

# 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

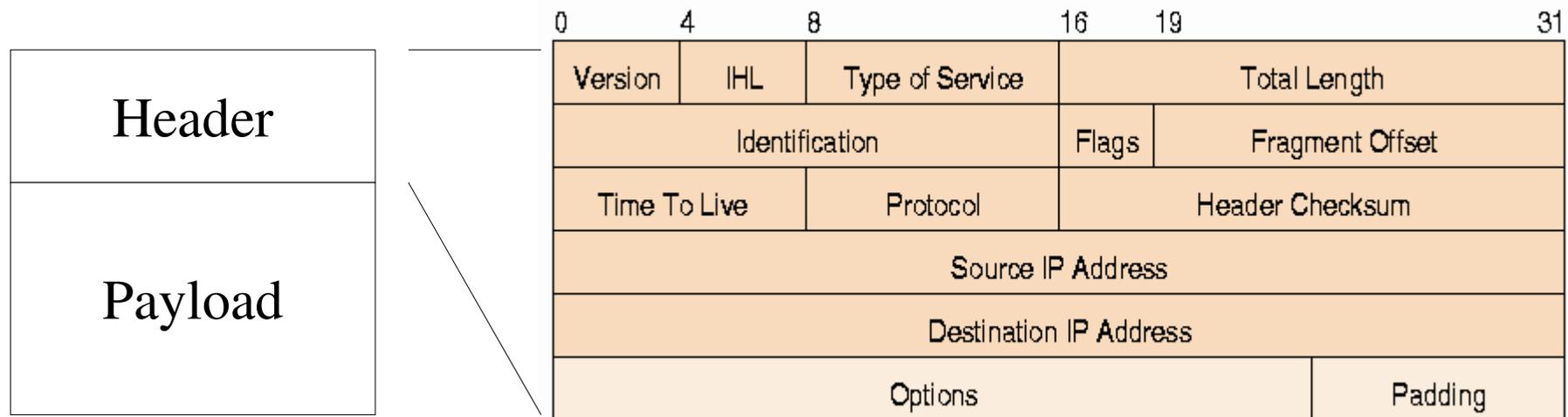
- Grundlagen
  - Internet (Film)
  - Was sind Firewalls?
- Linux-Firewalls
- pf/OpenBSD Firewalls
- Regelgeneratoren
- Tunnel

# 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](http://en.wikipedia.org/wiki/Internet_protocol_suite)

- Application**  
"layer 7"

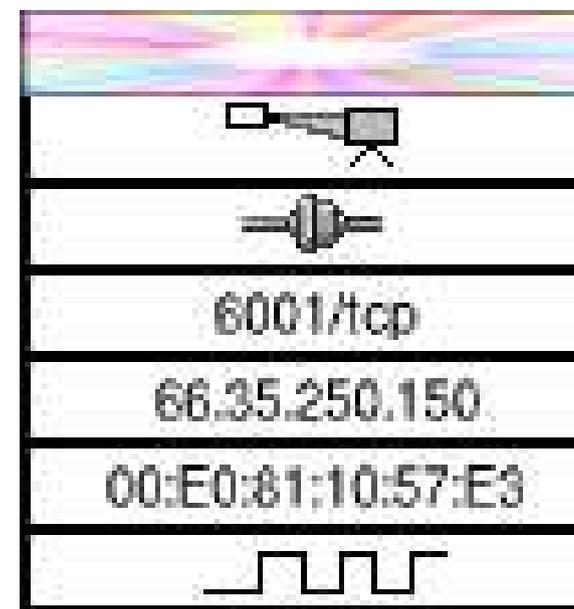
e.g. [HTTP](#), [FTP](#), [DNS](#)  
(routing protocols like [RIP](#), which for obscure reasons run over UDP, may also be considered part of the network layer)
- 4 **Transport**

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**

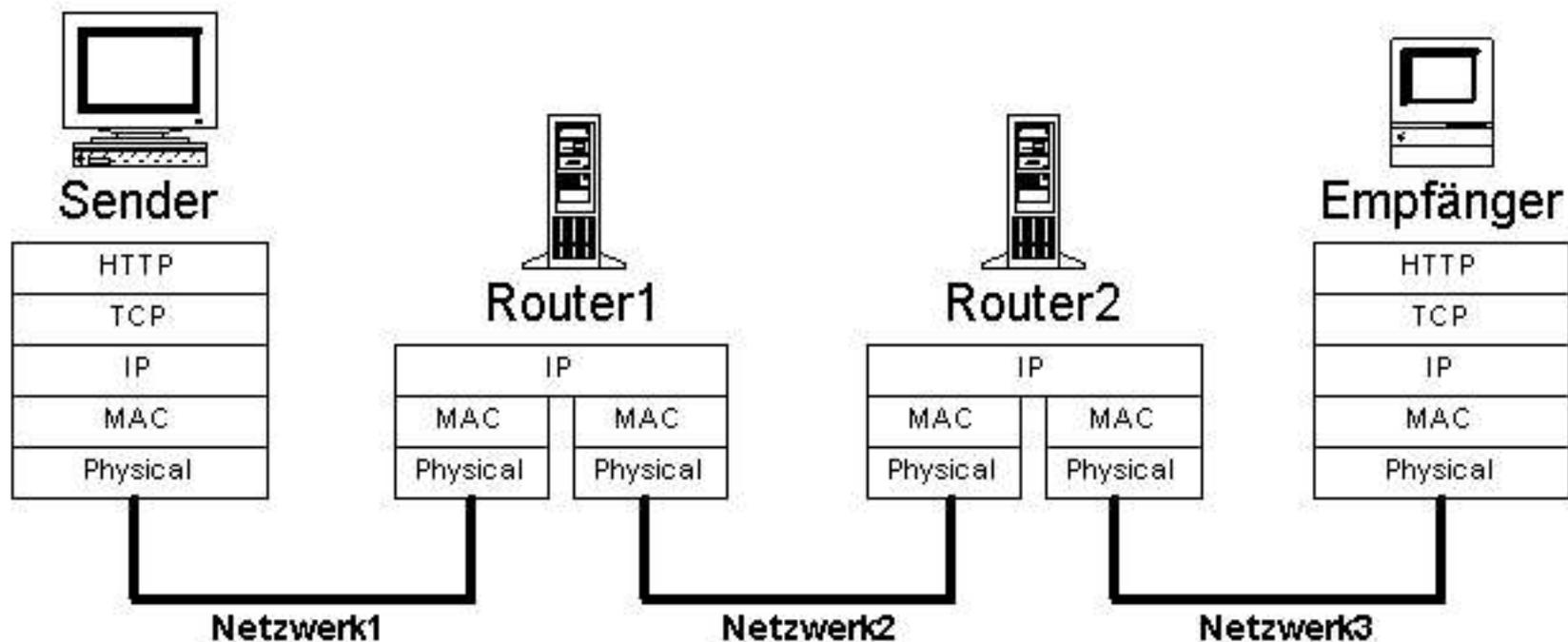
e.g. [Ethernet](#), [Token ring](#), etc.
- 1 **Physical**

e.g. physical media, and [encoding](#) techniques, [T1](#), [E1](#)



# IP-Pakete: Der Weg durch's Netz

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



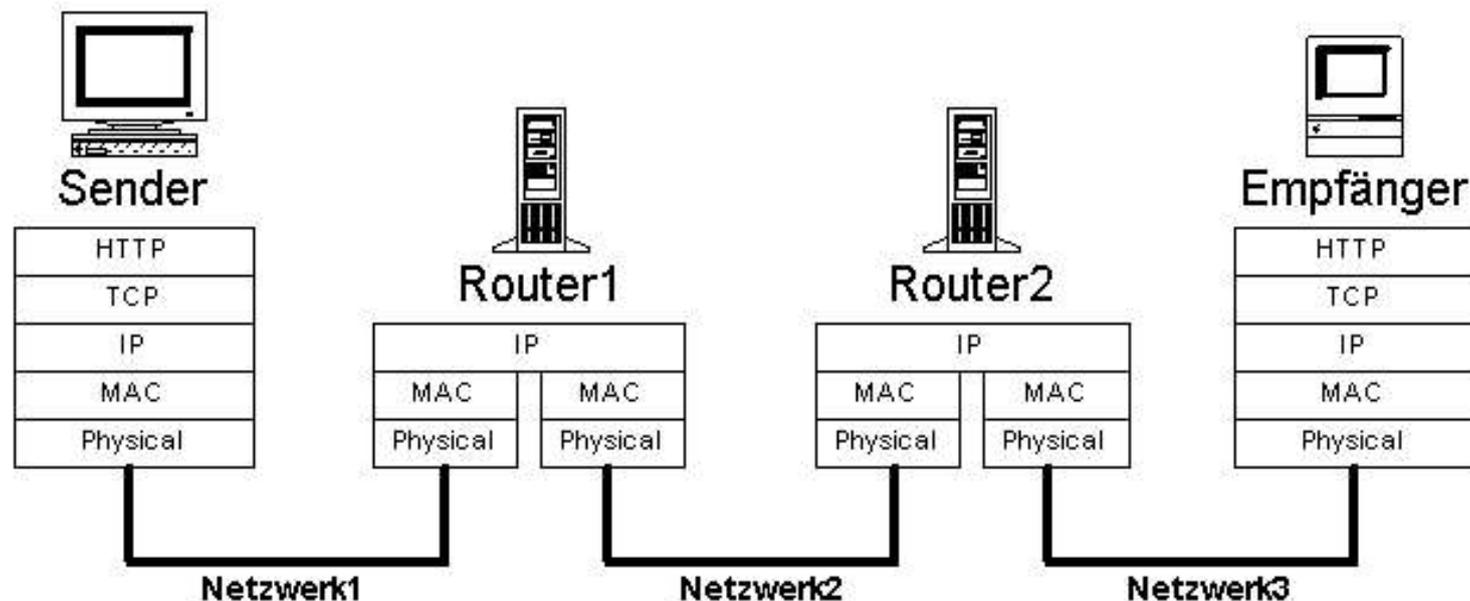


# Firewalls: Begriffe

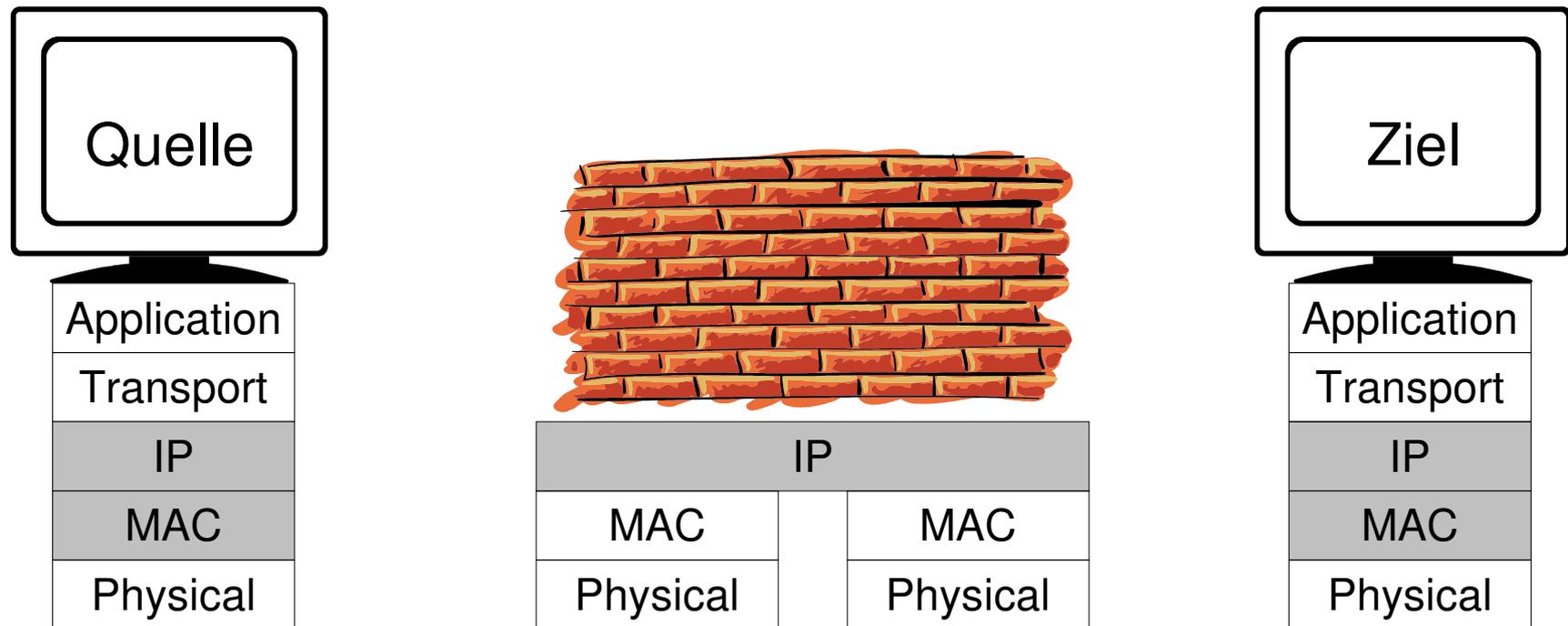
- Router
- Paket Filter
- NAT-Gateway
- NAPT
- Application Layer Gateway / Proxies

# Router

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

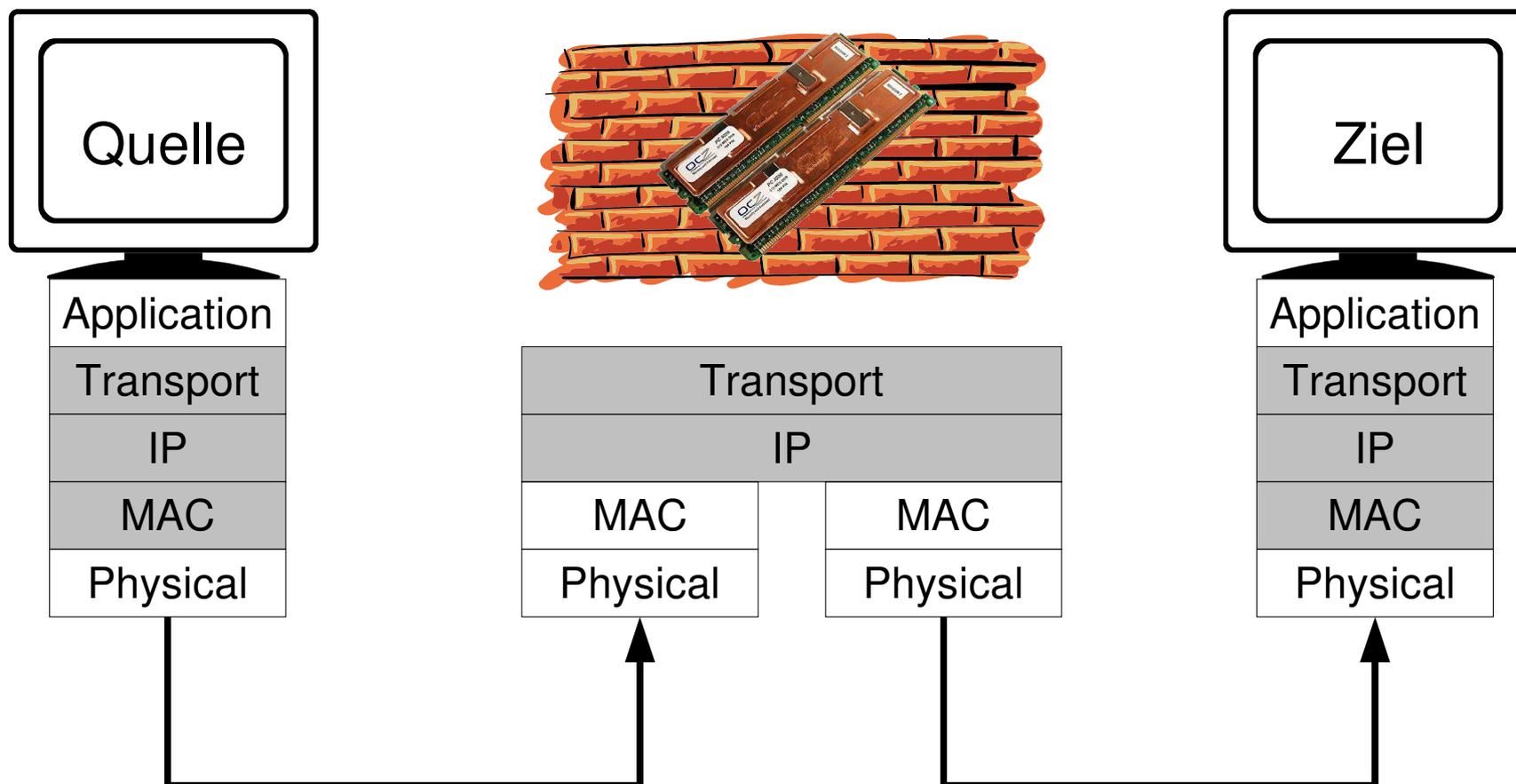


# Stateless Paket Filter



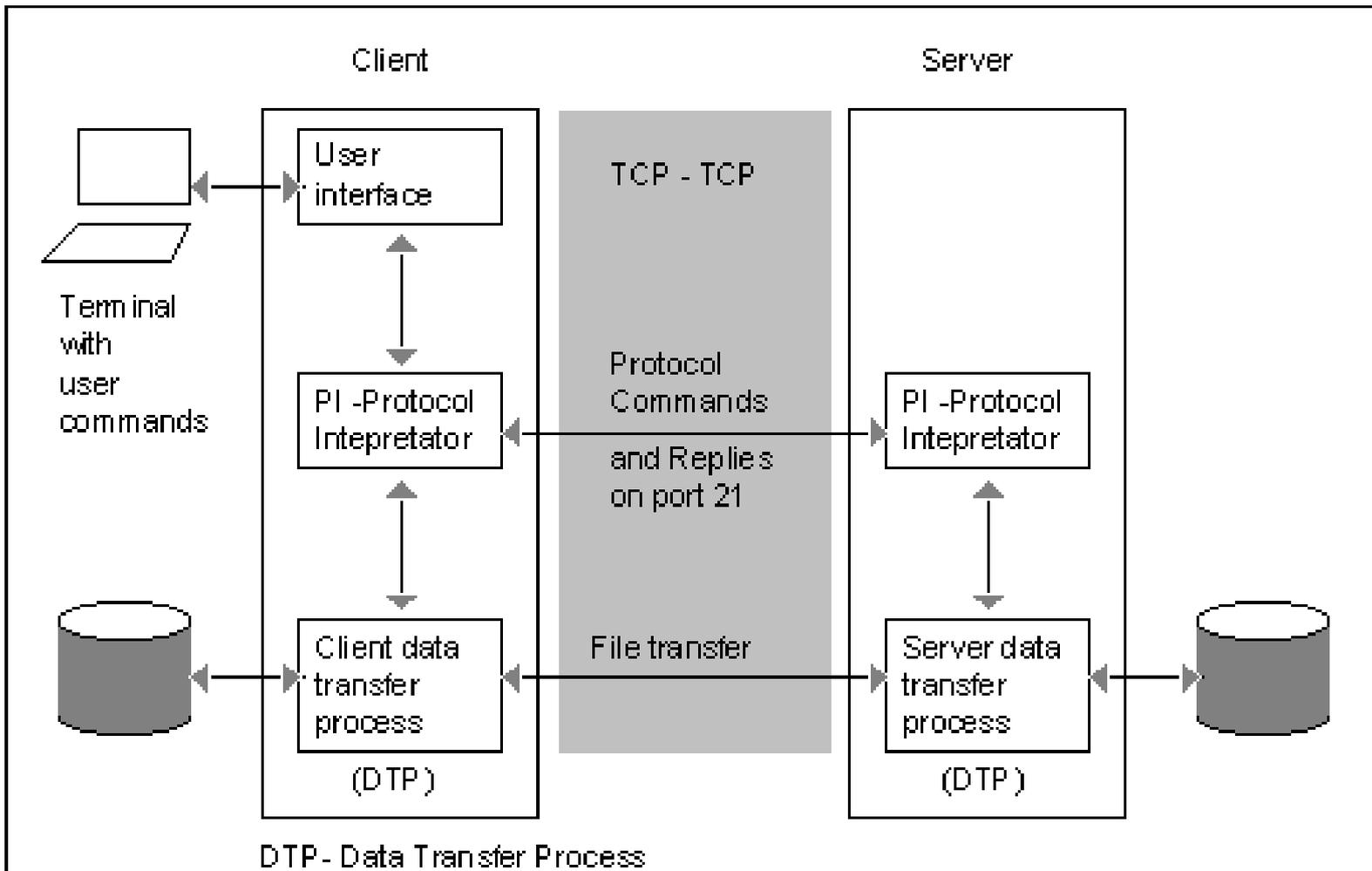
- IP Pakete werden aufgrund Layer 3 Header gefiltert
- kein Zusammenhang zwischen mehreren Paketen
- Bsp: ACK-Telnet Daemon von THC

