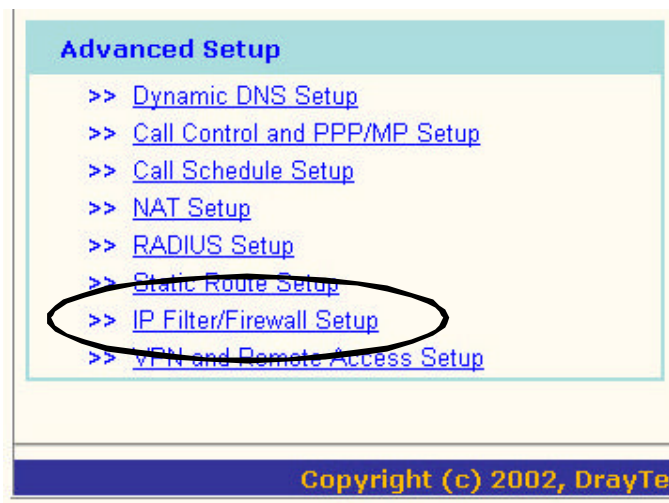
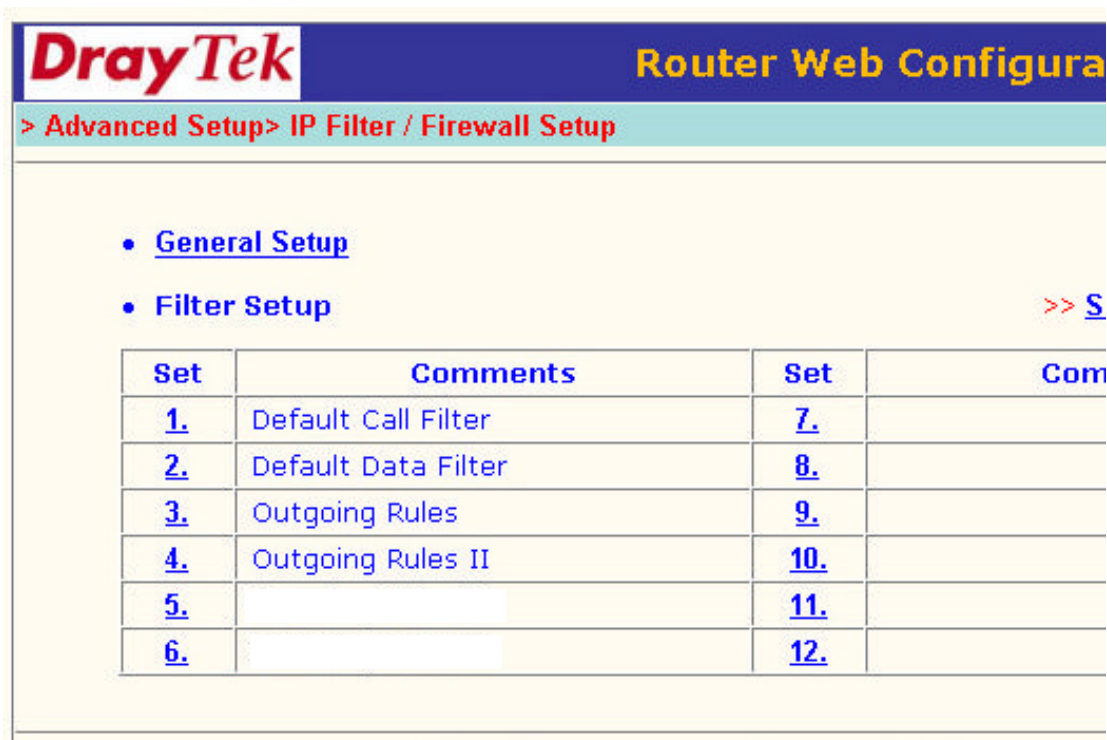


Firewall-Regeln Vigor 2200

Hier zu finden:



Anordnung der Regeln:



1. Der Default Call-Filter wird erweitert,
2. Der Default Data Filter wird nicht verändert !
- 3./4. Hier stehen die eigentlichen Regeln um das System zu schützen,

Grundeinstellungen:

DrayTek Router Web Configurator
> Advanced Setup > IP Filter / Firewall Setup << Main Menu

- **General Setup**
- Filter Setup >> Set to Factory Default

Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.	Outgoing Rules	9.	

