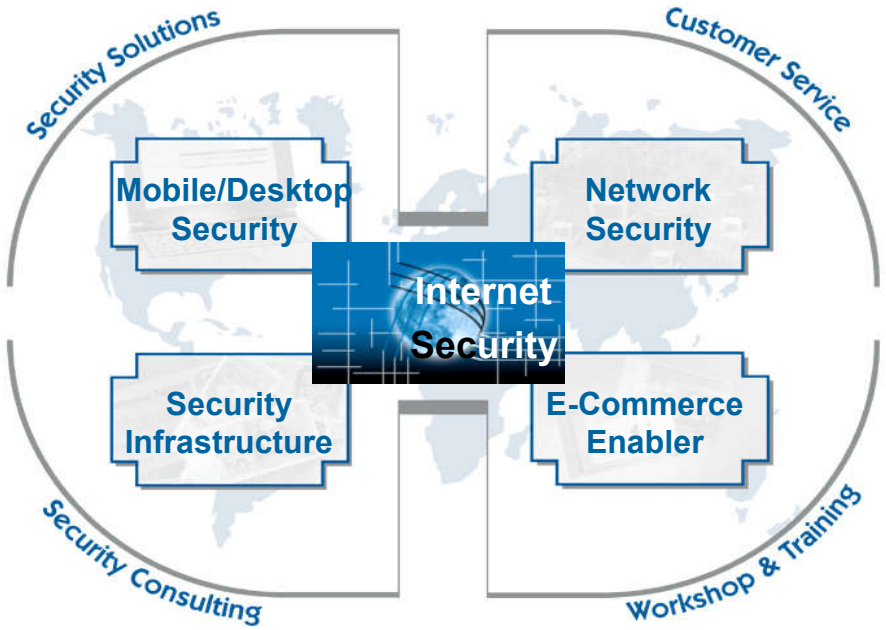
Sicherheit in verteilten Netzwerken

Verschlüsselung, Digitale Signatur, Firewall-Systeme

Norbert Pohlmann

Vorstand

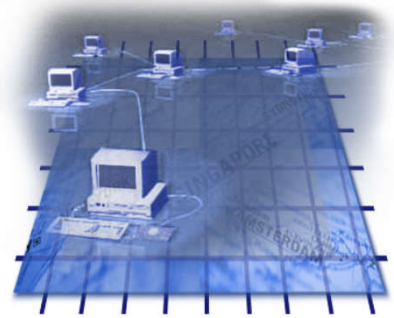
Utimaco Safeware AG



utimaco®
safeware

Inhalt

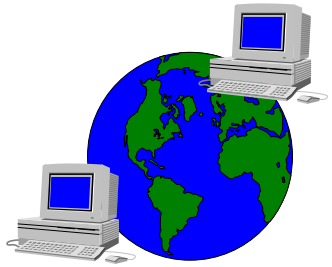
- Sicherheitsanforderungen in verteilten Netzwerken
- Sicherheitskonzepte
  - Verschlüsselung (Black-Box VPN-Lösung)
  - Digitale Signatur
  - Firewall-Systeme
- Kombinierte Lösungen



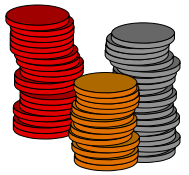
Warum Sicherheit?

- Fundamentaler Wandel durch die Informationsgesellschaft
  - Eine zunehmende Zahl von Arbeitsabläufen wird über IT-Systeme abgewickelt

    => Netzwerke als neue Angriffsziele



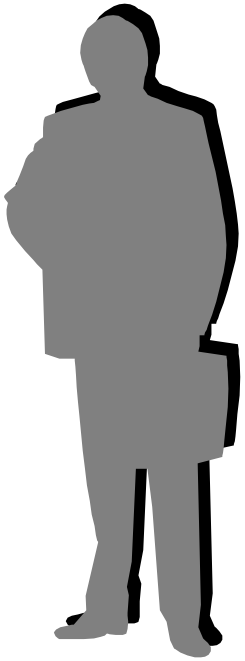
  - Der Wert von Information, die auf IT-Systemen gespeichert sind, wächst
    - die Ergebnisse allein einer Forschungs- und Entwicklungsabteilung können Werte in Millionenhöhe darstellen



  - Sichere und zuverlässige Zahlungen und Transaktionen über unsichere Netze (z.B. Internet)
  - Mangelndes Unrechtsbewußtsein

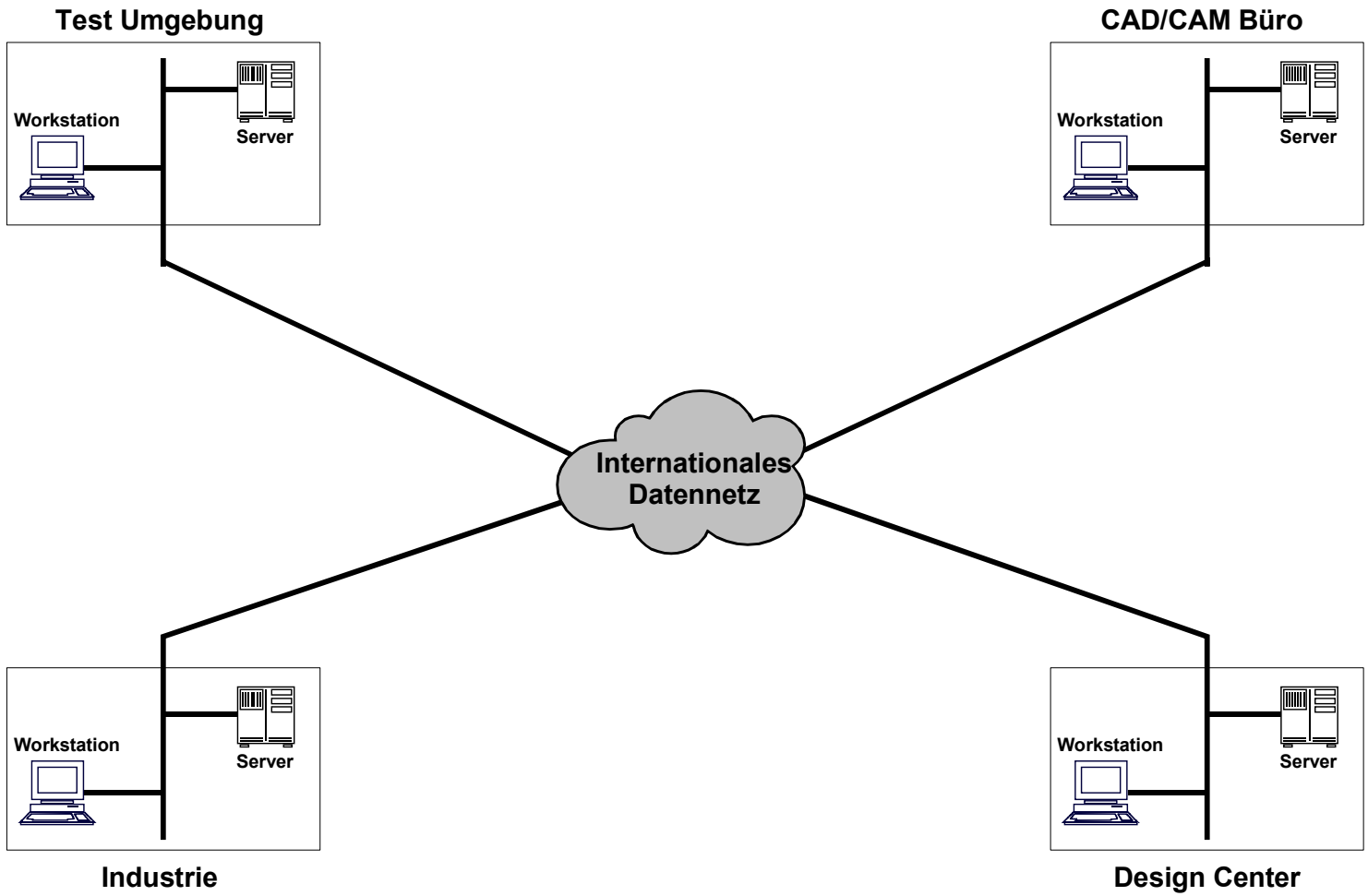
Warum Sicherheit?

