Design und Realisierung von E-Business- und Internet-Anwendungen

Raumänderung NUR für den
Termin am 16.Juni:
Hörsaal 317,LMU Hauptgebäude,
2. OG

„e-Service Areas“
Teil 1

Dr. Michael Nerb et al.,
Prof. Dr. Heinz-Gerd Hegering
SoSe 2005

Einordnung in die Vorlesung
Teil 2: Entwicklung von Lösungen

- ✓ Teil 1: „Grundlagen“ (Plan):
  - ✓ Welche Konzepte, Dienste und Technologien gibt es?
  - ✓ Was leisten sie, wie funktionieren sie, wie spielen sie zusammen?

- ■ Teil 2: „Entwicklung von Systemlösungen“ (Build):
  - Was sind typische Kundenanforderungen u. praxisnahe Szenarien?
  - Wie setze ich diese technisch um (Kosten, Machbarkeit, Qualität)?
  - Was ist während Beschaffung, Installation, Konfiguration, Test, Dokumentation, Abnahme, Projektmanagement usw. zu beachten?

- ■ Teil 3: „Betrieb von Systemlösungen“ (Run):
  - Wie erhalte ich die Lösung „am Leben“?
  - Wie manage ich die Weiterentwicklung über den Technologiezyklus

Entwicklung von Lösungen
Überblick über die nächsten beiden Termine

- Was verbirgt sich hinter dem Begriff „e-Service Area“?
- Exkurs: Typischer Ablauf einer Ausschreibung
- Fallbeispiel:
  - Internationales Unternehmen benötigt e-Service Area zur Abwicklung geschäftskritischer Anwendungen über das Internet
  - Unternehmen betreibt Web-Portal für eine Online-Zeitung
- Schwerpunkte:
  - Darstellung des Szenarios und der Kundenanforderungen
  - Design und Funktionsweise einer geeigneten e-Service Area
  - Diskussion alternativer Lösungsmöglichkeiten und Produkte, u.a.:
    - Hochverfügbarkeit, Performanz, Flexibilität der Lösung
    - Rechenzentrums-Infrastruktur, zentrale Basisdienste
  - Entwicklung einer Gesamtlösung, Kostenbestandteile, Management

Begrifflichkeiten
„e-Service Area“

- E-Service Area: (gesharte) Plattform für IP-basierte Kommunikation:
  - Vernetzung von Standorten und Organisationen auf Basis von IP-VPN‘s:
    - Intranets und Extranets
    - Gesicherte Übergänge ins Internet und Remote Access
  - Schwerpunkt auf netznahen Anwendungsdiensten, z.B.:
    - Naming/Directory, E-Mail
    - Web-Proxies, Web-Hosting, Zeitserver
    - Security (Firewalls, IDS, Virenscanning, URL-Blocking, usw.)
    - Administration: Reporting, Accounting, Beauftragung usw.

- E-Service Area bietet:
  - modulare und skalierbare Bausteine (Dienste), standardisiert (aber anpassbar) an kunden-individuelle Anforderungen
  - Einheitliche Prozesse und Werkzeuge für den Betrieb
  - Synergieeffekte und Kosteneinsparungen u.a. durch:
    - Reduktion der Investitionskosten
    - (Örtliche) Konzentration von qualifiziertem Personal, Skills und Know-How
    - Mitnutzung von Rechenzentren, Netzen, zentralen Diensten, Ressourcen

Typischer Ablauf von Ausschreibungen
RFI, NDA, RFP und LOI

- Request for Information (RFI):
  - Initiator ist der Kunde, Adressaten sind „potentielle“ Dienstleister
  - Aufforderung zur Beantwortung eines (umfangreichen) Fragenkatalogs
  - Ziel des Kunden: Vorqualifikation und Auswahl von Kooperationspartnern („Beauty Contest“) für einen nachfolgenden RFP
  - Oft verbunden mit einem „Non Disclosure Agreement“ (NDA)

- Request for Proposal (RFP):
  - Initiator ist der Kunde, Adressaten sind „qualifizierte“ Dienstleister laut RFI
  - Ausschreibung, Aufforderung zur Abgabe eines Angebots
  - Ziel des Kunden: Verbindliche Leistungsbeschreibung, Preise und Vergleichbarkeit von Angeboten unterschiedlicher Bieter

- Letter of Intent (LOI):
  - Initiatoren sind der Kunde und der „siegreiche“ Bieter des RFP‘s
  - Unverbindliche Absichtserklärung, eine Vertragspartnerschaft einzugehen
  - Ziel: Entwicklung eines für beide Seiten vertretbaren Vertragswerks

Typischer Ablauf von Ausschreibungen
Request for Information (RFI)

- Aufforderung zur Beantwortung eines Fragenkatalogs durch Dienstleister
- Allgemeine Bieterdarstellung, z.B.:
  - Eigentumsverhältnisse, Organisationsstruktur, (internationale) Präsenz
  - Kennzahlen des Dienstleisters (z.B. Größe, Umsatz, EBITDA)
  - Strategie, Marktpositionierung (z.B. im Vergleich zu Konkurrenten)
  - Branchenabdeckung, Kundenstruktur, Service Portfolio
  - Infrastrukturen (z.B. Rechenzentren, Netze, HelpDesk, Service usw.)
- Qualitative Antworten auf Anforderungsspezifikation des Kunden:
  - Technische Lösungsansätze und -vorschläge
  - Referenzinstallationen für vergleichbare Anforderungen
  - Angewandete Methoden bei Projektmanagement, Implementierung und Betrieb, u.a.:
    - Datenschutz, Dokumentation
    - Qualitätssicherung, ISO 900x, ITIL

Typischer Ablauf von Ausschreibungen
Request for Proposal (RFP)

- Ausschreibung, Aufforderung zur Abgabe eines Angebots für „qualifizierte“ Dienstleister laut RFI
- Inhalte des RFP (werden meist vom Kunden vorgegeben):
  - Service Beschreibungen (welche Dienste sollen erbracht werden?)
  - Service Levels (z.B. Ausfallzeiten, Verfügbarkeiten, MTTR) inkl. Messung und Überwachung
  - Anforderungen an Prozesse, Informations- und Eskalationswege, Change Management, Schnittstellen usw.
  - Mengengerüst (z.B. Hardware, SW, User, Bandbreiten o.ä.)
  - Ort der Leistungserbringung (ggf. mehrere Orte, auch international)
  - Vertragsaspekte (Pönale, Bindungsfristen, Laufzeiten, Deadlines usw.)
  - Aufschlüsselung der Kosten, z.B. nach:
    - Einmaligen und laufenden Kosten (z.B. je User oder Service)
    - Hardware-/Software-/Lizenzkosten (und Wartungskosten dafür)
    - Planungs-, Implementierungs und Betriebskosten

