Firewalld:

In Linux kernel there is (net filter) that is firewall functionality to manage it we use firewalld and it is the default management interface.

- To work with firewalld there is interfaces and each interface is mapped to zone (private, public, home, DMZ)
- We need to connect services to zones

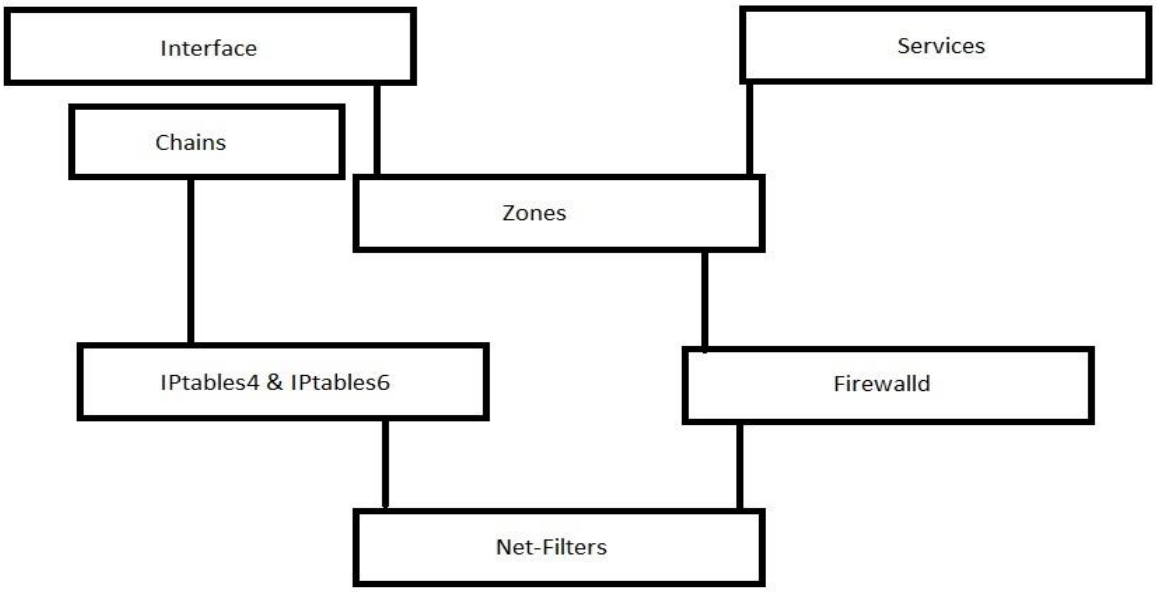
To manage our firewalld setting we use two tools: firewall-config (GUI) and firewall-cmd (CMD)

Using firewalld:

Package: firewalld

Firewall-zones:

Firewalls can be used to separate networks into different zones based on the level of trust the user has. Each zone connected to a physical NIC from the Network Manager Service.



Drop: Any incoming network packets are dropped, there is no reply (No ICMP Notification). Only outgoing network connections are possible.

Block: Any incoming network connections are rejected with an icmp-host-prohibited message for IPv4 and icmp6-adm-prohibited for IPv6. Only outgoing network connections are possible.

Public: It is the default zone, for use in public areas. You do not trust the other computers on the network to not harm your computer. Only selected incoming connections are accepted.

External: For use on external networks with **masquerading** enabled especially for **routers.** You do not trust the other computers on the network to not harm your computer. Only selected incoming connections are accepted.

DMZ: For computers in your demilitarized zone that are publicly-accessible with limited access to your internal network. Only selected incoming connections are accepted. decided to place on the devices and traffic within that network.

Internal: For use on internal networks. You mostly trust the other computers on the networks to not harm your computer. Only selected incoming connections are accepted.

Trusted: All network connections are accepted.

[root@server ~]#firewall-config (gui)
[root@server ~]#firewall-cmd (cli)
[root@server ~]#systemctl status firewalld ==> checking that the service is running
[root@server ~]#systemctl start firewalld ==> start firewall
[root@server ~]#systemctl enable firewalld ==> enable it permeant
[root@srv1 ~]# man firewall-cmd
[root@server ~]#firewall-cmd --get-zones ==> this is all the zones but we want to get the default zone
[root@server ~]#firewall-cmd –get-default-zone ==> to get the default firewall with the server services
[root@srv1 ~]# firewall-cmd --get-zone-of-interface=ens33 ==> to know the physical interface connected to which zone.

Note: the zone can have multiple interfaces because the zone is logical, but the interface is physical.

