Firewall Management in Linux

What is firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Firewalld is frontend controller used to implement persistent network traffic rules in Linux.

A packet filtering firewall reads incoming network packets and filters (allows or denies) each data packet based on the header information in the packet.

Firewall Zone

The firewall service allows you to separate networks into different zones based on the level of trust you want to place on the devices and traffic within a specific network.

Such as drop, block, home, public, trusted etc.

Firewall Zones

A brief explanation of each zone follows:

drop: Any incoming network packets are dropped, there is no reply. 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 network connections initiated from within the system are possible.

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

public: 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.

work: For use in work areas. You mostly trust the other computers on networks 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.

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.

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

trusted: All network connections are accepted

1. Configure Firewall Settings:

#firewall-cmd

2. For Check Firewall status

#systemctl status firewalld

3. For start/stop Firewall Service

#systemctl stop firewalld

#systemctl start firewalld

4. For enable/disable Firewall Service

#systemctl disable firewalld

#systemctl enable firewalld

5. For show available zone list

firewall-cmd --get-zones

6. For show available zone list in details

```
#firewall-cmd          --list-all-zones
```

7. For show current default zone

```
# firewall-cmd         --get-default-zone
```

8. For set Default Zone

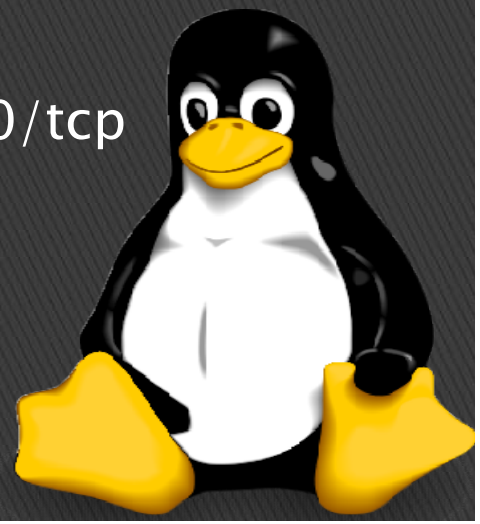
```
#firewall-cmd          --set-default-zone=work
#firewall-cmd                  --reload
```

9. For add service port in firewall

```
#firewall-cmd          --permanent    --add-service=http
```

Or

```
#firewall-cmd          --permanent    --add-port=80/tcp
#firewall-cmd          --reload
```



10. For show Active zone details

#firewall-cmd --get-active-zones

firewall-cmd --zone=work --list-services

11. For remove service/port in firewall

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

Or

#firewall-cmd --permanent --remove-port=80/tcp