Typischer Ablauf von Ausschreibungen
Bieterauswahl und Bietergespräche

- Kunde wertet nach RFP die Angebote der verschiedenen Bieter aus:
  - z.B. anhand technischer, kommerzieller, organisatorischer oder „politischer“ Kriterien (sowie den bisherigen Erfahrungen mit dem Bieter)
  - Führt oftmals bereits zum Ausschluss von Bietern
- Kunde lädt verbleibende Bieter (separat) zu sog. „Bietergesprächen“ ein:
  - Vorstellung des Angebots durch den Bieter
  - Fragen und Klarstellungen zu allen offenen/interessanten/relevanten Punkten
  - Aufforderung zur Nachbesserung, Konkretisierung, Erweiterung, Einschränkung von Leistungen (je nach Sachlage)
  - Preisverhandlungen
- Sukzessiver Ausschluss von Bietern (ggf. finden mehrere Bietergespräche statt) und schließlich Festlegung auf einen Bieter

Typischer Ablauf von Ausschreibungen
Letter of Intent (LOI) und weiteres Vorgehen

- Unverbindliche Absichtserklärung, eine Vertragspartnerschaft einzugehen:
  - D.h. kein Vertrag, kein Auftrag, keine Rechtsansprüche
  - Aber: Oftmals ist LOI Grundlage für den nachfolgenden Vertrag
- Nachfolgende Vertragsverhandlungen:
  - Weniger technische Aspekte
  - Vorwiegend Preisverhandlungen und
  - Konkretisierung von Liefer- und Leistungsbeziehungen, Zeitplänen, Meilensteinen, Vertragsaspekten, Ausstiegsklauseln, Pönalen usw.
- Vertragsunterzeichnung:
  - Rechtliche Bindung zwischen Kunden und Bieter
  - Spätestens jetzt sollte u.a. beginnen:
    - technische/prozessuale Detailplanung
    - Aufbau des Projektmanagements und der Projektorganisation (auf Kunden- und Bieterseite), Staffing der Teams, Zuteilung von Aufgaben usw.
    - Bestellung der erforderlichen HW/SW/Lizenzen, Vorleistungen usw.

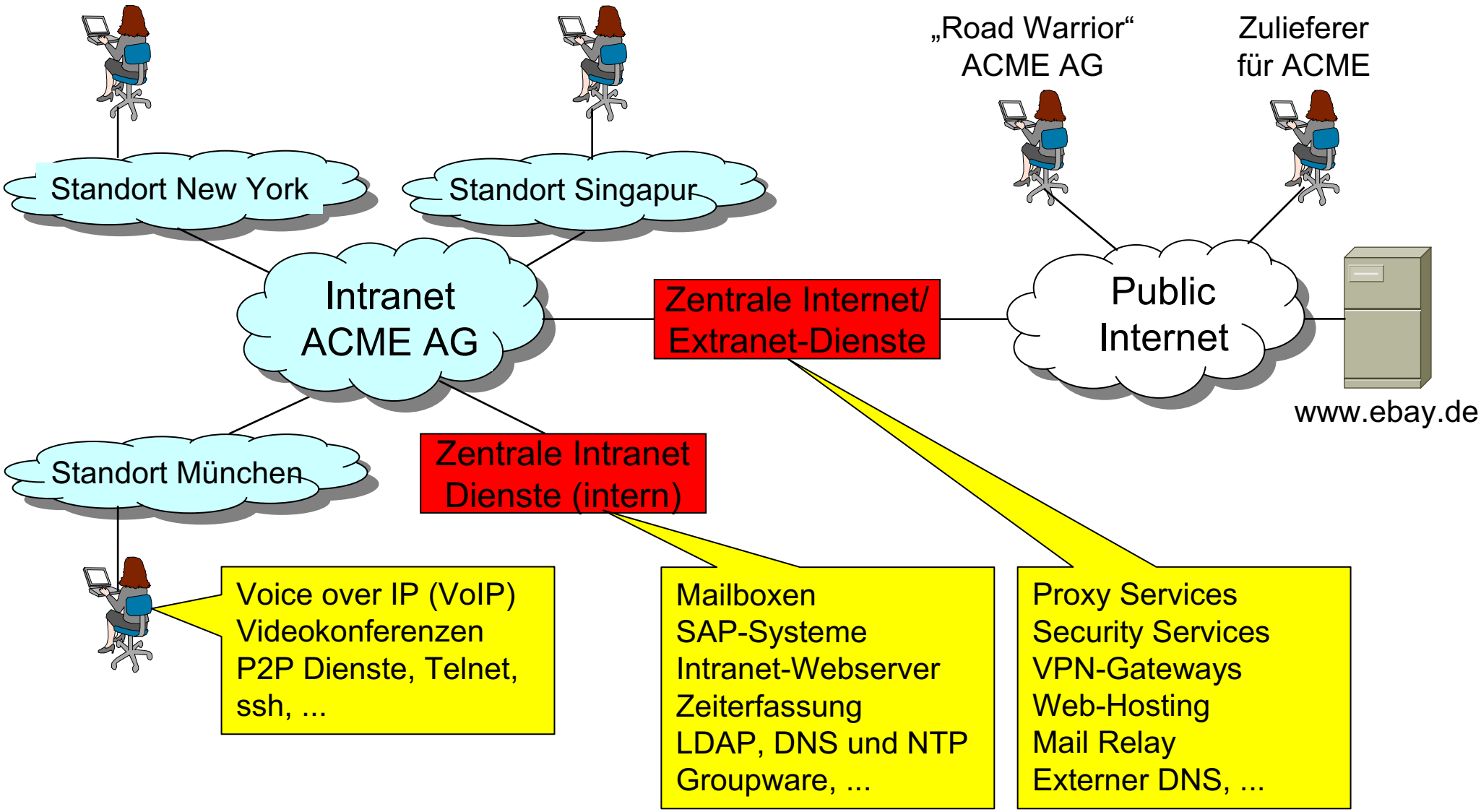
Typischer Ablauf von Ausschreibungen
Einige Anmerkungen zum Verfahren

