
hp
invent

Deploying Secure Business Portals

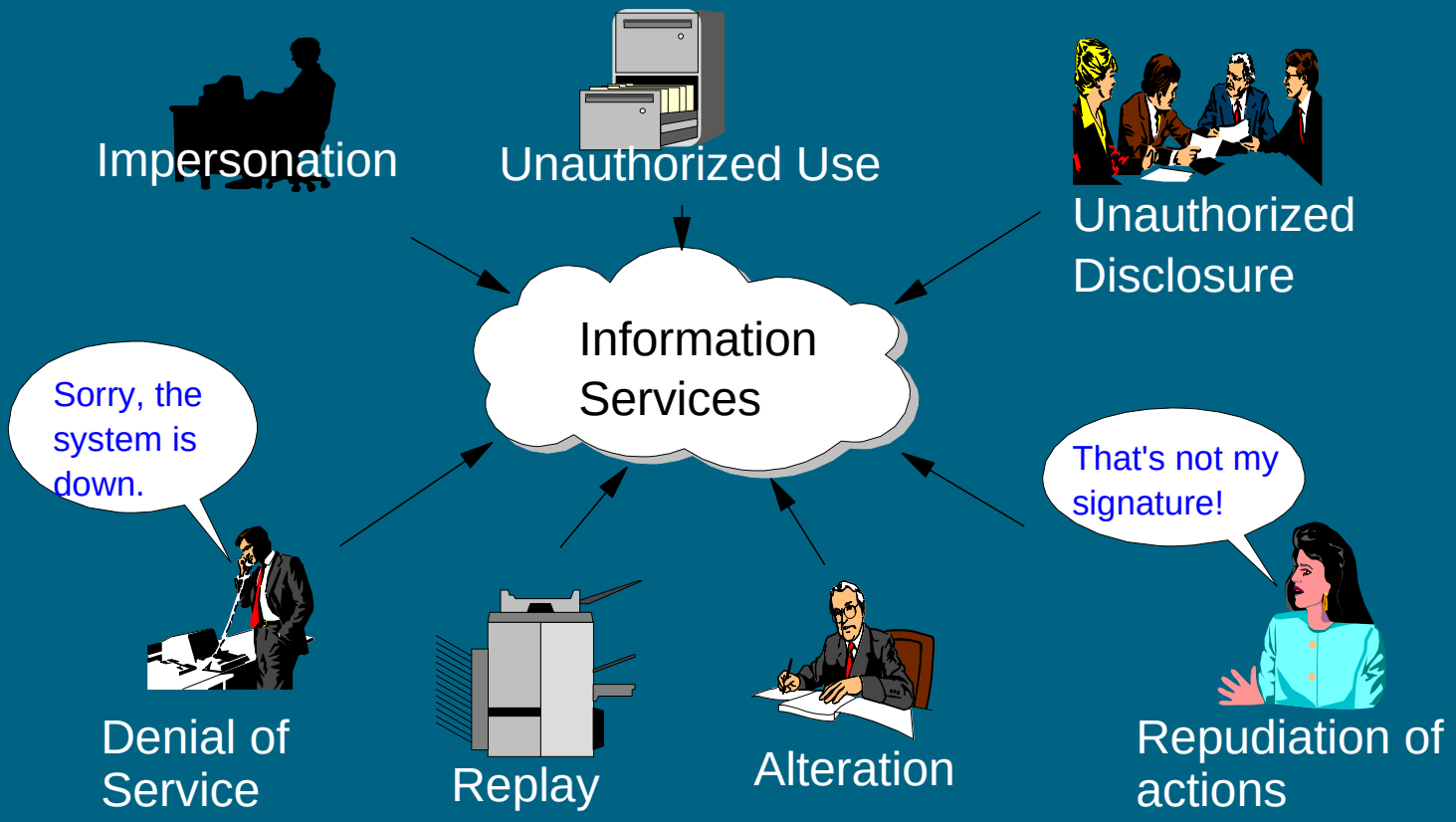
Daniel Dorr
Hewlett Packard
September, 2000

