How to open a port in the firewall on CentOS or RHEL

Author : Dan Nanni

Categories : CentOS, Networking, Security

Tagged as : firewalldiptables

Question: I am running a web/file server on my CentOS box, and to access the server remotely, I need to modify a firewall to allow access to a TCP port on the box. What is a proper way to open a TCP/UDP port in the firewall of CentOS/RHEL?

Out of the box, enterprise Linux distributions such as CentOS or RHEL come with a powerful firewall built-in, and their default firewall rules are pretty restrictive. Thus if you install any custom services (e.g., web server, NFS, Samba), chances are their traffic will be blocked by the firewall rules. You need to open up necessary ports on the firewall to allow their traffic.

On CentOS/RHEL 6 or earlier, the `iptables` service allows users to interact with netfilter kernel modules to configure firewall rules in the user space. Starting with CentOS/RHEL 7, however, a new userland interface called `firewalld` has been introduced to replace `iptables` service.

To check the current firewall rules, use this command:

```
$ sudo iptables -L
```

Now let's see how we can update the firewall to open a port on CentOS/RHEL.

Open a Port on CentOS/RHEL 7

Starting with CentOS and RHEL 7, firewall rule settings are managed by `firewalld` service daemon. A command-line client called `firewall-cmd` can talk to this daemon to update firewall rules permanently.

To open up a new port (e.g., TCP/80) permanently, use these commands.

```
$ sudo firewall-cmd --zone=public --add-port=80/tcp --permanent
$ sudo firewall-cmd --reload
```

Without "--permanent" flag, the firewall rule would not persist across reboots.

Check the updated rules with:

```
$ firewall-cmd --list-all
```

Open a Port on CentOS/RHEL 6

On CentOS/RHEL 6 or earlier, the `iptables` service is responsible for maintaining firewall rules.

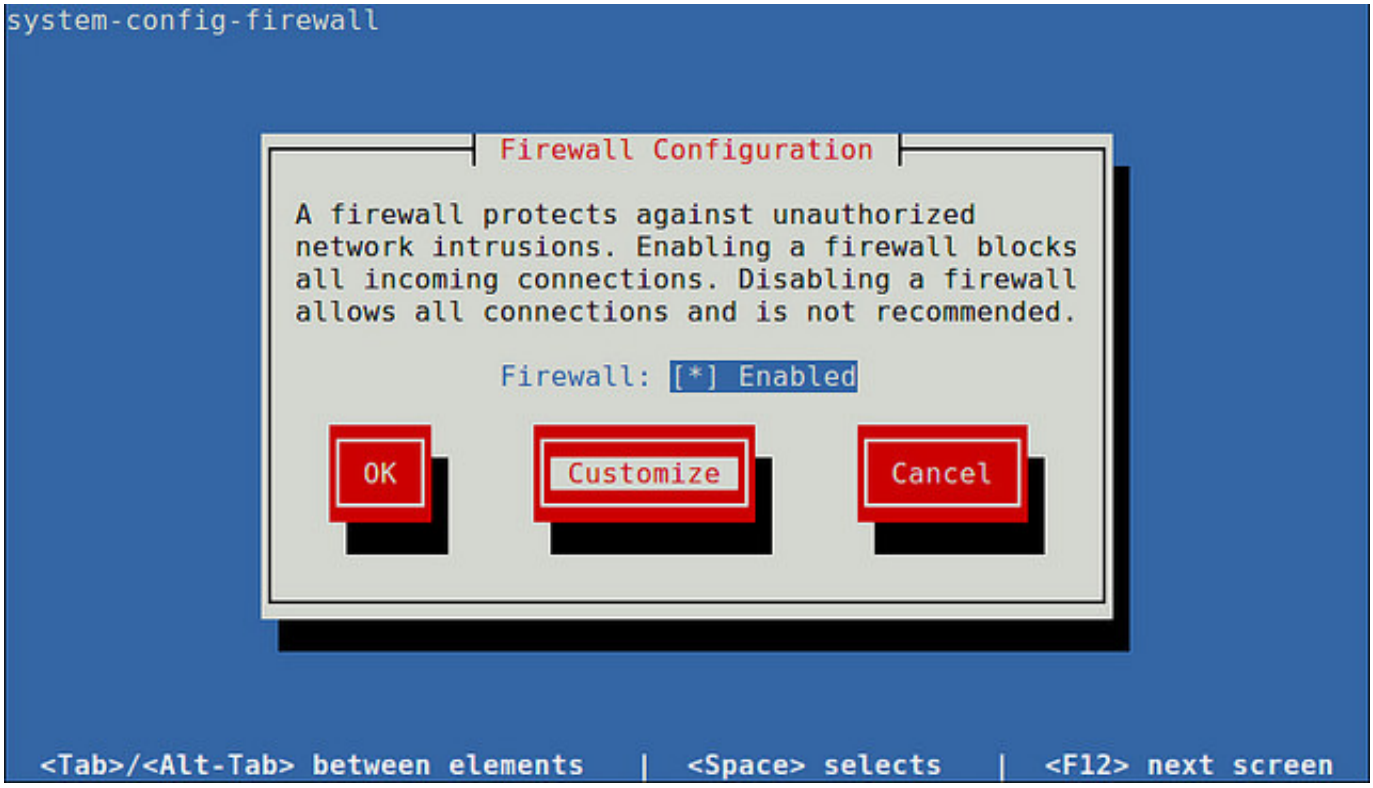
Use `iptables` command to open up a new TCP/UDP port in the firewall. To save the updated rule permanently, you need the second command.

```
$ sudo iptables -I INPUT -p tcp -m tcp --dport 80 -j ACCEPT
$ sudo service iptables save
```

