RV016, RV042, RV042G 및 RV082 VPN Router의 게이트웨이 대 게이트웨이 VPN 구성

목표

VPN(Virtual Private Network)은 공용 인터넷 또는 공유 인터넷을 통해 VPN 터널이라는 이름의 두 엔드포인트 간에 보안 연결을 형성하는 데 사용됩니다. 보다 구체적으로, 게이트웨이 간 VPN 연결에서는 두 라우터가 서로 안전하게 연결할 수 있으며 한 쪽 끝에 있는 클라이언트가 다른 쪽 끝에 있는 네트워크의 일부인 것처럼 논리적으로 표시될 수 있습니다. 이를 통해 데이터와 리소스를 인터넷을 통해 보다 쉽고 안전하게 공유할 수 있습니다.

게이트웨이 간 VPN을 활성화하려면 두 라우터 모두에서 컨피그레이션을 수행해야 합니다. Local Group Setup(로컬 그룹 설정) 및 Remote Group Setup(원격 그룹 설정) 섹션에서 수행한 컨피그레이션을 두 라우터 간에 반전하여 한 라우터의 로컬 그룹이 다른 라우터의 원격 그룹이 되도록 해야 합니다.

이 문서의 목적은 RV016, RV042, RV042G 및 RV082 VPN Series Router에서 게이트웨이 간 VPN을 구성하는 방법을 설명하는 것입니다.

적용 가능한 디바이스

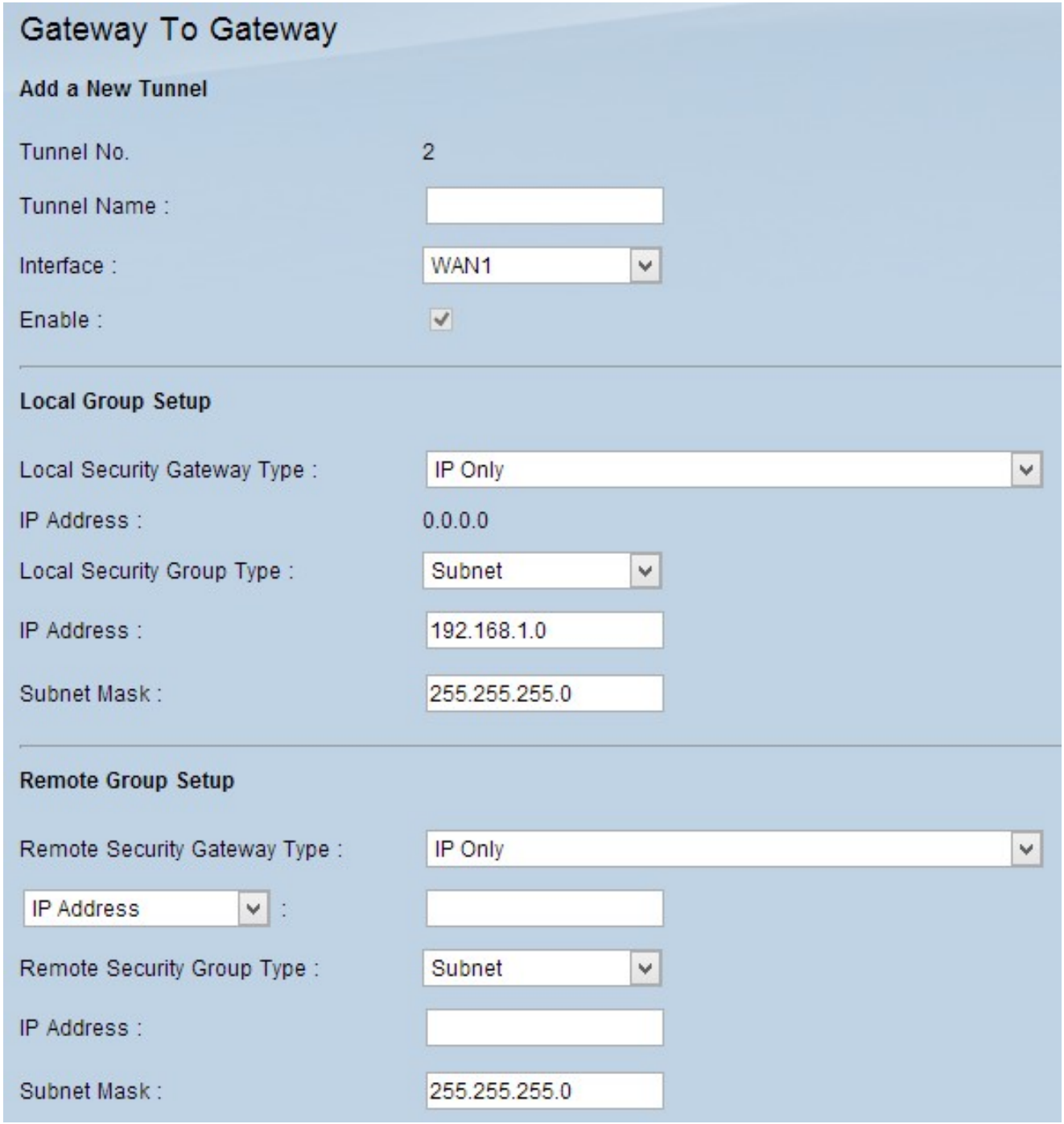
· RV016
· RV042
· RV042G
· RV082

소프트웨어 버전

· v4.2.2.08

게이트웨이 간 VPN 구성

1단계. Router Configuration Utility에 로그인하고 VPN > Gateway to Gateway를 선택합니다. 게이트웨이 투 게이트웨이 페이지가 열립니다.



게이트웨이 VPN에 대한 게이트웨이를 구성하려면 다음 기능을 구성해야 합니다.

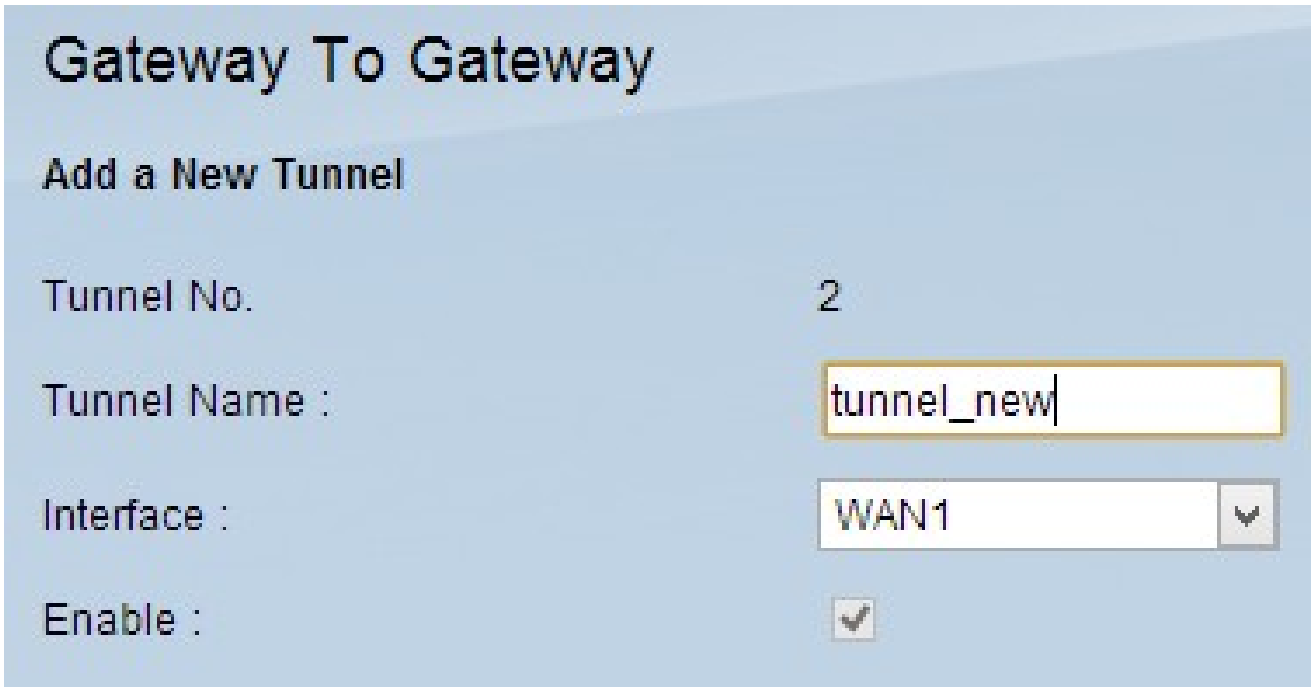
1. 새 터널 추가

2. 로컬 그룹 설정

3. 원격 그룹 설정

4. IPSec 설정

새 터널 추가



Tunnel No.(터널 번호)는 생성할 현재 터널을 표시하는 읽기 전용 필드입니다.

1단계. Tunnel Name 필드에 VPN 터널의 이름을 입력합니다. 터널의 다른 끝에서 사용되는 이름과 일치하지 않아도 됩니다.

2단계. Interface 드롭다운 목록에서 터널에 사용할 WAN(Wide Area Network) 포트를 선택합니다.

