

DrayTek

VPN

LAN-to-LAN IPSec



VPN LAN-to-LAN

De DrayTek producten beschikken over een geïntegreerde VPN server. Hierdoor kan een VPN tunnel gemaakt worden naar uw netwerk, zonder dat hiervoor een VPN server in het netwerk vereist is. VPN biedt een beveiligde verbinding over het internet naar uw eigen netwerk.

Er zijn verschillende vormen van VPN. DrayTek ondersteunt PPTP, L2TP, IPSec en SSL. Van deze protocollen is PPTP de minst beveiligde vorm van VPN. IPSec biedt een betere beveiliging door een encryptie die continu verandert. L2TP is, in combinatie met IPSec, de meest veilige vorm van VPN. Helaas is dit ook de reden dat het protocol moeilijk in gebruik is. Momenteel is IPSec de meest gebruikte vorm bij het opzetten van een LAN-to-LAN VPN tunnel.

Beveiliging van de VPN tunnel gebeurt door de verschillende encryptie protocollen. DrayTek ondersteunt DES, 3DES, AES. Standaard adviseren wij gebruik te maken van AES with encryption, dit is de meest veilige encryptie methode die je kunt gebruiken bij het opzetten van een VPN verbinding.

Met de DrayTek routers is het mogelijk twee netwerken transparant te koppelen. Dit kan door gebruik te maken van de LAN-to-LAN VPN. Met deze VPN tunnel wordt de verbinding opgezet tussen twee routers.

In deze handleiding zullen we ingaan op het opzetten van een LAN-to-LAN VPN verbinding doormiddel van het IPSec protocol.

Situatie

Een bedrijf heeft twee vestigingen die beide op elkaars netwerk moeten werken. U moet hiervoor een VPN verbinding opzetten zodat ze probleemloos met elkaar kunnen communiceren. Om een VPN verbinding op te zetten heeft u onderstaande gegevens nodig:

	Locatie 1	Locatie 2
Apparaat	DrayTek Vigor 2926	DrayTek Vigor 2862
LAN IP-subnet	192.168.100.0	10.1.1.0
LAN subnetmask	255.255.255.0	255.255.255.0
Publiek IP-adres	Publiek IP-adres	Publiek IP-adres
Verbindings richting (server/client)	Dial Out (client)	Dial In (server)
evt. gebruikersnaam	-	-
evt. wachtwoord	-	-
Protocol	IPSec	IPSec
Pre-Shared Key	draytek	
Encryptie	AES	

Aangezien het hier om een IPSec verbinding gaat moet u eerst controleren of deze functie wel geactiveerd is. Dit kunt u doen bij VPN and Remote Access >> Remote Access Control.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPSec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service

Note:
To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT Open Ports or Port Redirection is also configured.

OK Clear Cancel

Belangrijk: Indien een DrayTek router reeds achter een bestaand netwerk(NAT) staat zal deze DrayTek de Dial Out verbinding op moeten zetten.

DrayTek Vigor 2926 series

In het hoofdmenu van de DrayTek gaat u naar VPN and Remote Access hier klikt u vervolgens op LAN to LAN.



U krijgt een nieuw scherm te zien waarin u een lijst ziet met lege profielen. U klikt op een van de indexnummers om een nieuw profiel aan te maken.

The screenshot shows the "VPN and Remote Access >> LAN to LAN" configuration page. It features a "LAN-to-LAN Profiles:" section with a "View:" dropdown set to "All" and a "Set to Factory Default" link. Below is a table with 10 columns: Index, Enable, Name, Remote Network, Status, Index, Enable, Name, Remote Network, Status. The table contains 10 rows of empty profiles with index numbers 1 through 10 and "???" in the Name and Remote Network columns. The "Enable" column has checkboxes that are currently unchecked.

