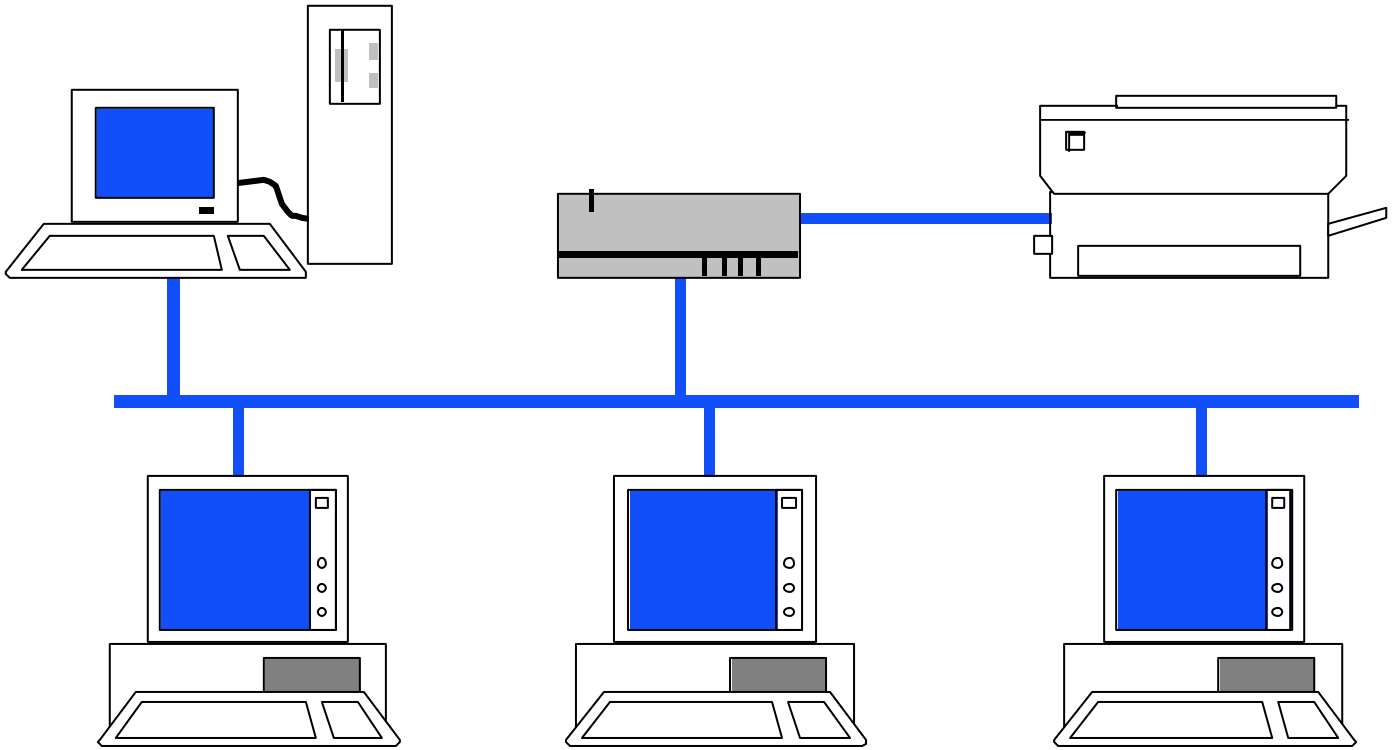
Datenschutz und Datensicherheit

Mag. Dr. Klaus Coufal



I. Übersicht

- Themenübersicht
  - Datenschutz
  - Datensicherheit

I.1. Datenschutz

- Einführung und Begriffe
- Zutritts- und Zugriffsschutz
- Verschlüsselungsverfahren
- Authentizitätsprüfung und Schlüsselverteilung
- Einbindung der Sicherheitsmechanismen in ein Netzwerkreferenzmodell
- Normen
- Realisierung einer Datenschutzeinrichtung

I.2. Datensicherheit

- Einführung und Begriffe
- Störprogramme
- Netzwerkbackupstrategien
- redundante Speicherformen
- Ausfallssicherheit
- Planen einer Vorsorgestrategie
- Erstellen eines Katastrophenhandbuches
- Desaster Recovery

I.3. Datenschutzgesetz

- Gesetz, das die Schutzwürdigkeit der Daten und die Folgen des Missbrauches beschreibt.
- Nicht mit welchen technischen und organisatorischen Maßnahmen dies erfolgt.

I.4. Datenschutz – Einteilung

- Zutrittsschutz
  - Schutz der Systeme vor unbefugten Personen
- Zugriffsschutz
  - Schutz der Daten vor unberechtigtem Zugriff
- Datensicherheit
  - Schutz vor Verlust

Einteilung nach Notwendigkeit

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Authentizität

II. Grundlagen

- Zutrittsschutz
- Zuverlässigkeit
- Zugriffsschutz
- Verschlüsselung

II.1. Zutrittsschutz

- Schutz vor innen (vor Ort)
  - Zutrittsschutzsysteme
  - ca. 80% der Angriffe kommen von innen
- Schutz vor außen (Internet, ...)
  - Firewall
  - nur ca. 20% der Angriffe kommen von außen

Zutrittsschutz

- Verhinderung des physikalischen Zuganges (z.B.: Mauer mit versperrter Tür), damit unbefugte Personen nicht an Systeme herankommen
- Probleme:
  - Zentralschlüssel
  - Reinigungspersonal
  - Notfall

Zutrittsschutz

- Softwarebasierender Zutrittsschutz
  - Accountname/Passwort bzw. PIN
  - Schlüsselverfahren
  - Biometrische Verfahren

Account – Beschreibung

- Ein Account besteht aus einem Benutzernamen und einem Passwort bzw. einem PIN, wobei aber der zweite Parameter auch leer sein kann
- Schwacher Zutrittsschutz, da eine Reihe von Problemen existieren
- Weitverbreitet

Account – Vorteile

- Einfach zu realisierendes System
- Lange vorhanden, daher viele Erfahrungen mit den Parametern
- Geringe Kosten
- Einfach Änderbar
- Viele weitere Systemparameter können an einen Account gebunden werden

Account – Nachteile

- Passwortweitergabe
- Vergessenes Passwort
- Passwörter werden notiert (Post-It)
- Einfache und damit unsichere Passwörter
- Passwörter werden ausspioniert
- ...

Schlüssel

- Schlüsselkarte
  - Magnetstreifen
  - Speicherkarte
  - Chipkarte
- Zertifikat
- Elektronische Signatur

Zuverlässigkeit Passwort/Schlüssel

- Berechtigte Personen werden i.a. korrekt akzeptiert
- Unberechtigte werden i.a. korrekt abgewiesen
- Große organisatorische Probleme bei Verlust
- Große Probleme mit Benutzern

Biometrische Verfahren

- Fingerabdruck
- Irisscan
- Gesichtserkennung
- Stimmerkennung
- Unterschriftserkennung
- Tipprhythmus
- ...

Fingerabdruck

- Weit fortgeschritten
- Leicht fälschbar
- Hygieneprobleme bei zentralen (= nicht persönlichen) Zugangspunkten
- Kostengünstig

Irisscan

- Akzeptanzprobleme auf Seiten der Benutzer
- Noch kostenaufwendig
- Fälschung aufwendig

Gesichtserkennung

- Statische Varianten leicht fälschbar (Foto)
- Dynamische Varianten Wartungsaufwendiger
- Oft in Kombination mit anderen Verfahren (Mimik, Stimme, ...)
- Zwillingsproblem

Stimmerkennung

- Noch nicht weit genug ausgereift, um als alleiniges Merkmal zur Verfügung zu stehen.
- Leicht realisierbar (Mikrophone sind weit verbreitet)
- Fälschbarkeit derzeit hoch

II.2. Zuverlässigkeit

	Akzeptiert	Abgewiesen
Berechtigt zum Zutritt	Ideal: 100% Real: ≈99%	Ideal: 0% Real: ≈1%
Unberechtigt zum Zutritt	Ideal: 0% Real: ≈2%	Ideal: 100% Real: ≈98%

Zuverlässigkeit - Meßdaten

	Akzeptiert	Abgewiesen
Berechtigt	a	b
Unberechtigt	c	d

- a+b = Anzahl der Berechtigten
- c+d = Anzahl der Unberechtigten
- a+c = Anzahl der Akzeptierten
- b+d = Anzahl der Abgewiesenen
- N = a+b+c+d Gesamtzahl der Vorgänge

Zuverlässigkeit - Berechnung

- Die **Sensitivität** wird geschätzt durch a/(a+b), das ist die **Akzeptanzrate** für Berechtigte.
- Die **Spezifität** wird geschätzt durch d/(c+d), das ist die **Abweisungsrate** für Unberechtigte.
- Je höher beide Werte, desto besser ist das Verfahren

II.3. Zugriffsschutz

- Nachdem die grundsätzliche Berechtigung eines Anwenders im Netz arbeiten zu dürfen über den Zutrittsschutz geklärt ist, müssen die Detailberechtigungen bis zur Datensatzebene festgelegt werden können.

Zugriffsschutz

- Im Bereich der Betriebssysteme (WS-OS, Server-OS, NOS) üblicherweise nur auf Verzeichnis bzw. Dateiebene möglich.
- In Datenbankanwendungen auf Satzebene verwirklichbar.
- In sonstigen Anwendungen ebenfalls detaillierter realisierbar.

Zugriffsschutz

- Auf Verzeichnis- bzw. Dateiebene:
  - Suchen [S]
  - Lesen [R]
  - Neuanlegen [C]
  - Schreiben [W]
  - Attribute verändern [M]
  - Löschen [E]
  - Rechte verwalten [A]

Zugriffsschutz

- Bei manchen Betriebssystemen stark vereinfachte Rechte:
  - Keine [ ]
  - Lesen [SR]
  - Ändern [SRCWM]
  - Vollzugriff [SRCWMA]

Zugriffsschutz

- Realisiert meist mit Hilfe von ACLs (Access Control Lists)
- Umfang und Funktion unterscheiden sich aber in den einzelnen Betriebssystemen oft erheblich
- Beispiele:
  - Unix, Netware, Windows

Zugriffsschutz

- Auf Arbeitsstationen oft leicht umgehbar, da ein Direktzugriff auf die Platte möglich ist (anderes Betriebssystem oder Boot von anderen Medien)
- Echter Schutz nur mit speziellen Dateisystemen oder eigener Software. (Verschlüsselung)

Zugriffsschutz

- Wenn für einen Anwender physischer Zugang zu unverschlüsselten Daten besteht, kann das beste Zugriffsschutz-system nicht wirken!
- Zugriffschutz ohne Zutrittsschutz ist i.a. wirkungslos!

II.4. Verschlüsselung

- symmetrische Verschlüsselung
- asymmetrische Verschlüsselung
- RSA
- PGP
- Schlüsselverwaltung

Symmetrische Verschlüsselung

- Der Schlüssel für die Verschlüsselung und Entschlüsselung ist gleich und muß daher beiden Kommunikationspartnern bekannt sein.
- Schlüsseltausch problematisch
- Bleibt lange Zeit konstant und ist daher der leichter herauszufinden

Einfachverschlüsselung

- Substitutionsverfahren (Cäsarcode, ...)
- Transpositionsverfahren (Permutation, Zick Zack, ...)

Private Key Verfahren

- Polyalphabetische Substitution
- Produktverschlüsselung
- Blockverschlüsselungen
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - CFB (Cipher Feed Back)
  - OFB (Output Feed Back)
- Bitstromverschlüsselungen

Asymmetrische Verschlüsselung

- Bei der asymmetrischen Verschlüsselung sind die Schlüssel für die Verschlüsselung bzw. Entschlüsselung verschieden
- Kein Schlüsseltausch notwendig
- Einer der beiden Schlüssel wird öffentliche verfügbar (public) gemacht.

Public Key Verfahren

- Merkel Hellman Verfahren
- RSA (Rivest, Shamir, Adleman, 1978) Verfahren
- Für verschlüsselte Kommunikation wird der Verschlüsselungsschlüssel „public“
- Für die digitale Unterschrift wird der Entschlüsselungsschlüssel „public“

Sicherheit – RSA

- $\text{Schlüsseltext} = \text{Klartext}^{e} \pmod{n}$
- $\text{Klartext} = \text{Schlüsseltext}^{d} \pmod{n}$
- (e,n) Public Key
- (d,n) Secret Key
- n ist das Produkt zweier sehr großer Primzahlen (100-stellig und mehr)

Sicherheit – PGP

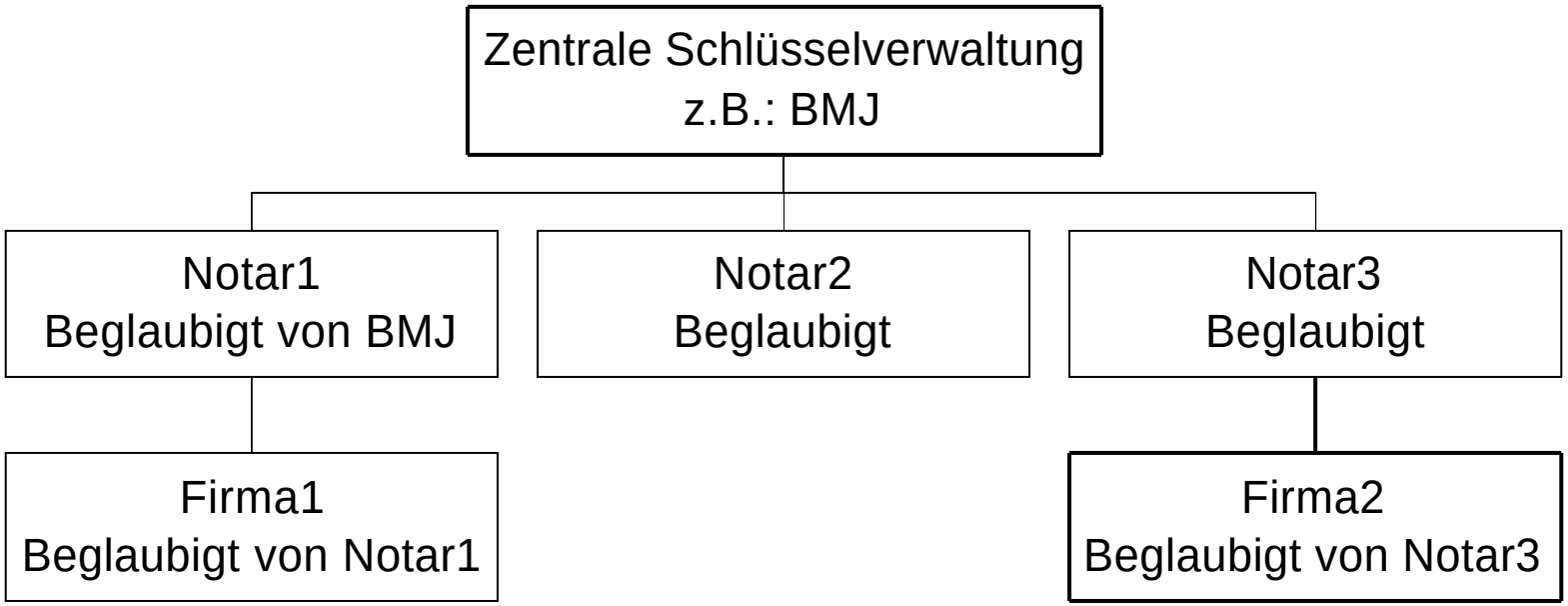
- PGP ist eine Anwendung des RSA-Verfahren, daß diese Methode in das e-Mail-System (den Client) einbindet bzw. beliebige Texte über die Zwischenablage behandeln kann.
- lokale Schlüsselverwaltung integriert
- Verschlüsselung und Signatur möglich

Schlüsselverwaltung

- Das verbleibende Problem ist die Schlüsselverwaltung
- Wie kann sichergestellt werden, daß bestimmter Schlüssel zu einer bestimmten Person gehört?
- Persönliche Übergabe weltweit?
- Übertragung über e-Mail?

Schlüsselverwaltung

- Zentrale hierarchische Schlüsselverteilung



III. Schutz der Kommunikation

- Gefährdungen
- Sicherheitsdienste
- Sicherheitsmechanismen

III.1. Gefährdungen

- Passive Angriffe
- Aktive Angriffe
- Zufällige Verfälschungen

Passive Angriffe

- Abhören der Teilnehmeridentitäten
  - Wer mit wem
- Abhören der Daten
  - Mißbrauch der Daten
- Verkehrflußanalyse
  - Größenordnungen, Zeitpunkte, Häufigkeit, Richtung des Datentransfers

Aktive Angriffe

- Wiederholung oder Verzögerung einer Information
- Einfügen oder Löschen bestimmter Daten
- Boykott des Informationssystems
- Modifikation der Daten
- Vortäuschung einer falschen Identität
- Leugnen einer Kommunikationsbeziehung

Zufällige Verfälschungsmöglichkeiten

- Fehlrouting von Information
  - Durch „Vermittlungsfehler“ in Knotenrechner
- Fehlbedienung
  - Löschen noch nicht versandter Informationen
  - Ausdrucken sensibler Daten

III.2. Sicherheitsdienste 1

- Aus den Gefährdungen können nun die notwendigen Sicherheitsdienste abgeleitet werden:
  - Vertraulichkeit der Daten
  - Verhinderung einer Verkehrflußanalyse
  - Datenunversehrtheit
  - Authentizitätsprüfung des Kommunikationspartners

Sicherheitsdienste 2

- Authentizitätsprüfung des Datenabsenders
- Zugangskontrolle
- Sendernachweis
- Empfängernachweis

III.3. Sicherheitsmechanismen

- Verschlüsselung
- Digitale Unterschrift
- Hashfunktion
- Authentizitätsprüfung
- Zugangskontrolle
- Sicherstellung der Datenunversehrtheit
- Verhinderung der Verkehrsflußanalyse

Sicherheitsmechanismen 2

- Routingkontrolle
- Notariatsfunktion
- Vertrauenswürdige Implementation
- Abstrahlsichere Endgeräte und Vermittlungseinrichtungen
- Überwachung und Alarmierung (Alert)
- Logbuch

IV. Authentizitätsprüfung und Schlüsselverteilung

- Schlüsselverwaltung
- Authentizitätsprüfungsverfahren
- Schlüsselverteilung mit Private Keys
- Schlüsselverteilung mit Public Keys

IV.1. Schlüsselverwaltung

- Schlüsselerzeugung
- Interne Schlüsselverteilung
- Externe Schlüsselverteilung
- Schlüsselinstallation

Schlüsselerzeugung

- Deterministisch
  - Pseudozufallszahlen
  - Rekonstruierbar
- Nicht deterministisch
  - „Echte“ Zufallszahlen
  - „Nicht“ rekonstruierbar

Interne Schlüsselverteilung

- Erfolgt im Netz
  - Abhörgefährdet
  - Gefahr der Fälschung des Schlüssels
  - Fälschung der Identität

Externe Schlüsselverteilung

- Erfolgt durch systemfremde Übertragung (z.B.: Boten)
  - Weniger Abhörgefährdet
  - Geringere Fälschungsgefahr des Schlüssels
  - Fälschung der Identität aufwendiger

Schlüsselinstallation

- Laden der Schlüssel
- Speichern der Schlüssel
- Erschwerung des Zugangs
- Für Richtigkeitsprüfung soll die Kenntnis des Schlüssel nicht notwendig sein

IV.2. Authentizitätsprüfungs-verfahren

- 2 Arten
  - Schwache Authentizitätsprüfung (Passwort, ...)
  - Starke Authentizitätsprüfung (Verschlüsselung eines „Tokens“ mit kryptographischen Methoden)
- Das Problem der Übertragung ist bei beiden Arten gleich

IV.3. Schlüsselverteilung mit Private Keys

- Anzahl der Schlüssel: n/2 * (n-1)
- Master-Keys
- Schlüsselverteilzentrale mit zweiseitiger Teilnehmerkommunikation
- Schlüsselverteilung mit einseitiger Teilnehmerkommunikation

Master-Keys

- Masterkeys werden für den Austausch der „Session“-Keys benutzt.
- Allerdings verlagert sich das Problem der Schlüsselverteilung auf die Masterkeys (Seltener im Einsatz).
- Sessionkeys können oft gewechselt werden.

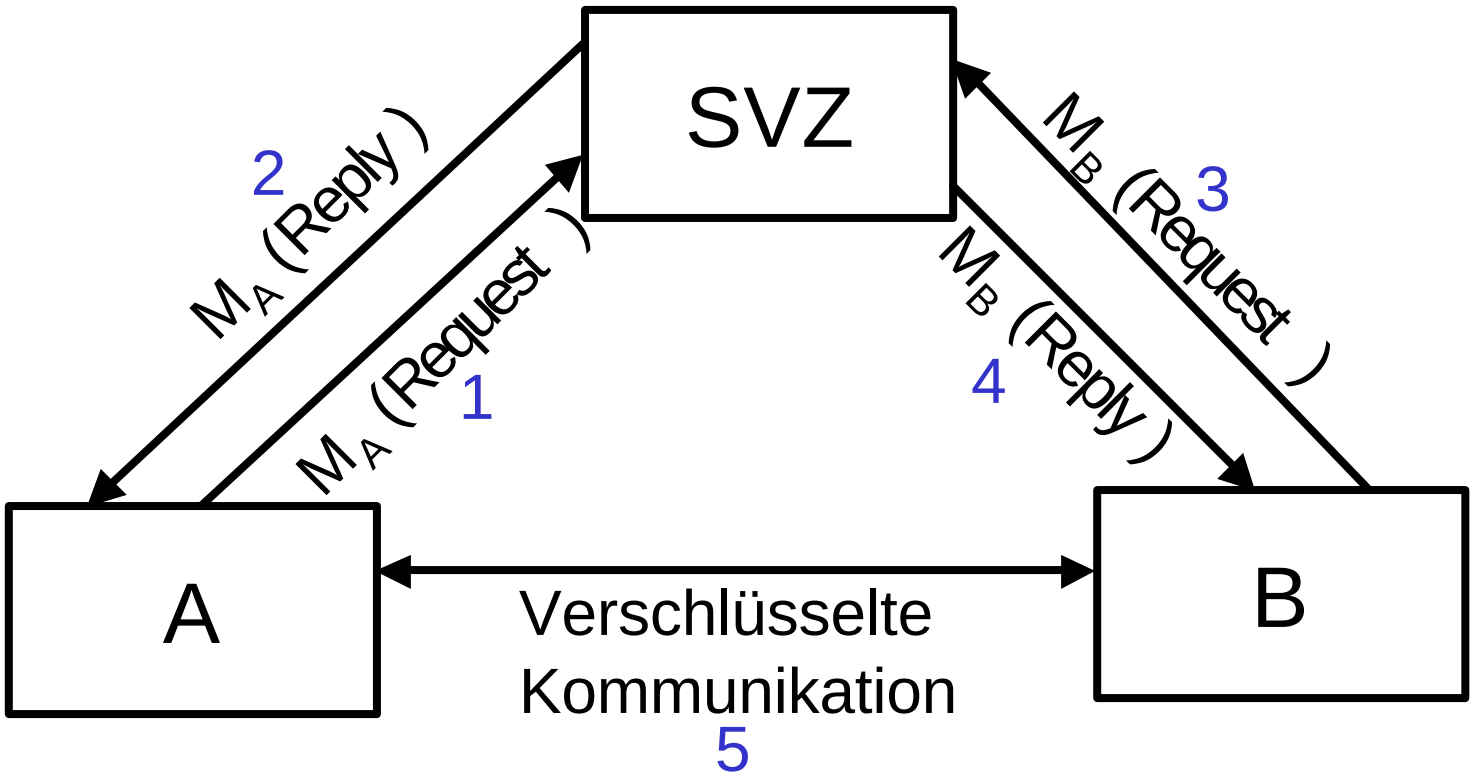
Verteilung mit zweiseitiger Teilnehmerkommunikation 1

- Schlüsselverteilzentrale (SVZ) reduziert den Aufwand für die Verwaltung der Schlüssel bei den einzelnen Teilnehmern.
- A möchte mit B kommunizieren
- M_A und M_B sind die Masterkeys von A bzw. B

Verteilung mit zweiseitiger Teilnehmerkommunikation 2

- A fordert von SVZ einen Sessionkey an
- SVZ schickt den Sessionkey an A
- B fordert ebenfalls von der SVZ diesen Sessionkey an
- SVZ schickt den Sessionkey an B
- A und B kommunizieren
- Jede Station hat nur einen Key

Verteilung mit zweiseitiger Teilnehmerkommunikation 3



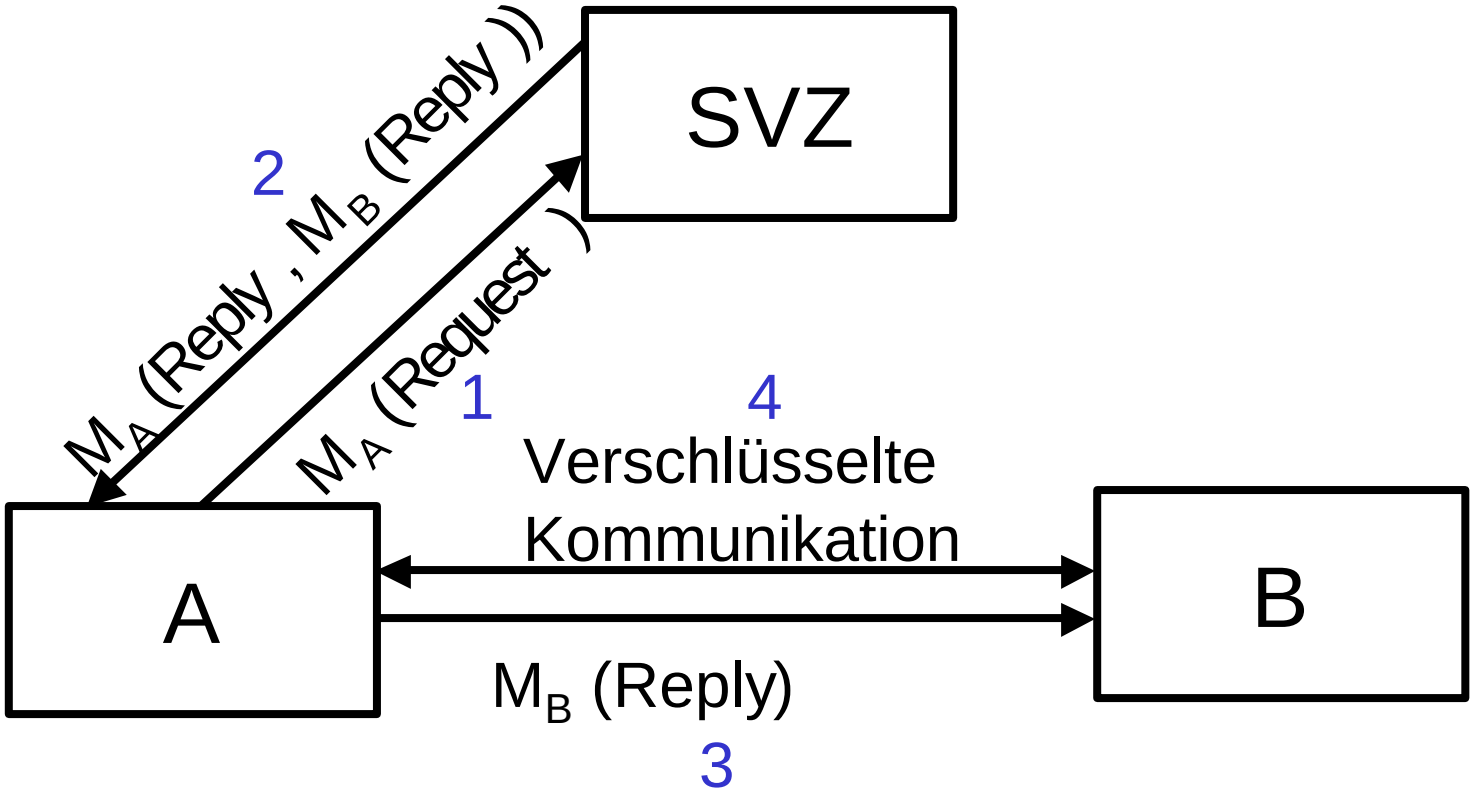
Verteilung mit einseitiger Teilnehmerkommunikation 1

- Schlüsselverteilzentrale (SVZ) reduziert auch hier den Aufwand für die Verwaltung der Schlüssel bei den einzelnen Teilnehmern.
- A möchte mit B kommunizieren
- M_A und M_B sind die Masterkeys von A bzw. B

Verteilung mit einseitiger Teilnehmerkommunikation 2

- A fordert von SVZ einen Sessionkey an
- SVZ schickt den Sessionkey und einen Block für B an A (inkl. Zeitstempel)
- A schickt das für B bestimmte Paket an B (Inhalt ist für A unbrauchbar)
- A und B kommunizieren
- Jede Station hat nur einen Key

Verteilung mit einseitiger Teilnehmerkommunikation 3



IV.4. Schlüsselverteilung mit Public Keys 1

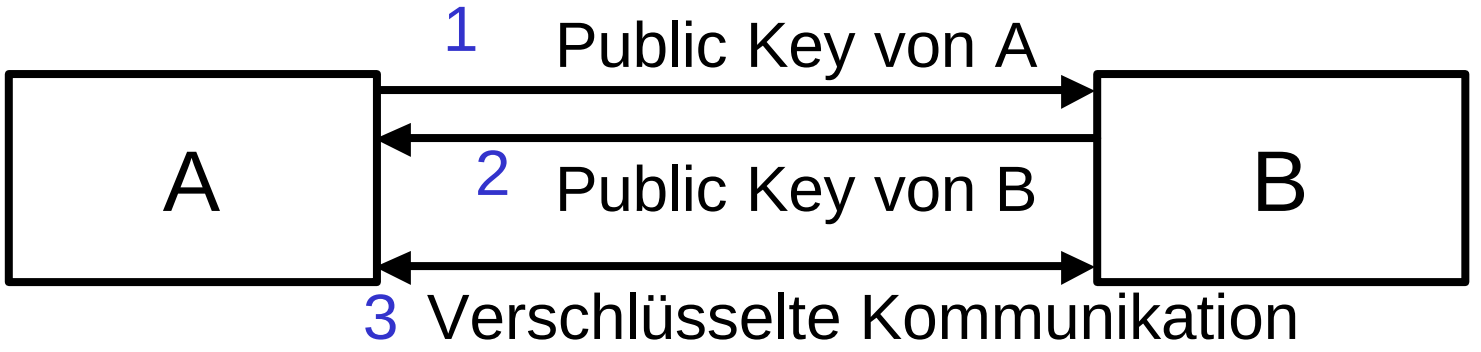
- Schlüsselaustausch zu Beginn der Kommunikation
- Teilnehmer haben Public-Key-Verzeichnis
- Schlüsselverteilzentrale mit zweiseitiger Teilnehmerkommunikation
- Schlüsselverteilung mit einseitiger Teilnehmerkommunikation

Schlüsselverteilung mit Public Keys 2

- Authentizitätsprüfung bei mehreren Schlüsselverteilzentralen
- Normung
- Schlüsselerzeugung
- Hardwarelösungen (Chipcard)

Schlüsselaustausch zu Beginn der Kommunikation

- Austausch der jeweiligen öffentlichen Schlüssel vor der eigentlichen Kommunikation



Teilnehmer haben Public-Key-Verzeichnis

- Vorteile
  - Sichere Kommunikation ohne Schlüsselaustausch möglich
  - Authentizität ist „gewährleistbar“
- Nachteile
  - Verzeichnis wird rasch umfangreich
  - Alle Teilnehmer müssen von einem Schlüsselwechsel informiert werden

Verteilzentrale mit zweiseitiger Teilnehmerkommunikation

- Analog zum Private Key-Verfahren, statt der Masterkeys werden aber auch für die Kommunikation zur SVZ Public-Keys verwendet
- Wenig praktische Bedeutung, da hier mit hoher Sicherheit auf das „einseitige“ Verfahren ausgewichen werden kann.

