Het configureren van een site-to-site VPN-tunnel tussen Cisco RV320 Gigabit VPN-router met dubbel WAN en Cisco 500 Series geïntegreerde services adapter

Doel

Een Virtual Private Network (VPN) bestaat als een technologie die veel wordt gebruikt om externe netwerken aan te sluiten op een hoofdnetwerk, waarbij een particuliere link wordt gesimuleerd in de vorm van een versleuteld kanaal via openbare lijnen. Een extern netwerk kan met een privé hoofdnetwerk verbinden alsof het als deel van het privé hoofdnetwerk zonder veiligheidszorgen bestaat vanwege een 2-fase onderhandeling die het VPN-verkeer versleutelt op een manier die alleen de VPN-endpoints weten hoe ze moeten decrypteren. Deze korte handleiding biedt een voorbeeldontwerp voor het bouwen van een site-to-site IPsec VPN-tunnel tussen een Cisco 500 Series geïntegreerde services adapter en een Cisco RV Series router.

Toepasselijke apparaten

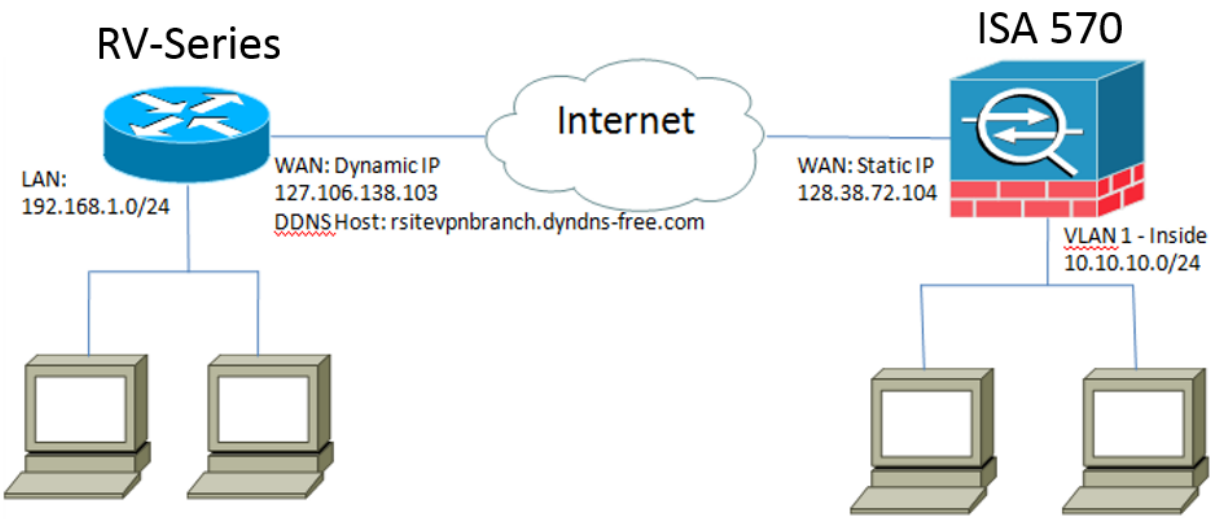
- Cisco RV Series routers (RV320)
- Cisco 500 Series geïntegreerde services adapters (ISA570)

Softwareversie

- 4.2.2.08 [Cisco RV0xx Series VPN-routers]

Voorconfiguratie

Netwerkdiagram
Het volgende toont een Site-to-Site VPN-topologie.



Een site-to-site IPsec VPN-tunnel wordt geconfigureerd en geïnstalleerd tussen de Cisco RV Series router in het Remote Office en Cisco 500 Series ISA in het hoofdkantoor. Dankzij deze configuratie kan een host in LAN 192.168.1.0/24 bij het Remote Office en een host in LAN 10.10.10.0/24 bij het Main Office veilig via VPN met elkaar communiceren.

Core Concepts

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is het protocol dat wordt gebruikt om een Security Association (SA) in de IPsec-protocolreeks in te stellen. IKE bouwt voort op het Oakley Protocol, Internet Security Association en Key Management Protocol (ISAKMP), en gebruikt een Diffie-Hellman sleuteluitwisseling om een gedeeld sessiegeheim op te zetten, waarvan cryptografische sleutels zijn afgeleid.

Internet Security Association en Key Management Protocol (ISAKMP)

Internet Security Association en Key Management Protocol (ISAKMP) wordt gebruikt om te onderhandelen over de VPN-tunnel tussen twee VPN-endpoints. De client definieert de procedures voor verificatie, communicatie en sleutelgeneratie, en wordt door het IKE-protocol gebruikt om encryptiesleutels uit te wisselen en de beveiligde verbinding tot stand te brengen.

Internet Protocol Security (IPsec)

IP Security Protocol (IPsec) is een protocolreeks om IP-communicatie te beveiligen door elk IP-pakket van een gegevensstroom te authentiseren en te versleutelen. IPsec omvat ook protocollen voor het instellen van wederzijdse authenticatie tussen agents aan het begin van de sessie en het onderhandelen over cryptografische sleutels die tijdens de sessie gebruikt moeten worden. IPsec kan worden gebruikt om gegevensstromen tussen een paar hosts, gateways of netwerken te beveiligen.

Ontwerptips

VPN-topologie - Een point-to-point VPN-topologie betekent dat een beveiligde IPsec-tunnel wordt geconfigureerd tussen de hoofdsite en de externe site.
Bedrijven vereisen vaak meerdere verre plaatsen in een multisite topologie, en voeren of een hub-en-gesproken VPN topologie of de volledige topologie van vermaasd VPN uit. Een hub-en-gesproken VPN-topologie betekent dat externe sites geen communicatie met andere externe sites nodig hebben, en elke externe site stelt alleen een beveiligde IPsec-tunnel met de hoofdsite in. Een volledige netwerk van VPN topologie betekent dat de verre plaatsen communicatie met andere verre plaatsen vereisen en elke verre plaats voert een beveiligd IPsec tunnelpunt met de hoofdplaats en alle andere verre plaatsen in.
VPN-verificatie - Het IKE-protocol wordt gebruikt om VPN-peers voor verificatie te zorgen bij het maken van een VPN-tunnel. Er bestaan verschillende IKE-authenticatiemethoden en een vooraf gedeelde sleutel is de meest handige methode. Cisco raadt het toepassen van een sterke voorgedeelde toets aan.
VPN Encryptie - Om de vertrouwelijkheid van gegevens te verzekeren die over VPN worden getransporteerd, worden er encryptie-algoritmen gebruikt om de lading van IP-pakketten te versleutelen. DES, 3DES en AES zijn drie gemeenschappelijke coderingsstandaarden. AES wordt als het meest beveiligde beschouwd in vergelijking met DES en 3DES. Cisco raadt het toepassen van AES-128-bits of hogere codering (bijvoorbeeld AES-192 en AES-256) sterk aan. Niettemin, vereisen de sterkere encryptie algoritmen meer verwerkingsmiddelen van een router.
Dynamic WAN IP Adressatie en Dynamic Domain Name Service (DDNS) — De VPN-tunnel moet tussen twee openbare IP-adressen worden ingesteld. Als de WAN-routers statische IP-adressen van de Internet Service Provider (ISP) ontvangen, kan de VPN-tunnel rechtstreeks worden geïmplementeerd via statische openbare IP-adressen. Maar de meeste kleine bedrijven gebruiken rendabele breedbandinternetservices zoals DSL of kabel en ontvangen dynamische IP-adressen van hun ISP's. In dergelijke gevallen kan Dynamic Domain Name Service (DDNS) worden gebruikt om het dynamische IP-adres in kaart te brengen naar een volledig gekwalificeerde domeinnaam (FQDN).
LAN IP-adressering — Het privé LAN-netwerkadres van elke site mag geen overlappingen hebben. Het standaard LAN IP-netwerkadres op elke externe site moet altijd worden gewijzigd.

Tips voor configuratie

Selectieknop vooraf configureren
Stap 1. Sluit een Ethernet-kabel tussen de RV320 en de DSL- of kabelmodem en sluit een Ethernet-kabel aan tussen de ISA570 en zijn DSL- of kabelmodem.
Stap 2. Sluit de RV320 aan en sluit vervolgens interne pc’s, servers en andere IP-apparaten aan op de LAN-poorten van RV320.
Stap 3. Sluit de ISA570 aan en sluit vervolgens interne PC's, servers en andere IP-apparaten aan op de LAN-poorten van de ISA570.
Stap 4. Controleer of u de IP-adressen van het netwerk op elke locatie op verschillende subnetwerken wilt configureren. In dit voorbeeld wordt gebruik gemaakt van 192.168.1.0 op de Remote Office-LAN-router en wordt 10.10.10.0 gebruikt.
Stap 5. Controleer of de lokale pc’s op hun respectievelijke routers en andere pc’s op hetzelfde LAN kunnen aansluiten.

