RV320 및 RV325 VPN Router Series에서 단일 클라이언트에서 게이트웨이 VPN(Virtual Private Network)으로 구성

목표

이 문서의 목적은 RV32x Series VPN Router의 게이트웨이 VPN(Virtual Private Network)에 단일 클라이언트를 구성하는 방법을 보여 주는 것입니다.

소개

VPN은 공용 네트워크를 통해 원격 사용자를 가상으로 연결하는 데 사용되는 사설 네트워크입니다. VPN의 한 가지 유형은 클라이언트-게이트웨이 VPN입니다.클라이언트-게이트웨이 VPN은 원격 사용자와 네트워크 간의 연결입니다.클라이언트는 VPN 클라이언트 소프트웨어를 사용하여 사용자의 디바이스에 구성됩니다.사용자가 원격으로 네트워크에 안전하게 연결할 수 있습니다.

적용 가능한 디바이스

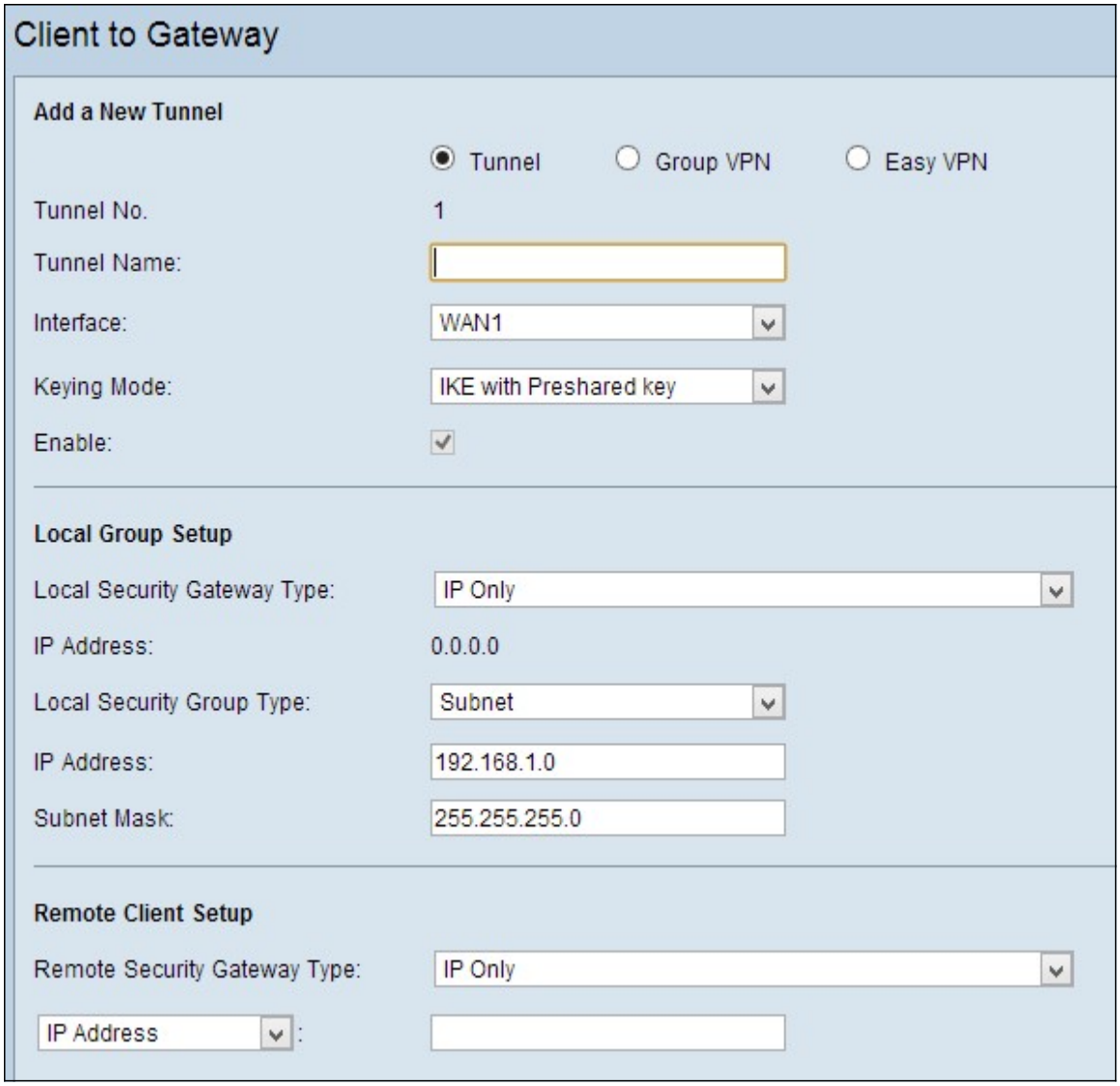
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

소프트웨어 버전

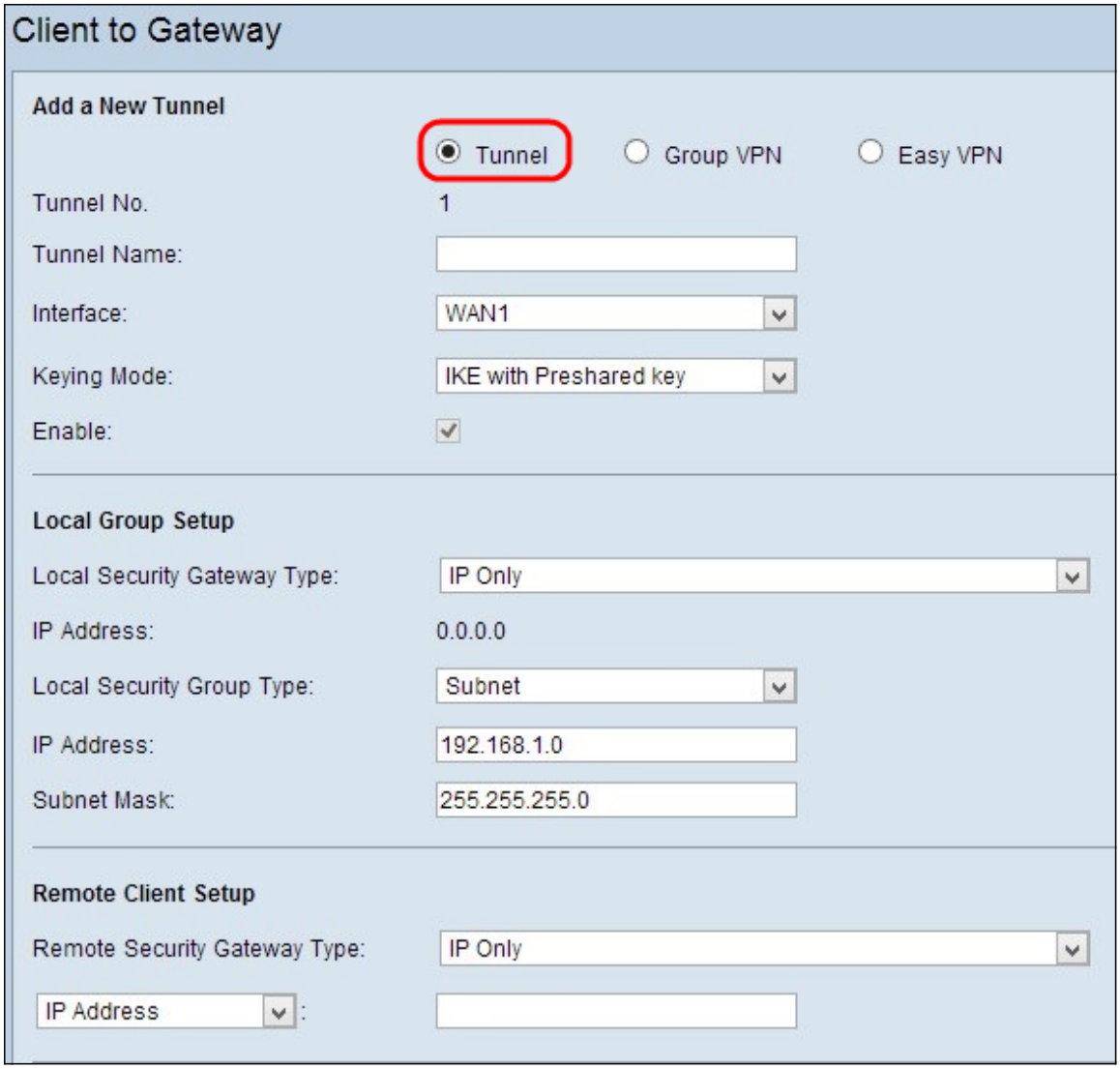
- v1.1.0.09

단일 클라이언트-게이트웨이 VPN 구성

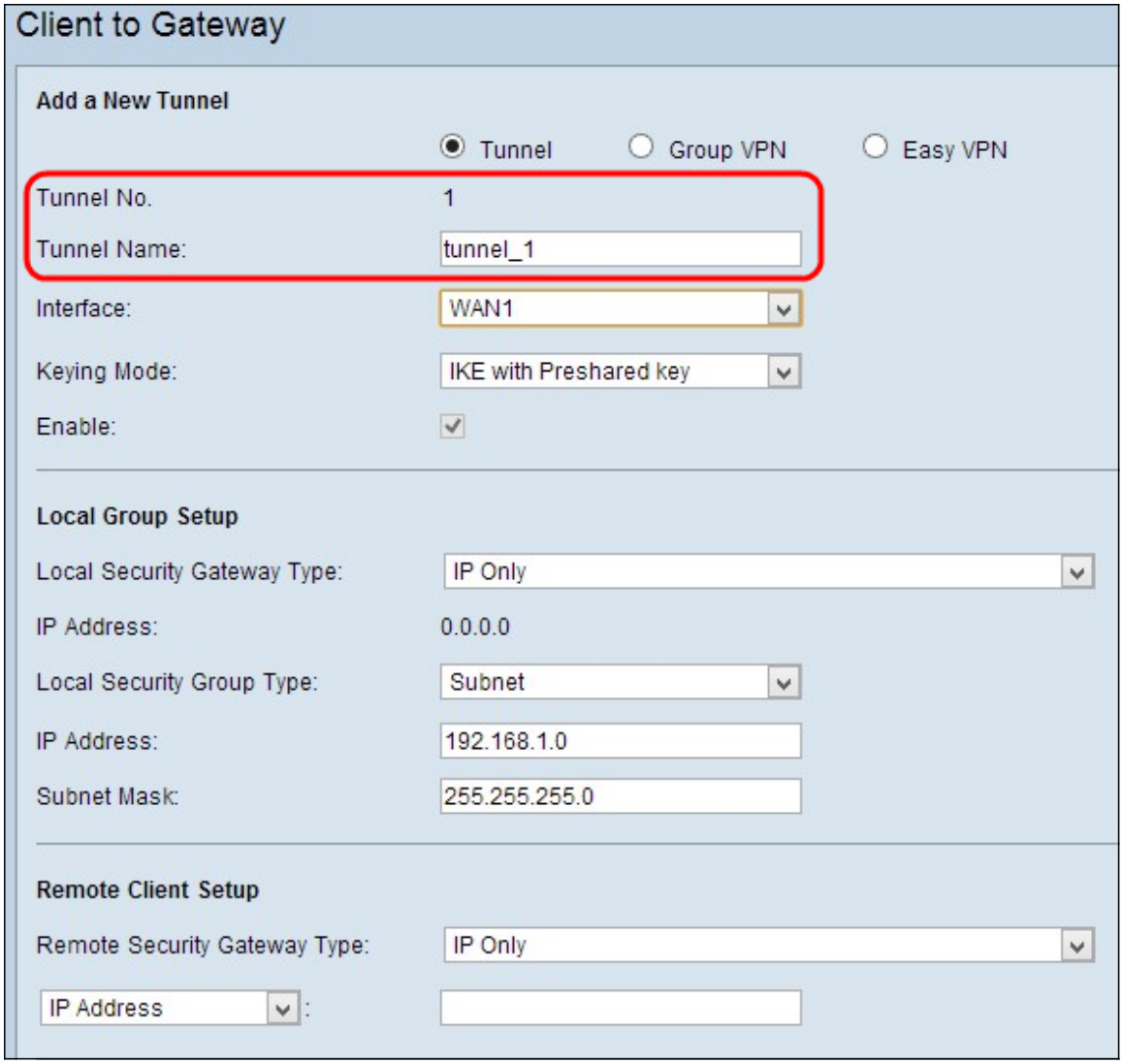
1단계. 웹 컨피그레이션 유틸리티에 로그인하고 **VPN > Client to Gateway**를 선택합니다 .Client to *Gateway(클라이언트-게이트웨이)* 페이지가 열립니다.



2단계. Tunnel(**터널**) 라디오 버튼을 클릭하여 클라이언트-게이트웨이 VPN에 대한 단일 터널을 추가합니다.


