What is Firewall and Firewalld ?

- Firewalls are tools that can protect an OS.
- Linux has iptables and firewalld, which contain firewall rules and can manage firewall rules in Linux.
- Essentially, iptables and firewalld are configured by the systems administrator to reject or accept traffic.

Benefits of using firewalld

- Changes can be done immediately in the runtime environment.
- No restart of the service or daemon is needed.

Firewalld in Linux ?

- With the introduction of the Red Hat Enterprise Linux 7.0 (RHEL) in 2011, Firewalld is an advance version of IP-Tables.
- Firewalld is an open source, host-based firewall that seeks to prevent unauthorized access to your computer.
- A firewall is usually a minimum requirement by any information security team at any modern organization.
- Firewalld can restrict access to services, ports, and networks. You can block specific subnets and IP addresses.
- Firewalld uses the concept of zones to segment traffic that interacts with your system.
- A network interface is assigned to one or more zones, and each zone contains a list of allowed ports and services.
- A default zone is also available to manage traffic that does not match any zones.
- Firewalld is the daemon's name that maintains the firewall policies.
- Zone-based firewalls are network security systems that monitor traffic and take actions based on a set of defined rules applied against incoming/outgoing packets.

All About Zone

zones

```
# ls -l /usr/lib/firewalld/zones/
```

```
# cat /usr/lib/firewalld/zones/drop.xml
```

- Firewalld provides different levels of security for different connection zones.
- A zone is associated with at least one network interface (eth0, for example).

We see the preconfigured zones by using the following command:

```
[ root @servera  ~ ] #  firewall-cmd --get-zones
```

```
block dmz drop external home internal libvirt public trusted work
```

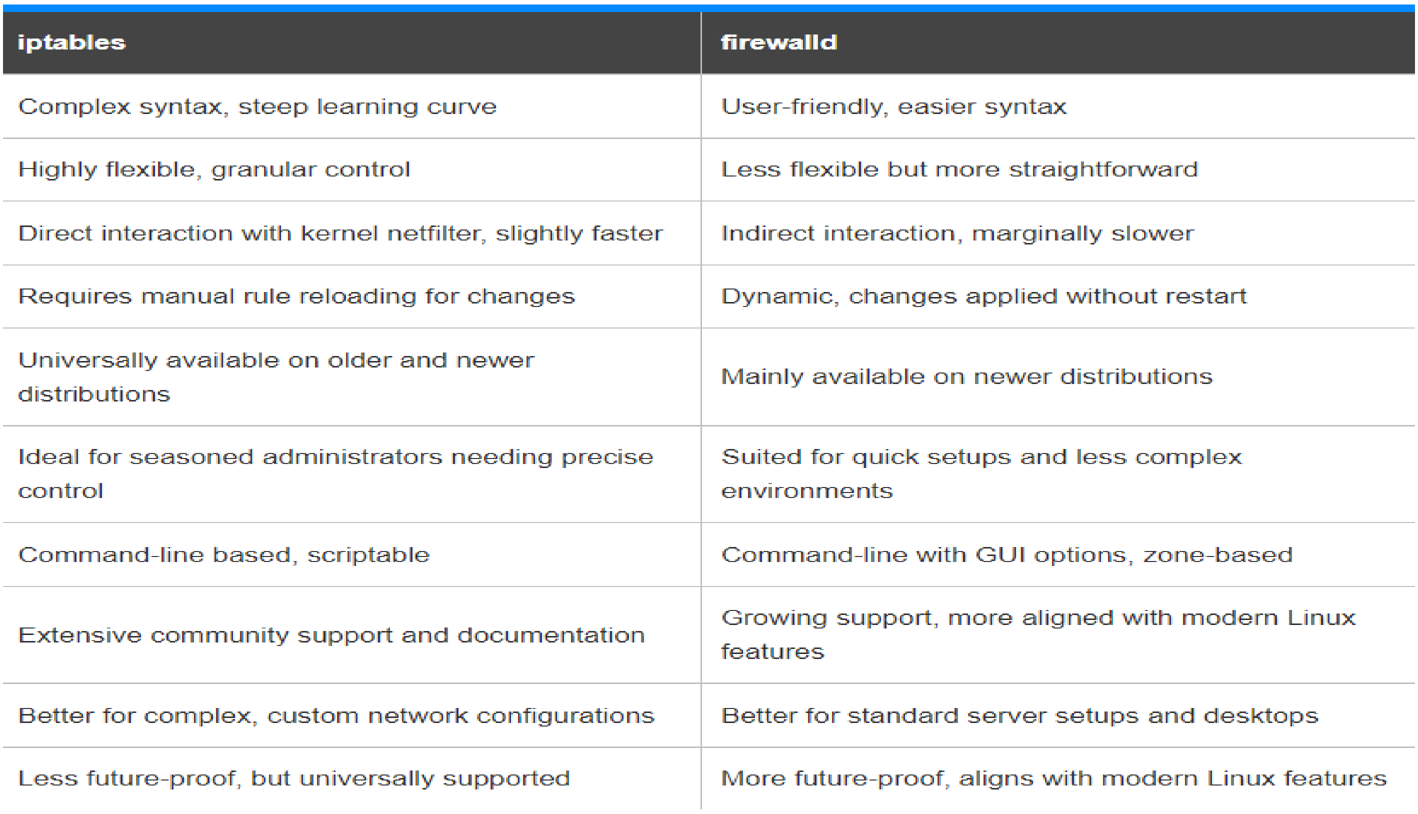
As you see, the zones listed by default are:

- block
- dmz
- drop
- external
- home
- internal
- libvirt
- public
- trusted
- work

Note:-

Generally, the default rule of a firewall is to deny everything and only allow specific exceptions to pass through for needed services.

Difference between IP-Tables and Firewalld ?



iptables	firewalld
Complex syntax, steep learning curve	User-friendly, easier syntax
Highly flexible, granular control	Less flexible but more straightforward
Direct interaction with kernel netfilter, slightly faster	Indirect interaction, marginally slower
Requires manual rule reloading for changes	Dynamic, changes applied without restart
Universally available on older and newer distributions	Mainly available on newer distributions
Ideal for seasoned administrators needing precise control	Suited for quick setups and less complex environments
Command-line based, scriptable	Command-line with GUI options, zone-based
Extensive community support and documentation	Growing support, more aligned with modern Linux features
Better for complex, custom network configurations	Better for standard server setups and desktops
Less future-proof, but universally supported	More future-proof, aligns with modern Linux features

```
firewall-cmd --zone=mytest --permanent --add-rich-rule='rule family=ipv4 source address=
192.168.1.70 port port=22 protocol=tcp reject'
```