

Gebruik Shrew Soft VPN-client om verbinding te maken met IPSec VPN Server op RV130 en RV130W

Doel

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

De RV130 en RV130W werken als IPSec VPN servers en ondersteunen de Shrew Soft VPN client.

Zorg ervoor dat u de nieuwste release van de clientsoftware downloadt.

·Shrew Soft (<https://www.shrew.net/download/vpn>)

Opmerking: Om de Shrew Soft VPN-client met succes te kunnen configureren met een IPSec VPN-server, moet u eerst de IPSec VPN-server configureren. Raadpleeg het artikel [Configuration of a IPSec VPN Server op RV130 en RV130W voor informatie over het uitvoeren van dit programma](#).

Het doel van dit document is om u te tonen hoe u de Shrew Soft VPN-client kunt gebruiken om verbinding te maken met een IPSec VPN-server op de RV130 en RV130W.

Toepasselijke apparaten

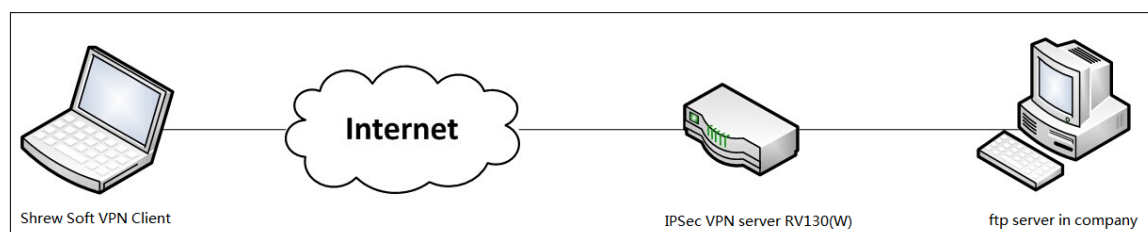
- RV130W Wireless-N VPN-firewall
- RV130 VPN-firewall

Systeemvereisten

- 32- of 64-bits systemen
- Windows 2000, XP, Vista of Windows 7/8

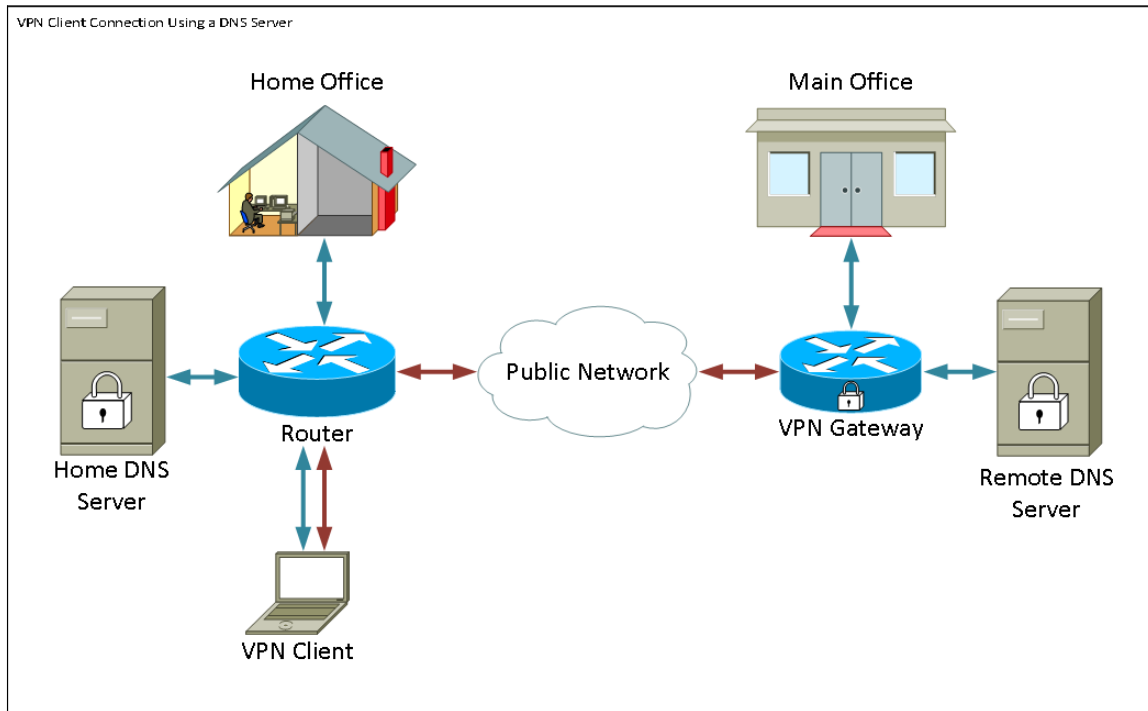
Topologie

Hieronder wordt een topologie op topniveau getoond waarin de apparaten worden geïllustreerd die betrokken zijn bij de configuratie van een Shrewsoft-client naar een locatie.



Een gedetailleerder stroomschema dat de rol van DNS-servers in een netwerkgeving

voor kleine bedrijven illustreert, wordt hieronder getoond.



Softwareversie

•1.0.1.3

Shrew zachte VPN-client instellen

Configuratie van IPSec VPN en gebruikersconfiguratie

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **VPN > IPSec VPN Server > Setup**. De pagina *Instellen* wordt geopend.

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm:


Authentication Algorithm:

PFS Key Group: Enable

DH Group:

[Stap 2](#). Controleer dat de IPSec VPN Server voor de RV130 correct is geconfigureerd. Als de IPSec VPN Server niet is geconfigureerd of verkeerd is geconfigureerd, raadpleegt u [Configuratie van een IPSec VPN-server op RV130 en RV130W](#) en klikt u op **Opslaan**.

Setup

 Configuration settings have been saved successfully

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group: Enable

DH Group:

Opmerking: De bovenstaande instellingen zijn een voorbeeld van een RV130/RV130W IPSec VPN-serverconfiguratie. De instellingen zijn gebaseerd op het document, [Configuration of an IPSec VPN Server op RV130 en RV130W](#) en worden in de volgende stappen vermeld.

Stap 3. Navigeer naar **VPN > IPSec VPN Server > Gebruiker**. De *User*-pagina verschijnt.

User

User Account Table

<input type="checkbox"/>	UserName	Password
<input type="checkbox"/>	No data to display	

Stap 4. Klik op **Rij toevoegen** om gebruikersaccounts toe te voegen, om de VPN-clients te verifiëren (uitgebreide verificatie) en de gewenste gebruikersnaam en wachtwoord in te voeren in de daarvoor bestemde velden.

User

You must save before you can edit or delete.

User Account Table	
<input type="checkbox"/>	UserName
	Password
<input type="checkbox"/>	TestUser

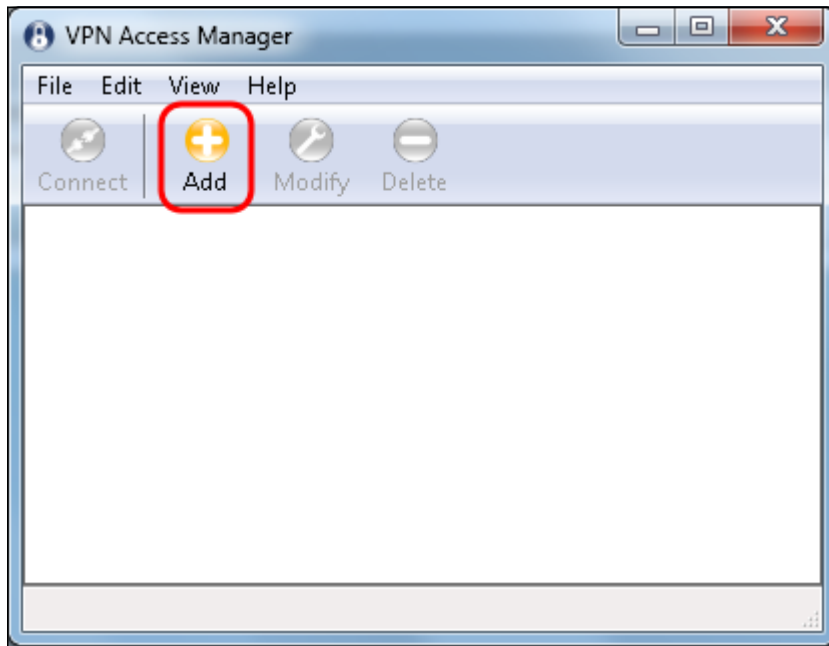
Add Row Edit Delete Import

Save Cancel

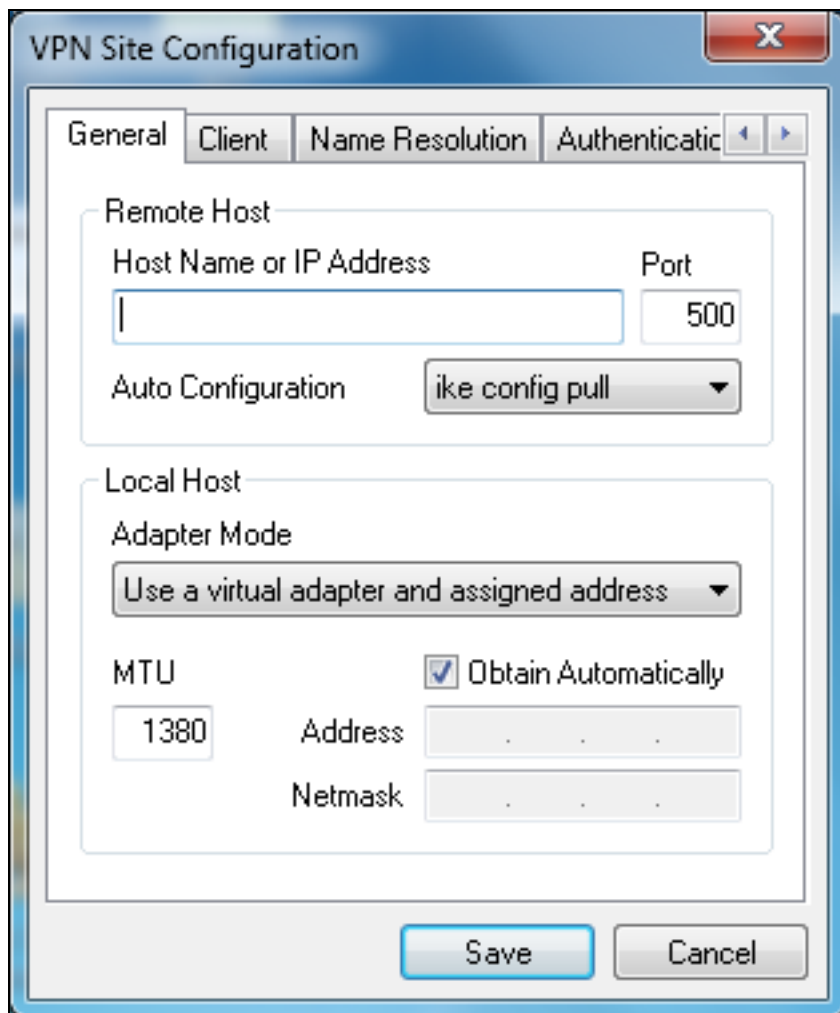
Stap 5. Klik op **Opslaan** om de instellingen op te slaan.

