RV320 및 RV325 VPN Router Series에서 Group Client to Gateway Virtual Private Network(VPN) 구성

목표

VPN(가상 사설망)은 보안을 제공하기 위해 공용 네트워크를 통해 원격 사용자의 장치를 가상으로 연결하는 데 사용되는 사설 네트워크입니다. VPN 유형 중 하나는 클라이언트-게이트웨이 VPN입니다.Client-to-Gateway를 사용하면 서로 다른 지역에 위치한 회사의 서로 다른 지사를 원격으로 연결하여 해당 영역 간에 데이터를 보다 안전하게 전송하고 수신할 수 있습니다.그룹 VPN은 각 사용자에 대한 VPN 컨피그레이션을 제거하므로 VPN을 쉽게 구성할 수 있습니다.RV32x VPN Router Series는 최대 2개의 VPN 그룹을 지원할 수 있습니다.

이 문서의 목적은 RV32x Series VPN Router에서 게이트웨이 VPN에 대한 그룹 클라이언트를 구성하는 방법을 설명하는 것입니다.

적용 가능한 디바이스

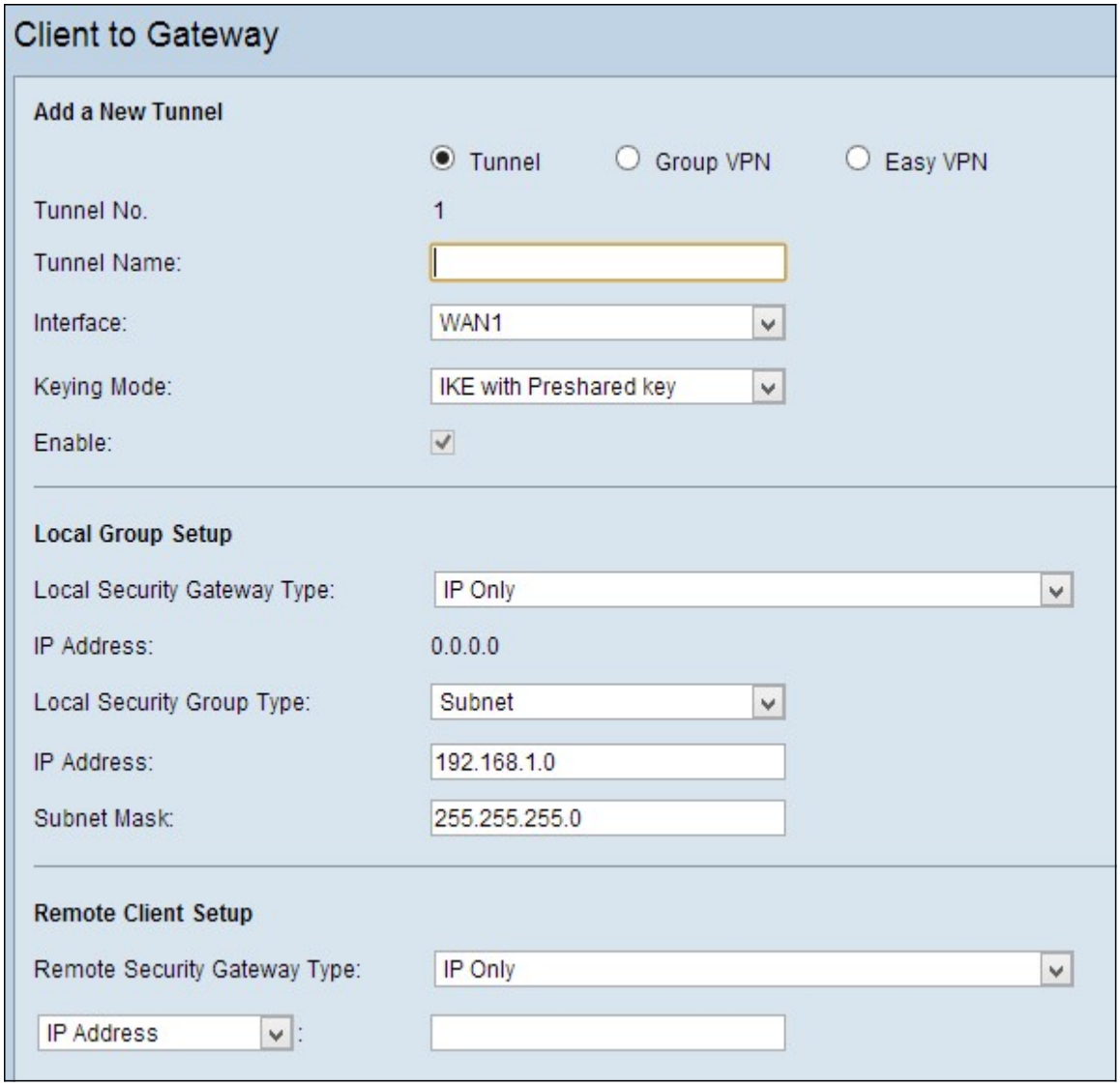
·RV320 Dual WAN VPN Router
· RV325 Gigabit Dual WAN VPN Router

소프트웨어 버전

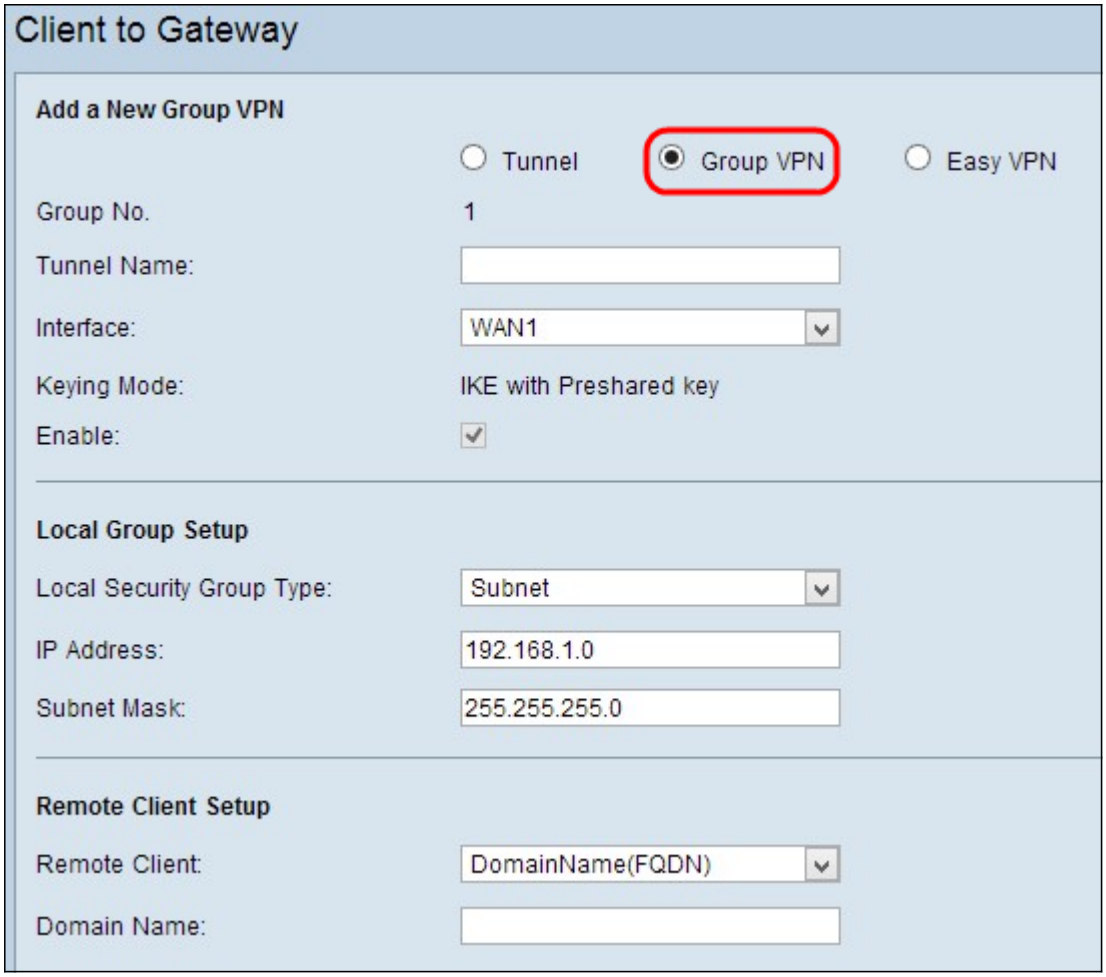
·v1.1.0.09

그룹 클라이언트에서 게이트웨이 VPN으로 구성

1단계. 라우터 컨피그레이션 유틸리티에 로그인하고 **VPN > Client to Gateway**를 선택합니다.Client to *Gateway(클라이언트-게이트웨이)* 페이지가 열립니다.

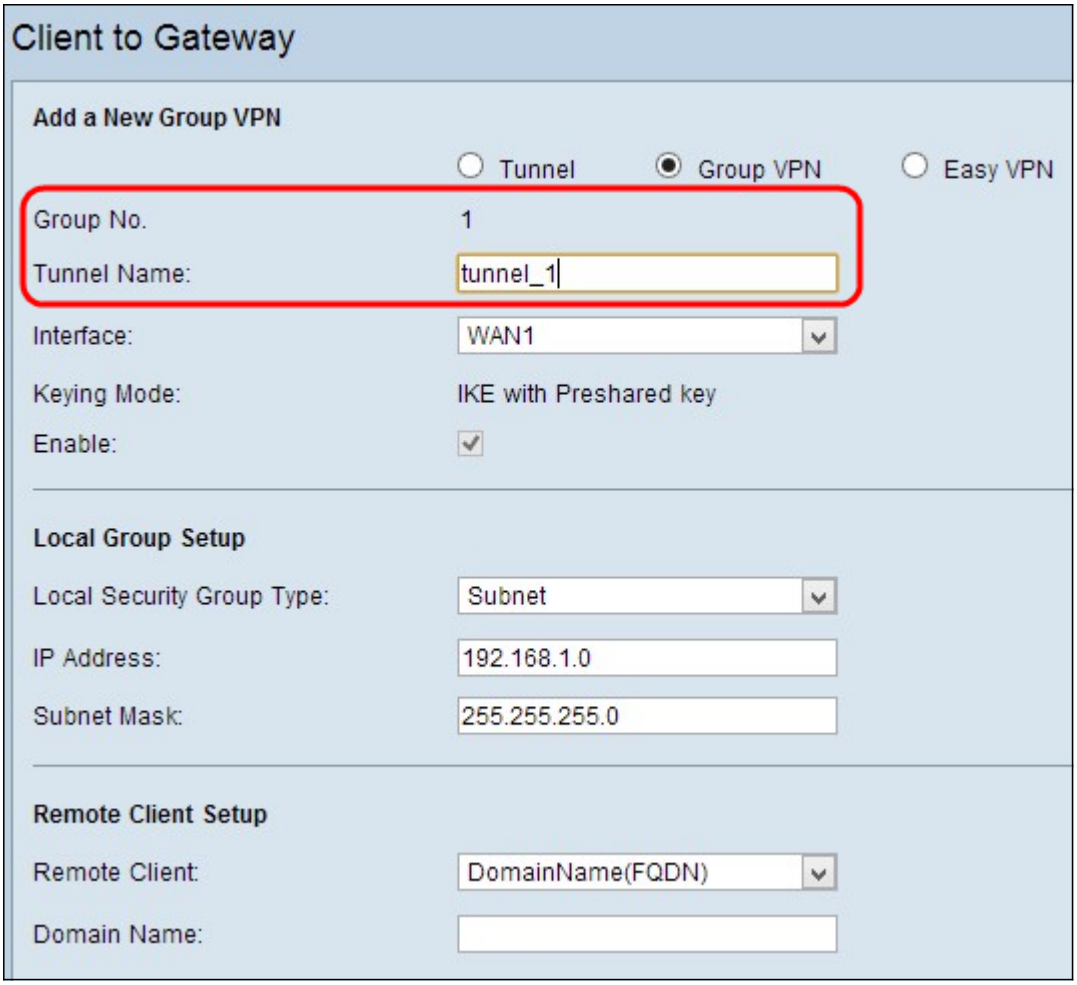


2단계. Group **VPN** 라디오 버튼을 클릭하여 그룹 클라이언트-게이트웨이 VPN을 추가합니다.



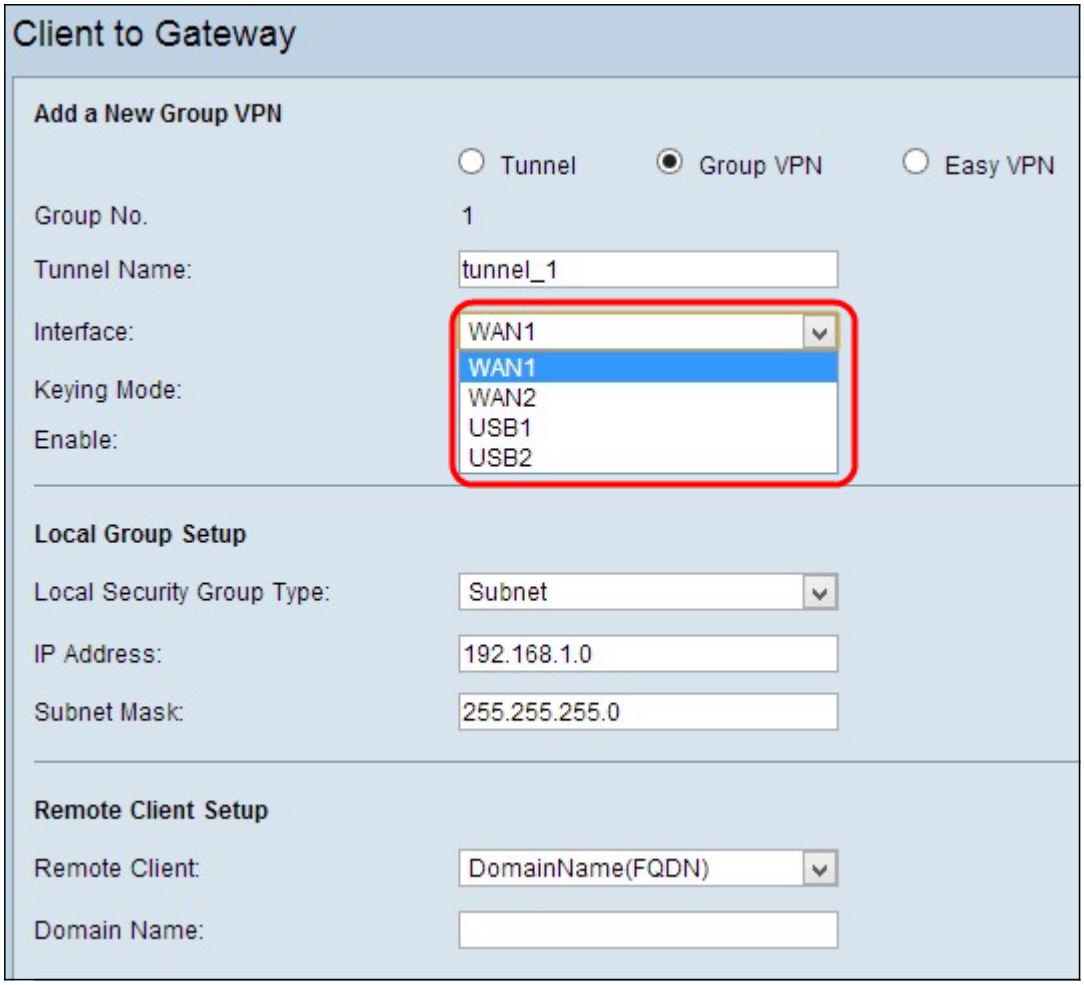
새 터널 추가

1단계. Tunnel *Name* 필드에 터널 이름을 입력합니다.

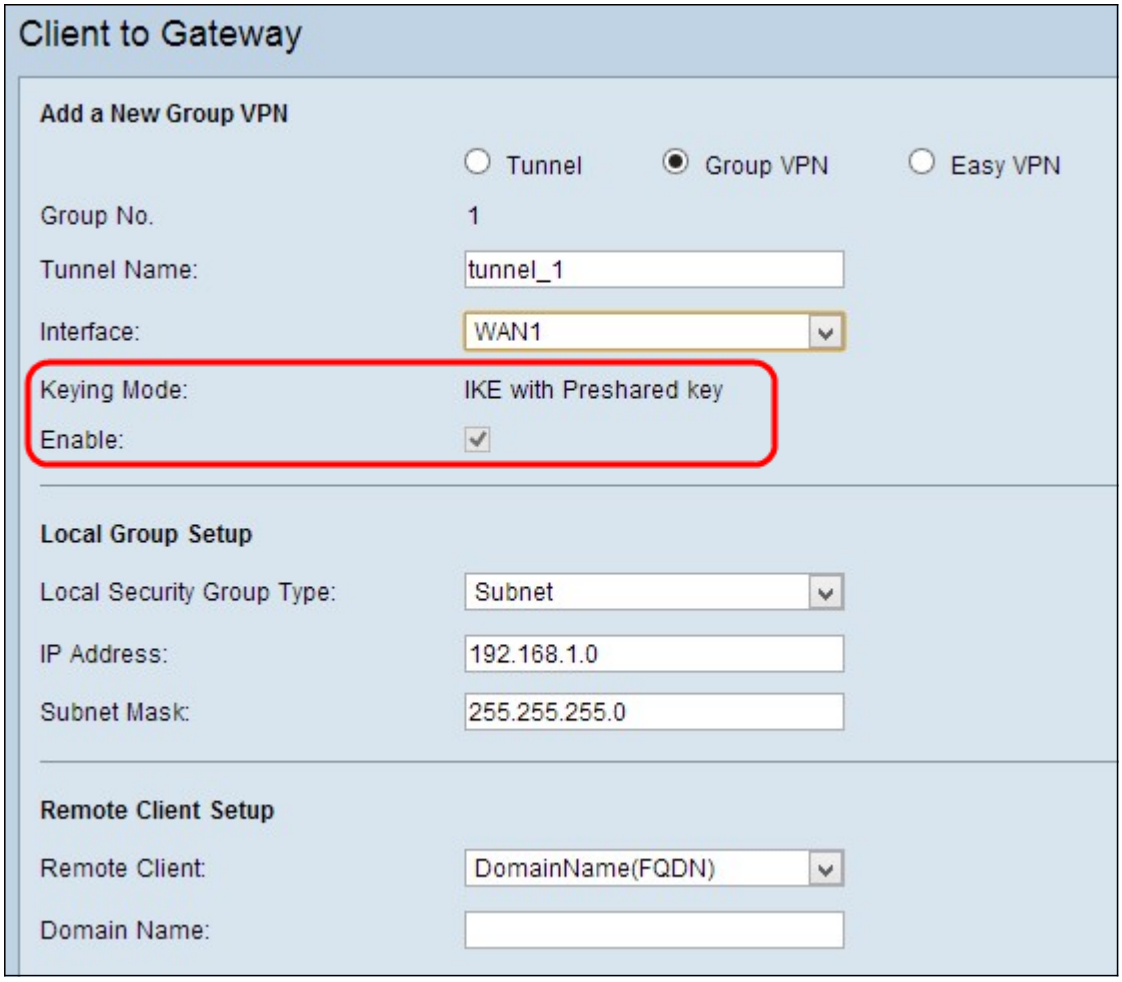


참고: Group No - 그룹 번호를 나타냅니다.자동 생성 필드입니다.

