Subscribe

UFW Essentials: Common Firewall Rules and Commands

106

Posted August 20, 2015 608.3k FIREWALL SECURITY NETWORKING UBUNTU

By: Mitchell Anicas

Introduction

UFW is a firewall configuration tool for iptables that is included with Ubuntu by default. This cheat sheet-style guide provides a quick reference to UFW commands that will create iptables firewall rules are useful in common, everyday scenarios. This includes UFW examples of allowing and blocking various services by port, network interface, and source IP address.

How To Use This Guide

- If you are just getting started with using UFW to configure your firewall, check out our introduction to UFW
- Most of the rules that are described here assume that you are using the default UFW ruleset. That is, it is set to allow outgoing and deny incoming traffic, through the default policies, so you have to selectively allow traffic in
- Use whichever subsequent sections are applicable to what you are trying to achieve. Most sections are not predicated on any other, so you can use the examples below independently
- Use the Contents menu on the right side of this page (at wide page widths) or your browser's find function to locate the sections you need
- Copy and paste the command-line examples given, substituting the values in red with your own values

Remember that you can check your current UFW ruleset with `sudo ufw status` or `sudo ufw status verbose`.

Block an IP Address

To block all network connections that originate from a specific IP address, `15.15.15.51` for example, run this command:

```
$ sudo ufw deny from 15.15.15.51
```

In this example, `from 15.15.15.51` specifies a **source** IP address of "15.15.15.51". If you wish, a subnet, such as `15.15.15.0/24`, may be specified here instead. The source IP address can be specified in any firewall rule, including an **allow** rule.

Block Connections to a Network Interface

To block connections from a specific IP address, e.g. `15.15.15.51`, to a specific network interface, e.g. `eth0`, use this command:

```
$ sudo ufw deny in on eth0 from 15.15.15.51
```

This is the same as the previous example, with the addition of `in on eth0`. The network interface can be specified in any firewall rule, and is a great way to limit the rule to a particular network.

Service: SSH

If you're using a cloud server, you will probably want to allow incoming SSH connections (port 22) so you can connect to and manage your server. This section covers how to configure your firewall with various SSH-related rules.

Allow SSH

To allow all incoming SSH connections run this command:

```
$ sudo ufw allow ssh
```

An alternative syntax is to specify the port number of the SSH service:

```
$ sudo ufw allow 22
```

Allow Incoming SSH from Specific IP Address or Subnet

To allow incoming SSH connections from a specific IP address or subnet, specify the source. For example, if you want to allow the entire `15.15.15.0/24` subnet, run this command:

```
$ sudo ufw allow from 15.15.15.0/24  to any port 22
```

Allow Incoming Rsync from Specific IP Address or Subnet

Rsync, which runs on port 873, can be used to transfer files from one computer to another.

To allow incoming rsync connections from a specific IP address or subnet, specify the source IP address and the destination port. For example, if you want to allow the entire `15.15.15.0/24` subnet to be able to rsync to your server, run this command:

```
$ sudo ufw allow from 15.15.15.0/24 to any port 873
```

Service: Web Server

Web servers, such as Apache and Nginx, typically listen for requests on port 80 and 443 for HTTP and HTTPS connections, respectively. If your default policy for incoming traffic is set to drop or deny, you will want to create rules that will allow your server to respond to those requests.

Allow All Incoming HTTP

To allow all incoming HTTP (port 80) connections run this command:

```
$ sudo ufw allow http
```

An alternative syntax is to specify the port number of the HTTP service:

```
$ sudo ufw allow 80
```

Allow All Incoming HTTPS

To allow all incoming HTTPS (port 443) connections run this command:

```
$ sudo ufw allow https
```

An alternative syntax is to specify the port number of the HTTPS service:

```
$ sudo ufw allow 443
```

Allow All Incoming HTTP and HTTPS

If you want to allow both HTTP and HTTPS traffic, you can create a single rule that allows both ports. To allow all incoming HTTP and HTTPS (port 443) connections run this command:

```
$ sudo ufw allow proto tcp from any to any port 80,443
```

Note that you need to specify the protocol, with `proto tcp`, when specifying multiple ports.

Service: MySQL

MySQL listens for client connections on port 3306. If your MySQL database server is being used by a client on a remote server, you need to be sure to allow that traffic.

Allow MySQL from Specific IP Address or Subnet

To allow incoming MySQL connections from a specific IP address or subnet, specify the source. For example, if you want to allow the entire `15.15.15.0/24` subnet, run this command:

```
$ sudo ufw allow from 15.15.15.0/24 to any port 3306
```

Allow MySQL to Specific Network Interface

To allow MySQL connections to a specific network interface—say you have a private network interface `eth1`, for example—use this command:

```
$ sudo ufw allow in on eth1 to any port 3306
```

Service: PostgreSQL

PostgreSQL listens for client connections on port 5432. If your PostgreSQL database server is being used by a client on a remote server, you need to be sure to allow that traffic.

