DrayTek

IKEv2 Site-to-Site

DrayTek naar Fortigate

Inhoudsopgave

IKEv2
Deze handleiding beschrijft stap voor stap hoe een IKEv2 IPsec Site-to-Site VPN-tunnel wordt opgezet tussen een FortiGate firewall en een DrayTek Vigor Router. Na voltooiing kunnen apparaten op beide lokale netwerken veilig met elkaar communiceren via een versleutelde verbinding over internet.

Voor deze handleiding is gebruikgemaakt van een DrayTek Vigor2928. De Vigor2928 maakt gebruik van DrayOS5.

Voorwaarden:
- Een werkende internetverbinding op beide locaties.
- Beheerrechten op zowel de DrayTek als de Fortigate.
- Bekende LAN-subnetten van beide locaties.
- Een vooraf afgesproken Pre-Shared Key (PSK).
- Openbaar IP-adres of FQDN van de FortiGate.
- FortiOS 7.0 of nieuwer.

Netwerkvoorbeeld:
Locatie A (FortiGate)
LAN: 192.168.1.0/24

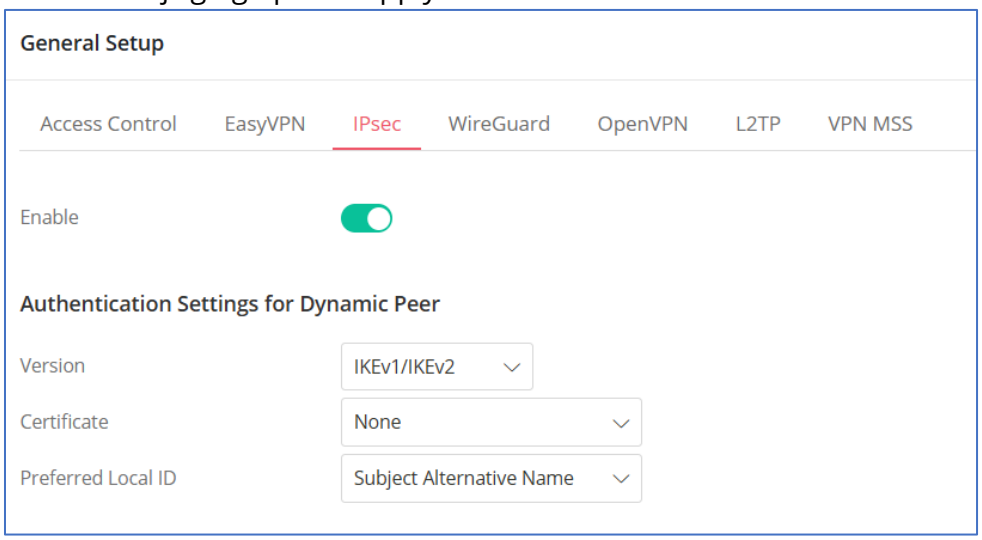
Locatie B (DrayTek Vigor)
LAN: 192.168.10.0/24

Deze waarden zijn voorbeelden en moeten worden vervangen door de daadwerkelijke netwerken.

Configuratie DrayTek

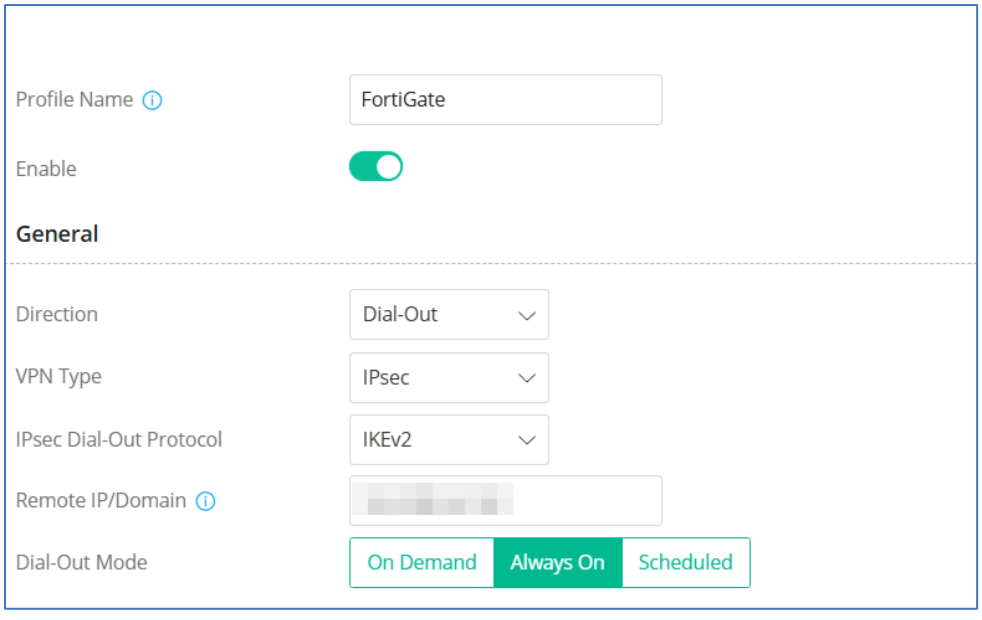
IPsec service inschakelen

Ga naar VPN and Remote Access > General Setup > IPsec. Activeer de optie IPsec Service en sla de wijziging op met Apply.



VPN profiel aanmaken.

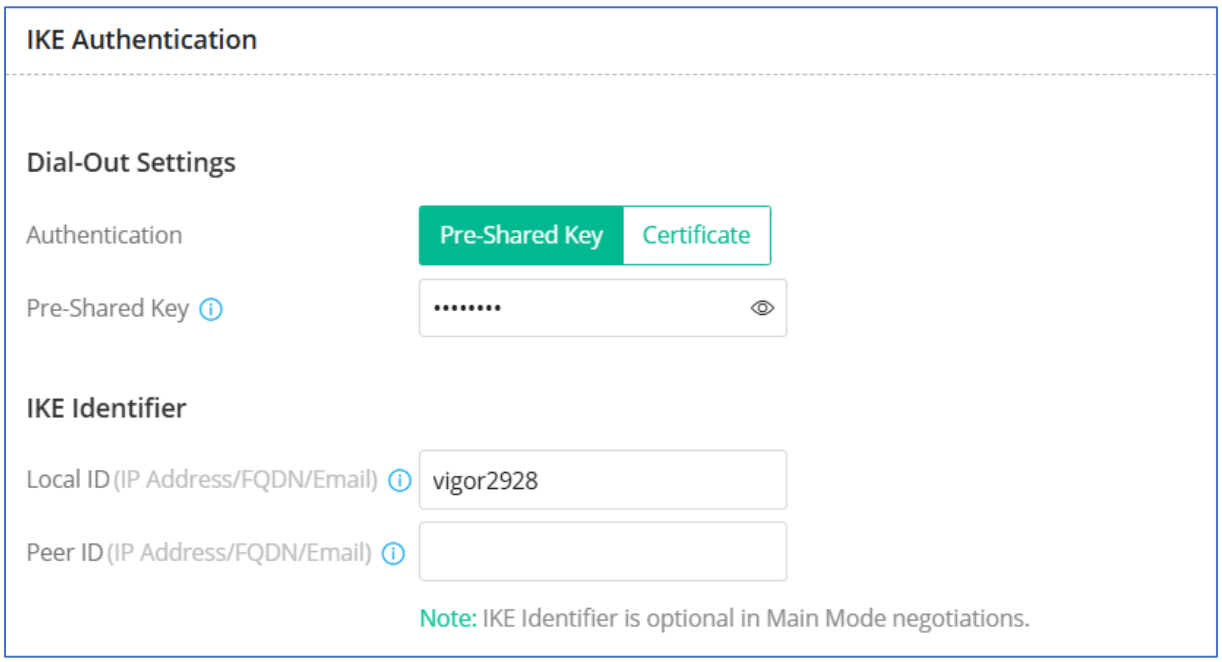
Open VPN / Site-to-Site VPN en kies Add. Geef het profiel een duidelijke naam en schakel het profiel in.



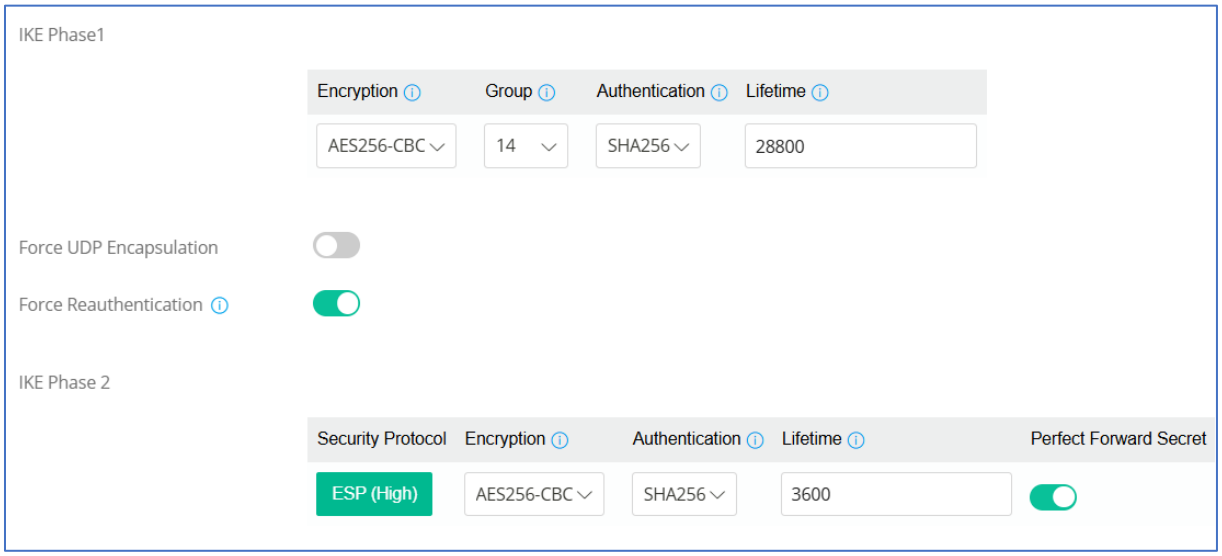
Algemene instellingen

Direction: Dial-Out
VPN Type: IPsec Tunnel
IPsec Dial-Out Protocol: IKEv2
Server IP/Host Name: Publiek IP-adres of FQDN van de FortiGate
Dial-Out Mode: Always On

IKE-Authenticatie
Selecteer Pre-Shared Key als authenticatiemethode en voer dezelfde sleutel in als op de FortiGate. Vul vervolgens de IKEv2 Local ID in. Deze waarde moet exact overeenkomen met de Peer ID die op de FortiGate is geconfigureerd.

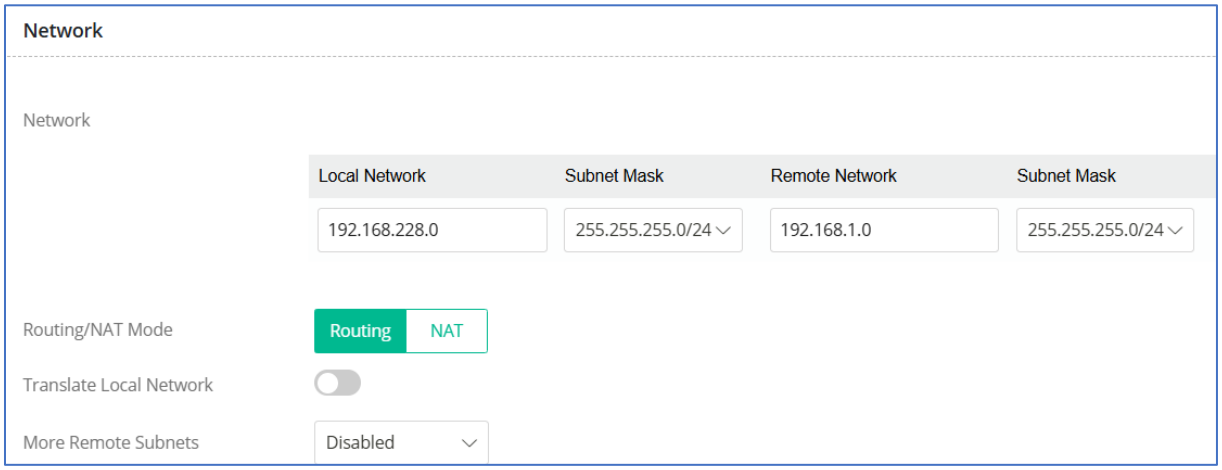


Via More Settings kunnen aanvullende opties zoals Force Reauthentication en Perfect Forward Secrecy (PFS) worden geactiveerd. Zorg ervoor dat encryptie- en authenticatie-instellingen overeenkomen met de FortiGate-configuratie.



TCP/IP Netwerk instellingen

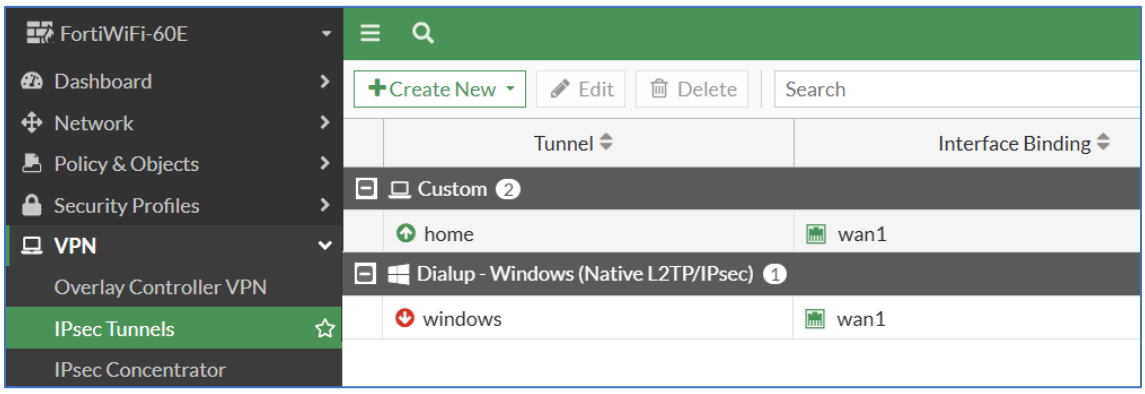
Voer bij Local Network het lokale subnet van de DrayTek in. Bij Remote Network voert u het subnet van de FortiGate in. Sla vervolgens het profiel op.



