

# RV130 및 RV130W VPN Router의 IKE(Internet Key Exchange) 정책 설정

## 목표

IKE(Internet Key Exchange)는 두 네트워크 간의 보안 통신을 설정하는 프로토콜입니다. IKE를 사용하면 패킷이 암호화되고 잠기며 두 당사자가 사용하는 키로 잠금 해제됩니다.

VPN 정책을 구성하기 전에 인터넷 키 교환 정책을 생성해야 합니다. 자세한 내용은 [RV130 및 RV130W에서 VPN 정책](#) 구성을 참조하십시오.

이 문서의 목적은 IKE 프로필을 RV130 및 RV130W VPN Router에 추가하는 방법을 설명하는 것입니다.

## 적용 가능한 장치

- RV130
- RV130W

## 절차 단계

1단계. Router Configuration Utility를 사용하여 왼쪽 메뉴에서 **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup**을 선택합니다. *Advanced VPN Setup* 페이지가 나타납니다.

Advanced VPN Setup

NAT Traversal:  Enable

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group	
<input type="checkbox"/> No data to display								
Add Row Edit Delete								

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Algorithm	Local	Remote	
<input type="checkbox"/> No data to display								
Add Row Edit Enable Disable Delete								

Save Cancel

IPSec Connection Status

2단계. IKE Policy Table(IKE 정책 테이블)에서 Add Row(행 추가)를 클릭합니다. 새 창이 나타납니다.

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group	
<input type="checkbox"/> No data to display								
Add Row Edit Delete								

3단계. IKE Name 필드에 IKE 정책의 이름을 입력합니다.

**Add / Edit IKE Policy Configuration**

IKE Name:

Exchange Mode:

4단계. *Exchange Mode* 드롭다운 메뉴에서 키 교환을 사용하여 보안 통신을 설정하는 모드를 선택합니다.

**Add / Edit IKE Policy Configuration**

IKE Name:

Exchange Mode:

**Local**

Main  
Main  
Aggressive

사용 가능한 옵션은 다음과 같이 정의됩니다.

- Main — 피어의 ID를 보호하여 보안을 강화합니다.
- 적극적인 — 피어 ID를 보호하지 않지만 더 빠른 연결을 제공합니다.

5단계. *Local Identifier Type*(로컬 식별자 유형) 드롭다운 메뉴에서 프로필의 ID 유형을 선택합니다.

**Local**

Local Identifier Type:

Local Identifier:

Local WAN IP  
Local WAN IP  
IP Address

사용 가능한 옵션은 다음과 같이 정의됩니다.

- 로컬 WAN(인터넷) IP — 인터넷을 통해 연결합니다.
- IP Address — 네트워크를 통해 통신하는 인터넷 프로토콜을 사용하여 각 시스템을 식별하는 고유한 숫자 문자열을 마침표로 구분합니다.

6단계. (선택 사항) 5단계의 드롭다운 목록에서 IP 주소를 선택한 경우 Local Identifier 필드에 로컬 IP 주소를 입력합니다.

**Local**

Local Identifier Type:

Local Identifier:

7단계. *Remote Identifier Type*(원격 식별자 유형) 드롭다운 메뉴에서 프로필에 있는 ID의 유형을 선택합니다.

**Remote**

Remote Identifier Type:

Remote Identifier:

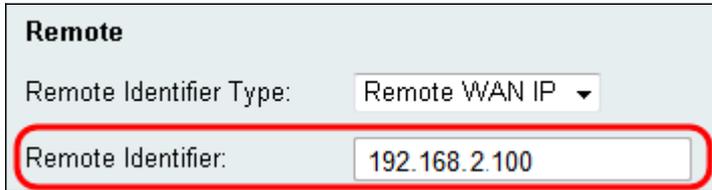
Remote WAN IP  
Remote WAN IP  
IP Address

사용 가능한 옵션은 다음과 같이 정의됩니다.

·로컬 WAN(인터넷) IP — 인터넷을 통해 연결합니다.

