# RV160 및 RV260에서 IPSec 프로파일 구성(자동 키잉 모드)

이 문서에서는 RV160 및 RV260 시리즈 라우터에서 자동 키 모드를 사용하여 새 IPsec(Internet Protocol Security) 프로필을 생성하는 방법을 살펴봅니다.

IPsec은 인터넷을 통해 안전한 개인 통신을 보장합니다.인터넷을 통해 중요한 정보를 전송하는 데 필요한 2개 이상의 호스트의 프라이버시, 무결성 및 신뢰성을 제공합니다.IPsec은 일반적으로 VPN(Virtual Private Network)에서 사용되며 IP 레이어에서 구현되며, 이를 사용하면 보안이 부족한 많은 애플리케이션을 지원할 수 있습니다.VPN은 인터넷과 같은 보안되지 않은 네트워크를 통해 전송되는 민감한 데이터 및 IP 정보에 대한 보안 통신 메커니즘을 제공하는 데 사용됩니다.원격 사용자와 조직을 위해 동일한 네트워크의 다른 사용자로부터 중요한 정보를 보호할 수 있는 유연한 솔루션을 제공합니다.

VPN 터널의 두 끝이 성공적으로 암호화되어 설정되려면 암호화, 암호 해독 및 인증 방법에 모두 동의해야 합니다.IPsec 프로파일은 IPsec의 중앙 컨피그레이션으로, 자동 모드 및 수동 키 지정 모드에서의 Phase I 및 II 협상에 대한 암호화, 인증 및 DH(Diffie-Hellman) 그룹과 같은 알고리즘을 정의합니다.1단계에서는 보안 인증 통신을 만들기 위해 사전 공유 키를 설정합니다.2단계에서는 트래픽이 암호화됩니다.프로토콜, 모드, 알고리즘, PFS(Perfect Forward Secrecy), SA(Security Association) 수명, 키 관리 프로토콜 등 대부분의 IPsec 매개변수를 구성할 수 있습니다.

Site-to-Site VPN을 구성할 때 원격 라우터는 로컬 라우터와 동일한 프로파일 설정을 가져야 합니다.

Cisco IPsec 기술에 대한 추가 정보는 다음 링크에서 확인할 수 있습니다.Cisco IPSec 기술 소개.

VPN 설정 마법사를 사용하여 IPsec 프로필 및 Site-to-Site VPN을 구성하려면 다음 링크를 클릭하십시오.RV160 및 RV260에서 VPN 설정 마법사 구성.

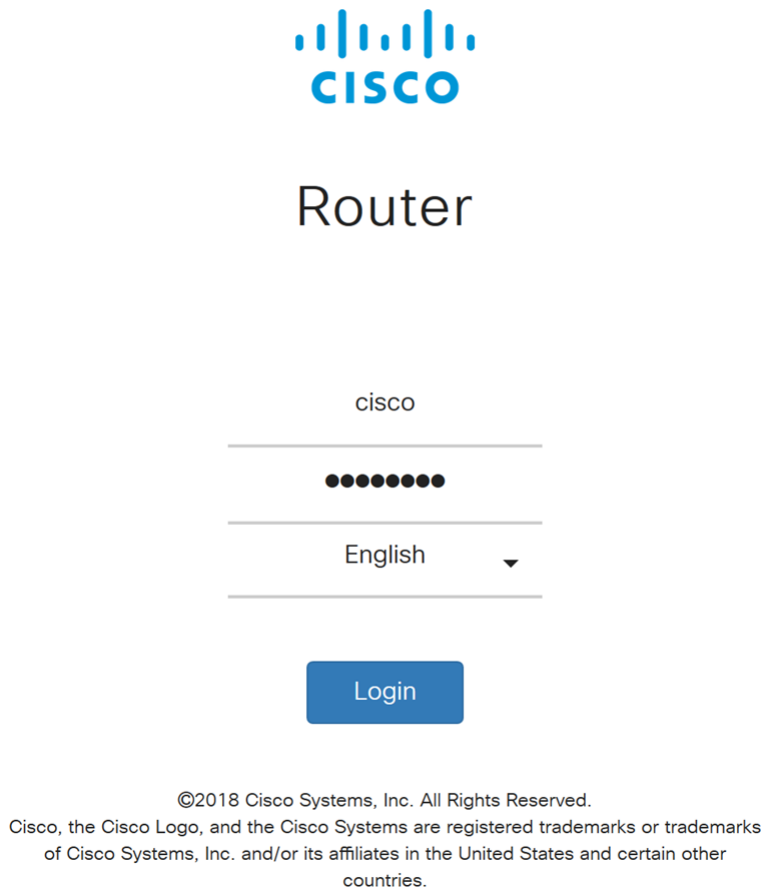
사이트 대 사이트 VPN을 구성하려면 다음 문서를 참조하십시오.RV160 및 RV260에서 Site-to-Site VPN 구성.

- RV160
- RV260

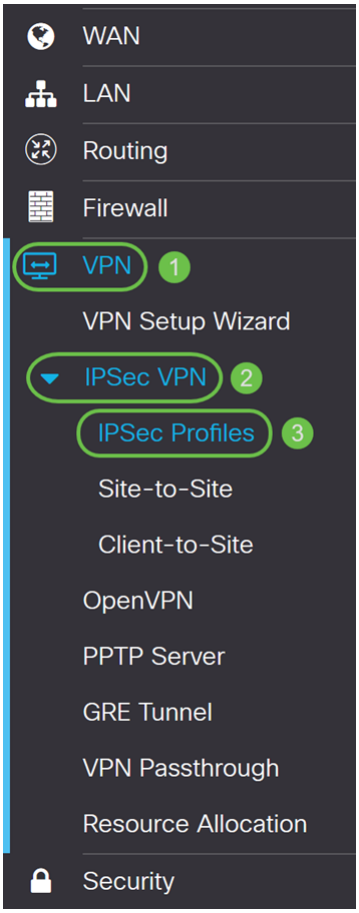
·1.0.00.13

IPsec

1단계. 라우터의 웹 컨피그레이션 페이지에 로그인합니다.

