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

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

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

SIMPLE RULES (cont.)

`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 limit ssh`
Allow but throttle repeats

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

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

MANAGE RULES

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

`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

LOGGING AND REPORTS

`sudo ufw logging on`
Enable logging