Verteilung mit einseitiger Teilnehmerkommunikation 1

Annahmen:

- SVZ kennt alle Public-Keys und den eigenen Secret-Key
- SVZ_{pk}, A_{pk}, B_{pk} ... Public Keys
- SVZ_{sk}, A_{sk}, B_{sk} ... Secret Keys
- A möchte gesichert mit B kommunizieren

Verteilung mit einseitiger Teilnehmerkommunikation 2

- A fordert von SVZ den öffentlichen Schlüssel von B an (Anfrage ist mit SVZ_{pk} verschlüsselt und enthält Teilnehmerkennungen von A und B sowie Datum/Uhrzeit)
- SVZ antwortet mit einer Nachricht, die zwei Zertifikate enthält

Zertifikat für A

- Enthält:
  - Teilnehmernummer von B
  - Den öffentlichen Schlüssel von B: B_{pk}
  - Datum/Uhrzeit
- Ist von SVZ digital unterschrieben und mit A_{pk} verschlüsselt

Zertifikat für B

- Enthält:
  - Teilnehmernummer von A
  - Den öffentlichen Schlüssel von A: A_{pk}
  - Datum/Uhrzeit
- Ist von SVZ digital unterschrieben und mit B_{pk} verschlüsselt

Auswertung durch A

- A entschlüsselt sein Paket, überprüft die Unterschrift und übernimmt B_{pk}.
- Das zweite Zertifikat wird an B weitergeleitet
- Eine Kontrollnachricht mit den Daten im Zertifikat der SVZ wird ebenfalls an B geleitet (von A unterschrieben und mit B_{pk} verschlüsselt).

Auswertung durch B

- B prüft das Zertifikat und die Kontrollnachricht
- B sendet seinerseits eine analoge Kontrollnachricht an A
- Nach Prüfung dieser kann die gesicherte Kommunikation beginnen.

Authentizitätsprüfung bei mehreren SVZs

- Analog zur gesicherten Kommunikation zwischen A und B muß eine verschlüsselte Kommunikation zwischen den SVZs hergestellt werden und die öffentlichen Schlüssel der Teilnehmer zwischen den SVZs ausgetauscht werden.

„Normung“

- L2F (Layer 2 Forwarding, Cisco ...)
- PPTP (Point-to-Point Tunneling Protocol, Microsoft ...)
- L2TP (Layer 2 Tunneling Protocol, L2F+PPTP nach RFC 2661)
- IPv6
- IPSec (IP Security Protocol, RFCs 2401 – 2412)

Schlüsselerzeugung

- Erzeugung der Schlüssel durch die Teilnehmer selbst
- Erzeugung der Schlüssel durch die SVZ (Transport der Schlüssel?)
- Erzeugung der Schlüssel durch Dritte (Signaturstellen, ... ,Transport der Schlüssel?)

Hardwarelösungen (Chipcard)

- Sichere Aufbewahrung der Secret-Keys in einer Chipcard
- Hardware zu Lesen der Karte notwendig

V. Einbindung in ein Referenzmodell

- ISO-Referenzmodell
  - Application Layer
  - Presentation Layer
  - Session Layer
  - Transport Layer
  - Network Layer
  - Data Link Layer
  - Physical Layer

V.0. Problem des Routings

- Für den Verbindungsaufbau sind Daten notwendig, die nicht verschlüsselt sein dürfen
- Sicherung bis zur Schicht 3 schwierig
- Paketvermittlung
- Leitungsvermittlung

V.1. Schicht 1

- Dienste:
  - Vertraulichkeit der Verbindung
  - Verhinderung einer Verkehrflußanalyse
- Mechanismen
  - Verschlüsselung (außer Start- und Stopbits) zwischen nächsten Nachbarn (meist auf HW-Ebene).

Schicht 1

- Einsatzmöglichkeiten
  - Nur in Schicht 1 ist der gesamte Verkehrsfluß schützbar.
  - Entzieht sich aber den Möglichkeiten eines Anwenders.
  - Derzeit von keinem Leitungsprovider angeboten.

V.2. Schicht 2

- Dienste
  - Vertraulichkeit bei verbindungsorientierten und verbindungslosen Kommunikationen.
- Mechanismen
  - Verschlüsselung der Verbindung (Linkverschlüsselung).

Schicht 2

- Einsatzmöglickeiten
  - Entzieht sich den Möglichkeiten eines Anwenders
  - Derzeit von keinem Leitungsprovider angeboten (anders im Funkbereich)

V.3. Schicht 3

- Dienste
  - Authentizitätsprüfung der Instanz des Kommunikationspartners
  - Zugangskontrolle
  - Vertraulichkeit bei verbindungsorientierten und verbindungslosen Kommunikationen
  - Verhinderung einer Verkehrsflußanalyse
  - Datenunversehrtheit ohne Recovery
  - Authentizitätsprüfung des Absenders der Daten

Schicht 3

- Mechanismen 1
  - Die Authentizitätsprüfung wird durch eine Kombination aus kryptographischen Methoden, digitaler Unterschrift, Paßwörtern und ein eigenes Authentizitätsprüfungsprotokoll unterstützt.

Schicht 3

- Mechanismen 2
  - Die Zugangskontrolle erfordert eigene Zugangskontrollmechanismen sowohl in den Vermittlungsknoten (Kontrolle durch den Netzbetreiber) als auch im Zielsystem (Abweisung unerwünschter Verbindungen)

Schicht 3

- Mechanismen 3
  - Knotenverschlüsselung für die Vertraulichkeit der Verbindung und die Vertraulichkeit der Daten. Zusätzlich Routingkontrollfunktionen können dem Benutzer eine Auswahl der Wege erlauben.

Schicht 3

- Mechanismen 4
  - Zur Verhinderung der Verkehrflußanalyse werden vom Netzbetreiber Fülldaten geschickt (müssen verschlüsselt sein oder von einer der unteren Schichten verschlüsselt werden); dabei muß aber durch eine Flußkontrolle gewährleistet bleiben, daß noch immer Daten übertragen werden können.

Schicht 3

- Mechanismen 5
  - Die Datenunversehrtheit kann durch eine Prüfsumme oder Hashwerte sichergestellt werden, dabei ist in dieser Schicht keine „Recovery“ vorgesehen (siehe auch ISO-Referenzmodell).

Schicht 3

- Mechanismen 6
  - Der Sendernachweis wird ebenfalls über die Authentizitätsprüfung (des Senders) erreicht.
- Einsatzmöglichkeiten
  - Durch Netzbetreiber (siehe oben)
  - Durch Anwender (VPN)

V.4. Schicht 4

- Dienste
  - Authentizitätsprüfung der Instanz des Kommunikationspartners
  - Zugangskontrolle
  - Vertraulichkeit bei verbindungsorientierten und verbindungslosen Kommunikationen
  - Datenunversehrtheit der Verbindung mit bzw. ohne Recovery
  - Authentizitätsprüfung des Absenders der Daten

Schicht 4

- Mechanismen
  - Siehe Schicht 3 allerdings werden aus den „Next Hop“-Mechanismen „End-to-End“-Mechanismen.
- Einsatzmöglichkeiten
  - Ab dieser Schicht liegt der Einsatz der Mechanismen vollständig in der Verantwortung des Netzbenutzers.

V.5. Schicht 5

- Dienste
  - Keine eigenen Sicherheitsdienste aber die Vereinbarung von notwendigen Diensten für die Session
- Mechanismen
  - Keine
- Einsatzmöglichkeiten
  - Keine außer der Vereinbarung

V.6. Schicht 6

- Dienste
  - Keine eigenen Dienste
- Mechanismen
  - Sendernachweis
  - Empfängernachweis
  - Notariatsfunktion

Schicht 6

- Einsatzmöglichkeiten
  - Anbieten von Mechanismen um der Anwendungschicht alle notwendigen Dienste zu ermöglichen

V.7. Schicht 7

- Dienste
  - Anwendungsabhängig
- Mechanismen
  - Entweder anwendungseigene Mechanismen
  - Nutzung von Mechanismen der darunter liegenden Schichten

VI. Normen

VI. „Normen“

- L2F
- PPTP
- L2TP
- IPv4 – IPv6
- IPSec

VI.1. L2F

- Layer 2 Forwarding
- Entwickelt von Cisco (Nortel, Shiva)
- RFC 2341 aus 1998 (historic)
- Reines Tunnelprotokoll (d.h. keine Verschlüsselung)
- Punkt zu Mehrpunktverbindungen möglich
- ISO-Schicht 2

VI.2. PPTP

- Point-to-Point Tunneling Protocol
- Entwickelt vom PPTP-Forum (Microsoft, U.S.-Robotics, ...)
- Kein Standard, kein Keymanagement, keine Integritätsprüfung
- Verschlüsselung (40, 56 und 128 Bit)
- ISO-Schicht 2

VI.3. L2TP

- Layer 2 Tunneling Protocol
- Zusammenführung von L2F und PPTP
- RFC 2661 aus 1999 (proposed)
- Unterstützung von Mehrpunktverbindungen und NAT
- Authentifizierung mittels PAP/CHAP

VI.4. IPv4

- Im IPv4-Protokoll keine Sicherheitsfunktionen implementiert
- Daher kann auch nur innerhalb der Nutzdaten mit Hilfe von Sicherheitsfunktionen (Verschlüsselung) gearbeitet werden
- IPSec (s.u.) später für IPv4 adaptiert.

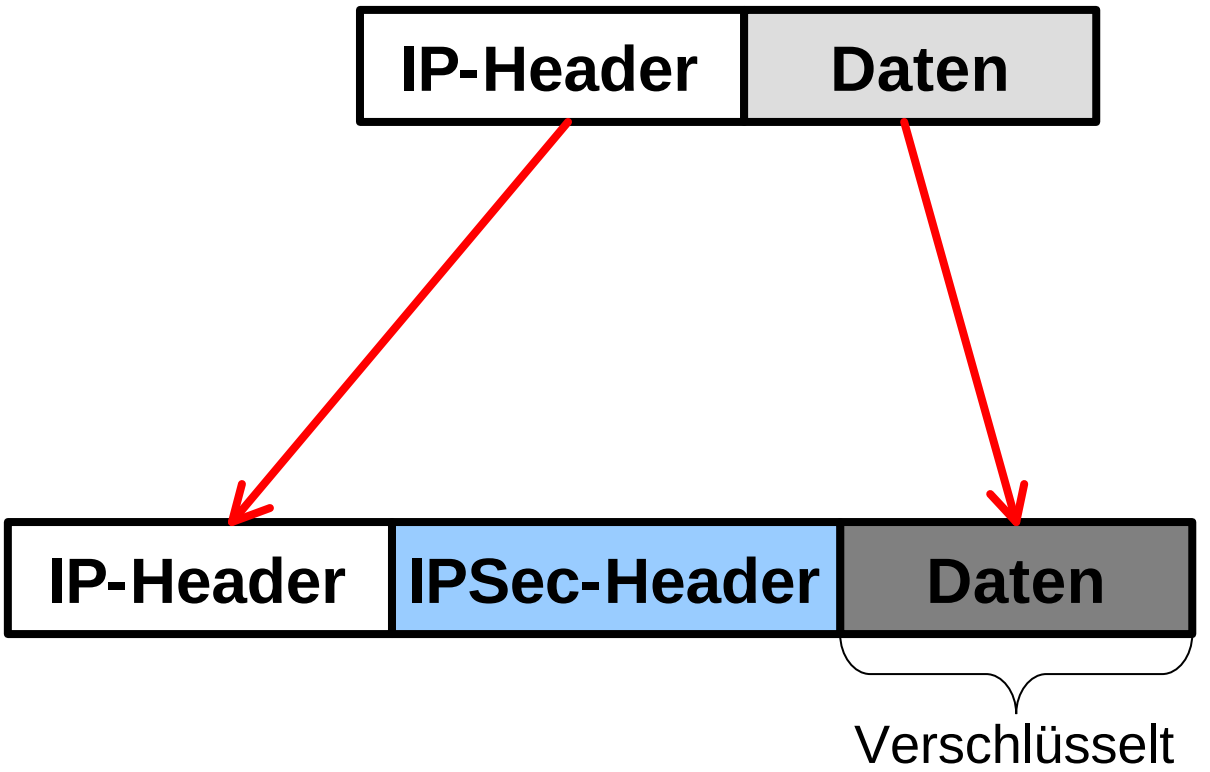
VI.5. IPv6

- Sicherheitsfunktionen in das Protokoll implementiert.
- Mehr Sicherheit, da ganze Packete gesichert werden können.
- Sonstige neue Funktionen nicht sicherheitsrelevant.

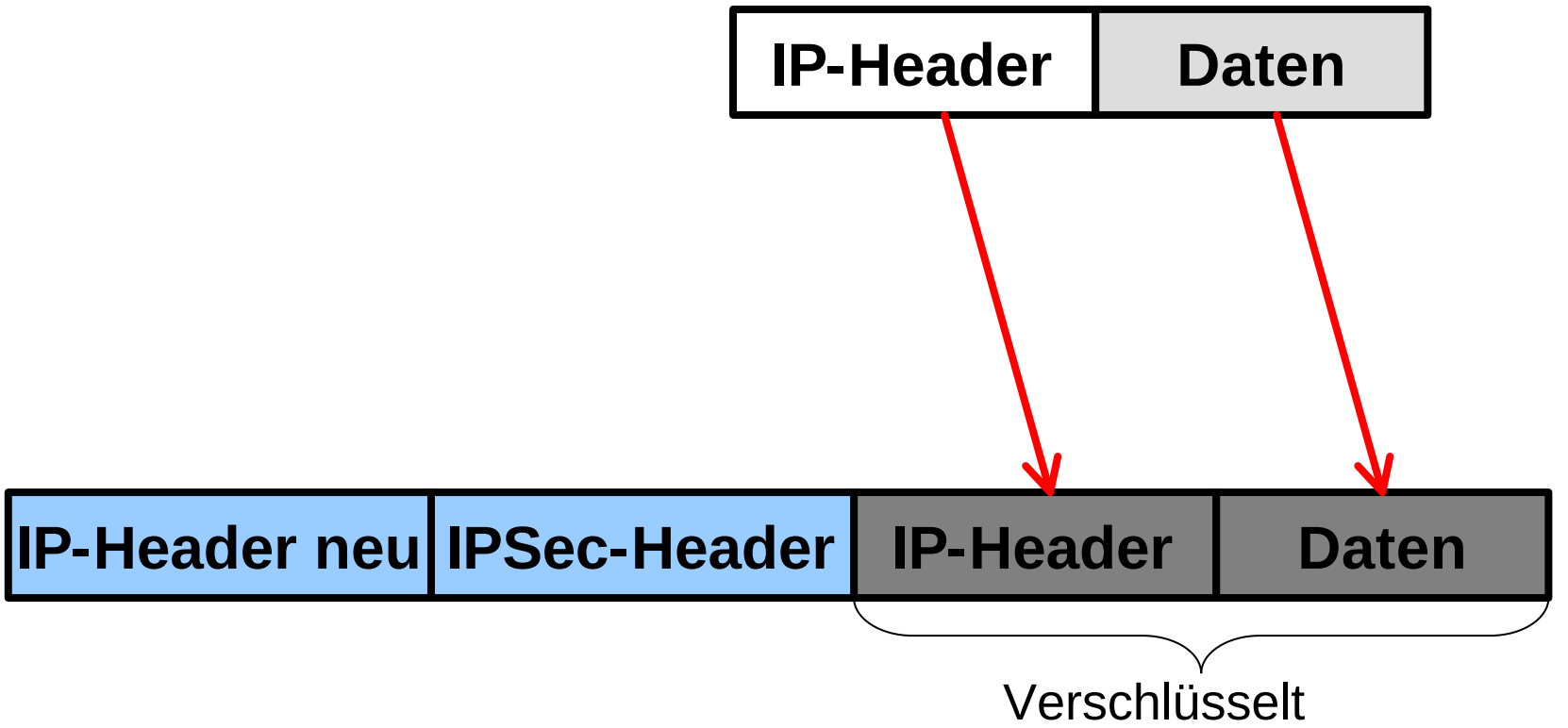
VI.6. IPSec

- RFCs 2401 – 2412
- IP Security Protocol
- Soll PPTP ablösen
- 2 Modi
  - Transportmodus (nur die Daten werden verschlüsselt)
  - Tunnelmodus (ganzes Paket verschlüsselt)

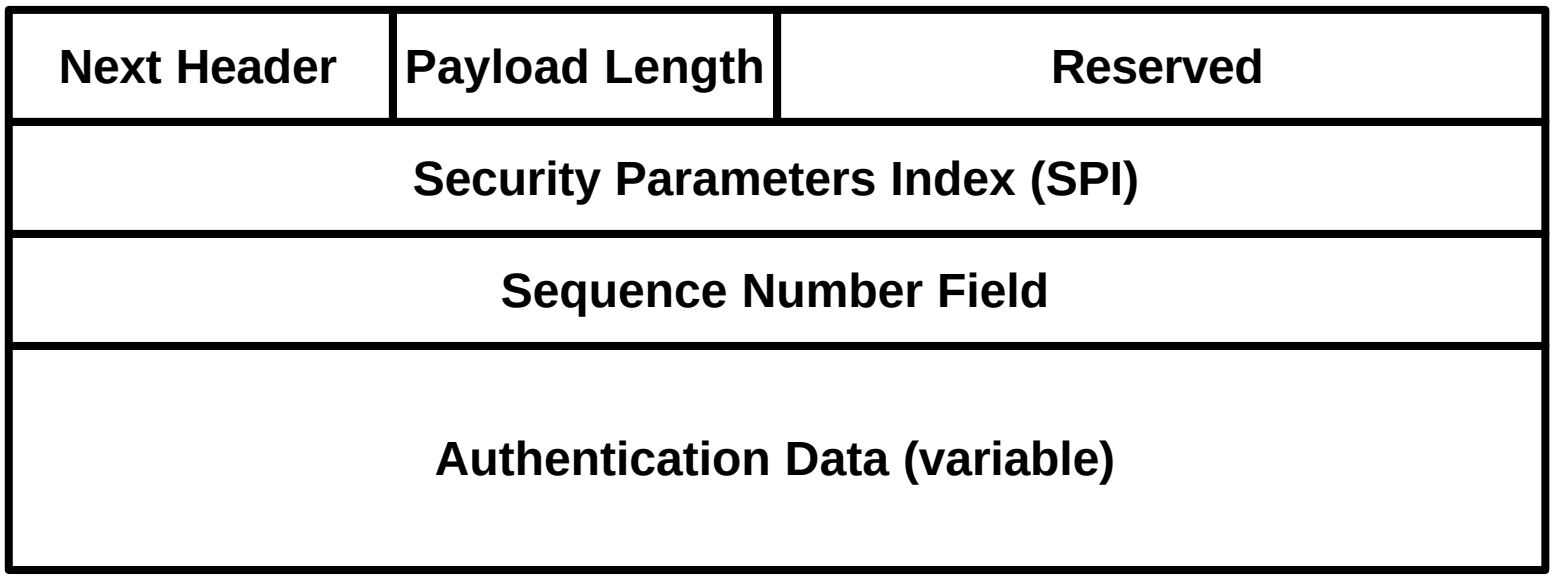
Transportmodus



Tunnelmodus



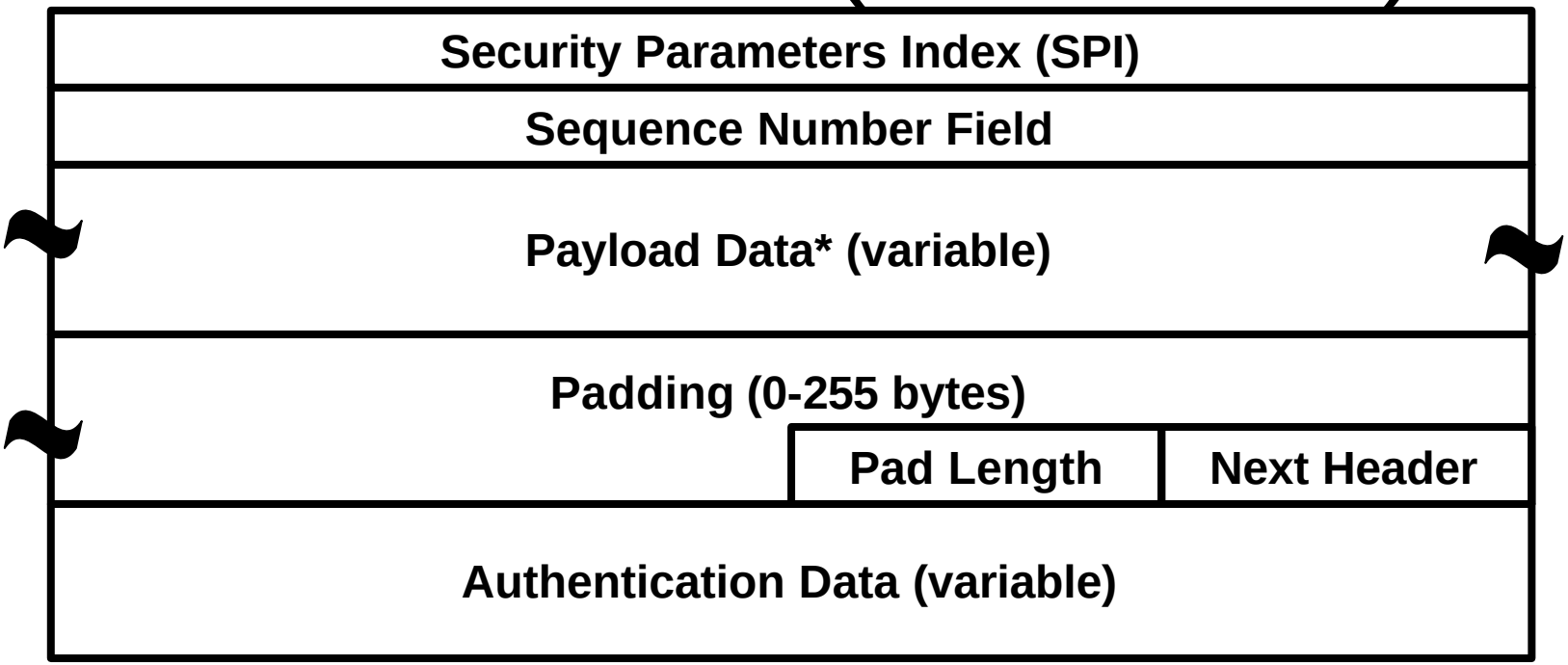
AH-Header (RFC 2402)



Im Header davor steht 51 als Protokolltyp

(IPv4 Protocol- bzw. IPv6 Next Header-Field)

ESP-Packet (RFC 2406)



1 Byte

Im Header davor steht 50 als Protokolltyp

(IPv4 Protocol- bzw. IPv6 Next Header-Field)

