Geavanceerde VPN-instelling op RV215W

Doel

Een Virtual Private Network (VPN) is een beveiligde verbinding die binnen een netwerk of tussen netwerken tot stand is gebracht. VPNs dient om verkeer tussen gespecificeerde hosts en netwerken te isoleren van het verkeer van onbevoegde hosts en netwerken. Dit artikel legt uit hoe u de Advanced VPN-instelling op de RV215W kunt configureren.

Toepasselijke apparaten

- RV215W

Softwareversie

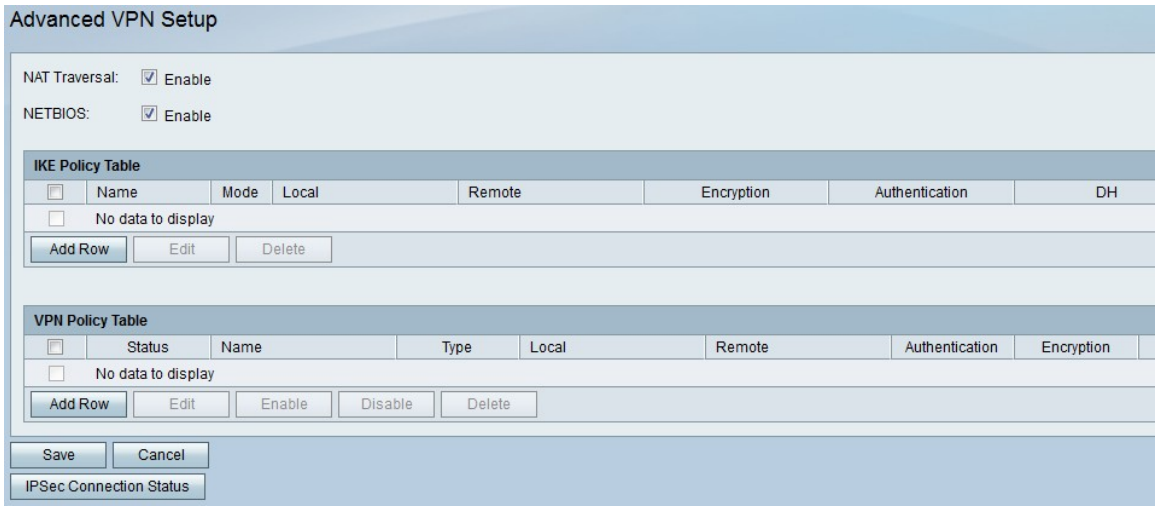
•1.1.0.5

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:



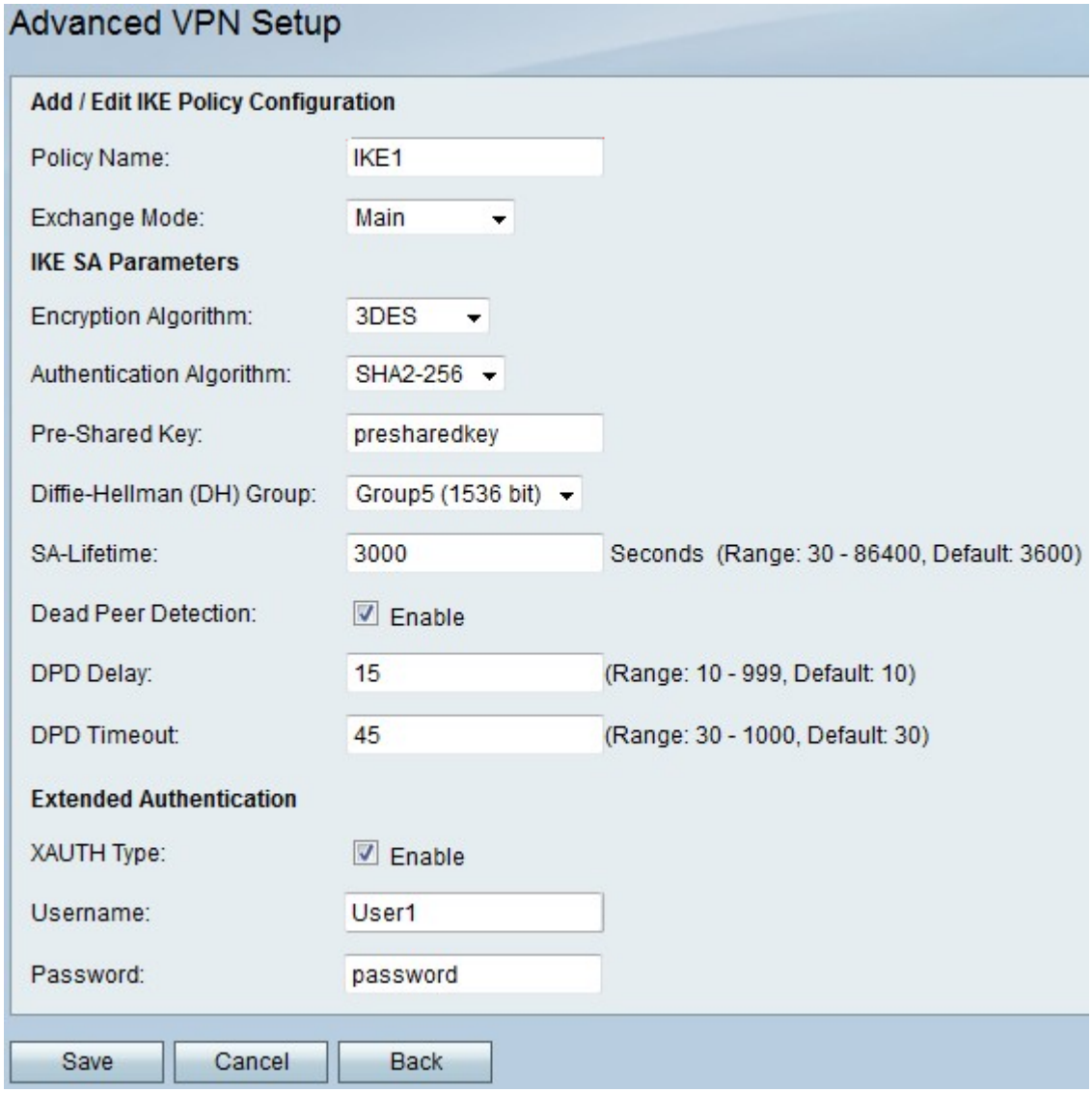
Stap 2. (Optioneel) Controleer het aanvinkvakje **Enable** in het veld NAT-verplaatsing als u NAT-adresomzetting (NAT) voor de VPN-verbinding wilt inschakelen. NAT Traversal maakt het mogelijk om een VPN-verbinding te maken tussen gateways die NAT gebruiken. Kies deze optie als uw VPN-verbinding door een NAT-enabled gateway gaat.

Stap 3. (Optioneel) Controleer het aanvinkvakje **Enable** in het veld NETeuropa indien u netwerkbasis I/O-uitzendingen (Netoverheid) wilt inschakelen om door de VPN-verbinding te worden verzonden. Netoverheid stelt hosts in staat met elkaar te 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.

Stap 1. Klik in de tabel IKE-beleid op **Weg toevoegen** om een nieuw IKE-beleid te maken. U kunt een IKE-beleid bewerken door het aanvinkvakje voor het beleid te controleren en door op **Bewerken** te klikken. De pagina *Geavanceerde VPN Setup* wijzigt:

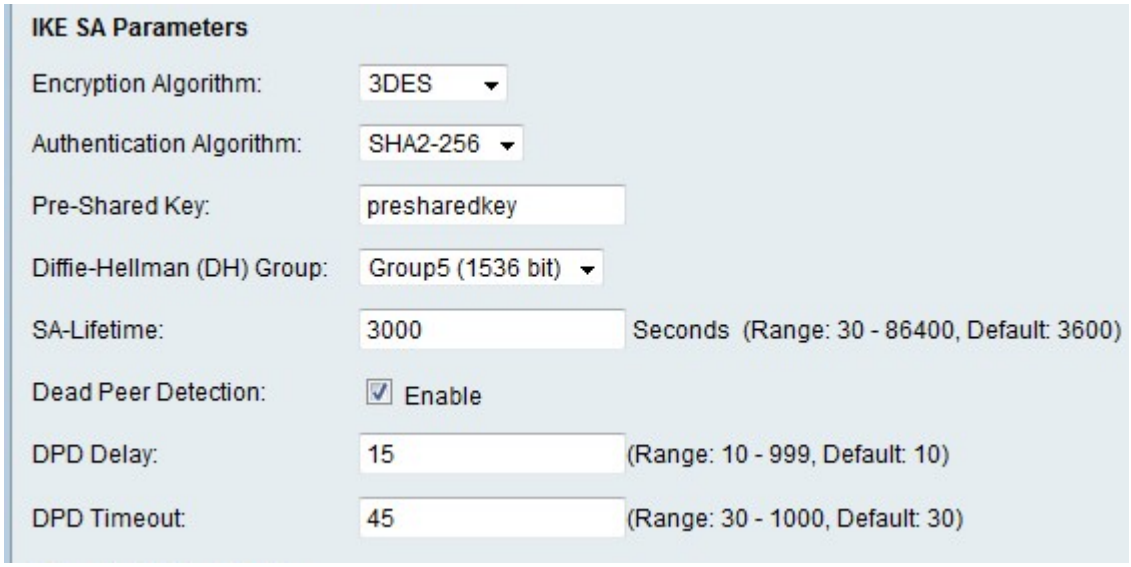


Stap 2. Voer in het veld Naam beleid een naam in voor het IKE-beleid.

Stap 3. Kies een optie uit de vervolgkeuzelijst Exchange Mode.

- Hoofdstroom — Deze optie stelt het IKE-beleid in staat beter maar langzamer te werken dan agressieve modus. Kies deze optie als een meer beveiligde VPN-verbinding nodig is.

- Aggressief — Met deze optie kan het IKE-beleid sneller maar minder goed werken dan de hoofdmodus. Kies deze optie als er een snellere VPN-verbinding nodig is.



Stap 4. Kies een optie uit de vervolgkeuzelijst Encryption Algorithm.

- DES — Data Encryption Standard (DES) is een 56-bits oude encryptiemethode die niet erg veilig is, maar wel vereist is voor compatibiliteit met de achterzijde.

- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits eenvoudige coderingsmethode die wordt gebruikt om de grootte van het bestand 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 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 en veiliger dan 3DES. 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-1920 is langzamer maar veiliger dan AES-128 en sneller maar minder beveiligd 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 5. Kies een optie uit 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.

Stap 6. Voer in het veld Vooraf gedeelde sleutel een vooraf gedeelde sleutel in die het IKE-beleid gebruikt.

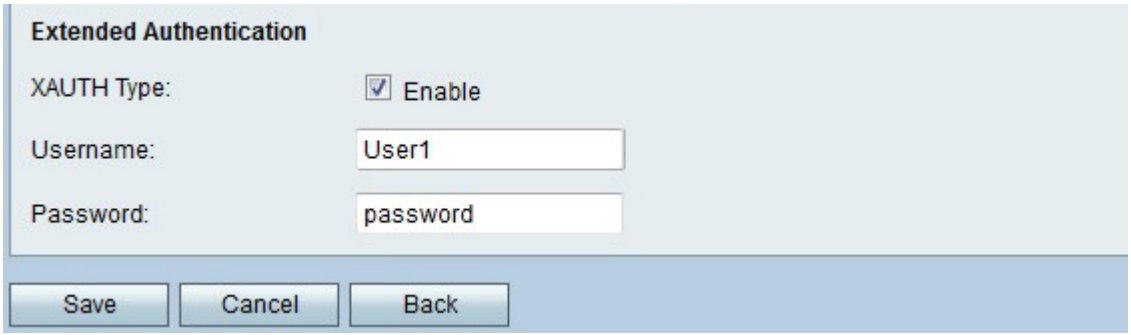
Stap 7. Kies in de vervolgkeuzelijst Diffie-Hellman (DH) groep welke DH de IKE-toepassing groepeert. Organisatoren in een DH-groep kunnen sleutels uitwisselen zonder elkaar te kennen. Hoe hoger het aantal groepsbits is, hoe veiliger de groep is.

Stap 8. Voer in het veld SA-Lifetime in hoe lang een SA in seconden voor de VPN duurt voordat de SA wordt vernieuwd.

Stap 9. (Optioneel) Controleer het aanvinkvakje **Enable** in het veld Dead Peer Detectie (DPD) om Dead Peer Detectie in te schakelen. DPD controleert IKE-peers om te zien of een peer niet meer werkt. DPD voorkomt de verspilling van netwerkbronnen op inactieve peers.

