Firewalld

Zones

Pre-defined zones within firewalld are:

- **drop**: The lowest level of trust. All incoming connections are dropped without reply and only outgoing connections are possible.
- **block**: Similar to the above, but instead of simply dropping connections, incoming requests are rejected with an icmp-host-prohibited or icmp6-adm-prohibitedmessage.
- **public**: Represents public, untrusted networks. You don't trust other computers but may allow selected incoming connections on a case-by-case basis.
- **external**: External networks in the event that you are using the firewall as your gateway. It is configured for NAT masquerading so that your internal network remains private but reachable.
- **internal**: The other side of the external zone, used for the internal portion of a gateway. The computers are fairly trustworthy and some additional services are available.
- **dmz**: Used for computers located in a DMZ (isolated computers that will not have access to the rest of your network). Only certain incoming connections are allowed.
- **work**: Used for work machines. Trust most of the computers in the network. A few more services might be allowed.
- **home**: A home environment. It generally implies that you trust most of the other computers and that a few more services will be accepted.
- **trusted**: Trust all of the machines in the network. The most open of the available options and should be used sparingly.

Verify what zone is used by default

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

Verify what zones are active

```
firewall-cmd --get-active-zones
```

View all info for default zone

```
firewall-cmd --list-all
```

List pre-defined zones and custom zone names

```
firewall-cmd --get-zones
```

View all information for a specific zone

```
firewall-cmd --permanent --zone= home  --list-all
```

Change default zone

```
firewall-cmd --set-default-zone= home
```

Adding a service to a zone

> First it is recommended to not add --permanent and to test of the service is reachable, if it works add the --permanent

```
firewall-cmd --zone=public  --permanent  --add-service=http
```

Removing/Denying a service

```
firewall-cmd --zone=public --permanent --remove-service=http
```

List services

```
firewall-cmd --zone=public --permanent --list-services
```

Removing/Denying a port

```
firewall-cmd --zone=public --permanent --remove-port=12345/tcp
```

To add a custom port

```
firewall-cmd --zone=public --permanent --add-port=8096/tcp
```

Add a port range

```
firewall-cmd --zone=public --permanent --add-port=4990-4999/udp
```

Check if port is added

```
firewall-cmd --list-ports
```

Services are simply collections of ports with an associated name and description, the simplest way to add a port to a service would be to copy the xml file and change the definition/port number.

```
cp /usr/lib/firewalld/services/service.xml /etc/firewalld/services/example.xml
```

Then reload

```
firewall-cmd --reload && firewall-cmd --get-services
```

Creating Your Own Zones

```
firewall-cmd --permanent --new-zone=my_zone
firewall-cmd --reload
firewall-cmd --zone=my_zone --add-service=ssh
firewall-cmd --zone=my_zone --change-interface=eth0
```

> Then add the zone to your /etc/sysconfig/network-scripts/ifcfg-eth0

> ZONE=my_zone

```
systemctl restart network
systemctl restart firewalld
```

And check if it works

```
firewall-cmd --zone=my_zone --list-services
```

Port Forwarding

Forward traffic coming from 80 to 12345

```
firewall-cmd --zone="public" --add-forward-port=port=80:proto=tcp:toport=12345
```

To forward a port to a different server:

> Forwards traffic from local port 80 to port 8080 on *a remote server* located at the IP address: 123.456.78.9.

```
firewall-cmd --zone=public --add-masquerade
firewall-cmd --zone="public" --add-forward-port=port=80:proto=tcp:toport=8080:toaddr=123.456.78.
```

If you need to remove it

```
sudo firewall-cmd --zone=public --remove-masquerade
```

Rich Rules

Allow all IPv4 traffic from host 192.168.0.14.

```
firewall-cmd --zone=public --add-rich-rule 'rule family="ipv4" source address=192.168.0.14 accep
```

Deny IPv4 traffic over TCP from host 192.168.1.10 to port 22.

```
firewall-cmd --zone=public --add-rich-rule 'rule family="ipv4" source address="192.168.1.10" por
```

Allow IPv4 traffic over TCP from host 10.1.0.3 to port 80, and forward it locally to port 6532.

```
firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=10.1.0.3 forward-por
```

Forward all IPv4 traffic on port 80 to port 8080 on host 172.31.4.2 (masquerade should be active on the zone).

```
firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 forward-port port=80 protocol=tcp t
```

To list your current Rich Rules:

```
firewall-cmd --list-rich-rules
```

Revision #3
Created 2017-07-23 05:57:38 UTC by Dave
Updated 2017-12-16 08:42:06 UTC by Dave