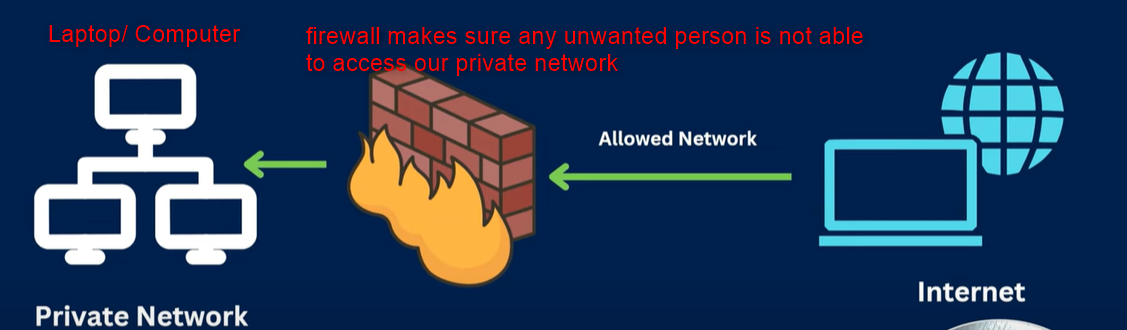
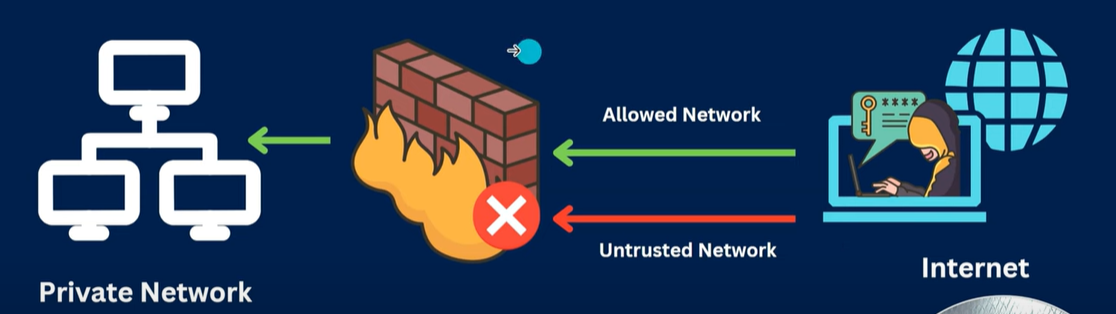
**Linux FIREWALL Management - firewalld service, rules | MPrashant**

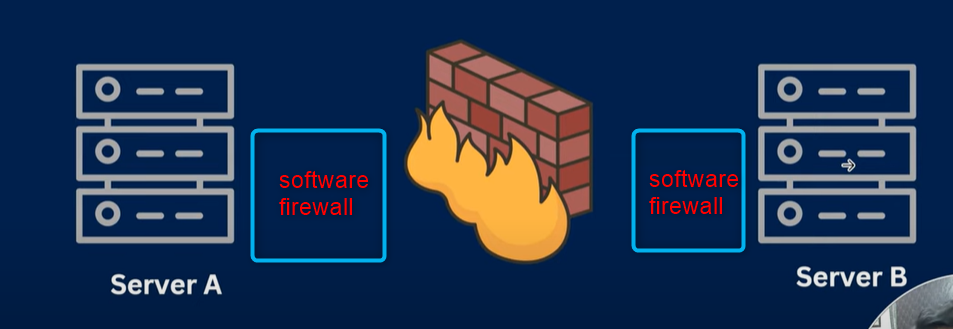
* A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on the rules defined
* Firewall is basically used to determine and block untrusted network to not be able to access the system



* Say I get a request from a unwanted server, so firewall will check if the requested server/ ip can be trustworthy or not and based on the response it will allow the connection



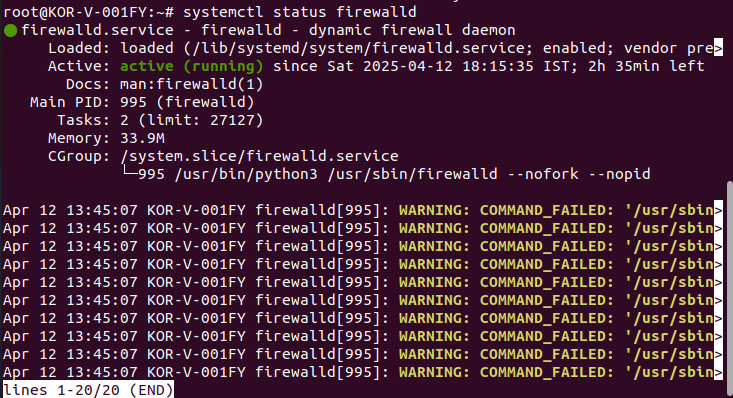
* There are 2 types of firewall
  + Software based – Running on the OS, present in windows and linux
  + Hardware based – A dedicated appliance(hardware like router) with firewall software between two different networks(mostly used by network team). So the appliance/hardware will be dedicated only for firewall to make sure that none of the harmful connections to the server are made
* Different firewall cases
  + CASE-1: We have 2 servers each with a software based firewall and then we have one hardware firewall in between the 2 servers
  + Since server 1 wants to establish a connection with server 2, server 1 software firewall will allow the connection, say the hardware firewall in middle also allows the connection but the server 2 firewall didn’t allow the connection and we get error saying connection request refused



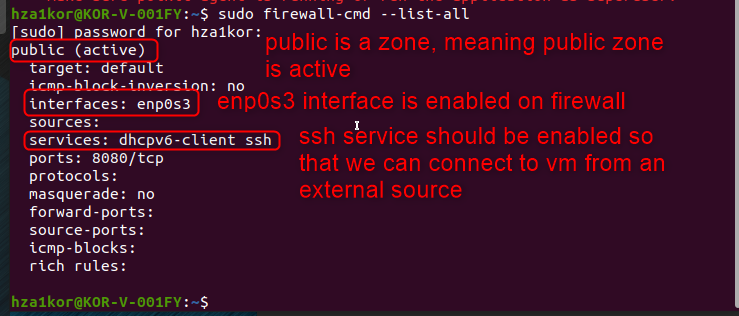
* There are different tools that can be used to manage firewall
  + iptables
  + firewalld – newer version in centos, fedora, redhat etc
* Command to check if firewalld service is installed in ubuntu – dpkg -l | grep firewalld

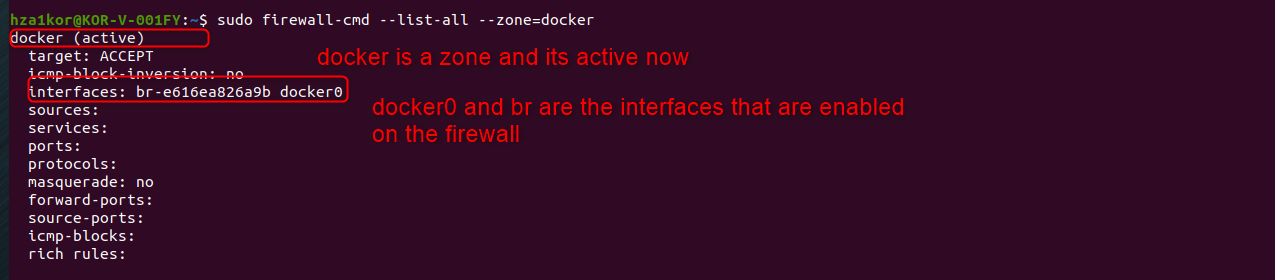


* Command to check if firewalld service is installed in red hat distros – rpm -qa| grep firewalld
* Commands to start/ stop/ enable/ disable/ restart and check status of firewalld
  + systemctl start/stop firewalld
  + systemctl enable/disable firewalld
  + systemctl status firewalld
  + systemctl restart firewalld

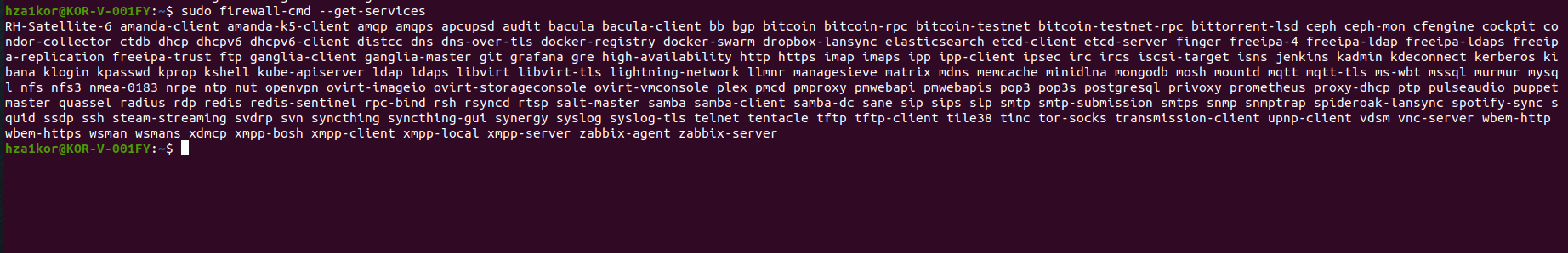


* to check the rules of firewalld, like what all services are enabled, to specify ports, interfaces, protocols etc, we can run **sudo firewall-cmd --list-all**

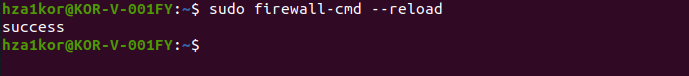




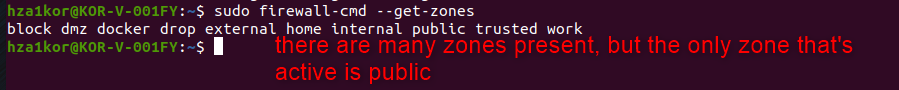
* command to list all the services that firewalld is aware of – sudo **firewall-cmd --get-services**
* this command basically means firewalld has knowledge of all the below services on this particular linux server

****

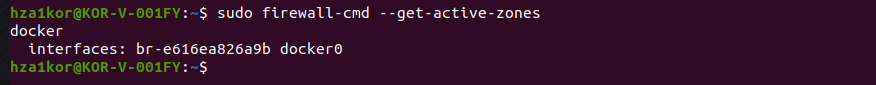
* say I want to add a few more services in firewall, then I have to make sure the service I add should belong to this list of services that firewall knows about
* to reload the configuration of firewalld use – **sudo firewall-cmd –reload**
* this command is useful when we perform some changes in the firewall and want to refresh/ reload the new changes

****

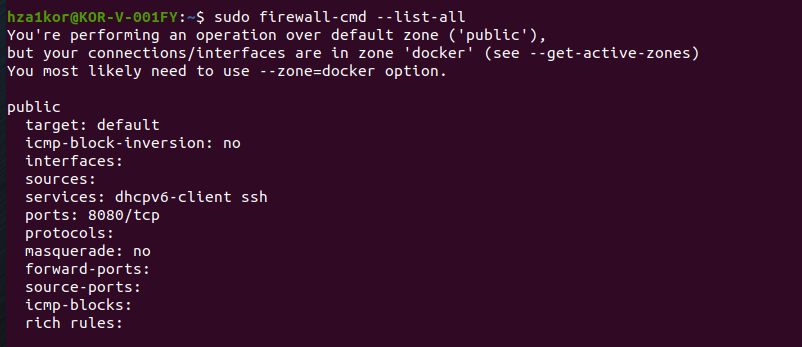
* firewall has multiple zones, to list all the firewall zones – **sudo firewall-cmd --get-zones**

