

RV130 및 RV130W에서 IPSec VPN 서버 구성

목표

IPSec VPN(Virtual Private Network)을 사용하면 인터넷을 통해 암호화된 터널을 설정하여 기업 리소스에 대한 원격 액세스를 안전하게 얻을 수 있습니다.

이 문서의 목적은 RV130 및 RV130W에서 IPSec VPN 서버를 구성하는 방법을 보여 주는 것입니다.

참고: RV130 및 RV130W에서 Shrew Soft VPN Client를 사용하여 IPSec VPN 서버를 구성하는 방법에 대한 자세한 내용은 RV130 및 RV130W에서 [Shrew Soft VPN Client with IPSec VPN Server 사용 문서를](#) 참조하십시오.

적용 가능한 장치

- RV130W Wireless-N VPN Firewall
- RV130 VPN Firewall

소프트웨어 버전

·v1.0.1.3

IPSec VPN 서버 설정

1단계. 웹 구성 유틸리티에 로그인하고 **VPN > IPSec VPN Server > Setup**을 선택합니다. 설정 페이지가 열립니다.

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP: Single

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES

Authentication Algorithm: MD5

PFS Key Group: Enable

DH Group: Group 1(768 bit)

2단계. 인증서를 **활성화**하려면 **Server Enable** 확인란을 선택합니다.

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

3단계(선택 사항) VPN 라우터 또는 VPN 클라이언트가 NAT 게이트웨이 뒤에 있는 경우 Edit를 클릭하여 NAT 통과를 구성합니다. 그렇지 않으면 NAT 통과를 비활성화한 상태로 둡니다.

참고: NAT 접근 설정을 구성하는 방법에 대한 자세한 내용은 [RV130 및 RV130W VPN Router의 IKE\(Internet Key Exchange\) 정책 설정을 참조하십시오.](#)

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

4단계. 디바이스와 원격 엔드포인트 간에 교환될 8-49자 길이의 키를 *Pre-Shared Key*(사전 공유 키) 필드에 입력합니다.

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

5단계. *Exchange Mode* 드롭다운 목록에서 IPsec VPN 연결의 모드를 선택합니다. **Main**이 기본 모드입니다. 그러나 네트워크 속도가 낮은 경우 **Aggressive** 모드를 선택합니다.

Server Enable:

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

참고: Aggressive(적극적인) 모드는 연결 중에 터널 엔드포인트의 ID를 일반 텍스트로 교환하므로 교환 시간이 짧지만 보안 수준이 낮습니다.

6단계. **Encryption Algorithm** 드롭다운 목록에서 1단계에서 사전 공유 키를 암호화하는 데 적합한 암호화 방법을 선택합니다. 높은 보안 및 빠른 성능을 위해 AES-128을 사용하는 것이 좋습니다. VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

사용 가능한 옵션은 다음과 같이 정의됩니다.

- DES — DES(Data Encryption Standard)는 56비트 이전 암호화 방법으로 매우 안전하지 않지만 이전 버전과의 호환성을 위해 필요할 수 있습니다.

- 3DES — 3DES(Triple Data Encryption Standard)는 데이터를 3번 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 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.

7단계. *Authentication Algorithm* 드롭다운 목록에서 적절한 인증 방법을 선택하여 ESP(Encapsulating Security Payload) 프로토콜 헤더 패킷이 1단계에서 검증되는 방법을 결정합니다. VPN 터널은 연결의 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

The screenshot shows the 'Phase 1 Configuration' window. The 'Authentication Algorithm' dropdown menu is open, showing options: MD5 (selected), MD5, SHA-1, and SHA2-256. A red box highlights the dropdown menu. Other fields include Pre-Shared Key: Testkey, Exchange Mode: Main, Encryption Algorithm: DES, DH Group: (partially visible), and IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600).

사용 가능한 옵션은 다음과 같이 정의됩니다.

·MD5 — MD5는 128비트 다이제스트를 생성하는 단방향 해싱 알고리즘입니다. MD5는 SHA-1보다 빠르게 계산하지만 SHA-1보다 안전하지 않습니다. MD5는 권장되지 않습니다.

·SHA-1 — SHA-1은 160비트 다이제스트를 생성하는 단방향 해싱 알고리즘입니다. SHA-1은 MD5보다 느리게 계산하지만 MD5보다 안전합니다.

·SHA2-256 — 256비트 다이제스트를 사용하여 보안 해시 알고리즘 SHA2를 지정합니다.

