Data Interoperability & Data Handling Framework

PST 2005, October 14th, 2005

Robin T Wakefield
Senior Security Analyst

Agenda

- Who is Sun? Who Am I?
- Data Interoperability
  - Background & Challenges
- Data Handling Framework
  - SunRay and Trusted Solaris
  - Secure Network Access Platform
    - Case Study
  - Multi Layer Gateway
  - Secure Data store
- Case Study

Who is Sun?

- Sun’s Security Vision is to be the premier provider of secure network computing products, technologies, and services delivering comprehensive solutions that enable customers to manage risk and engender trust
- Security is baked into every product
- Evolutionary processes to deliver and solve security concerns
- Focussed security people
- Managed security services

Who Am I? I am an Analyst

- Over 25 years of experience with extensive knowledge in computational security
- Spent the last 8 years under Sun Microsystem’s CTO as a Senior Security Analyst in the Global Security Practice
- Worked abroad at highly sensitive date centres and difficult customers
- Founding member of the Honeynet project
- Published security papers for Sun Microsystems

Who Am I? I am an Analyst

- Security and Privacy Analyst for Sun Microsystems of Canada
- Advisor for research directed by Public Safety and Solicitor General in BC and consult to CIO's office
- Member of ICURS - undertake projects in criminology and public safety for government and law enforcement
- Preparing doctoral thesis and developing post graduate courses at UCFV & SFU
- Developing a Centre of Excellence in Computational Safety and Security

Background

- ICURS receives data from many diversified sources
- Data ranges from Classified to Open Source
- Different consumers of information
- Security & Privacy compliance verses Info Sharing
- Rigorous physical requirements for the labs and data centre
- Rigorous audit requirements
- Improved paradigm for data management

