Beveiligde toegang configureren met Sonicwall Firewall

Inhoud

Inleiding

In dit document wordt beschreven hoe u een IPsec VTI-tunnel configureert tussen Secure Access to Sonicwall firewall met statische routering.

Voorwaarden

- Provisioning van gebruiker configureren
- ZTNA SSO-verificatieconfiguratie
- Remote Access VPN Secure Access configureren

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SonicWall-firewall (NSv270 - SonicOSX 7.0.1)

- beveiligde toegang
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless ZTNA

Gebruikte componenten

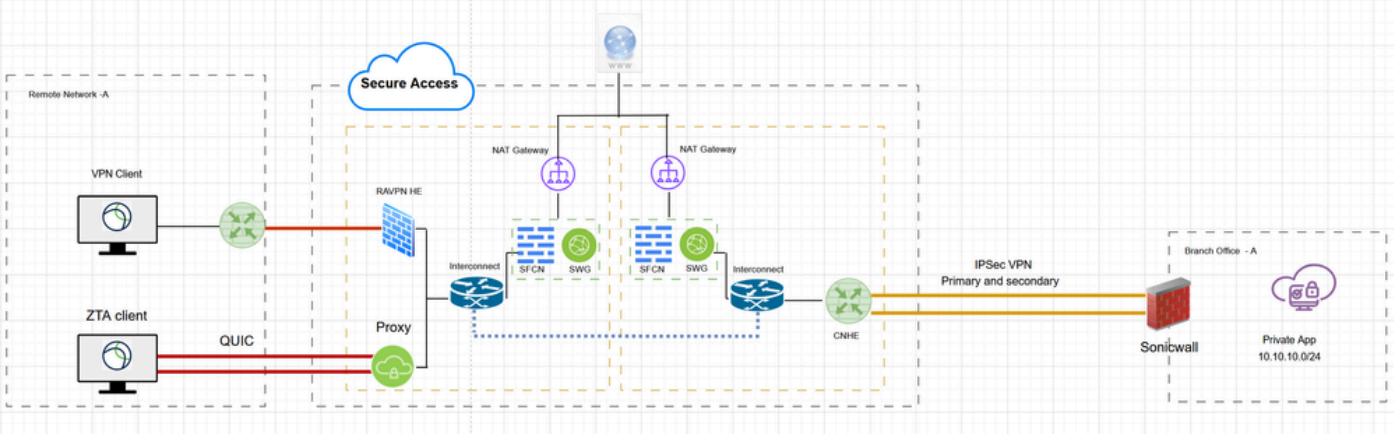
De informatie in dit document is gebaseerd op:

- SonicWall-firewall (NSv270 - SonicOSX 7.0.1)
- beveiligde toegang
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Netwerkdiagram



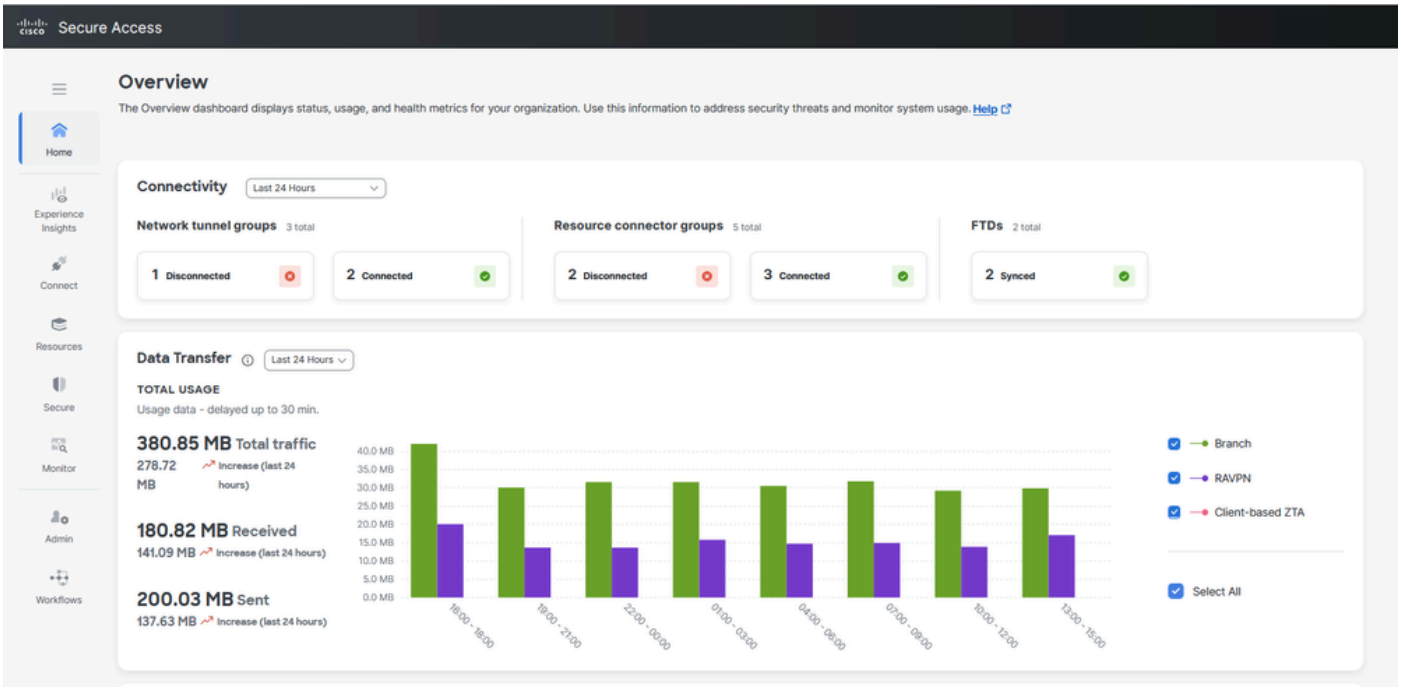
Netwerkdiagram

Configureren

Network Tunnel Group (VPN) configureren voor beveiligde toegang

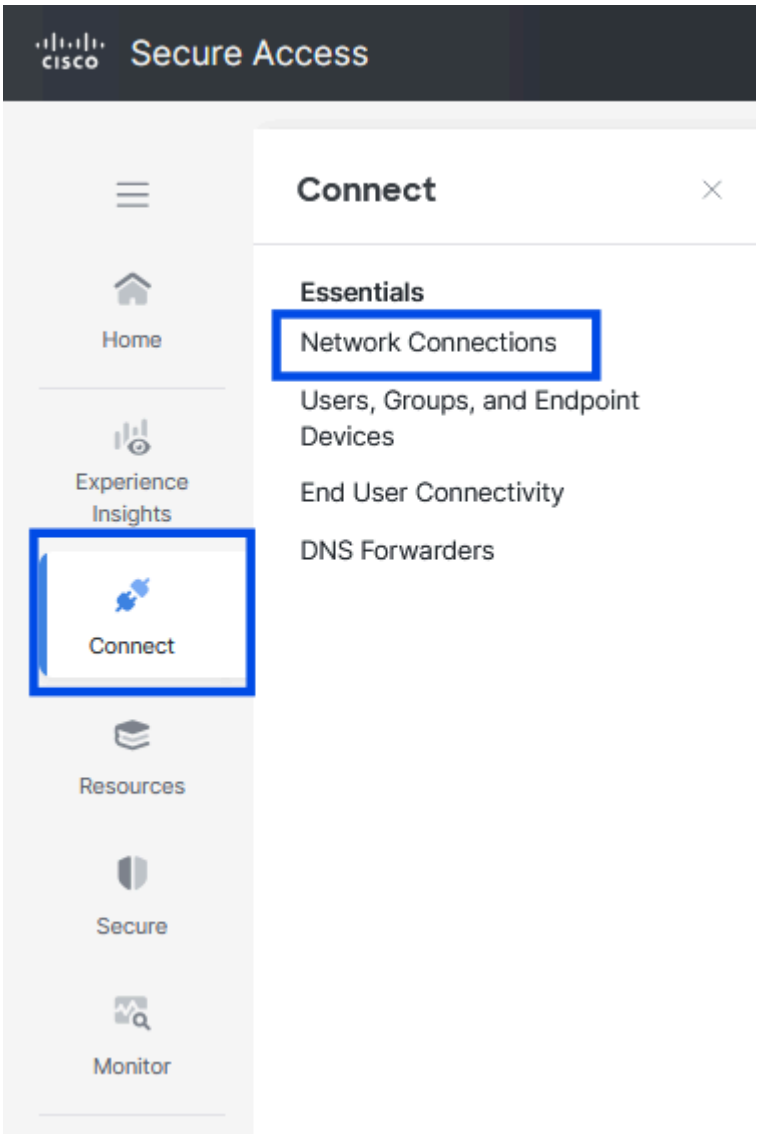
Om VPN-tunnel tussen Secure Access en Sonicwall te configureren

