

DrayTek

DrayOS5
WireGuard VPN - macOS



Inhoudsopgave

- WireGuard 3
- DrayTek General setup 4
 - Default key pairs 4
 - Listen on interface 4
 - VPN Access List 5
 - Brute Force Protection 5
- Teleworker VPN settings 6
 - General 7
 - User Information 7
 - Teleworker VPN 8
 - WireGuard Settings 9
 - Local IP Assignment 9
- macOS setup 10
 - Add New Tunnel 10
- WireGuard Tunnel activeren 12
- Export WireGuard configuratie 12

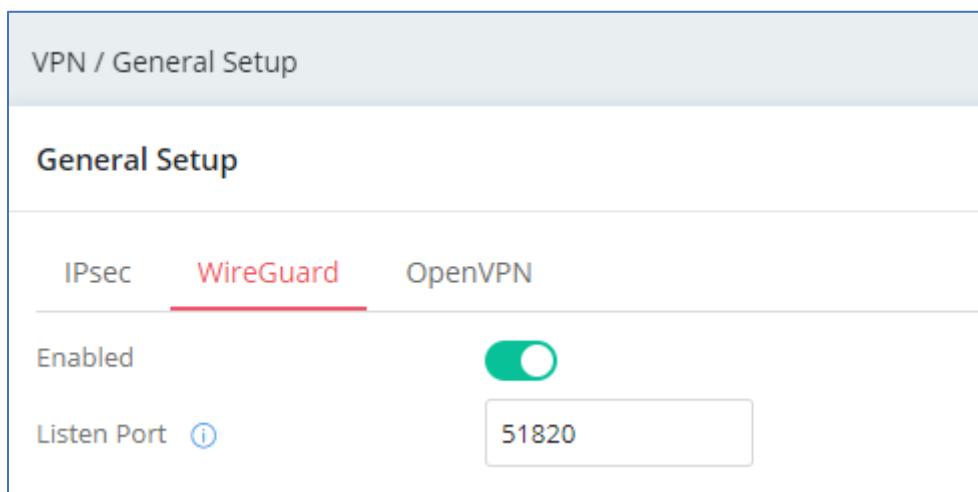
WireGuard

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

Dit artikel laat zien hoe u een WireGuard VPN-tunnel tot stand kunt brengen tussen de DrayTek Vigor2136 en de WireGuard VPN Client software op macOS.

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

Controleer daarnaast of WireGuard als VPN protocol is ingeschakeld op de DrayTek. Dit kan onder VPN >> General Setup.



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



DrayTek General setup

Default key pairs

Om gebruik te maken van een WireGuard VPN tunnel dient u een default key pair te genereren. Deze private en public key zijn uniek. De WireGuard VPN-clients hebben de public key van de Vigor-router nodig om het WireGuard VPN-profiel aan te maken.

Default Key Pairs

Private Key

Generate Private Key

Public Key

Listen on interface

Deze instelling bepaalt welke WAN interface één of meerdere VPN-verbindingen zal accepteren. Standaard zal elke WAN interface reageren op een VPN verzoek vanaf het internet. U kunt zelf bepalen aan welke WAN interface, IPv4 adres en/of welk VPN protocol u toestaat.

In onderstaand voorbeeld wordt enkel het WireGuard VPN protocol toegestaan op de WAN1 interface.

Listen on Interface

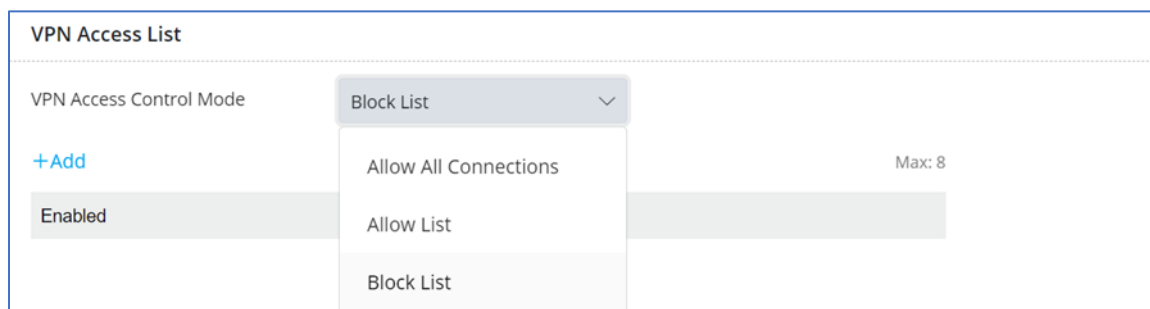
Accept VPN Connections on All Interfaces Specified Interface

[+Add](#) Max: 8

WAN	IPv4 Address	Allowed VPN Protocols	Option
<input type="text" value="[WAN] WAN1 ()"/>	<input type="text" value="Default WAN IP"/>	<input type="text" value="WireGuard"/>	<input type="button" value="Delete"/>

VPN Access List

Selecteer de vereiste VPN-toegangscontrolemodus. Standaard staat de Vigor-router VPN verbindingen toe vanaf alle externe IP-adressen. Gebruik de blocklist of allow list om specifieke IP-adressen toe te staan of te blokkeren. Hiervoor dient u objecten aan te maken in het menu Configuration > Objects.



VPN Access List

VPN Access Control Mode

+Add

Enabled

Block List

Allow All Connections

Allow List

Block List

Max: 8

Brute Force Protection

Geef het maximale aantal mislukte VPN-inlogpogingen op en de periode voor het blokkeren van toegang nadat de drempel is bereikt.

In onderstaand voorbeeld zal er een penalty (blokkade) volgen wanneer een client zich 3 keer foutief probeert aan te melden middels VPN. Het externe IP-adres van deze client wordt op de block list gezet voor een duur van 600 seconden.



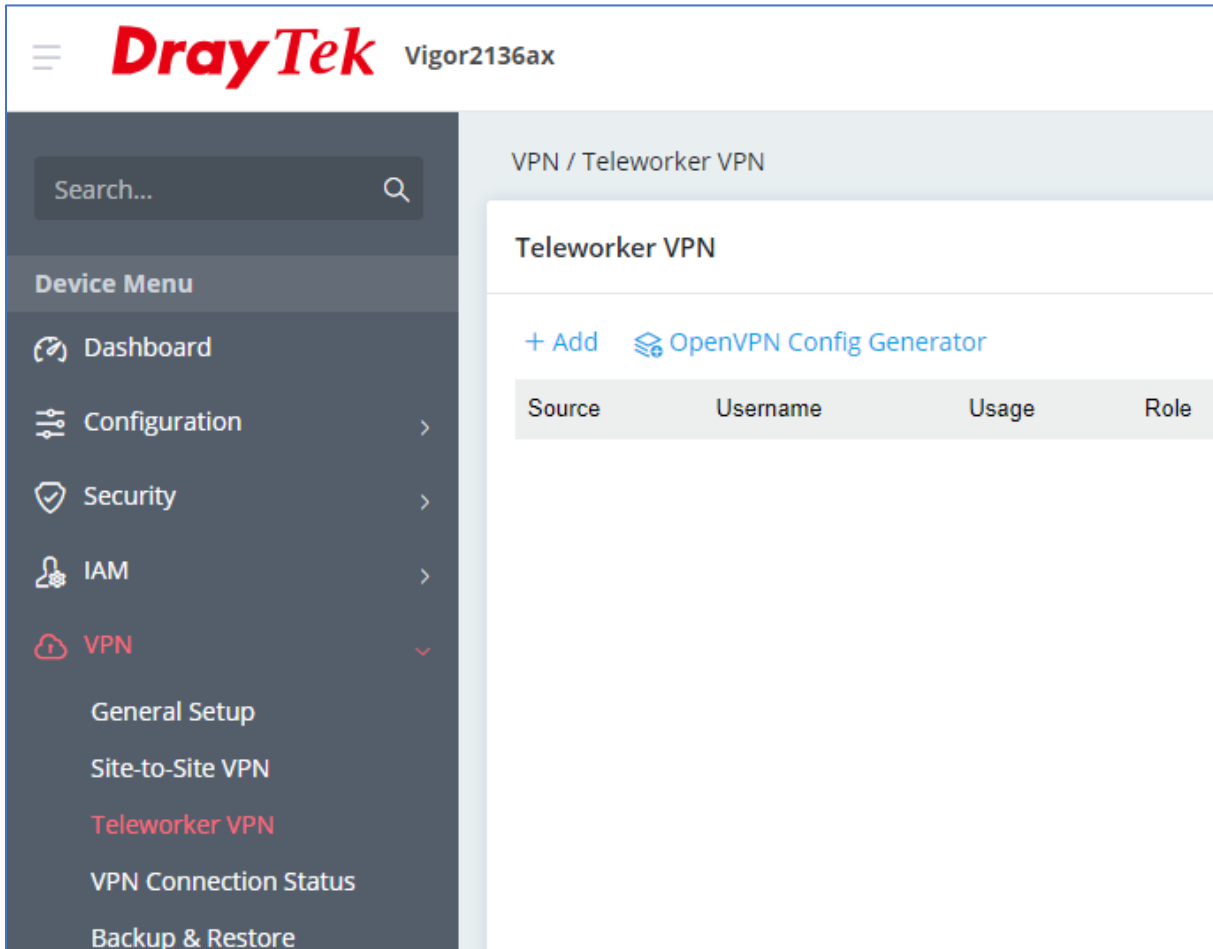
Brute Force Protection

Maximum VPN Login Failures (times) 3

Penalty Period (seconds) 600

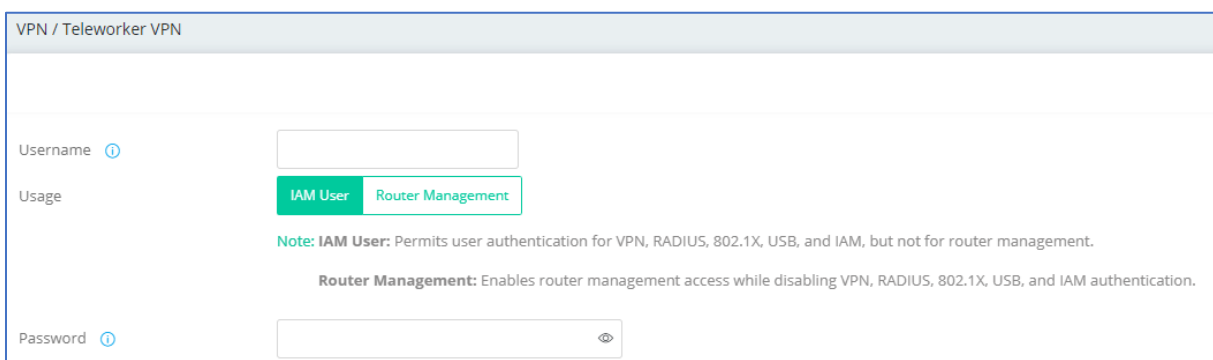
Teleworker VPN settings

Voor het aanmaken van een VPN account kunt u bij Teleworker VPN een nieuw account toevoegen om op + Add te klikken.



The screenshot shows the DrayTek Vigor2136ax web interface. The top navigation bar includes the DrayTek logo and the device model Vigor2136ax. A left sidebar menu is visible with options: Dashboard, Configuration, Security, IAM, VPN (highlighted), General Setup, Site-to-Site VPN, Teleworker VPN, VPN Connection Status, and Backup & Restore. The main content area is titled 'VPN / Teleworker VPN' and contains a 'Teleworker VPN' section with a '+ Add' button and an 'OpenVPN Config Generator' link. Below this is a table with columns: Source, Username, Usage, and Role.

Geef vervolgens een username en password op, selecteer IAM user om gebruik te kunnen maken van VPN.



