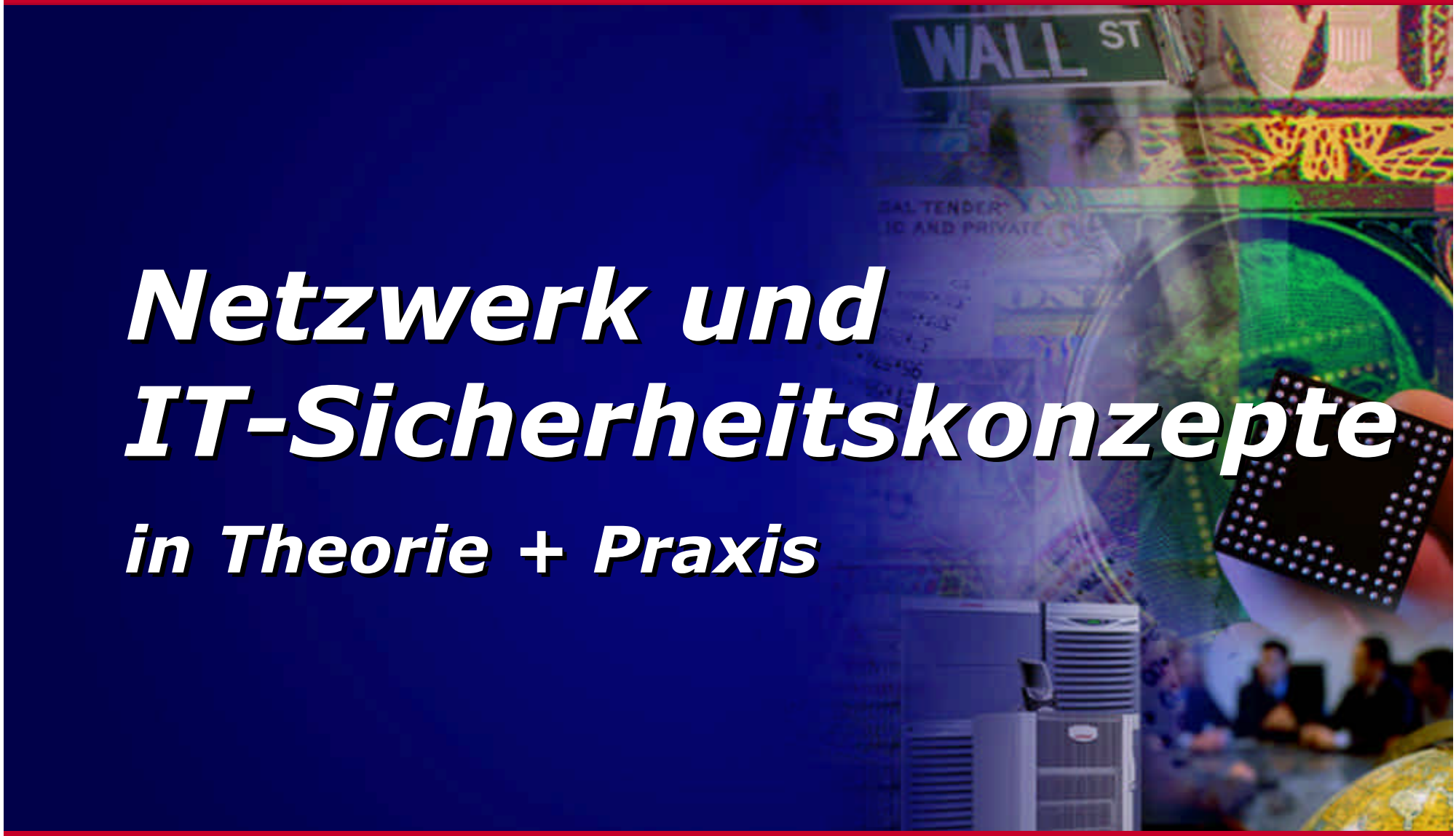
COMPAQ
Inspiration Technology




# Netzwerk und IT-Sicherheitskonzepte

## in Theorie + Praxis

# Vorstellung


Holger Rank

Project Manager Global Services

Compaq Computer GmbH

Kieler Straße 147

22769 Hamburg

Tel: 0172 4505057

Email: Holger.Rank@Compaq.com

COMPAQ

# Agenda

- Vorstellung Compaq Security Services
- Themeneinführung Security
- BSI Security-Konzept Aufbau
- Security Lösungen und Komponenten
  - Network Security
  - Firewall inkl. Content/Virus
  - Access / VPN
  - Intrusion Detection
  - Security Standard 802.1X
  - Desktop / Device Security
- Security Gesamtbild

COMPAQ

# Vorstellung Compaq

COMPAQ *Global Services* der Kompetenzpartner in:

- *Networking*
- *eCommerce*
- ***COMPAQ** Server*
- ***COMPAQ** PC's*
- *Consulting*
- *Projectmanagement*
- *Security Konzepte, Produkte und Lösungen*
- *Storage Area Networks*
- *Development*
- *Komplexes Troubleshooting*
  (Netzwerk, Betriebsysteme und Anwendungen)

- *Cisco Systems*
- *Cabletron Systems / Enterasys*
- *Microsoft Solutions*
- *Citrix Systems*
- *Novell Networking*
- *Unix, Tru64, Linux*
- *Systemsmangement*
  - *Tivoli*
  - *Aprisma / Spectrum*
  - *TNG*

COMPAQ

# Compaq Security Themen

- Security Checks / Basis Sicherheitschecks
- Security Konzepte
- Security Reviews
- Network Security
- Application/System Security
- Firewall Security
- Virus und Content Security
- VPN / Session Encryption
- Email Security / PKI

COMPAQ
Inspiration Technology

Compaq Global Services

# Themeneinführung Security

- **Themeneinführung Security**
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

COMPAQ

# Themeneinführung Security

## Warum brauchen wir Security Lösungen?

- Die Firmen müssen die **Vertraulichkeit**, **Integrität** sowie die **Verfügbarkeit** der IT-Systeme und Daten sicherstellen

- Ein Imageschaden wäre für die meisten Firmen existenzbedrohlich

- Datenschutzauflagen der Regierung und Länder

COMPAQ

# Themeneinführung Security

## Was sind die Gefahren die uns bedrohen?

- Keine sicherheitssensiblen Mitarbeiter
  - kein Sicherheitsbewusstsein - wichtige Daten liegen frei zugänglich
  - Informationen werden unbeabsichtigt nach außen getragen
  - die offene Tür des Büros
  - Fremde Personen im Gebäude
  - Notizen über Passwörter
  - Schwache Passwortverfahren - alle verwenden das gleiche Passwort

COMPAQ

# Themeneinführung Security

## Was sind die Gefahren die uns bedrohen?

- Der gezielte Angriff von **innen** auf Firmendaten
  - 60-80% der Angriffe kommen von innen!
  - Beispiel: bewusstes platzieren von Fehlern z.B. in der Datenbank
- gezielte Angriff von außen auf Firmendaten
  - „Das neue Produkt“
  - Konkurrenz - Konkurrenten ausschalten
  - Bei Schulen Angriffe der Schüler/Studenten auf die Zensurdatenbank, Klausuren usw.

COMPAQ

# Themeneinführung Security

## Was sind die Gefahren die uns bedrohen?

Der Draht nach außen….

- Die Internetanbindung der Firma
- Daten und Sprachleitungen zwischen den einzelnen Standorten der Firma
- Fax
- Telefon
- Email
- Post (Brief / Paket)

COMPAQ

# Themeneinführung Security

## Was sind die Gefahren die uns bedrohen?

Das Hausnetz….

- Frei zugängliche PC‘s und Server
- Ungenügend geschützte Daten (Files usw.) auf den PC‘s und Servern
- keine Passwörter für den Bildschirmschoner usw.
- Standard Passwortschutz - keine Smartcards usw.
- Viren ( I love you )
- Diskettenlaufwerke

COMPAQ

# Definition einer “Security Policy”

COMPAQ

# Themeneinführung Security

***Wie sieht die***

***Lösung aus?***

COMPAQ

## Themeneinführung Security

# Was fehlt… ?

ein ***Sicherheitskonzept***

COMPAQ
Inspiration Technology

Compaq Global Services

# Security-Konzept Aufbau

- Themeneinführung Security
- **Security-Konzept Aufbau**
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

COMPAQ

# Themeneinführung Security

## Der Inhalt eines Security Konzeptes

1. Ist-Aufnahme aller IT-Systeme
2. Schutzbedarfsfeststellung
3. Bedrohungsanalyse
4. Anforderungskatalog
5. Einteilen in Sicherheitsbereiche
6. Mögliche Sicherheitsmaßnahmen
7. Empfohlenen Sicherheitsmaßnahmen
8. Stufenkonzept

COMPAQ
Inspiration Technology

Compaq Global Services

# BSI Security-Konzept Vorgehensmodell

- Themeneinführung Security
- Security-Konzept Aufbau
- **BSI Security-Konzept**
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

COMPAQ
Inspiration Technology

# Ist-Situation

Schutzbedarfsfeststellung

Bedrohungsanalyse

Anforderungskatalog

Einteilen in Sicherheitsbereiche

Mögliche Sicherheitsmaßnahmen

Empfohlene Sicherheitsmaßnahmen

Stufenplan

COMPAQ

# Ist-Situation

- Netzwerkstrukturen
- Betriebssysteme
- Anwendungen
- Dateninhalte
- Kommunikationsverhalten
- Schutzanforderungen
- Wie sieht die Policy heute aus?
- Wie ist das Sicherheitsgefühl?

COMPAQ
Inspiration Technology

Ist-Situation

## Schutzbedarfsfeststellung

Bedrohungsanalyse

Anforderungskatalog

Einteilen in Sicherheitsbereiche

Mögliche Sicherheitsmaßnahmen

Empfohlene Sicherheitsmaßnahmen

Stufenplan

COMPAQ

# Schutzbedarfsfeststellung

## Erfassung aller IT-Systeme

| Nr. | Bezeichnung | Lokation | Vernetzt mit | Status | Benutzer |
|---|---|---|---|---|---|
| 1 | HOST | Haus 7 | allen Werken<br>Fernwartung<br>Zulieferer<br>2,3,4,6,7,8 | in Betrieb | alle |
| 2 | PC-LAN | in allen Häusern | Fernwartung<br>1,2,7 | in Betrieb | alle |
| 3 | ... | ... | ... | ... | ... |

COMPAQ

# Schutzbedarfsfeststellung

## Erfassung der schutzbedürftigen IT-Anwendungen

| Nr. | **Bezeichnung** | **Schutzbedürftige IT-Anwendungen (grob absteigend vorsortiert)** |
|---|---|---|
| 1 | HOST | Personalwesen<br>Zeiterfassung<br>Rechnungswesen<br>Beschaffungsmarkt<br>Vertrieb<br>Controlling<br>Materialwirtschaft<br>Anwenderprogramme |
| 2 | PC-LAN | MS-Word<br>MS-Excel<br>MS-Powerpoint<br>MS-Access<br>MS-Mail<br>usw. |
| 3 | ... | ... |

COMPAQ

# Schutzbedarfsfeststellung

## Feststellung des Schutzbedarfs für jedes IT-System

| Nr. | Bezeichnung | Grundwert | mittel | hoch | sehr hoch | Begründung |
|---|---|---|---|---|---|---|
| 1 | HOST | Vertrau-lichkeit | | X | | Auf diesem System stehen strategische Informationen wie Geldströme und Warenströme von und zu Kunden/Lieferanten, die für den Wettbewerb einen erheblichen Wert darstellen (deutlich mehr als DM 25.000). |
| | | Integrität | | | X | Durch eine Manipulation der Materialwirtschaft kann die Logistik so stark beeinflußt werden, daß die Produktion falsch läuft, das notwendige Material fehlt, falsche Lieferzeiten berücksichtigt werden, usw. Dieser Umstand kann zu einem finanziellen Schaden über 5 Millionen DM führen. |
| | | Verfüg-barkeit | | X | | Verzögerte Bearbeitung von Verwaltungsvorgängen und verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen sind bis zu einem Tag tolerabel. Ein längerer Ausfall des Systems hätte einen Renommeeverlust des Unternehmens zur Folge und würde zu einen finanziellen Schaden deutlich über DM 25.000,--führen. |
| 2 | PC-LAN | Vertrau-lichkeit | | | X | Auf diesen Rechnersystemen wird die Korrespondenz gespeichert. Da hier streng vertrauliche Informationen |

COMPAQ
Inspiration Technology

Ist-Situation

Schutzbedarfsfeststellung

**Bedrohungsanalyse**

Anforderungskatalog

Einteilen in Sicherheitsbereiche

Mögliche Sicherheitsmaßnahmen

Empfohlene Sicherheitsmaßnahmen

Stufenplan

COMPAQ

# Bedrohungsanalyse

| Bedrohungen | Bewertung/relevant |
|---|---|
| Höhere Gewalt<br>- G 1.1 Personalausfall<br>- G 1.2 Ausfall des IT-Systems<br>- G 1.4 Feuer<br>- G 1.5 Wasser<br>- G 1.8 Staub, Verschmutzung | Wird als geringe Bedrohung angesehen. Bei Ausfall des Systemadministrators ist eine Vertretung sichergestellt. Ein Ausfall des IT-Systems wird durch ein vorhandenes Ersatzssystem aufgefangen. Die entsprechenden Räume sind gegen evtl. auftretende Schäden gesichert. |
| Menschliche Fehlhandlungen<br>- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten<br>- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen<br>- G 3.5 Unbeabsichtigte Leitungsbeschädigung<br>- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal<br>- G 3.8 Fehlerhafte Nutzung des IT-Systems<br>- G 3.9 Fehlerhafte Administration des IT-Systems | Aufgrund der Ausbildung und ständigen Information des zuständigen Technik-Personals wird eine geringe Bedrohung gesehen. Der Zutritt und Aufenthalt Außenstehender zu den schutzbedürftigen Räumen erfolgt nur in Anwesenheit der Zutrittsberechtigten |
| | |

COMPAQ
Inspiration Technology

Ist-Situation

Schutzbedarfsfeststellung

Bedrohungsanalyse

## Anforderungskatalog

Einteilen in Sicherheitsbereiche

Mögliche Sicherheitsmaßnahmen

Empfohlene Sicherheitsmaßnahmen

Stufenplan

COMPAQ

# Anforderungskatalog

- Der Anforderungskatalog ist geprägt durch die Anforderungen der Sicherheitspolitik (Policy) und des Datenschutzes
- Basis für den Anforderungskatalog ist das Abschlussdokument der Schutzbedarfsfeststellung
- Ziel des Anforderungskataloges ist die genaue Beschreibung der Anforderungen eines oder einer Gruppe von IT-Systemen an das Sicherheitskonzept

COMPAQ

# Anforderungskatalog

## Die einzusetzenden Sicherheitskriterien

- Verlust der Vertraulichkeit
  - Daten werden bekannt
- Verlust der Integrität
  - Daten werden verändert und verfälscht
- Verlust der Verfügbarkeit
  - Systemstillstand

COMPAQ
Inspiration Technology

Ist-Situation

Schutzbedarfsfeststellung

Bedrohungsanalyse

Anforderungskatalog

## Einteilen in Sicherheitsbereiche

Mögliche Sicherheitsmaßnahmen

Empfohlene Sicherheitsmaßnahmen

Stufenplan

COMPAQ

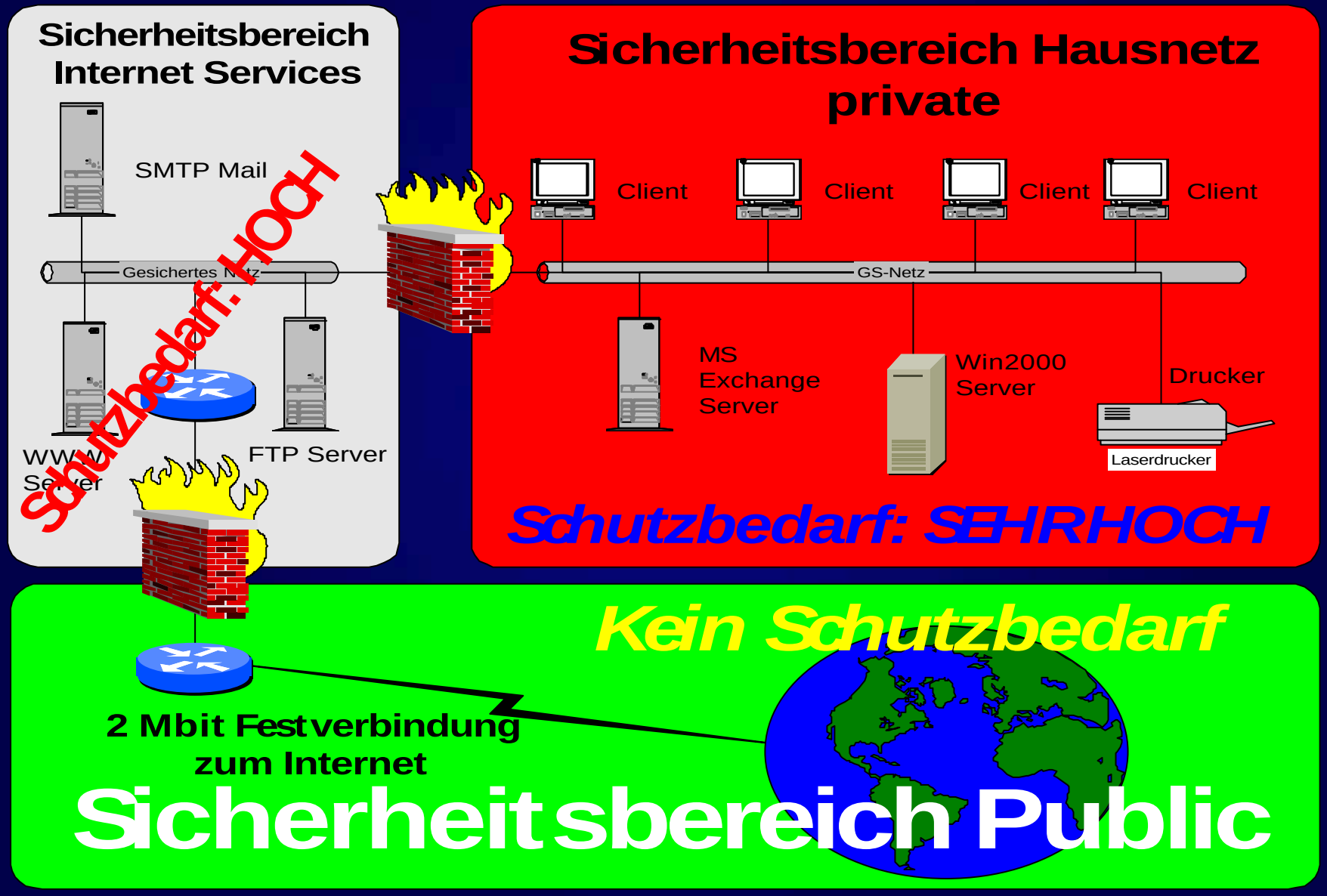
# Sicherheitsbereiche

Zweck von Sicherheitsbereichen:

- Schaffung einer klaren Sicherheitstopologie und IT-Infrastruktur
- Einbringen von Kontrollstrukturen beim Übergang von einem zum anderen Sicherheitsbereich
- Zusammenfassen von IT-Systemen mit gleichem Schutzbedarf
- Bildung klarer Kommunikationsflüsse
- Definition der anzuwendenden Sicherheitsmaßnahmen wie z.B. Verschlüsselung
- Kosteneinsparungen

COMPAQ

# Sicherheitsbereiche



COMPAQ
Inspiration Technology

Ist-Situation

Schutzbedarfsfeststellung

Bedrohungsanalyse

Anforderungskatalog

Einteilen in Sicherheitsbereiche

**Mögliche Sicherheitsmaßnahmen**

Empfohlene Sicherheitsmaßnahmen

Stufenplan

COMPAQ

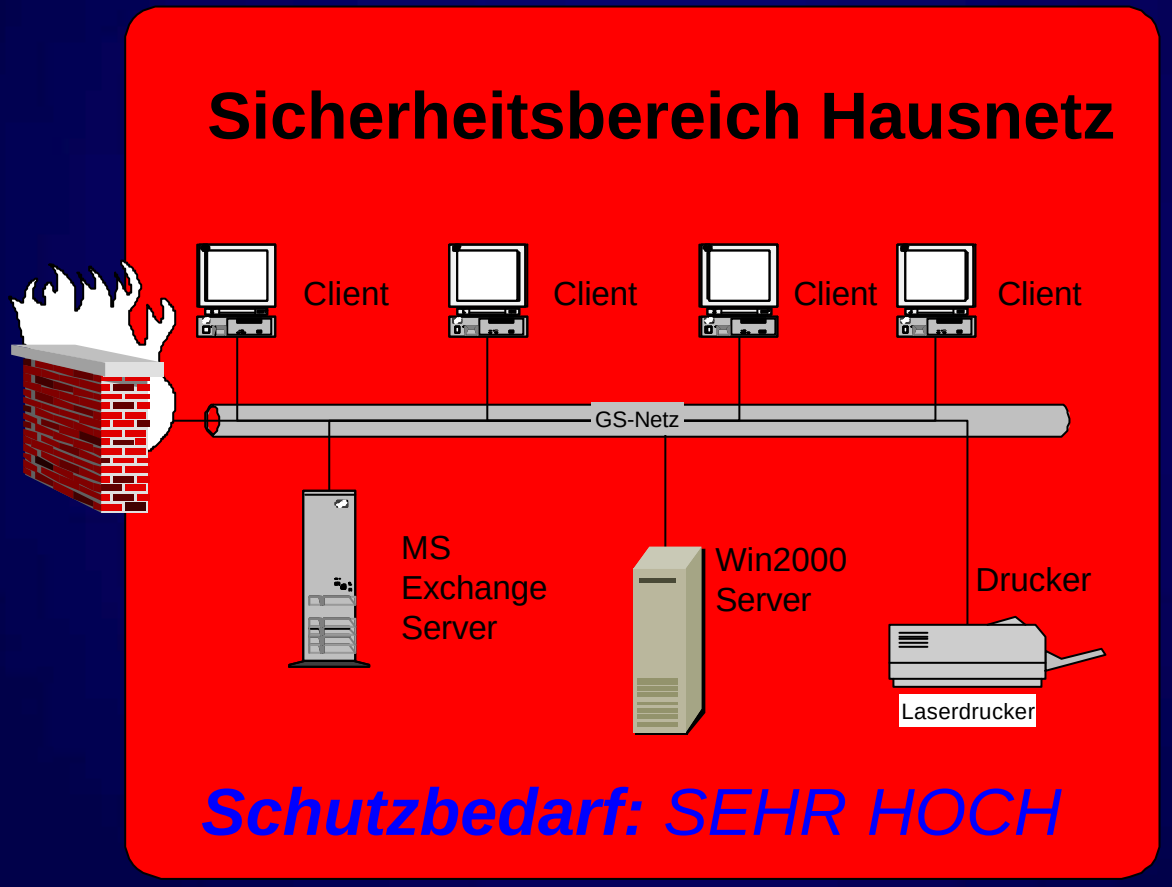
# Mögliche Sicherheitsmaßnahmen

- Hier werden alle möglichen Grundschutz-Sicherheitsmaßnahmen für ein IT-System benannt
- Als Basis dient das BSI Grundschutzhandbuch (BSI GSHB)
- Die BSI GSHB Maßnahmen werden unterteilt in
  - Infrastruktur
  - Organisation
  - Personal
  - Hard- / Software
  - Kommunikation
  - Notfallvorsorge
- Tiefergehende Maßnahmen als die des BSI-GSHB

