

***DrayTek***

*VPN*

***IKEv2 EAP tussen NordVPN en  
Vigor Router***



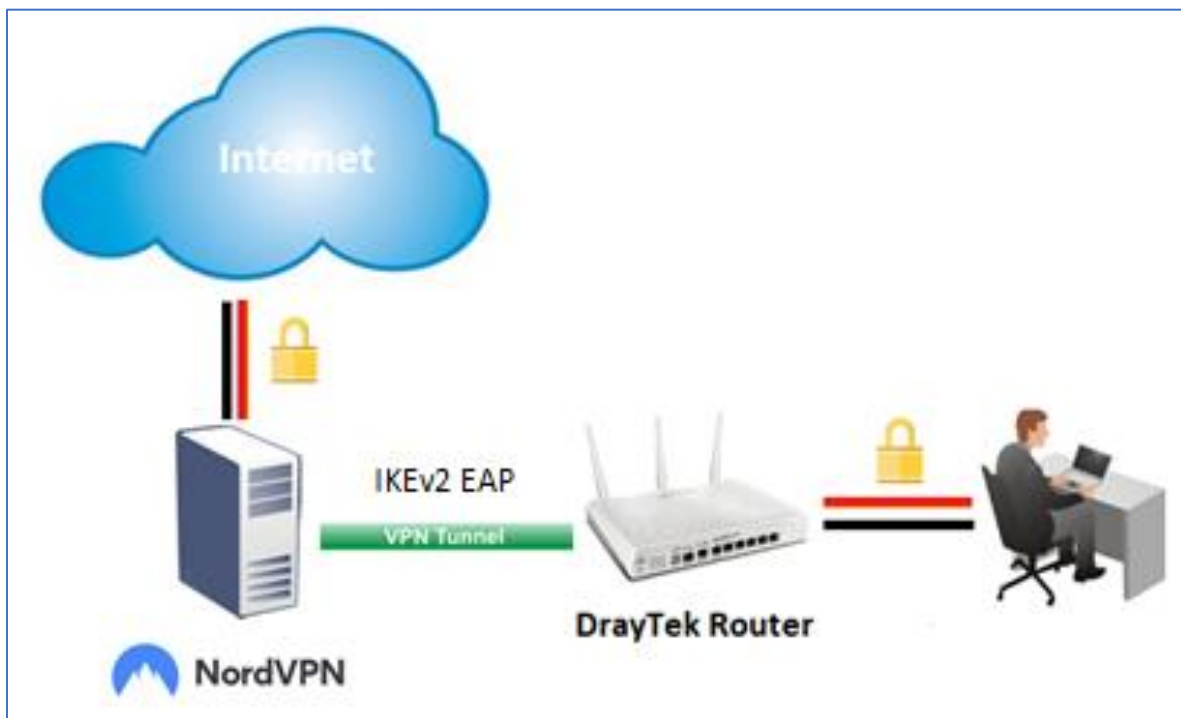
## Inhoudsopgave

NordVPN & DrayTek.....	3
NordVPN account.....	4
DrayTek VPN configuratie.....	5
Trusted CA Certificate.....	5
IPsec Peer Identify .....	6
LAN-to-LAN .....	7
Dial-Out Settings.....	8
IPSec Security Method.....	9
TCP/IP Network Settings .....	10
VPN Connection Management .....	11
Load Balance / Policy Route Regel.....	12
Controle & FAQ.....	13

## 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/](http://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/](https://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.

### Server recommended by NordVPN

Let our smart algorithm select the best server for you.