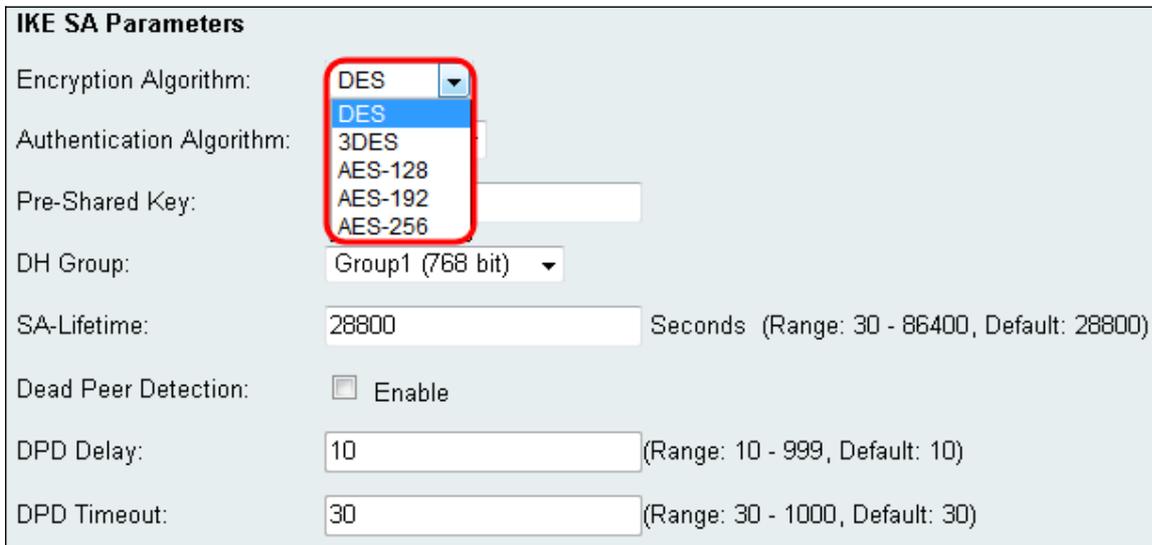
·IP Address — 네트워크를 통해 통신하는 인터넷 프로토콜을 사용하여 각 시스템을 식별하는 고유한 숫자 문자열을 마침표로 구분합니다.

8단계(선택 사항) 7단계의 드롭다운 목록에서 IP 주소를 선택한 경우 Remote Identifier 필드에 원격 IP 주소를 입력합니다.



The screenshot shows a configuration window titled "Remote". It contains two fields: "Remote Identifier Type" with a dropdown menu set to "Remote WAN IP", and "Remote Identifier" with a text input field containing "192.168.2.100". A red rectangle highlights the "Remote Identifier" field.

9단계. *Encryption Algorithm* 드롭다운 메뉴에서 통신을 암호화할 알고리즘을 선택합니다. AES-128이 기본값으로 선택됩니다.



The screenshot shows the "IKE SA Parameters" configuration window. The "Encryption Algorithm" dropdown menu is open, showing options: DES, 3DES, AES-128, AES-192, and AES-256. A red rectangle highlights this dropdown menu. Other fields include "Authentication Algorithm", "Pre-Shared Key", "DH Group" (set to Group1 (768 bit)), "SA-Lifetime" (28800), "Dead Peer Detection" (unchecked), "DPD Delay" (10), and "DPD Timeout" (30).

사용 가능한 옵션은 최소 보안 수준에서 최대 보안 수준까지 다음과 같이 나열됩니다.

·DES — 데이터 암호화 표준

·3DES — 3중 데이터 암호화 표준

·AES-128 — Advanced Encryption Standard는 128비트 키를 사용합니다.

·AES-192 — Advanced Encryption Standard는 192비트 키를 사용합니다.

·AES-256 — Advanced Encryption Standard는 256비트 키를 사용합니다.

