

Geavanceerde Virtual Private Network (VPN)-instelling configureren op een RV130 of RV130W router

Doel

Een Virtual Private Network (VPN) is een beveiligde verbinding die binnen een netwerk of tussen netwerken wordt gemaakt. VPN's dienen om verkeer tussen gespecificeerde hosts en netwerken te isoleren van het verkeer van onbevoegde hosts en netwerken. Een site-to-site (gateway-to-gateway) VPN verbindt volledige netwerken met elkaar en houdt de beveiliging in stand door een tunnel te maken via een openbaar domein dat ook wel bekend staat als het internet. Elke site heeft alleen een lokale verbinding met hetzelfde openbare netwerk nodig, waardoor geld wordt bespaard op lange private huurlijnen-s.

VPN's zijn voordelig voor bedrijven op een manier dat het zeer schaalbaar is, de netwerktopologie vereenvoudigt en de productiviteit verbetert door de reistijd en kosten voor externe gebruikers te verminderen.

Internet Key Exchange (IKE) is een protocol dat wordt gebruikt om een beveiligde verbinding tot stand te brengen voor communicatie in een VPN. Deze beveiligde verbinding wordt een Security Association (SA) genoemd. U kunt beleid tot stand brengen IKE om de veiligheidsparameters te bepalen die in dit proces zoals authenticatie van de edele, encryptiealgoritmen, etc. moeten worden gebruikt. Om een VPN goed te laten functioneren, moet het IKE-beleid voor beide eindpunten identiek zijn.

Dit artikel heeft als doel te tonen hoe je de Advanced VPN Setup kunt configureren op een RV130- of RV130W-router, die IKE-beleidsinstellingen en VPN-beleidsinstellingen bevat.

Toepasselijke apparaten

- RV130
RV130W

Softwareversie

- 1.0.3.22

Geavanceerde VPN-instellingen configureren

Beleidsinstellingen voor Internet Key Exchange (IKE) toevoegen/bewerken

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en kies **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup**.

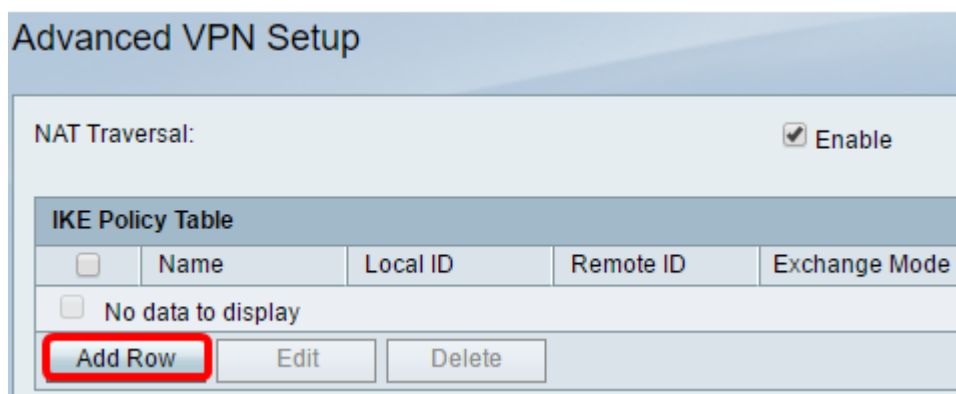


Stap 2. (Optioneel) Schakel het aankruisvakje **Enable** in NAT-transversale modus in als u Network Address Translation (NAT) Transversale modus wilt inschakelen voor de VPN-verbinding. NAT-transversale maakt het mogelijk een VPN-verbinding te maken tussen gateways die NAT gebruiken. Kies deze optie als uw VPN-verbinding doorloopt via een NAT-enabled gateway.



Stap 3. Klik in de IKE Policy Table op **Add Row** om een nieuw IKE-beleid te maken.

Opmerking: Als de basisinstellingen zijn geconfigureerd, zal de onderstaande tabel de gemaakte standaard VPN-instelling bevatten. U kunt een bestaand IKE-beleid bewerken door het aankruisvakje voor het beleid aan te vinken en op **Bewerken** te klikken. De pagina Geavanceerde VPN-instellingen verandert:



Stap 4. Voer in het veld *IKE-naam* een unieke naam in voor het IKE-beleid.

Opmerking: Als de basisinstellingen zijn geconfigureerd, wordt de verbindingsnaam ingesteld als IKE-naam. In dit voorbeeld is VPN1 de gekozen IKE-naam.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

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 5. Kies een optie uit de vervolgkeuzelijst Exchange Mode.

- Main — Deze optie staat het IKE-beleid toe om de VPN-tunnel te onderhandelen met een hogere beveiliging dan agressieve modus. Klik op deze optie als een veiligere VPN-verbinding een prioriteit is boven een snelheid van onderhandeling.
- Agressief — Met deze optie kan het IKE-beleid een snellere maar minder beveiligde verbinding tot stand brengen dan in de hoofdmodus. Klik op deze optie als een snellere VPN-verbinding voorrang heeft op een hoge beveiliging.

Opmerking: In dit voorbeeld is Main gekozen.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode: ▼

Main

Aggressive

Local Identifier Type: ▼

Stap 6. Kies uit de lijst Local Identifier Typedrop-down om de Internet Security Association en Key Management Protocol (ISAKMP) van uw lokale router te identificeren of te specificeren. De opties zijn:

- Local WAN IP — Router gebruikt IP van Local Wide Area Network (WAN) als belangrijkste identificatiecode. Deze optie maakt verbinding via internet. Bij deze optie wordt het veld *Local Identifier* hieronder grijs weergegeven.
- IP-adres — Als u op deze knop klikt, kunt u een IP-adres invoeren in het veld *Local Identifier*.
- FQDN — Met een volledig gekwalificeerde domeinnaam (FQDN) of uw domeinnaam zoals <http://www.example.com> kunt u uw domeinnaam of IP-adres invoeren in het veld *Local Identifier*.
- Gebruiker-FQDN — Deze optie is een e-mailadres zoals user@email.com. Voer een domeinnaam of IP-adres in in het veld *Local Identifier*.
- DER ASN1 DN — Deze optie is een herkenningstype voor de Onderscheidbare Naam (DN) die Onderscheidbare Coderingsregels Abstracte Syntax Notatie One (DER ASN1) gebruikt om informatie door te geven. Dit gebeurt wanneer de VPN-tunnel is gekoppeld aan een gebruikerscertificaat. Als u deze optie kiest, voert u een domeinnaam of IP-adres in het veld *Local Identifier* in.