DrayTek Router Web Configurator
> Advanced Setup > IP Filter / Firewall Setup > General Setup << Main Menu

General Setup << Back

Call Filter Enable Disable Start Filter Set

Data Filter Enable Disable Start Filter Set

Log Flag

MAC Address for Logged Packets Duplication
0x

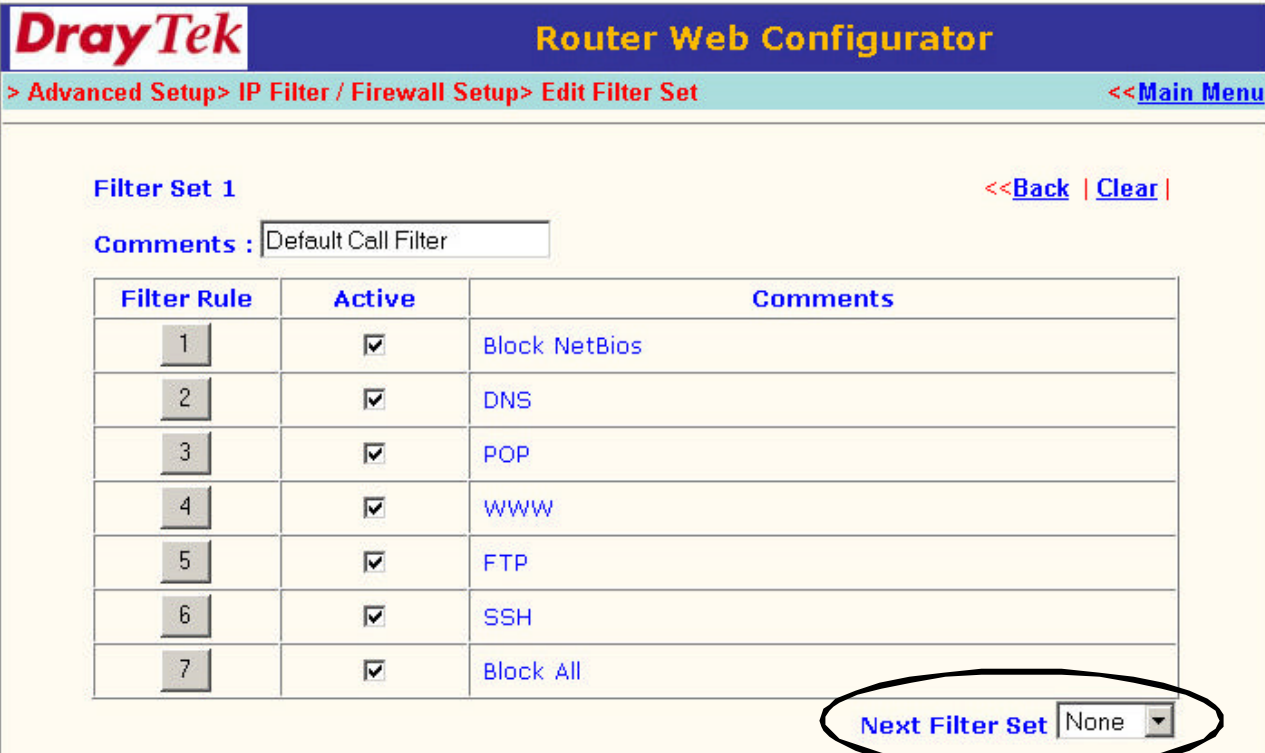
Verzweigung auf die Filter-Sets
Wichtig !!!

Log-Optionen

Default Call-Filter:

Mit den "Default Call-Filtern" kann man steuern, durch welche Protokolle der Vigor eine Verbindung mit dem Internet aufbaut.

Sinnvolle Protokolle sind unten aufgezeigt. Wichtig ist jedoch, dass von diesem Filterset auf kein weiteres verzweigt wird !



