

# Konfiguration eines IPSec VPN Servers auf RV130 und RV130W

## Ziel

IPSec VPN (Virtual Private Network) ermöglicht den sicheren Remote-Zugriff auf Unternehmensressourcen durch die Einrichtung eines verschlüsselten Tunnels über das Internet.

In diesem Dokument wird erläutert, wie Sie einen IPSec-VPN-Server auf dem RV130 und dem RV130W konfigurieren.

**Anmerkung:** Weitere Informationen zur Konfiguration eines IPSec VPN Servers mit dem Shrew Soft VPN Client auf RV130 und RV130W finden Sie im Artikel [Use Shrew Soft VPN Client with IPSec VPN Server on RV130 and RV130W \(Verwenden des Shrew Soft VPN Clients mit IPSec VPN Server auf RV130W\)](#).

## Unterstützte Geräte

- RV130W Wireless-N VPN Firewall
- RV130 VPN-Firewall

## Software-Version

- v1.0.1.3

## IPSec-VPN-Server einrichten

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **VPN > IPSec VPN Server > Setup**. Die Seite Setup wird geöffnet.

**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)

Schritt 2: Aktivieren Sie das Kontrollkästchen **Server aktivieren**, um das Zertifikat zu aktivieren.

**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)

Schritt 3: (Optional) Wenn sich Ihr VPN-Router oder VPN-Client hinter einem NAT-Gateway befindet, klicken Sie auf **Edit**, um NAT Traversal zu konfigurieren. Andernfalls lassen Sie NAT Traversal deaktiviert.

**Anmerkung:** Weitere Informationen zur Konfiguration der NAT-Überbrückungseinstellungen finden Sie unter [IKE-Richtlinieneinstellungen für RV130- und RV130W-VPN-Router](#).

**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)

Schritt 4: Geben Sie einen Schlüssel mit einer Länge zwischen 8 und 49 Zeichen ein, der zwischen dem Gerät und dem Remote-Endpunkt im Feld *Vorinstallierter Schlüssel* ausgetauscht wird.

**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)

Schritt 5: Wählen Sie aus der Dropdown-Liste "Exchange Mode" den Modus für die IPSec-VPN-Verbindung aus. **Main (Hauptmodus)** ist der Standardmodus. Wenn Ihre Netzwerkgeschwindigkeit jedoch niedrig ist, wählen Sie den **aggressiven** Modus aus.

Server Enable:

**Phase 1 Configuration**

Pre-Shared Key: Testkey

Exchange Mode: Main

Encryption Algorithm: Aggressive

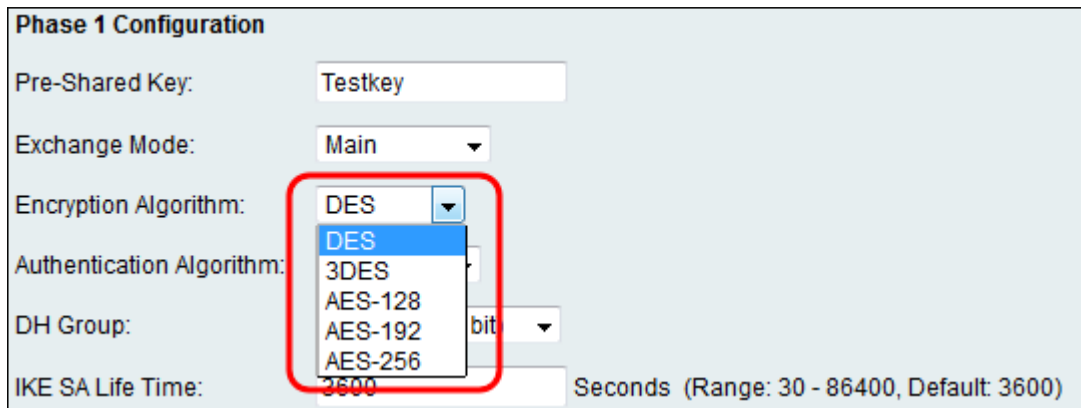
Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

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

**Anmerkung:** Der aggressive Modus tauscht die IDs der Endpunkte des Tunnels während der Verbindung im Klartext aus, was weniger Zeit für den Austausch benötigt, aber weniger Sicherheit bietet.

Schritt 6: Wählen Sie aus der Dropdown-Liste **Encryption Algorithm** (**Verschlüsselungsalgorithmus**) die geeignete Verschlüsselungsmethode zum Verschlüsseln des vorinstallierten Schlüssels in Phase 1 aus. AES-128 wird für hohe Sicherheit und schnelle Leistung empfohlen. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.



