

***DrayTek***

***InterLAN Routing***  
*DrayOS*



## Inhoudsopgave

Inter-LAN Routing .....	3
Inter-LAN Routing icm Firewall.....	5
Situatie 1 .....	5
Situatie 2.....	6

## Inter-LAN Routing

Middels de functionaliteit Inter-LAN Routing kunt u ervoor zorgen dat interne LAN segmenten met elkaar kunnen communiceren. Bij gebruik van Inter-LAN Routing zorgt u er namelijk voor dat LAN segmenten elkaar kunnen zien. Bijvoorbeeld voor het benaderen van een centrale printer of beveiliging camera's.

De functie Inter-LAN Routing is tevens te gebruiken in combinatie met de Firewall in de DrayTek modem/router. Hierdoor kunt u Inter-LAN routing verder beperken.

In deze handleiding leggen wij uit hoe u Inter-LAN Routing configureert en deze in combinatie met een Firewall kunt inrichten om verkeer van LAN segmenten onderling te beperken.

We gaan hierbij uit van onderstaande situatieschets en beschrijven twee situatie voorbeelden:

**Bedrijfs netwerk:** \_\_\_\_\_ **IP Subnet: 192.168.1.0 / 24**

**Gasten netwerk:** \_\_\_\_\_ **IP Subnet: 192.168.2.0 / 24**

### Situatie 1

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

### Situatie 2

We willen dat de Gasten alléén kunnen printen op het Bedrijfs netwerk, alle andere apparaten in het bedrijfs netwerk mogen niet benaderd worden.

*IP adres printer: 192.168.1.100*

Voor het aanmaken van meerdere LAN subnetten middels Port of Tag-based VLAN kunt u op <http://www.draytek.nl/support> een voorbeeld handleidingen vinden gerelateerd aan uw DrayTek product.

Nadat u meerdere LAN subnetten hebt ingesteld is het standaard nog niet mogelijk om onderling tussen de LAN subnetten te communiceren. Om dit mogelijk te maken gaat u in het hoofdmenu van de DrayTek Vigor naar LAN >> General Setup >> Inter-LAN Routing. Om communicatie tussen LAN subnet 1 en 2 toe te staan dient u een vinkje te zetten zoals in onderstaande situatie te zien is.

LAN >> General Setup

---

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.2	Details Page	IPv6
LAN 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	IPv6
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	IPv6
LAN 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	IPv6
LAN 6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.6.1	Details Page	IPv6
LAN 7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.7.1	Details Page	IPv6
LAN 8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.8.1	Details Page	IPv6
DMZ Port	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.17.1	Details Page	IPv6
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	Details Page	

You can configure DHCP server options here.

Force router to use "DNS server IP address" settings specified in

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMZ Port	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Note:**  
 LAN2/3/4/5/6/7/8 are available when VLAN is enabled.  
 DMZ subnet is default bound to P1, and will overwrite the settings of P1 at LAN>>VLAN page.

Klik vervolgens op **OK** om de instellingen op te slaan.

Op basis van deze setup is het mogelijk om tussen beide LAN subnetten te communiceren, let wel op: Een standaard firewall(oa Windows) blokkeert verkeer vanaf een ander LAN subnet. Om te controleren of het pingen onderling werkt, dient u de firewall tijdelijk uit te schakelen.

## Inter-LAN Routing icm Firewall

De firewall kunt u gebruiken om de geconfigureerde Inter-LAN Routing te beperken. De firewall kunt u configureren door in de webinterface van de DrayTek te navigeren naar Firewall > Filter Setup > Default Data Filter. Klik hierin op een vrij beschikbare index regel.

### Situatie 1

Onderstaand voorbeeld geeft aan hoe een firewall regel ervoor kan zorgen dat verkeer van LAN2(*Gasten netwerk*) naar LAN1(*Bedrijfs netwerk*) geblokkeerd zal worden. Verkeer van LAN1(*Bedrijfs netwerk*) naar LAN2(*Gasten netwerk*) is vanwege eerder geconfigureerde Inter-LAN Routing nog wel mogelijk.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 2

Enable

Comments: Block L2 to L1

Schedule Profile: None, None, None, None

Clear sessions when schedule is ON

Direction: LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN [Advanced]

Source IP/Country: 192.168.2.0/255.255.255.0 [Edit]

Destination IP/Country: 192.168.1.0/255.255.255.0 [Edit]

Service Type: Any [Edit]

Fragments: Don't Care

Application	Action/Profile	Syslog
Filter	Block If No Further Match	<input type="checkbox"/>
Branch to Other Filter Set	None	<input type="checkbox"/>
Sessions Control	0 / 60000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>

Advance Setting [Edit]

Klik vervolgens op **OK** om de instellingen op te slaan.