2단계. Interface 드롭다운 목록에서 VPN 그룹이 게이트웨이와 연결되는 적절한 인터페이스를 선택합니다.



3단계. Enable(**활성화**) 확인란을 선택하여 게이트웨이 간 VPN을 활성화합니다.기본적으로 활성화되어 있습니다.

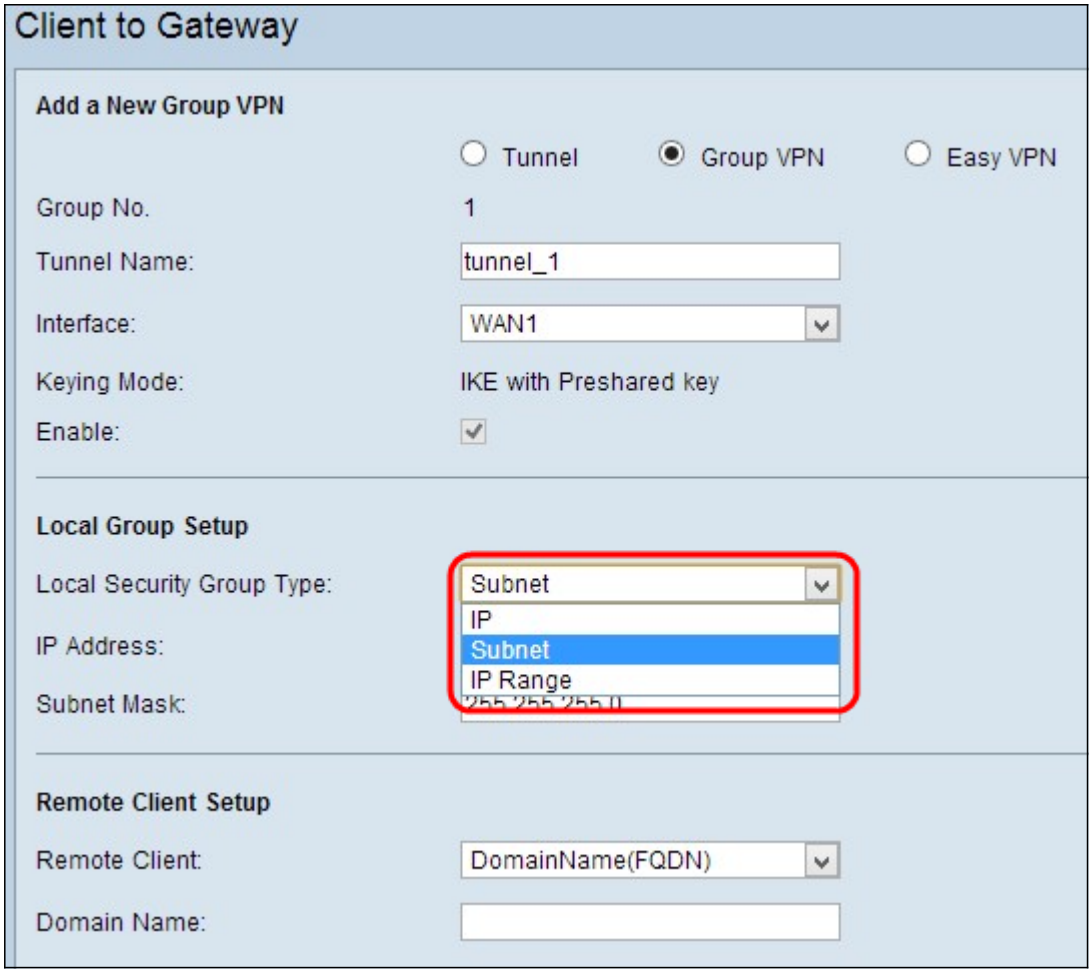


참고:키 지정 모드 - 사용된 인증 모드를 표시합니다.IKE with Preshared key(사전 공유 키가 있는 IKE가 유일한 옵션입니다. 즉, IKE(Internet Key Exchange) 프로토콜을 사용하여 터널에 대해 인증된 통신을 설정하기 위해 사전 공유 키를 자동으로 생성하고 교환합니다.

4단계. 지금까지 설정한 설정을 저장하고 나머지는 기본값으로 두려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

로컬 그룹 설정

1단계. *Local Security Group Type* 드롭다운 목록에서 VPN 터널에 액세스할 수 있는 적절한 로컬 LAN 사용자 또는 사용자 그룹을 선택합니다.기본값은 서브넷입니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

·IP — 하나의 특정 LAN 디바이스만 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *IP Address* 필드에 LAN 디바이스의 IP 주소를 입력합니다.기본 IP는 192.168.1.0입니다.

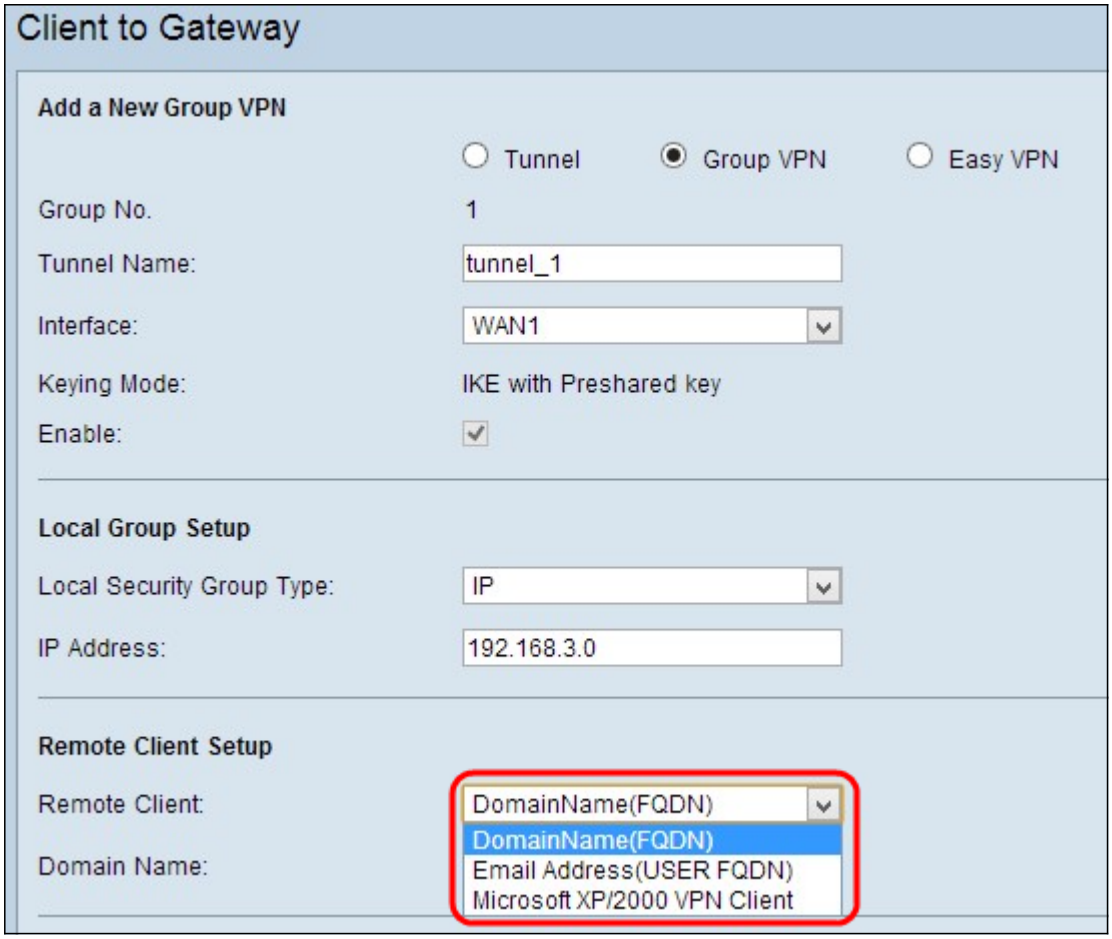
·서브넷 — 특정 서브넷의 모든 LAN 디바이스는 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 LAN 디바이스의 IP 주소와 서브넷 마스크를 *IP Address* 및 *Subnet Mask* 필드에 각각 입력합니다.기본 마스크는 255.255.255.0입니다.

