# **Dray**Tek

## **Firewall cases** DrayTek Vigor 2960 & 3900

Oroy Te



### **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 :	Block		
🔽 Enable			
Comment :	Blokkeer alles		(Optional)
		Apply Apply	🔇 Cancel

### Pass groep:

IP Filter			_×_
Group :	Pass		
📝 Enable			
Comment :	Uitzonderingen		(Optional)
		Apply	🚫 Cancel

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

IP	Filter IPv6 Filter Application Filter URL/Web Category Filter QQ Filter	Default Policy	
ľ,	Add 🔀 Edit 🛅 Delete 🕩 Refresh 🍲 Move Up 😽 Move Down		
	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 kennis geving.

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.

Profile :	Block_SMTP									
	Chable									
Action :	Block If No Fu	urther Ma 👻								
Next Group :	Pass	*								
Hint :	1. Terminate in 2. Traverse filt empty.	n IP Filter if group is er functions from I	s assigned. eft to right until Defaul	t Policy if group is set						
SysLog :	Enable (	Disable								
Input Interface :	ALL LANS	*								
utput Interface :	wan1	~								
object is select	ted in a categor	y, the case of 'Any	' is applied							
Firewall Obje	ects									
Time Schedul	e									
Time Object										
Time Group										
Service Protoc	col									
Service Protoc	col e Obiect									
Service Protoc	col e Object Pr	rotocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit			
Service Protoc Service Type Profile	col e Object Pi	rotocol CP/UDP	Source Port Start	Source Port End	Destination Por	Destination Por	Edit			
Service Protoc Service Type Profile RTSP SFTP	e Object Pi T(	rotocol CP/UDP CP	Source Port Start	Source Port End 65535 65535	Destination Por 554 115	Destination Por 554 115	Edit			
Service Protoc Service Type Profile RTSP SFTP SFTP SMTP	col e Object Pi T( T( T(	rotocol CP/UDP CP CP	Source Port Start 1 1 1 1	Source Port End 65535 65535 65535	Destination Por 554 115 25	Destination Por 554 115 25	Edit X X			
Service Protoc Service Type Profile RTSP SFTP SMTP SNMP	col e Object T( T( T( T( T(	rotocol CP/UDP CP CP CP CP/UDP	Source Port Start 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535	Destination Por 554 115 25 161	Destination Por 554 115 25 161	Edit ××××			
Service Protoc Service Protoc Profile RTSP SFTP V SMTP SNMP SNMP	e Object Pi TC	rotocol CP/UDP CP CP CP/UDP CP/UDP CP/UDP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535	Destination Por 554 115 25 161 162	Destination Por 554 115 25 161 162	Edit ****	m N	<b>(</b> )	
Service Protoc Service Profile RTSP SFTP SMTP SNMP SOL_NE	e Object Pi Tr Tr Tr Tr TRAPS Tr ET T	rotocol CP/UDP CP CP CP/UDP CP/UDP CP/UDP CP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535	Destination Por 554 115 25 161 162 1521	Destination Por 554 115 25 161 162 1521	Edit ***	[M]		
Service Protoc Service Profile RTSP SFTP SIMP SNMP SNMP SQL_NE SSH	col e Object TC TC TC TRAPS TC TRAPS TC TC TC TC TC	rotocol CP/UDP CP CP CP/UDP CP/UDP CP CP/UDP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 554 115 25 161 162 1521 22	Destination Por 554 115 25 161 162 1521 22	Edit: ** ** ** ** **	A M	() () ()	
Service Protoc Service Protoc Profile RTSP SFTP SIMP SNMP SNMP SOL_NE SSH Service Type	col e Object T( T( T( T( T( TRAPS T( ET T( te Group	rotocol CP/UDP CP CP CP/UDP CP/UDP CP/UDP CP/UDP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 554 115 25 161 162 1521 22	Destination Por 554 115 25 161 162 1521 22	Editt ** ** ** ** ** **		() ()	
Service Protoco Service Protoco Profile RTSP SFTP SMTP SNMP SNMP SNMP SUL_NE SSH Service Type Incoming Cou	col e Object P T T T T T T T T T T C T T T C E T T C E T T C C T T C T C	rotocol CP/UDP CP CP CP/UDP CP/UDP CP/UDP CP/UDP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 554 115 25 161 162 1521 22	Destination Por 554 115 25 161 162 1521 22	Edit ** ** ** **	A M	<b>(</b> ) <b>(</b> )	
Service Protoc Service Protoc Profile RTSP SFTP SMTP SNMP SNMP SOL_NE SSH Service Type Incoming Cou	col e Object P T( T( T( T( TRAPS T( ET C e Group Intry Filter ntry Object (At n	rotocol CP/UDP CP CP CP/UDP CP/UDP CP/UDP CP/UDP	Source Port Start	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 554 115 25 161 162 1521 22	Destination Por 554 115 25 161 162 1521 22	Edit X X X X X X	A M	<b>(</b> )	
Service Protoc Service Protoc Profile RTSP SFTP SMTP SNMP SNMP SOL_NE SSH Service Type Incoming Cou Source Cour	col e Object T( T( T( T( TRAPS T( ET C e Group untry Filter Try Object (At n untry Filter	rotocol CP/UDP CP CP CP/UDP CP/UDP CP/UDP CP/UDP	Source Port Start  1  1  1  1  1  1  1  1  1  1  1  1  1	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 554 115 25 161 162 1521 22	Destination Por 554 115 25 161 162 1521 22			<b>(</b> )	

