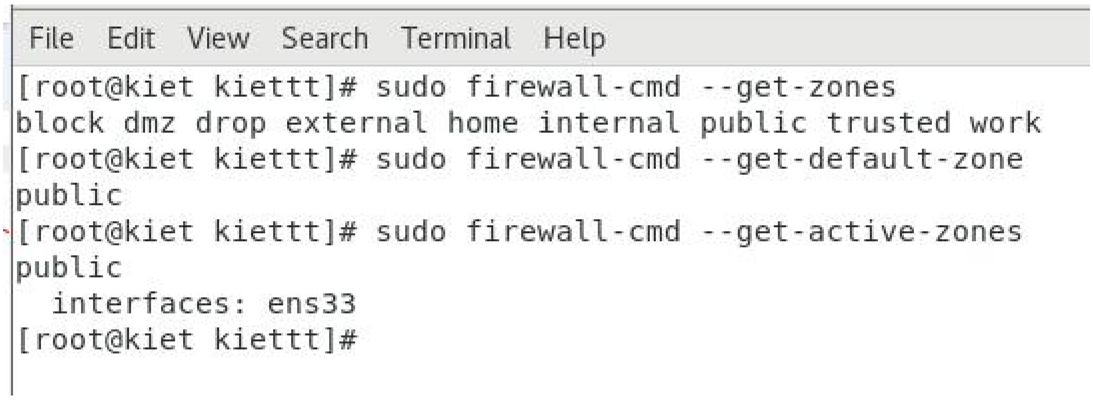
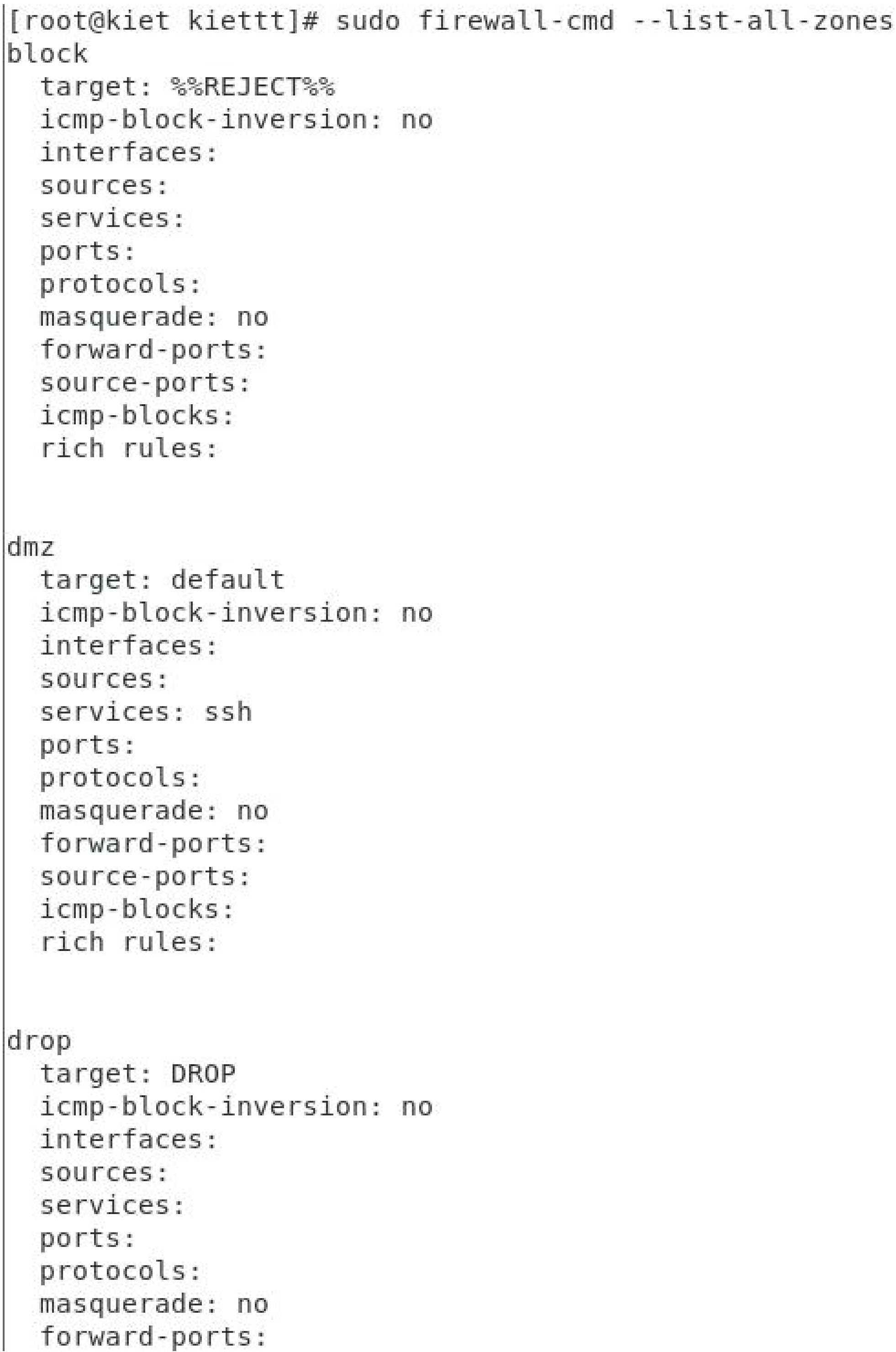
1/ Identify existing network settings and apply the appropriate firewall configuration for your environment.

