RV130 또는 RV130W 라우터에서 Advanced Virtual Private Network(VPN) 설정 구성

목표

VPN(Virtual Private Network)은 네트워크 내에서 또는 네트워크 간에 설정되는 보안 연결입니다. VPN은 지정된 호스트와 네트워크 간의 트래픽을 인증되지 않은 호스트와 네트워크의 트래픽으로부터 격리합니다. Site-to-Site(게이트웨이-게이트웨이) VPN은 전체 네트워크를 서로 연결하여 인터넷이라고 하는 공용 도메인을 통해 터널을 생성하여 보안을 유지합니다. 각 사이트는 동일한 공용 네트워크에 대한 로컬 연결만 필요하므로 긴 전용 임대 회선에서 비용-절약할 수 있습니다.

VPN은 확장성이 뛰어나고, 네트워크 토폴로지를 단순화하며, 원격 사용자의 이동 시간과 비용을 줄여 생산성을 개선하는 등 기업에 유용합니다.

IKE(Internet Key Exchange)는 VPN에서 통신을 위한 보안 연결을 설정하는 데 사용되는 프로토콜입니다. 이러한 보안 연결을 SA(Security Association)라고 합니다. 피어 인증, 암호화 알고리즘 등 이 프로세스에서 사용할 보안 매개변수를 정의하기 위해 IKE 정책을 생성할 수 있습니다. VPN이 제대로 작동하려면 두 엔드포인트의 IKE 정책이 동일해야 합니다.

이 문서에서는 IKE 정책 설정 및 VPN 정책 설정을 다루는 RV130 또는 RV130W 라우터에서 Advanced VPN Setup을 구성하는 방법을 보여 줍니다.

적용 가능한 장치

·RV130
· RV130W

소프트웨어 버전

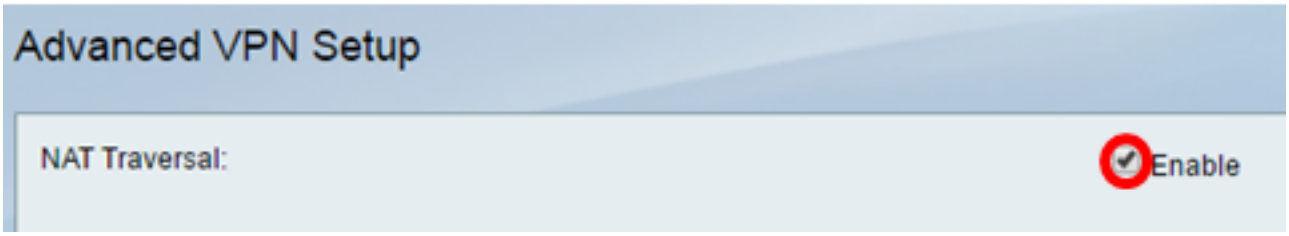
•1.0.3.22

고급 VPN 설정 구성

IKE(인터넷 키 교환) 정책 설정 추가/편집

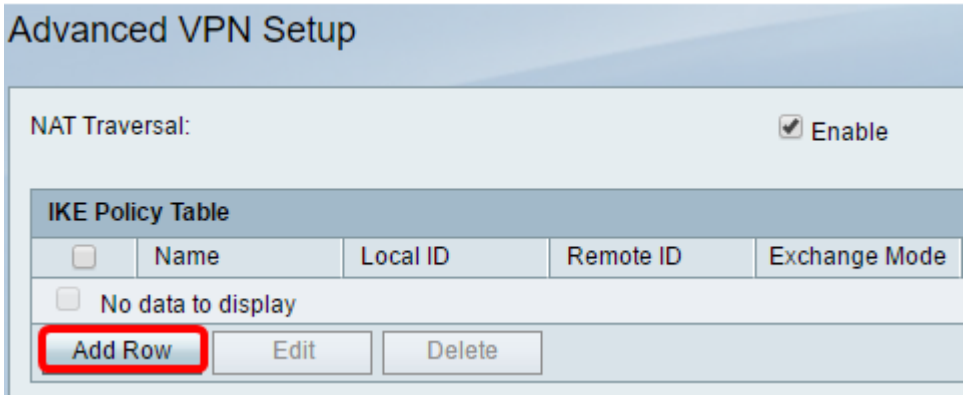
1단계. 웹 기반 유틸리티에 로그인하고 **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup을 선택합니다**.

2단계(선택 사항) VPN 연결에 대해 NAT(Network Address Translation) Traversal을 활성화하려면 NAT Traversal에서 Enable 확인란을 선택합니다. NAT 통과를 사용하면 NAT를 사용하는 게이트웨이 간에 VPN 연결을 설정할 수 있습니다. VPN 연결이 NAT 지원 게이트웨이를 통과하는 경우 이 옵션을 선택합니다.



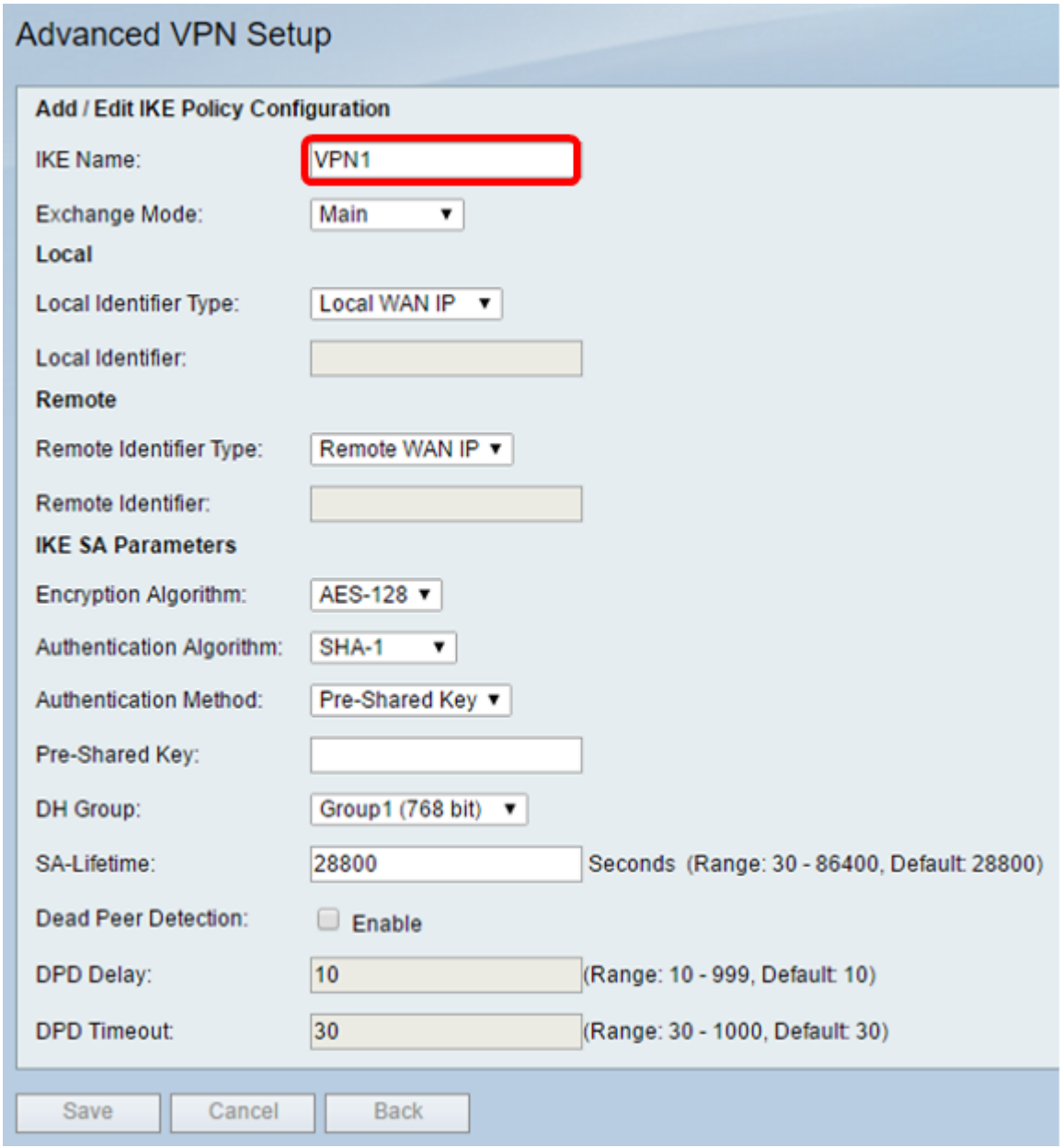
3단계. IKE Policy Table(IKE 정책 테이블)에서 **Add Row(행** 추가)를 클릭하여 새 IKE 정책을 생성합니다.

참고: 기본 설정이 구성된 경우 아래 표에는 생성된 기본 VPN 설정이 포함됩니다. 정책에 대한 확인란을 선택하고 Edit를 클릭하여 기존 IKE 정책을 수정할 수 **있습니다**. Advanced VPN Setup 페이지가 변경됩니다.



4단계. IKE *Name(IKE 이름)* 필드에 IKE 정책의 고유한 이름을 입력합니다.

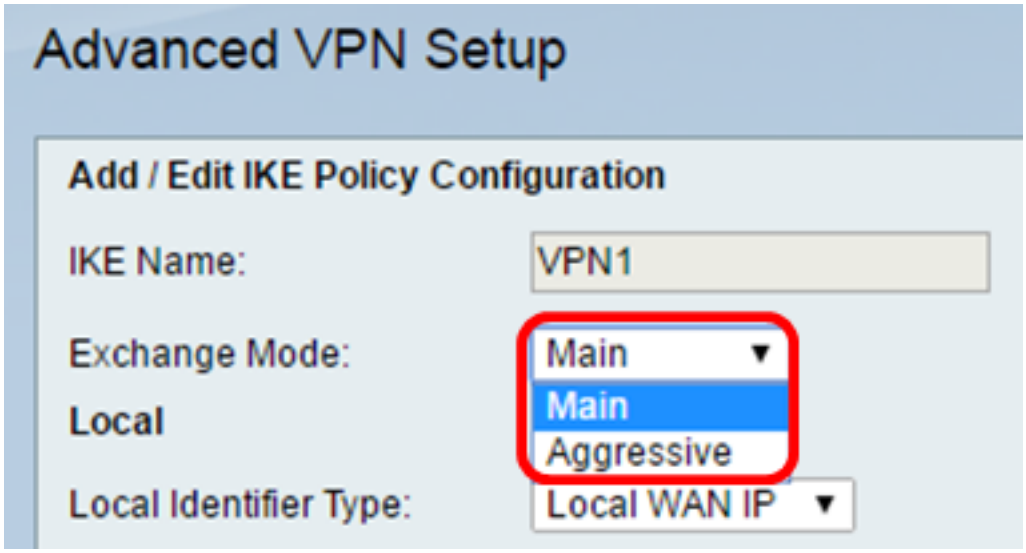
참고: 기본 설정이 구성된 경우 생성된 연결 이름이 IKE 이름으로 설정됩니다. 이 예에서는 VPN1이 선택한 IKE 이름입니다.



5단계. Exchange Mode(교환 모드) 드롭다운 목록에서 옵션을 선택합니다.

- Main — 이 옵션을 사용하면 IKE 정책이 적극적인 모드보다 높은 보안으로 VPN 터널을 협상할 수 있습니다. 더 안전한 VPN 연결이 협상 속도보다 우선적인 경우 이 옵션을 클릭합니다.
- Aggressive(적극적인) - 이 옵션을 사용하면 IKE 정책이 기본 모드보다 빠르지만 덜 안전한 연결을 설정할 수 있습니다. 더 빠른 VPN 연결이 높은 보안보다 우선인 경우 이 옵션을 클릭합니다.

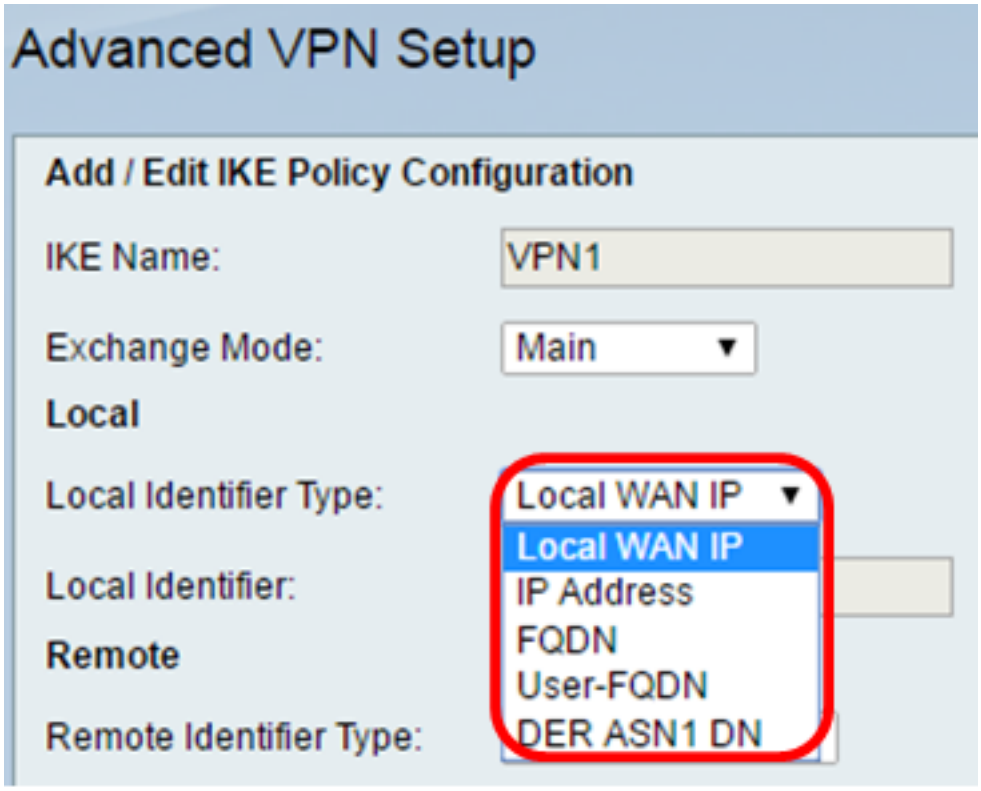
참고: 이 예제에서는 Main을 선택합니다.