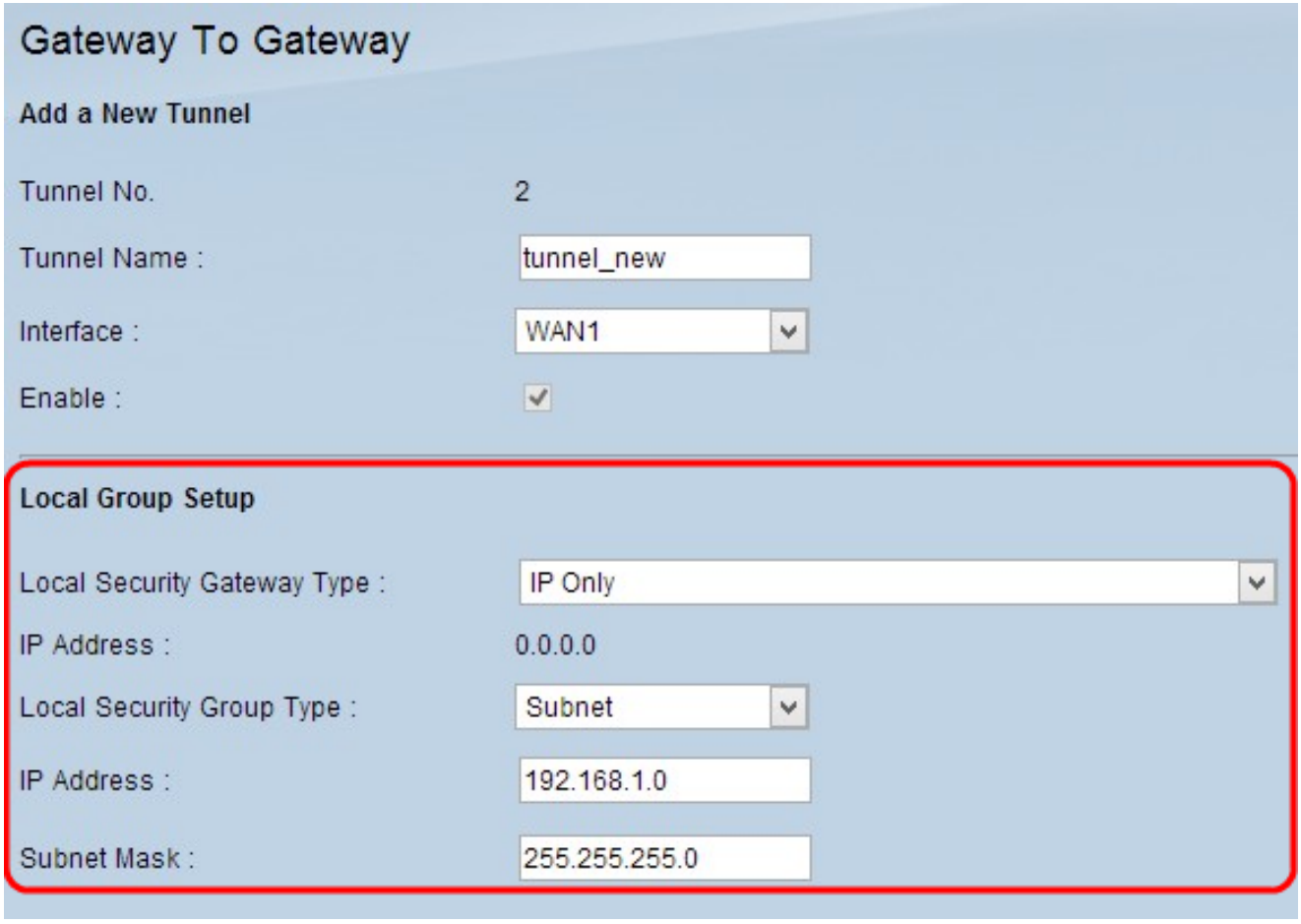
· WAN1 — RV0XX Series VPN 라우터의 전용 WAN 포트.

· WAN2 — RV0XX Series VPN 라우터의 WAN2/DMZ 포트. DMZ(비무장화 영역) 포트가 아닌 WAN으로 구성된 경우에만 드롭다운 메뉴에 표시됩니다.

3단계. (선택 사항) VPN을 활성화하려면 Enable(활성화) 필드의 확인란을 선택합니다. VPN은 기본적으로 활성화되어 있습니다.

로컬 그룹 설정

참고: 한 라우터의 로컬 그룹 설정에 대한 컨피그레이션은 다른 라우터의 원격 그룹 설정에 대한 컨피그레이션과 동일해야 합니다.



1단계. Local Security Gateway Type(로컬 보안 게이트웨이 유형) 드롭다운 목록에서 VPN 터널을 설정하기 위한 적절한 라우터 식별 방법을 선택합니다.

· IP Only — 로컬 라우터(이 라우터)는 고정 IP 주소로 인식됩니다. 라우터에 고정 WAN IP가 있는 경우에만 이 옵션을 선택할 수 있습니다. 고정 WAN IP 주소는 IP Address 필드에 자동으로 표시됩니다.

· IP + FQDN (Domain Name) 인증 — 고정 IP 주소 및 등록된 도메인을 통해 터널 액세스가 가능합니다. 이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메인의 이름을 입력합니다. 고정 WAN IP 주소는 IP Address 필드에 자동으로 표시됩니다.

· IP + E-mail Addr(USER FQDN) 인증 — 고정 IP 주소 및 이메일 주소를 통해 터널 액세스가 가능합니다. 이 옵션을 선택하는 경우 Email Address(이메일 주소) 필드에 이메일 주소를 입력합니다. 고정 WAN IP 주소는 IP Address 필드에 자동으로 표시됩니다.

· 동적 IP + FQDN(Domain Name) 인증 — 동적 IP 주소 및 등록된 도메인을 통해 터널 액세스가 가능합니다. 이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메

인의 이름을 입력합니다.

· 동적 IP + 이메일 주소(사용자 FQDN) 인증 — 동적 IP 주소 및 이메일 주소를 통해 터널 액세스가 가능합니다. 이 옵션을 선택하는 경우 Email Address(이메일 주소) 필드에 이메일 주소를 입력합니다.

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

· IP — 하나의 LAN 디바이스만 VPN 터널에 액세스할 수 있습니다. 이 옵션을 선택하는 경우 IP Address(IP 주소) 필드에 LAN 디바이스의 IP 주소를 입력합니다.

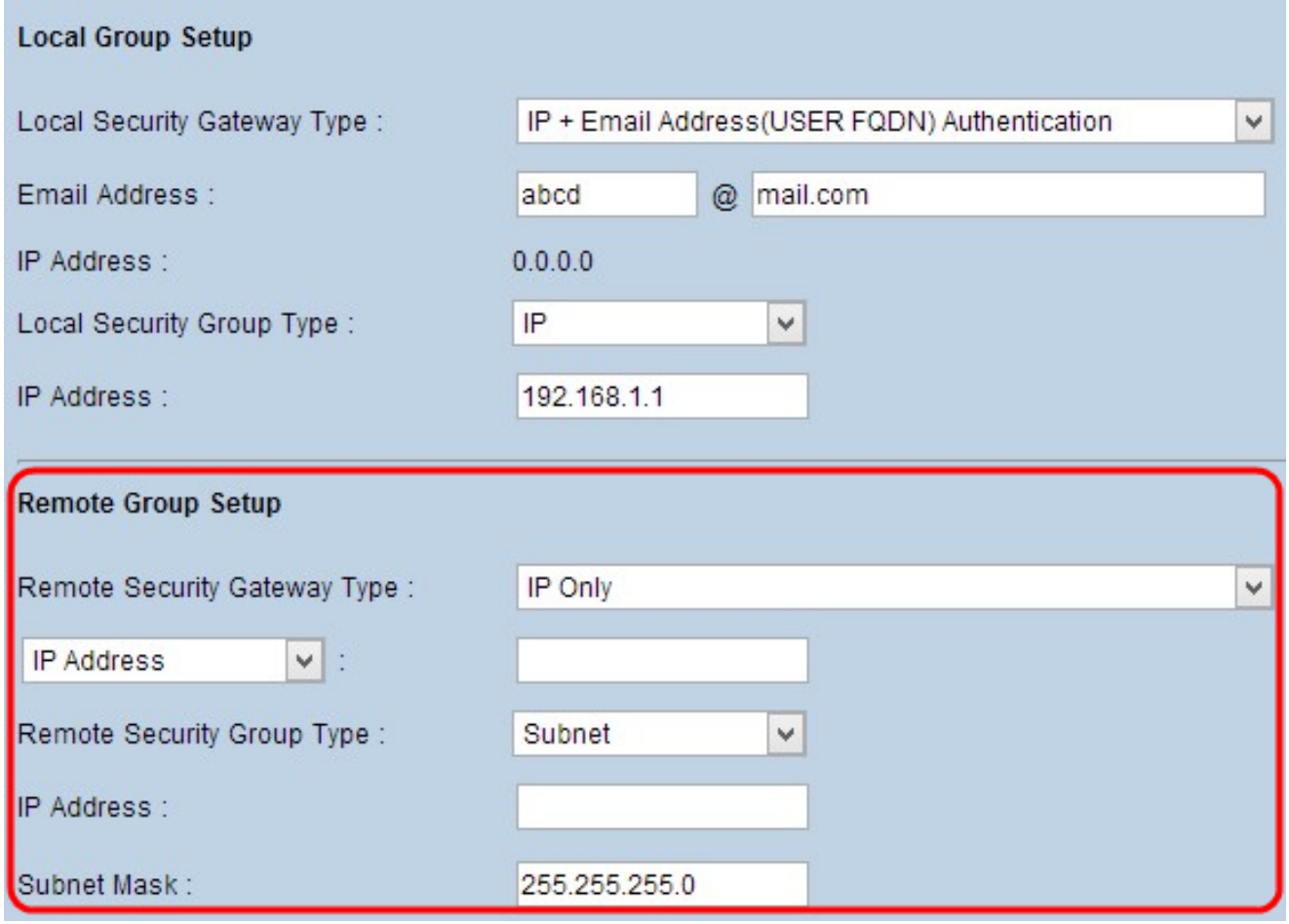
· 서브넷 — 특정 서브넷의 모든 LAN 디바이스가 터널에 액세스할 수 있습니다. 이 옵션을 선택하는 경우 IP Address(IP 주소) 및 Subnet Mask(서브넷 마스크) 필드에 LAN 디바이스의 서브네트워크 IP 주소와 서브넷 마스크를 각각 입력합니다. 기본 마스크는 255.255.255.0입니다.

· IP 범위 — 다양한 LAN 장치가 터널에 액세스할 수 있습니다. 이 옵션을 선택하는 경우 Begin IP(시작 IP) 및 End IP(종료 IP) 필드에 각각 시작 및 종료 IP 주소를 입력합니다.

3단계. Save(저장)를 클릭하여 설정을 저장합니다.

원격 그룹 설정

참고: 한 라우터의 원격 그룹 설정에 대한 컨피그레이션은 다른 라우터의 로컬 그룹 설정에 대한 컨피그레이션과 동일해야 합니다.



1단계. Remote Security Gateway Type(원격 보안 게이트웨이 유형) 드롭다운 목록에서 VPN 터널을 설정하기 위해 원격 라우터를 식별하는 방법을 선택합니다.

· IP Only — 고정 WAN IP를 통해 터널 액세스가 가능합니다. 원격 라우터의 IP 주소를 알고 있는 경우 Remote Security Gateway Type(원격 보안 게이트웨이 유형) 필드 바로 아래의 드롭다운 목록에서 IP 주소를 선택하고 IP 주소를 입력합니다. IP 주소를 모르지만 도메인 이름을 아는 경우 IP by DNS Resolved(DNS로 확인된 IP)를 선택하고 IP by DNS Resolved(IP by DNS로 확인된) 필드에 라우터의 도메인 이름을 입력합니다.

· IP + FQDN(Domain Name) 인증 — 고정 IP 주소 및 라우터에 등록된 도메인을 통해 터널 액세스가 가능합니다. 원격 라우터의 IP 주소를 알고 있는 경우 Remote Security Gateway Type(원격 보안 게이트웨이 유형) 필드 바로 아래의 드롭다운 목록에서 IP 주소를 선택하고 주소를 입력합니다. IP 주소를 모르지만 도메인 이름을 아는 경우 IP by DNS Resolved(DNS로 확인된 IP)를 선택하고 IP by DNS Resolved(IP by DNS로 확인된) 필드에 라우터의 도메인 이름을 입력합니다. 어떤 방법으로 라우터를 식별할지 여부에 관계없이 Domain Name(도메인 이름) 필드에 라우터의 도메인 이름을 입력합니다.

