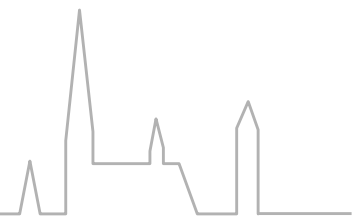


# Theorie und Praxis der IT Sicherheit

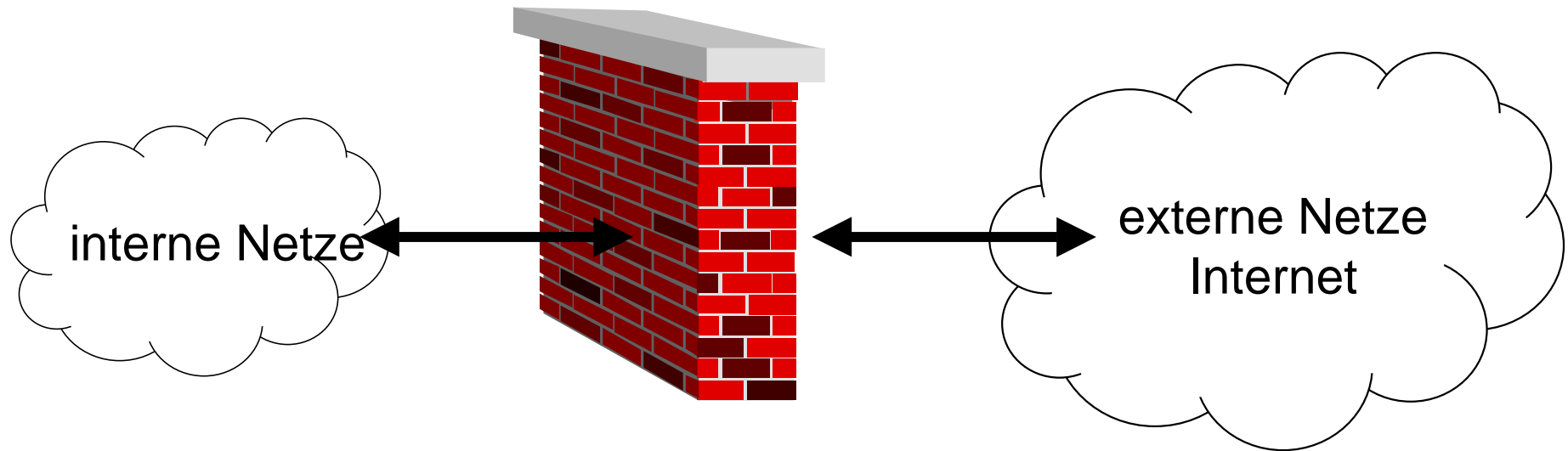
## Firewalls und Intrusion Detection Systeme



# Firewall - Was ist das?

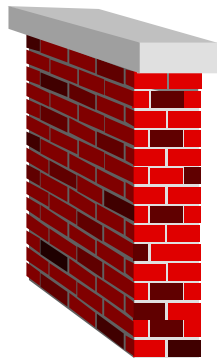


Schutz vor den Gefahren des Internet

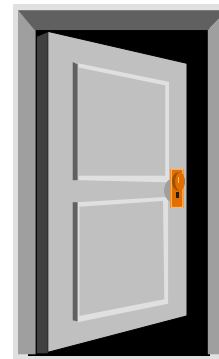


Datenaustausch erforderlich:

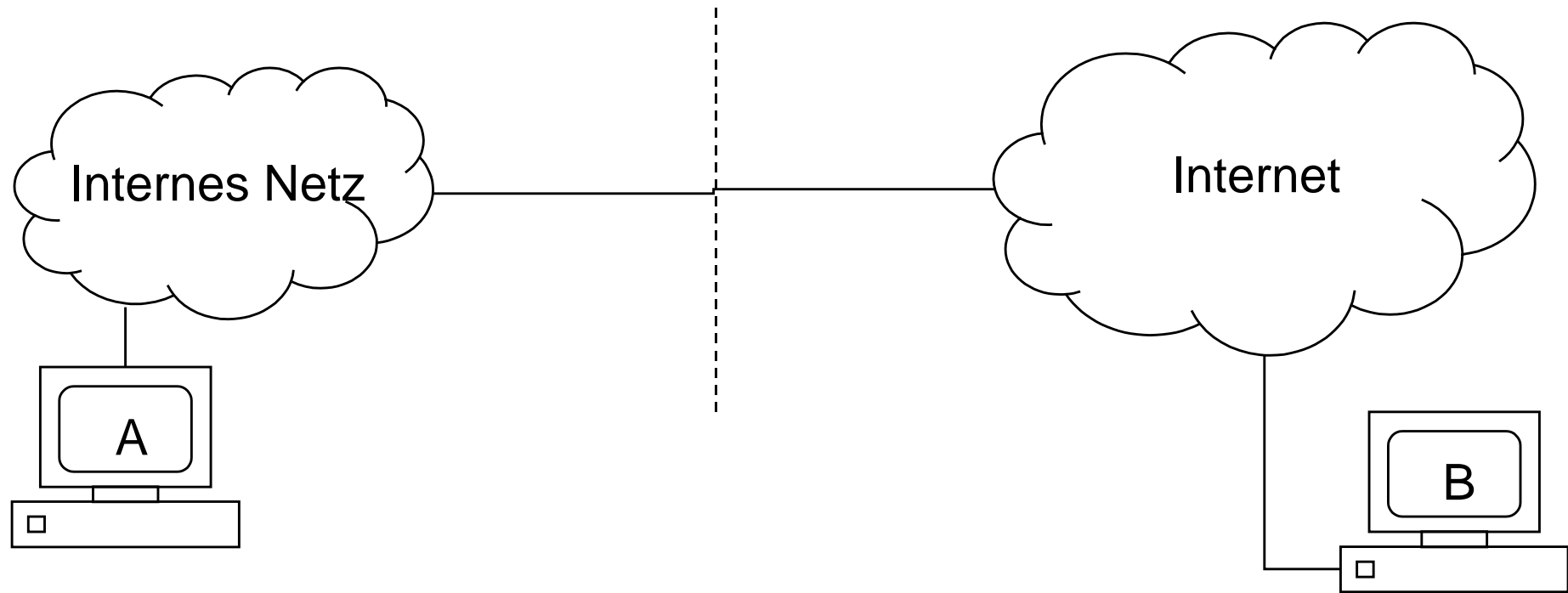
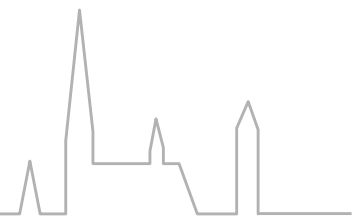
Ersatz von