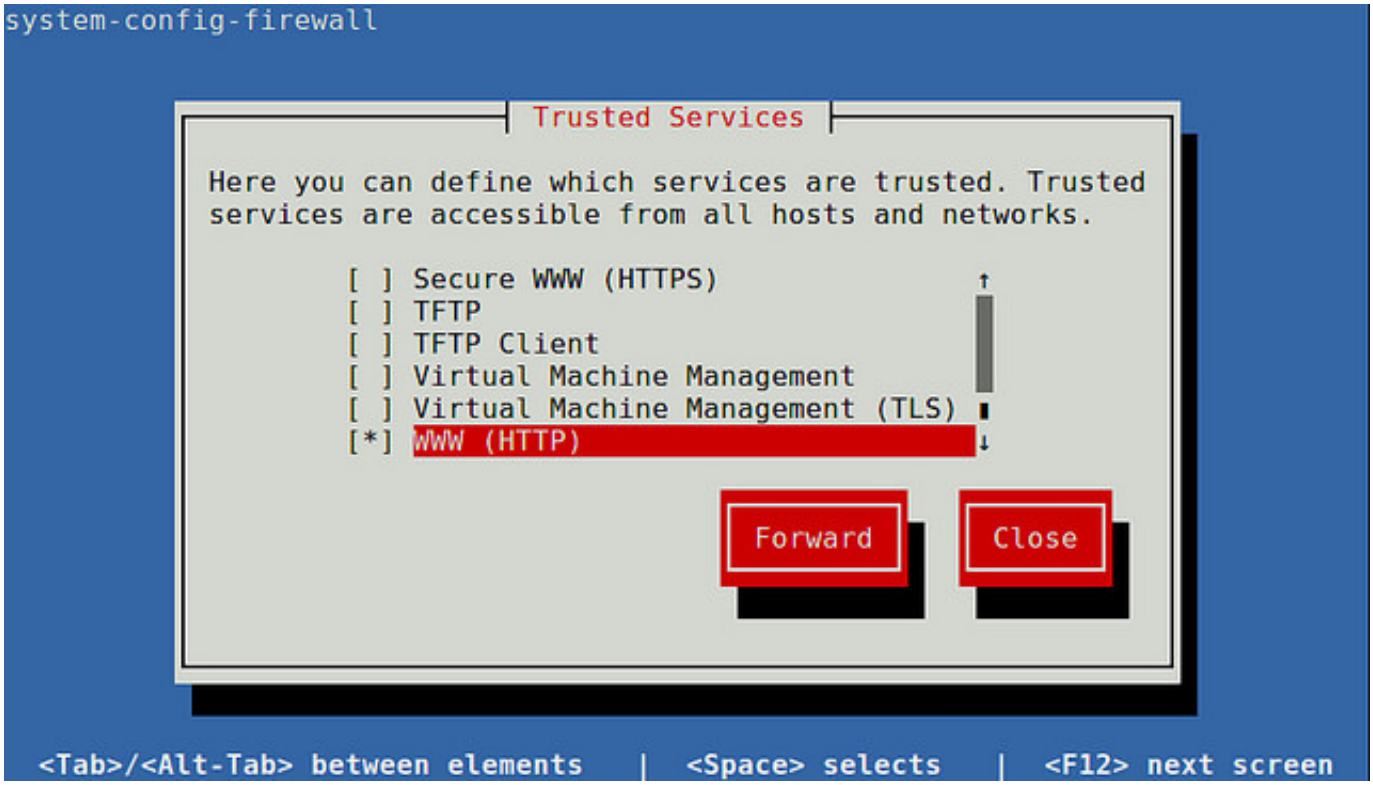
Another way to open up a port on CentOS/RHEL 6 is to use a terminal-user interface (TUI) firewall client, named `system-config-firewall-tui`.

```
$ sudo system-config-firewall-tui
```

