



••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

Netzwerksicherheit Firewall-Architekturen

Stephen Wolthusen





Ansätze bei der Realisierung von Firewalls

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Default Allow

- „*Alles, was nicht explizit verboten ist, ist erlaubt*“.
- Erlaubt nur reaktives Vorgehen des Administrators
- Unwirksam, da Dienste einfach auf „noch nicht“ verbotene Ports umgelenkt werden können

■ Default Deny

- „*Alles, was nicht explizit erlaubt ist, ist verboten*“.
- Folge: Viele vertraute Dienste sind nicht (mehr) verfügbar
- Erfordert Planung der bereitzustellenden Dienste





Paketfilter

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Konzept entstand parallel zu Ethernet am Xerox PARC (Alto)
 - Filterung auf Ethernet-Ebene (heute: Bridge)
- Weiterentwicklung an CMU und Stanford
 - erste Unix-Implementierung 1980
- Abgeleitete Implementierungen:
 - DEC Ultrix Packet Filter
 - Sun NIT (Network Interface Tap) ⇒ **snoop(1M)**
 - Berkeley Packet Filter (BPF)





Paketfilter (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Erste Generation der Firewalls

- Erste Implementierung 1987 am DEC WRL (**screend**)
- Geht davon aus, daß vertrauenswürdige Dienste an „privileged ports“ bereitgestellt sind

■ Berücksichtigt nur einzelne Pakete, keine Datenströme

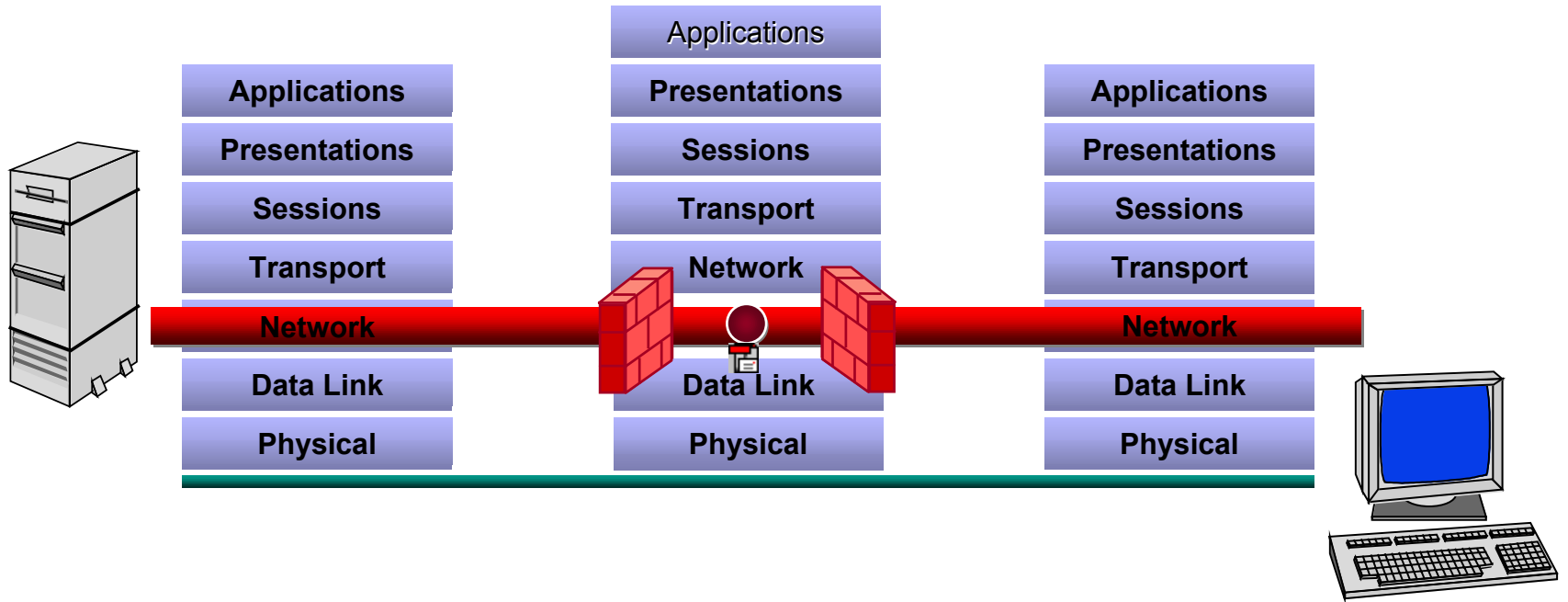
- Ausschließlich auf Ebene 3 im OSI-Referenzmodell
- Kann neben anderen Aufgaben parallel zu Routing durchgeführt werden





Paketfilter (2)

... department security technology ... department security technology ... department security technology ... department security technology ...





Für Paketfilter zur Verfügung stehende Informationen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- IP-Quelleadresse
- IP-Zieladresse
- Protokolltyp (TCP,UDP,ICMP,IGMP)
- TCP oder UDP Quell-Port
- TCP oder UDP Ziel-Port
- ICMP- oder IGMP-Nachrichtentyp
- Physikalische Schnittstelle, auf der Datagramm empfangen wird
- Physikalische Schnittstelle, auf der Datagramm versendet wird





Einsatzgebiet: Pre-Filtering

... department security technology ... department security technology ... department security technology ... department security technology ...

- Router können bei Implementierung in ASICs Pakete mit voller Bandbreite verarbeiten sofern die Regeln nicht zu komplex sind
 - Schutz vor Spoofing
 - Blockieren von privaten Adressen nach innen/außen
 - Schutz vor unerwünschten ICMP/IGMP-Nachrichten
 - Blockierung von unerwünschten Protokollen

- Viele (kleine/ältere) Router müssen bei Angabe von Paketfilter-Regeln durch reguläre CPU verarbeiten - bei massiver Reduktion der Routing-Geschwindigkeit





Einsatzgebiet: Aufbereitung

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Eine Reihe von Betriebssystemen setzt „fragile“ TCP/IP-Stacks ein
- Filterung und/oder Normalisierung auf
 - ungewöhnliche Optionen
 - Flags, Kombinationen von Flags, Optionen
 - Fragmentierung
 - ▲ Zu große / zu kleine Segmente
 - ▲ Pathologische Offsets
- Problem: Widerspricht eigentlich RFC 1812
„*Requirements for IP version 4 routers*“





Einsatzgebiet: Schutz vor Denial of Service

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Eine Reihe von DoS-Angriffen können mittels Paketfilter eliminiert werden
 - SYN-Floods, Smurf: Mehr dazu nächste Woche
 - Von DoS-Angriffen genutzte Verkehrsmuster haben selten legitime Grundlagen
 - ▲ Keinen Datenverkehr zulassen sofern nicht Notwendigkeit demonstriert wurde

- Traffic Shaping
 - Auswirkungen von DDoS auf interne Netzwerke beschränken





Konfigurationsmöglichkeiten (2)

... department security technology ... department security technology ... department security technology ... department security technology ...

```
default reject notify log;  
for ftc-net netmask is 255.255.255.0;  
# more configuration data in between omitted  
between host mail-relay tcp port smtp  
    and any accept;  
between host mail-relay  
    and any tcp port smtp accept;
```

■ screend (Digital, 1989ff.)

- Leserliche Syntax
- Detaillierte Sammlung von Revisionsdaten





Paketfilterung in Cisco IOS: Access Control Lists

... department security technology ... department security technology ... department security technology ... department security technology ...

