Firewall

1. Network level firewall :
   Firewalls employed at the network level use either dedicated hardware or sophisticated software appliances to form a shield around the network.

2. Server level firewall : referred to as host-based firewalls and they run in a computer operating system to monitor and manage traffic in and out. Firewalls defend a network or an individual server from undesired traffic.

   Based on predefined rules, a firewall intercepts each inbound and outbound data packet, inspects its header, and decides whether to allow the packet to pass through.

Basic Networking concepts
A data packet is formed by the procedure called encapsulation

Header message attached to the packet called : payload

Payload has info about source ip , destination ip, type of data, port number,

Ports are defined in the /etc/services file for common network services that are standardized across all network operating systems, including RHEL

The host-based firewall solution employed in RHEL uses a kernel module called netfilter together with a filtering and packet classification framework called nftables for policing the traffic movement.

firewalld

Firewalld is the hostbased firewall available on RHEL 8 version

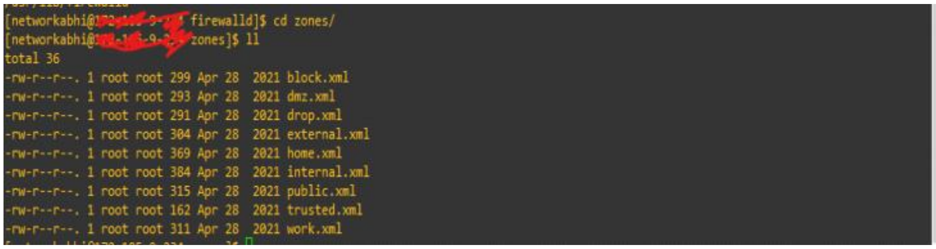
The firewalld service lets you perform management operations at the command line using the firewall-cmd command, graphically using the web console, or manually by editing rules files. firewalld stores the default rules in files located in the /usr/lib/firewalld directory, and those that contain custom rules in the /etc/firewalld directory.

Firewalld zones

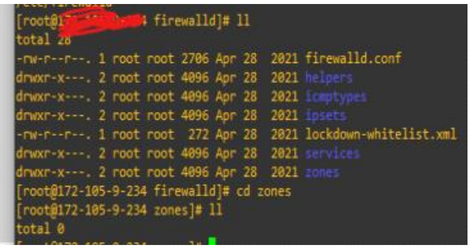
Zones define policies based on the trust level of network connections and source IP addresses. A network connection can be part of only one zone at a time; however, a zone can have multiple network connections assigned to it. Zone configuration may include services, ports, and protocols that may be open or closed. It may also include rules for advanced configuration items such as masquerading, port forwarding, NATting, ICMP filters, and rich language. Rules for each zone are defined and manipulated independent of other zones.
firewalld inspects each incoming packet to determine the source IP address and applies the rules of the zone that has a match for the address. In the event no zone configuration matches the address, it associates the packet with the zone that has the network connection defined, and applies the rules of that zone. If neither works, firewalld associates the packet with the default zone, and enforces the rules of the default zone on the packet

2 locations where the zone rules stored in xml format

1. System defined rules : /usr/lib/firewalld/zones directory
2. User defined rules : /etc/firewalld/zones



```
[networkabhi@[redacted] firewalld]$ cd zones/
[networkabhi@[redacted] zones]$ ll
total 36
-rw-r--r--. 1 root root 299 Apr 28  2021 block.xml
-rw-r--r--. 1 root root 293 Apr 28  2021 dmz.xml
-rw-r--r--. 1 root root 291 Apr 28  2021 drop.xml
-rw-r--r--. 1 root root 304 Apr 28  2021 external.xml
-rw-r--r--. 1 root root 369 Apr 28  2021 home.xml
-rw-r--r--. 1 root root 384 Apr 28  2021 internal.xml
-rw-r--r--. 1 root root 315 Apr 28  2021 public.xml
-rw-r--r--. 1 root root 162 Apr 28  2021 trusted.xml
-rw-r--r--. 1 root root 311 Apr 28  2021 work.xml
```



```
[root@[redacted] firewalld]# ll
total 28
-rw-r--r--. 1 root root 2706 Apr 28  2021 firewalld.conf
drwxr-x---. 2 root root 4096 Apr 28  2021 helpers
drwxr-x---. 2 root root 4096 Apr 28  2021 icmptypes
drwxr-x---. 2 root root 4096 Apr 28  2021 ipsets
-rw-r--r--. 1 root root  272 Apr 28  2021 lockdown-whitelist.xml
drwxr-x---. 2 root root 4096 Apr 28  2021 services
drwxr-x---. 2 root root 4096 Apr 28  2021 zones
[root@172-105-9-234 firewalld]# cd zones
[root@172-105-9-234 zones]# ll
total 0
```

Firewall Management

1. Firewall-cmd - command line to perform the activities
2. Graphical interface - web interface -
3. Use of the zones and templates and edit them as desired

firewall-cmd Command

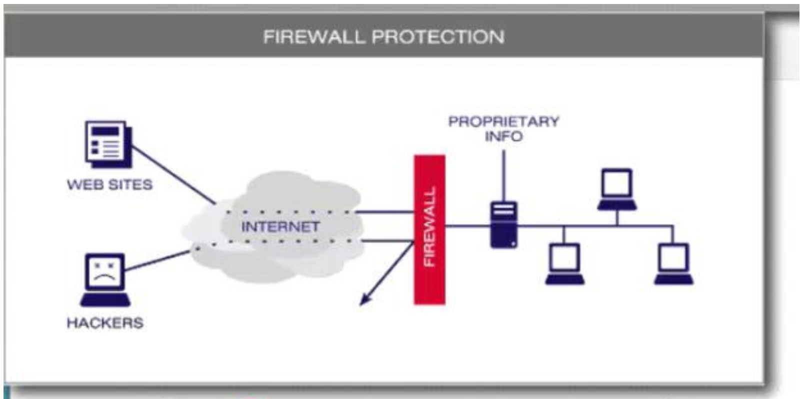
add or remove rules from the runtime configuration, or save any modifications to service configuration for persistence. It supports numerous options for the management of zones, services, ports, connections, and so on;

Checking if it's running

Firewall-cmd --state

Or systemctl status firewalld

Default -Firewall management - Firewalld



Zones/ predefined zones

Drop zones: all incoming packets/ connections are dropped

Block zone : drop but a ICMP reply

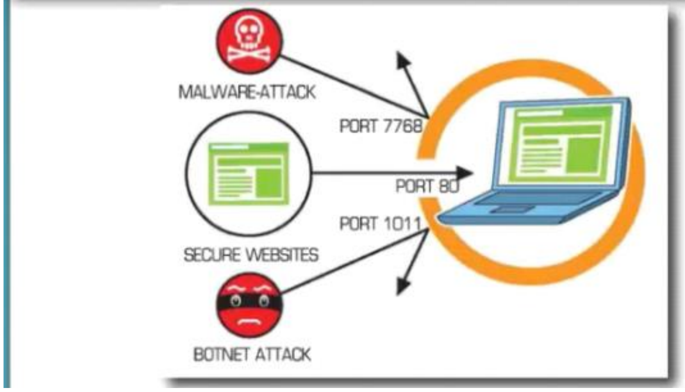
Public : untrusted network but allow some selected connections on

External zone: NAT

Internal :

Computers are trusted

DMZ :
Only certain incoming connections are allowed



Work

Home

Tursted

You can add , remove - ports , services and manage zones