The screenshot shows the configuration form for a Teleworker VPN user. It includes the following fields and options:

- Username:** A text input field.
- Usage:** Two radio button options: **IAM User** (selected) and **Router Management**.
- Note:** IAM User: Permits user authentication for VPN, RADIUS, 802.1X, USB, and IAM, but not for router management.
- Note:** Router Management: Enables router management access while disabling VPN, RADIUS, 802.1X, USB, and IAM authentication.
- Password:** A text input field with a toggle icon to show/hide the password.

General

Naast het in en uitschakelen van een VPN profiel kunt u hier tevens een group policy koppelen aan het VPN account. Daarnaast kunt u een verval datum koppelen aan het VPN profiel. De Group Policy kunt u verder inrichten in het IAM menu, raadpleeg hiervoor de IAM handleiding op onze website voor meer informatie.

Status	Active	▼
Group Policy	None	▼
Expiration Time	Never	▼

User Information

Per gebruikers account kunt u e-mail adres of 06-nummer achterlaten. Deze informatie kan gebruikt worden wanneer u gebruik maakt van MFA. Indien u hier gebruik van wilt maken dient u een koppeling te hebben met een SMTP server of SMS provider, verder configuratie is mogelijk onder Configuration > Notification Services.

User Information	
Enable Email	<input checked="" type="checkbox"/>
Email	<input type="text"/>
	<input checked="" type="checkbox"/> Send Email Notification to the newly created User
Enable SMS	<input checked="" type="checkbox"/>
SMS	<input type="text"/>

Teleworker VPN

Hier activeert u het VPN profiel voor dit account, daarnaast kunt u hier aangeven welke VPN protocollen gebruikt kunnen worden om een VPN tunnel op te bouwen. We selecteren in dit geval enkel WireGuard.

General **Teleworker VPN**

General

Enable Teleworker VPN

Idle Timeout (Seconds) ⓘ

VPN Schedule Always On Scheduled On

Download SmartVPN Client [Download SmartVPN Client](#)

Allowed VPN Protocols

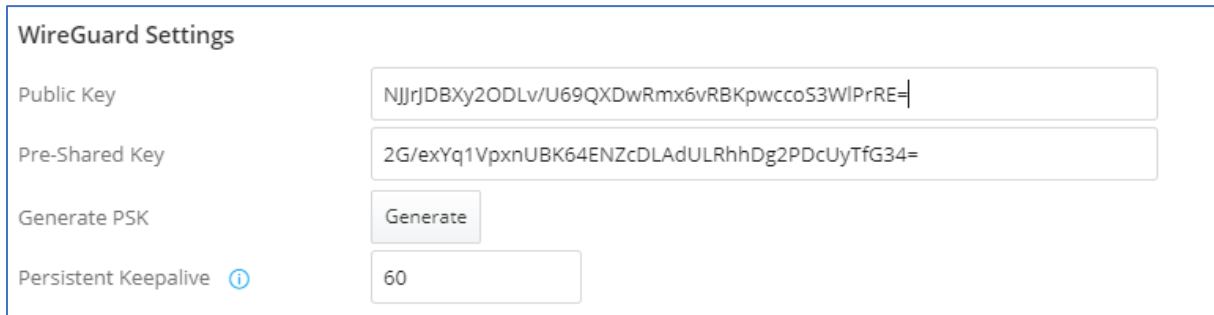
Enable IPsec

Enable WireGuard

Enable OpenVPN

WireGuard Settings

De beheerder moet aan de gebruiker van de client vragen om de public key te verstrekken via de WireGuard VPN-client (door een lege tunnel toe te voegen). De public key die hier wordt getoond, moet vervolgens worden overgenomen in de WireGuard-instellingen op de DrayTek-router. Op pagina 10 ziet u de public key van de VPN client, deze hebben we overgenomen in onderstaand screenshot.