- Navigeer naar het beheerdersportaal van de beveiligde toegang



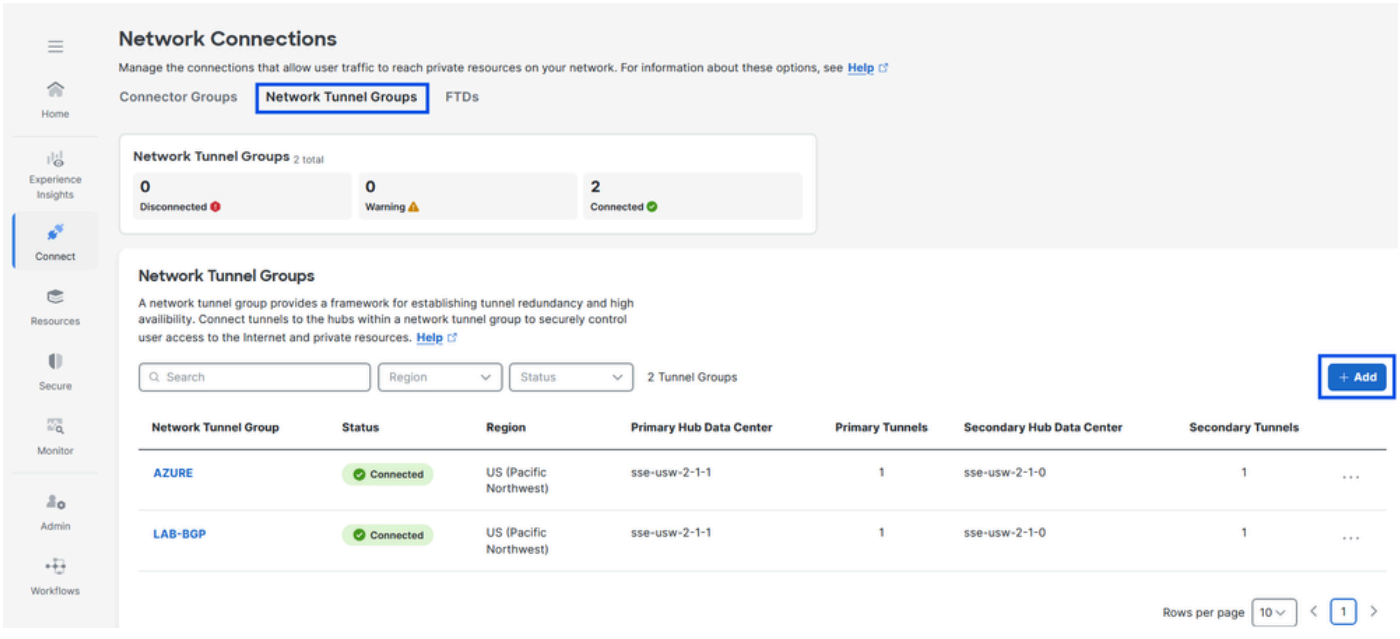
Veilige toegang - Hoofdpagina

- Klik op Verbinden > Netwerkverbindingen



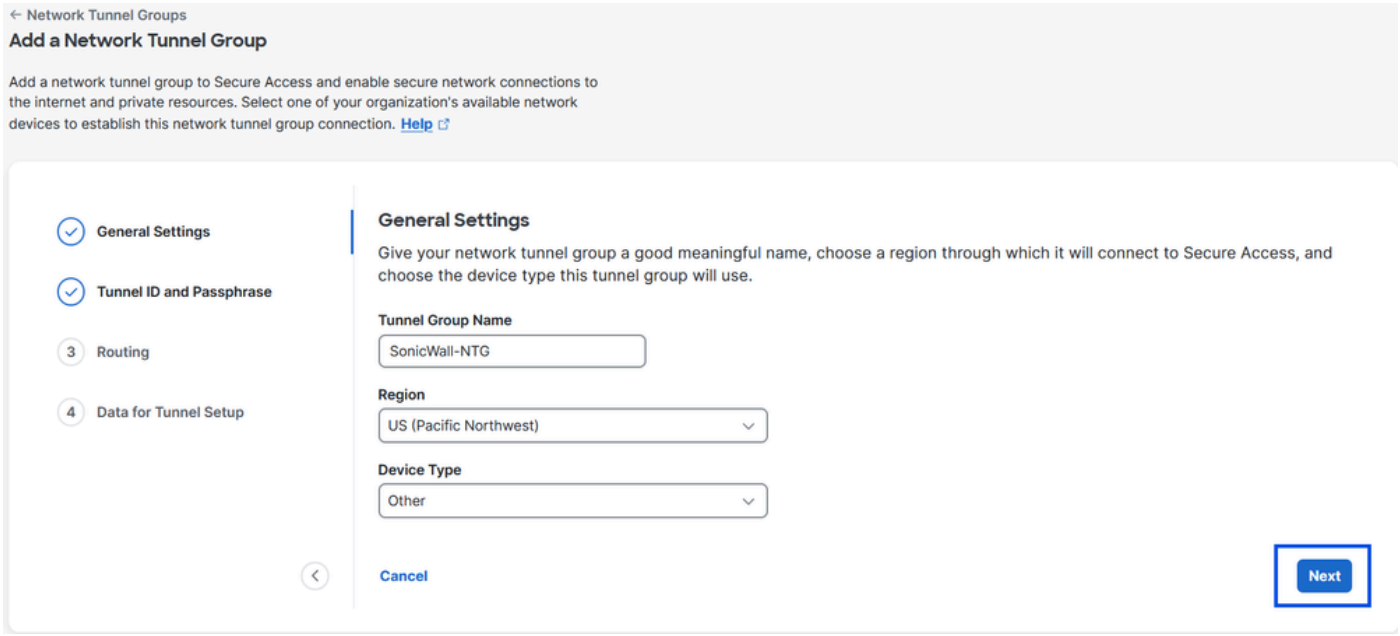
Veilige toegang - netwerkverbindingen

- Klik onder Netwerktunnelgroepen op + Toevoegen



Veilige toegang - Netwerktunnelgroepen

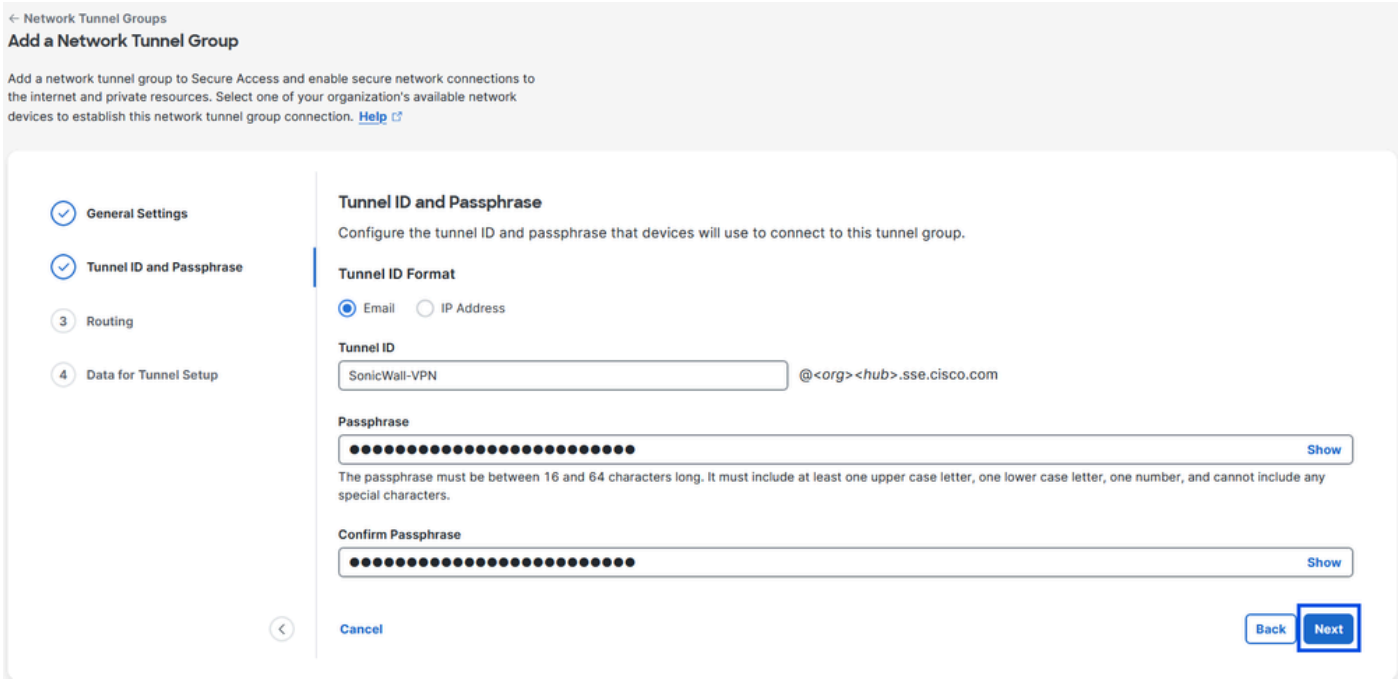
- Naam, regio en apparaattype van tunnelgroep configureren
- Klik op Volgende



Veilige toegang - Netwerktunnelgroep - Algemene instellingen

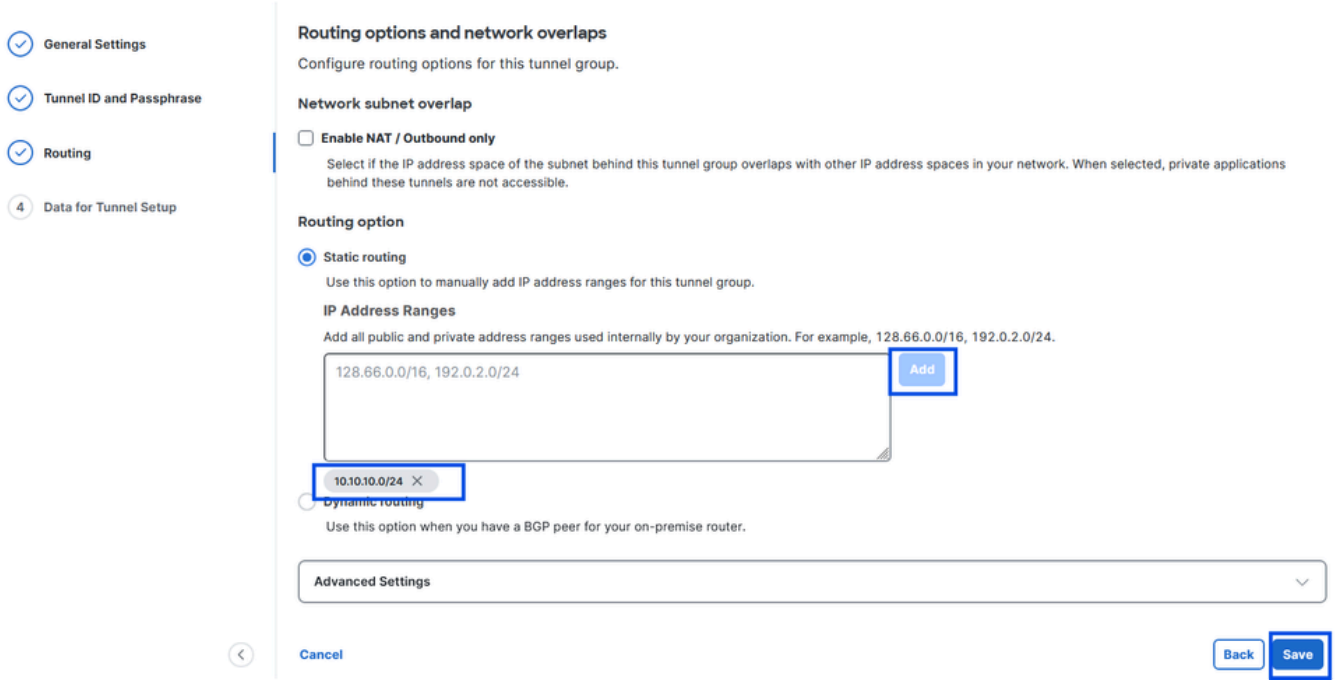
Opmerking: Kies de regio die het dichtst bij de locatie van uw firewall ligt.

