Configuratie van een IPSec VPN-server op RV130 en RV130W

Doel

Met IPSec VPN (Virtual Private Network) kunt u veilig externe toegang tot bedrijfsresources verkrijgen door een versleutelde tunnel over het internet te maken.

Het doel van dit document is u te tonen hoe u een IPSec VPN Server kunt configureren op RV130 en RV130W.

Opmerking: Raadpleeg voor informatie over het configureren van een IPSec VPN Server met de Shrew Soft VPN Client op RV130 en RV130W het artikel *Use Shrew Soft VPN Client met IPSec VPN Server op RV130 en RV130W*.

Toepasselijke apparaten

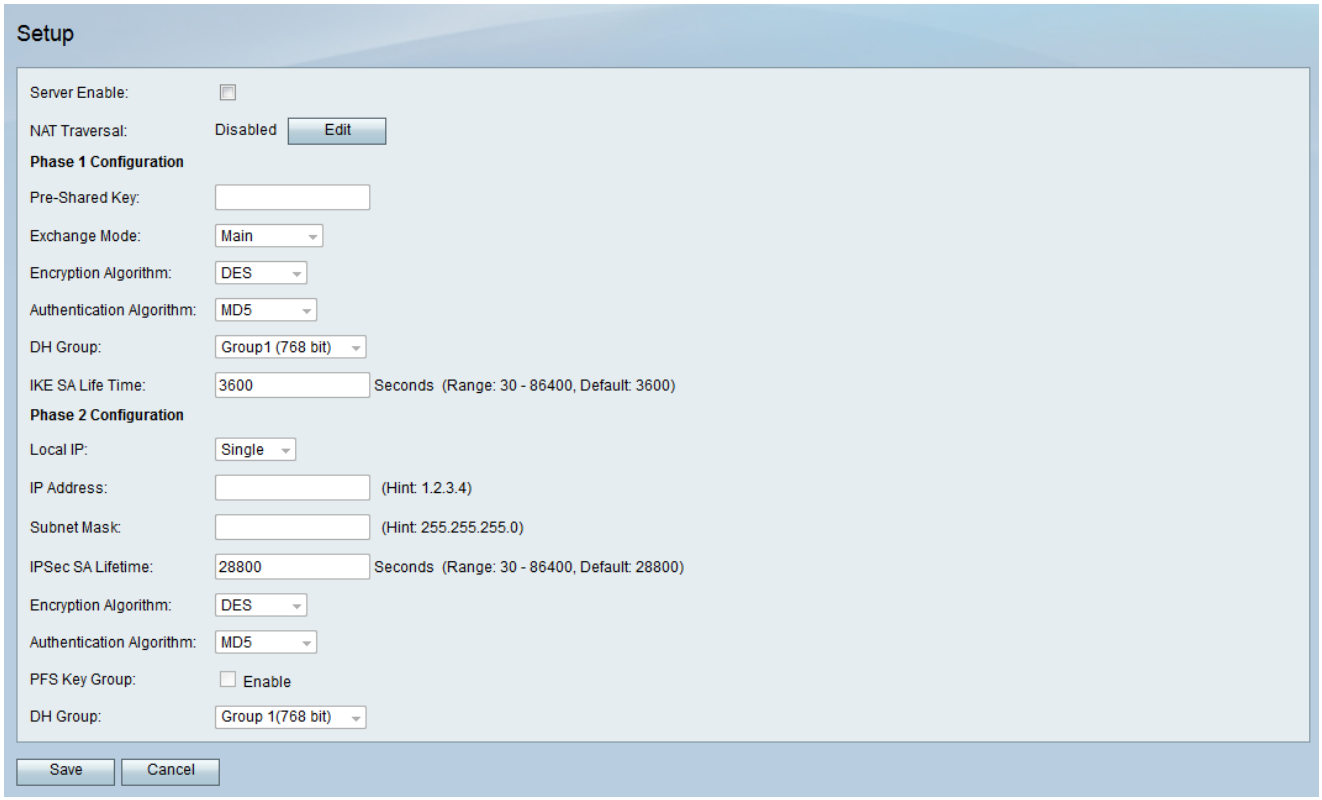
·RV130W Wireless-N VPN-firewall
· RV130 VPN-firewall

Softwareversie

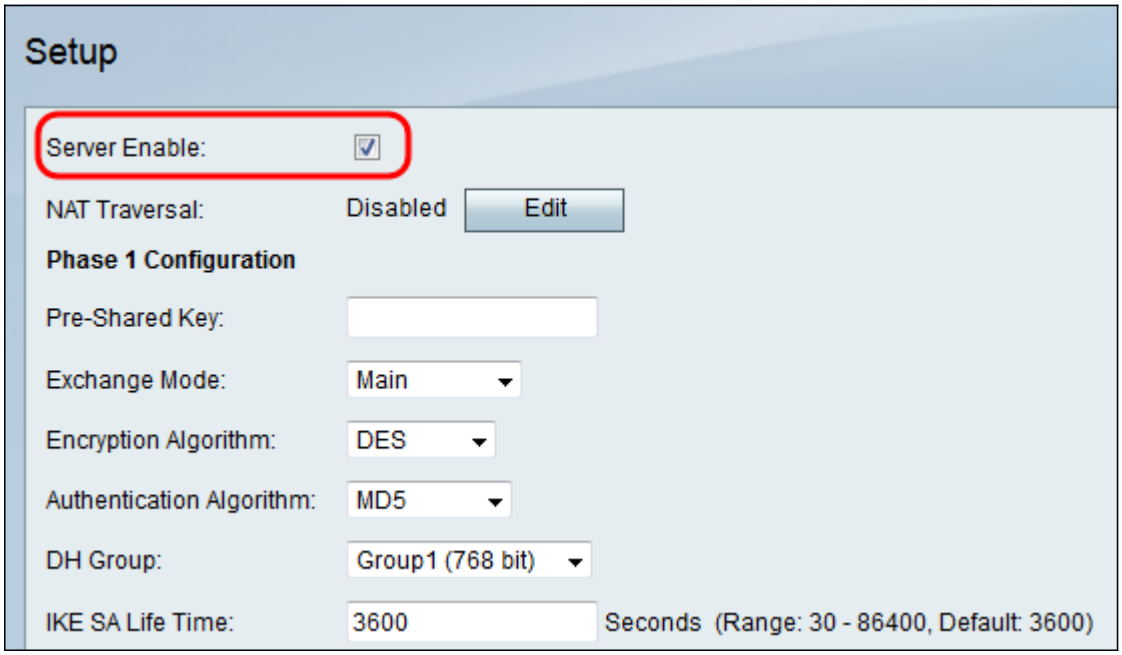
·v1.0.1.3

IPSec VPN-server instellen

Stap 1. Log in op het hulpprogramma voor webconfiguratie en kies **VPN > IPSec VPN Server > Setup**. De pagina Instellen wordt geopend.

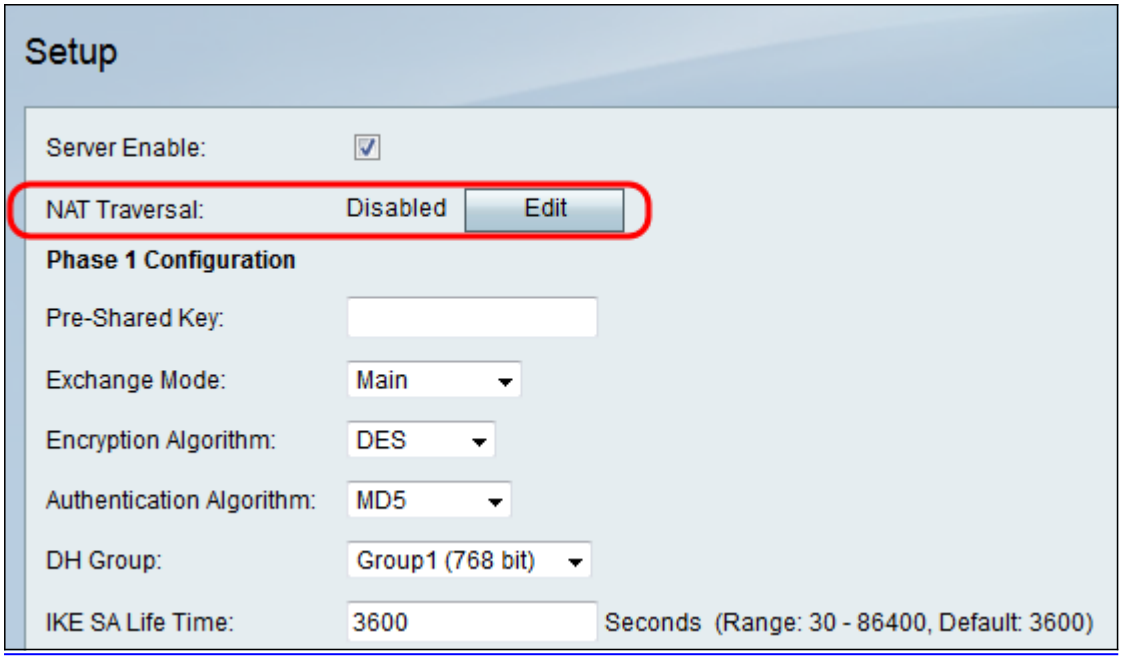


Stap 2. Controleer of het vakje **Server inschakelen** om het certificaat in te schakelen.

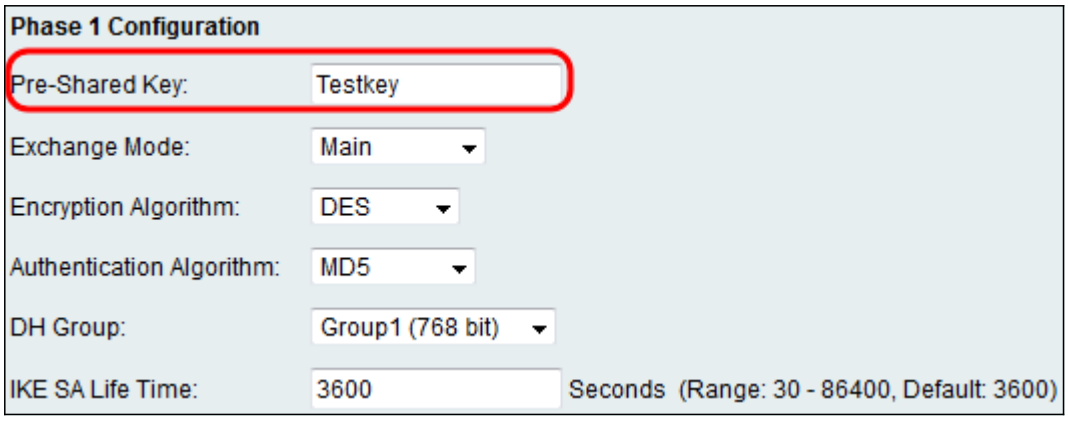


Stap 3. (Optioneel) Als uw VPN-router of VPN-client zich achter een NAT-gateway bevindt, klikt u op **Bewerken** om NAT-transversaal te configureren. Anders laat u NAT Trauniversal uitgeschakeld.

