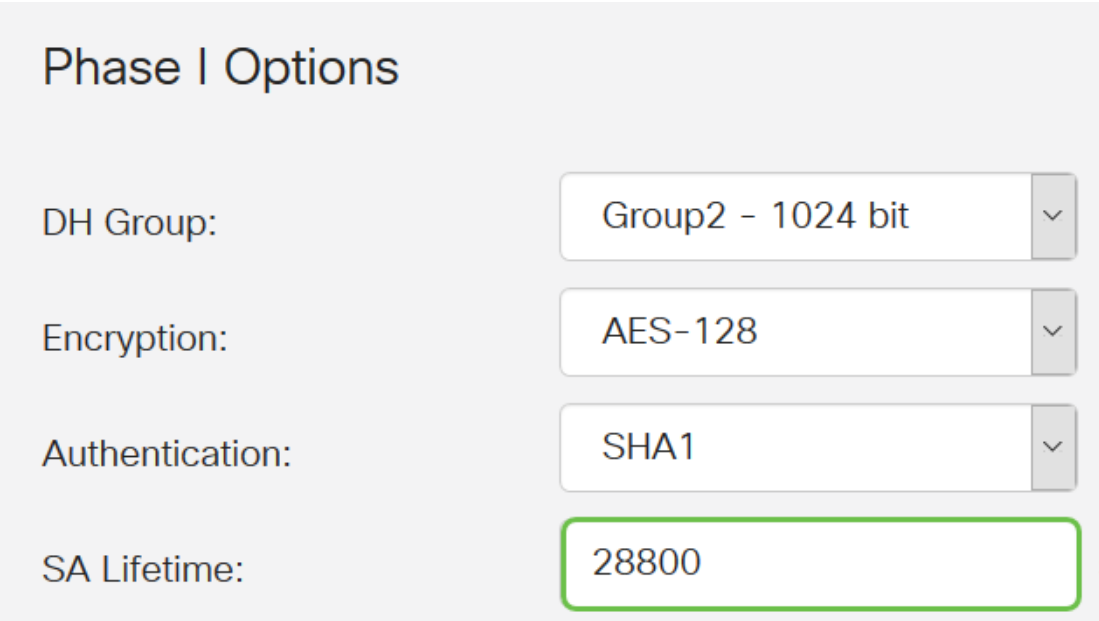
참고:VPN 터널의 양쪽 끝이 동일한 인증 방법을 사용하는지 확인합니다.



참고:MD5 및 SHA는 모두 암호화 해시 함수입니다.데이터를 가져와서 압축하고 일반적으로 재현할 수 없는 고유한 16진수 출력을 만듭니다.이 예에서는 SHA1이 선택됩니다.

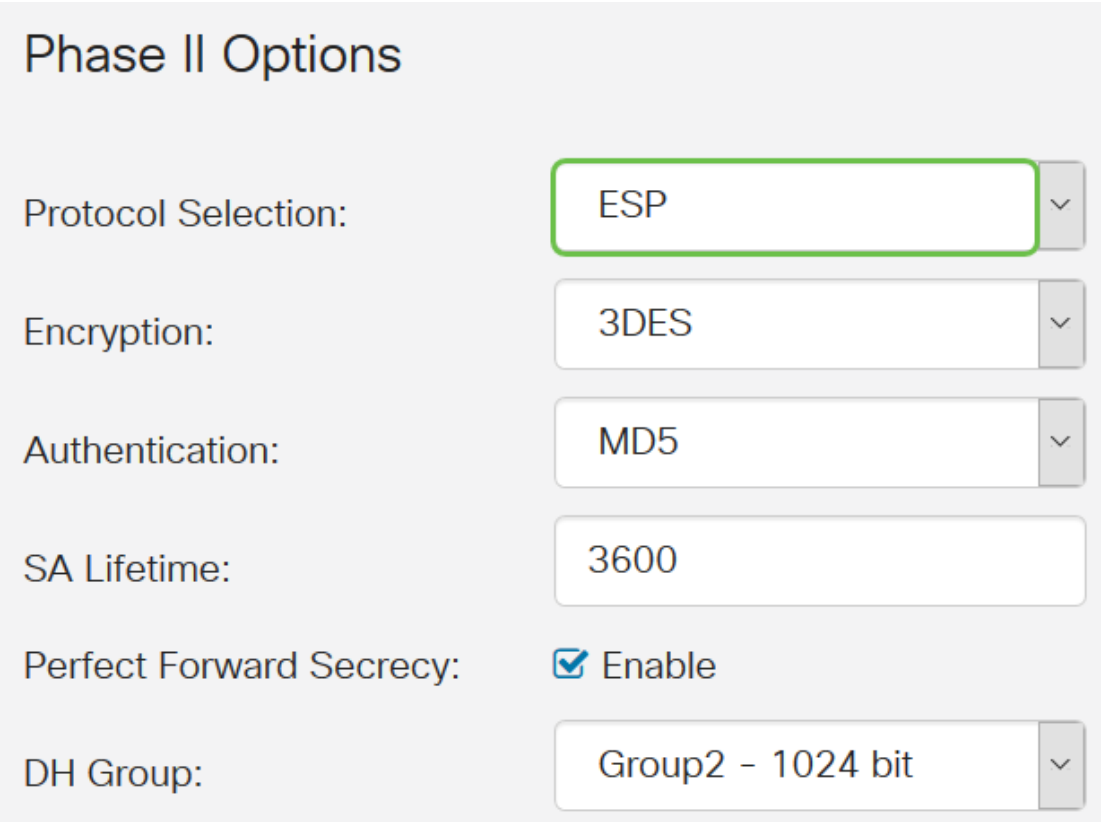
4단계. *SA Lifetime* 필드에 120에서 86400 사이의 값을 입력합니다. 기본값은 28800입니다. *SA Lifetime (Sec)*은 이 단계에서 IKE SA가 활성화된 시간을 초 단위로 알려줍니다.기존 SA가 만료될 때 새 SA를 사용할 수 있도록 수명 만료 전에 새 SA(Security Association)가 협상됩니다.기본값은 28800이고 범위는 120~86400입니다. 28800초를 I단계의 SA Lifetime으로 사용합니다.

참고:1단계의 SA 수명이 2단계 SA 수명보다 긴 것이 좋습니다.Phase I를 Phase II보다 짧게 만들면 데이터 터널이 아닌 터널을 앞뒤로 반복해서 재협상해야 합니다.데이터 터널은 더 많은 보안이 필요하므로 1단계보다 짧은 2단계의 수명을 제공하는 것이 좋습니다.



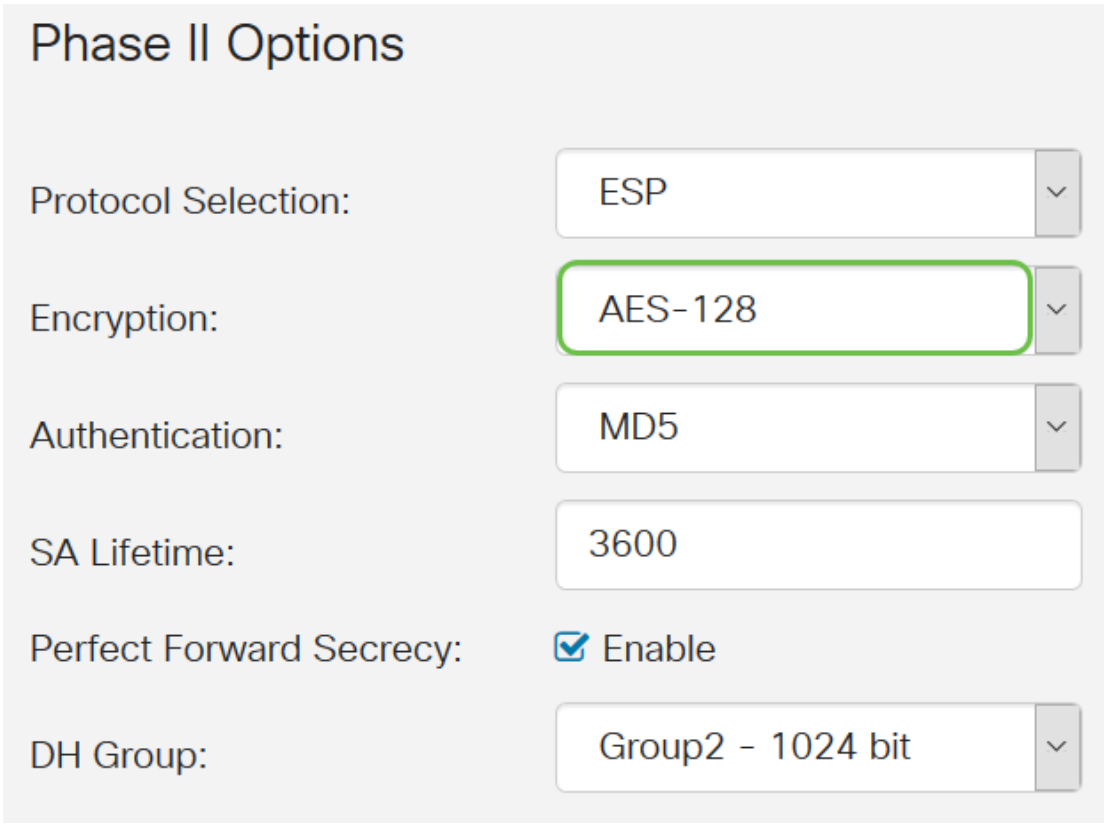
5단계. *II* 단계 옵션 영역의 프로토콜 선택 드롭다운 목록에서 협상의 두 번째 단계에 적용할 프로토콜 유형을 선택합니다.옵션은 다음과 같습니다.

- ESP — 이 옵션은 보안 페이로드 캡슐화라고도 합니다.이 옵션은 보호할 데이터를 캡슐화합니다.이 옵션을 선택한 경우 6단계로 이동하여 암호화 방법을 선택합니다.
- AH — 이 옵션은 AH(Authentication Header)라고도 합니다. 데이터 인증 및 선택적 재전송 방지 서비스를 제공하는 보안 프로토콜입니다.AH는 보호할 IP 데이터그램에 포함되어 있습니다.이 옵션을 선택한 경우 7단계로 건너뜁니다.



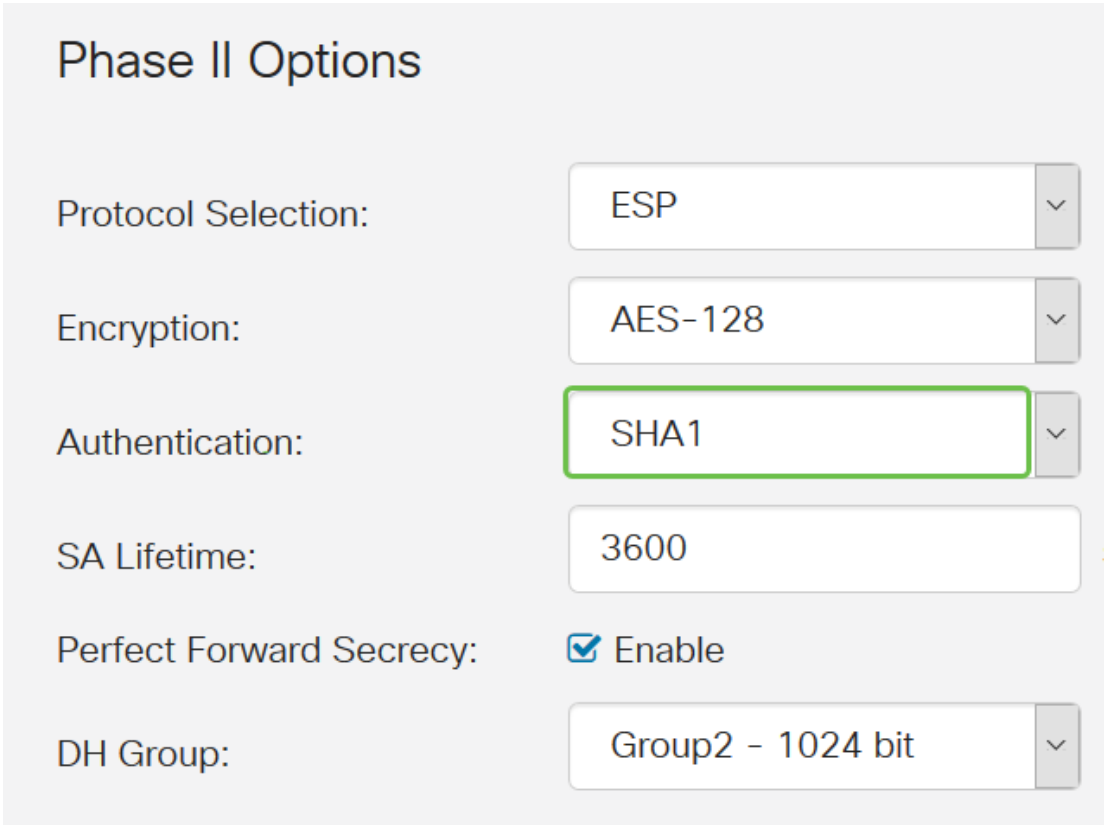
6단계. 6단계에서 ESP를 선택한 경우 *암호화*를 선택합니다.옵션은 다음과 같습니다.

- 3DES — 3중 데이터 암호화 표준
- AES-128 — 고급 암호화 표준은 128비트 키를 사용합니다.
- AES-192 — 고급 암호화 표준은 192비트 키를 사용합니다.
- AES-256 — 고급 암호화 표준은 256비트 키를 사용합니다.

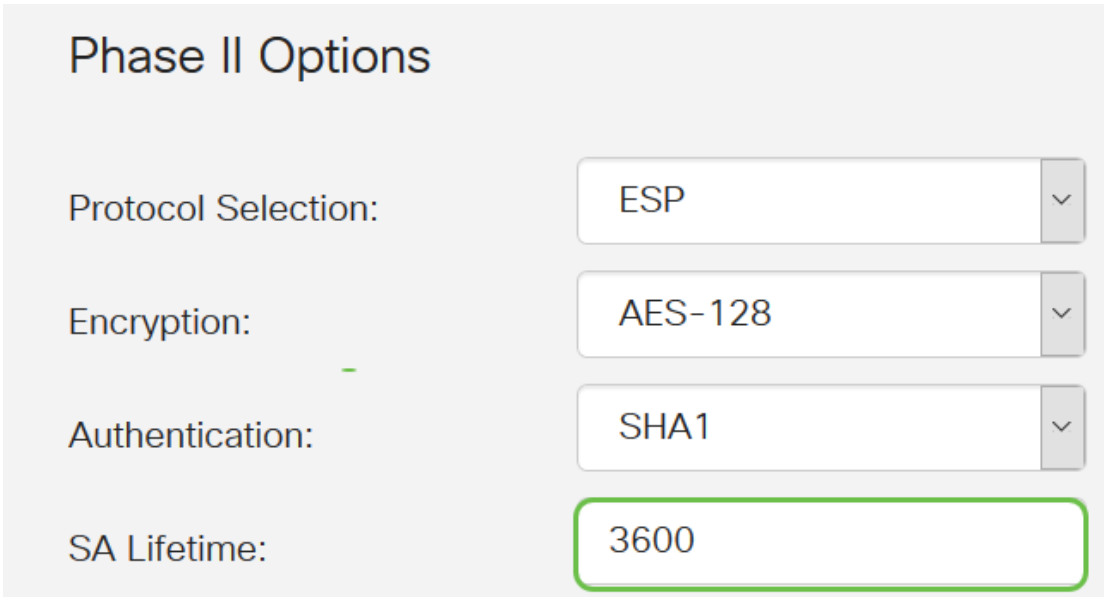


7단계. Authentication(*인증*) 드롭다운 목록에서 ESP 및 ISAKMP의 인증 방법을 결정하는 인증 방법을 선택합니다.옵션은 다음과 같습니다.