HP World

Agenda

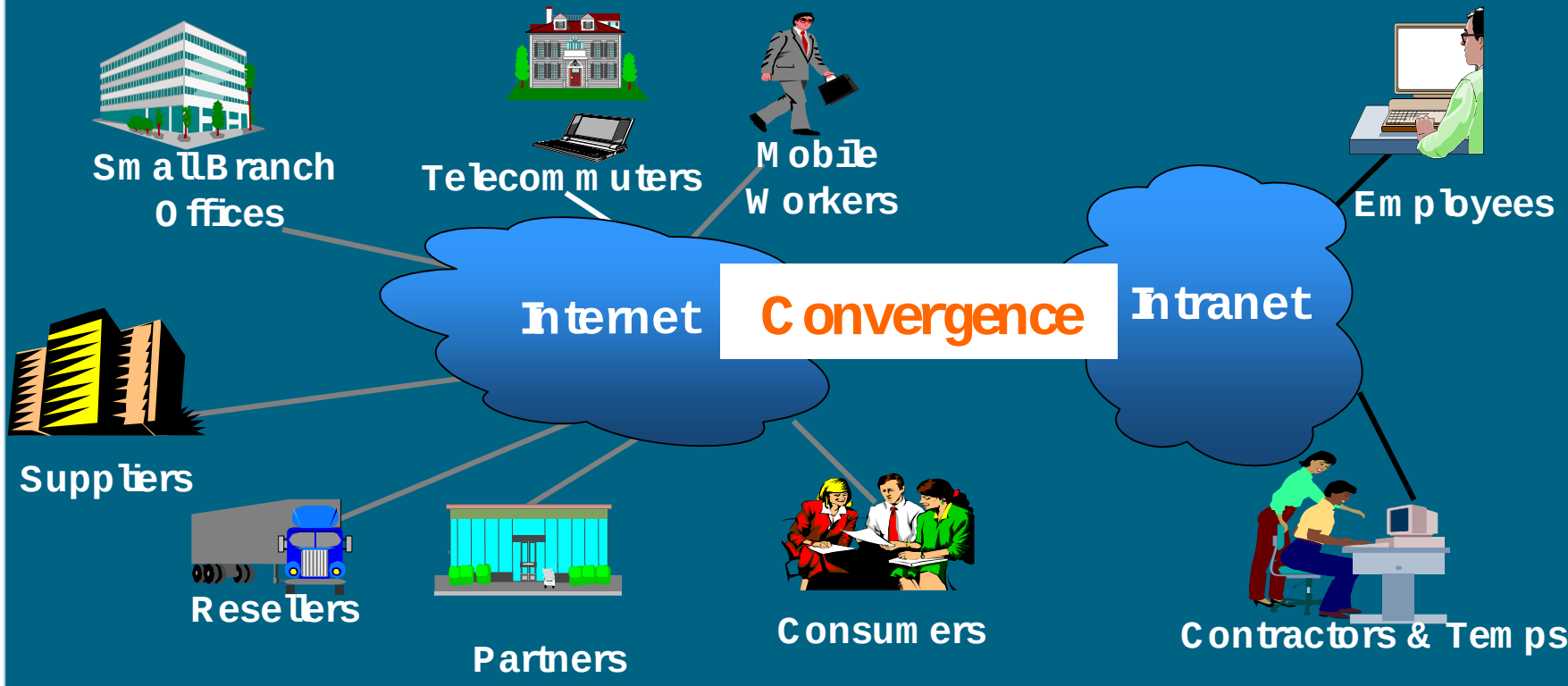
- Market Issues
- Organizational issues
- Technology deployed today
  - Typical architectures
  - Authentication
  - Authorization and Access Control
  - Separation and Containment
- Customer examples
- Visions of future

Increasing Security Threats



Systems Converge

The New World of E-Services



Fact: **Internal and external network converge.**

Question: **Where does the Internal network end and the external network starts?**

Economic Drivers for Business Portals

The Impact on IT Investments

- Success in the information economy will depend on a company's ability to build, maintain, and leverage business relationships using network technology
- Companies with superior network infrastructure will have a distinct competitive advantage

Source: The Burton Group

How do organization's deploy extranet applications?