- Erstellung und Beantwortung von Ausschreibungen kann sehr arbeits- und zeitaufwändig sein (hängt maßgeblich von der Größe und Umfang ab)
- Je nach Qualität der Ausschreibungsunterlagen ist man (mehr oder weniger) auf Annahmen und Mutmaßungen angewiesen:
  - Falls erlaubt: Rückfragen stellen
  - Andernfalls: Konkrete Leistungsumfänge definieren oder Leistungsausschlüsse benennen
- Ausschreibungen sind auch ein Instrument des Kunden, gezielt Preise und Leistungen zu steuern, z.B. durch:
  - „Benchmarking“:
    - Scheinausschreibung, um den bisherigen Dienstleister im Preis zu drücken
    - Bewertung von internen Outsourcing-Bestrebungen des Kunden
  - Gegenseitiges Ausspielen von Bietern durch den Kunden
  - Kommunikation von Budgets und Zielpreises

Fallbeispiel
Überblick

- Internationales Unternehmen ACME AG benötigt e-Service Area zur Abwicklung geschäftskritischer Anwendungen über das Internet
- Zentrale Standorte (als Konzentrationspunkte regionaler Strukturen):
  - „EMEA“ (Europe, Middle East and Africa): Deutschland
  - „Asia/Pacific“: Singapur
  - „Americas“: New York
- Aufbau eines:
  - Intranets: Verbindung der Standorte und zentrale Intranet-Dienste
  - Gesicherten, zentralen Übergangs ins Internet mit folgenden Diensten:
    - Security Services (Firewalls, URL Blocking, Virenscanning), Zeitserver
    - Web-Access (Proxies für HTTP, FTP, NNTP, usw.)
    - E-Mail (Relaying und Mailboxen mit Virenscanning und SPAM-Filter)
    - Naming und Directory Services (DNS und LDAP)
  - Extranets: Anbindung von Drittfirmen, Lieferanten usw.
  - Remote Access: Anbindung von mobilen Nutzern über das Internet

ACME AG
Kommunikationsflüsse und Beteiligte (schematisch)



Design des Corporate Networks
Entscheidungsfindung

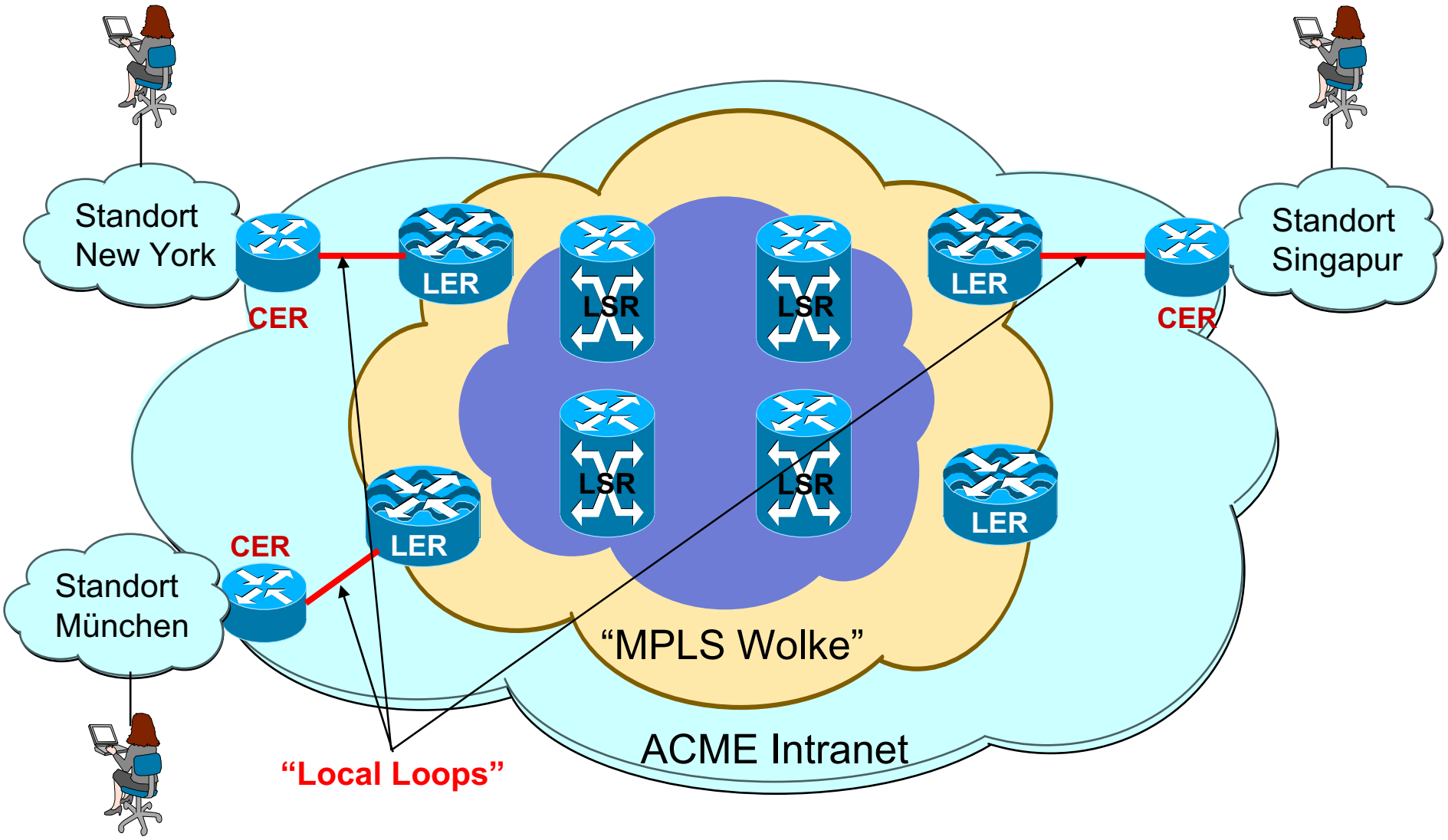
- Aufgabenstellung: Internationales VPN als Intranet für die ACME AG
- Alternativen zur Realisierung:
  - IPSec über das öffentliche Internet
  - MPLS über eine gesharte MPLS Plattform des Dienstleisters
- Einige Entscheidungskriterien:
  - Anzahl und Lage der Standorte
  - Verfügbarkeit und Preise von „Local Loops“ an den Standorten
  - Notwendigkeit von Quality of Service (QoS) und Bandbreiten
  - Zuverlässigkeit, Verfügbarkeit und Flexibilität der Anbindung
  - Technische und betriebliche Aufwände zur Sicherung der Anbindung (im Falle von Internet-basierten VPN‘s)
- Entscheidung für ACME AG:
  - Aufbau eines VPN‘s auf Basis der MPLS-Plattform
  - Implementierung von QoS für verschiedene Anwendungsklassen

