firewalld

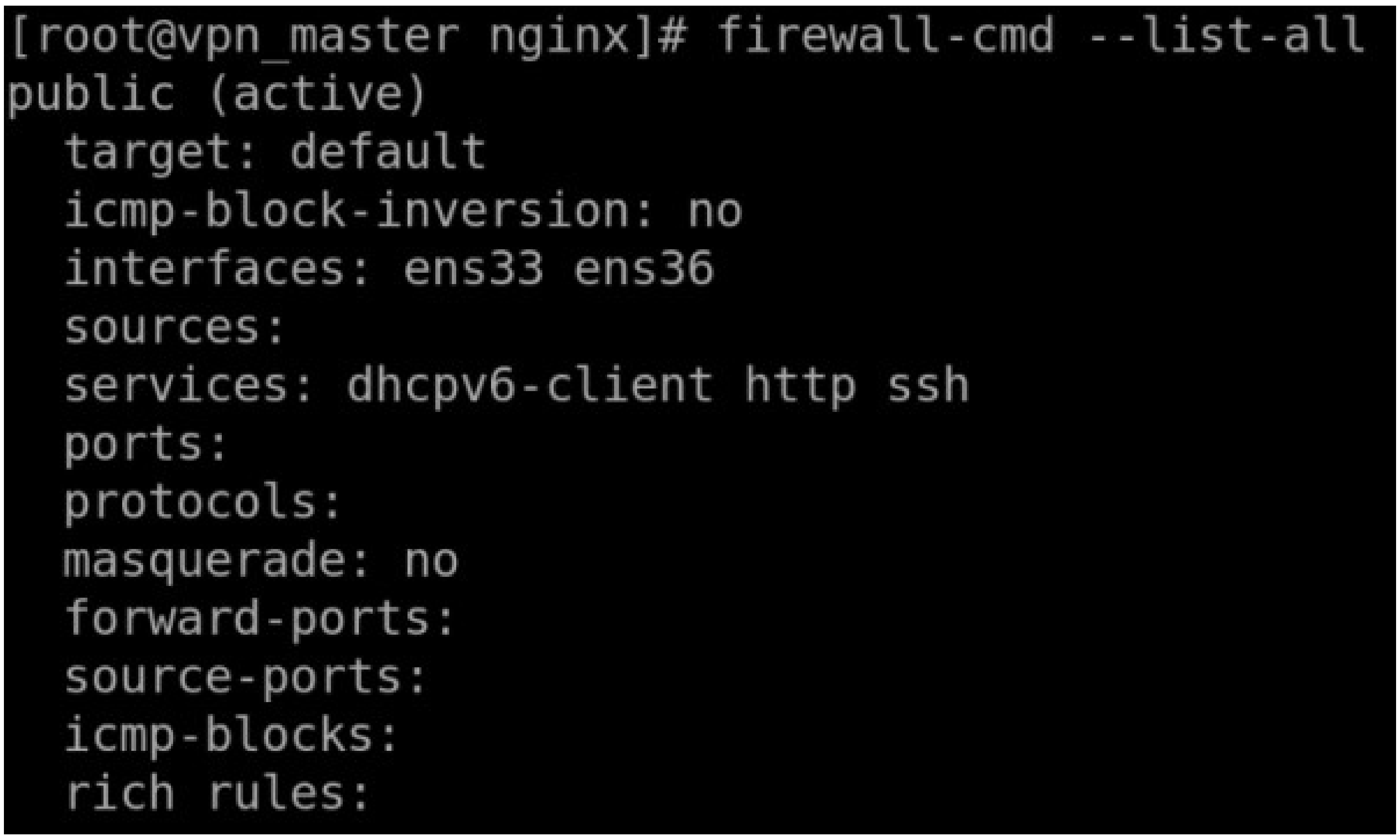
Zones in firewalld

1. Public
2. Work
3. DMZ : demilitarlized zones

first check if firewall is running or not
-> systemctl status firewalld

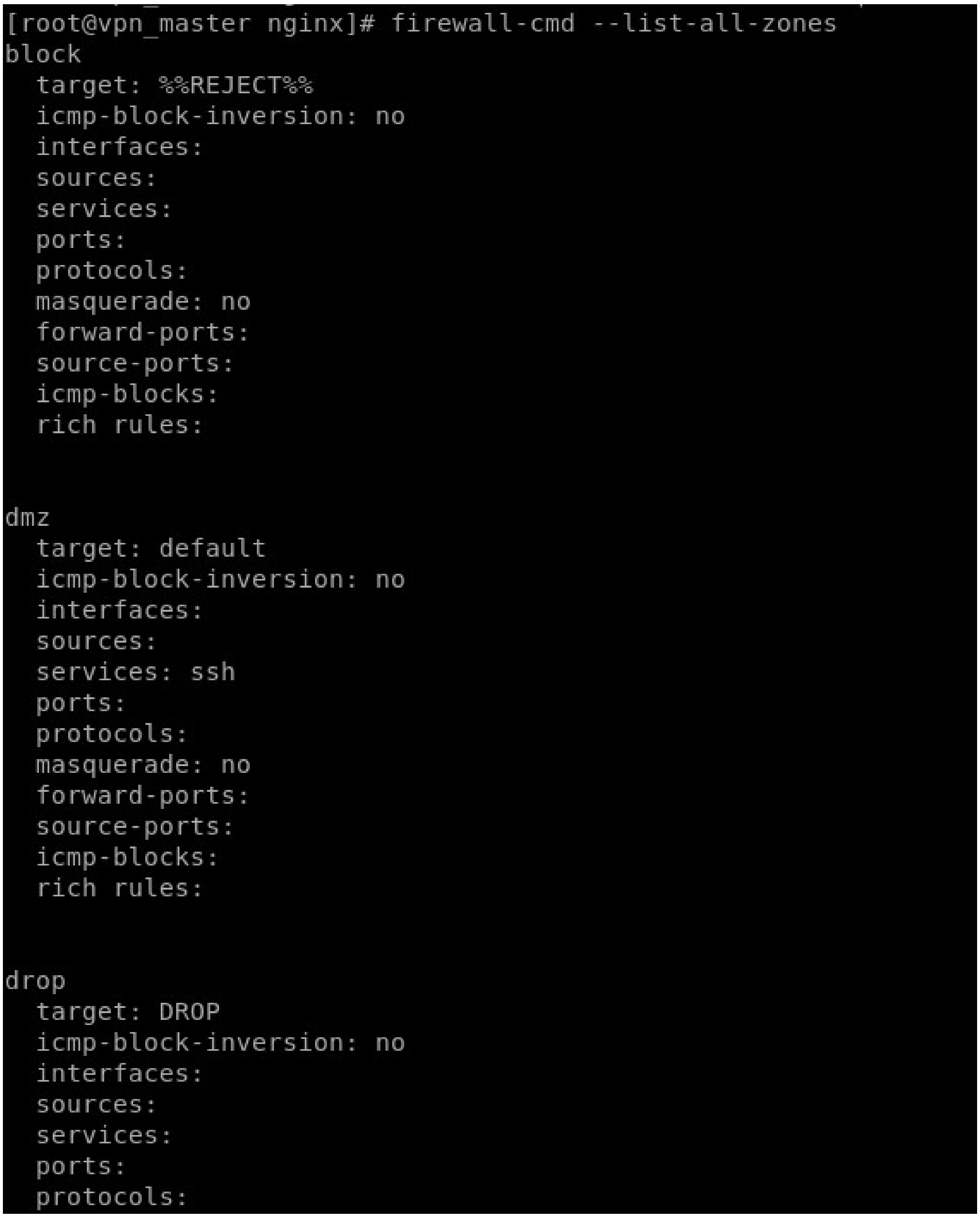
firewall command line tool : firewall-cmd

# how to list all the zone in firewall
-> firewall-cmd --list-all



```
[root@vpn_master nginx]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33 ens36
  sources:
  services: dhcpv6-client http ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

-> firewall-cmd --list-all-zones



```
[root@vpn_master nginx]# firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


dmz
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


drop
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
```

```
→ firewall-cmd --get-active-zone
→ firewall-cmd --zone=[zone_name] --list-all
→ firewall-cmd --zone=[zone_name] --list-interfaces
# only one interface is allowed in one zone
→ firewall-cmd --zone=[zone_name] --remove-interface=[interface-name]
# firewall-cmd --zone=public --remove-interface=ens33
→ firewall-cmd --zone=[zone_name] --add-interface=[interface-name]
# firewall-cmd --zone=work --add-interface=ens33

# how to add a zone
→ firewall-cmd --permanent --new-zone=zone-name
# firewall-cmd --permanent --new-zone=hpcsa

# reload the firewall in order to see the newly created zone
→ firewall-cmd --list-all-zone | grep hpcsa
```

```
# now we'll see the newly update
→ firewall-cmd --zone=work --list-interfaces
# after reload all the interfaces get's reset reason being, we've not made the changes permanent
→ firewall-cmd --zone=public --list-interfaces
# after reload all the interfaces were showing in the default public zone

# to see newly created zone
→ firewall-cmd --zone=hpcsa --list-all

# how to block ssh login from one of the interface

→ firewall-cmd --zone=public --remove-interface=ens33