Typically driven by line of business

- Competitive pressure
- New business opportunities

Clear objectives

- Technical expectations
- Business expectations

Some companies move at corporate level

- Organization depends on Internet presence

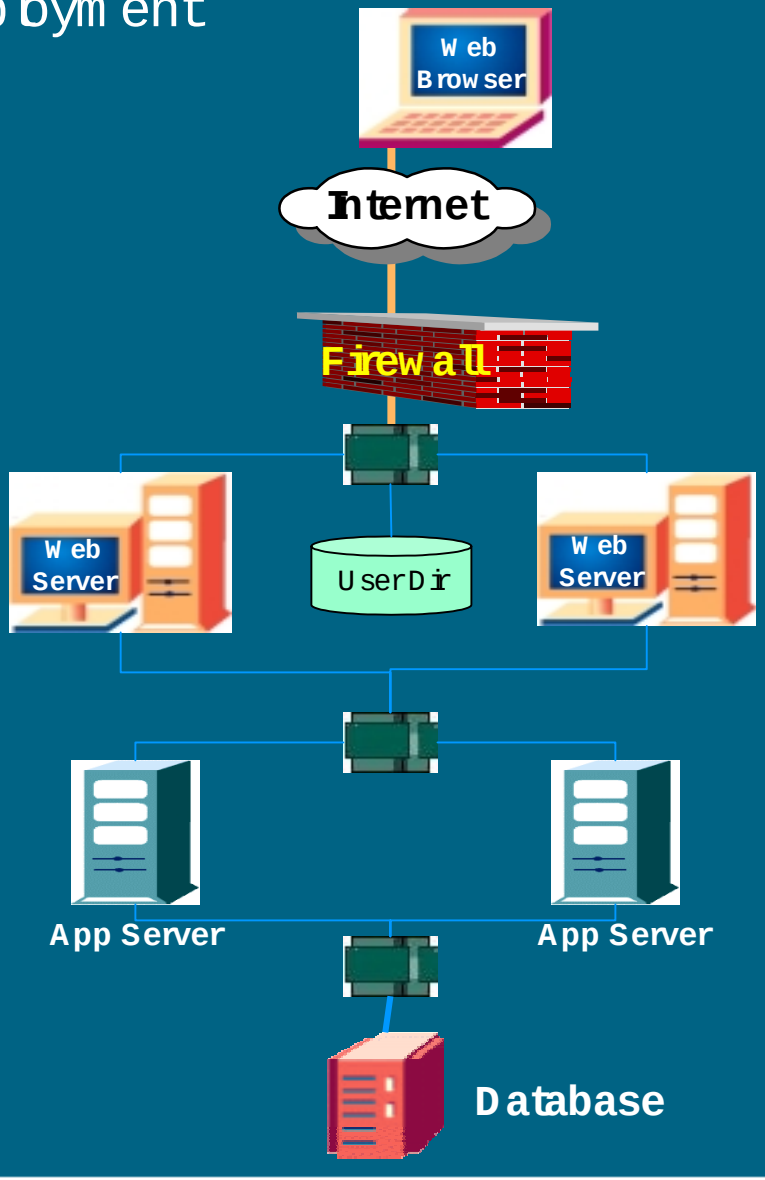
FYI: Security now considered at design!

- Previously an after-thought
- Strong sign of need for security

Typical Architecture

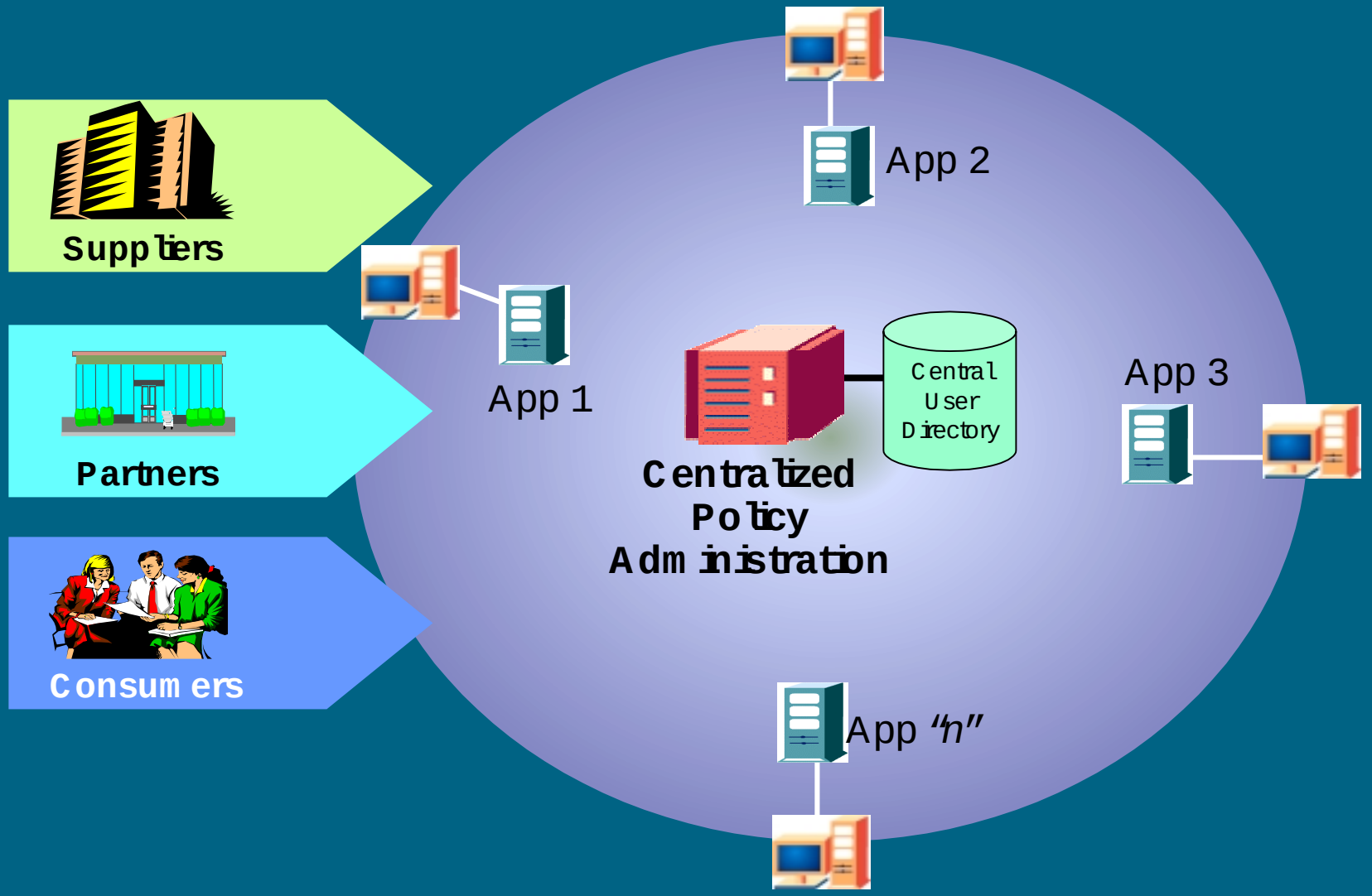
LOB Deployment

- Objective:
  - Allow partners/suppliers/ customers access to specific business functions
- Usage:
  - User authenticates with userID and password
  - User sees personalized web page with list of applications he/she has access to
  - Access only allowed to authorized info
  - User only authenticates once
  - User can view business information, order supplies, check pricing and payment status for authorized only



Typical Architecture

Organization Deployment



Typical Customer Requirements

- Secure
  - Ensure identity of user (Authentication)
  - Strong boundary presence (Separation and Containment)
  - Access control to static and dynamic content (Access control and Authorization)
  - Privacy of information (Encryption)
- Easy to deploy and manage
  - No need to custom code security
  - Delegate administration of users and access rights to partners
- Enterprise level scalability
  - Scalable to thousands of users now and 1M+ users in near future
  - Available 24 hours a day 7 days a week
- Simple end-user experience
  - Users only authenticate once
  - Personalized Web page for users once they authenticate

Authentication
Definition

Purpose:

- Determines who you are. (Proof of identity)
- For people, systems, processes, routers, printers...