· IP + Email Addr(USER FQDN) 인증 — 고정 IP 주소 및 이메일 주소를 통해 터널 액세스가 가능합니다. 원격 라우터의 IP 주소를 알고 있는 경우 Remote Security Gateway Type(원격 보안 게이트웨이 유형) 필드 바로 아래의 드롭다운 목록에서 IP 주소를 선택하고 주소를 입력합니다. IP 주소를 모르지만 도메인 이름을 아는 경우 IP by DNS Resolved(DNS로 확인된

IP)를 선택하고 IP by DNS Resolved(IP by DNS로 확인된) 필드에 라우터의 도메인 이름을 입력합니다. 이메일 주소 필드에 이메일 주소를 입력합니다.

· 동적 IP + FQDN(Domain Name) 인증 — 동적 IP 주소 및 등록된 도메인을 통해 터널 액세스가 가능합니다. 이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메인의 이름을 입력합니다.

· 동적 IP + 이메일 주소(사용자 FQDN) 인증 — 동적 IP 주소 및 이메일 주소를 통해 터널 액세스가 가능합니다. 이 옵션을 선택하는 경우 Email Address(이메일 주소) 필드에 이메일 주소를 입력합니다.

2단계. Remote Security Group Type(원격 보안 그룹 유형) 드롭다운 목록에서 VPN 터널에 액세스할 수 있는 적절한 원격 LAN 사용자 또는 사용자 그룹을 선택합니다.

· IP — 특정 LAN 디바이스 하나만 터널에 액세스할 수 있습니다. 이 옵션을 선택하는 경우 IP Address(IP 주소) 필드에 LAN 디바이스의 IP 주소를 입력합니다.

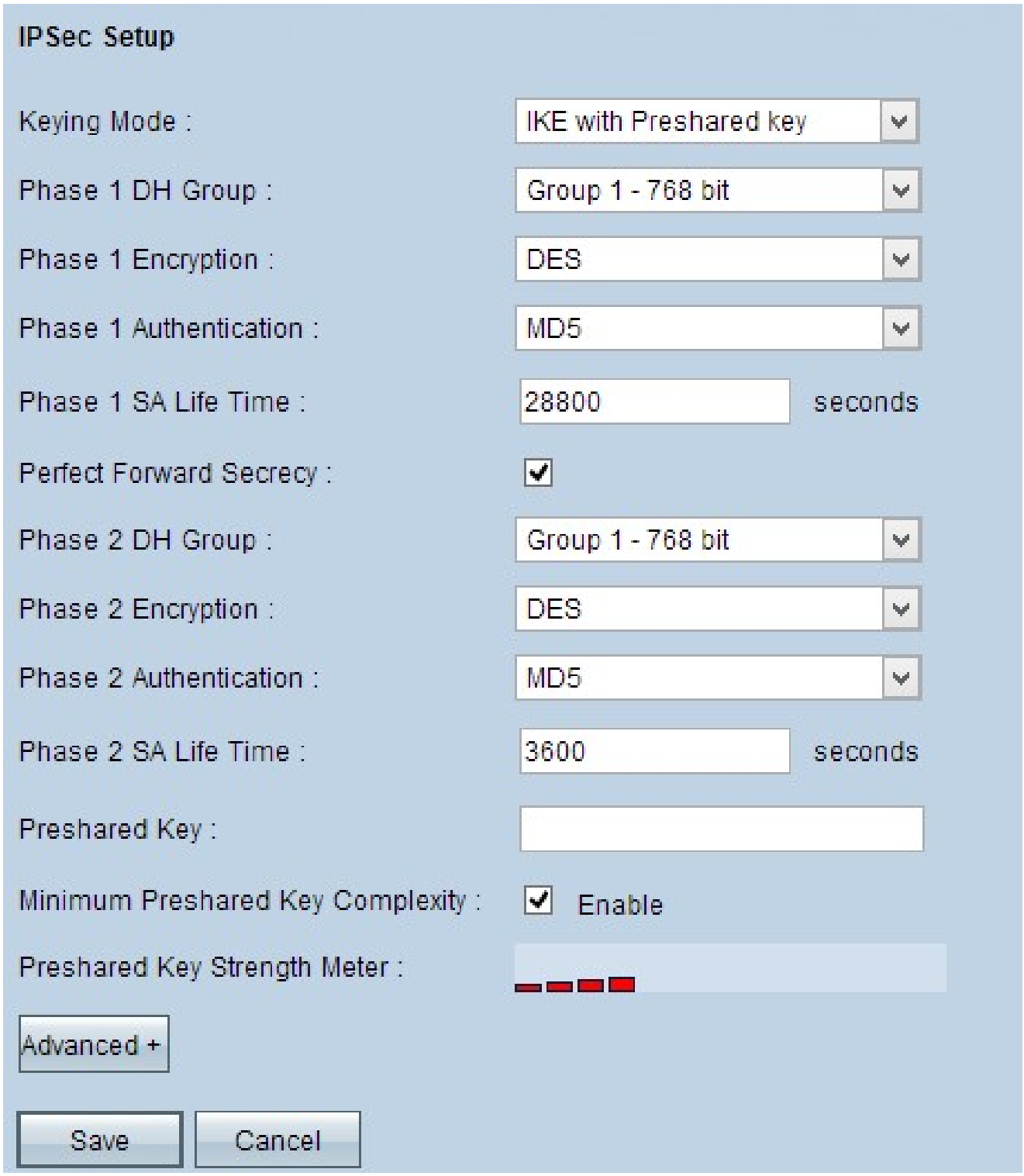
· 서브넷 — 특정 서브넷의 모든 LAN 디바이스가 터널에 액세스할 수 있습니다. 이 옵션을 선택하는 경우 IP Address(IP 주소) 및 Subnet Mask(서브넷 마스크) 필드에 LAN 디바이스의 서브네트워크 IP 주소와 서브넷 마스크를 각각 입력합니다.

· IP Range — 다양한 LAN 장치가 터널에 액세스할 수 있습니다. 이 옵션을 선택하는 경우 Begin IP(시작 IP) 및 End IP(종료 IP) 필드에 각각 시작 및 종료 IP 주소를 입력합니다.

참고: 터널 끝에 있는 두 라우터는 동일한 서브넷에 있을 수 없습니다.

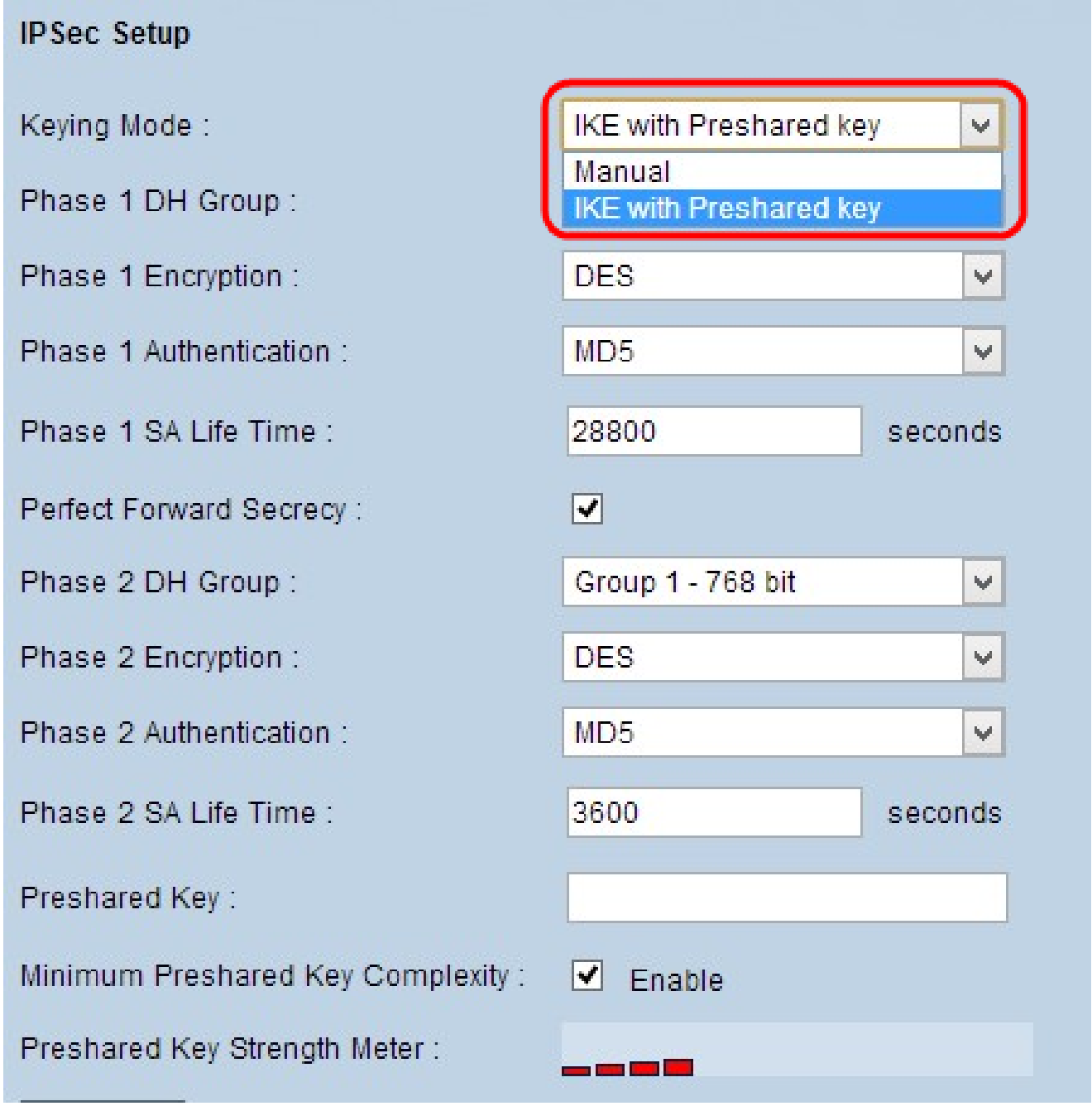
3단계. Save(저장)를 클릭하여 설정을 저장합니다.

IPSec 설정



IPSec(Internet Protocol Security)은 통신 세션 중에 인증 및 암호화를 통해 엔드 투 엔드 보안을 제공하는 인터넷 레이어 보안 프로토콜입니다.

참고: VPN의 양쪽 끝이 암호화, 암호 해독 및 인증 방법이 같아야 제대로 작동합니다. 두 라우터에 대해 동일한 IPSec 설정 설정을 입력합니다.