Client to Gateway
Add a New Tunnel
Tunnel
Group VPN
Easy VPN
Tunnel No.
1
Tunnel Name:
Interface:
WAN1
Keying Mode:
IKE with Preshared key
Enable:
Local Group Setup
Local Security Gateway Type:
IP Only
IP Address:
0.0.0.0
Local Security Group Type:
Subnet
IP Address:
192.168.1.0
Subnet Mask:
255.255.255.0
Remote Client Setup
Remote Security Gateway Type:
IP Only
IP Address
:

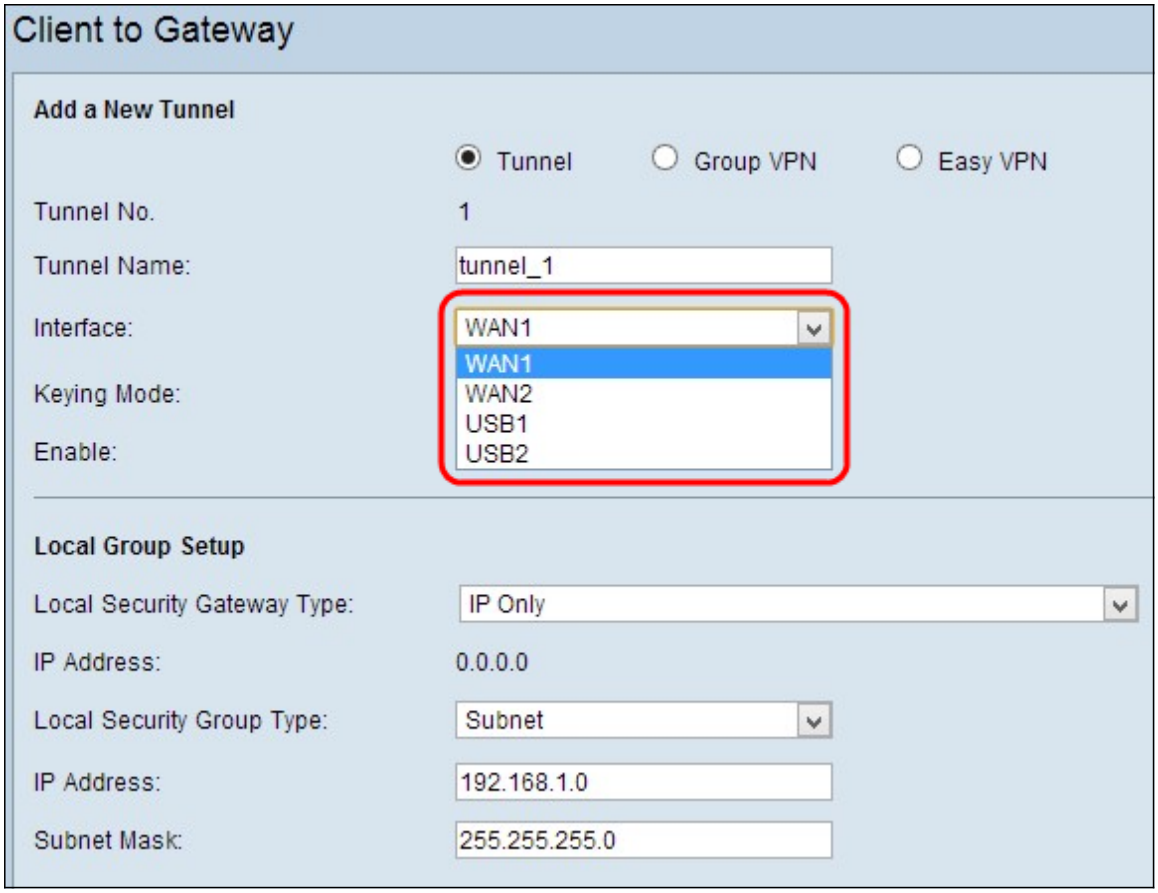
새 터널 추가



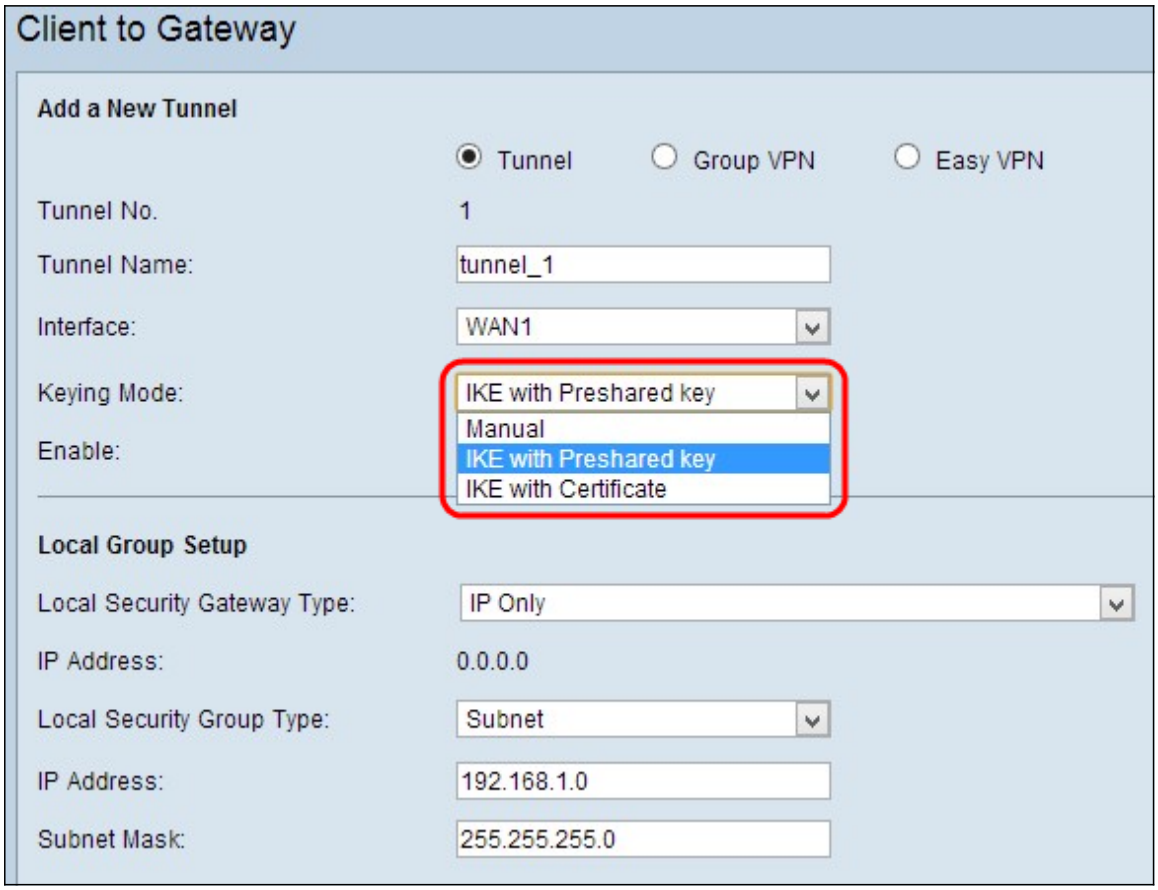
참고: Tunnel No - 터널 수를 나타냅니다.이 번호는 자동으로 생성됩니다.

1단계. Tunnel *Name* 필드에 터널 이름을 입력합니다.

2단계. 원격 클라이언트가 *Interface* 드롭다운 목록에서 VPN에 액세스하는 인터페이스를 선택합니다.



3단계. 키 모드 드롭다운 목록에서 보안을 유지하려면 적절한 키 관리 모드를 선택합니다.기본 모드는 사전 공유 키가 있는 IKE입니다.



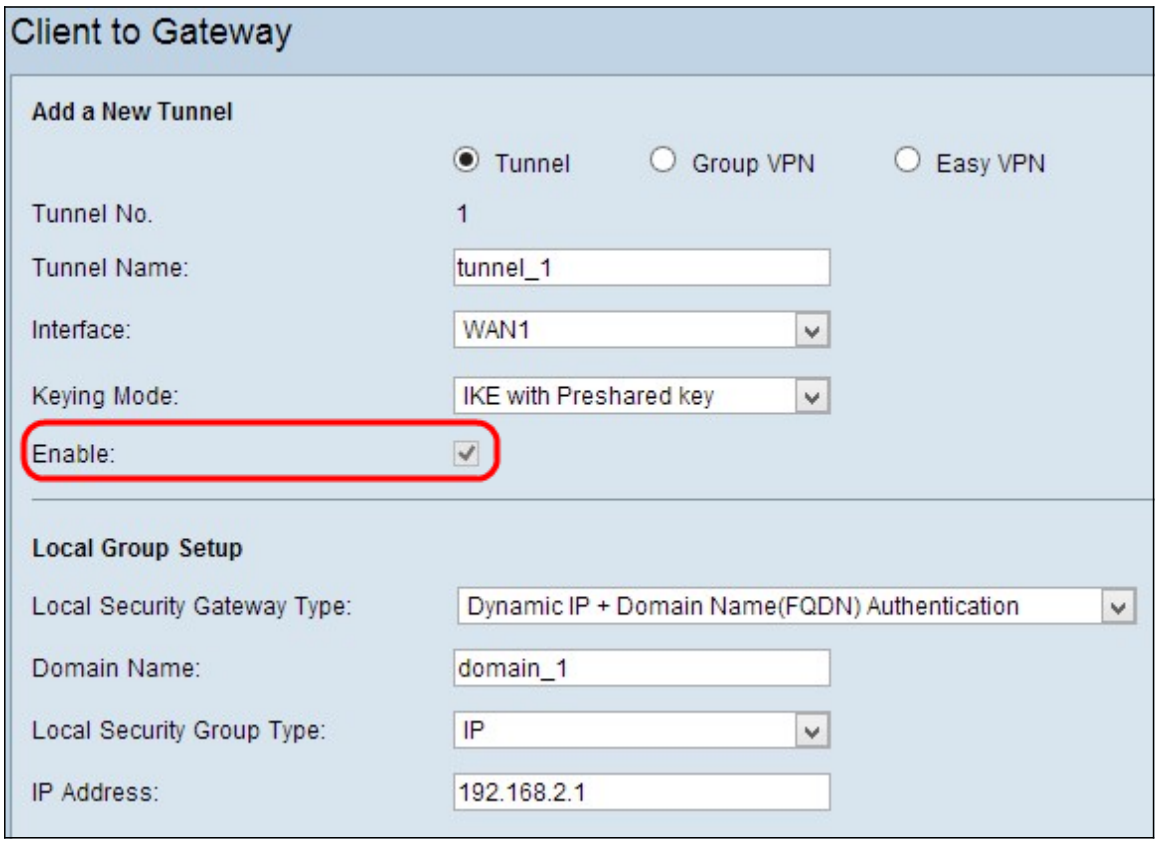
옵션은 다음과 같이 정의됩니다.

- 수동 - 사용자 스스로 새 보안 키를 생성하고 키와의 협상이 없는 사용자 지정 보안 모드.트러블

슈팅 중에 또는 작은 정적 환경에서 사용하는 것이 가장 좋습니다.

- 사전 공유 키를 사용하는 IKE - IKE(Internet Key Exchange) 프로토콜은 사전 공유 키를 자동으로 생성하고 교환하여 터널에 대해 인증된 통신을 설정하는 데 사용됩니다.
- IKE with Certificate - IKE(Internet Key Exchange) 프로토콜은 터널에 대한 보다 안전한 통신을 설정하기 위해 사전 공유 키를 자동으로 생성하고 교환하는 보다 안전한 방법입니다.

4단계. Enable(활성화) 확인란을 선택하여 클라이언트에서 게이트웨이 VPN을 활성화합니다 .기본적으로 활성화되어 있습니다.



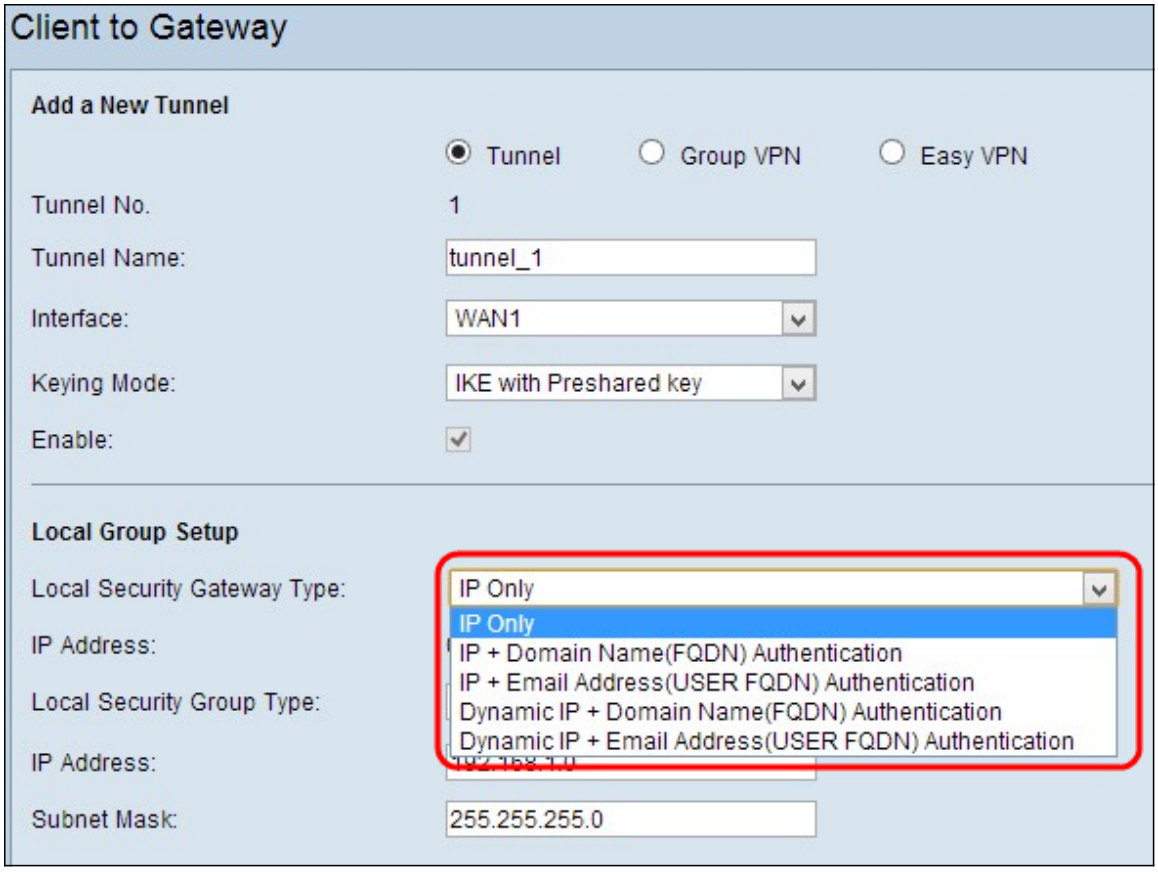
5단계. 현재 설정을 저장하려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

로컬 그룹 설정

수동 또는 사전 공유 키가 있는 IKE를 사용하는 로컬 그룹 설정

참고: Add a New Tunnel(새 터널 추가) 섹션의 3단계의 Keying *Mode(키잉 모드*) 드롭다운 목록에서 Manual(수동) 또는 IKE with Preshared(사전 공유 키가 있는 IKE)를 선택한 경우 아래 단계를 수행합니다.