# Stateful Paket Filter

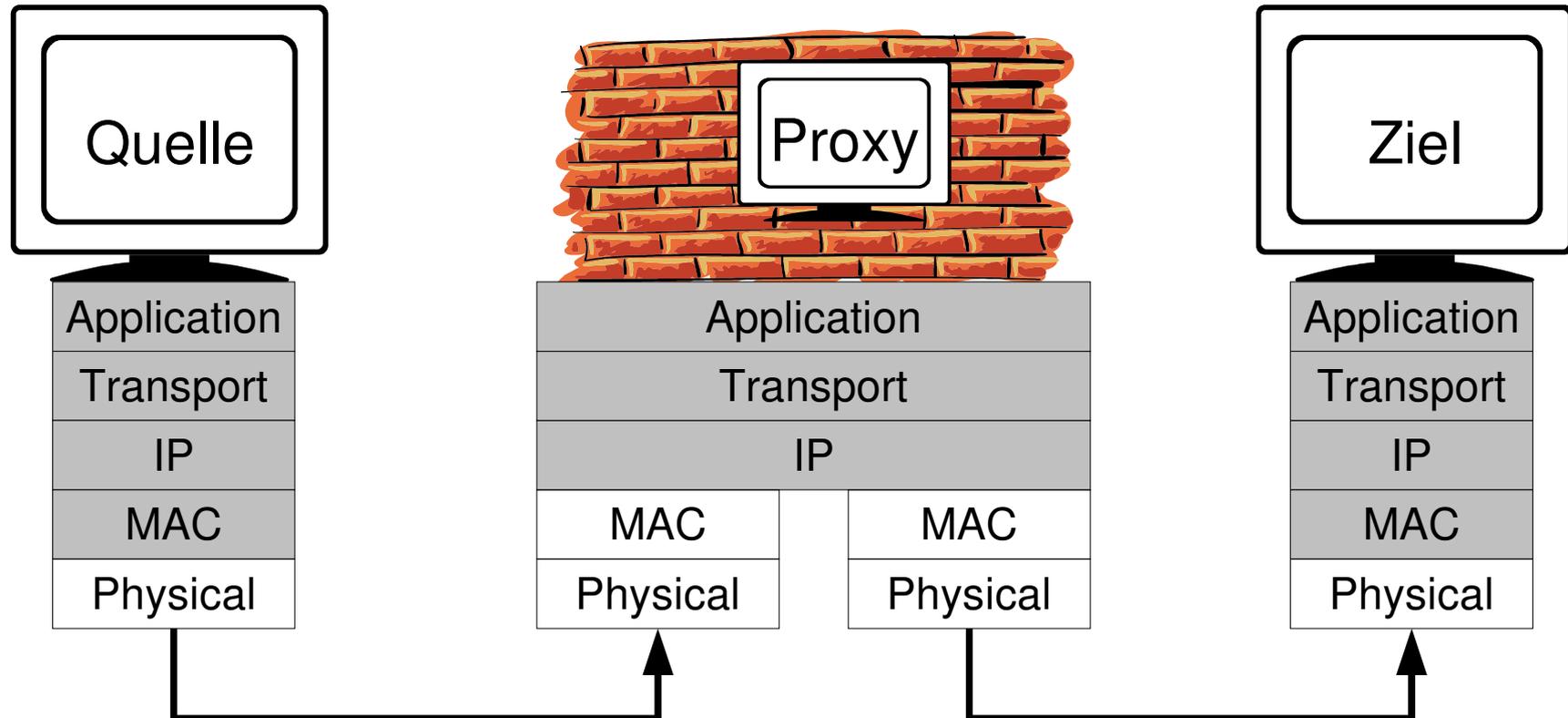


- IP Pakete werden aufgrund Layer 3&4 Header gefiltert
- Paketfilter merkt sich Zustand der Verbindungen, beliebtes Bsp: ftp

