

Firewall Configuration

Configuring The Firewall

Start and enable the firewall

1. To start and enable the firewall use the commands below

```
systemctl start firewalld  
systemctl enable firewalld
```

Get an overview

Default Zone

1. Find the default zone. The default zone is usually public

```
firewall-cmd --get-default-zone
```

```
root@aza2-jhb-azandi /home/aza_admin # firewall-cmd --get-default-zone  
public  
root@aza2-jhb-azandi /home/aza_admin # █
```

Display Allowed Services

1. Display the allowed services of the zone

```
firewall-cmd --list-service --zone=external
```

By default, "public" zone is applied with a NIC and dhcpv6-client and ssh are allowed.

```
root@aza2-jhb-azandi /home/aza_admin # firewall-cmd --list-service --zone=public  
dhcpv6-client http https ssh  
root@aza2-jhb-azandi /home/aza_admin # █
```

Display Services Defined By Default

1. To list all service defined by default use the command below

```
firewall-cmd --get-services
```

It should give you an output similar to

```
[root@dlp ~]# firewall-cmd --get-services
amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns ftp high-availability http https imaps ipp
ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql nfs ntp openvpn
pmcd pmproxy pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba samba-client smtp ssh
telnet tftp tftp-client transmission-client vnc-server wbem-https
```

Add/Remove services

1. Add or Remove allowed services. The change will be back after rebooting the system. If you change settings permanently, add the "--permanent" option.

```
# for example, add http (the change will be valid at once)
[root@dlp ~]# firewall-cmd --add-service=http
success
[root@dlp ~]# firewall-cmd --list-service
dhcpv6-client http ssh

# for example, remove http
[root@dlp ~]# firewall-cmd --remove-service=http
success
[root@dlp ~]# firewall-cmd --list-service
dhcpv6-client ssh

# for example, add http permanently. (this permanent case, it's necessary to reload the FirewallD to enable
the change)
[root@dlp ~]# firewall-cmd --add-service=http --permanent
success
[root@dlp ~]# firewall-cmd --reload
success
[root@dlp ~]# firewall-cmd --list-service
dhcpv6-client http ssh
```

Add/Remove Ports

1. Add or remove allowed ports

```
# for example, add TCP 465
[root@dlp ~]# firewall-cmd --add-port=465/tcp
success
[root@dlp ~]# firewall-cmd --list-port
465/tcp

# for example, remove TCP 465
[root@dlp ~]# firewall-cmd --remove-port=465/tcp
success
[root@dlp ~]# firewall-cmd --list-port

# for example, add TCP 465 permanently
[root@dlp ~]# firewall-cmd --add-port=465/tcp --permanent
success
[root@dlp ~]# firewall-cmd --reload
success
[root@dlp ~]# firewall-cmd --list-port
465/tcp
```

Add/Remove Prohibited ICMP Types

1. Add or remove prohibited ICMP types

```
# for example, add echo-request to prohibit it
[root@dlp ~]# firewall-cmd --add-icmp-block=echo-request
success
[root@dlp ~]# firewall-cmd --list-icmp-blocks
echo-request

# for example, remove echo-request
[root@dlp ~]# firewall-cmd --remove-icmp-block=echo-request
success
[root@dlp ~]# firewall-cmd --list-icmp-blocks

# display ICMP types
[root@dlp ~]# firewall-cmd --get-icmpatypes
destination-unreachable echo-reply echo-request parameter-problem redirect
router-advertisement router-solicitation source-quench time-exceeded
```

Revision #1

Created 15 April 2020 01:17:59 by Admin

Updated 15 April 2020 02:03:26 by Admin