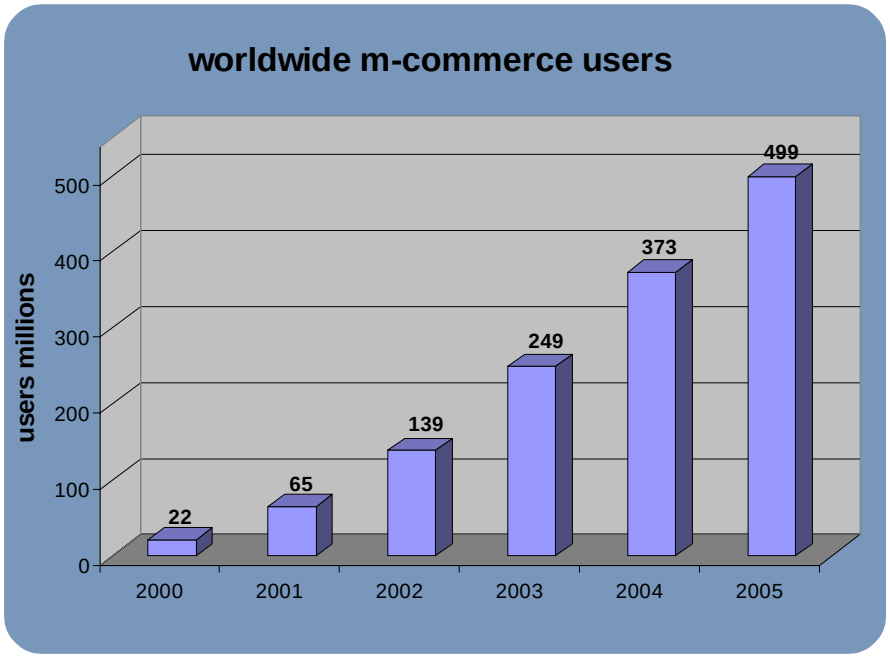
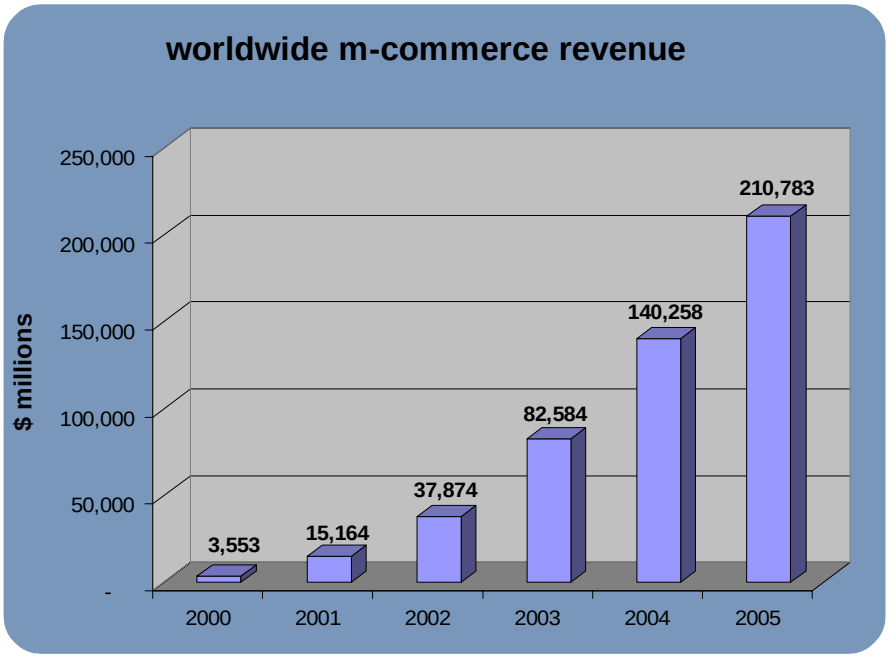
Protecting your Mobile Infrastructure

