

Configuratie van Advanced Virtual Private Network (VPN) Setup op RV110W-firewall

Doel

Virtual Private Network (VPN) gebruikt het openbare netwerk, of het internet, om een privaat netwerk op te zetten om veilig te communiceren. Een Internet Key Exchange (IKE) is een protocol dat beveiligde communicatie tussen twee netwerken tot stand brengt. Het wordt gebruikt om een sleutel vóór de verkeersstromen uit te wisselen, die authenticiteit voor beide uiteinden van de VPN-tunnel garandeert.

Beide extremen van VPN moeten hetzelfde VPN-beleid volgen om met elkaar te communiceren.

Het doel van dit document is te verklaren hoe u een IKE-profiel kunt toevoegen en VPN-beleid op de RV110W draadloze router kunt configureren.

Toepasselijke apparaten

- RV110W

Softwareversie

- 1.2.0.9

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.

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

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

Advanced VPN Setup

IKE Policy Table				
<input type="checkbox"/>	Name	Mode	Local	Remote
No data to display				
<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
No data to display				
<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 2. Klik op **Weg toevoegen** om een nieuw IKE-beleid te maken. De pagina *Geavanceerde VPN-instellingen* wordt geopend:

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode: ▼

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

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

Stap 3. In het veld *Beleidsnaam* typt u een naam voor het IKE-beleid om dit gemakkelijk te herkennen.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode: **Main** Aggressive

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

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

Stap 4. Kies een optie uit de vervolgkeuzelijst Wisselmodus:

- Maand — Hiermee kan het IKE-beleid beter maar langzamer werken dan agressieve. Kies deze optie als een meer beveiligde VPN-verbinding nodig is.
- Aggressief — Hiermee kan het IKE-beleid sneller maar minder goed werken dan de hoofdmodus. Kies deze optie als er een snellere VPN-verbinding nodig is.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

IKE SA Parameters

Encryption Algorithm:

- DES
- 3DES
- AES-128**
- AES-192
- AES-256

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

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

Dead Peer Detection: Enable

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

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

Stap 5. Kies een algoritme van de vervolgkeuzelijst *Encryption Algorithm*:

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelformaat voor gegevensencryptie. DES is verouderd en mag alleen 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. In het algemeen is AES ook sneller maar minder veilig dan 3DES, maar sommige soorten 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.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

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

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

Stap 6. Kies de gewenste verificatie in de vervolgkeuzelijst *Verificatiealgoritme*:

- 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 Functie 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 met een 256-bits hashwaarde (SHA2-256) gebruikt een 256-bits hashwaarde voor verificatie. SHA2-256 is langzamer maar beveiligd dan MD5 en SHA-1.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

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

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

Stap 7. Voer in het veld *Vooraf gedeelde sleutel* in die het IKE-beleid gebruikt.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

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

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

Stap 8. Kies in de vervolgkeuzelijst de *Diffie-Hellman (DH)* groep welke DH de IKE gebruikt. Organisatoren in een DH-groep kunnen sleutels uitwisselen zonder elkaar te kennen. Hoe hoger het aantal groepsbits is, hoe veiliger de groep is.

- Groep 1 - 768 bit - De laagste sterkte en de meest onveilige authenticatiegroep. Maar het kost

minder tijd om de IKE-toetsen te berekenen. Deze optie heeft de voorkeur wanneer de snelheid van het netwerk laag is.

- Groep 2 - 1024 bit - De hogere sterktesleutel en een veiliger authenticatiegroep. Maar het heeft wat tijd nodig om de IKE-toetsen te berekenen.
- Groep 5 - 1536 bit - vertegenwoordigt de hoogste sterktesleutel en de meest beveiligde authenticatiegroep. Het heeft meer tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk hoog is.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

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

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

Stap 9. Voer in hoe lang (in seconden) een SA voor VPN duurt voordat de SA in het *SA-Lifetime* veld wordt vernieuwd.

Stap 10. (Optioneel) Controleer het aanvinkvakje **Enable** in het veld *Dead Peer Detectie* om detectie van dode peer in te schakelen. Deed Peer Detectie controleert IKE-peers om te zien of een peer niet meer werkt. Dead Peer Detectie voorkomt het verspillen van netwerkbronnen aan inactieve peers.

Stap 11. (Optioneel) Als u Deed Peer Detection in Stap 9 hebt ingeschakeld, specificeert u hoe vaak (in seconden) de peer wordt gecontroleerd op activiteit in het veld *Deed Peer Delay*.

Stap 12. (Optioneel) Als u Deed Peer Detectie in Stap 9 hebt ingeschakeld, specificeert u hoeveel seconden u wilt wachten voordat een inactieve peer wordt verbroken in het veld Time-out bij detectie van peer.

Stap 13. Klik op **Save** om alle instellingen toe te passen.

VPN-beleidsconfiguratie

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **VPN >Advanced VPN**. De


pagina *Geavanceerde VPN Setup* wordt geopend:

Advanced VPN Setup

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

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

Advanced VPN Setup

 Configuration settings have been saved successfully

<input type="checkbox"/>	Name	Mode	Local	Remote
<input type="checkbox"/>	policy1	Aggressive		

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

Stap 2. Klik op **Add Row** in de *VPN-beleidstabel*. Het venster *Advanced VPN Policy Setup* verschijnt:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

VPN-beleidsconfiguratie toevoegen/bewerken



Advanced VPN Setup

Add / Edit VPN Policy Configuration

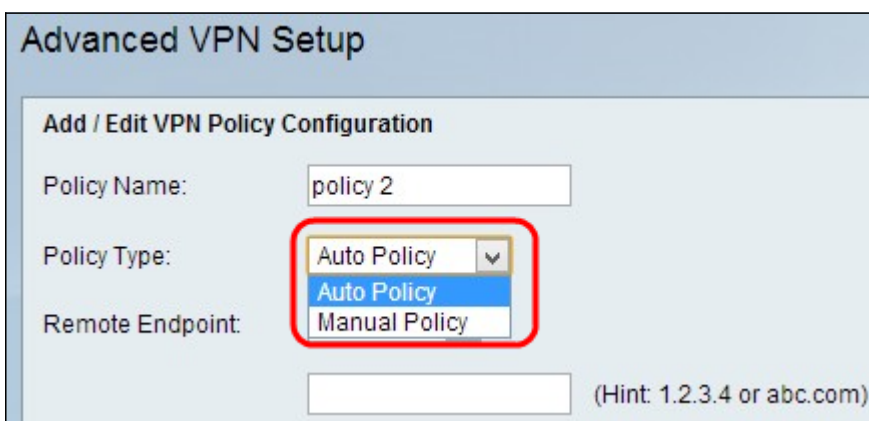
Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Stap 1. Voer een unieke naam voor het beleid in het veld *Beleidsnaam* in om dit gemakkelijk te herkennen.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

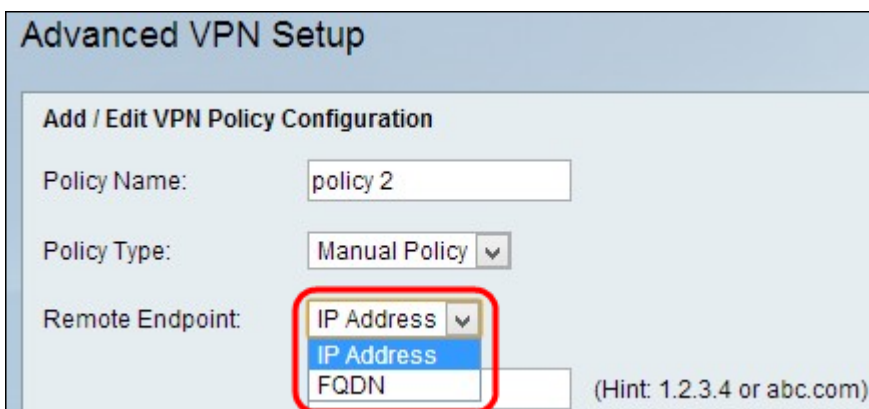
Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Stap 2. Kies het juiste beleidstype in de vervolgkeuzelijst *Beleidstype*.

