Praxisnahe, sicherheitsorientierte UFW-Konfiguration mit Erläuterungen. Du kannst sie je nach Bedarf anpassen. Wichtig: teste immer erst aus einer bestehenden SSH-Session, damit du dich nicht aus dem Server aussperrst.

Grundlagen (empfohlen als Ausgangspunkt)

- Default-Richtlinien:
  - Incoming: verweigern
  - Outgoing: zulassen
- Loopback-Verkehr zulassen
- Logs aktivieren, damit du Anomalien sehen kannst
- SSH sinnvoll absichern (Limit, nur von bestimmten IPs erlauben, ggf. kein offenes Port-Forwarding)

Schritte (alle Befehle als sudo ausführen)

1. UFW installieren (falls noch nicht)

- Debian/Ubuntu: sudo apt update && sudo apt install ufw

2. Allgemeine Defaults

- sudo ufw default deny incoming
- sudo ufw default allow outgoing
- sudo ufw allow in on lo
- sudo ufw logging on

3. SSH absichern Option A: SSH allgemein erlauben, aber mit Limit (Brute-Force-Schutz)

- sudo ufw limit 22/tcp Option B: SSH nur von deiner Admin-IP zulassen
- sudo ufw allow from <DEINE_ADMIN_IP> to any port 22 proto tcp Ersetze <DEINE_ADMIN_IP> durch deine feste IP-Adresse. Falls du dynamische IP hast, ziehe Alternativen wie VPN in Betracht.

4. Dienste je nach Bedarf freigeben

- Webserver (HTTP/HTTPS):
  - sudo ufw allow 'Nginx Full' oder explizit:
  - sudo ufw allow 80/tcp
  - sudo ufw allow 443/tcp
- OpenVPN/WireGuard (falls du einen VPN-Server betreibst):
  - OpenVPN (typisch UDP 1194): sudo ufw allow 1194/udp
  - WireGuard (typisch UDP 51820): sudo ufw allow 51820/udp
- DNS (falls dein Host DNS-Anfragen bedienen soll):
  - sudo ufw allow 53/tcp
  - sudo ufw allow 53/udp
- Andere Dienste nach Bedarf (SSH-Remote-Desktop, File shares, etc.)
  - Nutze entweder Ports direkt, oder nutze UFW-App-Profile, z.B.:
    - sudo ufw app list
    - sudo ufw allow 'Apache Full' oder 'Apache 2' etc.

5. Wenn der Host nur im privaten Netz erreichbar sein soll (LAN-Segmente)

- Erlaube Zugriffe nur aus deinem LAN, z.B. 192.168.1.0/24:
    - sudo ufw allow from 192.168.1.0/24 to any port 22 proto tcp
    - sudo ufw allow from 192.168.1.0/24 to any port 80 proto tcp
    - Hinweis: Generell besser nur notwendige Ports freigeben, nicht das ganze LAN-Subnetz zulassen, falls nicht nötig.

6. Optional: IPv6 unterstützen

- Falls dein Server IPv6 verwendet, stelle sicher, dass UFW IPv6 aktiviert ist:
    - Bearbeite /etc/ufw/ufw.conf und setze IPV6=yes
    - Dann dieselben Regeln wie oben anwenden (erreichbar mit IPv6-Adressen)

7. Regeln prüfen und aktivieren

- sudo ufw status verbose
- Falls noch nicht aktiviert:
    - sudo ufw enable
    - Warnung: Bei SSH-Zugang muss der SSH-Port offen bleiben, sonst kommst du ggf. aus der Remote-Session raus.

Beispielkonfigurationen (kompakt)

A. Minimaler, sicherer Desktop-Server (Admin-IP bekannt, nur SSH)

- sudo ufw default deny incoming
- sudo ufw default allow outgoing
- sudo ufw allow from <ADMIN_IP> to any port 22 proto tcp
- sudo ufw limit 22/tcp
- sudo ufw allow in on lo
- sudo ufw logging on
- sudo ufw enable

B. Webserver-Profil (öffentlicher Zugriff auf HTTP/HTTPS, SSH nur Admin-IP)

- sudo ufw default deny incoming
- sudo ufw default allow outgoing
- sudo ufw allow from <ADMIN_IP> to any port 22 proto tcp
- sudo ufw limit 22/tcp
- sudo ufw allow 'Nginx Full' # oder: sudo ufw allow 80/tcp && sudo ufw allow 443/tcp
- sudo ufw allow in on lo
- sudo ufw logging on
- sudo ufw enable

C. Server hinter VPN (Nur VPN-Verkehr ins interne Netz)

- sudo ufw default deny incoming
- sudo ufw default allow outgoing
- sudo ufw allow in on lo
- sudo ufw allow 51820/udp # WireGuard, ggf. anpassen
- sudo ufw allow 80/tcp
- sudo ufw allow 443/tcp
- sudo ufw enable
- (Zusatz) VPN-Client-IP-Bereich im Firewall-Kontext zulassen, falls nötig: sudo ufw allow from 10.8.0.0/24 to any

Wichtige Hinweise

- Verifiziere, dass du dich nicht selbst aussperrst: immer eine laufende SSH-Verbindung testen oder eine Notfall-SSH-Backdoor-IP/Management-Interface vorbereitet haben.
- Nutze Fail2ban zusammen mit UFW für weitere Schutzmechanismen gegen Brute-Force-Attacken auf SSH.
- Für komplexere Netzwerke: Du kannst auch mehrere Profile nutzen (z. B. "server", "webserver", "lan-only") und je nach Bedarf aktivieren.
- Überlege, zusätzliche Regeln für ICMP (Pings) gezielt zu erlauben/zu blockieren, je nach Sicherheitsbedürfnis. UFW behandelt ICMP standardmäßig als Teil von normalen Regeln; du kannst gezielt ICMP-Typen freigeben, falls gewünscht.