

***DrayTek***

*VPN*

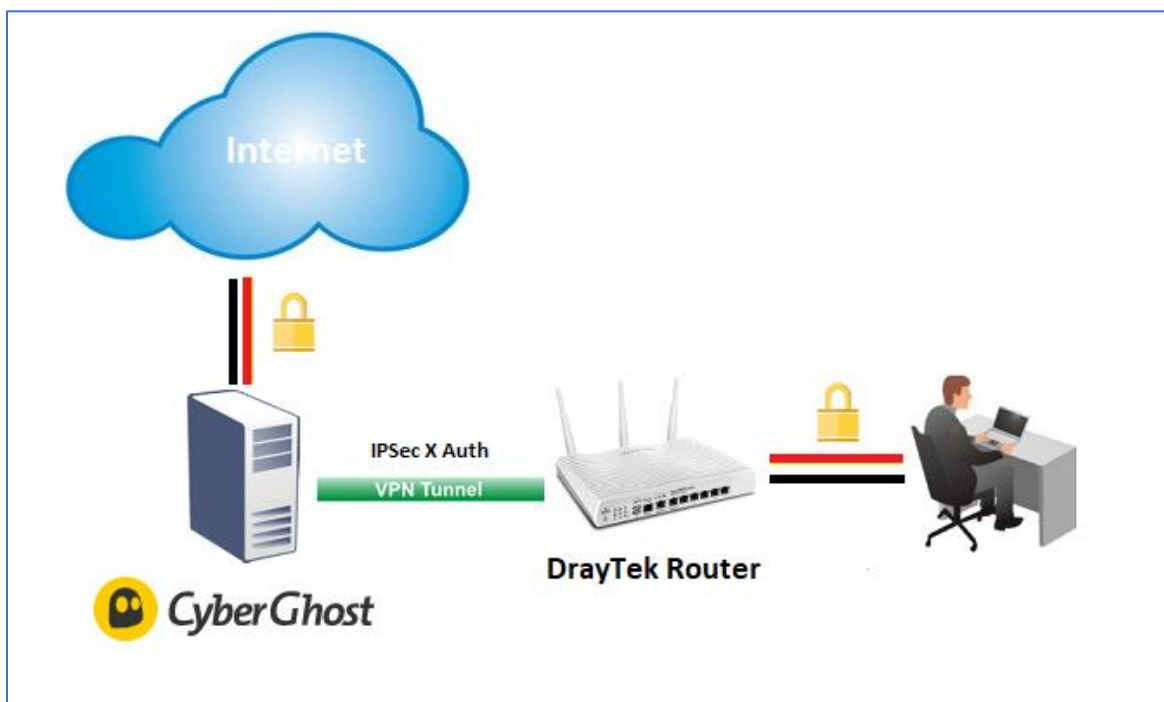
***DrayTek naar Cyberghost***



## Cyberghost

CyberGhost is een Cloud VPN Server dienst waarmee o.a Anoniem surfen ondersteund wordt en u geografische restricties kunt omzeilen. Vooral het laatste is erg handig voor Streaming diensten zoals Netflix en Disney+. Cyberghost ondersteund VPN Protocollen zoals PPTP, L2TP over IPSec , IPSec XAuth en OpenVPN.

In deze handleiding laten we zien hoe u VPN tunnel kunt op zetten met CyberGhost op basis van IPSec XAuth.