- Automatisch beleid - De parameters kunnen automatisch worden ingesteld. In dit geval is, naast het beleid, het vereist dat het IKE (Internet Key Exchange)-protocol tussen de twee VPN-endpoints onderhandelt.
- Handmatig beleid - In dit geval worden alle instellingen die instellingen voor de toetsen voor de VPN-tunnel omvatten, handmatig ingevoerd voor elk eindpunt.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

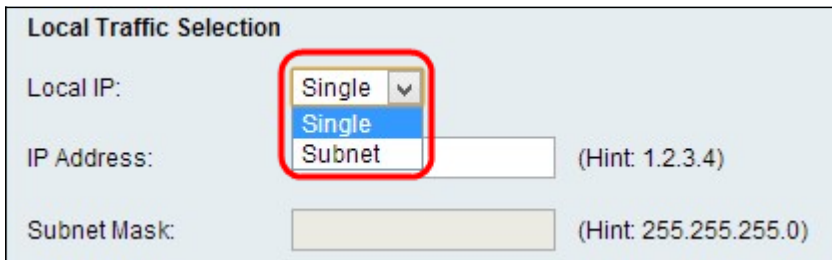
(Hint: 1.2.3.4 or abc.com)

Stap 3. Kies het type IP-identificator dat de gateway op het externe eindpunt identificeert in de vervolgkeuzelijst *Remote Endpoint*.

- IP-adres - IP-adres van de gateway op het externe eindpunt. Als u deze optie kiest, voert u het IP-adres in het veld in.
- FQDN (Full Qualified Domain Name) - Voer de Full Qualified Domain Name in van de gateway

op het verre eindpunt. Als u deze optie kiest, voer u de volledig gekwalificeerde domeinnaam in het daarvoor bestemde veld in.

Selectie lokaal verkeer



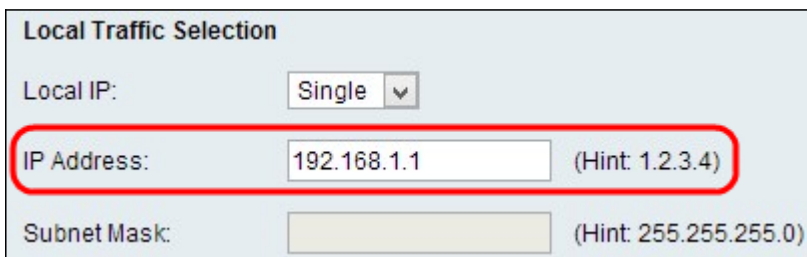
Local Traffic Selection

Local IP: (Hint: 1.2.3.4)

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Stap 1. Kies het type id dat u voor het eindpunt wilt instellen in de vervolgkeuzelijst *Local IP*.



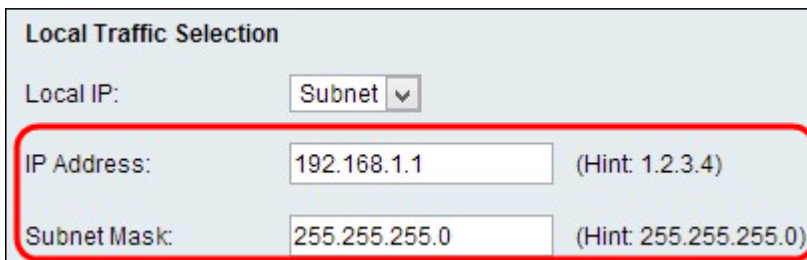
Local Traffic Selection

Local IP: (Hint: 1.2.3.4)

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

- Enkelvoudig — Dit beperkt het beleid tot één gastheer. Als u deze optie kiest, voert u het IP-adres in het veld *IP-adres in*.



Local Traffic Selection

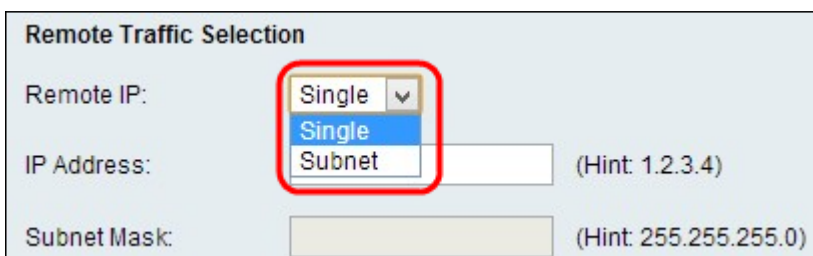
Local IP: (Hint: 1.2.3.4)

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

- Subnet - Dit is een masker dat de grenzen van een IP definieert. Dit staat slechts hosts van gespecificeerd type toe om met VPN te verbinden. Om aan te sluiten op VPN wordt een computer geselecteerd door een logische en operationele modus. Een computer is geselecteerd als de IP binnen hetzelfde bereik valt als vereist. Als u deze optie kiest, voert u het IP-adres en het subnetveld in op het IP-adres en het subnetveld.

