

DrayTek

DrayOS5
IKEv2 EAP - macOS



Inhoudsopgave

IKEv2 EAP	3
IPsec General Setup.....	4
Teleworker VPN instellingen.....	5
General	6
User Information	6
Teleworker VPN	7
Security.....	7
Local IP Assignment.....	8
macOS setup	9
Smart-VPN setup	9
VPN Connection Status.....	12
Connection History.....	12
Failed VPN Connection Attempts.....	13
Blocked by Brute Force Protection.....	13

IKEv2 EAP

IKEv2 staat voor Internet Key Exchange version 2 en is een protocol dat wordt gebruikt voor het opzetten van Virtual Private Network (VPN) tunnels voor veilige communicatie over internet. Het is een belangrijk onderdeel van IPsec (Internet Protocol Security), dat wordt gebruikt voor het versleutelen en authenticeren van gegevens die over een netwerk worden verzonden. EAP is een flexibel authenticatieframework dat verschillende methoden ondersteunt voor het verifiëren van de identiteit van gebruikers of apparaten die verbinding maken met een netwerk. Met IKEv2 EAP kunnen apparaten een veilige communicatieverbinding tot stand brengen en kunnen ze EAP gebruiken voor de authenticatie van de gebruiker.

Voor het gebruik van IKEv2 EAP is het noodzakelijk een Let's Encrypt certificaat te hebben, deze kunt u gratis aanvragen icm een DrayDDNS account. De configuratie stappen kunt u terug vinden in de DrayDDNS handleiding op onze website.

Dit artikel demonstreert hoe je een DrayOS 5 Vigor Router configureert als een VPN-server voor IKEv2 EAP-clients, en welke configuratie vereist is op macOS om de VPN op te zetten. In het voorbeeld wordt de Vigor2136 router gebruikt icm de Smart VPN applicatie van DrayTek.

IPsec General Setup

Belangrijk is dat u IPsec op enable zet zodat dit VPN protocol gebruikt kan worden.

General Setup

IPsec WireGuard OpenVPN

Enabled

Authentication Settings for Dynamic Peer

Certificate

Preferred Local ID

Daarnaast dient u bij Certificate het DrayDDNS certificaat te selecteren, op dit DrayDDNS account dient u de Let's Encrypt te activeren.

Let's Encrypt Certificate

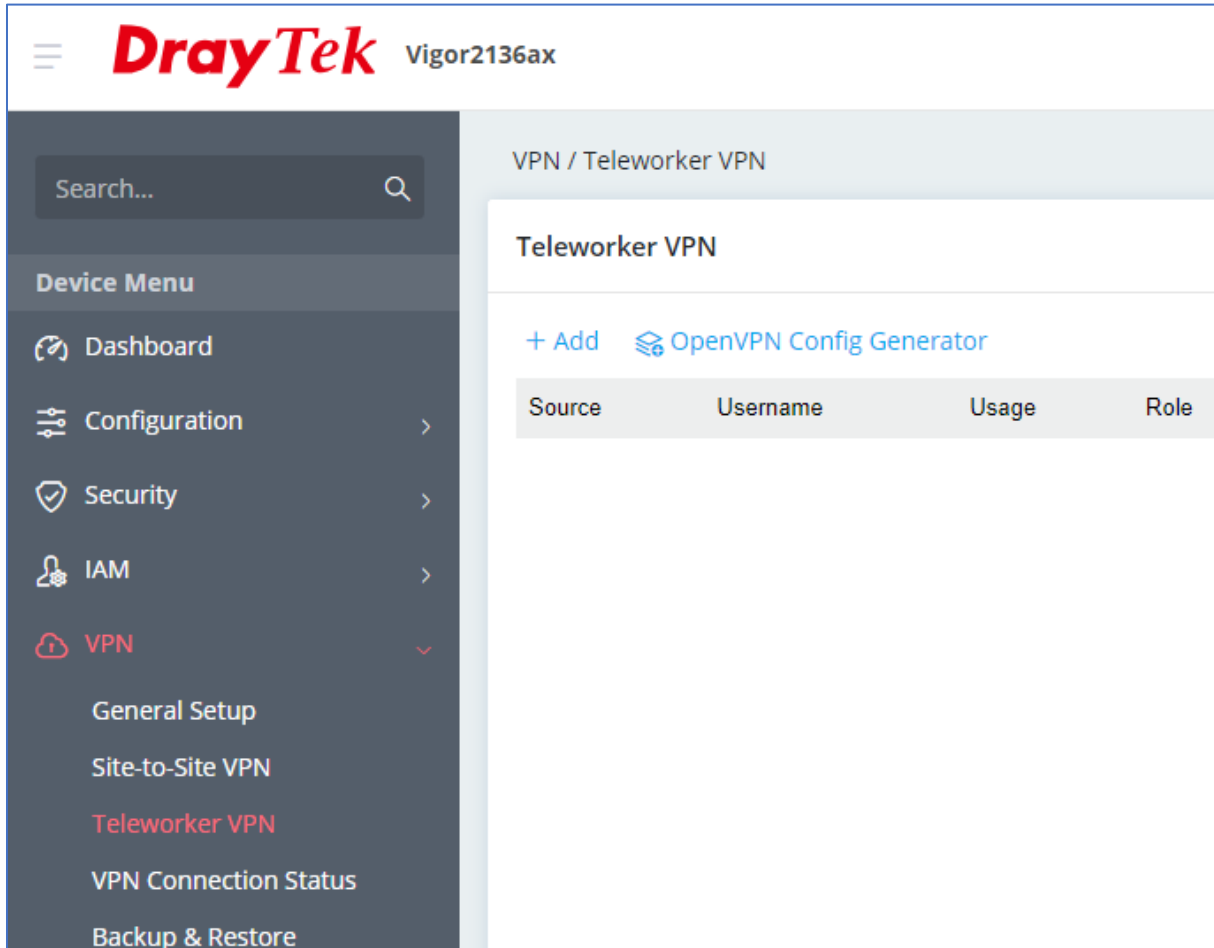
Enable ACME Client

Status Valid, Expires on: Jun 26 18:58:31 2024 GMT

Note: Enable ACME Client to create and allow certificate to be auto-renewed before expire date.

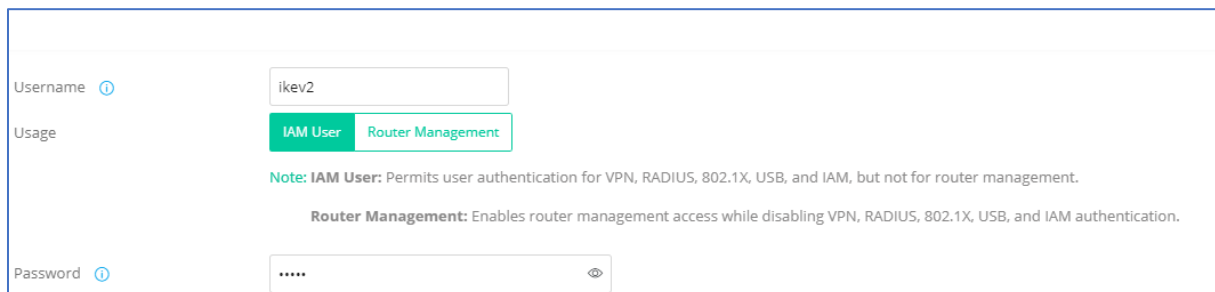
Teleworker VPN instellingen

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 left features the DrayTek logo and the device model Vigor2136ax. A search bar is located below the logo. On the left side, there is a 'Device Menu' with the following items: Dashboard, Configuration, Security, IAM, VPN (highlighted in red), General Setup, Site-to-Site VPN, Teleworker VPN (highlighted in red), VPN Connection Status, and Backup & Restore. The main content area is titled 'VPN / Teleworker VPN' and contains a section for 'Teleworker VPN'. This section includes a '+ Add' button and a link to 'OpenVPN Config Generator'. Below this is a table with the following 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 containing 'ikev2'.
- 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 masked password '....' and a visibility toggle icon.

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 EAP.

General

Enable Teleworker VPN

Idle Timeout (Seconds) ⓘ

VPN Schedule Always On Scheduled On

Download SmartVPN Client [Download SmartVPN Client](#)

Allowed VPN Protocols

Enable IPsec

Allowed IPsec Protocols IKEv1/v2 EAP XAuth

Enable WireGuard

Enable OpenVPN

Security

In verband met Zero Trust is het noodzakelijk dat u hier het publieke/Internet IP-adres opgeeft van de VPN client die verbinding wil maken. Het is helaas niet mogelijk om met een Dynamic IP-adres een IKEv2 EAP verbinding op te zetten.

Security

Specify VPN Peer

Remote Client IP ⓘ

Pre-Shared Key ⓘ ⓘ

Local IP Assignment

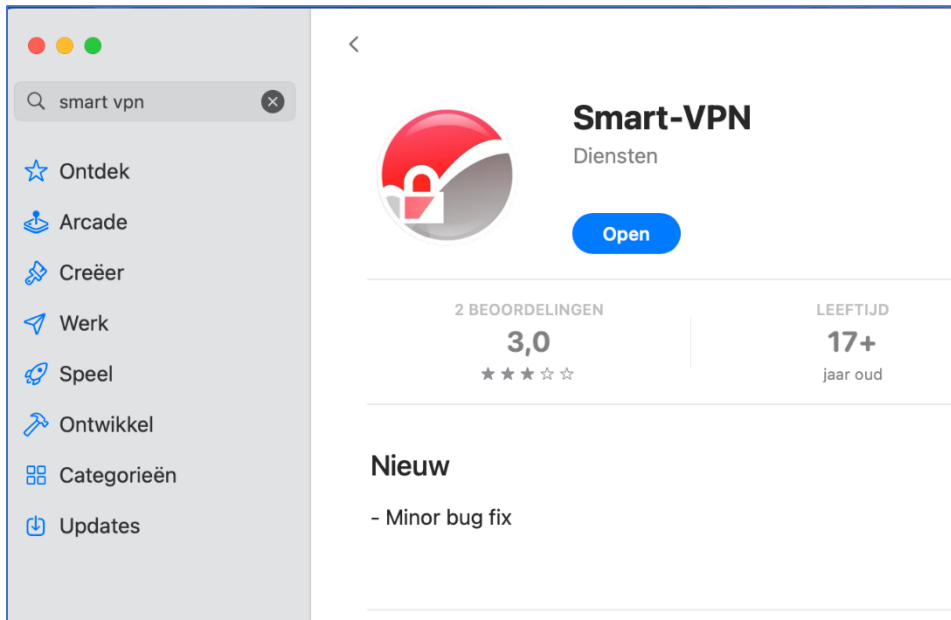
Bij Local IP Assignment kunt u de VPN client een vast IP-adres geven of de keuze op DHCP laten staan, de VPN client zal dan een IP-adres ontvangen van de DHCP server in de DrayTek.

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"/> <input type="button" value="v"/>
Assign DNS By	<input checked="" type="radio"/> LAN DHCP <input type="radio"/> Manually