COMPAQ

# Mögliche Sicherheitsmaßnahmen

## Beispiel für ein Sicherheitsbereich

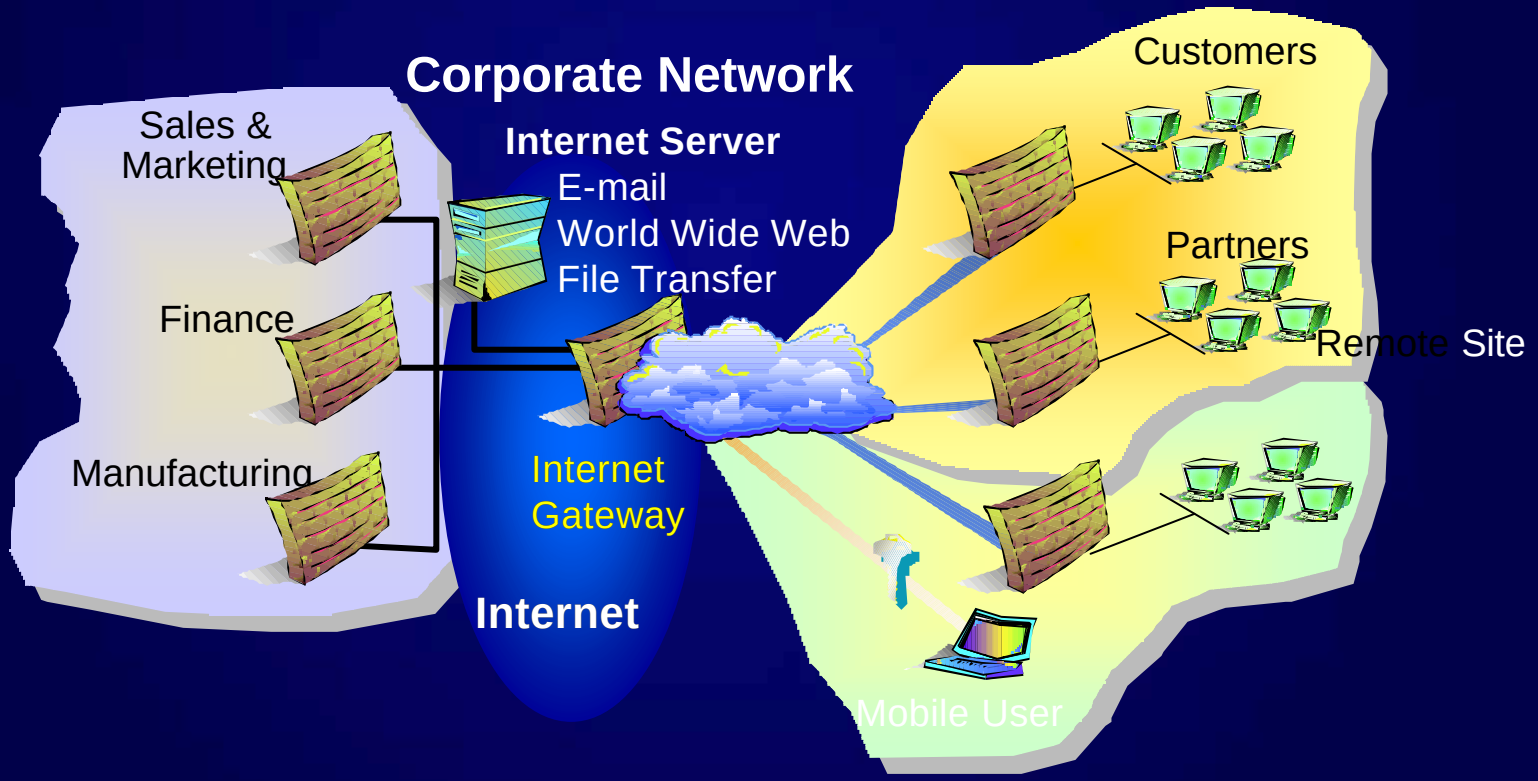


COMPAQ

# Mögliche Sicherheitsmaßnahmen

## Beispiel für eine Maßnahme

## Extranet VPN



COMPAQ
Inspiration Technology

Ist-Situation

Schutzbedarfsfeststellung

Bedrohungsanalyse

Anforderungskatalog

Einteilen in Sicherheitsbereiche

Mögliche Sicherheitsmaßnahmen

**Empfohlene Sicherheitsmaßnahmen**

Stufenplan

COMPAQ

# Empfohlene Sicherheitsmaßnahmen

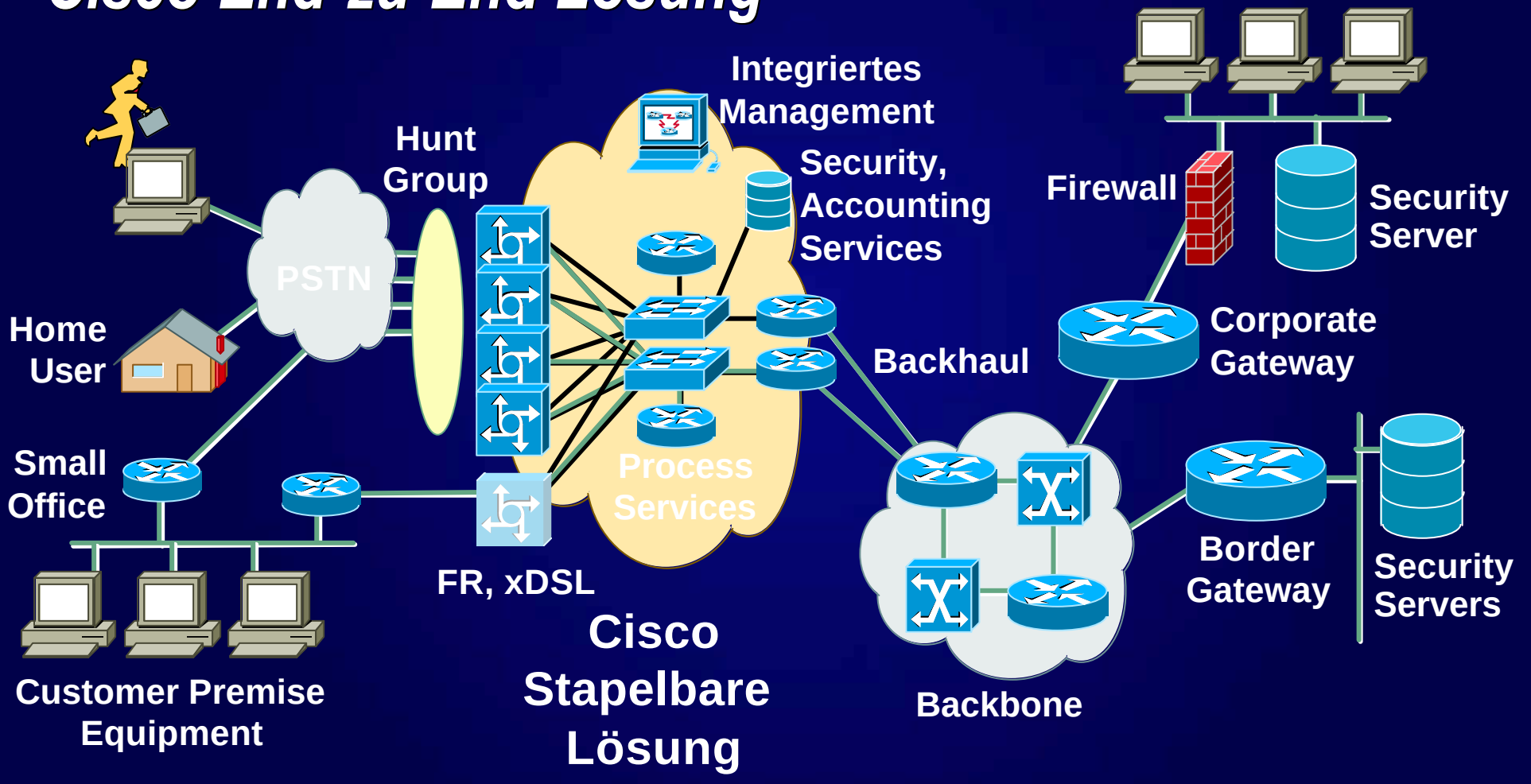
## Beispiele...

- Einsatz von VPNs mit Verschlüsselung
- Bildung verschiedener Sicherheitsbereiche wie z.B. DMZ (Demilitarisierte Zone)
- Einsatz von Firewalls inkl. Proxies für
  - Content Checking
  - Virusscanning
  - Mail und Traffic Entkopplung
- Intrusion Detection Systeme

COMPAQ

# Empfohlene Sicherheitsmaßnahmen

## *Cisco End-zu-End Lösung*



COMPAQ
Inspiration Technology

- Ist-Situation
- Schutzbedarfsfeststellung
- Bedrohungsanalyse
- Anforderungskatalog
- Einteilen in Sicherheitsbereiche
- Mögliche Sicherheitsmaßnahmen
- Empfohlene Sicherheitsmaßnahmen
- Stufenplan

COMPAQ

# Stufenplan

Der Stufenplan definiert die zeitliche Vorgehensweise unterteilt in:

- kurzfristige Umsetzung
- mittelfristige Umsetzung
- langfristige Umsetzung

COMPAQ

# Stufenplan kurzfristige Umsetzung

- Je nach Dringlichkeit wird ein Zeitrahmen von 1 Woche bis ca. 1 Monat zugrunde gelegt
- Sind Sicherheitsmaßnahmen die eine direkte vorhandene Gefahr mindern sollen
- Es sollen die gefährlichsten Punkte des Sicherheitskonzeptes bzw. der festgestellten Mängel behoben werden
- Ein Beispiel: Alle Laufwerke der Windows NT Maschinen sind für alle freigegeben

COMPAQ

# Stufenplan mittelfristige Umsetzung

- Je nach Dringlichkeit wird ein Zeitrahmen von 1 Monat bis zu 6 Monaten zugrunde gelegt
- Aktionen die eine genauere Planung für die Umsetzung der geforderten Maßnahmen erfordern
- Aufgaben die nicht in der kurzfristigen Umsetzung bearbeitet bzw. vollendet werden konnten
- Alle Aufgaben des Sicherheitskonzeptes mit einer mittleren Priorität

COMPAQ

# Stufenplan langfristige Umsetzung

- Je nach Dringlichkeit wird ein Zeitrahmen von mehr als 6 Monaten zugrunde gelegt
- Aufgaben mit einer niedrigen Priorität
- Aufgaben die nicht in der mittelfristigen Umsetzung bearbeitet bzw. vollendet werden konnten
- Teilprojekte die einen erheblichen Aufwand in der Planung benötigen

COMPAQ
Inspiration Technology

Compaq Global Services

# Security Lösungen und Komponenten

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- **Security Lösungen und Komponenten**
- Network Security
- Firewall
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

COMPAQ
Inspiration Technology

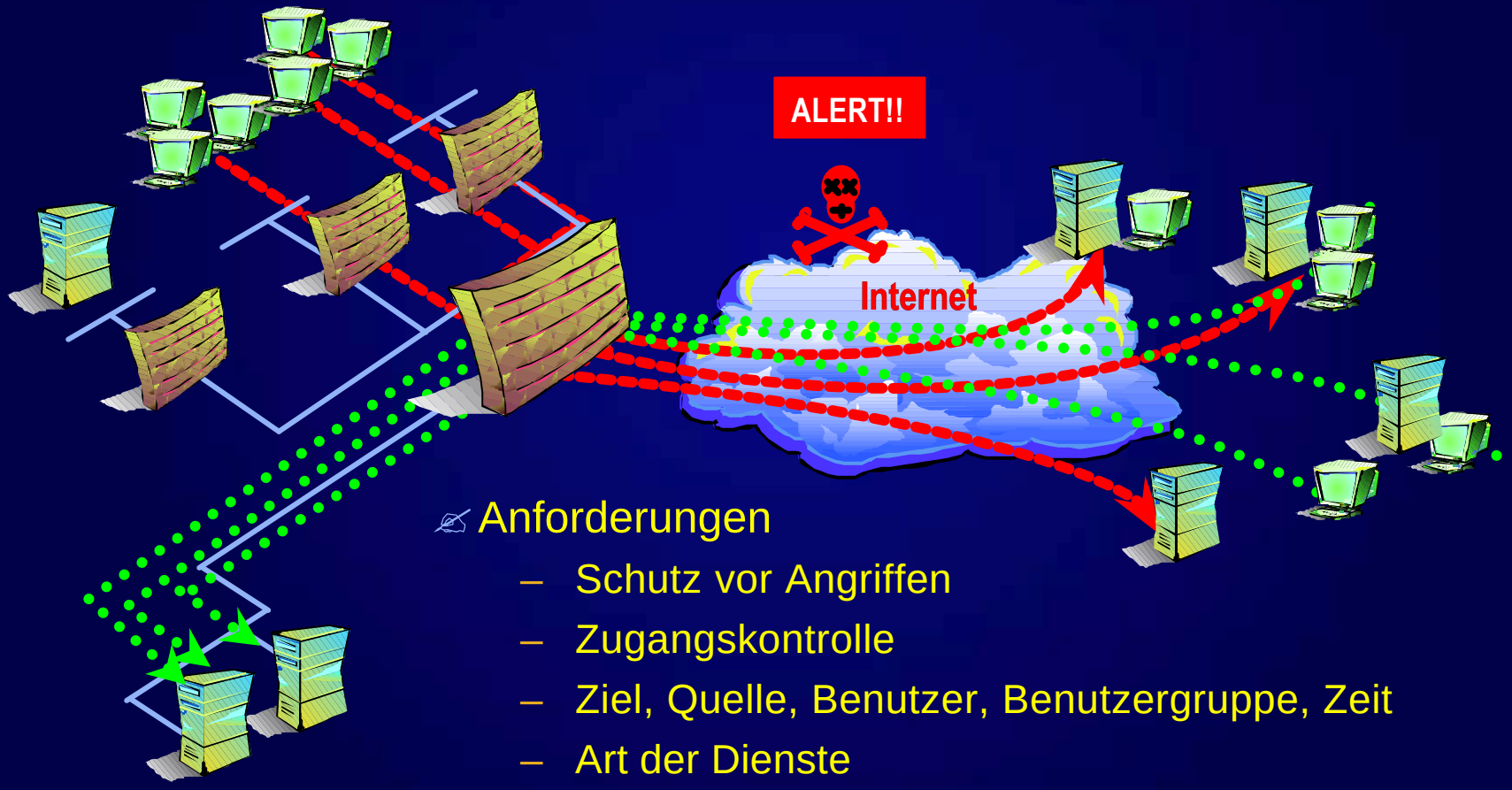
Compaq Global Services

# Network Security

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- **Network Security**
- Firewall
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

COMPAQ

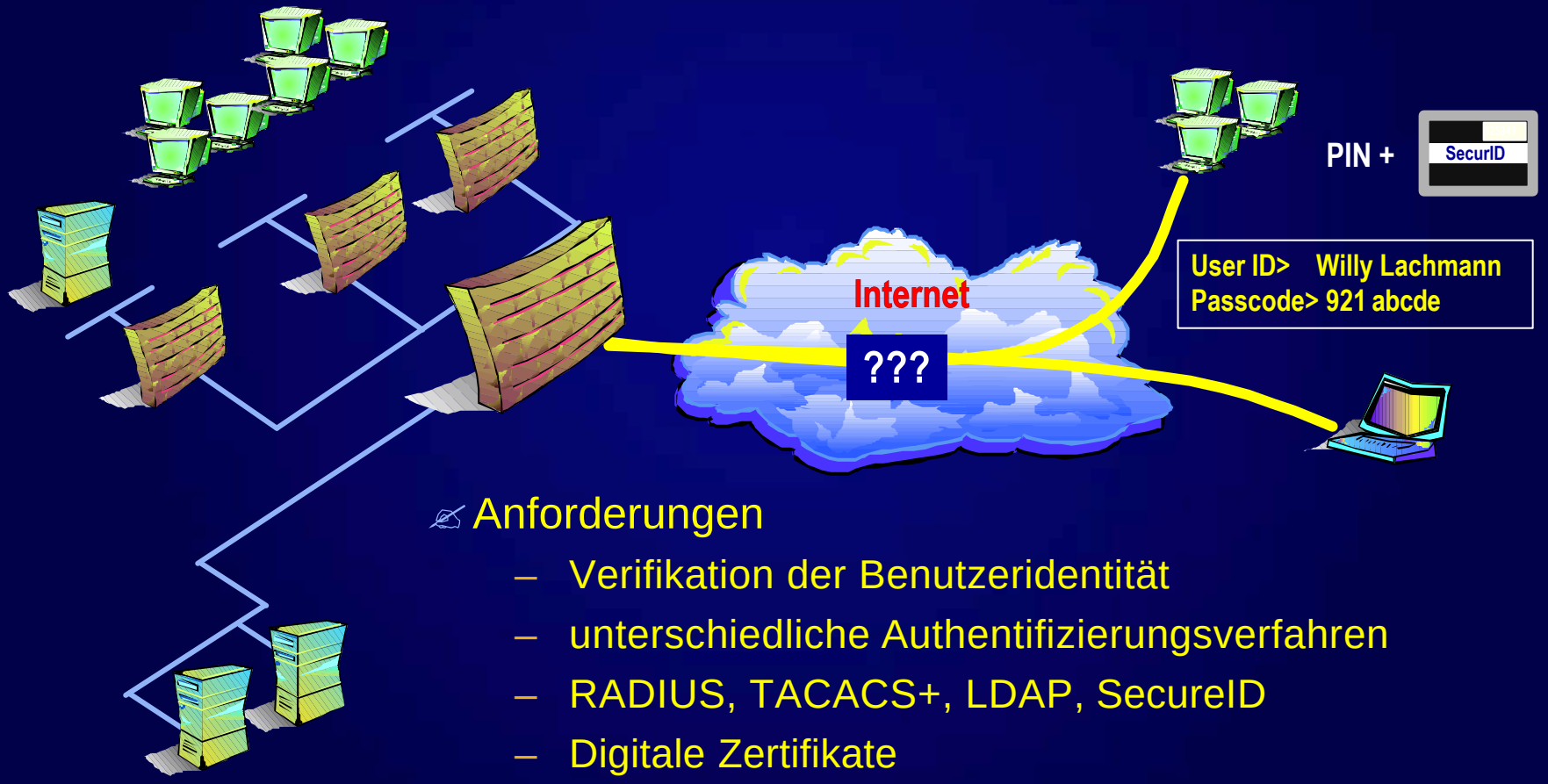
# Security Solution: Access Control




- Anforderungen
  - Schutz vor Angriffen
  - Zugangskontrolle
  - Ziel, Quelle, Benutzer, Benutzergruppe, Zeit
  - Art der Dienste

COMPAQ

# Security Solution: Authentifizierung




- Anforderungen
  - Verifikation der Benutzeridentität
  - unterschiedliche Authentifizierungsverfahren
  - RADIUS, TACACS+, LDAP, SecureID
  - Digitale Zertifikate

COMPAQ

# Security Solution: Encryption + Integrität


- Anforderungen
  - Sicherstellung der Vertraulichkeit
  - Selektive Verschlüsselung von Verbindungen
  - Standard-basierende VPN-Unterstützung, z.B. IKE (IPSec/ISAKMP Oakley)
  - strenge Algorithmen (MD5, SHA-1, DES, 3DES)

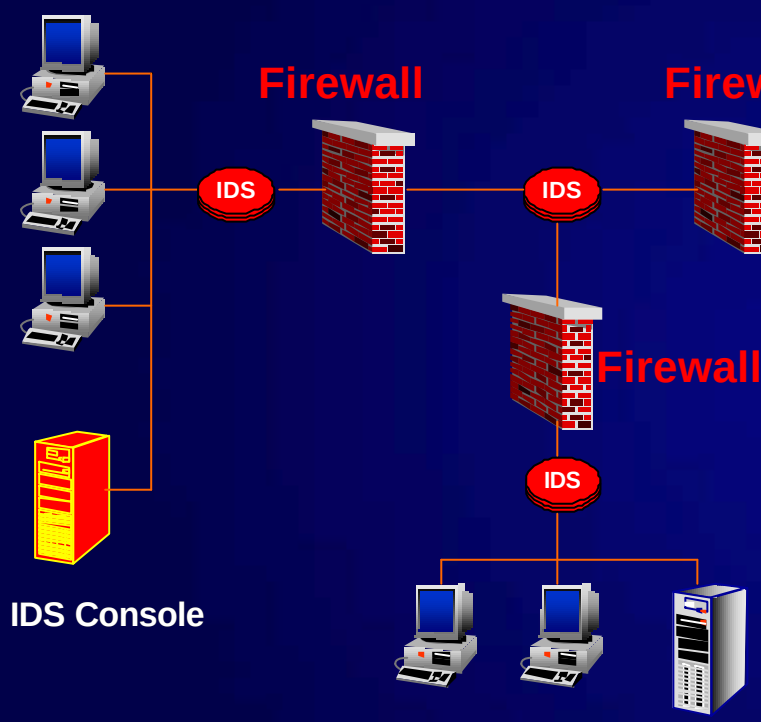
COMPAQ

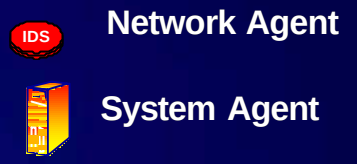
# Security Solution: Content Security


- Anforderungen
  - Schutz vor böswilligem Inhalt und Viren
  - Java, ActiveX, VBScript etc.
  - Real-Time Scanning

COMPAQ

# Security Solution: Intrusion Detection




- Anforderungen
  - proaktives Erkennen u. Identifizieren von Attacken
  - Session Recording
  - Rekonfiguration von Firewall-Systemen
  - Host-basierend, Netzwerk-basierend
  - Durchsetzung der Sicherheitspolicies

COMPAQ
Inspiration Technology

Compaq Global Services

# Firewall

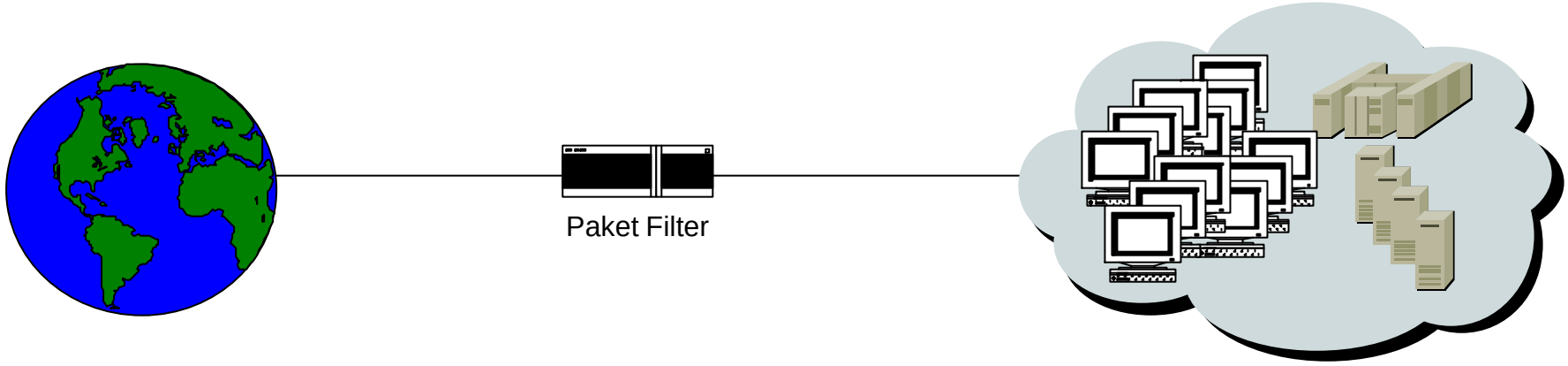
- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- **Firewall**
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

COMPAQ

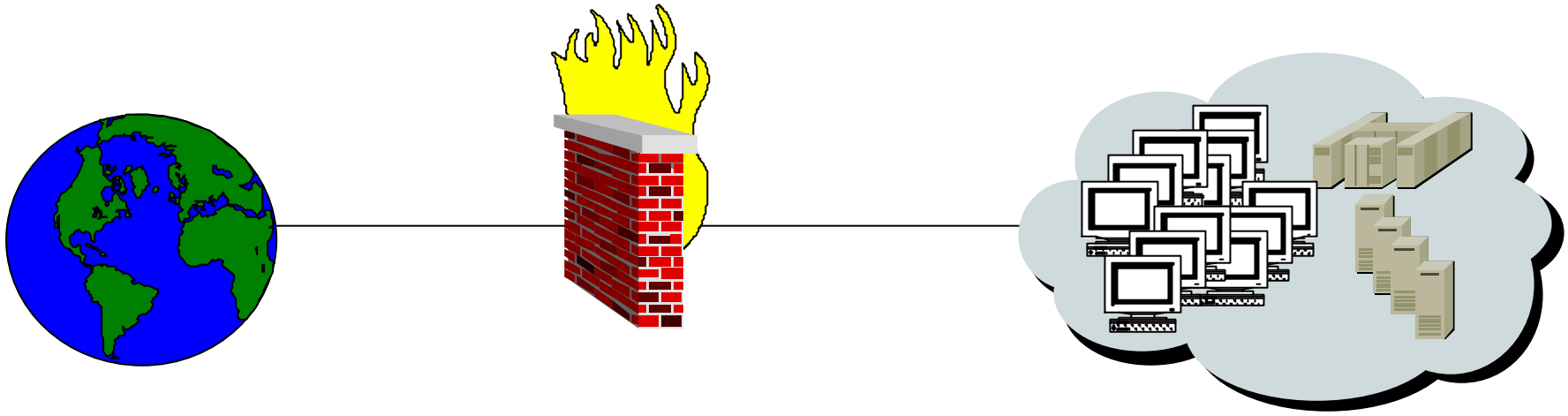
# Überblick Firewall

- Paket Filter (Router, Switches)
- Stateful Inspection Firewall
- Application Gateway Firewall
- Kombination aus allen
- Verschiedene technische FW-Konzepte
- Firewall Lösungen für spezielle Erfordernisse

