VPN

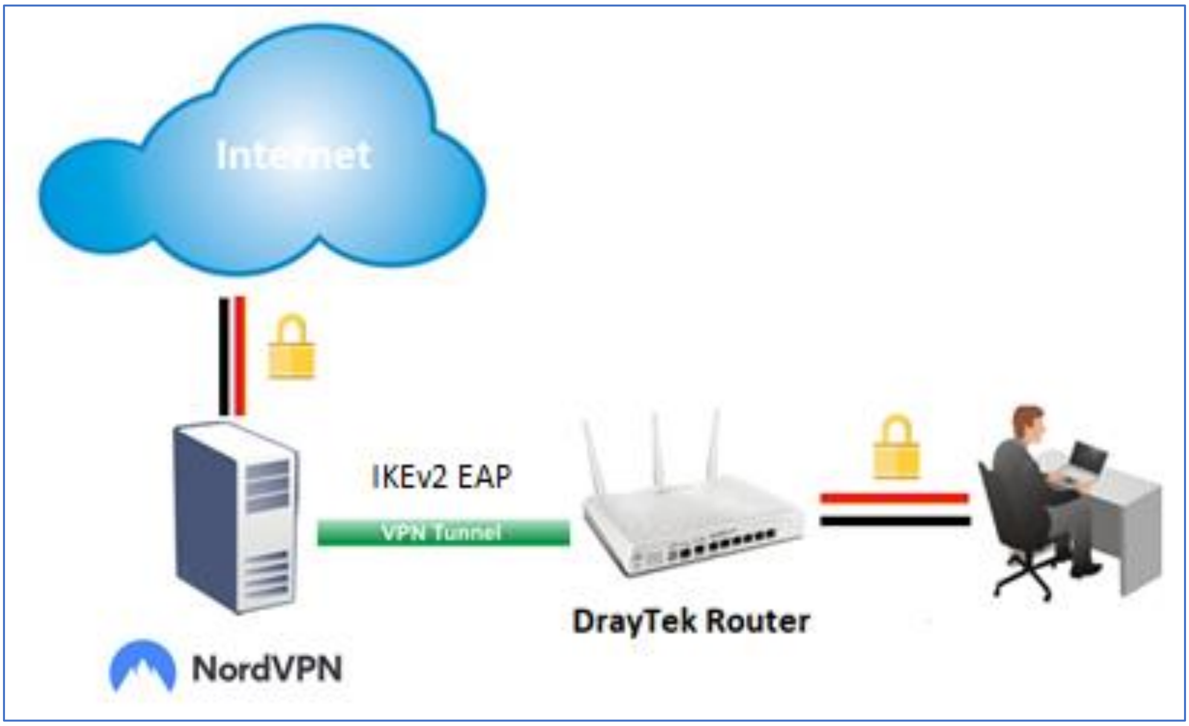
IKEv2 EAP tussen NordVPN en Vigor Router

Inhoudsopgave

NordVPN & DrayTek

In firmware versie 3.9.0 of hoger is het mogelijk om op een Vigor router gebruik te maken van de NordVPN dienst. NordVPN is een Cloud VPN Server dienst waarmee o.a. anoniem surfen ondersteund wordt en geografische restricties kunt omzeilen. Vooral het laatste is erg handig voor streaming diensten zoals Netflix en Disney+.

In deze handleiding laten we zien hoe u op een DrayTek een VPN tunnel kunt opzetten naar NordVPN op basis van het IPsec IKEv2 EAP beveiligings protocol.