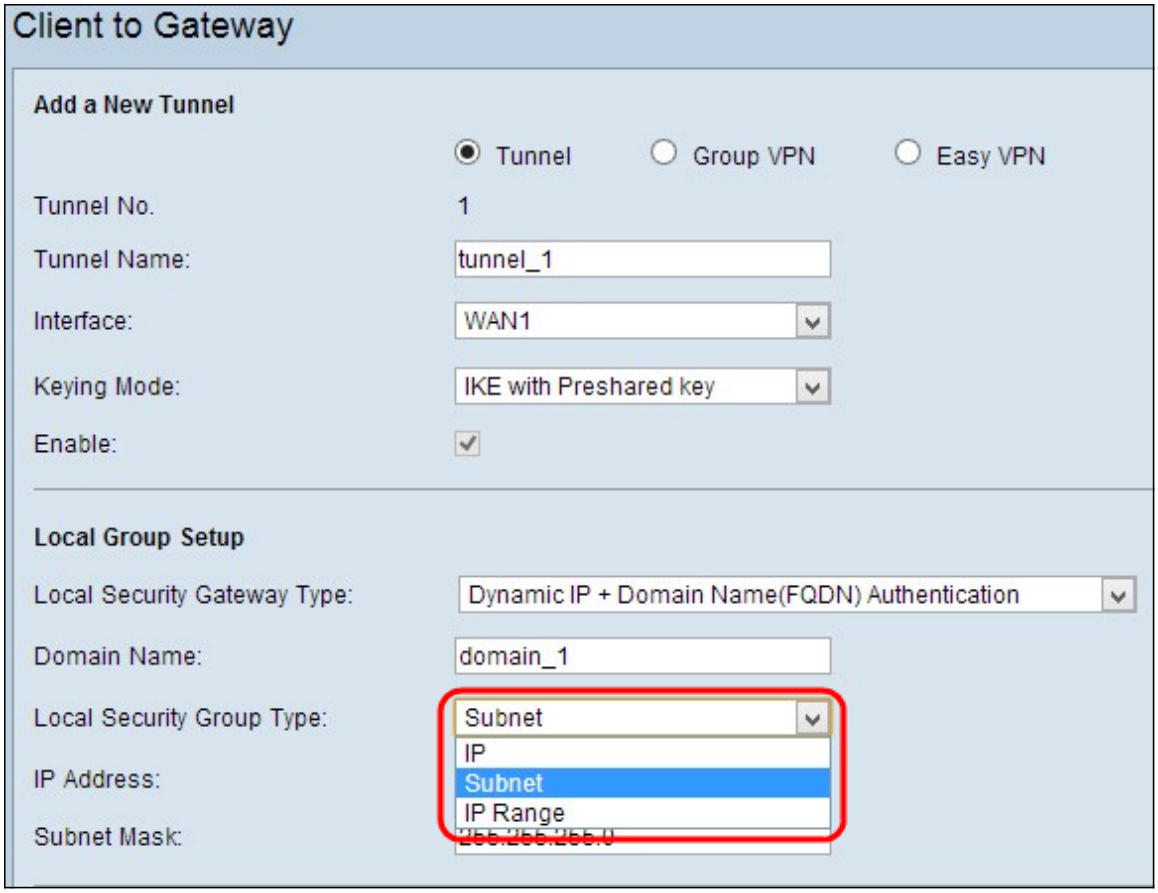
1단계. *Local Security Gateway(로컬 보안 게이트웨이)* 드롭다운 목록에서 적절한 라우터 식별 방법을 선택하여 VPN 터널을 설정합니다.



옵션은 다음과 같이 정의됩니다.

- IP Only(IP 전용) - 고정 WAN IP를 통해서만 터널에 액세스할 수 있습니다.라우터에만 고정 WAN IP가 있는 경우 이 옵션을 선택할 수 있습니다.고정 WAN IP 주소는 자동으로 생성됩니다 .
- IP + 도메인 이름(FQDN) 인증 - 고정 IP 주소 및 등록된 도메인을 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *Domain Name* 필드에 등록된 도메인의 이름을 입력합니다.고정 WAN IP 주소는 자동으로 생성됩니다.
- IP + 이메일 주소(USER FQDN) 인증 - 고정 IP 주소 및 이메일 주소를 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *Email Address* 필드에 이메일 주소를 입력합니다.고정 WAN IP 주소는 자동으로 생성됩니다.
- 동적 IP + 도메인 이름(FQDN) 인증 — 동적 IP 주소 및 등록된 도메인을 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *Domain Name* 필드에 등록된 도메인의 이름을 입력합니다.
- 동적 IP + 이메일 주소(USER FQDN) 인증 - 동적 IP 주소 및 이메일 주소를 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *Email Address* 필드에 이메일 주소를 입력합니다.
- IP Address - WAN 인터페이스의 IP 주소를 나타냅니다.읽기 전용 필드입니다.

2단계. *Local Security Group Type* 드롭다운 목록에서 VPN 터널에 액세스할 수 있는 적절한 로컬 LAN 사용자 또는 사용자 그룹을 선택합니다.기본값은 서브넷입니다.

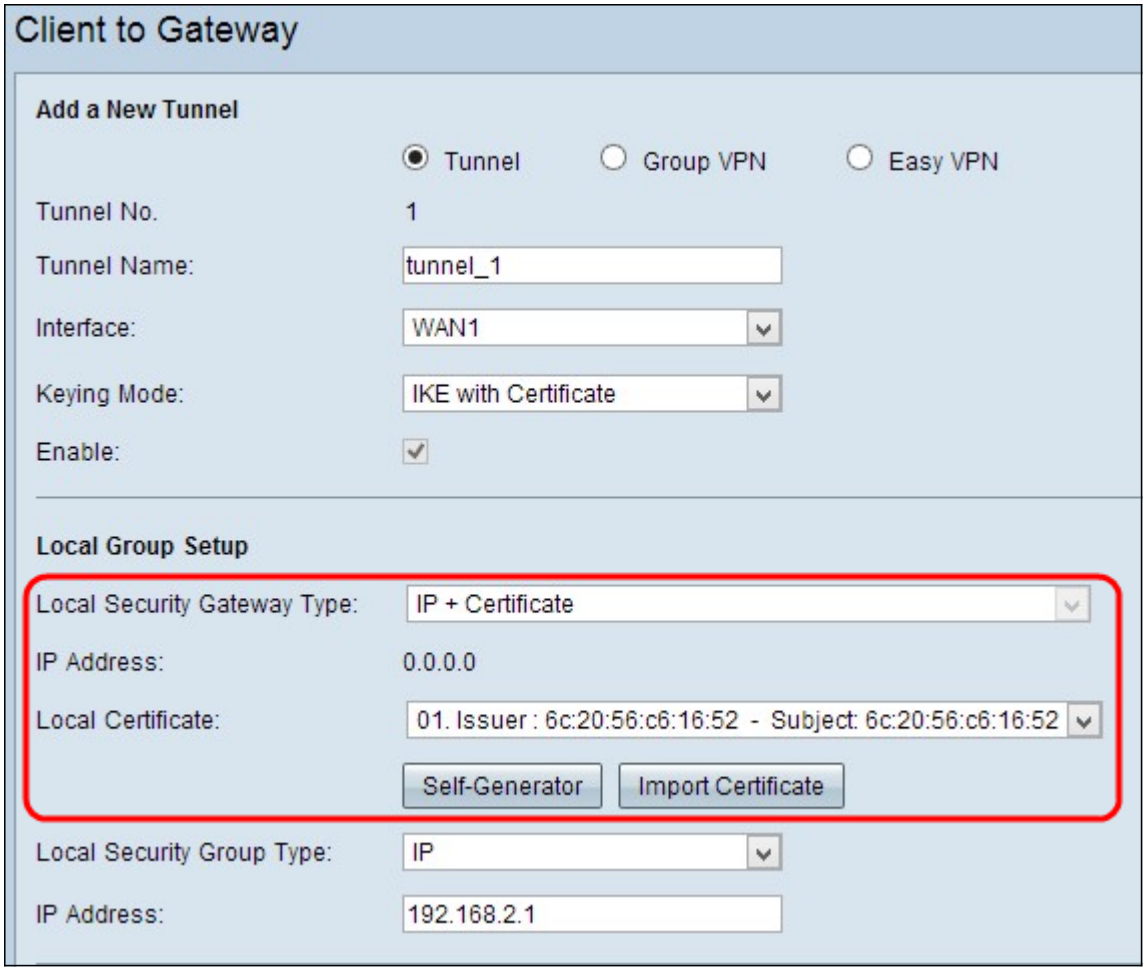


- IP - 하나의 특정 LAN 디바이스만 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 *IP Address* 필드에 LAN 디바이스의 IP 주소를 입력합니다.기본 IP는 192.168.1.0입니다.
- 서브넷 - 특정 서브넷의 모든 LAN 디바이스는 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 LAN 디바이스의 IP 주소와 서브넷 마스크를 *IP Address* 및 *Subnet Mask* 필드에 각각 입력합니다.기본 마스크는 255.255.255.0입니다.
- IP Range(IP 범위) - 다양한 LAN 디바이스가 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 시작 *IP* 및 *끝 IP* 필드에 시작 및 끝 IP 주소를 각각 입력합니다.기본 범위는 192.168.1.0~192.168.1.254입니다.

3단계. 현재 설정을 저장하려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

터널 VPN용 인증서가 있는 IKE를 통한 로컬 그룹 설정

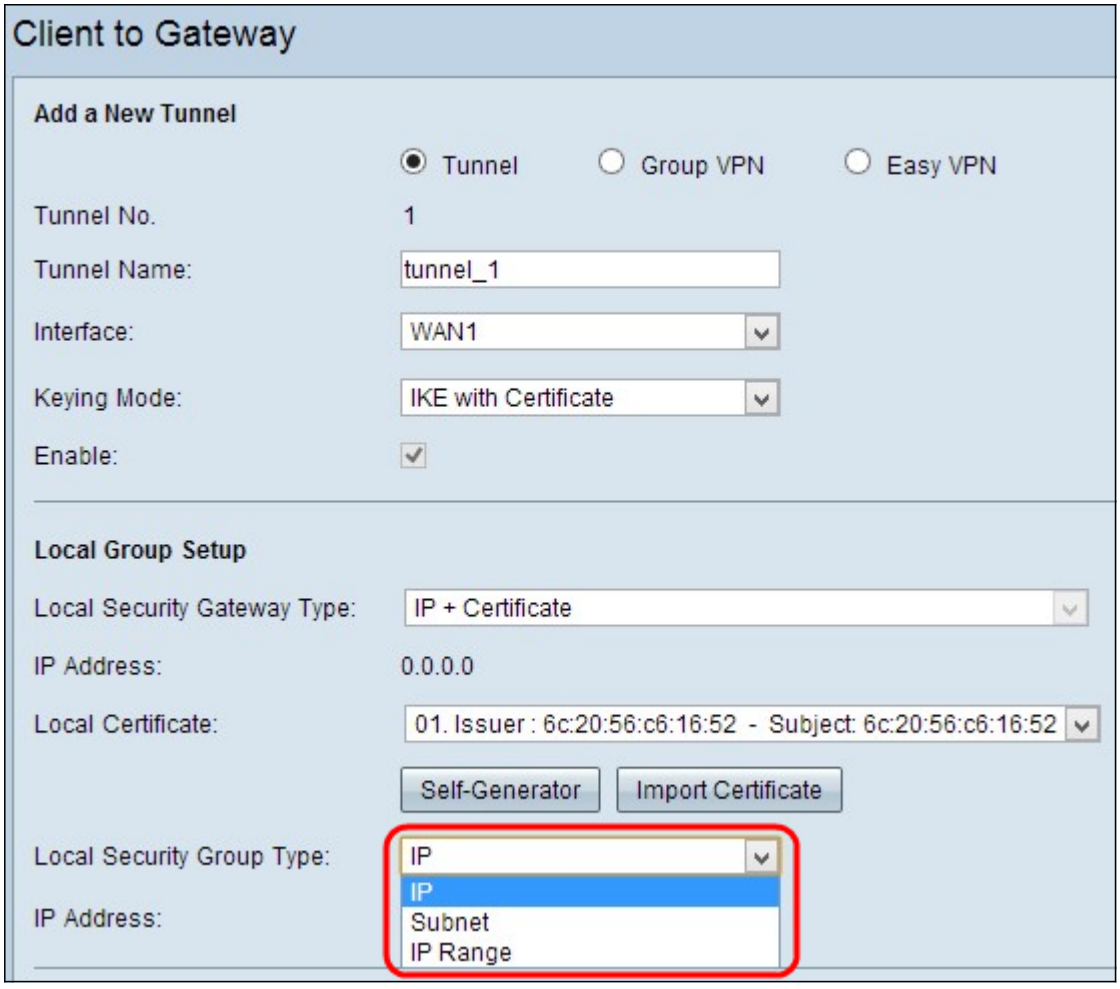
참고: Add a *New Tunnel* 섹션의 3단계의 Keying *Mode* 드롭다운 목록에서 IKE with Certificate를 선택한 경우 아래 단계를 수행합니다.



- Local Security Gateway Type(로컬 보안 게이트웨이 유형) - 인증서가 있는 IP를 통해 터널에 액세스할 수 있습니다.
- IP Address - WAN 인터페이스의 IP 주소를 나타냅니다.읽기 전용 필드입니다.

1단계. Local Certificate(*로컬 인증서*) 드롭다운 목록에서 라우터를 식별하기 위한 적절한 로컬 인증서를 선택합니다.Self-**Generator**를 클릭하여 인증서를 자동으로 생성하거나 Import **Certificate**를 클릭하여 새 인증서를 가져옵니다.

참고:인증서를 자동으로 생성하는 방법에 대한 자세한 내용은 RV320 라우터의 *인증서 생성*을 참조하고, 인증서를 가져오는 방법에 대한 자세한 내용은 *RV320 라우터의 내 인증서 구성을 참조하십시오*.



2단계. *Local Security Group Type(로컬 보안 그룹 유형)* 드롭다운 목록에서 VPN 터널에 액세스할 수 있는 로컬 LAN 사용자 또는 사용자 그룹의 적절한 유형을 선택합니다.기본값은 서브넷입니다.