durch

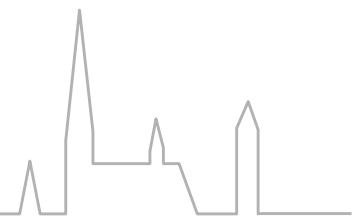


# Firewall - Wieso?

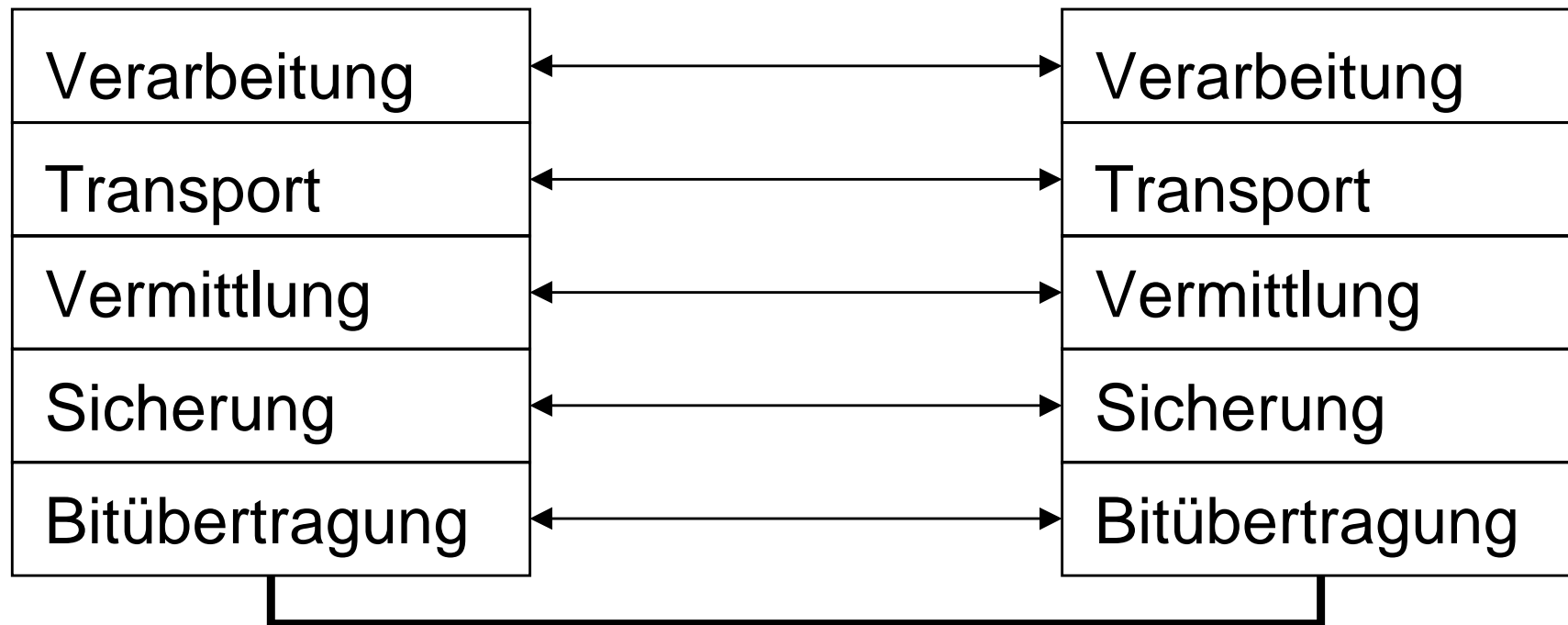


Multiplexgewinn des Schutzes  
Single Point of Administration  
Trennung: Innen - Aussen

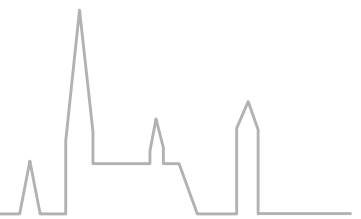
# Firewall - Schichtenmodell



Nach Tanenbaum



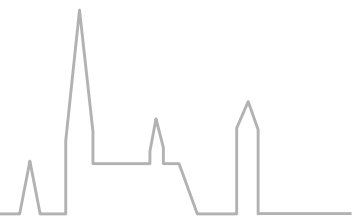
# Firewall - Internet Protokolle



Dienste:

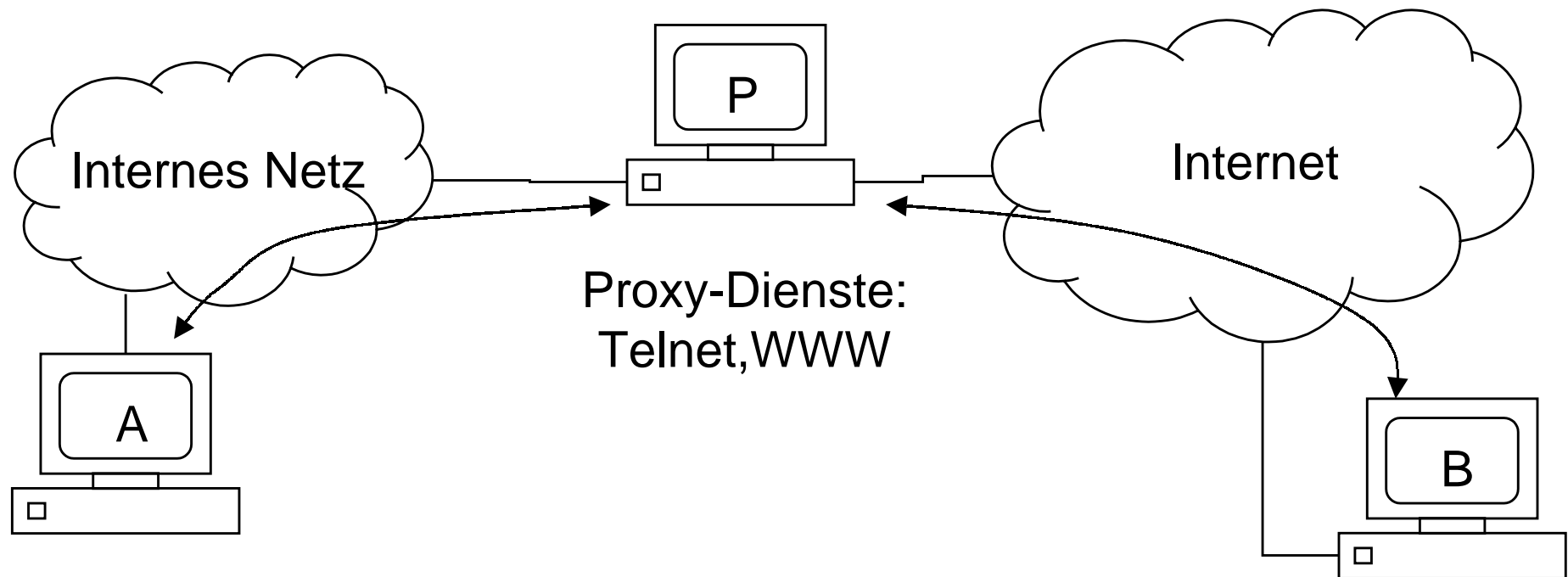
FTP	SMTP	Telnet	HTTP	DNS	RPC	NFS
TCP				UDP		
IP				ICMP	ARP	
Ethernet, Token Ring, FDDI, PPP, ATM						
Twisted Pair, LWL, Koaxialkabel, Funk, Laser						



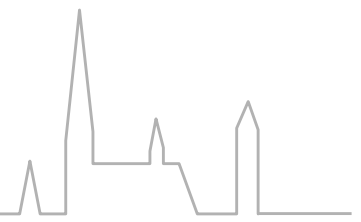


## Proxy: Stellvertreter

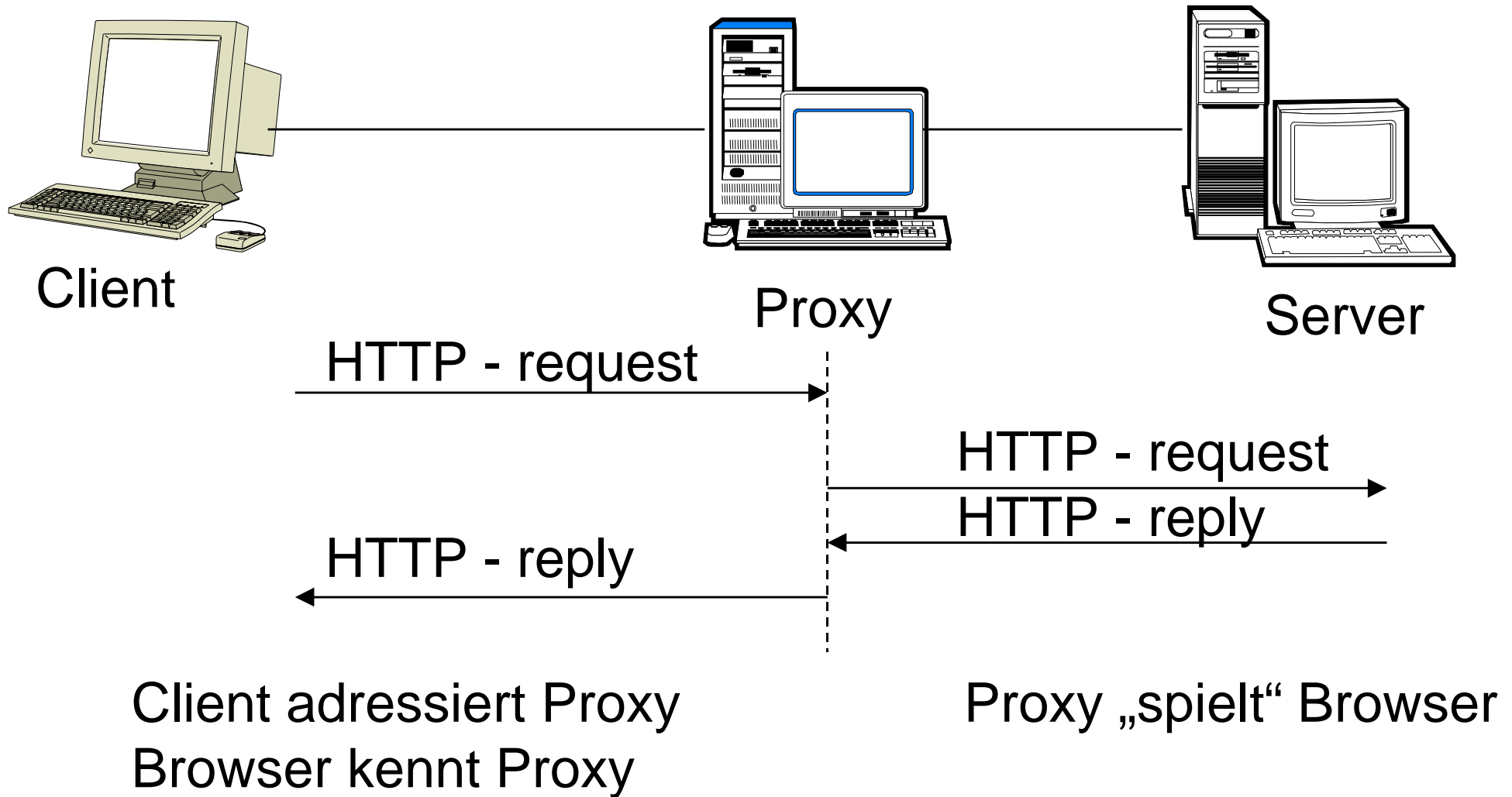
- Anwendungs-Proxy
- transparenter Proxy
- generischer Proxy (Socks)



