# Themenabend Mauerbau

## *von schützenden Wänden und Tunneln*

Andreas Kretschmer <andreas_kretschmer@despammed.com>
Frank Becker <fb@alien8.de>
Mirko Swillus <mechko@gmx.de>
Tibor Varkonyi <tibyr@c3d2.de>

Chaostreff Dresden http://www.c3d2.de

2004-08-13

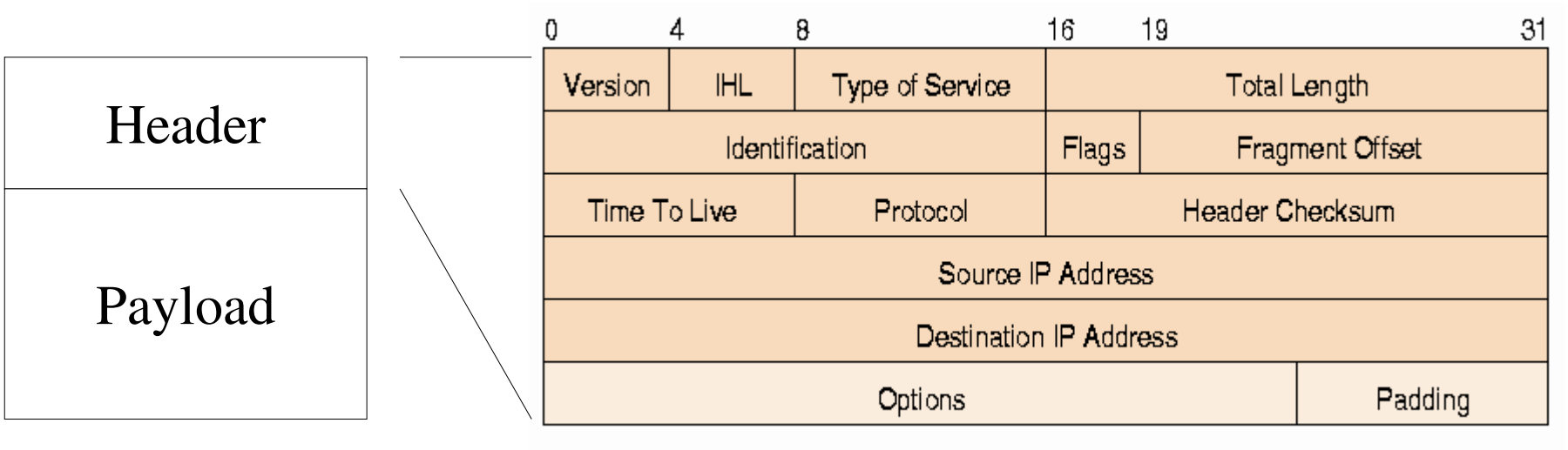
# Agenda

- Grundlagen
  - Internet (Film)
  - Was sind Firewalls?
- Linux-Firewalls
- pf/OpenBSD Firewalls
- Regelgeneratoren
- Tunnel

# Grundlagen

# Internet Protokoll: Pakete

http://www.freesoft.org/CIE/Course/Section3/7.htm

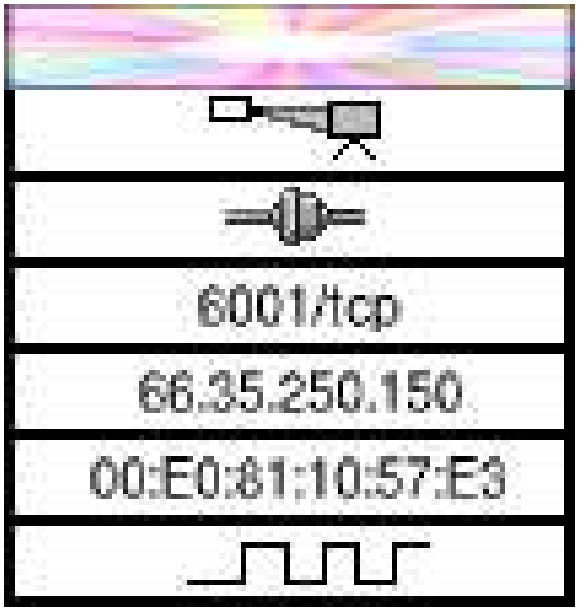



- Pakete bestehen aus
  - Header: Wohin, Woher, Was, andere Infos
  - Payload: Nutzdaten

# IP: Schichtenmodell

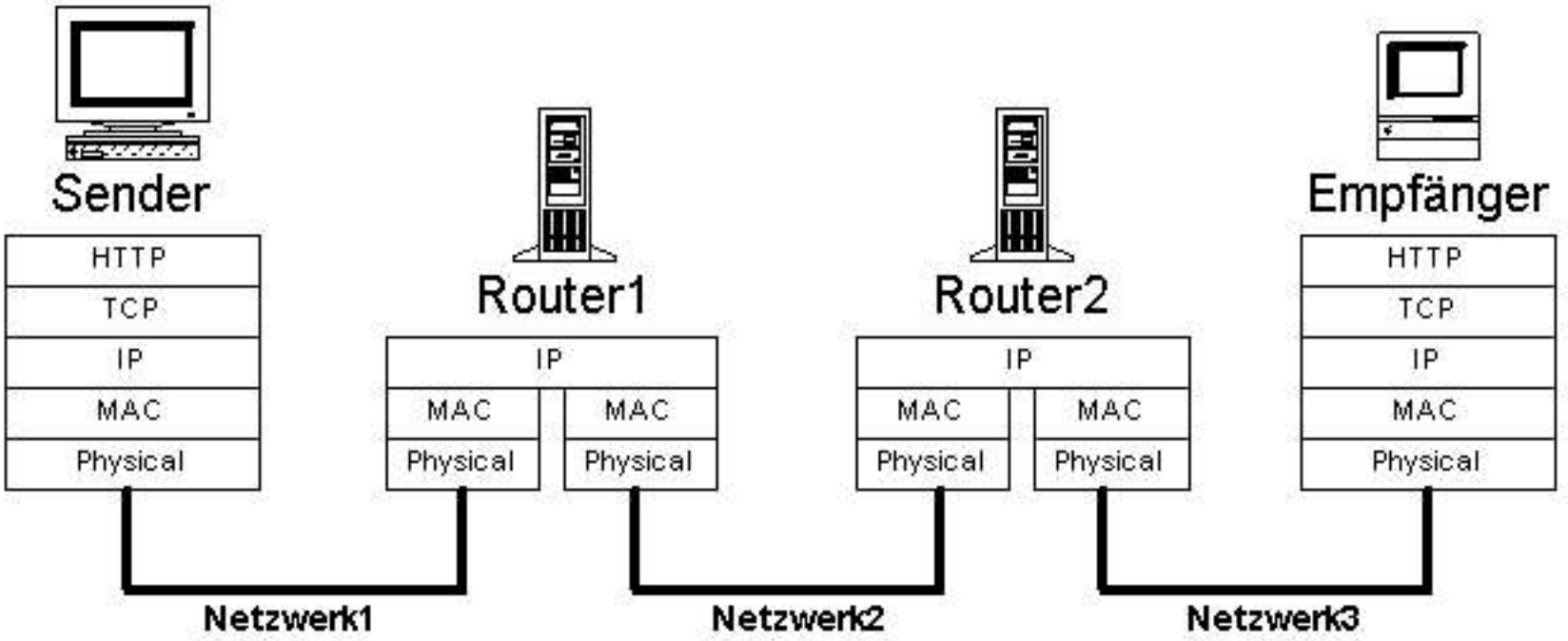
http://en.wikipedia.org/wiki/Internet_protocol_suite

| | | |
|---|---|---|
| | **Application** *"layer 7"* | e.g. HTTP, FTP, DNS *(routing protocols like RIP, which for obscure reasons run over UDP, may also be considered part of the network layer)* |
| 4 | **Transport** | e.g. TCP, UDP, RTP, SCTP *(routing protocols like OSPF, which run over IP, may also be considered part of the Network layer)* |
| 3 | **Network** | For TCP/IP this is the Internet Protocol (IP) *(required protocols like ICMP and IGMP run over IP, but may still be considered part of the network layer; ARP does not run over IP)* |
| 2 | **Data Link** | e.g. Ethernet, Token ring, etc. |
| 1 | **Physical** | e.g. physical media, and encoding techniques, T1, E1 |



