

RV34x Series 라우터에서 IPSec(Internet Protocol Security) 프로파일 구성

목표

IPSec(Internet Protocol Security)은 두 개의 피어(예: 두 라우터) 간에 보안 터널을 제공합니다. 민감한 것으로 간주되고 이러한 보안 터널을 통해 전송되어야 하는 패킷과 이러한 민감한 패킷을 보호하는 데 사용해야 하는 매개변수를 이러한 터널의 특성을 지정하여 정의해야 합니다. 그런 다음 IPSec 피어가 그러한 민감한 패킷을 발견하면 적절한 보안 터널을 설정하고 이 터널을 통해 패킷을 원격 피어로 전송합니다.

IPSec이 방화벽 또는 라우터에 구현되면 경계를 지나는 모든 트래픽에 적용할 수 있는 강력한 보안을 제공합니다. 회사 또는 작업 그룹 내의 트래픽은 보안 관련 처리 오버헤드를 발생시키지 않습니다.

이 문서의 목적은 RV34x Series Router에서 IPSec 프로파일을 구성하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스

- RV34x 시리즈

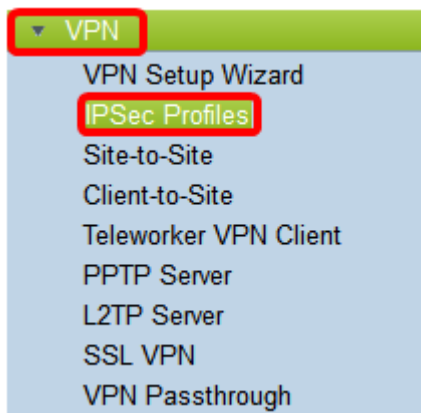
소프트웨어 버전

- 1.0.1.16

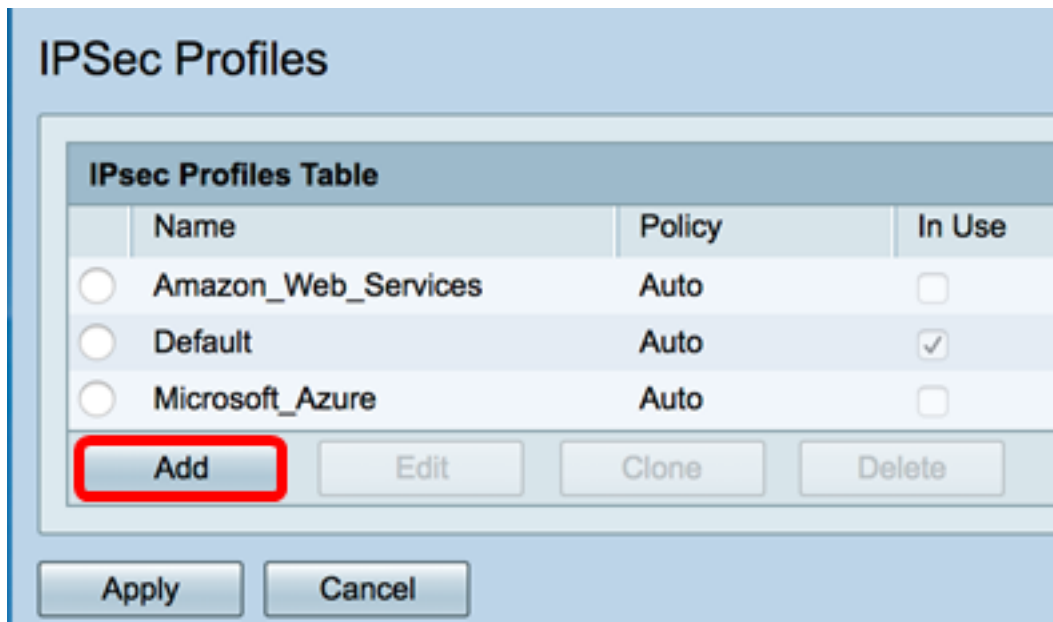
IPSec 프로파일 구성

IPSec 프로파일 생성

1단계. 라우터의 웹 기반 유틸리티에 로그인하고 VPN > IPSec 프로파일을 선택합니다.

