How to Open And Close a Port on RockyLinux Server?

written by sysadmin | 18 January 2025

By default, the RockyLinux/AlmaLinux/CentOS distro provides two firewalls, iptables and firewalld. This article will explain how to open and close a port using Firewalld on the distro. If you have opened and closed a port using Firewalld, you don't need to open and close a port in iptables.

Problem

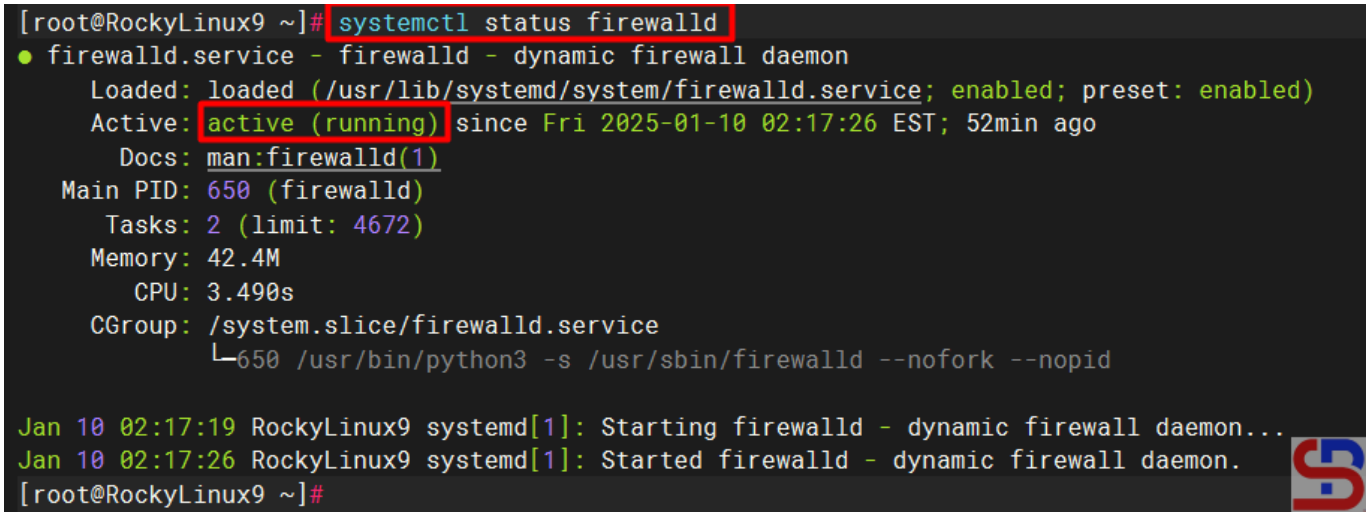
How to open and close a port on the RockyLinux server?

Solution

A. Check the Firewalld status

By default, the Firewalld package is installed automatically using the command:

```
systemctl status firewalld
```



Check the status of Firewalld

From the picture above, you can see that the firewall on the

server is already running. If the Firewalld is not already running, use the command below:

```
systemctl enable --now firewalld
```

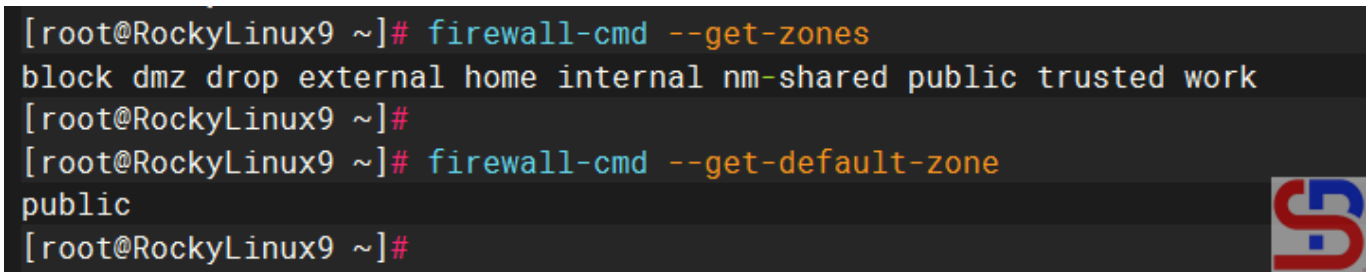
But if on your server there is no firewall package, you can install it using the command below:

```
yum install -y firewalld
```