# IP-Pakete: Der Weg durch's Netz

http://de.wikipedia.org/wiki/IP-Adresse



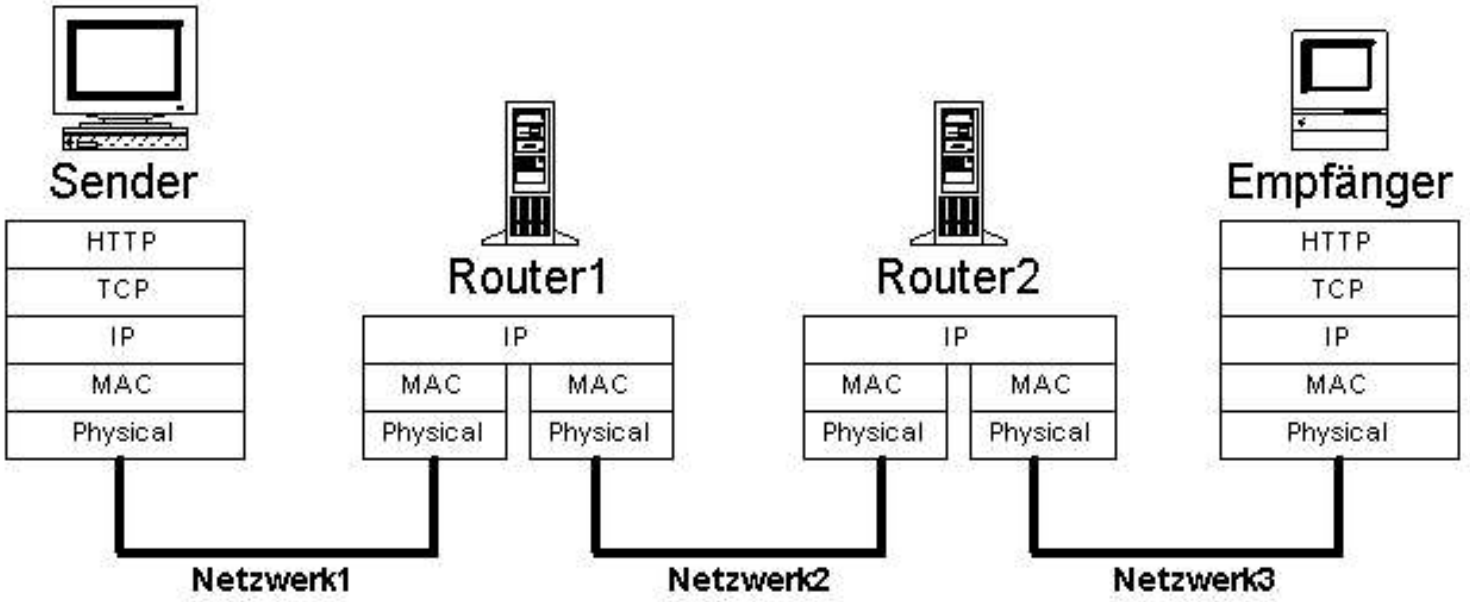
# Film

# Firewalls: Begriffe

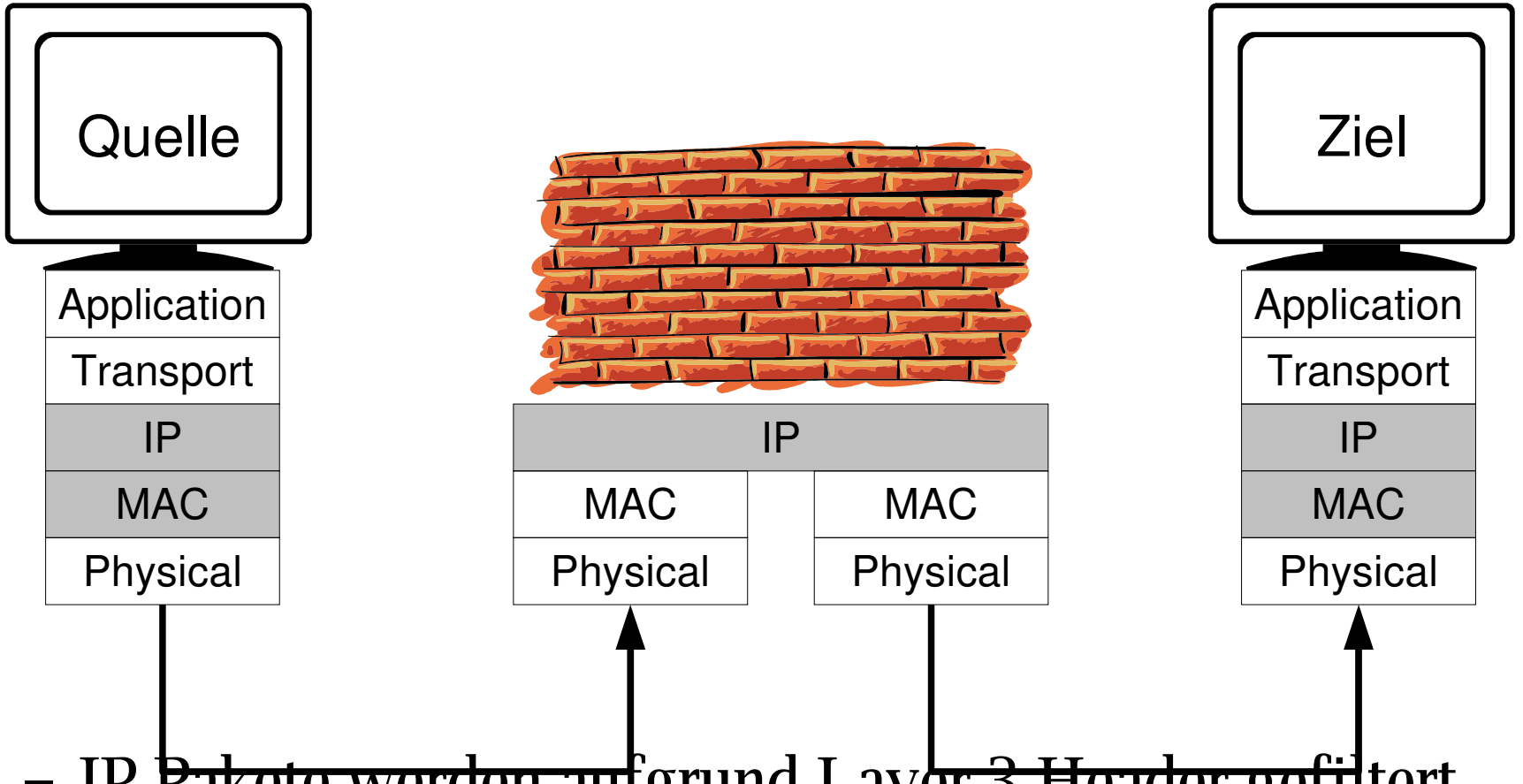
- Router
- Paket Filter
- NAT-Gateway
- NAPT
- Application Layer Gateway / Proxies

# Router

- schickt IP-Pakete durch das Netz
  - kann Pakete verwerfen
  - kann Pakete zu eingestellten Hosts routen

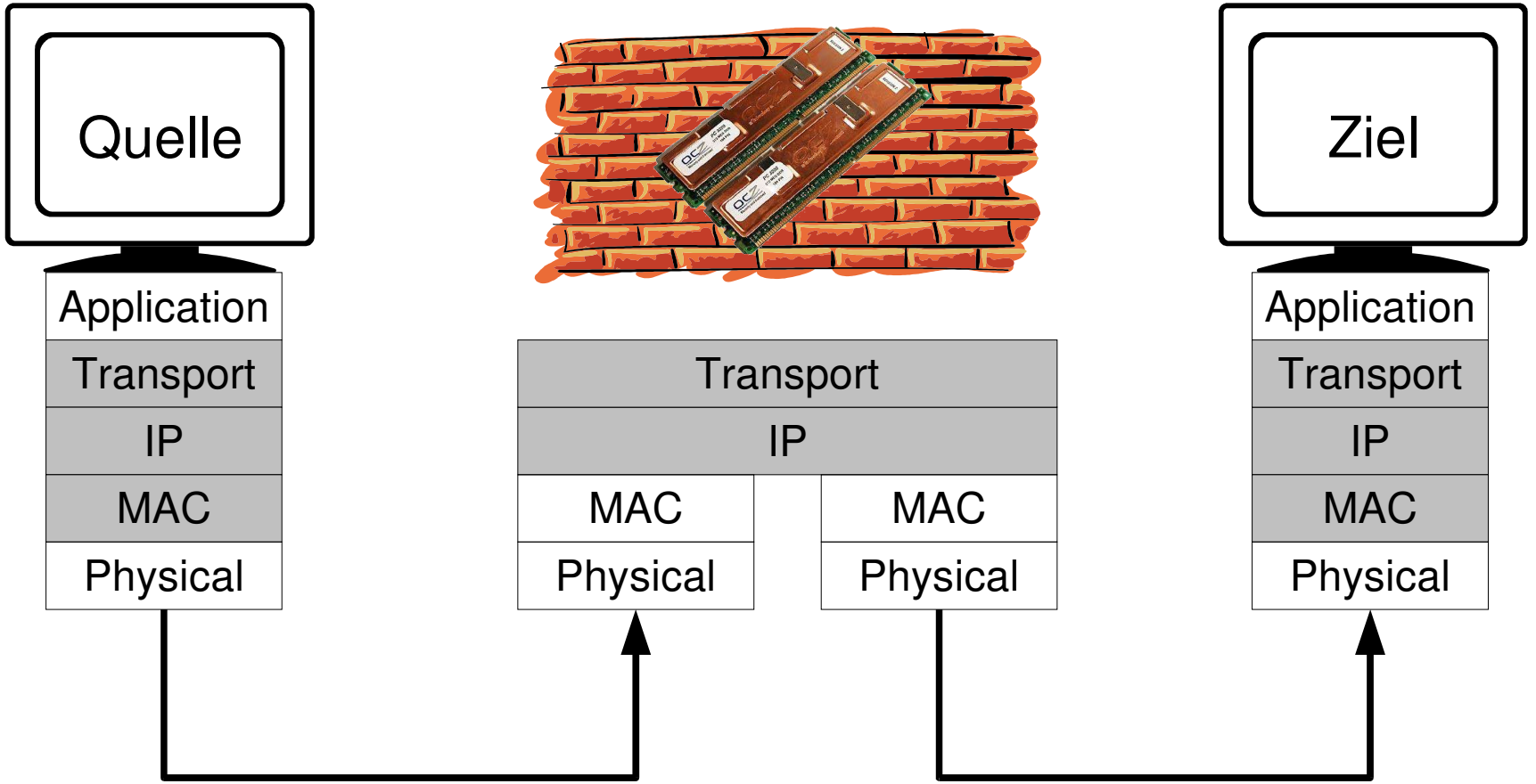


# Stateless Paket Filter



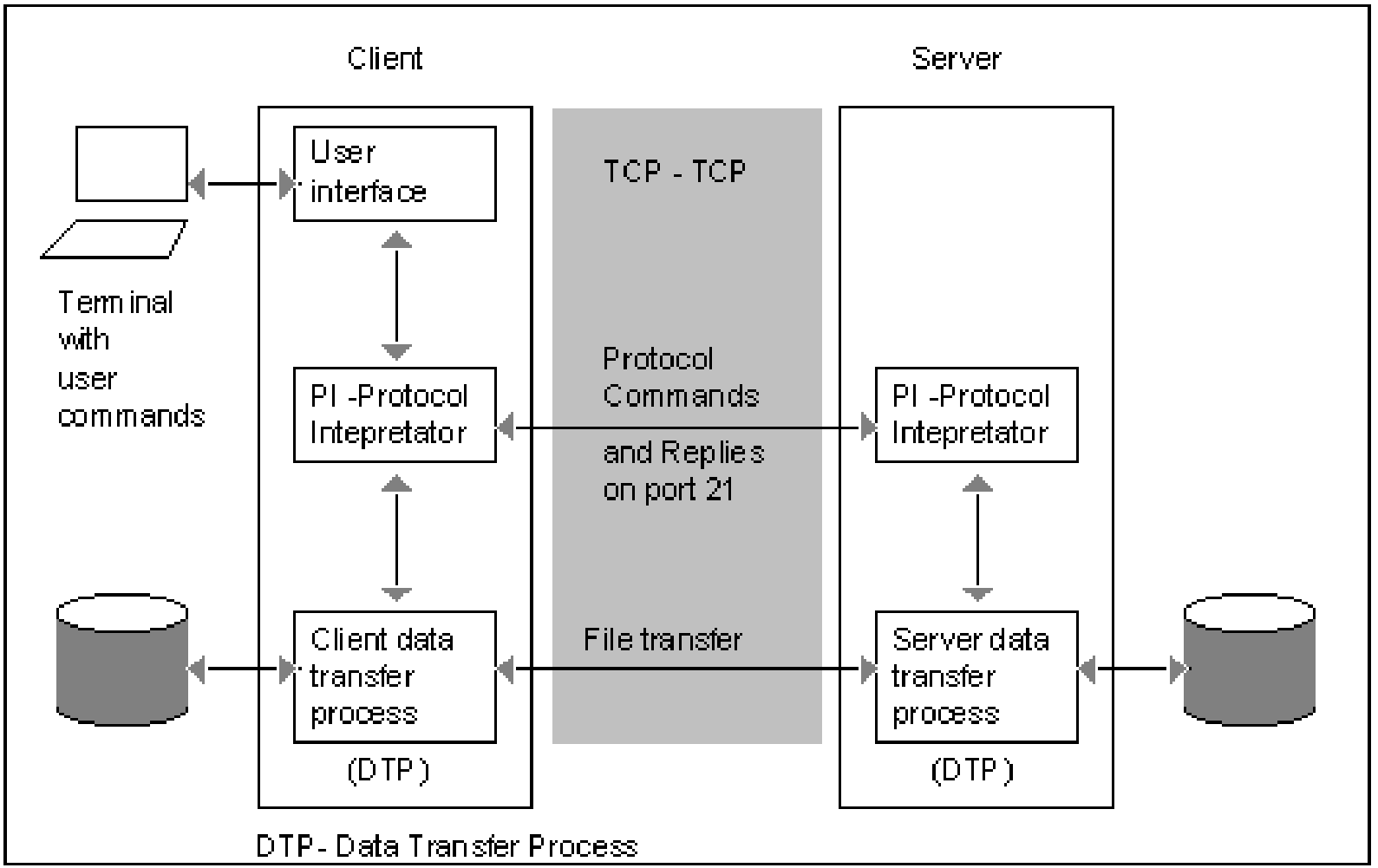

- IP Pakete werden aufgrund Layer 3 Header gefiltert
- kein Zusammenhang zwischen mehreren Paketen
- Bsp: ACK-Telnet Daemon von THC