****

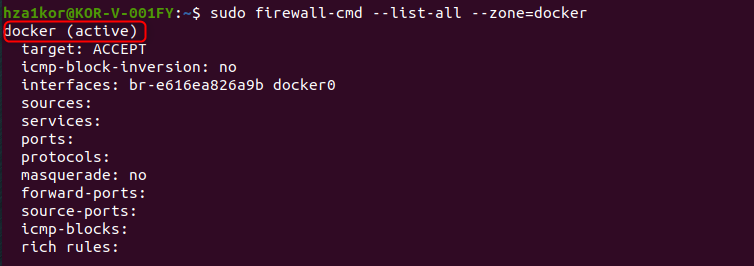
* to see the list of all the active firewall zones – **sudo firewall-cmd --get-active-zones**

****

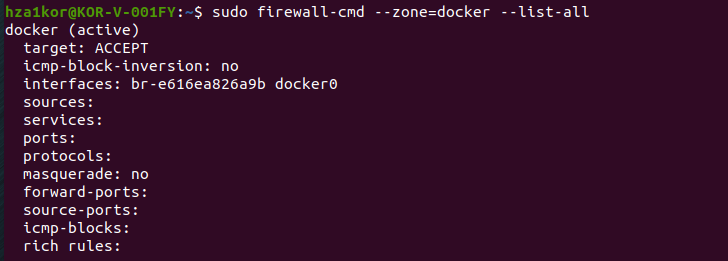
* currently I see that docker is active and not public, and when I run **sudo firewall-cmd --list-all,** somehow public is not enabled now

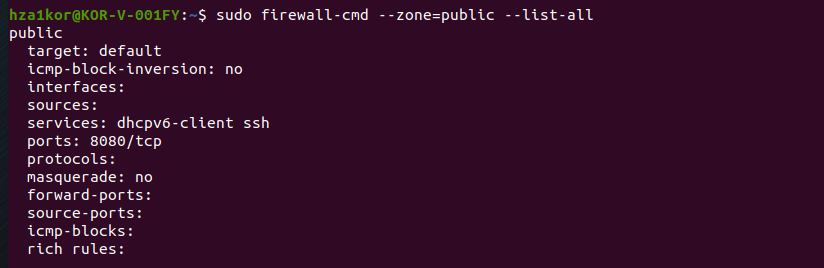
****

* when I run list all with –zone=docker option is see docker is active .
* command - **sudo firewall-cmd --list-all --zone=docker**