# Stateful Protokoll Bsp: ftp



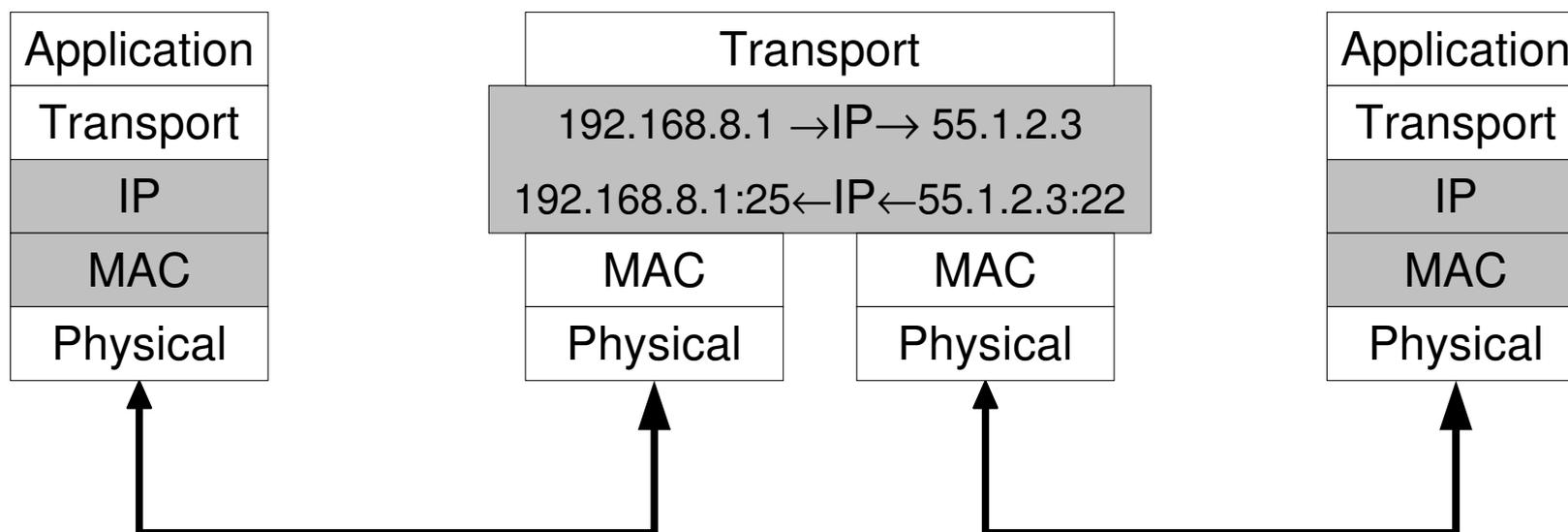
# Application Layer Gateway / Proxy



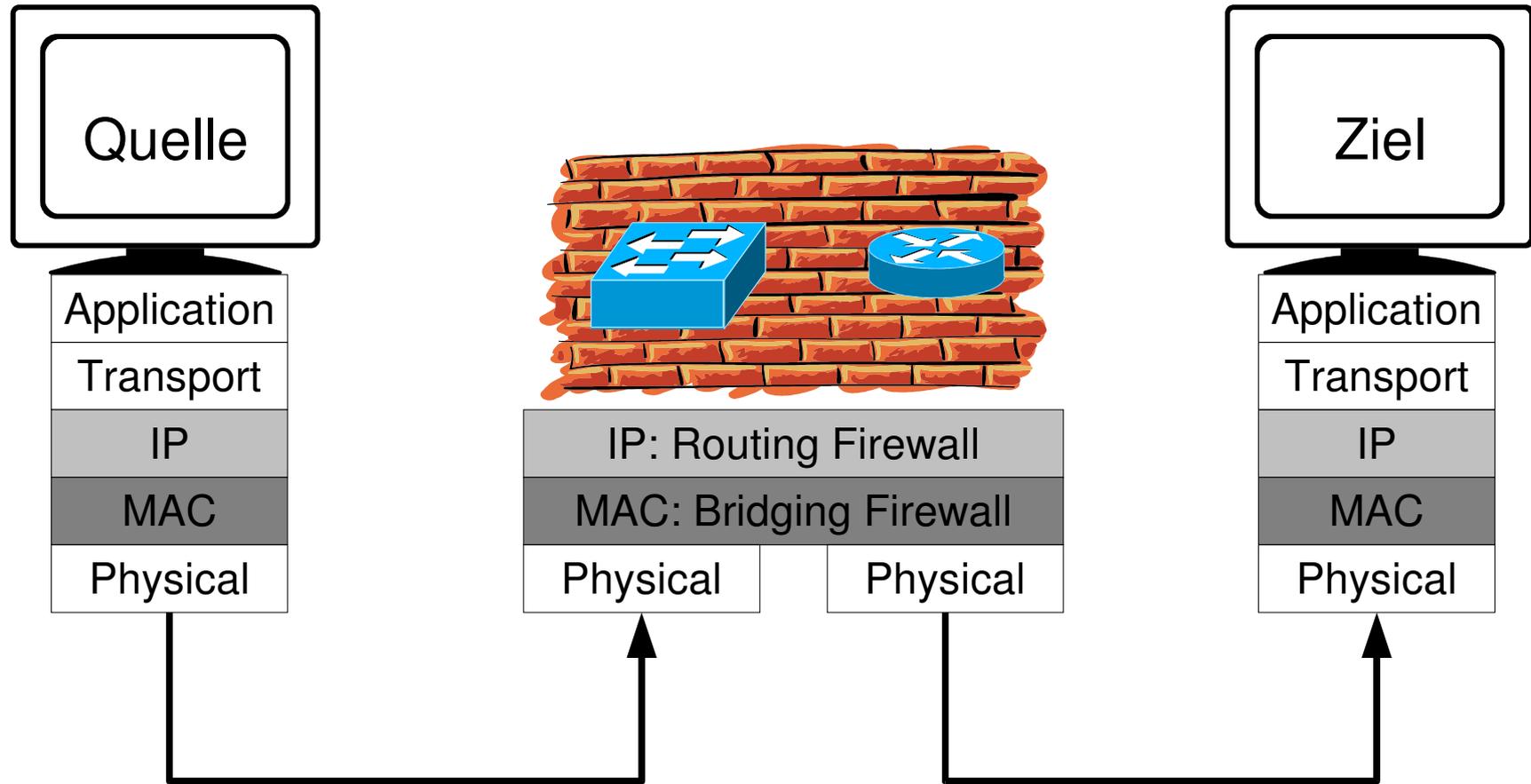
- Proxy spricht Layer 7 - Protokoll
- Proxy übernimmt stellvertretend für Quelle Kommunikation mit Ziel
- optional, erzwungen oder transparent möglich (TRACE für Web)

# 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/>

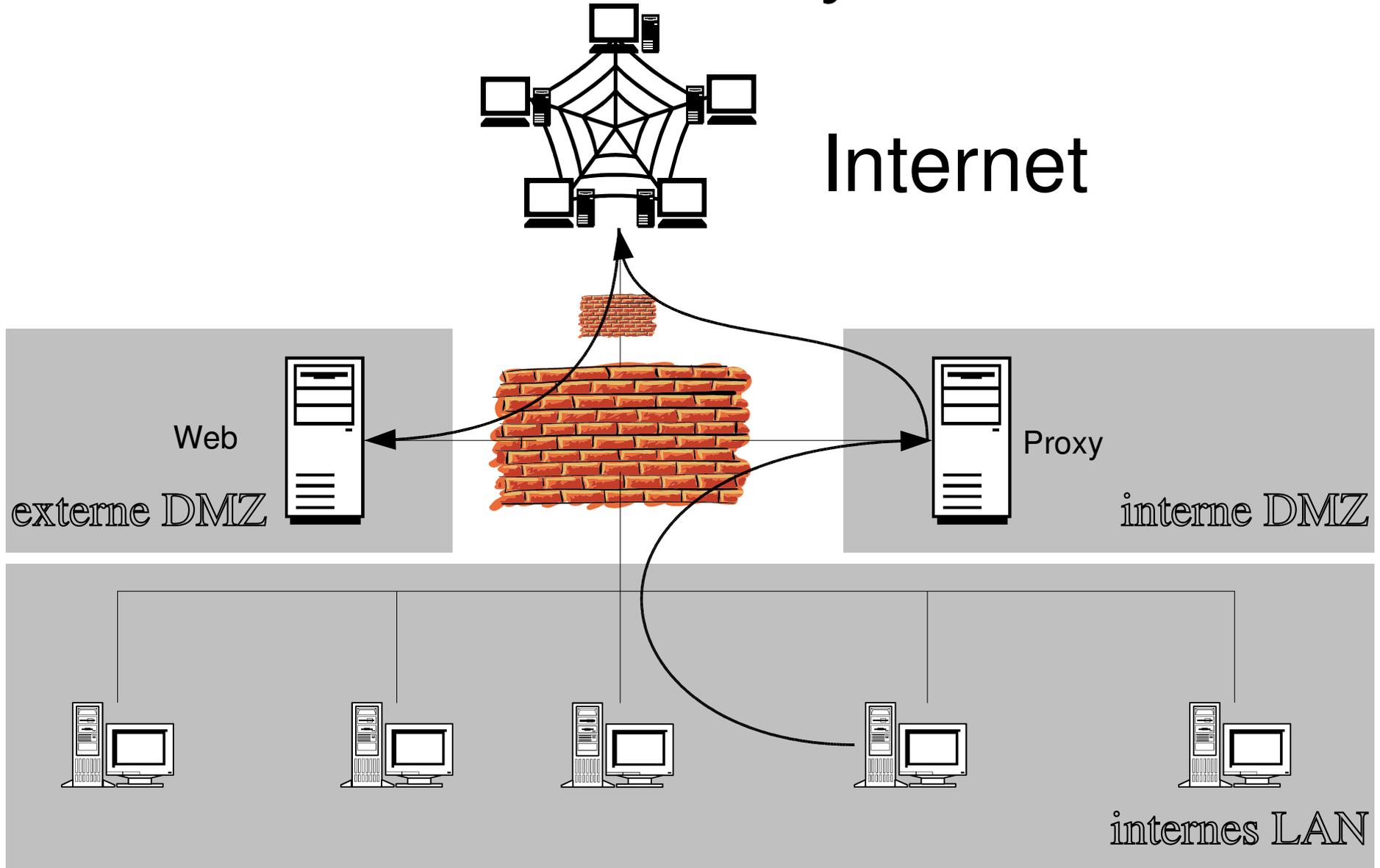
- Reguläre Ausdrücke auf Layer 7 um Protokolle zu erkennen
- besteht aus:
  - Kernel Patch
  - netfilter/iptables Patch
  - Reguläre Ausdrücke zur Protokoll-Klassifikation

# Firewall Design Principles

Building Internet Firewalls (O'Reilly, 2<sup>nd</sup> edition, 2000)

- geringste Privilegien (least Privileges)
- **Keep It Simple Stupid**
- 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

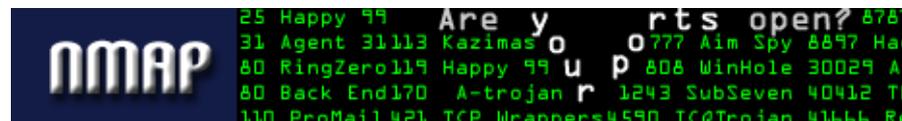


# Personal Firewalls

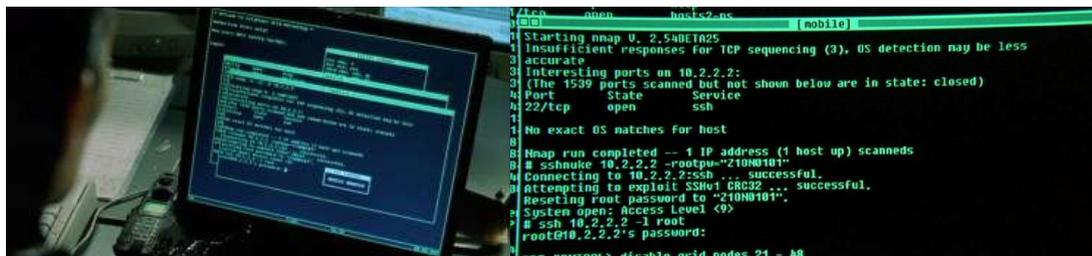
- Rundumschutz auf Desktoprechnern

# Meinungen?

# Firewall Tests

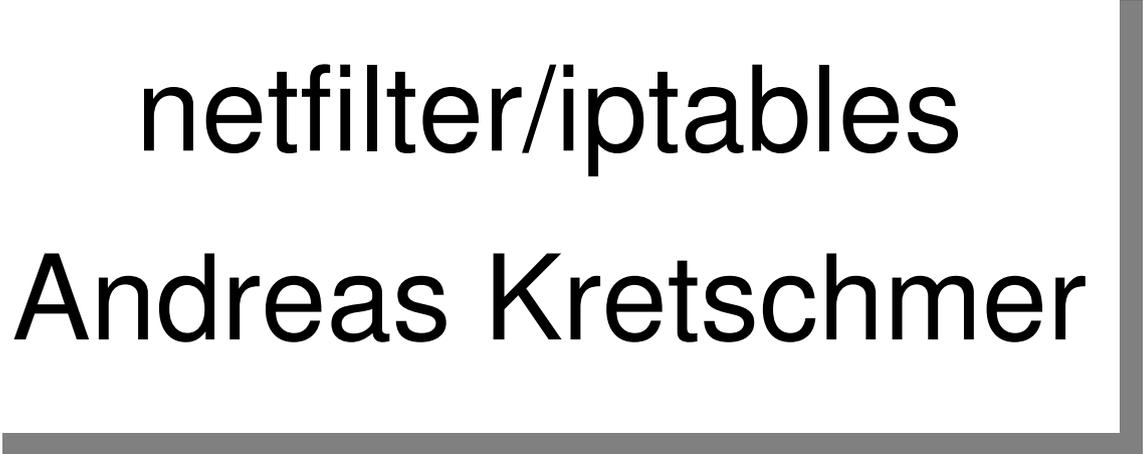


- Portscanner:
  - versucht sich auf alle Ports zu verbinden (und mehr)
    - TCP
    - UDP
- Standard: nmap  
<http://www.insecure.org/nmap>
- man nmap
- <http://www.linux-magazin.de/Artikel/ausgabe/2000/12/SnortNmap/SnortNmap.html>