# Stateful Paket Filter

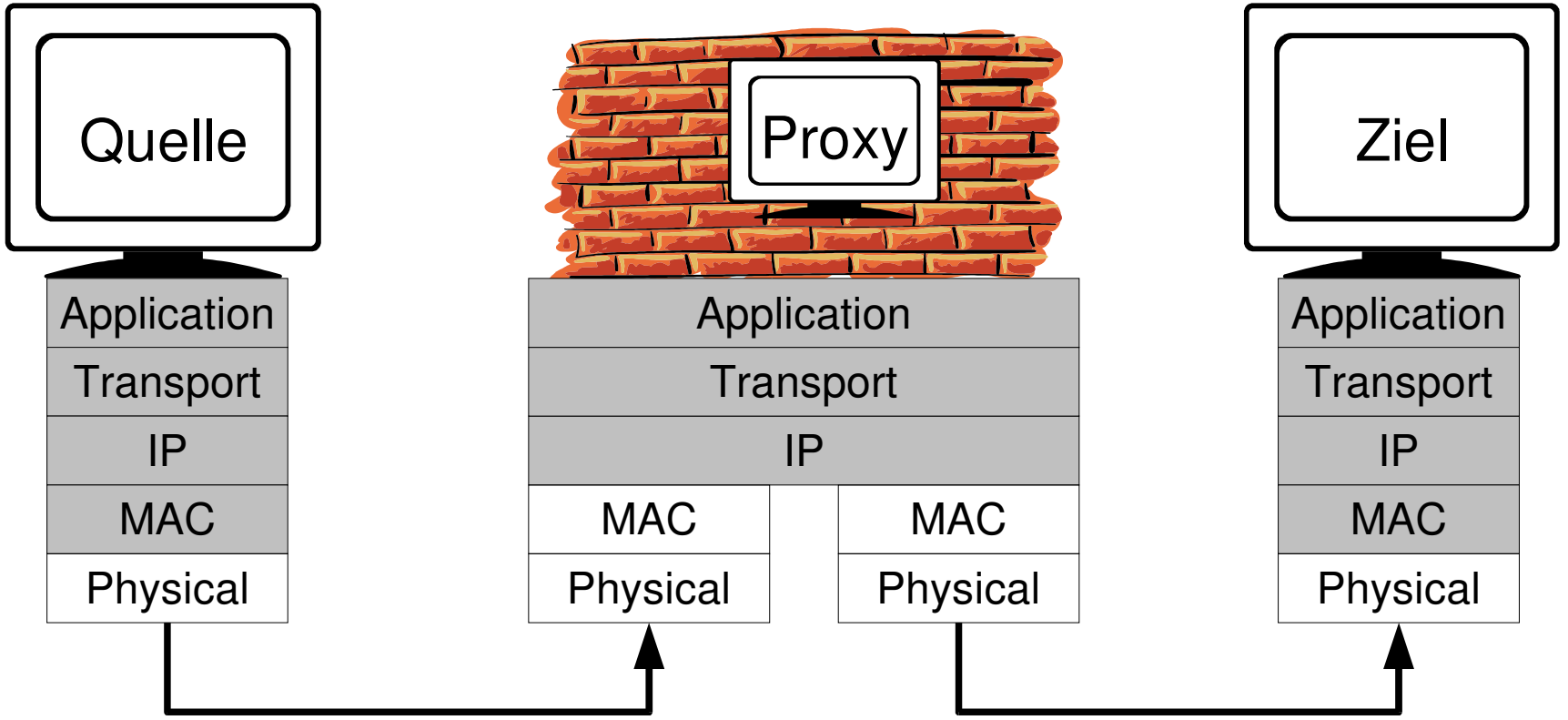



- IP Pakete werden aufgrund Layer 3&4 Header gefiltert
- Paketfilter merkt sich Zustand der Verbindungen, beliebtes Bsp: ftp

# Stateful Protokoll Bsp: ftp



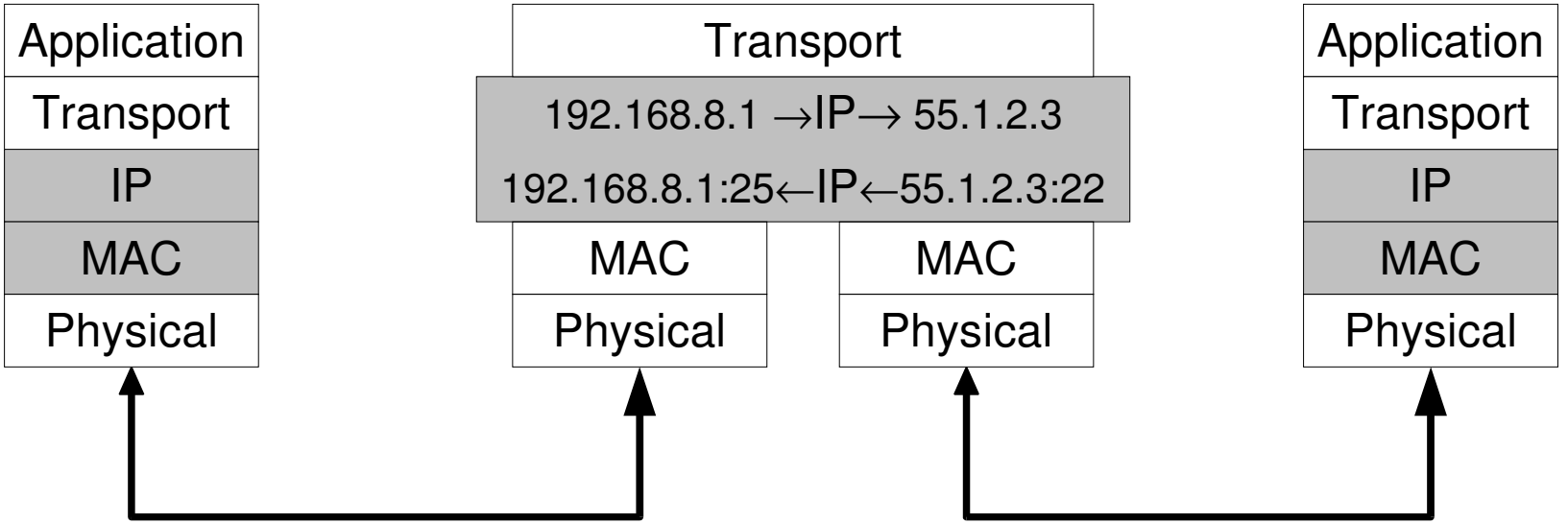
# Application Layer Gateway / Proxy



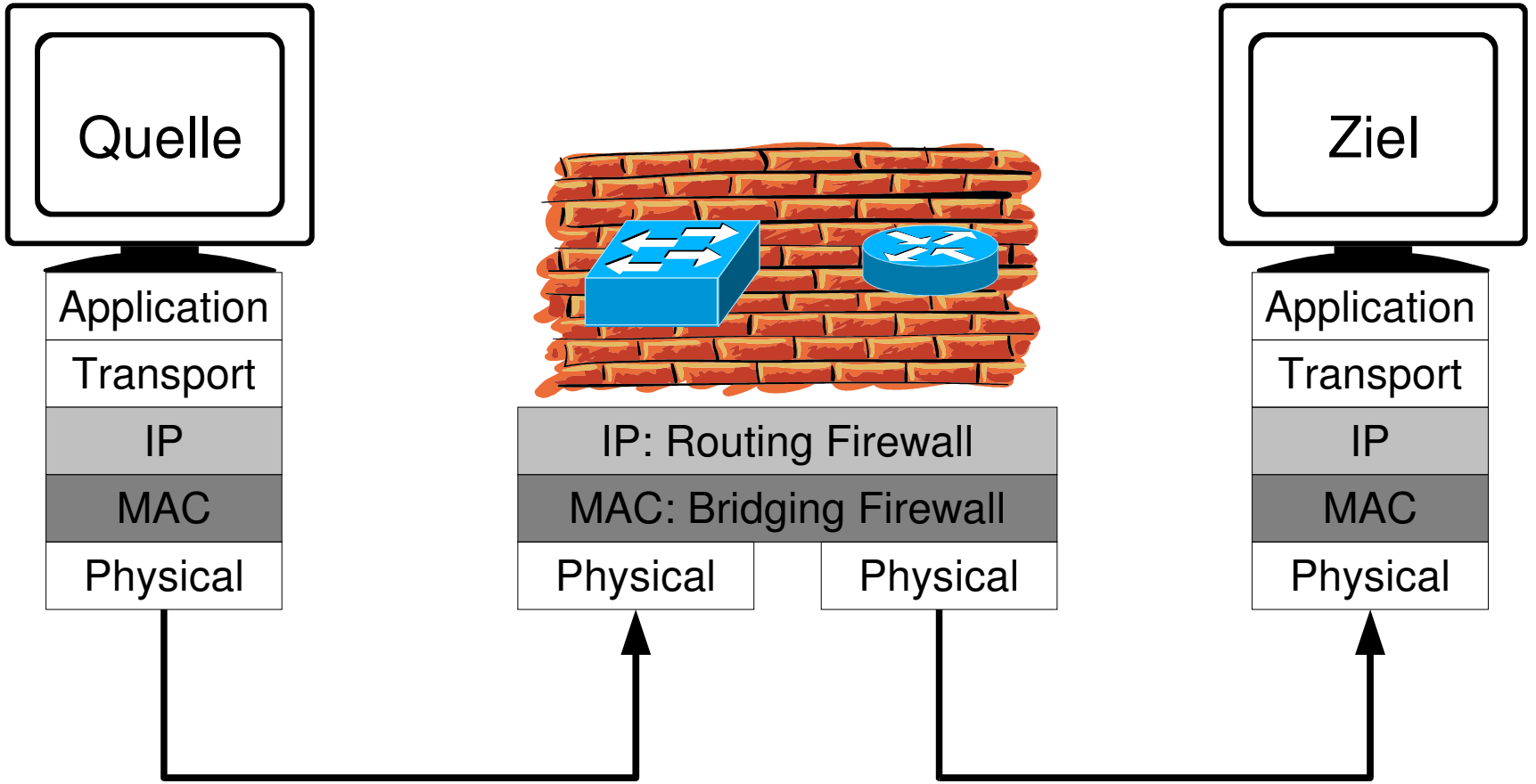

- Proxy spricht Layer 7 - Protokoll
- Proxy übernimmt stellvertretend für Quelle Kommunikation mit Ziel
- optional, erzwungen oder transparent möglich (TRACE für Web)