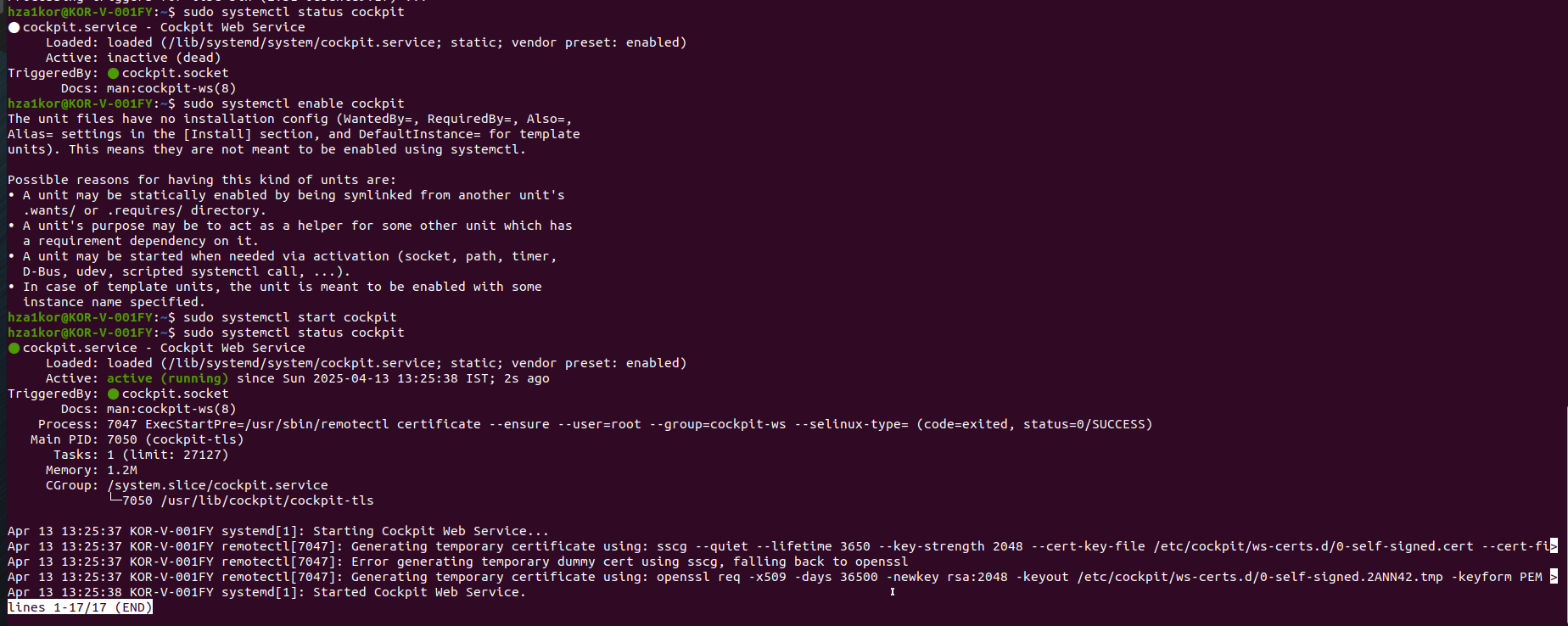
****

* To get the firewall rules for a particular zone – **firewall-cmd –-zone=docker/public –list-all**

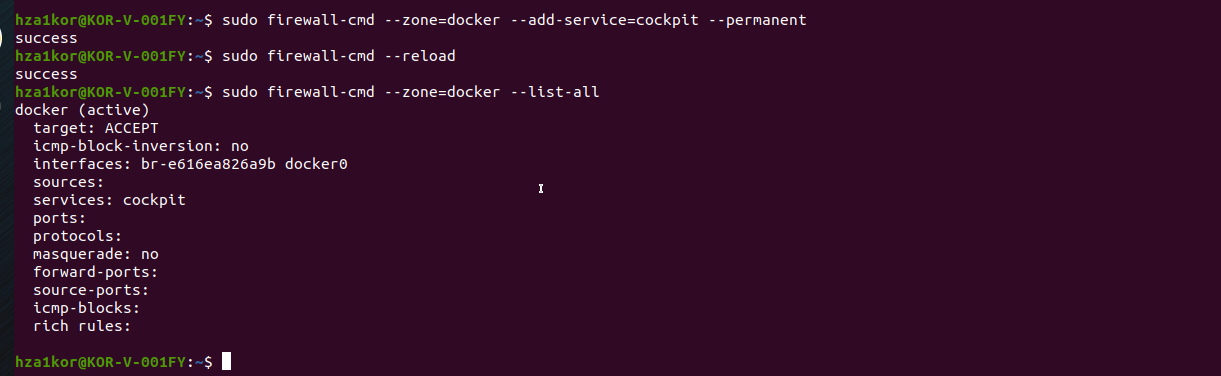
****

****

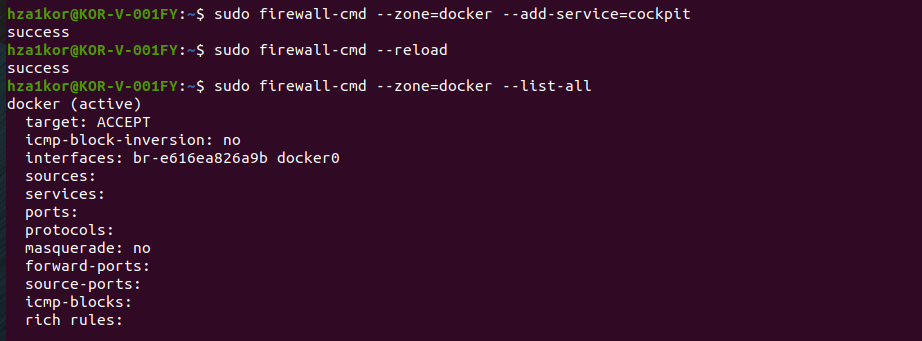
* to add a new service in the firewall rules – **sudo firewall-cmd --add-service=<name\_of\_service> --permanent**
* to remove a service in the firewall rules – **sudo firewall-cmd --remove-service=<name\_of\_service>**
* say for zone docker, I want to add cockpit as a service, so I will run the below commands
  + firewall-cmd –zone=docker --add-service=cockpit
  + firewall-cmd --reload
  + firewall-cmd --zone=docker --list-all
* **note that** when I tried running this, I was not able to see cockpit service, then I checked the status of cockpit, and the o/p was cockpit.service not found
* **so then I installed cockpit service using sudo apt install cockpit**
* then again ran – sudo systemctl status cockpit, it was inactive, then I tried enabling, I got error so I just started the service