Opmerking: In dit voorbeeld is IP met lokaal WAN gekozen.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

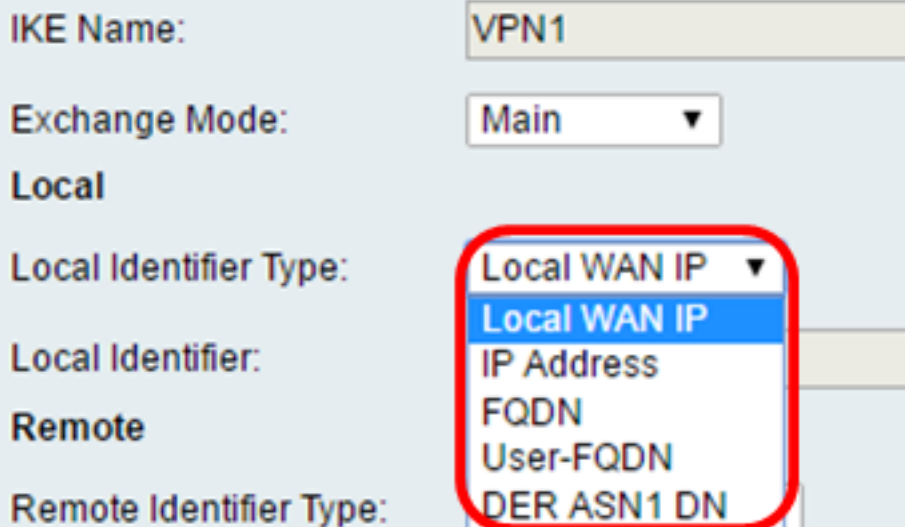
Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:



Stap 7. Kies uit de vervolgkeuzelijst Remote Identifier Type om de Internet Security Association en Key Management Protocol (ISAKMP) van uw externe router te identificeren of te specificeren. De opties zijn Remote WAN IP, IP-adres, FQDN, User FQDN en DER ASN1 DN.

Opmerking: In dit voorbeeld is Remote WAN IP gekozen.

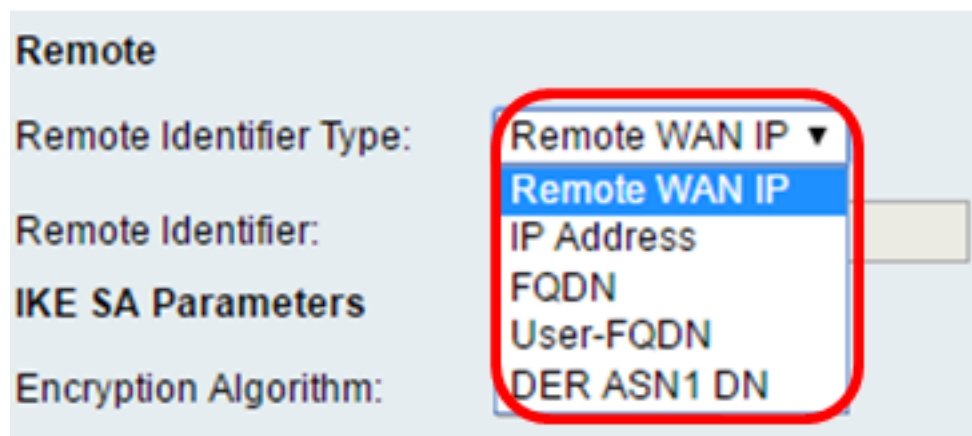
Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

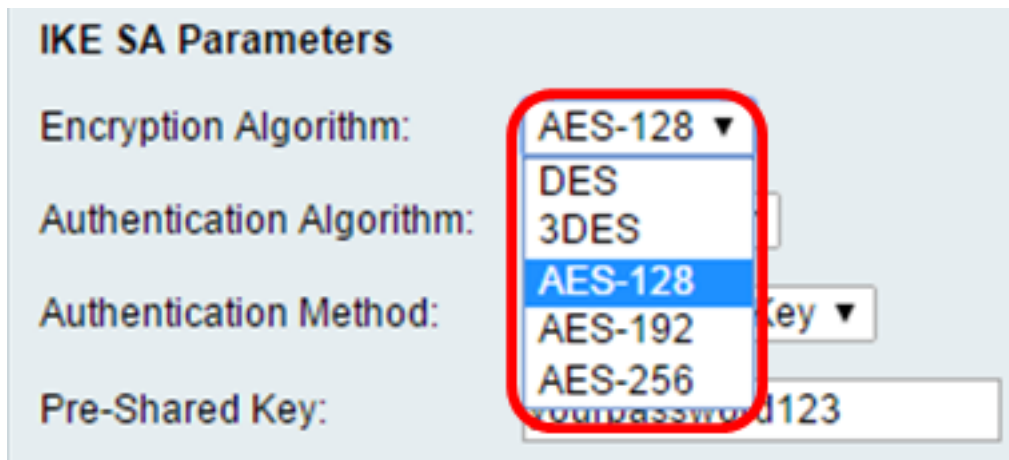


Stap 8. Kies een optie uit de vervolgkeuzelijst Encryptiealgoritme.

