ufw Simple Linux firewall

START HERE

`sudo ufw allow ssh`
Keep SSH open first

`sudo ufw deny from <ip>`
Block an address

`sudo ufw enable`
Turn the firewall on

`sudo ufw status numbered`
List rules with numbers

`sudo ufw status verbose`
Show state and rules

`sudo ufw delete <num>`
Remove a rule

`sudo ufw allow 80/tcp`
Open a port

`sudo ufw limit ssh`
Rate-limit brute force



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

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.

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
Asks for confirmation; --force skips it. Rule files get a timestamped backup.

`sudo ufw --force enable`
Enable without the SSH prompt

`sudo ufw --dry-run <command>`
Preview changes, apply nothing

DEFAULT POLICY

`sudo ufw default deny incoming`
Block unsolicited inbound

`sudo ufw default allow outgoing`
Allow all outbound

`sudo ufw default deny outgoing`
Whitelist outbound only

`sudo ufw default reject incoming`
Refuse with an error reply

DEFAULT POLICY (cont.)

`sudo ufw default deny routed`
Block forwarded traffic

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
Denies an address with 6 or more connection attempts in 30 seconds.

`sudo ufw allow 6000:6007/tcp`
Allow a port range
Ranges need an explicit protocol (/tcp or /udp).

`sudo ufw allow 22,80,443/tcp`
Several ports in one rule
At most 15 ports per 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

FULL SYNTAX (cont.)

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

`sudo ufw allow from <ip> to any app <profile>`
Host to an app profile

`sudo ufw route allow in on <iface1> out on <iface2> to <ip>`
Allow forwarded traffic
Also needs forwarding set in /etc/ufw/sysctl.conf, then ufw disable and enable.

MANAGE RULES

`sudo ufw delete <num>`
Delete by rule number
Numbers shift after each deletion; list again before the next.

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

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

`sudo ufw prepend deny from <ip>`
Insert at the top

`sudo ufw allow log <port>/tcp`
Log new matches of a rule

`sudo ufw allow log-all <port>/tcp`
Log every matching packet

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

`sudo ufw app update <profile>`
Refresh a profile's rules

`sudo ufw app default skip`
Default app policy

Profiles are INI files in /etc/ufw/applications.d with title, description and ports.

LOGGING AND REPORTS

`sudo ufw logging on`
Enable logging

`sudo ufw logging off`
Disable logging

`sudo ufw logging medium`
Set the log level
Levels: off, low, medium, high, full. Above medium can fill the disk.

`sudo ufw show added`
Rules as you typed them

`sudo ufw show listening`
Open ports and their programs

`sudo ufw show raw`
Full underlying ruleset
status hides rules from the /etc/ufw/.rules files; raw shows them.*

`sudo ufw show user-rules`
Your rules as iptables output

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

Config lives in /etc/default/ufw (IPv6 switch, policies) and /etc/ufw/*.rules.

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
```

Close a port you opened

```
sudo ufw status numbered
sudo ufw delete 3
# or by rule: sudo ufw delete
allow 8080/tcp
```