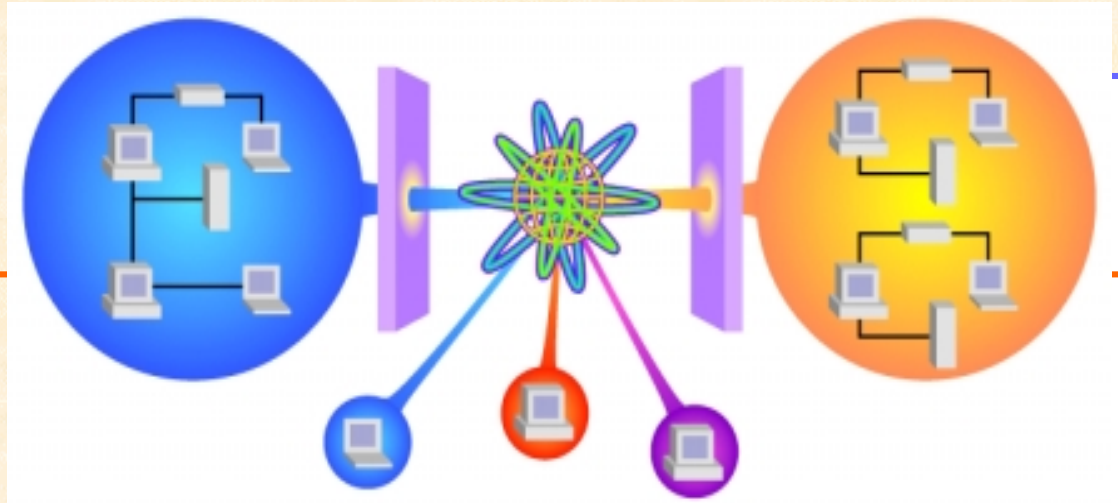
POWERED BY HP...
HPe3000



# Internet Security on Your HP *e*3000


OnOn Hong
Hewlett-Packard Company
19447 Pruneridge Ave., MS 47UE
Cupertino, CA 95014
(408)447-5637
onon_hong@hp.com

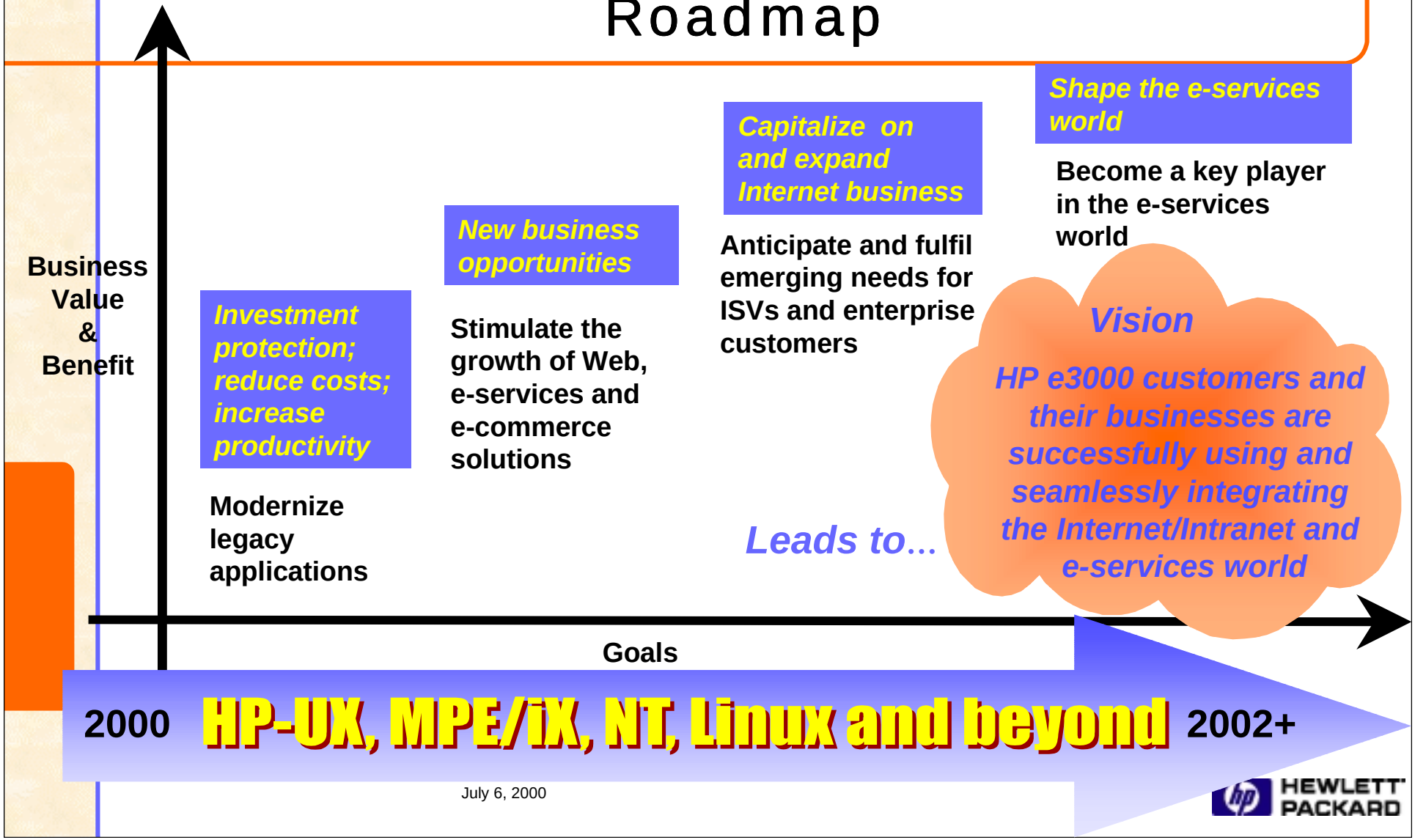



HEWLETT PACKARD

With the advent of the Internet and the creation and rapid success of e-business, security has never been more important

POWERED BY HP...
HP e3000

# HP e3000 Internet & Interoperability Roadmap






HEWLETT PACKARD

# Internet Security Vision

HP e3000 customers and their businesses are successfully using and seamlessly integrating the Internet and the e-services world..... SECURELY, PRIVATELY (IF DESIRED), AND WITH TRUST.

# Common Internet Security Risks

- System Access
  - Unauthorized access
  - Denial of service
- Data privacy, integrity, authorization and authentication
  - Eavesdropping
  - Tampering
  - Impersonation
  - Repudiation

# Internet Security Key Objectives

- Provide robust system host security and ensure system integrity while connected to the Internet
- Provide the ability to guarantee the privacy and integrity of data exchanged over the Internet

Strategy

# Internet Security Strategy

## Focus on KEY Internet security areas

- Leverage existing security products and services running on UNIX and NT
- Provide robust system security (MPE/iX OS)
- Embrace key Internet building blocks
- Provide key security Internet services
- Strong partnership with ISV to provide Internet security products and solutions
- Continue research and evolve

# HP *e*3000 Internet Security in General

- Access control

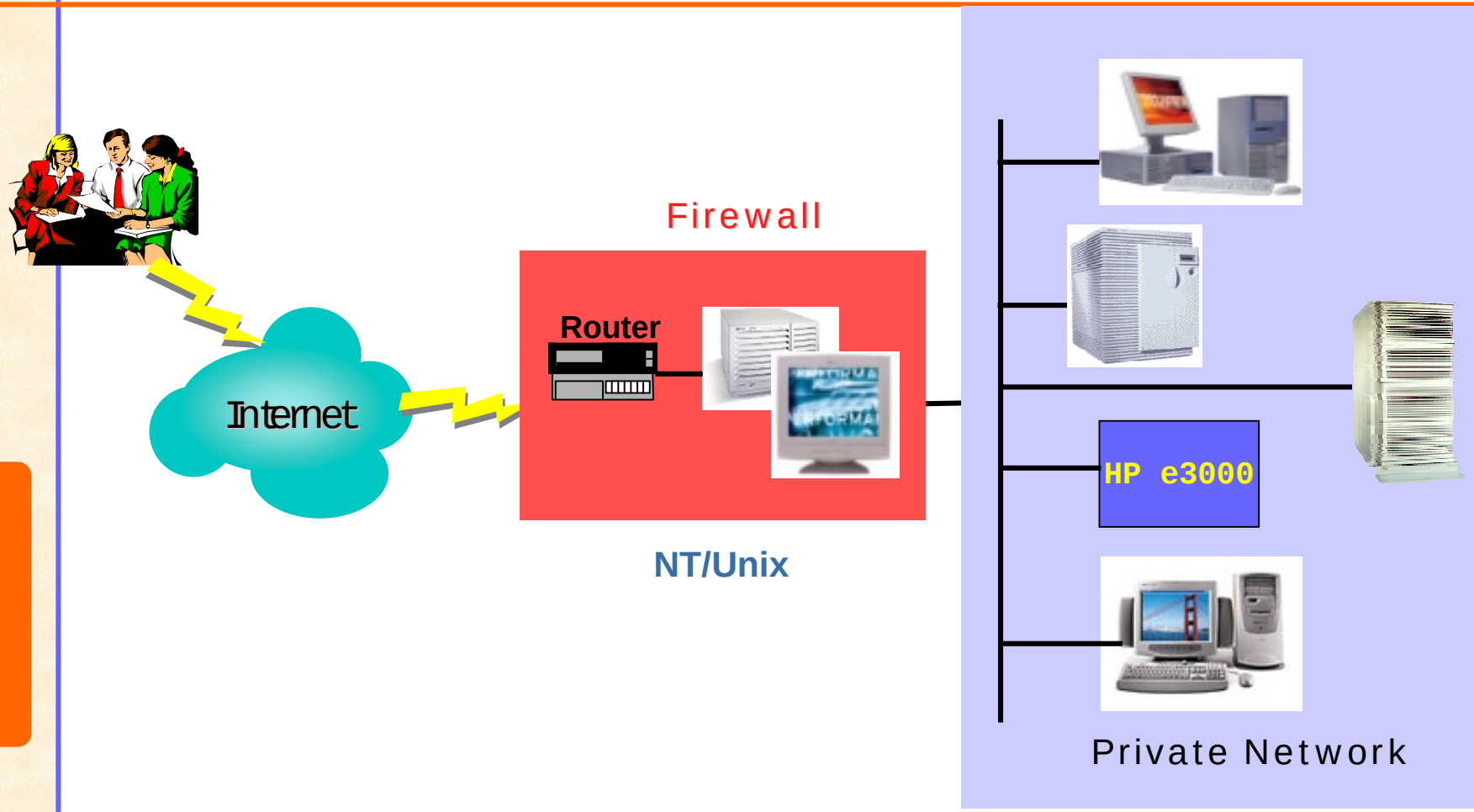
  Protect internet connected systems against unwanted access

  - **Perimeter defense**
  - **System host security**
- Secure communications

  Ensure privacy of data transmitted over an external and internal network and protect against eavesdropping, tampering and forgery

  - **RSA BSAFE SSL-C toolkit**
  - **HP WebWise Secure Web Server**
  - **HP Secure Web Console**

# Perimeter Defense: Firewalls



# System Host Security

- Physical security
- Basic OS security measures
- 3rd party security products

# System Host Security
## Basic OS Security Measures

- Logon
  - **Unique logon ID, user.account + password**
  - **logon UDC**
- System access
  - **Account structure (accounts, groups, users, files)**
  - **User roles, capabilities (SM, AM, OP, PM, etc.) determine access level**
- File access
  - **File access restrictions and lockwords**
  - **ACD (Access Control Definition)**

# System Host Security
## Basic OS Security Measures

- Logging facilities
  - **System logging**
  - **User logging**
- Security monitor
  - **Security Configurator (secconf.pub.sys)**
- Internet services
  - **INETDCNF.NET.SYS or /etc/inetd.conf**
  - **INETDSEC.NET.SYS**

# HP *e*3000 Security Partner
# SAFE/3000

## SAFE/3000 (Monterey Software)

- Prevention of unauthorized access at *both* the system and file/database level
- Control of authorized access at both the system and file/database level
- Verification of authorized system and file/database access through an integrated audit facility
- Detection of unauthorized access attempts at both the system and file/database level through the audit facility

- http://www.editcorp.com/business/montereysoftware/

# HP e3000 Security Partner
## Security/3000 and Audit/3000

- Security/3000 (VESOFT)
  - **Adds extra protection on basic user/account/group password approach**
  - **Positive user identification, day of week, time of day restrictions, physical location assignment (by LDEV number), session name enforcement and etc.**
- Audit/3000 (VESOFT)
  - **Reports Security loopholes**
  - **Reports on passwordless users, job streams with embedded passwords, improperly secured files, possible "Trojan Horses", recent changes to your system security, users that can DISABLE your UDC-based security system and etc.**
- http://www.vesoft.org

# Secure Communication

- Data Privacy
  - **Ensure no one else has access to data**
- Data Integrity
  - **Prevent data tampering**
- Authentication
  - **Confirm the sender's and receiver's identity**
- Authorization
  - **Grant or deny access or services to a particular user**
- Non-repudiation
  - **Prevents the sender of information from denying at a later date that the information was ever sent**