# Firewall - Anwendungs-Proxies

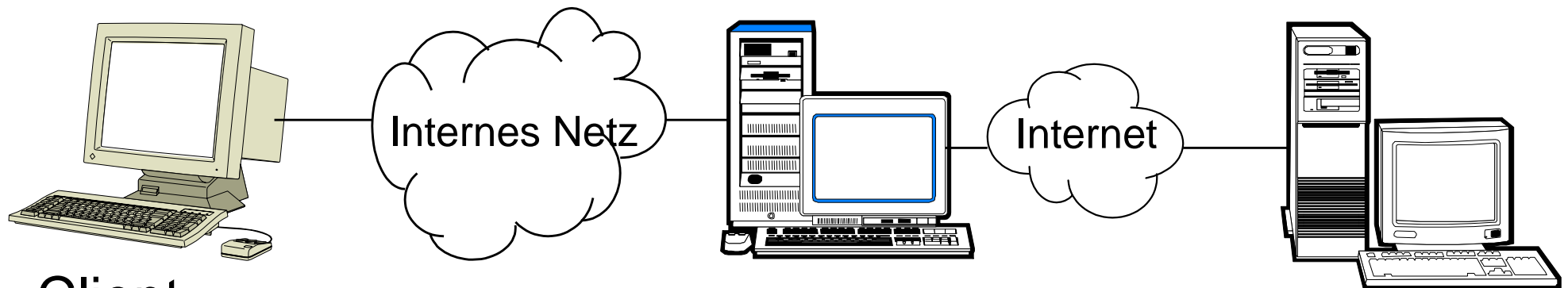


## Beispiel: HTTP-Proxy



# Firewall - transparente Proxies

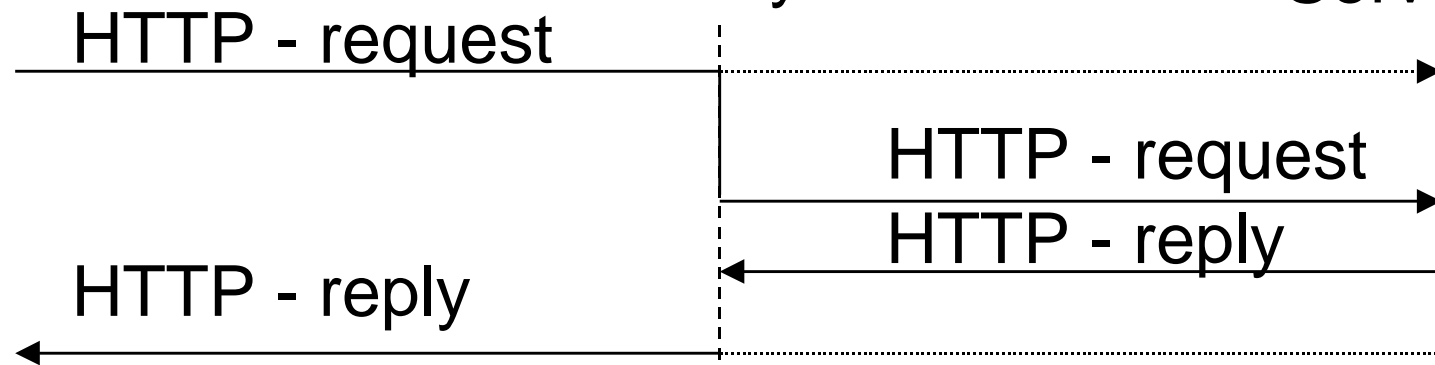
## Beispiel: HTTP-Proxy



Client

Proxy

Server

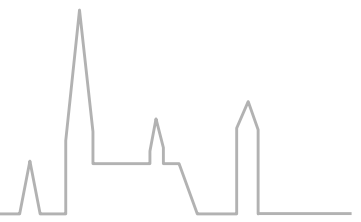


Client adressiert Server  
Browser kennt Proxy nicht

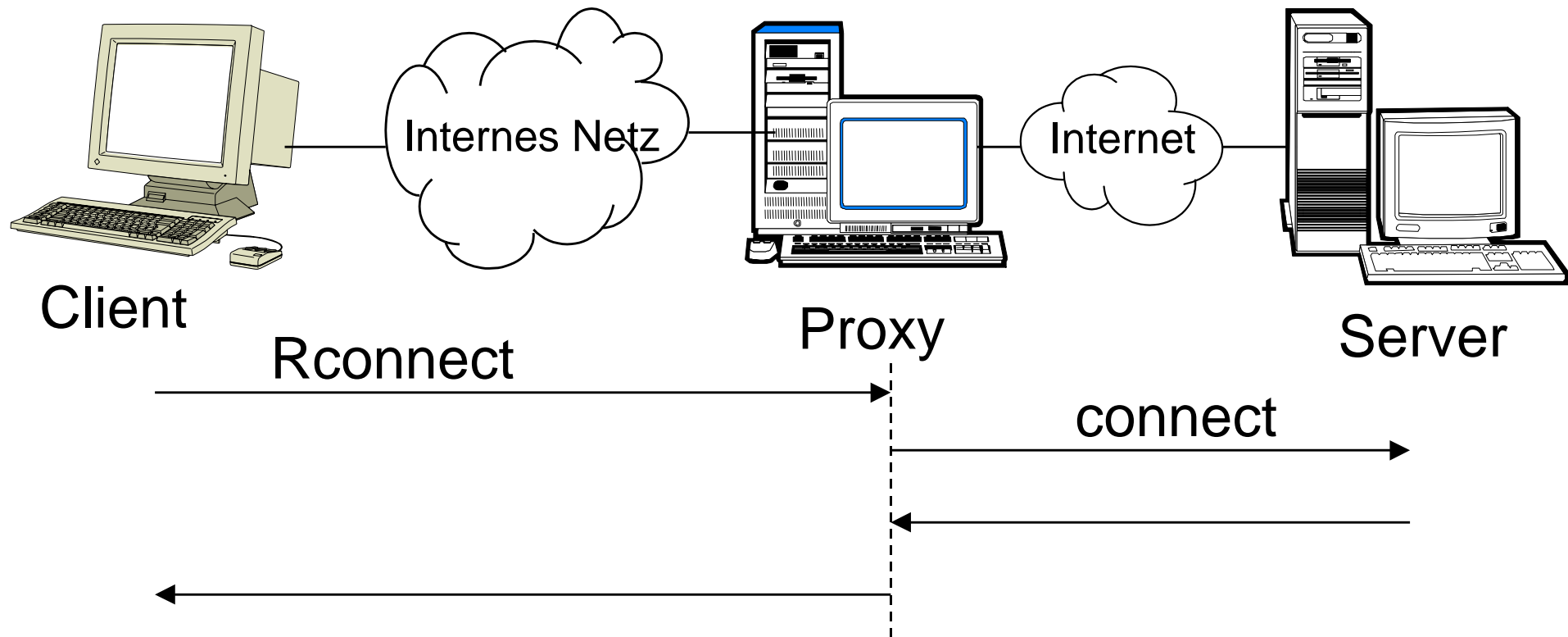
Proxy fängt Verkehr ab  
Proxy „spielt“ Browser



