Eine Firewall für’s Heimnetzwerk

Linux-Cafe 2026-05-06

Aldo Brießmann
Bernd Strößenreuther

Lizenz

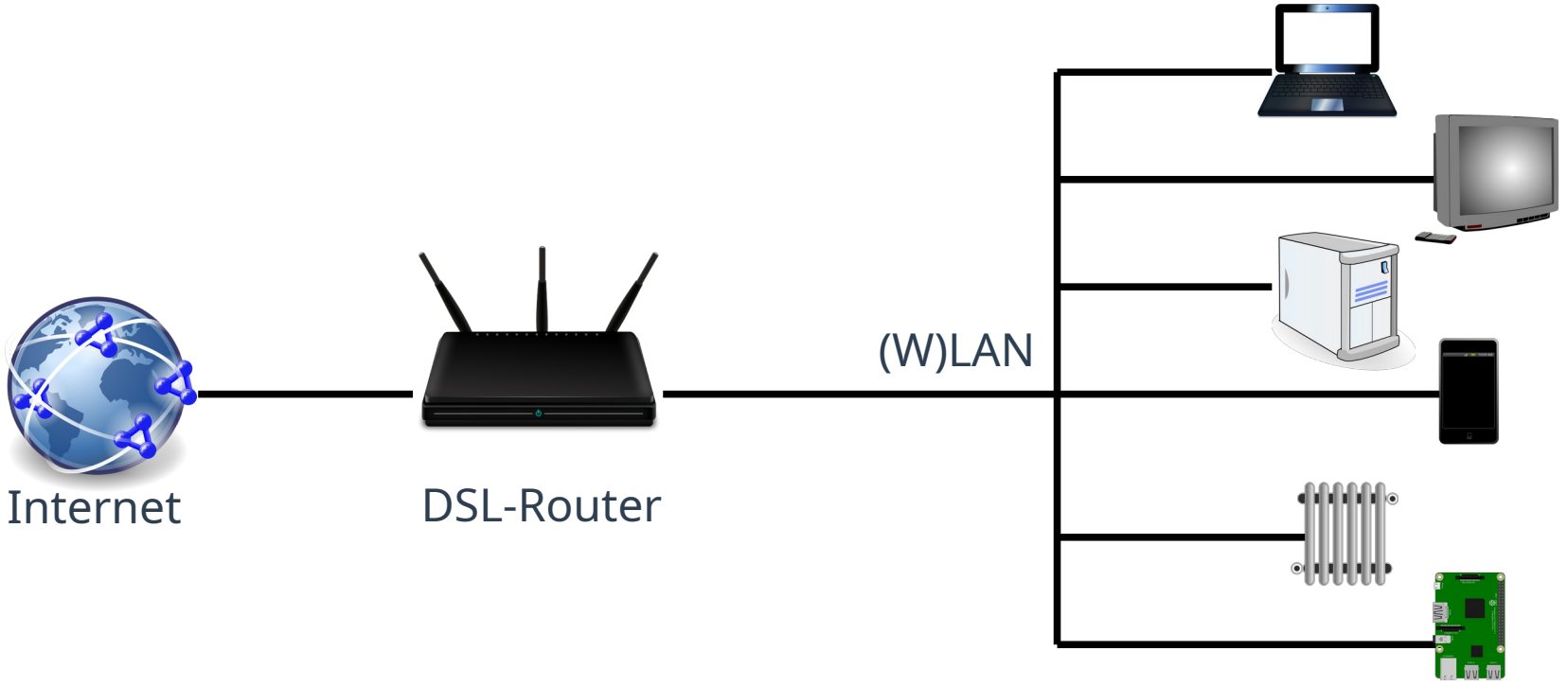
Agenda

- **Eine Firewall im Heimnetzwerk: Warum?**
- **Minimal-Lösungen**
  - Einschränkungen
- **Volle Kontrolle: Filtern an zentraler Stelle**
  - Shorewall
  - OPNsense
- **Fragen**

Eine Firewall im Heimnetzwerk: Warum?