[root@server ~]#firewall-cmd --get-services ==> to get the actual services that the server is using either allowed or denied
[root@server ~]# firewall-cmd --get-icmptypes ==> ICMP protocol options
[root@server ~]#firewall-cmd set-default-zone (name of default zone) ==> to set the default zone.
[root@srv1 ~]# firewall-cmd --add-interface=ens37 ==> add interface
[root@srv1 ~]# firewall-cmd --zone=internal --add-interface=ens37 –permanent ==> add interface to zone
[root@srv1 ~]# firewall-cmd --zone=internal --list-all

Service definition is a protocol with port number
[root@server services]#cd /etc/firewalld/services ==> here is service folder where we can add service
[root@server service]#cd /usr/lib/firewalld/services/ ==> default system services in xml files, it is very easy it contains description and protocol tcp with port number and kernel modules loaded.

Note: we cannot change the configuration in this directory, we have to get copy of the service and change it in the location /etc/firewalld/services/ directory.

[root@server service]#vim high-avilability
<?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="5405-5412"/>
  <port protocol="tcp" port="9929"/>
  <port protocol="udp" port="9929"/>
  <port protocol="tcp" port="21064"/>
</service>

[root@server ~]# firewall-cmd --zone=home --add-service=http ==> to add service to home zone

[root@srv1 ~]# firewall-cmd --remove-service=ssh --permanent ==> removing service
[root@server ~]# firewall-cmd --list-all ==> to list services in the home zone with the active zone and other details
[root@server ~]# firewall-cmd --list-all-zones ==> list the zones with services, target, options
[root@server ~]# firewall-cmd --list-services ==> list service allowed in this zone

Note: if we did not specify the zone it will take the default zone.

Note: everything that done with firewalld is not permanent, to make it permanent we must do the following:

[root@server ~]# firewall-cmd --permanent --zone=home --add-service=http ==> to let the service permanent
[root@srv1 ~]# firewall-cmd --add-port=123/udp --permanent ==> add specific port
[root@srv1 ~]# firewall-cmd --add-source=192.168.11.0/24 --permanent ==> add source network.
[root@srv1 ~]# firewall-cmd --add-source=192.168.10.128 --permanent ==> add source ip address.
[root@srv1 ~]# firewall-cmd --add-source-port=22/tcp –permanent ==> add source port.
[root@srv1 ~]# firewall-cmd --add-icmp-block=echo-request –permanent ==> block any ping traffic.

```
[root@srv1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources: 192.168.11.0/24 192.168.10.128
  services: dhcpv6-client ssh
  ports: 123/udp
  protocols:
  masquerade: no
  forward-ports:
  source-ports: 22/tcp
  icmp-blocks: echo-request
  rich rules:
```

[root@server ~]# firewall-cmd --reload ==> to reread the firewall rules again, this task is very important when we change firewall settings.
[root@server ~]# firewall-cmd --state ==> to show current state of the firewall

IP Forwarding and Masquerade:
With Masquerade, the system will forward packets that are not directly addressed to itself to the indented recipient, while changing the source address of the packet that go through to its own public address.

Note: Masquerade or NAT is used with ipv4 address only.

