



High Assurance Trusted
e-Commerce & PKI Servers

ACSAC, December 9, 1999

Paul A. McNabb
Vice President and CTO



Summary

- ◆ **New commercial Internet architectures are demanding new security technologies**
- ◆ **A new generation of trusted operating systems has come out of the commercial market**
- ◆ **TOS technology enables mission critical architectures for e-commerce and PKI**

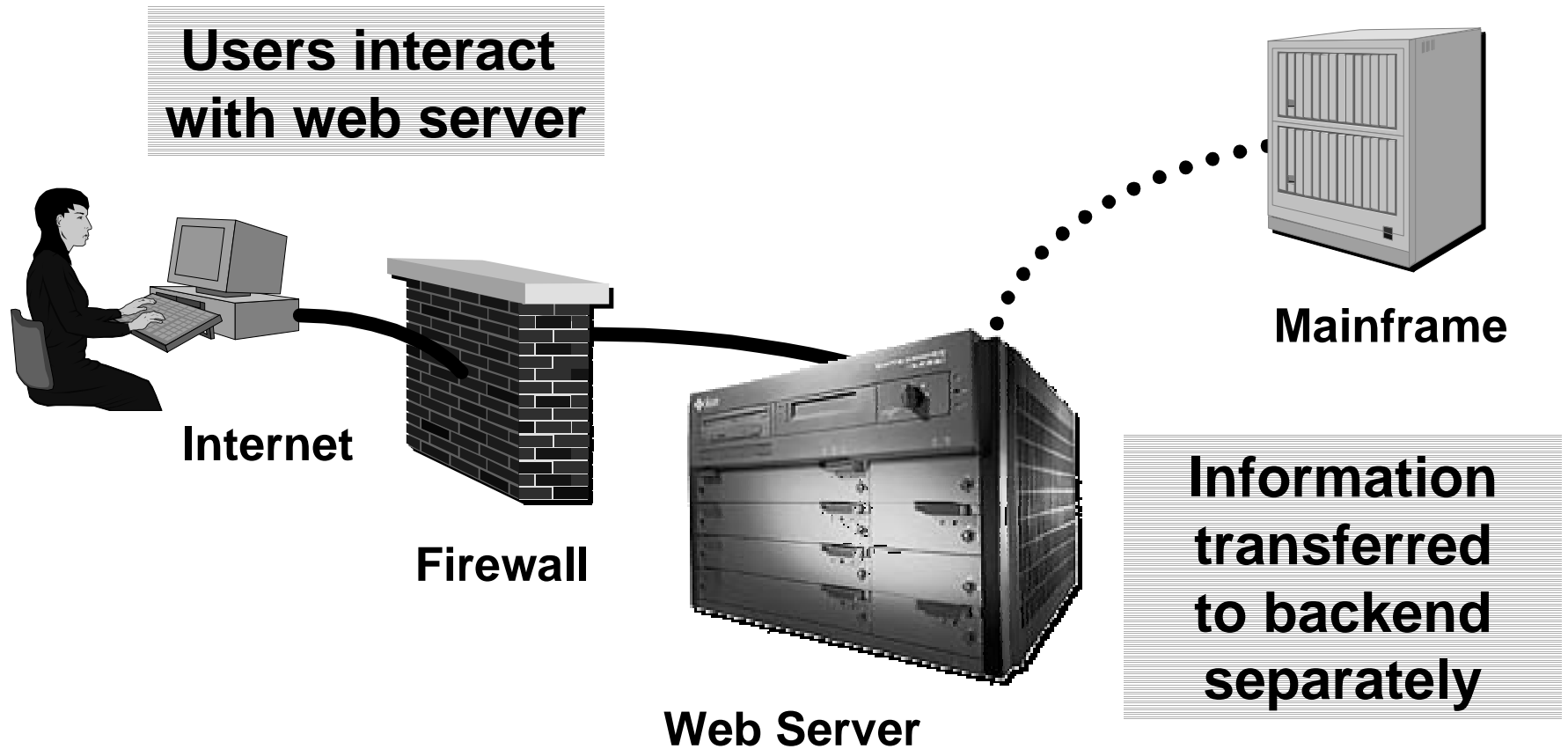


Advanced Internet Architectures

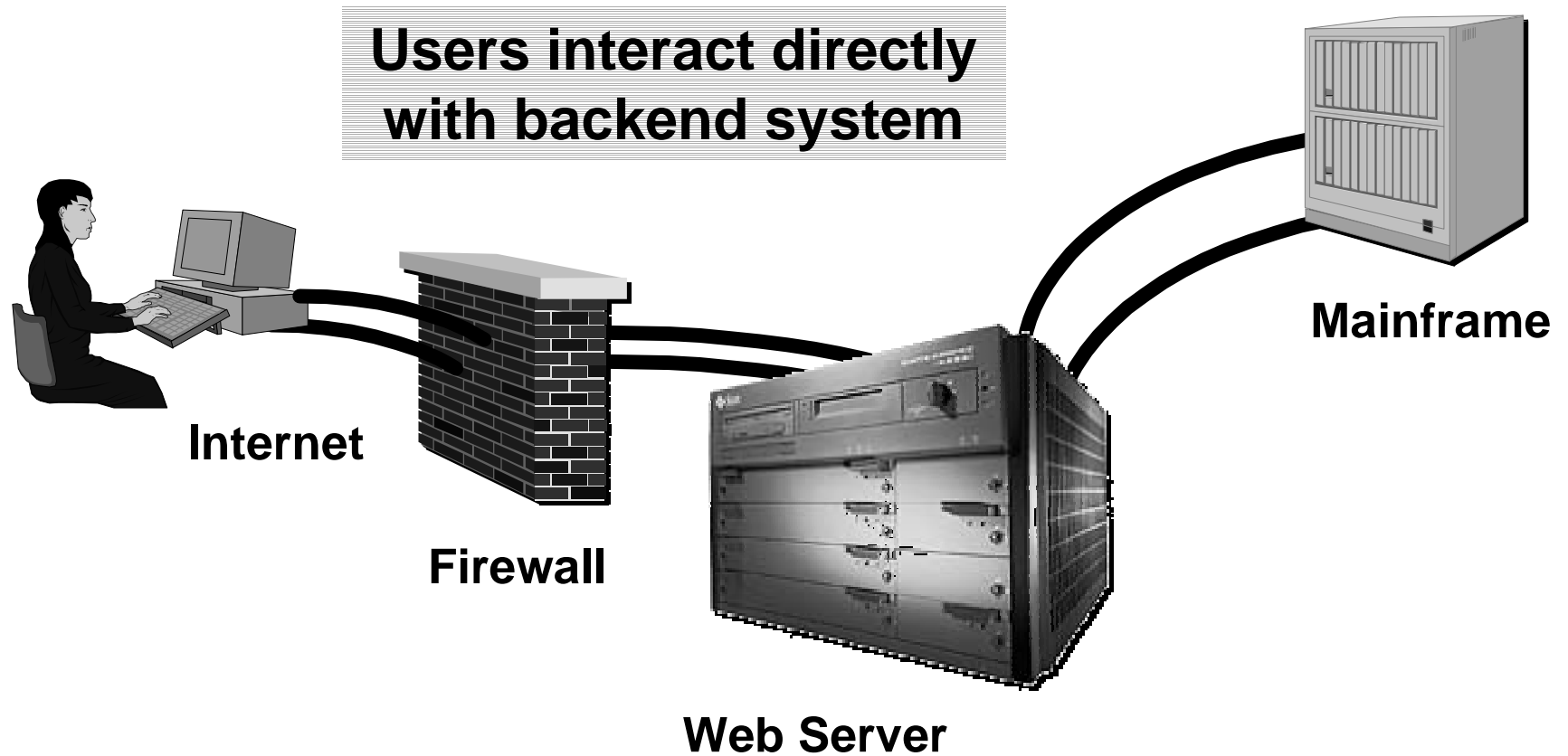
Paradigm Shifts

- ◆ **Collapsing Walls**
 - ◆ **Perimeters cannot easily be defined**
 - ◆ **Perimeters of networks are no longer defensible**
- ◆ **Internet as a Transaction Platform**
 - ◆ **Transaction servers will be attacked for their financial assets and information**
 - ◆ **Transaction servers have become gateways to backend systems and networks**

Traditional Web Server



Direct Transaction Server



Direct Connect Model

Security Challenge

- ◆ **Opens a new high-speed, direct conduit to sensitive back-end systems**
- ◆ **Commercial, third party applications are running on critical “gateway” systems**

E-Commerce Systems Under Attack

As E-Commerce Grows So Does Crime

In a 1999 Computer Security Institute/FBI study of 521 large organizations—including banks and government agencies—

- ◆ 62% of respondents had experienced security breaches over the past 12 months.
- ◆ 21% answered “don’t know”
 - ◆ 91% utilize firewalls
 - ◆ 98% use anti-virus software
 - ◆ 93% deploy access control
 - ◆ 42% have intrusion detection

PKI Hacker Threats

- ◆ **“By 2002, 80% of businesses using a PKI to support e-commerce applications or extranets will experience hacking attacks against the PKI components....”**

-Gartner Group Research Note

“Network Security for Public Key Infrastructures”

6 August 1999

Certificate Authority Endorsement

- ◆ **“The certificate authority and repository should run on hardened OSs. For high-sensitivity environments, we recommend use of OSs designed to meet B1 principles....”**

-Gartner Group Research Note

“Network Security for Public Key Infrastructures”

6 August 1999



T e c h n o l o g y S u m m a r y

T r u s t e d O p e r a t i n g S y s t e m s

Unassailable Security Fact

“The threats posed by the modern computing environment cannot be addressed without secure operating systems. Any security effort which ignores this fact can only result in a ‘fortress built upon sand.’”