Realisierung des Corporate Networks
Umsetzung

- Überbrückung der „letzten Meile“ vom Kunden zum LER:
  - Erfordert einen Local Loop (typischerweise eine Festverbindung)
  - Bei internationalen Standorten erfordert dies ggf. den Zukauf von Leistungen (d.h. Leitungen) von lokalen Carriern
- Roll-Out, Installation und Anschaltung je eines CER pro Standort
  - Typischerweise in den Räumlichkeiten des Kunden
  - Konfiguration der verfügbaren Bandbreiten, QoS-Klassen, Routing, Labels usw.
- Ergebnis:
  - CER labeln IP Pakete (mit interior und exterior Labels)
  - MPLS Netz routet/switcht die IP Pakete zwischen ACME-Standorten
  - Any-to-Any Kommunikation der User untereinander, z.B. für
    - VoIP (Voice over IP), Videokonferenzen
    - Ende-zu-Ende Dienste (telnet, ssh, File-Sharing usw.)

Realisierung des Corporate Networks

Aufbau eines MPLS-basierten VPN‘s



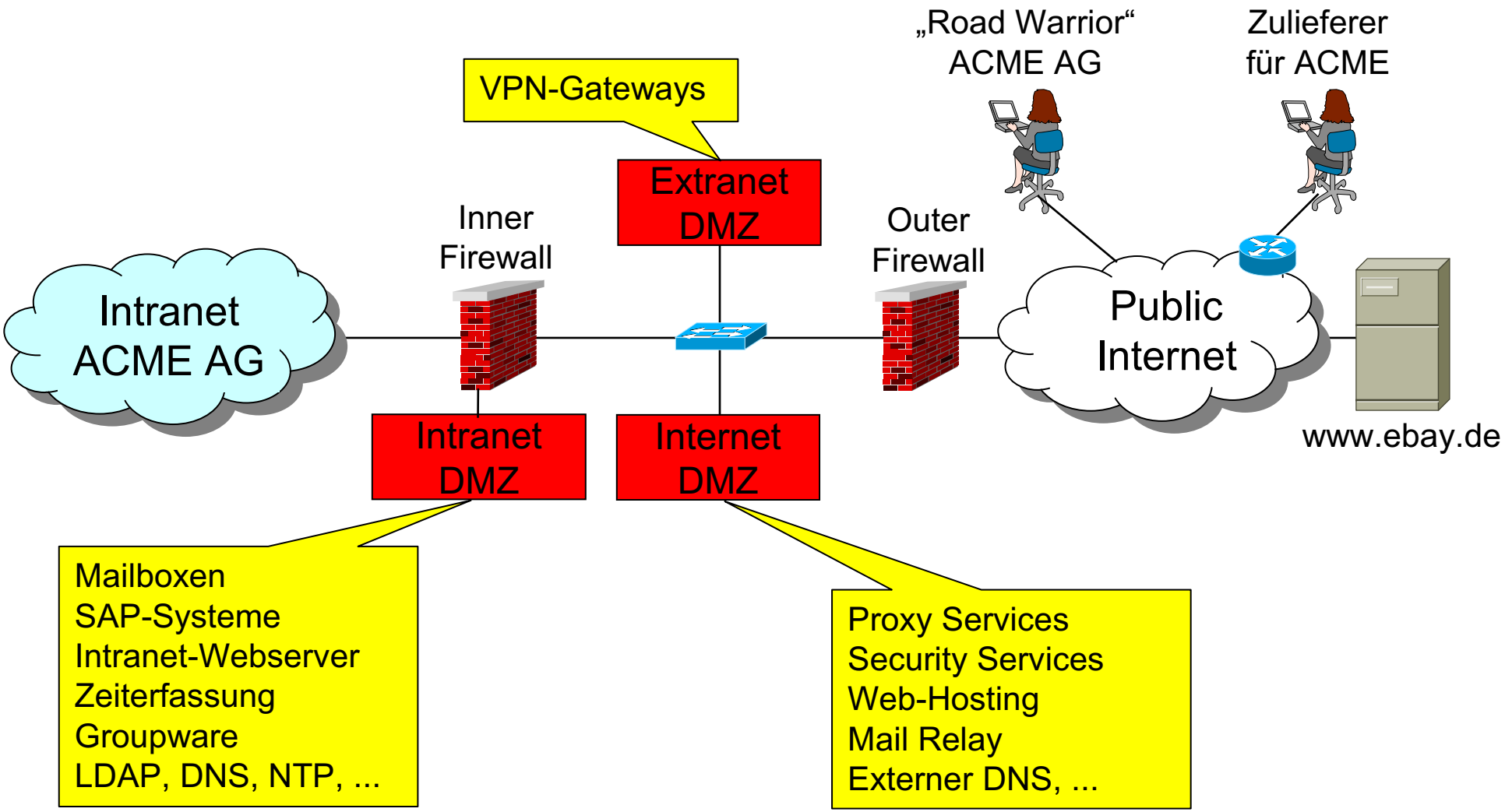
Design der zentralen Dienste
Entscheidungsfindung

- Aufgabenstellung:
  - Anbindung des ACME Intranets an das Internet
  - Trennung und Sicherung der Dienste im Intranet/Internet/Extranet
  - Beschränkung der Kommunikationsflüsse auf ein Minimum
  - Bereitstellung der bereits angesprochenen Dienste:
    - Security Services (Firewalls, URL Blocking, Virenscanning), NTP-Server
    - Web-Access (Proxies für HTTP, FTP, NNTP, usw.)
    - E-Mail (Relaying und Mailboxen mit Virenscanning und SPAM-Filter)
    - Naming und Directory Services (DNS und LDAP)

- Einige Entscheidungskriterien:
  - Sicherheitspolitik des Kunden (bestimmt maßgeblich das Design durch technisch ableitbare Sicherheitsanforderungen)
  - Verfügbarkeit von Produkten, Kosten
  - Technische Machbarkeit, und resultierende betriebliche Aufwände
  - Benutzerfreundlichkeit, Flexibilität und Praktikabilität

