

## Rule set 1

```
# Generated by iptables-save v1.4.14 on Thu Oct 29 10:59:25 2015
*filter
:INPUT DROP [1:229]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth1 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Thu Oct 29 10:59:25 2015
# Generated by iptables-save v1.4.14 on Thu Oct 29 10:59:25 2015
*mangle
:PREROUTING ACCEPT [658:32445]
:INPUT ACCEPT [658:32445]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [891:68234]
:POSTROUTING ACCEPT [891:68234]
COMMIT
# Completed on Thu Oct 29 10:59:25 2015
# Generated by iptables-save v1.4.14 on Thu Oct 29 10:59:25 2015
*nat
:PREROUTING ACCEPT [1:229]
:POSTROUTING ACCEPT [3:450]
:OUTPUT ACCEPT [3:450]
-A POSTROUTING -o eth0 -j SNAT --to-source 195.233.192.1
COMMIT
# Completed on Thu Oct 29 10:59:25 2015
```

## Rule set 2

```
# Generated by iptables-save v1.4.21 on Wen Dec 09 12:18:31 2015
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:TCP - [0:0]
:UDP - [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -p icmp -m icmp --icmp-type 8 -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p udp -m conntrack --ctstate NEW -j UDP
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j TCP
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
-A INPUT -p tcp -j REJECT --reject-with tcp-reset
-A INPUT -j REJECT --reject-with icmp-proto-unreachable
-A TCP -p tcp -m tcp --dport 22 -j ACCEPT
COMMIT
# Completed on Wen Dec 09 12:18:31 2015
```

## Rule set 3

```
# Generated by iptables-save v1.4.21 on Mon Jan 4 14:55:01 2016
*raw
:PREROUTING ACCEPT [4:516]
:OUTPUT ACCEPT [4:280]
-A PREROUTING ! -s 10.137.2.15/32 -i vif112.0 -j DROP
COMMIT
# Completed on Mon Jan 4 14:55:01 2016
# Generated by iptables-save v1.4.21 on Mon Jan 4 14:55:01 2016
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [4:280]
:POSTROUTING ACCEPT [0:0]
:PR-QBS - [0:0]
:PR-QBS-SERVICES - [0:0]
-A PREROUTING -j PR-QBS
-A PREROUTING -j PR-QBS-SERVICES
-A POSTROUTING -o vif+ -j ACCEPT
-A POSTROUTING -o lo -j ACCEPT
-A POSTROUTING -j MASQUERADE
-A PR-QBS -d 10.137.2.1/32 -p udp -m udp --dport 53 -j DNAT --to-destination 10.137.1.1
-A PR-QBS -d 10.137.2.1/32 -p tcp -m tcp --dport 53 -j DNAT --to-destination 10.137.1.1
-A PR-QBS -d 10.137.2.254/32 -p udp -m udp --dport 53 -j DNAT --to-destination 10.137.1.254
-A PR-QBS -d 10.137.2.254/32 -p tcp -m tcp --dport 53 -j DNAT --to-destination 10.137.1.254
COMMIT
# Completed on Mon Jan 4 14:55:01 2016
# Generated by iptables-save v1.4.21 on Mon Jan 4 14:55:01 2016
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [4:280]
-A INPUT -i vif+ -p udp -m udp --dport 68 -j DROP
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i vif0.0 -j ACCEPT
-A FORWARD -i vif+ -o vif+ -j DROP
-A FORWARD -s 10.137.2.15/32 -d 10.137.1.1/32 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -s 10.137.2.15/32 -d 10.137.1.254/32 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -s 10.137.2.15/32 -d 10.137.1.1/32 -p tcp -m tcp --dport 53 -j ACCEPT
-A FORWARD -s 10.137.2.15/32 -d 10.137.1.254/32 -p tcp -m tcp --dport 53 -j ACCEPT
-A FORWARD -s 10.137.2.15/32 -p icmp -j ACCEPT
-A FORWARD -s 10.137.2.15/32 -d 10.137.255.254/32 -p tcp -m tcp --dport 8082 -j DROP
-A FORWARD -s 10.137.2.15/32 -j ACCEPT
COMMIT
# Completed on Mon Jan 4 14:55:01 2016
```

