DrayTek

DoS Defense & Spoofing Defense

Inhoudsopgave

DoS Defense 3
Spoofing Defense 5
ARP Spoofing Defense 5
IP Spoofing Defense 6
Syslog 7
Syslog Utility 7
Syslog Explorer 8

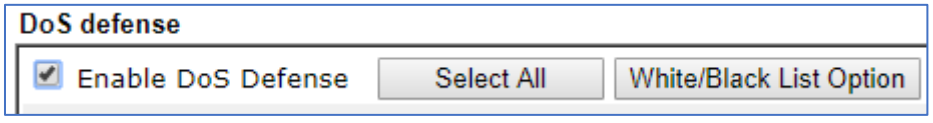
DoS Defense

De functie DoS Defense (Denial of Service) helpt u met het detecteren en verminderen van DoS aanvallen. Deze aanvallen zijn over het algemeen op te delen in 2 types, 'Flooding-Type Attacks' en 'Vulnerability Attacks'. De 'Flooding-type Attacks' zullen proberen uw systeembronnen te vernielen, terwijl 'Vulnerability Attacks' uw systeem probeert te besmetten.

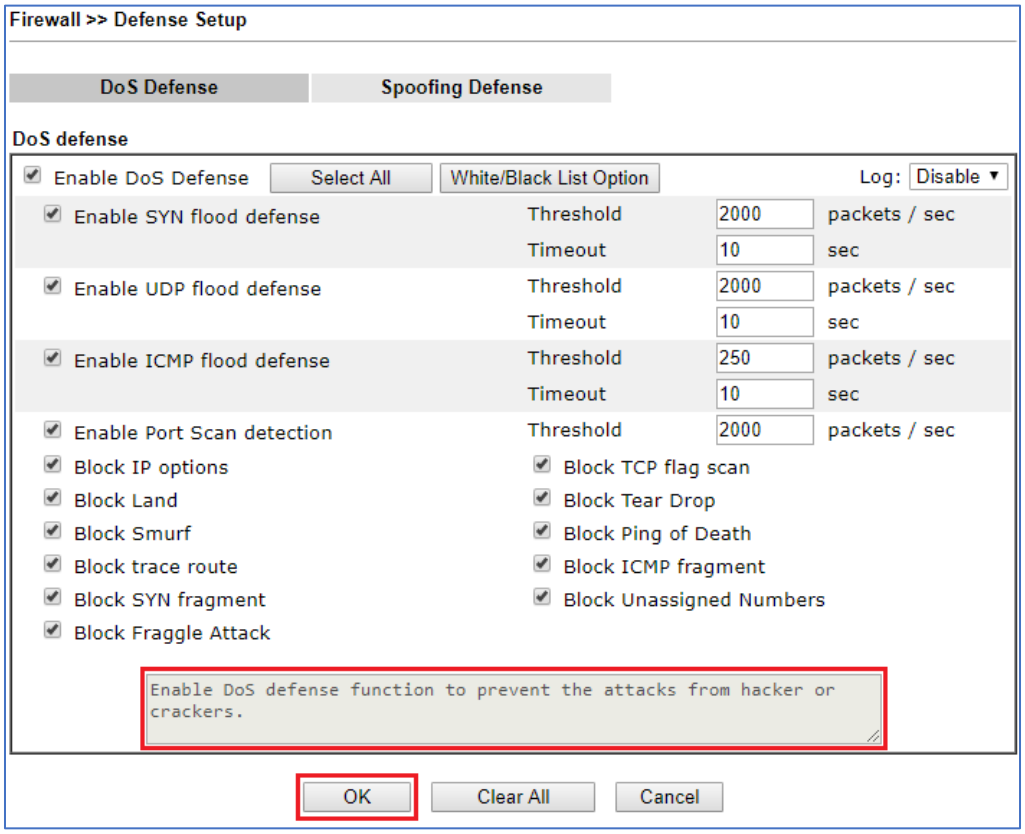
De DoS Defense functie zorgt ervoor dat de DrayTek Vigor router al het inkomend verkeer controleert op grond van de 'Attack signature database'. Elk verdacht pakketje dat zich misschien kan vermenigvuldigen om zo het systeem te besmetten, zal worden geblokkeerd. Wanneer er pakketjes worden geblokkeerd zal de DrayTek een waarschuwingsbericht versturen. Deze melding kunt u alleen zien wanneer u de Syslog server hebt ingeschakeld. De Vigor zal tevens al het verkeer monitoren, wanneer er abnormaal verkeer wordt gesignaleerd, zal de Vigor dit voorkomen.