- DES — Data Encryption Standard (DES) is een 56-bits, oude coderingsmethode die geen zeer veilige coderingsmethode is, maar die wellicht nodig is voor achterwaartse compatibiliteit.
- 3DES — Triple Data Encryption Standard (3DES) is een 168-bits, eenvoudige coderingsmethode die wordt gebruikt om de sleutel te vergroten omdat de gegevens drie keer worden versleuteld. Dit biedt meer beveiliging dan DES maar minder beveiliging dan AES.
- AES-128 — Advanced Encryption Standard met 128-bits sleutel (AES-128) gebruikt een 128-bits sleutel voor AES-encryptie. AES is sneller en veiliger dan DES. Over het algemeen is AES ook sneller en veiliger dan 3DES. AES-128 is het standaard encryptie algoritme en is sneller maar minder veilig dan AES-192 en AES-256.

- AES-192 — AES-192 gebruikt een 192-bits sleutel voor AES-encryptie. AES-192 is trager maar veiliger dan AES-128, en sneller maar minder veilig dan AES-256.
- AES-256 — AES-256 gebruikt een 256-bits sleutel voor AES-encryptie. AES-256 is langzamer maar veiliger dan AES-128 en AES-192.

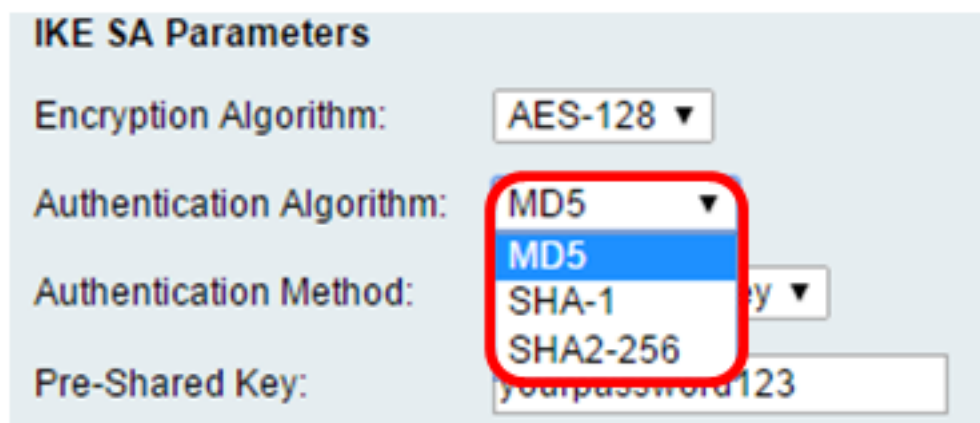
Opmerking: In dit voorbeeld is AES-128 geselecteerd.



Stap 9. Kies uit de volgende opties in de vervolgkeuzelijst Verificatiealgoritme:

- MD5 — Message Digest 5 (MD5) is een verificatiealgoritme dat een 128-bits hashwaarde voor verificatie gebruikt. MD5 is minder veilig, maar sneller dan SHA-1 en SHA2-256.
- SHA-1 — Secure Hash-functie 1 (SHA-1) gebruikt een 160-bits hashwaarde voor verificatie. SHA-1 is trager maar veiliger dan MD5. SHA-1 is het standaard verificatiealgoritme en is sneller maar minder veilig dan SHA2-256.
- SHA2-256 — Secure Hash Algorithm 2 met een 256-bits hashwaarde (SHA2-256) gebruikt een 256-bits hashwaarde voor verificatie. SHA2-256 is langzamer maar veiliger dan MD5 en SHA-1.

Opmerking: In dit voorbeeld is MD5 gekozen.



Stap 10. Kies uit de volgende opties in de vervolgkeuzelijst Verificatiemethode:

- Vooraf gedeelde sleutel — voor deze optie is een wachtwoord vereist dat wordt gedeeld met de IKE-peer.
- RSA-handtekening — Bij deze optie worden certificaten gebruikt om de verbinding te verifiëren. Als dit wordt gekozen, wordt het veld Vooraf gedeelde sleutel uitgeschakeld. Naar [Stap 12](#).

Opmerking: In dit voorbeeld is de Pre-Shared sleutel gekozen.

IKE SA Parameters

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

Authentication Method: Pre-Shared Key ▼

Pre-Shared Key:

DH Group: Group2 (1024 bit) ▼

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

Opmerking: In dit voorbeeld wordt uw wachtwoord123 gebruikt.

IKE SA Parameters

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

Authentication Method: Pre-Shared Key ▼

Pre-Shared Key:

[Stap 12.](#) Kies in de vervolgkeuzelijst DH-groep welk Diffie-Hellman (DH) groepsalgoritme de IKE gebruikt. Hosts in een DH-groep kunnen sleutels uitwisselen zonder dat ze elkaar kennen. Hoe hoger het nummer van het groepsbit, hoe beter de beveiliging.

Opmerking: In dit voorbeeld is Group1 gekozen.

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)

Save Cancel Back

Stap 13. Voer in het veld *SA-Lifetime* in hoe lang een SA voor VPN duurt voordat de SA

wordt vernieuwd. Het bereik loopt van 30 tot 86400 seconden. De standaardwaarde is 28800.

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)

Save Cancel Back

[Stap 14](#). (optioneel) Controleer het aanvinkvakje **Enable** Dead Peer Detection (DPD) om Dead Peer Detection (DPD) in te schakelen. DPD monitort IKE-peers om te zien of een peer niet meer werkt of nog leeft. Als de peer dood wordt gedetecteerd, verwijdert het apparaat de IPsec en IKE Security Association. DPD voorkomt de verspilling van netwerkbronnen op inactieve peers.

Opmerking: Als u Dead Peer Detection niet wilt inschakelen, gaat u naar [Stap 17](#).

Dead Peer Detection: Enable

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

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

Save Cancel Back

Stap 15. (Optioneel) Als u DPD in [Stap 14](#) hebt ingeschakeld, voert u in hoe vaak (in seconden) de peer wordt gecontroleerd op activiteit in het veld *DPD Delay*.

Opmerking: De DPD Delay is het interval in seconden tussen opeenvolgende DPD R-U-ER berichten. DPD R-U-DAAR berichten worden alleen verstuurd wanneer het IPsec-verkeer niet actief is. De standaardwaarde is 10.