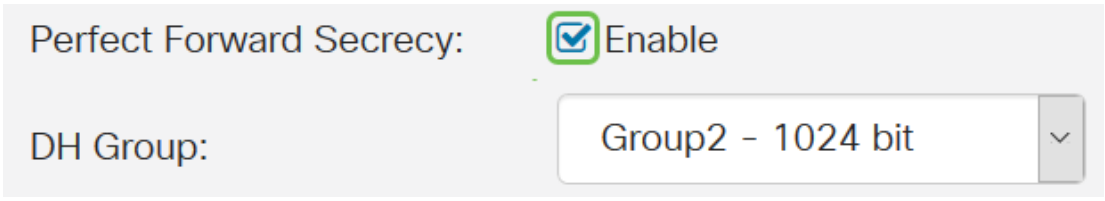
- MD5 — 메시지 다이제스트 알고리즘에 128비트 해시 값이 있습니다.
- SHA-1 — 보안 해시 알고리즘에는 160비트 해시 값이 있습니다.
- SHA2-256 — 256비트 해시 값을 사용하는 보안 해시 알고리즘.



8단계. *SA Lifetime* 필드에 120에서 28800 사이의 값을 입력합니다. 이 단계에서는 IKE SA가 활성 상태로 유지되는 시간입니다.기본값은 3600입니다.

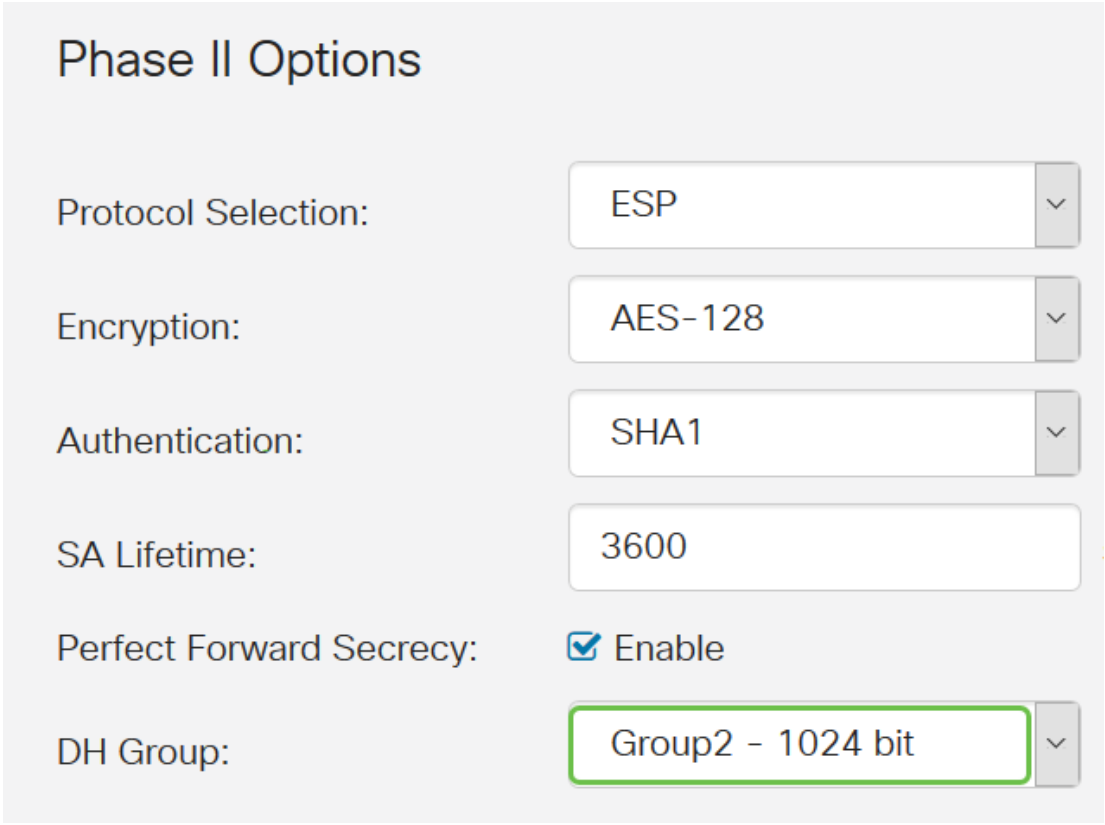


9단계. (선택 사항) Enable **Perfect** Forward Secrecy 확인란을 선택하여 IPsec 트래픽 암호화 및 인증을 위한 새 키를 생성합니다.Perfect Forward Secrecy는 공개 키 암호화를 사용하여 인터넷을 통해 전송되는 통신의 보안을 개선하는 데 사용됩니다.이 기능을 활성화하려면 확인란을 선택하고, 이 기능을 비활성화하려면 확인란의 선택을 취소합니다.이 기능을 사용하는 것이 좋습니다.



10단계. *DH 그룹* 드롭다운 목록에서 2단계의 키와 함께 사용할 DH 그룹을 선택합니다. 옵션은 다음과 같습니다.

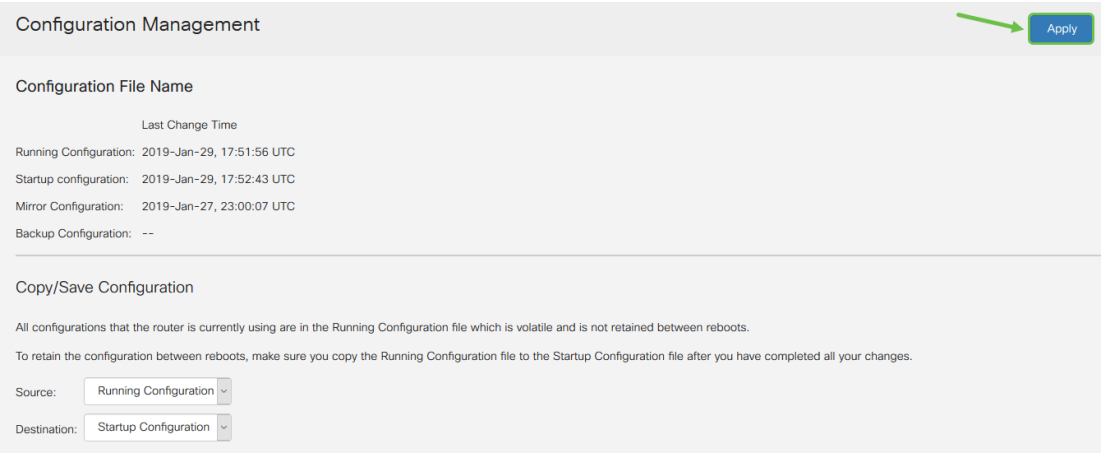
- Group2-1024비트 — 이 옵션은 키를 더 빠르게 계산하지만 안전하지 않습니다.
- Group5-1536비트 — 이 옵션은 가장 느린 키를 계산하지만 가장 안전합니다.



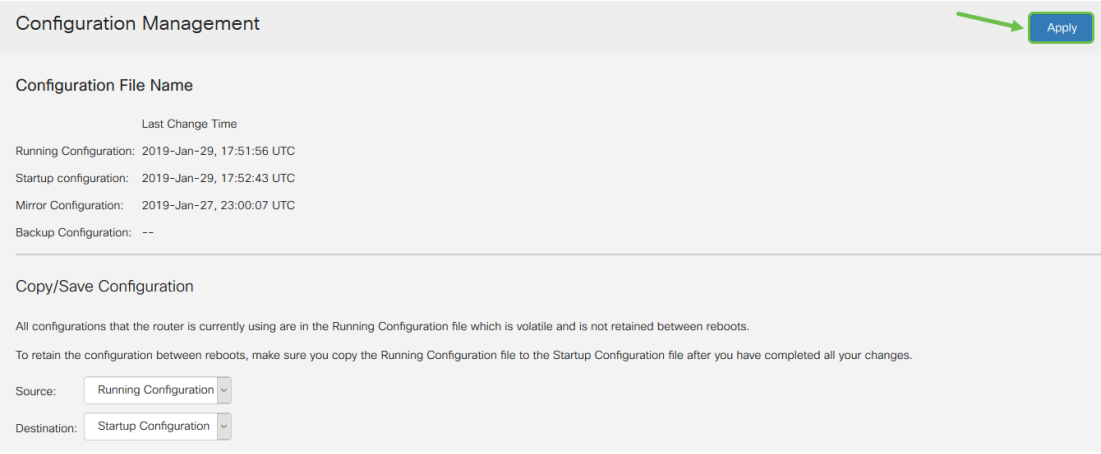
11단계. 적용을 **클릭합니다**.

12단계. **저장**을 클릭하여 구성을 영구적으로 저장합니다.

13단계. **Apply(적용)**를 다시 한 번 클릭하여 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.



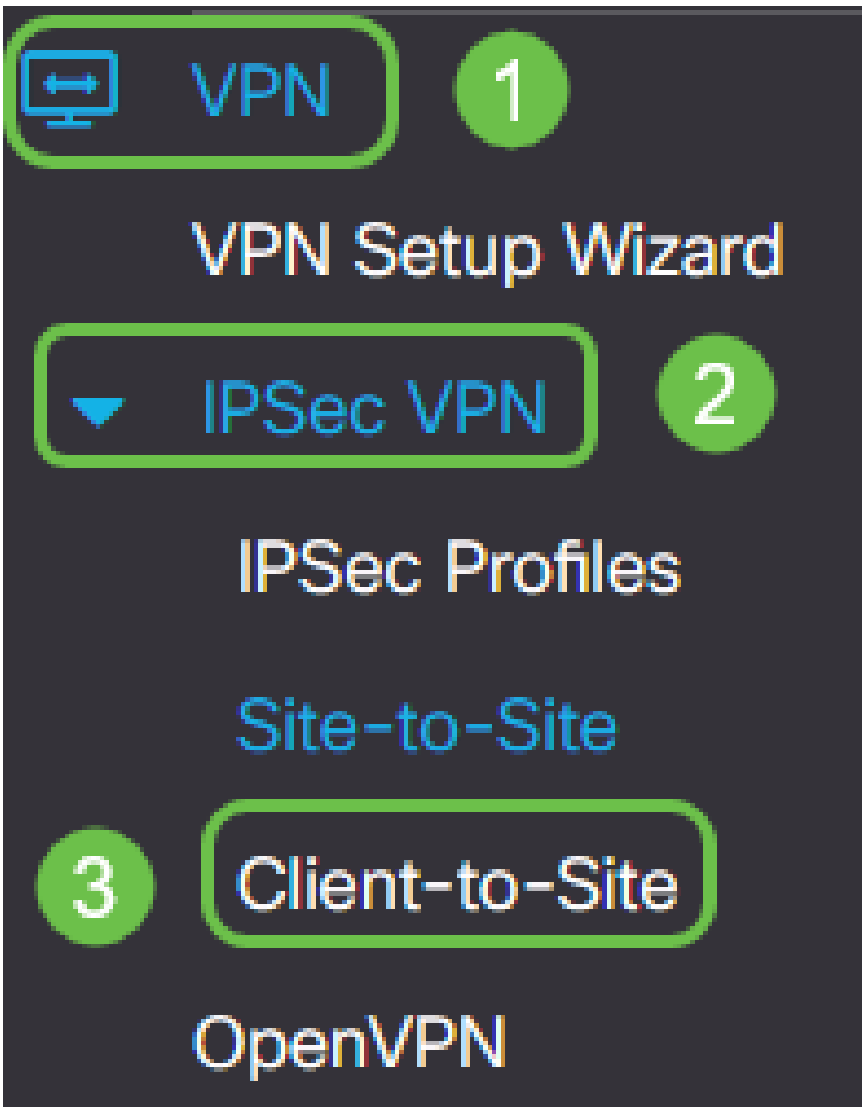
14단계. 확인 메시지가 표시되면 **확인**을 클릭합니다.



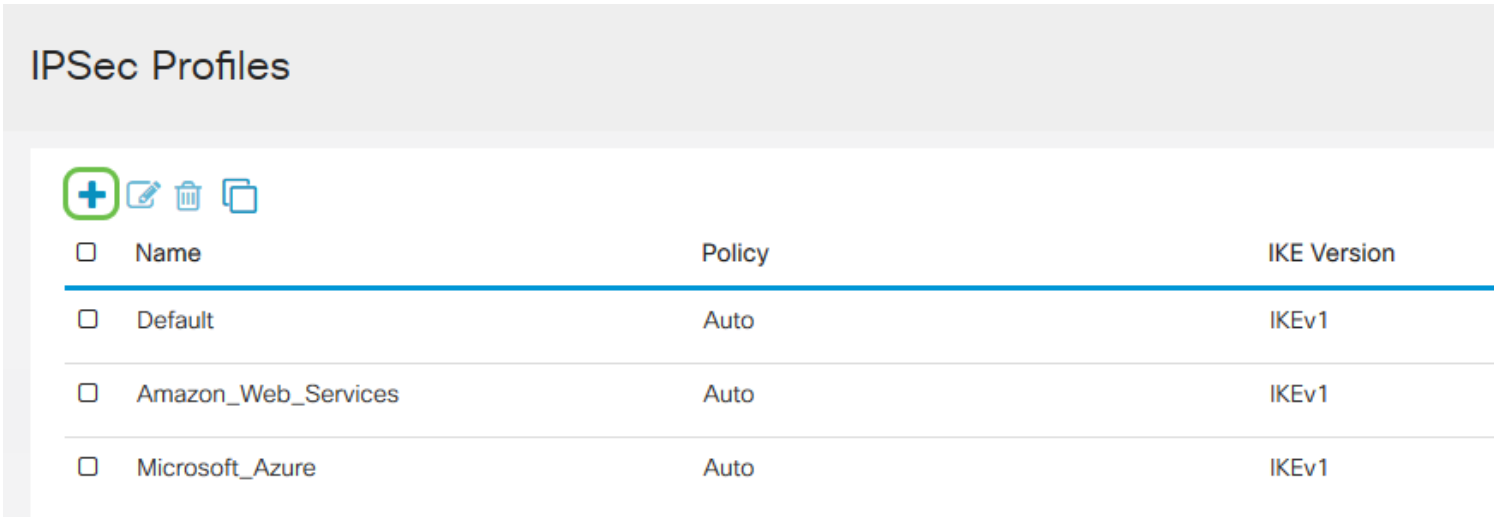
이제 RV160 또는 RV260 라우터에서 IPsec 프로파일을 성공적으로 구성했어야 합니다.

클라이언트-사이트 프로파일 생성

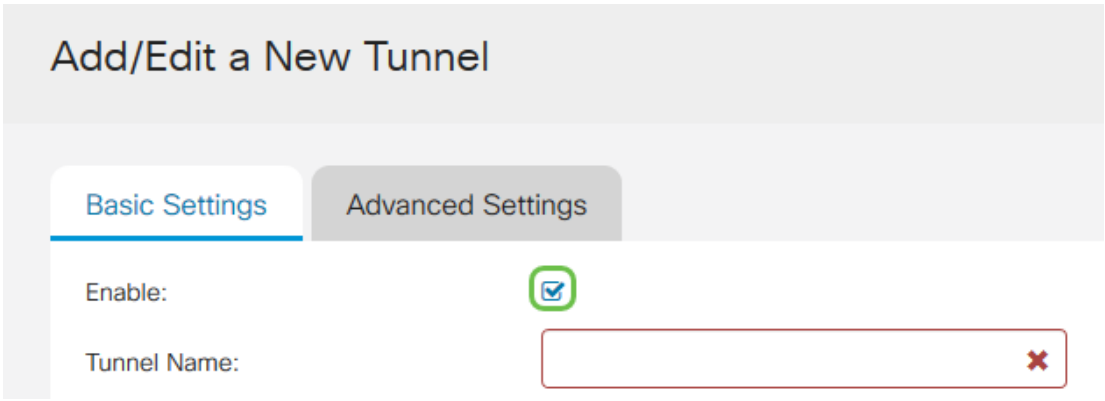
1단계. **VPN > IPSec VPN > Client-to-Site를 선택합니다**.