- Sicherheitsanforderungen
  - Unternehmen müssen sich selbst gegen Wirtschaftsspionage schützen
  - Einhaltung von Datenschutzgesetzen



utimaco safeware

Internationale Vernetzung von Kommunikationsabläufen



Sicherheitsanforderungen an Kommunikationsprozesse in Netzwerken

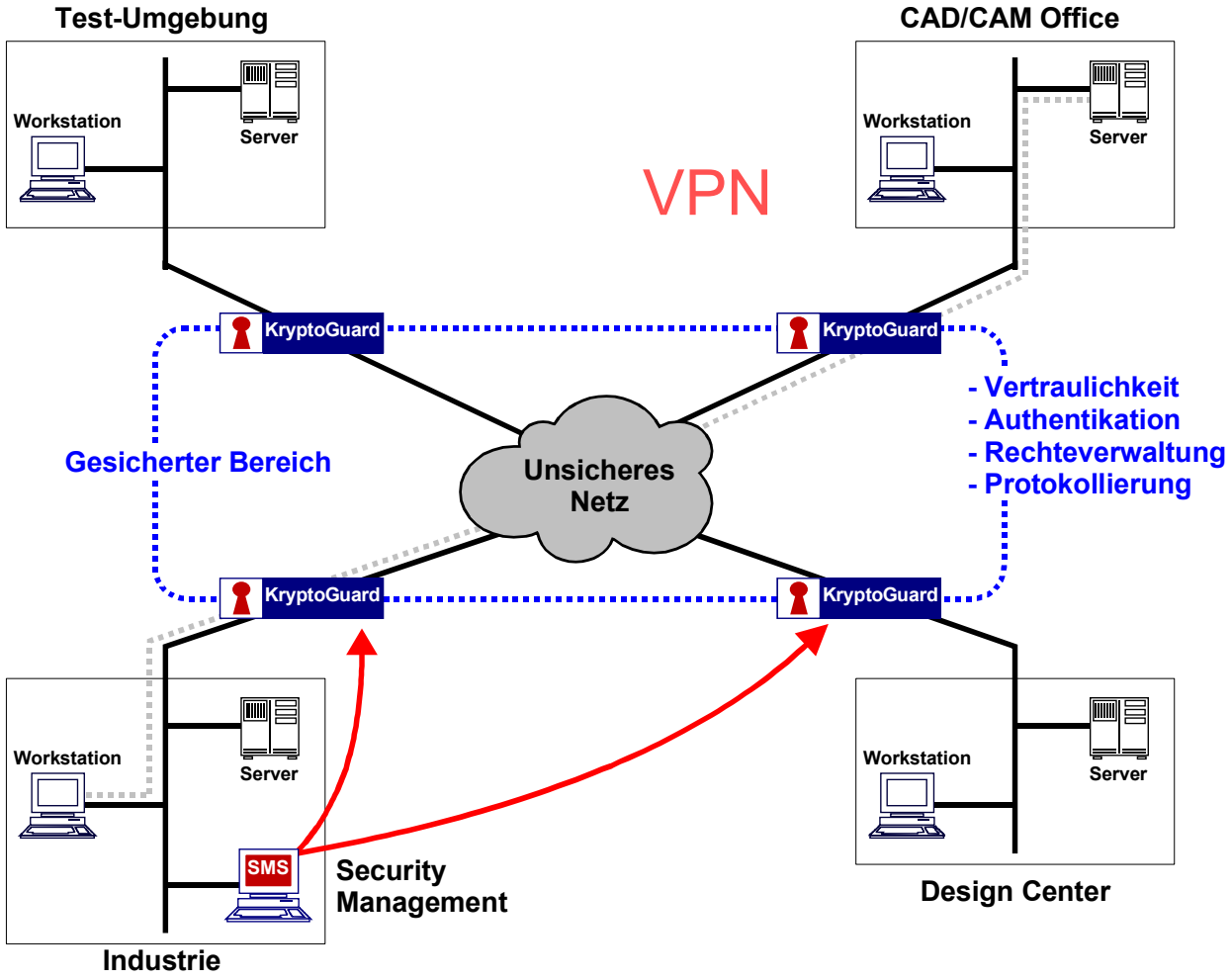
- Vertraulichkeit
  - Schutz des vorhandenen Know-hows
  - Konkurrenten versuchen, Zugang zu sensiblen Entwicklungsdaten zu erlangen
- Sende- und Empfängernachweis
  - Gewährleistung, daß die korrekten Informationen nachweislich empfangen worden sind → Kündigung
  - Absender eines Dokuments muß nachweislich identifizierbar sein → Bestellung
- Datenintegrität
  - Keine Manipulationsmöglichkeit während der Datenübertragung (Daten erreichen den Adressaten unverändert)
  - Virenschutz

utimaco safeware

Sicherheitsanforderungen an Kommunikationsprozesse in Netzwerken

- Authentifizierung
  - Eindeutige Identifizierung und Authentisierung von Personen
  - Nur authorisierte Personen dürfen Zugangsrechte auf die angeschlossenen Rechnersysteme haben
- Zugangskontrolle
  - Unberechtigte Personen dürfen keinen Zugang auf die zu schützenden Rechner und Netzwerke haben
- Rechteverwaltung
  - Nur zugelassene Protokolle und Dienste zu definierten Zeiten dürfen benutzt werden
- Protokollierung
  - Sicherheitsrelevante Ereignisse werden festgehalten
  - Dokumentierte Ereignisse können als Beweis genutzt werden

Verschlüsselung mit Hilfe der Black-Box VPN -Lösung



Black-Box VPN-Lösung: Sicherheitsdienste

- Vertraulichkeit von Daten (VPN)
  - Daten können nicht im Klartext gelesen werden
- Authentifikation
  - Erfolgt indirekt über die Verschlüsselung
  - Erfolgt direkt durch Authentisierungsmethoden
- Zugangskontrolle
  - Nur zugelassene logische Verbindungen können hergestellt werden
  - Fremde haben keinen Zugang auf das Endsystem
- Rechteverwaltung
  - Nur erlaubte Protokolle und Dienste können verwendet werden
- Protokollierung
  - Sicherheitsrelevante Ereignisse können festgehalten und analysiert werden

