
DrayTek

Firewall cases

DrayTek Vigor 2960 & 3900

DrayTek

Your reliable networking solutions partner

Firewall Cases

In deze handleiding gaan we een aantal voorbeelden geven hoe u een bepaalde situatie kunt oplossen door middel van de Firewall.

Situatie 1

U maakt gebruik van een e-mail server in uw bedrijfs netwerk, het is de bedoeling dat alleen deze e-mail server gebruik mag maken van TCP poort 25 uitgaand. Dit is eenvoudig te configureren in de Firewall configuratie van de DrayTek.

U gaat naar het **Firewall >> Filter Setup** menu en maakt hier een nieuwe filter groep aan. Deze Filter groep zal ervoor zorgen dat al het e-mail verkeer van **LAN > WAN** geblokkeerd wordt.

In dit geval maakt u twee Filter groepen aan.

Block groep:

IP Filter

Group :

Enable

Comment : (Optional)

Apply Cancel

Pass groep:

IP Filter

Group :

Enable

Comment : (Optional)

Apply Cancel

Klik op **Apply** om de groep aan te maken en op te slaan.

Firewall >> Filter Setup >> IP Filter

Group	Enable	Comment
▶ Block	true	Blokkeer alles
▶ Pass	true	Uitzonderingen

U klikt de Block groep aan om vervolgens een Filter regel aan te maken, in deze filter regel geeft u aan dat al het verkeer van **LAN > WAN** op poort 25 geblokkeerd wordt.

Bij het aanmaken van deze Block regel zijn onderstaande instellingen van belang:

Profile : Geef de Firewall regel een naam ter kennisgeving.

Enable : Aanvinken om de firewall regel te activeren.

Action: Geef hier aan of je een Block of een Pass regel wilt maken. Omdat we in dit geval een blokkering willen opzetten voor poort 25 selecteren we : Block if no further match.

Next Group: Na het blokkeren dient de Firewall door te gaan naar de Pass group. In deze Pass group zal de uitzondering voor de e-mail server staan.

Input Interface: Hier selecteert u de LAN interface, de input interface is de interface waarvan het verkeer afkomstig is. In dit voorbeeld selecteren we alle LAN interfaces.

Output Interface: Hier selecteert u de WAN interface, de output interface is de interface waar het verkeer naar toe gaat. In dit voorbeeld selecteren we WAN1.

Service Type Object: Om welk type verkeer gaat het? In dit geval is het SMTP verkeer.

If no object is selected in a category, the case of 'Any' is applied

Profile	Protocol	Source Port Start	Source Port End	Destination Port...	Destination Port...	Edit
<input type="checkbox"/> RTSP	TCP/UDP	1	65535	554	554	
<input type="checkbox"/> SFTP	TCP	1	65535	115	115	
<input checked="" type="checkbox"/> SMTP	TCP	1	65535	25	25	
<input type="checkbox"/> SNMP	TCP/UDP	1	65535	161	161	
<input type="checkbox"/> SNMP_TRAPS	TCP/UDP	1	65535	162	162	
<input type="checkbox"/> SQL_NET	TCP	1	65535	1521	1521	
<input type="checkbox"/> SSH	TCP/UDP	1	65535	22	22	

Apply Cancel

Na het aanmaken van deze firewall regel moet het niet meer mogelijk zijn om middels SMTP poort 25 naar buiten te communiceren.

Bij het aanmaken van deze Pass regel zijn onderstaande instellingen van belang:

Profile : Geef de Firewall regel een naam ter kennisgeving.

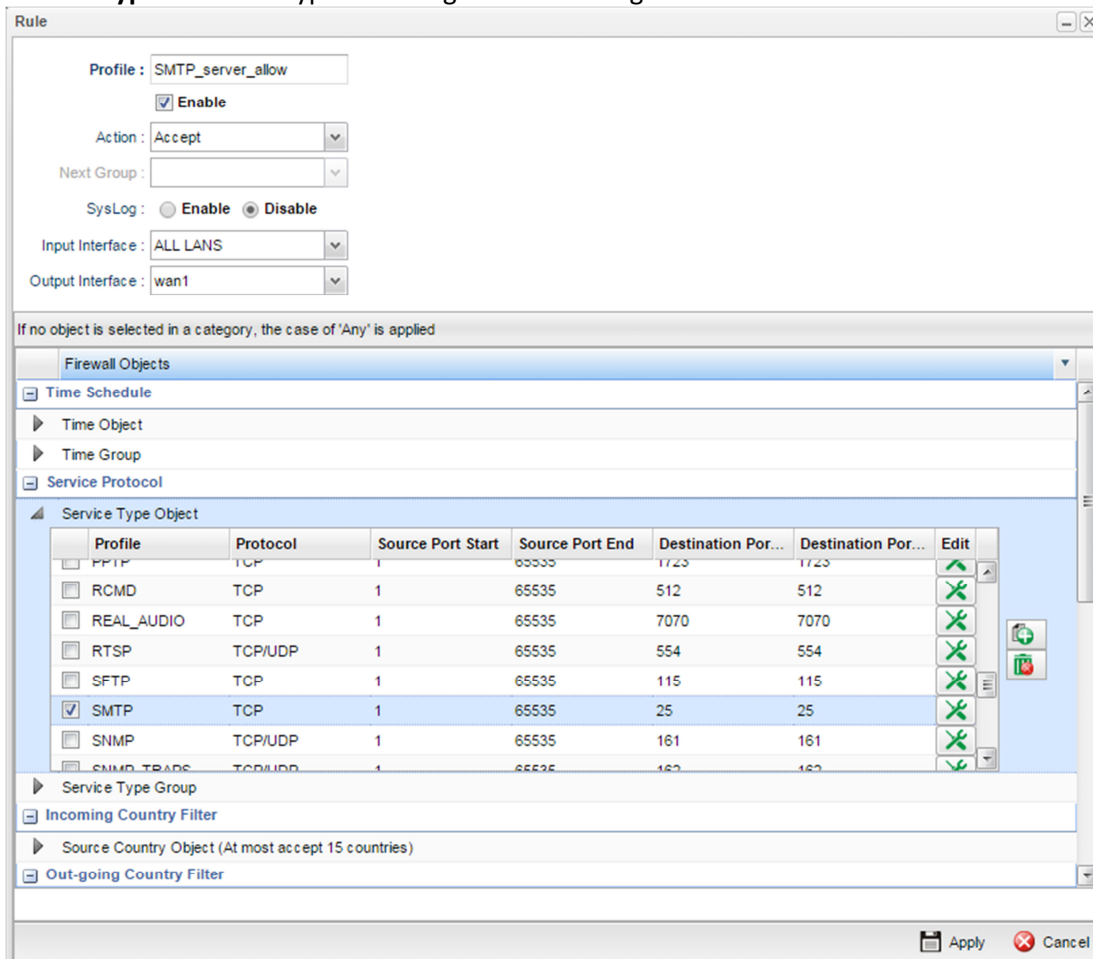
Enable : Aanvinken om de firewall regel te activeren.

Action: Geef hier aan of je een Block of een Pass regel wilt creëren. In dit geval gaat het om een Pass regel.

Input Interface: Hier selecteert u de LAN interface, de input interface is de interface waarvan het verkeer afkomstig is. In dit voorbeeld selecteren we alle LAN interfaces.

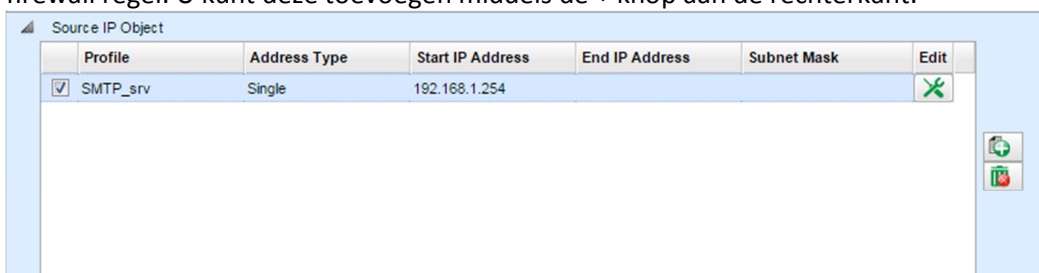
Output Interface: Hier selecteert u de WAN interface, de output interface is de interface waar het verkeer naar toe gaat. In dit voorbeeld selecteren we WAN1.

Service Type: Om welk type verkeer gaat het? In dit geval is het SMTP verkeer.



Source IP Object

Hier dient u het IP-adres van de server toe te voegen zodat alleen deze gekoppeld wordt aan de firewall regel. U kunt deze toevoegen middels de + knop aan de rechterkant.



Na het toevoegen van deze Firewall regel kan alleen de SMTP server middels poort 25 naar buiten communiceren, alle overige werkstations hebben geen toegang tot poort 25 uitgaand.

Situatie 2

U maakt gebruik van een FTP server in uw bedrijfs netwerk, deze FTP server zal wanneer u een port forwarding of open port regel aanmaakt bereikbaar zijn voor het hele internet. Nu kunt u de Firewall van de DrayTek zo configureren dat alleen bepaalde Public IP adressen toegang krijgen tot de FTP server.

Het is natuurlijk belangrijk dat de FTP server reeds bereikbaar is vanaf het internet. Dit kunt u regelen middels een Port Redirection regel.

The screenshot shows the 'Port Redirection' configuration window. The 'Profile' is set to 'FTP'. The 'Enable' checkbox is checked. The 'Port Redirection Mode' is set to 'One to One'. The 'WAN Profile' is 'wan1', 'Use IP Alias' is 'No', and 'Protocol' is 'TCP'. The 'Public Port' is '21'. The 'Private IP' is set to '192.168.1.254' and the 'Private Port' is '21'. A note at the bottom states: 'Note: In 'Range-to-Range(IP)' Mode the Private IP End will be calculated automatically once the Public Port Start and Public Port End have been entered.' The 'Apply' and 'Cancel' buttons are at the bottom right.

U gaat naar het **Firewall >> Filter Setup** menu en maakt hier een nieuwe filter groep aan. Deze Filter groep zal ervoor zorgen dat de FTP server niet meer bereikbaar is vanaf het internet. (WAN > LAN)

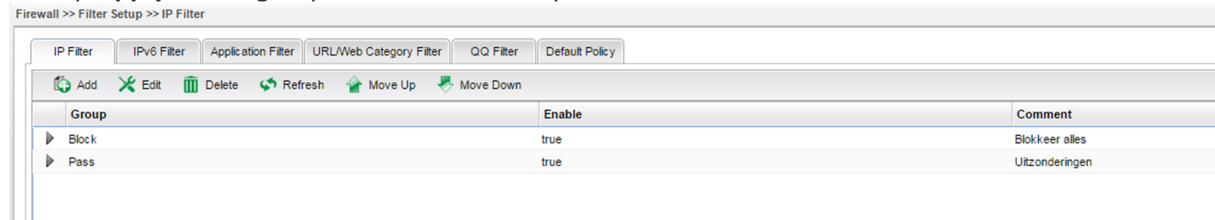
Block groep:

The screenshot shows the 'IP Filter' configuration window for a 'Block' group. The 'Group' is 'Block', 'Enable' is checked, and the 'Comment' is 'Blokkeer alles (Optional)'. The 'Apply' and 'Cancel' buttons are at the bottom right.

Pass groep:

The screenshot shows the 'IP Filter' configuration window for a 'Pass' group. The 'Group' is 'Pass', 'Enable' is checked, and the 'Comment' is 'Uitzonderingen (Optional)'. The 'Apply' and 'Cancel' buttons are at the bottom right.

Klik op **Apply** om de groep aan te maken en op te slaan.



U klikt de Block groep aan om vervolgens een Filter regel aan te maken, in deze filter regel geeft u aan dat al het verkeer van **WAN > LAN** op poort 21 geblokkeerd wordt.

Bij het aanmaken van deze Block regel zijn onderstaande instellingen van belang:

Profile :

Action: Geef hier aan of je een Block of een Pass regel wilt creëren. In dit geval willen we alles blokkeren.

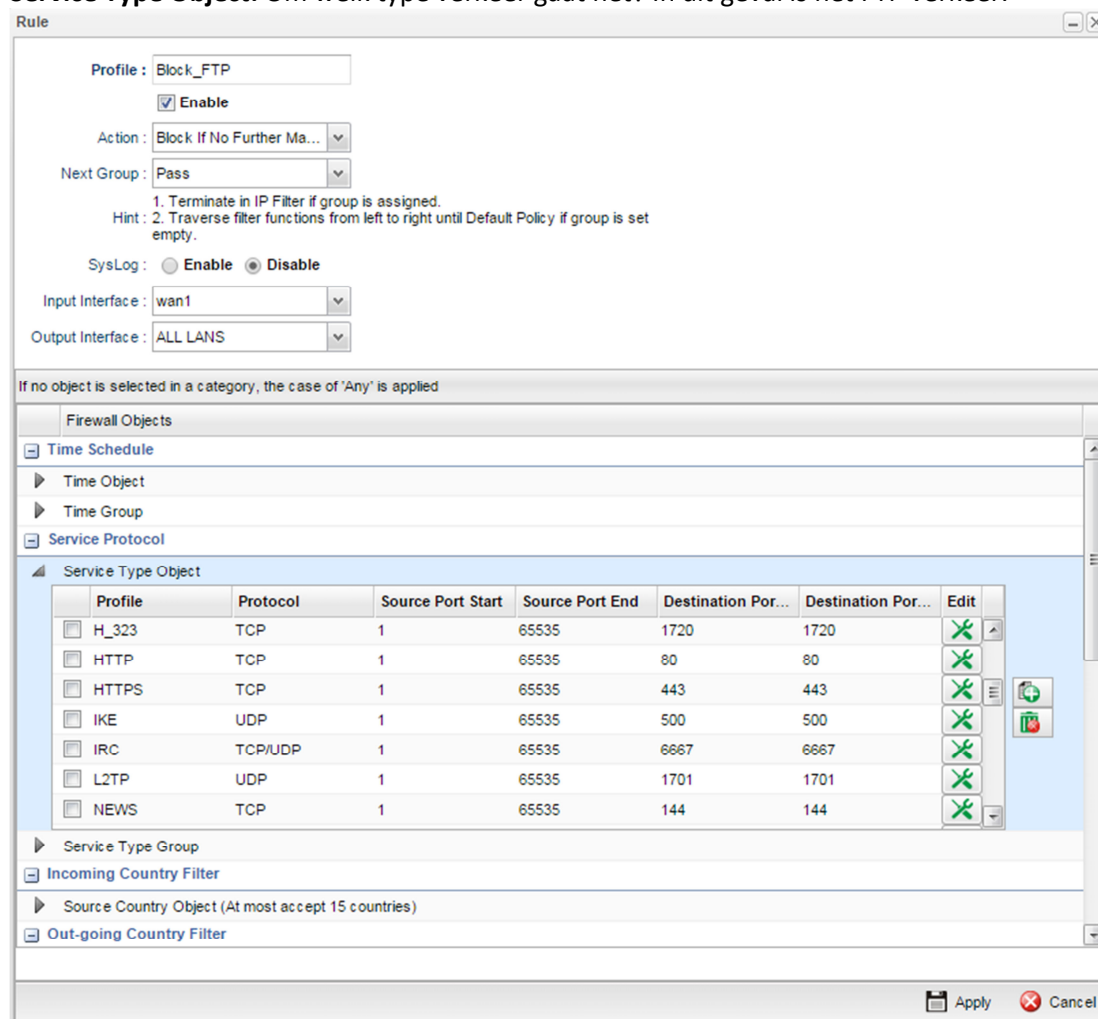
Enable : Aanvinken om de firewall regel te activeren.

Next Group: Na het blokkeren dient de Firewall door te gaan naar de Pass group. In deze Pass group zal de uitzondering voor de e-mail server staan.