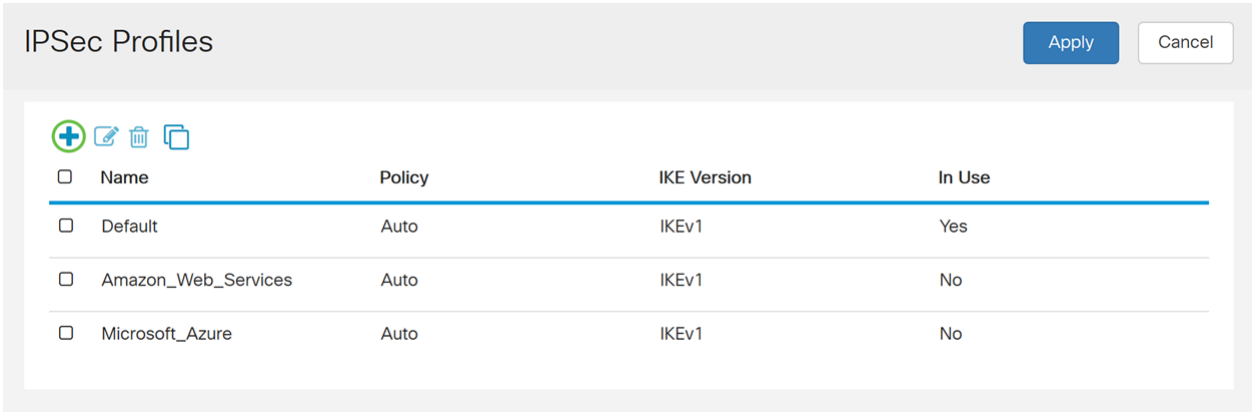



2단계. **VPN > IPSec VPN > IPSec 프로필로 이동합니다.**




3단계. IPSec *Profiles* 테이블에서 **Add**를 클릭하여 새 IPsec 프로필을 생성합니다.프로파일을

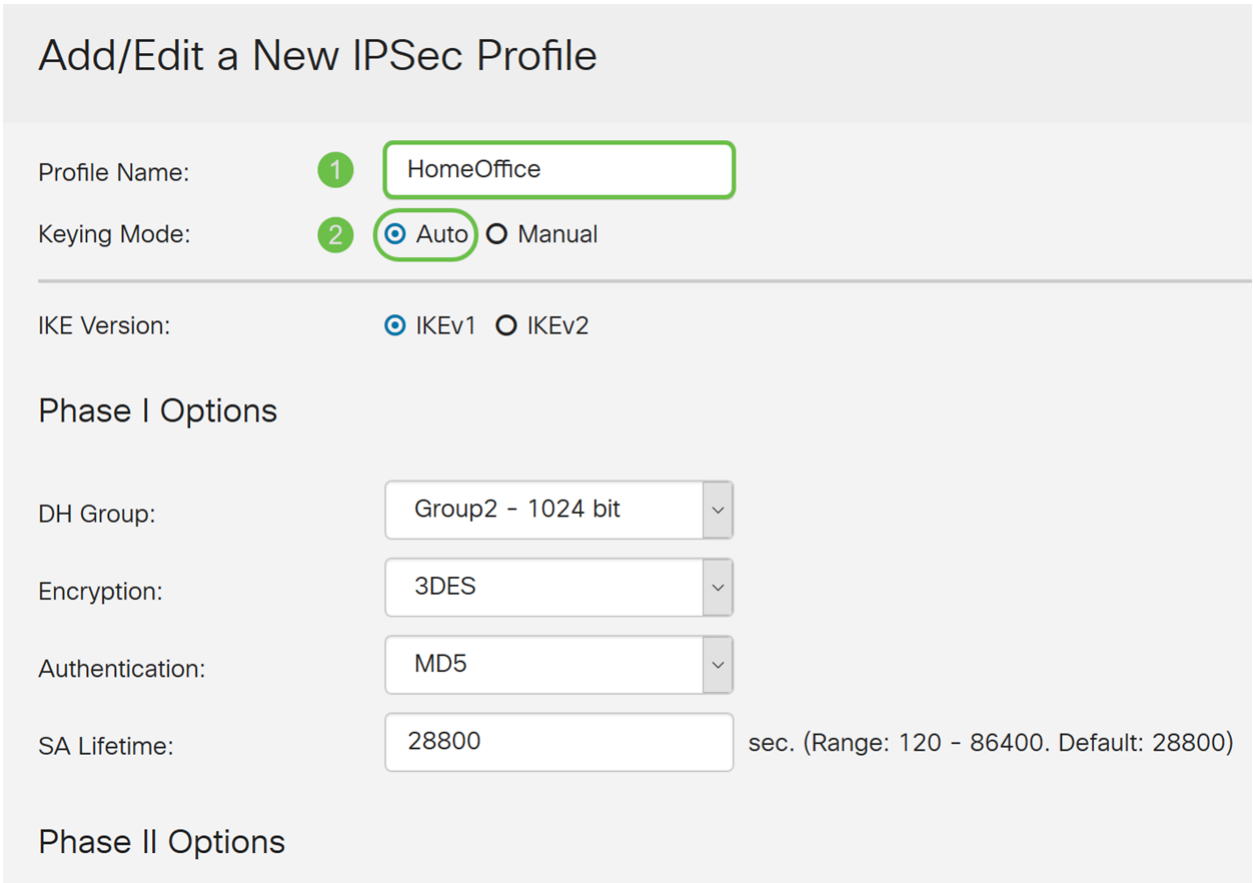
편집, 삭제 또는 복제할 수도 있습니다.




4단계. 프로파일 이름을 입력하고 키 모드(자동 또는 수동)를 선택합니다.

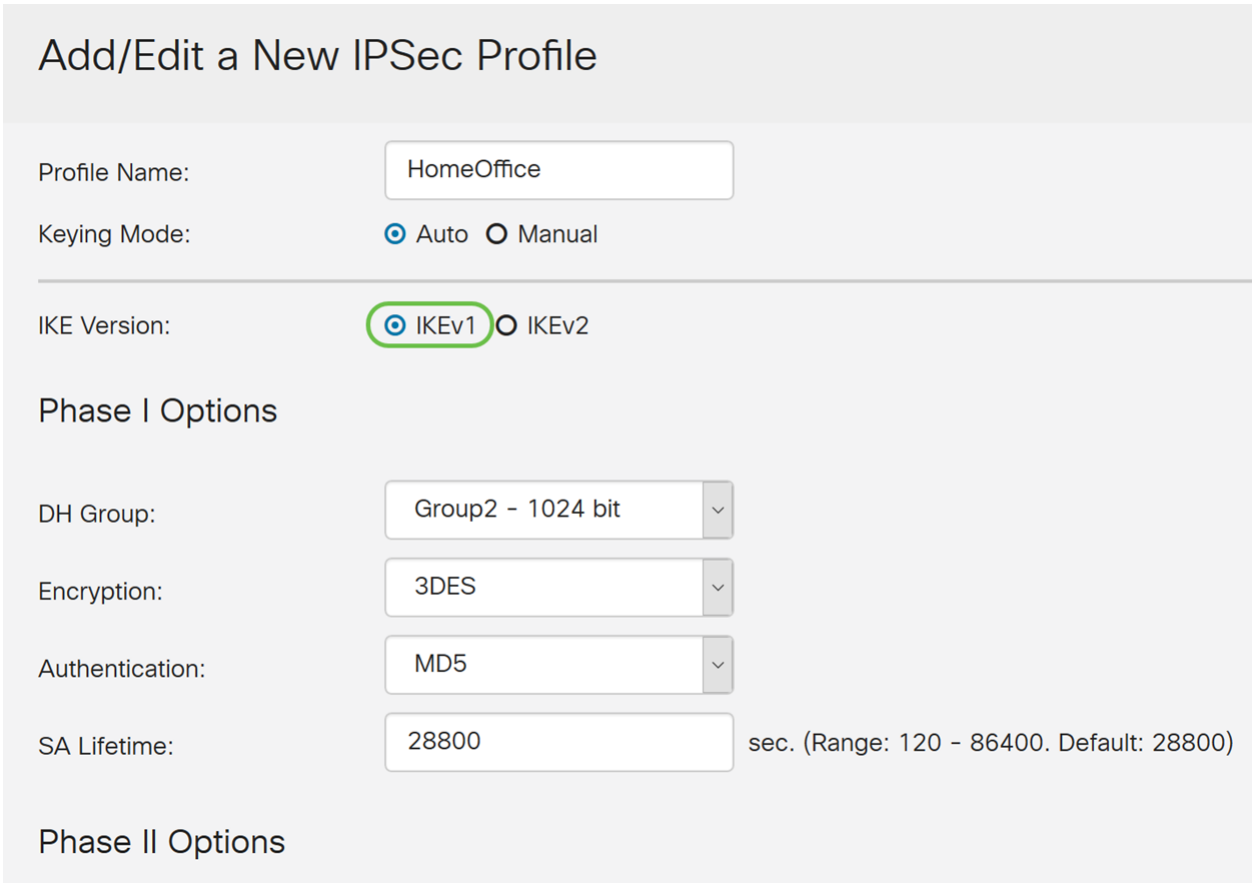
**HomeOffice**가 *프로필 이름*으로 *입력됩니다*.