Sicherheitssystem mit Packet Filter

Vorteile

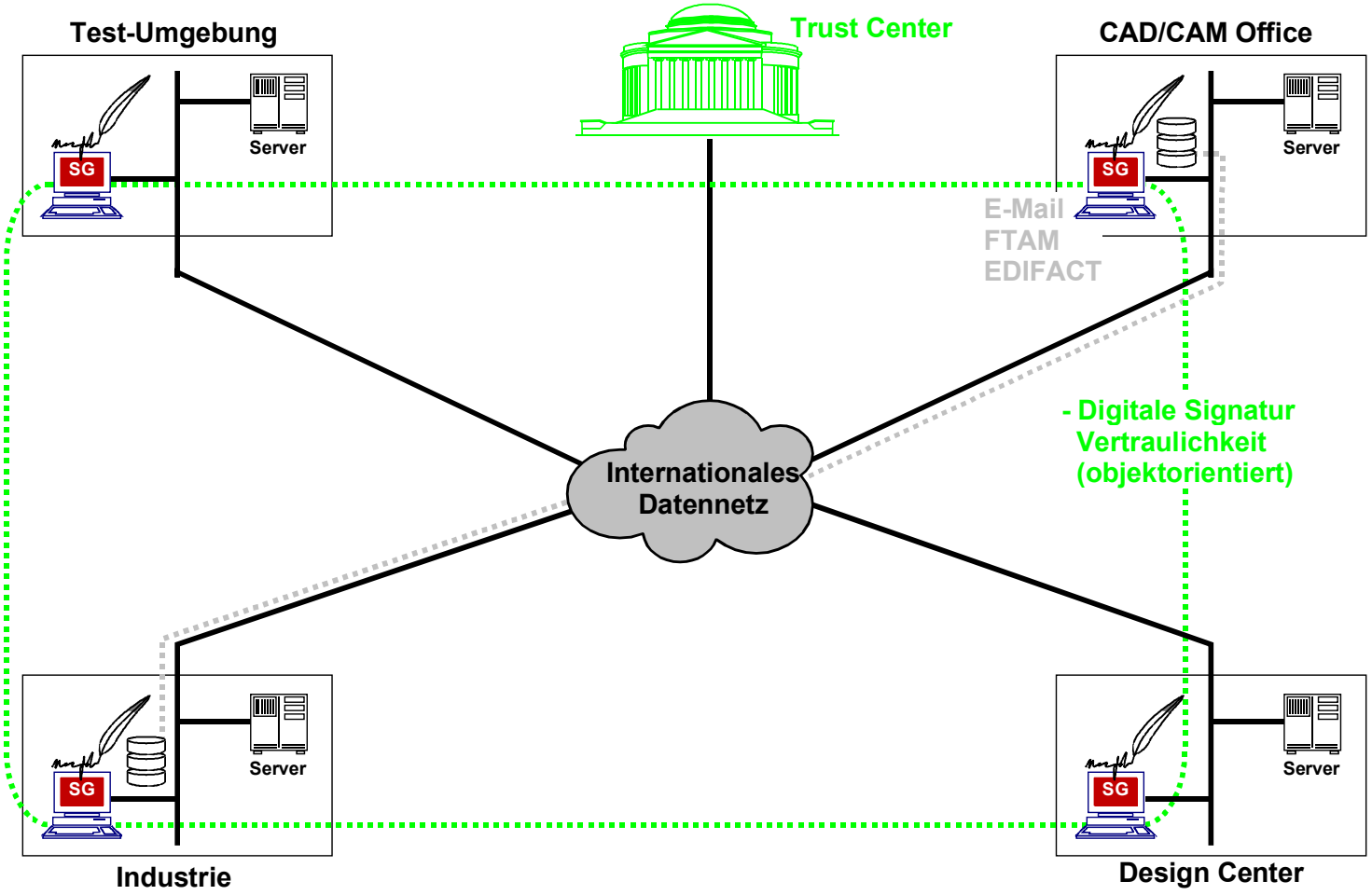
- Black-Box VPN Lösung
  - Transparente Sicherheit
    - einfach zu bedienen
    - keine Änderung der Anwendung notwendig
    - unabhängig von Computer- und Betriebssystem
    - unterstützt alle Kommunikationsarten:
      - **Session orientiert (Telnet etc.)**
      - **„store and forward“ (e-mail)**
  - Kombiniert einfache Handhabung mit klar definierten Verantwortlichkeiten

Nachteile

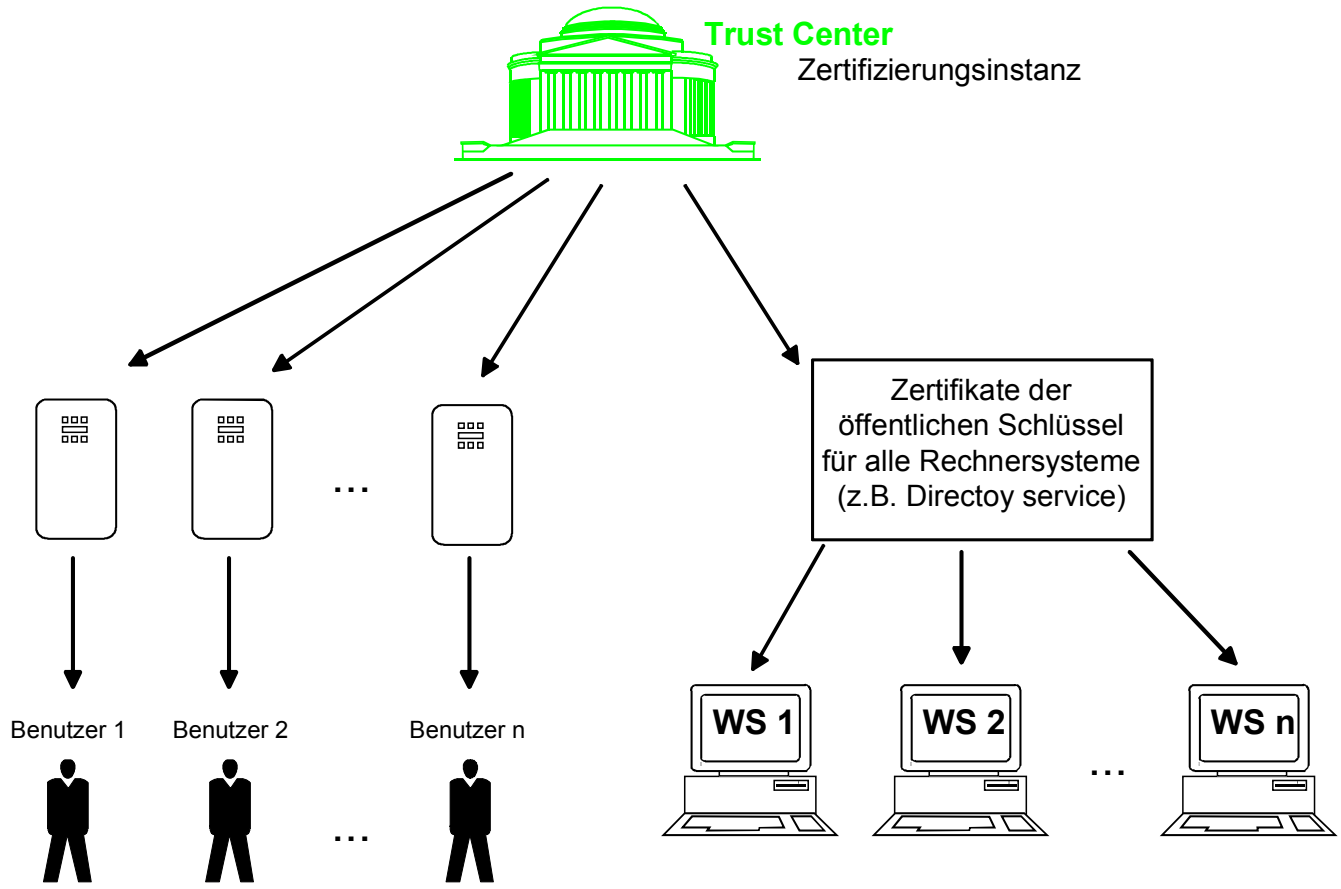
- Key Management
  - Entweder eine Organisation trägt die Verantwortung (i.d.R. die, die auch zahlt)
  - Oder alle müssen das gleiche Produkt einsetzen *(Problem: es existiert noch keine vertrauenswürdige Infrastruktur)*
  - Sende- und Empfängernachweis
    - Muß mit anderen Mechanismen realisiert werden
  - Keine Kontrolle auf Anwendungsebene