# Paketfilter



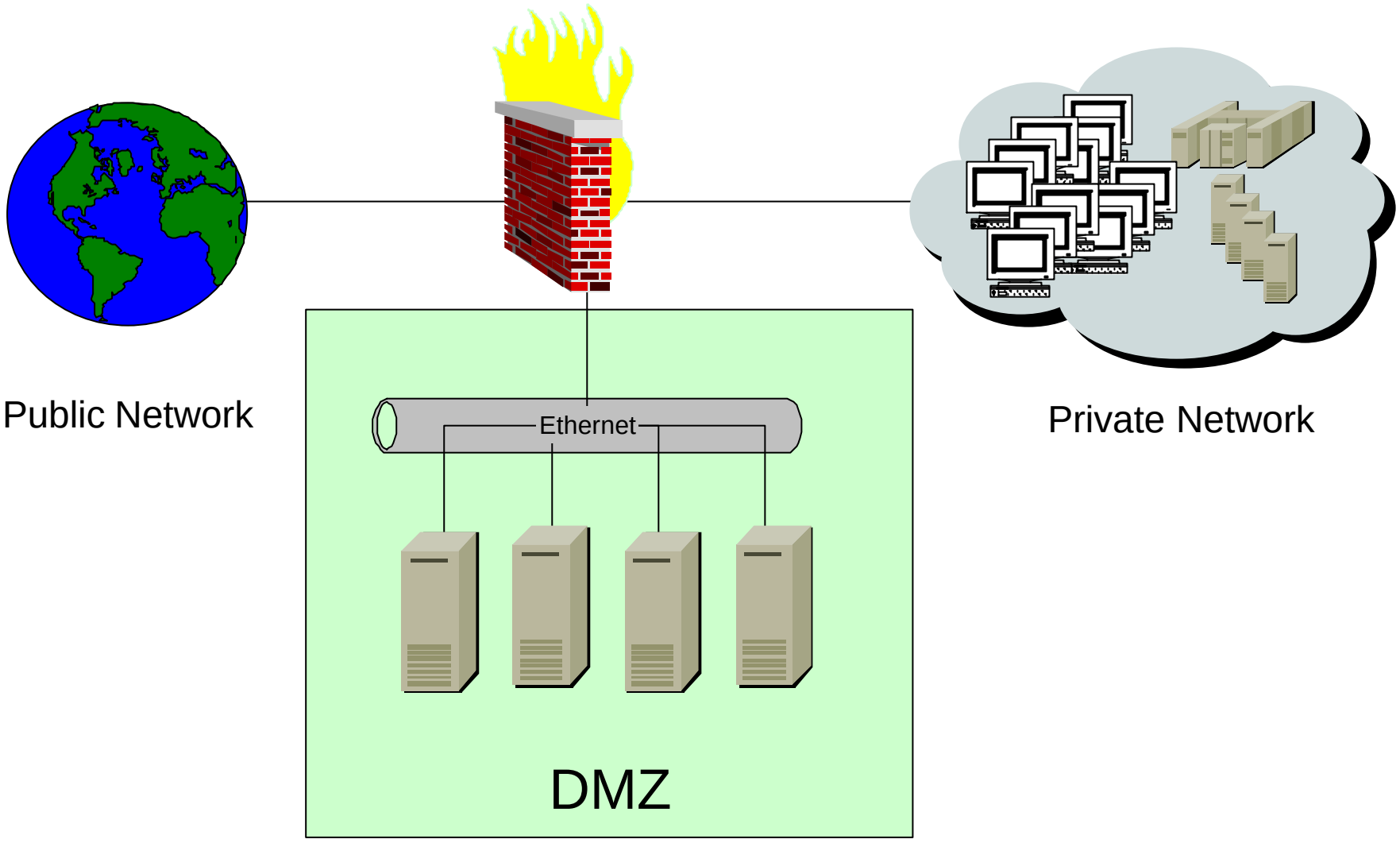
# Firewall Typ 1 - Standard



Public Network

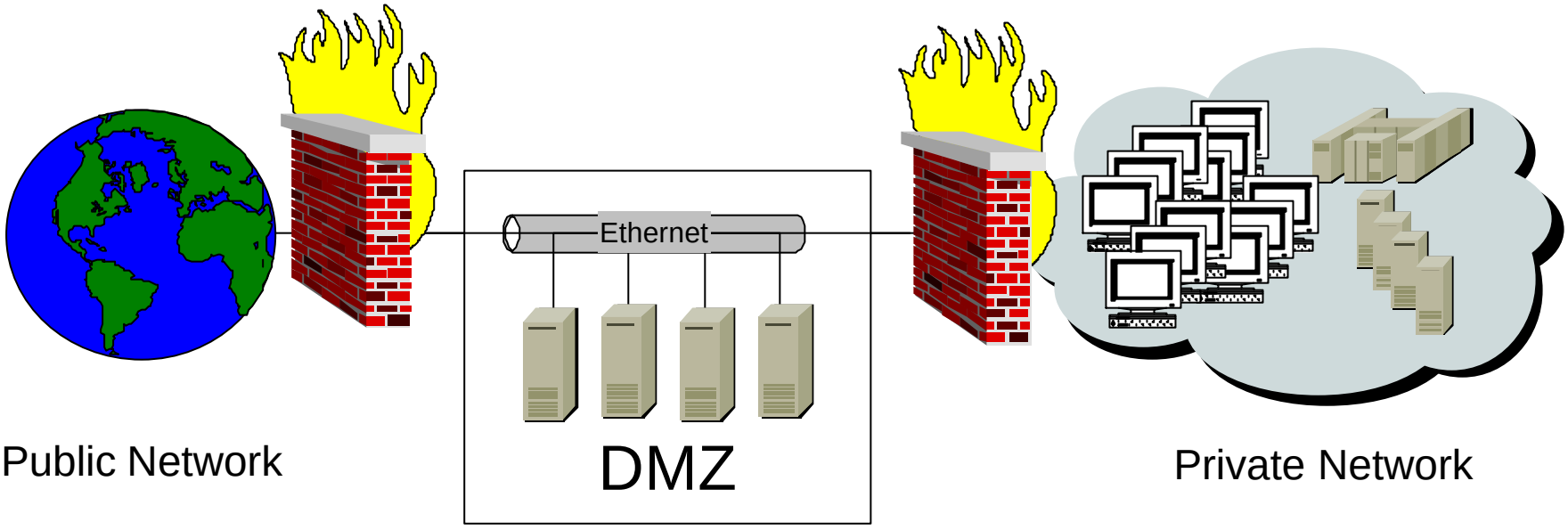
Private Network

# Firewall Typ 2 – Standard DMZ

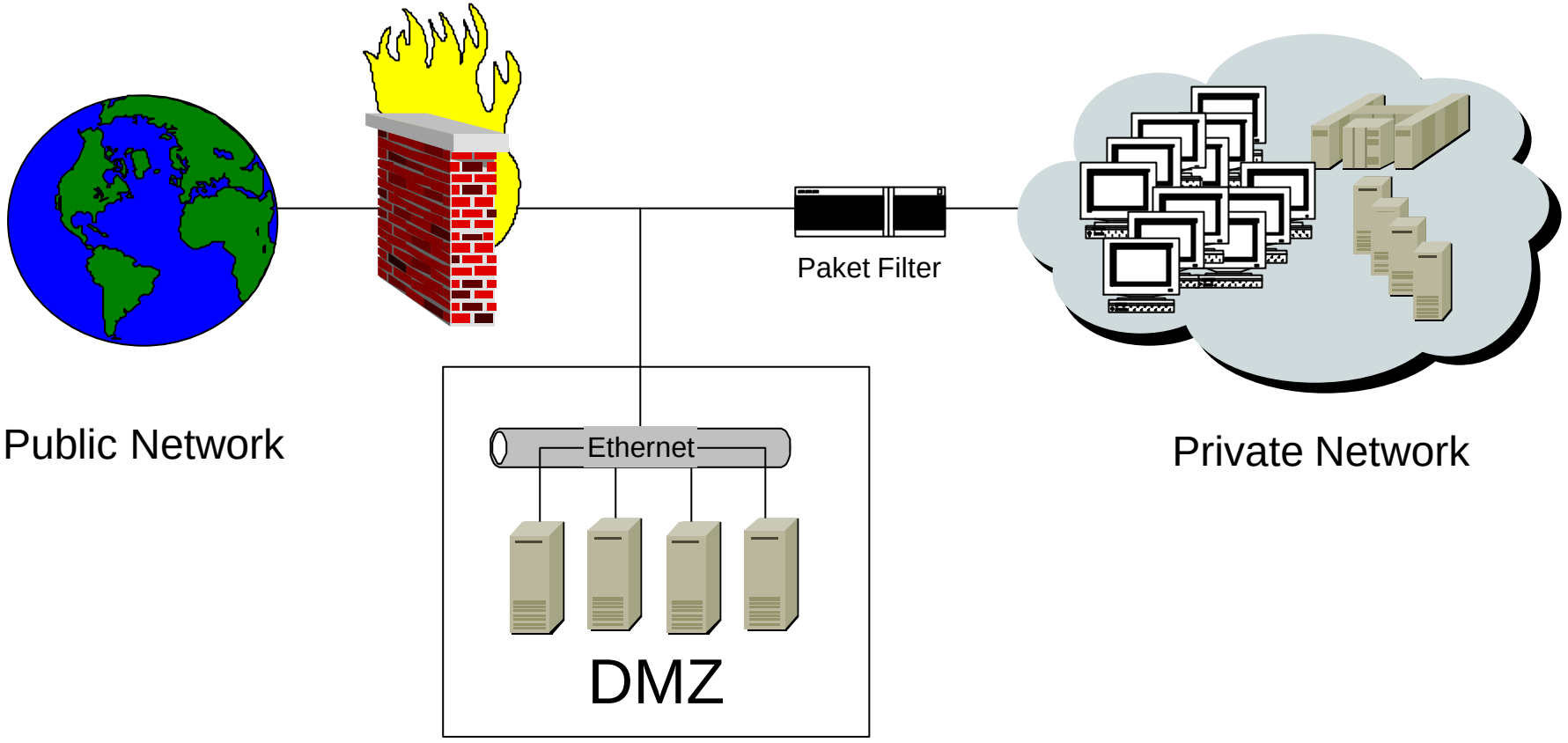


COMPAQ

# Firewall Typ 3 – 2x FW

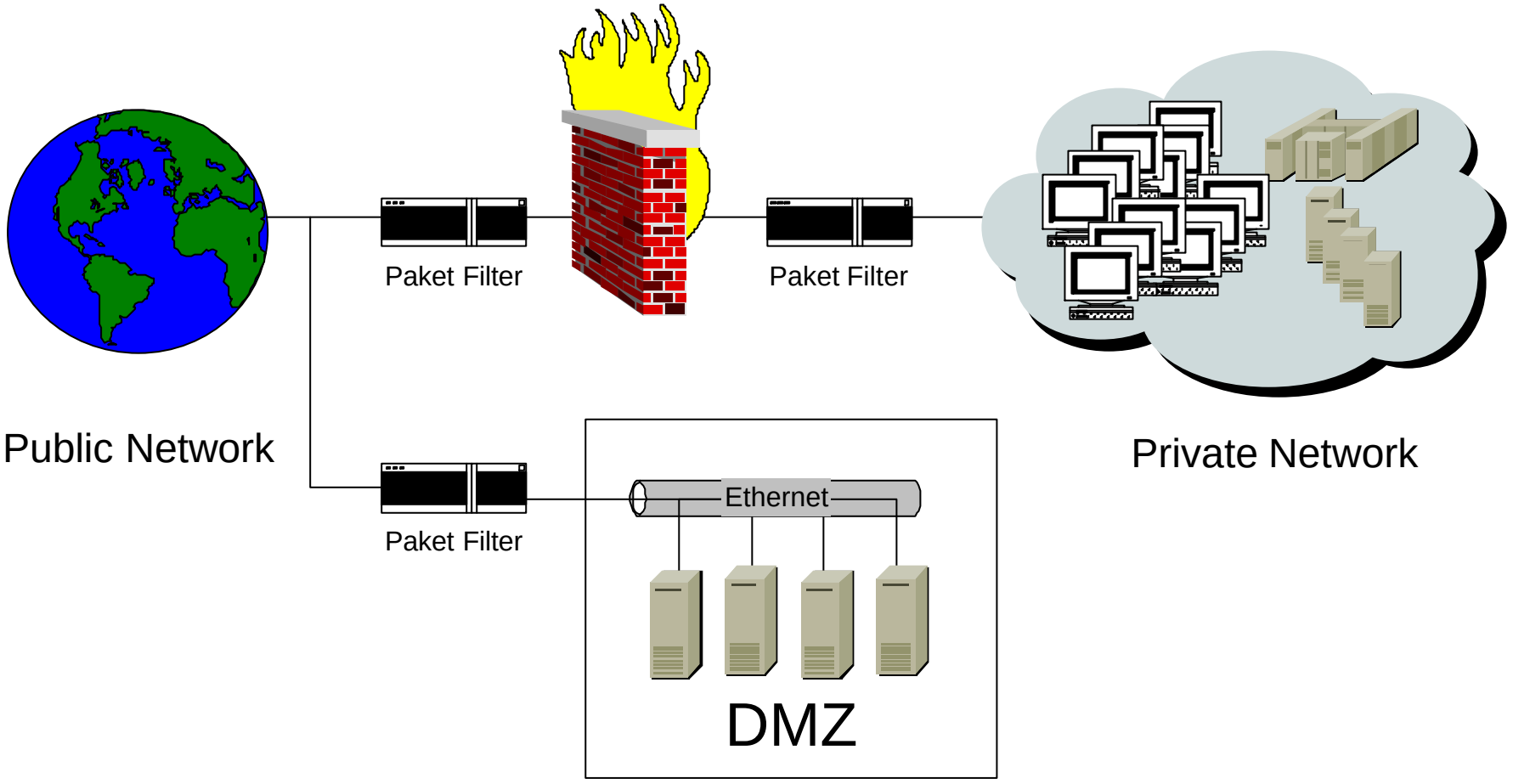


# Firewall Typ 4 – FW + PF



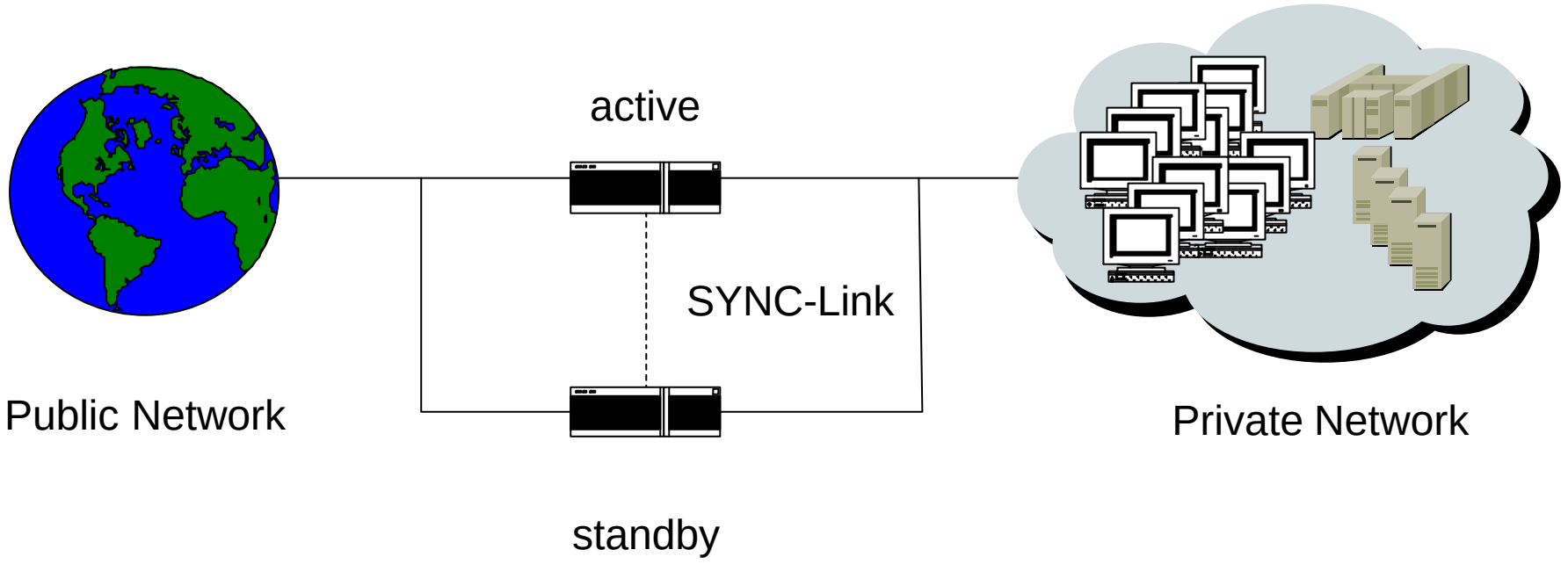
COMPAQ

# Firewall Typ 5 – Kryptokom (Utimaco)



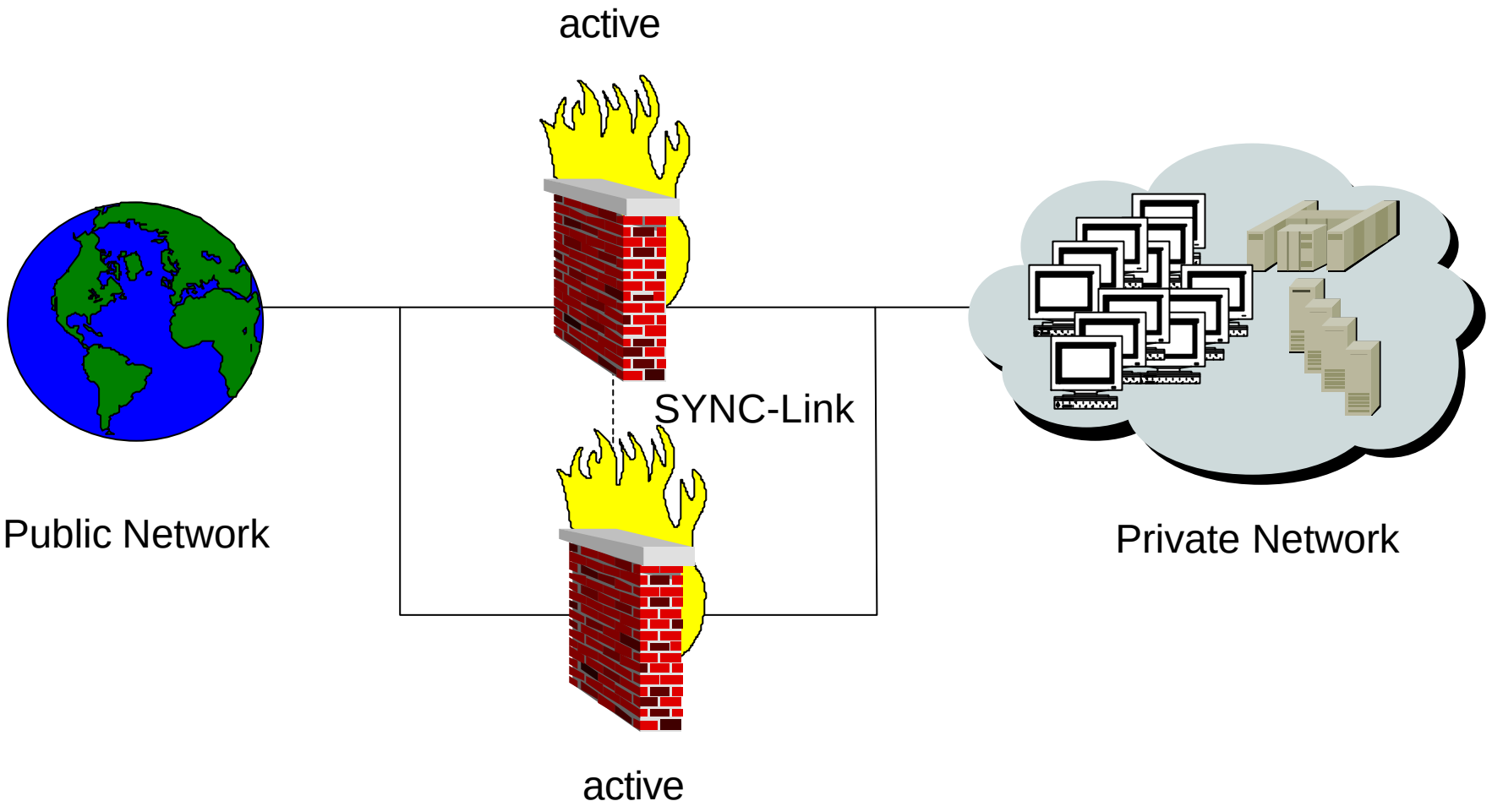
COMPAQ

# Firewall Redundanz – Einfach (Appliance)



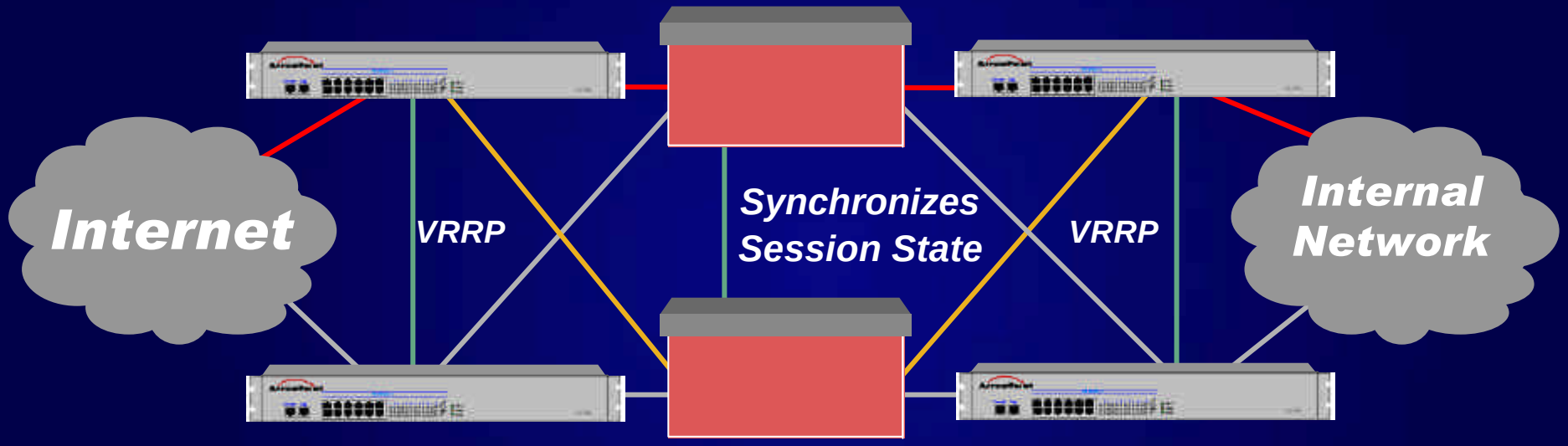
COMPAQ

# Firewall Redundanz – Software



COMPAQ

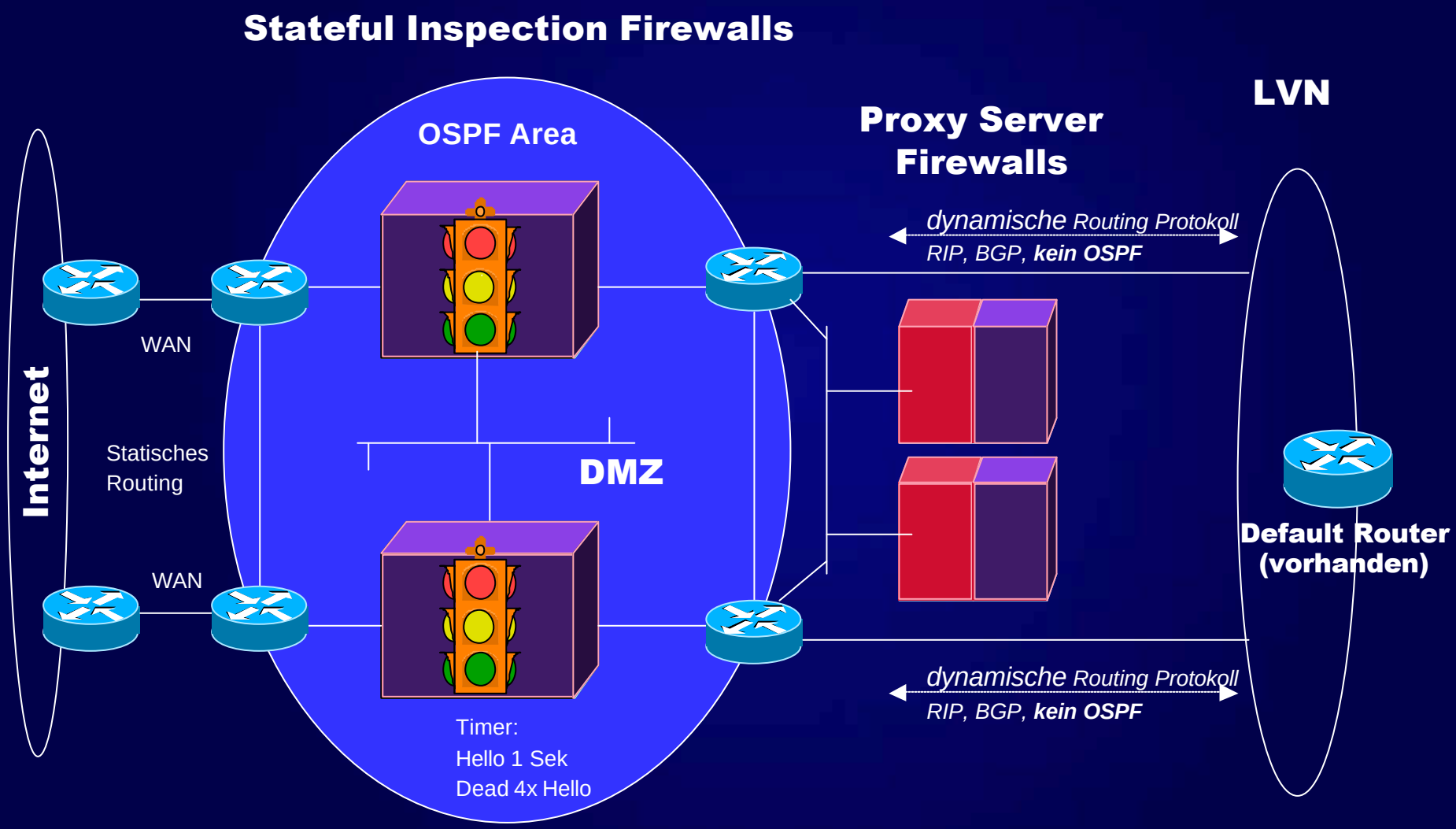
# High Performance Firewall + Load Balancing