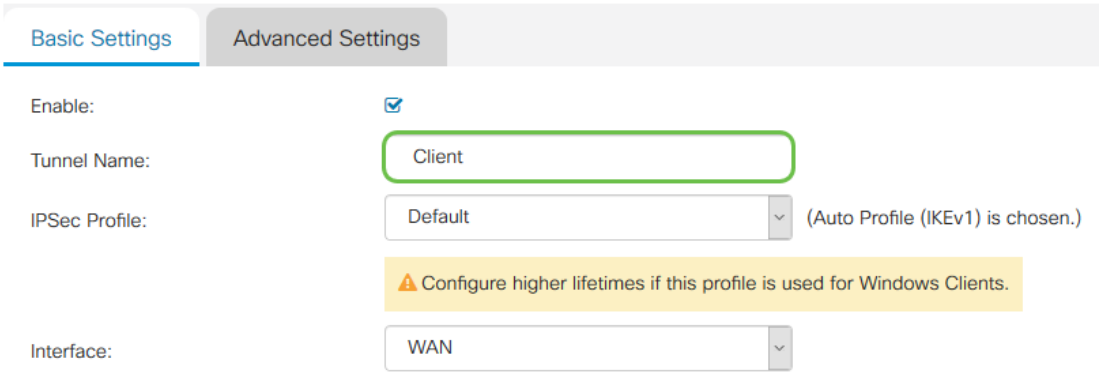
2단계. **더하기** 아이콘을 클릭합니다.



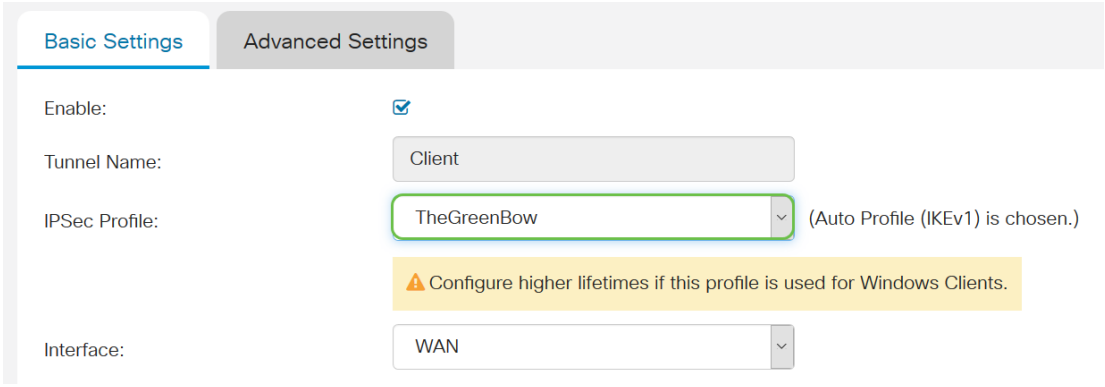
3단계. Basic Settings(기본 설정) 탭에서 Enable(**활성화**) 확인란을 선택하여 VPN 프로파일이 활성화되어 있는지 확인합니다.



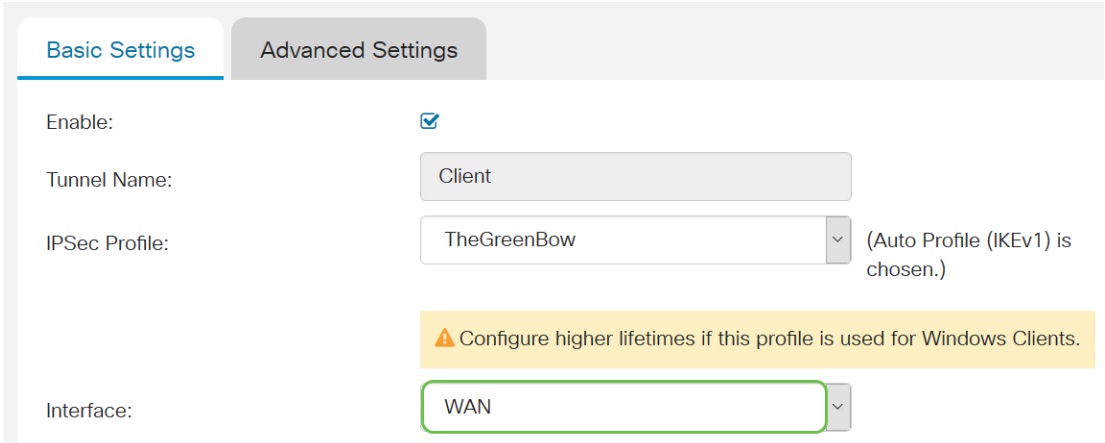
4단계. Tunnel *Name* 필드에 VPN 연결의 이름을 입력합니다.



5단계. IPsec 드롭다운 목록에서 사용할 IPsec *프로필*을 선택합니다.



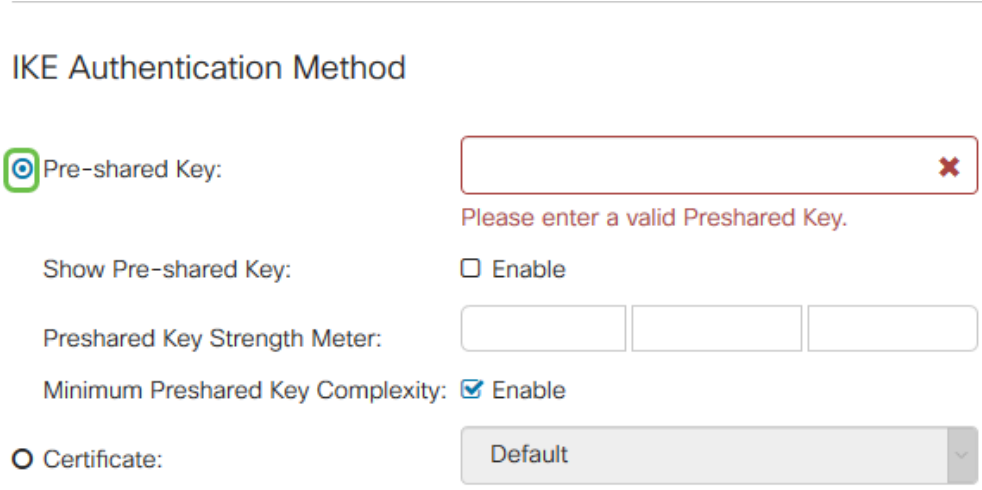
6단계. Interface(인터페이스) 드롭다운 목록에서 Interface(인터페이스)를 선택합니다.



참고:옵션은 사용 중인 라우터 모델에 따라 달라집니다.이 예에서는 WAN을 선택합니다.

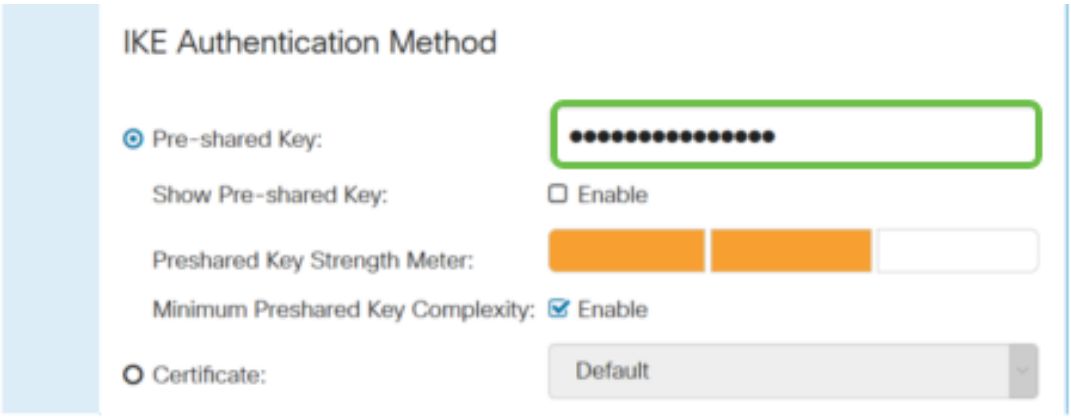
7단계. IKE 인증 방법을 선택합니다.옵션은 다음과 같습니다.

- 사전 공유 키 — 이 옵션을 사용하면 VPN 연결에 공유 비밀번호를 사용할 수 있습니다.
- 인증서 — 이 옵션은 이름 또는 IP 주소, 일련 번호, 인증서 만료 날짜, 인증서 전달자의 공개 키 사본 등의 정보를 포함하는 디지털 인증서를 사용합니다.

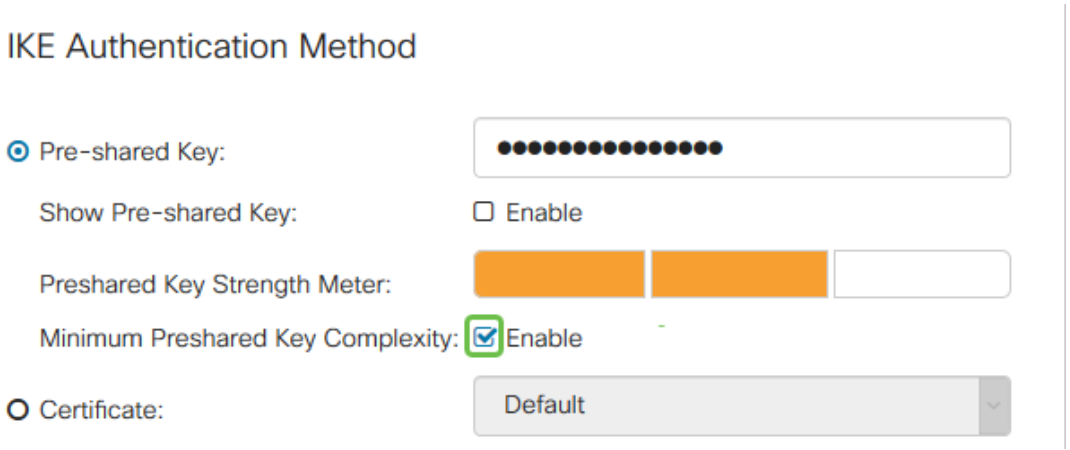


참고:사전 공유 키는 원하는 대로 사용할 수 있으며, 컴퓨터에서 TheGreenBow 클라이언트를 설정할 때 사이트 및 클라이언트와 일치해야 합니다.

8단계. Pre-shared *Key* 필드에 연결 비밀번호를 입력합니다.

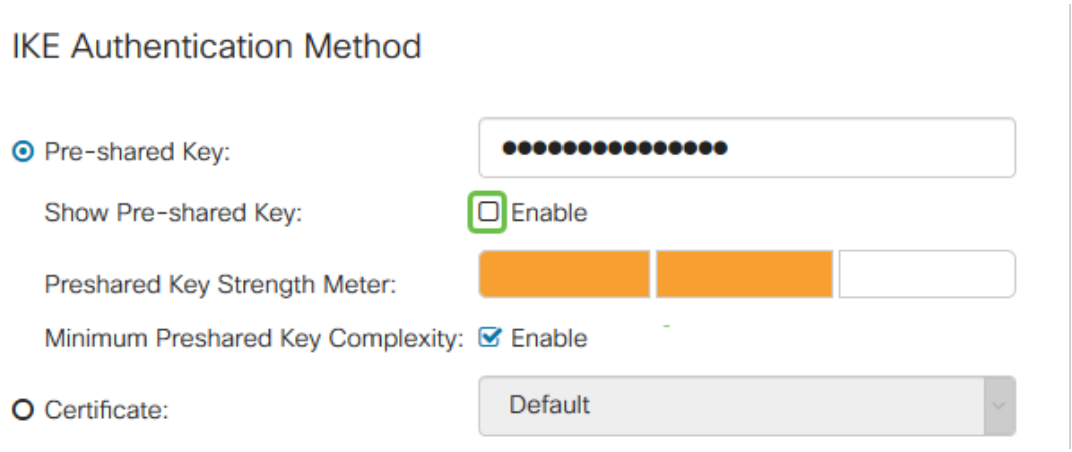


9단계. (선택 사항) 간단한 비밀번호를 사용하려면 *Minimum Pre-shared Key Complexity Enable(사전 공유 키 복잡성 최소 활성화)* 확인란의 선택을 취소합니다.



참고:이 예에서는 최소 사전 공유 키 복잡성이 활성화되어 있습니다.

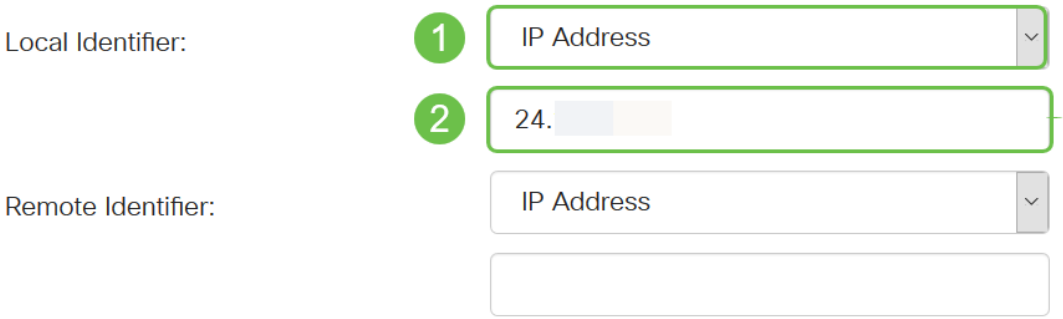
10단계(선택 사항) Show Pre-shared Key Enable(*사전 공유 키* **활성화**) 확인란을 선택하여 비밀번호가 일반 텍스트로 표시됩니다.



참고:이 예에서는 Show Pre-shared key(사전 공유 키 표시)가 비활성화된 상태로 유지됩니다.

11단계. *Local Identifier* 드롭다운 목록에서 로컬 식별자를 선택합니다.옵션은 다음과 같습니다.

- 로컬 WAN IP — 이 옵션은 VPN 게이트웨이의 WAN(Wide Area Network) 인터페이스의 IP 주소를 사용합니다.
- IP Address — 이 옵션을 사용하면 VPN 연결에 대한 IP 주소를 수동으로 입력할 수 있습니다.사이트(사무실)에 있는 라우터의 WAN IP 주소입니다.
- FQDN — 이 옵션은 FQDN(Fully Qualified Domain Name)이라고도 합니다. 이 기능을 사용하면 인터넷의 특정 컴퓨터에 전체 도메인 이름을 사용할 수 있습니다.
- 사용자 FQDN — 이 옵션을 사용하면 인터넷의 특정 사용자에 대해 전체 도메인 이름을 사용할 수 있습니다.

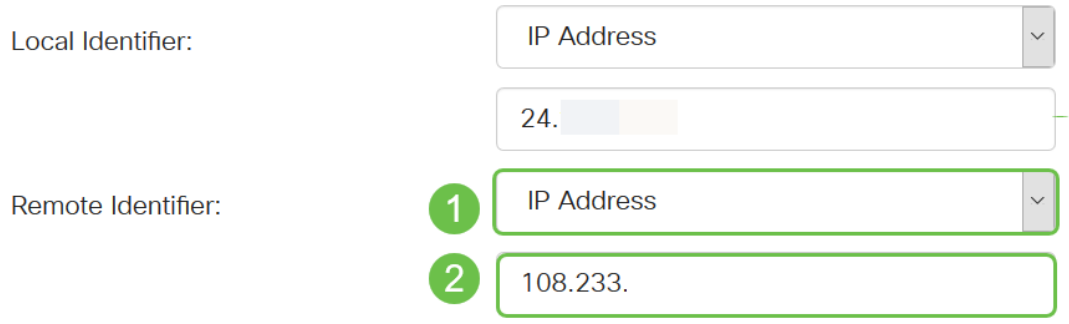


참고:이 예에서는 IP Address(IP 주소)가 선택되고 사이트에 있는 라우터의 WAN IP 주소가 입력됩니다.이 예에서는 24.x.x.x를 입력했습니다.개인 정보 보호를 위해 전체 주소가 불분명해졌습니다.