## Rule set 4

```
# Generated by iptables-save v1.4.21 on Thu Apr 14 11:26:14 2016
*mangle
:PREROUTING ACCEPT [168740:136206530]
:INPUT ACCEPT [4643:958901]
:FORWARD ACCEPT [163957:135236766]
:OUTPUT ACCEPT [4475:2161128]
:POSTROUTING ACCEPT [168437:137398054]
-A PREROUTING -m policy --dir in --pol ipsec -j NFLOG --nflog-group 5
-A POSTROUTING -m policy --dir out --pol ipsec -j NFLOG --nflog-group 5
COMMIT
# Completed on Thu Apr 14 11:26:14 2016
# Generated by iptables-save v1.4.21 on Thu Apr 14 11:26:14 2016
*nat
:PREROUTING ACCEPT [6538:472590]
:INPUT ACCEPT [37:7803]
:OUTPUT ACCEPT [266:15960]
:POSTROUTING ACCEPT [922:60960]
-A PREROUTING -i br0v100 -p udp -m udp --dport 15000:30000 -j DNAT --to-destination 172.16.199.126
-A PREROUTING -i br0v100 -p udp -m udp --dport 5060 -j DNAT --to-destination 172.16.199.126
-A POSTROUTING -s 172.16.201.101/32 -d 35.126.36.212/32 -j ACCEPT
-A POSTROUTING -s 172.16.201.101/32 -d 35.126.36.213/32 -j ACCEPT
-A POSTROUTING -s 172.16.201.102/32 -d 35.126.36.212/32 -j ACCEPT
-A POSTROUTING -s 172.16.201.102/32 -d 35.126.36.213/32 -j ACCEPT
-A POSTROUTING -d 172.16.0.0/26 -j SNAT --to-source 172.16.0.1
-A POSTROUTING -s 192.168.100.0/24 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 192.168.101.0/24 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 172.16.199.0/28 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 172.16.199.16/28 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 172.16.199.32/28 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 172.16.0.0/26 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 172.16.200.0/21 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 172.16.199.64/26 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 192.168.0.0/24 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 172.16.198.0/24 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 10.8.0.0/24 -o br0v100 -j SNAT --to-source 35.126.36.234
-A POSTROUTING -s 10.8.0.0/24 -o br0v502 -j SNAT --to-source 172.16.200.1
-A POSTROUTING -s 10.8.0.0/24 -o br0v700 -j SNAT --to-source 172.16.200.1
-A POSTROUTING -s 10.8.0.0/24 -o br0v701 -j SNAT --to-source 172.16.200.1
-A POSTROUTING -s 10.8.0.0/24 -o br0v702 -j SNAT --to-source 172.16.200.1
-A POSTROUTING -s 10.224.0.0/20 -o br0v100 -j SNAT --to-source 35.126.36.234
COMMIT
# Completed on Thu Apr 14 11:26:14 2016
# Generated by iptables-save v1.4.21 on Thu Apr 14 11:26:14 2016
*filter
:INPUT ACCEPT [4588:951451]
:FORWARD ACCEPT [163873:135176001]
:OUTPUT ACCEPT [4432:2162468]
:LOG_DROP [0:0]
```

```

-A INPUT -m addrtype ! --dst-type LOCAL -m policy --dir in --pol ipsec -j NFLOG --nflog-group 5
-A INPUT -m addrtype --dst-type LOCAL -m policy --dir in --pol ipsec -j NFLOG --nflog-group 5
-A INPUT -p udp -m multiport --dports 500,4500 -j NFLOG --nflog-group 5
-A INPUT -p ah -j NFLOG --nflog-group 5
-A INPUT -p esp -j NFLOG --nflog-group 5
-A INPUT -s 35.126.36.215/24 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 192.168.100.0/24 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 192.168.101.0/24 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.199.0/28 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.199.16/28 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.199.32/28 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.0.0/26 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.200.0/21 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.199.64/26 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.8.0.0/24 -i br0v100 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i br0v100 -p tcp -m tcp --dport 22 -j DROP
-A FORWARD -s 192.168.101.0/24 -o br0v502 -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -s 192.168.100.0/24 -o br0v700 -j ACCEPT
-A FORWARD -s 192.168.101.0/24 -o br0v700 -j ACCEPT
-A FORWARD -s 172.16.199.0/28 -o br0v700 -j ACCEPT
-A FORWARD -s 172.16.199.16/28 -o br0v700 -j ACCEPT
-A FORWARD -s 172.16.199.32/28 -o br0v700 -j ACCEPT
-A FORWARD -s 172.16.0.0/26 -o br0v700 -j ACCEPT
-A FORWARD -s 172.16.200.0/21 -o br0v700 -j ACCEPT
-A FORWARD -s 172.16.199.64/26 -o br0v700 -j ACCEPT
-A FORWARD -s 192.168.0.0/24 -o br0v700 -j ACCEPT
-A FORWARD -s 10.8.0.0/24 -o br0v700 -j ACCEPT
-A FORWARD -s 35.126.37.87/32 -o br0v700 -j ACCEPT
-A FORWARD -s 209.248.190.193/32 -o br0v700 -j ACCEPT
-A FORWARD -s 41.10.56.224/20 -o br0v700 -p udp -m multiport --ports 5060 -j ACCEPT
-A FORWARD -s 41.121.8.27/20 -o br0v700 -p udp -m multiport --ports 5060 -j ACCEPT
-A FORWARD -s 41.10.56.224/20 -o br0v700 -p icmp -j ACCEPT
-A FORWARD -s 41.121.8.27/20 -o br0v700 -p icmp -j ACCEPT
-A FORWARD -o br0v700 -p udp -m multiport --ports 5060 -j DROP
-A FORWARD -s 190.69.176.151/32 -o br0v700 -p tcp -m multiport --ports 3478,3479,10000,10001 -j ACCEPT
-A FORWARD -s 190.69.176.151/32 -o br0v700 -p udp -m multiport --ports 3478,3479,10000,10001 -j ACCEPT
-A FORWARD -o br0v700 -p tcp -m multiport --ports 3478,3479,10000,10001 -j DROP
-A FORWARD -o br0v700 -p udp -m multiport --ports 3478,3479,10000,10001 -j DROP
-A FORWARD -s 41.10.56.224/20 -o br0v700 -p udp -j ACCEPT
-A FORWARD -s 41.121.8.27/20 -o br0v700 -p udp -j ACCEPT
-A FORWARD -s 35.247.96.203/19 -o br0v700 -p udp -j ACCEPT
-A FORWARD -s 35.173.8.195/24 -o br0v700 -p udp -j ACCEPT
-A FORWARD -o br0v700 -p udp -m multiport --ports 15000:30000 -j DROP
-A FORWARD -s 35.126.36.96/32 -o br0v700 -j ACCEPT
-A FORWARD -o br0v700 -j LOG
-A OUTPUT -m policy --dir out --pol ipsec -j NFLOG --nflog-group 5
-A OUTPUT -p udp -m multiport --dports 500,4500 -j NFLOG --nflog-group 5
-A OUTPUT -p ah -j NFLOG --nflog-group 5