·IP 범위 — 다양한 LAN 디바이스가 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *Start IP* 및 *End IP* 필드에 범위의 첫 번째 및 마지막 IP 주소를 각각 입력합니다.기본 범위는 192.168.1.0~192.168.1.254입니다.

2단계. 지금까지 설정한 설정을 저장하고 나머지는 기본값으로 두려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

원격 클라이언트 설정

1단계. *Remote Security Group Type* 드롭다운 목록에서 VPN 터널에 액세스할 수 있는 적절한 원격 LAN 사용자 또는 사용자 그룹을 선택합니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

·FQDN(Domain Name) 인증 — 등록된 도메인을 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *Domain Name* 필드에 등록된 도메인의 이름을 입력합니다.

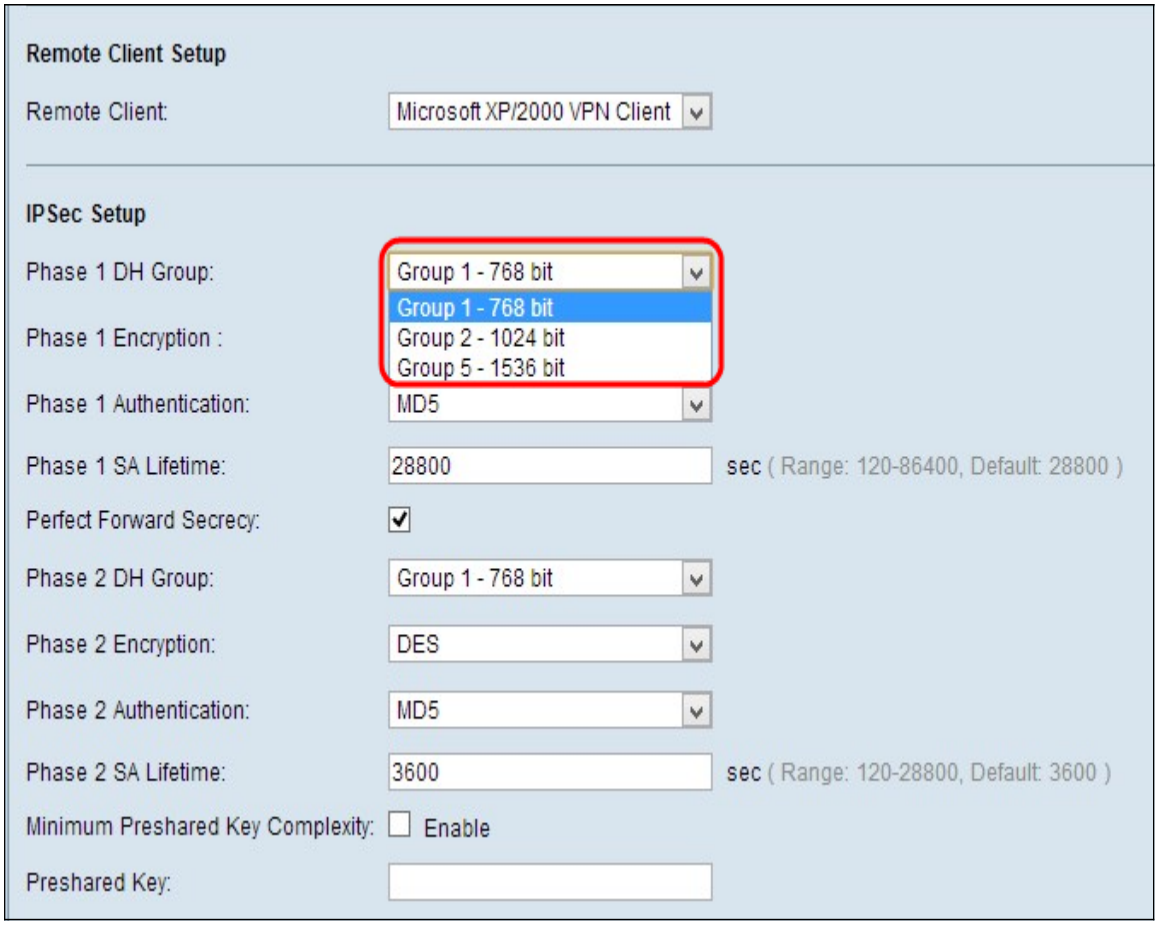
·이메일 주소(USER FQDN) 인증 — 이메일 주소를 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *Email Address* 필드에 이메일 주소를 입력합니다.

·Microsoft XP/2000 VPN 클라이언트 — Microsoft XP 또는 2000 VPN 클라이언트 소프트웨어가 내장된 클라이언트 소프트웨어를 통해 터널에 액세스할 수 있습니다.

2단계. 지금까지 설정한 설정을 저장하고 나머지는 기본값으로 두려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

IPSec 설정

1단계. *Phase 1 DH Group* 드롭다운 목록에서 적절한 DH(Diffie-Hellman) 그룹을 선택합니다.1단계는 안전한 인증 통신을 지원하기 위해 터널의 양쪽 끝 사이에 단방향 SA(논리적 보안 연결)를 설정하는 데 사용됩니다.Diffie-Hellman은 통신을 인증하기 위해 1단계 연결에서 비밀 키를 공유하는 데 사용되는 암호화 키 교환 프로토콜입니다.



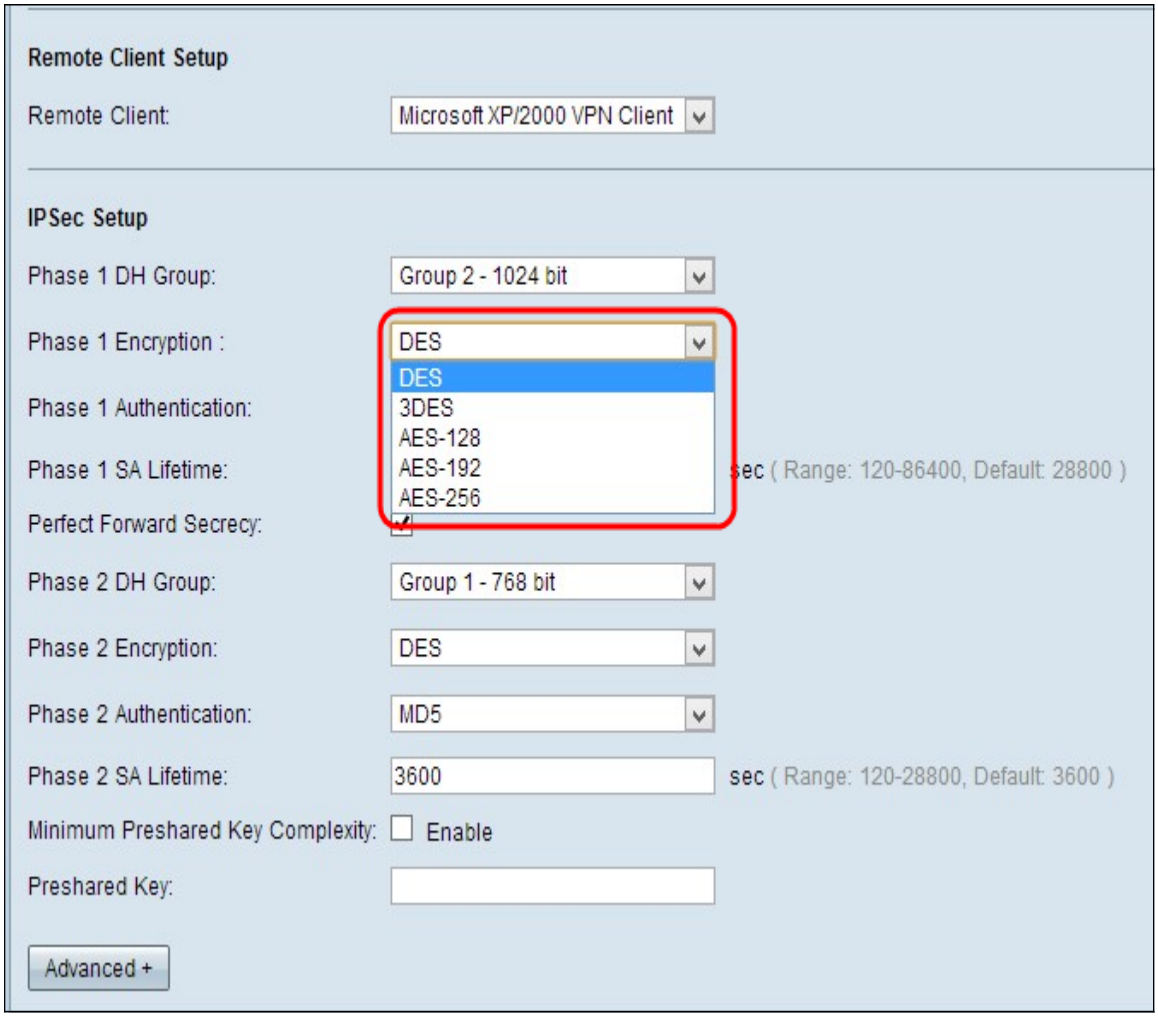
사용 가능한 옵션은 다음과 같이 정의됩니다.