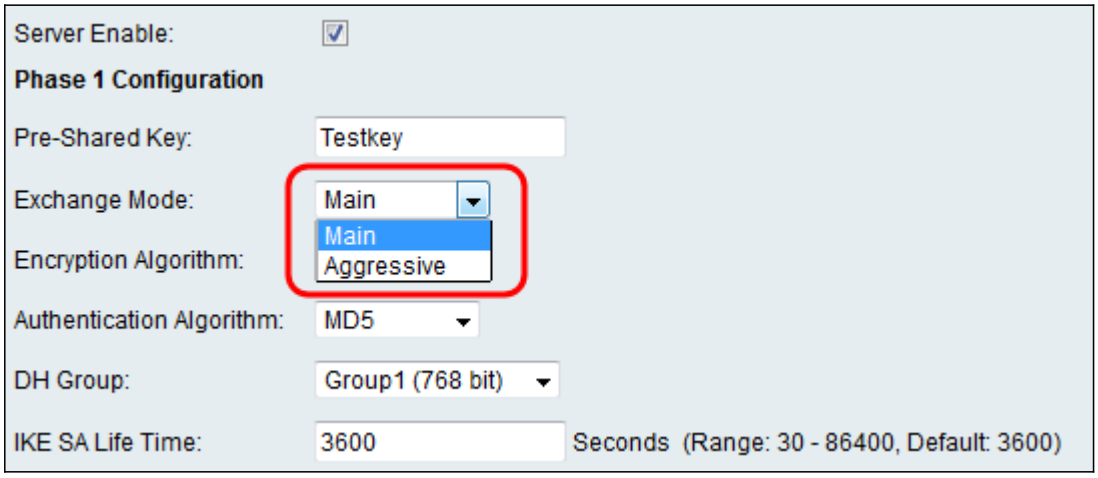
Opmerking: Raadpleeg *Beleidsinstellingen voor Internet Key Exchange (IKE) op RV130 en RV130W VPN-routers voor* meer informatie over het configureren *van* NAT-traversinstellingen.



Stap 4. Voer een sleutel in tussen 8 tot 49 tekens die tussen uw apparaat en het externe eindpunt in het veld *Vooraf gedeelde sleutel* worden uitgewisseld.



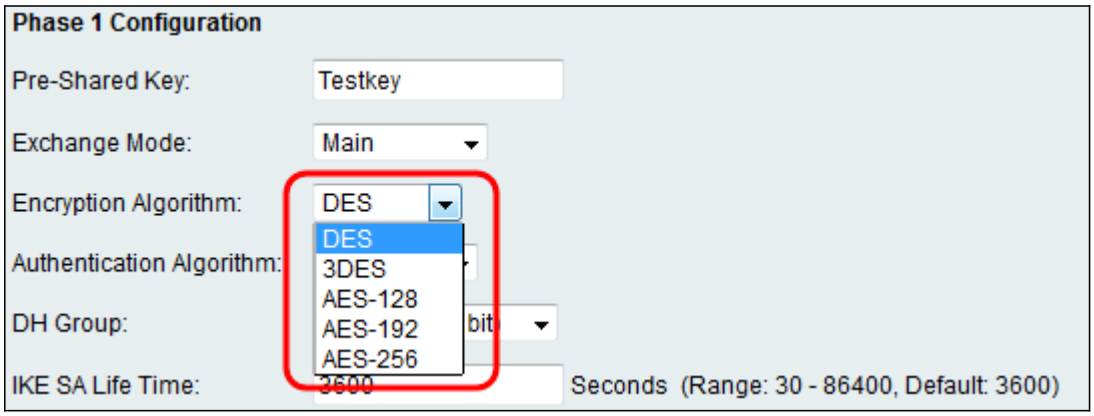
Stap 5. Kies in de vervolgkeuzelijst *Exchange Mode* de modus voor de IPSec VPN-verbinding. **De** standaardmodus is de **hoofdmodus**. Als uw netwerksnelheid echter laag is, kiest u de modus **Agressief**.



Opmerking: Agressieve modus ruilt de ID's van de eindpunten van de tunnel in heldere tekst tijdens de verbinding, die minder tijd nodig heeft om te ruilen maar minder veilig is.

Stap 6. Kies in de vervolgkeuzelijst **Encryptie-algoritme** de juiste coderingsmethode om de

vooraf gedeelde sleutel in fase 1 te versleutelen. AES-128 wordt aanbevolen voor de hoge beveiliging en snelle prestaties ervan. De VPN-tunnel moet voor beide doeleinden dezelfde coderingsmethode gebruiken.



De beschikbare opties zijn als volgt gedefinieerd:

·DES — Data Encryption Standard (DES) is een 56-bits, oude coderingsmethode die niet erg veilig is, maar mogelijk nodig is voor achterwaartse compatibiliteit.

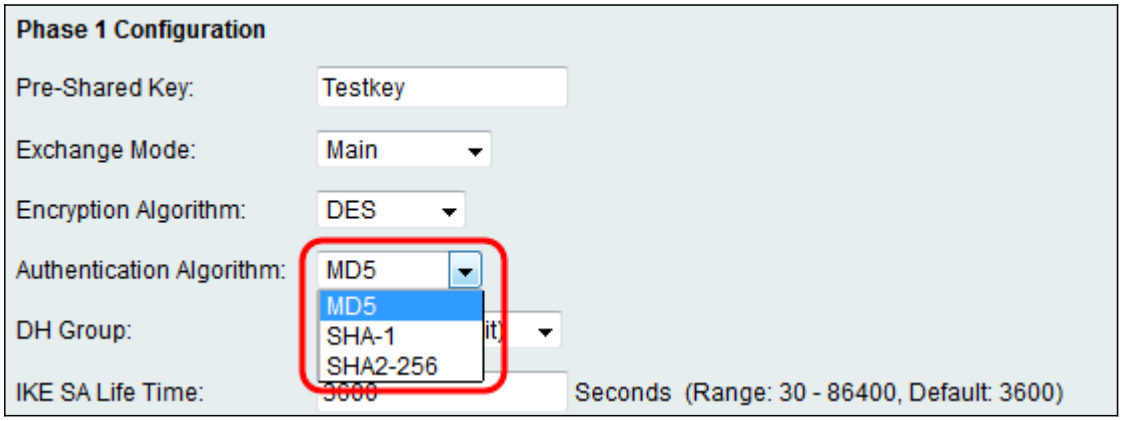
·3DES — Triple Data Encryption Standard (3DES) is een 168-bits, eenvoudige coderingsmethode die wordt gebruikt om de sleutel te vergroten omdat de gegevens drie keer worden versleuteld. Dit biedt meer beveiliging dan DES maar minder beveiliging dan AES.

