GreenBow VPN 클라이언트를 사용하여 RV34x Series 라우터와 연결

특별 공지:라이센싱 구조 - 펌웨어 버전 1.0.3.15 이상앞으로 AnyConnect는 클라이언트 라이센스에만 요금이 부과됩니다.

RV340 Series 라우터의 AnyConnect 라이센스에 대한 자세한 내용은 RV340 Series 라우터용 AnyConnect 라이센싱 문서를 참조하십시오.

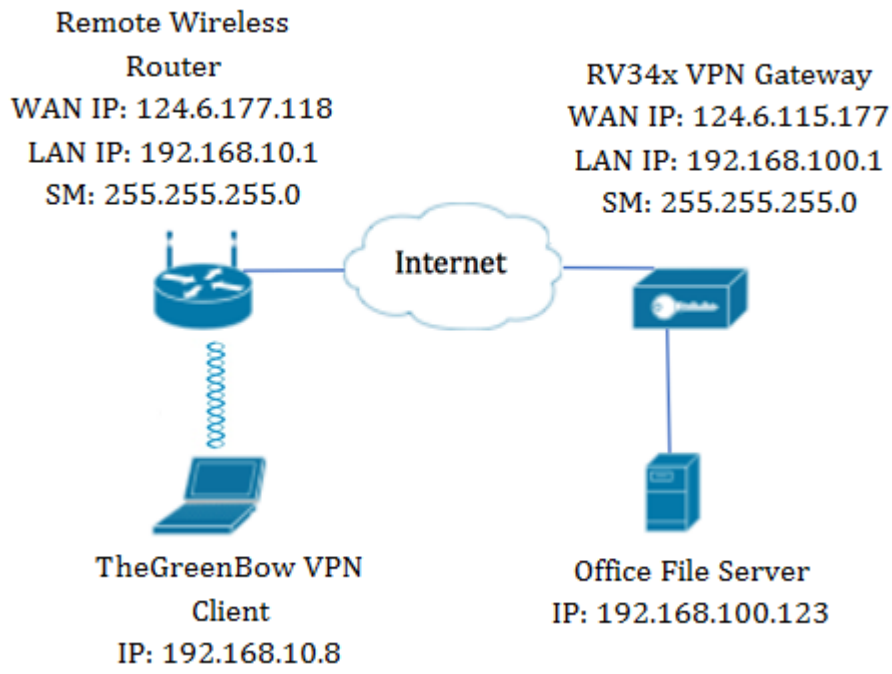
소개

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 주로 사용합니다.

VPN을 사용하면 원격 호스트가 동일한 로컬 네트워크에 있는 것처럼 작동할 수 있습니다.라우터는 최대 50개의 터널을 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.

GreenBow VPN Client는 RV34x Series Router를 사용하여 호스트 디바이스에서 사이트 간 IPSec 터널에 대한 보안 연결을 구성할 수 있도록 하는 타사 VPN 클라이언트 애플리케이션입니다.



다이어그램에서 컴퓨터는 네트워크 외부의 사무실에 있는 파일 서버에 연결하여 해당 리소스에 액세스합니다.이를 위해 컴퓨터의 GreenBow VPN 클라이언트는 RV34x VPN 게이트웨이에서 설정을 가져올 수 있도록 구성됩니다.

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 쉽게 확장 가능하므로 네트워크에 새 사용자 또는 사용자 그룹을 쉽게 추가할 수 있습니다.추가 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, 사설 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 중단 없이 보장하려면 검증되고 테스트된 평판을 가진 공급자를 보유하는 것이 중요합니다.
3. 확장성.새로운 인프라 또는 새로운 구성 집합을 추가해야 하는 상황이 발생할 경우, 특히 이미 사용 중인 제품 또는 공급업체가 아닌 다른 제품과 관련된 경우 비호환성으로 인해 기술 문제가 발생할 수 있습니다.
4. 모바일 장치의 보안 문제.모바일 디바이스에서 VPN 연결을 시작할 때 특히 모바일 디바이스가 로컬 네트워크에 무선으로 연결되어 있을 때 보안 문제가 발생할 수 있습니다.
5. 느린 연결 속도.무료 VPN 서비스를 제공하는 VPN 클라이언트를 사용 중인 경우 이러한 공급자가 연결 속도의 우선 순위를 지정하지 않으므로 연결 속도가 느려질 수 있습니다.

GreenBow VPN 클라이언트 사용 전제 조건

다음 항목은 먼저 VPN 라우터에서 구성해야 하며 여기를 클릭하여 연결을 설정하여 GreenBow VPN 클라이언트에 적용됩니다.

1. VPN 게이트웨이에 클라이언트-사이트 프로파일 생성
2. VPN 게이트웨이에 사용자 그룹 생성
3. VPN 게이트웨이에서 사용자 계정 생성
4. VPN 게이트웨이에 IPSec 프로파일 생성
5. VPN 게이트웨이에서 단계 I 및 단계 II 설정 구성

적용 가능한 디바이스

- RV34x 시리즈

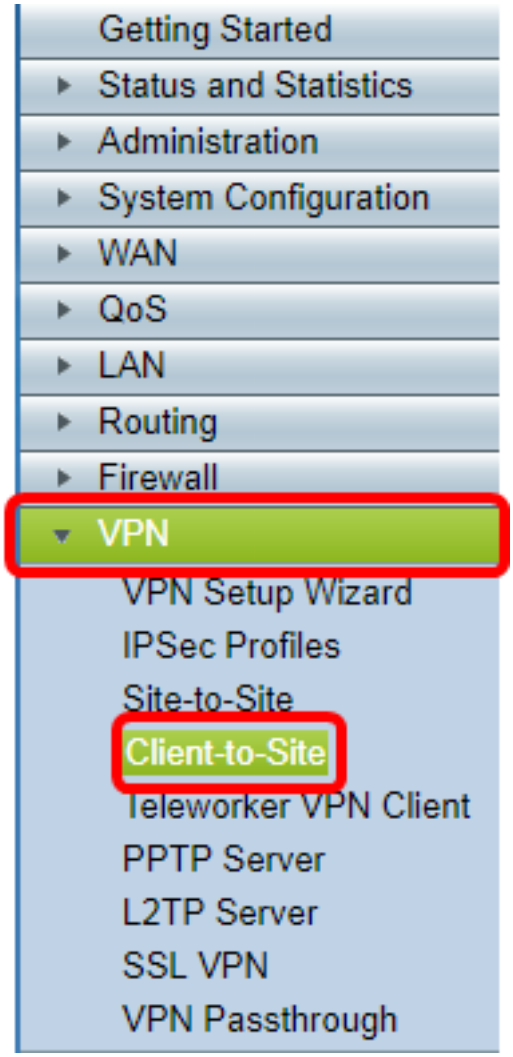
소프트웨어 버전

- 1.0.01.17

GreenBow VPN 클라이언트 사용

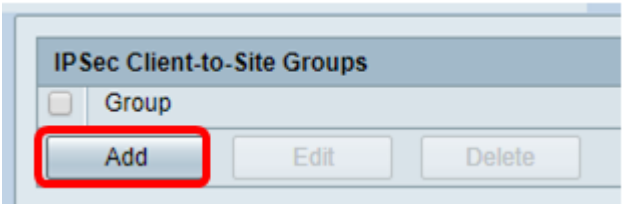
라우터에 클라이언트-사이트 프로파일 생성

1단계. RV34x 라우터의 웹 기반 유틸리티에 로그인하고 **VPN > Client-to-Site**를 선택합니다.



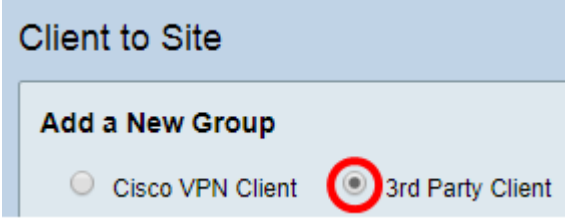
참고:이 문서의 이미지는 RV340 라우터에서 가져온 것입니다.옵션은 디바이스의 모델에 따라 달라질 수 있습니다.

2단계. **추가**를 클릭합니다.



3단계. **서드파티 클라이언트를 클릭합니다**.

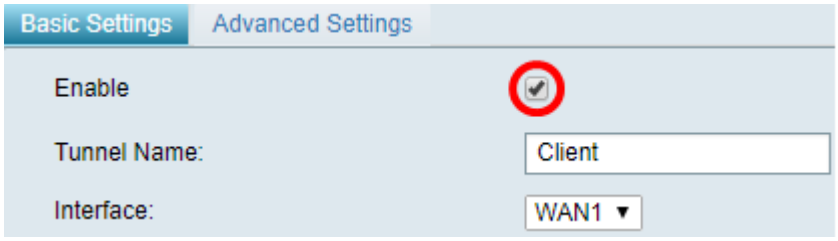
참고: AnyConnect는 Cisco VPN 클라이언트의 예이며 GreenBow VPN 클라이언트는 서드파티 VPN 클라이언트의 예입니다.



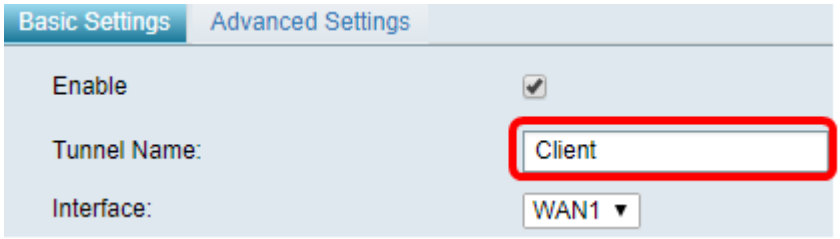
참고:이 예에서는 서드파티 클라이언트가 선택됩니다.

4단계. Basic Settings(기본 설정) 탭에서 **Enable(활성화)** 확인란을 선택하여 VPN 프로파일이

활성화되어 있는지 확인합니다.

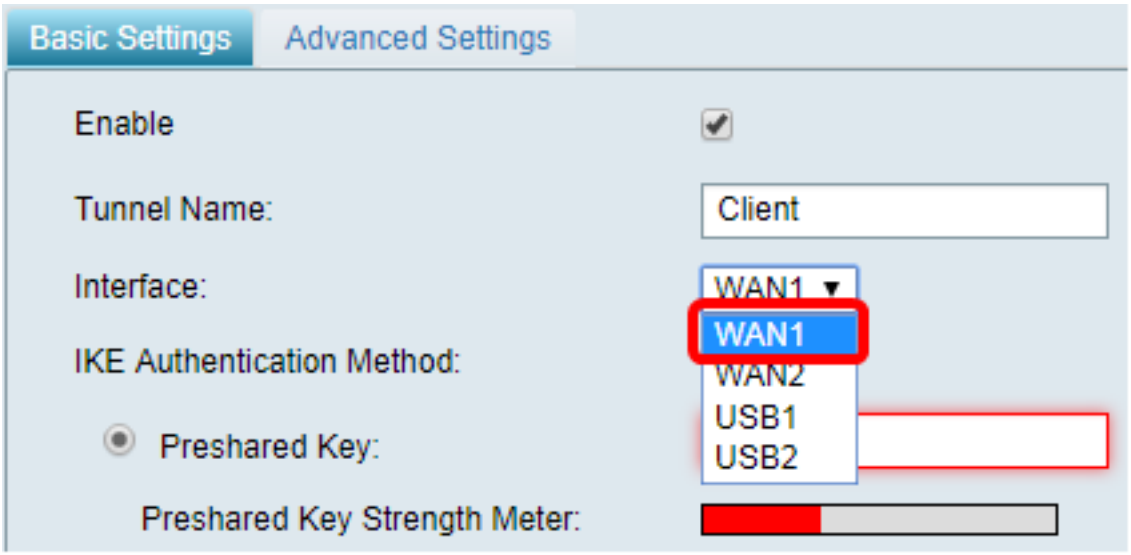


5단계. Tunnel Name(*터널 이름*) 필드에 VPN 연결의 이름을 입력합니다.



참고:이 예에서는 **클라이언트**가 입력됩니다.

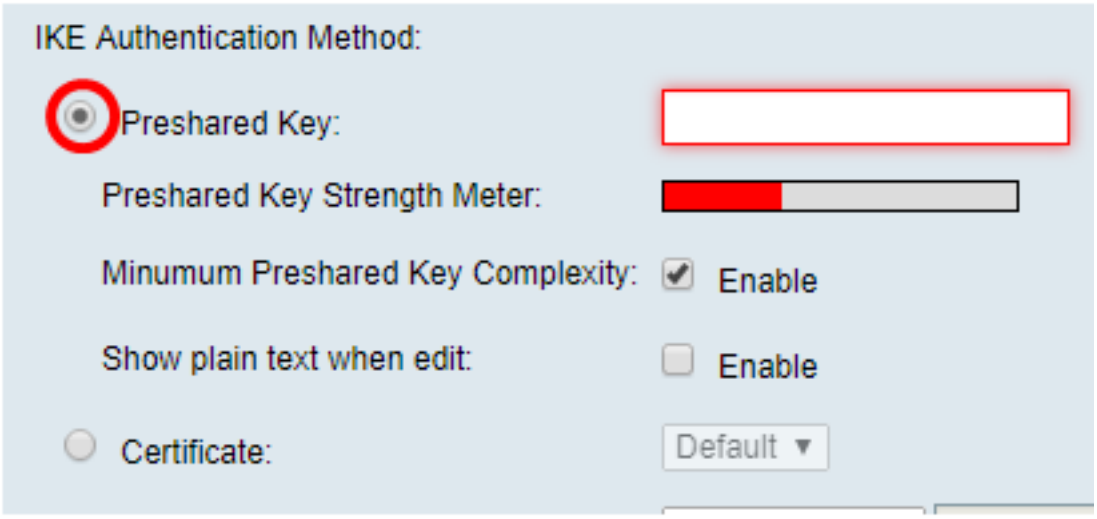
6단계. Interface 드롭다운 목록에서 사용할 인터페이스를 선택합니다.옵션은 VPN 연결을 위해 라우터의 해당 인터페이스를 사용할 WAN1, WAN2, USB1 및 USB2입니다.



참고:옵션은 사용 중인 라우터 모델에 따라 달라집니다.이 예에서는 WAN1이 선택됩니다.

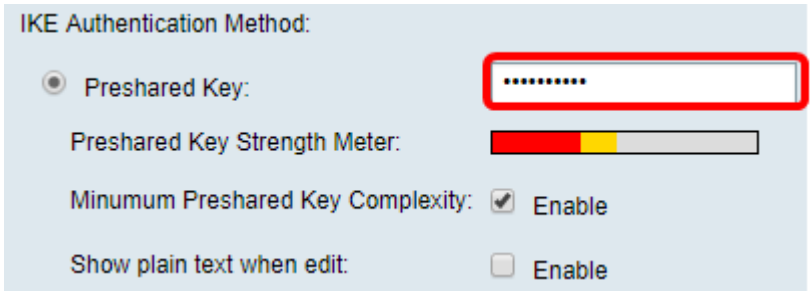
7단계. IKE 인증 방법을 선택합니다.옵션은 다음과 같습니다.

- 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.

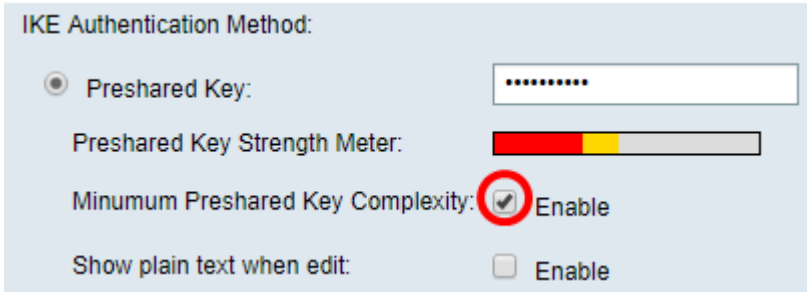


참고:이 예에서는 사전 공유 키가 선택됩니다.

8단계. Preshared *Key* 필드에 연결 비밀번호를 입력합니다.

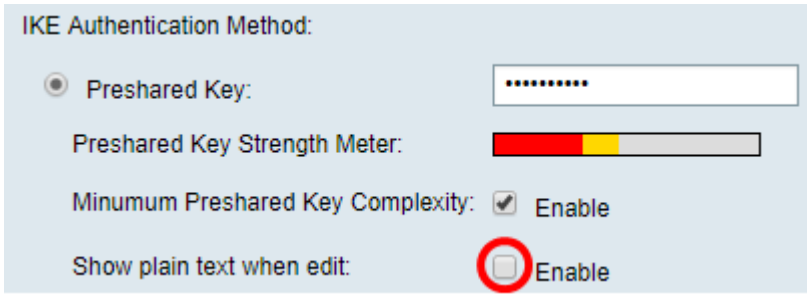


9단계. (선택 사항) 단순 비밀번호를 사용할 수 있도록 Minimum Preshared Key Complexity **Enable** 확인란을 선택 취소합니다.



참고:이 예에서는 최소 사전 공유 키 복잡성이 활성화되어 있습니다.

10단계. (선택 사항) Show plain text when edit **Enable** 확인란을 선택하여 비밀번호를 일반 텍스트로 표시합니다.

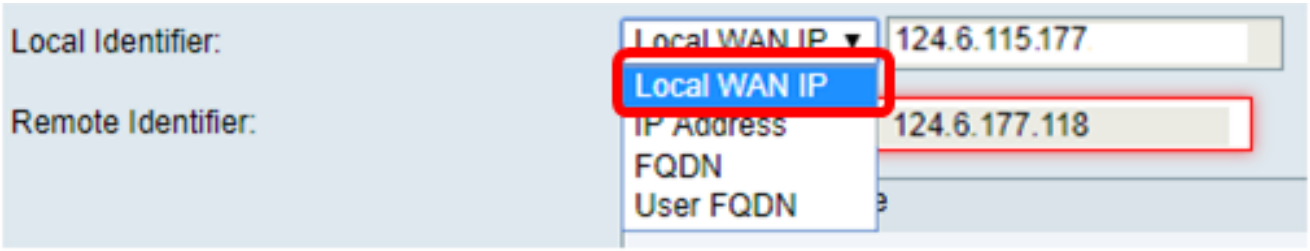


참고:이 예에서는 편집이 비활성화된 상태에서 일반 텍스트 표시를 합니다.

11단계. Local Identifier(로컬 식별자) 드롭다운 목록에서 로컬 식별자를 선택합니다.옵션은 다

음과 같습니다.

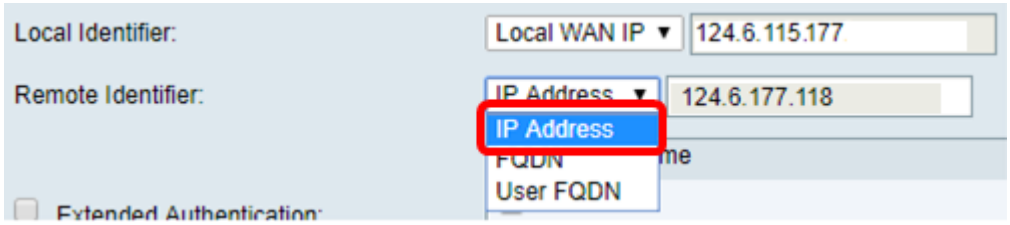
- 로컬 WAN IP — 이 옵션은 VPN 게이트웨이의 WAN(Wide Area Network) 인터페이스의 IP 주소를 사용합니다.
- IP Address — 이 옵션을 사용하면 VPN 연결에 대한 IP 주소를 수동으로 입력할 수 있습니다.
- FQDN — 이 옵션은 FQDN(Fully Qualified Domain Name)이라고도 합니다. 이 기능을 사용하면 인터넷의 특정 컴퓨터에 전체 도메인 이름을 사용할 수 있습니다.
- 사용자 FQDN — 이 옵션을 사용하면 인터넷의 특정 사용자에 대해 전체 도메인 이름을 사용할 수 있습니다.



참고:이 예에서는 Local WAN IP가 선택됩니다.이 옵션을 사용하면 로컬 WAN IP가 자동으로 탐지됩니다.

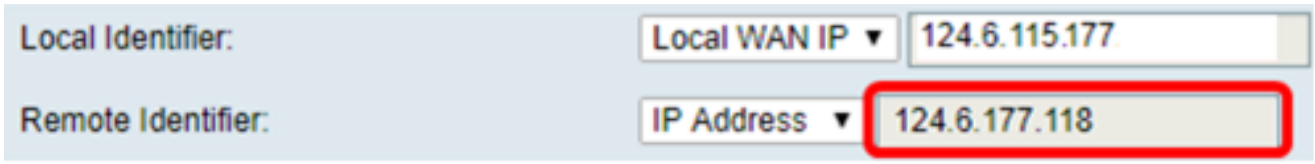
12단계(선택 사항) 원격 호스트의 식별자를 선택합니다.옵션은 다음과 같습니다.

- IP Address — 이 옵션은 VPN 클라이언트의 WAN IP 주소를 사용합니다.
- FQDN — 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.



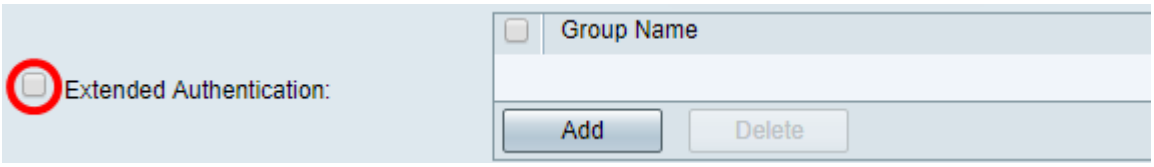
참고:이 예에서는 IP 주소가 선택됩니다.

13단계. Remote Identifier(*원격 식별자)* 필드에 원격 식별자*를* 입력합니다.



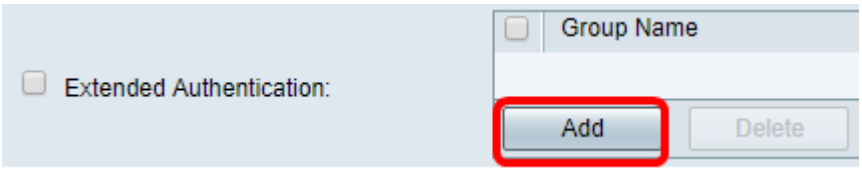
참고:이 예에서는 124.6.115.177을 입력합니다.

14단계. (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.