Active paths
Standby paths

COMPAQ

# Redundanz / Lastteilung

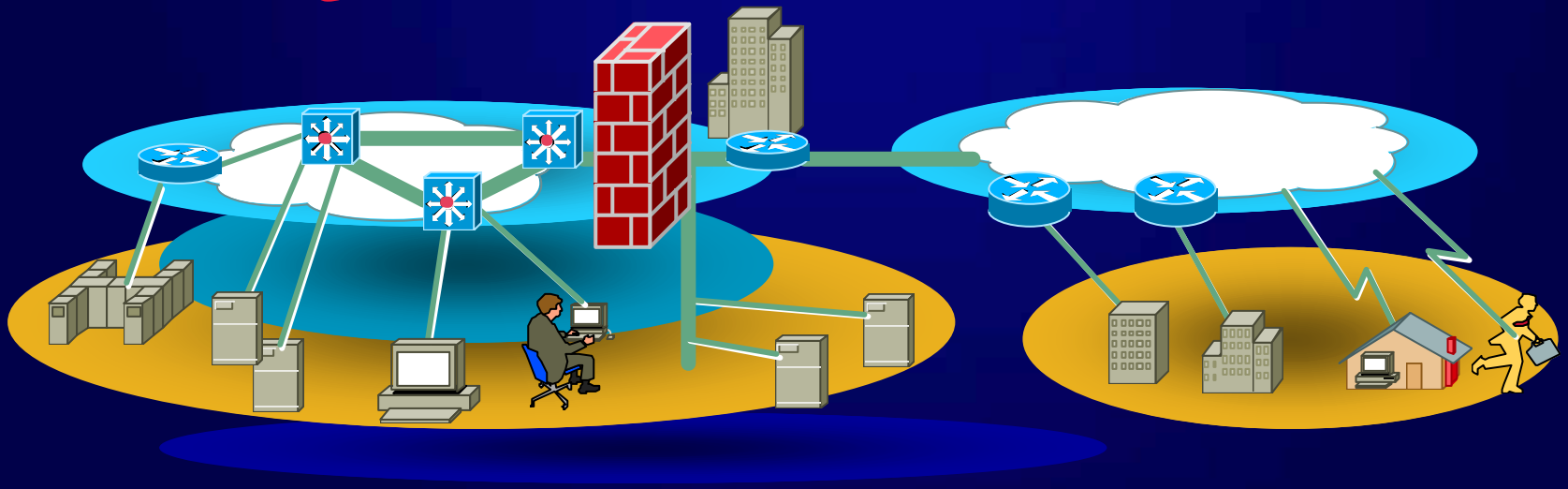


COMPAQ

# Sicherheitsverständnis ...

Sicherheit = Firewall

*... ist nicht genug !!!*



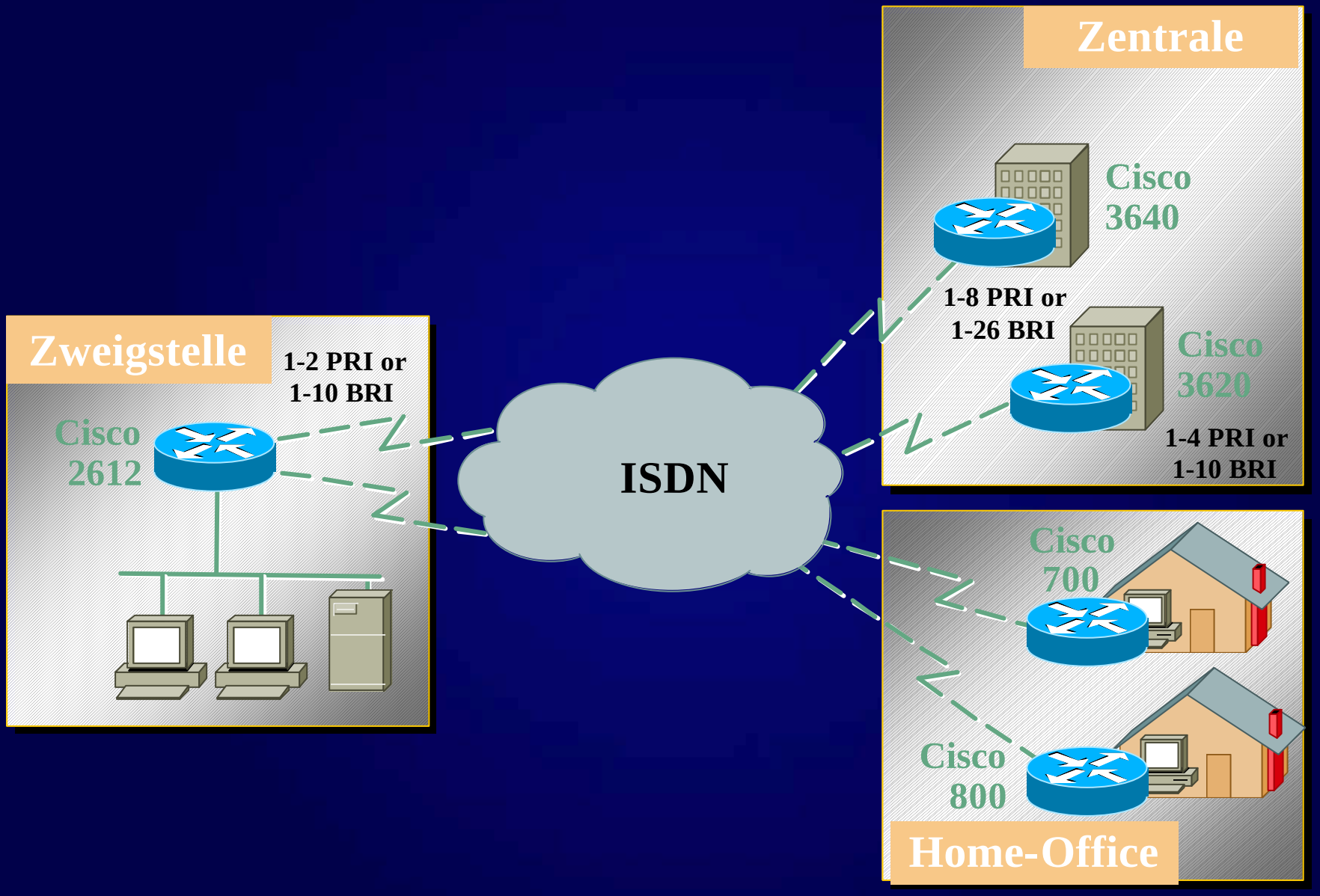
COMPAQ
Inspiration Technology

Compaq Global Services

# Access / VPN

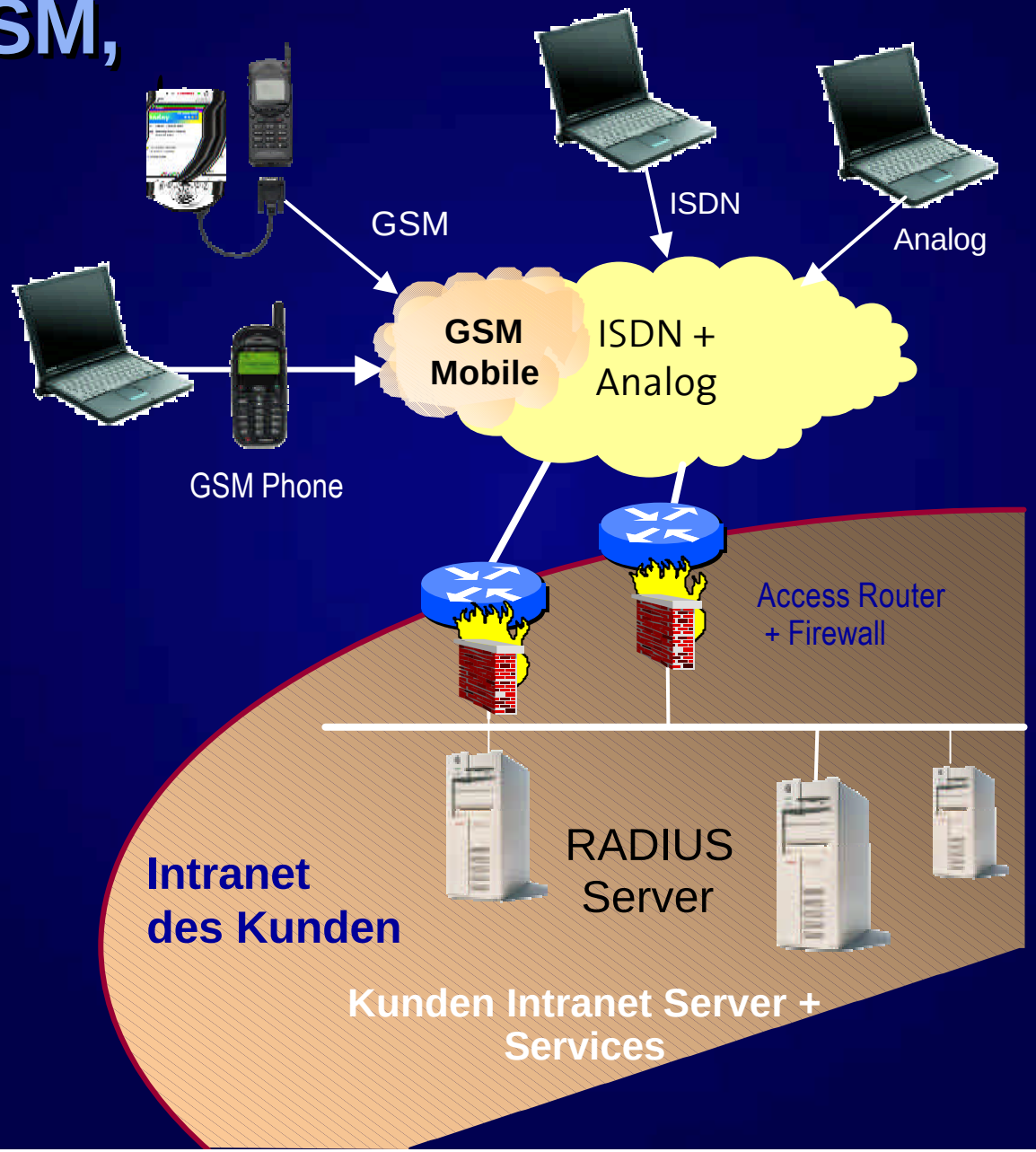
- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- **Access / VPN**
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

# ISDN Dial-In Konzentration



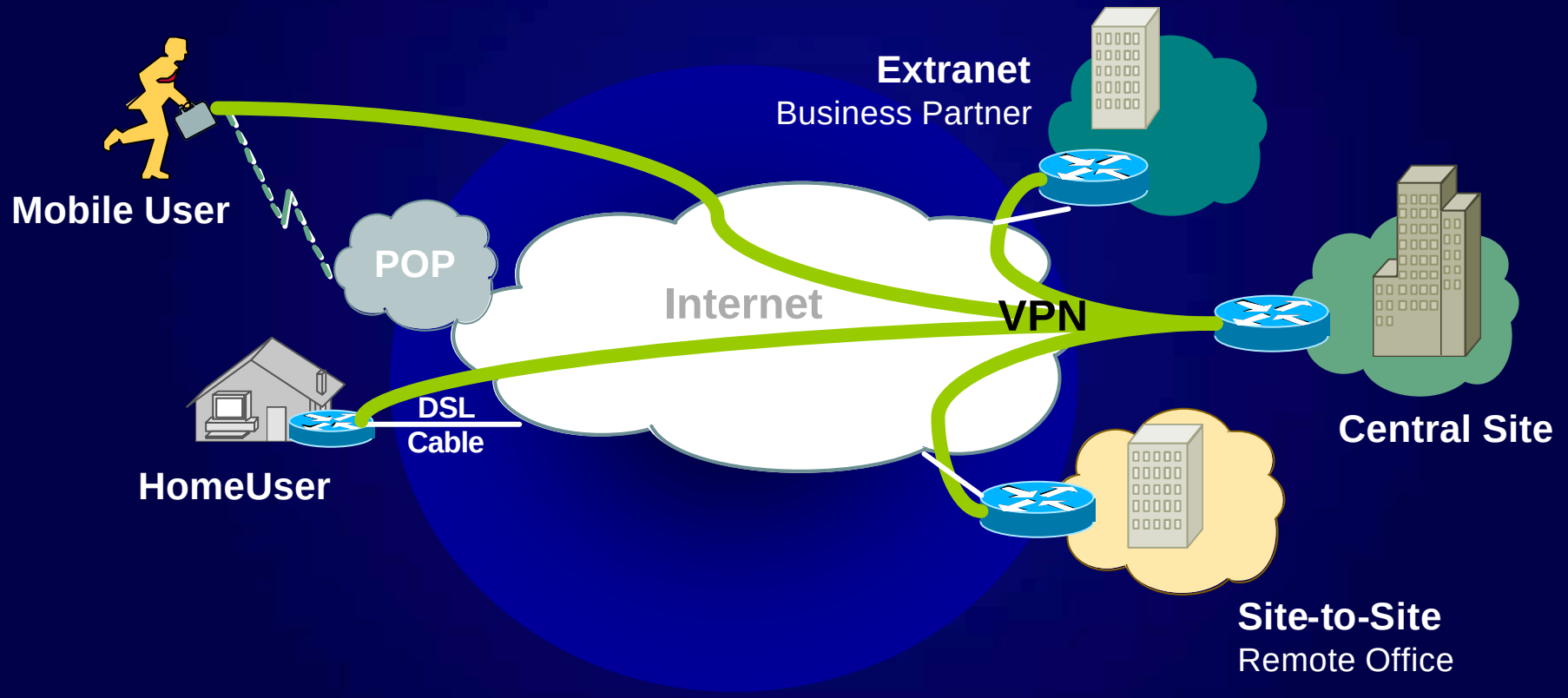
COMPAQ

# ISDN, GSM, Analog Access



COMPAQ

# VPN

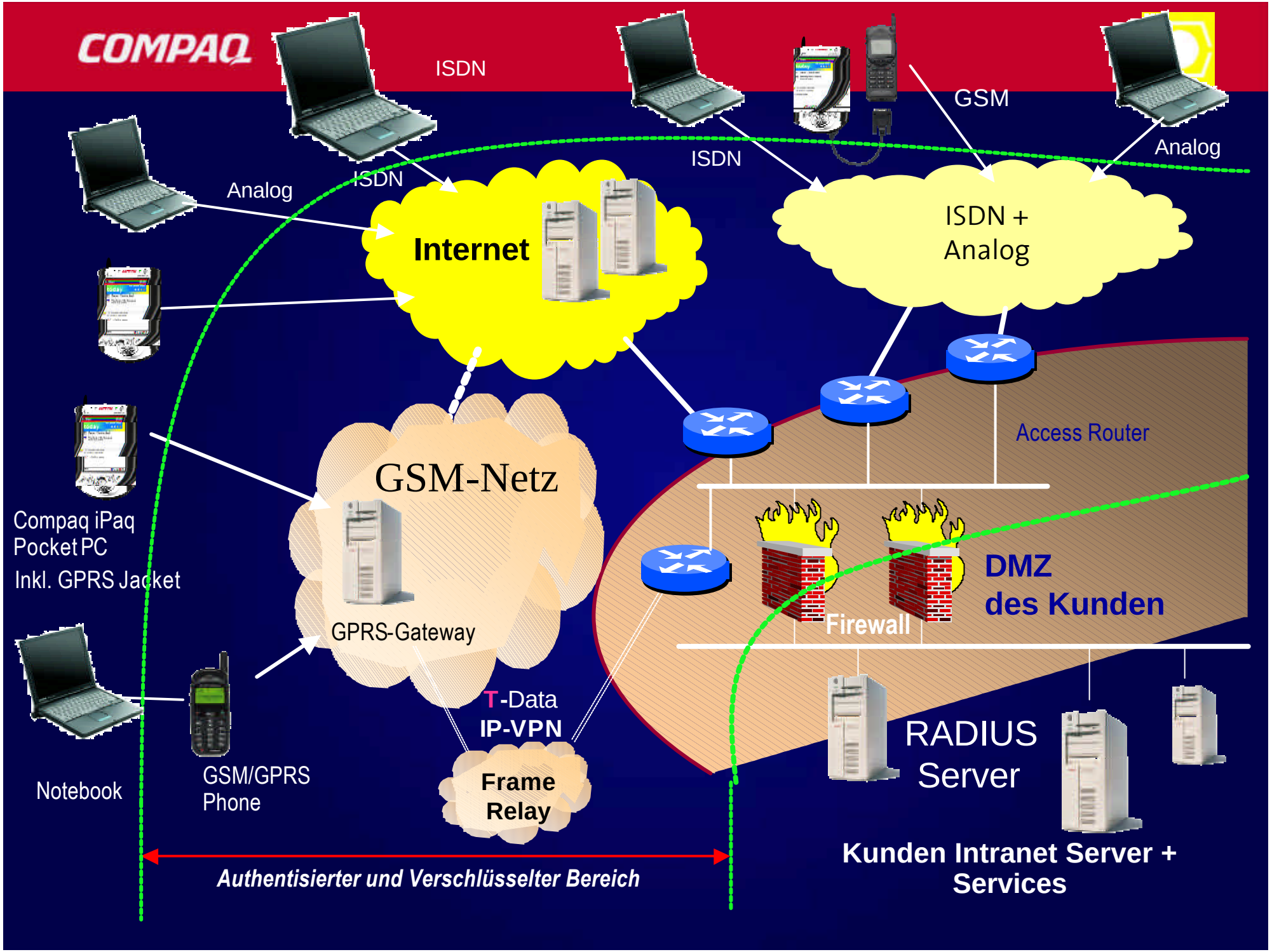

Extranet
Business Partner
Mobile User
POP
Internet
VPN
Central Site
DSL
Cable
HomeUser
Site-to-Site
Remote Office

COMPAQ

Und nun....

alles zusammen:

ISDN, Analog, GSM, GPRS, Wireless LAN und VPN

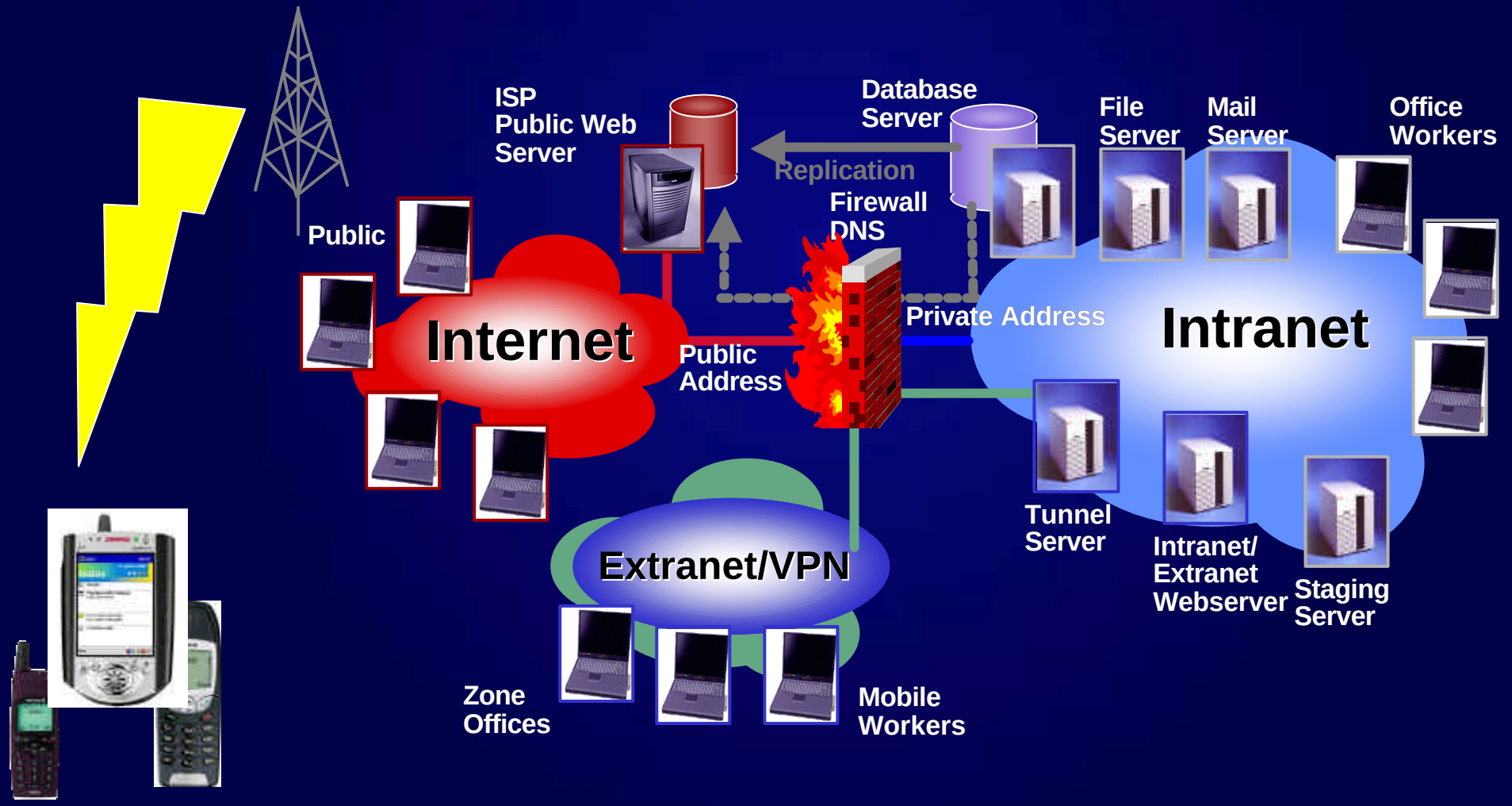

COMPAQ
ISDN
ISDN
ISDN
GSM
Analog
Analog
Internet
ISDN +
Analog
Access Router
GSM-Netz
GPRS-Gateway
Compaq iPaq
Pocket PC
Inkl. GPRS Jacket
Notebook
GSM/GPRS
Phone
T-Data
IP-VPN
Frame
Relay
Firewall
DMZ
des Kunden
RADIUS
Server
Kunden Intranet Server +
Services
Authentisierter und Verschlüsselter Bereich

COMPAQ

# VPN Überblick

COMPAQ

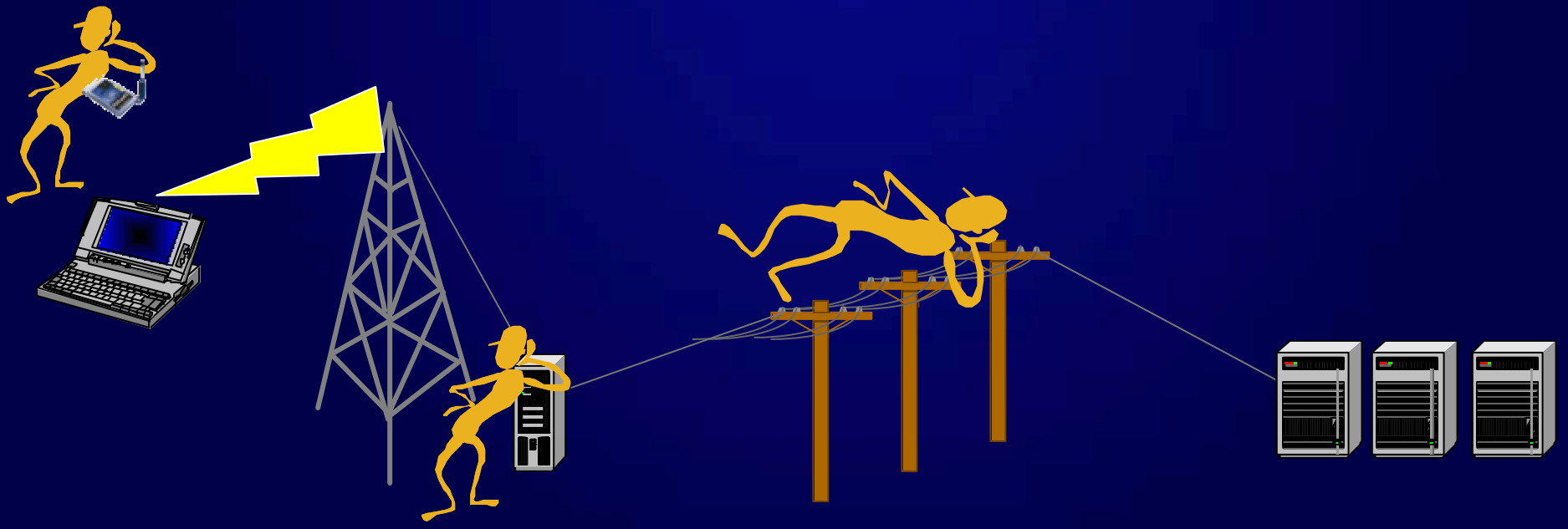
# What does the typical system look like?