****

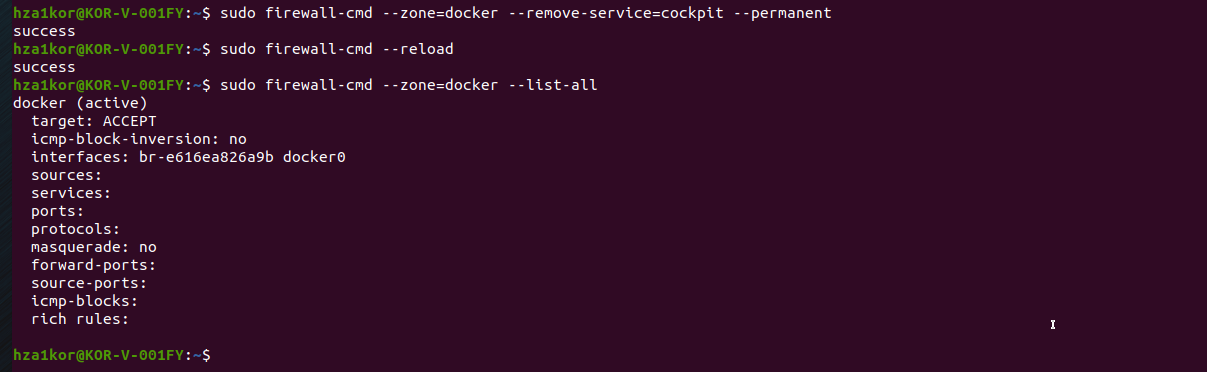
* make sure that whenever you want to add a new service, it should be enabled or active, and also without the permanent option in adding a service, I was not getting the proper response
* O/p using permanent option

****

* **o/p without using permanent option**

****

* **Now to remove the cockpit service –**
  + firewall-cmd --zone=docker --remove-service=cockpit --permanent
  + firewall-cmd --reload
  + firewall-cmd --zone=docker --list-all