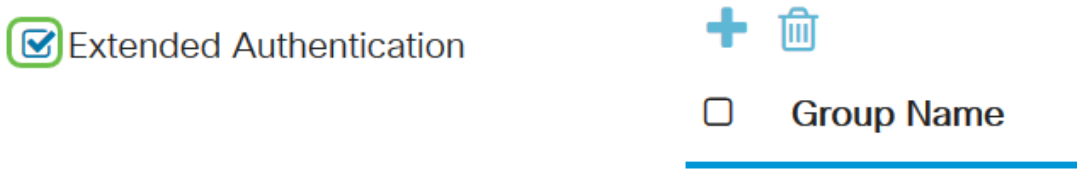
12단계. 원격 호스트의 식별자를 선택합니다.옵션은 다음과 같습니다.

- IP Address — 이 옵션은 VPN 클라이언트의 WAN IP 주소를 사용합니다.WAN IP 주소를 확인하려면 웹 브라우저에 "내 IP가 무엇이냐"를 입력할 수 있습니다.클라이언트 IP 주소입니다.
- FQDN — 정규화된 도메인 이름.이 옵션을 사용하면 인터넷의 특정 컴퓨터에 대해 전체 도메인 이름을 사용할 수 있습니다.
- 사용자 FQDN — 이 옵션을 사용하면 인터넷의 특정 사용자에 대해 전체 도메인 이름을 사용할 수 있습니다.

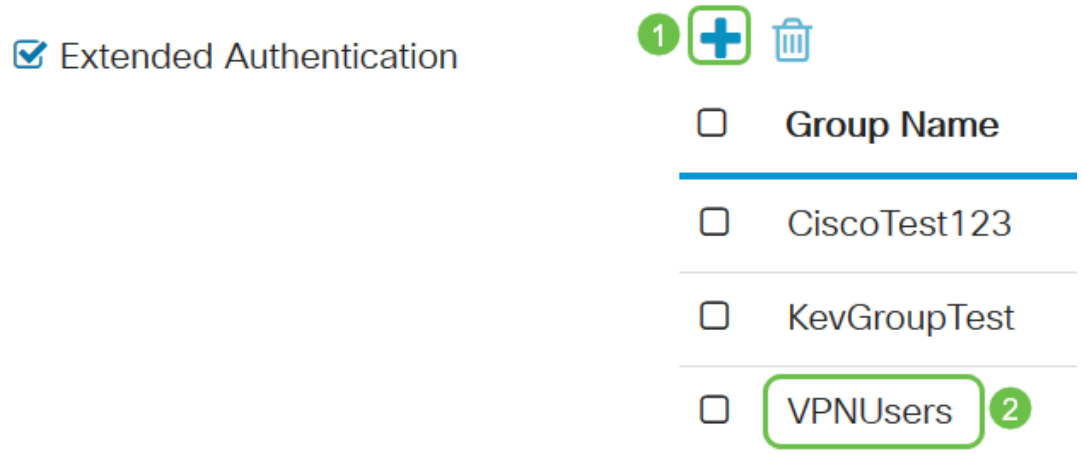
참고:이 예에서는 IP Address(IP 주소)가 선택되고 클라이언트 위치에 있는 라우터의 현재 IPv4 주소가 입력됩니다.웹 브라우저에서 "내 IP 주소"를 검색하여 확인할 수 있습니다.이 주소는 변경될 수 있으므로 컨피그레이션이 성공한 후 연결하는 데 문제가 있는 경우 클라이언트와 사이트에서 모두 확인하고 변경할 수 있습니다.



13단계. (선택 사항) Extended **Authentication** 확인란을 선택하여 기능을 활성화합니다.활성화되면 원격 사용자가 VPN에 대한 액세스 권한을 부여받기 전에 자격 증명에서 키를 입력해야 하는 추가 수준의 인증이 제공됩니다.



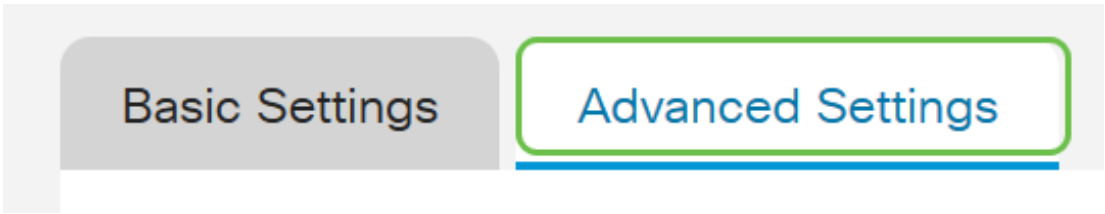
14단계(선택 사항) **더하기** 아이콘을 클릭하여 확장 인증을 사용할 그룹을 선택하고 드롭다운 목록에서 사용자를 선택합니다.



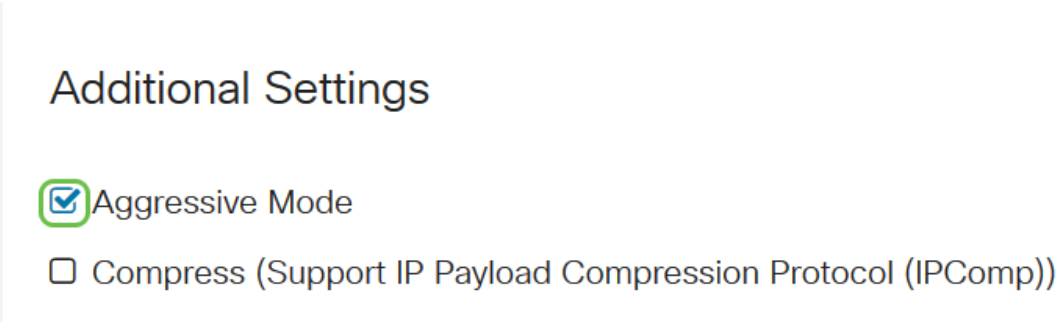
참고:이 예에서는 VPNUsers**가** 선택됩니다.

15단계. *Pool Range for Client LAN(클라이언트 LAN의 풀 범위)*에서 VPN 클라이언트에 할당할 수 있는 첫 번째 IP 및 끝 IP 주소를 입력합니다.이 주소는 사이트 주소와 겹치지 않는 주소 풀이어야 합니다.이를 가상 인터페이스라고 할 수 있습니다.가상 인터페이스를 변경해야 한다는 메시지가 나타나면 이를 수정할 수 있습니다.

16단계. **고급 설정 탭을** 선택합니다.

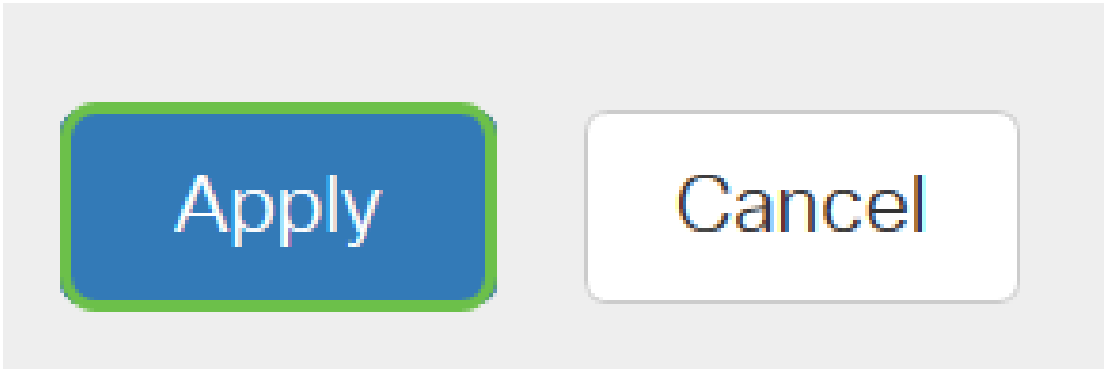


17단계. (선택 사항) 페이지 아래쪽으로 스크롤하고 **Aggressive Mode(적극적인 모드)를** 선택합니다.Aggressive Mode 기능을 사용하면 IPsec(IP 보안) 피어에 대한 RADIUS 터널 특성을 지정하고 터널과의 IKE(Internet Key Exchange) 적극적인 모드 협상을 시작할 수 있습니다.Aggressive Mode(적극적인 모드)와 Main Mode(기본 모드)에 대한 자세한 내용을 보려면 여기를 클릭하십시오.

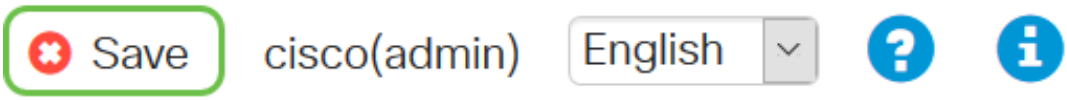


참고: Compress 확인란을 사용하면 라우터가 연결을 시작할 때 압축을 제안할 수 있습니다.이 프로토콜은 IP 데이터그램의 크기를 줄입니다.응답자가 이 제안을 거부할 경우 라우터는 압축을 구현하지 않습니다.라우터가 responder인 경우 압축이 활성화되지 않은 경우에도 압축을 수락합니다.이 라우터에 대해 이 기능을 활성화한 경우 원격 라우터(터널의 다른 쪽 끝)에서 활성화해야 합니다. 이 예에서 *압축*은 선택 취소된 상태로 남았습니다.

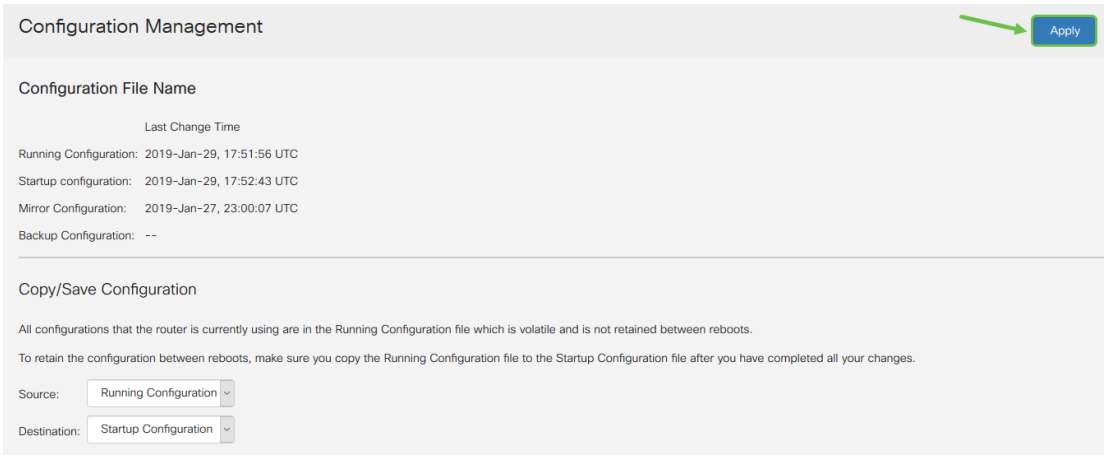
18단계. 적용을 **누릅니다**.



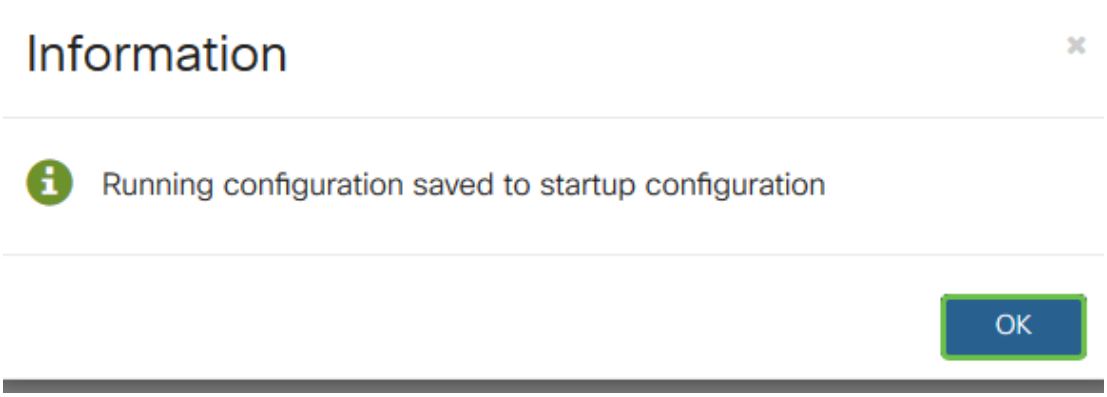
19단계. **저장**을 클릭합니다.



20단계. **Apply(적용)**를 다시 한 번 클릭하여 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.



21단계. 확인 메시지가 표시되면 **확인**을 클릭합니다.



이제 GreenBow VPN Client용 라우터에 클라이언트-사이트 터널을 구성해야 합니다.

원격 작업자 컴퓨터에서 GreenBow VPN 클라이언트 구성

1단계 설정 구성

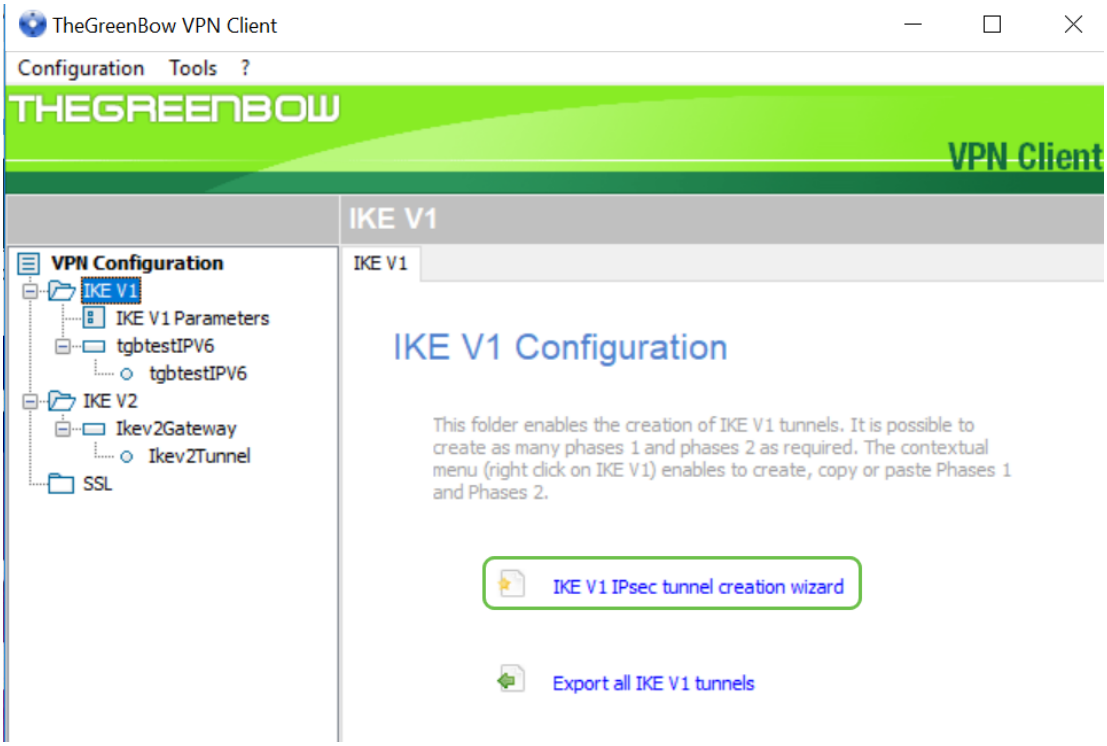
TheGreenBow IPsec VPN Client 소프트웨어의 최신 릴리스를 다운로드하려면 여기를 클릭하십시오.

1단계. GreenBow VPN Client 아이콘을 마우스 오른쪽 버튼으로 클릭합니다.작업 표시줄의 오른쪽 아래 모서리에 있습니다.

2단계. 구성 **패널을 선택합니다**.

참고:이것은 Windows 컴퓨터의 예입니다.사용하는 소프트웨어에 따라 달라질 수 있습니다.