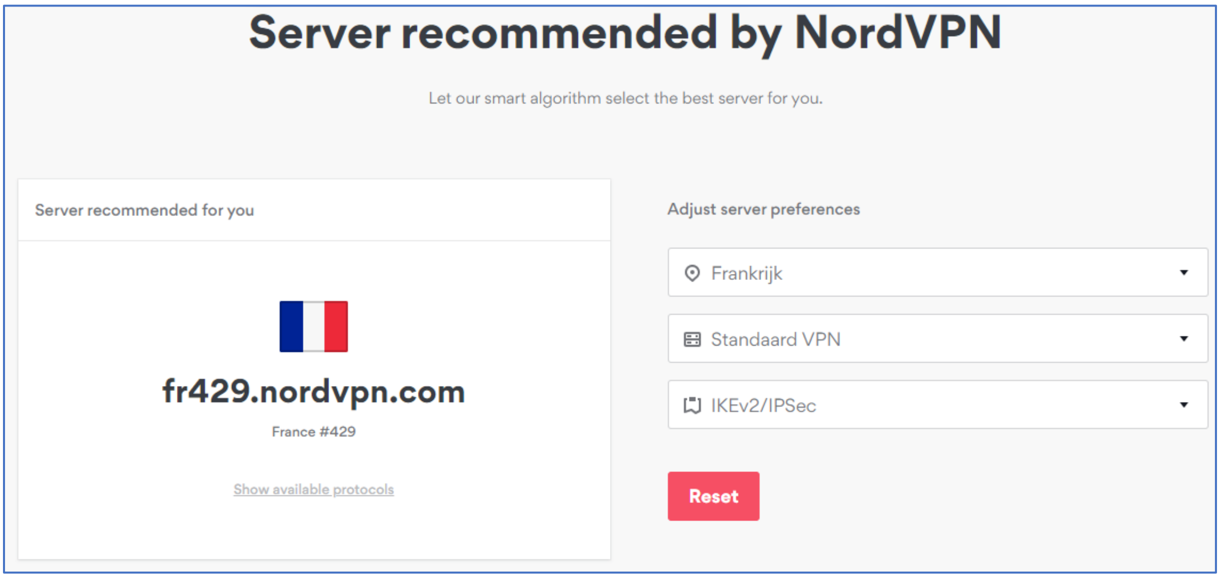
Opmerking:
De Vigor 2860 en Vigor 2925 series ondersteunen IKEv2 EAP vanaf firmware versie 3.8.9.4.
De meest recente firmware versies zijn te downloaden op onze website: www.draytek.nl/

NordVPN account

Om NordVPN te gebruiken dient u een account te registreren bij NordVPN en de NordVPN root CA certificate te downloaden. Hierna dienen we het certificaat te importeren in de DrayTek.

1. Ga naar www.nordvpn.com/ en registreer een account
2. Download de NordVPN Root CA Certificate via de volgende link: https://downloads.nordvpn.com/certificates/root.der
3. Kies een gewenst NordVPN Server via de volgende link: https://nordvpn.com/servers/tools/

Nadat u een NordVPN server hebt gekozen, zal NordVPN de aanbevolen server tonen. Let op dat de aanbevolen server wel IKEv2/IPsec ondersteuning biedt. In ons voorbeeld hebben we de NordVPN server van Frankrijk gebruikt.

