

Geavanceerde VPN-instelling op de CVR100W VPN-router

Doel

Een Virtual Private Network (VPN) wordt gebruikt om endpoints op verschillende netwerken onderling te verbinden via een openbaar netwerk, zoals het internet. Deze functie biedt externe gebruikers die niet op een lokaal netwerk zitten, de mogelijkheid om verbinding te maken met het netwerk via het internet.

Dit artikel legt uit hoe u geavanceerde VPN op de CVR100W VPN-router kunt configureren. Raadpleeg voor de basisinstellingen van VPN het artikel [Basic VPN Setup op de CVR100W VPN-router](#).

Toepasselijke apparaten

- CVR100W VPN-router

Softwareversie

- 1.0.1.19

Geavanceerde VPN-instellingen

Initiële instellingen

Deze procedure legt uit hoe u de oorspronkelijke instellingen van de Advanced VPN-instelling kunt configureren.

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **VPN > Geavanceerde VPN-instelling**. De pagina *Geavanceerde VPN-instellingen* wordt geopend:

Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

IKE Policy Table

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						

Add Row Edit Delete

VPN Policy Table

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

Stap 2. (Optioneel) Om NAT-traversal (Network Address Translation) voor de VPN-verbinding in te schakelen, schakelt u het aankruisvakje **Enable** in het veld NAT Traversal in. NAT Traversal maakt het mogelijk een VPN-verbinding te maken tussen gateways die NAT

gebruiken. Kies deze optie als uw VPN-verbinding door een NAT-enabled gateway gaat.

Stap 3. (Optioneel) Controleer het aanvinkvakje **Enable** in het veld NETeuropa. Neteuropa-OS. Hiermee kunnen hosts met elkaar communiceren binnen een netwerk.

IKE-beleidsinstellingen

Internet Key Exchange (IKE) is een protocol dat wordt gebruikt om een beveiligde verbinding voor communicatie in een VPN op te zetten. Deze gevestigde beveiligde verbinding wordt een Security Association (SA) genoemd. Deze procedure legt uit hoe u een IKE-beleid voor de VPN-verbinding kunt configureren die voor de beveiliging moet worden gebruikt. Om een VPN goed te laten functioneren, moet het IKE-beleid voor beide eindpunten identiek zijn.

Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

IKE Policy Table

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
<input type="checkbox"/>	<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>				

VPN Policy Table

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

Stap 1. In de tabel IKE-beleid klikt u op **Rijen toevoegen** om een nieuw IKE-beleid te maken. De pagina *Geavanceerde VPN-instellingen* wijzigt:

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

Respondent Mode: Respondent
 Auto Manual

Local ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)
 Auto Manual

Remote ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)
 Auto Manual

Redundancy Remote ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

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

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

Stap 2. Voer in het veld Naam beleid een naam in voor het IKE-beleid.

Stap 3. Kies een optie uit de vervolgkeuzelijst Exchange Mode om te bepalen hoe het IKE-beleid werkt.

- Hoofdstroom — Met deze optie kan het IKE-beleid beter werken. Hij is langzamer dan agressief. Kies deze optie als een meer beveiligde VPN-verbinding nodig is.
- agressief — Met deze optie kan het IKE-beleid sneller werken maar is het minder veilig dan de hoofdmodus. Kies deze optie als er een snellere VPN-verbinding nodig is.

Stap 4. (optioneel) Controleer het vakje **respondent** om de modus voor respons in te schakelen. Als de responsmodus is ingeschakeld, kan de CVR100W VPN-router alleen het VPN-verzoek van het externe VPN-eindpunt ontvangen.

Stap 5. Klik in het veld Local ID op de gewenste radioknop om te identificeren hoe de lokale ID te specificeren.

- Auto — Aan deze optie wordt automatisch een lokale ID toegewezen.
- Handmatig - Deze optie wordt gebruikt om handmatig lokale ID toe te wijzen.

Stap 6. (Optioneel) Kies in de vervolgkeuzelijst Local ID de gewenste identificatiemethode voor het lokale netwerk.

- IP-adres - Deze optie identificeert het lokale netwerk met een openbaar IP-adres.
- FQDN - Deze optie gebruikt een Full Qualified Domain Name (FQDN) om het lokale netwerk te identificeren.

