DrayTek

DrayTek Firewall

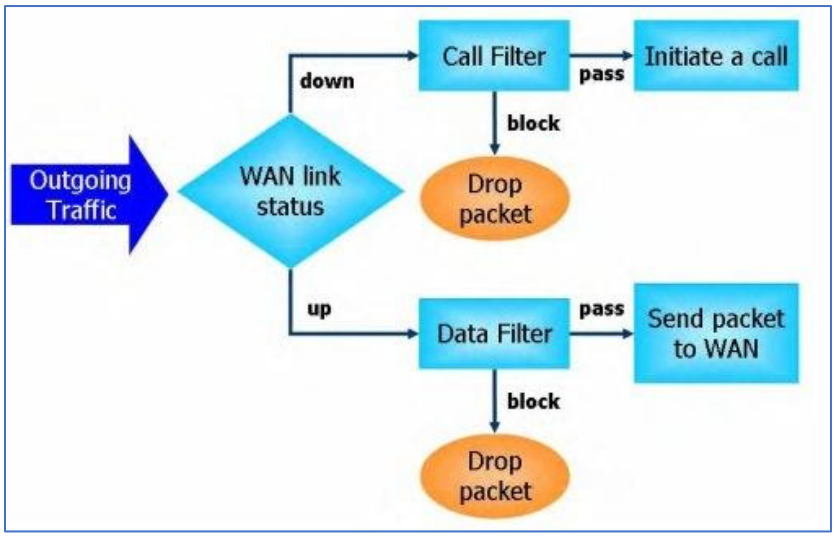
Hoe werkt de DrayTek Firewall?

In deze handleiding zullen wij de werking van de DrayTek Firewall uitleggen.
Een DrayTek modem/router wordt standaard uitgeleverd met een default firewall setup. In deze default firewall setup staan een Default Call en Default Data filter. In beide Filter sets staat een Firewall regel die uitgaand NetBios verkeer blokkeert. Al het andere verkeer wordt in deze standaard firewall configuratie toegestaan.

Default Call en Data Filter

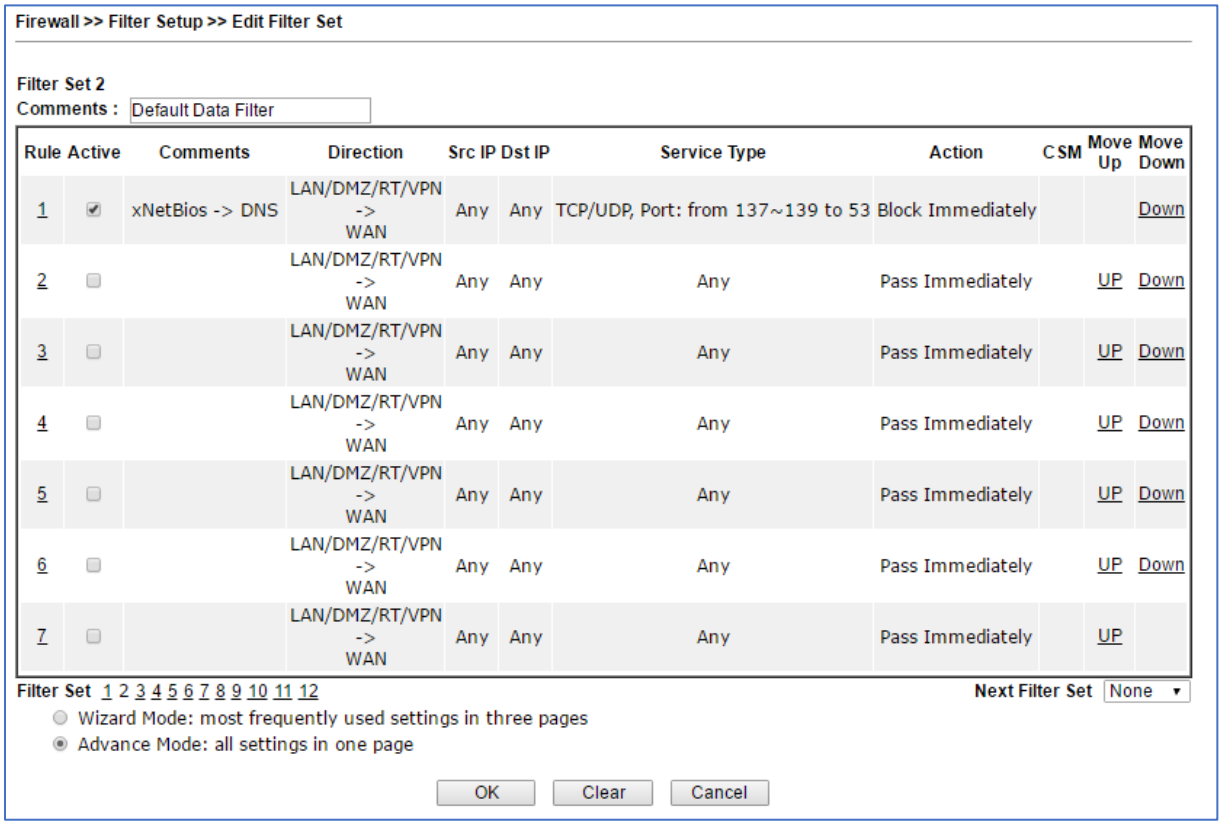
Afhankelijk van de WAN link zal de DrayTek kijken naar de Call en Data Filter. Wanneer een actieve internet verbinding wordt aangesloten op de DrayTek is de Default Call Filter niet te gebruiken. Wij adviseren daarom om geen Firewall regels in de Default Call Filter te plaatsen, deze zullen bij een actieve internet verbinding niet functioneren.

