The Nautilus system admins team recently deployed a web UI application for their backup utility running on the Nautilus backup server in Stratos Datacenter. The application is running on port 8082. They have firewalld installed on that server. The requirements that have come up include the following:

Open all incoming connection on 8082/tcp port. Zone should be public.

thor@jump\_host ~$ ssh clint@stbkp01

[clint@stbkp01 ~]$ sudo su

1. You can see the list . Here ports are blank. Ports:

[root@stbkp01 clint]# firewall-cmd --zone=public --list-all

public

target: default

icmp-block-inversion: no

interfaces:

sources:

services: dhcpv6-client ssh

ports:

protocols:

masquerade: no

forward-ports:

source-ports:

icmp-blocks:

rich rules:

2.

Check the port , zone and protocol according to you task and add it using the command below

[root@stbkp01 clint]# firewall-cmd --permanent --zone=public --add-port=8082/tcp

Success

3.

Reload the firewalld rules and restart the firewalld services to apply the changes.

[root@stbkp01 clint]# firewall-cmd --reload

Success

4. now restart the service.

[root@stbkp01 clint]# systemctl restart firewalld

5. Before submitting ensure to check the rules are correctly implemented and visible in the table.

[root@stbkp01 clint]# firewall-cmd --zone=public --list-all

public

target: default

icmp-block-inversion: no

interfaces:

sources:

services: dhcpv6-client ssh

ports: 8082/tcp

protocols:

masquerade: no

forward-ports:

source-ports:

icmp-blocks:

rich rules: