

DrayTek

DrayOS5
Site-to-Site IPsec



Inhoudsopgave

VPN Site-to-Site	3
VPN General Setup	4
Dial In profiel (VPN server)	5
General.....	5
IKE Authentication.....	6
More settings (IKE phase 1 & IKE phase 2).....	7
Network.....	7
Dial Out profiel (VPN client).....	8
General.....	8
IKE Authentication.....	9
More settings (IKE phase 1 & IKE phase 2).....	10
Network.....	10
IKEv2 tunnel.....	11
XAuth tunnel.....	11
VPN Connection Status.....	12
Connection History.....	12
Failed VPN Connection Attempts	13
Blocked by Brute Force Protection	13

VPN Site-to-Site

DrayTek-producten bevatten een ingebouwde VPN-server, waarmee een VPN-tunnel kan worden opgezet naar uw netwerk zonder dat er een aparte VPN-server nodig is. VPN biedt een veilige verbinding over het internet naar uw eigen netwerk.

Er zijn verschillende vormen van VPN. DrayTek ondersteunt IPsec, WireGuard en OpenVPN. Momenteel is IPsec de meest gebruikte vorm bij het opzetten van een Site-to-Site VPN-tunnel.

De beveiliging van de VPN-tunnel wordt verzorgd door verschillende encryptieprotocollen. DrayTek ondersteunt DES, 3DES en AES. Standaard adviseren wij het gebruik van AES met encryptie. Dit is de meest veilige encryptiemethode die u 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 Site-to-Site VPN. Met deze VPN tunnel wordt de verbinding opgezet tussen twee routers.

Deze handleiding zal u begeleiden bij het opzetten van een Site-to-Site VPN-verbinding tussen twee Vigor2136-routers met behulp van het IPsec-protocol op basis van IKEv1/IKEv2. Houd er rekening mee dat de Vigor2136-serie DrayOS5 gebruikt, wat resulteert in een andere WebUI dan zijn voorganger(s).

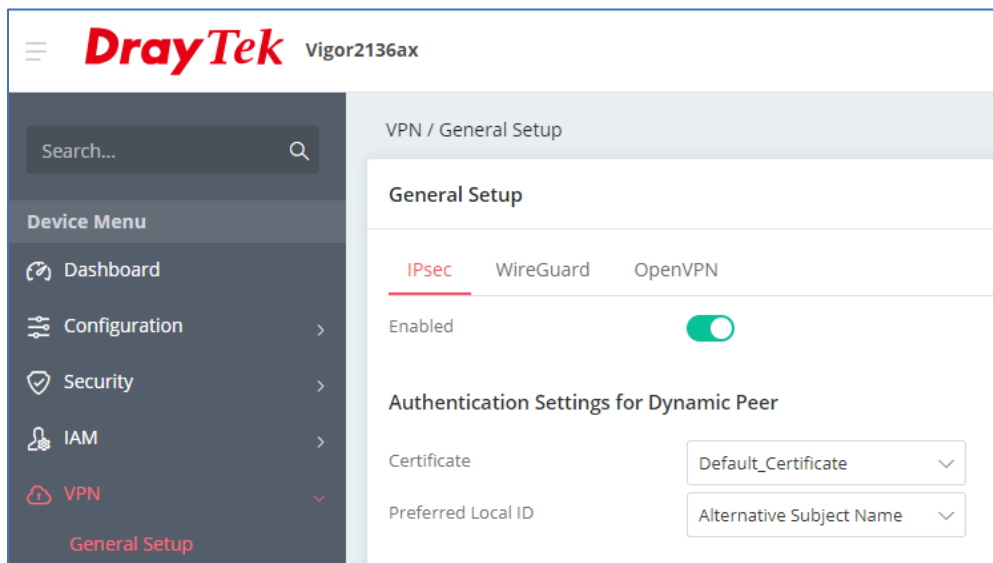
Situatie

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 2136	DrayTek Vigor 2136
LAN IP-subnet	172.31.254.1	192.168.1.1
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)
VPN protocol	IPsec IKEv1 of IKEv2	IPsec IKEv1 of IKEv2
Pre-Shared Key		
Encryptie	AES256	
Authenticatie	SHA256	