VPN-clientconfiguratie

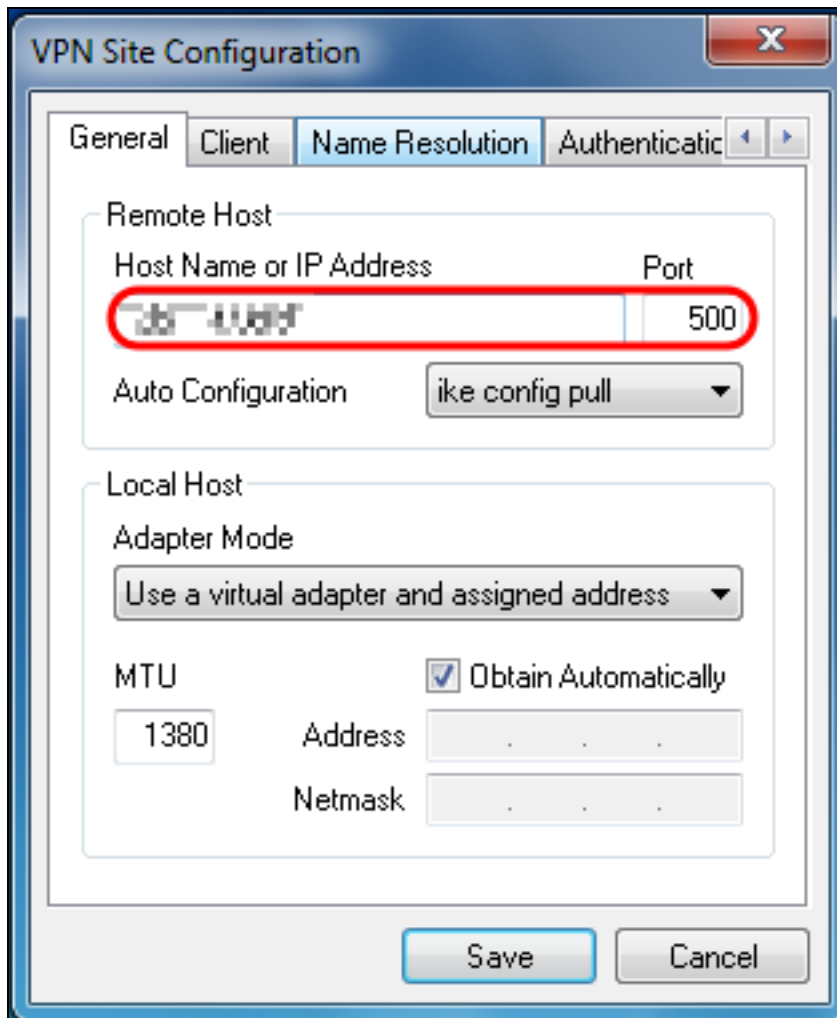
Stap 1. Open Shrew VPN Access Manager en klik op **Add** om een profiel toe te voegen.



Het venster *VPN Site Configuration* verschijnt.

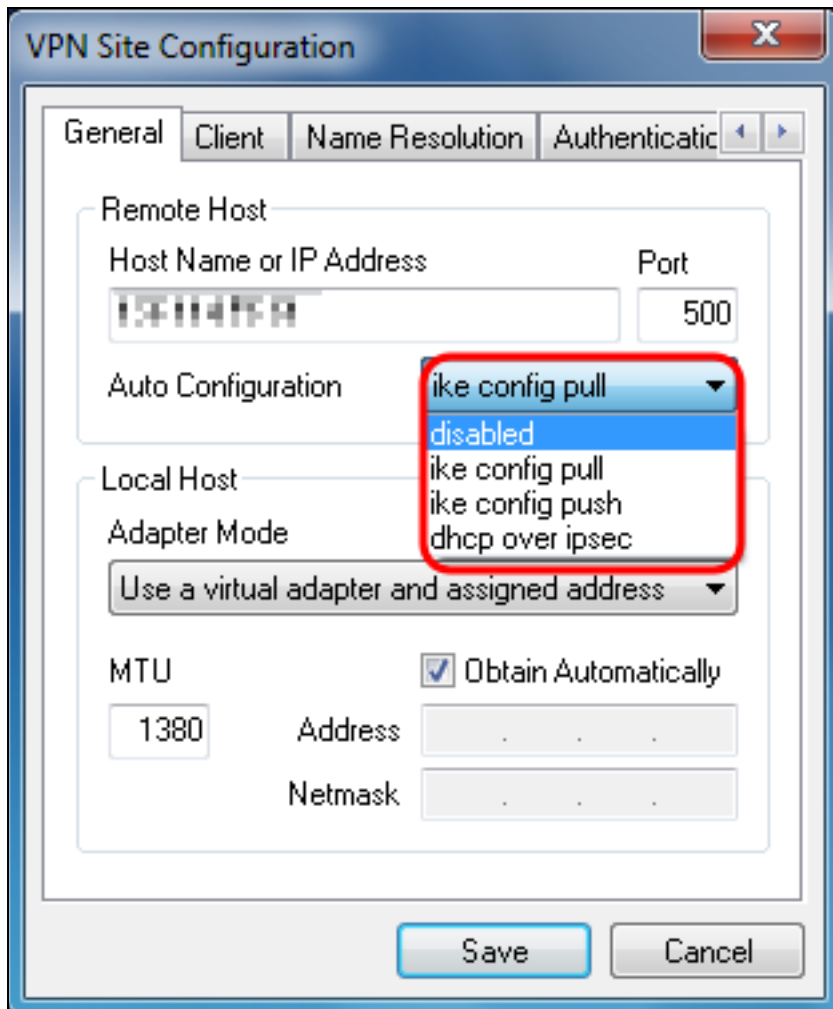


Stap 2. Voer in het gedeelte *Remote Host* onder het tabblad *General* de openbare hostnaam of het IP-adres in van het netwerk waarmee u verbinding wilt maken.



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

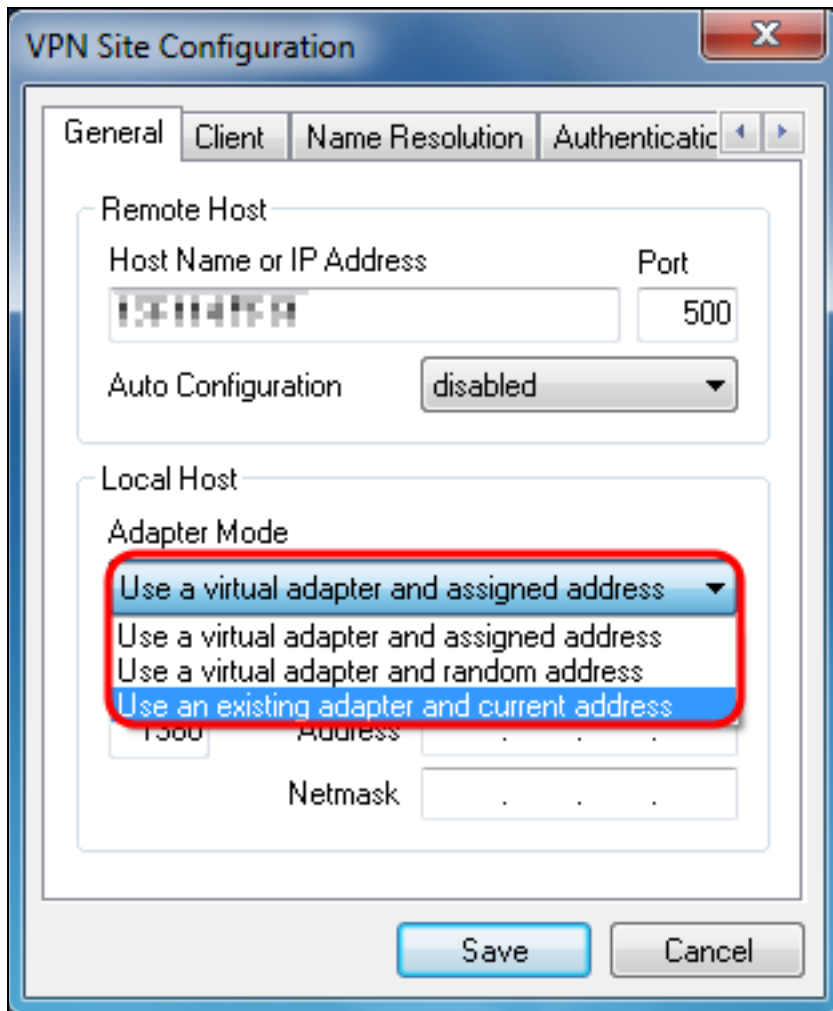
Stap 3. Kies **uitgeschakeld** in de vervolgkeuzelijst *Auto Configuration*.



De beschikbare opties zijn als volgt gedefinieerd:

- Uitgeschakeld — schakelt alle automatische clientconfiguraties uit.
- IKE Config Pull — hiermee kunnen aanvragen van een computer door de client worden ingesteld. Met de ondersteuning van de Pull methode door de computer, geeft het verzoek een lijst met instellingen terug die worden ondersteund door de client.
- IKE Config Push — geeft een computer de mogelijkheid om instellingen aan de client aan te bieden tijdens het configuratieproces. Met ondersteuning van de Push methode door de computer, geeft het verzoek een lijst met instellingen terug die worden ondersteund door de client.
- DHCP over IPsec — geeft de client de mogelijkheid om instellingen aan te vragen bij de computer via DHCP via IPsec.

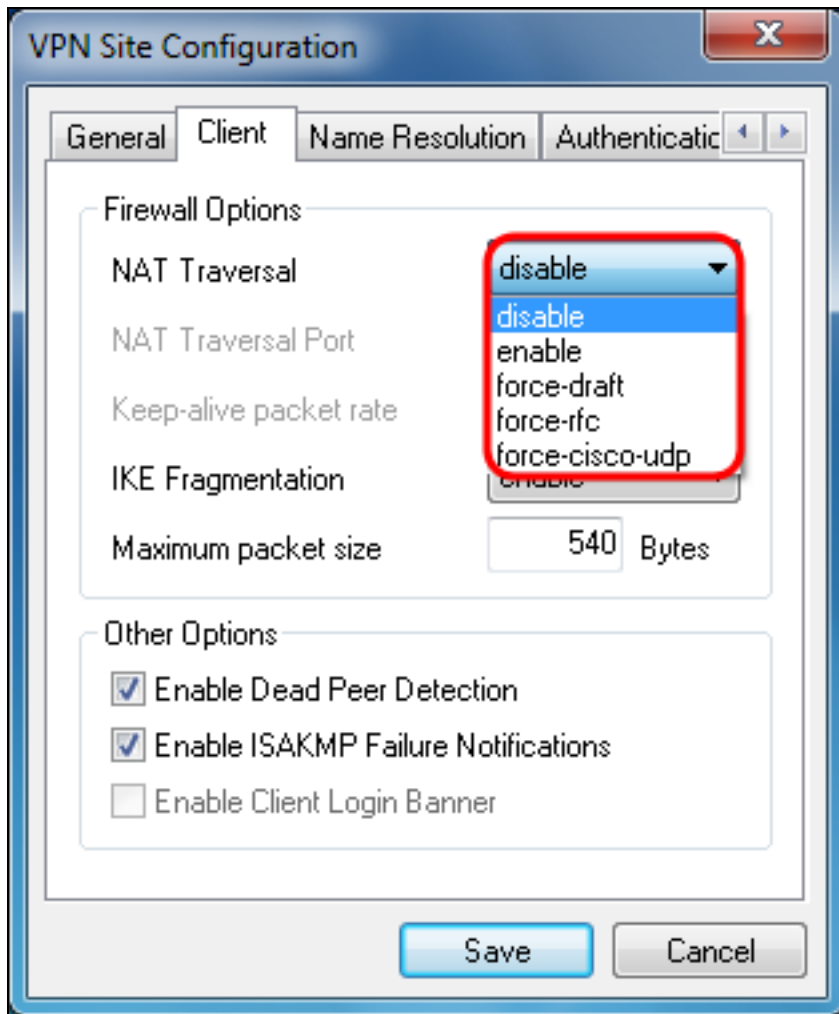
Stap 4. Kies in het gedeelte *Local Host* een bestaande adapter en huidig adres gebruiken in de vervolgkeuzelijst *Adaptermodus*.



