Internet-Firewalls

Vortrag im Rahmen des Seminars Verschlüsselung und Sicherheit in vernetzten Systemen

29. Juni 2001

von Michael Dirska

Sicherheit im Internet?

Verbindung zum Netzwerk → keine Sicherheit

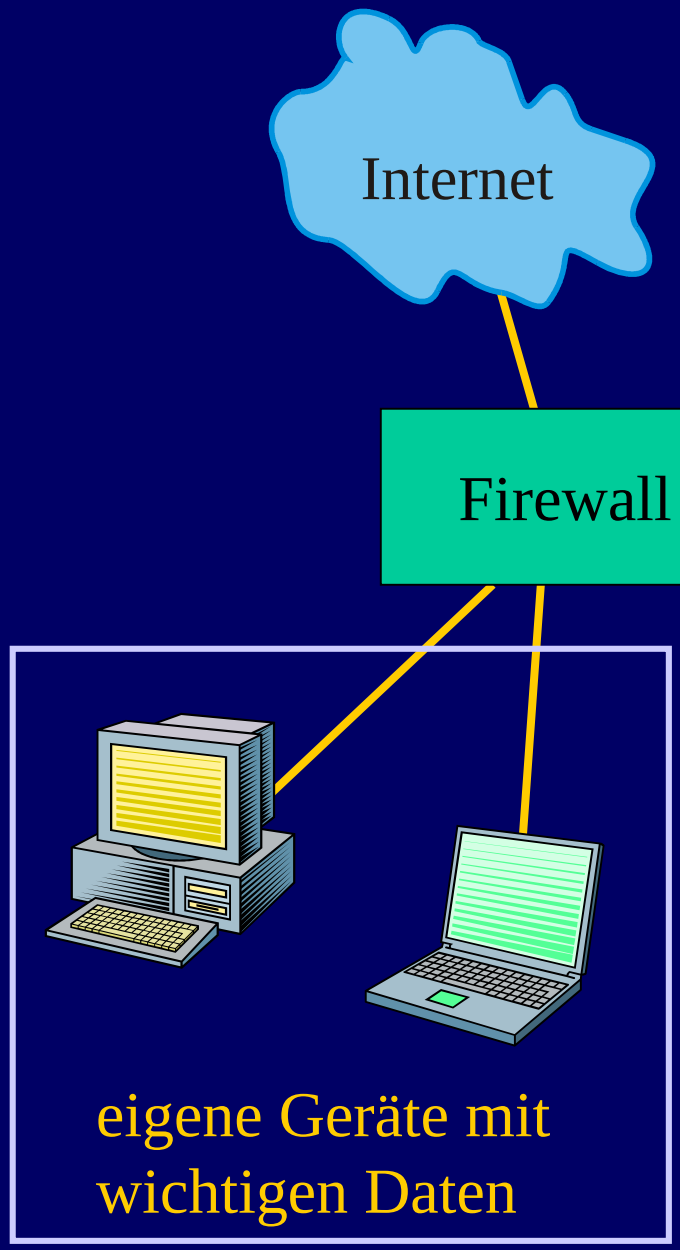
Sicherheit im Internet?

keine Verbindung zum Netzwerk → Sicherheit

Sicherheit im Internet?

gefilterte Verbindung → etwas Sicherheit

Eine Firewall ist...