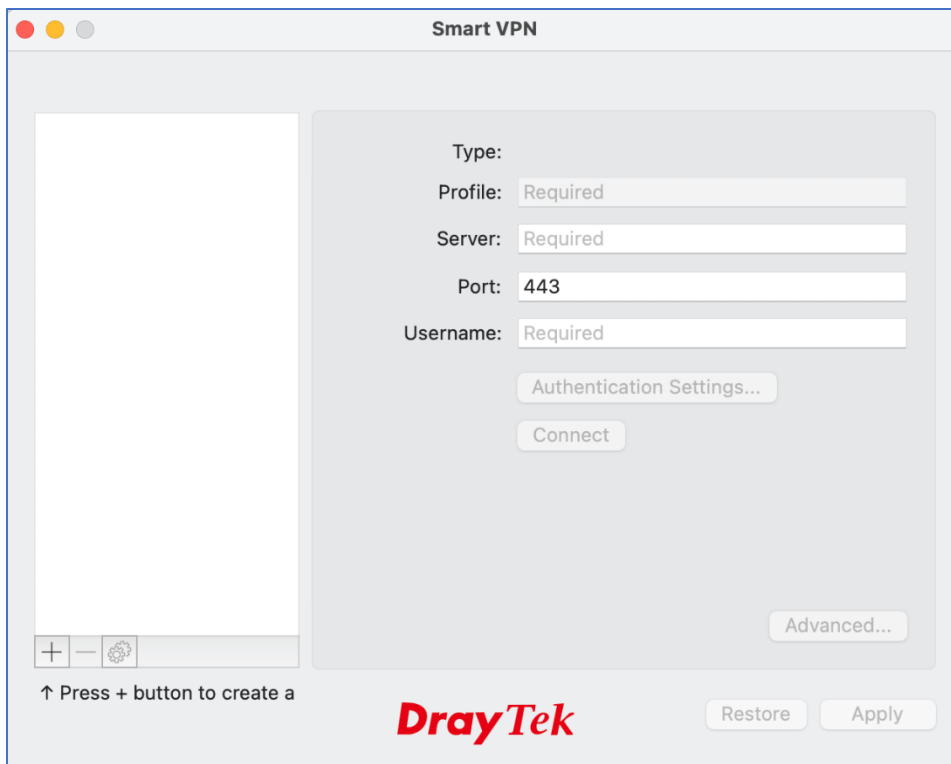
macOS setup

Smart-VPN setup

DrayTek heeft tevens een eigen VPN client beschikbaar voor macOS gebruikers, deze VPN client app kunt u gratis downloaden in de App Store op uw Apple device. Deze tool is beschikbaar voor zowel macOS als iOS.



Door op het + teken te klikken kunt u een nieuw VPN profiel inrichten.



Selecteer bij Type IKEv2 EAP, vervolgens kunt u het profiel een naam geven. Bij Server geeft u het DrayDDNS account in van de DrayTek. Het Remote ID wordt automatisch ingevuld op basis van uw DrayDDNS account. Bij User name kunt u de gebruikersnaam opgeven van de VPN Teleworker die u hebt aangemaakt.

Create a new Smart VPN profile:

Type: IKEv2 EAP

Profile: Required

Server: vpn.example.com

Remote ID: Required

User name: Required

Authentication ?

Cancel Create

Klik vervolgens op Authentication om het wachtwoord en de XAuth pre-shared key in te vullen. Klik hierna op OK en op Create om het VPN profiel op te slaan.

Create a new Smart VPN profile:

Type: IKEv2 EAP

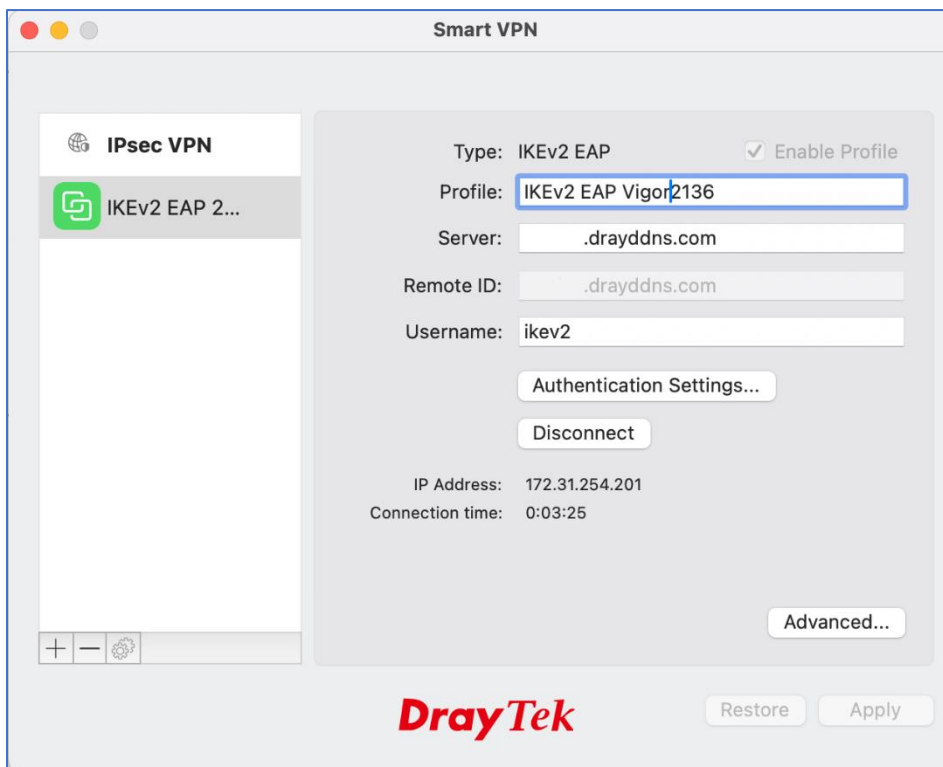
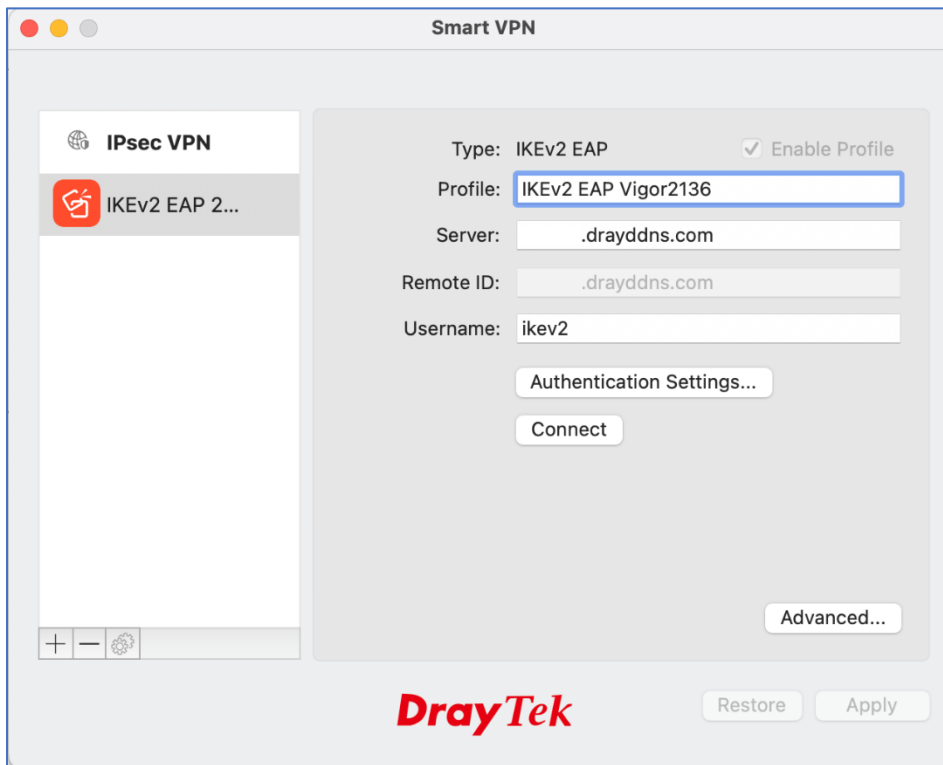
User Authentication:

Password:

Cancel OK

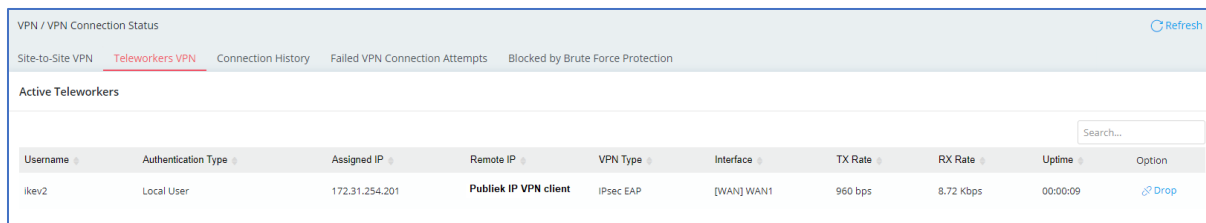
Cancel Create

Activeer het profiel door Enable Profile aan te vinken, vervolgens kunt u op Connect klikken om de VPN tunnel op te bouwen.



VPN Connection Status

In de DrayTek kunt u onder VPN Connection Status de verbinding informatie terug vinden.



VPN / VPN Connection Status Refresh

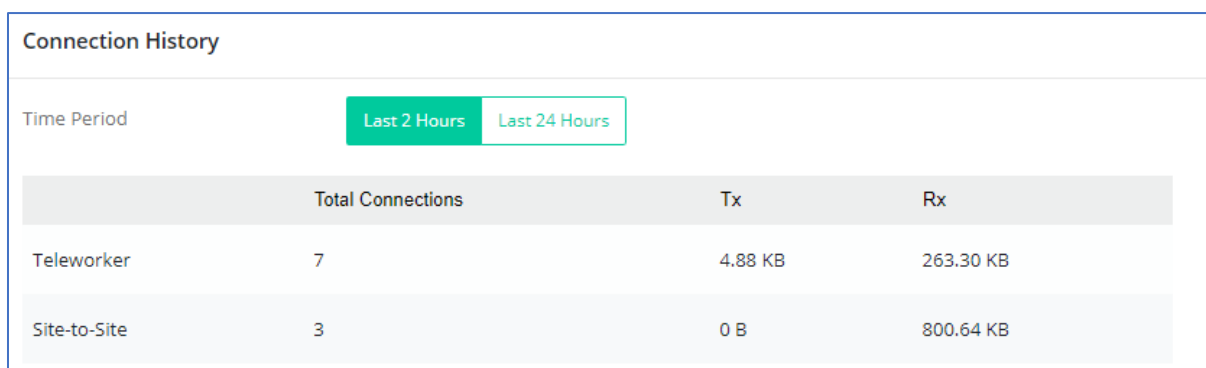
Site-to-Site VPN **Teleworkers VPN** Connection History Failed VPN Connection Attempts Blocked by Brute Force Protection

Active Teleworkers

Username	Authentication Type	Assigned IP	Remote IP	VPN Type	Interface	TX Rate	RX Rate	Uptime	Option
ikev2	Local User	172.31.254.201	Publiek IP VPN client	IPsec EAP	[WAN] WAN1	960 bps	8.72 Kbps	00:00:09	Drop

Connection History

Op basis van de laatste 2 uur of laatste 24 uur kunt u bij Connection History informatie terug vinden over de hoeveelheid clients (Teleworkers) of Site-to-Site (LAN-to-LAN) VPN verbindingen er actief zijn geweest.

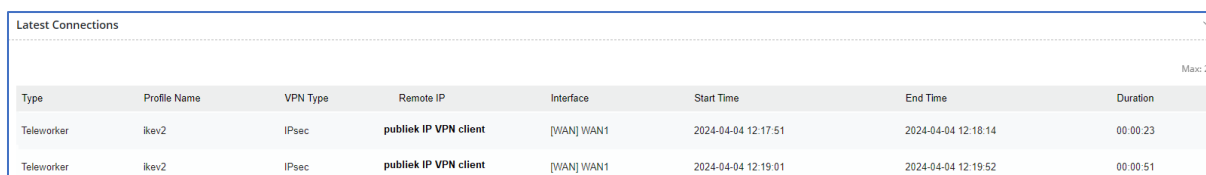


Connection History

Time Period Last 2 Hours Last 24 Hours

	Total Connections	Tx	Rx
Teleworker	7	4.88 KB	263.30 KB
Site-to-Site	3	0 B	800.64 KB

Bij Latest Connections kunt u zien vanaf welk IP-adres deze client verbonden is geweest, op welk moment deze online is gekomen en voor welke duur de tunnel online is geweest.



Latest Connections Max: 20

Type	Profile Name	VPN Type	Remote IP	Interface	Start Time	End Time	Duration
Teleworker	ikev2	IPsec	publiek IP VPN client	[WAN] WAN1	2024-04-04 12:17:51	2024-04-04 12:18:14	00:00:23
Teleworker	ikev2	IPsec	publiek IP VPN client	[WAN] WAN1	2024-04-04 12:19:01	2024-04-04 12:19:52	00:00:51

Failed VPN Connection Attempts

Indien de VPN tunnel niet online komt zal deze informatie terug te vinden zijn bij het tabblad Failed VPN Connection Attempts. Op basis van de laatste 2 uur of 24 uur kunt u deze informatie inzien.

Failed VPN Connection Attempts	
Time Period	Last 2 Hours Last 24 Hours
Protocol	Failed Attempts
IPsec	13
WireGuard	0
OpenVPN	0

Blocked by Brute Force Protection

Indien u Brute Force Protection hebt aangezet onder VPN > General Setup kunt u hier informatie vinden over IP-adressen die zijn geblokkeerd vanwege Brute Force Protection. Dit kan gebeuren als gevolg van onjuiste VPN-inloggegevens, zoals een verkeerd wachtwoord. Het kan echter ook een onbekend IP-adres zijn dat probeert een tunnel op te zetten via een specifiek VPN-protocol.

VPN / VPN Connection Status Refresh							
Site-to-Site VPN Teleworkers VPN Connection History Failed VPN Connection Attempts Blocked by Brute Force Protection							
Blocked by Brute Force Protection							
External IP	Location	VPN Type	VPN Profile	Interface	Start Time	End Time	Option
Publiek IP	NL	IPsec	N/A	[WAN] WAN1	2024-04-04 12:10:54	2024-04-04 12:27:33	Unblock
Publiek IP	NL	IPsec	N/A	[WAN] WAN1	2024-04-04 11:19:58	2024-04-04 11:36:37	Unblock
Publiek IP	NL	IPsec	N/A	[WAN] WAN1	2024-04-04 10:50:32	2024-04-04 11:07:11	Unblock

Vorbehoud

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.