Usage:

- User authentication (e.g. desktop login)
- Client-Server authentication (e.g. browser - webserver)
- Data origin authentication (e.g. email)

Mechanisms:

- What you know (passwords)
- What you have (tokens, SmartCards, certificates)
- Who you are (finger print, retinal scan, DNA)

Authentication
Requirements

Driven by applications

- Order status systems might use Id/Password
- Contracts and high value transaction focus on PKI
  - Financial services good example
  - Stronger authentication
  - Sign transactions

Organization need solutions that support major offerings

- PKI
  - Large number of users, high value transactions
- Tokens
  - Small number of users, need for high security
- UserID/Passwords
  - Most common deployment

Certificate Authority & PKI

Details

Certification Authority:

- Trusted 3rd Party that vouches identity of user/entity.
- CA maintains a database (LDAP directory) of user's distinguished names and certificates.
- Examples: Verisign, Netscape, Microsoft...

Public Key Infrastructure (PKI):

- Provides key management services, which includes
  - Key generation and registration.
  - Key escrow and recovery.
  - Key expiration and revocation.
- Examples: Baltimore/CyberTrust, Entrust...

Access Control & Authorization

Definition

Purpose:

- Determines what you are allowed to do.
- Typically based on who are (user, group, role, domain)

Usage:

- Access control to networks, hosts/ports, web-pages, files
- Authorization to use applications, functions and transactions

Mechanisms:

- Access Control Lists
- Capability Lists (privilege-list), Security Labels
- Business Access Rules
- Time-of-day, Duration of access

Access Control & Authorization

Requirements

- Centralize authorization management
  - Single point to manage all users access rights
  - Security can set organizational policy for user management
- Delegate user administration out to partners and customers
  - One organization can't manage millions of users
  - Transfer liability and ownership back to partners
  - Ensures those with most knowledge make decisions

Separation & Containment

Definition

Purpose:

- Protects a private network from public network
- Prevents unauthorized users from accessing sensitive data

Usage:

- Firewalls for boundary systems
- Secure gateways
- Single choke-point for access control

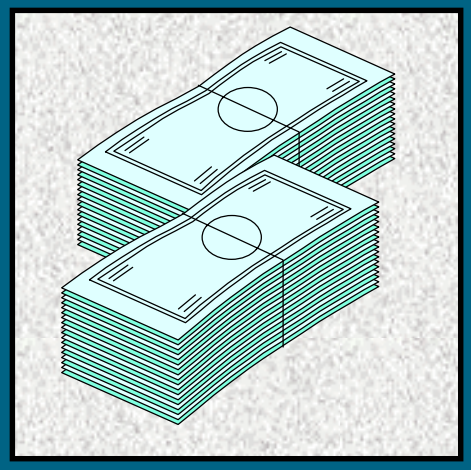
Mechanisms:

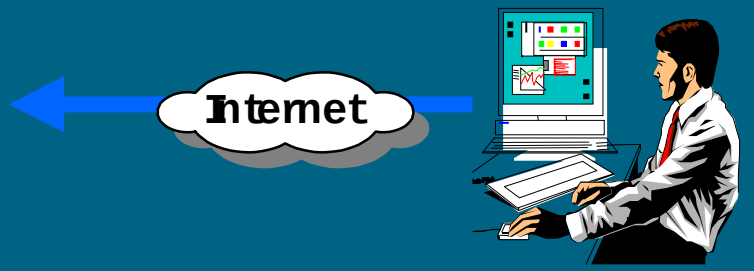
- Application-level proxies to permit/deny requests.
- Generic SOCKS proxy.
- Trusted OS: Compartments (labels), no "super-user" privilege