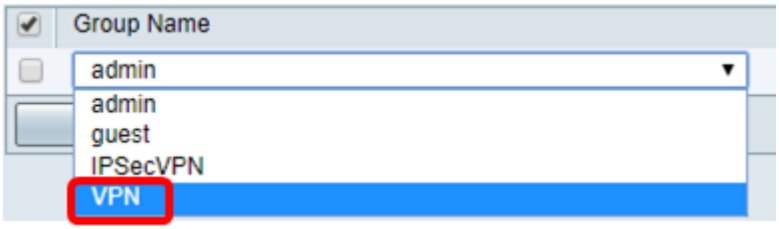


참고:이 예에서는 Extended Authentication(확장 인증)이 선택 취소되어 있습니다.

15단계. Group Name(그룹 이름)에서 Add(**추가**)를 클릭합니다.

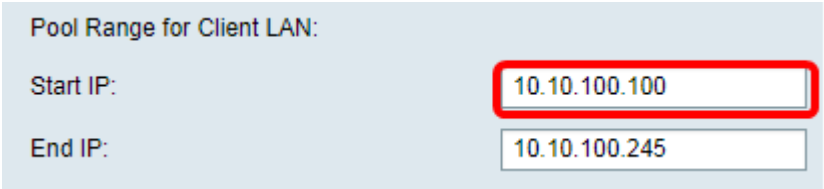


16단계. 그룹 이름 드롭다운 목록에서 확장 인증을 사용할 그룹을 선택합니다.



참고:이 예에서는 VPN이 선택됩니다.

17단계. Pool Range for Client LAN(클라이언트 LAN의 풀 범위)에서 *Start IP* 필드에 VPN 클라이언트에 할당할 수 있는 첫 번째 IP 주소를 입력합니다.

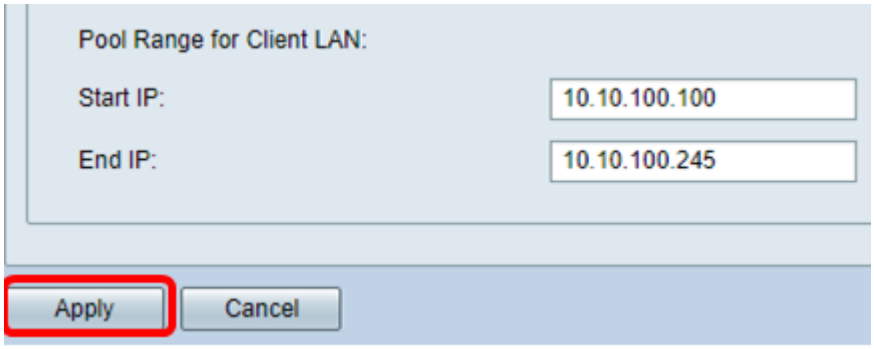


참고:이 예에서는 10.10.100.100을 입력합니다.

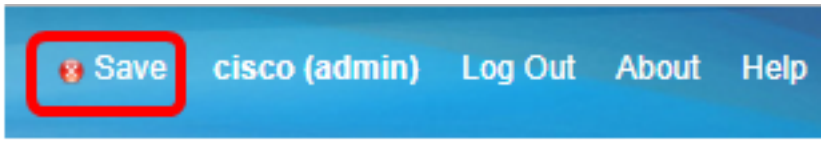
18단계. End *IP* 필드에서 VPN 클라이언트에 할당할 수 있는 마지막 IP 주소를 입력합니다.

참고:이 예에서는 10.10.100.245을 입력합니다.

19단계. 적용을 **클릭합니다**.



20단계. 저장을 **클릭합니다**.

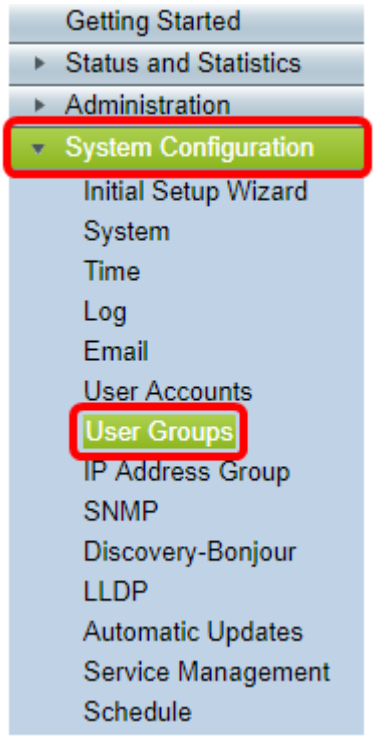


이제 GreenBow VPN Client용 라우터에서 클라이언트-사이트 프로파일을 구성했어야 합니다 .

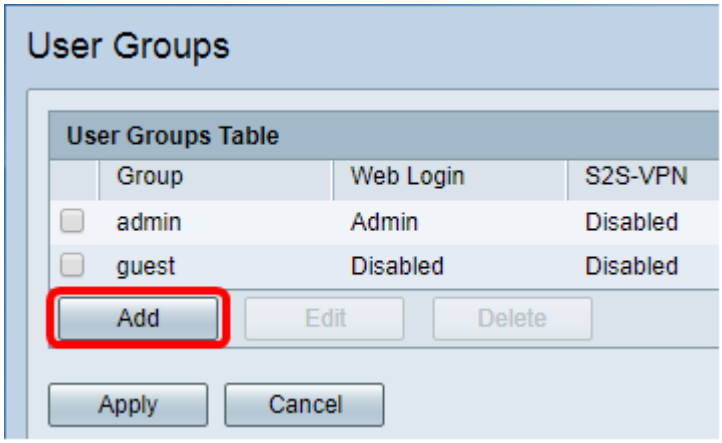
사용자 그룹 생성

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

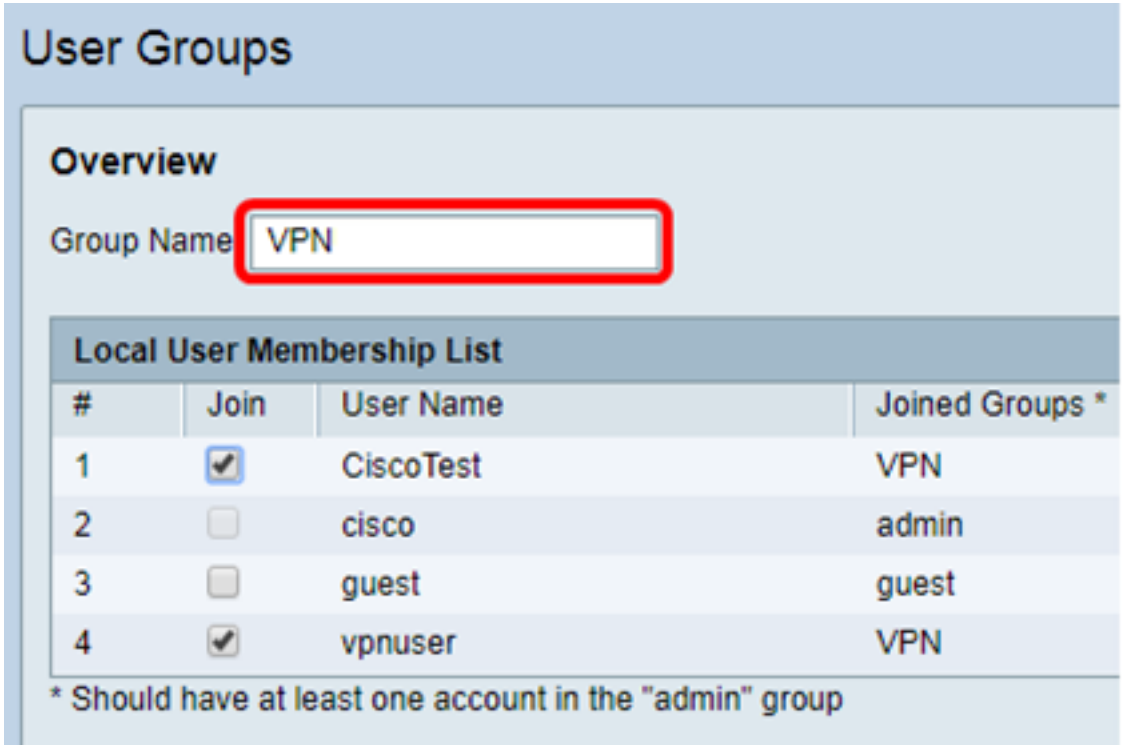
참고:이 문서의 이미지는 RV340 라우터에서 가져온 것입니다.옵션은 디바이스의 모델에 따라 달라질 수 있습니다.



2단계. **Add(추가)**를 클릭하여 사용자 그룹을 추가합니다.

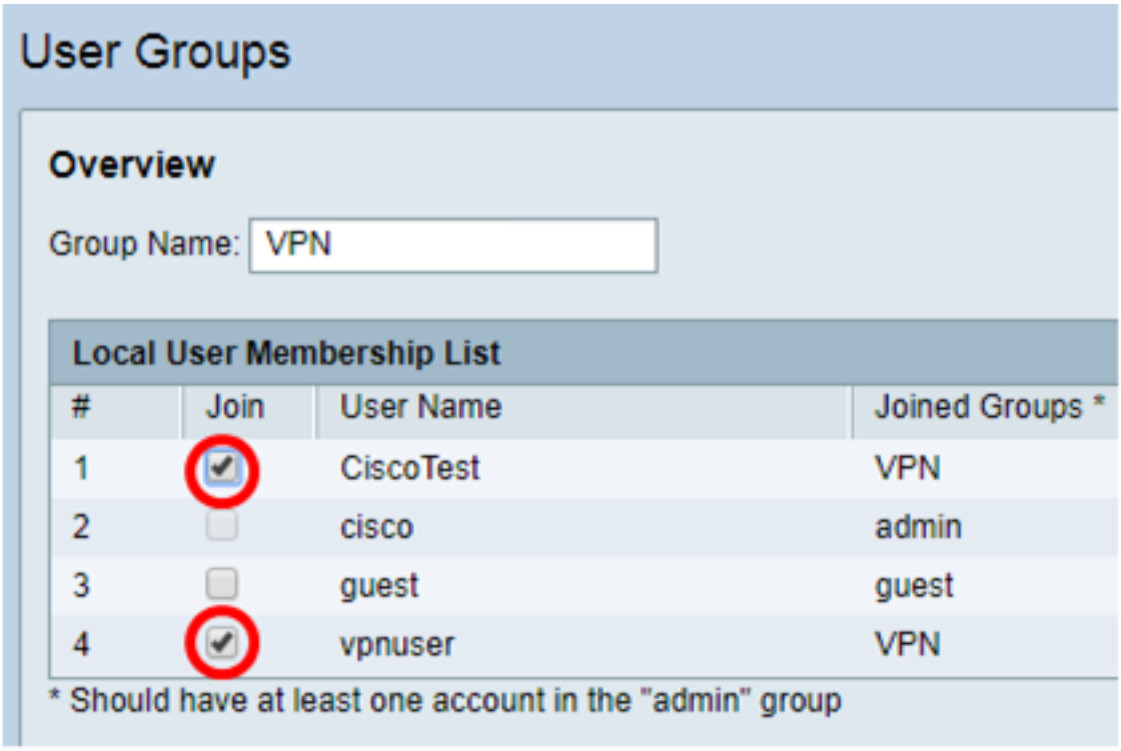


3단계. Overview(개요) 영역의 *Group Name(그룹 이름)* 필드에 그룹 이름을 입력합니다.



참고:이 예에서는 VPN이 사용됩니다.

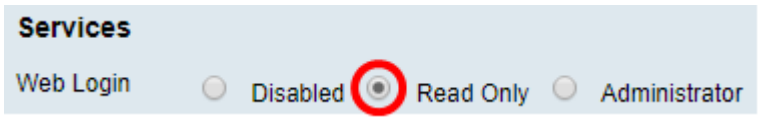
4단계. Local Membership List(로컬 구성원 목록)에서 동일한 그룹에 있어야 하는 사용자 이름의 확인란을 선택합니다.



참고:이 예에서는 CiscoTest 및 vpnuser를 선택합니다.

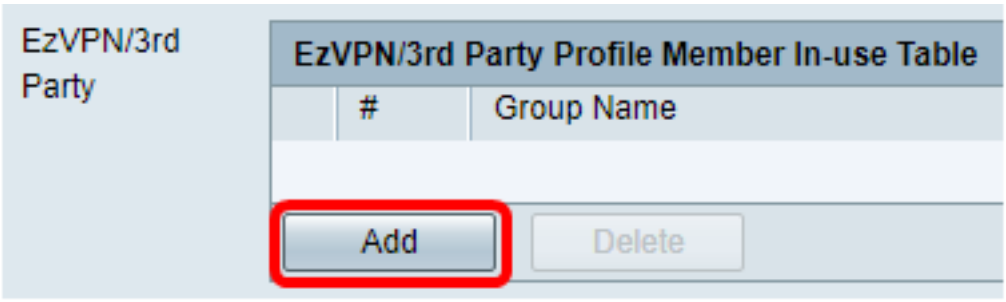
5단계. Services(서비스)에서 그룹의 사용자에게 부여할 권한을 선택합니다.옵션은 다음과 같습니다.

- 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.
- 관리자 — 이 옵션은 그룹 구성원에게 읽기 및 쓰기 권한을 제공하며 시스템 상태를 구성할 수 있습니다.

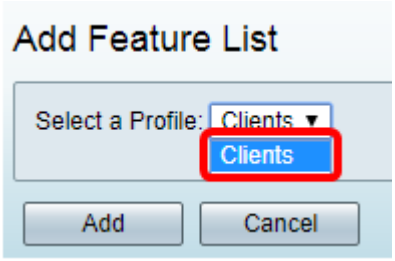


참고:이 예에서는 읽기 전용이 선택됩니다.

6단계. EzVPN/타사 프로필 구성원 사용 중 테이블에서 **추가**를 클릭합니다.

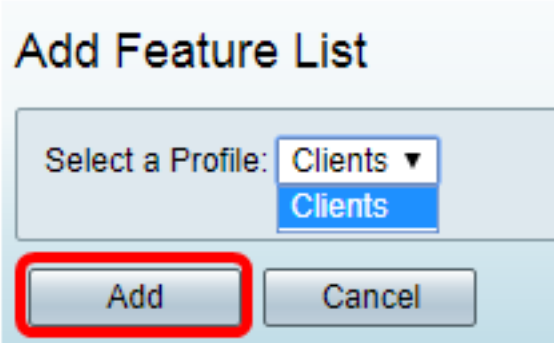


7단계. 프로파일 선택 드롭다운 목록에서 프로파일을 선택합니다.옵션은 VPN 게이트웨이에 구성된 프로필에 따라 달라질 수 있습니다.

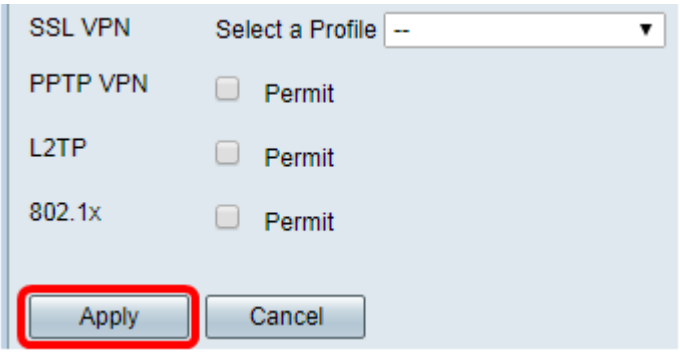


참고:이 예에서는 클라이언트가 선택됩니다.

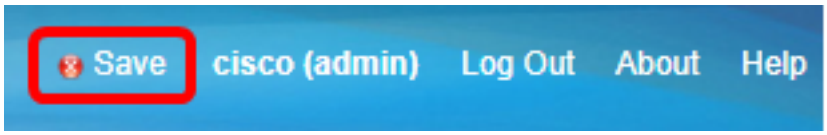
8단계. **추가**를 클릭합니다.



9단계. **적용**을 클릭합니다.



10단계. 저장을 **클릭합니다**.

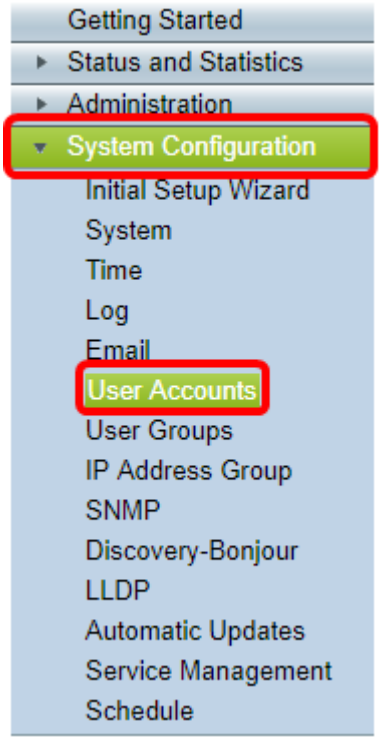


이제 RV34x Series Router에서 사용자 그룹을 성공적으로 생성해야 합니다.

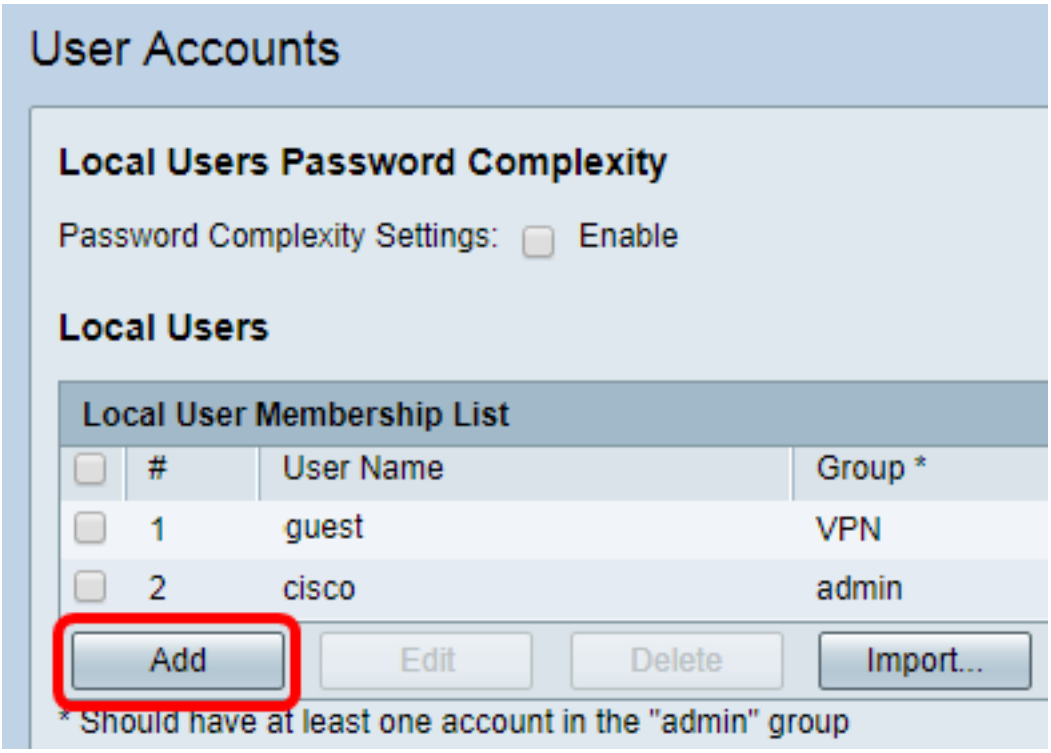
사용자 계정 생성

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

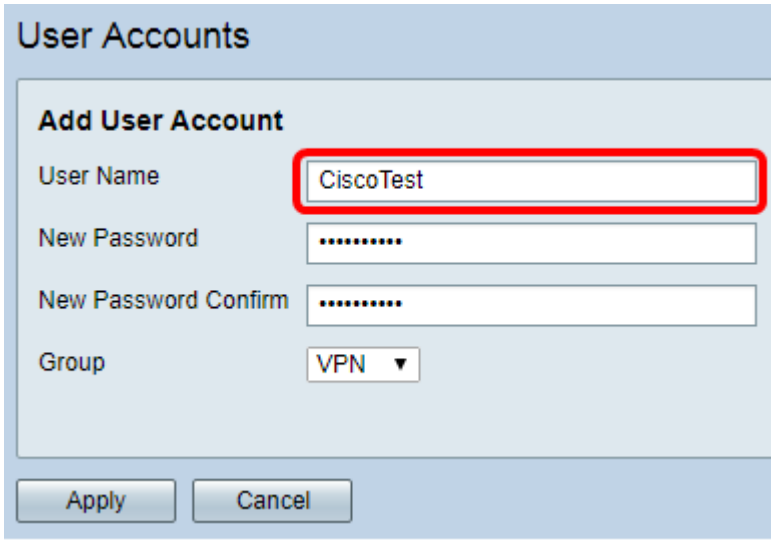
참고:이 문서의 이미지는 RV340 라우터에서 가져온 것입니다.옵션은 디바이스의 모델에 따라 달라질 수 있습니다.



2단계. Local User Membership List(로컬 사용자 구성원 목록) 영역에서 Add(**추가**)를 클릭합니다.

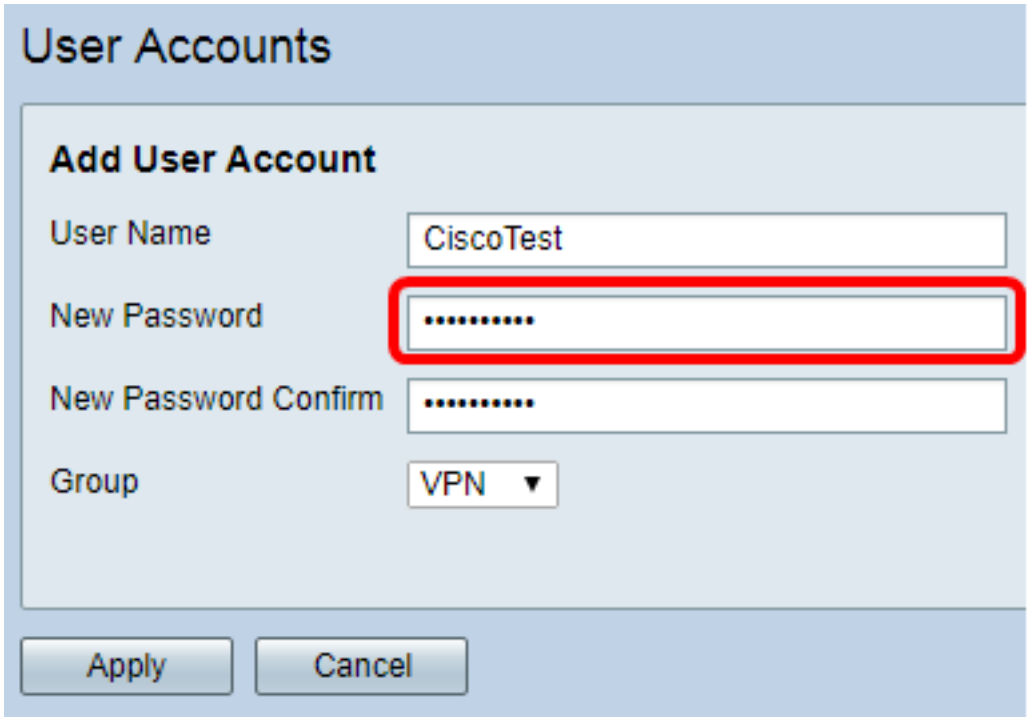


3단계. *사용자 이름* 필드에 사용자 이름을 입력합니다.

