

FIREWALLS

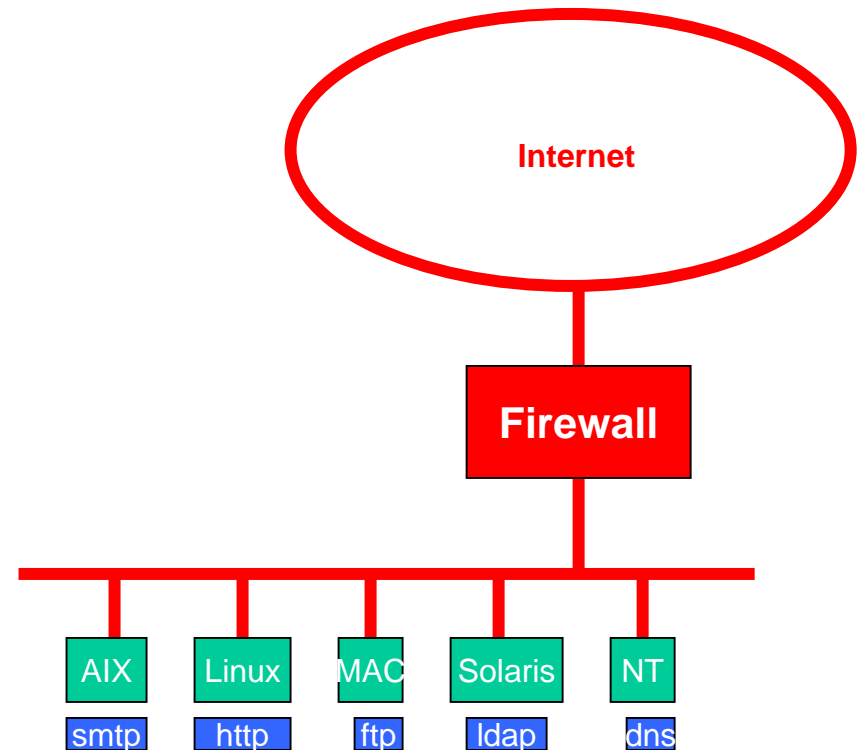
Technik - Typen - Topologien

Helmut Elschner
helmut.elschner@materna.de

IT - Security

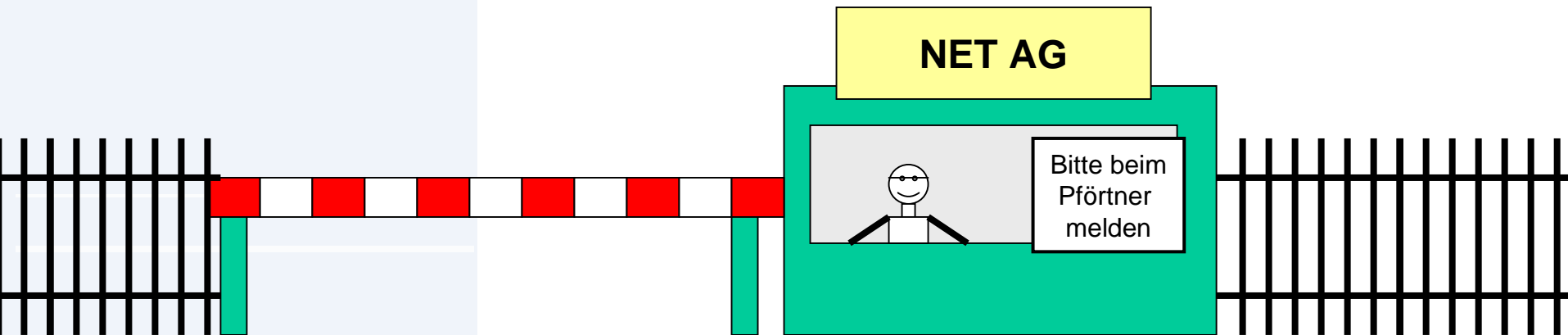
hat verschiedene Aspekte, z.B.:

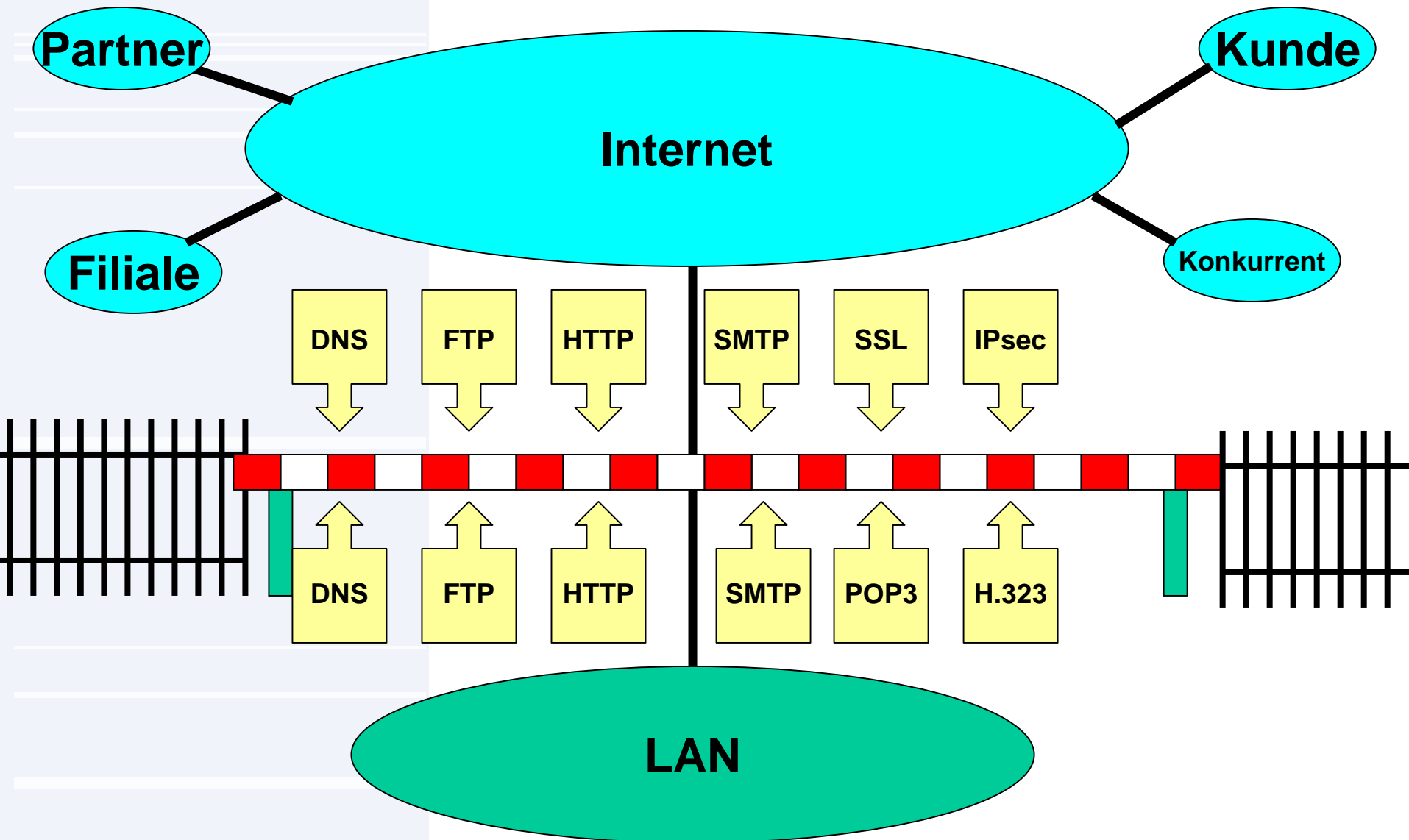
- **Network - Security**
- **Host - Security**
- **Content - Security**



Definition „Firewall“

Eine FIREWALL ist ein System, das den Datenverkehr zwischen einem zu schützenden Netz (z.B. LAN) und einem unsicheren Netz (z.B. Internet) gemäß einer festgelegter Sicherheitsregeln überwacht, kontrolliert und protokolliert.





WER DARF WAS?

WER darf mit WEM kommunizieren?

WER darf WELCHEN DIENST nutzen?

Unterscheidung nach IP-Adressen, Ports, Benutzern, Gruppen, ...

Zwei unterschiedliche Ansätze:

1. „DENY ALL“ - alles was nicht explizit erlaubt ist, ist verboten!
2. „LAISSEZ FAIRE“ - alles was nicht explizit verboten ist, ist erlaubt!

Alle internen LAN-User sollen über den Proxy surfen können.

E-Mails sollen nur über den Firmenserver verschickt werden.

Alle Internetbenutzer dürfen unsere Webserver besuchen.

Alle Internetsysteme dürfen uns E-Mail schicken.

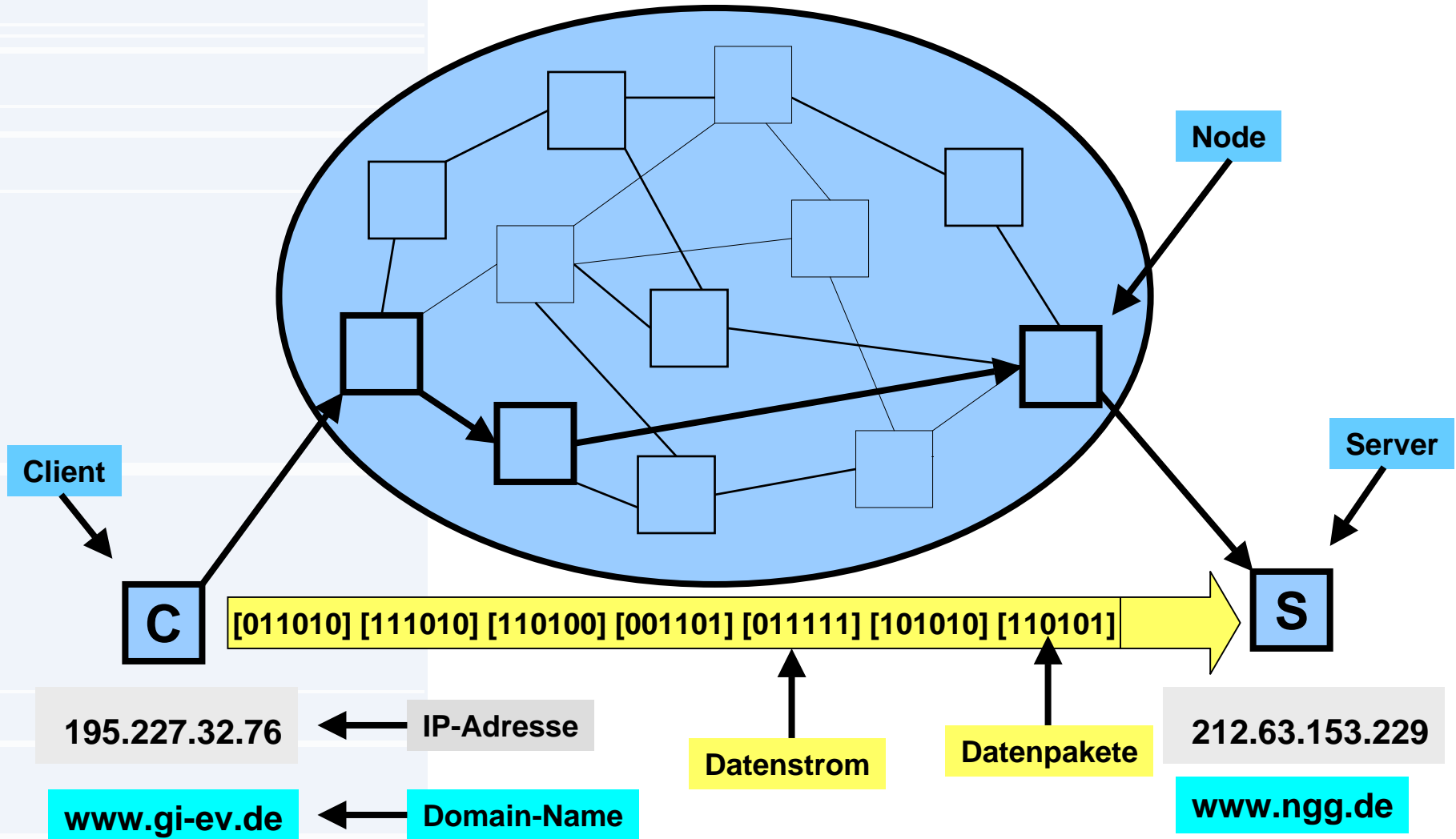
Die Filiale Hongkong soll eine VPN-Verbindung aufbauen können.

Die Nutzung von Telnet ist untersagt.

FTP-Zugriff von aussen nur lesend erlaubt.

Die Gruppe der Administratoren darf den Webserver per FTP pflegen.

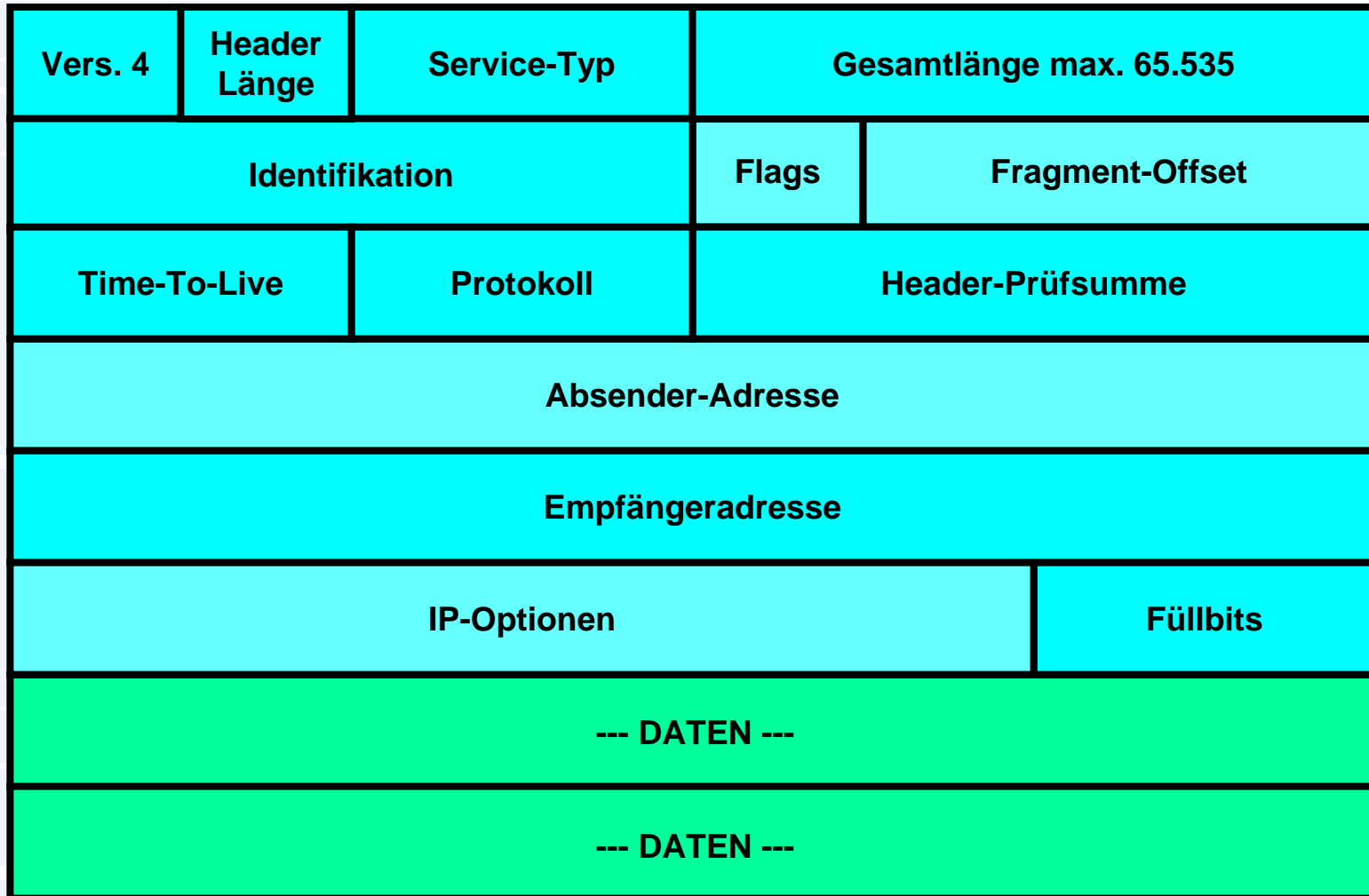
Modem- und ISDN-Verbindungen sind strikt untersagt!