**키** *모드*에 대해 자동*이 선택됩니다*.



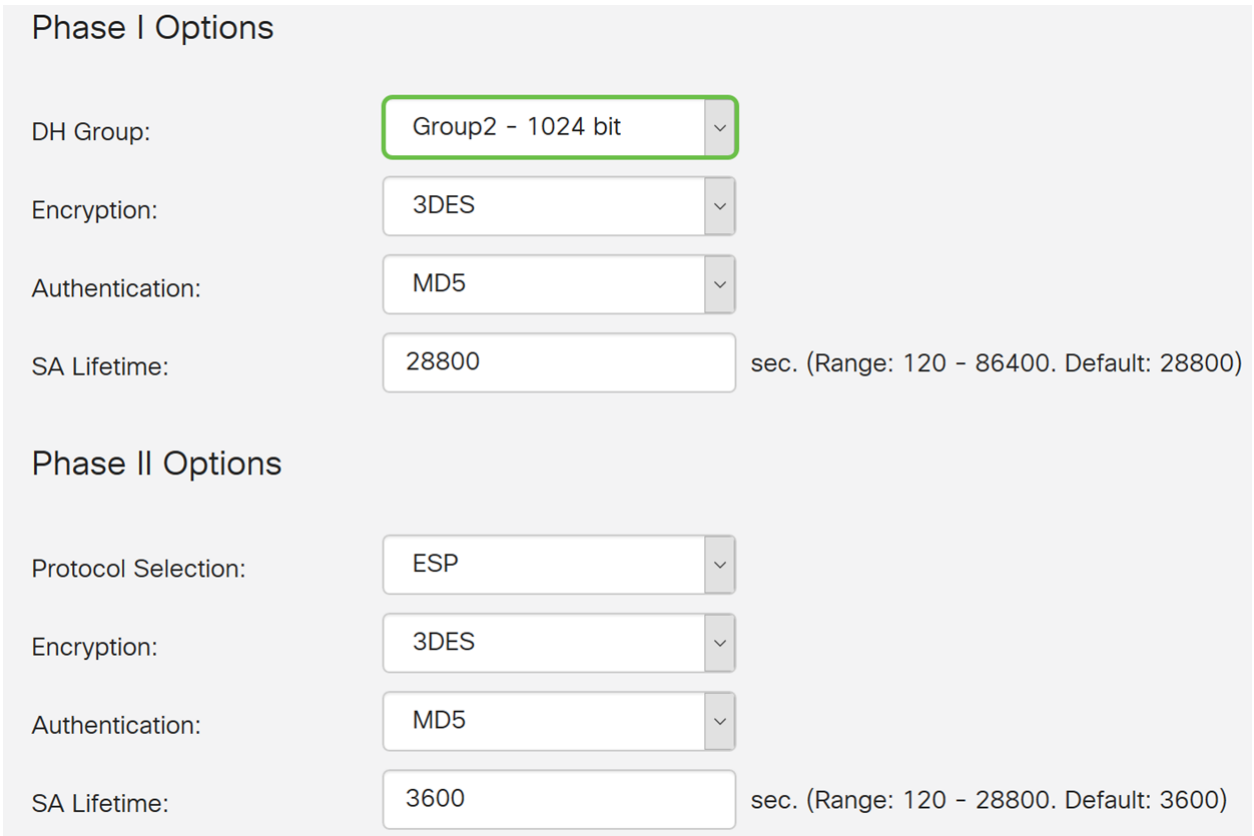

5단계. *IKEv1(Internet Key Exchange Version 1*) 또는 *IKEv2(Internet Key Exchange Version 2)*를 IKE 버전으로 선택합니다.IKE는 ISAKMP(Internet Security Association and Key Management Protocol) 프레임워크 내에서 Oakley 키 교환 및 SKEME 키 교환을 구현하는 하이브리드 프로토콜입니다.오클리와 스케미는 모두 인증된 키 자료를 도출하는 방법을 정의하지만, 스키엠은 빠른 키 재질도 포함하고 있다.IKE는 IPsec 피어에 대한 인증을 제공하고 IPsec 키를 협상하며 IPsec 보안 연결을 협상합니다.IKEv2는 키 교환을 수행하는 데 필요한 패킷 수가 적고, 더 많은 인증 옵션을 지원하는 반면, IKEv1은 공유 키 및 인증서 기반 인증만 수행하기 때문에 더 효율적입니다.이 예에서는 **IKEv1**이 IKE 버전으로 선택되었습니다.