·Group1(768비트) — 가장 빠르지만 가장 안전하지 않은 키를 계산합니다.

·Group2(1024비트) — 키를 느리게 계산하지만 Group1보다 안전합니다.

·Group5(1536비트) — 가장 느린 키를 계산합니다. 하지만 가장 안전합니다.

2단계. Phase *1 Encryption* 드롭다운 목록에서 키를 암호화하는 적절한 암호화 방법을 선택합니다.높은 보안 및 빠른 성능을 위해서는 AES-128이 권장됩니다. VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

·DES — DES(Data Encryption Standard)는 56비트 오래된 암호화 방법이며, 매우 안전한 암호화 방법은 아니지만 이전 버전과의 호환성을 위해 필요할 수 있습니다.

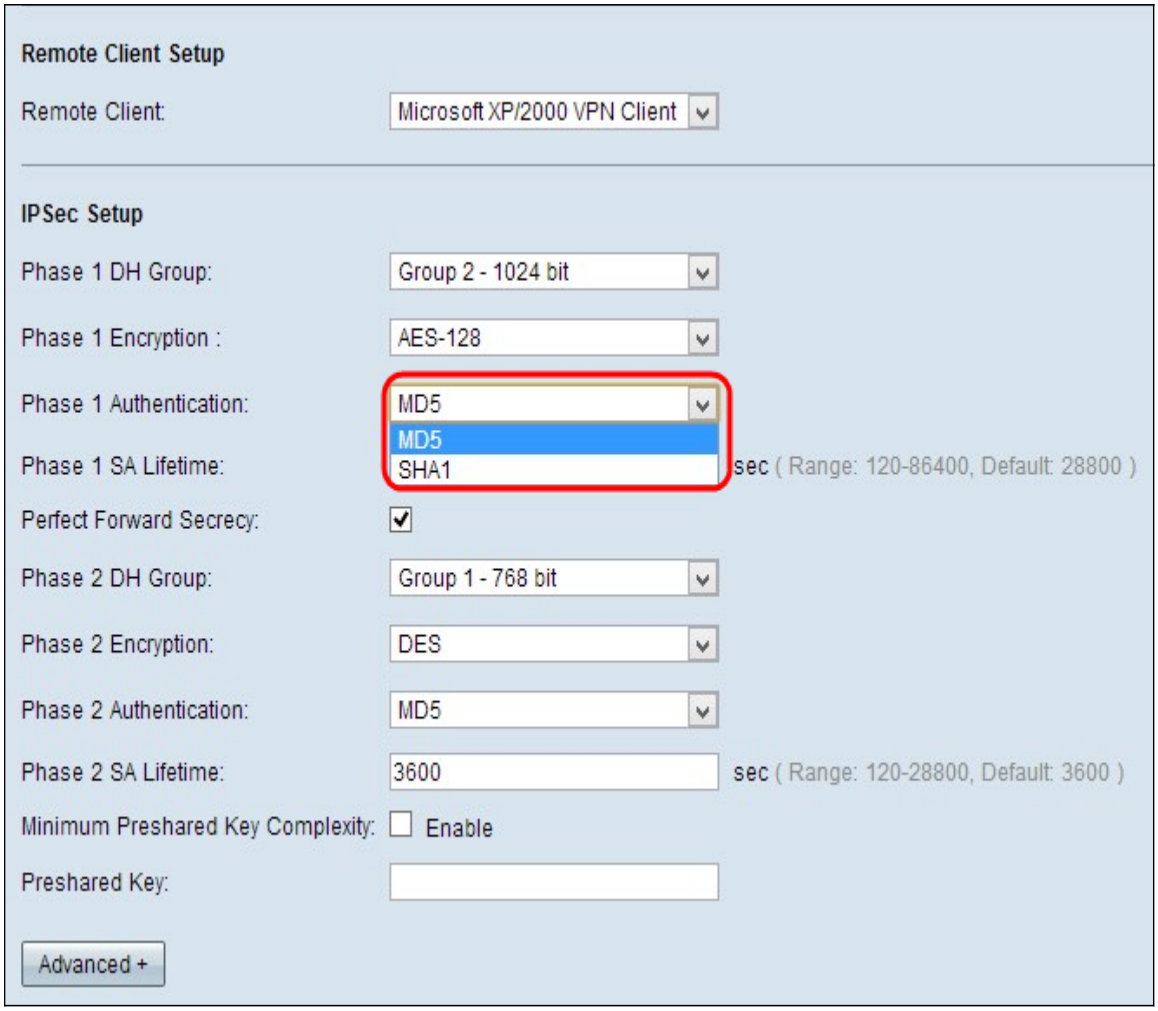
·3DES — 3DES(Triple Data Encryption Standard)는 데이터를 세 번 암호화하므로 키 크기를 늘리는 데 사용되는 168비트 간단한 암호화 방법입니다.이는 DES보다 더 많은 보안을 제공하지만 AES보다 적은 보안을 제공합니다.

·AES-128 — 128비트 키(AES-128)가 포함된 고급 암호화 표준은 AES 암호화를 위해 128비트 키를 사용합니다.AES는 DES보다 빠르고 안전합니다.일반적으로 AES는 3DES보다 빠르고 안전합니다.AES-128은 AES-192 및 AES-256보다 빠르지만 안전하지 않습니다.

·AES-192 — AES-192는 AES 암호화를 위해 192비트 키를 사용합니다.AES-192는 AES-128보다 느리지만 안전성이 높고 AES-256보다 빠르지만 보안성이 낮습니다.

·AES-256 — AES-256은 AES 암호화를 위해 256비트 키를 사용합니다.AES-256은 AES-128 및 AES-192보다 느지만 안전합니다.

3단계. *1단계 인증* 드롭다운 목록에서 적절한 인증 방법을 선택합니다. VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

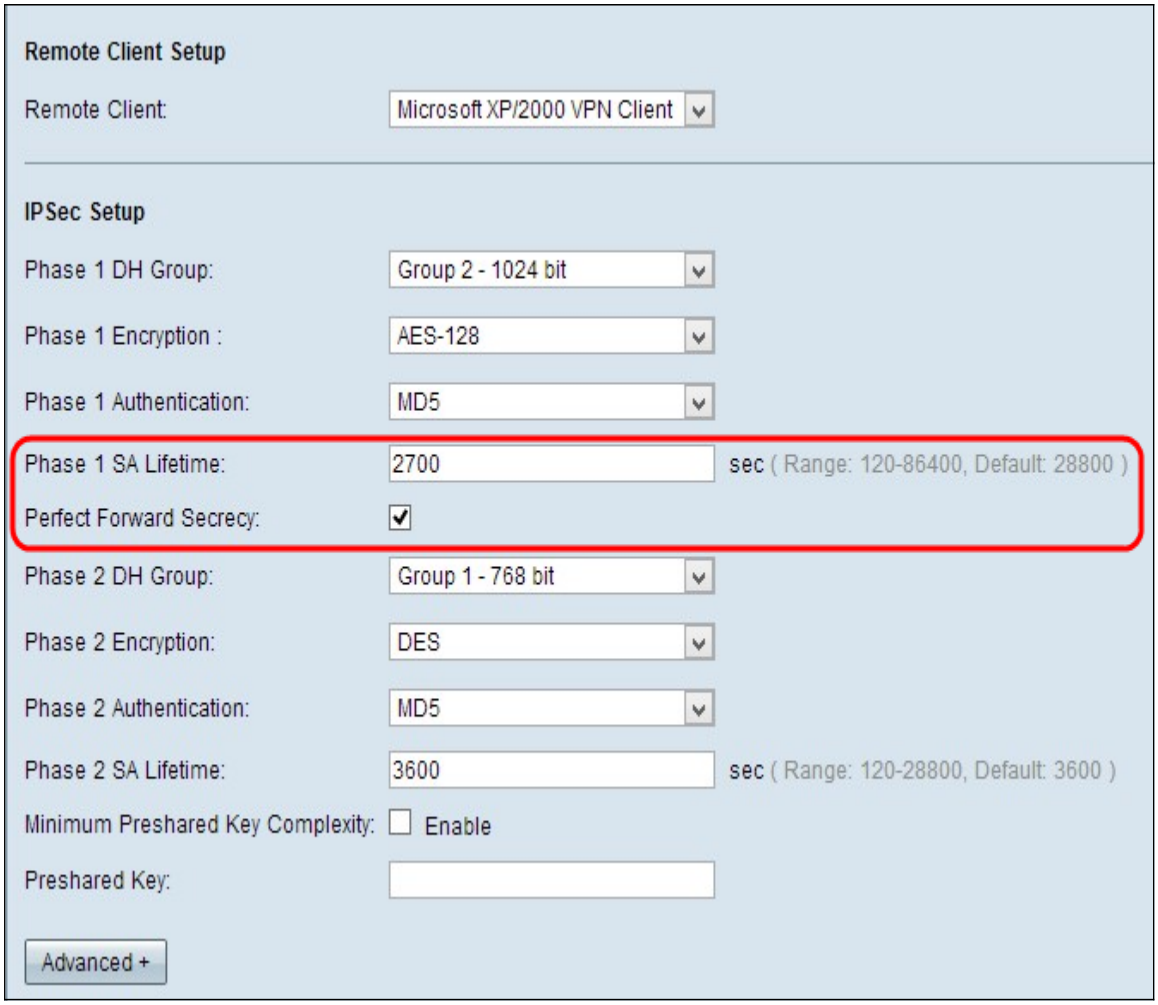


사용 가능한 옵션은 다음과 같이 정의됩니다.