DrayTek Router Web Configurator

> [Advanced Setup](#) > [IP Filter / Firewall Setup](#) > [Edit Filter Set](#) << [Main Menu](#)

Filter Set 1 << [Back](#) | [Clear](#) |

Comments :

Filter Rule	Active	Comments
<input type="text" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios
<input type="text" value="2"/>	<input checked="" type="checkbox"/>	DNS
<input type="text" value="3"/>	<input checked="" type="checkbox"/>	POP
<input type="text" value="4"/>	<input checked="" type="checkbox"/>	WWW
<input type="text" value="5"/>	<input checked="" type="checkbox"/>	FTP
<input type="text" value="6"/>	<input checked="" type="checkbox"/>	SSH
<input type="text" value="7"/>	<input checked="" type="checkbox"/>	Block All

Next Filter Set ▼

Der allgemeine Filteraufbau wird nachher noch besprochen.

Default Data Filter:

Im "Default Data Filter" ändern wir nichts an der Grundeinstellung. Es wird nur an das dritte Filter-Set verzweigt.

The screenshot shows the DrayTek Router Web Configurator interface. The breadcrumb trail is "> Advanced Setup> IP Filter / Firewall Setup> Edit Filter Set". The page title is "Filter Set 2". There are navigation links for "<<Back" and "Clear". A "Comments" field contains the text "Default Data Filter". Below this is a table with 7 rows and 3 columns: "Filter Rule", "Active", and "Comments". The first row is active and has the comment "xNetBios -> DNS". The "Next Filter Set" dropdown menu is set to "Set#3" and is circled in red.

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	xNetBios -> DNS
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

Next Filter Set: Set#3

Outgoing Rules:

In den Outgoing Rules definieren wir selbst, was überhaupt ins Internet raus darf und was nicht. Da die paar Einstellmöglichkeiten nichtausreichen, müssen wir auch hier auf ein weiteres Filterset verzweigen. Das Wichtigste überhaupt ist die Schluß-Regel. Mit der Schlußregel verbieten wir grundsätzlich alles. Somit sind nur die vorher definierten Protokolle möglich. Die Schlußregel wird in der Fachsprache auch Clean-Up-Rule genannt.

The screenshot shows the 'Edit Filter Set' page for 'Filter Set 3'. The breadcrumb trail is '> Advanced Setup> IP Filter / Firewall Setup> Edit Filter Set'. The page title is 'Filter Set 3' with '<<Back | Clear |' links. The 'Comments' field contains 'Outgoing Rules'. Below is a table with 7 rows:

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	DNS
2	<input checked="" type="checkbox"/>	WWW
3	<input checked="" type="checkbox"/>	SSL
4	<input checked="" type="checkbox"/>	High
5	<input checked="" type="checkbox"/>	POP
6	<input checked="" type="checkbox"/>	FTP
7	<input type="checkbox"/>	

At the bottom right, the 'Next Filter Set' dropdown is set to 'Set#4' and is circled in black. An 'OK' button is centered at the bottom. The footer reads 'Copyright (c) 2002, DrayTek Corp. All Rights Reserved.'

The screenshot shows the 'Edit Filter Set' page for 'Filter Set 4'. The breadcrumb trail is '> Advanced Setup> IP Filter / Firewall Setup> Edit Filter Set'. The page title is 'Filter Set 4' with '<<Back | Clear |' links. The 'Comments' field contains 'Outgoing Rules II'. Below is a table with 7 rows:

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	SMTP
2	<input checked="" type="checkbox"/>	ICMP
3	<input checked="" type="checkbox"/>	SNMP
4	<input checked="" type="checkbox"/>	HTTP Proxy
5	<input checked="" type="checkbox"/>	Telnet/SSH
6	<input type="checkbox"/>	
7	<input checked="" type="checkbox"/>	Deny all

The 'Deny all' row (row 7) is circled in black. At the bottom right, the 'Next Filter Set' dropdown is set to 'Set#5'. An 'OK' button is centered at the bottom. The footer reads 'Copyright (c) 2002, DrayTek Corp. All Rights Reserved.'

Regeln:

Wie schon erwähnt, sehen die Regeln für der "Default Call-Filter" und den "Outgoing Rules" prinzipiell gleich aus.