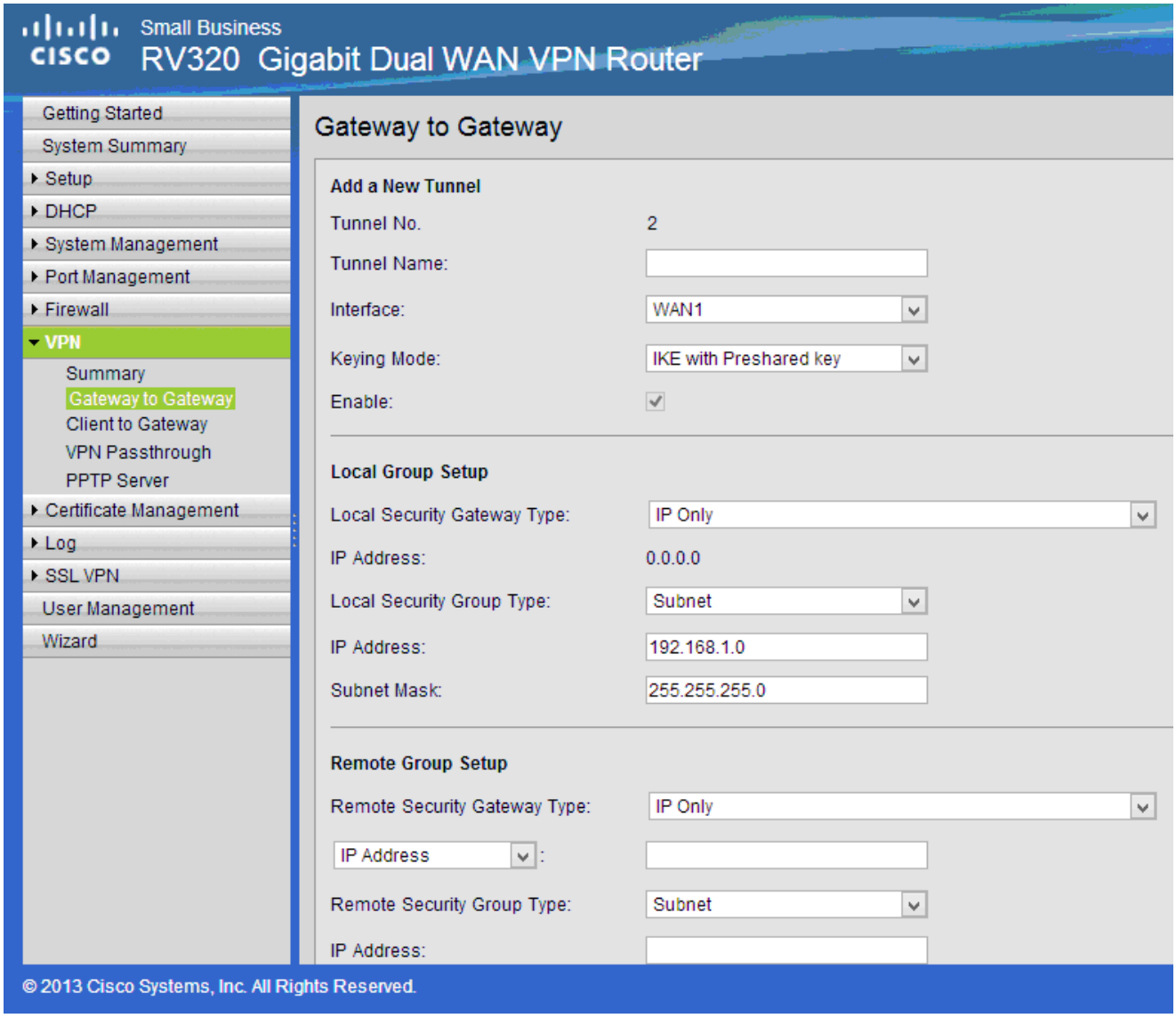
WAN-verbinding identificeren

U moet weten of uw ISP een dynamisch IP-adres of een statisch IP-adres verstrekt. De ISP verstrekt gewoonlijk een dynamisch IP adres, maar u zou dit moeten bevestigen alvorens de

