Configuratie van een profiel van het Protocol van Internet Protocol (IPSec) op een RV34x Series router

Doel

Internet Protocol Security (IPSec) biedt beveiligde tunnels tussen twee peers, zoals twee routers. Packets die als gevoelig worden beschouwd en moeten door deze beveiligde tunnels worden verzonden, evenals de parameters die moeten worden gebruikt om deze gevoelige pakketten te beschermen, moeten worden gedefinieerd door de kenmerken van deze tunnels te specificeren. Wanneer IPsec peer zo'n gevoelig pakket ziet, stelt het de juiste beveiligde tunnel in en stuurt het pakket door deze tunnel naar de externe peer.

Wanneer IPsec in een firewall of een router wordt geïmplementeerd, biedt het sterke beveiliging die kan worden toegepast op alle verkeer dat de perimeter oversteekt. Het verkeer binnen een bedrijf of een werkgroep heeft geen invloed op de overheadkosten van de veiligheidsgerelateerde verwerking.

Het doel van dit document is u te tonen hoe u het IPSec Profile op een RV34x Series router kunt configureren.

Toepasselijke apparaten

- RV34x Series

Softwareversie

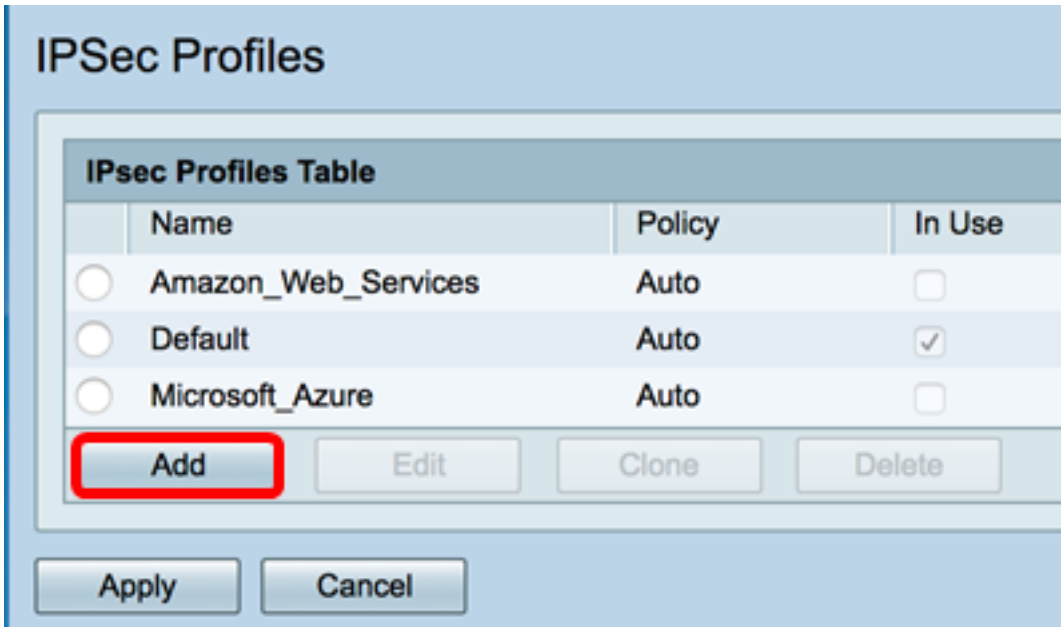
- 1.0.1.16

IPsec-profiel configureren

Een IPSec-profiel maken

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van de router en kies **VPN > IPSec-profielen**.

Stap 2. De tabel met IPsec-profielen toont de bestaande profielen. Klik op **Add** om een nieuw profiel te maken.



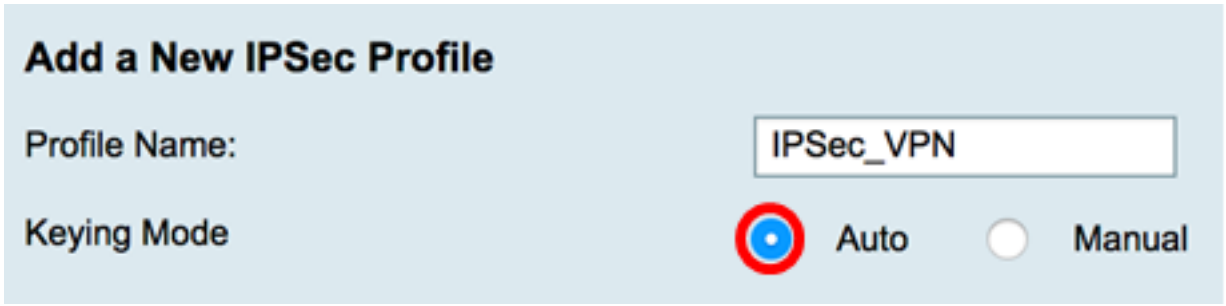
Stap 3. Maak een naam voor het profiel in het veld *Profile Name*. De profielnaam mag alleen alfanumerieke tekens en een underscore (_) voor speciale tekens bevatten.

