

DrayTek

VPN
LAN-to-LAN IPsec



Inhoudsopgave

VPN LAN-to-LAN	3
Situatieschets	4
Dial Out (Client) configuratie.....	5
IKE Phase 1 Settings	6
IKE Phase 2 Settings	7
IKE Advanced Settings	7
Ping to keep alive.....	7
Dial In (Server) instellingen	9
Allowed VPN Type	10
Allowed IKE Authentication Method	10
Allowed IPsec Security Method	10

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. DrayTek heeft in de nieuwe product serie (firmware versie 4.x.x) een nieuwe VPN LAN-to-LAN configuratie toegevoegd. Op basis van de Call Direction zal de WebGUI worden aangepast zodat alleen de noodzakelijke configuratie instellingen getoond zullen worden.

Situatieschets

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 2927	DrayTek Vigor 2865
LAN IP-subnet	172.31.254.0	10.0.0.0
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 IKEv1	IPsec IKEv1
Pre-Shared Key	DrayTek123!	
Encryptie	AES128	

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

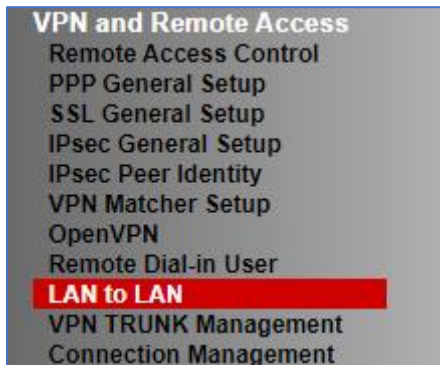
Remote Access Control Setup

- Enable PPTP VPN Service
- Enable IPsec VPN Service
- Enable L2TP VPN Service
- Enable SSL VPN Service
- Enable OpenVPN Service

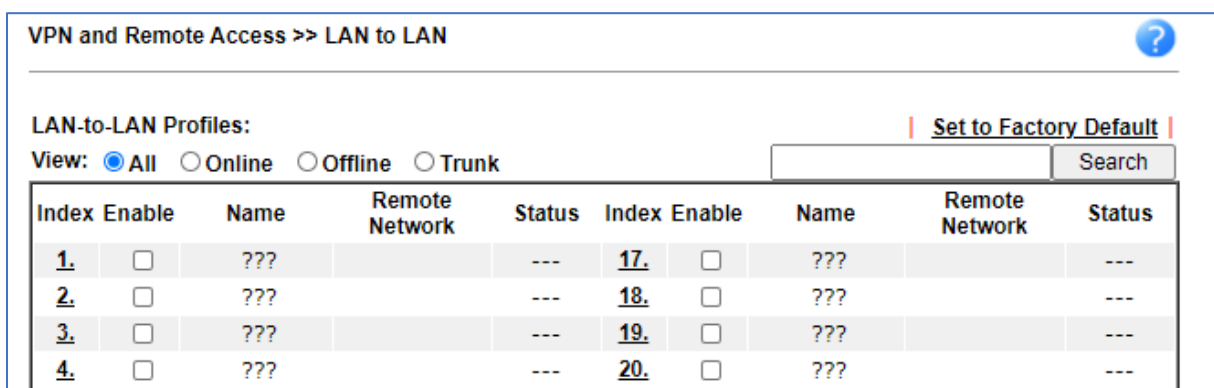
Belangrijk: Indien een DrayTek router reeds achter een bestaand netwerk(NAT) staat zal deze DrayTek de Dial Out verbinding op moeten zetten.