Dead Peer Detection: Enable

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

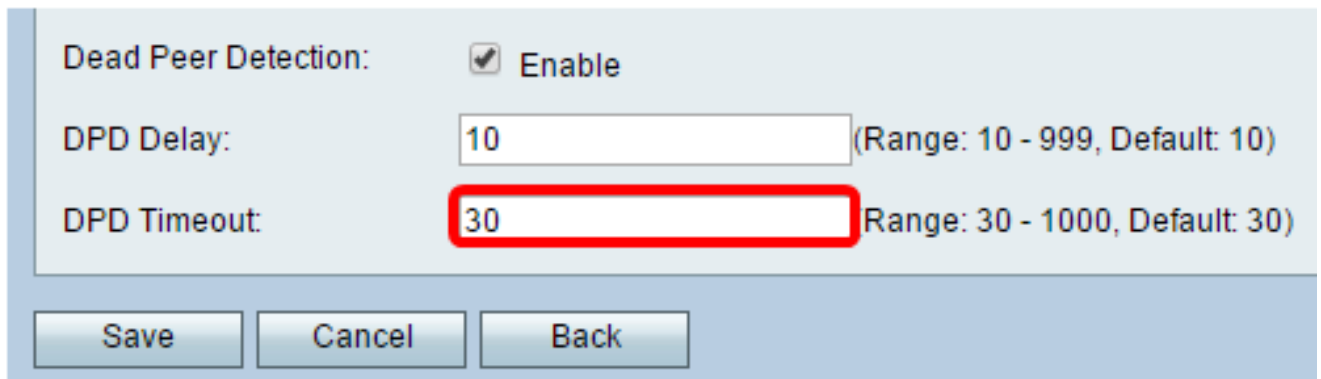
DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Save Cancel Back

Stap 16. (Optioneel) Als u DPD in [Stap 14](#) hebt ingeschakeld, voert u in hoeveel seconden u

moet wachten voordat een inactieve peer in het veld *DPD Time-out* wordt gedropt.

Opmerking: Dit is de maximumtijd dat het apparaat zou moeten wachten om een reactie op het DPD- bericht te ontvangen alvorens de peer als dood te beschouwen. De standaardwaarde is 30.



Dead Peer Detection: Enable

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

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

Save Cancel Back

[Stap 17.](#) Klik op **Opslaan**.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

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)

Opmerking: De belangrijkste pagina voor geavanceerde VPN-instellingen wordt opnieuw weergegeven.

U had nu met succes de IKE Policy Settings op uw router moeten configureren.

VPN-beleidsinstellingen configureren

Opmerking: voor een VPN om goed te functioneren, moet het VPN-beleid voor beide eindpunten identiek zijn.

Stap 1. Klik in de VPN Policy Table op **Add Row** om een nieuw VPN-beleid te maken.

Opmerking: U kunt ook een VPN-beleid bewerken door het aanvinkvakje voor het beleid aan te vinken en op **Bewerken** te klikken. De pagina Geavanceerde VPN-instellingen verschijnt:

The screenshot shows the 'Advanced VPN Setup' window. At the top, there is a 'NAT Traversal' section with an unchecked checkbox. Below it is the 'IKE Policy Table' with columns for Name, Local ID, Remote ID, Exchange Mode, and an unchecked checkbox. A row is visible with 'VPN1' in the Name column, 'Local WAN IP' in the Local ID column, 'Remote WAN IP' in the Remote ID column, and 'Main' in the Exchange Mode column. Below the table are 'Add Row', 'Edit', and 'Delete' buttons. The 'VPN Policy Table' section below has columns for Status, Name, Policy Type, and Encryption, with an unchecked checkbox and the text 'No data to display'. The 'Add Row' button in this section is highlighted with a red rectangle. At the bottom of the window are 'Save', 'Cancel', and 'IPSec Connection Status' buttons.

Stap 2. Voer in het veld *IPSec Name* onder het gebied Add/Edit VPN Configuration een naam in voor het VPN-beleid.

Opmerking: In dit voorbeeld wordt VPN1 gebruikt.

The screenshot shows the 'Advanced VPN Setup' window, specifically the 'Add / Edit VPN Policy Configuration' section. The 'IPSec Name' field is set to 'VPN1' and is highlighted with a red rectangle. The 'Policy Type' dropdown menu is set to 'Auto Policy', and the 'Remote Endpoint' dropdown menu is set to 'IP Address'.

[Stap 3.](#) Kies een optie uit de vervolgkeuzelijst *Beleidstype*.

- Handmatig beleid — Met deze optie kunt u de sleutels voor gegevenscodering en integriteit voor de VPN-tunnel handmatig configureren. Als u deze optie kiest, worden de configuratie-instellingen onder het gebied Handmatige beleidsparameters ingeschakeld. Ga door met de stappen tot Remote Traffic Selection. Klik [hier](#) om de stappen te kennen.
- Automatisch beleid — Beleidsparameters worden automatisch ingesteld. Deze optie maakt gebruik van een IKE-beleid voor gegevensintegriteit en het uitwisselen van coderingssleutels. Als dit wordt gekozen, worden de configuratie-instellingen onder het gebied Auto Policy Parameters ingeschakeld. Klik [hier](#) om de stappen te kennen. Zorg ervoor dat uw IKE-protocol automatisch onderhandelt tussen de twee VPN-endpoints.

Opmerking: In dit voorbeeld is Auto Policy gekozen.

The screenshot shows the 'Advanced VPN Setup' interface. Under the 'Add / Edit VPN Policy Configuration' section, the 'IPSec Name' is 'VPN1'. The 'Policy Type' dropdown menu is open, with 'Auto Policy' selected. The 'Remote Endpoint' field is empty.

Stap 4. Kies een optie uit de vervolgkeuzelijst Remote Endpoint.