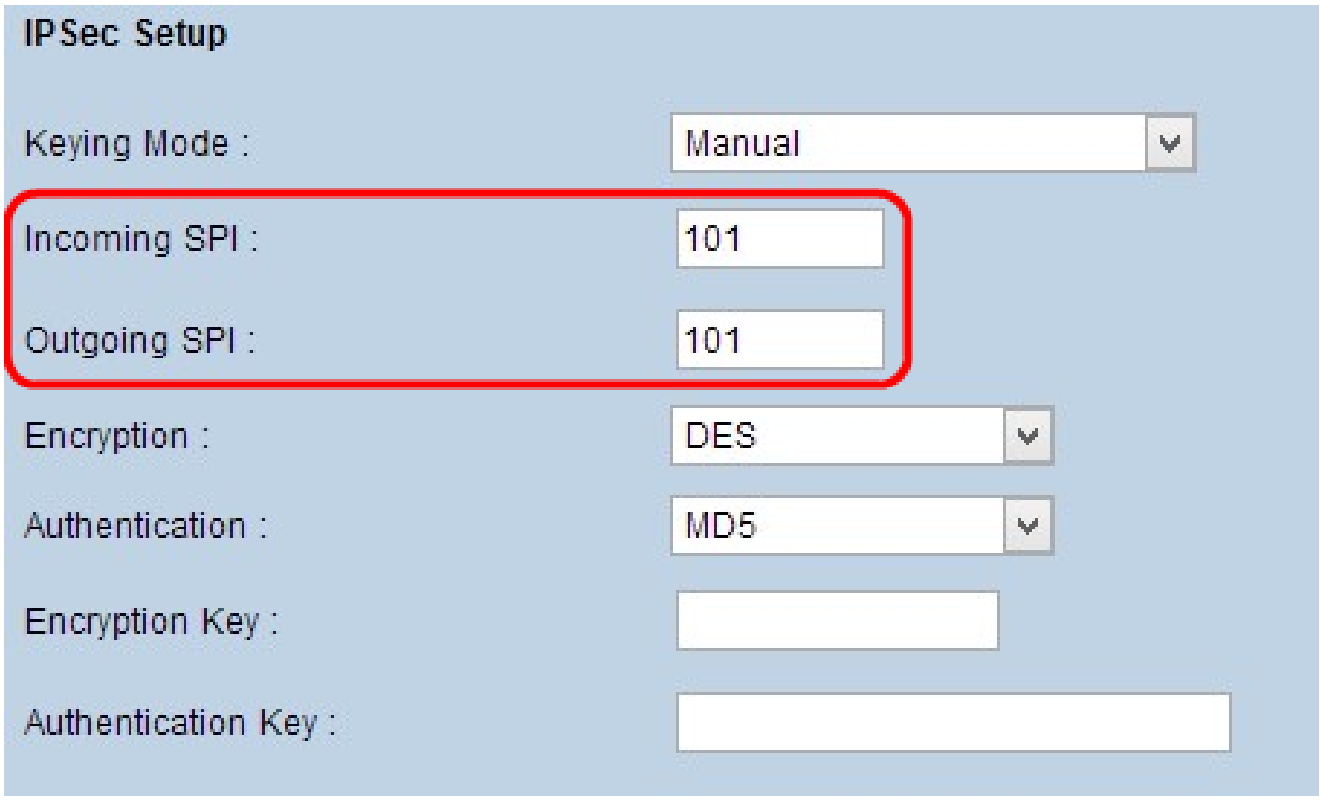


1단계. Keying Mode 드롭다운 목록에서 보안을 유지하려면 적절한 키 관리 모드를 선택합니다. 기본 모드는 사전 공유 키가 있는 IKE입니다.

· 수동 — 새 보안 키를 직접 생성하는 사용자 지정 보안 모드이며 키와 협상하지 않습니다. 문제 해결 중에 그리고 작은 정적 환경에서 사용하는 것이 가장 좋습니다.

· 사전 공유 키가 있는 IKE — IKE(Internet Key Exchange) 프로토콜은 터널에 대한 인증 통신을 설정하기 위해 사전 공유 키를 자동으로 생성하고 교환하는 데 사용됩니다.

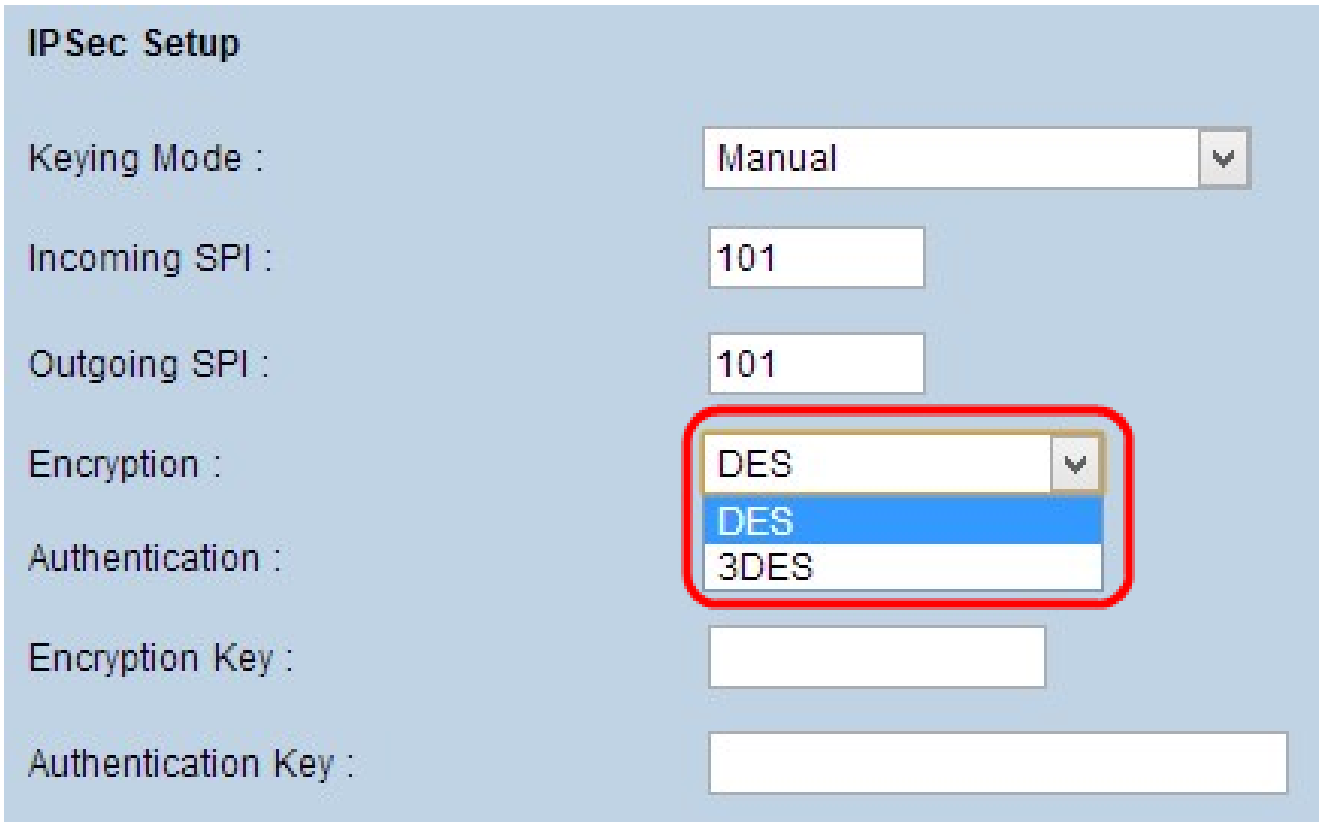
수동 키 지정 모드에 대한 IPSec 설정



1단계. Incoming SPI(Security Parameter Index) 필드에 SPI에 대한 고유한 16진수 값을 입력합니다. SPI는 ESP(Encapsulating Security Payload Protocol) 헤더에서 전송되며 수신 패킷에 대한 보호를 결정합니다. 100에서 ffffffff 사이의 값을 입력할 수 있습니다. 로컬 라우터의 수신 SPI는 원격 라우터의 발신 SPI와 일치해야 합니다.

2단계. 발신 SPI 필드에 발신 SPI(Security Parameter Index)의 고유한 16진수 값을 입력합니다. 100에서 ffffffff 사이의 값을 입력할 수 있습니다. 원격 라우터의 나가는 SPI는 로컬 라우터의 들어오는 SPI와 일치해야 합니다.

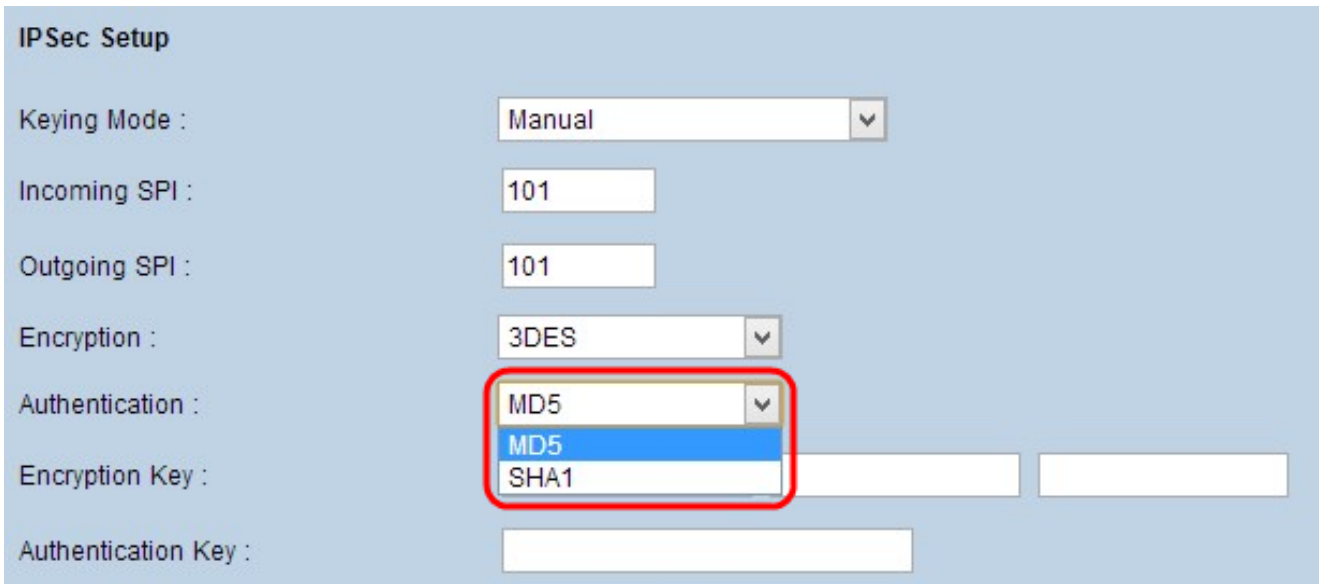
참고: 동일한 SPI를 가질 수 있는 터널은 두 개가 없습니다.



3단계. Encryption 드롭다운 목록에서 데이터에 적합한 암호화 방법을 선택합니다. 권장되는 암호화는 3DES입니다. VPN 터널은 양쪽 끝에서 동일한 암호화 방법을 사용해야 합니다.