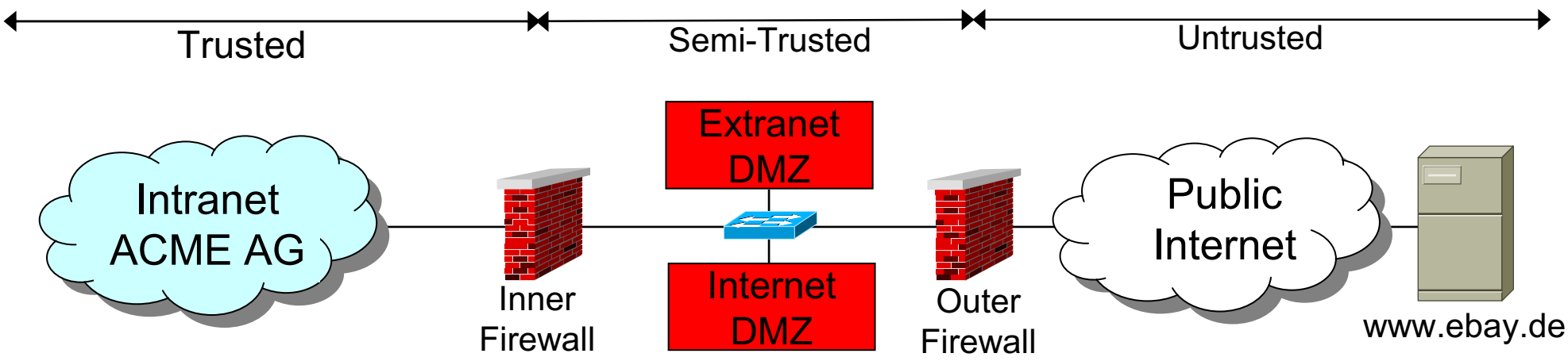
Design der zentralen Dienste

Mögliche Variante der Internet-Anbindung und DMZ



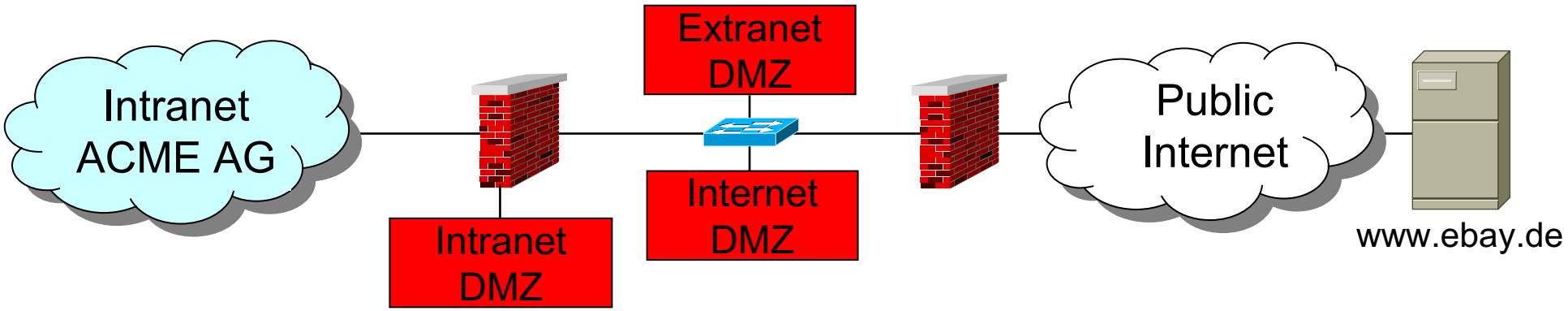
Design des Internet-Übergangs
Details zu den Firewalls

- 2-stufige Firewall-Architektur (Produkte verschiedener Hersteller):
  - „Outer Firewall“ (z.B. Cisco PIX, ...):
    - Screening Router, Stateful Packet Filtering, ggf. NAT
    - „First Line of Defense“, entlastet die „Inner Firewall“
  - „Inner Firewall“ (z.B. Checkpoint VPN-1, Stonesoft Stonegate, ...)
    - Stateful Packet Filtering
    - Beschränkung der Kommunikationsbeziehungen auf einzelne Hosts
- Trennung in die Sicherheitsbereiche Untrusted/Semi-Trusted/Trusted
  - (Vorsicht: „Trusted“ heißt nicht, dass diese Zone vertrauenswürdig ist!!!!)



Design des Internet-Übergangs
Details zu den DMZ‘s

- Trennung der Intranet, Extranet- und Internet-Dienste:
  - Intranet-DMZ: Bereich für ACME-interne Dienste
    - nicht im Internet bekannt und nicht aus dem Internet ansprechbar
  - Internet-DMZ: Bereich für Internet-Dienste
    - Typischerweise im Internet bekannt und auch ansprechbar
  - Extranet-DMZ: Anbindung von Fremdfirmen und Road Warriors
    - Ebenfalls im Internet bekannt und ansprechbar
- Kommunikationsflüsse nur zwischen:
  - „Intranet ACME“ <-> „Intranet DMZ“
  - „Intranet DMZ“ <-> „Internet DMZ“, „Intranet DMZ“ <-> „Extranet DMZ“
  - „Internet DMZ“ <-> „Internet“ und „Extranet DMZ“ <-> „Internet“