# Firewalls - SOCKS Proxy



## Generischer Proxy Transport-Ebene

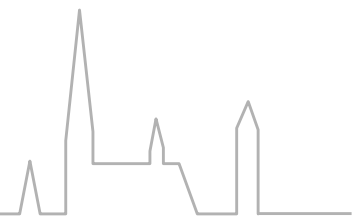


Socksified TCP-Stack  
Anwendung kennt Proxy nicht

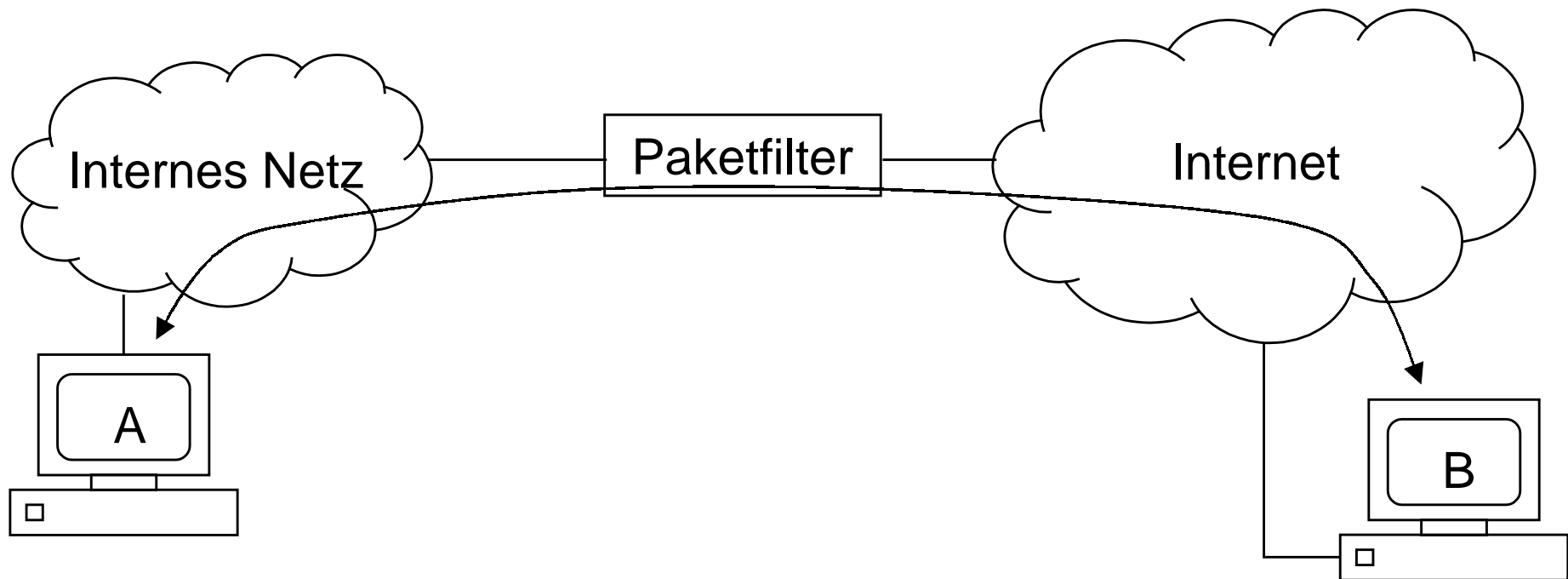
Proxy kennt Socks Protokoll  
Proxy „spielt“ TCP-Client



# Firewalls - Paketfilter



Regeln auf IP-Ebene  
meist im Router

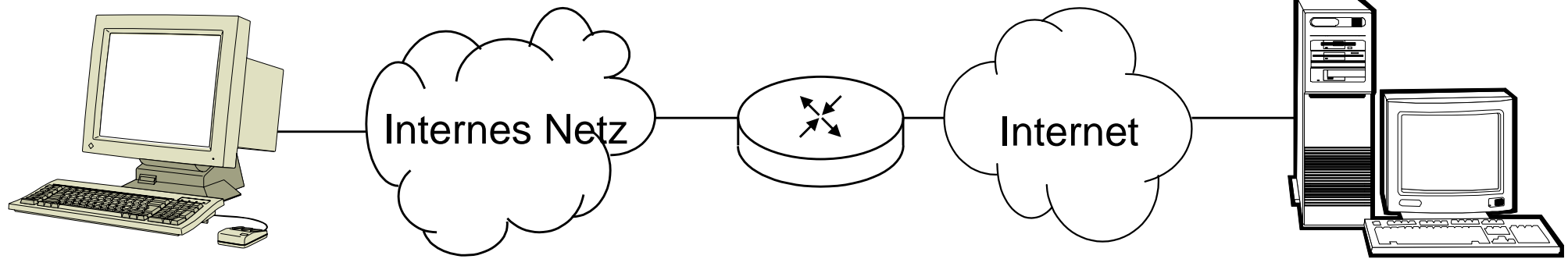


Pakete werden **nur** zwischen A nach B zugelassen



# Firewalls - Paketfilter

## Beispiel: telnet



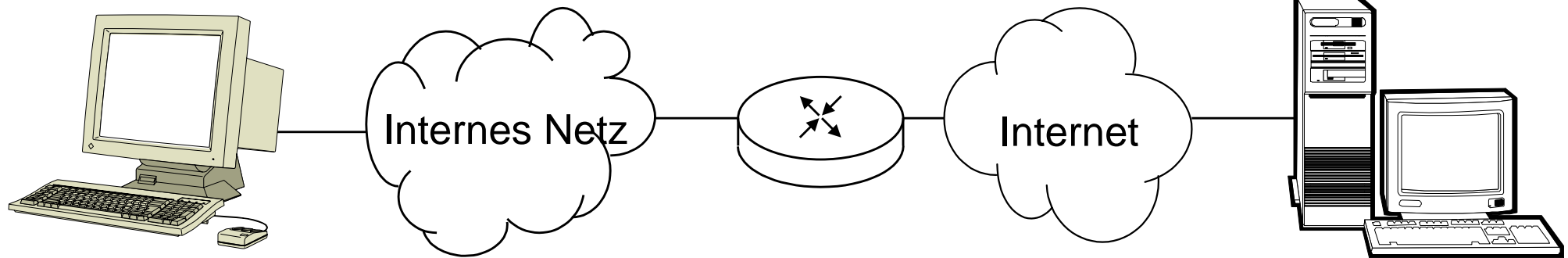
Client: 132.230.16.1

Server:132.230.151.15

proto	src-address	port	dst-address	port	flags	action
tcp	132.230.16.*	>1023	*	23	*	allow
tcp	*	23	132.230.16.*	>1023	A	allow
*	*	*	*	*	*	deny

# Firewalls - dynamische Paketfilter

## Beispiel: ftp



Client: 132.230.16.1

Server: 132.230.151.15

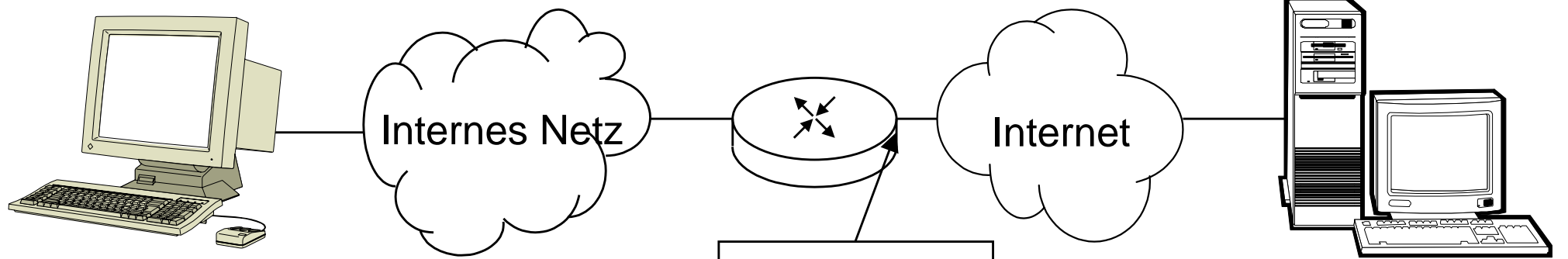
#	proto	src-address	port	dst-address	port	flags	action
1	tcp	132.230.16.*	>1023	*	21	*	allow
2	tcp	*	21	132.230.16.*	>1023	A	allow
3	*	*	*	*	*	*	deny

Client>PORT 132,230,16,1,4,150 (132.230.16.1:1174)

## Führt zu Änderung der Regeln

3	tcp	132.230.151.15	20	132.230.16.1	1174	*	allow
4	tcp	132.230.16.1	1174	132.230.151.15	20	A	allow
5	*	*	*	*	*	*	deny