Omdat de WAN verbinding altijd online/actief is, zal de DrayTek gebruik maken van de Default Data Filter. Firewall regels die in deze set worden geplaatst, zijn actief indien juist geconfigureerd.



Default Data Filter

Zoals aangegeven is de Default Data Filter de eerste Filter Set welke u kunt gebruiken voor het inrichten van de firewall. Omdat de 1e firewall regel al in gebruik is kunt u hier tot 6 extra firewall regels aanmaken.



Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2
Comments : Default Data Filter

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	☑	xNetBios -> DNS	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53	Block Immediately			Down
2	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12 Next Filter Set None

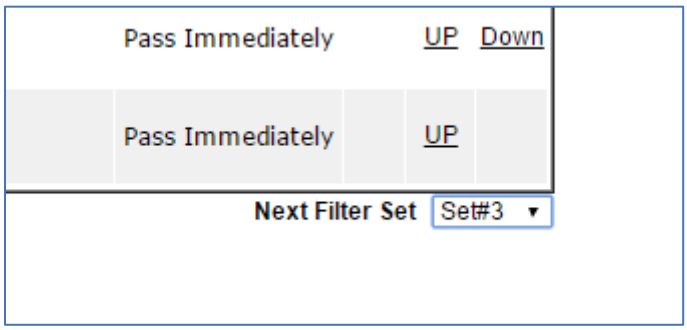
Wizard Mode: most frequently used settings in three pages
Advance Mode: all settings in one page

OK Clear Cancel

Filter Set 3 of hoger

Wanneer u Filter Set 3 of hoger wilt gebruiken dient u de Next Filter Set op te geven.

De firewall van de DrayTek stopt standaard na de Default Data Filter. U dient in de Default Data Filter bij 'Next Filter Set' aan te geven welke Filter set u nog meer wilt gebruiken. In onderstaand voorbeeld zal de DrayTek Firewall ook Filter Set 3 meenemen.



	Pass Immediately		UP	Down
	Pass Immediately		UP	

Next Filter Set Set#3

Direction

Bij het aanmaken van een Firewall regel is de Direction van essentieel belang, hier geeft u namelijk aan of de firewall regel bedoelt is voor inkomend/uitgaand of intern verkeer.

LAN/DMZ/RT/VPN → WAN:

Firewall regel op basis van uitgaand verkeer. Hierbij is de Source een intern adres (LAN/DMZ/RT/VPN) en de Destination een extern adres (WAN).

WAN → LAN/DMZ/RT/VPN:

Firewall regel op basis van inkomend verkeer. Hierbij is de Source een extern WAN adres en de Destination een intern adres (LAN/DMZ/RT/VPN)

LAN/DMZ/RT/VPN → LAN/DMZ/RT/VPN:

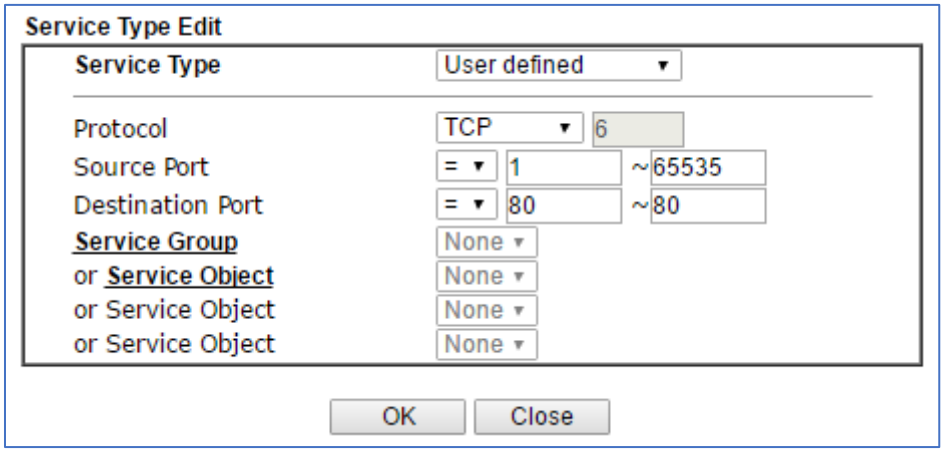
Firewall regel op basis van intern verkeer. Hierbij is je Source en Destination een intern adres (LAN/DMZ/RT/VPN).

Advanced: U kunt hier aangeven voor welke LAN of WAN interface u een Firewall regel wilt aanmaken. Standaard zijn alle interfaces ingeschakeld zodat de firewall regel voor elke interface actief is.

Service Type

Bij het creëren van een Firewall regel dient u er rekening mee te houden dat de Source Port een Pseudo poort is. Een Pseudo poort is een poort die de DrayTek koppelt aan een inkomende en uitgaande sessie. Deze is nooit hetzelfde waardoor het niet mogelijk is om de Source Port te definiëren. Advies is om deze default op 1 t/m 65535 te laten staan.

Wanneer u bijvoorbeeld uitgaand poort 80 wil blokkeren zal de Service Type er als volgt uitzien :