Server recommended for you



**fr429.nordvpn.com**  
France #429

[Show available protocols](#)

Adjust server preferences

📍 Frankrijk

📄 Standaard VPN

🔒 IKEv2/IPSec

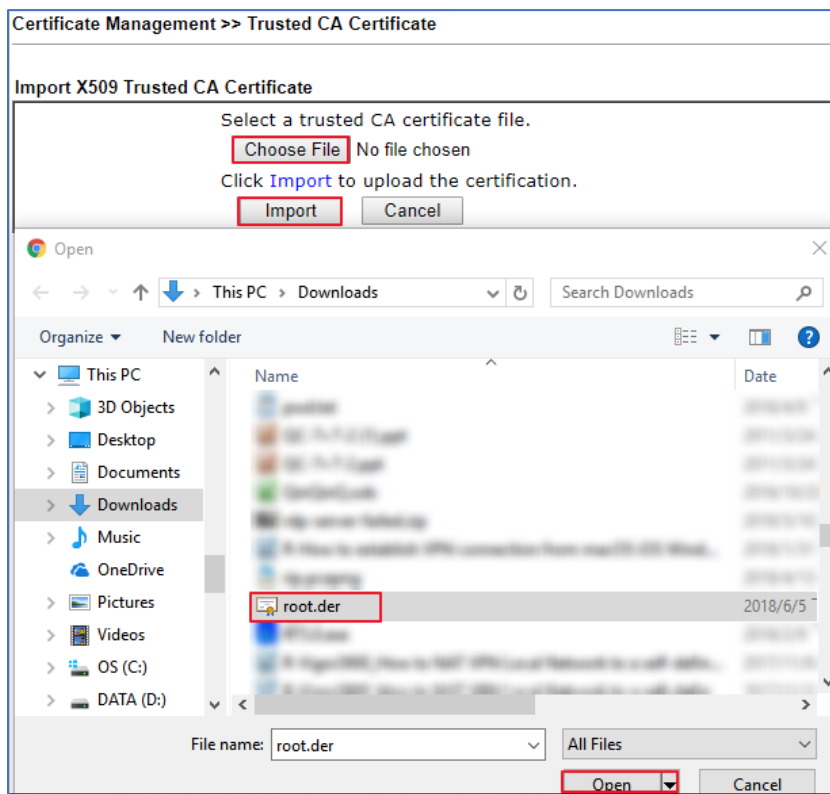
**Reset**

## DrayTek VPN configuratie

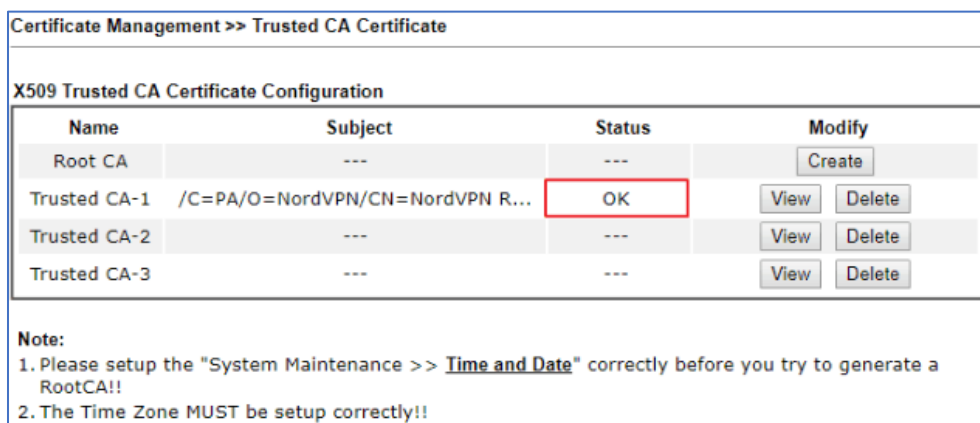
### Trusted CA Certificate

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.



