Firewalls

Information is transmited in packets across networks, each one contains:

1. **Header and footer**

..Contain information about destination and source addresses, what kind of packet it is and which protocol it obeys, various flags, which packet number this is in a stream, all sorts of metadata about transmissions.

1. **Payload:** the actual data

* What are firewall are why are they are necessary
  + First generation  **packet filtering**
  + Second gen. **connection state.**  next gen.  **stateful filters** which also examine connection state of the packets
  + Third generation **Application layer Firewalls.** And are aware of the kind of connection state of the packet. New connection, part of already existing one, or part of none.
* Tolls available both for the command line and using graphical interfaces
  + Low –level tools from command line, combined with editing files in /etc subdirectory tree:
    - Iptables
    - Firewall-cmd
    - Ufw
  + Graphical interfaces:
    - System-config-firewall
    - Firewall-config
    - Gufw
    - yast
* Firewalld and firewall-cmd
  + **Firewalld ( Dynamic Firewall Manager )** is a service which needs to running to use and configure the firewall.

Utilizes network/firewall zones, which have defined levels of thrust for network interfaces or connections.

Configuration files are kept in  **/etc/firewalld (** this file contect overwrites the other directory) and **/usr/firewalld.**

**T**he actual tool is **firewall-cmd**

$firewall-cmd --help

**Enable/disable start/stop firewalld service**

$sudo systemctl [enable/disable] firewalld

$sudo systemctl [start/stop] firewalld

**Show current status firewalld**

$sudo systemctl status firewalld

$sudo firewall-cmd --state

to turn on **ip forwarding :**

$sudo systemctl net.ipv4.ip\_forward=1

$echo 1 > /proc/sys/net/ipv4/ip\_foward ( need to be runned as root)

To make it persistent:

Add the following line to **/etc/sysctl.conf:**

Net.ipv4.ip\_forward=1

And then reboot or type:

$sudo sysctl –p (to read the new setting without rebooting

* Work with **zones, sources, services**  and **ports**
  + **Zone management:**

**Get default zone:**

$ sudo firewall-cmd --get-default-zone

**list of zones currently being used:**

$sudo firewall-cmd - -get-active-zones

List all available zones:

$sudo firewall-cmd - -get-zones

Change the default zone to **trusted:**

$sudo firewall-cmd - -set-deault-zone=trusted

Assign an **interface**  temporarily to a particular zone:

$ sudo firewall-cmd - -zone=internal - -change-interface=eno1

**Asssing an interface** to a particular zone **permantently:**

$sudo firewall-cmd - -permanent- -zone=internal - -change-interface=eno1

Which creates the **file /etc/firewalld/zones/interal.xml**.

To get the details of a particular zone

$sudo firewall-cmd - -zone=public - -list-all

**Source Management.**

**A packet is associated with a zone if:**

* + It comes from a source address already bound to the zone; or if not.
  + It comes form an interface bound to the zone

Any packet not fitting the above criteria is assigned to the  **default zone (** usually public**).**

To assigned a source to a zone ( permanently ):

$ sudo firewall-cmd - -permanent **- -zone=trusted** - -add-source=192.168.1.0/24

anyone whit ip address of 192.168.1.x will be added to the **trusted zone to remove zone:** change to - -remove-source or Change **zone** by using **- - change source**

To list sources bound to a zone:

$sudo firewall-cmd - -permanent - -zone=trusted - - list-sources

**Service and port Management**

To see all services available:

$ sudo firewall-cmd - -get-services

Or to see currently accessible in a particular zone:

$sudo firewall-cmd - -list-services - -zone=public

To add a service to a zone:

$sudo firewall-cmd - -permanent - -zone=home - -add-service=dhcp

$ sudo firewall-cmd --reload …. This is needed to make changes effective.

Note: It is also possible to add services by editing the file **/etc/firewalld/services**

**Port management is very similar to service management:**

$ sudo firewall-cmd - -zone=home - -add-port=21/tcp

$sudo firewall-cmd - -zone=home - -list-ports

By cheking /etc/services we can ascertain that port 21 corresponds to ftp:

$ grep “21/tcp” /etc/services