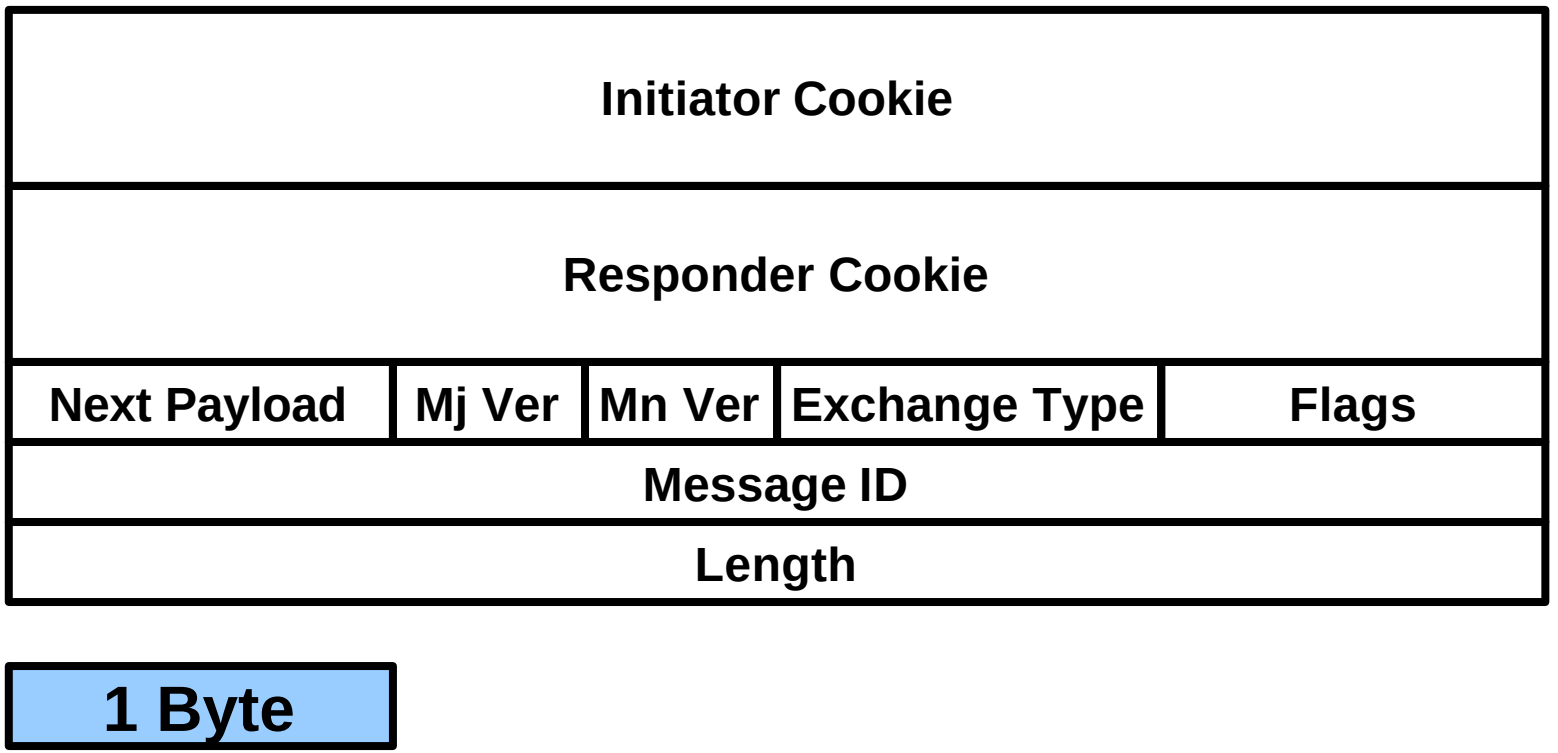
Schlüsselaustausch

- Diffie-Hellman (IEEE Transactions on Information Theory, V. IT-22, n. 6, June 1977)
- Oakley (RFC2412)
- SKEME (IEEE Proceeding 1996)

  Secure Key Exchange Mechanism
- IKE (RFC 2409)

  Internet Key Exchange

ISAKMP-Header (RFC 2408)



Hashfunktionen

- HMAC (RFC2104)

  keyed-Hashing for Message AuthentiCation
- MD5 (RFC 1321)

  Message Digest algorithm
- SHA (FIPS 180-1 1994)

  Secure HAsh standard

Verschlüsselungsalgorithmen

- IDEA (ETH Series in Inf.Proc., v. 1)
- DES (ANSI X3.106)

  Data Encryption Standard
- Blowfish (Dr.Dobb's Journal, April 1994)
- RC4/RC5 (RSA Data Security)

L2TP using IPSec

- RFC 3193 aus 2001 (proposed)
- Verwendet UDP-Port 1701
- Authentifikation, Verschlüsselung, Datenintegrität und Verhinderung von Replayattacken
- Erlaubt freiwillige und verpflichtende Tunnel

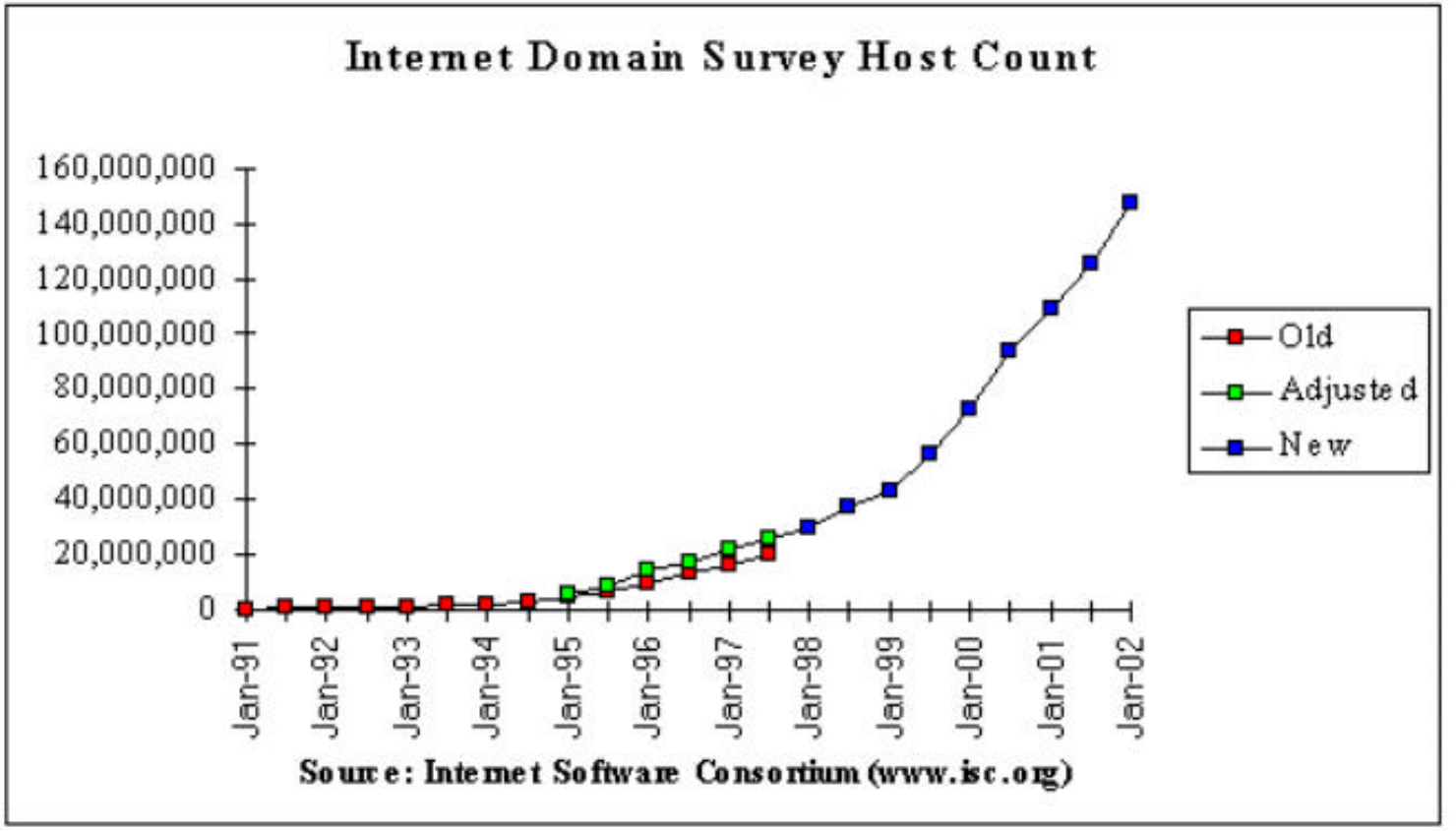
VII. Datenschutzeinrichtung

- Motivation
- Die 7 Schritte zur Sicherheit
- Firewall
- IDS

VII.1. Motivation 1

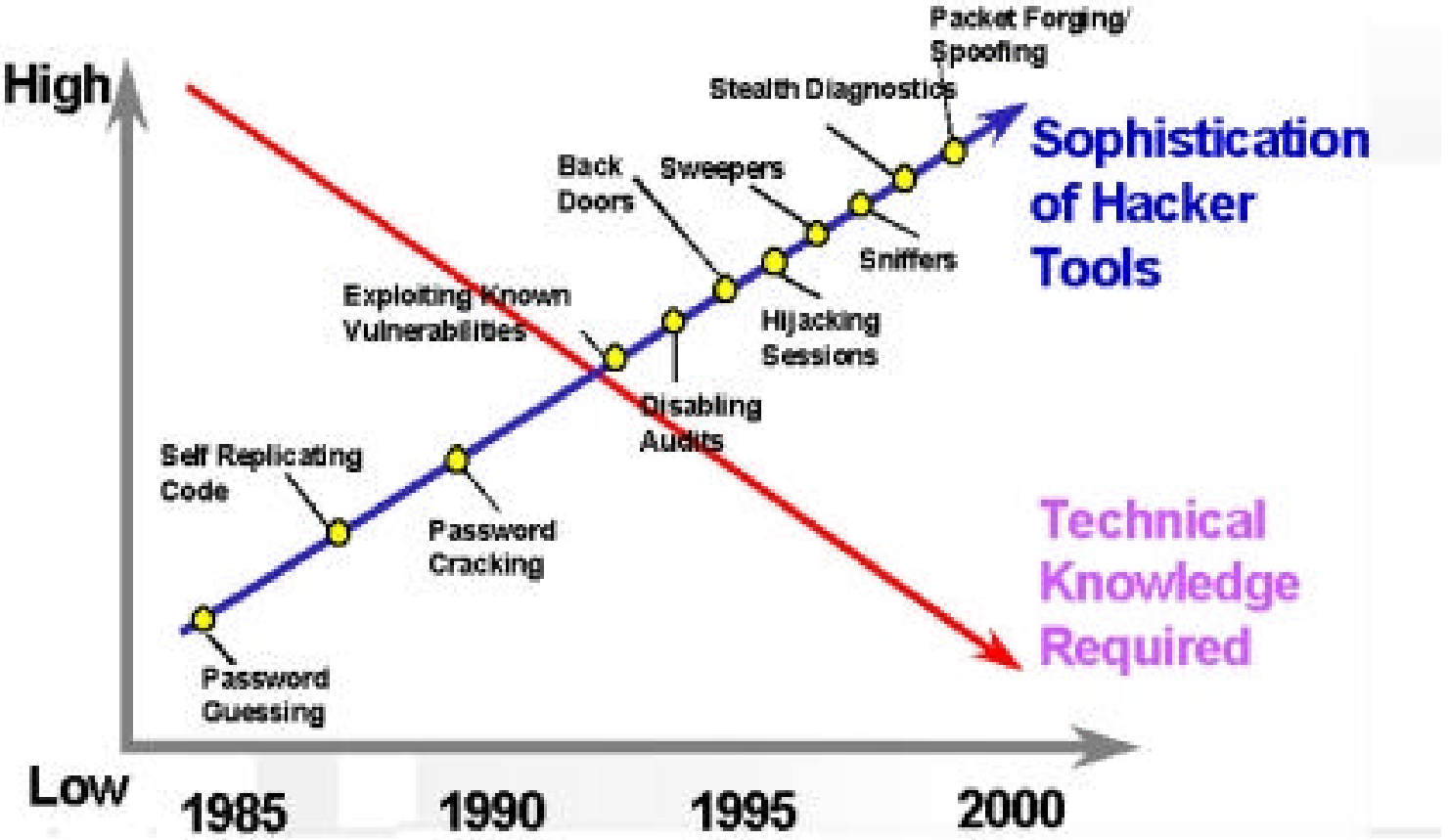
- Durch das zunehmende Bedrohungspotential muß wesentlich mehr als bisher für die Sicherheit getan werden:
  - Technisch (Hardware, Software, ...)
  - Organisatorisch (K-Pläne, Outsourcing, ...)
- „If you can reach them, they can reach you!“

Motivation 2



Ca. 300.000.000 Benutzer ⇨ ca. 300.000 „Hacker“

Motivation 3

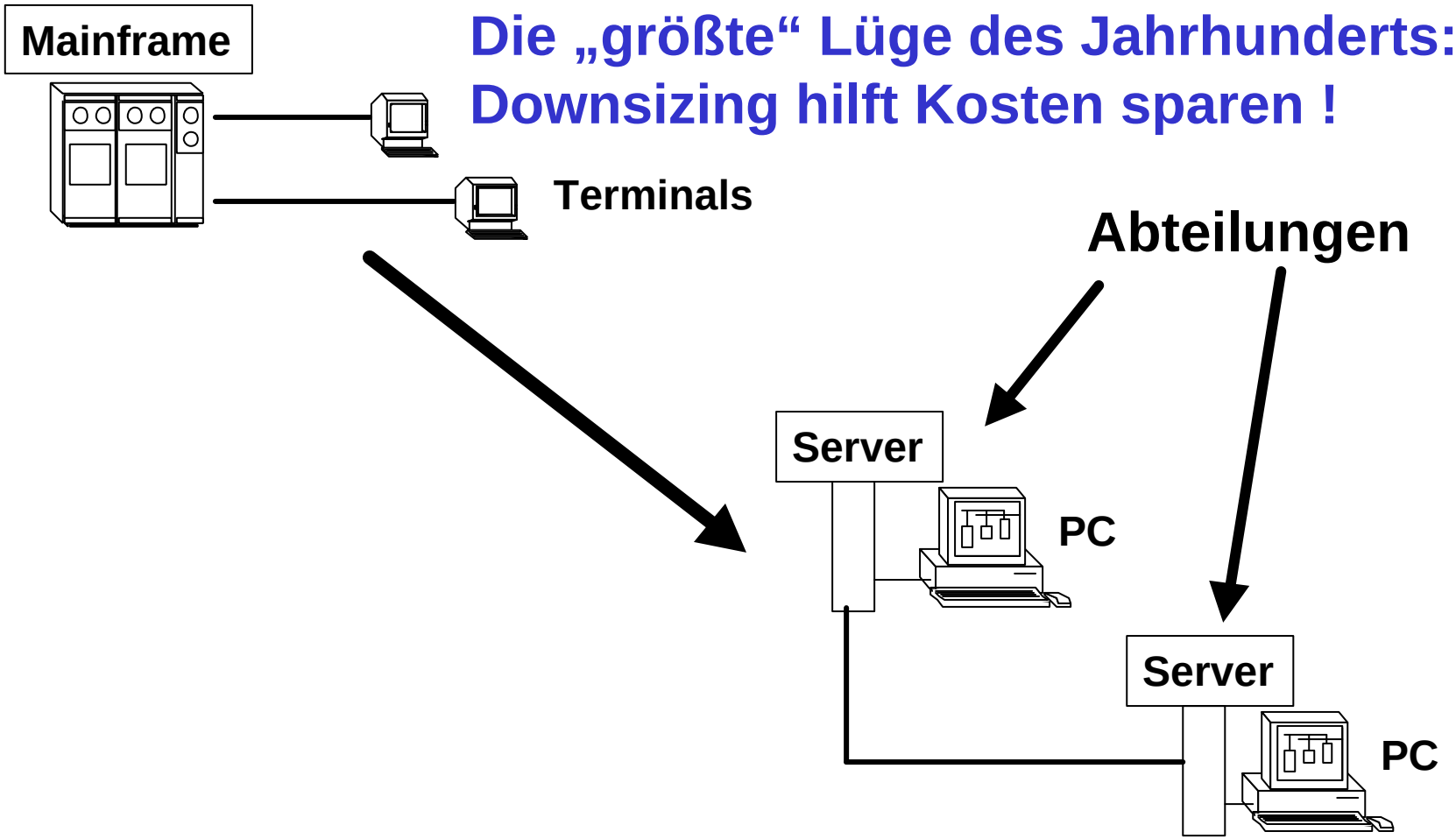


VII.2. 7 Schritte zur Sicherheit

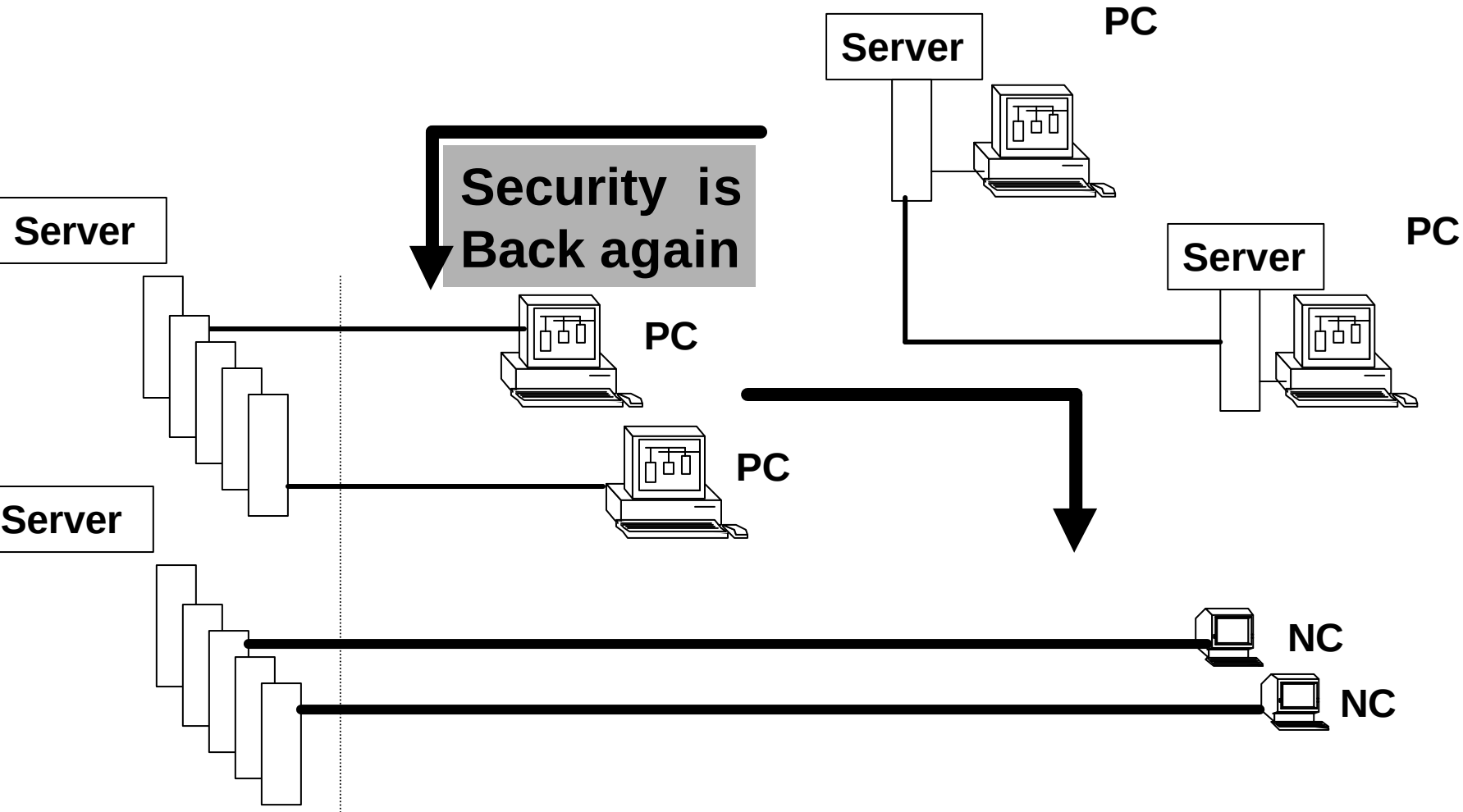
- Downsizing
- VLANs
- Firewall
- VPN (Virtual Private Network)
- VDN (Virtual Division Network)
- Appliances
- High Availability and Load Balancing

Downsizing

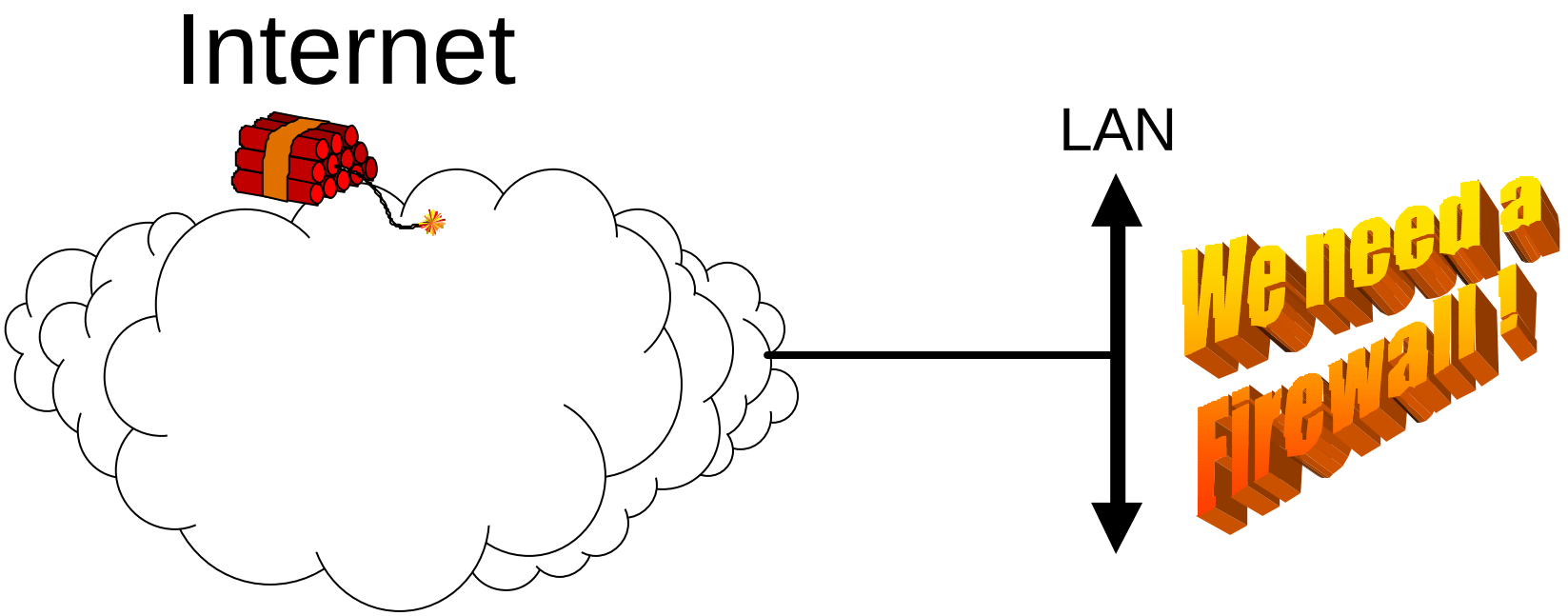
Die „größte“ Lüge des Jahrhunderts:
Downsizing hilft Kosten sparen !



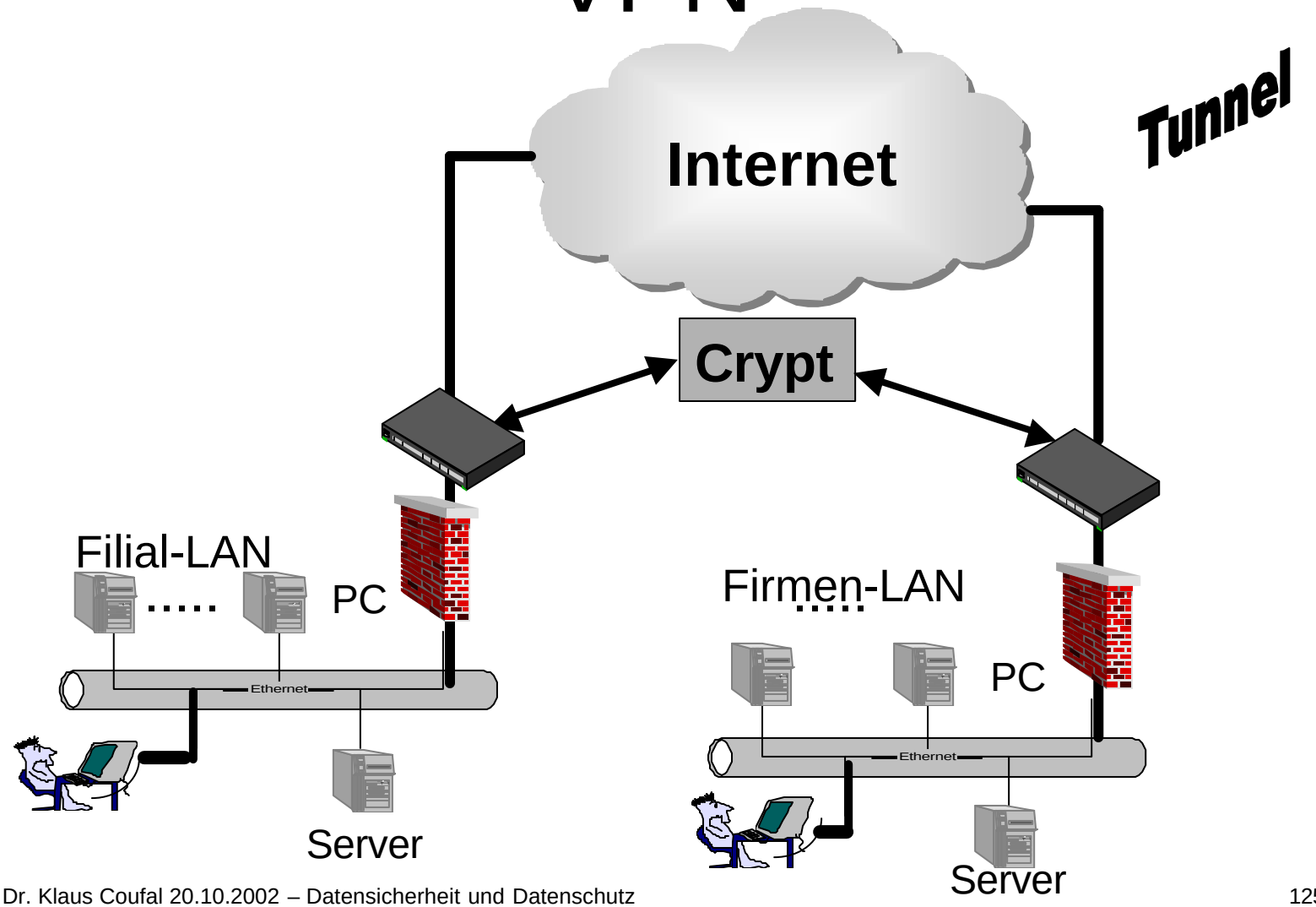
VLANs


Server
PC
Security is Back again
Server
PC
Server
PC
PC
Server
NC
NC

Firewall

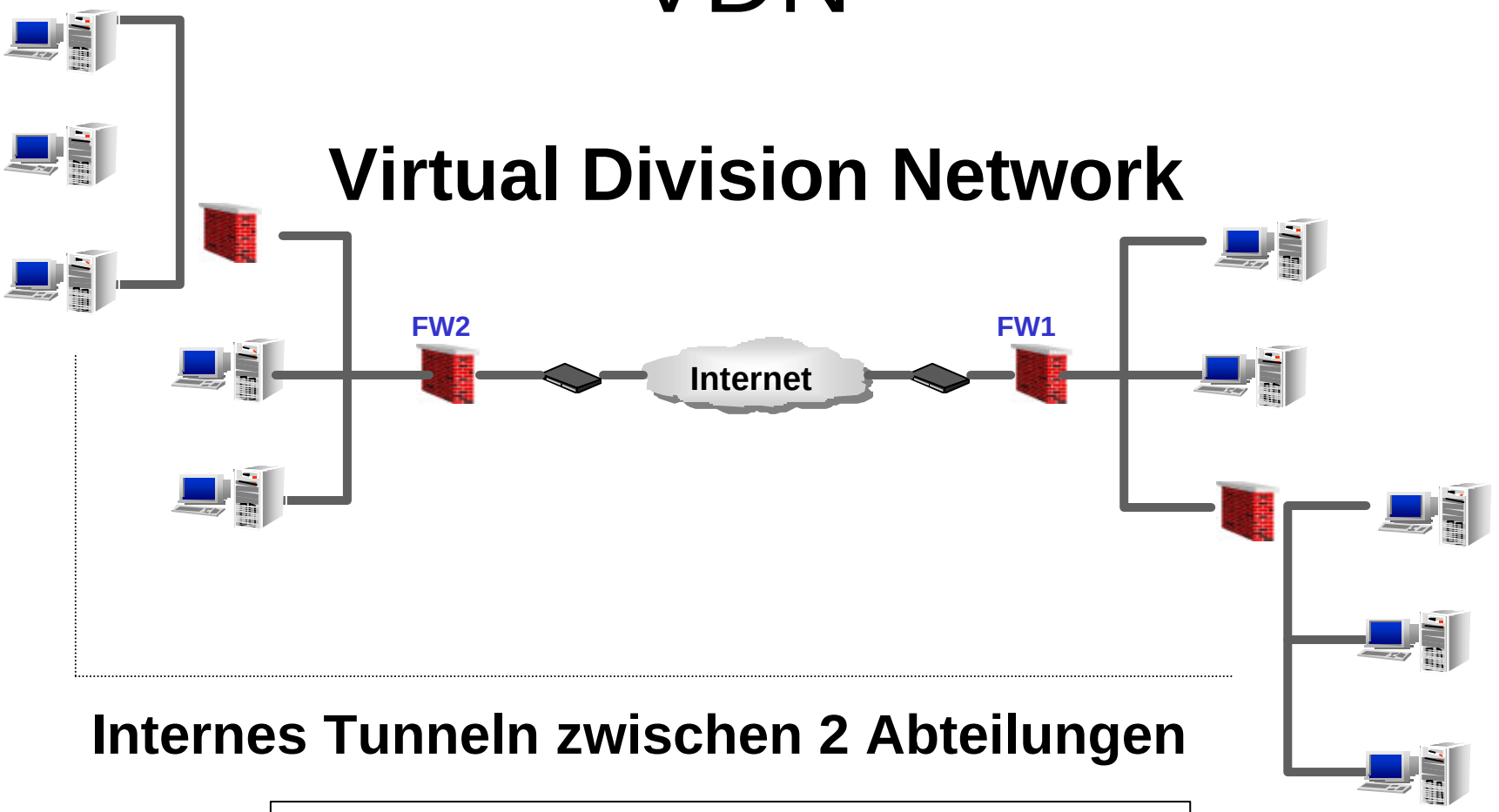


VPN


Internet
Tunnel
Crypt
Filial-LAN
PC
Ethernet
Server
Firmen-LAN
PC
Ethernet
Server