→ firewall-cmd --zone=hpcsa --add-interface=ens33

# default zone: public

# how to get services running in a specific zones
→ firewall-cmd --get-services | grep ssh

# how to add service in a specific zones
→ firewall-cmd --add-service=ssh --zone=hpcsa

# how to remove service in a specific zones
→ firewall-cmd --remove-service=ssh --zone=hpcsa

# how to add port in a specific zones
→ firewall-cmd --add-port=22/tcp --zone=hpcsa

# how to remove port in a specific zones
→ firewall-cmd --remove-port=22/tcp --zone=hpcsa

# how to confirm if port has been added or not
→ firewall-cmd --list-all --zone=hpcsa

# how to add service in a specific zones
→ firewall-cmd --add-service=http --zone=hpcsa

# how to remove service in a specific zones
→ firewall-cmd --remove-service=http --zone=hpcsa

# how to add multiple port in a specific zones
```

```
→ firewall-cmd --add-port={443/tcp,53/udp,3336/tcp} --zone=hpcsa

# how to confirm if ports has been added or not
→ firewall-cmd --list-all --zone=hpcsa

# how to add or remove range of port in a specific zones
→ firewall-cmd --add-port=2500-3000/tcp --zone=hpcsa
→ firewall-cmd --remove-port=2500-3000/tcp --zone=hpcsa

# how to add protocol
→ firewall-cmd --add-protocol=icmp --zone=hpcsa
→ firewall-cmd --remove-protocol=icmp --zone=hpcsa



# how to block ping
→ firewall-cmd --add-icmp-block echo-request --zone=hpcsa
# how to unblock ping from all networks
→ firewall-cmd --remove-icmp-block echo-request --zone=hpcsa
# how to check if ping is blocked or note from all networks
→ firewall-cmd --query-icmp-block echo-request --zone=hpcsa

# how to allow to deny from specific source or destination
→ firewall-cmd --zone=hpcsa --add-rich-rule [further rule]
# firewall-cmd --zone=hpcsa --add-rich-rule="rule family=ipv4 source
address=[ip_address] service name=ssj accept" --permanent

# location where config file of firewalld has been stored
→ cd /etc/firewalld
→ ll
→ vi hpcsa.xml
→
```