```

```
-A OUTPUT -p esp -j NFLOG --nflog-group 5  
COMMIT  
# Completed on Thu Apr 14 11:26:14 2016
```

## Rule set 5

```
# Generated by iptables-save v1.4.21 on Mon Nov 23 13:56:38 2015
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:fail2ban-ssh - [0:0]
-A INPUT -p tcp -m multiport --dports 22 -j fail2ban-ssh
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m state --state NEW -m multiport --dports 88,123 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m multiport --dports 22,88,4949 -j ACCEPT
-A INPUT -s 192.168.1.0/24 -p tcp -m state --state NEW -m tcp --dport 754 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -m limit --limit 2/sec -j ACCEPT
-A fail2ban-ssh -j RETURN
COMMIT
# Completed on Mon Nov 23 13:56:38 2015
```

## Rule set 6

```
# Generated by iptables-save v1.4.21 on Wed Jan 27 14:01:36 2016
*nat
:PREROUTING ACCEPT [5783:628415]
:INPUT ACCEPT [2017:311774]
:OUTPUT ACCEPT [469:36017]
:POSTROUTING ACCEPT [2618:182003]
-A OUTPUT -p udp -m udp --dport 53
-A OUTPUT -p tcp -m tcp --dport 53
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Wed Jan 27 14:01:36 2016
# Generated by iptables-save v1.4.21 on Wed Jan 27 14:01:36 2016
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i eth1 -p udp -m udp --sport 67:68 --dport 67:68 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 61141 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -i eth1 -p tcp -m tcp --dport 3306 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 5432 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 5432 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 6659 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 6667 -j ACCEPT
-A INPUT -p udp -m udp --dport 6659 -j ACCEPT
-A INPUT -p udp -m udp --dport 6667 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 25 --dport 25 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 2049 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p udp -m udp --dport 2049 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 111 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p udp -m udp --dport 111 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 137 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p udp -m udp --dport 137 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 138 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p udp -m udp --dport 138 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 139 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p udp -m udp --dport 139 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 389 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p udp -m udp --dport 389 -j ACCEPT
-A INPUT -p udp -m udp --dport 123 -j ACCEPT
-A INPUT -s 192.168.11.0/24 -p udp -m udp --dport 8140 -j ACCEPT
```



```

-A INPUT -s 192.168.11.0/24 -p tcp -m tcp --dport 8140 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -j DROP
-A FORWARD -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 61141 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 53 -j ACCEPT
-A FORWARD -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 3306 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 5432 -j ACCEPT
-A FORWARD -p tcp -m tcp --sport 5432 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 6659 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 6667 -j ACCEPT
-A FORWARD -p udp -m udp --dport 6659 -j ACCEPT
-A FORWARD -p udp -m udp --dport 6667 -j ACCEPT
-A FORWARD -p tcp -m tcp --dport 25 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p tcp -m tcp --dport 2049 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p udp -m udp --dport 2049 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p tcp -m tcp --dport 111 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p udp -m udp --dport 111 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p tcp -m tcp --dport 137 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p udp -m udp --dport 137 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p tcp -m tcp --dport 138 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p udp -m udp --dport 138 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p tcp -m tcp --dport 139 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p udp -m udp --dport 139 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p tcp -m tcp --dport 389 -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p udp -m udp --dport 389 -j ACCEPT
-A FORWARD -p udp -m udp --dport 123 -j ACCEPT
-A FORWARD -s 192.168.11.0/24 -p udp -m udp --dport 8140 -j ACCEPT
-A FORWARD -s 192.168.11.0/24 -p tcp -m tcp --dport 8140 -j ACCEPT
-A FORWARD -j DROP
-A OUTPUT -p udp -m udp --sport 67:68 --dport 67:68 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 61141 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --sport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 3306 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 5432 -j ACCEPT