# netfilter/iptables

## Andreas Kretschmer



# Der Paketfilter pf tibr



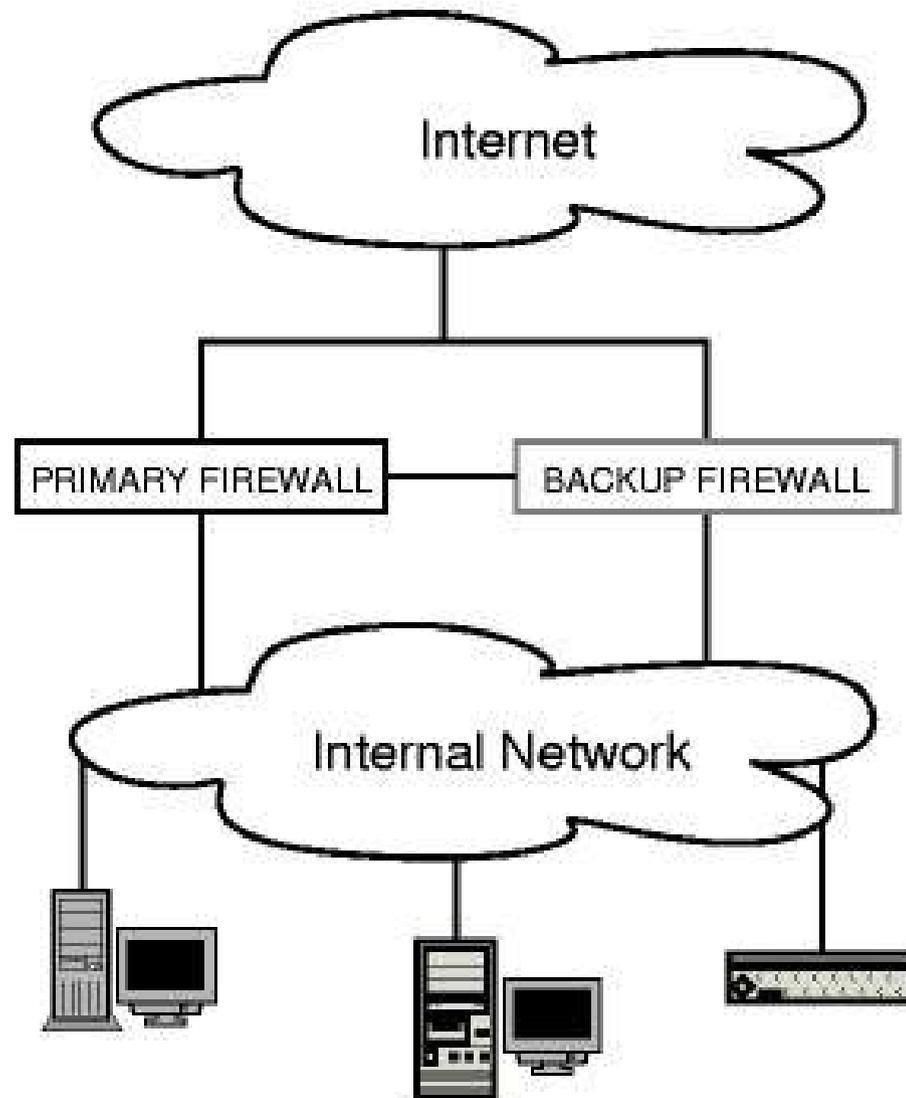
# Hot-Standby Firewall mit carp/pfsync unter OpenBSD

# 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



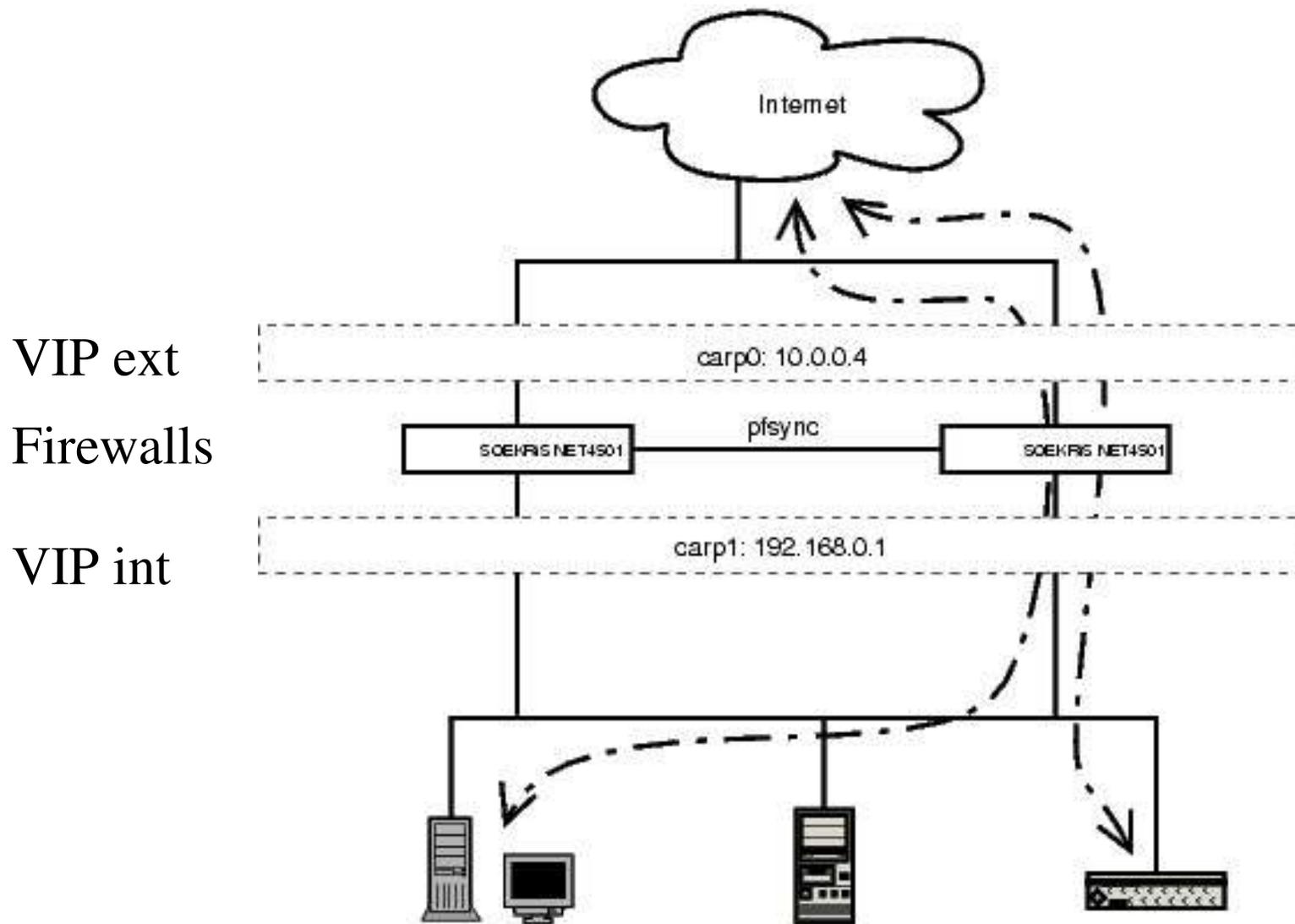
# Tools: CARP

- **Common Address Redundancy Protocol (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)**