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 kennis geving.

Enable : Aanvinken om de firewall regel te activeren.

Action: Geef hier aan of je een Block of een Pass regel wilt creeren. 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.

Rule											-×
	Profile :	SMTP serv	er allow								
		Enable	-								
	Action :	Accept		<b>v</b>							
	Next Group :			~							
	Syst og :	Enable	Disable								
	eyeleg.		0								
"	iput interface :	ALL LANS		•							
Ou	tput Interface :	wan1		*							
lf no	object is select	ed in a categ	ory, the case o	f 'Any' is applied							
	Firewall Obje	ects									•
•	lime Schedule	ê									-
▶	Time Object										
₽	Time Group										
-	Service Protoc	:ol									
4	Service Type	e Object									
	Profile		Protocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit			
			тер	1	65535	512	512		-		
			тор	1	65535	7070	7070	-			L
		.0010		1	65535	554	554	-			
	SETP		TCP	1	65535	115	115	<del>x</del>			
	SMTP		тср	1	65535	25	25	×	٦		
	SNMP		TCP/UDP	1	65535	161	161	×			
	CNIMD 7	EADS .		1	65595	160	160	1	-		
	Service Type	Group									
	ncoming Cou	ntry Filter									_
	Source Coun	try Object (A	t most accept 1	15 countries)							
	Out-going Co	untry Filter									1
									_		
							t i	App	ły	🚫 Ca	ancel

### Source IP Object

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

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
SMTP_srv	Single	192.168.1.254		L	×
_					

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.

Profile :	FTP	
V Enable		
Port Redirection Mode	One to One	
WAN Profile :	wan1	~
Use IP Alias :	No	*
Protocol :	TCP	~
Public Port :	21	
Private IP :	192 . 168 . 1	254
Private Port :	21	
lote : In Range-to-Range(IP)' Moo alculated automatically once the Public lave been entered.	de the Private IP End will be c Port Start and Public Port	End

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:** 

IP Filter			- ×
	Disch		1
Group :	BIOCK		
V Enable			
Comment	Blokkeer alles		(Optional)
		Apply Apply	🔇 Cancel

Pass groep:

IP Filter			-×
Group :	Pass		
V Enable			
Comment	Uitzonderingen		(Optional)
		Apply Apply	🔇 Cancel

### **Dray** Tek

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

_						
I	IP Filter	IPv6 Filter	Application Filter	URL/Web Category Filte	r QQ Filter	Default Policy
1	🕒 Add	🔀 Edit 🛛 🔟	Delete 🗳 Ref	resh 🔺 Move Up	🐣 Move Down	
	Group					Enable
₽	Block					true
₽	Pass					true

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 creeren. 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.

									=)0
Profile :	: Block_FTP								
	🔽 Enable								
Action	Block If No Further Ma	*							
Next Group	: Pass	*							
Hint	1. Terminate in IP Filter if g 2. Traverse filter functions empty.	roup is assigned. from left to right until Defaul	t Policy if group is set	t					
SysLog	: 🔵 Enable 💿 Disable								
Input Interface	: wan1	*							
Output Interface	: ALL LANS	*							
no object is selec	cted in a category, the case of	of 'Any' is applied							
Firewall Obj	jects								
Time Schedul	le								
Time Object	t								
Time Group	)								
									- 11
Service Proto	col								
Service Proto	ocol De Object								_
Service Proto	e Object Protocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit			
Service Proto Service Typ Profile H_323	e Object Protocol TCP	Source Port Start	Source Port End	Destination Por 1720	Destination Por 1720	Edit	•		
Service Proto Service Typ Profile H_323 HTTP	e Object Protocol TCP TCP	Source Port Start 1 1	Source Port End 65535 65535	Destination Por 1720 80	Destination Por 1720 80	Edit ×			
Service Proto Profile H_323 HTTP HTTPS	e Object Protocol TCP TCP TCP TCP TCP	Source Port Start 1 1 1 1 1	Source Port End 65535 65535 65535	Destination Por 1720 80 443	Destination Por 1720 80 443	Edit *			
Service Proto Profile H_323 HTTP HTTPS IKE	e Object Protocol TCP TCP TCP TCP UDP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535	Destination Por 1720 80 443 500	Destination Por 1720 80 443 500	Edit × × ×	I III		
Service Proto Profile H_323 HTTP HTTPS IKE IRC	e Object Protocol TCP TCP UDP TCP/UDP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535	Destination Por 1720 80 443 500 6667	Destination Por 1720 80 443 500 6667	Edit * * *		() ()	
Service Proto Profile H_323 HTTP HTTPS IKE IRC L2TP	e Object Protocol Protocol CP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535	Destination Por 1720 80 443 500 6667 1701	Destination Por 1720 80 443 500 6867 1701	Edit ** ** ** **		í¢ B	
Service Proto Profile H_323 HTTP HTTPS IKE IRC L2TP NEWS	e Object Protocol TCP TCP TCP UDP TCP/UDP UDP TCP UDP TCP	Source Port Start	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 1720 80 443 500 6867 1701 144	Destination Por 1720 80 443 500 6667 1701 144	Edit *****			
Service Proto Service Typ Profile H_323 HTTP HTTPS IKE IRC L2TP NEWS Service Typ	e Object Protocol TCP TCP CP C	Source Port Start           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 1720 80 443 500 6667 1701 144	Destination Por 1720 80 443 500 6667 1701 144	Edit ** ** ** **		r t	
Service Proto Service Typ Profile H_323 HTTP HTTPS IKE IRC L2TP NEWS Service Typ Incoming Cot	e Object Protocol TCP TCP CP CO	Source Port Start           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por           1720           80           443           500           6867           1701           144	Destination Por 1720 80 443 500 6667 1701 144	Edit ** ** ** **			
Service Proto Profile H_323 HTTP HTTPS IKE IRC L2TP NEWS Service Typ Incoming Cotton	e Object Protocol TCP TCP UDP CCP/UDP UDP TCP ODP CCP/UDP UDP TCP TCP TCP TCP TCP TCP TCP TCP TCP TC	Source Port Start	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 1720 80 443 500 6667 1701 144	Destination Por 1720 80 443 500 6667 1701 144	Edit ** ** ** **		() ()	
Service Proto Profile H_323 HTTP HTTPS IKE IKE IRC L2TP NEWS Service Typ Incoming Cou Source Cou Out-going Co	e Object Protocol TCP TCP UDP UDP CCP/UDP UDP TCP UDP UDP TCP UDP UDP TCP UDP UDP TCP UDP TCP UDP TCP UDP TCP UDP TCP TCP TCP TCP TCP TCP TCP TCP TCP TC	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 1720 80 443 500 6667 1701 144	Destination Por 1720 80 443 500 6667 1701 144	Edit ****		( <u>)</u>	



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 :

	Destination IP						
4	Destination IP Object						
	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit	
	SMTP_srv	Single	192.168.1.253			×	
	PC	Single	192.168.1.11			*	
	FTP_srv	Single	192.168.1.254			×	1
							Ī

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 kennis geving.

Enable : Aanvinken om de firewall regel te activeren.

Action: Geef hier aan of je een Block of een Pass regel wilt creeren. 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.

	Profile :	FTP_Cus	tomers								
		V Enabl	e								
	Action :	Accept		•							
	Next Group :			~							
	SysLog :	Enab	le   Disable								
Inp	out Interface :	wan1		*							
Outp	out Interface :	ALL LANS	\$	*							
no ol	biect is select	ed in a cate	egory, the case o	f 'Any' is applied							
	Firewall Obje	ente							_		-
аті	ime Schedule										
	inc Schedule	-									
b.	Time Object										
	Time Object										
	Time Object Time Group	ol.									
► ► Se	Time Object Time Group ervice Protoc	ol									
▶ Se	Time Object Time Group ervice Protoc Service Type	ol Object	Protocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit			
▶ Se	Time Object Time Group ervice Protoc Service Type Profile	ol Object	Protocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit			
Se	Time Object Time Group ervice Protoc Service Type Profile CU_SEE	Object	Protocol TCP/UDP	Source Port Start	Source Port End	Destination Por 27002 7648	Destination Por 24002 7648	Edit	•		
Se	Time Object Time Group ervice Protoc Service Type Profile CU_SEE DNS	Object	Protocol TCP/UDP TCP/UDP	Source Port Start	Source Port End 65535 65535	Destination Por 7648 53	Destination Por 24002 7648 53	Edit X		6	1
Se	Time Object Time Group ervice Protoc Service Type Profile CU_SEE DNS FINGER	Object	Protocol TCP/UDP TCP/UDP TCP	Source Port Start	Source Port End 65535 65535 65535	Destination Por 24002 7648 53 79	Destination Por 27002 7648 53 79	Edit			
Se	Time Object Time Group ervice Protoc Service Type Profile CU_SEE DNS FINGER V FTP	ol Object ME_LO	Protocol TCP/UDP TCP/UDP TCP TCP	Source Port Start 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535	Destination Por 27002 7648 53 79 20	Destination Por 24002 7648 53 79 21	Edit ×××××	III >		
See	Time Object Time Group ervice Protoc Service Type Profile CU_SEE DNS FINGER V FTP H_323	ol Object ME_LO	Protocol TCP/UDP TCP/UDP TCP TCP TCP	Source Port Start	Source Port End 65535 65535 65535 65535 65535 65535	Destination Por 27002 7648 53 79 20 1720	Destination Por 7648 53 79 21 1720	Edit ××××××	m N		
See	Time Object Time Group ervice Protoc Service Type Profile CU_SEE DNS FINGER V FTP H_323 HTTP	ol Object ME_LO	Protocol TCP/UDP TCP/UDP TCP TCP TCP TCP TCP	Source Port Start  Source Port Start  1  1  1  1  1  1  1  1  1  1  1  1  1	Source Port End 65535 65535 65535 65535 65535 65535 65535	Destination Por 7648 53 79 20 1720 80	Destination Por 7648 53 79 21 1720 80	Edit ** ** ** **		(c) (b)	
See	Time Object Time Group ervice Protoc Service Type Profile CU_SEE DNS FINGER FINGER FINGER H_323 HTTP HTTPS	ol Object ME_LO	Protocol TCP/UDP TCP/UDP TCP TCP TCP TCP TCP TCP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535 65535 65535	Destination Por 7648 53 79 20 1720 80 443	Destination Por 24002 7648 53 79 21 1720 80 443	Edit ** ** ** ** **	T III		
See	Time Object Time Group ervice Protoc Service Type Profile CU_SEE DNS FINGER FTP H_323 HTTP HTTPS Service Type	col cobject ME_LO constant const	Protocol TCP/UDP TCP/UDP TCP TCP TCP TCP TCP TCP TCP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535 65535 65535	Destination Por 7648 53 79 20 1720 80 443	Destination Por 7648 53 79 21 1720 80 443	Edit *** ** ** **		<b>(</b> )	
See	Time Object Time Group ervice Protoc Service Type CU_SEE DNS FINGER FINGER H_323 HTTP H_323 HTTP Service Type coming Cou	e Group	Protocol TCP/UDP TCP/UDP TCP TCP TCP TCP TCP TCP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535 65535 65535	Destination Por           7648           53           79           20           1720           80           443	Destination Por 7648 53 79 21 1720 80 443		M N	(÷	
	Time Object Time Group ervice Protoc Service Type CU_SEE DNS FINGER H_323 HTTP H_323 HTTP Service Type coming Cou	e Group ntry Object	Protocol TCP/UDP TCP/UDP TCP TCP TCP TCP TCP TCP	Source Port Start 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Source Port End 65535 65535 65535 65535 65535 65535 65535 65535	Destination Por 7648 53 79 20 1720 80 443	Destination Por 7648 53 79 21 1720 80 443		A M		

**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 :

🕼 Add 🧏 Edit 🔟 Delete 🦃 Refresh							
Profile (max length:7)	Enable	Description	VLAN ID	IPv4 Protocol	IP Address	Subnet Mask	
an1	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

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

L	AN >> General Se	tup >> Inter-LAN	Route			
	General Setup	DHCP Relay	Inter-LAN Route	RADVD	DHCPv6	
	🔽 Enable I	Routing Betwee	n Internal LANs			

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

#### **Block groep:**

IP Filter			_×
Group :	Block		
📝 Enable			
Comment :	Blokkeer alles		(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 creeren. 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		
SvsLog	Enable  Disable	
Input Interface	nasten	
Output Interface		
Ouput interface		
If no object is selec	cted in a category, the case of 'Any' is applied	
Firewall Obj	bjects	
🖃 Time Schedu	ıle	A
Time Object	:t	
Time Group	p	
Service Proto	pcol	
Service Typ	pe Object	
Service Typ	pe Group	
Incoming Cor	ountry Filter	E
Source Cou	untry Object (At most accept 15 countries)	
Out-going Co	ountry Filter	
Destination	Country Object (At most accept 15 countries)	
Source IP		
Source IP O	Object	
Source IP G	Group	
Source Use	er Profile	
Source Use	er Group	
Source LDA	AP Group	
Destination If	P	+
		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.

### **Dray** Tek

### 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.