```

```
-A OUTPUT -p tcp -m tcp --sport 5432 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 6659 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 6667 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 6659 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 6667 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 25 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 2049 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p udp -m udp --dport 2049 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 111 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p udp -m udp --dport 111 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 137 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p udp -m udp --dport 137 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 138 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p udp -m udp --dport 138 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 139 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p udp -m udp --dport 139 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 389 -j ACCEPT
-A OUTPUT -s 192.168.0.0/16 -p udp -m udp --dport 389 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 123 -j ACCEPT
-A OUTPUT -s 192.168.11.0/24 -p udp -m udp --dport 8140 -j ACCEPT
-A OUTPUT -s 192.168.11.0/24 -p tcp -m tcp --dport 8140 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -j DROP
COMMIT
# Completed on Wed Jan 27 14:01:36 2016
```

## Rule set 7

```
# Generated by iptables-save v1.6.0 on Sun Jul 3 15:28:59 2016
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [59:9932]
:DOS_PROTECT - [0:0]
:FORWARD_FIREWALL - [0:0]
:INPUT_FIREWALL - [0:0]
-A INPUT -j DOS_PROTECT
-A INPUT -j INPUT_FIREWALL
-A FORWARD -j FORWARD_FIREWALL
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth1 -p icmp -m icmp --icmp-type 8 -j DROP
-A DOS_PROTECT -i eth1 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 1/sec -j
RETURN
-A DOS_PROTECT -i eth1 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -j DROP
-A DOS_PROTECT -i eth1 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m limit --limit 10000/sec
--limit-burst 100 -j RETURN
-A DOS_PROTECT -i eth1 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j DROP
-A DOS_PROTECT -i eth0 -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j RETURN
-A DOS_PROTECT -i eth0 -p icmp -m icmp --icmp-type 8 -j DROP
-A DOS_PROTECT -i eth0 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 1/sec -j
RETURN
-A DOS_PROTECT -i eth0 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -j DROP
-A DOS_PROTECT -i eth0 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m limit --limit 10000/sec
--limit-burst 100 -j RETURN
-A DOS_PROTECT -i eth0 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j DROP
-A FORWARD_FIREWALL -i lo -j ACCEPT
-A FORWARD_FIREWALL -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD_FIREWALL -p udp -m multiport --sports 65001,5004,5002 -j RETURN
-A FORWARD_FIREWALL -p tcp -m multiport --dports 80,443,50002,50001,9025:9040 -j RETURN
-A FORWARD_FIREWALL -p udp -m multiport --dports 1900,65001,5004,5002 -j RETURN
-A FORWARD_FIREWALL -p tcp -m multiport --dports 873,631,515,3260,3261,3262,21 -j DROP
-A FORWARD_FIREWALL -p tcp -m multiport --dports 548,443,80,3493,3306,22,23 -j DROP
-A FORWARD_FIREWALL -p udp -m multiport --dports 68,67,123,514,19999,5353,161 -j DROP
-A FORWARD_FIREWALL -p tcp -m multiport --dports 111,892,2049 -j DROP
-A FORWARD_FIREWALL -p udp -m multiport --dports 111,892,2049 -j DROP
-A FORWARD_FIREWALL -s 192.168.0.0/16 -j RETURN
-A FORWARD_FIREWALL -j DROP
-A FORWARD_FIREWALL -i eth0 -j DROP
-A FORWARD_FIREWALL -i eth1 -j RETURN
-A INPUT_FIREWALL -i lo -j ACCEPT
-A INPUT_FIREWALL -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT_FIREWALL -p udp -m multiport --sports 65001,5004,5002 -j RETURN
-A INPUT_FIREWALL -p tcp -m multiport --dports 80,443,50002,50001,9025:9040 -j RETURN
-A INPUT_FIREWALL -p udp -m multiport --dports 1900,65001,5004,5002 -j RETURN
-A INPUT_FIREWALL -p tcp -m multiport --dports 873,631,515,3260,3261,3262,21 -j DROP
-A INPUT_FIREWALL -p tcp -m multiport --dports 548,443,80,3493,3306,22,23 -j DROP
```

```
-A INPUT_FIREWALL -p udp -m multiport --dports 68,67,123,514,19999,5353,161 -j DROP
-A INPUT_FIREWALL -p tcp -m multiport --dports 111,892,2049 -j DROP
-A INPUT_FIREWALL -p udp -m multiport --dports 111,892,2049 -j DROP
-A INPUT_FIREWALL -s 192.168.0.0/16 -j RETURN
-A INPUT_FIREWALL -j DROP
-A INPUT_FIREWALL -i eth0 -j DROP
-A INPUT_FIREWALL -i eth1 -j RETURN
COMMIT
# Completed on Sun Jul 3 15:28:59 2016
```