# Key Internet Building Block: Secure Sockets Layer (SSL)

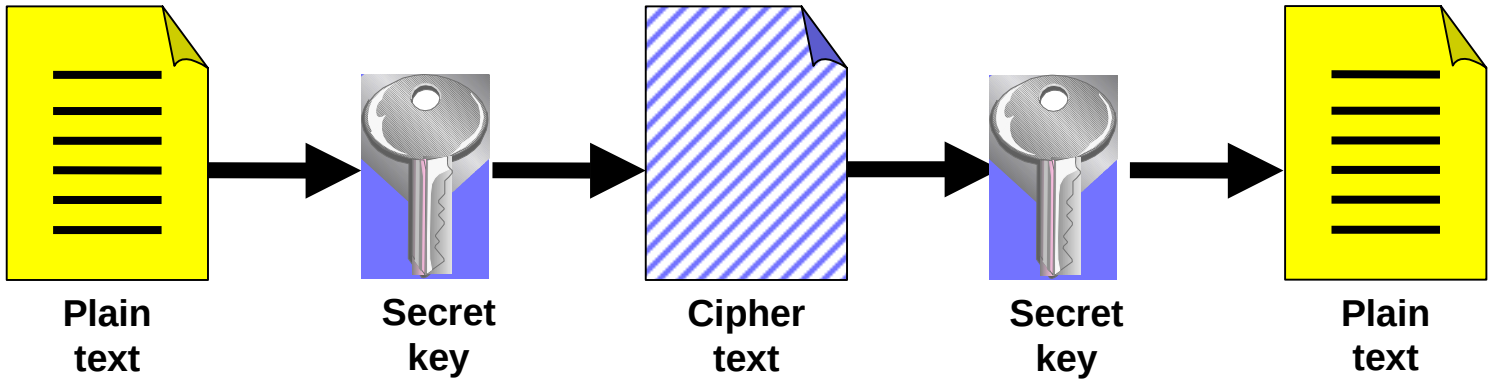
- An Internet protocol designed to provide secure communication between a client and a server via encryption, message digests, digital signatures, and certificate authentication
- De facto standard for securing data flowing across the Internet

# Encryption and Decryption

- Encryption is a process of scrambling data into an unintelligible form (cipher text) by applying a cryptographic algorithm
- Decryption converts the cipher back to its original form
- Require key(s) with the algorithm to produce an encrypted result or to decrypt previously encrypted
- The strength of the encryption is dependent on:
  - **the nature of the algorithm**
  - **the size of the keys (40 bits? 56 bits? 128 bits? 1024 bits? )**
- Address the problem of eavesdropping

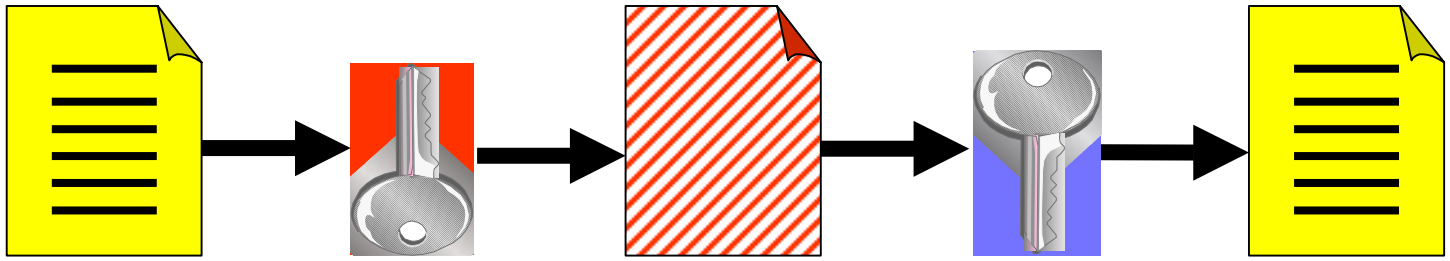
# Secret Key Encryption

- A single key is used for both encryption and decryption
- The key is "shared" by the sender and receiver
- Common symmetric algorithms are RC4, DES and 3-DES