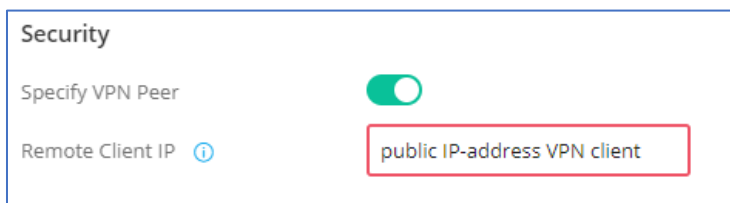


The screenshot shows the 'WireGuard Settings' configuration page. It includes the following fields and controls:

- Public Key:** A text input field containing the value: `NJjrjDBXy2ODLv/U69QXDwRmx6vRBKpwccoS3WIPrRE=`
- Pre-Shared Key:** A text input field containing the value: `2G/exYq1VpxnUBK64ENZcDLAdULRhhDg2PDcUyTfG34=`
- Generate PSK:** A button labeled 'Generate'.
- Persistent Keepalive:** A text input field with a value of '60' and an information icon.

Klik daarnaast op "Generate" om een Pre-Shared Key te genereren. Deze Pre-Shared Key is nodig op de VPN-client om de VPN-tunnel op te kunnen bouwen.

Bij de Security instellingen hebt u ook de mogelijkheid om de locatie van de VPN-peer te specificeren door het publieke IP-adres van de VPN-client op te geven. Hierdoor is het alleen mogelijk om vanaf deze specifieke locatie een VPN-tunnel op te zetten naar de DrayTek. Als dit IP-adres echter voortdurend verandert, is het beter om deze optie uitgeschakeld te laten.

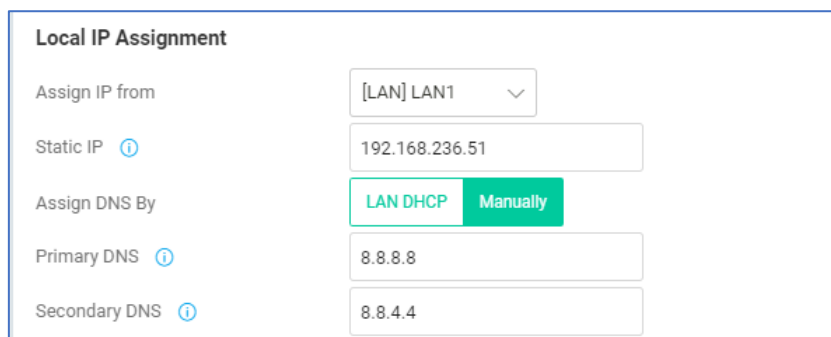


The screenshot shows the 'Security' configuration page. It includes the following controls:

- Specify VPN Peer:** A toggle switch that is currently turned on (green).
- Remote Client IP:** A text input field containing the value: `public IP-address VPN client`, which is highlighted with a red border.

Local IP Assignment

Bij Local IP Assignment dient u de VPN client een vast IP-adres geven. Welke zich bevindt in een bestaand LAN netwerk van de DrayTek.