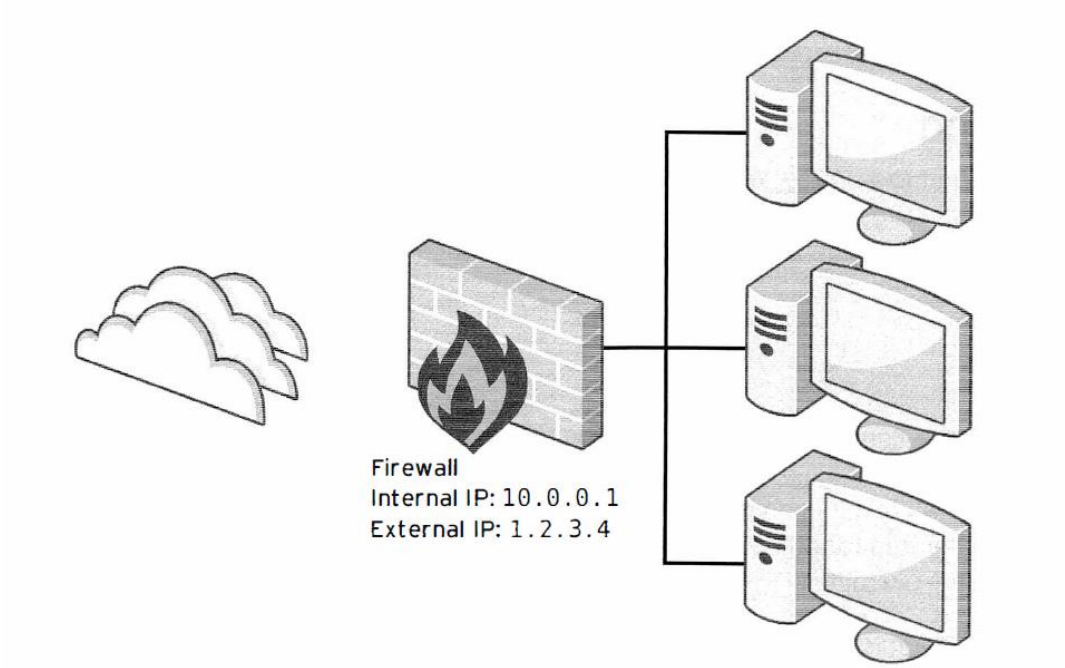


Figure 4.1: A sample network layout for NAT

[root@srv1 ~]# firewall-cmd --zone=external --add-masquerade
[root@srv1 ~]# firewall-cmd --add-forward-port=port=22:proto=tcp:toport=2222:proto=tcp --permanent
[root@srv1 ~]# firewall-cmd –reload
[root@srv1 ~]# firewall-cmd --remove-forward-port=port=22:proto=tcp:toport=2222:proto=tcp –permanent
[root@srv1 ~]# firewall-cmd –reload

Firewall-Rich- Rules:

It is used to allow/deny specific host/network to/from accessing specific service on a server. The basics firewall is very limited, so we need more advanced firewall configuration via rich rules:
-Combination of source ip or destination ip with services or ports
-Combination of source ipv6 or destination ipv6 with service or ports
-logging some traffic either allowed or denied for a period with a prefix

The basic syntax of a rich rule can be expressed by the following block:

```
rule
  [source]
  [destination]
  service|port|protocol|icmp-block|masquerade|forward-port
  [log]
  [audit]
  [accept|reject|drop]
```

Firewall processing with the rich rules:

Rule ordering

Once multiple rules have been added to a zone (or the firewall in general), the ordering of rules can have a big effect on how the firewall behaves.

The basic ordering of rules inside a zone is the same for all zones:

1. Any port forwarding and masquerading rules set for that zone.
2. Any logging rules set for that zone.
3. Any allow rules set for that zone.
4. Any deny rules set for that zone.

In all cases, the first match will win. If a packet has not been matched by any rule in a zone, it will typically be denied, but zones might have a different default; for example, the **trusted** zone will **accept** any unmatched packet. Also, after matching a logging rule, a packet will continue to be processed as normal.

Allow a Network to access ssh service:
[root@srv1 ~]# firewall-cmd --add-rich-rule='rule family=ipv4 source address=192.168.10.0/24 service name=ssh accept' --permanent
[root@srv1 ~]# firewall-cmd --reload
[root@srv1 ~]# firewall-cmd --list-all

Reject some traffic from a certain network
[root@srv1 ~]# firewall-cmd --zone=public --add-rich-rule='rule family=ipv4 source address=192.168.11.0/24 reject' --permanent
[root@srv1 ~]# firewall-cmd --reload
[root@srv1 ~]# firewall-cmd --list-all

Drop Service Traffic from any ip:
[root@srv1 ~]# firewall-cmd --zone=public --add-rich-rule='rule protocol value=esp drop' --permanent
[root@srv1 ~]# firewall-cmd --reload
[root@srv1 ~]# firewall-cmd --list-all

Accept range of ports from a source Network:
[root@srv1 ~]# firewall-cmd --zone=public --add-rich-rule='rule family=ipv4 source address=192.168.10.0/24 port port=7900-7905 protocol=tcp accept' --permanent
[root@srv1 ~]# firewall-cmd --reload
[root@srv1 ~]# firewall-cmd --list-all

Allow access to ftp server from only ip 192.168.10.131
[root@srv1 ~]# firewall-cmd --zone=public --add-rich-rule='rule family='ipv4' source address='192.168.10.131' port port='21' protocol='tcp' accept’ --permanent
[root@srv1 ~]# firewall-cmd –reload

Removing rule:
[root@srv1 ~]# firewall-cmd --zone=public --remove-rich-rule='rule family=ipv4 source address=192.168.11.0/24 reject' --permanent
[root@srv1 ~]# firewall-cmd --reload