De beschikbare opties zijn als volgt gedefinieerd:

- Gebruik een virtuele adapter en toegewezen adres — hiermee kan de client een virtuele adapter met een opgegeven adres gebruiken als bron voor IPsec-communicatie.
- Gebruik een virtuele adapter en een willekeurig adres. Hiermee kan de client een virtuele adapter met een willekeurig adres gebruiken als bron voor IPsec-communicatie.
- Gebruik een bestaande adapter en huidig adres. Hiermee kan de client alleen de bestaande, fysieke adapter met het huidige adres gebruiken als bron voor IPsec-communicatie.

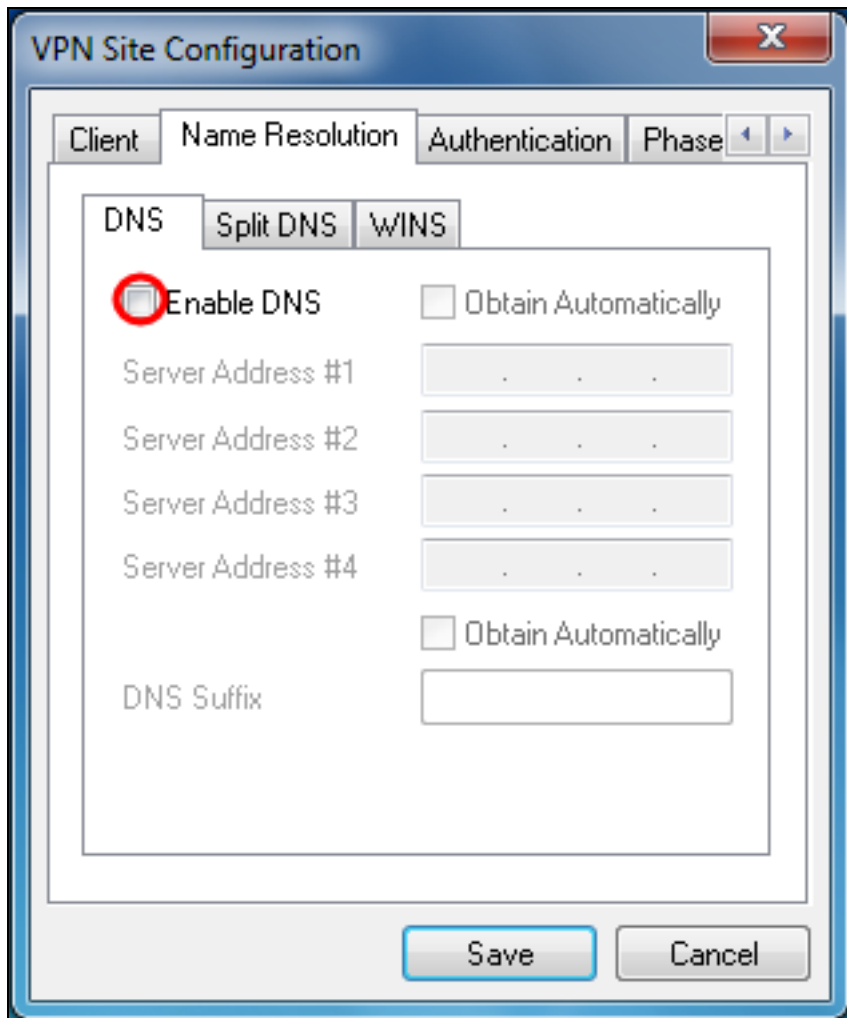
Stap 5. Klik op het tabblad *Client*. Selecteer in de vervolgkeuzelijst NAT Traversal de instelling die u in het artikel [Configuration of a IPsec VPN Server op RV130 en RV130W](#) hebt ingesteld voor de RV130/RV130W voor NAT Traversal.



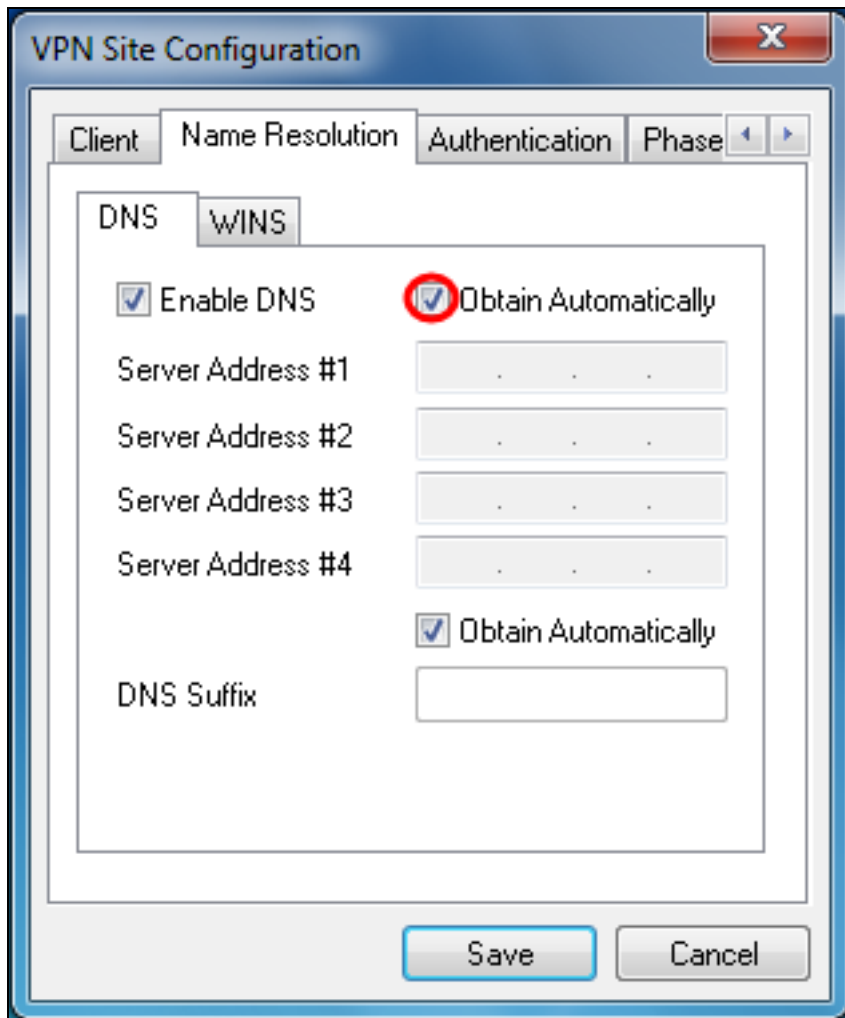
De beschikbare menuopties voor Network Address Translation Transversal (NATT) zijn als volgt gedefinieerd:

- Uitschakelen — De NAT-protocolextensies worden niet gebruikt.
- Inschakelen — De NAT-protocoluitbreidingen worden alleen gebruikt als de VPN-gateway aangeeft dat er tijdens de onderhandelingen ondersteuning is en NAT wordt gedetecteerd.
- Force-Draft — De conceptversie van de NAT-protocoluitbreidingen wordt gebruikt ongeacht of de VPN-gateway aangeeft dat er tijdens de onderhandelingen ondersteuning is verleend of dat NAT is gedetecteerd.
- Force-RFC — De RFC-versie van het NAT-protocol wordt gebruikt ongeacht of de VPN-gateway aangeeft dat er tijdens de onderhandelingen ondersteuning is of dat NAT is gedetecteerd.
- Force-Cisco-UDP — Force UDP-insluiting voor VPN-clients zonder NAT.

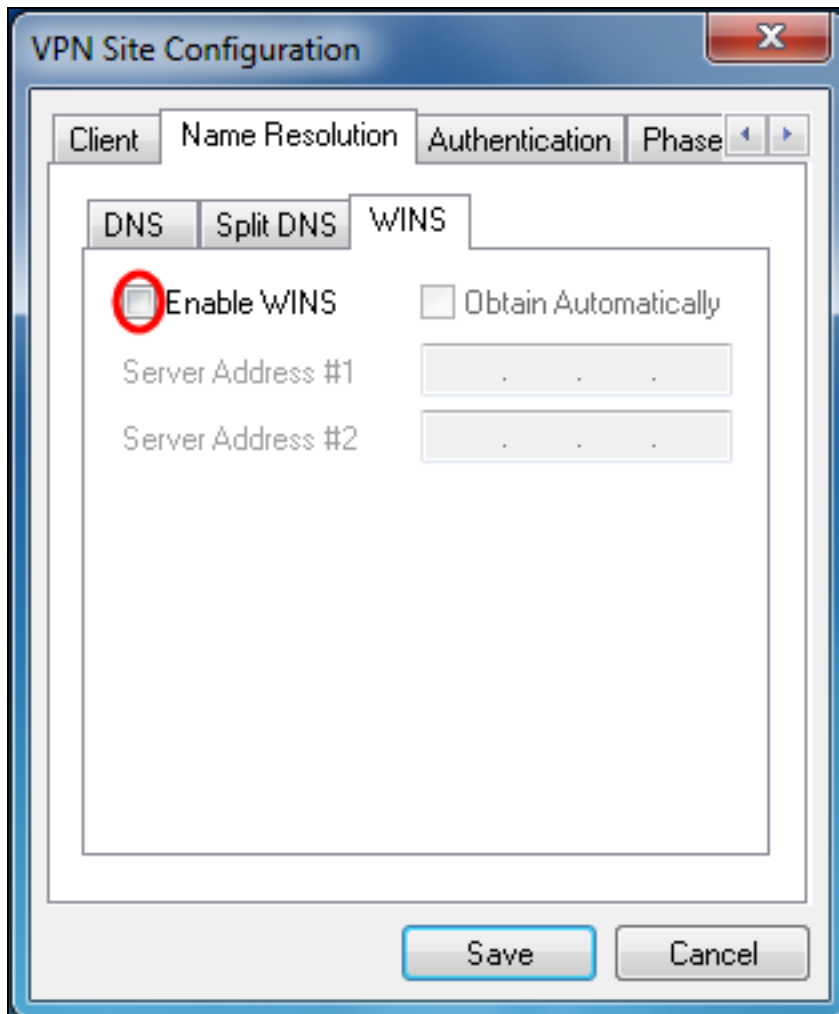
Stap 6. Klik op het tabblad *Naamresolutie* en controleer het vakje **DNS inschakelen** als u DNS wilt inschakelen. Als er geen specifieke DNS-instellingen vereist zijn voor de configuratie van uw site, schakelt u het selectievakje **DNS inschakelen** uit.



Stap 7. (Optioneel) Als uw externe gateway is geconfigureerd om de Configuration Exchange te ondersteunen, kan de gateway automatisch DNS-instellingen leveren. Als dit niet het geval is, controleert u of het aanvinkvakje **Automatisch verkrijgen** niet is ingeschakeld en voert u handmatig een geldig DNS-serveradres in.