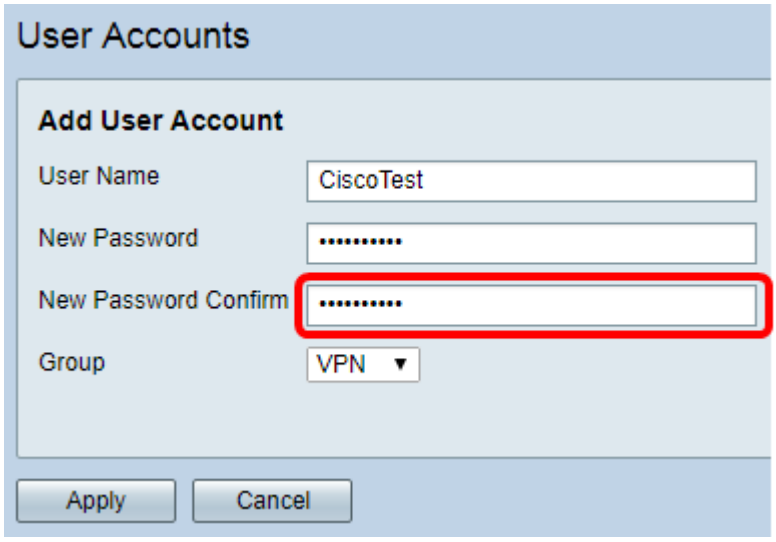


참고:이 예제에서는 CiscoTest를 입력합니다.

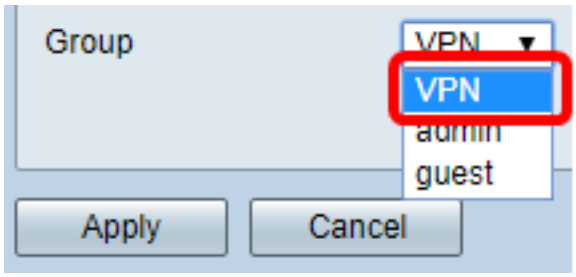
4단계. *새 비밀번호* 필드에 사용자 비밀번호를 입력합니다.



5단계. *새 비밀번호 확인* 상자에서 비밀번호를 확인합니다.

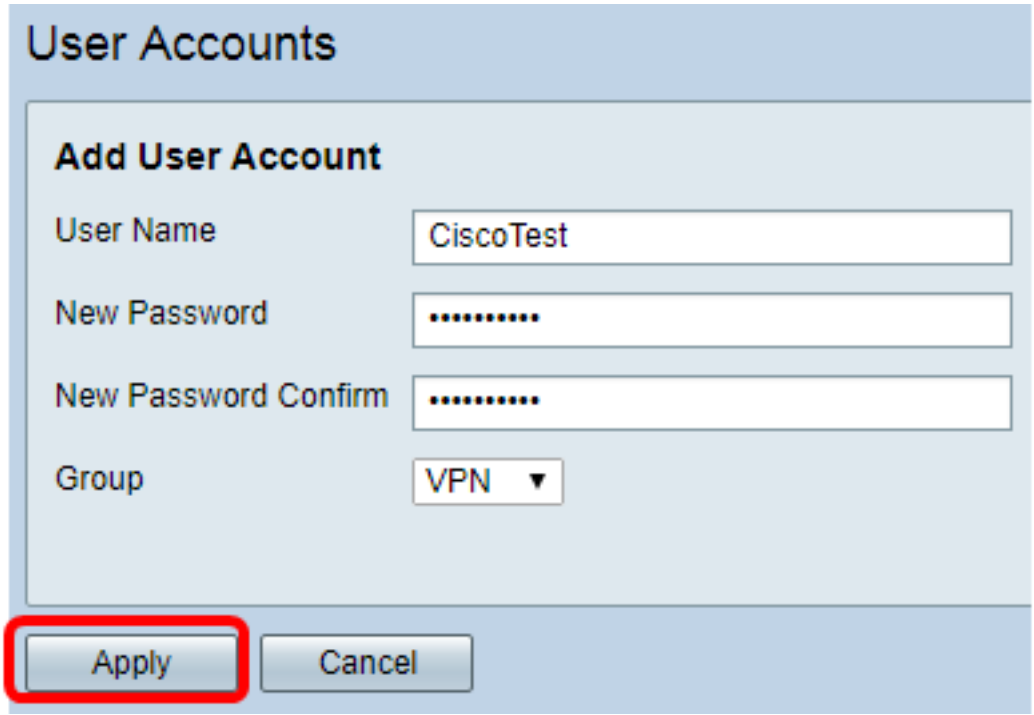


6단계. 그룹 드롭다운 목록에서 그룹을 선택합니다.사용자가 연결될 그룹입니다.

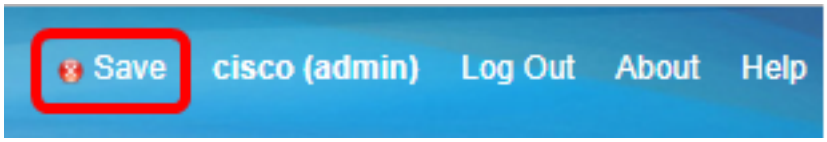


참고:이 예에서는 VPN이 선택됩니다.

7단계. 적용을 **클릭합니다**.



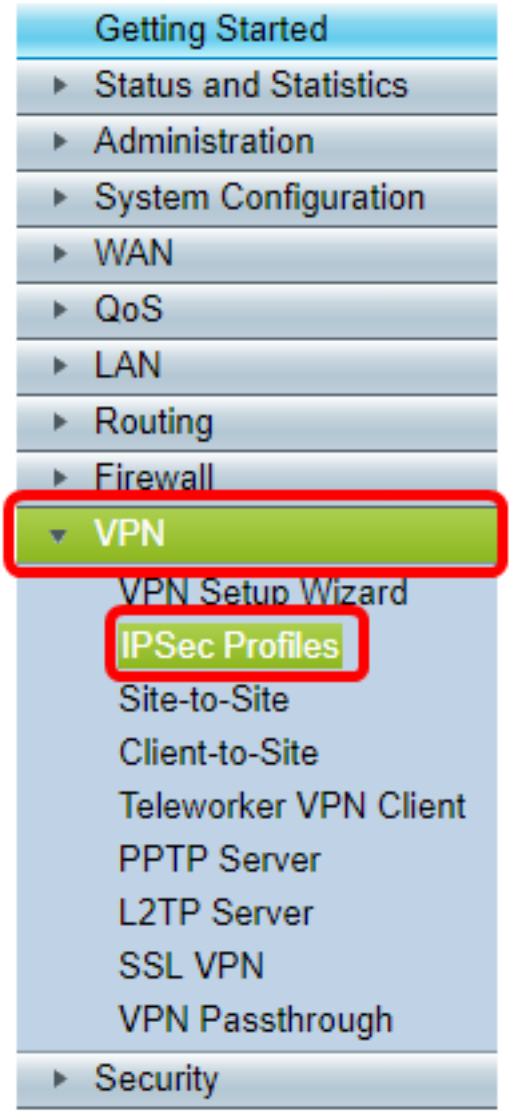
8단계. **저장**을 클릭합니다.



이제 RV34x Series 라우터에 사용자 계정을 생성해야 합니다.

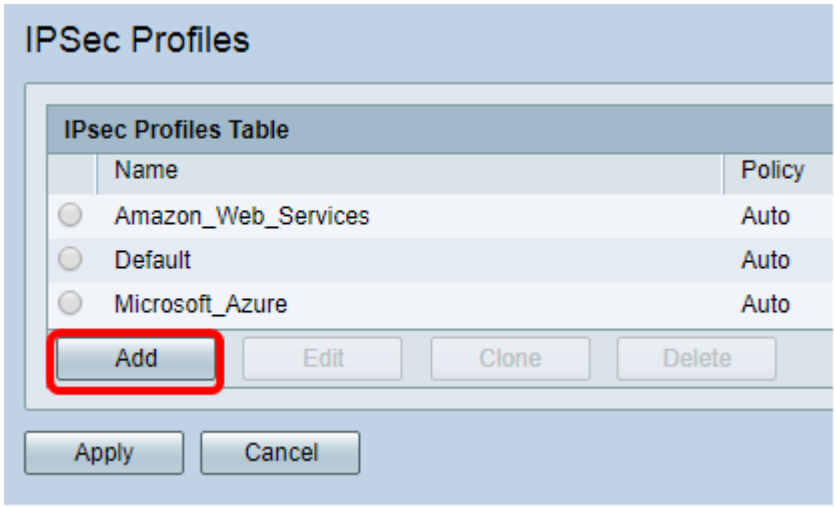
IPSec 프로필 구성

1단계. RV34x 라우터의 웹 기반 유틸리티에 로그인하고 **VPN > IPSec Profiles**를 선택합니다.



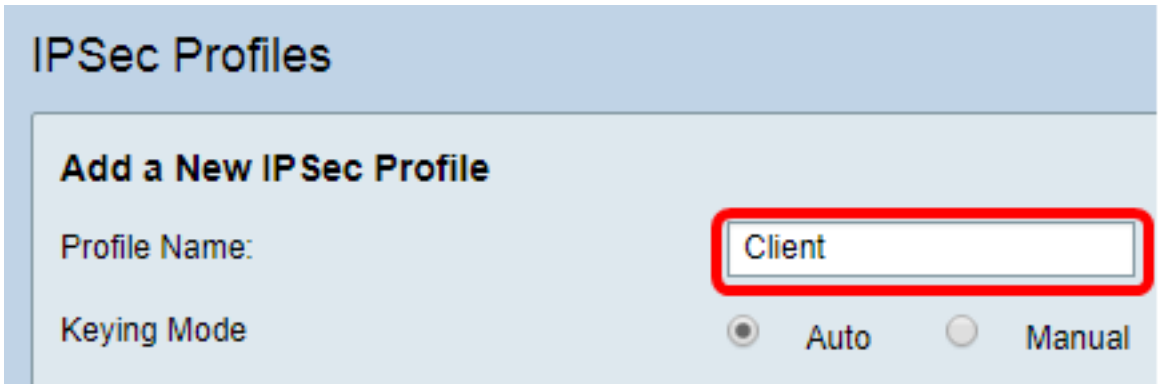
참고:이 문서의 이미지는 RV340 라우터에서 가져온 것입니다.옵션은 디바이스의 모델에 따라 달라질 수 있습니다.

2단계. IPSec 프로파일 테이블에는 기존 프로파일이 표시됩니다.Add(**추가**)를 클릭하여 새 프로필을 생성합니다.



참고: Amazon_Web_Services, Default 및 Microsoft_Azure는 기본 프로필입니다.

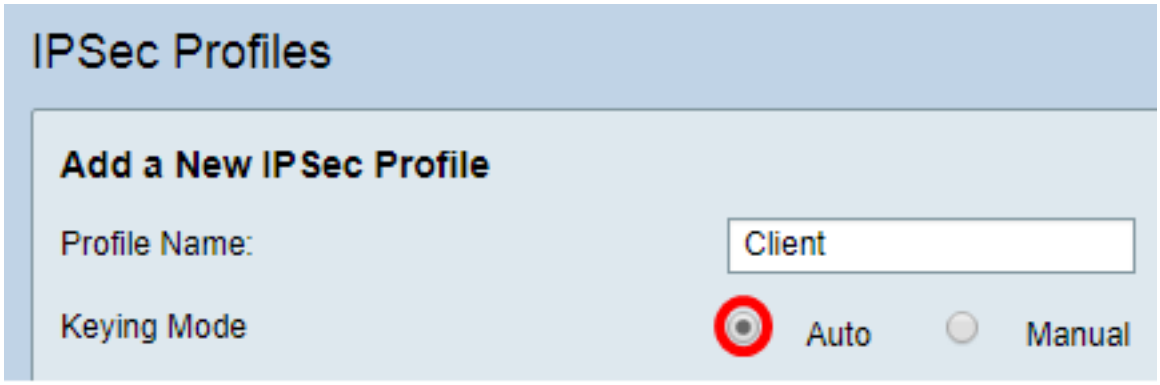
3단계. 프로파일 이름 필드에 프로파일 이름을 생성합니다.프로파일 이름은 특수 문자의 영숫자 문자 및 밑줄(_)만 포함해야 합니다.



참고:이 예에서는 클라이언트가 입력됩니다.

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.이 옵션을 선택한 경우 Configure Auto Settings(자동 설정 구성)로 건너뜁니다.
- 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.이 옵션을 선택한 경우 Configure Manual Settings(수동 설정 구성)로 건너뜁니다.



참고:이 예에서는 Auto가 선택되었습니다.

[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.

참고:이 예에서는 Group5-1536비트가 선택됩니다.

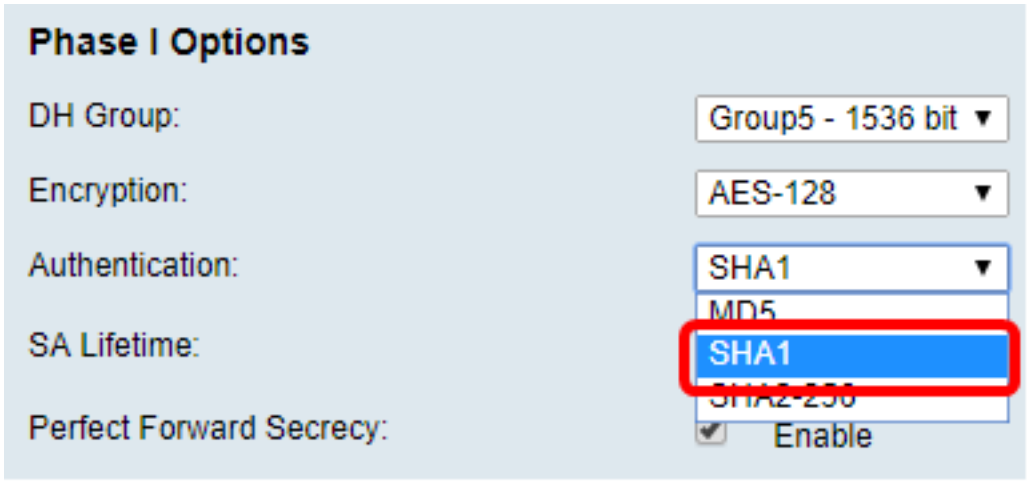
2단계. Encryption(암호화) 드롭다운 목록에서 암호화 방법을 선택하여 ESP(Encapsulating Security Payload) 및 ISAKMP(Internet Security Association and Key Management Protocol)를 암호화하고 해독합니다. 옵션은 다음과 같습니다.

- 3DES — 3중 데이터 암호화 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.

참고:AES는 DES와 3DES를 통한 암호화의 표준 방법으로 성능과 보안을 강화합니다.AES 키를 늘리면 성능이 저하되어 보안이 강화됩니다.이 예에서는 AES-128이 선택됩니다.

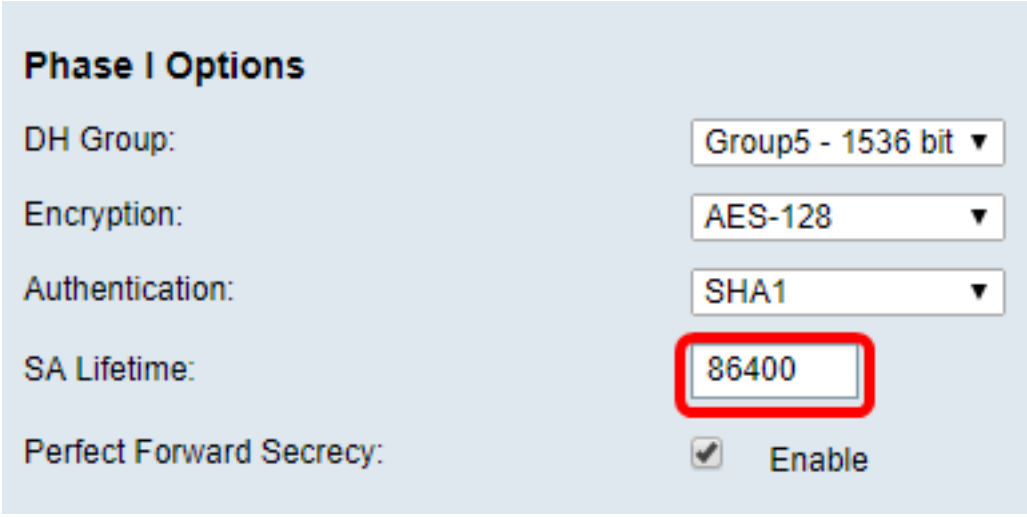
3단계. Authentication(인증) 드롭다운 목록에서 ESP 및 ISAKMP의 인증 방법을 결정하는 인증 방법을 선택합니다.옵션은 다음과 같습니다.

- 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.



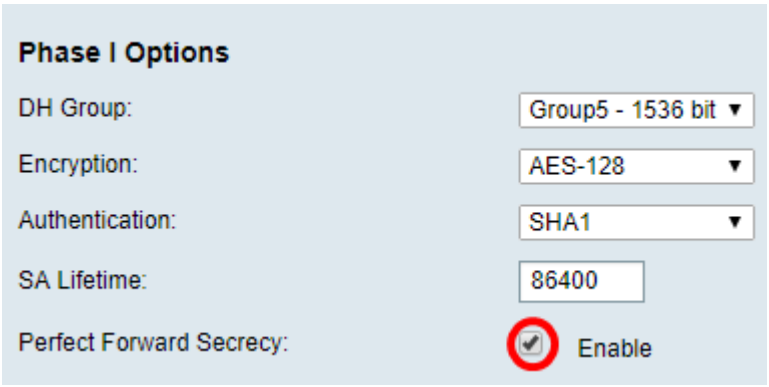
참고:MD5 및 SHA는 모두 암호화 해시 함수입니다.데이터를 가져와서 압축하고 일반적으로 재현할 수 없는 고유한 16진수 출력을 만듭니다.이 예에서는 SHA1이 선택됩니다.

4단계. *SA Lifetime* 필드에 120에서 86400 사이의 값을 입력합니다. 이는 단계에서 IKE(Internet Key Exchange) SA(Security Association)가 활성 상태로 유지되는 시간입니다.기본값은 28800입니다.



참고:이 예에서는 86400을 입력합니다.

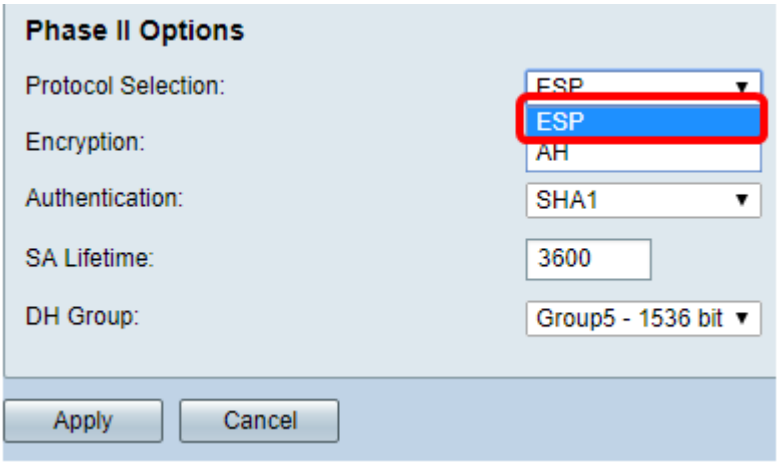
5단계. (선택 사항) Enable **Perfect** Forward Secrecy 확인란을 선택하여 IPSec 트래픽 암호화 및 인증을 위한 새 키를 생성합니다.



참고:이 예에서는 Perfect Forward Secrecy가 활성화됩니다.

6단계. II 단계 옵션 영역의 프로토콜 선택 드롭다운 목록에서 협상의 두 번째 단계에 적용할 프로토콜 유형을 선택합니다.옵션은 다음과 같습니다.

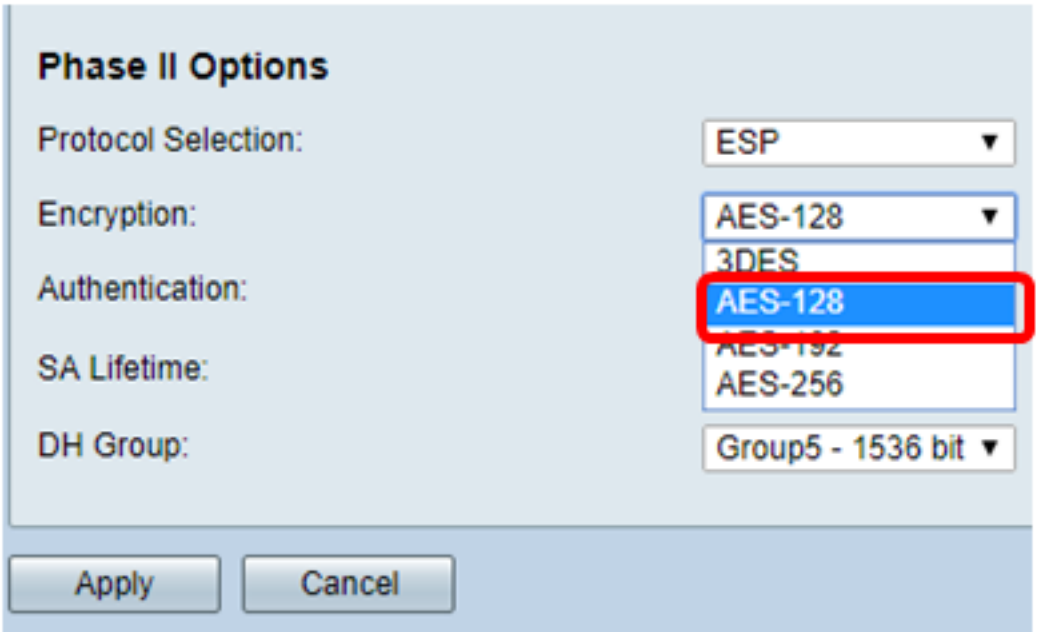
- ESP — 이 옵션은 보호할 데이터를 캡슐화합니다.이 옵션을 선택한 경우 7단계로 이동하여 암호화 방법을 선택합니다.
- AH — 이 옵션은 AH(Authentication Header)라고도 합니다. 데이터 인증 및 선택적 재전송 방지 서비스를 제공하는 보안 프로토콜입니다.AH는 보호할 IP 데이터그램에 포함되어 있습니다.이 옵션을 선택한 경우 8단계로 건너뜁니다.