· DES — DES(Data Encryption Standard)는 데이터 암호화에 56비트 키 크기를 사용합니다. DES는 오래되었으며 하나의 엔드포인트가 DES만 지원하는 경우에만 사용해야 합니다.

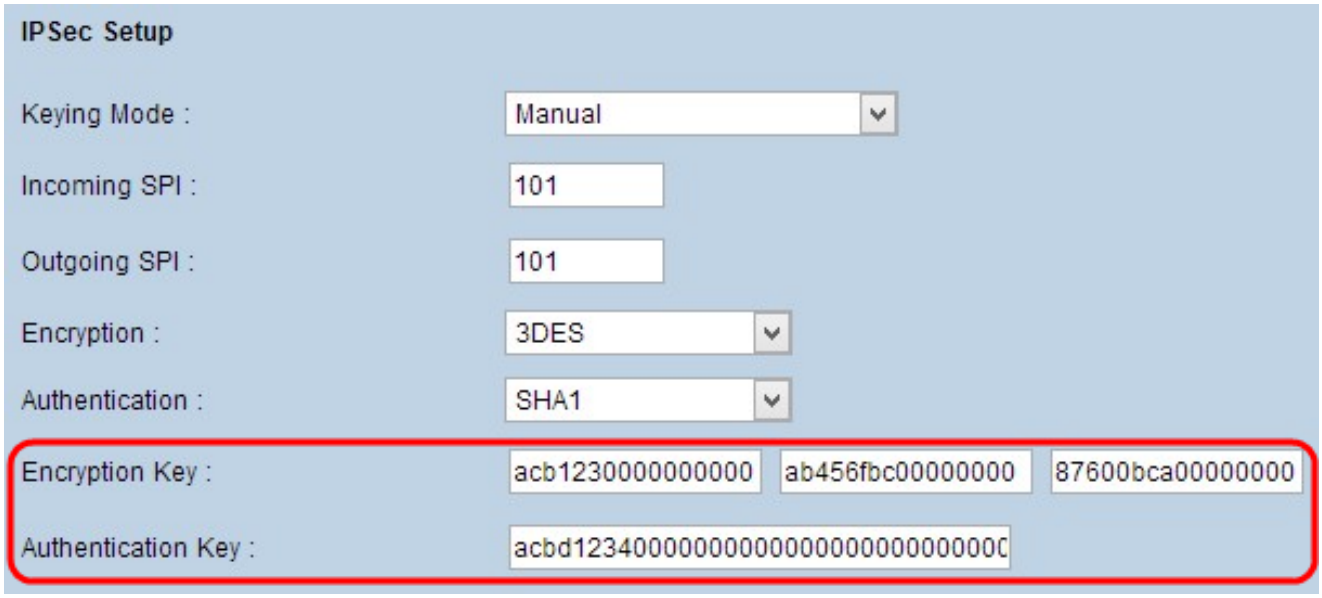
· 3DES — 3DES(Triple Data Encryption Standard)는 168비트의 간단한 암호화 방법입니다. 3DES는 데이터를 세 번 암호화하므로 DES보다 더 강력한 보안을 제공합니다.



4단계. Authentication 드롭다운 목록에서 데이터에 적합한 인증 방법을 선택합니다. MD5보다 안전하므로 권장되는 인증은 SHA1입니다. VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

· MD5 — MD5(Message Digest Algorithm-5)는 체크섬 계산을 통해 악의적인 공격으로부터 데이터를 보호하는 128비트 해시 함수입니다.

· SHA1 — SHA1(Secure Hash Algorithm version 1)은 160비트 해시 함수로 MD5보다 안전하지만 계산에는 시간이 더 걸립니다.

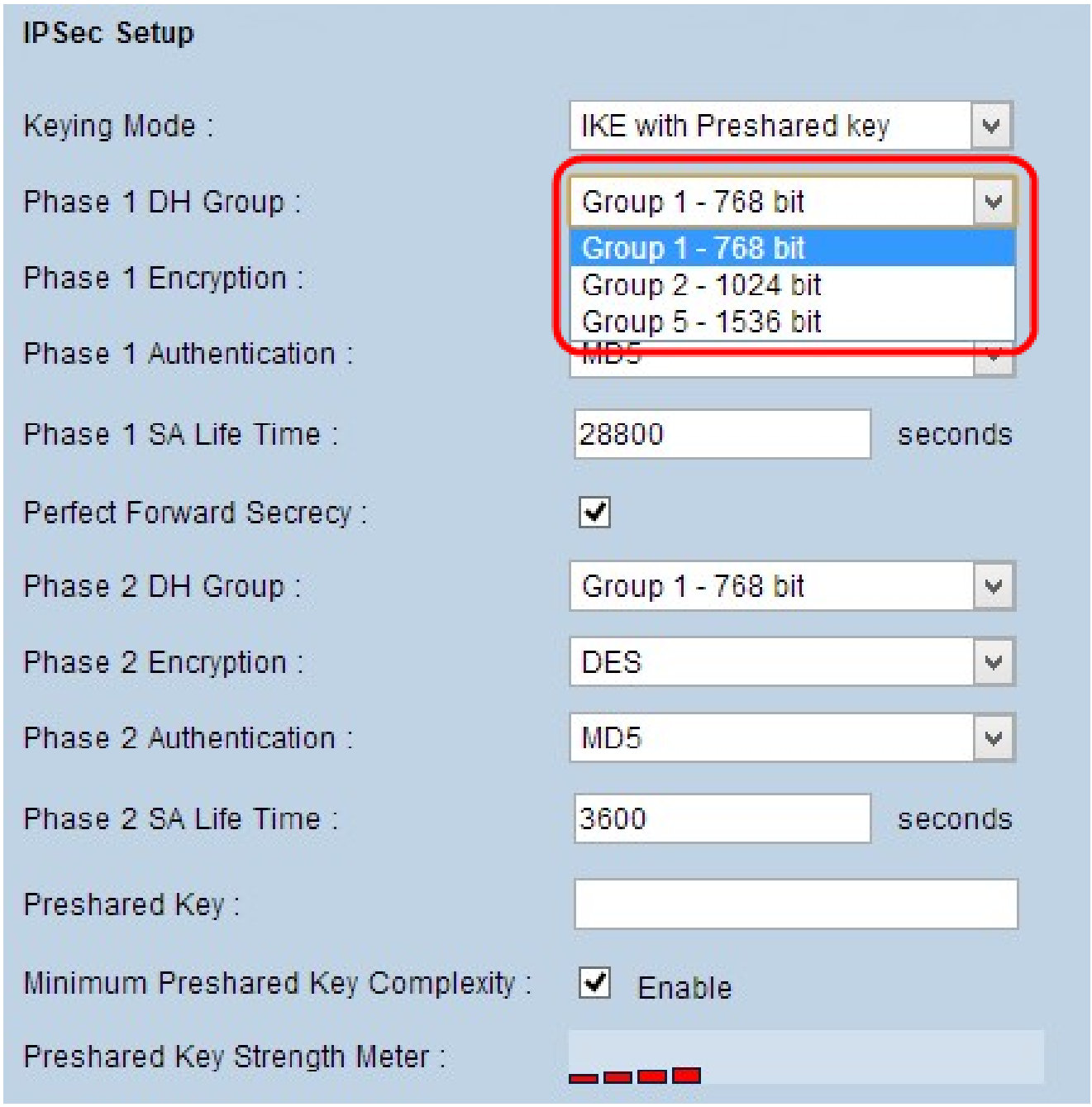


5단계. Encryption Key(암호화 키) 필드에 데이터를 암호화하고 해독할 키를 입력합니다. 3단계에서 암호화 방법으로 DES를 선택하는 경우 16자리 16진수 값을 입력합니다. 3단계에서 암호화 방법으로 3DES를 선택한 경우 40자리 16진수 값을 입력합니다.

6단계. Authentication Key(인증 키) 필드에 트래픽을 인증하기 위한 사전 공유 키를 입력합니다. 4단계에서 MD5를 인증 방법으로 선택하는 경우 32자리 16진수 값을 입력합니다. 4단계에서 인증 방법으로 SHA1을 선택하는 경우 40자리 16진수 값을 입력합니다. 충분한 숫자를 추가하지 않으면, 충분한 숫자가 있을 때까지 끝에 0이 추가됩니다. VPN 터널은 양쪽 끝에 동일한 사전 공유 키를 사용해야 합니다.

7단계. Save(저장)를 클릭하여 설정을 저장합니다.