Configuratie Fortigate

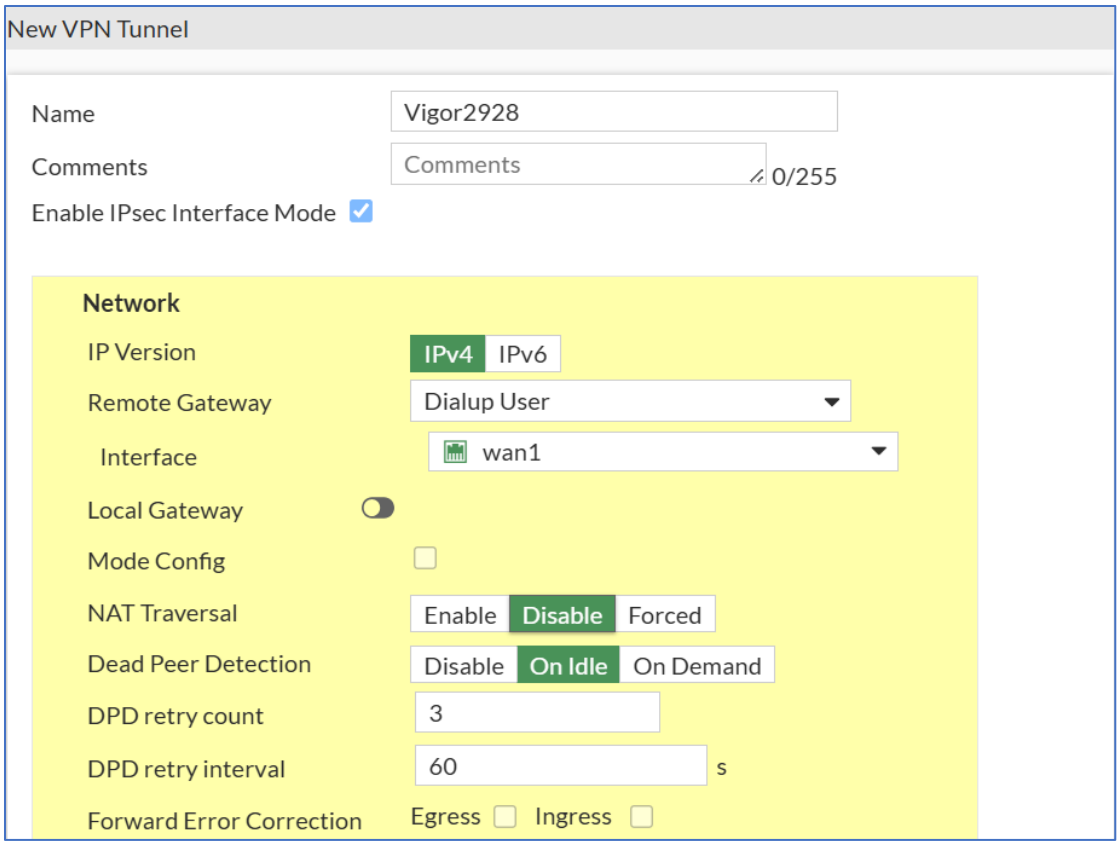
IPsec VPN tunnel aanmaken

Log eerst in op uw Fortigate. Navigeer naar VPN > IPsec Tunnels en kies Create New. Geef de tunnel een herkenbare naam, bijvoorbeeld 'VPN-DrayTek'. Selecteer Custom als template en klik op Next.



