ufw Simple Linux firewall

CONCEPTS

> **Do not lock yourself out**
> Over SSH, allow ssh (or your custom port) before 'ufw enable'. Enabling flushes the chains and may drop your session.

Packet in direction + port
↓ built-in rules
ufw rules top to bottom
↓ no match
Default policy incoming: deny
↓ verdict
Allow / deny optional log

Packet check: first matching rule wins, else the default policy

> Defaults after install: incoming deny, outgoing allow, firewall disabled. Rules are added for IPv4 and IPv6 together.

> Rule order matters. Put narrow exceptions (insert 1) above broad denies.

FIREWALL STATE

`sudo ufw enable`
Enable now and at boot

`sudo ufw disable`
Stop the firewall

`sudo ufw status`
Active or inactive, plus rules

`sudo ufw status verbose`
Also defaults and logging

`sudo ufw status numbered`
Rules with index numbers

`sudo ufw reload`
Reapply the rules

`sudo ufw reset`
Disable and wipe all rules

DEFAULT POLICY

`sudo ufw default deny incoming`
Block unsolicited inbound

`sudo ufw default allow outgoing`
Allow all outbound

SIMPLE RULES

`sudo ufw allow <port>`
Allow a port, tcp and udp

`sudo ufw allow <port>/tcp`
Allow one protocol

`sudo ufw allow <service>`
Allow by name from /etc/services

`sudo ufw deny <port>/tcp`
Silently drop a port

`sudo ufw reject <port>/tcp`
Refuse with a reply

`sudo ufw limit ssh`
Allow but throttle repeats

`sudo ufw allow 6000:6007/tcp`
Allow a port range

`sudo ufw allow 22,80,443/tcp`
Several ports in one rule

`sudo ufw allow out <port>/tcp`
Allow outbound only

`sudo ufw allow <port>/tcp comment '<text>'`
Annotate a rule

FULL SYNTAX

`sudo ufw allow from <ip>`
Allow all from one host

`sudo ufw deny from <ip>`
Block one host

`sudo ufw allow from <cidr> to any port <port>`
Allow a subnet to a port

`sudo ufw allow from <ip> to any port <port> proto tcp`
Host, port and protocol

`sudo ufw allow in on <iface> to any port <port>`
Limit to an interface

`sudo ufw allow from <ip> to <dest-ip> port <port>`
Match destination address

`sudo ufw deny proto udp from <ip> to any port <port>`
Drop UDP from a host

MANAGE RULES

`sudo ufw delete <num>`
Delete by rule number

MANAGE RULES (cont.)

`sudo ufw delete allow <port>/tcp`
Delete by repeating the rule

`sudo ufw insert <num> deny from <ip>`
Insert at a position

APPLICATION PROFILES

`sudo ufw app list`
Available profiles

`sudo ufw app info '<profile>'`
Ports a profile opens

`sudo ufw allow '<profile>'`
Allow by profile name

LOGGING AND REPORTS

`sudo ufw logging on`
Enable logging

`sudo ufw logging off`
Disable logging

`sudo ufw logging medium`
Set the log level

`sudo ufw show added`
Rules as you typed them

`sudo ufw show listening`
Open ports and their programs

> Blocked packets are logged as [UFW BLOCK] in the kernel log; search with journalctl -k or /var/log/ufw.log.

RECIPES

Lock down a new server

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw limit ssh
sudo ufw allow 80,443/tcp
sudo ufw enable
```

Allow a service only from the LAN

```
sudo ufw allow from 192.168.1.0/24
to any port 5432 proto tcp
# nothing else can reach it
sudo ufw status numbered
```

Block an address above all else

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