**Firewalld (Old name was iptables)**

* 1. **RHEL6 / RHEL5 ----> iptables**
  2. **CENTOS 7 /8 RHEL7 /8 ---> firewalld**
* **Software firewall**
* **Prevent unauthorized / unwanted packets coming inside / outside from your server**
* **Available in two modes**
  + **Software firewall (iptables / firewalld / ipcop / pfsense / opensense)**
    - **OS based (Computer / Server)**
  + **Hardware firewall** 
    - **Hardware + Software Inbuilt and provided by vendor**
    - **Example: CISCO Miraci / Cyberoam / Cisco PIX / Junipher**

**HUB :**

**ROUTER : Communicate WAN to LAN and**

**LAN to WAN**

**Routing algorithm :**

**RIP / EIGRP / BGP / EGP / ARP / RARP**

**SWITCH: 4 / 8 /12 / 16 /32 /48**

**Manageable**

**Unmanageable**

**Firewall :**

**L3 / L2 Firewall**

**OSI Layers**

**Applicarion**

**Presentation**

**Session**

**Transport**

**Network L3**

**Data link L2**

**Physical**

**--------------------------------------------------------------------------------**

**$ yum install bash-completion**

**$ source /etc/profile.d/bash\_completion.sh**

**Abbreviations :**

**Zone: --->** Zones. The firewalld daemon manages groups of rules using entities called “zones”.

**Public zone (default): →** the default zone for firewalld is set to the public zone. Note: When network interfaces added to firewalld they are assigned to the default zone.

**Dmz zone : →** A *demilitarized zone* (*DMZ*) is a perimeter *network* that protects an organization's internal local-area *network* (LAN) from untrusted traffic. A common *DMZ* meaning is a subnetwork that sits between the public internet and private networks.

**Masquerading: --->** Masquerade NAT allows you to translate multiple IP addresses to another single IP address. You can

use masquerade NAT to hide one or more IP addresses on your internal network behind an IP address that you want to make public.

**NAT** :--> To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP addresses are translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.

**----------------------------------------------------------------------------------**

**Step-1 How to start and enable firewalld service in Centos7 /8**

**systemctl start firewalld && systemctl enable firewalld**

**Step-2 List zones**

**firewall-cmd --list-all-zones**

**Step-3 Check Active & Default**

**List all zones:**

**firewall-cmd --get-zones**

**Check Active list:**

**firewall-cmd --list-all**

**Step-4**

***Add service***

***Add port***

***Remove Service***

***Remove port***

***Add Source***

***Remove Source***

**firewall-cmd --get-zones**

**firewall-cmd --list-all**

**firewall-cmd --add-service=ftp --permanent**

**firewall-cmd --reload**

**firewall-cmd --list-all**

**firewall-cmd --add-port=3306 --permanent**

**firewall-cmd --add-port=443/tcp --permanent**

**firewall-cmd --add-port=3306/tcp --permanent**

**firewall-cmd --reload**

**firewall-cmd --list-all**

**firewall-cmd --reload**

**firewall-cmd --list-all**

**firewall-cmd --add-source=192.168.18.0/24 --zone=public --permanent**

**firewall-cmd --reload**

**firewall-cmd --list-all**

**firewall-cmd --remove-source=192.168.18.0/24 --permanent**

**firewall-cmd --reload**

**firewall-cmd --list-all**

**firewall-cmd --remove-service=http --permanent**

**firewall-cmd --reload**

**firewall-cmd --list-all**

**firewall-cmd --remove-port=3306/tcp --permanent**

**firewall-cmd --remove-port=3306/tcp --permanent**

**--zone=external**

**firewall-cmd --list-all --zone=dmz**

**firewall-cmd --list-all**

**firewall-cmd --list-all-zones**

**Step-4 Rich rules in Firewalld**

***firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=192.168.1.0/24 service name="mysqld" drop'***

**firewall-cmd --reload**

**firewall-cmd --list-all**

**Step-5 Block all incoming / outgoing traffic in your Network :**

**Enable Panic mode:**

**firewall-cmd --panic-on**

**Disable Panic Mode:**

**firewall-cmd --panic-off**

**Step-6 : block icmp (Internet connection messaging protocol) service for all user**

**firewall-cmd --permanent --zone=public --add-icmp-block-inversion**

**firewall-cmd --reload**

**Step-7 Setup Masquerade**

**firewall-cmd --add-masquerade --permanent**

**firewall-cmd --reload**

**Specify Masquerade in specific zone**

**firewall-cmd --add-masquerade --permanent --zone=external**

**firewall-cmd --reload**

**Step-8 Set Default Zone (Change Default Zone)**

**firewall-cmd --set-default-zone=external**

**firewall-cmd --reload**

**Step-9 Add Interface :**

**firewall-cmd --permanent --add-interface=enp0s3**

**firewall-cmd --reload**

**Step-10 SHOW ACTIVE / DEFAULT firewalld**

**firewall-cmd --list-all**

**Step-11 Add port Forwarding**

**Enable port at which you want to send trafiifc :**

**firewall-cmd --permanent --add-port=12345/tcp**

**Now write forward rule**

**firewall-cmd --permanent --add-forward-port=port=80:proto=tcp:toport=12345**

**Reload Firewall**

**firewall-cmd --reload**

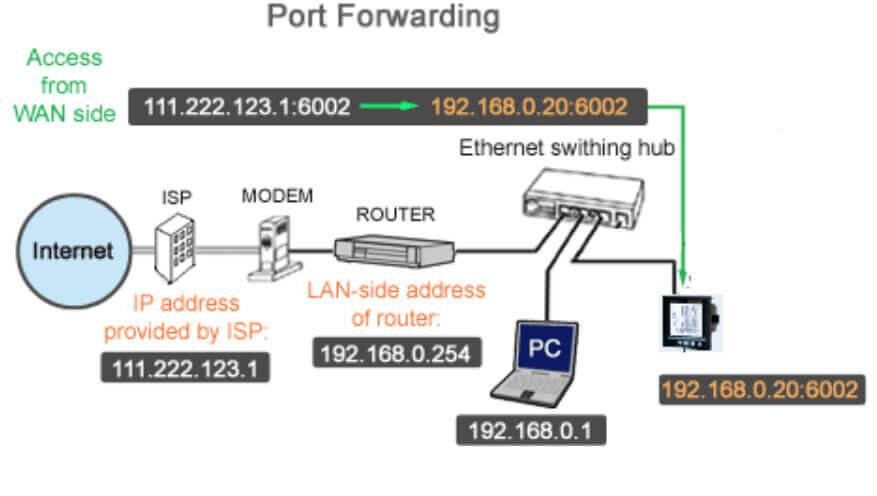
**Show Forward Rules in Default / Active Zone**

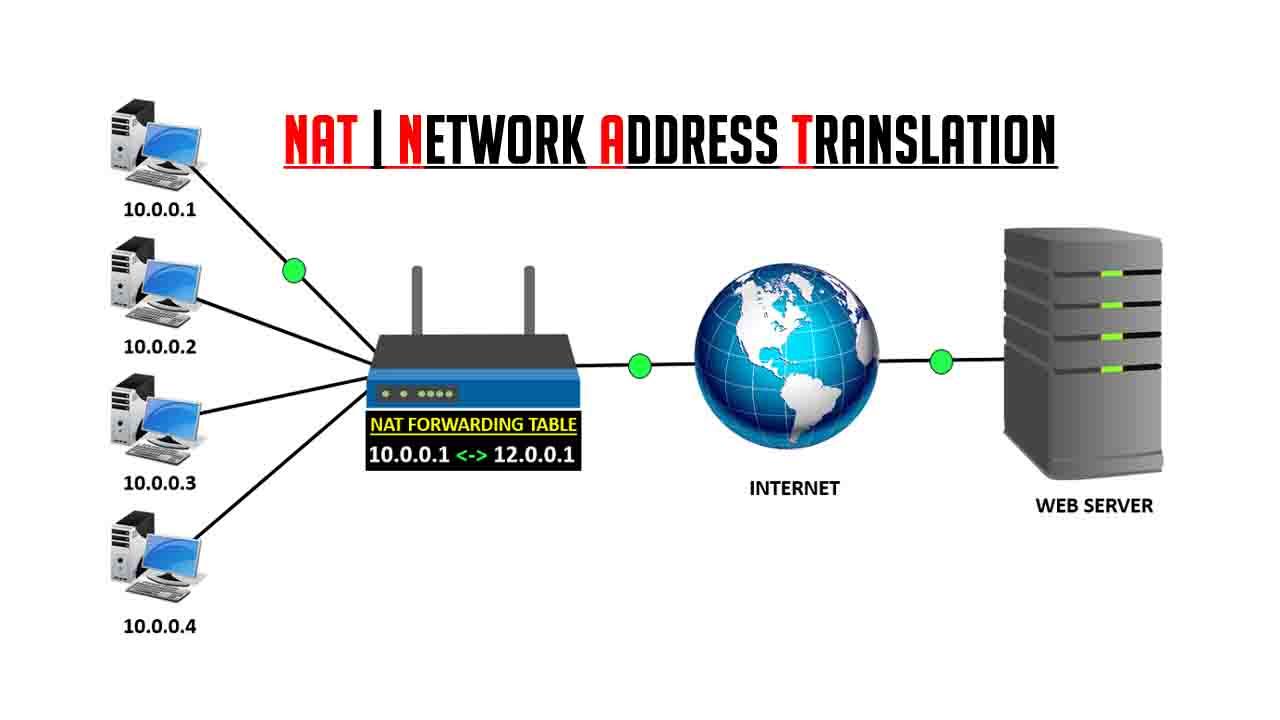
**firewall-cmd --list-all**

**QUESTION ? Can we create our own Zone ?**

**If yes then HOW ?**

**----------------------------xxxxxxxxxxxxxxxx---------------------**

****

****

**10.118.113.5/3128**

**----------------------------------------------------------------------------**

**Iptables: (Centos 6 / RHEL6)**

**Tables**

**Nat → Network Address Translation**

**Filter → ping / pong**

**Mangle ---> Youtube (No one can see ip / Geoloation)**

**Chains (Routing rule) ---> Airport**

***PREROUTING***

**INPUT OUTPUT FORWARD   
 *POSTROUTING***

**ACCEPT : All pckts are accepted by default  
REJECT : Acknowledgement   
DROP : No Acknowledgement**

**---------------------------------------------------------------------------**

**iptables -I INPUT -t nat -p tcp --source 192.168.1.0/24 --dport 3306/tcp -j DROP**

**------------------------------------------------------------------------------**