Stap 7. (Optioneel) Voer in het veld Local ID het IP-adres of de domeinnaam in. Het item is afhankelijk van de optie die in Stap 6 is gekozen.

Stap 8. Klik in het veld Remote-ID op de gewenste radioknop om de Remote-ID te specificeren.

- Auto — Deze optie wijst automatisch Remote-ID toe.
- Handmatig — Deze optie wordt gebruikt om handmatig Remote-ID toe te wijzen

Stap 9. (optioneel) Kies in de vervolgkeuzelijst Remote-ID de gewenste identificatiemethode voor het externe netwerk.

- IP-adres - Deze optie identificeert het externe netwerk via een openbaar IP-adres.
- FQDN - Deze optie gebruikt een Full Qualified Domain Name (FQDN) om het externe netwerk te identificeren.

Stap 10. (Optioneel) Voer in het veld Remote-ID het IP-adres of de domeinnaam in. Het item is afhankelijk van de optie die in Stap 9 is gekozen.

Stap 11. In het veld Remote-ID voor redundantie klikt u op de gewenste radioknop om de Remote-ID voor redundantie te specificeren. De Remote-ID van Redundantie is een alternatieve Remote-ID die wordt gebruikt om de VPN-tunnel in de externe gateway in te stellen.

- Auto — Deze optie wijst automatisch redundantie-ID toe.
- Handmatig — Deze optie wordt gebruikt om zelf een Remote-ID voor redundantie toe te wijzen.

Stap 12. (Optioneel) Kies in de vervolgkeuzelijst Redundantion Remote ID de gewenste identificatiemethode voor het redundantie-netwerk.

- IP-adres - Deze optie identificeert het externe netwerk van redundantie door een openbaar IP-adres.
- FQDN - Deze optie gebruikt een Full Qualified Domain Name (FQDN) om het afstandsnetwerk van redundantie te identificeren.

Stap 13. (Optioneel) Voer in het veld Remote-ID voor redundantie in het IP-adres of de domeinnaam. Het item is afhankelijk van de optie die in Stap 12 is gekozen.

IKE SA Parameters	
Encryption Algorithm:	AES-128 ▼
Authentication Algorithm:	SHA-1 ▼
Pre-Shared Key:	1234abcd
Diffie-Hellman (DH) Group:	Group1 (768 bit) ▼
SA-Lifetime:	3600 Seconds (Range: 30 - 86400, Default: 3600)
Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	10 Seconds (Range: 10 - 999, Default: 10)
DPD Timeout:	30 Seconds (Range: 30 - 1000, Default: 30)

Stap 14. Kies een optie om in de vervolgkeuzelijst Encryption Algorithm te onderhandelen met de Security Association (SA).

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelformaat voor gegevensencryptie. DES is verouderd en dient te worden gebruikt als één eindpunt alleen DES ondersteunt.
- 3DES - Triple Data Encryption Standard (3DES) voert DES drie keer uit maar varieert de sleutelgrootte van 168 bits tot 112 bits en van 112 bits tot 56 bits, afhankelijk van de ronde van DES die wordt uitgevoerd. 3DES is veiliger dan DES en AES.
- AES-128 — Advanced Encryption Standard met 128-bits toets (AES-128) gebruikt een 128-bits toets voor AES-encryptie. AES is sneller en veiliger dan DES. Sommige typen hardware maken het mogelijk 3DES sneller te gebruiken. AES-128 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 langzamer maar veiliger dan AES-128, en AES-192 is sneller maar minder veilig dan AES-256.
- AES-256 — AES-256 gebruikt een 256-bits toets voor AES-encryptie. AES-256 is langzamer maar veiliger dan AES-128 en AES-192.

Stap 15. Kies een optie uit de vervolgkeuzelijst Verificatiealgoritme om de VPN-header te authenticeren.

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

Stap 16. Voer in het veld Vooraf gedeelde sleutel een vooraf gedeelde sleutel in die het IKE-beleid gebruikt.

Stap 17. Kies in de vervolgkeuzelijst Diffie-Hellman (DH) groep de DH-groep waarvan het IKE wordt gebruikt. Organisatoren in een DH-groep kunnen sleutels uitwisselen zonder elkaar te kennen. Hoe hoger het aantal groepsbits, hoe veiliger de groep is.