Separation & Containment

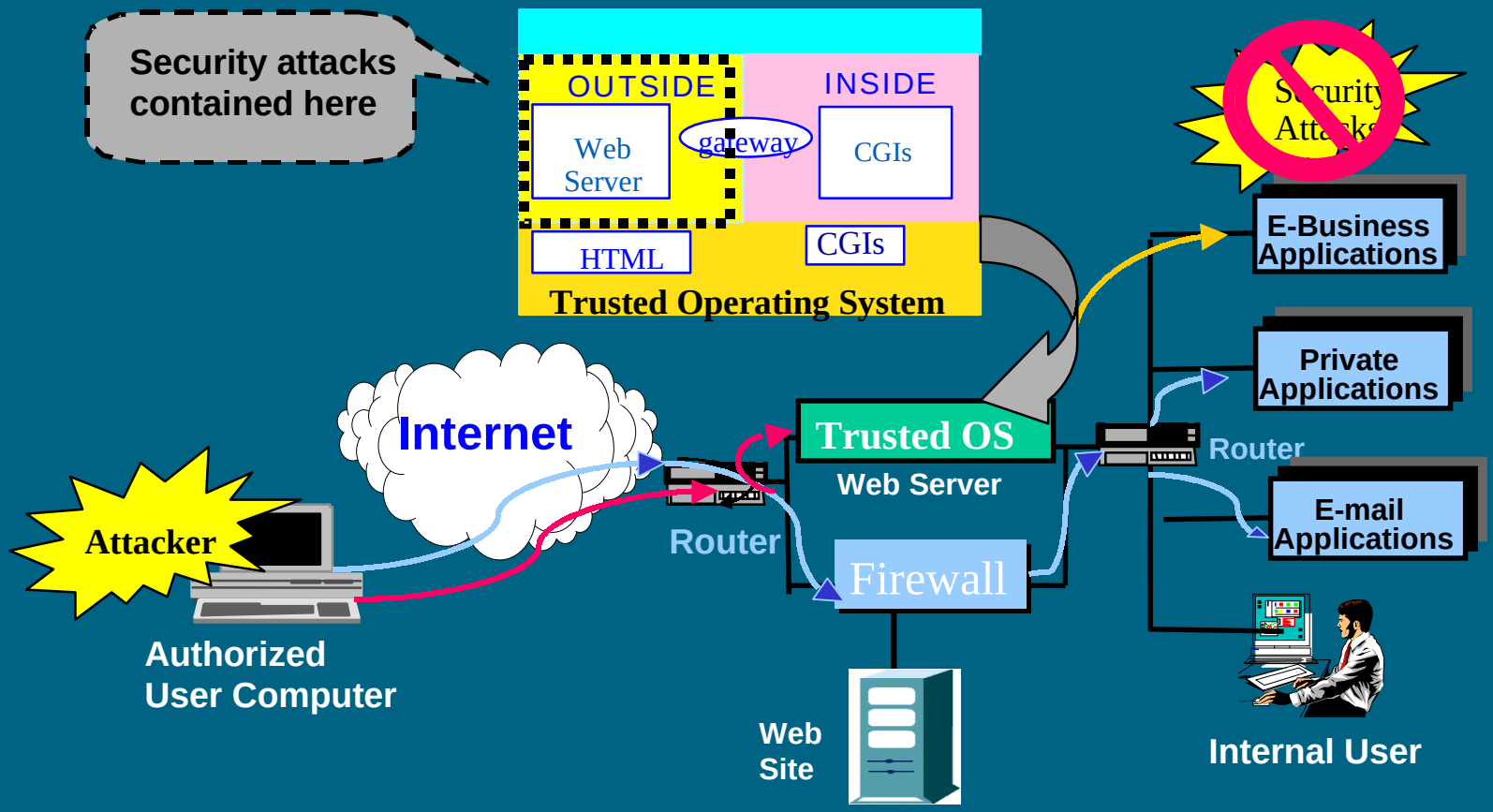
Requirements

- Secure valuable data and applications
  - Ensure users don't have direct access to application
  - Ensure outside systems cannot easily be compromised
- Provide guaranteed access
  - Protect against denial of service attacks
  - Prioritize users based on activities and value