Design der Proxy und Security Services
Anforderungen

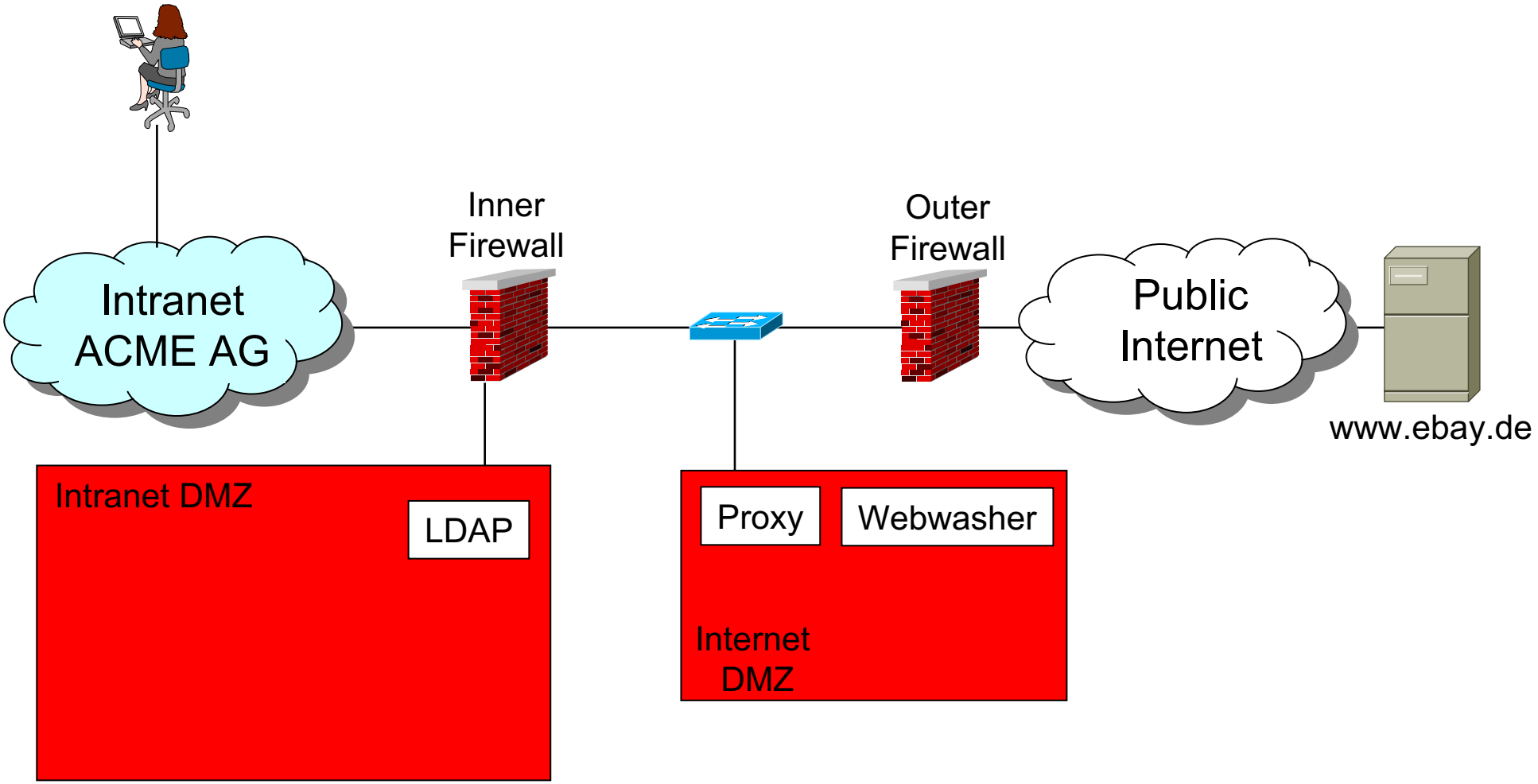
- Zentraler Proxy und Cache für ca. 5.000 User und folgende Protokolle:
  - HTTP (inklusive „ftp over http“)
  - FTP native (d.h. ftp über Kommandozeile)
  - HTTPS (sog. „CONNECT Methode“)
  - NNTP (Newsproxy für einen festgelegten News-Feeder)
- Authentifizierung von Usern über LDAP
- URL Blocking für folgenden Inhalt:
  - Porno/Sex, Illegale und kriminelle Aktivitäten
  - Rassismus, Haß, Unterdrückung
- Content Scanning des Web-Verkehrs:
  - Prüfen auf Viren, Malicous Codes, Embedded Objects (ActiveX Controls o.ä.)
  - Entpacken und Scannen von Archiven bis zur „Schachtelungstiefe N“
  - Unterdrücken von verschlüsselten Archiven, Popup-Fenstern, Werbebannern, ...
  - Kein Scanning von https-Verkehr (wäre technisch auch machbar)
- Sammlung von Loginformationen zur späteren Aufbereitung, z.B.
  - Nutzungsstatistiken (pro Benutzer, Gruppe, Kostenstelle o.ä.)
  - Analyse der typischen Verkehrsbeziehungen

Design der Proxy und Security Services
Entscheidungsfindung

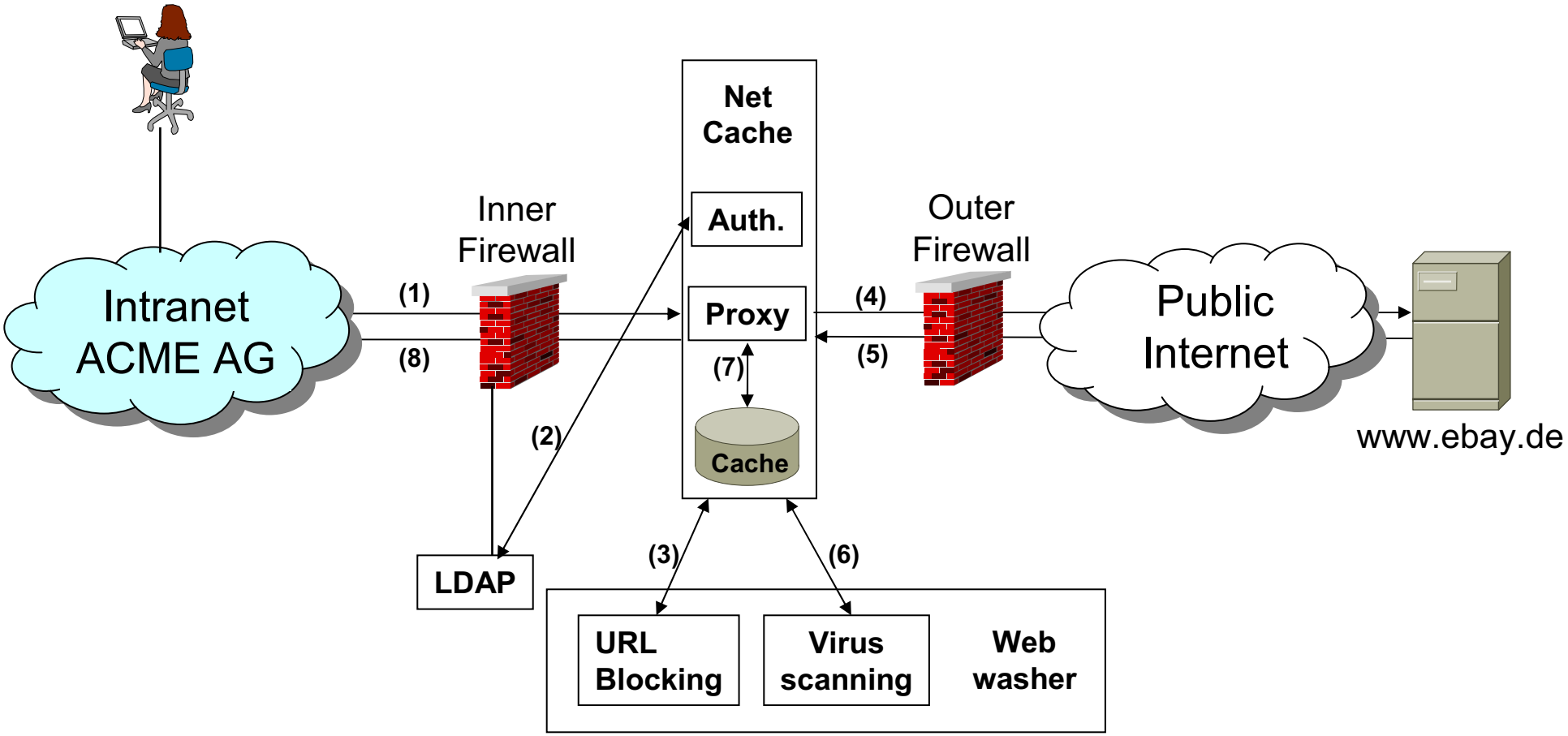
- Proxy und Cache:
  - Open Source: Squid
  - Kommerzielle Lösungen: z.B. BlueCoat, Network Applicance (Netcache)
- URL Blocking und Virenscanning:
  - Webwasher „Content Security Management“, Websense, SmartFilter
  - Trend Micro Viruswall, McAfee Virus Scanner, ...
- Einige Entscheidungskriterien:
  - Kommerzielle Produkte vs. Open Source
  - Wartung und Support, Reaktionszeiten (z.B. bei Bugs oder neuen Viren)
  - Redaktionsteam und Klassifikation von Content (für URL Blocking)
- Entscheidung für ACME AG:
  - Network Appliance und Webwasher (Kopplung über ICAP)