참고:이 예에서는 ESP가 선택됩니다.

7단계. 6단계에서 ESP를 선택한 경우 ESP 및 ISAKMP의 인증 방법을 결정하는 인증 방법을 선택합니다.옵션은 다음과 같습니다.

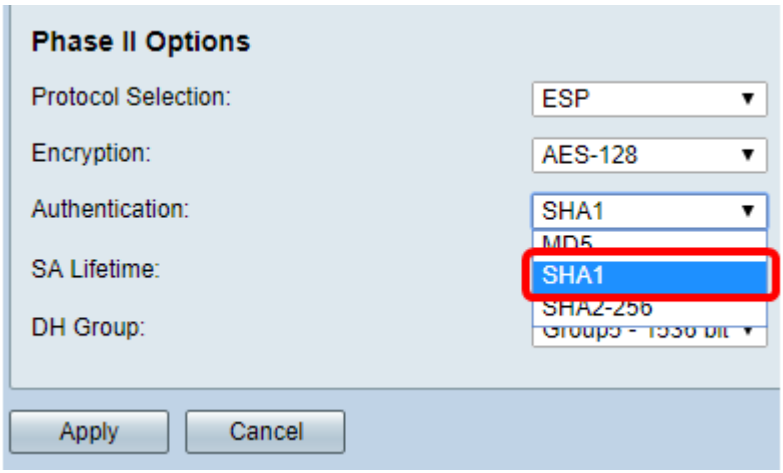
- 3DES — 3중 데이터 암호화 표준
- AES-128 — 고급 암호화 표준은 128비트 키를 사용합니다.
- AES-192 — 고급 암호화 표준은 192비트 키를 사용합니다.
- AES-256 — 고급 암호화 표준은 256비트 키를 사용합니다.



참고:이 예에서는 AES-128이 선택됩니다.

8단계. 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.

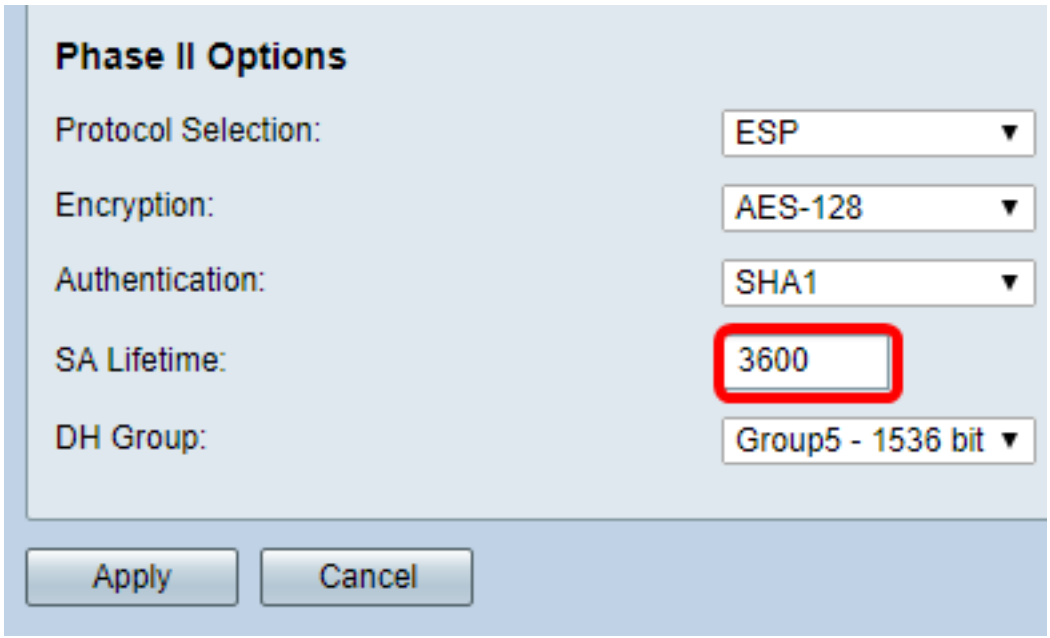


참고:이 예에서는 SHA1이 선택됩니다.

9단계. *SA Lifetime* 필드에 120에서 28800 사이의 값을 입력합니다. 이 단계에서는 IKE SA가 활성 상태로 유지되는 시간입니다.기본값은 3600입니다.

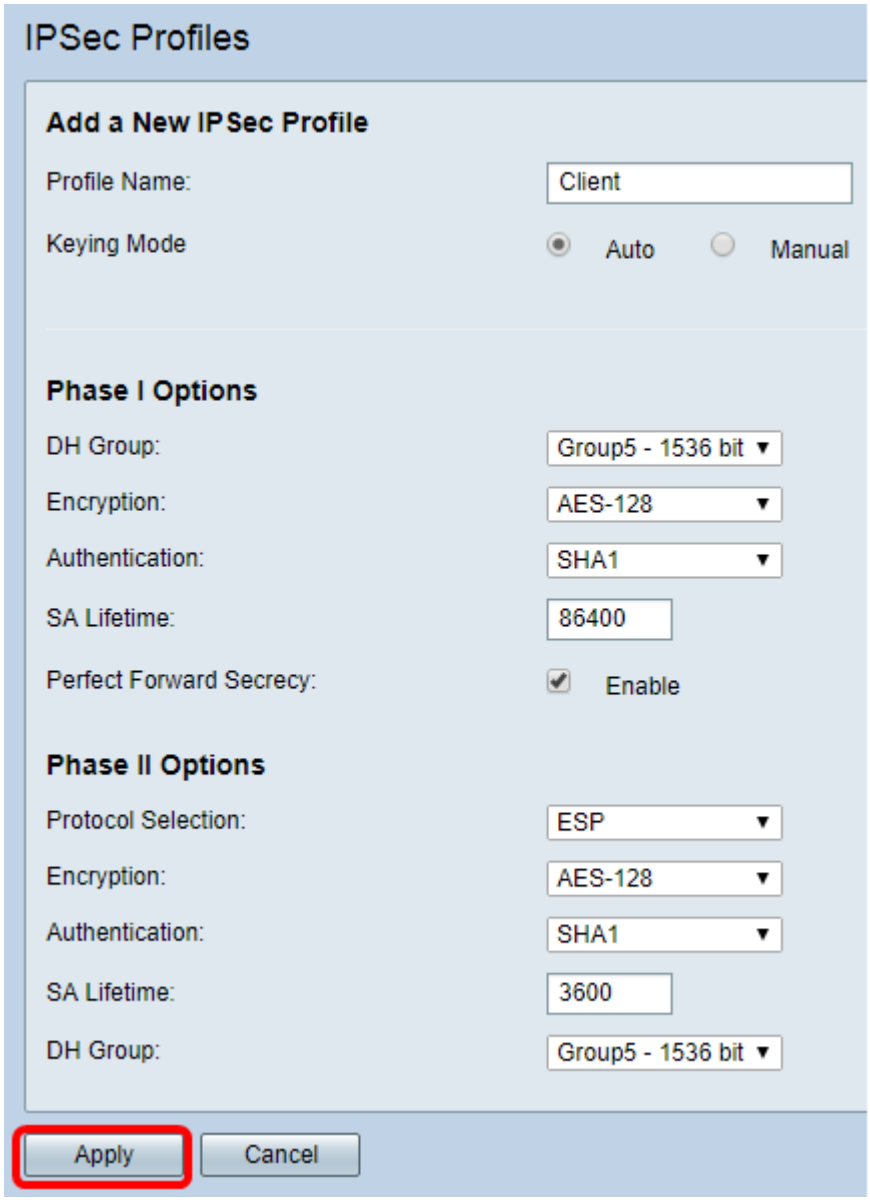
10단계. DH 그룹 드롭다운 목록에서 2단계의 키와 함께 사용할 DH 그룹을 선택합니다. 옵션은 다음과 같습니다.

- Group2-1024비트 — 이 옵션은 키를 느리게 계산하지만 Group1보다 안전합니다.
- Group5-1536비트 — 이 옵션은 가장 느린 키를 계산하지만 가장 안전합니다.

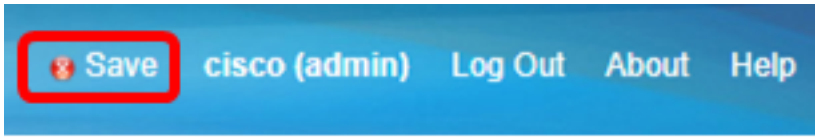


참고:이 예에서는 3600을 입력합니다.

11단계. 적용을 **클릭합니다**.



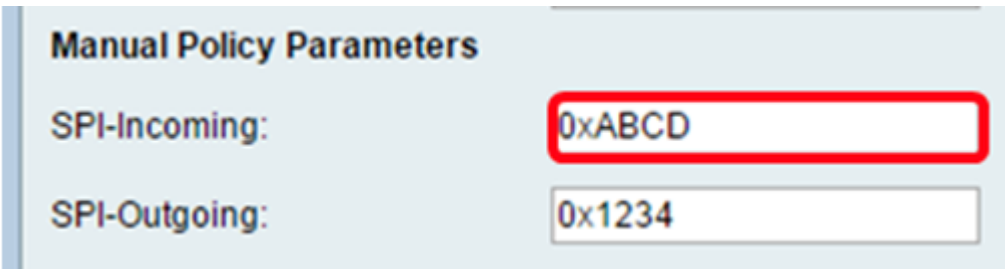
12단계. **저장**을 클릭하여 구성을 영구적으로 저장합니다.



이제 RV34x Series Router에서 Automatic IPSec 프로파일을 성공적으로 구성했어야 합니다.

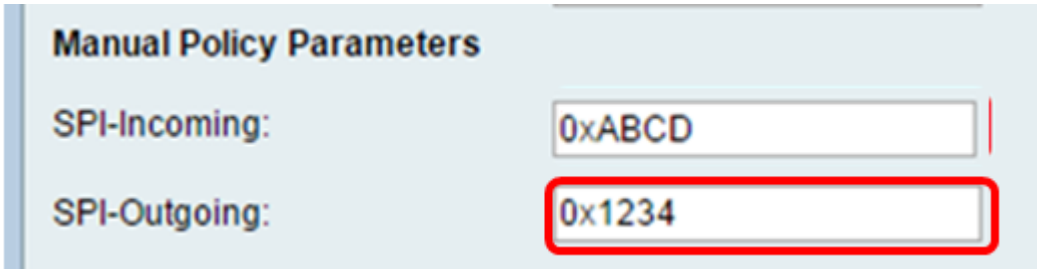
수동 설정 구성

1단계. *SPI-Incoming* 필드에 VPN 연결에서 들어오는 트래픽에 대한 SPI(Security Parameter Index) 태그에 100에서 FFFFFFFFF까지의 16진수 값을 입력합니다.SPI 태그는 한 세션의 트래픽과 다른 세션의 트래픽을 구분하는 데 사용됩니다.



참고:이 예에서는 0xABCD가 입력됩니다.

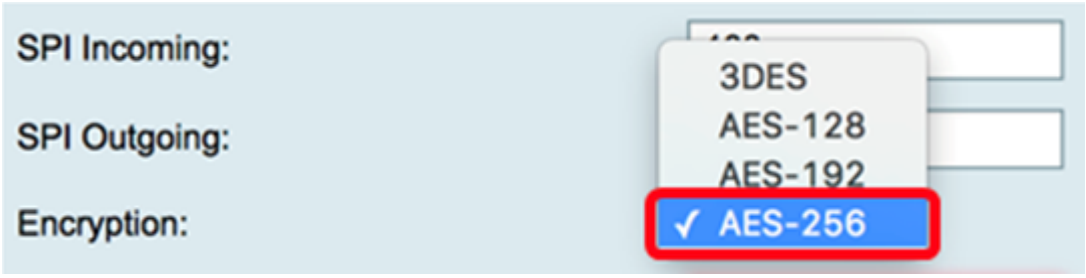
2단계. *SPI-Outgoing* 필드에서 VPN 연결에서 발신 트래픽에 대한 SPI 태그의 16진수 값을 100에서 FFFFFFF로 입력합니다.



참고:이 예에서는 0x1234를 입력합니다.

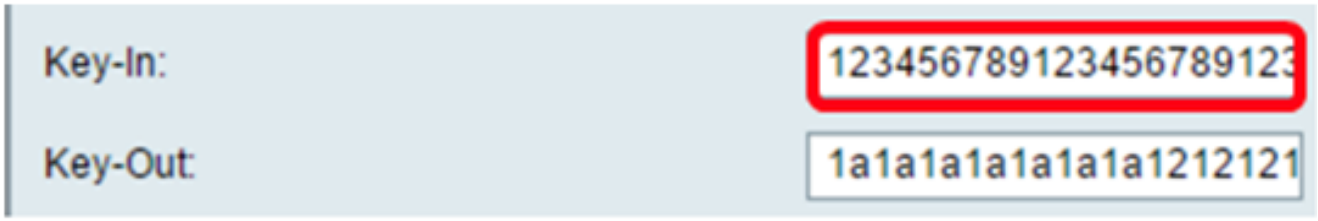
3단계. 드롭다운 목록에서 암호화 값을 선택합니다.옵션은 다음과 같습니다.

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



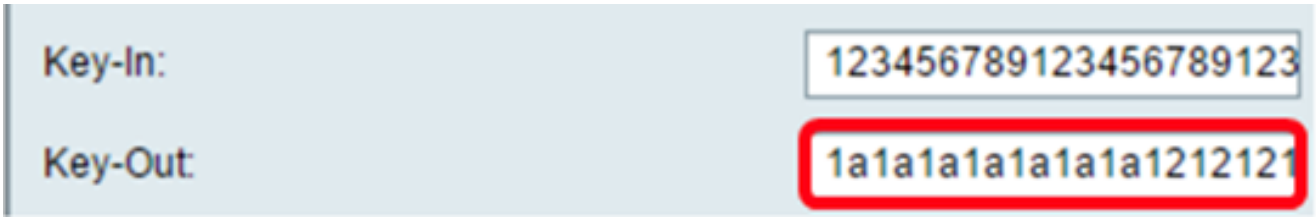
참고:이 예에서는 AES-256이 선택됩니다.

4단계. *Key-In* 필드에 인바운드 정책의 키를 입력합니다.키의 길이는 3단계에서 선택한 알고리즘에 따라 달라집니다.



참고:이 예에서는 123456789123456789123...을 입력합니다.

5단계. *Key-Out* 필드에 발송 정책의 키를 입력합니다.키의 길이는 3단계에서 선택한 알고리즘에 따라 달라집니다.



참고:이 예에서는 1a1a1a1a1a1a1a1212121212를 입력합니다.

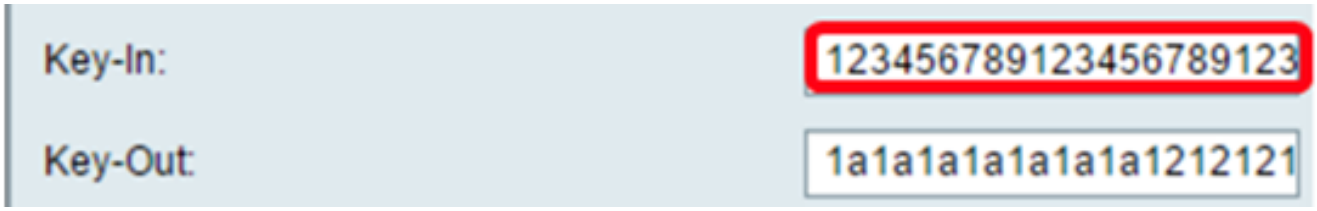
6단계. Authentication(인증) 드롭다운 목록에서 인증 방법을 선택합니다.옵션은 다음과 같습

니다.

- 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.

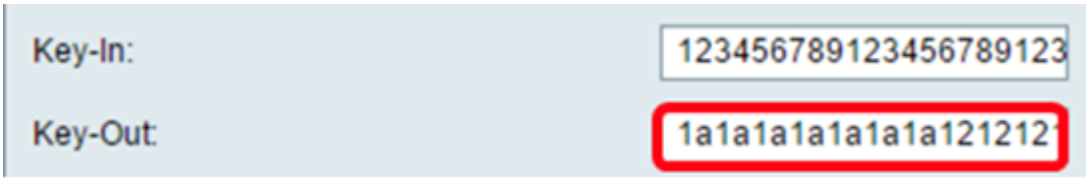
참고:이 예에서는 MD5가 선택됩니다.

7단계. *Key-In* 필드에 인바운드 정책의 키를 입력합니다.키의 길이는 6단계에서 선택한 알고리즘에 따라 달라집니다.

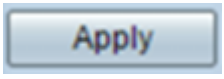


참고:이 예에서는 123456789123456789123...을 입력합니다.

8단계. *Key-Out* 필드에 발신 정책의 키를 입력합니다.키의 길이는 6단계에서 선택한 알고리즘에 따라 달라집니다.

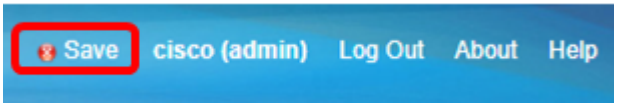


참고:이 예에서는 1a1a1a1a1a1a1a1212121212를 입력합니다.

9단계. 을 클릭합니다 

.

10단계. **저장**을 클릭하여 구성을 영구적으로 저장합니다.

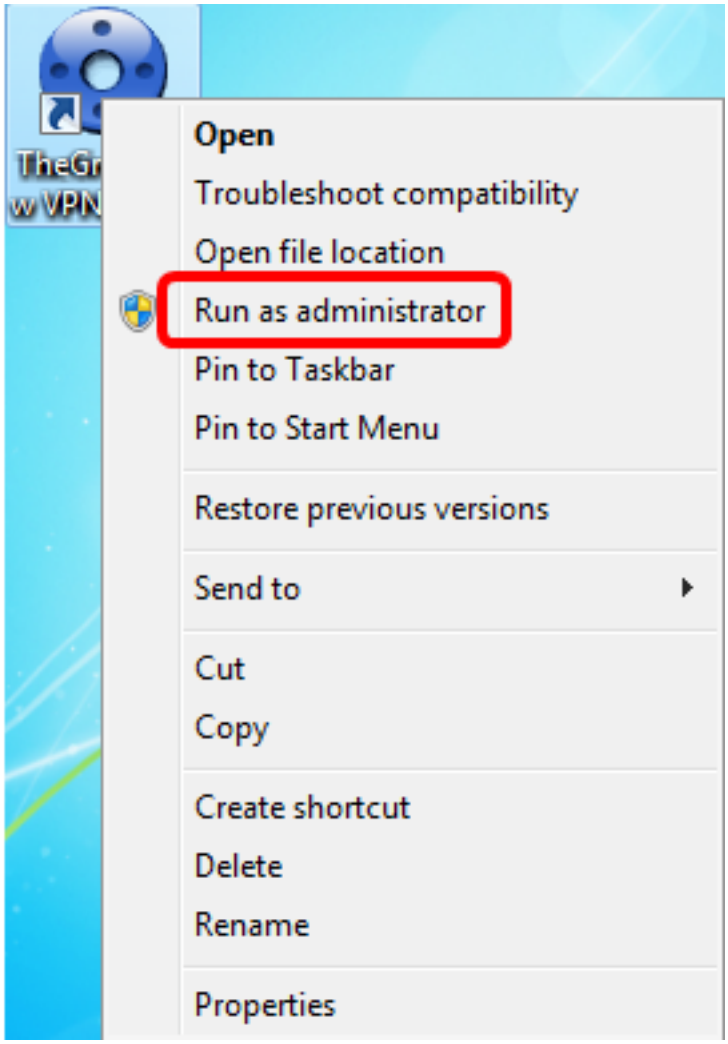


이제 RV34x Series Router에서 수동 IPSec 프로파일을 구성했어야 합니다.

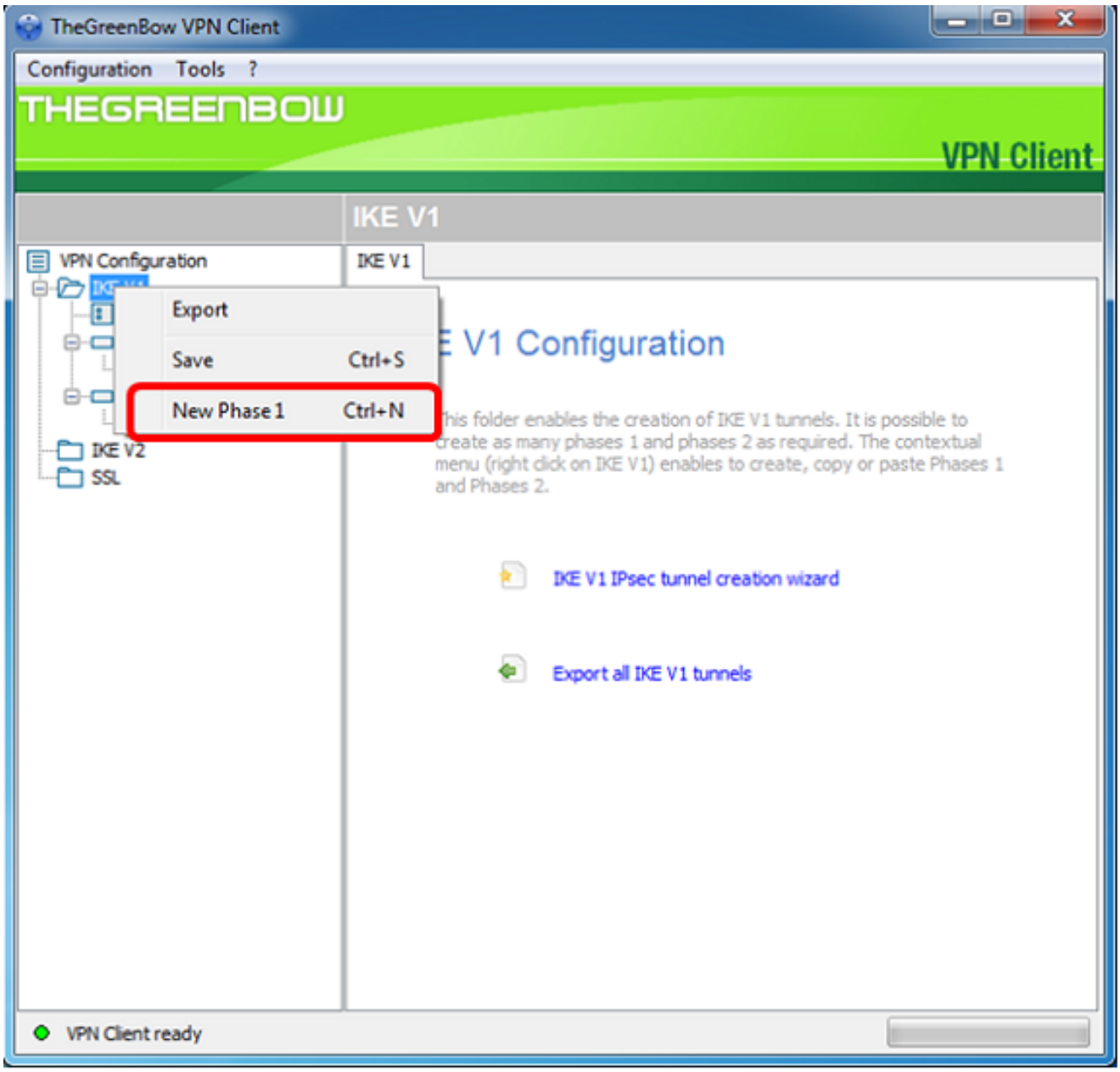
GreenBow VPN 클라이언트 소프트웨어 구성

1단계 설정 구성

1단계. GreenBow VPN Client(GreenBow VPN 클라이언트) 아이콘을 마우스 오른쪽 버튼으로 클릭하고 Run as **administrator(관리자로 실행)를** 선택합니다.