Dial Out (Client) configuratie

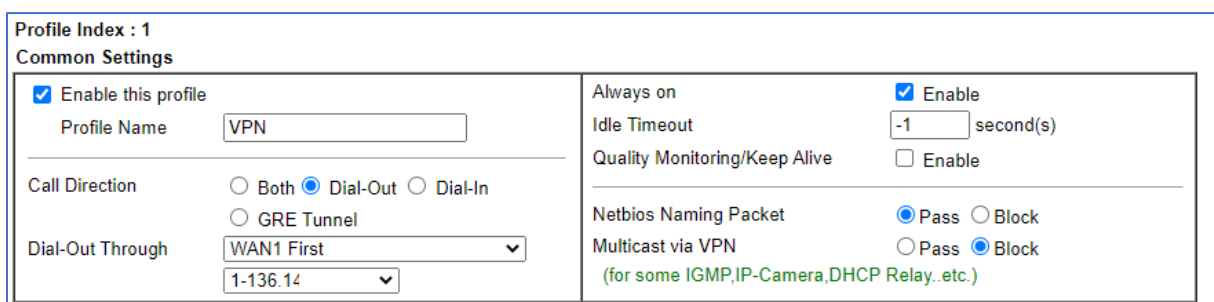
In het hoofdmenu van de DrayTek gaat u naar VPN and Remote Access hier klikt u vervolgens op LAN to LAN.



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.



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.



U gaat daarna naar 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 2865 ontvangt op zijn WAN poort. Let er wel op dat dit een publiek IP-adres of Hostname moet zijn.

Dial-Out Settings	
VPN Server <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel IKEv1 ▼ <input type="radio"/> L2TP with IPsec Policy None ▼ <input type="radio"/> SSL Tunnel <input type="radio"/> Openvpn Tunnel TCP ▼	IKE Phase 1 Settings Mode <input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode Authentication Pre-Shared Key ▼ Pre-Shared Key <input type="text" value="....."/> Local ID <input type="text" value="Max: 47 characters"/> proposal Encryption Auto ▼ proposal ECDH Group G14 ▼ proposal Authentication SHA256 ▼
Server IP/Host Name <input type="text" value="publiek.IP.Vigor.2865"/>	IKE Phase 2 Settings Security Protocol <input checked="" type="radio"/> ESP(High) <input type="radio"/> AH(Medium) Proposal Encryption AES128 ▼ Proposal Authentication All ▼
Dial-Out Schedule Profile <input type="text" value="None"/> <input type="text" value="None"/> <input type="text" value="None"/> <input type="text" value="None"/>	IKE Advanced Settings + Ping to Keep Alive <input type="checkbox"/> Enable

IKE Phase 1 Settings

In de Phase 1 instellingen geeft u de Pre Shared Key op, deze key moet hetzelfde zijn als bij de andere locatie. Daarnaast kun u de proposal Encryption bepalen, advies is om deze op Auto te zetten zodat de VPN server kant bepaald welke Encryptie wordt gebruikt.

IKE Phase 1 Settings	
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
Authentication	Pre-Shared Key ▼
Pre-Shared Key	<input type="text" value="....."/>
Local ID	<input type="text" value="Max: 47 characters"/>
proposal Encryption	Auto ▼
proposal ECDH Group	G14 ▼
proposal Authentication	SHA256 ▼

IKE Phase 2 Settings

In de Phase 2 configureren we het Security Protocol en Proposal, in dit geval kiezen we als security protocol voor ESP (high) en als Encryptie AES128. De Proposal Authentication laten we op All staan.

IKE Phase 2 Settings	
Security Protocol	<input checked="" type="radio"/> ESP(High) <input type="radio"/> AH(Medium)
Proposal Encryption	AES128 ▼
Proposal Authentication	All ▼

IKE Advanced Settings

Eventueel hebt u de mogelijkheid om de Phase 1 en Phase 2 key life times aan te passen. Standaard waarde is 28800 seconden voor Phase 1 en 3600 seconden voor Phase 2. Deze waarde is voor een DrayTek naar DrayTek VPN tunnel de correcte/default waarde. Indien een VPN wordt opgezet naar een ander merk VPN router/firewall kan het zijn dat u deze waardes moet wijzigen.