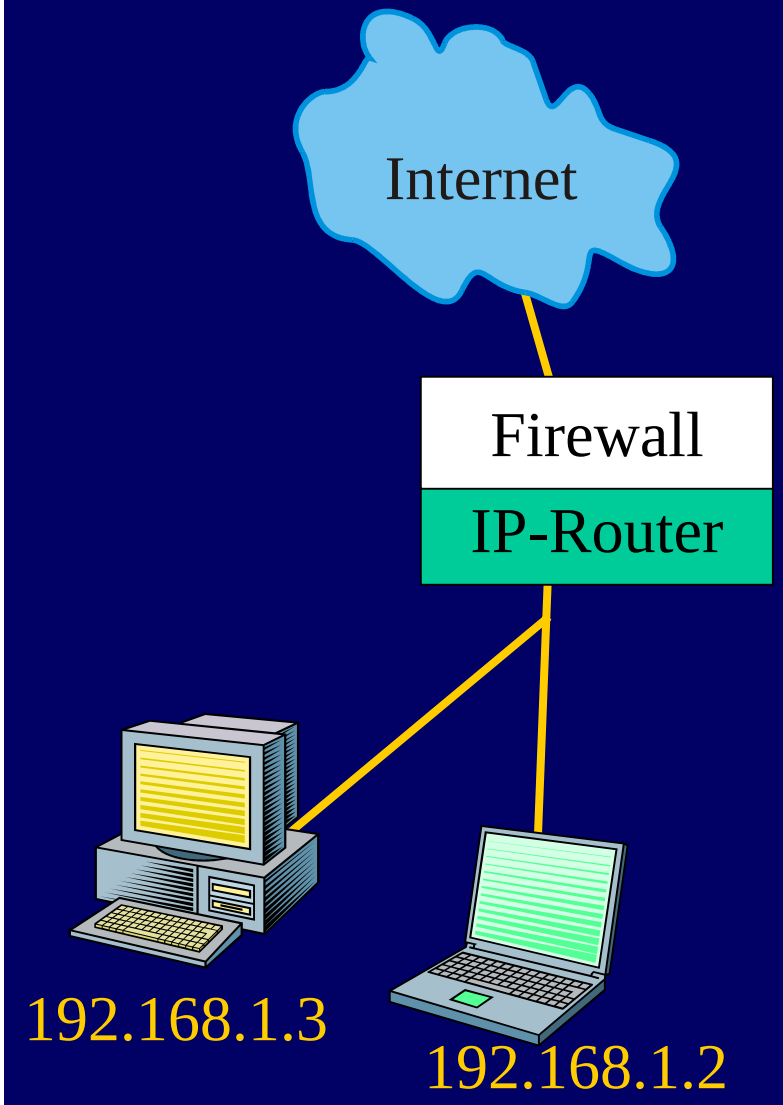


- ein System von Geräten, das den Zugang zum Internet regelt
- ein System, das die eigenen Sicherheitsrichtlinien (security policy) in die Realität umsetzt

security policy

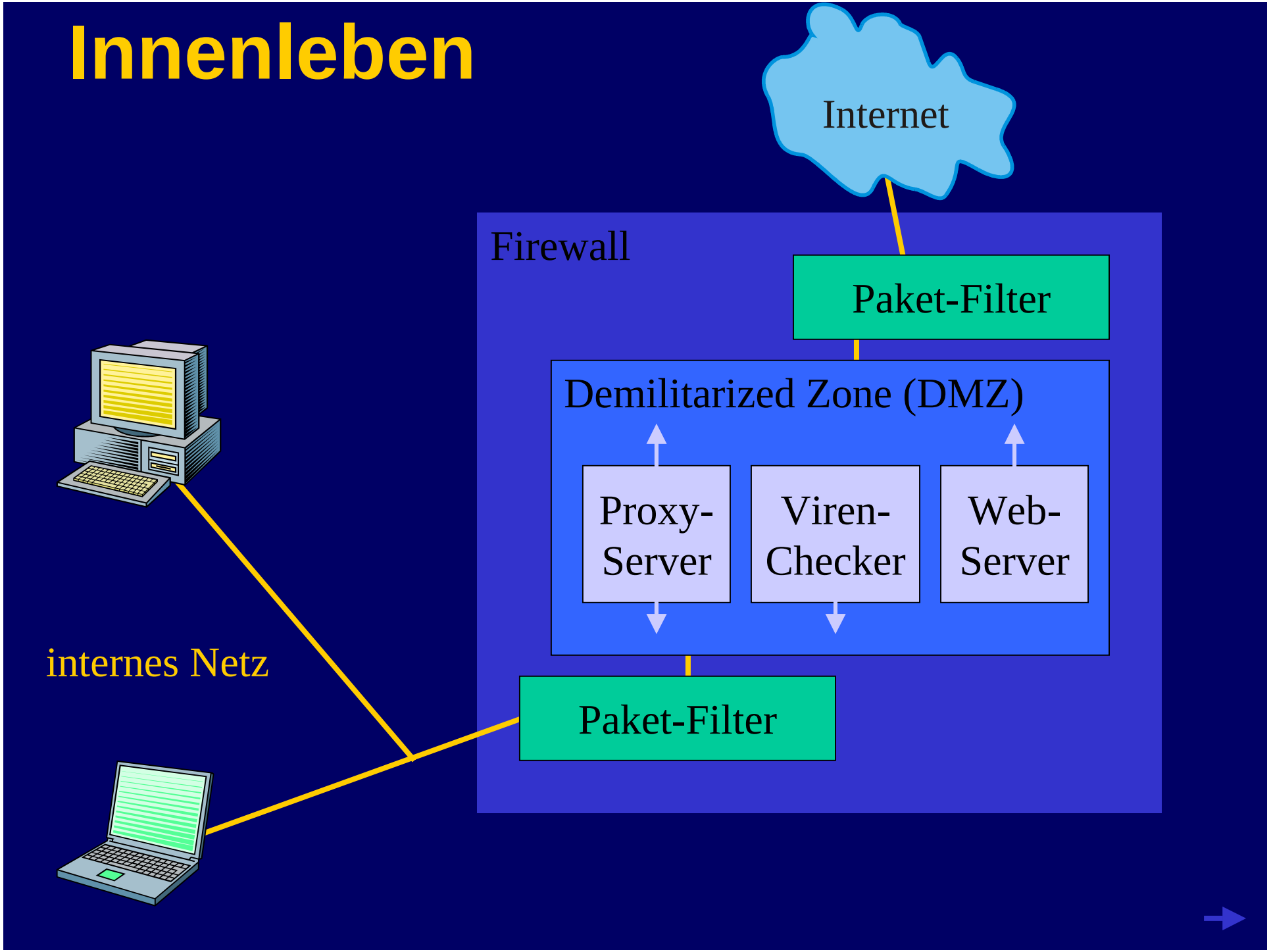
Nur eine gute security policy kann die eigenen Daten schützen.

Position einer Firewall



- eine Firewall muss an der Stelle stehen, wo Datenpakete das lokale Netz verlassen
- Beispiel: Wenn der Laptop-Rechner Daten an einen Computer schicken will, der nicht im Netz 192.168.1.0/24 liegt, müssen die Pakete von einem IP-Router weitergeleitet werden
- Router sind ideale Standorte für Firewalls

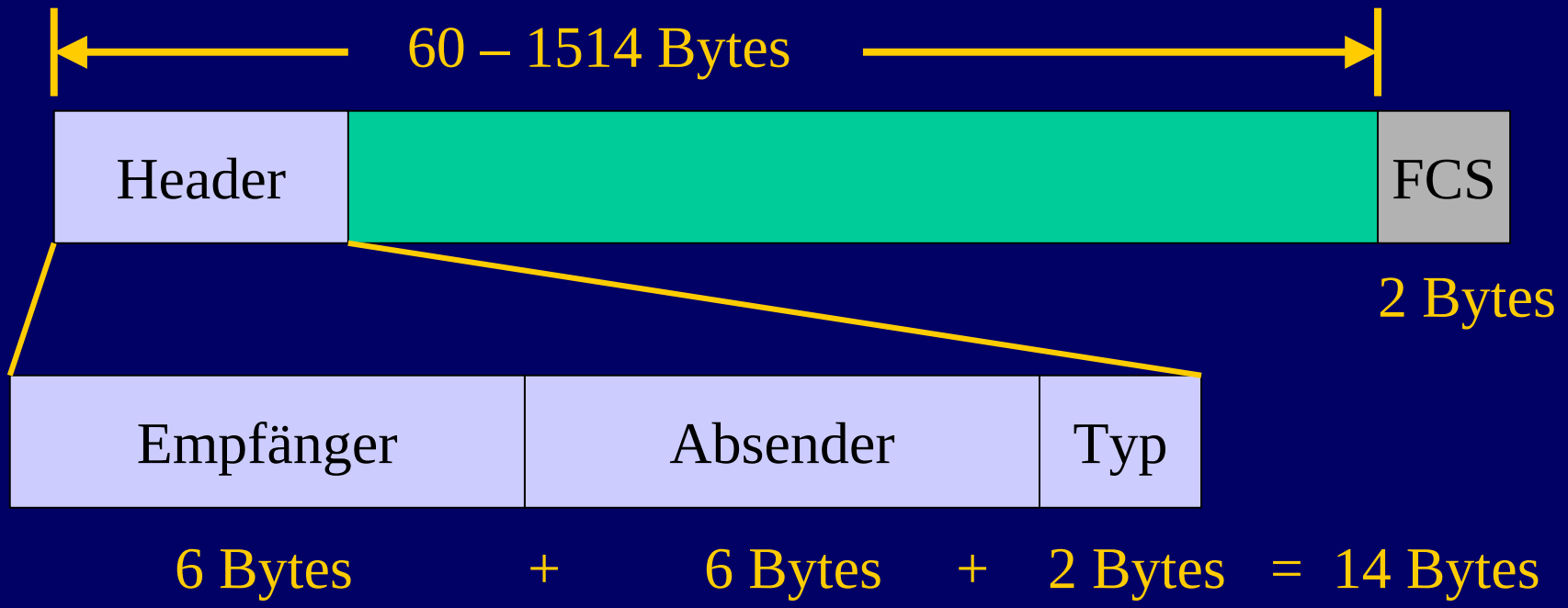
Innenleben


Internet
Firewall
Paket-Filter
Demilitarized Zone (DMZ)
Proxy-Server
Viren-Checker
Web-Server
Paket-Filter
internes Netz

Paket-Filter

- IP-Pakete können anhand von Merkmalen wie Absender- und Empfänger-Adresse oder Diensten (Port-Nummern) gefiltert werden
- IP-Pakete lassen sich auch aufgrund ihrer Zugehörigkeit zu einer IP-Verbindung filtern (stateful inspection – Erfindung des Firewall-Marktführers Checkpoint http://www.checkpoint.com/products/firewall-1/index.html)
- „Filtern“ lässt sich mit drei unterschiedliche Aktionen beschreiben:
  - ACCEPT – das Paket wird weitergeleitet
  - DROP – das Paket wird weggeworfen
  - REJECT – das Paket wird nicht weitergeleitet, stattdessen wird eine Fehlermeldung an den Absender zurückgeschickt