utimaco safeware

Digitale Signatur und Objektverschlüsselung



Zertifizierungsinstanz



Digitale Signatur und Objektverschlüsselung

Vorteile

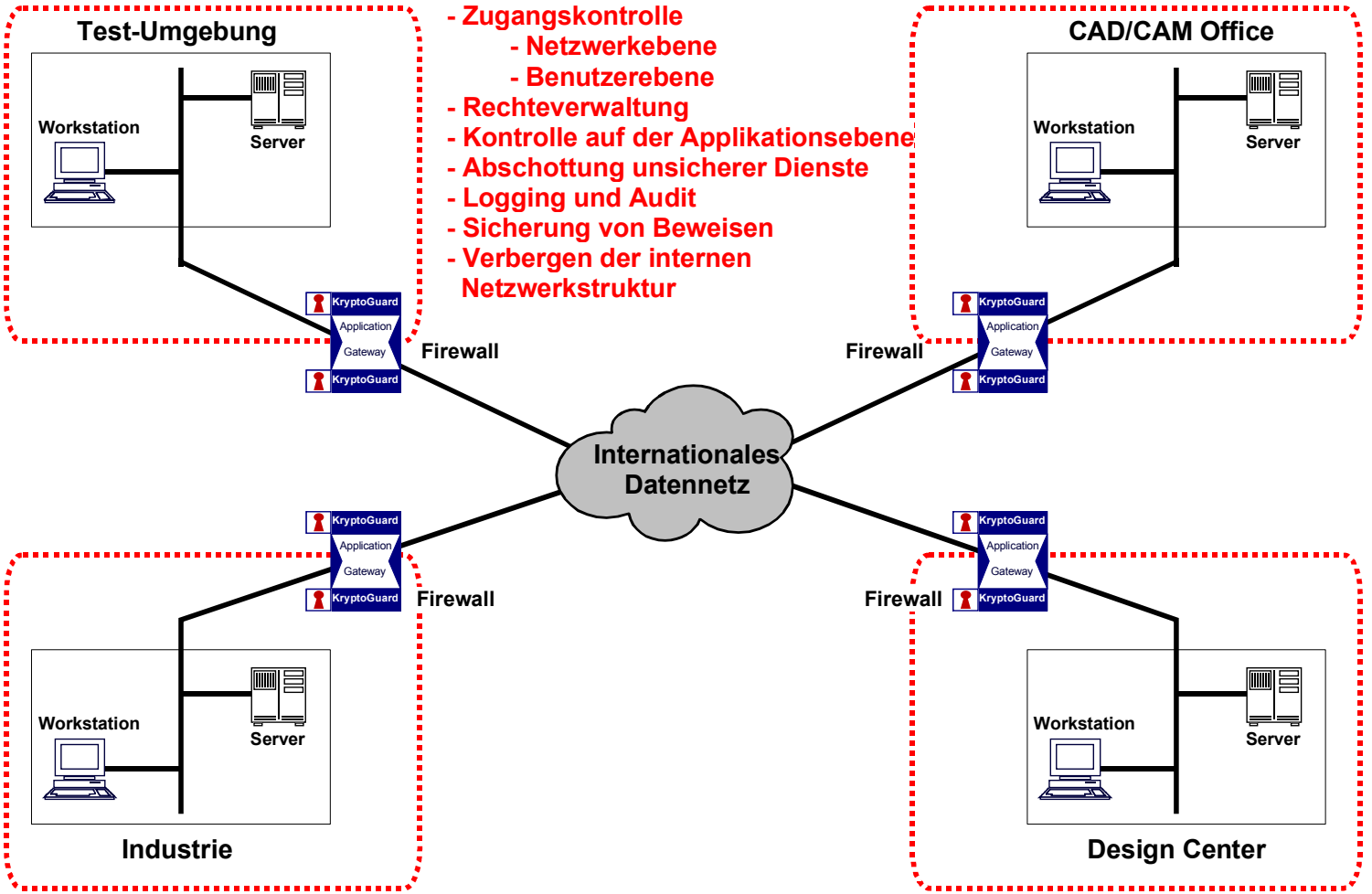
- In die Applikation integriert
- Gesetzlich anerkannte Signatur (als Signatur unter einem Dokument)
- Sichert nur, was gesichert werden soll (Auswahl möglich)
- Anforderungen:
  - Sichere, vertrauenswürdige Infrastruktur
    - ⇒ Signaturgesetz
- Sende- und Empfänger-nachweis möglich

Nachteile

- Keine Zugangskontrolle
- Keine Rechteverwaltung
- Nicht mit session-orientierter Kommunikation kombinierbar

als Umschlag und Unterschrift

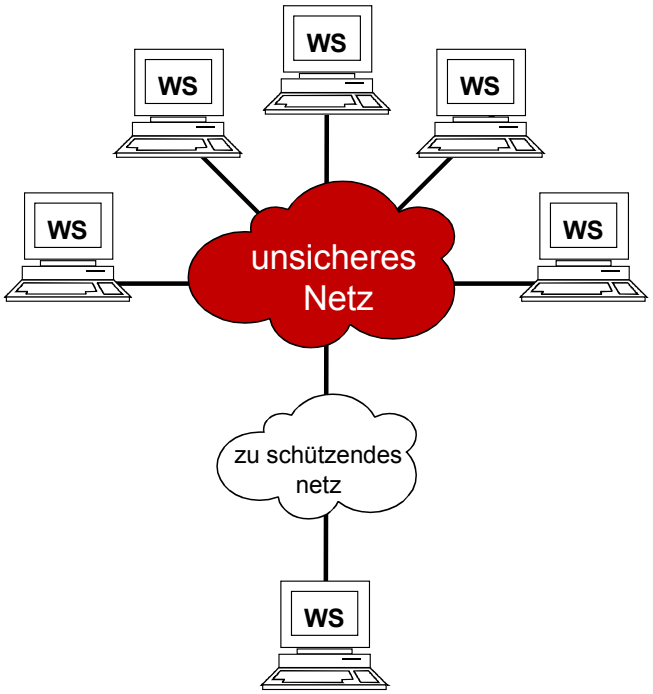
Firewall-System



Ein öffentliches Netzwerk ist keine “Einbahnstrasse”

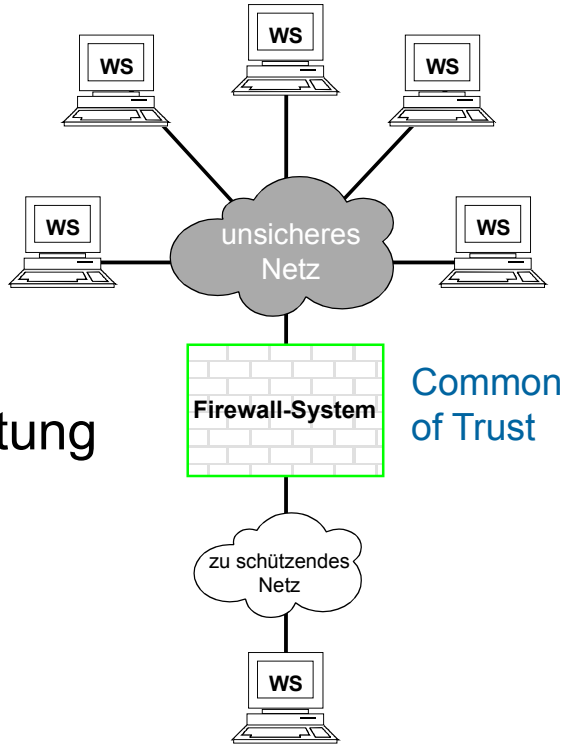
Risiken in öffentlichen Netzen: Was sind die Probleme ?

- High-tech Spione stehlen das Know-how eines Unternehmens und verkaufen es gewinnbringend an die Konkurrenz.
- Hacker dringen in lokale Netze öffentlicher Einrichtungen und Unternehmen ein, manipulieren ihre Daten oder schmuggeln falsche Informationen ein.
- Netzsurfer lähmen das Rechnersystem eines Unternehmens und verursachen wirtschaftlichen Schaden in Millionenhöhe.

