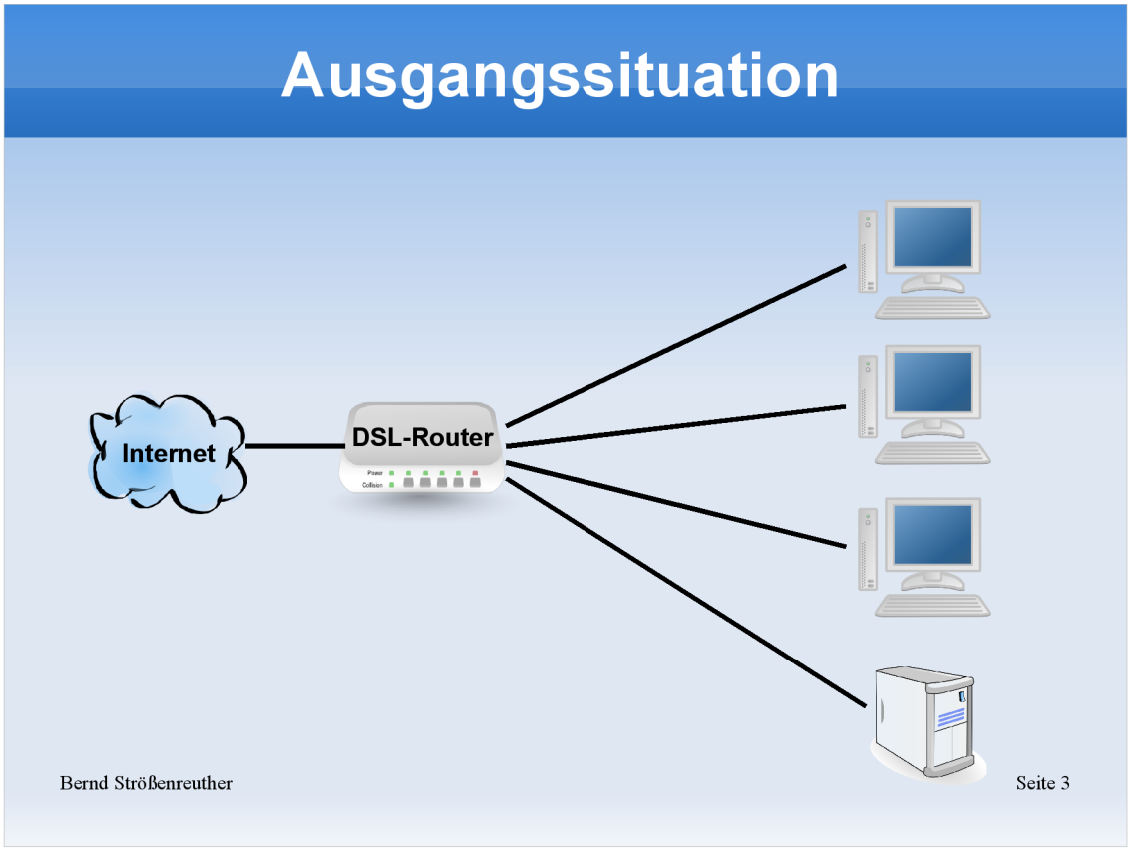
Firewall unter Linux

für Heimanwender
am Beispiel von Shorewall

Ubuntu-Users Nürnberg
2009-09-11

Referent:
Bernd Strößenreuther
<ubuntuusers@stroessenreuther.net>

Lizenz



DSL-Router
wenige PCs

Eingehende Verbindungen werden unterbunden
alle ausgehenden Verbindungen sind erlaubt
Schadsoftware darf frei nach Hause telefonieren, Spam verschicken, an DDoS-Angriffen teilnehmen, ...

Windows-PCs ohne getrennte Accounts für User und Administration dürfen als verseucht gelten (XP oder UAC) - Personal Firewall ist nicht mehr verläßlich

Home-Router
- auch für Schädlinge anfällig
- meist extrem wenig Konfigurationsmöglichkeiten
- schlecht Debug-Möglichkeiten

Was ist eine Firewall?

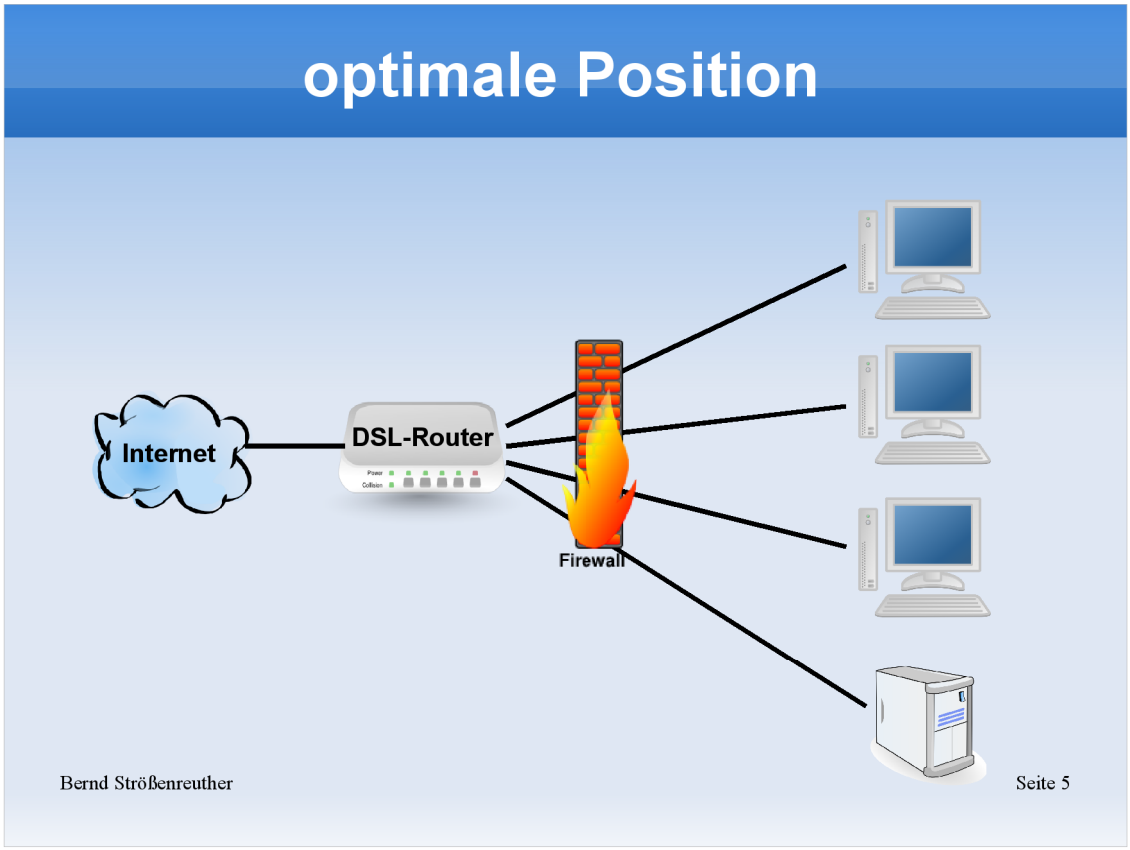
- Soft- oder Hardware, die in der Lage ist Netzwerkverkehr zu filtern
- Hardware: Router (mit mehreren Netzwerk-Interfaces) der Filterregeln umsetzen kann
- Software: Filterregeln laufen auf bestehender Hardware im IP-Stack mit

Linux: eigentlich immer iptables / netfilter

manuelle iptables-Konfiguration aufwändig, komplex und damit fehleranfällig

Details siehe z. B. ”Linux” - Galileo Computing Kap. 23.6
http://openbook.galileocomputing.de/linux/linux_kap23_006.htm#mj0ff6ad1f43cbb55350e27de3941f9778

Administration daher oft über Aufsätze wie z. B. Shorewall, Uncomplicated Firewall (ufw) sogar mit GUI (Gufw), fwbuilder (http://www.fwbuilder.org/) ebenfalls grafisch und für div. Firewalls