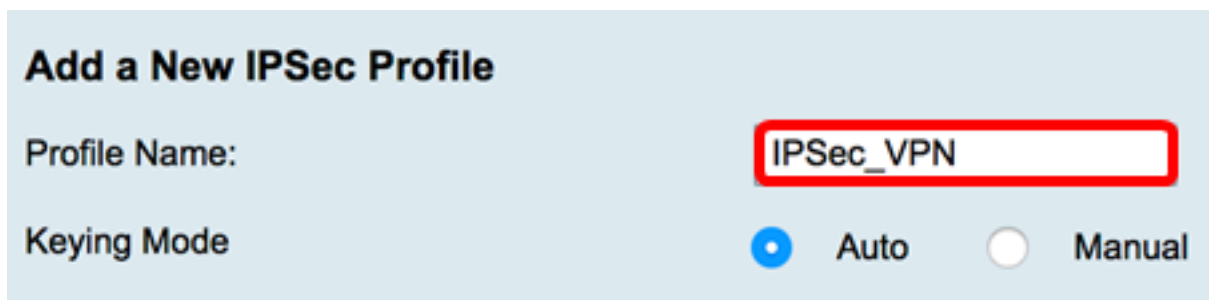


2단계. IPsec Profiles Table(IPsec 프로파일 테이블)에 기존 프로파일이 표시됩니다. Add(추가)를 클릭하여 새 프로파일을 생성합니다.



3단계. 프로파일 이름 필드에 프로파일 이름을 생성합니다.프로파일 이름은 특수 문자의 영숫자 문자 및 밑줄(_)만 포함해야 합니다.

참고:이 예에서는 IPsec_VPN이 IPsec 프로필 이름으로 사용됩니다.



4단계. 라디오 버튼을 클릭하여 프로파일에서 인증에 사용할 키 교환 방법을 결정합니다.옵션은 다음과 같습니다.

- 자동 — 정책 매개변수가 자동으로 설정됩니다.이 옵션은 데이터 무결성 및 암호화 키 교환을 위해 IKE(Internet Key Exchange) 정책을 사용합니다.이 옵션을 선택하면 Auto Policy Parameters(자동 정책 매개변수) 영역 아래의 컨피그레이션 설정이 활성화됩니다.[여기](#)를 클릭하여 자동 설정을 구성합니다.
- 수동 — 이 옵션을 사용하면 VPN(Virtual Private Network) 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.[여기](#)를 클릭하여 수동 설정을 구성합니다.

참고:이 예에서는 Auto가 선택되었습니다.



자동 설정 구성

1단계. Phase 1 Options(1단계 옵션) 영역에서 DH Group(DH 그룹) 드롭다운 목록에서 1단계의 키와 함께 사용할 적절한 DH(Diffie-Hellman) 그룹을 선택합니다. Diffie-Hellman은 사전 공유 키 집합을 교환하기 위해 연결에 사용되는 암호화 키 교환 프로토콜입니다. 알고리즘의 강도는 비트로 결정됩니다. 옵션은 다음과 같습니다.

- Group2 - 1024비트 — 키를 느리게 계산하지만 Group1보다 안전합니다.
- Group5 - 1536비트 — 가장 느린 키를 계산합니다. 하지만 가장 안전합니다.

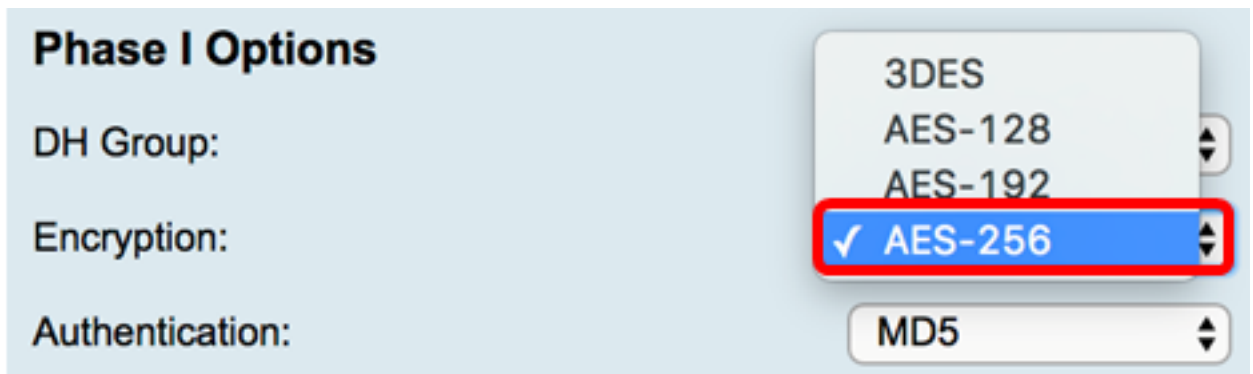
참고: 이 예에서는 Group2-1024비트가 선택됩니다.