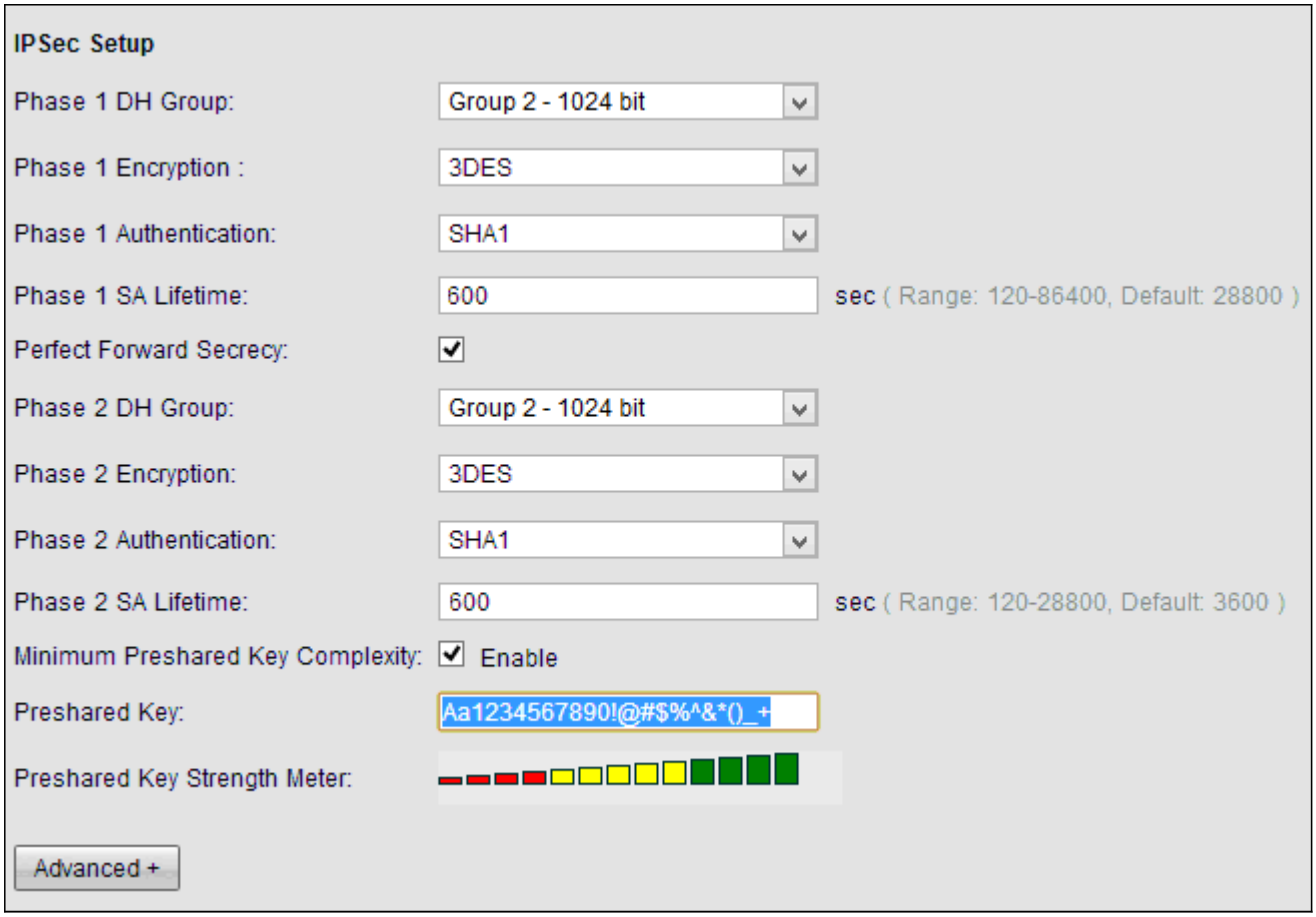
site-to-site VPN tunnelconfiguratie uit te voeren.