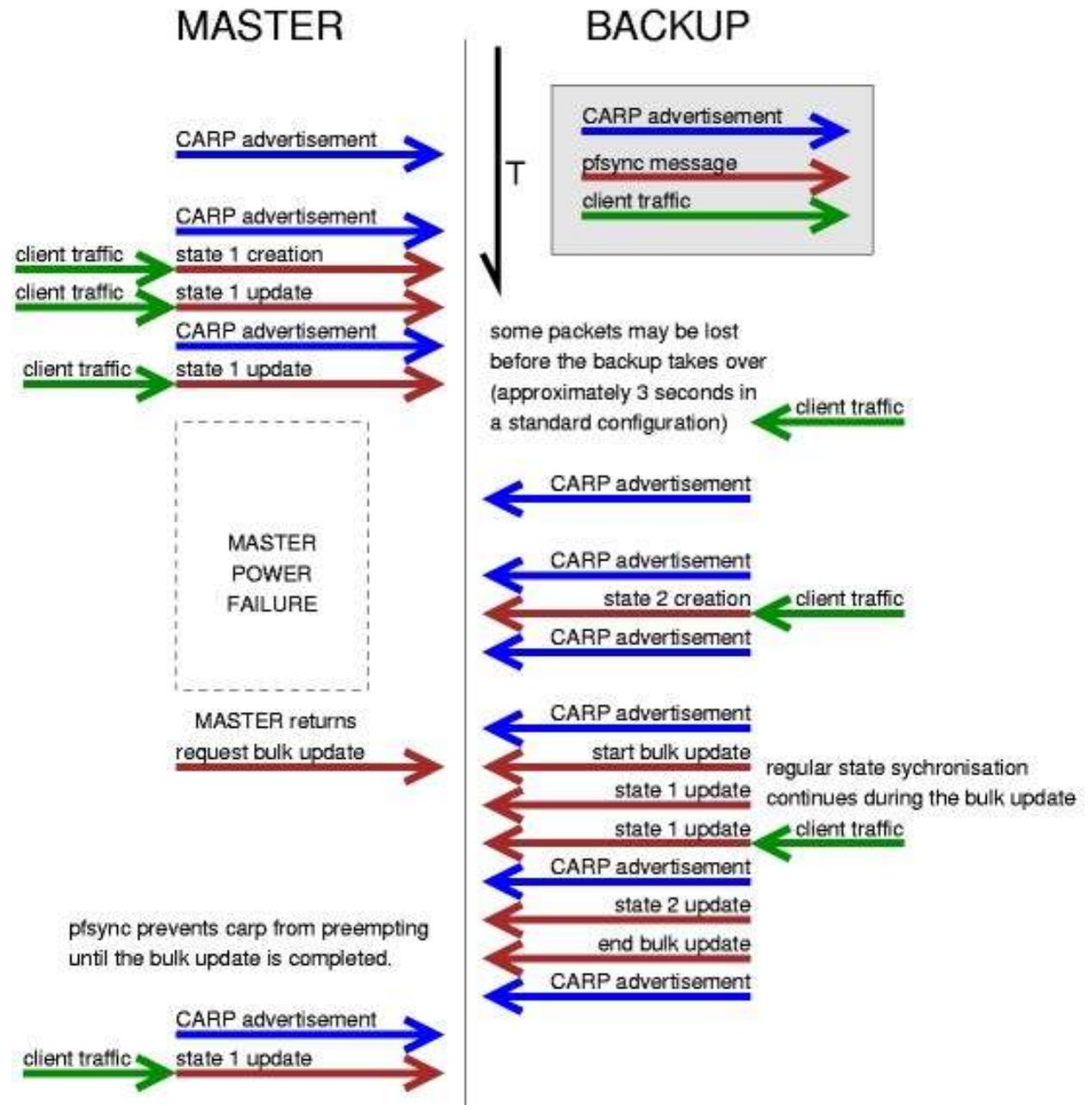
# Tools: pfsync

- 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



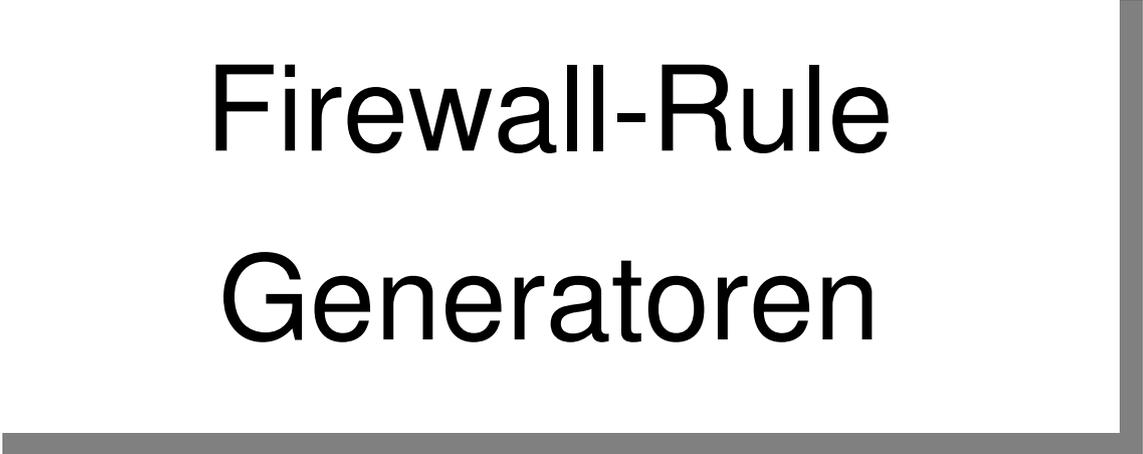
# Failover



# Skalierbarkeit

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

# Firewall-Rule Generatoren

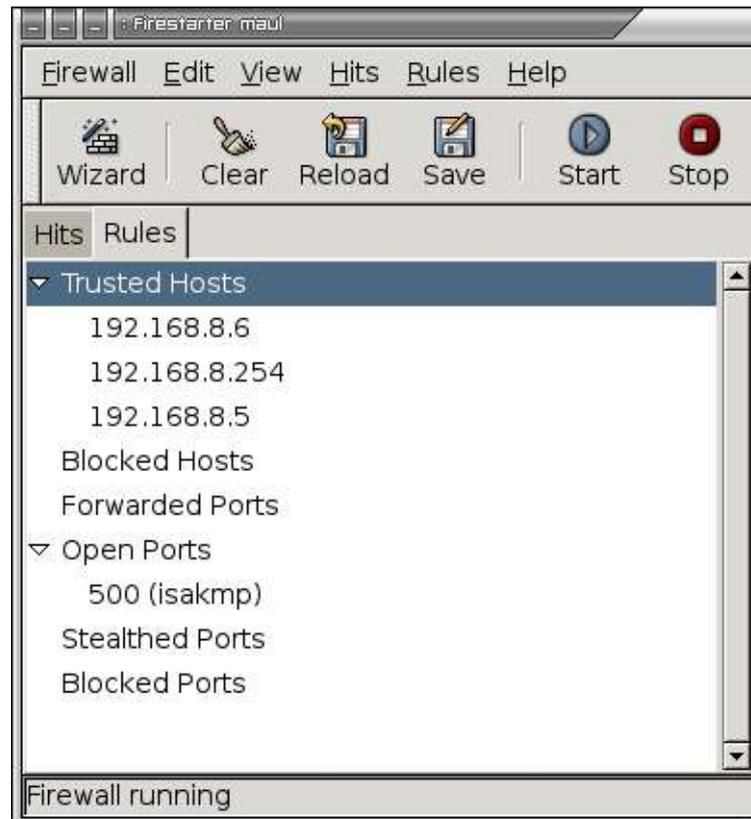


# Firestarter

<http://firestarter.sourceforge.net/>



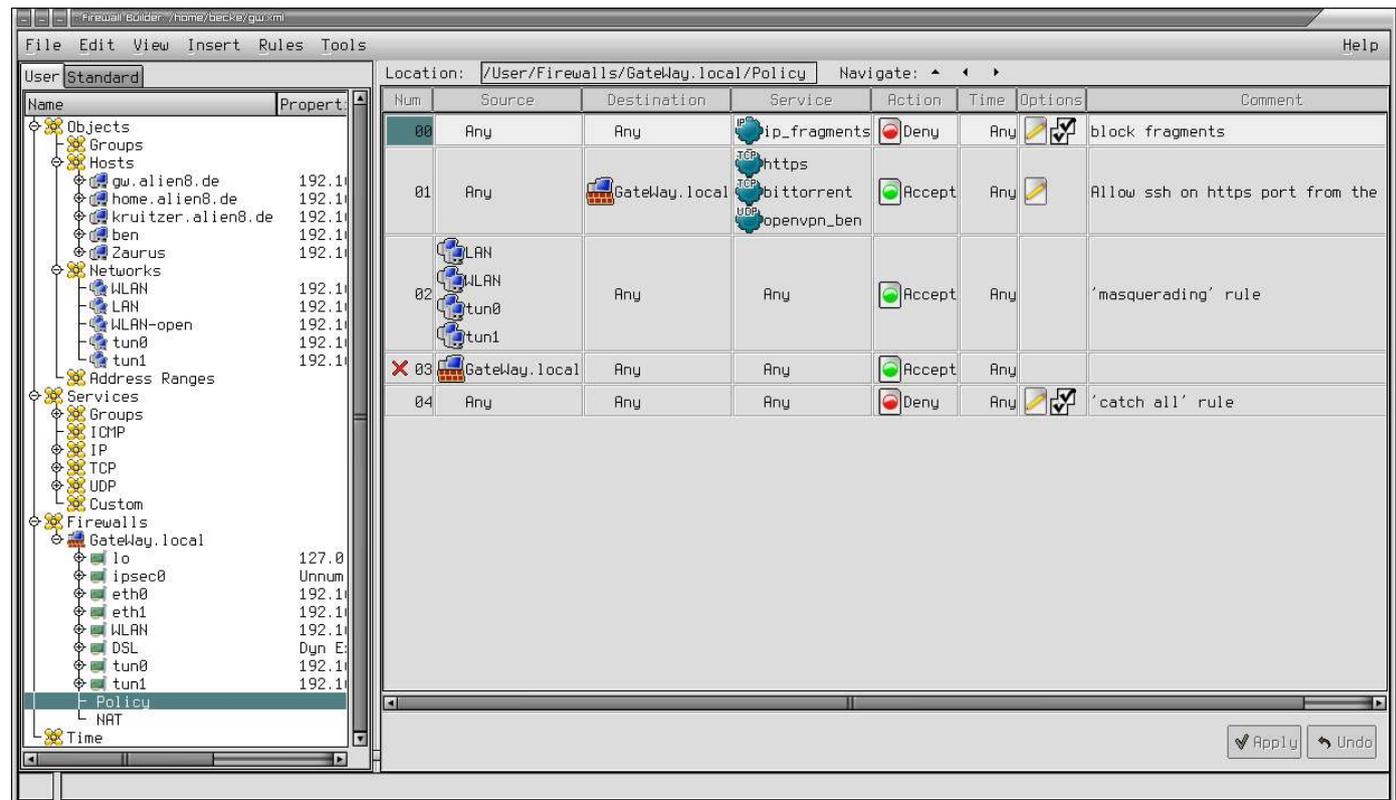
- „Personal Firewall“ für Linux



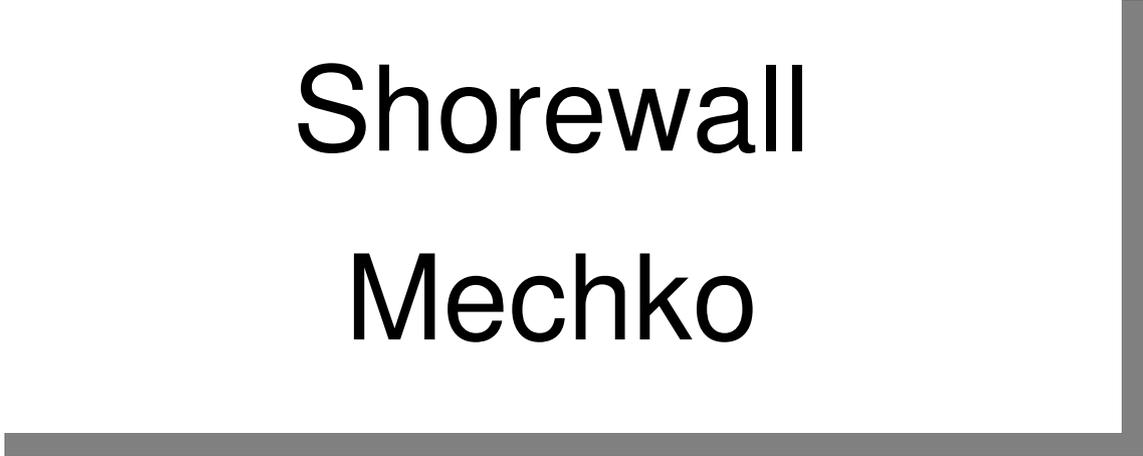
# FWBuilder

<http://firestarter.sourceforge.net/>

- GUI für:
  - Linux
  - WinXP
  - Cisco PIX
  - OpenBSD
- auch für  
Win verfügbar