2단계. Encryption(암호화) 드롭다운 목록에서 적절한 암호화 방법을 선택하여 ESP(Encapsulating Security Payload) 및 ISAKMP(Internet Security Association and Key Management Protocol)를 암호화하고 해독합니다. 옵션은 다음과 같습니다.

- 3DES — 3중 데이터 암호화 표준
- AES-128 — 고급 암호화 표준은 128비트 키를 사용합니다.
- AES-192 — 고급 암호화 표준은 192비트 키를 사용합니다.
- AES-256 — 고급 암호화 표준은 256비트 키를 사용합니다.

참고: AES는 DES와 3DES를 통해 암호화하는 표준 방법으로서 성능과 보안을 강화합니다. AES 키를 늘리면 느린 성능으로 보안이 향상됩니다. 이 예에서는 AES-256이 선택됩니다.



3단계. Authentication(인증) 드롭다운 메뉴에서 ESP 및 ISAKMP의 인증 방법을 결정하는 인증 방법을 선택합니다. 옵션은 다음과 같습니다.

- MD5 — 메시지 다이제스트 알고리즘에 128비트 해시 값이 있습니다.
- SHA-1 — 보안 해시 알고리즘에는 160비트 해시 값이 있습니다.
- SHA2-256 — 256비트 해시 값을 사용하는 보안 해시 알고리즘.

참고: MD5 및 SHA는 모두 암호화 해시 함수입니다. 데이터 조각을 가져와서 압축하고 일반적으로 재생산성이 없는 고유한 16진수 출력을 만듭니다. 이 예에서는 SHA2-256이 선택됩니다.

DH Group: Group2 - 1024 bit

Encryption: MD5
SHA1

Authentication: **✓ SHA2-256**

4단계. SA Lifetime 필드에 120~86400 범위의 값을 입력합니다. 이 단계에서는 IKE(Internet Key Exchange) SA(Security Association)가 활성 상태로 유지되는 시간입니다. 기본값은 28800입니다.

참고: 이 예에서는 28801이 사용됩니다.

Authentication: SHA2-256

SA Lifetime: **28801**

Perfect Forward Secrecy: Enable

5단계. (선택 사항) Enable Perfect Forward Secrecy(완벽한 전달 보안 활성화) 확인란을 선택하여 IPSec 트래픽 암호화 및 인증을 위한 새 키를 생성합니다.

Authentication: SHA2-256

SA Lifetime: 28801

Perfect Forward Secrecy: Enable

6단계. II 단계 옵션 영역의 프로토콜 선택 드롭다운 메뉴에서 협상의 두 번째 단계에 적용할 프로토콜 유형을 선택합니다. 옵션은 다음과 같습니다.

- ESP — 이 옵션을 선택한 경우 [7단계](#)로 건너뛰고 ESP 패킷의 암호화 및 암호 해독에 대한 암호화 방법을 선택합니다. 데이터 프라이버시 서비스 및 선택적 데이터 인증, 재전송 방지 서비스를 제공하는 보안 프로토콜. ESP는 보호할 데이터를 캡슐화합니다.
- AH — AH(Authentication Header)는 데이터 인증 및 선택적 재전송 방지 서비스를 제공하는 보안 프로토콜입니다. 보호할 데이터에 AH가 포함되어 있습니다(전체 IP 데이터그램). [8단계](#)로 건너뛰십시오.

Phase II Options

Protocol Selection: **✓ ESP**
AH

Encryption: **✓ AES**

[7단계](#). 6단계에서 ESP를 선택한 경우 Encryption(암호화) 드롭다운 목록에서 ESP 및 ISAKMP를 암호화하고 해독할 적절한 암호화 방법을 선택합니다. 옵션은 다음과 같습니다.

