Draytek 2820 VN annex A (50 EUR)

Locatie **Utrecht, Nieuwegein**
https://www.advertentiex.nl/x-321723-z

Wegen overstap van ADSL naar kabel internet biedt ik mijn ADSL modem en router te koop aan.

Productinformatie:

De Draytek V2820 heeft behalve een ingebouwd ADSL modem, ook nog een 2e WAN poort voor een extra internetverbinding. Tevens is deze modem de eerste modem met een Gigabit LAN poort. Al met al een uniek product!

Uniek aan de DrayTek Vigor 2820 is dat deze beschikt over een DSL poort en een ethernet WAN poort. Hiermee is de Vigor 2820 geschikt voor ADSL2+, kabel- en glasvezelverbindingen. Door 'second WAN', de tweede WAN poort, kan Load Balancing, Bandwidth on Demand en WAN connection fail-over worden toegepast.
De Vigor 2820 ondersteunt 32 simultane VPN verbindingen en heeft een USB printerpoort. De router beschikt over een Gigabit LAN poort, voor een snellere dataoverdracht binnen het netwerk. De volledige Vigor 2820 serie bestaat uit vijf verschillende modellen, met varianten voor VoIP en wireless (802.11n draft 2.0).

- Ingebouwd modem voor ADSL over een analoge telefoonlijn
- Tweede WAN poort naast een ingebouwd ADSL modem
- Gigabit LAN op één van de vier LAN poorten
- Bandwidth Management voor optimaal gebruik van het internet
- Quality of Service om voorrang te geven voor bepaalde poorten of gebruikers
- VPN voor maximaal 32 gelijktijdige VPN tot maximaal 32 gelijktijdige IPSec VPN tunnels
- Geavanceerde firewall met Statefull Packet Inspection

Second WAN
Dit model beschikt naast een ADSL modem over een tweede ethernet WAN poort. Als er gebruik gemaakt wordt van meerdere WAN poorten kan load balancing en fail-over worden toegepast. Door gebruik te maken van beide poorten op de router worden de netwerkprestaties, de schaalbaarheid en de betrouwbaarheid van de internetverbinding verbeterd

Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z

Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z
Draytek 2820 VN annex A
https://www.advertentiex.nl/x-321723-z

Load-balancing
Als er gebruik gemaakt wordt van beide WAN poorten kan load-balancing worden toegepast. Voor elke datastroom kan gedefinieerd worden over welke WAN poort het verkeer naar buiten gaat.

Onderstaand enkele voorbeelden van toe te passen load-balancing regels.
Regulier internetverkeer en uitgaande e-mail afkomstig van de mailserver dient te verlopen over WAN poort 1.
VoIP verkeer dient te verlopen over WAN poort 2.

Er kunnen 20 load-balancing regels aangemaakt worden.
Met de functie "auto weight" bepaalt de router zelf wanneer deze overgaat naar de andere WAN interface. Ook is het mogelijk om zelf in te stellen, dat als een bepaalde bandbreedte verbruikt wordt, de 2e WAN interface automatisch ingeschakeld wordt. Zo is het mogelijk om bijvoorbeeld regulier internetverkeer en uitgaande email afkomstig van de mailserver te laten verlopen over WAN poort 1. VoIP verkeer dient dan te verlopen over WAN poort 2.
Ook kan QoS toegepast worden op beide WAN poorten.

Fail-over
Op beide WAN poorten kan "fail-over/backup" worden toegepast. Als één van de twee WAN poorten uitvalt, neemt de andere WAN poort de taken over. Op deze manier is er dus altijd een werkende internetverbinding. Als de weggevallen verbinding hersteld is, wordt automatisch overgeschakeld naar de herstelde verbinding. De gebruikers merken nagenoeg niets van deze overschakeling.

Gigabit LAN
Één van de vier LAN poorten is een gigabit LAN poort. Deze gigabit LAN poort zorgt voor een snellere dataoverdracht. De poort kan bijvoorbeeld worden gebruikt voor een uplink naar een gigabit switch.

Bind IP to MAC
Met de functie 'Bind IP to MAC' wordt een IP adres gekoppeld aan het MAC adres van een netwerkapparaat.

Het is lastig om firewall regels toe te passen op IP adressen die continu veranderen. Wanneer de PC automatisch een IP adres krijgt toegewezen van de router dan is dit een willekeurig adres. Doordat het IP adres verandert, is het dus niet mogelijk firewall regels of port forwarding toe te passen. De functie Bind IP to MAC zorgt ervoor dat de PC altijd hetzelfde IP adres krijgt toegewezen. Dit gebeurt op basis van het MAC adres van de netwerkaart in de PC. Doordat de PC altijd hetzelfde IP adres krijgt, worden automatisch alle firewall regels correct toegepast. Er kunnen 300 IP adressen gekoppeld worden.

De functie "strict bind" voegt extra beveiliging toe aan het netwerk. Als deze functie ingeschakeld wordt, dan krijgen alleen de MAC adressen die zijn gedefinieerd in de Bind IP to MAC lijst toegang tot het

internet.

Wake on LAN
Wake on LAN is een functie om de PC op afstand aan te zetten. De meeste netwerkkaarten ondersteunen dit. Bij Wake on LAN stuurt de router een "Magic Packet" naar het MAC adres van de PC terwijl deze uitstaat. De netwerkkaart herkent het signaal en zal de computer opstarten. Deze functie kan gebruikt worden als bijvoorbeeld thuis via een beveiligde VPN tunnel de PC op het werk aangezet moet worden. Vervolgens kan de PC gebruikt worden.

VLAN
Met de VLAN functionaliteit kunt u van alle vier de ethernet aansluitingen een apart netwerk maken. Dit kan betekenen dat niemand op een ander netwerk kan of alleen op een vooraf geselecteerd netwerk. Zo kan het zijn dat twee bedrijven van dezelfde breedbandverbinding gebruik maken, maar niet bij elkaar op het netwerk kunnen.

Bandwidth management

Met bandwidth management kan optimaal gebruik gemaakt worden van de internet verbinding. Deze functie bestaat uit 3 onderdelen:

1) Session limit
Met de session limit functie kan het maximaal aantal sessies per IP adres of groep van IP adressen worden aangegeven. Hiermee wordt voorkomen dat één gebruiker alle beschikbare bandbreedte verbruikt.
bwm-limitsession

2) Bandwidth limit
Met behulp van bandwidth limit kan worden aangegeven hoeveel bandbreedte bepaalde IP adressen mogen gebruiken. Er kan een standaard waarde worden ingesteld. Ook kan een groep van IP adressen gedefinieerd worden. Bandwidth limit is toe te passen op zowel up- als download verkeer.
bwm-limitbandwith

3) Quality of Service
De QoS-functie zorgt ervoor dat datastromen, zowel inkomend als uitgaand, met een bepaalde prioriteit worden behandeld. Er kan bijvoorbeeld per poort of per IP adres de bandbreedte worden aangeven. Quality of Service (QoS) zorgt eveneens voor gegarandeerde VoIP kwaliteit. De toepassing van QoS garandeert dat overige datastromen, zoals HTTP en FTP, geen invloed hebben op de kwaliteit van het telefoongesprek.
bwm-qos

Online statistics
Met behulp van de online statistics kan de bandbreedte per service weergegeven worden. Hier is in één oogopslag te zien hoeveel bandbreedte door een bepaalde service gebruikt wordt.

Traffic graph
Traffic graph geeft in een grafiek een overzicht van de totaal gebruikte bandbreedte die de laatste 24 tot 48 uur verbruikt is.

Data flow monitor
Geeft aan hoeveel bandbreedte er momenteel verbruikt wordt. In dit menu is het tevens mogelijk gebruikers te blokkeren voor een periode van 5 minuten.

VPN

De DrayTek producten beschikken over een geïntegreerde VPN server. Dit model ondersteunt tot 32 IPSec LAN-to-LAN VPN tunnels. Hierdoor kan een VPN tunnel gemaakt worden naar uw netwerk, zonder dat hiervoor een VPN server in het netwerk vereist is. VPN biedt een beveiligde verbinding over het internet naar uw eigen netwerk.

Er zijn verschillende vormen van VPN. DrayTek ondersteunt L2TP, IPSec en PPTP. Van deze protocollen is PPTP de snelste, doch de minst beveiligde vorm van VPN. IPSec biedt een betere beveiliging door een encryptie die continu veranderd. L2TP is, in combinatie met IPSec, de meest veilige vorm van VPN. Helaas is dit ook de reden dat het protocol moeilijk in gebruik is. Momenteel is IPSec de meest gebruikte vorm van VPN.

Beveiliging van de VPN tunnel gebeurt door de verschillende encryptie protocollen. DrayTek ondersteunt DES, 3DES, AES en MPPE. Van deze protocollen is MPPE de meest eenvoudige vorm van encryptie. Deze wordt toegepast bij een PPTP verbinding. DES biedt aanzienlijk meer veiligheid ten opzichte van MPPE. Dit door het verbeterde algoritme dat wordt gebruikt. 3DES is, zoals de naam wellicht doet vermoeden, een 3-voudige DES encryptie. Dit verbetert de beveiliging aanzienlijk. De laatst ontwikkelde encryptie standaard is AES. Dit is de meest veilige vorm van encryptie. Helaas ondersteunen vooral de oudere producten deze standaard niet.

Met de DrayTek routers is het mogelijk twee netwerken transparant te koppelen. Dit kan door gebruik te maken van de LAN-to-LAN VPN. Met deze VPN tunnel wordt de verbinding opgezet tussen 2 routers. Om vanaf een PC verbinding te kunnen maken met het netwerk, kan gebruik gemaakt worden van een Telewerker profiel. DrayTek stelt een gratis programma beschikbaar om ook een veilige telewerker verbinding op te kunnen zetten.

Firewall

Voor betere beveiliging van het netwerk kan gebruik gemaakt worden van de ingebouwde firewall.

Wat doet de firewall?
De firewall kan policy-based toestaan of blokkeren van in- en uitgaand verkeer. Aan de hand van regels kan communicatie van en naar een netwerk verboden of juist toegestaan worden. De router is in staat om firewall toe te passen op basis van IP adres, poort nummer en protocol. Alle firewall regels kunnen ook voor inkomende VPN verbindingen worden toegepast.

Stateful Packet Inspection (SPI)
Doordat de firewall is voorzien van Stateful Packet Inspection (SPI) worden alle pakketten gecontroleerd op "connection state". Als een pakket volgens de firewall regels wordt doorgelaten, dan wordt het ook gecontroleerd op actieve connecties. Zijn er geen actieve connecties, dan zal de router de pakketten alsnog blokkeren.

firewall-filterset

DoS / DDoS defense
De DrayTek router is in staat uw netwerk te beschermen tegen DoS aanvallen vanaf het internet. Met een paar simpele handelingen wordt het netwerk beschermd tegen een groot aantal bekende aanvallen zoals port scans, ping of death en onbekende protocollen.

Object-based firewall
Met een object-based firewall is het mogelijk in de firewall groepen aan te maken. Deze groepen kunnen vervolgens gebruikt worden om firewall regels te definiëren. Een groep kan bestaan uit een IP adres of een groep van IP adressen.

Er hoeft dan niet bij elke regel het IP adres of de groep van IP adressen te worden ingevoerd. Ook kan er gebruik worden gemaakt van de vooraf ingestelde regels voor Instant Messaging (IM), Voice over IP protocollen en Peer 2 Peer download programma's (P2P). Het is mogelijk zelf servicetypen te definiëren zoals HTTP of FTP. Zo is de firewall snel en efficiënt in te stellen.

De groepen kunnen bijvoorbeeld als volgt ingedeeld worden:
Er zijn 5 afdelingen in een bedrijf; verkoop, inkoop, directie, administratie en systeembeheer. De administratie heeft toegang tot het internet, maar mag geen P2P programma's of IM clients zoals MSN gebruiken. De verkoop- en inkoopafdeling heeft ook toegang tot het internet en mag wel gebruik maken van IM clients om met hun klanten te communiceren. De directie en de systeembeheerder hebben onbeperkt toegang tot het internet.

objects-ipgrouptable

Instant Messaging blocking
Met Instant Messaging blocking kunt u eenvoudig Instant Messaging programma's zoals MSN Messenger en Yahoo Messenger blokkeren. Door een vinkje te zetten voor een service is eenvoudig de toegang tot deze service te blokkeren. Door middel van Time Schedule is het ook mogelijk deze toepassingen op bepaalde tijden wel toe te staan.