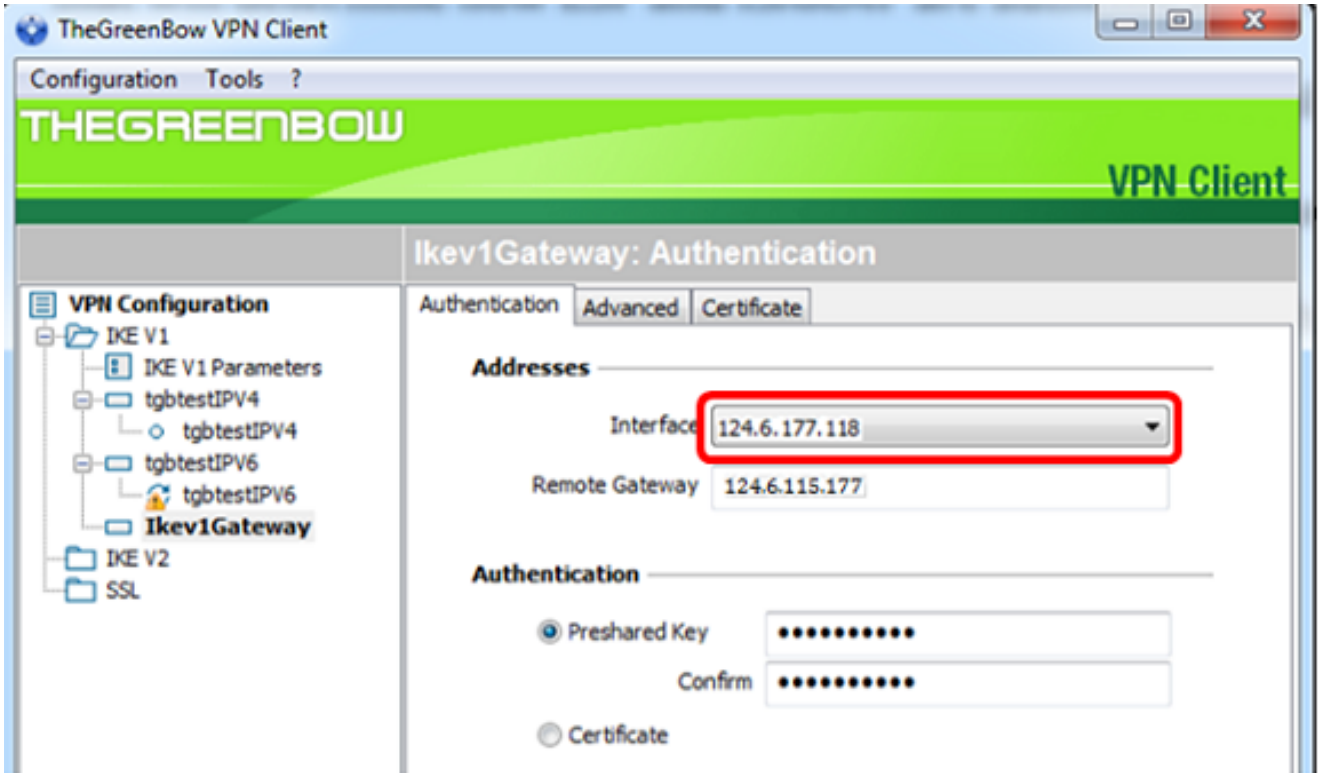


2단계. VPN 컨피그레이션 아래의 왼쪽 창에서 **IKE V1**을 마우스 오른쪽 버튼으로 클릭하고 **New Phase 1(새 단계 1)을 선택합니다**.



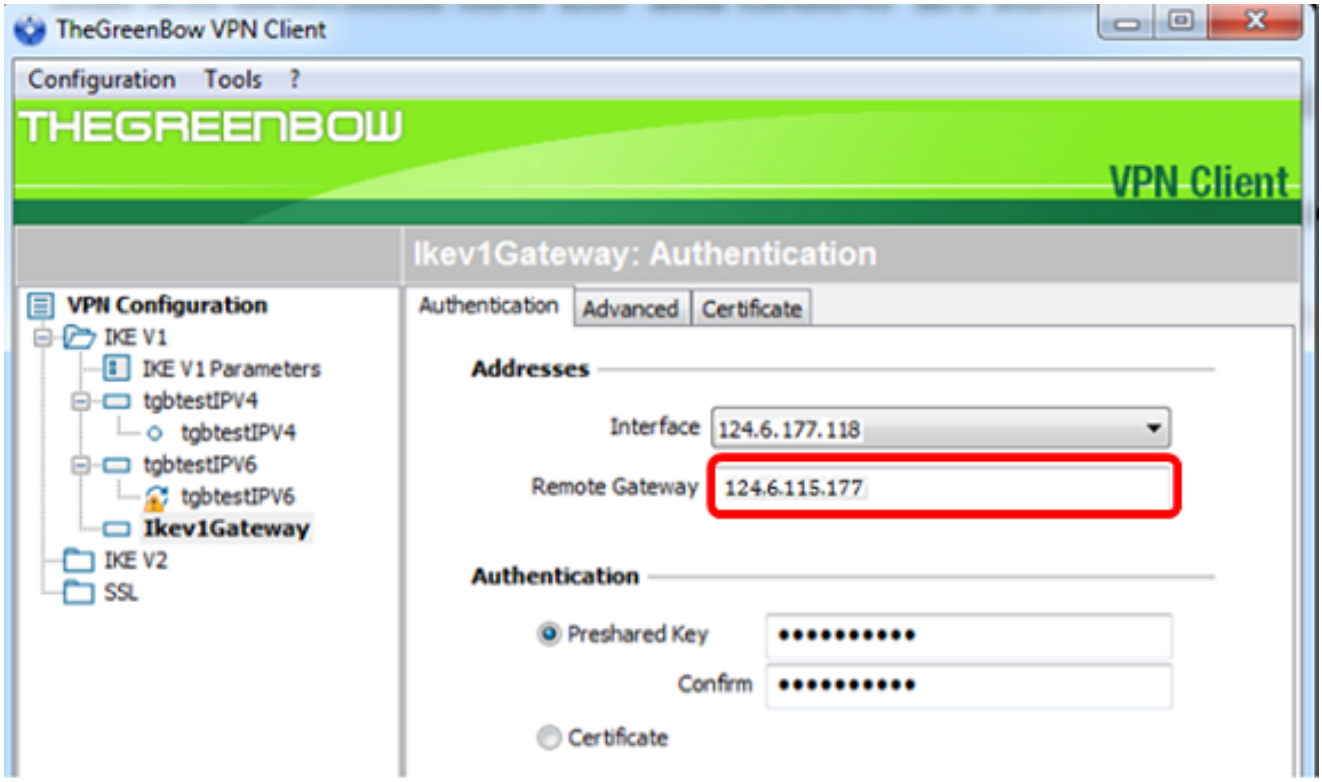
3단계. Authentication(인증) 탭의 Addresses(주소)에서 Interface(인터페이스) 영역의 IP 주소가 GreenBow VPN 클라이언트가 설치된 컴퓨터의 WAN IP 주소와 동일한지 확인합니다.

참고:이 예에서는 IP 주소가 124.6.177.118입니다.



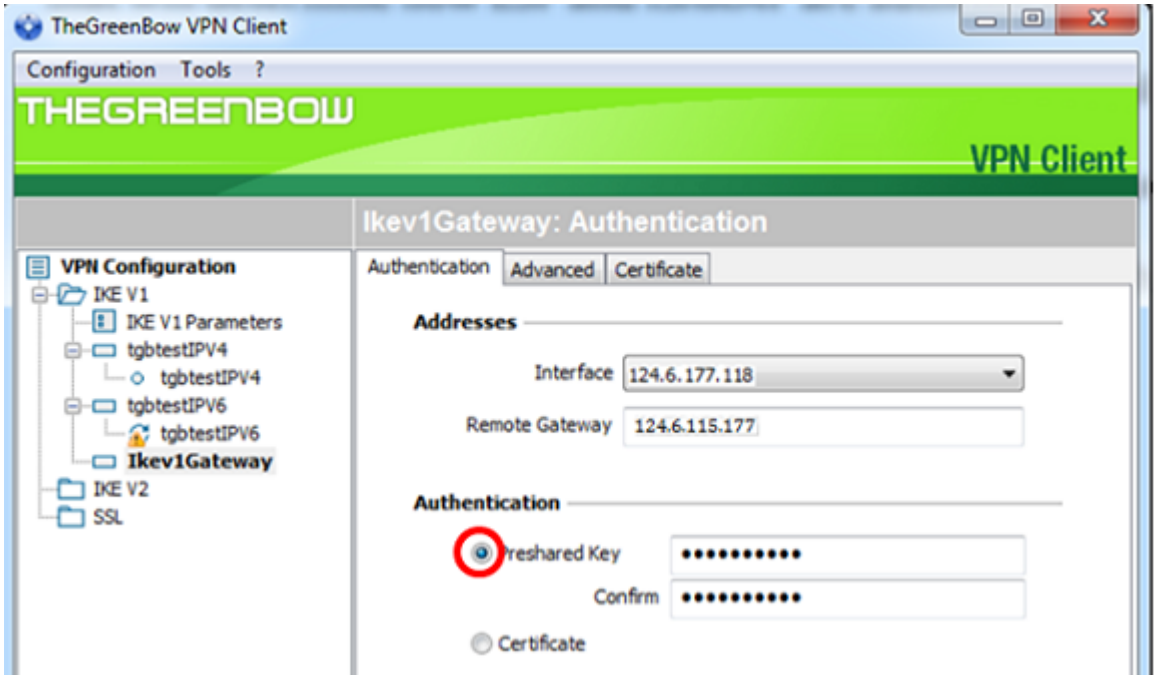
4단계. *Remote Gateway* 필드에 원격 게이트웨이의 주소를 입력합니다.

참고:이 예에서는 원격 RV34x 라우터의 IP 주소가 124.6.115.177입니다.



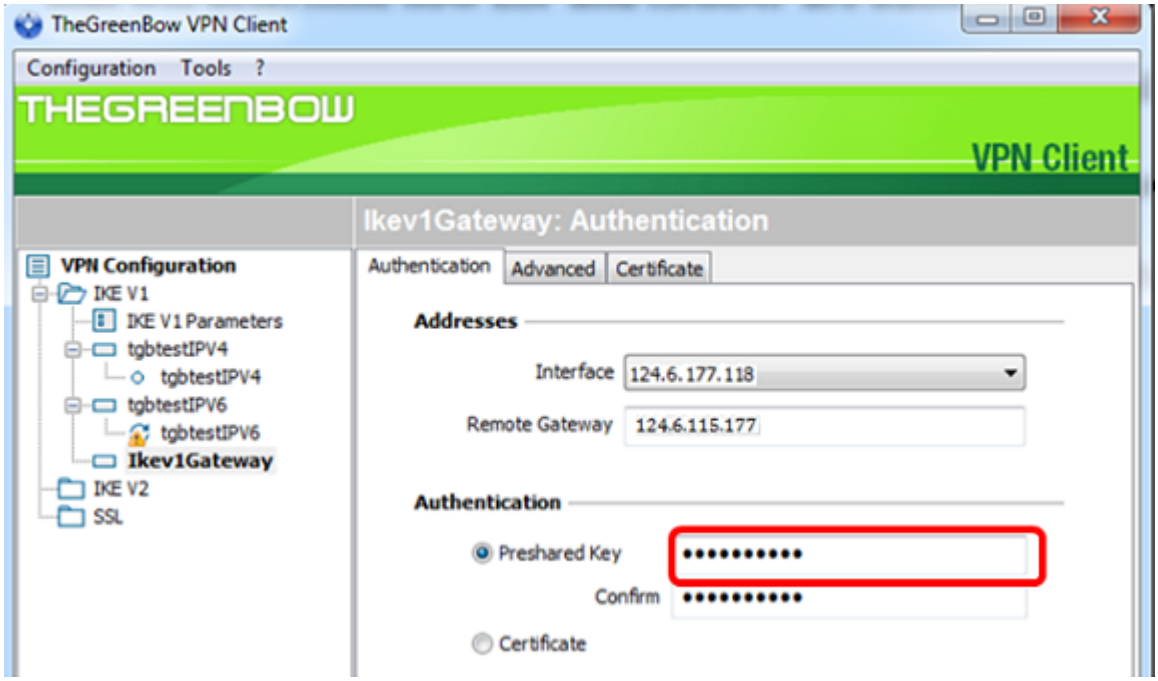
5단계. Authentication(인증)에서 인증 유형을 선택합니다.옵션은 다음과 같습니다.

- 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.

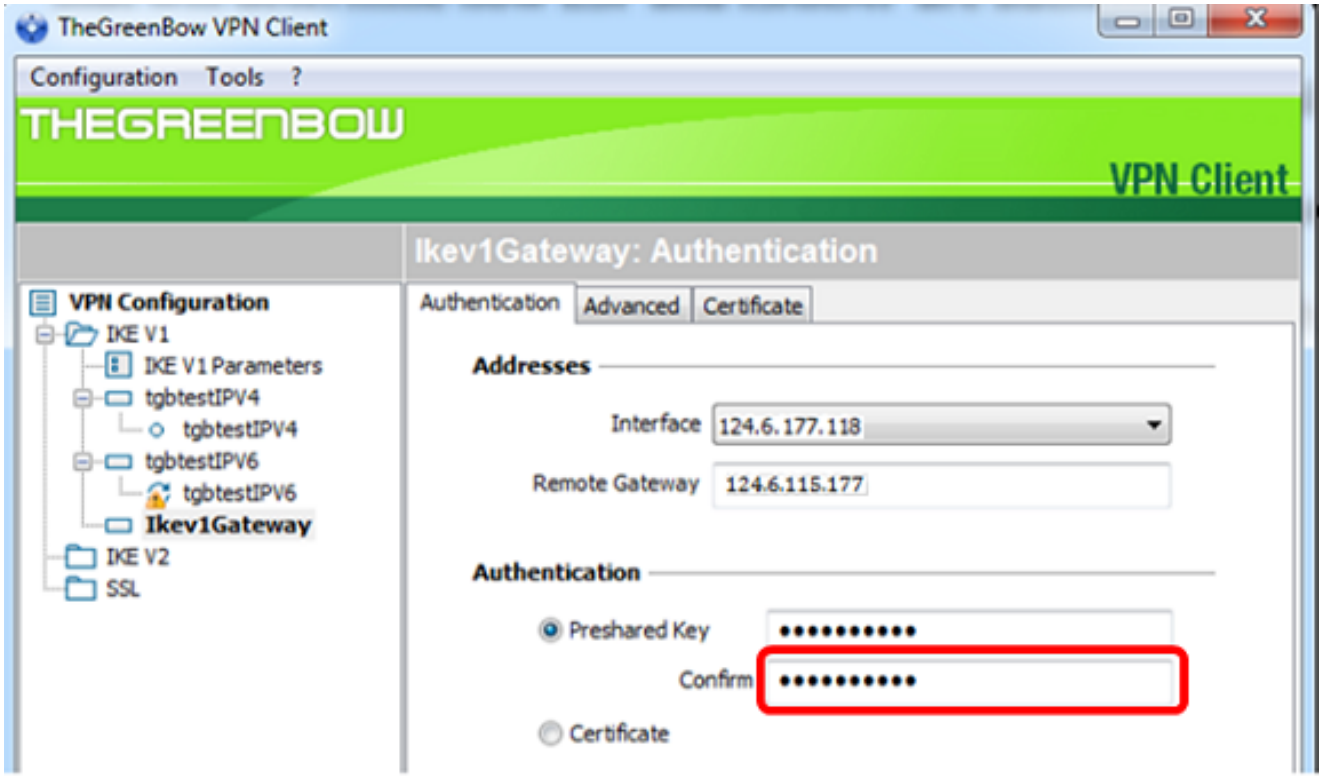


참고:이 예에서는 RV34x VPN 게이트웨이의 컨피그레이션과 일치하도록 Preshared Key(사전 공유 키)를 선택합니다.

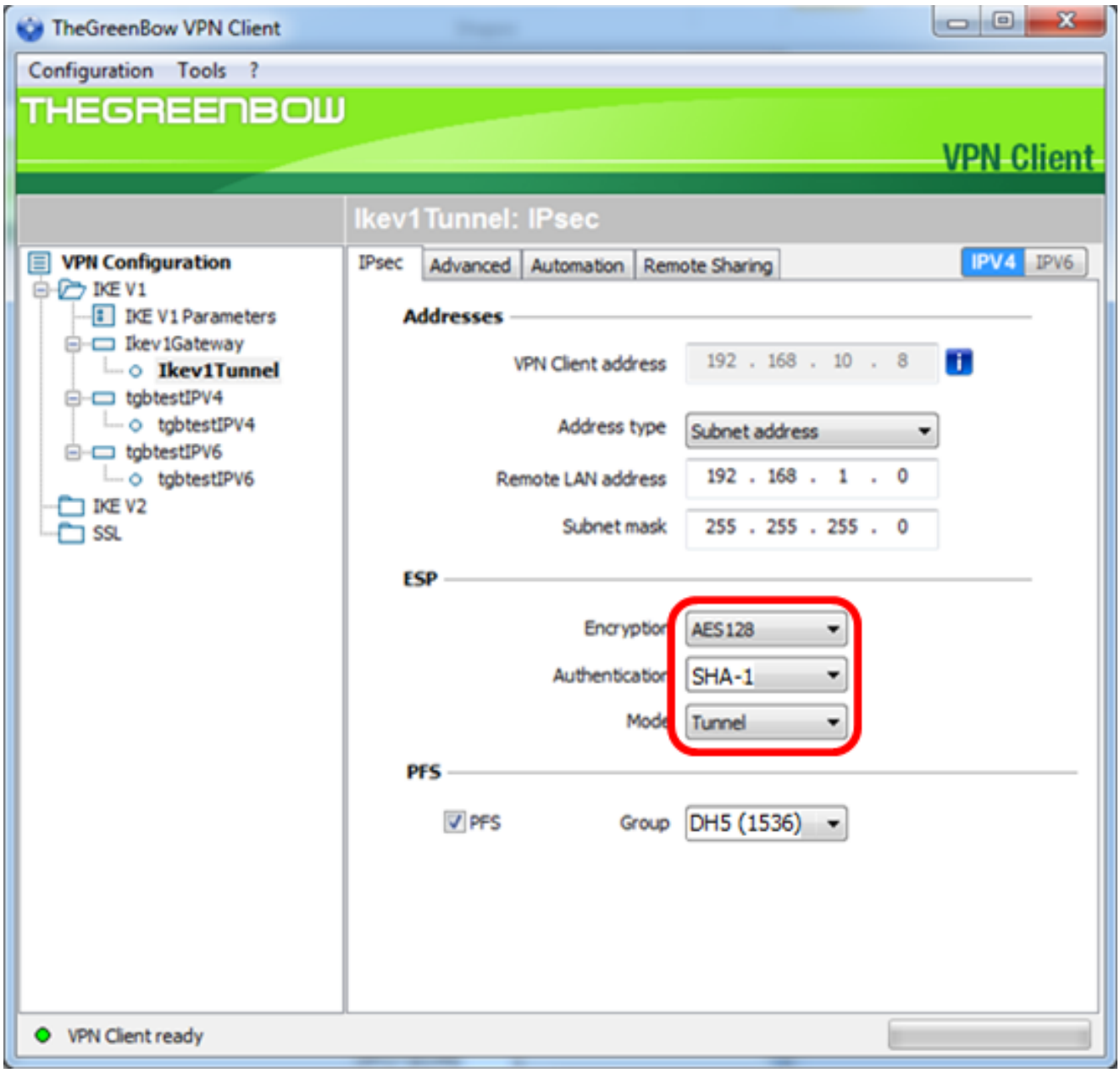
6단계. 라우터에 구성된 사전 공유 키를 입력합니다.