Application	7	Anwendung
Presentation	6	Darstellung
Session	5	Sitzung
Transport	4	Transport
Network	3	Vermittlung
Data Link	2	Sicherung
Physical	1	Bitübertragung

Application	TELNET - SMTP - FTP - DNS - SNMP
Presentation	
Session	
Transport	TCP - UDP
Network	ARP - IP - ICMP
Data Link	Ethernet - Token Ring - FDDI
Physical	

Aufbau eines IP-Paketes



Einige IP - Protokolle

1	ICMP	Internet Control Message Protocol
4	IP/IP	IP in IP (encapsulation)
6	TCP	Transmission Control Protocol
8	EGP	Exterior Gateway Protocol (Routing Protocol)
9	IGP	Interior Gateway Protocol (Routing Protocol)
17	UDP	User Datagram Protocol
41	IPv6	IP - Version 6
50	ESP	Encapsulated Security Payload (IPsec - VPN)
51	AH	Authentication Header (IPsec - VPN)
57	SKIP	Simple Key Management for Internet Protocols (IPsec - VPN)
89	OSPF	Open Shortest Path First (Routing Protocol)
94	IPIP	IP in IP (encapsulation)
106	QNX	QNX (Kommunikation für Echtzeitbetriebssystem)
115	L2TP	Layer Two Tunneling Protocol

IP - Internet Protocol

- **Paketvermittlung von Host zu Host**
- **Routing über Zwischenknoten**
- **Keine Adressierung von Diensten**

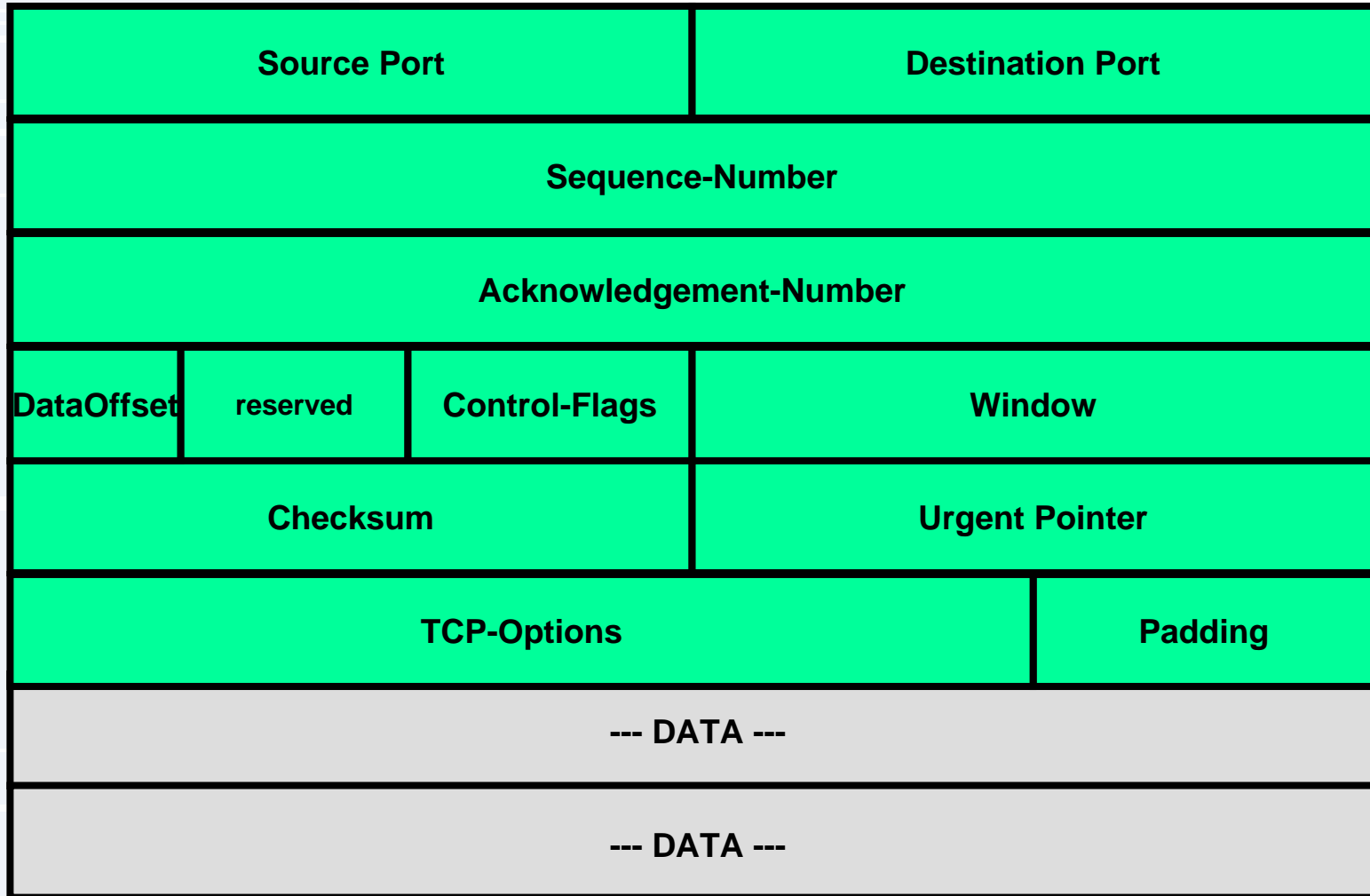
UDP - User Datagram Protocol

- **Adressierung von Diensten / Programmen auf Hosts**
- **keine gesicherte Übertragung**

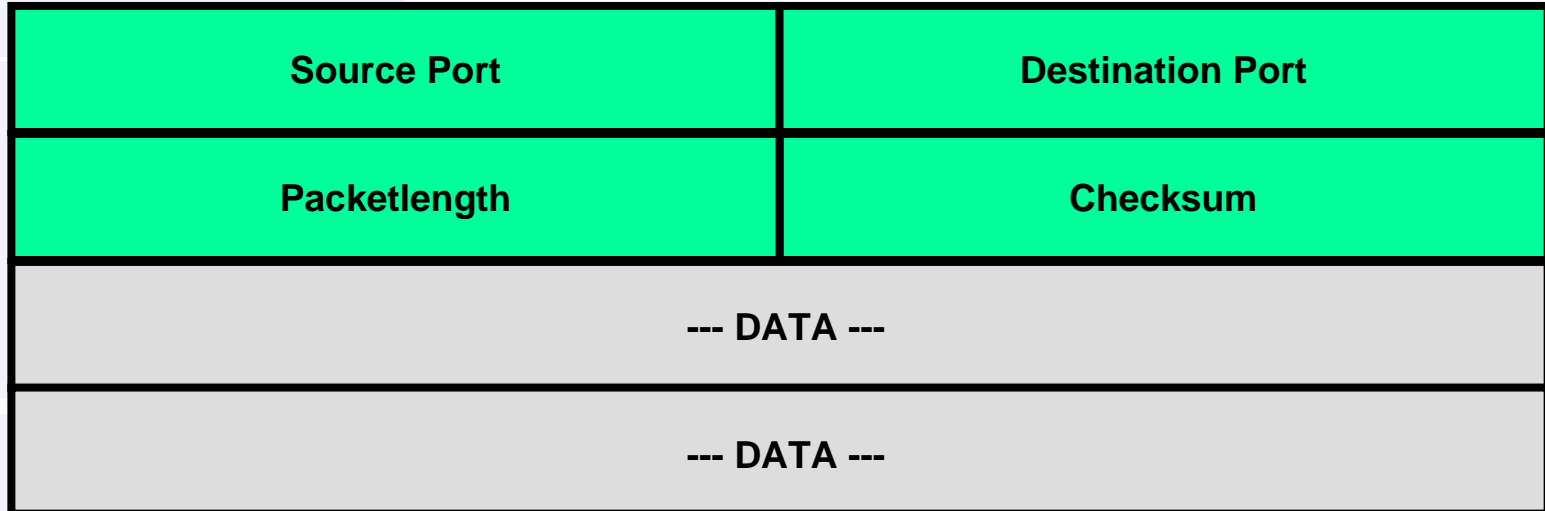
TCP - Transmission Control Protocol

- **Adressierung von Diensten / Programmen auf Hosts**
- **gesicherte Übertragung**
- **Neusenden verlorener Pakete**
- **garantierte Zustellung in der Reihenfolge des Absendens**

Aufbau eines TCP-Paketes

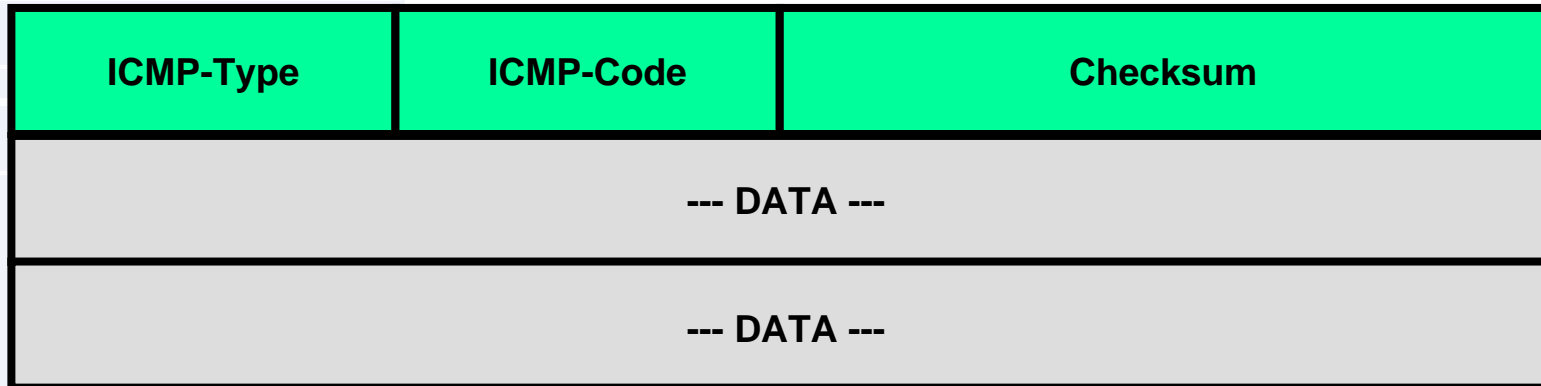


Aufbau eines UDP-Paketes



Einige UDP / TCP - Ports

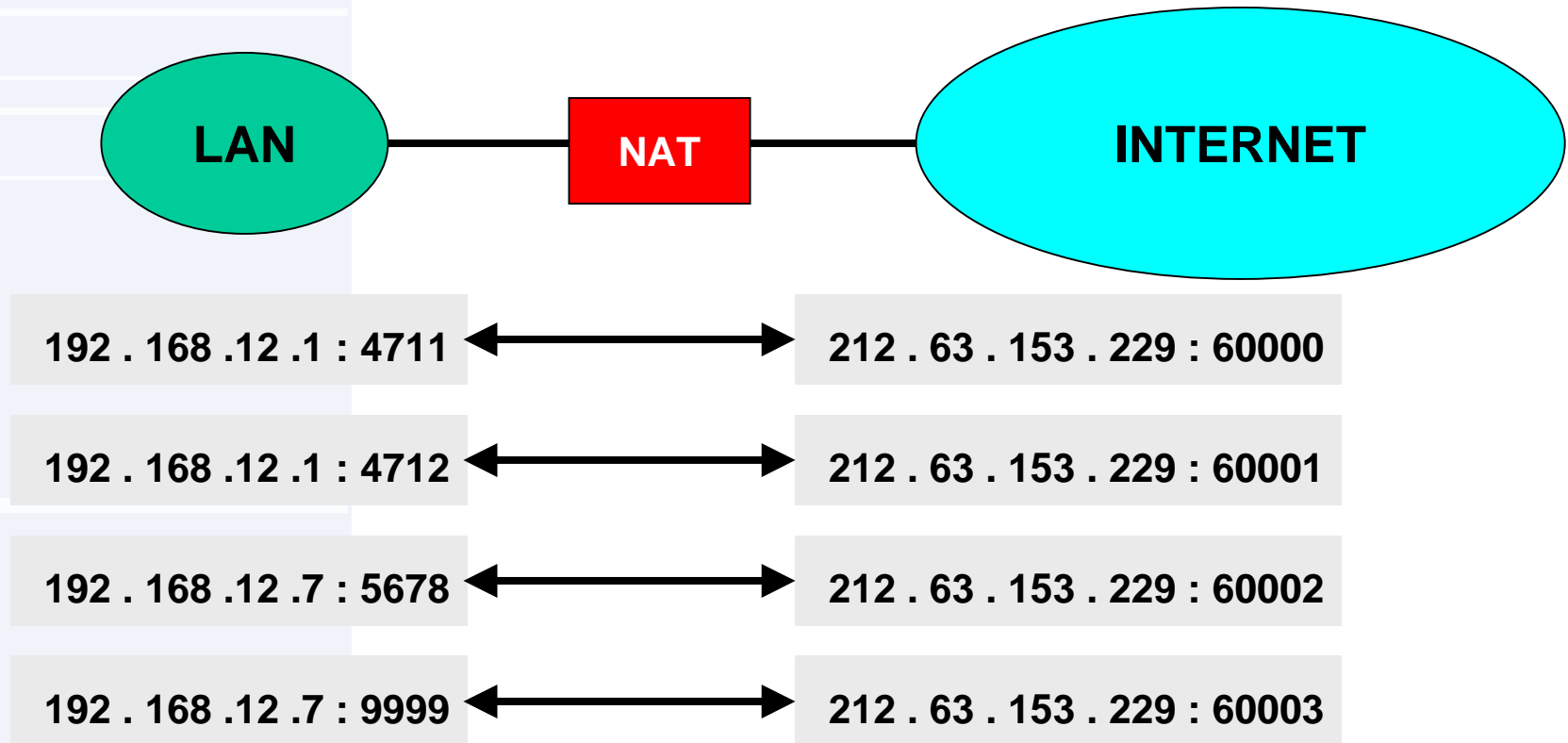
7	TCP/UDP	ECHO
20	TCP	FTP-DATA - File Transfer Protocol (Datenverbindung)
21	TCP	FTP - File Transfer Protocol (Kontrollverbindung)
23	TCP	TELNET - Rechnerfernsteuerung (Unix-Welt)
25	TCP	SMTP - Simple Mail Transfer Protocol (E-Mail versenden)
53	TCP/UDP	DNS - Domain Name System
79	TCP	finger - Abfrage von Informationen
80	TCP	HTTP - Hyper Text Transfer Protocol (World Wide Web)
110	TCP	POP3 - Post Office Protocol 3 (E-Mail abholen)
137	TCP/UDP	NETBIOS Name Service
138	UDP	NETBIOS Datagram Service
139	TCP	NETBIOS Session Service
389	TCP	LDAP - Lightweight Directory Access Protokoll
443	TCP	HTTPS - HTTP über gesicherte Verbindung (SSL)
500	UDP	ISAKMP - IKE Internet Key Exchange



0	Echo Reply Message (Echo-Antwort)
3	Destination Unreachable Message
4	Source Quench Message (Senderate drosseln)
5	Redirect Message (Route ändern)
8	Echo Request Message (Echo-Anforderung)
9	Router Advertisement Message (Router-Bekanntmachung)
10	Router Solicitation Message (Suche nach einem Router)
11	Time Exceed Message (Lebenszeit eines IP-Pakets überschr.)
12	Parameter Problem Message (Parameterfehler im IP-Paket)
13	Time Stamp Request Message (Uhrzeitangabe-Anforderung)
14	Time Stamp Reply Message (Uhrzeitangabe-Antwort)
15	Information Request Message
16	Information Reply Message
17	Address Mask Request (Abfrage der Subnetz-Maske)
18	Address Mask Reply (Antwort auf Abfrage der Subnetz-Maske)

TCP/IP-Paket mit IP- und TCP-Header

Vers. 4	Header Länge	Service-Typ	Gesamtlänge max. 65.535	
Identifikation			Flags	Fragment-Offset
Time-To-Live		Protokoll	Header-Prüfsumme	
Absender-Adresse				
Empfängeradresse				
IP-Optionen				Füllbits
Sendeport			Empfangsport	
Sequenz-Nummer				
Bestätigungs-Nummer				
H.-Länge	reserviert	Code-Bits	Fenster	
Prüfsumme				
TCP-Optionen				Füllbits
--- DATEN ---				
--- DATEN ---				



Unter Linux spricht man von Masquerading

Filterung der Datenpakete nach

- **Senderichtung**
- **IP-Adresse des Absenders**
- **IP-Adresse des Empfängers**
- **TCP/UDP-Port des Absenders**
- **TCP/UDP-Port des Empfängers**
- **ICMP-Typ**

Transport

Network

Data Link

Physical

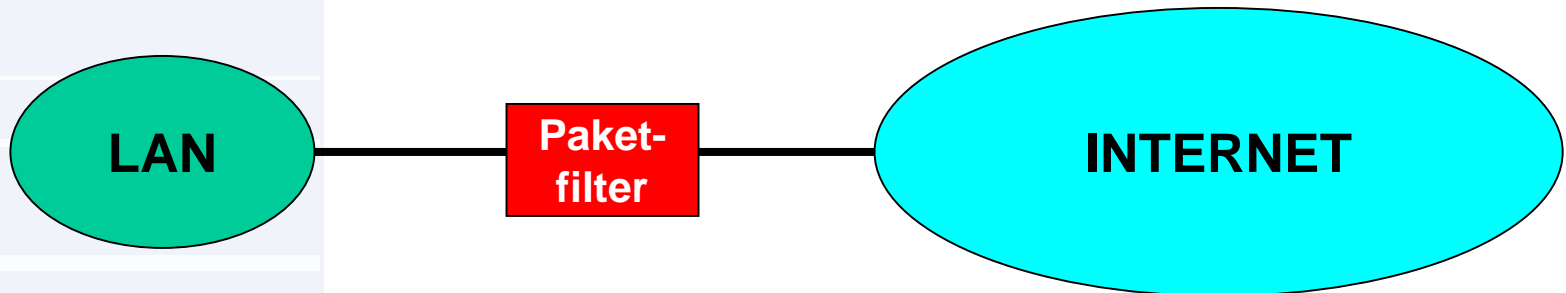
Paketfilter

Realisierung durch:

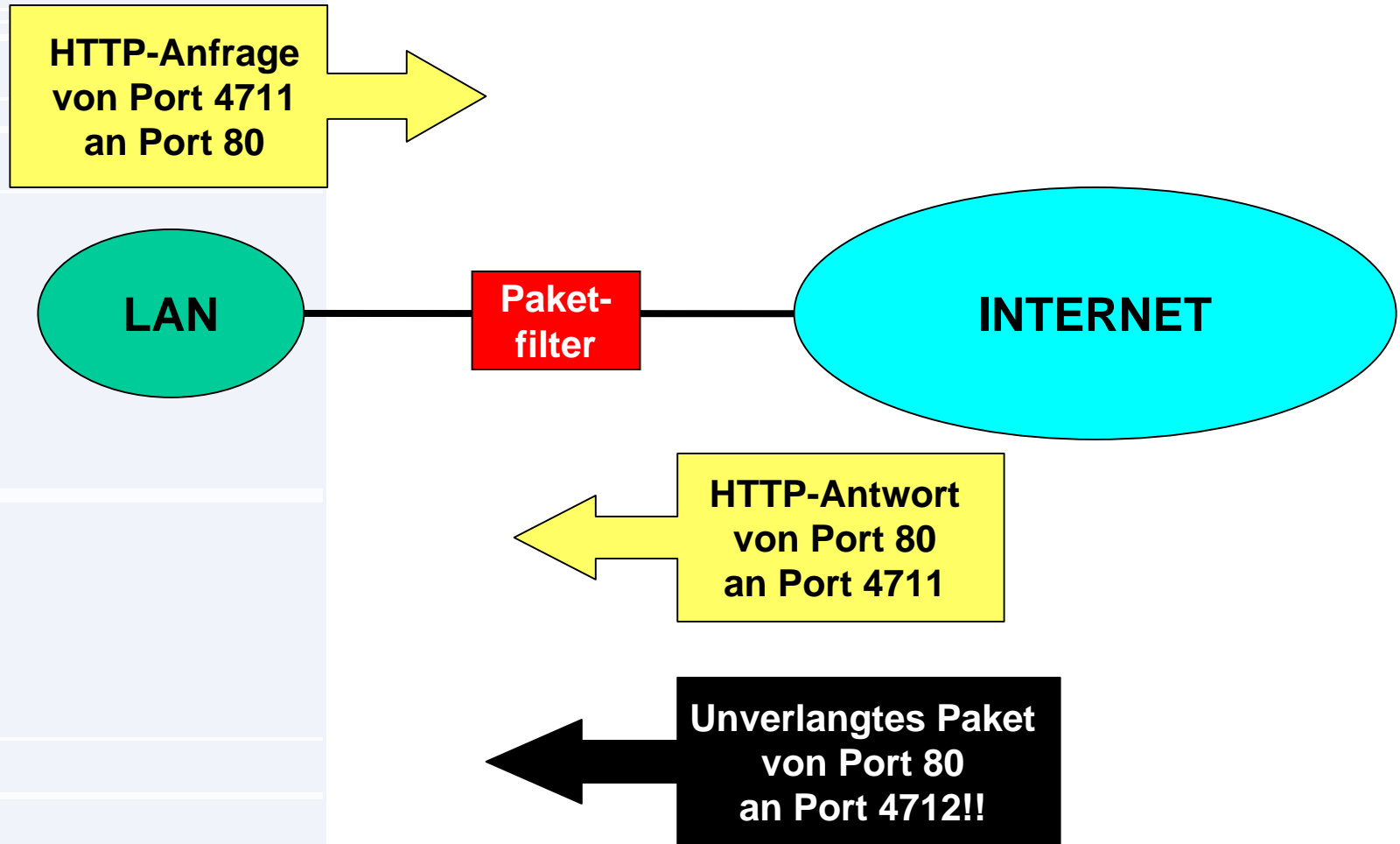
- Router mit Access-Control-Lists (ACL)
- Linux-Rechner mit ipchains/iptables
- Dual-Homed-Host (ohne Forwarding)

**PFÖRTNER-
PRINZIP:**

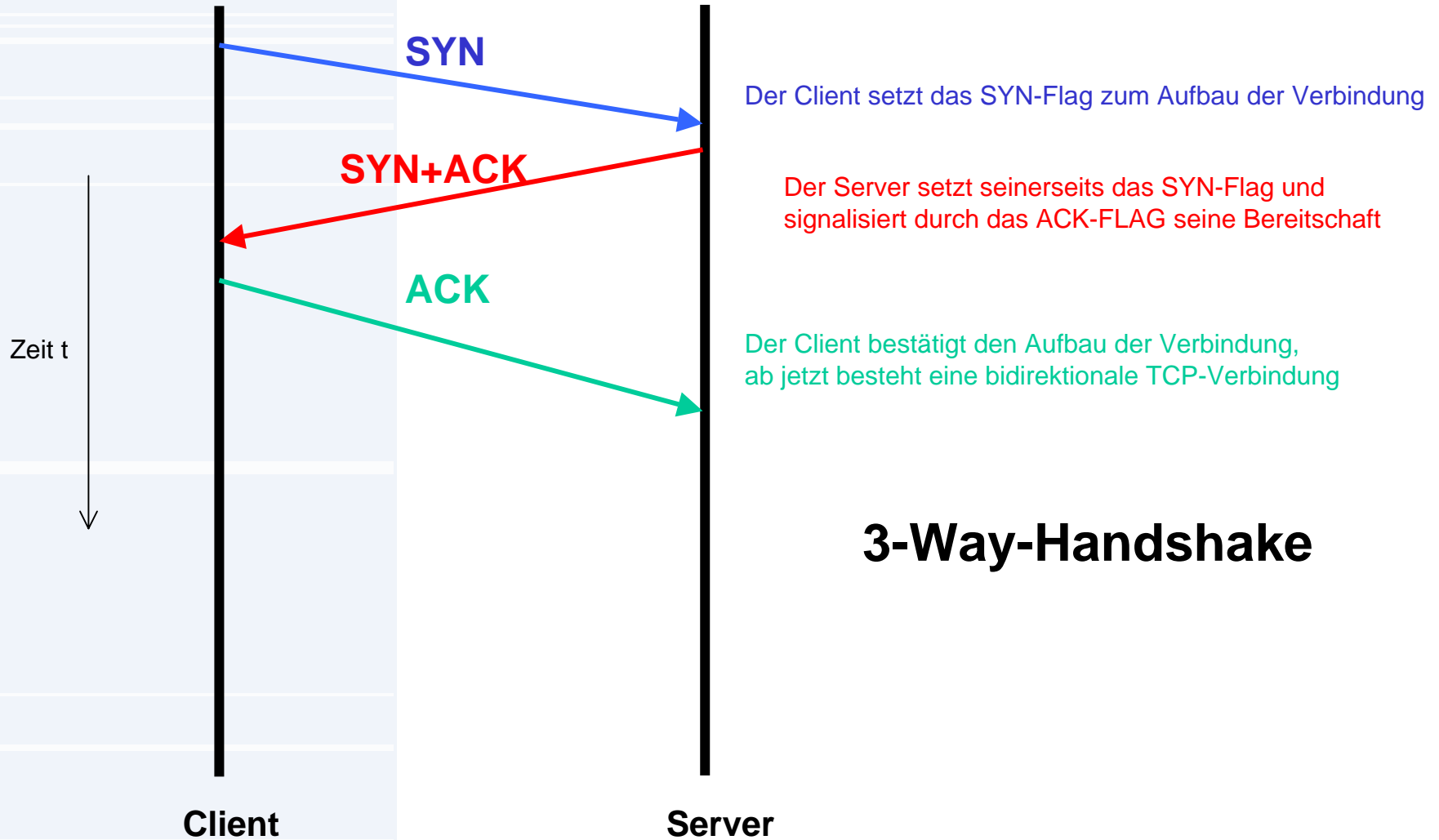
**DURCHLASSEN
ODER VERWERFEN
VON PAKETEN**



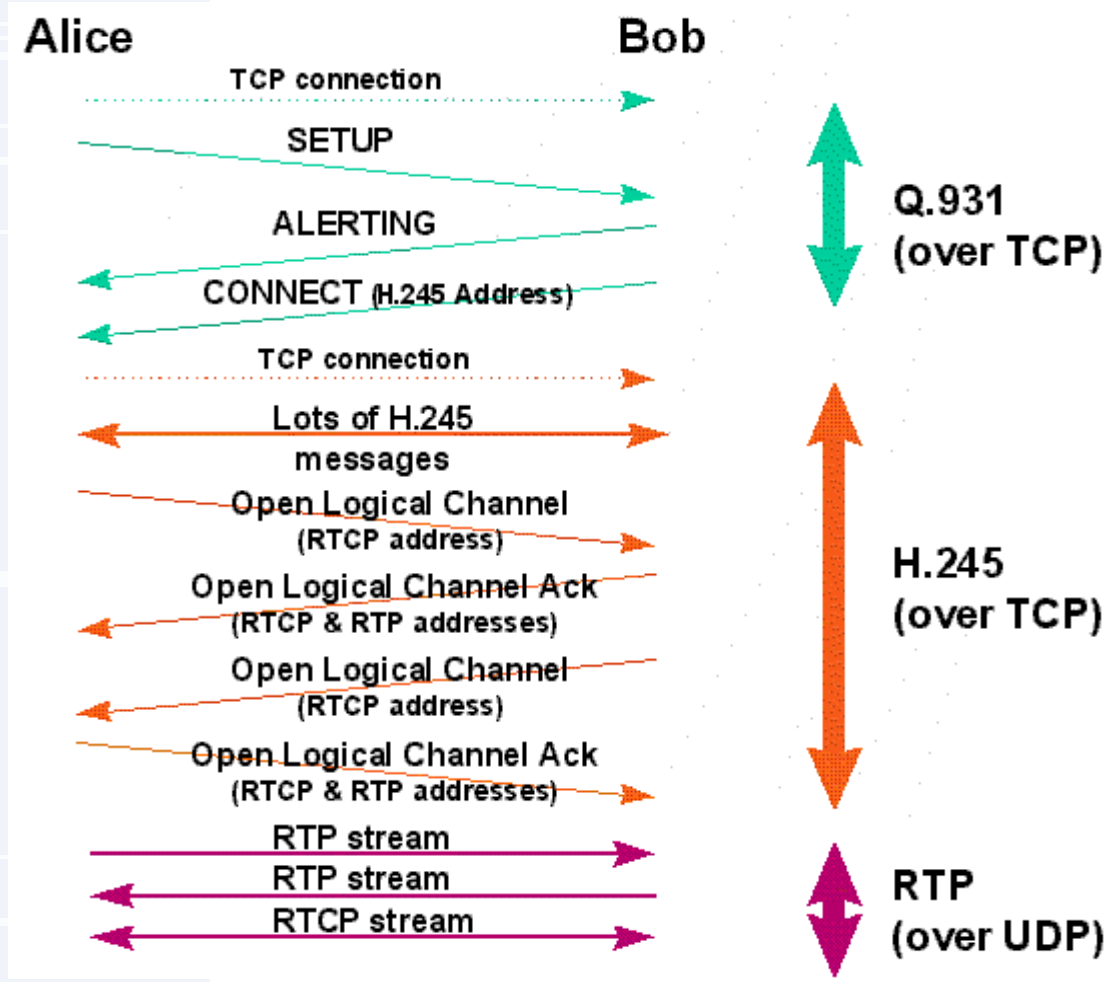
Problem der Antwortpakete



TCP - Verbindungsaufbau



Die Hölle für FW-Admins: H.323

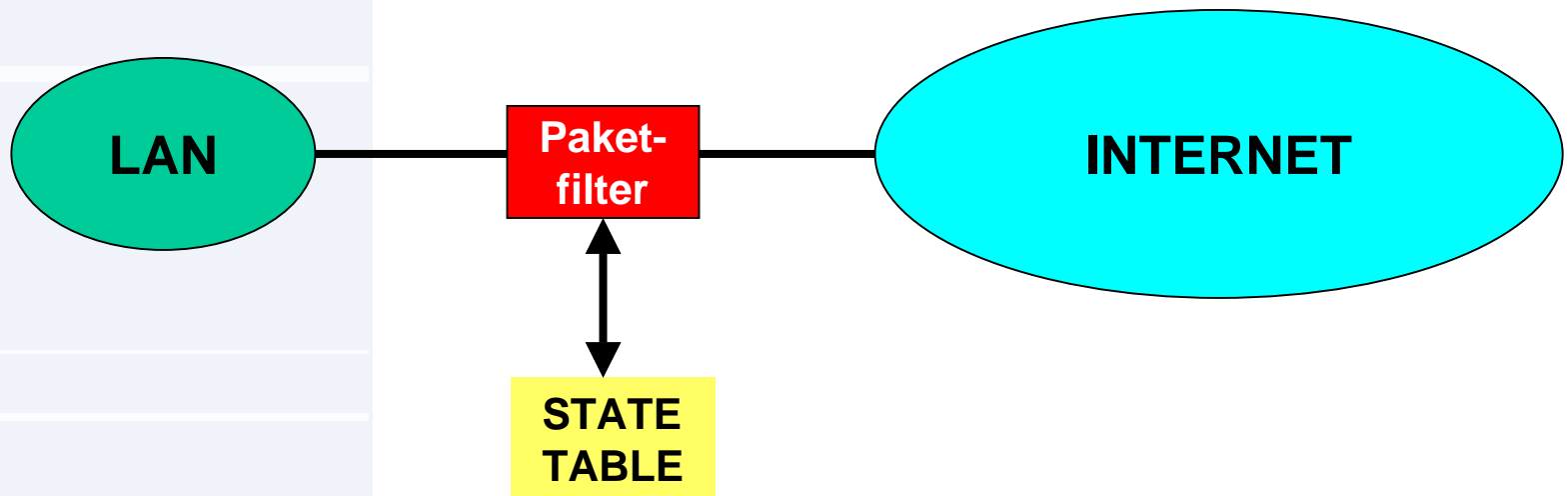


© INTEL: The Problems and Pitfalls of Getting H.323 Safely Through Firewalls
 Siehe unter http://support.intel.com/support/telephony/trial21/h323_wpr.htm

Dynamische Paketfilter

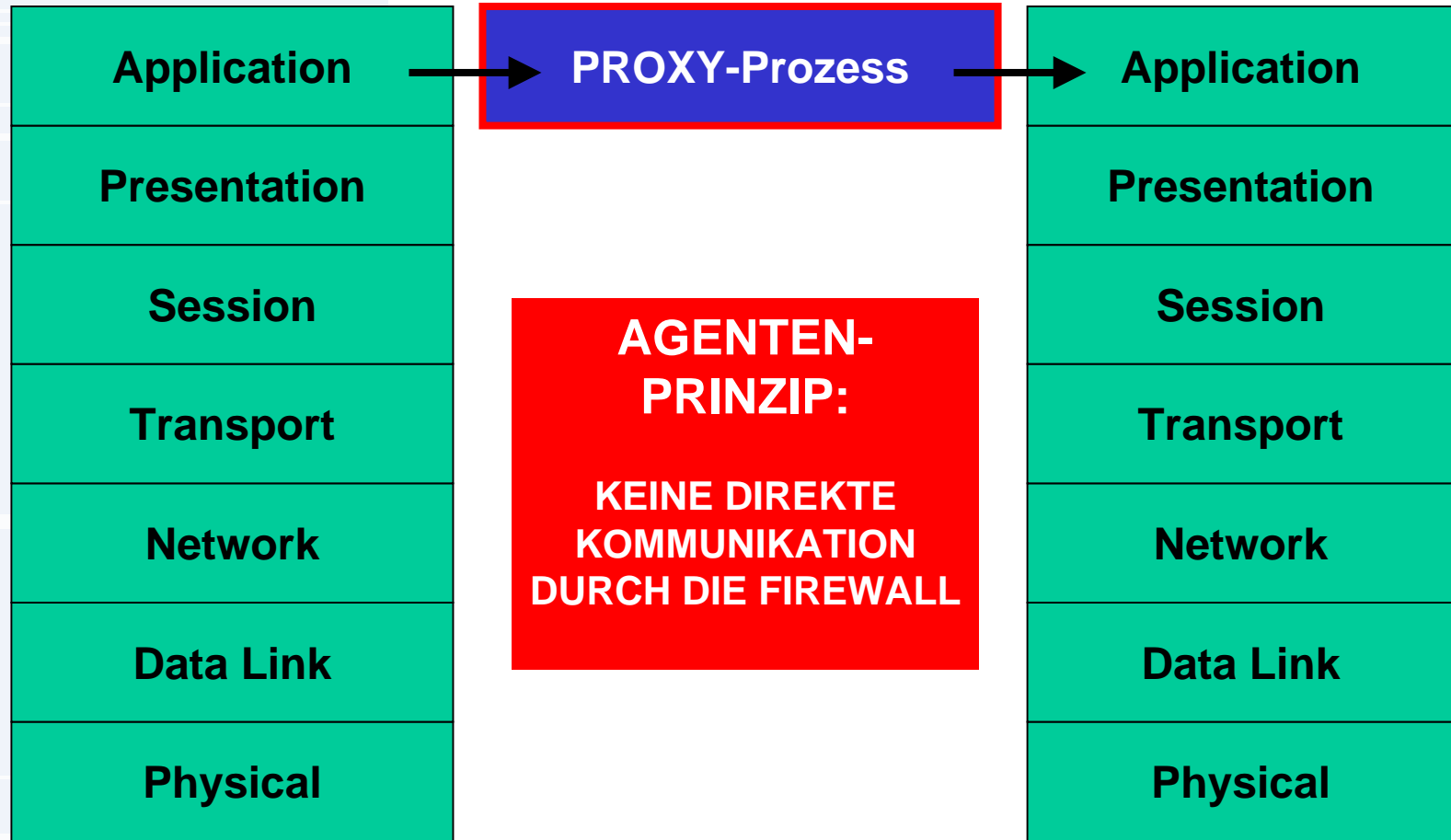
arbeiten wie statische Paketfilter, aber

