RRZN-Sicherheitstage 2001

Firewalls:
Technik und Lösungen

14.11.2001 Jörg Thiel

Übersicht

- **Einleitung und Begriffe**
- **Netzwerktechnik**
- **Grundlagen Netzwerksicherheit**
- **Firewalltypen**
- **Planung / Konfiguration**
- **Firewallbetrieb**
- **Einschränkungen**

Begriffe

- **Bastion-Host**

  Besonders geschütztes Rechnersystem mit offenem Zugang zum Internet (z.B. WWW - Server)

- **Client**

  Rechner/Software, die eine Verbindung zu einem anderen System aufbaut

- **Dual-Homed-Host**

  Rechner, der mit zwei Netzwerkverbindungen ausgestattet ist

- **Firewall**

  System (aus mehreren Komponenten), das zwischen einem zu schützenden und einem beliebigen Netz liegt

Begriffe

- **Internes Netz**

  Intranetbereich auf der gesicherten Seite der Firewall

- **Paketfilter**

  Einrichtung, die Datenpakete nach bestimmten Regeln prüft und dementsprechend passieren läßt oder zurückweist

- **Proxy-Server**

  Software, die auf der Anwendungsebene bei einem Verbindungsaufbau die Anfrage des Clients entgegennimmt und selbst an den Server weiterleitet

Begriffe

- **Port**

  Zugangspunkt für Netzwerkverbindungen, die zusammen mit den Adressen der Endpunkte eine Verbindung eindeutig beschreiben.

  Die Protokolle TCP/UDP besitzen jeweils 65.535 Ports

- **Server**

  Rechner/Software, die als Informations- oder Dienstquelle im Netzwerk anderen Rechnern zur Verfügung steht.

Warum Firewalls?

- Anzahl der Internetnutzer steigt seit einigen Jahren
  - ⇨ Anzahl der „unfreundlichen“ Nutzer steigt ebenso
  - ⇨ Wertvolle Daten müssen geschützt werden vor:
    - Diebstahl - fremde Nutzung eigener Entwicklungen
    - Ausspähen - z.B. Geschäftsunterlagen
    - Manipulation
- Kontrolle der eigenen Nutzer
  - Onlinekosten
  - Illegale Inhalte
  - Beteiligung an Spionage

Situation Uni Hannover

- Freizügiger Umgang in Instituten und Arbeitsräumen
- Einwahlserver (uni@home)
- Direkter Zugang zum Internet (nur einige Ports geschlossen)
- Kein umfassender zentraler Schutz

  ⇨ Eigenverantwortung bei Instituten

Arbeitsweise

- Firewalls bilden den Übergang zwischen dem Intra- und dem Internet
- Zugangsmöglichkeiten werden verringert
- Firewalls bieten keinen 100%igen Schutz
- Firewalls nutzen die Mechanismen der Netzwerkprotokolle

Internet

Struktur:

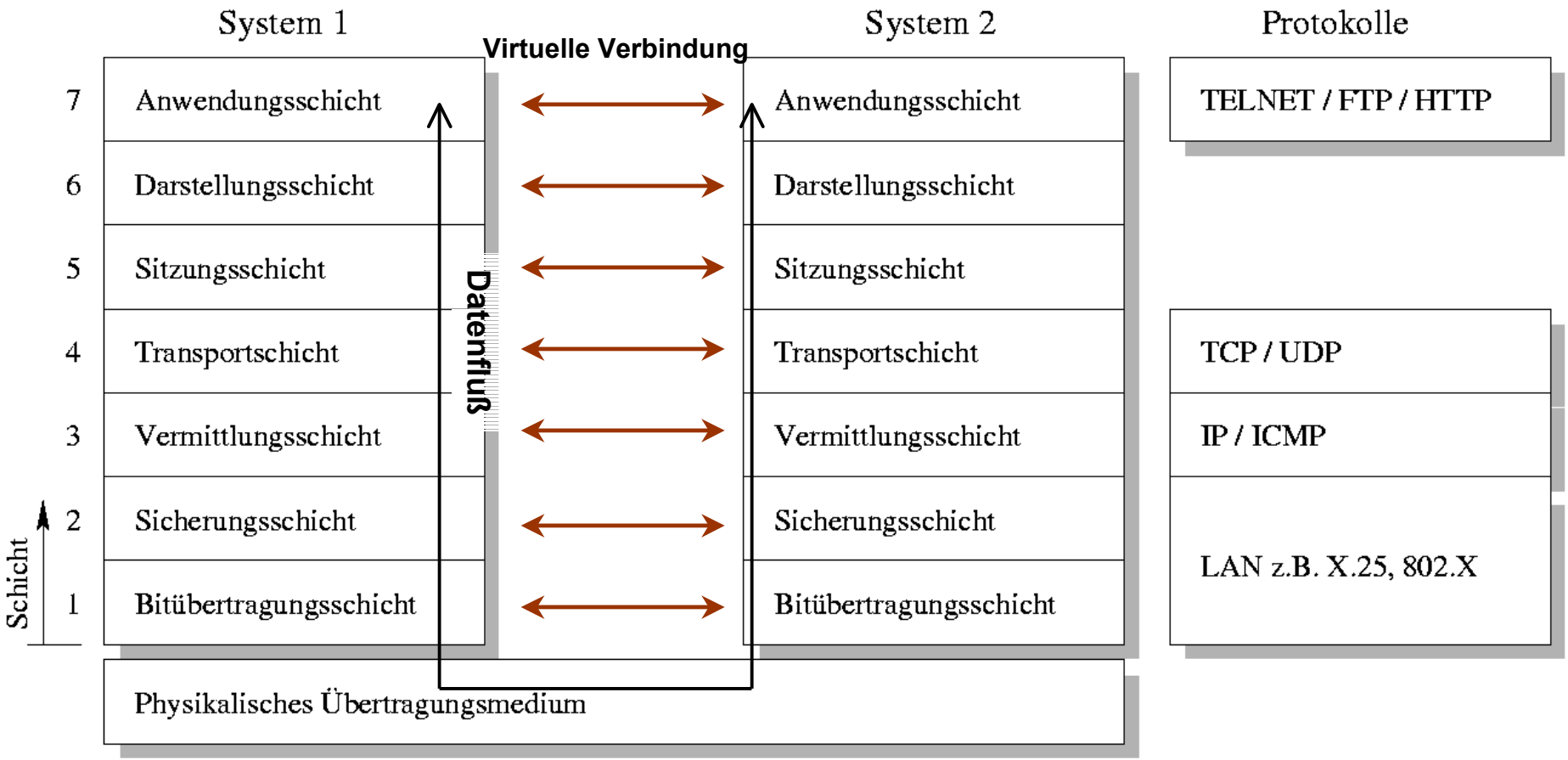
- Zusammenschluß einer Vielzahl autonomer Netze
- Dezentrale Administration
- Weltweite Standards
- Kopplung der Netze über Router und Gateways
- Automatische Wegefindung (militärischer Ursprung)