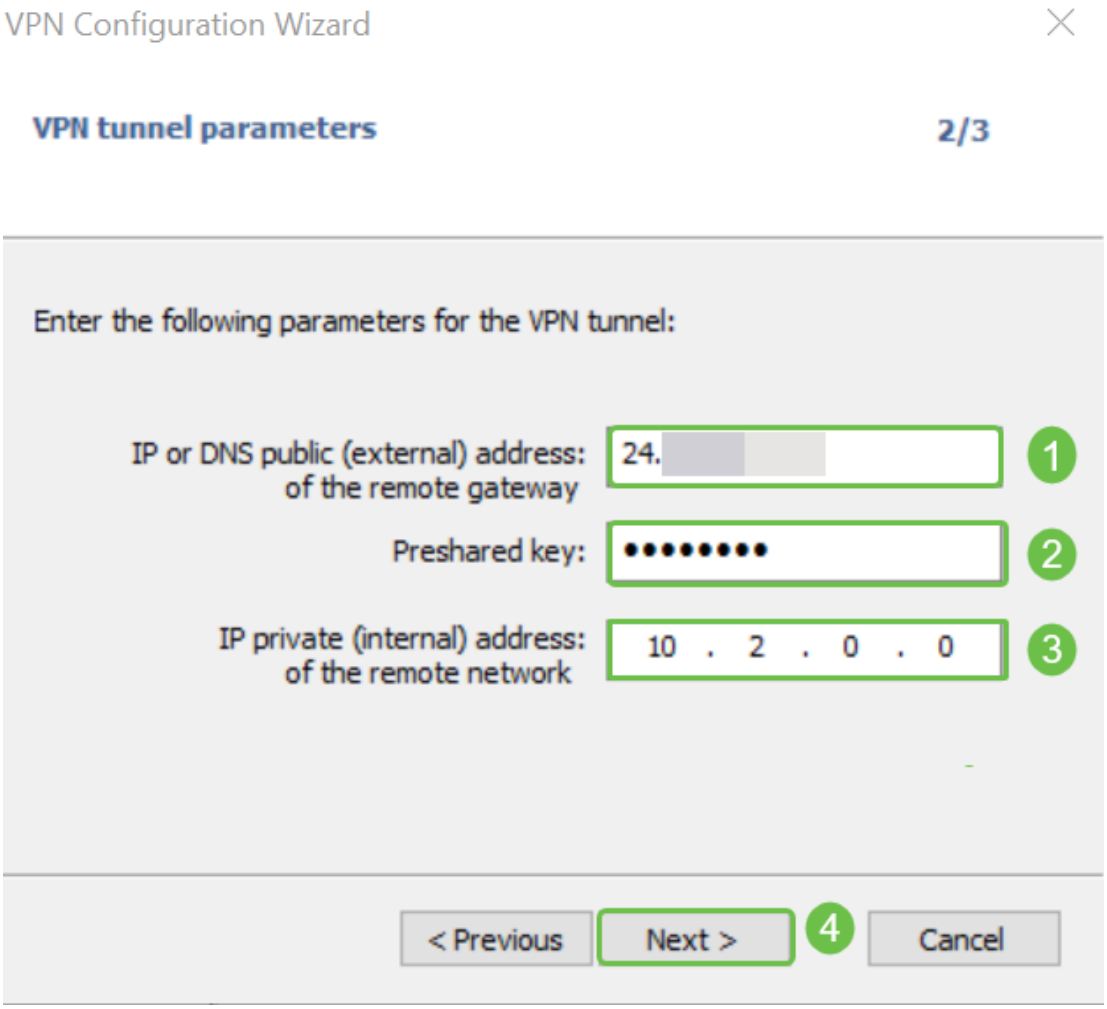
3단계. **IKE V1 IPsec 터널 생성 마법사를 선택합니다**.



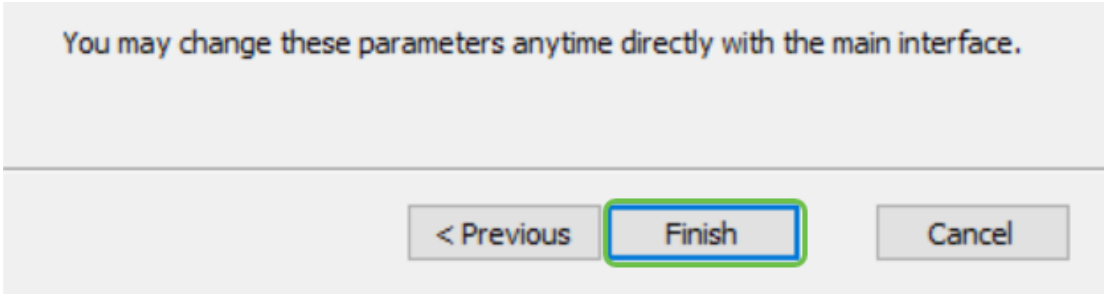
참고:이 예에서는 IKE 버전 1을 구성하고 있습니다.IKE 버전 2를 구성하려면 동일한 단계를 따르지만 IKE V2 폴더를 마우스 오른쪽 버튼으로 클릭합니다.또한 사이트의 라우터에 있는 IPsec 프로파일에 대해 IKEv2를 선택해야 합니다.

4단계. 파일 서버가 있는 사이트(사무실)에 있는 라우터의 공용 WAN IP 주소, 사전 공유 키 및 원격

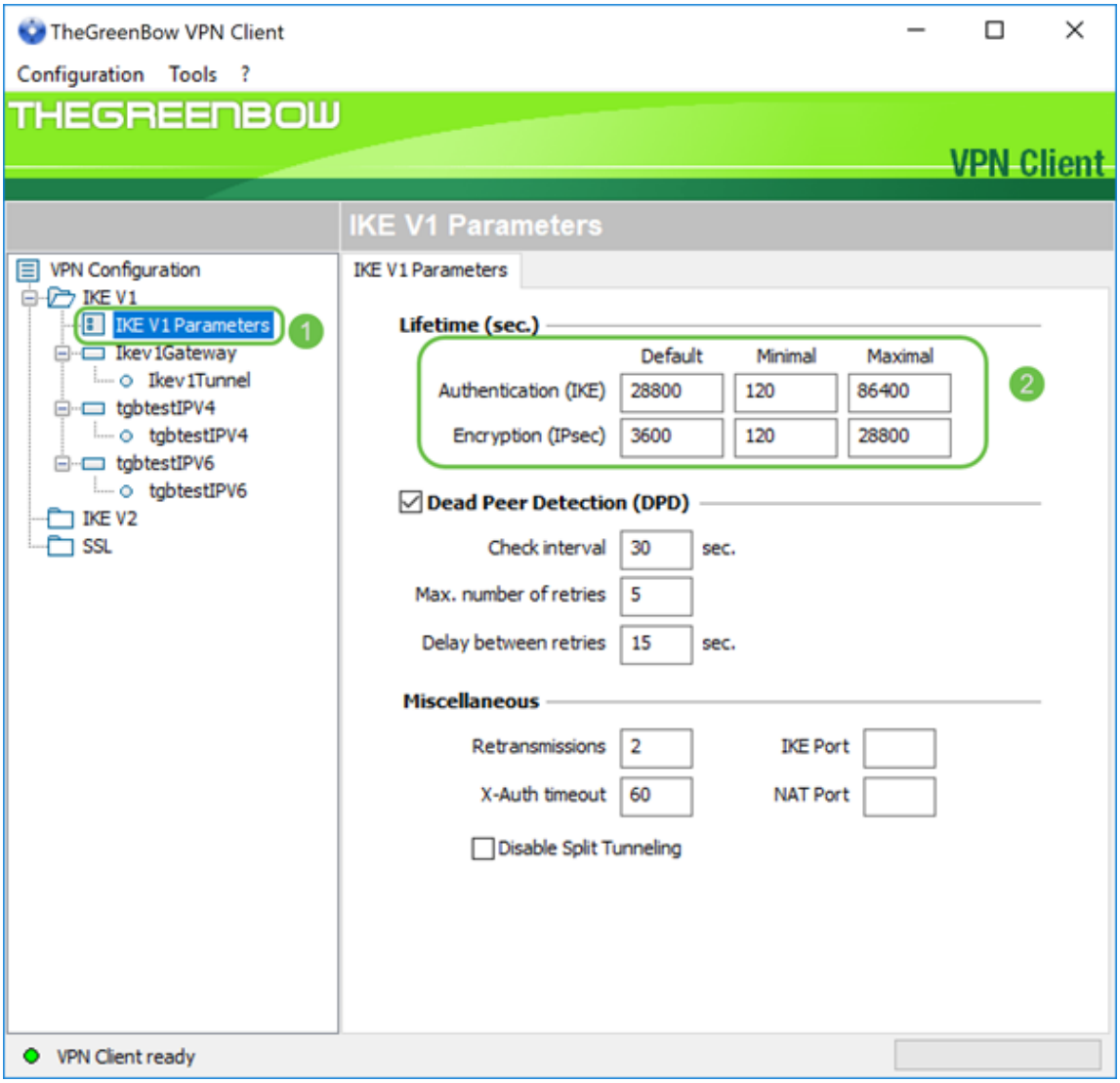
네트워크의 사이트 내부 주소를 입력합니다.Next(**다음)를 클릭합니다**.이 예에서는 사이트가 24.x.x.x입니다.이 네트워크를 보호하기 위해 마지막 3개의 8진수(이 IP 주소의 숫자 집합)가 x로 교체되었습니다.전체 IP 주소를 입력합니다.



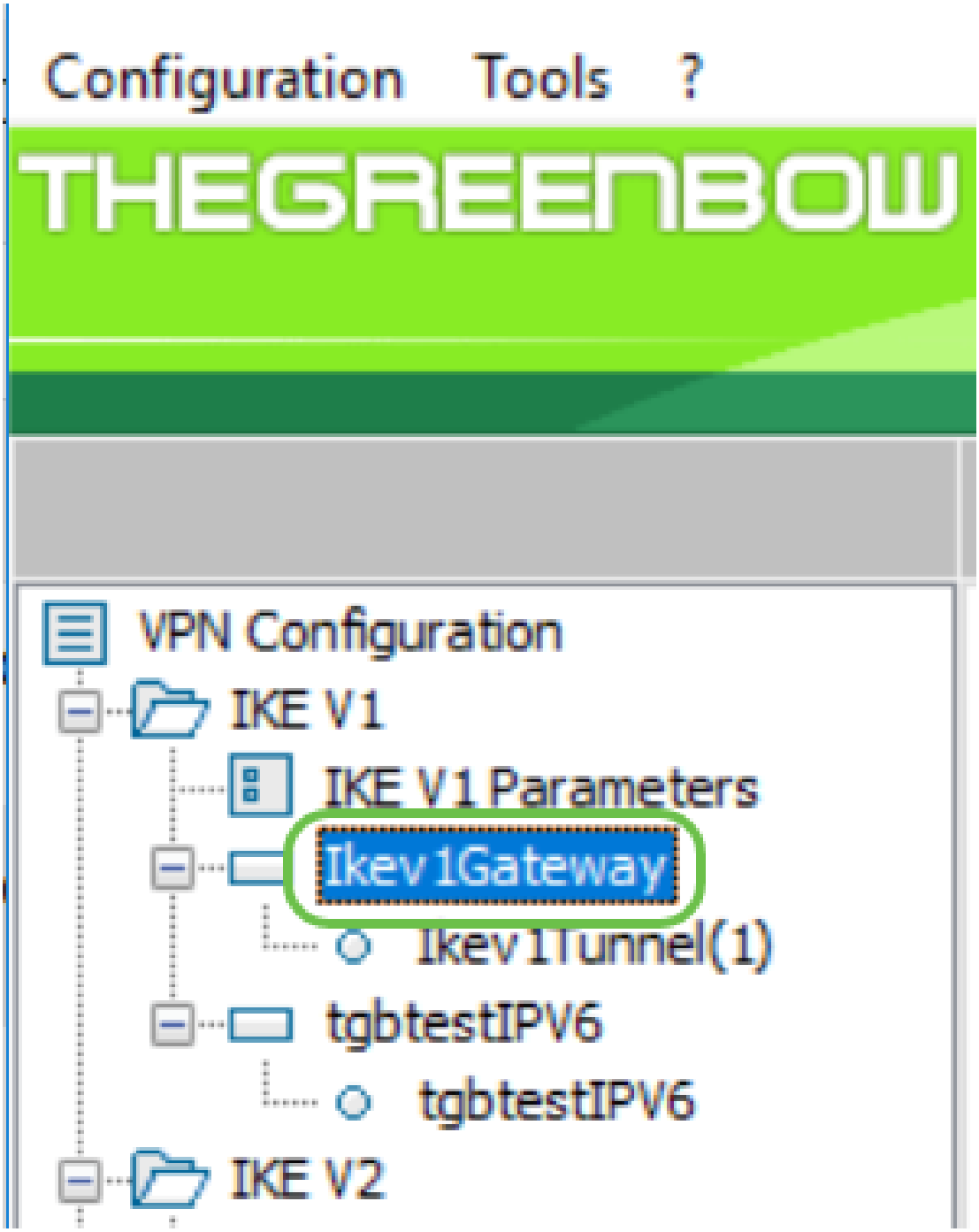
5단계. 완료를 **클릭합니다**.



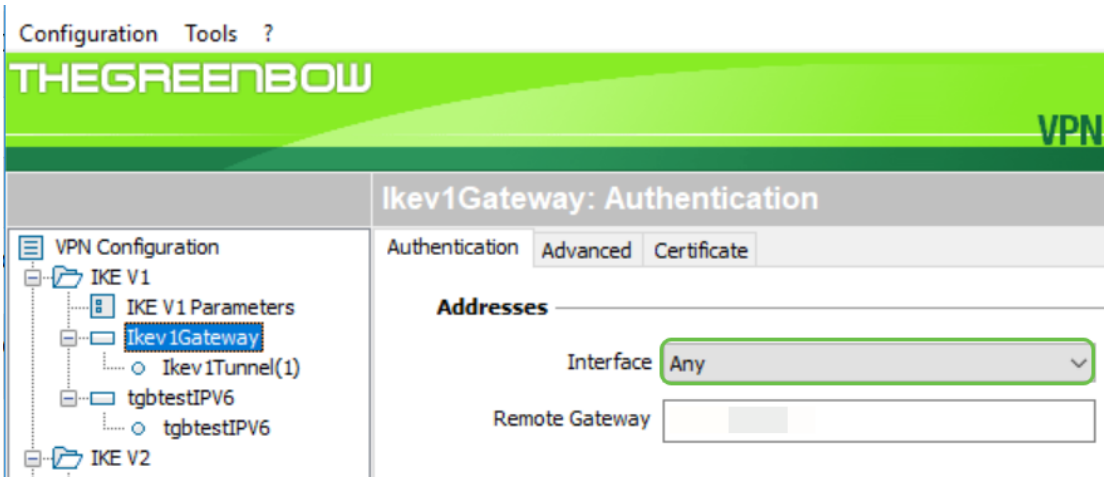
6단계(선택 사항) IKE V1 매개변수를 변경할 수 있습니다.GreenBow 기본값, Minimal 및 Maximal 수명을 조정할 수 있습니다.이 위치에서는 라우터가 허용하는 수명 범위를 입력할 수 있습니다.



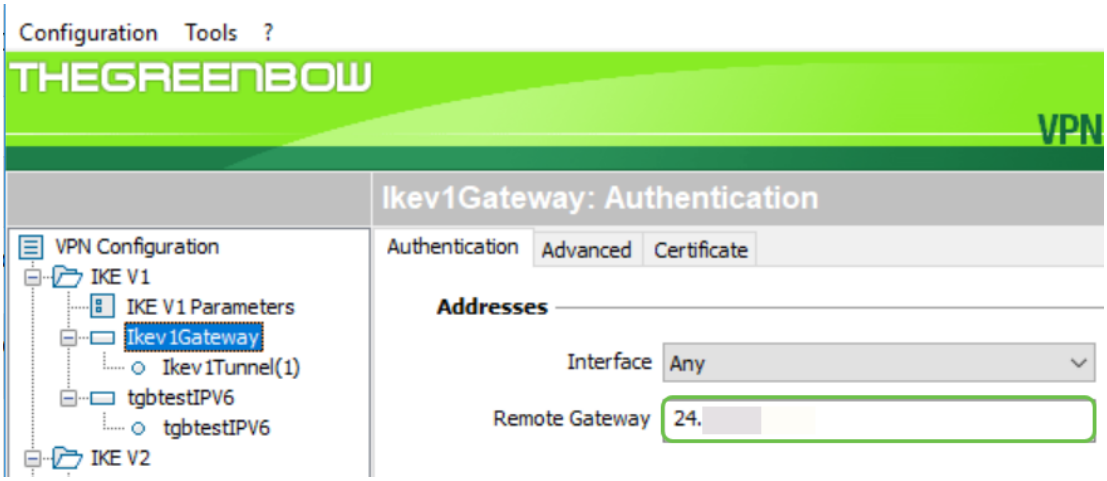
7단계. 생성한 게이트웨이를 클릭합니다.



