

DrayTek

RoutIT
IPVPN en BGP



Inhoudsopgave

Wat wordt in deze handleiding behandeld.....	3
Vorbereiding.....	3
Neighbor configuratie.....	5
Te adverteren netwerken opgeven.....	6
GRE tunnel (optioneel: alleen bij 4G verbindingen)	7
BGP Prepending (optioneel: alleen bij back-up verbindingen)	9

Wat wordt in deze handleiding behandeld

Sinds enige tijd biedt RoutIT een IPVPN oplossing om locaties op een veilige manier met elkaar te kunnen koppelen. Deze oplossing kan gecombineerd worden met de andere security oplossingen om een totaaloplossing te kunnen bieden.

Binnen het IPVPN worden de beschikbare netwerken op basis van BGP geadverteerd. Hoe deze oplossing te realiseren is met DrayTek producten wordt in deze handleiding uitgelegd.

Voor verbindingen met het IPVPN via een mobiele (4G) verbinding is het noodzakelijk een GRE tunnel op te zetten. De configuratie hiervoor is ook in deze handleiding opgenomen, maar hoeft enkel toegepast te worden bij mobiele verbindingen! Voor andersoortige verbindingen hoeft deze configuratie niet toegepast te worden.

Voorbereiding

Gezien BGP toegepast wordt is het uiteraard noodzakelijk een router te kiezen die ondersteuning biedt voor BGP. Modellen uit de volgende series bieden ondersteuning voor BGP;

- Vigor 2862 serie
- Vigor 2865 serie
- Vigor 2926 serie
- Vigor 2927 serie
- Vigor 2952 serie
- Vigor 2962 serie
- Vigor 3910

Zorg ervoor dat de router(s) beschikk en over de laatste firmware versie die te downloaden is op www.draytek.nl/firmware.

Naast een geschikte router is natuurlijk ook informatie vanuit RoutIT nodig. Alle benodigde informatie is te vinden in IRMA en/of op de orderbevestiging.

Om IPVPN te kunnen gebruiken is het van belang dat de WAN interface van de router online is. Zorg er dus voor dat de WAN verbinding online is voordat het IPVPN geconfigureerd wordt.

Local BGP configuratie

Configuratie van het BGP protocol wordt gedaan in het menu **Routing > BGP**.

Het BGP protocol maakt gebruik van *neighbors* waar routes aan geadverteerd worden. De *neighbor* is in dit geval de router van RoutIT in het IPVPN. Deze router moet echter weten door wie het geadverteerde subnet afkomstig is. Dit onderscheid wordt gemaakt op basis van het AS nummer in combinatie met het Router ID. Deze gegevens worden opgegeven bij het inschakelen van BGP;

Routing >> BGP ?

Basic Settings **Static Network** | [Refresh](#) | [View Routing Table](#) |

Local

Enable BGP

Local AS Number (1~4294967295)

Hold Time (10~65535 Sec)

Connect Retry Time (3~255 Sec)

Router ID (e.g. 1.2.3.4)

Configuratie optie	Wat doet het	Wat in te vullen
Enable BGP	Schakelt BGP op de router in	'Enable'
Local AS Number	AS nummer van de lokale router	Zie IRMA
Hold Time	Negotiation timeout tussen BGP peers	180
Connect Retry Time	Timeout voor het krijgen van verbinding met de peer	120
Router ID	Identificer van de lokale router	Zie IRMA (veelal WAN IP adres)

Neighbor configuratie

De lokale router moet weten naar welke remote router geadverteerd moet worden. Dit is aan te geven door een *neighbor* op te geven. De opgegeven netwerken worden naar deze routers geadverteerd.

Configureer een *neighbor* door op een index nummer te klikken in het menu **Routing > BGP**.

Routing >> Neighbor Setup

Index 1

Enable

Profile Name

AS Number (1~4294967295)

IP Address

MD5 Auth

4-Byte As Number

Prepend Weight

Configuratie optie	Wat doet het	Wat in te vullen
Enable	Schakelt het adverteren naar deze neighbor in	'Enable'
Profile Name	Geeft de mogelijkheid de neighbor een naam te geven zodat deze makkelijk te herkennen is	Een herkenbare naam voor de neighbor
AS Number	Geeft aan in welk BGP AS het netwerk geadverteerd moet worden	Zie IRMA
IP Address	Het IP adres van de BGP neighbor om het netwerk aan te adverteren	Afhankelijk van de verbinding; zie IRMA
MD5 Auth	Schakelt encryptie in voor de communicatie met de BGP neighbor	Aanvinken en het MD5 voor de BGP connectie invullen. Zie IRMA.

