Een zachte VPN-client configureren met RV160 en RV260

Doel

Het doel van dit document is om u te tonen hoe u de vereiste instellingen kunt configureren om een korte VPN-client aan te sluiten via RV160 of RV260 Series routers.

Inleiding aan de basisbeginselen van VPN

Een Virtual Private Network (VPN) is een goede manier om externe gebruikers te verbinden met een beveiligd netwerk. Het voert een versleutelde verbinding in via een minder beveiligd netwerk als het internet.

Een VPN-tunnel stelt een privaat netwerk in dat gegevens veilig kan verzenden met behulp van encryptie en verificatie. Bedrijven maken gebruik vaak van een VPN-verbinding omdat het zowel nuttig als noodzakelijk is om hun werknemers toegang te geven tot hun interne bronnen, zelfs als ze niet op kantoor zijn.

De RV160-router ondersteunt tot 10 VPN-tunnels en RV260 ondersteunt tot 20 tunnels.

Dit artikel zal u door de stappen lopen die nodig zijn om de RV160/RV260-router en de snelle VPN-client tonen. U leert hoe u een gebruikersgroep, gebruikersaccount, IPsec-profiel en client-naar-site profiel kunt maken. Op de client Shrew Soft VPN leert u hoe u de tabbladen General, Client, Name Resolutie, Verificatie, Fase 1 en Fase 2 kunt configureren.

Wat zijn de Pros en Cons als ik een VPN wil gebruiken?

VPN's behandelen casescenario's voor reëel gebruik die veel industrieën en bedrijfstypen gemeen hebben. De onderstaande tabel toont een aantal voor- en nadelen van het gebruik van een VPN.

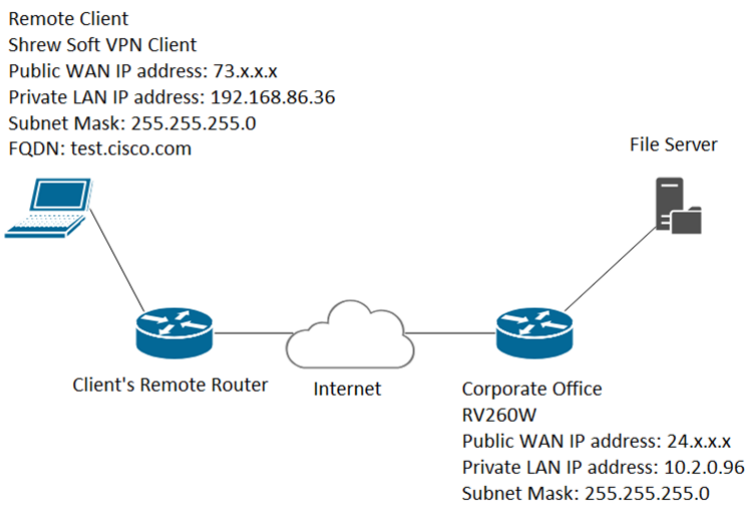
Pros	Cons
Biedt veilige communicatie, gemak en toegankelijkheid met toegangsrechten die op individuele gebruikers zijn afgestemd, zoals werknemers, aannemers of partners.	Lage verbindingssnelheid kan voorkomen. Een sterkere encryptie kost tijd en middelen om anonimiteit zowel als veiligheid te waarborgen. De encryptie van netwerkverkeer vereist gewoonlijk een beetje meer overhead. Je kunt een paar VPN providers vinden die een goede connectiviteitssnelheid behouden, terwijl ze anonimiteit en beveiliging bewaren, maar meestal betaalde services.
Verbetert de productiviteit door het netwerk en de toepassingen	Potentieel veiligheidsrisico door misverstanden. Het ontwerpen en

van bedrijven uit te breiden.	implementeren van een VPN kan gecompliceerd zijn. Het is noodzakelijk om een ervaren professional in te schakelen om uw VPN-netwerk te configureren om er zeker van te zijn dat het netwerk niet gecompromitteerd wordt.
Vermindert communicatiekosten en verhoogt de flexibiliteit.	Als er een situatie is waarin er een nieuwe infrastructuur of een nieuwe reeks configuraties moet worden toegevoegd, kunnen technische problemen ontstaan door onverenigbaarheid, vooral als er andere producten of verkopers bij betrokken zijn dan de producten die u al gebruikt.
De werkelijke geografische locatie van de gebruikers is beschermd en is niet blootgesteld aan het publiek of aan gedeelde netwerken zoals het internet.	
Bescherm vertrouwelijke netwerkgegevens en -bronnen.	
Een VPN kan nieuwe gebruikers of een groep gebruikers toevoegen zonder dat u extra onderdelen of een gecompliceerde configuratie nodig hebt.	

Topologie

Dit is een eenvoudige topologie van het netwerk.

Opmerking: Het openbare WAN IP-adres is leeg.



Toepasselijke apparaten

RV160

RV260

Softwareversie

1.0.0.xx (RV160 en RV260)

2.2.1 wordt aanbevolen omdat 2.2.2 problemen met de connectiviteit kunnen hebben met onze routers (Verkrijg de zachte VPN-client)

Inhoud

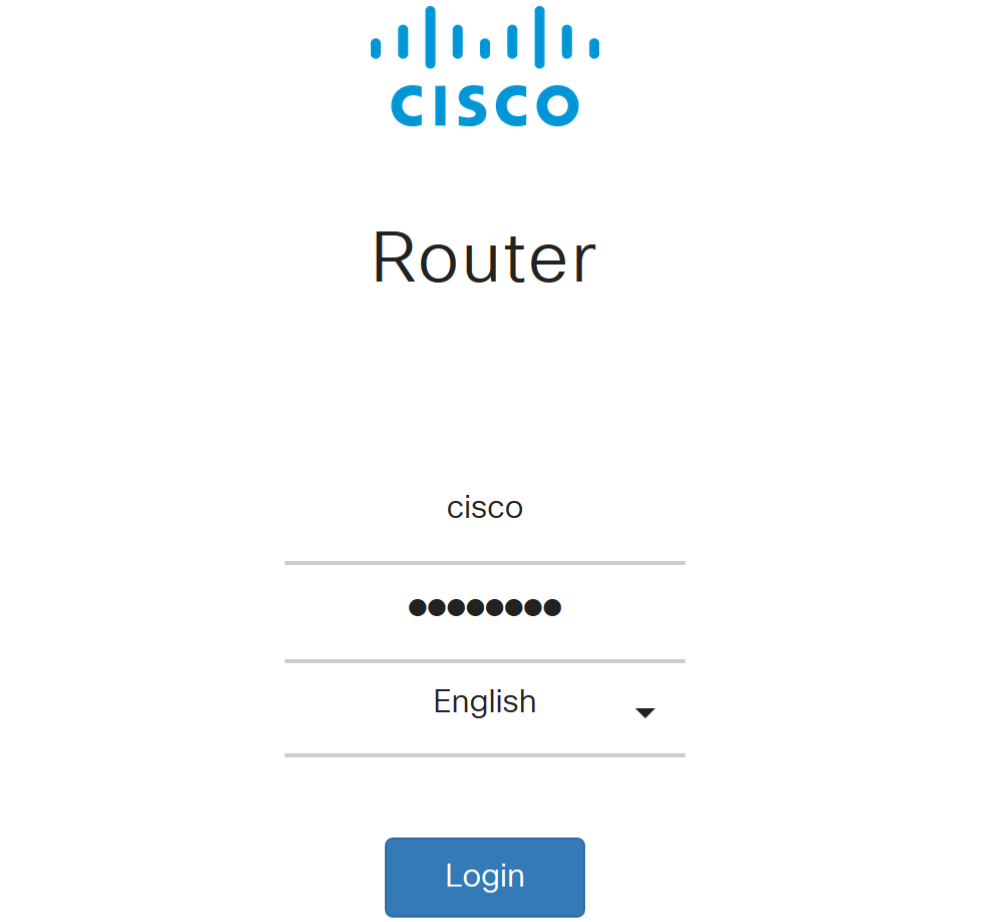
1. Gebruikersgroepen maken
2. Gebruikersrekeningen maken
3. IPsec-profiel configureren
4. Client-to-Site configureren
5. Een zachte VPN-client configureren
6. Een zachte VPN-client tonen: tabblad Algemeen
7. Een zachte VPN-client tonen: Clienttabblad
8. Een zachte VPN-client tonen: Tabblad Resolutie naam
9. Een zachte VPN-client tonen: Tabblad Verificatie
10. Een zachte VPN-client tonen: Tabblad Fase 1
11. Een zachte VPN-client tonen: Tabblad Fase 2
12. Een zachte VPN-client tonen: Aansluiten
13. Tips voor het oplossen van VPN-verbinding
14. Verificatie
15. Conclusie

Gebruikersgroepen maken

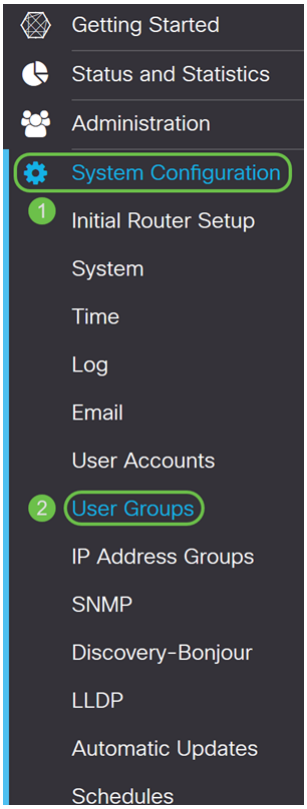
Belangrijke opmerking: Laat de standaard-beheeraccount in de beheergroep achter en maak een nieuwe gebruikersaccount en gebruikersgroep voor Shrew Soft. Als u uw Admin-

account naar een andere groep verplaatst, voorkomt u dat u zich in de router registreert.

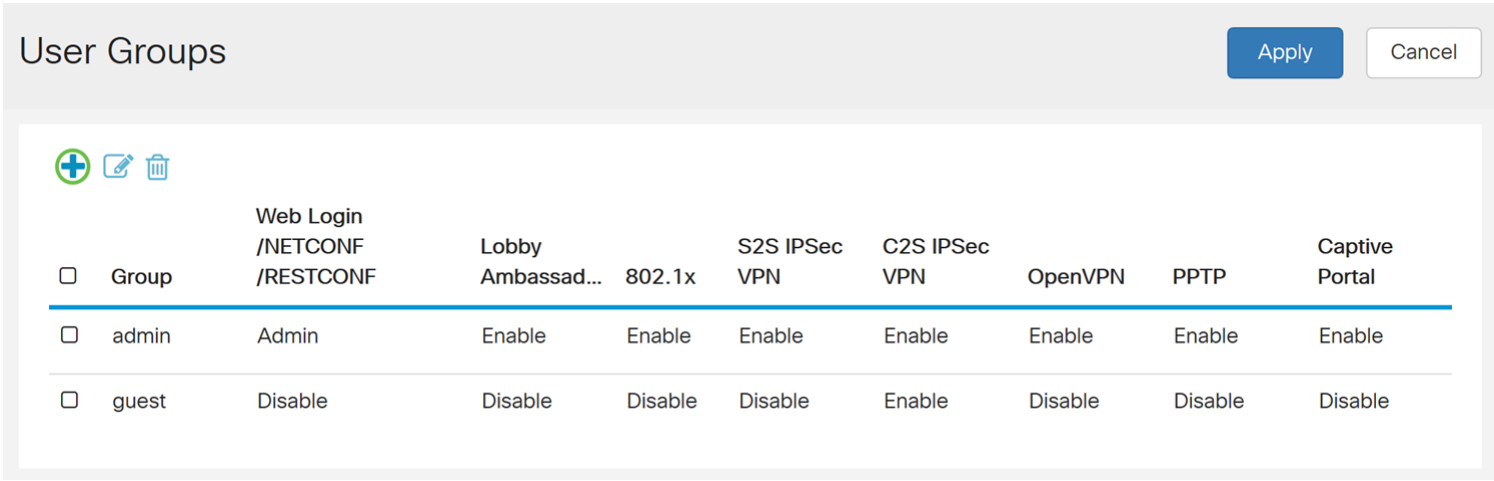
Stap 1. Meld u aan bij de webconfiguratie.



Stap 2. Navigeer naar **systeemconfiguratie > gebruikersgroepen**.

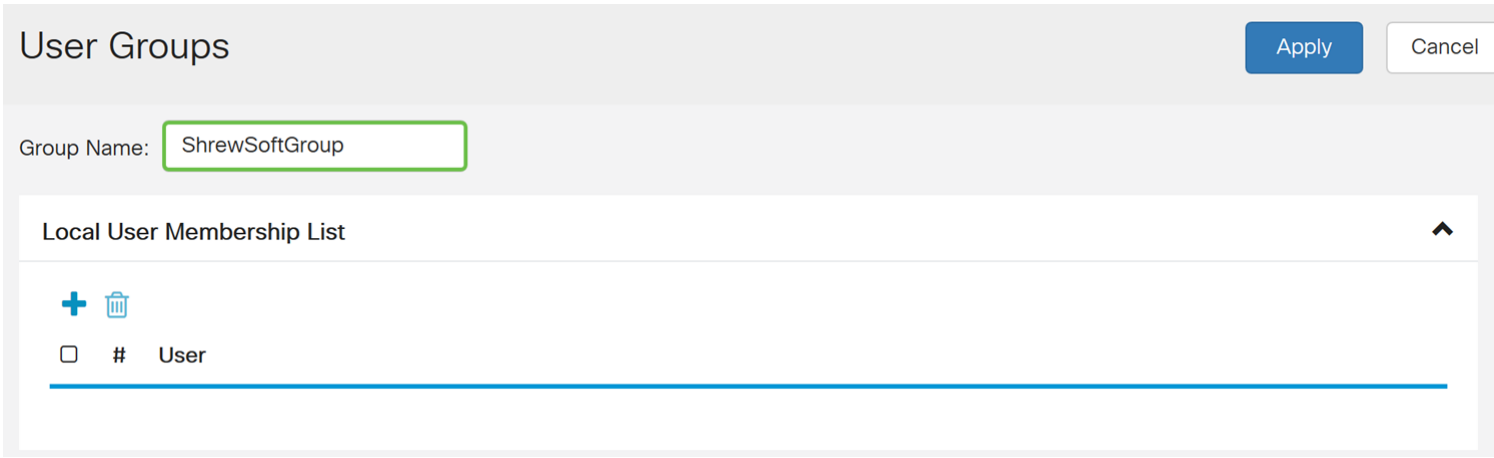


Stap 3. Klik op het pictogram **plus** om een nieuwe gebruikersgroep toe te voegen.

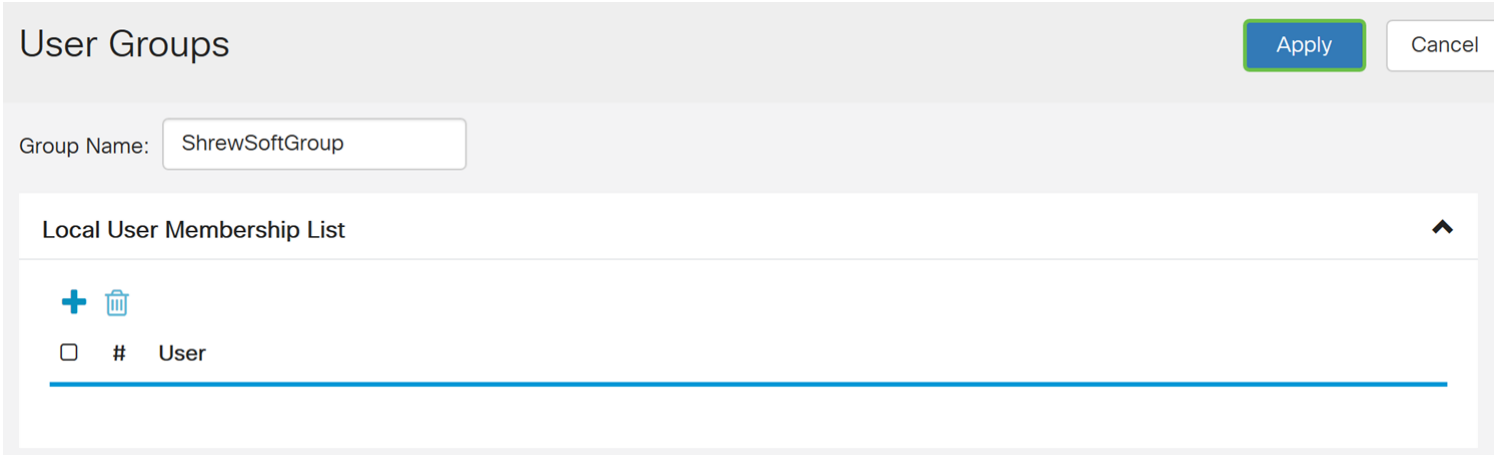


Stap 4. Voer een naam in voor de groep in het veld *groepsnaam*.

We gebruiken **ShrewSoftGroup** als voorbeeld.

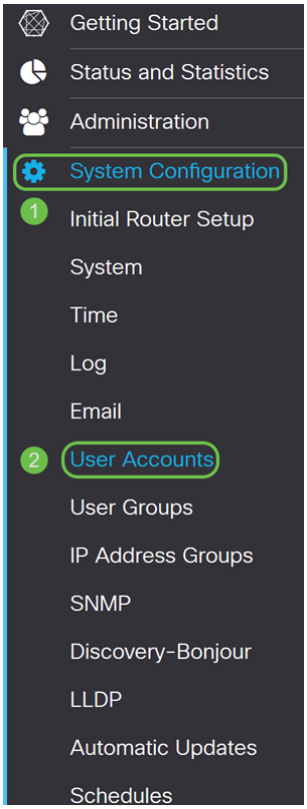


Stap 5. Druk op **Toepassen** om een nieuwe groep te maken.