Ethernet-Pakete



- Beispiel: 00:10:B5:5E:D9:A6
- jede Netzwerkkarte hat eine eindeutige Nummer
- die Pakete sind zusätzlich mit einer Prüfsumme versehen (Frame Check Sequence, FCS)
- kaputte Pakete werden nicht repariert sondern ignoriert

Ethernet-Paket-Typen

http://www.iana.org/assignments/ethernet-numbers

Ethernet		Exp. Ethernet		Description	References
decimal	Hex	decimal	octal		
0000	0000-05DC	-	-	IEEE802.3 Length Field	[XEROX]
0257	0101-01FF	-	-	Experimental	[XEROX]
0512	0200	512	1000	XEROX PUP (see 0A00)	[8,XEROX]
0513	0201	-	-	PUP Addr Trans (see 0A01)	[XEROX]
	0400			Nixdorf	[XEROX]
1536	0600	1536	3000	XEROX NS IDP	[133,XEROX]
	0660			DLOG	[XEROX]
	0661			DLOG	[XEROX]
2048	**0800**	513	1001	**Internet IP (IPv4)**	[IANA]
2049	0801	-	-	X.75 Internet	[XEROX]
2050	0802	-	-	NBS Internet	[XEROX]
2051	0803	-	-	ECMA Internet	[XEROX]
2052	0804	-	-	Chaosnet	[XEROX]
2053	0805	-	-	X.25 Level 3	[XEROX]
2054	**0806**	-	-	**ARP**	[IANA]
2055	0807	-	-	XNS Compatability	[XEROX]
2056	0808	-	-	Frame Relay ARP	[RFC1701]
2076	081C	-	-	Symbolics Private	[DCP]
2184	0888-088A	-	-	Xyplex	[XEROX]
2304	0900	-	-	Ungermann-Bass net debugr	[XEROX]
2560	0A00	-	-	Xerox IEEE802.3 PUP	[XEROX]
2561	0A01	-	-	PUP Addr Trans	[XEROX]
2989	0BAD	-	-	Banyan VINES	[XEROX]
...					
...					

0800 Internet IP (IPv4)

0806 ARP

- ARP (Address Resolution Protocol) schafft die Verbindung zwischen Ethernet-Adressen und IP-Adressen
- ARP wird vom Betriebssystem automatisch gemacht

IP-Pakete

ftp://ftp.isi.edu/in-notes/rfc791.txt

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

20 Bytes

IP-Protokoll-Typen

http://www.isi.edu/in-notes/iana/assignments/protocol-numbers

Decimal	Keyword	Protocol	References
0	HOPOPT	IPv6 Hop-by-Hop Option	[RFC1883]
1	**ICMP**	**Internet Control Message**	**[RFC792]**
2	IGMP	Internet Group Management	[RFC1112]
3	GGP	Gateway-to-Gateway	[RFC823]
4	IP	IP in IP (encapsulation)	[RFC2003]
5	ST	Stream	[RFC1190,RFC1819]
6	**TCP**	**Transmission Control**	**[RFC793]**
7	CBT	CBT	[Ballardie]
8	EGP	Exterior Gateway Protocol	[RFC888,DLM1]
9	IGP	any private interior gateway (used by Cisco for their IGRP)	[IANA]
10	BBN-RCC-MON	BBN RCC Monitoring	[SGC]
11	NVP-II	Network Voice Protocol	[RFC741,SC3]
12	PUP	PUP	[PUP,XEROX]
13	ARGUS	ARGUS	[RWS4]
14	EMCON	EMCON	[BN7]
15	XNET	Cross Net Debugger	[IEN158,JFH2]
16	CHAOS	Chaos	[NC3]
17	**UDP**	**User Datagram**	**[RFC768,JBP]**
18	MUX	Multiplexing	[IEN90,JBP]
19	DCN-MEAS	DCN Measurement Subsystems	[DLM1]

...