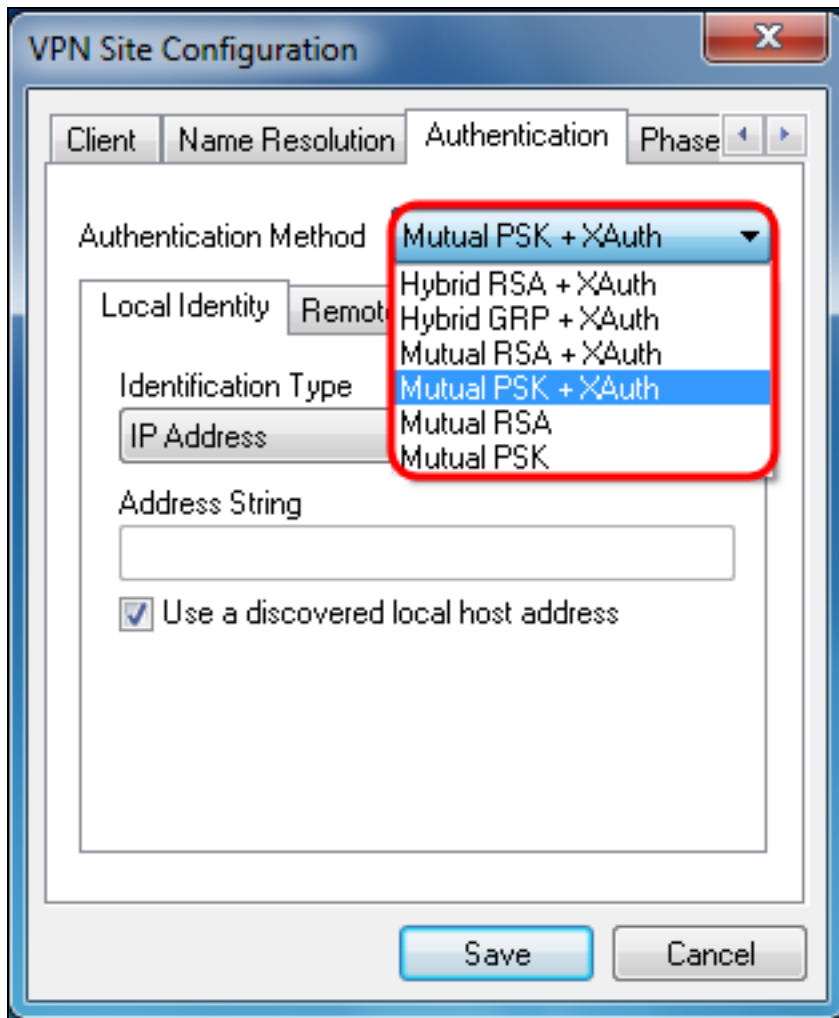


Stap 8. (Optioneel) Klik op het tabblad *Naamresolutie* en controleer het aanvinkvakje **Enable WINS** als u de Windows Internet Name Server (WINS) wilt inschakelen. Als uw externe gateway is geconfigureerd om de Configuration Exchange te ondersteunen, kan de gateway automatisch WINT-instellingen leveren. Als dit niet het geval is, controleer dan of het aanvinkvakje **Automatisch verkrijgen** niet is ingeschakeld en voer handmatig een geldig WINS-serveradres in.



Opmerking: Door WINT configuratie informatie te verstrekken, zal een client in staat zijn om WINT namen op te lossen met behulp van een server die zich in het externe privé netwerk bevindt. Dit is handig wanneer u probeert externe Windows-netwerkbronnen te benaderen met behulp van een naam van een Uniform Naming Convention path. De WINS-server zou doorgaans behoren tot een Windows Domain Controller of een Samba Server.

Stap 9. Klik op het tabblad *Verificatie* en selecteer **Mutual PSK + XAuth** in de vervolgkeuzelijst *Verificatiemethode*.



De beschikbare opties zijn als volgt gedefinieerd:

·Hybrid RSA + XAuth — De klant credential is niet nodig. De client zal de gateway verifiëren. De referenties worden geleverd in de vorm van PEM- of PKCS12-certificaatbestanden of het type sleutelbestanden.

·Hybrid GRP + XAuth — De clientreferenties zijn niet nodig. De client zal de gateway verifiëren. De referenties worden geleverd in de vorm van een PEM- of PKCS12-certificaatbestand en een gedeelde geheime tekenreeks.

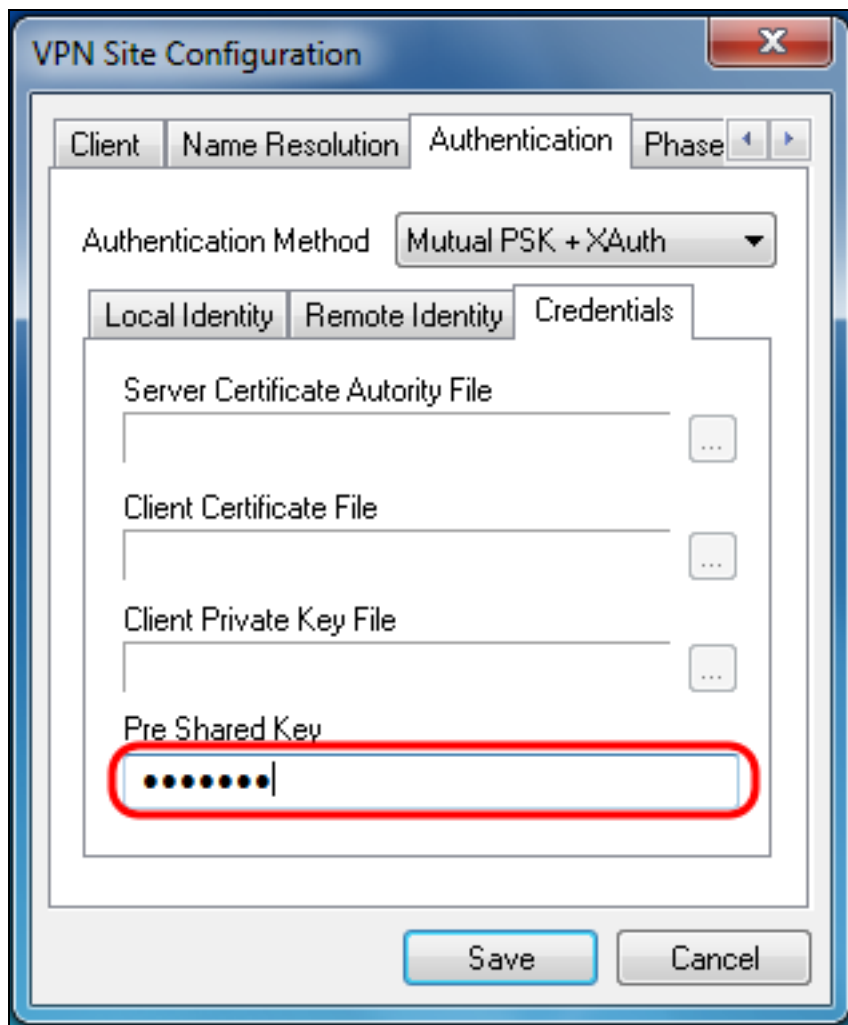
·Wederzijdse RSA + XAuth — client en gateway hebben beide referenties nodig om te verifiëren. De referenties worden geleverd in de vorm van PEM- of PKCS12-certificaatbestanden of sleuteltype.

·Wederzijdse PSK + XAuth — client en gateway hebben beide referenties nodig om te verifiëren. De referenties worden in de vorm van een gedeelde geheime string gegeven.

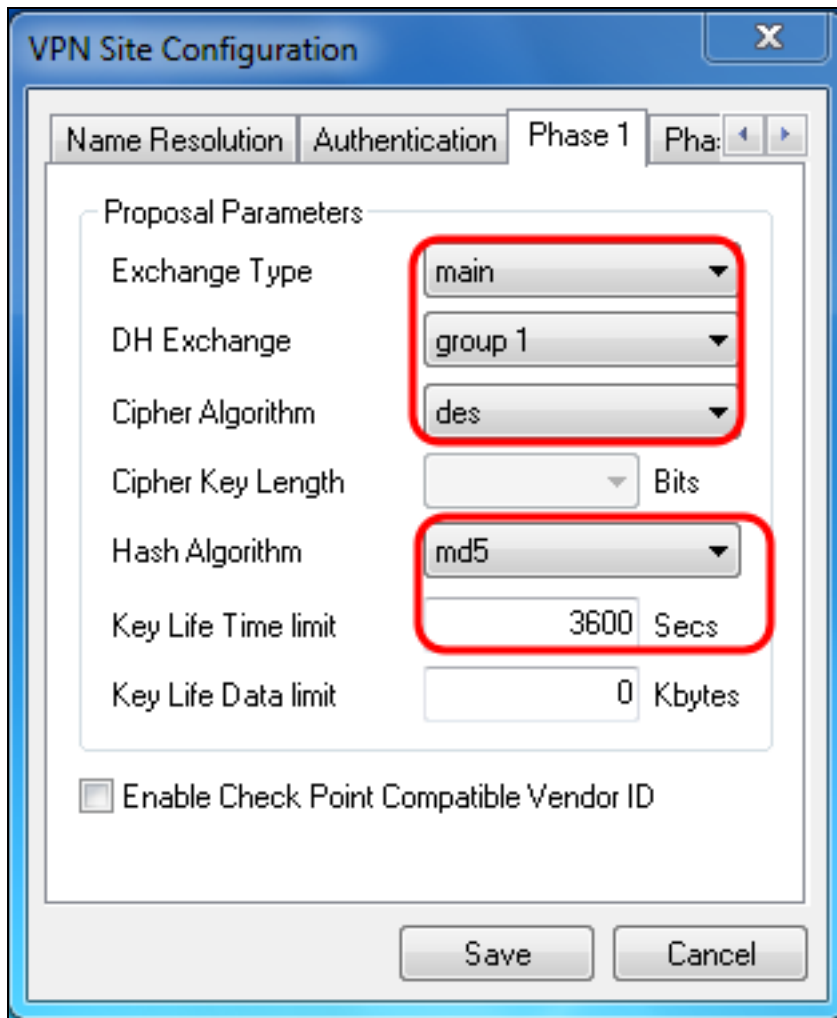
·Wederzijdse RSA — client en gateway hebben beide referenties nodig om te verifiëren. De referenties worden geleverd in de vorm van PEM- of PKCS12-certificaatbestanden of sleuteltype.

·Wederzijdse PSK — client en gateway hebben beide referenties nodig om te verifiëren. De referenties worden in de vorm van een gedeelde geheime string gegeven.

Stap 10. Klik in het gedeelte *Verificatie* op het subtabblad *Credentials* en voer in het veld *Vooraf gedeelde sleutel* in op de pagina *IPsec VPN Server Setup* in.