- **Im (W)LAN tummel sich unterschiedlichste Geräte**
  - PCs/Notebooks, Smartphones/Tablets, Fernseher, Wallboxen, Hausautomatisierungskomponenten, Fernwartungszugang der Heizung, Staubsauger-Roboter, smart* (Gadgets), Shelly, NAS, Scanner, Drucker, etc.
- **Viele davon: Schlechte Versorgung mit Updates**
- **Will ich, dass alle davon alle meine privaten Bilder auf dem NAS sehen können?**
- **Will ich, dass alle davon sämtliche Netzwerkverbindungen von allen anderen sehen können?**
- **Will ich, dass alle Gadgets frei nach Hause telefonieren können?**

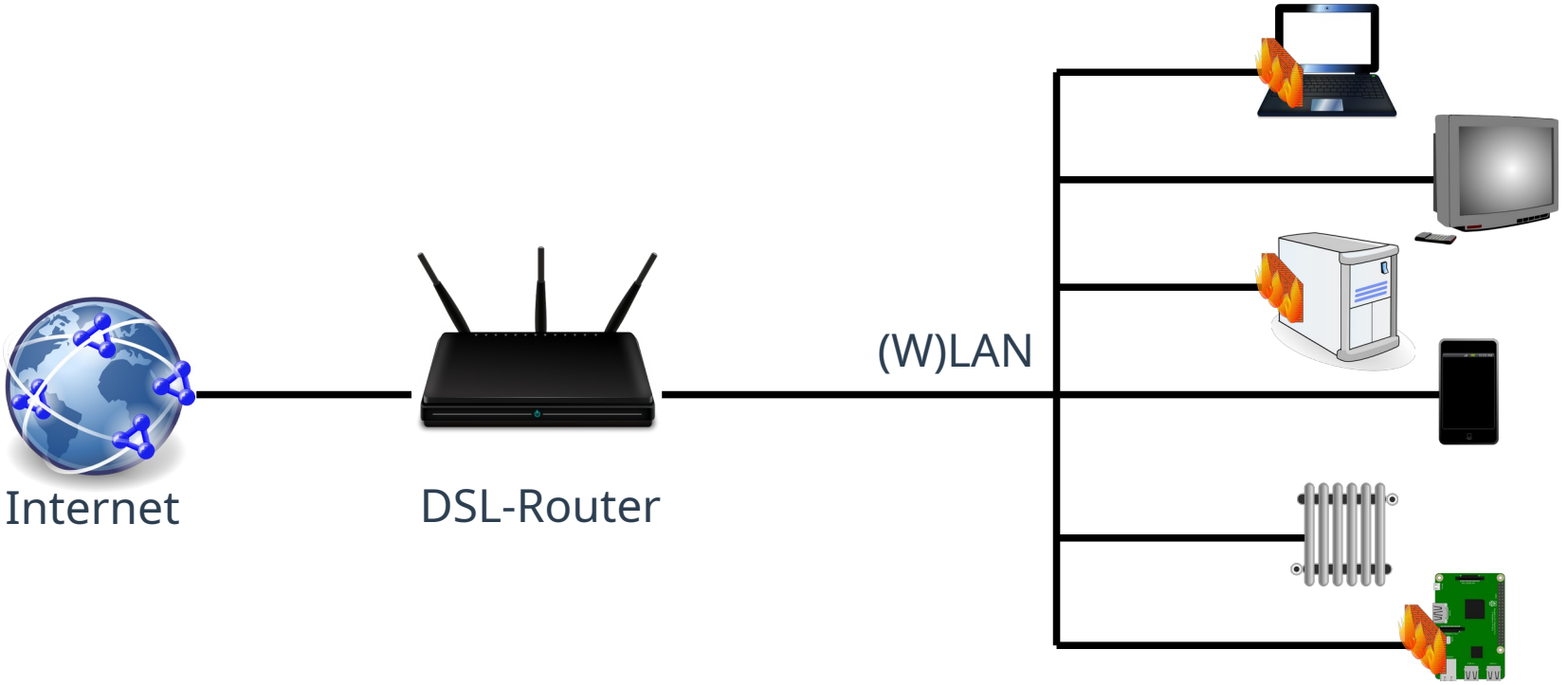
Ausgangssituation: Jeder darf alles mit jedem



Minimallösung 1

- **Auf den PCs / Notebooks eine Firewall installieren**
- **Nachteile**
  - Kann ich auf dem NAS überhaupt eine Firewall einrichten?
  - Viele verschiedene einzelne Firewalls zu pflegen