- Het Tunnel ID-formaat en de wachtwoordgroep configureren
- Klik op Volgende



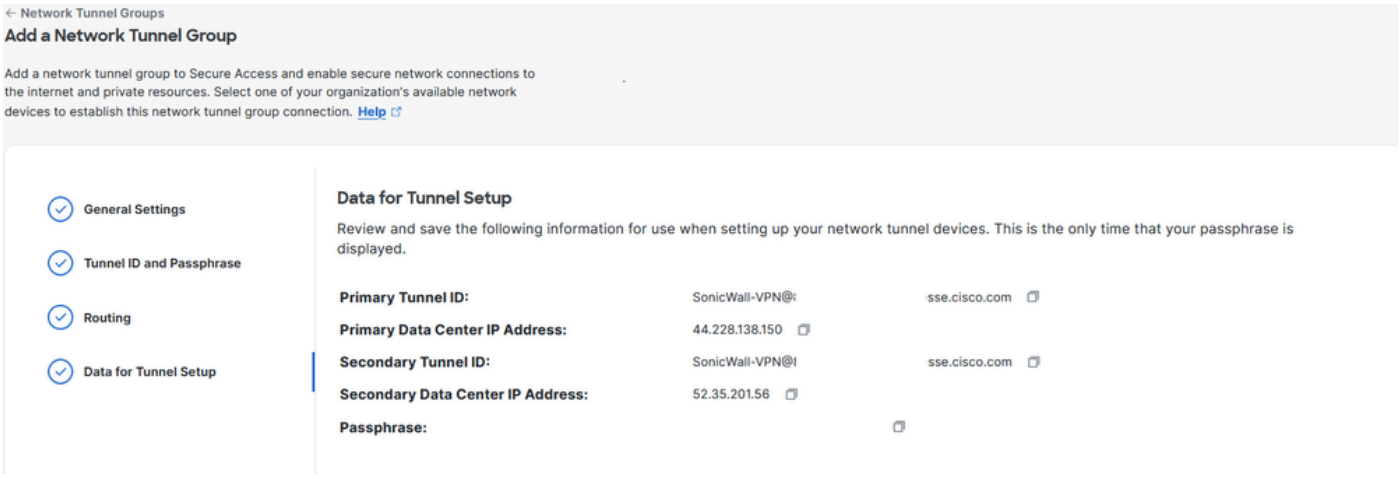
Veilige toegang - Tunnel-ID en wachtwoordgroep

- Configureer de IP-adresbereiken, hosts of subnetten die u in uw netwerk hebt geconfigureerd en die het verkeer via Secure Access willen doorgeven
- Klik op Toevoegen
- Klik op Opslaan



Veilige toegang - tunnelgroepen - routeringsopties

Nadat u op Opslaan hebt geklikt, wordt de informatie over de tunnel weergegeven. Bewaar deze informatie voor de volgende configuratiestap



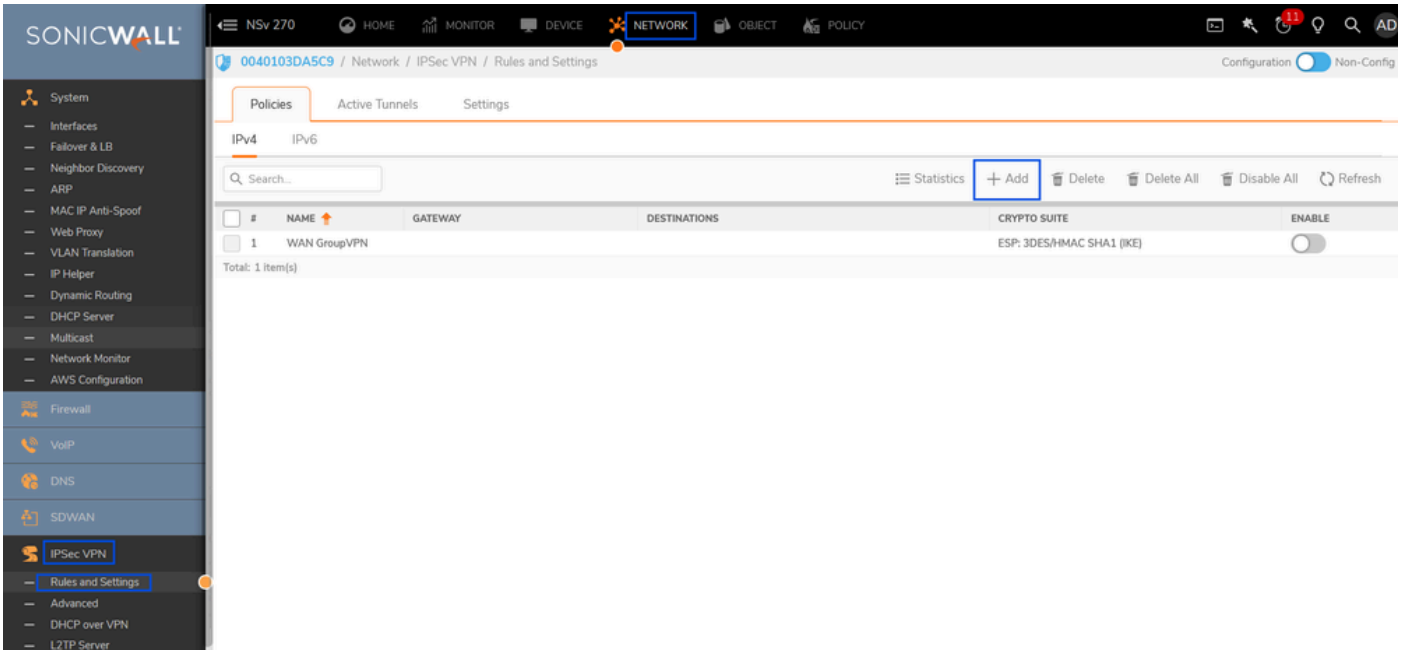
Veilige toegang - Gegevens voor tunnelinstallatie

Configureer de tunnel op Sonicwall

De tunnel configureren - Regels en instellingen

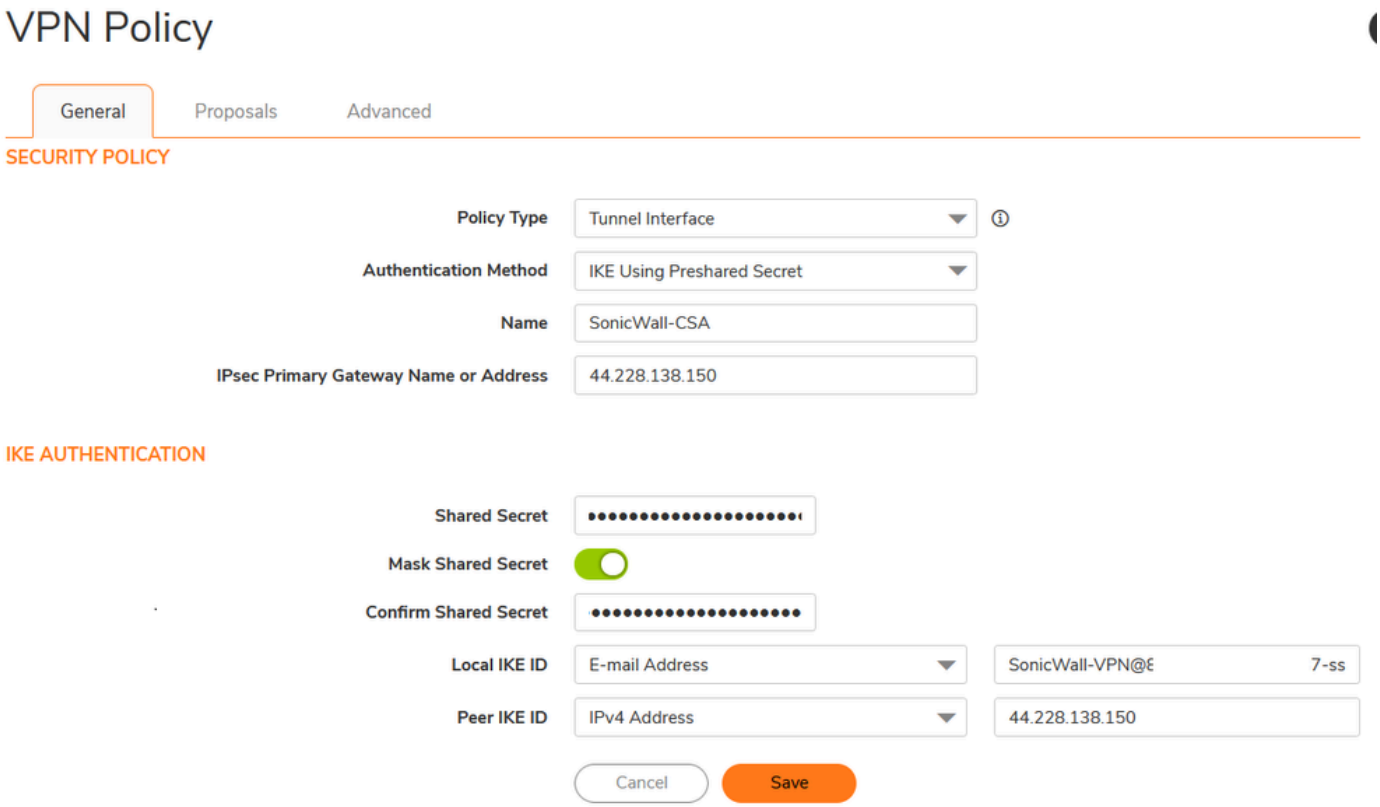
Navigeer naar het Sonicwall Dashboard.

- Netwerk > IPsec VPN > Regels en instellingen
- Klik op + Toevoegen



Sonicwall - IPSec VPN - Regels en instellingen

- Onder VPN-beleid vult u de VPN-configuratie in op basis van de tunnelgegevens van Secure Access en [ondersteunde ipsec-parameters]