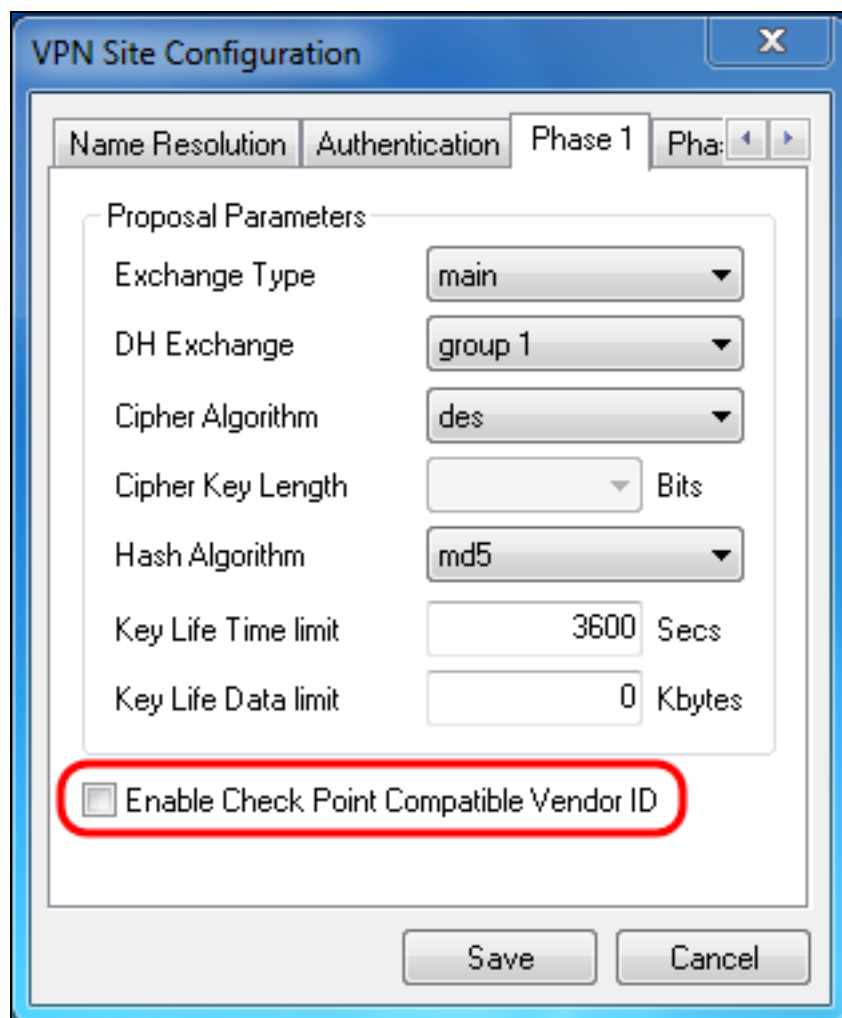
Stap 1. Klik op het tabblad *Fase 1*. Configureer de volgende parameters zodat ze dezelfde instellingen hebben als die u voor de RV130/RV130W hebt ingesteld in [Stap 2 van het gedeelte *Gebruikersconfiguratie van IPSec VPN Server*](#) in dit document.



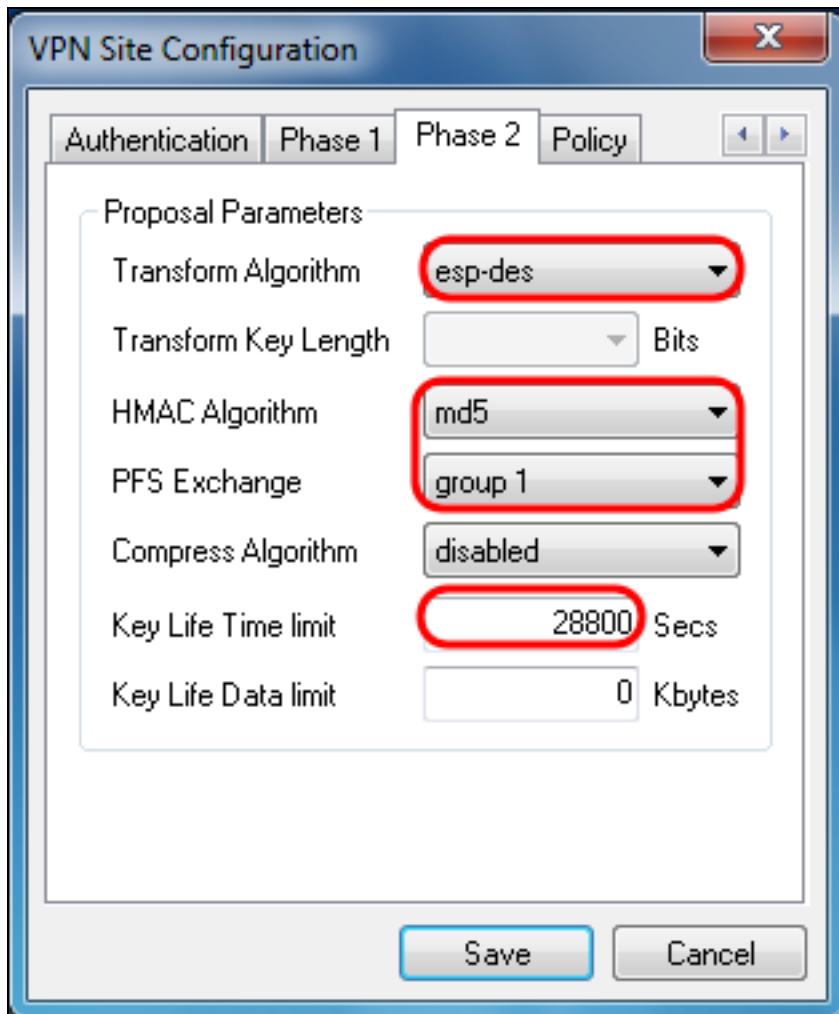
De parameters in Shrew Soft moeten als volgt overeenkomen met de RV130/RV130W-configuraties in fase 1:

- "Type uitwisseling" moet overeenkomen met "Exchange Mode".
- "DH Exchange" moet overeenkomen met "DH Group".
- De "algoritme voor codering" moet overeenkomen met de "algoritme voor codering".
- "Hash Algorithm" moet overeenkomen met "Verificatiealgoritme".

Stap 12. (Optioneel) Als uw gateway een Cisco-compatibele verkoper-ID aanbiedt tijdens fase1-onderhandelingen, vinkt u het aanvinkvakje **Enable Check Point Compatible Vendor ID** aan. Als de gateway niet, of u bent onzeker, laat de controledoos ongecontroleerd.



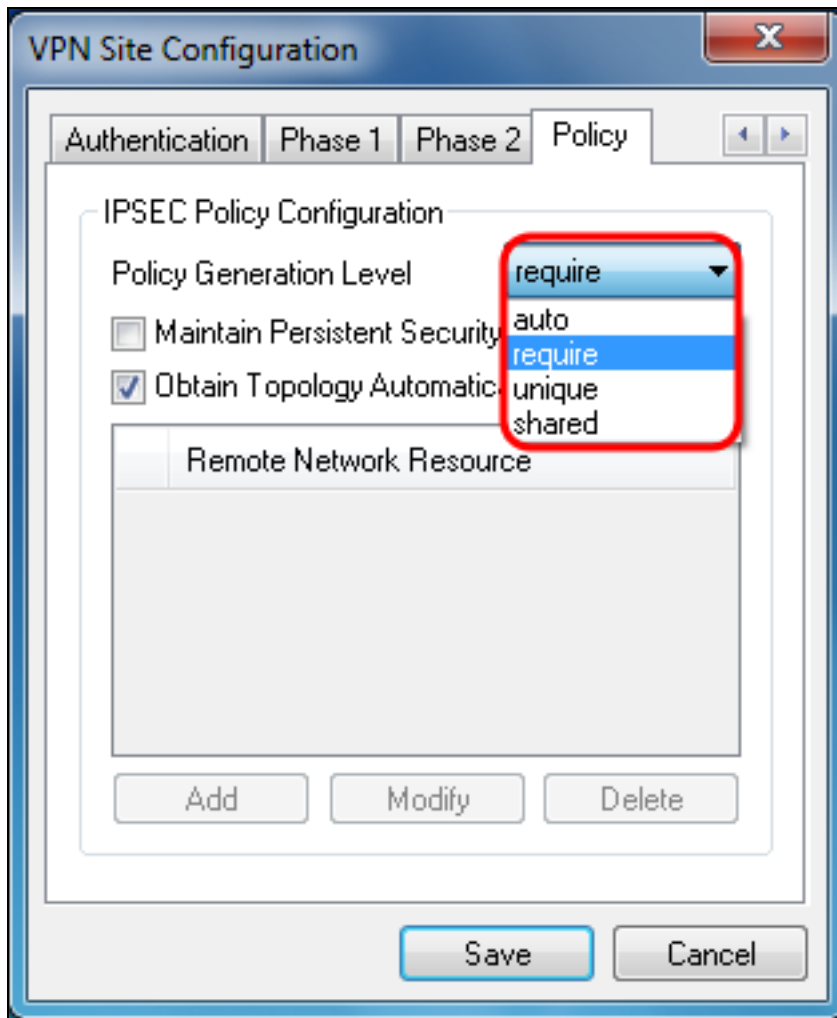
Stap 13. Klik op het tabblad *Fase 2*. Configureer de volgende parameters zodat ze dezelfde instellingen hebben als die u voor de RV130/RV130W hebt ingesteld in [Stap 2 van het gedeelte *Gebruikersconfiguratie van IPSec VPN Server*](#) in dit document.



De parameters in Shrew Soft moeten als volgt overeenkomen met de RV130/RV130W-configuraties in fase 2:

- "Transformeer algoritme" moet overeenkomen met "Encryptie algoritme".
- "HMAC-algoritme" moet overeenkomen met "Verificatiealgoritme".
- "PFS Exchange" moet overeenkomen met "DH Group" als PFS Key Group is ingeschakeld op de RV130/RV130W. Anders selecteert u **uitgeschakeld**.
- "Key Life Time limit" moet overeenkomen met "IPSec SA Lifetime".

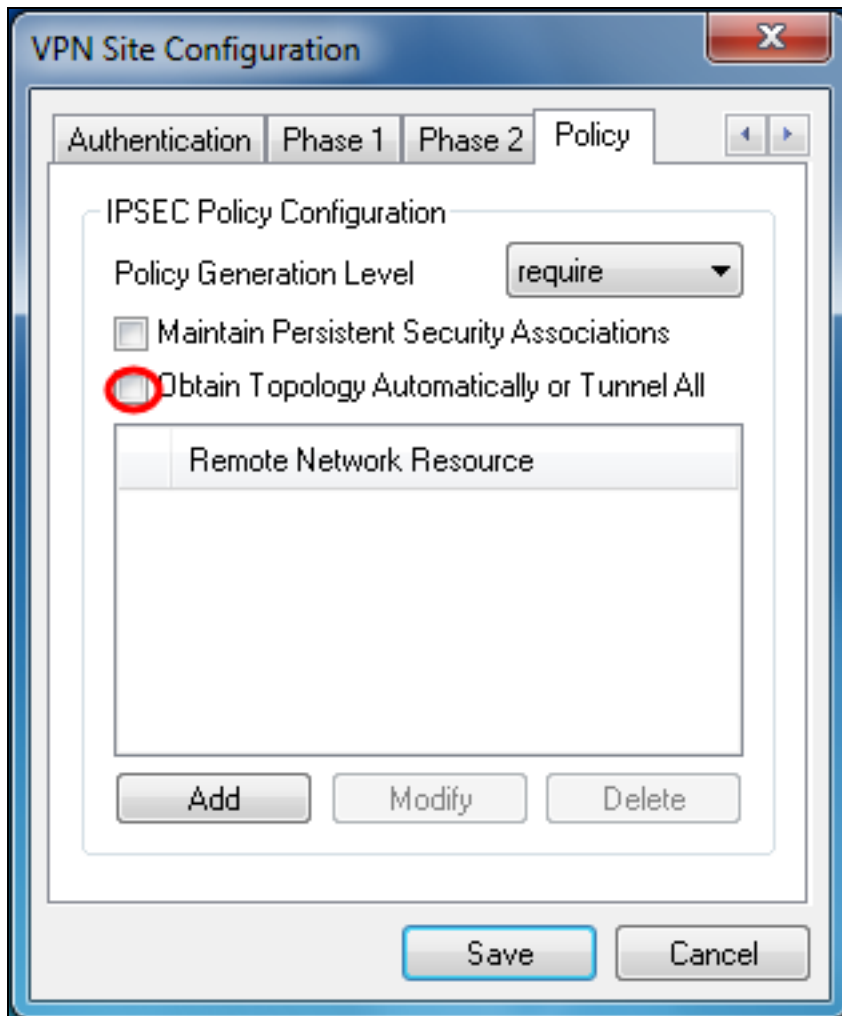
Stap 14. Klik op het tabblad *Beleid* en selecteer **Vereisen** in de vervolgkeuzelijst *Beleidsgeneratieniveau*. De optie *Policy Generation Level* wijzigt het niveau waarop IPsec-beleid wordt gegenereerd. De verschillende niveaus die in de vervolgkeuzelijst worden verstrekt brengen aan IPsec SA onderhandelingsgedrag in kaart dat door verschillende verkopersimplementaties wordt uitgevoerd.