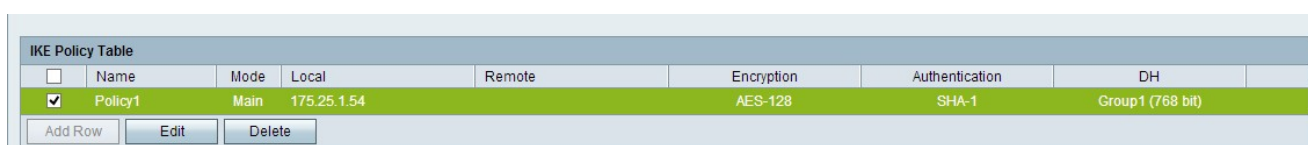
Stap 18. Voer in het veld SA-Lifetime in hoe lang (in seconden) de Security Association (SA) voor VPN duurt voordat de SA wordt vernieuwd.

Stap 19. (optioneel) Schakel DPD (Dead Peer Detection) in door het vakje **Enable** in het veld Detectie peer in te schakelen. DPD wordt gebruikt om IKE-peers te controleren of een peer niet meer werkt. DPD voorkomt de verspilling van netwerkbronnen op inactieve peers.

Stap 20. (Optioneel) Om aan te geven hoe vaak de peer voor activiteit is geselecteerd, specificeert u het tijdsinterval (in seconden) in het veld DPD Delay. Deze optie is beschikbaar als DPD in Stap 19 is ingeschakeld.

Stap 21. (Optioneel) Om aan te geven hoe lang u moet wachten voordat een inactieve peer wordt laten vallen, specificeert u hoe lang (in seconden) in het veld Time-out bij DPD. Deze optie is beschikbaar indien DPD is ingeschakeld in Stap 19.

Stap 2. Klik op **Opslaan**. De oorspronkelijke pagina *Geavanceerde VPN Setup* verschijnt opnieuw.



<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input checked="" type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

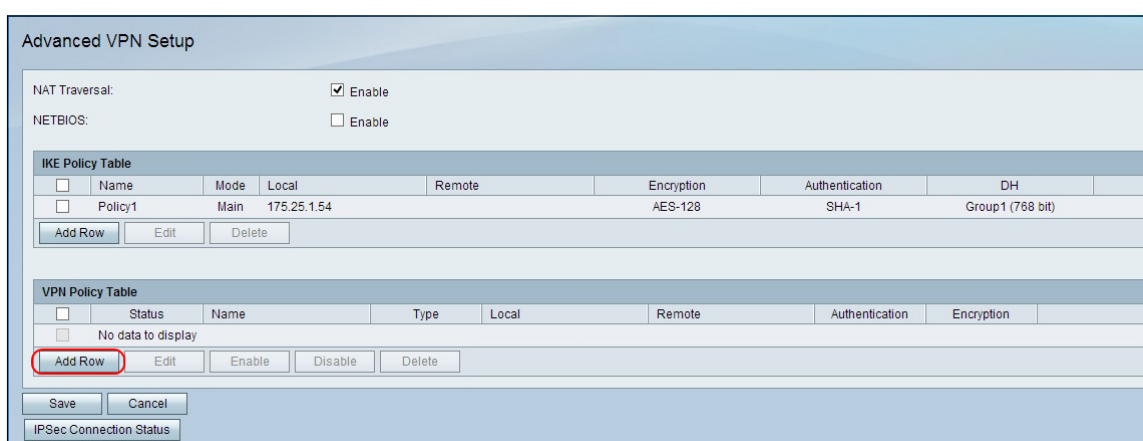
Add Row Edit Delete

Stap 23. (Optioneel) Om een IKE-beleid te bewerken in de tabel met IKE-beleid, schakelt u het vakje voor het beleid in. Klik vervolgens op **Bewerken**, de gewenste velden bewerken en klik op **Opslaan**.

Stap 24. (Optioneel) Om een IKE-beleid te verwijderen in de tabel met IKE-beleid, schakelt u het vakje voor het beleid in en klikt u op **Verwijderen**. Klik vervolgens op **Opslaan**.

VPN-beleidsinstellingen

Deze procedure legt uit hoe u een VPN-beleid kunt configureren voor de VPN-verbinding die u wilt gebruiken. Om een VPN goed te laten functioneren, moet het VPN-beleid voor beide eindpunten identiek zijn.



Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

Add Row Edit Delete

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

Stap 1. In de tabel VPN-beleid klikt u op **Weg toevoegen** om een nieuw VPN-beleid te maken. De pagina *Geavanceerde VPN-instellingen* wijzigt:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

(Hint: 1.2.3.4 or abc.com)

Rollback enable

Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type: ▼

Remote Endpoint: ▼

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

▼

(Hint: 1.2.3.4 or abc.com)

Rollback enable

Stap 2. Voer in het veld Naam beleid een naam in voor het VPN-beleid.

Stap 3. Selecteer in de vervolgkeuzelijst Beleidstype een optie om te bepalen hoe de instellingen van de VPN-tunnel worden gegenereerd.

- Handmatig beleid - Met deze optie kunt u de toetsen voor gegevensencryptie en integriteit configureren.
- Auto Policy — Deze optie maakt gebruik van een IKE-beleid voor gegevensintegriteit en coderingssleuteluitwisselingen.

Stap 4. Kies in de vervolgkeuzelijst Remote Endpoint een optie om aan te geven hoe u de Remote-ID handmatig wilt toewijzen.

- IP-adres - Deze optie identificeert het externe netwerk via een openbaar IP-adres.
- FQDN - Deze optie gebruikt een Full Qualified Domain Name (FQDN) om het externe netwerk te identificeren.

Stap 5. Voer in het veld tekst-ingang onder de vervolgkeuzelijst Remote Endpoint in het openbare IP-adres of de domeinnaam van het externe adres.

Stap 6. (Optioneel) Om redundantie in te schakelen, controleert u het aankruisvakje **Enable** in het veld Redundantie. De optie EINDpunt voor redundantie stelt de CVR100W VPN-router in staat om verbinding te maken met een VPN-eindpunt op back-up wanneer de primaire VPN-verbinding faalt.

Stap 7. (Optioneel) Om de redundantie-ID handmatig toe te wijzen, kiest u een optie uit de vervolgkeuzelijst Redundantie-endpoints.

- IP-adres - Deze optie identificeert het externe netwerk van redundantie door een openbaar IP-adres.
- FQDN - Deze optie gebruikt een Full Qualified Domain Name (FQDN) om het afstandsnetwerk van redundantie te identificeren.

Stap 8. (Optioneel) Om het redundantieadres in te voeren, in het veld tekst-ingang onder de vervolgkeuzelijst Redundantie-eindpunt, voert u ofwel het openbare IP-adres of de domeinnaam in.

Stap 9. (Optioneel) Schakel het terugdraaien in door het aanvinkvakje **Rollback in te schakelen**. Met deze optie kunt u automatisch overschakelen van de back-up VPN-verbinding naar de primaire VPN-verbinding wanneer de primaire VPN-verbinding na een storing is hersteld.

Local Traffic Selection		
Local IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="192.168.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.255.255.0"/>	(Hint: 255.255.255.0)
Remote Traffic Selection		
Remote IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="10.1.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.0.0.0"/>	(Hint: 255.255.255.0)

Stap 10. Kies een optie uit de vervolgkeuzelijst Local IP om te identificeren welke hosts invloed hebben op het beleid.

- Enkelvoudig - Deze optie gebruikt één host als het lokale VPN-verbindingspunt.
- Subnet - Deze optie gebruikt een net van het lokale netwerk als het lokale VPN-verbindingspunt.

Stap 11. In het veld IP-adres voert u het host- of subnetadres van het lokale net of de host in.

Stap 12. (Optioneel) Als de Subnetoptie in Stap 10 is geselecteerd, voer het subnetmasker voor het lokale subnetmasker in het veld Subnetmasker in.

Stap 13. Kies een optie uit de vervolgkeuzelijst Remote IP om te identificeren welke hosts invloed hebben op het beleid.

- Enkelvoudig - Deze optie gebruikt één host als het externe VPN-verbindingspunt.
- Subnet - Deze optie gebruikt een net van het externe netwerk als het externe VPN-verbindingspunt.

Stap 14. In het veld IP-adres voert u het host- of subnetadres van het externe subnetwerk of de host in.

Stap 15. (Optioneel) Als de Subnet optie in Stap 13 is geselecteerd, voer het subnetmasker voor het externe subnetmasker in het veld Subnetmasker in.

