Firewalld (CentOS 7)

This lab gives the most common actions you can perform with firewall-cmd.

1. Check if firewalld is running. If not, then start it and enable it.

```
[root@centos11 ~]# firewall-cmd --state
not running
[root@centos11 ~]# systemctl start firewalld
[root@centos11 ~]# systemctl enable firewalld
Created symlink from
/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service to
/usr/lib/systemd/system/firewalld.service.
Created symlink from
/etc/systemd/system/basic.target.wants/firewalld.service to
/usr/lib/systemd/system/firewalld.service.
```

2. What is the default zone

```
[root@centos11 ~]# firewall-cmd --get-default-zone
public
```

3. List which zones are connected to which interfaces

```
[root@centos11 ~]# firewall-cmd --get-active-zones
public
  interfaces: ens33
```

4. List the service settings for the default zone.

```
[root@centos11 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
```

```
  icmp-blocks:
  rich rules:
```

5. List all available zones

```
[root@centos11 ~]# firewall-cmd --get-zones
work drop internal external trusted home dmz public block
```

6. What are the service settings of the *home* zone?

```
[root@centos11 ~]# firewall-cmd --zone=home --list-all
home
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client mdns samba-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:
```

7. List the service settings of all zones

```
[root@centos11 ~]# firewall-cmd --list-all-zones | less
```

8. List all available services

```
[root@centos11 ~]# firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client
ceph ceph-mon dhcp dhcpv6 dhcpv6-client dns docker-registry
dropbox-lansync freeipa-ldap freeipa-ldaps freeipa-replication ftp
high-availability http https imap imaps ipp ipp-client ipsec
iscsi-target kadmin kerberos kpasswd ldap ldaps libvirt libvirt-tls
mdns mosh mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy pmwebapi
pmwebapis pop3 pop3s postgresql privoxy proxy-dhcp ptp pulseaudio
puppetmaster radius rpc-bind rsyncd samba samba-client sane smtp
smtps snmp snmptrap squid ssh synergy syslog syslog-tls telnet tftp
tftp-client tinc tor-socks transmission-client vdsm vnc-server
wbem-https xmpp-bosh xmpp-client xmpp-local xmpp-server
```

9. Add the nfs service to the public zone. This will add nfs to /etc/firewalld/zones/public.xml

```
[root@centos11 ~]# firewall-cmd --zone=public --add-service=nfs
success
[root@centos11 ~]# firewall-cmd --zone=public --list-services
dhcpv6-client ssh nfs
```

10. Make the service permanent. This will add nfs to */etc/firewalld/zones/public.xml*

```
[root@centos11 ~]# firewall-cmd --zone=public --permanent \
--add-service=http
success
[root@centos11 ~]# firewall-cmd --zone=public --permanent \
--list-services
dhcpv6-client http ssh
```

11. Add port 3011/tcp to the public zone and make it permanent.

```
[root@centos11 ~]# firewall-cmd --zone=public --add-port=3011/tcp
success
[root@centos11 ~]# firewall-cmd --zone=public --permanent \
--add-port=3011/tcp
success
```

12. Create a new service by copying an existing one to */etc/firewalld/services/*

```
[root@centos11 ~]# cp /usr/lib/firewalld/services/ftp.xml
/etc/firewalld/services/ftp_new.xml
[root@centos11 ~]#
```

13. Change the ftp port from 21 rto 7021

```
[root@centos11 ~]# cat /etc/firewalld/services/ftp_new.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>FTP</short>
  <description>FTP is a protocol used for remote file transfer. If
you plan to make your FTP server publicly available, enable this
option. You need the vsftpd package installed for this option to be
useful.</description>
  <port protocol="tcp" port="7021"/>
  <module name="nf_conntrack_ftp"/>
```

```
</service>
```

14. Reload the firewall configuration

```
[root@centos11 ~]# firewall-cmd --reload
success
[root@centos11 ~]# firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client
ceph ceph-mon dhcp dhcpv6 dhcpv6-client dns docker-registry
dropbox-lansync freeipa-ldap freeipa-ldaps freeipa-replication ftp
ftp_new high-availability http https imap imaps ipp ipp-client ipsec
iscsi-target kadmin kerberos kpasswd ldap ldaps libvirt libvirt-tls
mdns mosh mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy pmwebapi
pmwebapis pop3 pop3s postgresql privoxy proxy-dhcp ptp pulseaudio
puppetmaster radius rpc-bind rsyncd samba samba-client sane smtp
smtps snmp snmptrap squid ssh synergy syslog syslog-tls telnet tftp
tftp-client tinc tor-socks transmission-client vdsm vnc-server
wbem-https xmpp-bosh xmpp-client xmpp-local xmpp-server
```

15. Create a new zone called publictest

```
[root@centos11 ~]# firewall-cmd --permanent --new-zone=publictest
success
[root@centos11 ~]# firewall-cmd --reload
success
[root@centos11 ~]# firewall-cmd --get-zones
work drop internal external trusted publictest home dmz public block
```

16. Manually add the ssh service to the publictest xml file and reload

```
[root@centos11 zones]# cat publictest.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
<service name="ssh"/>
</zone>
[root@centos11 zones]# firewall-cmd --reload
success
```

17. Connect the new zone to ens34

```
[root@centos11 ~]# firewall-cmd --zone=publictest \
--change-interface=ens34
success
```

18. Check the interface configuration file for the new zone

```
[root@centos11 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ens34
TYPE=Ethernet
(snipped)
DEVICE=ens34
ONBOOT=no
ZONE=publictest
```

19. Restart the relevant services

```
[root@centos11 ~]# sudo systemctl restart network
[root@centos11 ~]# sudo systemctl restart firewalld
```