8단계. *DH Group* 드롭다운 목록에서 1단계의 키와 함께 사용할 적절한 DH(Diffie-Hellman) 그룹을 선택합니다. Diffie-Hellman은 사전 공유 키 집합을 교환하기 위한 연결에서 사용되는 암호화 키 교환 프로토콜입니다. 알고리즘의 세기는 비트에 의해 결정된다.

The screenshot shows the 'Phase 1 Configuration' window. The 'DH Group' dropdown menu is open, showing options: Group1 (768 bit) (selected), Group1 (768 bit), Group2 (1024 bit), and Group5 (1536 bit). A red box highlights the dropdown menu. Other fields include Pre-Shared Key: Testkey, Exchange Mode: Main, Encryption Algorithm: DES, Authentication Algorithm: MD5, and IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600). The 'Phase 2 Configuration' section is partially visible at the bottom.

사용 가능한 옵션은 다음과 같이 정의됩니다.

- Group1(768비트) — 가장 빠르지만 가장 안전하지 않은 키를 계산합니다.
- Group2(1024비트) — 키를 느리게 계산하지만 Group1보다 안전합니다.
- Group5(1536비트) — 가장 느리지만 가장 안전한 키를 계산합니다.

9단계. IKE SA Life Time 필드에 자동 IKE 키가 유효한 시간을 초 단위로 입력합니다. 이 시간이 만료되면 새 키가 자동으로 협상됩니다.

Phase 1 Configuration	
Pre-Shared Key:	Testkey
Exchange Mode:	Main
Encryption Algorithm:	DES
Authentication Algorithm:	MD5
DH Group:	Group1 (768 bit)
IKE SA Life Time:	3600 Seconds (Range: 30 - 86400, Default: 3600)

10단계. Local IP 드롭다운 목록에서 **Single**(로컬 IP)을 선택하여 단일 로컬 LAN 사용자가 VPN 터널에 액세스하도록 하거나, Subnet(서브넷)을 선택하여 여러 사용자가 VPN 터널에 액세스하도록 할 수 있습니다.

Phase 2 Configuration	
Local IP:	Single
IP Address:	Single Subnet (Hint: 1.2.3.4)
Subnet Mask:	(Hint: 255.255.255.0)
IPSec SA Lifetime:	28800 Seconds (Range: 30 - 86400, Default: 28800)
Encryption Algorithm:	DES
Authentication Algorithm:	MD5
PFS Key Group:	<input type="checkbox"/> Enable
DH Group:	Group 1(768 bit)

11단계. 10단계에서 서브넷을 선택한 경우 IP Address 필드에 하위 네트워크의 네트워크 IP 주소를 입력합니다. 10단계에서 Single(단일)을 선택한 경우 단일 사용자의 IP 주소를 입력하고 13단계로 건너뛵니다.

Phase 2 Configuration

Local IP: Subnet ▼

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

12단계. (선택 사항) 10단계에서 서브넷을 선택한 경우 Subnet Mask 필드에 로컬 네트워크의 서브넷 마스크를 입력합니다.

Phase 2 Configuration

Local IP: Subnet ▼

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

13단계. IPSec SA 수명 필드에 2단계에서 VPN 연결이 활성 상태로 유지되는 시간(초)을 입력합니다. 이 시간이 만료되면 VPN 연결에 대한 IPSec 보안 연결이 재협상됩니다.

Phase 2 Configuration

Local IP: Subnet ▼

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

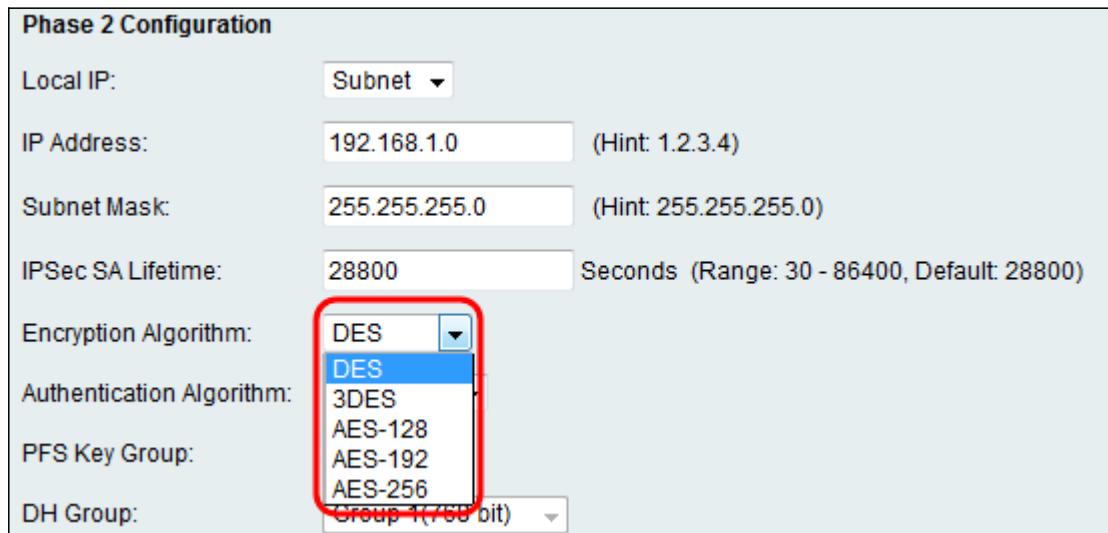
Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