IKE Advanced Settings ▾	
Phase 1 Key Lifetime	<input type="text" value="28800"/> seconds
Phase 2 Key Lifetime	<input type="text" value="3600"/> seconds
Phase 2 Network ID	<input type="text" value="0.0.0.0"/> (For NAT Mode)
<input type="checkbox"/> Enable Perfect Forward Secret	

Ping to keep alive

Middels Ping to keep alive kunt ervoor zorgen dat er altijd verkeer over de tunnel gaat op basis van een ping. Zorg er in dat geval voor dat het IP-adres in het LAN subnet van de remote vestiging zit en reageert op een ping.

Ping to Keep Alive	<input checked="" type="checkbox"/> Enable
PING Target IP	<input type="text" value="10.0.0.254"/>

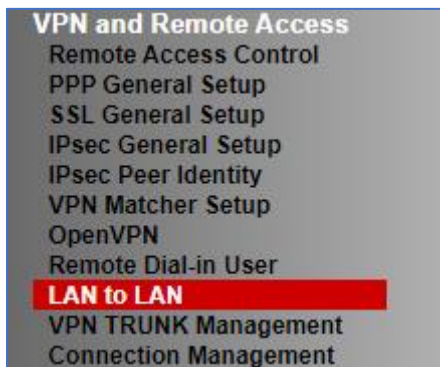
De Tunnel Settings en 6in4 Settings kunt u bij een standaard VPN LAN-to-LAN profiel overslaan.

Ga door naar de TCP/IP Network Settings. Hier geeft u het Remote Network op van de DrayTek Vigor 2865. Dit betreft het LAN subnet van de Vigor 2865. Klik vervolgens op OK om het profiel op te slaan.

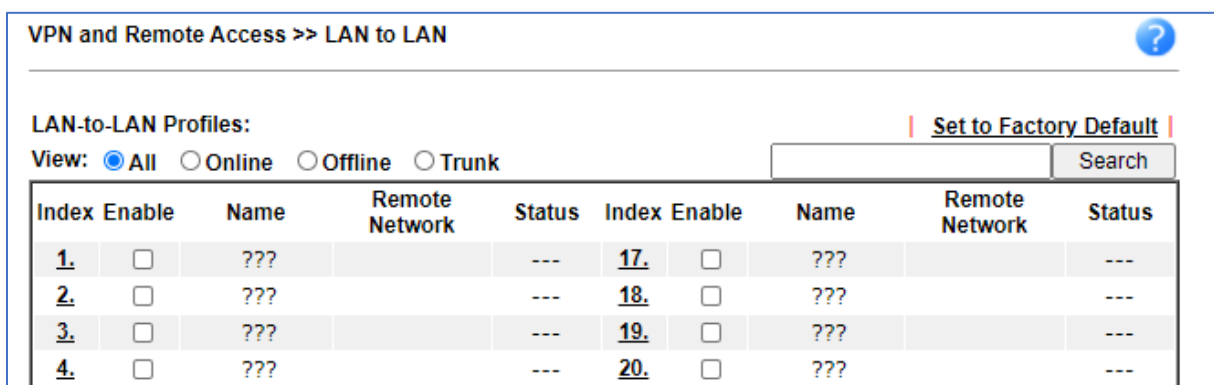
TCP/IP Network Settings	
Local Network IP <input type="text" value="172.31.254.0"/> / Mask <input type="text" value="255.255.255.0 / 24"/>	Mode <input checked="" type="radio"/> Routing <input type="radio"/> NAT
Remote Network IP <input type="text" value="10.0.0.0"/> / Mask <input type="text" value="255.255.255.0 / 24"/>	RIP via VPN <input type="text" value="Disable"/>
More Remote Subnet <input type="button" value="+"/>	Translate Local Network <input type="checkbox"/> Enable
	<input type="checkbox"/> Change Default Route to this VPN tunnel (This only works if there is only one WAN online)

Dial In (Server) instellingen

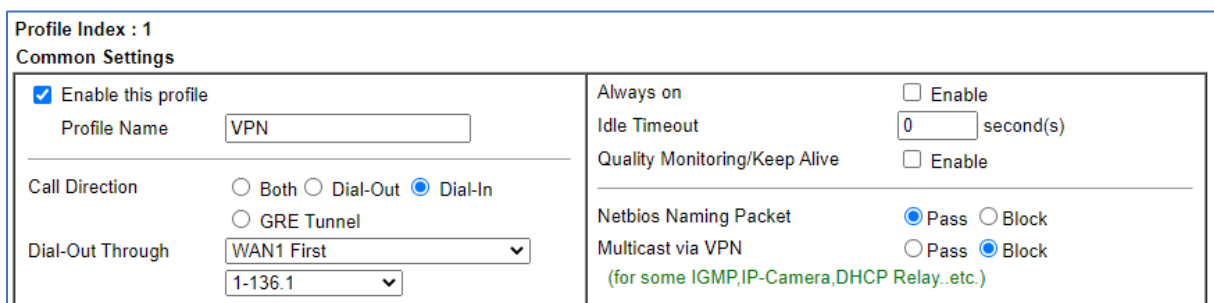
In het hoofdmenu van de DrayTek gaat u naar VPN and Remote Access. Klik vervolgens op LAN to LAN.



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.



U zet als eerste weer een vinkje bij Enable this profile. Hierna selecteert u Dial-In als Call Direction.



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.

Allowed VPN Type

Bij de Dial-In Settings geeft u aan dat het om een IPsec Tunnel(IKEv1/IKEv2) gaat. Zet een vinkje bij Specify Remote VPN Gateway en vul bij Remote IP het publieke IP-adres in van de DrayTek Vigor 2927.

Allowed IKE Authentication Method

Bij de IKE Authentication Method geeft u de Pre-Shared Key op welke tevens is geconfigureerd op de Vigor2927 serie. Deze Pre-Shared Key moet hetzelfde zijn, indien dit niet het geval is zal de VPN tunnel niet online komen.


Allowed IPsec Security Method

Hier geeft u aan welke security methode gebruikt mag worden. Belangrijk is dat beide locaties gebruik maken van dezelfde security methode, in dit geval zorgen we ervoor dat minimaal ESP-AES is geselecteerd.

Dial-In Settings	
Allowed VPN Type <ul style="list-style-type: none"><input type="checkbox"/> PPTP<input checked="" type="checkbox"/> IPsec Tunnel(IKEv1/IKEv2)<input type="checkbox"/> IPsec XAuth<input type="checkbox"/> L2TP with IPsec Policy None ▾<input type="checkbox"/> SSL Tunnel<input type="checkbox"/> Openvpn Tunnel	Username <input type="text" value="???"/> Password <input type="text" value="Max: 128 characters"/>
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Remote IP <input type="text" value="IP.Vigor.2927"/> Peer ID <input type="text" value="Max: 128 characters"/> Local ID <input type="text" value="Max: 47 characters"/>	PPP Advanced Settings + Openvpn Advanced Settings + Allowed IKE Authentication Method <ul style="list-style-type: none"><input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="....."/><input type="checkbox"/> X.509 Digital Signature None ▾Preferred Local ID Alternative Subject Name ▾
	Allowed IPsec Security Method <input checked="" type="checkbox"/> AH <input checked="" type="checkbox"/> ESP-DES <input checked="" type="checkbox"/> ESP-3DES <input checked="" type="checkbox"/> ESP-AES

Geef bij Remote Network het LAN IP Subnet op van de DrayTek Vigor 2927.

TCP/IP Network Settings	
Local Network IP <input type="text" value="10.0.0.0"/> / Mask <input style="border: none; border-bottom: 1px solid black;" type="text" value="255.255.255.0 / 24"/>	Mode <input checked="" type="radio"/> Routing <input type="radio"/> NAT RIP via VPN <input style="border: none; border-bottom: 1px solid black;" type="text" value="Disable"/>
Remote Network IP <input type="text" value="172.31.254.0"/> / Mask <input style="border: none; border-bottom: 1px solid black;" type="text" value="255.255.255.0 / 24"/>	Translate Local Network <input type="checkbox"/> Enable
More Remote Subnet +	<input type="checkbox"/> Change Default Route to this VPN tunnel (This only works if there is only one WAN online)



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.