

ufw - Uncomplicated Firewall

Uncomplicated Firewall??? UFW?? Ubuntu ????????????UFW ??????? iptables
?????????UFW ?????????????????? IPV4?IPV6?????????UFW ? Ubuntu 8.04 LTS
????????????????

Tutorials

- [Linux Firewalls: Uncomplicated Firewall \(ufw\)](#)
- [Using Firewall With UFW in Ubuntu Linux \[Beginner's Guide\] \(itsfoss.com\)](#)

Basic Commands

```
# Install
sudo apt-get install ufw

# Enable the UFW
sudo ufw enable
sudo ufw status

# Allow the services and ports
sudo ufw allow OpenSSH
sudo ufw allow 655
```

For Cloudflare Traffic

Cloudflare [publishes the IP addresses of its servers online](#).

```
# For HTTP with IPv4
sudo ufw allow from 173.245.48.0/20 to any port http
sudo ufw allow from 103.21.244.0/22 to any port http
sudo ufw allow from 103.22.200.0/22 to any port http
sudo ufw allow from 103.31.4.0/22 to any port http
sudo ufw allow from 141.101.64.0/18 to any port http
```

```
sudo ufw allow from 108.162.192.0/18 to any port http
sudo ufw allow from 190.93.240.0/20 to any port http
sudo ufw allow from 188.114.96.0/20 to any port http
sudo ufw allow from 197.234.240.0/22 to any port http
sudo ufw allow from 198.41.128.0/17 to any port http
sudo ufw allow from 162.158.0.0/15 to any port http
sudo ufw allow from 104.16.0.0/12 to any port http
sudo ufw allow from 172.64.0.0/13 to any port http
sudo ufw allow from 131.0.72.0/22 to any port http
```

For HTTP with IPv6

```
sudo ufw allow from 2400:cb00::/32 to any port http
sudo ufw allow from 2606:4700::/32 to any port http
sudo ufw allow from 2803:f800::/32 to any port http
sudo ufw allow from 2405:b500::/32 to any port http
sudo ufw allow from 2405:8100::/32 to any port http
sudo ufw allow from 2a06:98c0::/29 to any port http
sudo ufw allow from 2c0f:f248::/32 to any port http
```

For HTTPS with IPv4

```
sudo ufw allow from 173.245.48.0/20 to any port https
sudo ufw allow from 103.21.244.0/22 to any port https
sudo ufw allow from 103.22.200.0/22 to any port https
sudo ufw allow from 103.31.4.0/22 to any port https
sudo ufw allow from 141.101.64.0/18 to any port https
sudo ufw allow from 108.162.192.0/18 to any port https
sudo ufw allow from 190.93.240.0/20 to any port https
sudo ufw allow from 188.114.96.0/20 to any port https
sudo ufw allow from 197.234.240.0/22 to any port https
sudo ufw allow from 198.41.128.0/17 to any port https
sudo ufw allow from 162.158.0.0/15 to any port https
sudo ufw allow from 104.16.0.0/12 to any port https
sudo ufw allow from 172.64.0.0/13 to any port https
sudo ufw allow from 131.0.72.0/22 to any port https
```

Cheat Sheet



Linux ufw Firewall Command

ufw is a user-friendly frontend for **iptables** on Linux

Basics: enable/disable ufw and modify its settings

`ufw status <verbose|numbered>` show firewall rules with optional verbosity
`ufw [enable|disable]` enable or disable ufw
`ufw reload` refresh modified ufw rules without stopping ufw service
`ufw logging [on|off] <log-level>` enable logging (log-level: low/medium/high/full)

Rule addition: add allow/deny/limit rules

`ufw default [allow|deny|reject] [incoming|outgoing]` change default in/out action
`ufw deny on eth0 from 1.1.1.0/24` drop all traffic on eth0 from 1.1.1.0/24 subnet
`ufw reject in from 1.1.1.1` reject all traffic from 1.1.1.1 with error packet sent back
`ufw deny ssh` reject block all incoming ssh connections by default
`ufw allow 5555/udp` allow udp connection to port 5555
`ufw allow from 1.1.1.1 proto tcp to any port 22` allow ssh traffic from 1.1.1.1 only
`ufw limit ssh/tcp rate limit ssh connections (only allow 6 connections in 30 secs)`

Rule removal: remove one or more rules

`ufw delete deny on eth0 from 1.1.1.0/24` remove a specified rule
`ufw delete <rule-number>` remove a rule by rule number
`ufw reset` remove all existing rules and reset firewall rules to defaults

App profiles: enable/disable rules based on app profiles

`ufw app list` show app profiles in /etc/ufw/applications.d
`ufw allow <profile-name>` enable an app profile
`ufw delete allow <profile-name>` disable an app profile



Created by
@dan_nanni
on Instagram

Revision #7

Created 17 September 2022 09:50:23 by Admin

Updated 17 July 2024 20:53:01 by Admin