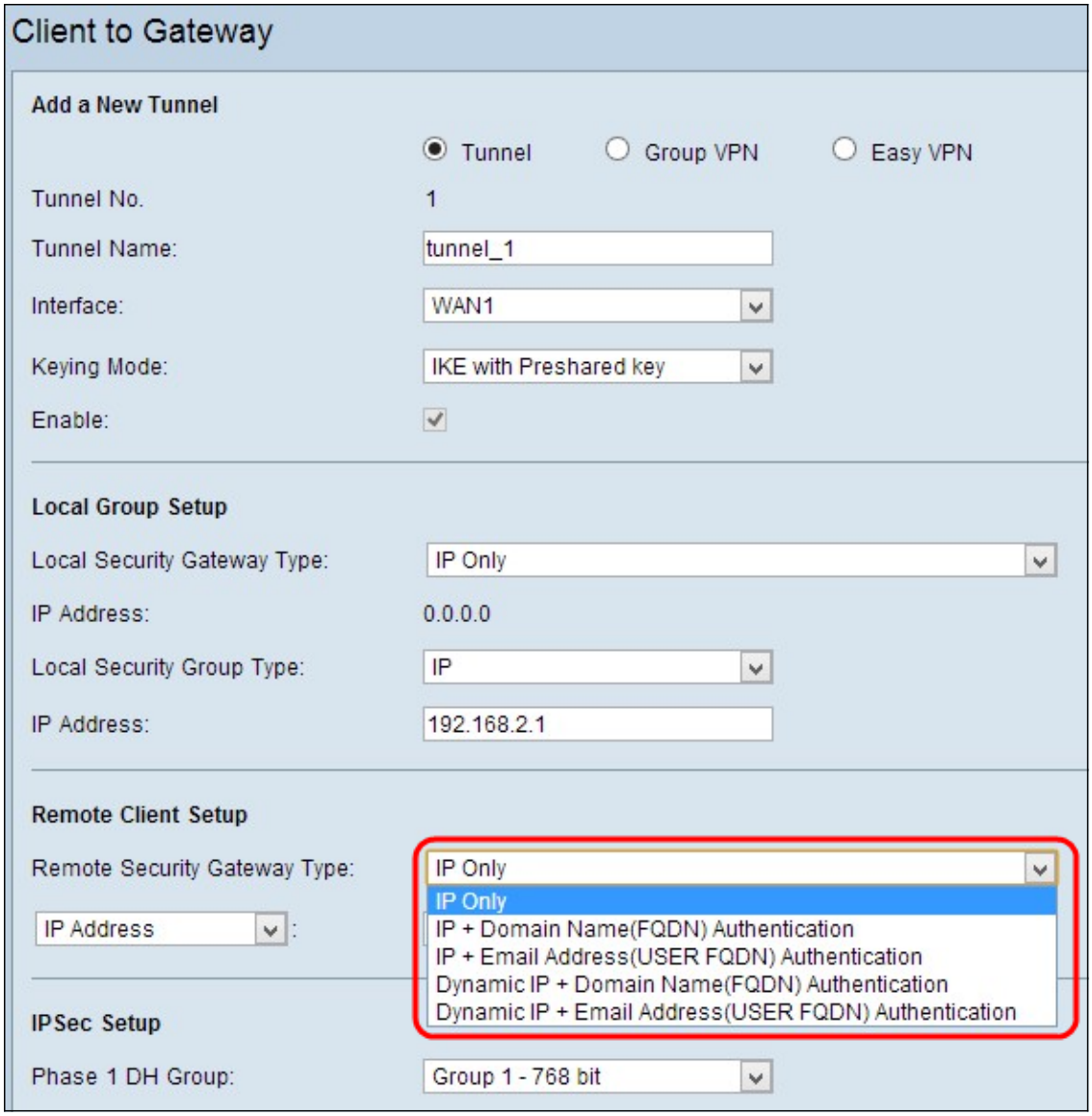
- IP - 하나의 특정 LAN 디바이스만 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 IP Address 필드에 LAN 디바이스의 IP 주소를 입력합니다.기본 IP는 192.168.1.0입니다.
- 서브넷 - 특정 서브넷의 모든 LAN 디바이스는 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 IP Address(IP 주소) 및 Subnet Mask(서브넷 마스크) 필드에 LAN 디바이스의 IP 주소와 서브넷 마스크를 각각 입력합니다.기본 마스크는 255.255.255.0입니다.
- IP Range(IP 범위) - 다양한 LAN 디바이스가 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 Start IP(시작 IP) 및 End IP(종료 IP) 필드에 시작 및 종료 IP 주소를 각각 입력합니다.기본 범위는 192.168.1.0~192.168.1.254입니다.

3단계. 현재 설정을 저장하려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

원격 클라이언트 설정

수동 또는 사전 공유 키가 있는 IKE를 사용하는 원격 클라이언트 설정

참고: Add a New Tunnel 섹션의 3단계의 *Keying Mode* 드롭다운 목록에서 Manual 또는 IKE with Preshared Key*를 선택한 경우 아래 단계를 수행합니다*.



1단계. *Remote Security Gateway* 드롭다운 목록에서 VPN 터널을 설정하기 위한 적절한 클라이언트 식별 방법을 선택합니다.기본값은 IP Only입니다.

- IP Only(IP 전용) - 클라이언트의 고정 WAN IP를 통해서만 터널에 액세스할 수 있습니다.클라이언트의 고정 WAN IP 또는 도메인 이름을 알고 있는 경우에만 이 옵션을 선택할 수 있습니다.드롭다운 목록에서 IP Address(IP 주소)를 선택하고 인접 필드에 클라이언트의 고정 IP를 입력하거나 드롭다운 목록에서 IP by DNS Resolved(DNS별 IP 해결됨)를 선택하고 인접 필드에 IP 주소의 도메인 이름을 입력합니다.IP 주소의 로컬 DNS 서버를 통해 라우터는 IP 주소를 자동으로 검색할 수 있습니다.

  참고: Add a New Tunnel Through Tunnel or Group VPN(터널을 통해 새 터널 추가 또는 그룹 VPN) 섹션의 3단계에서 Keying *Mode*(키잉 모드) 드롭다운 목록에서 Manual(수동)을 선택하면 이 옵션만 사용할 수 있습니다.

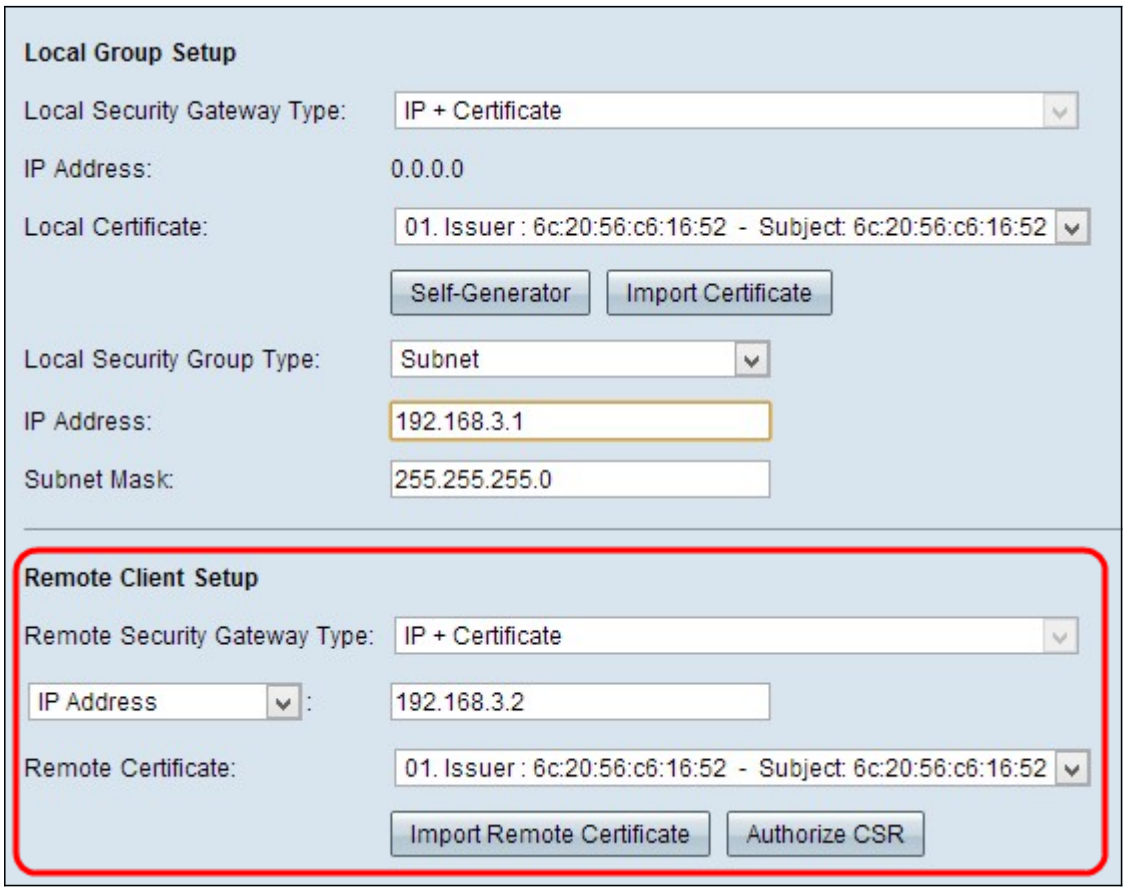
- IP + 도메인 이름(FQDN) 인증 - 클라이언트 및 등록된 도메인의 고정 IP 주소를 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메인의 이름을 입력합니다.드롭다운 목록에서 IP Address(IP 주소)를 선택하고 인접 필드에 클라이언트의 고정 IP를 입력하거나 드롭다운 목록에서 IP by DNS Resolved(DNS별 IP 해결됨)를 선택하고 인접 필드에 IP 주소의 도메인 이름을 입력합니다.IP 주소의 로컬 DNS 서버를 통해 라우터는 IP 주소를 자동으로 검색할 수 있습니다.

- IP + 이메일 주소(USER FQDN) 인증 - 터널에 액세스할 수 있는 방법은 클라이언트의 고정 IP 주소 및 이메일 주소입니다.이 옵션을 선택하는 경우 [전자 메일 주소] 필드에 전자 메일 주소를 입력합니다. 드롭다운 목록에서 IP 주소를 선택하고 인접한 필드에 클라이언트의 고정 IP를 입력하거나 드롭다운 목록에서 IP by DNS Resolved를 선택하고 인접한 필드에 IP 주소의 도메인 이름을 입력합니다.IP 주소의 로컬 DNS 서버를 통해 라우터는 IP 주소를 자동으로 검색할 수 있습니다.
- 동적 IP + 도메인 이름(FQDN) 인증 - 클라이언트 및 등록된 도메인의 동적 IP 주소를 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메인의 이름을 입력합니다.
- 동적 IP + 전자 메일 주소(USER FQDN) 인증 - 터널에 액세스할 수 있는 방법은 클라이언트의 동적 IP 주소 및 이메일 주소입니다.이 옵션을 선택하는 경우 이메일 주소 필드에 이메일 주소를 입력합니다.

2단계. 현재 설정을 저장하려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

IKE와 인증서 함께 원격 그룹 설정

참고: Add a New Tunnel 섹션의 3단계의 Keying *Mode* 드롭다운 목록에서 IKE with Certificate*를* 선택한 경우 아래 단계*를* 수행합니다.



- Remote Security Gateway Type(원격 보안 게이트웨이 유형) - VPN 연결을 설정하기 위해 인증서가 있는 IP를 통해 클라이언트 식별이 가능합니다.

1단계. 드롭다운 목록에서 **IP 주소** 또**는 DNS Resolved**를 선택합니다.

- IP Address(IP 주소) - 클라이언트의 고정 WAN IP를 통해서만 터널에 액세스할 수 있습니다.클라이언트의 고정 WAN IP를 알고 있는 경우에만 이 옵션을 선택할 수 있습니다.*IP* 주소 필드에 클라이언트의 고정 IP를 입력합니다.

- IP By DNS Resolved - 클라이언트의 IP 주소를 모르지만 해당 IP 주소의 도메인을 아는 경우 유용합니다.IP 주소의 도메인 이름을 입력합니다.IP 주소의 로컬 DNS 서버를 통해 라우터는 IP 주소를 자동으로 검색할 수 있습니다.

2단계. *Remote Certificate* 드롭다운 목록에서 적절한 원격 인증서를 선택합니다.Import **Remote Certificate(원격 인증서 가져오기)**를 클릭하여 새 인증서를 가져오거나 Authorize CSR(**CSR 권한 부여)**을 클릭하여 디지털 서명 요청이 있는 인증서를 식별합니다.

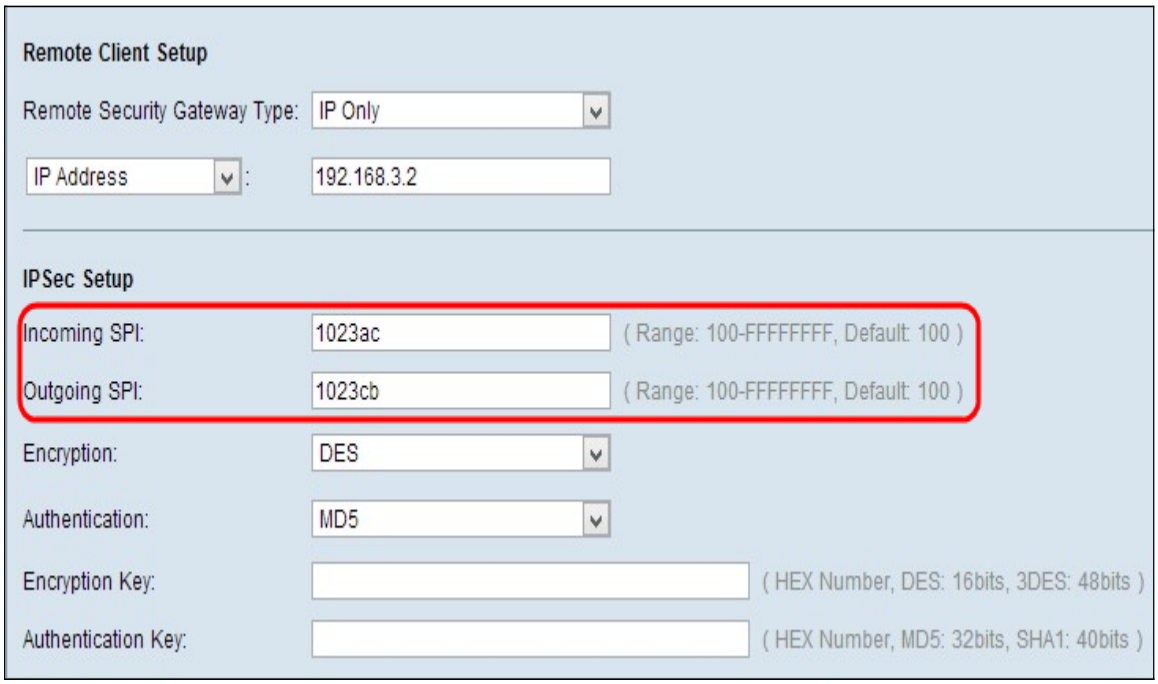
참고:새 인증서를 가져오는 방법에 대한 자세한 내용은 *RV320 Routers의 View/Add Trusted SSL Certificate on RV320 Routers*를 참조하고, 인증된 CSR에 대한 자세한 내용은 RV*320 라우터의 CSR(Certificate Signing Request)*을 참조하십시오.