-- The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments

Loscocco, Smalley, Muckelbauer, Taylor, Turner, and Farrell
National Security Agency

Traditional Security

- ◆ **Firewalls**
- ◆ **Encryption**
 - ◆ **Network Encryption**
 - ◆ **Public Key Infrastructure (PKI)**
- ◆ **Authentication**
 - ◆ **Digital Certificates**
 - ◆ **Access Tokens**
- ◆ **Intrusion Detection**
- ◆ ***Hardened* Operating Systems**

Where does a Trusted OS fit?

- ◆ **A TOS doesn't take the place of encryption, firewalls, intrusion detection, or authentication mechanisms**
- ◆ **It adds extra layer of security that can strengthen other security mechanisms**
- ◆ **It provides strong platform and network interface security for Internet-based commercial applications**
- ◆ **It prevents damage outside of a partition, and limits damage from buffer overflows**

Capabilities Unique to the OS

There are certain threats and risks that can only be controlled via the operating system:

- ◆ **Stack overwrite bugs**
- ◆ **Administrator hijacking**
- ◆ **Multi-network communication**
- ◆ **Improper application interaction**
- ◆ **Other COTS/middleware software bugs**

The OS can impose controls on all software.

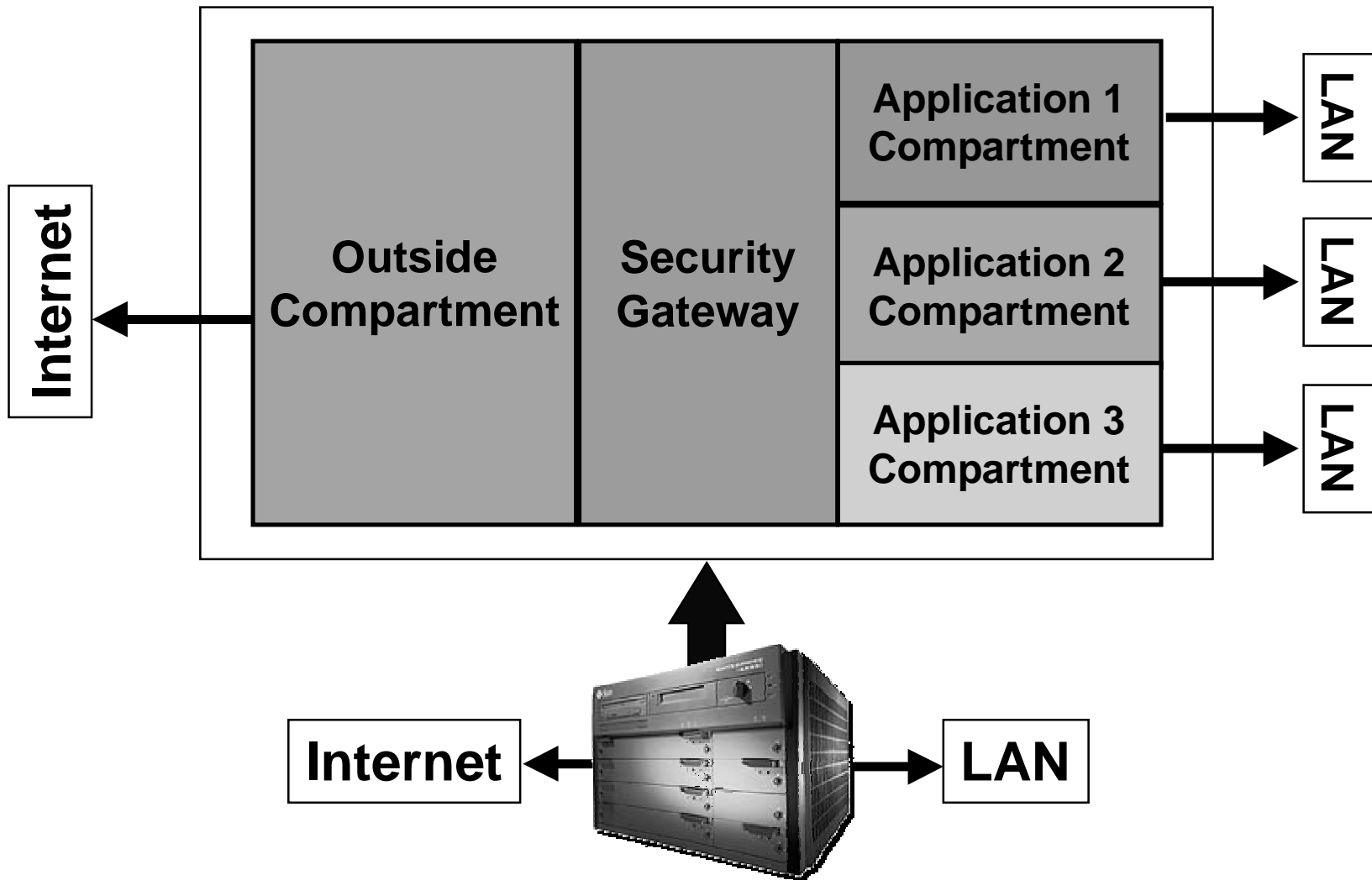
Trusted OS Product Generations

Characteristic	1st Generation	2nd Generation	3rd Generation
Emphasis	Access Control	Access + Admin	Access + Admin + Integration
Feature Set	Very Limited	Moderate	Very Rich
Configurability	None	Limited	Extensive
Networking	No MLS	MLS	MLS+
Installation	Replace OS	Replace OS	Upgrade OS
Interface	Command Line	Graphical	Browser
Criteria/Eval	TCSEC	TCSEC / ITSEC	CC

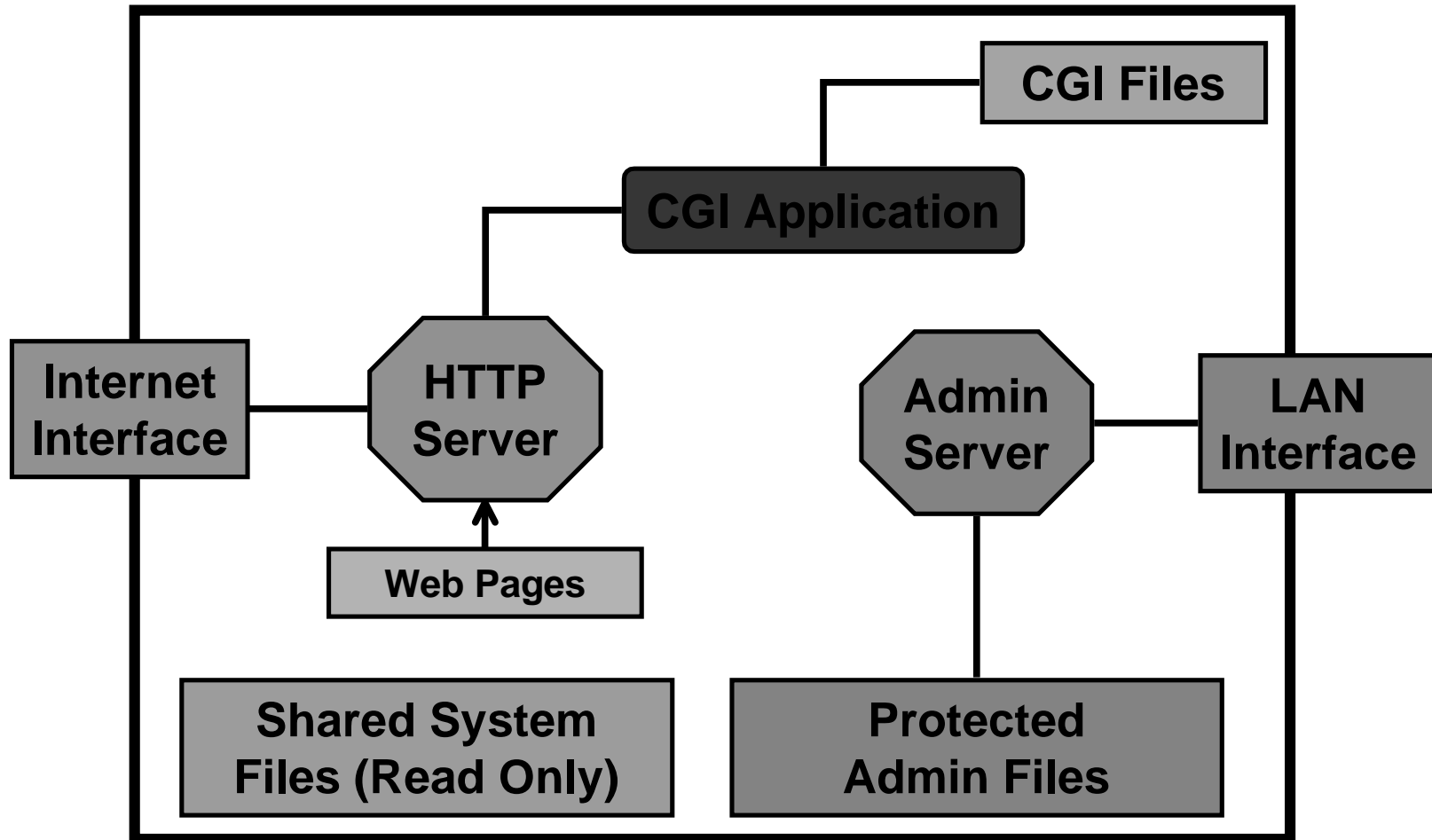
Trusted OS Trend

- ◆ **Losing image of old DoD systems**
- ◆ **Being designed to meet commercial stability and functionality requirements**
- ◆ **Becoming requirement for direct transaction servers**
- ◆ **Becoming part of the standard toolkit for security professionals securing high risk environments.**

Multiple Compartment Isolation



Isolated System Compartments

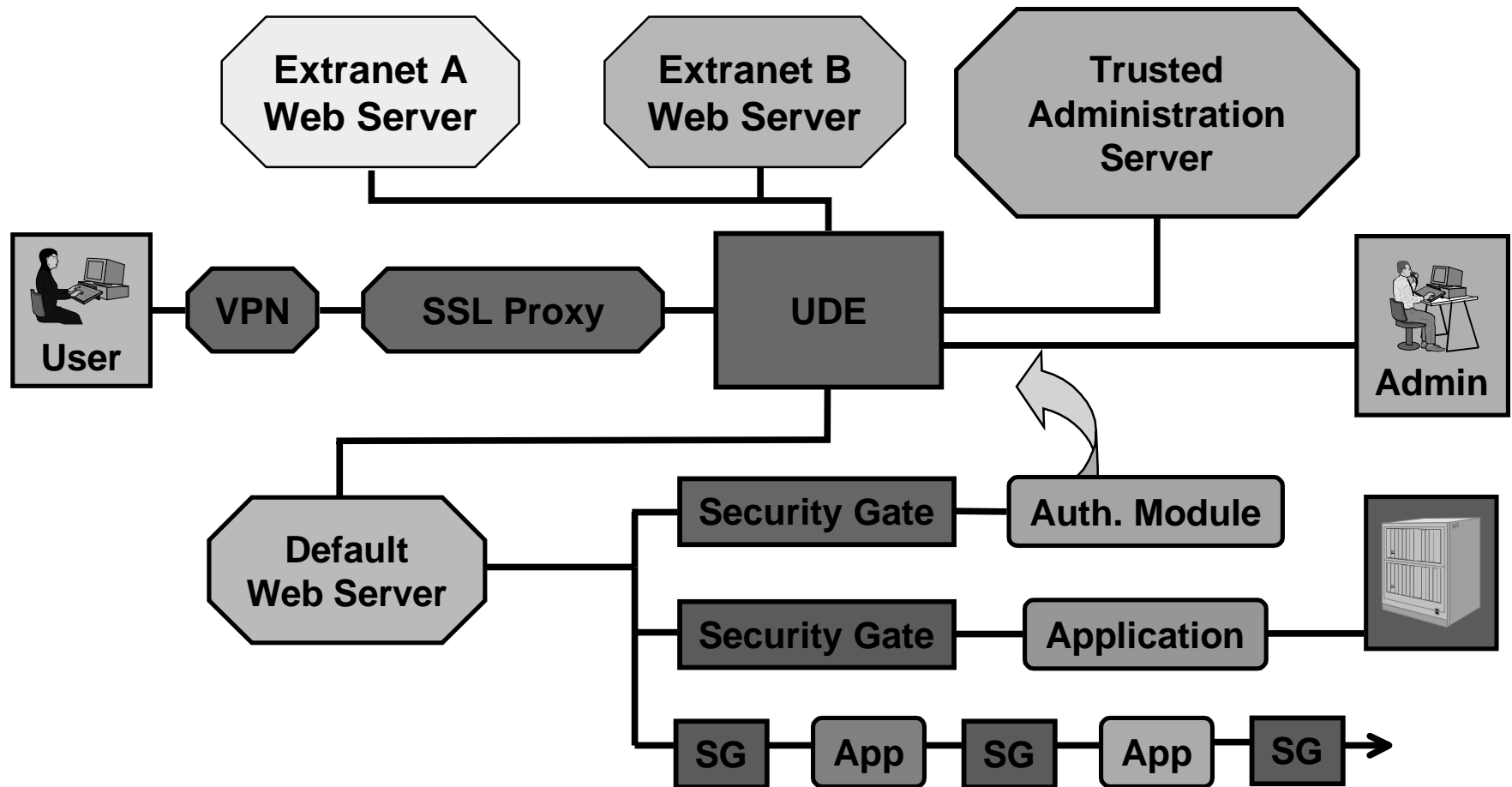




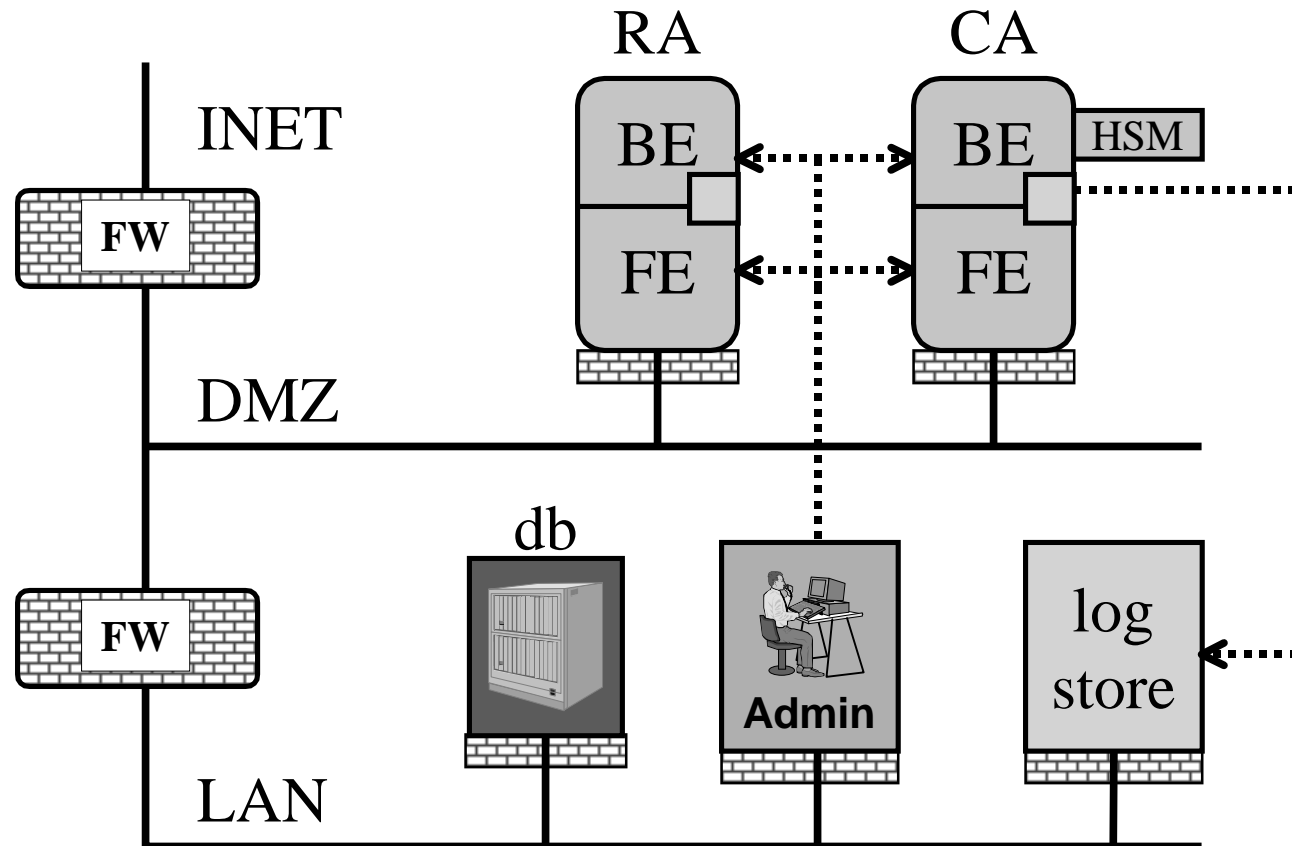
T OS -enabled

Architectures and Solutions

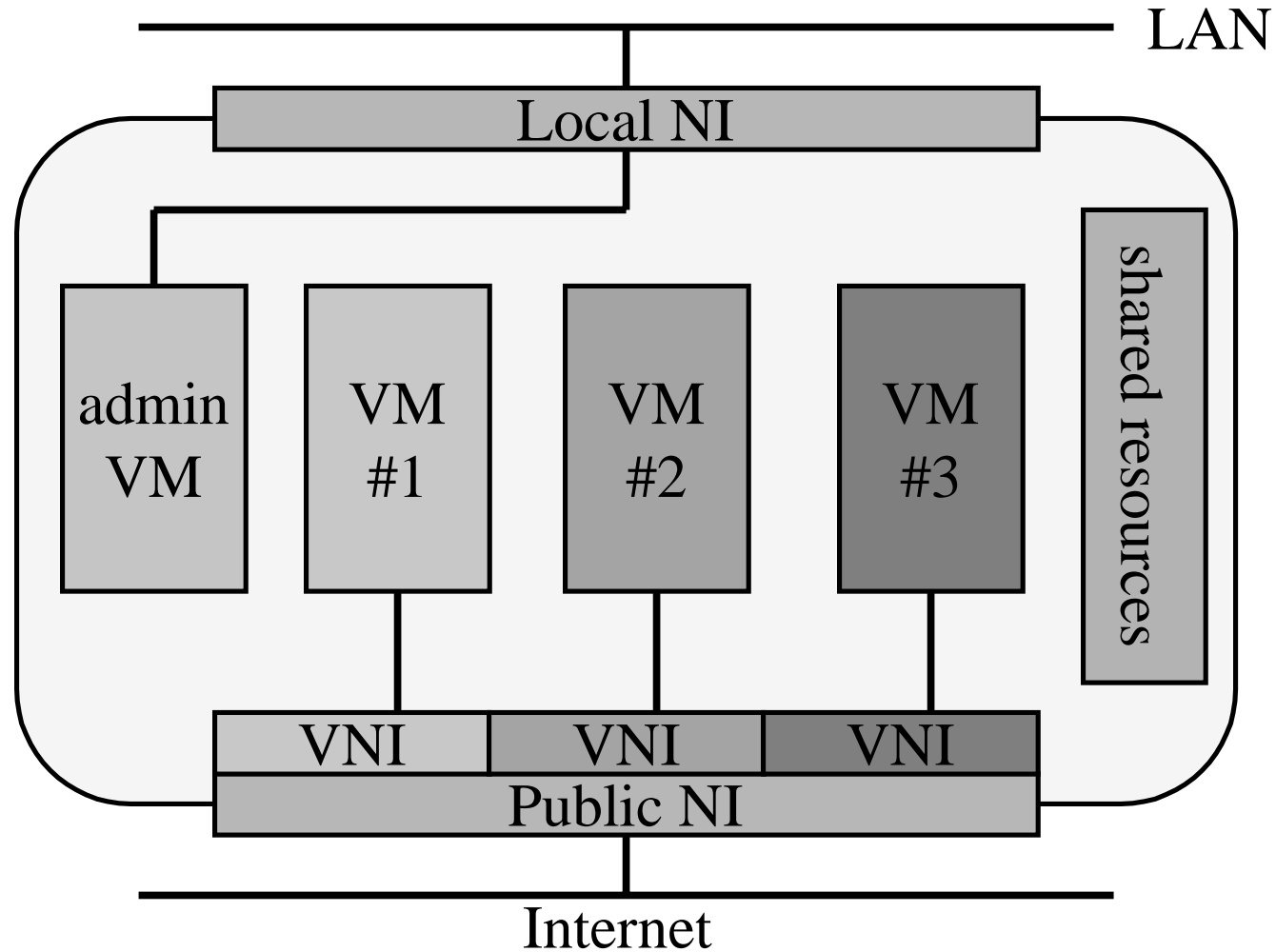
T OS -based Webserver Architectures



T OS -based PKI Architectures



Virtual MLS Machines for AS P /CS P



High-End Secure Environments



- ◆ **Electronic Commerce**
- ◆ **Internet Banking / Finance**
- ◆ **Multilevel Intranet http Servers**
- ◆ **Multi-National Commands**
- ◆ **Multi-Disciplined Collection Transaction Database Servers**
- ◆ **Medical/Health Services**
- ◆ **Secure Web Servers**
- ◆ **PKI / Certificate Authorities**
- ◆ **Trusted Firewalls**

Argus Products

- ◆ **PitBull**

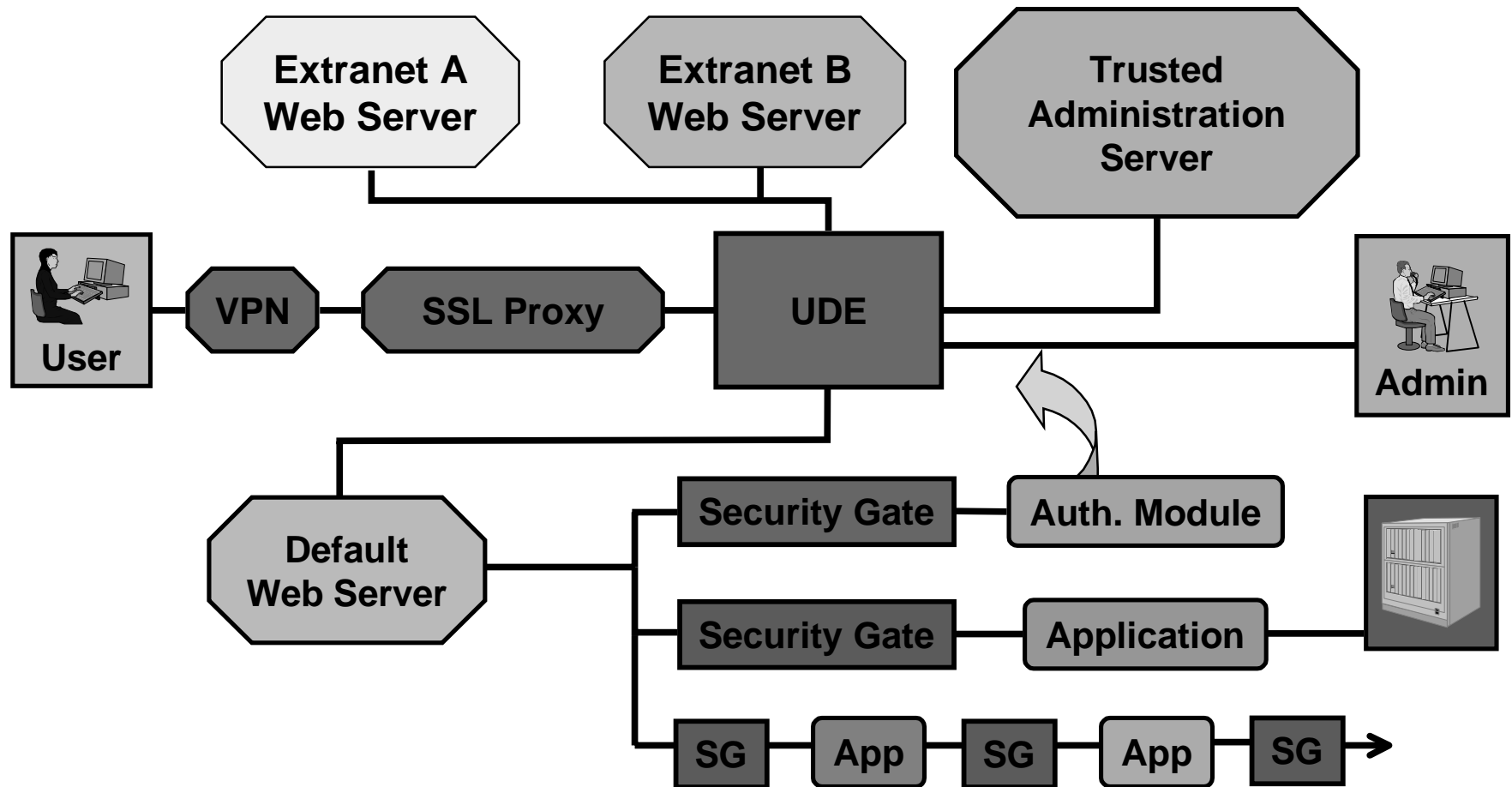
A third generation trusted OS undergoing CC LSPP/EAL4 evaluation. Available on:

- ◆ Sun Solaris (2.5.1, 7, 8; SPARC & x86)
- ◆ IBM AIX (4.3.2, 4.3.3)
- ◆ SCO Unixware (7.1)

- ◆ **Gibraltar**

A complete e-platform architecture based on PitBull and running on the same platforms.

Gibraltar Product Architecture



Summary

- ◆ **New commercial Internet architectures are demanding new security technologies**
- ◆ **A new generation of trusted operating systems has come out of the commercial market**
- ◆ **TOS technology enables mission critical architectures for e-commerce and PKI**



Argus Systems

**Securing the
Future**

 **ARGUS**
SYSTEMS GROUP, INCORPORATED

For More Information



www.argus-systems.com



info@argus-systems.com



Tel: 217-355-6308
Fax: 217-355-1433



1809 Woodfield Drive
Savoy, IL 61874 USA