DrayTek

# VPN Passthrough

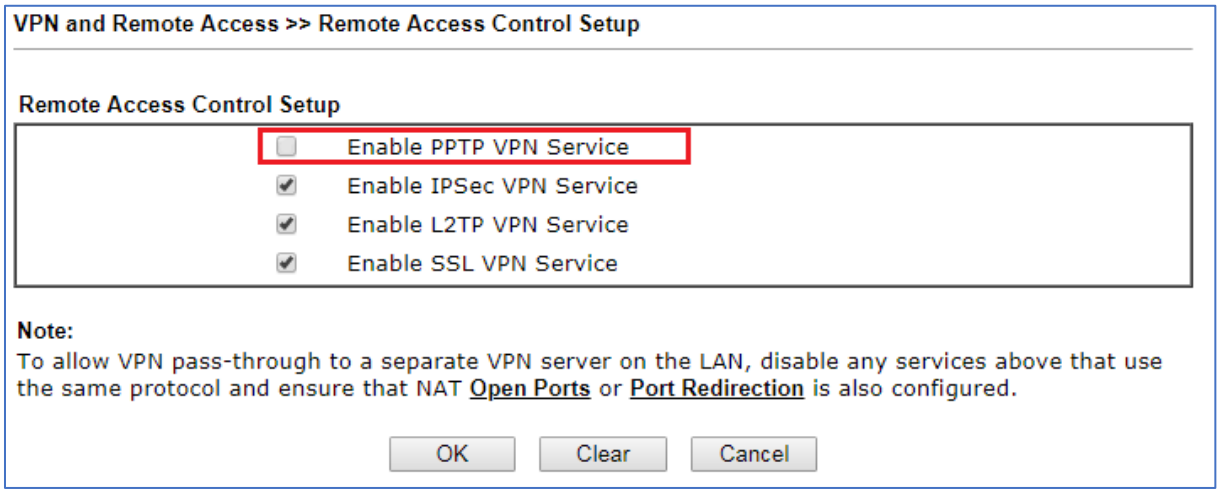
## VPN Passthrough

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.

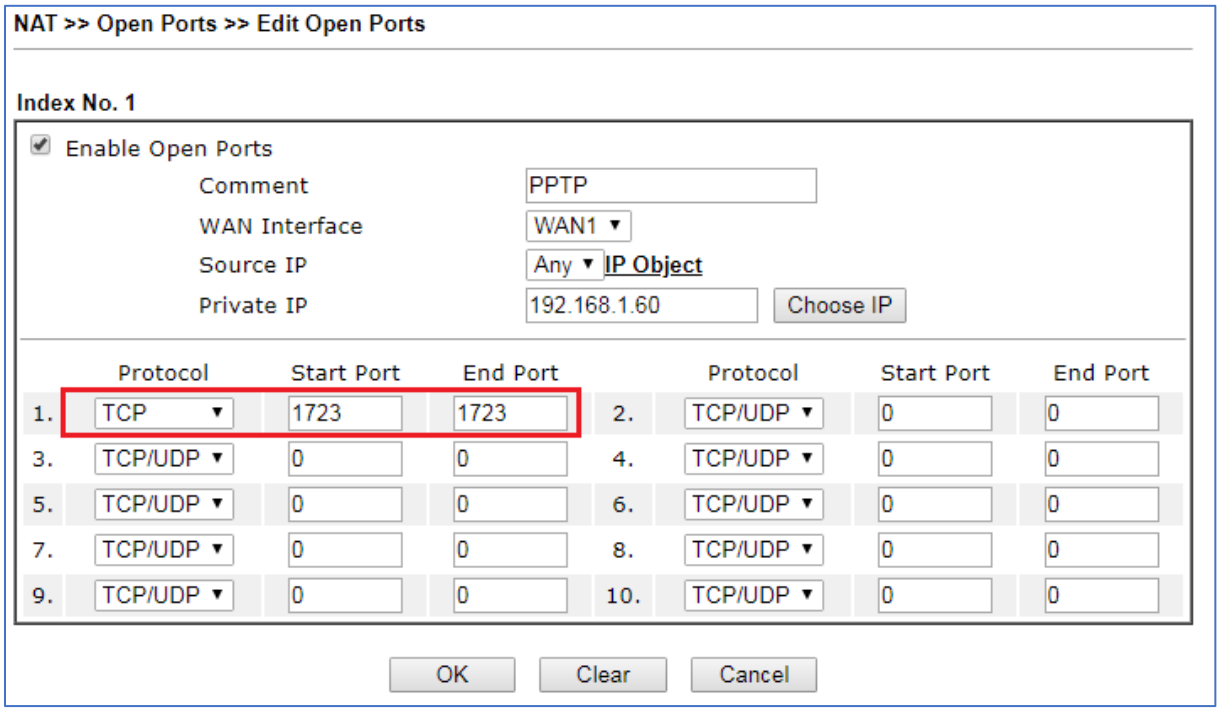
In deze handleiding leggen wij simpel uit hoe u een DrayTek **VPN Passthrough** kunt maken.