Index	Enable	Name	Remote Network	Status	Index	Enable	Name	Remote Network	Status
1.	<input type="checkbox"/>	???		---	17.	<input type="checkbox"/>	???		---
2.	<input type="checkbox"/>	???		---	18.	<input type="checkbox"/>	???		---
3.	<input type="checkbox"/>	???		---	19.	<input type="checkbox"/>	???		---
4.	<input type="checkbox"/>	???		---	20.	<input type="checkbox"/>	???		---
5.	<input type="checkbox"/>	???		---	21.	<input type="checkbox"/>	???		---

Als eerste vinkt u Enable this profile aan om het profiel te activeren. Geef vervolgens een bijpassende naam aan dit profiel. Aangezien het hier om een Dial out profiel gaat, zet u de Call Direction op Dial-Out. Ook vinkt u Always On aan zodat de VPN Tunnel altijd online moet blijven. Always On kunt u alleen gebruiken bij een Dial Out verbinding.

The screenshot shows the configuration page for "Profile Index : 1". It is divided into two main sections. The left section, "1. Common Settings", includes: Profile Name (VPN), a checked "Enable this profile" checkbox, a "VPN Dial-Out Through" dropdown menu (WAN1 First), and radio buttons for "Netbios Naming Packet" (Pass) and "Multicast via VPN" (Block). The right section includes: "Call Direction" (Dial-Out selected), "Tunnel Mode" (GRE Tunnel), a checked "Always on" checkbox, "Idle Timeout" (set to -1 second(s)), and checkboxes for "Enable PING to keep IPsec tunnel alive" and "PING to the IP".

U gaat daarna naar punt 2: Dial Out Settings. Als eerste geeft u aan dat het om een IPsec tunnel gaat, u kunt dan nog aangeven of u op basis van IKEv1 of IKEv2 een VPN wil opzetten. Bij Server IP/Host Name for VPN geeft u het publieke adres op van de andere locatie, dit is het WAN IP-adres welke de DrayTek Vigor 2862 ontvangt op zijn WAN poort. Let er wel op dat dit een publiek IP-adres moet zijn.

2. Dial-Out Settings	
Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel IKEv1 ▼ <input type="radio"/> L2TP with IPsec Policy None ▼ <input type="radio"/> SSL Tunnel	Username <input type="text" value="???"/> Password <input type="text" value="Max: 15 characters"/> PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2 ▼ VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="publiek IP-adres Vigor2862"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="*****"/> <input type="radio"/> Digital Signature(X.509) Peer ID None ▼ Local ID <input type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate None ▼
	IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) AES with Authentication ▼ <input type="button" value="Advanced"/>
	Schedule Profile None ▼ , None ▼ , None ▼ , None ▼

Vervolgens geeft u nog een Pre Shared Key op, dit kan door op IKE Pre-Shared Key te klikken. U krijgt een pop-up scherm te zien waarin u tweemaal de Pre-Shared Key moet invullen. Deze key moet hetzelfde zijn als bij de andere locatie. Na het opgeven van deze key geeft u de IPsec Security Method aan. We gaan in dit geval voor High (ESP) AES with Authentication.

De Dial In Settings hoeft u niet te configureren bij een Dial Out profiel.

Ga door naar punt 5: TCP/IP Network Settings. Hier geeft u het Remote Network IP op van de DrayTek Vigor 2862. Dit betreft het LAN subnet van de Vigor 2862. Klik vervolgens op OK om het profiel op te slaan.

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="10.1.1.0"/>
Remote Network Mask	<input type="text" value="255.255.255.0 / 24"/>
Local Network IP	<input type="text" value="192.168.100.0"/>
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="Route"/>
<input type="checkbox"/> IPsec VPN with the Same Subnets	
<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"/>	

Belangrijk: My WAN IP en Remote Gateway IP kunt u op 0.0.0.0 laten staan, beide adressen zijn namelijk reeds bekend bij de DrayTek.

DrayTek Vigor 2862 series

In het hoofdmenu van de DrayTek gaat u naar VPN and Remote Access. Klik vervolgens op LAN to LAN.



