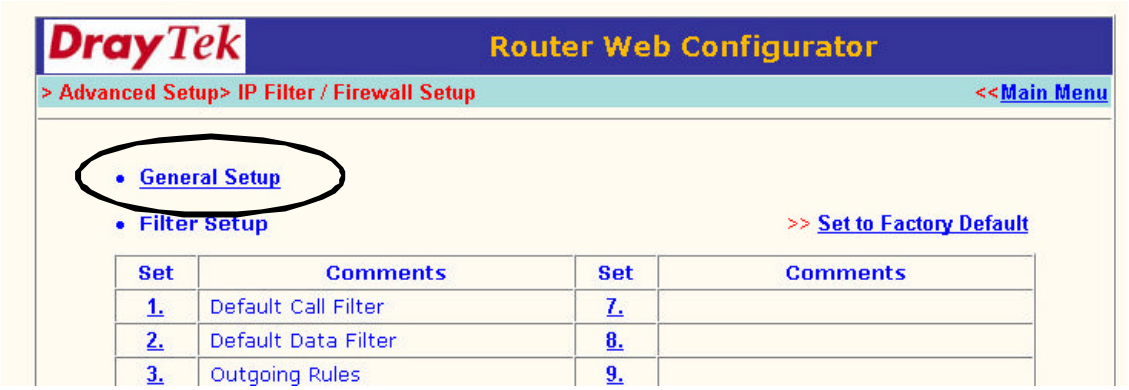
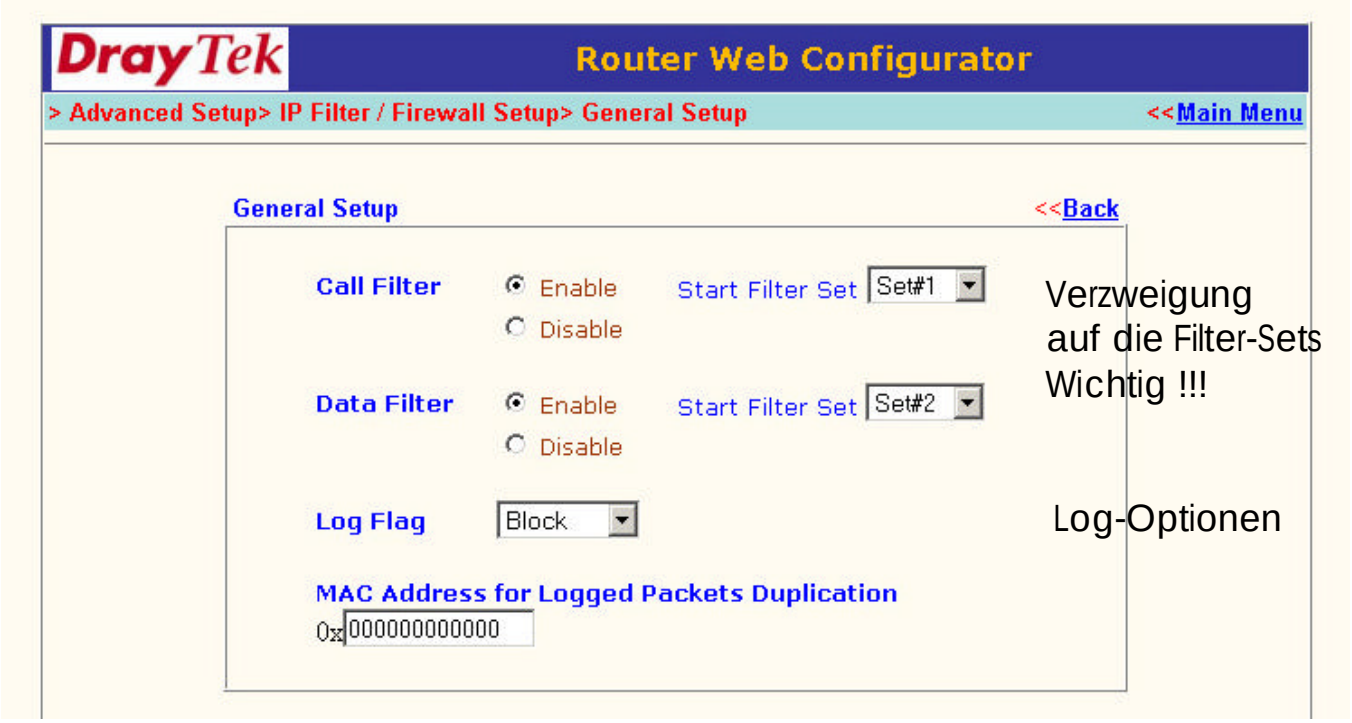
Grundeinstellungen:





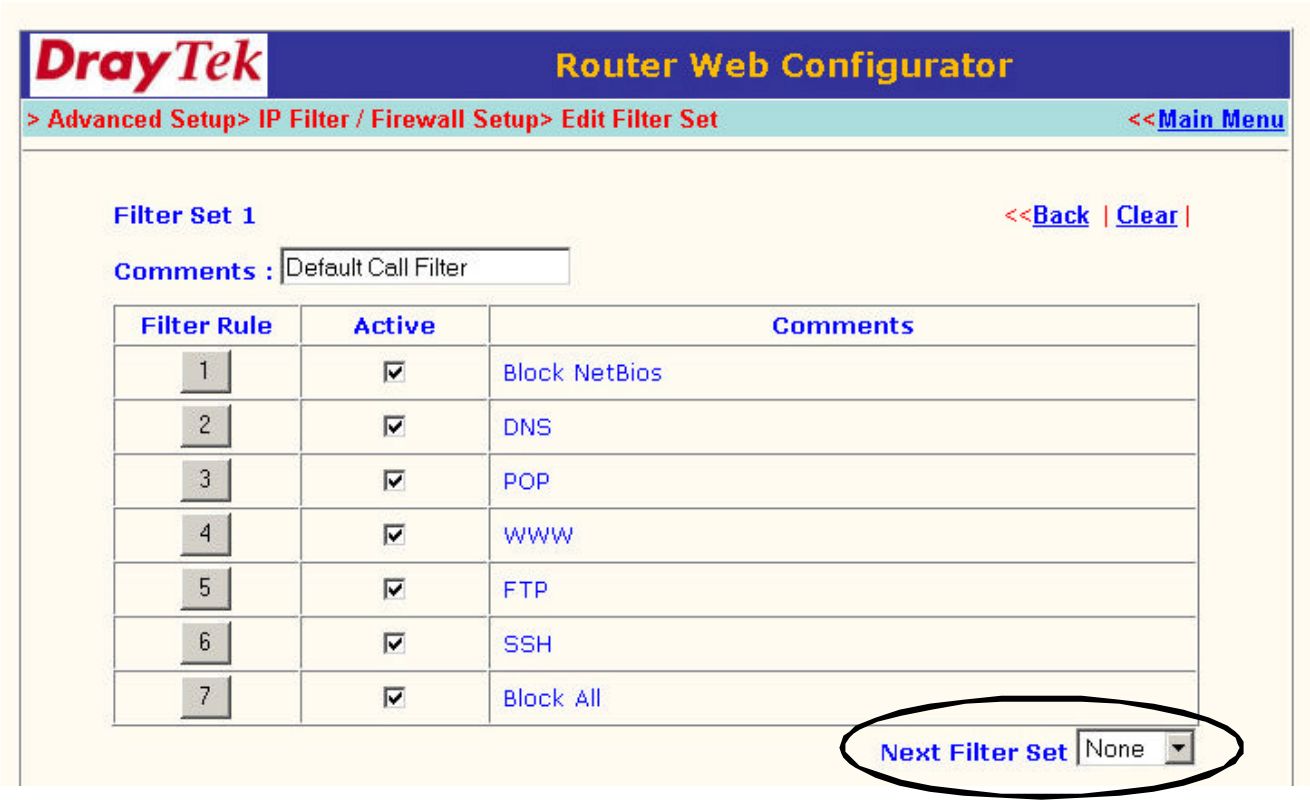
Verzweigung auf die Filter-Sets Wichtig !!!

Log-Optionen

Default Call-Filter:

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

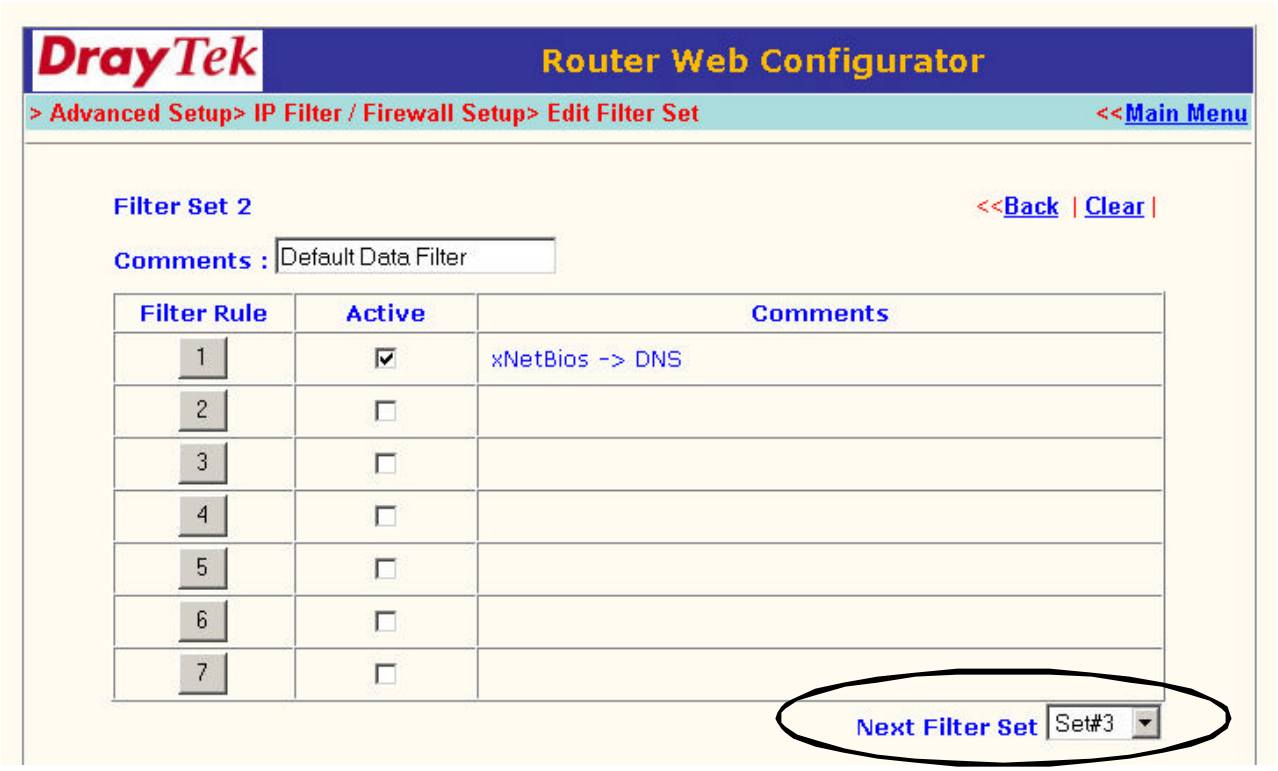
Sinnvolle Protokolle sind unten aufgezeigt. Wichtig ist jedoch, dass von diesem Filterset auf kein weiteres verzweigt wird !



Der allgemeine Filteraufbau wird nachher noch besprochen.

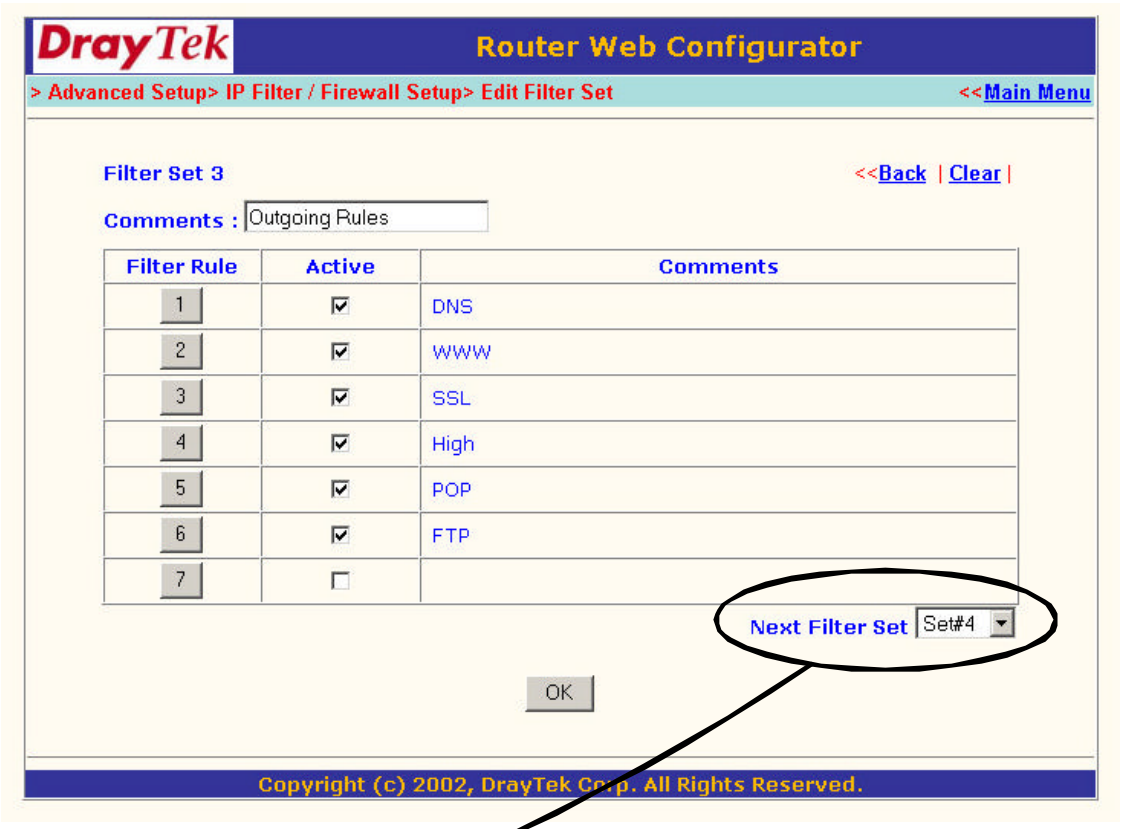
Default Data Filter:

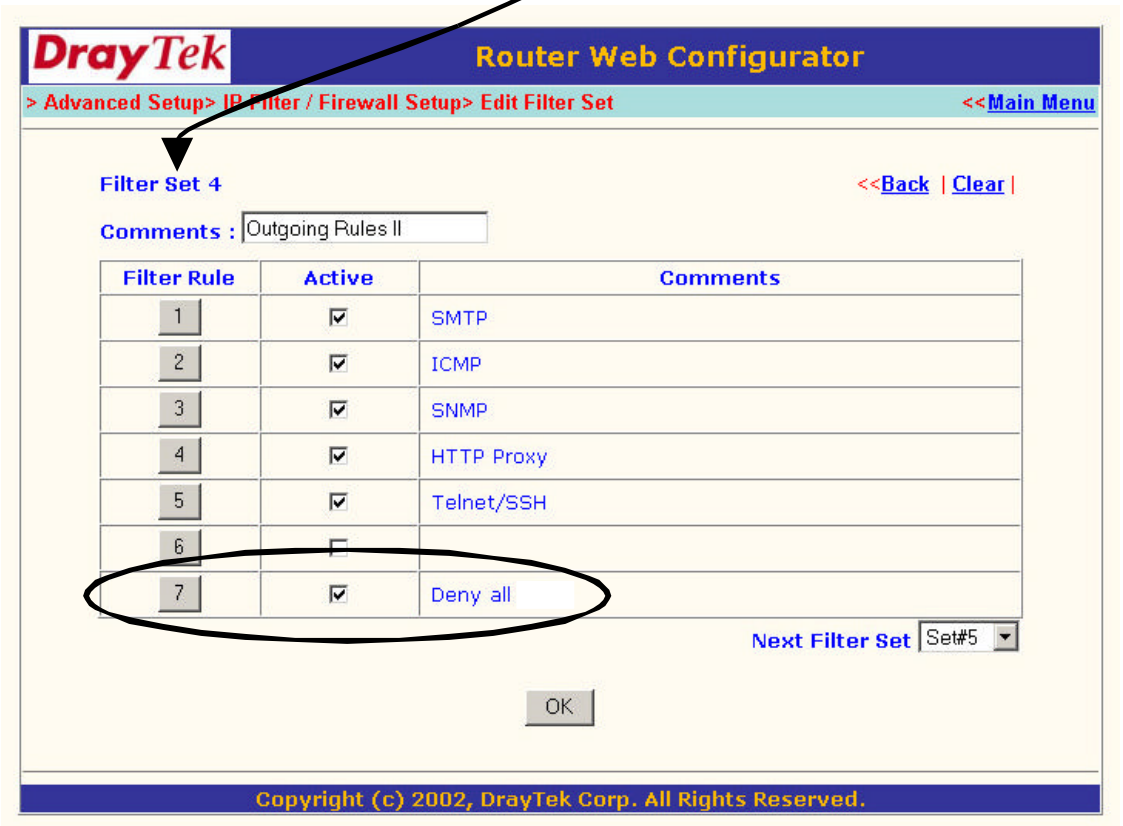
Im“Default Data Filter” ändern wir nichts an der Grundeinstellung. Es wird nur an das dritte Filter-Set verzweigt.