Selectie van RemoteTraffic



Remote Traffic Selection

Remote IP: (Hint: 1.2.3.4)

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Stap 1. Kies het type id dat u voor het eindpunt wilt instellen in de vervolgkeuzelijst *Local IP*:

Remote Traffic Selection

Remote IP: ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

- Enkelvoudig — Dit beperkt het beleid tot één gastheer. Als u deze optie kiest, voert u het IP-adres in het veld *IP-adres in*.

Remote Traffic Selection

Remote IP: ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

- Subnet - Dit is een masker dat de grenzen van een IP definieert. Dit staat slechts hosts van gespecificeerd type toe om met VPN te verbinden. Om aan te sluiten op VPN wordt een computer geselecteerd door een logische en operationele modus. Een computer is geselecteerd als de IP binnen hetzelfde bereik valt als vereist. Als u deze optie kiest, voert u het IP-adres en het subnetveld in op het IP-adres en het subnetveld.

Handmatige beleidsparameters

Om Handmatige beleidsparameters te configureren kiest u **Handmatig beleid** uit de vervolgkeuzelijst *Beleidsstypen* in Stap 2 van de sectie *VPN-beleidsconfiguratie toevoegen/bewerken*.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm: ▼

Key-In:

Key-Out:

Integrity Algorithm: ▼

Key-In:

Key-Out:

Stap 1. Voer een hexadecimale waarde in tussen 3 en 8 in het veld *SPI-inkomende*. Stateful Packet Inspection (SPI) is een technologie die diepgaande pakketinspectie wordt genoemd. SPI implementeert een aantal beveiligingsfuncties die uw computernetwerk veilig helpen houden. De SPI-inkomende waarde komt overeen met de SPI-Uitgang van het vorige apparaat. Elke waarde is acceptabel, mits het externe VPN-eindpunt dezelfde waarde heeft in zijn *SPI-Uitgaande* veld.

Stap 2. Voer een hexadecimale waarde in tussen 3 en 8 in het veld *SPI-Uitvoer*.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

- 3DES
- DES
- AES-128
- AES-192
- AES-256

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Stap 3. Kies het juiste encryptie-algoritme in de vervolgkeuzelijst Encryption Algorithm.

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelformaat voor gegevensencryptie. DES is verouderd en mag alleen 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 op basis 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. In het algemeen is AES ook sneller maar minder veilig dan 3DES, maar sommige soorten 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.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

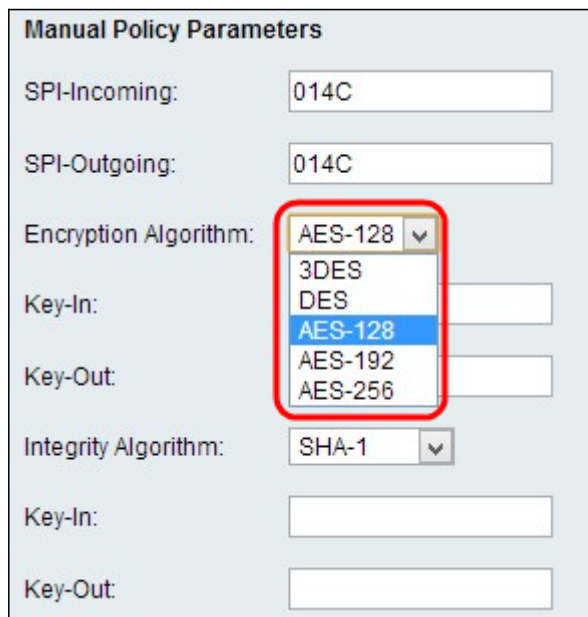
Key-In:

Key-Out:

Stap 4. Voer de coderingssleutel van het inkomende beleid in het veld *Key-In in*. De lengte van de

toets is afhankelijk van het algoritme dat in Stap 3 is gekozen.

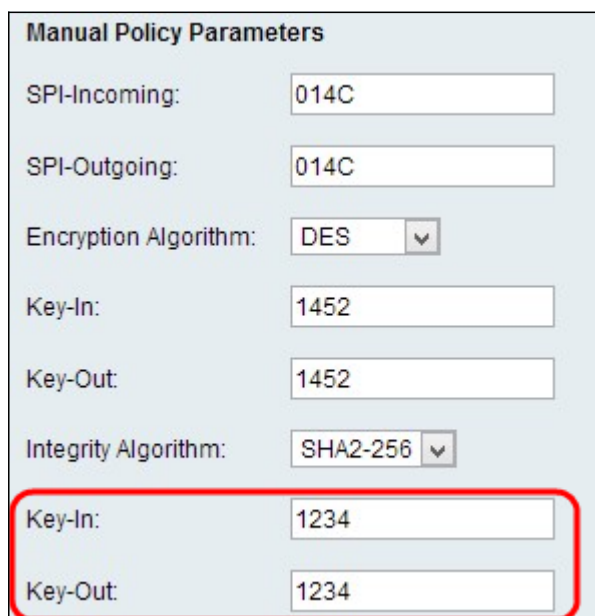
Stap 5. Voer de coderingssleutel van het uitgaande beleid in het veld *Key-Out*.