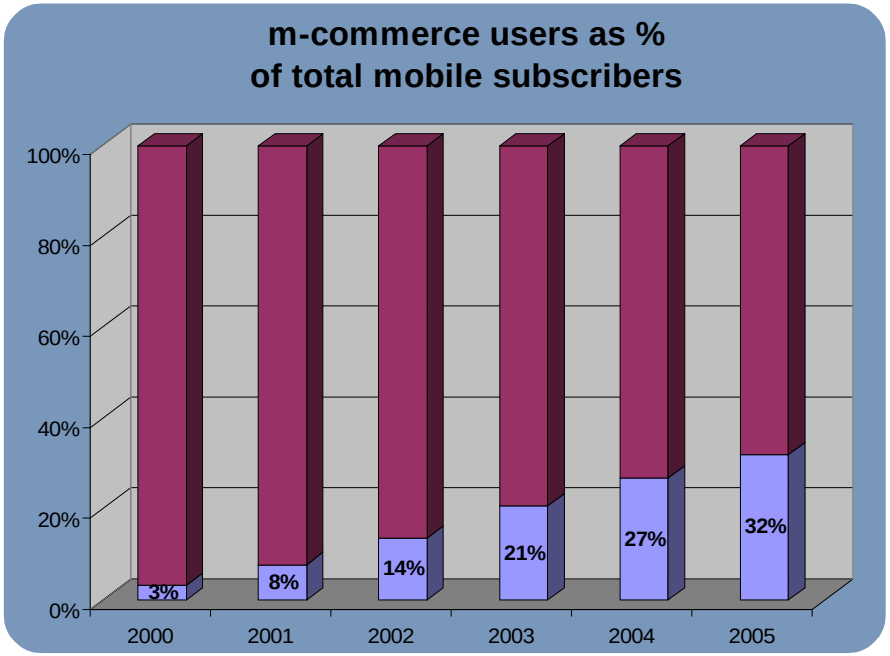
Daniel Dorr

Hewlett Packard

Internet Security Division





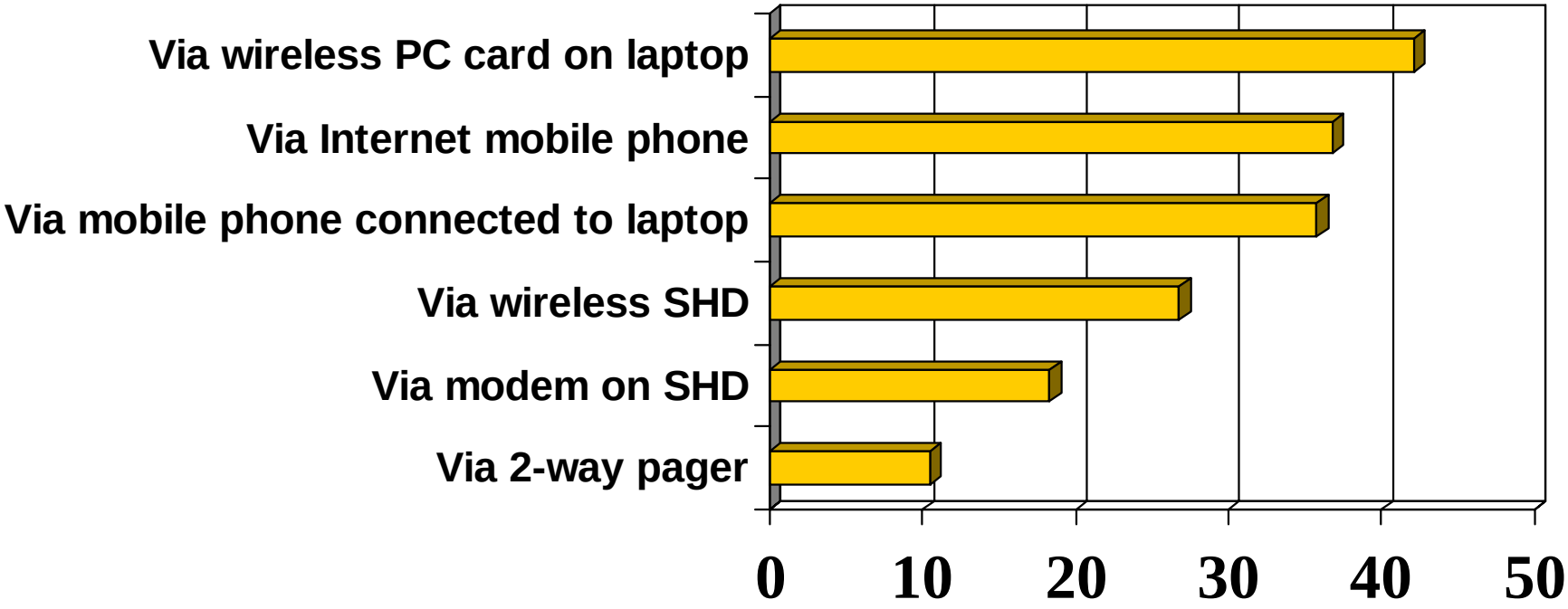


by the year 2003 there will be 250 million m-commerce users, accounting for 21% of the total worldwide mobile subscribers, generating $83 billion in m-commerce revenues

source: ovum

Mobile Market Trends

How do users access the mobile Internet?

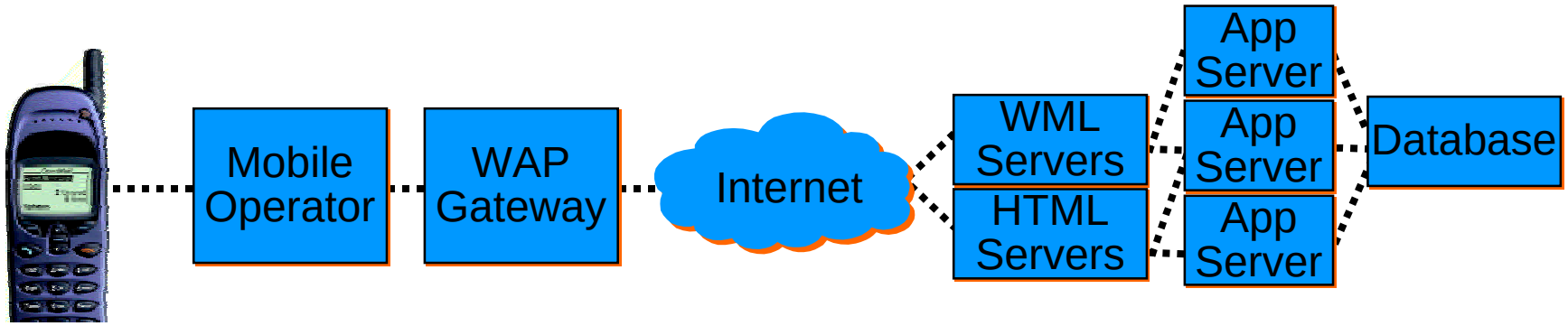


Source: IDC 2000

Security Issues With WAP

- Encryption/Data protection
  - Transactions are in clear text on WAP gateway
- Authentication
  - Phones are easy to lose/steal
  - Input difficult for complex names and passwords
  - Difficult interface for multi-form authentication

Wireless Application Protocol

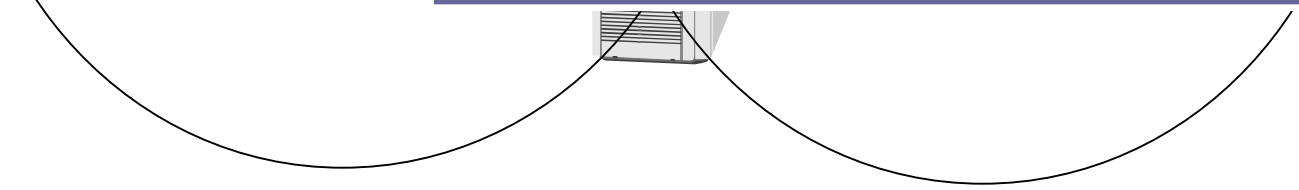


- **WAP is an end-to-end application protocol that:**
  - Allows mobile terminals to communicate with server applications
  - Guarantees interoperability among different terminals and servers
  - Implements end-to-end security between WAP client and WAP gateway