3단계. 현재 설정을 저장하려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

IPSec 설정

수동 키를 사용한 IPSec 설정

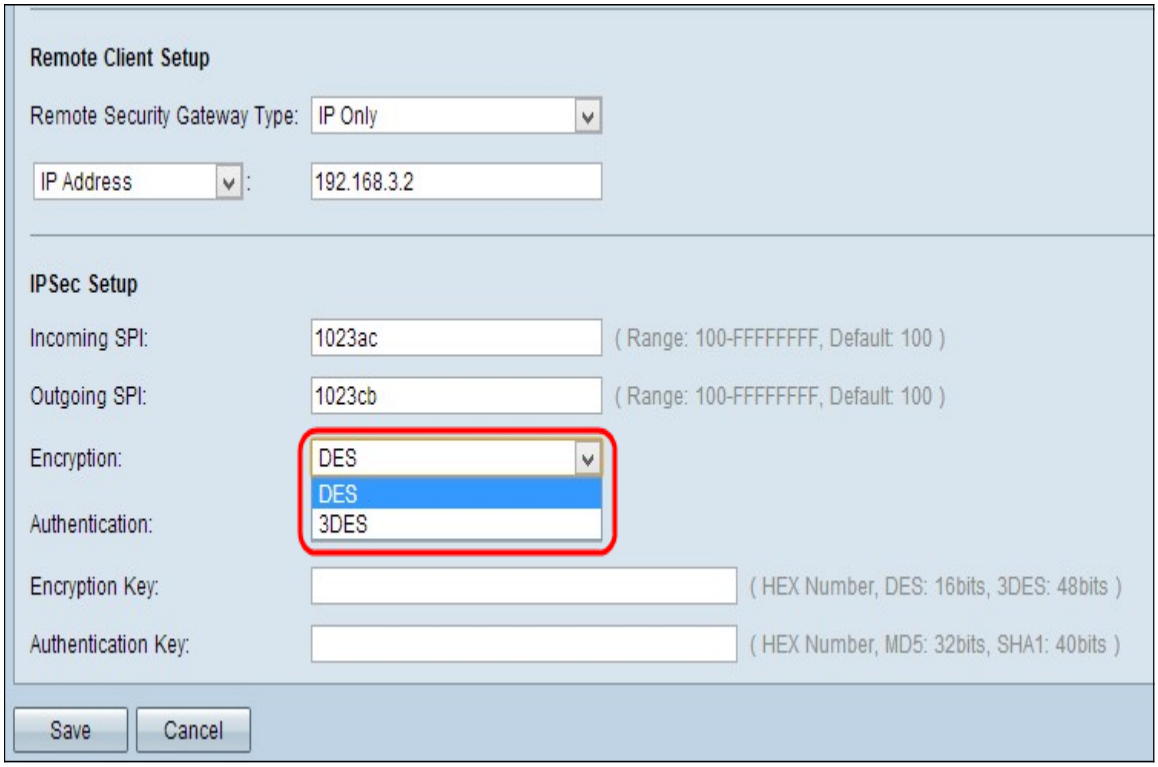
참고: Add a New Tunnel 섹션의 3단계의 *Keying Mode* 드롭다운 목록에서 Manual을 선택한 경우 아래 단계를 수행합니다.



1단계. 수신 SPI 필드에 들어오는 SPI(Security Parameter Index)에 대한 고유한 16진수 값을 입력합니다.SPI는 ESP(Encapsulating Security Payload Protocol) 헤더에 전달되며, 이 헤더는 함께 들어오는 패킷의 SA(Security Association)를 결정합니다.범위는 100에서 ffffff이며 기본값은 100입니다.

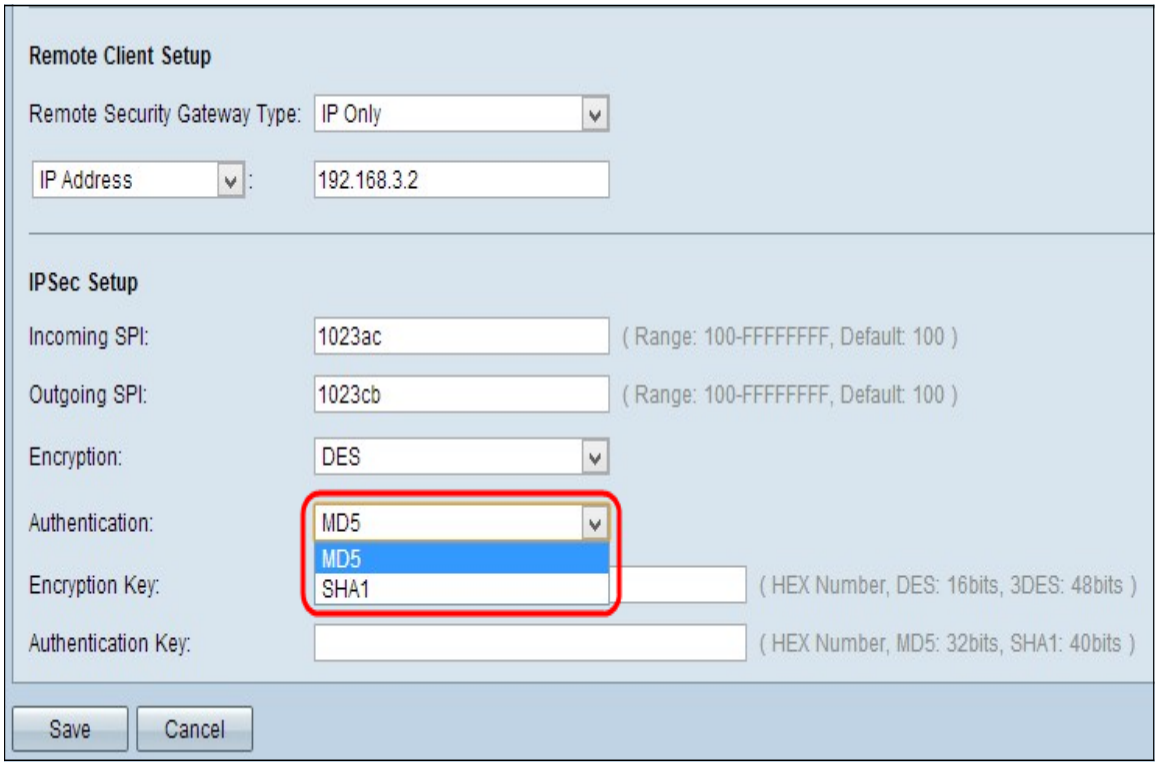
2단계. 나가는 SPI(Security Parameter Index)에 대한 고유한 16진수 값을 *Outgoing SPI* 필드에 입력합니다.SPI는 ESP(Encapsulating Security Payload Protocol) 헤더에 전달되며, 이 헤더는 함께 발신 패킷의 SA(Security Association)를 결정합니다.범위는 100에서 ffffff이며 기본값은 100입니다.

참고:연결된 디바이스의 수신 SPI와 터널의 다른 끝의 발신 SPI가 서로 일치해야 터널을 설정할 수 있습니다.



3단계. Encryption(암호화) 드롭다운 목록에서 적절한 암호화 방법을 선택합니다.권장되는 암호화는 3DES입니다.VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

- DES - DES(Data Encryption Standard)는 56비트, 이전 버전보다 호환성이 높은 이전 버전과의 암호화 방식이며 안전하지 않습니다.
- 3DES - 3DES(Triple Data Encryption Standard)는 168비트의 간단한 암호화 방법으로, 데이터를 3회 암호화하여 DES보다 더 많은 보안을 제공합니다.

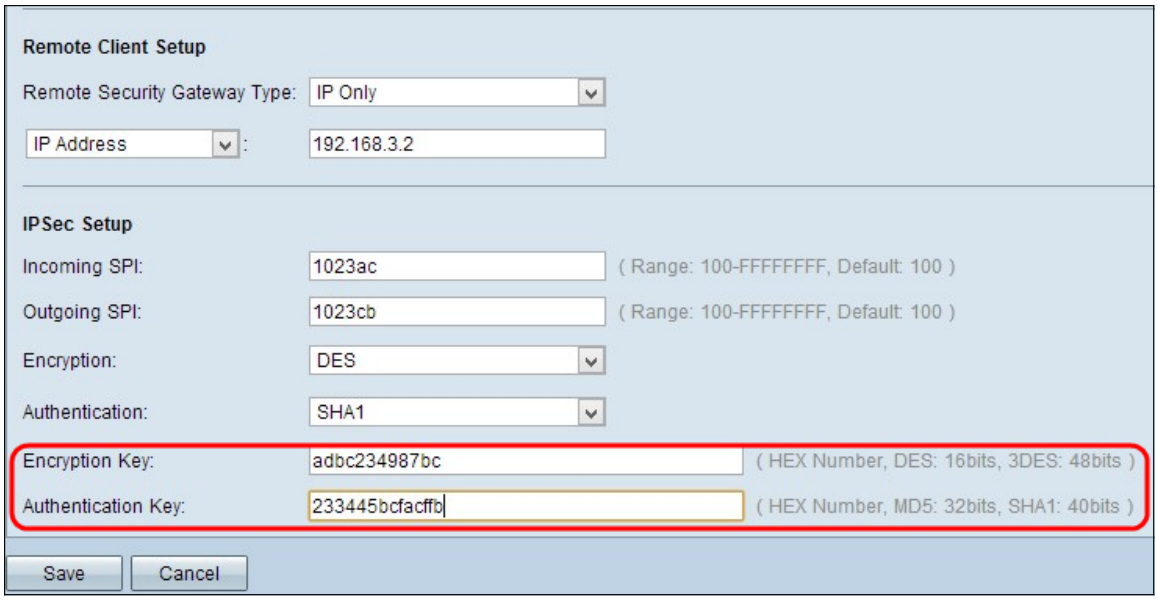


4단계. *Authentication* 드롭다운 목록에서 적절한 인증 방법을 선택합니다.권장되는 인증은 SHA1입니다. VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

- MD5 - MD5(Message Digest Algorithm-5)는 체크섬 계산에 의해 악의적인 공격으로부터 데이

터를 보호하는 32자리 16진수 해시 함수를 나타냅니다.

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



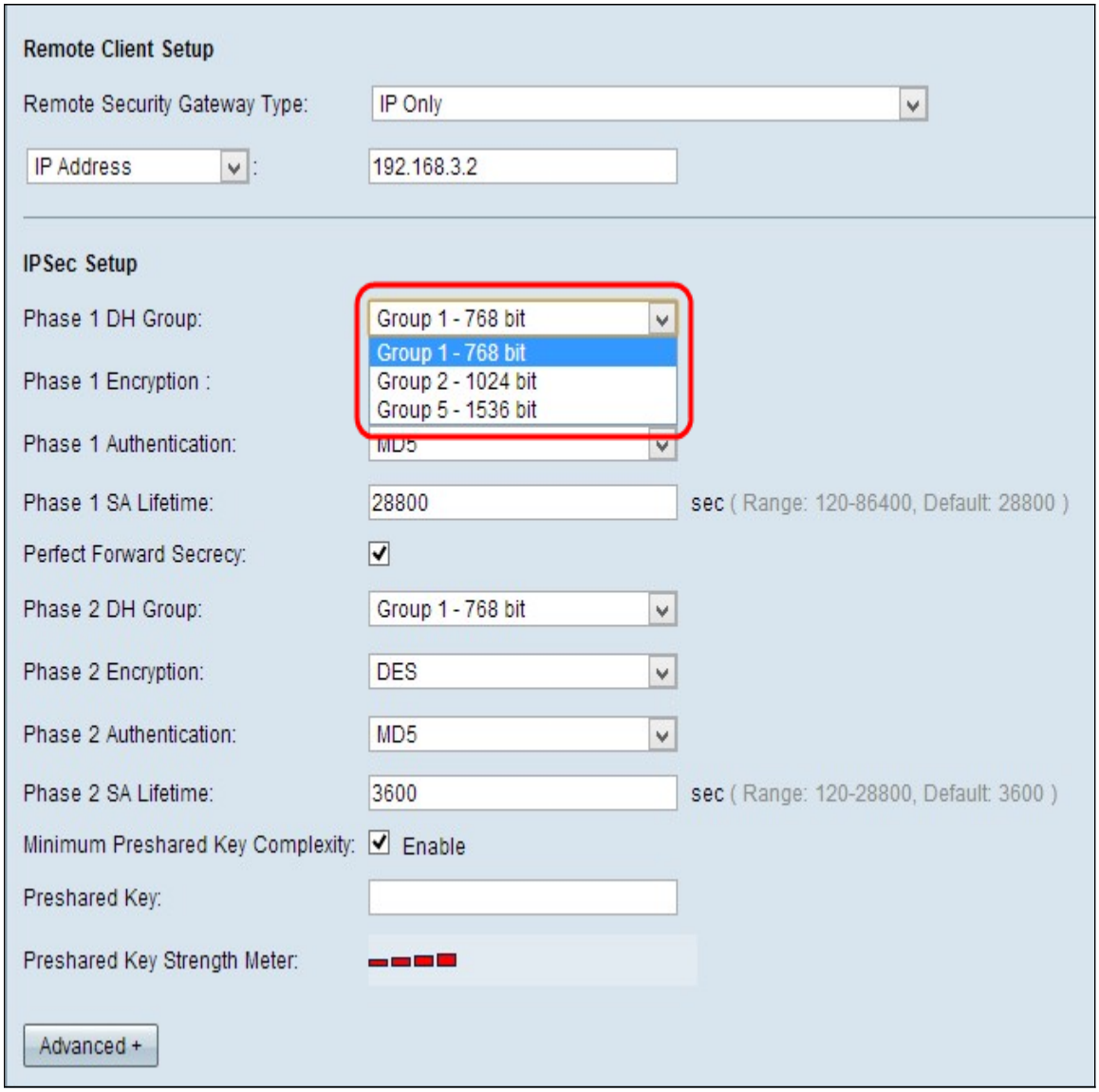
5단계. 암호화 키 필드에 데이터를 암호화하고 해독할 키를 *입력합니다*.3단계에서 DES를 암호화 방법으로 선택한 경우 16자리 16진수 값을 입력합니다.3단계에서 3DES를 암호화 방법으로 선택한 경우 40자리 16진수 값을 입력합니다.

6단계. Authentication *Key* 필드에서 트래픽을 인증하려면 사전 공유 키를 입력합니다.4단계에서 인증 방법으로 MD5를 선택한 경우 32자리 16진수 값을 입력합니다.4단계에서 인증 방법으로 SHA를 선택한 경우 40자리 16진수 값을 입력합니다.VPN 터널은 양쪽 끝에 동일한 사전 공유 키를 사용해야 합니다.

