Uncomplicated-Firewall (UFW)

Setup Basic Firewall With UFW

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed for easy use. It uses a command-line interface (CLI) with a small number of simple commands, and is configured withiptables . UFW is available by default in all Ubuntu installations after 18.04 LTS, and features tools for intrusion prevention which we will cover in this guide.

Setup

Start by checking the status of UFW.

```

Copy sudoufwstatus

```

Then proceed to configure your firewall with the following options, preferably in this order.

The order is important because UFW executes the instructions given to it in the order they are given, so putting the most important and specific rules first is a good security practice. You can insert UFW rules at any position you want to by using the following syntax (do not execute the following command when setting up your node security):

```

Copy ufwinsert1fromtoany//exampleonly

```

The example command above would be placed in the first position (instead of the last) of the UFW hierarchy and deny a specific IP address from accessing the server.

Set Outgoing Connections

This sets the default to allow outgoing connections unless specified they should not be allowed.

```

Copy sudoufwdefaultallowoutgoing

```

Set Incoming Connections

This sets the default to deny incoming connections unless specified they should be allowed.

```

Copy sudoufwdefaultdenyincoming

```

Set And Limit SSH Connections

This allows SSH connections by the firewall.

```

Copy sudoufwallowssh/tcp

```

This limits SSH login attempts on the machine. The default is to limit SSH connections from a specific IP address if it attempts 6 or more connections within 30 seconds.

```

Copy sudoufwlimitssh/tcp

```

Set Accessible Ports

Allow 26656 for a p2p networking port to connect with the Tendermint network; unless you manually specified a different port.

```

Copy sudoufwallow26656

```

Allow 1317 if you are running a public LCD endpoint from this node. Otherwise, you can skip this.

```

Copy sudoufwallow1317

```

Allow 26657 if you are running a public RPC endpoint from this node. Otherwise, you can skip this.

```

Copy sudoufwallow26657

```

Enable UFW Firewall

This enables the firewall you just configured.

```

Copy sudo ufw enable

```

At any point in time you can disable your UFW firewall by running the following command. ```

Copy sudoufwdisable

```

Last updated2 months ago On this page *Setup Basic Firewall With UFW * Setup * Set Outgoing Connections * Set Incoming Connections * Set And Limit SSH Connections * Set Accessible Ports * Enable UFW Firewall

Was this helpful? Edit on GitHub Export as PDF
```