De site-to-Site IPsec VPN-tunnelheid configureren voor RV320 op het Remote Office

Stap 1. Ga naar **VPN > Gateway-to-Gateway** (zie afbeelding)
a.) Voer een tunnelnaam in, zoals RemoteOffice.
b) Interface op WAN1 instellen.
c.) Zet de Keying Mode in op IKE met de PreShared Key.
d.) Voer lokaal IP-adres en Remote IP-adres in.
De volgende afbeelding toont RV320 Gigabit VPN-routergateway met dubbel WAN naar gateway:



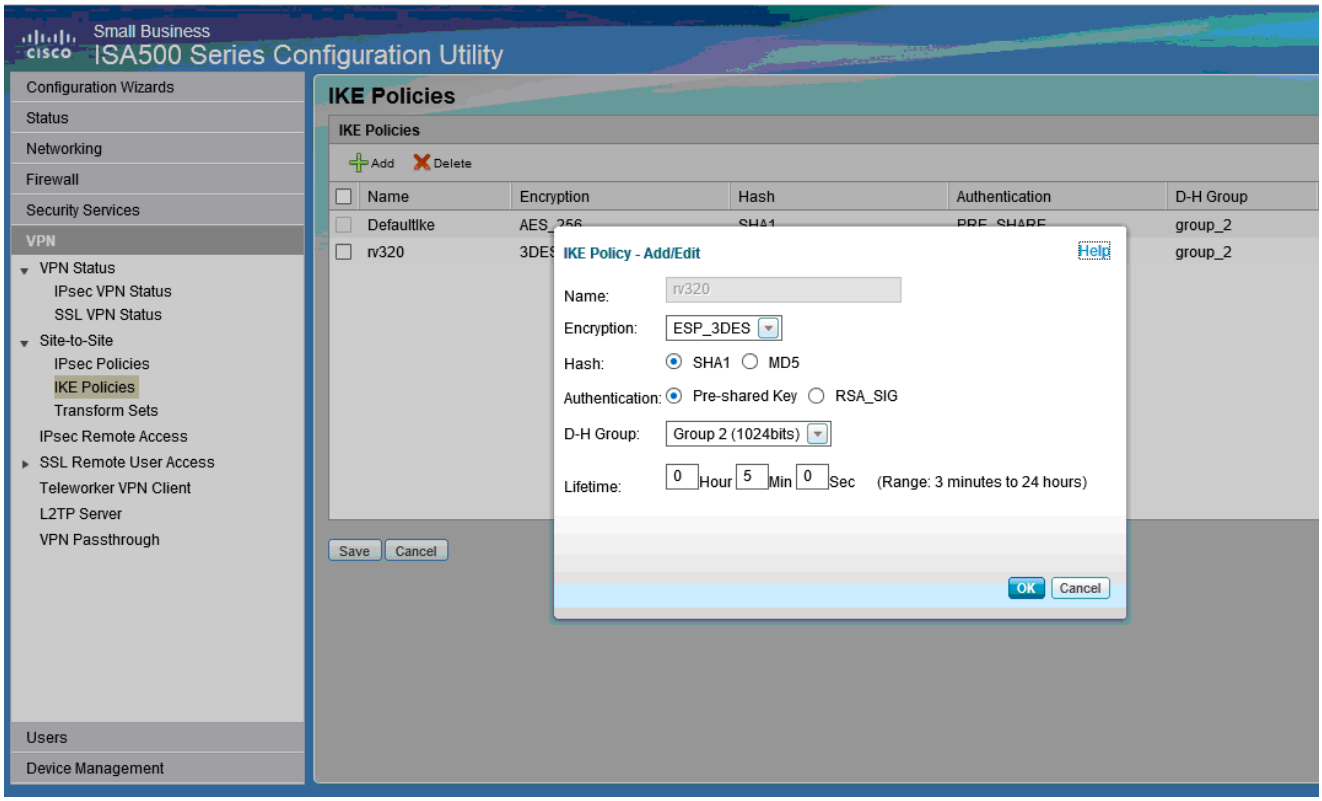
Stap 2. Stel IPSec Tunnel instellingen in (zie afbeelding)
a.) Stel *encryptie* in op 3DES.
b) Stel *verificatie* in op SHA1.
c.) Controleer *of uw geheimhouding perfect is.*
d.) Stel de *gedeelde sleutel in* (dit moet hetzelfde zijn op beide routers).
Hieronder staat IPSec Setup (Fase 1 en 2):