7단계. 현재 설정을 저장하려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

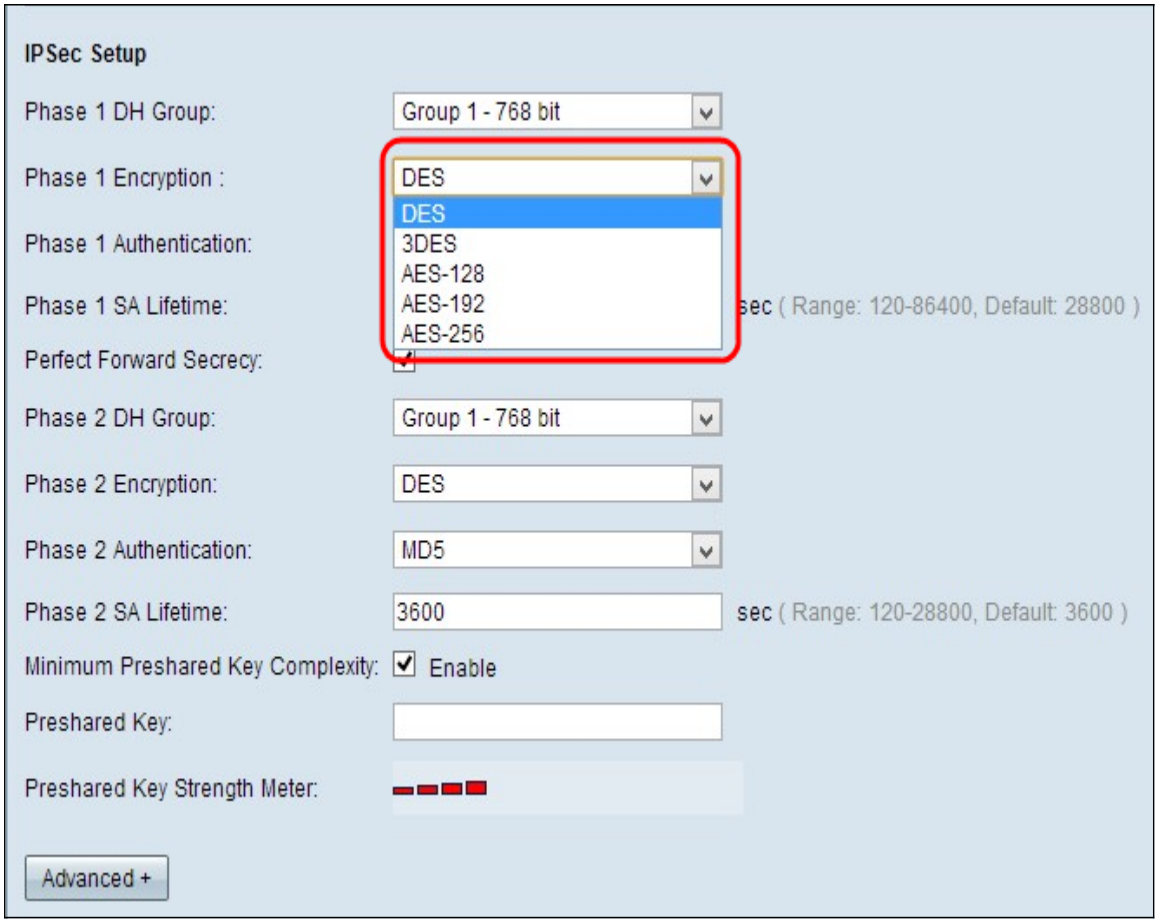
사전 공유 키가 있는 IKE를 통한 IPSec 설정 또는 인증서가 있는 IKE

참고: Add a New Tunnel 섹션의 3단계의 Keying Mode(키 *모드*) 드롭다운 목록에서 IKE with Preshared Key(사전 공유 키가 있는 IKE) 또는 IKE with Certificate(인증서가 있는 IKE)를 선택한 경우 아래 단계*를* 수행합니다.



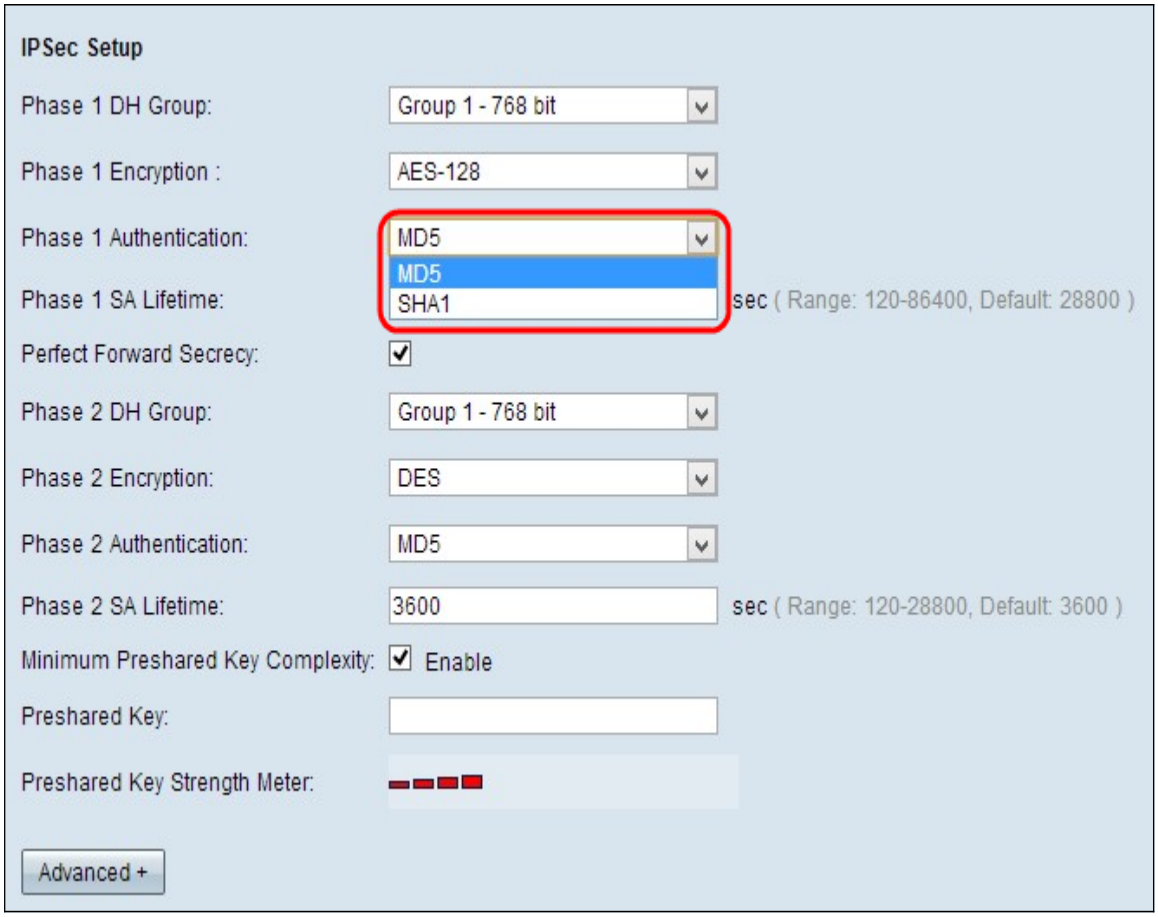
1단계. *Phase 1 DH* Group(*1단계 DH 그룹)* 드롭다운 목록에서 적절한 1단계 DH 그룹을 선택합니다.1단계는 안전한 실제 통신을 지원하기 위해 터널의 양쪽 끝 사이에 단방향 SA(논리적 보안 연결)를 설정하는 데 사용됩니다.DH(Diffie-Hellman)는 통신을 인증하기 위해 1단계 연결 중에 비밀 키를 공유하는 데 사용되는 암호화 키 교환 프로토콜입니다.

- Group 1 - 768비트 - 가장 낮은 강도 키 및 가장 안전하지 않은 인증 그룹을 나타냅니다.그러나 IKE 키를 계산하는 데 시간이 덜 걸립니다.네트워크 속도가 낮으면 이 옵션을 사용하는 것이 좋습니다.
- Group 2 - 1024비트 - 더 높은 강도 키 및 더 안전한 인증 그룹을 나타냅니다.하지만 IKE 키를 계산하려면 시간이 좀 필요합니다.
- Group 5 - 1536비트 - 가장 높은 강도 키 및 가장 안전한 인증 그룹을 나타냅니다.IKE 키를 계산하려면 더 많은 시간이 필요합니다.네트워크 속도가 높으면 이 옵션을 사용하는 것이 좋습니다.



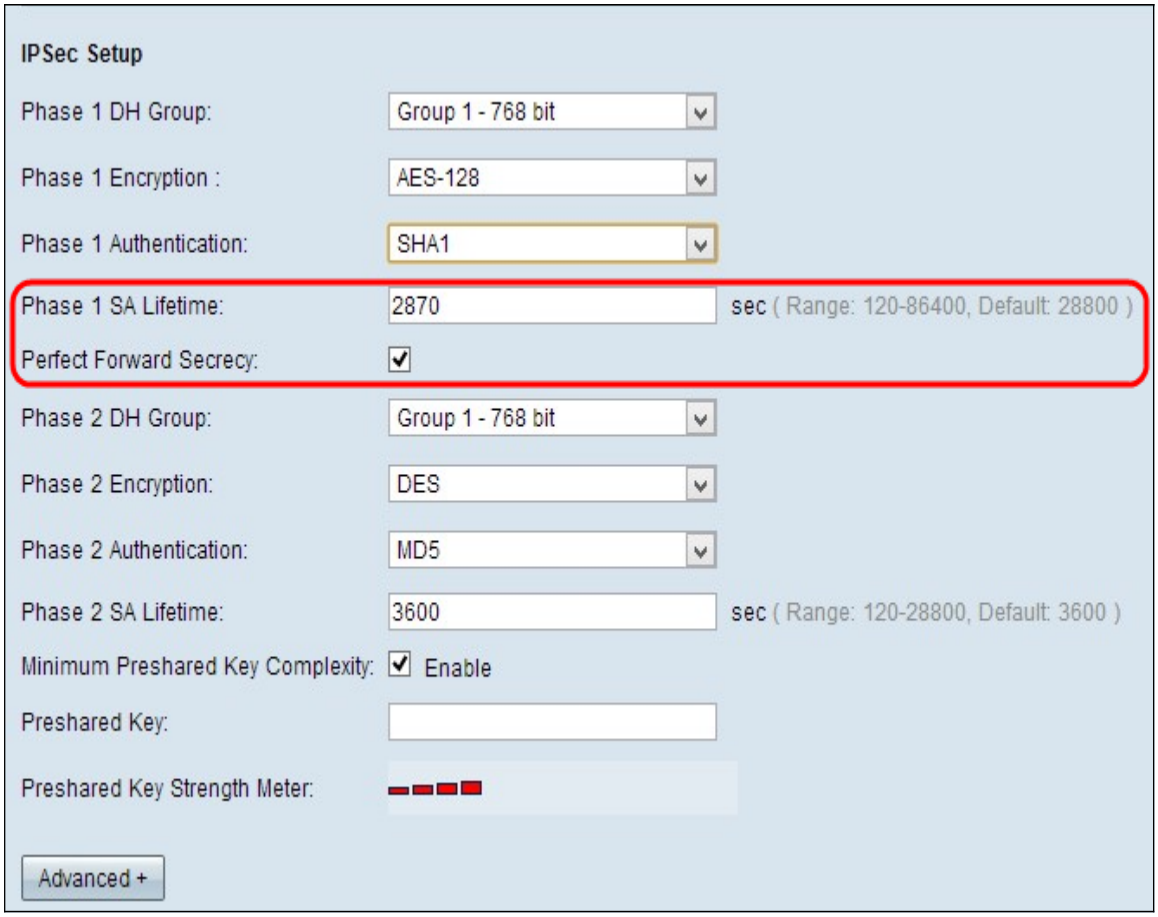
2단계. Phase 1 Encryption(1단계 암호화) 드롭다운 목록에서 키를 암호화하기 위해 적절한 Phase 1 Encryption(1단계 암호화)을 선택합니다.AES-256은 가장 안전한 암호화 방법이므로 권장됩니다.VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

- DES - DES(Data Encryption Standard)는 56비트 이전 암호화 방법이며 그다지 안전한 암호화 방법이 아닙니다.
- 3DES - 3DES(Triple Data Encryption Standard)는 168비트의 간단한 암호화 방법으로, 데이터를 3회 암호화하여 DES보다 더 많은 보안을 제공합니다.
- AES-128 - AES(Advanced Encryption Standard)는 128비트 암호화 방법으로 일반 텍스트를 암호 텍스트로 변환하여 반복 주기를 10회 단축합니다.
- AES-192 - AES(Advanced Encryption Standard)는 192비트 암호화 방법으로 일반 텍스트를 암호 텍스트로 변환하여 반복 주기를 12회 반복합니다.
- AES-256 - AES(Advanced Encryption Standard)는 256비트 암호화 방법으로 일반 텍스트를 암호 텍스트로 변환하여 14사이클의 반복을 수행합니다.



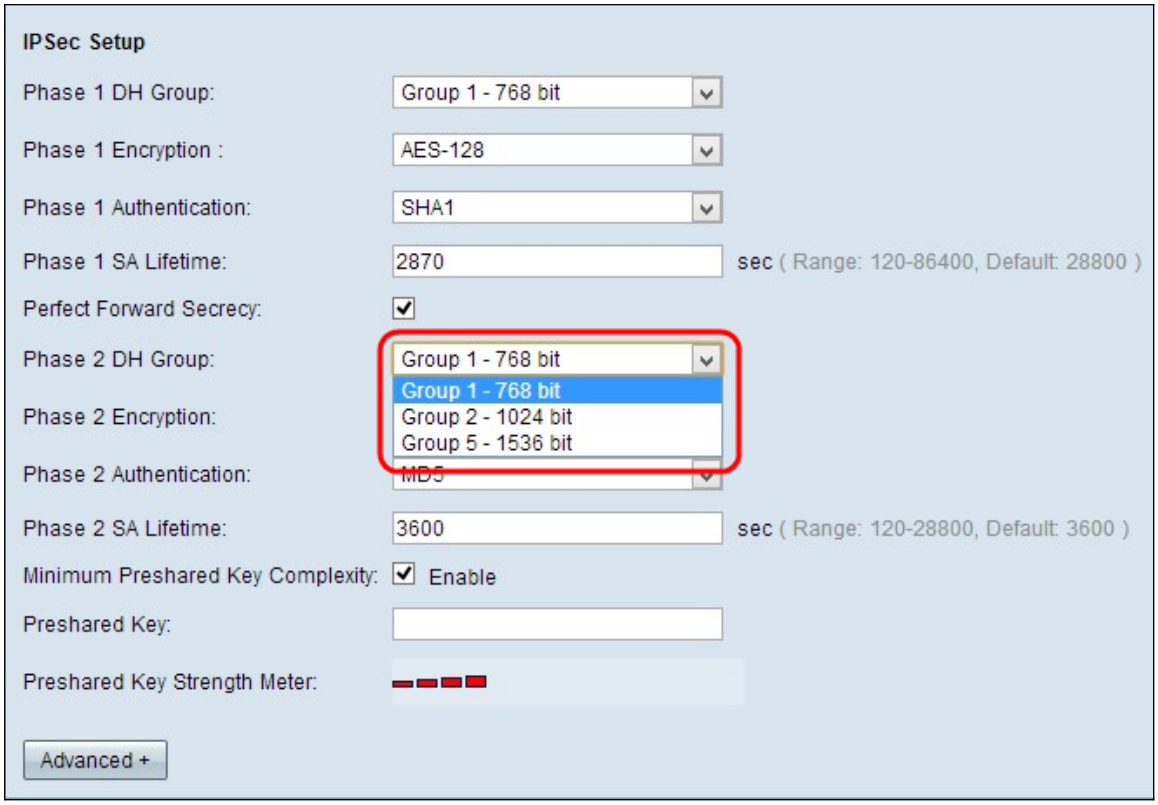
3단계. *Phase 1 Authentication* 드롭다운 목록에서 적절한 인증 방법을 선택합니다.VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

- MD5 - MD5(Message Digest Algorithm-5)는 체크섬 계산에 의해 악의적인 공격으로부터 데이터를 보호하는 32자리 16진수 해시 함수를 나타냅니다.
- SHA1 - SHA1(Secure Hash Algorithm version 1)은 MD5보다 더 안전한 160비트 해시 함수입니다.



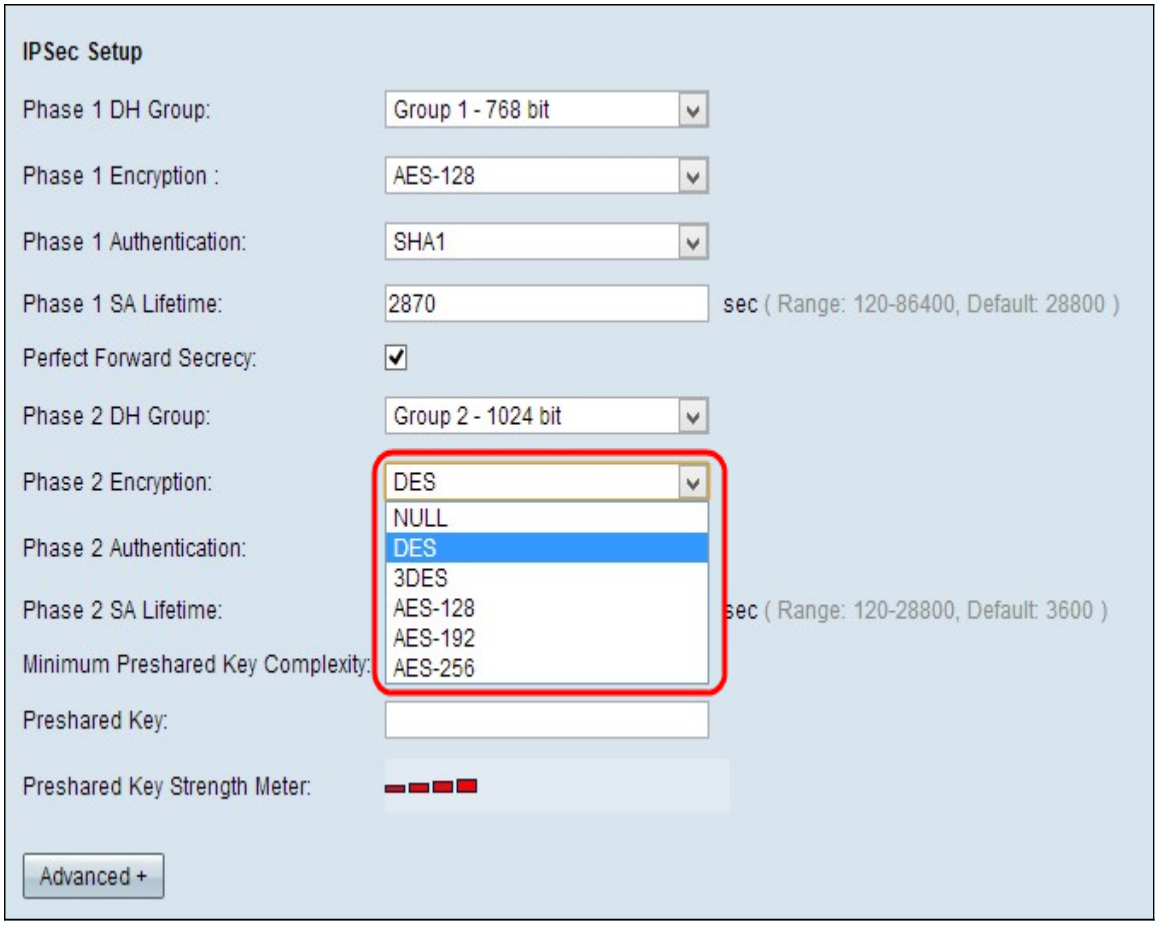
4단계. 1단계에서 VPN 터널이 Phase *1 SA Lifetime* 필드에서 활성 상태로 유지되는 시간(초)을 입력합니다. 기본 시간은 28800초입니다.

5단계. **Perfect Forward Secrecy** 확인란을 선택하여 키를 더 안전하게 보호합니다.이 옵션을 사용하면 키가 손상된 경우 새 키를 생성할 수 있습니다.암호화된 데이터는 감염된 키를 통해서만 감염됩니다.따라서 키가 손상되더라도 다른 키를 보호하므로 보다 안전하게 통신을 인증하고 인증합니다.이는 더 많은 보안을 제공하기 때문에 권장되는 작업입니다.



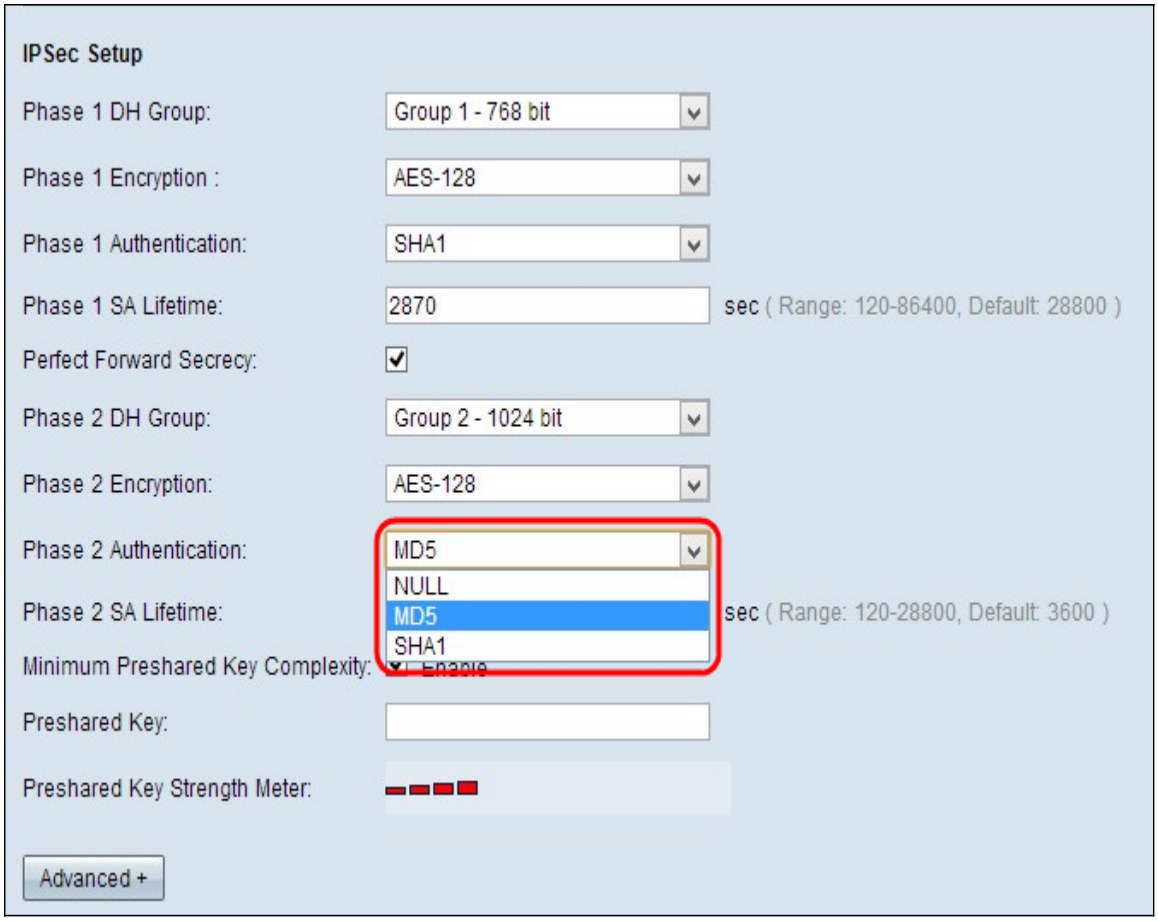
6단계. Phase *2 DH Group* 드롭다운 목록에서 적절한 Phase 2 DH Group을 선택합니다.1단계는 안전한 인증 통신을 지원하기 위해 터널의 양쪽 끝 사이에 단방향 SA(논리적 보안 연결)를 설정하는 데 사용됩니다.DH(Diffie-Hellman)는 통신을 인증하기 위해 1단계 연결 중에 비밀 키를 공유하는 데 사용되는 암호화 키 교환 프로토콜입니다.

- Group 1 - 768비트 - 가장 낮은 강도 키 및 가장 안전하지 않은 인증 그룹을 나타냅니다.그러나 IKE 키를 계산하는 데 시간이 덜 걸립니다.네트워크 속도가 낮으면 이 옵션을 사용하는 것이 좋습니다.
- Group 2 - 1024비트 - 더 높은 강도 키 및 더 안전한 인증 그룹을 나타냅니다.하지만 IKE 키를 계산하려면 시간이 좀 필요합니다.
- Group 5 - 1536비트 - 가장 높은 강도 키 및 가장 안전한 인증 그룹을 나타냅니다.IKE 키를 계산하려면 더 많은 시간이 필요합니다.네트워크 속도가 높으면 이 옵션을 사용하는 것이 좋습니다.



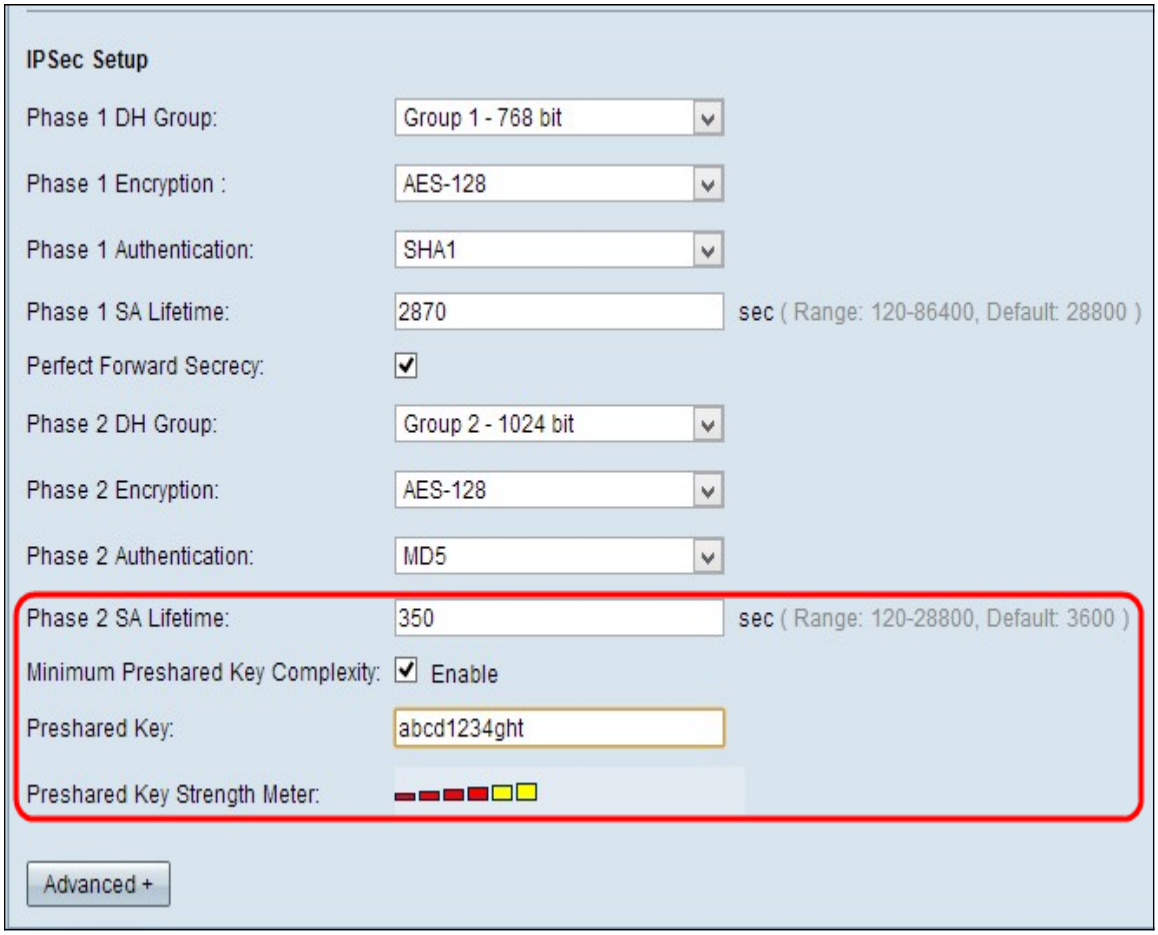
7단계. Phase 2 Encryption(*2단계 암호화)* 드롭다운 목록에서 키를 암호화하려면 적절한 Phase 2 Encryption(2단계 암호화)을 선택합니다.AES-256은 가장 안전한 암호화 방법이므로 권장됩니다.VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

- DES - DES(Data Encryption Standard)는 56비트 이전 암호화 방법이며 그다지 안전한 암호화 방법이 아닙니다.
- 3DES - 3DES(Triple Data Encryption Standard)는 168비트의 간단한 암호화 방법으로, 데이터를 3회 암호화하여 DES보다 더 많은 보안을 제공합니다.
- AES-128 - AES(Advanced Encryption Standard)는 128비트 암호화 방법으로 일반 텍스트를 암호 텍스트로 변환하여 10회 반복됩니다.
- AES-192 - AES(Advanced Encryption Standard)는 192비트 암호화 방법으로 일반 텍스트를 암호 텍스트로 변환하여 12회 반복됩니다.
- AES-256 - AES(Advanced Encryption Standard)는 256비트 암호화 방법으로 일반 텍스트를 암호 텍스트로 변환하여 14회 반복됩니다.



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

- MD5 - MD5(Message Digest Algorithm-5)는 체크섬 계산에 의해 악의적인 공격으로부터 데이터를 보호하는 32자리 16진수 해시 함수를 나타냅니다.
- SHA1 - SHA1(Secure Hash Algorithm version 1)은 MD5보다 더 안전한 160비트 해시 함수입니다.
- Null - 인증 방법이 사용되지 않습니다.



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

10단계. 사전 공유 키에 **대해 강도** 측정기를 활성화하려면 Minimum Preshared Key Complexity 확인란을 선택합니다.