Opmerking: In dit voorbeeld wordt IPSec_VPN gebruikt als de naam van het IPSec-profiel.

Stap 4. Klik op een radioknop om de belangrijkste uitwisselingsmethode te bepalen het profiel zal gebruiken om authentiek te verklaren. De opties zijn:

- Auto — Beleidsparameters worden automatisch ingesteld. Deze optie gebruikt een beleid voor de uitwisseling van gegevens (Internet Key Exchange, IKE) en de uitwisseling van encryptiesleutels. Als dit geselecteerd is, worden de configuratie instellingen onder het gebied Auto Policy parameters ingeschakeld. Klik hier om de automatische instellingen te configureren.
- Handmatig - Met deze optie kunt u de toetsen voor gegevensencryptie en integriteit voor de VPN-tunnel (Virtual Private Network) handmatig configureren. Als dit wordt geselecteerd, worden de configuratie instellingen onder het gebied Handmatige beleidsparameters ingeschakeld. Klik hier om de handmatige instellingen te configureren.

Opmerking: Auto is bijvoorbeeld geselecteerd.



De automatische instellingen configureren

Stap 1. Selecteer in het gebied Fase 1 Opties de juiste Diffie-Hellman (DH) groep die met de toets in Fase 1 moet worden gebruikt in de vervolgkeuzelijst DH Group. Diffie-Hellman is een cryptografisch sleuteluitwisselingsprotocol dat wordt gebruikt in de verbinding om vooraf gedeelde sleutelgroepen uit te wisselen. De sterkte van het algoritme wordt bepaald door bits. De opties zijn:

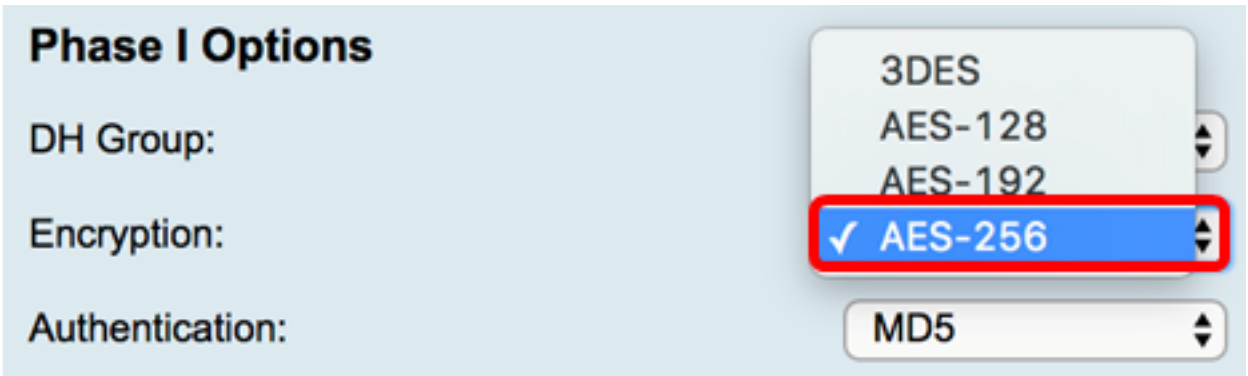
- Group2 - 1024 bit - compileert de toets trager, maar is veiliger dan Group1.
- Groep 5 - 1536-bits - compileert de sleutel het traagste, maar is het veiligst.

Opmerking: In dit voorbeeld wordt het bit Group2-1024 gekozen.