VPN Policy

General | Proposals | Advanced

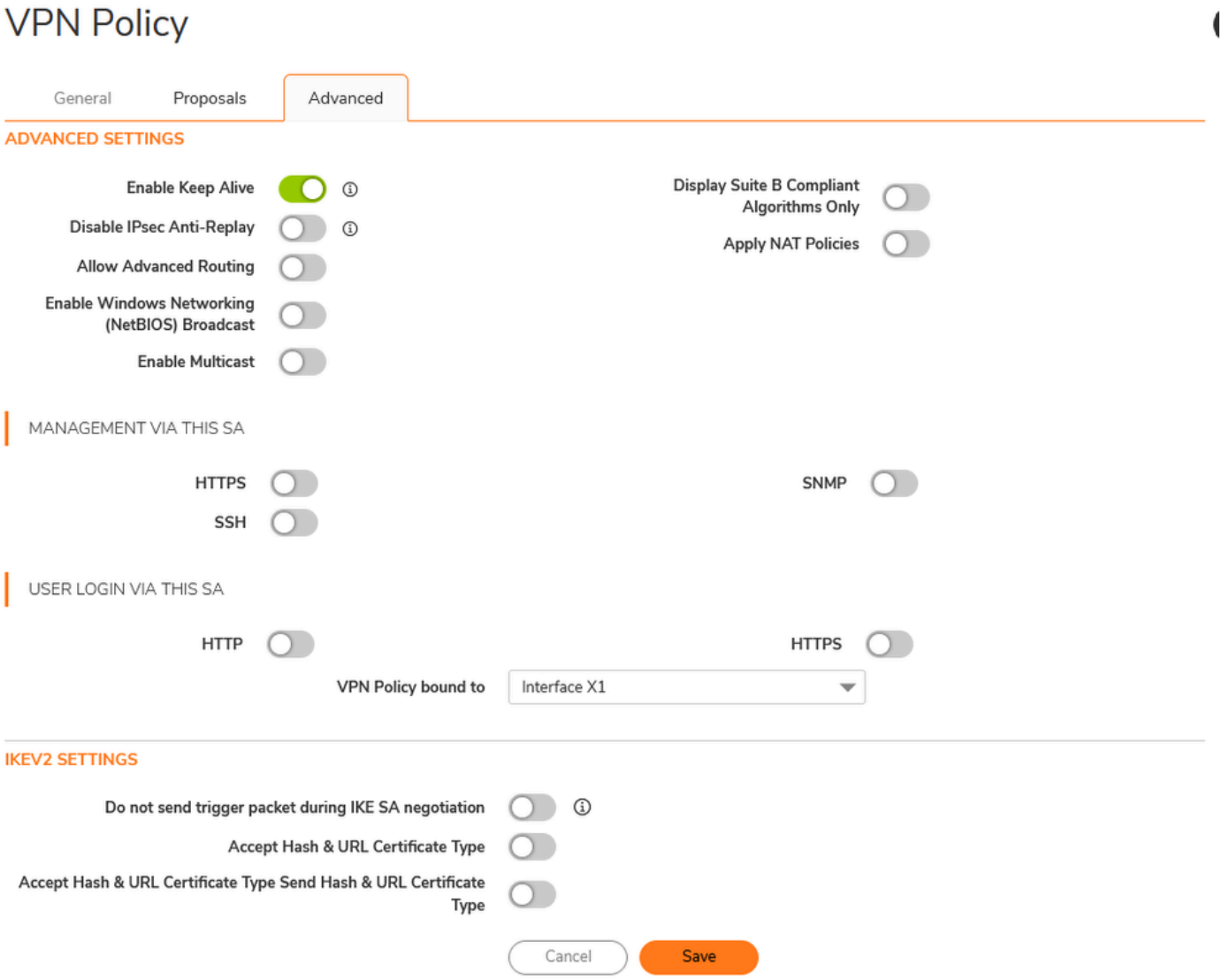
IKE (PHASE 1) PROPOSAL

Exchange	IKEv2 Mode
DH Group	Group 14
Encryption	AES-256
Authentication	SHA256
Life Time (seconds)	28800

IPSEC (PHASE 2) PROPOSAL

Protocol	ESP
Encryption	AESGCM16-256
Authentication	None
Enable Perfect Forward Secrecy	
DH Group	Group 14
Life Time (seconds)	28800

Cancel Save

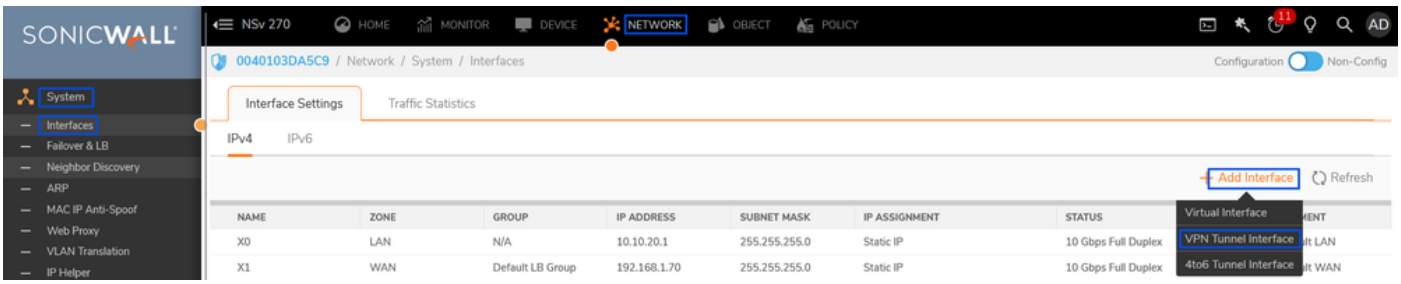


- Klik op Opslaan

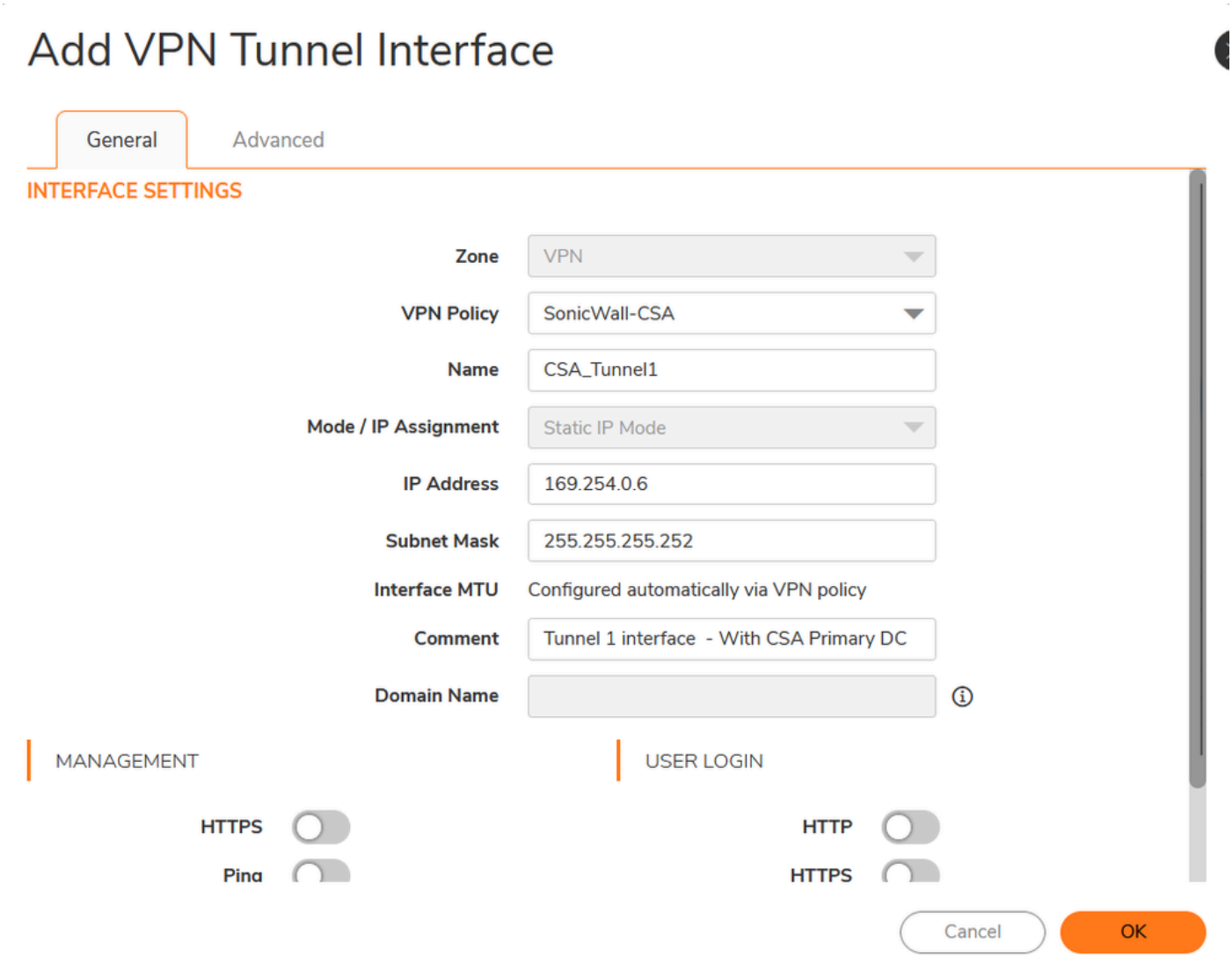
VPN-tunnelinterface toevoegen

Navigeer naar het Sonicwall Dashboard.

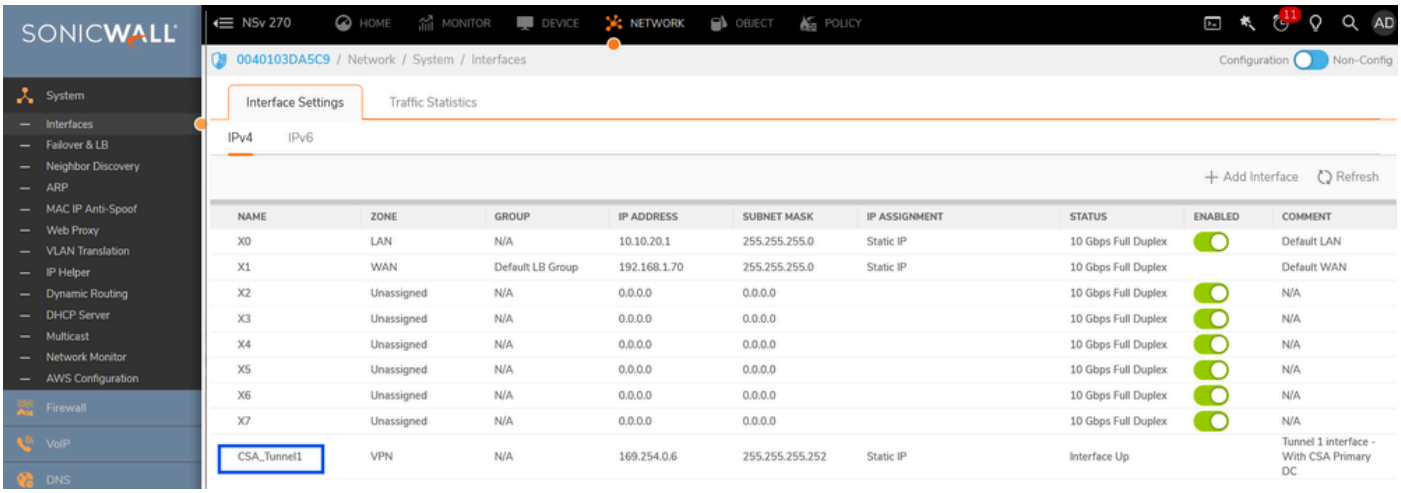
- Netwerk > Systeem > Interface
- Klik op + Add Interface
- Selecteer VPN-tunnelinterface