B. Check the zones

Firewalld uses zones and services, compared to iptables, which use chains and rules. Zones are a collection of rules that have been set for what network connections should be permitted based on the level of confidence in the network connected to the system. We can determine the name of the network interface and the network source into zones. To see the zones in firewalld and which zone is the default, use the command below:

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



Show all zones in Firewalld

From the picture above, there are 9 zones, and the explanation can be seen in the picture below, which is sorted from the most trusted

Zone Name	Description
Trusted	This zone accepts all the incoming traffic. You can use this zone to manage the traffic on a trusted network because it will not filter anything.
Home	This zone is designed for only the home network. It permits only selected incoming traffic and reject all.
Work	This zone designed for only the work (corporate) networking. It permits only selected incoming traffic and reject all.
Internal	This zone intended to design for the internal network. It permits only what is allowed and rejects all.
Public	This zone rejects all the incoming traffic, except what is granted. Using with the default zone, we can add any newly network interfaces on it. It is designed to use only the public places.
External	This zone designed for outgoing traffic forwarded with masquerading is enabled. Also, we can use this for NAT
Dmz	This zone designed to use the demilitarized zone with limited public access. It permits only selected incoming traffic and reject all.
Block	This zone designed to reject all incoming traffic with an ICMP-host-prohibited message is returned. It permits only outgoing traffic.
Drop	This zone designed to drop all incoming traffic with no notification like ICMP errors. It is purely used in high secure places.

The zones in Firewalld (Image credit for linuxteck.com)

To view all settings for all zones, use the following command:

```
firewall-cmd --list-all-zones
```

```
[root@RockyLinux9 ~]# firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

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

View all the settings in Firewalld

But, if you want to view all settings in a specific zone, for example, a public zone, use the following command:

```
firewall-cmd --zone=public --list-ports
```

C. Open the Port

Now, if you want to open port 43210 with TCP protocol, use the command below:

```
firewall-cmd --add-port=43210/tcp --permanent
firewall-cmd --reload
```

```
[root@RockyLinux9 ~]# firewall-cmd --add-port=43210/tcp --permanent
success
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# firewall-cmd --reload
success
[root@RockyLinux9 ~]#
```

Open the port

Use the command below to see the ports that have been opened:

```
firewall-cmd --list-ports
```

```
[root@RockyLinux9 ~]# firewall-cmd --list-ports
43210/tcp
[root@RockyLinux9 ~]#
```

List all opened ports

D. Open the port from a certain IP

If you want to open a port from a certain IP, for example, you only allow IP 192.168.56.100 to access port 22 on this server, then use the command below:

```
firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source
address=192.168.56.100 port port=22 protocol=tcp accept'
firewall-cmd --reload
firewall-cmd --list-rich-rules
```

```
[root@RockyLinux9 ~]# sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="192.168.56.100" port port="22" protocol="tcp" accept'
success
[root@RockyLinux9 ~]# firewall-cmd --reload
success
[root@RockyLinux9 ~]# firewall-cmd --list-rich-rules
rule family="ipv4" source address="192.168.56.100" port port="22" protocol="tcp" accept
[root@RockyLinux9 ~]#
```

Allow the IP to a certain port

If you want to reject a host with IP 192.168.56.100 to access port 22, use the command below:

```
sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source
address="192.168.56.100" port port="22" protocol="tcp" reject'
firewall-cmd --reload
```