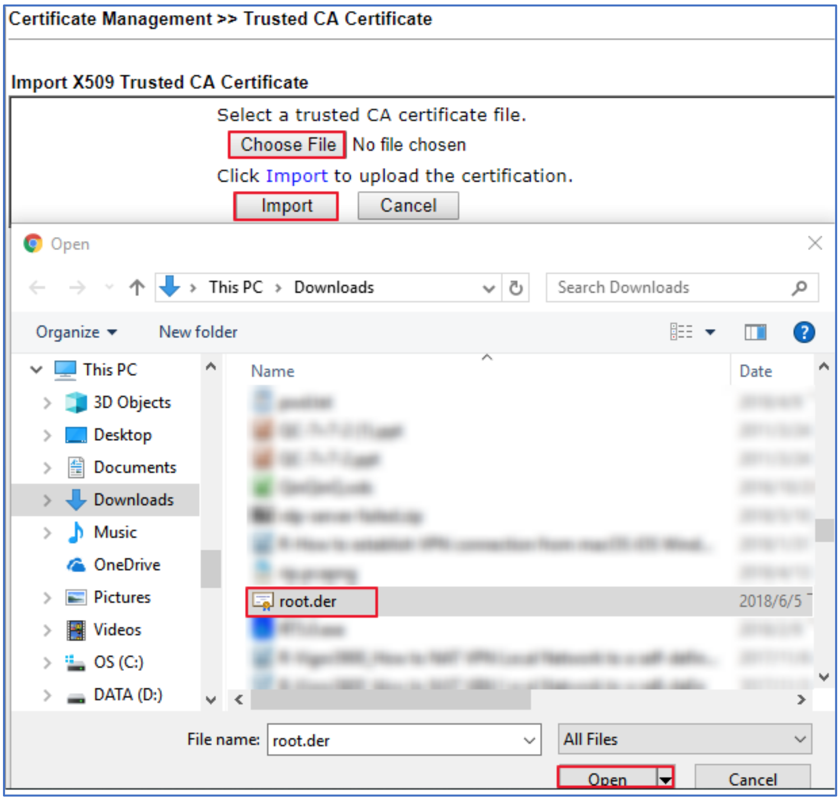


DraytTek VPN configuratie

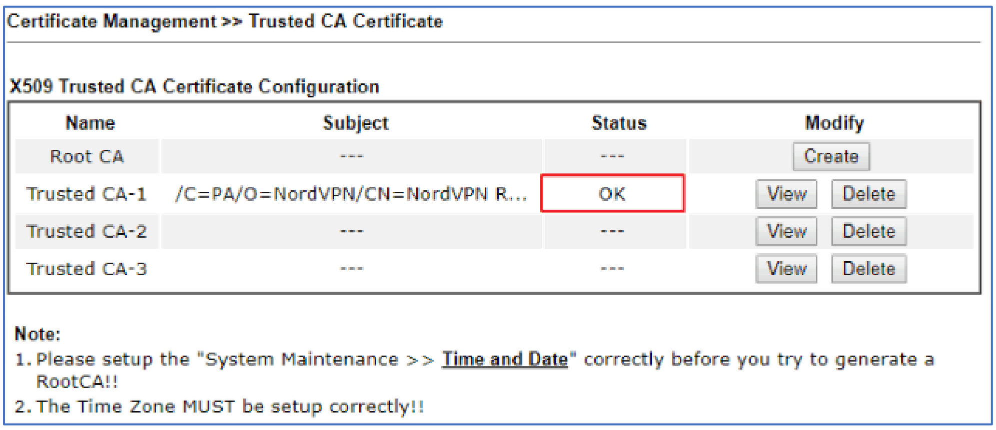
Trusted CA Certificate

Login op de management pagina van de DrayTek en navigeer naar **“Certificate Management >> Trusted CA Certificate”** Pagina en klik onderaan op **IMPORT.** Klik op **Choose File** en selecteer het zojuist gedownloade **root.der** bestand.

Klik vervolgens op **Import.**



Wacht tot de melding “Import Success” tevoorschijn komt en de Certificaat Status OK vertoond.



Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

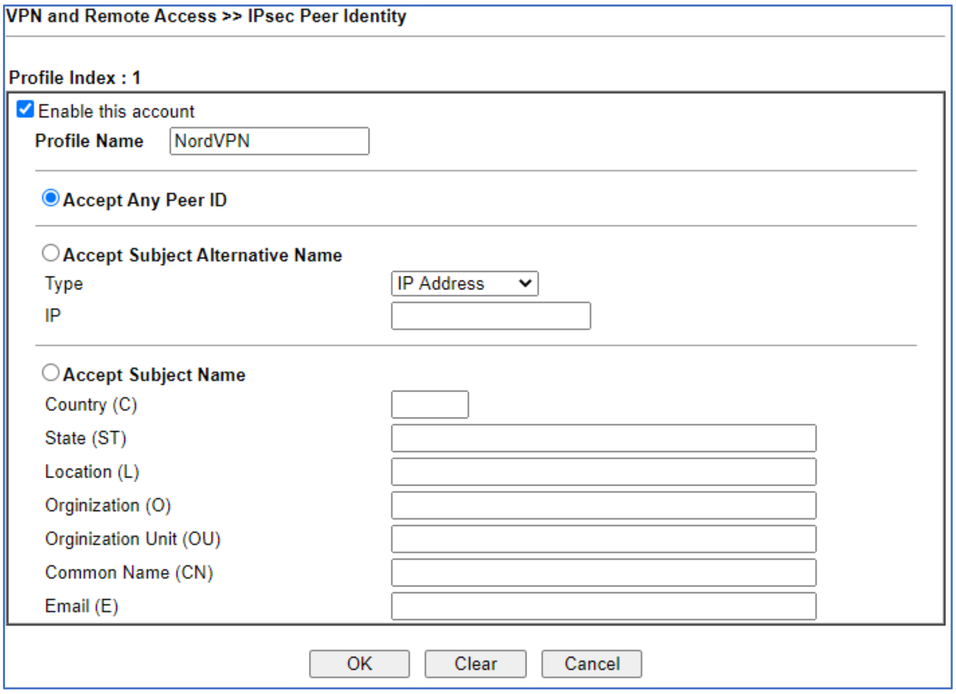
Name	Subject	Status	Modify
Root CA	---	---	Create
Trusted CA-1	/C=PA/O=NordVPN/CN=NordVPN R...	OK	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