# Firewalls -Network Address Translation



Client: 10.1.1.3

98.56.132.12

Server:132.230.151.15

„Private Adressen“: keine Routen im Internet

10.\*.\*, 172.16.\*.\*, 192.168.\*.\*

Umschreiben der privaten Adressen auf dem Router

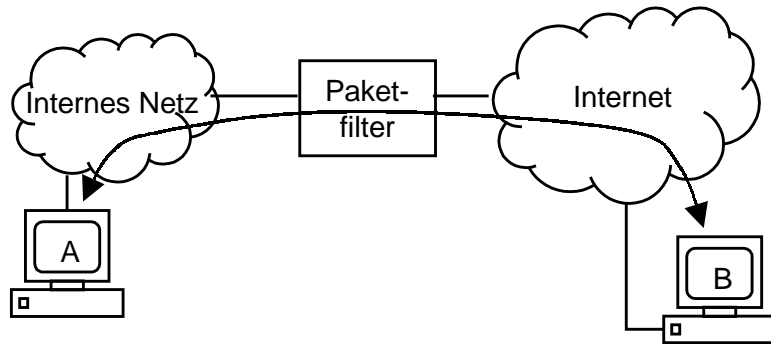
src-addr: 10.1.1.3:1074 wird src-addr: 98.56.132.12:65001

Antwort wird ebenfalls wieder umgeschrieben

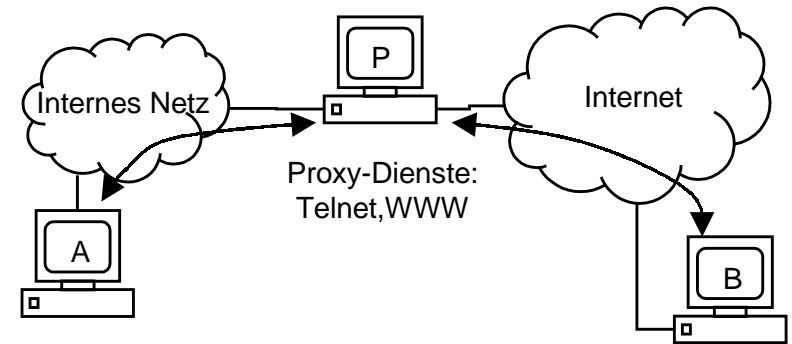
dynamisch oder statisch

(für nicht von intern initiierte Verbindungen)

# Firewalls - Paketfilter vs Proxies



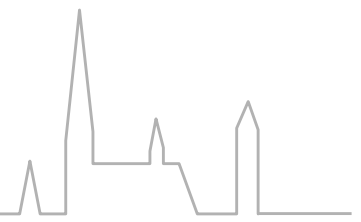
- Auf IP Ebene
- meist auf Routerhardware
- erlaubt Verkehr zwischen einzelnen Adressen
- Auswerten des TCP Headers ermöglicht Filterung von Ports (SMTP, TELNET)
- Filterung von Protokollen (RIP)
- Filterung von IP-Optionen (Source Routing) und Abwehr von IP-Spoofing



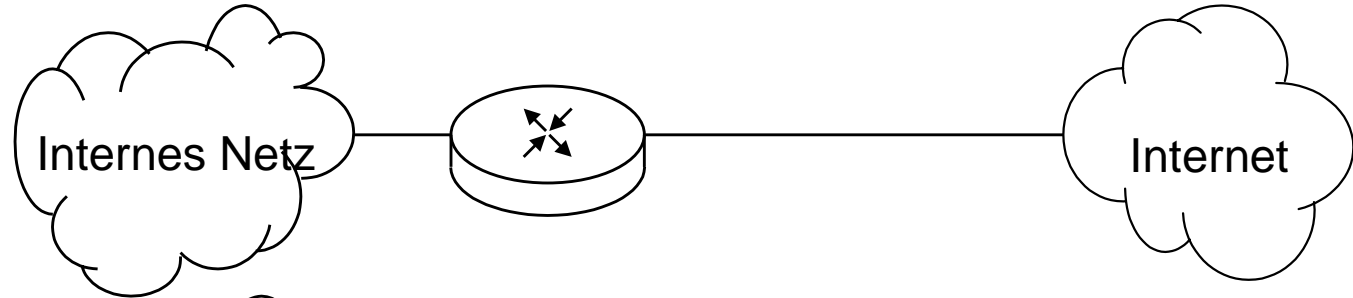
- Auf Anwendungsebene
- Benutzerauthentisierung möglich
- kein direkter Datenaustausch (Pufferüberlauf- und Flutungsattacken auf das interne Netz nicht möglich)
- Auswerten des Anwendungsprotokolls ermöglicht Filterung von Diensten (SMTP Befehle VRFY, EXPN)

Hybridlösung: dynamische Paketfilter, Stateful Inspection

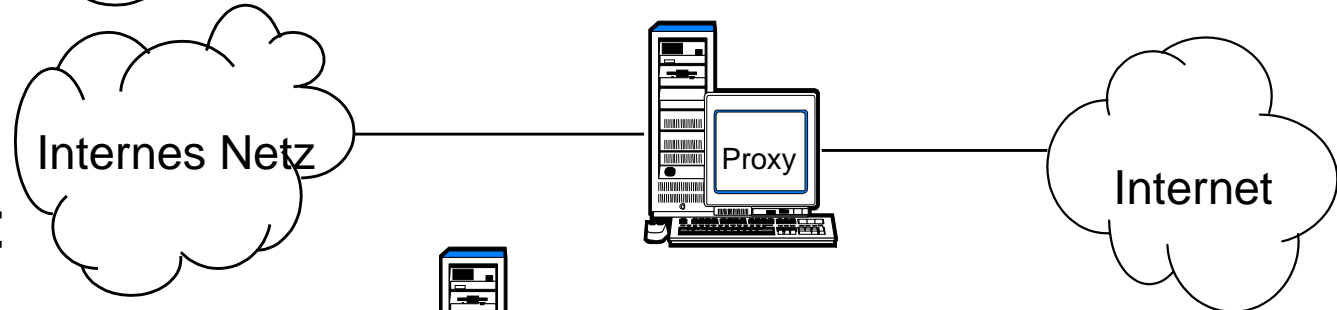
# Firewalls - Konfigurationen



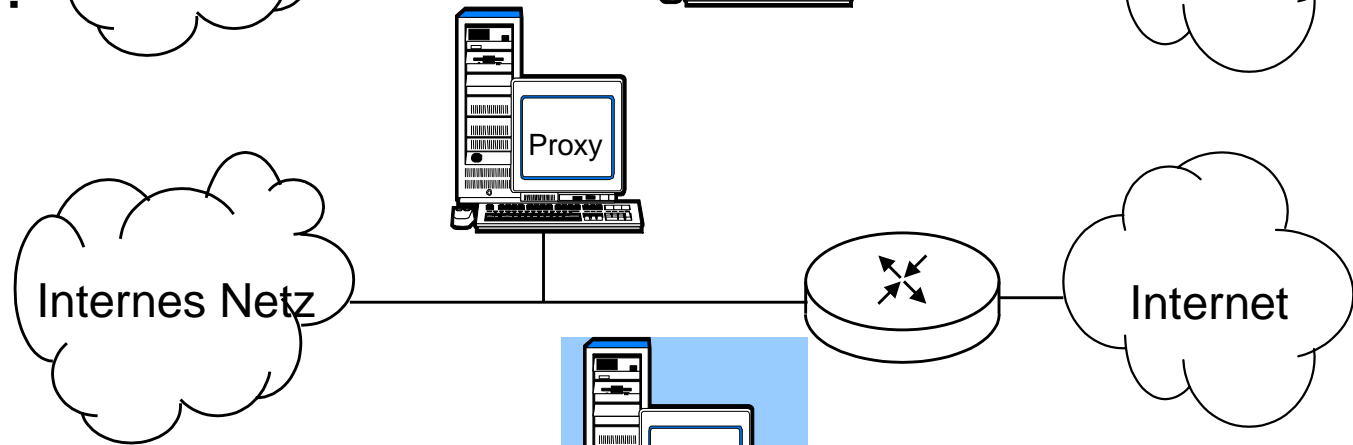
Paketfilter:



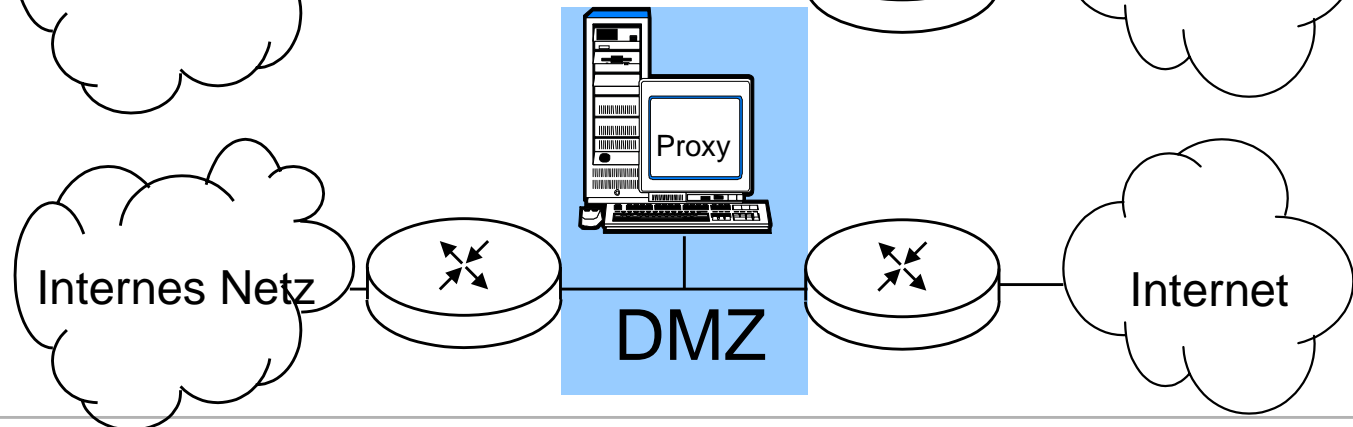
Dual homed application gateway:



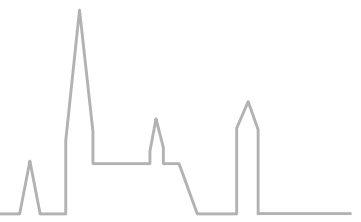
Screened host:



Screened subnet:

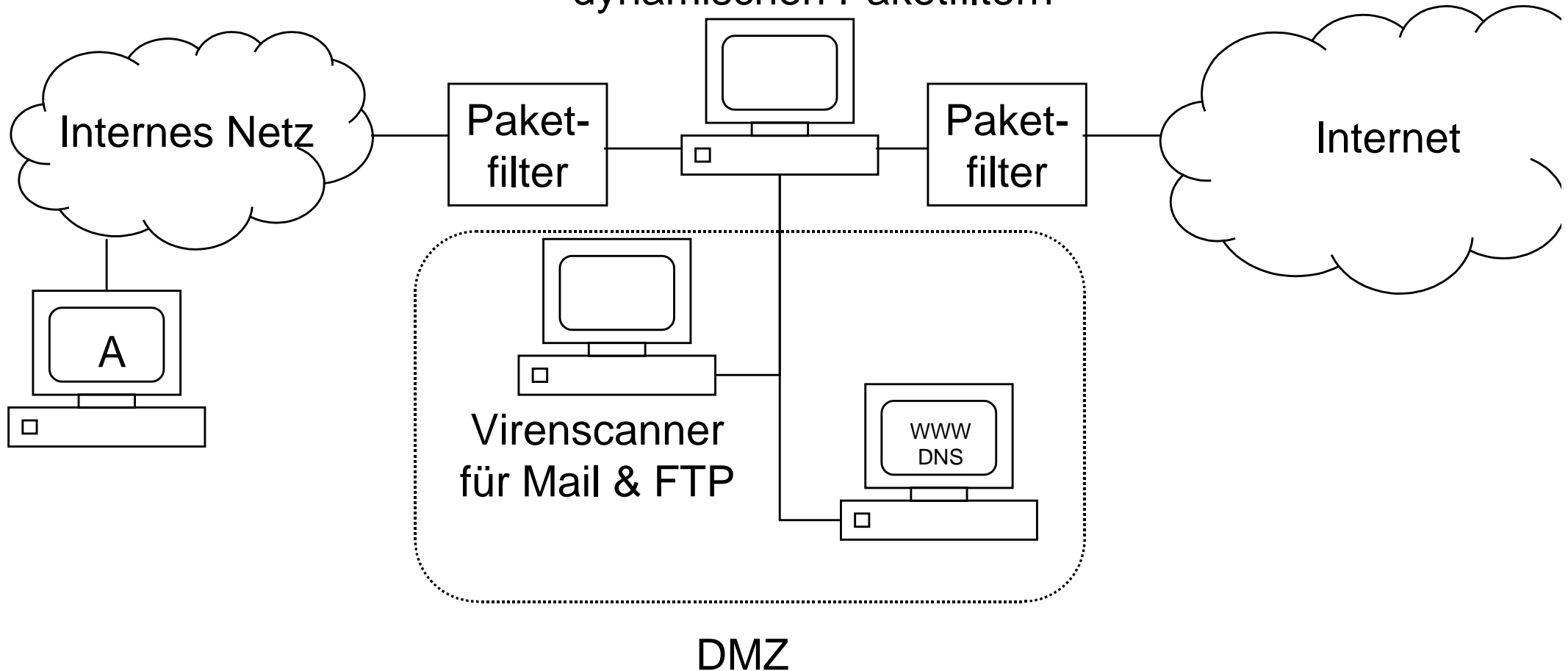


# Firewalls - Beispiel

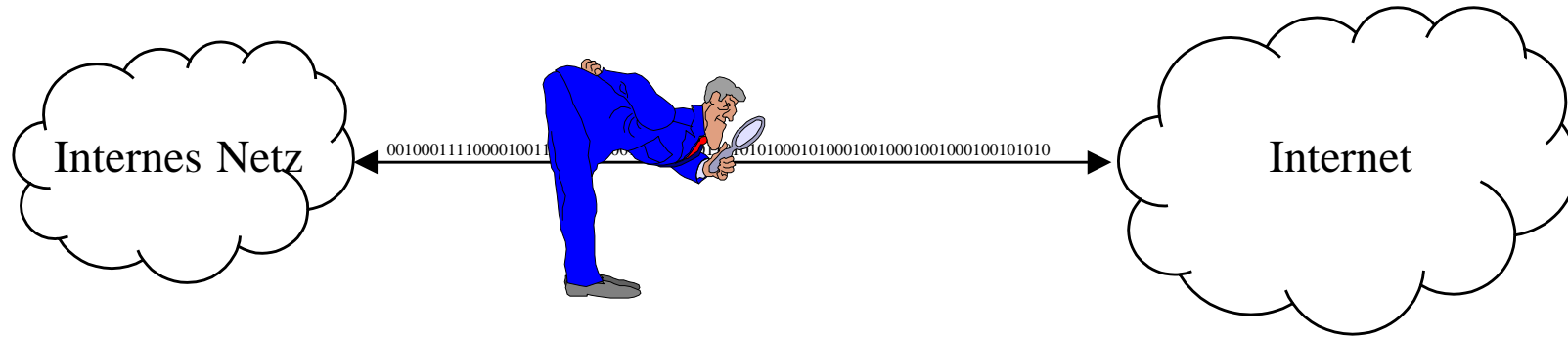
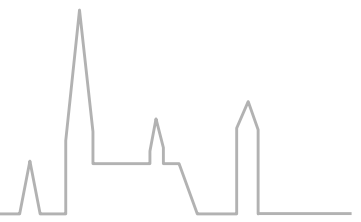


## Zusätzliche Funktion: Content Filtering

Firewall mit Proxies und dynamischen Paketfiltern



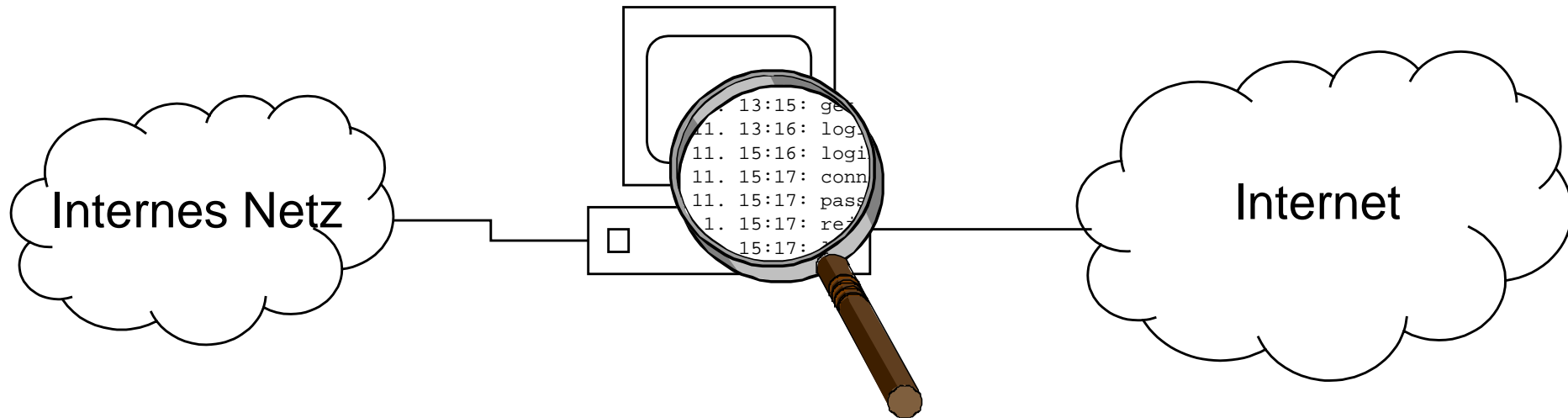
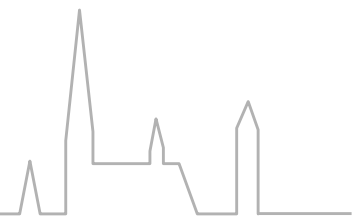




Aller Internetverkehr geht über die Firewall:

- Aus den Log-Dateien lassen sich Benutzerprofile erstellen
- Wer Zugang zur Firewall hat, kann den gesamten Internetverkehr mitlesen
- Administrativer Aufwand
- interne Benutzer können Sicherheitskonzept unterlaufen (Modems)
- Angriffe von innen werden nicht abgewehrt!

