

Beleidsinstellingen voor Internet Key Exchange (IKE) op RV130 en RV130W VPN-routers

Doel

Internet Key Exchange (IKE) is een protocol dat beveiligde communicatie tussen twee netwerken tot stand brengt. Met IKE worden pakketten versleuteld en vergrendeld en ontgrendeld met sleutels die door twee partijen worden gebruikt.

U moet een Internet Key Exchange-beleid maken voordat u een VPN-beleid configureert. Raadpleeg [VPN Policy Configuration op RV130 en RV130W](#) voor meer informatie.

Het doel van dit document is u te tonen hoe u een IKE-profiel kunt toevoegen aan RV130- en RV130W VPN-routers.

Toepasselijke apparaten

- RV130
- RV130W

Werkwijze

Stap 1. Gebruik het hulpprogramma voor routerconfiguratie om **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup** te kiezen in het menu links. De pagina *Advanced VPN Setup* verschijnt:

Advanced VPN Setup

NAT Traversal: Enable

IKE Policy Table

<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				

VPN Policy Table

<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

Stap 2. Klik onder de IKE-beleidstabel op **Rij toevoegen**. Er verschijnt een nieuw venster:

IKE Policy Table

<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				

Stap 3. Voer een naam in voor het IKE-beleid in het veld *IKE-naam*.

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Stap 4. Kies in het vervolgkeuzemenu *Exchange Mode* de modus waarin een sleuteluitwisseling wordt gebruikt om beveiligde communicatie tot stand te brengen.

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Main
Main
Aggressive

De beschikbare opties zijn als volgt gedefinieerd:

- Main — Beschermt de identiteit van peers voor meer veiligheid.
- Agressief — geen bescherming van de identiteit van deelnemers, maar zorgt voor een snellere verbinding.

Stap 5. Kies in het vervolgkeuzemenu *Local Identifier Type* het type identiteit van het profiel.

Local

Local Identifier Type:

Local Identifier:

Local WAN IP
Local WAN IP
IP Address

De beschikbare opties zijn als volgt gedefinieerd:

- Lokale WAN (Internet) IP — maakt verbinding via internet.
- IP-adres — unieke reeks getallen, gescheiden door punten, die elke machine identificeert met behulp van het Internet Protocol om via een netwerk te communiceren.

Stap 6. (Optioneel) Als **IP-adres** is geselecteerd in de vervolgkeuzelijst in stap 5, voert u het lokale IP-adres in het veld *Local Identifier in*.

Local

Local Identifier Type:

Local Identifier:

Stap 7. Kies in het vervolgkeuzemenu *Remote Identifier Type* het type identiteit van het profiel.

Remote

Remote Identifier Type:

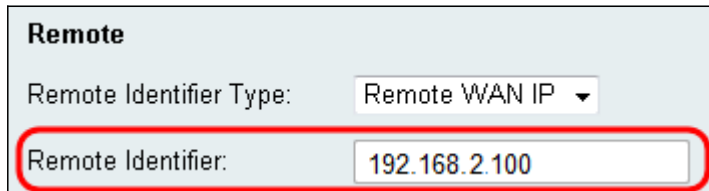
Remote Identifier:

Remote WAN IP
Remote WAN IP
IP Address

De beschikbare opties zijn als volgt gedefinieerd:

- Lokale WAN (Internet) IP — maakt verbinding via internet.
- IP-adres — unieke reeks getallen, gescheiden door punten, die elke machine identificeert met behulp van het Internet Protocol om via een netwerk te communiceren.

Stap 8. (Optioneel) Als **IP-adres** is geselecteerd in de vervolgkeuzelijst in stap 7, voert u het externe IP-adres in het veld *Remote Identifier in*.