VDN

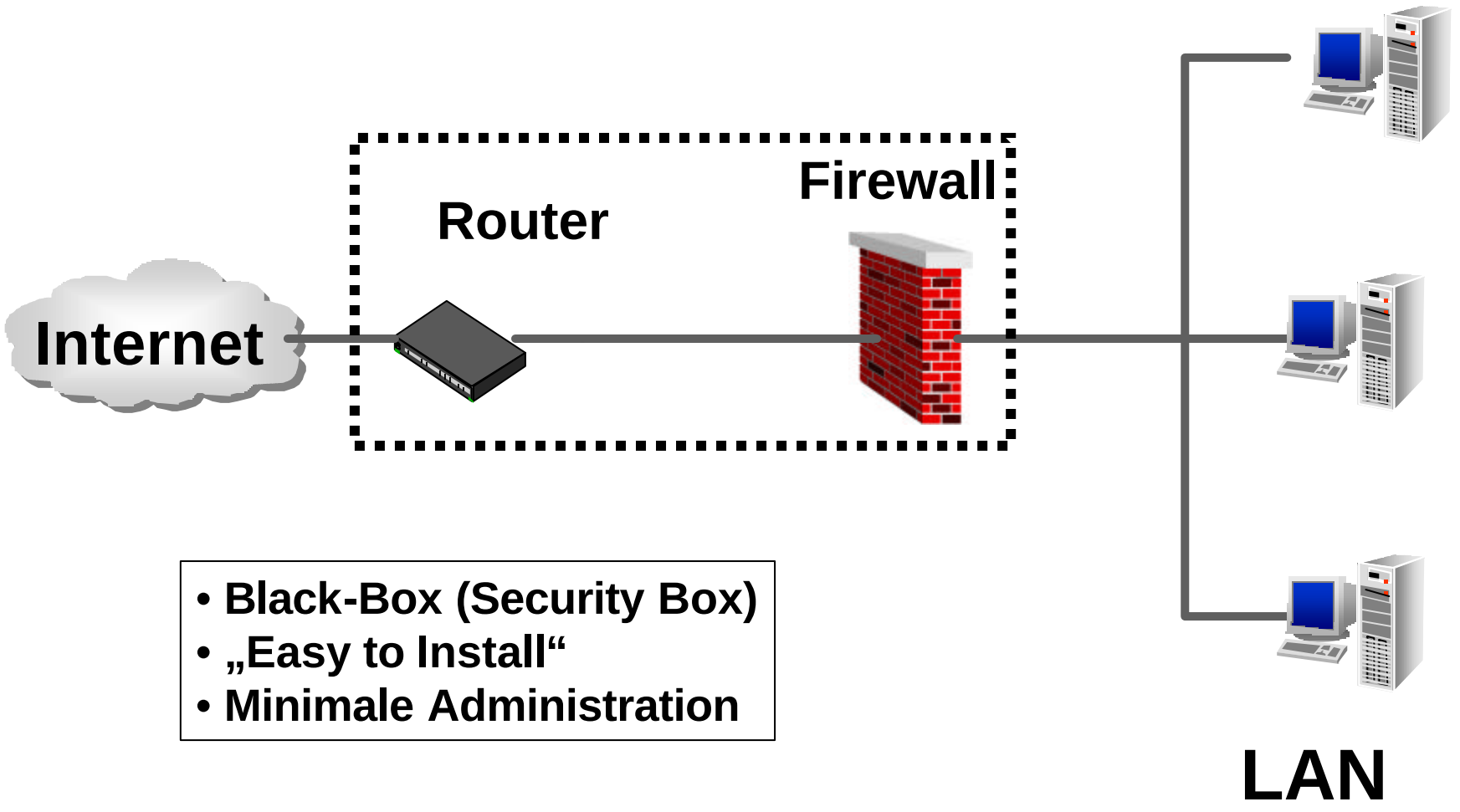
Virtual Division Network



Internes Tunneln zwischen 2 Abteilungen

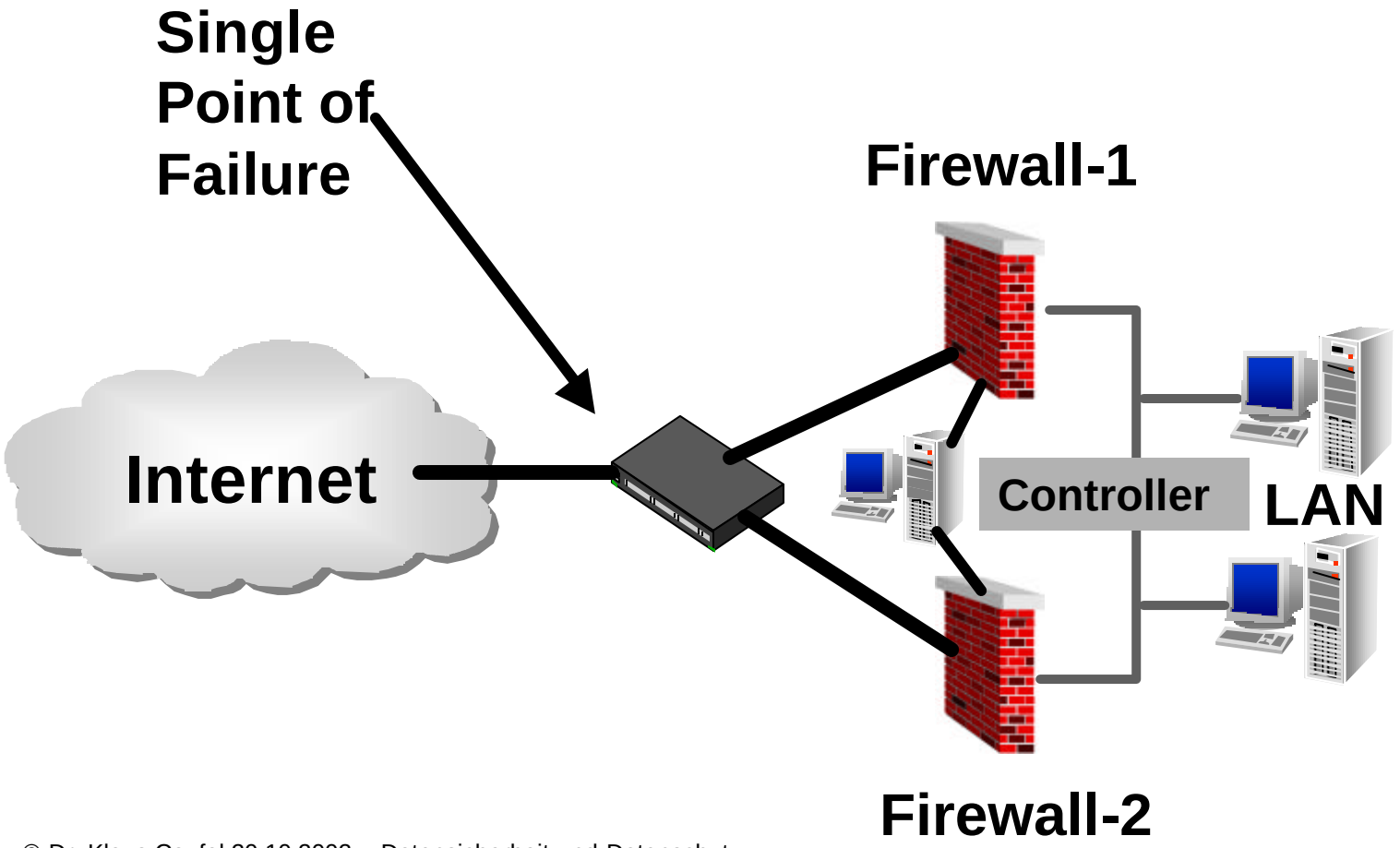
VLAN → VPN → VDN

Appliances



- **Black-Box (Security Box)**
- **„Easy to Install“**
- **Minimale Administration**

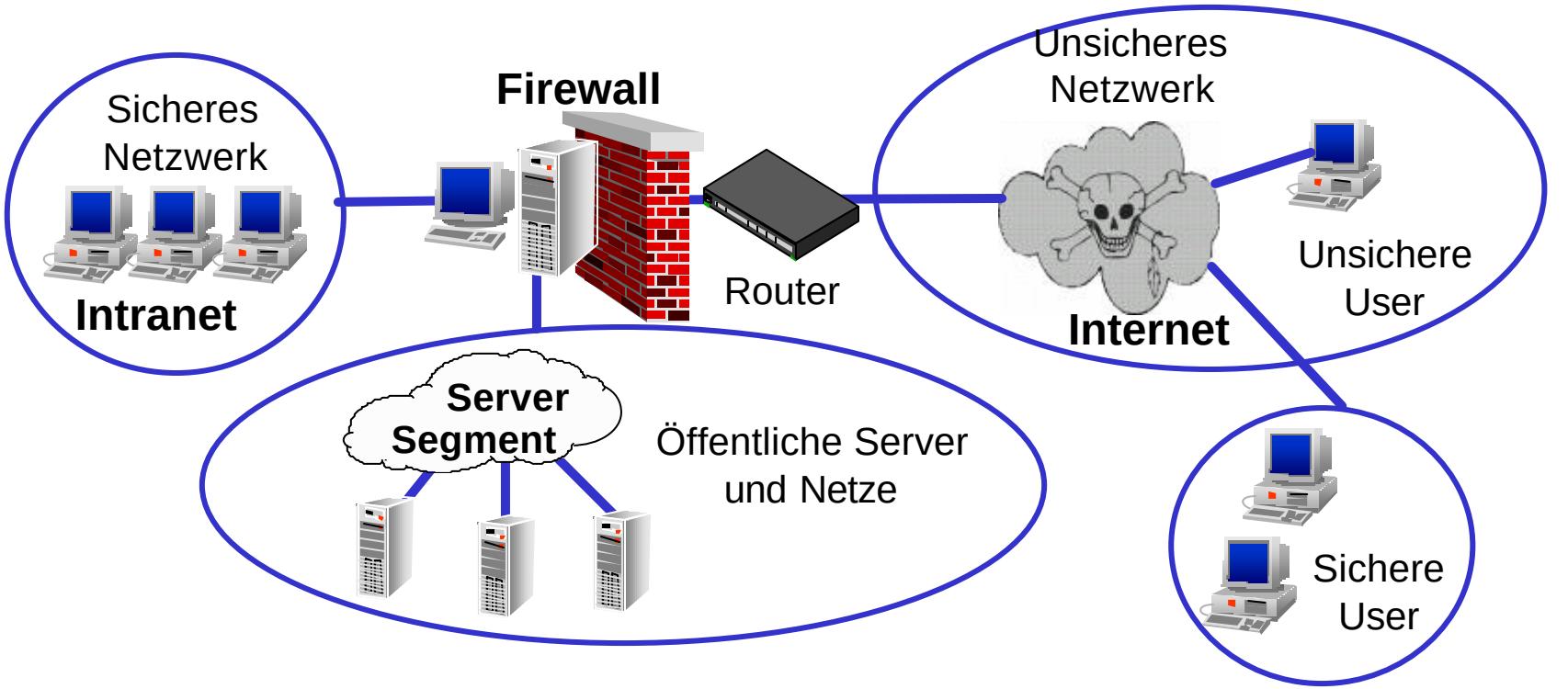
High Availability and Load Balancing



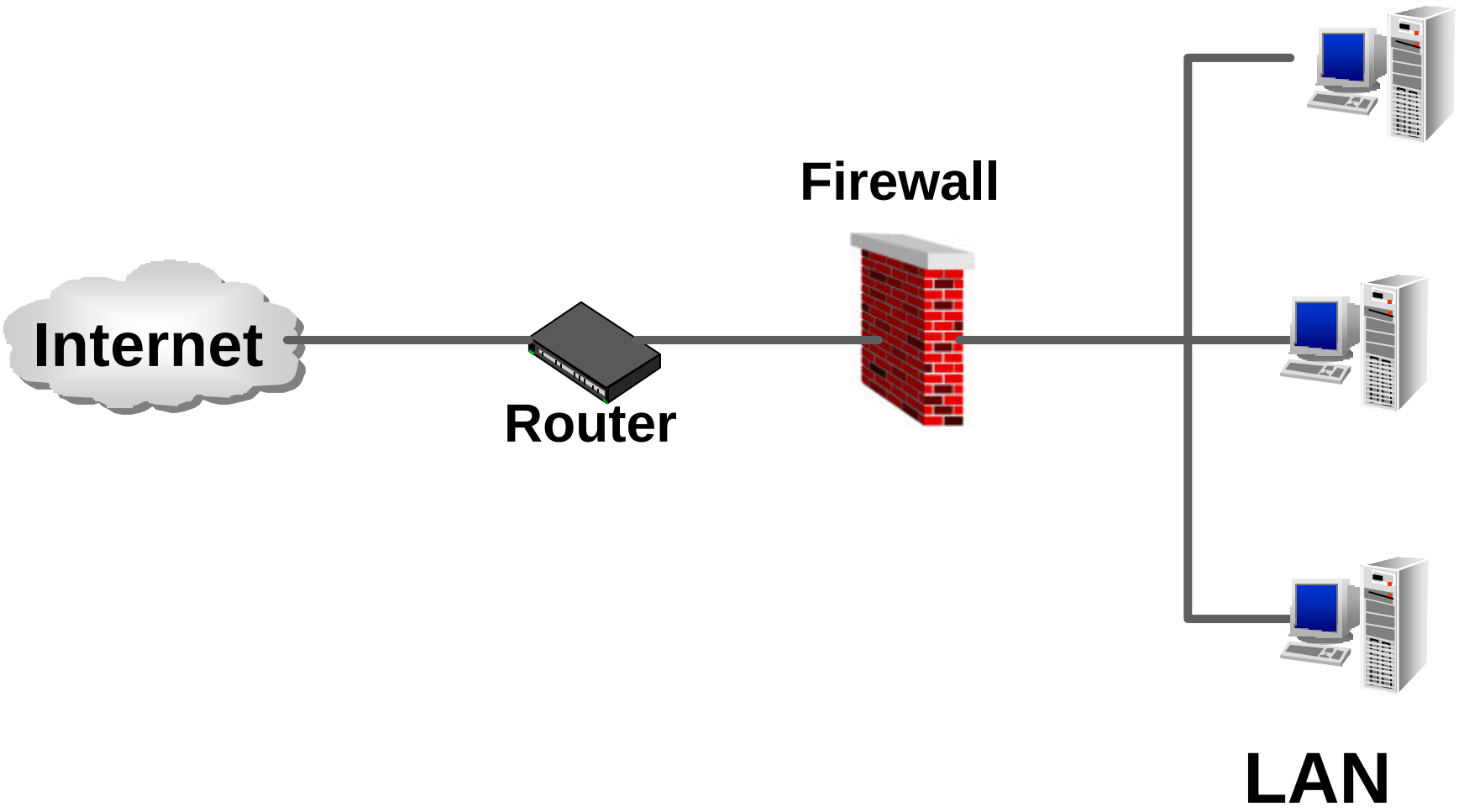
VII.3. Firewalls

- Firewallarchitekturen
- Funktionsweise
  - Application Layer Gateway
  - Packet Filtering
  - Stateful Inspection

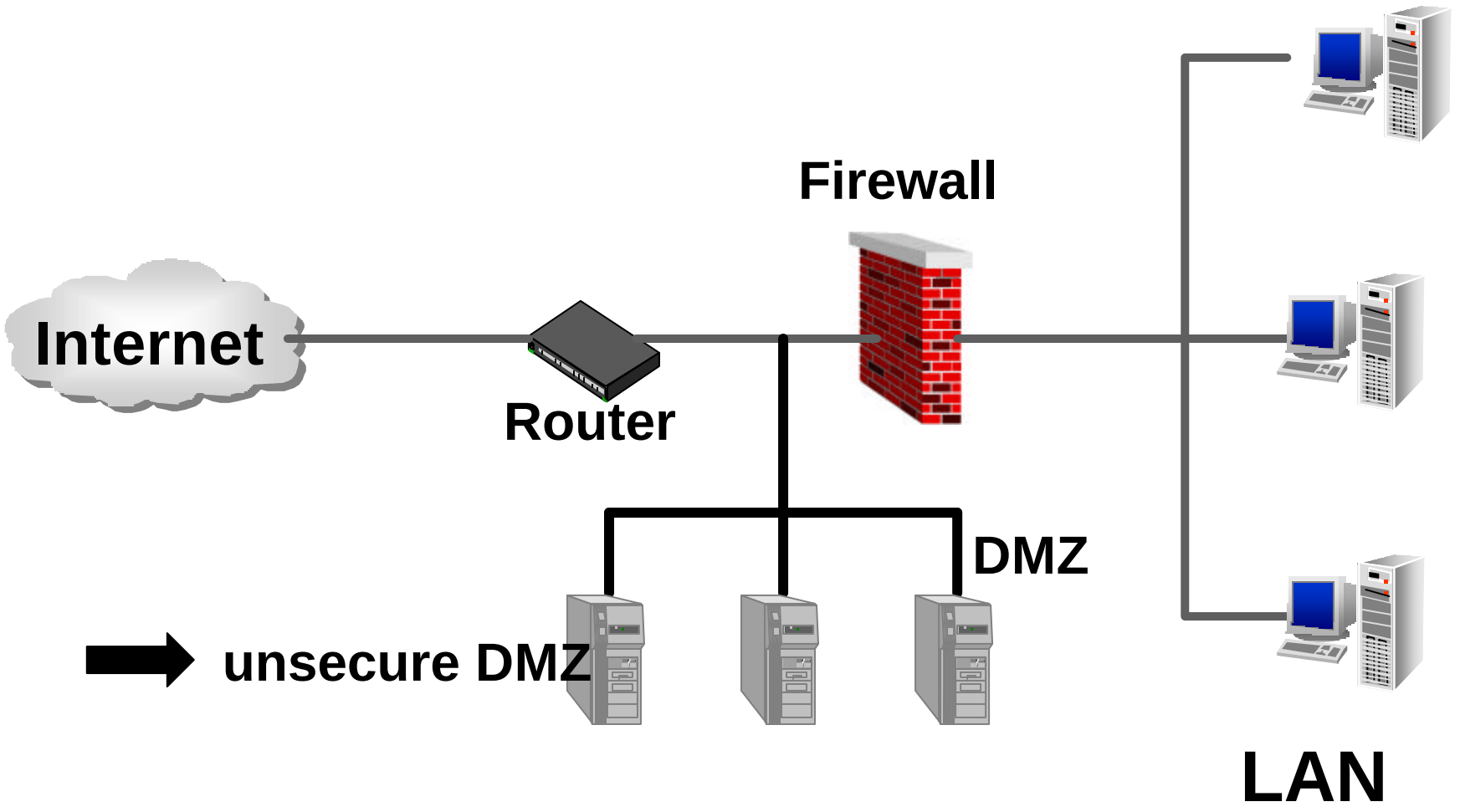
Standardposition der Firewall



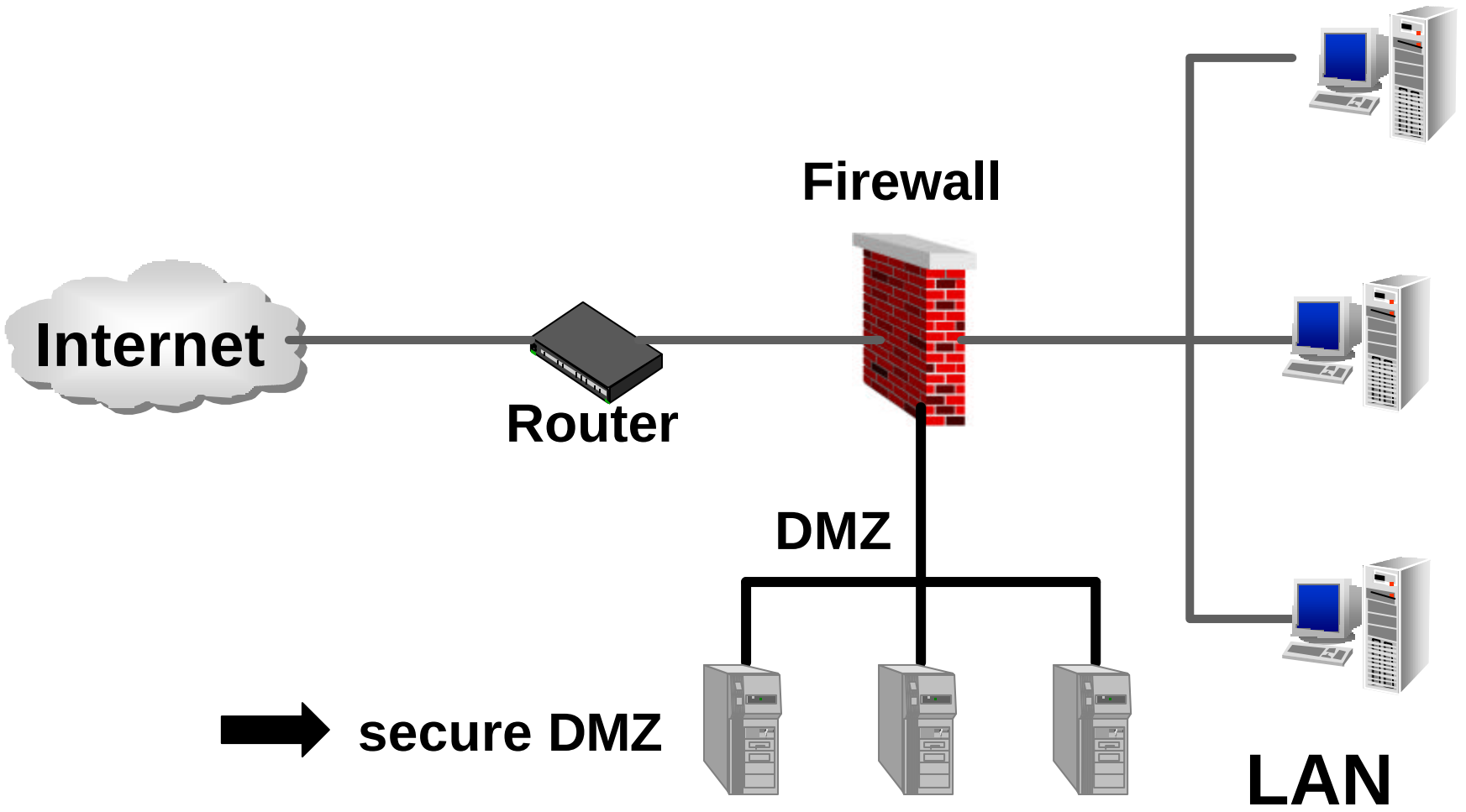
Single Firewall



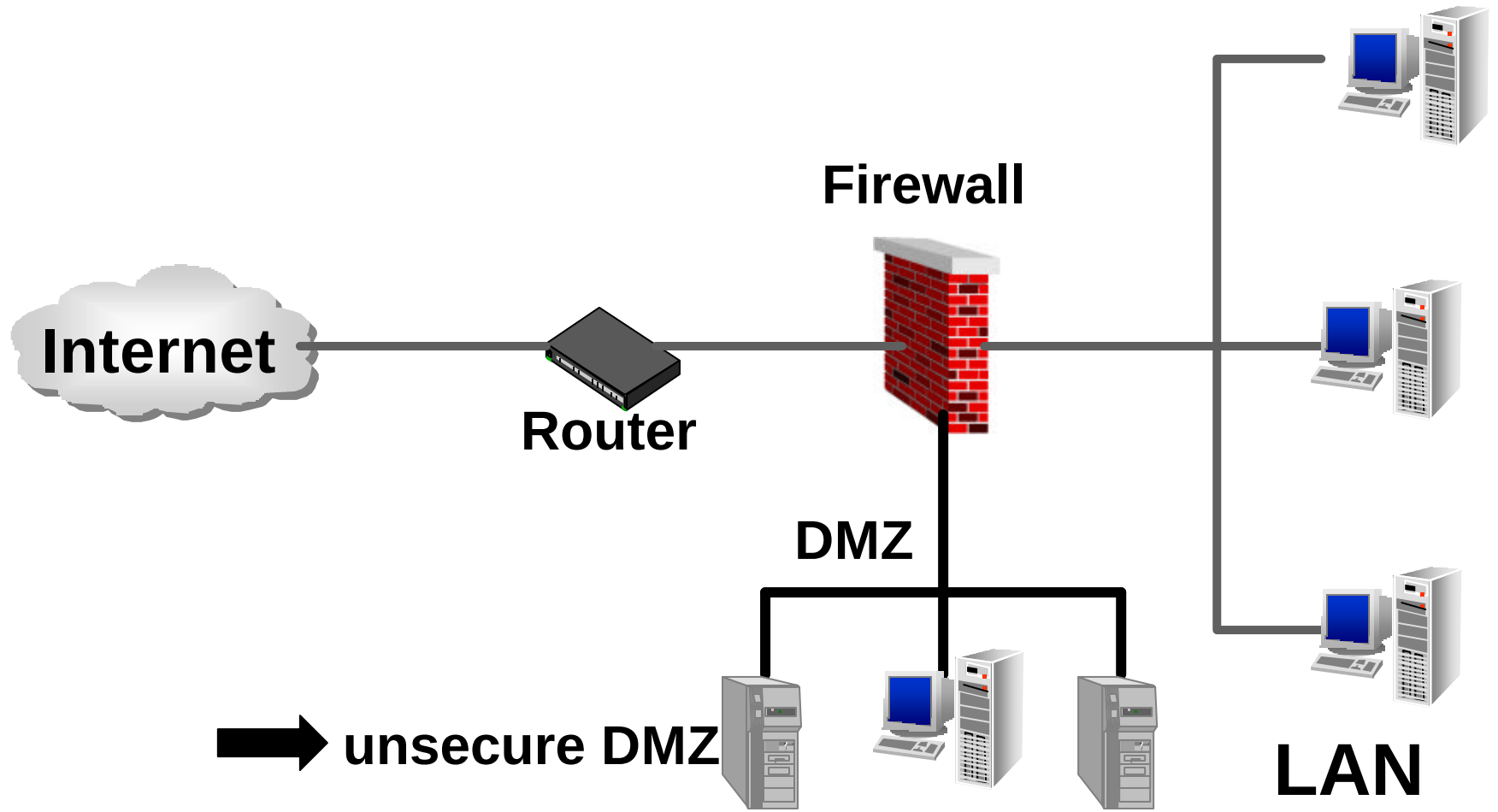
Unsecure DMZ



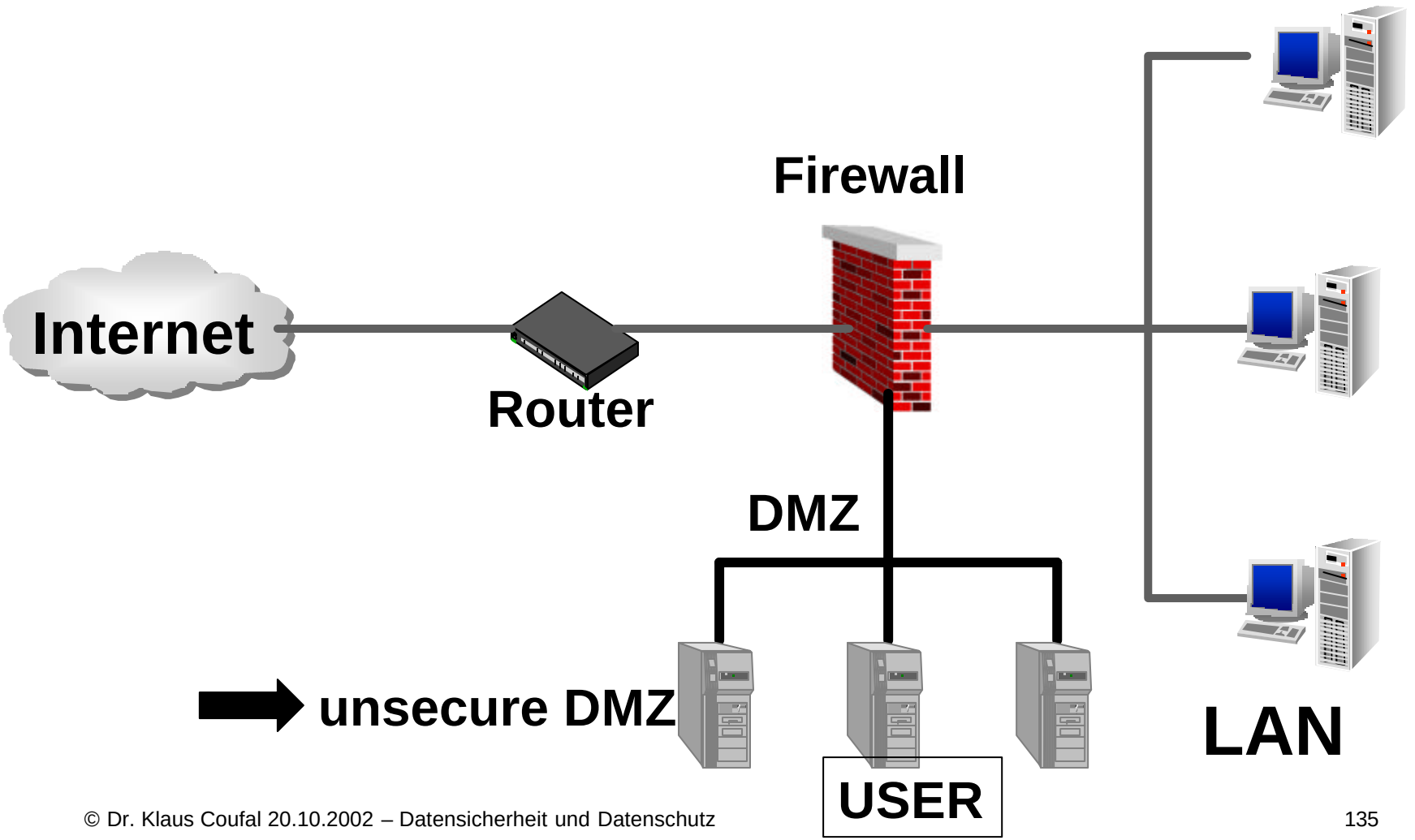
Secure DMZ



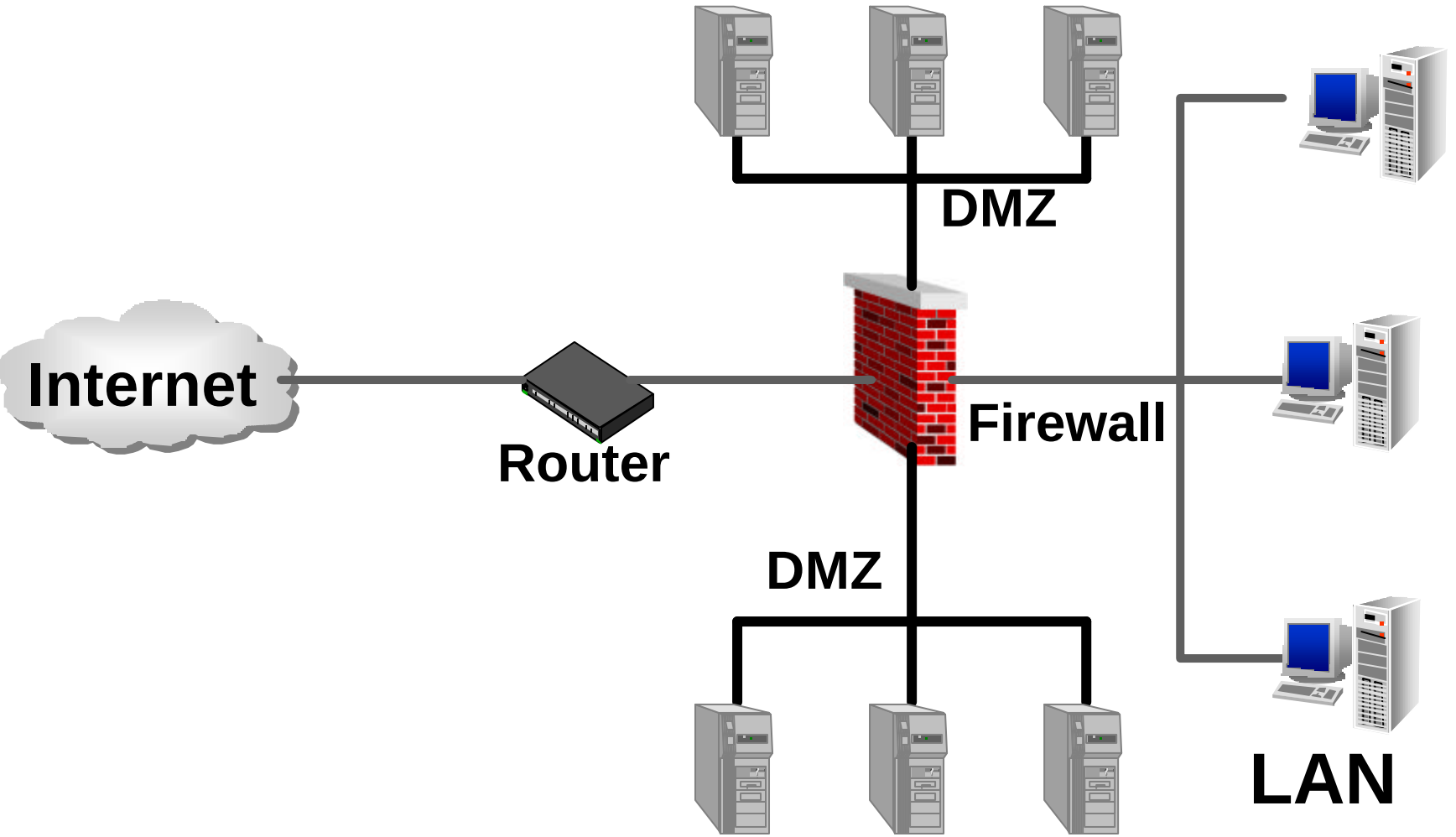
Unsecure DMZ 2



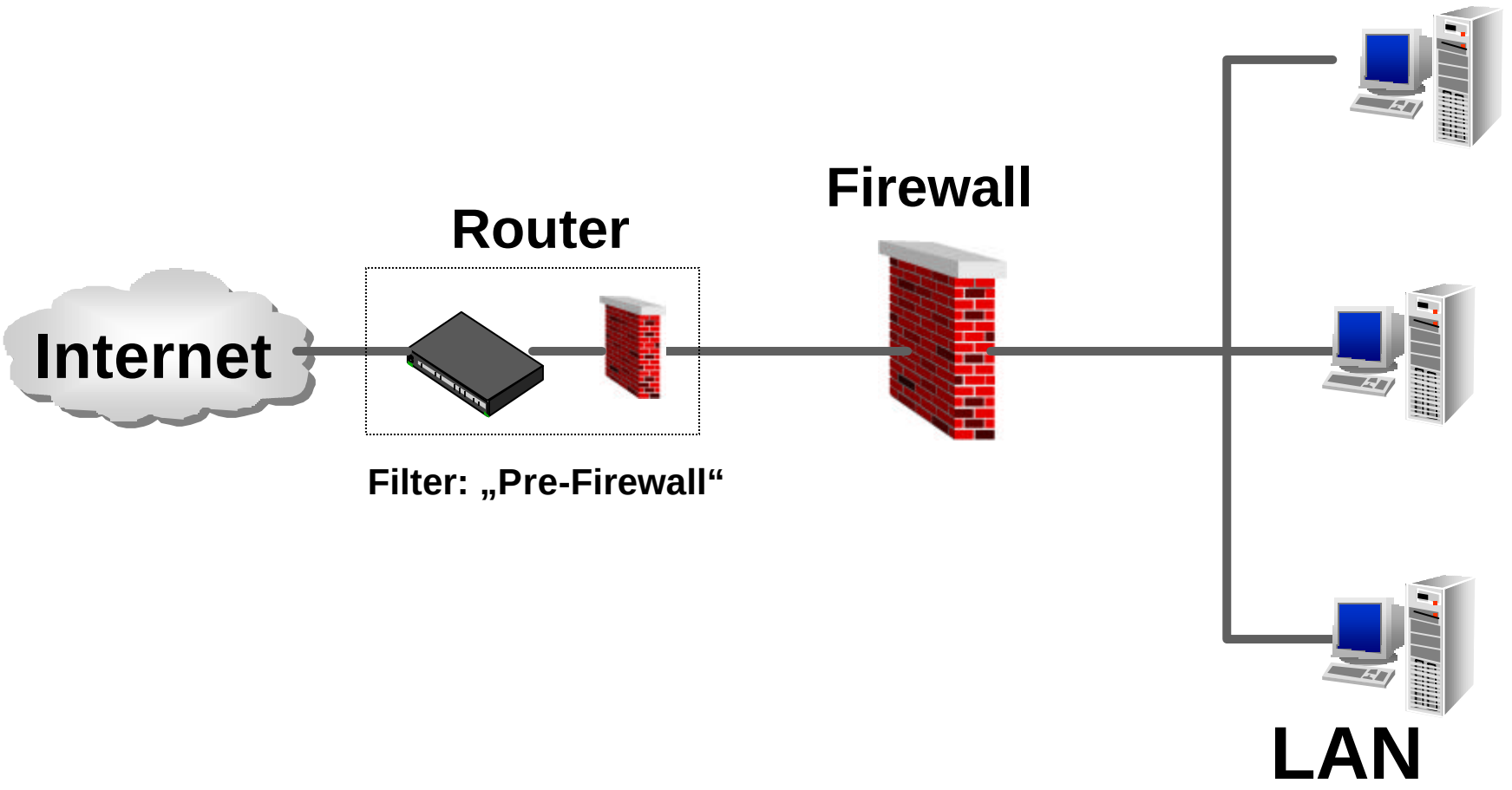
Unsecure DMZ 3



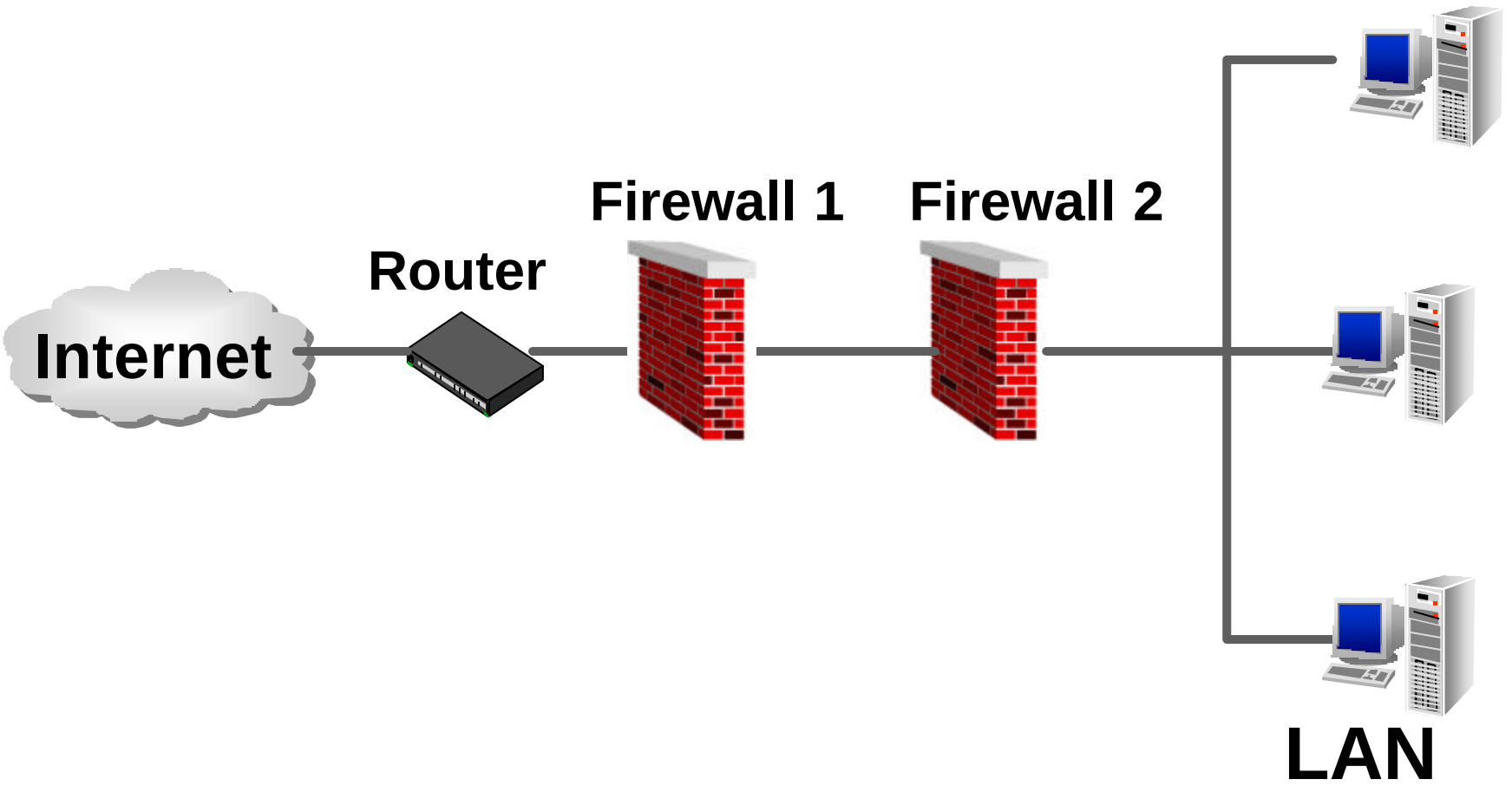
Multiple DMZ



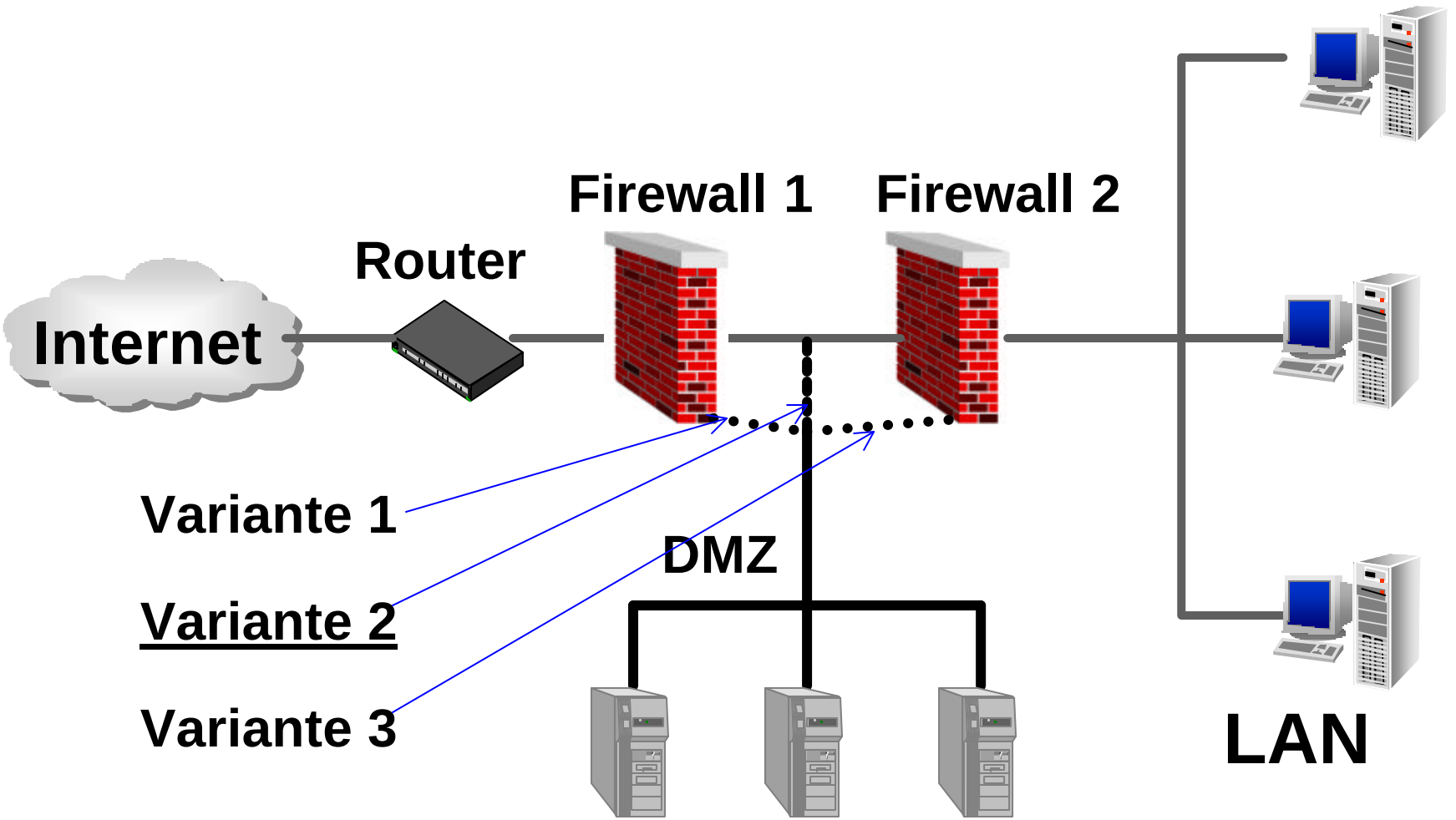
Router als Filter



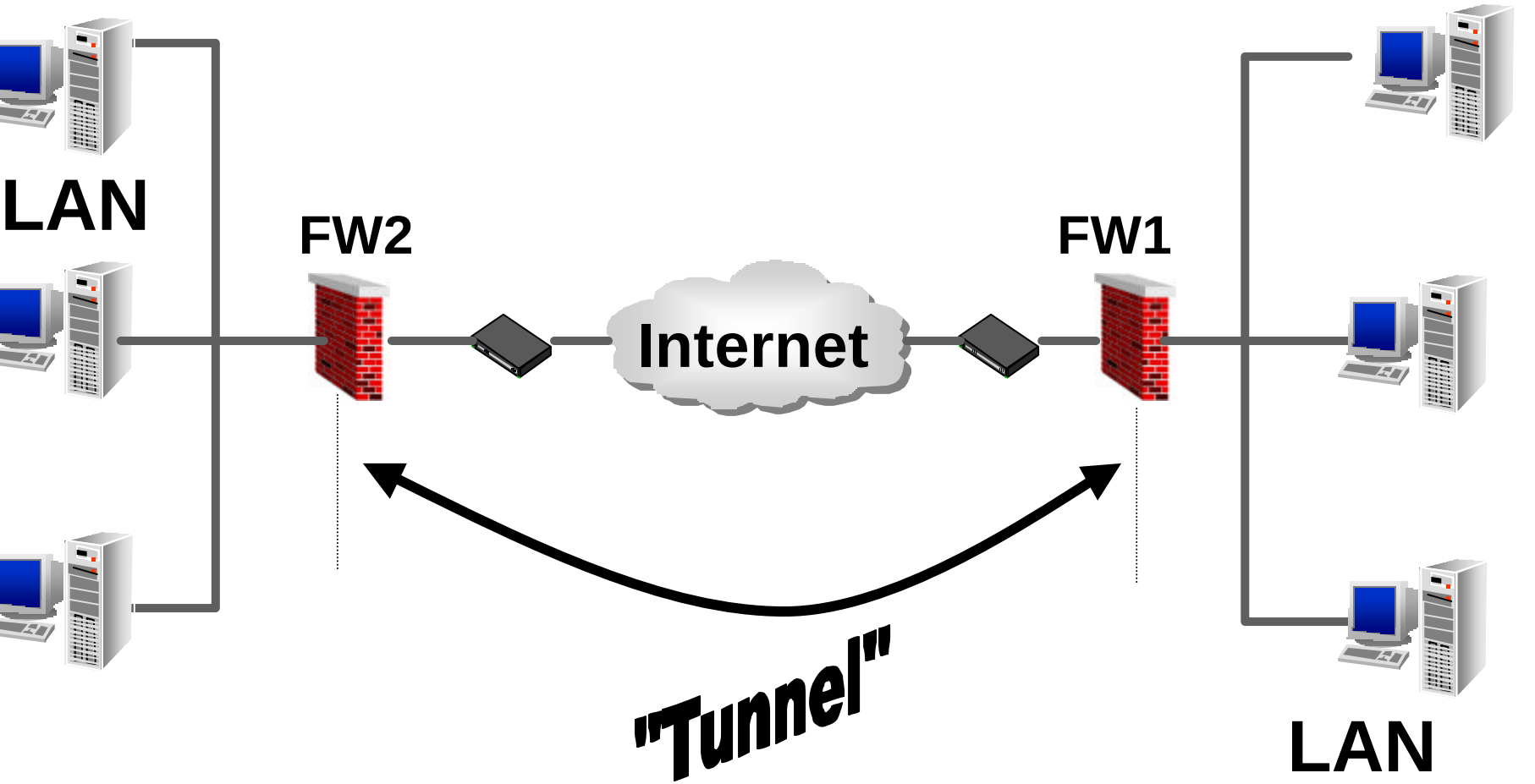
Dual Firewall



Dual Firewall mit DMZ

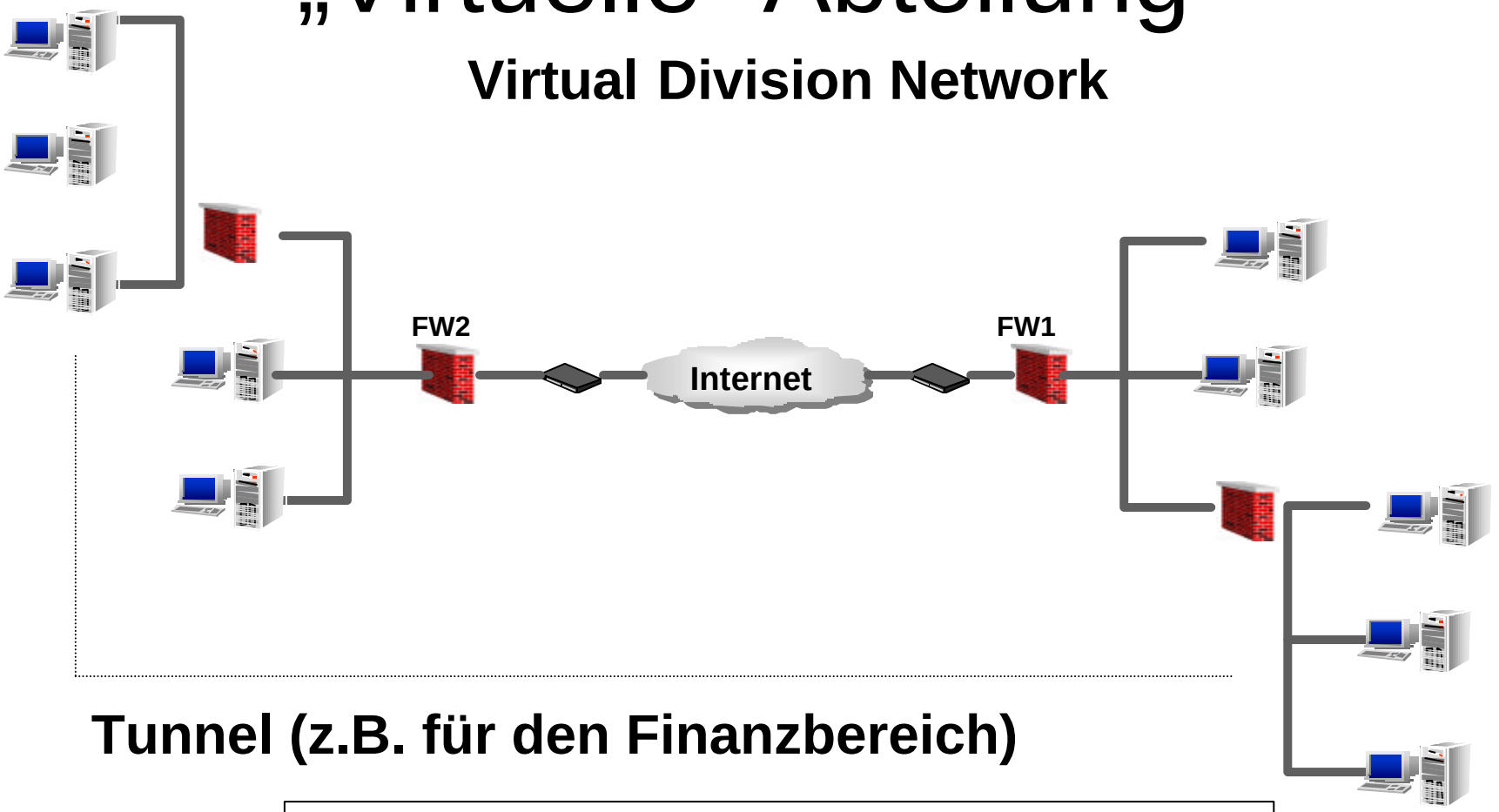


Single Firewall mit Tunnel



„Virtuelle“ Abteilung

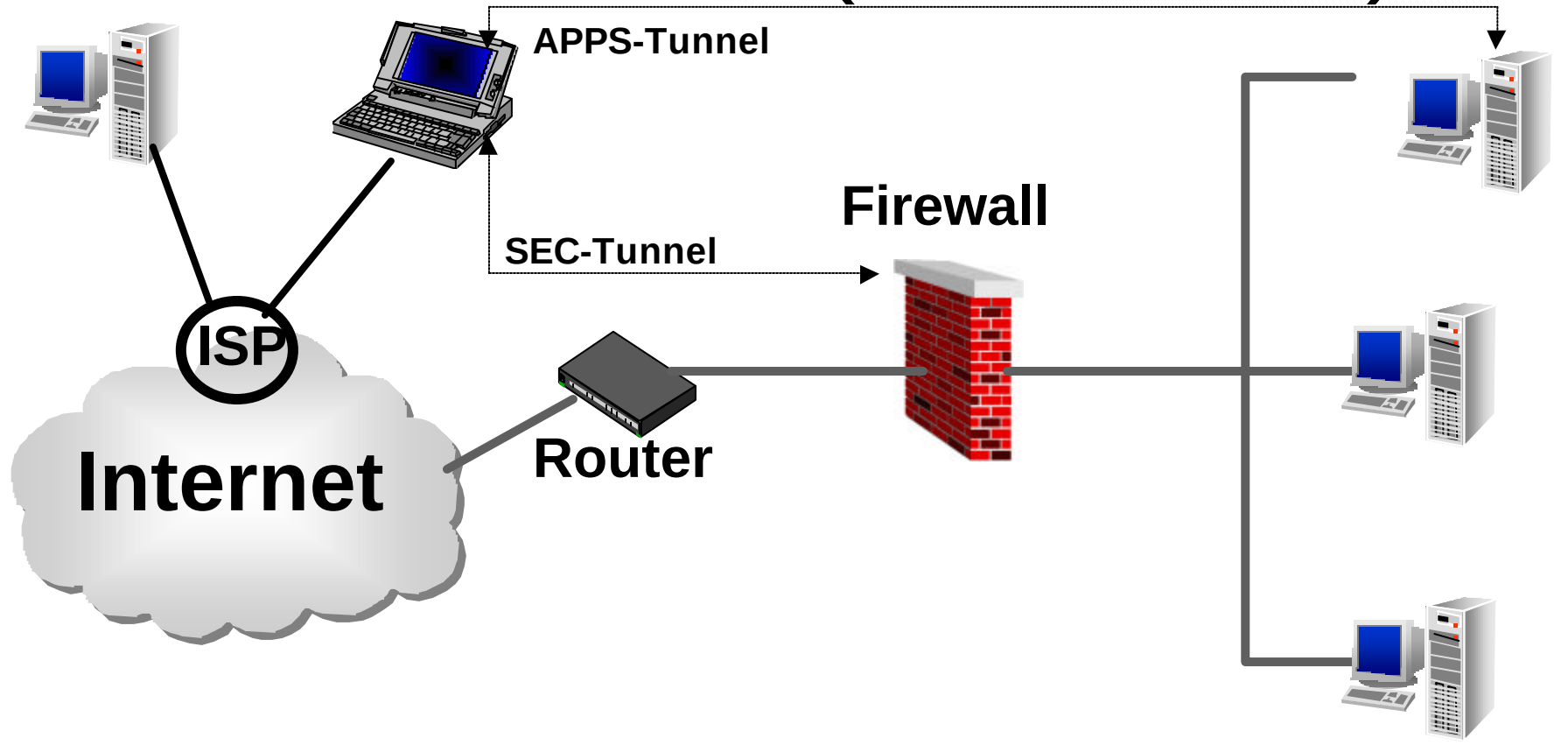
Virtual Division Network



Tunnel (z.B. für den Finanzbereich)