## Rule set 8

```
# Generated by iptables-save v1.4.8 on Mon Mar 2 13:23:48 2015
*mangle
:PREROUTING ACCEPT [1651136551:1999075911109]
:INPUT ACCEPT [1606555924:1968435594521]
:FORWARD ACCEPT [1438262194:1920724591045]
:OUTPUT ACCEPT [205688113:60041773672]
:POSTROUTING ACCEPT [1646179191:1981317656496]
COMMIT
# Completed on Mon Mar 2 13:23:48 2015
# Generated by iptables-save v1.4.8 on Mon Mar 2 13:23:48 2015
*nat
:PREROUTING ACCEPT [142268687:12248077987]
:POSTROUTING ACCEPT [2397716:490027083]
:OUTPUT ACCEPT [4690731:705137262]
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Mon Mar 2 13:23:48 2015
# Generated by iptables-save v1.4.8 on Mon Mar 2 13:23:48 2015
*filter
:INPUT ACCEPT [310244:283396379]
:FORWARD ACCEPT [235389:312082112]
:OUTPUT ACCEPT [1:40]
:fail2ban-ProFTPD - [0:0]
:fail2ban-RoundCube - [0:0]
:fail2ban-SSH - [0:0]
:fail2ban-asterisk-tcp - [0:0]
:fail2ban-asterisk-udp - [0:0]
:fail2ban-dovecot - [0:0]
:fail2ban-exim - [0:0]
:fail2ban-lighttpd-auth - [0:0]
:fail2ban-mysql - [0:0]
:fail2ban-recvdiv - [0:0]
:fail2ban-sasl - [0:0]
:fail2ban-suhosin - [0:0]
:fail2ban-webmin - [0:0]
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-RoundCube
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-lighttpd-auth
-A INPUT -p tcp -m multiport --dports 110,995,143,993,587,465,4190 -j fail2ban-dovecot
-A INPUT -p tcp -m multiport --dports 5060,5061 -j fail2ban-asterisk-tcp
-A INPUT -p udp -m multiport --dports 5060,5061 -j fail2ban-asterisk-udp
-A INPUT -p tcp -m multiport --dports 10000 -j fail2ban-webmin
-A INPUT -p tcp -m tcp --dport 25 -j fail2ban-sasl
-A INPUT -p tcp -m multiport --dports 25,465,587 -j fail2ban-exim
-A INPUT -p tcp -m tcp --dport 22 -j fail2ban-SSH
-A INPUT -p tcp -j fail2ban-recvdiv
-A INPUT -p tcp -m tcp --dport 21 -j fail2ban-ProFTPD
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-suhosin
-A INPUT -p udp -m multiport --dports 5060,5061 -j fail2ban-asterisk-udp
```

```

-A INPUT -p tcp -m tcp --dport 3306 -j fail2ban-mysql
-A INPUT -p tcp -m tcp --dport 3306 -j fail2ban-mysql
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i eth1 -j ACCEPT
-A INPUT -p igmp -j ACCEPT
-A INPUT -p igmp -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i eth1 -j ACCEPT
-A INPUT -p igmp -j ACCEPT
-A FORWARD -i eth1 -o eth0 -j ACCEPT
-A FORWARD -i eth0 -o lan -j ACCEPT
-A FORWARD -i eth1 -o eth0 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -o eth0 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth1 -j ACCEPT
-A OUTPUT -o eth0 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth1 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A fail2ban-ProFTPD -j RETURN
-A fail2ban-RoundCube -j RETURN
-A fail2ban-SSH -j RETURN
-A fail2ban-asterisk-tcp -j RETURN
-A fail2ban-asterisk-udp -j RETURN
-A fail2ban-asterisk-udp -j RETURN
-A fail2ban-dovecot -j RETURN
-A fail2ban-exim -j RETURN
-A fail2ban-lighttpd-auth -j RETURN
-A fail2ban-mysql -j RETURN
-A fail2ban-mysql -j RETURN
-A fail2ban-recidive -j RETURN
-A fail2ban-sasl -j RETURN
-A fail2ban-suhosin -j RETURN
-A fail2ban-webmin -j RETURN
COMMIT
# Completed on Mon Mar 2 13:23:48 2015

```

## Rule set 9

# Generated by iptables-save v1.2.7a on Mon May 12 02:11:23 2003

\*filter

:INPUT ACCEPT [67:6686]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [47:4622]

-A FORWARD -p tcp -m tcp --sport 410:415 -m time --timestart 06:59 --timestop 23:59 --days Sun,Mon,Tue,Wed,Thu,Fri,Sat -j DROP

-A FORWARD -p tcp -m tcp --sport 6881:6889 -m time --timestart 06:59 --timestop 23:59 --days Sun,Mon,Tue,Wed,Thu,Fri,Sat -j DROP

-A FORWARD -p tcp -m tcp --sport 4661:4669 -m time --timestart 06:59 --timestop 23:59 --days Sun,Mon,Tue,Wed,Thu,Fri,Sat -j DROP

-A FORWARD -p tcp -m time --timestart 06:59 --timestop 23:59 --days Sun,Mon,Tue,Wed,Thu,Fri,Sat -m string --string X-Kazaa-User -j DROP

-A FORWARD -s 192.168.1.1 -p tcp --syn -m mac --mac 00:60:08:76:35:51 -m connlimit --connlimit-above 15 -j REJECT

-A FORWARD -s 192.168.1.2 -p tcp --syn -m mac --mac 00:50:BF:6A:D3:F9 -m connlimit --connlimit-above 15 -j REJECT

-A FORWARD -s 192.168.1.3 -p tcp --syn -m mac --mac 00:00:B4:3F:67:1C -m connlimit --connlimit-above 15 -j REJECT

-A FORWARD -s 192.168.1.4 -p tcp --syn -m mac --mac 00:30:4F:2E:70:72 -m connlimit --connlimit-above 15 -j REJECT

-A FORWARD -s 192.168.1.5 -p tcp --syn -m mac --mac 00:30:4F:2E:70:72 -m connlimit --connlimit-above 15 -j REJECT