사전 공유 키 모드 컨피그레이션이 있는 IKE

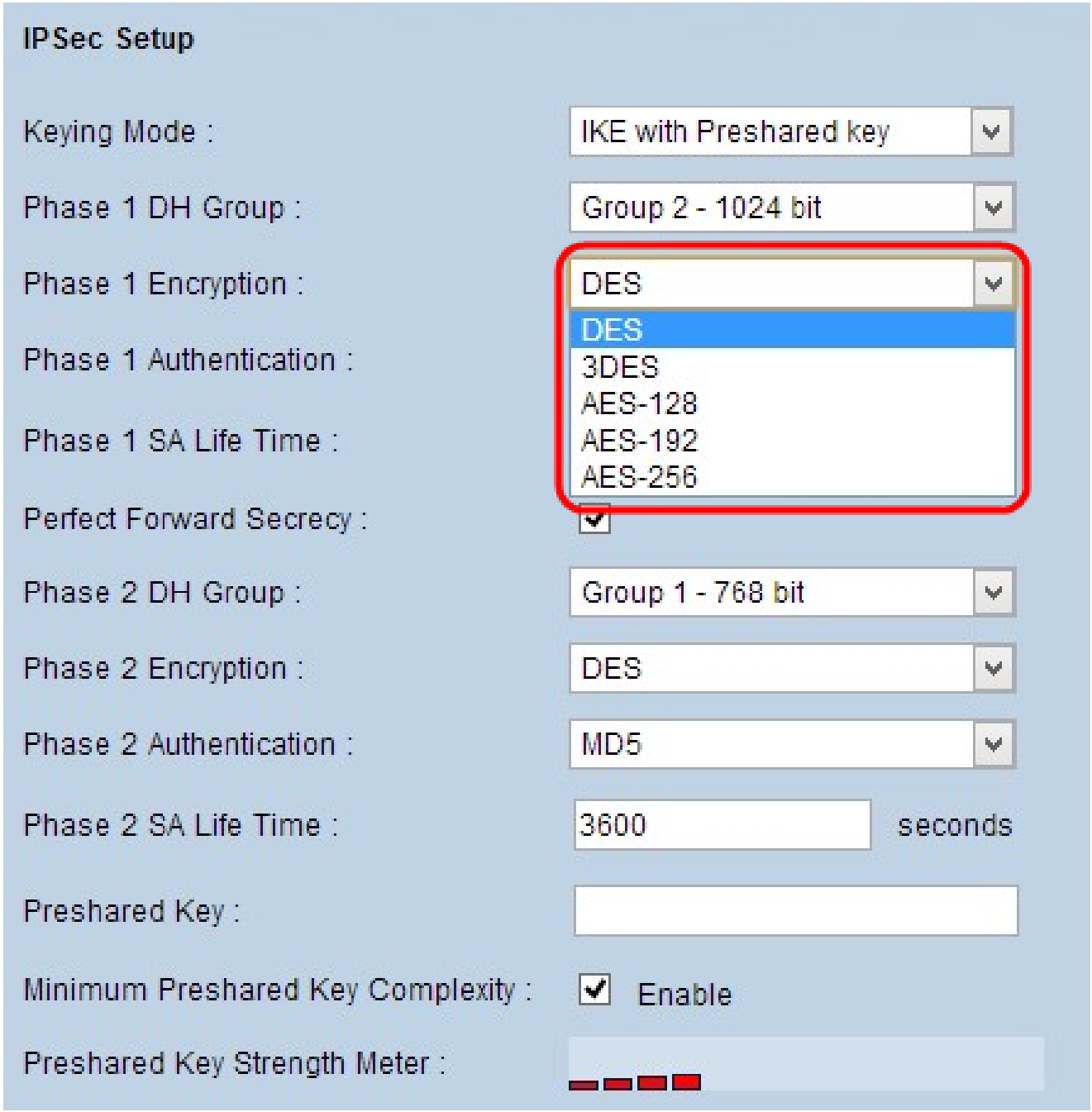


1단계. Phase 1 DH Group(1단계 DH 그룹) 드롭다운 목록에서 적절한 1단계 DH 그룹을 선택합니다. 1단계는 안전한 인증 통신을 지원하기 위해 터널의 양쪽 끝 간에 간단한 SA(Logical Security Association)를 설정하는 데 사용됩니다. DH(Diffie-Hellman)는 1단계 중에 키의 강도를 확인하는 데 사용되는 암호화 키 교환 프로토콜이며 통신을 인증하기 위해 비밀 키를 공유합니다.

· Group 1 - 768 bit(그룹 1 - 768비트) - 가장 약한 키 및 가장 안전하지 않은 인증 그룹이지만 IKE 키를 계산하는 데 가장 적은 시간이 걸립니다. 이 옵션은 네트워크 속도가 낮은 경우 사용하는 것이 좋습니다.

· Group 2 - 1024비트 — Group 1보다 더 강력한 키와 더 안전한 인증 그룹이지만 IKE 키를 계산하는 데 더 많은 시간이 걸립니다.

· Group 5 - 1536비트 — 가장 강력한 키와 가장 안전한 인증 그룹입니다. IKE 키를 계산하는 데 시간이 더 필요합니다. 네트워크 속도가 빠른 것이 좋습니다.



2단계. Phase 1 Encryption(1단계 암호화) 드롭다운 목록에서 키를 암호화하기에 적합한 1단계 암호화를 선택합니다. AES-128, AES-192 또는 AES-256이 권장됩니다. VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

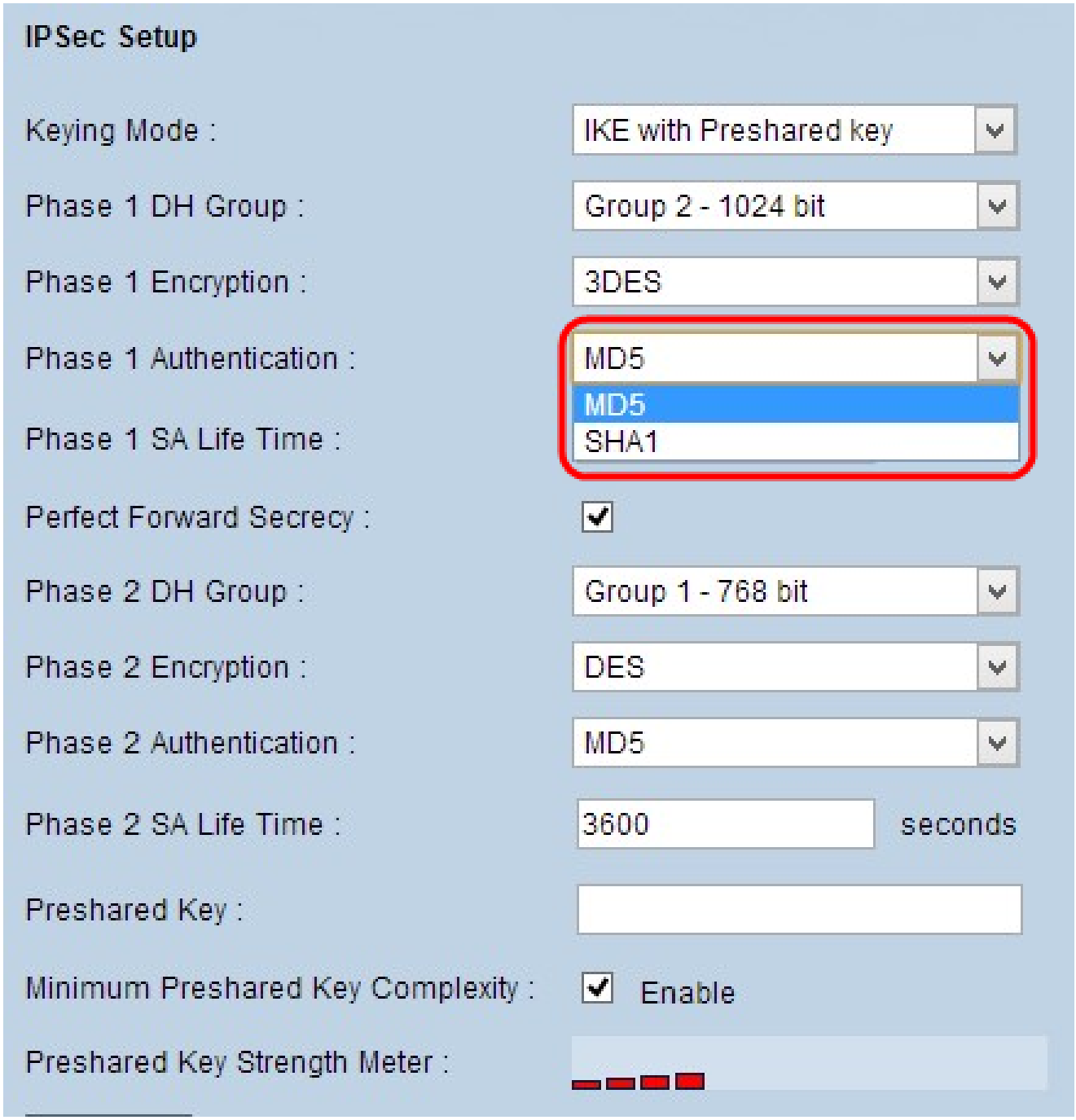
· DES — DES(Data Encryption Standard)는 데이터 암호화에 56비트 키 크기를 사용합니다. DES는 오래되었으며 하나의 엔드포인트가 DES만 지원하는 경우에만 사용해야 합니다.

· 3DES — 3DES(Triple Data Encryption Standard)는 168비트의 간단한 암호화 방법입니다. 3DES는 데이터를 세 번 암호화하므로 DES보다 더 강력한 보안을 제공합니다.

· AES-128 — AES(Advanced Encryption Standard)는 128비트 암호화 방법으로 일반 텍스트를 10회의 반복 과정을 거쳐 암호 텍스트로 변환합니다.

· AES-192 — AES(Advanced Encryption Standard)는 192비트 암호화 방법으로 일반 텍스트를 12회의 반복 과정을 거쳐 암호 텍스트로 변환합니다. AES-192는 AES-128보다 안전합니다.

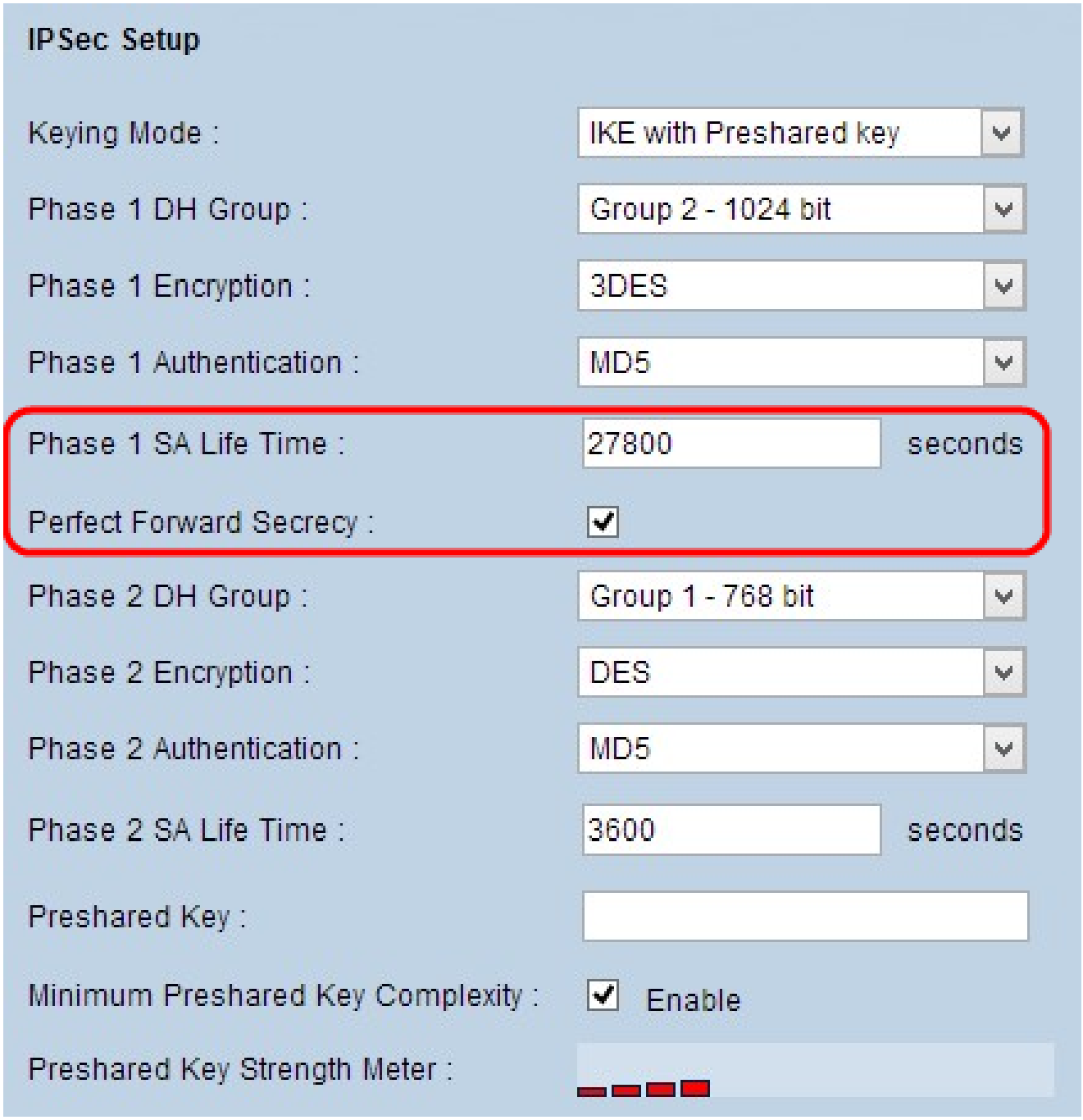
· AES-256 — AES(Advanced Encryption Standard)는 256비트 암호화 방법으로 일반 텍스트를 14회의 반복 과정을 거쳐 암호 텍스트로 변환합니다. AES-256은 가장 안전한 암호화 방법입니다.