Vom VLAN über VPN bis VDN

Remote User (Teleworker)

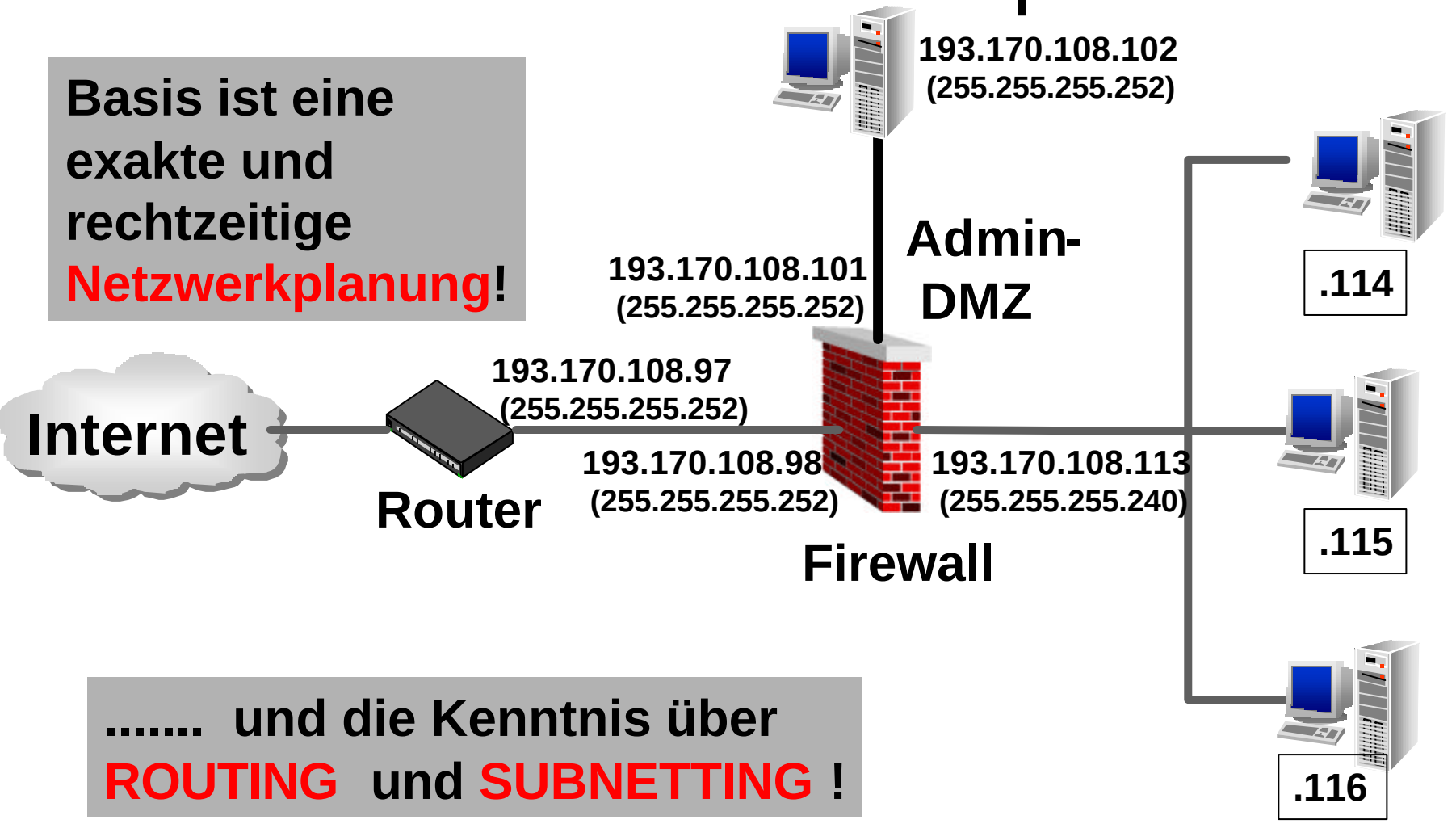


- **Remote-User: z.B. SOHO**
- **Teleworker: „Mobile-Users“**

Firmen LAN

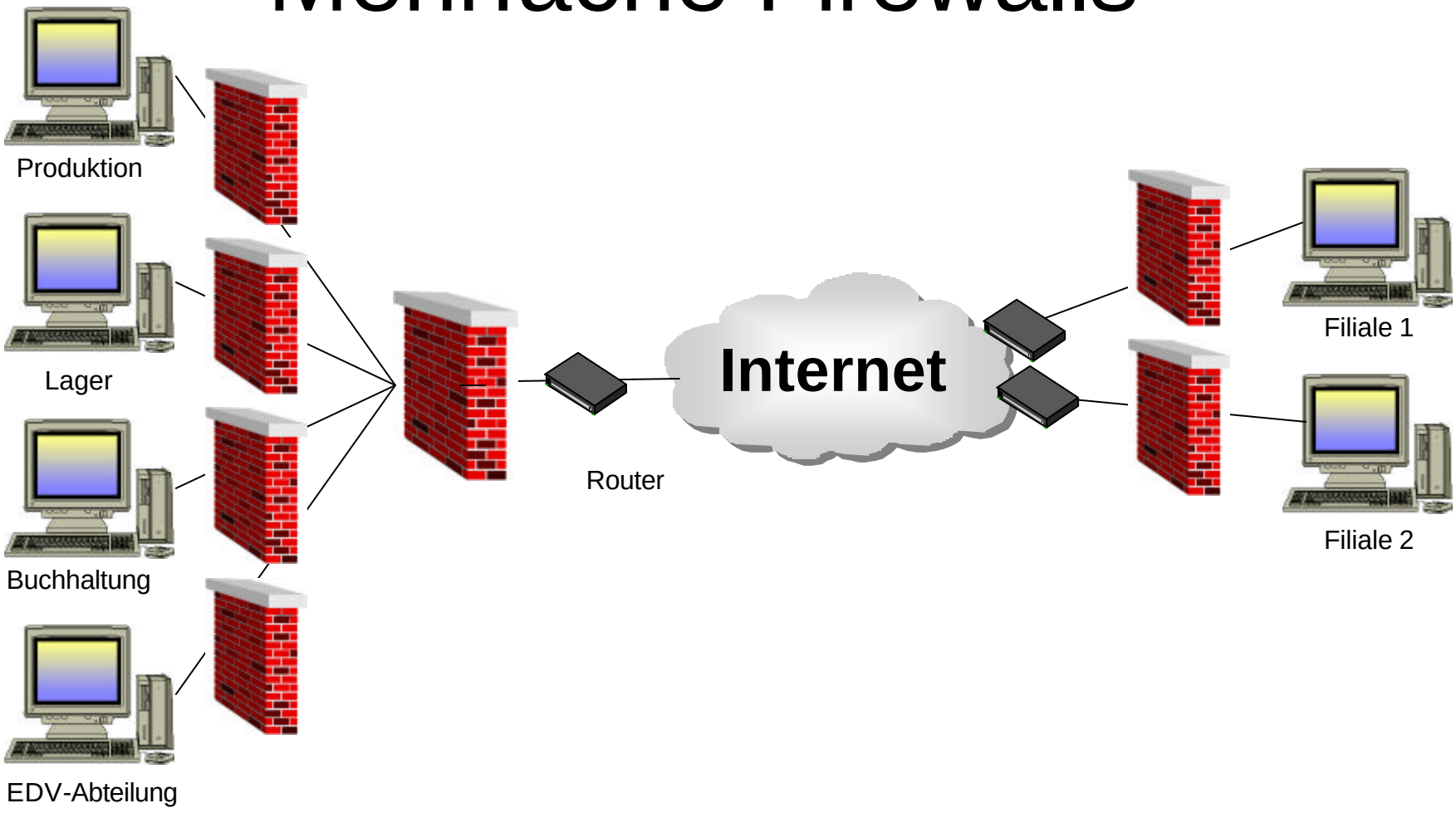
Praktisches Beispiel

Basis ist eine exakte und rechtzeitige Netzwerkplanung!

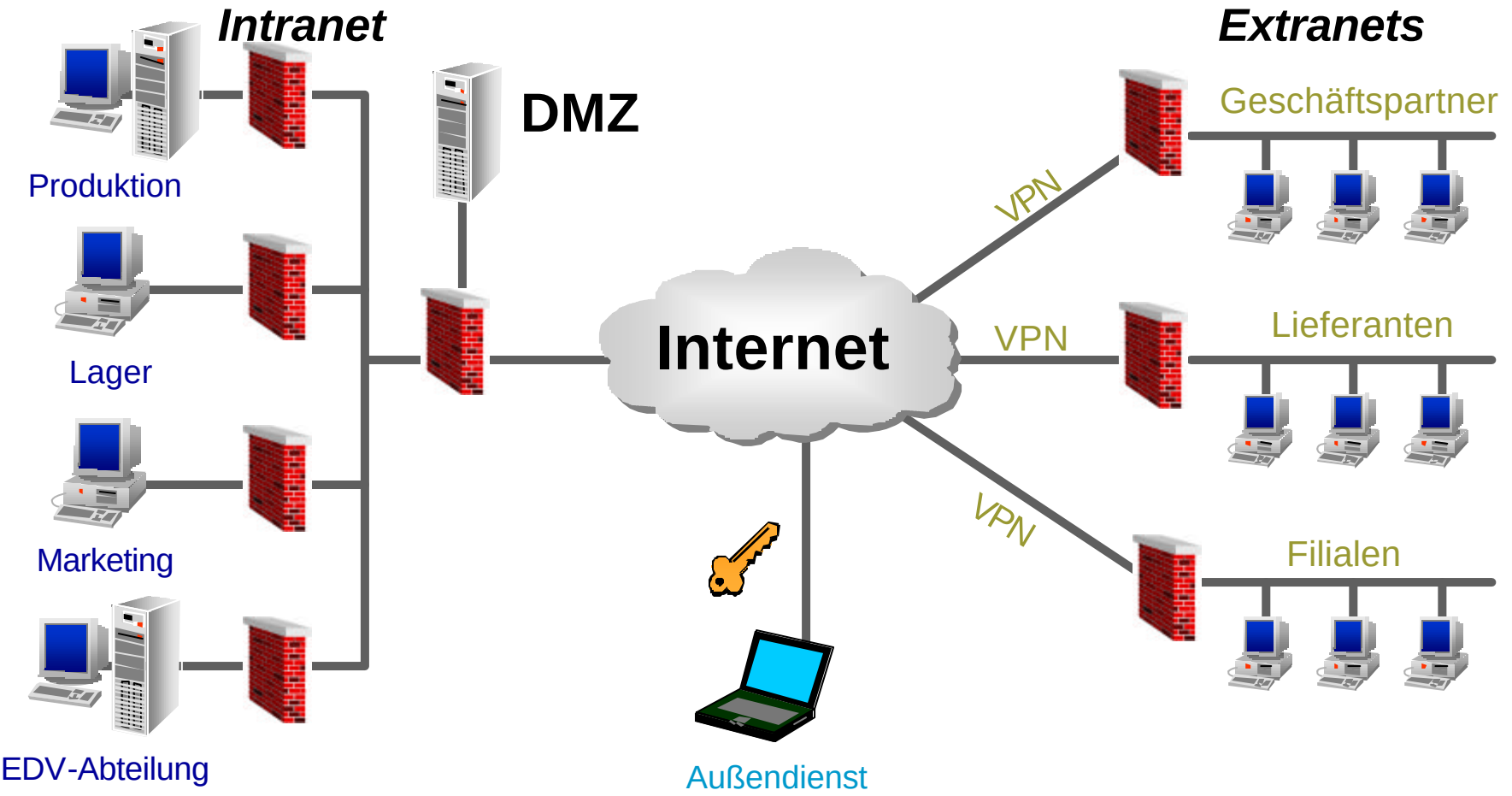


..... und die Kenntnis über ROUTING und SUBNETTING !

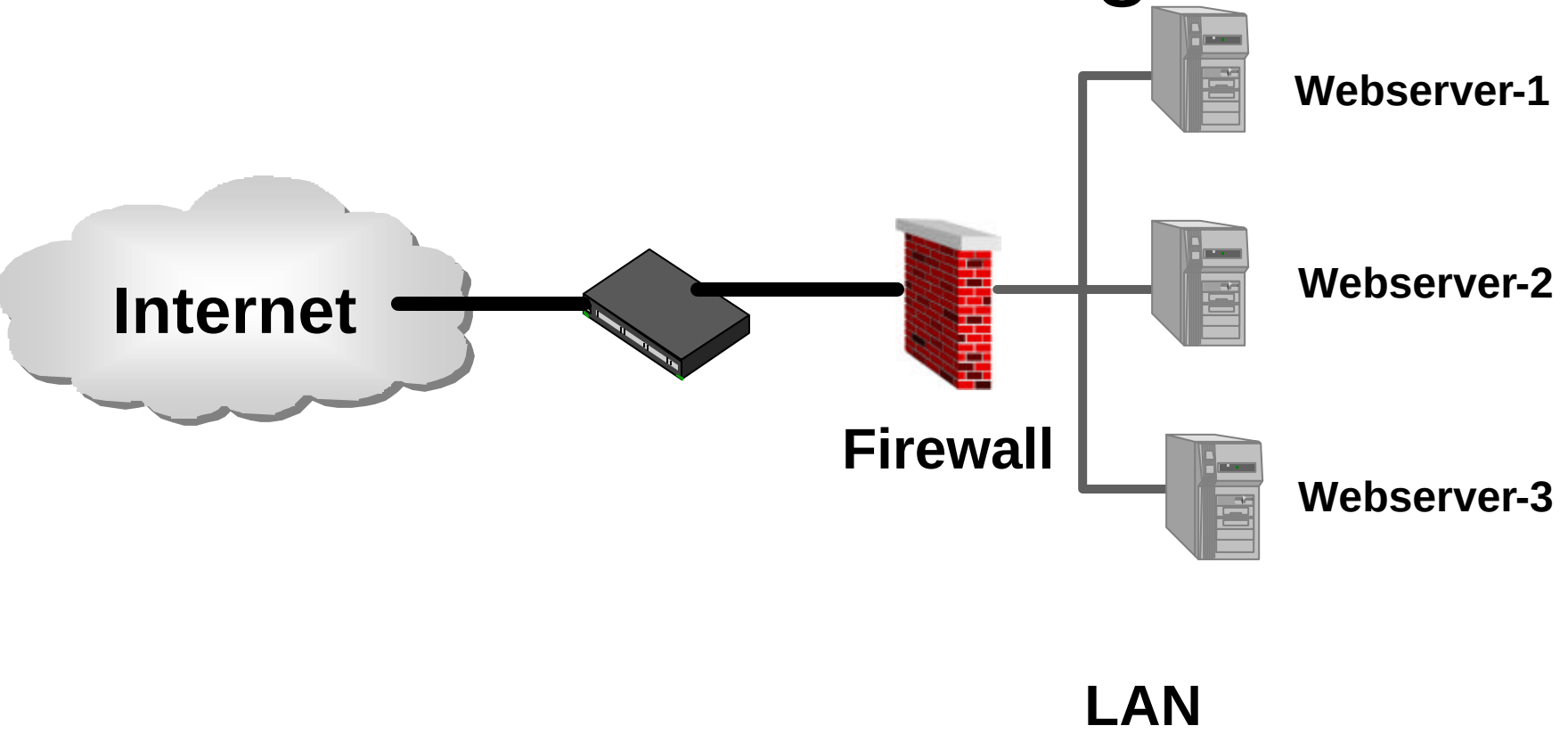
Mehrfache Firewalls



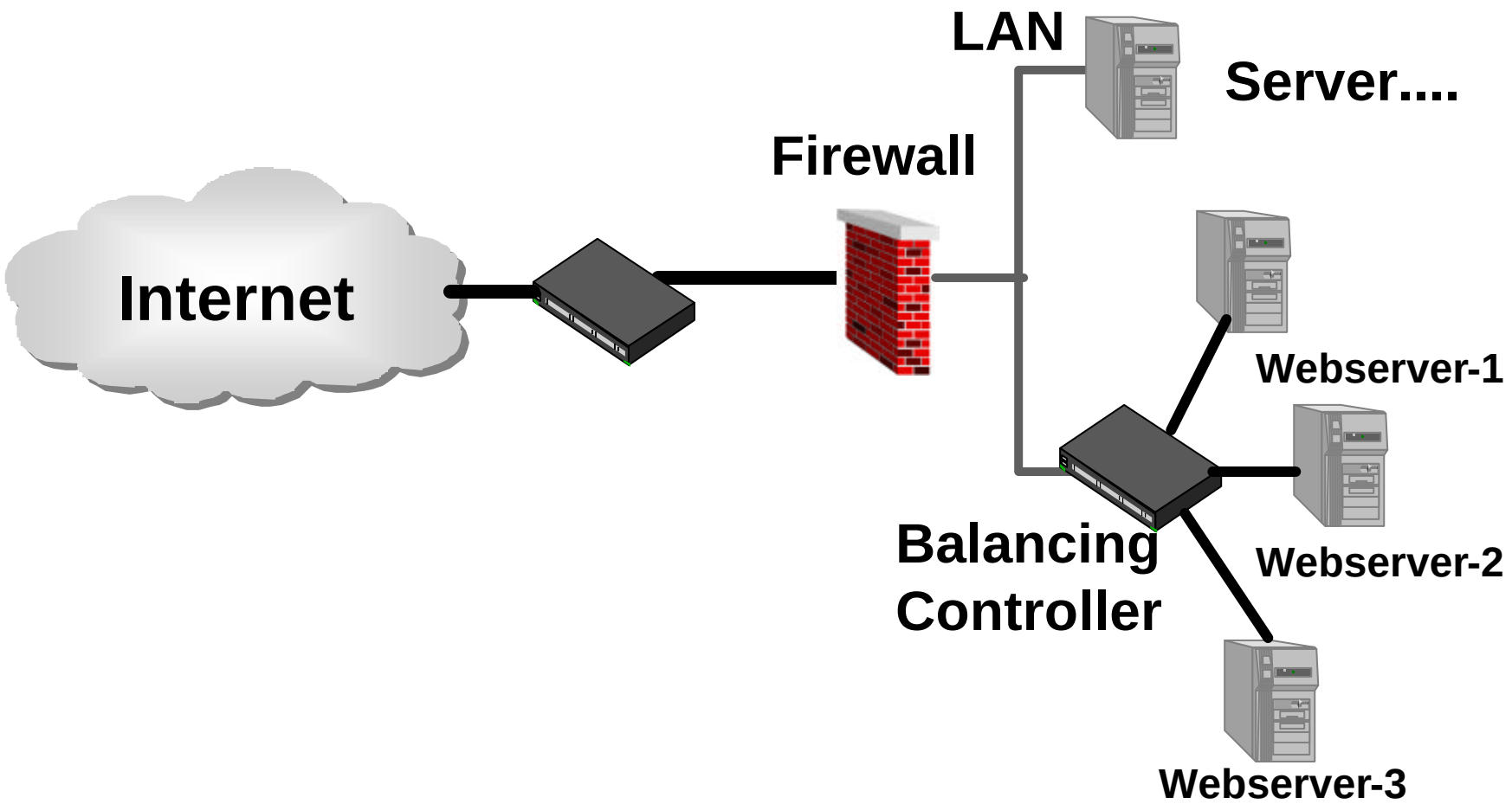
Enterprise Security



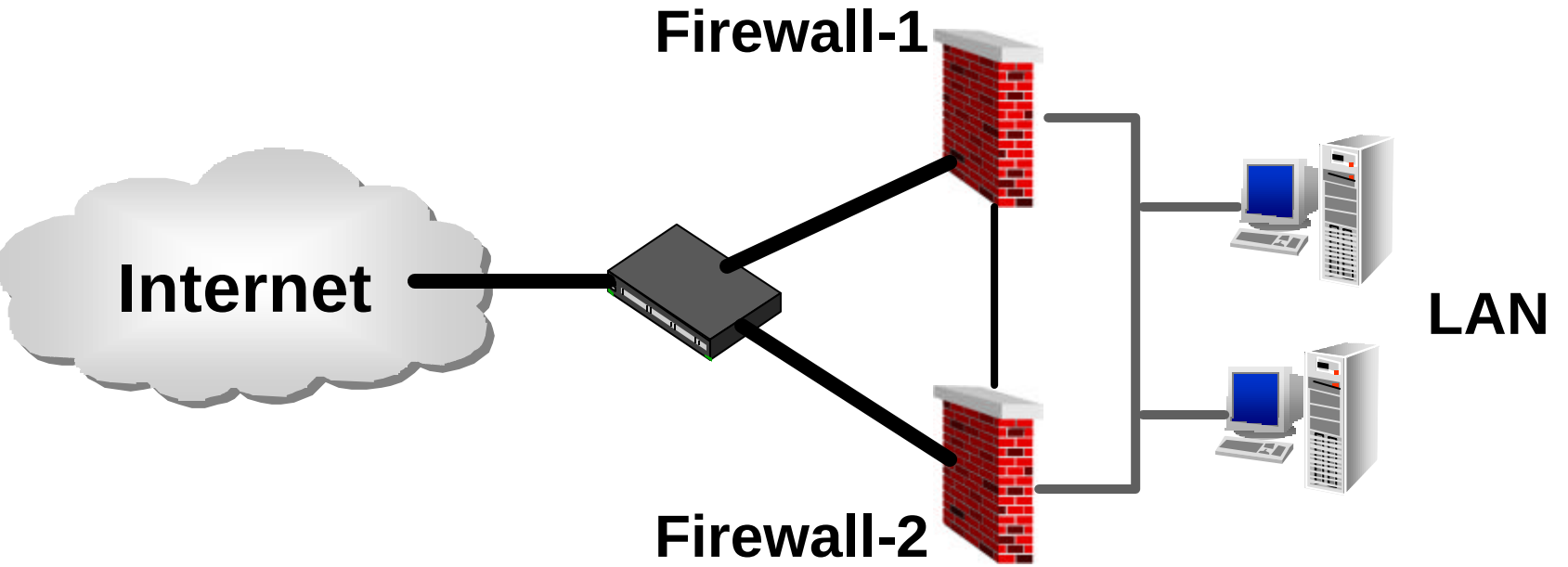
Spezialkonfiguration: Loadbalancing



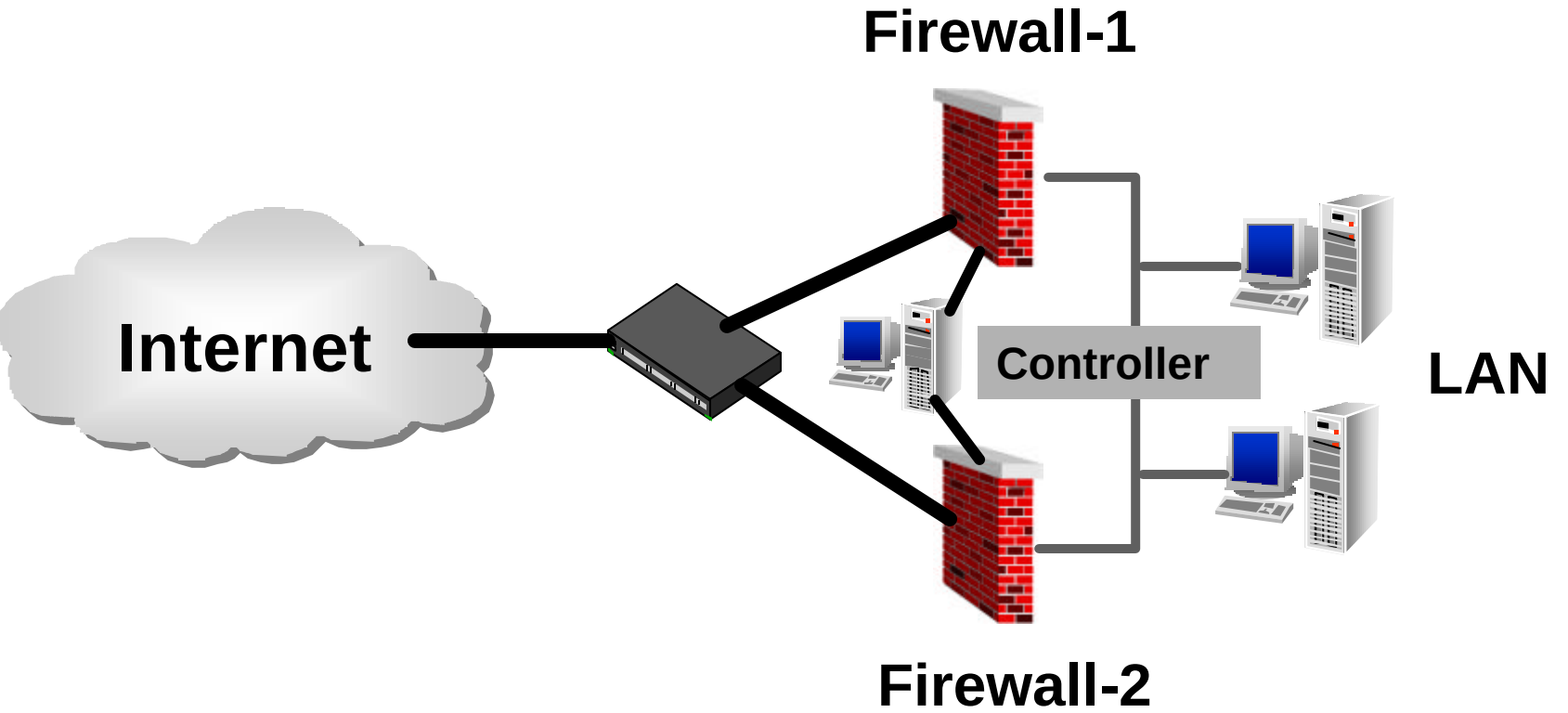
Loadbalancing 2



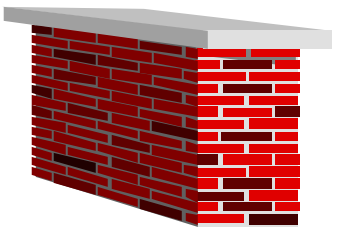
Loadbalancing 3



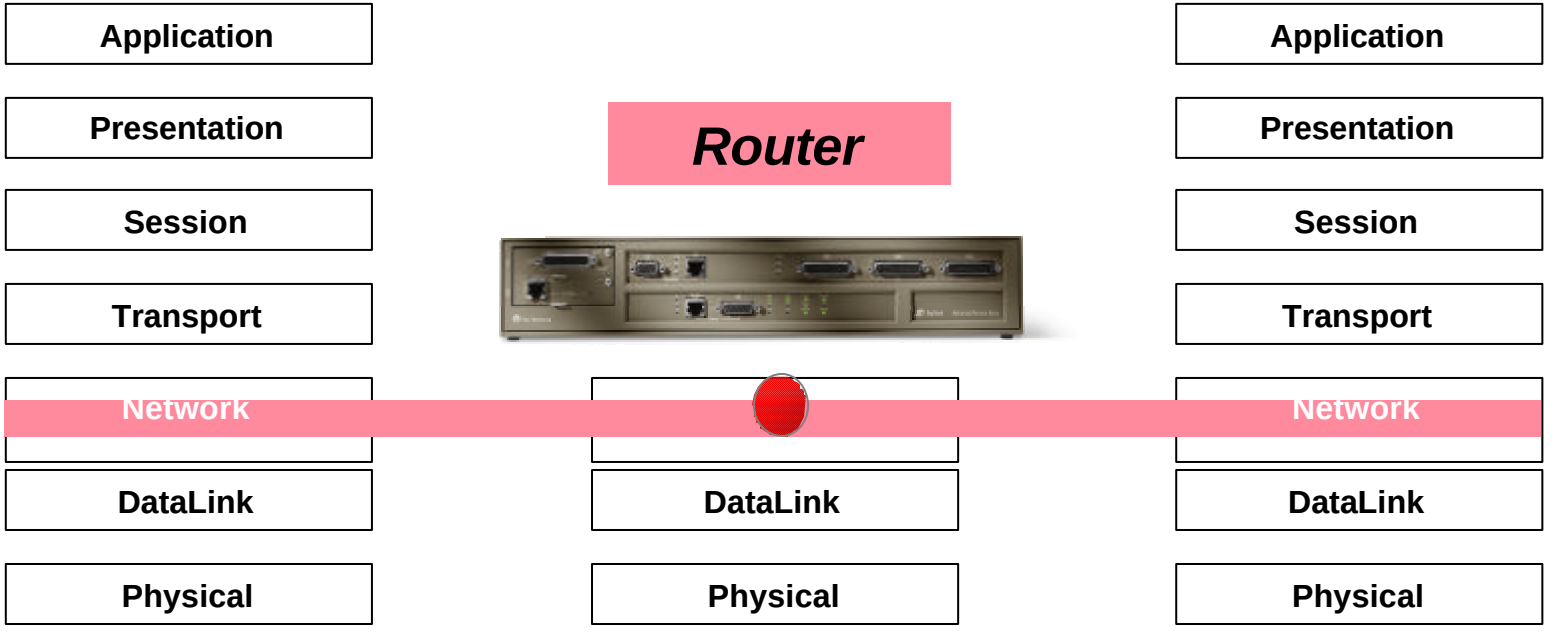
Loadbalancing 4



Firewall Funktionsweise

Application	**Application Layer Gateway**
Presentation	
Session	
Transport	
Network	**Packet Filtering**
	**Stateful Inspection Engine**
Data Link	
Physical	