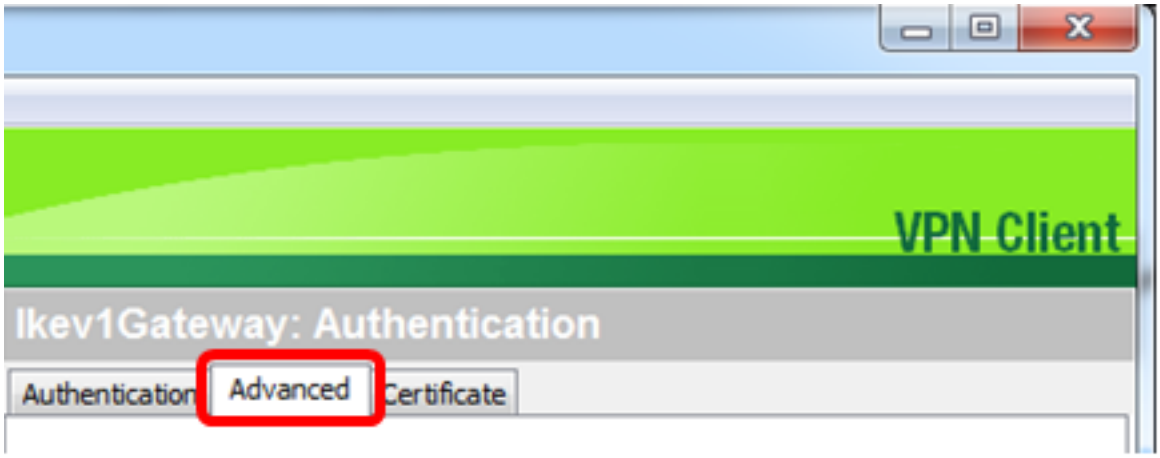
7단계. 확인 필드에 동일한 사전 공유 키를 *입력합니다*.



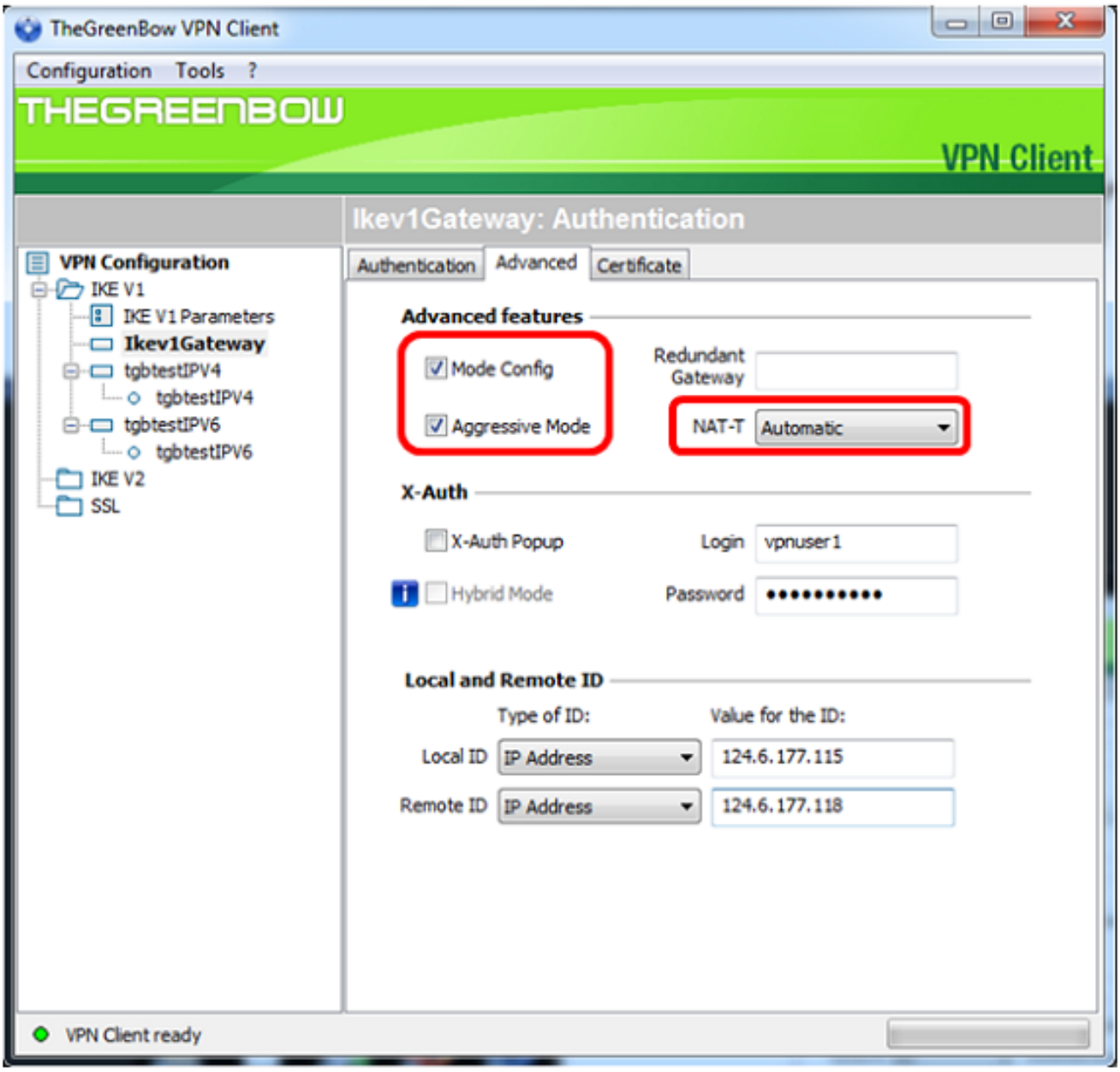
8단계. IKE에서 Encryption, Authentication 및 Key Group 설정을 라우터의 컨피그레이션과 일치하도록 설정합니다.



9단계. **고급** 탭을 클릭합니다.

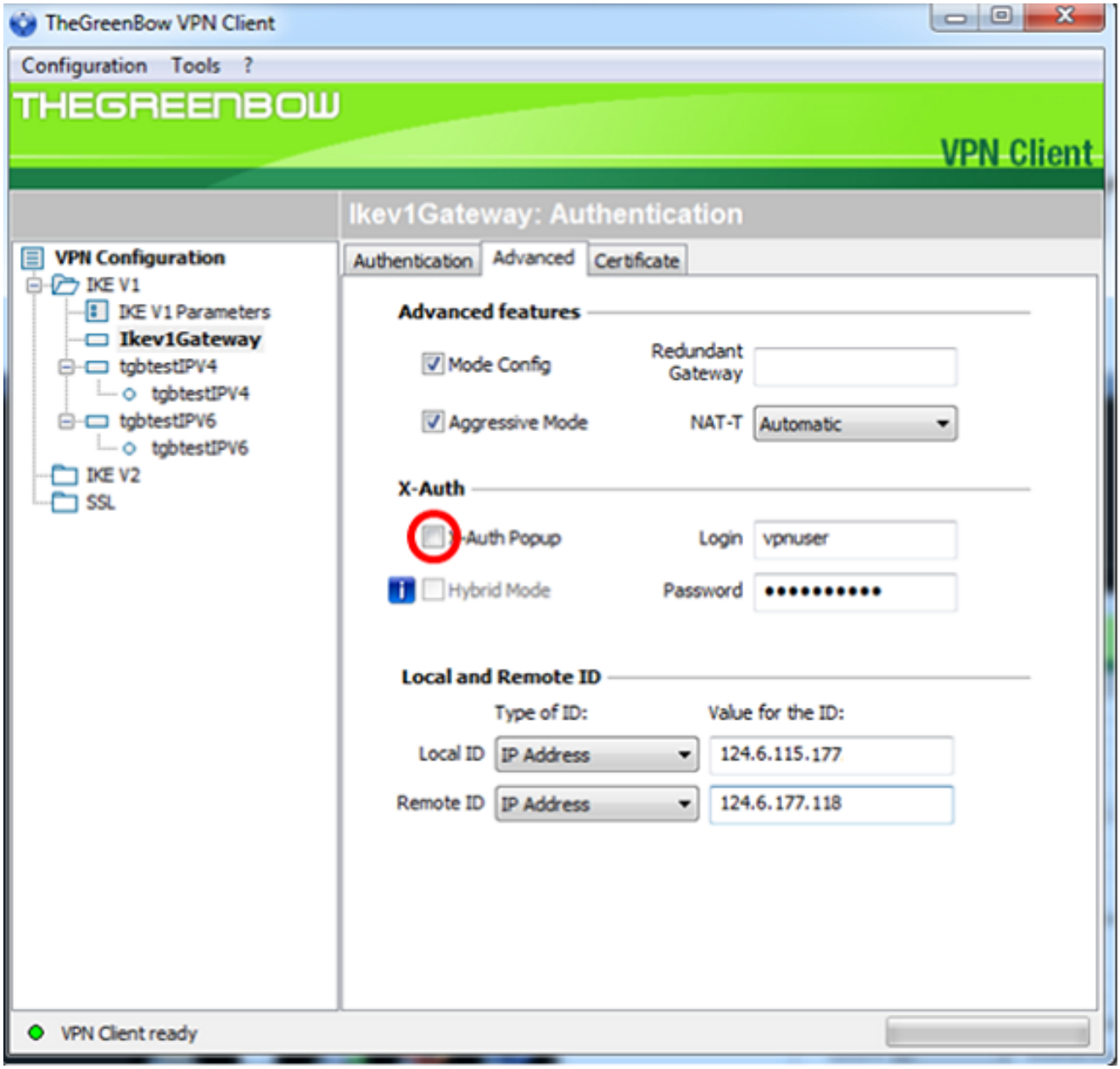


10단계(선택 사항) Advanced features(고급 기능)에서 **Mode Config** and **Aggressive Mode(모드 컨피그레이션** 및 **적극적인 모드**) 확인란을 선택하고 NAT-T 설정을 Automatic(자동)으로 설정합니다.



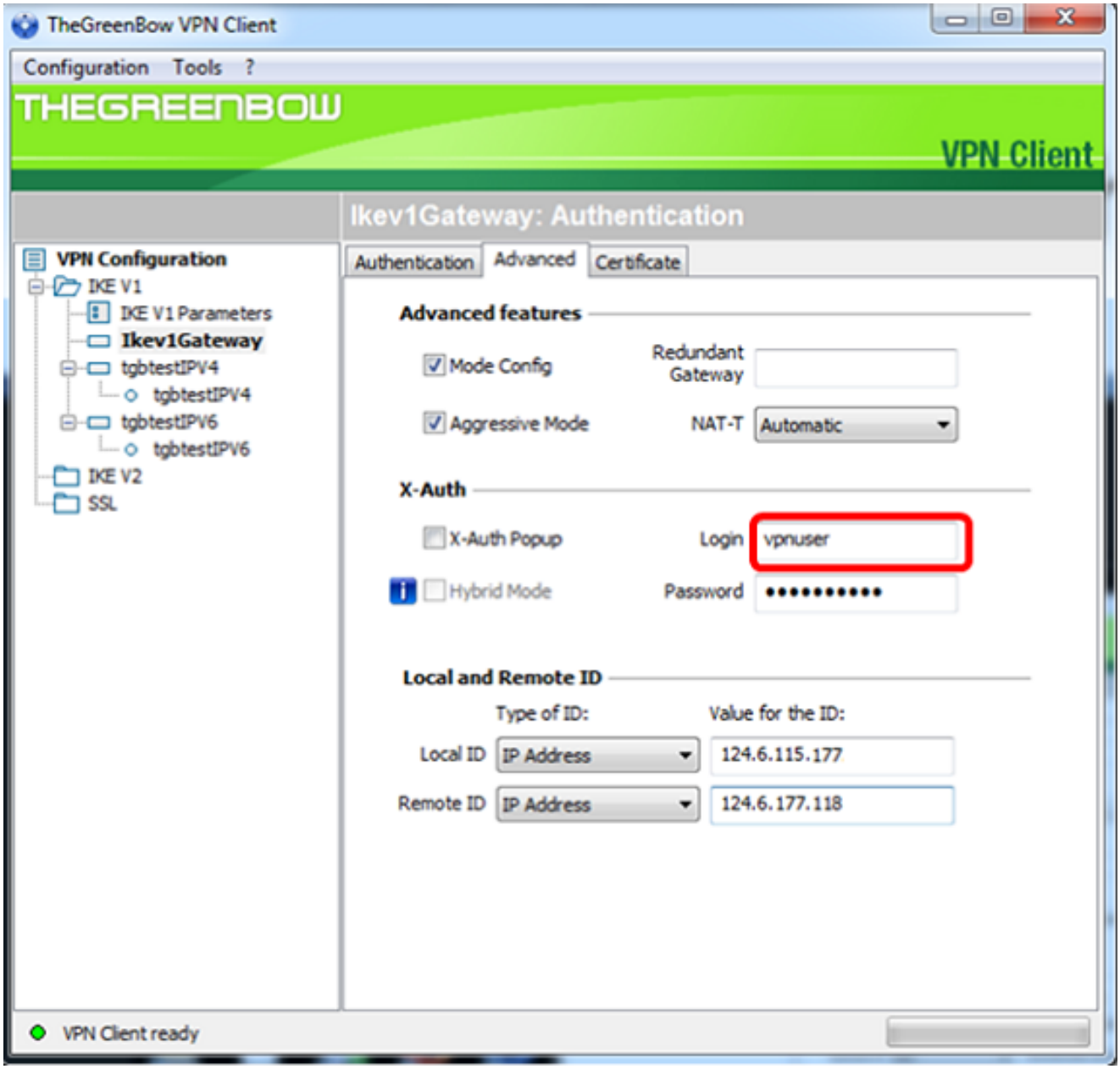
참고: Mode Config(모드 컨피그레이션)를 활성화하면 GreenBow VPN Client는 VPN 게이트웨이에서 설정을 가져와 터널 설정을 시도하는 동시에 Aggressive Mode(적극적인 모드) 및 NAT-T를 활성화하여 연결을 더 빠르게 설정합니다.

11단계(선택 사항) X-Auth 아래에서 연결을 시작할 때 로그인 창을 자동으로 당겨받으려면 **X-Auth Popup** 확인란을 선택합니다.로그인 창에서는 사용자가 터널을 완료할 수 있도록 자격 증명을 입력합니다.

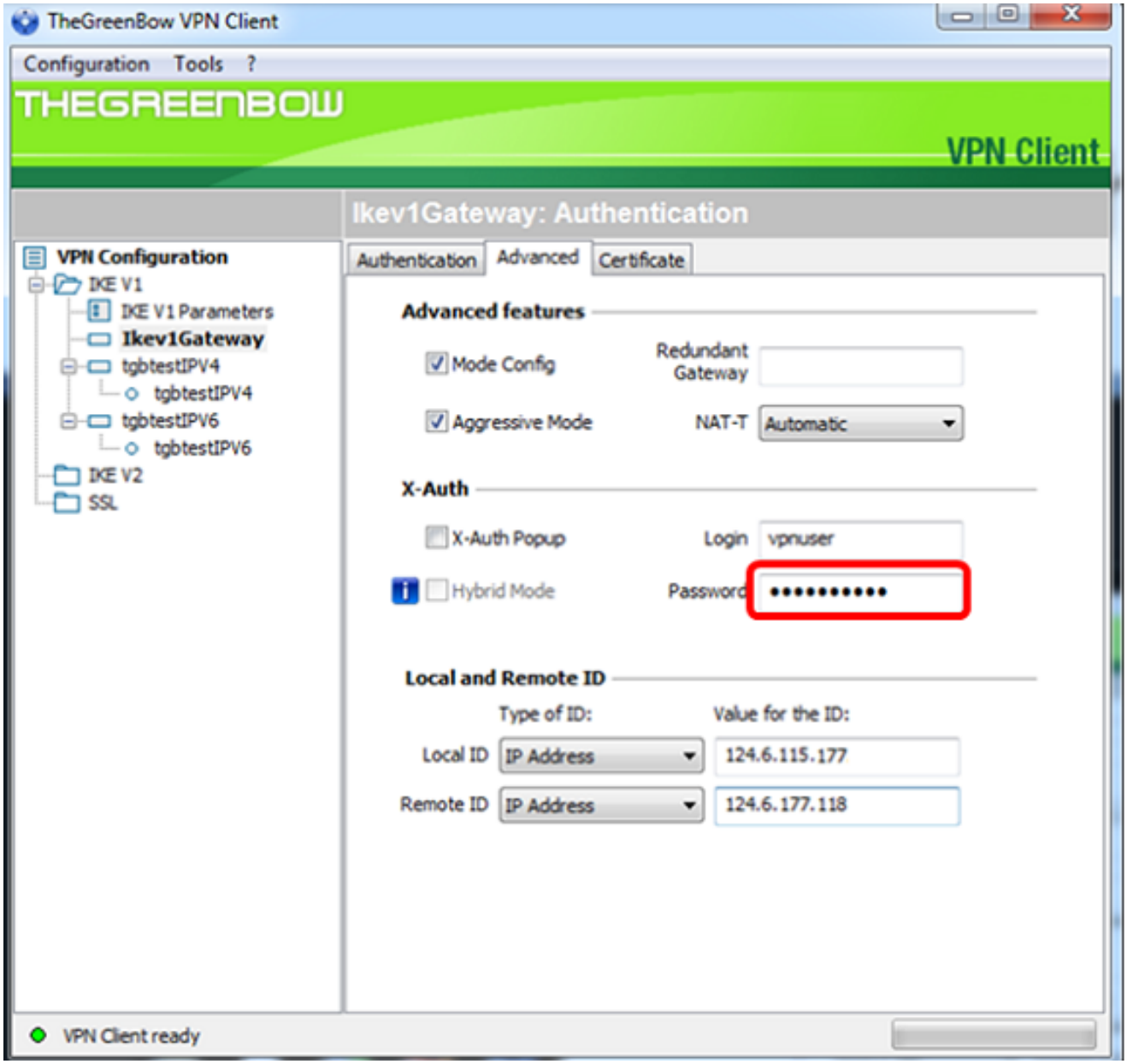


참고:이 예에서는 X-Auth Popup(X-인증 팝업)이 선택되어 있지 않습니다.

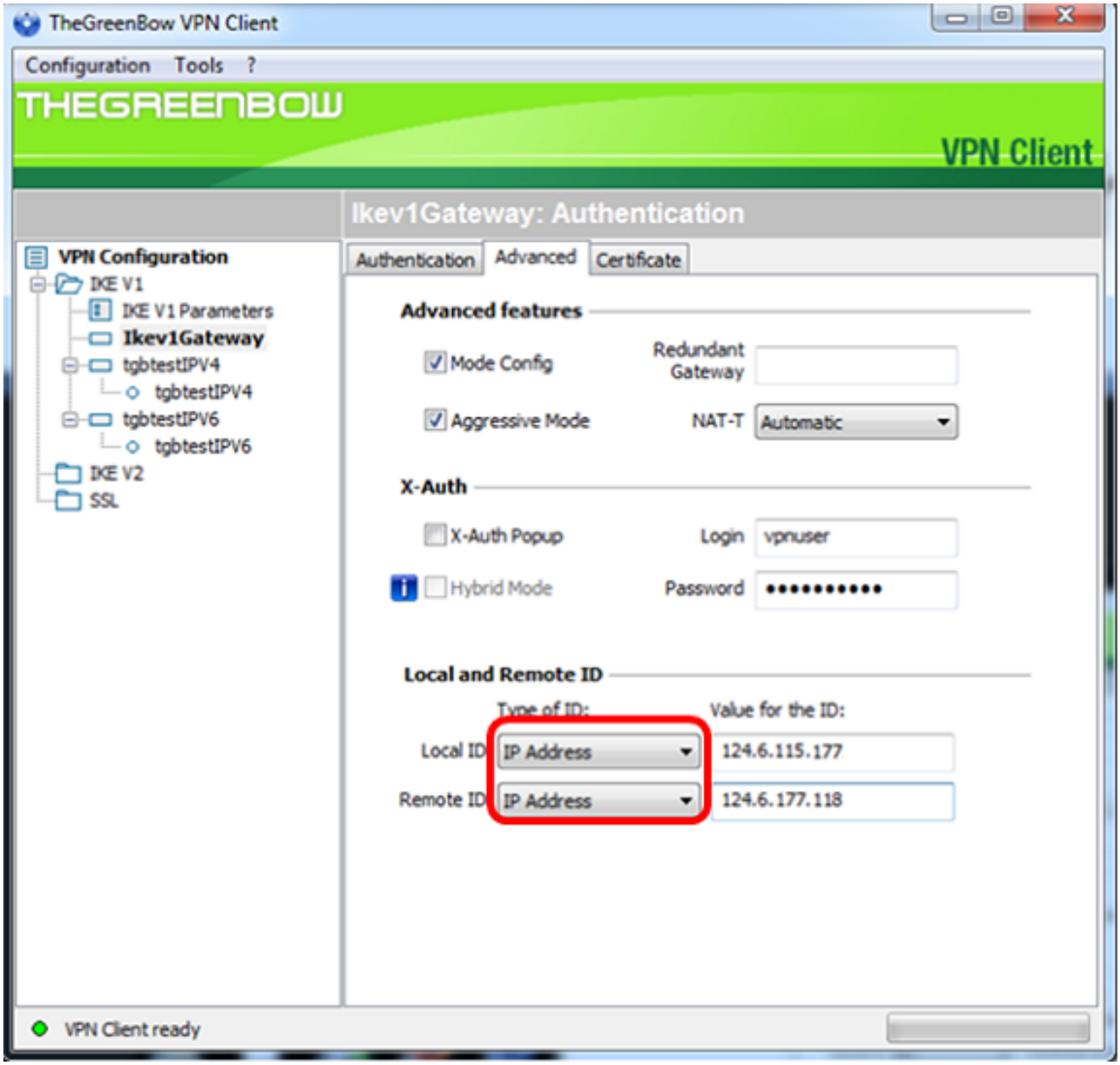
12단계. *Login* 필드에 사용자 이름을 입력합니다.VPN 게이트웨이에서 사용자 그룹을 생성하도록 구성된 사용자 이름입니다.



13단계. *비밀번호* 필드에 비밀번호를 입력합니다.