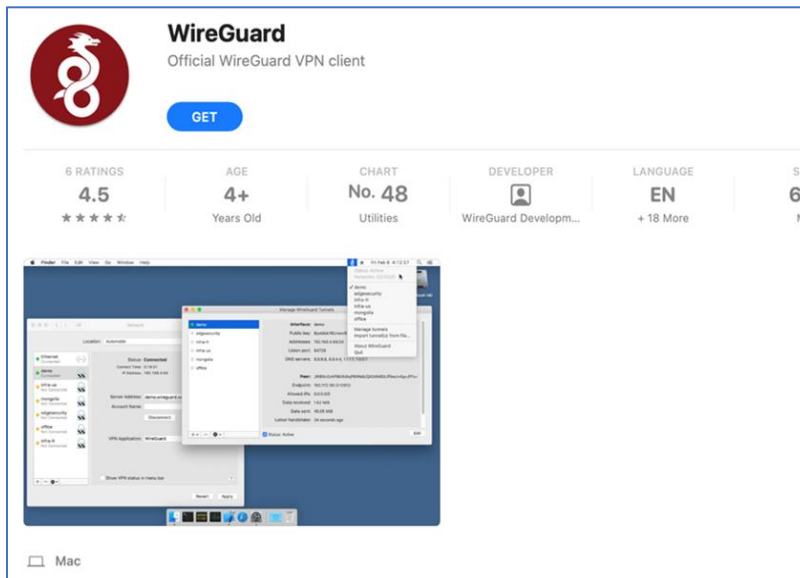


The screenshot shows the 'Local IP Assignment' configuration page. It includes the following fields and controls:

- Assign IP from:** A dropdown menu with the selected option: `[LAN] LAN1`.
- Static IP:** A text input field containing the value: `192.168.236.51`.
- Assign DNS By:** Two radio buttons: `LAN DHCP` (selected) and `Manually`.
- Primary DNS:** A text input field containing the value: `8.8.8.8`.
- Secondary DNS:** A text input field containing the value: `8.8.4.4`.

macOS setup

Open op uw macOS apparaat de App Store om hier de WireGuard app te installeren.



Add New Tunnel

Open de WireGuard app en klik op + Add Empty Tunnel. Geef het profiel een naam en kopieer de public key, deze dient u over te nemen in de DrayTek zoals op de vorige pagina is besproken.

Name:

Public key:

On-Demand: Ethernet Wi-Fi

[Interface]
PrivateKey = +BgsCz3qVbdLLkZ7dOeZtjS5g8FVayVn9ZZXrFMadn8=

Voeg de volgende configuratie regels toe aan de WireGuard configuratie.

[Interface]

PrivateKey = ONsQUBPPKdCdKRWFph55zFtci4eBQD85ID50nNfSRnQ=

Address = 192.168.236.51/32

DNS = 8.8.8.8, 8.8.4.4

MTU = 1400

[Peer]

PublicKey = mscSc6Hkzk0tHQz7stM1b61BxPhDOVNEww/cQjixI0U=

PresharedKey = UDvehtiA2gP1HMrd/NZ5g/6lx5OdmHwLMW4mDIJ/Xc=

AllowedIPs = LAN subnet van de DrayTek/24

Endpoint = WAN IP-adres of hostname:51820

PersistentKeepalive = 60

Uitleg van de verschillende configuratie regels:

[Interface]	de instellingen van de WireGuard VPN-client.
Address	het statische IP-adres dat de VPN-server heeft geconfigureerd voor de client.
DNS	verwijst naar het gespecificeerde IP-adres van de DNS-server.
MTU	de MTU (Maximum Transmission Unit) van deze WireGuard VPN-verbinding.
[Peer]	de instellingen van de WireGuard VPN-server.
Public Key	De Peer Public Key is de openbare sleutel van de Vigor2136. Deze kan worden gevonden bij de VPN General Setup pagina.
PresharedKey	De PresharedKey-instelling bevindt zich in het Teleworker VPN-profiel
AllowedIPs	het LAN netwerk waartoe de WireGuard VPN-client toegang heeft. Voeg "0.0.0.0/1" en "128.0.0.0/1" toe als de gebruiker de WireGuard VPN als standaardgateway wil gebruiken.
Endpoint	is het IP-adres of de domeinnaam van de WireGuard VPN-server.

WireGuard Tunnel activeren

Als het profiel correct is ingevoerd, kunt u het activeren door op "Activeren" te klikken. De WireGuard-tunnel wordt opgebouwd als alle instellingen (zoals public keys, pre-shared key) succesvol zijn geconfigureerd, zoals te zien is in onderstaande afbeelding.

Na activering is het mogelijk om lokale apparaten, zoals het LAN IP-adres van de DrayTek, te benaderen.

Export WireGuard configuratie

Wanneer de VPN-tunnel is opgezet en online is, kunt u het profiel exporteren om het mogelijk op andere clients en/of VPN-software te laden, zoals de Smart VPN Client van DrayTek.

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 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.