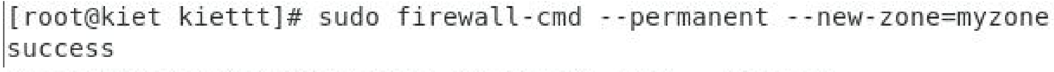


```
[root@kiet kiettt]# sudo firewall-cmd --get-zones
block dmz drop external home internal public trusted work
[root@kiet kiettt]# sudo firewall-cmd --get-default-zone
public
[root@kiet kiettt]# sudo firewall-cmd --get-active-zones
public
  interfaces: ens33
[root@kiet kiettt]#
```

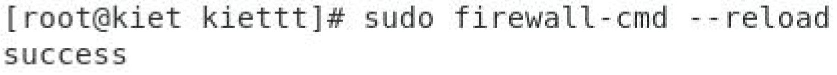
2/ Create a new zone:



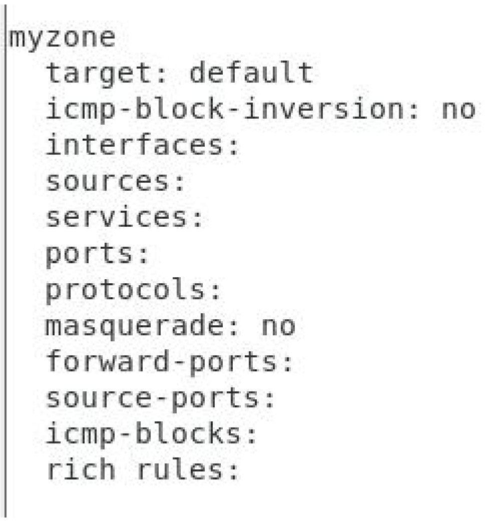
```
[root@kiet kiettt]# sudo firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


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:
  masquerade: no
  forward-ports:
```



```
[root@kiet kiettt]# sudo firewall-cmd --permanent --new-zone=myzone
success
```

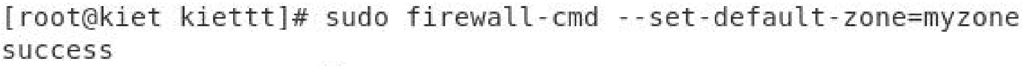


```
[root@kiet kiettt]# sudo firewall-cmd --reload
success
```