Stap 2. Kies in de vervolgkeuzelijst Encryptie de juiste encryptie-methode om de Encapsulation Security Payload (ESP) en Internet Security Association en Key Management Protocol (ISAKMP) te versleutelen en decrypteren. De opties zijn:

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

Opmerking: AES is de standaardmethode voor codering via DES en 3DES voor betere prestaties en beveiliging. Door de AES-toets te verlengen, wordt de beveiliging verbeterd met een vervolgkeuzemogelijkheid. Voor dit voorbeeld wordt AES-256 gekozen.



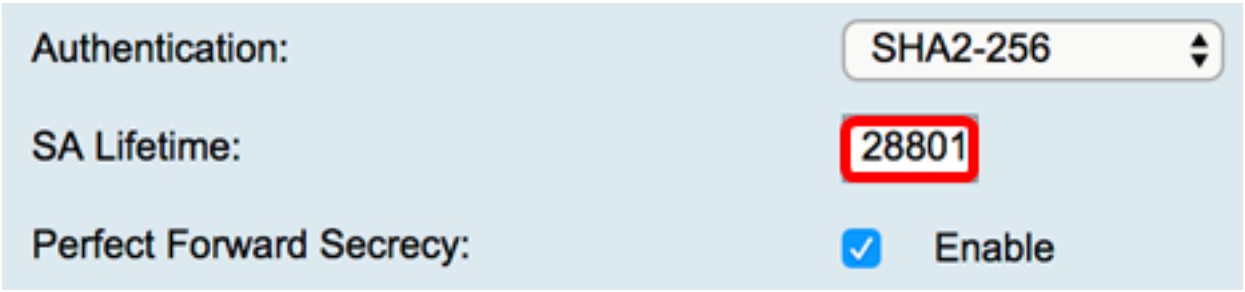
Stap 3. Kies in het vervolgkeuzemenu Verificatie een verificatiemethode die bepaalt hoe ESP en ISAKMP geauthentiseerd zijn. De opties zijn:

- MD5 — Message Digest-algoritme heeft een hashwaarde van 128 bits.
- SHA-1 — Secure Hash Algorithm heeft een 160-bits hashwaarde.
- SHA2-256 — Secure Hash Algorithm met een hashwaarde van 256 bits.

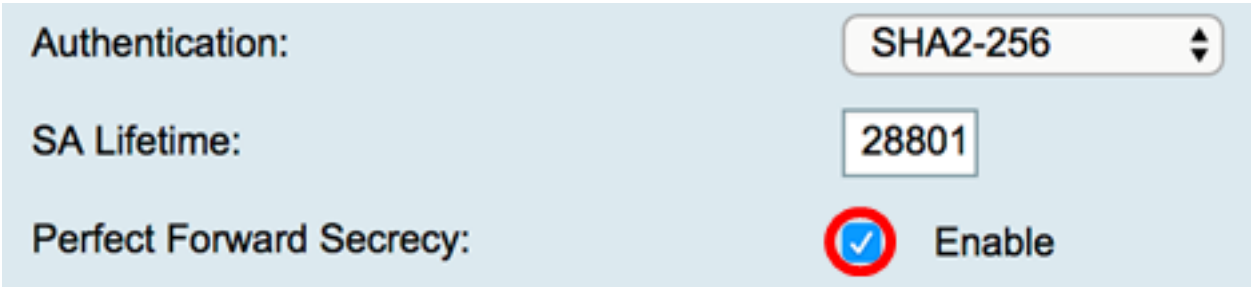
Opmerking: MD5 en SHA zijn beide cryptografische hashfuncties. Ze nemen een stuk gegevens, compacte ze en maken een unieke hexadecimale output die doorgaans niet reproduceerbaar is. In dit voorbeeld wordt SHA2-256 gekozen.

Stap 4. In het veld *SA Lifetime* voert u een waarde in die varieert tussen 120 en 86400. Dit is de duur van de tijd dat de Internet Key Exchange (IKE) Security Association (SA) actief blijft in deze fase. De standaardwaarde is 28800.

Opmerking: In dit voorbeeld wordt 28801 gebruikt.