·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 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.

Stap 7. Kies in de vervolgkeuzelijst *Verificatiealgoritme* de juiste verificatiemethode om te bepalen hoe de ESP-pakketten (Encapsulating Security Payload) in fase 1 zijn gevalideerd. De VPN-tunnel moet dezelfde verificatiemethode voor beide uiteinden van de verbinding gebruiken.



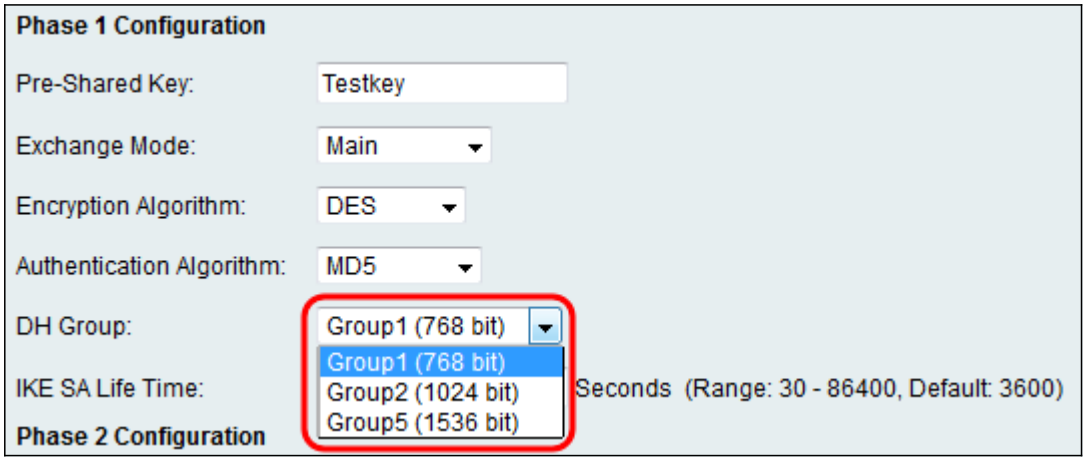
De beschikbare opties zijn als volgt gedefinieerd:

·MD5 — MD5 is een one-way hashing algoritme dat een 128-bit samenvatting produceert. MD5 verwerkt sneller dan SHA-1, maar is minder veilig dan SHA-1. MD5 wordt niet aanbevolen.

·SHA-1 — SHA-1 is een one-way hashing algoritme dat een 160-bit samenvatting produceert. SHA-1 verwerkt langzamer dan MD5, maar is veiliger dan MD5.

·SHA2-256 — Specificeert het Secure Hash-algoritme SHA2 met de 256-bits samenvatting.

Stap 8. Kies in de vervolgkeuzelijst *DH Group* de juiste Diffie-Hellman (DH) groep die in fase 1 met de sleutel moet worden gebruikt. Diffie-Hellman is een cryptografisch sleuteluitwisselingsprotocol dat in de verbinding wordt gebruikt om vooraf gedeelde sleutelsets te ruilen. De sterkte van het algoritme wordt bepaald door bits.



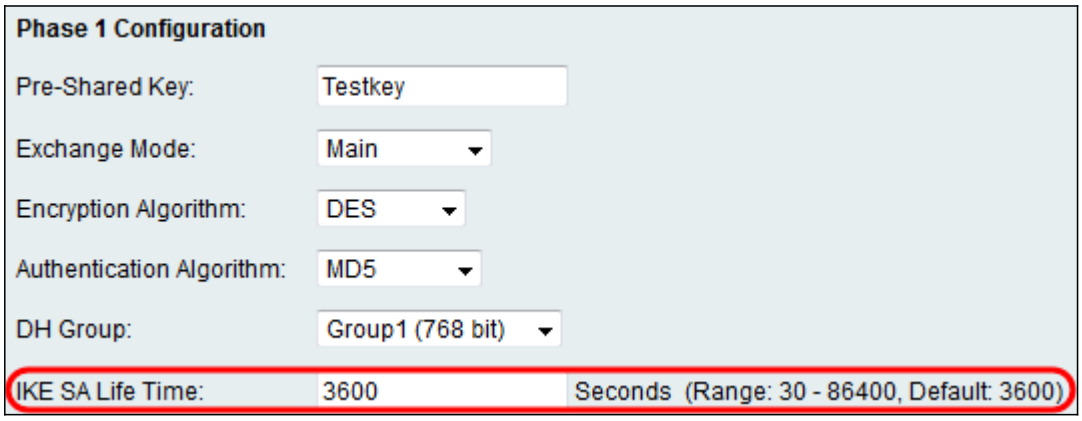
De beschikbare opties zijn als volgt gedefinieerd:

·Group1 (768 bit) — berekent de sleutel het snelst, maar is de minst beveiligde.