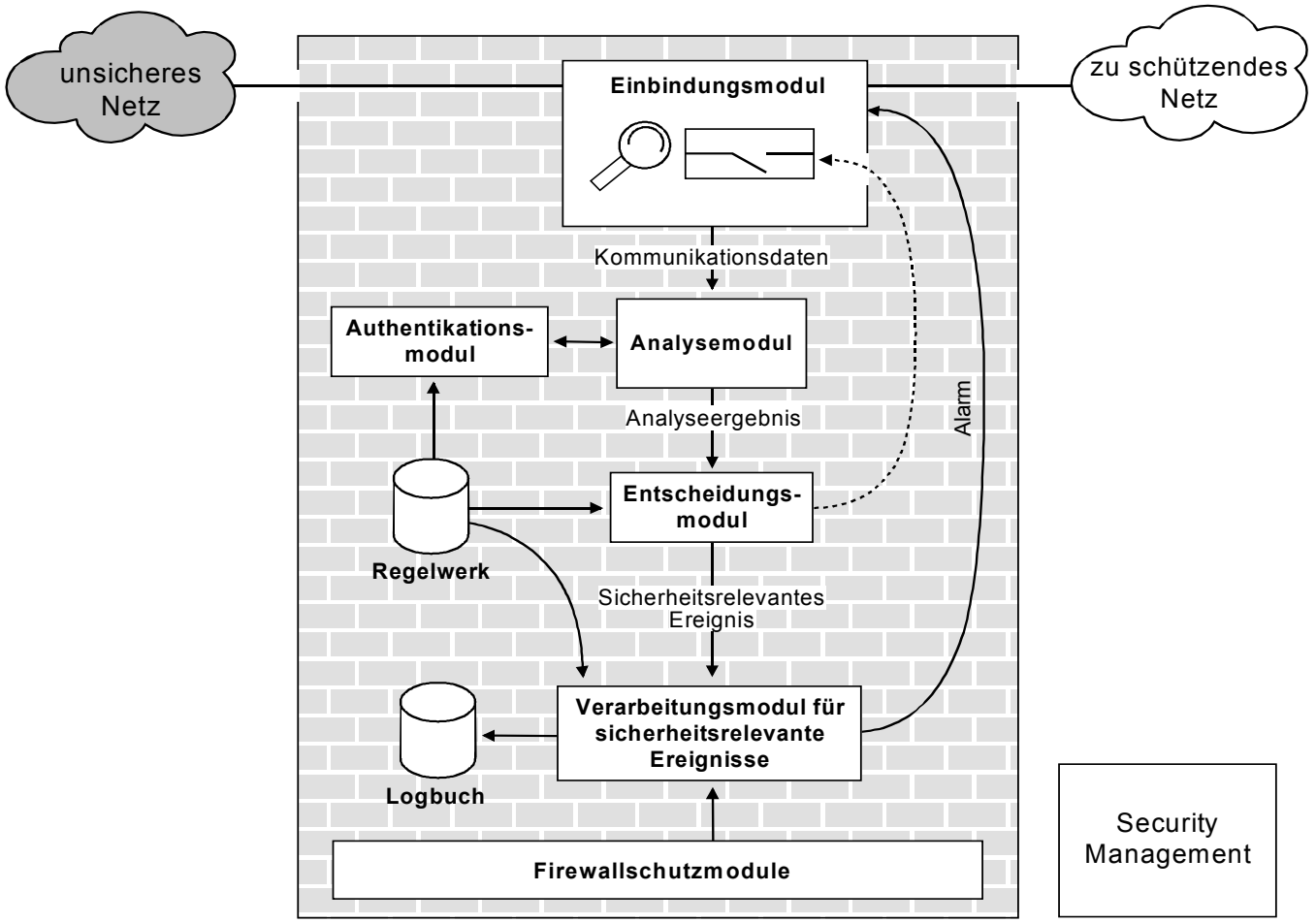


Sicherheitsziele eines Firewall-Systems

- Zugangskontrolle auf der Netzebene
- Zugangskontrolle auf Benutzerebene
- Rechteverwaltung
- Kontrolle auf der Applikationsebene
- Entkopplung von unsicheren Diensten
- Beweissicherung und Protokollauswertung
- Alarmierung
- Verbergen der internen Netzstruktur
- Vertraulichkeit der Nachrichten