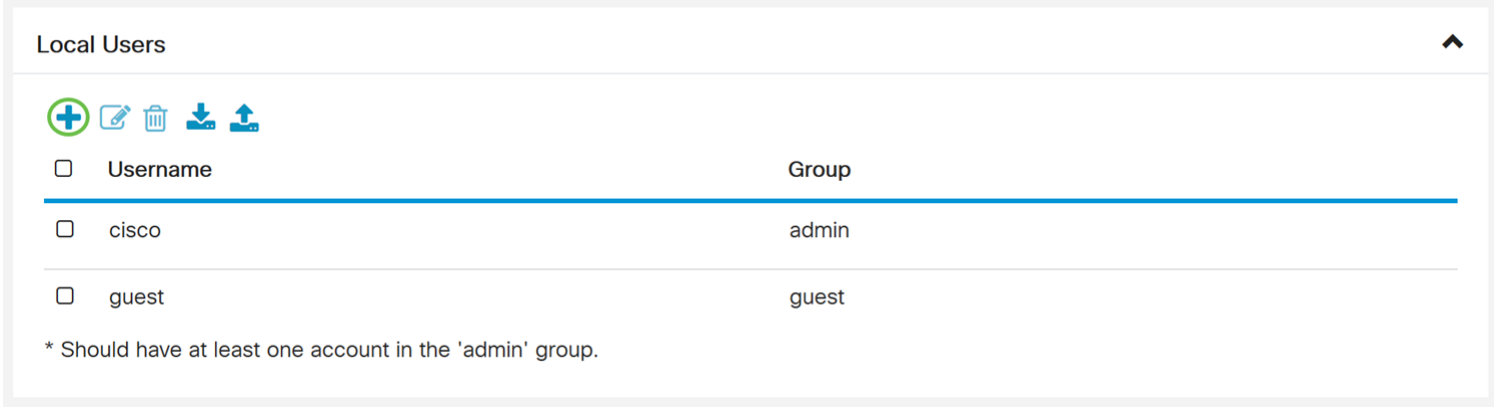


Gebruikersrekeningen maken

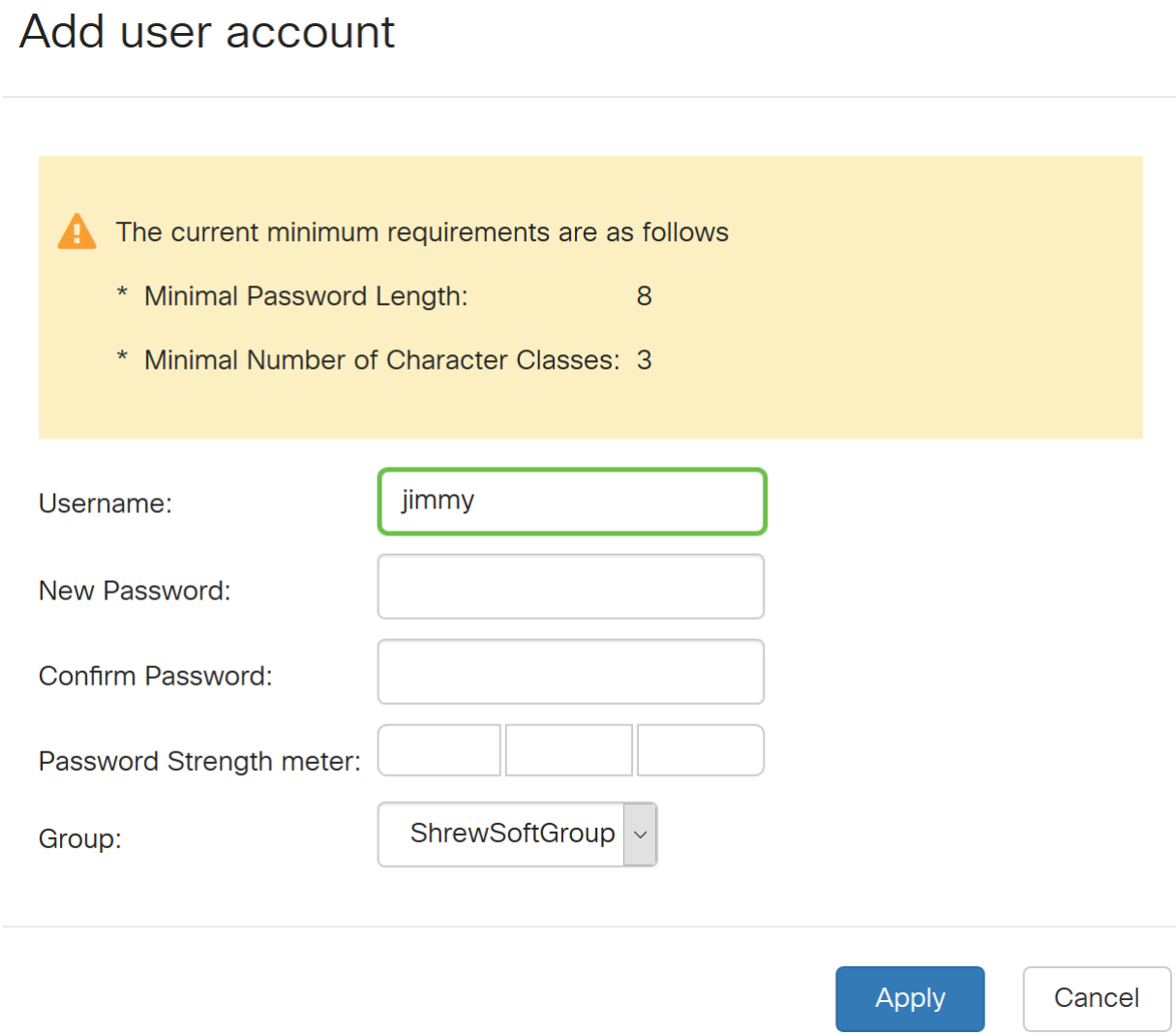
Stap 1. Navigeer naar **systeemconfiguratie > Gebruikersrekeningen**.



Stap 2. Scrolt naar de tabel *van lokale gebruikers* en druk op het pictogram **plus** om een nieuwe gebruiker toe te voegen.

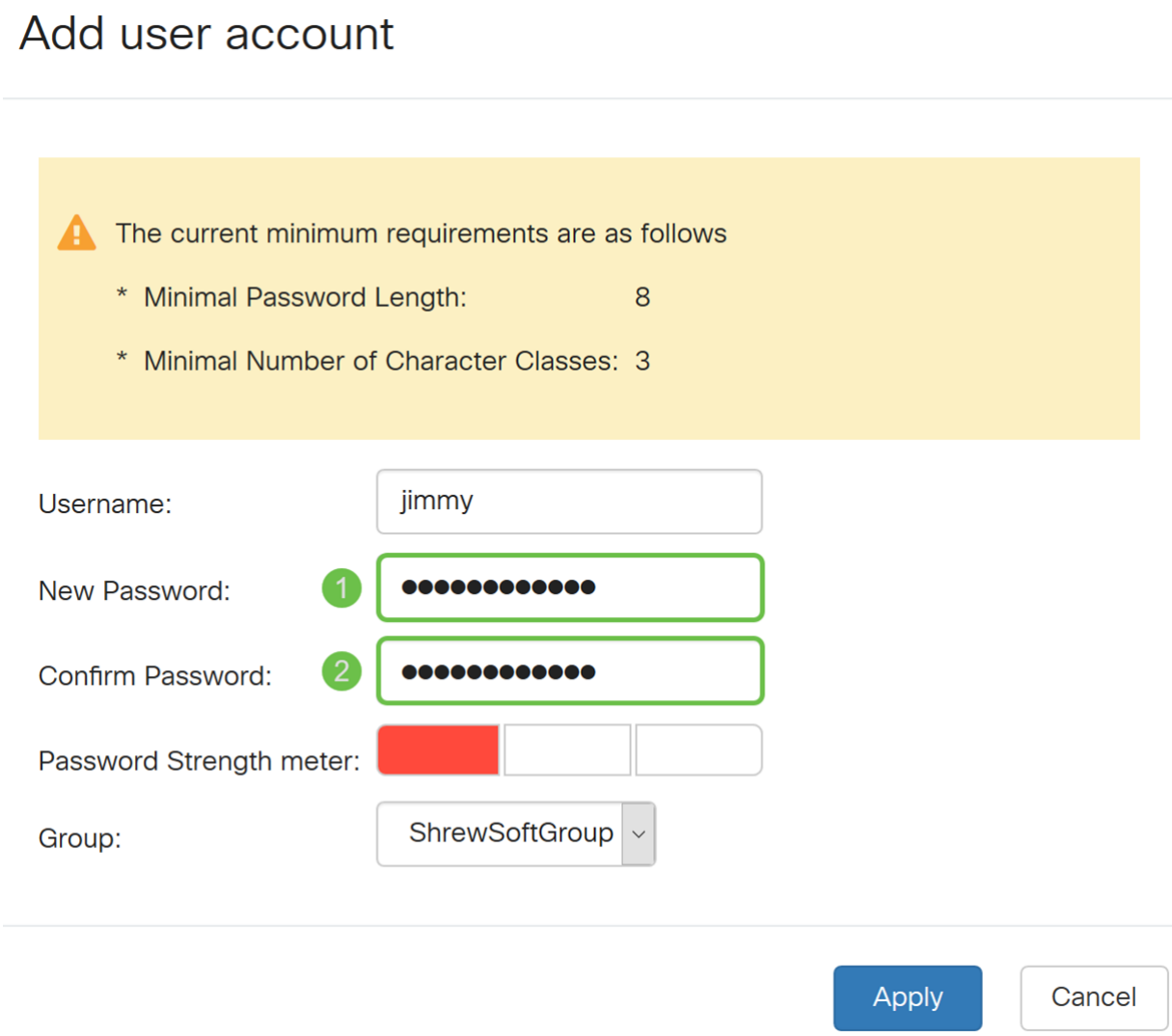


Stap 3. De pagina *gebruikersrekeningen toevoegen* wordt geopend. Voer een gebruikersnaam in voor de gebruiker.

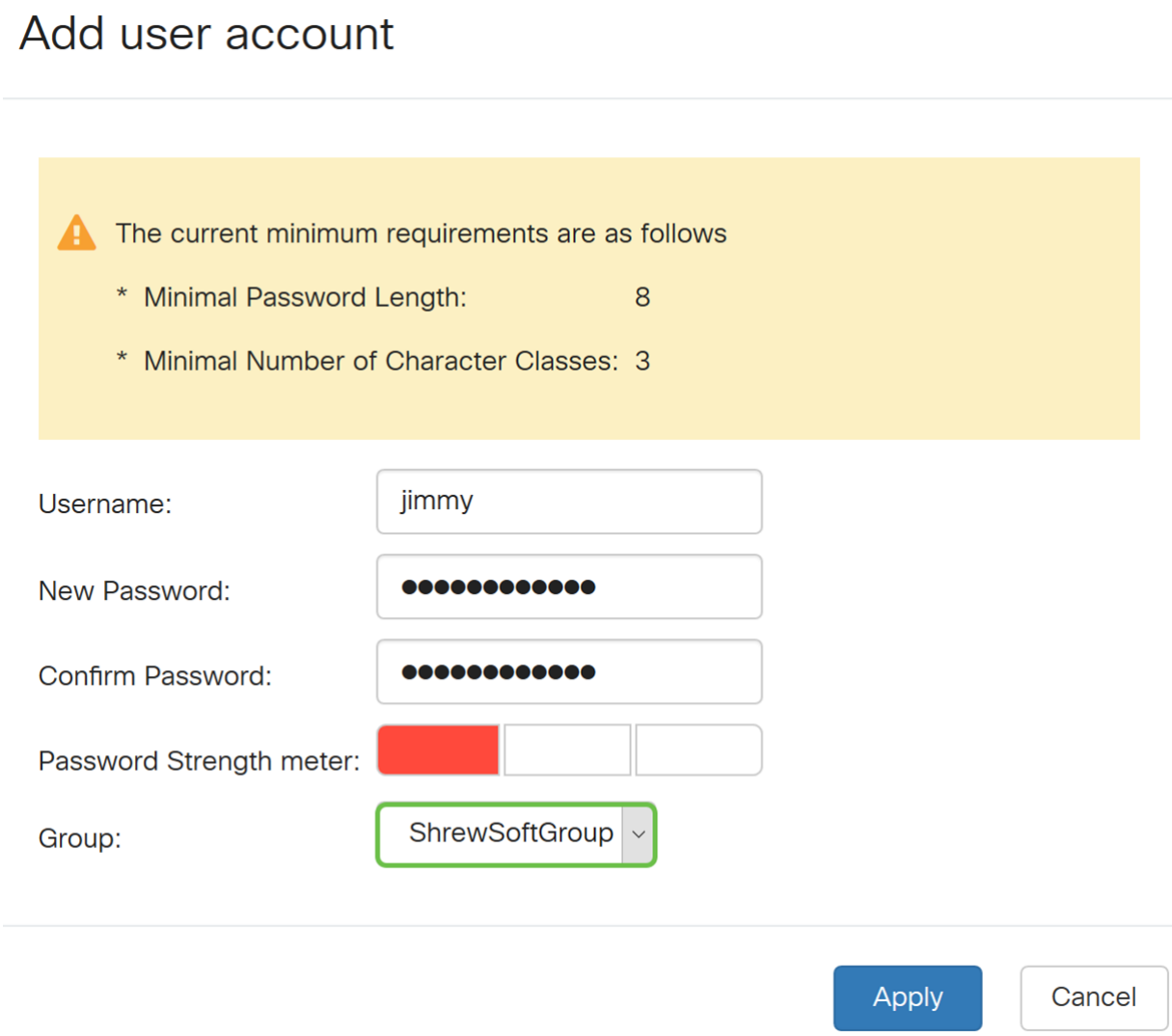


Stap 4. Voer een wachtwoord in het veld *Nieuw wachtwoord* in. Voer hetzelfde wachtwoord opnieuw in het veld *Wachtwoord bevestigen*. In dit voorbeeld zullen we **CiscoTest123** als wachtwoord gebruiken.

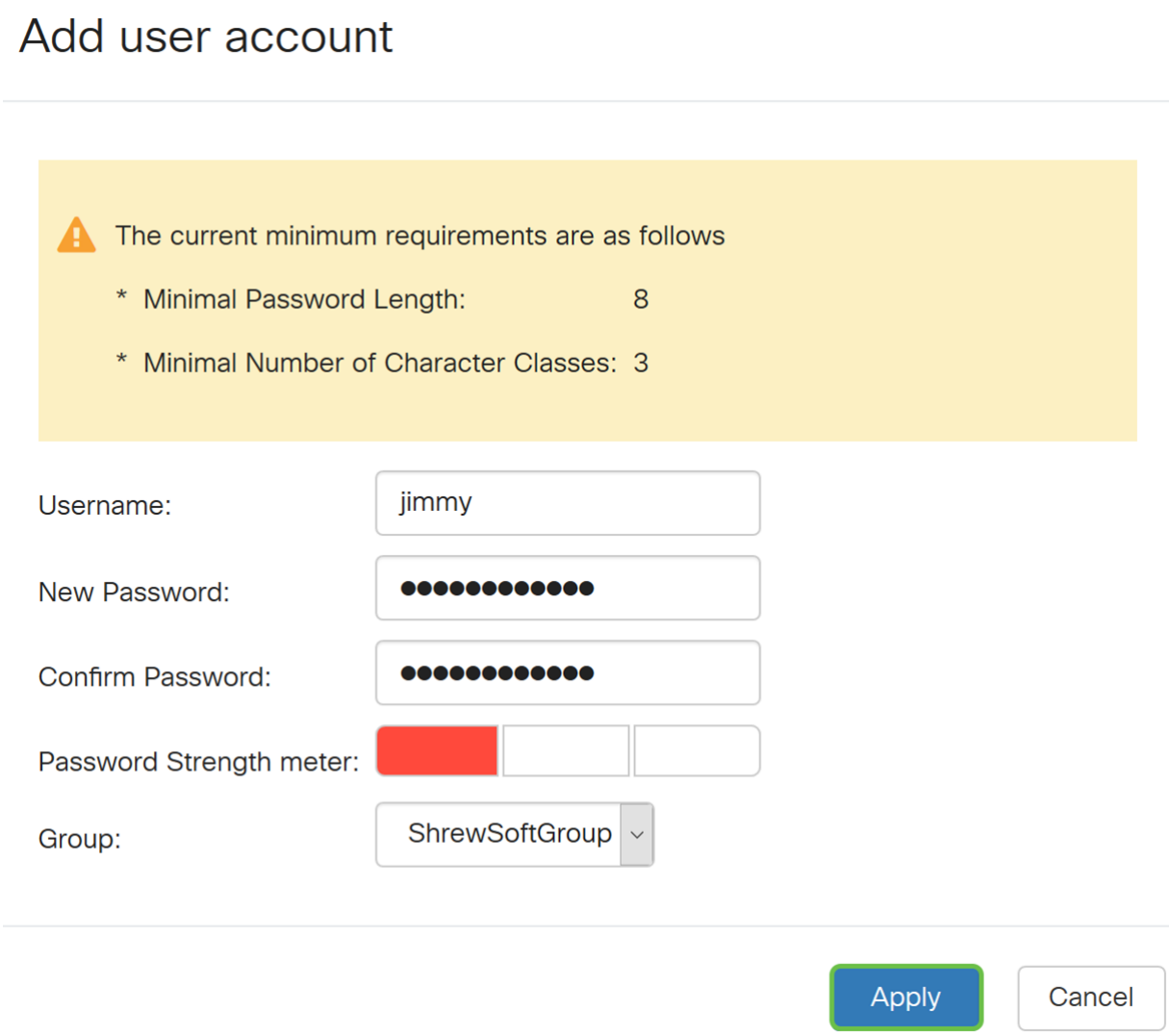
Opmerking: Het wachtwoord dat hier wordt gebruikt is bijvoorbeeld een voorbeeld. Aanbevolen wordt om uw wachtwoord complexer te maken.



Stap 5. Selecteer in de vervolgkeuzelijst *Groep* een groep waarin u de gebruiker wilt plaatsen.

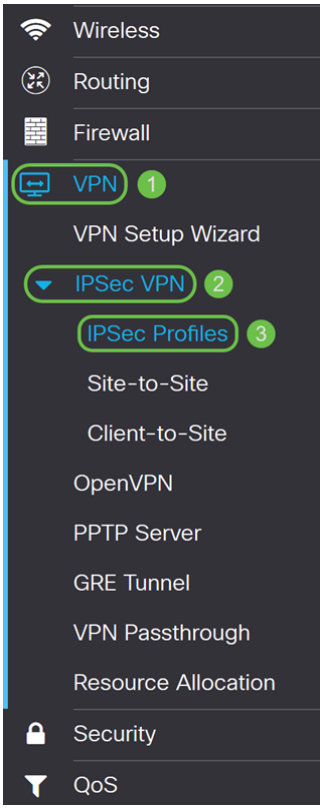


Stap 6. Druk op **Toepassen** om een nieuwe gebruikersaccount te maken.



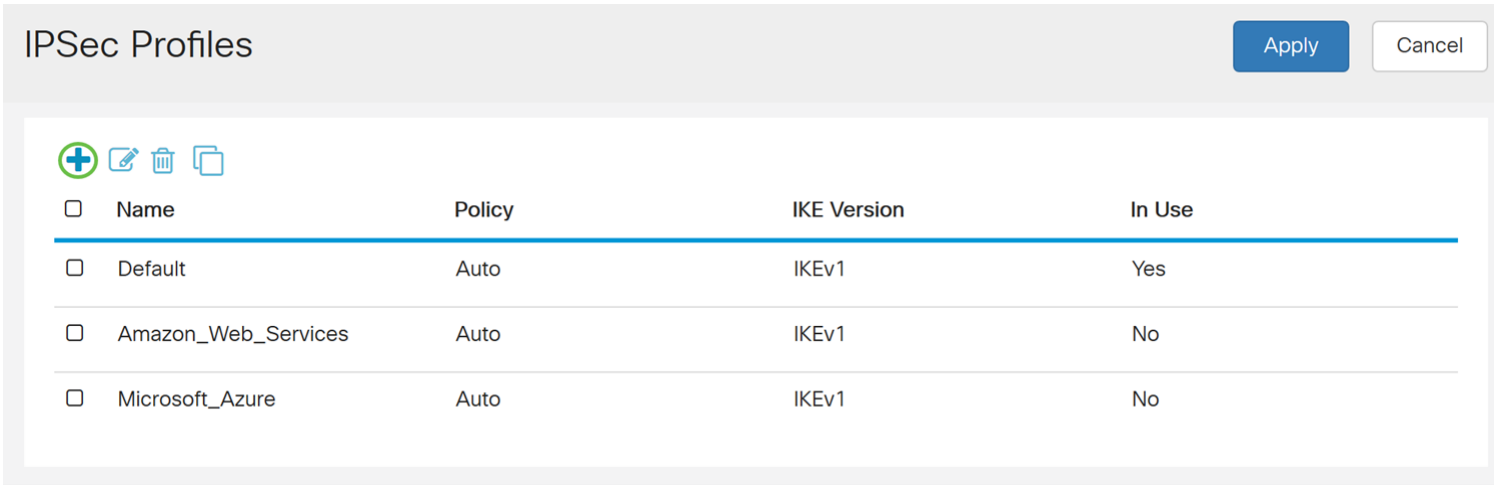
IPsec-profiel configureren

Stap 1. Navigeer naar **VPN > IPSec VPN > IPSec VPN-profielen**.