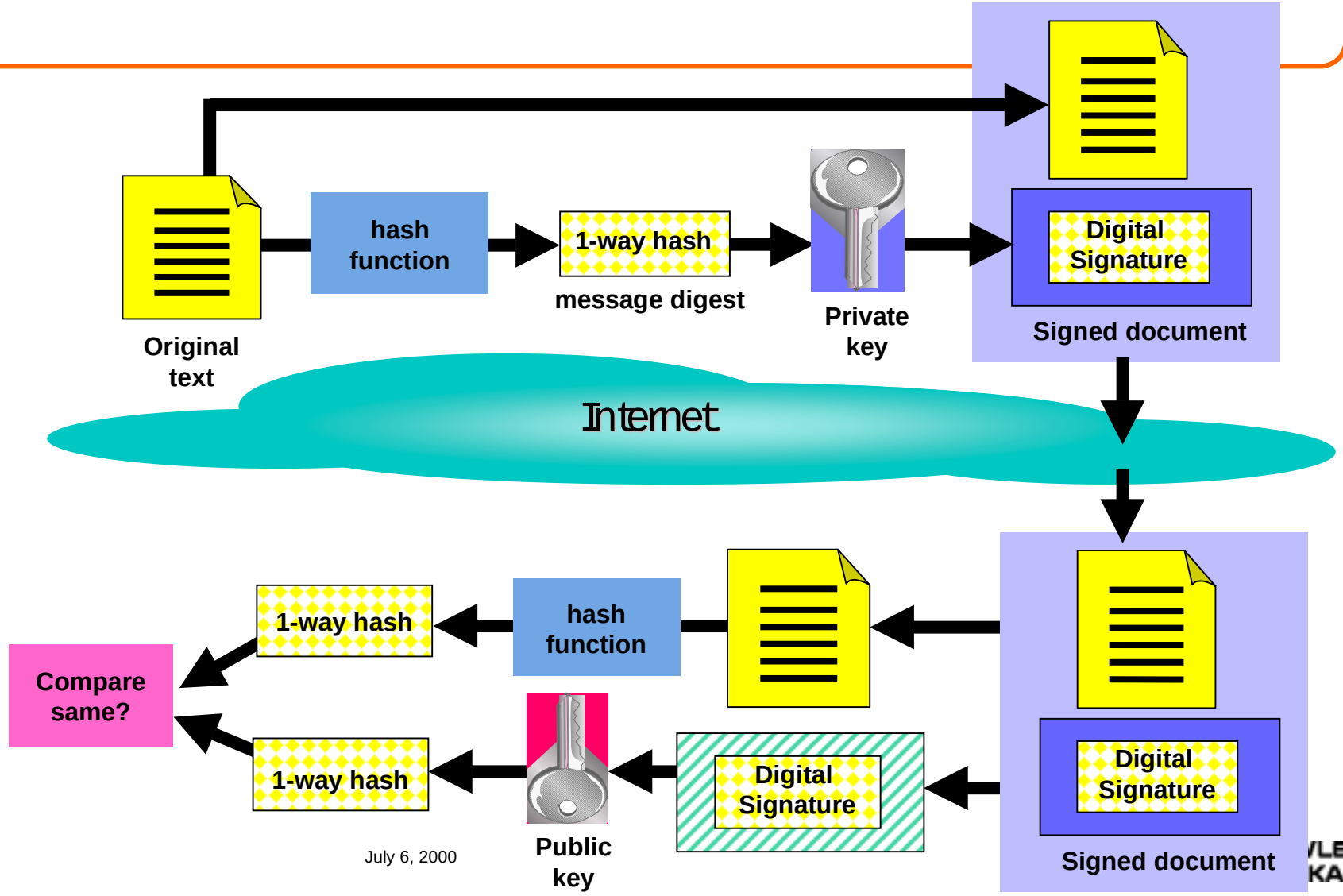


# Public key Encryption

- **Two keys are used. The two keys provide inverse functions.**
  - **Private - Known only to the owner of the key**
    - **create digital signatures**
    - **create digital certificates**
  - **Public - Exposed to the world**
    - **included in digital certificate**
- **Most well known public/private key algorithm is RSA**

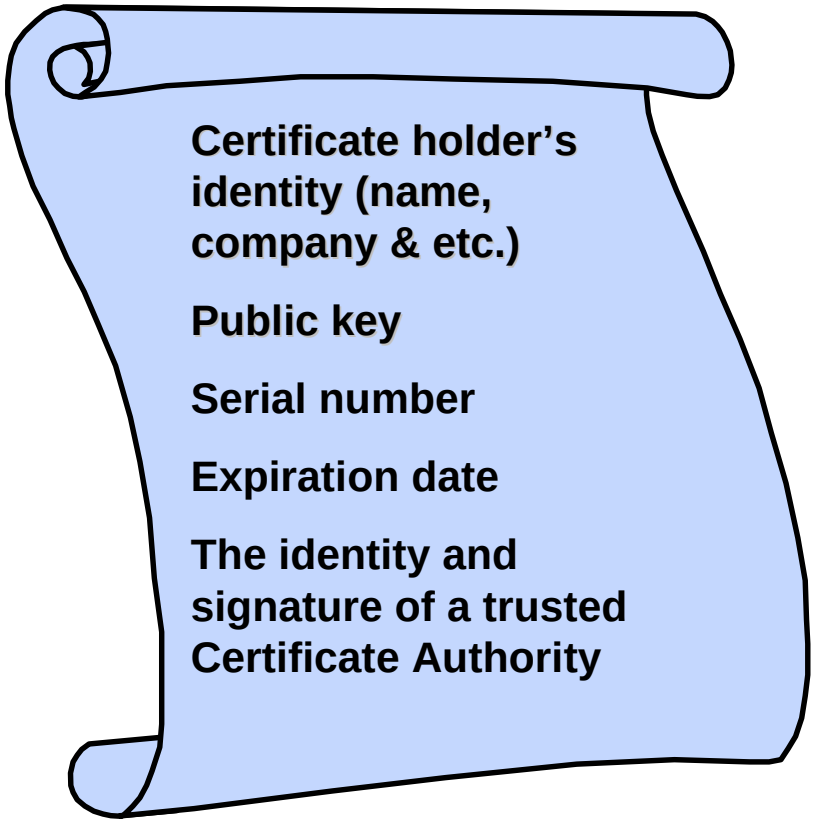


# Message Digests and Digital Signatures



# Digital Certificates

- A digital document created and signed by Certificate Authority
- Validates certificate holder's identity-public key to others
- Format defined by X.509 standard



# SSL is NOT

- a substitute for a firewall
- a substitute for good host security practices
- a substitute for good application security practices
- a substitute for good human security practices

# RSA BSAFE SSL-C toolkit Overview

- What is it?
  - **A software development suite for building SSL-enabled applications, combined with full suite of RSA algorithms**
  - **SSL-C toolkit provides a set of C-APIs which interact with the underlying SSL toolkit library**
- Benefits
  - **Enables developers to easily embed SSL-based encryption capabilities into their applications**
  - **Developers can quickly deploy e-commerce applications without being encryption experts**

# RSA BSAFE SSL-C toolkit

- RSA BSAFE SSL-C v.1.0 key features
  - **SSL v2, v3, and TLS v1 compliance**
  - **128-bit encryption**
  - **X.509 certificates support and Client authentication**
  - **Support for session caching**
- Includes
  - **Library libsslc.a**
  - **Product application interface header and configuration files**
  - **Sample programs and source code**
  - **Utility for key generation, certificate management etc.**
  - **Full documentation**
- Can be ordered directly from RSA

# Key Internet Security Services
# HP WebWise.

- A solution suite for Internet-enabling your e3000 businesses
- First suite component is the HP WebWise MPE/iX Secure Web Server
  - **Orderable as of May 1st, 2000**
  - **On-line order, purchase, and download available in the near future from HP Software Depot**
  - **CD ROM media with marketing extras**
  - **Available for MPE/iX 6.0 or later**

# HP WebWise. Secure Web Server Overview

- Based on Apache, mod_ssl, openssl and RSA BSAFE Crypto-C
- Easily installed and configured
- Provides full-strength encryption and X.509 authentication
- First component of new HP WebWise suite
- Leverages the robustness and rapid evolution of opensource software
- Full HP support via the Response Center