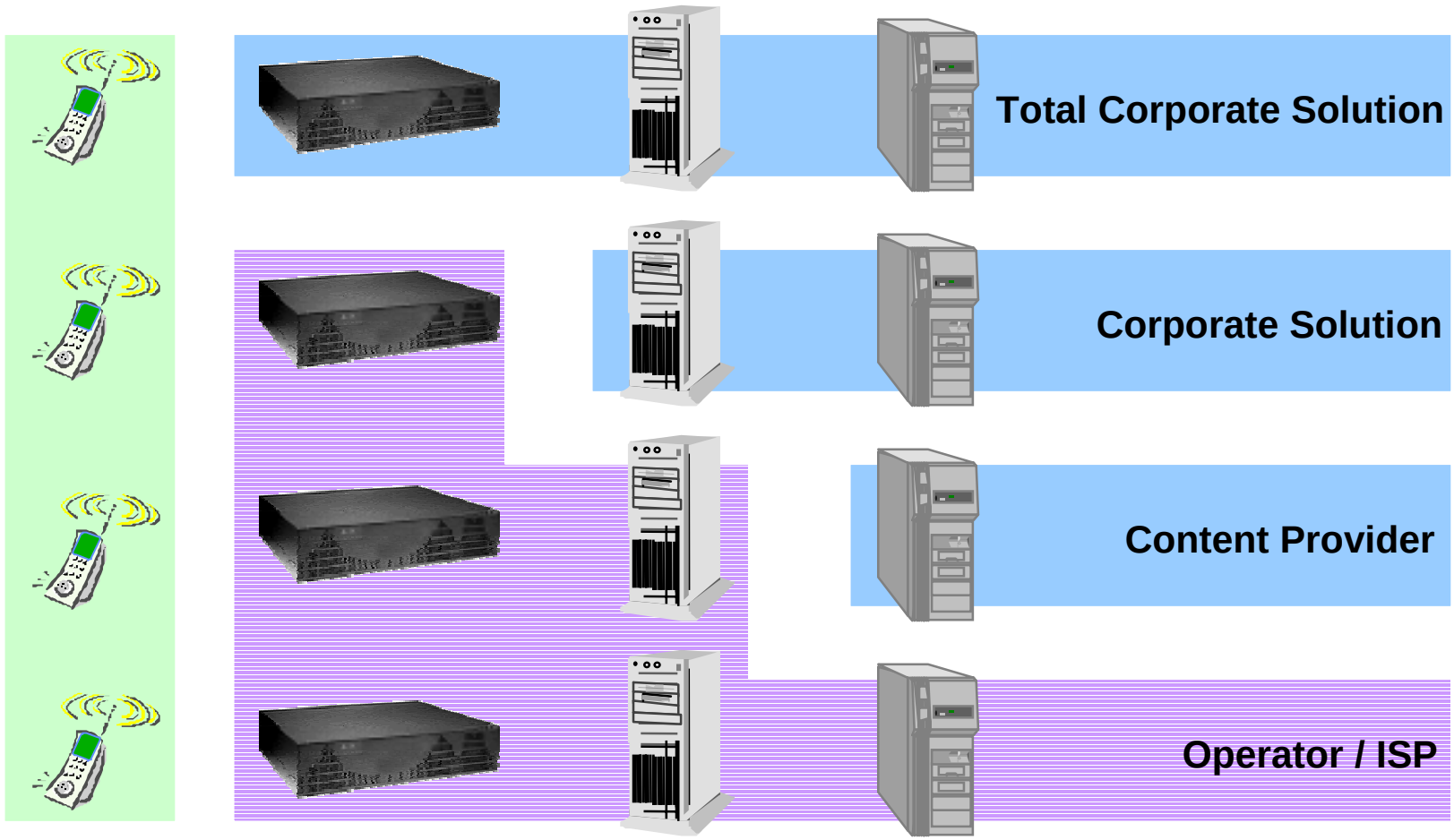
WAP Application Environment

- WAP Gateway allows a WAE user agent (eg. a browser) navigate internet/intranet content
- Acts as a proxy to an origin server
- Runs WAP over wireless bearers, both connection-mode (e.g. CSD)

- Origin servers provide application services and content
- Content can be static or dynamic:
  - HTTP servers can act as origin servers
  - Applications can generate and serve content directly

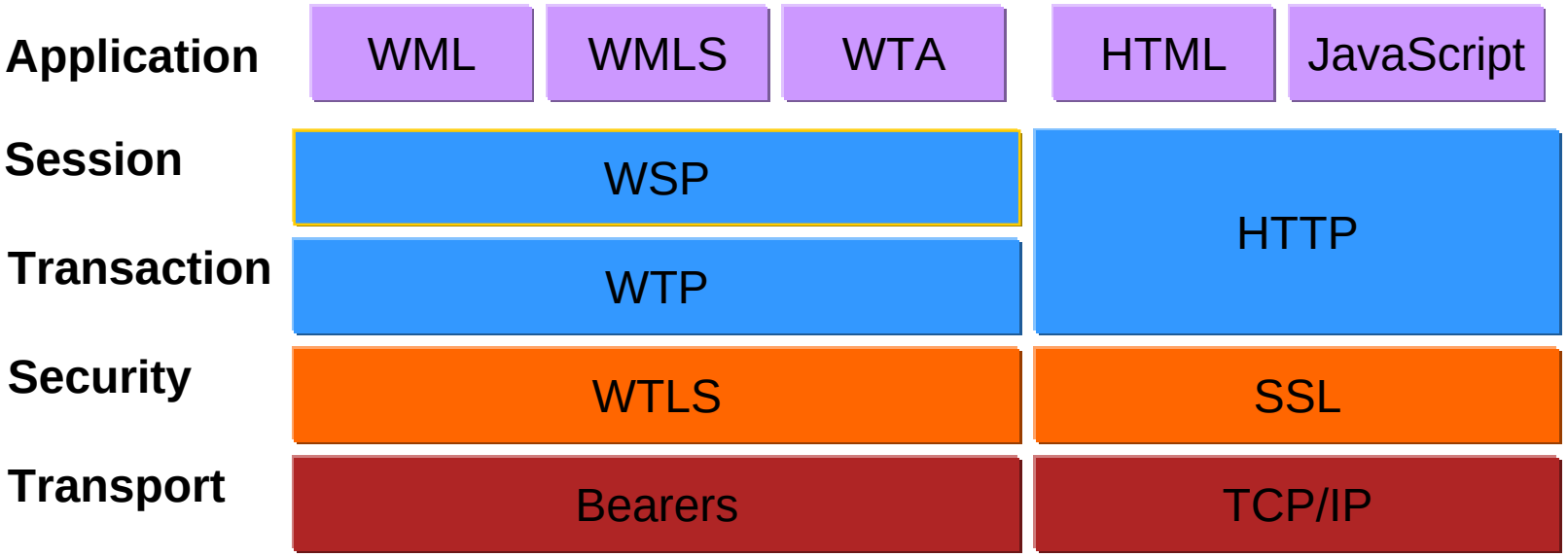


WAP deployment scenarios



WAP vs. Web

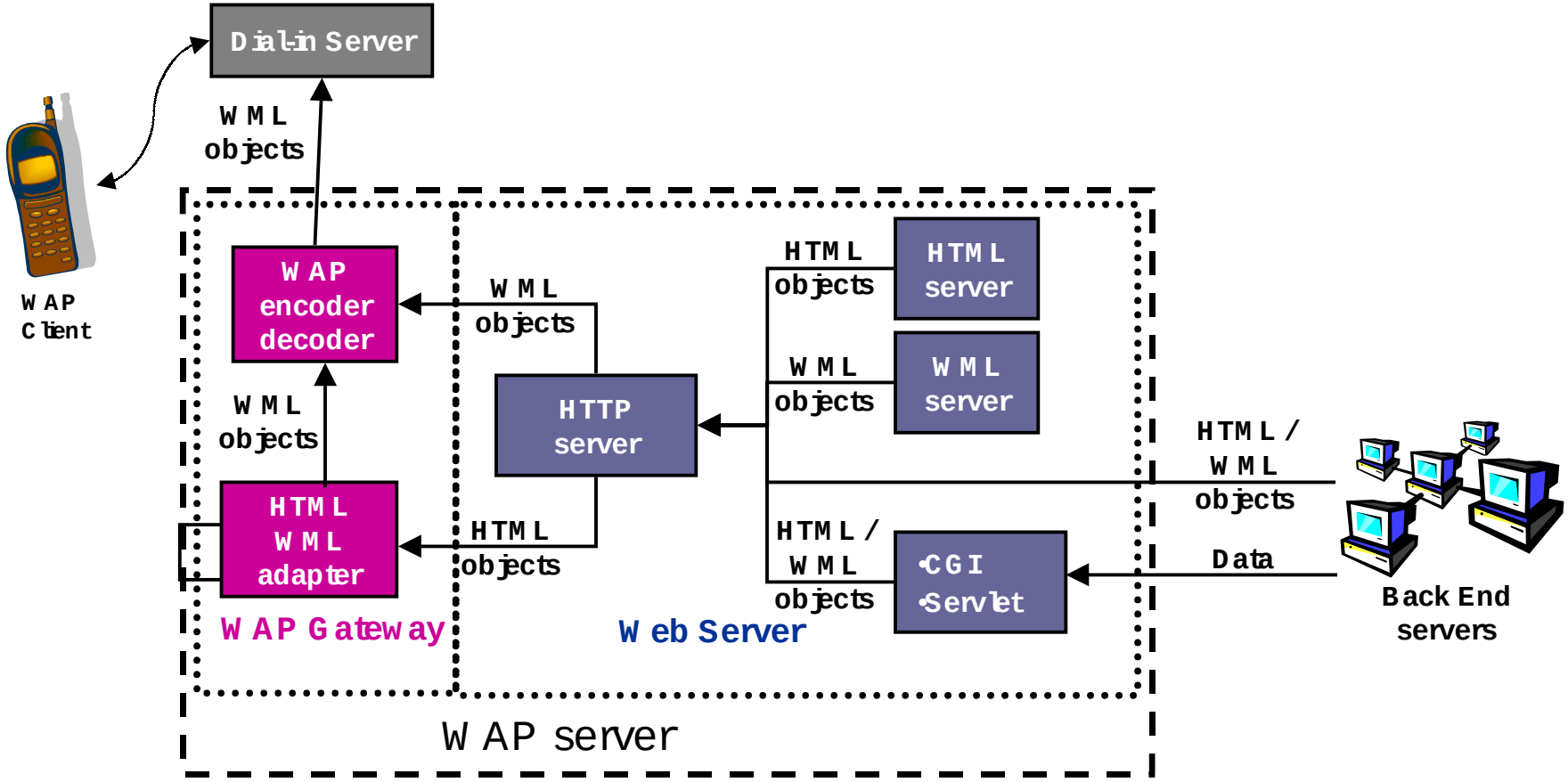
- Technologically WAP is a sibling to WWW
- Both environments are based on browsing concept, i.e. the client requests and loads documents from server
- Similar features are presented in the following table:



Wireless Transport Layer Security (WTLS)

- Provides connection security between two applications
- Security services:
  - Confidentiality (encryption)
  - Data integrity (hash, HMAC)
  - Authentication (symmetric and public-key)
- Supports both server and client certificates

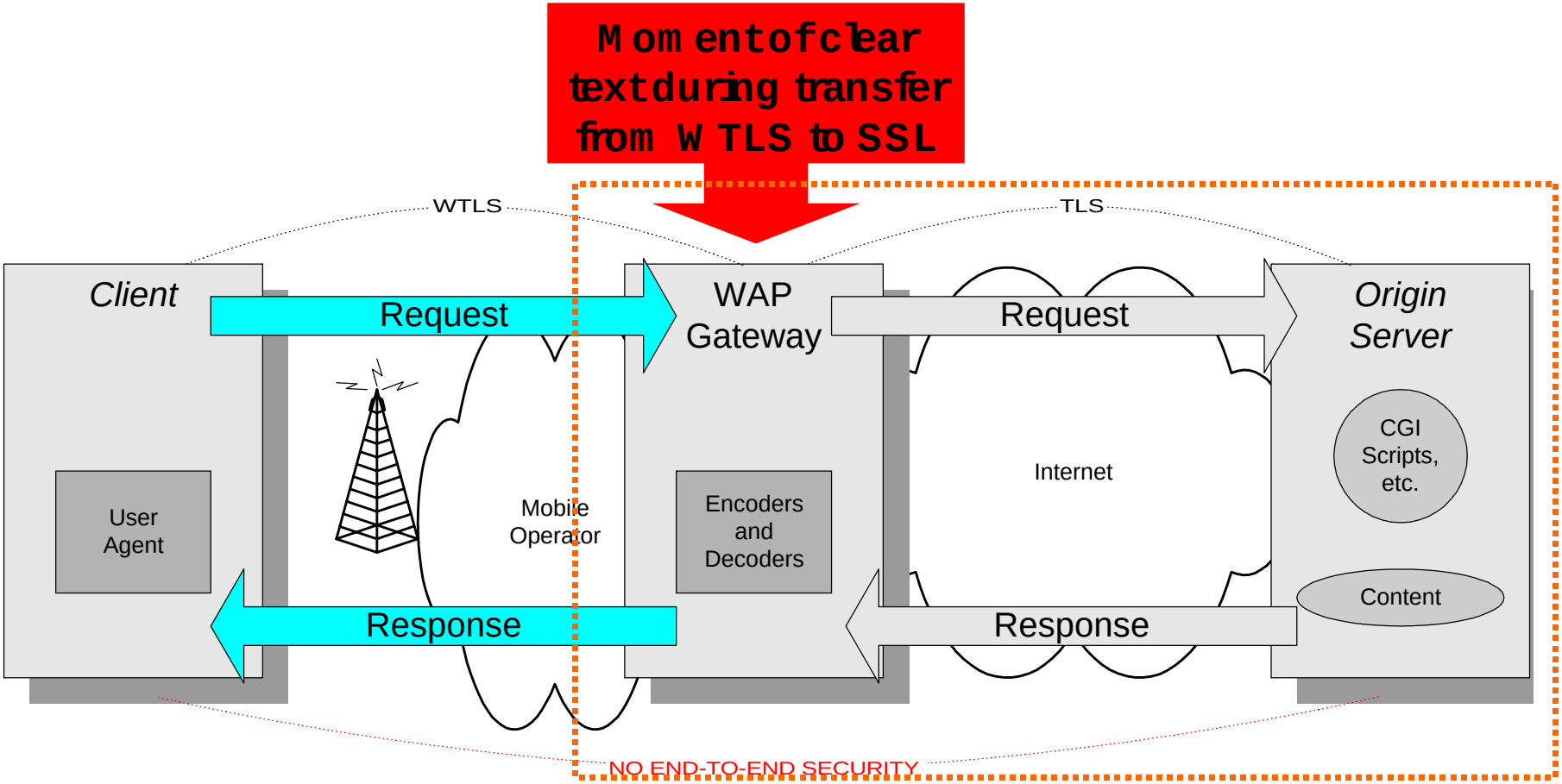
WAP server architecture



- When the WAP gateway and Web server functions are consolidated in one system, it is called WAP server.
- The WAP server needs to be resistant to attacks.