3단계. Phase 1 Authentication 드롭다운 목록에서 적절한 Phase 1 인증 방법을 선택합니다. VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다. SHA1을 사용하는 것이 좋습니다.

· MD5 — MD5(Message Digest Algorithm-5)는 체크섬 계산으로 악의적인 공격으로부터 데이터를 보호하는 128비트 해시 함수입니다.

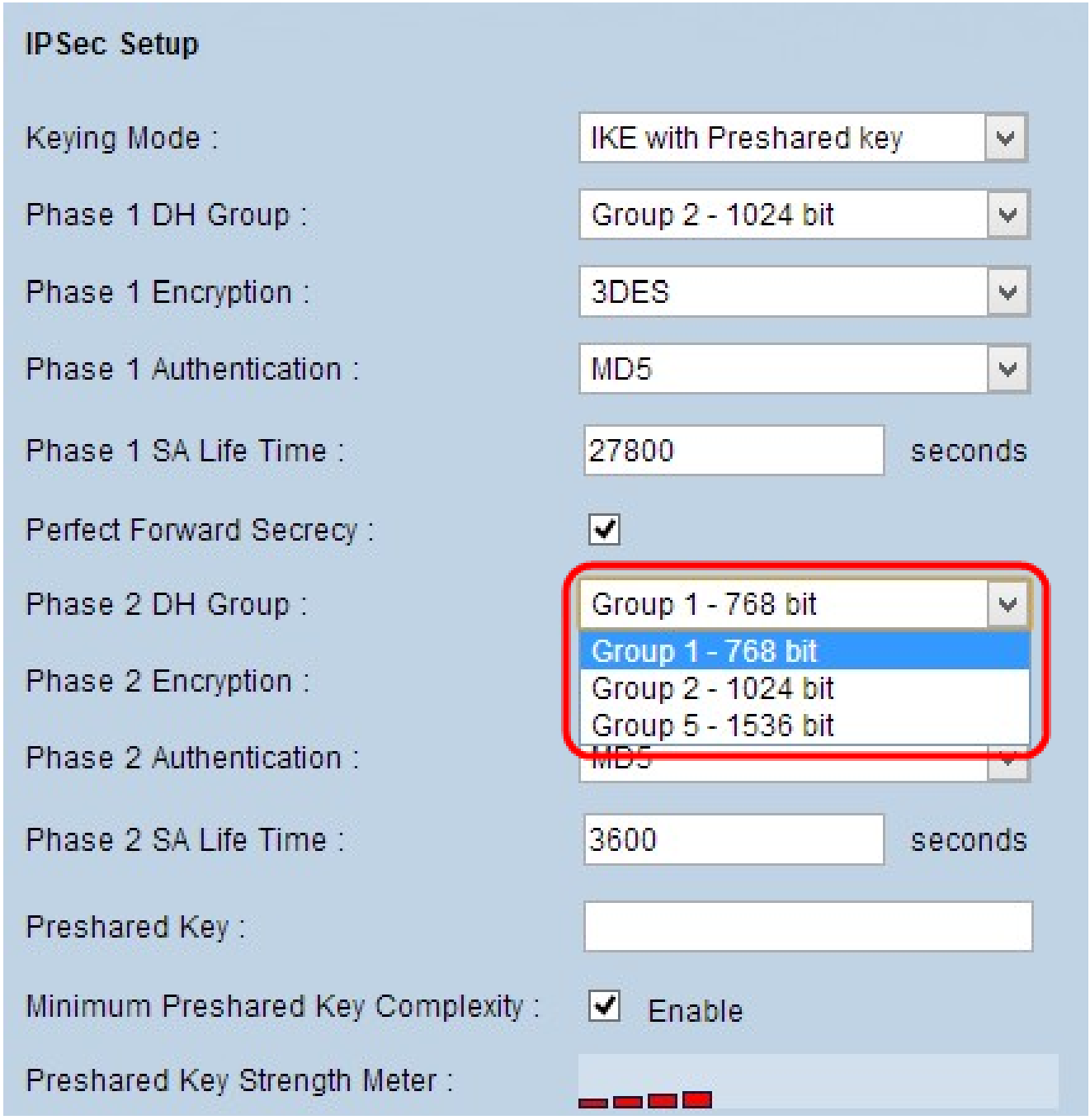
· SHA1 — SHA1(Secure Hash Algorithm version 1)은 160비트 해시 함수로 MD5보다 안전하지만 계산에는 시간이 더 걸립니다.



4단계. 1단계 키가 유효하고 VPN 터널이 활성 상태로 유지되는 시간을 1단계 SA 수명 필드에

초 단위로 입력합니다.

5단계. 키에 더 많은 보호를 제공 하려면 Perfect Forward Secrecy 확인 란을 선택 합니다. 이 옵션을 사용하면 키가 손상된 경우 라우터에서 새 키를 생성할 수 있습니다. 암호화된 데이터는 감염된 키를 통해서만 감염됩니다. 이는 더 많은 보안을 제공하므로 권장되는 조치입니다.



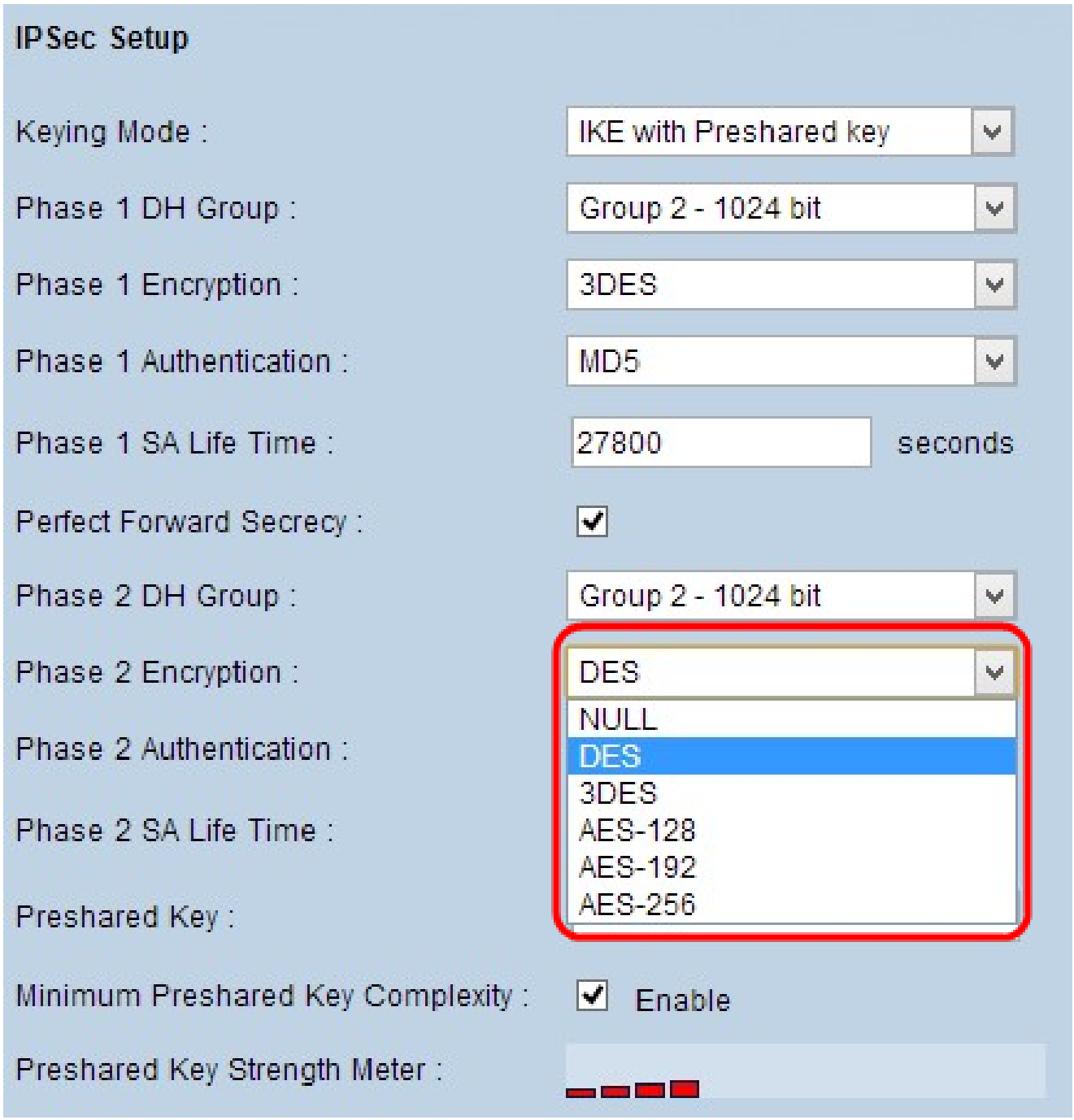
6단계. Phase 2 DH Group(Phase 2 DH 그룹) 드롭다운 목록에서 적절한 Phase 2 DH 그룹을 선택합니다. 2단계에서는 보안 연계를 사용하며 데이터 패킷이 두 엔드포인트를 통과할 때 보안을 결정하는 데 사용됩니다.

· Group 1 - 768 bit(그룹 1 - 768비트) - 가장 낮은 수준의 키와 가장 안전하지 않은 인증 그룹

이지만 IKE 키를 계산하는 데 가장 적은 시간이 걸립니다. 이 옵션은 네트워크 속도가 낮은 경우 사용하는 것이 좋습니다.

· Group 2 - 1024비트 — Group 1보다 더 강력한 키와 더 안전한 인증 그룹이지만 IKE 키를 계산하는 데 더 많은 시간이 걸립니다.

· Group 5 - 1536비트 — 가장 강력한 키와 가장 안전한 인증 그룹입니다. IKE 키를 계산하는 데 시간이 더 필요합니다. 네트워크 속도가 빠른 것이 좋습니다.



7단계. Phase 2 Encryption(2단계 암호화) 드롭다운 목록에서 키를 암호화하기에 적합한 2단계 암호화를 선택합니다. AES-128, AES-192 또는 AES-256이 권장됩니다. VPN 터널은 양쪽

끝에 동일한 암호화 방법을 사용해야 합니다.

· NULL — 암호화가 사용되지 않습니다.