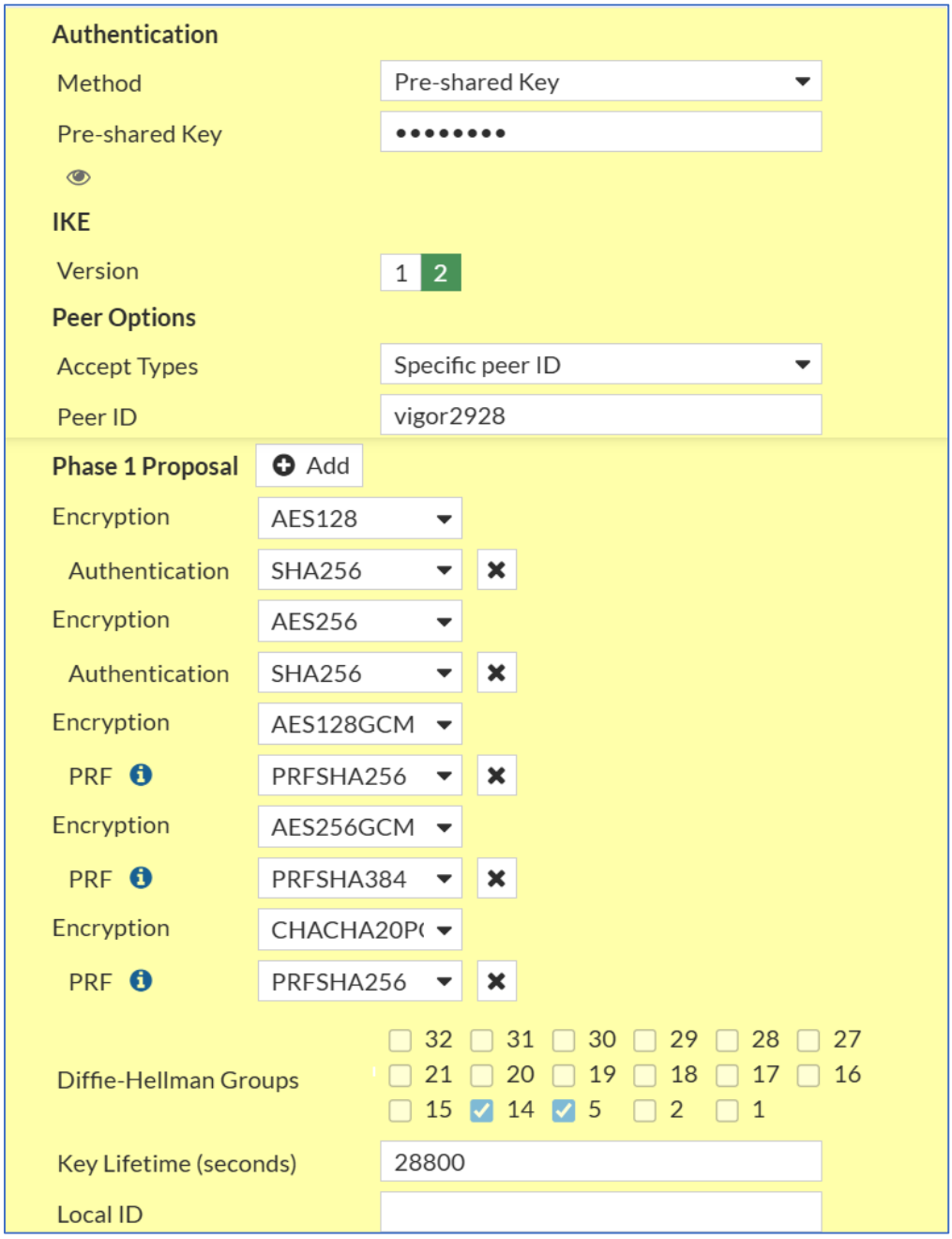
Netwerkinstellingen configureren

Selecteer de juiste IP-versie. Wanneer de DrayTek-router een dynamisch WAN-adres gebruikt, kiest u bij Remote Gateway voor Dialup User. Selecteer vervolgens de WAN-interface waarop de VPN actief moet worden.



