

DrayTek

DrayOS5
IPsec – Smart VPN Client



Inhoudsopgave

| | |
|------------------------------------|----|
| IPsec Teleworker | 3 |
| IPsec Protocol..... | 4 |
| Teleworker VPN instellingen | 5 |
| General | 6 |
| User Information | 6 |
| Teleworker VPN..... | 7 |
| Security..... | 7 |
| Local IP Assignment..... | 8 |
| Smart VPN Client setup | 9 |
| Smart VPN client configuratie..... | 10 |
| VPN profiel toevoegen..... | 11 |
| VPN ping controle..... | 13 |
| VPN Connection Status | 13 |

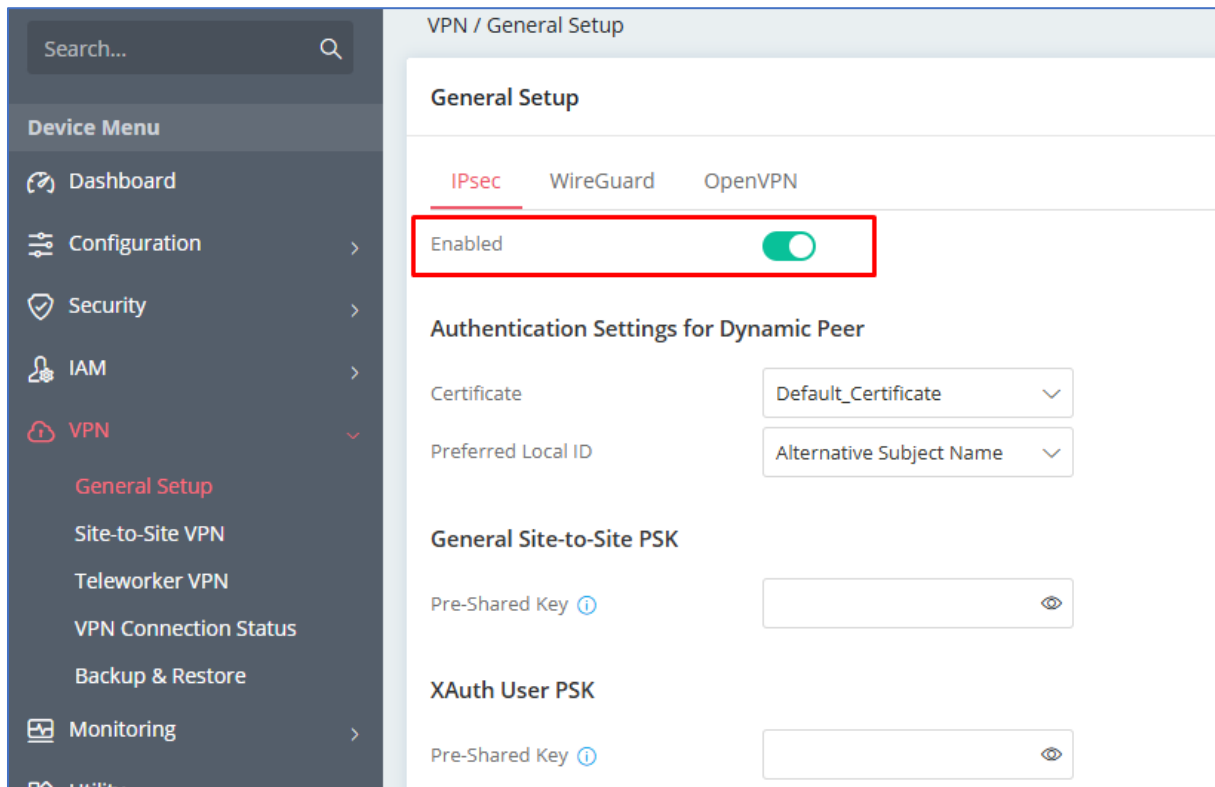
IPsec Teleworker

IPsec is een VPN-protocol waarmee thuiswerkers veilig verbinding kunnen maken met het bedrijfsnetwerk via het internet. Met behulp van het IPsec-protocol, dat encryptie en authenticatie biedt, kunnen thuiswerkers een beveiligde tunnel opzetten tussen hun apparaat (zoals een laptop) en het bedrijfsnetwerk. Dit zorgt ervoor dat gegevens die tussen beide eindpunten worden verzonden, beschermd zijn tegen onderschepping en ongeautoriseerde toegang. IPsec maakt gebruik van UDP 500 & 4500, indien de DrayTek geen publiek IP-adres op de WAN poort ontvangt dient u ervoor te zorgen dat deze poorten open staan naar het WAN IP-adres van de DrayTek.