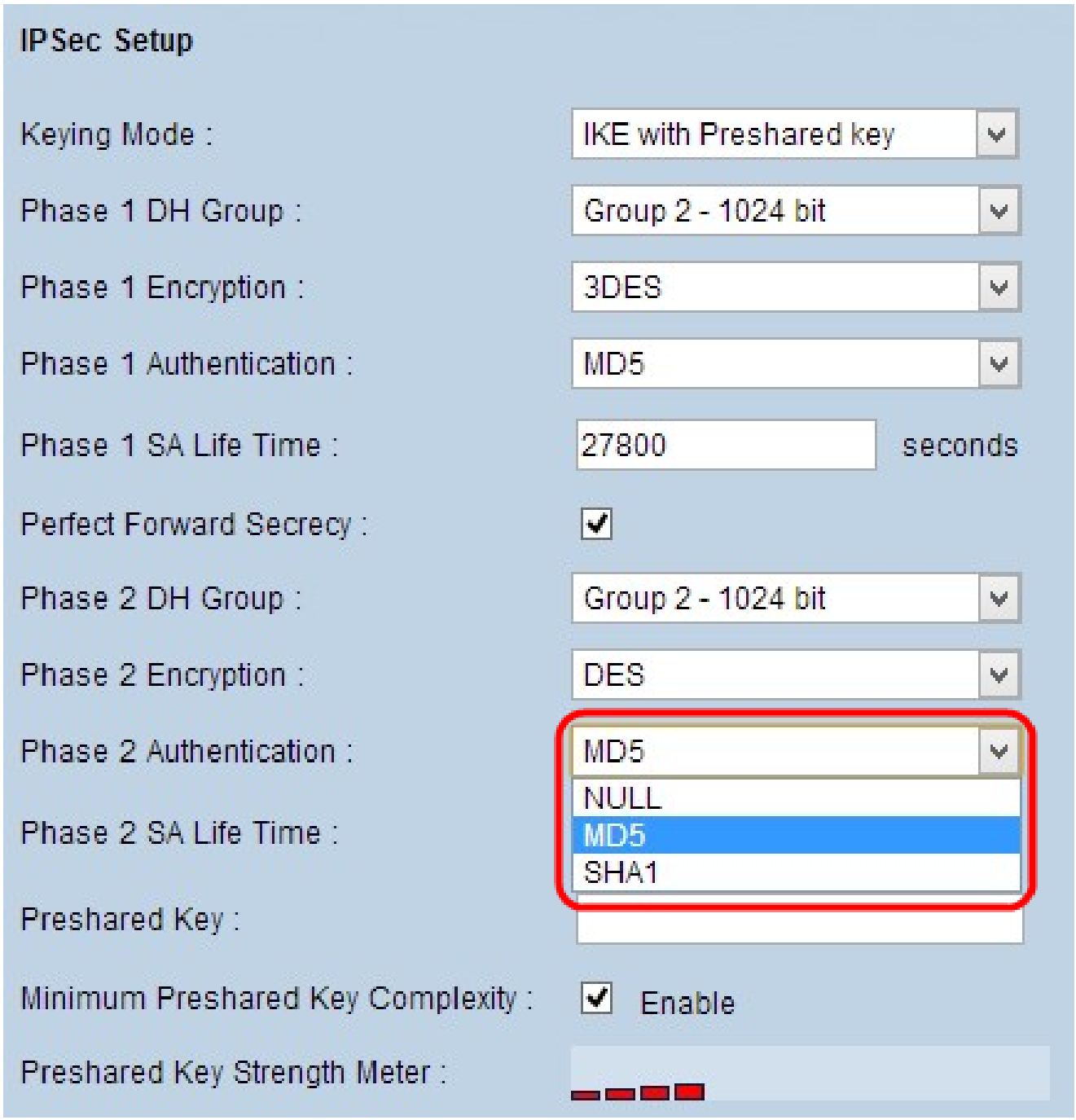
· DES — DES(Data Encryption Standard)는 데이터 암호화에 56비트 키 크기를 사용합니다. DES는 오래되었으며 하나의 엔드포인트가 DES만 지원하는 경우에만 사용해야 합니다.

· 3DES — 3DES(Triple Data Encryption Standard)는 168비트의 간단한 암호화 방법입니다. 3DES는 데이터를 세 번 암호화하므로 DES보다 더 강력한 보안을 제공합니다.

· AES-128 — AES(Advanced Encryption Standard)는 128비트 암호화 방법으로 일반 텍스트를 10회의 반복 과정을 거쳐 암호 텍스트로 변환합니다.

· AES-192 — AES(Advanced Encryption Standard)는 192비트 암호화 방법으로 일반 텍스트를 12회의 반복 과정을 거쳐 암호 텍스트로 변환합니다. AES-192는 AES-128보다 안전합니다.

· AES-256 — AES(Advanced Encryption Standard)는 256비트 암호화 방법으로 일반 텍스트를 14회의 반복 과정을 거쳐 암호 텍스트로 변환합니다. AES-256은 가장 안전한 암호화 방법입니다.

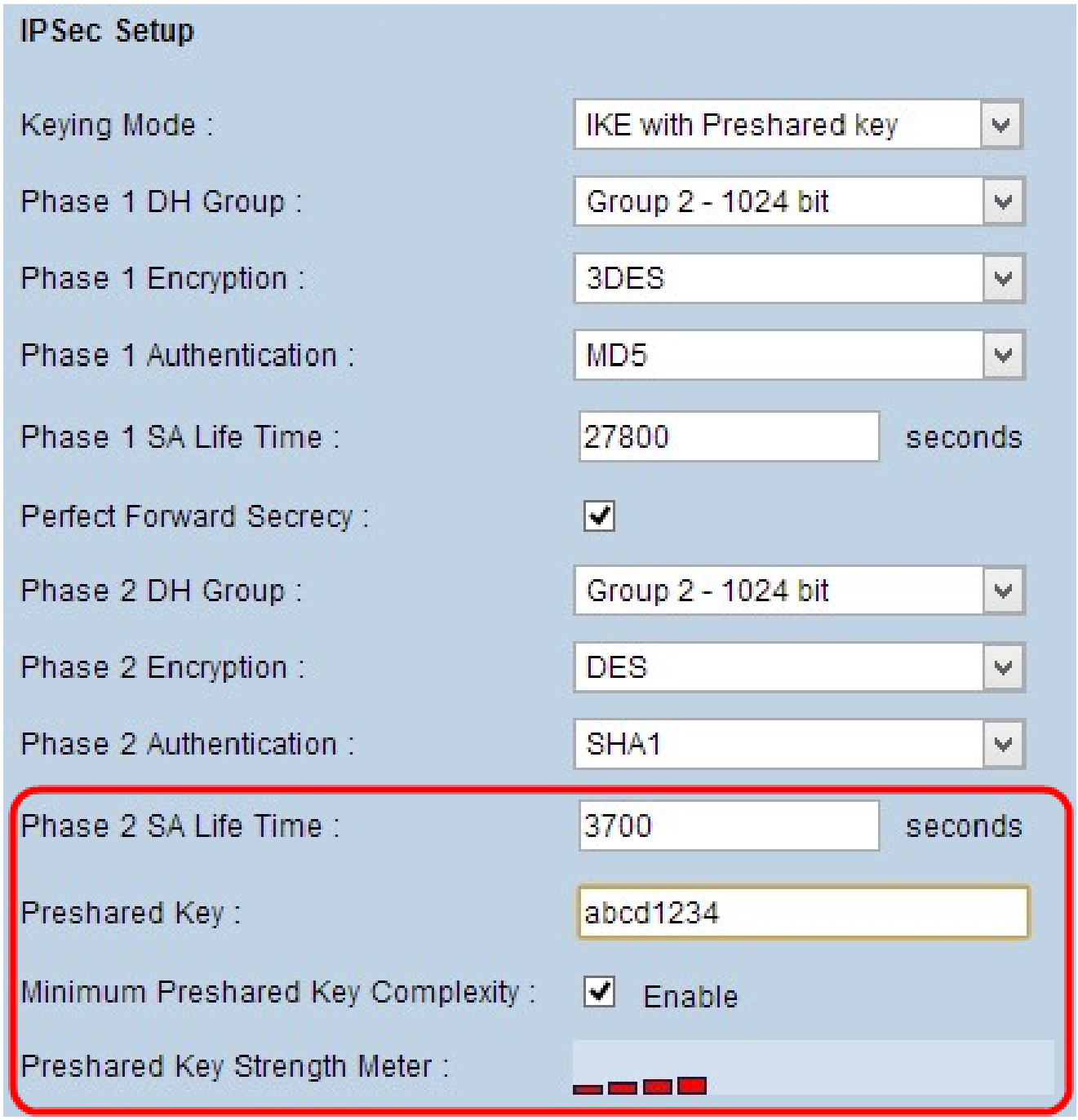


8단계. Phase 2 Authentication 드롭다운 목록에서 적절한 인증 방법을 선택합니다. VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다. SHA1을 사용하는 것이 좋습니다.

· MD5 — MD5(Message Digest Algorithm-5)는 체크섬 계산으로 악의적인 공격으로부터 데이터를 보호하는 128비트 16진수 해시 함수입니다.

· SHA1 — SHA1(Secure Hash Algorithm version 1)은 160비트 해시 함수로 MD5보다 안전하지만 계산에는 시간이 더 걸립니다.

· Null — 인증 방법이 사용되지 않습니다.



9단계. Phase 2 키가 유효하고 VPN 터널이 활성 상태로 유지되는 시간을 Phase 2 SA Life Time 필드에 초 단위로 입력합니다.

10단계. Preshared Key(사전 공유 키) 필드에 피어를 인증하기 위해 IKE 피어 간에 이전에 공유되는 키를 입력합니다. 최대 30개의 16진수 및 문자를 사전 공유 키로 사용할 수 있습니다. VPN 터널은 양쪽 끝에 동일한 사전 공유 키를 사용해야 합니다.

참고: VPN의 보안을 유지하려면 IKE 피어 간의 사전 공유 키를 자주 변경하는 것이 좋습니다 .

11단계. (선택 사항) 사전 공유 키에 강도 측정기를 사용하려면 Minimum Preshared Key

Complexity(사전 공유 키 복잡성 최소) 확인란을 선택합니다. 색상 막대를 통해 사전 공유 키의 강도를 확인하는 데 사용됩니다.

· 사전 공유 키 강도 측정기 — 색상 막대를 통해 사전 공유 키의 강도를 표시합니다. 빨강은 약한 강도, 노랑은 수용가능한 강도, 녹색은 강한 강도를 나타냅니다.

12단계. Save(저장)를 클릭하여 설정을 저장합니다.

참고: 게이트웨이 간 VPN에 대한 고급 섹션에서 사용 가능한 옵션을 구성하려면 RV016, RV042, RV042G 및 RV082 VPN Router에서 게이트웨이 간 VPN에 대한 고급 설정 구성을 참조하십시오.

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.