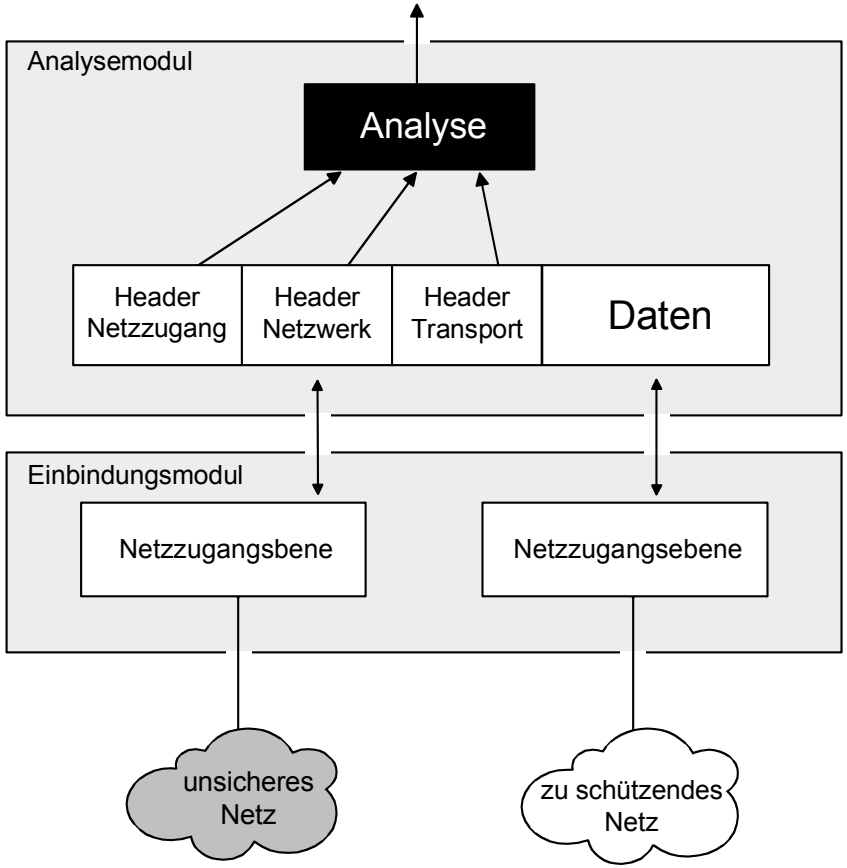


Aufbau eines aktiven Firewall-Elementes

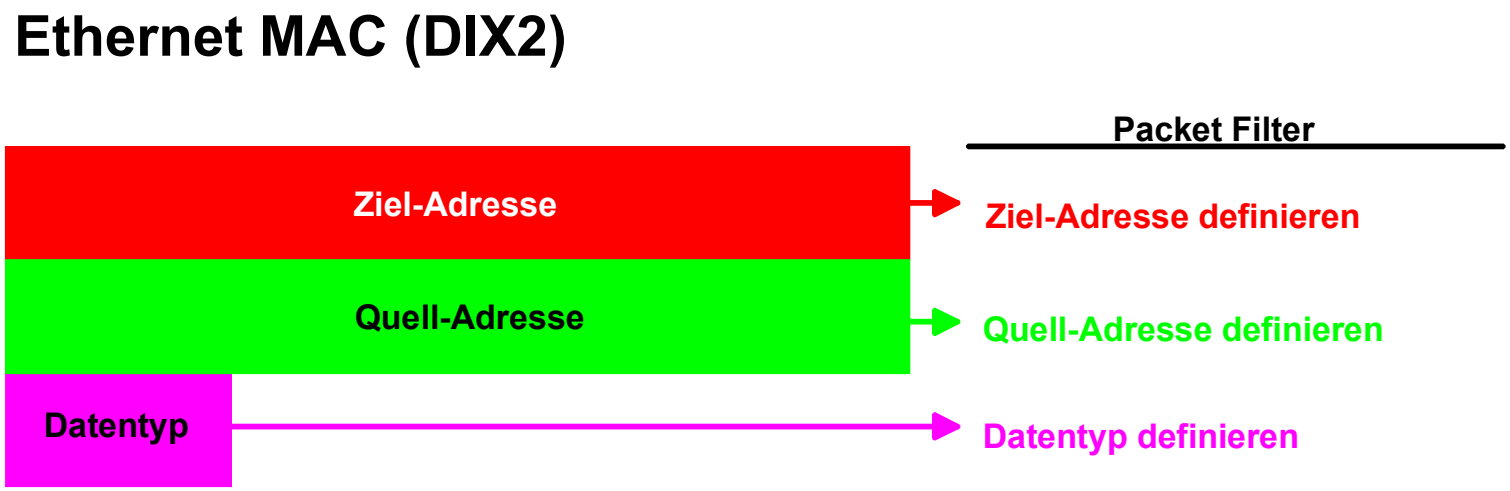


utimaco safeware

Allgemeine Arbeitsweise eines Packet Filters

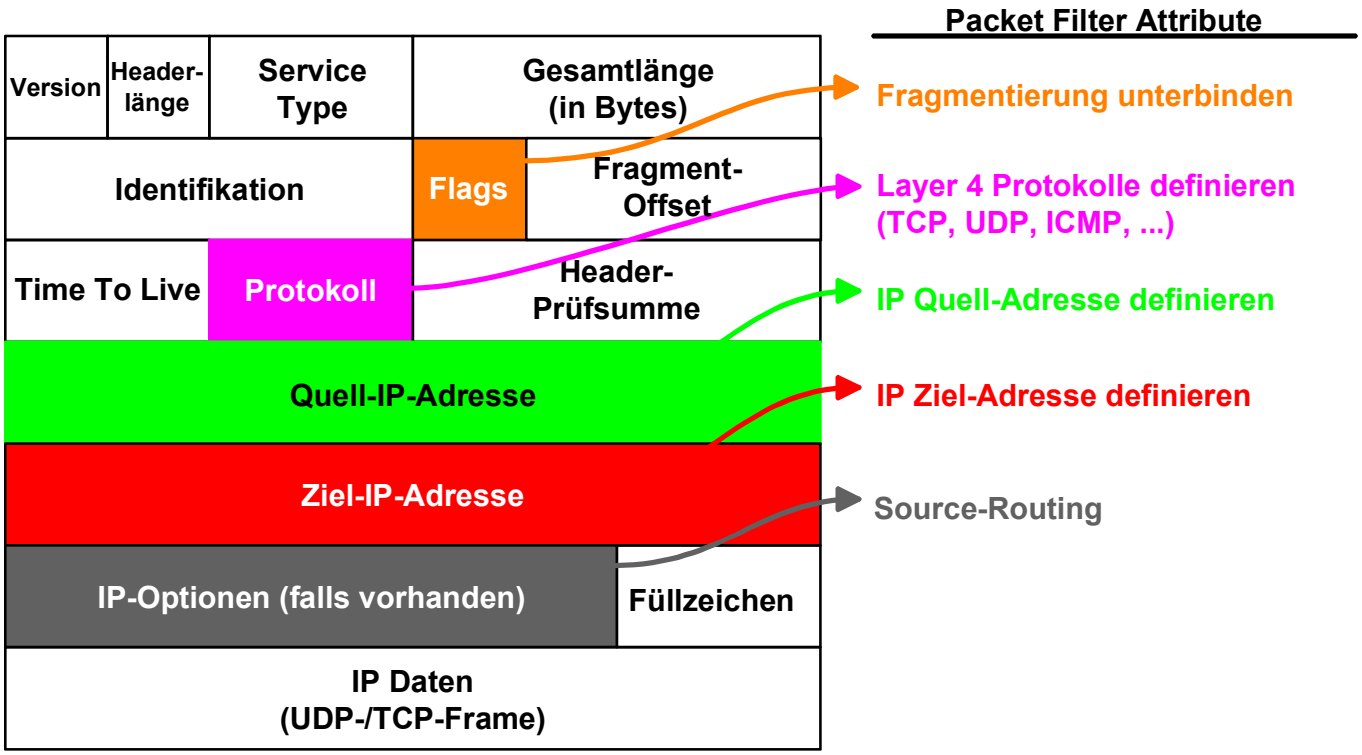


Analysemöglichkeit eines Ethernet MAC Frames (DIX 2)

