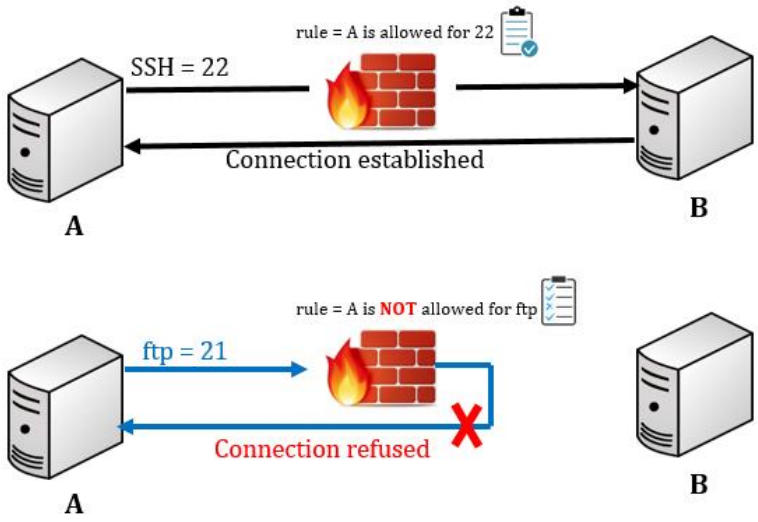
Firewall (iptables)

What is Firewall

- A wall that prevents the spread of fire
- When data moves in and out of a server its packet information is tested against the firewall rules to see if it should be allowed or not
- In simple words, a firewall is like a watchman, a bouncer, or a shield that has a set of rules given and based on that rule they decide who can enter and leave

There are 2 type of firewalls in IT

- Software = Runs on operating system
- Hardware = A dedicated appliance with firewall software



There are 2 tools to manage firewall in most of the Linux distributions

- iptables = For older Linux versions but still widely used
- firewalld = For newer versions like 7 and up

You can run one or the other

- iptables or firewalld but you cannot run both at the same time

Before working with iptables make sure firewalld is not running and disable it

- **service OR systemctl stop firewalld** = To stop the service
- **systemctl disable firewalld** = To prevent from starting at boot time
- **systemctl mask firewalld** = To prevent it from running by other programs

Before running iptables make sure its package is installed

- **rpm –qa | grep iptables-services**
- **yum install iptables-services** - If not installed then

Start the service

- **systemctl start iptables**
- **systemctl enable iptables**

To check the iptables rules

- **iptables –L**

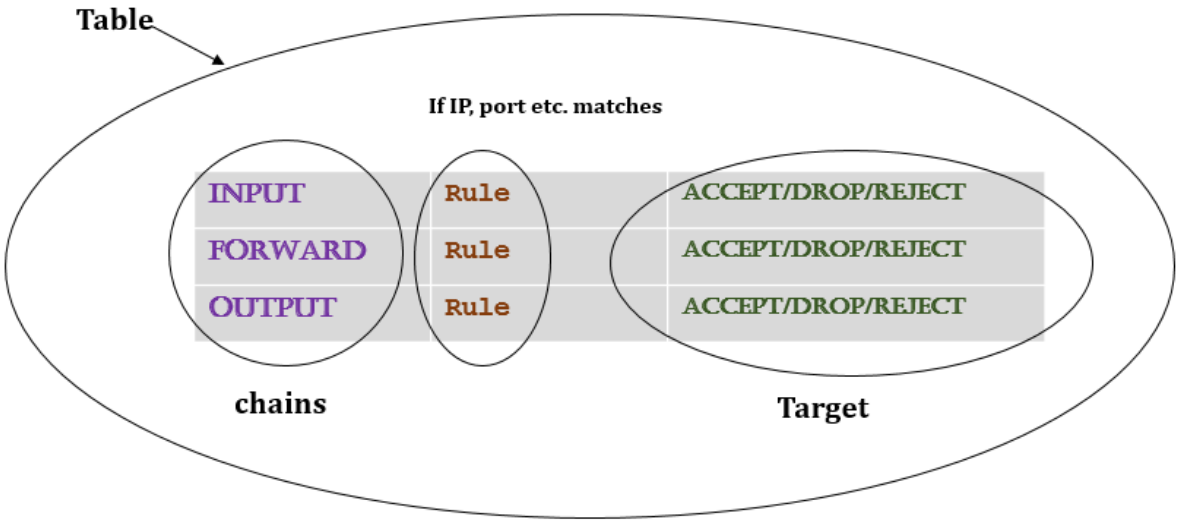
To flush iptables.