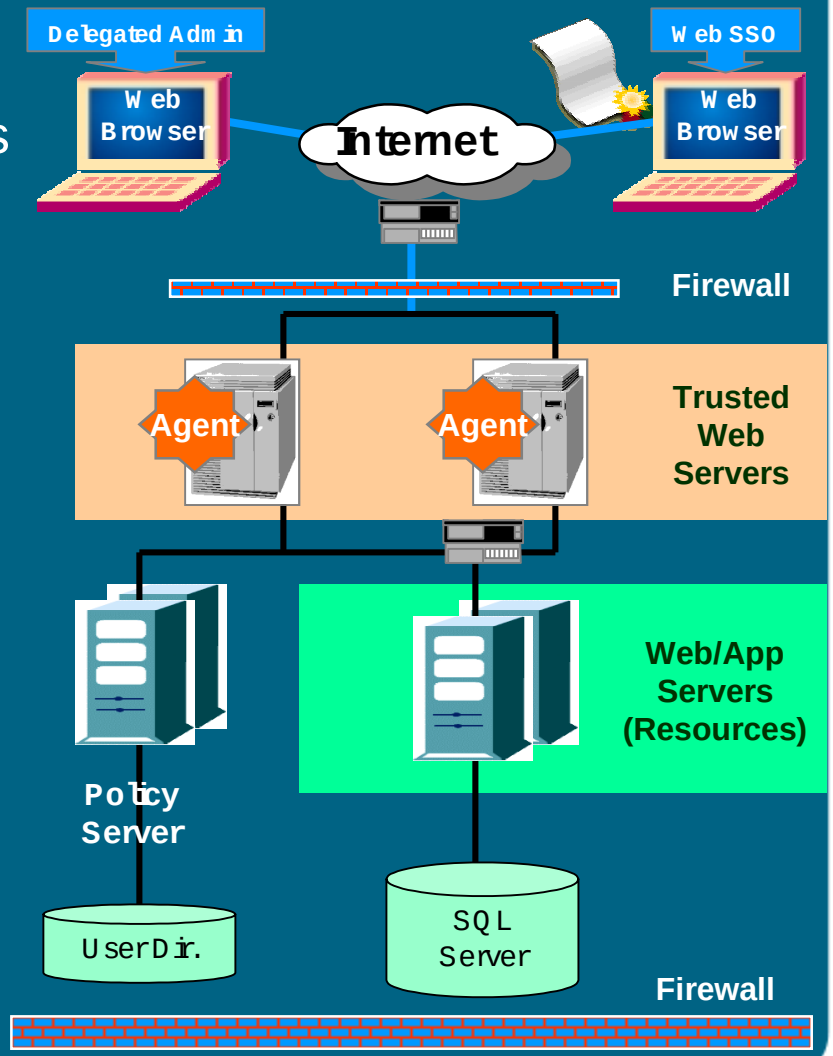
Firewalls Vs. Trusted Platforms



Example Scenario

Financial Services

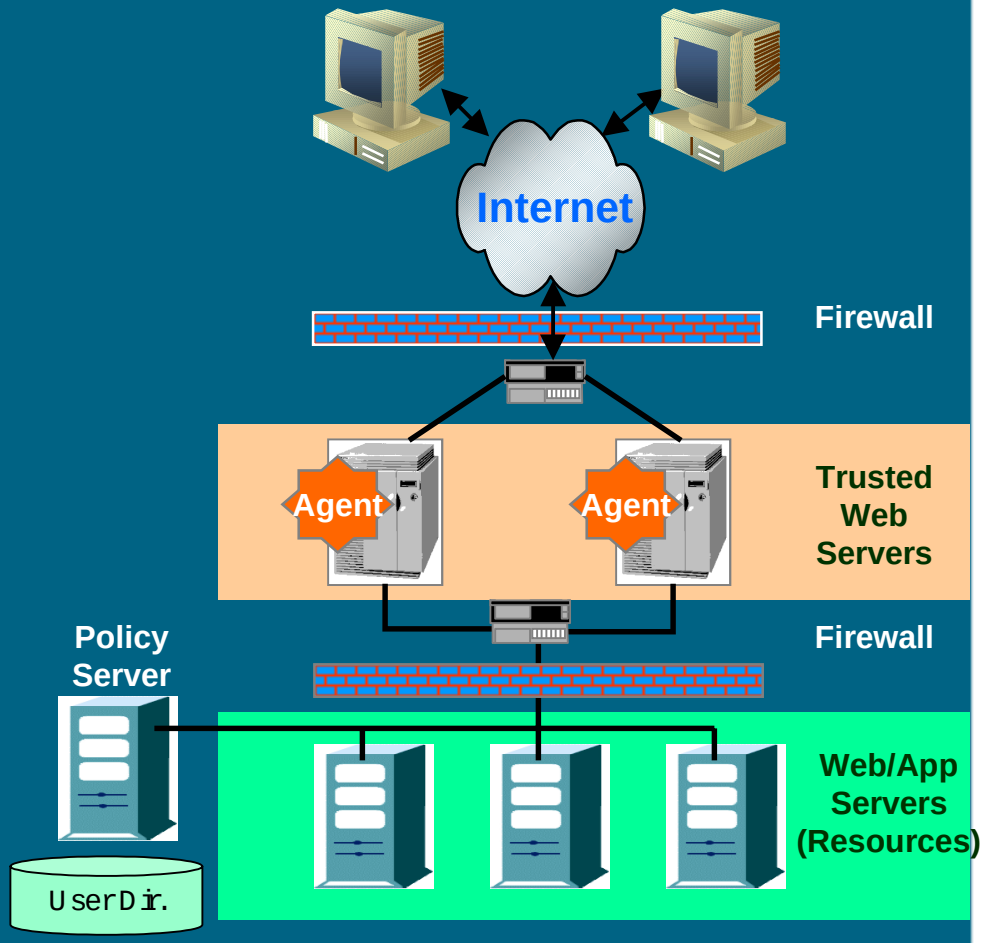
- Objective:
  - Allow commercial credit card holders to access account information and customer service applications
- Secure Solution Provides:
  - Credit card company to sign up account manager through user management
  - Delegates user profile management to customer
  - Authenticates user with digital certificate
  - Access control within applications through APIs
  - Present user with list of where he/she has access
  - Web SSO