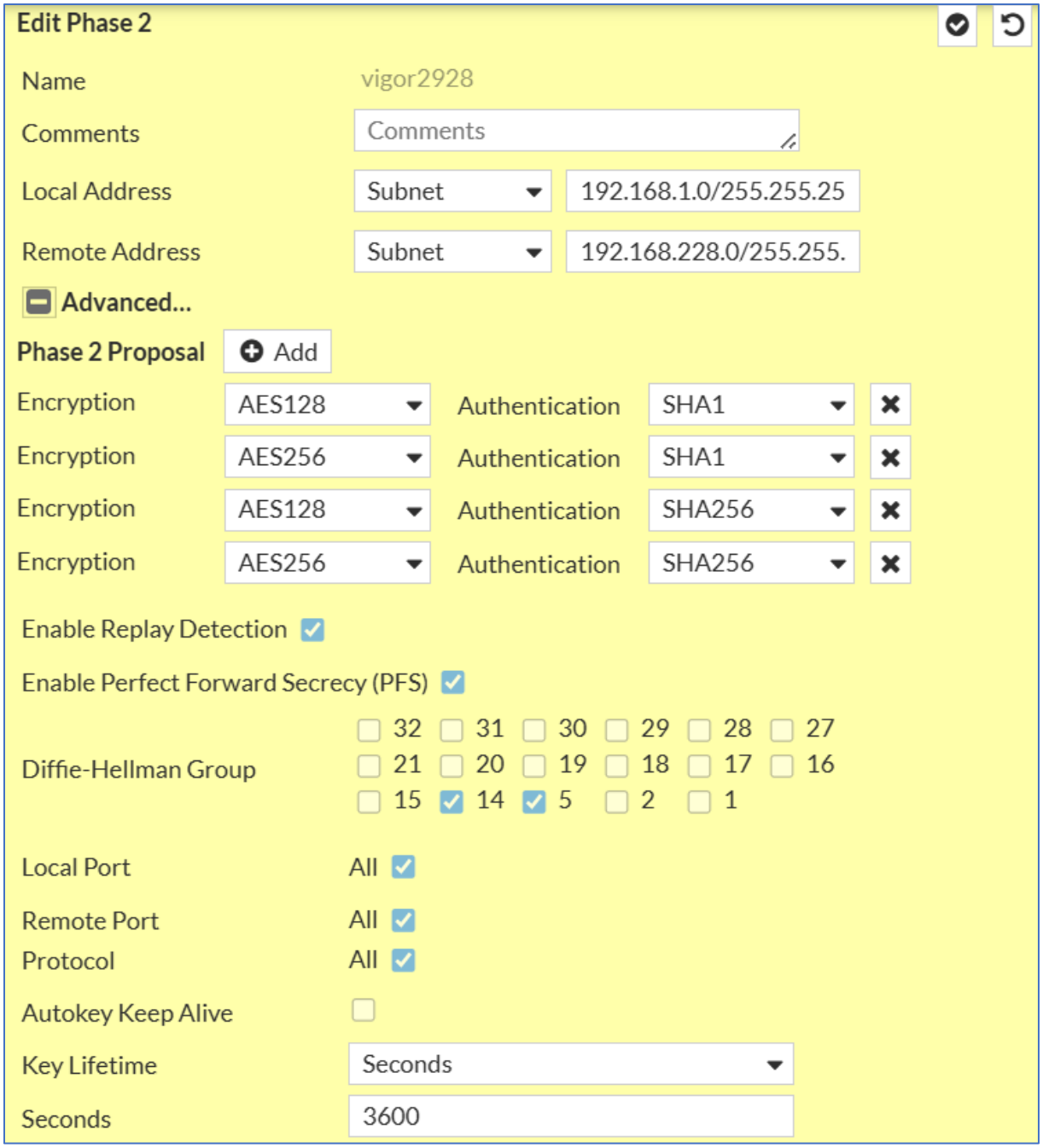
IKE Phase 1 configureren

Selecteer IKEv2 als protocolversie. Kies Pre-Shared Key als authenticatiemethode en voer de afgesproken sleutel in. Configureer de Peer ID zodat deze overeenkomt met de Local ID op de DrayTek. Stel de Key Lifetime in op 28800 seconden.



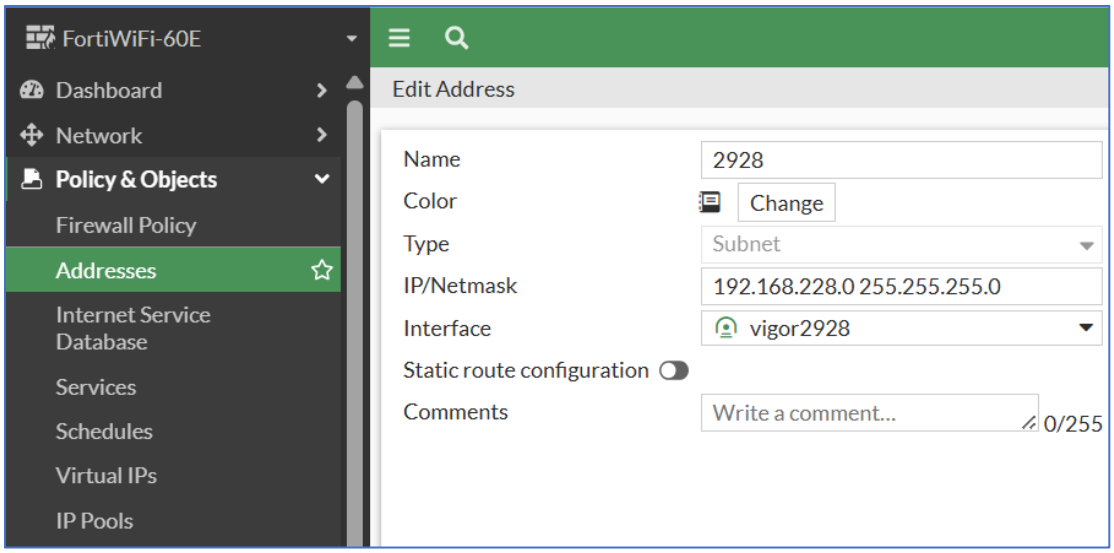
IKE Phase 2 configureren

Voer het lokale subnet van de FortiGate in als Local Address en het subnet van de DrayTek als Remote Address. Open de Advanced-instellingen en configureer de gewenste encryptie- en authenticatiealgoritmen. Stel de Key Lifetime in op 3600 seconden.