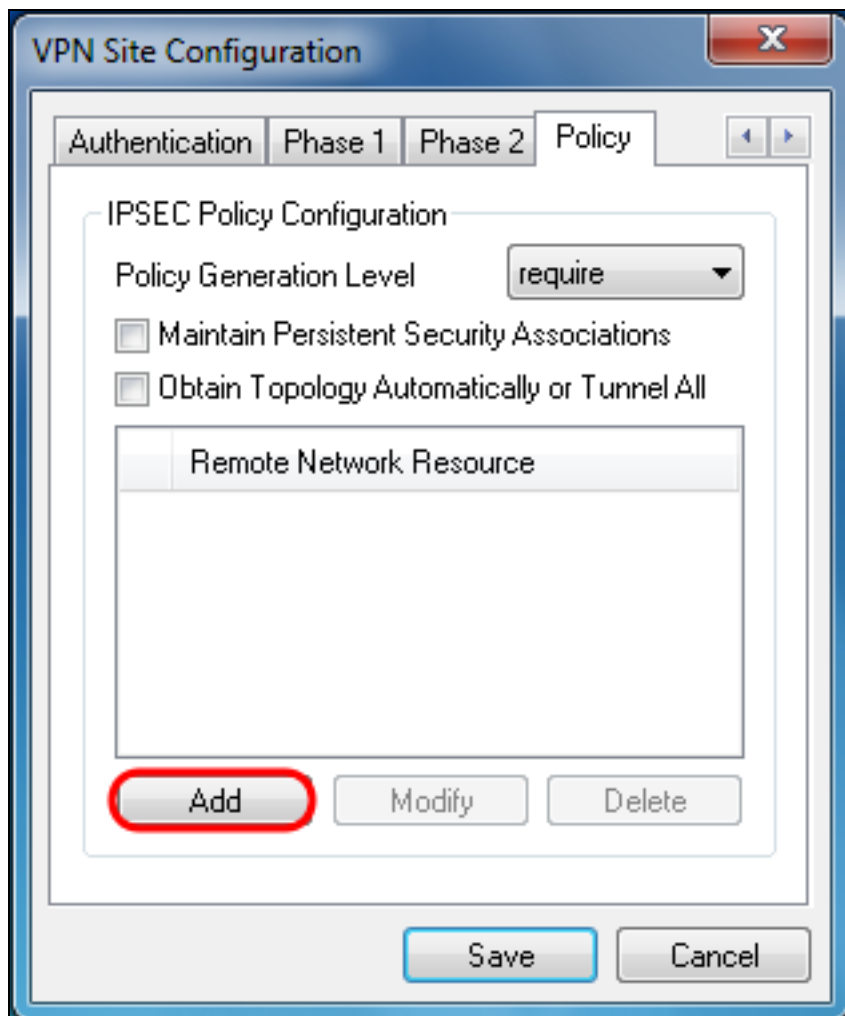
De beschikbare opties zijn als volgt gedefinieerd:

- Auto — De client bepaalt automatisch het juiste IPSec-beleidsniveau.
- Vereist — De klant zal niet onderhandelen over een unieke Security Association (SA) voor elk beleid. Beleid wordt gegenereerd met behulp van het lokale openbare adres als de lokale beleids-ID en de Remote Network Resources als de externe beleids-ID. Voor het voorstel voor fase 2 worden de beleids-ID's tijdens de onderhandelingen gebruikt.
- Uniek — De klant onderhandelt over een unieke SA voor elk beleid.
- Gedeeld - Beleid wordt gegenereerd op het vereiste niveau. In het voorstel voor fase 2 wordt de lokale beleids-ID gebruikt als lokale ID en Any (0.0.0.0/0) als externe ID tijdens de onderhandeling.

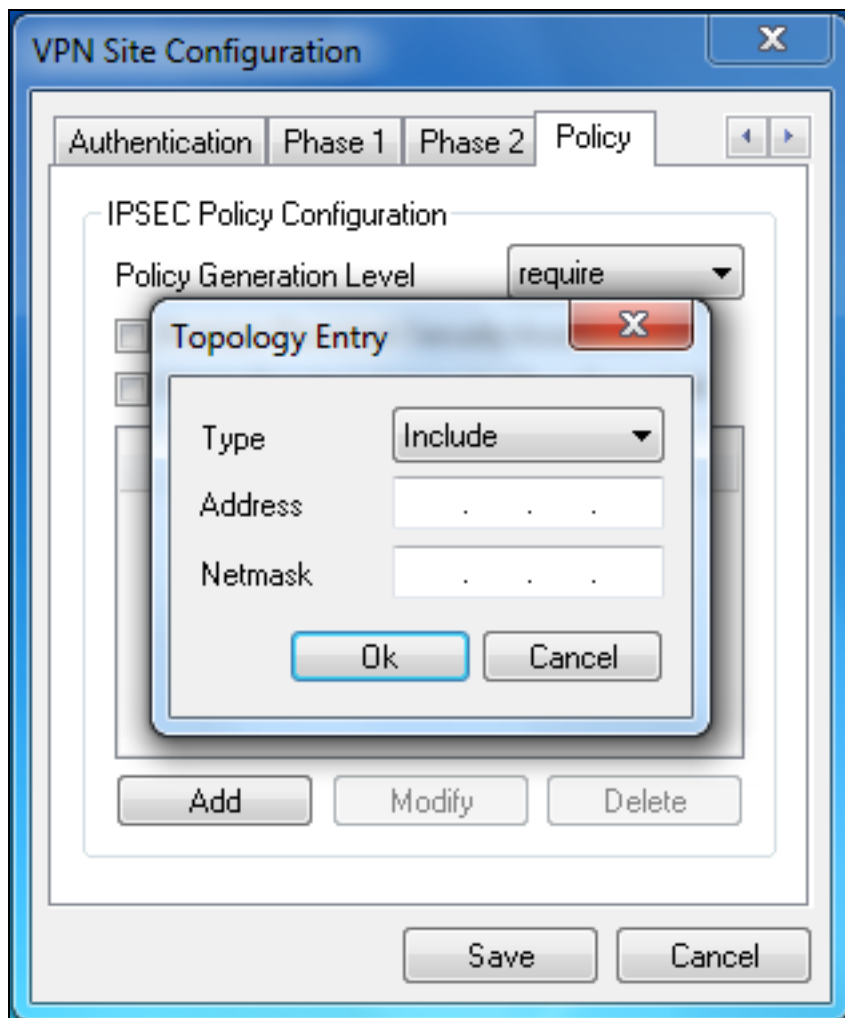
Stap 15. Schakel het aankruisvakje **Automatisch topologie verkrijgen of Alles** tunnels uit. Deze optie wijzigt de manier waarop het beveiligingsbeleid voor de verbinding is geconfigureerd. Als deze optie wordt uitgeschakeld, moet de handmatige configuratie worden uitgevoerd. Als deze optie is ingeschakeld, wordt de automatische configuratie uitgevoerd.



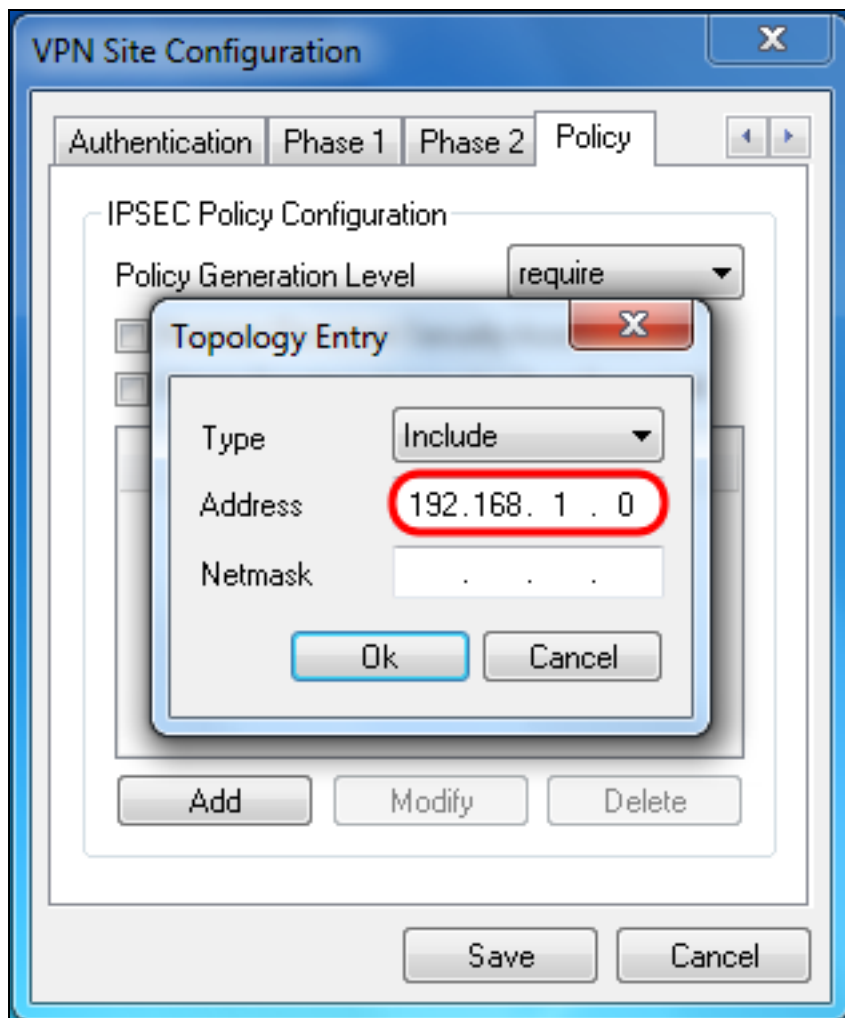
Stap 16. Klik op **Add** om de Remote Network Resource toe te voegen waarmee u verbinding wilt maken. Externe netwerkresources omvatten externe desktoptoegang, afdelingsresources, netwerkdrives en beveiligde elektronische post.