Nachfolgend eine Beschreibung einer Regel für DNS, also der Namensauflösung.

Wie die anderen Regeln aufgebaut sind, ist nachfolgend tabellarisch dargestellt.

DrayTek Router Web Configurator

> [Advanced Setup](#) > [IP Filter / Firewall Setup](#) > [Edit Filter Set](#) > [Edit Filter Rule](#) << [Main Menu](#)

Filter Set 3 Rule 1 << [Back](#) | [Clear](#) |

Comments : **Check to enable the Filter Rule**

Pass or Block <input type="text" value="Pass Immediately"/>	Branch to Other Filter Set <input type="text" value="None"/>
<input type="checkbox"/> Duplicate to LAN	<input type="checkbox"/> Log

Direction <input type="text" value="OUT"/>	Protocol <input type="text" value="UDP"/>			
Source IP Address <input type="text" value="172.17.1.1"/>	Subnet Mask <input type="text" value="255.255.255.0 (/24)"/>	Operator <input type="text" value=">"/>	Start Port <input type="text" value="1024"/>	End Port <input type="text"/>
Destination <input type="text" value="any"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text" value="="/>	<input type="text" value="53"/>	<input type="text"/>

<input checked="" type="checkbox"/> Keep State	<input type="checkbox"/> Source Route	Fragments <input type="text" value="Don't Care"/>
--	---------------------------------------	---

Copyright (c) 2002, DrayTek Corp. All Rights Reserved.

Comments	Klar, eine Bezeichnung für die Regel,
Check to enable...	Sollte auch klar sein,
Pass or Block	Hier geben wir an, ob diese Regel eine positive oder negative ist, also ob geblockt oder durchgelassen wird.
Direction	Da wir nur ausgehenden Datenverkehr erlauben, sollte nur OUT (außer in den Call-Filtern) verwendet werden,
Protocol	Hier können wir TCP/UDP/ICMP auswählen,
Source	Die Quelle, also unser internes LAN, als Ports sind alle über 1024 zuzulassen,
Destination	Das Ziel der Regel, any heißt, das ganze Internet Zielport ist der jeweiligen Anwendung zugeordnet,
Keep State	Hiermit aktivieren wir die "Stateful"-Funktion der Firewall. Damit ersparen wir uns die Regeln für den Paket-Rückweg.

Filterregeln kontrollieren per Telnet:

Kontrollieren lassen sich die Regeln über das Telnet-GUI.

Der Befehl lautet:

ipf view -r

Die Ausgabe sollte dann etwa wie folgt aussehen:

```
router> ipf view -r
Call Filter Rules
0 0 @1 block in quick proto tcp/udp from any port 136 >< 140 to any
0 0 @2 pass in quick proto udp from 172.17.1.0/24 port > 1024 to any port = domain keep state
0 0 @3 pass in quick proto tcp from 172.17.1.0/24 port > 1024 to any port = pop3 keep state
0 0 @4 pass in quick proto tcp from 172.17.1.0/24 port > 1024 to any port = www keep state
0 0 @5 pass in quick proto tcp from 172.17.1.0/24 port > 1024 to any port 19 >< 22 keep state
0 0 @6 pass in quick proto tcp from 172.17.1.2/32 port > 1024 to any port = ssh
0 0 @7 block in quick from any to any

Data Filter Rules
Incoming Filter Rules
0 0 @1 pass in log quick proto tcp from 53.142.0.0/16 port 1023 >< 0 to 172.17.1.0/24 port = ssh
0 0 @2 block in quick from any to any
Outgoing Filter Rules
0 0 @1 block out quick proto tcp/udp from any port 136 >< 140 to any port = domain
0 0 @2 pass out quick proto udp from 172.17.1.0/24 port > 1024 to any port = domain keep state
0 0 @3 pass out quick proto tcp from 172.17.1.0/24 port > 1024 to any port = www keep state
0 0 @4 pass out quick proto tcp from 172.17.1.0/24 port > 1024 to any port = 443 keep state
0 0 @5 pass out quick proto tcp/udp from 172.17.1.0/24 port > 1024 to any port > 1024 keep state
0 0 @6 pass out quick proto tcp from 172.17.1.0/24 port > 1024 to any port = pop3 keep state
0 0 @7 pass out quick proto tcp from 172.17.1.0/24 port > 1024 to any port 19 >< 22 keep state
0 0 @8 pass out quick proto tcp from 172.17.1.0/24 port > 1024 to any port = smtp keep state
0 0 @9 pass out quick proto icmp from 172.17.1.0/24 to any keep state
0 0 @10 pass out quick proto udp from 172.17.1.0/24 port > 1024 to 172.17.1.0/24 port = 161
                                keep state
0 0 @12 pass out quick proto tcp from 172.17.1.0/24 port > 1024 to any port = ssh keep state
0 0 @13 block out quick from any to any

router>
```