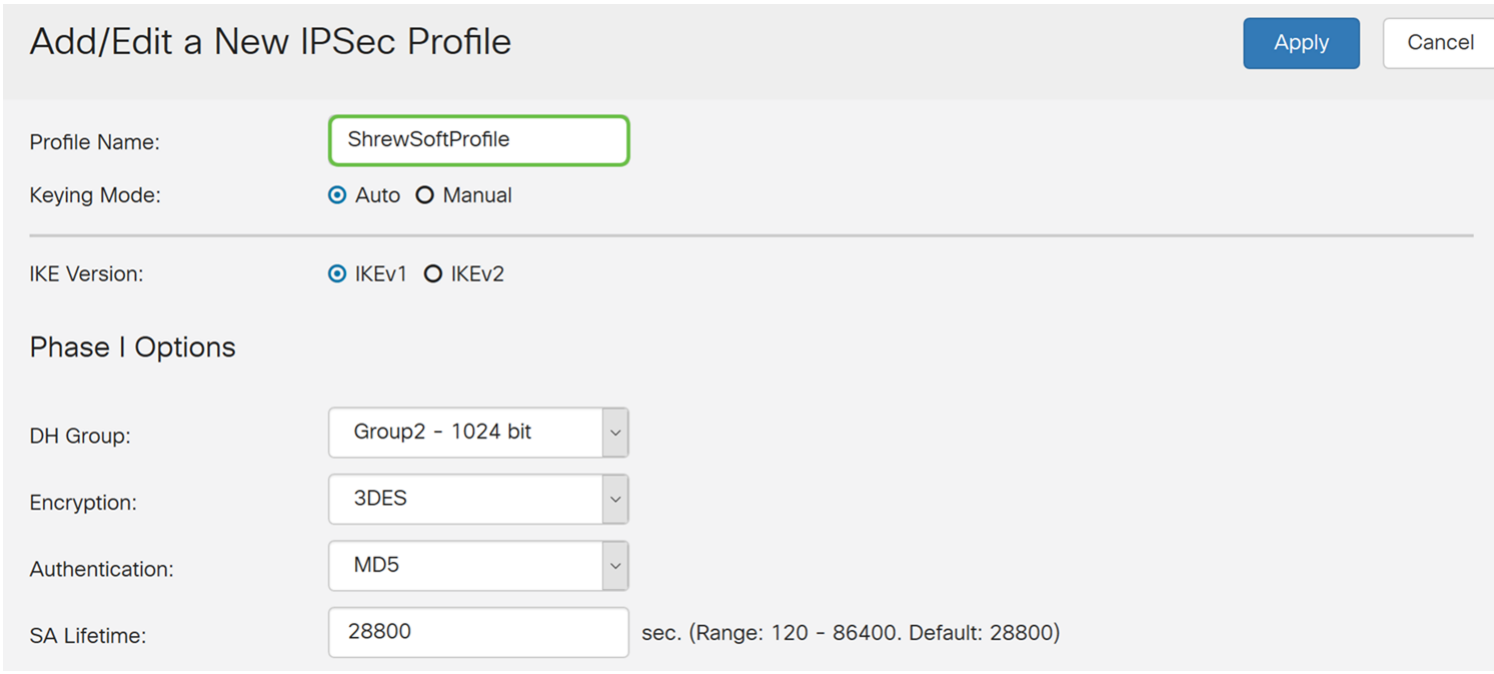


Opmerking: Voor meer uitleg over het configureren van IPsec-profielen klikt u op de link om het artikel te zien: [IPsec-profielen configureren (Auto Keying Mode) op de RV160 en RV260]

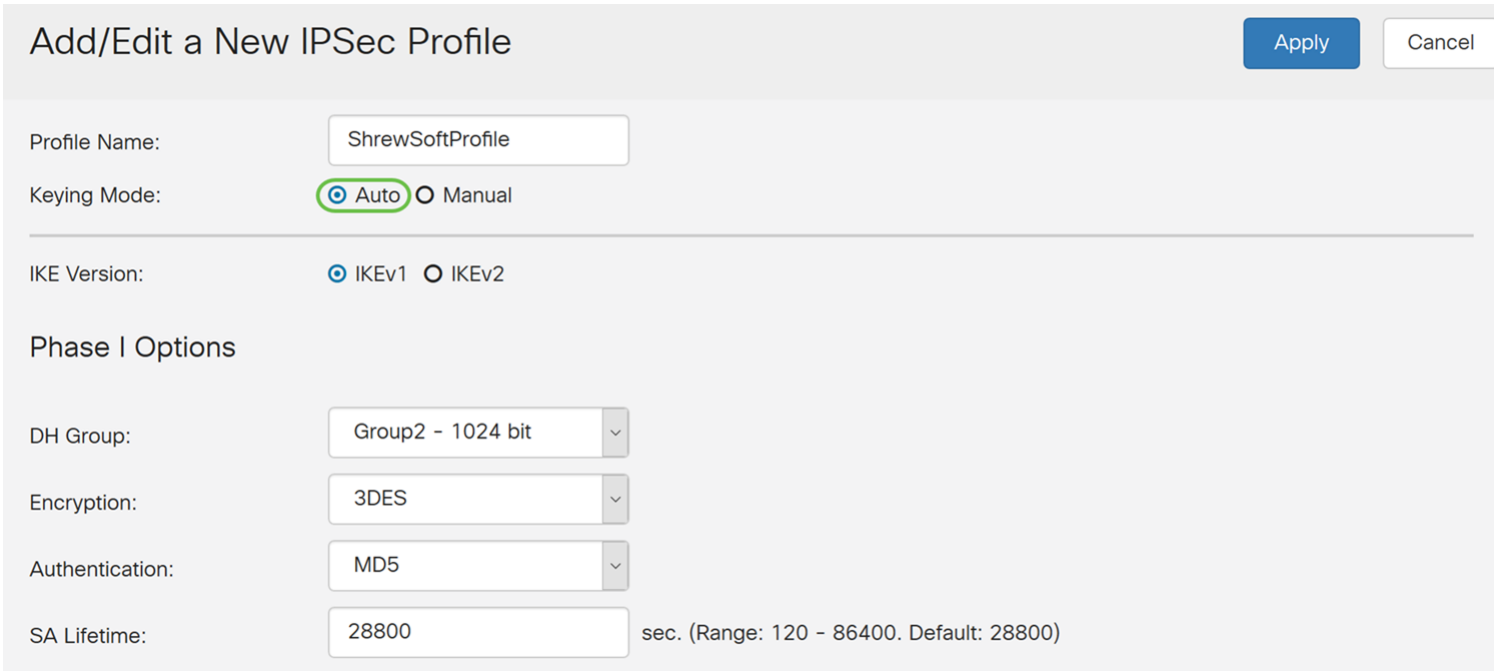
Stap 2. Klik op het pictogram **plus** om een nieuw IPsec-profiel toe te voegen.



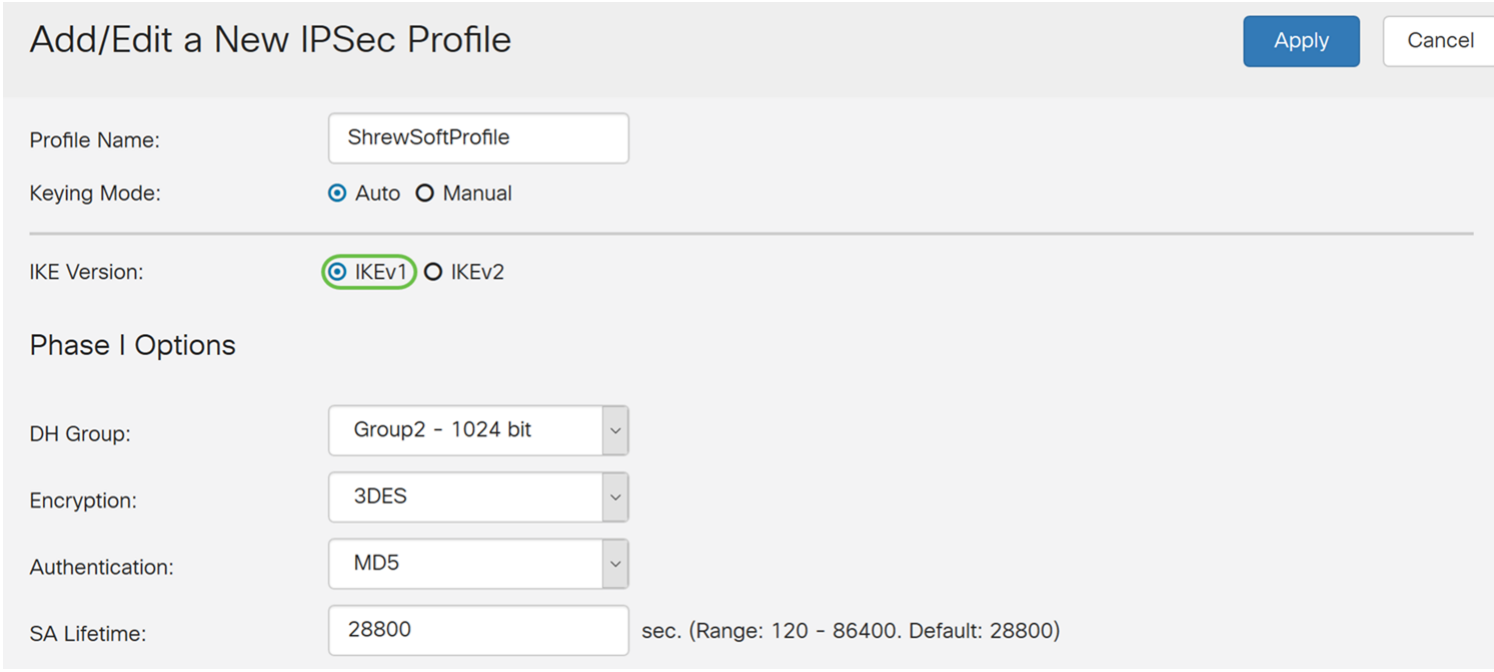
Stap 3. Voer een naam voor het profiel in het veld *Profile Name*. We voeren **ShrewSoftProfile in** als onze profielnaam.



Stap 4. Selecteer **Auto** voor *het toetsenbord*.



Stap 5. Selecteer **IKEv1** of **IKEv2** als *IKE versie*. In dit voorbeeld werd IKEv1 geselecteerd.



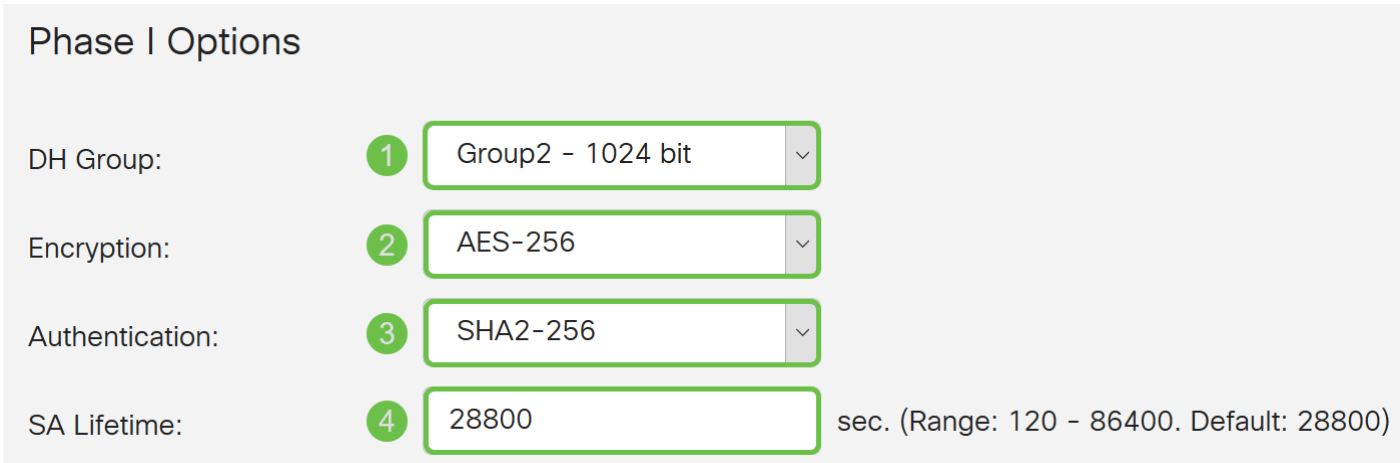
Stap 6. In het gedeelte *Phase I Opties* hebben we dit artikel ingesteld.

DH-groep: **Group2 - 1024-bits**

Encryptie: **AES-256**

Verificatie: **SHA2-256**

SA Lifetime: **28800**



Stap 7. Onder *Fase II Opties* hebben we dit artikel geconfigureerd.

Protocolselectie: **ESP**

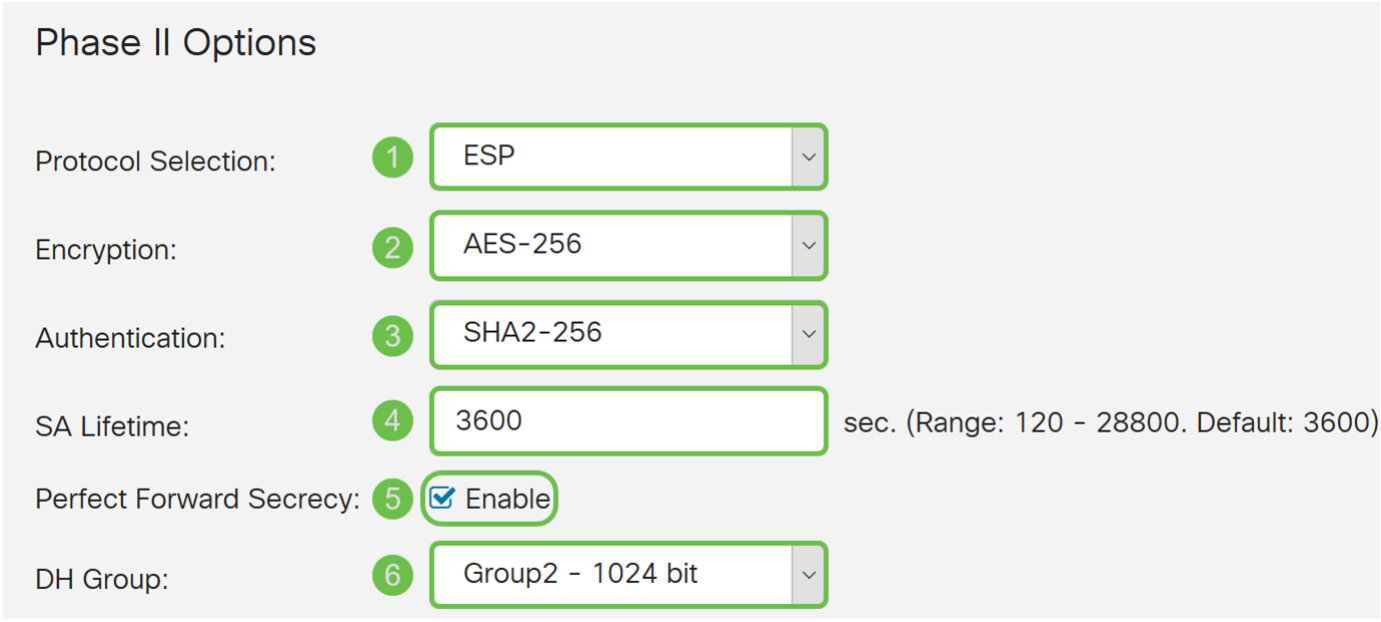
Encryptie: **AES-256**

Verificatie: **SHA2-256**

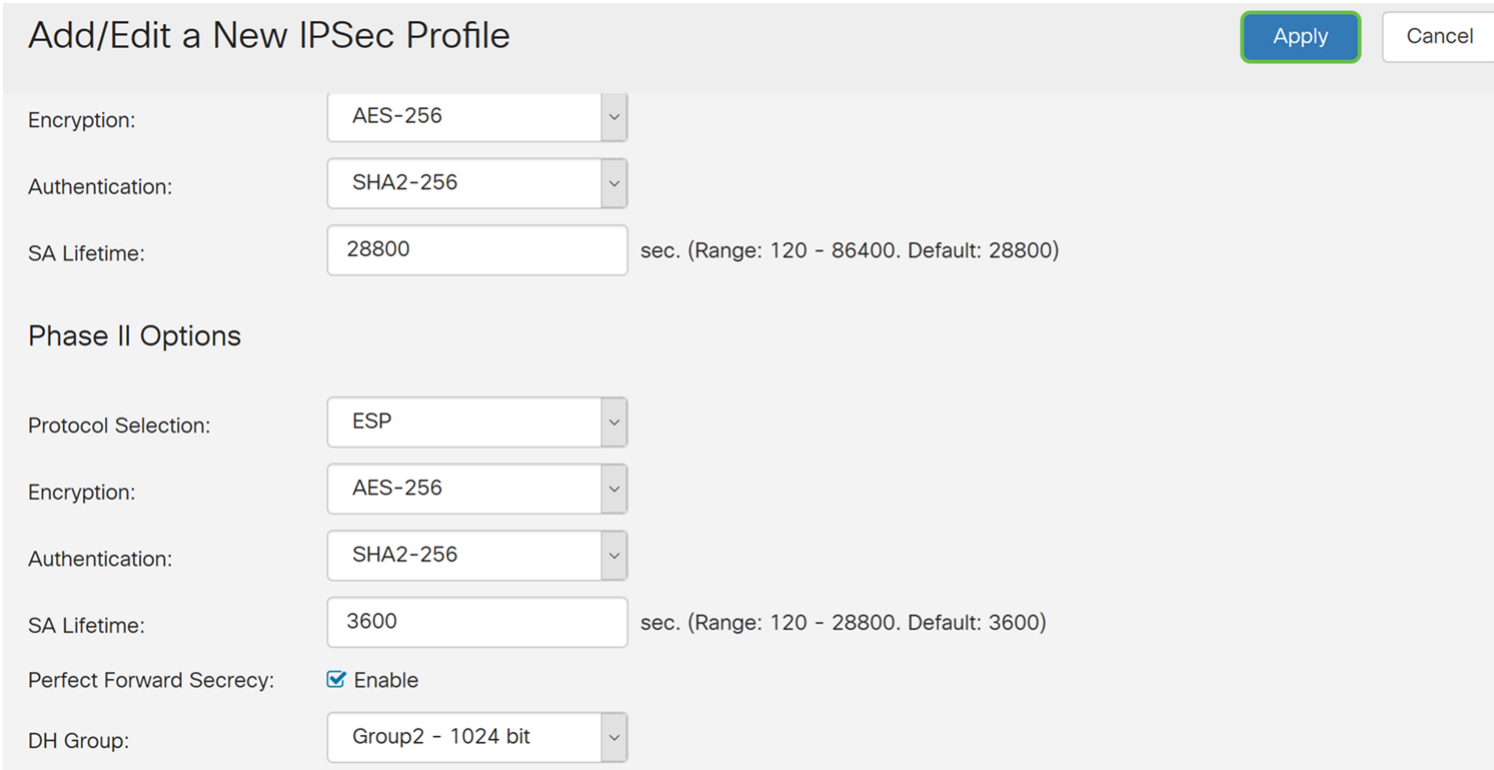
SA Lifetime: **3600**

Perfect voorwaartse geheimhouding: **Ingeschakeld**

DH-groep: **Group2 - 1024-bits**

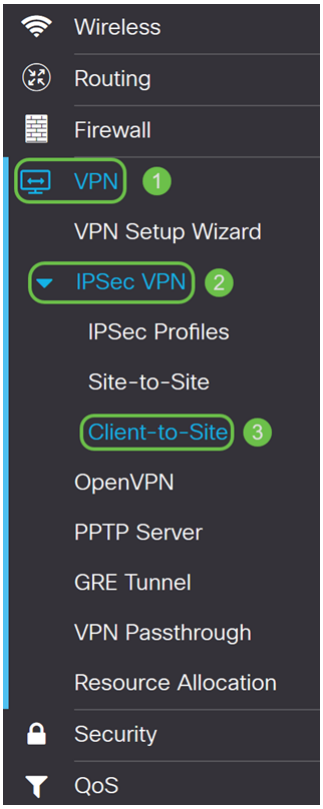


Stap 8. Klik op **Toepassen** om uw nieuwe IPsec-profiel te maken.