Sonicwall - Interfaces



- Klik op OK

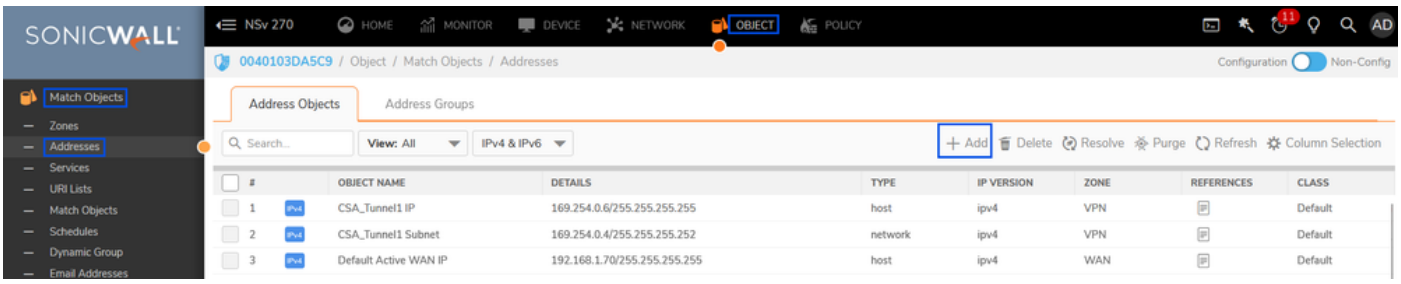


Sonicwall - Interfaces - VPN Tunnel Interface

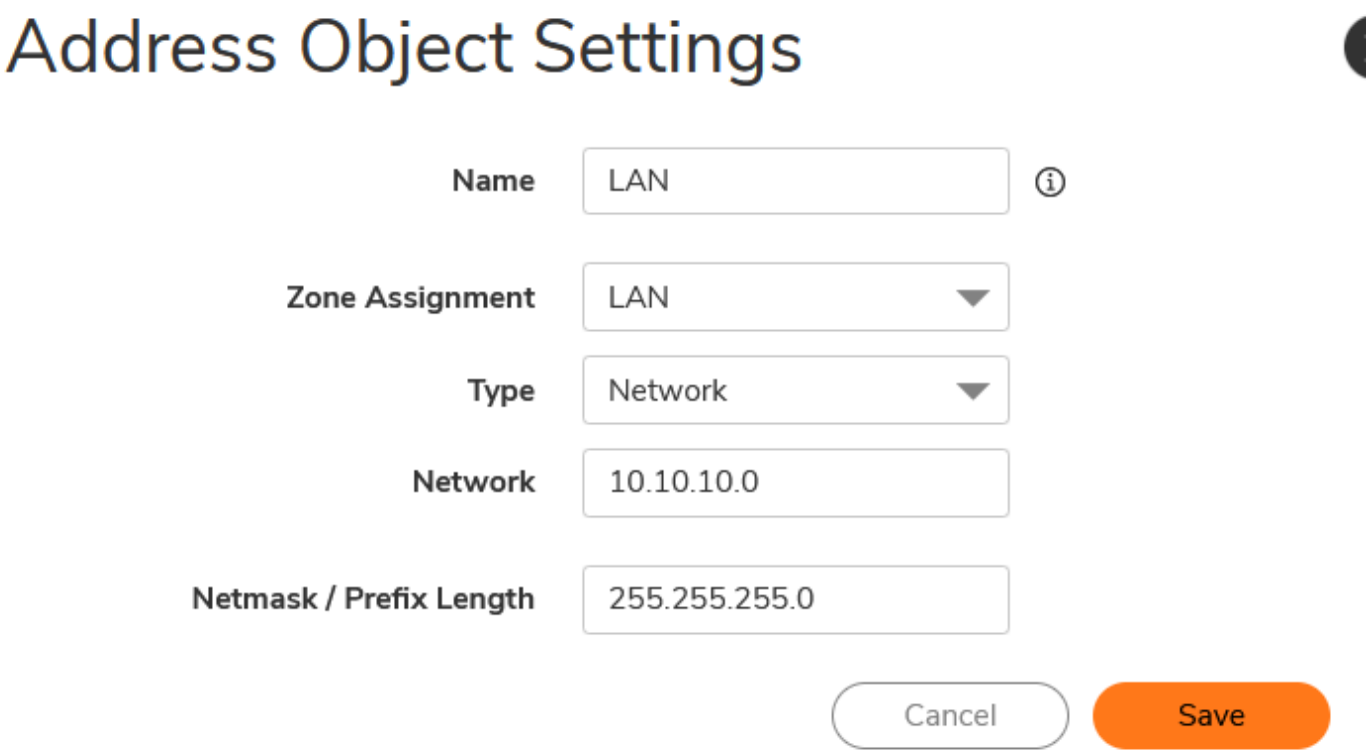
Netwerkobject en groepen toevoegen

Navigeer naar het Sonicwall Dashboard.

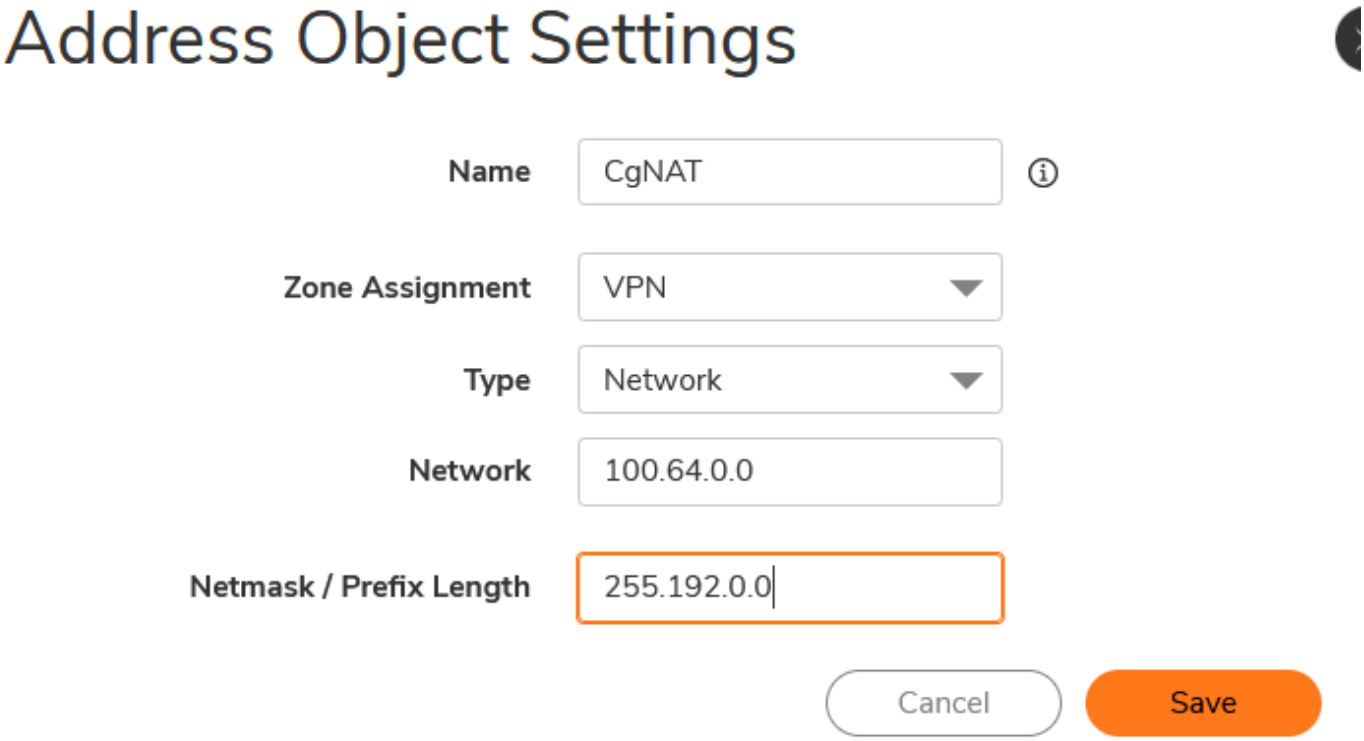
- Object > Overeenkomende objecten >Adressen
- Adresobjecten
- Klik op +Add