# Shorewall Mechko



# Tunnel

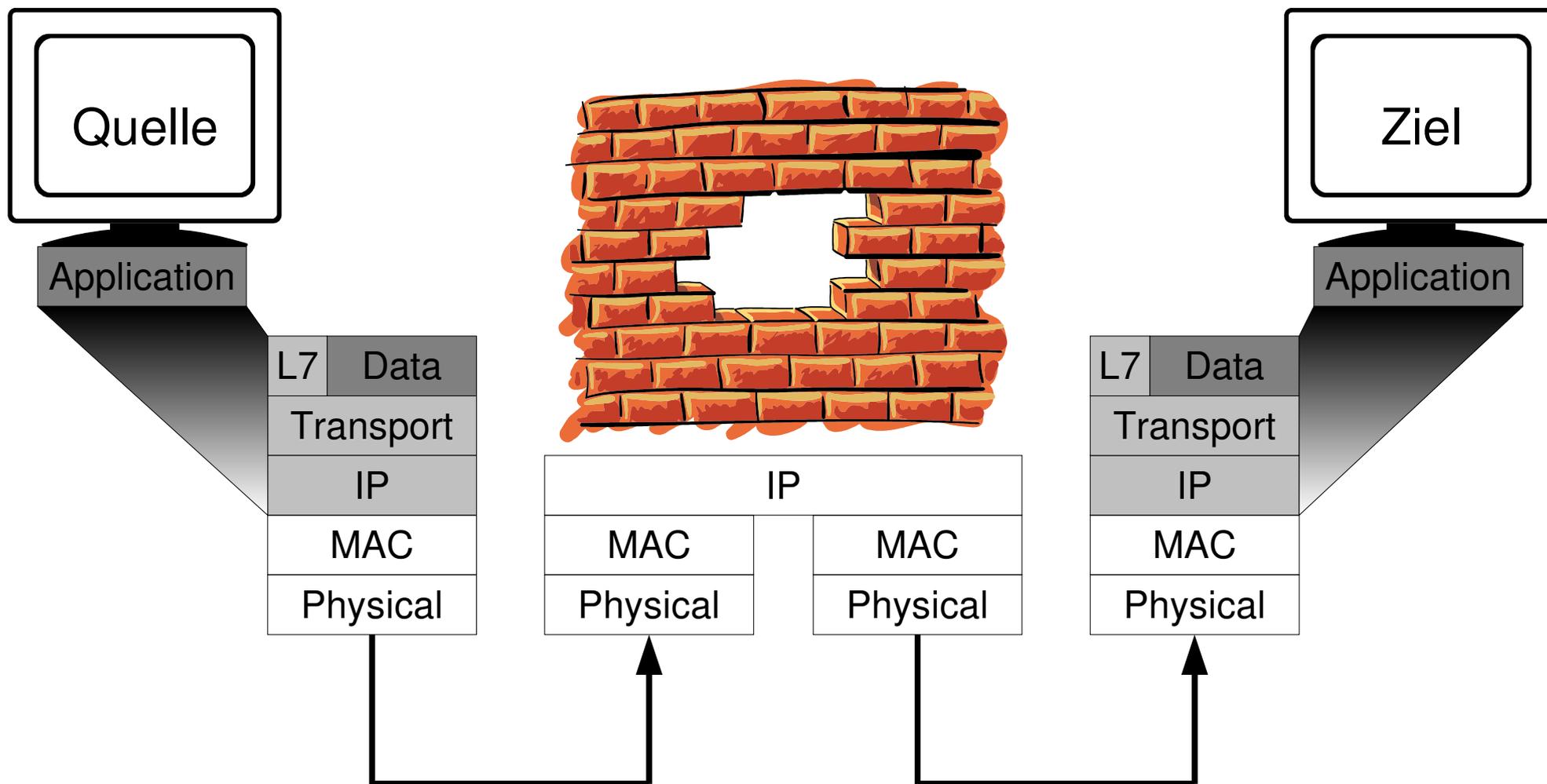


*Das Internet ist fehlertolerant. Filter wertet es als Fehler und arbeitet um diese herum.* weissnichtvonwemdaswar

# Tunnel

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

PPP,SSH...
HTTP
Transport
IP
MAC
Physical

# 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>

## PhpShell 2.0

Current Working Directory: /home/gimpster/public\_html/tmp/phpshell-2.0

```
Bugs?
-----
If you find a bug or miss something in PhpShell, please don't hesitate
to mail me at <gimpster@gimpster.com>!

Enjoy! - Martin Geisler <gimpster@gimpster.com>
$ ll
total 72K
-rw-r--r--  1 gimpster gimpster      871 Mar 27 01:52 AUTHORS
-rw-r--r--  1 gimpster gimpster     18K Mar 27 01:52 COPYING
-rw-r--r--  1 gimpster gimpster     5.7K Mar 27 01:52 ChangeLog
-rw-r--r--  1 gimpster gimpster     2.7K Mar 27 01:52 INSTALL
-rw-r--r--  1 gimpster gimpster     4.5K Mar 27 01:52 README
-rw-r--r--  1 gimpster gimpster     416 Mar 27 01:52 phpshell.css
-rw-r--r--  1 gimpster gimpster     9.2K Mar 27 02:00 phpshell.php
-rw-r--r--  1 gimpster gimpster     793 Mar 27 01:52 release.sh
-rw-r--r--  1 gimpster gimpster     2.4K Mar 27 01:52 valid-xhtml10.png
-rw-r--r--  1 gimpster gimpster     1.2K Mar 27 01:52 vcss.png
$ wc *
 28  106   871 AUTHORS
339 2971 17985 COPYING
188  820  5746 ChangeLog
 76  424  2757 INSTALL
120  747  4538 README
 37   62   416 phpshell.css
287 1017  9418 phpshell.php
 42   94   793 release.sh
  9   29  2414 valid-xhtml10.png
  4   27  1134 vcss.png
1130 6297 46072 total
$
```

Execute Command  Rows:

Please consult the [README](#) and [INSTALL](#) files for instruction on how to use PhpShell.

Copyright © 2000–2004, [Martin Geisler](#). Get the latest version at [www.gimpster.com/wiki/PhpShell](http://www.gimpster.com/wiki/PhpShell).

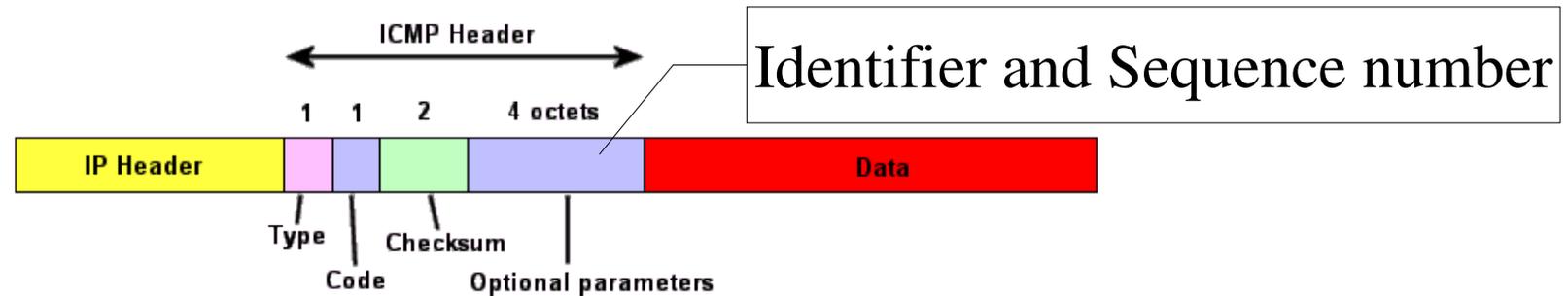


# SSH



- 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

Quell-Host

it quell-host

it zielhost < Makefile

No..	Time	Source	Destination	Protocol	Info
1	0.000000	172.20.18.7	172.20.203.176	ICMP	Echo (ping) reply

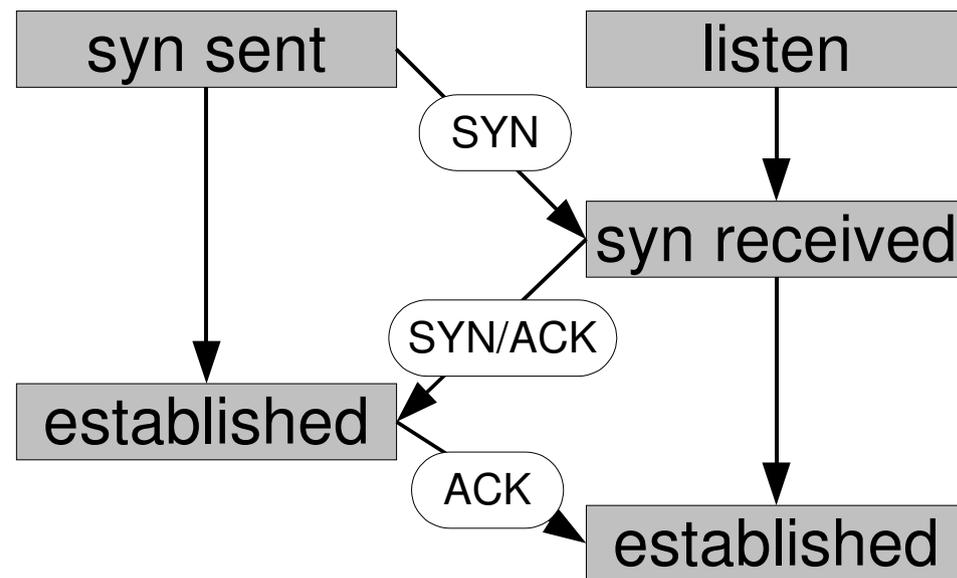
> Frame 1 (123 bytes on wire, 123 bytes captured)  
 > Ethernet II, Src: 00:04:75:f1:bc:fc, Dst: 00:00:0c:07:ac:03  
 > Internet Protocol, Src Addr: 172.20.18.7 (172.20.18.7), Dst Addr: 172.20.203.176 (172.20.203.176)  
 > Internet Control Message Protocol  
   Type: 0 (Echo (ping) reply)  
   Code: 0  
   Checksum: 0x28d2 (correct)  
   Identifier: 0x6ald  
   Sequence number: 0x0000  
   Data (81 bytes)

```

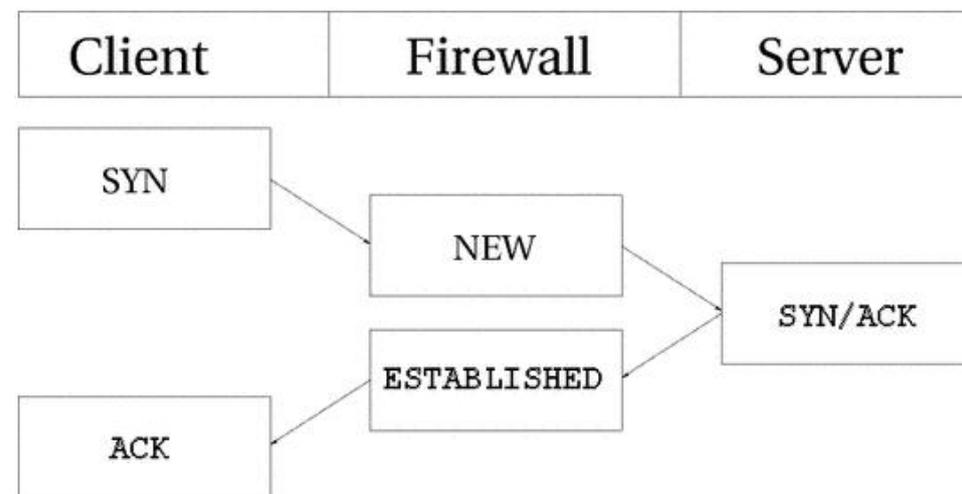
0000  00 00 0c 07 ac 03 00 04 75 f1 bc fc 08 00 45 00  ..... u.....E.
0010  00 6d 00 00 40 00 40 01 04 b0 ac 14 12 07 ac 14  .m.@.@. ....
0020  cb b0 00 00 28 d2 6a 1d 00 00 43 43 3d 67 63 63  .... (.j. ..CC=gcc
0030  0a 43 46 4c 41 47 53 3d 2d 57 61 6c 6c 0a 0a 61  .CFLAGS=-Wall.a
0040  6c 6c 3a 20 69 74 0a 0a 63 6c 65 61 6e 3a 0a 09  ll: it.. clean:..
0050  72 6d 20 2d 66 20 69 74 0a 0a 25 3a 09 25 2e 63  rm -f it ..%:.%c
0060  0a 09 24 28 43 43 29 20 24 28 43 46 4c 41 47 53  .$(CC) $(CFLAGS
0070  29 20 2d 6f 20 24 40 20 24 3c 0a                ) -o $@ $<
  
```

# 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.tcpiptide.com/free/t\\_TCPConnectionEstablishmentProcessTheThreeWayHandsh-3.htm](http://www.tcpiptide.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.aliens.de)
- **Client:**
  - bekommt in TXT-Resource-Record- Feldern Daten
- benötigt also authoritative 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

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.8.5	192.168.8.1	DNS	Standard query TXT cTpdlhKuaafqareaaqagVnScObotaQat9cabIphDhaewxhHXbC8qmaaGjcG
2	0.078678	192.168.8.1	192.168.8.5	DNS	Standard query response TXT
3	0.078740	192.168.8.5	192.168.8.1	DNS	Standard query TXT cTpdmhRb5, tun, skyhub, de
4	0.082346	192.168.8.1	192.168.8.5	DNS	Standard query response TXT
5	0.082402	192.168.8.5	192.168.8.1	DNS	Standard query TXT cTpdnhGdK, tun, skyhub, de
6	1.000849	192.168.8.5	192.168.8.1	DNS	Standard query TXT cTpdohKuaafqaruuaaqagVnCcObotaQat9caarohDhaeAyhHXbW8CmaaGjcG
7	1.082599	192.168.8.1	192.168.8.5	DNS	Standard query response TXT
8	1.083802	192.168.8.1	192.168.8.5	DNS	Standard query response TXT
9	1.083864	192.168.8.5	192.168.8.1	DNS	Standard query TXT cTpdphSH4, tun, skyhub, de
10	2.001696	192.168.8.5	192.168.8.1	DNS	Standard query TXT cTpdohKuaafqaruuaaqagVnCcObotaQat9caadam2DhaeEzhhHXbW8CmaaGjcG

> User Datagram Protocol, Src Port: domain (53), Dst Port: 32796 (32796)  
 < Domain Name System (response)  
   Transaction ID: 0x1ec4  
   Flags: 0x8480 (Standard query response, No error)  
   Questions: 1  
   Answer RRs: 1  
   Authority RRs: 0  
   Additional RRs: 0  
   Queries  
     < cTpdfhKuaafqaquaaqagVnCcObotaQat9cabusxDhaekuhHXbHmOmaaGjcGSmdg, 3pebeseXqvfhCYgrOBhb-EhYaHiImKjsyNkcKQkYWTlI7WmtiZndulnWaa, tun, skyhub, de: type TXT, cl  
       Name: cTpdfhKuaafqaquaaqagVnCcObotaQat9cabusxDhaekuhHXbHmOmaaGjcGSmdg, 3pebeseXqvfhCYgrOBhb-EhYaHiImKjsyNkcKQkYWTlI7WmtiZndulnWaa, tun, skyhub, de  
       Type: Text strings  
       Class: inet  
   Answers  
     < cTpdfhKuaafqaquaaqagVnCcObotaQat9cabusxDhaekuhHXbHmOmaaGjcGSmdg, 3pebeseXqvfhCYgrOBhb-EhYaHiImKjsyNkcKQkYWTlI7WmtiZndulnWaa, tun, skyhub, de: type TXT, cl  
       Name: cTpdfhKuaafqaquaaqagVnCcObotaQat9cabusxDhaekuhHXbHmOmaaGjcGSmdg, 3pebeseXqvfhCYgrOBhb-EhYaHiImKjsyNkcKQkYWTlI7WmtiZndulnWaa, tun, skyhub, de  
       Type: Text strings  
       Class: inet  
       Time to live: 0 time  
       Data length: 90  
       Text:  
       Text:

```

0000  00 0e a6 56 e6 ef 00 a0 24 4b e9 d6 08 00 45 00  ...V... $K...E.
0010  01 1c 00 00 40 00 40 11 a8 7a c0 a8 08 01 c0 a8  ...@.@. .z.....
0020  08 05 00 35 80 1c 01 08 c4 52 1e c4 84 80 00 01  ...5... .R.....
0030  00 01 00 00 00 00 3f 63 54 70 64 66 68 4b 75 61  ....?c Tpdfhkua
0040  61 66 71 61 71 75 61 61 71 61 67 56 6e 43 63 4f  afqaguaa qagVnCc0
0050  62 6f 74 61 51 61 74 39 63 61 62 75 73 78 44 68  botaQat9 cabusDh
0060  61 65 6b 75 68 48 58 62 48 6d 4f 6d 61 61 47 6a  aekuhHXb HmOmaaGj
0070  63 47 53 64 64 71 3a 33 70 65 62 65 73 65 58 71  cGSmdg.3 pebeseXq
  
```

File: dns 7759 bytes 00:00:09 P: 43 D: 43 M: 0

# 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/httpunnel.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](mailto:sky@sysv.de)), Julien Oster([frodo@sysv.de](mailto: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](mailto: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](mailto:route@infonexus.com))
- icmptunnel 0.1.3, <http://www.detached.net/icmptunnel/index.html>, Magnus Lundström ([logic@nocrew.org](mailto:logic@nocrew.org))
- AckCmd, <http://www.ntsecurity.nu/toolbox/ackcmd>, Arne Vidstrom ([arne.vidstrom@ntsecurity.nu](mailto:arne.vidstrom@ntsecurity.nu))
- FTP-tunnel, <http://dhirajbhuyan.hypermart.net/ftp-tunnel.html>, Dhiraj Bhuyan ([dbhuyans@yahoo.com](mailto:dbhuyans@yahoo.com))
- Gray-World NET Team, <http://gray-world.net/papers.shtml>
- Tools: <http://www.indianz.ch/lxntoolsd.htm>
- itunnel: <http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=itunnel&type=archives&%5Bsearch%5D.x=0&%5Bsearch%5D.y=01>
- 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 Through 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](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](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/>