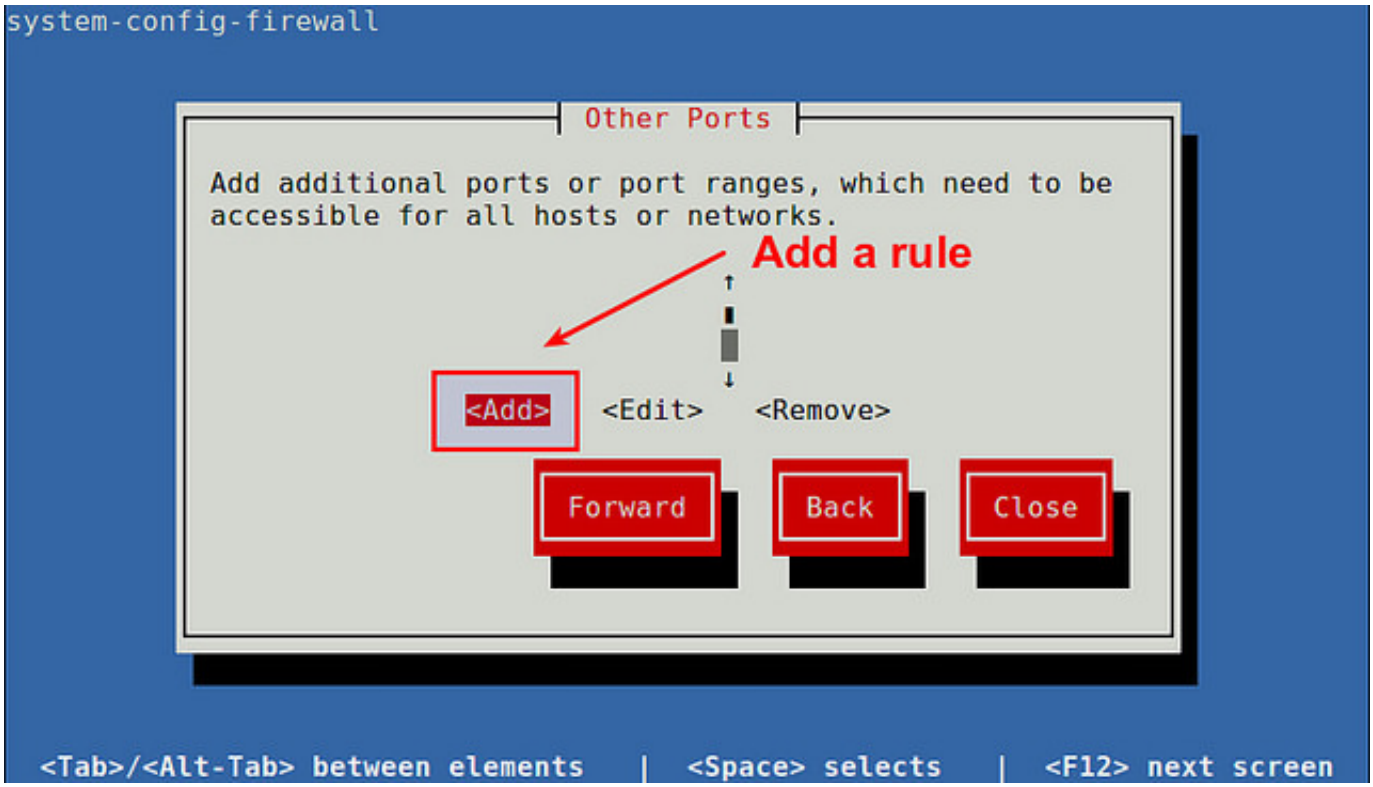
Choose "Customize" button in the middle and press ENTER.