·MD5 — MD5(Message Digest Algorithm-5)는 체크섬 계산에 의한 악의적인 공격으로부터 데이터를 보호하는 128비트 해시 함수를 나타냅니다.

·SHA1 — SHA1(Secure Hash Algorithm version 1)은 160비트 해시 함수로, MD5보다 더 안전합니다.

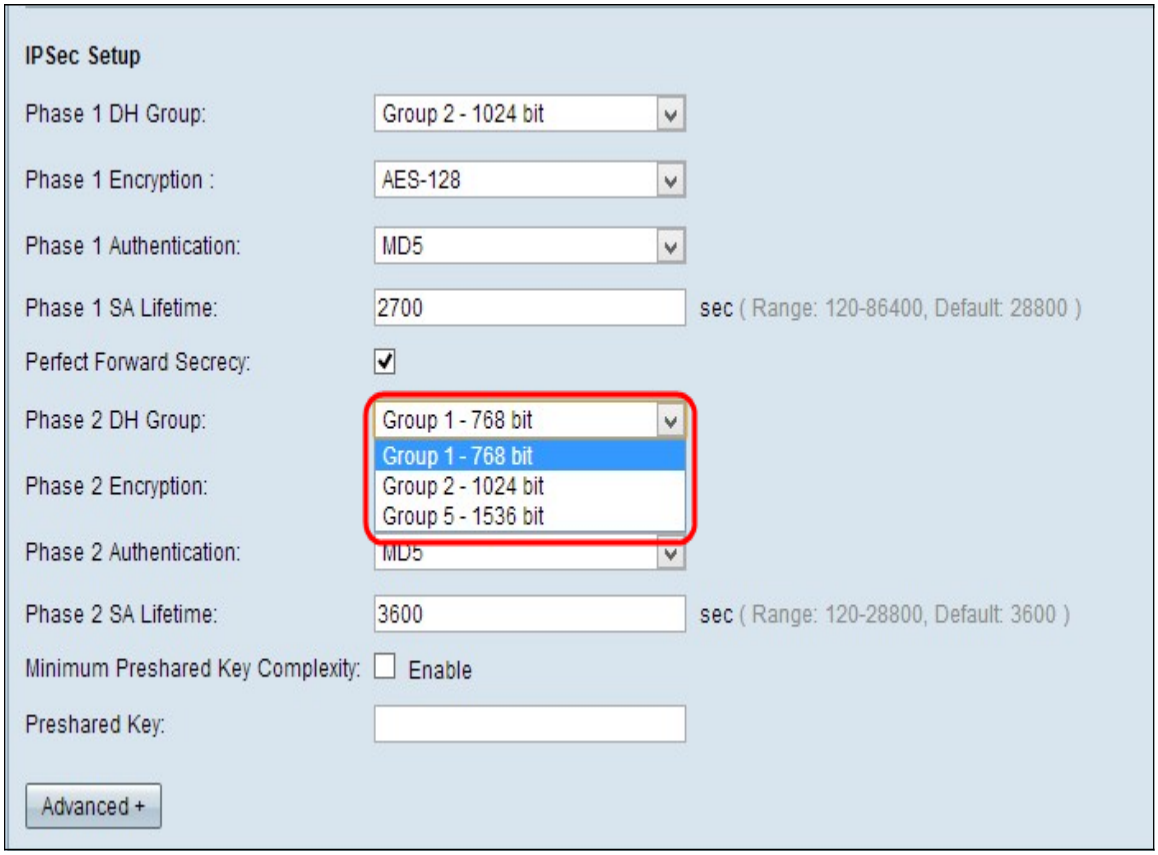
4단계. Phase *1 SA Life Time*(단계 1 SA 수명) 필드에 VPN 터널이 1단계에서 활성 상태로 유지되는 시간(초)을 입력합니다. 기본 시간은 28,800초입니다.



5단계. (선택 사항) 키에 대한 보호를 강화하려면 **Perfect Forward Secrecy** 확인란을 선택합니다.이 옵션을 사용하면 키가 손상된 경우 새 키를 생성할 수 있습니다.이는 더 많은 보안을 제공하기 때문에 권장되는 작업입니다.

참고: 5단계에서 **Perfect Forward Secrecy**를 선택 취소하면 2단계 DH 그룹을 구성할 필요가 없습니다.

6단계. *Phase 2 DH Group* 드롭다운 목록에서 적절한 DH 그룹을 선택합니다.



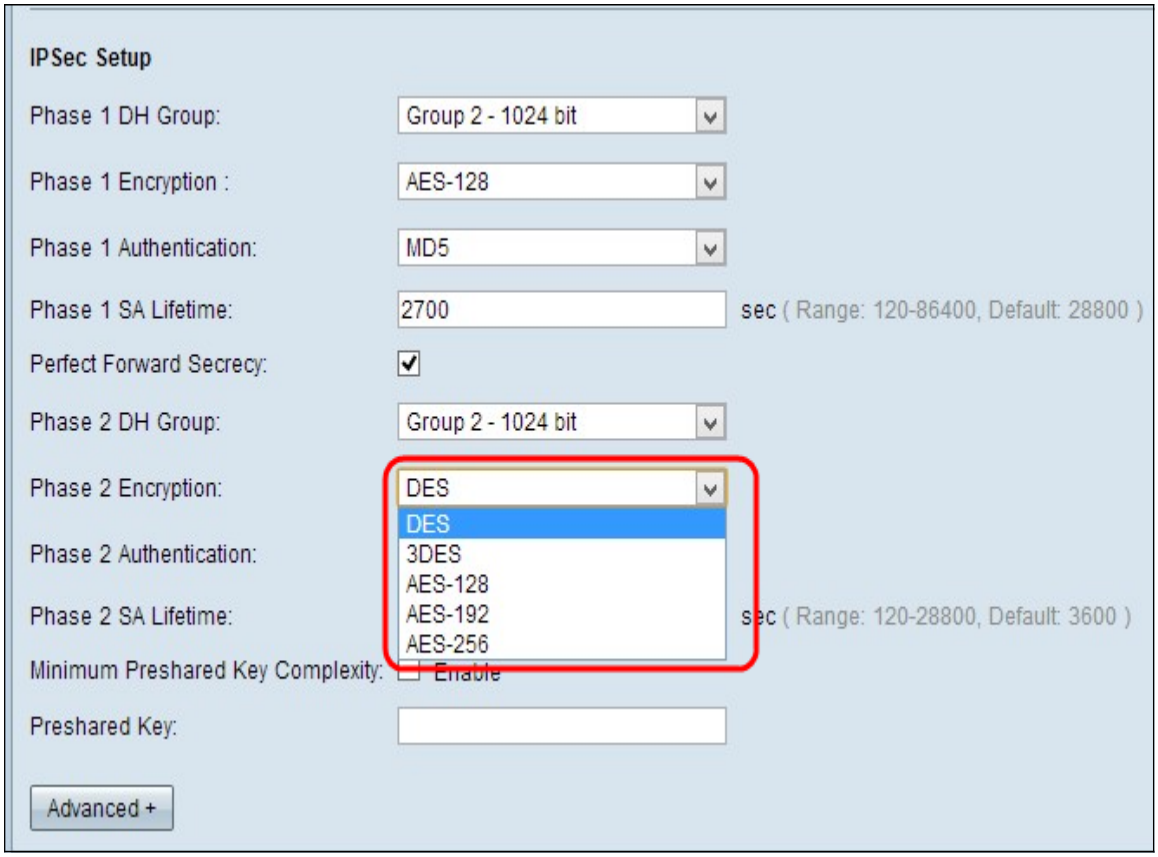
사용 가능한 옵션은 다음과 같이 정의됩니다.

·Group1(768비트) — 가장 빠르지만 가장 안전하지 않은 키를 계산합니다.

·Group2(1024비트) — 키를 느리게 계산하지만 Group1보다 안전합니다.

·Group5(1536비트) — 가장 느린 키를 계산합니다. 하지만 가장 안전합니다.

2단계. Phase *1 Encryption* 드롭다운 목록에서 키를 암호화하는 적절한 암호화 방법을 선택합니다.높은 보안 및 빠른 성능을 위해서는 AES-128이 권장됩니다. VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.



사용 가능한 옵션은 다음과 같이 정의됩니다.

·DES — DES(Data Encryption Standard)는 56비트 오래된 암호화 방법이며, 매우 안전한 암호화 방법은 아니지만 이전 버전과의 호환성을 위해 필요할 수 있습니다.