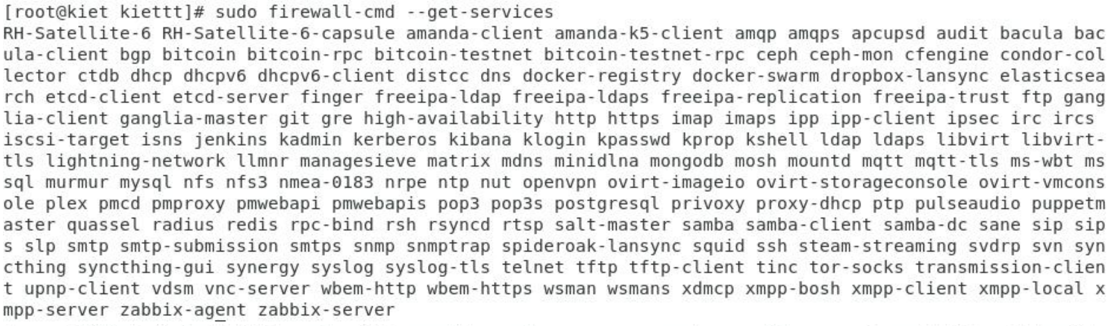


```
myzone
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

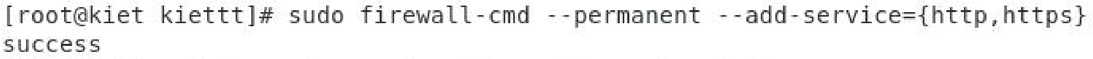
3/Set the default zone to myzone.



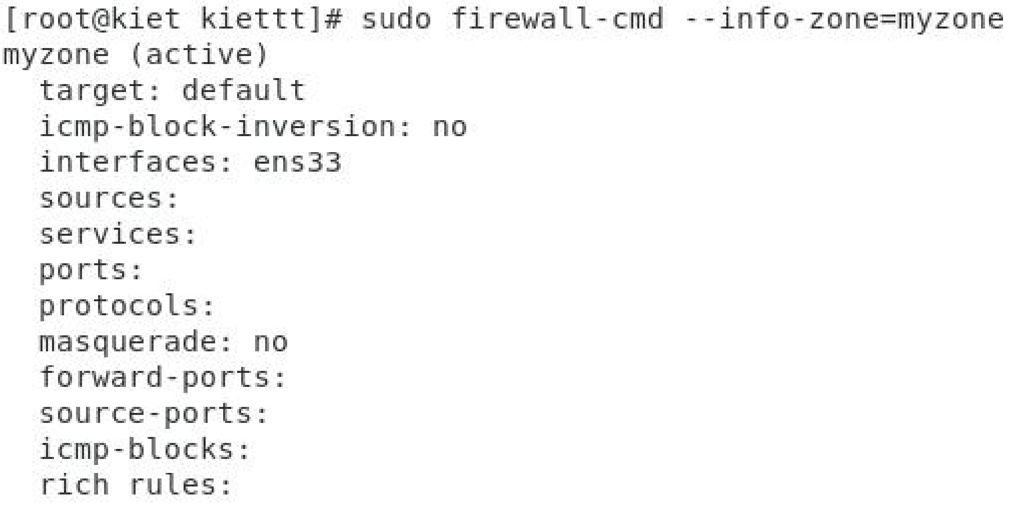
```
[root@kiet kiettt]# sudo firewall-cmd --set-default-zone=myzone
success
```



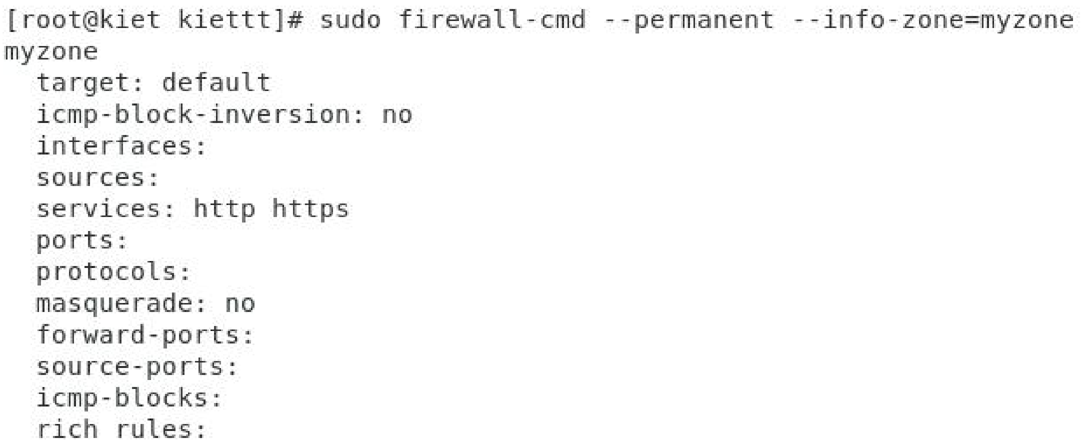
```
[root@kiet kiettt]# sudo firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bac
ula-client bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-col
lector ctdb dhcp dhcpv6 dhcpv6-client distcc dns docker-registry docker-swarm dropbox-lansync elasticsea
rch etcd-client etcd-server finger freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp gang
lia-client ganglia-master git gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs
iscsi-target isns jenkins kadmin kerberos kibana klogin kpasswd kprop kshell ldap ldaps libvirt libvirt-
tls lightning-network llmnr managesieve matrix mdns minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt ms
sql murmur mysql nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmcons
ole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy proxy-dhcp ptp pulseaudio puppetm
aster quassel radius redis rpc-bind rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sip
s slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh steam-streaming svdrp svn syn
cthing syncthing-gui synergy syslog syslog-tls telnet tftp tftp-client tinc tor-socks transmission-clien
t upnp-client vdsm vnc-server wbem-http wbem-https wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local x
mpp-server zabbix-agent zabbix-server
```