## 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.

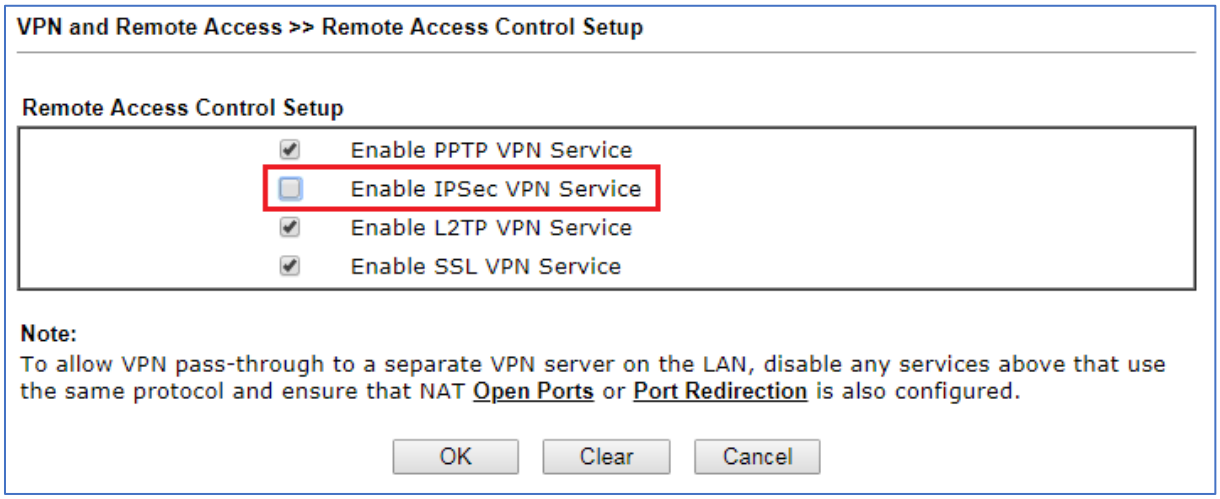



Vervolgens gaat u naar **NAT > Open Ports** om hier de PPTP poort (**TCP 1723**) te openen voor uw interne VPN server. In ons voorbeeld heeft de VPN server een 192.168.1.60 IP-adres.