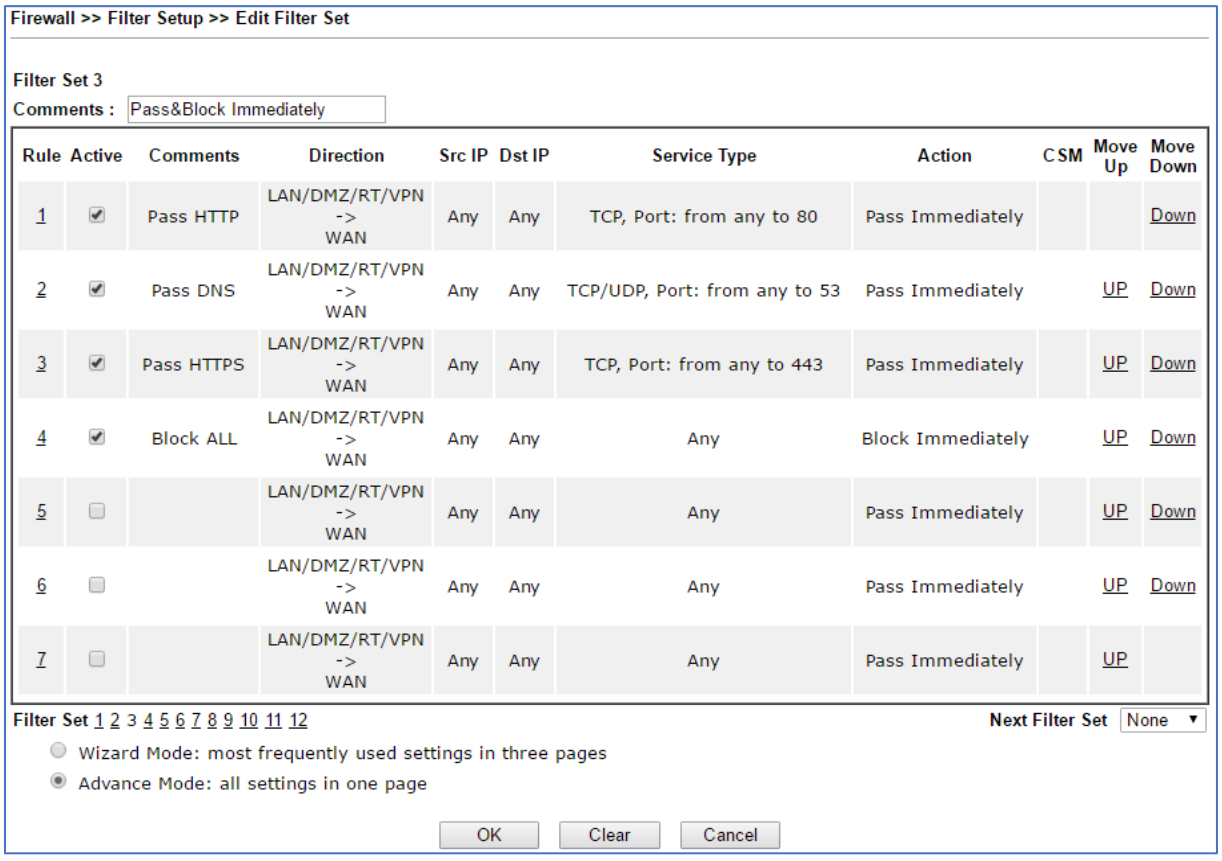
Block Immediately of Block if no further match ?

De keuze voor 'Block Immediately' of 'Block if no further match' is geheel aan u. Met beide mogelijkheden kunt u de gewenste firewall setup bereiken. Het gedrag van beide mogelijkheden verschilt wel enigszins.

Block Immediately: De firewall regel die u aanmaakt zal geblokkeerd worden, indien u hierop een uitzondering wil maken dient u een Pass regel aan te maken die boven deze regel komt te staan. Er zal niet naar volgende regels gekeken worden. De uitvoering van de firewall stop als verkeer een hit op een regel met deze actief heeft.

In geval van een Block Immediately zal een Firewall setup er als volgt uit komen te zien :

Pass Immediately (HTTP)
Pass Immediately (DNS)
Pass Immediately (HTTPS)
Block Immediately (ALL)



Firewall >> Filter Setup >> Edit Filter Set

Filter Set 3
Comments : Pass&Block Immediately

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	☑	Pass HTTP	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP, Port: from any to 80	Pass Immediately			Down
2	☑	Pass DNS	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from any to 53	Pass Immediately		UP	Down
3	☑	Pass HTTPS	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP, Port: from any to 443	Pass Immediately		UP	Down
4	☑	Block ALL	LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Block Immediately		UP	Down
5	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12 Next Filter Set None

Wizard Mode: most frequently used settings in three pages
Advance Mode: all settings in one page