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="0xABCD"/>
SPI-Outgoing:	<input type="text" value="0x1234"/>
Encryption Algorithm:	<input type="text" value="AES-128"/> ▼
Key-In:	<input type="text" value="12345678ABCDE"/>
Key-Out:	<input type="text" value="12345678ABCDE"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/> ▼
Key-In:	<input type="text" value="12345678ABCD"/>
Key-Out:	<input type="text" value="12345678ABCD"/>

Opmerking: Als de optie Handmatig beleid in Stap 3 is geselecteerd, voert u Stap 16 tot en met Stap 23 uit. in het overige geval, overslaan naar [Stap 24](#).

Stap 16. Voer in het veld SPI-Inkomend in drie tot acht hexadecimale tekens in voor de tag Security Parameter Index (SPI) voor inkomend verkeer op de VPN-verbinding. De SPI-tag wordt gebruikt om het verkeer van de ene sessie te onderscheiden van het verkeer van andere sessies. De binnenkomende SPI aan één kant van de tunnel zou de uitgaande SPI van de andere kant van de tunnel moeten zijn.

Stap 17. In het veld SPI-Uitgaande voert u drie tot acht hexadecimale tekens in voor SPI-tag voor uitgaande verkeer op de VPN-verbinding. De SPI-tag wordt gebruikt om het verkeer van één sessie te onderscheiden van het verkeer van andere sessies. De vertrekkende SPI aan één kant van de tunnel zou de inkomende SPI aan de andere kant van de tunnel moeten zijn.

Stap 18. Kies een optie om in de vervolgkeuzelijst Encryption Algorithm te onderhandelen met de Security Association (SA).

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelmaat voor gegevensencryptie. DES is verouderd en dient te worden gebruikt als één eindpunt alleen DES ondersteunt.
- 3DES - Triple Data Encryption Standard (3DES) voert DES drie keer uit maar varieert de sleutelgrootte van 168 bits tot 112 bits en van 112 bits tot 56 bits, afhankelijk van de ronde van DES die wordt uitgevoerd. 3DES is veiliger dan DES en AES.
- AES-128 — Advanced Encryption Standard met 128-bits toets (AES-128) gebruikt een 128-bits toets voor AES-encryptie. AES is sneller en veiliger dan DES. Sommige typen hardware maken 3DES sneller mogelijk. AES-128 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 langzamer maar veiliger dan AES-128, en AES-192 is sneller maar minder veilig dan AES-256.
- AES-256 — AES-256 gebruikt een 256-bits toets voor AES-encryptie. AES-256 is langzamer maar veiliger dan AES-128 en AES-192.

Stap 19. Voer in het veld Key-In een sleutel in voor het inkomende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 18 is gekozen.

- DES gebruikt een 8-tekentoets.
- 3DES gebruikt een 24-tekensleutel.
- AES-128 gebruikt een 12-tekentoets.
- AES-192 maakt gebruik van een 24-tekens-toets.
- AES-256 gebruikt een 32-tekentoets.

Stap 20. Voer in het veld Uitbel een sleutel in voor het uittredende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 18 is geselecteerd. De sleutellengte is afhankelijk van het algoritme dat in Stap 18 is gekozen.

- DES gebruikt een 8-tekentoets.
- 3DES gebruikt een 24-tekensleutel.
- AES-128 gebruikt een 12-tekentoets.
- AES-192 maakt gebruik van een 24-tekens-toets.
- AES-256 gebruikt een 32-tekentoets.

Stap 21. Kies een optie uit de vervolgkeuzelijst Integrity Algorithm om de VPN-header voor echt te maken.

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

Stap 2. Voer in het veld Key-In een sleutel in voor het inkomende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 21 is geselecteerd.

- MD5 gebruikt een 16-teken.
- SHA-1 gebruikt een 20-tekensleutel.
- SHA2-256 gebruikt een 32-tekens-toets.

Stap 23. Voer in het veld Uitbel een sleutel in voor het uittredende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 21 is geselecteerd. De sleutellengte is afhankelijk van het algoritme dat in Stap 21 is gekozen.

- MD5 gebruikt een 16-teken.
- SHA-1 gebruikt een 20-tekensleutel.

- SHA2-256 gebruikt een 32-tekens-toets.