Te adverteren netwerken opgeven

Nu de router geconfigureerd is om netwerk te adverteren via BGP, moet opgegeven worden welke netwerken geadverteerd moeten worden.

Om optimaal gebruik te maken van het IPVPN is het aan te bevelen het geadverteerde subnet als zijnde een routed subnet te configureren. Op deze manier zijn alle apparaten binnen dit subnet direct beschikbaar binnen het IPVPN.

Instructies voor het aanmaken van een gerouteerd subnet zijn te vinden in de [IP Routed Subnet handleiding](#), onder het item 'IP Routing Usage (specifieke LAN poort)'.

Geef vervolgens het te adverteren subnet op in het menu **Routing > BGP** op het tabblad **Static Network**.

Routing >> BGP ?

Basic Settings		Static Network		View Routing Table
Select	Index	IP Address	Subnet Mask	
<input type="checkbox"/>	1	<input type="text" value="192.168.101.0"/>	<input type="text" value="255.255.255.0 / 24"/>	
<input type="checkbox"/>	2	<input type="text"/>	<input type="text" value="255.255.255.254 / 31"/>	
<input type="checkbox"/>	3	<input type="text"/>	<input type="text" value="255.255.255.254 / 31"/>	
<input type="checkbox"/>	4	<input type="text"/>	<input type="text" value="255.255.255.254 / 31"/>	
<input type="checkbox"/>	5	<input type="text"/>	<input type="text" value="255.255.255.254 / 31"/>	
<input type="checkbox"/>	6	<input type="text"/>	<input type="text" value="255.255.255.254 / 31"/>	
<input type="checkbox"/>	7	<input type="text"/>	<input type="text" value="255.255.255.254 / 31"/>	
<input type="checkbox"/>	8	<input type="text"/>	<input type="text" value="255.255.255.254 / 31"/>	

Configuratie optie	Wat doet het	Wat in te vullen
Select	Adverteert het netwerk na op 'OK' gedruk te hebben	Aanvinken
IP Address	Dit is het subnet dat geadverteerd wordt naar het IPVPN	Het netwerk adres dat geadverteerd moet worden
Subnet Mask	Het subnet mask van het te adverteren subnet	Het subnet mask van het netwerk

Het is nu mogelijk vanaf het opgegeven netwerk verkeer naar het IPVPN in te sturen.

GRE tunnel (optioneel: alleen bij 4G verbindingen)

Voor mobiele (4G) verbindingen is het nodig eerst een GRE tunnel op te zetten om middels BGP netwerken te kunnen adverteren naar het IPVPN.

Het configureren van een GRE tunnel wordt gedaan in het menu **VPN and Remote Access > LAN to LAN**. Klik hier op een Index nummer om een GRE tunnel te configureren.

VPN and Remote Access >> LAN to LAN	
Profile Index : 1	
Common Settings	
<input checked="" type="checkbox"/> Enable this profile Profile Name: <input type="text" value="RoutIT Mobile Interconnect"/>	Always on: <input type="checkbox"/> Enable Idle Timeout: <input type="text" value="300"/> second(s) Quality Monitoring/Keep Alive: <input type="checkbox"/> Enable
Call Direction: <input type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input checked="" type="radio"/> GRE Tunnel	Netbios Naming Packet: <input checked="" type="radio"/> Pass <input type="radio"/> Block
Dial-Out Through: <input type="text" value="LTE Only"/> <input type="text" value="1-172.31.140.144"/>	Multicast via VPN: <input checked="" type="radio"/> Pass <input type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay,.etc.)</small>
Tunnel Settings	
<input type="checkbox"/> Enable IPsec Dial-Out function GRE over IPsec Tunnel Local IP: <input type="text" value="172.21.1.1"/> Local WAN IP: <input type="text" value="172.31.140.144"/>	<input type="checkbox"/> Logical Traffic Tunnel Remote IP: <input type="text" value="172.21.1.2"/> Remote WAN IP: <input type="text" value="172.31.255.20"/>
6in4 Settings	
<input type="checkbox"/> Enable 6in4 over PPTP LAN Interface: <input type="text" value="LAN1"/> Remote LAN IP: <input type="text" value="0.0.0.0"/> LAN IPv6 Prefix: <input type="text" value="::"/> / <input type="text" value="64"/> Remote IPv6 Prefix: <input type="text" value="::"/> / <input type="text" value="64"/> Tunnel TTL: <input type="text" value="255"/>	
TCP/IP Network Settings	
Local Network IP: <input type="text" value="172.21.1.1"/> / Mask: <input type="text" value="255.255.255.255 / 32"/> Remote Network IP: <input type="text" value="172.21.1.2"/> / Mask: <input type="text" value="255.255.255.255 / 32"/> More Remote Subnet: <input type="button" value="+"/>	Mode: <input checked="" type="radio"/> Routing <input type="radio"/> NAT RIP via VPN: <input type="text" value="Disable"/> <input type="checkbox"/> Change Default Route to this VPN tunnel <small>(This only works if there is only one WAN online)</small>
<input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	