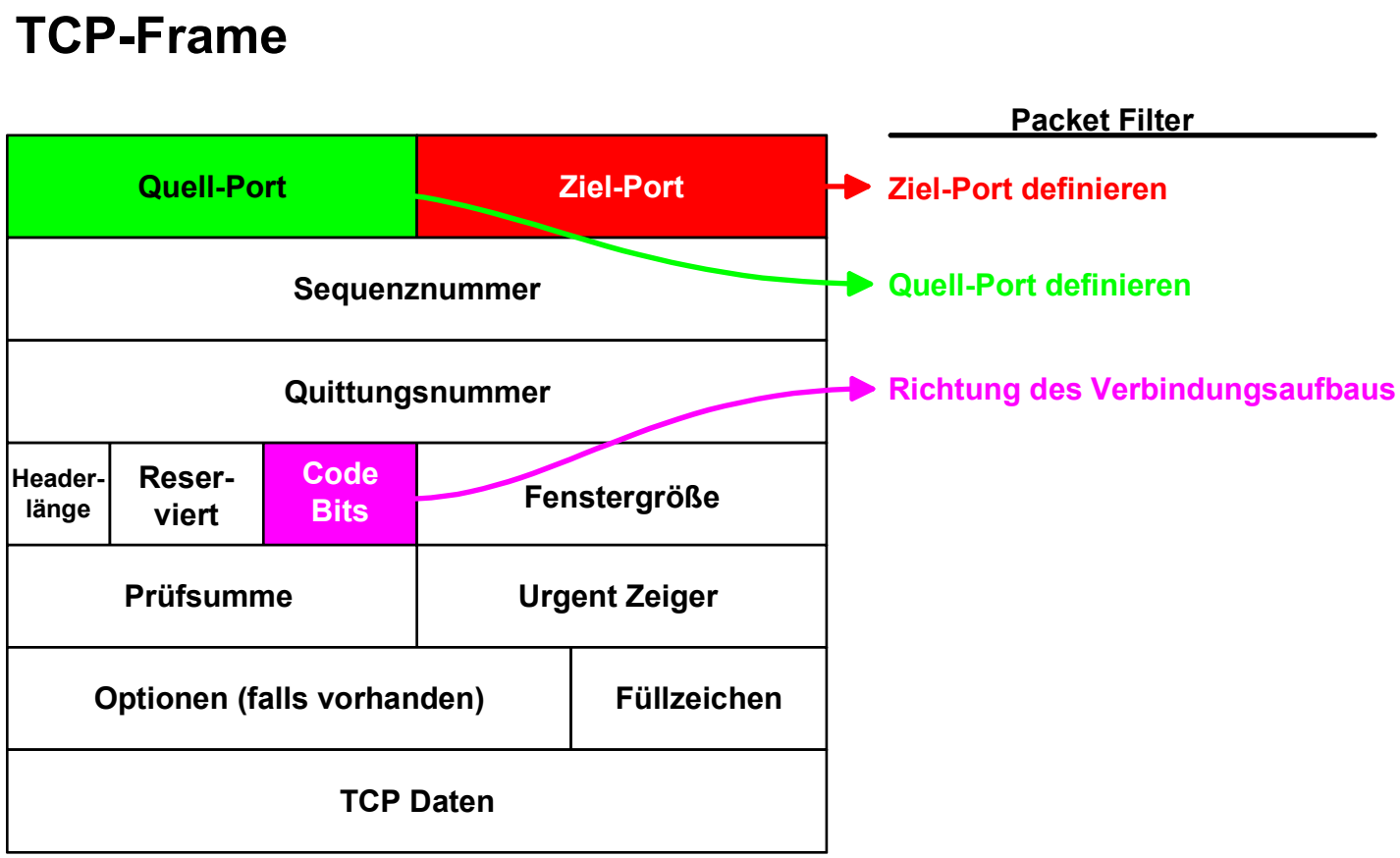


Analysemöglichkeit eines IP-Frames

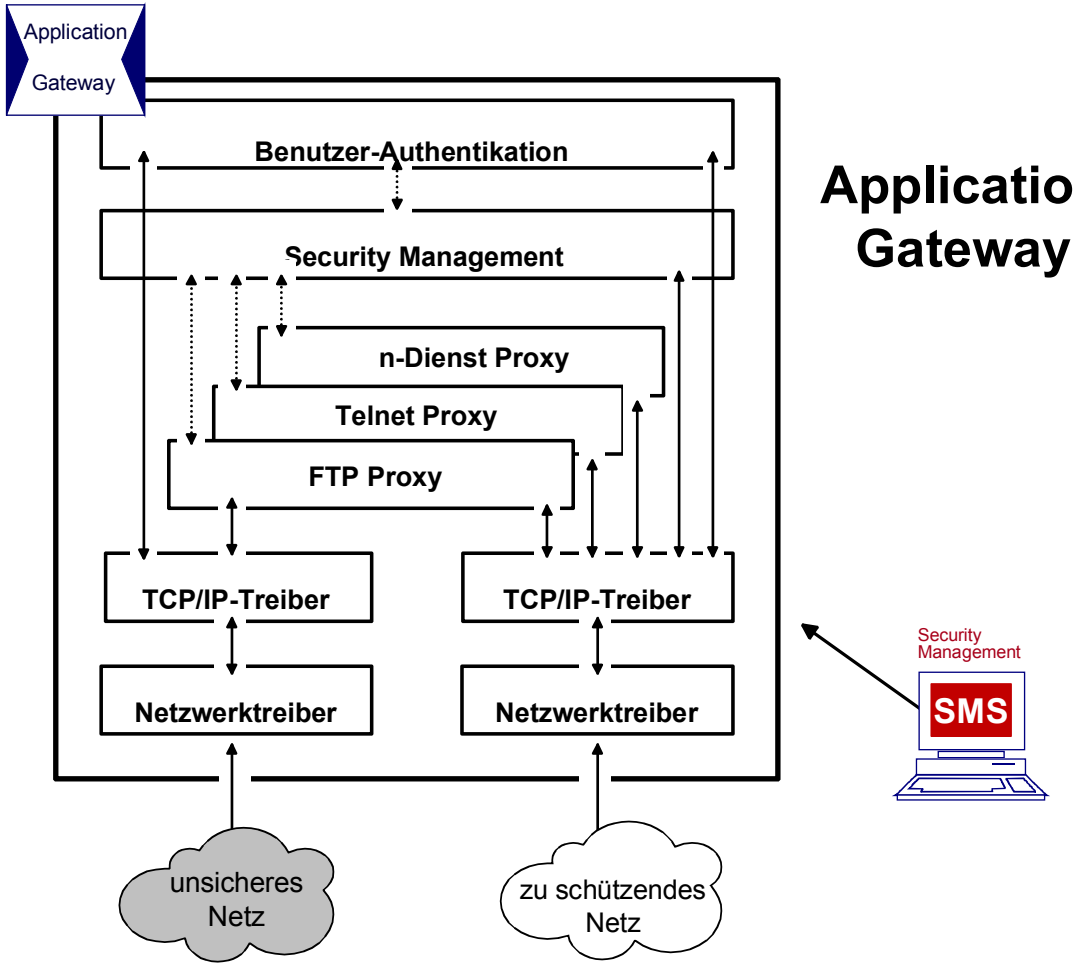
IP-Frame



Analysemöglichkeit eines TCP-Frames

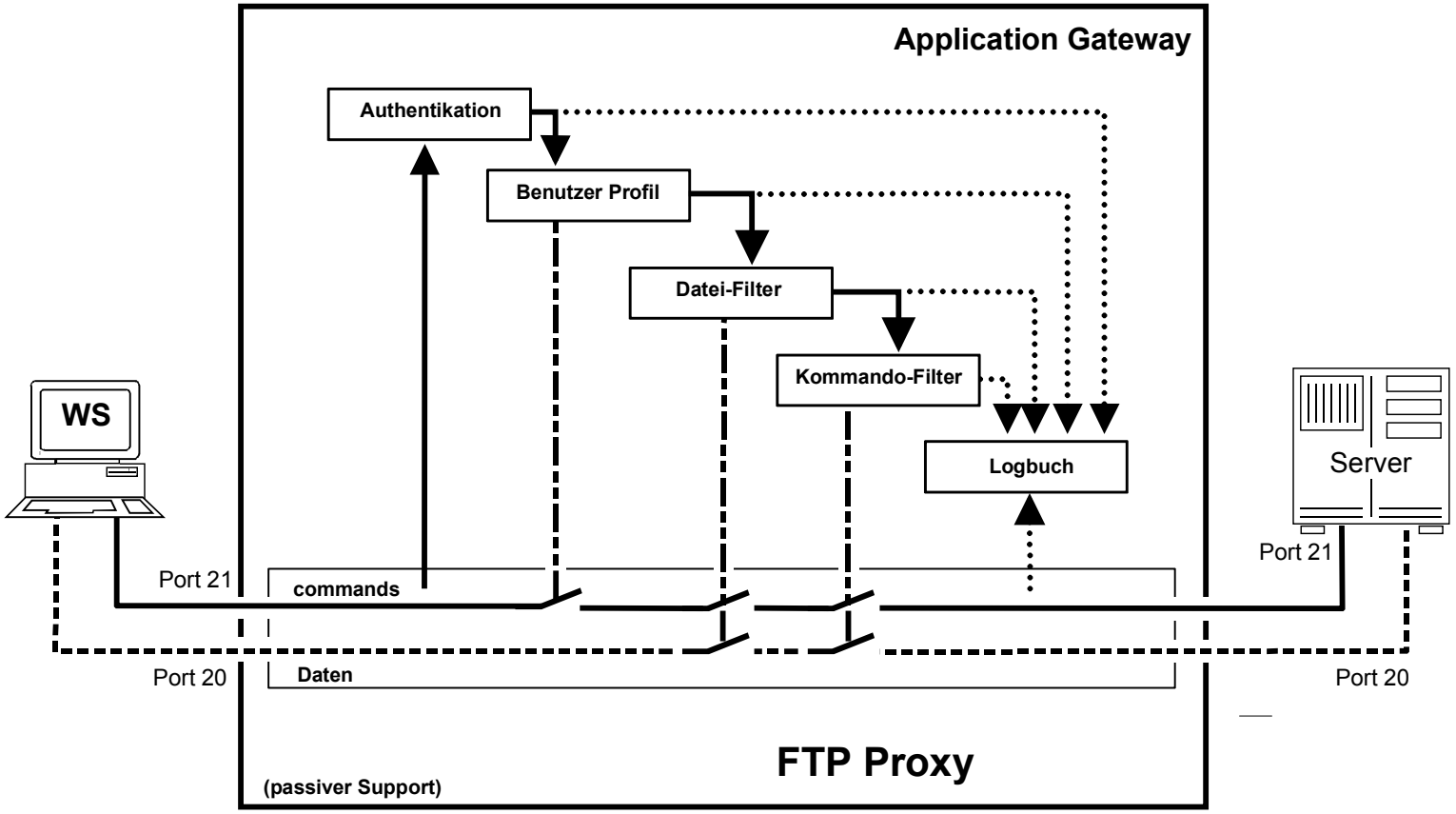


Application Gateway



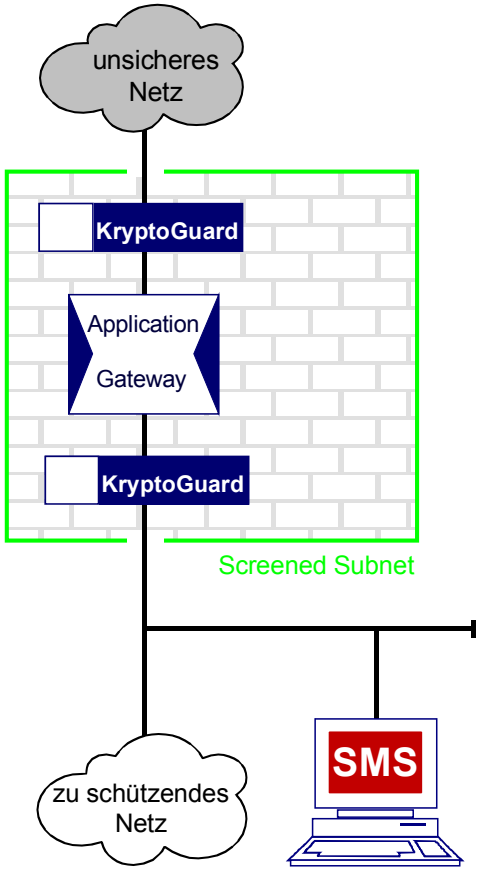
Application Gateway

FTP Proxy



High-level Security Firewall-System

- Einfache Regeln
- Gegenseitiger Schutz
- Geschachtelte Sicherheit
- Verschiedene Betriebssysteme
- Unterschiedliche Einbindungs- und Analysemöglichkeiten
- Separates Security Management



utimaco safeware

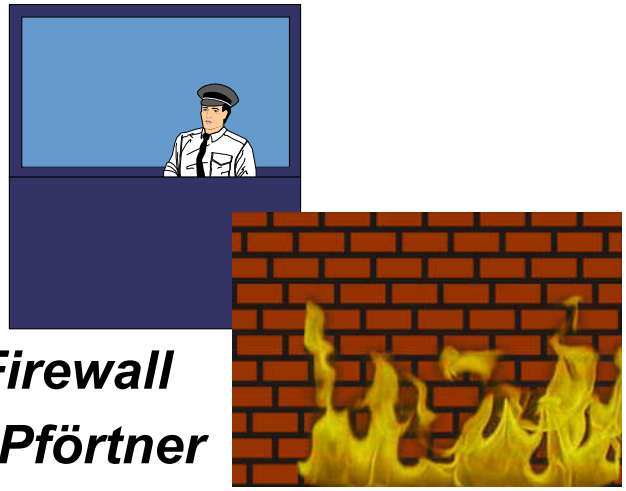
Firewall-System

Vorteile

- Jede Organisation ist für interne Sicherheit selbst verantwortlich
- Kein unerlaubter Zugang auf zu schützende Rechner
- Rechteverwaltung
- Beweissicherung

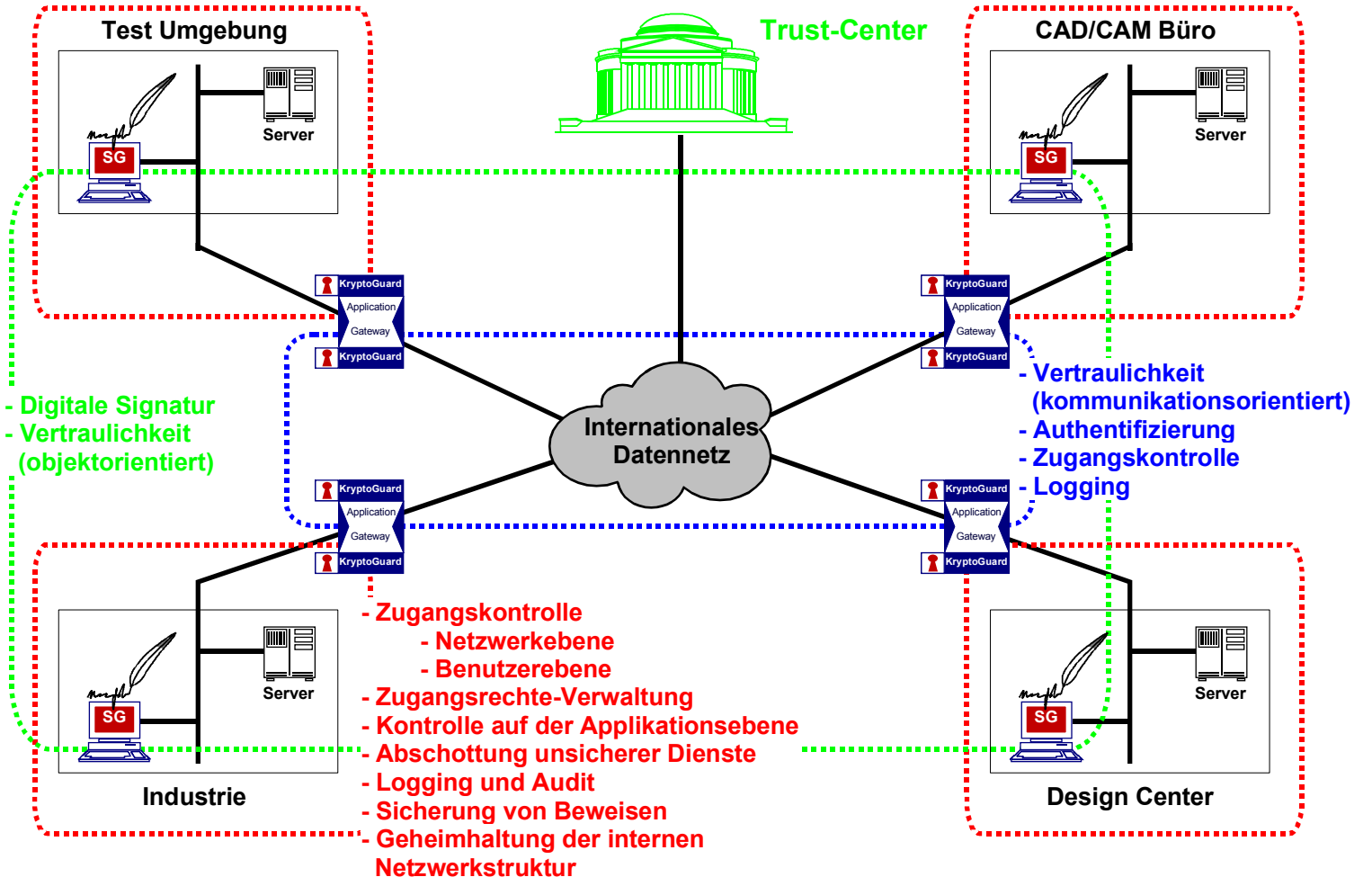
Nachteile

- Datenintegrität und Vertraulichkeit müssen mit anderen Mitteln realisiert werden
- Keine Verfügbarkeit
- Kein Sende- und Empfängernachweis möglich



als Firewall und Pförtner

Kombinationsmöglichkeiten



Zusammenfassung

- Lösungen für sichere Netzwerke sind vorhanden
- Kombination verschiedener Konzepte gewährleistet, daß alle Sicherheitsanforderungen erfüllt werden
- Organisationen mit eigener Verantwortung können unabhängig agieren
- Es besteht die Notwendigkeit, daß jeder seinen Schutzbedarf kennt

utimaco safeware

Utimaco Safeware AG

Your global partner for IT security

www.utimaco.com

info.de@utimaco.de