De volgende **'Attack types'** kan de **DoS/DDoS Defense** detecteren:
1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. TCP Flag scan
5. Trace route
6. IP options
7. Unassigned Numbers
8. Land attack
9. Smurf attack
10. SYN fragment
11. ICMP fragment
12. Teardrop attack
13. Fraggle attack
14. Ping of Death attack
15. TCP/UDP port scan

U gaat voor deze functie naar 'Firewall >> DoS Defense' in het hoofdmenu van de DrayTek en vinkt hier 'Enable DoS Defense' aan.

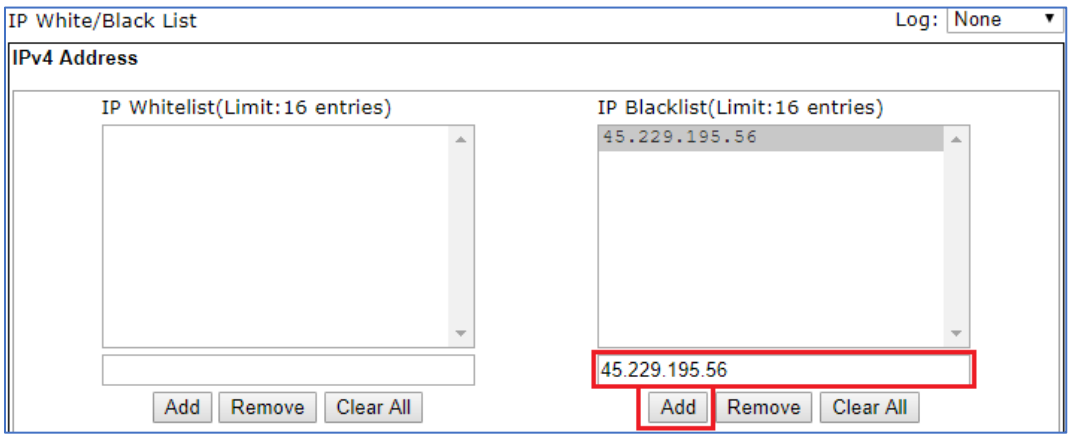


Vervolgens kunt u zelf selecteren van welke beveiliging opties u gebruik wilt maken. Telkens als u een optie selecteert zal in het onderstaande balkje een beschrijving te voorschijn komen.



Vergeet na het instellen niet op **'Ok'** te drukken anders worden de instellingen niet opgeslagen.

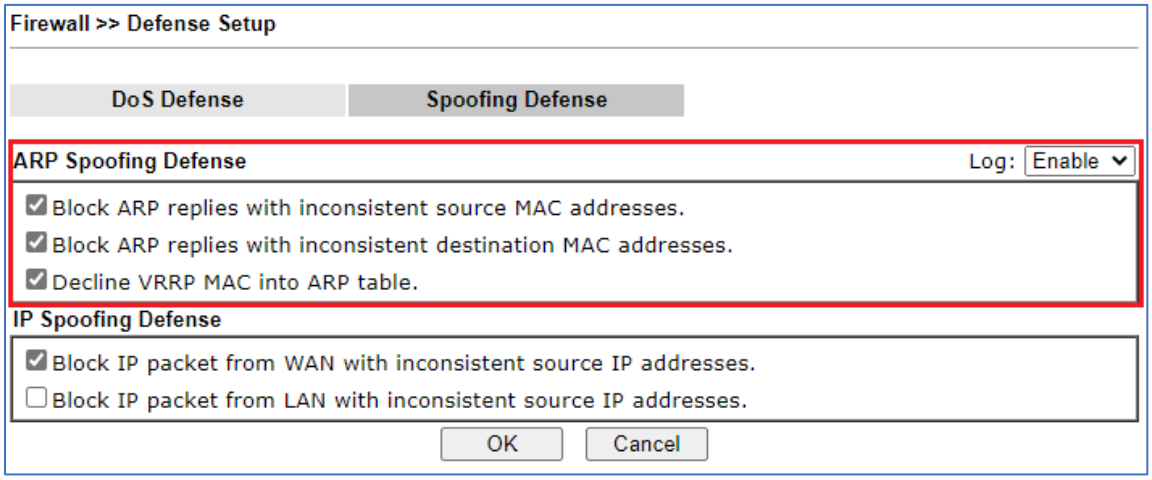
U hebt ook de mogelijkheid om bepaalde IP adressen door de DrayTek wel of niet laten controleren op ongewenste pakketjes. Klik hiervoor bovenaan op **White/Black List Option**. De Whitelist is om bepaalde IP adressen niet te laten controleren en de Blacklist juist wel.



Spoofing Defense

ARP Spoofing Defense

Het Address Resolution Protocol (ARP) heeft vanwege zijn staatloosheid en het ontbreken van een authenticatie-mechanisme voor het verifiëren van de identiteit van de afzender een lange geschiedenis van kwetsbaarheid voor spoofing-aanvallen. ARP-spoofing is soms het startpunt voor meer geavanceerde LAN-aanvallen zoals denial of service, man in the middle en sessie-kaping. ARP Spoofing Defense is een passieve benadering, waarbij het ARP-verkeer wordt bewaakt en er wordt gezocht naar inconsistenties in de toewijzing van Ethernet naar IP-adressen.



Block ARP replies with inconsistent source MAC addresses

De DrayTek blokkeert ARP antwoorden van niet overeenkomende bron MAC-adressen. Deze optie staat standaard aan.

Block ARP replies with inconsistent destination MAC addresses

De DrayTek blokkeert ARP antwoorden van niet overeenkomende bestemming MAC-adressen. Deze optie staat standaard aan.

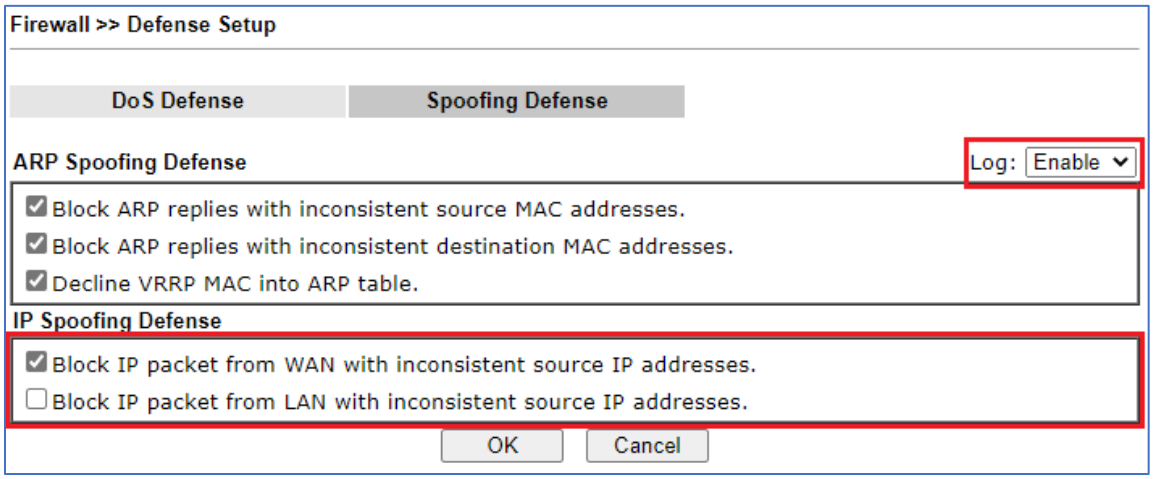
Decline VRRP MAC into ARP table

De DrayTek negeert standaard virtuele IP- en MAC-adressen van VRRP zoals sommige cluster PCs of Firewalls zodat ze niet worden vermeld in de ARP-tabel van de DrayTek. Wanneer u deze functie uitschakelt zal de Vigor Router VRRP accepteren en registreren in de ARP tabel.

Spoofing Defense

IP Spoofing Defense

IP-spoofing is een methode dat een hacker met een aantal tools misbruik kan maken van het netwerk om het oorspronkelijke adres in de IP-header te wijzigen. Zodoende het ontvangende system/apparaat te laten denken dat het pakket afkomstig is van een vertrouwde bron, zoals een andere computer op een lokaal netwerk, en het te accepteren. De Vigor Router ondersteunt IP Spoofing Defense om dergelijke spoofing-gebeurtenissen te voorkomen.