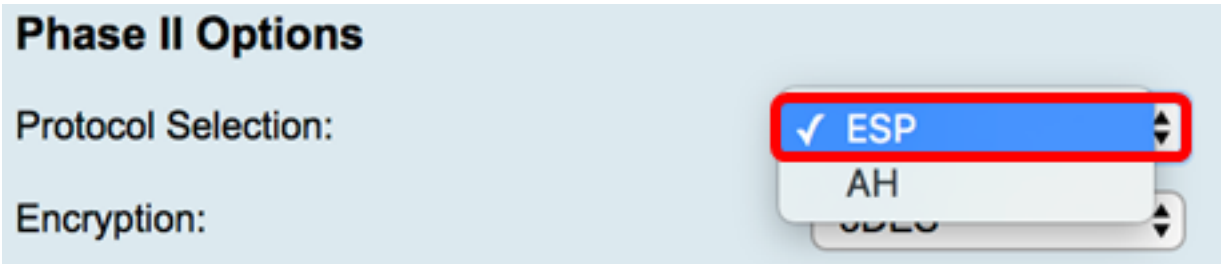
Stap 5. (Optioneel) Controleer het aankruisvakje **Perfect Forward Security** inschakelen om een nieuwe toets voor IPSec traffic encryptie en verificatie te genereren.



Stap 6. Kies in het vervolgkeuzemenu Protocol-selectie in het gebied Fase II Opties een protocoltype dat moet worden toegepast op de tweede fase van de onderhandelingen. De opties zijn:

- ESP — Als dit geselecteerd is, sla dan over naar Stap 7 om een coderingsmethode te kiezen voor de versleuteling en decryptie van de ESP-pakketten. Een beveiligingsprotocol dat diensten voor dataprivacy en optionele gegevensverificatie biedt en diensten tegen terugspelen. ESP bevat de te beschermen gegevens.

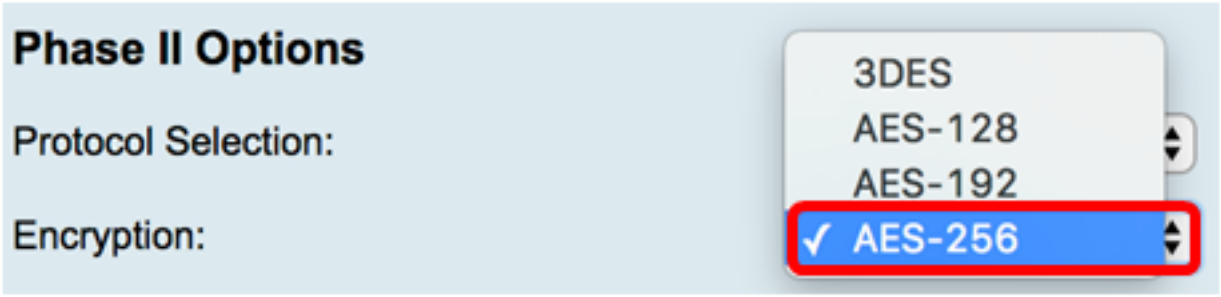
- AH — Verificatieheader (AH) is een beveiligingsprotocol dat gegevensverificatie en optionele antireplay-services biedt. AH is ingesloten in de te beschermen gegevens (een volledig IP-datagram). Naar Stap 8 indien dit is geselecteerd.



Stap 7 . Als ESP in Stap 6 is geselecteerd, kiest u de juiste encryptie-methode om ESP en ISAKMP te versleutelen en te decrypteren in de vervolgkeuzelijst Encryptie. De opties zijn:

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

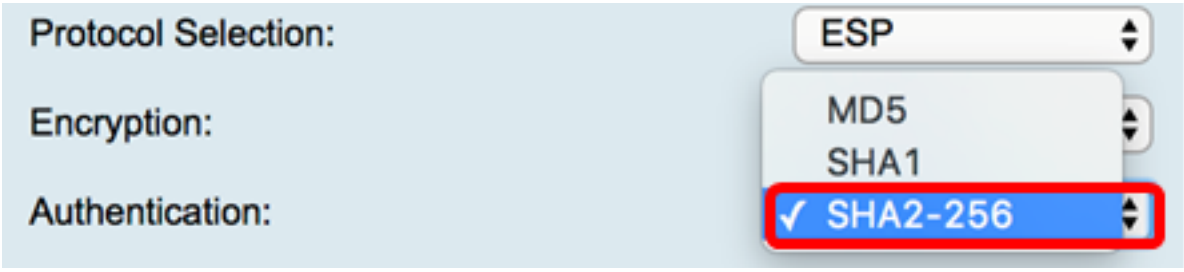
Opmerking: In dit voorbeeld wordt AES-256 gekozen.



