

Ubuntu UFW Firewall Commands Cheat Sheet

Get more Linux command cheat sheets at [UbuntuFree.com](https://ubuntufree.com)

Full guide with explanations: www.ubuntufree.com/ufw-firewall-commands-in-ubuntu-with-examples/

Updated for Ubuntu 26.04 LTS (2026)

UFW, the Uncomplicated Firewall, is the standard firewall front end on Ubuntu 26.04 LTS and Ubuntu 26.10. It is installed by default but switched off. This guide shows how to enable it safely, open and close ports, manage rules and read the firewall log, with copy-ready examples and a free cheat sheet.

Turn on UFW safely

Set the defaults and allow SSH first, then enable. On a desktop without an SSH server you can skip the SSH rule.

1. Check firewall status

Shows whether ufw is active, the default policies and every rule.

```
sudo ufw status verbose
```

2. Set the default policies

Blocks unsolicited incoming connections and lets the machine connect out.

```
sudo ufw default deny incoming  
sudo ufw default allow outgoing
```

3. Allow SSH before enabling

Uses the OpenSSH app profile, which opens port 22/tcp. The profile appears once openssh-server is installed.

```
sudo ufw allow OpenSSH
```

Without the profile, use `sudo ufw allow 22/tcp`.

4. Enable the firewall

Activates ufw now and at every boot. It asks for confirmation because it may disrupt SSH sessions.

```
sudo ufw enable
```

Allow and deny traffic

Rules are matched top to bottom and the first match wins. ufw adds IPv4 and IPv6 versions of each rule automatically.

5. Allow a port

Opens a TCP port, here for a web server.

```
sudo ufw allow 80/tcp  
sudo ufw allow 443/tcp
```

6. Allow a service by name

ufw looks up names in `/etc/services`.

```
sudo ufw allow http  
sudo ufw allow https
```

7. Allow a port range

Ranges need a protocol.

```
sudo ufw allow 6000:6007/tcp
```

8. Allow one IP address

Trusts every port from a single machine.

```
sudo ufw allow from 192.168.1.50
```

9. Allow a subnet to one port

Lets only your LAN reach SSH.

```
sudo ufw allow from 192.168.1.0/24 to any  
port 22 proto tcp
```

10. Deny a port or address

Drops matching traffic silently.

```
sudo ufw deny 23/tcp  
sudo ufw deny from 203.0.113.7
```

11. Reject instead of deny

Sends an error back so the client fails fast instead of timing out.

```
sudo ufw reject 25/tcp
```

13. Rule for one interface

Applies the rule only to traffic arriving on the named network card. Find names with `ip -br a`.

```
sudo ufw allow in on enp3s0 to any port 80  
proto tcp
```

15. Add a comment to a rule

Comments show in `ufw status` and remind you why a port is open.

```
sudo ufw allow 8080/tcp comment 'dev server'
```

12. Rate-limit SSH

Blocks an address that opens 6 or more connections within 30 seconds.

```
sudo ufw limit OpenSSH
```

14. Block outgoing traffic

Outgoing rules work the same way with `out`.

```
sudo ufw deny out 25/tcp
```

List, delete and reorder rules

Numbered output makes it easy to remove or insert rules without retyping them.

16. Show numbered rules

Lists rules with an index number.

```
sudo ufw status numbered
```

17. Delete a rule by number

Removes rule 3 after a confirmation. Numbers shift after each delete, so list again before the next one.

```
sudo ufw delete 3
```

18. Delete a rule by its text

Repeat the original rule after delete.

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

19. Insert a rule at the top

Puts a block rule before existing allow rules so it matches first.

```
sudo ufw insert 1 deny from 203.0.113.7
```

20. Preview a change

`--dry-run` prints the resulting rules without applying them.

```
sudo ufw --dry-run allow 3000/tcp
```

21. Show rules you added

Lists your rules as commands, even while `ufw` is disabled.

```
sudo ufw show added
```

22. Reload, disable or reset

`reload` re-reads the rules. `disable` turns the firewall off. `reset` disables `ufw` and deletes all rules, after making backups.

```
sudo ufw reload  
sudo ufw disable  
sudo ufw reset
```

App profiles and logging

Packages can ship app profiles in `/etc/ufw/applications.d` so you can allow a service by name instead of remembering ports.

23. List app profiles

Shows the profiles available on this machine.

```
sudo ufw app list
```

24. Show what a profile opens

Prints the ports and protocols behind a profile.

```
sudo ufw app info OpenSSH
```

25. Turn on logging

low is the default level. medium also logs invalid and new connections.

```
sudo ufw logging on
sudo ufw logging medium
```

26. Read the firewall log

Blocked packets are tagged [UFW BLOCK] in the kernel log.

```
sudo journalctl -k | grep UFW
sudo tail -f /var/log/ufw.log
```

27. Check IPv6 is covered

IPv6=yes in this file makes ufw manage IPv6 rules too. It is the default.

```
grep IPV6 /etc/default/ufw
```

28. See the generated nftables rules

On Ubuntu 26.04, ufw drives the kernel firewall through the nftables based iptables backend.

```
sudo nft list ruleset | less
```

Common UFW rules

Goal	Command
SSH from anywhere	<code>sudo ufw allow OpenSSH</code>
SSH from LAN only	<code>sudo ufw allow from 192.168.1.0/24 to any port 22 proto tcp</code>
Web server	<code>sudo ufw allow 80/tcp && sudo ufw allow 443/tcp</code>
Slow down brute force	<code>sudo ufw limit OpenSSH</code>
Block an attacker first	<code>sudo ufw insert 1 deny from 203.0.113.7</code>
Remove a rule	<code>sudo ufw status numbered</code> , then <code>sudo ufw delete N</code>
Start over	<code>sudo ufw reset</code>

Tips and best practices

Keep a second SSH session open while you change firewall rules on a remote server. If a rule locks you out of new sessions, you can still fix it from the open one.

Docker publishes container ports with its own rules that can bypass ufw. If you run Docker, bind published ports to 127.0.0.1 or check the Docker documentation on firewall rules.