P2P blocking
Naast Instant Messaging blocking is ook P2P (Peer-to-Peer) blocking een nieuwe toepassing in de firewall. Door P2P blocking in te schakelen kunnen eenvoudig de meest gebruikte P2P programma's geblokkeerd of juist toegelaten worden. Ook is het mogelijk om bij gebruik van enkele P2P programma's het uploaden tegen te gaan. Voor het blokkeren van de verschillende P2P programma's hoeft enkel 'Disallow' aangevinkt te worden achter de applicatie.

DoS defense
Door DOS defense te activeren wordt het netwerk beschermd tegen bijvoorbeeld UDP of SYN flood. Eveneens kunnen trace route, fraggle attack of ping of death worden geblokkeerd.

Content filtering
Met content filtering kan misbruik van de internettoegang tegen worden gegaan. Door middel van keywords kunnen websites geblokkeerd worden. Tevens kan de router zo ingesteld worden dat deze alleen een vooraf ingestelde website of alle websites, met uitzondering van ingestelde websites, kan laten zien. Ook JAVA / Active X applet downloads, Cookies, HTML of specifieke bestandstypen (ZIP, EXE, etc.) kunnen worden geblokkeerd. Om verder misbruik van de internetverbinding tegen te gaan of gebruikers te beschermen tegen ongewenste inhoud, kunnen nu ook peer-to-peer applicaties alsmede instant messaging geblokkeerd worden. Ook kan een tijdschema op worden gesteld waarin het gebruik van dit soort programma's is toegestaan.

URL content filtering
URL content filtering geeft de mogelijkheid om een white- en blacklist op te stellen met URL's (Uniform Resource Locator) die wel of niet bezocht mogen worden. Een URL is bijvoorbeeld http:www.hotmail.com
In de blacklist kunnen woorden worden vermeld die niet in de URL mogen voorkomen zoals bijvoorbeeld het woord 'mail'.
Bij Enable Restrict Web Features kunnen bepaalde bestanden zoals ActiveX of Multimediafiles worden geblokkeerd.
Aan deze URL content filtering kan vervolgens een tijdschema worden gekoppeld wanneer wel en wanneer geen toegang tot de URL's mag plaatsvinden.

SurfControl
DrayTek heeft de dienst van SurfControl geïntegreerd in deze router. In de web user interface kan

worden aangegeven, dat het netwerk gebruik dient te maken van de dienst van SurfControl. Hierdoor is het nog eenvoudiger om bepaalde websites te blokkeren. Voor een klein bedrag per jaar kunt u zich abonneren op deze service.

QoS (Quality of Service)

De QoS-functie zorgt ervoor dat datastromen, zowel inkomend als uitgaand, met een door u bepaalde prioriteit worden behandeld. U kunt bijvoorbeeld per poort of per IP-adres de bandbreedte aangeven. Quality of Service (QoS) zorgt eveneens voor gegarandeerde VoIP kwaliteit. De toepassing van QoS in de V-modellen garandeert dat overige datastromen, zoals HTTP en FTP, geen invloed hebben op de kwaliteit van het telefoongesprek. Voor de toepassing van QoS voor VoIP is geen configuratie nodig.

qos

Windows Syslog Tool

Met de Windows Syslog Tool kan de routerstatus en activiteit gelogd worden. Deze tool kan op één of meerder pc's gedraaid worden. In de log file kunt u informatie krijgen over de activiteit van iedere individuele PC/gebruiker. Ook kunnen de firewall rules en de werking van de router bekeken worden. Syslog programma's voor andere besturingssystemen zijn beschikbaar bij derde partijen. Deze router ondersteunt SNMP (MIB-II) hiermee kan een SNMP cliënt de router zowel lokaal als op afstand.
Tel: 0653168254