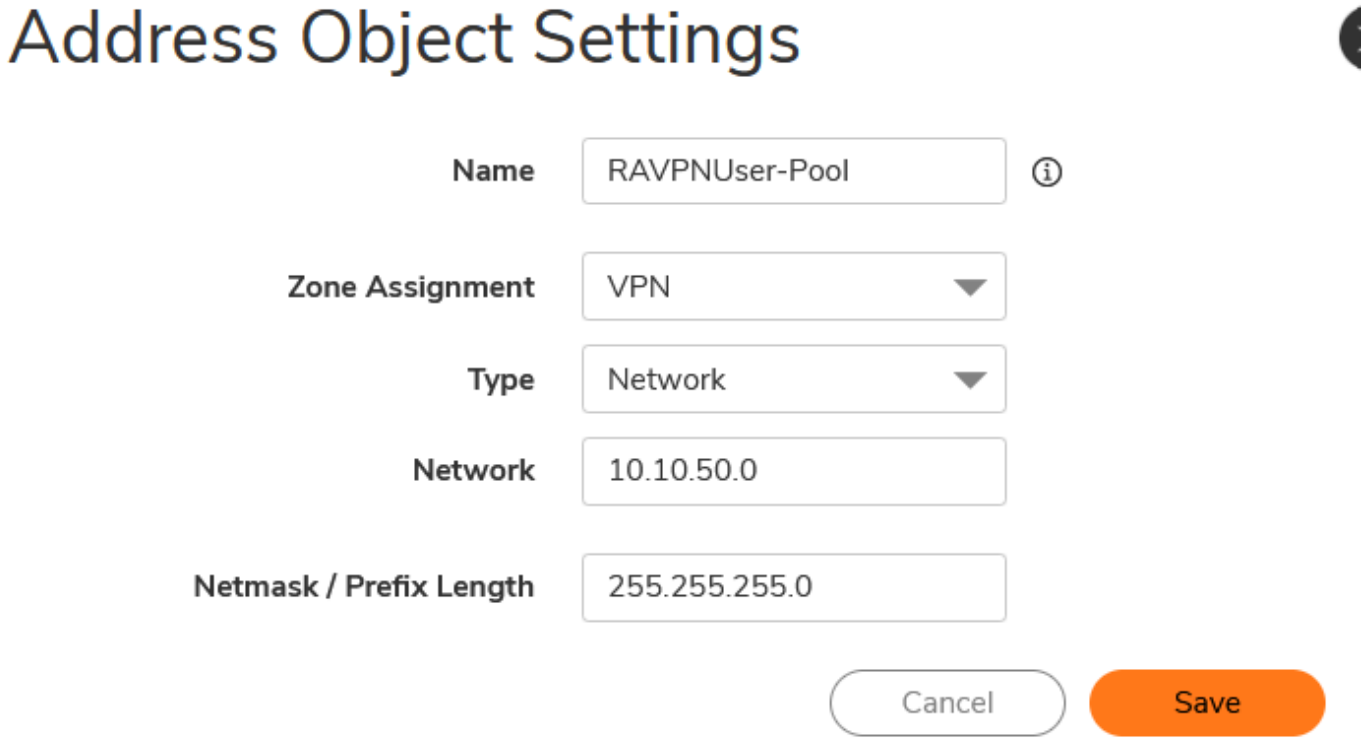
SonicWall - Object- Adresobjecten



- Klik op Opslaan

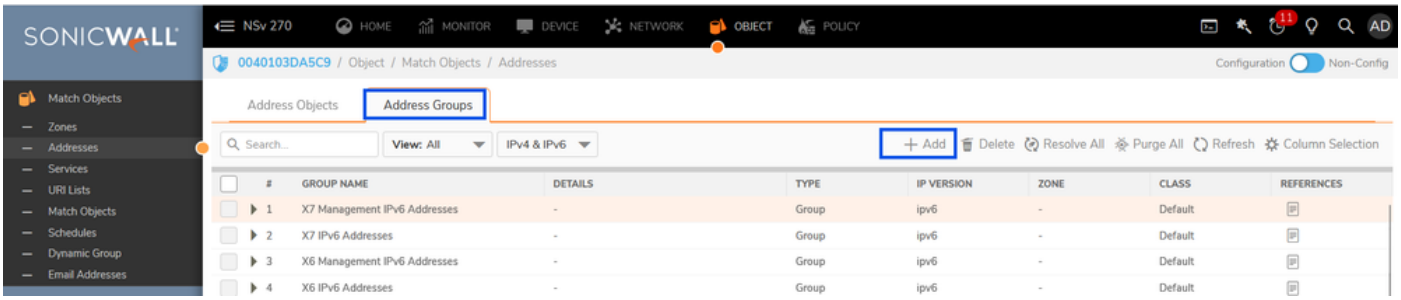


- Klik op Opslaan

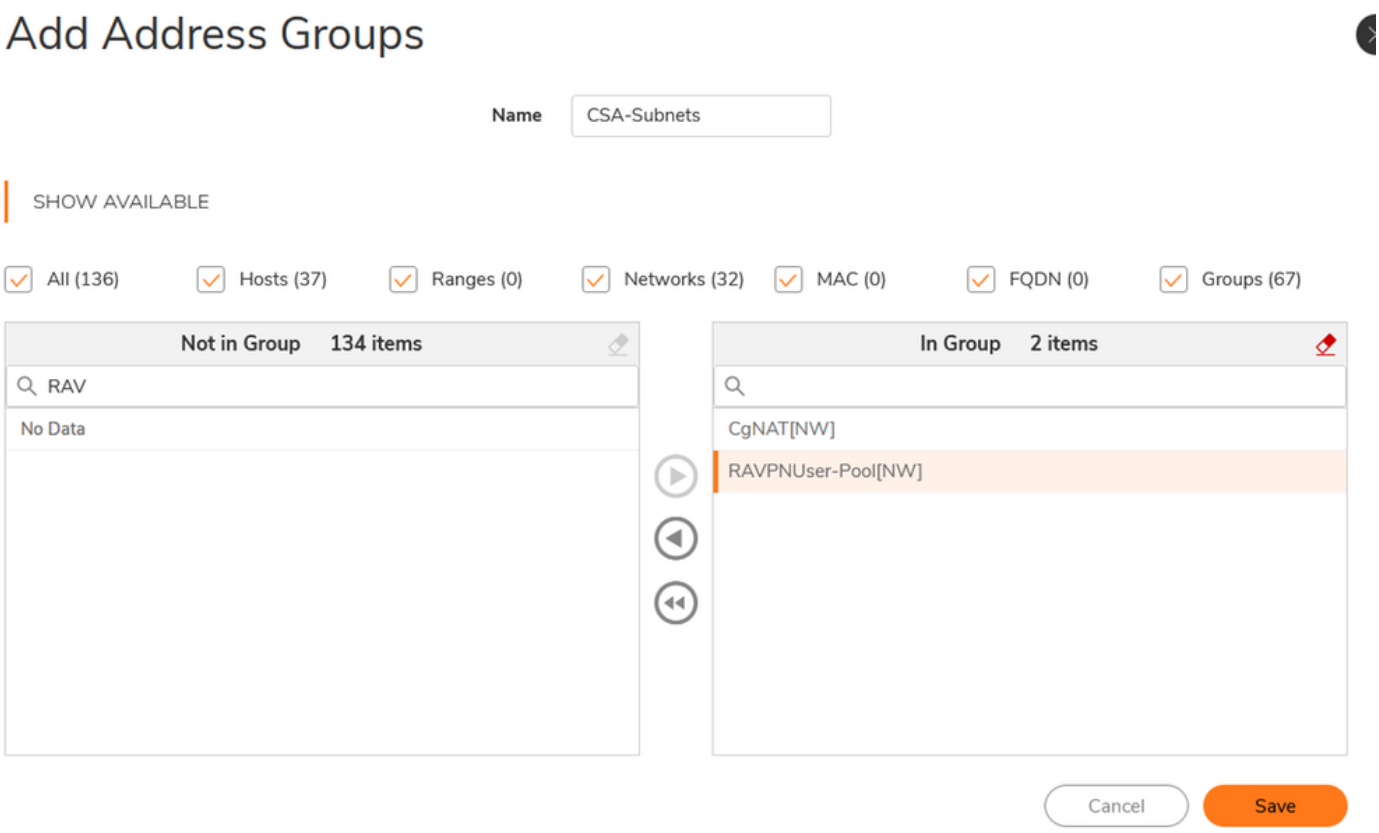


- Klik op Opslaan

- Adresgroepen maken
- Klik op +Toevoegen
- Selecteer het Adresobject en voeg ze toe aan Adresgroepen



SonicWall - Object- Adresgroepen

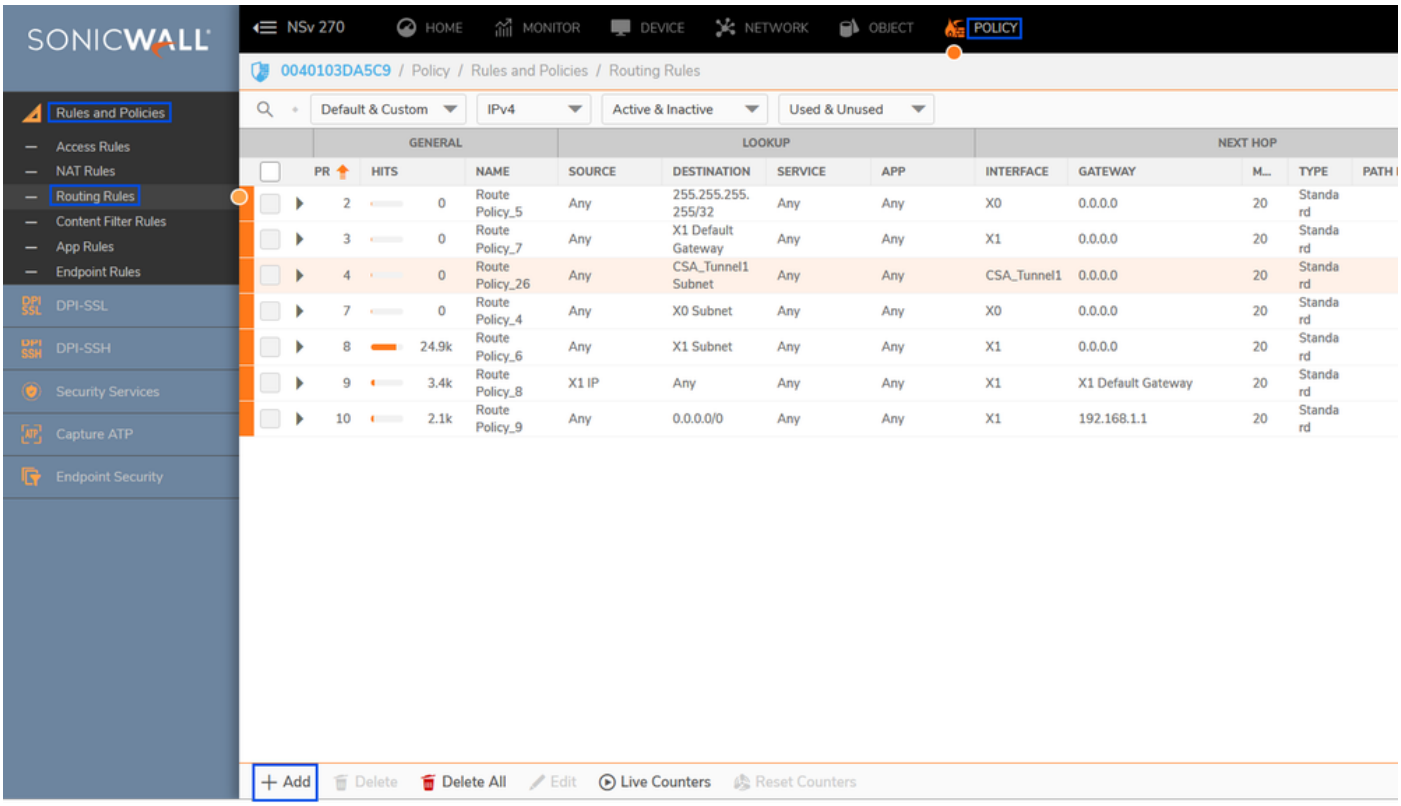


- Klik op Opslaan

Route toevoegen

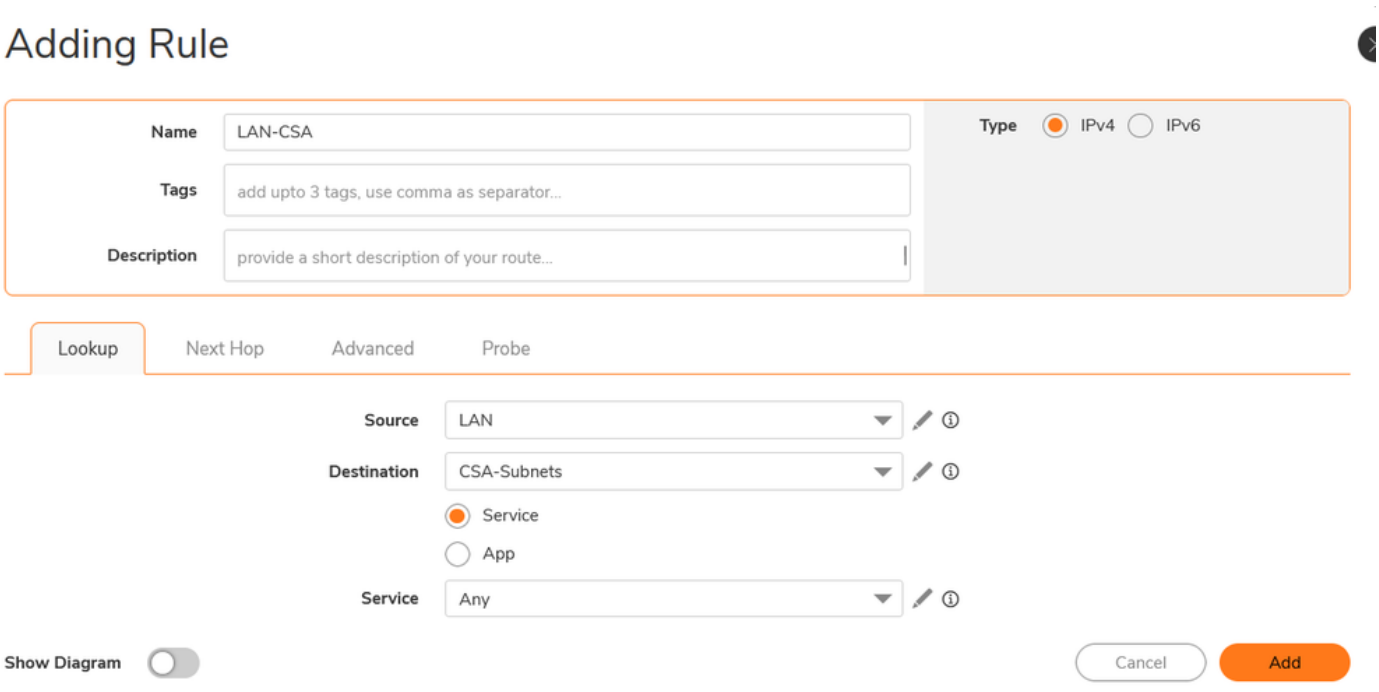
Navigeer naar het Sonicwall Dashboard.