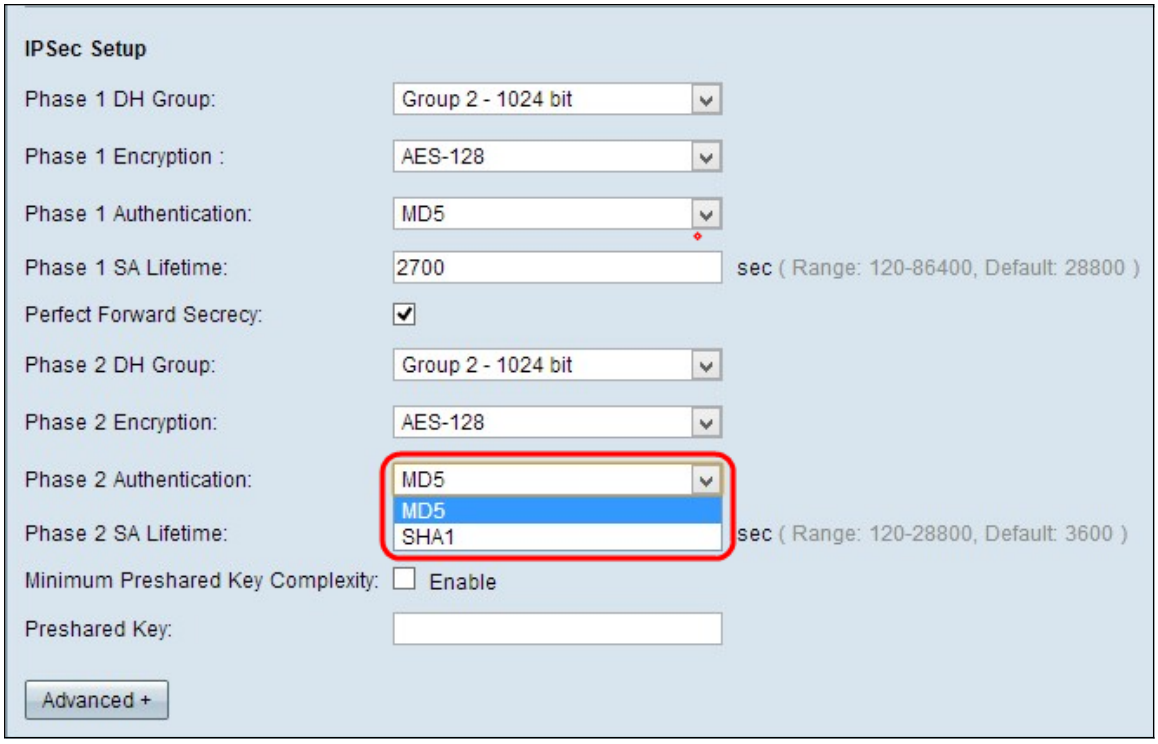
·3DES — 3DES(Triple Data Encryption Standard)는 데이터를 세 번 암호화하므로 키 크기를 늘리는 데 사용되는 168비트 간단한 암호화 방법입니다.이는 DES보다 더 많은 보안을 제공하지만 AES보다 적은 보안을 제공합니다.

·AES-128 — 128비트 키(AES-128)가 포함된 고급 암호화 표준은 AES 암호화를 위해 128비트 키를 사용합니다.AES는 DES보다 빠르고 안전합니다.일반적으로 AES는 3DES보다 빠르고 안전합니다.AES-128은 AES-192 및 AES-256보다 빠르지만 안전하지 않습니다.

·AES-192 — AES-192는 AES 암호화를 위해 192비트 키를 사용합니다.AES-192는 AES-128보다 느리지만 안전성이 높고 AES-256보다 빠르지만 보안성이 낮습니다.

·AES-256 — AES-256은 AES 암호화를 위해 256비트 키를 사용합니다.AES-256은 AES-128 및 AES-192보다 느지만 안전합니다.

8단계. *2단계 인증* 드롭다운 목록에서 적절한 인증 방법을 선택합니다. VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

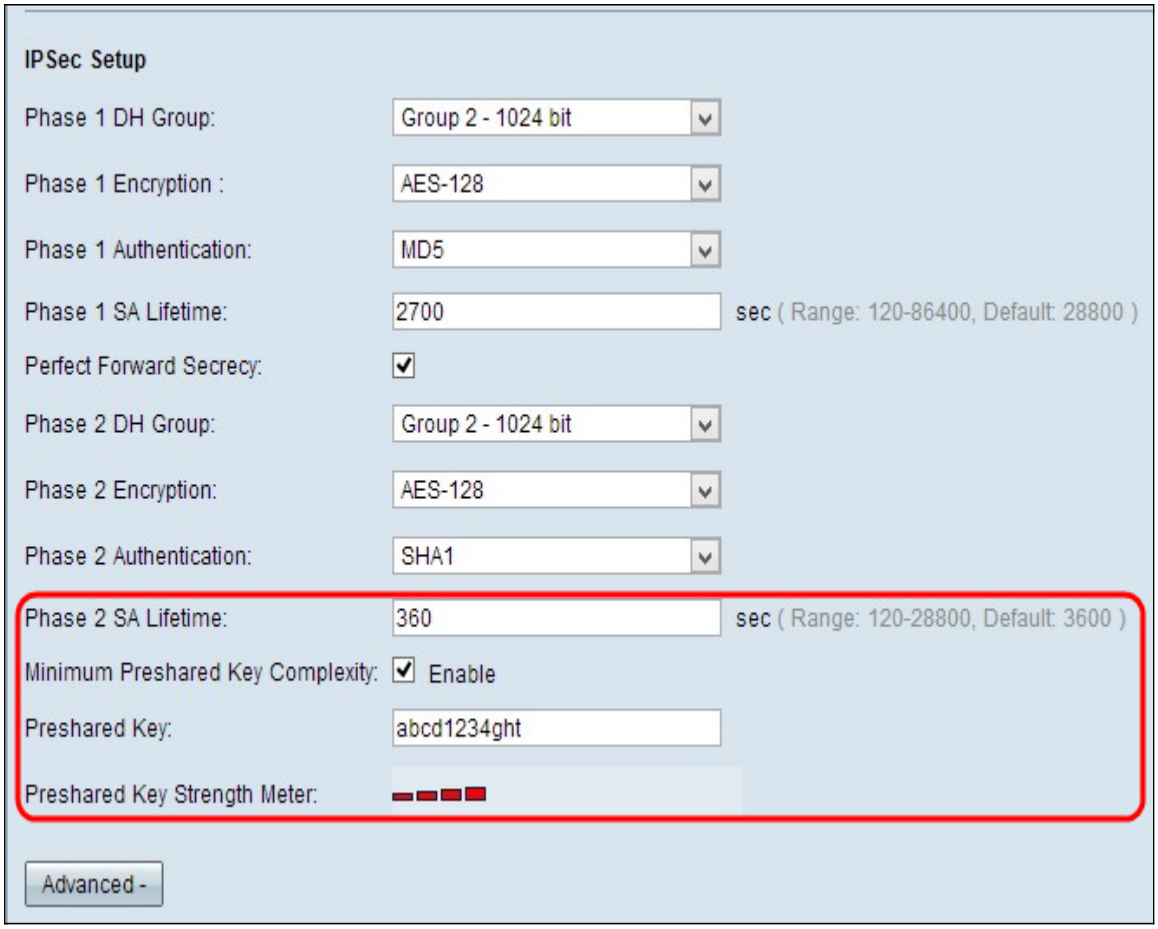


사용 가능한 옵션은 다음과 같이 정의됩니다.

·MD5 — MD5(Message Digest Algorithm-5)는 체크섬 계산에 의한 악의적인 공격으로부터 데이터를 보호하는 128비트 해시 함수를 나타냅니다.

·SHA1 — SHA1(Secure Hash Algorithm version 1)은 MD5보다 더 안전한 160비트 해시 함수입니다.

9단계. Phase *2 SA Lifetime* 필드에 2단계에서 VPN 터널이 활성 상태로 유지되는 시간(초)을 입력합니다. 기본 시간은 3600초입니다.



10단계(선택 사항) 사전 공유 키에 대한 강도 측정기를 활성화하려면 Minimum Preshared Key Complexity(**최소 사전 공유 키 복잡성**) 확인란을 선택합니다.

참고: Minimum Preshared **Key Complexity** 확인란을 선택하면 Preshared *Key Strength Meter*가 색상 막대를 통해 사전 공유 키의 강도를 표시합니다.빨간색은 약한 강도를 나타내고, 노란색은 적정 강도를 나타내고, 녹색은 강한 힘을 나타냅니다.