6단계. 로컬 식별자 유형 드롭다운 목록에서 선택하여 로컬 라우터의 ISAKMP(Internet Security Association and Key Management Protocol)를 식별하거나 지정합니다. 옵션은 다음과 같습니다.

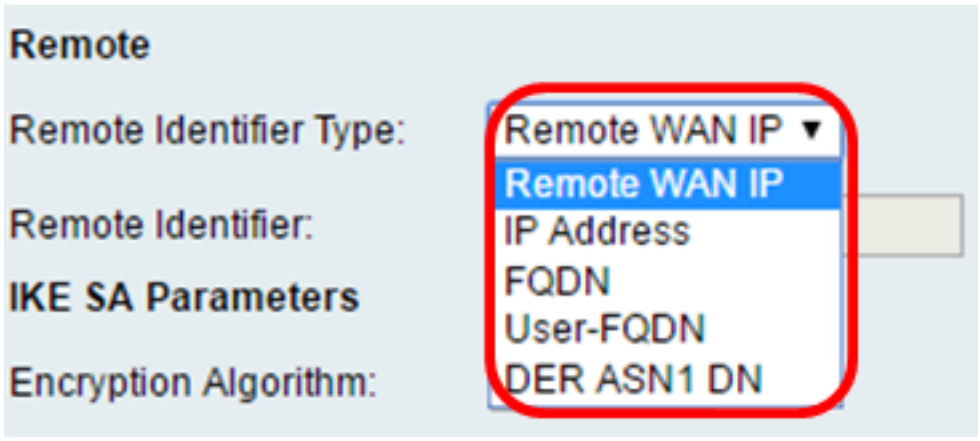
- 로컬 WAN IP — 라우터는 로컬 WAN(Wide Area Network) IP를 기본 식별자로 사용합니다. 이 옵션은 인터넷을 통해 연결됩니다. 이 옵션을 선택하면 아래의 *Local Identifier* 필드가 흐리게 표시됩니다.
- IP Address — 이 필드를 클릭하면 Local Identifier 필드에 IP 주소를 *입력할* 수 있습니다.
- FQDN — FQDN(Fully Qualified Domain Name) 또는 도메인 이름(예: http://www.example.com)을 사용하면 *Local Identifier 필드*에 도메인 이름 또는 IP 주소를 입력할 수 있습니다.
- User-FQDN — 이 옵션은 user@email.com과 같은 사용자 이메일 주소입니다. Local Identifier 필드에 도메인 이름 또는 IP *주소를* 입력합니다.
- DER ASN1 DN — 이 옵션은 DN(Distinguished Name)의 식별자 유형으로, DER ASN1(Distinguished Encoding Rules Abstract Syntax Notation One)을 사용하여 정보를 전송합니다. 이는 VPN 터널이 사용자 인증서와 연결될 때 발생합니다. 이 옵션을 선택한 경우 Local Identifier 필드에 도메인 이름 또는 IP *주소를* 입력합니다.

참고: 이 예에서는 Local WAN IP(로컬 WAN IP)를 선택합니다.



7단계. Remote Identifier Type(원격 식별자 유형) 드롭다운 목록에서 선택하여 원격 라우터의 ISAKMP(Internet Security Association and Key Management Protocol)를 식별하거나 지정합니다. 옵션은 Remote WAN IP(원격 WAN IP), IP Address(IP 주소), FQDN, User FQDN(사용자 FQDN), DER ASN1 DN(DER ASN1 DN)입니다.

참고: 이 예에서는 Remote WAN IP(원격 WAN IP)를 선택합니다.

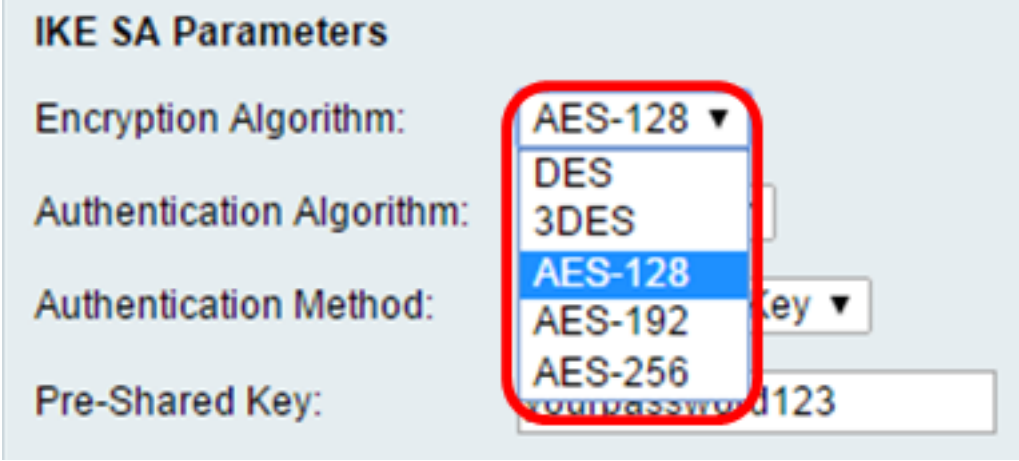


8단계. Encryption Algorithm 드롭다운 목록에서 옵션을 선택합니다.

- DES — DES(Data Encryption Standard)는 매우 안전한 암호화 방법은 아니지만 이전 버전과의 호환성을 위해 필요할 수 있는 56비트 이전 암호화 방법입니다.
- 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 키가 있는 고급 암호화 표준(AES-128)은 AES 암호화에 128비트 키를 사용합니다. AES는 DES보다 빠르고 안전합니다. 일반적으로 AES는 3DES보다 더 빠르고 안전합니다. AES-128은 기본 암호화 알고리즘이며 AES-192 및 AES-256보다 빠르지만 안전하지 않습니다.

- AES-192 — AES-192는 AES 암호화에 192비트 키를 사용합니다. AES-192는 AES-128보다 느리지만 안전하며, AES-256보다 빠르지만 안전하지 않습니다.
- AES-256 — AES-256은 AES 암호화에 256비트 키를 사용합니다. AES-256은 AES-128 및 AES-192보다 느리지만 안전합니다.

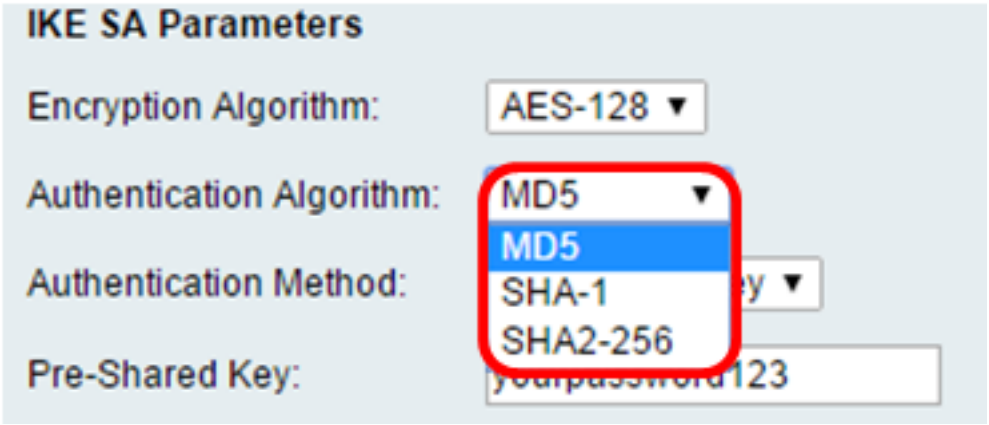
참고: 이 예에서는 AES-128을 선택합니다.



9단계. Authentication Algorithm(인증 알고리즘) 드롭다운 목록에서 다음 옵션 중에서 선택합니다.

- MD5 — MD5(Message Digest 5)는 인증에 128비트 해시 값을 사용하는 인증 알고리즘입니다. MD5는 SHA-1 및 SHA2-256보다 안전하지 않지만 더 빠릅니다.
- SHA-1 — SHA-1(Secure Hash Function 1)은 인증에 160비트 해시 값을 사용합니다. SHA-1은 MD5보다 느리지만 더 안전합니다. SHA-1은 기본 인증 알고리즘이며 SHA2-256보다 빠르지만 덜 안전합니다.
- SHA2-256 — 256비트 해시 값(SHA2-256)이 있는 Secure Hash Algorithm 2는 인증에 256비트 해시 값을 사용합니다. SHA2-256은 MD5 및 SHA-1보다 느리지만 더 안전합니다.

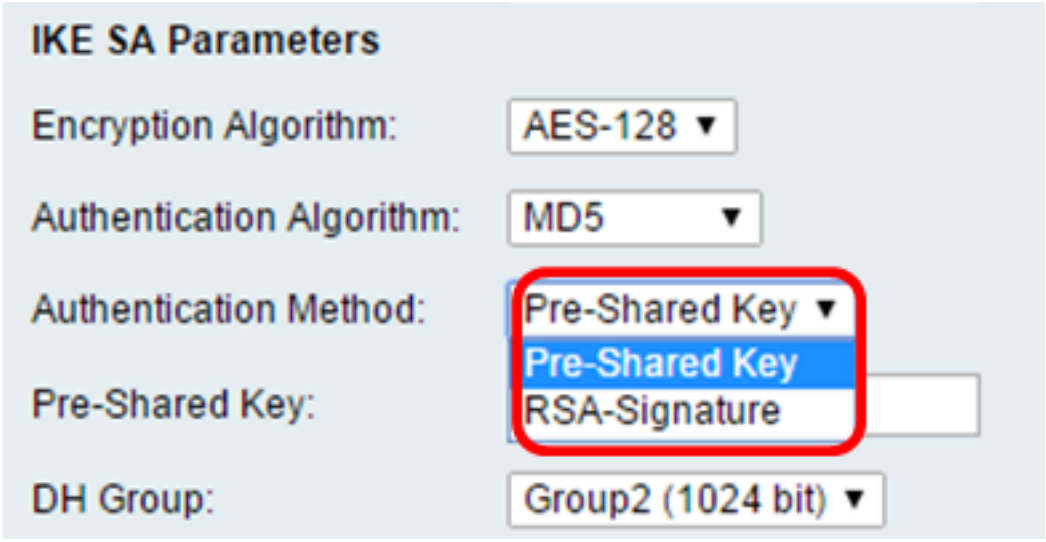
참고: 이 예제에서는 MD5를 선택합니다.



10단계. Authentication Method(인증 방법) 드롭다운 목록에서 다음 옵션 중에서 선택합니다.

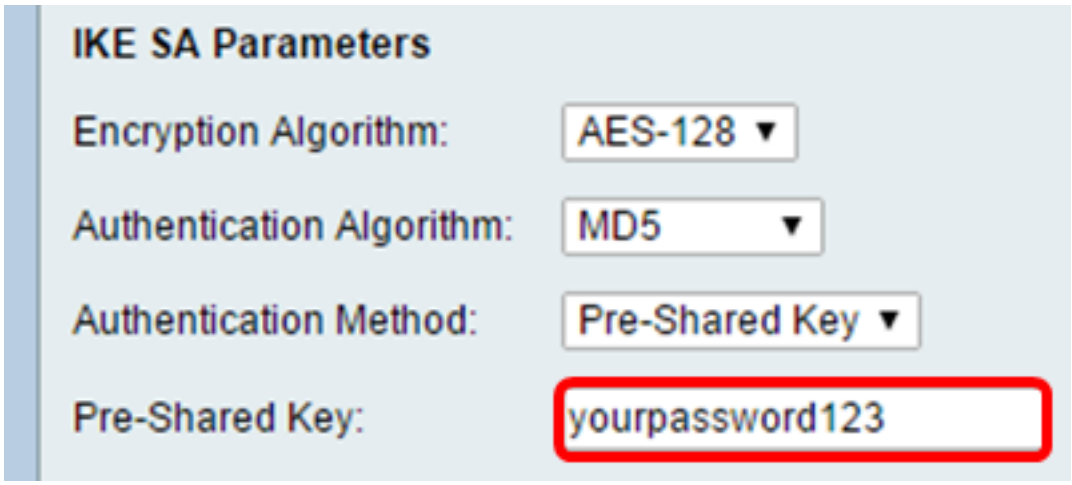
- 사전 공유 키 — 이 옵션을 사용하려면 IKE 피어와 공유하는 비밀번호가 필요합니다.
- RSA-Signature — 이 옵션은 인증서를 사용하여 연결을 인증합니다. 이 옵션을 선택하면 사전 공유 키 필드가 비활성화됩니다. 12단계로 건너뜁니다.