14단계. Encryption Algorithm 드롭다운 목록에서 2단계에서 사전 공유 키를 암호화하는 데 적합한 암호화 방법을 선택합니다. 높은 보안 및 빠른 성능을 위해 AES-128을 사용하는 것이 좋

습니다. VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.



The screenshot shows the 'Phase 2 Configuration' window. The 'Encryption Algorithm' dropdown menu is open, showing the following options: DES (selected), 3DES, AES-128, AES-192, and AES-256. The 'Authentication Algorithm' field is empty. Other fields include Local IP (Subnet), IP Address (192.168.1.0), Subnet Mask (255.255.255.0), IPsec SA Lifetime (28800), PFS Key Group, and DH Group (Group 1 (160 bit)).

사용 가능한 옵션은 다음과 같이 정의됩니다.

·DES — DES(Data Encryption Standard)는 56비트 이전 암호화 방법으로, 가장 안전하지 않지만 이전 버전과의 호환성이 필요할 수 있습니다.

·3DES — 3DES(Triple Data Encryption Standard)는 데이터를 3번 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 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.

15단계. *Authentication Algorithm* 드롭다운 목록에서 적절한 인증 방법을 선택하여 ESP(Encapsulating Security Payload) 프로토콜 헤더 패킷이 2단계에서 검증되는 방법을 결정합니다. VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

Phase 2 Configuration

Local IP: Subnet ▾

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▾

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

PFS Key Group:
 Group 1(768 bit) ▾

DH Group: Group 1(768 bit) ▾

사용 가능한 옵션은 다음과 같이 정의됩니다.

- MD5 — MD5는 128비트 다이제스트를 생성하는 단방향 해싱 알고리즘입니다. MD5는 SHA-1보다 빠르게 계산하지만 SHA-1보다 안전하지 않습니다. MD5는 권장되지 않습니다.
- SHA-1 — SHA-1은 160비트 다이제스트를 생성하는 단방향 해싱 알고리즘입니다. SHA-1은 MD5보다 느리게 계산하지만 MD5보다 안전합니다.
- SHA2-256 — 256비트 다이제스트를 사용하여 보안 해시 알고리즘 SHA2를 지정합니다.

16단계. (선택 사항) PFS *Key Group*(PFS 키 그룹) 필드에서 Enable(활성화) **확인란**을 선택합니다. PFS(Perfect Forward Secrecy)는 2단계에서 새 DH 키를 보장하여 데이터를 보호하는데 추가적인 보안 계층을 생성합니다. 이 프로세스는 1단계에서 생성된 DH 키가 전송 중에 손상되는 경우에 수행됩니다.

Phase 2 Configuration

Local IP: Subnet ▾

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▾

Authentication Algorithm: MD5 ▾

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▾

17단계. *DH Group* 드롭다운 목록에서 2단계의 키와 함께 사용할 적절한 DH(Diffie-Hellman) 그룹을 선택합니다.

Phase 2 Configuration

Local IP: Subnet ▾

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▾

Authentication Algorithm: MD5 ▾

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▾

Group 1(768 bit)

Group 2(1024 bit)

Group 5(1536 bit)

Save Cancel

사용 가능한 옵션은 다음과 같이 정의됩니다.

- Group1(768비트) — 가장 빠르지만 가장 안전하지 않은 키를 계산합니다.
- Group2(1024비트) — 키를 느리게 계산하지만 Group1보다 안전합니다.
- Group5(1536비트) — 가장 느리지만 가장 안전한 키를 계산합니다.

18단계. **저장**을 클릭하여 설정을 저장합니다.

Phase 2 Configuration

Local IP: Subnet ▾

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▾

Authentication Algorithm: MD5 ▾

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▾

Save Cancel

자세한 내용은 다음 문서를 참조하십시오.

- [RV130 데이터 시트](#) - RV130 Series 라우터의 VPN 기능에 대해 설명합니다.
- [RV130 제품 페이지](#) - Cisco의 모든 RV130 기사에 대한 링크 포함

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.