Example Scenario

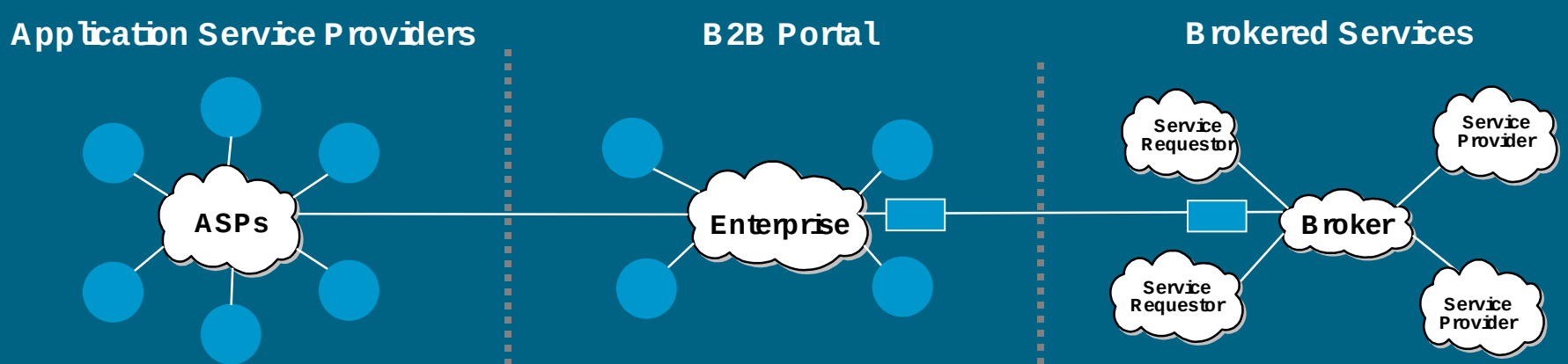
ASP Applications on Tap

- **Objective:**
  - Allow users access to Web and non-Web applications and charge by application usage
- Secure Solution Provides:
  - Customer can add new users
  - Authenticates user with userID/password, certificate or token
  - Provide access control to application frontend
  - Present user with list of access
  - Provides web SSO
  - Non-web access through VPN



Evolution to E-Services

Moving from B2B to E-Services



Solution Categories:

- Boundary protection
- Trusted Web Servers
- Web Access Management
- Brokered Services
- Quality of Service
- Performance

Security solutions for enterprises, ASPs, and brokered services

Summary

- Market Issues
  - Organizations need to be able to leverage the web to offer new services and attack new business opportunities
  - An organization's infrastructure is quickly becoming a competitive factor
- Organizational issues
  - Tactical (LOB) vs. Strategic (Company) deployments
- Technology deployed today
  - Focus on open standards
  - Prepare for change and growth (Don't get locked in)
  - Deployments depend on application, trust and level of integration

Thank You

Daniel Dorr
Hewlett Packard
Internet Security Division
www.hp.com/security

Questions?