COMPAQ

# Virtual Private Networks

- Use encryption to secure data across an untrusted network
- Provides confidentiality and integrity
- Extend our private network to mobile users



COMPAQ

# Cisco Site-to-Site VPNs

**Access CPE - Remote Site**
Cisco VPN-Optimized Routers -
800, 1700, 2600, 3600, 7100
Cisco Broadband Access Platforms -
1400 Cable Modem, uBR DSL Modem

**Enterprise - Central Site**
Cisco VPN Routers - 7x00: Routing + VPN
Cisco Secure PIX Firewall: Firewalling


- **Breiteste VPN Implementation**
- **Anforderungsspezifische Skalierbarkeit, Routing Protokolle, Multicast, Multiprotokoll**
- **Vielfältigste VPN Funktionalität in der Cisco IOS Software**
- **QoS Funktionalitäten**

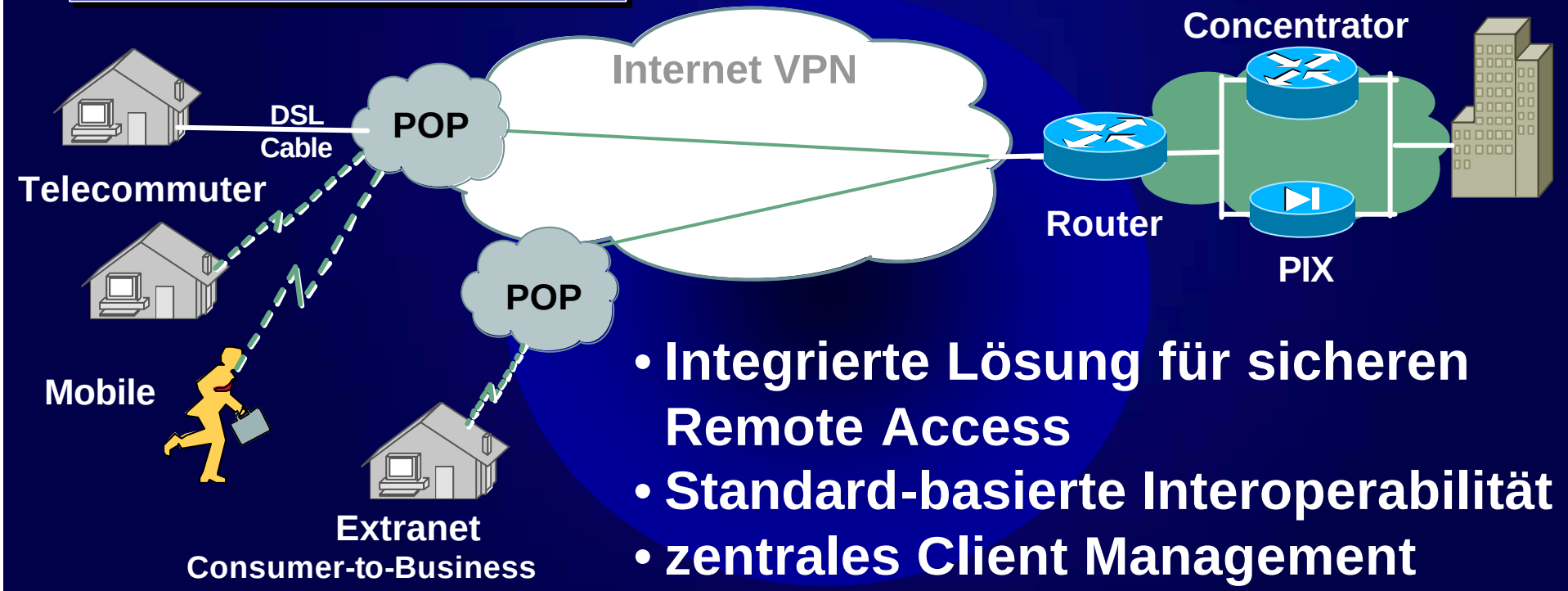
COMPAQ

# Remote Access VPNs: Cisco VPN 3000 Concentrator

**Remote Access Client**
Cisco VPN Clients

Microsoft Win 2000 (IPsec, PPTP)
Microsoft Win 9x/NT (PPTP)

**Enterprise - Central Site**
WAN Router - 7x00: Routing
Cisco Secure PIX Firewall: Firewalling
Cisco VPN Concentrator: VPN Tunnel Termination



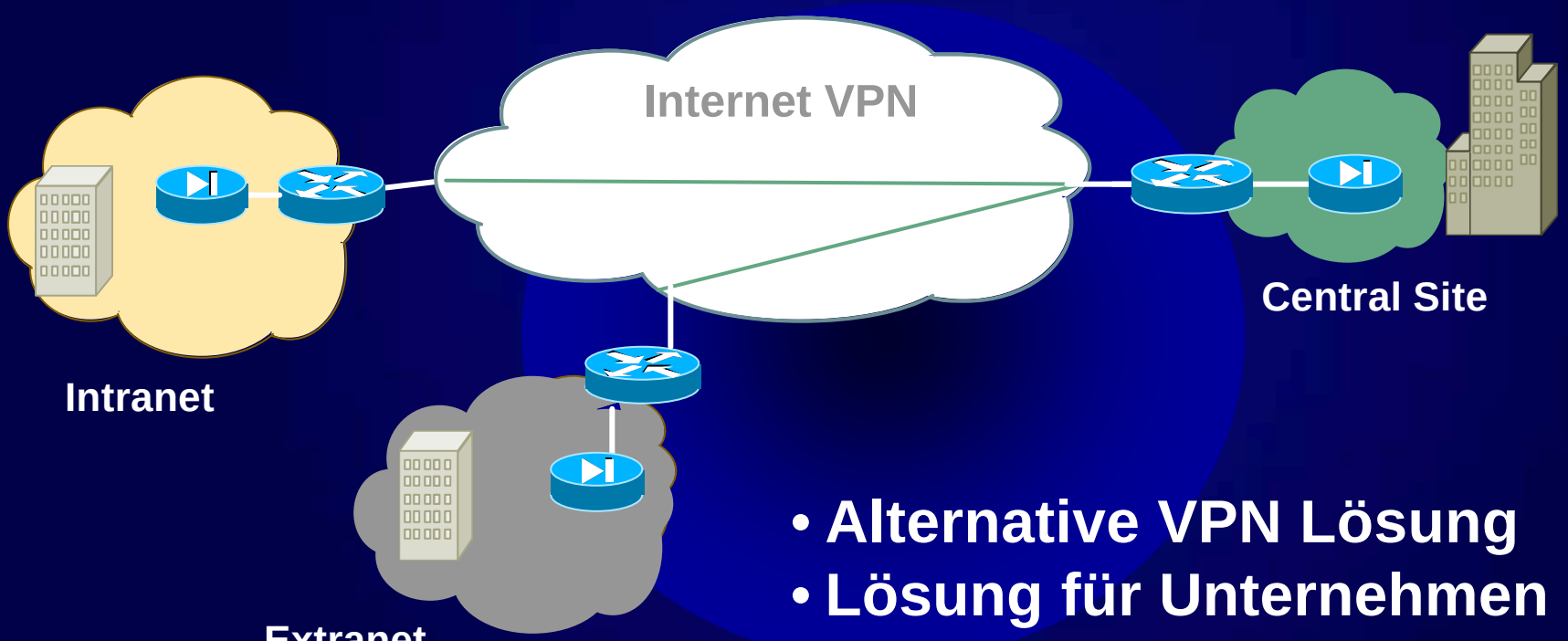

- Integrierte Lösung für sicheren Remote Access
- Standard-basierte Interoperabilität
- zentrales Client Management (push)

COMPAQ

# Cisco Firewall-Based VPN

**Access CPE - Remote Site**
Cisco Secure PIX Firewall 506/515

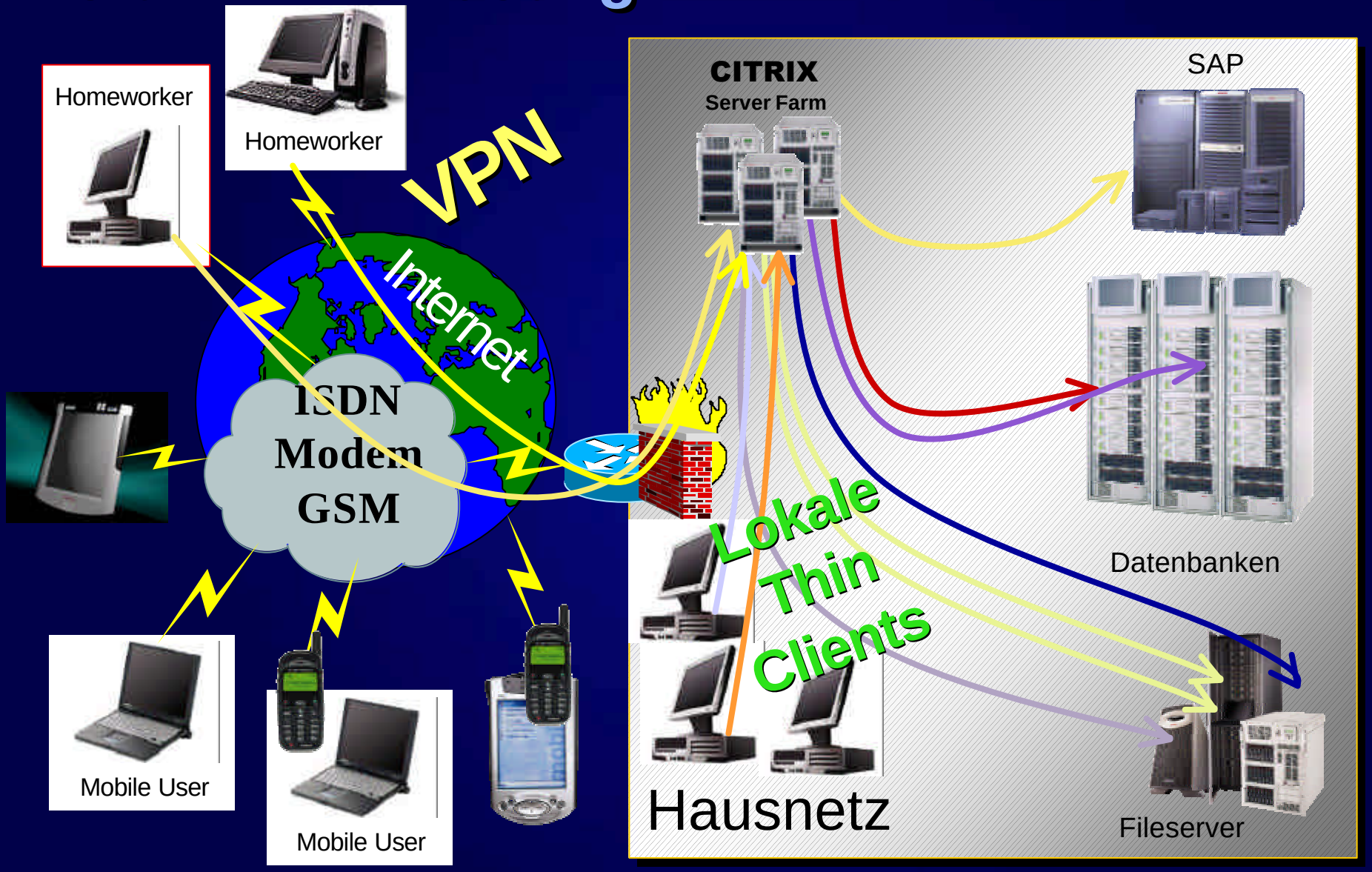
**Enterprise - Central Site**
Cisco VPN Routers - 7x00: Routing
Cisco Secure PIX Firewall 520: Firewalling + VPN




- Alternative VPN Lösung
- Lösung für Unternehmen mit Firewalls als Basis für VPNs

COMPAQ

# Citrix VPN Lösung



COMPAQ
Inspiration Technology

Compaq Global Services

# Intrusion Detection

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- **Intrusion Detection**
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

COMPAQ

# IDS - Baustein zur Verteidigung

- Hostsensoren
- Netzsensoren
- Zentraler Log und Management Server
- Alarming
- Korrelation


COMPAQ

# Was ist Intrusion Detection ??

Erkennung von

- Angriffsversuchen
- Einbrüchen
- Schadensumfang
- Viren
- Zielgenaue Analyse

COMPAQ

# Wie Hacker z. B. angreifen

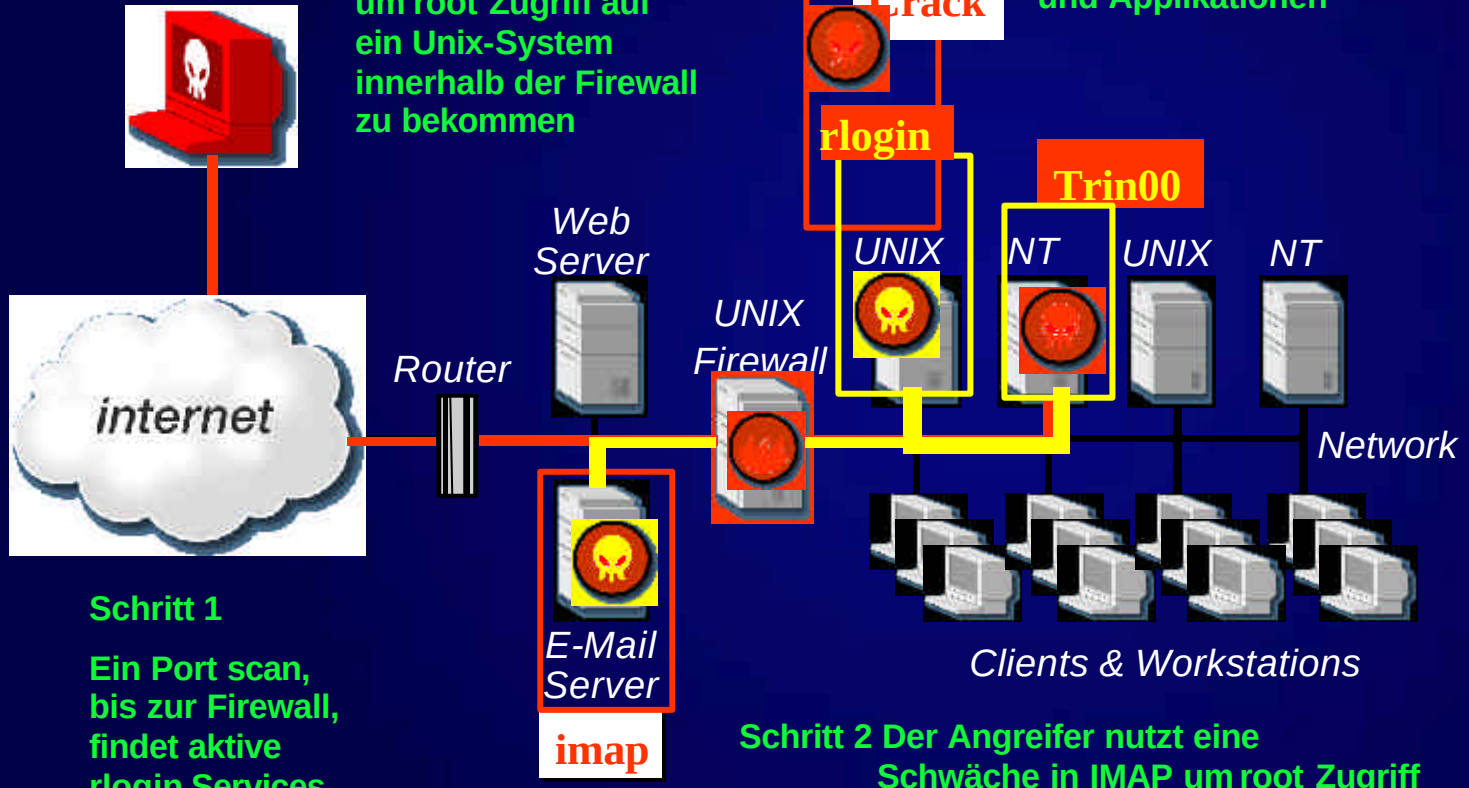
**Schritt 3**

**Der Angreifer nutzt Vertrauensstellungen um root Zugriff auf ein Unix-System innerhalb der Firewall zu bekommen**

**Schritt 4 .** **Der Angreifer crackt Passwordfiles und hat nun ROOT/ADMINISTRATOR Rechte auf verschiedenen Systemen und Applikationen**

**Schritt 5**

**Der Angreifer benutzt das NT-Admin Password um den PC des Vorsitzenden in einen Trin00 Zombie umzuwandeln**

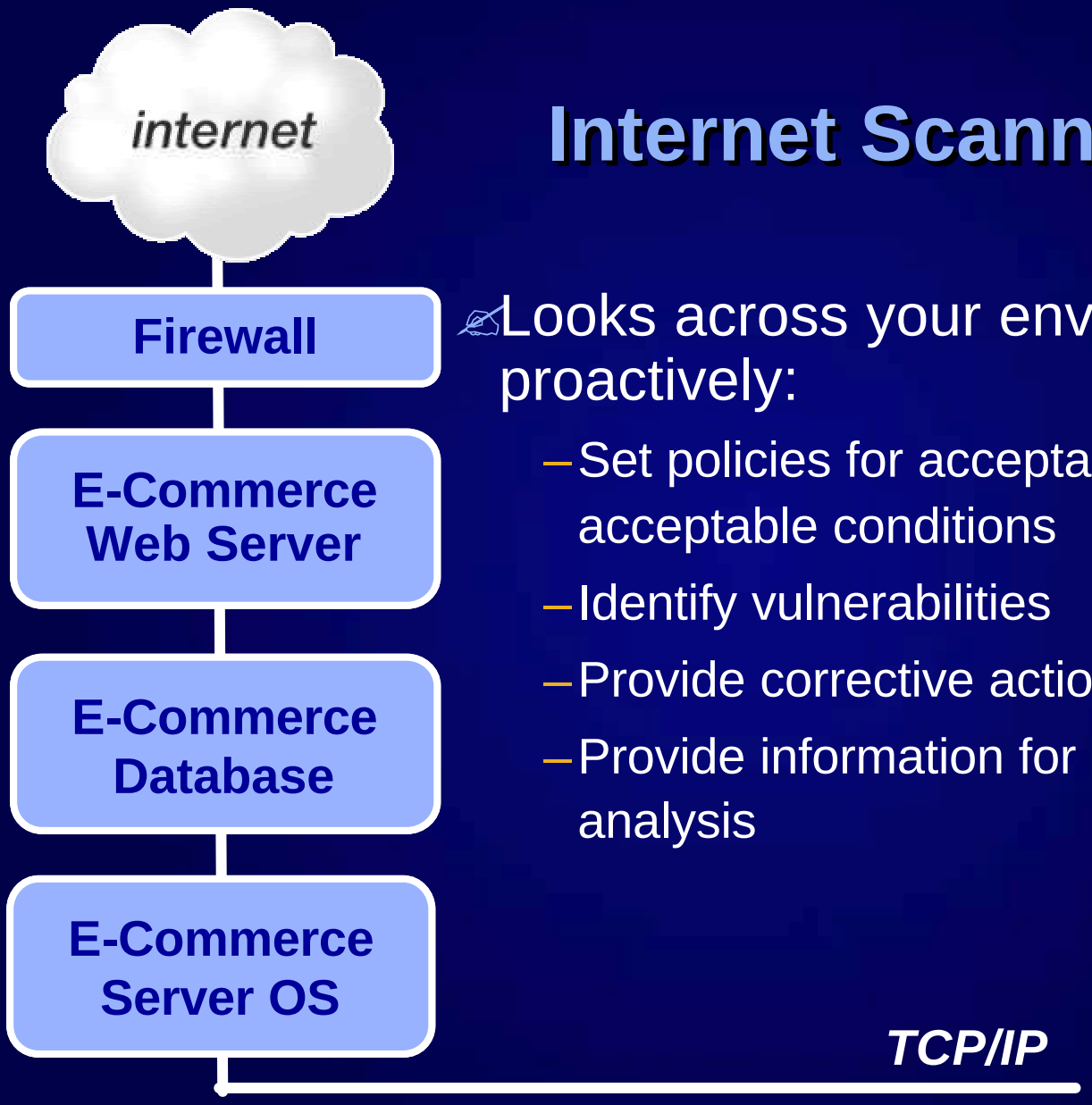



**Schritt 1**

**Ein Port scan, bis zur Firewall, findet aktive rlogin Services auf verschiedenen Systemen**

**Schritt 2 Der Angreifer nutzt eine Schwäche in IMAP um root Zugriff auf den E-Mail Server auserhalb der Firewall zu bekommen**