Packet Filter (Überwachungsrouter)



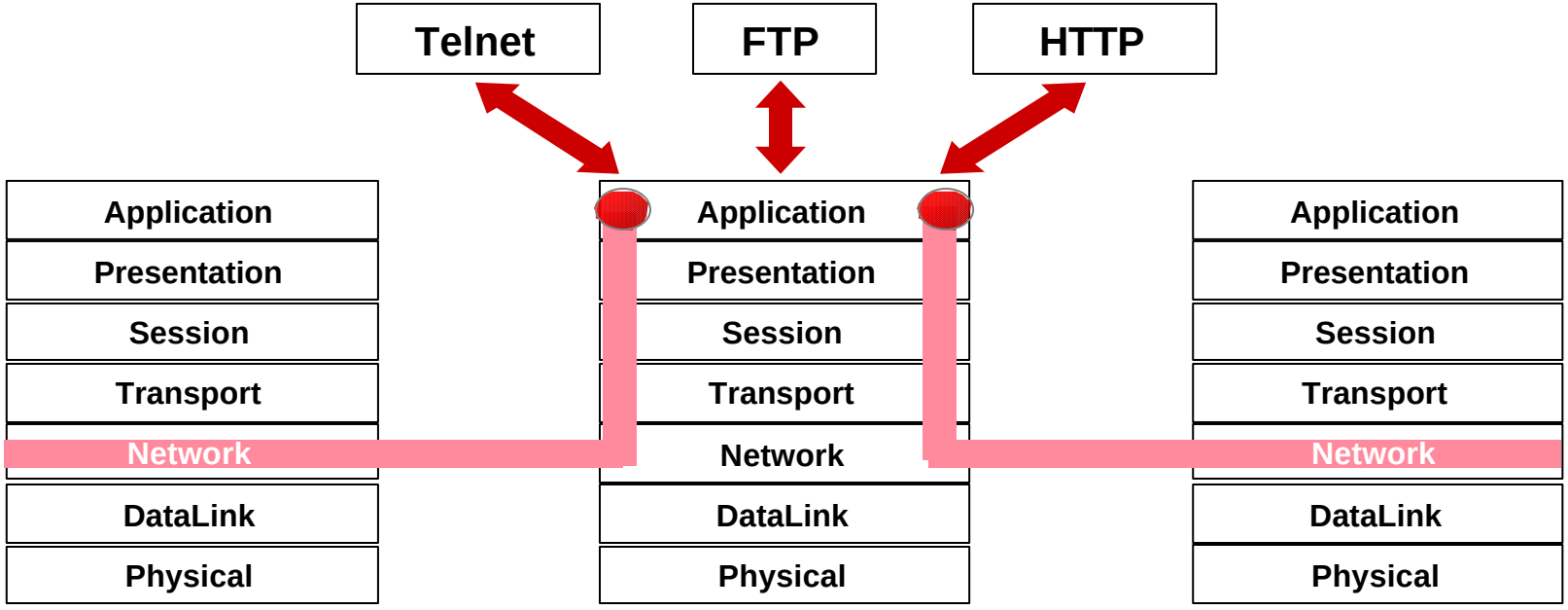
Vorteile:

- Einfach und billig
- Transparent für Applikationen

Nachteile:

- Geringe Security
- IP-Spoofing möglich
- ACLs schwer realisierbar
- Nicht erweiterbar

Application Layer Gateway



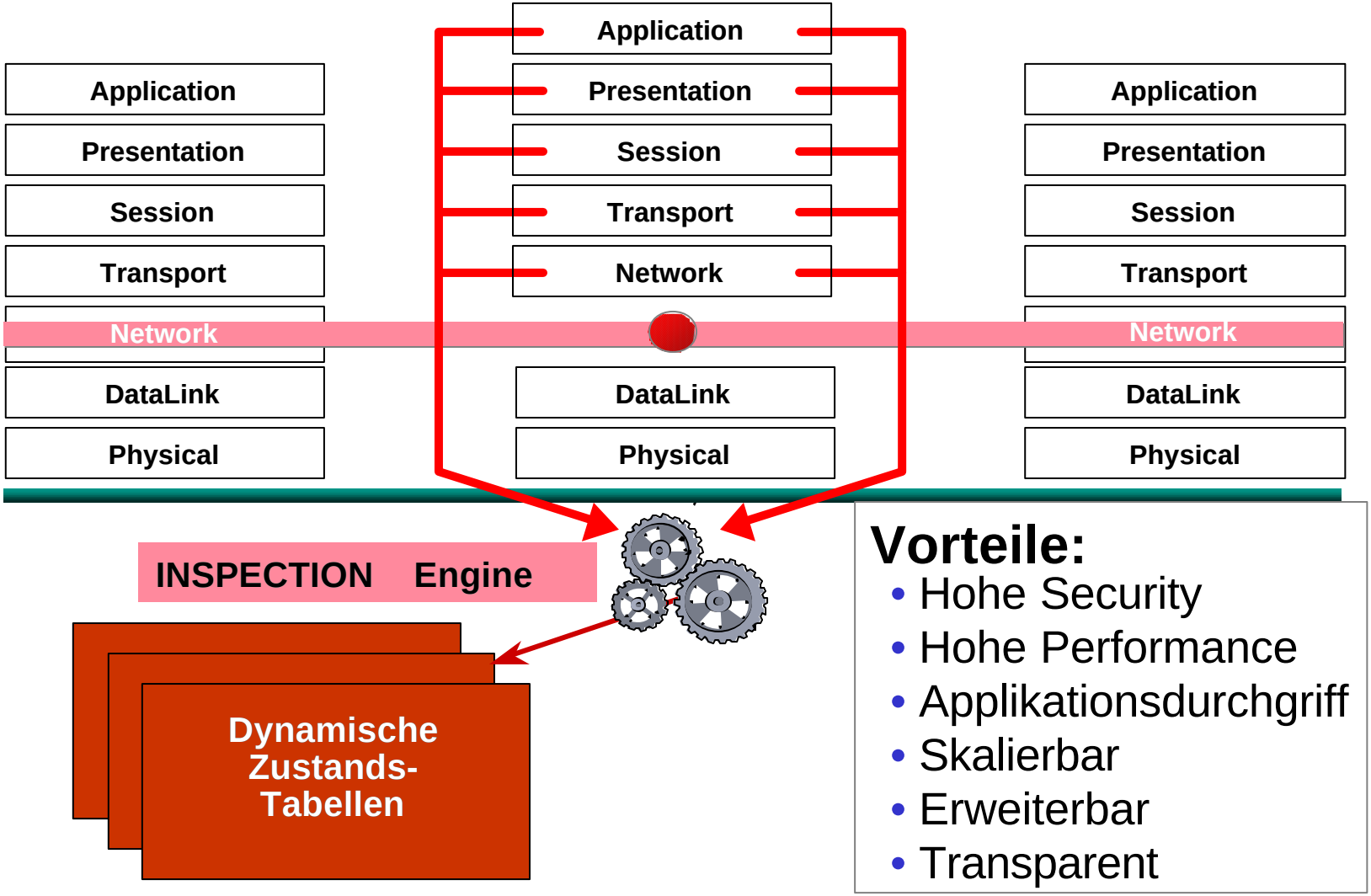
Vorteile:

- Hohe Sicherheit
- Im Bereich der Applikationen

Nachteile:

- Schwache Performance
- Nicht Transparent
- Schwer Skalierbar
- Eingeschränkte Applikationsunterstützung

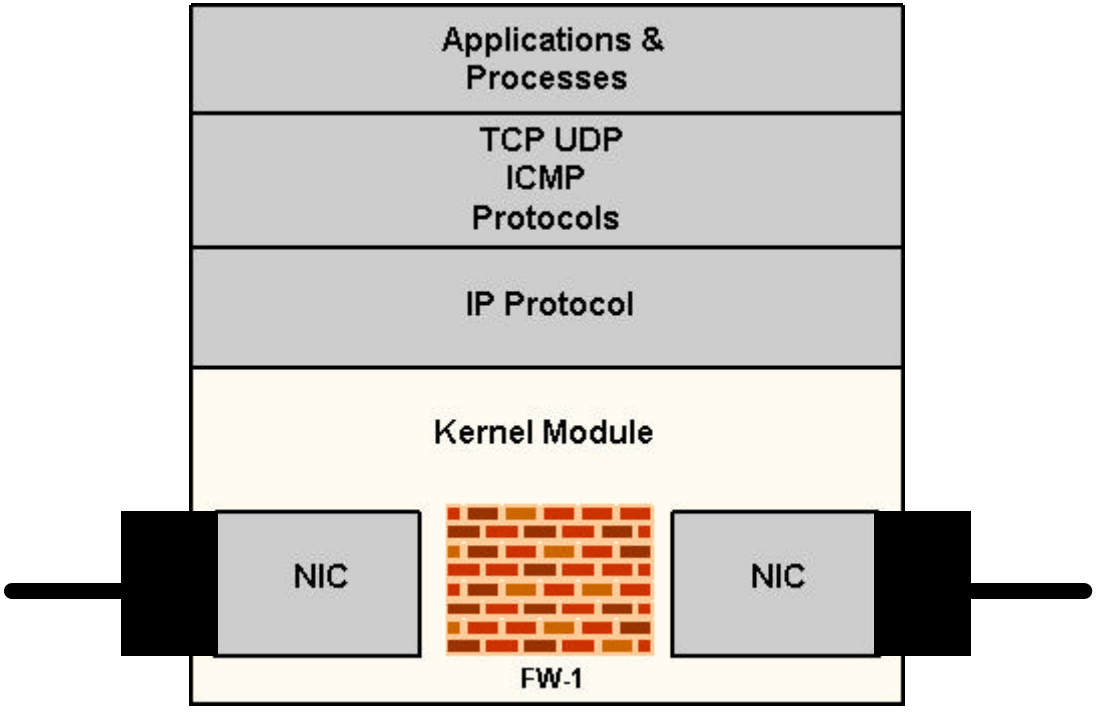
Stateful Inspection



Vorteile:

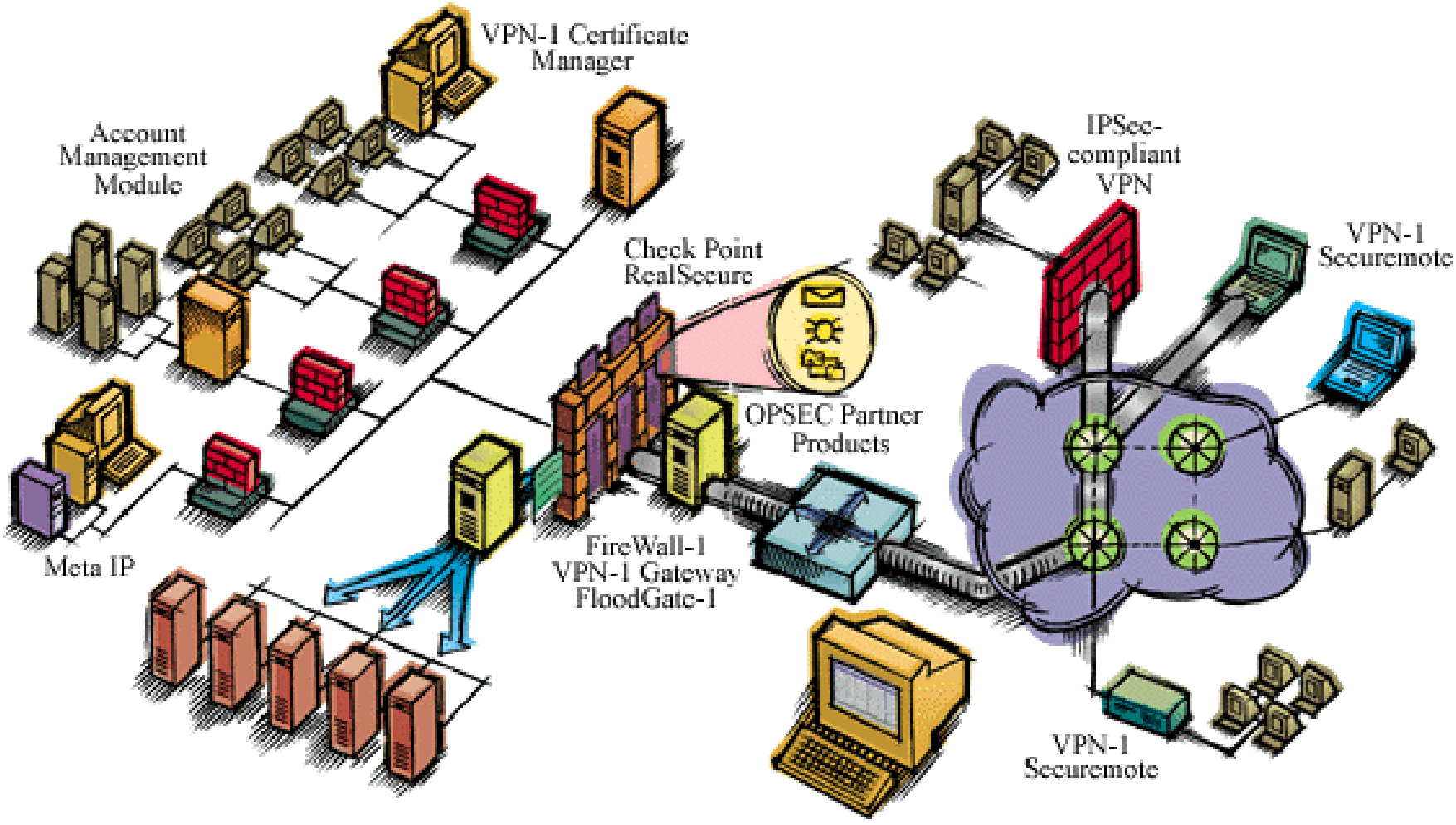
- Hohe Security
- Hohe Performance
- Applikationsdurchgriff
- Skalierbar
- Erweiterbar
- Transparent

Inspection Engine (FW-1)



- Ist im Kernel als Modul integriert
- Aktzeptiert Pakete, wirft sie zurück oder vergißt sie
- Schont die Systemressourcen

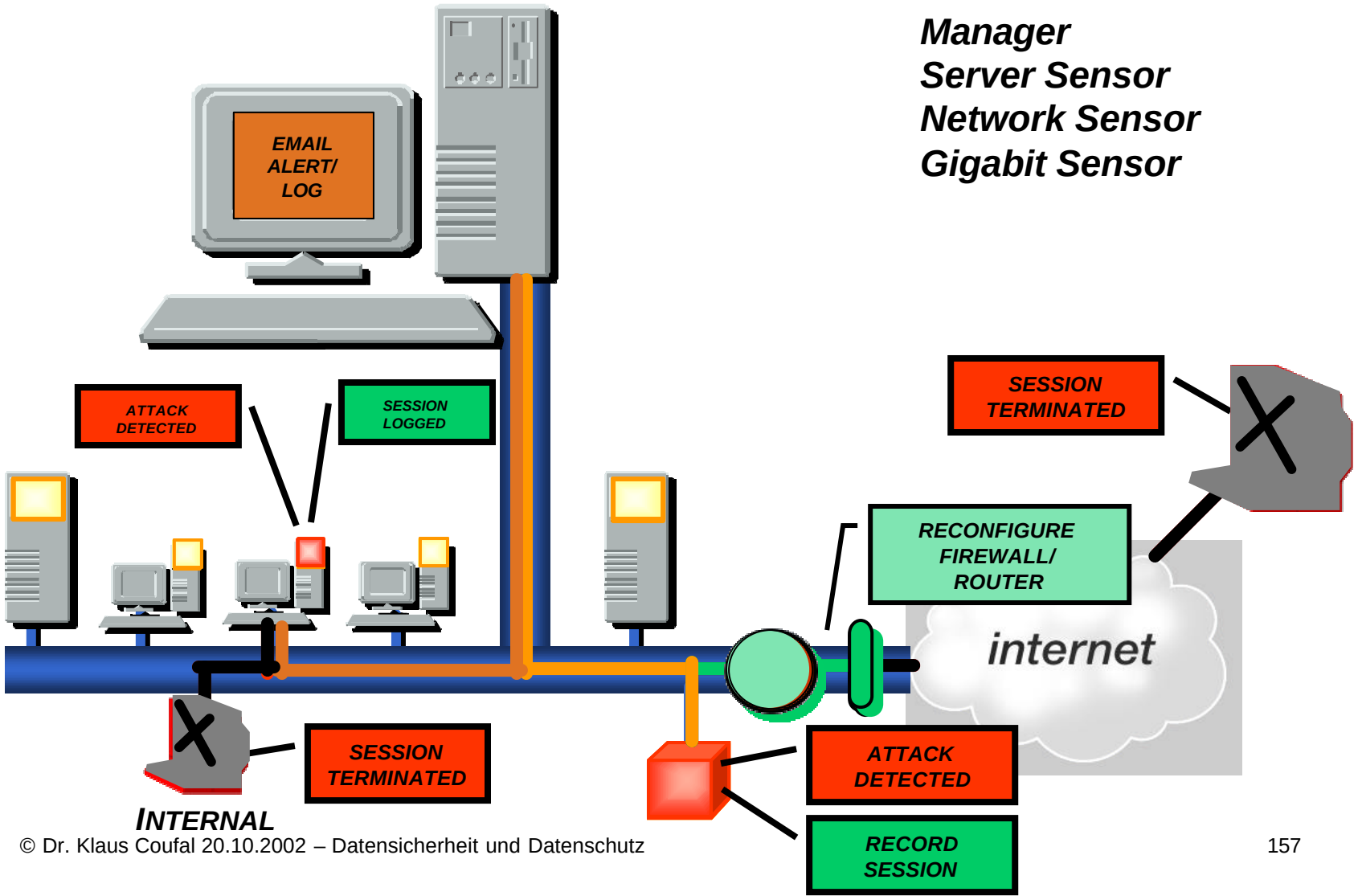
Firewall-1 Beispiel



VII.4. IDS

- Angriffsabwehrmanagement
- Hackerarbeitsweise
- IDS (Intrusion Detection System)
- IRS (Intrusion Response System)
- Arbeitsweise
- Honeypot

Angriffs-Abwehr- Management



Hackerarbeitsweise

Schritt 1.

Ein port scan findet aktive Dienste auf verschiedenen Systemen

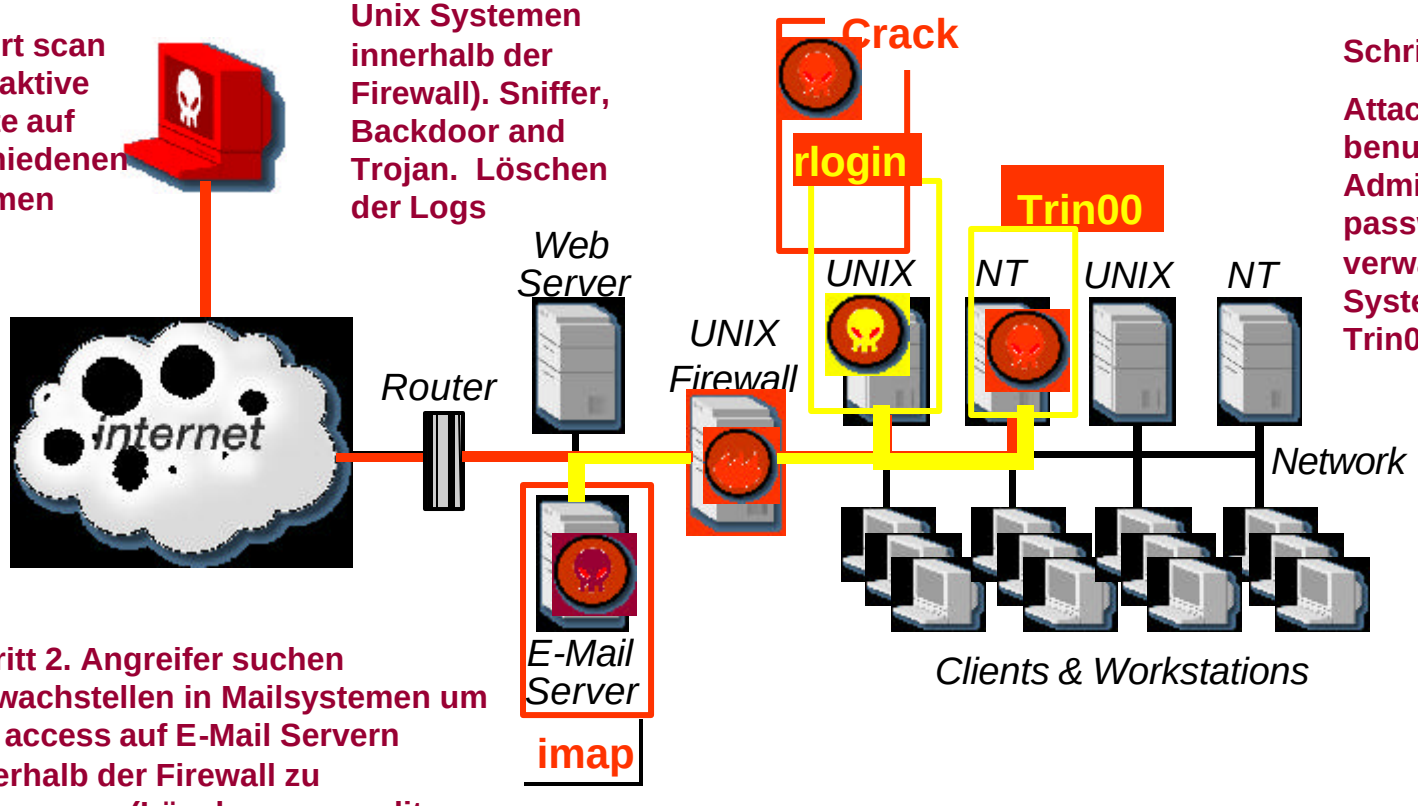
Schritt 3.

Angreifer suchen Schwachstellen (root access auf Unix Systemen innerhalb der Firewall). Sniffer, Backdoor and Trojan. Löschen der Logs

Schritt 4. Attacker cracken password files und haben nun root/administrator access zu verschiedenen Systems und Applikationen im LAN.

Schritt 5.

Attacker benutzen NT Admin passwords und verwandeln Systeme in Trin00 Zombies

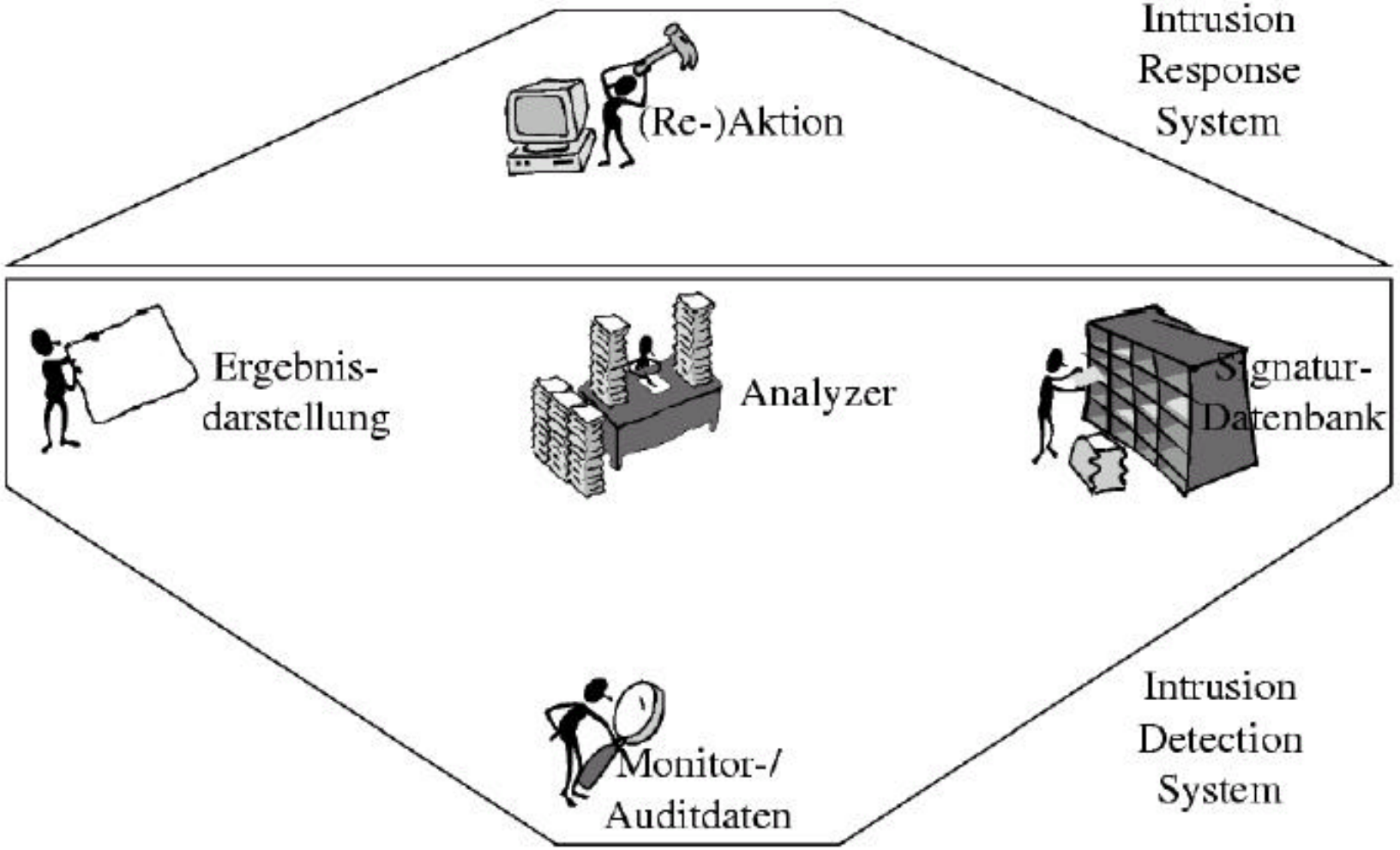


Schritt 2. Angreifer suchen Schwachstellen in Mailsystemen um root access auf E-Mail Servern außerhalb der Firewall zu bekommen. (Löschen von audit logs.)