Note:
1. Please setup the "System Maintenance >> Time and Date" correctly before you try to generate a RootCA!!
2. The Time Zone MUST be setup correctly!!

IPsec Peer Identify

Navigeer in de webinterface naar **“VPN and Remote Access >> IPsec Peer Identify”** en klik op een **index nummer** om een profiel aan te maken voor de NordVPN server.

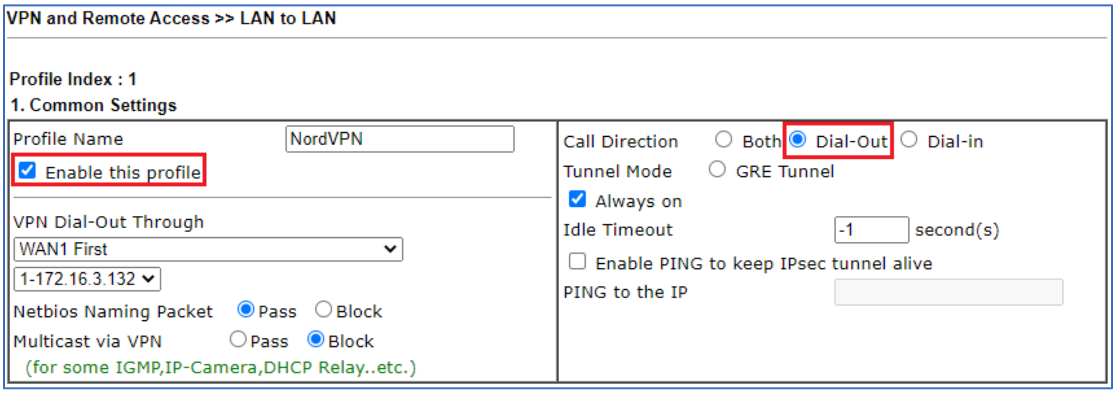
Enable this account : Aanvinken om het profiel in te schakelen
Profile Name : Geef het profiel een naam.
Accept Any Peer ID : Selecteer Any Peer ID en klik op OK



LAN-to-LAN

Navigeer naar **"VPN and Remote Access >> LAN to LAN"** en klik op een index profiel. Onderstaande instellingen zijn belangrijk:

Profile name	: Geef het VPN profiel een naam.
Enable this profile	: Aanvinken om het profiel te activeren.
Call Direction	: De DrayTek moet de VPN opzetten naar NordVPN, de DrayTek zal dus de Dial Out kant zijn.
VPN Dial-Out Through	: Via welke WAN interface moet de VPN worden opgezet.
Always On	: Indien de VPN tunnel altijd online moet zijn kunt u Always On aanvinken.