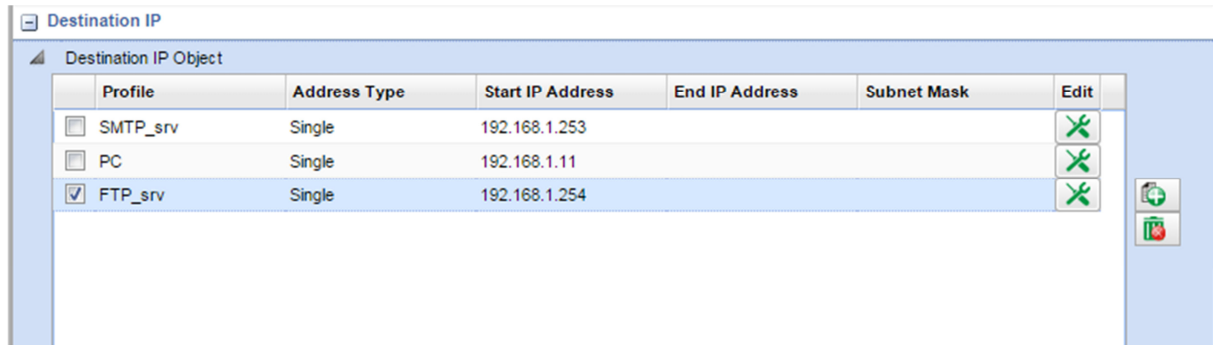
Input Interface: Hier selecteert u de WAN interface, de input interface is de interface waarvan het verkeer afkomstig is. In dit voorbeeld selecteren we WAN1.




Output Interface: Hier selecteert u de LAN interface, de output interface is de interface waar het verkeer naar toe gaat. In dit voorbeeld selecteren we alle LAN interfaces.

Service Type Object: Om welk type verkeer gaat het? In dit geval is het FTP verkeer.



In dit geval blokkeert de DrayTek al het FTP verkeer van WAN naar LAN. U kunt eventueel het Destination IP-adres nog opgeven. Zodoende zal de firewall regel alleen actief zijn voor FTP verkeer naar een specifiek intern IP-adres(FTP server). Dit kunt u instellen bij Destination IP Object :



Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input type="checkbox"/> SMTP_srv	Single	192.168.1.253			
<input type="checkbox"/> PC	Single	192.168.1.11			
<input checked="" type="checkbox"/> FTP_srv	Single	192.168.1.254			

Na het aanmaken van deze firewall regel mag de FTP server niet meer bereikbaar zijn vanaf het internet.

Om hier vervolgens een uitzondering voor te maken dient u een Pass regel aan te maken. Dit dient u te doen in de Pass groep. Bij het aanmaken van deze Pass regel zijn onderstaande instellingen van belang:

Profile : Geef de Firewall regel een naam ter kennisgeving.

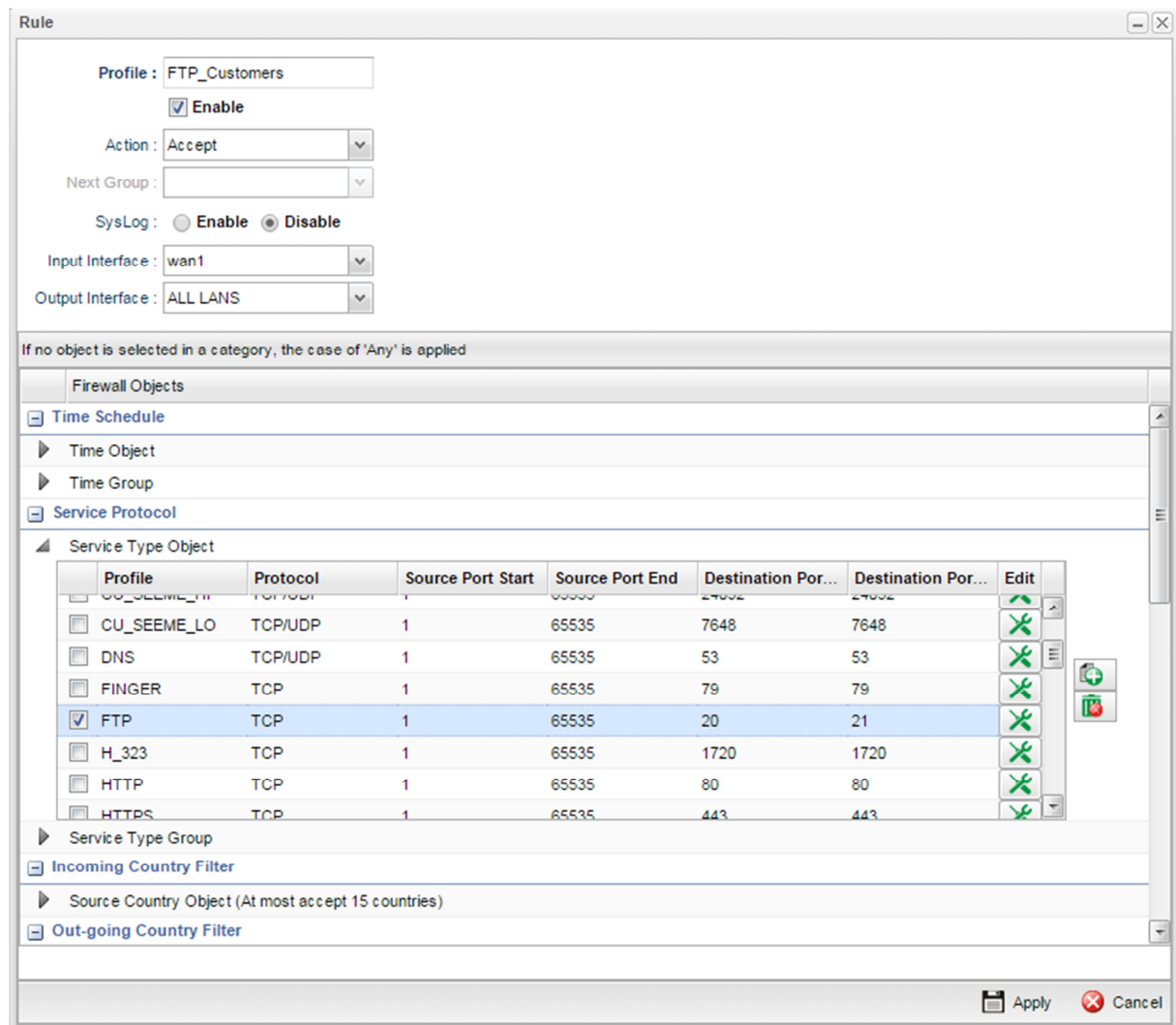
Enable : Aanvinken om de firewall regel te activeren.

Action: Geef hier aan of je een Block of een Pass regel wilt creëren. In dit geval gaat het om een Pass regel.

Input Interface : Hier selecteert u de WAN interface, de input interface is de interface waarvan het verkeer afkomstig is. In dit voorbeeld selecteren we WAN1.

Output Interface : Hier selecteert u de LAN interface, de output interface is de interface waar het verkeer naar toe gaat. In dit voorbeeld selecteren we ALL LAN's.

Service Type : Om welk type verkeer gaat het? In dit geval is het FTP verkeer.



Source IP Object : Bij het Source IP Object dien je het publieke IP-adres op te geven welke je toegang wilt geven tot je FTP server.

Destination IP Object : Bij Destination IP Object selecteer je de FTP server.

Na het aanmaken van deze firewall regel moet het mogelijk zijn om de FTP server van het zojuist opgegeven Source IP te bereiken.

Situatie 3:

U maakt gebruik van diverse LAN interfaces op de DrayTek. Omdat u Inter LAN Routing in hebt geschakeld kunnen alle LAN interfaces elkaar zien en benaderen. Dit wilt u gaan limiteren wat mogelijk is doormiddel van de firewall.

In dit voorbeeld gebruiken we de volgende LAN interfaces :

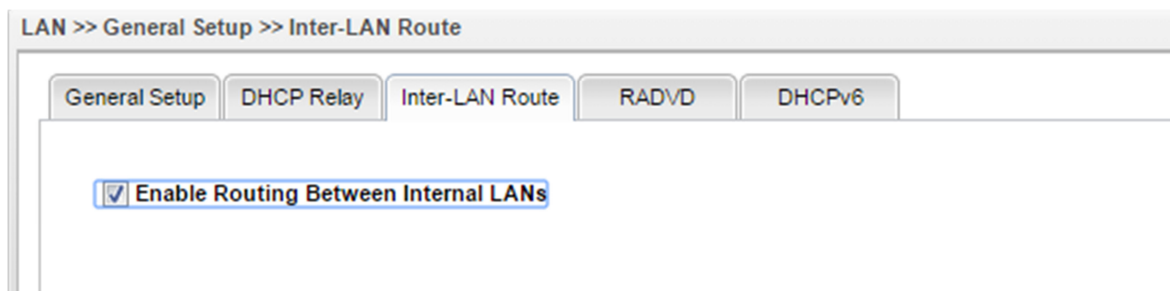
Profile (max length:7)	Enable	Description	VLAN ID	IPv4 Protocol	IP Address	Subnet Mask
lan1	true	BedrijfsNetwerk	10	static	192.168.1.1	255.255.255.0
gasten	true	Gasten	11	static	172.16.16.1	255.255.255.0

Hierbij willen we ervoor zorgen dat de Gasten niet op het Bedrijfs netwerk kunnen, het Bedrijf netwerk mag wel gewoon naar het Gasten netwerk.

Voor het creeren van meerdere LAN interfaces op de DrayTek kunt u onderstaande handleiding volgen.

[http://draytek.nl/files/Multiple%20LAN%20Subnets%20Vigor2960%20&%203900%20\[V1.0\].pdf](http://draytek.nl/files/Multiple%20LAN%20Subnets%20Vigor2960%20&%203900%20[V1.0].pdf)

Om communicatie toe te staan tussen de LAN interfaces dient u Inter-LAN Route in te schakelen.



Vervolgens kunt u onder Firewall >> Filter setup een Block groep aanmaken.

Block groep:

IP Filter

Group :

Enable

Comment : (Optional)

Apply Cancel

Bij het aanmaken van deze Block regel zijn onderstaande instellingen van belang:

Profile : Geef het profiel een naam.

Enable : Aanvinken om de firewall regel te activeren.

Action: Geef hier aan of je een Block of een Pass regel wilt creëren. In dit geval willen we alles blokkeren van het Gasten netwerk naar het Bedrijfs netwerk.

Input Interface: Hier selecteert u de LAN interface waarvan het verkeer afkomstig is. In dit geval selecteren we gasten.

Output Interface: Hier selecteert u de LAN interface waar het verkeer naar toe gaat. Dit betreft het Bedrijfs netwerk, we selecteren hier dus lan1.

Rule

Profile : BlockGasten

Enable

Action : Block

Next Group :

SysLog : Enable Disable

Input Interface : gasten

Output Interface : lan1

If no object is selected in a category, the case of 'Any' is applied

Firewall Objects

- Time Schedule
 - Time Object
 - Time Group
- Service Protocol
 - Service Type Object
 - Service Type Group
- Incoming Country Filter
 - Source Country Object (At most accept 15 countries)
- Out-going Country Filter
 - Destination Country Object (At most accept 15 countries)
- Source IP
 - Source IP Object
 - Source IP Group
 - Source User Profile
 - Source User Group
 - Source LDAP Group
- Destination IP

Apply Cancel

Nadat u op OK hebt geklikt is het voor het Gasten netwerk niet meer mogelijk om het Bedrijfs netwerk te benaderen. Het bedrijfsnetwerk kan echter nog wel naar het Gasten netwerk.

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.

Copyright verklaring

© 2011 DrayTek. Alle rechten voorbehouden. Niets uit deze uitgave mag worden vermenigvuldigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j° het Besluit van 20 juni 1974, St.b. 351, zoals gewijzigd bij Besluit van 23 augustus 1985, St.b. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht. Voor het opnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers of andere compilatie- of andere werken (artikel 16 Auteurswet 1912), in welke vorm dan ook, dient men zich tot de uitgever te wenden.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

Registreren

U kunt via www.draytek.nl/registratie uw product registreren. Geregistreerde gebruikers worden per e-mail op de hoogte gehouden van nieuwe firmware versies en ontwikkelingen.

Trademarks

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.