## Situatie 2

Onderstaand voorbeeld geeft aan hoe een firewall regel ervoor kan zorgen dat verkeer uit LAN subnet 2 (*Gasten netwerk*) alléén toegang mogen krijgen tot een printer gevestigd in LAN subnet 1 (*Bedrijfs netwerk*). Omdat verkeer tussen LAN1 en LAN2 nu mogelijk is vanwege eerder geconfigureerde Inter-LAN Routing, zullen we twee firewall regels aan moeten maken.

We maken eerst een "Block If No Further Match" regel aan waarin we aangeven dat al het verkeer geblokkeerd moet worden tussen (alle) LAN segmenten.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 2

Enable

Comments: Block ALL LAN

Schedule Profile: None, None, None, None

Clear sessions when schedule is ON

Direction: LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN [Advanced]

Source IP/Country: Any [Edit]

Destination IP/Country: Any [Edit]

Service Type: Any [Edit]

Fragments: Don't Care

Application	Action/Profile	Syslog
Filter	Block If No Further Match	<input type="checkbox"/>
Branch to Other Filter Set	None	<input type="checkbox"/>
Sessions Control	0 / 60000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>

Advance Setting [Edit]

**Opmerking:** Met de optie Any voor Source en Destination IP wordt VPN verkeer tussen verschillende LAN segmenten ook geblokkeerd.

Klik vervolgens op **OK** om de instellingen op te slaan.

Hierna maken we een tweede "Pass Immediately" regel aan waarin we aangeven dat LAN2(*Gasten netwerk*) toegang mag krijgen tot één IP adres(*de printer*) gevestigd in LAN1(*Bedrijfs netwerk*).

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 3

Enable

Comments

**Schedule Profile**

Clear sessions when schedule is ON

---

Direction

Source IP/Country

Destination IP/Country

Service Type

Fragments

---

Application	Action/Profile	Syslog
Filter <input type="text" value="Pass Immediately"/>	<input type="text" value="Pass Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set <input type="text" value="None"/>	<input type="text" value="None"/>	<input type="checkbox"/>
Sessions Control <input type="text" value="0 / 60000"/>	<input type="text" value="0 / 60000"/>	<input type="checkbox"/>
MAC Bind IP <input type="text" value="Non-Strict"/>	<input type="text" value="Non-Strict"/>	<input type="checkbox"/>
<b>Quality of Service</b> <input type="text" value="None"/>	<input type="text" value="None"/>	<input type="checkbox"/>
<b>User Management</b> <input type="text" value="None"/>	<input type="text" value="None"/>	<input type="checkbox"/>
<b>APP Enforcement</b> <input type="text" value="None"/>	<input type="text" value="None"/>	<input type="checkbox"/>
<b>URL Content Filter</b> <input type="text" value="None"/>	<input type="text" value="None"/>	<input type="checkbox"/>
<b>Web Content Filter</b> <input type="text" value="None"/>	<input type="text" value="None"/>	<input type="checkbox"/>
<b>DNS Filter</b> <input type="text" value="None"/>	<input type="text" value="None"/>	<input type="checkbox"/>

---

Advance Setting

Klik vervolgens op **OK** om de instellingen op te slaan.

Het LAN2(*Gasten netwerk*) zal nu alléén toegang hebben tot de printer gevestigd in LAN1(*Bedrijfs netwerk*). Al het andere verkeer tussen het bedrijfs netwerk en het Gasten netwerk is geblokkeerd.

Zie volgende pagina voor een voorbeeld van de twee geconfigureerde firewall regels.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1  
 Comments :

Rule	Enable	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137-139 to 53	Block Immediately			<a href="#">Down</a>
2	<input checked="" type="checkbox"/>	Block ALL LAN	LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN	Any	Any	Any	Block If No Further Match		<a href="#">UP</a>	<a href="#">Down</a>
3	<input checked="" type="checkbox"/>	Toegang Printer	LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN	192.168.2.0/255.255.255.0	192.168.1.100	Any	Pass Immediately		<a href="#">UP</a>	<a href="#">Down</a>
4	<input type="checkbox"/>		LAN/DMZ/RT/VPN ->	Any	Any	Any	Pass Immediately		<a href="#">UP</a>	<a href="#">Down</a>

Meer informatie over de werking van de DrayTek firewall kunt u vinden in onze firewall handleidingen op [www.draytek.nl/support](http://www.draytek.nl/support).





### **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**

© 2021 DrayTek

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

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.

### **Trademarks**

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