- 3DES — 3중 데이터 암호화 표준
- AES-128 — 고급 암호화 표준은 128비트 키를 사용합니다.
- AES-192 — 고급 암호화 표준은 192비트 키를 사용합니다.
- AES-256 — 고급 암호화 표준은 256비트 키를 사용합니다.

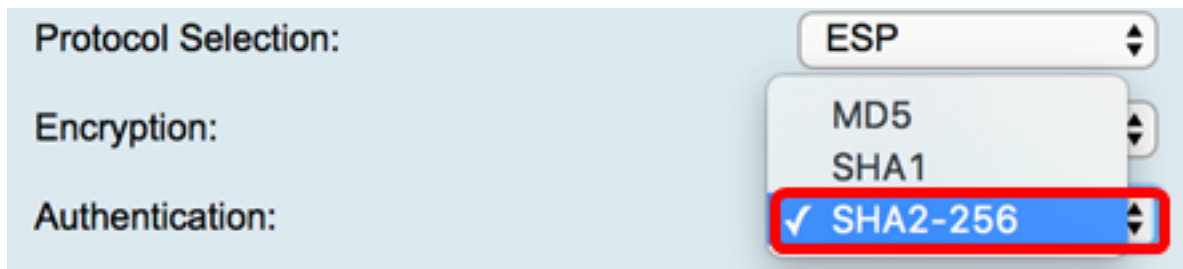
참고:이 예에서는 AES-256이 선택됩니다.



8단계. Authentication(인증) 드롭다운 메뉴에서 ESP 및 ISAKMP 인증 방법을 결정하는 인증 방법을 선택합니다. 옵션은 다음과 같습니다.

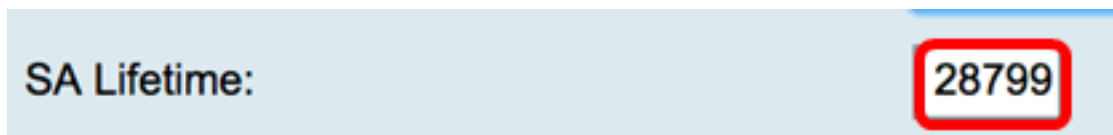
- MD5 — 메시지 다이제스트 알고리즘에 128비트 해시 값이 있습니다.
- SHA-1 — 보안 해시 알고리즘에는 160비트 해시 값이 있습니다.
- SHA2-256 — 256비트 해시 값을 사용하는 보안 해시 알고리즘.

참고:이 예에서는 SHA2-256이 사용됩니다.



9단계. SA Lifetime 필드에 120~28800 범위의 값을 입력합니다. 이 단계에서는 IKE SA가 활성 상태로 유지되는 시간입니다. 기본값은 3600입니다.

참고:이 예에서는 28799가 사용됩니다.



10단계. DH 그룹 드롭다운 목록에서 2단계의 키와 함께 사용할 적절한 DH(Diffie-Hellman) 그룹을 선택합니다. 옵션은 다음과 같습니다.

- Group2 - 1024비트 — 키를 느리게 계산하지만 Group1보다 안전합니다.
- Group5 - 1536비트 — 가장 느린 키를 계산하지만 가장 안전한 키입니다.

참고:이 예에서는 Group5 - 1536비트가 선택됩니다.

SA Lifetime: 28700

DH Group: Group2 - 1024 bit
✓ Group5 - 1536 bit

11단계. **Apply** 버튼을 클릭합니다.

참고:IPSec 프로파일 테이블로 다시 이동되며 새로 생성된 IPSec 프로파일이 나타납니다.

IPSec Profiles

✓ Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

IPsec Profiles Table			
Name	Policy	In Use	
<input type="radio"/> Amazon_Web_Services	Auto	<input checked="" type="checkbox"/>	
<input type="radio"/> Default	Auto	<input checked="" type="checkbox"/>	
<input type="radio"/> Microsoft_Azure	Auto	<input type="checkbox"/>	
<input type="radio"/> IPSec_Vpn	Auto	<input type="checkbox"/>	

Add Edit Clone Delete

Apply Cancel

12단계(선택 사항) 구성을 영구적으로 저장하려면 구성 복사/저장 페이지로 이동하거나 페이지 상단의 **Save** 아이콘을 클릭합니다.

이제 RV34x Series Router에서 Auto IPSec 프로파일을 성공적으로 구성했어야 합니다.

수동 설정 구성

1단계. *SPI-Incoming* 필드에 VPN 연결에서 들어오는 트래픽에 대한 SPI(Security Parameter Index) 태그의 100부터 FFFFFFFF까지의 16진수 숫자를 입력합니다.SPI 태그는 한 세션의 트래픽과 다른 세션의 트래픽을 구분하는 데 사용됩니다.

참고:이 예에서는 0xABCD가 사용됩니다.

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

2단계. *SPI-Outgoing* 필드에 VPN 연결에서 발신 트래픽에 대한 SPI 태그의 100에서 FFFFFFFF까지의 16진수 숫자를 입력합니다.

참고:이 예에서는 0x1234가 사용됩니다.

SPI-Incoming:	0xABCD
SPI-Outgoing:	0x1234

3단계. Encryption 드롭다운 목록에서 옵션을 선택합니다. 옵션은 3DES, AES-128, AES-192 및 AES-256입니다.

참고: 이 예에서는 AES-256이 선택됩니다.

SPI Incoming:	
SPI Outgoing:	
Encryption:	<ul style="list-style-type: none"> 3DES AES-128 AES-192 <input checked="" type="checkbox"/> AES-256

4단계. Key-In 필드에 인바운드 정책의 키를 입력합니다. 키 길이는 **3단계**에서 선택한 알고리즘에 따라 달라집니다.

- 3DES는 48자 키를 사용합니다.
- AES-128은 32자 키를 사용합니다.
- AES-192는 48자 키를 사용합니다.
- AES-256은 64자 키를 사용합니다.

참고: 이 예에서는 123456789123456789123...가 사용됩니다.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

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

참고: 이 예에서는 1a1a1a1a1a1a1a1a121212가 사용됩니다.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

6단계. Manual Integrity Algorithm 드롭다운 목록에서 옵션을 선택합니다.

- MD5 — 데이터 무결성에 128비트 해시 값을 사용합니다. MD5는 안전하지 않지만 SHA-1 및 SHA2-256보다 빠릅니다.
- SHA-1 — 데이터 무결성을 위해 160비트 해시 값을 사용합니다. SHA-1은 MD5보다 느리지만 보안 수준이 더 높고, SHA-1은 SHA2-256보다 빠르지만 보안 수준이 낮습니다.
- SHA2-256 — 데이터 무결성을 위해 256비트 해시 값을 사용합니다. SHA2-256은 MD5 및 SHA-1보다 느리지만 안전합니다.

참고:이 예에서는 MD5가 선택됩니다.

Authentication: MD5
 SHA1
 SHA2-256

Key-In

Key-Out

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

- MD5는 32자 키를 사용합니다.
- SHA-1은 40자 키를 사용합니다.
- SHA2-256은 64자 키를 사용합니다.

참고:이 예에서는 123456789123456789123...가 사용됩니다.

Key-In:

Key-Out:

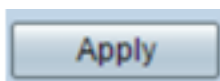
8단계. Key-Out 필드에 발신 정책의 키를 입력합니다.키 길이는 6단계에서 선택한 알고리즘에 따라 달라집니다.

참고:이 예에서는 1a1a1a1a1a1a1a1a121212가 사용됩니다.

Key-In:


Key-Out:

9단계. 을 클릭합니다




참고:IPSec 프로파일 테이블로 다시 이동되며 새로 생성된 IPSec 프로파일이 나타납니다.

IPSec Profiles

 Success. To permanently save the configuration, Go to [Configuration Management page](#) or click Save icon.

IPsec Profiles Table			
	Name	Policy	In Use
<input type="radio"/>	Amazon_Web_Services	Auto	<input checked="" type="checkbox"/>
<input type="radio"/>	Default	Auto	<input checked="" type="checkbox"/>
<input type="radio"/>	Microsoft_Azure	Auto	<input type="checkbox"/>
<input type="radio"/>	IPSec_Vpn	Manual	<input type="checkbox"/>

10단계(선택 사항) 구성을 영구적으로 저장하려면 구성 복사/저장 페이지로 이동하거나 페이지 상단의  아이콘을 클릭합니다.

이제 RV34x Series Router에서 수동 IPSec 프로파일을 구성했어야 합니다.