

DrayTek

VPN Passthrough



VPN Passthrough

VPN Passthrough zorgt ervoor dat een DrayTek niet meer luistert naar de VPN pakketjes die binnenkomen op de WAN/xDSL poort van de DrayTek. Het kan voorkomen dat u in uw interne netwerk al een VPN server hebt staan welke gebruikt maakt van PPTP/IPSec of L2TP VPN verbindingen. In dat geval dient u de VPN features op de DrayTek uit te schakelen om ervoor te zorgen dat er geen conflicten optreden.

In deze handleiding leggen wij simpel uit hoe u een DrayTek **VPN Passthrough** kunt maken.

PPTP VPN

In het hoofdmenu van de DrayTek gaat u naar **VPN And Remote Access > Remote Access Control**. Hier schakelt u de **PPTP VPN Service** uit, klik vervolgens op **OK** en reboot de DrayTek.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<input type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPSec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service

Note:
To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT Open Ports or Port Redirection is also configured.

Vervolgens gaat u naar **NAT > Open Ports** om hier de PPTP poort (**TCP 1723**) te openen voor uw interne VPN server. In ons voorbeeld heeft de VPN server een 192.168.1.60 IP-adres.

NAT >> Open Ports >> Edit Open Ports

Index No. 1

<input checked="" type="checkbox"/>	Enable Open Ports
Comment	<input type="text" value="PPTP"/>
WAN Interface	<input type="text" value="WAN1"/>
Source IP	<input type="text" value="Any"/> <input type="text" value="IP Object"/>
Private IP	<input type="text" value="192.168.1.60"/> <input type="button" value="Choose IP"/>

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	<input type="text" value="TCP"/>	<input type="text" value="1723"/>	<input type="text" value="1723"/>	2.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	4.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
5.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	6.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
7.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	8.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
9.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	10.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

IPSec VPN

In het hoofdmenu van de DrayTek gaat u naar **VPN And Remote Access > Remote Access Control**. Hier schakelt u de **IPSec VPN Service** uit, klik vervolgens op **OK** en reboot de DrayTek.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input type="checkbox"/>	Enable IPSec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service

Note:
To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT Open Ports or Port Redirection is also configured.

OK Clear Cancel

Vervolgens gaat u naar **NAT > Open Ports** om hier de IPSec (**UDP500**) en NAT-T (**UDP4500**) te openen voor uw interne VPN server. In ons voorbeeld heeft de VPN server een 192.168.1.60 IP-adres.

NAT >> Open Ports >> Edit Open Ports

Index No. 1

Enable Open Ports

Comment: IPSec

WAN Interface: WAN1

Source IP: Any **IP Object**

Private IP: 192.168.1.60

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	UDP	500	500	2.	UDP	4500	4500
3.	TCP/UDP	0	0	4.	TCP/UDP	0	0
5.	TCP/UDP	0	0	6.	TCP/UDP	0	0
7.	TCP/UDP	0	0	8.	TCP/UDP	0	0
9.	TCP/UDP	0	0	10.	TCP/UDP	0	0

OK Clear Cancel

Als de IPSec verbinding PKI beveiliging gebruikt in plaats van Preshared Key zal de **“Always pass inbound fragmented large packets (required for certain games and streaming)”** in de Firewall Setup aangevinkt moeten om deze pakketten door te laten.

Firewall >> General Setup

General Setup

General Setup Default Rule

Call Filter Enable Start Filter Set Set#1 ▼
 Disable

Data Filter Enable Start Filter Set Set#2 ▼
 Disable

Always pass inbound fragmented large packets (required for certain games and streaming)

Enable Strict Security Firewall

Block routing connections initiated from WAN IPv4 IPv6

L2TP VPN

In het hoofdmenu van de DrayTek gaat u naar **VPN And Remote Access > Remote Access Control**. Hier schakelt u de **L2TP VPN Service** uit, klik vervolgens op **OK** en reboot de DrayTek.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

- Enable PPTP VPN Service
- Enable IPsec VPN Service
- Enable L2TP VPN Service**
- Enable ISDN Dial-In

Vervolgens gaat u naar **NAT > Open Ports** om hier de **L2TP** poort (**UDP 1701**) te openen voor uw interne VPN server. In ons voorbeeld heeft de VPN server een 172.16.1.60 IP-adres.

NAT >> Open Ports >> Edit Open Ports

Index No. 1

Enable Open Ports

Comment: IPsec

WAN Interface: WAN1

Source IP: Any **IP Object**

Private IP: 192.168.1.60

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	UDP	1701	1701	2.	TCP/UDP	0	0
3.	TCP/UDP	0	0	4.	TCP/UDP	0	0
5.	TCP/UDP	0	0	6.	TCP/UDP	0	0
7.	TCP/UDP	0	0	8.	TCP/UDP	0	0
9.	TCP/UDP	0	0	10.	TCP/UDP	0	0

IPSec VPN limitations

1. IPSec with Authentication Header (AH) cannot pass through NAT because AH does not allow changing the IP header
2. To pass through multiple outgoing IPSec tunnels, it requires that both the VPN client and server support NAT-Traversal (NAT-T). Without NAT-T, it only allows one outgoing IPSec VPN at the same time.
3. L2TP with IPSec policy is in transport mode, which can only pass through NAT if both VPN client and server support NAT-T (Note: All Vigor Router support NAT-T).

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

© 2020 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.