- Müssen für jede Schnittstelle und Richtung eingerichtet werden
- Regeln werden an das Ende einer ACL angefügt, die Regel `deny all traffic` wird implizit an das Ende angefügt
- Syntax für ACLs:

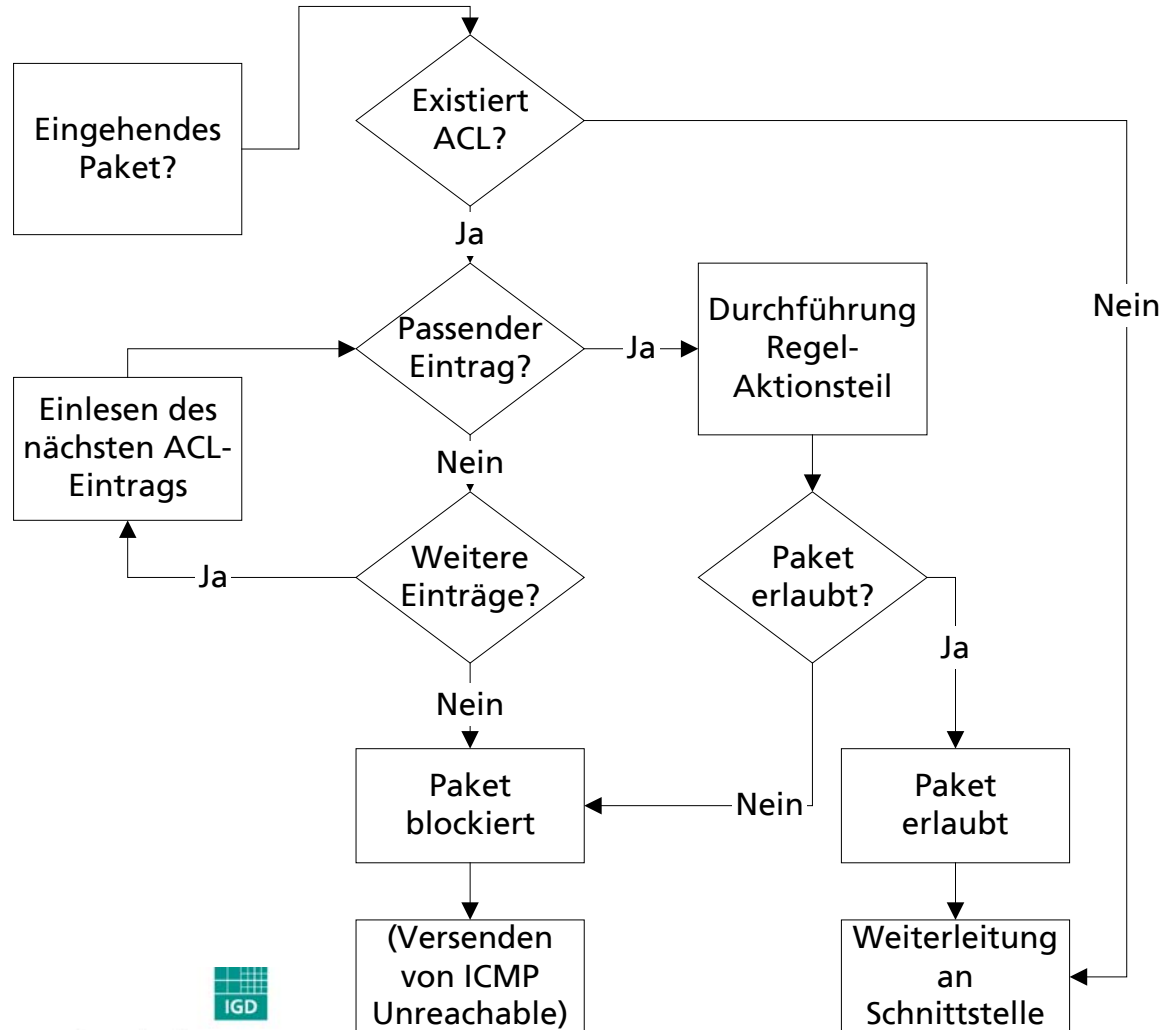
```
access-list {ACL Number} {permit|deny} [protocol]
           {source address and mask}
           [source port number or range]
           [destination address and mask]
           [destination port number or range]
           [options]
```





Paketfilterung in IOS: Verarbeitung von ACLs

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Beispiele für einfache ACL-Regeln

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Löschen bestehender ACL

- `no acc 101`

■ Blockieren vor Spoofing

- `acc 101 deny ip 146.140.210.0 0.0.0.255 0.0.0.0
255.255.255.255`

■ Zulassen von DNS Resolving

- `acc 101 permit udp any gt 1023 host 146.140.210.38 eq
53`

■ Zulassen von Pings auf den Nameserver

- `acc 101 permit icmp any host 146.140.210.38 echo-reply`





Regeln für Schutz der Topologie, eingehendes TCP

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Verhinderung von ARP-Anfragen
 - `no ip proxy-arp`
- Verhinderung von Erreichbarkeits-Nachrichten
 - `no ip-unreachables`
- Verhinderung von Source Routes
 - `no ip source-route`
- Zulassen nur von ausgehenden TCP-Verbindungen
 - `acc 101 permit tcp 0.0.0.0 255.255.255.255
146.140.210.0 0.0.0.255 est`





Schutz vor DoS: TCP Intercept

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- ❑ `ip tcp intercept list 101`
- ❑ `ip tcp intercept mode watch`
- ❑ `ip tcp intercept drop-mode random`
- ❑ `ip tcp intercept watch-timeout 30`
- ❑ `ip tcp intercept finrst-timeout 5`
- ❑ `ip tcp intercept connection-timeout 3600`
- ❑ `ip tcp intercept max-incomplete low 900`
- ❑ `ip tcp intercept max-incomplete high 1100`
- ❑ `ip tcp intercept one-minute low 1000`
- ❑ `ip tcp intercept one-minute high 1500`





Proxy-System / Application Level Gateway

... department security technology ... department security technology ... department security technology ... department security technology ...

- Ziel: Maximale Absicherung von Netzwerkverkehr
- Basiert auf regulärem (gehärtetem) Betriebssystem, TCP/IP Stack
 - hängt von Qualität des Wirtssystems ab
- Muß in Verbindung mit Screening Router/Subnet betrieben werden bzw. Dual-Homed Host sein
 - Schutz vor DoS durch vorgeschalteten Paketfilter
 - Paketfilter ordnet Verkehr der DMZ oder dem ALGW zu
 - Verkehr aus geschütztem Netzwerk wird nur von ALGW akzeptiert





