Chapter 1

Configuring a Firewall

1.1 Understanding Firewall Configuration

The Linux kernel has a firewalling functionality called **netfilter**. In previous versions of RHEL, it used to be managed with **iptables**. However, now the default management interface is **firewalld** (even though iptables can still be used).

The design purpose of firewalld was to make firewall configuration easy, and this has been achieved with interfaces. Each of these interfaces is assigned a zone. There can be a private zone for private messages, where nothing is filtered, or a public zone for a server directly connected to the internet.

Next, services have to be connected to zones. Many services are already available by default and those that aren't are easy to configure and connect to the appropriate zone. Once these services are configured and are available, there are only a couple of command line utilities that we can use to setup our firewall.

1.2 Using Firewalld

To configure the Linux kernel firewall on RHEL 7, we use **firewalld**. While using iptables is still a valid option, it isn't the recommended way since many utilities write directly to firewalld. To ensure that everything is compatible, we should only use firewalld. To ensure that the firewalld service is running, we use:

```
# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
 ↪  enabled)
Active: active (running) since Fri 2017-12-22 10:29:51 IST; 18s ago
Docs: man:firewalld(1)
Main PID: 890 (firewalld)
CGroup: /system.slice/firewalld.service
└─890 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Dec 22 10:29:49 vmPrime.somuVMnet.com systemd[1]: Starting firewalld - dynami...
Dec 22 10:29:51 vmPrime.somuVMnet.com systemd[1]: Started firewalld - dynamic...
```

There are a couple of ways to add rules to the firewall. First there is the **firewall-cmd**, which is a command line utility to manage the firewall, and then there's **firewall-config**, a GUI utility which allows us to click to add services.

The basic configuration of a firewall in Linux is done with zones and services. To list all available zones and services we use:

```
# firewall-cmd --get-zones
block dmz drop external home internal public trusted work
# firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bitcoin bitcoin-rpc
 ↪  bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb
 ↪  dhcp dhcpv6 dhcpv6-client dns docker-registry dropbox-lansync elasticsearch
 ↪  freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client
 ↪  ganglia-master high-availability http https imap imaps ipp ipp-client ipsec
 ↪  iscsi-target kadmin kerberos kibana klogin kpasswd kshell ldap ldaps libvirt
 ↪  libvirt-tls managesieve mdns mosh mountd ms-wbt mssql mysql nfs nrpe ntp openvpn
 ↪  ovirt-imageio ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis
 ↪  pop3 pop3s postgresql privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius
 ↪  rpc-bind rsh rsyncd samba samba-client sane sip sips smtp smtp-submission smtps snmp
 ↪  snmptrap spideroak-lansync squid ssh synergy syslog syslog-tls telnet tftp
 ↪  tftp-client tinc tor-socks transmission-client vdsm vnc-server wbem-https xmpp-bosh
 ↪  xmpp-client xmpp-local xmpp-server
```

1.2.1 Default Zone

Now, if we need to find the default zone, the command is:

```
# firewall-cmd --get-default-zone
public
```

To set the default zone, the command is:

```
# firewall-cmd --set-default-zone home
success
# firewall-cmd --get-default-zone
home
```

1.2.2 Services

As far as the firewall is concerned, a service is a name assigned to a **protocol** and a **port**. And administrator can create his own services in `/etc/firewalld/services` directory. The default system services are stored in `/usr/lib/firewalld/services`. A typical service, such as the *high-availability.xml*, looks like:

```
<?xml version="1.0" encoding="utf-8"?>
<service>
<short>Red Hat High Availability</short>
<description>This allows you to use the Red Hat High Availability (previously named Red
 ↪  Hat Cluster Suite). Ports are opened for corosync, pcsd, pacemaker_remote, dlm and
 ↪  corosync-qnetd.</description>
<port protocol="tcp" port="2224"/>
<port protocol="tcp" port="3121"/>
<port protocol="tcp" port="5403"/>
```

```
<port protocol="udp" port="5404"/>
<port protocol="udp" port="5405"/>
<port protocol="tcp" port="21064"/>
</service>
```

This services binds multiple ports that we want open (for varied uses) to the TCP or UDP protocol. Another such complicated service is the *samba.xml* service, which is also a collection of ports:

```
<?xml version="1.0" encoding="utf-8"?>
<service>
<short>Samba</short>
<description>This option allows you to access and participate in Windows file and printer sharing networks. You need the samba package installed for this option to be useful.</description>
<port protocol="udp" port="137"/>
<port protocol="udp" port="138"/>
<port protocol="tcp" port="139"/>
<port protocol="tcp" port="445"/>
<module name="nf_conntrack_netbios_ns"/>
</service>
```

The last line, `<module name="nf_conntrack_netbios_ns"/>` states that for this service, a specific kernel module has to be loaded. Thus, if we want to create our own service in `/etc/firewalld/services` directory, it just needs to be contained within a valid XML file with the service tag, containing a short name, a description and port definition(s).

1.2.3 Adding services to zones

To add a service, we use the command:

```
# firewall-cmd --zone=home --add-service=high-availability
success
```

To get the configuration of the current zone, we use the command:

```
# firewall-cmd --list-all
home (active)
target: default
icmp-block-inversion: no
interfaces: ens33
sources:
services: ssh mdns samba-client dhcpv6-client high-availability
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

To list all the services in a non-default zone, we use:

```
# firewall-cmd --zone=public --list-all
public
```

```
target: default
icmp-block-inversion: no
interfaces:
sources:
services: ssh dhcpv6-client
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

Note that all services added in this manner are non-persistent and wiped with every reboot. To make them permanent, we just have to add the `--permanent` flag to each command:

```
# firewall-cmd --permanent --zone=home --add-service=high-availability
success
```

1.2.4 firewall-config

The firewall-config utility provides tabs of zones with a list of services in each, and the admin can check the services that should be available in each zone. The configuration can be set to either *runtime* or *permanent*.