Problems with WAP

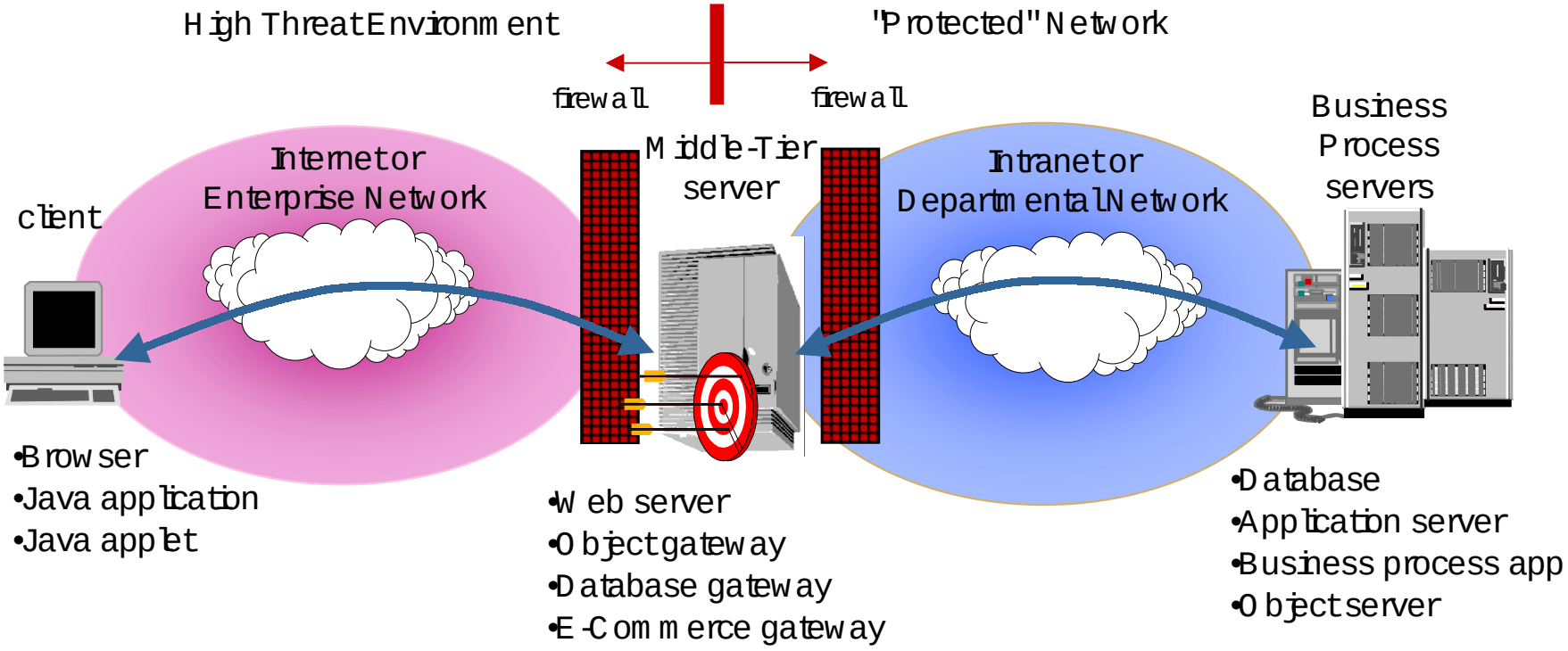
End-to-End Security



Are firewalls good enough defense?

- A firewall is designed to regulate information flow, not to run applications
- The entire software base on the firewall is trusted:
  A firewall is a hardened OS and proxy/filter/scanning code
- Putting application code on the firewall violates its design philosophy (small, verifiable)
- A Trusted Run-time Application Gateway complements firewalls that the organization already has in place

Secure Multi-tier Application Strategy



- The gateway that provides access to critical business resources is the weak link in the security chain
- Immature software is being rushed to market without adequate testing or security review

Challenges to firewalls
Web-enabling applications

- Firewall protects against:
  - packet modification
  - packet insertion
  - packet disclosure
  - IP spoofing
  - attack "inside" machines

- Firewall challenges:
  - getting "root"
  - trojan horses
  - user spoofing
  - access to services/data

- Immature application technologies rushing to the market
  - Developed in "Internet Time"
  - Inadequate security analysis
  - Inadequate penetration testing
  - Security/functionality flaws discovered "live"

HP's Implementation of a Secure Mobile Infrastructure

Secure from the client:

- Wireless PKI
- Soft-tokens (for PDAs)

Secure the boundary

- Secure WAP servers
- Hardened WAP servers
- Secure server for SP environment

Secure the content:

- Authorization and access control
- Secure application server

Source: Ovum

Secure Web Front-ends

Web front-ends on trusted OS

- Provides security framework for middle-tier
- Reduces security risk of front-end
- Transparent to applications
- Provides additional layers of security
  - No all powerful user account
  - Applications, files, network interfaces separated
  - Ability to record system events
- Removes/disables unused services (e.g., Mail server daemon)

Web front-ends on Off-the-shelf operating systems

- Off the shelf Unix & NT do not provide sufficient risk reduction for Web Front-Ends
  - Difficult to configure securely
  - Potentially dangerous services available/enabled by default
  - Insufficient security protection for applications
  - Configuration errors may expose application data
  - Attacks against services running as "root"

Application platform architecture

- Secure boundary system concept
- Protects intranet from Internet
- Forbids traditional Unix "root" attacks
- Uses secure OS features to separate applications
  - Protected network interfaces
  - Process and file separation
- Intranet access mediated by cross-boundary IPC
- "root" capability removed from OS
- Provides comprehensive auditing capabilities
- Includes system integrity checking mechanisms
- Provides status feedback for bad balancing