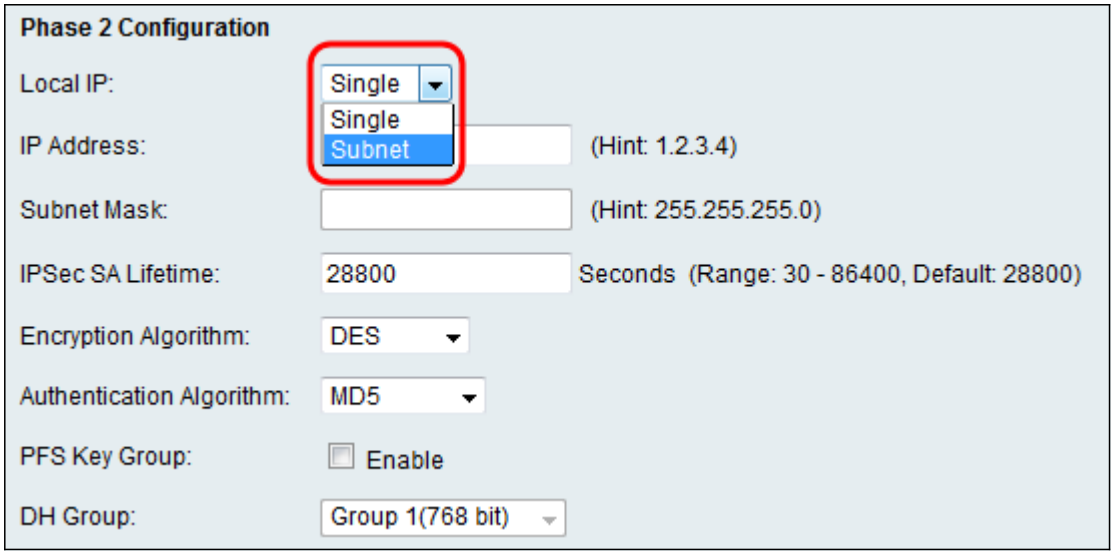
·Groep2 (1024 bit) — berekent de sleutel langzamer, maar is veiliger dan groep1.

·Groep 5 (1536 bit) — berekent de sleutel met de langzaamste, maar is de veiligste.

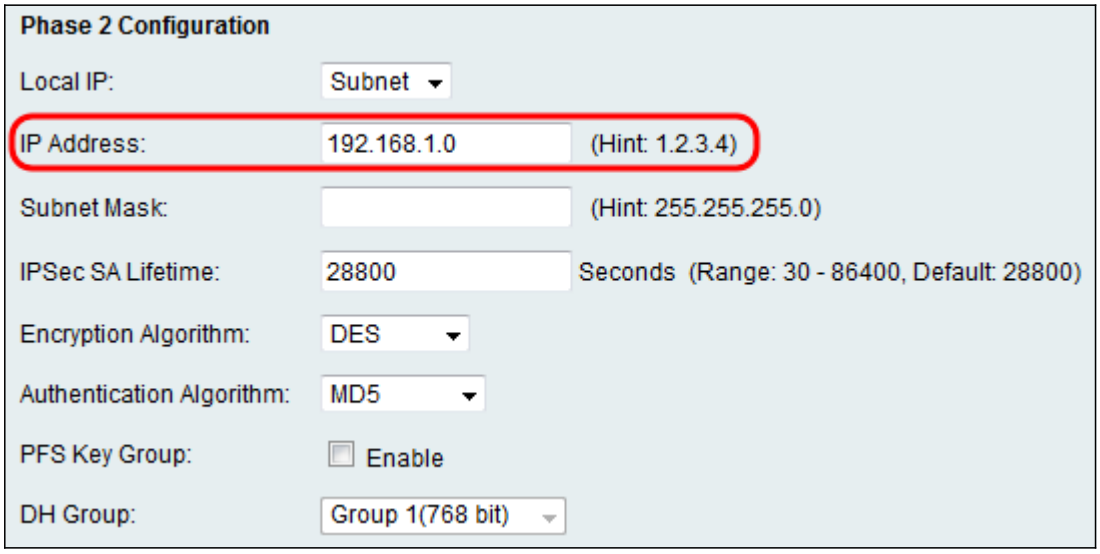
Stap 9. Voer in het veld *IKE SA Life Time* de tijd in (in seconden) dat de automatische IKE-toets geldig is. Als deze tijd is verlopen, wordt er automatisch over een nieuwe sleutel onderhandeld.



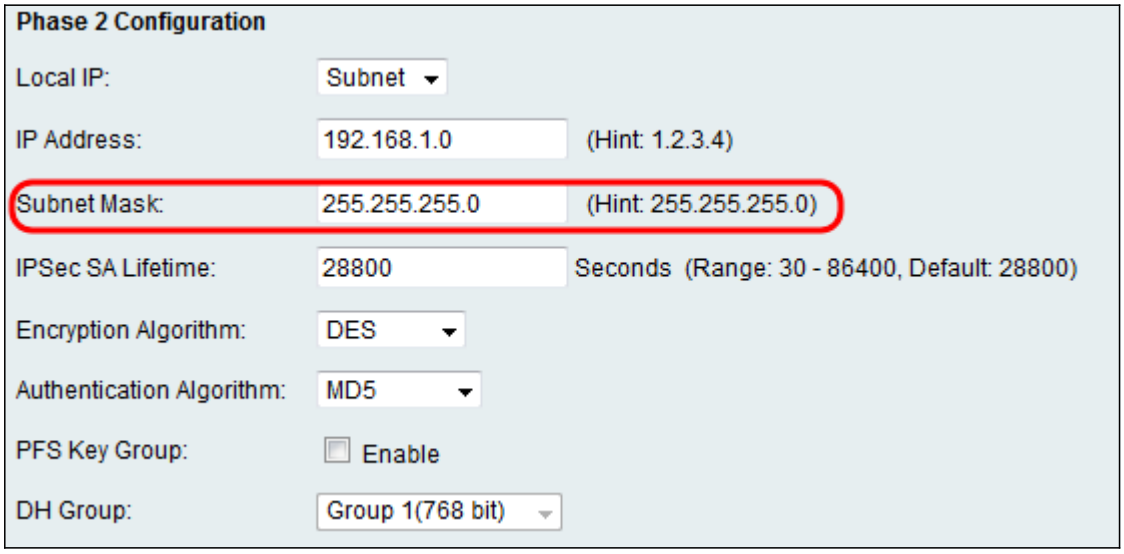
Stap 10. Kies in de vervolgkeuzelijst *Local IP* **Single** als u wilt dat één lokale LAN-gebruiker toegang heeft tot de VPN-tunnel of kies **Subnet** als u wilt dat meerdere gebruikers toegang hebben tot de tunnel.



Stap 1. Als **Subnet** in stap 10 is gekozen, voert u in het veld IP-adres van het subnetwerk het IP-adres in. Als **Single** is gekozen in Stap 10, voert u het IP-adres van de enkele gebruiker in en gaat u verder naar Stap 13.

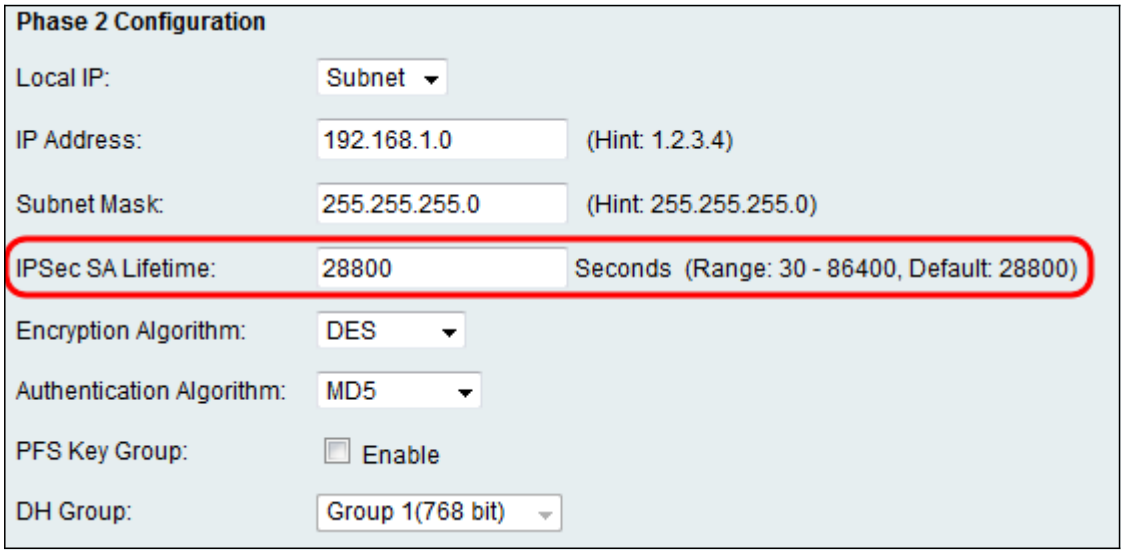


Stap 12. (Optioneel) Als **Subnet** in Stap 10 is gekozen, voert u het subnetmasker van het lokale netwerk in het veld *Subnetmasker in*.

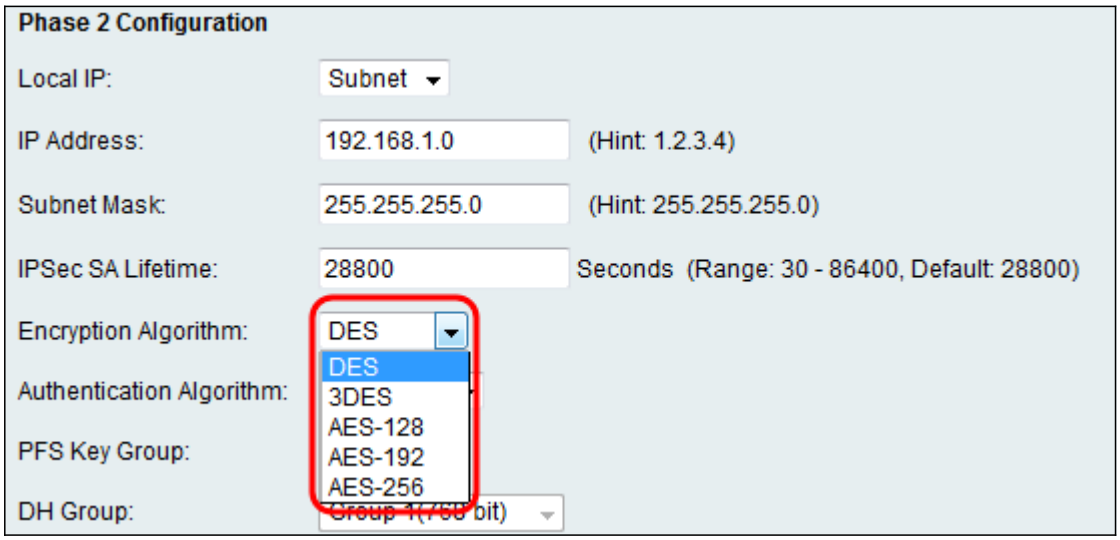


Stap 13. Voer in het veld *IPSec SA Lifetime* de tijd in in seconden dat de VPN-verbinding

actief blijft in fase 2. Zodra deze tijd is verlopen, wordt opnieuw onderhandeld over de IPSec Security Association voor de VPN-verbinding.



Stap 14. Kies uit de vervolgkeuzelijst *Encryptiealgoritme* de juiste coderingsmethode om de vooraf gedeelde sleutel in fase 2 te versleutelen. AES-128 wordt aanbevolen voor de hoge beveiliging en snelle prestaties ervan.De VPN-tunnel moet voor beide doeleinden dezelfde coderingsmethode gebruiken.