Mit dem Befehl :

ipf view

kann man sich eine Statistik über die Regeln ansehen:

```
router> ipf view
input packets:          blocked 786 passed 14890 nomatch 0 counted 0
output packets:        blocked 521 passed 14875 nomatch 0 counted 0
input packets logged:  blocked 786 passed 0
output packets logged: blocked 521 passed 0
packets logged:        input 0 output 352
log failures:         input 2 output 0
fragment state(in):   kept 0 lost 0
fragment state(out):  kept 0 lost 0
packet state(in):     kept 0 lost 0
packet state(out):    kept 13763 lost 46
ICMP replies:        4      TCP RSTs sent: 0
Result cache hits(in): 0      (out): 0
IN Pullups succeeded: 0      failed: 0
OUT Pullups succeeded: 0      failed: 0
TCP cksum fails(in):  0      (out): 0
Packet log flags set: (20000000)
                    packets blocked by filter

router>
```

Empfohlene Regeln:

Default Call Filter

Regelname	Pass or Block	Direction	Protocol	Source IP/Mask	Source Port	Destination /Mask	Destination Port	Keep State	Beschreibung
Block Netbios	Block	IN	TCP/UDP	any/32	= 137 - 139	any/32	=	-	Kein Windoof-Klumb
DNS	Pass	IN	UDP	172.17.1.1/24	> 1024	any/32	= 53	x	Namensauflösung
POP	Pass	IN	TCP	172.17.1.1/24	> 1024	any/32	= 110	x	Mails abholen
WWW	Pass	IN	TCP	172.17.1.1/24	> 1024	any/32	= 80	x	Internet-Surfen
FTP	Pass	OUT	TCP	172.17.1.1/24	> 1024	any/32	= 20 - 21	x	FTP
SSH	Pass	OUT	TCP	172.17.1.1/24	> 1024	any/32	= 22	x	SSH
Block all	Block	IN	any	any/32	=	any/32	=	-	sonst nix

Outgoing Rules

Regelname	Pass or Block	Direction	Protocol	Source IP/Mask	Source Port	Destination /Mask	Destination Port	Keep State	Beschreibung
DNS	Pass	OUT	UDP	172.17.1.1/24	> 1024	any/32	= 53	x	Namensauflösung
WWW	Pass	OUT	TCP	172.17.1.1/24	> 1024	any/32	= 80	x	Internet-Surfen
SSL	Pass	OUT	TCP	172.17.1.1/24	> 1024	any/32	= 443	x	HTTPS
High	Pass	OUT	TCP/UDP	172.17.1.1/24	> 1024	any/32	> 1024	x	High-Port für passives FTP
POP	Pass	OUT	TCP	172.17.1.1/24	> 1024	any/32	= 110	x	Mails abholen
FTP	Pass	OUT	TCP	172.17.1.1/24	> 1024	any/32	= 20 - 21	x	FTP
SMTP	Pass	OUT	TCP	172.17.1.1/24	> 1024	any/32	= 25	x	Mails verschicken
ICMP	Pass	OUT	ICMP	172.17.1.1/24	=	any/32	=	x	Ping, Traceroute,...
Telnet/SSH	Pass	OUT	TCP	172.17.1.1/24	> 1024	any/32	= 22 - 23	x	Telnet und SSH
Deny all out	Block	OUT	any	any/32	=	any/32	=	-	sonst nix