참고: 이 예에서는 사전 공유 키를 선택합니다.



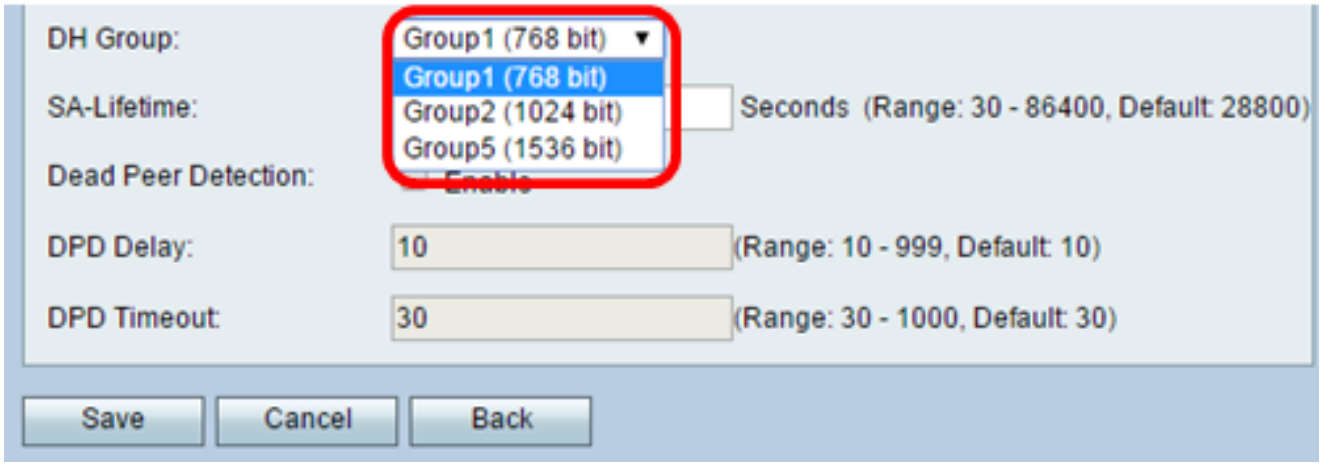
11단계. *Pre-Shared Key(사전 공유 키)* 필드에 8~49자의 비밀번호를 입력합니다.

참고: 이 예에서는 password123이 사용됩니다.

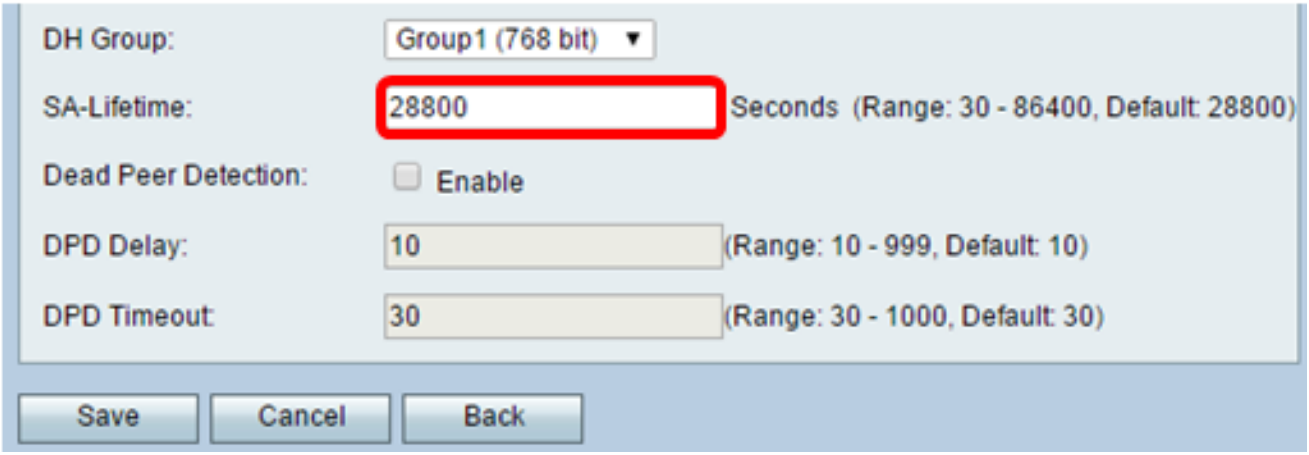


12단계. DH Group(DH 그룹) 드롭다운 목록에서 IKE에서 사용하는 DH(Diffie-Hellman) 그룹 알고리즘을 선택합니다. DH 그룹의 호스트는 서로 모르게 키를 교환할 수 있습니다. 그룹 비트 번호가 높을수록 보안성이 향상됩니다.

참고: 이 예제에서는 Group1을 선택합니다.

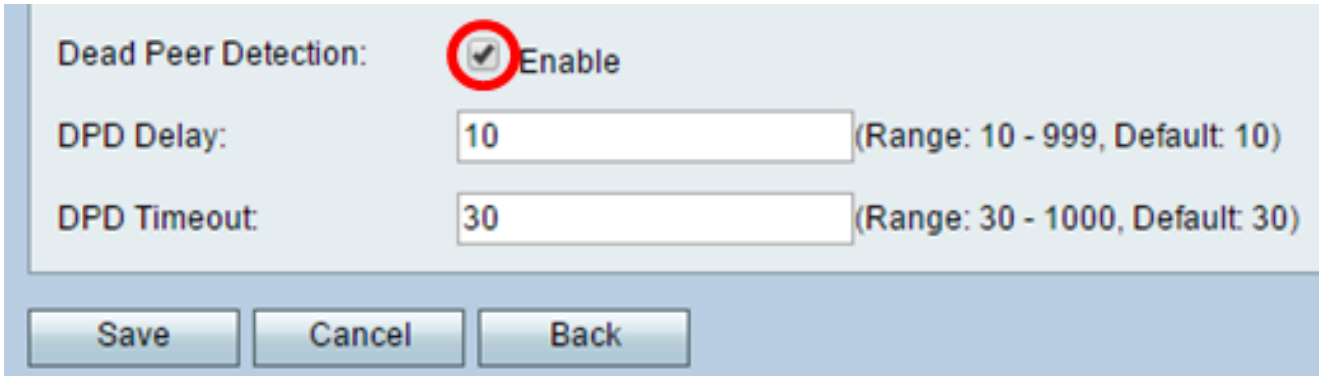


13단계. *SA-Lifetime 필드*에서 SA가 갱신되기 전까지 VPN에 대한 SA가 지속되는 시간을 초 단위로 입력합니다. 범위는 30~86400초입니다. 기본값은 28800입니다.



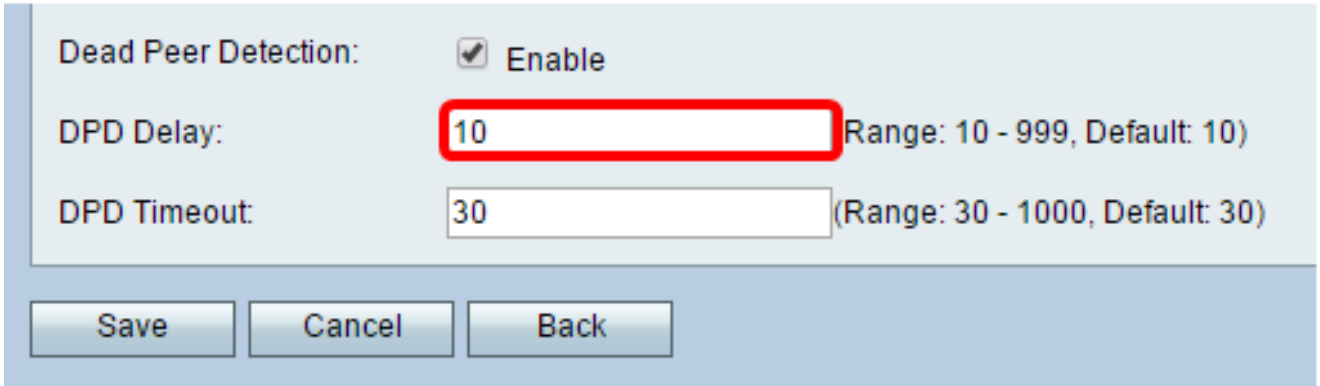
14단계(선택 사항) Enable Dead Peer Detection(**데드** 피어 탐지 활성화) 확인란을 선택하여 DPD(Dead Peer Detection)를 활성화합니다. DPD는 IKE 피어를 모니터링하여 피어가 더 이상 작동하지 않거나 아직 활성 상태인지 확인합니다. 피어가 dead로 감지되면 디바이스는 IPsec 및 IKE 보안 연결을 삭제합니다. DPD는 비활성 피어에서의 네트워크 리소스 낭비를 방지합니다.

참고: Dead Peer Detection을 활성화하지 않으려면 17단계로 건너뜁니다.



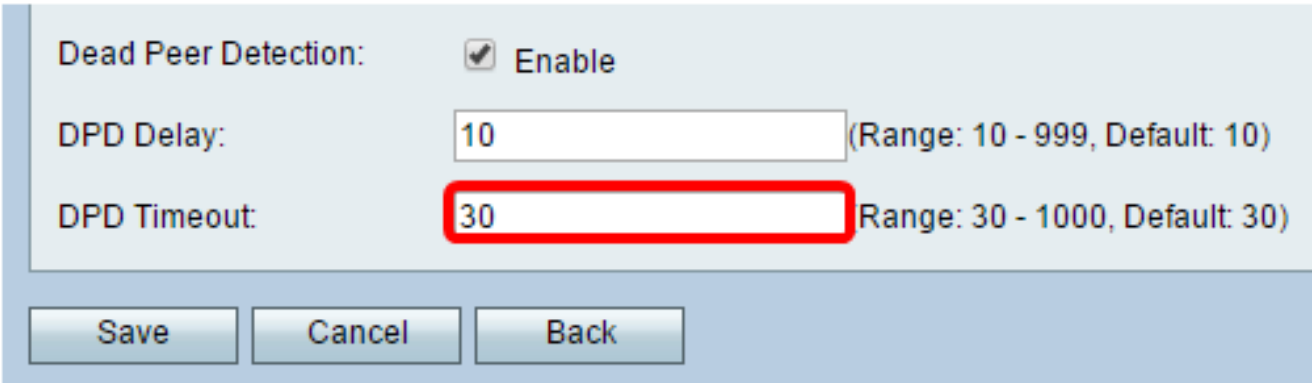
15단계. (선택 사항) 14단계에서 DPD를 활성화한 경우 DPD *Delay 필드*에 피어의 활동을 확인하는 빈도(초)를 입력합니다.

참고: DPD 지연은 연속 DPD R-U-THERE 메시지 간의 간격(초)입니다. DPD R-U-THERE 메시지는 IPsec 트래픽이 유휴 상태일 때만 전송됩니다. 기본값은 10입니다.

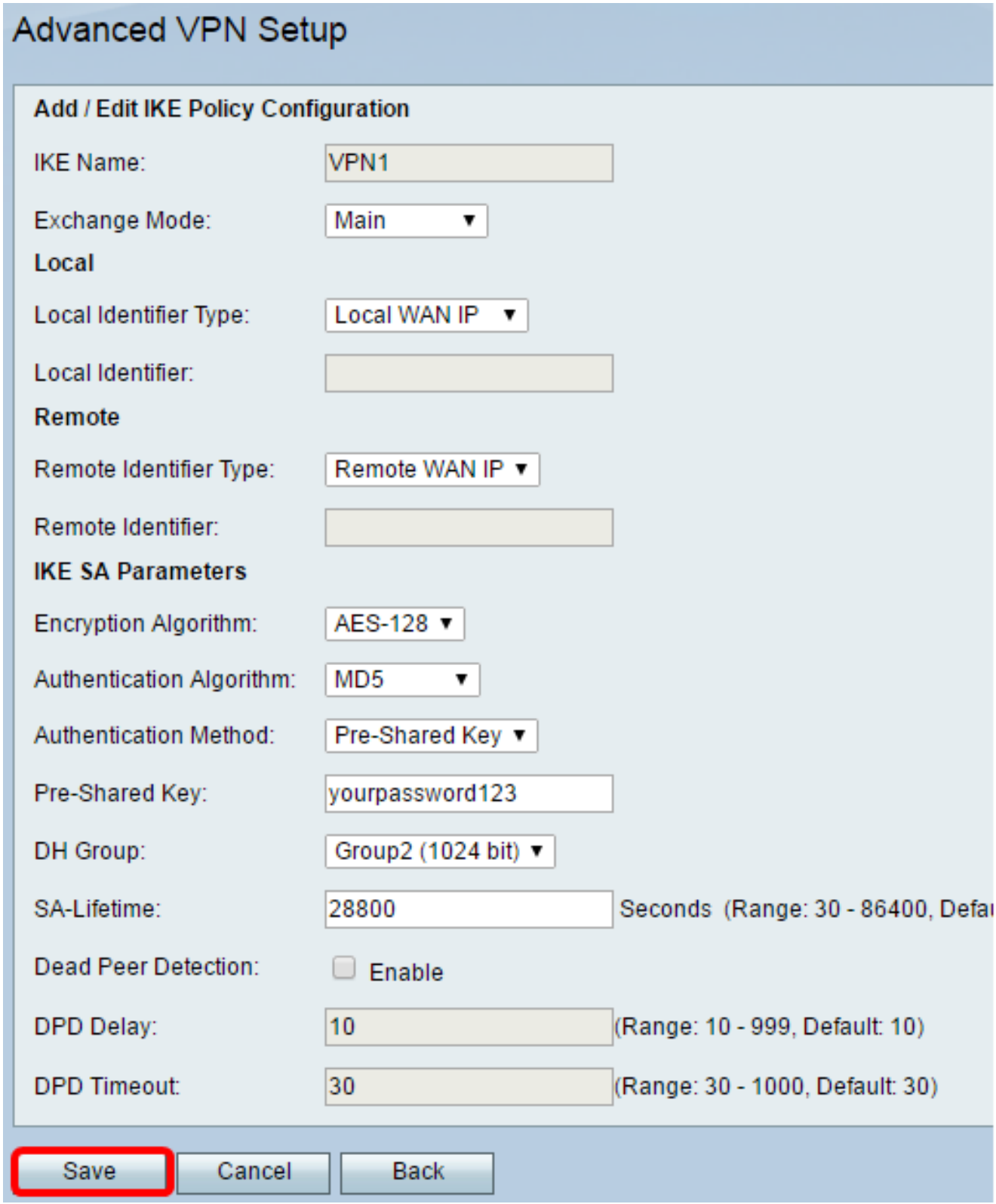


16단계. (선택 사항) 14단계에서 DPD를 활성화한 경우, DPD Timeout 필드에 비활성 피어가 삭제되기 전까지 대기할 시간(초)을 입력합니다.