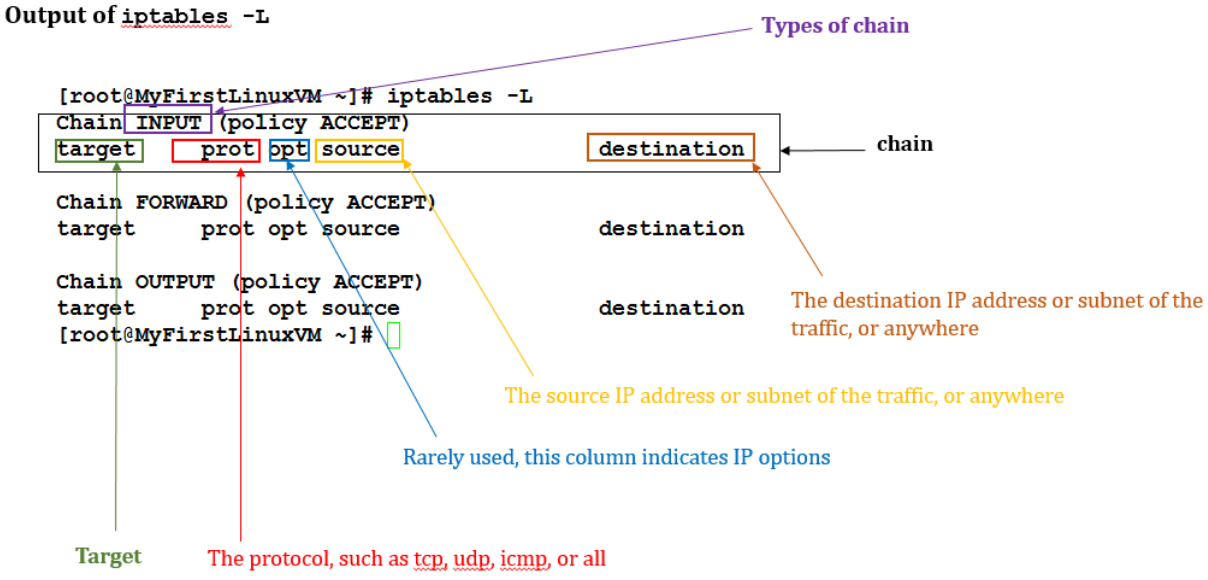
- **iptables –F**

The function of iptables tool is packet filtering

- The packet filtering mechanism is organized into three different kinds of structures: **tables, chains** and **targets**
    1. **tables** = table is something that allows you to process packets in specific ways. There are 4 different types of tables, **filter**, mangle, nat and raw
    2. **chains** = The chains are attached to tables, These chains allow you to inspect traffic at various points. There are 3 main chains used in iptables
        - **INPUT =** incoming traffic
        - **FORWARD =** going to a router, from one device to another
        - **OUTPUT =** outgoing traffic
            - chains allow you to filter traffic by adding rules to them
            - Rule = if traffic is coming from **192.168.1.35** then go to defined target

3. **targets** = target decides the fate of a packet, such as allowing or rejecting it. There are 3 different type of targets
    - **ACCEPT =** connection accepted
    - **REJECT =** Send reject response
    - **DROP =** drop connection without sending any response





Firewall *(iptables – practical examples)*

- Drop all traffic coming from a specific IP (192.168.0.25)
    - **iptables –A INPUT –s 192.168.0.25 –j DROP**

- Drop all traffic coming from a range of IPs (192.168.0.0)
    - **iptables –A INPUT –s 192.168.0.0/24 –j DROP**

- List all rules in a table by line numbers
    - **iptables –L --line-numbers**

- Delete a specific rule by line number
    - **iptables –D INPUT 1**

- To flush the entire chain
    - **iptables –F**

- To block a specific protocol with rejection (e.g. ICMP)
    - **iptables -A INPUT -p icmp -j REJECT**

- To block a specific protocol without rejection (e.g. ICMP)
    - **iptables -A INPUT -p icmp -j DROP**

- To block a specific port # (e.g. http port 80)
    - **iptables -A INPUT -p tcp --dport 80 -j DROP**

- Block connection to a network interface
    - **iptables -A INPUT -i enps03 -s 192.168.0.25 -j DROP**

- Drop all traffic going to www.facebook.com
    - **host -t a www.facebook.com = find IP address**
    - **iptables –A OUTPUT –d 31.13.71.36 –j DROP**

- Block all outgoing traffic to a network range
    - **iptables –A OUTPUT –d 31.13.71.0/24 –j DROP**

- Block all incoming traffic except SSH
    - **iptables -A INPUT -p tcp --dport 22 -j ACCEPT**
    - **iptables -P INPUT DROP**

- After making all the changes save the iptables. Again make sure firewalld is not running
    - **iptables-save** = The file is save in /etc/sysconfig/iptables

- iptables saved file can also be restored
    - **iptables-restore /LOCATION/FILENAME**

- By default everything is logged in
    - **/var/log/messages**