OSI-Modell

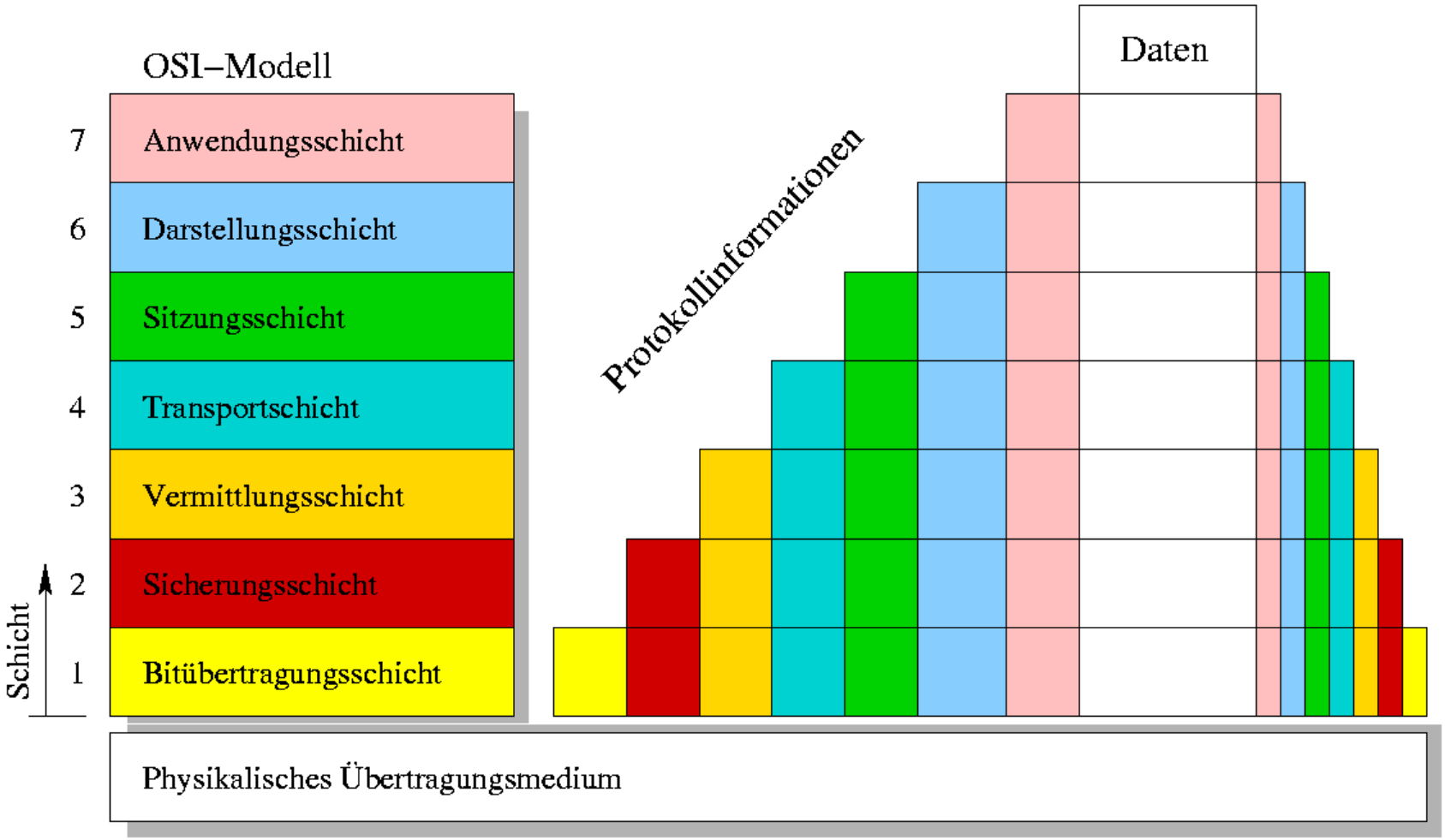
*O*pen *S*ystems *I*nterconnection

- Frühe Rechnernetze waren abgeschlossene Systeme einzelner Hersteller
- „Internet communication“ erfordert offene Schnittstellen zwischen den Netzwerken
- Offene Systeme halten sich an allgemeine Standards und sind somit zueinander kompatibel
- Abstraktes Modell
- Aufteilung der Aufgaben in einzelne Instanzen (Schichten)
- Es kommunizieren nur die gleichen Instanzen zweier Systeme miteinander

OSI-Modell


System 1
Virtuelle Verbindung
System 2
Protokolle
7 Anwendungsschicht
Anwendungsschicht
TELNET / FTP / HTTP
6 Darstellungsschicht
Darstellungsschicht
5 Sitzungsschicht
Sitzungsschicht
Datenfluß
4 Transportschicht
Transportschicht
TCP / UDP
3 Vermittlungsschicht
Vermittlungsschicht
IP / ICMP
2 Sicherungsschicht
Sicherungsschicht
LAN z.B. X.25, 802.X
1 Bitübertragungsschicht
Bitübertragungsschicht
Schicht
Physikalisches Übertragungsmedium

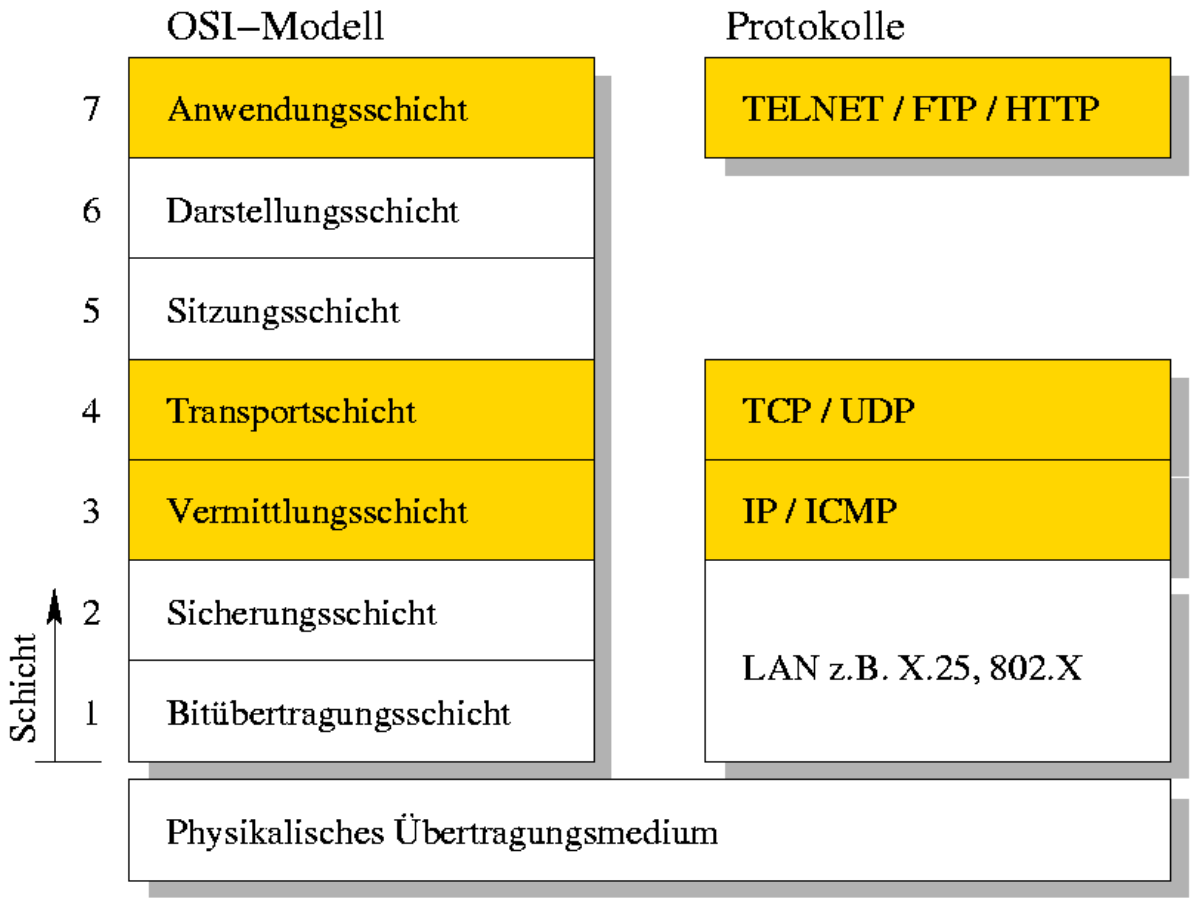
OSI-Modell


OSI–Modell
7 Anwendungsschicht
6 Darstellungsschicht
5 Sitzungsschicht
4 Transportschicht
3 Vermittlungsschicht
2 Sicherungsschicht
1 Bitübertragungsschicht
Schicht
Daten
Protokollinformationen
Physikalisches Übertragungsmedium

OSI-Modell

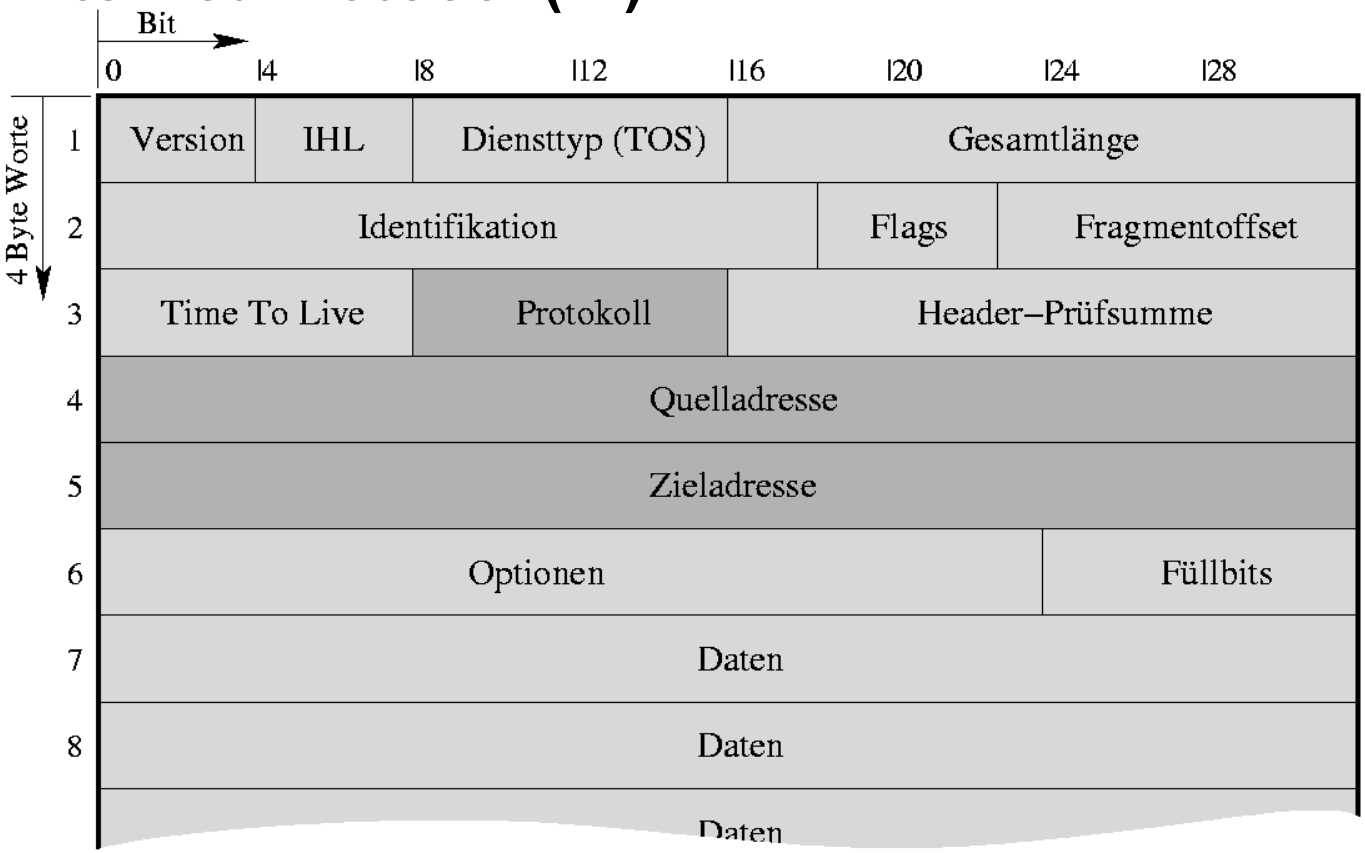
Für die Firewall interessant:

Schichten 3,4 und 7



Protokolle

Das Internet Protocol (IP)



Protokolle

Das Internet Protocol (IP)

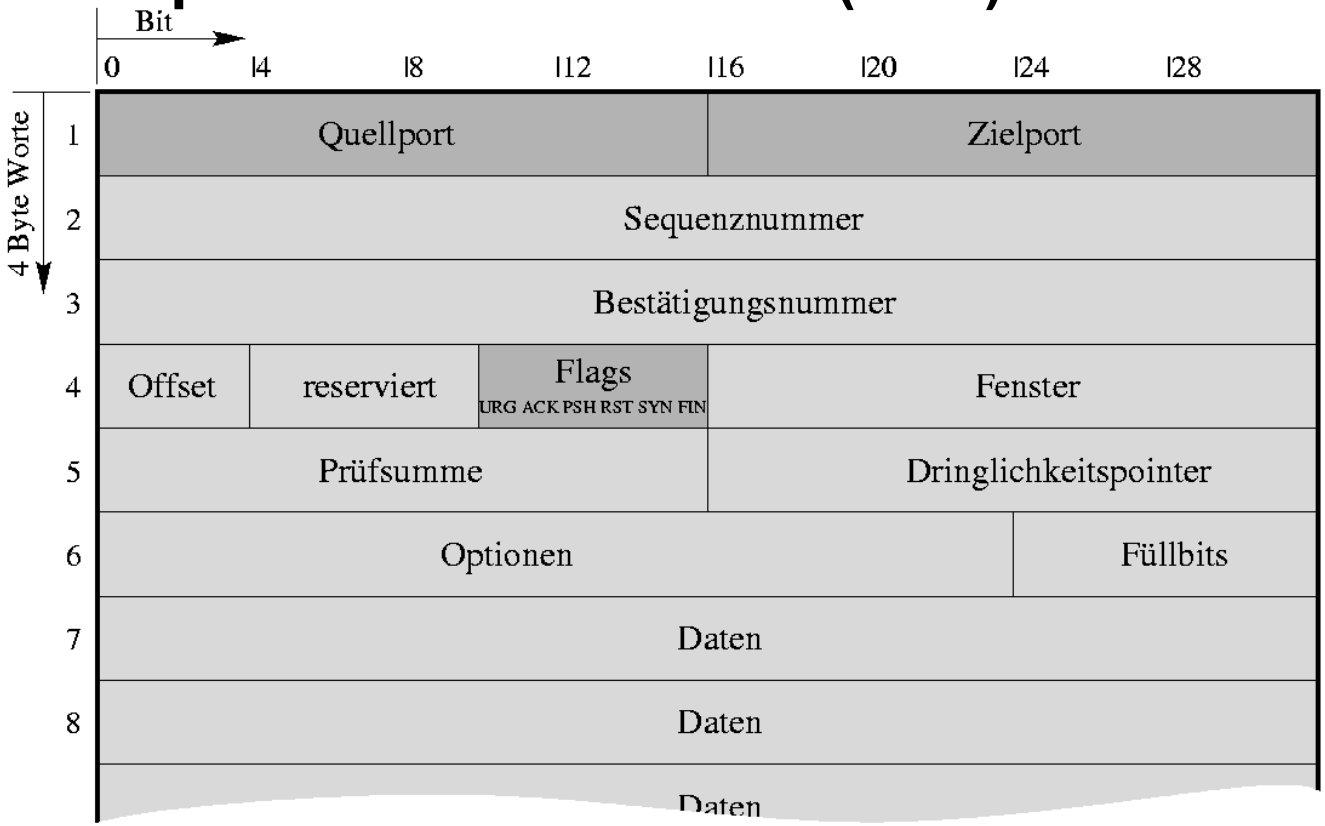
- 32 Bit lange Adressen (z.B. 130.75.1.32)
- Einmalige Vergabe der Adressen im öffentlichen Bereich
- Reservierte Adreßbereiche für die Verwendung in privaten Netzen

⇨ keine Weiterleitung im öffentlichen Netz

- IP unterstützt Fragmentierung großer Datenpakete

Protokolle

Das Transport Control Protocol (TCP)



Protokolle

Das Transport Control Protocol (TCP)

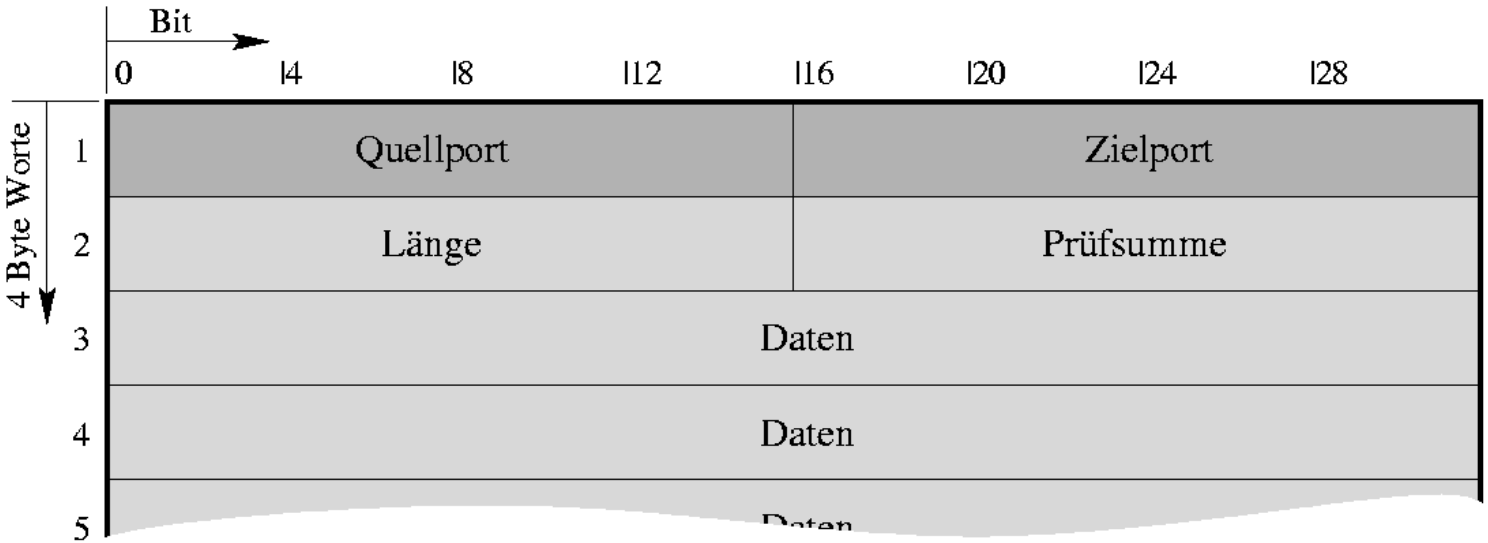
- Verbindungsorientiert

⇨ Verbindungsaufbau, Verbindungsdurchführung und Verbindungsabbau

- Stellt dem Anwender eine virtuelle duplex Ende-zu-Ende-Verbindung zur Verfügung
- Absicherung durch Sequenz- und Quittungsnummern
- Für Anwendungen durch Ports ansprechbar

Protokolle

Das User Datagram Protocol (UDP)



Protokolle

Das User Datagram Protocol (UDP)

- Zugriff auf Anwendungen ebenfalls durch Ports
- Keine feste Verbindung

Sicherheit im lokalen Netzwerk

- **Physikalische Struktur des Netzes**
  - Daten sollten sich nur auf einem absolut notwendigen Bereich des Netzes bewegen
  - Repeater und Hubs verteilen alle Pakete auf allen Segmenten

  ⇨ ein Mitschreiben des Datenverkehrs an einem beliebigen Punkt im Netz ist möglich
  - Switches leiten Pakete nur auf das Zielsegment weiter

  ⇨ auf den anderen Strängen sind die Daten nicht zu erhalten
  - Switches verringern die Netzauslastung (Performancegewinn)

Sicherheit im lokalen Netzwerk

- **Vergabe administrativer Rechte an möglichst wenige Personen**
  - Zentral koordinierte Maßnahmen zur Sicherheit
  - Feste Zuständigkeiten und Verantwortung
- **Kein direkter Zugriff auf wichtige Systeme**
  - Durch Bootdiskette / CD kann jeder administrativen Zugriff erlangen und sich eventuell zum Server „weiterhangeln“
  - Die Firewall sollte nur lokal administrierbar sein und in einem abgeschlossenen Raum stehen

Sicherheit im lokalen Netzwerk

- **Restriktive Konfiguration der lokalen Rechner**
  - Ständige Kontrolle der lokalen Server auf Eindringlinge
  - Auswahl von Software unter Sicherheitsaspekten, besonders auf öffentlich erreichbaren Systemen
  - Lediglich Installation von unbedingt notwendigen Programmen
  - „Alles, was nicht ausdrücklich erlaubt ist (sein muß), wird verboten“