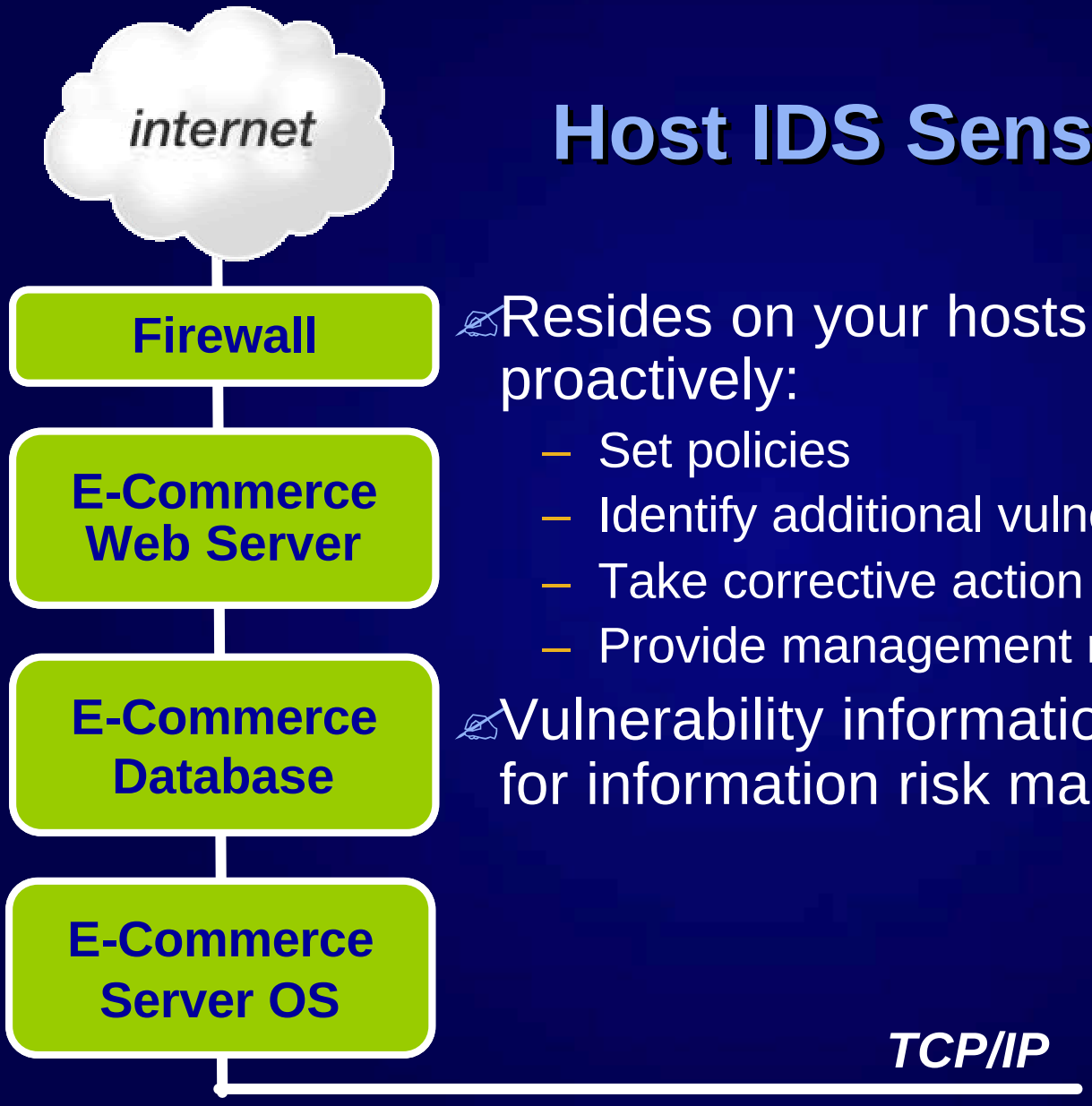
COMPAQ




# Internet Scanner

- Looks across your environment to proactively:
  - Set policies for acceptable and non acceptable conditions
  - Identify vulnerabilities
  - Provide corrective action reports
  - Provide information for Info Risk Mgt analysis

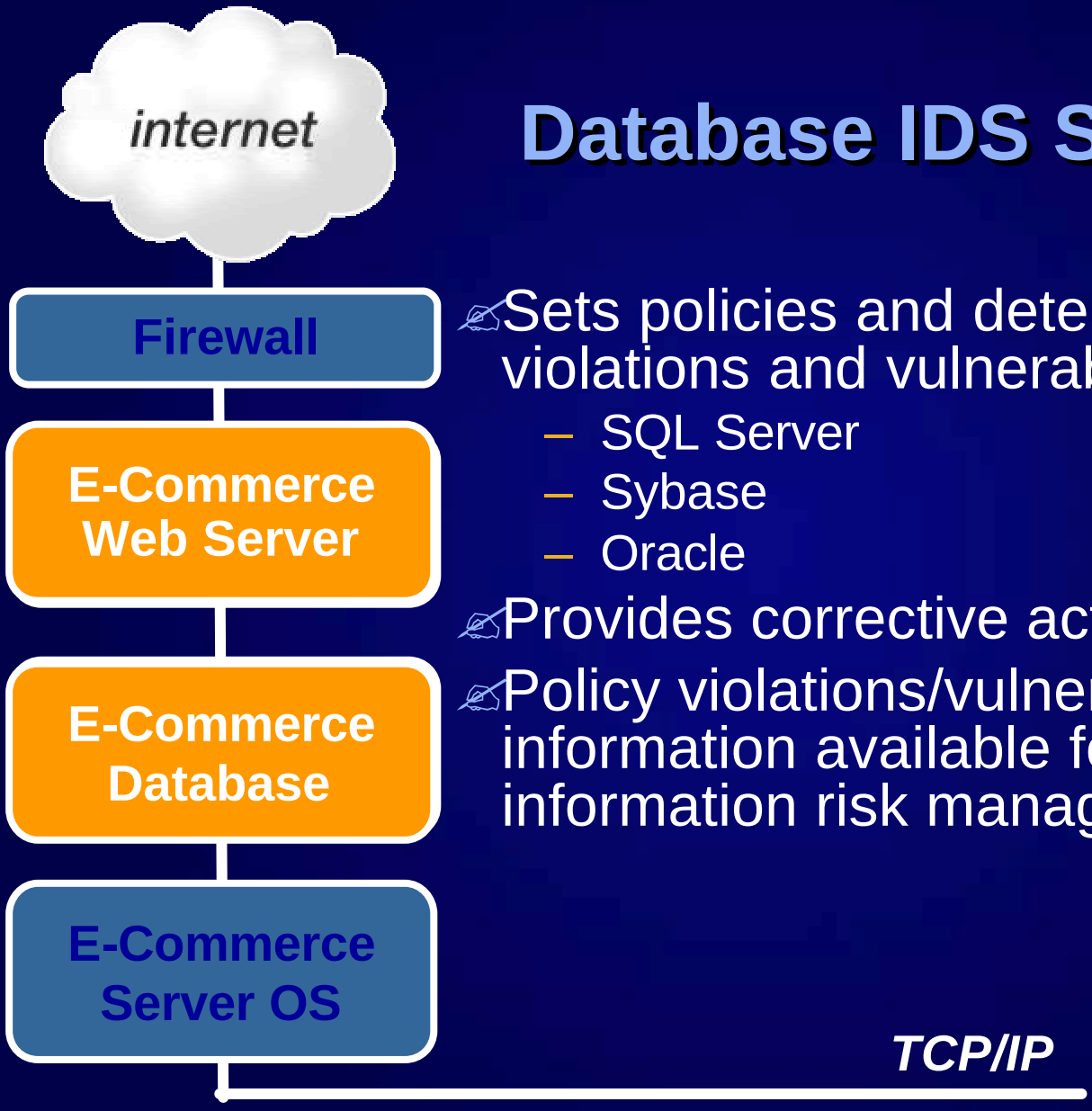
COMPAQ




# Host IDS Sensor

- Resides on your hosts to proactively:
  - Set policies
  - Identify additional vulnerabilities
  - Take corrective action
  - Provide management reports
- Vulnerability information available for information risk management

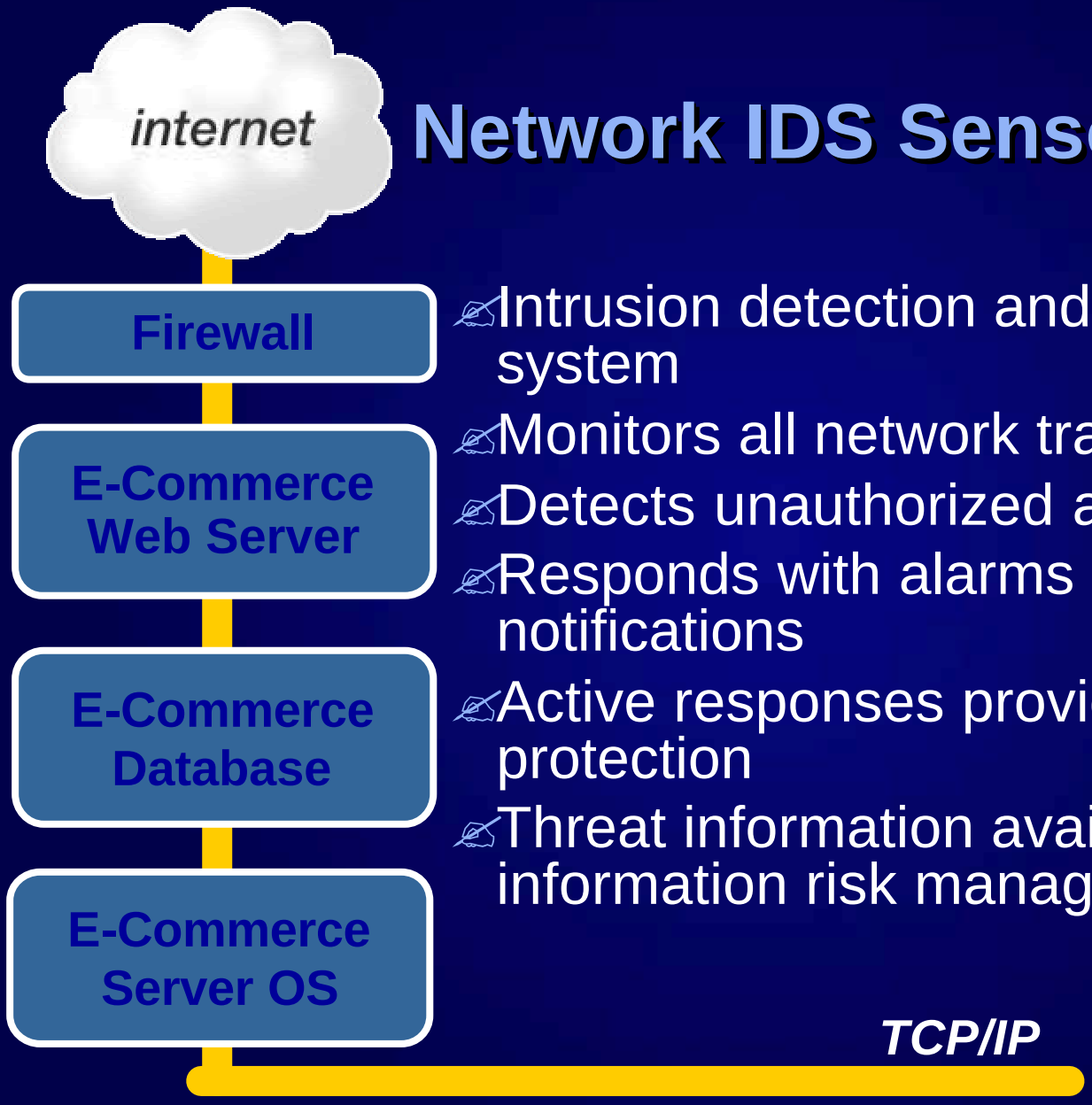
COMPAQ




# Database IDS Sensor

- Sets policies and determines violations and vulnerabilities
  - SQL Server
  - Sybase
  - Oracle
- Provides corrective action reports
- Policy violations/vulnerability information available for information risk management

COMPAQ

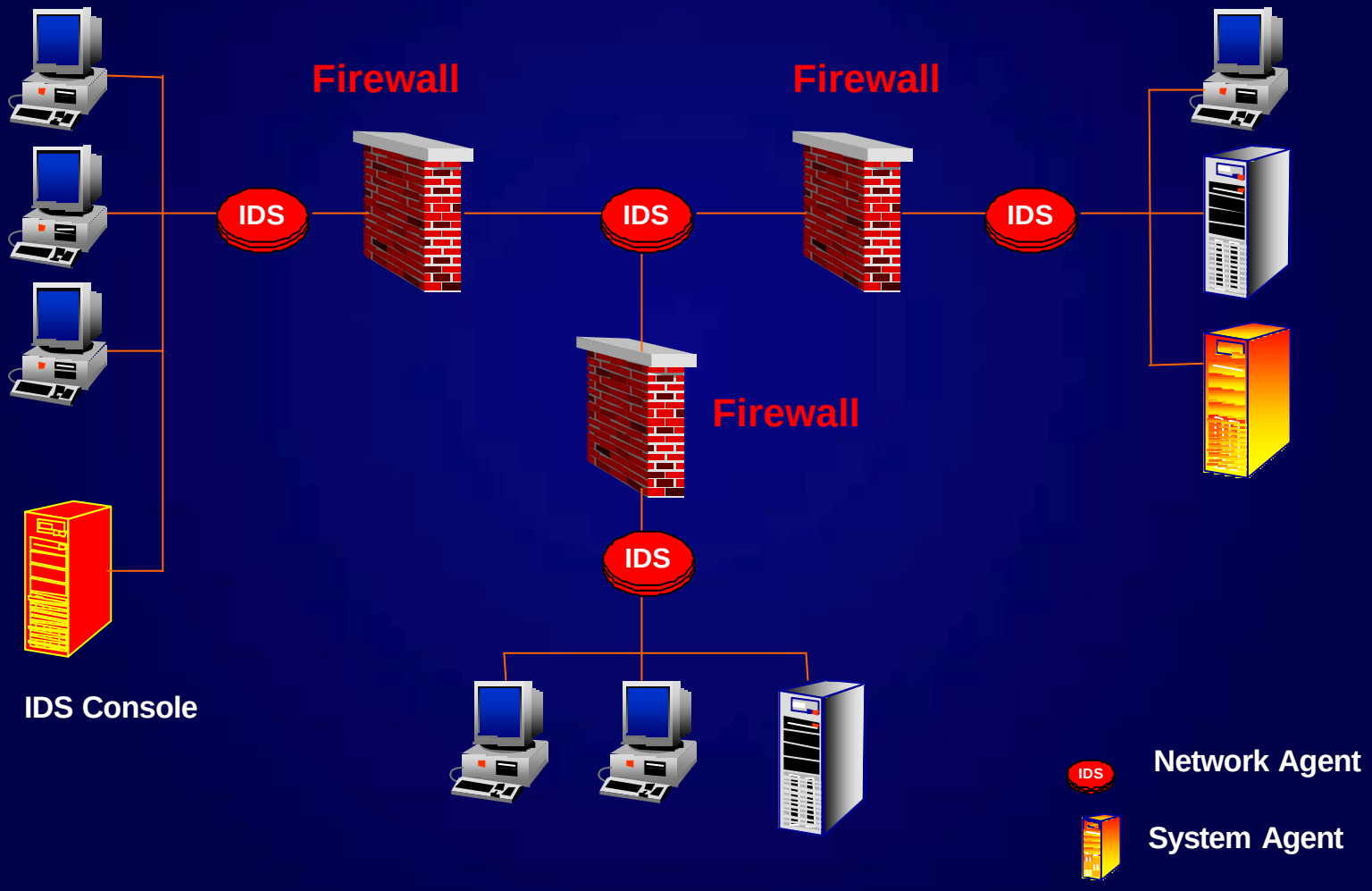



# Network IDS Sensor

- Intrusion detection and response system
- Monitors all network traffic
- Detects unauthorized activity
- Responds with alarms and email notifications
- Active responses provide ultimate protection
- Threat information available for information risk management

COMPAQ

# Übersicht: Intrusion Detection



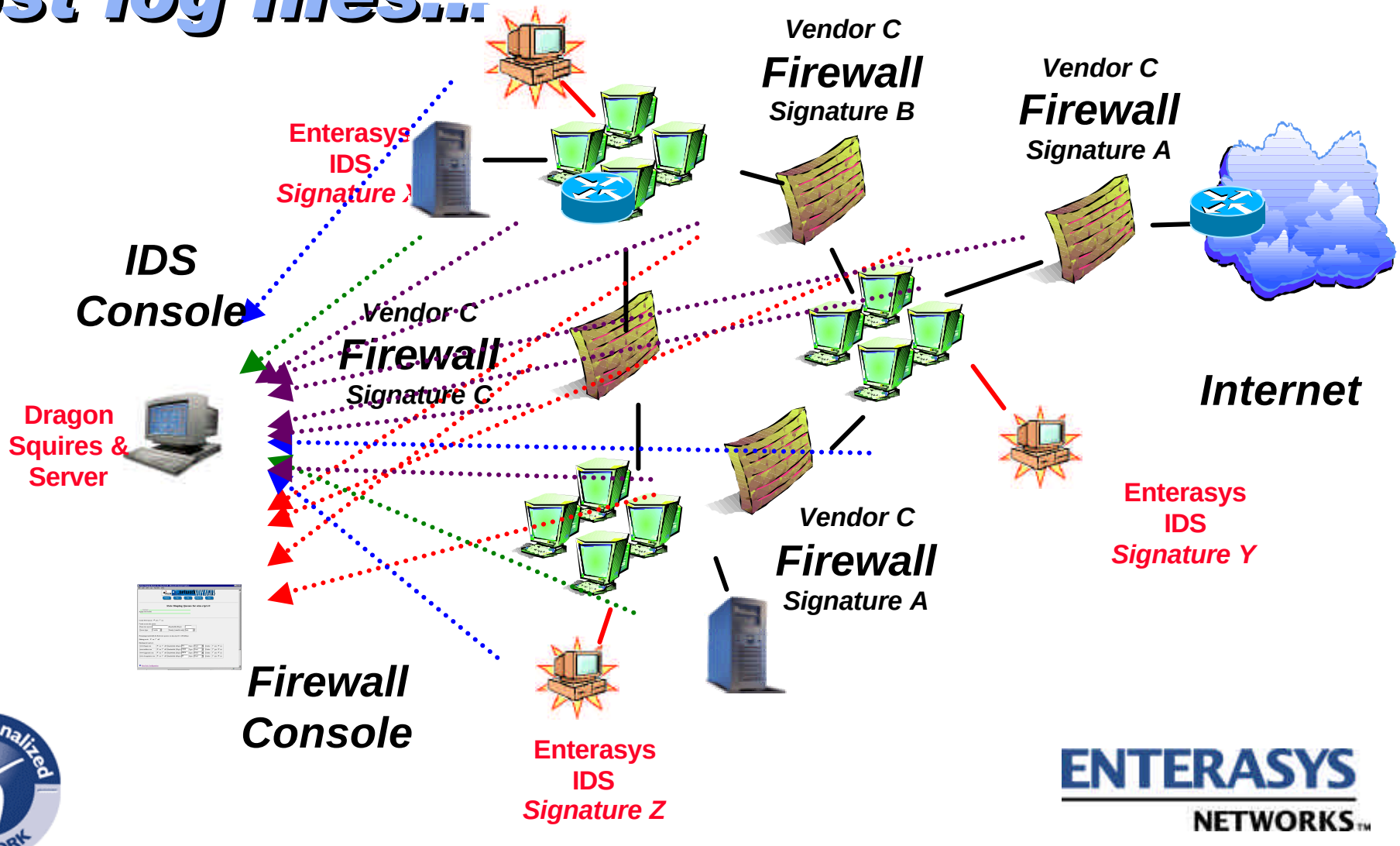
COMPAQ

# IDS Management

- Zentrales Management für alle IDS Sensoren
- Zentrale Auswertung von Log-Files (auch 3rd Party)
- Alarmfunktionen (Email, Pager, SNMP usw.)
- Angriffsreporting
- Automatischer Soft- und Regelupdate Download vom Hersteller
- Automatische Soft- und Regelupdates für alle IDS Sensoren

COMPAQ

# Intrusion Detection Firewall, Router, Host log files…




User Personalized Network

ENTERASYS NETWORKS™

COMPAQ
Inspiration Technology

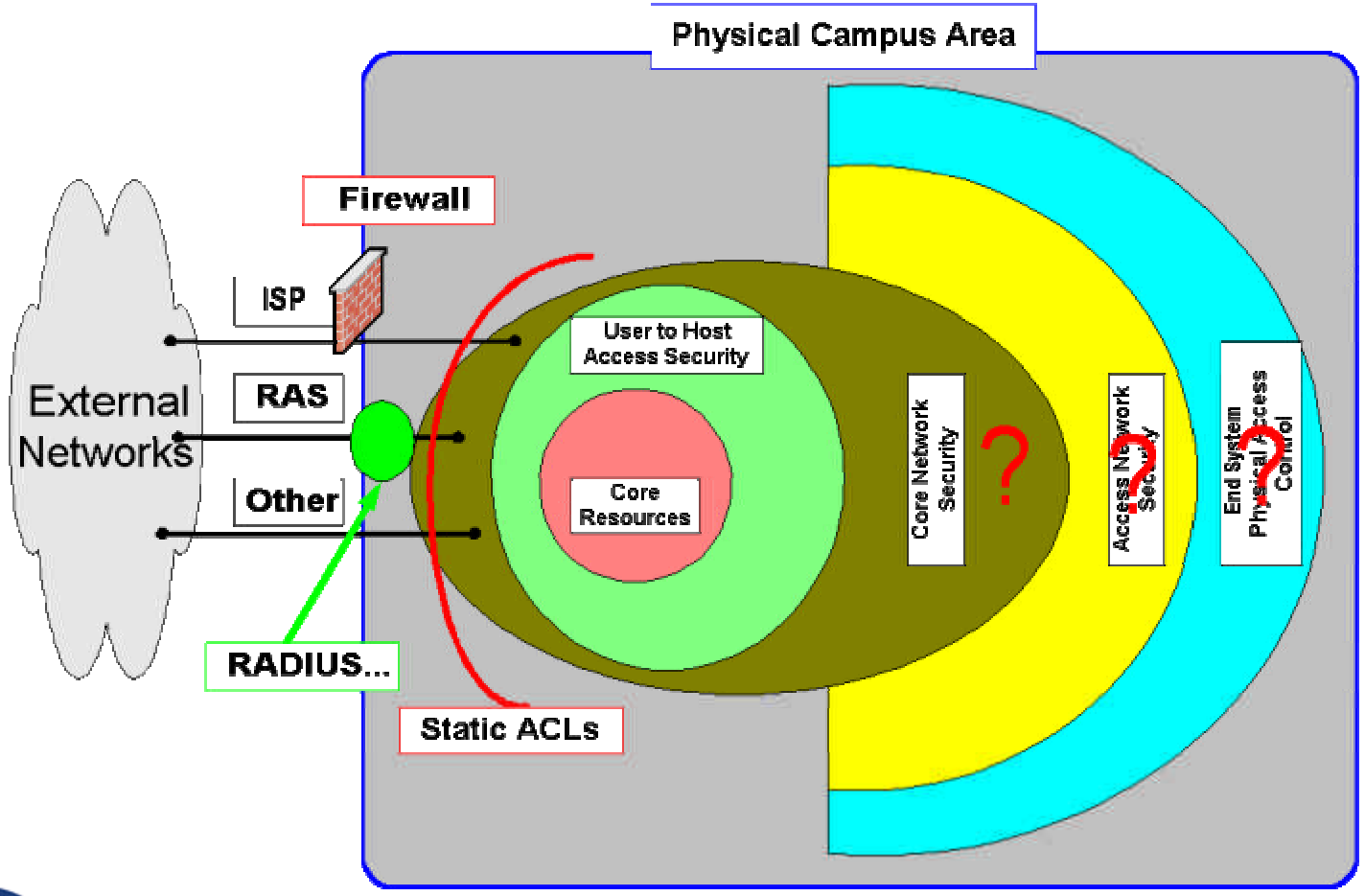
Compaq Global Services

# Security Standard 802.1X / UPN

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- Intrusion Detection
- **Security Standard 802.1X**
- Desktop / Device Security
- Security Gesamtbild