-A FORWARD -s 192.168.1.6 -p tcp --syn -m mac --mac 00:00:E8:69:76:31 -m connlimit --connlimit-above 15 -j REJECT

-A FORWARD -s 192.168.1.1 -m mac --mac 00:60:08:76:35:51 -j ACCEPT

-A FORWARD -s 192.168.1.2 -m mac --mac 00:50:BF:6A:D3:F9 -j ACCEPT

-A FORWARD -s 192.168.1.3 -m mac --mac 00:00:B4:3F:67:1C -j ACCEPT

-A FORWARD -s 192.168.1.4 -m mac --mac 00:30:4F:2E:70:7E -j ACCEPT

-A FORWARD -s 192.168.1.5 -m mac --mac 00:30:4F:2E:70:7E -j ACCEPT

-A FORWARD -s 192.168.1.6 -m mac --mac 00:00:E8:69:76:31 -j ACCEPT

-A FORWARD -d 192.168.0.0/255.255.0.0 -j ACCEPT

-A FORWARD -d 172.16.0.0/255.255.0.0 -j ACCEPT

-A FORWARD -p icmp -j ACCEPT

COMMIT

# Completed on Mon May 12 02:11:23 2003

# Generated by iptables-save v1.2.7a on Mon May 12 02:11:23 2003

\*nat

:PREROUTING ACCEPT [16:851]

:POSTROUTING ACCEPT [0:0]

:OUTPUT ACCEPT [0:0]

-A PREROUTING -d 80.51.240.202 -p tcp -m tcp --dport 5060 -j DNAT --to-destination 192.168.1.1:5060

-A PREROUTING -d 80.51.240.202 -p udp -m udp --dport 5060 -j DNAT --to-destination 192.168.1.1:5060

-A PREROUTING -d 80.51.240.202 -p tcp -m tcp --dport 16384:16403 -j DNAT --to-destination 192.168.3.10:16384:16403

```

-A PREROUTING -d 80.51.240.202 -p tcp -m tcp --dport 16969 -j DNAT --to-destination 192.168.3.10:16969
-A PREROUTING -d 80.51.240.202 -p udp -m udp --dport 16969 -j DNAT --to-destination 192.168.3.10:16969

-A PREROUTING -s 172.16.0.0/255.255.0.0 -p udp -m udp --dport 80 -j REDIRECT --to-ports 3128
-A PREROUTING -s 172.16.0.0/255.255.0.0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3128
-A PREROUTING -s 192.168.0.0/255.255.0.0 -p udp -m udp --dport 80 -j REDIRECT --to-ports 3128
-A PREROUTING -s 192.168.0.0/255.255.0.0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3128
-A PREROUTING -d 192.168.0.0/255.255.0.0 -j ACCEPT
-A PREROUTING -d 172.16.0.0/255.255.0.0 -j ACCEPT
-A POSTROUTING -s 192.168.1.1 -p tcp -m tcp --sport 5060 -j SNAT --to-source 80.51.240.202:5060
-A POSTROUTING -s 192.168.1.1 -p udp -m udp --sport 5060 -j SNAT --to-source 80.51.240.202:5060
-A POSTROUTING -s 192.168.3.10 -p udp -m udp --sport 16384:16403 -j SNAT --to-source 80.51.240.202:16384-16403
-A POSTROUTING -s 192.168.3.10 -p tcp -m tcp --sport 16969 -j SNAT --to-source 80.51.240.202:16969
-A POSTROUTING -s 192.168.3.10 -p udp -m udp --sport 16969 -j SNAT --to-source 80.51.240.202:16969
-A POSTROUTING -s 172.16.0.0/255.255.0.0 -d ! 172.168.0.0/255.255.0.0 -j MASQUERADE
-A POSTROUTING -s 192.168.0.0/255.255.0.0 -d ! 192.168.0.0/255.255.0.0 -j MASQUERADE
COMMIT

```

```

# Completed on Mon May 12 02:11:23 2003
# Generated by iptables-save v1.2.7a on Mon May 12 02:11:23 2003
*mangle
:PREROUTING ACCEPT [1872:1089694]
:INPUT ACCEPT [67:6686]
:FORWARD ACCEPT [1803:1082829]
:OUTPUT ACCEPT [47:4622]
:POSTROUTING ACCEPT [1854:1088257]
COMMIT
# Completed on Mon May 12 02:11:23 2003

```



## Rule set 10

```
# Generated by iptables-save v1.2.7a on Sat Sep 27 02:06:00 2003
*nat
:PREROUTING ACCEPT [38:1868]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
# Completed on Sat Sep 27 02:06:00 2003
# Generated by iptables-save v1.2.7a on Sat Sep 27 02:06:00 2003
*mangle
:PREROUTING ACCEPT [353:47034]
:INPUT ACCEPT [353:47034]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [323:141426]
:POSTROUTING ACCEPT [323:141426]
COMMIT
# Completed on Sat Sep 27 02:06:00 2003
# Generated by iptables-save v1.2.7a on Sat Sep 27 02:06:00 2003
*filter
:FORWARD ACCEPT [0:0]
:INPUT DROP [0:0]
:OUTPUT ACCEPT [0:0]
# Accept traffic from internal interfaces
-A INPUT ! -i eth0 -j ACCEPT
# Accept traffic with the ACK flag set
-A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT
# Allow incoming data that is part of a connection we established
-A INPUT -m state --state ESTABLISHED -j ACCEPT
# Allow data that is related to existing connections
-A INPUT -m state --state RELATED -j ACCEPT
# Accept responses to DNS queries
-A INPUT -p udp -m udp --dport 1024:65535 --sport 53 -j ACCEPT
# Accept responses to our pings
-A INPUT -p icmp -m icmp --icmp-type echo-reply -j ACCEPT
# Accept notifications of unreachable hosts
-A INPUT -p icmp -m icmp --icmp-type destination-unreachable -j ACCEPT
# Accept notifications to reduce sending speed
-A INPUT -p icmp -m icmp --icmp-type source-quench -j ACCEPT
# Accept notifications of lost packets
-A INPUT -p icmp -m icmp --icmp-type time-exceeded -j ACCEPT
# Accept notifications of protocol problems
-A INPUT -p icmp -m icmp --icmp-type parameter-problem -j ACCEPT
# Allow connections to our SSH server
-A INPUT -p tcp -m tcp -m multiport -j ACCEPT --dports ssh,www,https,pop3,smtp,imap,imaps,pop3s,10000
# Allow connections to our IDENT server
-A INPUT -p tcp -m tcp --dport auth -j ACCEPT
# Respond to pings
-A INPUT -p icmp -m icmp --icmp-type echo-request -j ACCEPT
# Protect our NFS server
```

```
-A INPUT -p tcp -m tcp --dport 2049:2050 -j DROP
# Protect our X11 display server
-A INPUT -p tcp -m tcp --dport 6000:6063 -j DROP
# Protect our X font server
-A INPUT -p tcp -m tcp --dport 7000:7010 -j DROP
# Allow connections to unprivileged ports
-A INPUT -p tcp -m tcp --dport 1024:63353 -j ACCEPT
# Accept traceroutes
-A INPUT -p udp -m udp --dport 33434:33523 -j ACCEPT
COMMIT
# Completed on Sat Sep 27 02:06:00 2003
```

## Rule set 11

```
# Generated by iptables-save v1.4.10 on Tue Mar 12 10:00:28 2013
*nat
:PREROUTING ACCEPT [121:10079]
:INPUT ACCEPT [16:1597]
:OUTPUT ACCEPT [64:5071]
:POSTROUTING ACCEPT [12:1338]
:nat_reflection_in - [0:0]
:nat_reflection_out - [0:0]
:postrouting_rule - [0:0]
:prerouting_lan - [0:0]
:prerouting_rule - [0:0]
:prerouting_wan - [0:0]
:zone_lan_nat - [0:0]
:zone_lan_prerouting - [0:0]
:zone_wan_nat - [0:0]
:zone_wan_prerouting - [0:0]
-A PREROUTING -j prerouting_rule
-A PREROUTING -i br-lan -j zone_lan_prerouting
-A PREROUTING -i eth1 -j zone_wan_prerouting
-A POSTROUTING -j postrouting_rule
-A POSTROUTING -o br-lan -j zone_lan_nat
-A POSTROUTING -o eth1 -j zone_wan_nat
-A postrouting_rule -j nat_reflection_out
-A prerouting_rule -j nat_reflection_in
-A zone_lan_prerouting -j prerouting_lan
-A zone_wan_nat -j MASQUERADE
-A zone_wan_prerouting -j prerouting_wan
COMMIT
# Completed on Tue Mar 12 10:00:28 2013
# Generated by iptables-save v1.4.10 on Tue Mar 12 10:00:28 2013
*raw
:PREROUTING ACCEPT [540:48054]
:OUTPUT ACCEPT [151:15989]
:zone_lan_notrack - [0:0]
:zone_wan_notrack - [0:0]
-A PREROUTING -i br-lan -j zone_lan_notrack
-A PREROUTING -i eth1 -j zone_wan_notrack
COMMIT
# Completed on Tue Mar 12 10:00:28 2013
# Generated by iptables-save v1.4.10 on Tue Mar 12 10:00:28 2013
*mangle
:PREROUTING ACCEPT [540:48054]
:INPUT ACCEPT [440:40168]
:FORWARD ACCEPT [10:508]
:OUTPUT ACCEPT [151:15989]
:POSTROUTING ACCEPT [161:16497]
:zone_wan_MSSFIX - [0:0]
-A FORWARD -j zone_wan_MSSFIX
```

```

-A zone_wan_MSSFIX -o eth1 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
COMMIT
# Completed on Tue Mar 12 10:00:28 2013
# Generated by iptables-save v1.4.10 on Tue Mar 12 10:00:28 2013
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:forward - [0:0]
:forwarding_lan - [0:0]
:forwarding_rule - [0:0]
:forwarding_wan - [0:0]
:input - [0:0]
:input_lan - [0:0]
:input_rule - [0:0]
:input_wan - [0:0]
:nat_reflection_fwd - [0:0]
:output - [0:0]
:output_rule - [0:0]
:reject - [0:0]
:syn_flood - [0:0]
:zone_lan - [0:0]
:zone_lan_ACCEPT - [0:0]
:zone_lan_DROP - [0:0]
:zone_lan_REJECT - [0:0]
:zone_lan_forward - [0:0]
:zone_wan - [0:0]
:zone_wan_ACCEPT - [0:0]
:zone_wan_DROP - [0:0]
:zone_wan_REJECT - [0:0]
:zone_wan_forward - [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j syn_flood
-A INPUT -j input_rule
-A INPUT -j input
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -j forwarding_rule
-A FORWARD -j forward
-A FORWARD -j reject
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -j output_rule
-A OUTPUT -j output
-A forward -i br-lan -j zone_lan_forward
-A forward -i eth1 -j zone_wan_forward
-A forwarding_rule -j nat_reflection_fwd
-A input -i br-lan -j zone_lan
-A input -i eth1 -j zone_wan
-A output -j zone_lan_ACCEPT