Realisierung der Proxy und Security Services

Benötigte Systeme



Realisierung der Proxy und Security Services
Kommunikationsflüsse und Nutzung der Dienste



(Vereinfachte Darstellung! Alle Kommunikationsflüsse gehen natürlich durch die Firewalls von und zu den entsprechenden DMZ!)

Design des „Extranets“
Anforderungen

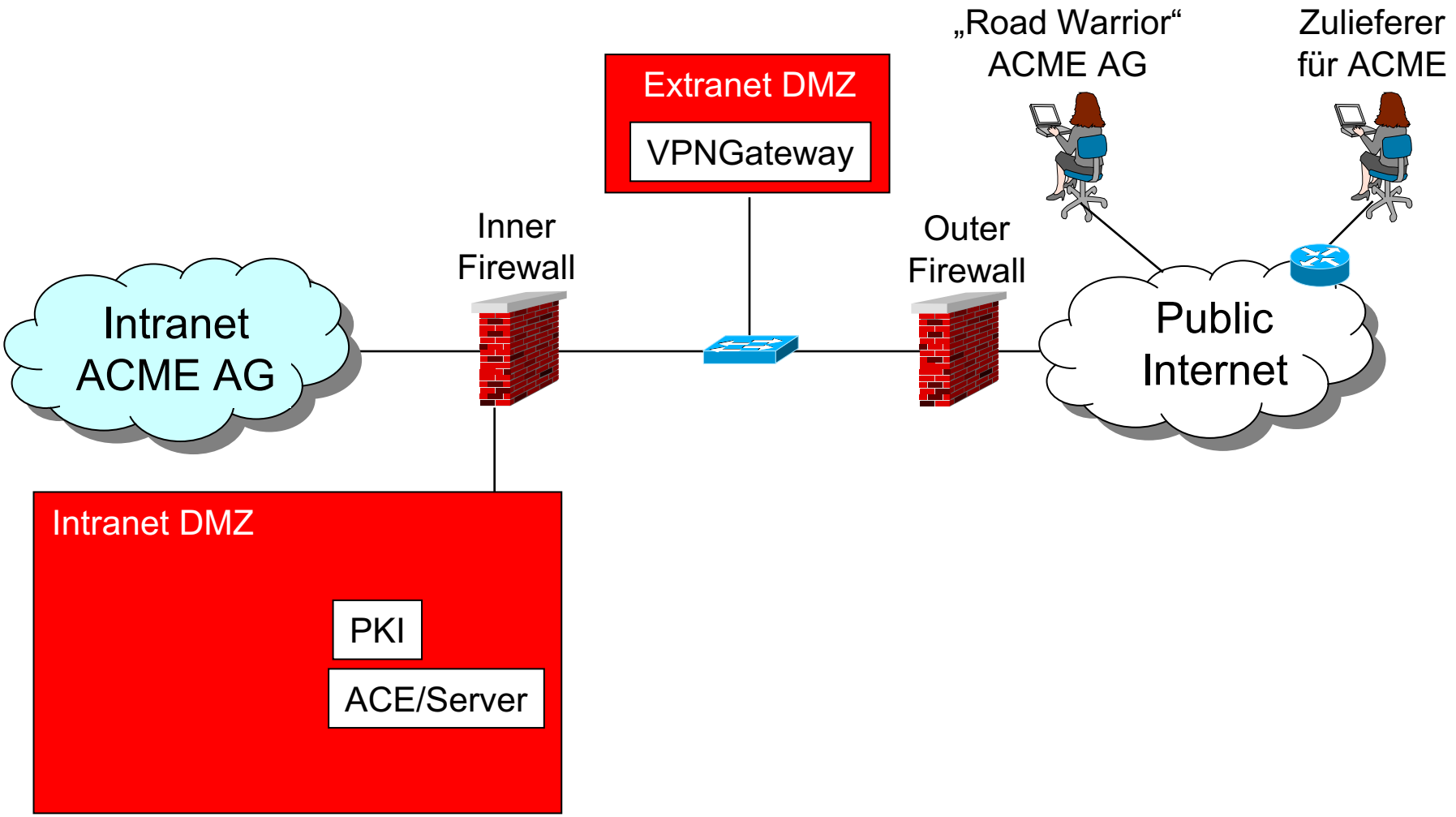
- Anbindung von ca. 200 Lieferanten, Fremdfirmen sowie 500 „Road Warriors“ erfolgt über eine eigene DMZ:
  - Road-Warriors: vgl. Remote Access Szenario (End-to-Site)
  - Lieferanten usw: vgl. Extranet Szenario (Site-to-Site)
- Zugang erfolgt ausschließlich auf Basis von AAA
  - Starke Authentifizierung (Zertifikate oder „One Time Pass“, OTP)
  - Starke Verschlüsselung (3DES, AES o.ä.)
- Zugang erfolgt über das öffentliche Internet (international):
  - Unterstützung von:
    - Road Warriors: POTS, GSM, GPRS, UMTS, WLAN, DSL
    - Lieferanten: DSL
  - Erforderliche Software:
    - VPN-Client, Dialer, Personal Firewall, Virenscanner
    - Plattformen: Windows, MAC, Linux usw.