COMPAQ

# Gängiges Sicherheits Modell

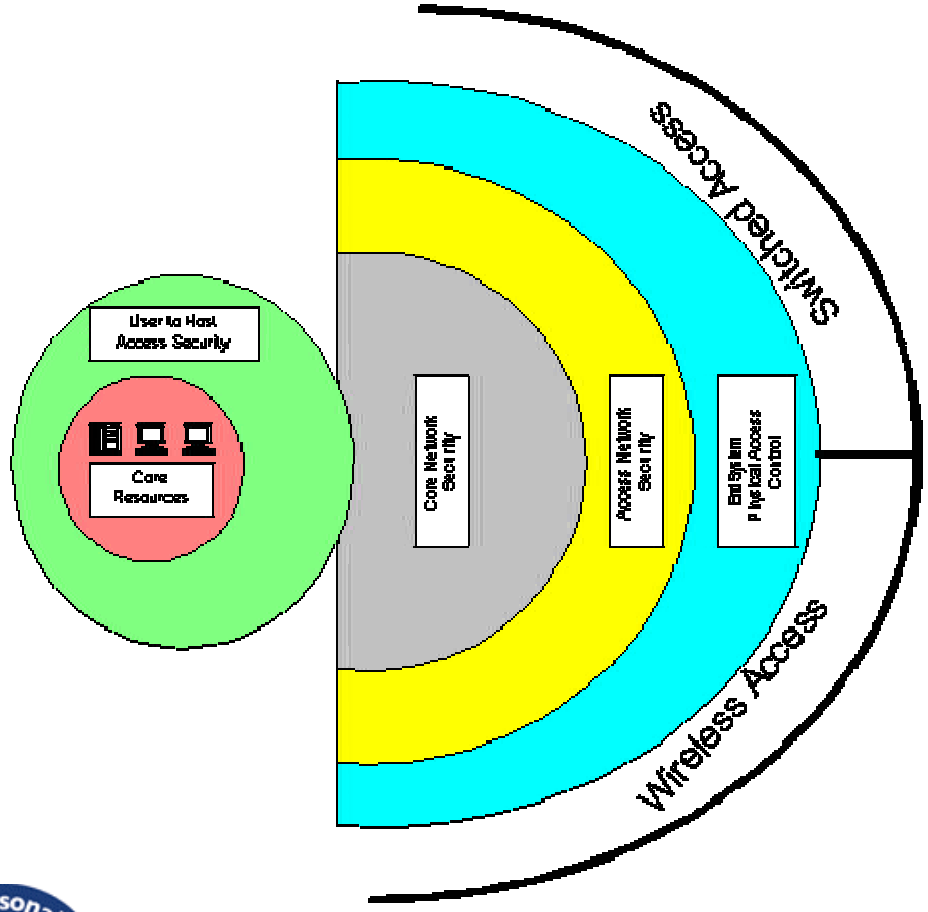



User Personalized NETWORK

ENTERASYS NETWORKS™

COMPAQ

# Verfügbare Edge Sicherheits Technologien




- Physical Port Security
- MAC VLANs
- User Authentication 802.1x
- VPN Overlay

- WEP/802.11
- Network Name Authenticaiton
- User Authentication 802.1x
- Per User Key Encryption
- VPN Overlay

User Personalized NETWORK

ENTERASYS NETWORKS™

COMPAQ

# User Personalized Networking - Szenarien

| | |
|---|---|
| Gäste im Netz | **"Ich möchte es ermöglichen, dass Besucher meines Unternehmens mein Netzwerk nutzen, ohne das sie auf unsere Ressourcen (Inhalte) zugreifen können"** |
| SAP Implementation | **"Ich muss in der Lage sein, den Mitarbeitern gezielt die für Sie jeweils businessrelevanten Applikationen jederzeit bereitzustellen.** |
| Veranstaltungsräume | **"Ich muss jede Woche das Netzwerk anpassen."** |
| Distributed Firewall | **"Ich bin nicht so besorgt wegen Attacken von Außen, sondern viel mehr über interne Nutzer, die bewusst oder unbewusst Schaden anrichten."** |
| Administration | **Schnelle Switche/Router, Policy und Authentifikation sind wichtig. Allerdings haben wir nur 3 Leute, wie sollen wir das Administrieren?"** |
| Konvergenz | **"Ich befürchte, es gibt ein enormes Risiko, wenn ich mit VoIP ein übliches Telefonnetz ersetzen will."** |

User Personalized NETWORK

ENTERASYS NETWORKS

COMPAQ

# Authentisierung

- **Ein UPN kennt die Person, die das Netzwerk nutzt**
- **Authentisierung existiert heutzutage nur in Remote Access Netzwerken**
- **2001 wurden einige Standards verabschiedet, um daraus einen universellen Dienst bereitzustellen**
  - IEEE 802.1X Authentication für Wired LANs, Wireless LANs und VPNs
  - Neue Sicherheitsdienste
    – Biometrics, Certificates….
  - Unterstützung der Operating Systeme – MS WindowsXP, WinNT, W2K, WIN 98, Linux, Unix

- **Einheitliche Identität unabhängig der Verbindungsvariante**
  - **VPN, LAN, WLAN…**

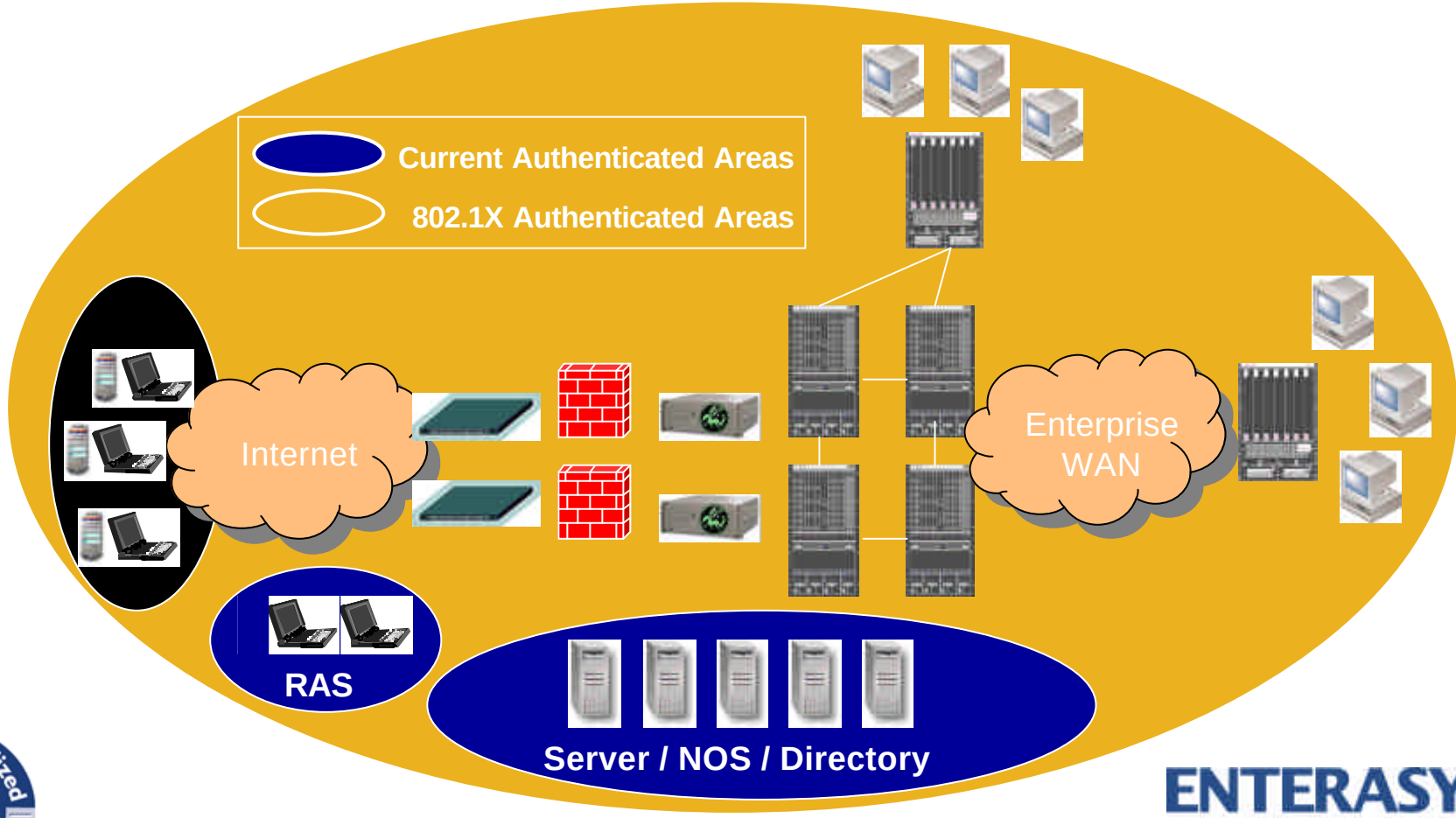
User Personalized NETWORK

ENTERASYS NETWORKS™

COMPAQ

# *Der Ruf nach Port-basierter Authentisierung…*

**Die IT-Security sollte bei jedem einzelnen Benutzer anfangen**




User Personalized NETWORK

ENTERASYS NETWORKS

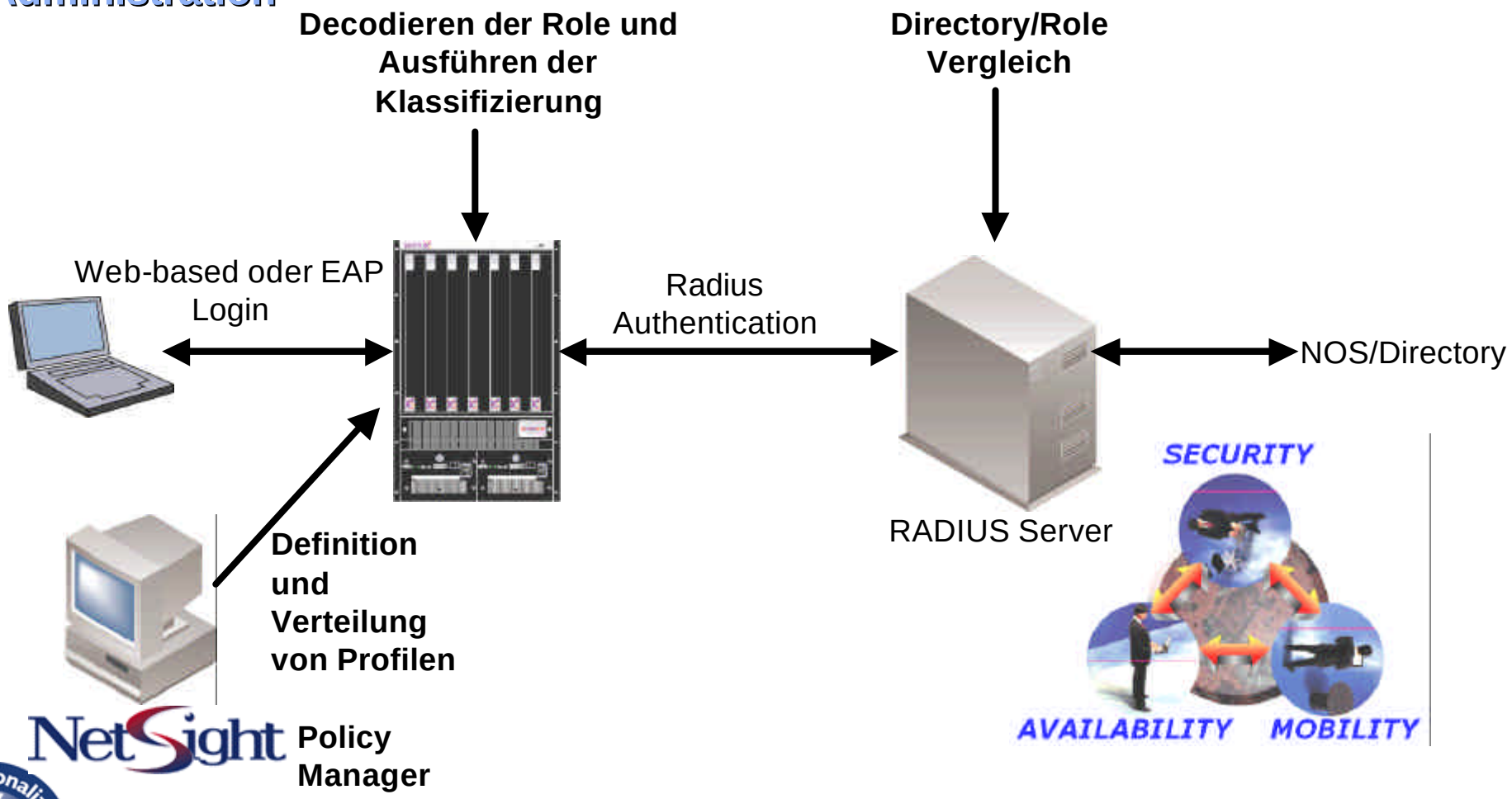
# IEEE 802.1X

- **Standard verabschiedet Juni 2001**
- **Port based Network Access Control**
- **Definiert**
  - Authentication Framework
  - Mechanismen zur Zugangskontrolle
  - Verschiedene Level zur Zugangskontrolle
  - Verhalten der Ports innnerhalb dieser Level (transmission, reception of frames)
  - Protokolle zur Kommunikation zwischen Authenticator und Authentication Server
- **Ermöglicht interoperable Benutzer-Identifikation, zentralisierte Authentisierung, Key Management**
  - Nutzt existierende Standards: EAP, RADIUS, MD5
  - Compatibel mit existierende Roaming Technologien, ermöglicht Nutzung in Hotel und öffentlichen Plätzen
- **Unterstützt wird Ethernet, Token Ring und IEEE 802.11(Wireless)**

COMPAQ

# UPN - User Personalized Network

## Kombination von Service-enabled Edge, Authentication und Role-based Administration




User Personalized NETWORK

ENTERASYS NETWORKS

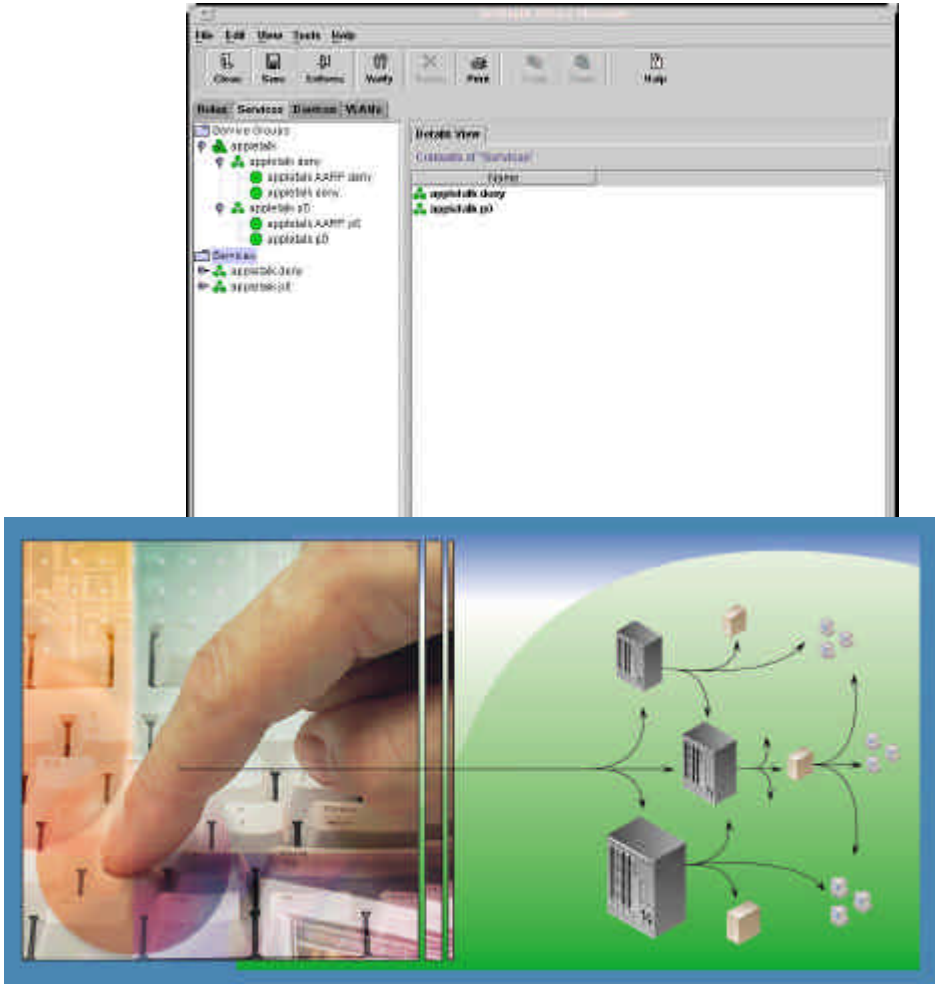
COMPAQ

# Rollenbezogene Administration

## NetSight™ Policy Manager

NetSight

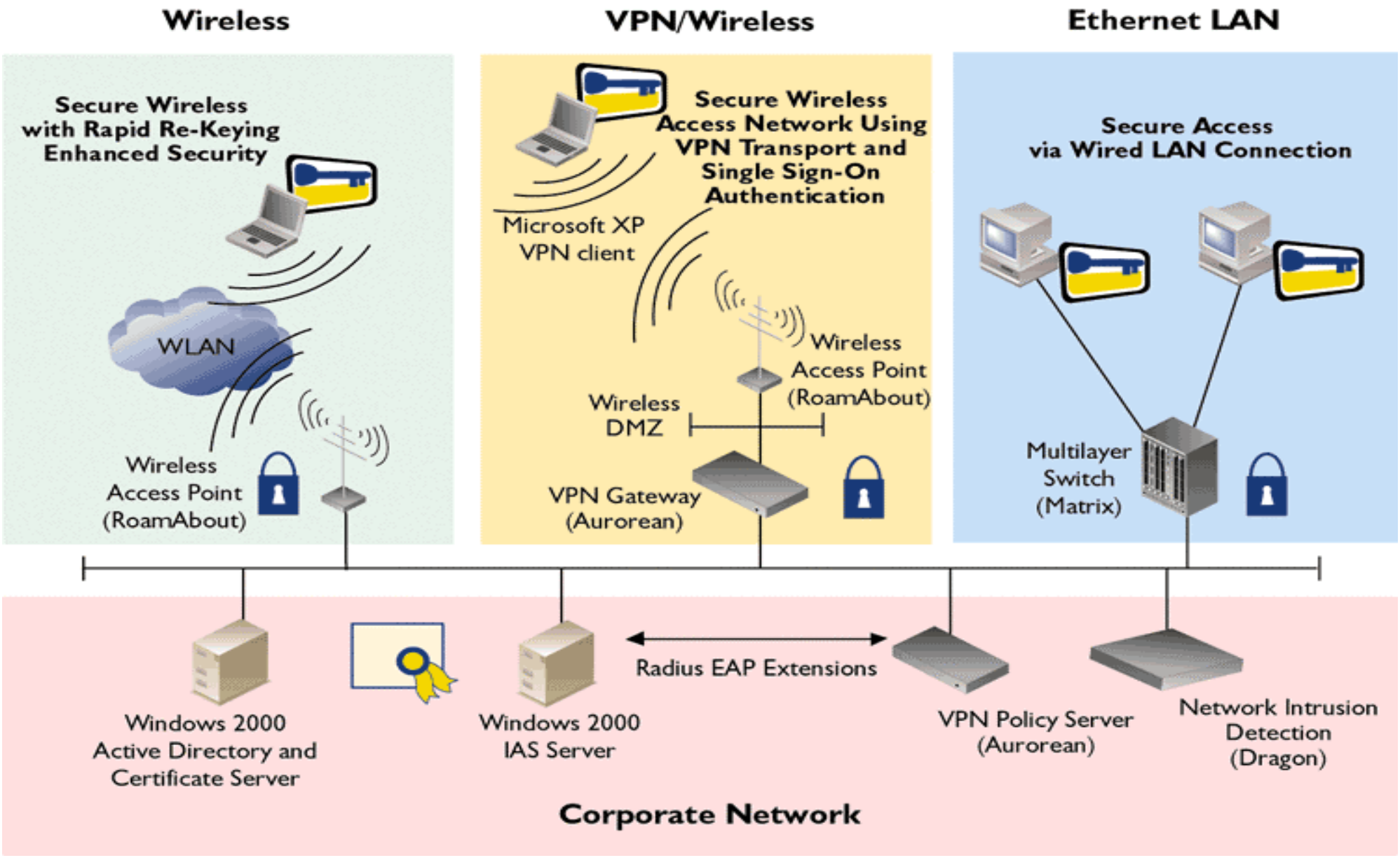
- **Ermöglicht das Zusammenspiel von IT und dem Business**
- **Definition von Regeln und Diensten**
- **Rollenbasierte Regelvergabe**
  - Nutzt eine dreifach Hierarchie zur Kombination von Technologie (Regeln) mit den Geschäfts-anforderungen (Rollen)
  - Versteht das Konzept der Bereitstellung von Diensten
- **Schreibt relevante Informationen auf die Komponenten**



User Personalized NETWORK

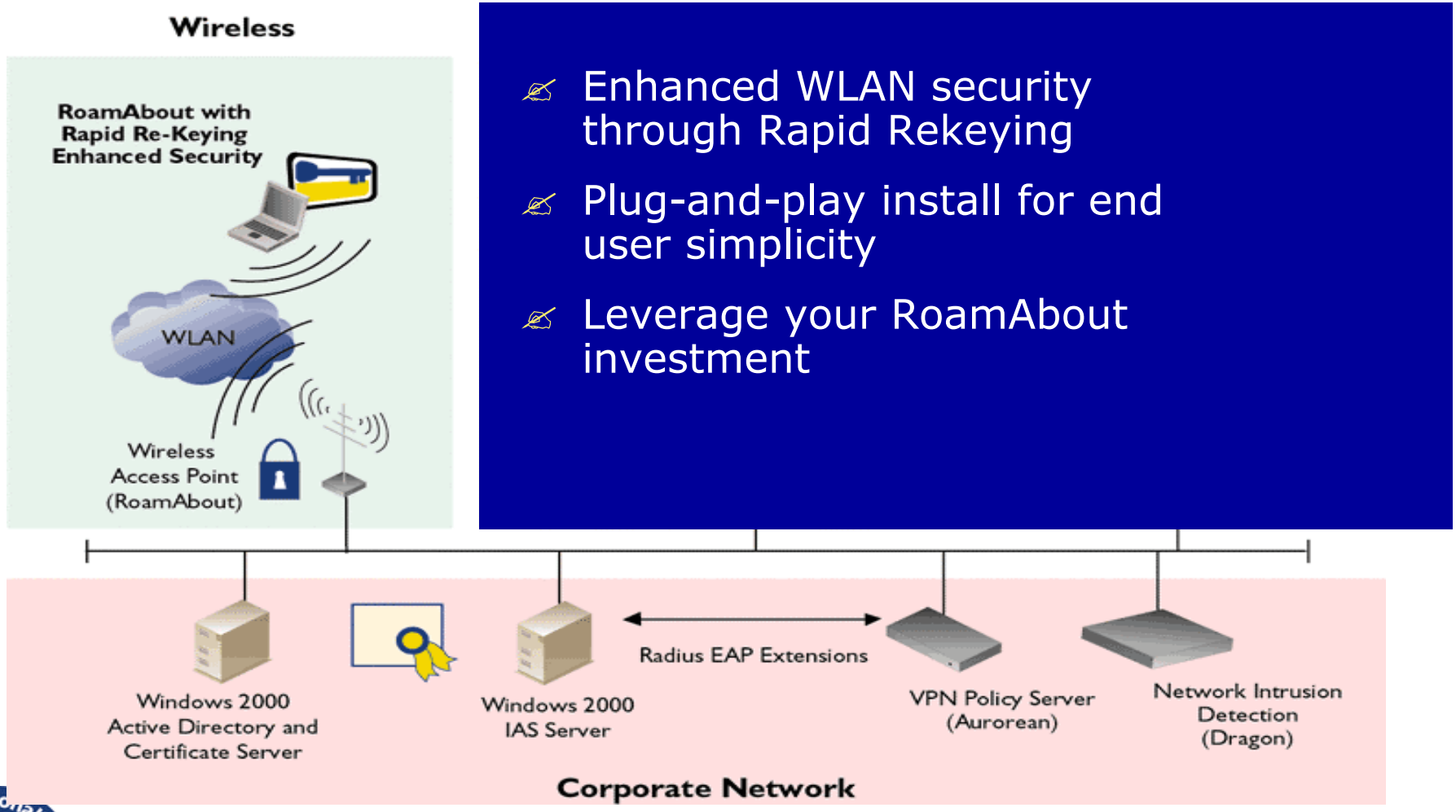
COMPAQ

# Secure Access Network Solutions



COMPAQ

# Secure Wireless Access



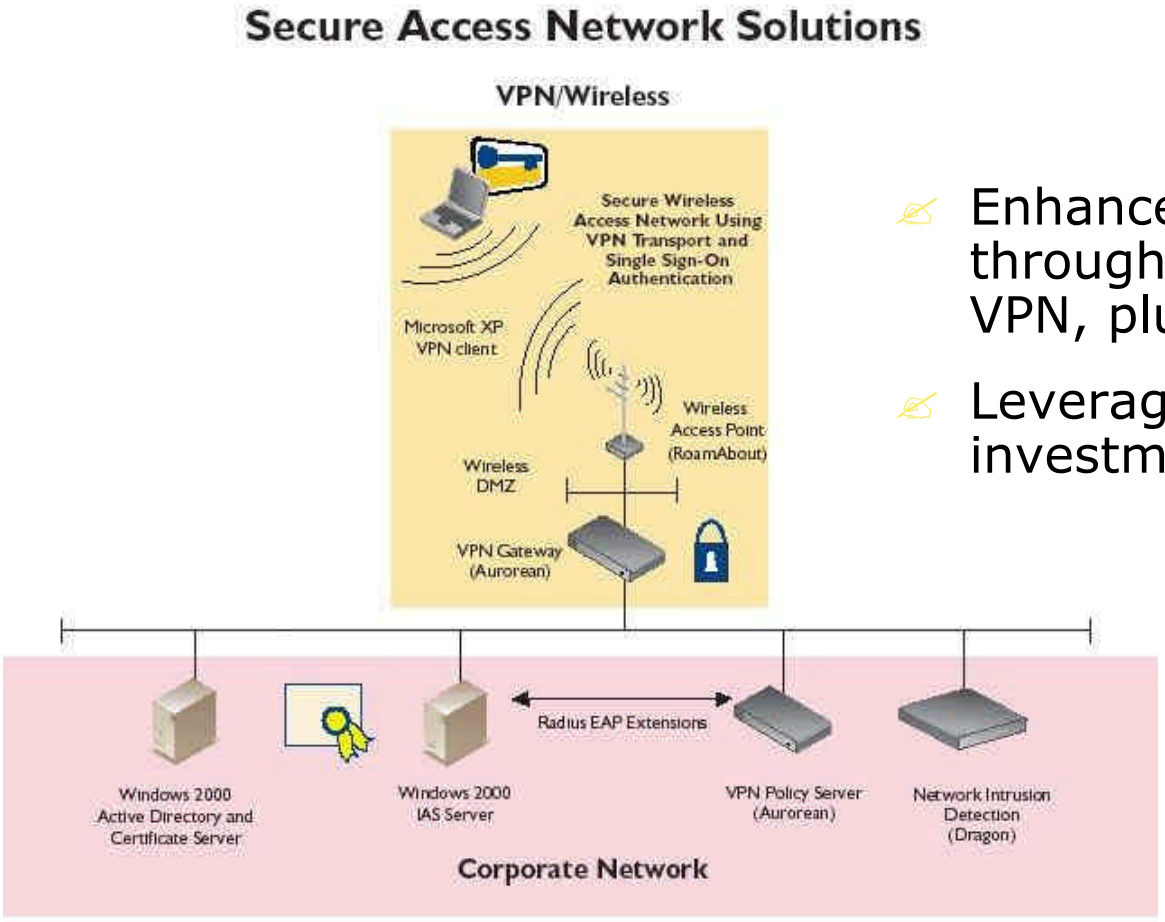

- Enhanced WLAN security through Rapid Rekeying
- Plug-and-play install for end user simplicity
- Leverage your RoamAbout investment