Stap 8. Kies in het vervolgkeuzemenu Verificatie een authenticatiemethode die bepaalt hoe ESP en ISAKMP geauthentiseerd zijn. De opties zijn:

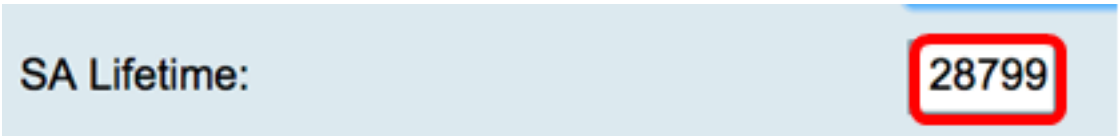
- MD5 — Message Digest-algoritme heeft een hashwaarde van 128 bits.
- SHA-1 — Secure Hash Algorithm heeft een 160-bits hashwaarde.
- SHA2-256 — Secure Hash Algorithm met een hashwaarde van 256 bits.

Opmerking: In dit voorbeeld wordt SHA2-256 gebruikt.



Stap 9. In het veld *SA Liftime* voert u een waarde in tussen 120 en 2800. Dit is de duur van de tijd dat de IKE SA in deze fase actief zal blijven. De standaardwaarde is 3600.

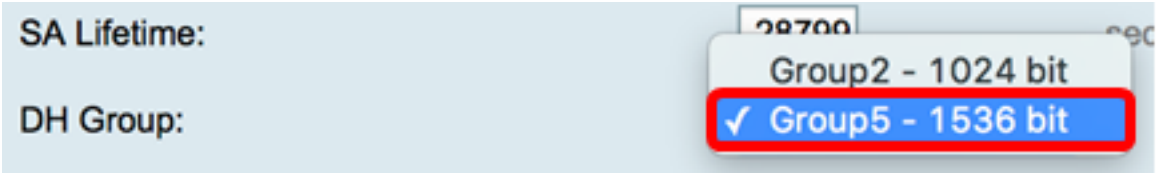
Opmerking: In dit voorbeeld wordt 28799 gebruikt.

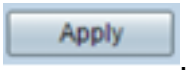


Stap 10. Kies in de vervolgkeuzelijst DH Group de juiste Diffie-Hellman (DH) groep die met de toets in fase 2 moet worden gebruikt. De opties zijn:

- Group2 - 1024 bit - compileert de toets trager, maar is veiliger dan Group1.
- Groep 5 - 1536 bit - compileert de toets de traagste, maar is de best beveiligde.

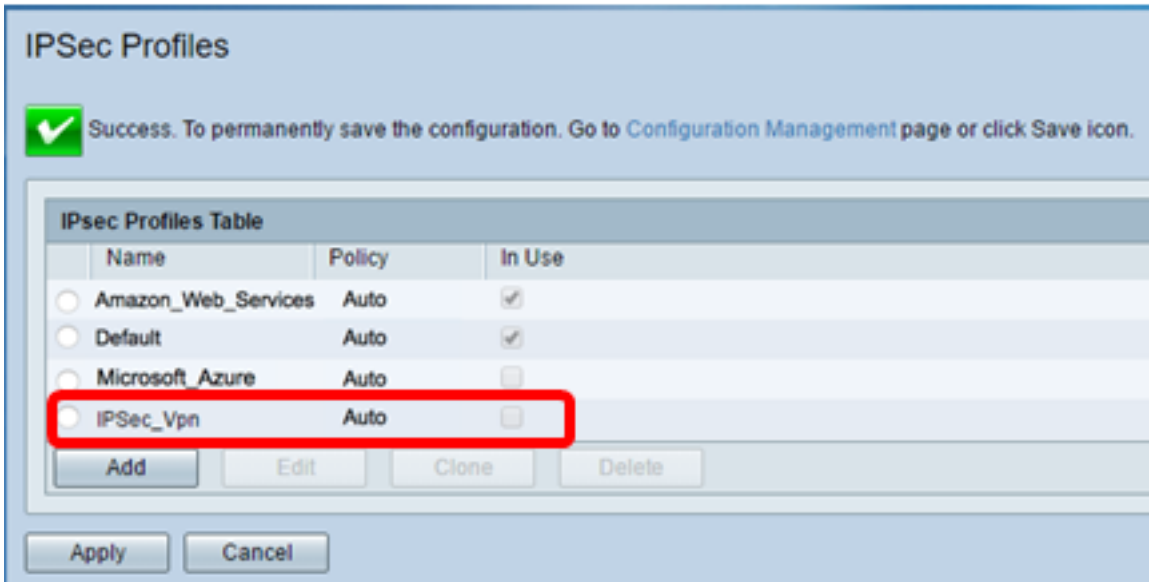
Opmerking: In dit voorbeeld wordt de bit Group5 - 1536 gekozen.



Stap 1. Klik op 

.

Opmerking: U wordt teruggebracht naar de tabel met IPSec-profielen en het nieuwe IPSec-profiel moet nu worden weergegeven.



Stap 12. (Optioneel) Ga om de configuratie permanent op te slaan naar de pagina Configuratie kopiëren/opslaan of klik op het 

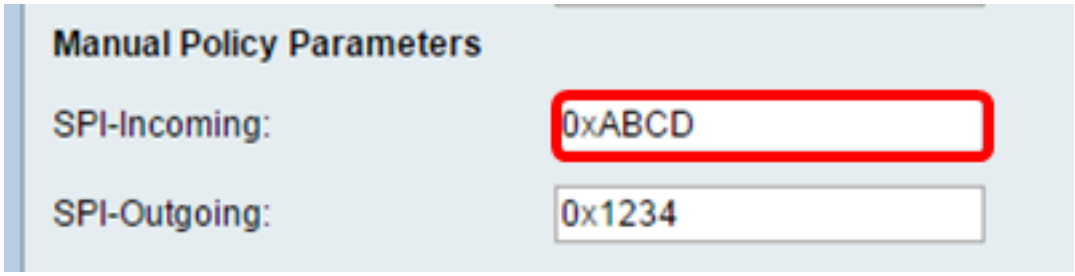
pictogram in het bovenste gedeelte van de pagina.

U hebt nu een automatisch IPSec profiel op een RV34x Series router ingesteld.

De handmatige instellingen configureren

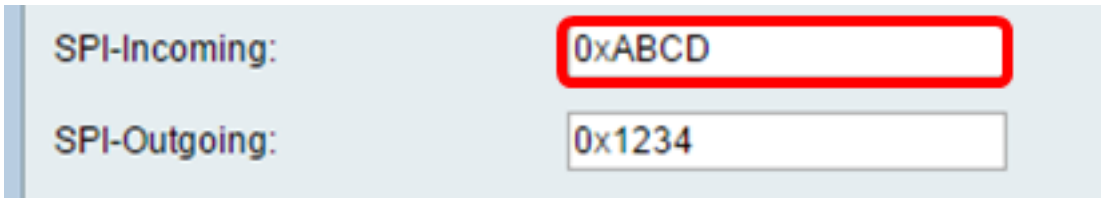
Stap 1. Voer in het veld *SPI-inkomende* veld een hexadecimaal getal in dat varieert van 100 tot FFFFF voor de tag Security Parameter Index (SPI) voor inkomend verkeer op de VPN-verbinding. De SPI-tag wordt gebruikt om het verkeer van de ene sessie te onderscheiden van het verkeer van andere sessies.

Opmerking: Bij dit voorbeeld wordt 0xABCD gebruikt.



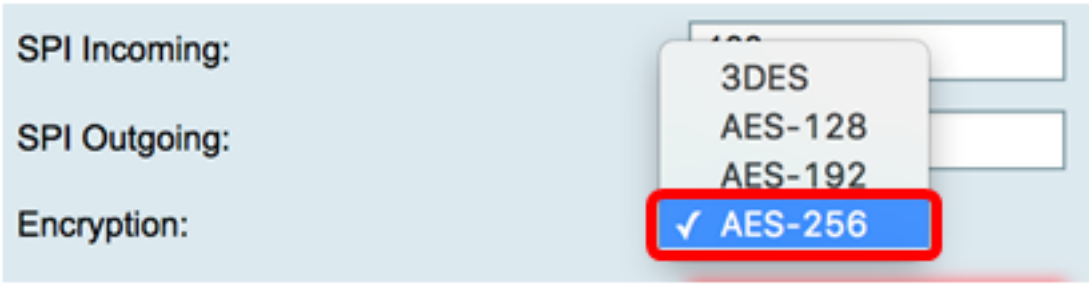
Stap 2. Voer in het veld *SPI-Uitgaande* een hexadecimaal getal in dat varieert van 100 tot FFFFF voor de SPI-tag voor uitgaande verkeer op de VPN-verbinding.

Opmerking: Bij dit voorbeeld wordt 0x1234 gebruikt.



Stap 3 . Kies een optie uit de vervolgkeuzelijst Encryptie. De opties zijn 3DES, AES-128, AES-192 en AES-256.

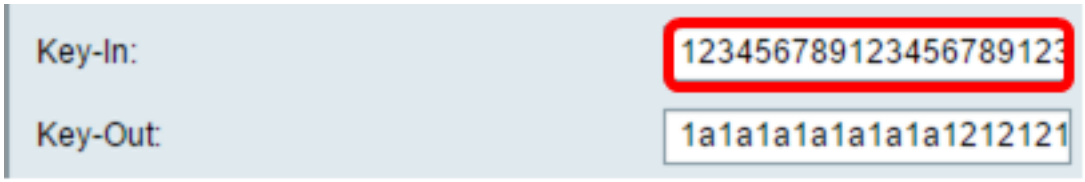
Opmerking: In dit voorbeeld wordt AES-256 gekozen.



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

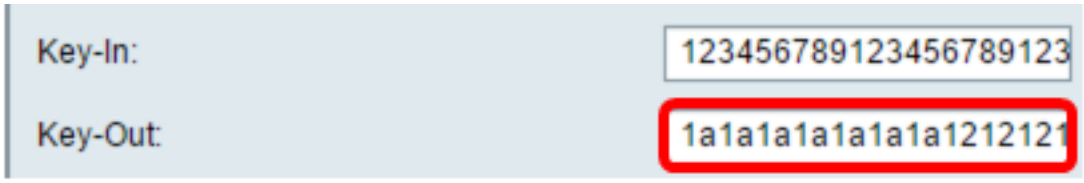
- 3DES gebruikt een 48-teken-toets.
- AES-128 maakt gebruik van een 32-tekens-toets.
- AES-192 maakt gebruik van een 48-tekensleutel.
- AES-256 maakt gebruik van een 64-tekensleutel.

Opmerking: In dit voorbeeld wordt 123456789123456789123.. gebruikt.



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

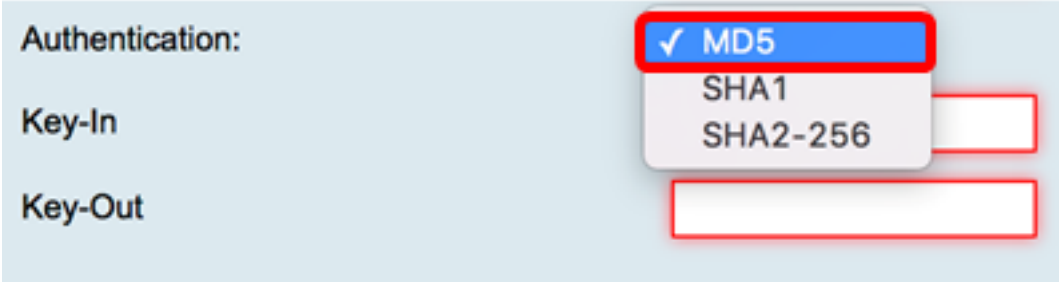
Opmerking: In dit voorbeeld wordt 1a1a1a1a1a1a1a1a1a121212.. gebruikt.



Stap 6. Kies een optie uit de vervolgkeuzelijst Handmatige integratiealgoritme.

- MD5 — Gebruik 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 beveiligd dan MD5 en SHA-1.

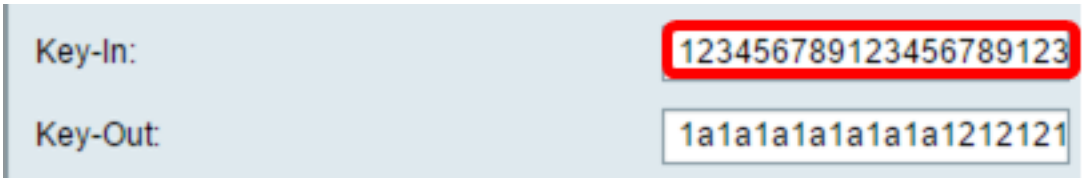
Opmerking: In dit voorbeeld wordt MD5 geselecteerd.



Stap 7. Voer in het *veld Key-In* een sleutel in voor het inkomende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 6 is gekozen.