Block IP packet from WAN with inconsistent source IP addresses.
Blokkeert een IP-pakket van WAN met niet-overeenkomend bron-IP-adres(sen). Tijdens het ontvangen van pakketten van WAN, zal de DrayTek controleren of het bron-IP-adres en de WAN-interface aannemelijk is. Als dit niet het geval is, zal DrayTek het pakket laten vallen in plaats van het door te sturen naar het interne netwerk.

Block IP packet from LAN with inconsistent source IP addresses
Blokkeer IP-pakket van LAN met niet overeenkomend bron-IP-adres(sen). Bij het ontvangen van pakketten van LAN, zal de DrayTek controleren of het bron IP-adres en de afkomstige LAN-interface aannemelijk is. Als dit niet het geval is, zal DrayTek het pakket laten vallen en dit in Syslog registreren.

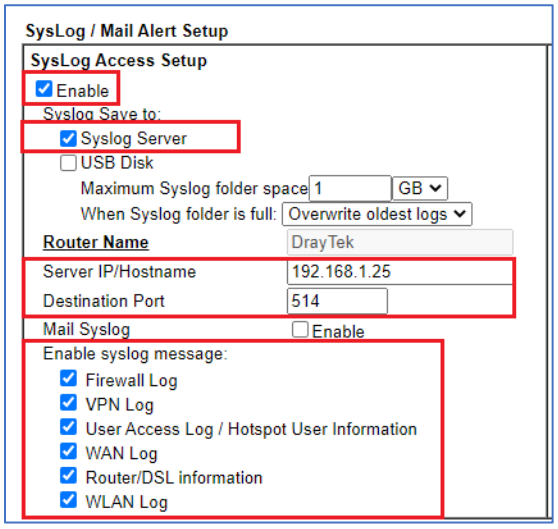
Log Enable
Zal de Spoofing Defense in Syslog registeren. Bijvoorbeeld op IP Spoofing: Als het IP-adres van het LAN-netwerk van de DrayTek bijvoorbeeld 192.168.1.1 is en het ontvangt een packet van WAN met het bron-IP 192.168.1.100, laat DrayTek het pakket vallen en zal dit in Syslog worden geregistreerd. Onderstaand een voorbeeld melding die terug te vinden is in Syslog: *[IP Spoofing Defense] Block-packet from WAN with source IP: 192.168.1.100*

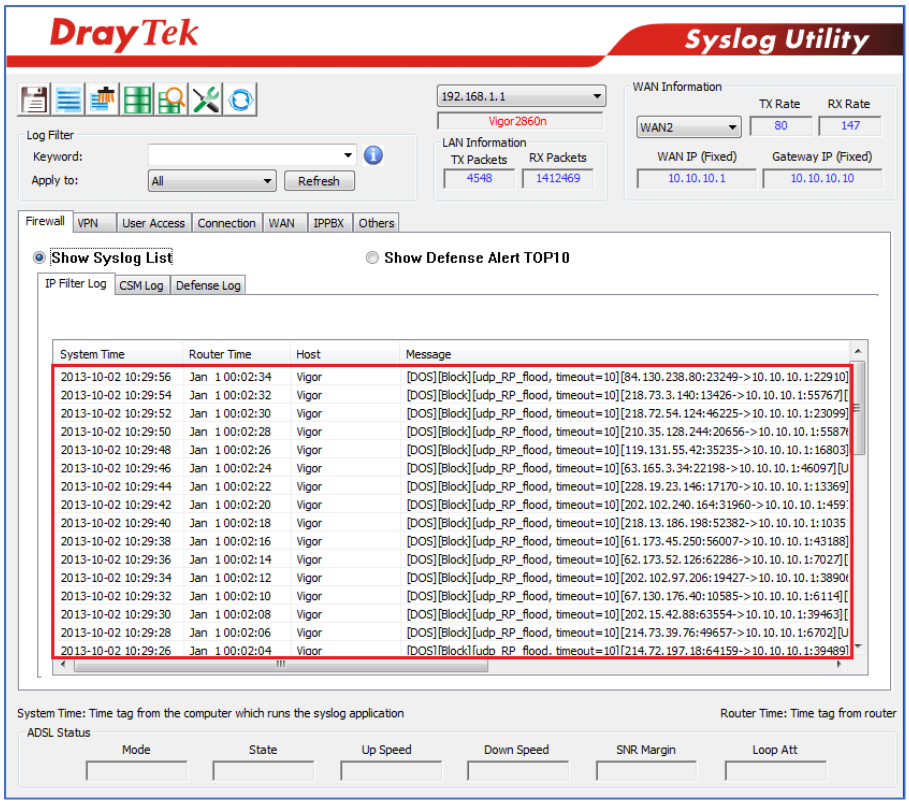
Syslog

Wanneer Log Enable is ingeschakeld worden alle DoS Defense & Spoofing Defense meldingen in Syslog geregistreerd. Syslog kunt u vervolgens op 2 manieren terug vinden in de DrayTek:

Syslog Utility

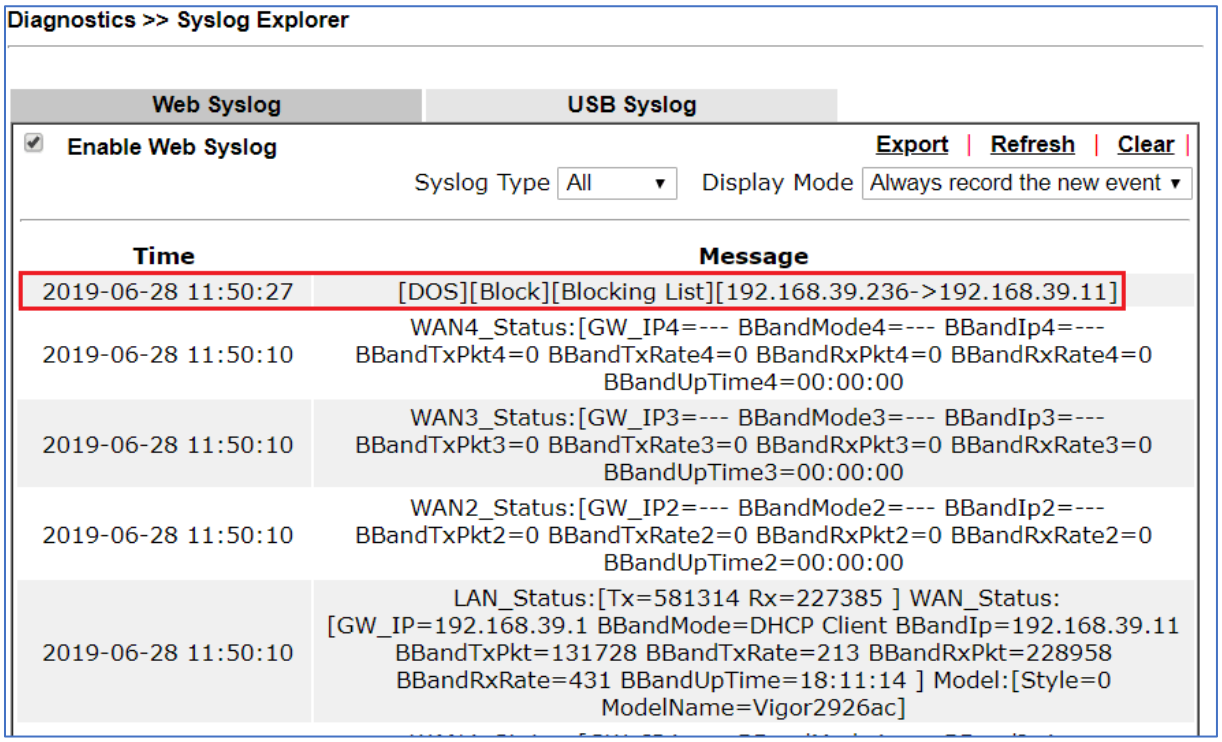
Deze software tool is gratis te downloaden op www.draytek.nl. Bij gebruik van deze tool is het belangrijk om de firewall van uw PC/server zo te configureren dat de tool wordt toegestaan, een standaard Windows firewall blokkeert deze tool namelijk.





Syslog Explorer

Syslog Explorer is een live-view Syslog tool welke terug te vinden is in het Diagnostics menu van de DrayTek. In deze tool is een beperkte hoeveelheid live logging terug te vinden.



Meer informatie over Syslog kunt u vinden op onze website.

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.