How To Setup a Firewall with UFW on an Ubuntu and Debian Cloud Server

What is UFW?

UFW, or Uncomplicated Firewall, is a front-end to iptables. Its main goal is to make managing your firewall drop-dead simple and to provide an easy-to-use interface. It’s well-supported and popular in the Linux community—even installed by default in a lot of distros. As such, it’s a great way to get started securing your sever.

Before We Get Started

First, obviously, you want to make sure UFW is installed. It should be installed by default in Ubuntu, but if for some reason it’s not, you can install the package using aptitude or apt-get using the following commands:

```
sudo aptitude install ufw
```

or

```
sudo apt-get install ufw
```

Check the Status

You can check the status of UFW by typing:

```
sudo ufw status
```

Right now, it will probably tell you it is inactive. Whenever ufw is active, you’ll get a listing of the current rules that looks similar to this:

Status: active

To Action From

-- ------ ----

22 ALLOW Anywhere

Using IPv6 with UFW

If your VPS is configured for IPv6, ensure that UFW is configured to support IPv6 so that will configure both your IPv4 and IPv6 firewall rules. To do this, open the UFW configuration with this command:

```
sudo vi /etc/default/ufw
```

Then make sure "IPV6" is set to "yes", like so:

```
IPV6=yes
```

Save and quit. Then restart your firewall with the following commands:

```
sudo ufw disable
```

```
sudo ufw enable
```

Now UFW will configure the firewall for both IPv4 and IPv6, when appropriate.

Set Up Defaults

One of the things that will make setting up any firewall easier is to define some default rules for allowing and denying connections. UFW’s defaults are to deny all incoming connections and allow all outgoing connections. This means anyone trying to reach your cloud server would not be able to connect, while any application within the server would be able to reach the outside world. To set the defaults used by UFW, you would use the following commands:

```
sudo ufw default deny incoming
```

and

```
sudo ufw default allow outgoing
```

Note: if you want to be a little bit more restrictive, you can also deny all outgoing requests as well. The necessity of this is debatable, but if you have a public-facing cloud server, it could help prevent against any kind of remote shell connections. It does make your firewall more cumbersome to manage because you'll have to set up rules for all outgoing connections as well. You can set this as the default with the following:

```
sudo ufw default deny outgoing
```

Allow Connections

The syntax is pretty simple. You change the firewall rules by issuing commands in the terminal. If we turned on our firewall now, it would deny all incoming connections. If you're connected over SSH to your cloud server, that would be a problem because you would be locked out of your server. Let's enable SSH connections to our server to prevent that from happening:

```
sudo ufw allow ssh
```

As you can see, the syntax for adding services is pretty simple. UFW comes with some defaults for common uses. Our SSH command above is one example. It's basically just shorthand for:

```
sudo ufw allow 22/tcp
```

This command allows a connection on port 22 using the TCP protocol. If our SSH server is running on port 2222, we could enable connections with the following command:

```
sudo ufw allow 2222/tcp
```

Other Connections We Might Need

Now is a good time to allow some other connections we might need. If we're securing a web server with FTP access, we might need these commands:

```
sudo ufw allow www
```

```
sudo ufw allow 80/tcp
```

```
sudo ufw allow ftp
```

```
sudo ufw allow 21/tcp
```

You mileage will vary on what ports and services you need to open. There will probably be a bit of testing necessary. In addition, you want to make sure you leave your SSH connection allowed.

Port Ranges

You can also specify port ranges with UFW. To allow ports 1000 through 2000, use the command:

```
sudo ufw allow 1000:2000/tcp
```

If you want UDP:

```
sudo ufw allow 1000:2000/udp
```

IP Addresses

You can also specify IP addresses. For example, if I wanted to allow connections from a specific IP address (say my work or home address), I'd use this command:

```
sudo ufw allow from 192.168.255.255
```

Denying Connections

Our default set up is to deny all incoming connections. This makes the firewall rules easier to administer since we are only selectively allowing certain ports and IP addresses through. However, if you want to flip it and open up all your server's ports (not recommended), you could allow all connections and then restrictively deny ports you didn't want to give access to by replacing "allow" with "deny" in the commands above. For example:

```
sudo ufw allow 80/tcp
```

would allow access to port 80 while:

```
sudo ufw deny 80/tcp
```

would deny access to port 80.

Deleting Rules

There are two options to delete rules. The most straightforward one is to use the following syntax:

```
sudo ufw delete allow ssh
```

As you can see, we use the command “delete” and input the rules you want to eliminate after that. Other examples include:

```
sudo ufw delete allow 80/tcp
```

or

```
sudo ufw delete allow 1000:2000/tcp
```

This can get tricky when you have rules that are long and complex.

A simpler, two-step alternative is to type:

```
sudo ufw status numbered
```

which will have UFW list out all the current rules in a numbered list. Then, we issue the command:

```
sudo ufw delete [number]
```

where “[number]” is the line number from the previous command.

Turn It On

After we’ve gotten UFW to where we want it, we can turn it on using this command (remember: if you’re connecting via SSH, make sure you’ve set your SSH port, commonly port 22, to be allowed to receive connections):

```
sudo ufw enable
```

You should see the command prompt again if it all went well. You can check the status of your rules now by typing:

```
sudo ufw status
```

or

```
sudo ufw status verbose
```

for the most thorough display.

To turn UFW off, use the following command:

```
sudo ufw disable
```

Reset Everything

If, for whatever reason, you need to reset your cloud server’s rules to their default settings, you can do this by typing this command:

```
sudo ufw reset
```

Revision #1
Created 17 November 2020 18:53:32 by Dino Edwards
Updated 17 November 2020 19:00:59 by Dino Edwards