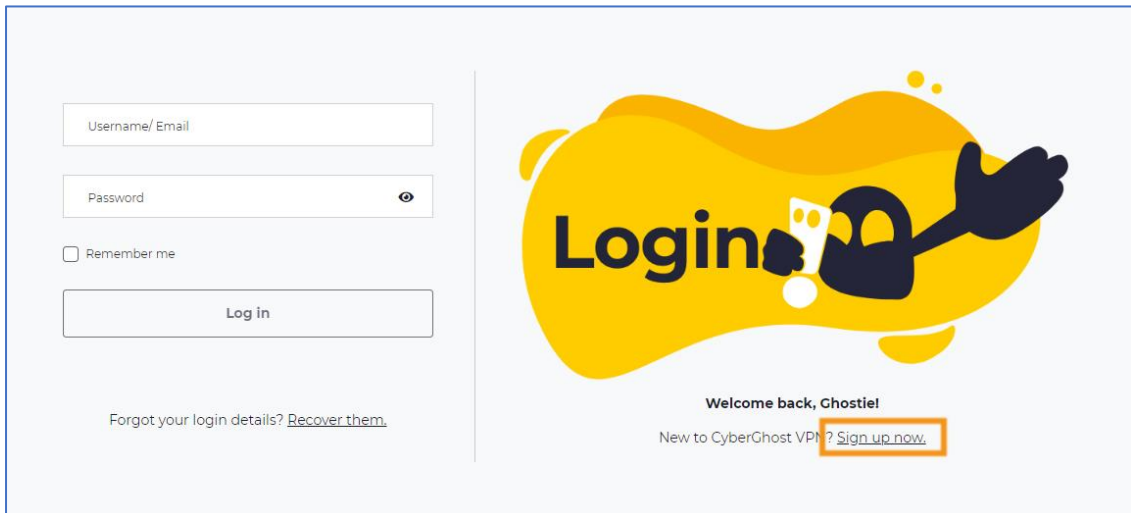


Om deze type VPN verbinding te kunnen gebruiken op de DrayTek Vigor Router zal de firmware 3.9.0 aanwezig moeten zijn.

Voor de laatste firmwares voor uw DrayTek router kunt u op onze [www.draytek.nl](http://www.draytek.nl) website terecht.

## CyberGhost Setup

1. Maak een account aan op CyberGhost  
[https://my.cyberghostvpn.com/nl\\_NL/signup](https://my.cyberghostvpn.com/nl_NL/signup)
2. Login met uw CyberGhost account



Username/ Email

Password

Remember me

Log in

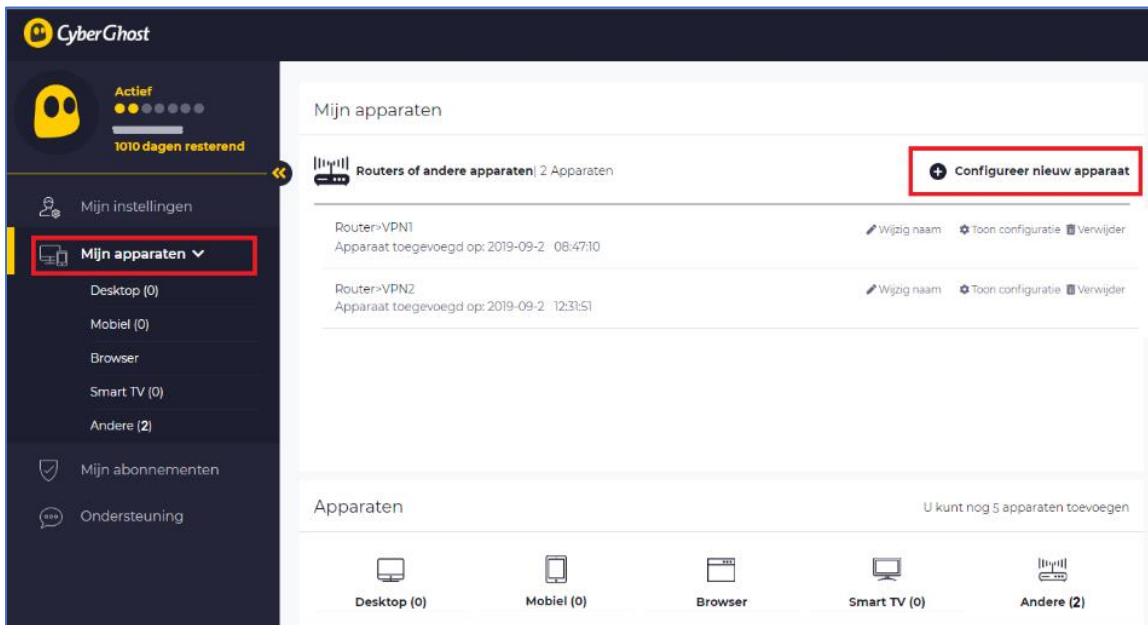
Forgot your login details? [Recover them.](#)

**Login!**

Welcome back, Ghostiel

New to CyberGhost VPN? [Sign up now.](#)

3. Voeg een nieuw apparaat toe in de Mijn apparaten



CyberGhost

Actief  
1010 dagen resterend

Mijn instellingen

**Mijn apparaten**

Desktop (0)

Mobiel (0)

Browser

Smart TV (0)

Andere (2)