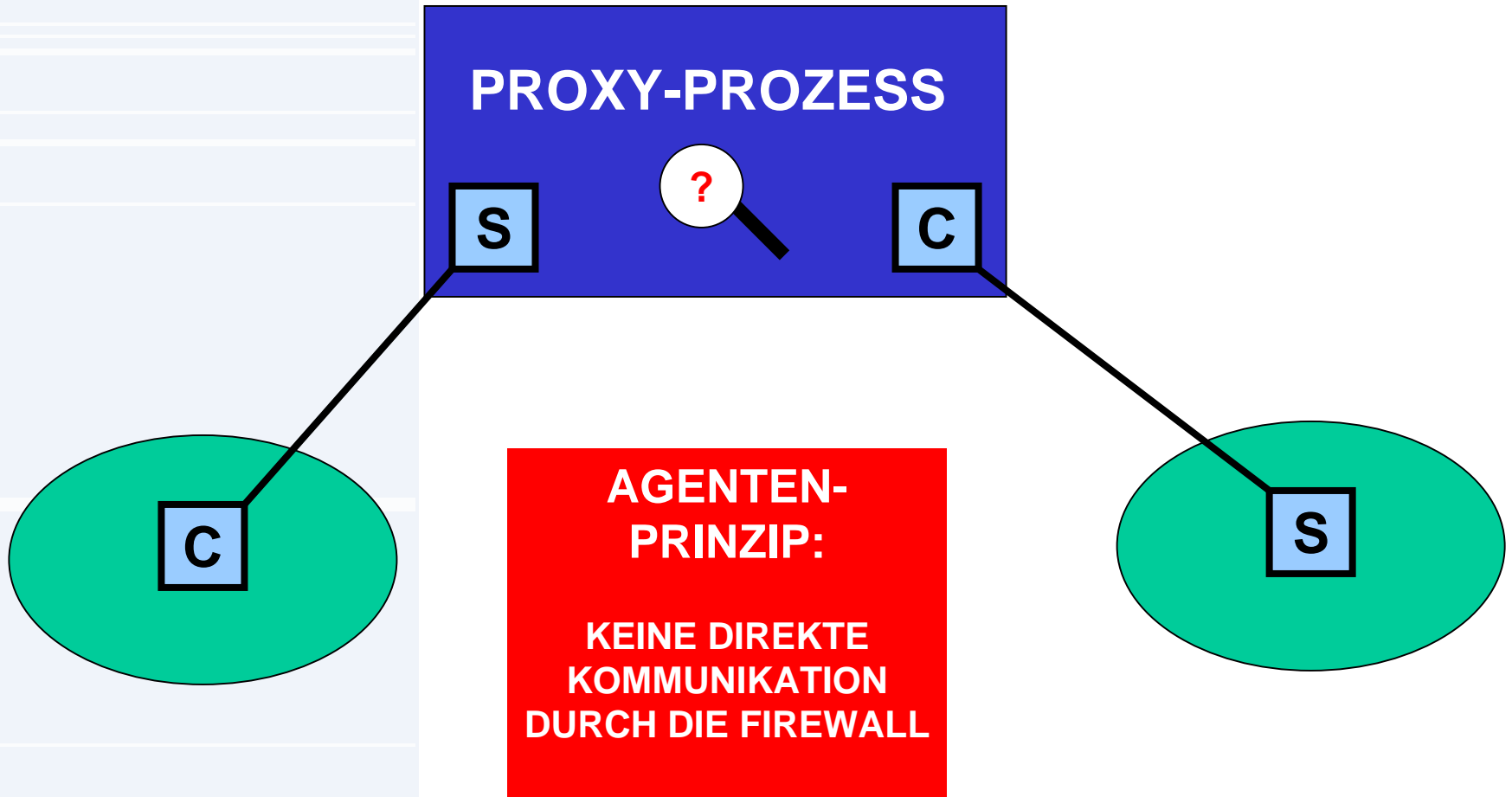
- kennen TCP-Verbindungsaufbau
- kennen „virtuelle“ UDP-Verbindungen
- kennen Besonderheiten einiger Protokolle



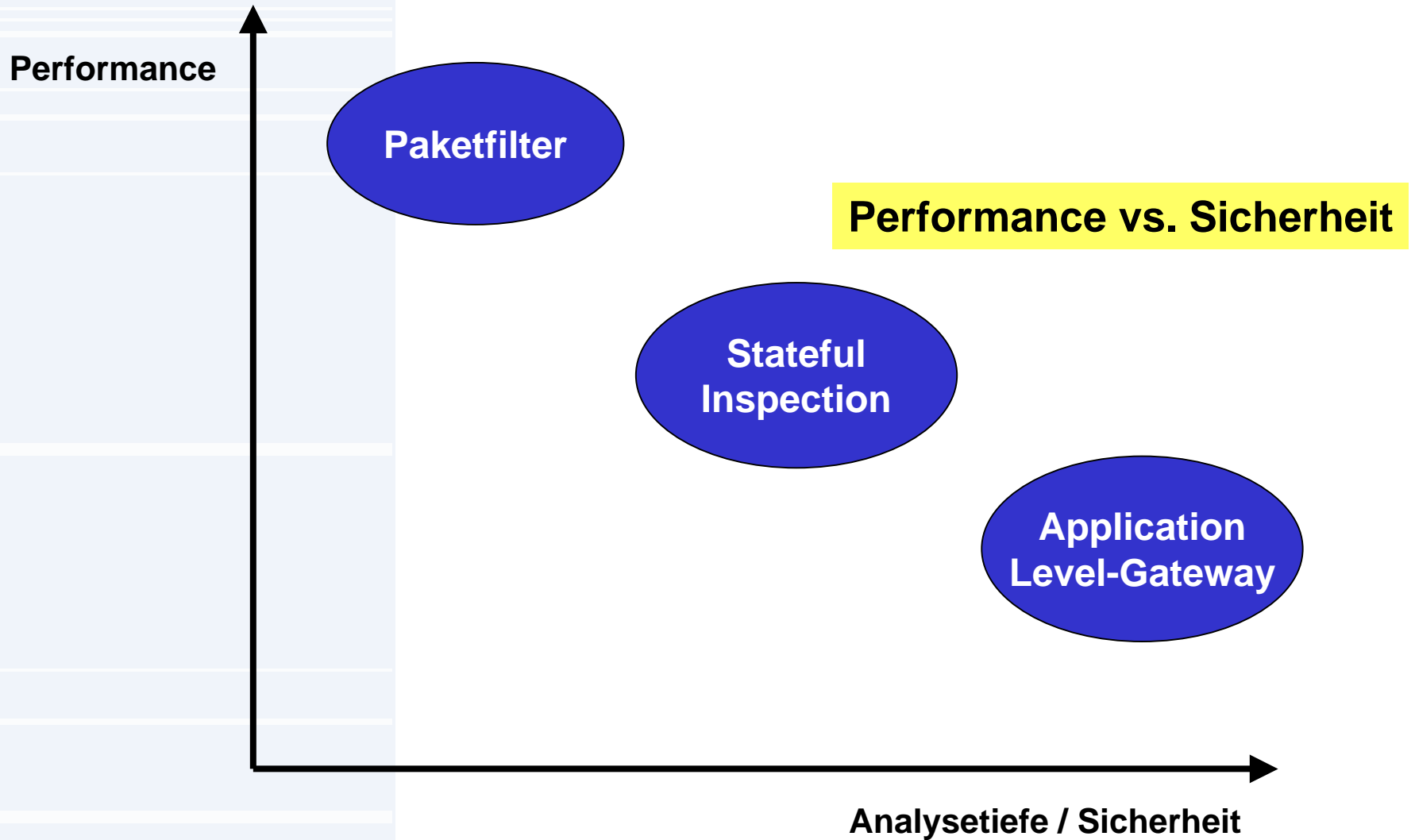
Source IP	Source Port	Dest. IP	Dest. Port	Protokoll	Timeout
192.168.7.131	10003	207.229.143.8	25	TCP	2845/3600
192.168.7.131	10002	207.229.143.8	24	TCP	2845/3600
192.168.7.131	10001	207.229.143.8	23	UDP	2845/3600