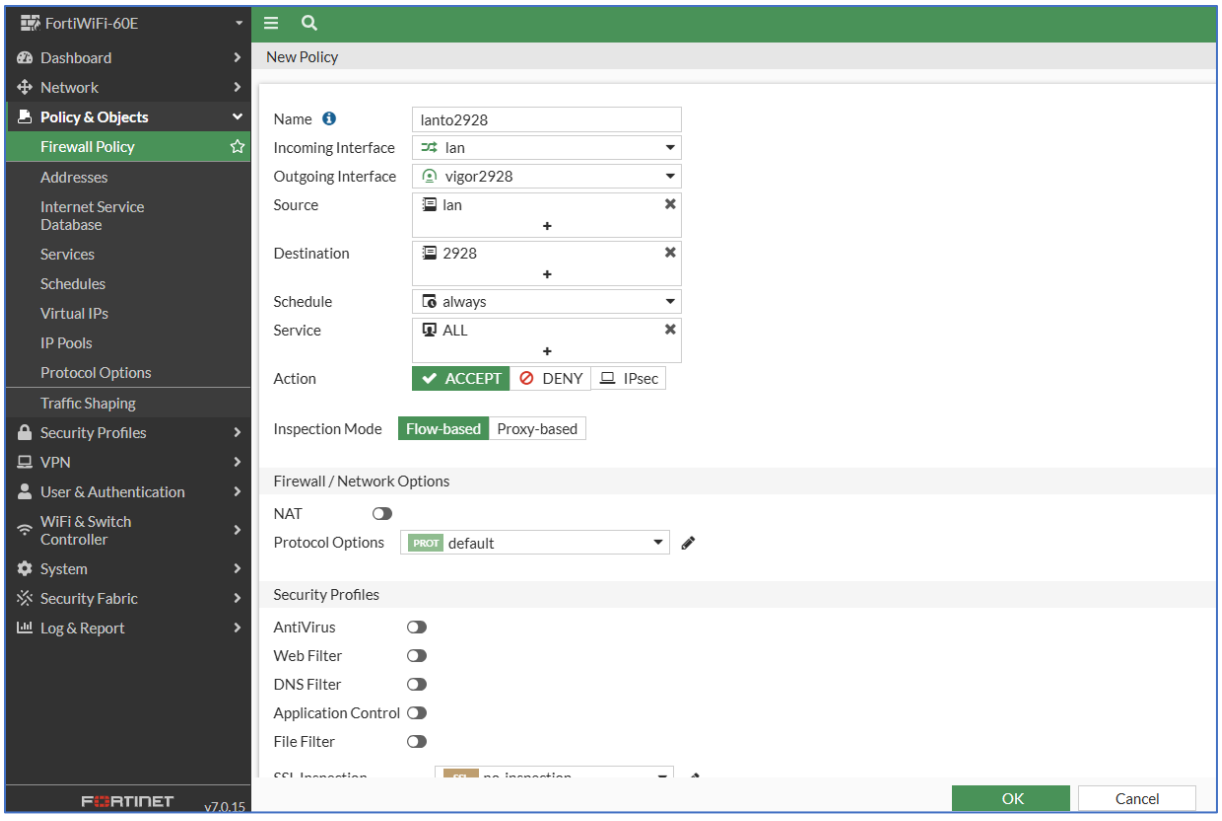
Address Object aanmaken

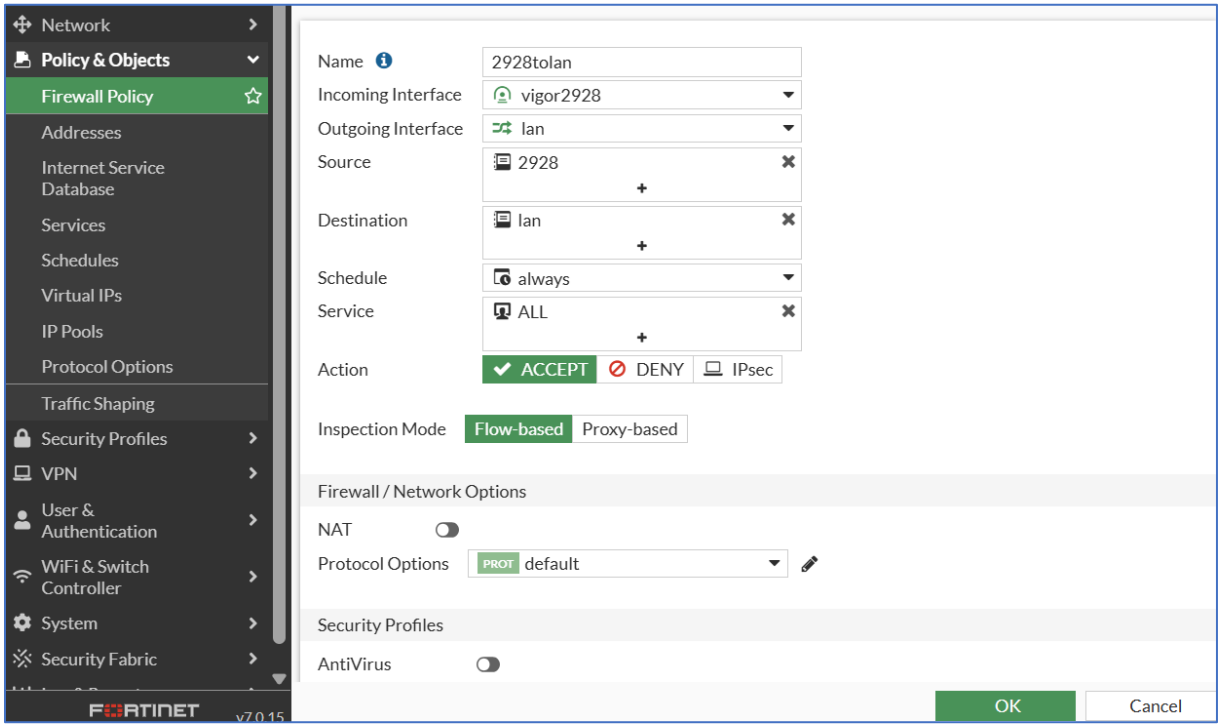
Ga naar Policy & Objects > Addresses en maak een nieuw object aan voor het LAN-subnet van de DrayTek. Koppel dit object aan de eerder aangemaakte IPsec-tunnel.