**참고:** AES는 DES 및 3DES를 통해 암호화하여 성능과 보안을 강화하는 표준 방법입니다. AES 키를 길게 하면 성능 저하와 함께 보안이 향상됩니다. AES-128은 속도와 보안 사이에 최상의 절충을 제공하므로 권장됩니다.

10단계. *Authentication Algorithm* 드롭다운 메뉴에서 통신을 인증하는 알고리즘을 선택합니다. SHA-1이 기본값으로 선택됩니다.

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: MD5 ▾  
 MD5  
 SHA-1  
 SHA2-256

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

사용 가능한 옵션은 다음과 같이 정의됩니다.

- MD5 — 메시지 다이제스트 알고리즘의 해시 값은 128비트입니다.
- SHA-1 — Secure Hash Algorithm에는 160비트 해시 값이 있습니다.
- SHA2-256 — 256비트 해시 값이 있는 보안 해시 알고리즘

**참고:** MD5와 SHA는 모두 암호화 해시 함수입니다. 데이터를 압축하여 일반적으로 재현할 수 없는 고유한 16진수 출력을 생성합니다. MD5는 해싱 충돌에 대한 보안을 기본적으로 제공하지 않으므로 충돌 저항이 필요하지 않은 소규모 비즈니스 환경에서만 사용해야 합니다. SHA1은 MD5보다 훨씬 느린 속도로 더 우수한 보안을 제공하기 때문에 더 나은 선택입니다. 최상의 결과를 얻기 위해 SHA2-256은 실질적인 관련성에 대해 알려진 공격이 없으며 최상의 보안을 제공합니다. 앞에서 언급한 것처럼, 보안 수준이 높을수록 속도가 느려집니다.

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

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

12단계. *DH Group* 드롭다운 메뉴에서 DH 그룹을 선택합니다. 비트 수는 보안 수준을 나타냅니다. 연결의 양쪽 끝이 같은 그룹에 있어야 합니다.

**IKE SA Parameters**

Encryption Algorithm: AES-128

Authentication Algorithm: SHA-1

Pre-Shared Key:

DH Group: Group1 (768 bit)

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

13단계. SA-Lifetime 필드에서 보안 연결이 유효한 기간을 초 단위로 입력합니다. 기본값은 28800초입니다.

**IKE SA Parameters**

Encryption Algorithm: AES-128

Authentication Algorithm: SHA-1

Pre-Shared Key:

DH Group: Group1 (768 bit)

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

14단계. (선택 사항) 비활성 피어와의 연결을 비활성화하려면 Dead Peer Detection(데드 피어 감지) 필드에서 Enable(활성화) 확인란을 선택합니다. Dead peer Detection을 활성화하지 않은 경우 17단계로 건너됩니다.

**IKE SA Parameters**

Encryption Algorithm: AES-128

Authentication Algorithm: SHA-1

Pre-Shared Key:

DH Group: Group1 (768 bit)

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

15단계(선택 사항) Dead Peer Detection(데드 피어 감지)을 활성화한 경우 DPD Delay(DPD

지연) 필드에 값을 입력합니다. 이 값은 라우터가 클라이언트 연결을 확인하기 위해 대기할 시간을 지정합니다.

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

16단계(선택 사항) Dead Peer Detection(데드 피어 감지)을 활성화한 경우 DPD Timeout(DPD 시간 제한) 필드에 값을 입력합니다. 이 값은 클라이언트가 시간 초과될 때까지 연결 상태를 유지하는 기간을 지정합니다.

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

17단계. 변경 사항을 저장하려면 저장을 누릅니다.

<b>IKE SA Parameters</b>	
Encryption Algorithm:	<input type="text" value="AES-128"/>
Authentication Algorithm:	<input type="text" value="SHA-1"/>
Pre-Shared Key:	<input type="text"/>
DH Group:	<input type="text" value="Group1 (768 bit)"/>
SA-Lifetime:	<input type="text" value="28800"/> Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>	

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.