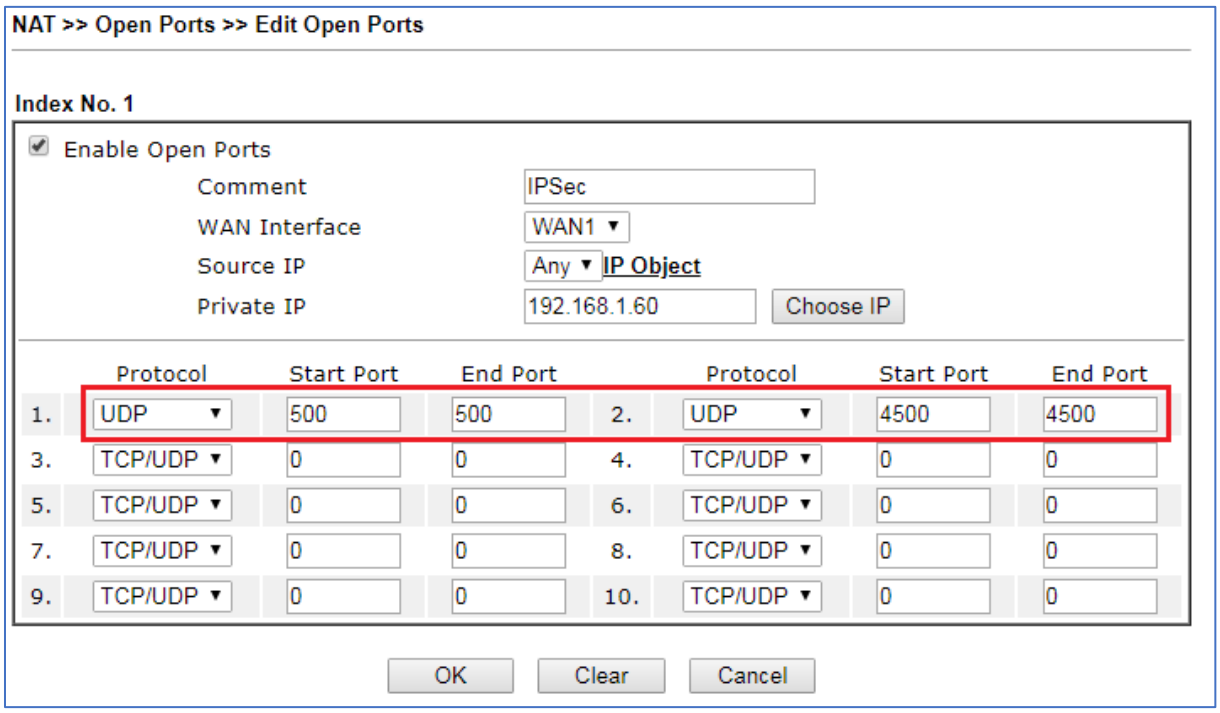


## IPSec VPN

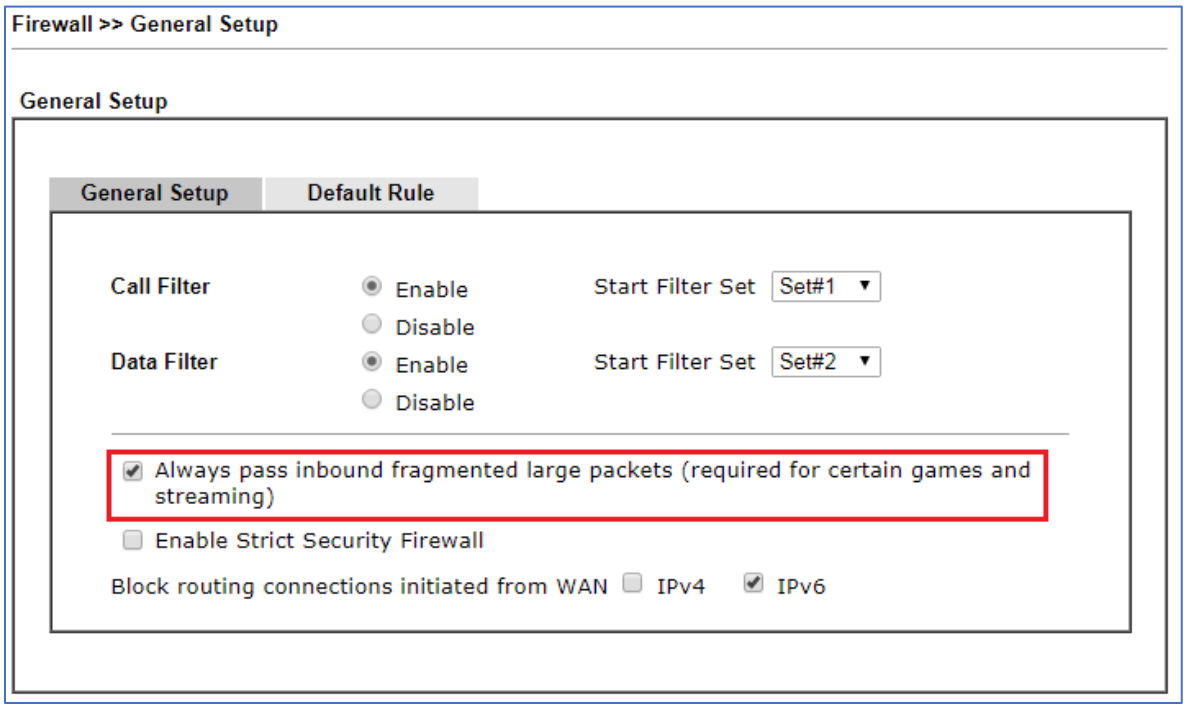
In het hoofdmenu van de DrayTek gaat u naar **VPN And Remote Access > Remote Access Control.** Hier schakelt u de **IPSec VPN Service** uit, klik vervolgens op **OK** en reboot de DrayTek.




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.