The screenshot shows the 'Phase 1 Configuration' window. The 'Pre-Shared Key' is 'Testkey', 'Exchange Mode' is 'Main', and 'IKE SA Life Time' is '3600' seconds. The 'Encryption Algorithm' dropdown menu is open, showing options: DES, 3DES, AES-128, AES-192, and AES-256. The 'Authentication Algorithm' dropdown is also open, showing options: DES, 3DES, AES-128, AES-192, and AES-256. The 'DH Group' dropdown is set to '1024' bits. The 'IKE SA Life Time' is '3600' seconds, with a range of 30 to 86400 seconds and a default of 3600 seconds.

Die verfügbaren Optionen sind wie folgt definiert:

- DES - Data Encryption Standard (DES) ist eine alte 56-Bit-Verschlüsselungsmethode, die nicht sehr sicher ist, aber möglicherweise für die Abwärtskompatibilität erforderlich ist.
- 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode, die verwendet wird, um die Schlüsselgröße zu erhöhen, da sie die Daten dreimal verschlüsselt. Dies bietet mehr Sicherheit als DES, aber weniger Sicherheit als AES.
- AES-128 — Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für die AES-Verschlüsselung. AES ist schneller und sicherer als DES. Generell ist AES auch schneller und sicherer als 3DES. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.
- AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128 und schneller, aber weniger sicher als AES-256.
- AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

Schritt 7: Wählen Sie aus der Dropdown-Liste *Authentication Algorithm* (*Authentifizierungsalgorithmus*) die entsprechende Authentifizierungsmethode aus, um zu bestimmen, wie die ESP-Protokoll-Headerpakete in Phase 1 validiert werden. Der VPN-Tunnel muss für beide Enden der Verbindung dieselbe Authentifizierungsmethode verwenden.

**Phase 1 Configuration**

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

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

Die verfügbaren Optionen sind wie folgt definiert:

- MD5 - MD5 ist ein unidirektionaler Hash-Algorithmus, der einen 128-Bit-Digest erzeugt. MD5 berechnet schneller als SHA-1, ist aber weniger sicher als SHA-1. MD5 wird nicht empfohlen.
- SHA-1 - SHA-1 ist ein unidirektionaler Hash-Algorithmus, der einen 160-Bit-Digest erzeugt. SHA-1 arbeitet langsamer als MD5, ist aber sicherer als MD5.
- SHA2-256 — Gibt den Secure Hash Algorithm SHA2 mit dem 256-Bit-Digest an.

Schritt 8: Wählen Sie aus der Dropdown-Liste "*DH Group*" (*DH-Gruppe*) die entsprechende Diffie-Hellman-Gruppe (DH-Gruppe) aus, die mit dem Schlüssel in Phase 1 verwendet werden soll. Diffie-Hellman ist ein kryptografisches Schlüsselaustauschprotokoll, das in der Verbindung zum Austausch von vorinstallierten Schlüsselsätzen verwendet wird. Die Stärke des Algorithmus wird durch Bits bestimmt.

**Phase 1 Configuration**

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

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

**Phase 2 Configuration**

Die verfügbaren Optionen sind wie folgt definiert:

- Group1 (768-Bit) - Berechnet den Schlüssel am schnellsten, aber am wenigsten sicher.
- Group2 (1024-Bit) — Berechnet den Schlüssel langsamer, ist aber sicherer als Group1.
- Group5 (1536-Bit) — Berechnet den Schlüssel am langsamsten, aber am sichersten.

Schritt 9: Geben Sie im Feld *IKE SA-Lebensdauer* die Zeit in Sekunden ein, die der automatische IKE-Schlüssel gültig ist. Nach Ablauf dieser Zeit wird automatisch ein neuer Schlüssel ausgehandelt.

**Phase 1 Configuration**

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

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

Schritt 10. Wählen Sie aus der Dropdown-Liste "*Lokale IP*" die Option **Single (Einzeln)** aus, wenn ein einzelner lokaler LAN-Benutzer auf den VPN-Tunnel zugreifen soll, oder **Subnet**, wenn mehrere Benutzer darauf zugreifen sollen.

**Phase 2 Configuration**

Local IP:

IP Address:   (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

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

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group:  Enable

DH Group:

Schritt 11: Wenn in Schritt 10 das **Subnetz** ausgewählt wurde, geben Sie die Netzwerk-IP-Adresse des Subnetzes in das Feld "IP-Adresse" ein. Wenn in Schritt 10 die Option **Single (Single)** ausgewählt wurde, geben Sie die IP-Adresse des einzelnen Benutzers ein, und fahren Sie mit Schritt 13 fort.