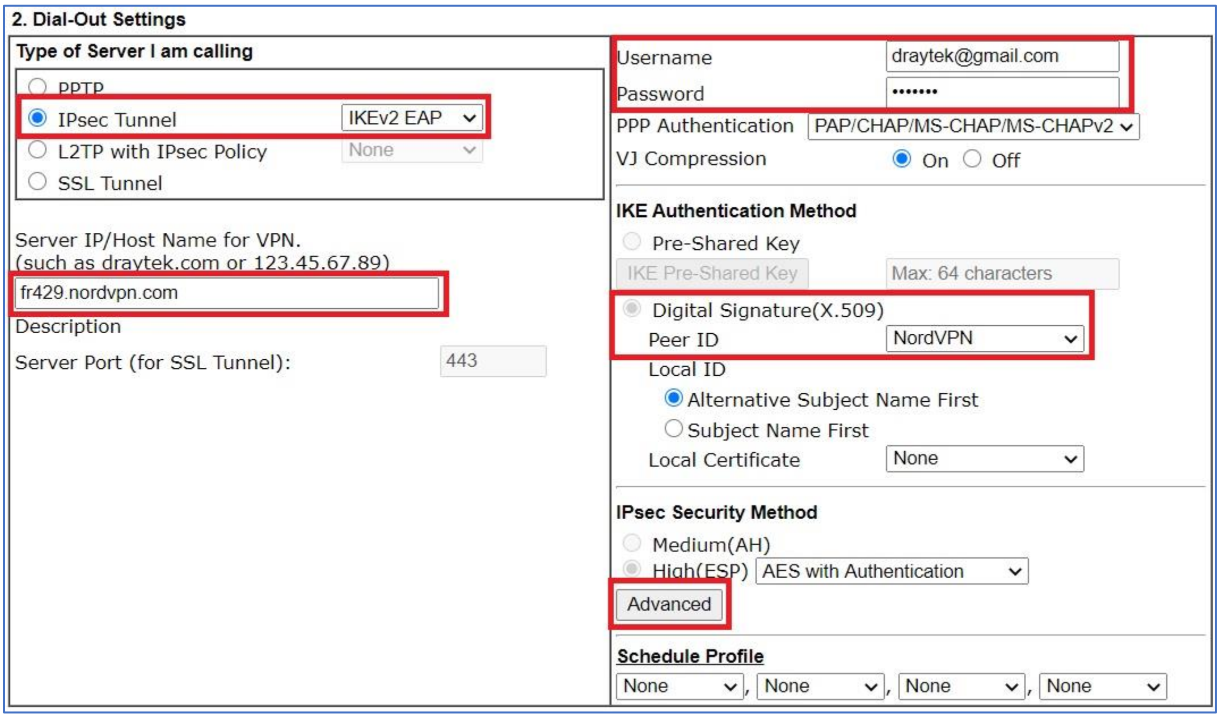


Dial-Out Settings

Bij het configureren van de Dial Out settings zijn onderstaande instellingen van belang:

Type of Server i am calling : Selecteer Type **IPsec Tunnel** met **IKEv2 EAP**
Server IP / Host Name : VPN server van NordVPN, in ons voorbeeld de server in Frankrijk.
Username : Vul uw gebruikersnaam in van NordVPN.
Password : Vul uw wachtwoord in van NordVPN.
(De inloggegevens van NordVPN zijn te vinden in het dashboard van uw NordVPN account)