Auto Policy Parameters

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

Encryption Algorithm: ▼

Integrity Algorithm: ▼

PFS Key Group: Enable

▼

Select IKE Policy: ▼

Opmerking: Als u in Stap 3 voor Auto Policy hebt gekozen, voert u Stap 24 tot en met Stap 29 uit. in het overige geval, overslaan naar [Stap 31](#).

Stap 24. Voer in het veld SA-Lifetime in hoe lang de SA in seconden duurt voor de vernieuwing.

Stap 25. Kies een optie om in de vervolgkeuzelijst Encryption Algorithm te onderhandelen met de Security Association (SA).

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelformaat voor gegevensencryptie. DES is verouderd en dient te worden gebruikt als één eindpunt alleen DES ondersteunt.
- 3DES - Triple Data Encryption Standard (3DES) voert DES drie keer uit maar varieert de sleutelgrootte van 168 bits tot 112 bits en van 112 bits tot 56 bits, afhankelijk van de ronde van DES die wordt uitgevoerd. 3DES is veiliger dan DES en AES.
- AES-128 — Advanced Encryption Standard met 128-bits toets (AES-128) gebruikt een 128-bits toets voor AES-encryptie. AES is sneller en veiliger dan DES. Sommige typen hardware maken het mogelijk 3DES sneller te gebruiken. AES-128 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 langzamer maar veiliger dan AES-128, en AES-192 is sneller maar minder veilig dan AES-256.
- AES-256 — AES-256 gebruikt een 256-bits toets voor AES-encryptie. AES-256 is langzamer maar veiliger dan AES-128 en AES-192.

Stap 26. Kies een optie uit de vervolgkeuzelijst Integrity Algorithm om de VPN-header voor echt te maken.

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

veilig dan SHA2-256.

- SHA2-256 — Secure Hash Algorithm 2 (SHA2-256) gebruikt een 256-bits hashwaarde voor verificatie. SHA2-256 is langzamer maar beveiligd dan MD5 en SHA-1.

Stap 27. Controleer het aanvinkvakje **Enable** in het veld PFS-sleutelgroep om Perfect Forward Security (PFS) mogelijk te maken. PFS verhoogt de VPN-beveiliging, maar vertraagt de verbindingssnelheid.

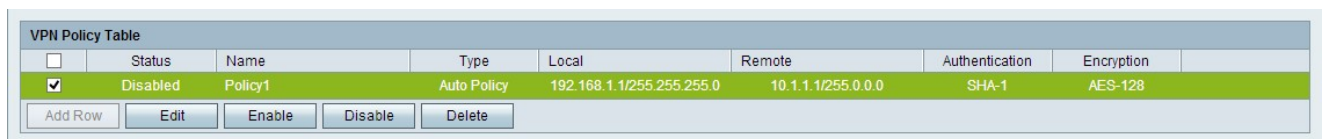
Stap 28. (Optioneel) Als u PFS in Stap 27 wilt inschakelen, kiest u een Diffie-Hellman (DH) groep om zich aan te sluiten bij de vervolgkeuzelijst onder het veld PFS Key Group. Hoe hoger het groepsnummer is, hoe veiliger de groep is.

Stap 29. Kies in de vervolgkeuzelijst IKE-beleid selecteren welk IKE-beleid u voor het VPN-beleid wilt gebruiken.

Stap 30. (Optioneel) Als u op **Weergave** klikt, wordt u gericht naar het IKE-configuratiescherm van de *Geavanceerde VPN*-pagina.

Stap 3. Klik op **Opslaan**. De oorspronkelijke pagina *Geavanceerde VPN Setup* verschijnt opnieuw.

Stap 3. Klik op **Opslaan**.



<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input checked="" type="checkbox"/>	Disabled	Policy1	Auto Policy	192.168.1.1/255.255.255.0	10.1.1.1/255.0.0.0	SHA-1	AES-128

Add Row Edit Enable Disable Delete

Stap 3. (Optioneel) Om een VPN-beleid te bewerken in de VPN-beleidstabel, schakelt u het aankruisvakje voor het beleid in. Klik vervolgens op **Bewerken**, de gewenste velden bewerken en klik op **Opslaan**.

Stap 34. (Optioneel) Om een VPN-beleid te verwijderen in de VPN-beleidstabel, controleert u het aankruisvakje voor het beleid, klikt u op **Verwijderen** en vervolgens klikt u op **Opslaan**.