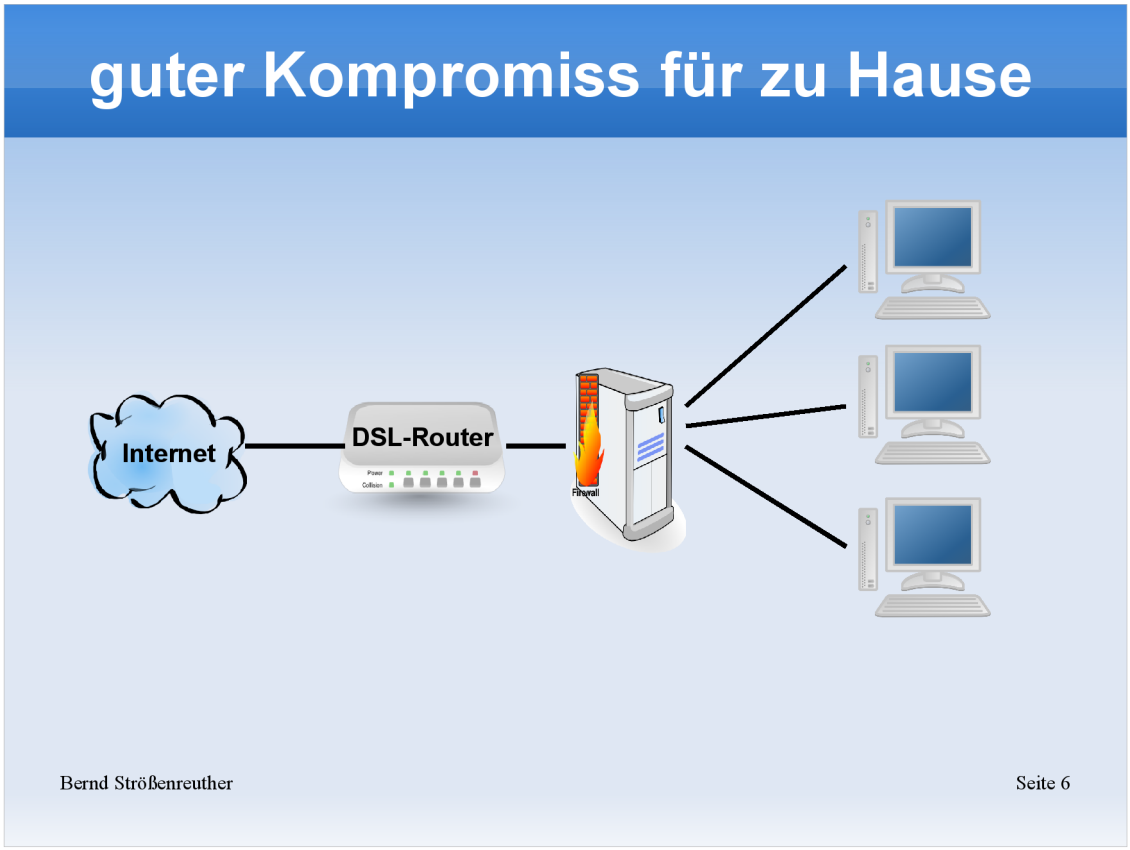
alle ein- und ausgehenden Verbindungen können kontrolliert werden

keine Möglichkeit für Schädlinge, die Firewall auszuhebeln oder zu umgehen

separate Hardware nötig

Proxies möglich als Application Level Firewall
Squid, FTP-Proxy, MTA (Postfix,...), ...