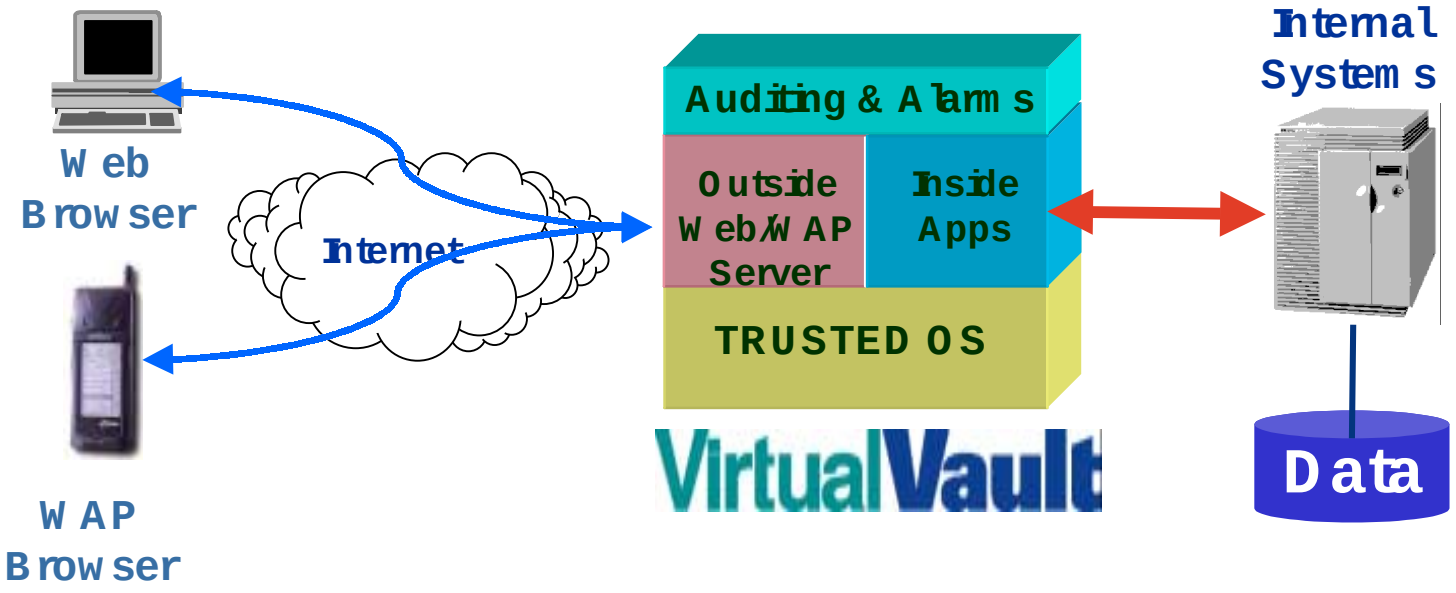
Praesidium VirtualVault

Application protection

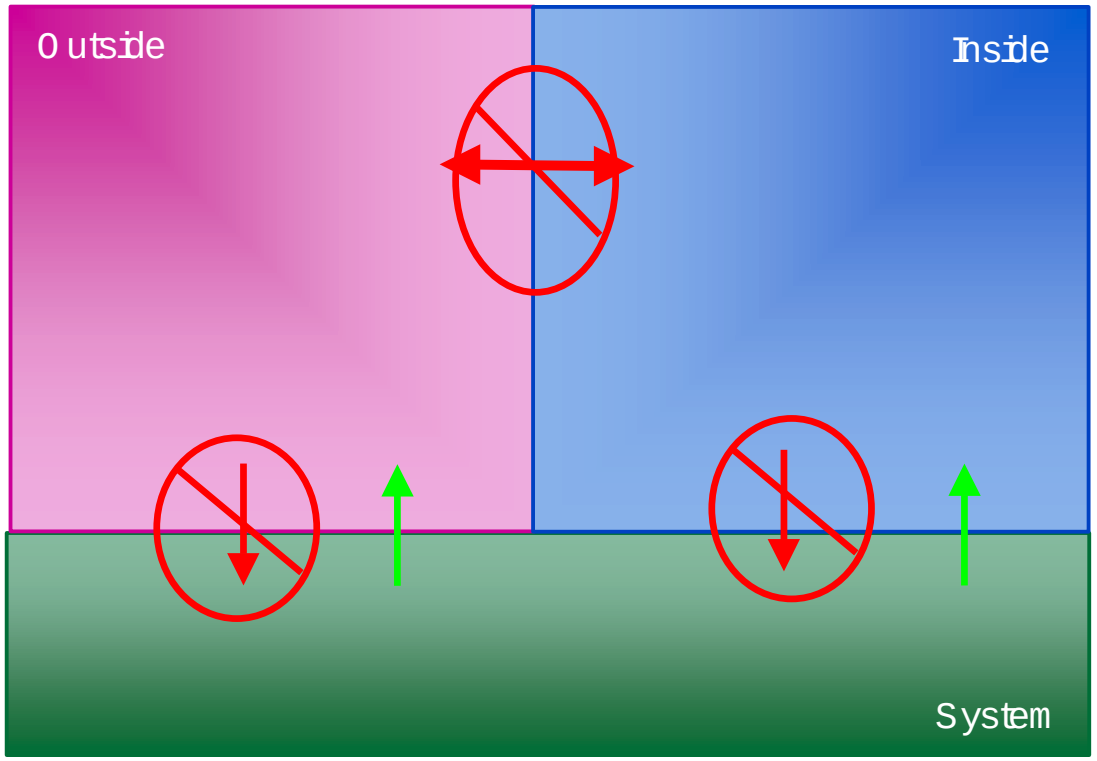
The highest level of boundary security available today

Ensures applications and customer data are not open for attacks over the Internet…

- Secure Web-Server platform
- Users stay on the outside, applications are secure on the inside
- Safe combination of Web, WAP, and Middleware on one box