11단계. 이전에 IKE 피어 간에 공유된 키를 Preshared *Key* 필드에 입력합니다.최대 30자의 영숫자를 사전 공유 키로 사용할 수 있습니다.VPN 터널은 양쪽 끝에 동일한 사전 공유 키를 사용해야 합니다.

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

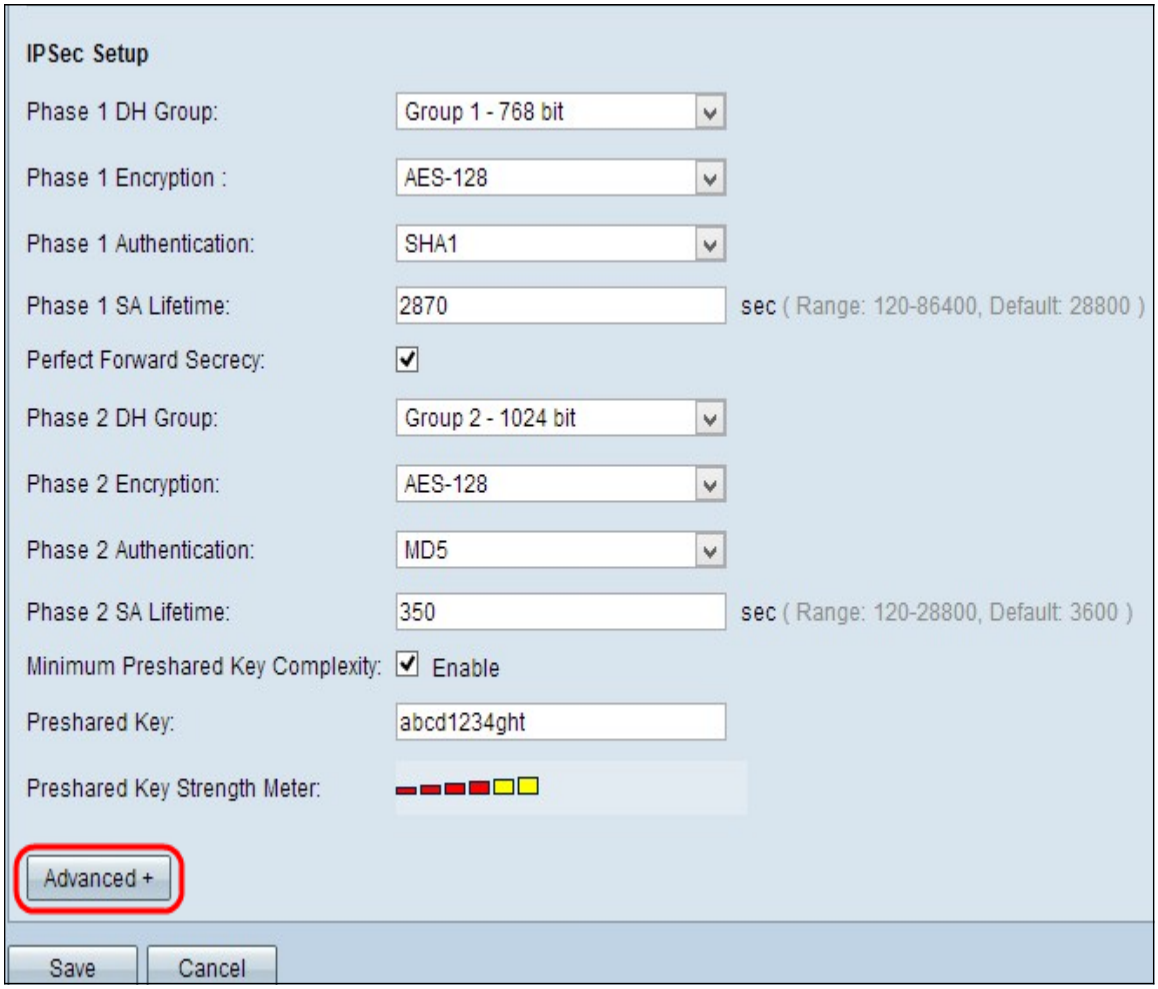
- 사전 공유 키 강도 측정기 - 색상 막대를 통해 사전 공유 키의 강도를 표시합니다.빨간색은 약한 강도를 나타내고, 노란색은 적정 강도를 나타내고, 녹색은 강한 힘을 나타냅니다.IPSec 설정 10단계**에서 Minimum Preshared Key Complexity** 확인란을 선택하면 Preshared Key Strength Meter만 표시됩니다.

참고: Add a New Tunnel(새 터널 추가) 섹션에 대해 3단계의 Keying Mode(키잉 *모드)* 드롭다운 목록에서 Preshared Key(사전 공유 키)를 선택한 경우, 11단계 10을 구성하고 Preshared Key Strength Meter(사전 공유 키 강도 측정기)를 보는 옵션만 사용할 수 있습니다.

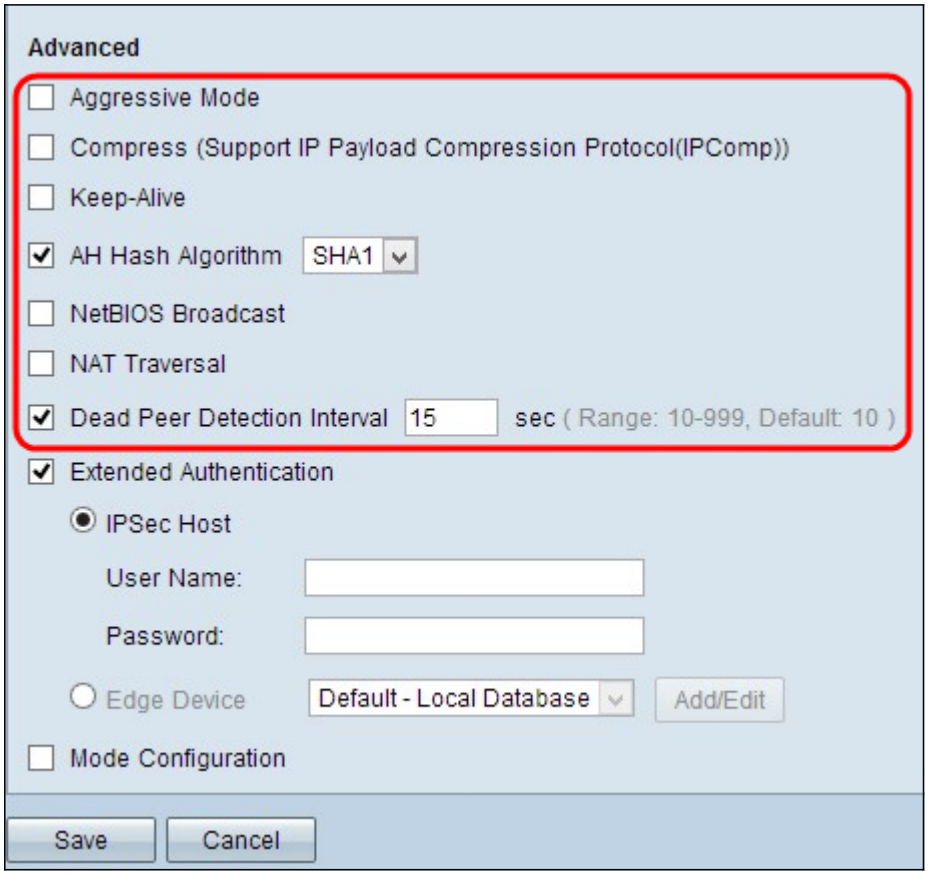
12단계. 현재 설정을 저장하려면 아래로 스크롤하여 **저장**을 클릭하여 설정을 저장합니다.

사전 공유 키가 있는 IKE 또는 인증서가 있는 IKE를 사용한 고급 설정

고급 설정은 사전 공유 키가 있는 IKE 및 인증 키가 있는 IKE에만 사용할 수 있습니다.수동 키 설정에 고급 설정이 없습니다.



1단계. Advanced(**고급**)를 클릭하여 Preshared 키가 있는 IKE에 대한 고급 설정을 가져옵니다
.



2단계. 네트워크 속도가 낮으면 **Aggressive Mode** 확인란을 선택합니다.SA를 연결하는 동안 터널의 엔드포인트의 ID를 일반 텍스트로 교환하므로 교환 시간은 적지만 보안은 낮습니다.

3단계. IP 데이터그램의 크기를 압축하려면 **Compress (Support IP Payload Compression Protocol (IPComp))** 확인란을 선택합니다.IPComp는 IP 데이터그램의 크기를 압축하는 데 사용되는 IP 압축 프로토콜입니다. 네트워크 속도가 낮고 사용자가 저속 네트워크를 통해 손실 없이 신속하게 데이터를 전송하려는 경우,

4단계. VPN 터널 연결을 항상 활성 상태로 유지하려면 Keep-Alive 확인란을 선택합니다.연결이 비활성화되면 즉시 연결을 재설정할 수 있습니다.

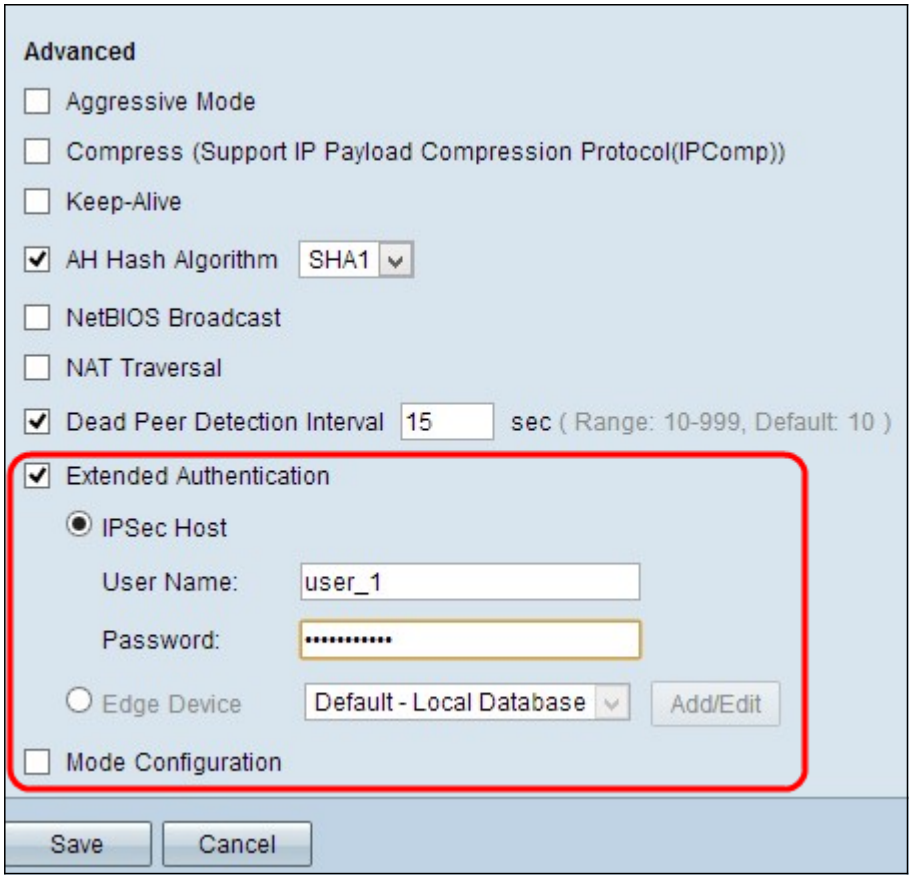
5단계. AH(Authenticate Header)를 인증하려면 **AH Hash Algorithm** 확인란을 선택합니다 .AH는 데이터 원본에 대한 인증을 제공하며, 체크섬 및 보호를 통한 데이터 무결성은 IP 헤더로 확장됩니다.터널의 양쪽 알고리즘은 동일해야 합니다.

- MD5 - MD5(Message Digest Algorithm-5)는 128자리 16진수 해시 함수를 나타내며, 이는 체크섬 계산에 의해 악의적인 공격으로부터 데이터를 보호합니다.
- SHA1 - SHA1(Secure Hash Algorithm version 1)은 MD5보다 더 안전한 160비트 해시 함수입니다.

6단계. VPN 터널을 통해 라우팅 불가능한 트래픽을 허용하려면 NetBIOS 브로드캐스트를 확인합니다.기본값은 선택되지 않습니다.NetBIOS는 일부 소프트웨어 애플리케이션 및 Network Neighbor와 같은 Windows 기능을 통해 네트워크의 프린터, 컴퓨터 등의 네트워크 리소스를 탐지하는 데 사용됩니다.

7단계. 프라이빗 LAN에서 공용 IP 주소를 통해 인터넷에 액세스하려면 **NAT Traversal** 확인란을 선택합니다.NAT 통과는 악성 공격 또는 검색으로부터 사설 IP 주소를 보호하기 위해 내부 시스템의 사설 IP 주소를 공용 IP 주소로 표시하는 데 사용됩니다.

8단계. Dead **Peer Detection Interval(데드 피어 탐지 간격)**을 확인하여 Hello 또는 ACK를 통해 VPN 터널의 수명을 정기적으로 확인합니다.이 확인란을 선택하는 경우 원하는 hello 메시지의 기간 또는 간격을 입력합니다.



9단계. VPN 연결**에** 더 많은 보안 및 인증을 제공하려면 Extended Authentication(확장 인증)을 선택합니다.적절한 라디오 버튼을 클릭하여 VPN 연결 인증을 확장합니다.

- IPSec 호스트 - IPSec 호스트를 통한 확장 인증.이 옵션을 선택하는 경우 User Name(사용자 이름) 필드에 IPSec 호스트의 사용자 이름과 Password(비밀번호) 필드에 비밀번호를 입력합니다.
- 에지 디바이스 - 에지 디바이스를 통한 확장 인증이 옵션을 선택하는 경우 드롭다운 목록에서 에지 디바이스가 포함된 데이터베이스를 선택합니다.데이터베이스를 추가하거나 편집하려면 **추가/편집**을 클릭합니다.

참고:로컬 데이터베이스를 추가하거나 편집하는 방법에 대한 자세한 내용은 RV*320 라우터의 User and Domain Management Configuration(사용자 및 도메인 관리 구성)을 참조하십시오.*

10단계.수신 터널 요청자의 IP 주소를 제공하려면 Mode Configuration을 선택합니다.

참고:9단계부터 11단계까지 터널 VPN에 대한 IKE Preshared Keying Mode(IKE 사전 공유 키 설정 모드)에 사용할 수 있습니다.

11단계. **저장**을 클릭하여 설정을 저장합니다.

결론

이제 RV32x Series VPN Router에서 단일 클라이언트에서 게이트웨이 VPN을 구성하는 단계를 배웠습니다.

이 문서와 관련된 비디오 보기...

여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.