# NAT / NAPT / Masquerading

- Private RFC 1918 Adressen (nicht im Internet geroutet)
- Masquerading: alles hinter einer IP „versteckt“
- NAT: Network Adress Translation
- NAPT: Network and Port Translation



# Bridging vs. Routing Firewall




- Unterschiedlicher Netzwerklayer
- Vorteil von Bridging FW: transparent (da auf MAC)

# Layer 7 Classifier

http://l7-filter.sourceforge.net/

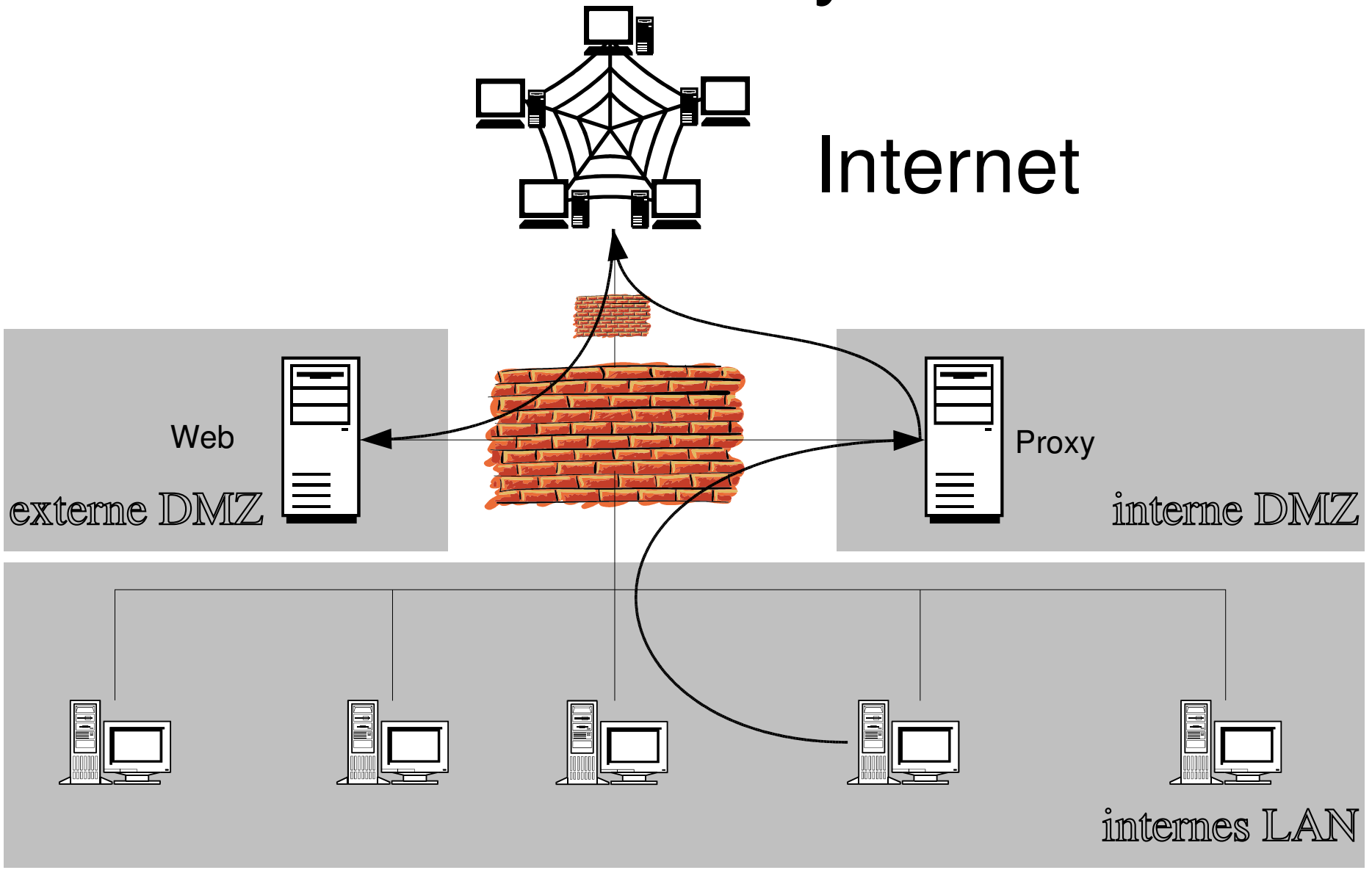
- Reguläre Ausdrücke auf Layer 7 um Protokolle zu erkennen
- besteht aus:
  - Kernel Patch
  - netfilter/iptables Patch
  - Reguläre Ausdrücke zur Protokoll-Klassifikation

# Firewall Design Principles

Building Internet Firewalls (O'Reilly, 2nd edition, 2000)

- geringste Privilegien (least Privileges)
- **K**eep **I**t **S**imple **S**tupid
- Defense in Depth / Diversity of Defense:
  *Verlasse Dich nie auf nur einen Mechanismus!*
  *Verlasse Dich nie auf nur ein System!*
- Choke Point: alles muss durch die Firewall
- ein System für eine Aufgabe
- Fail-Safe (Was ist im Fehlerfall?)
- Grundregel: alles verboten, explizit Traffic erlauben

# Firewall Netzwerk-Layout

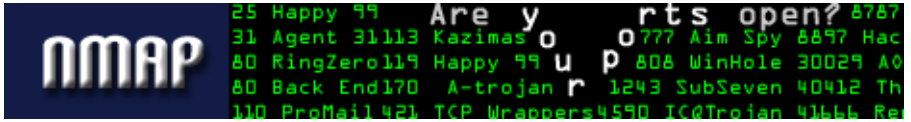


# Personal Firewalls

- Rundumschutz auf Desktoprechnern

# Meinungen?

# Firewall Tests




- Portscanner:
  - versucht sich auf alle Ports zu verbinden (und mehr)
    - TCP
    - UDP
- Standard: nmap
  http://www.insecure.org/nmap
- man nmap


- http://www.linux-magazin.de/Artikel/ausgabe/2000/12/SnortNmap/SnortNmap.html

# netfilter/iptables

Andreas Kretschmer

# Der Paketfilter pf

tibyr

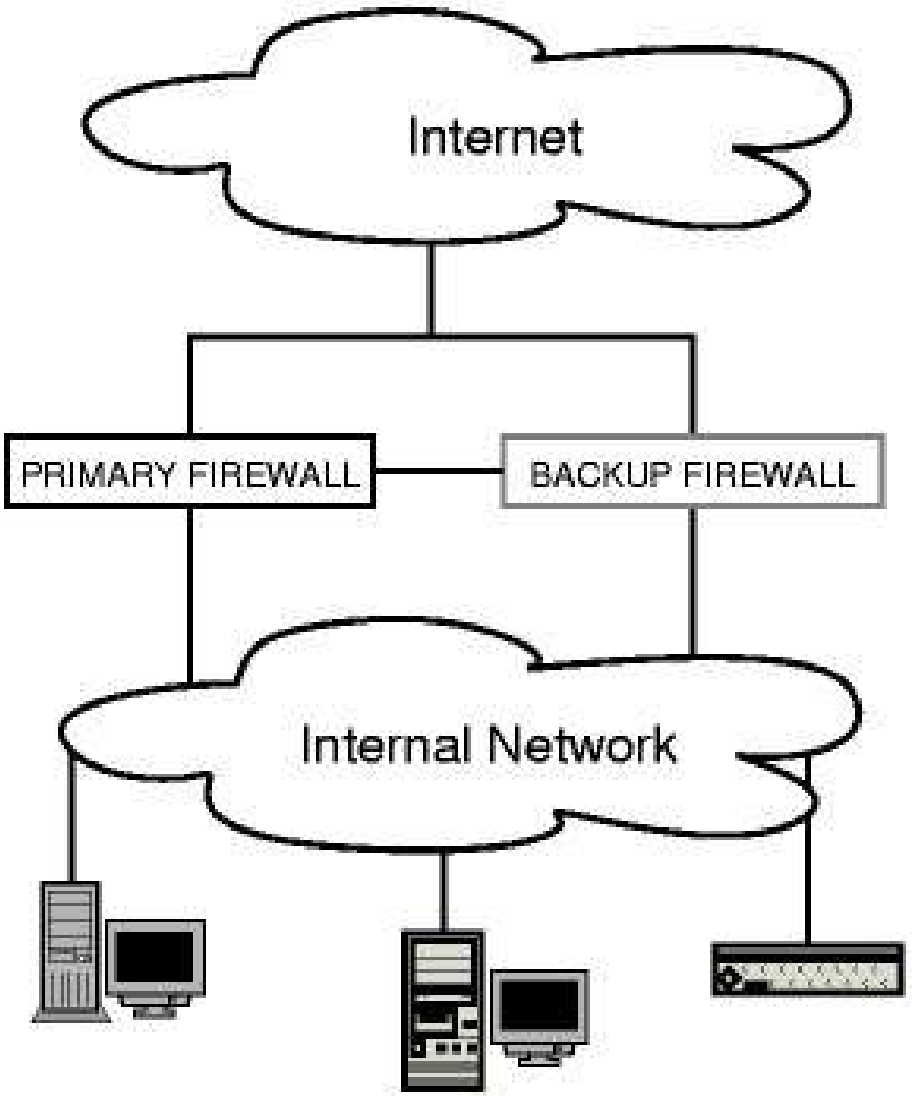
# Hot-Standby Firewall mit carp/pfsync unter OpenBSD

# Redundante Firewalls mit OpenBSD

http://www.countersiege.com/doc/pfsync-carp/

- Motivation:
  - Wenn eine Firewall (Choke Point) ausfällt, ist das Netz weg; single point of failure
  - zweite Kiste hot-standby aufstellen (muss automatisch umschalten)
  - States der Regeln müssen auf allen Cluster-Mitgliedern gleich synchronisiert sein
  - Upgrades möglich ohne Service-Unterbrechung
- Lösung mit carp (seit OpenBSD 3.5) und pfsync (seit OpenBSD 3.3)
- FreeX Ausgabe: 4' 2004