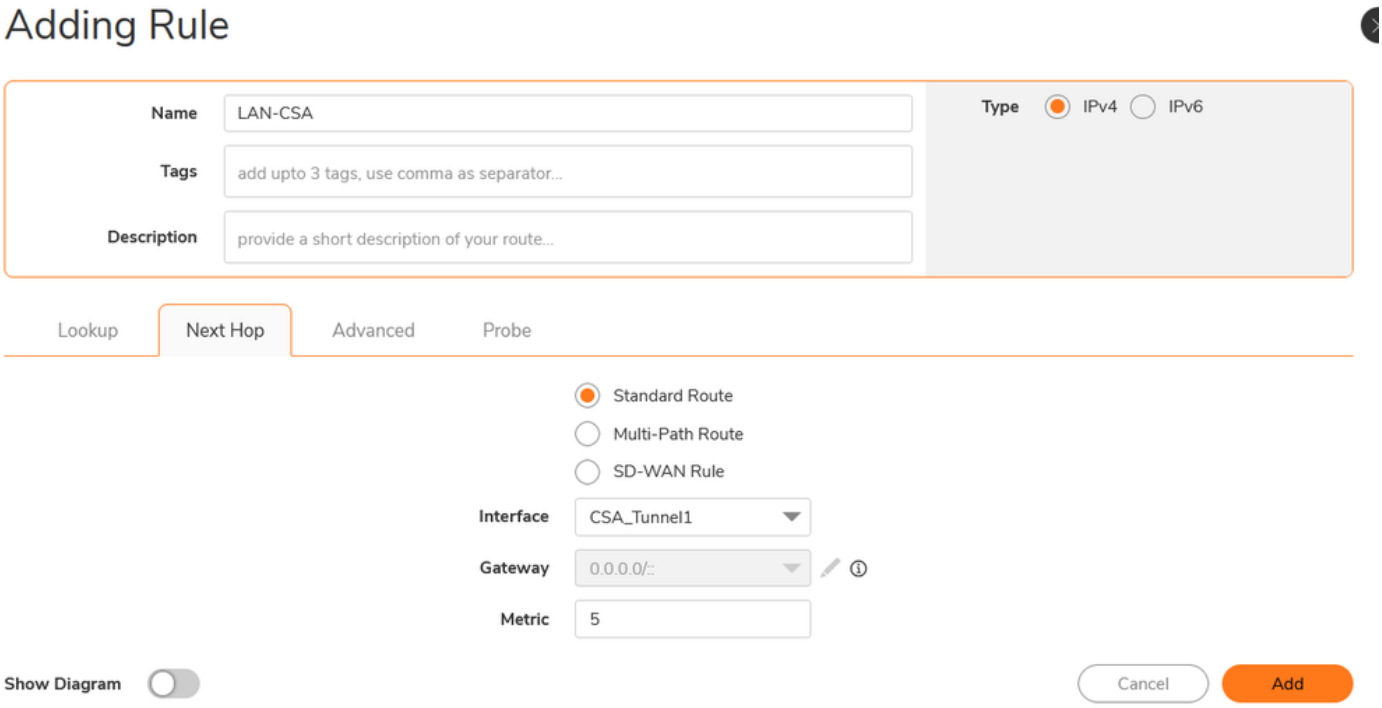
- Beleid > Regels en beleid > Routeringsregels
- Klik op + Toevoegen



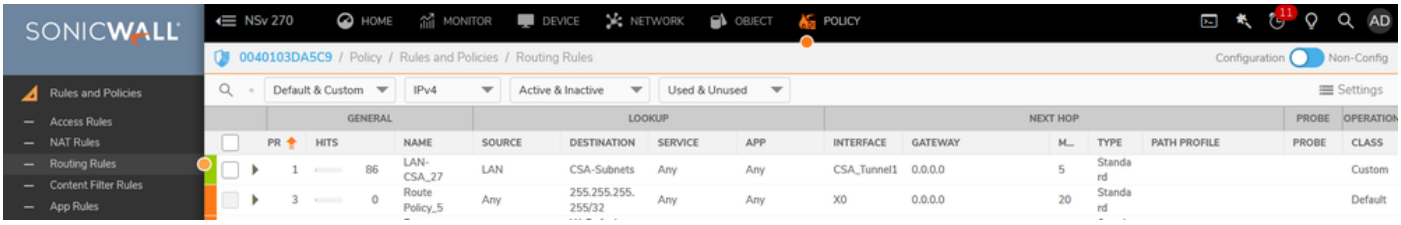
Sonicwall - Routeringsregels

- Routeringsregel toevoegen





- Klik op + Toevoegen

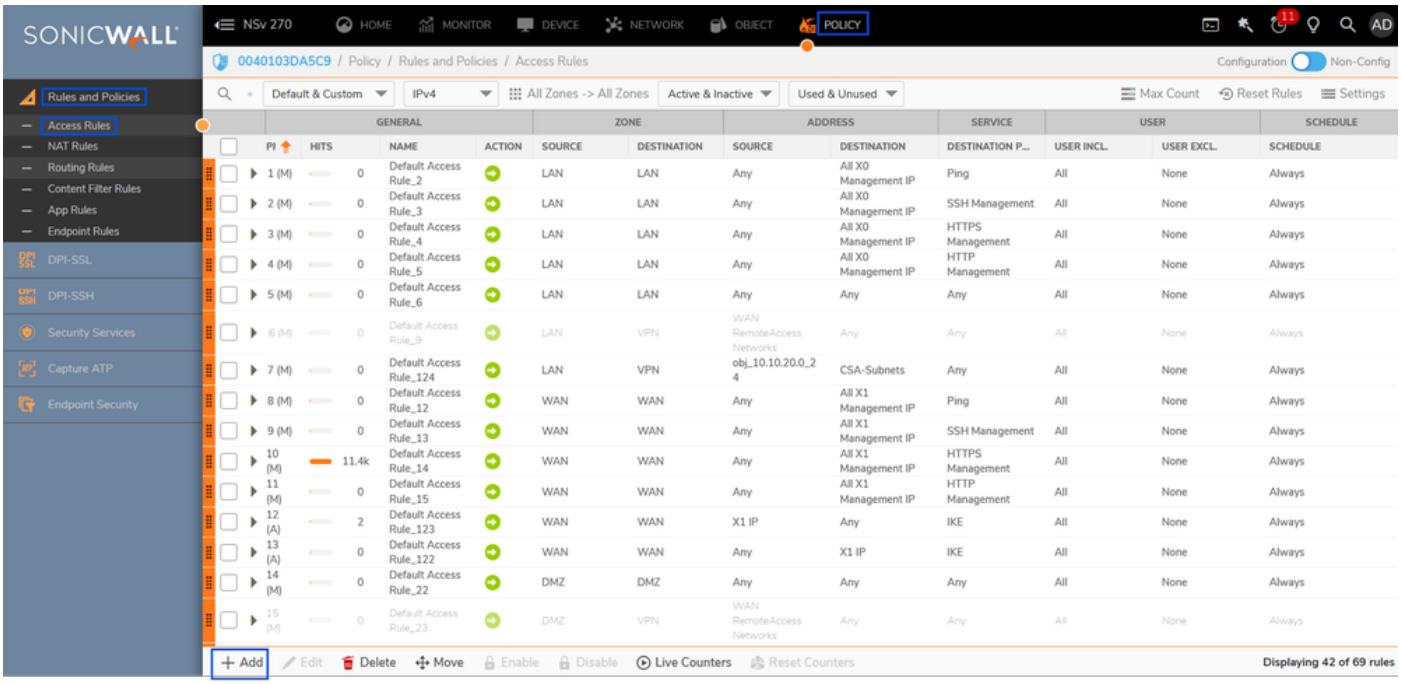


Sonicwall - Routeringsregels

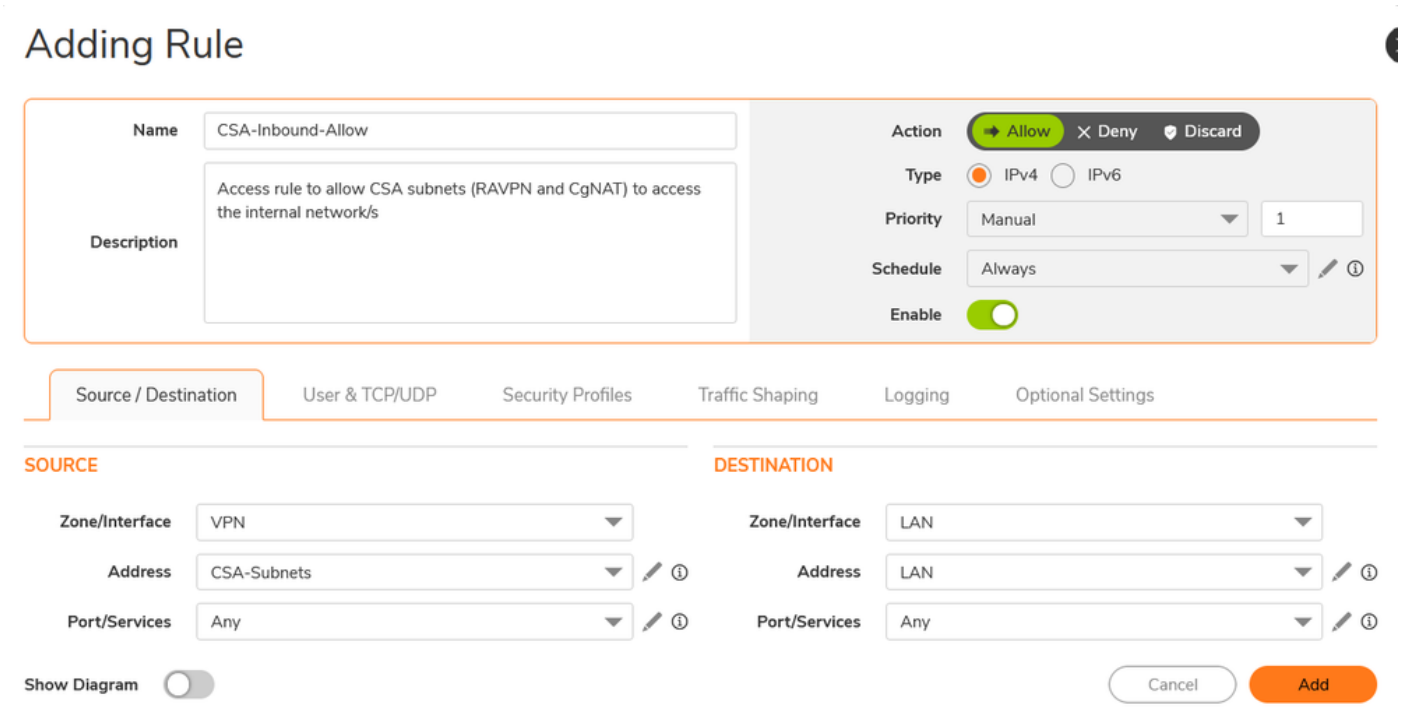
Toegangsregels toevoegen

Navigeer naar het Sonicwall Dashboard.