Application Level Gateway

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

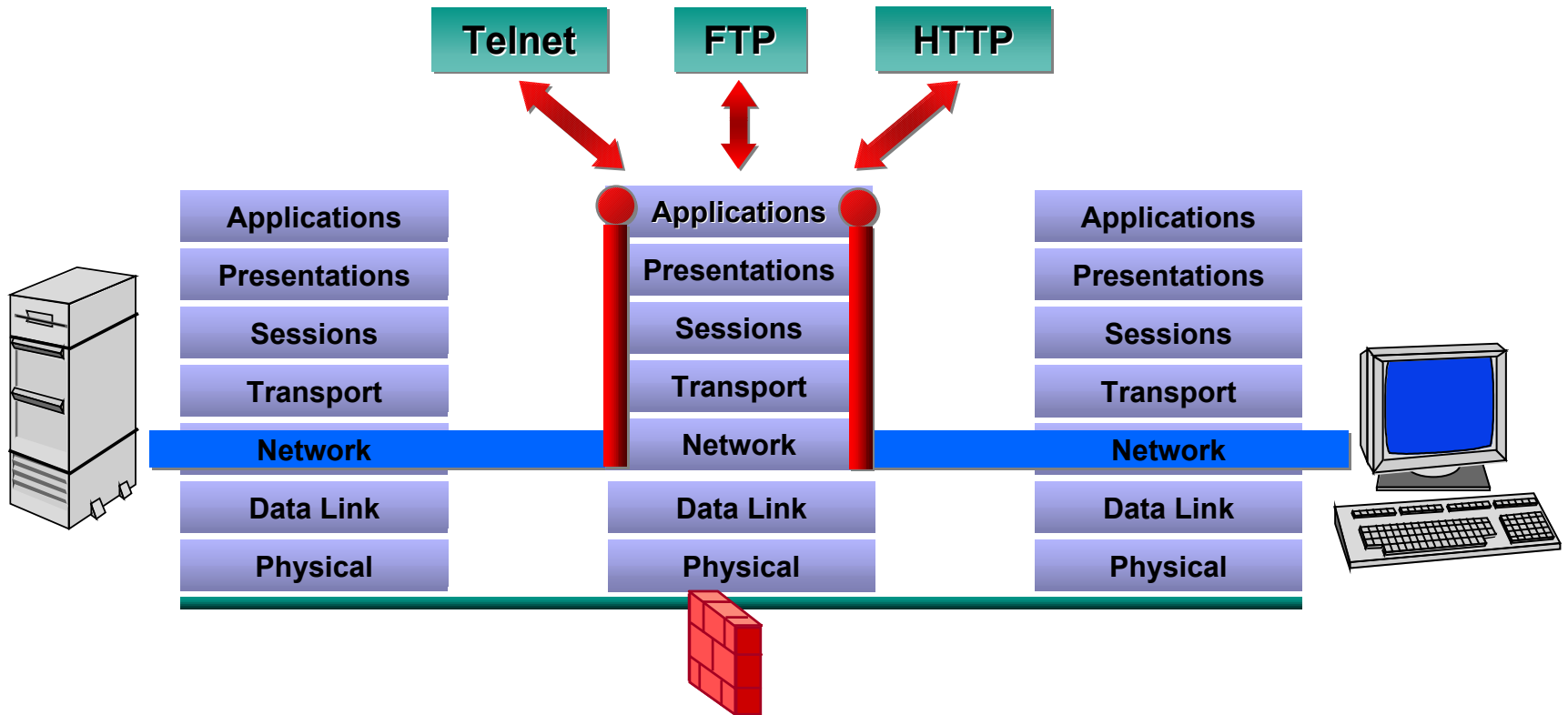
- **Anwendungsbasierte Filterung von spezifischen Protokollen**
 - kann mit Caching Proxy kombiniert werden, ist aber nicht sinnvoll
- **Implementierung durch direkten Login auf ALGW**
 - Wenig sinnvoll, erhöht Komplexität, reduziert Skalierbarkeit, nicht alle Protokolle unterstützen Umleitung
- **Implementierung als Proxies**
 - Proxy entscheidet über Zulässigkeit, Wohlgeformtheit
 - Zugriff auf semantische Informationen möglich
 - Nur bei Nutzung der Protokollsemantik wirklich sinnvoll





Proxy-System / Application Level Gateway

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Möglichkeiten des Client-Zugriffs auf ALGW-Proxies

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Spezifische Client-Software

- Zugriff auf Proxies wird innerhalb der Client-Software realisiert
- Protokolle wie HTTP unterstützen dies direkt
- Erfordert geeignete Konfiguration der Anwendungen

■ Änderung des Anwender-Verhaltens

- Authentisierung gegenüber ALGW muß getrennt erfolgen
- Bedienverhalten ändert sich gegenüber ungeschütztem Datenverkehr
- Beispiel: FTP





TIS Firewall-Toolkit

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- 1993 im Auftrag der ARPA entwickelt
 - einfache, kostenlos verfügbare Sammlung von Proxies
 - kommerziell zu NAI Gauntlet weiterentwickelt
- Dienste werden mittels `inetd(1M)` gestartet
- Zugriffskontrolle erfolgt mit Wrapper um bestehende TCP-Dienste: `netac1`
- `netac1` führt auch Sammlung von Revisionsdaten durch





Reguläre inetd.conf-Datei (Solaris)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

```
■ ftp      stream  tcp6    nowait  root    /usr/sbin/in.ftpd      in.ftpd
■ telnet   stream  tcp6    nowait  root    /usr/sbin/in.telnetd   in.telnetd
■ chargen stream  tcp6    nowait  root    internal
■ chargen dgram  udp6    wait    root    internal
```

- Dienste werden nur bei Bedarf als Kindprozesse von `inetd` gestartet
- Einige primitive/nutzlose Dienste sind bereits Bestandteil von `inetd`
- Standardkonfigurationen der meisten Betriebssysteme sind meist überladen mit unnötigen Diensten





FWTK-Konfiguration von inetd.conf

... department security technology ... department security technology ... department security technology ... department security technology ...

■	ftp	stream	tcp6	nowait	root	/usr/local/etc/netacl	in.ftpd
■	ftp-gw	stream	tcp6	nowait	root	/usr/local/etc/ftp-gw	ftp-gw
■	telnet-a	stream	tcp6	nowait	root	/usr/local/etc/netacl	in.telnetd
■	telnet	stream	tcp6	nowait	root	/usr/local/etc/tn-gw	tn-gw
■	login	stream	tcp6	nowait	root	/usr/local/etc/rlogin-gw	rlogin-gw
■	finger	stream	tcp6	nowait	nobody	/usr/local/etc/netacl	in.fingerd
■	smtp	stream	tcp6	nowait	root	/usr/local/etc/smmap	smmap

- Funktionsweise analog zu TCP Wrapper
- FWTK startet eigene Dienste anstelle Standarddienst
- Alternativ: Standarddienst wird nach Prüfung aktiviert





Spezifikation von Zugriffsmustern: FTP-GW

... department security technology ... department security technology ... department security technology ... department security technology ...

- ftp-gw: denial-msg /usr/local/etc/ftp-deny.txt
 - ftp-gw: welcome-msg /usr/local/etc/ftp-welcome.txt
 - ftp-gw: help-msg /usr/local/etc/ftp-help.txt
 - ftp-gw: permit-hosts 146.140.* -log { retr stor }
 - ftp-gw: timeout 3600
 - ftp-gw: deny-hosts unknown
 - ftp-gw: deny-hosts *
-
- Adressen können symbolisch, numerisch sein und positiv oder negativ Regeln formulieren





FTP-Sitzung durch FWTK FTP-GW

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- [columbia] <14> ftp firewall.ftc.igd.fhg.de
- Connected to firewall.ftc.igd.fhg.de
- 220-Proxy first requires authentication
- 220-firewall.ftc.igd.fhg.de FTP proxy (Version 3.1) ready.
- Name (firewall.ftc.igd.fhg.de:wolt): wolt
- 331 Skey Challenge: s/key 591 ik91626
- Password:
- 230 User authenticated to proxy
- ftp> user wolt@aulick
- 331- (-----GATEWAY CONNECTED TO aulick-----)
- 331- (220 aulick WU-FTP server ready.)
- 331 Password required for wolt.
- Password: #####
- 230 User wolt logged in.
- ftp>





Zustandsbasierter Paketfilter (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Auch bekannt als

- Dynamic Packet Filter
- Stateful Inspection
- Circuit Level Gateway
- Content Based Access Control
- Dynamic Access Lists

■ Grundidee:

- Verfolgung von Verbindungen innerhalb der Firewall über Zustandstabellen





Zustandsbasierter Paketfilter (2)

... department security technology ... department security technology ... department security technology ... department security technology ...