PostgreSQL from Specific IP Address or Subnet

To allow incoming PostgreSQL connections from a specific IP address or subnet, specify the source. For example, if you want to allow the entire `15.15.15.0/24` subnet, run this command:

```
$ sudo ufw allow from 15.15.15.0/24 to any port 5432
```

The second command, which allows the outgoing traffic of **established** PostgreSQL connections, is only necessary if the `OUTPUT` policy is not set to `ACCEPT`.

Allow PostgreSQL to Specific Network Interface

To allow PostgreSQL connections to a specific network interface—say you have a private network interface `eth1`, for example—use this command:

```
$ sudo ufw allow in on eth1 to any port 5432
```

The second command, which allows the outgoing traffic of **established** PostgreSQL connections, is only necessary if the `OUTPUT` policy is not set to `ACCEPT`.

Service: Mail

Mail servers, such as Sendmail and Postfix, listen on a variety of ports depending on the protocols being used for mail delivery. If you are running a mail server, determine which protocols you are using and allow the appropriate types of traffic. We will also show you how to create a rule to block outgoing SMTP mail.

Block Outgoing SMTP Mail

If your server shouldn't be sending outgoing mail, you may want to block that kind of traffic. To block outgoing SMTP mail, which uses port 25, run this command:

```
$ sudo ufw deny out 25
```

This configures your firewall to **drop** all outgoing traffic on port 25. If you need to reject a different service by its port number, instead of port 25, simply replace it.

Allow All Incoming SMTP

To allow your server to respond to SMTP connections, port 25, run this command:

```
$ sudo ufw allow 25
```

> **Note:** It is common for SMTP servers to use port 587 for outbound mail.

Allow All Incoming IMAP

To allow your server to respond to IMAP connections, port 143, run this command:

```
$ sudo ufw allow 143
```

Allow All Incoming IMAPS

To allow your server to respond to IMAPS connections, port 993, run this command:

```
$ sudo ufw allow 993
```

Allow All Incoming POP3

To allow your server to respond to POP3 connections, port 110, run this command:

```
$ sudo ufw allow 110
```

Allow All Incoming POP3S

To allow your server to respond to POP3S connections, port 995, run this command:

```
$ sudo ufw allow 995
```

Conclusion

That should cover many of the commands that are commonly used when using UFW to configure a firewall. Of course, UFW is a very flexible tool so feel free to mix and match the commands with different options to match your specific needs if they aren't covered here.

Good luck!

By: Mitchell Anicas

♡ Upvote (106) Subscribe

Related Tutorials

How To Migrate Iptables Firewall Rules to a New Server

How To Set Up a Firewall with UFW on Debian 9

How To Set Up a Firewall with UFW on Ubuntu 18.04

How To Secure Nginx with Let's Encrypt on FreeBSD

How to Block Unwanted SSH Login Attempts with PyFilter on Ubuntu 16.04

20 Comments

Leave a comment...

Log In to Comment

ktretyak *November 12, 2015*

0

```
sudo ufw deny in on eth0 from 15.15.15.51
```

Cool! But how to do it in CentOS?

ktretyak *November 12, 2015*

0 I found this

```
sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source addres
```

craiganderson *January 29, 2016*

0 Should the following command block web traffic as well? Meaning, prevent anyone accessing from this IP address from accessing any websites on the server?

```
sudo ufw deny from 15.15.15.51
```

manicas MOD *January 29, 2016*

0 Yes. That blocks all the network communication from that IP address. Web traffic is usually served on port 80 (HTTP) or 443 (HTTPS), if you want just block those ports specifically..

craiganderson *January 29, 2016*

0 Do I need to restart ufw after putting a rule in place? It doesn't seem like the rules I am adding are working. I just blocked my own IP address to test and I can still get on the site.

manicas MOD *February 1, 2016*

0 No, you just have to make sure they're in the correct order.

craiganderson *January 29, 2016*

0 These are my rules. Maybe 8, 9 and 10 are overriding 4, 5, 6 and 7?

```
[ 1] 22                         ALLOW IN    Anywhere
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 80                         ALLOW IN    Anywhere
[ 3] 443                        ALLOW IN    Anywhere
[ 4] Anywhere                   DENY IN     185.130.5.209
[ 5] Anywhere                   DENY IN     185.109.161.89
[ 6] Anywhere                   DENY IN     89.46.100.200
[ 7] Anywhere                   DENY IN     76.124.222.11
[ 8] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 9] 80 (v6)                    ALLOW IN    Anywhere (v6)
[10] 443 (v6)                   ALLOW IN    Anywhere (v6)
```

manicas MOD *February 1, 2016*

0 The first rule that matches a given packet will be applied to it. So you need to move the first 3 rules to after the deny rules.