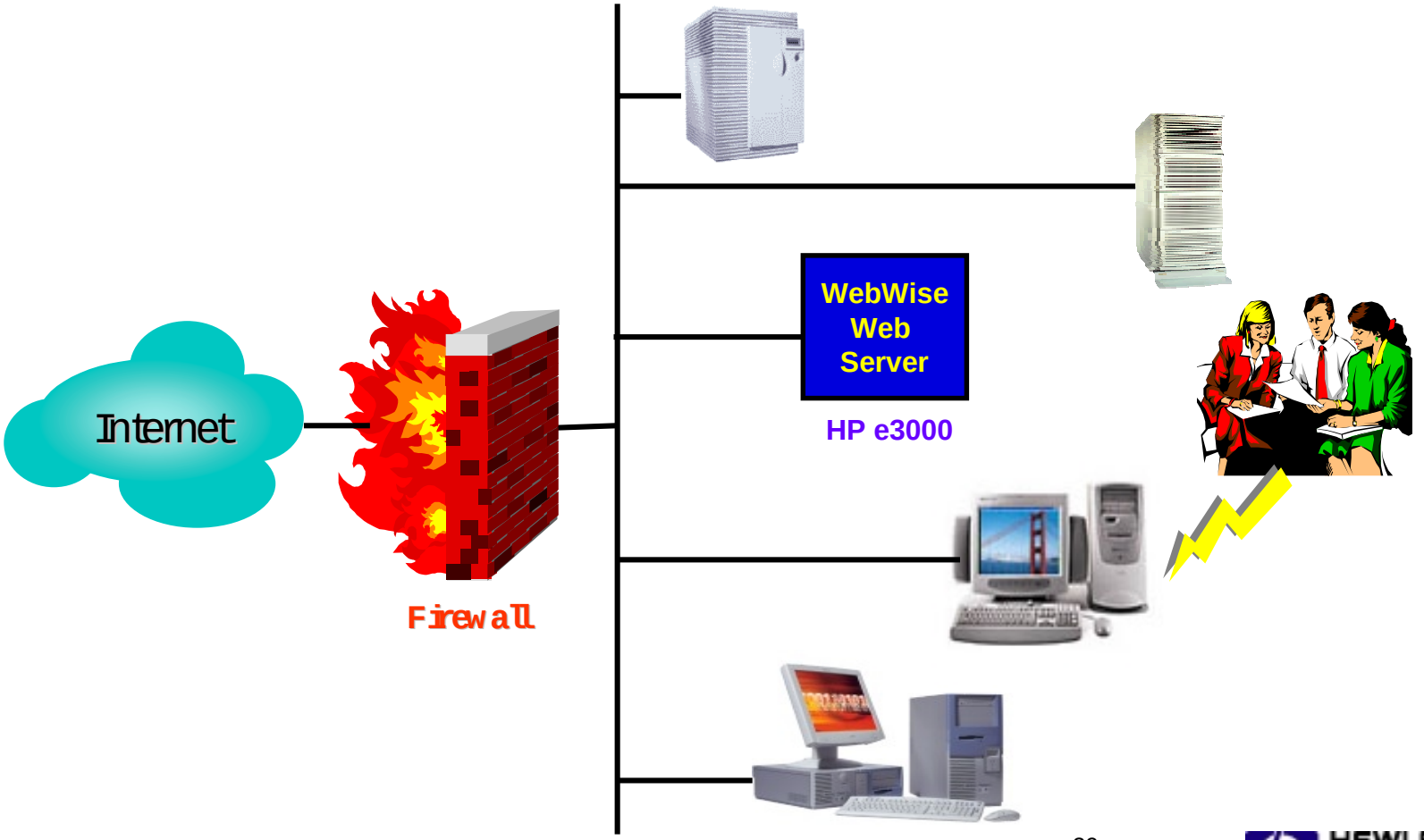
# HP WebWise. Secure Web Server
## Features & Benefits

- mod_ssl
  - **SSLv2.0, SSL v3.0, and TLS v1.0**
  - **full-strength encryption**
  - **X.509 certificate authentication**
  - **For e-commerce with e-confidence!**
- mod_so
  - **Dynamic Shared Objects (DSO)**
  - **Load customer's module at runtime**
  - **Customers can add their own functionality**
- mod_proxy
  - **Turn your e3000 into an ftp/http proxy server**

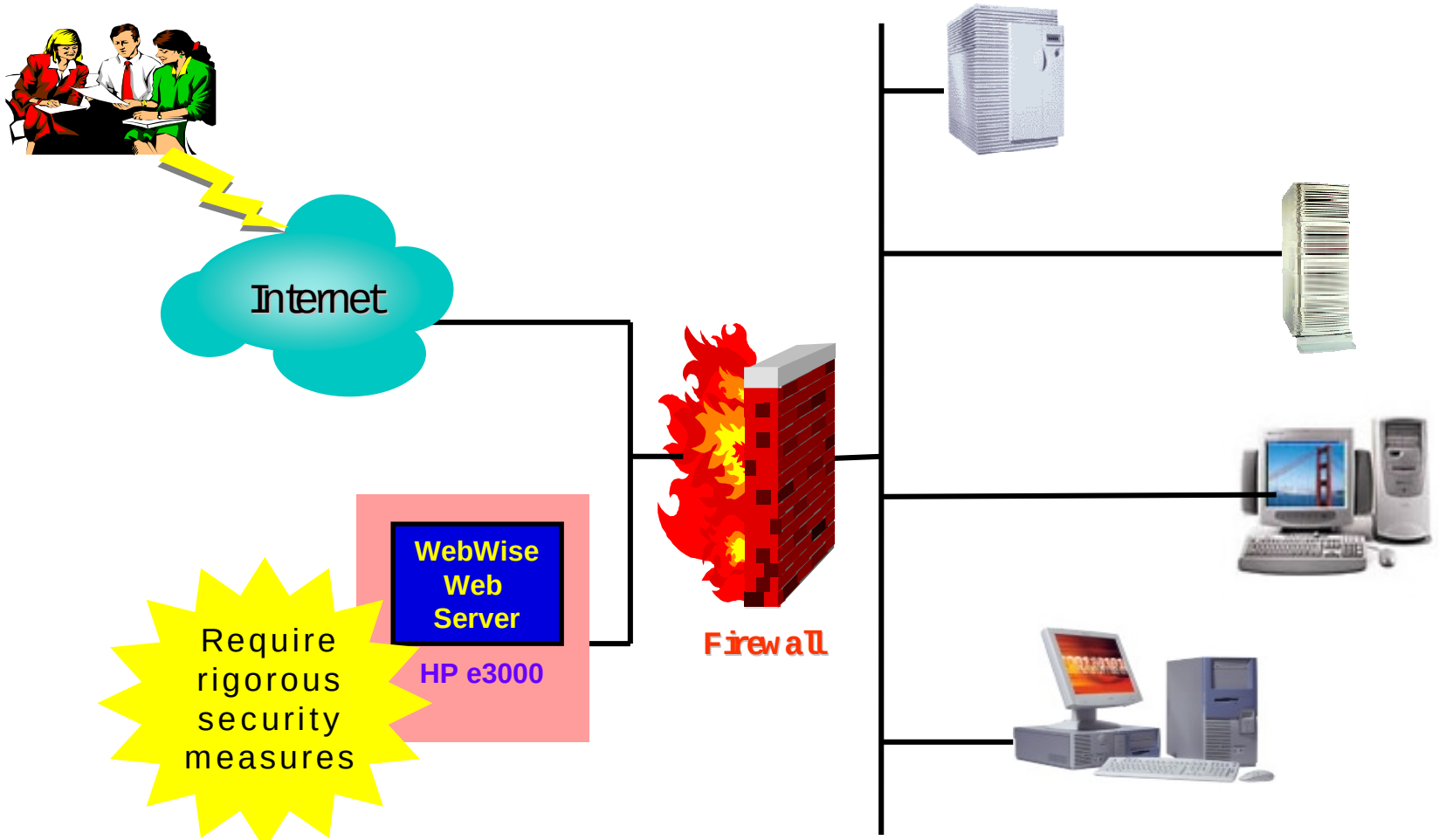
# HP WebWise. Secure Web Server
## Features & Benefits (cont..)

- mod_rewrite
  - **Modify incoming URLs before processing**
  - **For coping with highly dynamic content**
- mod_vhost_alias
  - **Simplifies the hosting of many virtual servers**
- plus all Apache enhancements since 1.3.4 up to 1.3.9

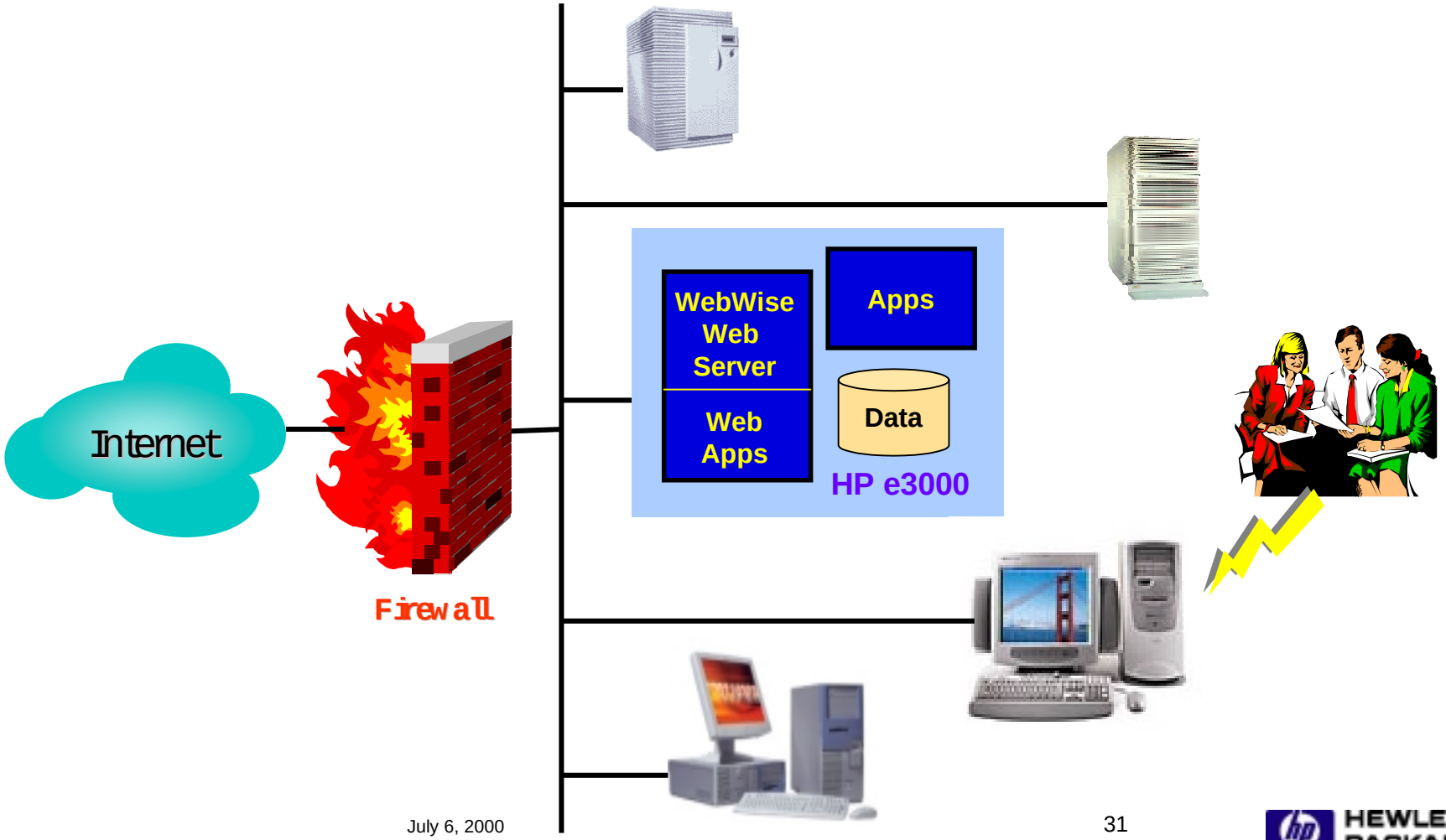
# Using WebWise. as a standalone Web Server #1



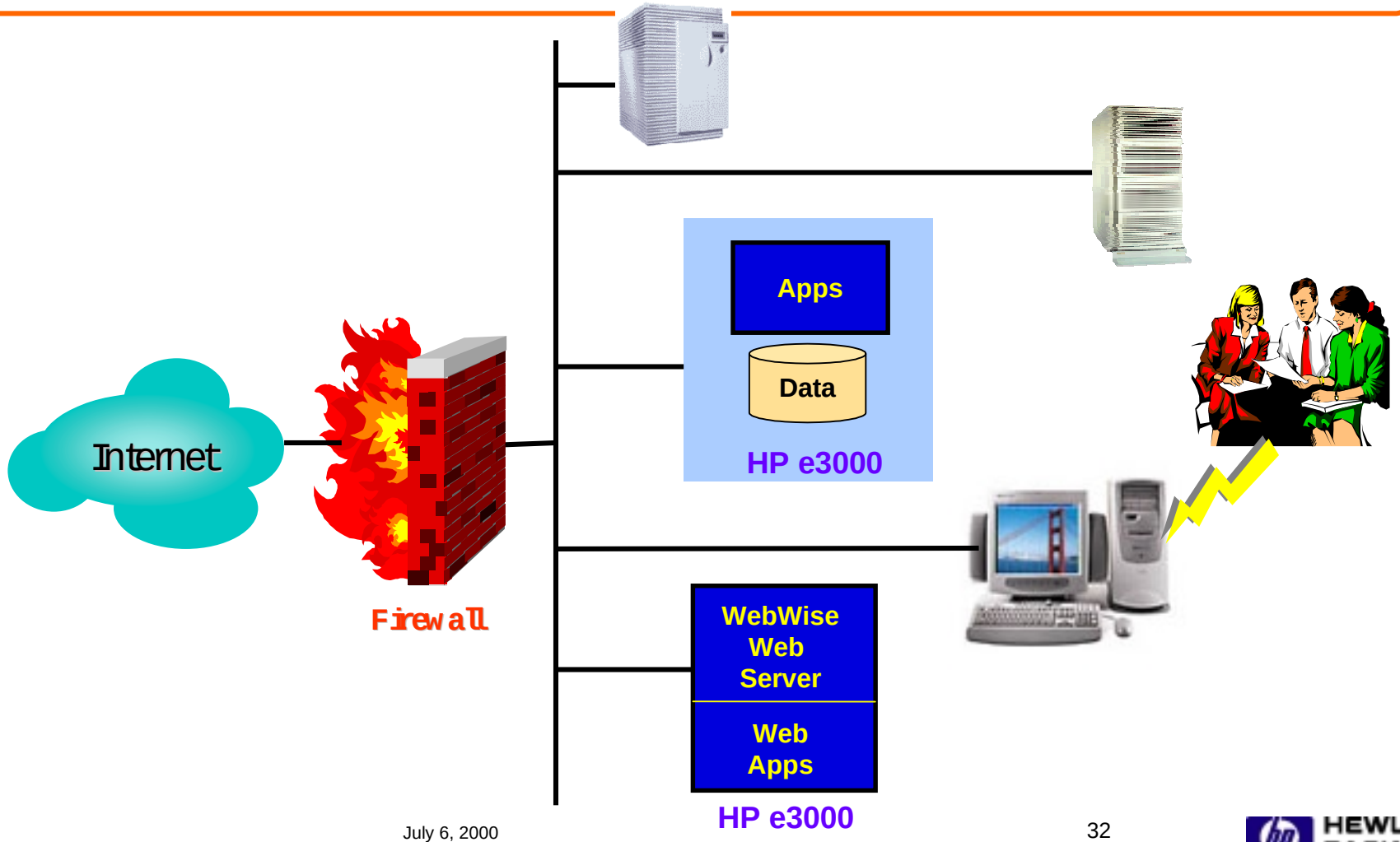
# Using WebWise. as a standalone Web Server #2