Mijn abonnementen

Ondersteuning

Mijn apparaten

Routers of andere apparaten | 2 Apparaten

**+ Configureer nieuw apparaat**

Router-VPN1  
Apparaat toegevoegd op: 2019-09-2 08:47:10

Router-VPN2  
Apparaat toegevoegd op: 2019-09-2 12:31:51

Apparaten

U kunt nog 5 apparaten toevoegen

Desktop (0) Mobiel (0) Browser Smart TV (0) Andere (2)

#### 4. Klik op de Configureer nieuw apparaat

← Andere apps

**Configureer nieuw apparaat**

**Serverconfiguratie**

Protocol **1.** Land **2.** Servergroep **3.**

IPsec Verenigd Koninkrijk Premium Servers - IPsec Config Europe

**Apparaatnaam** **4.**

DrayTek VPN

**Extra functies**

Bescherming tegen kwaadaardige websites  Blokkeer advertenties

Blokkeer online volgen  Stuur door naar HTTPS

**5.**

- 1.Protocol:** IPSEC
- 2.Land:** Het land waar u de VPN verbinding wilt maken. Dit is ook tevens het land het verkeer afkomstig zal zijn. In ons voorbeeld hebben we voor Verenigd Koninkrijk ( GB) gekozen.
- 3. Servergroep:** Kies een Premium Server en anders de Streaming Server. Premium is meestal stabiel en voor meeste toepassingen wenselijk.
- 4. Apparaatnaam:** Geef hier een naam op van de VPN verbinding
- 5. Opslaan:** Klik op deze knop om de gegevens op te slaan

- Om de VPN Server gegevens te achterhalen om een IPSec XAuth te kunnen maken zul je in het overzicht van Routers of andere apparaten op de nieuw aangemaakte apparaat op de **Toon Configuratie**

DrayTek VPN Apparaat toegevoegd op: 2019-09-26 10:39:28	Wijzig naam	<b>Toon configuratie</b>	Verwijder
--	-------------	--------------------------	-----------

Hierna nog een keer op de Download Configuratie knop klikken om een tekst bestand te downloaden . Wanneer deze geopend wordt ziet u de VPN gegevens zoals onderstaand

#### Device credentials

=====

Server: 20-1-gb.cg-dialup.net  
Username: AbCdEfGhI  
Password: JkLmNoPq  
Pre-shared: CyberGhost  
Device ID: 12345678

Deze gegevens zullen in de VPN Settings van de Vigor Router overgenomen moeten worden.

## DrayTek Setup

In de DrayTek dient u nu een LAN-to-LAN VPN profiel aan te maken, dit kan in het menu VPN and Remote Access > VPN LAN-to-LAN. Op de volgende pagina ziet u de instellingen die belangrijk zijn bij het configureren van een LAN-to-LAN VPN naar CyberGhost.

Profile Index : 1

### 1. Common Settings

Profile Name: CyberGhost

Enable this profile

Call Direction:  Both  Dial-Out  Dial-in

Always on

Idle Timeout: 120 second(s)

Enable PING to keep IPsec tunnel alive

PING to the IP: [ ]

Netbios Naming Packet:  Pass  Block

Multicast via VPN:  Pass  Block  
(for some IGMP,IP-Camera,DHCP Relay..etc.)

### 2. Dial-Out Settings

Type of Server I am calling:

PPTP

IPsec Tunnel XAuth

L2TP with IPsec Policy (None)

SSL Tunnel

Username: AbCdEfGhI

Password: [ ]

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

VJ Compression:  On  Off

Server IP/Host Name for VPN:  
(for L2TP, L2TP/IPsec, PPTP, and SSL Tunnel)

20-18-de.cg-dialup.net

Server Port (for SSL Tunnel): 443

IKE Authentication Method:

Pre-Shared Key

IKE Pre-Shared Key [ ]

Digital Signature(X.509)

Peer ID: [None]

Local ID:  Alternative Subject Name First  Subject Name First

Local Certificate: [None]

IPsec Security Method:

Medium(AH)

High(ESP) AES with Authentication

[Advanced]

Schedule Profile: [None], [None], [None], [None]

### 3. Dial-In Settings

Allowed Dial-In Type:

PPTP

IPsec Tunnel

IPsec XAuth

L2TP with IPsec Policy (None)

SSL Tunnel

Specify Remote VPN Gateway

Peer VPN Server IP: [ ]

or Peer ID: [Max: 47 characters]

Username: ???

Password(Max: 11 char): [Max: 11 characters]

VJ Compression:  On  Off

IKE Authentication Method:

Pre-Shared Key

IKE Pre-Shared Key [Max: 64 characters]

Digital Signature(X.509)

[None]

Local ID:  Alternative Subject Name First  Subject Name First

IPsec Security Method:

Medium(AH)

High(ESP)  DES  3DES  AES

### 4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 0.0.0.0

Remote Network Mask: 0.0.0.0/00

Local Network IP: 192.168.1.0

Local Network Mask: 255.255.255.0/24

[More]

RIP Direction: Disable

From first subnet to remote network, you have to do NAT

IPsec VPN with the Same Subnet

Change default route to this VPN tunnel ( Only active if one single WAN is up )

OK Clear Cancel

Vul in de VPN LAN-to-LAN Profiel het volgende :

- Profile Name :** Naam van VPN Verbinding
- Enable this profile :** Om het profiel aan te zetten en dat hij actief is.
- Call Direction:** Dial Out
- Always on :** Aanvinken dat de verbinding ten alle tijden aanstaat.  
Bij een disconnect wordt de VPN verbinding opnieuw geïnitieerd.
- Type of Server i am Calling:** IPSec Tunnel en selecteer **XAuth**
- Username:** Vul hier de gebruikersnaam wat in het tekstbestand staat.
- Password:** Vul hier het wachtwoord wat in het tekstbestand staat
- Server IP/Host Namefor VPN:** Vul hier het adres van de CyberGhost Server op .
- IKE Authentcation Method:** Klik op de **IKE Pre-Shared Key** en vul 2 keer de opgegeven Preshared Key wat in het tekstbestand staat op. Meestal is dit CyberGhost
- TCP/IP Network Settings:** My WAN IP op 0.0.0.0  
Remote Gateway IP 0.0.0.0  
Remote Network IP 0.0.0.0  
Remote Network Mak 0.0.0.0/00
- RIP Direction:** Disable
- From first subnet to remote:** NAT

Klik op OK om het VPN profiel op te slaan.

Bij VPN and Remote Access > Connection Management kunt u controleren of de VPN tunnel succesvol is opgezet.

VPN and Remote Access >> Connection Management

Dial-out Tool | Refresh |

( CyberGhost ) 20-16-de.cg-dialt ▾ 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 ( CyberGhost )	IPsec Tunnel AES-SHA1 Auth	83.97.23.182 via WAN1	0.0.0.0/0	408	1.82 K	321	2.54 K	0:4:59	Drop

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

Komt hij niet online controleer dan nogmaals de gegevens. Indien hij nog niet wil verbinden probeer dan ipv van een DNS adres bij Server IP het IP-adres in te vullen. DNS naar IP-adres is te achterhalen met bijvoorbeeld een ping opdracht naar het DNS adres , hier wordt dan het IP-adres getoond.

Nu moet er alleen nog een Policy Route regel aangemaakt te worden die er voor zorgt dat al het verkeer over de VPN van Cyberghost naar Internet wordt gestuurd. In de Policy Route kan ook wenselijk ingesteld worden dat een aantal computers/ netwerk apparaten via de "gewone " Internet gaan.

Ga naar Routing > Route Policy en maak daar een nieuwe regel aan.

**Comment:** de naam van de Policy Route regel  
**Protocol:** Alles dus **any**  
**Source:** Afkomstig van welk lokaal netwerk. In dit geval alles, dus selecteren we, maar hier kan ook ip-adressen (computers/netwerk apparaten) ingevuld worden  
**Destination:** Waar naar toe. In dit geval alles, dus selecteren we **Any**  
**Destination Port:** Welke applicatie poort. In dit geval alles, dus selecteren we **Any**  
**Interface :** VPN en selecteer hier de aangemaakte VPN Profiel

Op de volgende pagina is een voorbeeld configuratie te vinden.



Routing >> Route Policy

Index: 1

Enable

Comment

Criteria

Protocol  ▾

Source  ▾

Destination  ▾

Destination Port  ▾

Send via if Criteria Matched

Interface  WAN/LAN  ▾

VPN  ▾

Gateway  Default Gateway

Specific Gateway

Failover to  WAN/LAN  ▾

VPN  ▾

Route Policy  ▾

Gateway  Default Gateway

Specific Gateway

Priority

Wanneer u klaar bent met configureren klikt u op OK om het profiel op te slaan.

Om te controleren of al het verkeer over de CyberGhost verbinding gaat kunt u controle uitvoeren door naar de volgende website te gaan:

<https://www.whatsmyip.org/>

Het IP-adres wat je te zien krijgt moet anders zijn dat het Online Status> Physical Connection WAN IP-adres

### **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.