# Prinzip


Internet
PRIMARY FIREWALL
BACKUP FIREWALL
Internal Network

# Tools: CARP

- **C**ommon **A**ddress **R**edundancy **P**rotocol (IP 112)
  - Wie
    - alle Hosts teilen sich virtuelle IP-Adressen (VIP)
    - eine gemeinsame MAC für diese IP-Adressen
    - Master sendet kontinuierlich „Advertisements“
    - Wenn Slave keine „Advertisements“ mehr „hört“, übernimmt er und sendet sie selbst
  - Preemption: Verbindungen auf einer vorbestimmten Firewall
  - IPv6: ja
  - arpbalance: load-balancing mögl. (jeder host eine MAC)

# Tools: pfsync

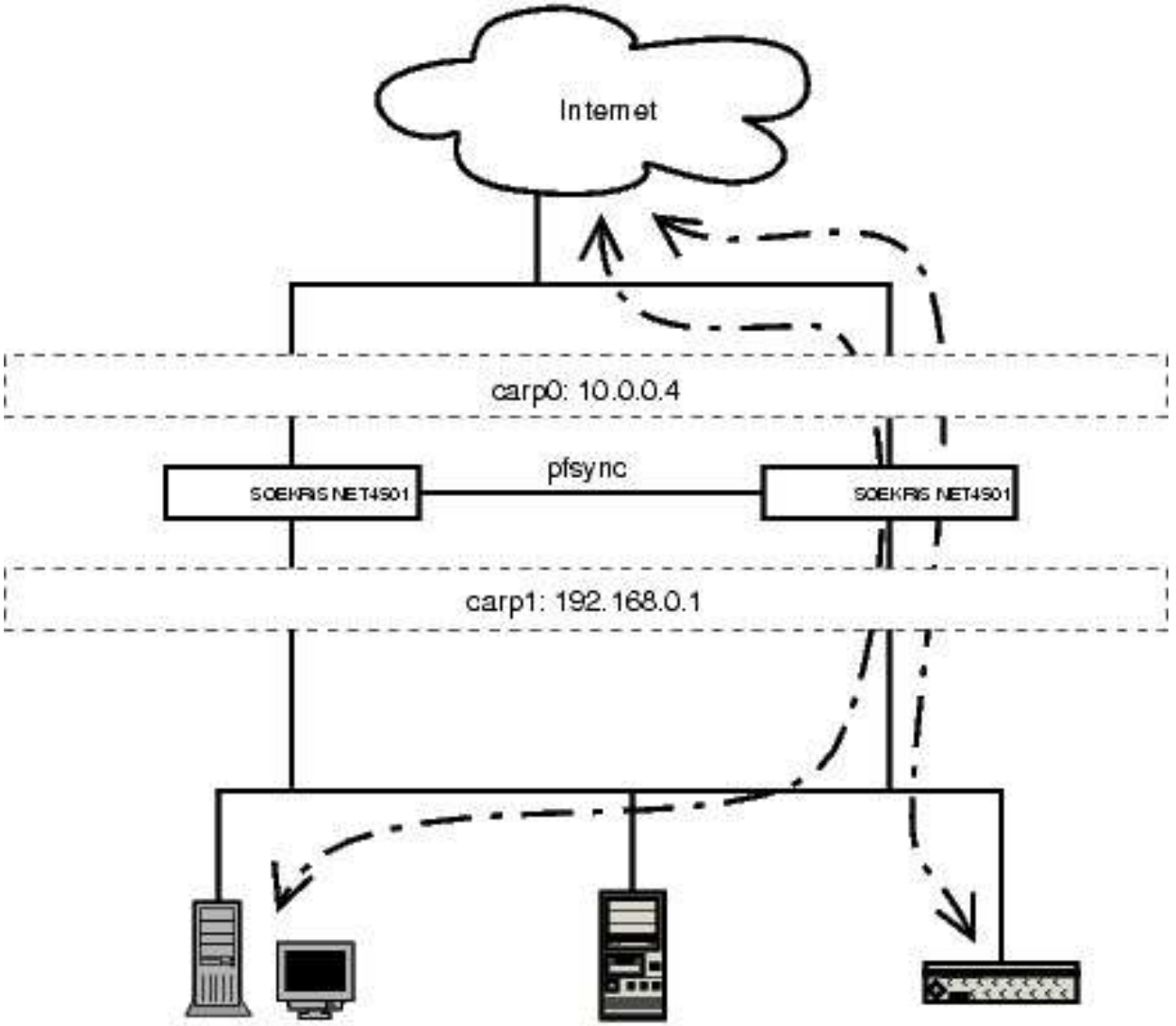
- PFSYNC Protokoll (IP 240)
  - states einfügen, update und löschen
  - jede FW sendet multicasts
  - Achtung: wegen Geschwindigkeit keine Authentifizierung oder Verschlüsselung der Pakete -> Eigenes physikalisches Netz verwenden (oder evtl. Tunnel)!!
- Sync-Traffic linear zu Verbindungen

# einfaches Beispiel

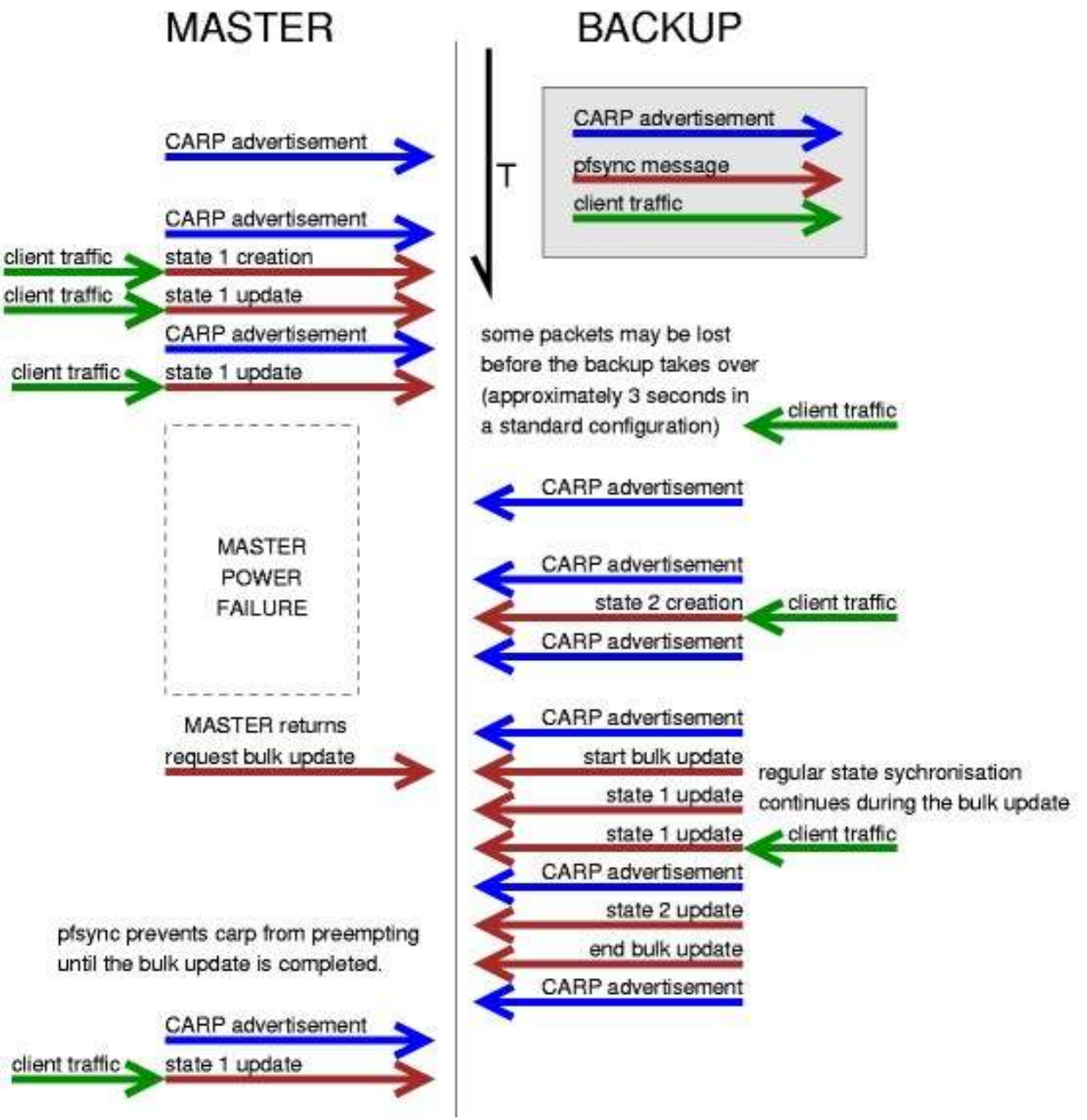
VIP ext

Firewalls

VIP int



# Failover


MASTER
BACKUP
T
CARP advertisement
pfsync message
client traffic
CARP advertisement
client traffic
state 1 creation
client traffic
state 1 update
CARP advertisement
client traffic
state 1 update
some packets may be lost
before the backup takes over
(approximately 3 seconds in
a standard configuration)
client traffic
CARP advertisement
MASTER
POWER
FAILURE
CARP advertisement
state 2 creation
client traffic
CARP advertisement
MASTER returns
request bulk update
CARP advertisement
start bulk update
regular state sychronisation
continues during the bulk update
state 1 update
state 1 update
client traffic
CARP advertisement
state 2 update
end bulk update
CARP advertisement
pfsync prevents carp from preempting
until the bulk update is completed.
CARP advertisement
client traffic
state 1 update

# Skalierbarkeit

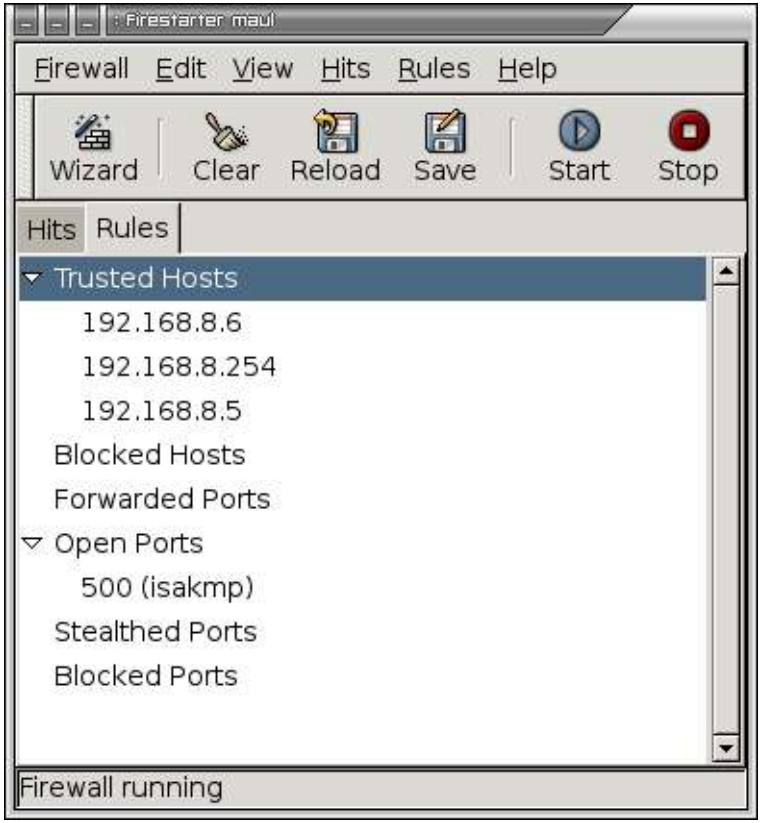
- kein Host-Limit im Protokoll
- Tests:
  - http://www.countersiege.com/doc/pfsync-carp/
    4 Hosts, gemischt: i386, Sprarc, Sparc64, AMD64
    -> keine Session verloren gegangen in 4 Tagen Test
  - 2x PCs
    - in Wochen keine Probleme