****

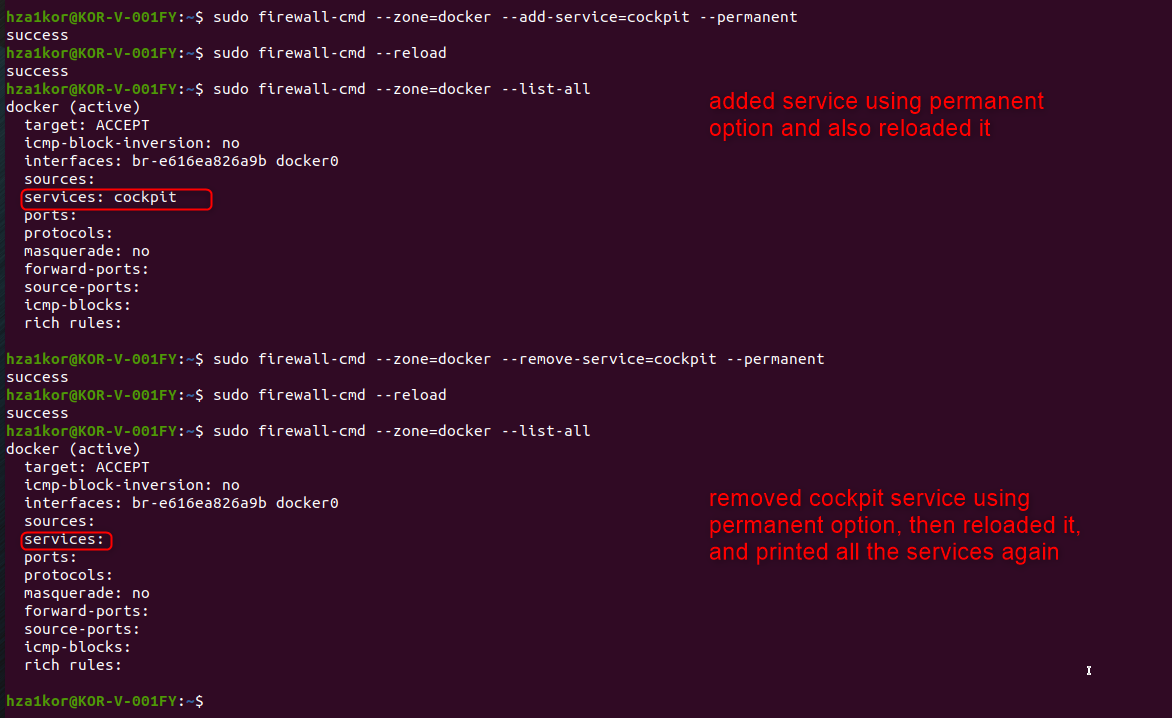
* One interesting thing I found is that, when I add a service, without permanent option, I do a reload then I list the services, I was not able to see that service added, so when I add a service its only added for temporary basis, when I do reload just after adding, since the firewall rules are reloaded, the temporary service is removed, so either add the permanent option, else don’t reload, do your task and then finally trya reload

****

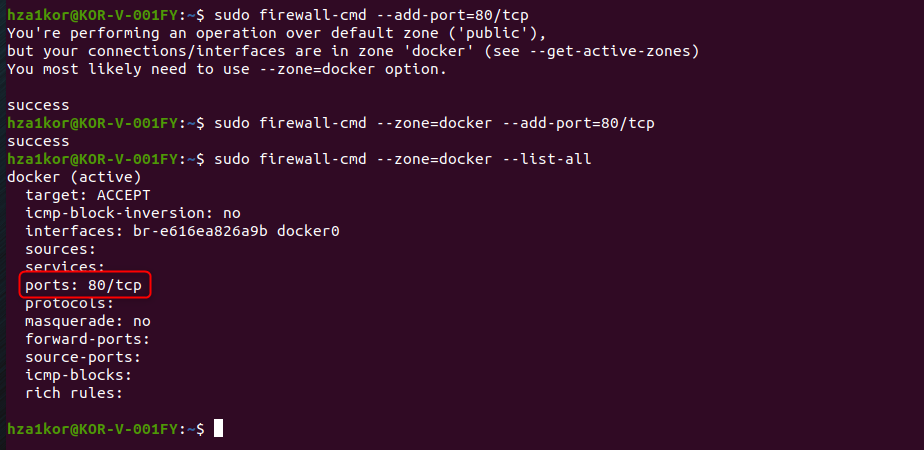
* New options to add or remove a service
  + Adding a service using permanent option
    - **sudo firewall-cmd --zone=docker --add-service=cockpit --permanent**
    - **sudo firewall-cmd --reload**
    - **sudo firewall-cmd --zone=docker --list-services**
* Adding a service without permanent option
  + **sudo firewall-cmd --zone=docker --add-service=cockpit**
  + **sudo firewall-cmd --zone=docker --list-services**
* Removing a service using permanent option
  + - **sudo firewall-cmd --zone=docker --remove-service=cockpit --permanent**
    - **sudo firewall-cmd --reload**
    - **sudo firewall-cmd --zone=docker --list-services**
* Removing a service without permanent option
  + **sudo firewall-cmd --zone=docker --remove-service=cockpit**
  + **sudo firewall-cmd --zone=docker --list-services**
* **Adding and removing without permanent option**