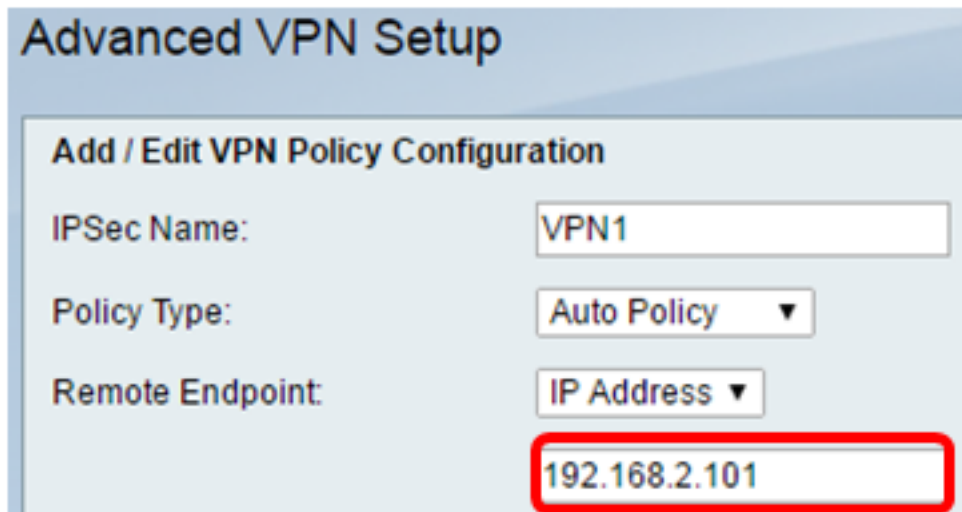
- IP-adres - met deze optie wordt het externe netwerk geïdentificeerd aan de hand van een openbaar IP-adres.
- FQDN — Complete domeinnaam voor een specifieke computer, host of internet. De FQDN bestaat uit twee delen: de hostnaam en de domeinnaam. Deze optie kan alleen worden ingeschakeld wanneer **Automatisch beleid** is geselecteerd in [stap 3](#).

Opmerking: Hierbij wordt bijvoorbeeld IP-adres gekozen.

The screenshot shows the 'Advanced VPN Setup' interface. Under the 'Add / Edit VPN Policy Configuration' section, the 'IPSec Name' is 'VPN1'. The 'Policy Type' dropdown menu is set to 'Auto Policy'. The 'Remote Endpoint' dropdown menu is open, with 'IP Address' selected.

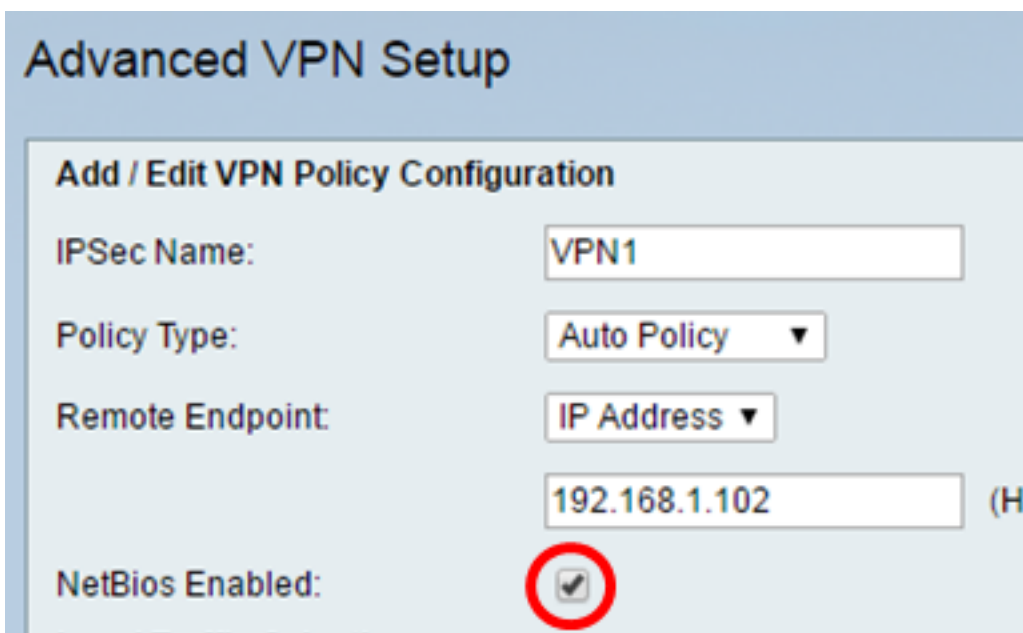
Stap 5. Voer in het veld *Remote Endpoint* het openbare IP-adres of de domeinnaam van het externe adres in.

Opmerking: In dit voorbeeld wordt 192.168.2.101 gebruikt.



The screenshot shows the 'Advanced VPN Setup' interface. Under the 'Add / Edit VPN Policy Configuration' section, the 'IPSec Name' is 'VPN1', 'Policy Type' is 'Auto Policy', and 'Remote Endpoint' is 'IP Address'. The IP address '192.168.2.101' is entered in the text field below and is highlighted with a red rectangle.

Stap 6. (Optioneel) Schakel het aanvinkvakje **NetBios Enabled in** als u wilt dat de uitzendingen van Network Basic Input/Output System (NetBIOS) via de VPN-verbinding worden verzonden. Met NetBIOS kunnen hosts met elkaar communiceren binnen een Local Area Network (LAN).



The screenshot shows the 'Advanced VPN Setup' interface. Under the 'Add / Edit VPN Policy Configuration' section, the 'IPSec Name' is 'VPN1', 'Policy Type' is 'Auto Policy', and 'Remote Endpoint' is 'IP Address'. The IP address '192.168.1.102' is entered in the text field below. The 'NetBios Enabled' checkbox is checked and highlighted with a red circle.

[Stap 7.](#) Kies een optie in de vervolgkeuzelijst Local IP onder Local Traffic Selection.

- Enkel — Beperkt het beleid tot één gastheer.
- Subnet — hiermee kunnen hosts binnen een IP-adresbereik verbinding maken met VPN.

Opmerking: In dit voorbeeld is Subnet geselecteerd.

Local Traffic Selection

Local IP:

IP Address:

Subnet Mask:

Stap 8. Voer in het veld IP-adres het IP-adres van de host of het subnetadres van het lokale subnet of de lokale host in.

Opmerking: In dit voorbeeld wordt het lokale subnetIP-adres van 10.10.10.1 gebruikt.

Local Traffic Selection

Local IP:

IP Address:

Subnet Mask:

Stap 9. (optioneel) Als Subnet is geselecteerd in [Stap 7](#), voert u het subnetmasker van de client in het veld *Subnetmasker* in. Het veld Subnet Mask is uitgeschakeld als in Stap 1 de optie Enkelvoudig is geselecteerd.

Opmerking: In dit voorbeeld wordt het subnetmasker van 25.25.0.0 gebruikt.

Local Traffic Selection

Local IP:

IP Address:

Subnet Mask:

[Stap 10](#). Kies een optie uit de vervolgkeuzelijst Remote IP onder het gedeelte Remote Traffic Selection.

- Enkel — Beperkt het beleid tot één gastheer.
- Subnet — hiermee kunnen hosts binnen een IP-adresbereik verbinding maken met VPN.

Opmerking: In dit voorbeeld is Subnet geselecteerd.

Remote Traffic Selection

Remote IP:

IP Address:

Subnet Mask:

Stap 1. Voer het bereik van IP-adressen van de host in die deel zullen uitmaken van VPN in het veld *IP-adres*. Als **Single** is geselecteerd in [Stap 10](#), voert u een IP-adres in.

Opmerking: In het onderstaande voorbeeld wordt 10.10.11.2 gebruikt.

Remote Traffic Selection

Remote IP:

IP Address:

Subnet Mask:

Stap 12. (optioneel) Als **Subnet** is geselecteerd in [stap 10](#), voert u het subnetmasker van het subnetadres in het veld *Subnetmasker* in.

Opmerking: In het onderstaande voorbeeld wordt 255.255.0.0 gebruikt.

Remote Traffic Selection

Remote IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

[Handmatig beleid Parameters](#)

Opmerking: deze velden kunnen alleen worden bewerkt als **Handmatig beleid** is geselecteerd.

Stap 1. Voer in het veld *SPI-inkomende* drie tot acht hexadecimale tekens in voor de Security Parameter Index (SPI)-tag voor inkomend verkeer op de VPN-verbinding. De SPI-tag wordt gebruikt om het verkeer van een sessie te onderscheiden van het verkeer van andere sessies.

Opmerking: In dit voorbeeld wordt 0xABCD gebruikt.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Stap 2. Voer in het veld *SPI-uitgaand* drie tot acht hexadecimale tekens in voor de SPI-tag voor uitgaand verkeer via de VPN-verbinding.

Opmerking: Bij dit voorbeeld wordt 0x1234 gebruikt.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

[Stap 3](#). Kies een optie uit de vervolgkeuzelijst *Handmatige encryptie-algoritme*. De opties zijn DES, 3DES, AES-128, AES-192, en AES-256.

Opmerking: In dit voorbeeld is AES-128 gekozen.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Manual Encryption Algorithm:

Key-In:

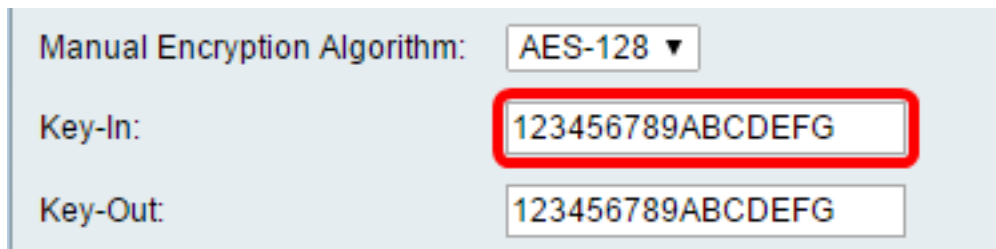
Key-Out:

Manual Integrity Algorithm:

Stap 4. Voer in het veld *Key-In* een sleutel in voor het inkomende beleid. De sleutellengte is afhankelijk van het in [Stap 3](#) gekozen algoritme.

- DES gebruikt een 8-karakter sleutel.
- 3DES gebruikt een 24-karakter sleutel.
- AES-128 gebruikt een 16-karakter sleutel.
- AES-192 gebruikt een 24-karakter sleutel.
- AES-256 gebruikt een 32-karakter sleutel.

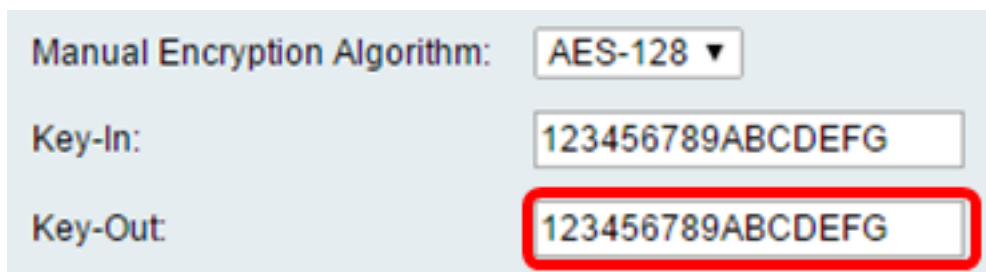
Opmerking: In dit voorbeeld wordt 123456789ABCDEFGG gebruikt.



Manual Encryption Algorithm: AES-128 ▼
Key-In: 123456789ABCDEFGG
Key-Out: 123456789ABCDEFGG

Stap 5. Voer in het veld *Key-Out* een sleutel in voor het uitgaande beleid. De sleutellengte is afhankelijk van het in [Stap 3](#) gekozen algoritme.