Stap 10. (Optioneel) Als u DPD in Stap 9 hebt ingeschakeld, specificeert u hoe vaak (in seconden) de peer wordt gecontroleerd op activiteit in het veld DPD Delay.

Stap 1. (Optioneel) Als u DPD in Stap 9 hebt ingeschakeld, specificeert u hoeveel seconden u wilt wachten voordat een inactief peer wordt laten vallen in het veld Time-out bij DPD.



Stap 12. (Optioneel) Controleer het aanvinkvakje **Enable** in het veld XAUTH Type om uitgebreide verificatie (XAUTH) mogelijk te maken. XAUTH biedt meerdere gebruikers de mogelijkheid één VPN-beleid in plaats van een VPN-beleid te gebruiken voor elke gebruiker.

Stap 13. (Optioneel) Als u XAUTH in Stap 12 hebt ingeschakeld, specificeert u de gebruikersnaam voor het beleid in het veld Gebruikersnaam.

Stap 14. (Optioneel) Als u XAUTH in Stap 12 hebt ingeschakeld, voert u het wachtwoord in om voor het beleid in het veld Wachtwoord te gebruiken.

Stap 15. Klik op **Opslaan**. De oorspronkelijke pagina *Geavanceerde VPN Setup* verschijnt opnieuw.

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.

Stap 1. In de VPN-beleidstabel klikt u op **Weg toevoegen** om een nieuw VPN-beleid te maken. U kunt een VPN-beleid bewerken door het aanvinkvakje voor het beleid te controleren en door op **Bewerken** te klikken. De pagina *Geavanceerde VPN Setup* wijzigt:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name: VPN1

Policy Type: Manual Policy

Remote Endpoint: IP Address

209.165.201.1 (Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP: Subnet

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: Subnet

IP Address: 192.168.2.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Encryption Algorithm: AES-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Integrity Algorithm: SHA2-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Auto Policy Parameters

SA-Lifetime: 20000 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-256

Integrity Algorithm: SHA2-256

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: IKE1

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

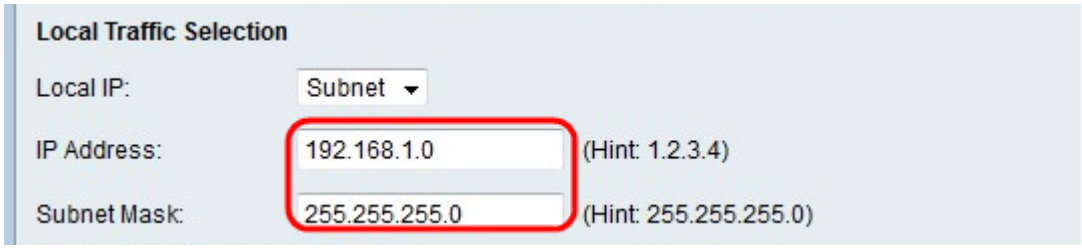
Stap 3. Kies een optie in de vervolgkeuzelijst Beleidstype.

- 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 een optie uit de vervolgkeuzelijst Remote Endpoint.

- 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. Kies een optie uit de vervolgkeuzelijst Local IP.

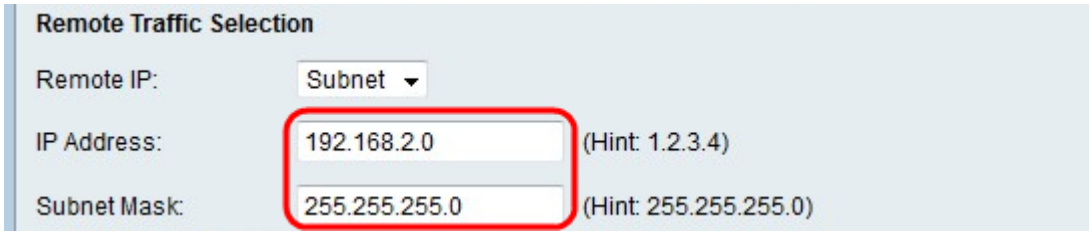
- Enkelvoudig - Deze optie gebruikt één host als het lokale VPN-verbindingspunt.
- Subnet - Deze optie gebruikt een net van het lokale netwerk als het lokale VPN verbindingspunt.

Stap 7. In het veld IP-adres voert u het host- of subnetadres van het lokale net of de host in.

Stap 8. (Optioneel) Als u Subnet in Stap 6 kiest, voer het subnetmasker voor het lokale subnetmasker in het veld Subnetmasker in.

Stap 9. Kies een optie uit de vervolgkeuzelijst Remote IP.

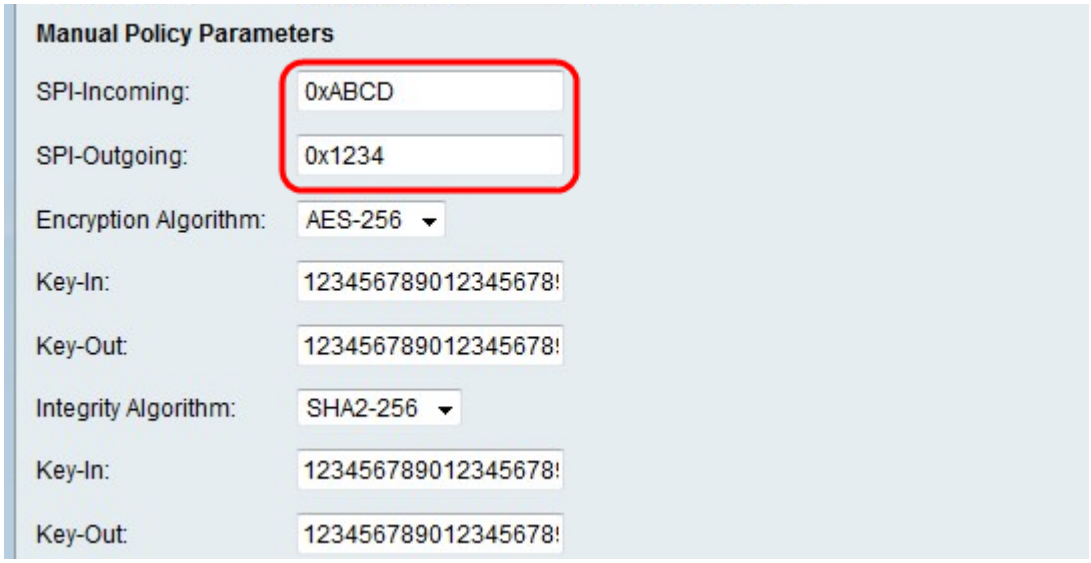
- Enkelvoudig - Deze optie gebruikt één host als het externe VPN-verbindingspunt.
- Subnet - Deze optie gebruikt een net van het externe netwerk als het externe VPN-verbindingspunt.



Stap 10. In het veld IP-adres voert u het host- of subnetadres van het externe subnetwerk of de host in.

Stap 1. (Optioneel) Als u Subnet in Stap 9 kiest, voer het subnetmasker voor het externe subnetmasker in het veld Subnetmasker in.

Opmerking: Als u in Stap 3 Handmatig beleid kiest, voert u Stap 12 tot en met Stap 19 uit. anders slaat u Stap 20 over.



Stap 12. Voer in het veld SPI-Inkomend in dat geval 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.

Stap 13. Voer in het veld SPI-Uitgaande een drievoudige tot acht hexadecimale tekens in voor een SPI-tag voor uitgaande verkeer op de VPN-verbinding.

Stap 14. Kies een optie uit de vervolgkeuzelijst Encryption Algorithm.

- DES — Data Encryption Standard (DES) is een 56-bits oude encryptiemethode die niet erg veilig is, maar wel vereist is voor compatibiliteit met de achterzijde.

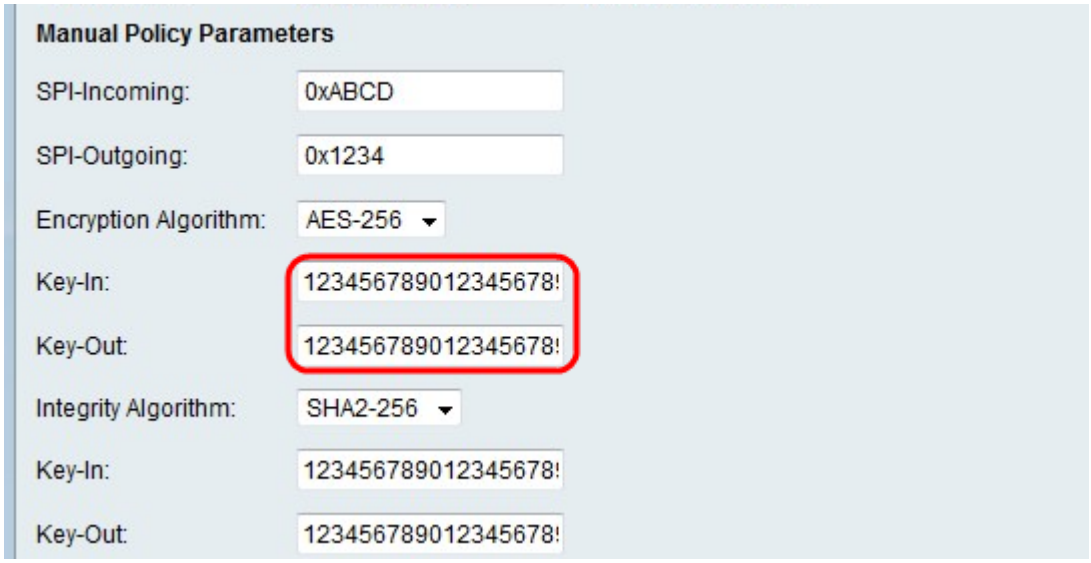
- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits eenvoudige coderingsmethode die wordt gebruikt om de grootte van het bestand te vergroten, omdat de gegevens drie keer worden versleuteld. Dit biedt meer beveiliging dan DES maar minder beveiliging dan AES.

- AES-128 — Advanced Encryption Standard met 128-bits 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 en veiliger dan 3DES. 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-1920 is

langzamer maar veiliger dan AES-128 en sneller maar minder beveiligd 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.



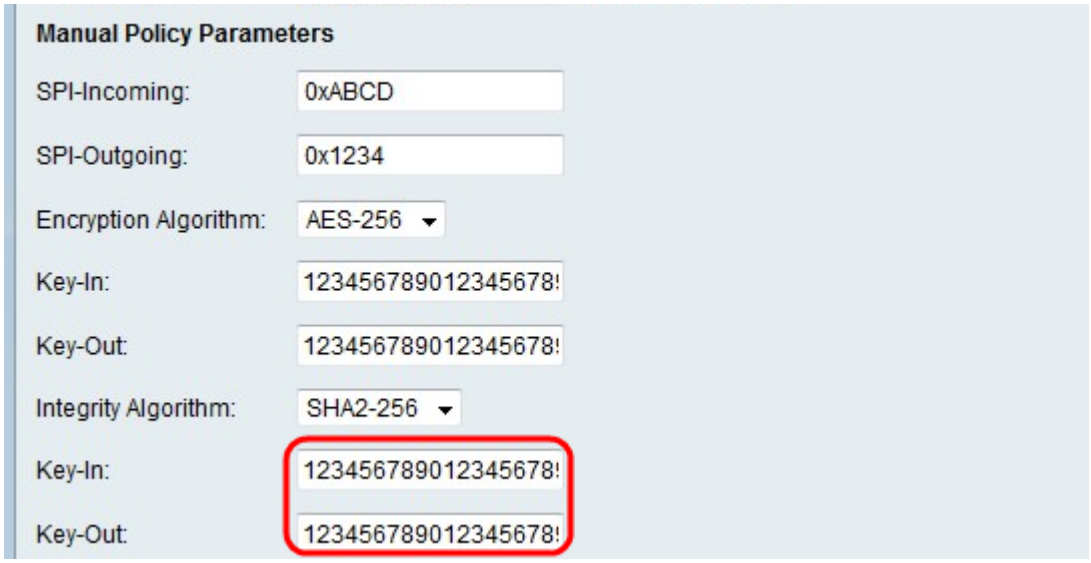
Stap 15. Voer in het veld Key-In een sleutel in voor het inkomende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 14 is gekozen.

- 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 16. Voer in het veld Uitbel een sleutel in voor het uittredende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 14 is geselecteerd. De sleutellengtes zijn hetzelfde als Stap 15.

Stap 17. Kies een optie uit de vervolgkeuzelijst Integrity Algorithm.

- MD5 — Message-Digest Algorithm 5 (MD5) gebruikt een 128-bits hashwaarde voor gegevensintegriteit. 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 gegevensintegriteit. 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 gegevensintegriteit. SHA2-256 is langzamer maar beveiligd dan MD5 en SHA-1.

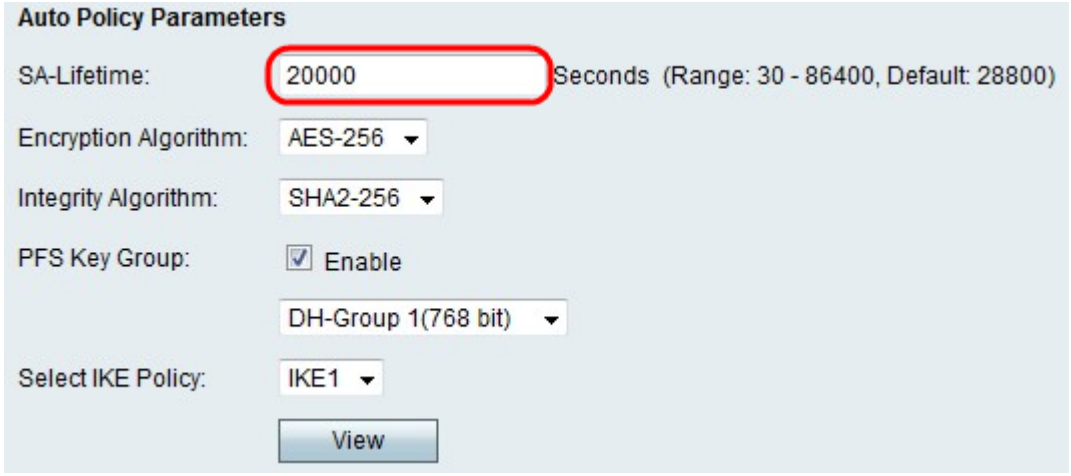


Stap 18. Voer in het veld Key-In een sleutel in voor het inkomende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 17 is gekozen.

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

Stap 19. Voer in het veld Uitbel een sleutel in voor het uittredende beleid. De sleutellengte is afhankelijk van het algoritme dat in Stap 17 is geselecteerd. De sleutellengtes zijn hetzelfde als Stap 18.

Opmerking: Als u in Stap 3 voor Auto Policy hebt gekozen, voert u Stap 20 tot en met Stap 25 uit. anders overslaan naar Stap 26.



Stap 20. Voer in het veld SA-Liftime in hoe lang de SA in seconden duurt voor de vernieuwing.

Stap 21. Kies een optie uit de vervolgkeuzelijst Encryption Algorithm.

- DES — Data Encryption Standard (DES) is een 56-bits oude encryptiemethode die niet erg veilig is, maar wel vereist is voor compatibiliteit met de achterzijde.
- 3DES - Triple Data Encryption Standard (3DES) is een 168-bits eenvoudige coderingsmethode die wordt gebruikt om de grootte van het bestand 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 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 en veiliger dan 3DES. 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-1920 is langzamer maar veiliger dan AES-128 en sneller maar minder beveiligd 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 2. Kies een optie uit de vervolgkeuzelijst Integrity Algorithm.

- MD5 — Message-Digest Algorithm 5 (MD5) gebruikt een 128-bits hashwaarde voor gegevensintegriteit. 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 gegevensintegriteit. 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 gegevensintegriteit. SHA2-256 is langzamer maar beveiligd dan MD5 en SHA-1.

Stap 23. Controleer het aanvinkvakje **Enable** in de PFS-sleutelgroep om Perfect Forward Security (PFS) mogelijk te maken. PFS verhoogt de VPN-beveiliging, maar vertraagt de verbindingssnelheid.

Stap 24. (Optioneel) Als u PFS in Stap 23 wilt inschakelen, kiest u een Diffie-Hellman (DH) groep om zich aan te sluiten voor de onderstaande vervolgkeuzelijst. Hoe hoger het groepsnummer is, hoe veiliger de groep is.

Stap 25. Kies in de vervolgkeuzelijst IKE-beleid selecteren welk IKE-beleid u voor het VPN-beleid wilt gebruiken.

Opmerking: Als u op **Weergave** klikt, wordt u verwezen naar het configuratiescherm IKE van de *Geavanceerde VPN Setup*-pagina.

Stap 26. Klik op **Opslaan**. De oorspronkelijke pagina *Geavanceerde VPN Setup* verschijnt opnieuw.

Stap 27. Klik op **Opslaan**.