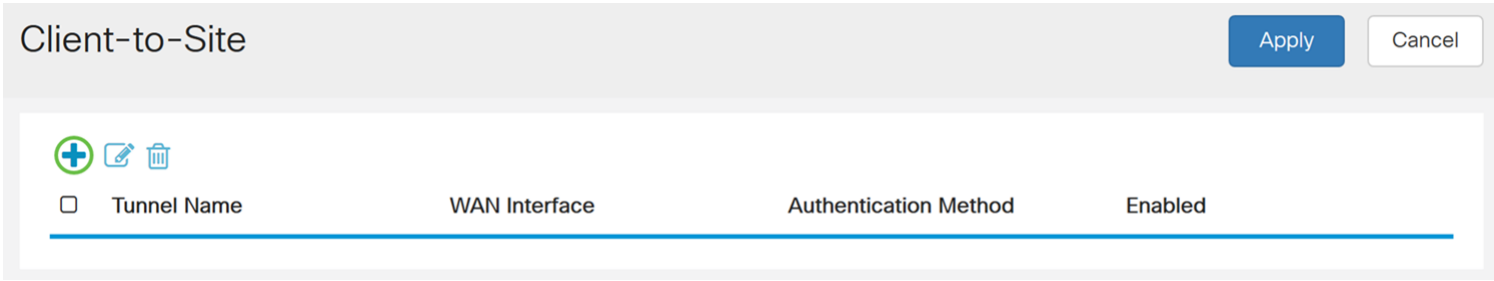


Client-to-Site configureren

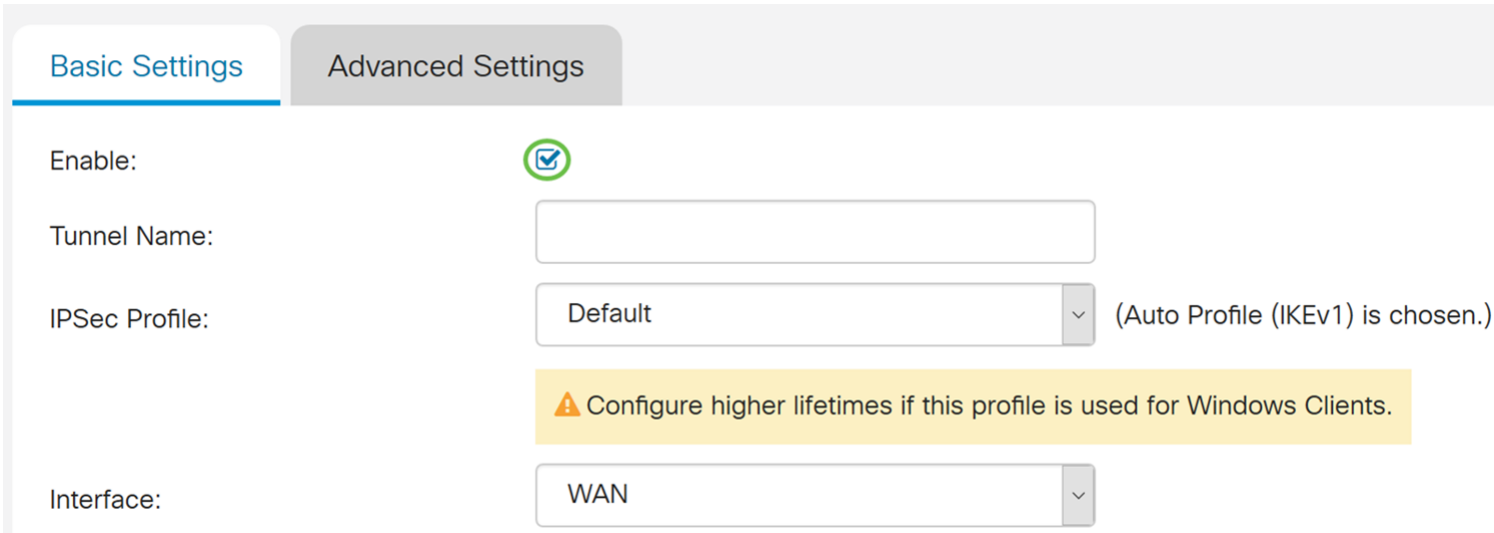
Stap 1. Navigeer naar **VPN > IPSec VPN > Client-to-Site**.



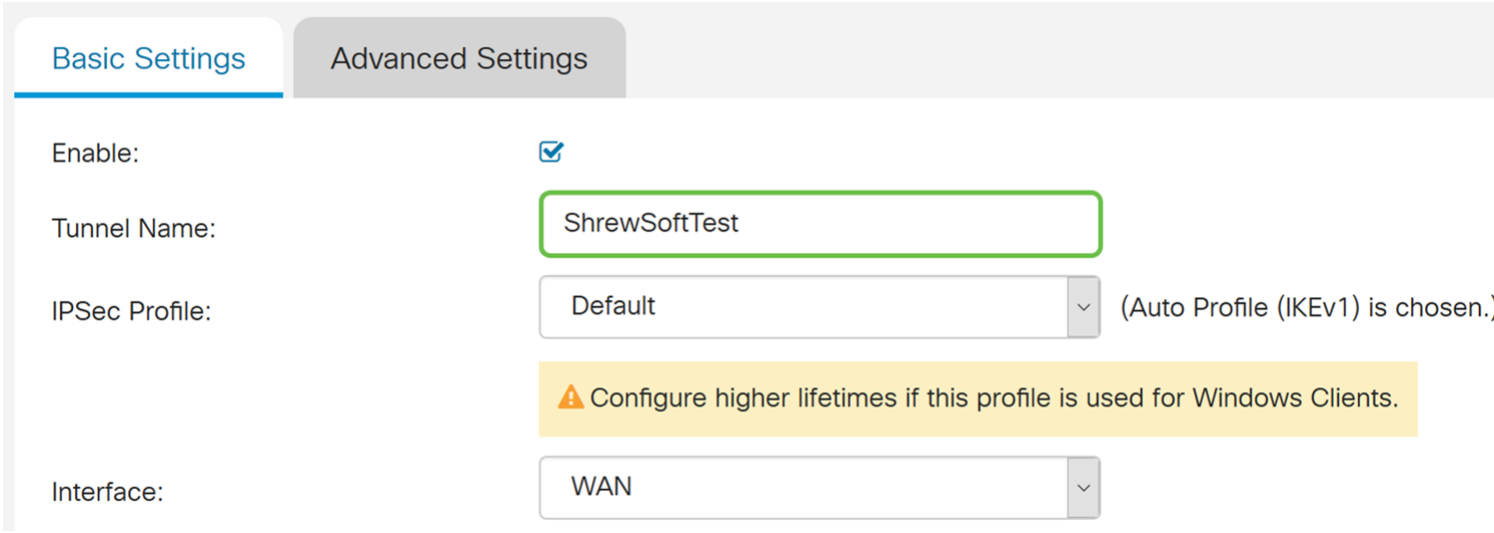
Stap 2. Klik op het pictogram **plus** om een nieuwe tunnel toe te voegen.



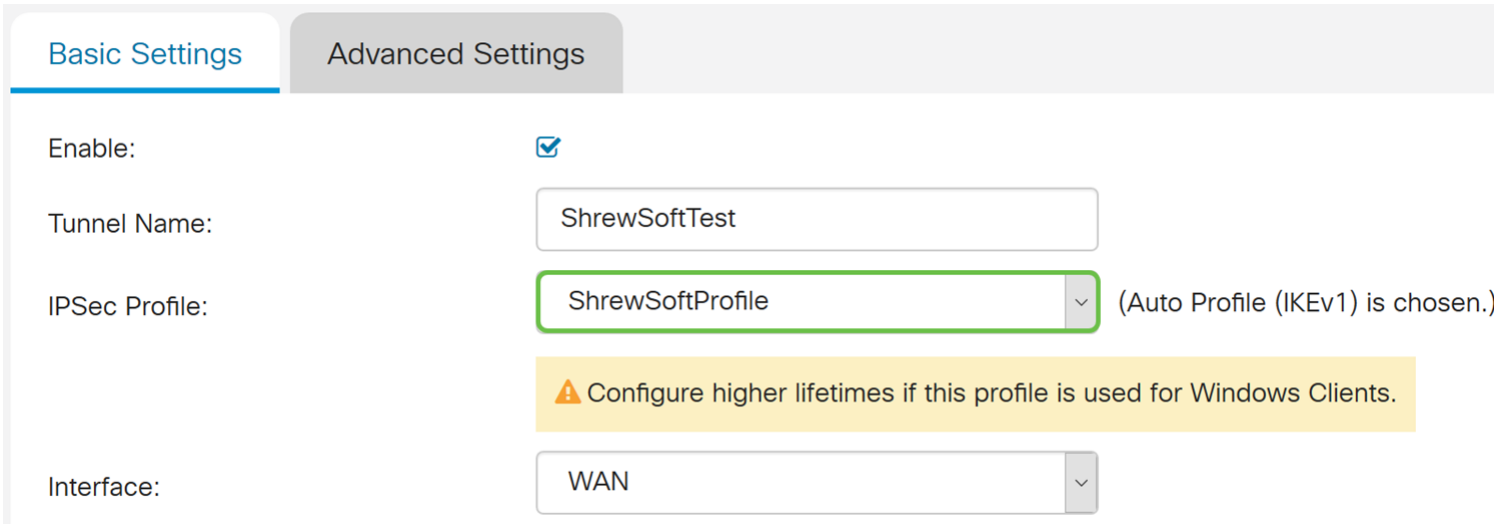
Stap 3. Controleer het selectieteken **Enable** om de tunnel in te schakelen.



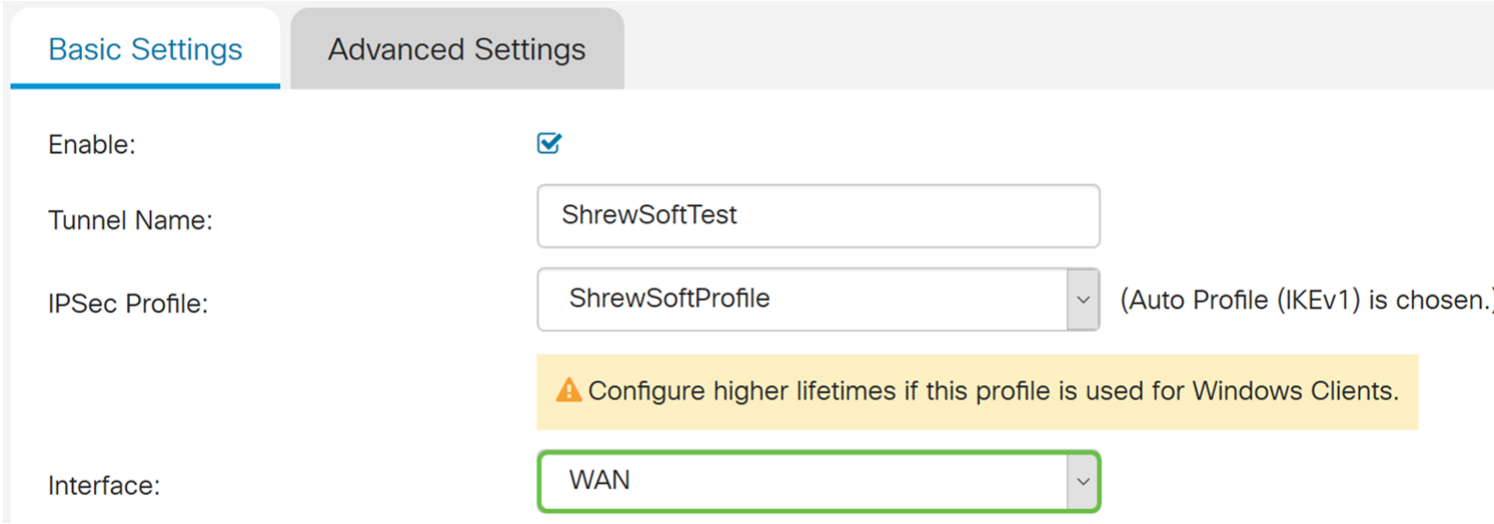
Stap 4. Voer een naam in voor de tunnel in het veld *Tunnelnaam*.



Stap 5. Selecteer in de vervolgkeuzelijst *IPSec Profile* een profiel dat u wilt gebruiken. We selecteren ShrewSoftProfile dat in de vorige sectie werd gemaakt: [IPsec-profiel configureren](#).



Stap 6. Selecteer de gewenste interface in de vervolgkeuzelijst *Interface*. We zullen **WAN** als interface gebruiken om de tunnel aan te sluiten.

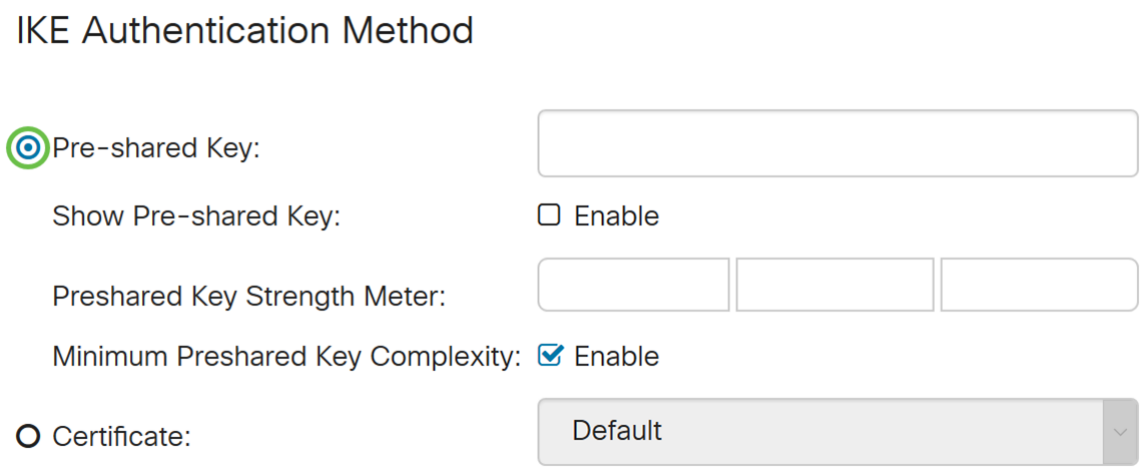


Stap 7. Selecteer onder het gedeelte *IKE-verificatiemethode* de optie *Vooraf gedeelde sleutel* of het *certificaat*. We zullen **Pre-Shared Key** gebruiken als onze IKE-authenticatiemethode.

Opmerking: IKE-peers authenticeren elkaar door gegevens te berekenen en te verzenden

die de voorgedeelde sleutel bevatten. Als het ontvangende peer in staat is om het zelfde hash onafhankelijk te creëren met gebruik van zijn Pre-gedeeld sleutel, weet het dat beide peers het zelfde geheim moeten delen en zo het andere peer authentiek te verklaren. Vooraf gedeelde toetsen schalen niet goed omdat elke IPsec-peer moet worden geconfigureerd met de voorgedeelde toetsen van elk ander peer waarmee het een sessie vastlegt.

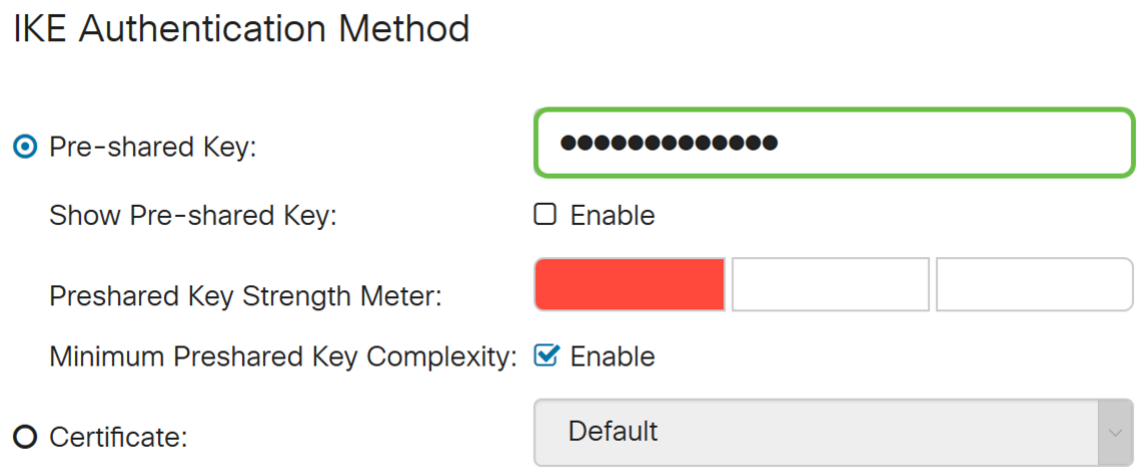
Het certificaat gebruikt een digitaal certificaat dat informatie bevat zoals de naam, het IP-adres, het serienummer, de vervaldatum van het certificaat en een kopie van de openbare sleutel van de houder van het certificaat.



Stap 8. Voer in de Pre-Shared Key in die u wilt gebruiken om te authentiseren. Vooraf gedeelde sleutel kan zijn wat je maar wilt. De vooraf gedeelde toets die is ingesteld op de Shrew Soft VPN-client moet hetzelfde zijn als hier wanneer u de client aanpast.

In dit voorbeeld, zullen we **CiscoTest123** gebruiken**!** als de vooraf gedeelde toets.

Opmerking: De vooraf gedeelde sleutel die hier werd ingevoerd is een voorbeeld. Aanbevolen wordt om een complexere, vooraf gedeelde sleutel in te voeren.



Stap 9. Selecteer het *lokale identificatienummer* in de vervolgkeuzelijst. De volgende opties zijn gedefinieerd als:

Lokale WAN IP - Deze optie gebruikt het IP-adres van de WAN-interface (Wide Area Network) van de VPN-gateway

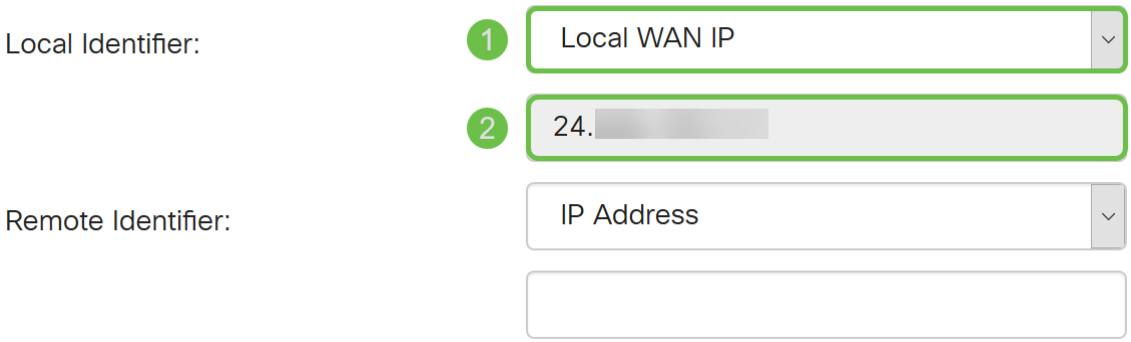
IP-adres - Met deze optie kunt u handmatig een IP-adres voor de VPN-verbinding invoeren. U moet het WAN IP-adres van de router op de website (kantoor) invoeren.

FQDN - Deze optie zal de Full Qualified Domain Name (FQDN) van de router gebruiken wanneer het opzetten van de VPN-verbinding.

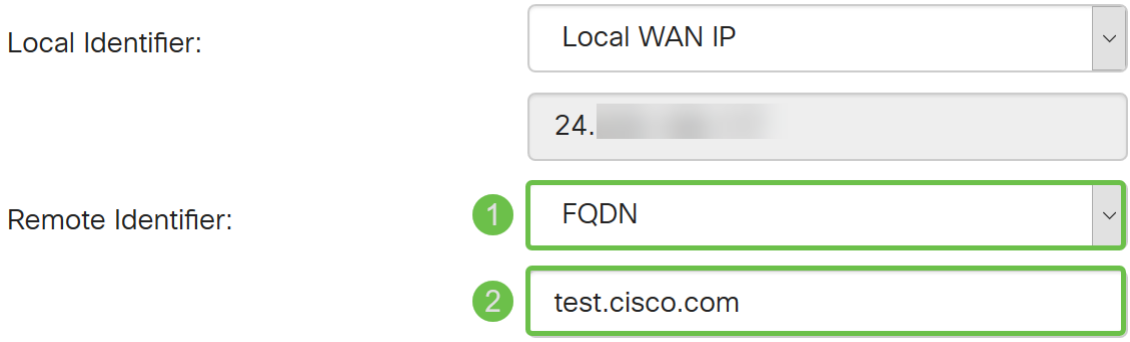
Gebruiker FQDN - Met deze optie kunt u een volledige domeinnaam voor een specifieke gebruiker op het internet gebruiken.

In dit voorbeeld, zullen we **Lokale WAN IP** als lokale identificator selecteren.

Opmerking: Het lokale WAN IP van de router wordt automatisch ingevuld.



Stap 10. In de vervolgkeuzelijst *Remote Identifier*, selecteert u of **IP-adres**, **FQDN**, of **User FQDN**. Typ vervolgens de gewenste reactie uit wat u hebt geselecteerd. In dit voorbeeld zullen we **FQDN** selecteren en **test.cisco.com** invoeren.



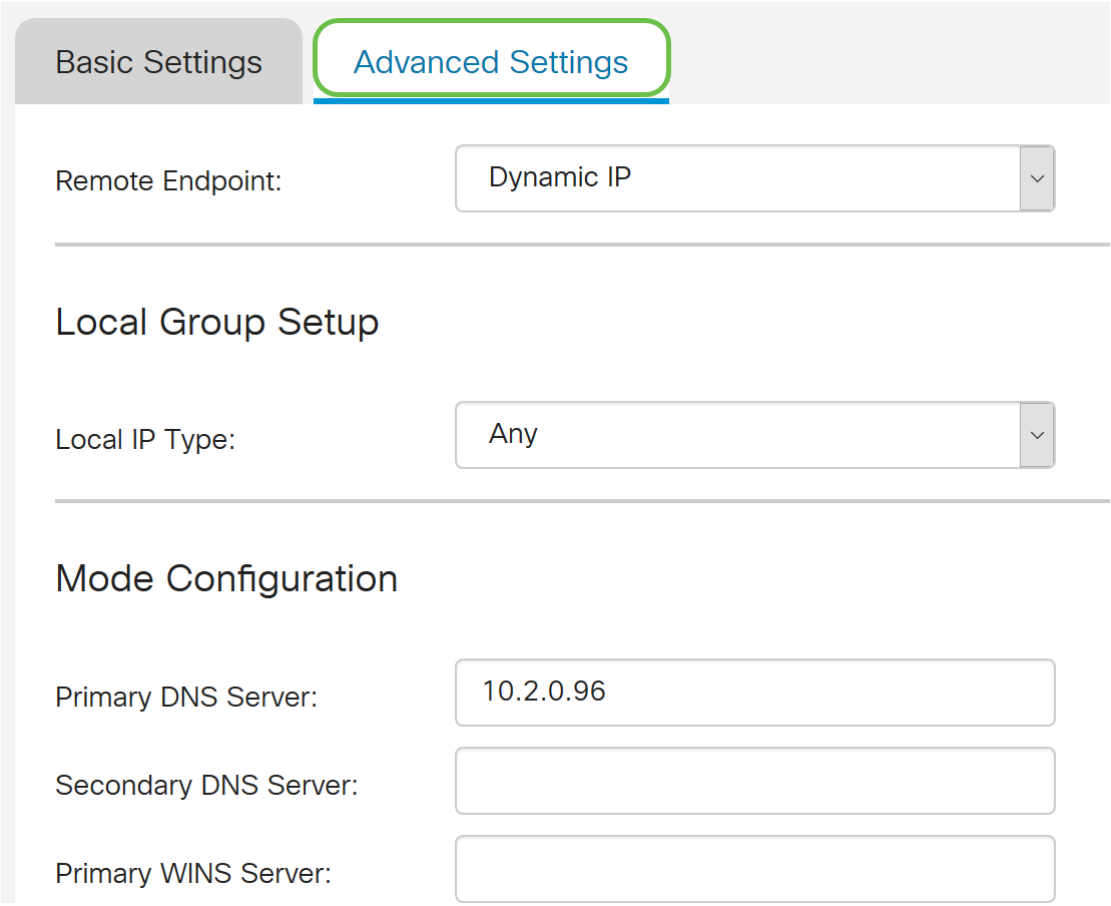
Stap 1. Controleer **het** selectieteken **Uitgebreide** verificatie om dit mogelijk te maken. Dit zal een extra niveau van authenticatie opleveren dat van externe gebruikers vereist is om in hun geloofsbrieven te toetsen voordat ze toegang tot VPN krijgen.

Als u *Uitgebreide verificatie* hebt ingeschakeld, *klikt u* op het pictogram **plus** om een gebruikersgroep toe te voegen. Selecteer de groep uit de vervolgkeuzelijst die u wilt gebruiken voor uitgebreide verificatie. Wij kiezen **ShrewSoftGroup** als groep.

Stap 12. In het *wolbereik voor clientadaptertools* specificeert u het bereik van IP-adressen dat aan een VPN-client kan worden toegewezen in het veld *Start IP* en *End IP*. Dit moet een pool van adressen zijn die niet met de site adressen overlapt.

We voeren **10.2.1.1** in als onze *Start IP* en **10.2.1.254** voor *onze end IP*.

Stap 13. (Optioneel) Klik op het tabblad **Geavanceerde instellingen**.



Stap 14. (Optioneel) Hier kunt u het IP-adres van het Remote Endpoint specificeren. In deze gids zullen we **Dynamische IP** gebruiken, aangezien het IP adres voor de eindclient niet is vastgesteld.

U kunt ook specificeren welke interne bronnen onder de *Local Group Setup* beschikbaar zullen zijn.

Als u **Any** selecteert, zijn alle interne bronnen beschikbaar.

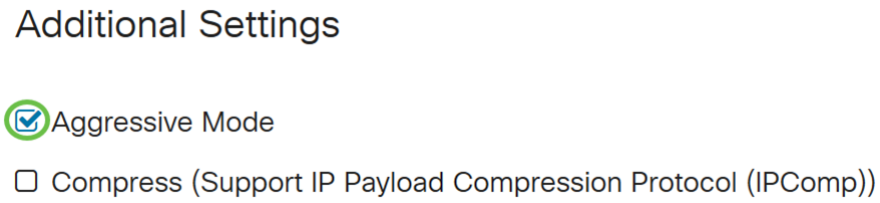
U kunt ook kiezen voor het gebruik van interne DNS- en WINS-servers. Daartoe moet u ze specificeren onder *Mode Configuration*.

U hebt ook de mogelijkheid om volledige of gesplitste tunnels te gebruiken en DNS te splitsen.

Naar *extra instellingen* bladeren. Controleer het selectieknop **Aggressive Mode** om Aggressive Mode in te schakelen. De agressieve modus is wanneer de onderhandeling voor IKE SA gecomprimeerd is in drie pakketten met alle SA vereiste gegevens die door de initiatiefnemer moeten worden doorgegeven. De onderhandelingen verlopen sneller, maar hebben in duidelijke tekst een kwetsbaarheid voor uitwisselingsidentiteiten.

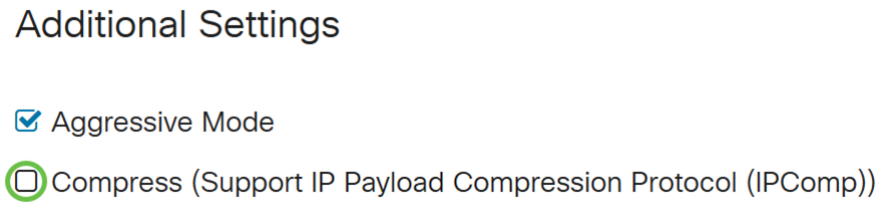
Opmerking: Extra informatie voor hoofdmodus vs agressieve modus, zie: Hoofdmode VS Aggressief Mode

In dit voorbeeld zullen we **agressieve mode** mogelijk maken.

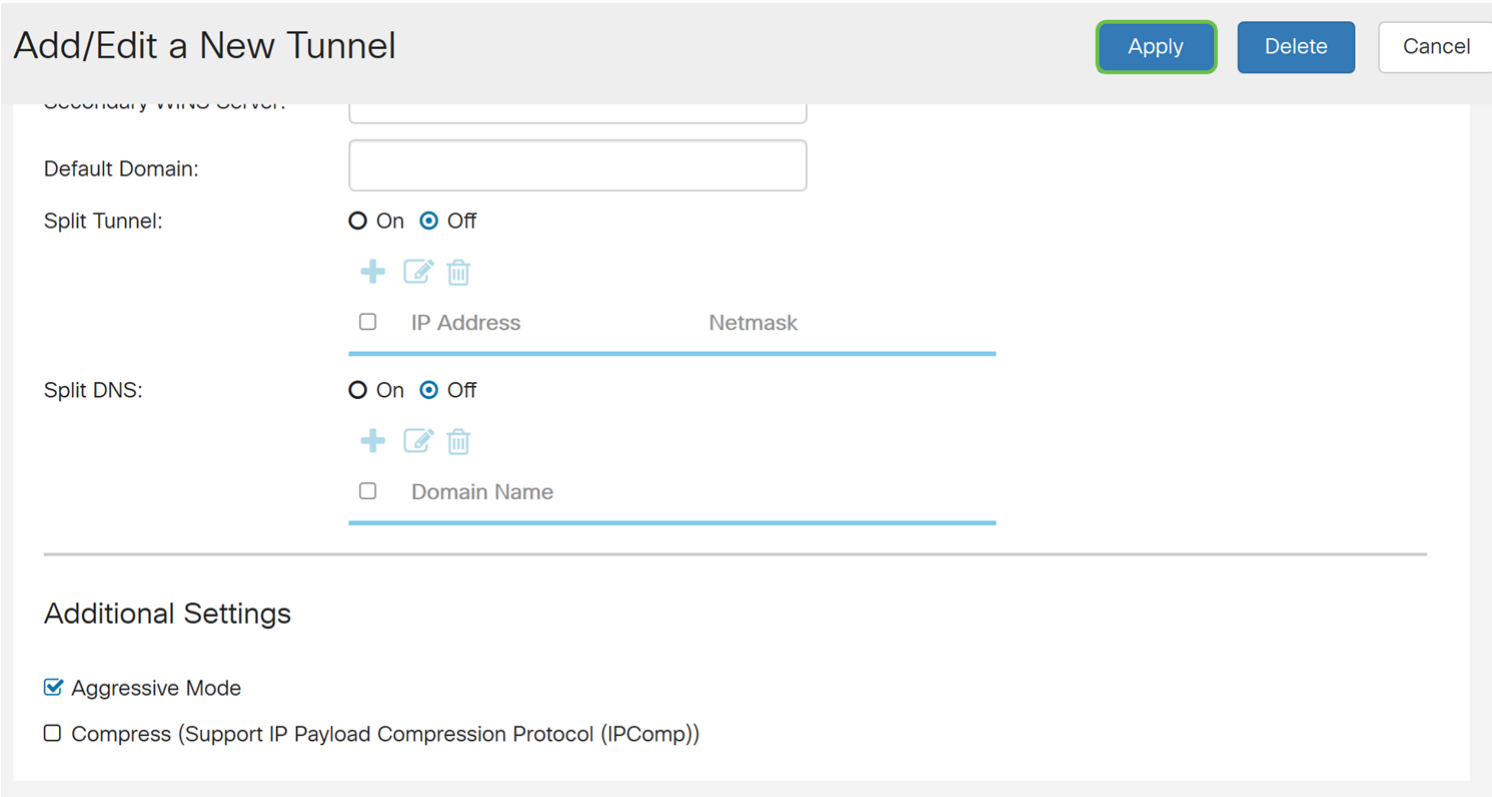


Stap 15. (Optioneel) Controleer het selectieteken **Compress (Support IP payload Compression Protocol (IPComp))** om de router in staat te stellen om compressie voor te stellen wanneer deze een verbinding start. Dit is een protocol dat de grootte van IP-datagrammen beperkt. Als de responder dit voorstel afwijst, dan voert de router geen compressie uit. Wanneer de router de responder is, accepteert het compressie, zelfs als compressie niet ingeschakeld is.

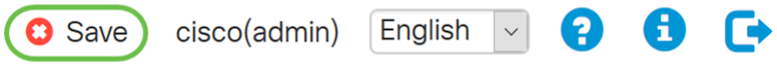
We laten *Compress* ongehinderd achter.



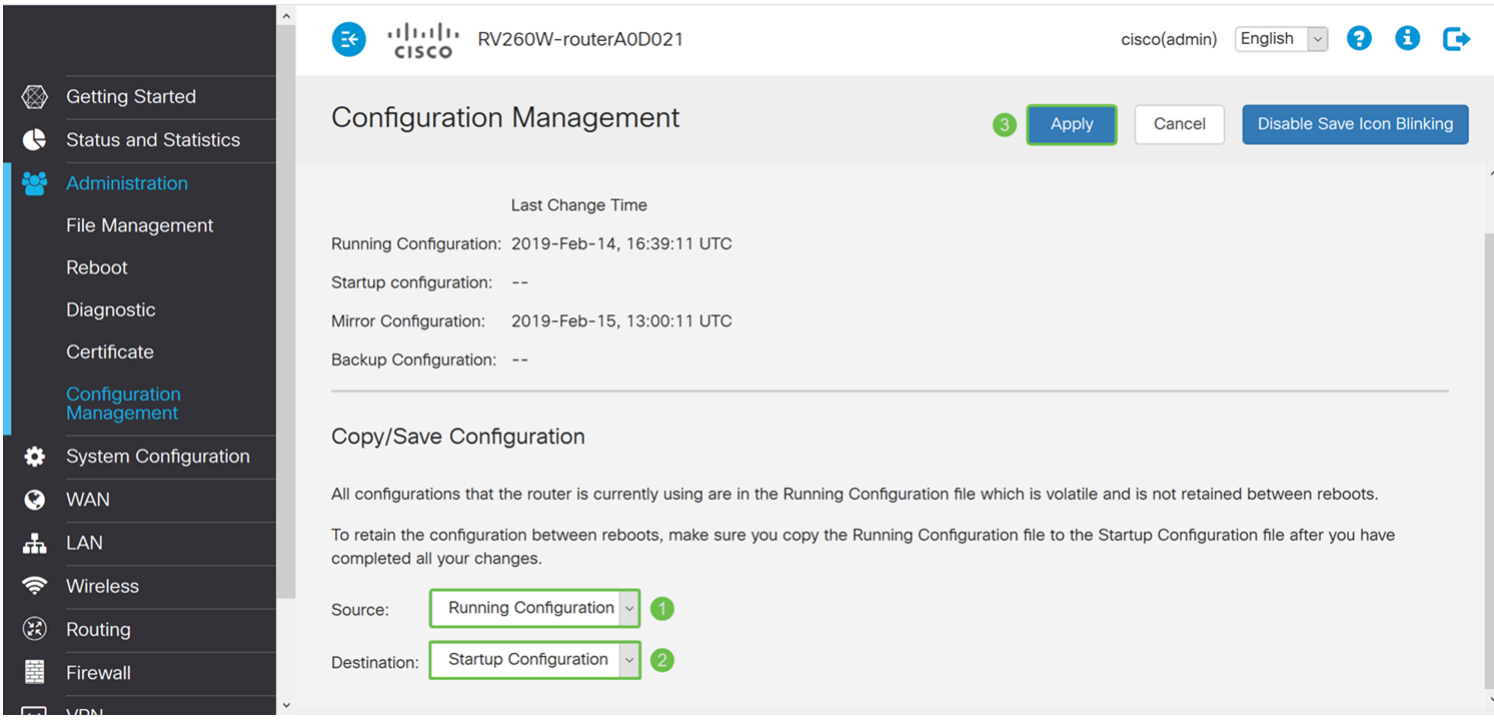
Stap 16. Klik op **Toepassen** om de nieuwe tunnel toe te voegen.



Stap 17. Klik op het pictogram knipperende **Save** bovenop de webconfiguratie pagina.



Stap 18. De pagina *Configuration Management* wordt geopend. Zorg er in het gedeelte *Configuration kopiëren/opslaan* voor dat het veld *Source* Configuration **heeft uitgevoerd** en *Destination* heeft **een opstartconfiguratie.** Druk vervolgens op **Toepassen**. Alle configuraties die de router momenteel gebruikt zijn in het bestand Configuration uitvoeren dat vluchtig is en niet tussen de herstart blijft behouden. Het kopiëren van het Configuration-bestand dat naar het opstartconfiguratiesbestand wordt uitgevoerd, behoudt de configuratie tussen de herstart.

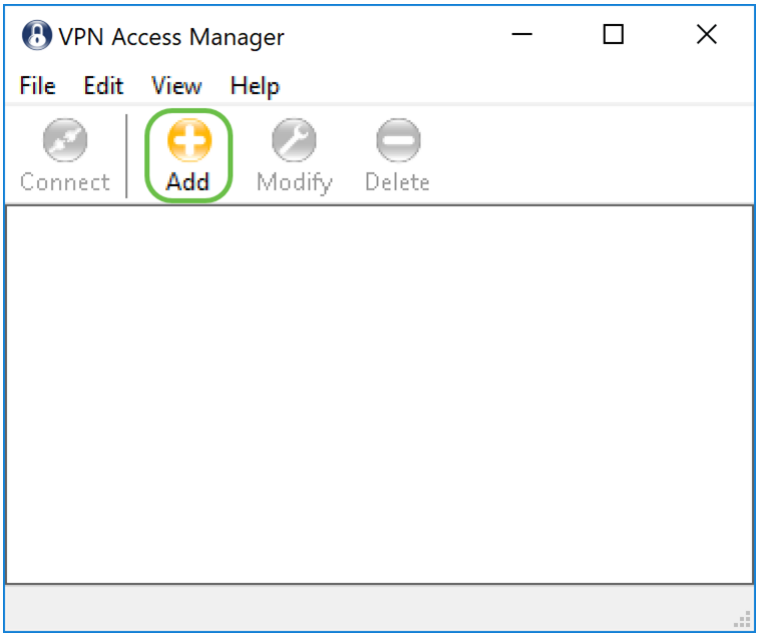


Een zachte VPN-client configureren

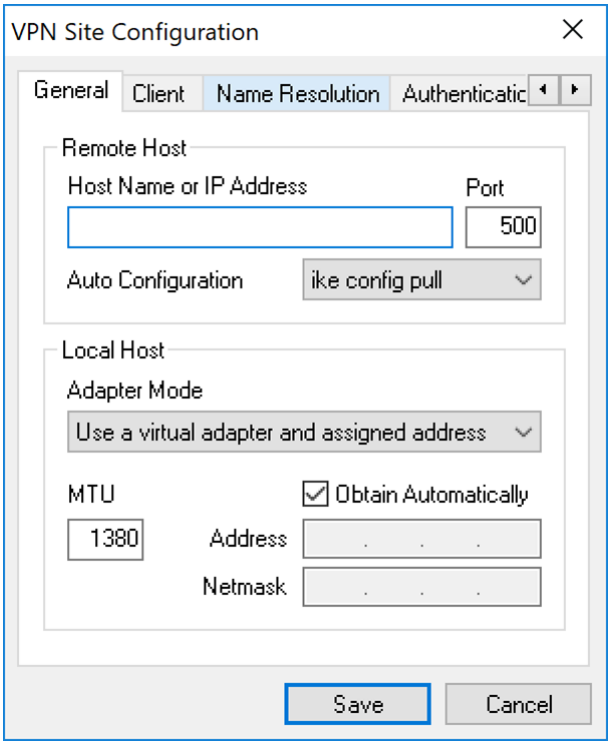
Als u de Shrew Soft VPN client niet hebt gedownload, kunt u de client downloaden door op deze link te klikken: Een zachte VPN-client voor Windows tonen. We gebruiken de standaard editie. Als u reeds Shrew Soft VPN client hebt gedownload, kunt u zich vrij om naar de eerste stap te gaan.

Een zachte VPN-client tonen: tabblad Algemeen

Stap 1. Open Windows VPN-toegangsbeheer en klik op **Add** om een nieuw profiel toe te voegen.

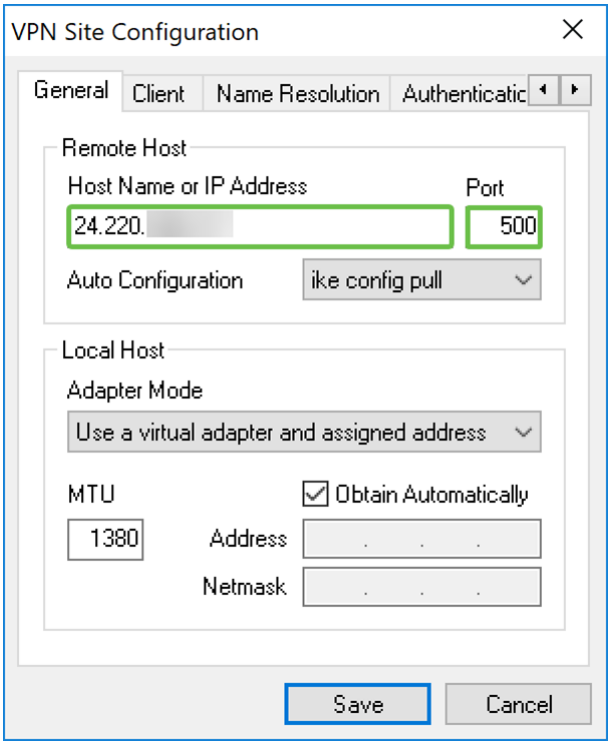


Het venster *VPN Site Configuration* verschijnt.



Stap 2. In het gedeelte *Remote Host* onder het *tabblad General* voert u het openbare hostnaam of IP-adres in van het netwerk waaraan u probeert te verbinden. In dit voorbeeld zullen we het WAN IP-adres van de RV160/RV260 op de site invoeren om de verbinding in te stellen.

Opmerking: Zorg dat het poortnummer is ingesteld op de standaardwaarde van 500. Om VPN te laten werken, gebruikt de tunnel UDP-poort 500, die moet worden ingesteld om ISAKMP-verkeer door te sturen in de firewall.



Stap 3. Selecteer in de vervolgkeuzelijst *Auto Configuration* een optie. De beschikbare opties zijn als volgt gedefinieerd:

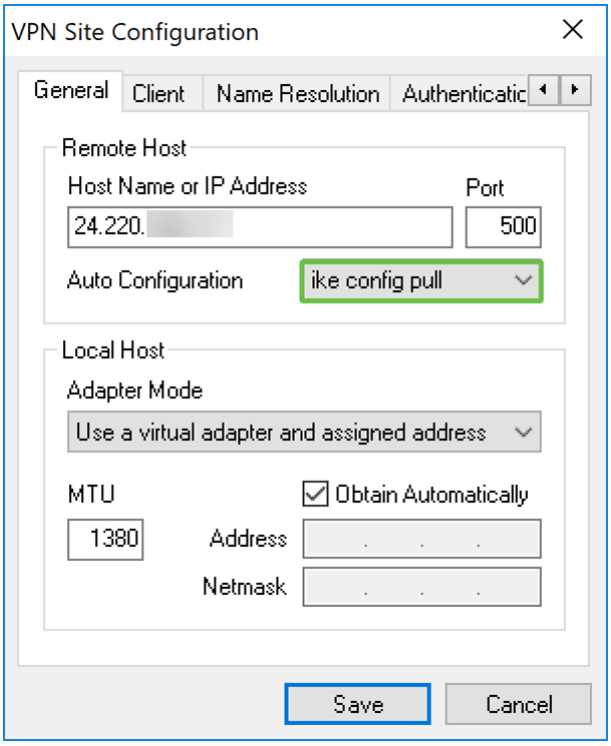
Uitgeschakeld - schakelt automatische clientconfiguratie uit

Ike Config - hiermee kan de **klant** verzoeken van een computer instellen. Met ondersteuning van de keuzemethode van de computer, retourneert het verzoek een lijst met instellingen die door de client worden ondersteund.

Ike Config Push - biedt een computer de mogelijkheid om instellingen aan de client aan te bieden tijdens het configuratie. Met steun van de drukkwaliteit van de computer, keert het verzoek een lijst terug van instellingen die door de client worden ondersteund.

DHCP over IPsec - biedt de client de mogelijkheid om instellingen van de computer te vragen via DHCP via IPsec.

In dit voorbeeld, zullen we **net** selecteren **configuratie pull**.

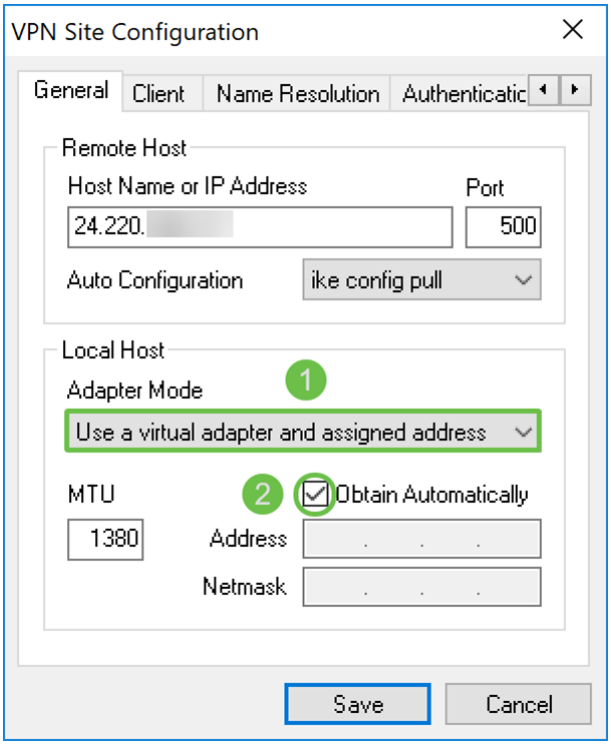


Stap 4. Kies in het gedeelte *Local Host* een **virtuele adapter gebruiken en geef het adres** aan in de vervolgkeuzelijst *Adapter Mode* en controleer het selectieteken **Automatisch** verkrijgen. De beschikbare opties zijn als volgt gedefinieerd:

Gebruik een virtuele adapter en toegewezen adres - Hiermee kan de client een virtuele adapter gebruiken met een bepaald adres als bron voor de IPsec-communicatie.

Gebruik een virtuele adapter en een willekeurig adres - Hiermee kan de client een virtuele adapter gebruiken met een willekeurig adres als bron voor de IPsec-communicatie.

Gebruik een bestaande adapter en een huidig adres - Hiermee kan de client alleen zijn bestaande, fysieke adapter gebruiken met zijn huidige adres als bron voor zijn IPsec-communicatie.



Een zachte VPN-client tonen: Clienttabblad

Stap 1. Klik op het tabblad *Client*. Selecteer in de vervolgkeuzelijst *NAT*-traject dezelfde instelling die u op de RV160/RV260 hebt ingesteld voor NAT-verplaatsing. De beschikbare opties van het menu Network Address Traversal (NATT) zijn als volgt gedefinieerd:

Uitgeschakeld - De NAVO-protocolverlengingen worden niet gebruikt.

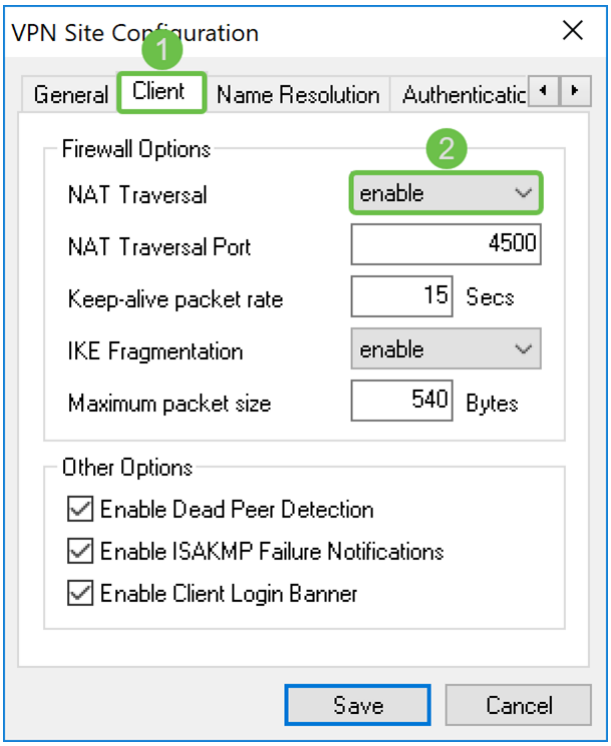
Ingeschakeld - De NATT protocol extensies zullen alleen gebruikt worden als de VPN gateway ondersteuning aangeeft tijdens onderhandelingen en NAT wordt gedetecteerd.

Force-Design - De ontwerpversie van het NATT-protocol extensies worden gebruikt, ongeacht of de VPN-gateway ondersteuning tijdens onderhandelingen aangeeft of NAT wordt gedetecteerd.

Force-RFC - De RFC-versie van het NATT-protocol wordt gebruikt, ongeacht of de VPN-gateway duidt op ondersteuning tijdens onderhandelingen of NAT wordt gedetecteerd.

Force-Cisco-UDP - Force UDP-insluiting voor VPN-clients zonder NAT.

In dit document **selecteren** we NAT-verkeer **in en** laten we *NAT Traversal Port* en *Houd het pakkettarief* in stand als de standaardwaarde.



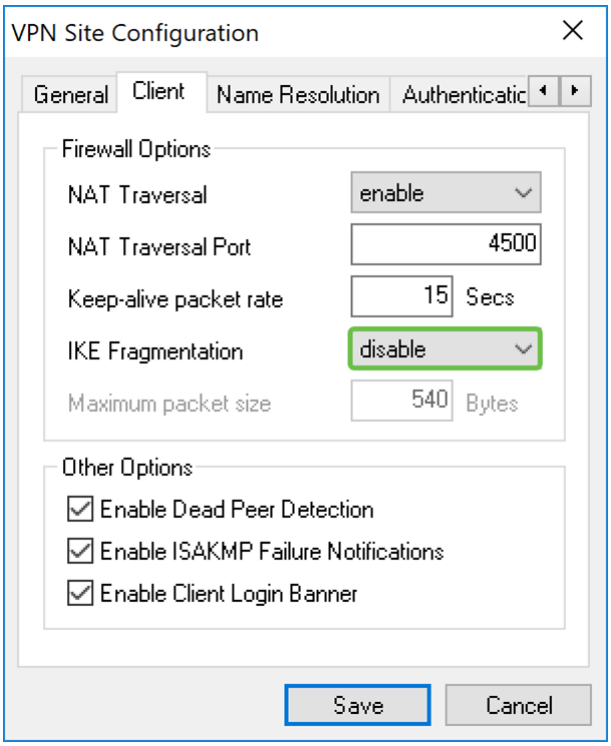
Stap 2. In de vervolgkeuzelijst *IKE Fragmentation*, selecteert u **Uitschakelen**, **Inschakelen** of **Maken**. De opties zijn als volgt gedefinieerd:

Uitschakelen - De IKE Fragmentation-protocolextensie wordt niet gebruikt.

- De IKE Fragmentation-protocolextensie wordt alleen gebruikt als de VPN-gateway ondersteuning tijdens onderhandelingen aangeeft.

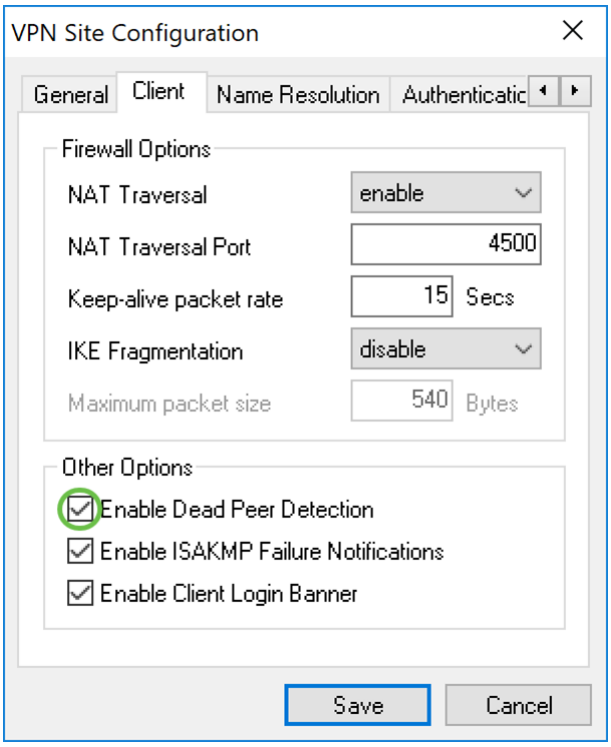
Force - De IKE Fragmentation protocol-extensie zal worden gebruikt, ongeacht of de VPN-gateway ondersteuning tijdens onderhandelingen aangeeft.

We hebben geselecteerd **voor** *IKE Fragmentation*.



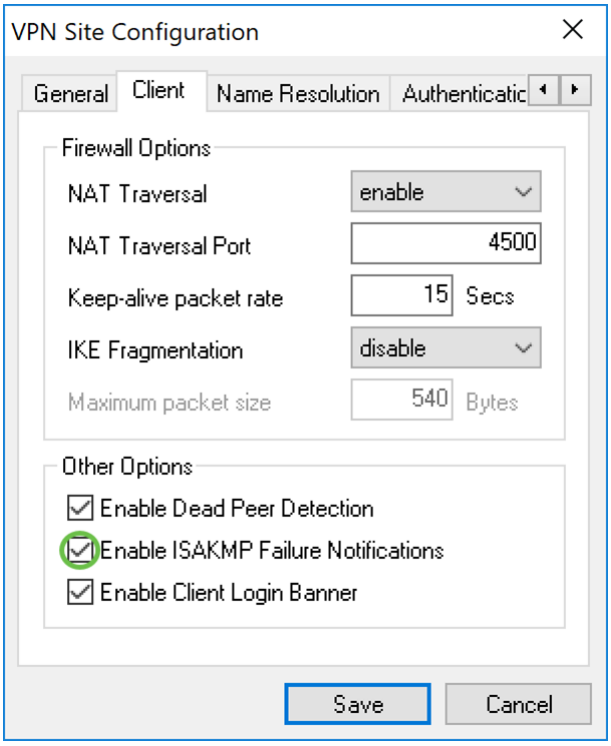
Stap 3. Controleer selectieknop **Detectie** van **dode peer** inschakelen om het protocol voor detectie van dial-peers in te schakelen. Als deze optie ingeschakeld is, zal deze alleen gebruikt worden als de router deze ondersteunt. Dit staat de client en de router toe om de status van de tunnel te controleren om te detecteren wanneer één kant niet langer kan reageren. Deze optie is standaard ingeschakeld.

In dit voorbeeld laten we de Dead Peer Detectie controleren.



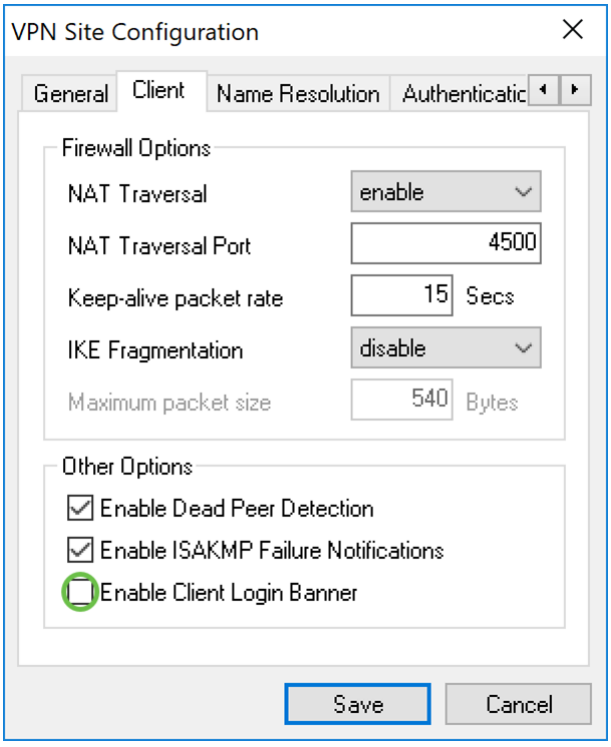
Stap 4. Controleer het selectieteken **voor** melding **van ISAKMP-fout inschakelen** om melding van ISAKMP-storing van de VPN-client-IPsec Daemon mogelijk te maken. Dit is standaard ingeschakeld.

In dit voorbeeld laten we de melding van mislukkingen van ISAKMP op de voet.



Stap 5. Schakel de **clientscanner uit** om deze uit te schakelen. Dit zal een logbanner tonen nadat de tunnel met de router is gevestigd. De router moet de Transaction Exchange ondersteunen en zijn geconfigureerd om een inlogbanner naar de client te verzenden. Deze waarde wordt standaard ingeschakeld.

We zullen de clientscanner niet controleren.



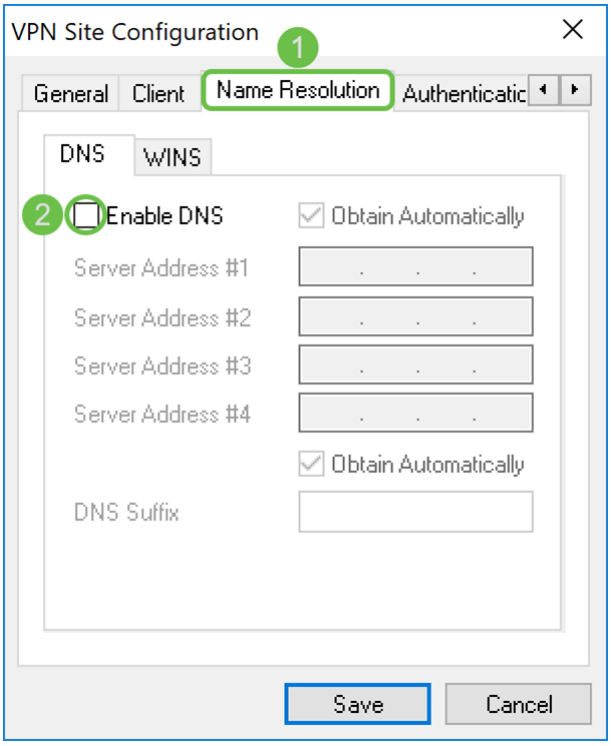
Een zachte VPN-client tonen: Tabblad Resolutie naam

Stap 1. Klik op het tabblad *Naam* en controleer het selectieteken **DNS** inschakelen als u DNS wilt inschakelen. Als specifieke DNS-instellingen niet nodig zijn voor uw gebiedsconfiguratie, schakelt u het selectieknop **DNS** inschakelen uit.

Als *DNS inschakelen* is ingeschakeld en uw externe gateway is ingesteld om de

Configuration Exchange te ondersteunen, kan de gateway DNS-instellingen automatisch leveren. Als dit niet het geval is, controleer dan of het selectieteken **automatisch** controleren is en voer handmatig een geldig DNS-serveradres in.

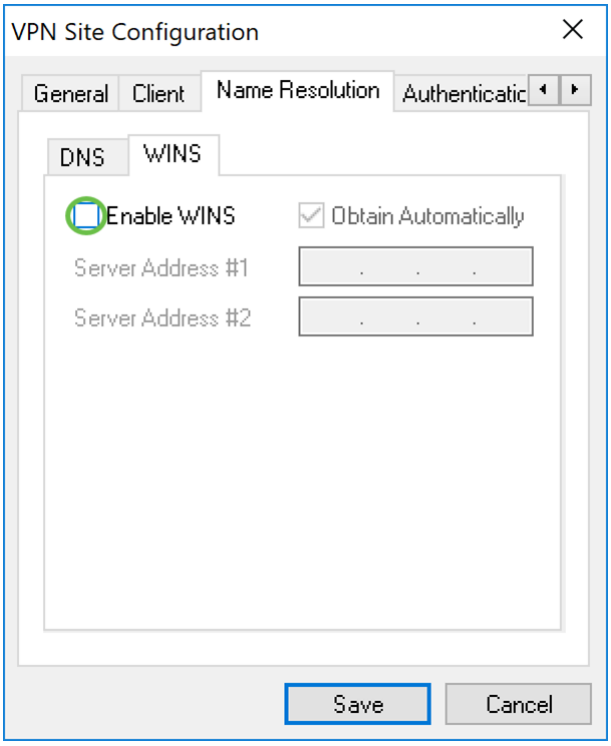
In dit voorbeeld is **DNS inschakelen** niet ingeschakeld.



Stap 2. Controleer het selectieteken **VENS inschakelen** als u de Windows Internet Name Server (WINS) wilt inschakelen. Als uw externe gateway is ingesteld om de Configuration Exchange te ondersteunen, kan de gateway automatisch WINS-instellingen bieden. Als dit niet het geval is, controleer dan of het selectieknop **Automatisch** aanschaffen niet is ingeschakeld en voer handmatig een geldig WINS Server-adres in.

Opmerking: Door WINS configuratieinformatie te verstrekken, zal een client WINS namen kunnen oplossen met een server in het externe privé netwerk. Dit is handig wanneer u toegang probeert te krijgen tot externe netwerkbronnen van Windows met behulp van een Unified Naming Convention path-naam. De WINS-server zou doorgaans behoren tot een Windows-controller of een Samba Server.

In dit voorbeeld is **VENS inschakelen** niet ingeschakeld.



Een zachte VPN-client tonen: Tabblad Verificatie

Stap 1. Klik op het tabblad *Verificatie* en selecteer **Wederzijdse PSK + XAuth** in de vervolgkeuzelijst *Verificatiemethode*. De beschikbare opties zijn als volgt gedefinieerd:

Hybride RSA + XAuth - De clientcreditering is niet nodig. De client zal de gateway echt maken. De aanmeldingsgegevens worden geleverd in de vorm van PEM- of PKCS12-certificaatbestanden of van een sleutelbestandstype.

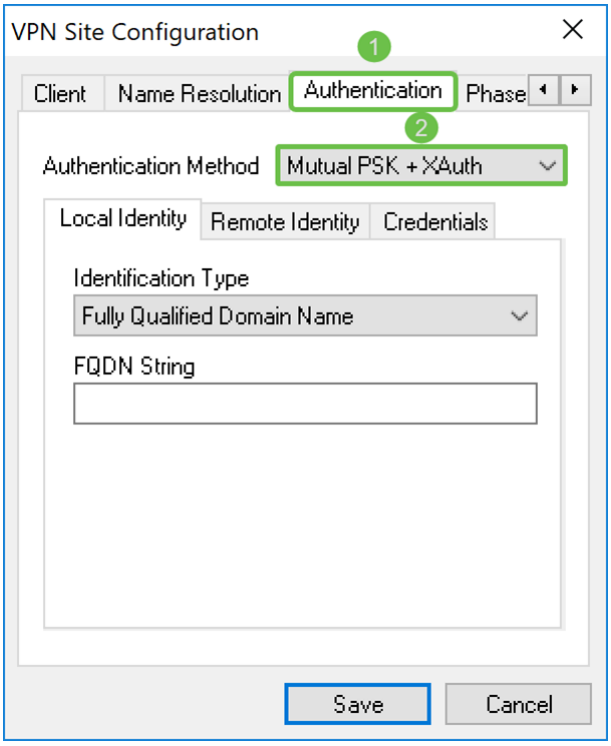
Hybride GRP + XAuth - De clientcreditering is niet nodig. De client zal de gateway echt maken. De geloofsbrieven zullen in de vorm van PEM of PKCS12 certificatenbestand en een gedeeld geheime string zijn.

Wederzijdse RSA + XAuth - Cliënt en gateway hebben beide geloofsbrieven nodig om authentiek te verklaren. De geloofsbrieven zullen in de vorm van PEM of PKCS12 certificaatbestanden of het sleuteltype zijn.

Wederzijdse PSK + XAuth - Cliënt en gateway hebben beide aanmeldingsgegevens nodig om te authentiseren. De geloofsbrieven zullen in de vorm van een gedeeld geheim strijkje zijn.

Wederzijdse RSA - Cliënt en gateway hebben beide geloofsbrieven nodig om authentiek te verklaren. De geloofsbrieven zullen in de vorm van PEM of PKCS12 certificaatbestanden of het sleuteltype zijn.

Wederzijdse PSK - Cliënt en poort hebben beide geloofsbrieven nodig om authentiek te verklaren. De geloofsbrieven zullen in de vorm van een gedeeld geheim strijkje zijn.



Stap 2. Selecteer in het tabblad *Local Identity* en voer vervolgens de gewenste string in het lege veld in. De volgende opties zijn gedefinieerd als:

- Dit wordt alleen geaccepteerd op het tabblad Remote Identity. De client accepteert elk type ID en elke waarde. Dit dient met voorzichtigheid te worden gebruikt aangezien het een deel van het identificatieproces van de IKE fase 1 voorbijgaat.

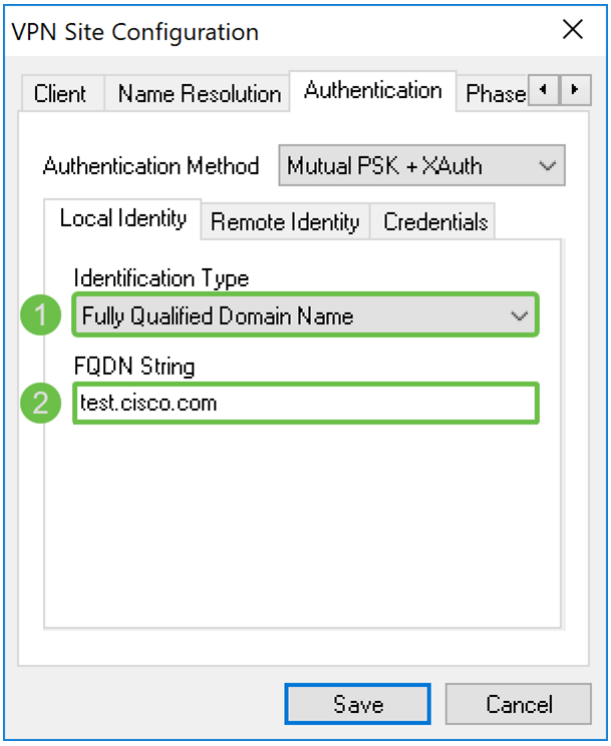
Volledig gekwalificeerde Naam van het Domein - Deze optie, moet u een KFDN-string verstrekken in de vorm van een DNS domeinstring. Bijvoorbeeld, "cisco.com" zou een aanvaardbare waarde zijn. De client laat deze optie alleen selecteren als er een PSK-verificatiemodus wordt gebruikt.

Gebruiker Volledig gekwalificeerde Naam van het Domein - U moet een Gebruiker FQDN-string verstrekken in de vorm van een user@domain string. Bijvoorbeeld, "dave@cisco.com" zou een aanvaardbare waarde zijn. De klant zou alleen toestaan dat deze optie wordt geselecteerd indien een PSK-verificatiemodus wordt gebruikt.

IP-adres - Wanneer het IP-adres is geselecteerd, wordt *het* selectieteken *Gebruik een ontdekt lokaal adres* automatisch gecontroleerd. Dit betekent dat de waarde automatisch wordt bepaald. Schakel het selectieteken uit als u een ander adres wilt gebruiken dan het adapteradres dat gebruikt wordt om met de clientgateway te communiceren. Voer vervolgens een specifieke adresstring in. De client laat deze optie alleen selecteren als er een PSK-verificatiemodus wordt gebruikt.

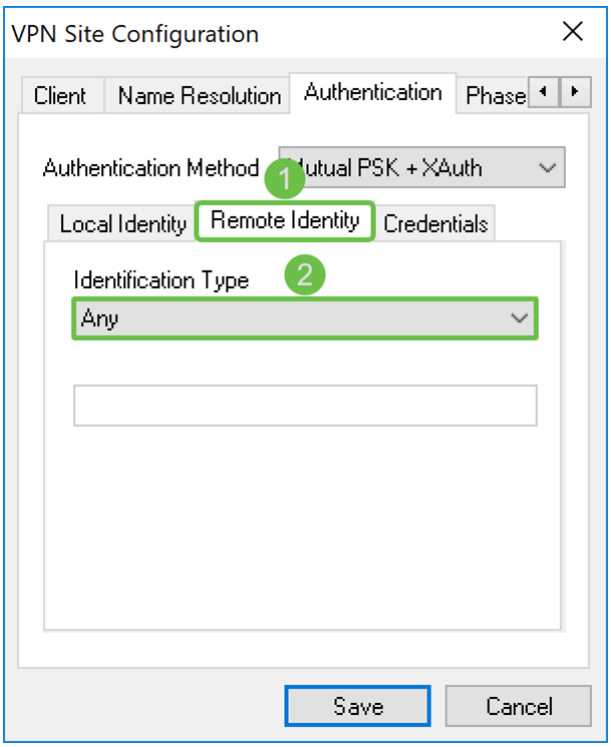
Key Identifier - Wanneer deze optie geselecteerd is, moet u een identificatietekens geven.

In dit voorbeeld, zullen we **Full Qualified Domain Name** selecteren en **test.cisco.com** invoeren in het veld *FQDN String*.



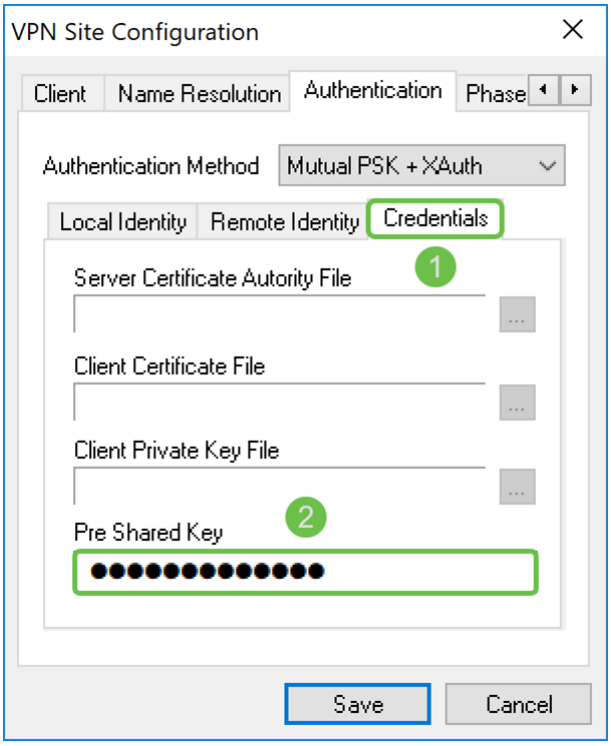
Stap 3. Klik op het tabblad *Remote Identity* en selecteer het gewenste type. Mogelijke opties zijn: Alle, volledig gekwalificeerd domeinnaam, volledig gekwalificeerde domeinnaam, IP-adres of Key Identifier.

In dit document gebruiken we **Any**leder type identificatie.



Stap 4. Klik op het tabblad *Credentials* en voer dezelfde voorgedeelde toets in die u op de RV160/RV260 hebt ingesteld.

We gaan **CiscoTest123** in**!** in het *veld Vooraf gedeelde sleutel*.



Een zachte VPN-client tonen: Tabblad Fase 1

Stap 1. Klik op het tabblad *Fase 1*. Configureer de volgende parameters met dezelfde instellingen als u voor de RV160/RV260 hebt ingesteld.

De parameters in Shrew Soft moeten overeenkomen met de configuratie RV160/RV260 die u in Fase 1 hebt geselecteerd. In dit document worden de parameters in Shrew Soft ingesteld op:

Wisseltype: **agressief**

DH Exchange: **groep 2**

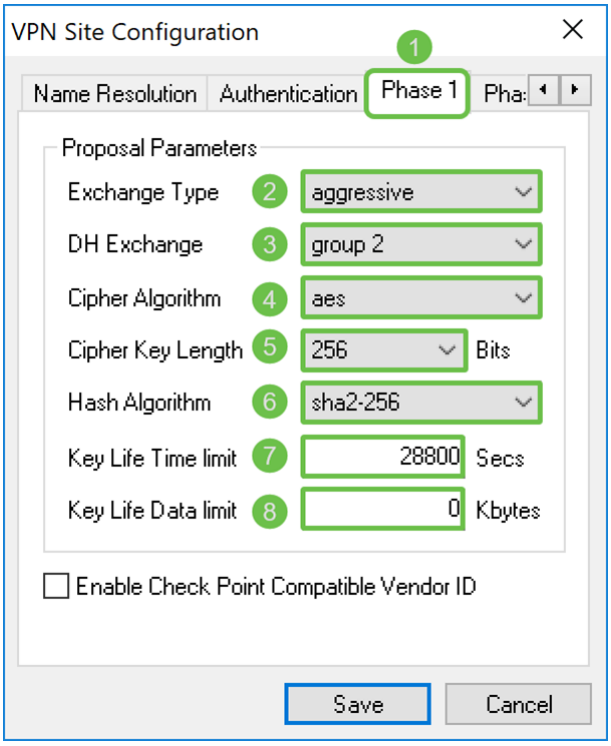
algoritme cipher: **aes**

Toetslengte: **256**

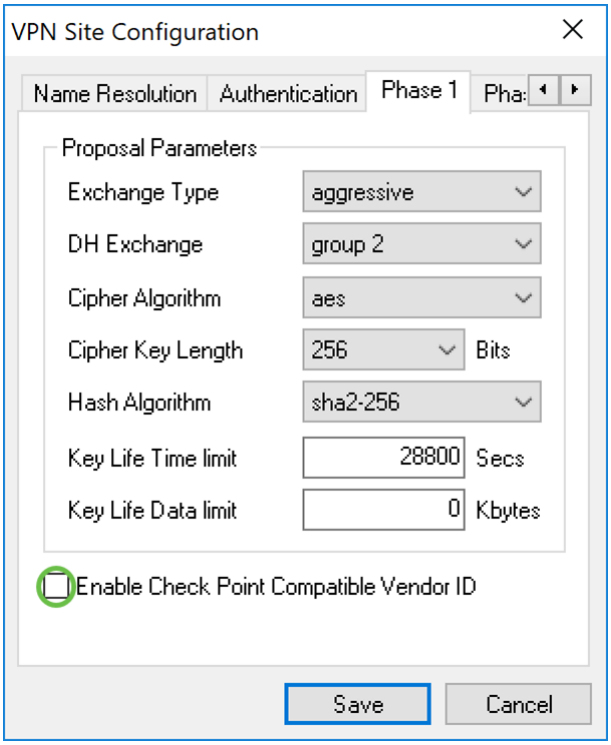
Hashalgoritme: **sha2-256**

Termijn sleutellevensduur: **28800**

Grenswaarde voor sleutellevensgegevens: **0**



Stap 2. (Optioneel) Als uw gateway een Cisco-compatibele verkoper-id tijdens fase 1-onderhandelingen biedt, schakelt u het selectieteken **Schakel het** vakje **aankruispunt-compatibele verkoper** in. Als de poort geen Cisco-compatibele verkoper-ID biedt of als u niet zeker bent, laat u het selectieteken oningeschakeld. We laten de selectieteken ongecontroleerd achter.



Een zachte VPN-client tonen: Tabblad Fase 2

Stap 1. Klik op het tabblad *Fase 2*. Configureer de volgende parameters met dezelfde instellingen als u voor de RV160/RV260 hebt ingesteld.

De parameters moeten in fase 2 overeenkomen met de configuratie van RV160/260 als volgt:

Algoritme omzetten: **esp**

Sleutellengte omzetten: **256**

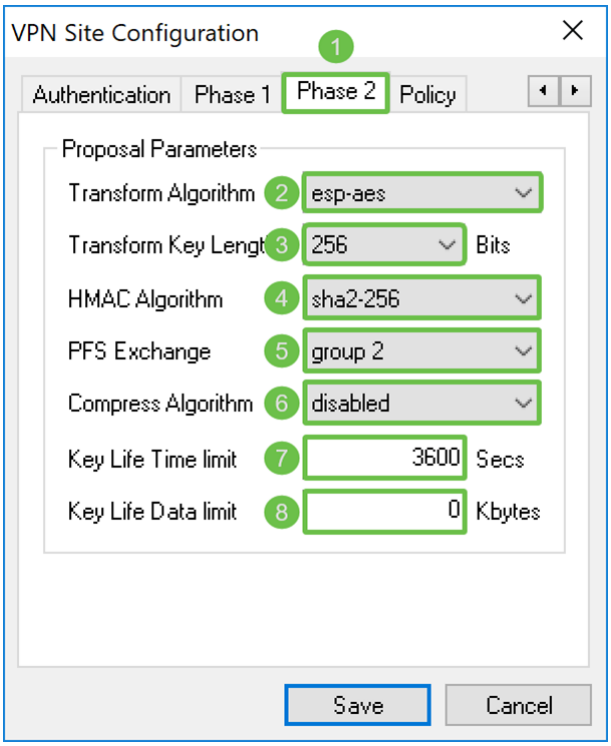
HMAC-algoritme: **sha2-256**

PFS Exchange: **groep 2**

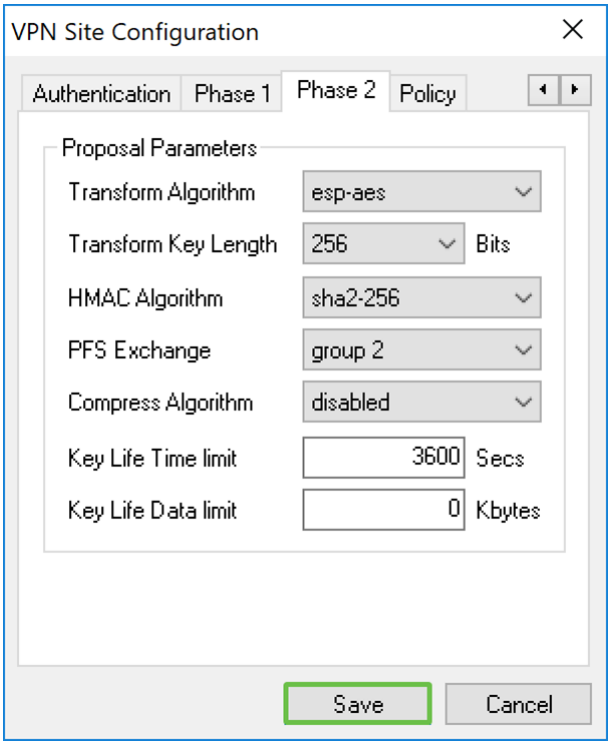
Comprimeer algoritme: **gehandicapt**

Termijn sleutellevensduur: **3600**

Grenswaarde voor sleutellevensgegevens: **0**



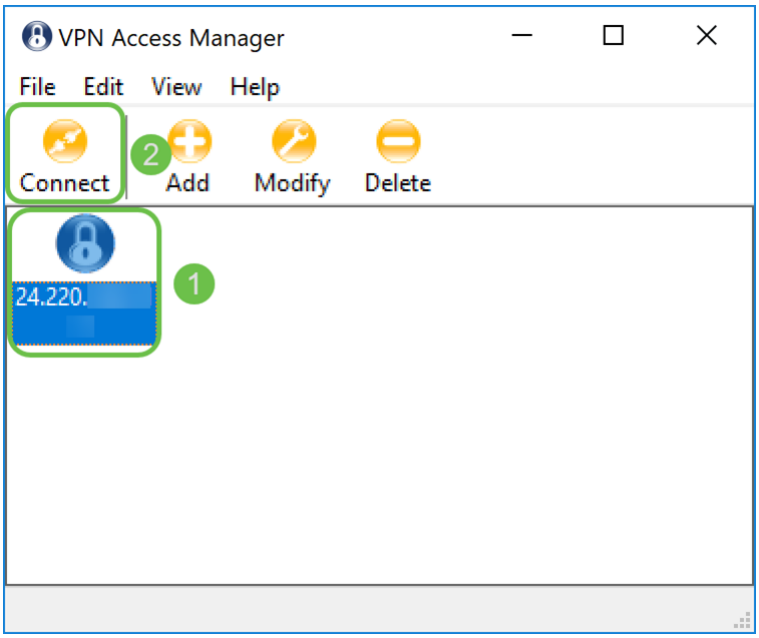
Stap 2. Druk op de knop **Opslaan** onder op de pagina om de configuratie op te slaan.



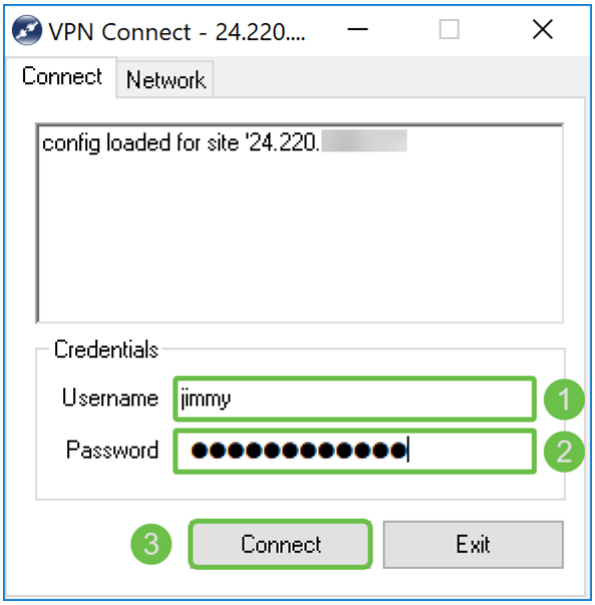
Een zachte VPN-client tonen: Aansluiten

Stap 1. In *VPN Access Manager* selecteert u het VPN-profiel dat u zojuist hebt gemaakt. Druk vervolgens op **Connect**.

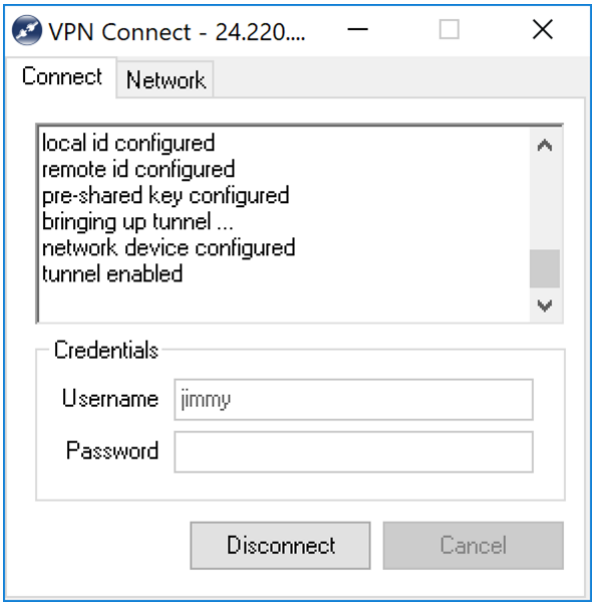
Opmerking: Als u het VPN-profiel een andere naam wilt geven, klikt u met de rechtermuisknop op het profiel en selecteert u **Hernoemen**. Een deel van het IP-adres in het profiel is leeg om dat netwerk te beschermen.



Stap 2. Er verschijnt een *VPN Connect*-venster. Voer de gebruikersnaam en het wachtwoord in die zijn aangemaakt in het gedeelte *Gebruikersaccount maken*. Druk vervolgens op **Connect**.

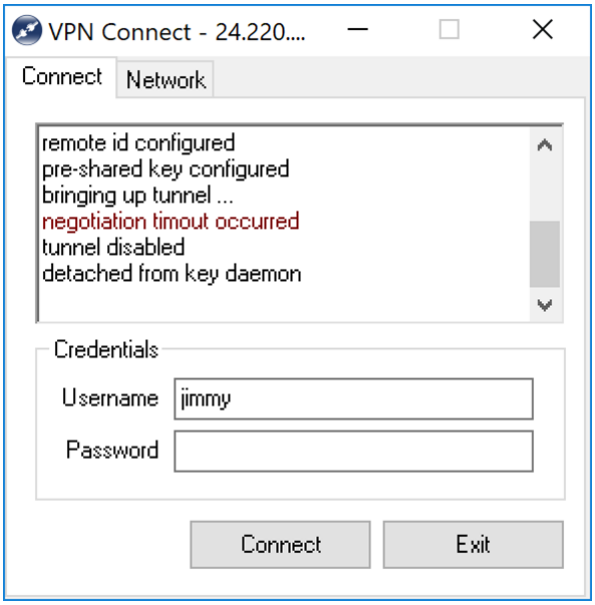


Stap 3. Na het drukken *van Connect* wordt de configuratieinformatie aan de IKE Daemon toegevoegd samen met een verzoek om te communiceren. Verschillende berichten van de verbindingsstaat worden weergegeven in het uitvoervenster. Als de verbinding slaagt, krijg je een bericht dat zegt, "netwerk device geconfigureerd" en "tunnel enabled". De knop *Verbinding* verandert nu in een knop *Koppelen*.

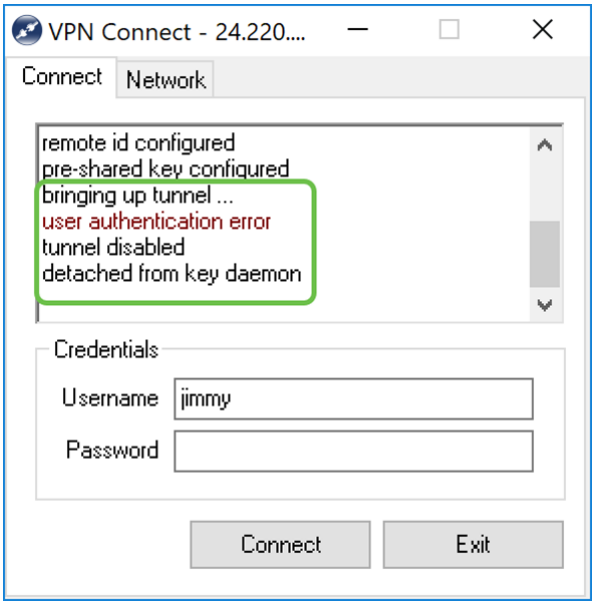


Tips voor het oplossen van VPN-verbinding

Als je foutmeldingen krijgt die zeggen: "onderhandelingstijd kwam voor", "tunnel gehandicapt", en "losgekoppeld van belangrijke daemon". U kunt de configuratie van uw router en uw Soft VPN client dubbel controleren om ervoor te zorgen dat ze overeenkomen.

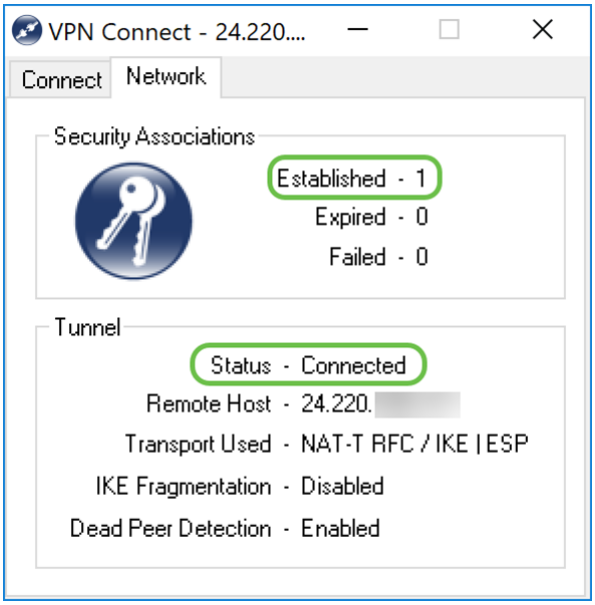


Als je een foutmelding krijgt die zegt: "gebruikersauthenticatiefout" betekent dat dat dat je het verkeerde wachtwoord voor die gebruikersnaam hebt ingevoerd. Controleer de gebruikersreferenties en controleer of deze correct zijn ingesteld en ingevoerd.

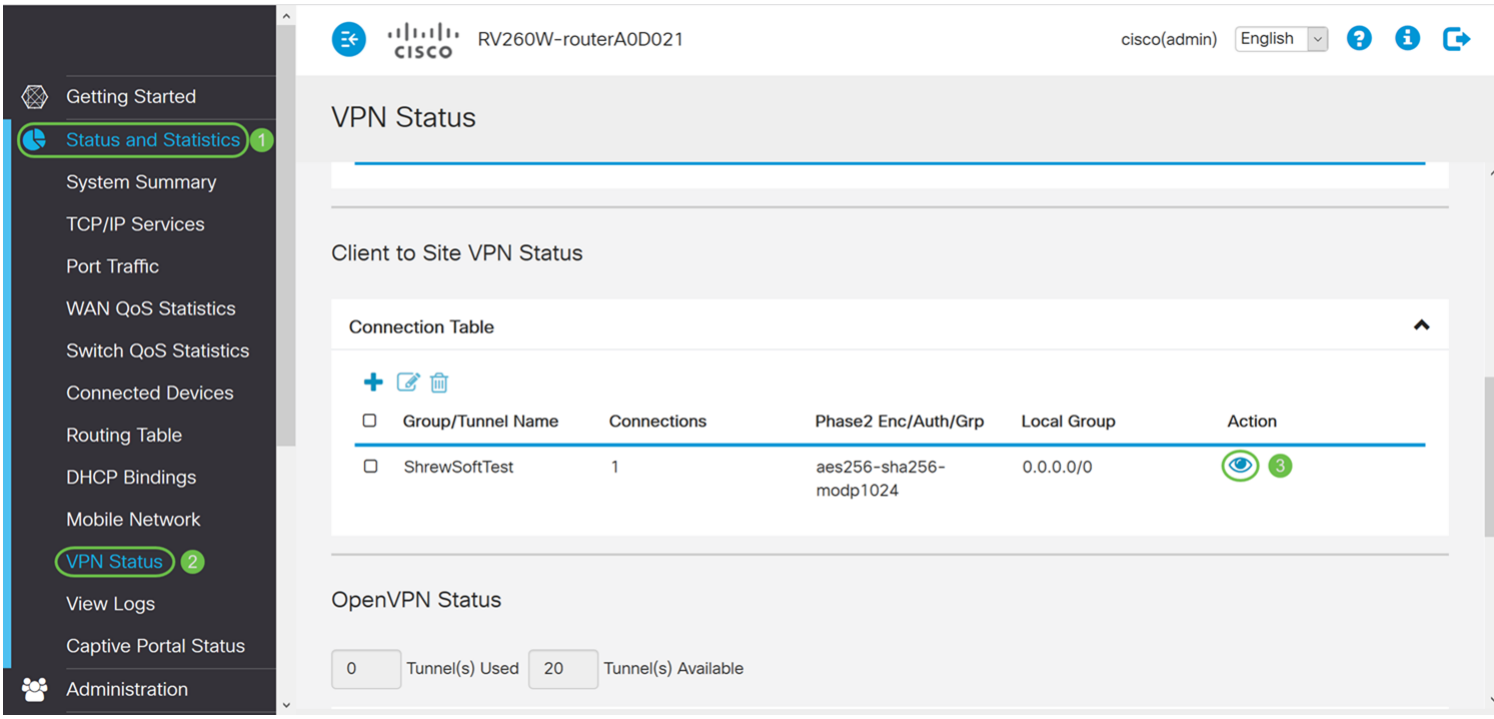


Verificatie

Stap 1. Klik op het tabblad *Network* in het venster *VPN-verbinding*. In dit tabblad kunt u de huidige netwerkstatistieken voor de verbinding weergeven. Onder het gedeelte *Tunnel* ziet u *Connected* als de status.

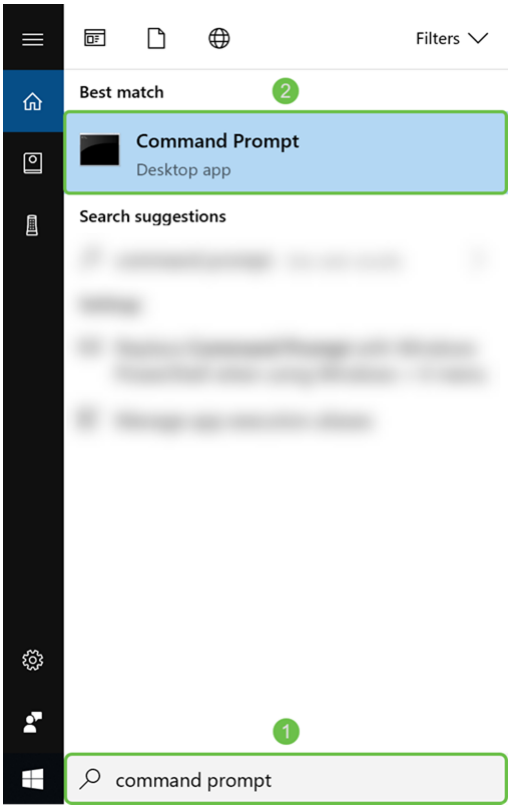


Stap 2. Op uw router, navigeer naar **Status en Statistieken > VPN-status**. In de pagina *VPN-status* scrollen *naar* de sectie *Client naar Site VPN-status*. In dit gedeelte kunt u alle client-naar-site verbindingen bekijken. Klik op het pictogram eye om meer informatie te bekijken.



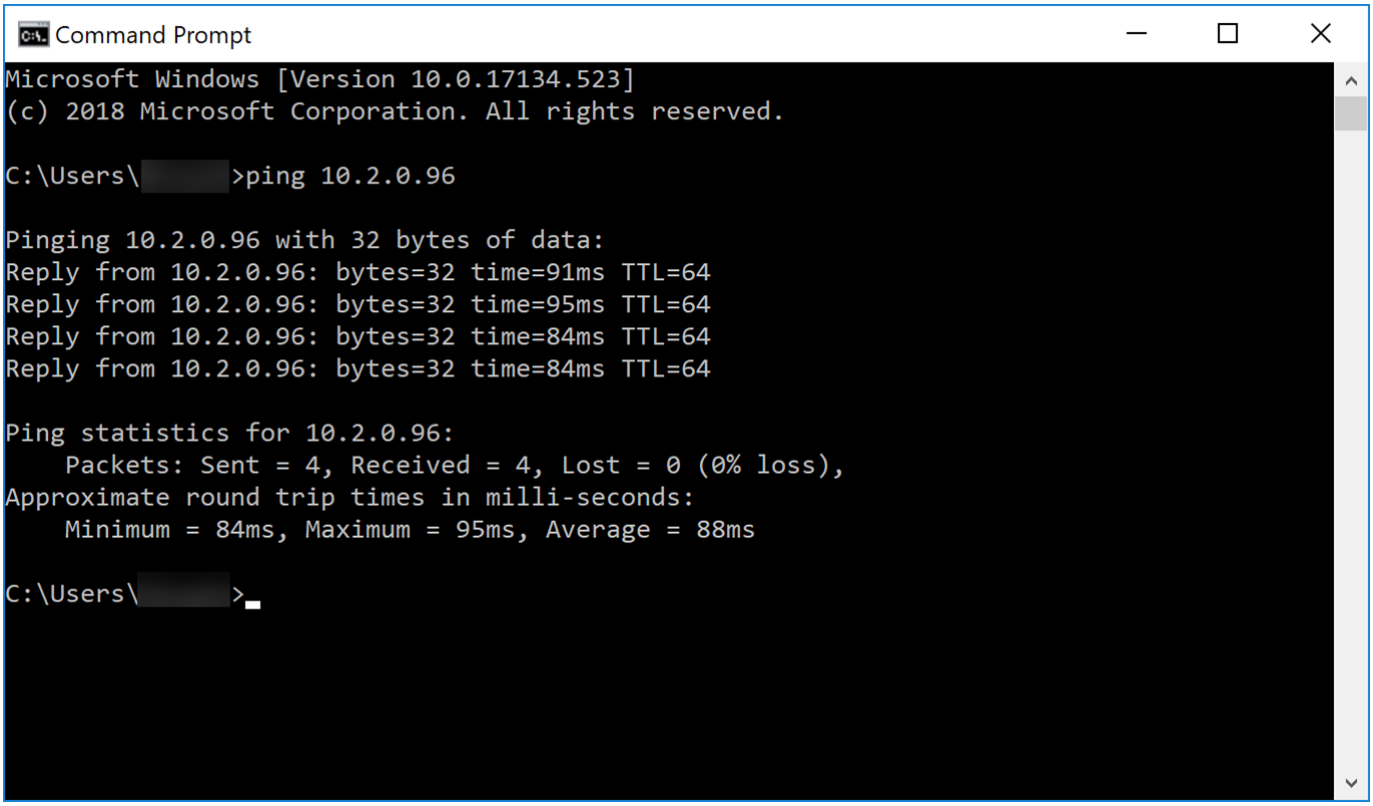
Stap 3. Navigeer naar uw zoekbalk op uw taakbalk en zoek naar **een opdracht**.

Opmerking: De volgende instructies worden gebruikt op een Windows 10-besturingssysteem. Dit kan variëren afhankelijk van het gebruikte besturingssysteem.



Stap 4. Type in de opdracht zonder de offertes, "**ping [*privé IP-adres van de router*]**" maar voer het privé-IP-adres in in in plaats van de woorden. U kunt met succes het privé IP-adres van de router pingelen.

In dit voorbeeld, zullen we typen in **ping 10.2.0.96**. 10.2.0.96 is het privé IP adres van onze router.



Conclusie

U dient nu met succes uw Shrew Soft VPN-client met RV160 of RV260 te hebben

verbonden.