8단계. Addresses(*주소*) 아래의 Authentication(*인증*) 탭에 로컬 주소의 드롭다운 목록이 표시됩니다.아래와 같이 하나 또는 **Any**를 선택할 수 있습니다.

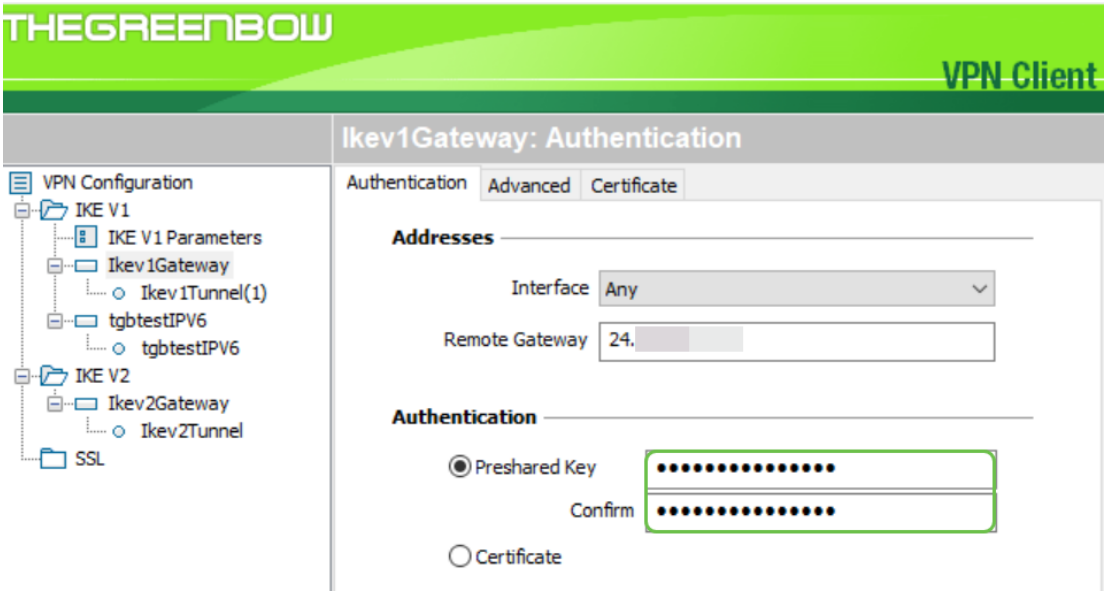


9단계. *Remote Gateway* 필드에 원격 게이트웨이의 주소를 입력합니다.IP 주소 또는 DNS 이름일 수 있습니다.사이트(사무실)에 있는 라우터의 공용 IP 주소 주소입니다.



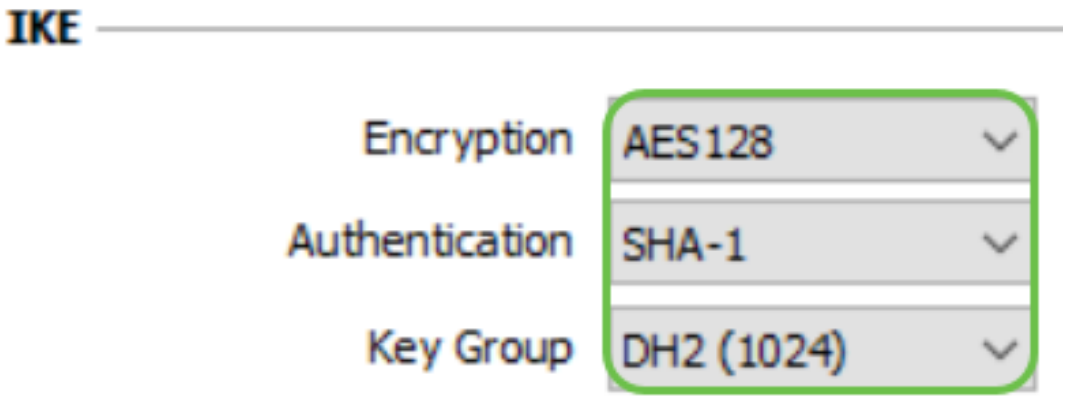
10단계. Authentication(*인증*)에서 인증 유형을 선택합니다.옵션은 다음과 같습니다.

- 사전 공유 키 — 이 옵션을 사용하면 사용자가 VPN 게이트웨이에 구성된 비밀번호를 사용할 수 있습니다.VPN 터널을 설정하려면 사용자가 비밀번호를 매칭해야 합니다.
- 인증서 — 이 옵션은 인증서를 사용하여 VPN 클라이언트와 VPN 게이트웨이 간의 핸드셰이크를 완료합니다.

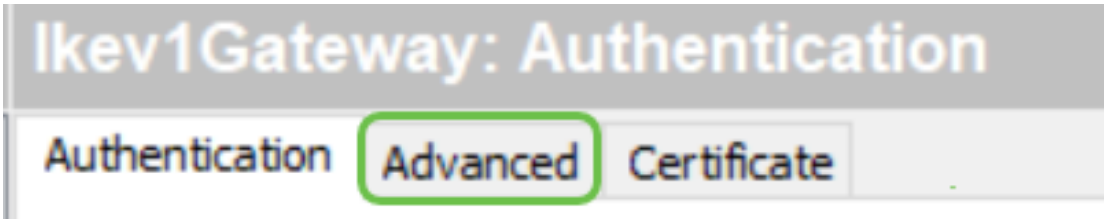


참고:이 예에서는 라우터에 구성된 사전 공유 키를 입력하고 확인했습니다.

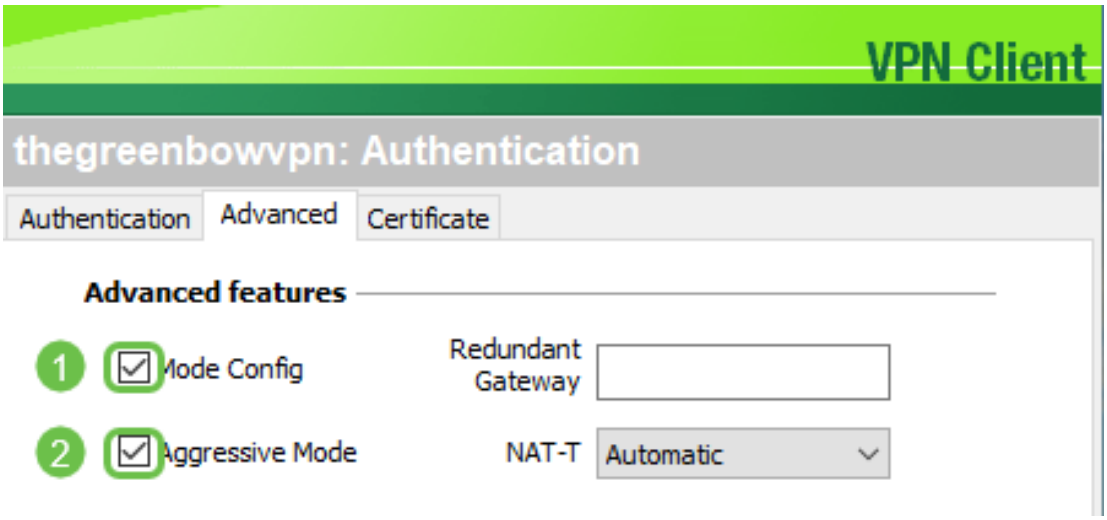
11단계. *IKE*에서 Encryption, Authentication 및 Key Group 설정을 라우터 컨피그레이션과 일치하도록 설정합니다.



12단계. **고급** 탭을 클릭합니다.

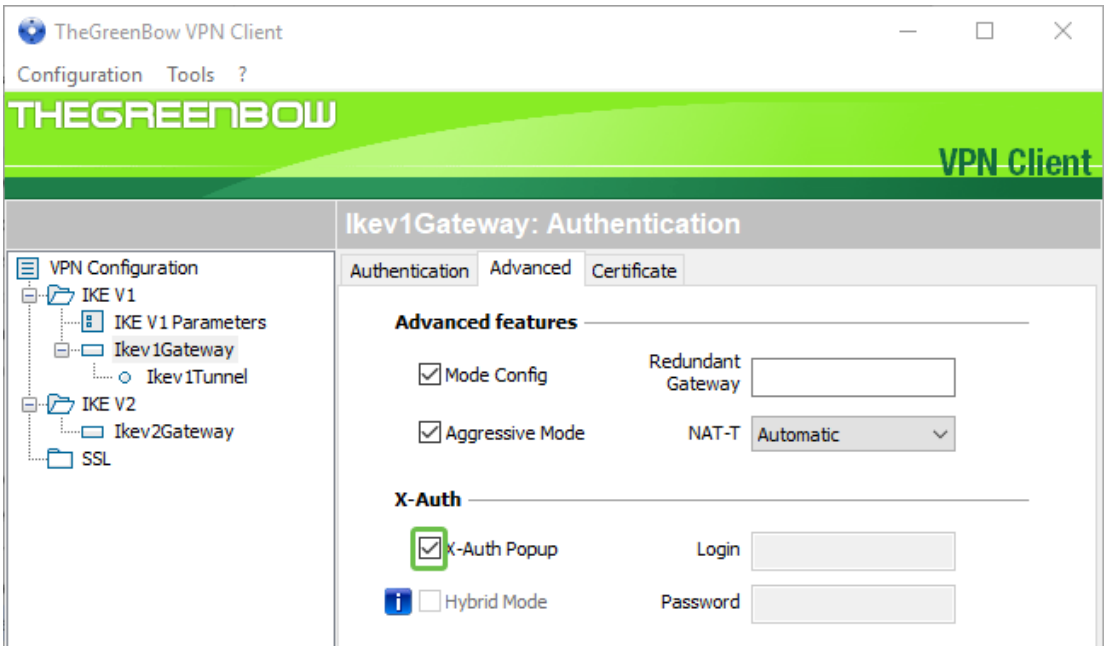


13단계. Advanced features(고급 기능)에서 **Mode Config(모드 컨피그레이션)** 및 Aggressive Mode(**적극적인 모드**) 확인란을 선택합니다.이 예제의 Client-to-Site 프로필에서 RV160에서 Aggressive Mode가 선택되었습니다.NAT-T 설정을 Automatic(자동)으로 유지합니다.

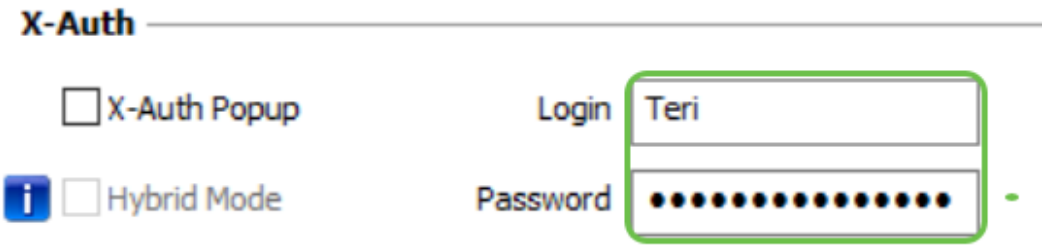


참고: Mode Config(모드 컨피그레이션)가 활성화된 경우 GreenBow VPN Client는 터널을 설정하기 위해 VPN 게이트웨이에서 설정을 가져옵니다.NAT-T를 사용하면 더 신속하게 연결을 설정할 수 있습니다.

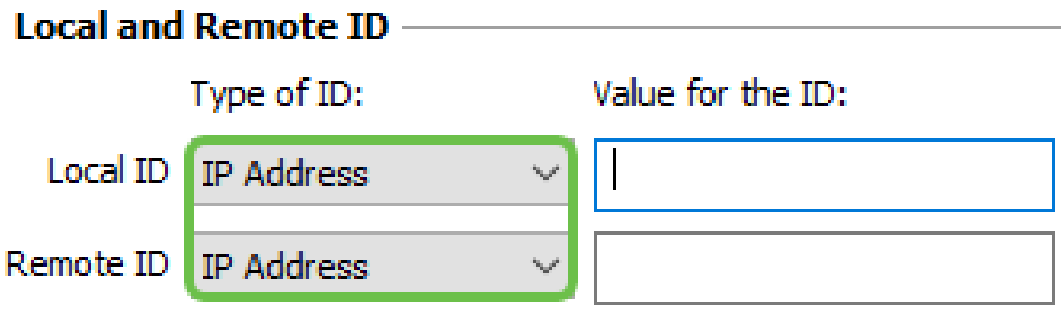
14단계(선택 사항) *X-Auth(X-Auth)*에서 연결 시작 시 로그인 창을 자동으로 당겨받기 위해 X-Auth Popup(**X-Auth Popup**) 확인란을 선택할 수 있습니다.로그인 창에서는 사용자가 터널을 완료할 수 있도록 자격 증명을 입력합니다.



15단계. (선택 사항) *X-Auth Popup*을 선택하지 않으면 Login 필드에 사용자 이름을 *입력합니다*.사용자 계정이 VPN 게이트웨이에 생성되었을 때 입력한 사용자 이름과 사이트의 비밀번호입니다.

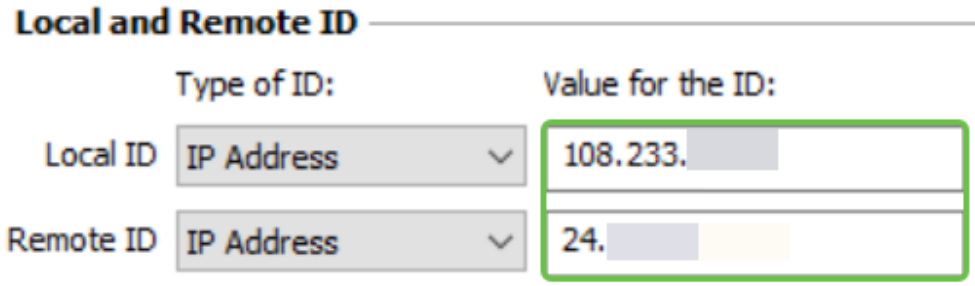


16단계. Local *and Remote ID(로컬 및 원격 ID)*에서 Local ID(로컬 ID) 및 Remote ID를 VPN 게이트웨이의 설정과 일치하도록 설정합니다.



참고:이 예에서는 RV160 또는 RV260 VPN 게이트웨이의 설정과 일치하도록 로컬 ID와 원격 ID를 모두 IP 주소로 설정합니다.

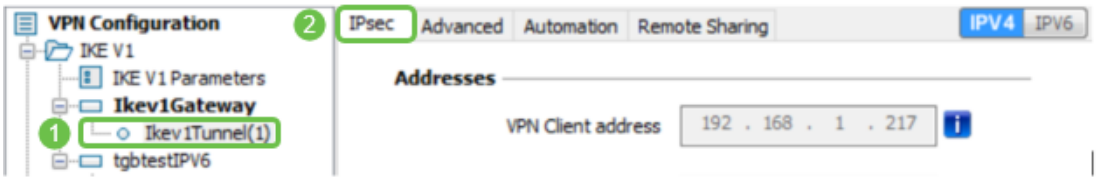
17단계. *ID의 값*에서 각 필드에 로컬 ID와 원격 ID를 입력합니다.로컬 ID는 클라이언트의 WAN IP 주소입니다.웹 검색을 통해 "What's my IP"를 찾을 수 있습니다.원격 ID는 사이트에 있는 라우터의 WAN IP 주소입니다.