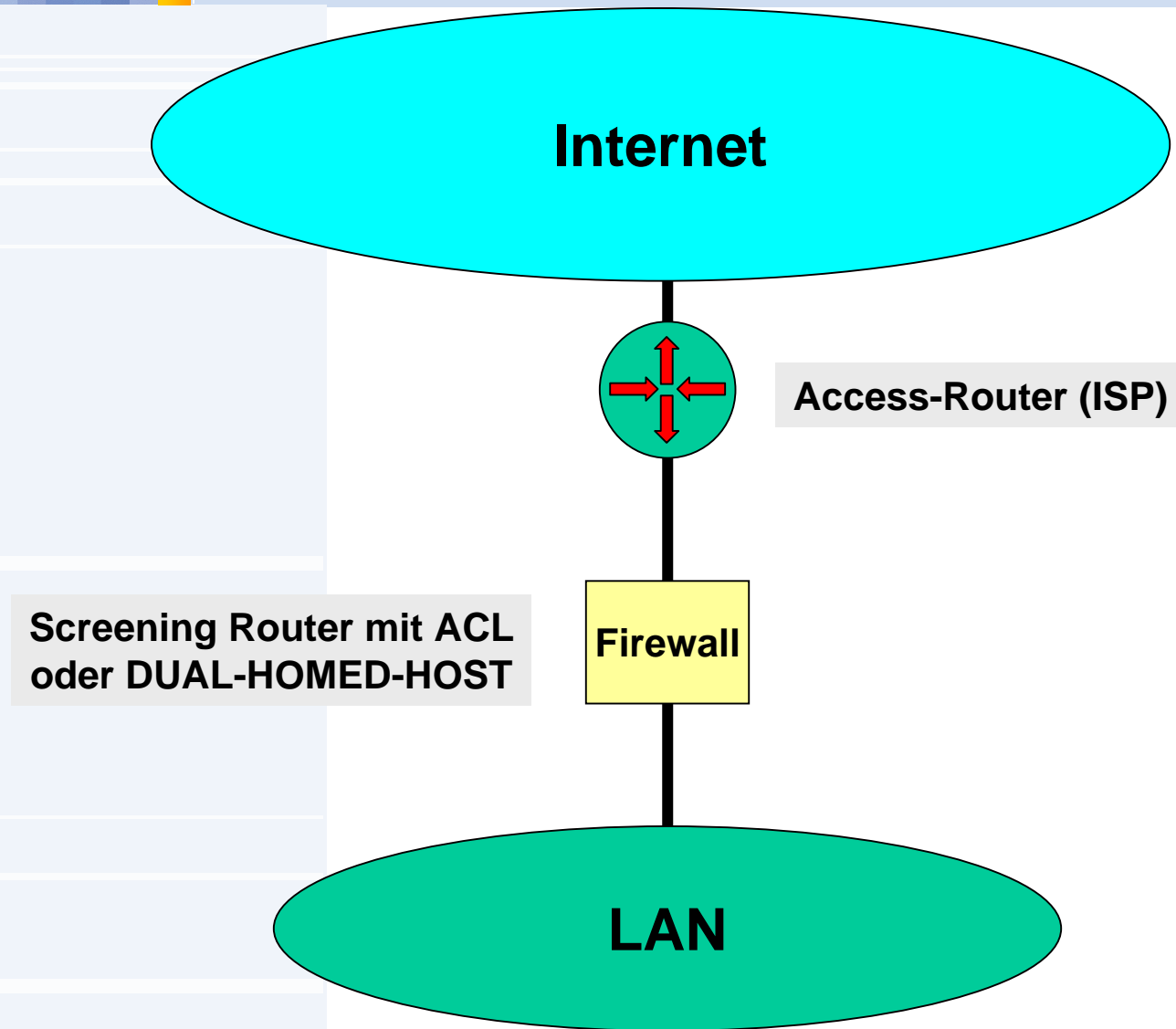
Application Level Gateways

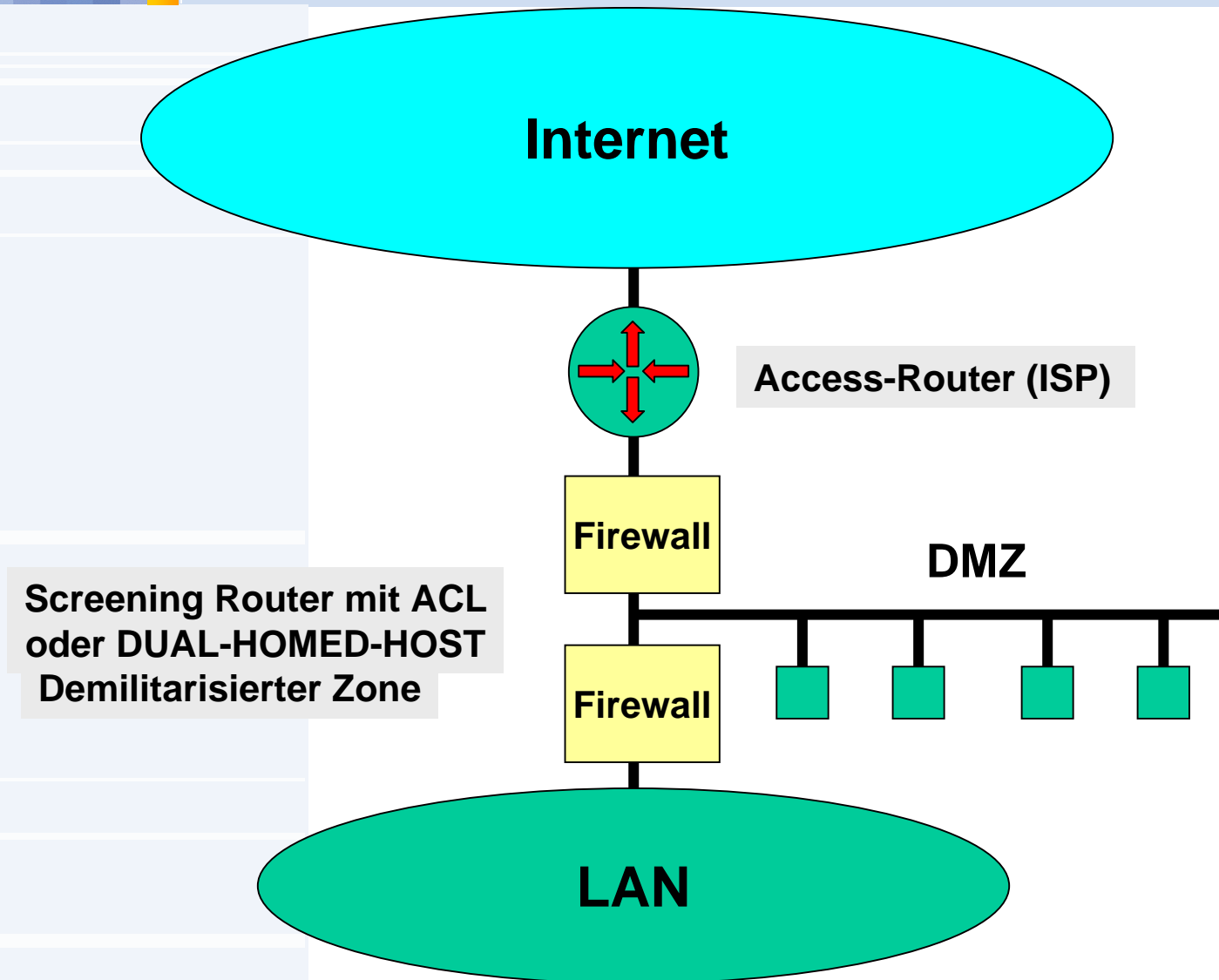


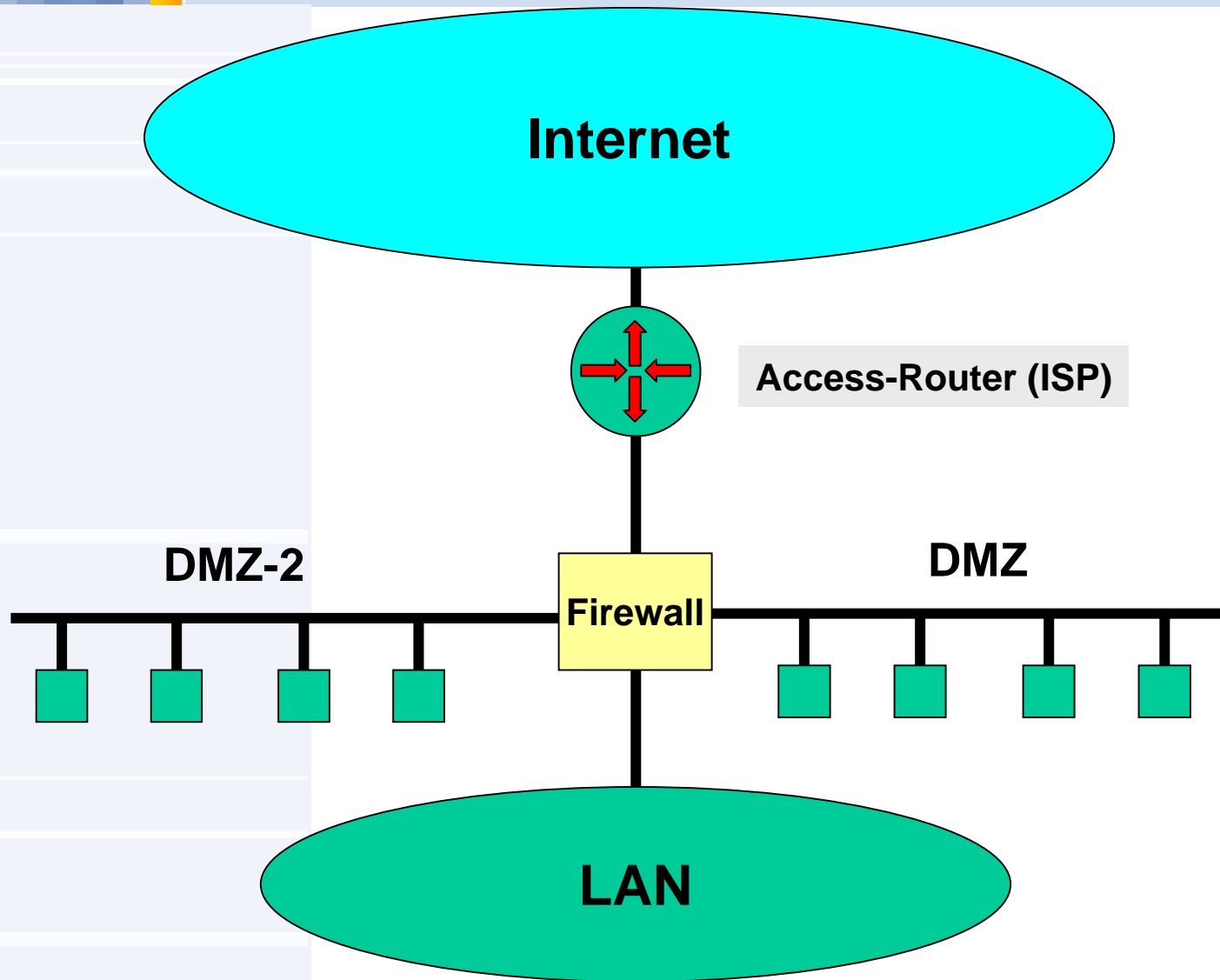


Firewall-Typen im Vergleich

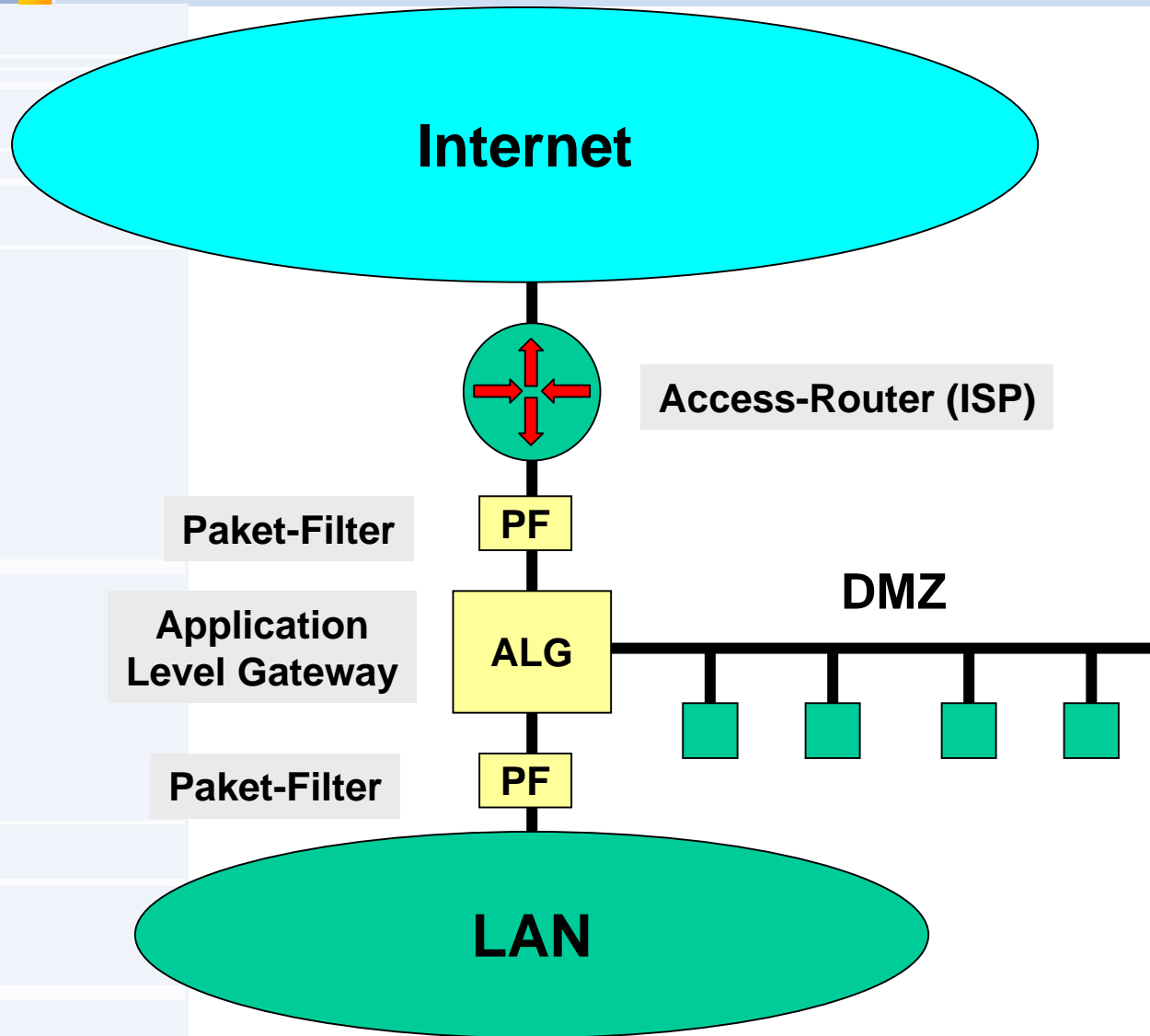


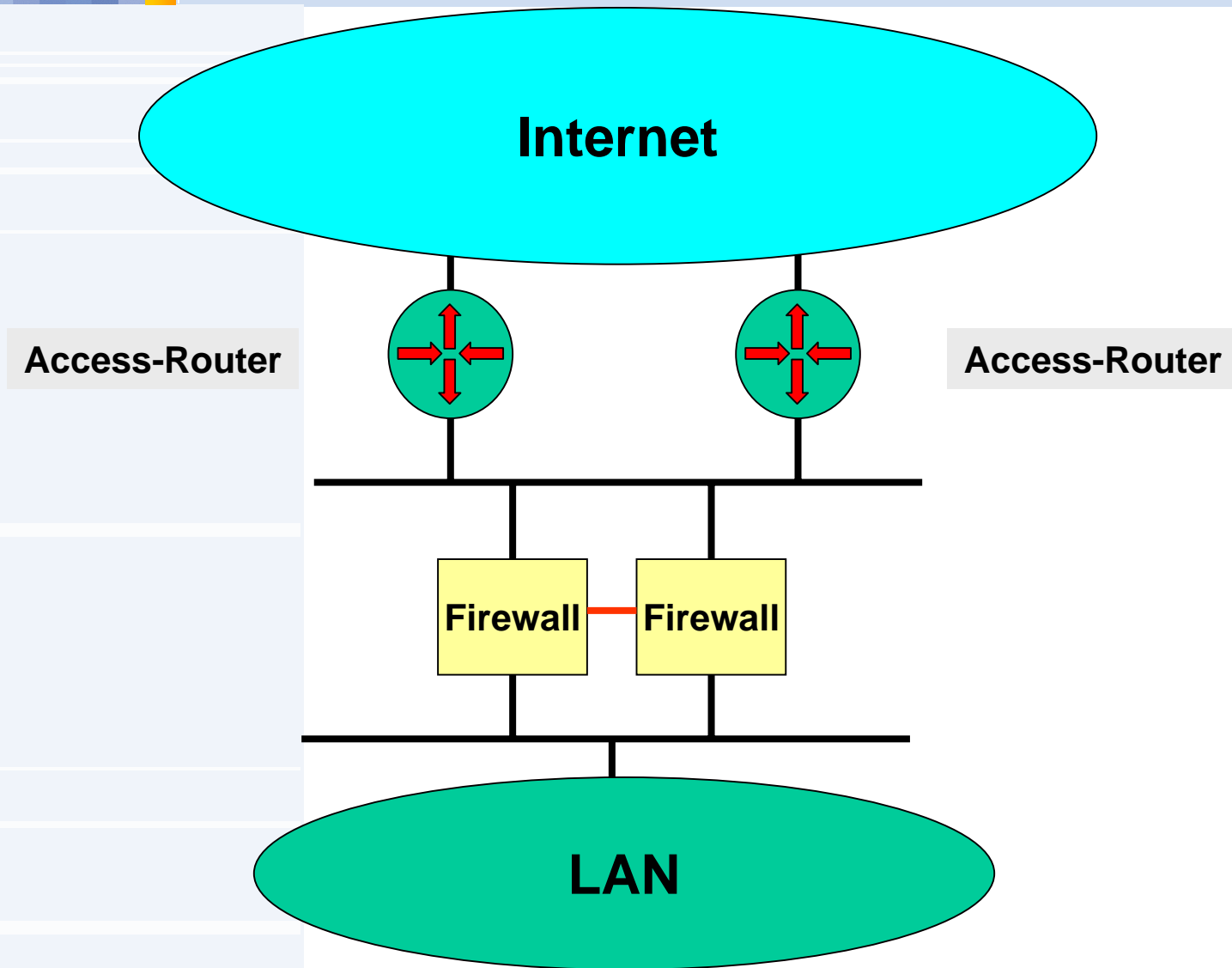






Dreistufige Firewall Topologie nach BSI



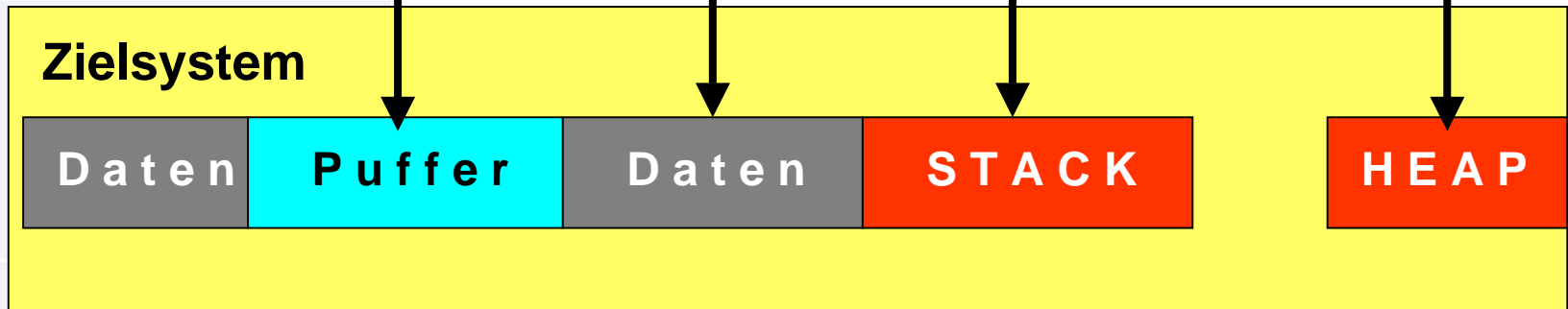


- **Buffer-Overflow**
- **SYN-Flooding**
- **Distributed Denial of Service (DDoS)**
- **Overlapping Fragment Attack**
- **Ping of Death**
- **Source Routing**
- **IP-Spoofing**
- **IP-Sequence-Number-Guessing**