Firewall policies configureren

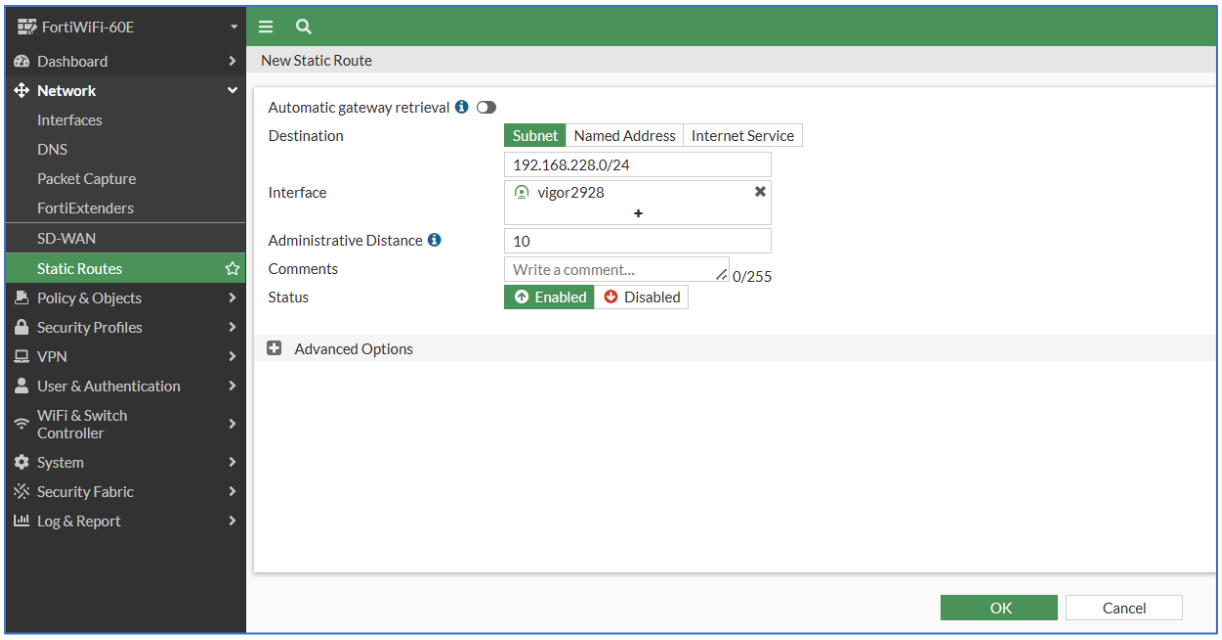
Maak twee firewallregels aan: één voor verkeer van het FortiGate LAN naar het DrayTek LAN en één voor verkeer in de tegenovergestelde richting. Schakel NAT uit voor beide regels. Controleer de volgorde van de policies zodat VPN-verkeer eerder wordt verwerkt dan algemene internetregels.





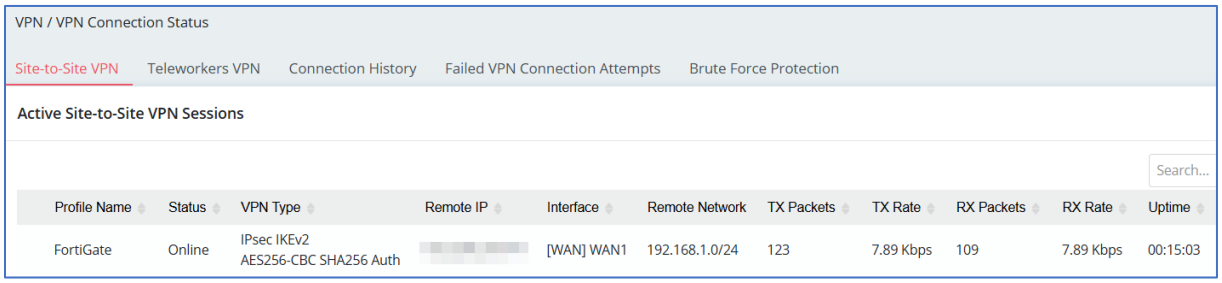
Static Route toevoegen

Ga naar Network > Static Routes en voeg een route toe naar het subnet van de DrayTek. Selecteer hierbij de IPsec-tunnel als uitgaand interface.



VPN status controleren

Wanneer Dial-Out Mode op Always On staat, probeert de router direct een verbinding op te bouwen. Controleer de status via VPN / VPN Connection Status. De tunnel moet zichtbaar zijn als Connected.



Veelvoorkomende problemen en oplossingen

VPN komt niet online:
- Controleer de Pre-Shared Key.
- Controleer Peer ID en Local ID.
- Controleer of IKEv2 aan beide zijden is geselecteerd.

Tunnel is actief maar verkeer werkt niet:
- Controleer firewallregels.
- Controleer de statische routes.
- Controleer de opgegeven subnetten in Phase 2.

Tunnel valt regelmatig weg:
- Controleer internetverbindingen.
- Controleer de Key Lifetime instellingen.
- Controleer of NAT-Traversal correct functioneert.

Reservation
We reserve the right to modify this and other documentation without the obligation to inform users. Images and screenshots may differ.