Firewall (firewalld – practical examples)

- The firewalld has multiple zone, to get a list of all zones

  `firewall-cmd --get-zones`

- To get a list of active zones

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

- To get firewall rules for public zone

  `firewall-cmd --zone=public --list-all`

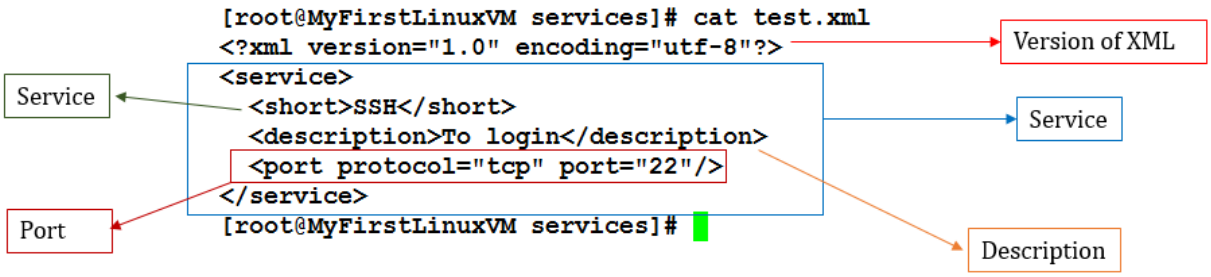
  `OR`

  `firewall-cmd --list-all`

- All services are pre-defined by firewalld. What if you want to add a 3rd party service

  `/usr/lib/firewalld/services/allservices.xml`

  `Simply cp any .xml file and change the service and port number`



- To add a service (http)

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

- To remove a service

  `firewall-cmd --remove-service=http`

- To reload the firewalld configuration

  firewall-cmd --reload

- To add or remove a service permanently

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

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

- To add a service that is not pre-defined by firewalld

  /usr/lib/firewalld/services/allservices.xml

  Simply cp any .xml file SERVICENAME.xml and change the service and port number

  systemctl restart firewalld

  firewall-cmd --get-services (to verify new service)

  firewall-cmd --add-service=SERVICENAME

- To add a port

  firewall-cmd --add-port=1110/tcp

- To remove a port

  firewall-cmd --remove-port=1110/tcp

- To reject incoming traffic from an IP address

  firewall-cmd --add-rich-rule='rule family="ipv4" source address="192.168.0.25" reject'

- To block and unblock ICMP incoming traffic

  firewall-cmd --add-icmp-block-inversion

  firewall-cmd --remove-icmp-block-inversion

- To block outgoing traffic to a specific website/IP address

  host -t a www.anywebsite.com **= find IP address**

  firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -d 192.168.1.0 -j DROP