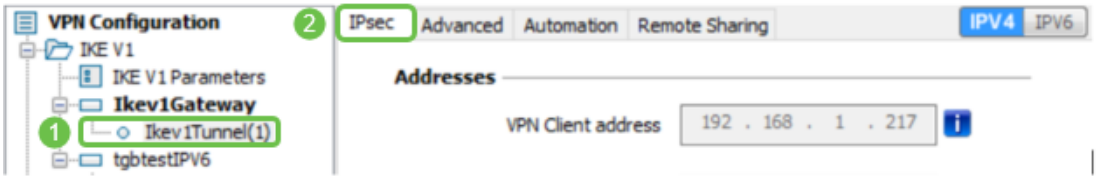
18단계. Configuration(컨피그레이션)을 **클릭하고 Save(저장)를 선택합니다**.

터널 설정 구성

1단계. IKev**1Tunnel(1)**(사용자 이름은 다를 수 있음) 및 IPsec **탭을** 클릭합니다.Ikev1Gateway 고급 설정에서 Mode Config를 선택한 경우 VPN 클라이언트 주소가 자동으로 채워집니다.원격 위치에 있는 컴퓨터/랩톱의 로컬 IP 주소가 표시됩니다.

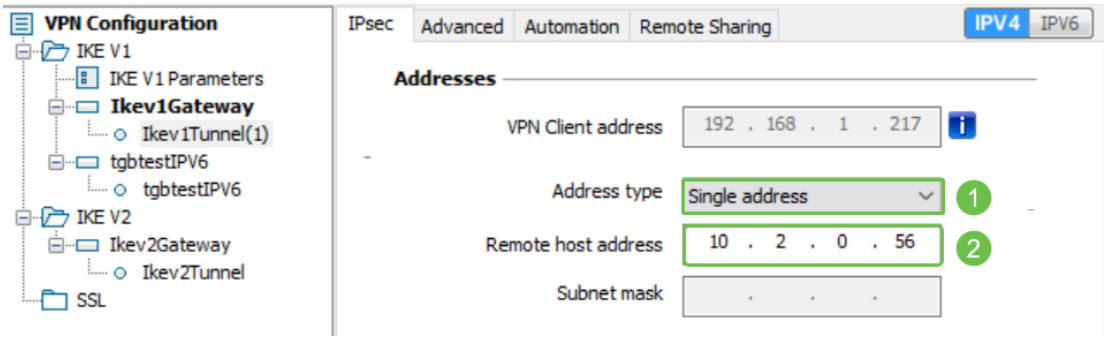


2단계. VPN 클라이언트가 Address *type* 드롭다운 목록에서 액세스할 수 있는 주소 유형을 선택합니다.단일 주소, 주소 범위 또는 서브넷 주소일 수 있습니다.기본값인 서브넷 주소는 VPN 클라이언트 주소(컴퓨터의 로컬 IP 주소), 원격 LAN 주소 및 서브넷 마스크를 자동으로 포함합니다.단일 주소 또는 주소 범위를 선택한 경우 이러한 필드를 수동으로 채워야 합니다.VPN 터널에서 액세스해야 하는 네트워크 주소를 *Remote LAN address* 필드에 입력하고 원격 네트워크의 서브넷 마스크를 *Subnet mask* 필드에 입력합니다.

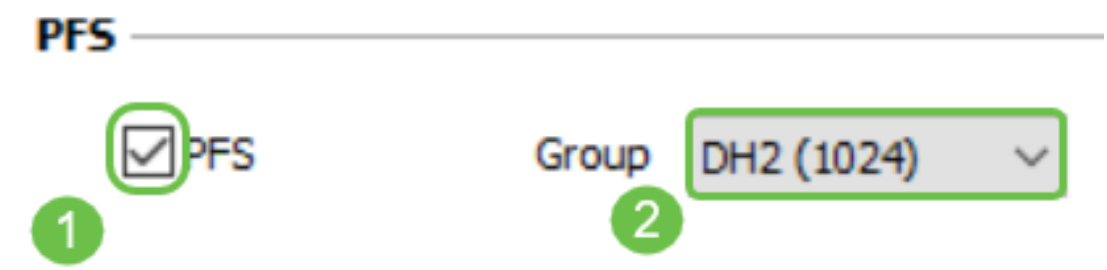


참고:이 예에서는 Single address(단일 주소)가 선택되었으며 사이트에 있는 라우터의 로컬 IP 주소가 입력됩니다.

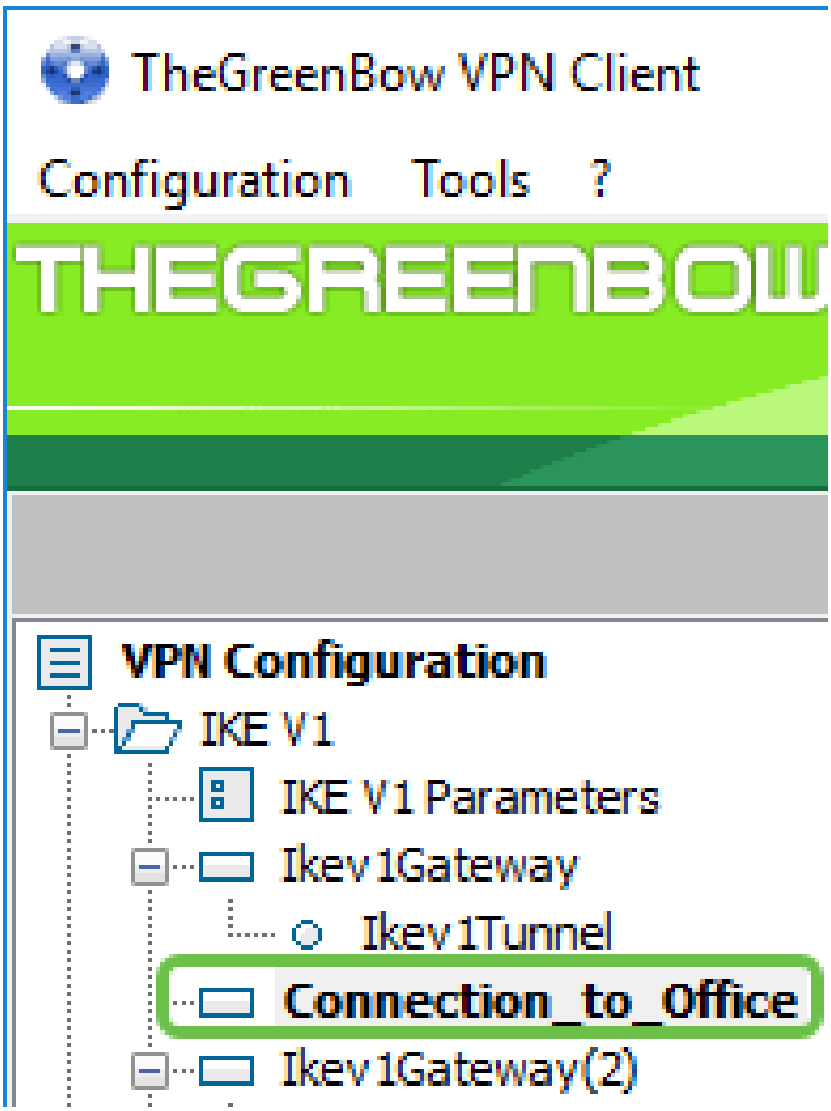
3단계. *ESP*에서 사이트(사무실)의 VPN 게이트웨이 설정과 일치하도록 암호화, 인증 및 모드를 설정합니다.



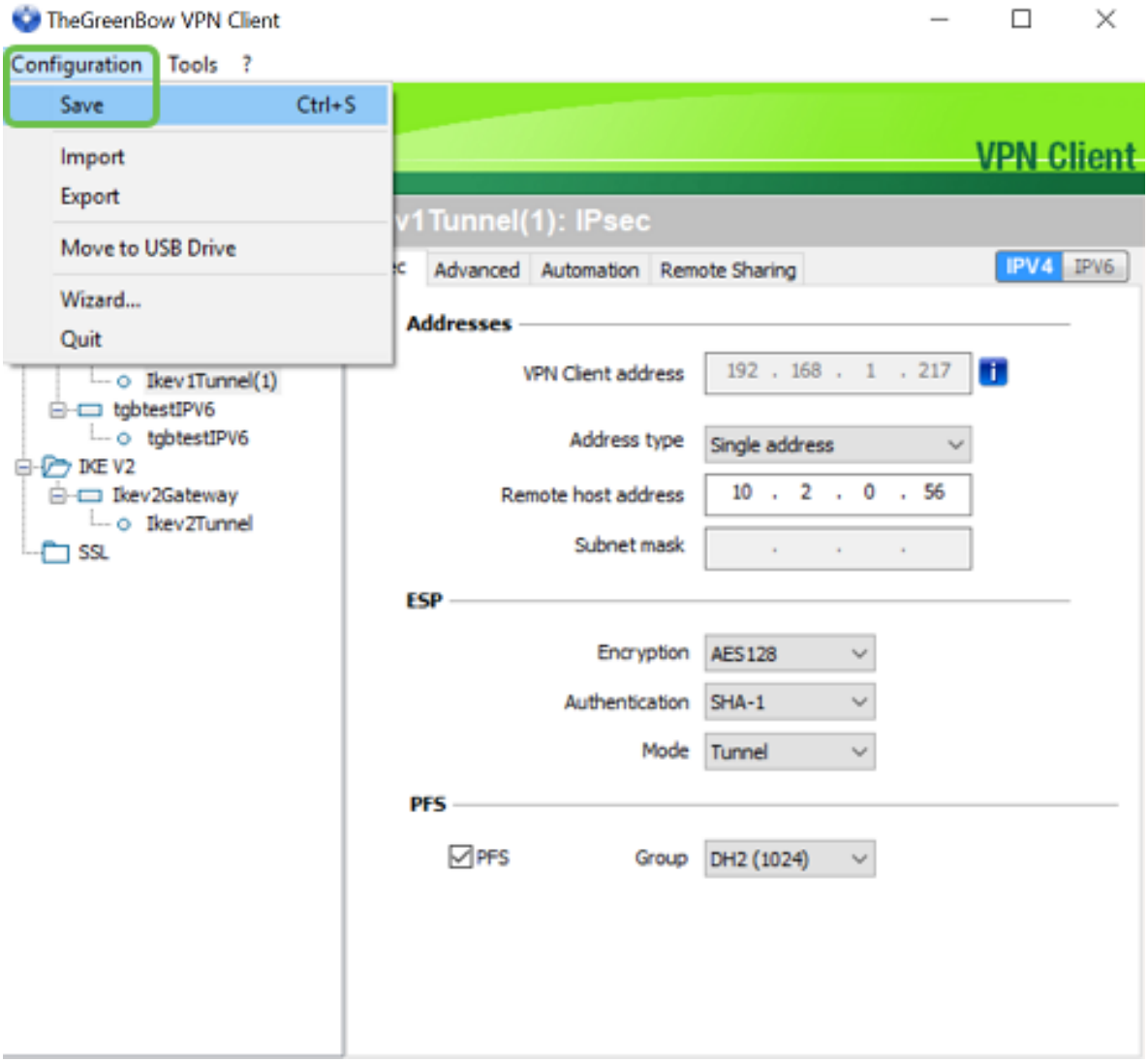
4단계. (선택 사항) PFS*에서* PFS(Perfect Forward Secrecy)를 활성화하려면 **PFS** 확인란을 선택합니다.PFS는 세션을 암호화하기 위해 임의의 키를 생성합니다.*Group* 드롭다운 목록에서 PFS 그룹 설정을 선택합니다.라우터에서 활성화한 경우 여기에서 활성화해야 합니다.



5단계. (선택 사항) Ikev1Gateway의 이름을 마우스 오른쪽 버튼으로 클릭하고 이름을 변경하려면 rename 섹션을 클릭합니다.



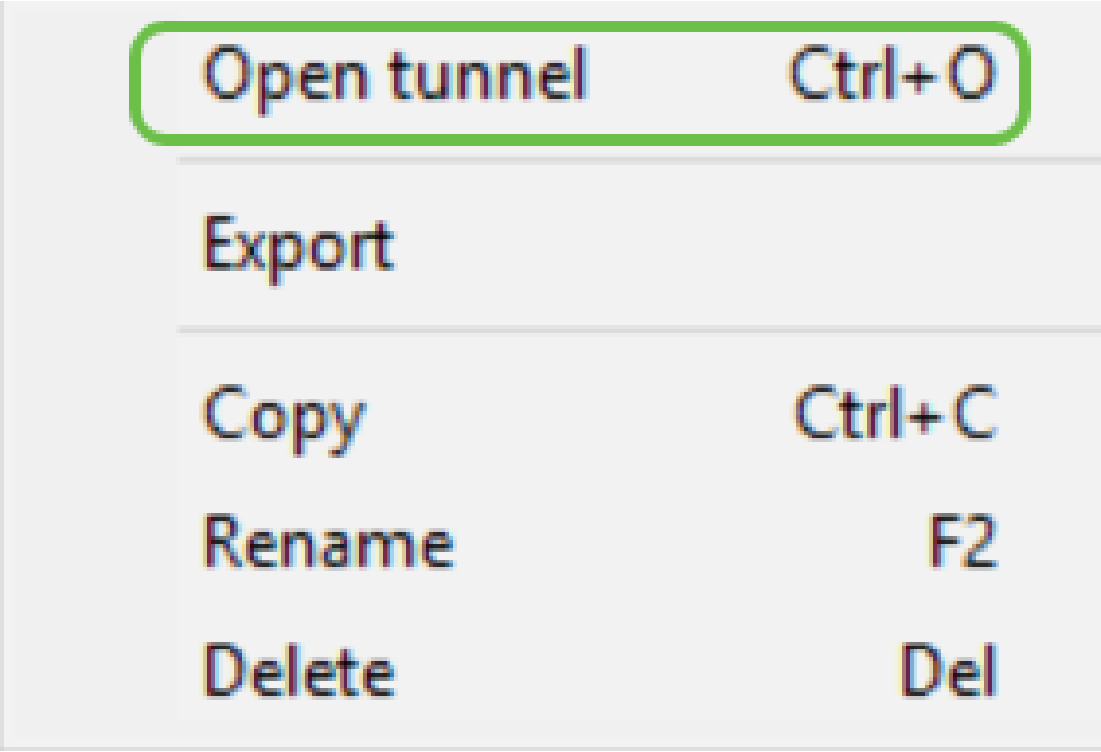
6단계. Configuration(컨피그레이션)을 **클릭하고 Save(저장)를 선택합니다.**



이제 VPN을 통해 RV160 또는 RV260 라우터에 연결하도록 TheGreenBow VPN Client를 성공적으로 구성해야 합니다.

클라이언트로 VPN 연결 시작

1단계. GreenBow가 열려 있으므로 터널을 마우스 오른쪽 단추로 클릭하고 **터널 열기**를 선택하여 **연결을 시작할** 수 있습니다.