**참고:**디바이스가 IKEv2를 지원하는 경우 IKEv2를 사용하는 것이 좋습니다. 디바이스가 IKEv2를 지원하지 않는 경우 IKEv1을 사용합니다.



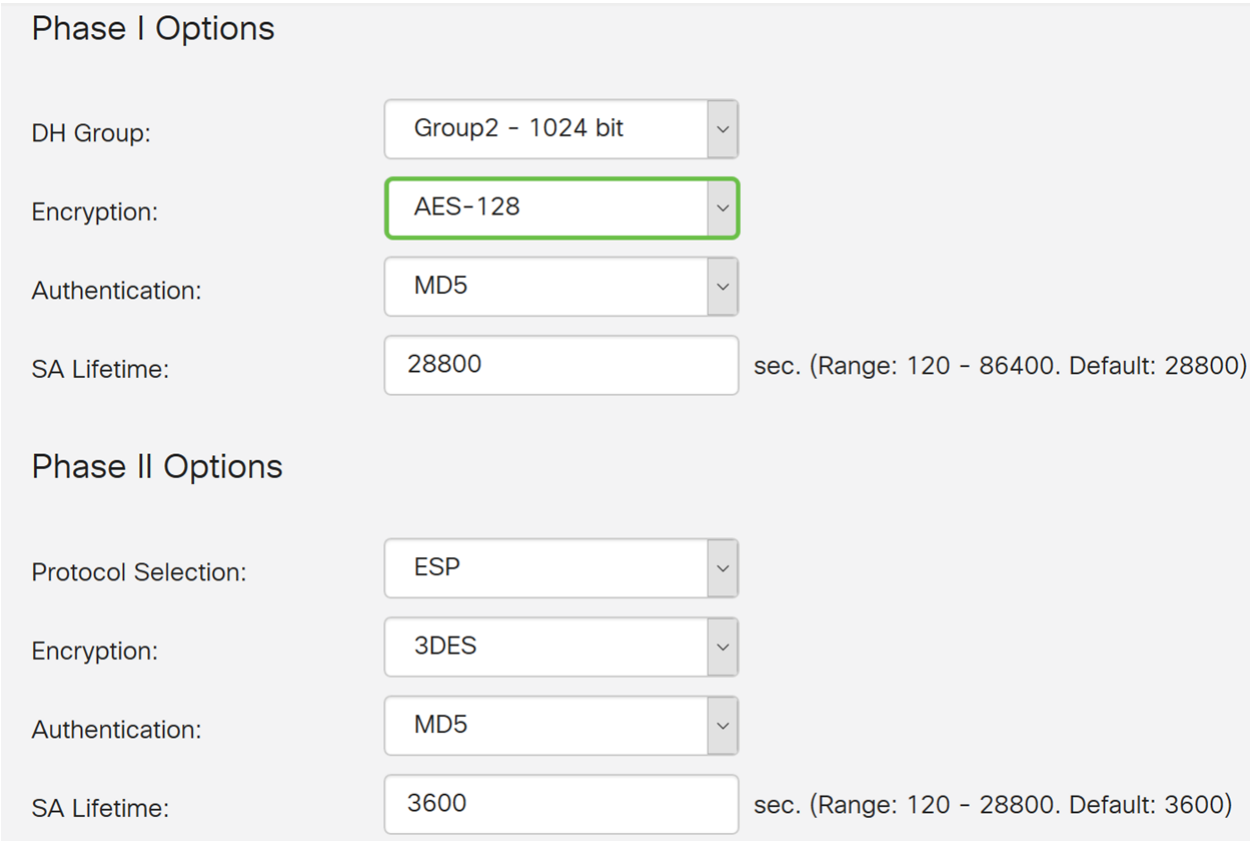

6단계. I 단계에서는 II 단계에서 데이터를 암호화하는 데 사용할 키를 설정하고 교환합니다 .Phase *I* 섹션에서 DH(Diffie-Hellman) 그룹을 선택합니다.DH는 키 교환 프로토콜로서, **그룹 2 - 1024비트** 및 **그룹 5 - 1536비트**의 서로 다른 기본 키 길이의 두 그룹**을 사용합니다**.이 데모에 **그룹 2 - 1024비트**를 선택했습니다.

**참고:**더 빠른 속도와 더 낮은 보안을 위해 그룹 2를 선택합니다. 더 느린 속도와 더 높은 보안을 위해 그룹 5를 선택합니다. 그룹 2가 기본값으로 선택됩니다.



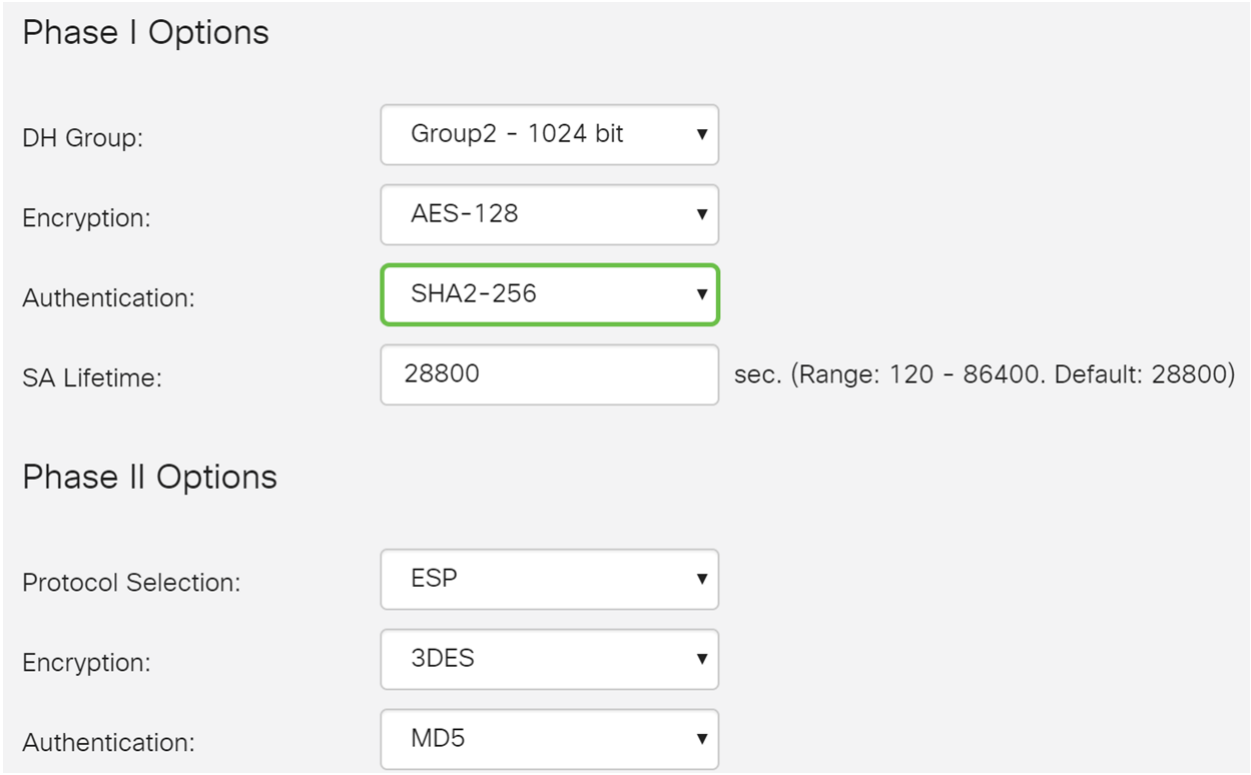
7단계. 드롭다운 목록에서 암호화 옵션(**3DES**, **AES-128**, **AES-192** 또는 **AES-256**)을 선택합니다.이 방법은 ESP/ISAKMP 패킷을 암호화하고 해독하는 데 사용되는 알고리즘을 결정합니다.3DES(Triple Data Encryption Standard)는 DES 암호화를 3번 사용하지만 이제 레거시 알고리즘입니다.이것은 한계적이지만 허용 가능한 보안 수준을 제공하기 때문에 더 나은 대안이 없을 때만 사용되어야 한다는 것을 의미한다.일부 "차단 충돌" 공격에 취약하기 때문에 이전 버전과의 호환성이 필요한 경우에만 사용해야 합니다.3DES는 안전한 것으로 간주되지 않으므로 사용하지 않는 것이 좋습니다.AES(Advanced Encryption Standard)는 DES보다 더 안전하도록 설계된 암호화 알고리즘입니다.AES는 더 큰 키 크기를 사용하여 메시지 해독에 알려진 유일한 방법은 침입자가 가능한 모든 키를 시도하기 위한 것입니다.장치에서 지원할 수 있는 경우 AES를 사용하는 것이 좋습니다.이 예에서는 AES-**128**을 암호화 옵션으로 선택했습니다.