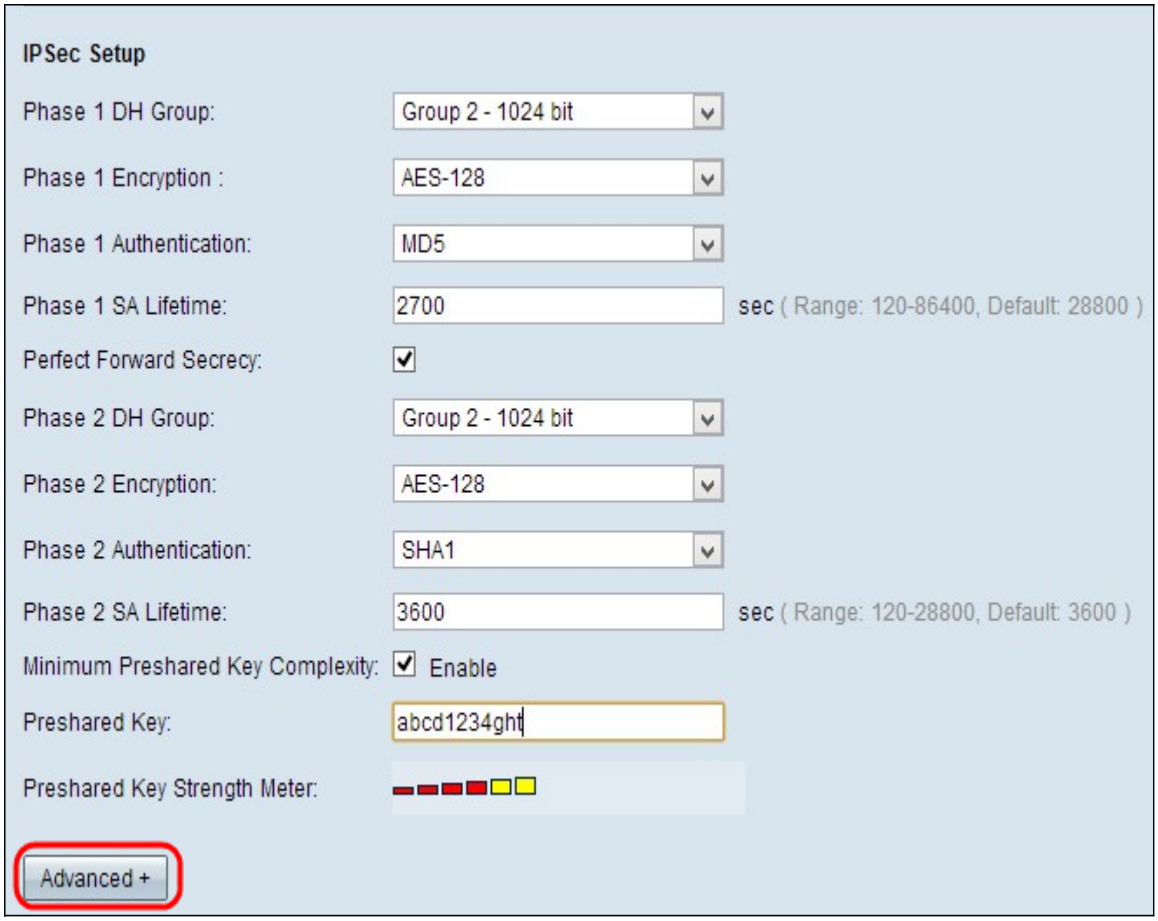
11단계. Preshared *Key* 필드에 원하는 키를 입력합니다.16진수 최대 30개를 사전 공유 키로 사용할 수 있습니다.VPN 터널은 양쪽 끝에 동일한 사전 공유 키를 사용해야 합니다.

참고:VPN이 보호되도록 IKE 피어 간에 사전 공유 키를 자주 변경하는 것이 좋습니다.

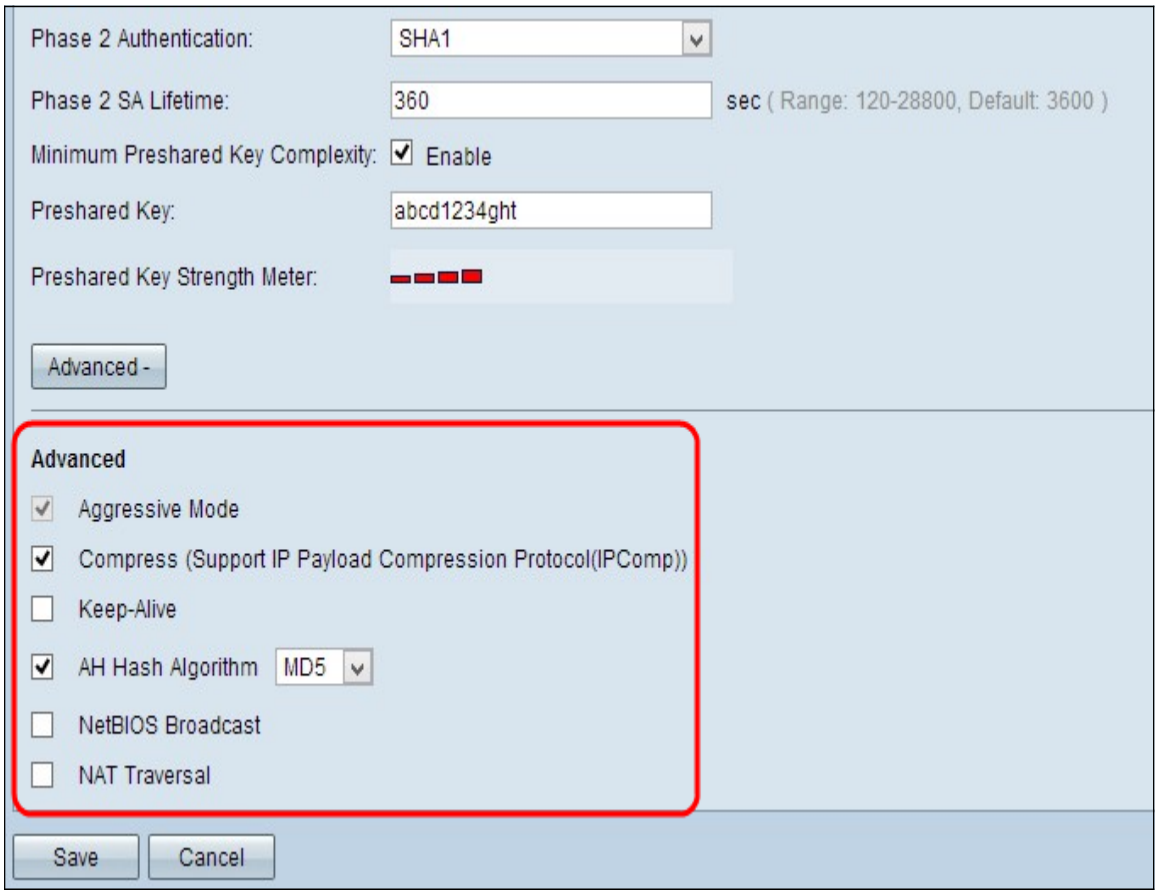
12단계. 지금까지 설정한 설정을 저장하고 나머지는 기본값으로 두려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

고급 설정

1단계. 고급 설정을 구성하려면 고급을 클릭합니다.



Advanced(*고급*) 영역이 새 필드가 사용 가능한 상태로 나타납니다.



2단계. (선택 사항) 네트워크 속도가 낮으면 **Aggressive Mode** 확인란을 선택합니다 .Aggressive Mode(적극적인 모드)는 SA 연결 중에 터널의 엔드포인트의 ID를 일반 텍스트로 교환합니다. 이 경우 교환 시간이 짧지만 보안은 떨어집니다.

3단계. (선택 사항) IP 데이터그램의 크기를 압축하려면 Compress **(Support IP Payload Compression Protocol(IPComp) 지원)** 확인란을 선택합니다.IPComp는 네트워크 속도가 낮을 경우 IP 데이터그램의 크기를 압축하고 사용자가 손실 없이 신속하게 데이터를 전송하려는 경우 사용하는 IP 압축 프로토콜입니다.

4단계. (선택 사항) VPN 터널 연결**을** 항상 활성 상태로 유지하려면 Keep-Alive 확인란을 선택합니다.Keep-Alive를 사용하면 연결이 비활성화되면 즉시 연결을 다시 설정할 수 있습니다.

5단계. (선택 사항) 데이터 원본에 대한 인증, 체크섬을 통한 데이터 무결성, IP 헤더에 확장된 보호를 원하는 경우 AH Hash Algorithm 확인란을 선택합니다.그런 다음 드롭다운 목록에서 적절한 인증 방법을 선택합니다.터널의 양쪽 알고리즘은 동일해야 합니다.

사용 가능한 옵션은 다음과 같이 정의됩니다.

·MD5 — MD5(Message Digest Algorithm-5)는 체크섬 계산에 의한 악의적인 공격으로부터 데이터를 보호하는 128비트 해시 함수를 나타냅니다.

·SHA1 — SHA1(Secure Hash Algorithm version 1)은 MD5보다 더 안전한 160비트 해시 함수입니다.

6단계. VPN 터널을 통해 라우팅 가능한 트래픽이 아닌 트래픽을 허용하려면 **NetBIOS Broadcast** 확인란을 선택합니다.기본값은 선택되지 않습니다.NetBIOS는 소프트웨어 애플리케이션 및 Network Neighbor와 같은 Windows 기능을 통해 네트워크에서 프린터, 컴퓨터 등의 네트워크 리소스를 탐지하는 데 사용됩니다.

7단계. (선택 사항) 공용 IP 주소를 통해 사설 LAN에서 인터넷에 액세스하려면 **NAT Traversal** 확인란을 선택합니다.NAT 통과는 내부 시스템의 사설 IP 주소가 공용 IP 주소로 나타나도록 하여 악성 공격 또는 검색으로부터 사설 IP 주소를 보호합니다.

8단계. **저장**을 클릭하여 설정을 저장합니다.