## 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

VPN and Remote Access >> IPsec Peer Identity

---

Profile Index : 1

Enable this account

Profile Name

---

Accept Any Peer ID

---

Accept Subject Alternative Name

Type  ▼

IP

---

Accept Subject Name

Country (C)

State (ST)

Location (L)

Organization (O)

Organization Unit (OU)

Common Name (CN)

Email (E)

---

## 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.

VPN and Remote Access >> LAN to LAN

Profile Index : 1  
1. Common Settings

Profile Name <input type="text" value="NordVPN"/>	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	Tunnel Mode <input type="radio"/> GRE Tunnel
VPN Dial-Out Through WAN1 First <input type="text" value="1-172.16.3.132"/>	<input checked="" type="checkbox"/> Always on
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	Idle Timeout <input type="text" value="-1"/> second(s)
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>



## 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.

**2. Dial-Out Settings**

**Type of Server I am calling**

PPTP

IPsec Tunnel IKEv2 EAP

L2TP with IPsec Policy None

SSL Tunnel

Server IP/Host Name for VPN.  
(such as draytek.com or 123.45.67.89)

fr429.nordvpn.com

Description

Server Port (for SSL Tunnel): 443

Username draytek@gmail.com

Password \*\*\*\*\*

PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2

VJ Compression  On  Off

**IKE Authentication Method**

Pre-Shared Key

Digital Signature(X.509)

IKE Pre-Shared Key Max: 64 characters

Peer ID NordVPN

Local ID

Alternative Subject Name First

Subject Name First

Local Certificate None

**IPsec Security Method**

Medium(AH)

High(FSP) AES with Authentication

Advanced

**Schedule Profile**

None, None, None, None



## 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"

IKE advanced settings

IKE phase 1 mode(IKEv1)	<input type="radio"/> Main mode	<input type="radio"/> Aggressive mode
IKE phase 1 proposal	AES256_SHA1_G14 ▼	
IKE phase 2 proposal	AES256_SHA1 ▼	
IKE phase 1 key lifetime	3600	(900 ~ 86400)
IKE phase 2 key lifetime	1200	(600 ~ 86400)
Perfect Forward Secret	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Local ID	<input type="text"/>	

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

5. TCP/IP Network Settings	
My WAN IP	<input type="text" value="0.0.0.0"/>
Remote Gateway IP	<input type="text" value="0.0.0.0"/>
Remote Network IP	<input type="text" value="0.0.0.0"/>
Remote Network Mask	<input type="text" value="0.0.0.0 / 00"/>
Local Network IP	<input type="text" value="192.168.1.1"/>
Local Network Mask	<input type="text" value="255.255.255.0 / 24"/>
<input type="button" value="More"/>	
RIP Direction	<input type="text" value="Disable"/>
From first subnet to remote network, you have to do	<input type="text" value="NAT"/>
<input type="checkbox"/> Change default route to this VPN tunnel ( Only active if one single WAN is up )	
<input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

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)*

**VPN and Remote Access >> Connection Management**

Dial-out Tool | Refresh |

General Mode:	( toNordVPN ) de241.nordvpn.cc ▼	Dial
Backup Mode:	▼	Dial
Load Balance Mode:	▼	Dial

**VPN Connection Status**

All VPN Status		LAN-to-LAN VPN Status		Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime	
1 ( toNordVPN )	IKEv2 IPsec Tunnel AES-SHA1 Auth	185.230.127.13 via WAN2	0.0.0.0/0	53155	24	53036	24	20:1:27	Drop

xxxxxxx : Data is encrypted.  
xxxxxxx : Data isn't encrypted.

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.

Routing >> Load-Balance/Route Policy

Index: 1

Enable

Comment: NordVPN Traffic [Delete]

Criteria

Protocol: Any

Source: IP Range (Start: 192.168.1.1, End: 192.168.1.254)

Destination: Any

Destination Port: Any

Send via if Criteria Matched

Interface:  WAN/LAN (WAN1)  VPN (VPN 1.NordVPN)

Gateway:  Default Gateway  Specific Gateway

Failover to:  WAN/LAN (Default WAN)  VPN (VPN 1.NordVPN)  Route Policy (Index 1)

Gateway:  Default Gateway  Specific Gateway (0.0.0.0)

Priority

[OK] [Clear] [Cancel] [Diagnose]

Klik op **OK**

## Controle & FAQ

### Werkt de VPN tunnel?

U kunt naar de website [www.whatsmyip.com](http://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.

### **Copyright verklaring**

© 2020 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

### **Trademarks**

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.