U krijgt een nieuw scherm te zien waarin u een lijst ziet met lege profielen. Omdat u een nieuw profiel wilt aanmaken, klikt u op een van deze Index nummers.

VPN and Remote Access >> LAN to LAN ?

LAN-to-LAN Profiles: | [Set to Factory Default](#) |

View: All Trunk

Index	Enable	Name	Remote Network	Status	Index	Enable	Name	Remote Network	Status
<u>1.</u>	<input type="checkbox"/>	???		---	<u>17.</u>	<input type="checkbox"/>	???		---
<u>2.</u>	<input type="checkbox"/>	???		---	<u>18.</u>	<input type="checkbox"/>	???		---
<u>3.</u>	<input type="checkbox"/>	???		---	<u>19.</u>	<input type="checkbox"/>	???		---
<u>4.</u>	<input type="checkbox"/>	???		---	<u>20.</u>	<input type="checkbox"/>	???		---
<u>5.</u>	<input type="checkbox"/>	???		---	<u>21.</u>	<input type="checkbox"/>	???		---

Aangezien het hier om een Dial In profiel gaat hoeft u het Dial Out profiel niet te configureren. U zet als eerste weer een vinkje bij Enable this profile. Hierna selecteert u Dial-In als Call Direction en gaat naar Punt 3. Dial In Settings.

Profile Index : 1
1. Common Settings

Profile Name <input type="text" value="VPN"/>	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	Tunnel Mode <input type="radio"/> GRE Tunnel
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	<input type="checkbox"/> Always on
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	Idle Timeout <input type="text" value="0"/> 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"/>

Belangrijk: Always on kunt u niet selecteren bij een Dial-In profiel, wel kunt u de Idle Timeout op 0 seconden zetten. Zodoende zal deze DrayTek de VPN tunnel niet verbreken indien er geen activiteit plaats vindt.

Bij de Dial-In Settings geeft u aan dat het om een IPsec Tunnel gaat, tevens geeft u bij Pre-Shared Key de key op die u bij de DrayTek Vigor 2926 ook hebt opgegeven. Zet een vinkje bij Specify Remote VPN Gateway en vul bij Peer VPN Server IP het publieke IP-adres in van de DrayTek Vigor 2926. Zorg er daarnaast voor dat AES geselecteerd is bij IPsec Security Method.

3. Dial-In Settings

Allowed Dial-In Type

- PPTP
- IPsec Tunnel
- L2TP with IPsec Policy None
- SSL Tunnel

Specify Remote VPN Gateway

Peer VPN Server IP
publiek IP 2926

or Peer ID Max: 47 characters

Username ???

Password(Max 11 char) Max: 11 characters

VJ Compression On Off

IKE Authentication Method

- Pre-Shared Key
- Digital Signature(X.509)

None

Local ID

- Alternative Subject Name First
- Subject Name First

IPsec Security Method

Medium(AH)

High(ESP) DES 3DES AES

Geef bij Remote Network IP het LAN IP Subnet op van de DrayTek Vigor 2926.

5. TCP/IP Network Settings

My WAN IP 0.0.0.0

Remote Gateway IP 0.0.0.0

Remote Network IP 192.168.100.0

Remote Network Mask 255.255.255.0 / 24

Local Network IP 10.1.1.0

Local Network Mask 255.255.255.0 / 24

More

RIP Direction Disable

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

- IPsec VPN with the Same Subnets
- Change default route to this VPN tunnel (Only active if one single WAN is up)

OK Clear Cancel

Vervolgens kunt u bij VPN and Remote Access >> Connection Management controleren of de VPN tunnel succesvol online is gekomen. Bij een Always On VPN tunnel zal de DrayTek automatisch de VPN tunnel opzetten.

Wanneer u geen Always On gebruikt dient u de VPN tunnel zelf te initiëren middels de Dial knop bij Connection Management. Deze Dial functie kan alleen aan de Dial Out kant gedaan worden.

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.