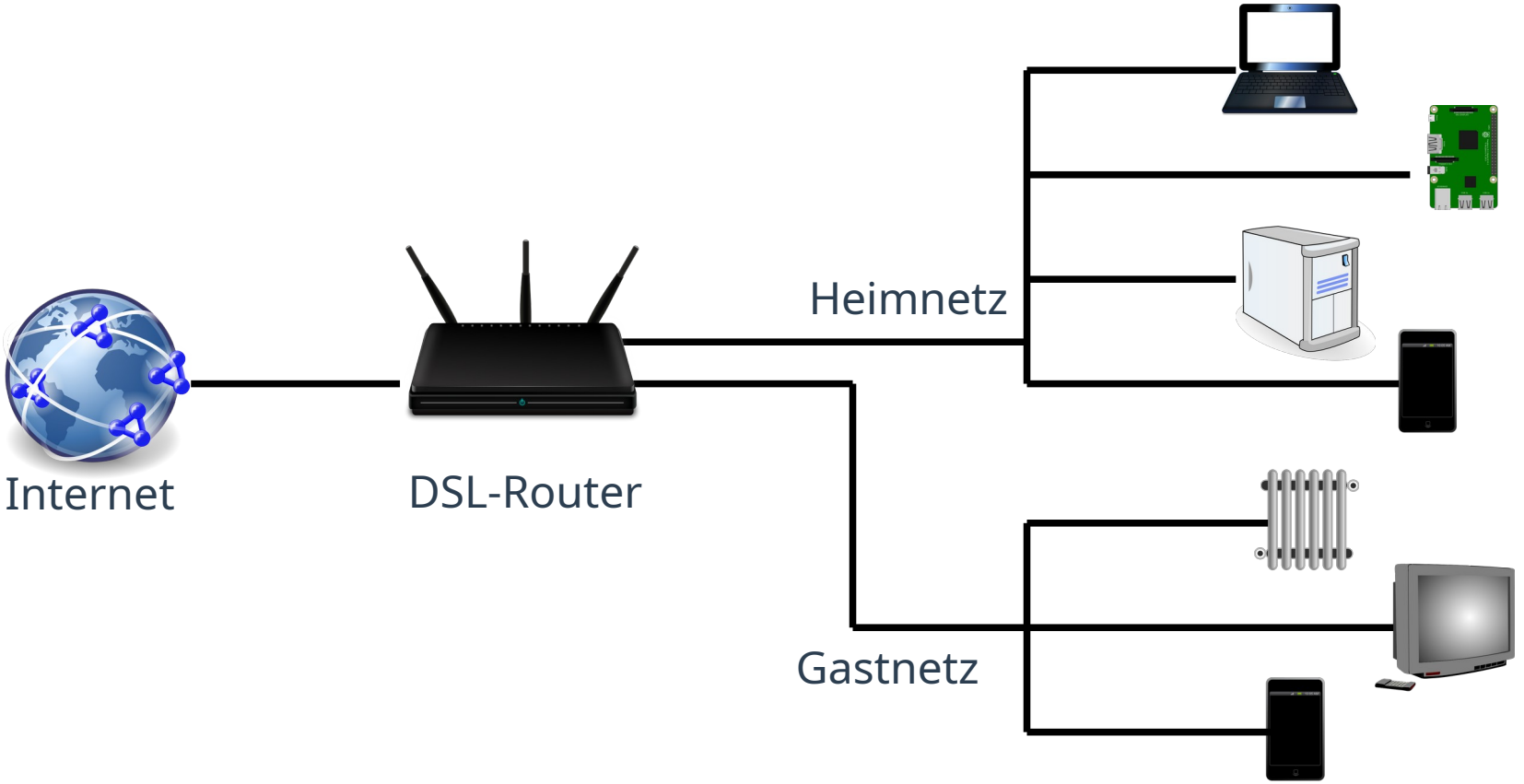
Minimallösung 1: Firewall am Gerät installiert