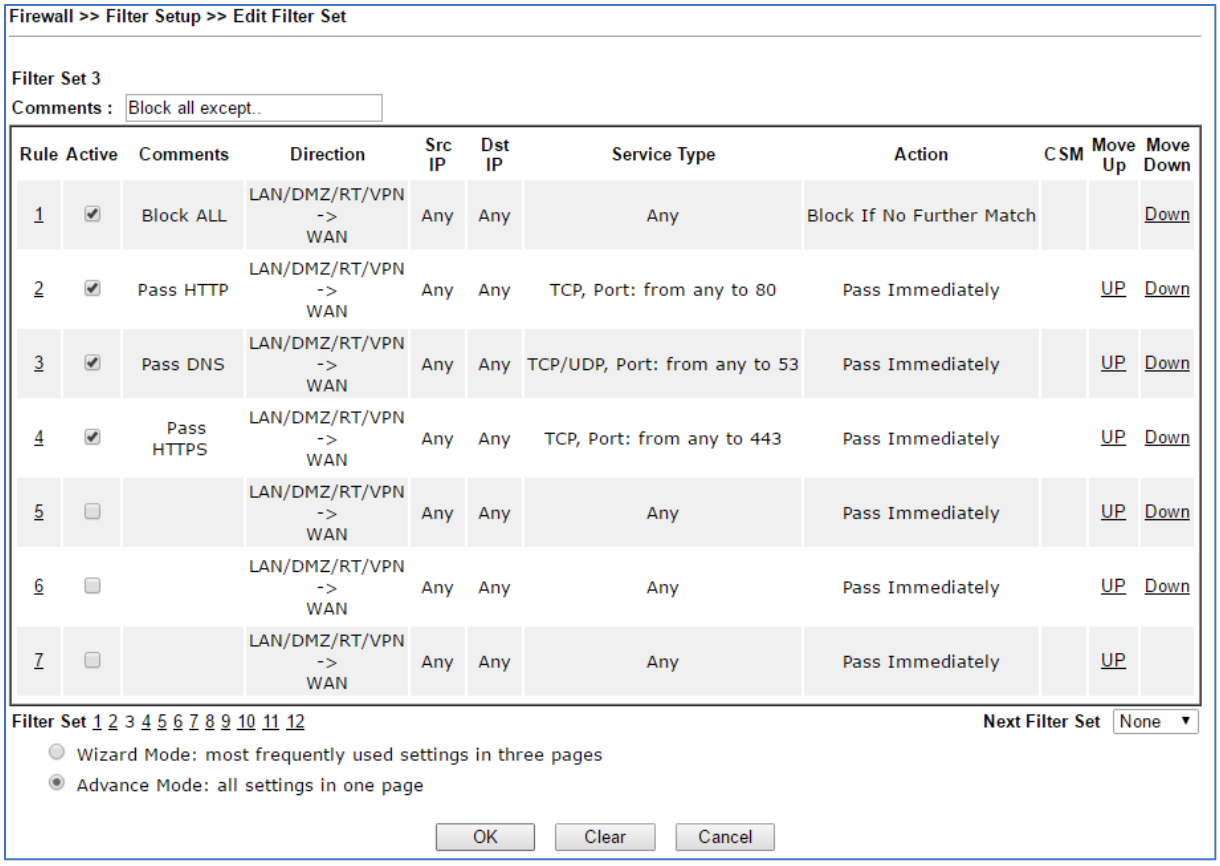
OK Clear Cancel

In bovenstaande setup is alleen HTTP/HTTPS en DNS verkeer mogelijk. De laatste firewall regel zorgt ervoor dat al het overige verkeer geblokkeerd wordt.

Block if no further match: Verkeer dat aan de criteria in de firewall regel voldoet wordt geblokkeerd, tenzij een pass regel gedefinieerd is. Indien verkeer toegestaan moet worden kan een opvolgende firewall regel aangemaakt worden waarin specifiek verkeer toegestaan kan worden.

In geval van een Block if no further match zal een Firewall setup er als volgt uit komen te zien :

Block if no further match (ALL)
Pass Immediately (HTTP)
Pass Immediately (DNS)
Pass Immediately (HTTPS)



In bovenstaande setup zal al het uitgaande verkeer geblokkeerd worden behalve als het verkeer voldoet aan de criteria in de Pass regels die eronder worden gezet. In dit geval worden HTTP, DNS en HTTPS toegestaan.

Wij adviseren in deze om altijd te starten met een Block if no further match regel. Op die manier is eenvoudig(er) te testen of de gewenste blokkade actief is. Vervolgens kunnen pass regels gemaakt worden en is direct te testen of deze correct werken.

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.