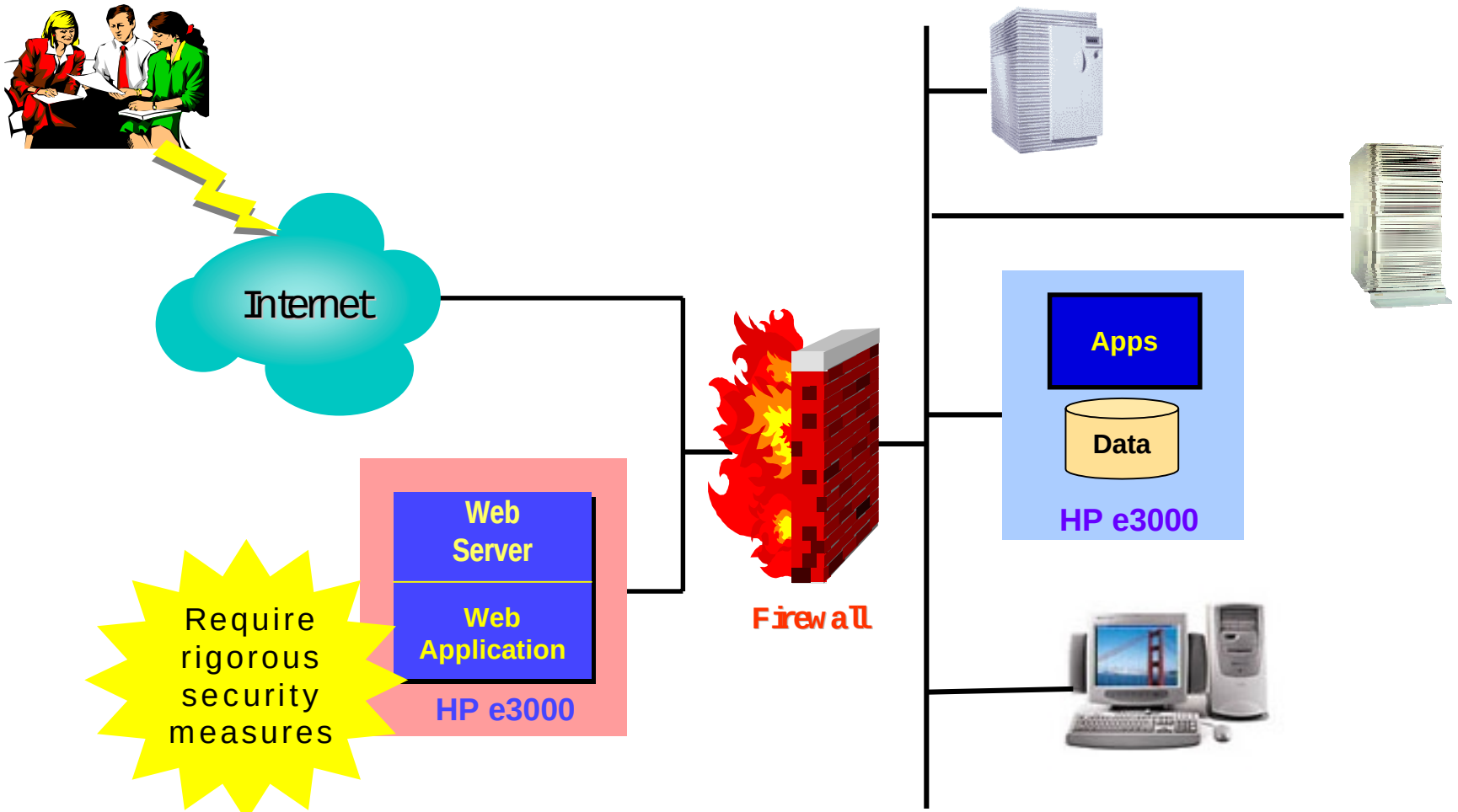
# Using WebWise. Web Server to access HP e3000 data #1