# Firewall - Intrusion Detection



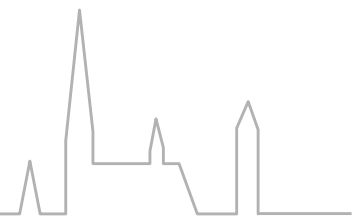
Auswertung der Firewall Logfiles:

- kontrolliert die Verbindungen zwischen internem Netz und Internet
- sichert die Integrität der Firewall
- stellt Portscans, Syn flooding etc. fest

Nachteil: Angriffe von innen werden nicht erkannt

# Intrusion Detection Systeme (IDS)

---



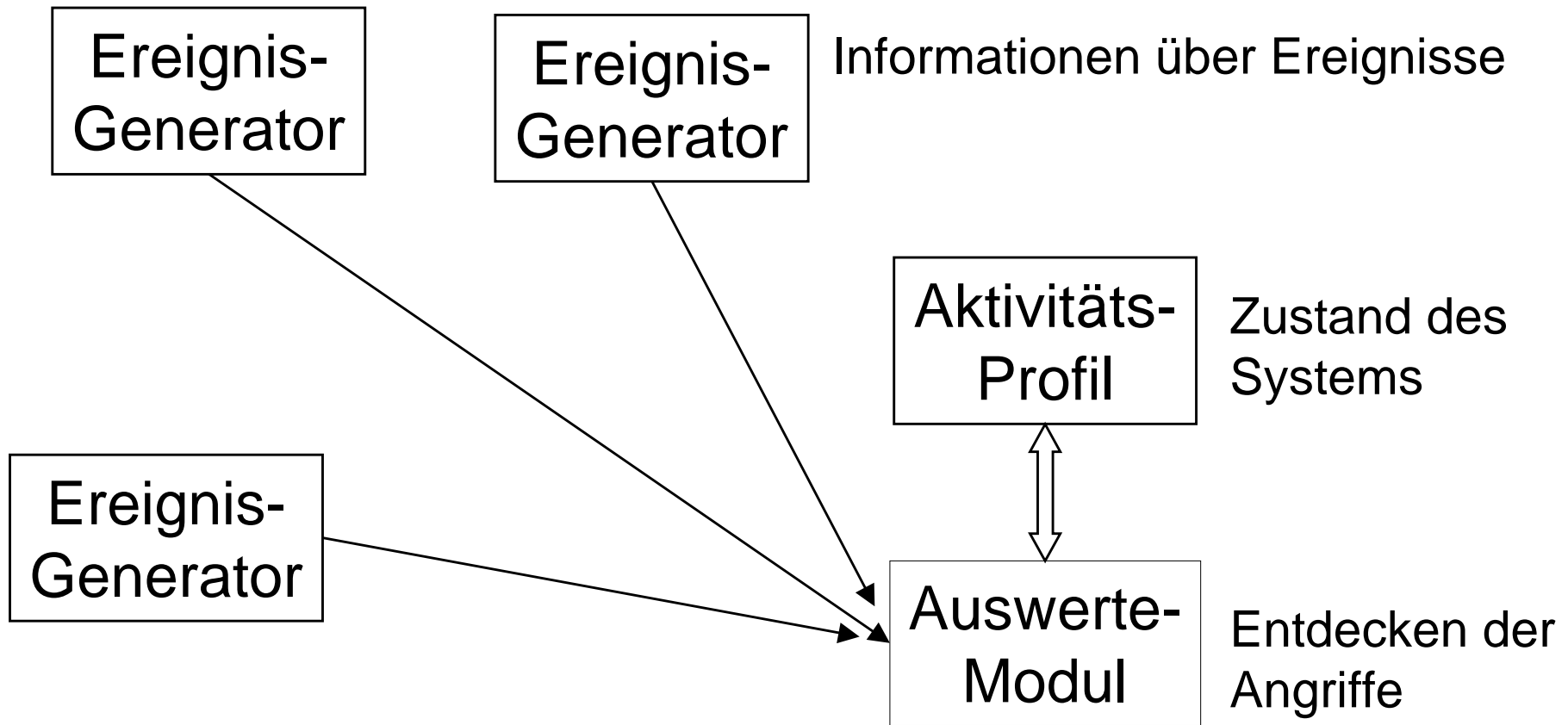
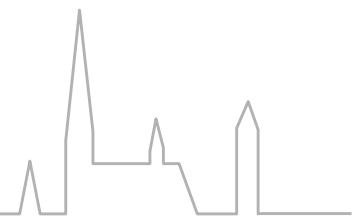
Intrusion: Aktion, die mit der gültigen Sicherheitspolicy nicht vereinbar ist

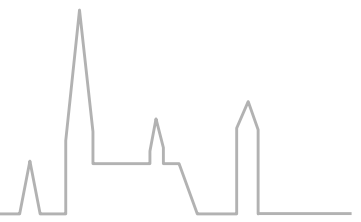
Beispiele:

- Viren
- Buffer-Overflows
- CGI-Fehler
- Denial of Service
- Address-Spoofing
- Race Conditions