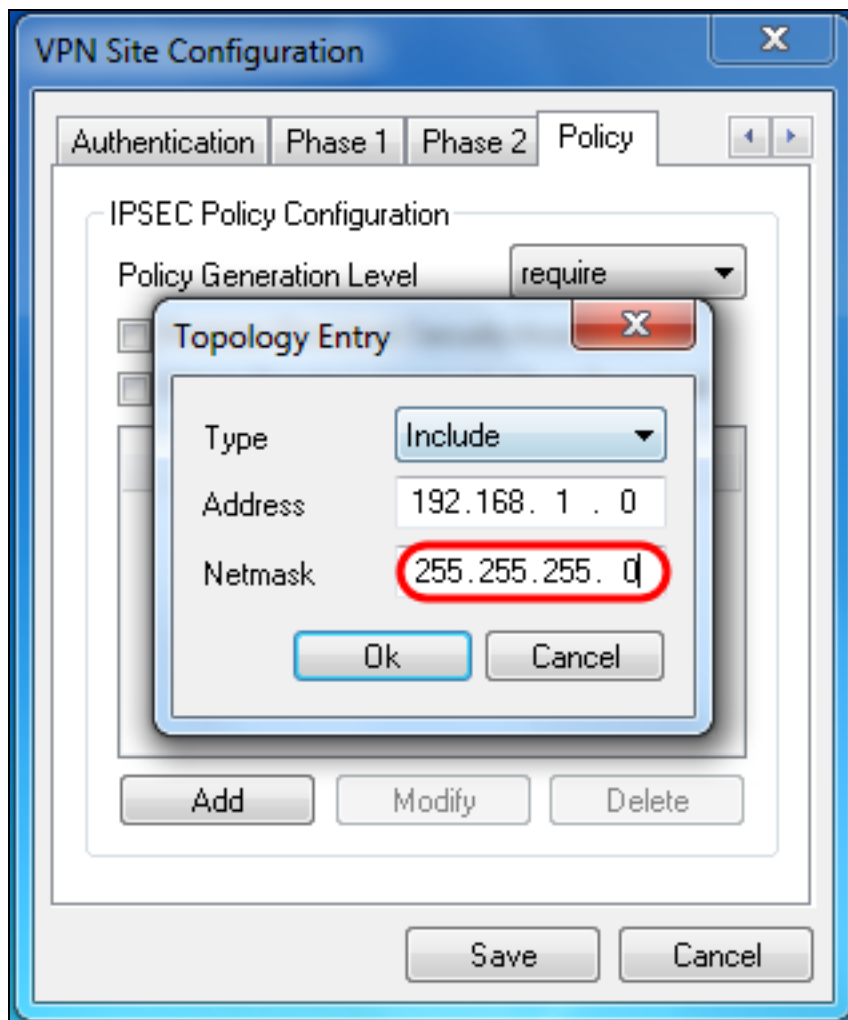
Het venster *Topology Entry* verschijnt:



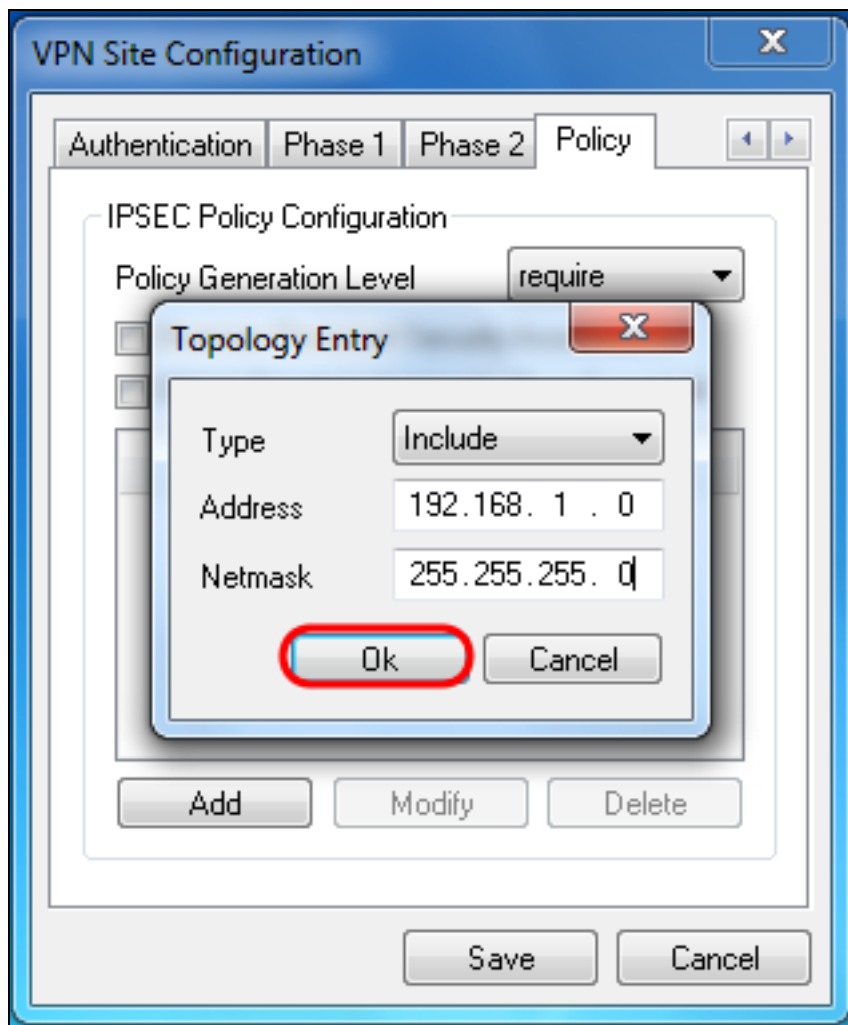
Stap 17. Voer in het veld *Adres* de subnetnummer van de RV130/RV130W in. Het adres moet overeenkomen met het veld *IP-adres* in [Stap 2 van de sectie *IPSec VPN Server Setup en Gebruikersconfiguratie*](#) van dit document.



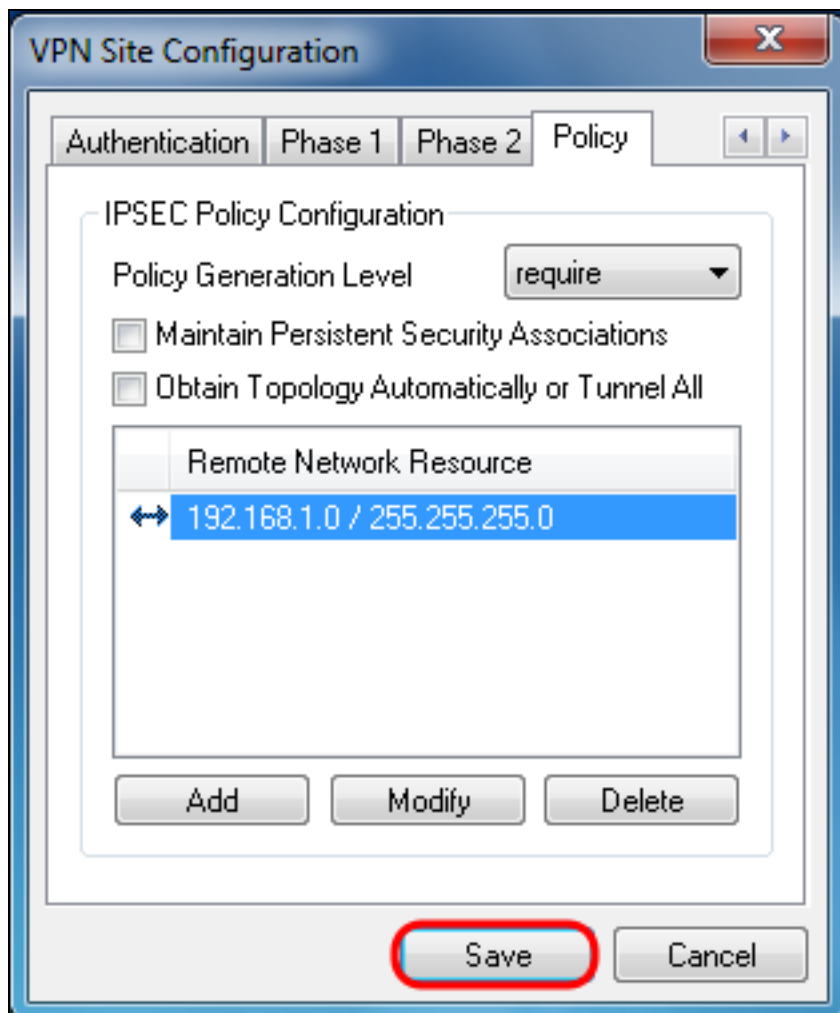
Stap 18. Voer in het veld *Netmasker* het subnetmasker in voor het lokale netwerk van de RV130/RV130W. Het netmasker moet overeenkomen met het veld *Subnet Mask* in [Stap 2 van de](#) sectie [Gebruikersconfiguratie IPsec VPN Server](#) van dit document.



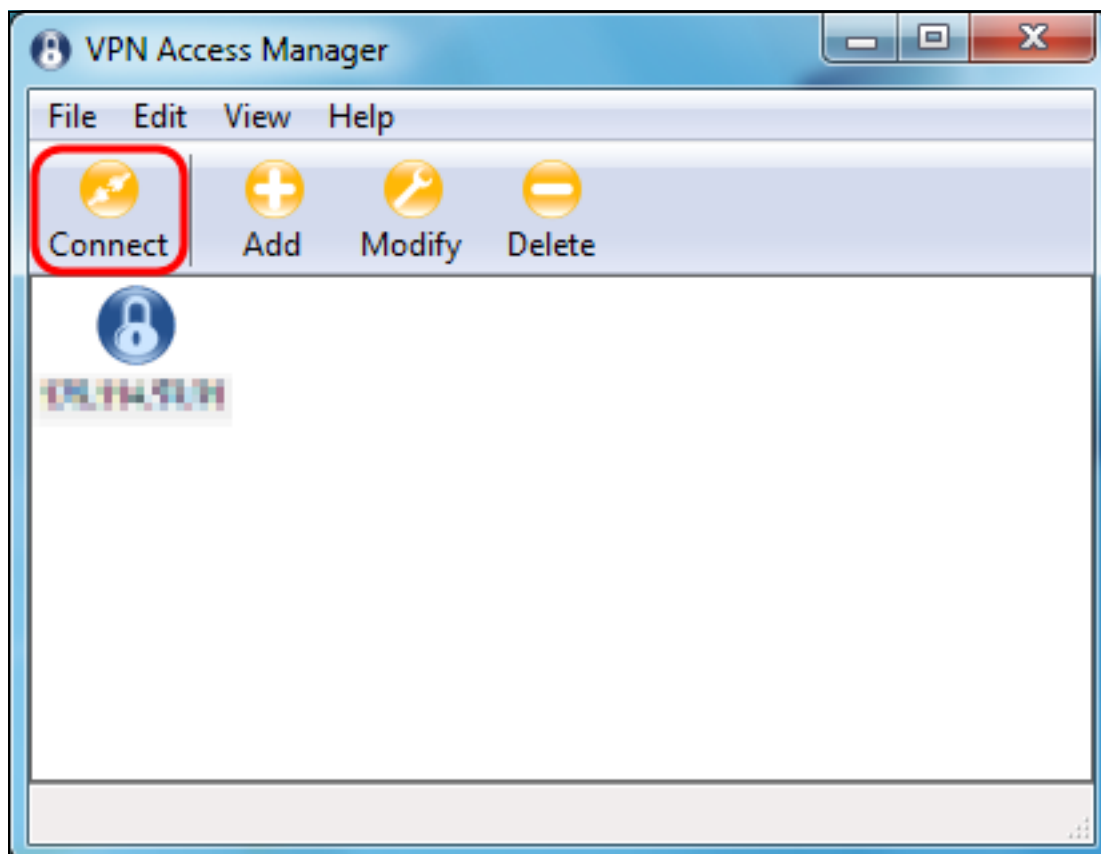
Stap 19. Klik op **OK** om de externe netwerkbron toe te voegen.