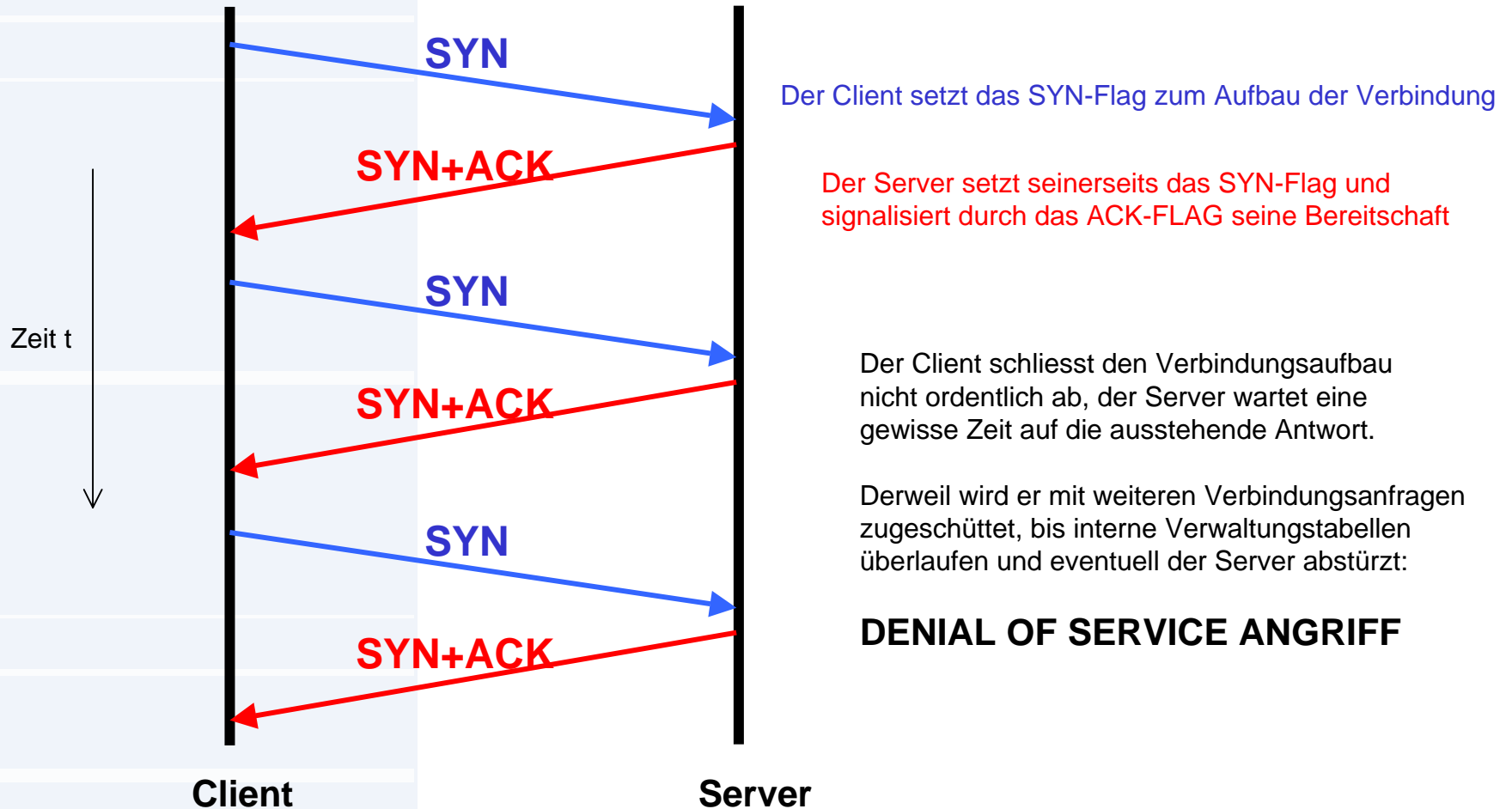
Angriff mittels Buffer-Overflow

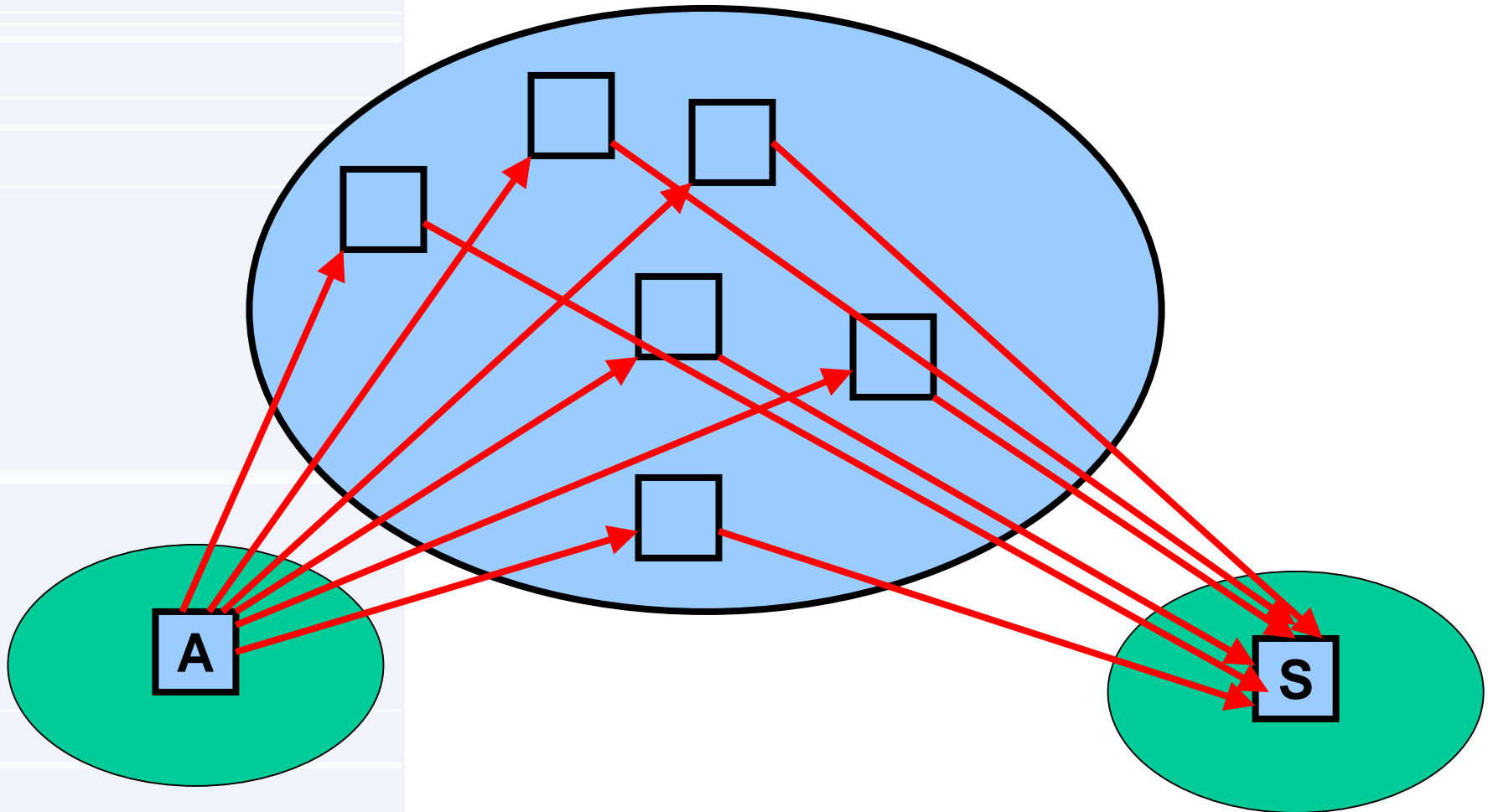
Das Datenpaket enthält Daten, die die vorgesehenen Puffer überschreiten. Die Datenlänge wird nicht sauber überprüft, das Zielsystem wird „abgeschossen“ oder übernommen!

URL: `http://ganz.lange.url/sprengt/den/im/Zielrechner/vorgesehenen/Pufferplatz`

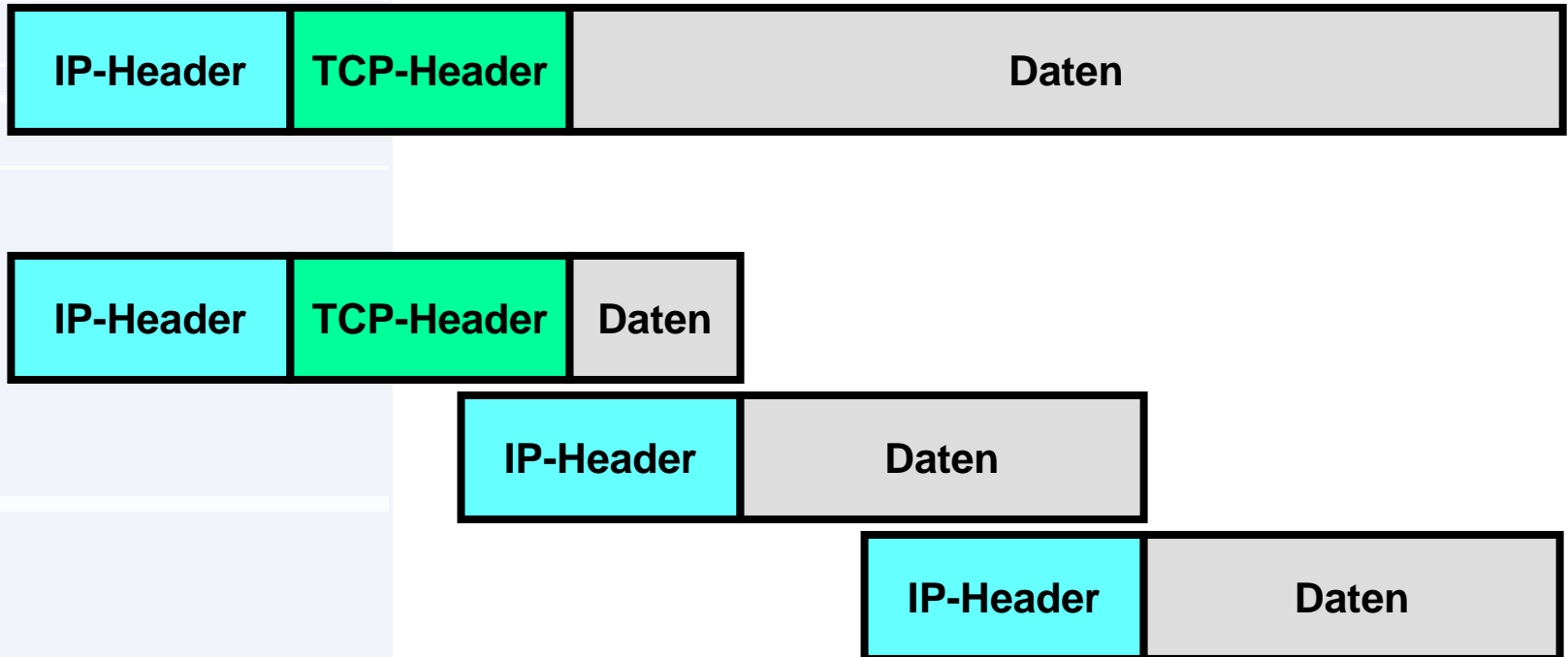


Zum Beispiel: <http://www.microsoft.com/technet/security/bulletin/MS01-023.asp>
„Unchecked Buffer in ISAPI Extension Could Enable Compromise of IIS 5.0 Server“



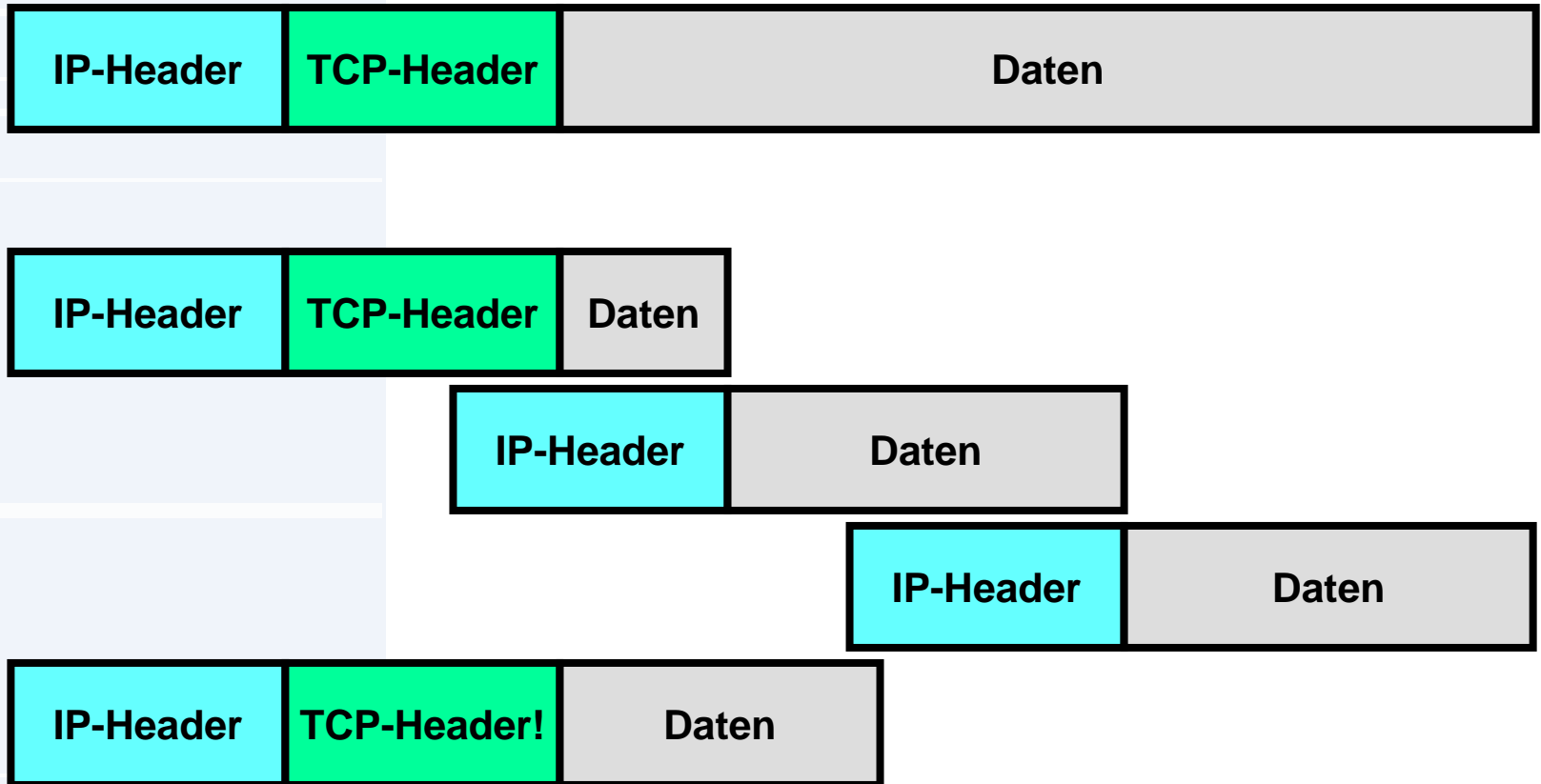


Der Angreifer erobert fremde Rechner, bereitet sie vor und lässt sie auf ein Signal hin gleichzeitig den Server angreifen!

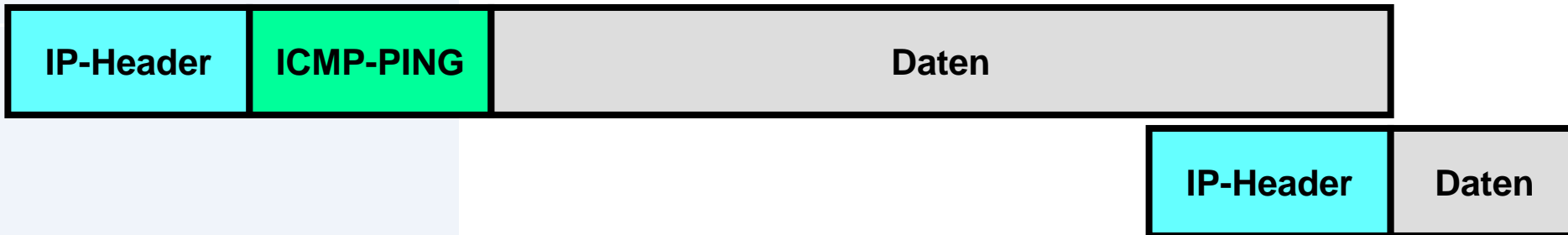


Das IP-Paket ist zu lang, um über die unterlagerten Schichten übertragen zu werden und wird daher in sogenannte Fragmente zerlegt

Overlapping Fragment Attack

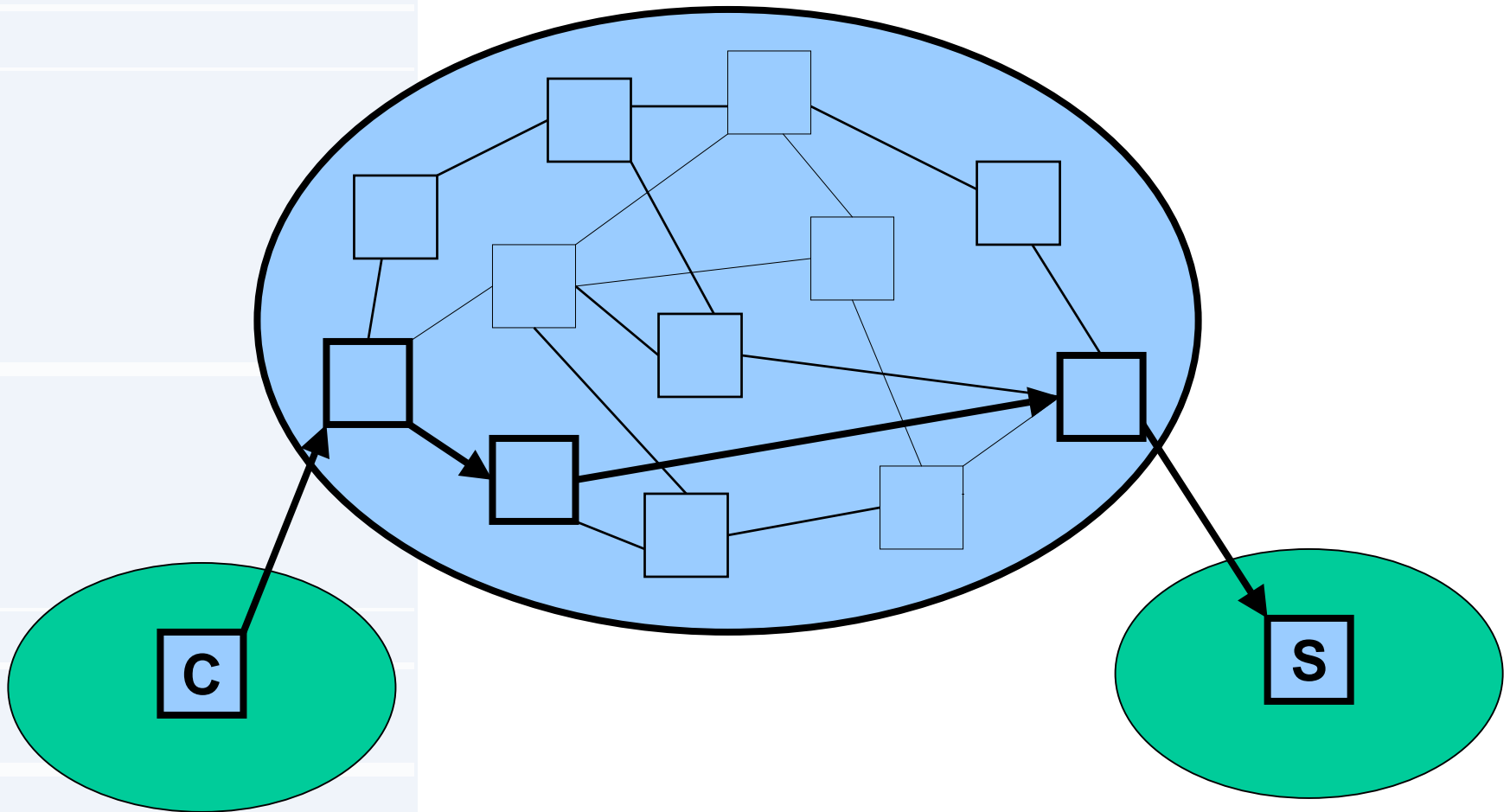


Die Fragmente überlappen sich, der TCP-Header wird überschrieben und kann nun auf einmal ganz andere Portnummern enthalten!