**Phase 2 Configuration**

Local IP:

**IP Address:  (Hint: 1.2.3.4)**

Subnet Mask:  (Hint: 255.255.255.0)

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

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group:  Enable

DH Group:

Schritt 12. (Optional) Wenn in Schritt 10 **Subnetz** ausgewählt wurde, geben Sie die Subnetzmaske des lokalen Netzwerks in das Feld *Subnetzmaske* ein.

**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) ▾

Schritt 13: Geben Sie im Feld "*IPSec SA Lifetime*" (*IPSec-SA-Lebensdauer*) die Zeit in Sekunden ein, die die VPN-Verbindung in Phase 2 aktiv bleibt. Nach Ablauf dieser Zeit wird die IPSec-Sicherheitszuordnung für die VPN-Verbindung neu ausgehandelt.

**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) ▾

Schritt 14: Wählen Sie aus der Dropdown-Liste *Encryption Algorithm* (*Verschlüsselungsalgorithmus*) die geeignete Verschlüsselungsmethode für die Verschlüsselung des vorinstallierten Schlüssels in Phase 2 aus. AES-128 wird für hohe Sicherheit und schnelle Leistung empfohlen. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

**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: DES

PFS Key Group: AES-128

AES-192

AES-256

DH Group: Group 1 (768 bit) ▼

Die verfügbaren Optionen sind wie folgt definiert:

- DES - Data Encryption Standard (DES) ist eine alte 56-Bit-Verschlüsselungsmethode, die am wenigsten sicher ist, aber möglicherweise für Abwärtskompatibilität erforderlich ist.
- 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode, die verwendet wird, um die Schlüsselgröße zu erhöhen, da sie die Daten dreimal verschlüsselt. Dies bietet mehr Sicherheit als DES, aber weniger Sicherheit als AES.
- AES-128 — Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für die AES-Verschlüsselung. AES ist schneller und sicherer als DES. Generell ist AES auch schneller und sicherer als 3DES. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.
- AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128 und schneller, aber weniger sicher als AES-256.
- AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

Schritt 15: Wählen Sie aus der Dropdown-Liste *Authentication Algorithm* (*Authentifizierungsalgorithmus*) die entsprechende Authentifizierungsmethode aus, um zu bestimmen, wie die ESP-Protokoll-Headerpakete in Phase 2 validiert werden. Der VPN-Tunnel muss für beide Enden dieselbe Authentifizierungsmethode verwenden.



**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:  Enable

DH Group: Group 1(768 bit) ▾

Die verfügbaren Optionen sind wie folgt definiert:

- MD5 - MD5 ist ein unidirektionaler Hash-Algorithmus, der einen 128-Bit-Digest erzeugt. MD5 berechnet schneller als SHA-1, ist aber weniger sicher als SHA-1. MD5 wird nicht empfohlen.
- SHA-1 - SHA-1 ist ein unidirektionaler Hash-Algorithmus, der einen 160-Bit-Digest erzeugt. SHA-1 arbeitet langsamer als MD5, ist aber sicherer als MD5.
- SHA2-256 — Gibt den Secure Hash Algorithm SHA2 mit dem 256-Bit-Digest an.

Schritt 16. (Optional) Aktivieren Sie im Feld *PFS-Schlüsselgruppe* das Kontrollkästchen **Aktivieren**. Perfect Forward Secrecy (PFS) schafft eine zusätzliche Sicherheitsebene für den Schutz Ihrer Daten, indem ein neuer DH-Schlüssel in Phase 2 sichergestellt wird. Der Prozess wird durchgeführt, falls der in Phase 1 generierte DH-Schlüssel bei der Übertragung beschädigt wird.

**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) ▾

Schritt 17: Wählen Sie aus der Dropdown-Liste *DH Group (DH-Gruppe)* die passende Diffie-Hellman-Gruppe (DH-Gruppe) aus, die mit dem Schlüssel in Phase 2 verwendet werden soll.

**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

Die verfügbaren Optionen sind wie folgt definiert:

- Group1 (768-Bit) - Berechnet den Schlüssel am schnellsten, aber am wenigsten sicher.
- Group2 (1024-Bit) — Berechnet den Schlüssel langsamer, ist aber sicherer als Group1.
- Group5 (1536-Bit) — Berechnet den Schlüssel am langsamsten, aber am sichersten.

Schritt 18: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

**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

Weitere Informationen finden Sie in der folgenden Dokumentation:

- [RV130-Datenblatt](#) - Erläuterung der VPN-Funktionen für Router der Serie RV130
- [RV130-Produktseite](#) - enthält Links zu allen RV130-Artikeln von Cisco

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.