# Firewall-Rule Generatoren

# Firestarter

http://firestarter.sourceforge.net/

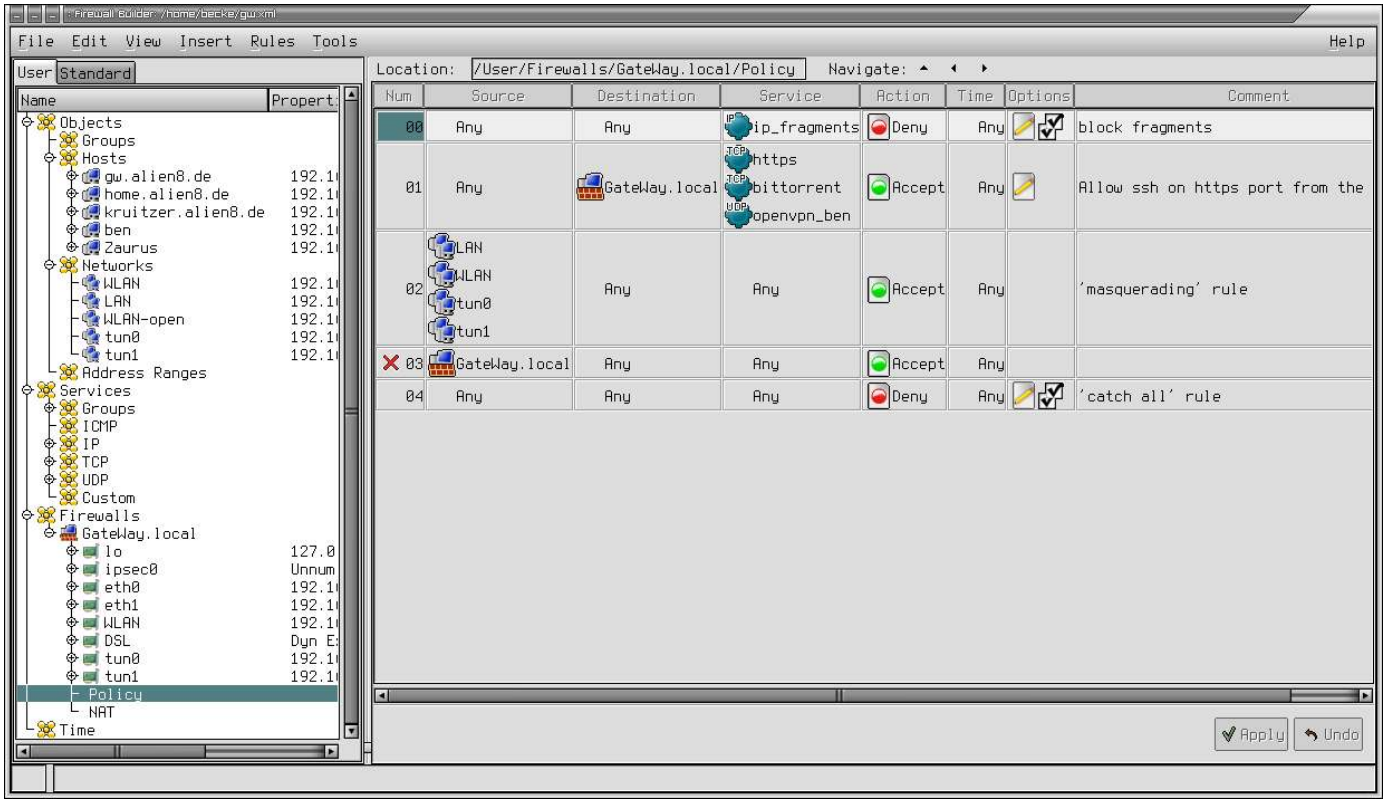
- „Personal Firewall“ für Linux



# FWBuilder

http://firestarter.sourceforge.net/

- GUI für:
  - Linux
  - WinXP
  - Cisco PIX
  - OpenBSD




- auch für Win verfügbar

# Shorewall

# Mechko

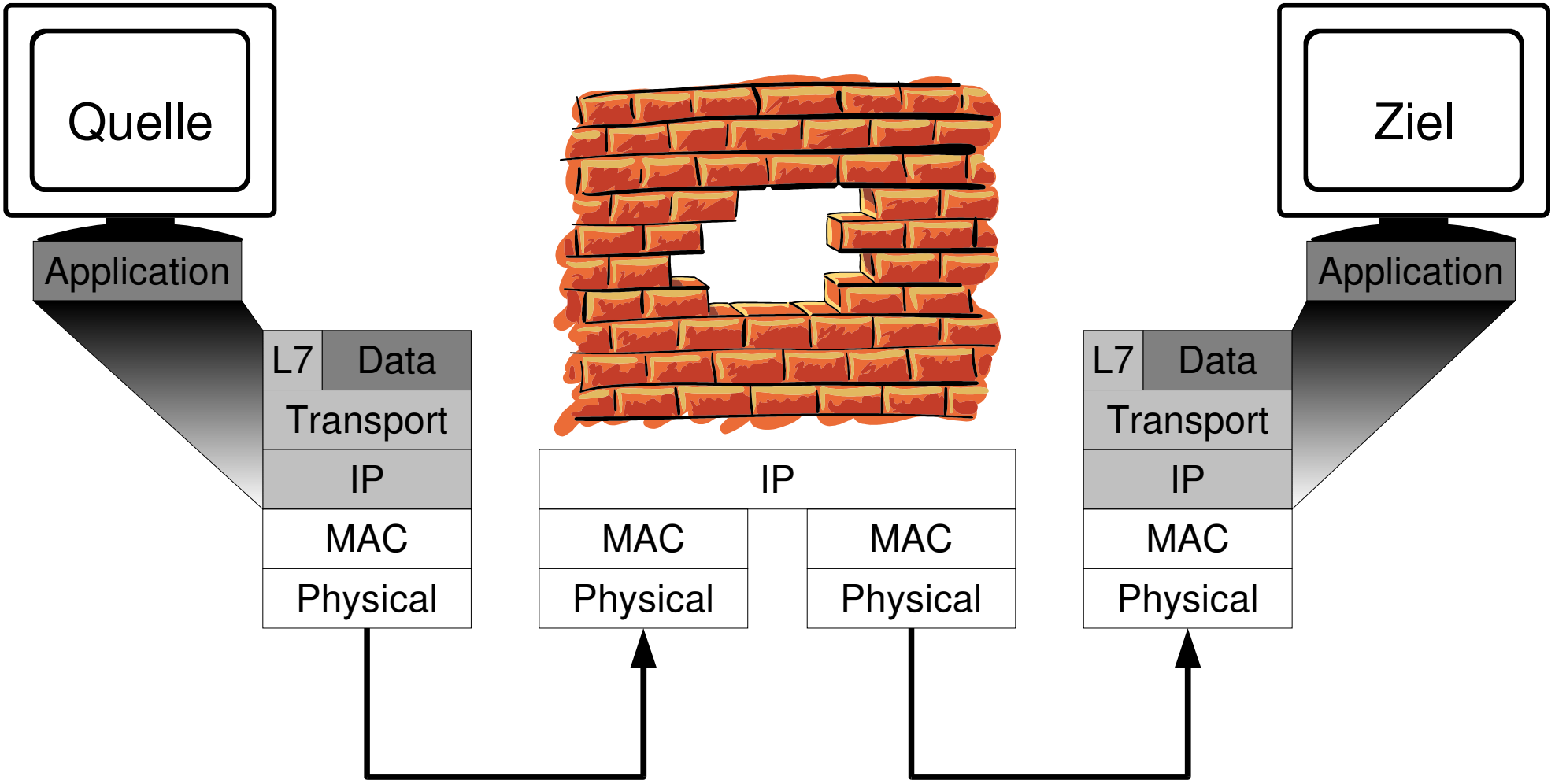
# Tunnel

*Das Internet ist fehlertolerant. Filter wertet es als Fehler und arbeitet um diese herum.* weissnichtvonwemdaswar

# Tunnel

- Nutzdaten in gestattetes Kommunikaitons-Protokoll „einbetten“
- kreativer Umgang mit Protokollen
- Bsp:
  - HTTPS/Connect - ACK Tunnel
  - HTTP - DNS
  - SSH - ICMP

# Tunnel allgemein

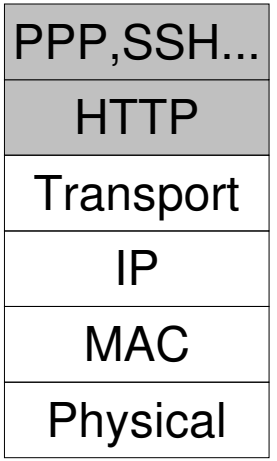


# Connect:// durch den Web-Proxy

- HTTPS nutzt CONNECT host.tld:Port
- verschlüsselte Ende zu Ende Verbindung: Proxy kann nicht in Pakete reinsehen
- d. h. kleiner Wrapper, der vorher noch CONNECT sagt
- Software:
  - Putty
  - OpenSSH: .ssh/config
    - `ProxyCommand /usr/local/bin/proxytunnel -g proxy -G 3128 \ -d ziel -D 443`
  - $SUCHMASCHINE (z. B. stunnel, proxytunnel)
- PPP over SSH Howto (Achtung vermeide TCP over TCP)

# HTTP-Tunnel


- Client redet mit Server http (GET, POST ...)
- Übertragen wird überlagertes Protokoll z. B.:
  - ssh, PPP, http ;)
- Software: GNU httptunnel (nur eine Verbindung möglich)
- Advanced HTTP-Tunnel:
  - verstecken des Datenstromes in HEAD Zeilen
- Shell über Web (Java, CGI, PHP, Perl)



# GNU httptunnel: Beispiel

- Server: `hts -w -F localhost:22 80`
- Client: `htc -F 1234 -P proxy:74 -B64k server:80`
  `ssh localhost -p 1234`
- Proxy:

1092305632.692 24025 172.20.18.7 TCP_MISS/200 4331 GET http://server/index.html? - DIRECT/1.2.3.4 text/html ALLOW

- tcpdump:

```
GET http://server:80/index.html?crap=1092313481 HTTP/1.1
Host: server:80
Connection: close
```

