

DrayTek

WireGuard VPN
LAN-to-LAN



Inhoudsopgave

WireGuard	3
DrayTek VPN server setup	4
DrayTek VPN client setup	6

WireGuard

WireGuard is een veilig, snel en modern VPN-protocol. Een WireGuard VPN-verbinding wordt gemaakt door het uitwisselen van openbare sleutels. W

Dit artikel laat zien hoe u een WireGuard VPN LAN-to-LAN tunnel kunt opzetten tussen twee DrayTek Vigor routers.

Belangrijk is dat beide DrayTek producten een publiek / internet IP-adres hebben op de WAN poort. Indien een DrayTek router achter een bestaande NAT omgeving staat, kan dit problemen opleveren met VPN.

Controleer daarnaast of WireGuard als VPN protocol reeds is ingeschakeld op de DrayTek. Dit kan onder VPN and Remote Access >> Remote Access Control, na inschakelen dient de DrayTek een herstart te krijgen.

VPN and Remote Access >> Remote Access Control

Remote Access Control Setup	Bind to WAN
<input 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	
<input type="checkbox"/> Enable OpenVPN Service	
<input checked="" type="checkbox"/> Enable WireGuard VPN Service	

Note:

1. To allow VPN pass-through to a separate VPN server on the LAN, disable the services listed above that use the same protocol and ensure that NAT **Open Ports** or **Port Redirection** is well-configured.
2. Disable unused VPN services, enable **Brute Force Protection**, and **block unknown IP access** to the used VPN services to reduce Cyberattacks.

WireGuard maakt gebruik van poort 51820. Deze poort moet bereikbaar zijn voor de VPN client. Eventueel is deze poort te wijzigen.



DrayTek VPN server setup

Creëer in de DrayTek router een nieuw LAN-to-LAN VPN profiel, welke als Dial-In (VPN server) fungeert. Hierbij is het belangrijk om onderstaande instellingen te gebruiken.

Enable this profile: Inschakelen om het VPN profiel te activeren.

Call Direction: Selecteer Dial-In.

Idle Timeout: Bepaalt na hoeveel seconden van in-activiteit de VPN tunnel wordt verbroken. Advies is deze te wijzigen naar 0 seconden.

Allowed VPN type: Selecteer WireGuard.

VPN and Remote Access >> LAN to LAN	
Profile Index : 1	
Common Settings	
<input checked="" type="checkbox"/> Enable this profile	Always on <input type="checkbox"/> Enable
Profile Name <input type="text" value="WGServer"/>	Idle Timeout <input type="text" value="0"/> second(s)
Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-In	Quality Monitoring/Keep Alive <input type="checkbox"/> Enable
<input type="radio"/> GRE Tunnel	Netbios Naming Packet <input type="radio"/> Pass <input checked="" type="radio"/> Block
Dial-Out Through <input type="text" value="WAN1 First"/>	Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)
<input type="text" value="1-118.166.196.203"/>	
Dial-In Settings	
Allowed VPN Type	Username <input type="text" value="???"/> Password <input type="text" value="Max: 128 characters"/>
<input type="checkbox"/> PPTP	PPP Advanced Settings +
<input type="checkbox"/> IPsec Tunnel(IKEv1/IKEv2)	OpenVPN Advanced Settings -
<input type="checkbox"/> IPsec XAuth	Cipher Algorithm <input type="text" value="AES256-CBC"/>
<input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="Must"/>	HMAC Algorithm <input type="text" value="SHA256"/>
<input type="checkbox"/> SSL Tunnel	
<input type="checkbox"/> OpenVPN Tunnel	
<input checked="" type="checkbox"/> WireGuard	

Na het selecteren van WireGuard als Allowed VPN type krijgt u een pop-up scherm te zien, waarin u de Private en Public keys kunt genereren. Klik op **Generate a Key Pair**, de Public Key dient u vervolgens te kopiëren. De Public Key dient u leeg te laten, deze kan pas ingevuld worden nadat ook de VPN client omgeving is geconfigureerd.

Selecteer **Generate** om een Pre-Shared Key te genereren en kopieer deze samen met de Public Key in bijvoorbeeld Kladblok/notepad.

WireGuard Settings:	
[Interface]	
Private Key <input type="text" value="SKmGb74xQtDiwPcxcGm4WCNVzqB92bFaj8UI+R7FXGQ="/> <input type="button" value="Generate a Key Pair"/>	
Public Key <input type="text" value="JlImHP5hVzB9XxX7wn1ucUoS1sAYgfg/iz5u/SIsagB0="/> <input type="button" value="Copy to Clipboard"/>	
[Peer]	
Public Key <input type="text"/>	
Pre-Shared Key <input type="text" value="cCp9VG45YU/gI/LHTEGpfJ5H4HR5ZLqcgQ/hBM7PxmM="/> <input type="button" value="Generate"/>	
Client IP Address <input type="text" value="0.0.0.0"/> (For NAT Mode)	
Keepalive <input type="text" value="0"/> seconds	

Bij Local Network geeft u het LAN subnet op van de VPN server omgeving en bij Remote Network het LAN subnet van de VPN client omgeving. Sla het VPN profiel vervolgens op door op OK te klikken.

TCP/IP Network Settings	
Local Network IP <input type="text" value="192.168.62.2"/> / Mask <input type="text" value="255.255.255.0 / 24"/> <input type="button" value="v"/>	Mode <input checked="" type="radio"/> Routing <input type="radio"/> NAT
Remote Network IP <input type="text" value="192.168.177.0"/> / Mask <input type="text" value="255.255.255.0 / 24"/> <input type="button" value="v"/>	RIP via VPN <input type="text" value="Disable"/> <input type="button" value="v"/>
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)

DrayTek VPN client setup

Bij de VPN client omgeving dient u tevens een VPN LAN-to-LAN profiel aan te maken, welke als Dial-Out profiel fungeert. Dit profiel zal de VPN tunnel initiëren.