- TCP-Verbindungen können leicht verfolgt werden
 - TCP-Sitzungsaufbau, -abbau sind explizit
 - Timeouts für inaktive, halboffene Verbindungen

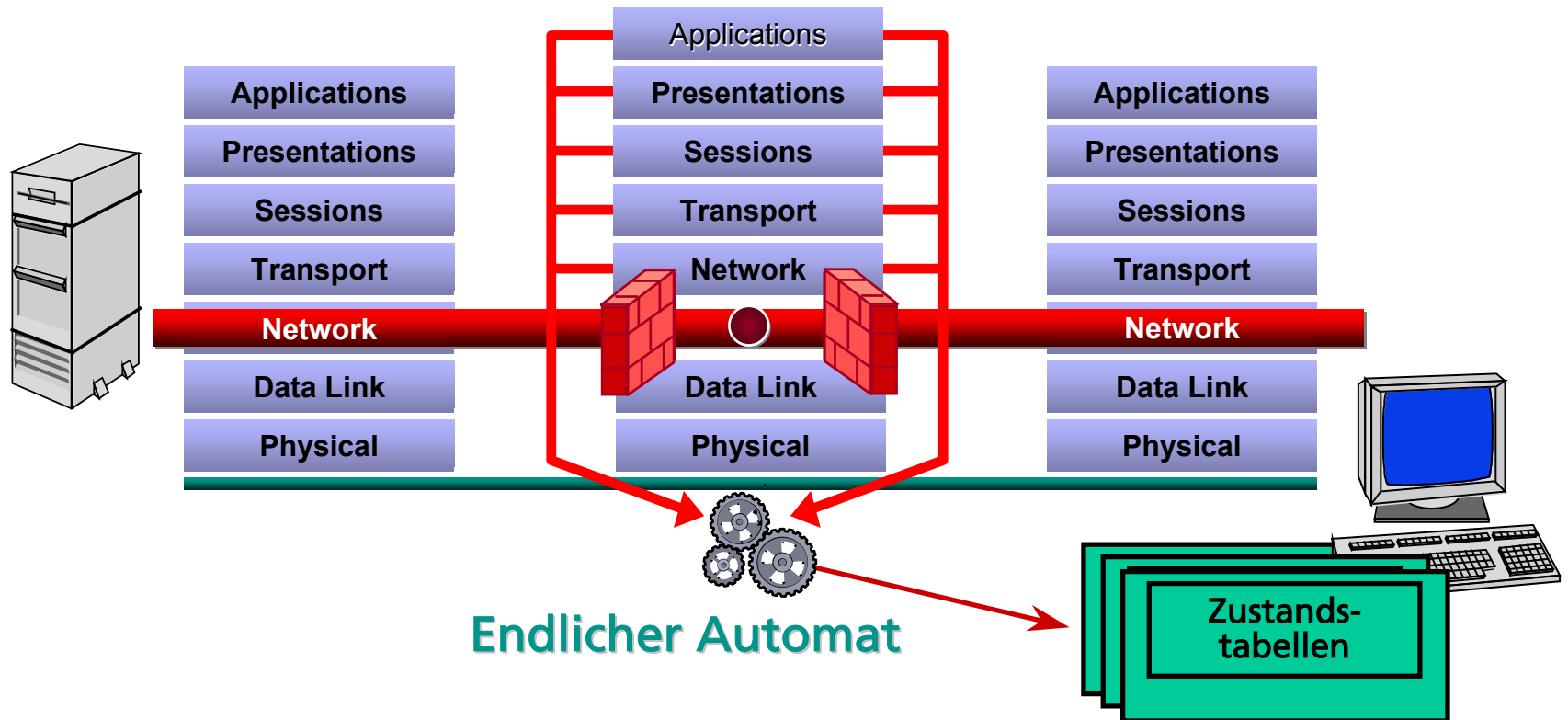
- UDP-Daten erfordern implizites Mitführen von Zustandsinformationen
 - Wissen über Protokolle erforderlich
 - ▲ Beispiel DNS: Erste Antwort beendet „Sitzung“
 - ▲ Beispiel H.323: „Sitzung“ kann mehrere Stunden bidirektionaler Kommunikation umfassen





Zustandsbasierter Paketfilter (3)

... department security technology ... department security technology ... department security technology ... department security technology ...





Dynamische ACLs in Cisco IOS

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Zulassen von Datenverkehr erst nach erfolgreicher Authentisierung: „Lock and Key“. Vorgehensweise:
 - Telnet-Sitzung zu Router
 - Authentisierung (via Paßwort, TACACS(+), RADIUS)
 - Router beendet Sitzung
 - Router modifiziert ACLs anhand von Schablonen-ACL
 - Zwei Zeitschranken: Inaktivität, globale Schranke





IOS Lock and Key: Authentisierungsschritt

... department security technology ... department security technology ... department security technology ... department security technology ...

- `telnet egw`
- `Trying 146.140.210.34 ... Open`
- `User Access Verification`
- `Username: tlow`
- `Password:`
- `[Connection to 146.140.8.34 closed by foreign host]`
- Anmeldung gegenüber externem Router/Firewall





IOS Lock and Key: ACL-Modifikation

... department security technology ... department security technology ... department security technology ... department security technology ...

■ Einträge vor Lock and Key-Authentisierung:

- ❑ `egw# sh access-list`
- ❑ `Extended IP access list 102`
- ❑ `permit tcp any host 146.140.210.34 eq telnet`
- ❑ `Dynamic test Max. 10 mins. permit ip any any timeout 5 min.`

■ Einträge nach Lock and Key-Authentisierung:

- ❑ `egw# sh access-list`
- ❑ `Extended IP access list 102`
- ❑ `permit tcp any host 146.140.210.34 eq telnet (13 matches)`
- ❑ `Dynamic test Max. 10 mins. permit ip any any timeout 5 min.`
- ❑ `permit ip host 146.140.210.70 any idle-time 5 min.`





Zeitbasierte ACLs in Cisco IOS

... department security technology ... department security technology ... department security technology ... department security technology ...

- Seit IOS 12.0: Zeitliche Einschränkung der Gültigkeit von ACLs
 - Zulässige Nutzungsmuster erzwingen
 - Notwendigkeit der Zeitsynchronisation: NTP
 - Zeitfenster können periodisch, einmalig sein

- Konfiguration (Teil 1):
 - `time-range deny-http`
 - `periodic daily 22:00 to 07:00`
 - `time-range allow-telnet`
 - `absolute start 08:00 11 august 2001 end 23:59 12 august 2001`





Konfiguration zeitbasierter ACLs in Cisco IOS (Forts.)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- `access-list 101 permit tcp any any eq www time-range deny-http`
- `access-list 103 permit tcp any any eq telnet time-range allow-telnet`
- `!`
- `clock timezone MET +1`
- `clock summer-time MEST recurring`
- `ntp update-calendar`
- `ntp server timesrv1.igd.fhg.de`
- `interface fastethernet 0`
- `ntp broadcast`





Reflexive ACLs in Cisco IOS

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Eingeführt mit IOS 11.3

- Erlaubt, Zustandsinformationen für Verbindungen zu nutzen
- Eintrag ist stets **permit**-Eintrag
- Eintrag weist gleiches Protokoll wie das verursachende Paket auf (TCP, UDP,...)
- Im Eintrag werden Quell- und Zieladressen (TCP,UDP: auch Ports) vertauscht
- Eintrag existiert bis Sitzung geschlossen ist oder Timeout erreicht ist





Konfiguration reflexiver ACLs (Teil 1)

... department security technology ... department security technology ... department security technology ... department security technology ...

- ❑ `interface fastethernet 0`
- ❑ `ip access-group infilter in`
- ❑ `ip access-group outfilter out`
- ❑ `! set global timeout`
- ❑ `ip reflexive-list timeout 120`
- ❑ `! set up reflex lists`
- ❑ `ip access-list extended outfilter`
- ❑ `permit tcp any any reflect refconn`
- ❑ `permit udp any any reflect refconn`
- ❑ `permit icmp any any reflect refconn`





Konfiguration reflexiver ACLs (Forts.)

... department security technology ... department security technology ... department security technology ... department security technology ...

- ❑ ! combined inbound access list
- ❑ ip access-list extended infiltrer
- ❑ ! some basic filtering rules
- ❑ deny ip 146.140.210.0 0.0.0.255 any
- ❑ deny ip 10.0.0.0 0.255.255.255 any
- ❑ deny ip 172.16.0.0 0.31.255.255 any
- ❑ deny ip 192.168.0.0 0.0.255.255 any
- ❑ ! now add the reflexive rules on top
- ❑ *evaluate refconn*





Content Based Access Control in Cisco IOS

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Als „Firewall Feature Set“ in IOS 11.2 eingeführt, seit IOS 12.0 im allgemeinen Funktionsumfang
 - Erweiterung reflexiver ACLs
 - Verwendung dynamischer Protokolle, mehrere TCP-, UDP-Verbindungen sind möglich
 - Neben Headern müssen dabei auch Teile des Inhalts analysiert werden
 - Protokolle können damit partiell auch inhaltsbasiert, nicht nur auf Grundlage von Adressen und Ports gefiltert werden
 - Nur TCP, UDP können bearbeitet werden
 - Verbindung mit IPSEC nicht möglich: Verarbeitungsreihenfolge





Vorgehen bei CBAC

... department security technology ... department security technology ... department security technology ... department security technology ...

- Paket auf ausgehender Schnittstelle wird gegen „outgoing“ ACL verglichen
- CBAC evaluiert Paket, speichert Informationen daraus in Tabelle
- Erzeugung temporärer Einträge in den korrespondierenden eingehenden ACLs
- Sofern Antwort auf virtuelle Verbindung in Tabelle eintrifft: Evaluierung durch CBAC, bei Weiterleitung kann auch „inbound“ ACL modifiziert werden
- Alle weiteren Pakete der virtuellen Verbindung werden von CBAC überwacht
- Bei Beendigung (FIN, RST, Timeout) werden Tabelleneinträge gelöscht





Hybride Architekturen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

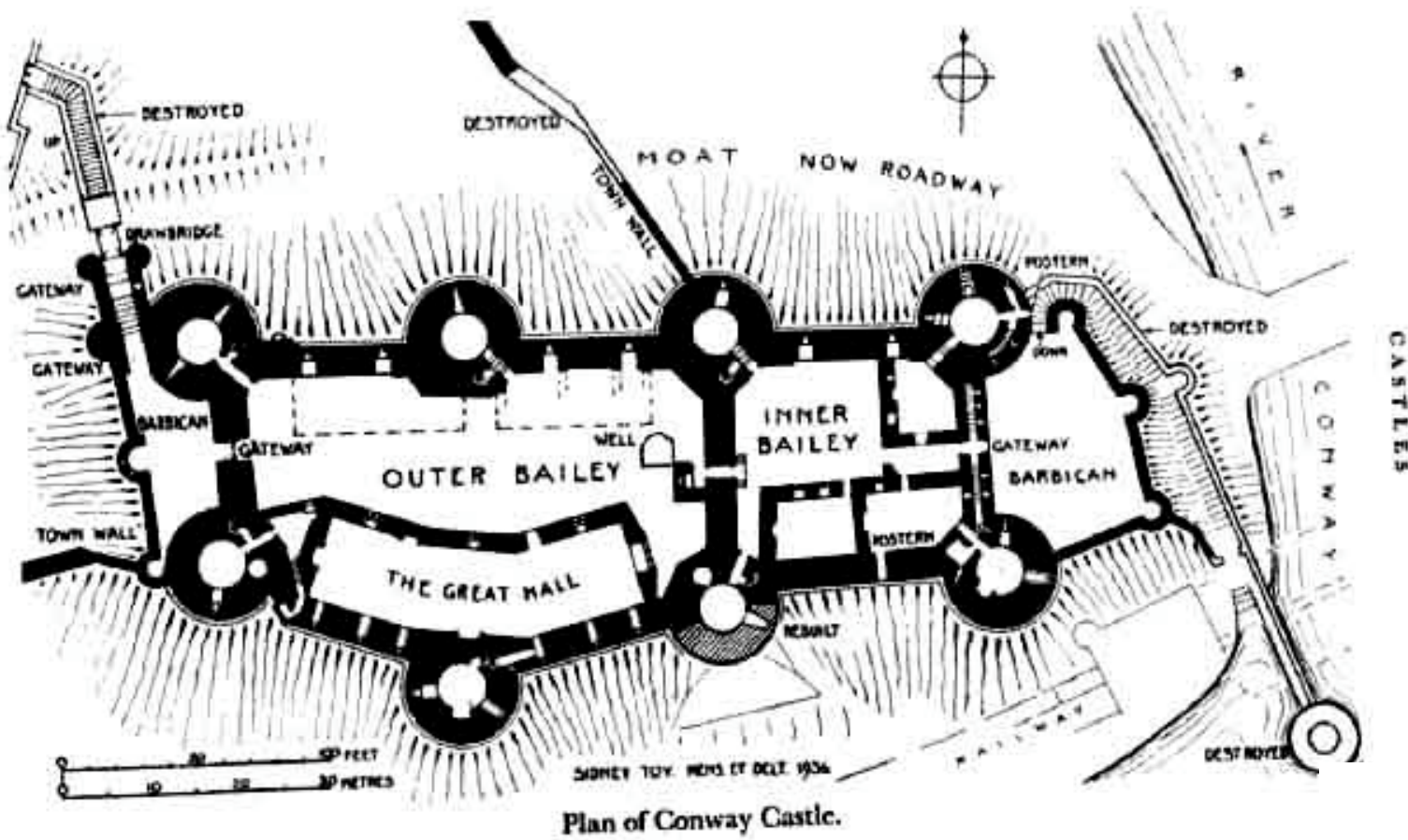
- Häufig gibt es nicht „die“ richtige Implementierung
- Kombination mehrerer Firewalling-Techniken ist sinnvoll
 - Paketfilter als primärer Schutz vor Spoofing, Fehlkonfiguration, (partiell) DoS
 - ALGW-Proxies für kritische Protokolle (HTTP,SMTP) bei denen die Protokollsemantik bekannt ist
 - Zustandsbasierte Paketfilterung für übrige Protokolle
 - Implementierungsfehler in einer Komponente können eventuell durch andere Komponenten ausgeglichen werden