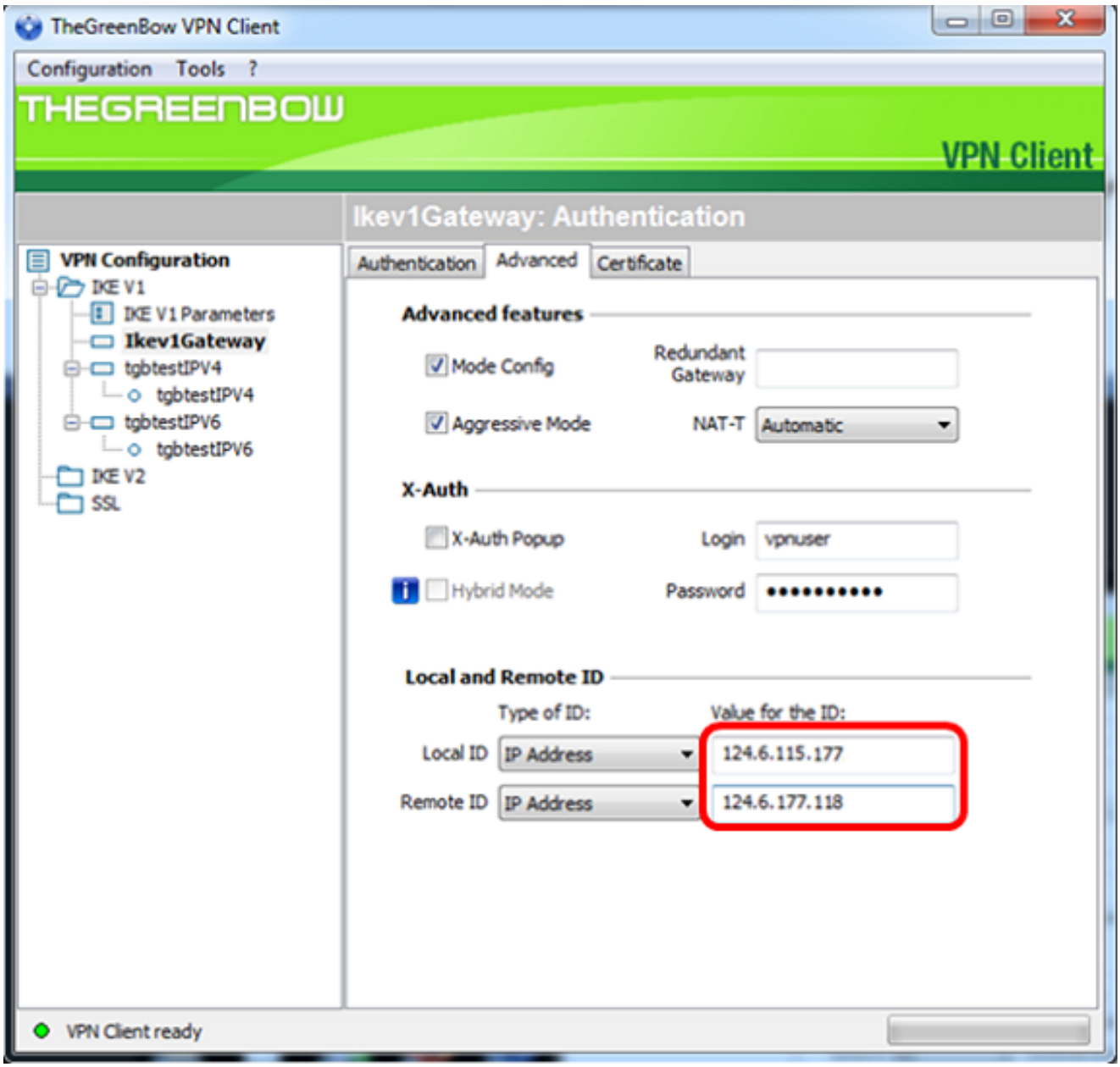


14단계. Local and Remote ID(로컬 및 원격 ID)에서 Local ID(로컬 ID) 및 Remote ID를 VPN 게이트웨이의 설정과 일치하도록 설정합니다.

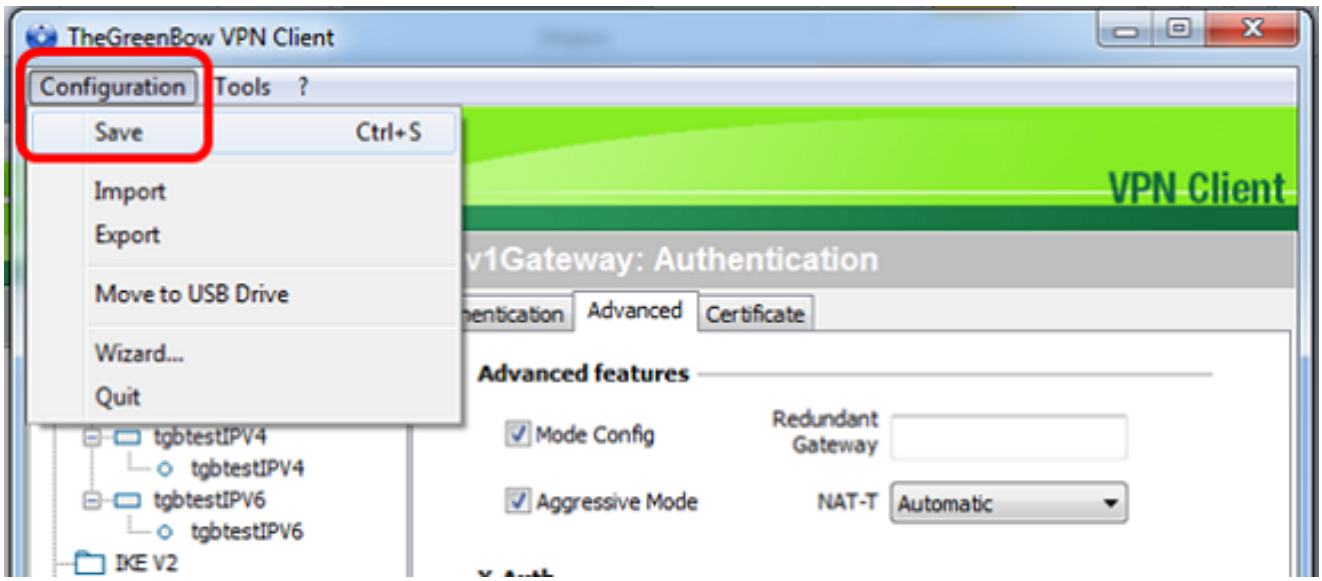


참고:이 예에서는 RV34x VPN 게이트웨이의 설정과 일치하도록 로컬 ID와 원격 ID가 모두 IP 주소로 설정됩니다.

15단계. ID의 Value(값)에서 각 필드에 로컬 ID와 원격 ID를 입력합니다.

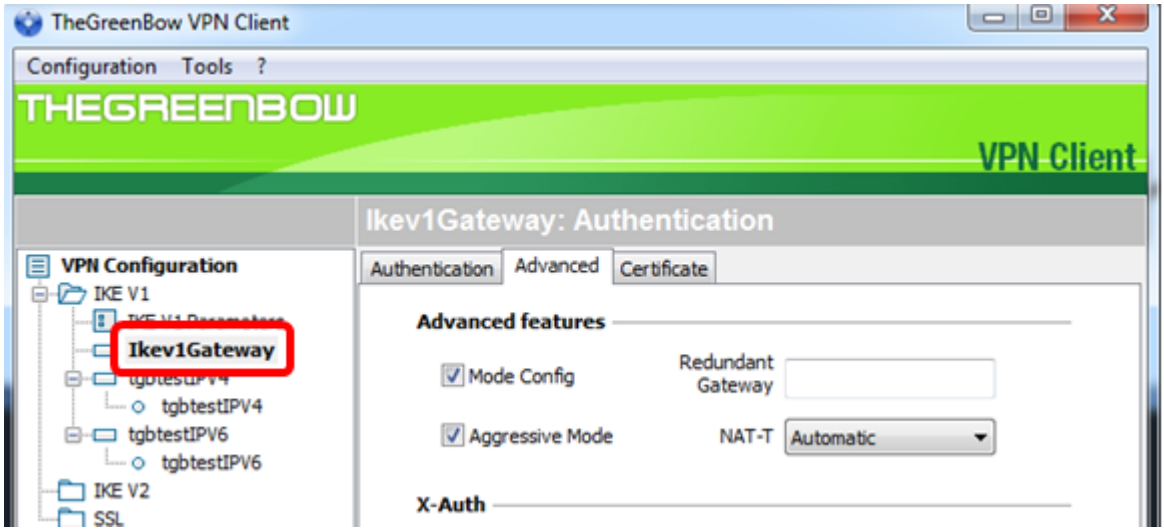


16단계. Configuration(컨피그레이션) > **Save(저장)**를 클릭하여 설정을 저장합니다.

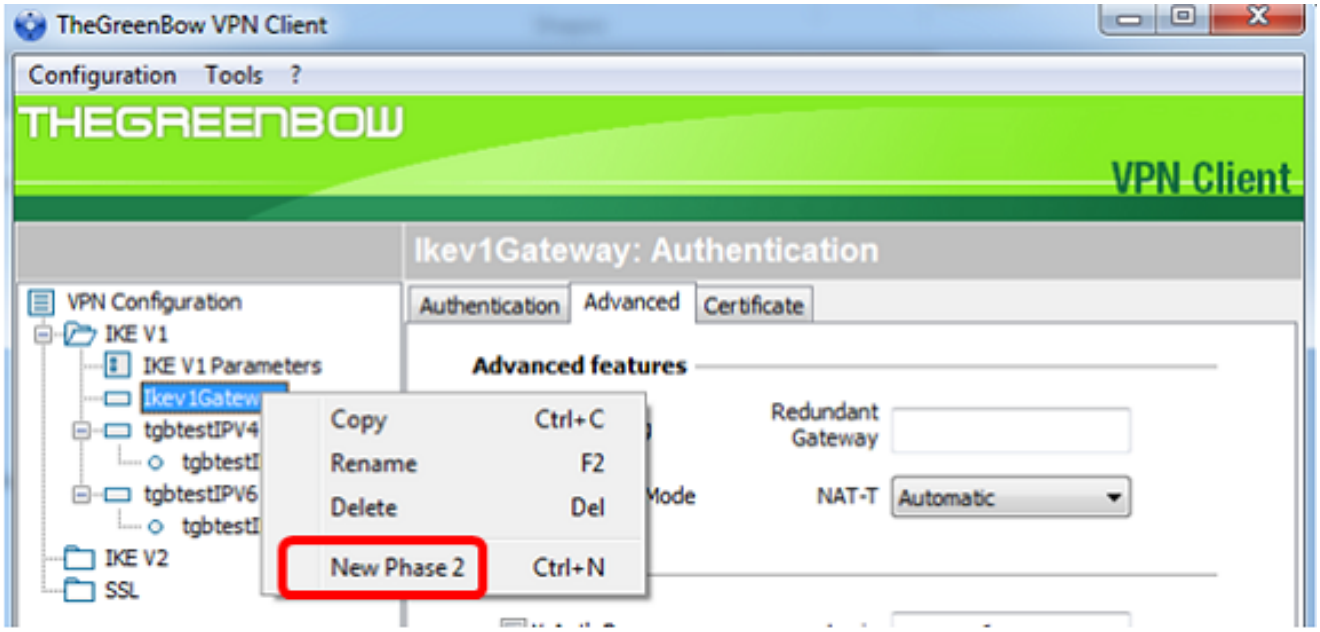


2단계 설정 구성

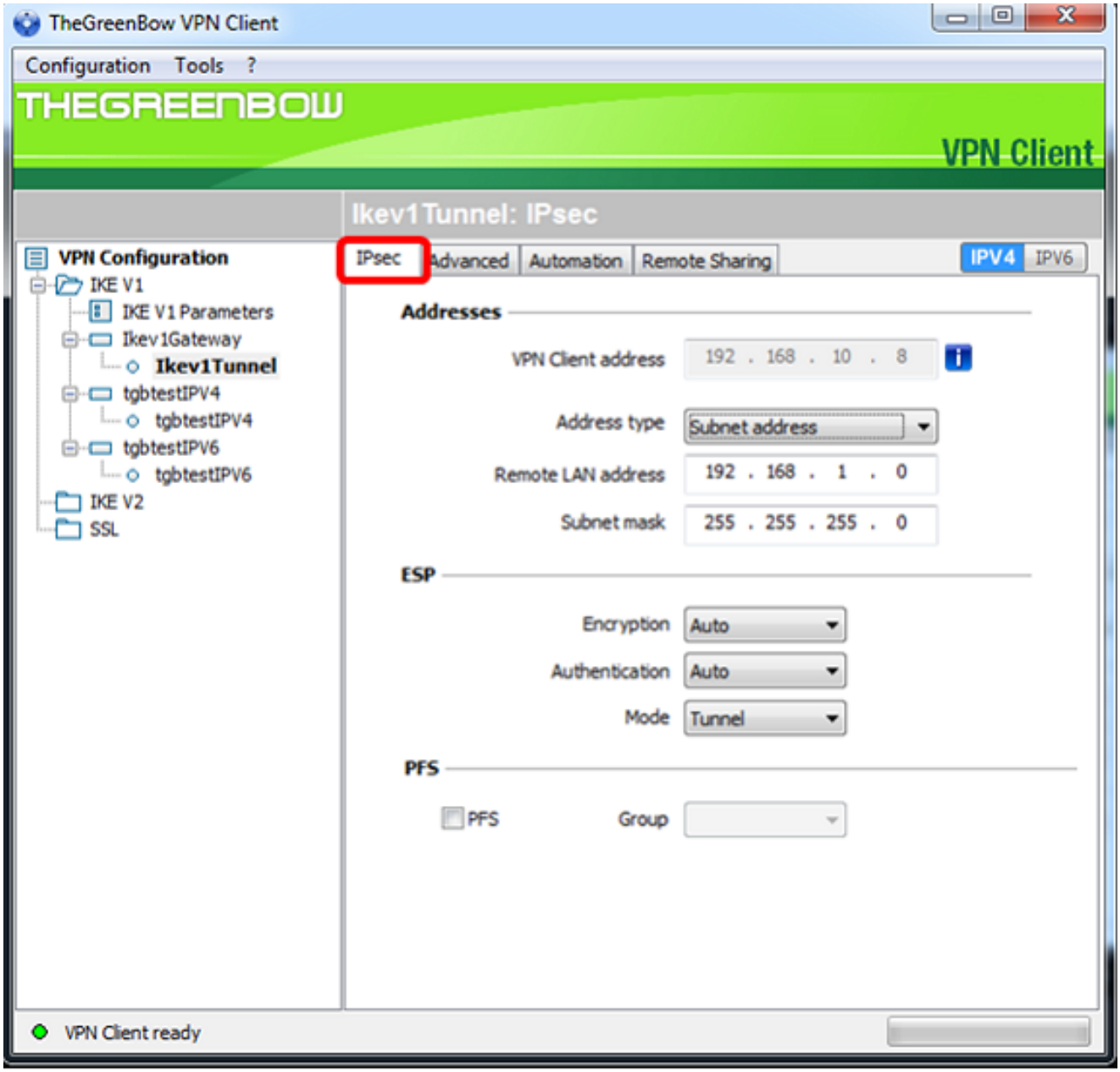
1단계. Ikev1 Gateway를 마우스 오른쪽 단추로 클릭합니다.



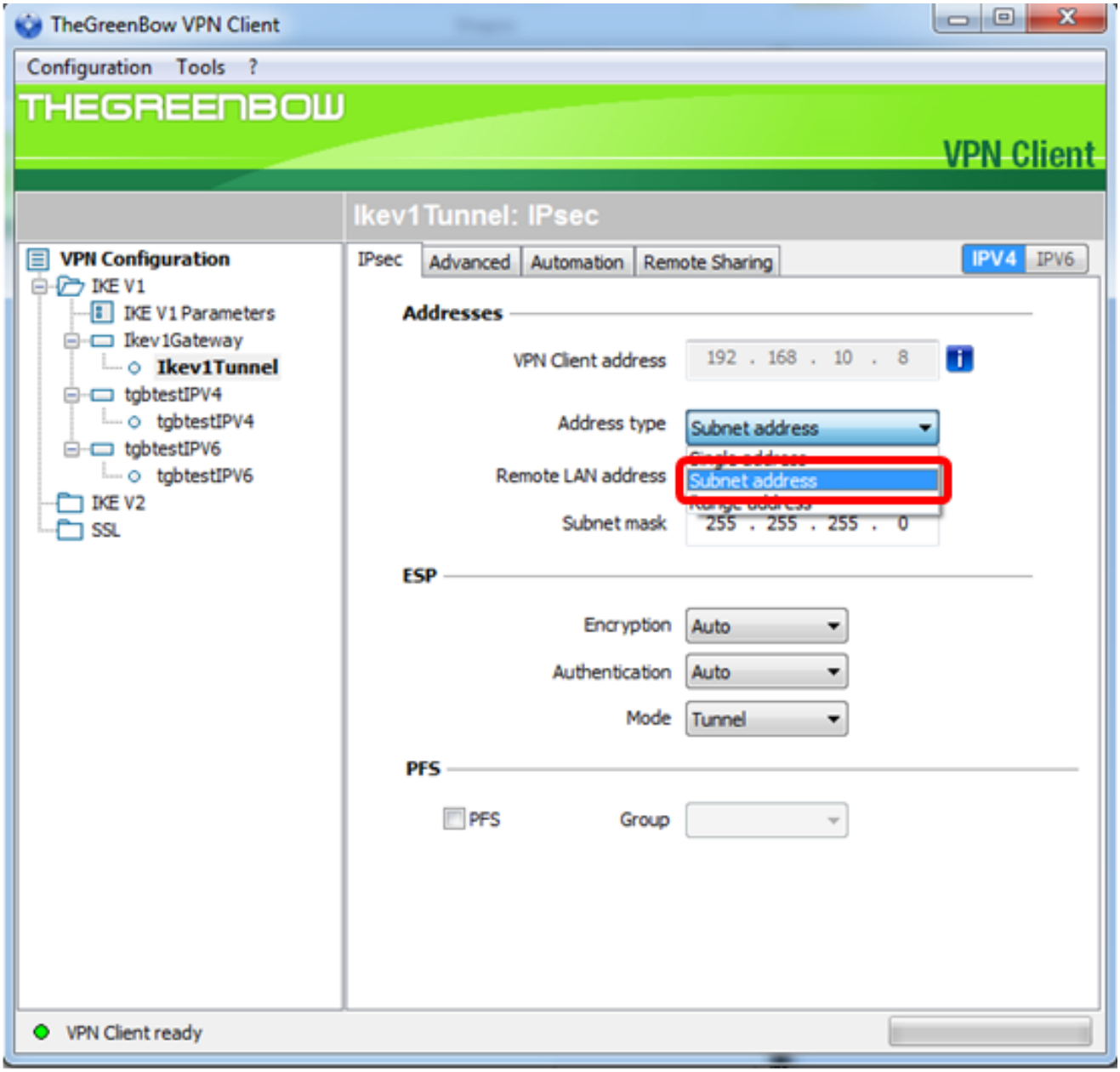
2단계. 새 단계 2를 선택합니다.



3단계. IPsec 탭을 클릭합니다.

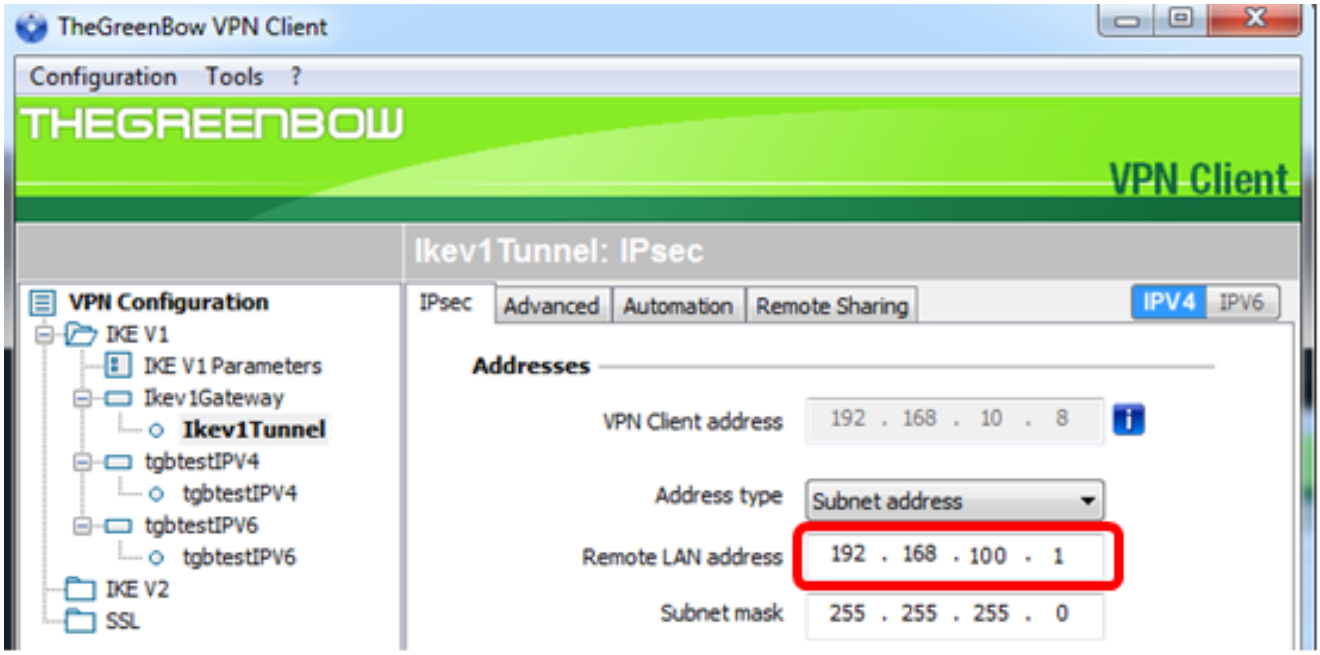


4단계. Address type(주소 유형) 드롭다운 목록에서 VPN 클라이언트가 액세스할 수 있는 주소 유형을 선택합니다.



참고:이 예에서는 서브넷 주소가 선택됩니다.

5단계. VPN 터널에서 액세스해야 하는 네트워크 주소를 *Remote LAN address* 필드에 입력합니다.