Dit artikel demonstreert hoe u een DrayOS 5 Vigor Router configureert als een VPN-server voor IPsec clients, en welke configuratie vereist is op Windows om de VPN op te zetten. In het voorbeeld wordt de Vigor2136 router gebruikt. Als VPN client wordt de Smart VPN Client van DrayTek gebruikt, deze client is gratis te downloaden op <https://www.draytek.nl/support/>

IPsec Protocol

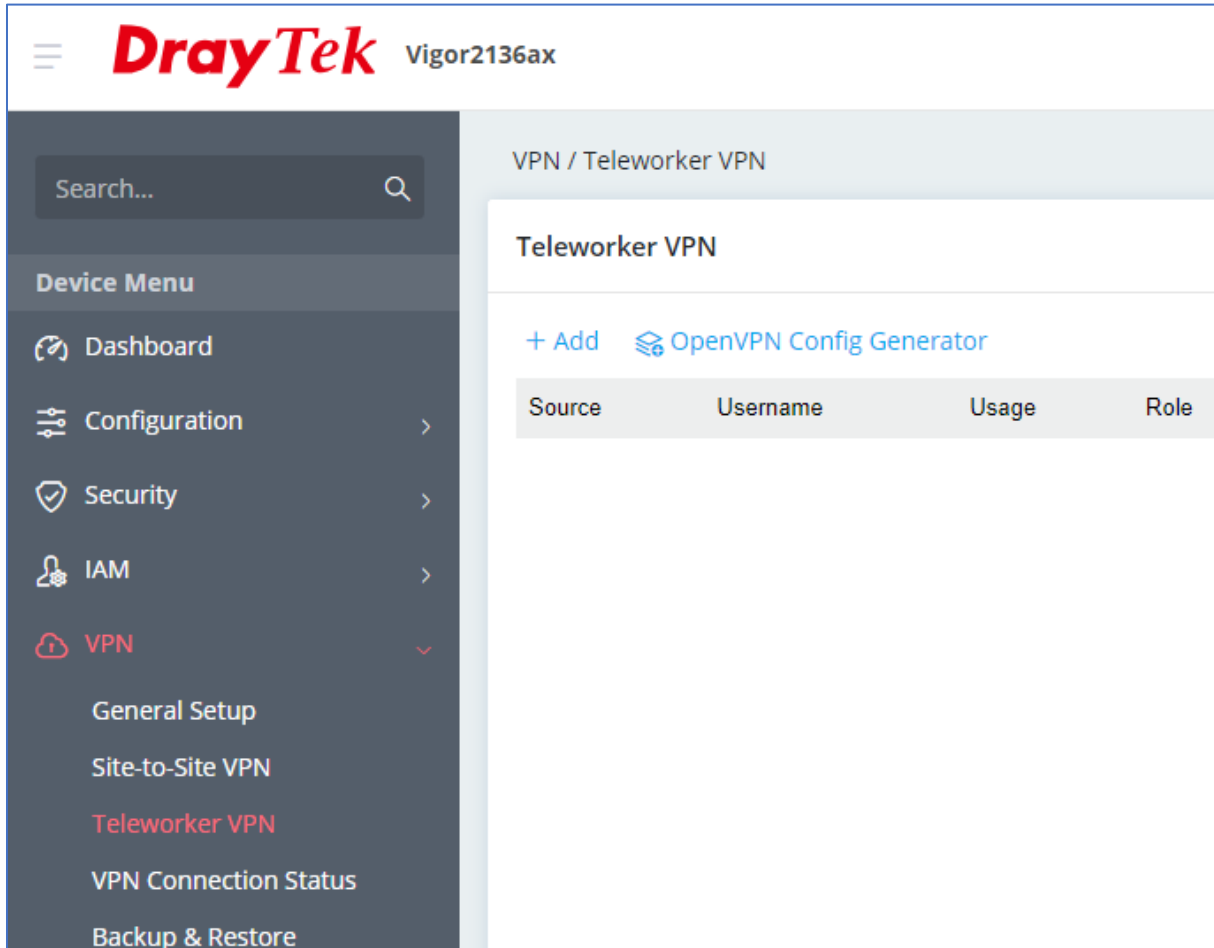
Alle VPN protocollen staan in een default configuratie uit. Zorg er daarom eerst voor dat IPsec VPN wordt aangezet onder **“VPN / General Setup”**. Zet het vinkje onder IPsec op Enable en klik onderaan op Apply.