**참고:**다음과 같은 추가적인 리소스가 도움이 될 수 있습니다.IPsec 및 차세대 암호화를 사용하여 VPN에 대한 보안 구성.




8단계. 인증 방법은 ESP 헤더 패킷의 검증 방법을 결정합니다.이것이 인증에서 A측과 B측 측면의 실제 자기라고 말하는 것을 검증하기 위해 사용되는 해싱 알고리즘입니다.MD5는 128비트 다이제스트를 생성하고 SHA1보다 빠른 단방향 해싱 알고리즘입니다. SHA1은 160비트 다이제스트를 생성하는 단방향 해싱 알고리즘이며 SHA2-256은 256비트 다이제스트를 생성합니다.SHA2-256은 더 안전하므로 권장됩니다.VPN 터널의 양쪽 끝이 동일한 인증 방법을 사용하는지 확인합니다.인증(**MD5, SHA1** 또는 **SHA2-256**)을 선택합니다.

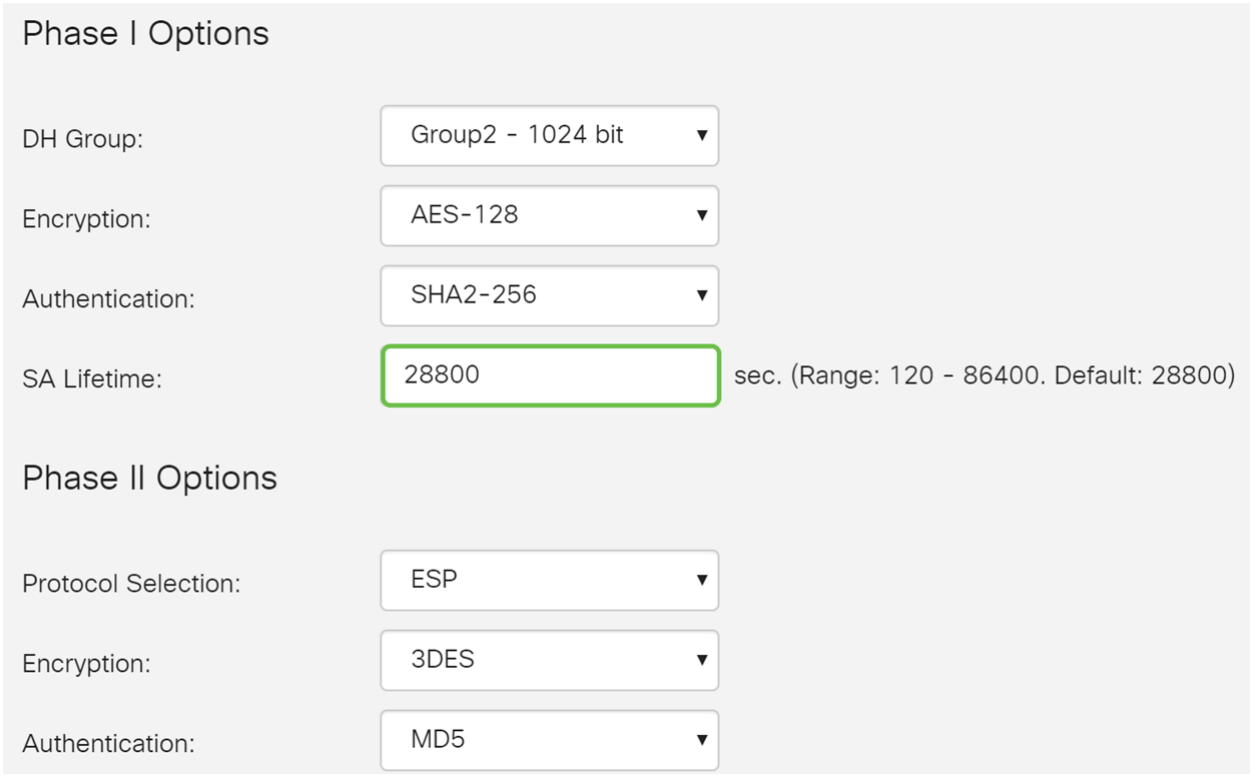
**이** 예제에 대해 **SHA2-256**이 선택되었습니다.




9단계. *SA 수명(초)*은 이 단계에서 IKE SA가 활성화된 시간을 알려줍니다.SA가 각 수명 후에 만료되면 새 협상에 대해 새 협상이 시작됩니다.범위는 120~86400이고 기본값은 28800입니다.

기본값인 **28800**초를 Phase I의 SA Lifetime으로 사용합니다.

**참고:**1단계의 SA 수명이 2단계 SA 수명보다 긴 것이 좋습니다.Phase I를 Phase II보다 짧게 만들면 데이터 터널이 아닌 터널을 앞뒤로 반복해서 재협상해야 합니다.데이터 터널은 더 많은 보안이 필요하므로 1단계보다 짧은 2단계의 수명을 제공하는 것이 좋습니다.

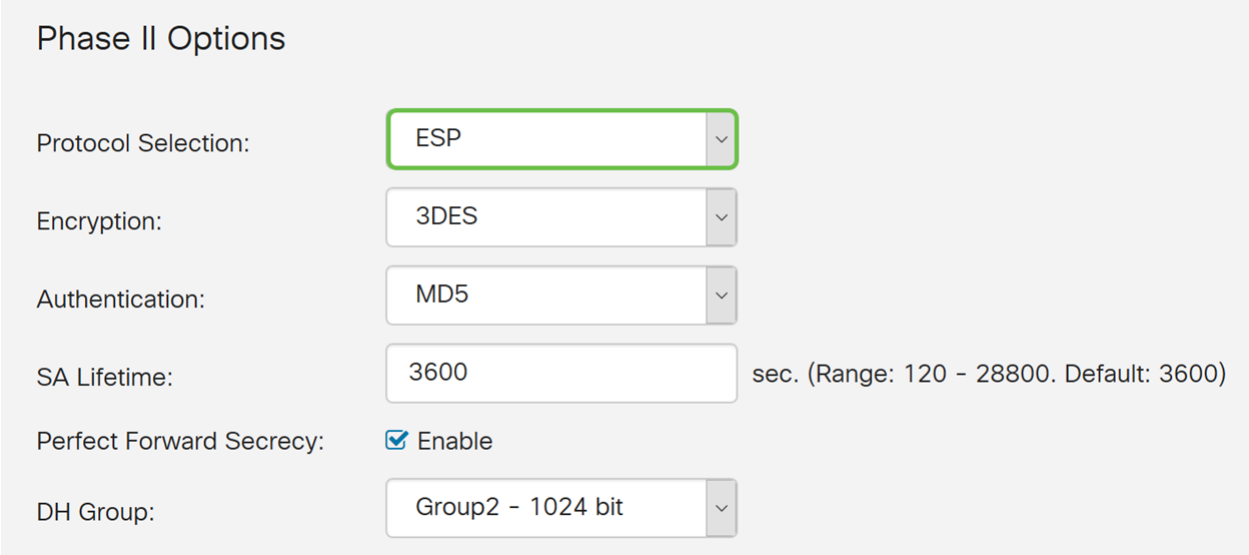



10단계. 2단계는 전달 중인 데이터를 암호화하는 단계입니다.Phase *2 Options*의 드롭다운 목록에서 프로토콜을 선택하면 다음과 같은 옵션이 제공됩니다.