User Personalized Network

ENTERASYS NETWORKS

COMPAQ

# Secure Wireless Access Single Sign On




- Enhanced WLAN security through Rapid Rekeying plus VPN, plus Single Sign On
- Leverage your RoamAbout investment

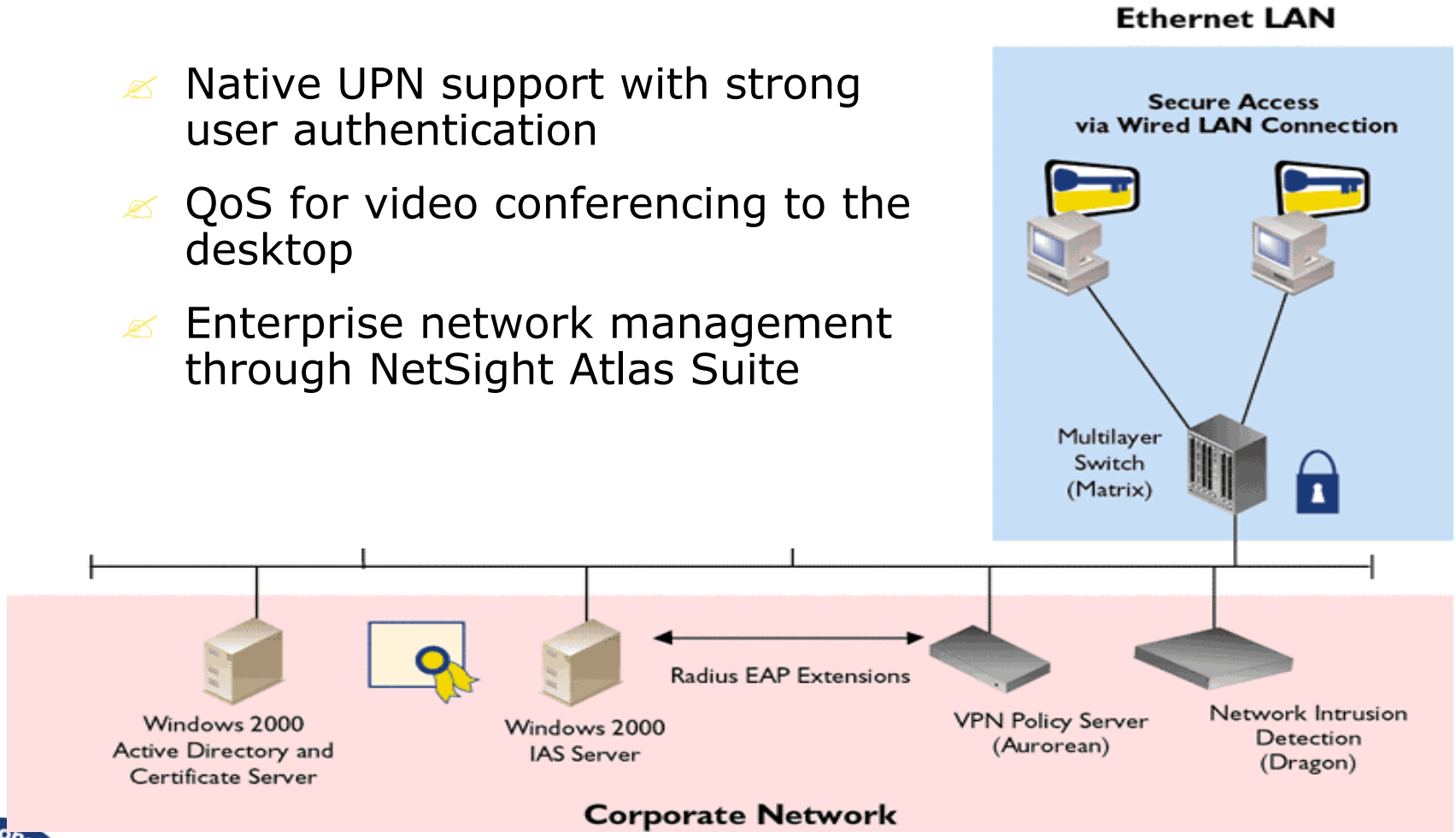
User Personalized Network

ENTERASYS NETWORKS

COMPAQ

# Secure LAN Access

- Native UPN support with strong user authentication
- QoS for video conferencing to the desktop
- Enterprise network management through NetSight Atlas Suite



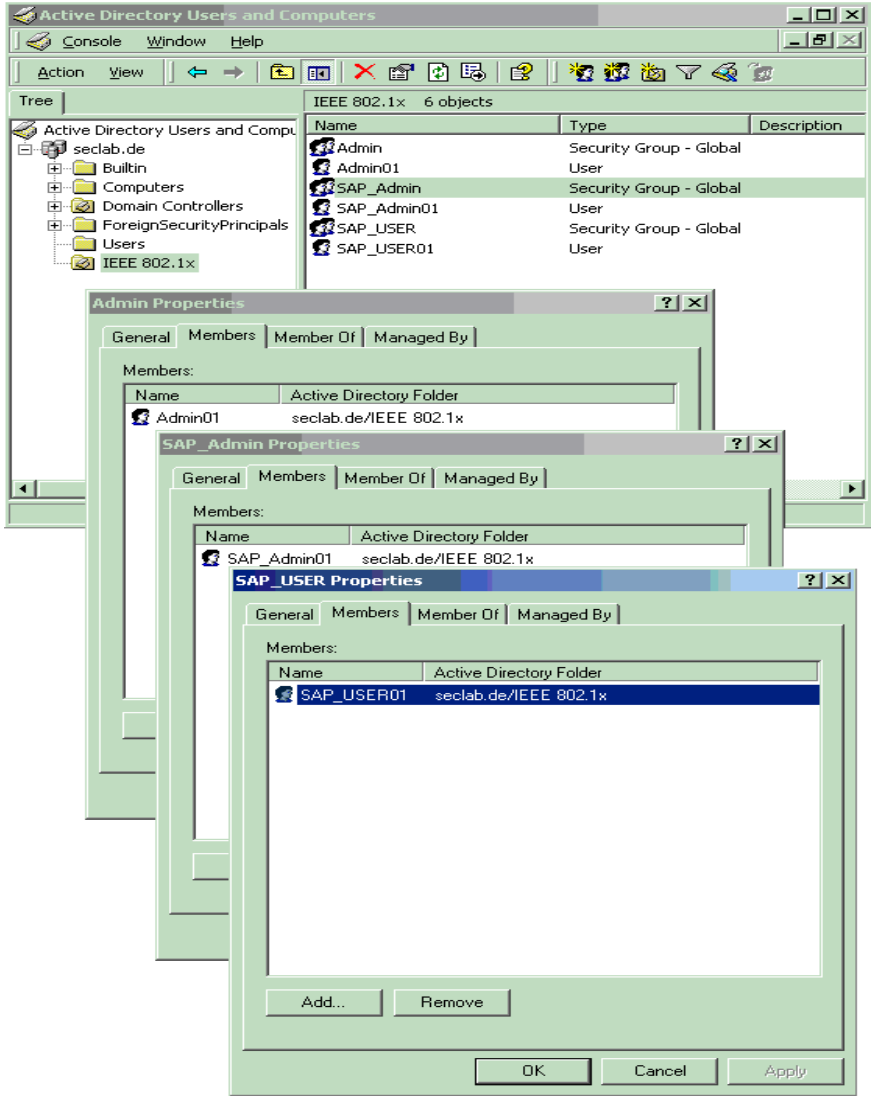

User Personalized Network

ENTERASYS NETWORKS

COMPAQ

# 802.1X - Volle Integration

- Keine proprietäre Technologie wird benutzt
- Integration in existierende Directory und NOS
- W2K, AD
- Siemens DirX
- Novell eNDS




NetSight

User Personalized Network

ENTERASYS NETWORKS

COMPAQ
Inspiration Technology

Compaq Global Services

# Desktop / Device Security

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- **Desktop / Device Security**
- Security Gesamtbild

COMPAQ

# Desktop Security

- Normales Username / Password Verfahren reicht nicht
- Einfaches aber sicheres Verfahren notwendig
- Rechtevergabe auf Basis der Policy (LDAP/AD)
- Bereitstellung von Applications nach Userpolicy
- Besitztum und Wissen als „Passwort“ (Smartcard + PIN)
- Einsatz von biometrischen Verfahren (Fingerprint, Iris Scan usw.)
- Single SignOn

COMPAQ

# Desktop Security Devices

- Alle IT-Systeme!
  - Server
  - PC‘s
  - Terminals
  - PDA
  - Notebooks
  - Unix Systeme
  - Other System (VMS usw.)

COMPAQ

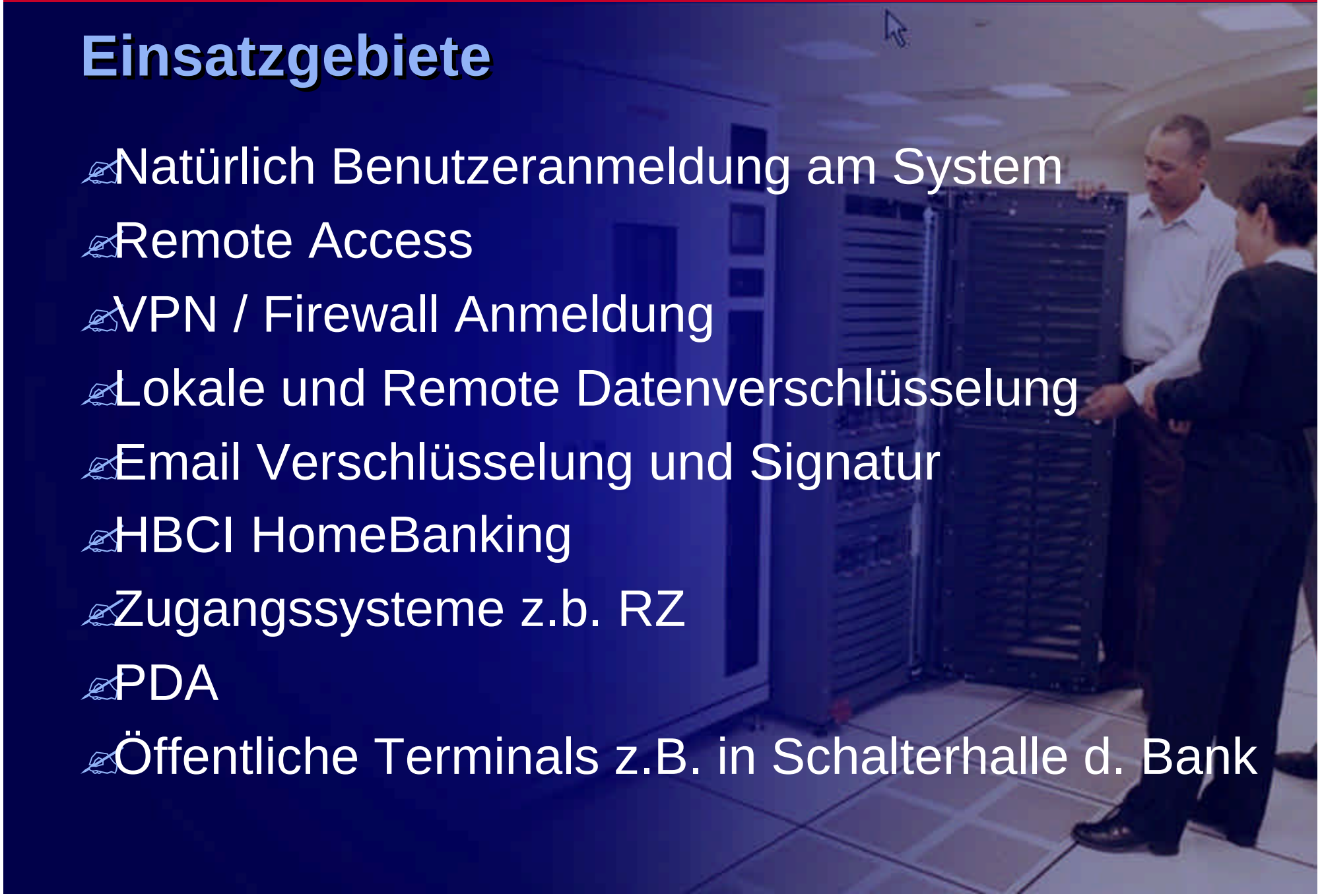
# Mögliche Verfahren

- One Time Password - SecureID Token
- SmartCard
- Fingerprint Reader (Builtin, Mouse, PCMCIA)
- Iris Scan (Festinstallation / Zugangsschutz)
- Spracheingabe
- Handy SMS Verfahren
- USB Dongles
- Sonstige Dongles (Serial usw.)

***Zielsetzung: So einfach und komfortable wie möglich für den User!!!***

COMPAQ

# Einsatzgebiete



- Natürlich Benutzeranmeldung am System
- Remote Access
- VPN / Firewall Anmeldung
- Lokale und Remote Datenverschlüsselung
- Email Verschlüsselung und Signatur
- HBCI HomeBanking
- Zugangssysteme z.b. RZ
- PDA
- Öffentliche Terminals z.B. in Schalterhalle d. Bank

COMPAQ

# Desktop Security – weitere Maßnahmen

- Lokale Virenscanner mit automatischen Update
- Lokale Festplattenverschlüsselung (Notebook) in Hard- oder Software
- Bios Passwort
- Keine FileShares freigeben!!
- Personal Firewall – sehr wichtig!
- Wirkliche Rechtevergabe für Access und Filezugriff lokal und remote
- Regelmäßige lokale Backups oder generelle Fileablage auf dem „sicheren“ Fileserver
- Persönlich auf sein Device achten (Sperren usw.)

COMPAQ

# FileCrypto for Pocket PC


## Settings and use

- Minimum length and character set of pass-phrase can be defined
- Automatic idle time setting
- Max. 10 user specified encrypted folders can be created
- Possibility to define encrypted folders as default folders e.g. for Excel files.

COMPAQ

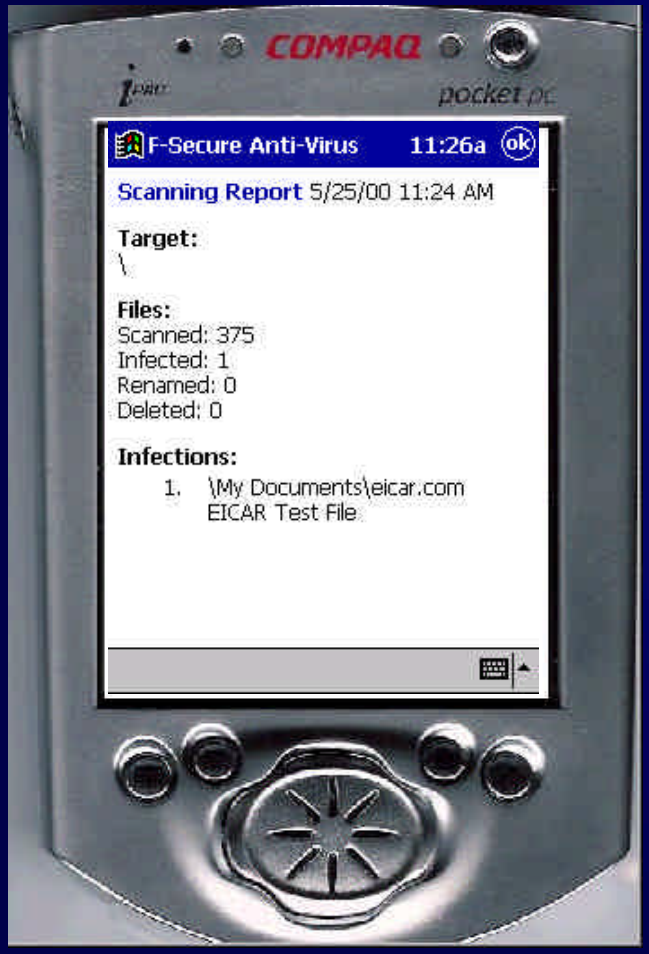
# Anti-Virus for Pocket PC


## Main Features

- Always available protection in the device
- Scans for all malware, also in e-mail messages, attachments and removable media
- Automatic anti-virus database update service through host PC or IP connectivity
- Automatic scanning after ActiveSync, scanning can also be manually invoked

COMPAQ

# Anti-Virus for Pocket PC




- **Automatic anti-virus database update service through the host PC or over IP connectivity**
- **Reporting of scan results**
- **Infected files can be deleted or renamed based on user preferences**

COMPAQ
Inspiration Technology

Compaq Global Services

# Security Gesamtbild

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- **Security Gesamtbild**

COMPAQ

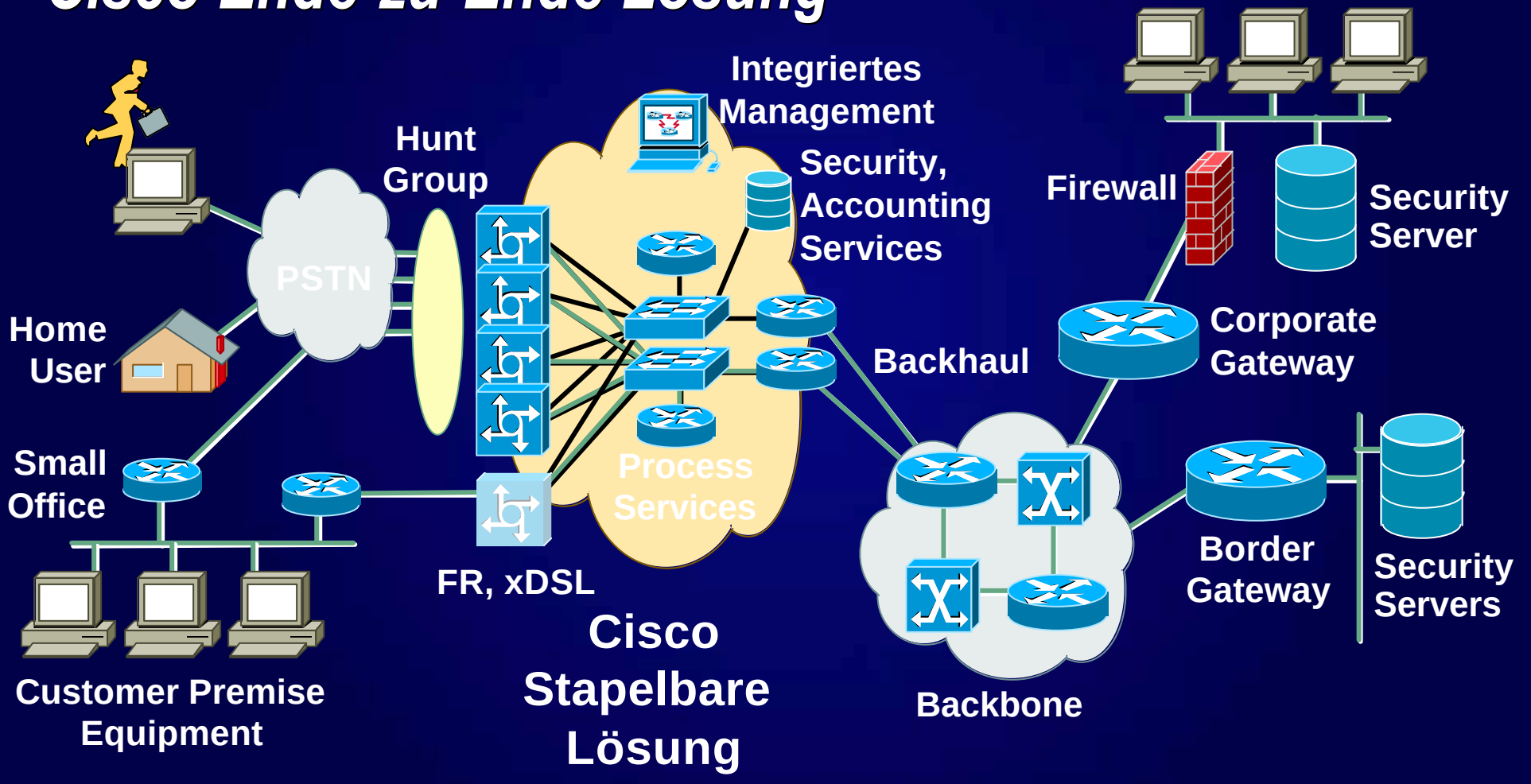
# Gesamtbild

- Security betrifft alle Bereiche einer Infrastruktur
- Security ist keine Einzellösung! (nicht nur Firewall)
- Security beinhaltet organisatorische wie technische Maßnahmen
- Security muss Abteilungsübergreifend in den Firmen betrachtet werden
- Einen 100% Schutz gibt es nicht, aber einen recht hohen Schutz!
- Security ist immer ein Kompromiss
- Schaden: 1. Image, 2. Wirtschaftlich!!!

COMPAQ

# Security Gesamtbild

## *Cisco Ende-zu-Ende Lösung*




COMPAQ
Inspiration Technology