craiganderson *February 1, 2016*

0 How do I do that? When I added the deny rules, they just appeared right there automatically.

manicas MOD *February 1, 2016*

2 Show rules with numbers:

```
$ sudo ufw status numbered
```

You can use this command to delete a rule:

```
$ sudo ufw delete rule_number
```

And this command to insert a rule in a particular place (1 for top of list):

```
$ sudo ufw insert 1 your_rule
```

okneloper *January 31, 2016*

0

"If your server shouldn't be sending outgoing mail, you may want to block that kind of traffic. To block outgoing SMTP mail, which uses port 25, run this command:"

```
    sudo ufw deny 25
```

This actully will block incoming SMTP traffic, not outgoing! Please fix this. The correct command is

```
 sudo ufw deny out 25
```

craiganderson *February 3, 2016*

0 I'm wondering if you can tell me what the following UFW log entries mean? (I replaced my server IP with xxx.xxx.xxx.xxx):

```
Feb  3 14:40:48 www kernel: [149871.434419] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:4b:
Feb  3 14:41:08 www kernel: [149891.197907] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:4b:
Feb  3 14:41:28 www kernel: [149911.255322] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:4b:
```

I have my UFW rules setup as follows:

```
To                         Action      From
--                         ------      ----
Anywhere                   DENY        89.248.171.5
22                         ALLOW       Anywhere
443                        ALLOW       Anywhere
80                         ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
```

manicas MOD *February 3, 2016*

0 I've read that those kinds of log entries have to do with handling connection termination between the server and the client. Should be safe to ignore.

douzr12 *February 28, 2016*

0 Thanks Mitchell Anicas for the article. It's helpful very much;
I have a question, Can I make rules to deny or allow MAC addresses ?

---

plsharevme *April 16, 2016*

0 after i enable ufw , i cannot get sudo apt-get update to work ,it keep say could not resolve mirror digitalocean

here is my ufw status.
imcoming denny all
outgoing allow all

To Action From

3690 ALLOW Anywhere
9418/tcp ALLOW Anywhere
80 ALLOW Anywhere
443 ALLOW Anywhere

80 ALLOW OUT Anywhere
443 ALLOW OUT Anywhere
53 ALLOW OUT Anywhere

Joswellve11a9f3 *April 28, 2016*

0 I have instaled wowza in my server and in step I was demanding to open the port 1935, i execute the commande "sudo ufw enable" and as a result I had no access to my ssh!
How can I get back to my SSH.
I need ur help please

---

okneloper *July 19, 2017*

0 Appreciate not relevant for @Joswellve11a9f3 anymore, just for future reference: if you have blocked yourself from accessing the server with UFW (which it warns you about this possibility when you enable it), you can access console from the DigitalOcean's account, which emulates direct terminal access and thus is not affected by firewalls. You can disable from there and login using SSH again to investigate what you have done wrong.

---

rejkpp *November 21, 2016*

0 What do I need to configure with wordpress installed?

I have followed the initial server setup for ubuntu 16.04, installed LEMP, set-up virtual hosts and installed wordpress all from digital ocean tutorials.

olivebay84 *August 9, 2017*

0 can you also add on how to save those rules , that is to make them persistent because I cant find it nowhere.

---

drhile *January 3, 2018*

0 A useful tip:

Usually a UFW profile such as OpenSSH is created when you install the `openssh-server` package. Using the already provided profile, you can restrict access to a specific subnet such as your home network's subnet. The command is: `sudo ufw allow from 192.168.0.0/24 to any app OpenSSH`. Obviously you change the subnet accordingly.

This is what it looks like in practice using only profiles:

```
To                          Action      From
--                          ------      ----
137,138/udp (Samba)         ALLOW IN    Anywhere
139,445/tcp (Samba)         ALLOW IN    Anywhere
80,443/tcp (Nginx Full)     ALLOW IN    Anywhere
3389/tcp (MySQL)            ALLOW IN    Anywhere
3389/udp (MySQL)            ALLOW IN    Anywhere
22/tcp (OpenSSH)            ALLOW IN    192.168.0.0/24
137,138/udp (Samba (v6))    ALLOW IN    Anywhere (v6)
139,445/tcp (Samba (v6))    ALLOW IN    Anywhere (v6)
80,443/tcp (Nginx Full (v6)) ALLOW IN    Anywhere (v6)
3389/tcp (MySQL (v6))       ALLOW IN    Anywhere (v6)
3389/udp (MySQL (v6))       ALLOW IN    Anywhere (v6)
```

Community Tutorials Questions Projects Tags Newsletter RSS

Distros & One-Click Apps Terms, Privacy, & Copyright Security Report a Bug Write for DOnations Shop