Opmerking: In dit voorbeeld wordt 123456789ABCDEFGG gebruikt.

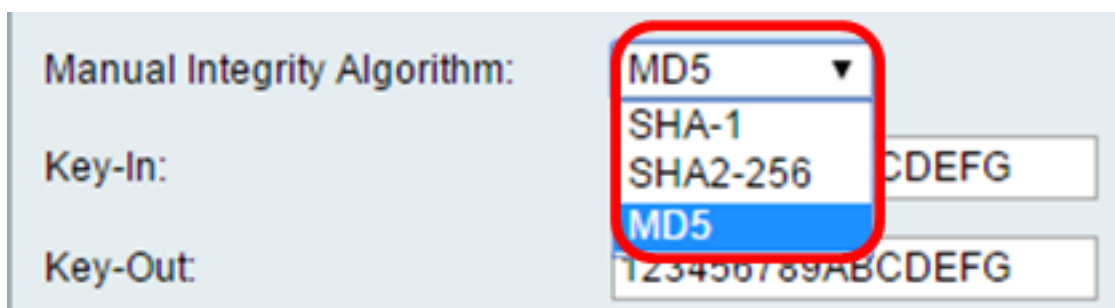


Manual Encryption Algorithm: AES-128 ▼
Key-In: 123456789ABCDEFGG
Key-Out: 123456789ABCDEFGG

[Stap 6](#). Kies een optie uit de vervolgkeuzelijst Manual Integrity Algorithm.

- MD5 — Gebruikt een 128-bits hashwaarde voor gegevensintegriteit. MD5 is minder veilig maar sneller dan SHA-1 en SHA2-256.
- SHA-1 — Gebruikt een 160-bits hashwaarde voor gegevensintegriteit. SHA-1 is langzamer maar veiliger dan MD5, en SHA-1 is sneller maar minder veilig dan SHA2-256.
- SHA2-256 — Gebruikt een 256-bits hashwaarde voor gegevensintegriteit. SHA2-256 is langzamer maar veilig dan MD5 en SHA-1.

Opmerking: In dit voorbeeld is MD5 gekozen.



Manual Integrity Algorithm: MD5 ▼
Key-In: 123456789ABCDEFGG
Key-Out: 123456789ABCDEFGG

Stap 7. Voer in het veld *Sleutel-in* een sleutel in voor het inkomende beleid. De sleutellengte is afhankelijk van het in [Stap 6](#) gekozen algoritme.

- MD5 gebruikt een 16-tekentoets.
- SHA-1 gebruikt een 20-tekentoets.
- SHA2-256 gebruikt een 32-karakter sleutel.

Opmerking: In dit voorbeeld wordt 123456789ABCDEFGG gebruikt.

Manual Integrity Algorithm:	MD5 ▼
Key-In:	123456789ABCDEFGG
Key-Out:	123456789ABCDEFGG

Stap 8. Voer in het veld *Key-Out* een sleutel in voor het uitgaande beleid. De sleutellengte is afhankelijk van het in [Stap 6](#) gekozen algoritme.

Opmerking: In dit voorbeeld wordt 123456789ABCDEFGG gebruikt.

Manual Integrity Algorithm:	MD5 ▼
Key-In:	123456789ABCDEFGG
Key-Out:	123456789ABCDEFGG

[Auto Beleidsparameters](#)

Opmerking: Voordat u een Auto VPN-beleid maakt, zorg ervoor dat u het IKE-beleid maakt op basis waarvan u het auto VPN-beleid wilt maken. Deze velden kunnen alleen worden bewerkt als **Auto Policy** is geselecteerd in [Stap 3](#).

Stap 1. Voer in het veld *IPSec SA-Lifetime* in hoe lang de SA in seconden duurt voordat de verlenging plaatsvindt. Het bereik loopt van 30-86400. De standaardinstelling is 3600.

Auto Policy Parameters	
IPSec SA Lifetime:	3600 Seconds (Range: 30 - 86400, Default 3600)
Encryption Algorithm:	AES-128 ▼
Integrity Algorithm:	SHA-1 ▼
PFS Key Group:	<input type="checkbox"/> Enable

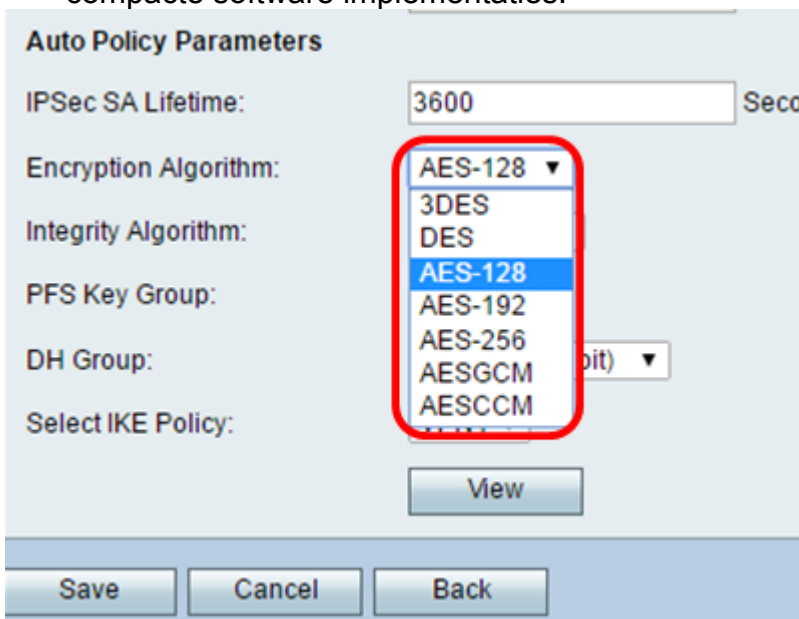
Stap 2. Kies een optie uit de vervolgkeuzelijst Encryptiealgoritme. De opties zijn:

Opmerking: In dit voorbeeld is AES-128 gekozen.