Let op: om gebruikt te maken van GRE is het momenteel nog noodzakelijk om de PPTP VPN Service ingeschakeld te hebben. Deze kan geactiveerd worden onder **VPN and Remote Access > Remote Access Control**.

Configuratie optie	Wat doet het	Wat in te vullen
Profile name	Een herkenbare naam voor de verbinding	Naam van de verbinding. Naar eigen inzicht.
Enable this profile	Schakelt het VPN profiel in	Aanvinken
VPN Dial-Out Through	Geeft aan via welke WAN verbinding de GRE tunnel opgezet moet worden	De WAN interface die via de 4G verbinding gaat
Tunnel mode	Stelt de VPN tunnel in als zijnde GRE tunnel	GRE Tunnel
Tunnel Local IP	Configureert het lokale IP adres van de router binnen de GRE tunnel	IP adres klanzijde (Zie IRMA)
Tunnel Remote IP	Stelt het IP adres van de andere zijde van de GRE verbinding in	IP adres klanzijde + 1
Local WAN IP	Bepaalt met welke source het VPN pakket verstuurd wordt	LTE IP adres (Zie IRMA)
Remote WAN IP	Zet een verbinding op naar het hier opgegeven IP adres	172.31.255.20 voor KPN 172.31.255.9 voor Vodafone en T-Mobile Zie IRMA
Remote Network IP	Het GRE adres van de remote zijde	Zelfde als Peer GRE IP
Remote Network Mask	Subnet voor de GRE remote	255.255.255.255 / 32
Local Network IP	Het GRE adres van de lokale tunnel	Zelfde als My GRE IP
Local Network Mask	Subnet voor de lokale zijde van de GRE tunnel	255.255.255.255 / 32

Let op: schakel in het menu **VPN and Remote Access > LAN to LAN** de optie 'Pass packets from LAN in Routing mode to VPN' in als deze beschikbaar is.

Change default route to ▼

Pass packets from LAN in Routing mode to VPN

Pass Packets to WAN when VPN disconnects

BGP Prepending (optioneel: alleen bij back-up verbindingen)

De DrayTek routers die geschikt zijn voor BGP ondersteunen ook BGP prepending, ook wel AS-path prepending genoemd. Dit is handig wanneer gebruik wordt gemaakt van een tweede WAN verbinding voor bijvoorbeeld een failover/back-up mogelijkheid i.c.m. BGP.

Met prepending kan de prioriteit van een neighbor doorgegeven worden naar de remote kantzijde. Door gebruik te maken van weights kan de router zelf de prioriteit bepalen van de neighbors.

Navigeer naar **Routing >> BGP** en klik op een neighbor welke de hoogste prioriteit moet hebben.

Prepend: Selecteer hier een prioriteit waarbij een lagere waarde beter is dan hoger.

Weight: Selecteer hier een prioriteit waarbij een hogere waarde beter is dan lager.

Routing >> Neighbor Setup

Index 1

Enable

Profile Name:

AS Number: (1~4294967295)

IP Address:

MD5 Auth:

4-Byte As Number

Prepend: Weight:

Note:
Prepend: When exchanging data with neighbor, inform the other party of priority (lower is better).
Weight: When different neighbors lead to the same result, let the router distinguish priority (higher is better).

Ga vervolgens naar de tweede neighbor die als failover/back-up BGP moet fungeren. Hierbij selecteren we een lagere prepend en een hogere weight ten opzichte van de primary BGP neighbor.

Routing >> Neighbor Setup

Index 2

Enable

Profile Name:

AS Number: (1~4294967295)

IP Address:

MD5 Auth:

4-Byte As Number

Prepend: Weight:

Note:
Prepend: When exchanging data with neighbor, inform the other party of priority (lower is better).
Weight: When different neighbors lead to the same result, let the router distinguish priority (higher is better).



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

© 2021 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.