# IDS - generelles Modell

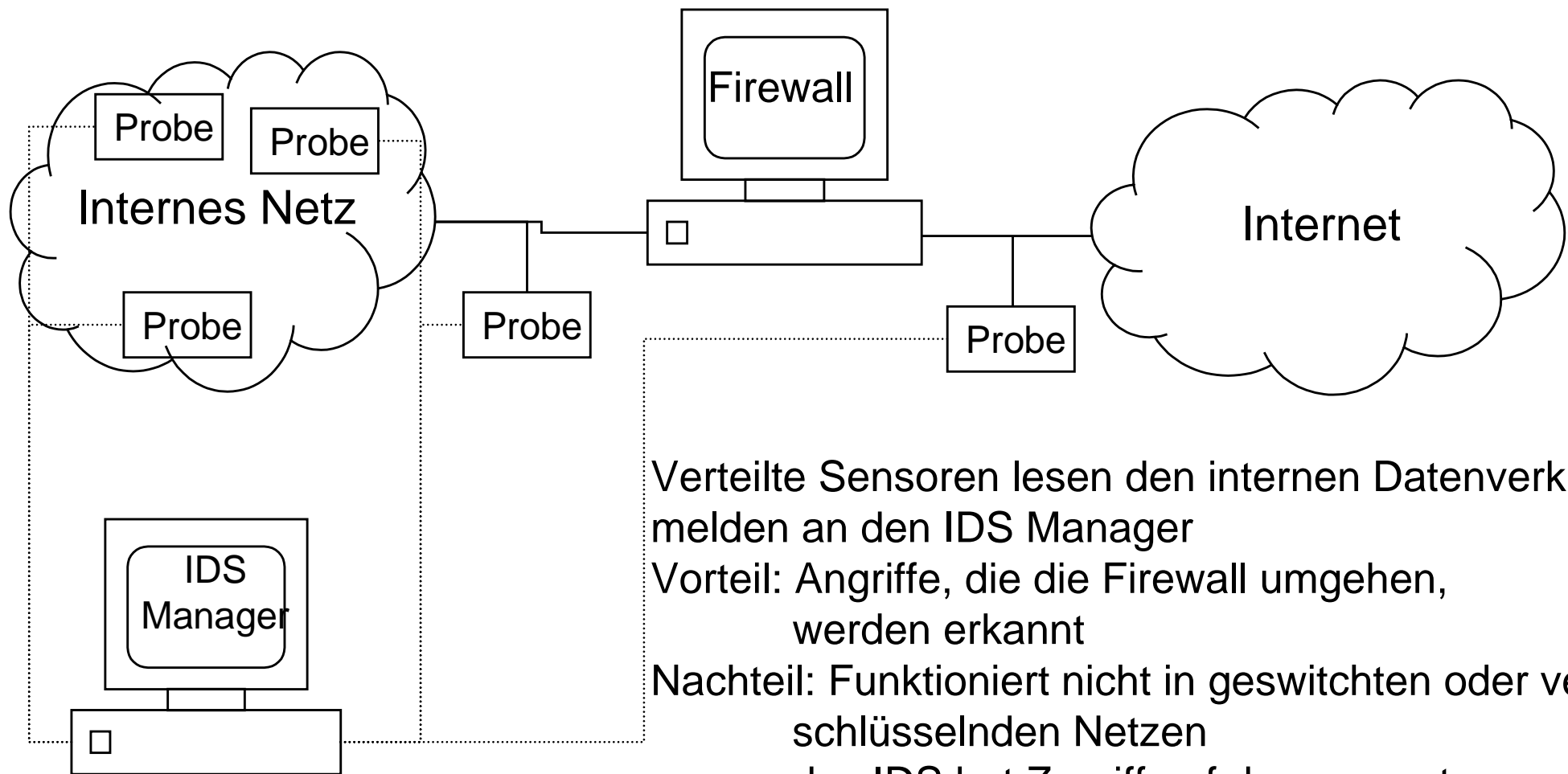




- **Detektions-Art**
  - Muster-Erkennung
  - Statistische Anomalie
  - Hybrid
- **Plazierung**
  - Host-basiert
  - Netzwerk-basiert
  - Hybrid
- **Zeitfaktor**
  - Beinahe Echtzeit
  - Post-mortem
- **Daten-Sammlung**
  - Push
  - Pull



# IDS - Netzwerkbasierend

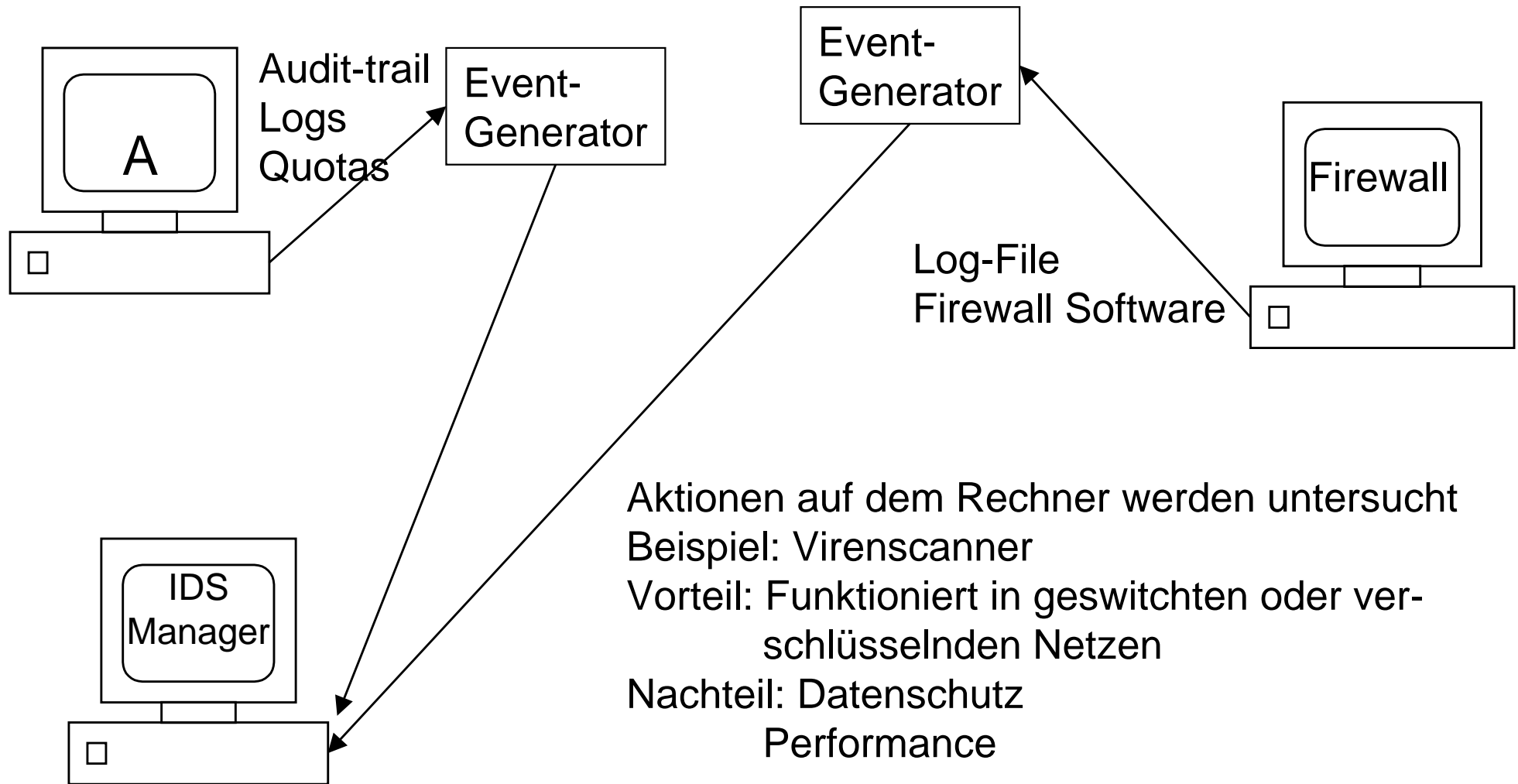
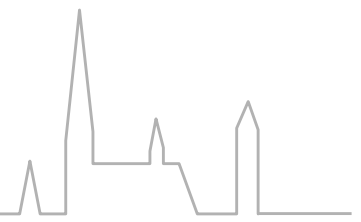


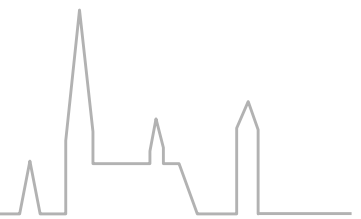
Verteilte Sensoren lesen den internen Datenverkehr, melden an den IDS Manager

Vorteil: Angriffe, die die Firewall umgehen, werden erkannt

Nachteil: Funktioniert nicht in geschichteten oder verschlüsselnden Netzen  
das IDS hat Zugriff auf den gesamten Datenverkehr (Datenschutz!)

# IDS - Host-basiert

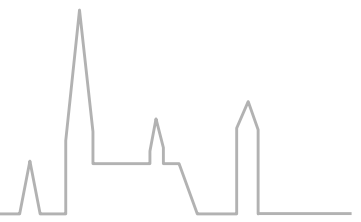




- Signatur Vergleich: bekannte Angriffs-Signaturen werden erkannt
- Anomalie: vom „Normalen“ abweichende Aktivitäten werden als Angriff gemeldet
- Bottleneck: privilegierte Operationen, die durch eine Hintertür ausgeführt werden, werden erkannt
- Integritäts-Checker

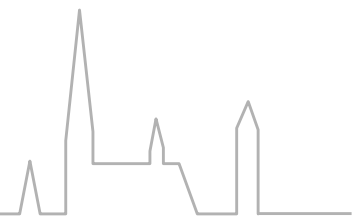






- sehr problematisch
- Verarbeitung personenbezogener Daten
- Auswertung begrenzt erlaubt
  - nur zu vorher festgelegten Zwecken
  - keine Arbeitsüberwachung
- Pseudonymisierung von Audit-Daten
  - Überschreiben der Benutzeridentifikation
  - Auflösung des Pseudonyms im Verdachtsfalle

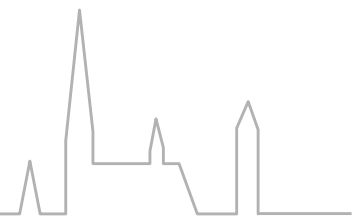




- Firewalls entspricht der mittelalterlichen Stadtmauer
- IDS entspricht „Big Brother“?
- Umgehen der Sicherheitsmechanismen ist möglich (Übung)

Sicherheitsarchitektur muss weiterentwickelt werden





- Rolf Oppliger - Internet and Intranet Security; 1998
- Norbert Pohlmann - Firewall Systeme; 1998
- Rainer Falk - Formale Spezifikation von Sicherheitspolitiken für Paketfilter; GI-Fachtagung VIS '97
  
- M. Sobirey - Aktuelle Anforderungen an Intrusion Detection Systeme...; GI-Fachtagung VIS '99
- Mark Krause and Clarissa Cook - Tutorial Intrusion Detection; ACSAC '98
  
- Andrew Tanenbaum - Computernetzwerke; 1996
- Richard Stevens - TCP/IP Illustrated, Volume 1; 1994