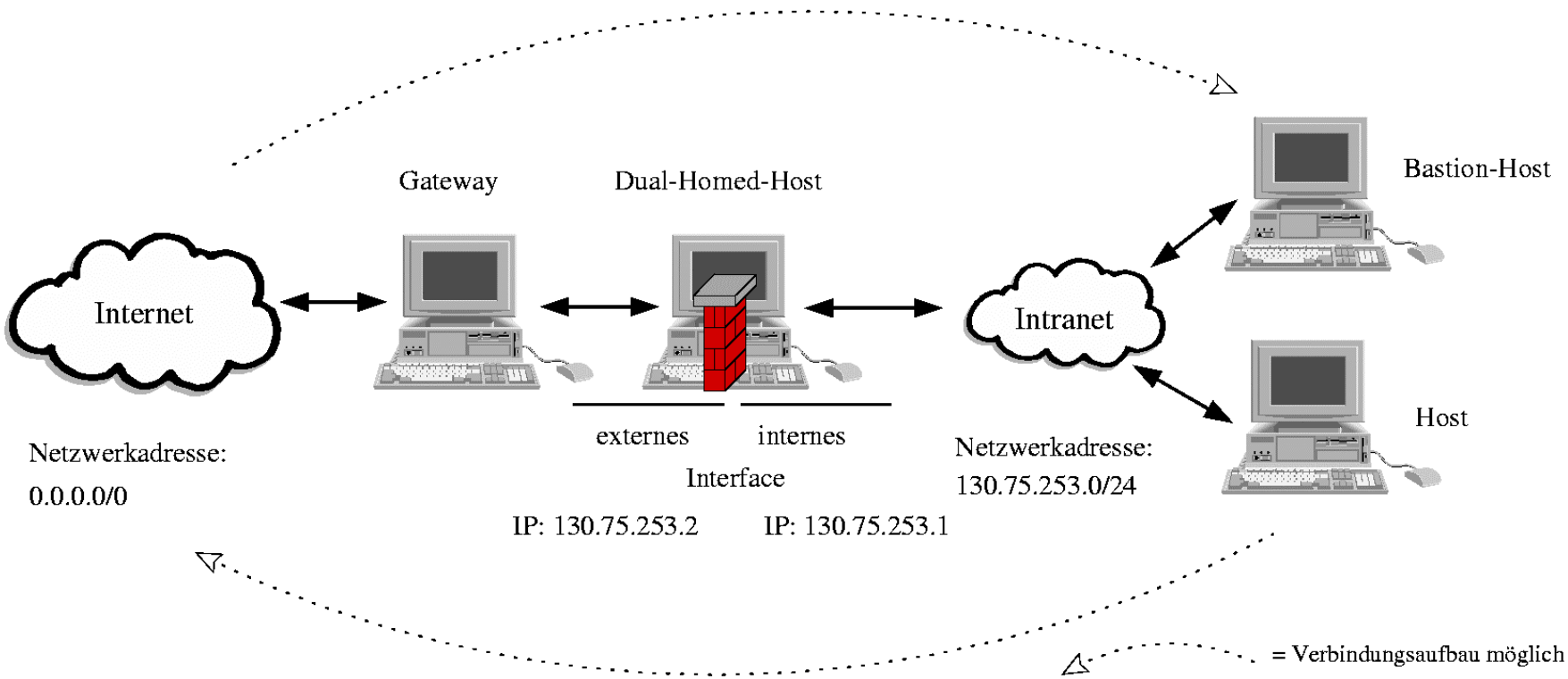
Firewallstrategien

- **Drei grundsätzliche Typen**
  - Paketfilter
  - Paketfilter mit IP-Masquerading
  - Paketfilter mit (transparentem) Proxy-Server

Firewallstrategien

Paketfilter

Arbeitet auf der Transport- und der Vermittlungsschicht



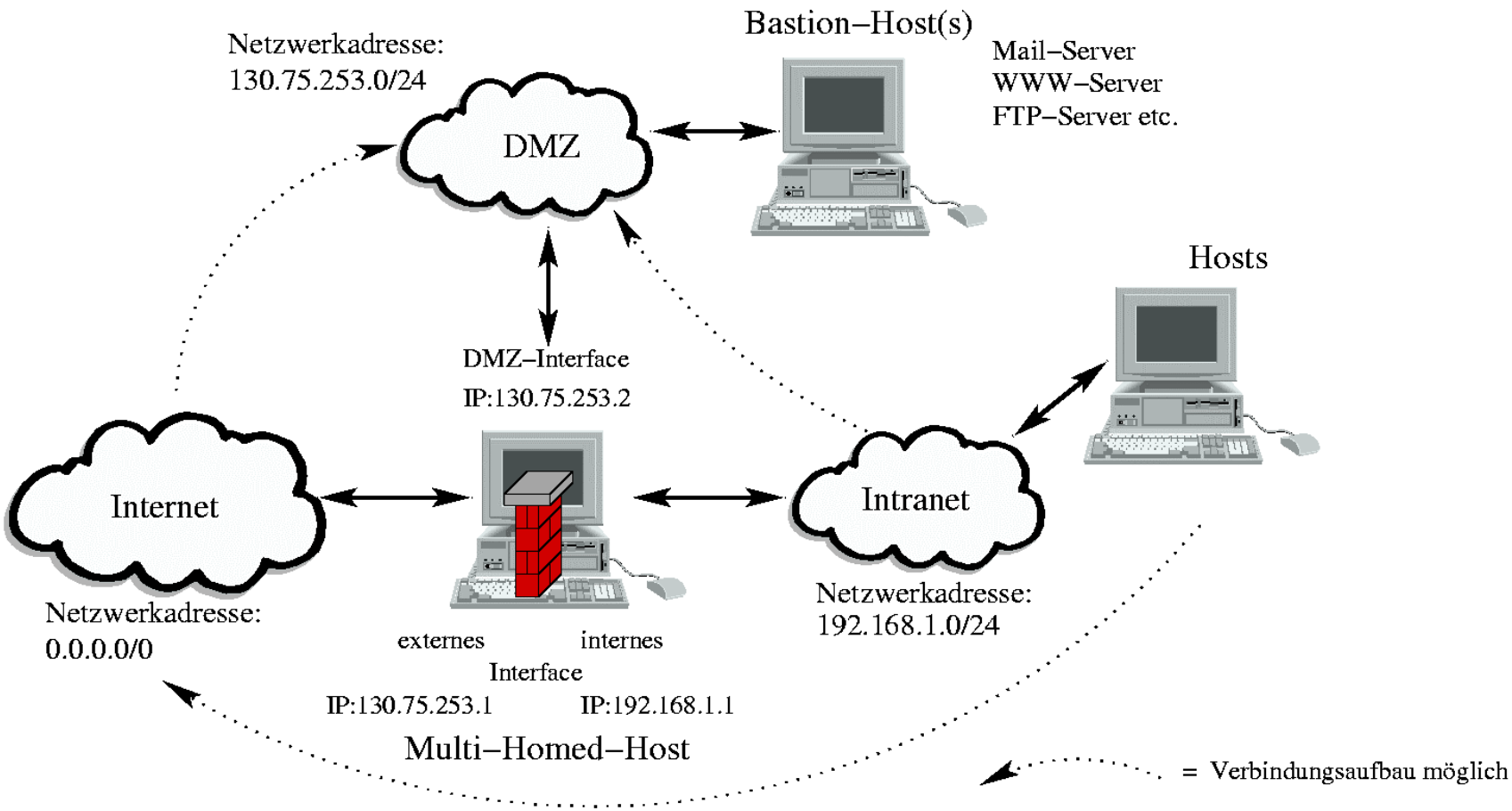
Firewallstrategien

Paketfilter

- Arbeitet auf der Transport- und der Vermittlungsschicht (OSI 3+4)
- Der Paketfilter ist eine Liste von Regeln
- Jede Regel bestimmt ein oder mehrere Prüfkriterien
- Pakete werden geprüft auf:
  - Quelladresse (IP)
  - Zieladresse (IP)
  - Fragmentierung
  - Quellport (TCP/UDP)
  - Zielport (TCP/UDP)
  - Flags (TCP) - Erkennung von Paketen, die zum Verbindungsaufbau dienen
- Abhängig vom Ergebnis der Prüfung wird das Paket weitergeleitet oder verworfen

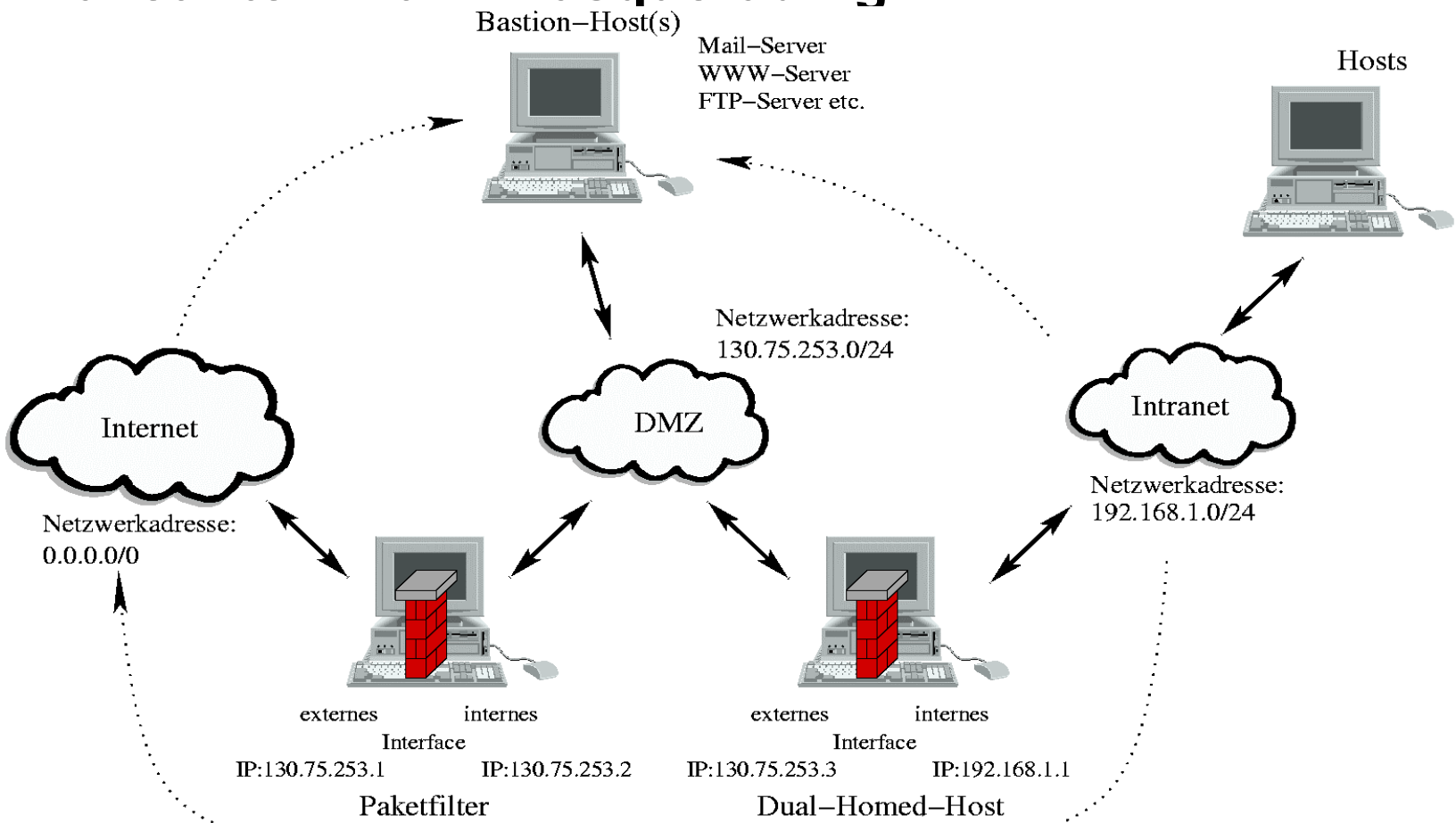
Firewallstrategien

Paketfilter mit IP-Masquerading



Firewallstrategien

Paketfilter mit IP-Masquerading



Firewallstrategien

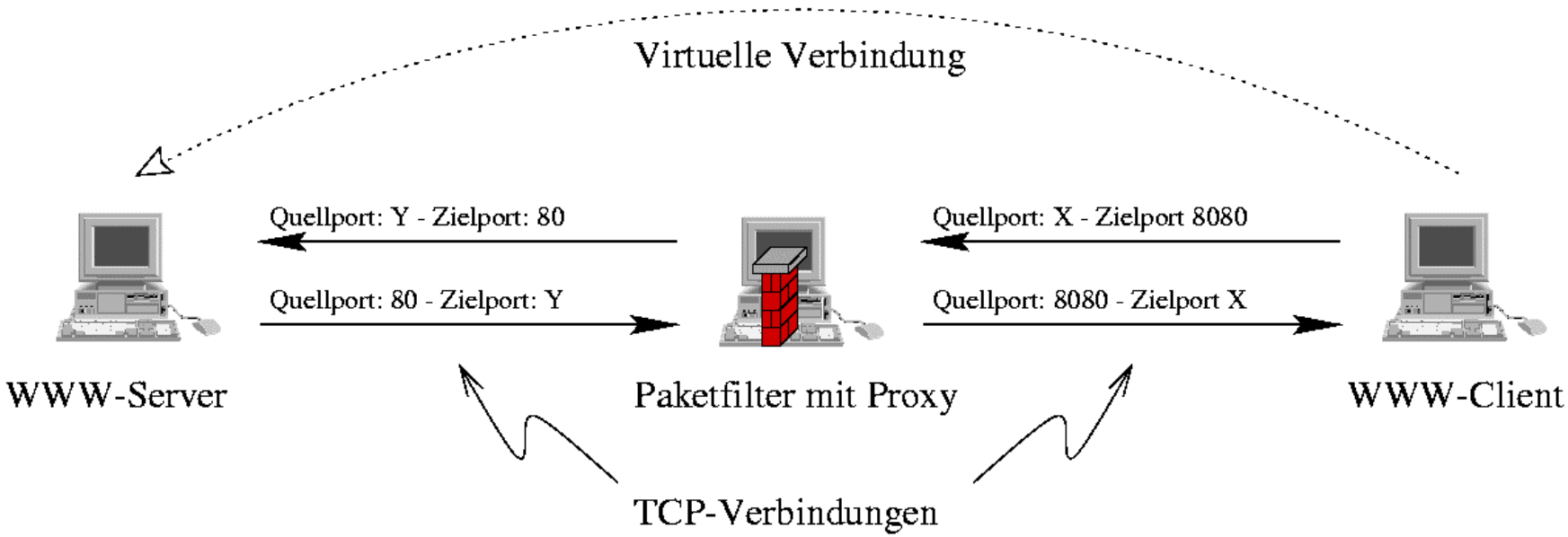
Paketfilter mit IP-Masquerading

- Arbeitet auf der Transport- und der Vermittlungsschicht (OSI 3+4)
- Aufteilung in Intranet, DMZ und Internet
- Öffentlich erreichbare Server werden aus dem Intranet ausgegliedert
- Im Intranet werden IP-Adressen aus dem Bereich der Adressen für private Netzwerke vergeben
- Der Dual-Homed-Host maskiert Pakete aus dem Intranet für das Internet mit seiner eigenen externen IP-Adresse
- Antwort-Pakete aus dem Internet werden vom Dual-Homed-Host demaskiert und an den Client im Intranet weiter geleitet

Firewallstrategien

Paketfilter mit Proxy-Server

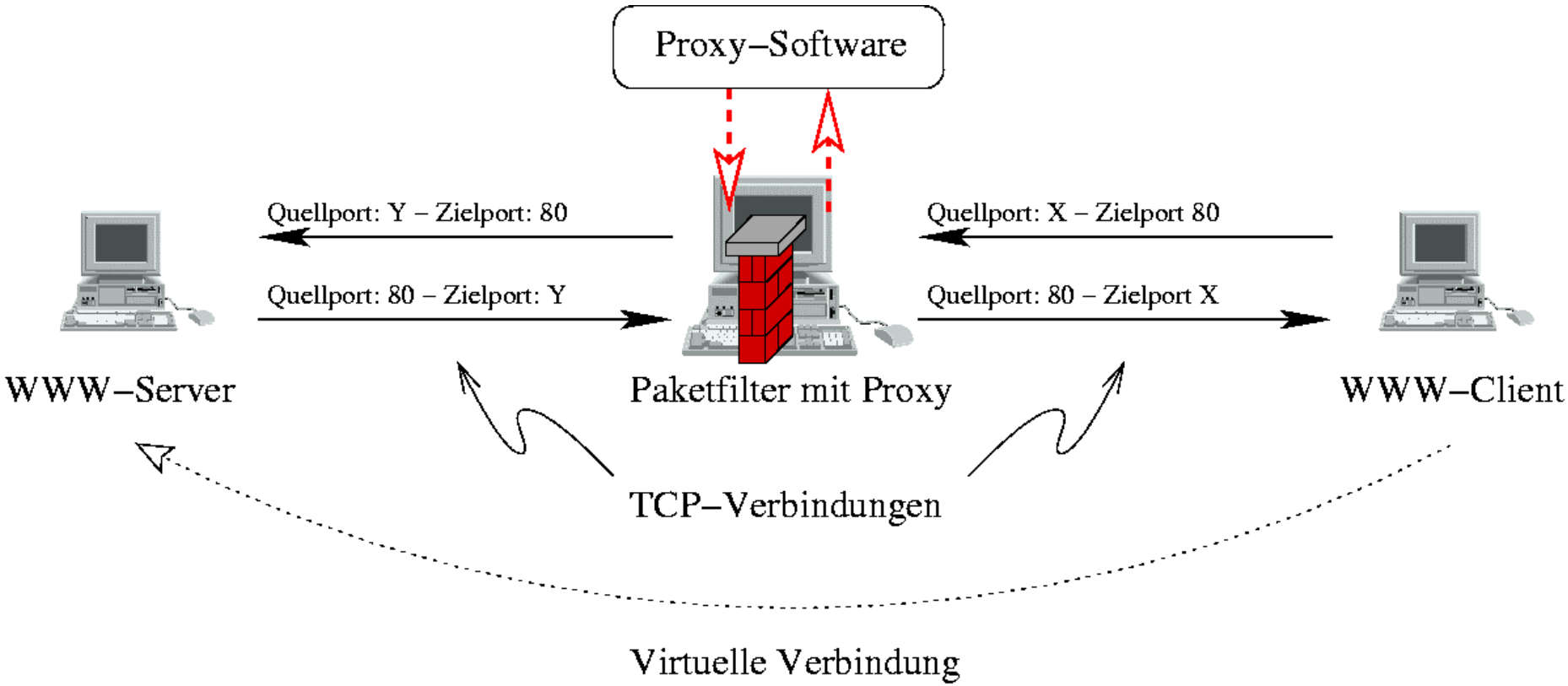
Hier beispielhaft für eine http-Verbindung



Firewallstrategien

Paketfilter mit transparentem Proxy-Server

Hier beispielhaft für eine http-Verbindung



Firewallstrategien

Paketfilter mit Proxy-Server

- Der Proxy-Server ist eine Anwendungs-Software
- Der Proxy-Server arbeitet auf der Anwendungsschicht
- Anfragen an Server im Internet werden nicht direkt vom Client gestellt, sondern vom Proxy-Server
- Der Client kommuniziert nur mit dem Proxy
- Benutzer melden sich beim Proxy-Server an