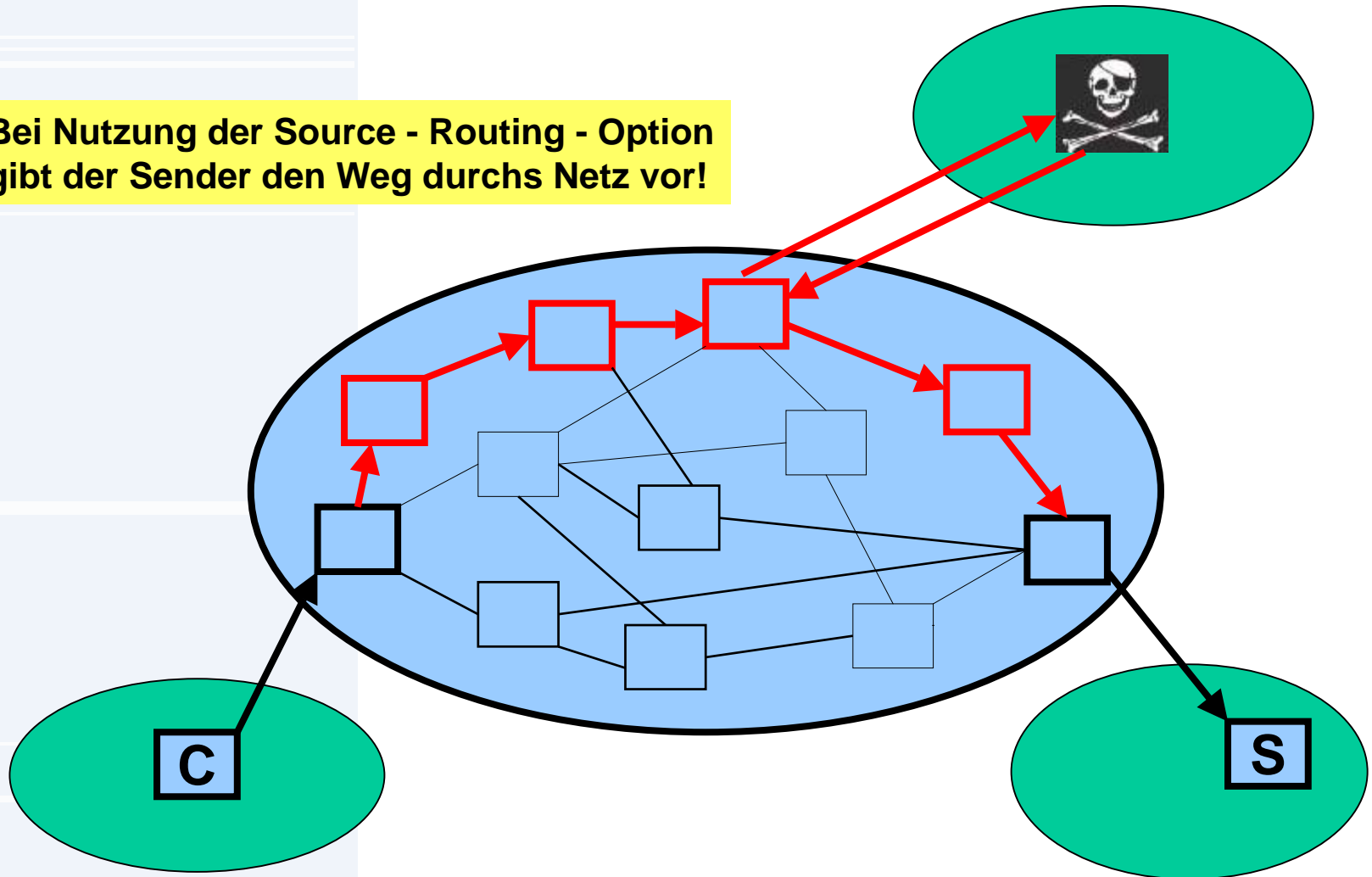


Die Fragmente ergeben zusammen ein IP-Paket, das länger als die erlaubte maximale Paketlänge ist! Fehlerhaft programmierte IP-Stacks stürzen ab!

Routing-Protokolle sorgen dafür, dass die Pakete ihren Weg finden

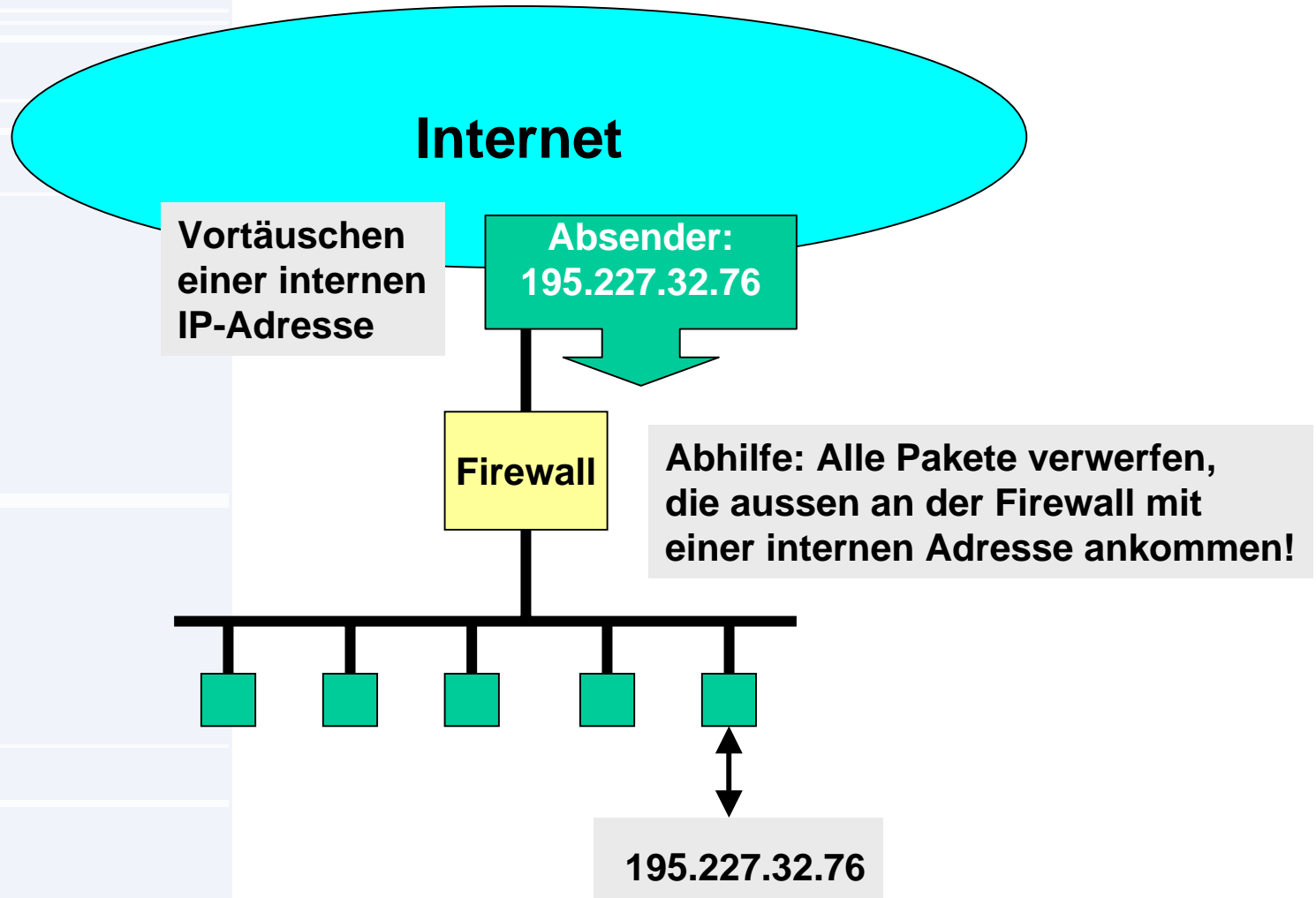


Bei Nutzung der Source - Routing - Option gibt der Sender den Weg durchs Netz vor!

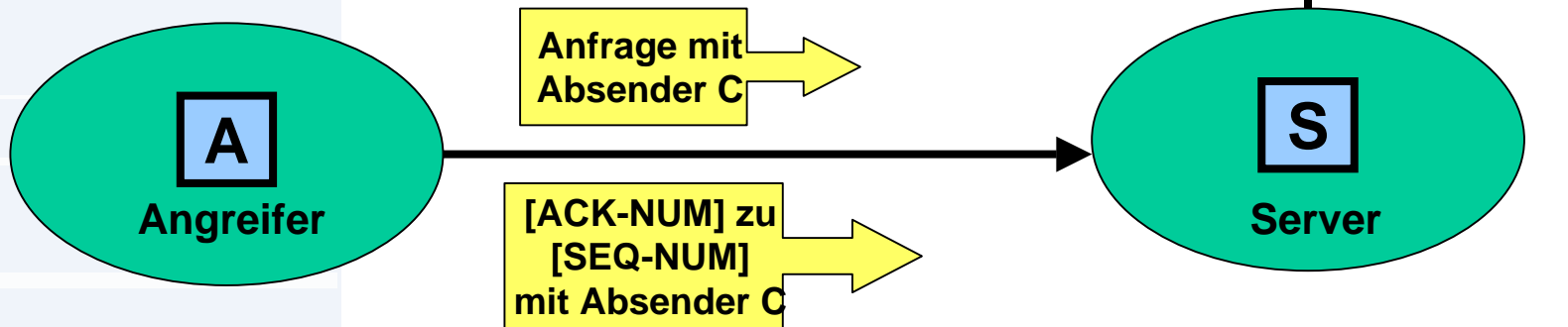
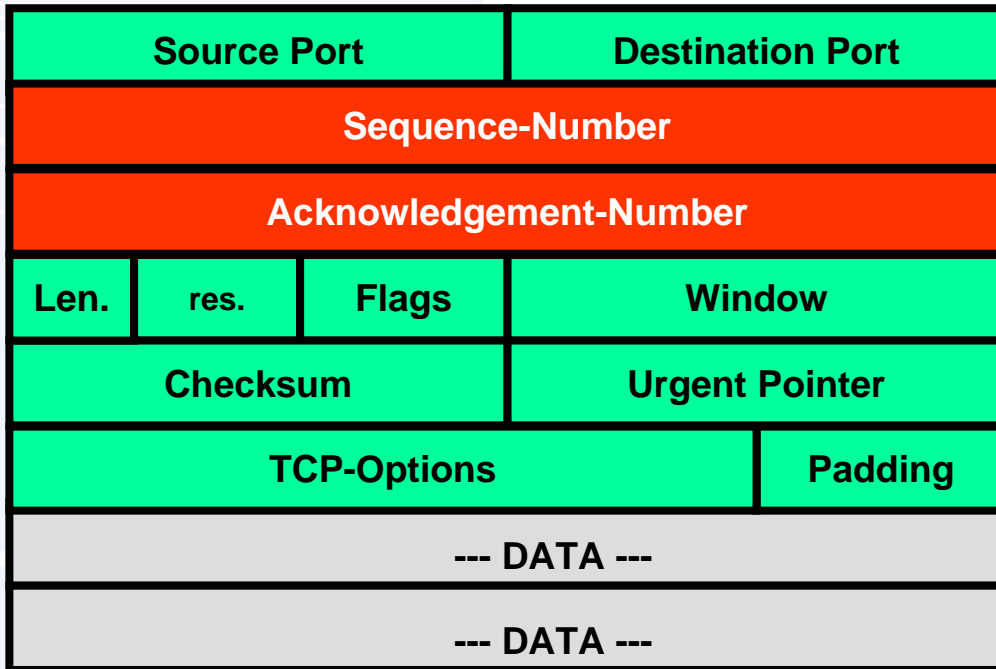


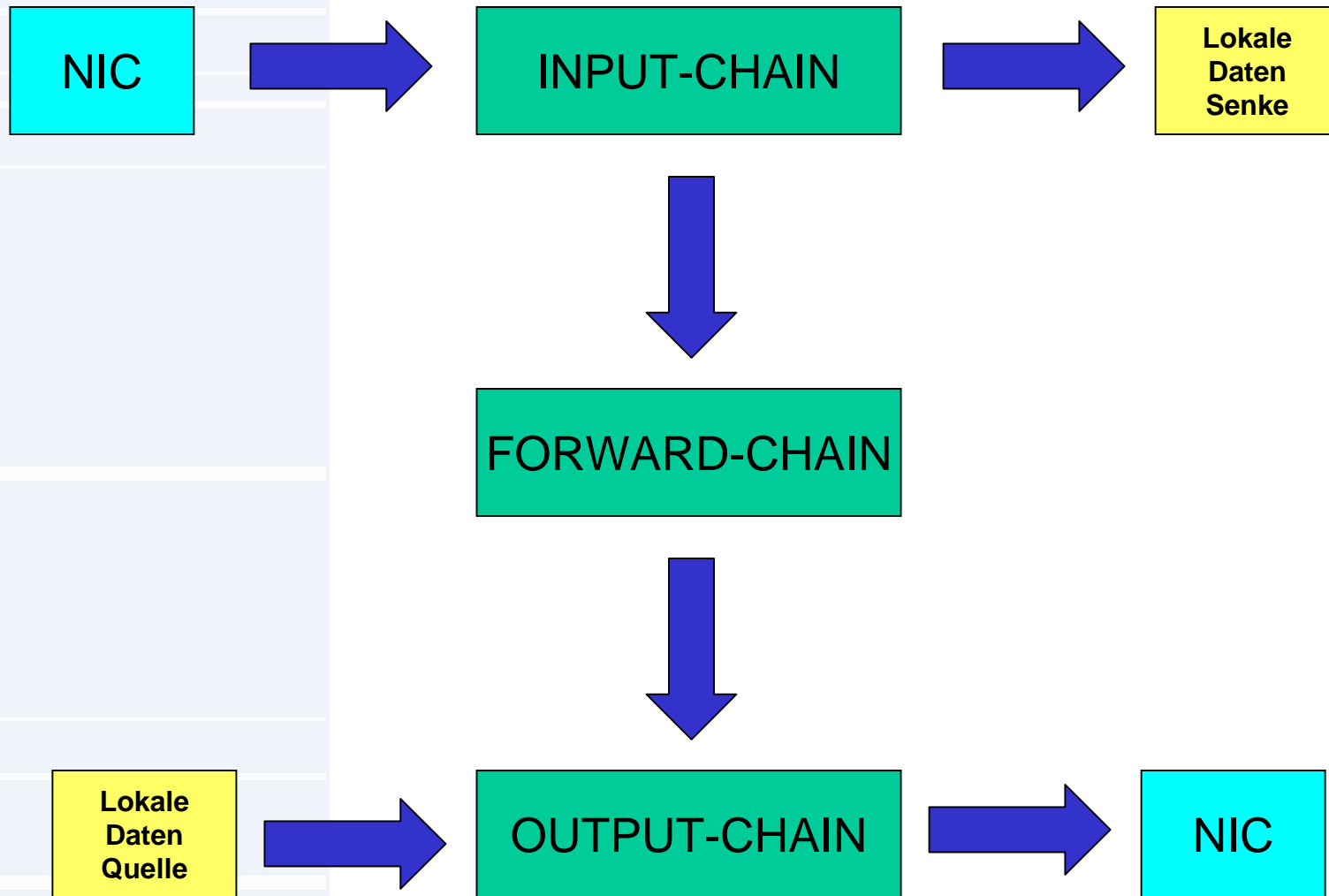
Abhilfe: Alle Pakete mit IP-Optionen verwerfen!