Plus ca change... Plus C'est La Même Chose

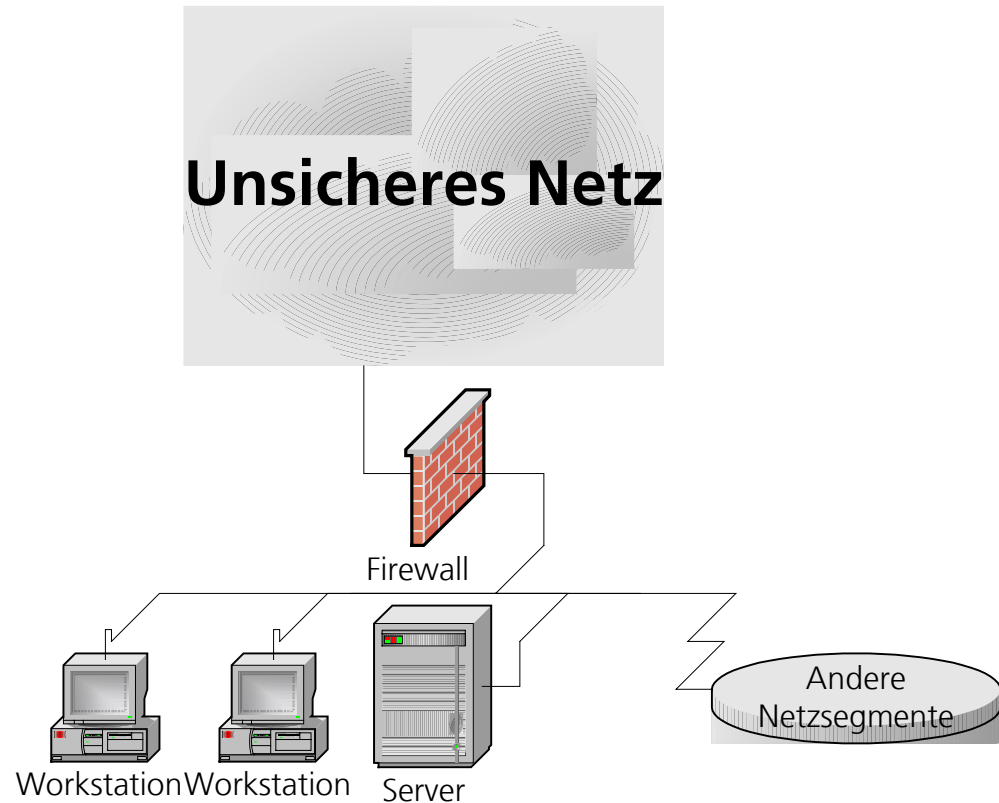
••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Elementare Topologie traditioneller Firewalls

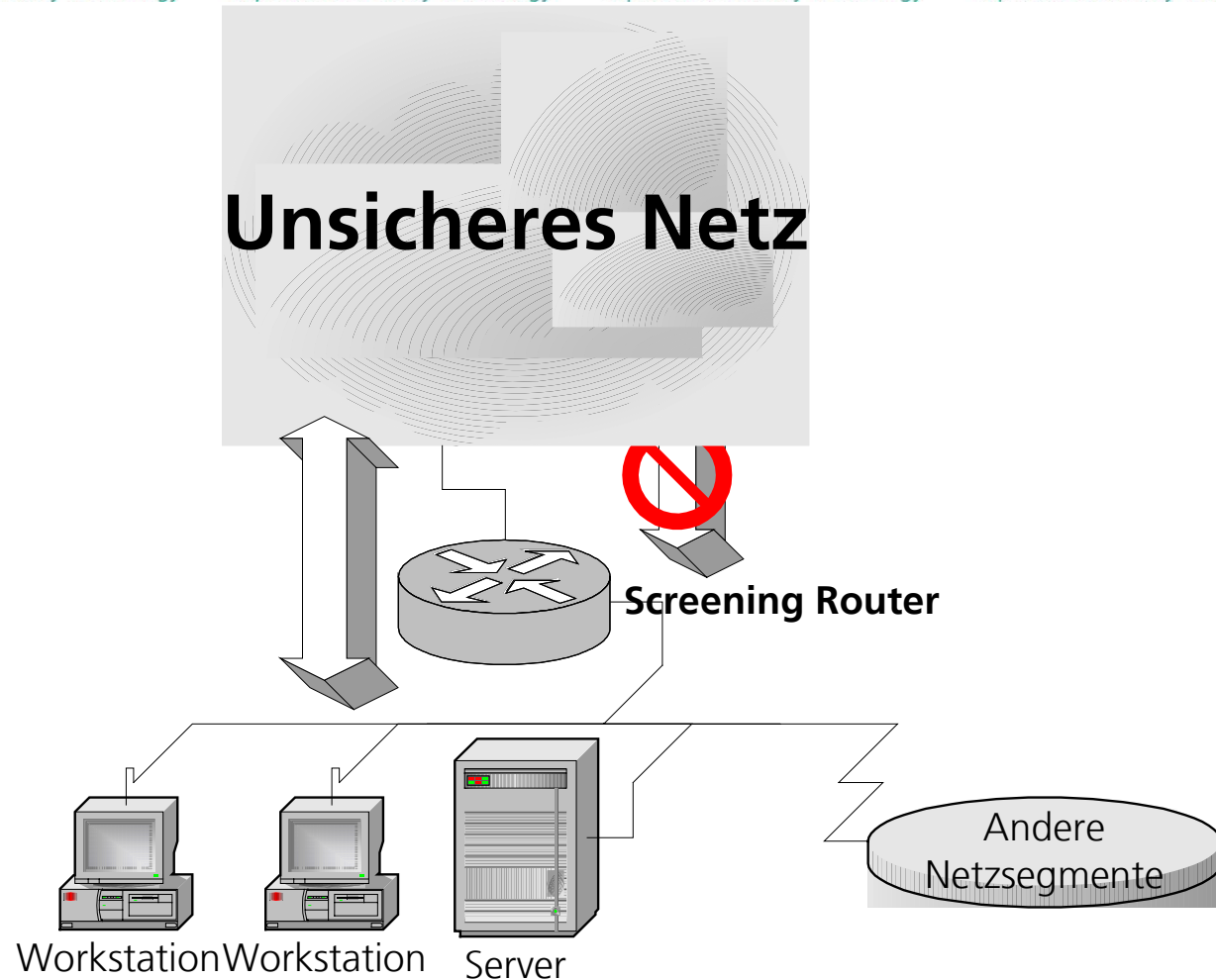
••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Screening Router

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Screening Router

... department security technology ... department security technology ... department security technology ... department security technology ...

■ Einfachste Implementierungsvariante

- nutzt ohnehin vorhandenen Router

■ Probleme:

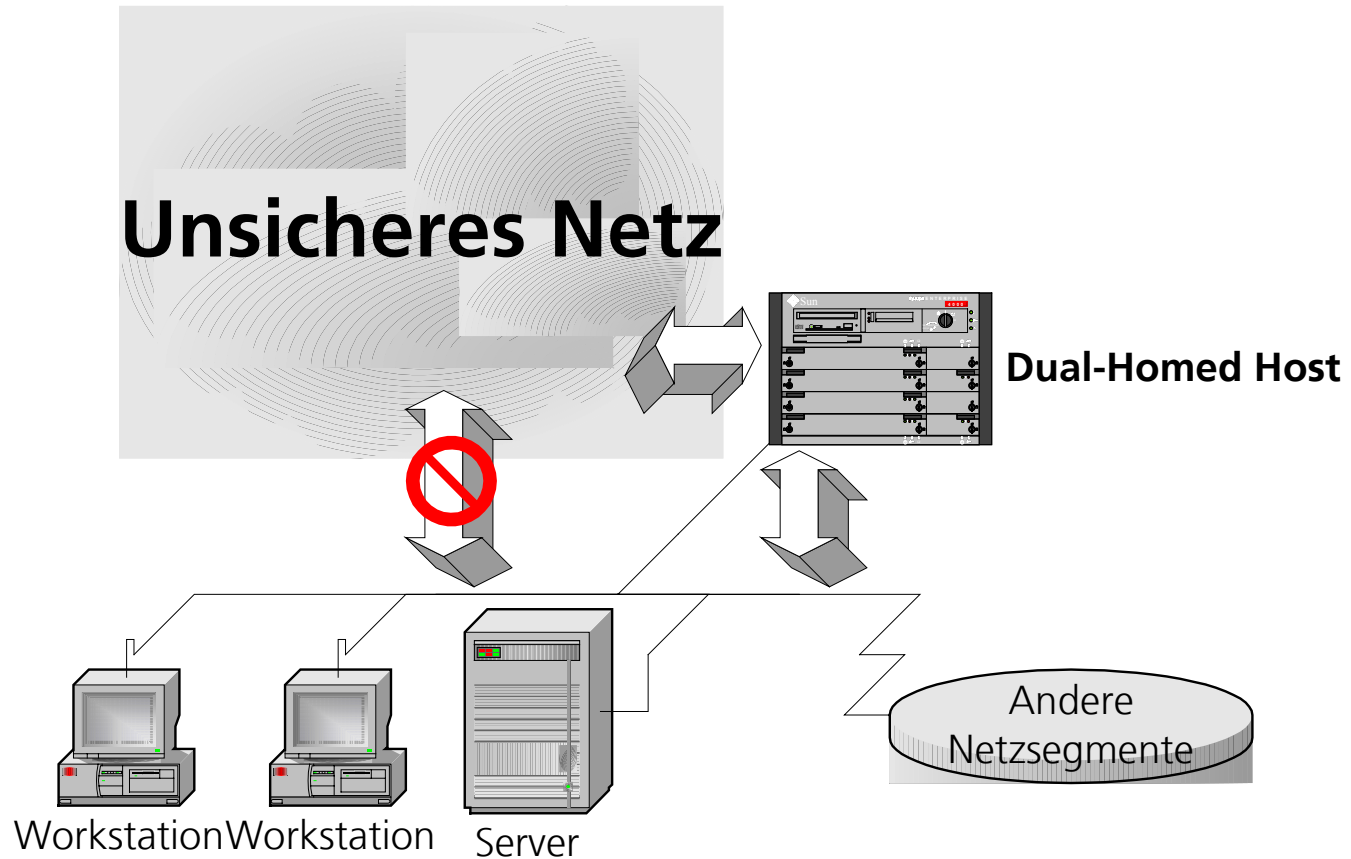
- Rechenleistung des Routers nicht immer ausreichend
- *single point of failure*
 - ▲ Fehlkonfiguration
 - ▲ Implementierungsfehler
 - ▲ Transitive Zugriffsmöglichkeiten durch notwendige Freischaltung von Servern (SMTP etc.)





