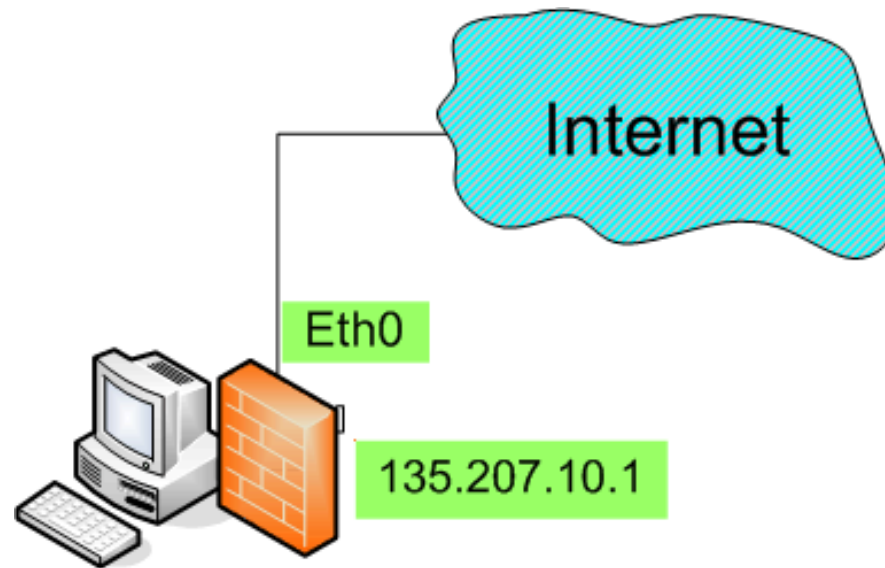


Single firewall with set of
sample filtering rules

A simple configuration



Sample rule 1

- Allow everything on loopback interface

```
<rule id="loop">  
  <action>permit</action>  
  <protocol>all</protocol>  
  <source>any</source>  
  <destination>any</destination>  
  <interface>  
    <via>lo0</via>  
  </interface>  
</rule>
```

Sample rule 1

- The Iptables translation

```
/sbin/iptables -A INPUT -i lo -s 0/0 -d 0/0 -p all -j ACCEPT  
/sbin/iptables -A OUTPUT -o lo -s 0/0 -d 0/0 -p all -j ACCEPT
```

- The Cisco Pix translation

```
access-list standard_loop permit ip any any  
access-group standard_loop in interface lo0  
access-group standard_loop out interface lo0
```

- The Ipfiler translation

```
pass quick on lo0 from any to any
```

- The Ipfirewall translation

```
ipfw add pass tcp/udp from any to any via lo0  
ipfw add pass icmp from any to any via lo0
```

Sample rule 2

- Allow tcp established connections

```
<rule id="est1">  
  <action>permit</action>  
  <protocol>tcp</protocol>  
  <source>any</source>  
  <destination>any</destination>  
  <options>  
    <state>established</state>  
  </options>  
</rule>
```

Sample rule 2

- The Iptables translation

```
/sbin/iptables -A INPUT -s 0/0 -d 0/0 -p tcp -j ACCEPT  
-m state --state established,related  
/sbin/iptables -A FORWARD -s 0/0 -d 0/0 -p tcp -j ACCEPT  
-m state --state established,related  
/sbin/iptables -A OUTPUT -s 0/0 -d 0/0 -p tcp -j ACCEPT  
-m state --state established,related
```

- The Cisco Pix translation

```
access-list standard_est1 permit tcp any any est  
access-group standard_est1 in interface all  
access-group standard_est1 out interface all
```

Sample rule 2

- The Ipfiler translation

```
pass quick tcp from any to any flags A/SA *
```

- * State established is translated with
“Ack tcpflag set, Syn tcp flag not set”

- The Ipfirewall translation

```
ipfw add pass tcp from any to any established
```

Sample rule 3

- Deny tcp connection requests from outside

```
<rule id="tcp_conn_in">  
  <action>deny</action>  
  <protocol>tcp</protocol>  
  <source>any</source>  
  <destination>135.207.10.208</destination>  
  <interface>  
    <direction>in</direction>  
    <via>eth0</via>  
  </interface>  
  <options>  
    <state>new</state>  
  </options>  
</rule>
```

Sample rule 3

- The Iptables translation

```
/sbin/iptables -A INPUT -i eth0 -s 0/0 -d 135.207.10.208 -p tcp  
-j DROP -m state --state new
```

(Just one rule, cause a specific direction is specified:
match new connections)

- The Cisco Pix translation

```
access-list standard_tcp_conn_in deny tcp any host 135.207.10.208 syn  
access-group standard_tcp_conn_in in interface eth0
```

(Match connections with SYN tcp flag set)

Sample rule 3

- The Ipfiter translation

```
block in quick on eth0 tcp from any to 135.207.10.208 flags S/SA *
```

- * Connection request is translated with
“Syn tcpflag set, Ack tcp flag not set”

- The Ipfirewall translation

```
ipfw add deny tcp from any to 135.207.10.208 setup in via eth0
```

(Match packets sent to ask for connection initiation)

Sample rule 4

- Prevent unroutable net 0.0.0.0/8 from entering the internet interface (eth0) and log attempts

```
<rule id="a">  
  <action>deny</action>  
  <protocol>all</protocol>  
  <source mask="255.0.0.0">0.0.0.0</source>  
  <destination>135.207.10.1</destination>  
  <interface>  
    <direction>in</direction>  
    <via>eth0</via>  
  </interface>  
  <log level="2"/>  
</rule>
```

Sample rule 4

- The Iptables translation

```
/sbin/iptables -A INPUT -i eth0 -s 0.0.0.0/255.0.0.0 -d 135.207.10.1  
-p all -j DROP  
/sbin/iptables -A INPUT -i eth0 -s 0.0.0.0/255.0.0.0 -d 135.207.10.1  
-p all -j LOG --log-level 2
```

- The Cisco Pix translation

```
access-list standard_a deny ip 0.0.0.0 255.0.0.0 host 135.207.10.1 log 2  
access-group standard_a in interface eth0
```

Sample rule 4

- The Ipfiter translation

```
block in log level auth.notice quick on eth0 from 0.0.0.0 mask  
255.0.0.0 to 135.207.10.1
```

- The Ipfirewall translation

```
ipfw add deny log tcp/udp from 0.0.0.0:255.0.0.0 to 135.207.10.1  
in via eth0  
ipfw add deny log icmp from 0.0.0.0:255.0.0.0 to 135.207.10.1  
in via eth0
```