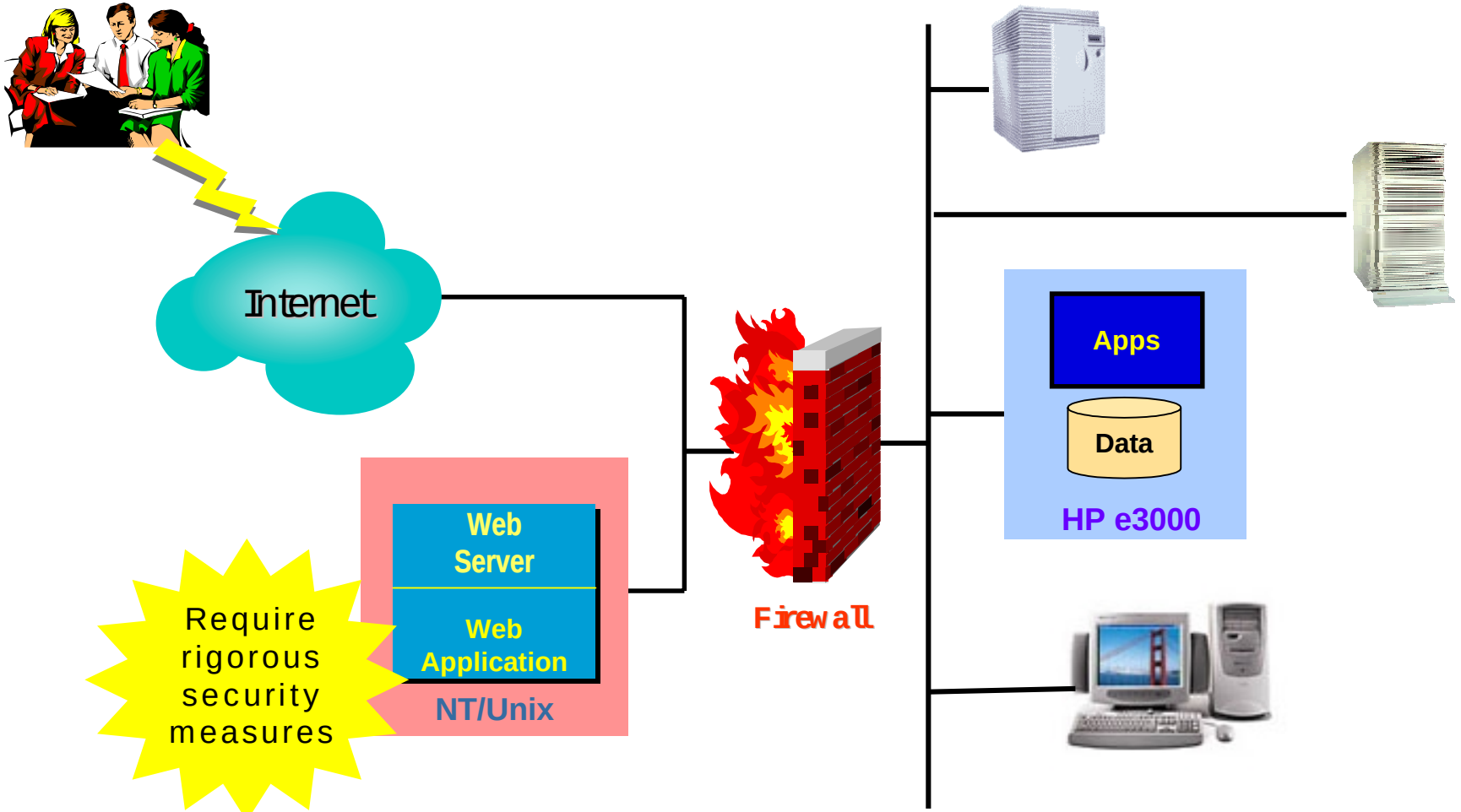
# Using WebWise. Web Server to access HP e3000 data #2



# Using WebWise. Web Server to access HP e3000 data #3

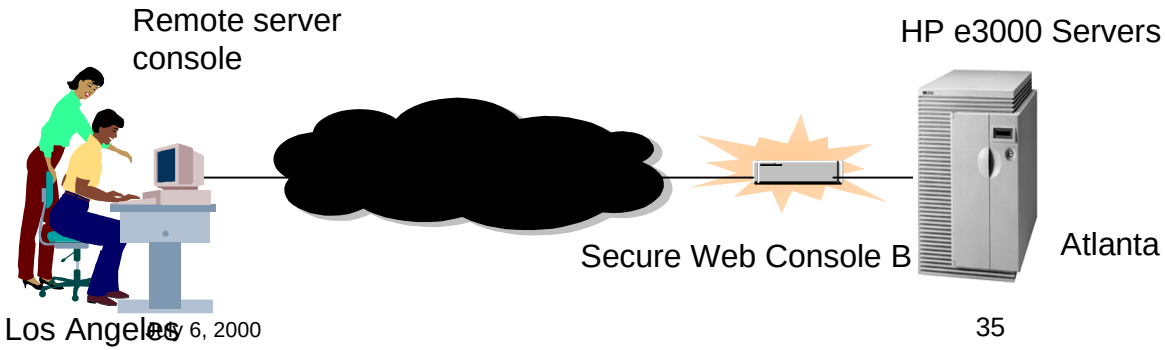


# Using NT/Unix as an Internet Web/Application Server



# HP's Secure Web Console

- Now, manage your servers over your intranet
  - **From any location in the world**
  - **From any browser based PC (Netscape or Microsoft IE)**
- Remote browser access to the server console port **(access to powerful, low level console commands)**
- One person, one “console”, several servers
  - **“Bookmark” the servers**
  - **Manage from the comfort of your office**



# Some Security Tips

- Use a firewall
- Put your sensitive data behind the firewall
- Disable unneeded in-bound network services
- Make sure remaining services are configured properly
- Activate logging facility and regularly examine the logs to detect intrusion attempts
- Stay current on releases & patches

# Some Security Tips (cont.)

- Properly configured all subsystems not to allow unintentional access points
  - **Restrict file system access by limiting read/write access using file access restrictions, permissions, lockwords and ACDs. For example:**
    - **Minimize the use of world-readable and world-writable permissions**
  - **Regularly change all accounts, group and/or users passwords**
  - **Limit the number of login accounts on the server**
- Secure your web server

# Web Server Security Tips

- Use WebWise to provide secure communication between browser and server
- Run the web server as an unprivileged user with minimum capabilities
- Configure the web server to restrict access control to directories and files

# Web Server Security Tips (cont..)

- Most security problems BY FAR are the result of sloppy CGI programming
  - **Validate all data fields from the browser and don't let input do something destructive**
  - **limit where CGI can run such as don't allow CGI/SSI to be used outside of the APACHE account**
- Disable unneeded web server features prone to misuse such as server side includes, symbolic links, user-supported directories, automated directory listing, etc.

# Continue to monitor security needs...

- Evaluate and strengthen system security
  - **logon user/password encryption/authentication, ftp and etc.**
- Explore key security services
  - **Single Sign-on**
  - **WebQos**
  - **Secure telnet**
  - **Secure ftp and etc.**
- Explore key security enabling technologies
  - **PKI, VPN, IPSec and etc.**

# Summary

- Strategy on HP *e*3000
- Security on HP *e*3000
  - **Access Control**
    - **Perimeter defense**
    - **Host security**
  - **Secure Communication**
    - **RSA BSAFE SSL-C**
    - **HP WebWise Secure Web Server**
    - **HP Secure Web Console**
  - **Tips**
- Continue to monitor and evolve

# References

- **Configuring and Managing MPE/iX Internet Services Manual**
- **Manager's Guide to MPE/iX Security**
- **HP Security Monitor/iX User's Guide**

- **http://www.businessservers.hp.com/solutions/internet/accesswp.html**
  ***(Web Enabling Your HP e3000 Applications and Data Access)***
- **http://www.businessservers.hp.com/solutions/internet/CSY0010UQ.html**
  **(*HP e3000 Internet and E-services Solutions Guide Overview)***
- **http://www.rsasecurity.com/products/bsafe/sslc.html**
  ***(RSA BSAFE SSL-C commercial product)***
- **http://jazz.external.hp.com**

# Questions?