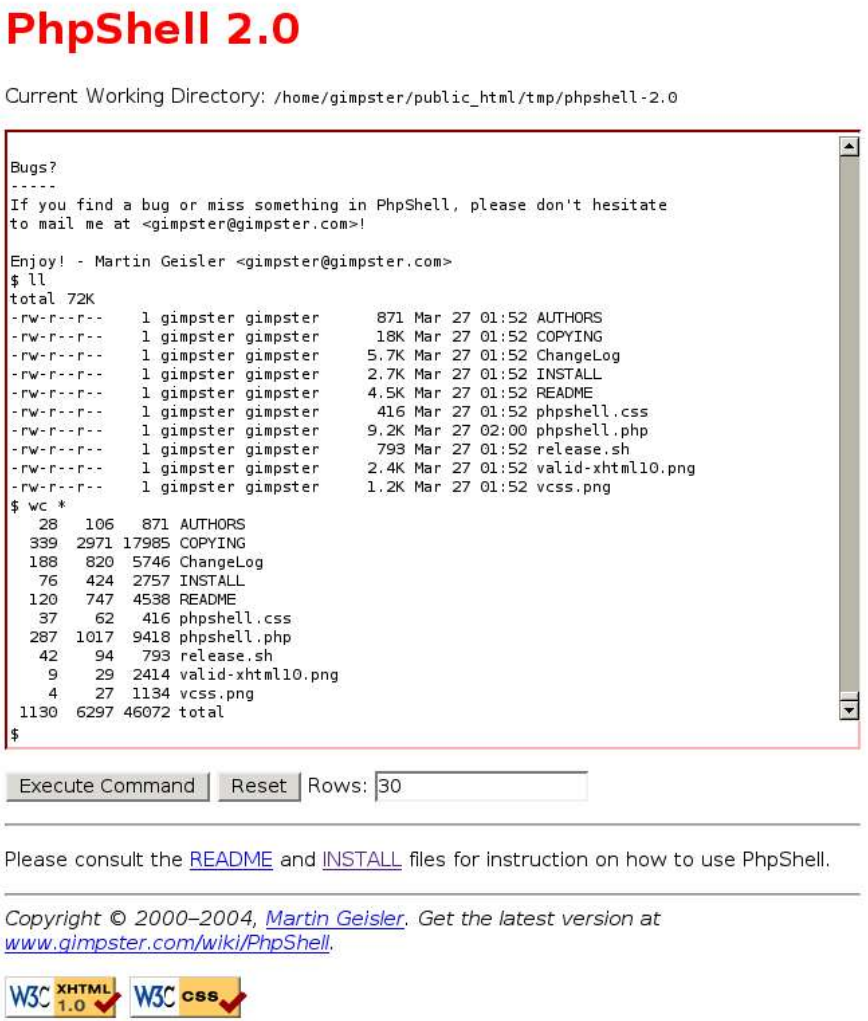
```
HTTP/1.0 200 OK
Content-Length: 102400
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate
Expires: 0
Content-Type: text/html
X-Cache: MISS from proxy
X-Cache-Lookup: MISS from proxy:74
Proxy-Connection: close

..'SSH-2.0-OpenSSH_3.8p1 Debian 1:3.8p1-3


.
.
`...\..ÇÈÀœÁó.UÁ.Û3Xjè*...=diffie-
```

# Beispiel: PHPShell

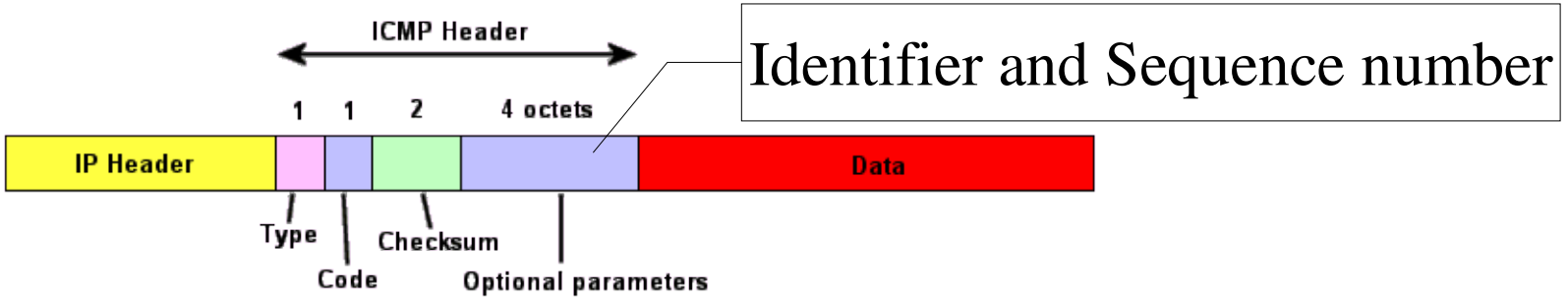
http://www.gimpster.com/wiki/PhpShell



# SSH


- Port-forwarding
- Wenn Firewall nur auf Layer 3 arbeitet
- Bsp:
  - `ssh -2 -N -f -L3306:localhost:3306 user@host`
    - -2 Protokoll in Version 2
    - -N kein Kommando remote ausführen
    - -f ssh im den Hintergrund schicken
    - -L localport:zielhost:zielport
- Remote Port-forwarding: man ssh

# ICMP-Tunnel




- ICMP-Pakete haben einen Data-Bereich der ist meist ungenutzt ... Guess u got it.
- Mehr zu icmp: RFC 792
  http://www.just2good.co.uk/index.php?ITFrameSet.php?ICMP.htm
- Software:
  - icmptunnel (kompiliert nicht mehr)
  - itunnel (Proof of concept, siehe Bsp.)

# itunnel: Beispiel

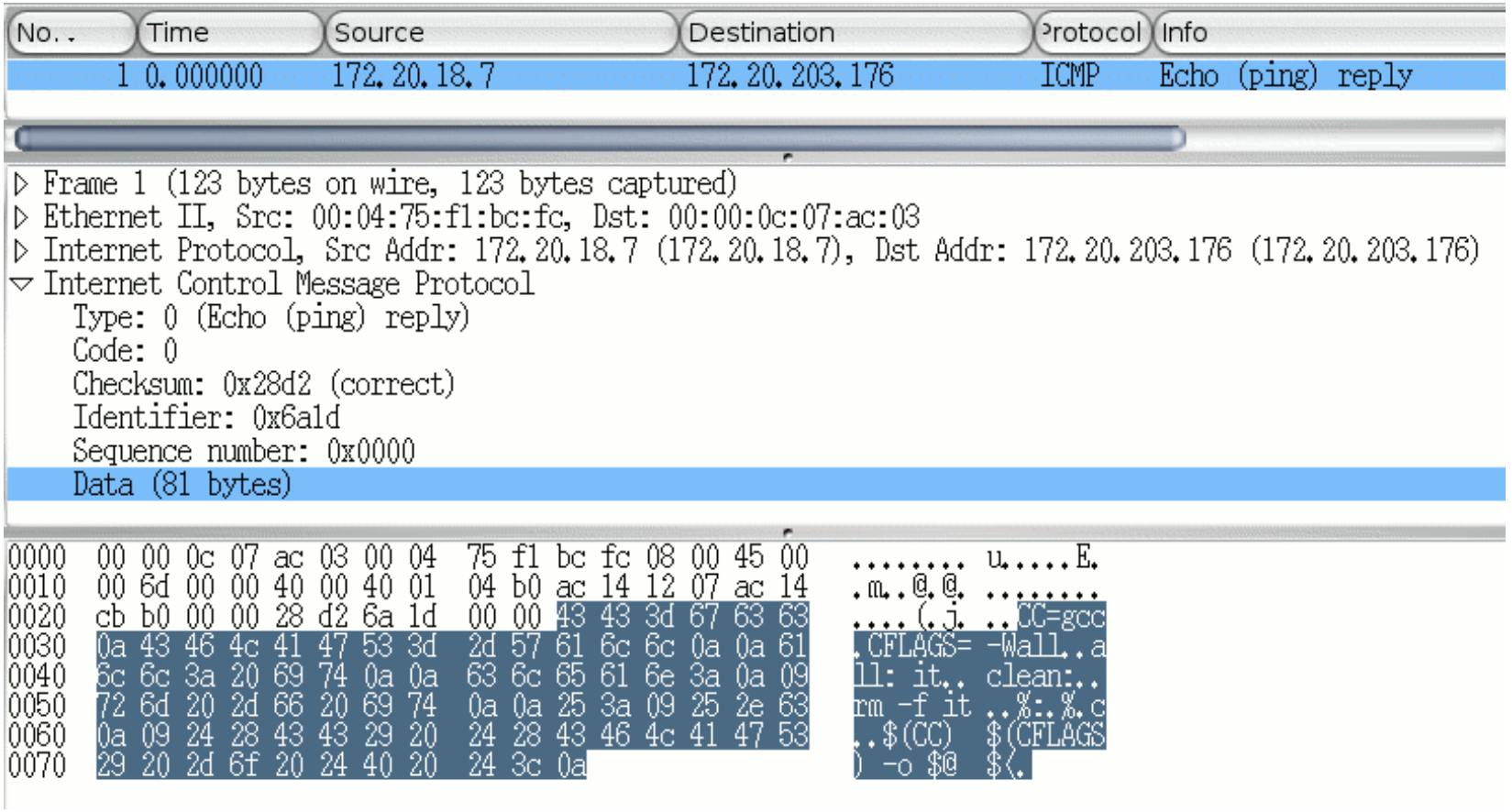
http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=itunnel

## Ziel-Host

```
it quell-host
```

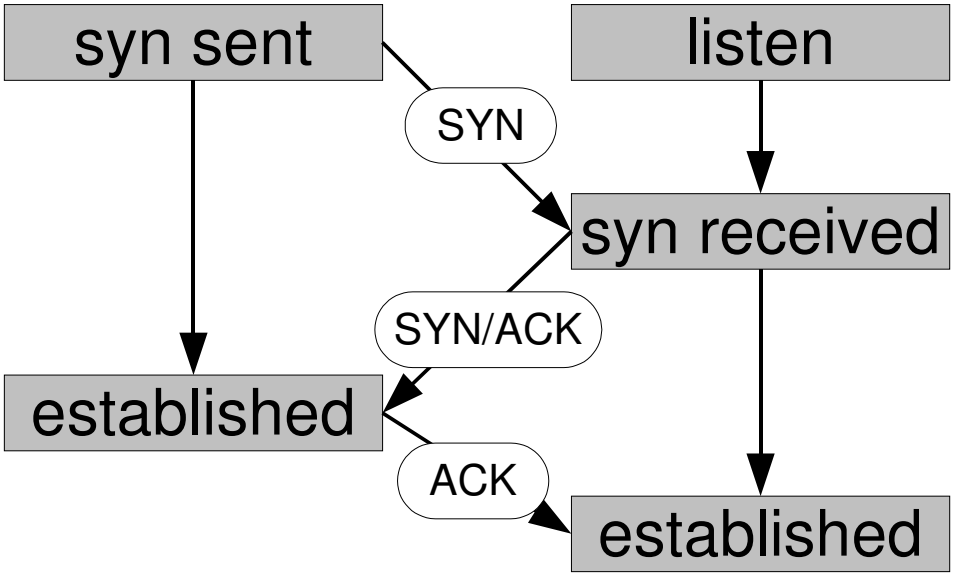
## Quell-Host

```
it zielhost < Makefile
```