The screenshot shows the 'VPN / General Setup' configuration page. On the left is a 'Device Menu' with options like Dashboard, Configuration, Security, IAM, VPN, and Monitoring. The 'VPN' menu item is expanded, showing 'General Setup' as the selected option. The main content area is titled 'VPN / General Setup' and has three tabs: 'IPsec', 'WireGuard', and 'OpenVPN'. The 'IPsec' tab is active and highlighted with a red box. Below the tabs, there is a toggle switch labeled 'Enabled' which is turned on (green). Underneath, there are sections for 'Authentication Settings for Dynamic Peer' with dropdown menus for 'Certificate' (Default_Certificate) and 'Preferred Local ID' (Alternative Subject Name). There are also sections for 'General Site-to-Site PSK' and 'XAuth User PSK', each with a 'Pre-Shared Key' input field and a toggle for visibility.

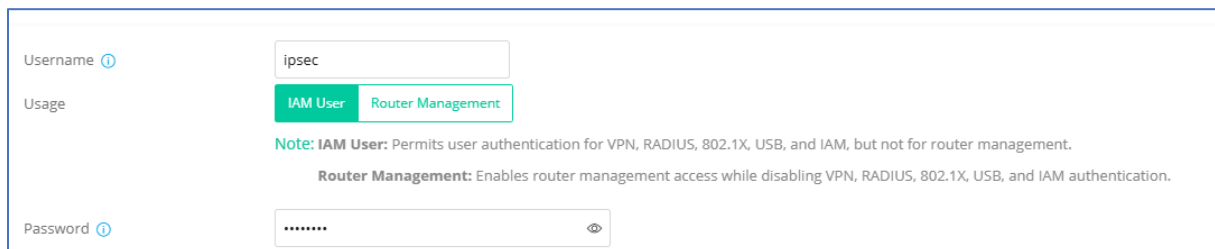
Teleworker VPN instellingen

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



The screenshot shows the DrayTek Vigor2136ax web interface. The left sidebar contains a 'Device Menu' 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 shows 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 VPN user. It includes the following fields and options:

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

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 type="checkbox"/> |
| Enable SMS | <input type="checkbox"/> |

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 IPsec IKEv1/v2.

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

IPsec

IKEv1/v2 EAP XAuth

Note: For IKEv1/v2, enable specify VPN peer with static IP and PSK to establish the identity and secure connection.

OpenVPN

WireGuard

Security

Vanwege Zero Trust is het verplicht om onder Security het WAN IP-adres van de VPN client een eigen Pre-Shared Key te geven. Deze Pre-Shared Key werkt alleen als de VPN-client verbinding probeert te maken vanaf het opgegeven Remote Client IP-adres.

Opmerking: Wanneer het Remote Client IP-adres telkens verandert, adviseren wij geen IPsec IKEv1/v2 te gebruiken; in dat geval kunt u gebruik maken van een protocol welke geschikt is om te verbinden vanaf verschillende IP adressen (zoals EAP of WireGuard).

Security

Specify VPN Peer

Remote Client IP ⓘ

Pre-Shared Key ⓘ

X.509 Digital Signature

Local IP Assignment

Bij Local IP Assignment kunt u de VPN client een vast IP-adres geven of de keuze op DHCP laten staan, de VPN client zal dan een IP-adres ontvangen van de DHCP server in de DrayTek. Selecteer bij Assign IP from het LAN subnet waarvan de VPN client een IP-adres dient te ontvangen.