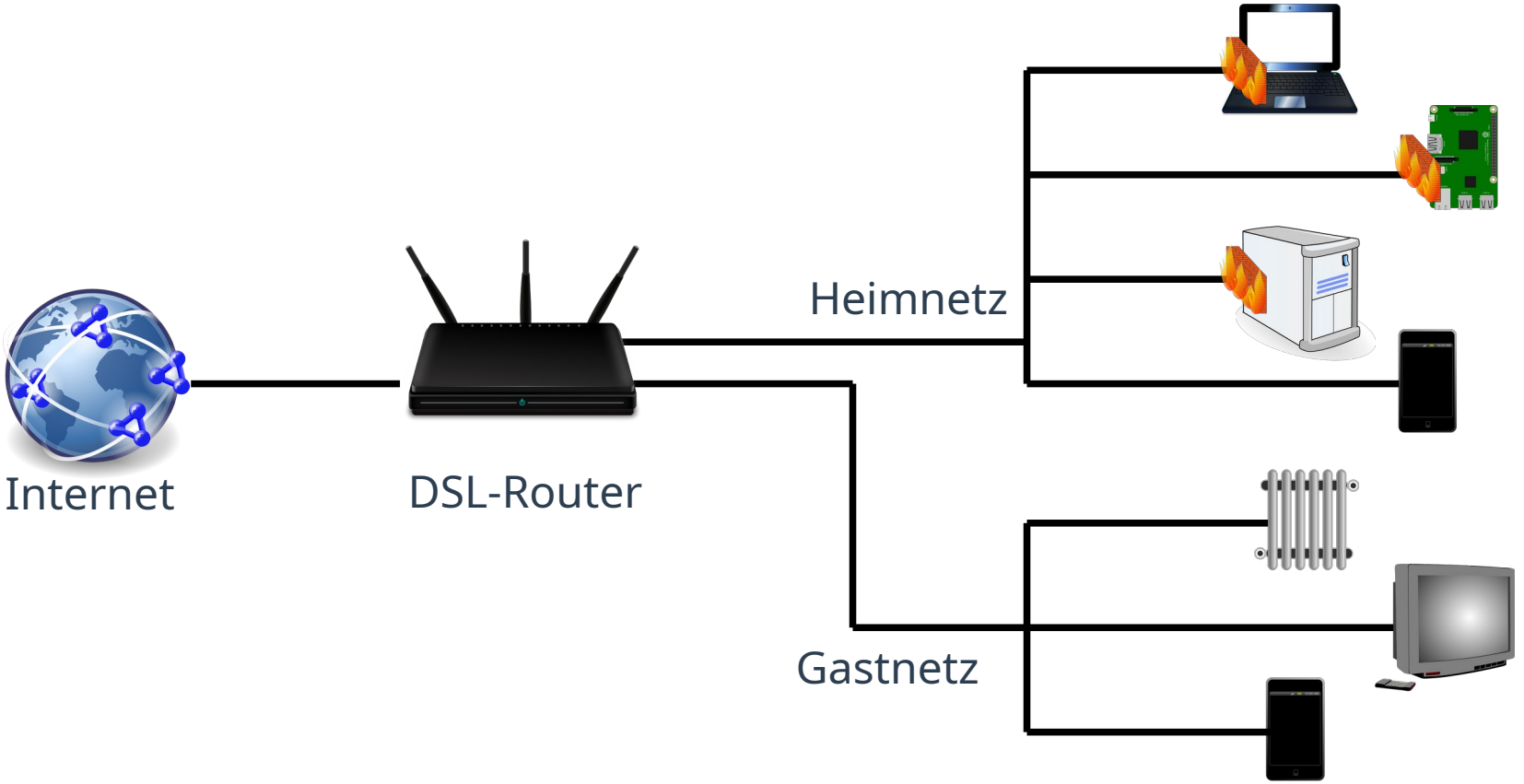
Minimallösung 2

- **Gast-WLAN / Gast-Netz des DSL-Routers nutzen**
- **Nachteile**
  - keine Verbindungen vom einen ins andere Netz
  - Will ich, dass alle Gadget Zugriff auf meine Heizungssteuerung haben?
  - Will ich, dass meine Gäste Zugriff auf alle Gadgets und meine Heizungssteuerung haben?

