3.7 Linux Firewalls

Linux has firewall capabilities built into the operating system. This has been a part of the Linux operating system for many years, with occasional improvements in the technology.

3.7.1 Iptables

The first widely used Linux firewall was called ipchains. It was essentially a chain of rules for filtering traffic. It was first introduced in version 2.2 of the Linux kernel and superseded the previous ipfwadm (which was not widely used). The more modern iptables replaced ipchains, being the primary firewall for Linux. The iptables service was first introduced in Linux kernel 2.4.

On most Linux systems, iptables is installed as /usr/sbin/iptables. However, if it is not included in your particular Linux installation, you can add it later.

An iptables firewall is made up of three different kinds of objects: tables, chains, and rules. Basically, the tables contain chains of rules. In other words, iptables is an expansion of the concept of ipchains. Each chain has a series of rules that define how to filter packets. There are actually three tables. Each table has certain standard rule chains in it. You can, of course, add your own custom rules. The three tables and their standard chains are as follow:

- **Packet filtering:** This table is the essential part of the firewall. It is a packet filtering firewall and it contains three standard chains: INPUT, OUTPUT, and Forward. The INPUT chain processes incoming packets, and the OUTPUT chain processes traffic sent out from the machine. If the firewall system is also acting as a router, only the FORWARD chain applies to routed packets.
- **Network address translation:** This table is used for performing network address translation on outbound traffic that initiates a new connection. This is used only if your machine serves as a gateway or proxy server.
- **Packet alteration:** This table is used only for specialized packet alteration. It is often called the mangle table because it alters, or mangles, packets. It contains two standard chains. This table might not even be needed for many standard firewalls.

3.7.2 Iptables Configuration

Iptables require certain configuration. You can do it through the GUI (KDE, GNOME, etc.) but the shell commands are common to most distributions. Let’s take a look at some common basic configuration.

To cause iptables to function as a basic packet filtering firewall, you need these commands:

- iptables -F
- iptables -N block
- iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT

Obviously, this is the most basic and essential iptables configuration. However, here are some others.

To list the current iptables rules use:

- iptables –L

To allow communication on a specific port, SSH port 22 and HTTP port 80 for example use:

- iptables –A INPUT –p tcp –dport ssh –j ACCEPT
- iptables –A INPUT –p tcp –dport 80 –j ACCEPT

Also there are several flags that can be passed to the iptables command. Below are listed the most common flags and their purpose. Several other flags exist but are not listed.

A: Append this rule to a rule chain

-L: List the current filter rules

-p: The connection protocol used

--dport: The destination port required for the rule. A single port can be given or a range.

-i: Only match if the packet is coming in on the specified interface.

-v: Verbose output

-s, --source: address source specification

-d, --destination: address destination specification