```
firewall-cmd --list-rich-rules
```

```
[root@RockyLinux9 ~]# sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="192.168.56.100" port port="22" protocol="tcp" reject'
success
[root@RockyLinux9 ~]# firewall-cmd --reload
success
[root@RockyLinux9 ~]# firewall-cmd --list-rich-rules
rule family="ipv4" source address="192.168.56.100" port port="22" protocol="tcp" reject
[root@RockyLinux9 ~]#
```

Block the IP to a certain port

E. Close the port from a certain IP

If you want to close a port from a certain IP, for example, you block a host with IP 192.168.56.100 from accessing port 22 on this server, then use the command below:

```
sudo firewall-cmd --permanent --remove-rich-rule='rule family="ipv4" source address="192.168.56.100" port port="22" protocol="tcp" accept'
firewall-cmd --reload
firewall-cmd --list-rich-rules
```

```
[root@RockyLinux9 ~]# firewall-cmd --list-rich-rules
rule family="ipv4" source address="192.168.56.100" port port="22" protocol="tcp" accept
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# sudo firewall-cmd --permanent --remove-rich-rule='rule family="ipv4" source address="192.168.56.100" port port="22" protocol="tcp" accept'
success
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# firewall-cmd --reload
success
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# firewall-cmd --list-rich-rules

[root@RockyLinux9 ~]#
```

Remove the IP to a certain port

INFO

In short, if you want to delete the rich rule, then change the option –add-rich-rule to **–remove-rich-rule**.

F. Close the port

Use the command below to close the newly opened port 43210:

```
firewall-cmd --remove-port=43210/tcp --permanent
firewall-cmd --reload
```

```
[root@RockyLinux9 ~]# firewall-cmd --list-ports
43210/tcp
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# firewall-cmd --remove-port=43210/tcp --permanent
success
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# firewall-cmd --reload
success
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# firewall-cmd --list-ports

[root@RockyLinux9 ~]#
```

Close the port in Firewalld

G. Open the service

Apart from using ports, Firewalld can also open and close services on the server. To see the services that have been opened, type the command below:

```
firewall-cmd --list-services
```

```
[root@RockyLinux9 ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
[root@RockyLinux9 ~]#
```

List all opened services

You can see in the picture above that the distro only opens 3 services. If you want to open the SMTP service, use the command below:

```
firewall-cmd --add-service=smtp --permanent
firewall-cmd --reload
```

```
[root@RockyLinux9 ~]# firewall-cmd --add-service=smtp --permanent
success
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# firewall-cmd --reload
success
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# firewall-cmd --list-services
cockpit dhcpv6-client smtp ssh
[root@RockyLinux9 ~]#
```

Add the service to the firewall

H. Close the service

To delete the SMTP service in Firewalld, use the command below:

```
firewall-cmd --remove-service=smtp --permanent
firewall-cmd --reload
```

Close the service in Firewalld

Note

If you use the OpenSUSE distro, you can use the above commands to open and close a port, like in the image below:

```
opensuse15:~ # systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-01-10 06:14:05 EST; 5min ago
       Docs: man:firewalld(1)
   Main PID: 833 (firewalld)
      Tasks: 2 (limit: 1125)
        CPU: 23.153s
     CGroup: /system.slice/firewalld.service
             └─833 /usr/bin/python3 /usr/sbin/firewalld --nofork --nopid

Jan 10 06:13:57 opensuse15 systemd[1]: Starting firewalld - dynamic firewall daemon...
Jan 10 06:14:05 opensuse15 systemd[1]: Started firewalld - dynamic firewall daemon.
opensuse15:~ #
opensuse15:~ # firewall-cmd --add-port=43210/tcp --permanent
success
opensuse15:~ #
opensuse15:~ # firewall-cmd --reload
success
opensuse15:~ #
opensuse15:~ # firewall-cmd --list-ports
43210/tcp
opensuse15:~ #
opensuse15:~ # firewall-cmd --remove-port=43210/tcp --permanent
success
opensuse15:~ #
opensuse15:~ # firewall-cmd --reload
success
opensuse15:~ #
opensuse15:~ # firewall-cmd --list-ports

opensuse15:~ #
```

The Firewalld commands in OpenSUSE

References

redhat.com
greenwebpage.com
inmotionhosting.com
baeldung.com
musaamin.web.id