•ESP(Encapsulating Security Payload) - 데이터 암호화를 위해 ESP를 선택하고 암호화를 입력합니다.

•Authentication Header(AH) - 데이터가 기밀이 아닌 경우, 즉 암호화되지 않지만 인증해야 하는 경우 데이터 무결성을 위해 선택합니다.트래픽의 소스 및 목적지를 검증하는 데만 사용됩니다.

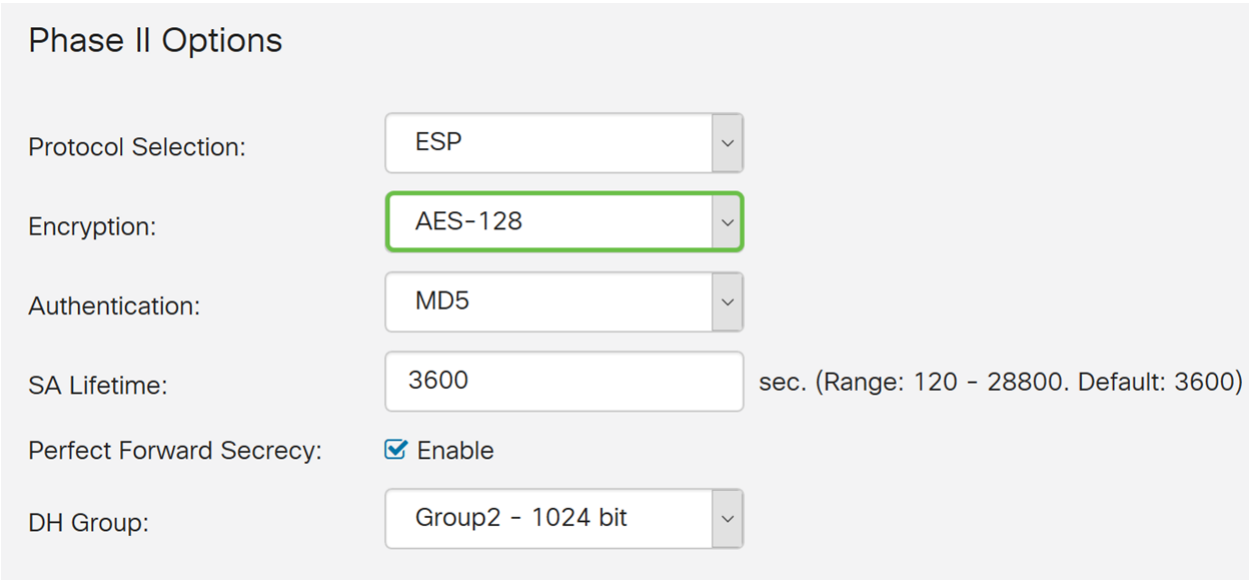
이 예에서는 ESP를 *프로토콜 선택*으로 *사용합니다*.




11단계. 드롭다운 목록에서 암호화 옵션(**3DES**, **AES-128**, **AES-192** 또는 **AES-256**)을 선택합니다.이 방법은 ESP/ISAKMP 패킷을 암호화하고 해독하는 데 사용되는 알고리즘을 결정합니다.

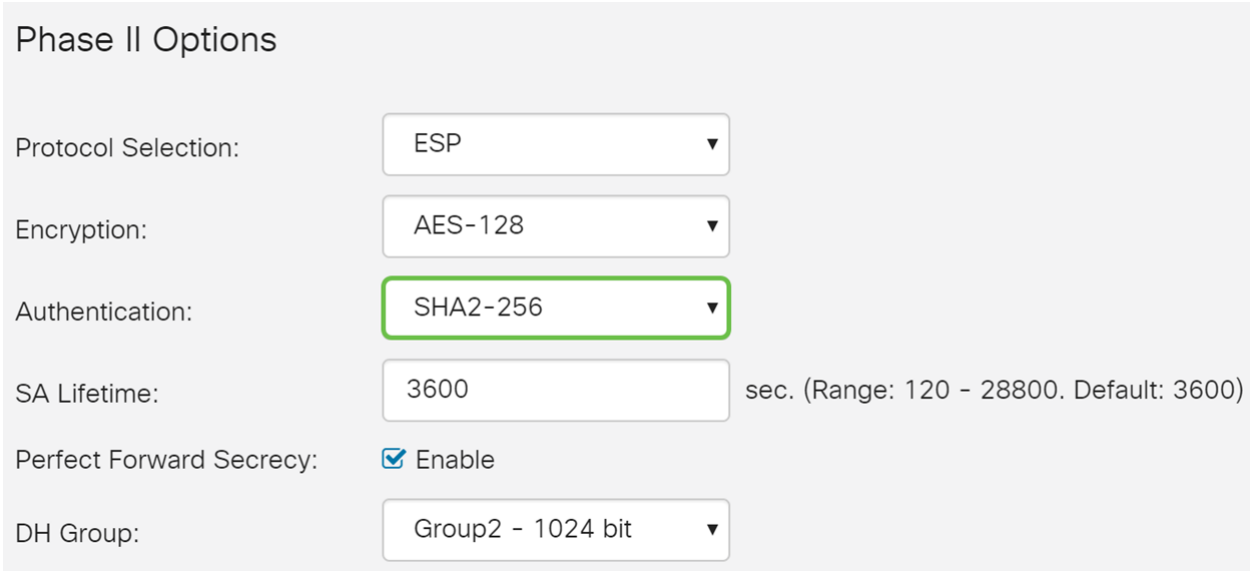
이 예에서는 AES-**128**을 암호화 옵션으로 사용합니다.

**참고:**다음과 같은 추가적인 리소스가 도움이 될 수 있습니다.IPsec 및 차세대 암호화를 사용하여 VPN에 대한 보안 구성.

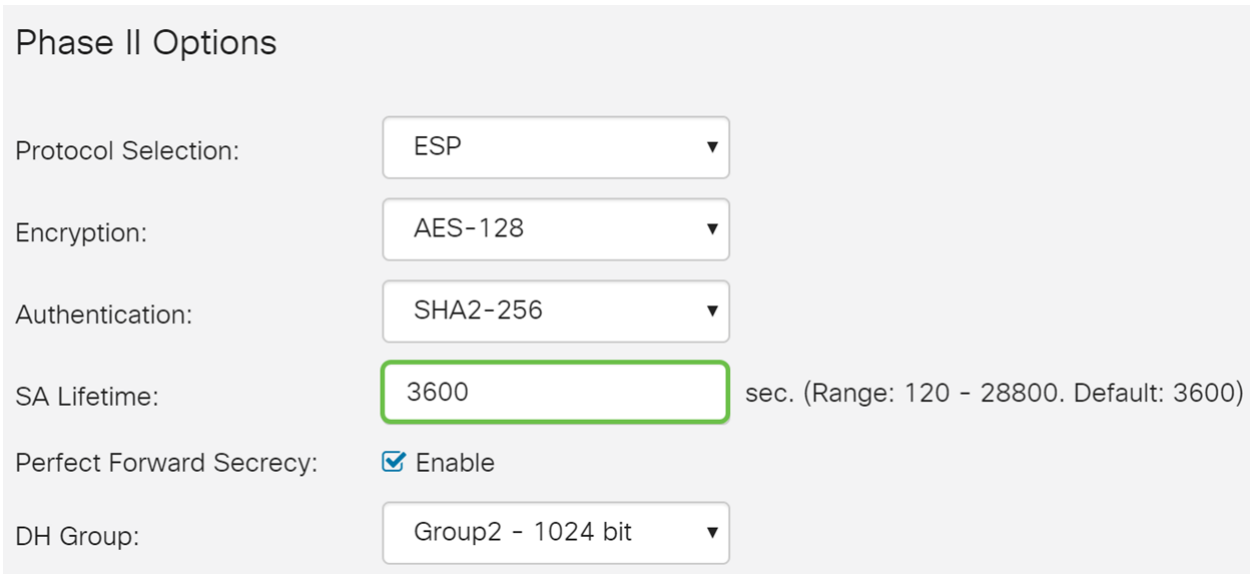



12단계. 인증 방법은 ESP(Encapsulating Security Payload Protocol) 헤더 패킷의 검증 방법을 결정합니다.인증(**MD5, SHA1** 또는 **SHA2-256**)을 선택합니다.

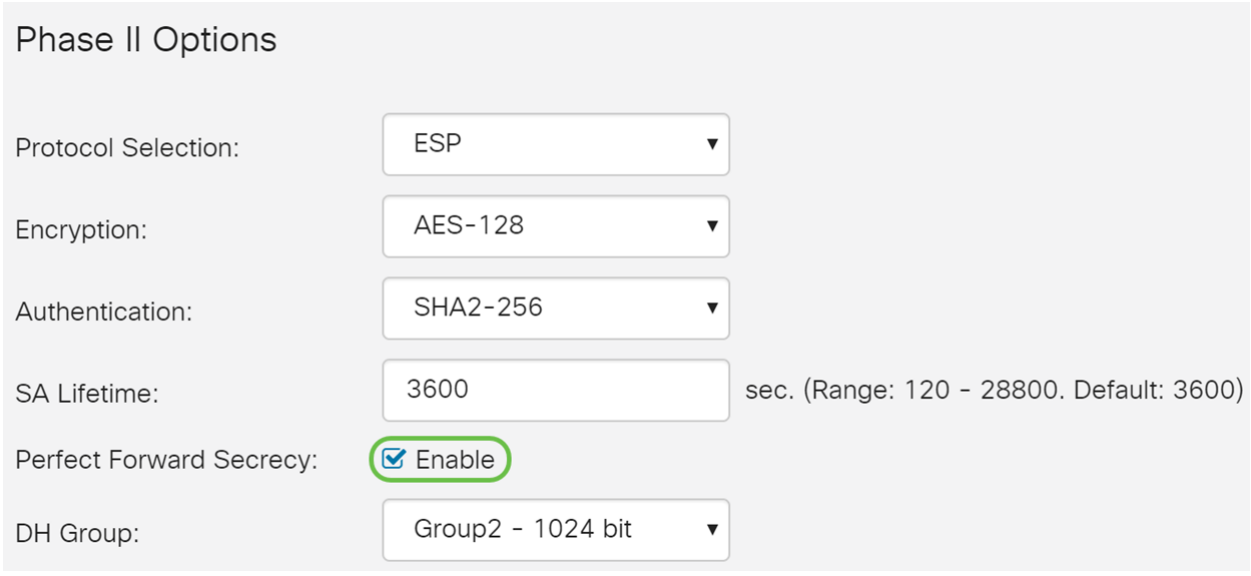
**이** 예제에 대해 **SHA2-256**이 선택되었습니다.




13단계. 이 단계에서 VPN 터널(IPsec SA)이 활성화된 시간을 입력합니다.2단계의 기본값은 3600초입니다.이 데모에서는 기본값을 사용합니다.

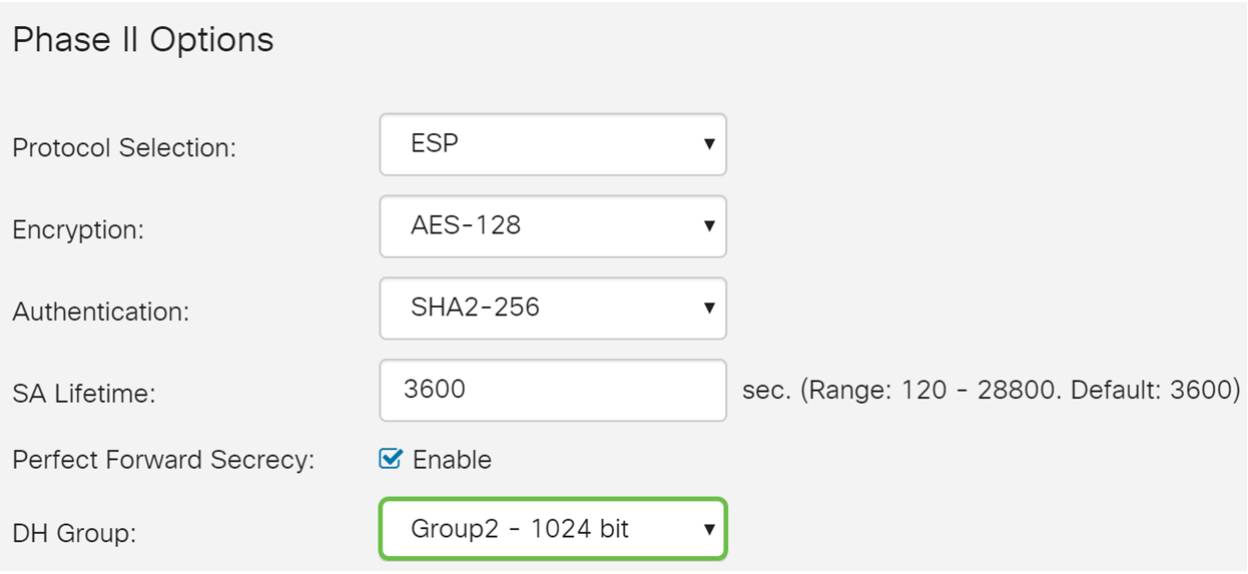



14단계. **Enable(활성화)**을 선택하여 PFS(Perfect Forward Secrecy)를 활성화합니다 .PFS(Perfect Forward Secrecy)가 활성화된 경우 IKE Phase 2 협상은 IPsec 트래픽 암호화 및 인증을 위한 새로운 키 자료를 생성합니다.PFS는 공개 키 암호화를 사용하여 인터넷을 통해 전송되는 통신의 보안을 개선하는 데 사용됩니다.장치에서 지원하는 경우 이 옵션을 사용하는 것이 좋습니다.

