Security Guide

Firewall

Firewall

UFW auf Hetzner

Installation:

```
ssh hetzner
apt install -y ufw
```

Regeln setzen:

```
ufw default deny incoming
ufw default allow outgoing

ufw allow 22/tcp comment 'SSH (wird später auf 9999 geändert)'
ufw allow 9999/tcp comment 'SSH Custom Port'
ufw allow 80/tcp comment 'HTTP'
ufw allow 443/tcp comment 'HTTPS'
ufw allow 51820/udp comment 'Wireguard'

ufw enable
ufw status verbose
```

Nach SSH Port Änderung:

```
ufw delete allow 22/tcp
ufw reload
```

Firewall

UFW auf Homeserver

Regeln:

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

# Tailscale erlauben
  sudo ufw allow in on tailscale0

# Wireguard erlauben
  sudo ufw allow in on wg0

# SSH nur über Tailscale
  sudo ufw allow from 100.0.0.0/8 to any port 22 proto tcp comment 'SSH via Tailscale'

  sudo ufw enable
  sudo ufw status verbose
```

SSH Hardening

Key-Only Login

SSH-Config

```
nano /etc/ssh/sshd_config
```

Wichtige Einstellungen

```
PasswordAuthentication no
ChallengeResponseAuthentication no
UsePAM no
PermitRootLogin prohibit-password
PermitEmptyPasswords no
Protocol 2
LoginGraceTime 60
MaxAuthTries 3
X11Forwarding no
```

SSH neustarten:

```
systemctl restart sshd
```

SSH Custom Port

Port ändern:

```
nano /etc/ssh/sshd_config
```

Ändere:

```
Port 1234
```

UFW anpassen:

```
ufw allow 1234/tcp
ufw delete 22/tcp
ufw reload
```

SSH reload

```
systemctl reload sshd
```

Lokale SSH Config anpassen:

```
nano /.ssh/config
```

```
Host Hetzner
  Hostname 1.2.3.4
  User root
  IdentityFile ~/.ssh/Hetznerkey
  Port 1234
```

Fail2Ban

Installation und Config

Auf Hetzner:

```
apt install -y fail2ban
nano /etc/fail2ban/jail.local
```

Inhalt:

```
[DEFAULT]
bantime = 3600
findtime = 600
maxretry = 5
ignoreip = 127.0.0.1/8 ::1

action = %(action_)s
         telegram

destemail = root@localhost
sendername = Fail2Ban
mta = mail

[sshd]
enabled = true
port = 9999
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 7200
```

Telegram-Action

```
nano /etc/fail2ban/action.d/telegram.conf
```

Inhalt (mit eigenen Werten)

```
[Definition]

actionstart = curl -s -X POST https://api.telegram.org/bot<TOKEN>/sendMessage -d
chat_id=<CHAT_ID> -d text="□□□Fail2Ban gestartet auf <fq-hostname>"

actionstop = curl -s -X POST https://api.telegram.org/bot<TOKEN>/sendMessage -d
chat_id=<CHAT_ID> -d text="⚠□ Fail2Ban gestoppt auf <fq-hostname>"

actioncheck =

actionban = curl -s -X POST https://api.telegram.org/bot<TOKEN>/sendMessage -d
chat_id=<CHAT_ID> -d parse_mode=HTML -d text="□□<b>IP gebannt!</b>%%0AServer: <fq-
hostname>%%0AJail: <name>%%0AIP: <ip>%%0AVersuche: <failures>%%0AZeit: $(date)"

actionunban = curl -s -X POST https://api.telegram.org/bot<TOKEN>/sendMessage -d
chat_id=<CHAT_ID> -d text="□ IP entsperrt: <ip> auf <fq-hostname>"

[Init]
```

Aktivieren:

```
systemctl restart fail2ban
systemctl status fail2ban
```

Wichtige Befehle

Status:

```
fail2ban-client status
fail2ban-cleint status sshd
```

Gebannte IP's:

```
fail2ban-client get sshd banned
```

IP bannen/entbannen

```
fail2ban-client set shhd banip 1.2.3.4
fail2ban-clien set shhd unbanip 1.2.3.4
```

Logs:

```
tail -f /var/log/fail2ban.log
```

Security Updates

Automatische Updates

Auf beiden Servern

```
apt install -y unattended-upgrades apt-listchanges
dpkg-reconfigure -plow unattended-upgrades
# Wähle yes
```

Config:

```
nano /etc/apt/apt.conf.d/50unattended-upgrades
```

> **Wichtig**
>
> Unattended-Upgrade::Automatic-Reboot "false";
>
> Unattended-Upgrade::Automatic-Reboot-Time "03:00";

Update Zeitplan

```
nano /etc/apt/apt.conf.d/20auto-upgrades
```

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

Status:

```
systemctl status unattended-upgrades
```

Logs:

```
cat /var/log/unattended-upgrades/unattended.upgrades.log
```