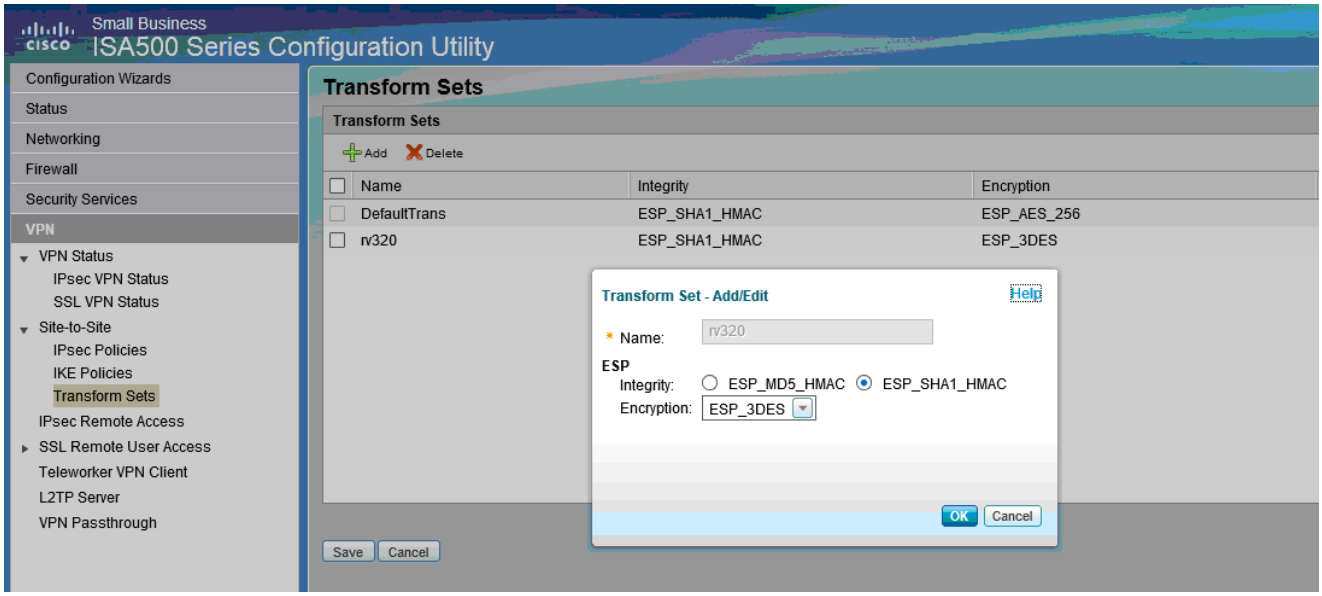
Opmerking: Houd in gedachten dat de IPsec-tunnelinstellingen aan beide zijden van de site-to-site IPsec VPN-tunnel moeten overeenkomen. Als er verschillen bestaan tussen de IPsec-tunnelinstellingen van RV320 en ISA570, kunnen beide apparaten niet onderhandelen over de coderingstoets en geen verbinding maken.
Stap 3. Klik op **Save** om de configuratie te voltooien.

Het configureren van de Site-to-Site IPsec VPN-tunnelheid voor ISA570 bij het hoofdkantoor

Stap 1. Ga naar **VPN > IKE-**beleid (zie afbeelding)
a.) Stel *encryptie* in op ESP_3DES.
b) Zet *Hash* op SHA1.
c.) Stel *verificatie in* op Pre-Shared Key.
d.) Stel *D-H groep* in op groep 2 (1024 bits).
De volgende afbeelding toont IKE-beleid:



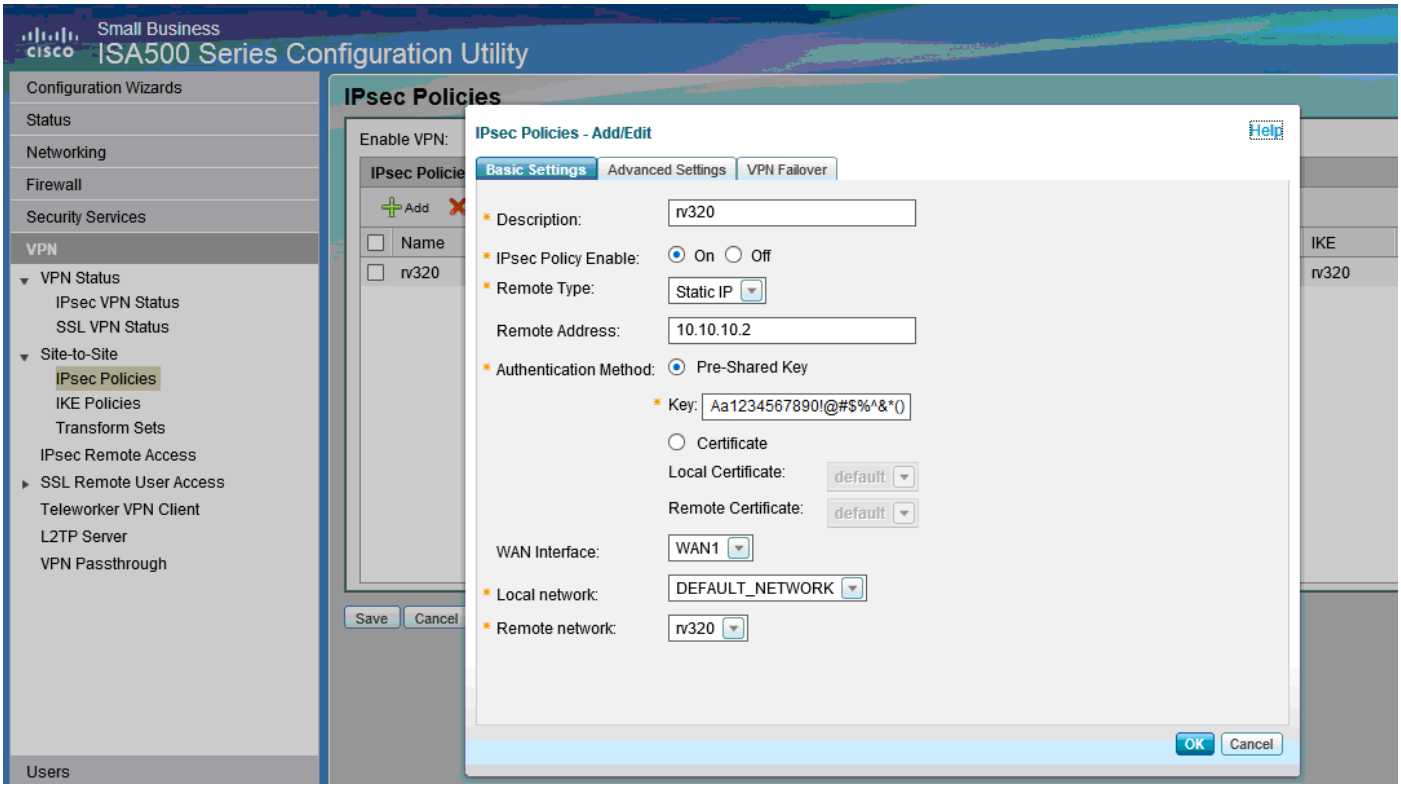
Stap 2. Ga naar **VPN > Stapels voor IKE-transformatie** (zie afbeelding)
a.) Stel *Integriteit* in op ESP_SHA1_HMAC.
b) Stel *encryptie* in op ESP_DES.
De volgende instellingen voor IKE-omzetting worden weergegeven:



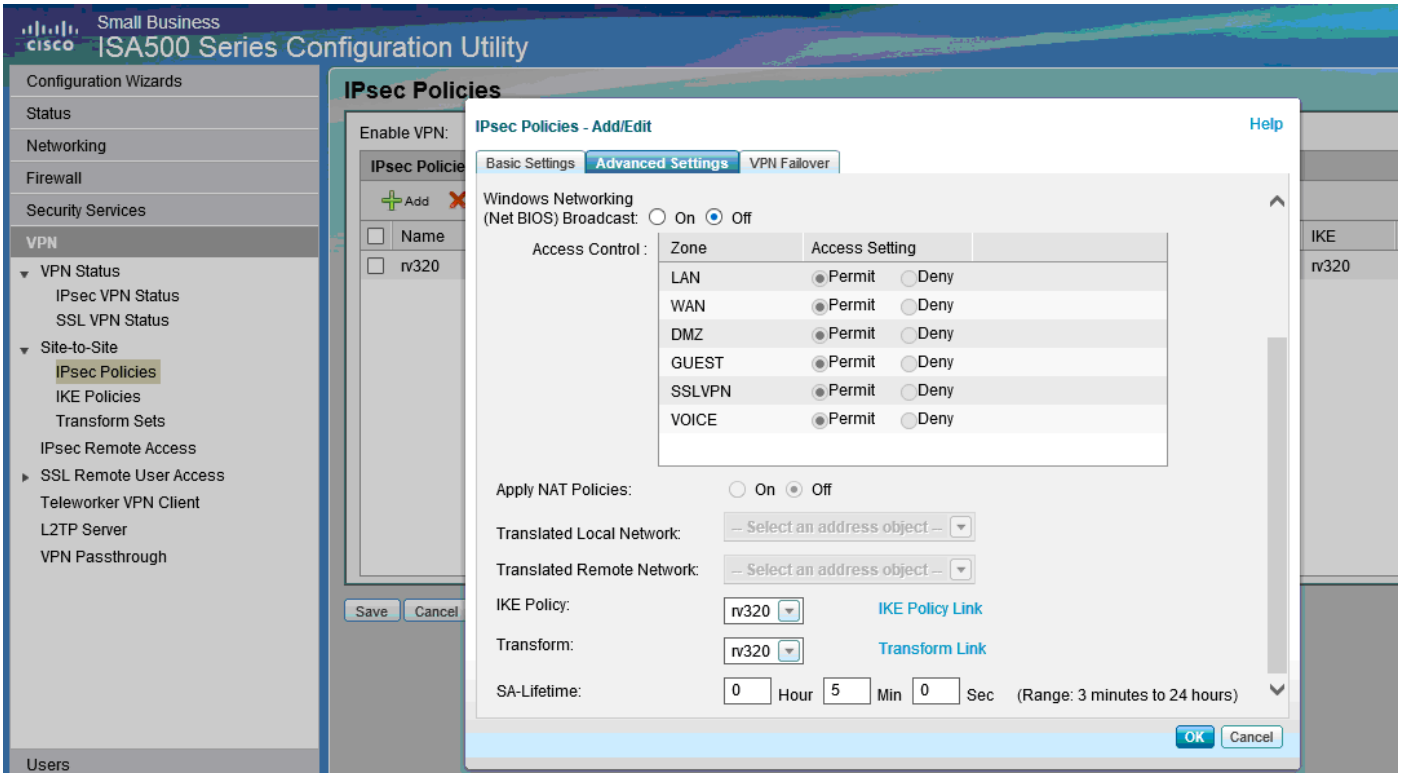
Stap 3. Ga naar **VPN > IPsec-beleid > Add > Basic-instellingen** (zie afbeelding)

a.) Voer een *omschrijving in*, zoals RV320.
b) Stel *IPsec-beleid in* op.
c.) Stel *het afstandstype in op statische IP*.
d.) Voer *afstandsbediening in*.
e.) Stel *de verificatiemethode in* op Vooraf gedeelde toets.
f.) Stel *WAN-interface* in op WAN1.
g.) Stel *Local Network* in op STANDAARD_NETWORK.

h) Stel *Remote Network* in op RV320.
In de volgende afbeelding worden basisinstellingen voor IPsec-beleid weergegeven:



Stap 4. Ga naar **VPN > IPsec-beleid > Add > Advanced Settings** (zie afbeelding)
a.) Stel *IKE-beleid* en *IKE-transformatiesets* in op *de* sets die in stap 1 en 2 zijn gemaakt.
b) Stel *SA-Lifetime* in op 0 uur 5 min 0 seconden.
c.) Klik op **OK**.
Hieronder staan geavanceerde instellingen voor IPsec-beleid:



Stap 5. Sluit de site-to-site IPsec VPN-tunnel (zie afbeelding) aan

a.) Stel *VPN* aan inschakelen in.
b) Klik op **de** knop **Connect**.
De volgende afbeelding toont de knop Connect: