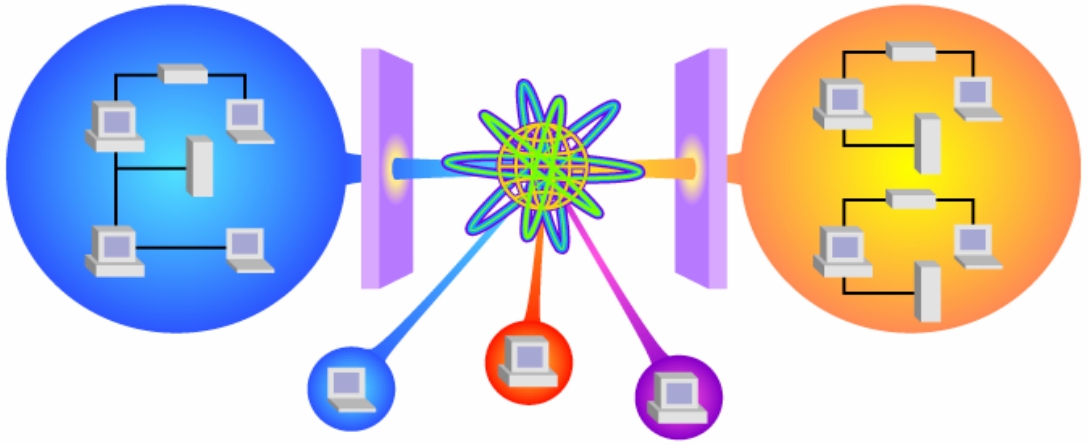
hp e3000

internet security



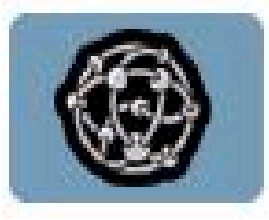
internet security on your hp e3000

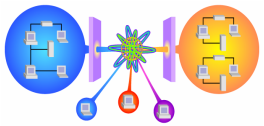
HPWorld 2000 session

OnOn Hong
onon_hong@hp.com

hp e3000

internet security

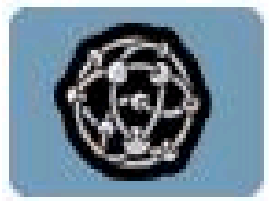




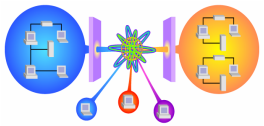
With the advent of the Internet and the creation and rapid success of e-business, security has never been more important

hp e3000

internet security



hp e3000 internet and interoperability roadmap



Business Value & Benefit

Investment protection; reduce costs; increase productivity

Modernize legacy applications

New business opportunities

Stimulate the growth of the Internet and e-solutions

Capitalize on and expand Internet business

Anticipate and fulfil emerging needs for ISVs and enterprise customers

Shape the e-services world

Become a key player in the e-services world

Leads to…

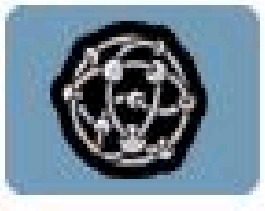
vision

HP e3000 customers and their businesses are successfully using and seamlessly integrating with the Internet/Intranet and the e-services world

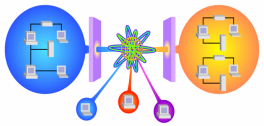
2000 **HP-UX, MPE/iX, NT, Linux and beyond** 2001+

hp e3000

internet security



Internet security vision



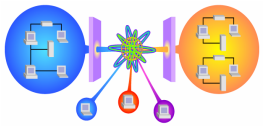
HP e3000 customers and their businesses are successfully using and seamlessly integrating the Internet and the e-services world...

SECURELY, PRIVATELY (IF DESIRED), AND WITH TRUST.

hp e3000

internet security

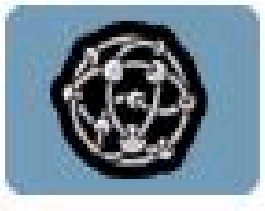
common internet security risks



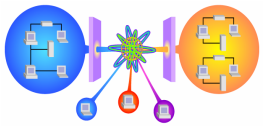
- System Access
  - **Unauthorized access**
  - **Denial of service**
- Network communication
  - **Eavesdropping**
  - **Tampering**
  - **Impersonation**
  - **Repudiation**

hp e3000

internet security



internet security key objectives

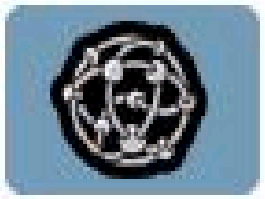


- Provide robust host security and ensure system integrity while connected to the Internet

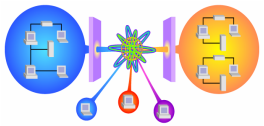
- Provide the ability to guarantee the privacy and integrity of data exchanged over the Internet

hp e3000

internet security



internet security strategy

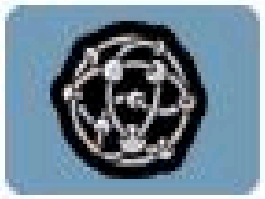


Focus on KEY Internet security areas

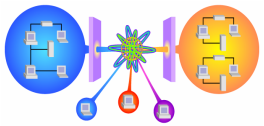
- Leverage existing security products and services (firewalls, VPN gateways) running on UNIX and NT
- Provide robust system security
- Embrace key Internet building blocks
- Provide key security Internet services
- Strong partnership with ISV to provide additional Internet security products and solutions
- Continue research and evolve

hp e3000

internet security



hp e3000 internet security in general



- Access control

  Protect internet connected systems against unwanted access

  - **Perimeter defense**
  - **System host security**

- Secure communication

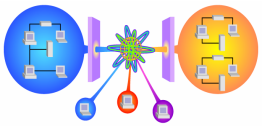
  Ensure privacy and integrity of data transmitted over the network and protect against eavesdropping, tampering and forgery

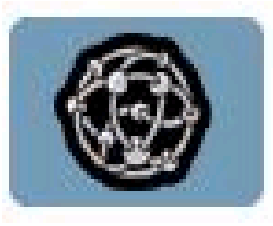
  - **RSA BSAFE SSL-C toolkit**
  - **HP WebWise MPE/iX Secure Web Server**
  - **HP Secure Web Console**

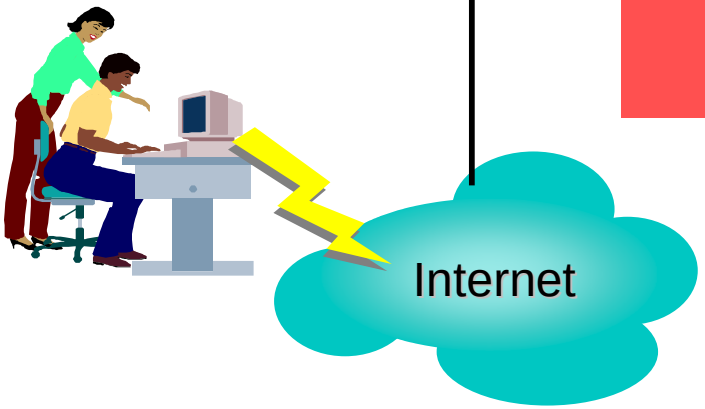
hp e3000

internet security

perimeter defense: firewalls



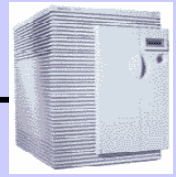




Firewall

Router

NT/Unix

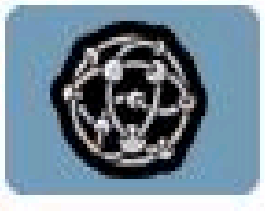


HP e3000

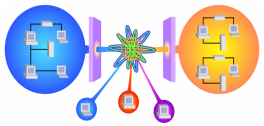
Private Network

hp e3000

internet security



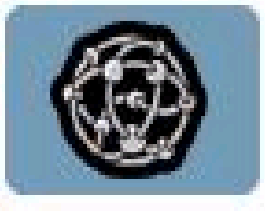
system host security



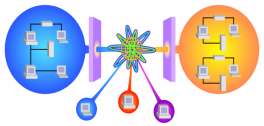
- Physical security
- Basic OS security measures
- 3rd party security products

hp e3000

internet security



system host security
basic os security measures

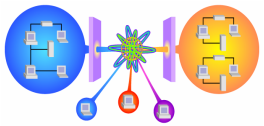


- Logon
  - **unique logon ID, user.account + password**
  - **logon UDC**
- System access
  - **Account structure (accounts, groups, users, files)**
  - **User identity, user roles, capabilities (SM, AM, OP, PM, etc.) determine access level**
- File access
  - **File access mode, permissions, and lockwords**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

hp e3000

internet security

system host security
basic os security measures

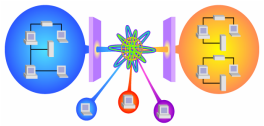


- Logging facilities
  - **System logging**
  - **User logging**
- Internet services
  - **INETDCNF.NET.SYS or /etc/inetd.conf**
  - **INETDSEC.NET.SYS or /usr/adm/inetd.sec**
- HP security monitor

hp e3000

internet security

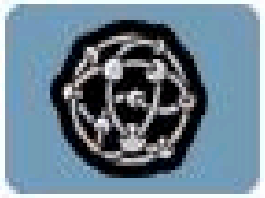
hp e3000 security partner products



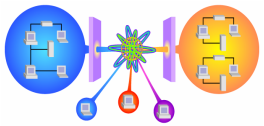
- SAFE/3000
  - **Monterey Software**
  - **http://www.editcorp.com/business/montereysoftware**
- Security/3000 and Audit/3000
  - **VESOFT**
  - **http://www.vesoft.org**

hp e3000

internet security



Secure Communication

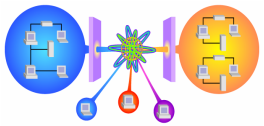


- Data Privacy
  - **Ensure no one else has access to data**
- Data Integrity
  - **Prevent data tampering**
- Authentication
  - **Confirm the sender's and receiver's identity**
- Authorization
  - **Grant or deny access or services to a particular user**
- Non-repudiation
  - **Prevents the sender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

hp e3000

internet security

key internet building block secure sockets layer (SSL)

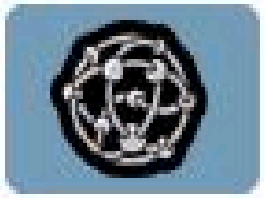


- An Internet protocol designed to provide secure communication between a client and a server via encryption, message digests, digital signatures, and certificate authentication

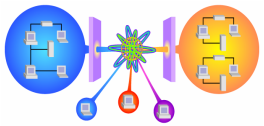
- De facto standard for securing data flowing across the Internet

hp e3000

internet security



encryption

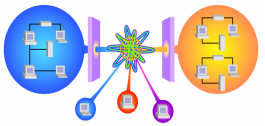


- Encryption is a process of scrambling data into an unintelligible form (cipher text) by applying a cryptographic algorithm
- Decryption converts the cipher back to its original form
- Require key(s) with the algorithm to produce an encrypted result or to decrypt previously encrypted
- The strength 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

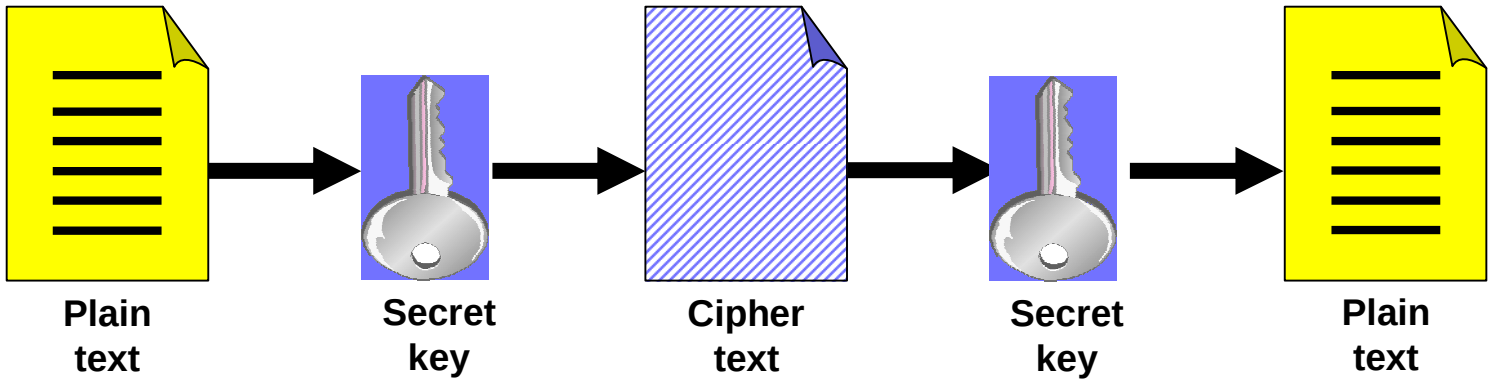
hp e3000

internet security

secret key cryptography



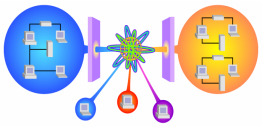
- A single key is used for both encryption and decryption
- The key is "shared" by the sender and receiver
- Common symmetric algorithms are RC4, DES and 3-DES



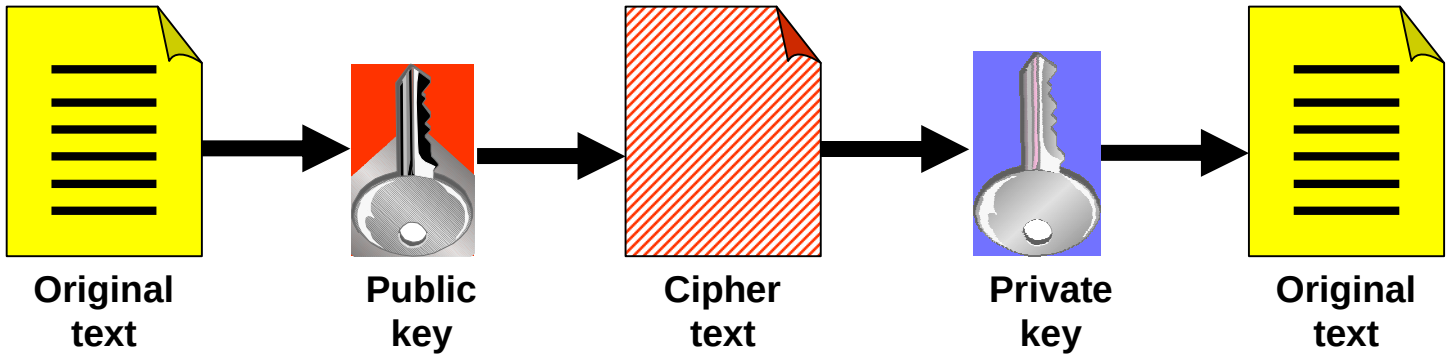
hp e3000

internet security

public key cryptography



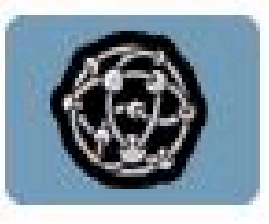
- Two keys are used. The two keys provide inverse functions.
  - **Private - Known only to the owner of the key**
    - **create digital signatures**
    - **create digital certificates**
  - **Public - Exposed to the world**
    - **included in digital certificate**
- Most well known public/private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

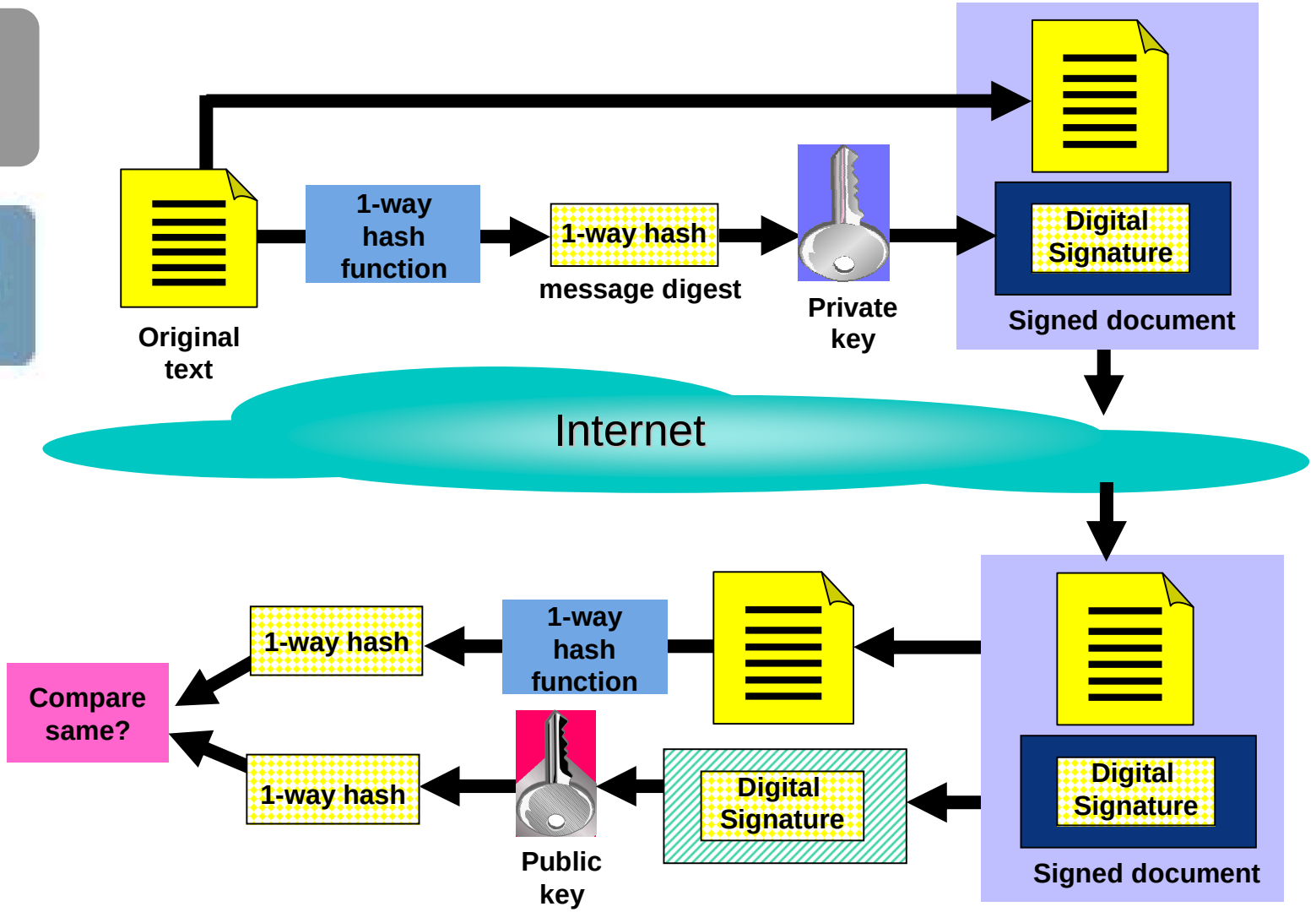


hp e3000

internet security

message digests and digital signatures

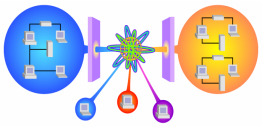




hp e3000

internet security

digital certificates



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

Certificate holder's identity (name, company & etc.)

Public key

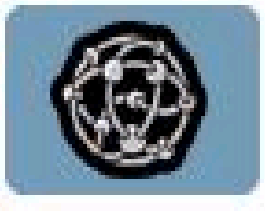
Serial number

Expiration date

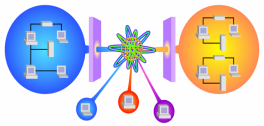
The identity and signature of a trusted Certificate Authority

hp e3000

internet security



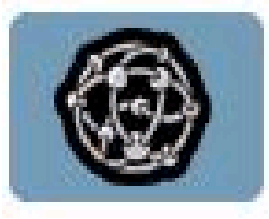
RSA BSAFE SSL-C toolkit overview



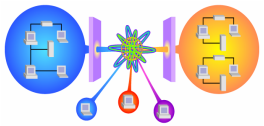
- What is it?
  - **A software development suite for building SSL-enabled applications, combined with full suite of RSA algorithms**
  - **Enable developers to easily embed SSL-based encryption capabilities into their applications**
- RSA BSAFE SSL-C v.1.0 key features
  - **SSL v2, v3, and TLS v1 compliance**
  - **128-bit encryption**
  - **X.509 authentication**
  - **Session caching**

hp e3000

internet security



RSA BSAFE SSL-C toolkit continued...



- Includes
  - **SSL Library with C APIs**
  - **Sample programs and source code**
  - **Utility for key generation, certificate management**
- Availability
  - **HP distribution**
    - **Available for downloading from Jazz "free"**
    - **For development and testing purpose only**
    - **No support from HP**
    - **Requires user license from RSA for support and deploying applications that use BSAFE SSL-C toolkit**
  - **Contact RSA directly**

Kevin DeJong

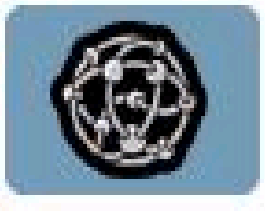
RSA Data Security Inc. Strategic Alliances manager

(650)-295-7758

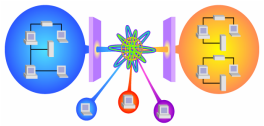
kdejong@rsasecurity.com

hp e3000

internet security



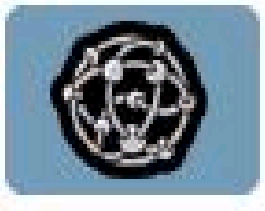
HP WebWise. Overview



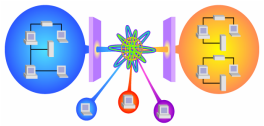
- A new Internet suite of key offerings for e-business and web-enabling your HP e3000
- First suite component is the HP WebWise MPE/iX Secure Web Server based on open-source Apache
  - ***Orderable and shipping now and available for MPE/iX 6.0 OS or greater.***
  - ***On-line order, purchase, and download available in the near future from HP Software Depot***
  - ***Full HP support via the Response Center***
  - ***Price ranges from US $1295 to US $1995 based on system performance tiers***
- Future offerings may include services such as web-consulting/training and third party products for easy, quick and affordable development and deployment

hp e3000

internet security



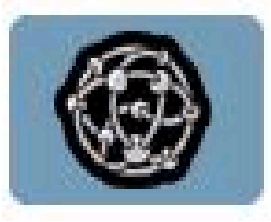
HP WebWise. secure web server key features & benefits

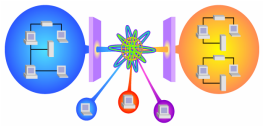


- Supports SSL and TLS
  - **Full-strength encryption**
  - **Client and server X.509 authentication**
  - **Allows customers to build internet applications with e-confidence!**
- Supports Dynamic Shared Objects (DSO)
  - **Apache modules dynamically loaded from external NMXLs**
  - **Allows customers to add-on extra functionality**
  - **Significant performance improvement over CGI**

hp e3000

internet security





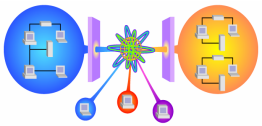
HP WebWise.
MPE/iX Secure Web Server Tutorial

Presented by Mark Bixby
Sept. 14 Thursday, 8:00am

hp e3000

internet security

operating environment



Internet

HP WebWise Secure Web Server

Firewall

PC

HP 9000 Server

HP 3000 Database Server

HP WebWise Secure Web Server

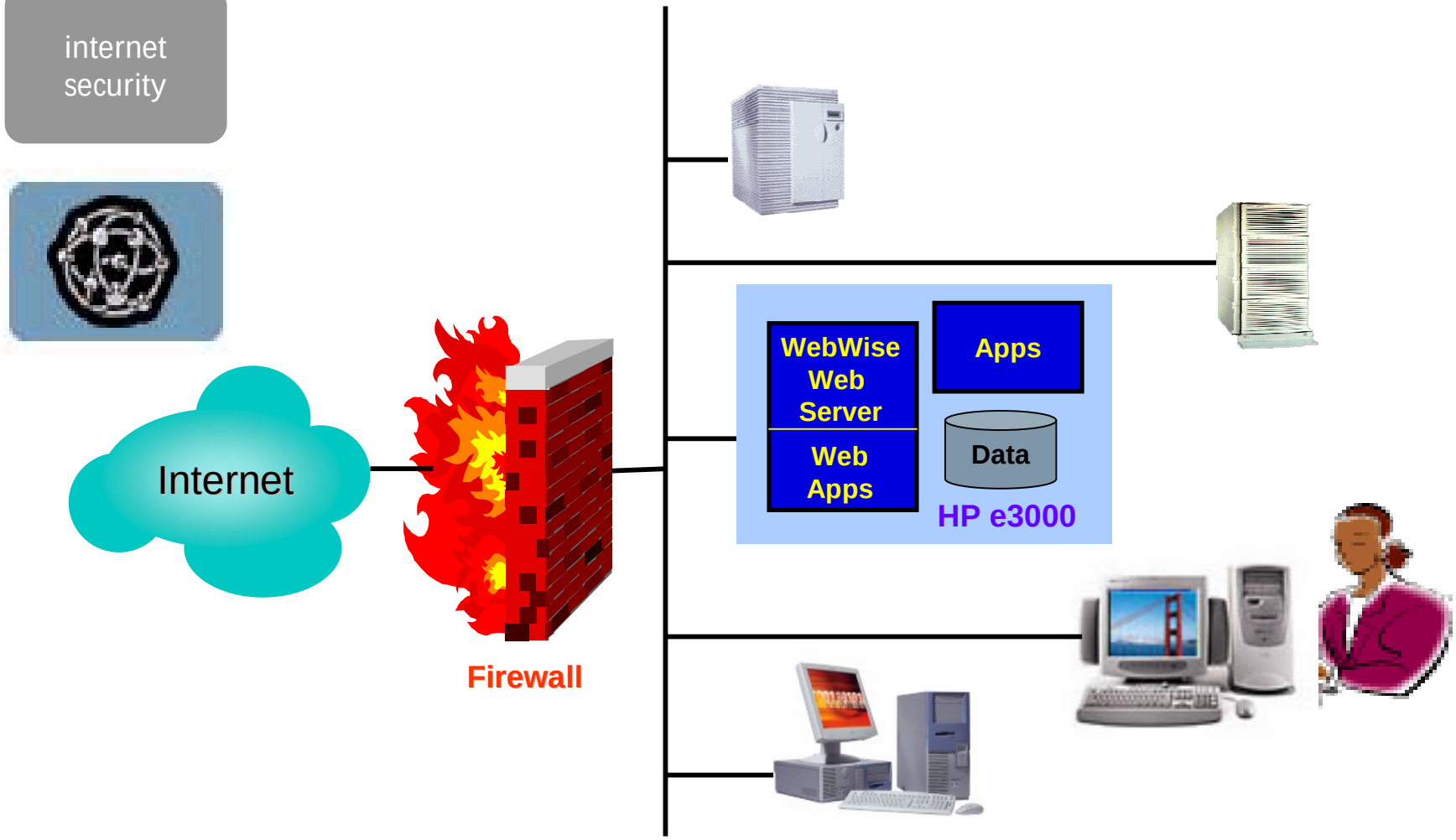
NT Server

Other Server

hp e3000

internet security

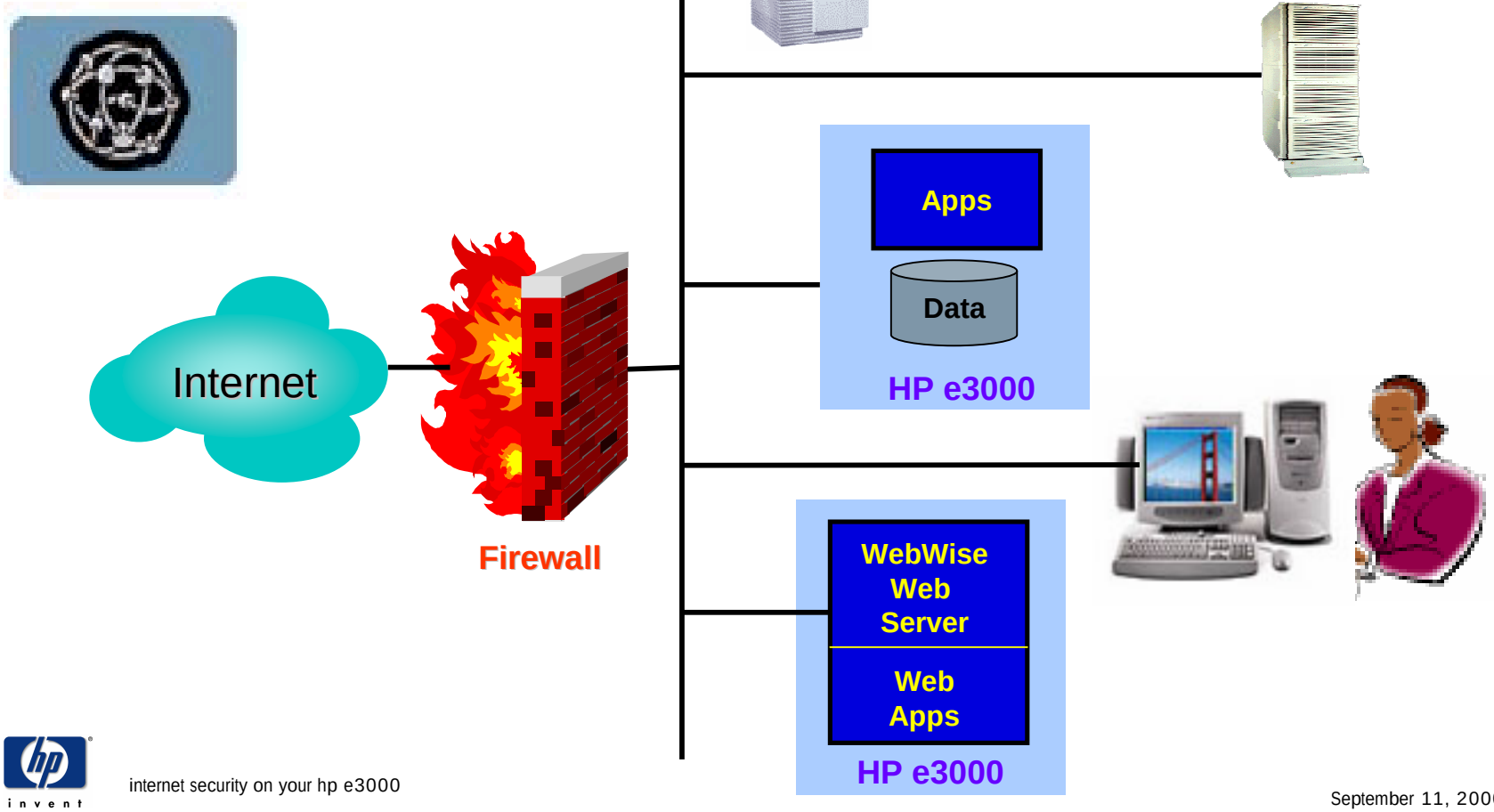
using WebWise. web server to access hp e3000 data #1



hp e3000

internet security

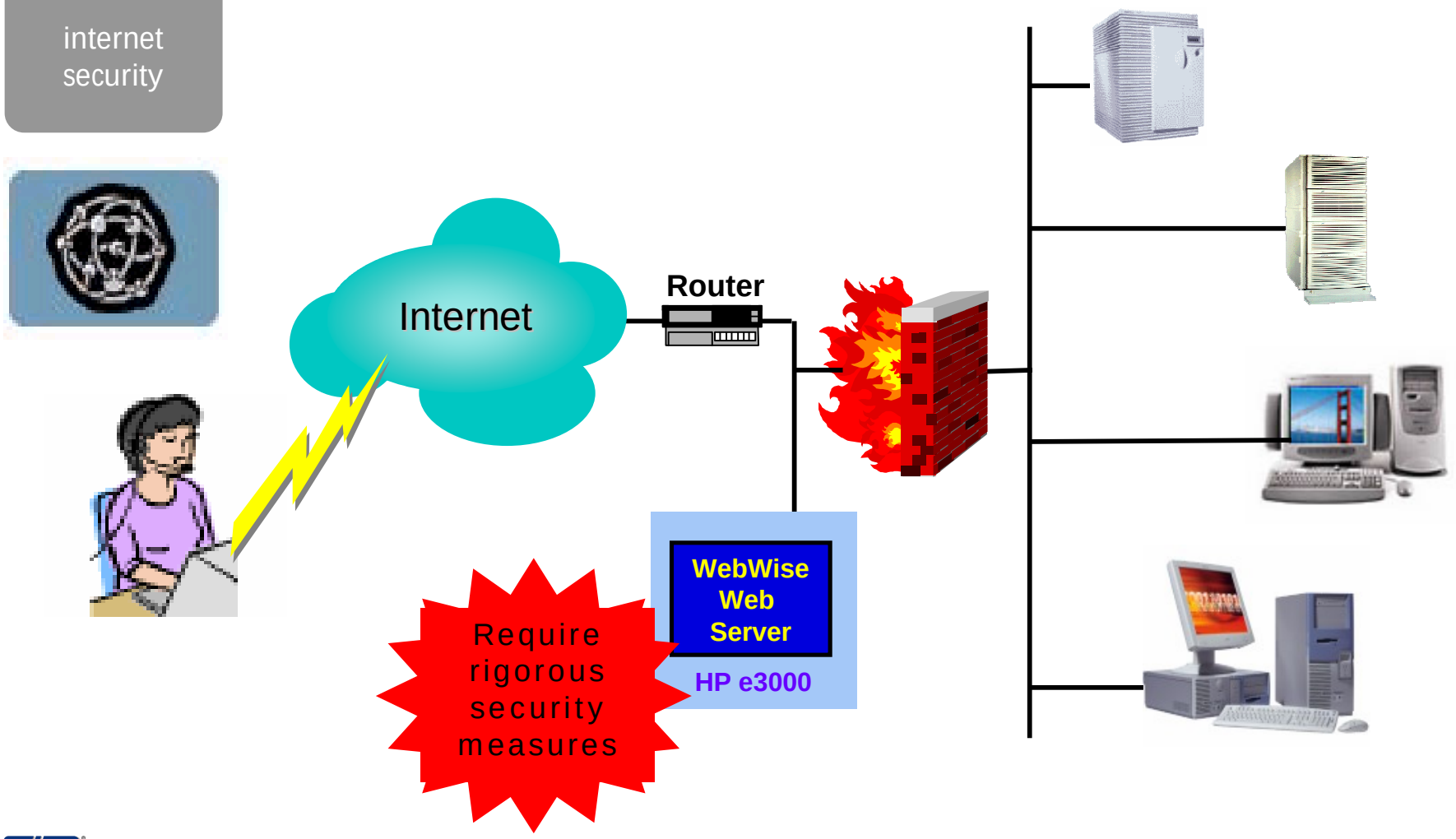
using WebWise. web server to access hp e3000 data #2



hp e3000

internet security

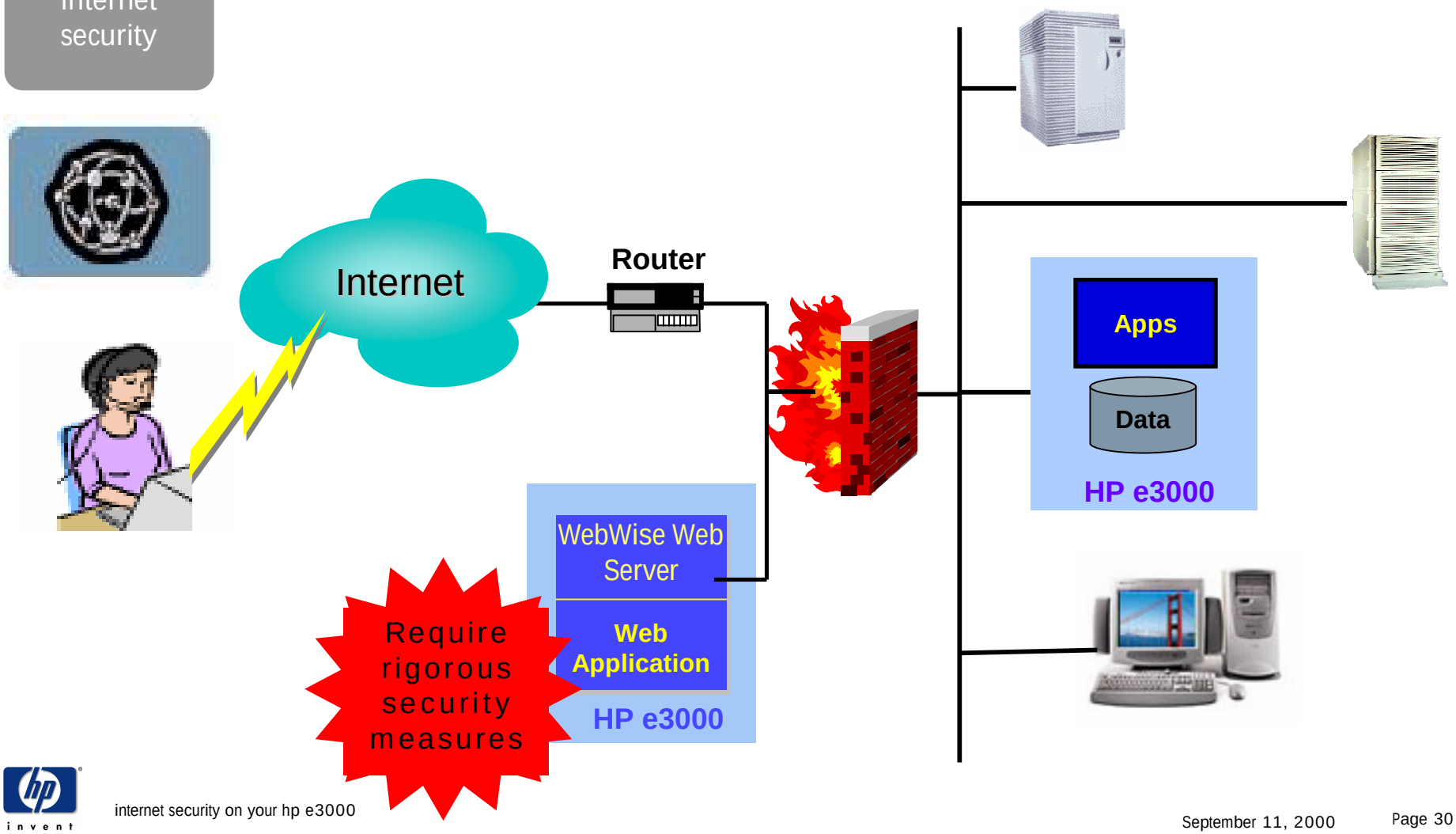
using WebWise. as a standalone web server



hp e3000

internet security

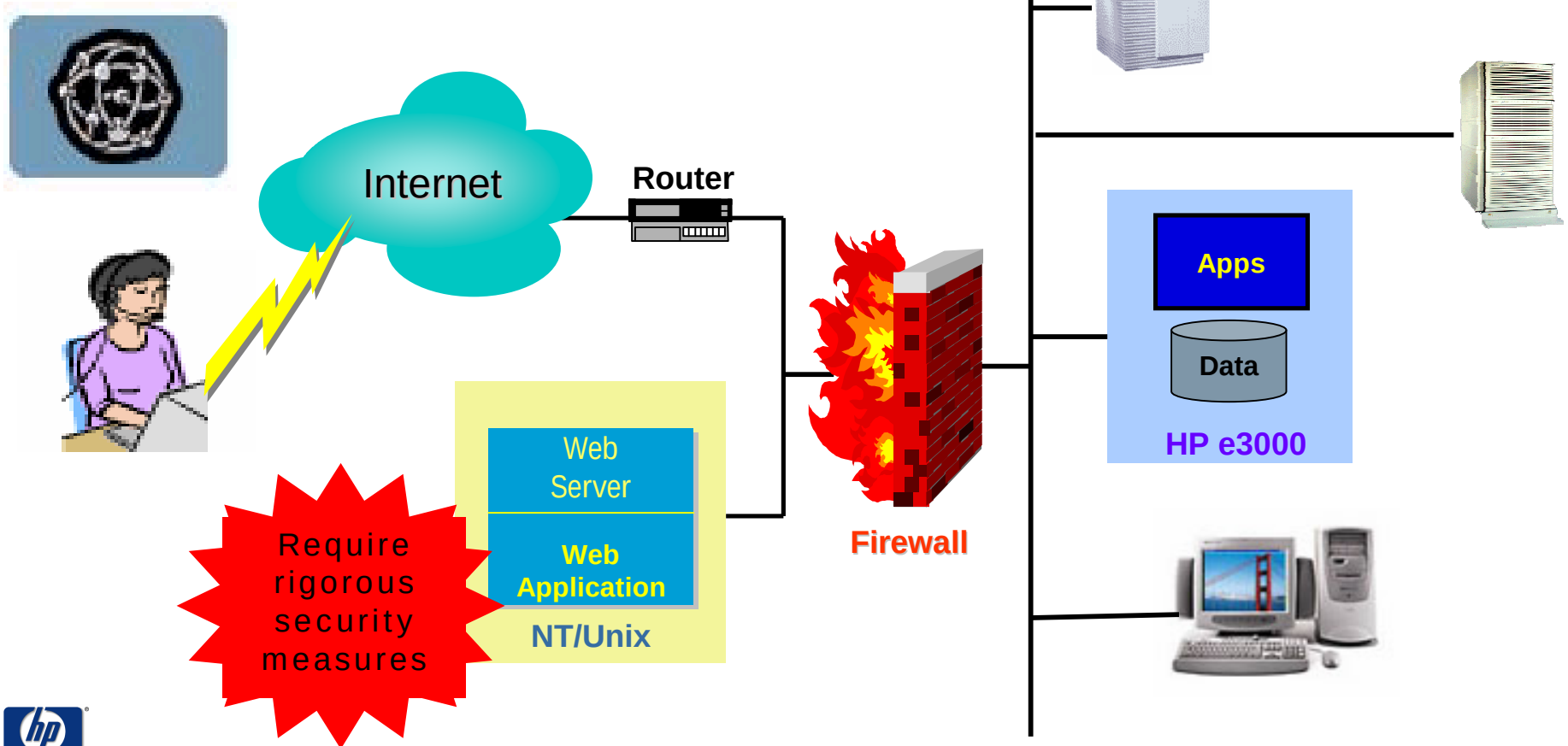
using WebWise. web server to access hp e3000 data #3



hp e3000

internet security

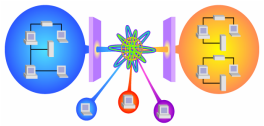
using NT/Unix web server to access hp e3000 data



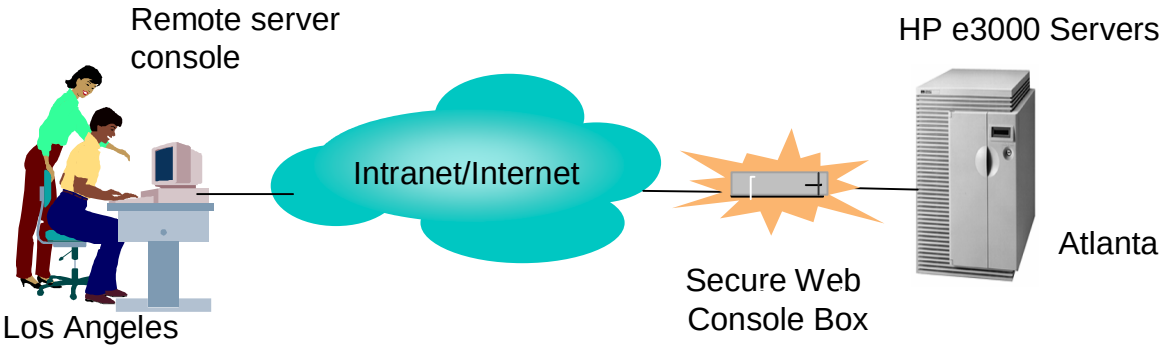
hp e3000

internet security

hp's secure web console



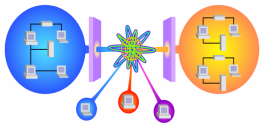
- Now, manage your servers over your intranet
  - **From any location in the world**
  - **From any browser** **(Netscape or Microsoft IE)**
- Remote browser access to the server console port
  (access to powerful, low level console commands)
- One person, one “console”, several servers
  - **“Bookmark”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



hp e3000

internet security

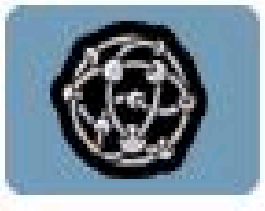
some security tips



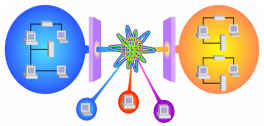
- Use a firewall
- Put your sensitive data behind the firewall
- Disable unneeded in-bound network services
- Make sure remaining services are configured properly
- Activate logging facility and regularly examine the logs to detect intrusion attempts
- Stay current on releases & patches

hp e3000

internet security



some security tips continued...



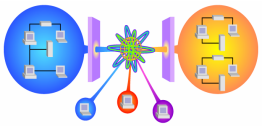
- Properly configured all subsystems not to allow unintentional access points
  - **Restrict file system access by using file access mode, permissions, lockwords and ACDs**
  - **Regularly change all accounts, group and/or users passwords**
  - **Limit the number of login accounts on the server**
- Use HP WebWise. secure web server for secure communication
- Web server security tips

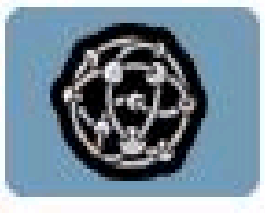
  please go to HP Web*Wise*. secure web server tutorial

hp e3000

internet security

Continue to monitor and evolve...

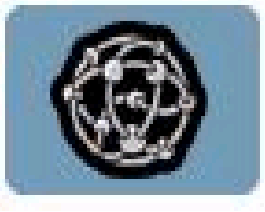




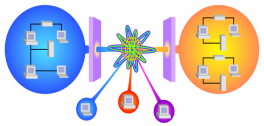
- Evaluate and strengthen the OS system security
- Explore key security enabling technologies
  - **secure protocols**
  - **PKI, VPN, IPSec and etc.**
- Explore key security services and products

hp e3000

internet security



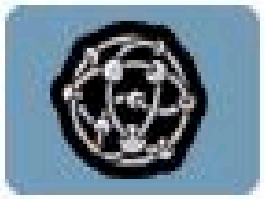
further references



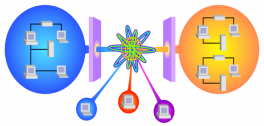
- **Configuring and Managing MPE/iX Internet Services Manual**
- **Manager's Guide to MPE/iX Security**
- **HP Security Monitor/iX User's Guide**
- **Web Enabling Your HP e3000 Applications and Data Access**
  http://www.businessservers.hp.com/solutions/internet/accesswp.html
- **HP e3000 Internet and E-services Solutions Guide Overview**
  http://www.businessservers.hp.com/solutions/internet/CSY0010UQ.html
- **RSA BSAFE SSL-C commercial product**
  http://www.rsasecurity.com/products/bsafe/sslc.html

hp e3000

internet security



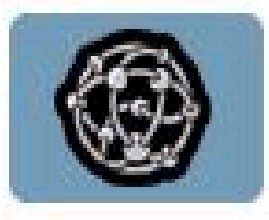
join the hp3000-l community

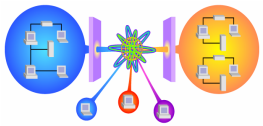


- Available as a mailing list and as the Usenet newsgroup comp.sys.hp.mpe
- In-depth discussions of all things HP e3000
- Talk with other e3000 users
  - **seek advice, exchange tips & techniques**
- Keep up with the latest HP e3000 news
- Interact with CSY
- **`http://jazz.external.hp.com/papers/hp3000-info.html`**

hp e3000

internet security





Questions?