Standard-Linux-Distribution + z. b. Shorewall oder spezialisten: IPCop, Endian

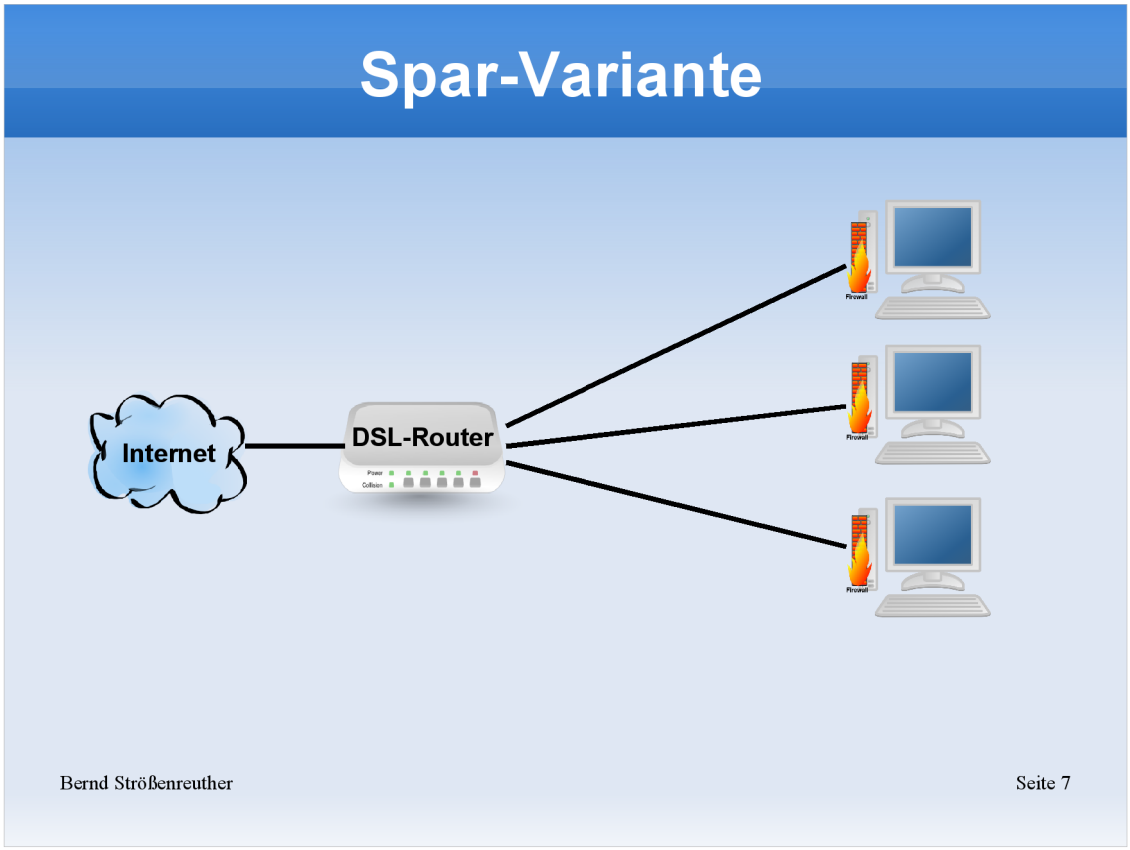


Firewall läuft am Server mit, sofern vorhanden

unter Linux kann hier z. B. shorewall zum Einsatz kommen (Aufsatz auf iptables)

ggf. in eigener virtueller Maschine

eigener Server (sparsame Hardware - 40 W) lohnt sich schon gegenüber z. B. einem dauerhaft laufenden NAS
- ähnlicher Stromverbrauch
- viel mehr Möglichkeiten



Firewall auf den Clients
-> auch hier ist shorewall (unter Linux) möglich

jeder Client ist einzeln zu konfigurieren

kann im Extermfall (Schädling erlangt root-Berechtigung) auch ausgehebelt werden

kaum Schutz für Windows-Clients, NAS-Systeme, ...

Konfigurationsbeispiel Shorewall (1)

```
aptitude install shorewall shorewall-doc
vi /etc/default/shorewall
   startup=1
cd /usr/share/doc/shorewall-common/examples
cd one-interface
cp * /etc/shorewall/
cd /etc/shorewall/
less interfaces
less policy
less zones
```

Konfigurationsbeispiel Shorewall (2)

```
vi rules
   # my own rules
   # allow incoming ssh
   ACCEPT    net    $FW    TCP     ssh
vi shorewall.conf
   STARTUP_ENABLED=Yes
/etc/init.d/shorewall start
tail -f /var/log/messages
iptables -L
```

ausgehende Verbindungen filtern

```
vi policy
   # reject outgoing traffic
   $FW   net   REJECT   info
vi rules
   # allow outgoing HTTP(S), DNS, SSH
   ACCEPT  $FW  net  TCP  http,https,domain,ssh
   ACCEPT  $FW  net  UDP  domain
/etc/init.d/shorewall restart
```

Literatur

- ”Linux” - Galileo Computing Kapitel 23.6 (http://openbook.galileocomputing.de/linux/linux_kap23_006.htm#mj0ff6ad1f43cbb55350e27de3941f9778 - direkter Link)
- FW-Builder (http://www.fwbuilder.org/) Linux-Magzin 12/2008 S. 75

Vielen Dank...

... für die Aufmerksamkeit

Noch Fragen?