참고: 피어가 데드 상태인 것을 고려하기 전에 디바이스가 DPD 메시지에 대한 응답을 받기 위해 대기해야 하는 최대 시간입니다. 기본값은 30입니다.



17단계. 저장을 **클릭합니다**.



참고: 기본 Advanced VPN Setup 페이지가 다시 나타납니다.

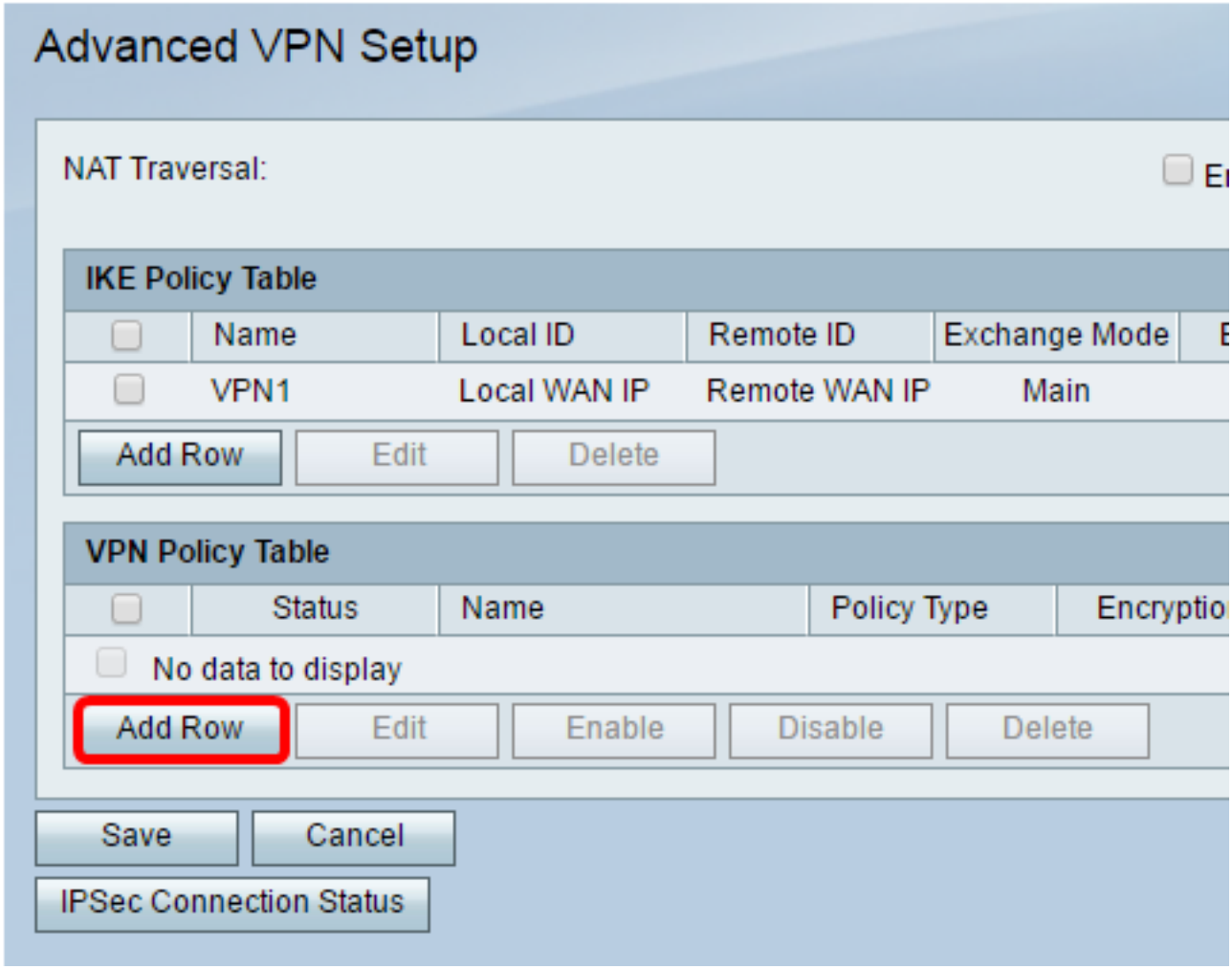
이제 라우터에서 IKE 정책 설정을 성공적으로 구성했어야 합니다.

VPN 정책 설정 구성

참고: VPN이 제대로 작동하려면 두 엔드포인트의 VPN 정책이 동일해야 합니다.

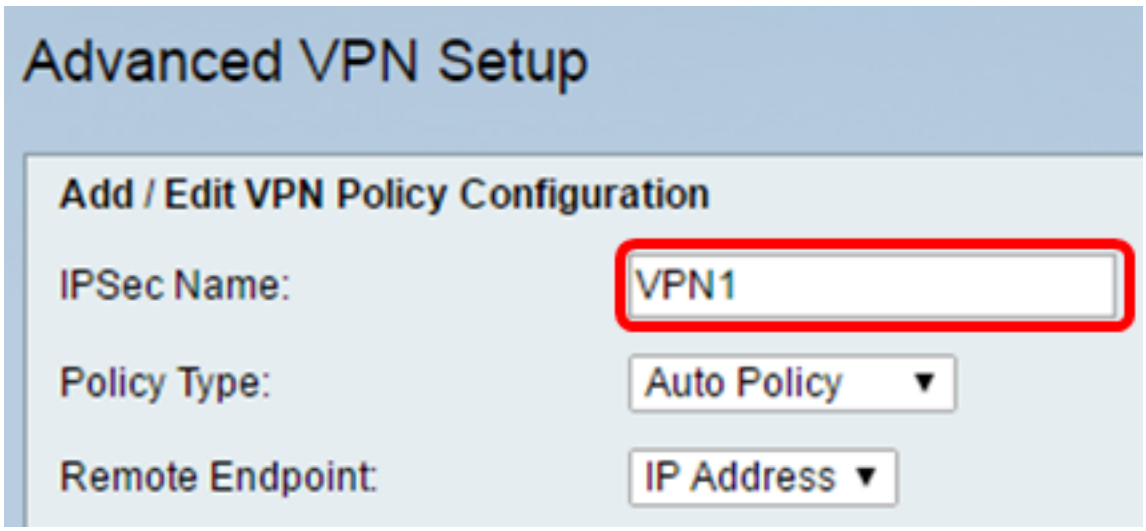
1단계. VPN Policy Table(VPN 정책 테이블)에서 **Add Row(행** 추가)를 클릭하여 새 VPN 정책을 생성합니다.

참고: 정책에 대한 확인란을 선택하고 Edit를 클릭하여 VPN 정책을 수정할 수도 **있습니다**. Advanced VPN Setup 페이지가 나타납니다.



2단계. Add/Edit *VPN Configuration*(VPN 컨피그레이션 추가/수정) 영역 아래의 IPSec Name(IPSec 이름) 필드에 VPN 정책의 이름을 입력합니다.

참고: 이 예에서는 VPN1이 사용됩니다.



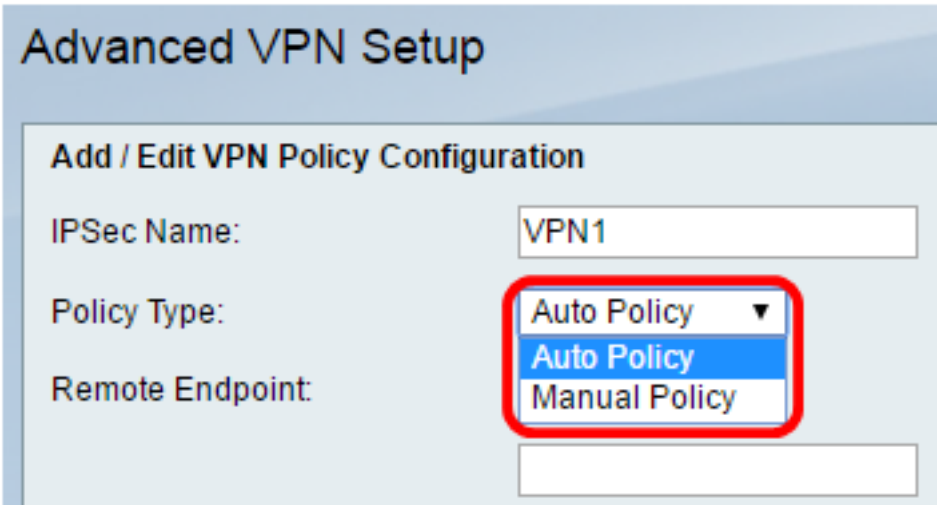
3단계. Policy Type(정책 유형) 드롭다운 목록에서 옵션을 선택합니다.

- 수동 정책 — 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. Remote Traffic Selection(원격 트래픽 선택)까지 단계를 계속합니다. 단계를 알아보려면 여기를 클릭하십시오.

- 자동 정책 — 정책 매개변수가 자동으로 설정됩니다. 이 옵션은 데이터 무결성 및 암호화 키 교환에 IKE 정책을 사용합니다. 이 옵션을 선택하면 Auto Policy Parameters(자동 정책 매개변수) 영역 아래의 컨피그레이션 설정이 활성화됩니다. 단계를 알아보려면 여기를 클릭하십시오. IKE 프로토콜이 두 VPN 엔드포인트 간에 자동으로 협상하는지 확인합니다.

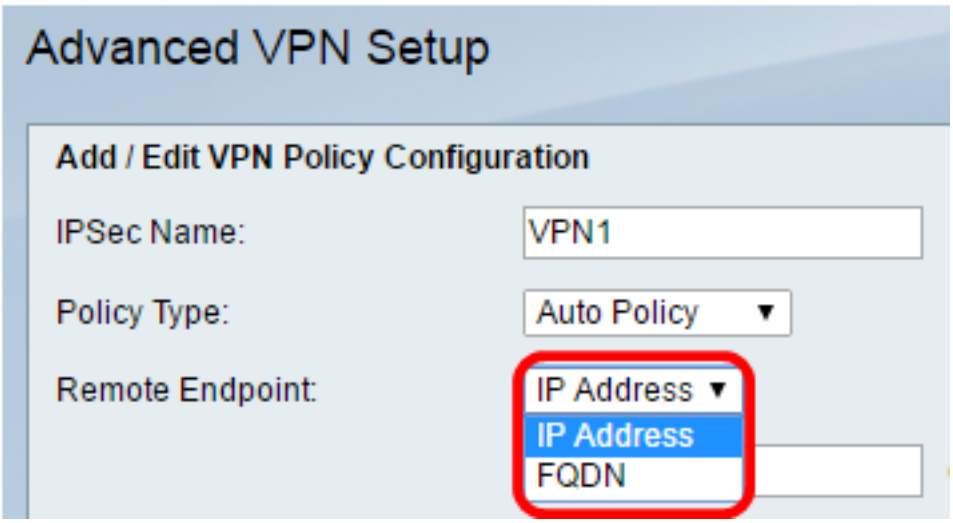
참고: 이 예에서는 Auto Policy(자동 정책)가 선택됩니다.



4단계. Remote Endpoint(원격 엔드포인트) 드롭다운 목록에서 옵션을 선택합니다.