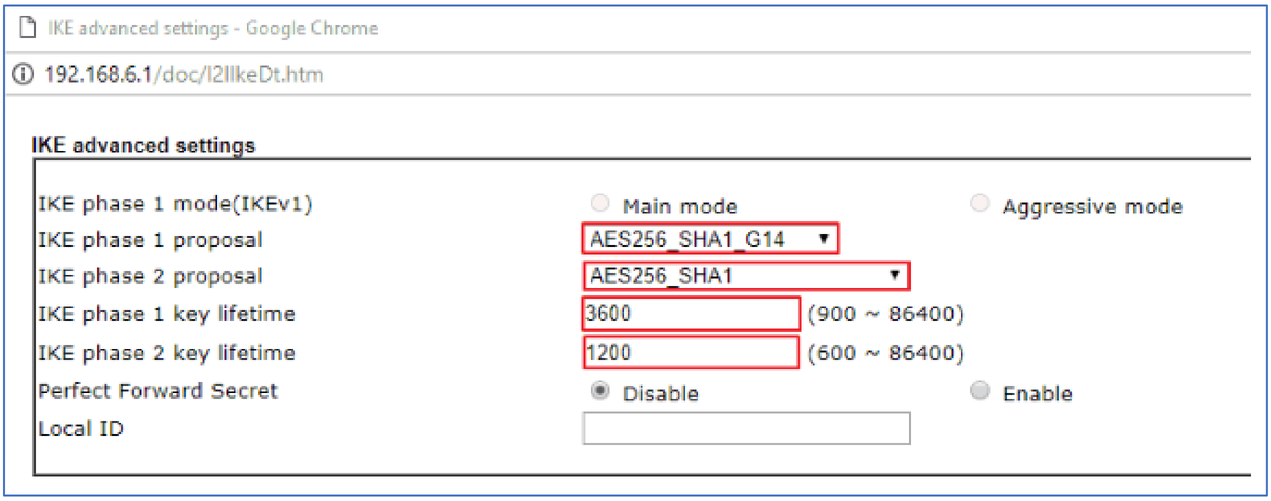
IKE Authentication Method : Selecteer **Digital Signature(X.509)** en klik bij Peer ID de Peer Identity die u zojuist hebt aangemaakt.



IPSec Security Method

Klik op de knop **Advanced** en neem de onderstaande gegevens over:

IKE phase 1 proposal: "AES256_SHA1_G14"
IKE phase 2 proposal: "AES256_SHA1"
IKE phase 1 key lifetime: "3600"
IKE phase 2 key lifetime: "1200"

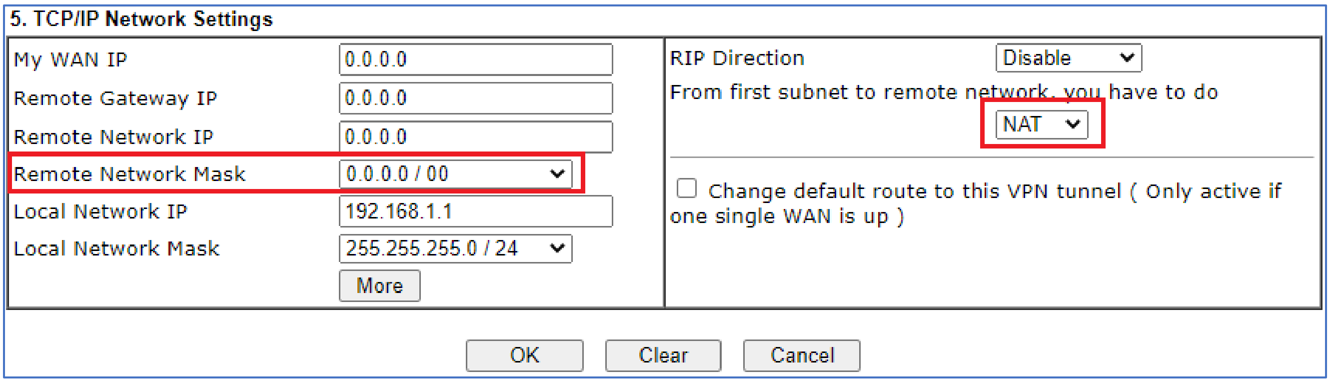


Klik op **OK** om het venster te sluiten

TCP/IP Network Settings

Vul de volgende gegevens in onder het kopje TCP/IP Network Settings:

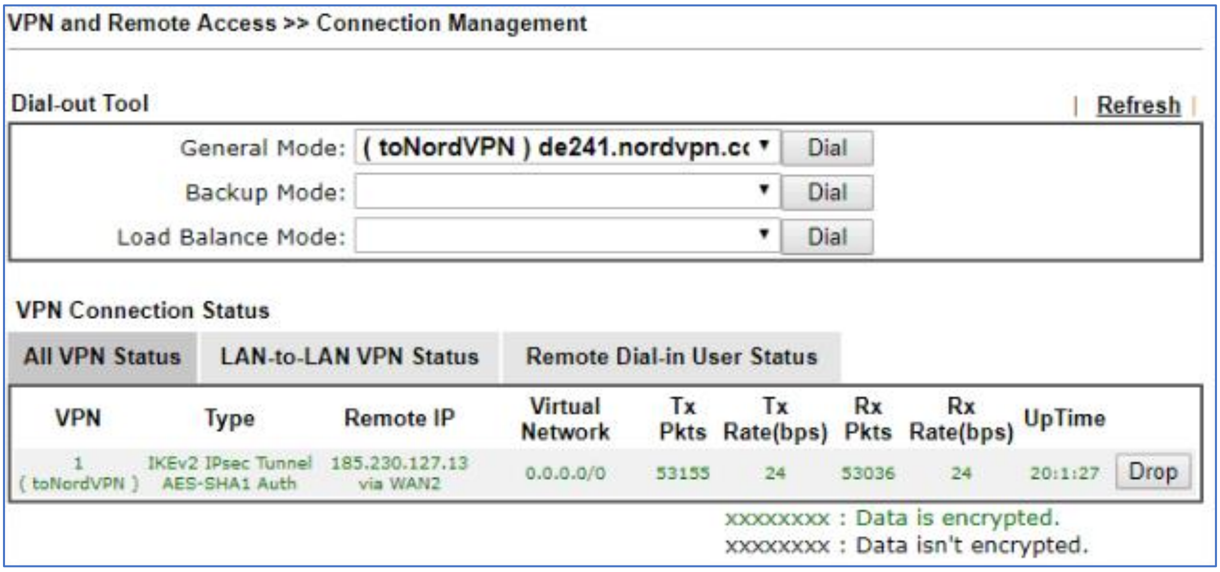
Remote Network IP	: 0.0.0.0
Remote Network Mask	: 0.0.0.0 /00
Local Network IP	: Lokaal netwerk IP-adres(LAN IP) van de DrayTek
Local Network Mask	: Lokaal subnet van de DrayTek, standaard is dit 255.255.255.0 /24
From first subnet to remote network	: NAT



Klik op **OK** om het profiel op te slaan.

VPN Connection Management

Controleer onder **“VPN and Remote Access >> Connection Management”** of de VPN tunnel tot stand is gebracht. *(het kan zijn dat u eenmalig op de Dial knop moet klikken)*