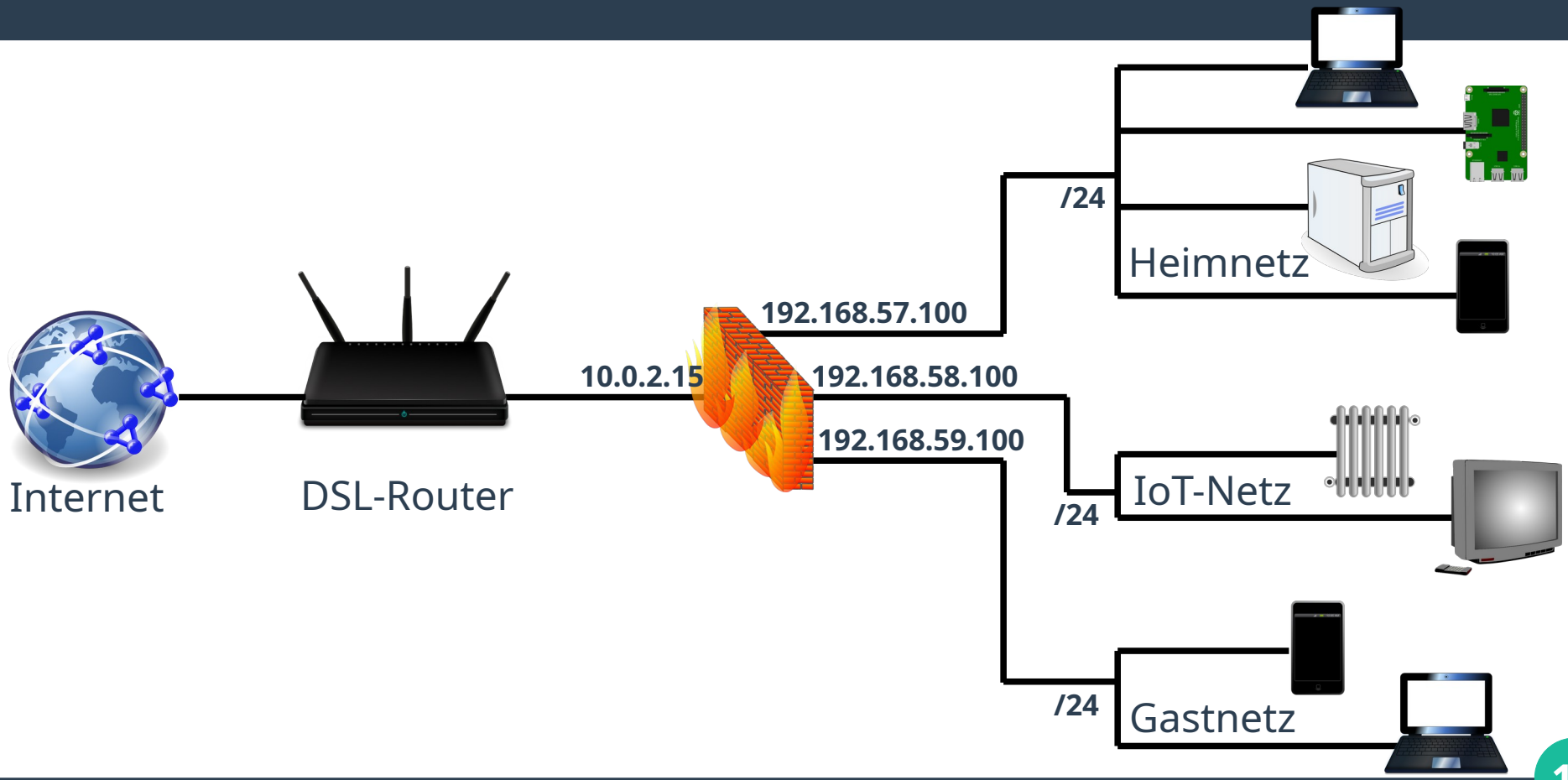
Minimallösung 2: Gastnetz



Minimallösung 2b: Gastnetz + lokale Firewall



Volle Kontrolle: Filtern an zentraler Stelle



Konfigurationsalternativen

Konfiguration über **Config-Files**

am Beispiel **Shorewall**

- kann in Git versioniert werden
  - Rollback auf letzten funktionierenden Stand sehr einfach
- kann per Ansible, Puppet, etc. auf das Gerät gebracht werden
  - Austausch der Hardware sehr einfach

Konfiguration per **GUI**

am Beispiel **OPNsense**

- einfacherer Einstieg

Demo-Time: Shorewall

```
apt install shorewall shorewall6
```

Sehr gut kommentierte Beispiele unter /usr/share/doc/shorewall/examples/

```
cp /usr/share/doc/shorewall/examples/three-interfaces/* /etc/shorewall
```

wenige Anpassungen an den Config-Files

```
systemctl start shorewall
```

Shorewall

Demo-Time

OPNsense

- Firewall- und Routing-Software auf Basis von FreeBSD mit Enterprise-Features (VLANs, VPNs, HA+HW Failover, …)
- Fork von pfSense seit 2014, v.a. durch Firma „Deciso“ entwickelt, FreeBSD-Lizenz
- Konfiguration per Web-Oberfläche oder API

OPNsense - Ressourcen-Anforderungen

- **Minimum: 1GHz Dual-Core CPU (x86-64), 3-4GB RAM, 10GB Disk, (+mehrere Ethernet-Ports und/oder WLAN)**
- **Hardware: z.B.**
  https://shop.opnsense.com/product-categorie/hardware-appliances/

OPNsense - Live-Demo

- **Web-Interface**
- **Firewall-Regeln**
  - Aliases (Achtung, werden zu IPs übersetzt!)
  - Auswertungs-Reihenfolge: 1. Quick-Regeln, 2. letzte passende Regel
  - Schedules
- **DHCP**

Links

- **Selbst ausprobieren?**
  Demo-Setup aus diesem Vortrag unter
  https://codeberg.org/booboo-at-gluga-de/firewall-playground-with-vagrant/


Noch Fragen?