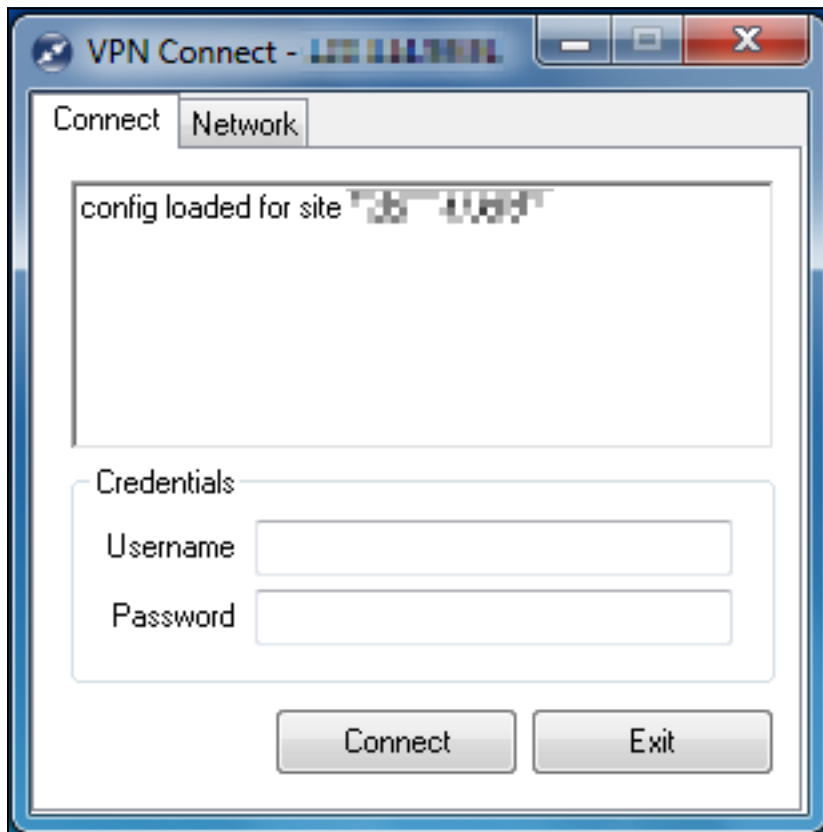
Stap 20. Klik op **Opslaan** om uw configuraties op te slaan voor verbinding met de VPN-site.



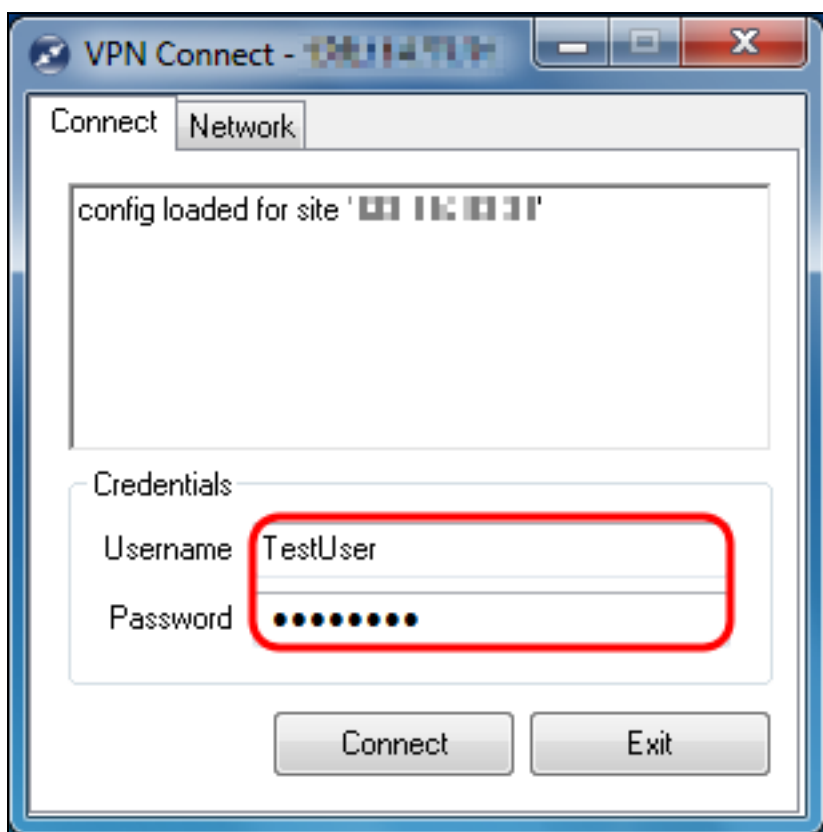
Stap 21. Ga terug naar het venster *VPN Access Manager* om de VPN-site te selecteren die u hebt geconfigureerd en klik op de knop **Verbinden**.



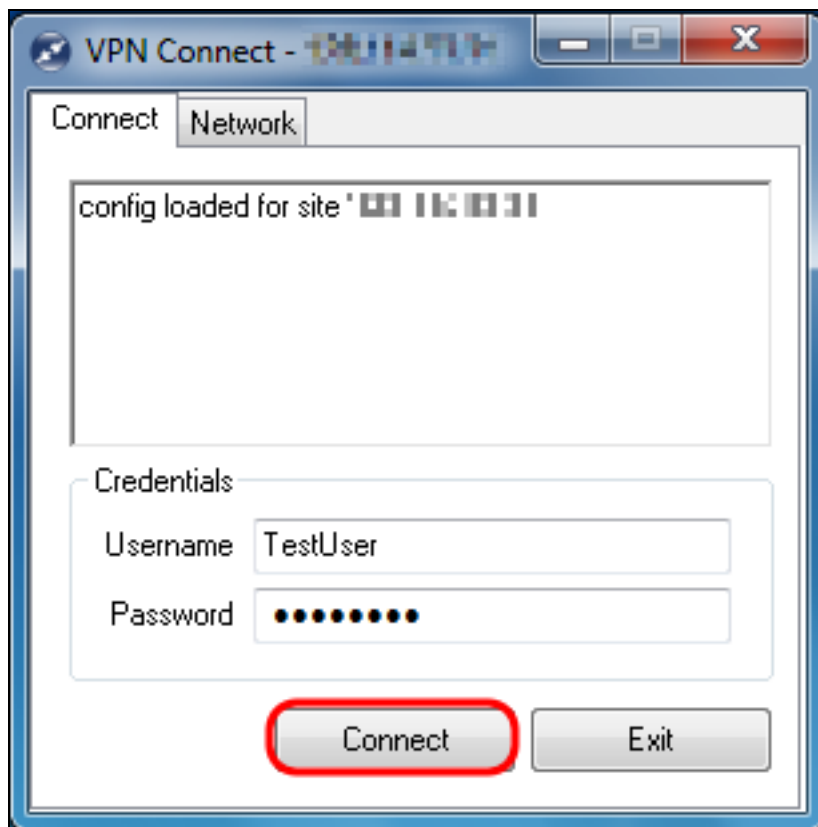
Het venster *VPN Connect* verschijnt.



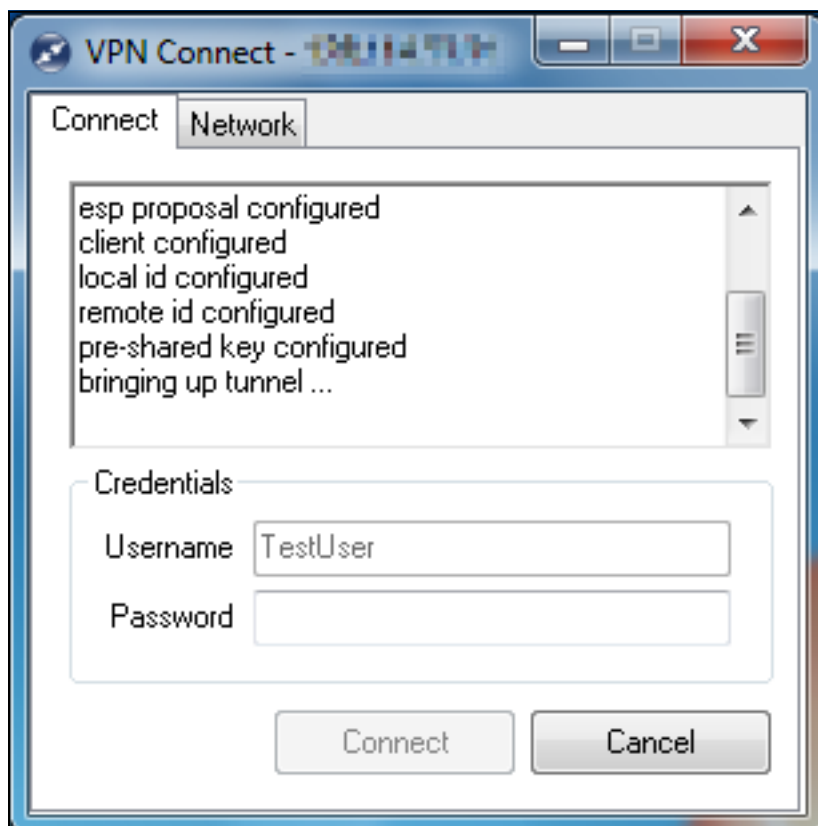
Stap 2. Voer in het gedeelte *Credentials* de gebruikersnaam en het wachtwoord in van de account die u in [Stap 4 van het](#) gedeelte [Gebruikersconfiguratie van de IPSec VPN-server](#) van dit document hebt ingesteld.

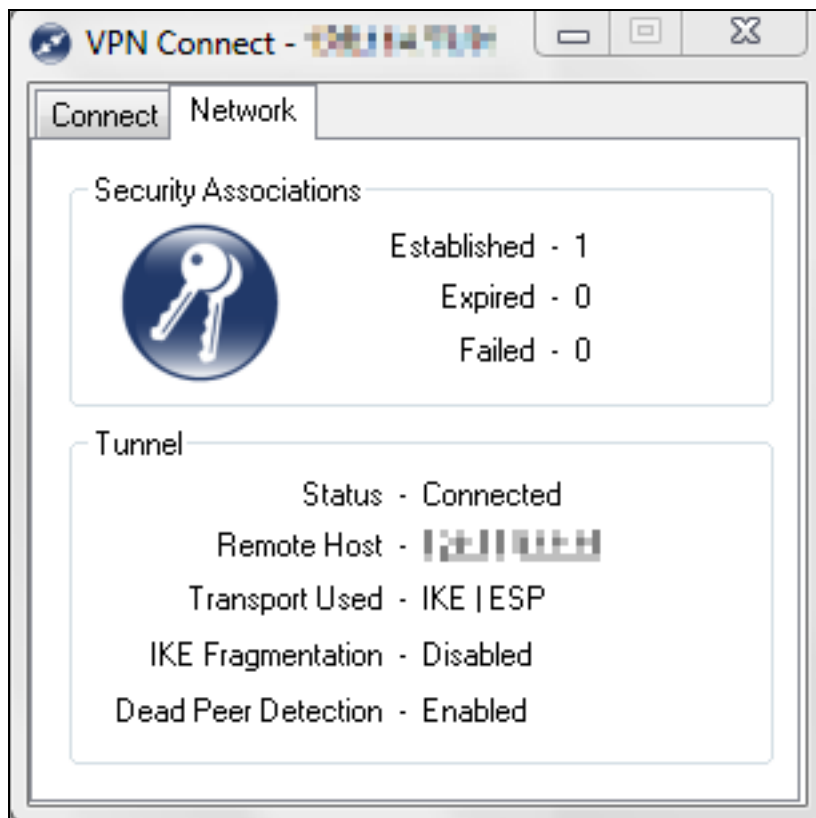


Stap 23. Klik op **Verbinding maken** met VPN in de RV130/RV130W.



De IPSec VPN-tunnel is tot stand gebracht en de VPN-client heeft toegang tot de bron achter de RV130/RV130W LAN.





[Bekijk een video met betrekking tot dit artikel...](#)

[Klik hier om andere Tech Talks van Cisco te bekijken](#)

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.