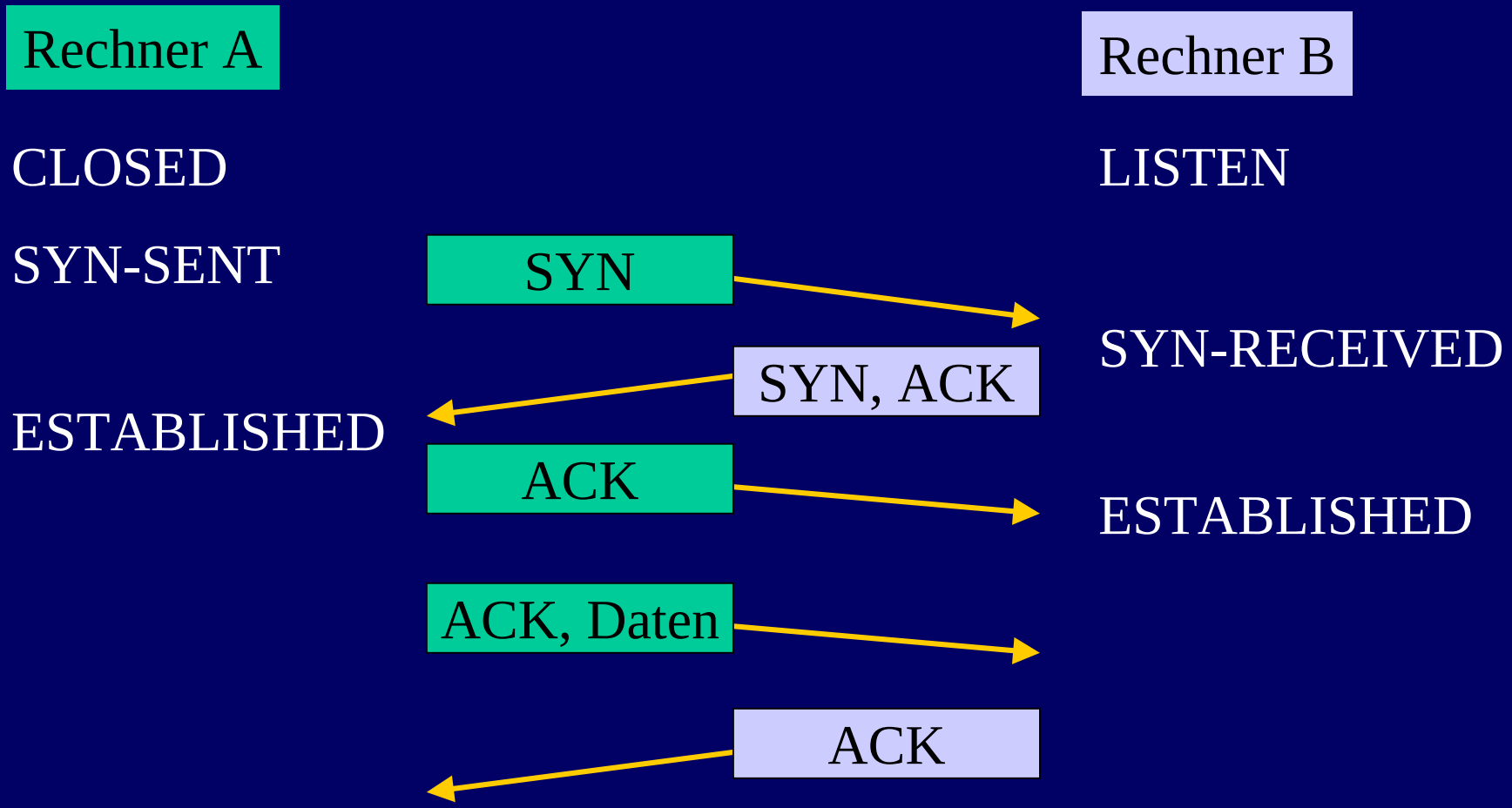
1	**ICMP Internet Control Message**	**[RFC792]**
6	**TCP Transmission Control**	**[RFC793]**
17	**UDP User Datagram**	**[RFC768,JBP]**

ICMP, TCP und UDP

- ICMP wird für die Übermittlung von Fehlermeldungen benötigt. Folgende Fehlersituationen führen u.a. zu ICMP-Meldungen:
  - Der Empfänger des Pakets kann nicht erreicht werden (destination unreachable).
  - Der Lebensdauer-Zähler des IP-Paketes ist abgelaufen (time exceeded)
  - Ein Paket war zu groß für einen Übertragungskanal auf dem Weg zum Empfänger und müsste in mehrere Stücke aufgeteilt werden (fragmentation needed)
- UDP wird für Broadcast-Anwendungen oder kurze Frage-Antwort-Sequenzen benutzt. Die Übertragung der Pakete ist nicht gesichert. Verlorene Pakete muss die Anwendung selbst rekonstruieren.
- TCP ermöglicht die gesicherte Übertragung von Byte-Strömen. Verlorene Pakete werden automatisch nochmal geschickt.
- UDP und TCP beinhalten Port-Nummern (16-Bit). Damit lassen sich verschiedene unabhängige Kommunikationskanäle auf einem Rechner realisieren (nur die IP-Nummer reicht dafür nicht).