VPN General Setup

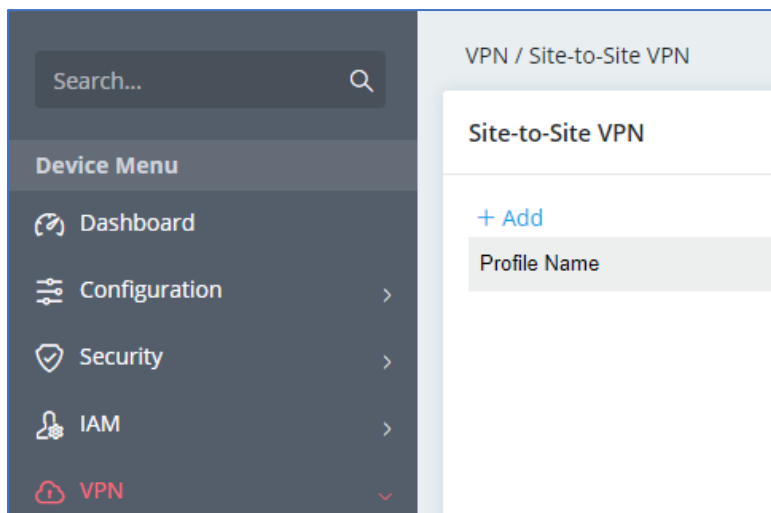
Aangezien het hier om een IPsec verbinding gaat moet u eerst controleren of deze functie wel geactiveerd is. Dit kunt u doen bij VPN >> General Setup.



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

Dial In profiel (VPN server)

In het hoofdmenu van de DrayTek gaat u naar VPN > Site-to-Site VPN. Klik vervolgens op Add om een nieuw VPN profiel toe te voegen.



General

In het General gedeelte van de Site-to-Site tunnel bepaalt u basis VPN configuratie. Hierbij zijn onderstaande instellingen van belang:

- Direction** : Keuze tussen Dial-In, Dial-Out of Both. In dit geval selecteren we Dial-In om deze DrayTek als VPN server in te richten.
- VPN Type** : VPN protocol welke gebruik wordt, selecteer IPsec.
- IPsec Dial-In Protocol** : Keuze tussen IKEv1/v2 en XAuth.
- Dial-in Allowed Schedule** : Mag de VPN tunnel altijd online zijn of enkel op specifieke tijdstippen. Hiervoor dient u dan een Time Schedule profiel aan te maken. Dit is mogelijk bij Configuration > Objects > Schedule. In ons voorbeeld kiezen we voor Always Allowed.

Profile Name ⓘ

Enabled

General

Direction

VPN Type

IPsec Dial-In Protocol IKEv1/v2 XAuth

Dial-In Allowed Schedule Always Allow Scheduled

IKE Authentication

Bij IKE (Internet Key Exchange) authenticatie in een VPN-profiel, configureert u de methoden en parameters die worden gebruikt voor het uitwisselen van sleutels en het authenticeren van VPN-verbindingen tussen de client en de VPN-server.

Dial-In Settings

Negotiation : Keuze tussen Main Mode en Aggressive Mode, we kiezen voor Main Mode.

Specify VPN Peer : Het Publieke IP-adres van de VPN Client (Dial Out) modem/router. Hier zal een controle op plaatsvinden.

Pre-Shared Key : Gedeelde geheime sleutel die overeen moet komen op beide routers.

IKE Identifier *verplicht bij Aggressive mode*

Local ID : Identificatie parameters die gebruikt kunnen worden voor het opzetten van de VPN verbinding. Local ID identificeert de lokale kant van de VPN-verbinding

Peer ID : Identificatie parameters die gebruikt kunnen worden voor het opzetten van de VPN verbinding. Peer ID identificeert de externe kant van de VPN-verbinding.

IKE Authentication

Dial-In Settings

Negotiation Main Mode Aggressive Mode

Specify VPN Peer

Remote IP ⓘ

Pre-Shared Key ⓘ

X.509 Digital Signature

IKE Identifier

Local ID ⓘ

Peer ID ⓘ

Note: IKE Identifier is optional in Main Mode negotiations.

More settings (IKE phase 1 & IKE phase 2)

Bij de sectie 'More settings' kunt u eventuele Phase 1 en Phase 2 instellingen aanpassen. Phase 1 legt de basisparameters vast voor de beveiligde communicatie tussen beide DrayTek producten, terwijl Phase 2 vervolgens de beveiligingsinstellingen voor de gegevensoverdracht instelt.

in onze opzet kiezen we voor de meest veilige en hoge phase1 en phase 2 encryptie en authenticatie instellingen.

The screenshot shows the 'More settings' configuration page. It is divided into two sections: 'IKE Phase 1' and 'IKE Phase 2'.
IKE Phase 1: This section has four columns: 'Encryption' (AES256-CBC), 'Group' (21 ec521), 'Authentication' (SHA256), and 'Lifetime' (28800). A note below states: 'Note: Phase1 Proposal may not take effect when VPN Peer is unspecified or direction is Dial-In with Aggressive Mode.'
IKE Phase 2: This section has five columns: 'Security Protocol' (ESP (High)), 'Encryption' (AES256-CBC), 'Authentication' (SHA256), 'Lifetime' (3600), and 'Perfect Forward Secret' (disabled). The 'Perfect Forward Secret' column has a toggle switch.

Network

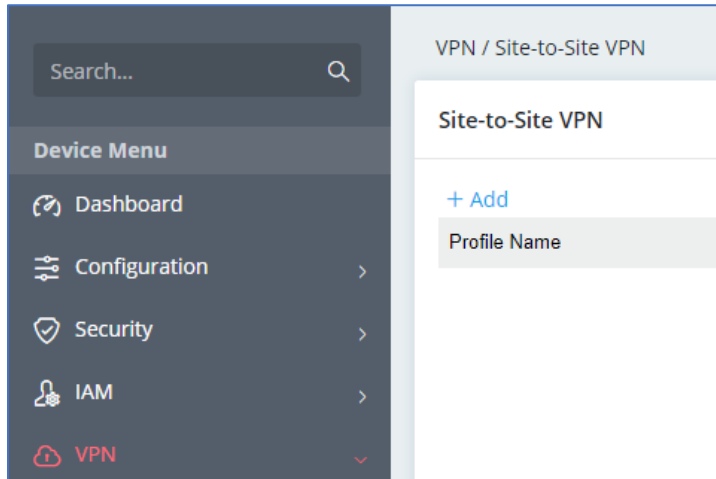
Bij netwerkinstellingen is het noodzakelijk om zowel het lokale LAN-netwerk als het LAN-subnet van de externe locatie te definiëren. Deze IP-subnetten moeten van elkaar verschillen om de VPN-tunnel op te zetten. Het is dus niet mogelijk om bijvoorbeeld 192.168.1.1/24 op beide locaties te gebruiken en hier een VPN-tunnel tussen op te zetten.

The screenshot shows the 'Network' configuration page. It has a table with four columns: 'Local Network', 'Subnet Mask', 'Remote Network', and 'Subnet Mask'.
- 'Local Network' contains 'LAN IP'.
- 'Subnet Mask' contains '255.255.255.0/24'.
- 'Remote Network' contains 'LAN IP remote locatie'.
- 'Subnet Mask' contains '255.255.255.0/24'.
Below the table, there is a 'More Remote Subnets' dropdown menu set to 'Disabled'.
At the bottom, there are 'Cancel' and 'Apply' buttons.

Klik op Apply om het VPN Dial In profiel op te slaan.

Dial Out profiel (VPN client)

In het hoofdmenu van de DrayTek gaat u naar VPN > Site-to-Site VPN. Klik vervolgens op Add om een nieuw VPN profiel toe te voegen.



General

In het General gedeelte van de Site-to-Site tunnel bepaalt u basis VPN configuratie. Hierbij zijn onderstaande instellingen van belang:

- | | |
|--------------------------------|---|
| Direction | : Keuze tussen Dial-In, Dial-Out of Both. In dit geval selecteren we Dial-In om deze DrayTek als VPN server in te richten. |
| VPN Type | : VPN protocol welke gebruik wordt, selecteer IPsec. |
| IPsec Dial-Out Protocol | : Keuze tussen IKEv1, IKEv2 en XAuth. |
| Remote Server | : Publiek IP-adres van de VPN server locatie. |
| Dial-Out Mode | : Mag de VPN tunnel altijd online zijn of enkel op specifieke tijdstippen. Hiervoor dient u dan een Time Schedule profiel aan te maken. Dit is mogelijk bij Configuration > Objects > Schedule. In ons voorbeeld kiezen we voor Always Allowed. |

General

Direction	Dial-Out
VPN Type	IPsec
IPsec Dial-Out Protocol	IKEv1
Remote Server ?	Publiek IP-adres VPN server
Dial-Out Mode	<input type="radio"/> On Demand <input checked="" type="radio"/> Always On <input type="radio"/> Scheduled

IKE Authentication

Bij IKE (Internet Key Exchange) authenticatie in een VPN-profiel, configureert u de methoden en parameters die worden gebruikt voor het uitwisselen van sleutels en het authenticeren van VPN-verbindingen tussen de client en de VPN-server.