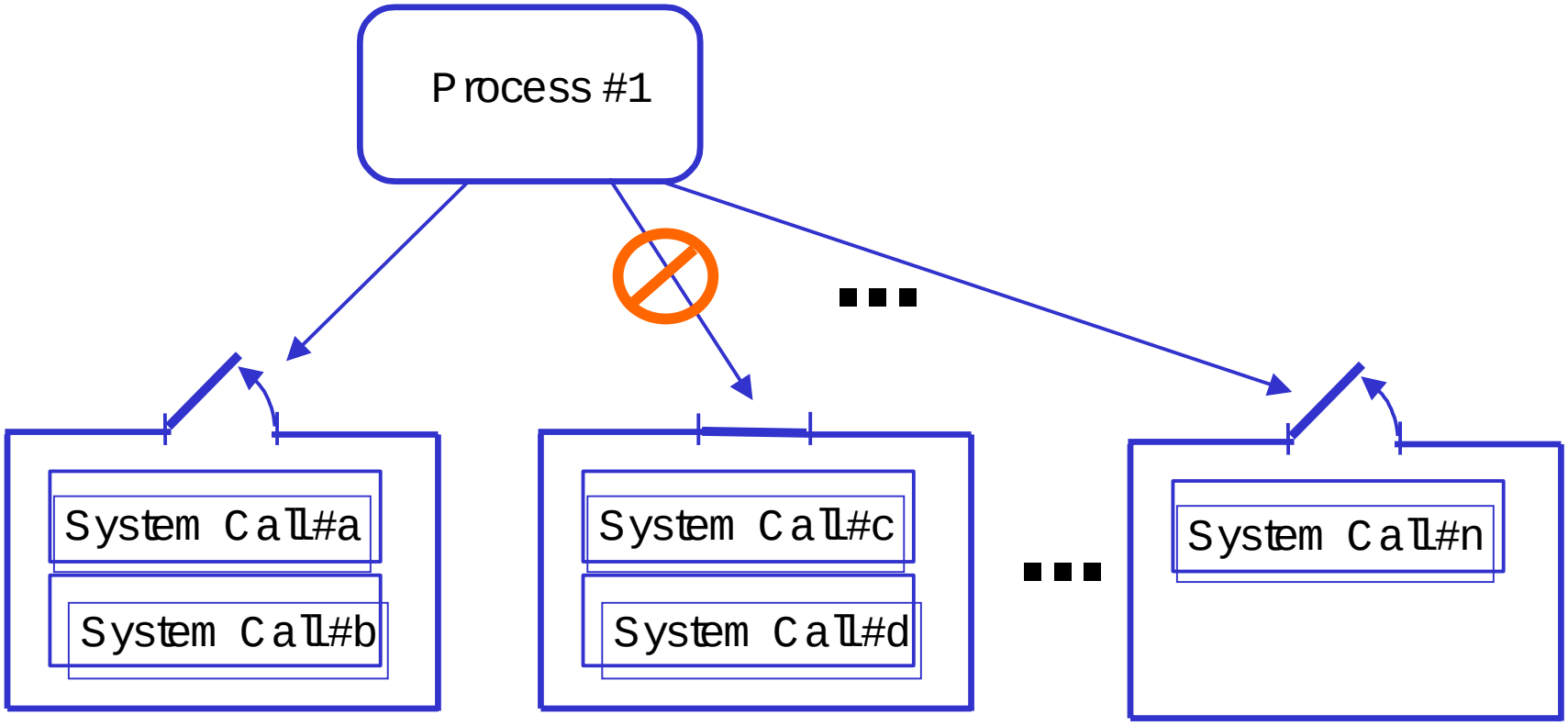


Separation of information



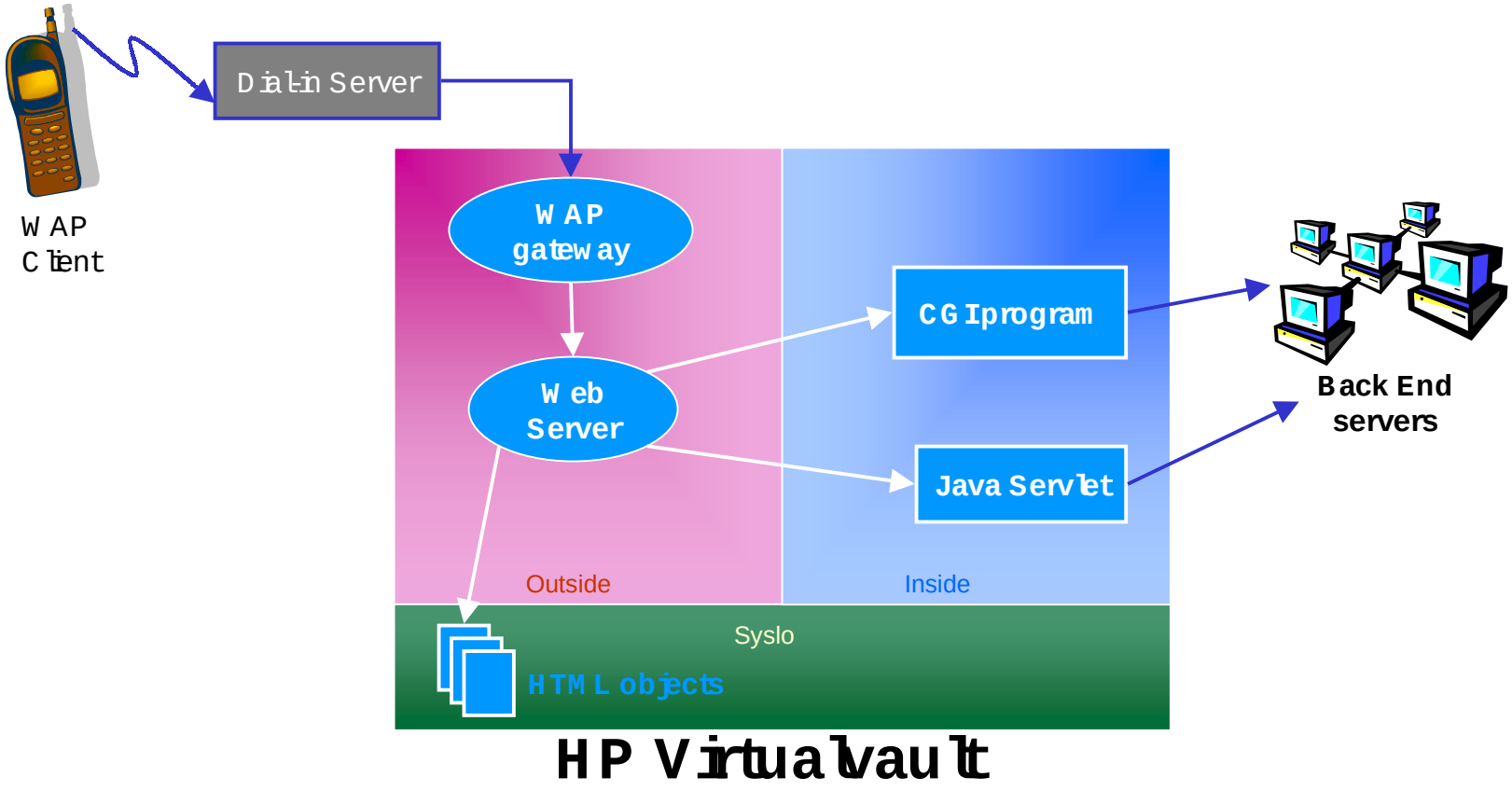
No information flows between Inside and Outside
Both Inside and Outside can read Information at System, but can not write it.

System call restriction



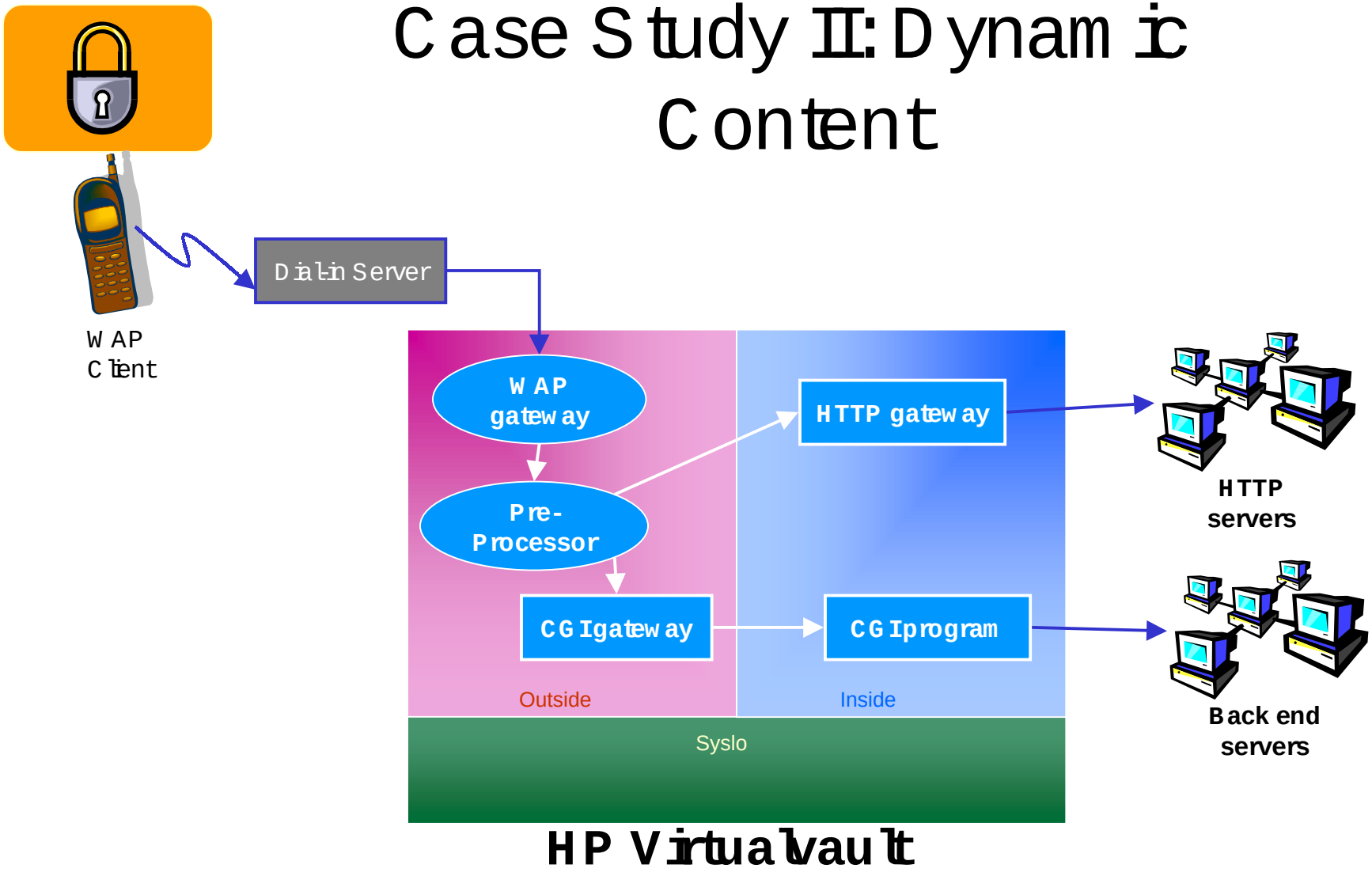
Access from each process to each system call is mediated by system call privileges