Local IP Assignment

| | |
|----------------|---|
| Assign IP By | <input checked="" type="radio"/> LAN DHCP <input type="radio"/> Static IP |
| Assign IP from | <input type="text" value="[LAN] LAN1"/> ▼ |
| Assign DNS By | <input checked="" type="radio"/> LAN DHCP <input type="radio"/> Manually |

Smart VPN Client setup

De Smart VPN Client van DrayTek is een gratis softwaretoepassing die gebruikers helpt om eenvoudig een VPN-verbinding op te zetten naar een DrayTek VPN-router. Het stelt gebruikers in staat om vanaf een externe locatie veilig verbinding te maken met het bedrijfsnetwerk of een privé-netwerk, waardoor ze toegang krijgen tot gedeelde netwerkbronnen alsof ze zich op kantoor bevinden.

De Smart VPN Client biedt eenvoudige configuratie-opties, automatische verbinding, en maakt gebruik van encryptie om de gegevensoverdracht te beveiligen. Het werkt zowel op Windows als macOS en kan een handige oplossing zijn voor telewerkers die betrouwbare toegang tot hun netwerk nodig hebben. De software kunt u gratis downloaden op onze website www.draytek.nl.

| Windows | macOS | Mobile |
|--|---|---|
| Supports PPTP, L2TP, L2TP/IPsec, IPsec, IKEv2, OpenVPN, WireGuard, and SSL VPN. | Supports SSL VPN, IPsec XAuth, and IKEv2 EAP | Supports SSL VPN, IPsec XAuth (iOS), and IKEv2 EAP (iOS) |
|  |  |  |
| Download Version 5.6.5 | Download on the Mac App Store | Download on the App Store GET IT ON Google Play |
| View Release Note  | | |
| Download File Checksum  | | |