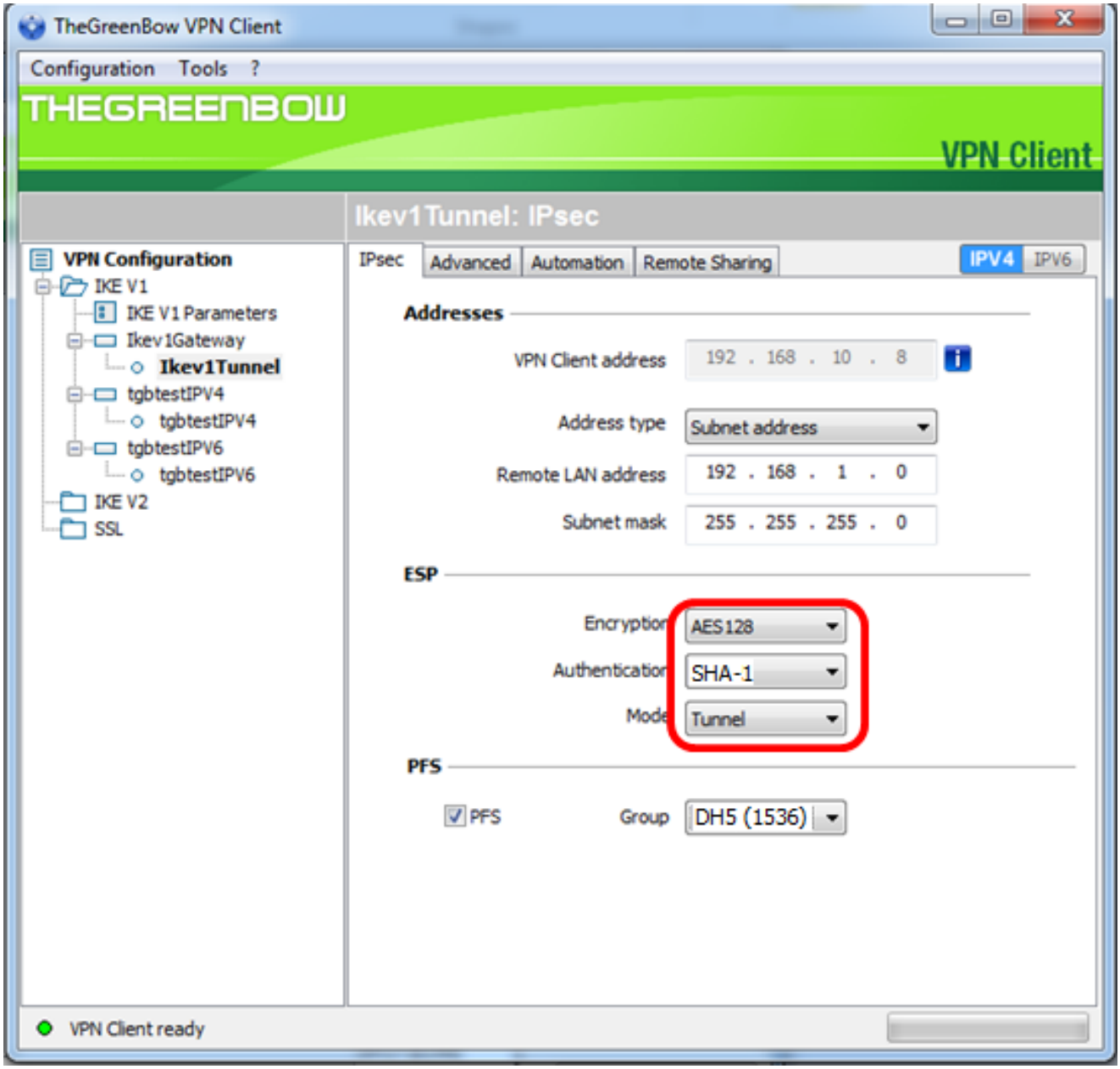


참고:이 예에서는 192.168.100.1을 입력합니다.

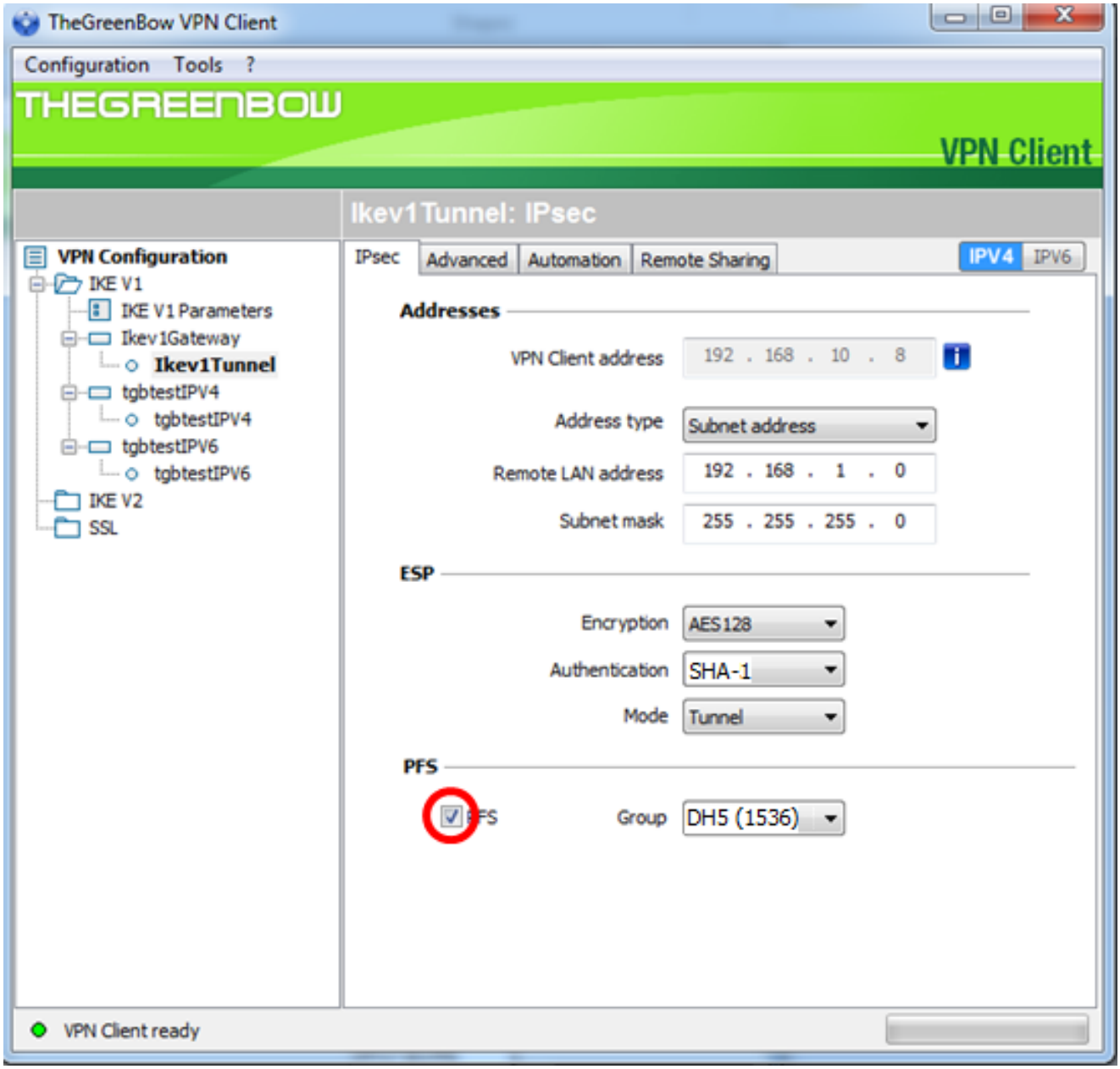
6단계. Subnet mask(서브넷 마스크) 필드에 원격 네트워크의 서브넷 마스크를 입력합니다.

참고:이 예에서는 255.255.255.0을 입력합니다.

7단계. ESP에서 VPN 게이트웨이의 설정과 일치하도록 암호화, 인증 및 모드를 설정합니다.

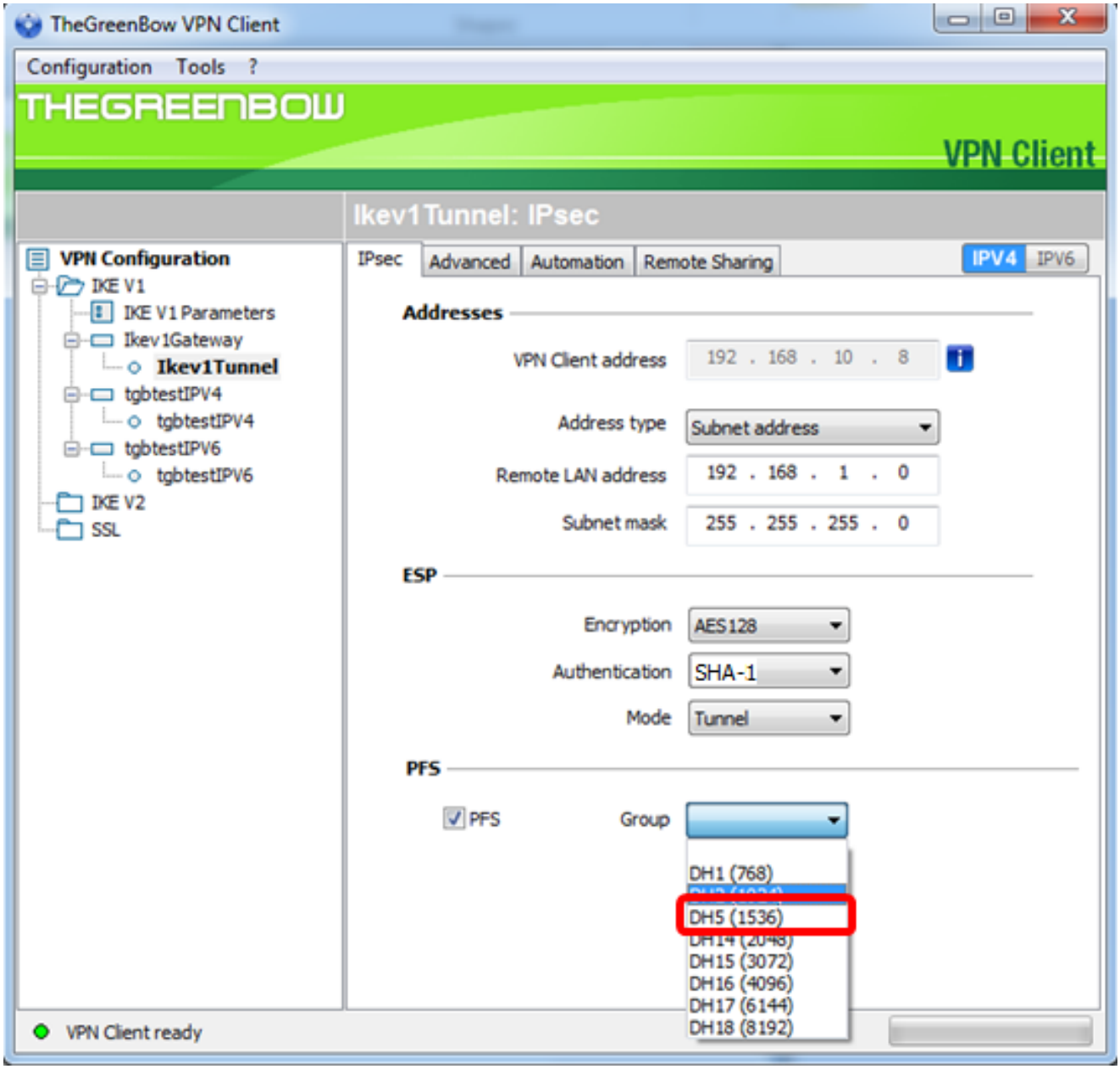


8단계(선택 사항) PFS 아래에서 PFS(Perfect Forward Secrecy)를 활성화하려면 **PFS** 확인란을 선택합니다.PFS는 세션을 암호화하기 위해 임의 키를 생성합니다.

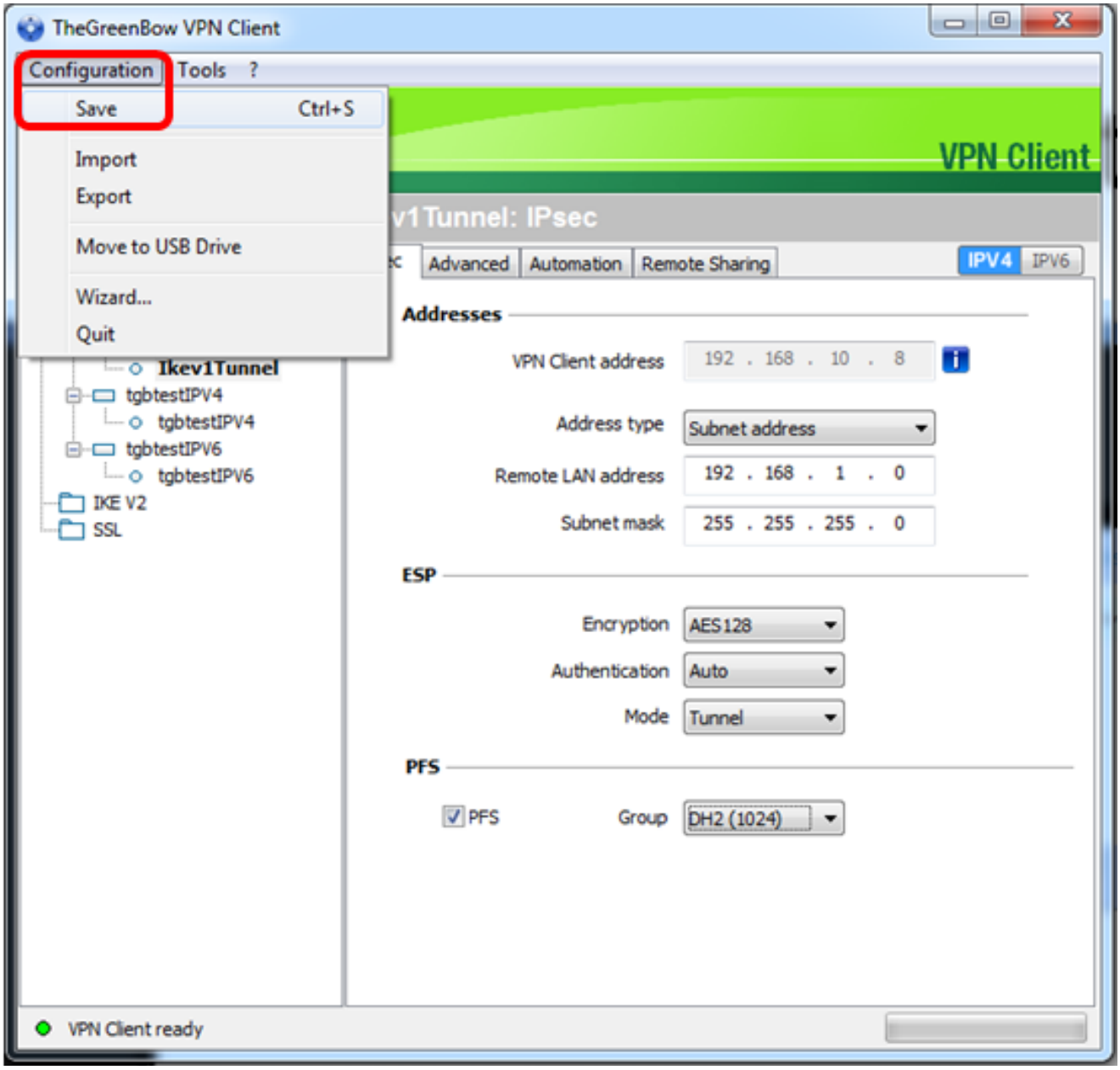


9단계. Group(그룹) 드롭다운 목록에서 PFS 그룹 설정을 선택합니다.

참고:이 예에서는 라우터의 DH 그룹 설정과 일치하도록 DH5(1536)를 선택합니다.



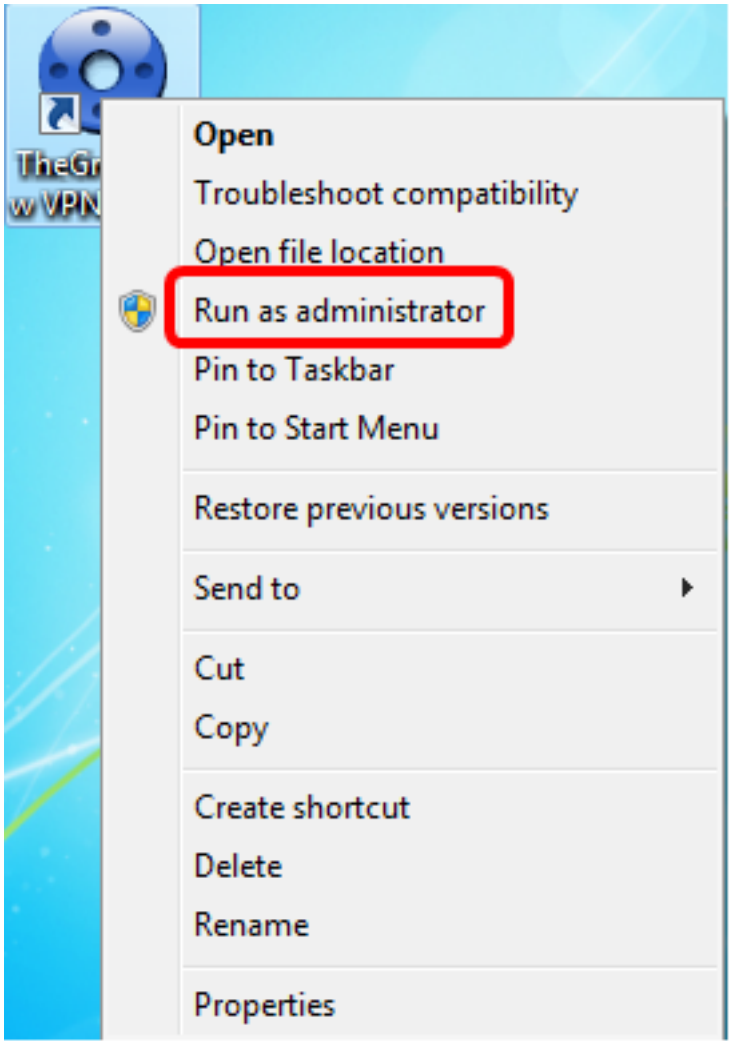
10단계. Configuration(컨피그레이션)을 마우스 오른쪽 버튼으로 클릭하고 **Save(저장)**를 선택합니다.



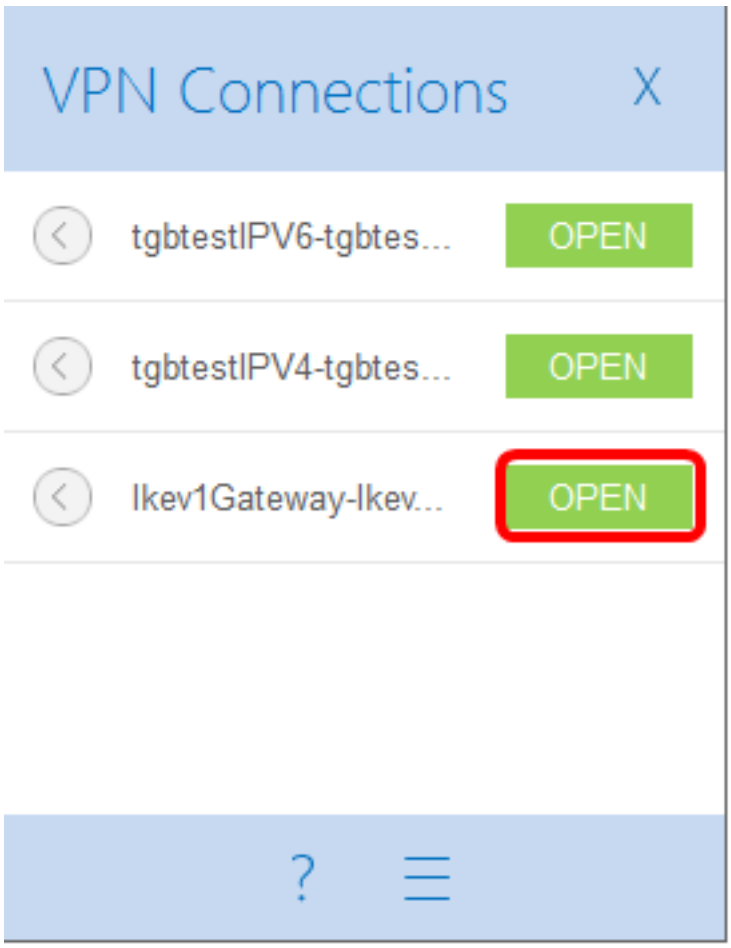
이제 VPN을 통해 RV34x Series 라우터에 연결하도록 TheGreenBow VPN Client를 성공적으로 구성해야 합니다.

VPN 연결 시작

1단계. TheGreenBow VPN Client(GreenBow VPN 클라이언트)를 마우스 오른쪽 버튼으로 클릭하고 Run as **administrator(관리자로 실행)**를 선택합니다.



2단계. 사용해야 하는 VPN 연결을 선택한 다음 **OPEN**을 클릭합니다.VPN 연결이 자동으로 시작됩니다.

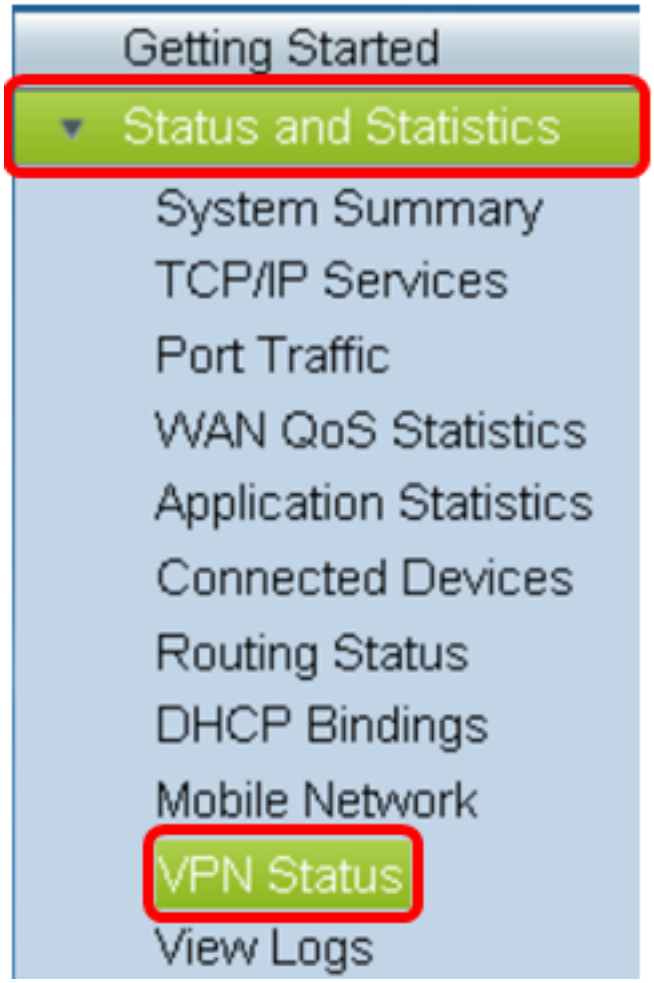


참고:이 예에서는 구성된 Ikev1Gateway를 선택했습니다.

VPN 상태 확인

1단계. 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.

참고:이 예에서는 하나의 VPN 연결이 설정되었습니다.

이제 RV34x Series Router에서 VPN 연결 상태를 확인했습니다.이제 GreenBow VPN Client가 VPN을 통해 라우터에 연결되도록 구성됩니다.