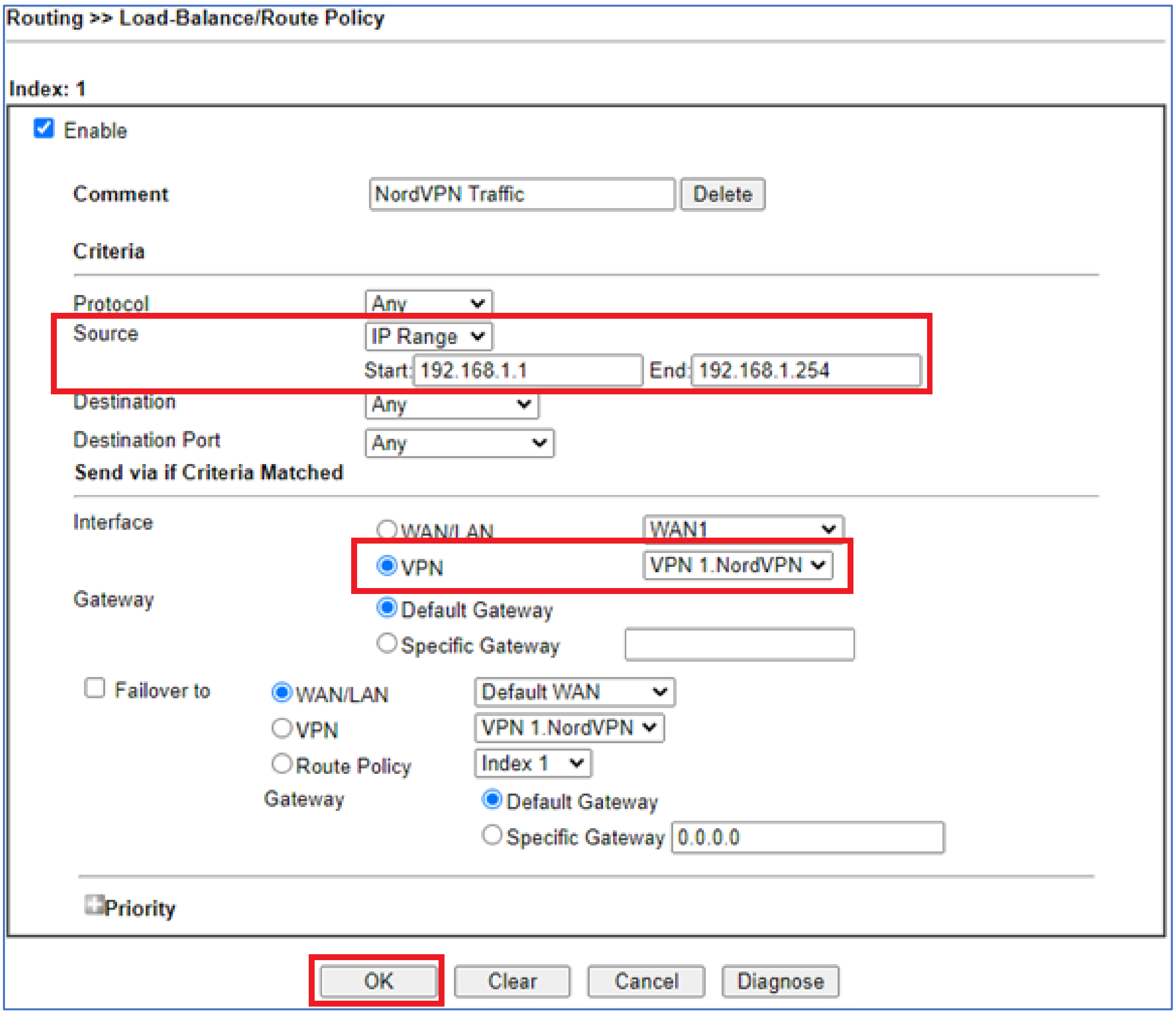


Op de volgende pagina laten we doormiddel van een policy regel zien hoe bepaalde data verkeer over de VPN tunnel gestuurd kan worden.

Load Balance / Policy Route Regel

Navigeer in het menu van de DrayTek naar **“Routing >> Load-Balance/Route Policy”.** Selecteer vervolgens onderaan de pagina de optie: **“Advance Mode: all settings in one page”** en klik op OK. Om een Load Balance / Route Policy profiel aan te maken klikt u op een Index nummer, onderstaande instellingen zijn belangrijk bij het aanmaken van een Load Balance / Policy Route regel:

Enable : Aanvinken om het profiel te activeren.
Comment : Geef het profiel een naam zodat u weet wat deze regel doet.
Protocol : Mogelijkheid tot selecteren van TCP/UDP/ICMP protocol.
Source : Lokaal IP-adres/subnet welke u gebruikt.
Destination : Bestemmingsverkeer, verkeer op het internet.
Destination Port : Bestemmingspoort, mogelijkheid tot definiëren van poort reeks.
Interface : Via welke interface moet dit verkeer naar buiten, in dit geval via de VPN verbinding naar NordVPN.



Klik op **OK**

Controle & FAQ

Werkt de VPN tunnel?

U kunt naar de website www.whatsmyip.com gaan om te controleren of het IP adres afkomstig is van de geselecteerde NordVPN server (land). Het IP adres dient hetzelfde te zijn als het IP adres die weergegeven staat onder “VPN and Remote Access >> Connection Management” onder het kopje Remote IP.

U kunt daarnaast de optie ‘tracert’ gebruiken via command prompt om te controleren of de route naar het internet via de VPN interface loopt.

Het is niet mogelijk om een website te benaderen via de NordVPN tunnel?

Controleer of u wel kunt pingen naar een website, bijvoorbeeld 8.8.8.8?
Het kan zijn dat u andere DNS servers dient te gebruiken op de DrayTek, deze kunt u instellen bij LAN > General Setup > LAN1. Vink daarna tevens de optie: Force router to use "DNS server IP address" settings specified in LAN1 aan.

Voorbehoud
We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.