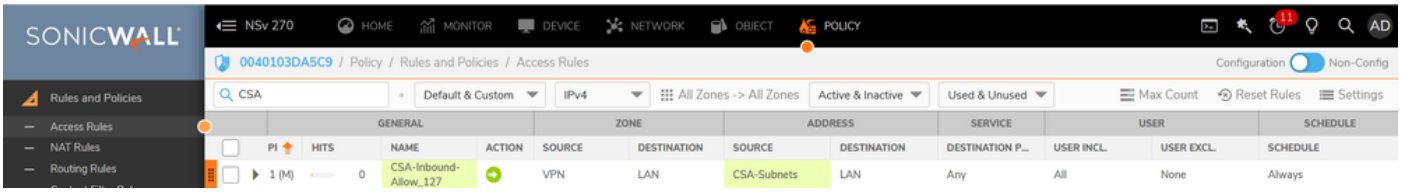
- Beleid > Regels en beleid > Toegangsregels
- Klik op + Toevoegen



Sonicwall - Toegangsregels



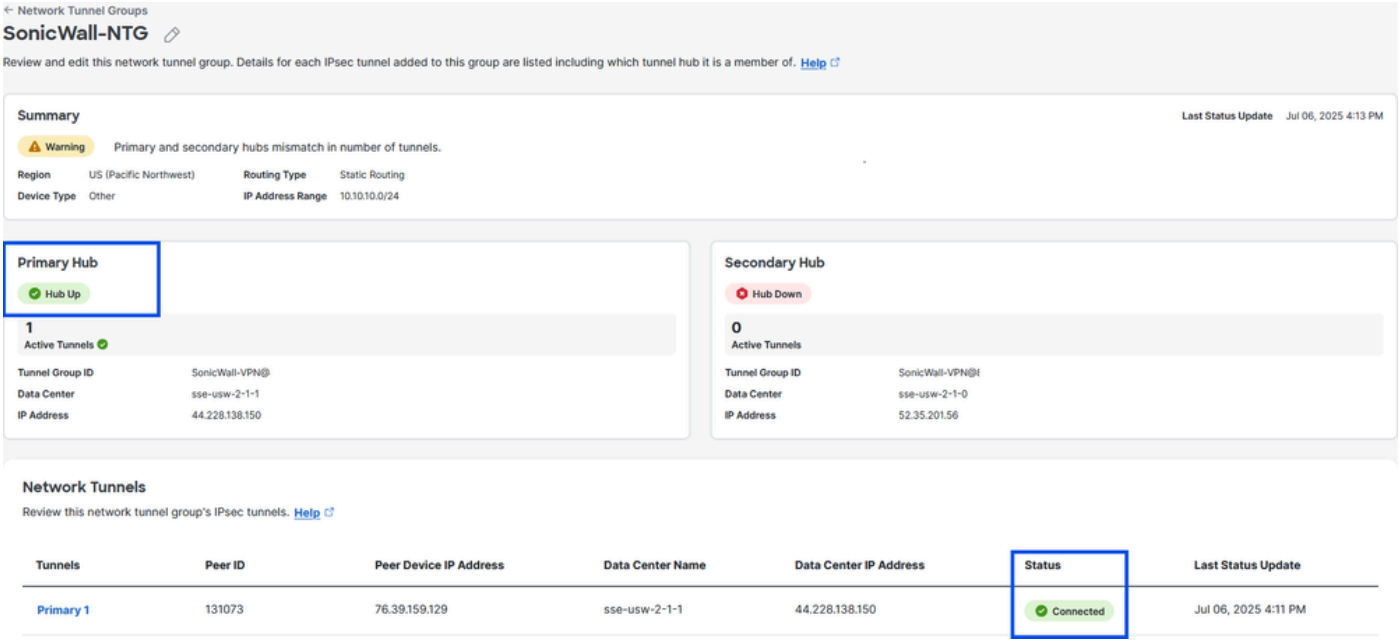
- Klik op +Toevoegen



Sonicwall - Toegangsregels

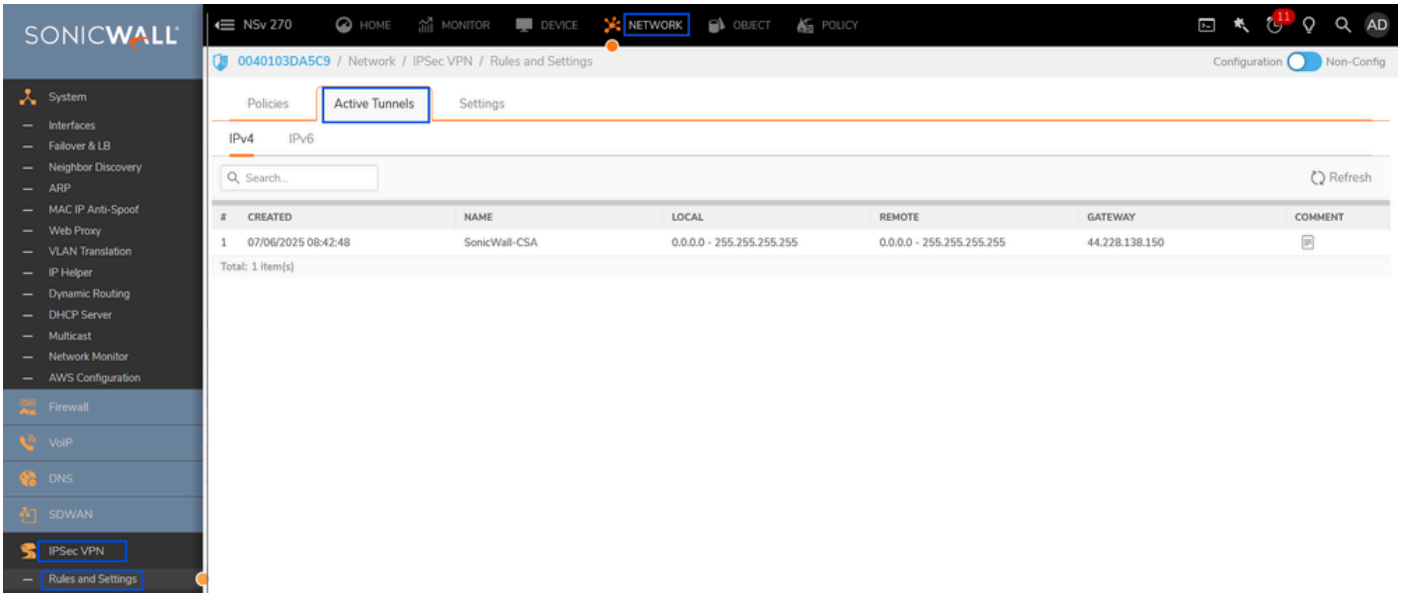
Verifiëren

- Tunnel status bij beveiligde toegang



Veilige toegang - Network Tunnel Group - VPN-status

- Tunnelstatus op SonicWall-firewall



Sonicwall - IPSec VPN-status

U kunt hetzelfde proces uitvoeren om de tunnel tussen het Secundaire datacenter met beveiligde toegang en de Sonicwall te configureren

Nu, de tunnel is UP op Secure Access en Sonicwall, kunt u doorgaan met het configureren van de toegang tot de particuliere bronnen via RA-VPN, browser-gebaseerde ZTA of client-gebaseerde ZTA op Secure Access Dashboard

Problemen oplossen

Gebruiker-pc

- Controleer of de gebruiker al dan niet succesvol verbinding kan maken met RAVPN/ZTNA. Als dat niet het geval is, kunt u het probleem verder oplossen waarom de verbinding van het besturingsvliegtuig niet werkt.
- Controleer of het netwerk waartoe de gebruiker toegang probeert te krijgen, via de RAVPN-tunnel of ZTNA moet gaan. Zo niet, controleer de configuratie op de kop.

beveiligde toegang

- Controleer de configuratie van de verkeersbesturing in het RAVPN-verbindingsprofiel om te bevestigen dat het bestemmingsnetwerk is geconfigureerd om via de tunnel naar Secure Access te verzenden.
- Controleer of Private Resource is gedefinieerd met geldige protocol/poorten en de verbindingsmechanismen van ZTNA/RAVPN zijn gecontroleerd.
- Verify Access-beleid is geconfigureerd om de RAVPN / ZTNA-gebruiker toegang te geven tot Private Resource Network en zijn geplaatst in een bestelling die geen andere regel heeft voorrang om het verkeer te blokkeren.
- Controleer of de IPSec-tunnel UP en Secure Access is en of geldige clientroutes worden weergegeven via statische routering die betrekking heeft op de privébronnen waartoe de gebruiker toegang probeert te krijgen.

Sonicwall

- Controleer of de IPSec-tunnel UP is of niet (IKE & IPSec SA).
- Controleer of de clientroute of -routes correct zijn geadverteerd.
- Controleer verkeersbronnen van RAVPN / ZTNA-gebruiker die bestemd is voor privébronnen achter Sonicwall bereikt de Sonicwall-firewall door de tunnel door pakketopnames op Sonicwall te maken.
- Controleer of het verkeer een privébron heeft bereikt en reageer op de RAVPN/ZTNA-client of niet. Zo ja, controleer of die pakketten de Sonicall X0 (LAN)-interface bereiken.
- Controleer of Sonicwall het retourverkeer via de IPSec-tunnel doorstuurt naar Secure Access.

Gerelateerde informatie

- Cisco Technical Support en downloads
- Cisco Secure Access Help Center
- Zero Trust Access Module
- Problemen oplossen bij fout bij beveiligde toegang "Inschrijvingsservice reageert niet. Neem contact op met uw IT-helpdesk"

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.