De beschikbare opties zijn als volgt gedefinieerd:

·DES — Data Encryption Standard (DES) is een 56-bits, oude coderingsmethode die het minst veilig 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.

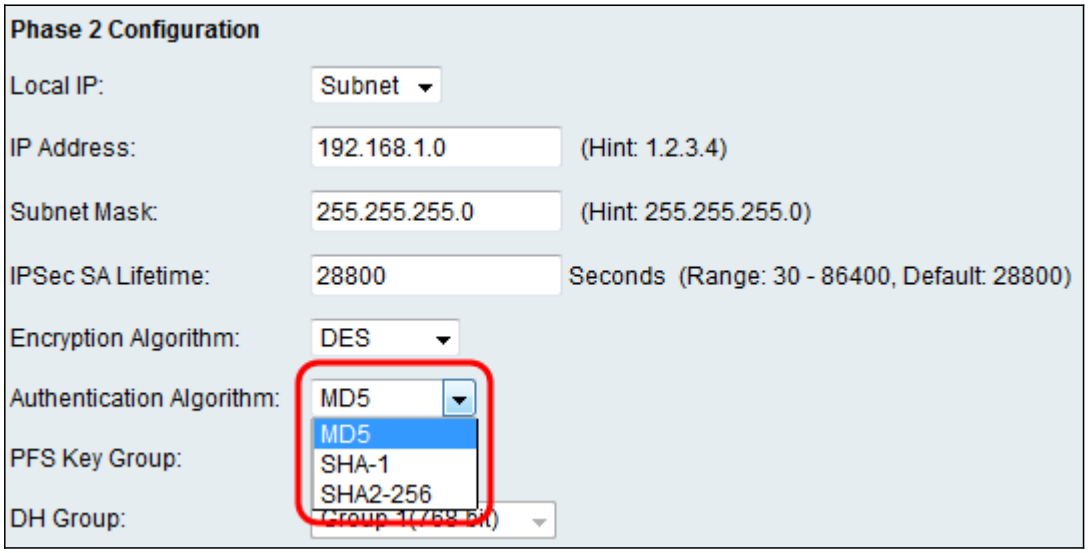
·AES-128 — Advanced Encryption Standard met 128-bits sleutel (AES-128) gebruikt een 128-bits sleutel voor AES-encryptie. AES is sneller en veiliger dan DES. Over het algemeen is AES ook sneller en veiliger dan 3DES. AES-128 is sneller maar minder veilig dan AES-192 en AES-256.

·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.

Stap 15. Kies in de vervolgkeuzelijst *Verificatiealgoritme* de juiste verificatiemethode om te bepalen hoe de ESP-pakketten (Encapsulating Security Payload) in fase 2 zijn gevalideerd. De VPN-tunnel moet voor beide doeleinden dezelfde verificatiemethode gebruiken.



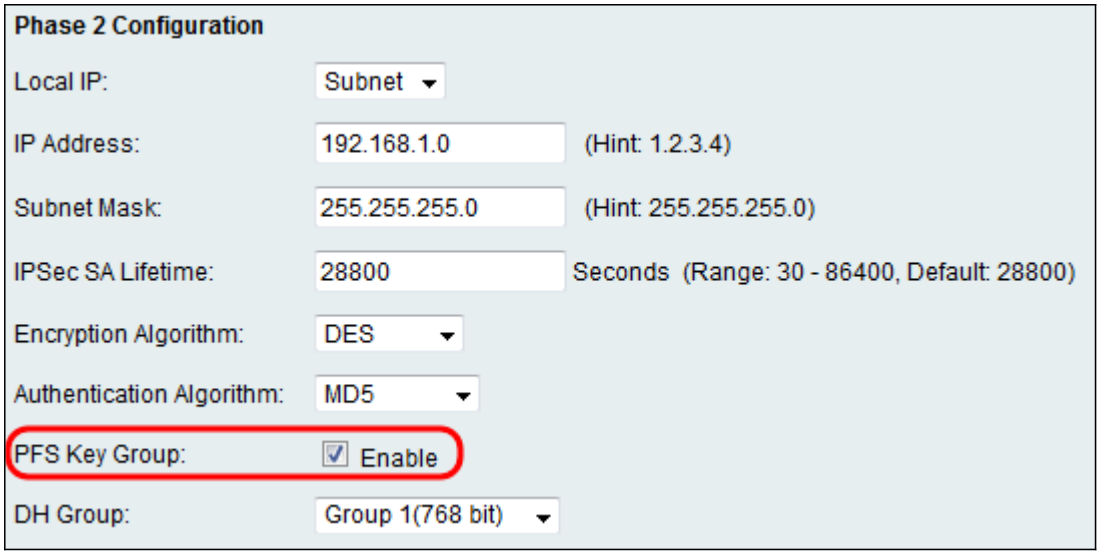
De beschikbare opties zijn als volgt gedefinieerd:

·MD5 — MD5 is een one-way hashing algoritme dat een 128-bit samenvatting produceert. MD5 verwerkt sneller dan SHA-1, maar is minder veilig dan SHA-1. MD5 wordt niet aanbevolen.