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 weiters 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.

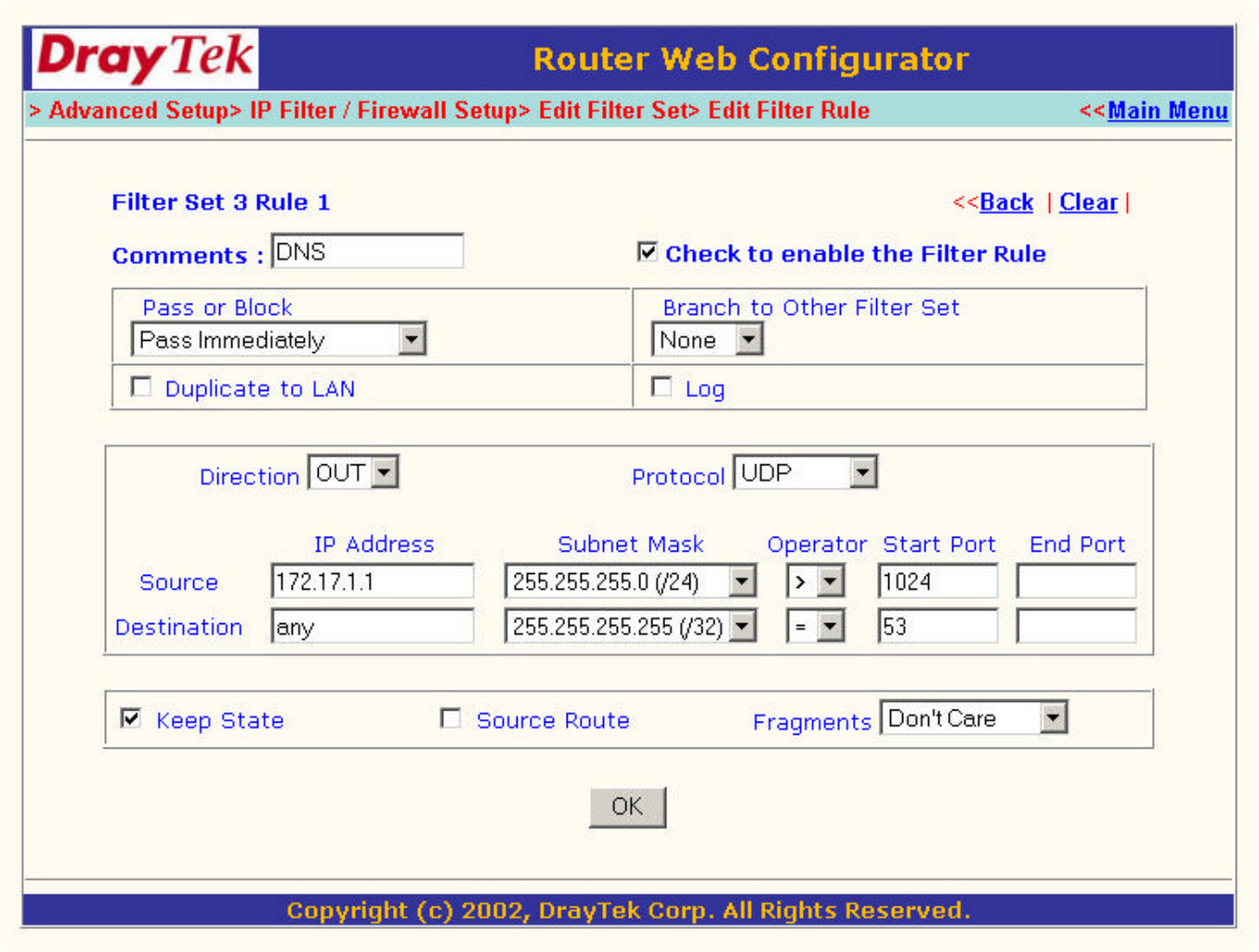




Regeln:

Wie schon erwähnt, sehen die Regeln für der “Default Call-Filter” und den “Outgoing Rules” prizipiell gleich aus.
Nachfolgend eine Beschreibung einer Regel für DNS, also der Namensauflösung.

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



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 o b geblockt oder durchgelassen wird.
Direction	Da wir nur ausgehenden Datenverkehrerlauben, 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>
```