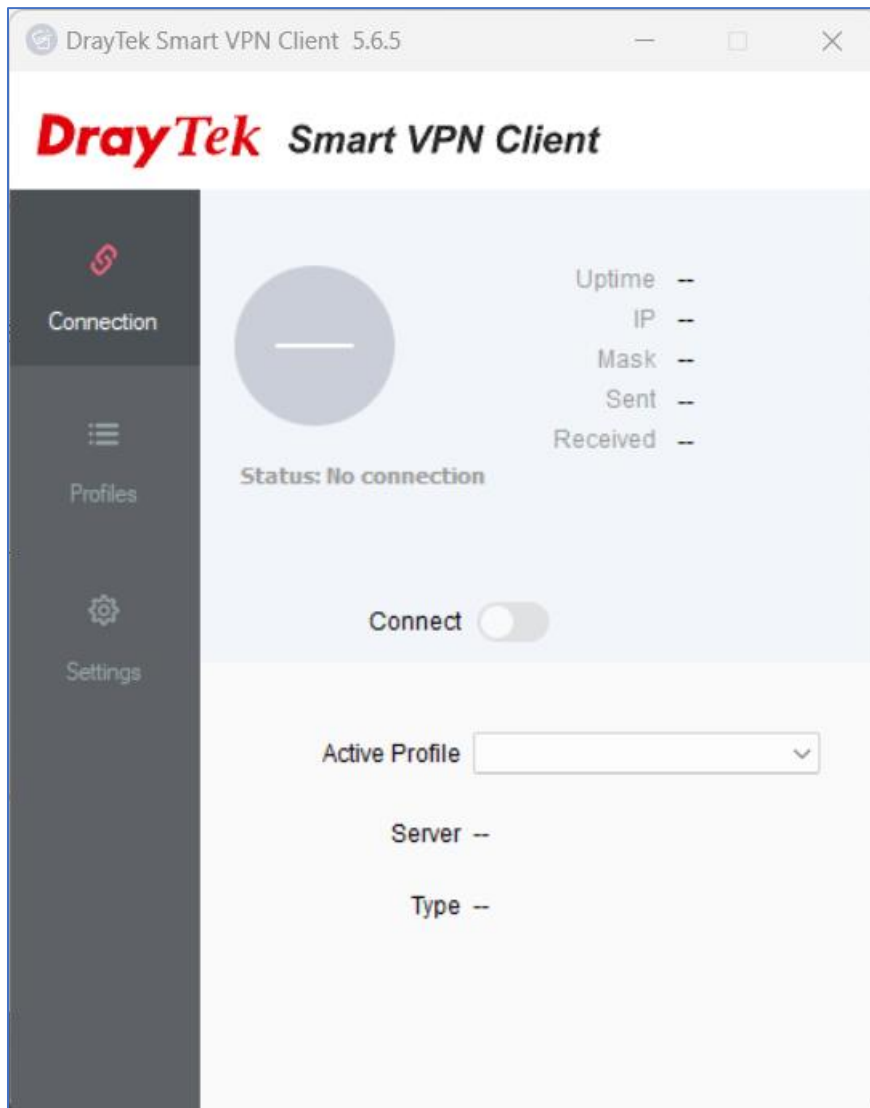
Smart VPN client configuratie

De Smart VPN Client bevat 3 tabbladen waarin u diverse configuraties kunt uitvoeren:

Connection : Hier kunt u de VPN tunnel opbouwen die u hebt aangemaakt onder profiles

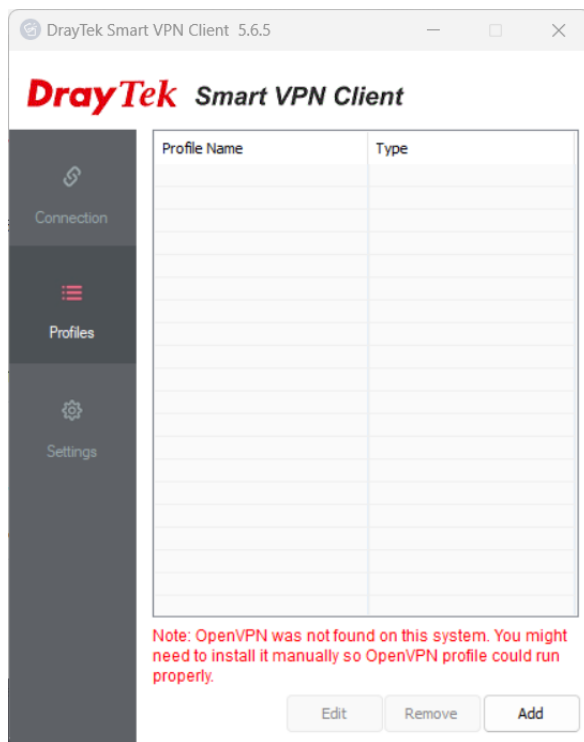
Profiles : In dit tabblad kunt u meerdere VPN profielen toevoegen.

Settings : Algemene VPN instellingen van de Smart VPN Client.



VPN profiel toevoegen

Ga naar Profiles en klik vervolgens op Add om een nieuw VPN profiel aan te maken.



Belangrijke informatie bij het inrichten van een IPsec VPN profiel:

Profile Name : Geef het profiel een duidelijke naam, vooral handig wanneer u meerdere VPN profielen wil gaan gebruiken.

Type : Selecteer IPsec Tunnel.

IP or Hostname : Het WAN IP-adres van de DrayTek waar u de VPN tunnel naar op wil zetten.

IP Property : Selecteer 'Standard IPsec Tunnel' of 'Specify an IP-address on'. In beide gevallen dient u het LAN subnet van de VPN server (DrayTek) te definiëren. In ons voorbeeld betreft dit het 172.31.254.1/24 LAN subnet.

Advanced Options

Pre-Shared Key : De Pre-Shared Key die u op de DrayTek hebt ingesteld, dit kan de algemene Pre-Shared Key zijn of de Pre-Shared Key in het VPN Teleworker profiel.

Op de volgende pagina ziet u een voorbeeld configuratie.