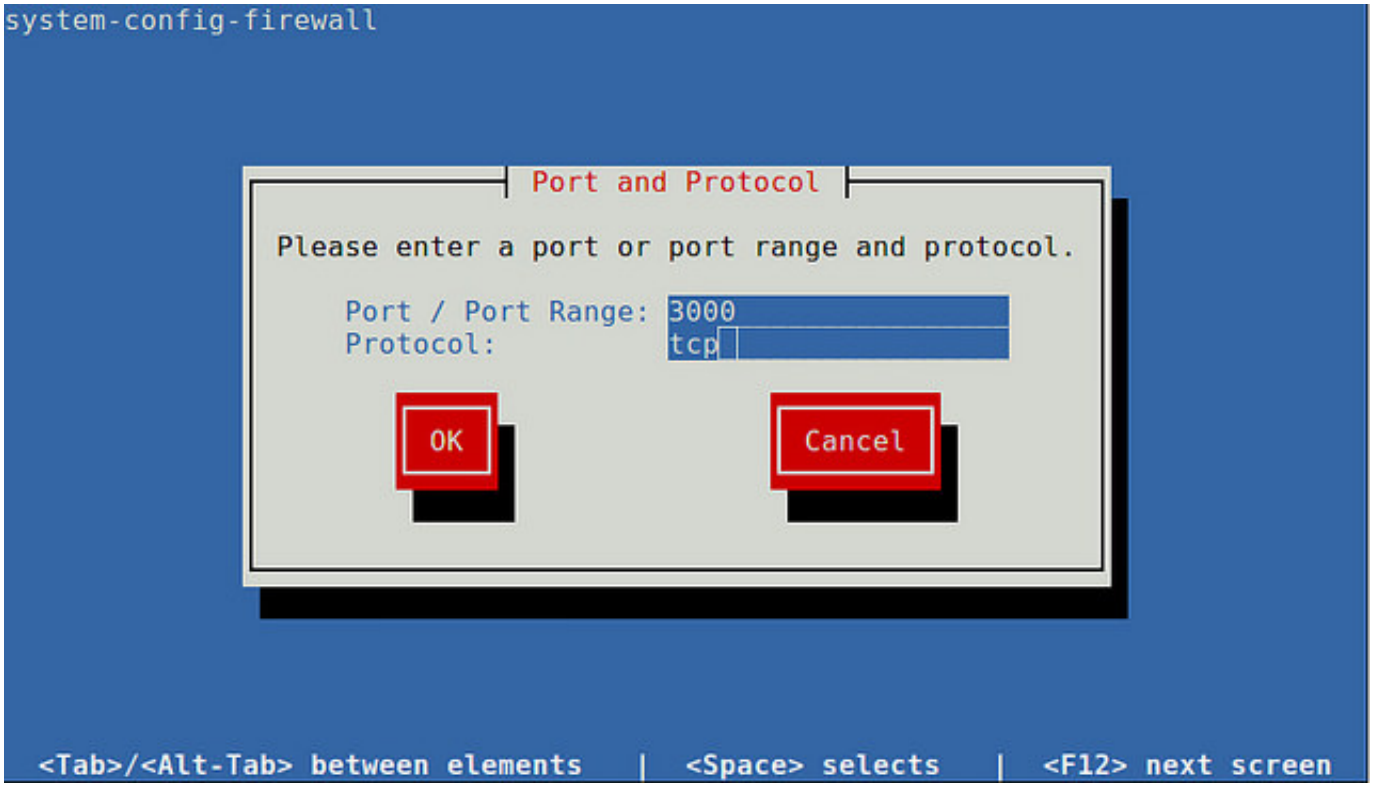
If you are trying to update the firewall for any well-known service (e.g., web server), you can easily enable the firewall for the service here, and close the tool. If you are trying to open up any arbitrary TCP/UDP port, choose "Forward" button and go to a next window.



Add a new rule by choosing "Add" button.



Specify a port (e.g., 80) or port range (e.g., 3000-3030), and protocol (e.g., tcp or udp).



Finally, save the updated configuration, and close the tool. At this point, the firewall will be saved permanently.