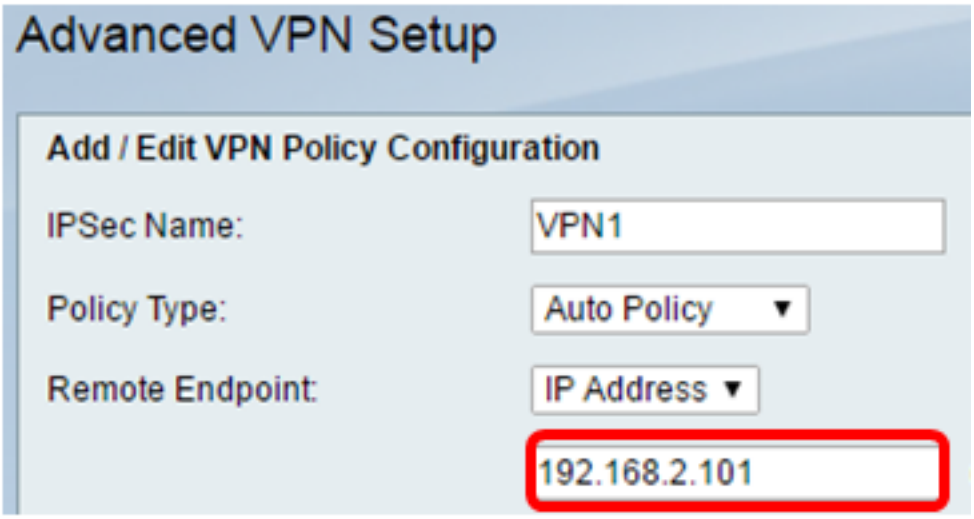
- IP Address — 이 옵션은 공용 IP 주소로 원격 네트워크를 식별합니다.
- FQDN — 특정 컴퓨터, 호스트 또는 인터넷의 전체 도메인 이름입니다. FQDN은 두 부분으로 구성됩니다. 호스트 이름 및 도메인 이름 이 옵션은 3단계에서 **Auto Policy(자동 정책)**를 선택한 경우에만 활성화할 수 있습니다.

참고: 이 예에서는 IP Address(IP 주소)가 선택됩니다.

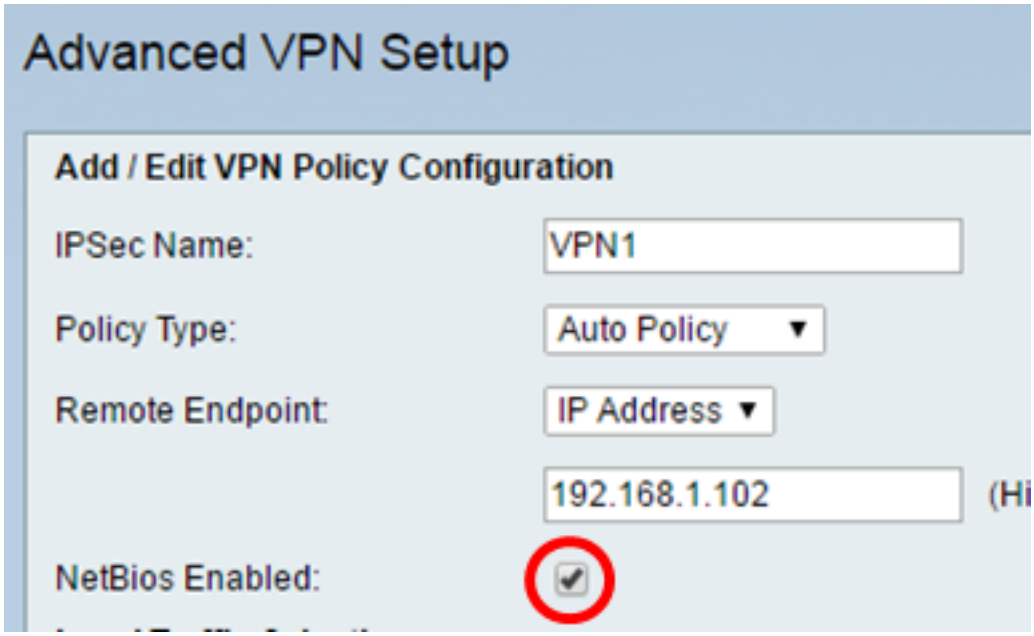


5단계. *Remote Endpoint(원격 엔드포인트)* 필드에 원격 주소의 공용 IP 주소 또는 도메인 이름을 입력합니다.

참고: 이 예에서는 192.168.2.101이 사용됩니다.



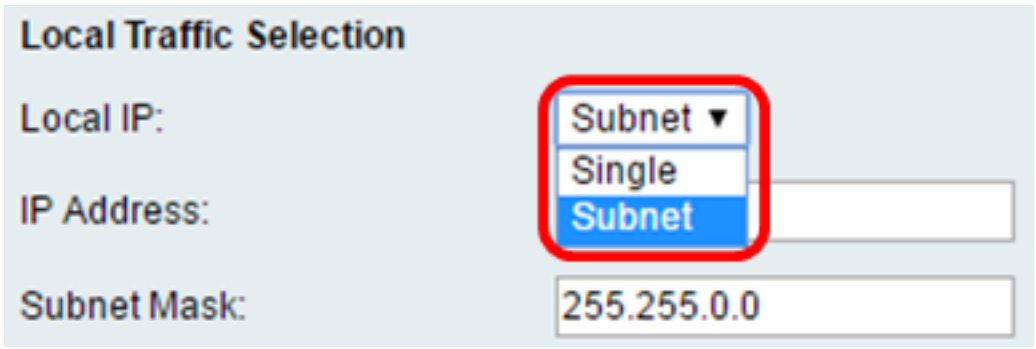
6단계. (선택 사항) NetBIOS(Network Basic Input/Output System) 브로드캐스트를 VPN 연결을 통해 전송하도록 활성화하려면 NetBios Enabled 확인란을 선택합니다. NetBIOS를 사용하면 호스트가 LAN(Local Area Network) 내에서 서로 통신할 수 있습니다.



7단계. Local Traffic Selection(로컬 트래픽 선택) 영역 아래의 Local IP(로컬 IP) 드롭다운 목록에서 옵션을 선택합니다.

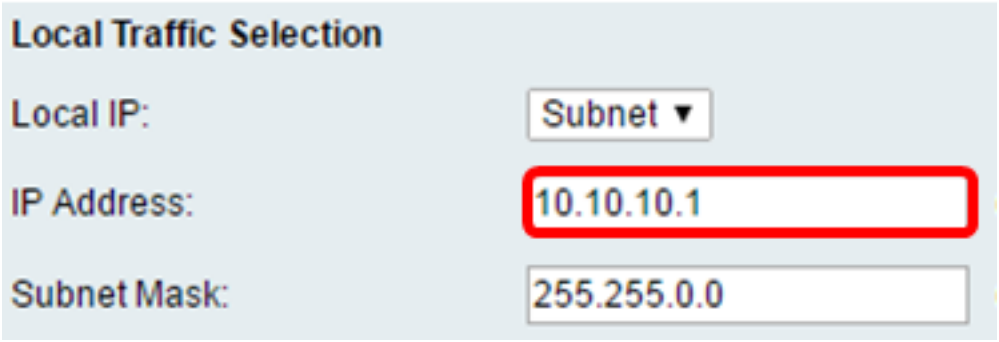
- Single — 정책을 하나의 호스트로 제한합니다.
- 서브넷 — IP 주소 범위 내의 호스트가 VPN에 연결되도록 허용합니다.

참고: 이 예에서는 서브넷을 선택합니다.



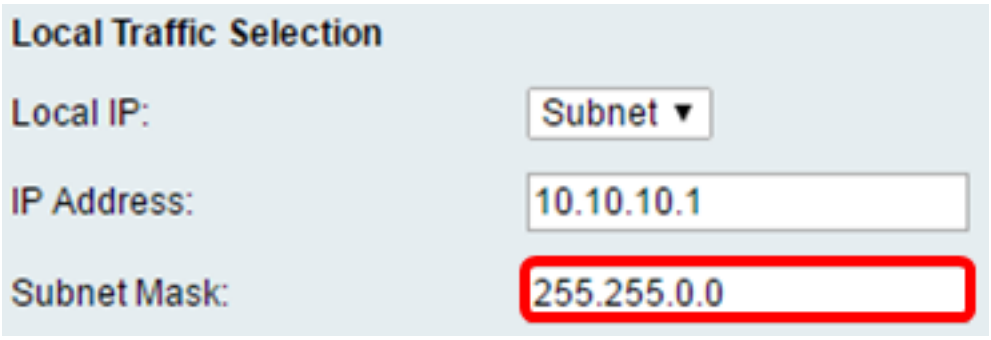
8단계. IP Address 필드에 로컬 서브넷 또는 호스트의 호스트 또는 서브넷 IP 주소를 입력합니다.

참고: 이 예에서는 로컬 서브넷 IP 주소 10.10.10.1이 사용됩니다.



9단계. (선택 사항) 7단계에서 서브넷을 선택한 경우, Subnet Mask 필드에 클라이언트의 서브넷 *마스크를* 입력합니다. 1단계에서 Single(단일)을 선택하면 Subnet Mask(서브넷 마스크) 필드가 비활성화됩니다.

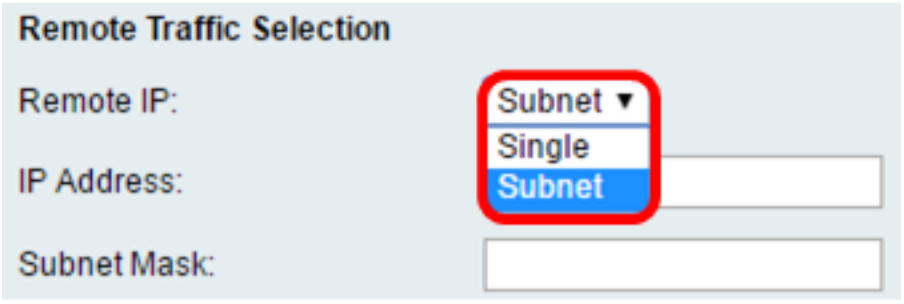
참고: 이 예에서는 서브넷 마스크 255.255.0.0이 사용됩니다.



10단계. Remote Traffic Selection(원격 트래픽 선택) 영역 아래의 Remote IP(원격 IP) 드롭다운 목록에서 옵션을 선택합니다.

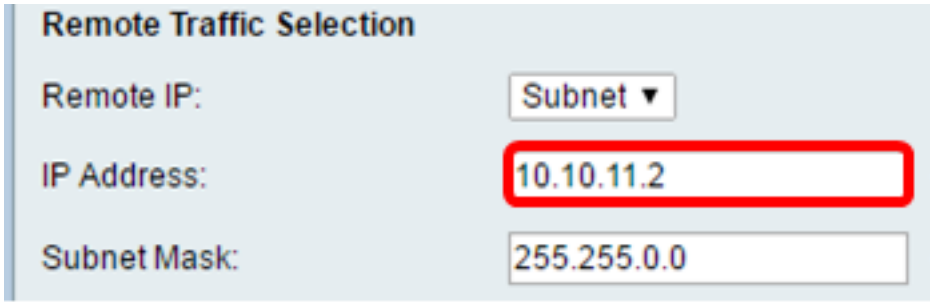
- Single — 정책을 하나의 호스트로 제한합니다.
- 서브넷 — IP 주소 범위 내의 호스트가 VPN에 연결되도록 허용합니다.

참고: 이 예에서는 서브넷을 선택합니다.



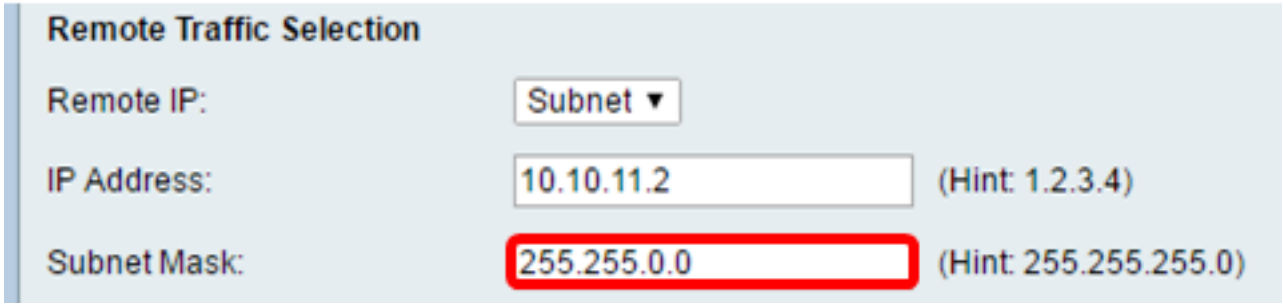
11단계. VPN에 속할 호스트의 IP 주소 범위를 IP Address(IP 주소) *필드에* 입력합니다. 10**단계**에서 Single을 선택한 경우 IP 주소를 입력합니다.

참고: 아래 예에서는 10.10.11.2가 사용됩니다.



12단계. (선택 사항) 10**단계**에서 서브넷을 선택한 경우 서브넷 마스크 필드에 서브넷 IP 주소의 *서브넷 마스크*를 입력합니다.

참고: 아래 예에서는 255.255.0.0이 사용됩니다.

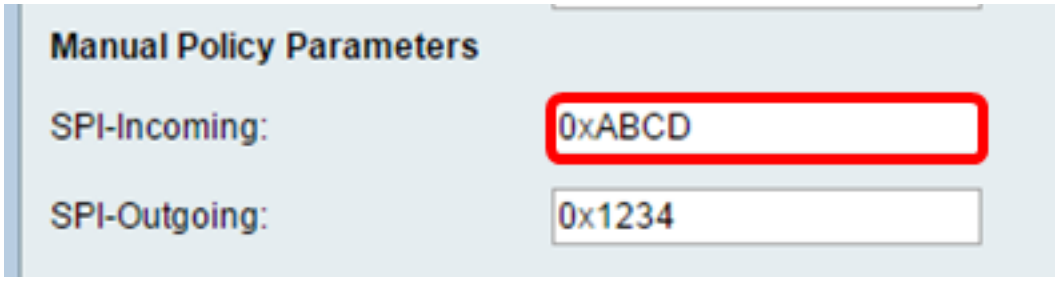


수동 정책 매개변수

참고: 수동 정책을 선택한 경우에만 이러한 필드를 편집할 수 있습니다.

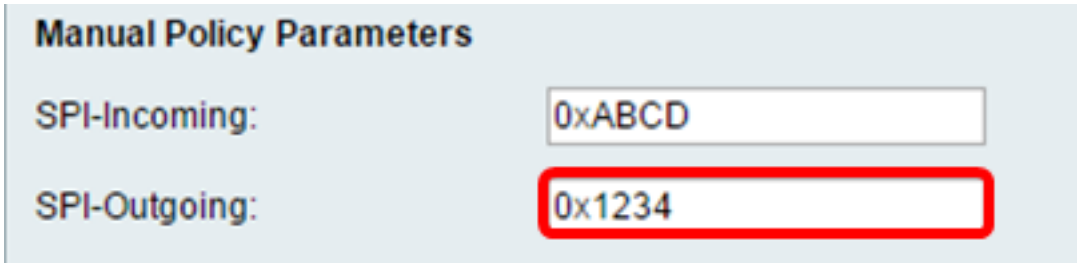
1단계. SPI-*Incoming 필드*에서 VPN 연결의 수신 트래픽에 대한 SPI(Security Parameter Index) 태그에 3~8자의 16진수 문자를 입력합니다. SPI 태그는 한 세션의 트래픽과 다른 세션의 트래픽을 구분하는 데 사용됩니다.

참고: 이 예에서는 0xABCD가 사용됩니다.



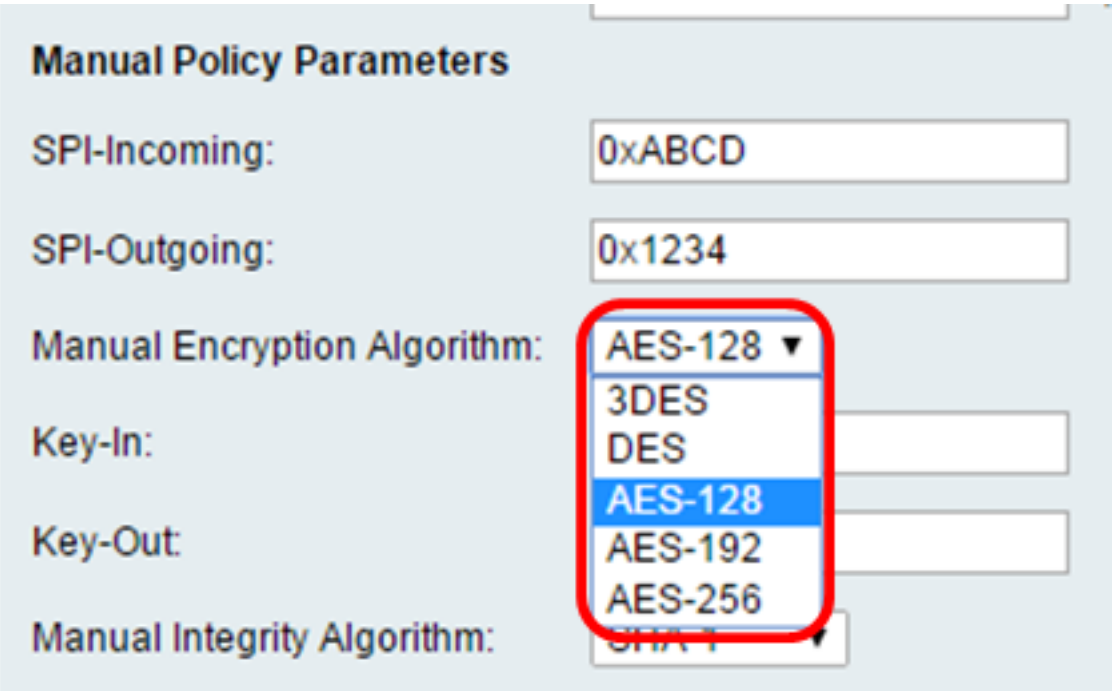
2단계. SPI-*Outgoing 필드*에서 VPN 연결의 발신 트래픽에 대한 SPI 태그에 3-8자의 16진수 문자를 입력합니다.

참고: 이 예제에서는 0x1234를 사용합니다.



3단계. Manual Encryption Algorithm(수동 암호화 알고리즘) 드롭다운 목록에서 옵션을 선택합니다. 옵션은 DES, 3DES, AES-128, AES-192 및 AES-256입니다.

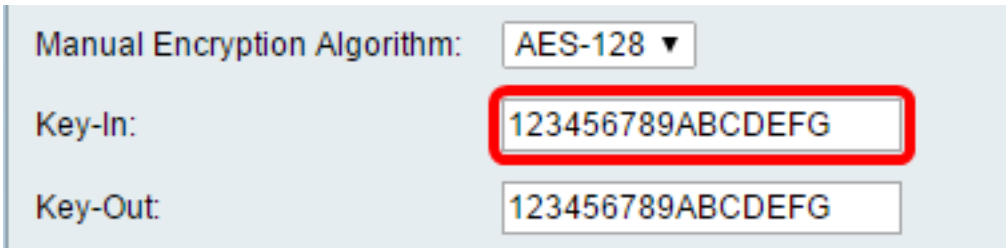
참고: 이 예에서는 AES-128을 선택합니다.



4단계. *Key-In 필드*에 인바운드 정책의 키를 입력합니다. 키 길이는 3단계에서 선택한 알고리즘에 따라 달라집니다.

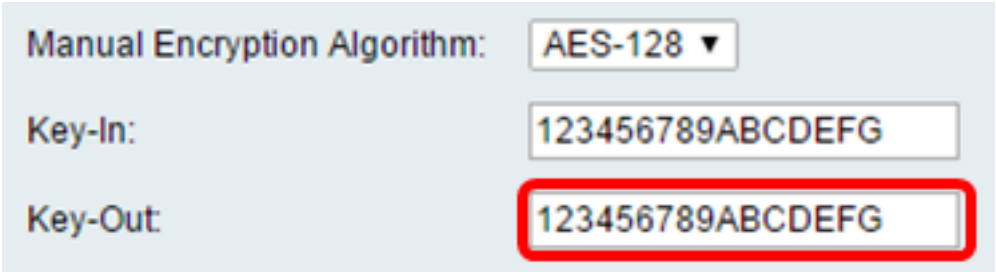
- DES는 8자 키를 사용합니다.
- 3DES는 24자 키를 사용합니다.
- AES-128은 16자 키를 사용합니다.
- AES-192는 24자 키를 사용합니다.
- AES-256은 32자 키를 사용합니다.

참고: 이 예에서는 123456789ABCDEFG가 사용됩니다.



5단계. *Key-Out(키-아웃)* 필드에 발신 정책의 키를 입력합니다. 키 길이는 3단계에서 선택한 알고리즘에 따라 달라집니다.

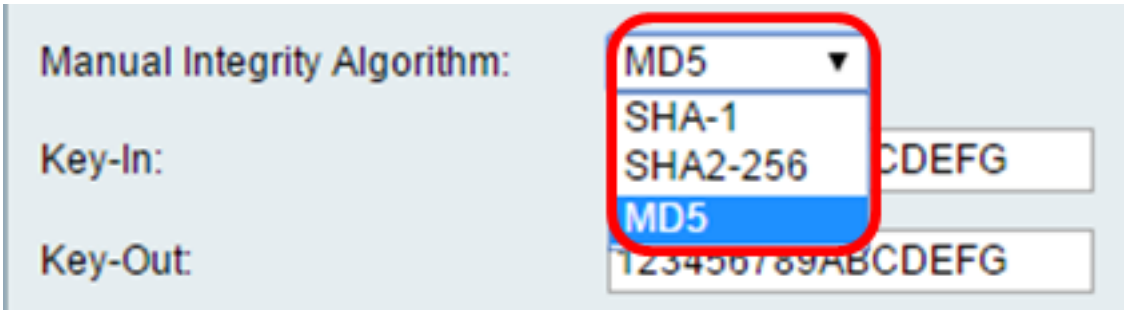
참고: 이 예에서는 123456789ABCDEFG가 사용됩니다.



6단계. Manual Integrity Algorithm(수동 무결성 알고리즘) 드롭다운 목록에서 옵션을 선택합니다.

- MD5 — 데이터 무결성을 위해 128비트 해시 값을 사용합니다. MD5는 SHA-1 및 SHA2-256보다 안전하지 않지만 더 빠릅니다.
- SHA-1 — 데이터 무결성을 위해 160비트 해시 값을 사용합니다. SHA-1은 MD5보다 느리지만 안전하며 SHA-1은 SHA2-256보다 빠르지만 안전하지 않습니다.
- SHA2-256 — 데이터 무결성을 위해 256비트 해시 값을 사용합니다. SHA2-256은 MD5 및 SHA-1보다 느리지만 안전합니다.

참고: 이 예제에서는 MD5를 선택합니다.



7단계. *Key-In 필드*에서 인바운드 정책의 키를 입력합니다. 키 길이는 6단계에서 선택한 알고리즘에 따라 달라집니다.

- MD5는 16자 키를 사용합니다.
- SHA-1은 20자 키를 사용합니다.
- SHA2-256은 32자 키를 사용합니다.

참고: 이 예에서는 123456789ABCDEFG가 사용됩니다.

8단계. *Key-Out 필드*에서 발신 정책의 키를 입력합니다. 키 길이는 6단계에서 선택한 알고리즘에 따라 달라집니다.

참고: 이 예에서는 123456789ABCDEFG가 사용됩니다.

[아우트o 정책 매개변수]

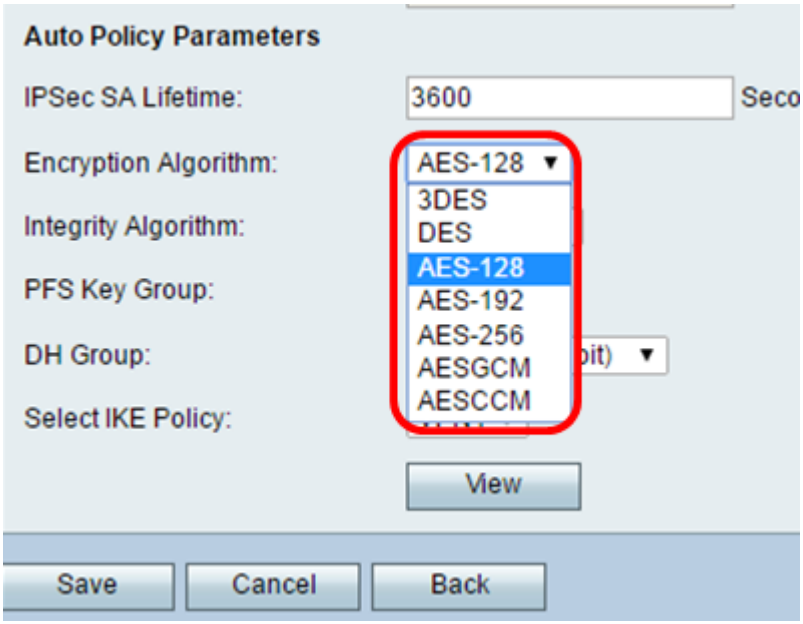
참고:자동 VPN 정책을 생성하기 전에 자동 VPN 정책을 생성하려는 IKE 정책을 생성해야 합니다. 이러한 필드는 3단계에서 **자동 정책**을 선택한 경우에만 편집할 수 있습니다.

1단계. *IPSec SA-Lifetime 필드*에서 갱신 전 SA의 지속 시간을 초 단위로 입력합니다. 범위는 30~86400입니다. 기본값은 3600입니다.

2단계. Encryption Algorithm(암호화 알고리즘) 드롭다운 목록에서 옵션을 선택합니다. 옵션은 다음과 같습니다.

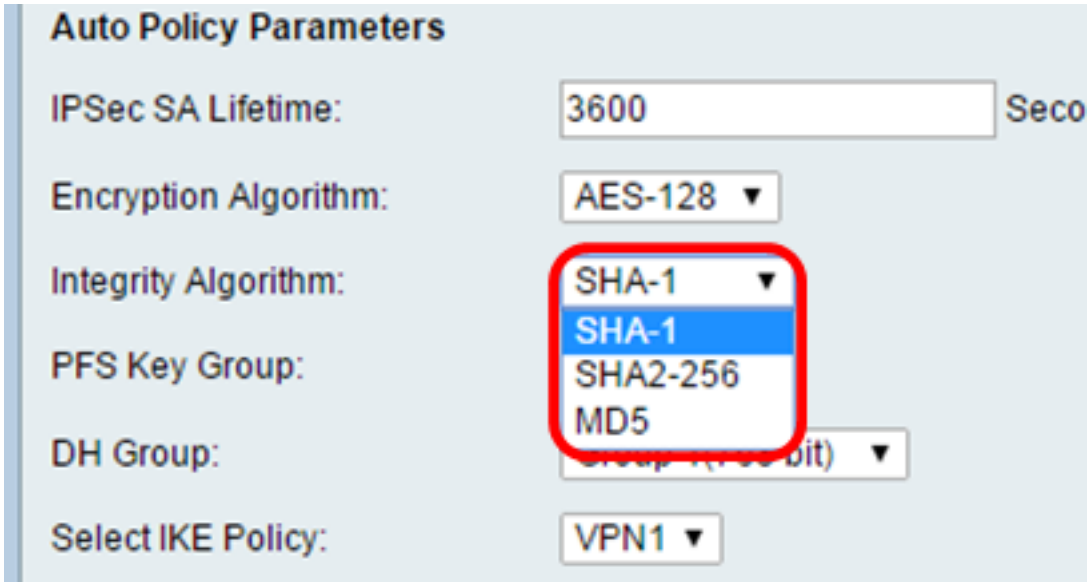
참고: 이 예에서는 AES-128을 선택합니다.

- DES — 매우 안전한 암호화 방법은 아니지만 이전 버전과의 호환성을 위해 필요할 수 있는 56비트 이전 암호화 방법입니다.
- 3DES — 데이터를 세 번 암호화하므로 키 크기를 늘리는 데 사용되는 168비트의 간단한 암호화 방법입니다. 이는 DES보다 더 많은 보안을 제공하지만 AES보다 적은 보안을 제공합니다.
- AES-128 — AES 암호화에 128비트 키를 사용합니다. AES는 DES보다 빠르고 안전합니다. 일반적으로 AES는 3DES보다 더 빠르고 안전합니다. AES-128은 AES-192 및 AES-256보다 빠르지만 안전하지 않습니다.
- AES-192 — AES 암호화에 192비트 키를 사용합니다. AES-192는 AES-128보다 느리지만 안전하며, AES-256보다 빠르지만 안전하지 않습니다.
- AES-256 — AES 암호화에 256비트 키를 사용합니다. AES-256은 AES-128 및 AES-192보다 느리지만 안전합니다.
- AESGCM — 고급 암호화 표준 갈루아 카운터 모드는 일반 인증 암호화 블록 암호 모드입니다. GCM 인증은 하드웨어의 효율적인 구현에 특히 적합한 작업을 사용하므로 고속 구현 또는 효율적이고 컴팩트한 회로의 구현에 특히 적합합니다.
- AESCCM — CBC-MAC 모드의 고급 암호화 표준 카운터는 일반 인증 암호화 블록 암호화 모드입니다. CCM은 소형 소프트웨어 구현에 적합합니다.

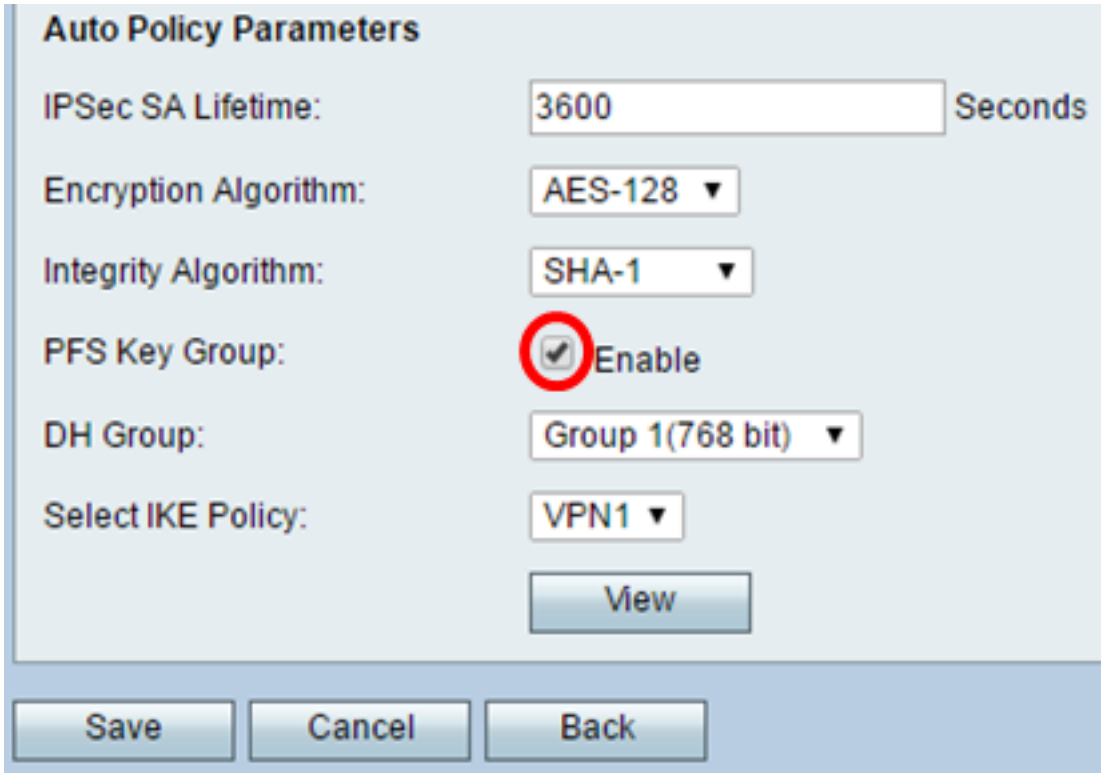


3단계. Integrity Algorithm(무결성 알고리즘) 드롭다운 목록에서 옵션을 선택합니다. 옵션은 MD5, SHA-1 및 SHA2-256입니다.

참고: 이 예에서는 SHA-1을 선택합니다.

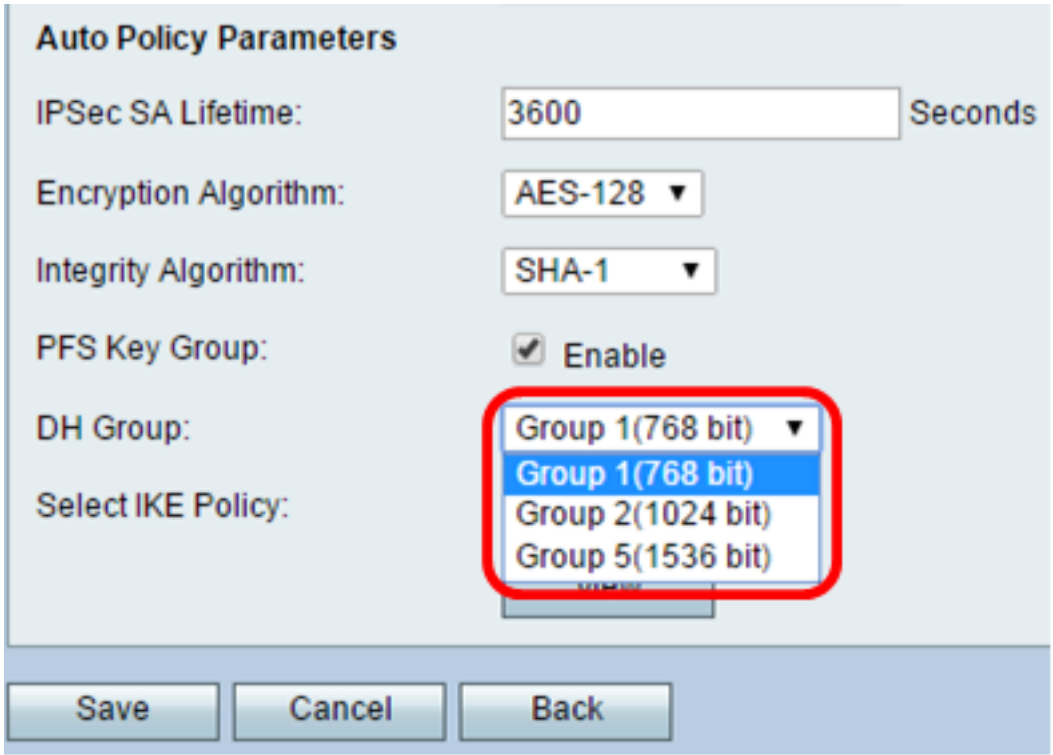


4단계. PFS(**Perfect** Forward Secrecy)를 활성화하려면 PFS 키 그룹에서 Enable 확인란을 선택합니다. PFS는 VPN 보안을 향상시키지만 연결 속도가 느려집니다.



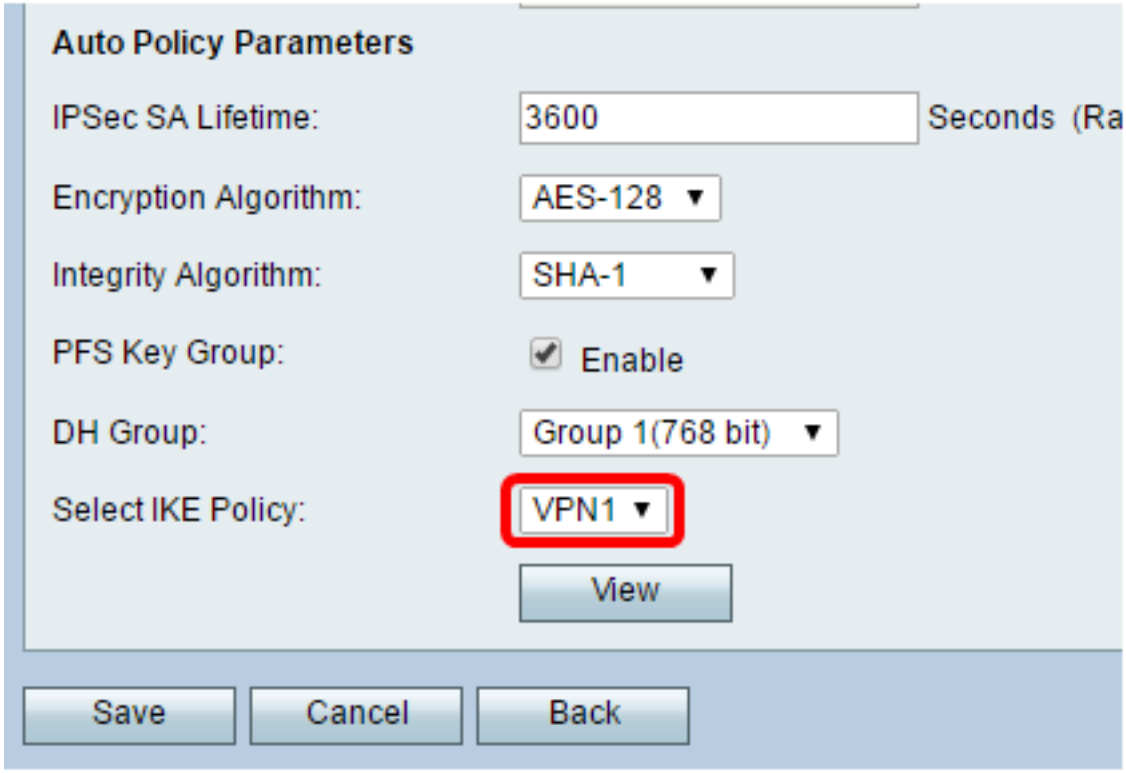
5단계. (선택 사항) 4단계에서 PFS를 활성화하도록 선택한 경우, DH 그룹 드롭다운 목록에서 가입할 DH 그룹을 선택합니다. 그룹 번호가 높을수록 보안이 향상됩니다.

참고: 이 예제에서는 그룹 1을 선택합니다.

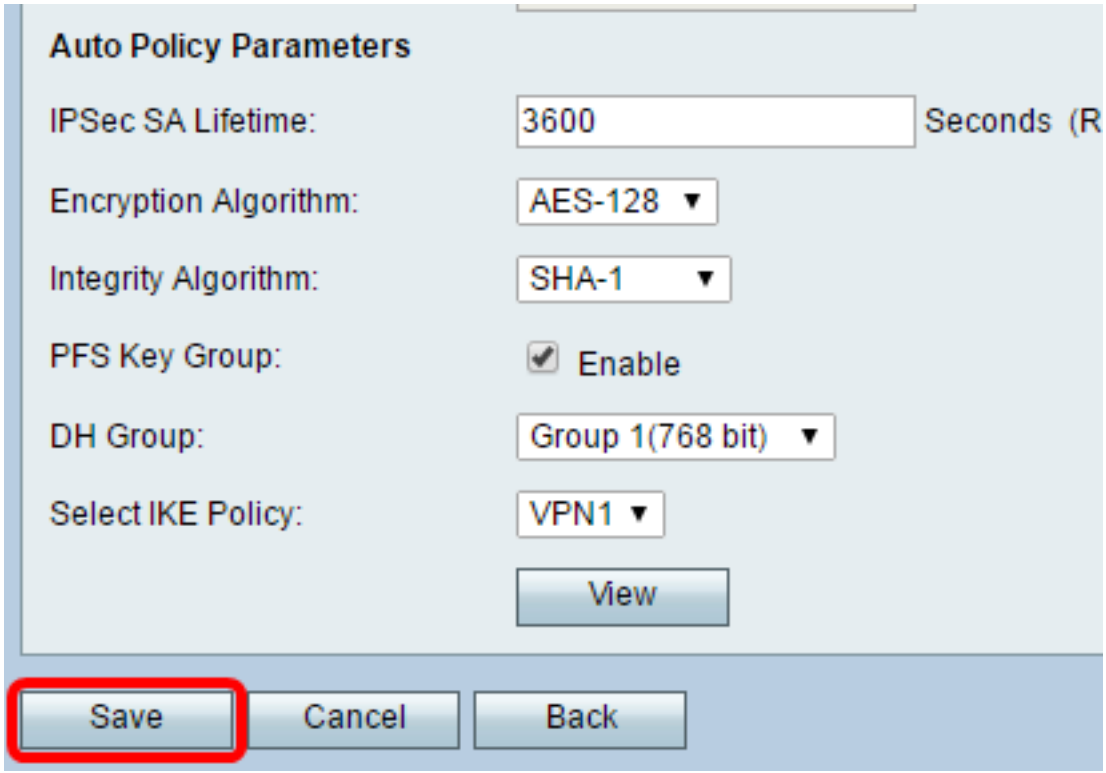


6단계. Select IKE Policy(IKE 정책 선택) 드롭다운 목록에서 VPN 정책에 사용할 IKE 정책을 선택합니다.

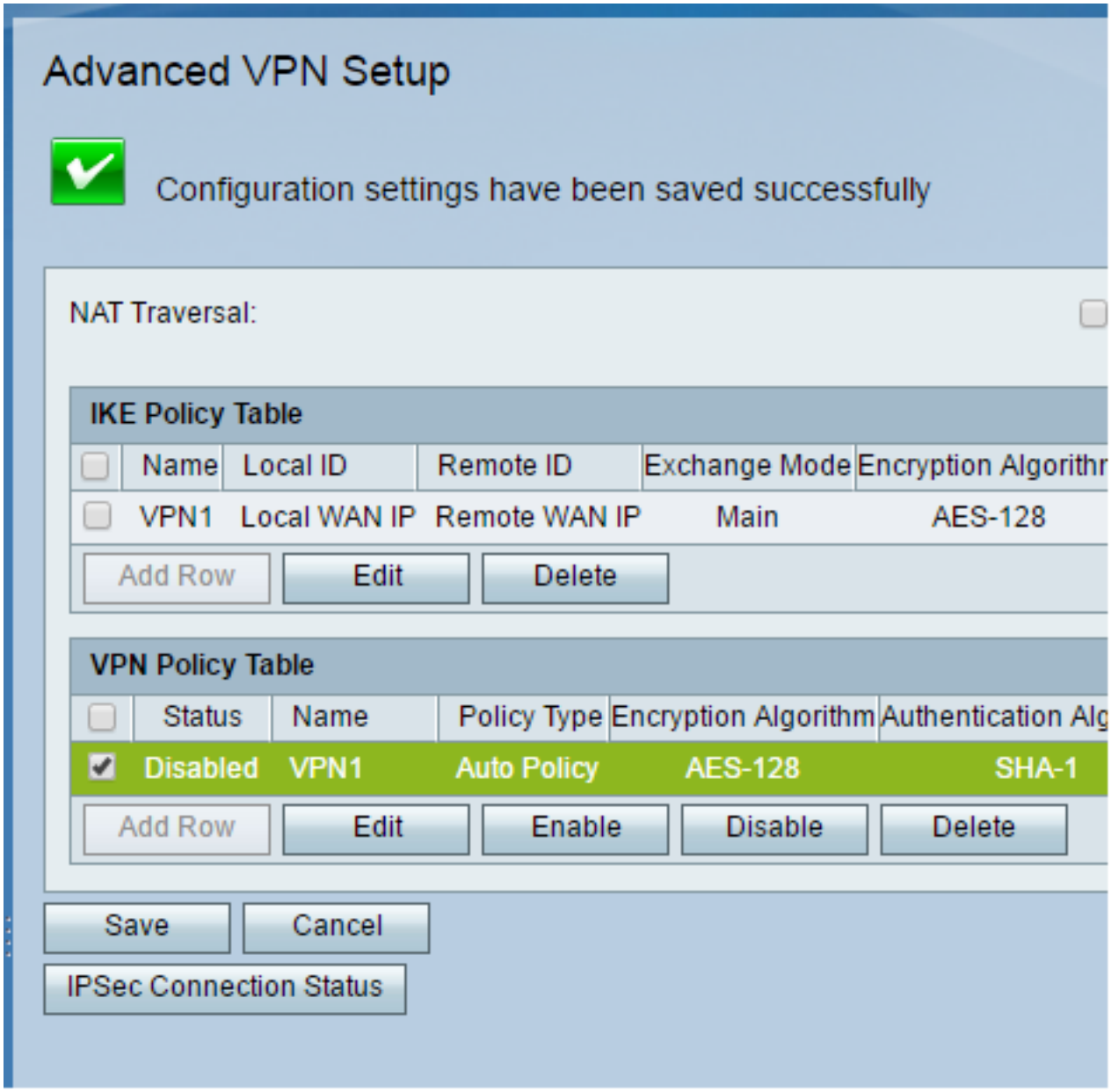
참고: 이 예에서는 하나의 IKE 정책만 구성되었으므로 하나의 정책만 나타납니다.



7단계. 저장을 **클릭합니다**.

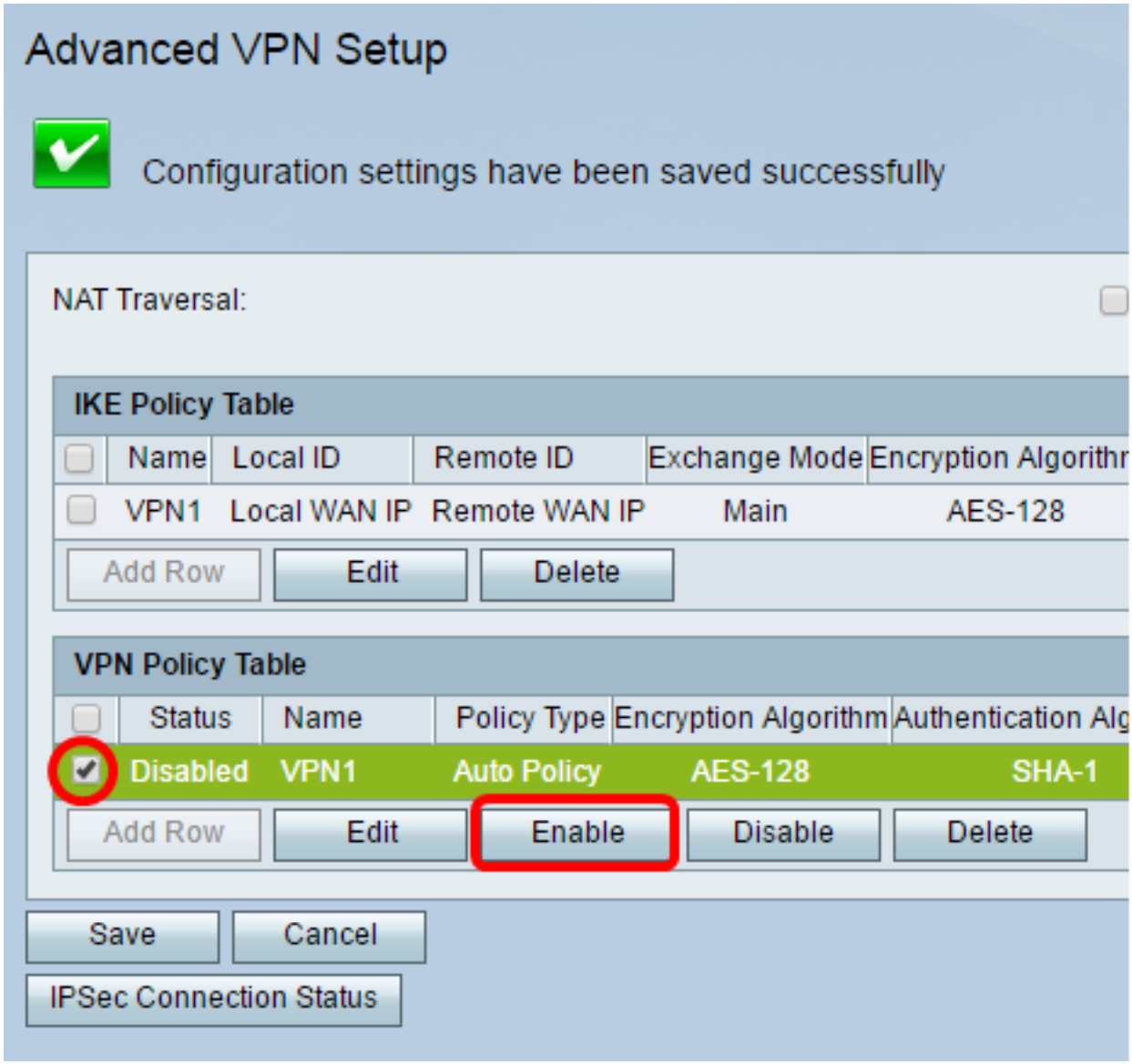


참고: 기본 Advanced VPN Setup 페이지가 다시 나타납니다. 컨피그레이션 설정이 성공적으로 저장되었다는 확인 메시지가 표시됩니다.

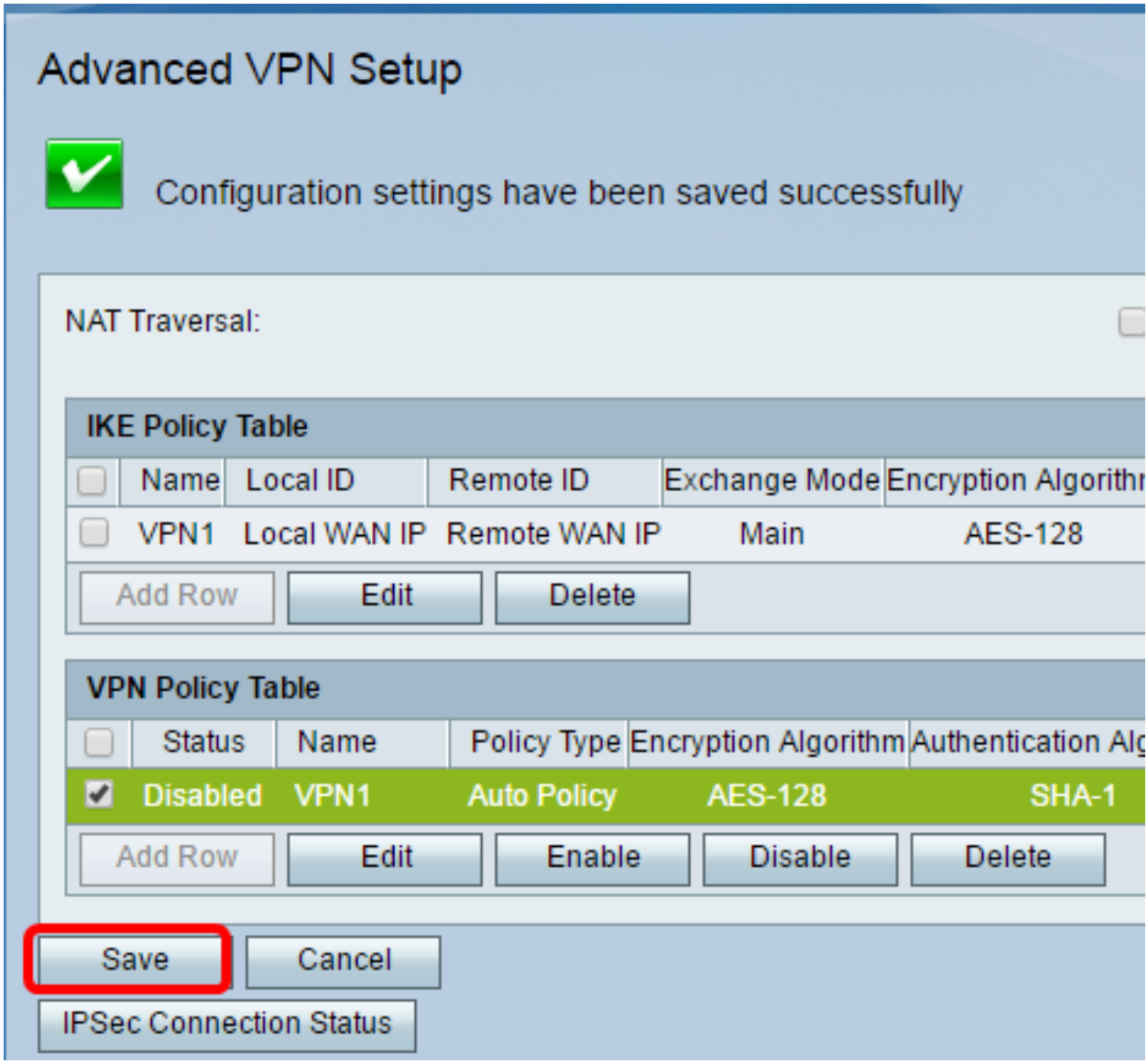


8단계. VPN Policy(VPN 정책) 테이블에서 확인란을 선택하여 VPN을 선택하고 Enable(활성화)을 **클릭합니다**.

참고: 구성된 VPN 정책은 기본적으로 비활성화되어 있습니다.



9단계. 저장을 **클릭합니다**.



이제 RV130 또는 RV130W 라우터에서 VPN 정책을 성공적으로 구성했어야 합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.