```
[root@kiet kiettt]# sudo firewall-cmd --permanent --add-service={http,https}
success
```

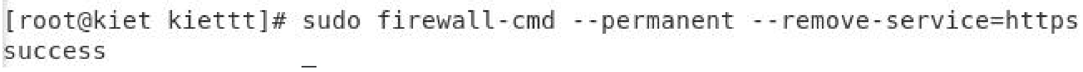


```
[root@kiet kiettt]# sudo firewall-cmd --info-zone=myzone
myzone (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```



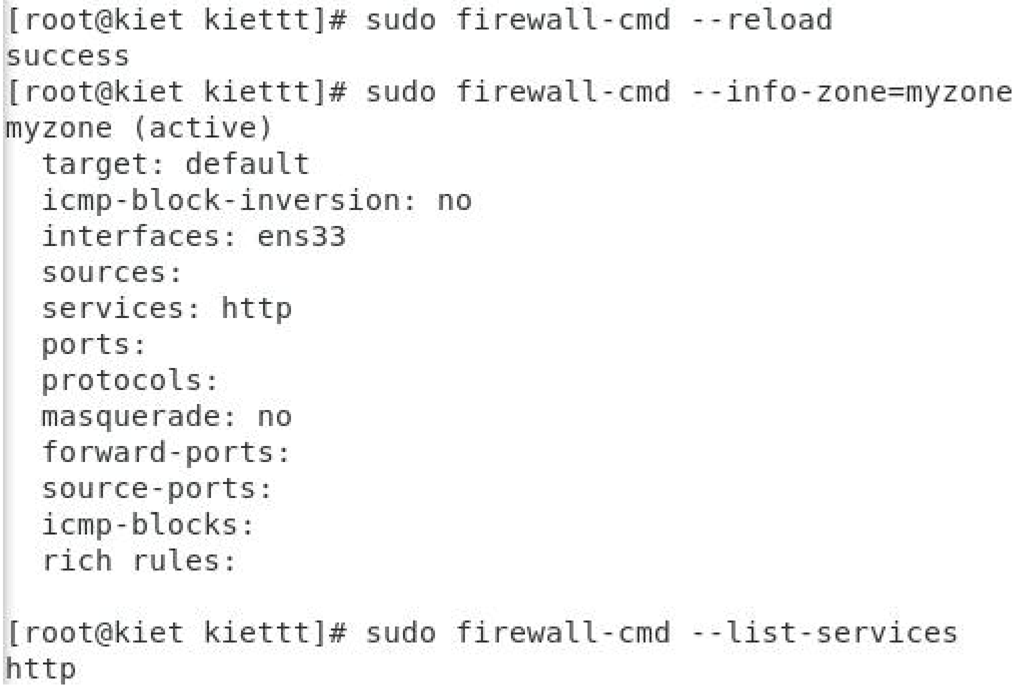
```
[root@kiet kiettt]# sudo firewall-cmd --permanent --info-zone=myzone
myzone
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: http https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

4/Remove https service:



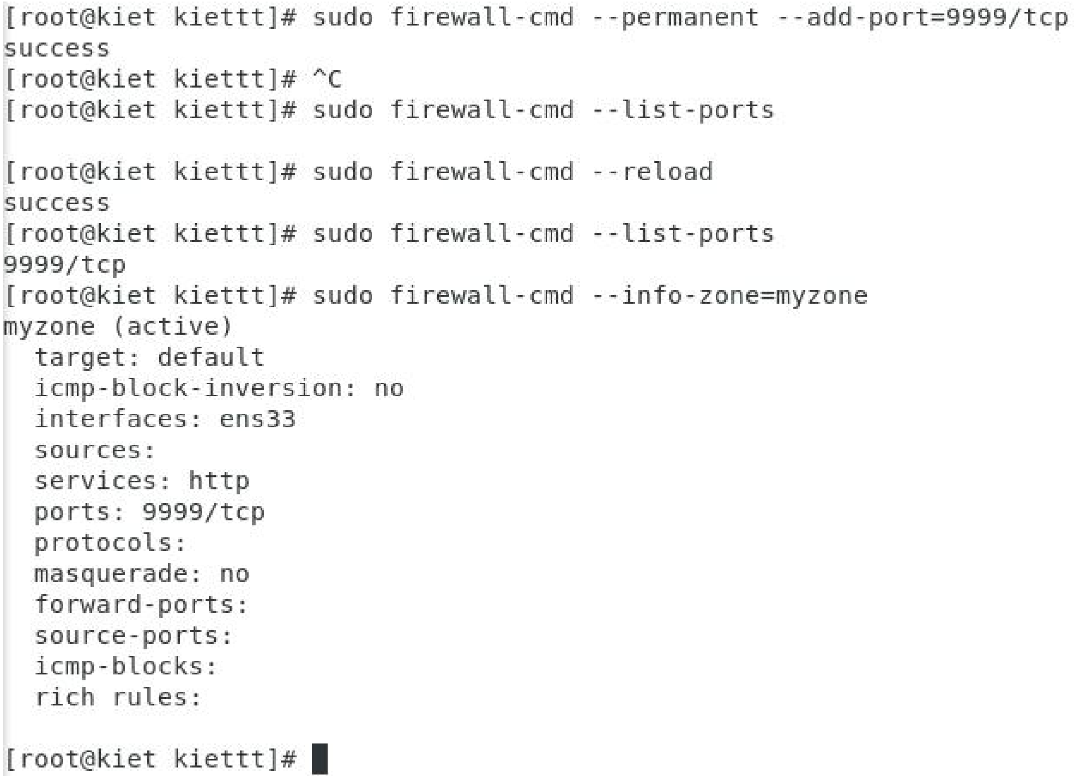
```
[root@kiet kiettt]# sudo firewall-cmd --permanent --remove-service=https
success
```

5/ Reload the firewall configuration and review the zone information. Then look at the list of available services be allowed:



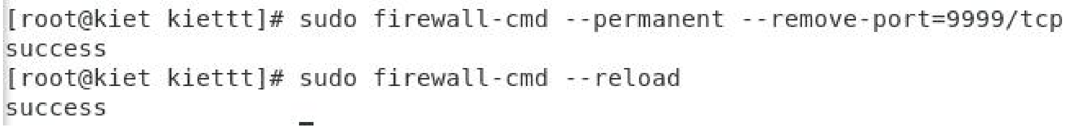
```
[root@kiet kiettt]# sudo firewall-cmd --reload
success
[root@kiet kiettt]# sudo firewall-cmd --info-zone=myzone
myzone (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: http
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[root@kiet kiettt]# sudo firewall-cmd --list-services
http
```

6/ let's set up the Port. Permanently open port 9999/tcp and see the results:



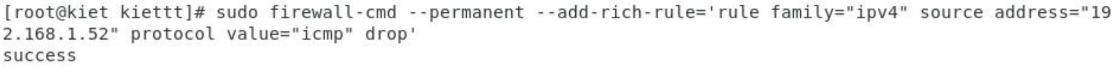
```
[root@kiet kiettt]# sudo firewall-cmd --permanent --add-port=9999/tcp
success
[root@kiet kiettt]# ^C
[root@kiet kiettt]# sudo firewall-cmd --list-ports

[root@kiet kiettt]# sudo firewall-cmd --reload
success
[root@kiet kiettt]# sudo firewall-cmd --list-ports
9999/tcp
[root@kiet kiettt]# sudo firewall-cmd --info-zone=myzone
myzone (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: http
  ports: 9999/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[root@kiet kiettt]# 
```

7/Remove port 9999/tcp:



```
[root@kiet kiettt]# sudo firewall-cmd --permanent --remove-port=9999/tcp
success
[root@kiet kiettt]# sudo firewall-cmd --reload
success
```

8/Add rich language rules to block geographical ranges of IPv4 addresses.



```
[root@kiet kiettt]# sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="19
2.168.1.52" protocol value="icmp" drop'
success
```

9// Delete zone.

```
[root@kiet kiettt]# sudo firewall-cmd --permanent --delete-zone=myzone
success
[root@kiet kiettt]# sudo firewall-cmd --reload
success
[root@kiet kiettt]# sudo 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:
```