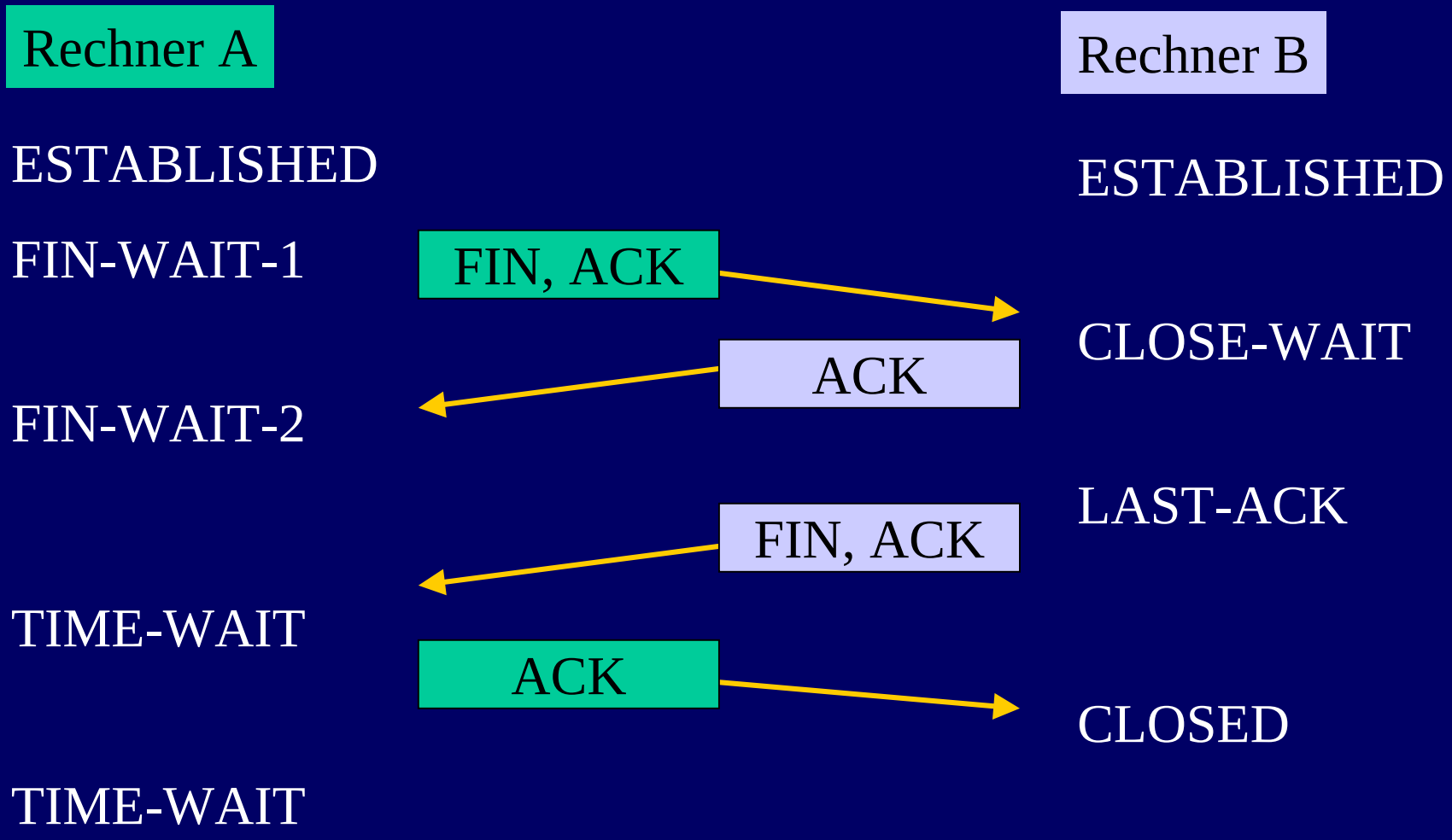
TCP-Verbindung

ftp://ftp.isi.edu/in-notes/rfc793.txt



TCP-Verbindungsabbau

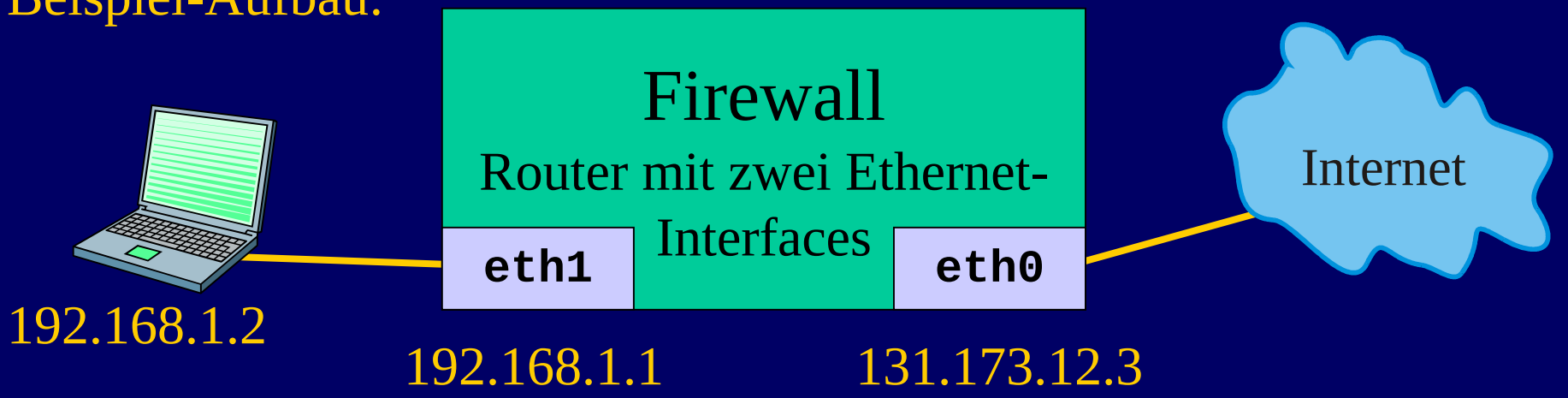
ftp://ftp.isi.edu/in-notes/rfc793.txt



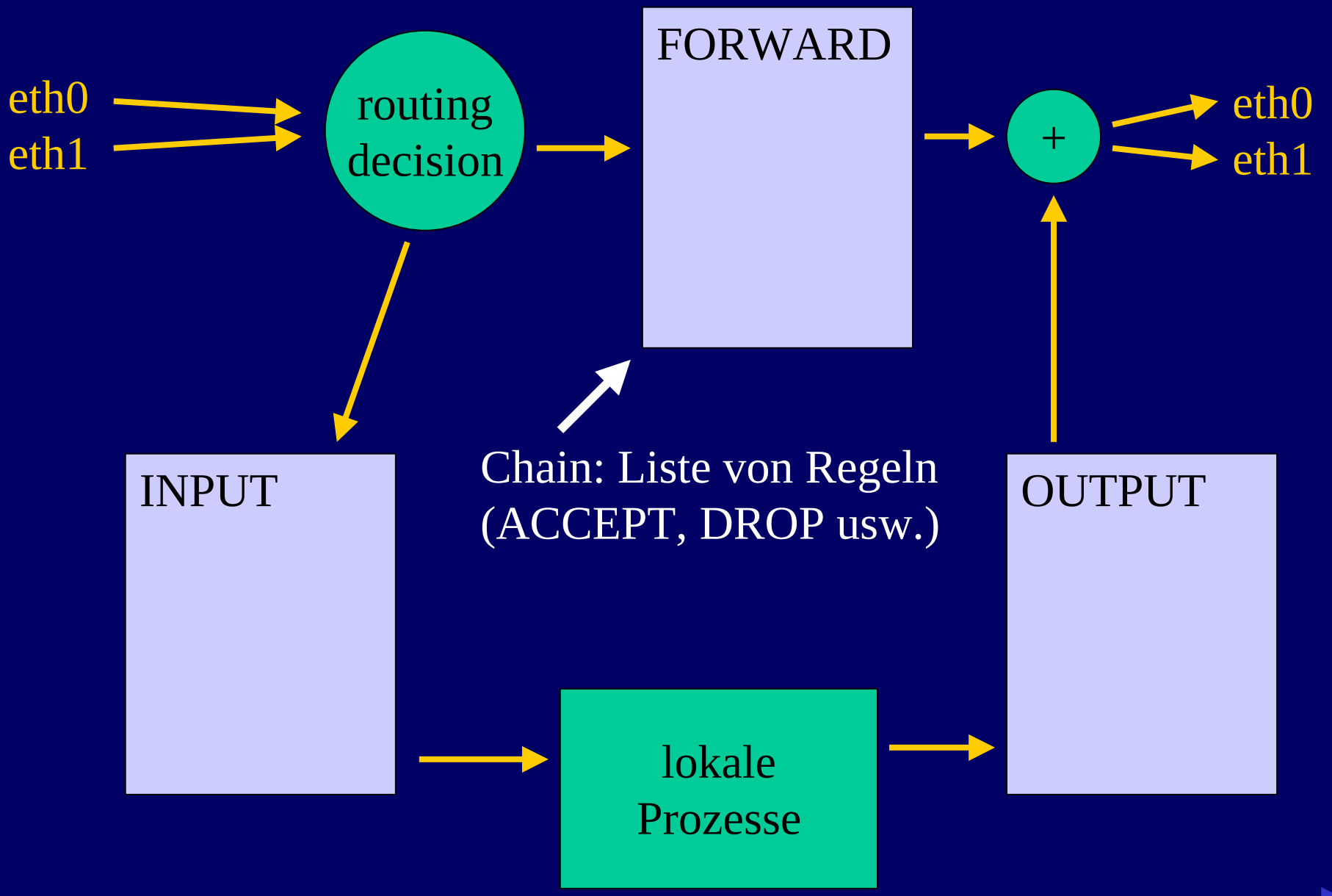
DIY-Firewall mit iptables

- http://netfilter.samba.org
- iptables ist in der neuen Linux-Version 2.4 enthalten
- modularer Aufbau, dadurch erweiterbar
- stateful inspection durch ip_conntrack-Modul
- einfache Konfiguration von NAT (Network Address Translation)
- in diesem Beispiel gibt es keine DMZ und deswegen „nur“ ein Paket-Filter