Dual-Homed Host

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Dual-Homed Host

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

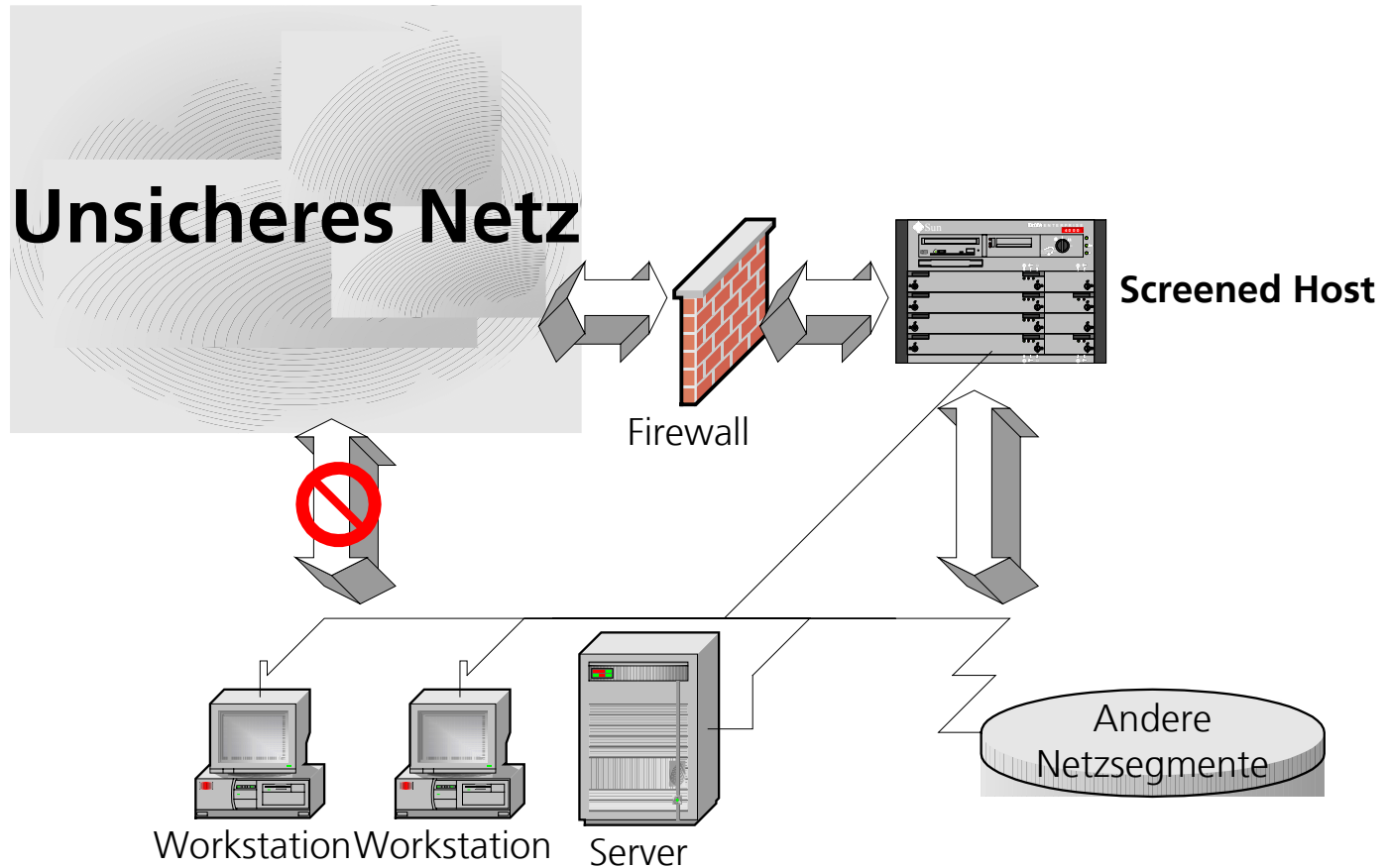
- Kostengünstig, aber auch single point of failure
 - Nutzer externer Dienste müssen Login auf DHH erhalten
 - Remote Login nicht von allen Betriebssystemen unterstützt
 - Zur Nutzung der Dienste erforderliche Anwendungen müssen auf dem DHH installiert sein
 - ▲ Sicherheitslücken durch komplexe Anwendungen
 - Revisionsdaten sind unübersichtlich
 - ▲ Trennung zwischen Verhalten legitimer Nutzer und Anomalien schwierig





Screened Host

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Screened Host

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Kombination aus Screening Router, Dual-Homed Host
 - Zugriff auf internes Netz nur über Bastion Host
 - Verbindungen aus internem Netz nur über Bastion Host

- Risiko der Kompromittierung geringer als bei Dual-Homed Host
 - Dennoch: Single Point of Failure in Form des Bastion Host
 - Datenverkehr zwischen externer Schnittstelle und Bastion Host läuft über internes Netzwerk
 - ▲ Gefahr von Spoofing durch interne Nutzer
 - ▲ Kompromittierte Bastion Hosts eignen sich hervorragend zum Belauschen interner Kommunikation



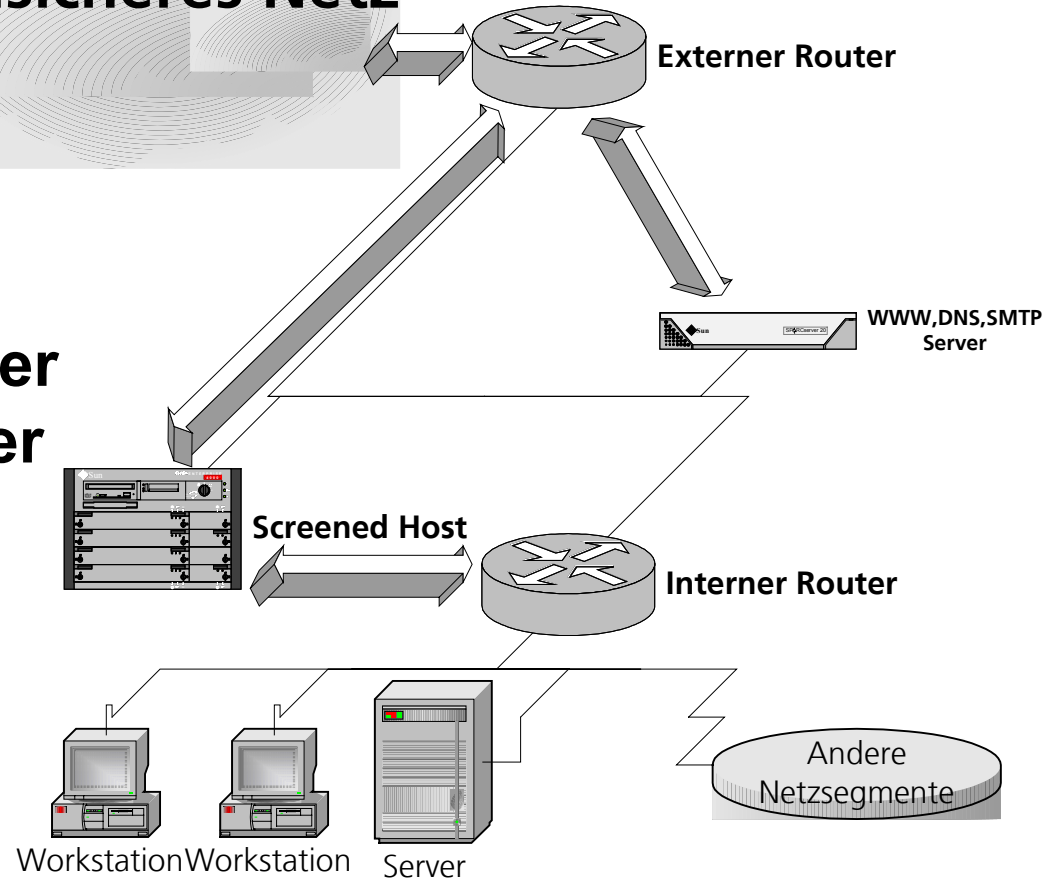


Screened Subnet

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

Unsicheres Netz

**Physikalisch
getrennter interner
und Choke-Router**





Screened Subnet

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Sauberste Implementierung

- Kein Single Point of Failure, Tiefenstaffelung der Verteidigung
- Angriffe auf Bastion Host ermöglicht nicht das Belauschen etc. des internen Datenverkehrs
- Saubere Trennung des Datenverkehrs
 - ▲ Bessere Revisionsdaten, Erkennbarkeit für IDS

■ Ermöglicht Integration von DMZ-Netzwerken

- Netzwerke mittlerer Sicherheitsstufe

■ Beste Lösung: Router unterschiedlicher Hersteller

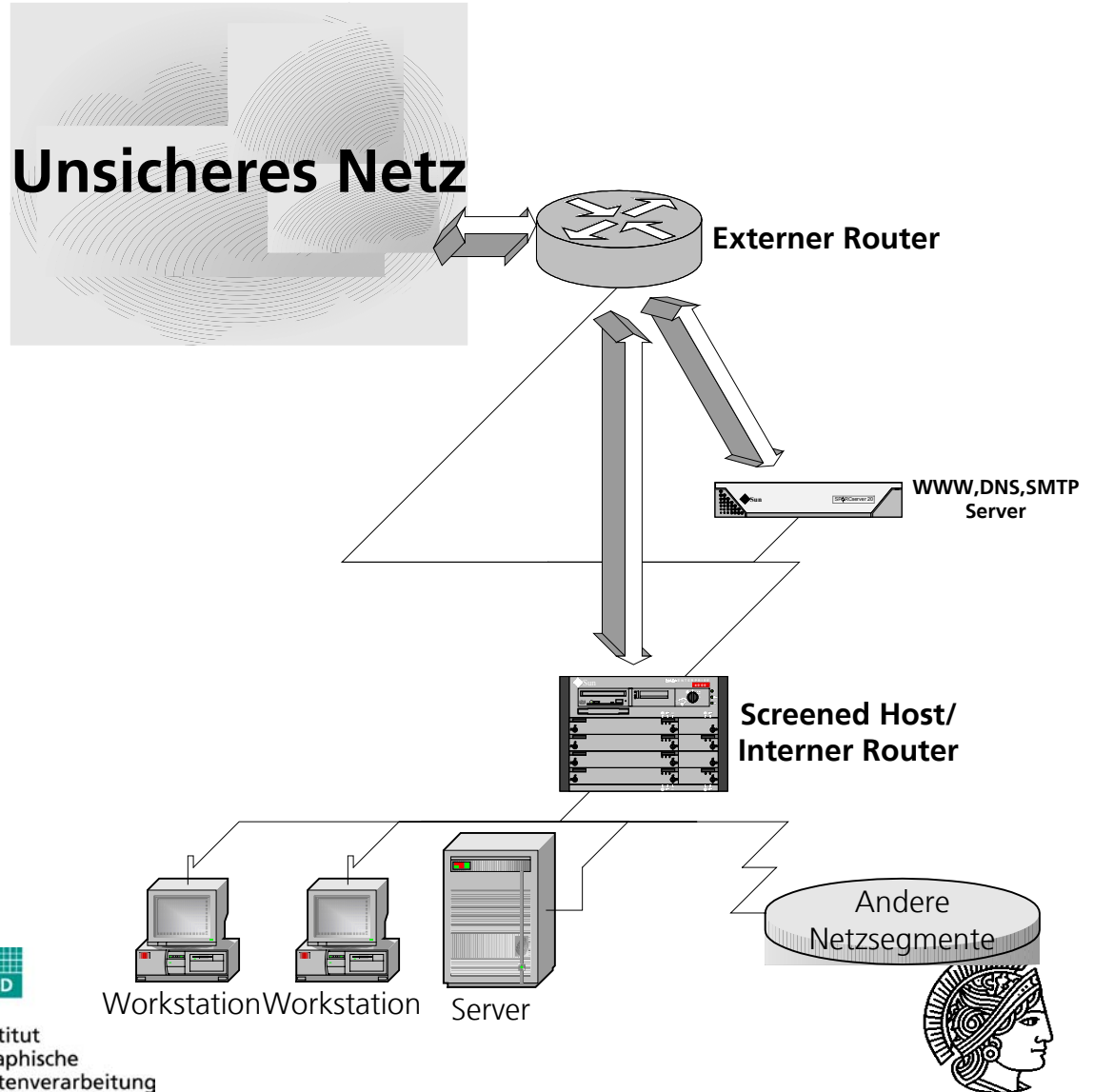




Screened Subnet

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

Konsolidierung des internen Routers mit dem Screened Host





Konsolidiertes Screened Subnet

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Durch Zusammenfassung von Choke Router und internem Router in einem Knoten kann dieselbe Topologie realisiert werden
- Probleme hierbei:
 - Single Point of Failure (Konfigurationsfehler)
 - Erfolgreiche Angriffe auf Router umgehen Bastion Host
- Variante in großen Netzwerken: Mehrere Choke Router
 - Gefahren durch asynchrone Konfiguration: Einheitliche Verwaltung, administrative Verantwortung erforderlich
 - Anderenfalls: Einstufung der Netzwerke unterschiedlicher administrativer Bereiche als „externe“ Netze