Design des „Extranets“
Entscheidungsfindung

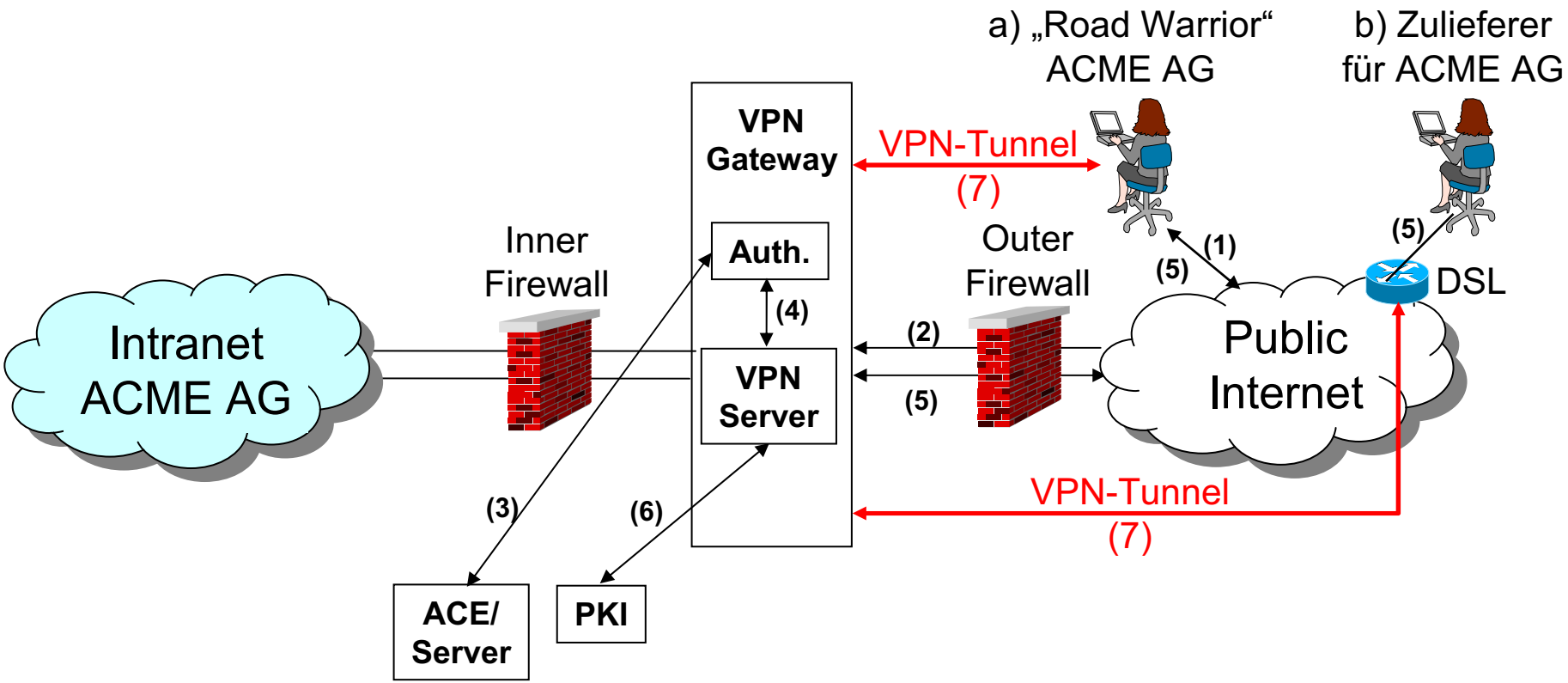
- VPN Gateways:
  - Open Source: FreeS/WAN, OpenSwan, StrongSwan
  - Kommerzielle Lösungen: z.B. Cisco VPN Concentrator, VPN1-Modul der Checkpoint oder Stonegate Firewall, NCP Software
- Starke Authentifizierung:
  - Road Warriors: RSA SecurID Token, Kobil Token
  - Lieferanten: X.509 Zertifikate, z.B. von Verisign, TeleSec o.ä.
- Einige Entscheidungskriterien:
  - Kommerzielle Produkte vs. Open Source, Unterstützte Plattformen
  - Wartung und Support, Reaktionszeiten (z.B. bei Bugs)
  - Trennung von Firewall- und VPN-Funktionalität

- Entscheidung für ACME AG:
  - Cisco VPN Concentrator und RSA SecurID Token (ACE/Server)

Realisierung des „Extranets“
Benötigte Systeme



Realisierung des „Extranets“
Kommunikationsflüsse und Nutzung der Dienste



(Vereinfachte Darstellung! Alle Kommunikationsflüsse gehen natürlich durch die Firewalls von und zu den entsprechenden DMZ!)

Literatur
Links zum Thema

- Hersteller von Produkten, z.B.:
  - Cisco Systems: www.cisco.com, Checkpoint: www.checkpoint.com
  - Stonesoft: www.stonesoft.com, Network Appliance: www.netapp.com
  - Webwasher: www.webwasher.com, TrendMicro: www.antivirus.com
  - RSA: www.rsasecurity.com, Kobil: www.kobil.com, NCP: www.ncp.de
- Open Source Lösungen, z.B.:
  - Squid: www.squid-cache.org, DNS: www.isc.org
  - LDAP: www.openldap.org, NTPD: www.ntp.org, Nagios: www.nagios.org
  - Postfix: www.postfix.org, Sendmail: www.sendmail.org
  - Für alles Andere: www.freshmeat.net
  - BSI, „Bundesamt für Sicherheit in der Informationstechnik“: www.bsi.de
- Helmar Gerloni, Barbara Oberhaitzinger, Helmut Reiser, Jürgen Plate: Praxisbuch „**Sicherheit für Linux-Server und Netze“**, Hanser Fachbuchverlag 2004

Das wärs für heute...

- Fragen / Diskussion
- Verbesserungsvorschläge
- Die Folien sind bereits auf die Web-Seite der Vorlesung:

  http://www.nm.ifi.lmu.de

- 16. Juni. 2005: e-Service Areas Teil 2, LMU Hauptgebäude HS 317!
  - DNS, E-Mail, NTP, Web-Portal
  - Schwerpunkt: RZ-Infrastrukturen, Ausfallsicherheit, Hochverfügbarkeit
  - Management der Lösung und Kostenbestandteile

- Einen schönen Abend !!!