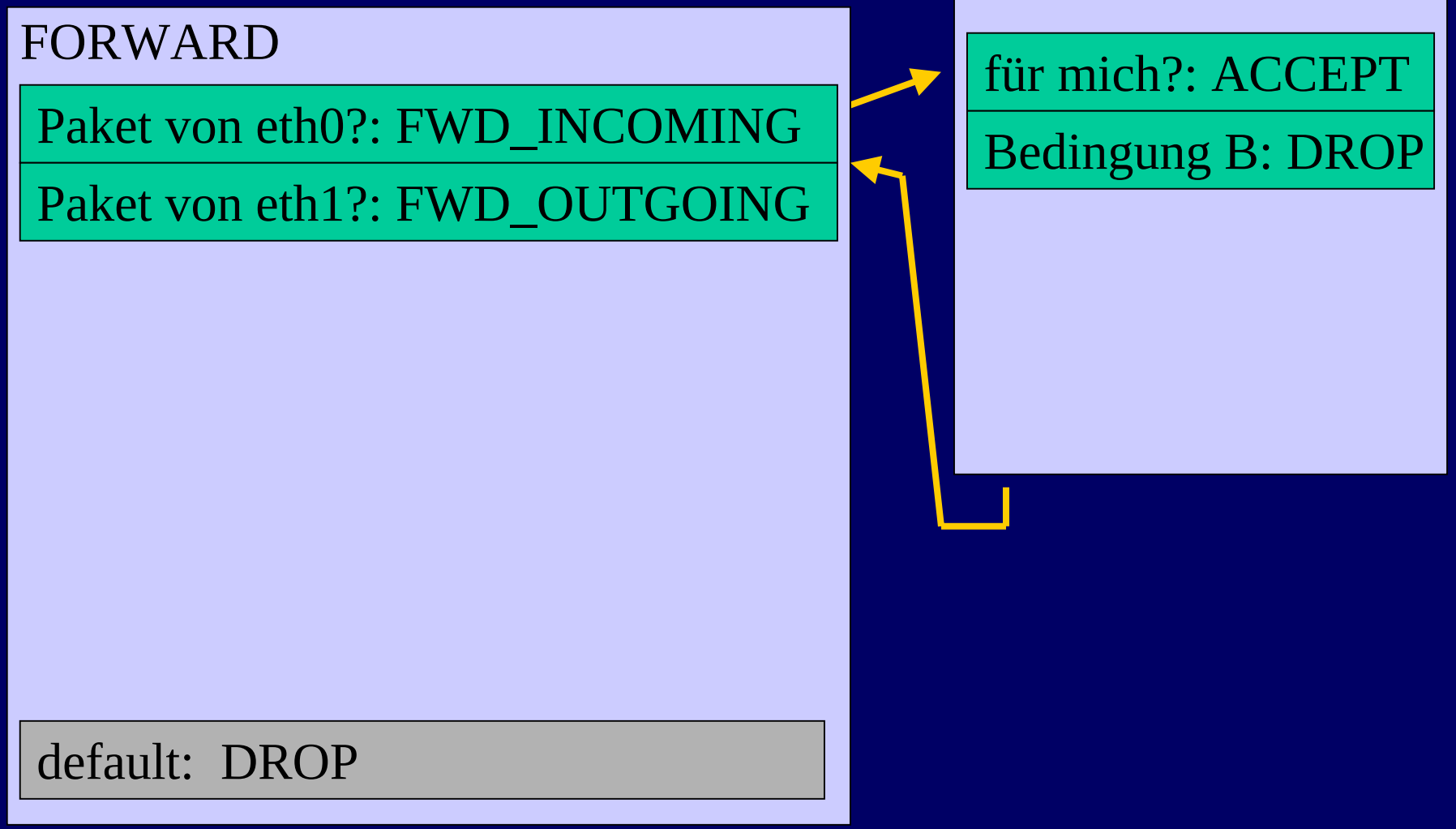
Beispiel-Aufbau:



iptables-Filter-Struktur



Chains


FORWARD
Paket von eth0?: FWD_INCOMING
Paket von eth1?: FWD_OUTGOING
default: DROP
FWD_INCOMING
für mich?: ACCEPT
Bedingung B: DROP