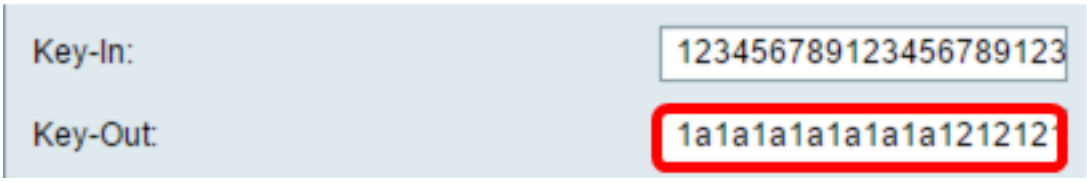
- MD5 gebruikt een toets van 32 tekens.
- SHA-1 gebruikt een 40-teken toets.
- SHA2-256 gebruikt een sleutel van 64 tekens.

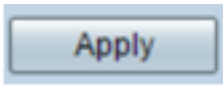
Opmerking: In dit voorbeeld wordt 123456789123456789123.. gebruikt.



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

Opmerking: In dit voorbeeld wordt 1a1a1a1a1a1a1a1a1a121212.. gebruikt.

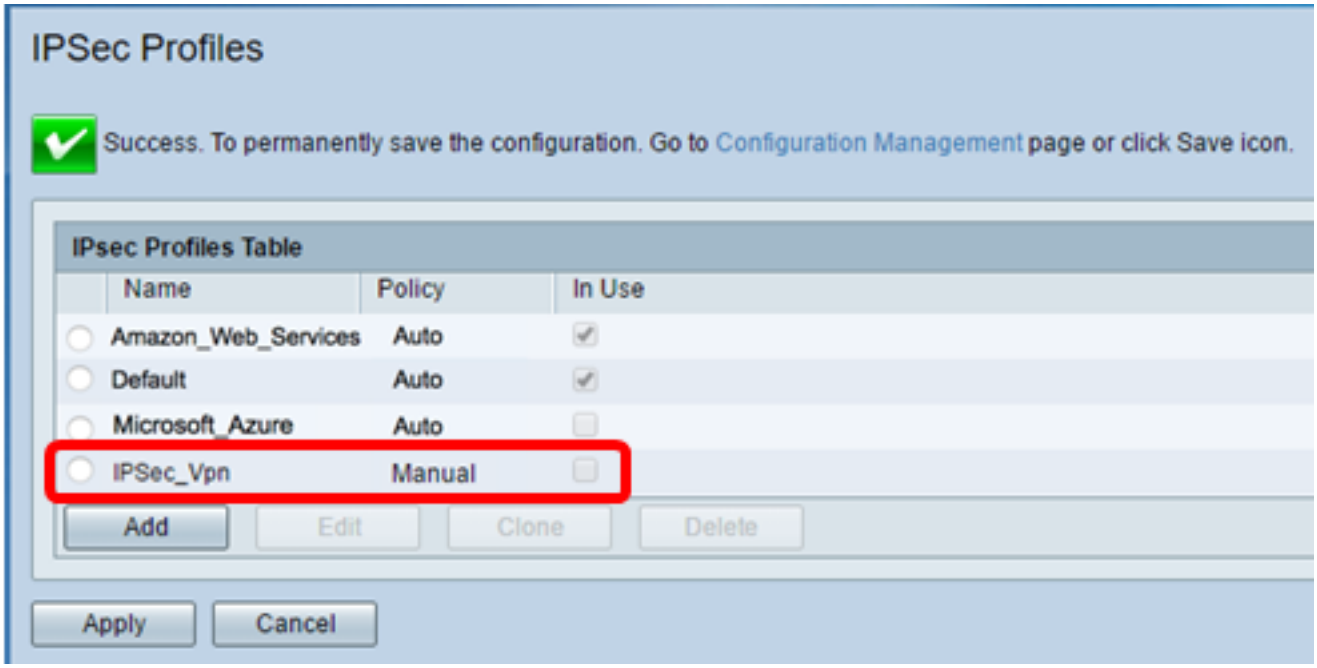


Stap 9. Klik op 

.

Opmerking: U wordt teruggebracht naar de tabel met IPSec-profielen en het nieuwe IPSec-

profiel moet nu worden weergegeven.



Stap 10. (Optioneel) Om de configuratie permanent op te slaan, gaat u naar de pagina Configuratie kopiëren/opslaan of klikt u op het 

pictogram in het bovenste gedeelte van de pagina.

U dient nu een handmatig IPSec profiel op een RV34x Series router te hebben ingesteld.