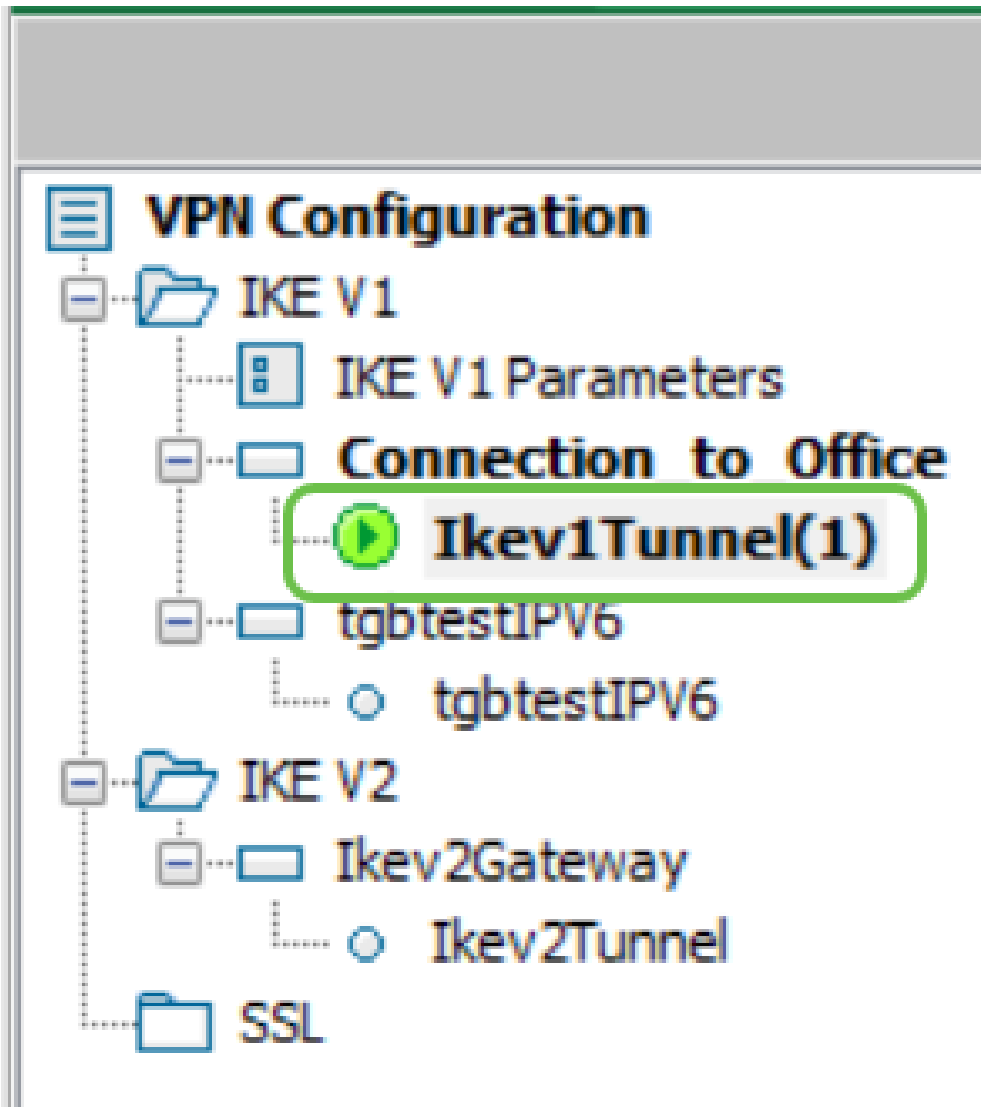


참고:터널을 두 번 클릭하여 터널을 열 수도 있습니다.

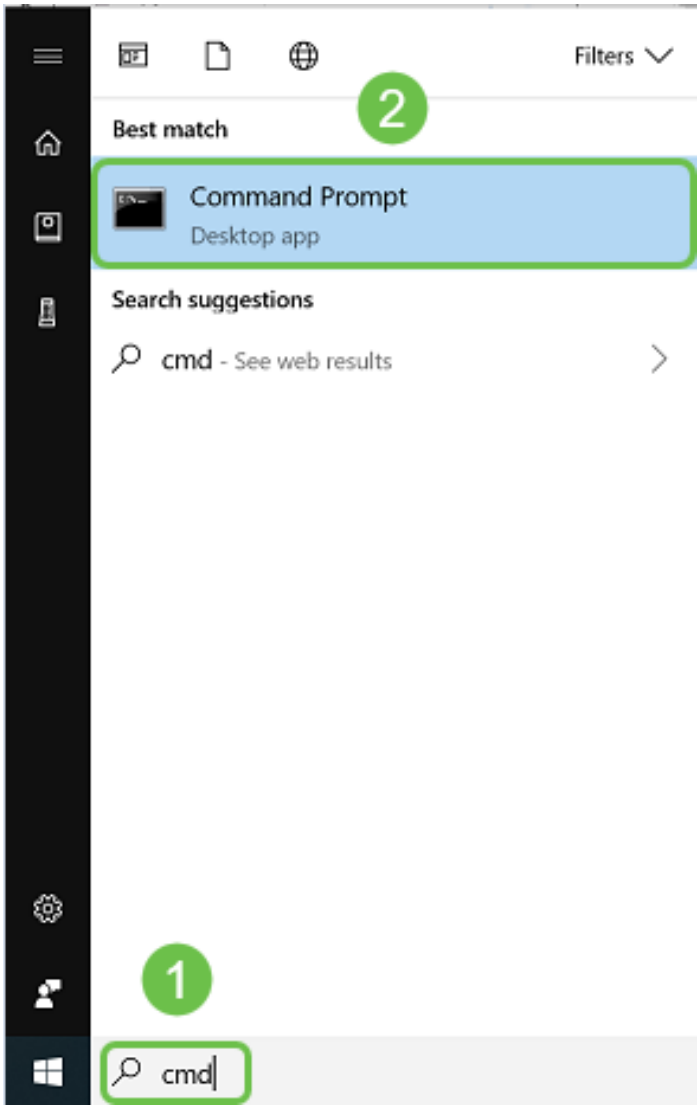
2단계. (선택 사항) 새 세션을 시작하고 GreenBow를 닫은 경우 화면 오른쪽**에서 TheGreenBow VPN Client** 아이콘**을** 클릭합니다.

3단계. (선택 사항) 이 단계는 새 세션을 설정하고 2단계를 수행한 경우에만 필요합니다. 사용해야 하는 VPN 연결을 선택한 다음 **OPEN**을 클릭합니다.VPN 연결이 자동으로 시작됩니다.

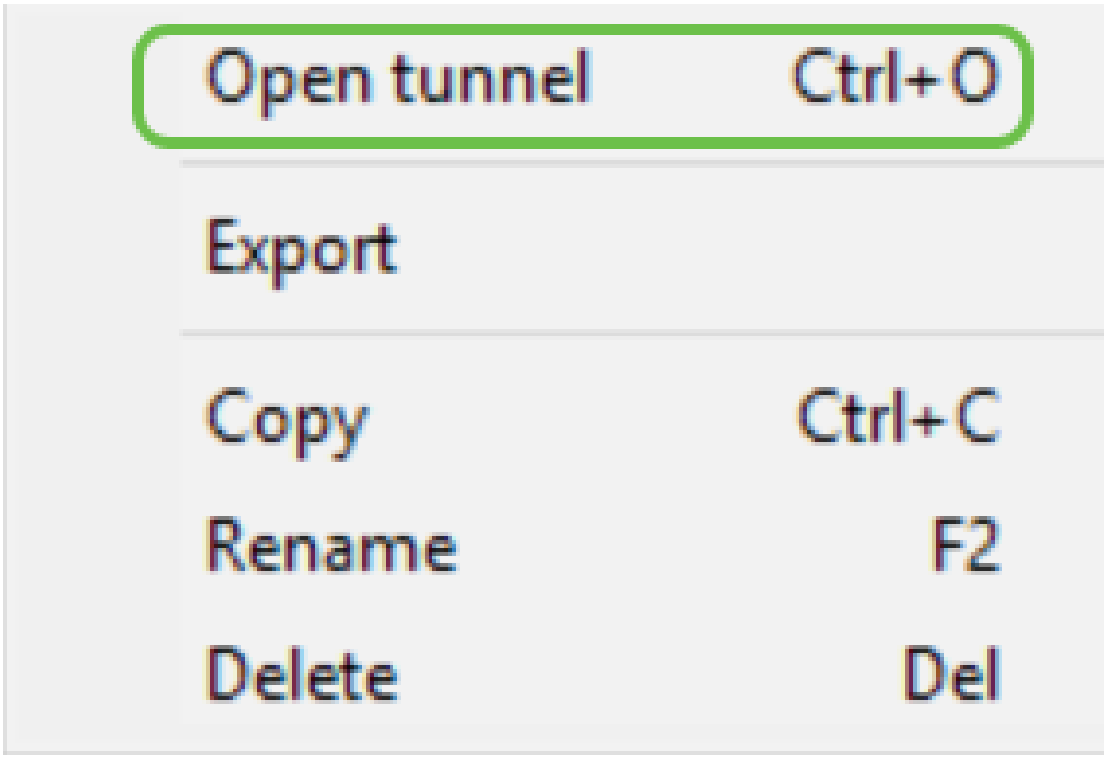
4단계. 터널이 연결되면 터널 옆에 녹색 원이 나타납니다.느낌표가 표시되면 이를 클릭하여 오류를 찾을 수 있습니다.



5단계. (선택 사항) 연결되어 있는지 확인하려면 클라이언트 컴퓨터에서 명령 프롬프트에 액세스합니다.



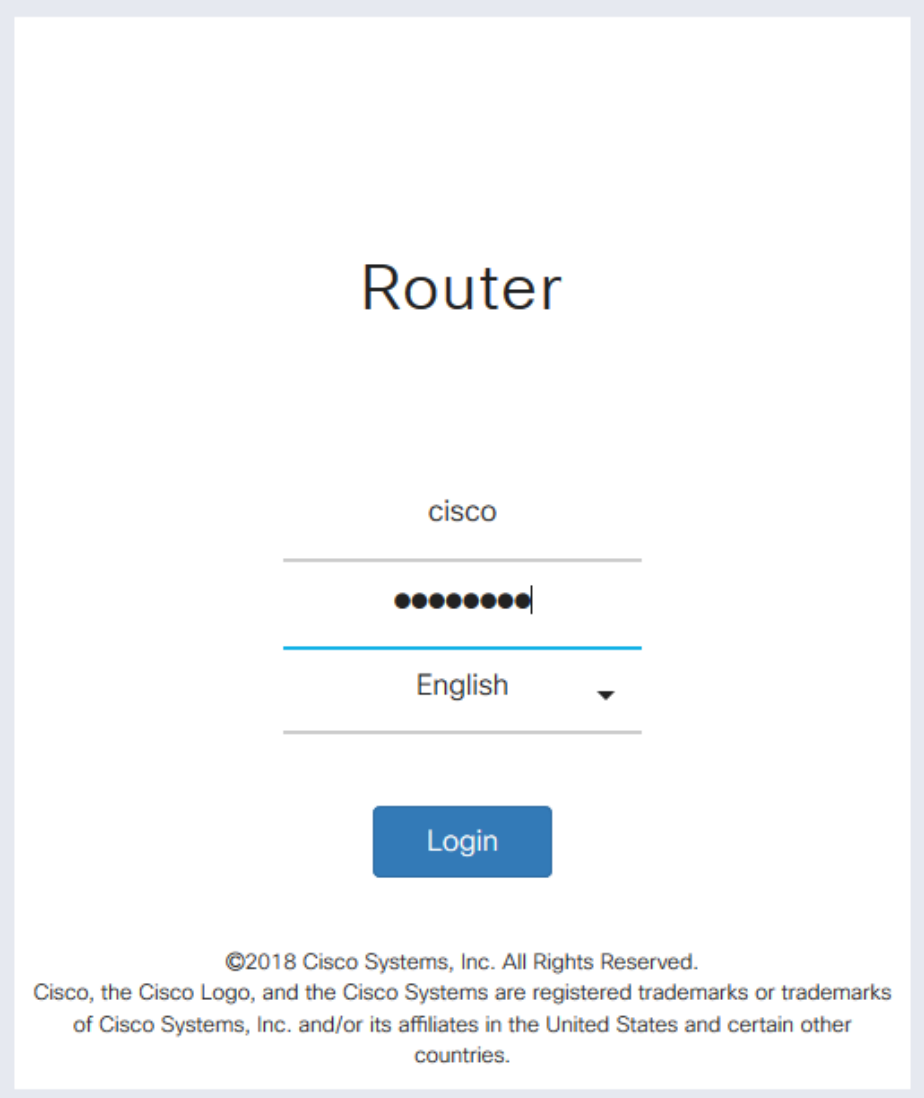
6단계. (선택 사항) ping을 입력한 다음 사이트에 있는 라우터의 전용 LAN IP 주소를 입력합니다.회신을 받으면 연결된 것입니다.



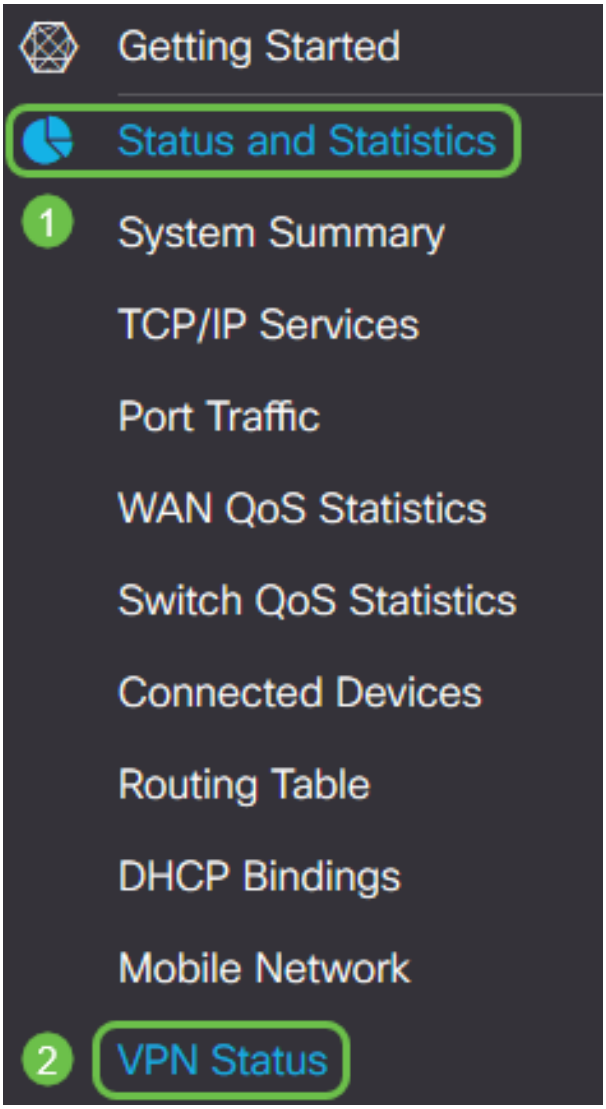
VPN 상태 확인

사이트에서 VPN 상태 확인

1단계. RV160 또는 RV260의 VPN 게이트웨이의 웹 기반 유틸리티에 로그인합니다.



2단계. Status **and Statistics(상태 및 통계) > VPN Status(VPN 상태)를** 선택합니다.

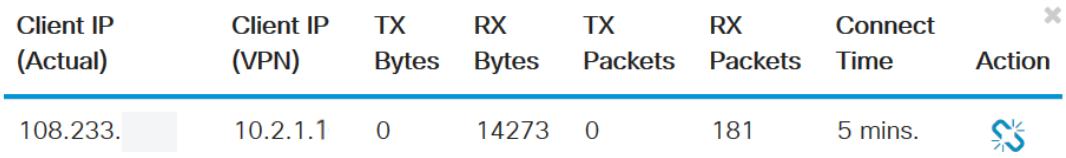


3단계. *Client-to-Site Tunnel Status(클라이언트-사이트 터널 상태)*에서 Connection Table(*연결 테이블*)의 *Connections(연결)* 열을 *선택합니다*.VPN 연결이 확인되었음을 확인해야 합니다.

4단계. **눈** 아이콘을 클릭하여 자세한 내용을 확인합니다.

5단계. Client-to-Site VPN Status(클라이언트-사이트 VPN 상태)의 세부 정보가 여기에 표시됩니다.설정 시 구성된 주소 풀에서 할당된 클라이언트의 WAN IP 주소, 로컬 IP 주소를 확인할 수 있습니다.또한 전송 및 수신된 바이트, 패킷 및 연결 시간도 표시합니다.클라이언트 연결을 끊으려면

Action(작업) 아래에서 파란색 **끊어진 체인** 아이콘을 클릭합니다.검사 후 닫으려면 오른쪽 상단 모서리에 있는 x를 클릭합니다.



Client IP (Actual)	Client IP (VPN)	TX Bytes	RX Bytes	TX Packets	RX Packets	Connect Time	Action
108.233.	10.2.1.1	0	14273	0	181	5 mins.	

결론

이제 RV160 또는 RV260 라우터에서 VPN 연결을 성공적으로 설정 및 확인하고 GreenBow VPN Client가 VPN을 통해 라우터에 연결되도록 구성되어야 합니다.