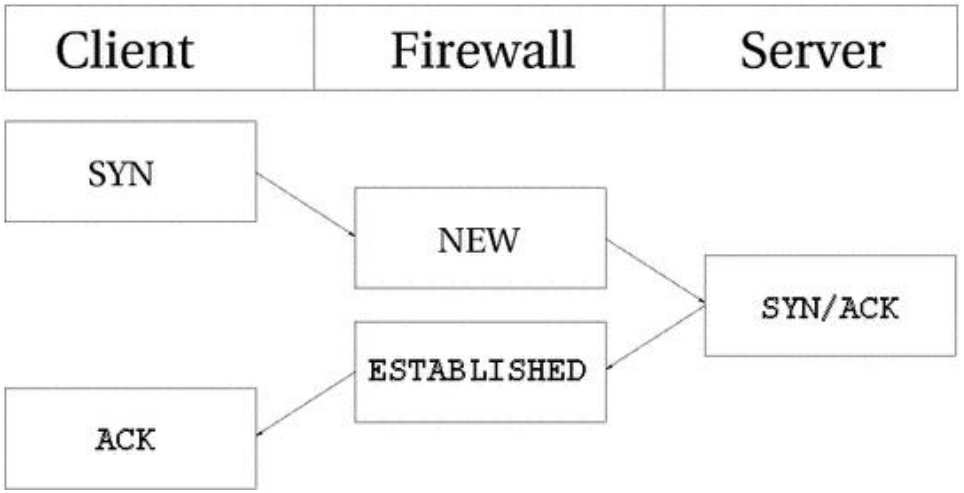


# ACK Tunnel

- TCP 3-Wegehandshake
- Stateless Firewalls müssen ACKs durchlassen
- D. h. Server-SW muss auf ACKs warten.
- Win-Implementation
  http://www.ntsecurity.nu/toolbox/ackcmd




http://www.tcpipguide.com/free/t_TCPConnectionEstablishmentProcessTheThreeWayHandsh-3.htm




Linux/iptables State-connection tracking, aus Iptables Tutorial, Chapter 4

# DNS-Tunnel

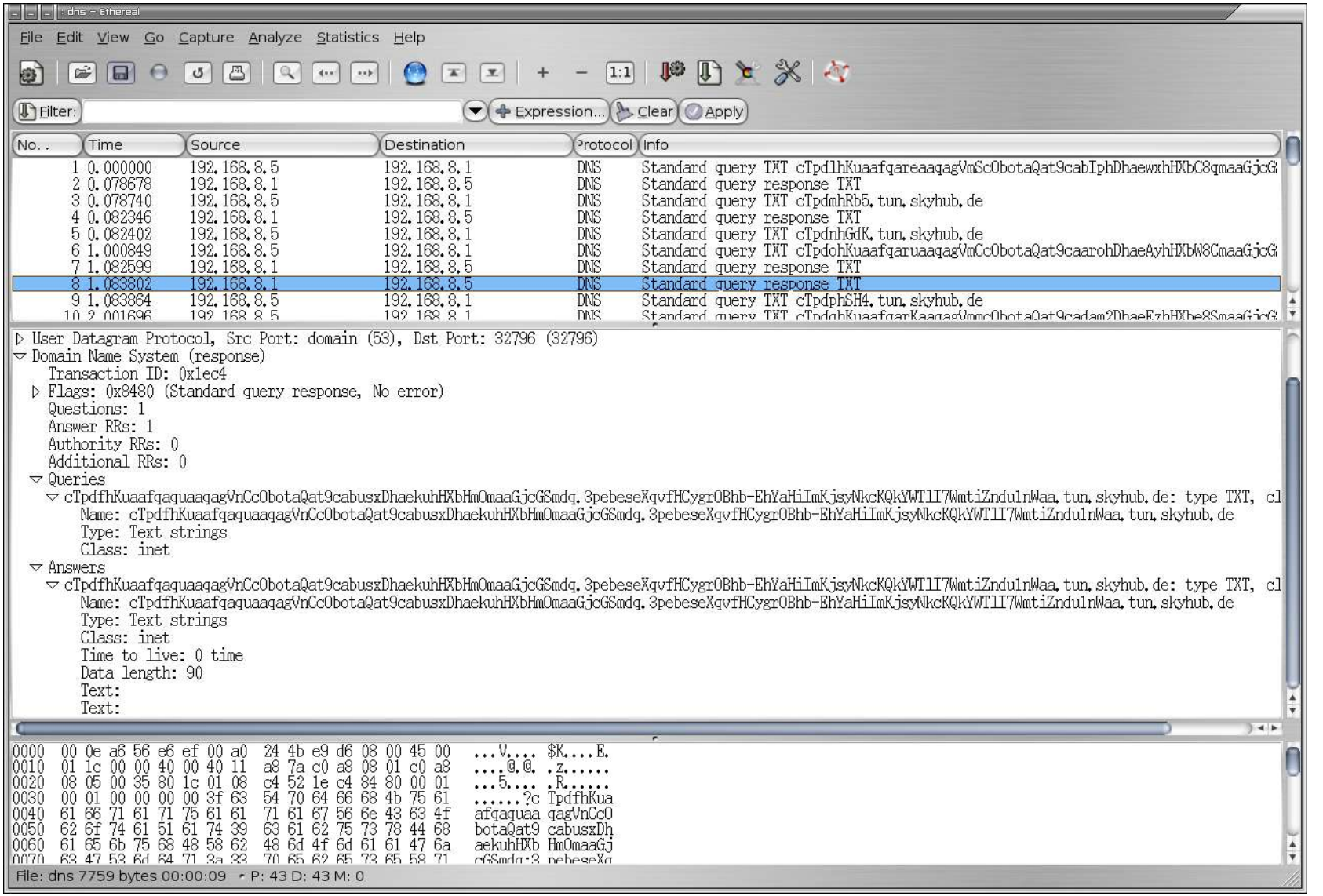
http://www.heise.de/security/artikel/43716/1

- Server:
  - bekommt DNS-Anfragen mit im Namen eingebetteten Daten (Bsp: 3l33thax0r.alien8.de)
- Client:
  - bekommt in TXT-Resource-Record– Feldern Daten
- benötigt also authoritive Nameserver
- ca. 4 kb/s

# DNS-Tunnel: nstx-Test

- Server (mit tun ethertap-dev):
  - `modprobe tun`
  - `./nstxd tunnel.alien8.de`
  - `ifconfig tun0 192.168.5.1`
  - DNS Zone-File für alien8.de:
    tunnel IN NS 1.2.3.4
- Client (mit tun ethertap-dev):
  - `./nstxcd tunnel.alien8.de 4.3.2.1 (LAN-DNS Server)`
  - `ifconfig tun0 192.168.5.1`
  - `ping 192.168.5.1`

# DNS-Tunnel: nstx-Test



# Links

- Placing Backdoors through Firewalls: http://packetstormsecurity.nl/groups/thc/fw-backd.htm
- Heise Security: Schleichpfade http://www.heise.de/security/artikel/43716
- Firewall Tunnel, http://www.employees.org/~hek2000/projects/firewallTunnel, Kaichuan He (http://www.employees.org/~hek2000/index.html)
- GNU HTTP Tunnel, http://www.nocrew.org/software/httptunnel.html, Lars Brinkhoff (http://lars.nocrew.org)
- HTTP Tunnel in Java, http://sourceforge.net/projects/javahttptunnel, Gokul Singh
- Zebedee Secure Tunnel, http://sourceforge.net/projects/zebedee, Neil Winton
- desproxy, http://sourceforge.net/projects/desproxy, Miguelanxo Otero Salgueiro
- nstx, http://nstx.dereference.de, Florian Heinz (sky@sysv.de), Julien Oster(frodo@sysv.de) http://slashdot.org/articles/00/09/10/2230242.shtml
- MailTunnel 0.2 (parrot), http://www.detached.net/mailtunnel, Magnus Lundström (logic@nocrew.org)
- Loki, http://www.phrack.org/show.php?p=49&a=6, http://www.phrack.org/show.php?p=51&a=6, daemon9 (route@infonexus.com)
- icmptunnel 0.1.3, http://www.detached.net/icmptunnel/index.html, Magnus Lundström (logic@nocrew.org)
- AckCmd, http://www.ntsecurity.nu/toolbox/ackcmd, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- FTP-tunnel, http://dhirajbhuyan.hypermart.net/ftp-tunnel.html, Dhiraj Bhuyan (dbhuyans@yahoo.com)
- Gray-World NET Team, http://gray-world.net/papers.shtml
- Tools: http://www.indianz.ch/lnxtoolsd.htm
- itunnel: http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=itunnel&type=archives&%5Bsearch%5D.x=0&%5Bsearch%5D.y=0l
- Protokolle: http://www.just2good.co.uk/index.php?ITFrameSet.php
- Wissen: http://www.wikipedia.org ; http://de.wikipedia.org
- iptables/netfilter: http://www.netfilter.org/
- Placing Backdoors Trhough Firewalls: http://www.thc.org/papers/fw-backd.htm
- TIS firewall toolkit: http://www.fwtk.org
- Vom Menschen zum Unix-Hacker: http://www.thc.org/papers/h2h.htm (und alles von http://www.thc.org)
- www-reverse shell: http://www.thc.org/download.php?t=r&f=rwwwshell-2.0.pl.gz
- Web-Shell: http://gray-world.net/pr_wsh.shtml
- Shell-in-a-box: http://shellinabox.com/
- CGI-Shell: http://cgi-shell.binaervarianz.de/
- PHPShell: http://www.gimpster.com/wiki/PhpShell
- Linux Advanced Routing and Traffic Control: http://www.lartc.org/lartc.htm
- Die Maus erklärt das Internet: http://www.die-maus.de/sachgeschichten/sachgeschichten.phtml
- Warriors of the Net (Film): http://www.warriorsofthe.net/
- Witzige Einführung zu Linux-Firewall, Ethernet, DNS,...: http://www.jaganelli.de/pingu_FrameSet/index.htm
- The Network mapper: http://www.insecure.org/nmap
- corkscrew TCP (e. g. ssh) through web-proxies: http://www.agroman.net/corkscrew/
- crywrap: http://bonehunter.rulez.org/CryWrap.phtml
- OpenBSD: http://www.openbsd.org
- Der OpenBSD Paketfilter pf: http://www.benzedrine.cx/pf.html
- Firewall Failover with pfsync and CARP: http://www.countersiege.com/doc/pfsync-carp/