```

```
-A output -j zone_wan_ACCEPT
-A reject -p tcp -j REJECT --reject-with tcp-reset
-A reject -j REJECT --reject-with icmp-port-unreachable
-A syn_flood -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m limit --limit 25/sec --limit-burst 50 -j
RETURN
-A syn_flood -j DROP
-A zone_lan -j input_lan
-A zone_lan -j zone_lan_ACCEPT
-A zone_lan_ACCEPT -o br-lan -j ACCEPT
-A zone_lan_ACCEPT -i br-lan -j ACCEPT
-A zone_lan_DROP -o br-lan -j DROP
-A zone_lan_DROP -i br-lan -j DROP
-A zone_lan_REJECT -o br-lan -j reject
-A zone_lan_REJECT -i br-lan -j reject
-A zone_lan_forward -j zone_wan_ACCEPT
-A zone_lan_forward -j forwarding_lan
-A zone_lan_forward -j zone_lan_REJECT
-A zone_wan -p udp -m udp --dport 68 -j ACCEPT
-A zone_wan -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A zone_wan -j input_wan
-A zone_wan -j zone_wan_REJECT
-A zone_wan_ACCEPT -o eth1 -j ACCEPT
-A zone_wan_ACCEPT -i eth1 -j ACCEPT
-A zone_wan_DROP -o eth1 -j DROP
-A zone_wan_DROP -i eth1 -j DROP
-A zone_wan_REJECT -o eth1 -j reject
-A zone_wan_REJECT -i eth1 -j reject
-A zone_wan_forward -j forwarding_wan
-A zone_wan_forward -j zone_wan_REJECT
COMMIT
# Completed on Tue Mar 12 10:00:28 2013
```

## Rule set 12

```
# Generated by iptables-save v1.4.8 on Fri Oct 28 16:08:03 2011
*mangle
:PREROUTING ACCEPT [68232:43165935]
:INPUT ACCEPT [1579:159656]
:FORWARD ACCEPT [66653:43006279]
:OUTPUT ACCEPT [1185:131888]
:POSTROUTING ACCEPT [67701:43129175]
-A FORWARD -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
COMMIT
# Completed on Fri Oct 28 16:08:03 2011
# Generated by iptables-save v1.4.8 on Fri Oct 28 16:08:03 2011
*nat
:PREROUTING ACCEPT [1579:110478]
:POSTROUTING ACCEPT [8:1480]
:OUTPUT ACCEPT [260:17655]
-A POSTROUTING -o eth1 -j MASQUERADE
COMMIT
# Completed on Fri Oct 28 16:08:03 2011
# Generated by iptables-save v1.4.8 on Fri Oct 28 16:08:03 2011
*filter
:INPUT ACCEPT [584:63835]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [1185:131888]
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -j ACCEPT
-A INPUT ! -i eth0 -p udp -m udp --dport 67 -j REJECT --reject-with icmp-port-unreachable
-A INPUT ! -i eth0 -p udp -m udp --dport 53 -j REJECT --reject-with icmp-port-unreachable
-A INPUT ! -i eth0 -p tcp -m tcp --dport 0:1023 -j DROP
-A INPUT ! -i eth0 -p udp -m udp --dport 0:1023 -j DROP
-A INPUT -m state --state INVALID -j LOG --log-prefix "INPUT DROP INVALID " --log-tcp-options
--log-ip-options
-A INPUT -m state --state INVALID -j DROP
-A FORWARD -d 192.168.0.0/16 -i eth0 -j DROP
-A FORWARD -s 192.168.0.0/16 -i eth0 -j ACCEPT
-A FORWARD -d 192.168.0.0/16 -i eth1 -j ACCEPT
-A FORWARD -m state --state INVALID -j LOG --log-prefix "FORWARD DROP INVALID " --log-tcp-
options --log-ip-options
-A FORWARD -m state --state INVALID -j DROP
-A FORWARD ! -i lo -j LOG --log-prefix "FORWARD DROP " --log-tcp-options --log-ip-options
-A OUTPUT -m state --state INVALID -j LOG --log-prefix "OUTPUT DROP INVALID " --log-tcp-
options --log-ip-options
COMMIT
# Completed on Fri Oct 28 16:08:03 2011
```