- DES — Een 56-bits oude coderingsmethode die geen zeer veilige coderingsmethode is, maar die nodig kan zijn voor achterwaartse compatibiliteit.
- 3DES — Een 168-bits, eenvoudige coderingsmethode die wordt gebruikt om de sleutel groter te maken, omdat de gegevens drie keer worden versleuteld. Dit biedt meer beveiliging dan DES maar minder beveiliging dan AES.
- AES-128 — Gebruikt een 128-bits sleutel voor AES-encryptie. AES is sneller en veiliger dan DES. Over het algemeen is AES ook sneller en veiliger dan 3DES. AES-128 is sneller maar

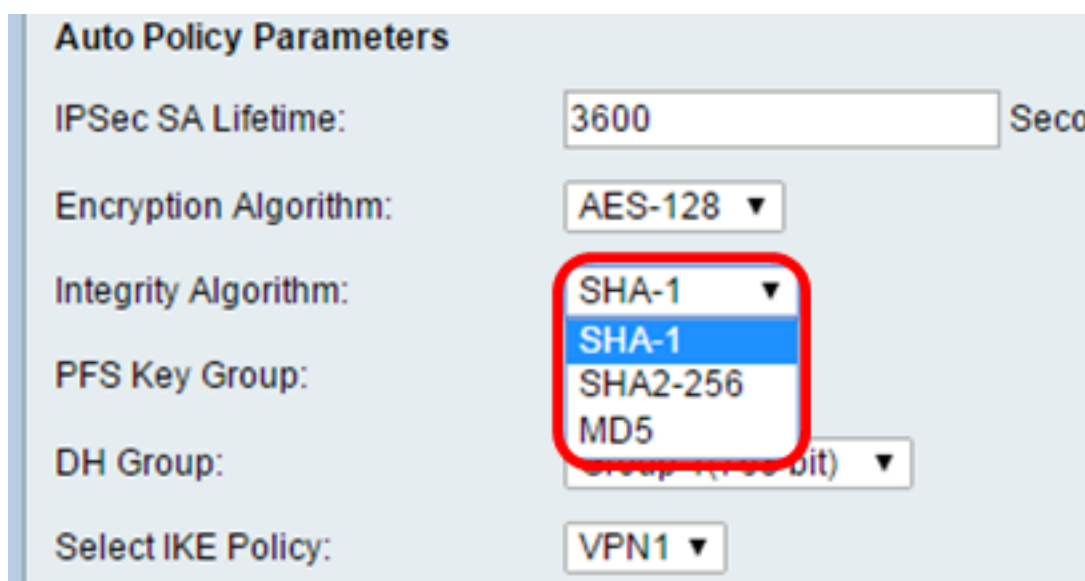
minder veilig dan AES-192 en AES-256.

- AES-192 — Gebruikt een 192-bits sleutel voor AES-encryptie. AES-192 is trager maar veiliger dan AES-128, en sneller maar minder veilig dan AES-256.
- AES-256 — Gebruikt een 256-bits sleutel voor AES-encryptie. AES-256 is langzamer maar veiliger dan AES-128 en AES-192.
- AESGCM — Advanced Encryption Standard Galois Counter Mode is een generische modus voor geauthenticeerde encryptie-blokalgoritmen. GCM-authenticatie maakt gebruik van operaties die bijzonder geschikt zijn voor efficiënte implementatie in hardware, waardoor het bijzonder aantrekkelijk is voor snelle implementaties of voor implementaties in een efficiënt en compact circuit.
- AESCCM — Advanced Encryption Standard Counter with CBC-MAC Mode is een algemene modus voor geauthenticeerde encryptie-blokalgoritmen. CCM is zeer geschikt voor gebruik in compacte software implementaties.



Stap 3. Kies een optie uit de vervolgkeuzelijst Integrity Algorithm. De opties zijn MD5, SHA-1 en SHA2-256.

Opmerking: In dit voorbeeld wordt SHA-1 gekozen.



Stap 4. Controleer het aanvinkvakje **Enable** in de PFS-sleutelgroep om Perfect Forward

Secrecy (PFS) in te schakelen. PFS verhoogt de VPN beveiliging, maar vertraagt de snelheid van verbinding.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seconds

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

Select IKE Policy: VPN1 ▼

View

Save Cancel Back

Stap 5. (Optioneel) Als u ervoor hebt gekozen om PFS in [Stap 4](#) in te schakelen, kiest u een DH-groep uit de vervolgkeuzelijst DH-groep. Hoe hoger het groepsnummer is, hoe beter de beveiliging.

Opmerking: In dit voorbeeld wordt Groep 1 gekozen.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seconds

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

Select IKE Policy: VPN1 ▼

Save Cancel Back

Stap 6. Kies in de vervolgkeuzelijst IKE-beleid selecteren welk IKE-beleid u voor het VPN-beleid wilt gebruiken.

Opmerking: In dit voorbeeld is slechts één IKE-beleid geconfigureerd, zodat slechts één beleid wordt weergegeven.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seconds (Ra

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

Select IKE Policy: **VPN1 ▼**

View

Save Cancel Back

Stap 7. Klik op **Opslaan**.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seconds (R

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

Select IKE Policy: VPN1 ▼

View

Save Cancel Back

Opmerking: De belangrijkste pagina voor geavanceerde VPN-instellingen wordt opnieuw weergegeven. Er moet een bevestigingsmelding verschijnen dat de configuratie-instellingen zijn opgeslagen.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Stap 8. Selecteer in de VPN Policy-tabel een selectievakje om een VPN te kiezen en klik op **Inschakelen**.

Opmerking: Het ingestelde VPN-beleid is standaard uitgeschakeld.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

Add Row

Edit

Delete

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Add Row

Edit

Enable

Disable

Delete

Save

Cancel

IPSec Connection Status

Stap 9. Klik op **Opslaan**.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

U moet nu met succes een VPN-beleid op uw RV130- of RV130W-router hebben geconfigureerd.

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.