Control the firewall at the command line - Fedora Magazine

A network *firewall* is more or less what it sounds like: a protective barrier that prevents unwanted network transmissions. They are most frequently used to prevent outsiders from contacting or using network services on a system. For instance, if you're running a laptop at school or in a coffee shop, you probably don't want strangers poking around on it.

Every Fedora system has a firewall built in. It's part of the network functions in the Linux kernel inside. This article shows you how to change its settings using *firewall-cmd*.

Network basics

This article can't teach you everything about computer networks. But a few basics suffice to get you started.

Any computer on a network has an *IP address*. Think of this just like a mailing address that allows correct routing of data. Each computer also has a set of *ports*, numbered 0-65535. These are not physical ports; instead, you can think of them as a set of connection points at the address.

In many cases, the port is a standard number or range depending on the application expected to answer. For instance, a web server typically reserves port 80 for non-secure HTTP communications, and/or 443 for secure HTTPS. The port numbers under 1024 are reserved for system and well-known purposes, ports 1024-49151 are registered, and ports 49152 and above are usually ephemeral (used only for a short time).

Each of the two most common protocols for Internet data transfer, TCP and UDP, have this set of ports. TCP is used when it's important that all data be received and, if it arrives out of order, reassembled in the right order. UDP is used for more time-sensitive services that can withstand losing some data.

An application running on the system, such as a web server, reserves one or more ports (as seen above, 80 and 443 for example). Then during network communication, a host establishes a connection between a source address and port, and the destination address and port.

A network firewall can block or permit transmissions of network data based on rules like address, port, or other criteria. The *firewall-cmd* utility lets you interact with the rule set to view or change how the firewall works.

Firewall zones

To verify the firewall is running, use this command with sudo. (In fairness, you can run *firewall-cmd* without the *sudo* command in environments where PolicyKit is running.)

```
$ sudo firewall-cmd --state
running
```

The firewalld service supports any number of *zones*. Each zone can have its own settings and rules for protection. In addition, each network interface can be placed in any zone individually The default zone for an external facing interface (like the wifi or wired network card) on a Fedora Workstation is the *FedoraWorkstation* zone.

To see what zones are active, use the *––get-active-zones* flag. On this system, there are two network interfaces, a wired Ethernet card *wlp2s0* and a virtualization (libvirt) bridge interface *virbr0*:

```
$ sudo firewall-cmd --get-active-zones
FedoraWorkstation
  interfaces: wlp2s0
libvirt
  interfaces: virbr0
```

To see the default zone, or all the defined zones:

```
$ sudo firewall-cmd --get-default-zone
FedoraWorkstation
$ sudo firewall-cmd --get-zones
FedoraServer FedoraWorkstation block dmz drop external home internal libvirt public trusted work
```

To see the services the firewall is allowing other systems to access in the default zone, use the *––list-services* flag. Here is an example from a customized system; you may see something different.

```
$ sudo firewall-cmd --list-services
dhcpv6-client mdns samba-client ssh
```

This system has four services exposed. Each of these has a well-known port number. The firewall recognizes them by name. For instance, the *ssh* service is associated with port 22.

To see other port settings for the firewall in the current zone, use the *––list-ports* flag. By the way, you can always declare the zone you want to check:

```
$ sudo firewall-cmd --list-ports --zone=FedoraWorkstation
1025-65535/udp 1025-65535/tcp
```

This shows that ports 1025 and above (both UDP and TCP) are open by default.

Changing zones, ports, and services

The above setting is a design decision.* It ensures novice users can use network facing applications they install. If you know what you're doing and want a more protective default, you can move the interface to the *FedoraServer* zone, which prohibits any ports not explicitly allowed. *(**Warning:** if you're using the host via the network, you may break your connection — meaning you'll have to go to that box physically to make further changes!)*

```
$ sudo firewall-cmd --change-interface=<ifname> --zone=FedoraServer
success
```

** This article is not the place to discuss that decision, which went through many rounds of review and debate in the Fedora community. You are welcome to change settings as needed.*

If you want to open a well-known port that belongs to a service, you can add that service to the default zone (or use *––zone* to adjust a different zone). You can add more than one at once. This example opens up the well-known ports for your web server for both HTTP and HTTPS traffic, on ports 80 and 443:

```
$ sudo firewall-cmd --add-service=http --add-service=https
success
```

Not all services are defined, but many are. To see the whole list, use the *––get-services* flag.

If you want to add specific ports, you can do that by number and protocol as well. (You can also combine *––add-service* and *––add-port* flags, as many as necessary.) This example opens up the UDP service for a network boot service:

```
$ sudo firewall-cmd --add-port=67/udp
success
```

Important: If you want your changes to be effective after you reboot your system or restart the firewalld service, you **must** add the *––permanent* flag to your commands. The examples here only change the firewall until one of those events next happens.

These are just some of the many functions of the *firewall-cmd* utility and the firewalld service. There is much more information on firewalld at the project's home page that's worth reading and trying out.

Photo by Jakob Braun on Unsplash.

Paul W. Frields

Paul W. Frields has been a Linux user and enthusiast since 1997, and joined the Fedora Project in 2003, shortly after launch. He was a founding member of the Fedora Project Board, and has worked on docsc, websites, advocacy, toolchain, and package maintenance. He joined Red Hat as Fedora Project Leader from February 2008 to July 2010, and remains with Red Hat as an engineering manager. He currently lives with his wife and two children in Virginia where he also runs a recording studio (5thdom.com).