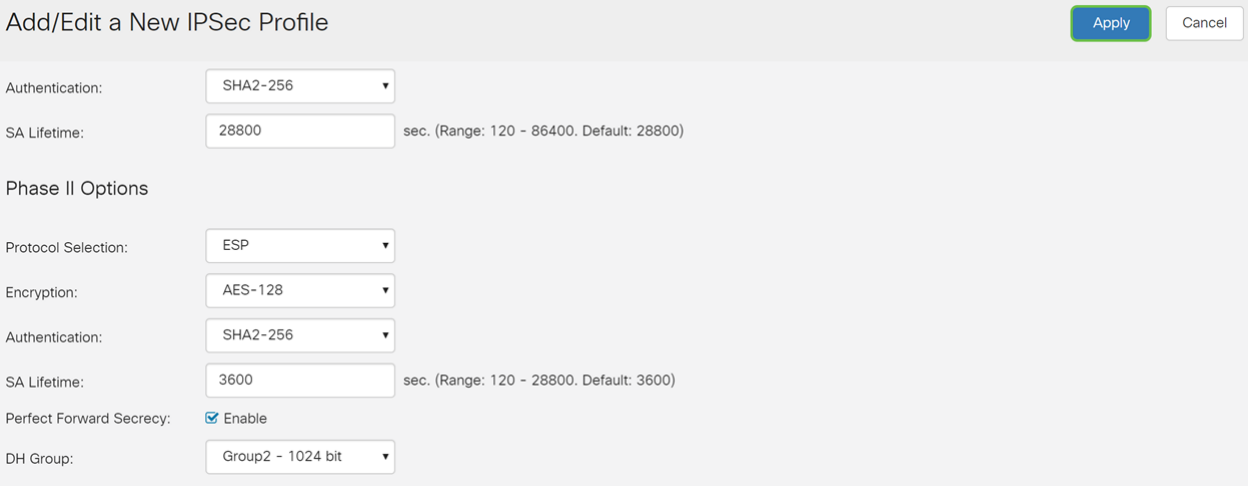


15단계. DH(Diffie-Hellman) 그룹을 선택합니다.DH는 키 교환 프로토콜로서, **그룹 2 - 1024비트** 및 **그룹 5 - 1536비트**의 서로 다른 기본 키 길이의 두 그룹**을 사용합니다**.이 데모에 **그룹 2 - 1024비트**를 선택했습니다.

**참고:**더 빠른 속도와 더 낮은 보안을 위해 그룹 2를 선택합니다. 더 느린 속도와 더 높은 보안을 위해 그룹 5를 선택합니다. 그룹 2가 기본적으로 선택됩니다.

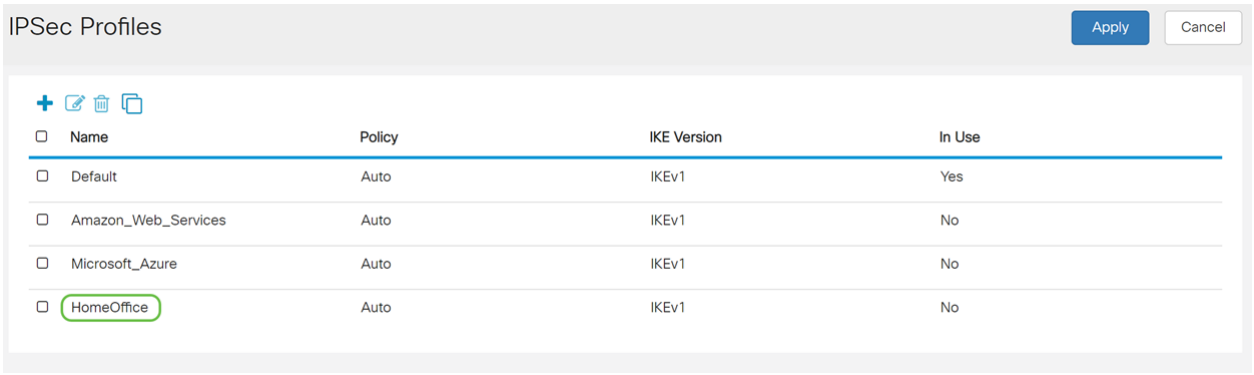



16단계. **Apply(적용)**를 클릭하여 새 IPsec 프로필을 추가합니다.

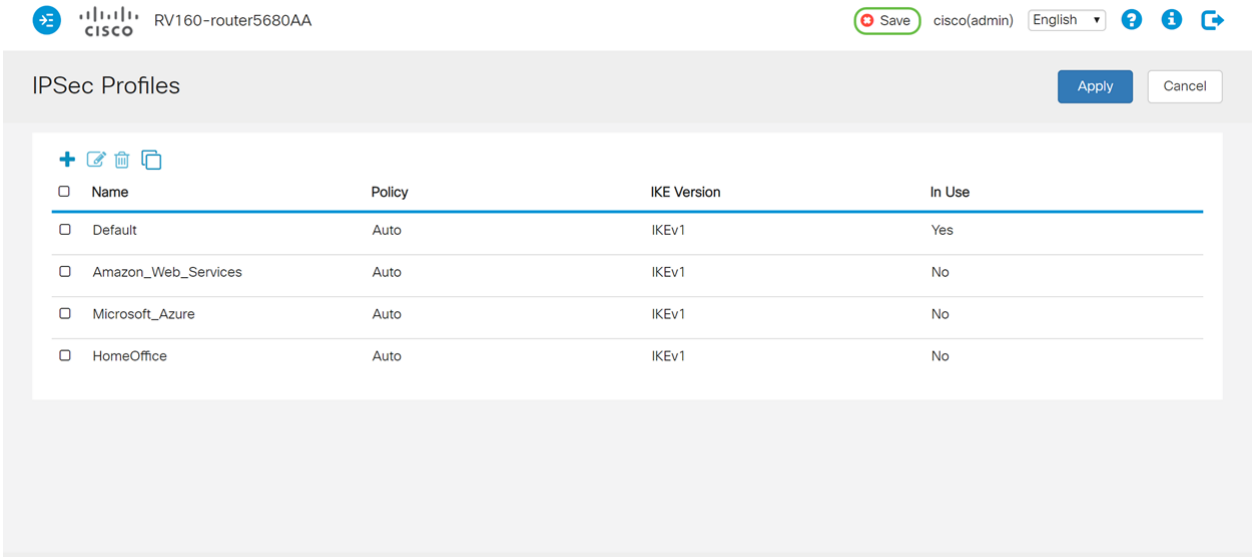



이제 새 IPsec 프로필을 생성했습니다.IPsec 프로필이 추가되었는지 확인하려면 아래에서 계속 진행하십시오.재부팅 중에 모든 컨피그레이션이 유지되도록 실행 중인 컨피그레이션 파일을 시작 컨피그레이션 파일에 복사하는 단계를 수행할 수도 있습니다.

1단계. Apply(*적용*)를 클릭한 후 새 IPsec 프로필을 추가해야 합니다.




2단계. 페이지 상단에서 **Save**(저장) 버튼을 클릭하여 Configuration Management(컨피그레이션 *관리*)로 이동하여 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.이는 재부팅 사이에 컨피그레이션을 유지하기 위한 것입니다.




3단계. *구성 관리*에서 소스가 **실행** 중인 **컨피그레이션**이고 대상이 *시작* 컨피그레이션인지 **확인합니다**.그런 다음 **Apply**를 눌러 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.라우터가 현재 사용 중인 모든 컨피그레이션은 휘발성이며 재부팅 중에 유지되지 않는 실행 중인 컨피그레이션 파일에 있습니다.실행 중인 컨피그레이션 파일을 시작 컨피그레이션 파일에 복사하면 재부팅 사이에 모든 컨피그레이션이 유지됩니다.