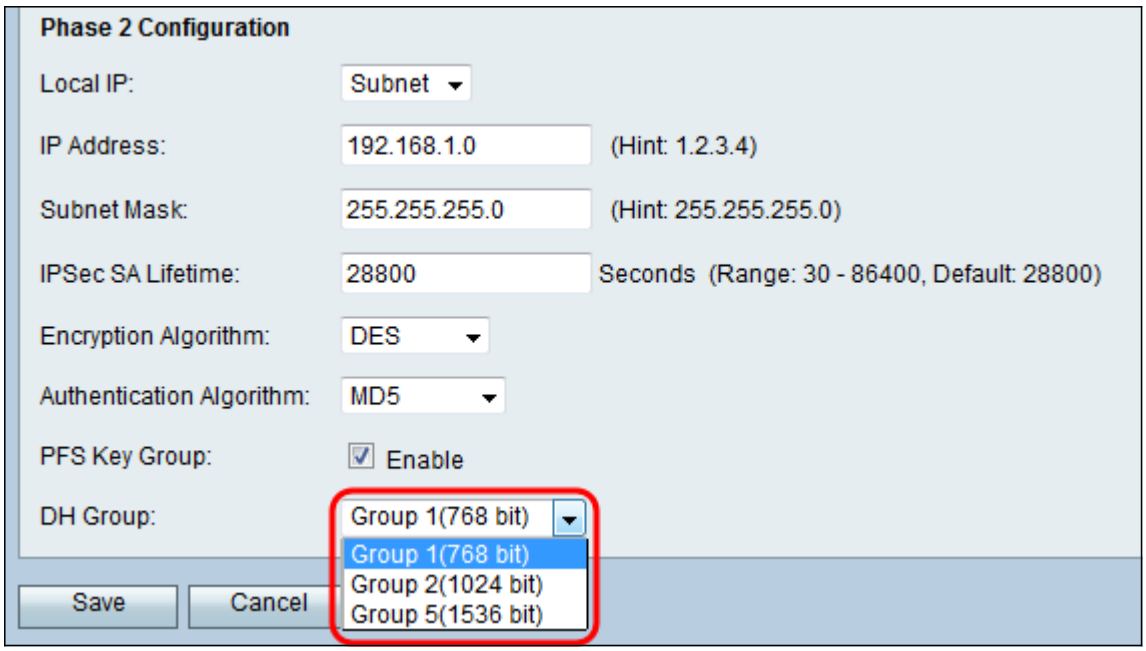
·SHA-1 — SHA-1 is een one-way hashing algoritme dat een 160-bit samenvatting produceert. SHA-1 verwerkt langzamer dan MD5, maar is veiliger dan MD5.

·SHA2-256 — Specificeert het Secure Hash-algoritme SHA2 met de 256-bits samenvatting.

Stap 16. (Optioneel) Selecteer in het veld *PFS-sleutelgroep* het selectievakje **Inschakelen**. Perfect Forward Secrecy (PFS) creëert een extra beveiligingslaag voor de bescherming van uw gegevens door een nieuwe DH-sleutel in fase 2 te waarborgen. Het proces wordt uitgevoerd voor het geval dat de DH-sleutel die in fase 1 wordt gegenereerd tijdens het transport wordt gecompromitteerd.



Stap 17. Kies uit de vervolgkeuzelijst *DH Group* de juiste Diffie-Hellman (DH) groep die in fase 2 met de toets moet worden gebruikt.



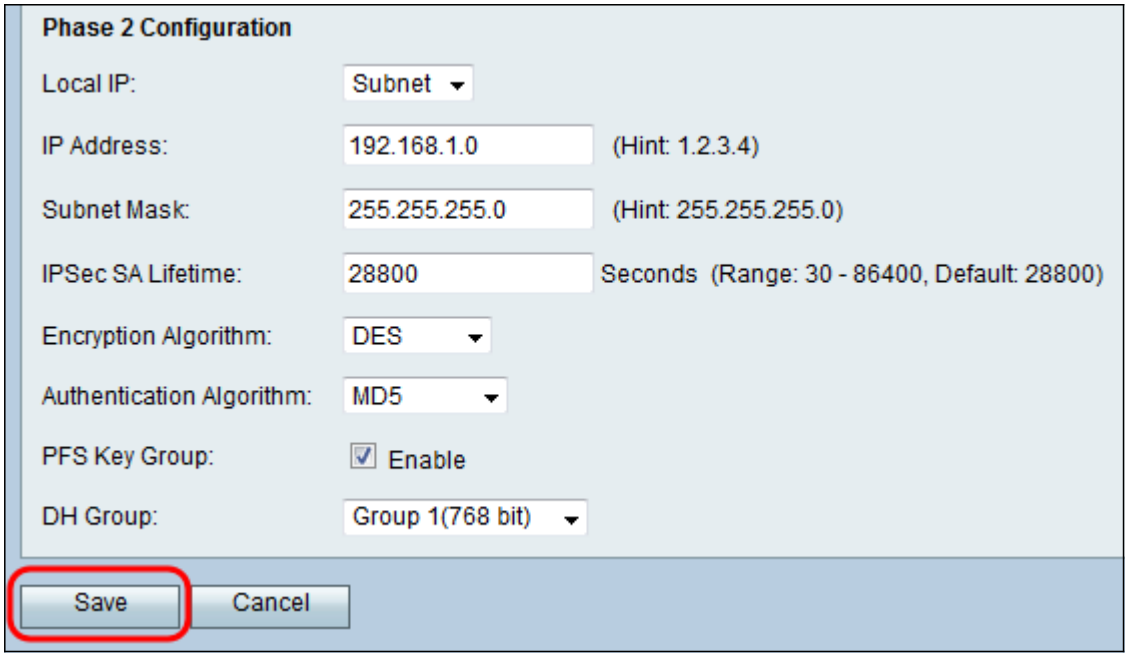
De beschikbare opties zijn als volgt gedefinieerd:

·Group1 (768 bit) — berekent de sleutel het snelst, maar is de minst beveiligde.

·Groep2 (1024 bit) — berekent de sleutel langzamer, maar is veiliger dan groep1.

·Groep 5 (1536 bit) — berekent de sleutel met de langzaamste, maar is de veiligste.

Stap 18. Klik op **Opslaan** om de instellingen op te slaan.



Kijk voor meer informatie op de volgende documentatie:

- RV130-gegevensblad - verklaart de VPN-mogelijkheden voor de RV130-Series routers
- RV130-productpagina - bevat koppelingen voor alle RV130-artikelen van Cisco

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.