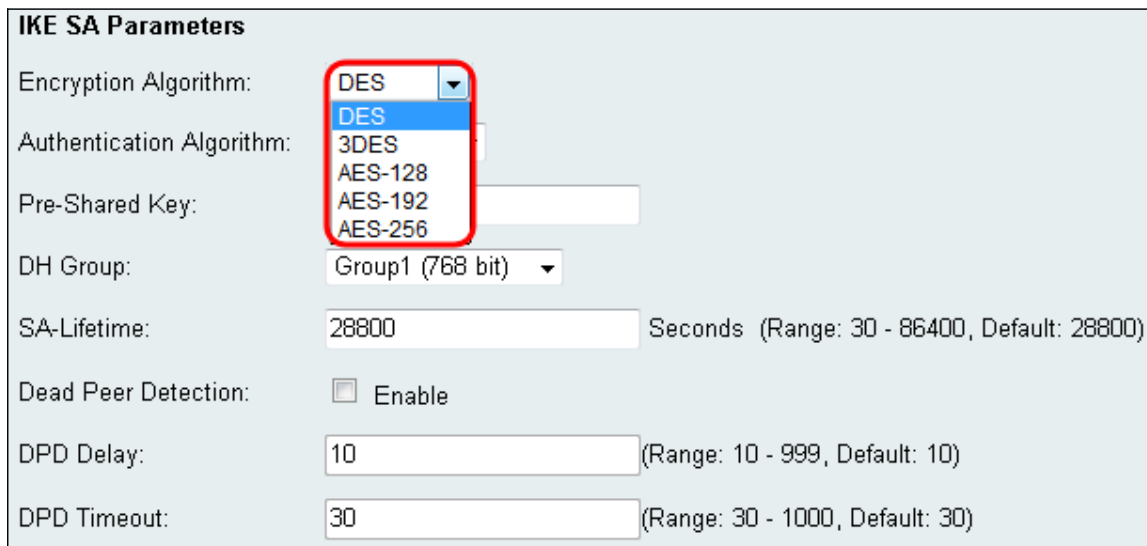


Remote

Remote Identifier Type: Remote WAN IP ▼

Remote Identifier: 192.168.2.100

Stap 9. Kies in het vervolgkeuzemenu *Encryptie Algorithm* een algoritme om uw communicatie te versleutelen. **AES-128** is standaard geselecteerd.



IKE SA Parameters

Encryption Algorithm: DES ▼

Authentication Algorithm:

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)

De beschikbare opties zijn als volgt weergegeven van de minste tot de grootste beveiliging:

- DES — Data Encryption Standard.
- 3DES — Triple Data Encryption Standard.
- AES-128 — Advanced Encryption Standard gebruikt een 128-bits sleutel.
- AES-192 — Advanced Encryption Standard gebruikt een 192-bits sleutel.
- AES-256 — Advanced Encryption Standard gebruikt een 256-bits sleutel.

Opmerking: AES is de standaardmethode voor codering via DES en 3DES om de prestaties en beveiliging te verbeteren. Door de AES-toets te verlengen, neemt de beveiliging toe met minder prestaties. AES-128 wordt aanbevolen omdat dit het beste compromis is tussen snelheid en beveiliging.

Stap 10. Kies in het vervolgkeuzemenu *Verificatiealgoritme* een algoritme om uw communicatie te verifiëren. **SHA-1** is standaard geselecteerd.

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)

De beschikbare opties zijn als volgt gedefinieerd:

- MD5 — Message Digest Algorithm heeft een 128-bits hashwaarde.
- SHA-1 — Secure Hash Algoritme heeft een 160 bit hash waarde.
- SHA2-256 — Secure Hash Algoritme met een 256 bit hash waarde.

Opmerking: MD5 en SHA zijn beide cryptografische hashfuncties. Ze nemen een stukje data, comprimeren het en creëren een unieke hexadecimale output die meestal niet reproduceerbaar is. MD5 biedt in wezen geen beveiliging tegen hashingbotsingen en mag alleen worden gebruikt in een omgeving voor kleine bedrijven waarin geen botsingsweerstand nodig is. SHA1 is een betere keuze dan de MD5 omdat het betere beveiliging biedt bij verwaarloosbaar langzamere snelheden. Voor het beste resultaat heeft SHA2-256 geen bekende aanvallen van praktisch belang en zal de beste beveiliging bieden. Zoals eerder gezegd betekent een hogere beveiliging een lagere snelheid.

Stap 1. Voer in het veld *Vooraf gedeelde sleutel* een wachtwoord in dat tussen 8 en 49 tekens lang is.

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)

Stap 12. Kies een *DH*-groep in het vervolgkeuzemenu *DH Group*. Het aantal bits geeft het beveiligingsniveau aan. Beide uiteinden van de verbinding moeten in de zelfde groep zijn.

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)

Stap 13. Voer in het veld *SA-Lifetime* in hoe lang de Security Association in seconden geldig zal zijn. De standaardinstelling is 28800 seconden.

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)

Stap 14. (Optioneel) Controleer het aanvinkvakje **Enable** in het veld *Dead Peer Detection* als u een verbinding met inactieve peer wilt uitschakelen. Ga verder naar stap 17 als u Dead peer Detection niet hebt ingeschakeld.

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)

Stap 15. (Optioneel) Als u Dead Peer Detection hebt ingeschakeld, voert u een waarde in

het veld *DPD Delay* in. Deze waarde zal specificeren hoe lang de router zal wachten om clientconnectiviteit te controleren.

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)

Stap 16. (Optioneel) Als u Dead Peer Detection hebt ingeschakeld, voert u een waarde in het veld *DPD Time-out* in. Deze waarde geeft aan hoe lang de client verbonden blijft tot de tijd is verstreken.

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)

Stap 17. Klik op **Opslaan** om de wijzigingen op te slaan.

IKE SA Parameters	
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"/>	

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.