• Proxy als Application Gateway

- Statt des eigentlichen Servers tritt nur das Application Gateway nach außen in Erscheinung
- Anfragen an den Server richtet nur der vertrauenswürdige Proxy

Firewallstrategien

- **Kombinationen aller Firewalltypen sind möglich**
- **Realisierung in Abhängigkeit der Anforderungen**

- **Vor der Realisierung steht die Planungsphase**

Planung

- **Das RRZN kann keinen umfassenden zentralen Schutz bieten**
  - Die Anforderungen der einzelnen Einrichtungen sind zu unterschiedlich
  - Der Aufbau und die Administration eines Schutzsystems, das allen Anforderungen gerecht wird, kann nicht geleistet werden
  - Eine Firewall gehört zum jeweiligen Netzwerk
- **Probebetrieb mit einem „Cisco Firewall Featureset“**
  - Zur Zeit auf ein Institut beschränkt

Planung

- **Für jedes Netzwerk ist ein eigenes Sicherheitskonzept notwendig**
- **Jeder Betreiber muß sich über seine Bedürfnisse klar sein**

Sicherheitskonzept

- **Erstellen eines Sicherheitskonzeptes**
  - Schritt 1: Aufbau einer Grundlage
  - Schritt 2: Risiko-Analyse
  - Schritt 3: Entwickeln des Sicherheitskonzeptes
  - Schritt 4: Vorstellung/Diskussion des Konzeptes mit den Benutzern
  - Schritt 5: Installation
  - Schritt 6: Wartung

Grundlage des Sicherheitskonzeptes

- **Ernennung von Beauftragten**
  - Die Verantwortung und die Organisation sollte zentral bei wenigen Personen liegen, die diese Aufgabe dauerhaft wahrnehmen.
- **Grundsätzliche Fragen:**
  - Was soll mit dem Sicherheitskonzept erreicht werden?
  - Gegen wen oder was soll abgesichert werden?
  - Was soll Gegenstand des Konzeptes sein?
  - Wer muß seine Zustimmung geben?
  - Wer ist betroffen?

Grundlage des Sicherheitskonzeptes

- **Informationen sind ein wertvolles Gut**
  - Die Integrität,
  - Die Vertraulichkeit
  - Die Verfügbarkeit

  müssen gewährleistet sein.
- **Erkennen von Werten im System**
  - Erstellen einer Liste von Posten, die besonders geschützt werden müssen mit Ort und Besitzer
  - Sicherheitskopien, Ausdrucke und Daten im Fluß über das Netzwerk müssen einbezogen werden

Grundlage des Sicherheitskonzeptes

- **Entwicklung eines Arbeitszieles**
  - Kurze Erklärung des Gesamtzieles
  - Hilfreich, wenn man noch am Anfang des Konzeptes steht
  - Liste der Verantwortlichkeiten aller am Projekt beteiligten Personen und Organisationen
- **Kosten - Nutzen - Rechnung**
- **Rückendeckung durch Institutsleitung**
- **Zeit, Ruhe, gute Einfälle**

Risikoanalyse

- **Untersuchung aller Risiken**
- **Mögliche Risiken:**
  - Unerlaubter Zugriff auf Rechner
  - Ausspähen sensibler Daten
  - Datenverlust
  - Beschädigung von Daten
- **Quelle der Gefahren liegt nicht nur im Internet**
- **Reihung aller Risiken nach Dringlichkeit**
  - Entsprechend der Dringlichkeit sollte später der Schutzaufwand angemessen sein

Entwicklung des Sicherheitskonzeptes

- **Das Sicherheitskonzept soll die erkannten Risiken minimieren**
- **Struktur des Konzeptes:**

  Zerlegung in
  - Konzepte - Antworten auf die Frage: „Was?“
  - Normen - Antworten auf die Frage: „Wie?“
  - Verfahren - Antworten auf die Frage: „Wie, genau....?“

Entwicklung des Sicherheitskonzeptes

- **Beispiele für festzulegende Normen:**
  - Klassifizierung der Daten
  - Zugriffskontrolle
  - Netzwerkdienste
  - Virus-Schutz
  - Datensicherung
  - Notfallprozeduren
  - Paßwortschutz
- **Festlegen von möglichen Ausnahmen**

Beteiligung der Benutzer

- **Jedes Sicherheitskonzept ist ohne die Unterstützung durch die Benutzer zum Scheitern verurteilt**
  - Die Benutzer sollten über das Konzept und seinen Sinn informiert werden
  - Anregungen sollten - sofern möglich - integriert werden
  - Die Benutzer müssen wissen, woran sie Fehlfunktionen z.B. durch einen Einbruch erkennen können
  - Jeder ist für die Datensicherheit verantwortlich

Installation

- **In Abhängigkeit der Ergebnisse der bisherigen Schritte erfolgt die Installation**
- **Überlegungen zur Installation:**
  - Soll das gesamte Netzwerk auf einmal umgestellt werden, oder ist eine schrittweise Umstellung möglich / nötig?
  - Welche konkreten Produkte werden für die Installation verwendet?
  - Wie wird das Sicherheitskonzept auf diese Produkte übertragen?
- **Festlegen von Notfallverfahren**
  - Die Verfahren sollten feststehen, bevor sie das erste Mal benötigt werden
  - Durch Probeangriffe lassen sich Verfahren testen

Installation

- **Dokumentation:**
  - Die Installation muß für Unbeteiligte nachvollziehbar dokumentiert werden, falls die Verantwortlichen wechseln.
  - Sollte es zu einem Vorfall kommen, muß dieser genau dokumentiert werden, um Erfahrungen zu sammeln
- **Das gesamte Sicherheitssystem muß ständig überwacht werden**

Wartung

- **Das Sicherheitskonzept muß bei jeder gravierenden Änderung im Netzwerk überarbeitet werden**
- **Veröffentlichungen über Probleme mit den verwendeten Produkten verfolgen**
- **Log-Dateien der Sicherheitssysteme ständig prüfen**

Planung der Firewall

- **Aus dem Sicherheitskonzept ergeben sich die Anforderungen an die Firewall**
  - Die im Konzept entwickelten Anforderungen müssen in Regeln für die Firewall umgesetzt werden
  - An der Qualität der Umsetzung hängt die Funktionsfähigkeit des gesamten Aufbaus
  - Die Auswahl der Software erfolgt auf Grundlage der Anforderungen durch das Konzept und die Vorliebe der Anwender
- **Die Anforderungen können sehr vielfältig sein**

  ⇨ **Es gibt kein Patentrezept**

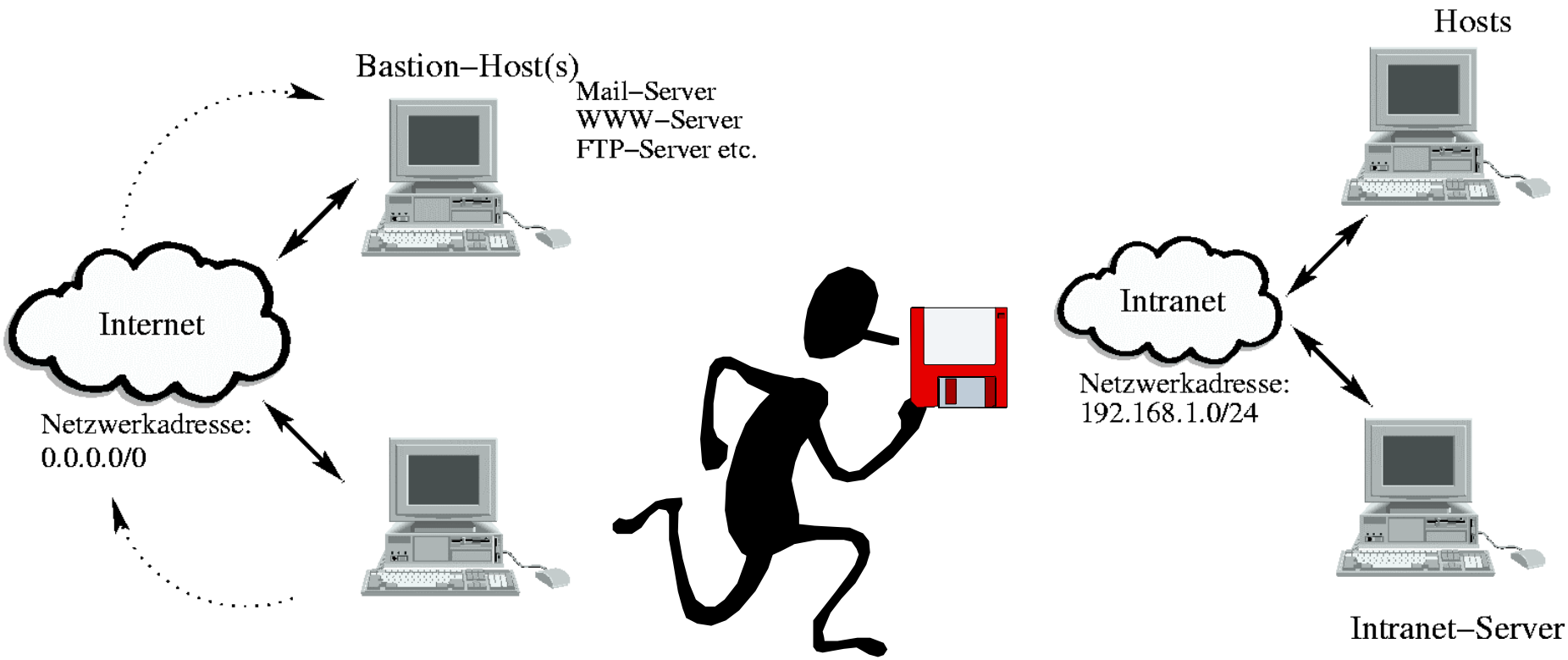
Planung der Firewall

- **Sicherste Lösung:**

Planung der Firewall

- **Sicherste Lösung:**
  - Trennung von Intra- und Internet
  - Einzelne Rechner stehen zur Recherche im Internet zur Verfügung
  - Das eigene Netzwerk mit dem Server für wertvolle Daten steht nur für die interne Arbeit zur Verfügung
  - Daten/Informationen, die aus dem Internet stammen und in eigene Produkte einfließen sollen, müssen „per Hand“ transportiert werden

Sicherste Lösung



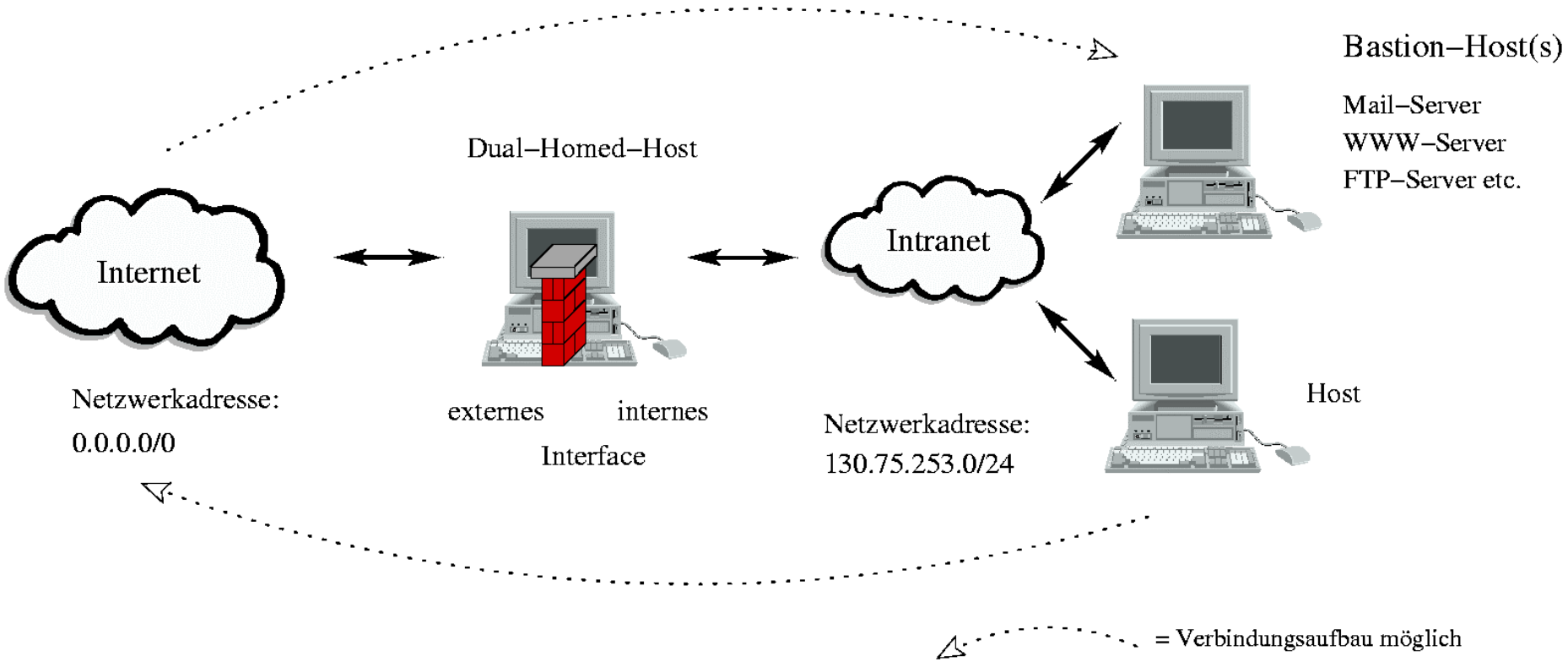
Sicherste Lösung

- **Vorteile:**
  - Kein Einbruch in den lokalen Server möglich
- **Nachteile:**
  - Das Einbinden von Daten aus dem Internet ist sehr umständlich
  - Recherche und Produktion verlangen zwei Rechner
  - nicht sehr zeitgemäß (oder noch nicht wieder?)

Beispielaufbau 1

- **Konzept:**
  - Recherche im Internet soll möglich sein
  - Einige Dienste stehen für die Außenwelt zur Verfügung
  - Die öffentlichen Server enthalten keine sicherheitsrelevanten Informationen
  - Die Struktur der Firewall soll einfach sein
  - Die Firewall soll einfach in ein vorhandenes Netzwerk integriert werden können
  - Es gibt keine sehr hohen Anforderungen an die Sicherheit

Beispielaufbau 1



Beispielaufbau 1

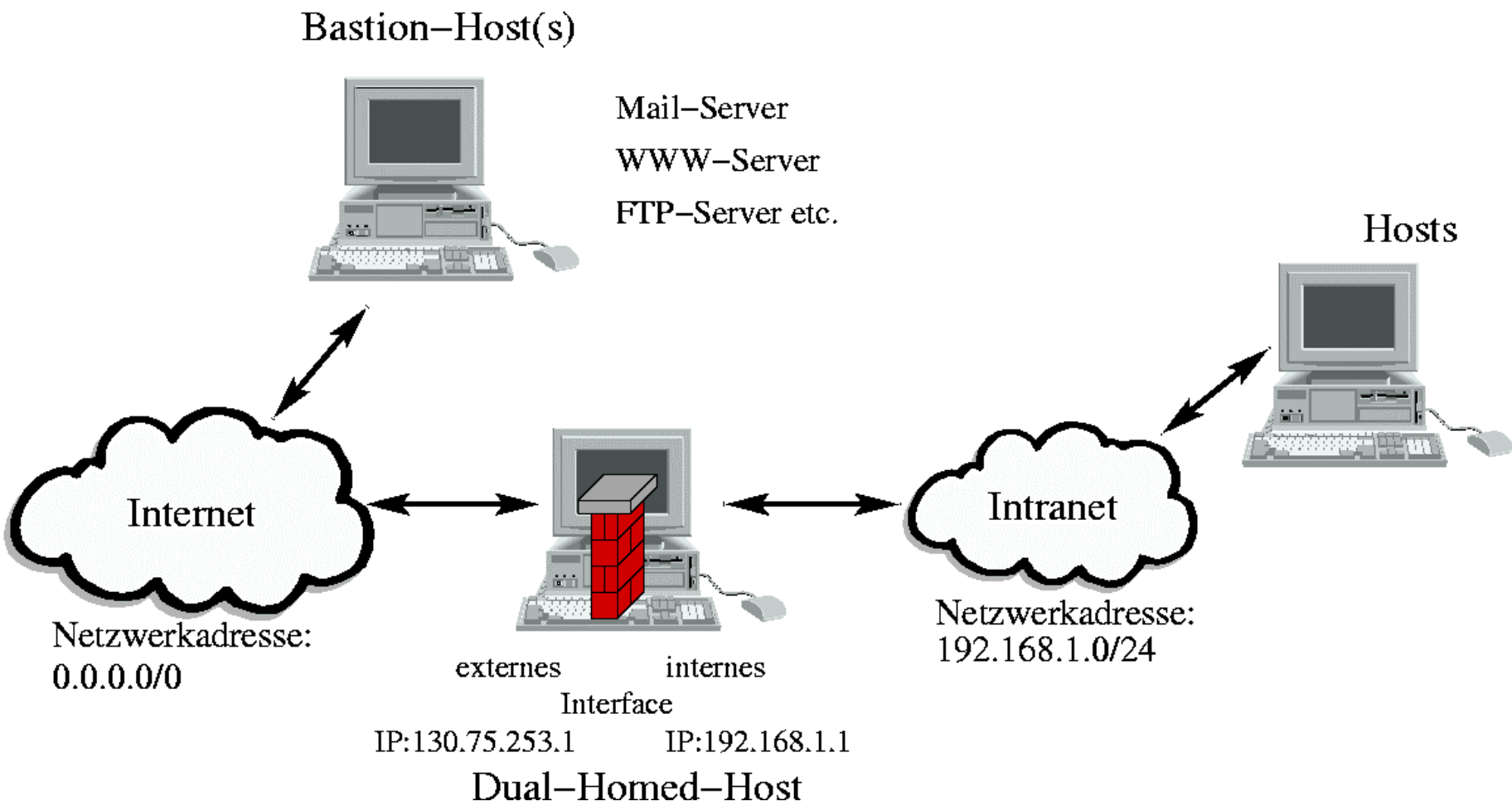
- **Vorteile:**
  - Informationen können im Internet veröffentlicht werden
  - Aus dem Intranet können Informationen im Internet abgerufen werden
  - Einfache Struktur
  - Keine Neukonfiguration im Intranet notwendig
  - Geringe Hardware-Anforderungen
- **Nachteile**
  - Es finden Zugriffe auf die Bastion-Hosts im Intranet statt
  - Die Rechner im Intranet sind adressierbar