IP - Spoofing



TCP-Sequence-Number-Guessing



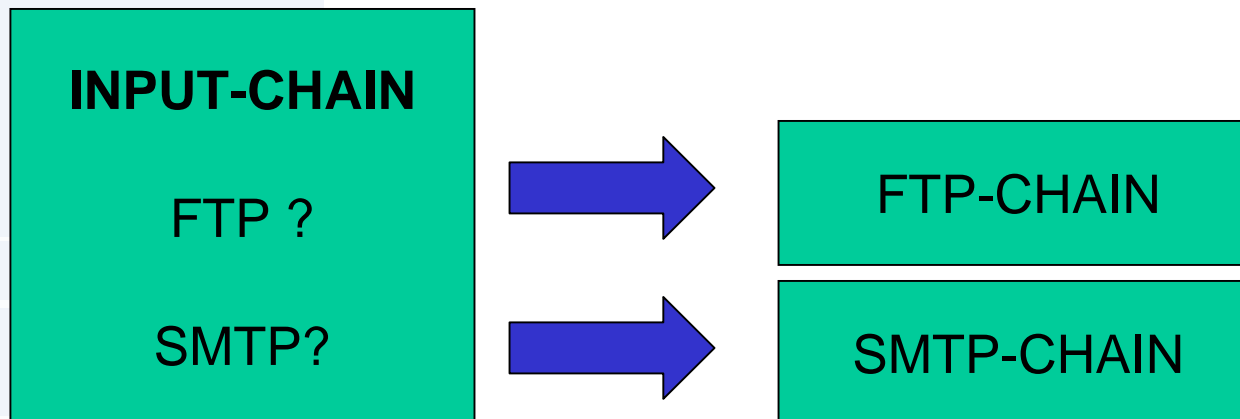


Filterbedingungen:

- Netzwerkinterface (NIC)
- IP-Absender
- IP-Empfänger
- IP-Protokoll (TCP, UDP, ...)
- TCP/UDP-Sende-Port
- TCP/UDP-Ziel-Port

Reaktionen:

- ACCEPT
- REJECT
- DENY
- MASQ
- verketteten zu neuer Chain
- Rückkehr zur vorherigen Chain



Löschen der Regeln in der input-, forward- und output-Chain:

```
ipchains -F
```

Löschen aller neu angelegten Chains

```
ipchains -X
```

Verbieten jeglichen Verkehrs:

```
ipchains -P input DENY
```

```
ipchains -P output DENY
```

```
ipchains -P forward DENY
```

Der gesamte Loopback-Verkehr wird gestattet:

```
ipchains -A input -i lo -j ACCEPT
```

```
ipchains -A output -i lo -j ACCEPT
```

Neue Chains anlegen

```
ipchains -N icmp-acc      # Chain für icmp-Verkehr
```

```
ipchains -N mail-out     # Chain für ausgehende Mails
```

```
ipchains -N mail-in      # Chain für eingehende Mails
```

ICMP-Pakete, die die Firewall „überqueren“, werden grundsätzlich maskiert:

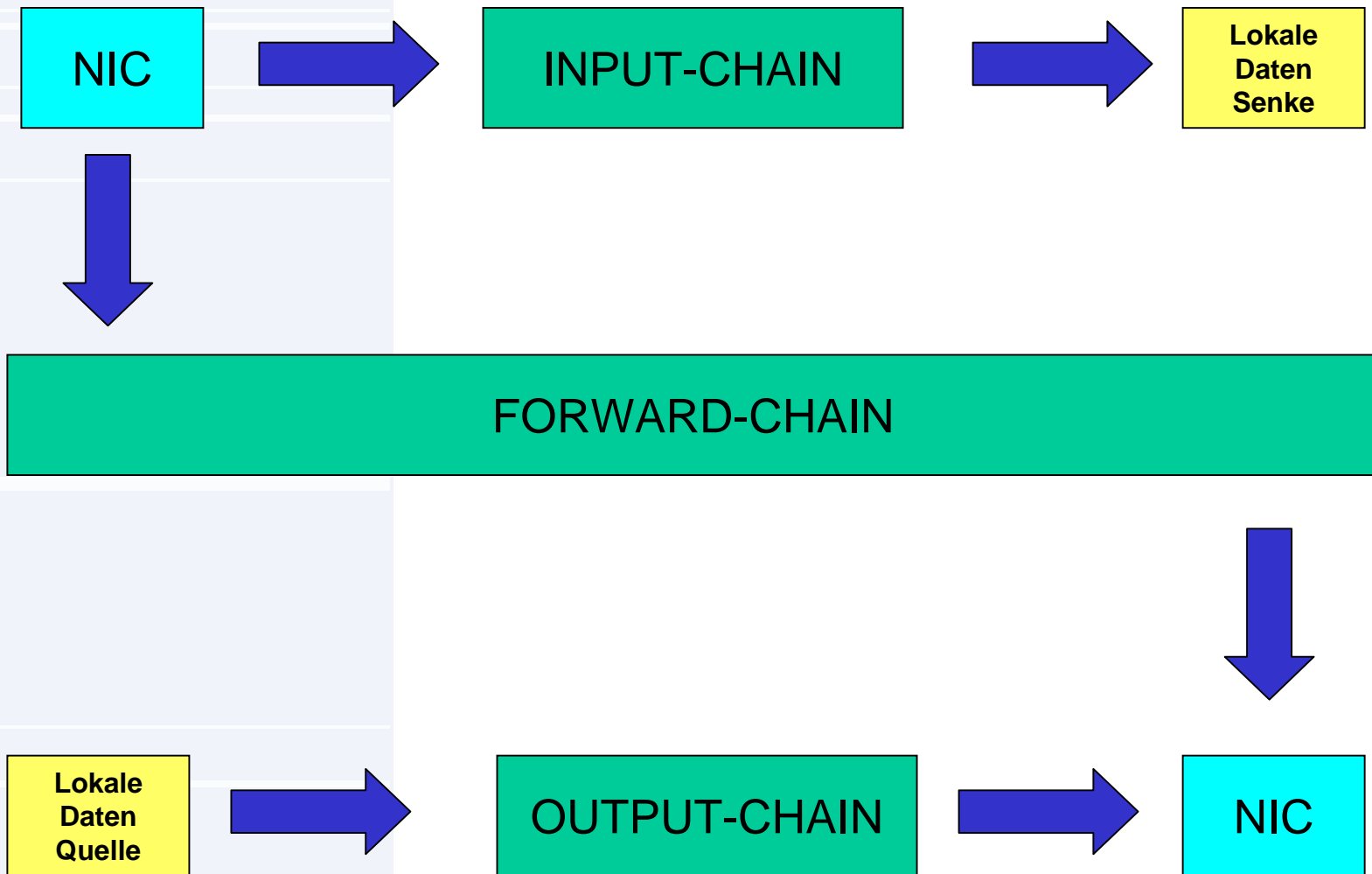
```
ipchains -A input -p icmp -j icmp-acc  
ipchains -A forward -p icmp -j MASQ  
ipchains -A output -p icmp -j icmp-acc
```

folgende ICMP-Pakete (z.B. Ping) werden akzeptiert:

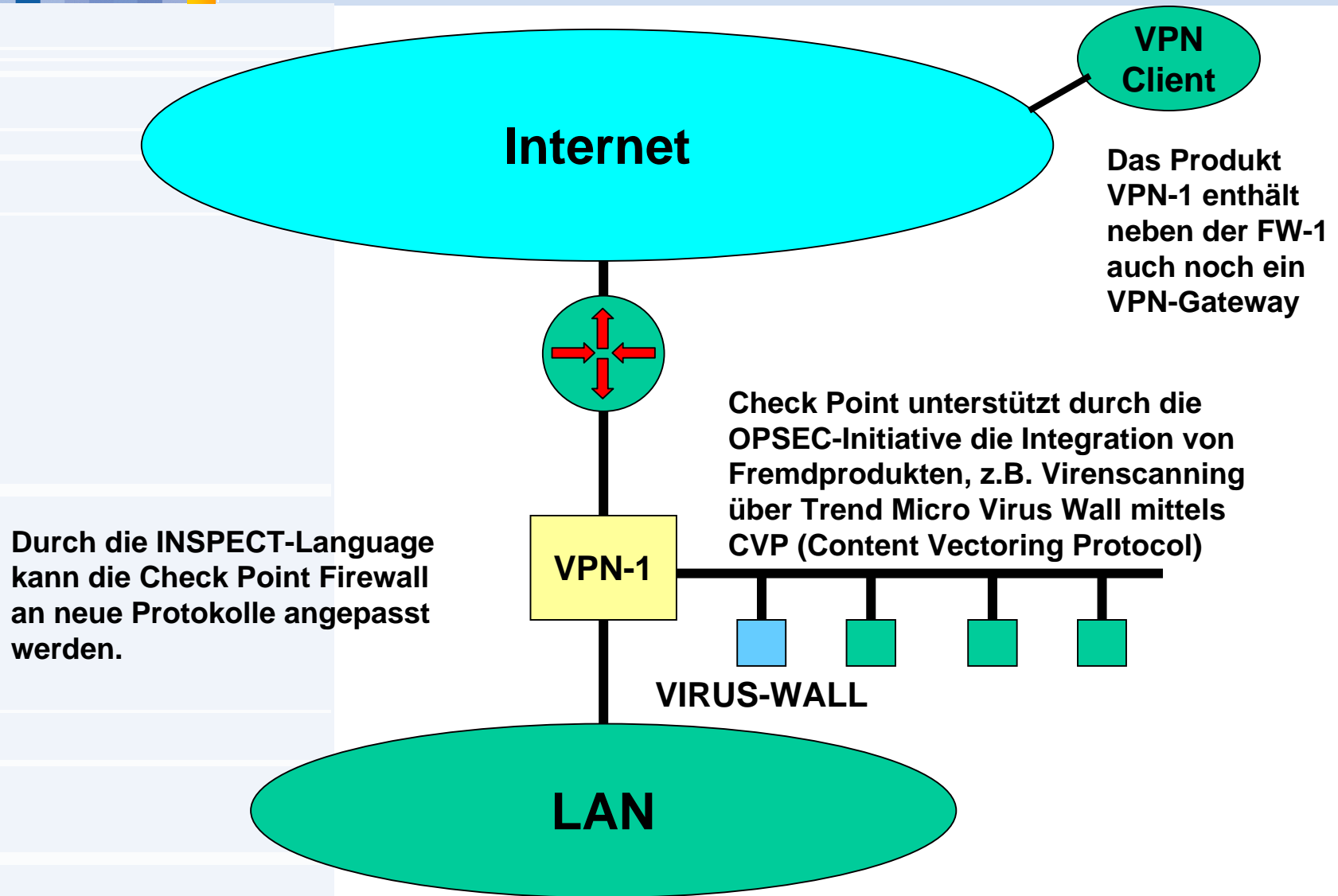
```
ipchains -A icmp-acc -p icmp --icmp-type echo-reply -j ACCEPT  
ipchains -A icmp-acc -p icmp --icmp-type echo-request -j ACCEPT  
ipchains -A icmp-acc -p icmp --icmp-type destination-unreachable -j ACCEPT  
ipchains -A icmp-acc -p icmp --icmp-type source-quench -j ACCEPT  
ipchains -A icmp-acc -p icmp --icmp-type time-exceeded -j ACCEPT  
ipchains -A icmp-acc -p icmp --icmp-type parameter-problem -j ACCEPT
```

ausgehende Mail

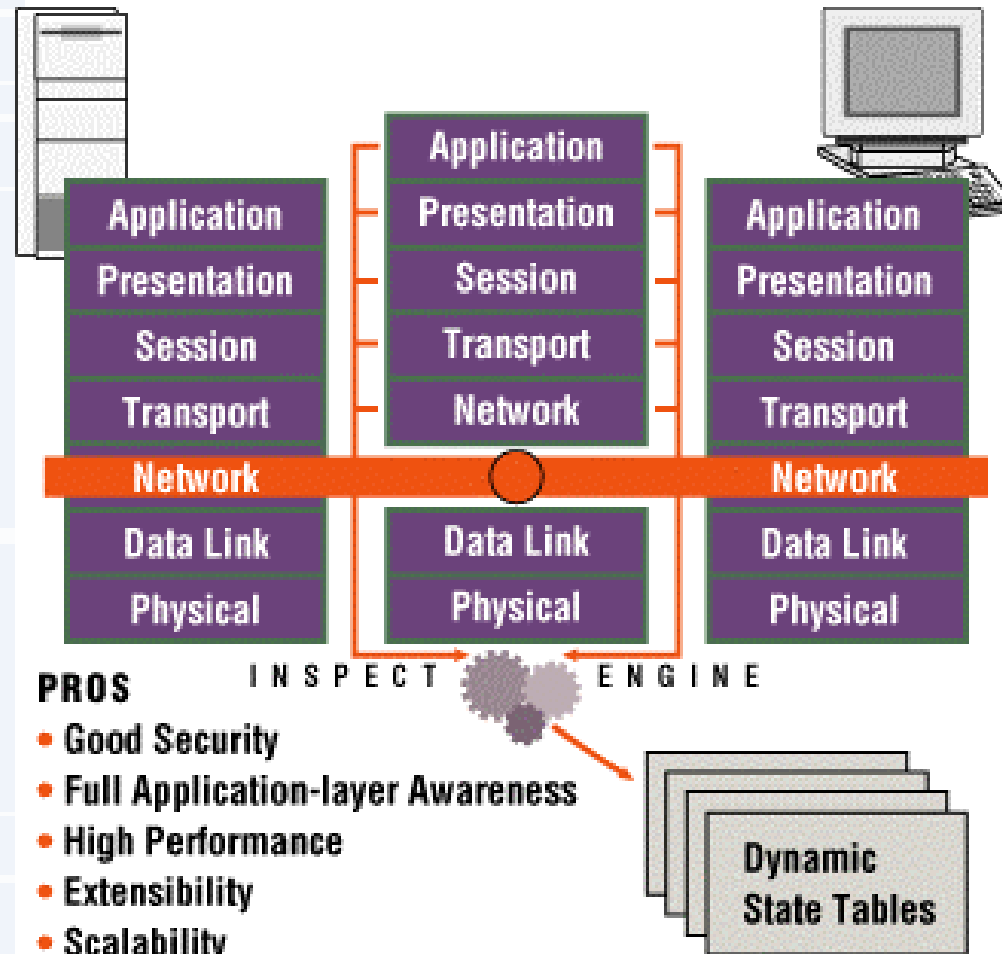
```
ipchains -A input -p tcp --dport smtp -i $DEV_DMZ -j mail-out  
ipchains -A input -p tcp --sport smtp -i $DEV_INET -j mail-out  
ipchains -A forward -p tcp --dport smtp -i $DEV_INET -j mail-out  
ipchains -A output -p tcp --dport smtp -i $DEV_INET -j mail-out  
ipchains -A output -p tcp --sport smtp -i $DEV_DMZ -j mail-out  
ipchains -A mail-out -p tcp -s $MTA_SERVER/32 1024: -d $GLOBAL/0 smtp -i $DEV_DMZ -j ACCEPT  
ipchains -A mail-out -p tcp -s $MTA_SERVER/32 1024: -d $GLOBAL/0 smtp -i $DEV_INET -j MASQ
```



Firewalling mit Check Point VPN-1



Stateful Inspection



PROS

- Good Security
- Full Application-layer Awareness
- High Performance
- Extensibility
- Scalability
- Transparency



Check Point Firewall-1 Policy Editor

*local - Check Point Policy Editor

File Edit View Manage Policy Window Help

Security Policy - 2 | Address Translation - 2 | Bandwidth Policy - VPN | Compression Policy - VPN

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
	Any	Any	Any	reject		Gateways	Any	
2	Known_hackers	Any	Any	drop	Alert	Gateways Routers	Any	
3	Email_Server	Any	smtp	accept		Gateways	Any	
4	Any	Email_Server	smtp	accept	Long	Gateways	Any	
5	Any	Public_FTP_Server	ftp	accept	Short	Gateways	Any	
6	Sales@Any	Web_Servers_Group	ftp http	accept	Long	Gateways	Any	
7	Partner_Net	Local_Gateway	IPSEC	Encrypt	Short	Gateways	Any	
8	Local_Net	Any	http->URL_Filtering	accept		Gateways	Any	
9	Any	Any	Any	drop		Gateways	Any	

For Help, press F1

*local NUM

Check Point Firewall-1 NAT

*local - Check Point Policy Editor

File Edit View Manage Policy Window Help

Security Policy - 2 | Address Translation - 2 | Bandwidth Policy - VPN | Compression Policy - VPN

No.	Original Packet			Translated Packet			Install On	Comr
	Source	Destination	Service	Source	Destination	Service		
1	Local_Net	Local_Net	Any	Original	Original	Original	All	Automatic rule (see the
2	Local_Net	Any	Any	Local_Net (Hiding Address)	Original	Original	All	Automatic rule (see the
3	Remote_Net	Remote_Net	Any	Original	Original	Original	All	Automatic rule (see the
4	Remote_Net	Any	Any	Remote_Net (Hiding Address)	Original	Original	All	Automatic rule (see the

For Help, press F1

*local NUM

Check Point Firewall-1 Log Viewer

The screenshot shows the 'fw.log - Check Point Log Viewer' application window. It features a menu bar (File, Edit, View, Select, Window, Help), a toolbar with various icons, and a dropdown menu set to 'Log'. The main area contains a table with the following data:

No.	Date	Time	In..	Origin	Type	Action	Service	Source	Destination	Proto.
0	9Jun95	10:38:55		199.203.73.197	control	ctl				
1	9Jun95	10:38:56		199.203.73.197	control	ctl				
2	9Jun95	10:39:01		199.203.73.197	control	ctl				
3	9Jun95	10:39:09		199.203.73.197	control	ctl				
4	9Jun95	10:42:54		199.203.73.240	log	accept	257	199.203.73.240	199.203.73.197	tcp
5	9Jun95	10:42:54		199.203.73.240	log	accept	257	199.203.73.240	199.203.73.241	tcp
6	9Jun95	10:42:54		199.203.73.240	control	ctl				
7	9Jun95	10:45:09		192.114.50.150	log	accept	mail	192.48.96.5	192.114.50.150	tcp
8	9Jun95	10:45:09		192.114.50.150	control	ctl				
9	9Jun95	10:50:32		199.203.73.240	log	accept	mail	192.114.50.150	199.203.73.241	tcp

At the bottom of the window, there is a status bar with the text 'For Help, press F1' on the left and 'logview.fw *local NUM' on the right.