Dial-Out Settings

Negotiation : Keuze tussen Main Mode en Aggressive Mode, we kiezen voor Main Mode.

Authentication : Keuze tussen Pre-Shared Key of Certificate, we kiezen in deze voor Pre-Shared Key.

Pre-Shared Key : Gedeelde geheime sleutel die overeen moet komen op beide routers.

IKE Identifier *verplicht bij Aggressive mode*

Local ID : Identificatie parameters die gebruikt kunnen worden voor het opzetten van de VPN verbinding. Local ID identificeert de lokale kant van de VPN-verbinding

Peer ID : Identificatie parameters die gebruikt kunnen worden voor het opzetten van de VPN verbinding. Peer ID identificeert de externe kant van de VPN-verbinding.

IKE Authentication

Dial-Out Settings

Negotiation Main Mode Aggressive Mode

Authentication Pre-Shared Key Certificate

Pre-Shared Key ⓘ

IKE Identifier

Local ID ⓘ

Peer ID ⓘ

Note: IKE Identifier is optional in Main Mode negotiations.

More settings (IKE phase 1 & IKE phase 2)

Bij de sectie 'More settings' kunt u eventuele Phase 1 en Phase 2 instellingen aanpassen. Phase 1 legt de basisparameters vast voor de beveiligde communicatie tussen beide DrayTek producten, terwijl Phase 2 vervolgens de beveiligingsinstellingen voor de gegevensoverdracht instelt.

in onze opzet kiezen we voor de meest veilige en hoge phase1 en phase 2 encryptie en authenticatie instellingen.

The screenshot shows the 'More settings' configuration page. It is divided into two sections: 'IKE Phase 1' and 'IKE Phase 2'.
IKE Phase 1: This section has four columns: 'Encryption' (AES256-CBC), 'Group' (21 ecp521), 'Authentication' (SHA256), and 'Lifetime' (28800). A note below states: 'Note: Phase1 Proposal may not take effect when VPN Peer is unspecified or direction is Dial-In with Aggressive Mode.'
IKE Phase 2: This section has five columns: 'Security Protocol' (ESP (High)), 'Encryption' (AES256-CBC), 'Authentication' (SHA256), 'Lifetime' (3600), and 'Perfect Forward Secret' (disabled).

Network

Bij netwerkinstellingen is het noodzakelijk om zowel het lokale LAN-netwerk als het LAN-subnet van de externe locatie te definiëren. Deze IP-subnetten moeten van elkaar verschillen om de VPN-tunnel op te zetten. Het is dus niet mogelijk om bijvoorbeeld 192.168.1.1/24 op beide locaties te gebruiken en hier een VPN-tunnel tussen op te zetten.

The screenshot shows the 'Network' configuration page. It has a table with four columns: 'Local Network', 'Subnet Mask', 'Remote Network', and 'Subnet Mask'.
- 'Local Network' contains 'LAN IP'.
- 'Subnet Mask' contains '255.255.255.0/24'.
- 'Remote Network' contains 'LAN IP remote locatie'.
- 'Subnet Mask' contains '255.255.255.0/24'.
Below the table, there is a 'More Remote Subnets' dropdown menu set to 'Disabled'.
At the bottom, there are 'Cancel' and 'Apply' buttons.

Klik op Apply om het VPN Dial Out profiel op te slaan.

IKEv2 tunnel

Door op het Dial Out profiel het IPsec Dial-Out Protocol aan te passen naar IKEv2 zal de tunnel online komen op basis van IKEv2. Op de VPN server locatie hoeft u niks aan te passen aangezien deze al standaard is ingericht voor IKEv1/IKEv2.

General

Direction

VPN Type

IPsec Dial-Out Protocol

VPN / VPN Connection Status Refresh

[Site-to-Site VPN](#) [Teleworkers VPN](#) [Connection History](#) [Failed VPN Connection Attempts](#) [Blocked by Brute Force Protection](#)

Active Site-to-Site VPN Sessions

Profile Name	Status	VPN Type	Remote IP	Interface	Remote Network	TX Rate	RX Rate	Uptime	Option
VPNClient	Online	IPsec IKEv2		[WAN] WAN1	192.168.1.0/24	0 bps	0 bps	00:03:07	Drop

XAuth tunnel

XAuth zorgt naast de aanwezige Pre-Shared Key ook nog voor een authenticatie op basis van een gebruikersnaam en wachtwoord die op beide locaties overeen moet komen. XAuth moet u op zowel de VPN server als VPN client configureren.

General

Direction

VPN Type

IPsec Dial-Out Protocol

Remote Server

Dial-Out Mode

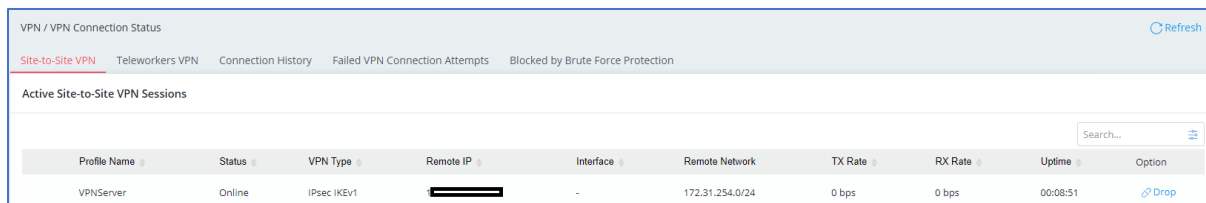
Username and Password

Username

Password

VPN Connection Status

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



VPN / VPN Connection Status Refresh

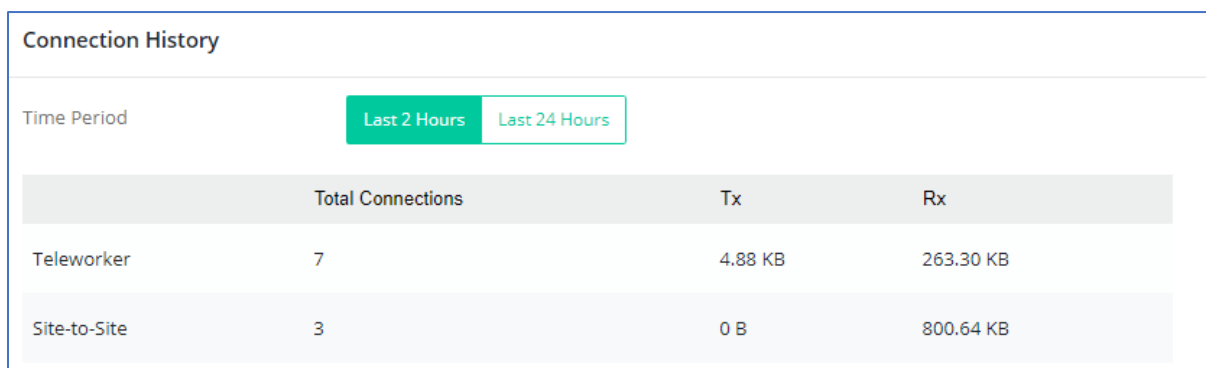
Site-to-Site VPN | Teleworkers VPN | Connection History | Failed VPN Connection Attempts | Blocked by Brute Force Protection

Active Site-to-Site VPN Sessions

Profile Name	Status	VPN Type	Remote IP	Interface	Remote Network	TX Rate	RX Rate	Uptime	Option
VPNServer	Online	IPsec IKEv1	[REDACTED]	-	172.31.254.0/24	0 bps	0 bps	00:08:51	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.

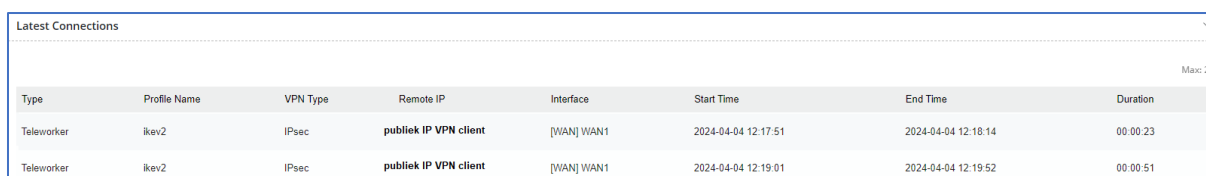


Connection History

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	<u>Blocked by Brute Force Protection</u>			
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

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.