Onderstaande instellingen zijn verder belangrijk bij het Dial-Out profiel:

VPN server: Selecteer WireGuard.

Server IP/Host Name: Geef het publiek/internet IP-adres of domeinnaam op van de VPN server omgeving.

Generate a Key Pair: Genereer een Private en Public Key, de Public Key dient u te kopiëren. Deze is nodig in het VPN profiel op de VPN server omgeving.

De Public Key en Pre-Shared Key die u op de VPN server omgeving heeft aangemaakt, dient u nu te kopiëren en plakken in dit VPN profiel onder [peer].

Profile Index : 15	
Common Settings	
<input checked="" type="checkbox"/> Enable this profile	Always on <input type="checkbox"/> Enable
Profile Name <input type="text" value="WireGuardClient"/>	Idle Timeout <input type="text" value="300"/> second(s)
Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In	Quality Monitoring/Keep Alive <input type="checkbox"/> Enable
<input type="radio"/> GRE Tunnel	Netbios Naming Packet <input type="radio"/> Pass <input checked="" type="radio"/> Block
Dial-Out Through <input type="text" value="WAN1 First"/>	Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)
Dial-Out Settings	
VPN Server	WireGuard Settings:
<input type="radio"/> PPTP	[Interface]
<input type="radio"/> IPsec Tunnel <input type="text" value="IKEv1"/>	Private Key <input type="text" value="MIUfoUa3hq9CVnf59V0+VQuk4/F6ShtIP25m1f2nyEs="/> <input type="button" value="Generate a Key Pair"/>
<input type="radio"/> L2TP with IPsec Policy <input type="text" value="Must"/>	Public Key <input type="text" value="Vd10i2qHXewycU49+qTVsvuS4Cb9CZvvqGmXQcJNPTY="/> <input type="button" value="Copy to Clipboard"/>
<input type="radio"/> SSL Tunnel	Address <input type="text" value="0.0.0.0"/> (For NAT Mode)
<input type="radio"/> OpenVPN Tunnel <input type="text" value="TCP"/>	[Peer]
<input checked="" type="radio"/> WireGuard	Public Key <input type="text" value="J1mHP5hVzB9XX7wn1ucUoS1sAYgfg/iz5u/SIsagB0="/> <input type="button" value="Generate"/>
Server IP/Host Name <input type="text"/> : Port <input type="text" value="51820"/>	Pre-Shared Key <input type="text" value="cCp9VG45YU/gI/LHTEGpfJ5H4HR5ZLqcgQ/hBM7PxmM="/> <input type="button" value="Generate"/>
	Keepalive <input type="text" value="0"/> seconds

Bij Local Network geeft u het LAN subnet op van de VPN server omgeving en bij Remote Network het LAN subnet van de VPN client omgeving. Sla het VPN profiel vervolgens op door op OK te klikken.

TCP/IP Network Settings	
Local Network	Mode <input checked="" type="radio"/> Routing <input type="radio"/> NAT
IP <input type="text" value="192.168.177.1"/> / Mask <input type="text" value="255.255.255.0 / 24"/>	RIP via VPN <input type="text" value="Disable"/>
Remote Network	<input type="checkbox"/> Change Default Route to this VPN tunnel (This only works if there is only one WAN online)
IP <input type="text" value="192.168.62.0"/> / Mask <input type="text" value="255.255.255.0 / 24"/>	
More Remote Subnet <input type="checkbox"/>	

Als laatste stap dient u op de VPN server omgeving de Public Key op te geven die u zojuist heeft aangemaakt in de VPN client omgeving. Klik op **OK** om de instellingen op te slaan.

WireGuard Settings:

[Interface]

Private Key: SKmGb74xQtDiwPcxcGm4WCNVzqB92bFaj8UI+R7FXGQ= Generate a Key Pair

Public Key: J1mHP5hVzB9XxX7wn1ucUoS1sAYgfg/iz5u/SIsagB0= Copy to Clipboard

[Peer]

Public Key: Vd10i2qHXewycU49+qTVsvuS4Cb9CZvvqGmXQCjNPTY= ←

Pre-Shared Key: cCp9VG45YU/gI/LHTEGpfJ5H4HR5ZLqcgQ/hBM7PxmM= Generate

Client IP Address: 0.0.0.0 (For NAT Mode)

Keepalive: 0 seconds

Indien alle instellingen correct zijn uitgevoerd zal de VPN tunnel online komen wanneer u op **Dial** klikt onder Connection Management.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh

General Mode: (WireGuardClient) vivian2960.r 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)	Up Time	
1	LAN-to-LAN VPN	192.168.62.2	192.168.62.0/24	0	0	284	248	0:24:24	Drop
2	WireGuard	192.168.62.2	192.168.62.0/24	10	336	10	368	0:0:22	Drop

No subpaging No auto refreshing

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

Een test op basis van Ping zal dit bevestigen.

```
CA Command Prompt
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Wivian>ping 192.168.62.2

Pinging 192.168.62.2 with 32 bytes of data:
Reply from 192.168.62.2: bytes=32 time=22ms TTL=254
Reply from 192.168.62.2: bytes=32 time=20ms TTL=254
Reply from 192.168.62.2: bytes=32 time=20ms TTL=254
Reply from 192.168.62.2: bytes=32 time=20ms TTL=254

Ping statistics for 192.168.62.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 22ms, Average = 20ms

C:\Users\Wivian>
```

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

© 2024 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden vervoelvoudigd, 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.