The screenshot shows the 'Manual Policy Parameters' form. The 'Encryption Algorithm' dropdown menu is open, showing options: AES-128 (selected), 3DES, DES, AES-192, and AES-256. Other fields include SPI-Incoming: 014C, SPI-Outgoing: 014C, Key-In: (empty), Key-Out: (empty), Integrity Algorithm: SHA-1, and another set of Key-In and Key-Out fields (both empty).

Stap 6. Kies het juiste integriteitsalgoritme uit de vervolgkeuzelijst *Integrity Algorithm*. Dit algoritme zal de integriteit van de gegevens verifiëren:

- MD5 — Dit algoritme specificeert de sleutellengte tot 16 tekens. Message-Digest Algorithm 5 (MD5) is geen botsingsbestendig en is geschikt voor toepassingen zoals SSL-certificaten of digitale handtekeningen die op dit bezit vertrouwen. MD5 comprimeert elke bytestroom tot een waarde van 128 bit, maar SHA comprimeert deze tot een waarde van 160 bit. MD5 is iets goedkoper om te berekenen, maar MD5 is een oudere versie van hash-algoritme en is kwetsbaar voor botsingsaanvallen.
- SHA1 — Secure Hash Algorithm, versie 1 (SHA1) is een 160-bits hashfunctie die veiliger is dan MD5, maar u hoeft er meer tijd voor te berekenen.
- SHA2-256 — Dit algoritme specificeert de sleutellengte tot 32 tekens.



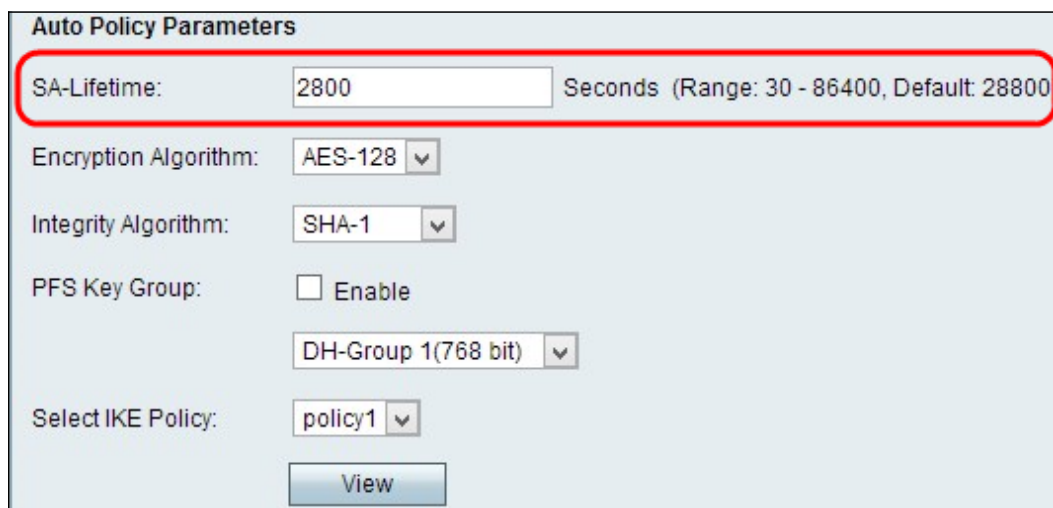
The screenshot shows the 'Manual Policy Parameters' form. The 'Integrity Algorithm' dropdown menu is set to SHA2-256. The 'Key-In' and 'Key-Out' fields are both set to 1234. Other fields include SPI-Incoming: 014C, SPI-Outgoing: 014C, Encryption Algorithm: DES, and another set of Key-In and Key-Out fields (both empty).

Stap 7. Voer de integriteitstoets in (voor ESP met integratiemodus) voor het inkomende beleid. De lengte van de toets is afhankelijk van het algoritme dat in Stap 6 is gekozen.