Edit Profile [X]

Profile Name:

Server Information

Type:

IP or Hostname:

VPN Information

Authentication Type:

User Name:

Password:

Remember My Credentials:

Always Prompt for Credentials:

IP Property

Standard IPSec Tunnel

Remote Subnet:

Remote Subnet Mask:

Specify an IP Address on

IP Address:

Subnet Mask:

WINS Server:

Advanced Options

My IP:

Mainmode Keyexchange Method

DH Group 1 DH Group 2 DH Group 14

Security Method

Medium(AH) High(ESP)

SHA1 AES256 with SHA1

Authentication Method

Pre-shared Key

Certificate Authentication

Enable PING to keep alive:

Ping to the IP:

(This IP should exist in the remote subnet!)

Klik op OK om de instellingen op te slaan, vervolgens kunt u de VPN tunnel opbouwen in het Connection tabblad.

DrayTek Smart VPN Client

Connection

Local IP 10.31.0.110

Remote Subnet 172.31.254.1/24

Encryption Type ESP: SHA1-AES256

Status: Connected

Inactive

Active Profile

Server WAN IP-adres 2136

Type IPSec / Tunnel

Profiles

Settings

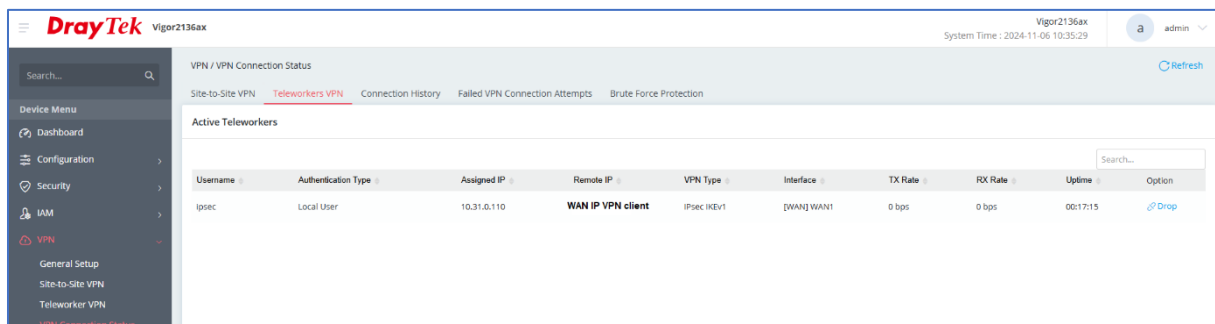
VPN ping controle

Omdat IPsec gebruikt maakt van UDP (verbindingloos) zal de Smart VPN Client altijd aangeven een actieve verbinding te hebben. Om te controleren of de VPN tunnel succesvol online is kan middels ping een controle worden uitgevoerd.

```
Pinging 172.31.254.1 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Reply from 172.31.254.1: bytes=32 time=17ms TTL=255  
Reply from 172.31.254.1: bytes=32 time=14ms TTL=255  
Reply from 172.31.254.1: bytes=32 time=16ms TTL=255  
Reply from 172.31.254.1: bytes=32 time=13ms TTL=255  
Reply from 172.31.254.1: bytes=32 time=11ms TTL=255  
Reply from 172.31.254.1: bytes=32 time=15ms TTL=255  
Reply from 172.31.254.1: bytes=32 time=12ms TTL=255  
Reply from 172.31.254.1: bytes=32 time=11ms TTL=255
```

VPN Connection Status

In de Vigor2136 kunt u onder VPN Connection Status de status inzien van de verbonden VPN gebruiker.



DrayTek Vigor2136ax
System Time : 2024-11-06 10:35:29
admin

VPN / VPN Connection Status
Site-to-Site VPN **Teleworkers VPN** Connection History Failed VPN Connection Attempts Brute Force Protection

Active Teleworkers

| Username | Authentication Type | Assigned IP | Remote IP | VPN Type | Interface | Tx Rate | Rx Rate | Uptime | Option |
|----------|---------------------|-------------|-------------------|-------------|------------|---------|---------|----------|----------------------|
| ipsec | Local User | 10.31.0.110 | WAN IP VPN client | IPsec IKEV1 | [WAN] WAN1 | 0 bps | 0 bps | 00:17:15 | Drop |

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.