

Draytek VigorIPPBX 2820 VoIP

Speciaal voor het gehele MKB heeft DrayTek de VigorIPPBX 2820 ontwikkeld.

Deze IPPBX biedt belangrijke telefoniefuncties zoals voicemail to e-mail, IVR, auto-attendant, dag- en nachtstand, etc.

SIP server

SIP server staat voor Session Initiation Protocol server.

De SIP clients, zoals IP telefoons, registreren zich bij een SIP server.

De VigorIPPBX heeft haar eigen sip server aan boord, waar maximaal 50 IP telefoons geregistreerd kunnen worden.

Ook externe IP telefoons buiten het netwerk kunnen geregistreerd worden bij de VigorIPPBX.

Specificaties

50 simultane SIP registraties - Voicemail (to e-mail)

6 externe SIP trunks - Auto attendant

Registratie via LAN, WAN, VPN - Dag- en nachtstand

IPPBX Features

Auto attendant

Door gebruik te maken van een auto attendant kan een gesprek zonder tussenkomst van een telefoniste direct worden afgeleverd bij een bepaalde extensie. Gesprekken worden na een welkomstboodschap gedistribueerd naar de juiste locatie, afdeling of persoon.

Voicemail (to e-mail)

De VigorIPPBX 2820 beschikt over geïntegreerde voicemail toepassingen. Met behulp van de voicemail to e-mail functie kunnen de voicemail berichten naar je eigen e-mail adres verstuurd worden, zodat geen enkel bericht gemist hoeft te worden. Dit is voor elke extensie (toestelaansluiting) die geconfigureerd is in de VigorIPPBX mogelijk. De voicemail berichten kunnen op ieder moment worden geraadpleegd. De voicemail opslagcapaciteit op basis van G711 codec is vier uur.

Hunt Groups

Door het gebruik van 'Hunt groups' kunnen meerdere extensies in een groep worden geplaatst. Zo kunnen er eenvoudig groepen worden gemaakt voor Sales/Directie/Support, etc. Bij binnenkomende gesprekken gaat de telefoon dan tegelijk over op alle extensies in een groep (simultaneous) of na elkaar (sequential).

Office & non office hours

In de VigorIPPBX kan worden aangegeven wanneer de kantooruren zijn. Buiten de kantooruren krijgen de mensen die bellen een melding dat het bedrijf is gesloten en wat men kan doen om contact met u op te nemen (bv. vermelding e-mailadres, webadres of de mogelijkheid om iets in te spreken). Ook bij vakantie- en/of feestdagen kunnen hier worden ingesteld.

Digit mapping

Met digit mapping kan worden aangegeven via welke netlijn, (SIP, ISDN of PSTN) gebeld wordt. Men kan dan bijvoorbeeld instellen dat via de ISDN lijn gebeld wordt, wanneer een 0 wordt ingetoetst. Toetst men een 8 dan wordt er gebeld over SIP 1. Wanneer een telefoonnummer wordt ingetoetst zal deze aan de hand van de Digit Map regel worden verwerkt.

Least Cost Routing

LCR (Least Cost Routing) verschaft u aan de hand van het gekozen nummer automatisch te laten bepalen via welke provider het gesprek het voordeligst is (Least Cost). Een doeltreffende manier van besparen op telefoonkosten!

SECOND WAN

De Draytek 2820 beschikt naast een ADSL modem over een tweede ethernet WAN poort. Als gebruik gemaakt wordt van deze WAN poort kan load balancing (verdelen van netwerkbelasting) en fail-over (bij uitval van de ene verbinding automatisch uitwijken naar de andere verbinding) worden toegepast. Zo kunnen de netwerkprestaties, schaalbaarheid en betrouwbaarheid van de internetverbinding worden verbeterd.

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.

WAN >> Load-Balance Policy

Index	Enable	Protocol	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End
1	<input checked="" type="checkbox"/>	TCP/UDP	WAN1	192.168.1.30	192.168.1.20				
2	<input checked="" type="checkbox"/>	TCP/UDP	WAN2	192.168.1.30	192.168.1.40				
3	<input type="checkbox"/>	any	WAN1						
4	<input type="checkbox"/>	any	WAN1						
5	<input type="checkbox"/>	any	WAN1						
6	<input type="checkbox"/>	any	WAN1						
7	<input type="checkbox"/>	any	WAN1						
8	<input type="checkbox"/>	any	WAN1						
9	<input type="checkbox"/>	any	WAN1						
10	<input type="checkbox"/>	any	WAN1						

Er kunnen 20 load-balancing regels aangemaakt worden.

Met de functie "auto weight" bepaalt de router 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 (Quality-of-Service) 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 zo optimaal mogelijke internetverbinding. Als de weggevallen verbinding hersteld is, wordt automatisch weer overgeschakeld naar de herstelde verbinding. De gebruikers merken nagenoeg niets van deze overschakeling.

USB printerpoort

De USB printerpoort op dit model is geschikt voor de meeste standaard USB printers. Indien een printer aangesloten wordt op de router, kan met meerdere PC's gebruik gemaakt worden van de printer.

3,5G UMTS / HSDPA

Op de USB poort van de router kan een 3,5G UMTS/HSDPA USB modem ('dongle') van mobiele providers worden aangesloten. Op deze wijze is de USB aansluiting te gebruiken als WAN poort en geschikt voor het UMTS/HSDPA netwerk.



LAN

Gigabit LAN

Één van de vier LAN poorten is een gigabit (1000 Mbs LAN poort. Deze gigabit LAN poort zorgt voor een snellere dataoverdracht. De poort kan bijvoorbeeld worden gebruikt voor een uplink naar een gigabit switch. Normale verbindingen zijn 100 Mbs.

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 netwerkkaart 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.

Firewall >> Bind IP to MAC

Bind IP to MAC

Note: IP-MAC binding can cooperate with router DHCP server, the host with IP-MAC binding can get specified IP through DHCP.
If Strict Bind selected, any IPs not bound to MAC cannot gain access to Internet.

Enable Disable Strict Bind

APP Table		IP Bind List		
IP Address	Mac Address	Index	IP Address	Mac Address
192.168.1.10	00-00-79-0A-0A-0F	1	192.168.1.10	00-00-29-0A-0A-0E
192.168.1.11	00-00-48-35-7A-53			

Add and Edit

IP Address: 192.168.1.10
Mac Address: 00 : 00 : 29 : 0a : 0a : 0f

Buttons: Add, Edit, Remove, OK

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.



WIRELESS LAN

Wireless n

De Vigor n-modellen beschikken over een 802.11n wireless access point (zender). Deze n-standaard is gebaseerd op de MIMO-techniek (Multiple Input – Multiple Output). Dit houdt in dat meerdere antennes op de router kunnen verzenden en ontvangen. De router maakt gebruik van 3 antennes.

De wireless n standaard biedt **hogere snelheden** en een **betere dekking** dan 802.11g standaard. Bovendien ondersteunt het access point tevens de traditionele 802.11b en de 802.11g standaard. Met de 11n standaard zijn snelheden tot in principe max 300Mbps mogelijk. NB: De werkelijke snelheid blijft altijd afhankelijk van de omgevingsfactoren.

Draadloze beveiliging

Het is belangrijk dat het draadloze netwerk goed beveiligd is. Deze router ondersteunt naast WEP en WPA ook WPA2 encryptie. Om het draadloze netwerk nog veiliger te maken kan toegangscontrole op MAC adres worden toegepast. Zo hebben MAC adressen die niet zijn geregistreerd geen toegang tot het draadloze netwerk. Voor grotere draadloze netwerken ondersteunt deze router 802.11x authenticatie. Er wordt dan ingelogd op een radius server. Deze server bepaalt de toegang tot het draadloze netwerk.

Multi SSID

SSID staat voor Service Set Identifier. Deze functionaliteit maakt het mogelijk om draadloze computernetwerken van elkaar te scheiden, door elk draadloos netwerk een aparte naam (SSID) te geven. Met SSID is het mogelijk om gebruik te maken van verschillende draadloze netwerken op één access point. Deze router heeft de mogelijkheid voor vier SSID's. Aan deze diverse netwerken kunnen rechten worden toegekend, voor de desbetreffende gebruiker.

Voorbeeld zakelijke dienstverlening

Hierbij kan gedacht worden aan bijvoorbeeld kantoren die een draadloos netwerk hebben voor hun werknemers, maar ook voor hun gasten. De werknemers kunnen het bedrijfsnetwerk en het internet benaderen met een beveiligingssleutel. De gasten kunnen alleen het internet benaderen.

Per SSID kunnen verschillende beveiligingsmethoden worden toegepast zoals:

- Keuze uit wireless encryptie per SSID (WEP/WPA/WPA2)
- Communicatie naar het LAN netwerk toestaan of verbieden (isolate LAN)
- Onderlinge communicatie binnen hetzelfde SSID toestaan of verbieden (isolate member)

Wireless rate control

Met behulp van wireless rate control is het mogelijk om per SSID de maximale bandbreedte voor zowel de up- als de downstream te bepalen. Onderlinge communicatie tussen verschillende SSID's is niet mogelijk.

Hidden SSID

Hidden SSID zorgt ervoor dat uw SSID niet zichtbaar is voor hackers die scannen op draadloze verbindingen.

Wireless aan/uit knop

Aan de voorkant van de router zit een WLAN aan/uit knop. Hiermee kan het WLAN gedeelte met één druk op de knop aan of uitgezet worden. Dat is op twee manieren veilig: er kan beslist geen onbevoegde draadloze toegang tot uw computers worden verkregen én er is geen radiosmog.

WDS

Met de WDS functie wordt het bereik van het draadloze netwerk vergroot. Dit kan op twee manieren. In repeater mode, dit betekent dat een tweede apparaat binnen het bereik staat van het access point en vanuit die positie het draadloze signaal uitstuurt. Hiermee kan het bereik verdubbelen. Dit is wel afhankelijk van de omgevingsfactoren. WDS kan ook in bridge mode worden gezet. In deze mode kunnen twee gescheiden netwerken worden gecombineerd tot één draadloos netwerk. Dit is ideaal in situaties waarbij twee kantoren gekoppeld moeten worden en er geen kabel mogelijk is.

WPS Wifi Protected Setup

De router beschikt over de functie WiFi Protected Setup (WPS). Met een druk op de WPS-knop van het apparaat wordt automatisch een beveiligde verbinding gemaakt met elk WiFi-apparaat dat compatibel is met WPS. Er hoeft dan geen beveiligingssleutel ingevuld te worden. Dankzij de maximale beveiliging die WPA/WPA2 encryptie biedt, worden inbraken op een draadloos thuisnetwerk voorkomen.

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.

Bandwidth Management >> Limit Session

Limit Session

Enable Disable

Default Max Sessions:

Limitation List

Index	Start IP	End IP	Max Sessions
1	192.168.1.50	192.168.1.60	50

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.

Firewall >> Bind IP to MAC

Bind IP to MAC

Note: IP-MAC binding can cooperate with router DHCP server, the host with IP-MAC binding can get specified IP through DHCP.
If Strict Bind selected, any IPs not bound to MAC cannot gain access to Internet.

Enable Disable Strict Bind

ARP Table | Select All | Sort | Refresh | IP Bind List | Select All | Sort |

IP Address	Mac Address	Index	IP Address	Mac Address
192.168.1.10	00-00-39-0a-0a-0f	1	192.168.1.10	00-00-39-0a-0a-0f
192.168.1.11	00-00-48-35-9a-53			

Add and Edit

IP Address:

Mac Address:

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 aangegeven. QoS wordt vaak toegepast bij VoIP spraakverkeer. Immers als een emailtje een paar seconden later binnenkomt is dat geen probleem en zal u de vertraging nooit bemerken. Maar zelfs vrij geringe vertragingen in spraakverkeer worden al hinderlijk gevonden. De toepassing van QoS garandeert dat overige datastromen geen invloed hebben op de kwaliteit van het telefoongesprek en u niet door een zware download wordt 'weggedrukt'.

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.

ISDN SO NT/TE

ISDN TE Poort

De ISDN TE poort is de poort op de Draytek 2820 waar de ISDN lijn op wordt aangesloten. Deze ISDN TE poort kan naast Internet toegang, Remote beheer en VPN ook gebruikt worden voor VoIP toepassingen.

Integratie van VoIP in een ISDN omgeving is door DrayTek mogelijk gemaakt door de ISDN TE poort de mogelijkheden te geven van ISDN on/off net en ISDN loopthrough functionaliteit. Hierdoor is het mogelijk om eenvoudig te switchen tussen VoIP telefonie en ISDN telefonie.

- A) ISDN on net

Met de ISDN on net functionaliteit is het mogelijk om een inkomend ISDN gesprek door te schakelen naar VoIP. Het is dus mogelijk om naar het ISDN nummer te bellen en vervolgens 'door-te-bellen' via het internet.

Het doorschakelen van een inkomend gesprek kan automatisch of met een pincode.

- *Automatisch doorschakelen*

Wilt u dat al uw gesprekken automatisch worden doorgezet naar een andere locatie op basis van VoIP dan kan dit standaard worden ingesteld.

- *Met pincode*

Om te voorkomen dat iedereen standaard kan 'doorbellen' heeft DrayTek de mogelijkheid voor een pincode. Wil men 'doorbellen' dan dient men eerst deze pincode in te voeren.

- B) ISDN off net

Met de ISDN off net functionaliteit is het mogelijk om een binnenkomende VoIP telefoonlijn door te schakelen naar traditionele ISDN telefonie. Het is dus mogelijk om naar het VoIP nummer te bellen en 'door-te-bellen' via het ISDN telefonienetwerk. Het doorschakelen van een inkomend gesprek kan automatisch of met een pincode. Wilt u dat alle medewerkers via de zaak uitbellen, dan kunnen de medewerkers via VoIP bellen naar de zaak en krijgen vervolgens kiestoon om weer door te bellen via ISDN. Om te voorkomen dat iedereen standaard kan 'doorbellen' heeft DrayTek de mogelijkheid voor een pincode. Wil men 'doorbellen' dan dient men eerst deze pincode in te voeren.

- C) ISDN loopthrough

De ISDN loopthrough functionaliteit biedt de mogelijkheid om met de toestellen die aan de FXS poorten gekoppeld zijn uit te bellen via de ISDN lijn. Dit is handig wanneer u met hetzelfde toestel zowel VoIP als ISDN wilt uitbellen. Ook bent u zo met uw toestel altijd bereikbaar op zowel uw ISDN nummer als uw VoIP nummer. U kunt eveneens in de router aangeven of u standaard via VoIP of ISDN wilt uitbellen.

Internet toegang

De ISDN TE poort kan eveneens gebruikt worden als back-up van de ADSL verbinding. Dit houdt in dat indien de ADSL verbinding uitvalt u verder kunt internetten of e-mailen via de traditionele ISDN verbinding

Remote Beheer

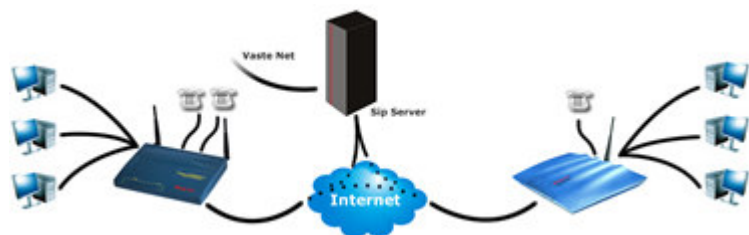
Voor Remote beheer doeleinden is de ISDN poort ook handig. Indien er op een bepaald moment geen ADSL verbinding is, kan met behulp van de ISDN worden ingebeld op de router. Hierdoor kunnen problemen op afstand eenvoudiger worden opgelost.

VPN

Via de ISDN poort kan zelfs indien nodig ook een VPN tunnel worden opgebouwd.

Voice over IP

Voice over IP (VoIP) is een technologie die het mogelijk maakt om te telefoneren via het Internet. De VoIP gesprekken van IP naar IP zijn geheel kosteloos. Door gebruik te maken van een SIP-dienst is het mogelijk om naar vaste aansluitingen en mobiele nummers te bellen (doorgaans niet geheel gratis).



Loopthrough

De Draytek 2820 beschikt over een lifeline/PSTN loopthrough. Met behulp van deze lifeline is het mogelijk de reeds bestaande telefonie infrastructuur te integreren met VoIP. Wanneer u gebeld wordt op uw VoIP nummer of uw bestaande nummer, gaan de op de FXS poorten aangesloten toestellen over.

Hotline

Het is mogelijk om een hotline in te stellen. Een hotline wil zeggen dat zodra de haak opgenomen wordt voor een uitgaand gesprek, er direct gebeld wordt naar het nummer dat als hotline is voorgeprogrammeerd.

DND

De Draytek modellen beschikken over een DND (Do Not Disturb) functie. Hiermee zal het telefoontoestel niet overgaan wanneer u wordt gebeld. Tevens is het mogelijk om in een schema aan te geven op welk tijdstip de DND functie moet worden ingeschakeld.

Call waiting

De call waiting functie zorgt ervoor dat, indien er tijdens een telefoongesprek een tweede gesprek binnen komt, dit tweede gesprek middels een aanklopton signaleerd wordt en aangenomen kan worden. Het andere gesprek kan dan in de wacht gezet worden. Het is mogelijk om te switchen tussen beide gesprekken.

Call forwarding

Met behulp van de functie call forwarding is het mogelijk om telefoongesprekken door te sturen naar een ander nummer. Er kan gekozen worden voor:

- doorsturen van alle telefoongesprekken;
- doorsturen bij in gesprek;
- doorsturen na het niet opnemen binnen x seconden.

VoIP over VPN

Het is mogelijk om door middel van een VPN tunnel gebruik te maken van VoIP telefonie. Thuiswerkers en nevenvestigingen kunnen op deze manier veilig uitbellen via het hoofdkantoor.

T.38 fax functie

De router ondersteunt het T.38 protocol. Dit protocol dient voor faxgebruik via VoIP. Op een FXS poort kan een fax kan worden aangesloten, voor zowel inkomend - als uitgaand faxen via VoIP. Via een SIP provider bestaat de mogelijkheid om te faxen naar het vaste net en om faxen te ontvangen vanaf het vaste net.

Single codec

Met behulp van deze functie kan aangegeven worden dat uitgaande gesprekken op een bepaalde codec worden gevoerd.

Hide Caller ID

Hide Caller ID is een functie waarmee het Caller ID (het telefoonnummer) tijdens een telefoongesprek verborgen kan worden gehouden.

Multiple SIP

Er kunnen **6** verschillende SIP accounts geconfigureerd worden. SIP accounts kunnen per FXS en ISDN S0 poort ingesteld worden. Hierdoor is het mogelijk verschillende nummers per poort te hebben. Zo kunnen bijvoorbeeld twee personen tegelijkertijd met een eigen telefoonnummer telefoneren.

VoIP >> SIP Accounts

SIP Accounts List Refresh

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
1				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
2				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
3				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
4				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
5				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
6				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-

R: success registered on SIP server
-: fail to register on SIP server

Digit Map Setup

In dit overzicht kan aangegeven worden van welk VoIP account gebruik gemaakt dient te worden bij ingave van een (deel van een) telefoonnummer.

Digit Map Setup

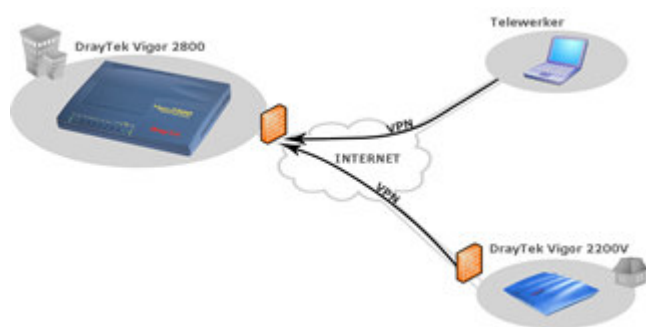
Enable	Prefix Number	Mode	OP Number	Min Len	Max Len	Interface
<input checked="" type="checkbox"/>	0031	None		0	0	VoIP1
<input checked="" type="checkbox"/>	06	None		0	0	VoIP1
<input checked="" type="checkbox"/>	0900	None		0	0	VoIP1
<input checked="" type="checkbox"/>	0800	None		0	0	VoIP2
<input checked="" type="checkbox"/>	0032	None		0	0	VoIP2

VPN (Virtual Private Network)

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 verandert. 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 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.

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.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 3 Rule 1

Check to enable the Filter Rule

Comments: WEB verkeer

Index(1-15) in Schedule Setup:

Direction: LAN->WAN

Source IP: Group1

Destination IP: Any

Service Type: Group1

Fragments: Don't Care

Pass or Block: Pass Immediately

Branch to Other Filter Set: None

Content Management: 1-Geen IM/VoIP

Log: Enable

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.

Objects Setting >> IP Group

IP Group Table:

Index	Name
1.	Medewerkers
2.	Beheer

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.

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 Security Management (CSM)

Met CSM (Content Security Management) kan misbruik van de internettoegang tegen worden gegaan. In deze router is het mogelijk websites met een bepaalde inhoud te blokkeren door middel van Instant Messaging/Peer 2 Peer blocking, URL content filtering en web content filtering.

Web Content Filter

Met de functie Web Content Filter in deze router is het mogelijk websites met een bepaalde inhoud te blokkeren. Indien het netwerk gebruik dient te maken van deze dienst, kan dat in de web user interface aangegeven worden. U kunt aangeven welke soort onderwerpen u wilt blokkeren door deze aan te vinken. Websites die betrekking op deze onderwerpen hebben, worden dan geblokkeerd. 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.

Het is eveneens mogelijk om een Time Schedule te gebruiken, dit is met name handig om bepaalde websites op bepaalde tijdstippen te blokkeren.

Instant Messaging/Peer 2 Peer blocking

Om verder misbruik van de internetverbinding tegen te gaan of gebruikers te beschermen tegen ongewenste inhoud, kunnen ook peer-to-peer applicaties alsmede instant messaging geblokkeerd worden.

URL content filtering

URL content filtering geeft de mogelijkheid om een white- en blacklist op te stellen met URL's (Uniform Resource Locator; oftewel websites) 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.

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 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.



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 monitoren.

