Linux firewall

- Need of firewall
  - Single connection between network
  - Allows restricted traffic between networks
  - Denies un authorized users
Linux firewall

- Linux is an open source operating system and any firewall in Linux is open source.
- Low-cost
- World wide support
Difference between Hardware firewall and software Firewall
Linux Firewall

Implementing iptables
Installing iptables

most Linux installs “iptables”. “iptables” has become a standard option, especially Red Hat. There is a very good chance that iptables is already installed on your machine.

Opening a terminal window (making sure to be logged in as root).

Typing: # iptables
Installing iptables

If iptables is installed, you should get the following message:

iptables v1.2.8: no command specified
Try 'iptables -h' or 'iptables --help' for more information
Installing iptables

If this message does not appear, then follow the directions below to install iptables.

- Downloads are available at http://www.netfilter.org/downloads
Installing iptables

```
# tar -xvjf ./iptables-1.*.*.tar.bz2 -C /usr/src
```
where the asterisks represent the version number of the file you downloaded.

Change to the directory it created (typically iptables-1.*.*), by typing:
```
# cd /usr/src/iptables-1.*.*
```
Installing iptables

- `# /bin/sh -c make`
- To finish the install, type:
- `# /bin/sh -c make install`
Features of Iptables

• Packet filtering
• Connection tracking
• Network Address Translation
Packet filtering

The real firewall is packet filtering

Packet filtering occurs in layer “3 and 4” of Open System Interconnect (OSI) model ie network and transport layer.
Net filter chains

- Filter table
- NAT table
- Mangle table
Net filter Architecture

Table

Chain

Policy

Rule

Match Specification

Target
# NETFILTER TABLES AND CHAINS

<table>
<thead>
<tr>
<th>TABLES</th>
<th>FILTER</th>
<th>NAT</th>
<th>MANGLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Output</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Forward</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>PREROUTING</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>POSTROUTING</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>
Net filter packet flow

- **PREROUTING**: DNAT
- **Routing Decision**: Filter table
- **FORWARD**: Filter table
- **POSTROUTING**: SNAT
- **INPUT**: Filter table
- **OUTPUT**: Filter table
- **Local process**
Implementing Rules and policy in iptables

Policy

#iptables –P INPUT DROP/ACCEPT
#iptables –P OUTPUT DROP/ACCEPT
#iptables –P FORWARD DROP/ACCEPT
Implementing Rules

```
#iptables -A INPUT -i eth0 -p tcp (-s 192.168.0.222) -dport 22 --j drop
```

- `-A` to append the rule at the bottom of specified chain
- `-I` to insert the rule at the top of the specified chain
- `-i` income interface
- `-p` protocol
- `-s` incoming ip
- `--dport` destination port
- `--sport` source port
- `-o` outgoing interface
- `-d` destination ip
- `-j` jump
Chain INPUT (policy ACCEPT)

<table>
<thead>
<tr>
<th>target</th>
<th>protocol</th>
<th>port</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>DROP</td>
<td>tcp</td>
<td>22</td>
<td>192.168.0.222</td>
<td>anywhere</td>
</tr>
</tbody>
</table>

Deleting rules

# iptables –D INPUT <number>

#iptables –D INPUT –i eth0 –p tcp -dport 22 –j DROP
Network Address Translation

NAT

SNAT SOURCE NAT
DNAT DESTINATION NAT
• Each IP address is translated to distinct external IP 1:1

• All internal IP address is translated to a single external IP address. Internal IP may be Dynamic x:1

• Masquerading. Special case

X:X

Dynamic internal IP converted to dynamic outgoing IP
Destination NAT translates the destination IP address to different value

- Translation 1:X

Incoming request for one IP address (and port) are translated to many different IP address (and port). This can be used to implement some kind of load balancing

- Translation 1:1

Incoming requests for one IP address (and port) are translated to a single internal IP address and port
Simple implementation of NAT

- Internal network connects to the internet with a dynamic public IP address

```
#iptables –t nat –A POSTROUTING –i eth0 –o ppp0 –j MASQUERADE
```
Redirection: redirection is a special case of the the above point.

Redirection translates incoming requests for one IP Address and port to a different local port. The packet is resubmitted to the firewall after translation.
PROXY
(Application Firewall)

PROXY or application Firewall is implemented at the application level of OSI model.
Screening Router

INTERNET

Screening Router

INTERNAL NETWORK
• A simple combined router and packet filter is called a screening Router
• A screening router is capable of implementing simple rule and simple NAT
• A simple screening router is thus able to restrict the packets transferred between the internet and the internal network.
• Usually commercially available routers implement these simple features
DMZ (Demilitarised Zone)
• Whenever an internal network needs to access to the internet it connects to the application level gateways in DMZ which then forward the request to the internet.
• The response reaches the application level gateways in DMZ which then forwards the request to the requesting client
Reverse Proxy

INTERNET

Screening router

PROXY

WEB SERVER
• Reverse proxy is not a firewall.
• Main feature of reverse proxy are
  • Protection against DoS attack tools
    – Since the proxy unpacks all IP packets it will drop invalid packets
  
  **Acceleration:**
  The proxy maintains cache so that it can give reply to the request from the cache also
  Load balancing is also done by the reverse proxy