Stap 8. Voer de integriteitstoets van het uitgaande beleid in het veld Key-Out in. De verbinding van VPN is opstelling voor uitgaand aan binnenkomend, daarom moeten de uitgaande sleutels van het ene eind aan de inkomende sleutels op het andere eind aan.

Opmerking: SPI-inkomende en uitgaande, Encryption Algorithm, Integrity Algorithm, en Keys moeten aan het andere uiteinde van VPN-tunnel voldoen om een succesvolle verbinding te kunnen maken.

Auto beleidsparameters



Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group: Enable
DH-Group 1(768 bit)

Select IKE Policy: policy1

View

Stap 1. Voer de duur van de beveiligingsinstelling in in seconden in het veld Tijd SA. De SA-levensduur is wanneer elke sleutel zijn levensduur heeft bereikt, wordt elke geassocieerde SA automatisch heronderhandeld.



Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group: Enable
DH-Group 1(768 bit)

Select IKE Policy: policy1

View

Stap 2. Kies het juiste Encryptiealgoritme in de vervolgkeuzelijst Encryption Algorithm:

- DES - Data Encryption Standard (DES) gebruikt een 56-bits sleutelformaat voor gegevensencryptie. DES is verouderd en mag alleen 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 op basis 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. In het algemeen is AES ook sneller maar minder veilig dan 3DES, maar sommige soorten 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.

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm: (Dropdown menu open showing: SHA-1, SHA-1, SHA2-256, MD5)

PFS Key Group:

Select IKE Policy:

Stap 3. Kies het juiste Integrity Algorithm in de vervolgkeuzelijst Integrity Algorithm. Dit algoritme verifieert de integriteit van de gegevens.

- MD5 — Dit algoritme specificeert de sleutellengte tot 16 tekens. Message-Digest Algorithm 5 (MD5) is geen botsingsbestendig en is geschikt voor toepassingen zoals SSL-certificaten of digitale handtekeningen die op dit bezit vertrouwen. MD5 comprimeert elke bytestroom tot een waarde van 128 bit, maar SHA comprimeert deze tot een waarde van 160 bit. MD5 is iets goedkoper om te berekenen, maar MD5 is een oudere versie van hash-algoritme en is kwetsbaar voor botsingsaanvallen.
- SHA1 — Secure Hash Algorithm, versie 1 (SHA1) is een 160-bits hashfunctie die veiliger is dan MD5, maar u hoeft er meer tijd voor te berekenen.
- SHA2-256 — Dit algoritme specificeert de sleutellengte tot 32 tekens.

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Stap 4. (Optioneel) Controleer het aanvinkvakje **Enable** in het veld *PFS Key Group* om Perfect Forward Security mogelijk te maken, wat de beveiliging moet verbeteren.

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

- DH-Group 1(768 bit)
- DH-Group 2(1024 bit)
- DH-Group 5(1536 bit)

Stap 5. Als u in Stap 4 **Schakel** in, kiest u de juiste Diffie-Hellman sleuteluitwisseling uit de vervolgkeuzelijst *PFS Key Group*.

- Groep 1 - 768 bit - vertegenwoordigt de laagste sterkte en de meest onveilige echtheidsgroep. Maar het heeft minder tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk laag is.
- Groep 2 - 1024 bit - vertegenwoordigt een hogere sterkte en een veiliger authenticatiegroep. Maar het heeft wat tijd nodig om de IKE-toetsen te berekenen.
- Groep 5 - 1536 bit - vertegenwoordigt de hoogste sterktesleutel en de meest beveiligde authenticatiegroep. Het heeft meer tijd nodig om de IKE-toetsen te berekenen. Het is de voorkeur dat de snelheid van het netwerk hoog is.

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

- policy1
- policy1

Stap 6. Kies het juiste IKE-beleid in de vervolgkeuzelijst *IKE-beleid selecteren*. 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. Om een VPN goed te laten functioneren, moet het IKE-beleid voor beide eindpunten identiek zijn.

Stap 7. Klik op **Save** om alle instellingen toe te passen.

Opmerking: SA - Lifetime, Encryption Algorithm, Integrity Algorithm, PFS Key Group en het IKE Policy moeten op het andere uiteinde van VPN-tunnel hetzelfde zijn voor een succesvolle verbinding.

Als u meer artikelen op de RV110W wilt bekijken, klikt u [hier](#).