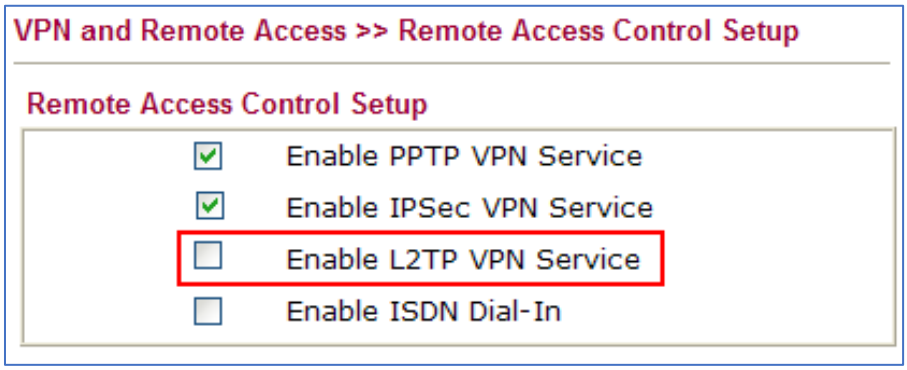


Als de IPSec verbinding PKI beveiliging gebruikt in plaats van Preshared Key zal de "**Always pass inbound fragmented large packets (required for certain games and streaming)"** in de Firewall Setup aangevinkt moeten om deze pakketten door te laten.

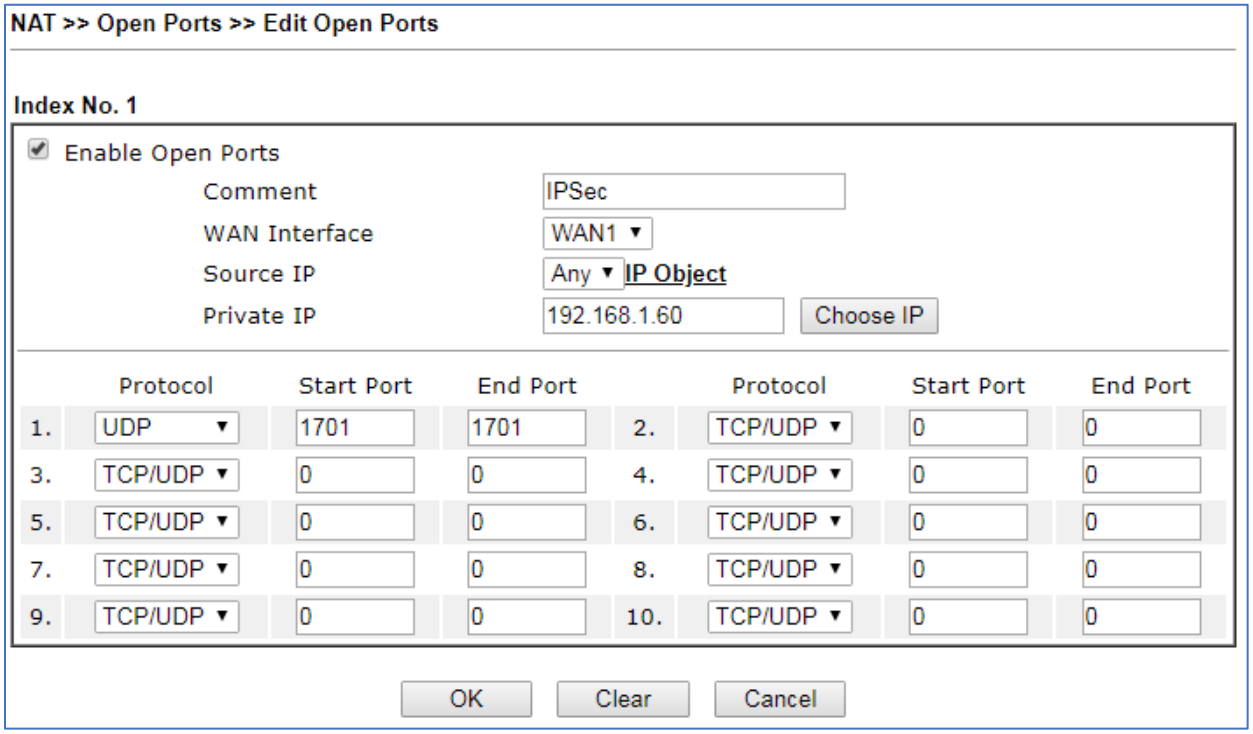


## L2TP VPN

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.




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.



**IPSec VPN limitaties**

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.