****

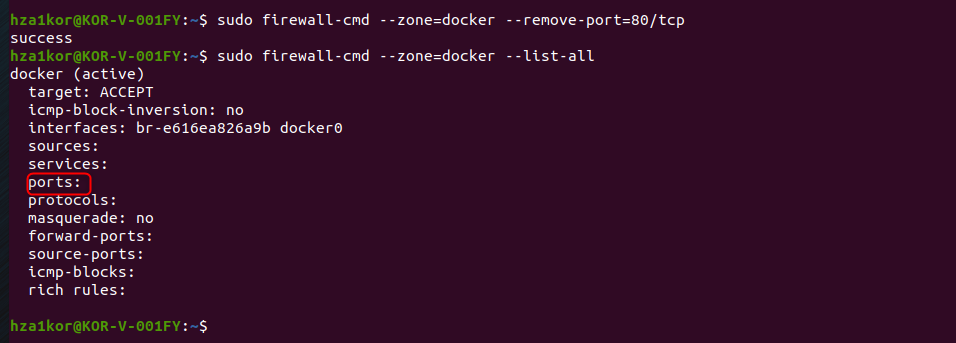
* **Adding and removing using permanent option**



* To add a port to firewall – **sudo firewall-cmd --zone=docker --add-port=<port\_number>/<protocol\_name> or sudo firewall-cmd --zone=docker --add-port=<port\_number>/<protocol\_name> --permanent**
  + Example - sudo firewall-cmd --zone=docker--add-port=80/tcp
* To remove a port from firewall - **sudo firewall-cmd --zone=docker --remove port=<port\_number>/<protocol\_name> or sudo firewall-cmd --zone=docker --remove port=<port\_number>/<protocol\_name> --permanent**
  + Example - sudo firewall-cmd --zone=docker--remove-port=80/tcp
* To add a port example without permanent option



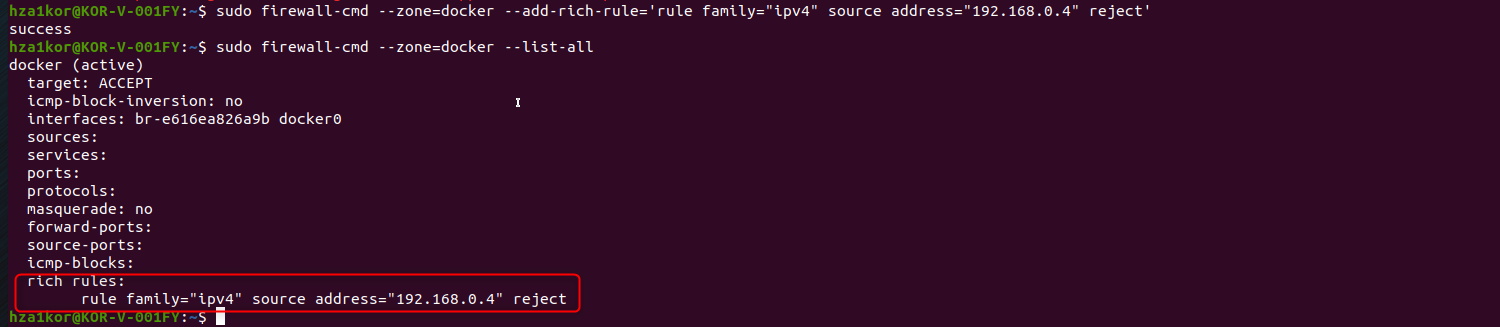
* To remove a port without permanent option



* **To block incoming traffic from an ip** address means if I ever receive any data from this ip, reject it –

sudo firewall-cmd --zone=docker --add-rich-rule='rule family="ipv4" source address="192.168.0.4" reject'

* Then run the command – sudo firewall-cmd --zone=docker --list-all



* **To block outgoing traffic to an IP or URL** meaning even by mistake I should not sent an paclets or data to this ip
* Command – sudo firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -d 192.168.0.4 -j DROP
* Example to block facebook.com so that we can’t ping facebook.com





* To block incoming ICMP traffic (meaning I don’t want anyone to be able to ping me from external vm or sever or windows)– **sudo firewall-cmd --add-icmp-block-inversion**
* With this option no one would be able to ping your server/ip address