  ⇨ ständige Überwachung und Wartung notwendig

Beispielaufbau 2

- **Konzept:**
  - Das Intranet soll dem Internet verborgen werden
  - Recherche im Internet soll möglich sein
  - Informationen sollen veröffentlicht werden, ansonsten stehen keine Dienste für die Außenwelt zur Verfügung
  - Die öffentlichen Server enthalten keine sicherheitsrelevanten Informationen
  - Die Struktur der Firewall soll einfach sein

Beispielaufbau 2



Beispielaufbau 2

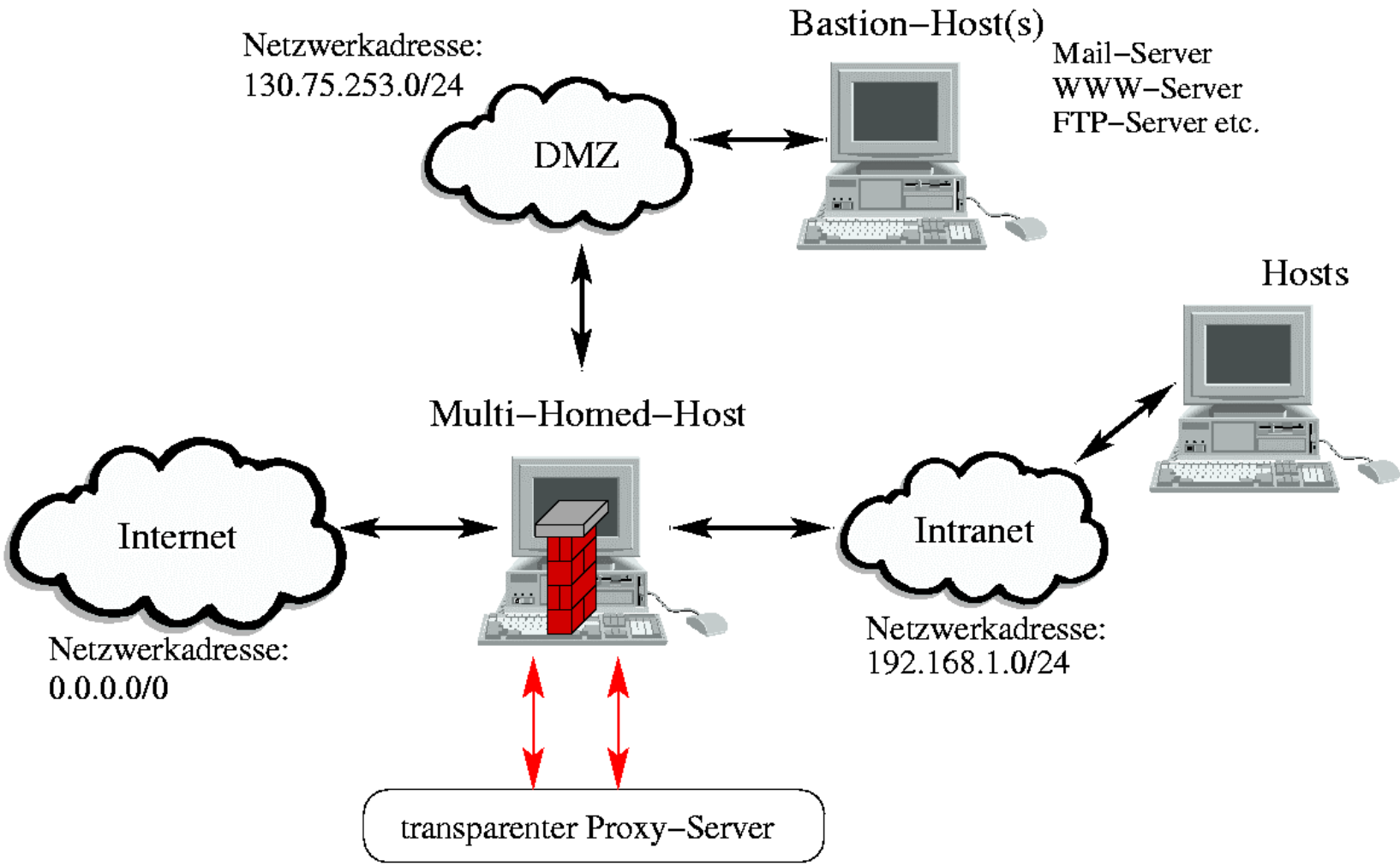
- **Vorteile:**
  - Informationen können im Internet veröffentlicht werden
  - Das eigene Netzwerk bleibt verborgen
  - Aus dem Intranet können Informationen im Internet abgerufen werden
  - Relativ einfache Struktur
- **Nachteile**
  - Neukonfiguration des Intranet erforderlich
  - Keine „Heimarbeit“ über den Einwahlserver möglich
  - Die eigenen öffentlichen Server stehen ungeschützt im Netz

  ⇨ ständige Überwachung und Wartung notwendig

Beispielaufbau 3

- **Konzept:**
  - Informationen sollen im Internet veröffentlicht werden
  - Vom Intranet sollen so wenig Informationen wie möglich preisgegeben werden
  - Der Zugriff auf das Internet soll kontrollierbar sein
  - Der Datenfluß zum Internet soll auf ein Minimum beschränkt werden
  - Eine generelle Neustrukturierung des Netzwerkes ist möglich

Beispielaufbau 3



Beispielaufbau 3

- **Vorteile:**
  - Informationen können im Internet veröffentlicht werden
  - Das eigene Netzwerk bleibt verborgen
  - Aus dem Intranet können Informationen im Internet abgerufen werden
  - Proxy-Server vermeidet überflüssigen Datenverkehr
  - Internetzugriffe lassen sich Benutzern zuordnen
- **Nachteile**
  - Neukonfiguration des Intranet erforderlich
  - Keine „Heimarbeit“ über den Einwahlserver möglich
  - Auf dem Dual-Homed-Host muß ein sehr aufwendiges System installiert, konfiguriert und überwacht werden.
  - Hohe Hardwareanforderungen an den Firewall-Rechner

Zusätzliche Maßnahmen

- **Absicherung der Bastion-Hosts**
  - Minimale Installationen
  - Sichere Betriebssysteme
  - Sichere Serversoftware
  - Keine sicherheitsrelevanten Daten

- **Auslagern von Diensten an externe Anbieter**
  - Kann der WWW-Auftritt extern realisiert werden?
  - Ist es möglich, über einen Free-Mail-Service den E-Mail-Verkehr abzuwickeln?

Weg zur Umsetzung

- **Nach Festlegen der Anforderungen:**
  - Auswahl der Hardware
    - Preis
    - Zuverlässigkeit
  - Auswahl der Software
    - Betriebsystem
      - Vorlieben
      - Kosten
    - Firewalltyp

  ⇨ Firewallprodukt

Firewallprodukte

- **WindowsNT/AIX**

  IBM SecureWay Firewall

  – Paketfilter
  – Proxy-Server
  – Circuit-Gateway
  – ... und mehr
  – Preis???

Firewallprodukte

- **WindowsNT/2000/Solaris7/8/RedHat Linux 6.2/7.0**
  - Checkpoint: Firewall-1
  - Paketfilter
  - Proxy-Server
  - Benutzerauthentifizierung
  - Modularer Aufbau
  - Sehr genaue Auswahl von zugelassenen Dokumenten möglich
  - Preis ??? (viel)

Firewallprodukte

- **Linux**
  - MASON
    - interaktiver Aufbau der Regeln für Linux Paketfilter
    - GNU
  - SINUS Firewall
    - grafische Oberfläche zur Konfiguration der Paketfilter
    - GNU
  - TIS Firewall Toolkit
    - Erstellen von Sicherheitsregeln
    - Proxy-Server für ftp, telnet
    - kostenlos für nicht kommerzielle Verwendung

Probleme

- **Jede Firewall hat Einschränkungen zur Folge**
  - Paktefilter und Proxys verursachen Verzögerungen
  - ⇨ Probleme mit zeitkritischen Anwendungen
  - Manche Dienste bauen rückwärtige Verbindungen auf
  - ⇨ Bei Verwendung von IP-Masquerading nicht möglich
  - Multicast-Pakete lassen sich nur mit Tricks weiterleiten
- **Der Firewallrechner wird zum Flaschenhals**
  - Beim Ausfall des Rechners wird die Verbindung vollständig unterbrochen
  - Komplexe Regelstrukturen können die Hardware überfordern

Einschränkungen

- **Eine Firewall schützt nicht vor:**
  - Viren (nur bedingt, da diese auf dem Wirt erkannt werden müssen)
  - Unvorsichtigen Benutzern
  - Überlastung der externen Netzwerkanbindung (auch, wenn sie durch Attacken verursacht wird)
  - Internen Angriffen

Zusammenfassung

- **Eine Firewall kann das Intranet schützen, wenn**
  - ein durchdachtes Gesamtkonzept vorliegt
  - konsequent nach Sicherheitsmaßstäben gehandelt wird
  - sie aufmerksam administriert wird
  - Einschränkungen in Kauf genommen werden

- **Eine Firewall funktioniert nicht von allein**

Literatur

- www.tis.com - Firewall-Toolkit für Linux und BSD
- www.checkpoint.com - kommerzielles Produkt
- www.fli4l.de - Projekt zur Firewall auf der Diskette
- www.rvs.uni-hannover.de - Arbeiten zur Netzwerksicherheit mit Bezug zur Uni Hannover
- www.sun.com - SunScreen Firewall, Firewall produkt der Firma Sun

- Norbert Pohlmann, Firewall-Systeme, MITP-Verlag, Bonn
- Chapman/Zwicky, Einrichten von Internert Firewalls, O‘Reilly/International Thomson Verlag, Bonn
- Helmut Kerner, Rechnernetze nach OSI, Addision-Wesley, Bonn