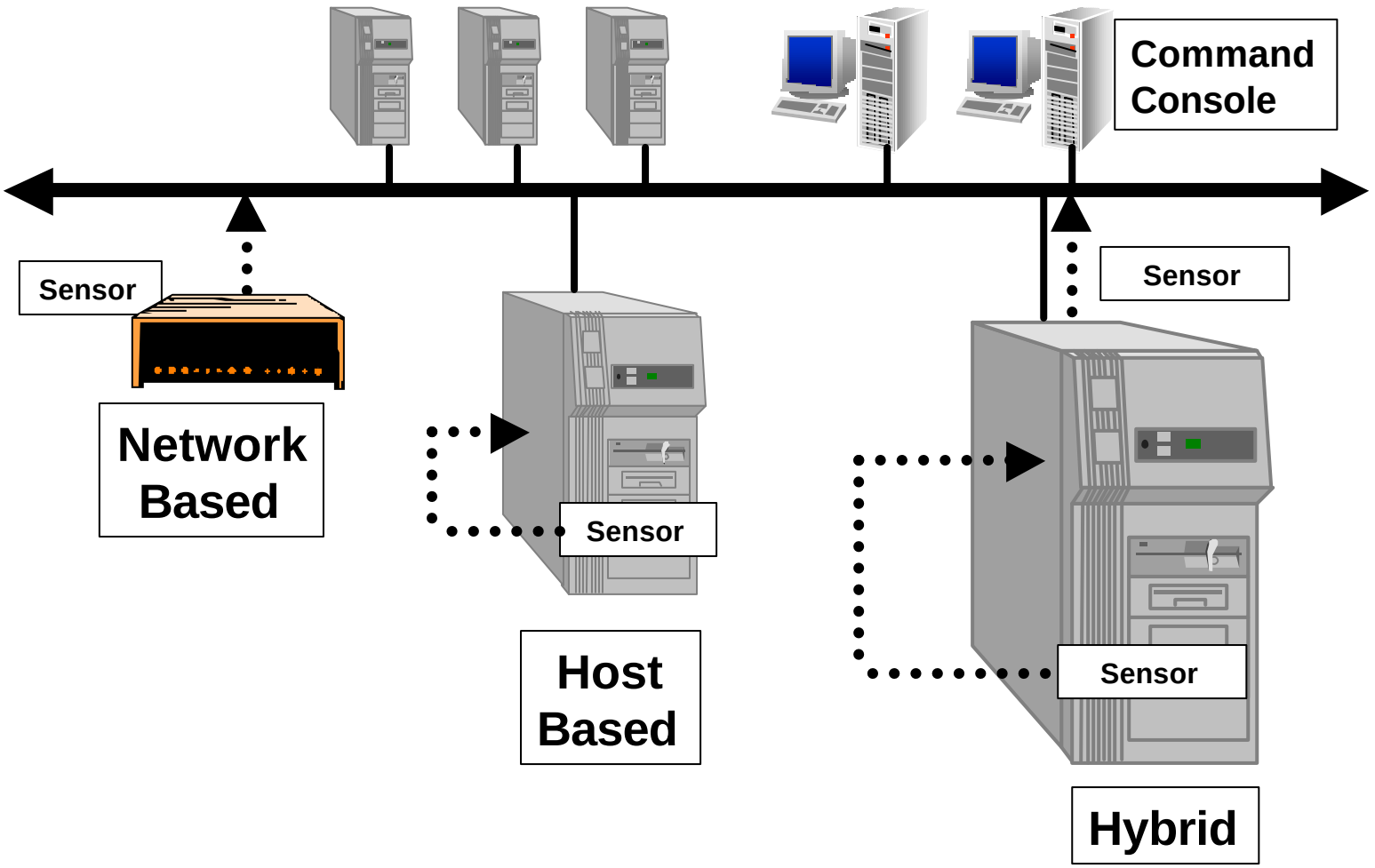
IDS – Definition

- Ein Intrusion Detection System ist ein Konglomerat von Möglichkeiten, Angriffe zu erkennen und – im Gegensatz zu statischen Firewallsystemen - darauf reagieren zu können.
- The ability to detect inappropriate, incorrect, or anomalous activity

IDS und IRS


Intrusion
Response
System
(Re-)Aktion
Ergebnis-
darstellung
Analyzer
Signatur-
Datenbank
Monitor-/
Auditdaten
Intrusion
Detection
System

Arbeitsweise



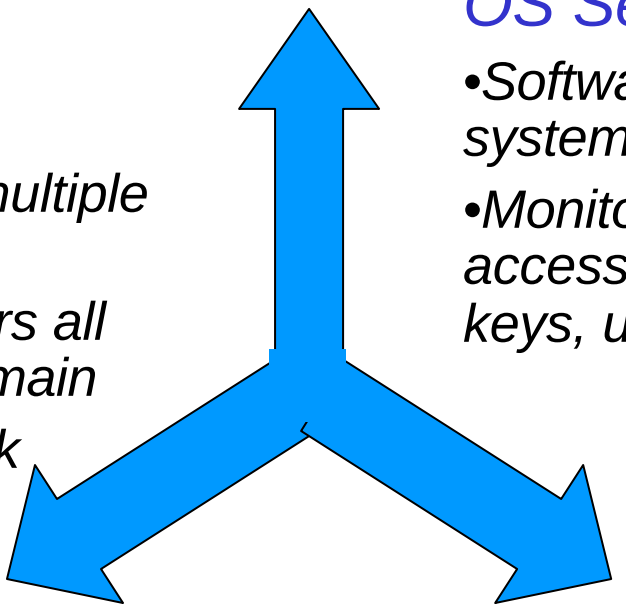
Host- bzw. Network-based

- Host based ID
  - Benötigt LOG-Files und auditing agents
  - Man muß Software auf das zu überwachende System laden
- Network based ID
  - Beobachtet den Netz-Traffic
  - Verwendet Daten-Pakete am Netz für die Informationsgewinnung

Sensoren

Network Sensor

- *Dedicated hardware/ software solution*
- *One sensor protects multiple systems*
- *Promiscuously monitors all traffic on a collision domain*
- *Diverse range of attack signatures*



OS Sensor

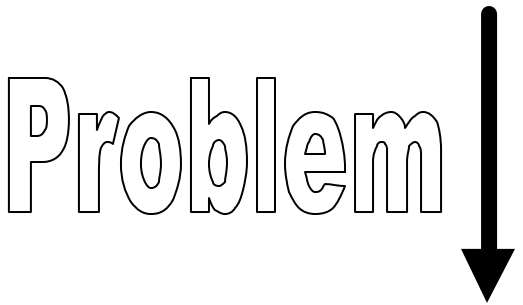
- *Software that runs on <u>each</u> system to be protected*
- *Monitors system logs, file access, port activity, registry keys, user activity*

Server Sensor

- *Combination of host and network sensors*
- *Software that runs on <u>each</u> system to be protected*
- *Tightly integrated with the TCP/IP stack to monitor all traffic to/from the system*

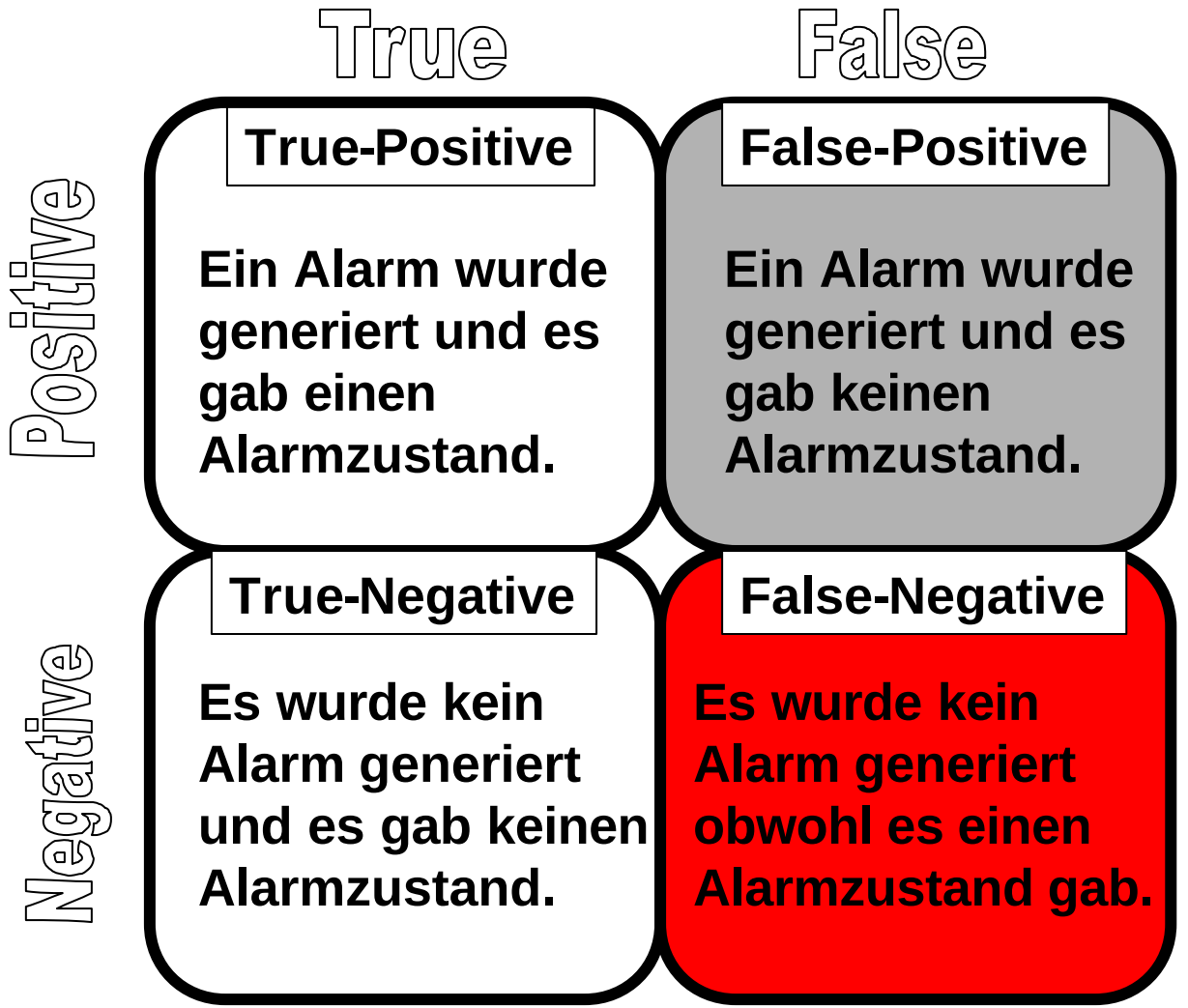
Fehlalarme 1

- **Intrusion Detection**
- **Misuse Detection**
- **Anomaly Detection**



- **False positiv**
- **False negative**

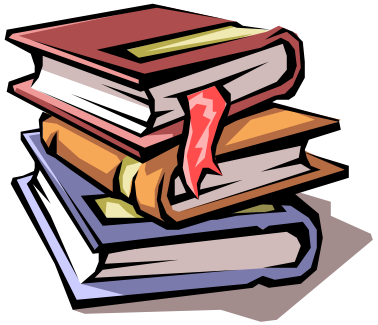
Fehlalarme 2



IDS – Varianten

- **Background Operation**
  Kein menschlicher Eingriff notwendig
- **On-demand Operation**
  Reaktion ja – aber erst nach Operator-Anforderung
- **Scheduled Operation**
  „On-Demand“, zu definierten Zeitpunkten
- **Real-Time Operation**
  Automatische Reaktion in Minuten oder Sekunden
- **24*7 Monitoring**
  Ständiges „human“ controlling für neue Situationen
- **Incident Response**
  Reaktion auf Meldungen von „außen“

IDS Aufgaben



Analysekomponente

Signaturanalyse

„Mißbrauchserkennung“

Bekannte Angriffe

Anomalieerkennung

„auffälliges“ Verhalten

Unbekannte Angriffe

Anomalieerkennung 1

Anforderungen:

- **Echtzeitfähigkeit**

  Schnelle Reaktion ist notwendig, da Intruder ihre Spuren verwischen

- **Adaptivität**

  Profile und Schwellwerte müssen ständig aktualisiert werden

- **Einfache Konfiguration**

  Mittels „Default-Profile“ muß ein schnelles Umkonfigurieren möglich sein.

Anomalieerkennung 2

Profilarten-1

- **Benutzerprofile**

  Individuelle Arbeitsprofile, die bei jeder Benutzeraktion aktualisiert werden

  Bsp: CPU-Auslastung
  Tippgeschwindigkeit
  Art & Häufigkeit der verwendeten Programme
  bevorzugte Arbeitszeit

- **Benutzergruppenprofile**

  Zusammenfassung von Benutzern mit ähnlichen Arbeitsmustern

Anomalieerkennung 3

Profilarten-2

- **Ressourcenprofile**

  Beschreibung systemweiter, benutzerunabhängiger System-ressourcen.

  Bsp: Speicherbedarf
  Dateizugriffe
  I/O-Aktivitäten an Ports
  verwendete Protokolle

- **Prozeßprofile**

  Überwachung der Systemprozesse, speziell, wenn sie keinem Benutzer zugeordnet sind (z.B: Hintergrundprogramme)

- **statische Benutzerprofile**

  Benutzerprofile, die nur in unregelmäßigen Abständen aktualisiert werden (gegen langsame, gezielte Benutzerveränderung der Hacker)

Anomalieerkennung 4

- **Operationales Modell**

  „Schwellwert-Modell“ – ein Alarm wird ausgelöst, wenn eine Variable einen bestimmten Wert erreicht (z.B.Loginversuche).

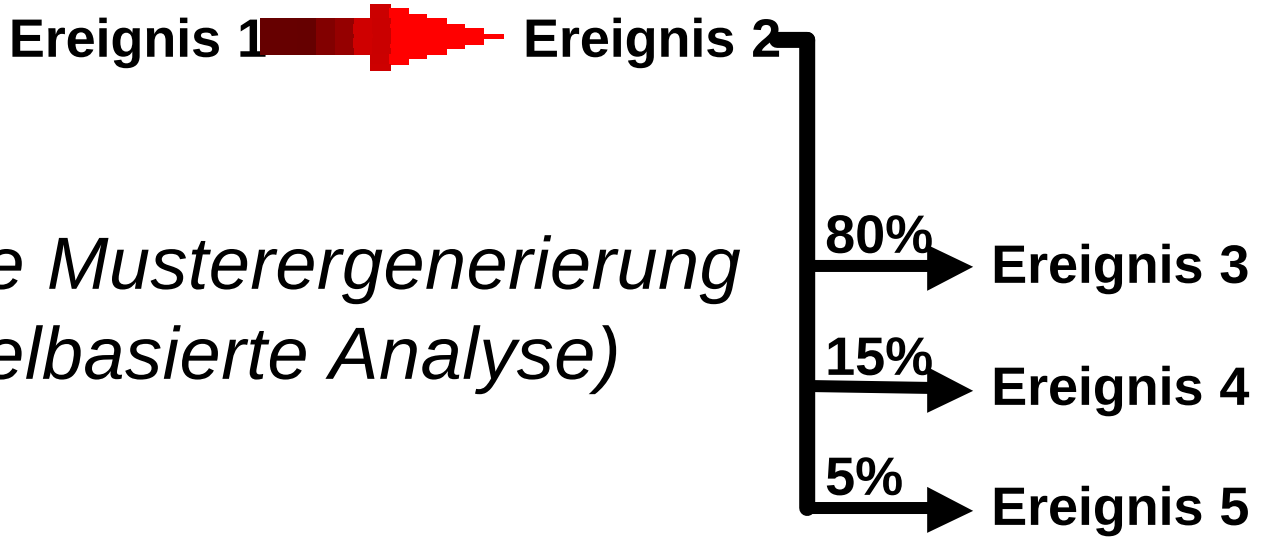
- **Modell von Mittelwert und Standardabweichung**

  Ein Alarm wird ausgelöst, wenn sich eine Beobachtung nicht in einem „Konfidenzintervall“ befindet.

- **Modell von Zeitreihen**

  Die Zeit, zu der ein Ereignis eintritt, fließt in die Entscheidung mit ein

Anomalieerkennung 5



Prädiktive Musterergenerierung
(Regelbasierte Analyse)

Regel:

Wenn das Ereignis 2 unmittelbar nach dem Ereignis 1 eingetreten ist, dann folgt Ereignis 3 mit einer Wahrschein-lichkeit von 80%, Ereignis 4 mit 15% und Ereignis 5 mit 5%

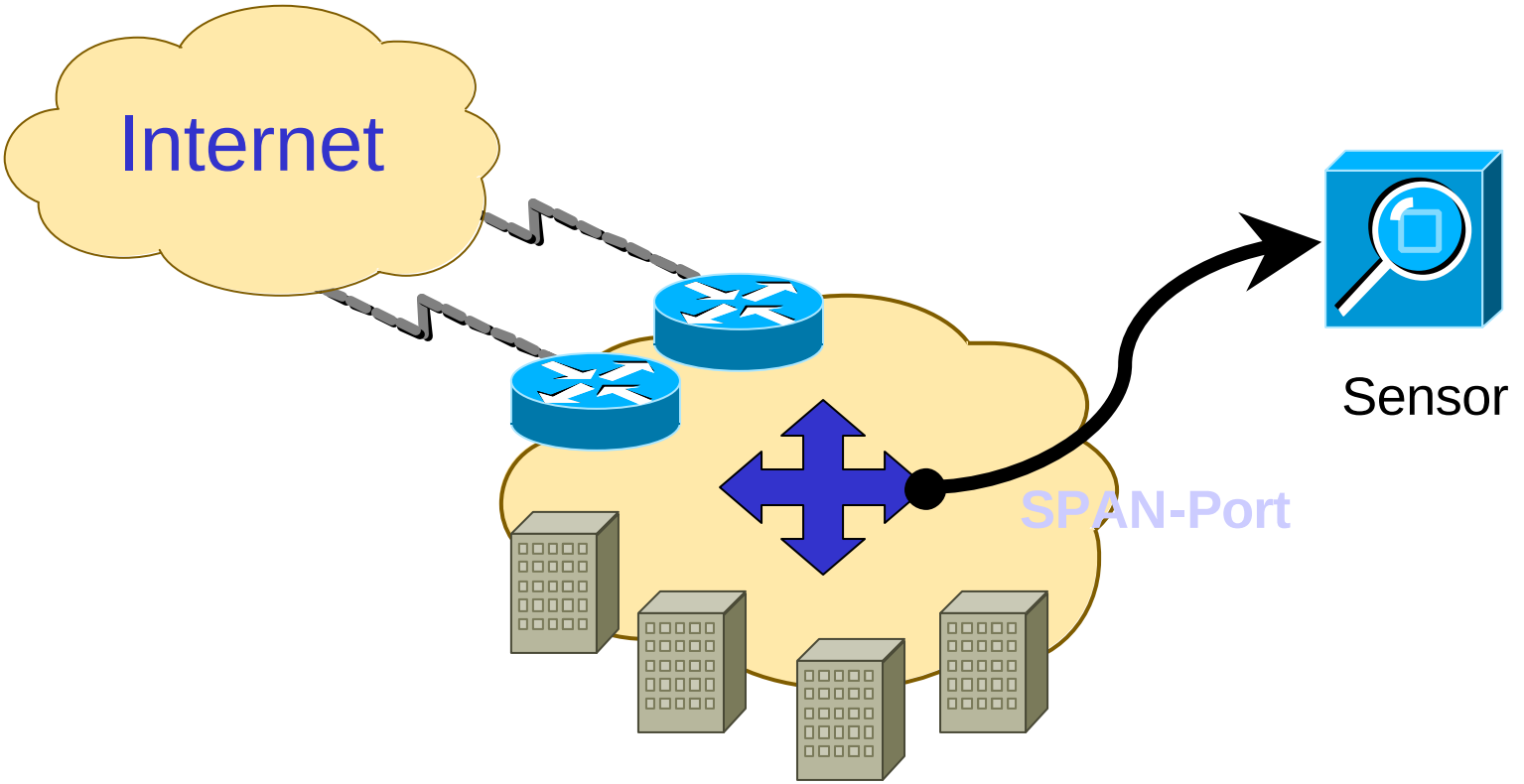
IDS und Neuronale Netze

Lernphase → **Vorhersagephase**

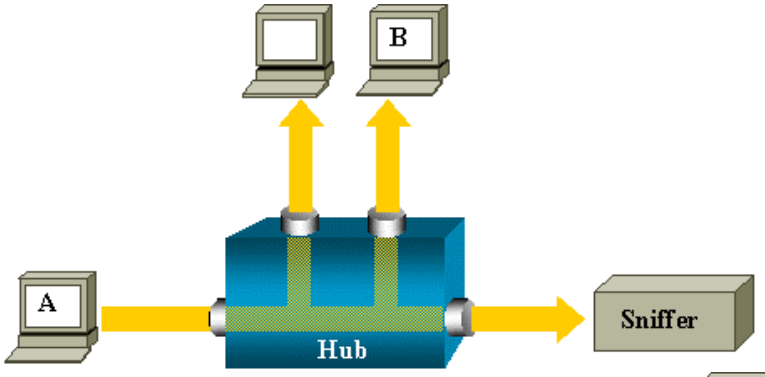
Vorteil:
- **Kann auch mit „verrauschten“ Daten umgehen**

Nachteil:
- **Benötigt viel „trial &error“ in der Lernphase**
- **Angreifbar in der Lernphase**

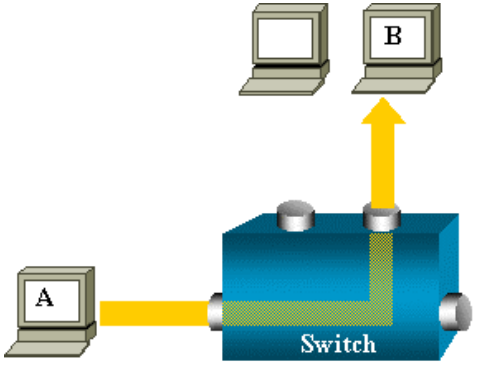
IDS – Beispiele 1



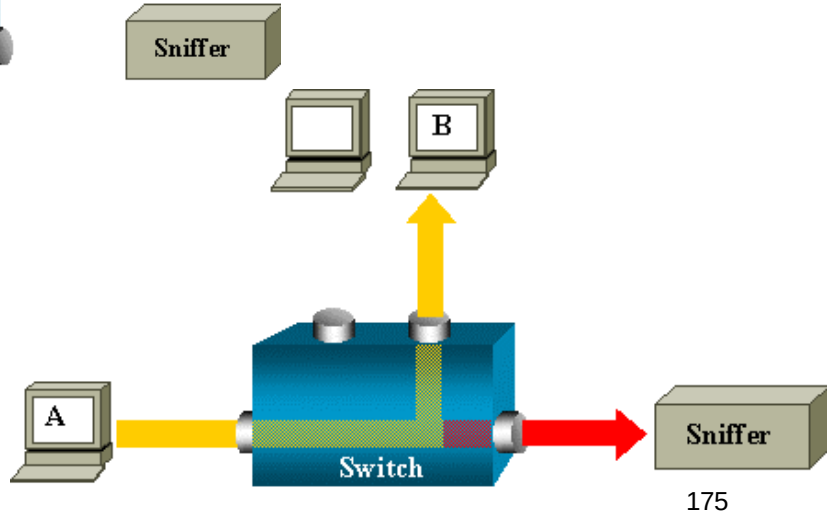
IDS – Beispiele 2



HUB

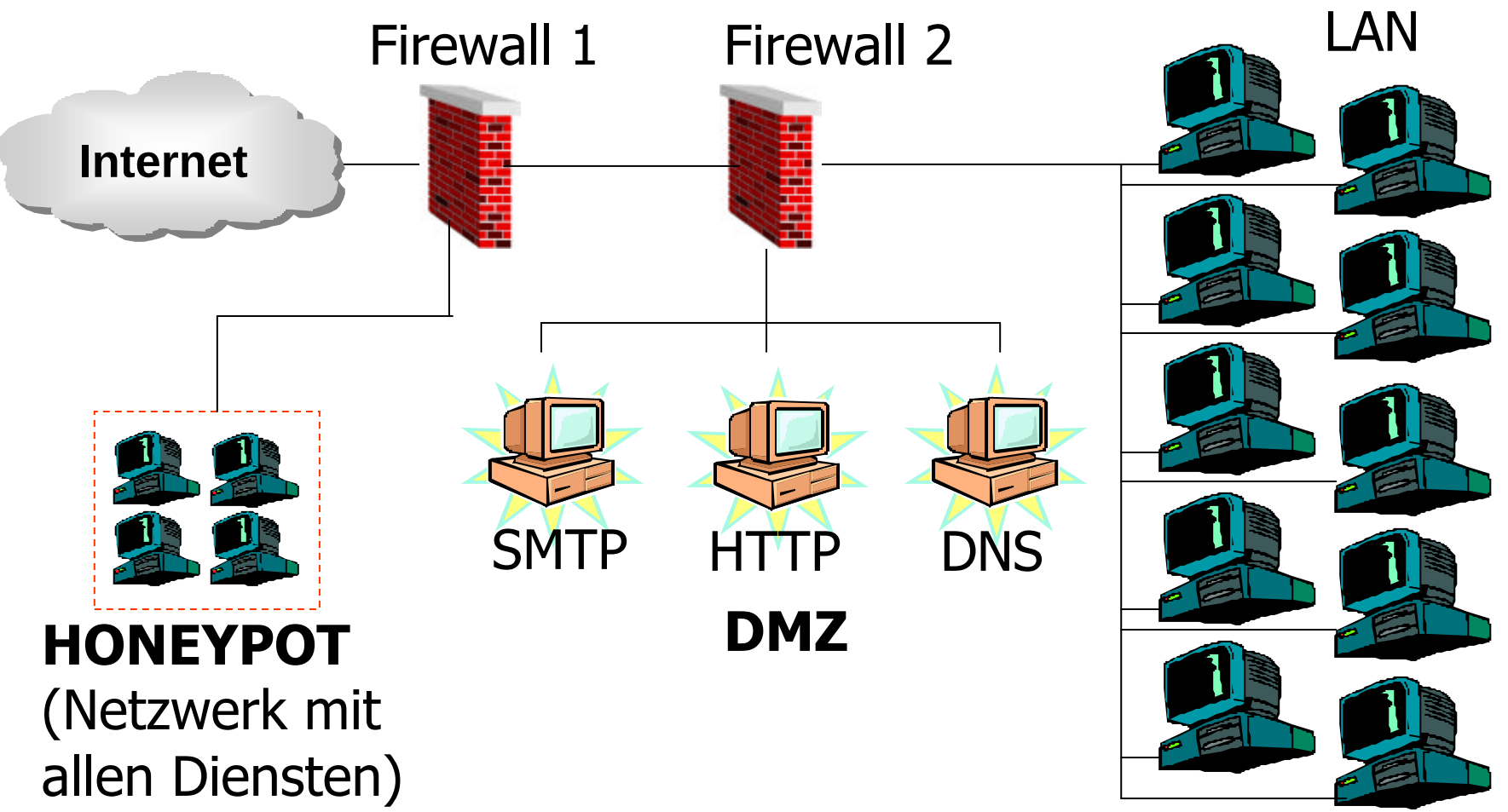


Switch



Switch mit SPAN-Port

Honeypots


Firewall 1
Firewall 2
LAN
Internet
SMTP
HTTP
DNS
DMZ
HONEYPOT
(Netzwerk mit
allen Diensten)