Case study I: Secure Mobile Gateway



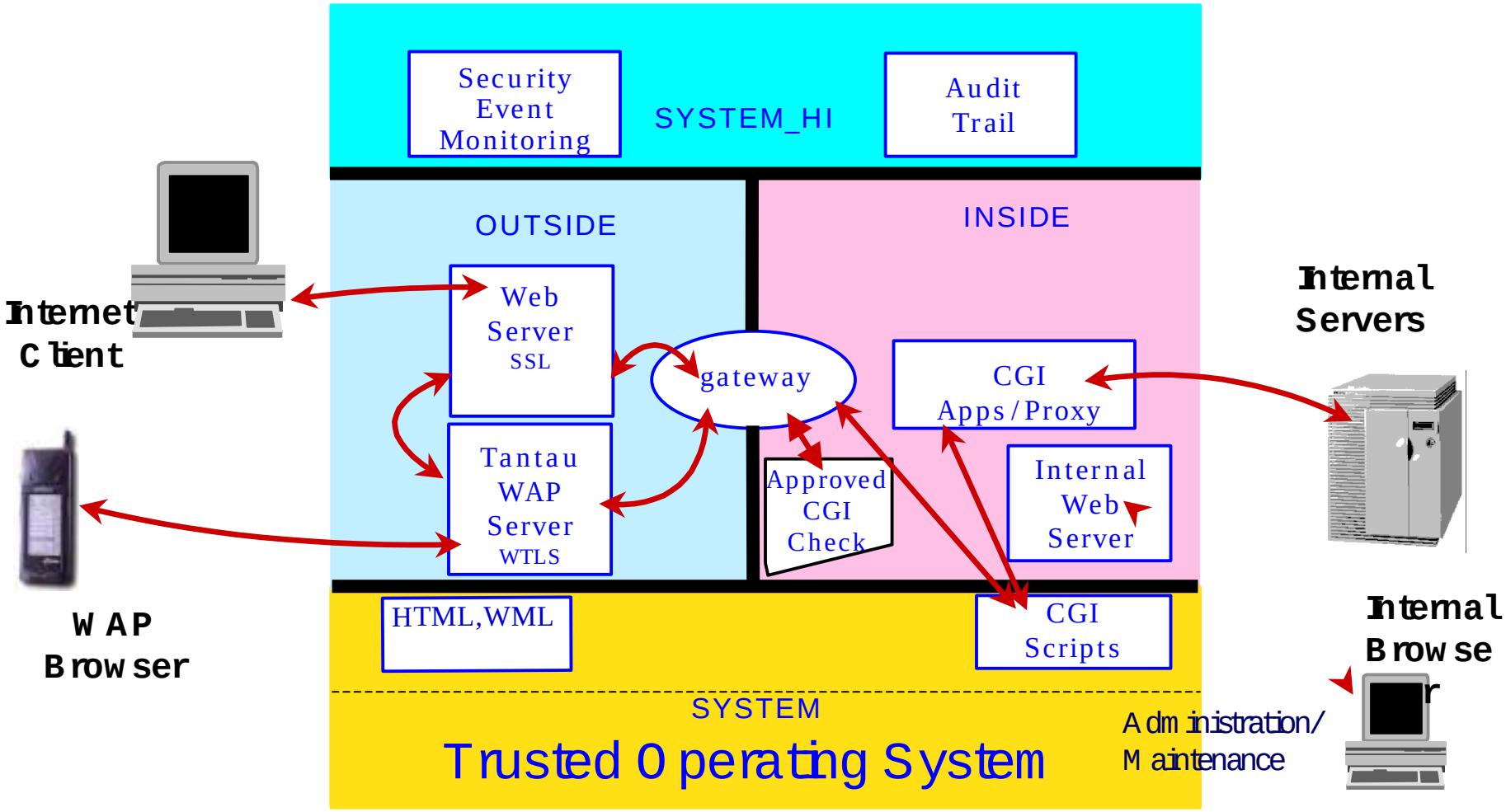
The WAP gateway provides access to an HTTP Web server

Case Study II: Dynamic Content



The WAP gateway requests documents via an HTTP proxy or dynamically generated content via CGI.

Mobile Gateway on Virtualvault



European Bank

Full-Service Internet and Mobile Banking

S-E-Banken

Objectives

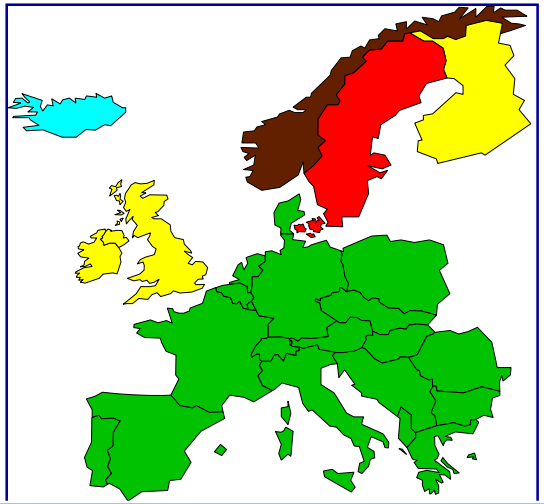
- **High value , 24 x 7 banking services**
- **Strong security**

Solution

- **VirtualVault protects Web and WAP server and Internet banking application**
- **Total integration with core banking systems**

Benefits

- **Secure wireless access to banking application**
- **Safeguards more then 20 banking applications**
- **500,000 customers/700,000 transaction per day**
- **Cost reduction for customers and bank**



"If HP had not been able to offer a secure Internet solution, S-E-Banken would not have even considered launching an Internet service like this at this time." - **Anders Lindqvist, Director Internet Service, S-E-Banken**

New Zealand Stock Exchange

World-leading WAP trading system

Objectives

- **High value , 24 x 7 banking services**
- **Strong security**

Solution

- **VirtualVault protects Web and WAP server and Internet banking application**
- **Total integration with core banking systems**

Benefits

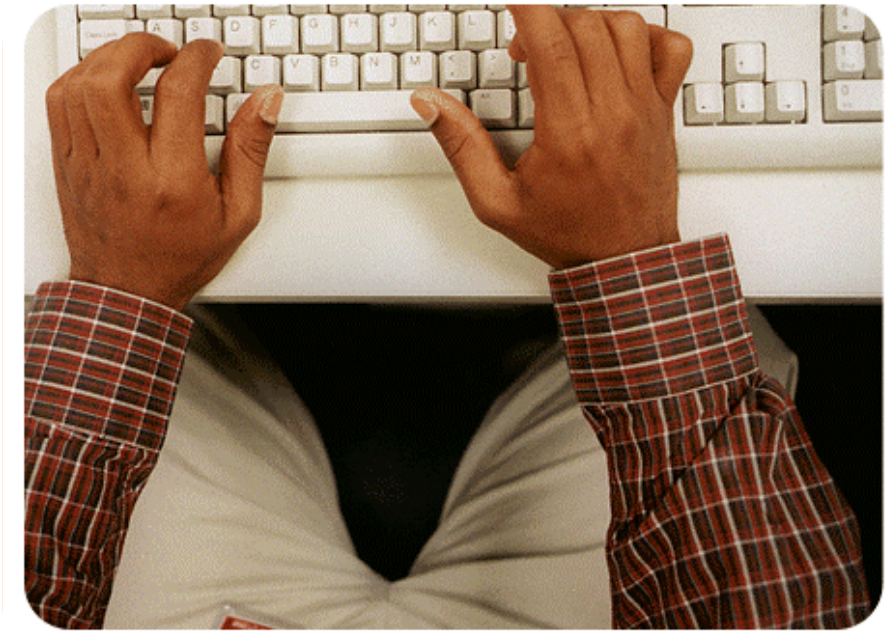
- **Secure wireless access to banking application**
- **Cost reduction for customers and bank**

NZSE
New Zealand
Stock Exchange

"Technology is the key to enabling us to achieve this; we need to use leading edge technology to help create an environment that will enhance our brokers competitiveness in the world market."
Bill Foster, CEO
New Zealand Stock Exchange

Hackers continue to openly share information

toward a secure infrastructure ...



- create an always-on infrastructure that correctly executes business strategy
- e-toolsecurity policies for nextgeneration interactions
- develop worldwide accepted standards and definitions
- share information across the industry

Thank you

DanielDorr

daniel_dorr@hp.com

408-447-4682