Data Interoperability

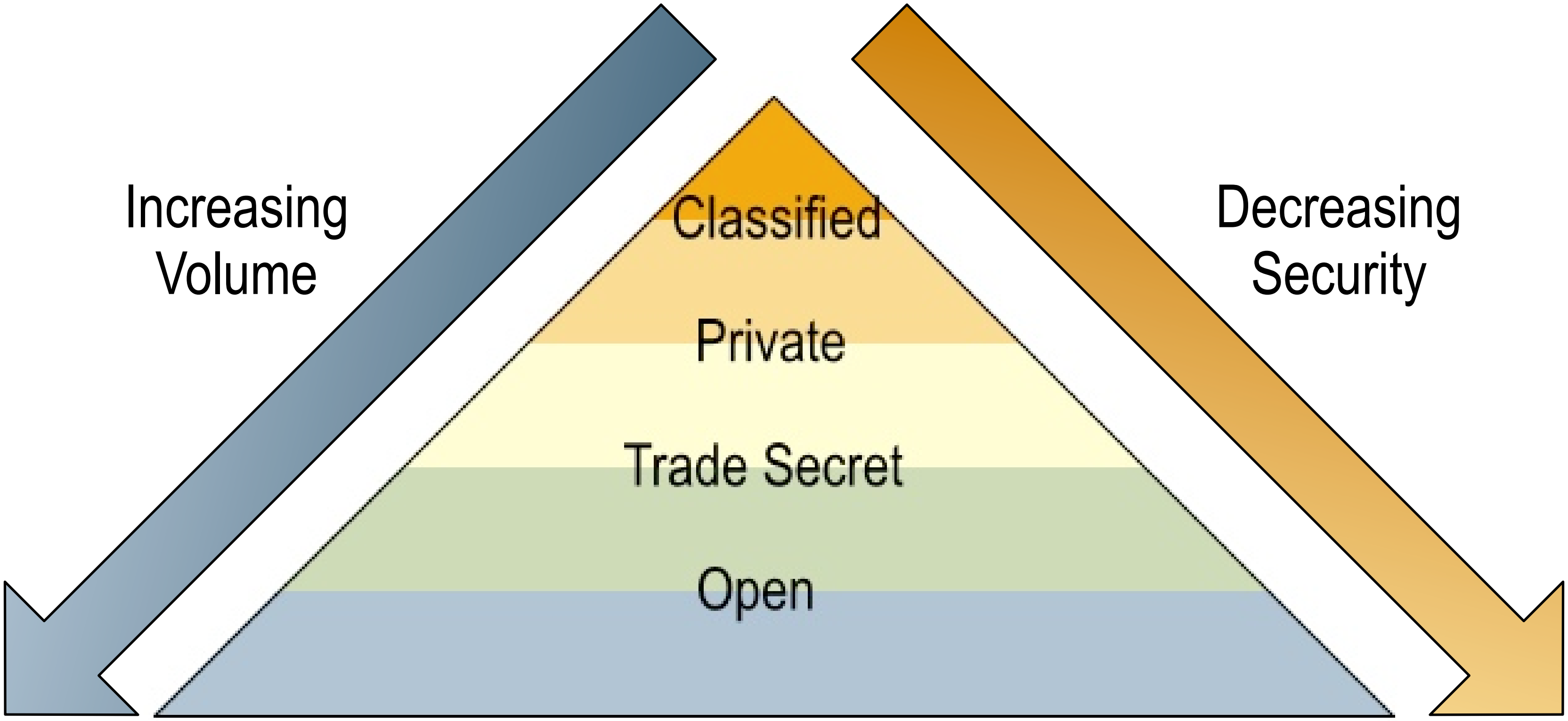
Data Sources

Law Enforcement & Military	Covert, HUMINT, SIGINT, IMINT, Ops, Criminal Records, Security
Government	Government LOB, Financial (taxation), Health (Vital Stats)
Crown Corporations & NGO	Utilities, Financial, Health Care, Public Safety, Labor, Enviro, Edu
Commercial	FIs (Banks, Credit), Transport Auth, Research (DT, IDC), Foreign Biz
Open Source	Print Media, Television, Internet

Data Sensitivity

Law Enforcement & Military	Classified
Government	Personal Information (PHI)
Crown Corporations & NGO	PI. PHI, Trade Secret
Commercial	Trade Secret
Open Source	None

Data State



Increasing Volume

Classified

Private

Trade Secret

Open

Decreasing Security

Consumers of Information

- Academia (models and algorithms)
- Policy Makers
- Support Operations
  - Law Enforcement
  - Military
  - Academic Computing Services (data centre)

Security & Privacy vs. Information

The emerging challenge is balancing the need for security and privacy with the need for increased information sharing and responsiveness.

> *“Defense intelligence is starting to come around to the idea that not sharing information is now a bigger threat than the people we’re trying to protect from it”*

Dr. Ryan Durante, DTW program manager, U.S.A.F. Research Laboratory

Security & Privacy vs. Information

This challenge applies to more than just defense and intelligence agencies. For example:

- Commercial crime (money laundering, fraud, identity theft)
- Organized crime (grow ops, cocaine and heroin in transit, crystal meth, auto theft, sex crimes)
- School violence (safe schools)
- Accident investigation (commercial vehicles)
- Health emergencies and drug abuse (avian flu, safe injection sites)

Physical Requirements

- Remote laboratories
  - Keyed access
  - Computers locked-down
  - 7x 24 monitoring
  - Highly controlled communications
- Central data centre
  - Caged racks over raised floor
  - Isolated power, cooling and wiring conduits
  - 7 x 24 monitoring
  - Extensive perimeter security controls
  - Highly controlled communications

Computational Requirements

- High Powered Computers
  - computing grid (processors and memory)
- Scalable data storage fabric (SANS, archive, video)
- Not so smart workstations
- High Speed Networks and Switching
- Extensive security devices (firewalls, IDS, etc)
- Identity Management and Audit software
- Data base software
- Application code that takes advantage of HPC

Great People

- Great consumers and clients
  - leaders and visionaries
  - dedicated to the process
- Great researchers (security clearances)
  - professors
  - grad students
- Great computer scientists
- Great IT support staff
- Great vendors

Audit Requirements

- Applicable today:
  - RCMP Security standards
  - ISO 17799, BS 7799 and ISO 13335
  - ITIL
  - PIPEDA, PIPA, FIOPPA
- Applicable as ICURS grows:
  - EU Directive
  - COBIT, COSI,
  - NIST 800 series
  - GLBA, SB1386, COPA, HIPAA, Sarbanes Oxley

Challenge

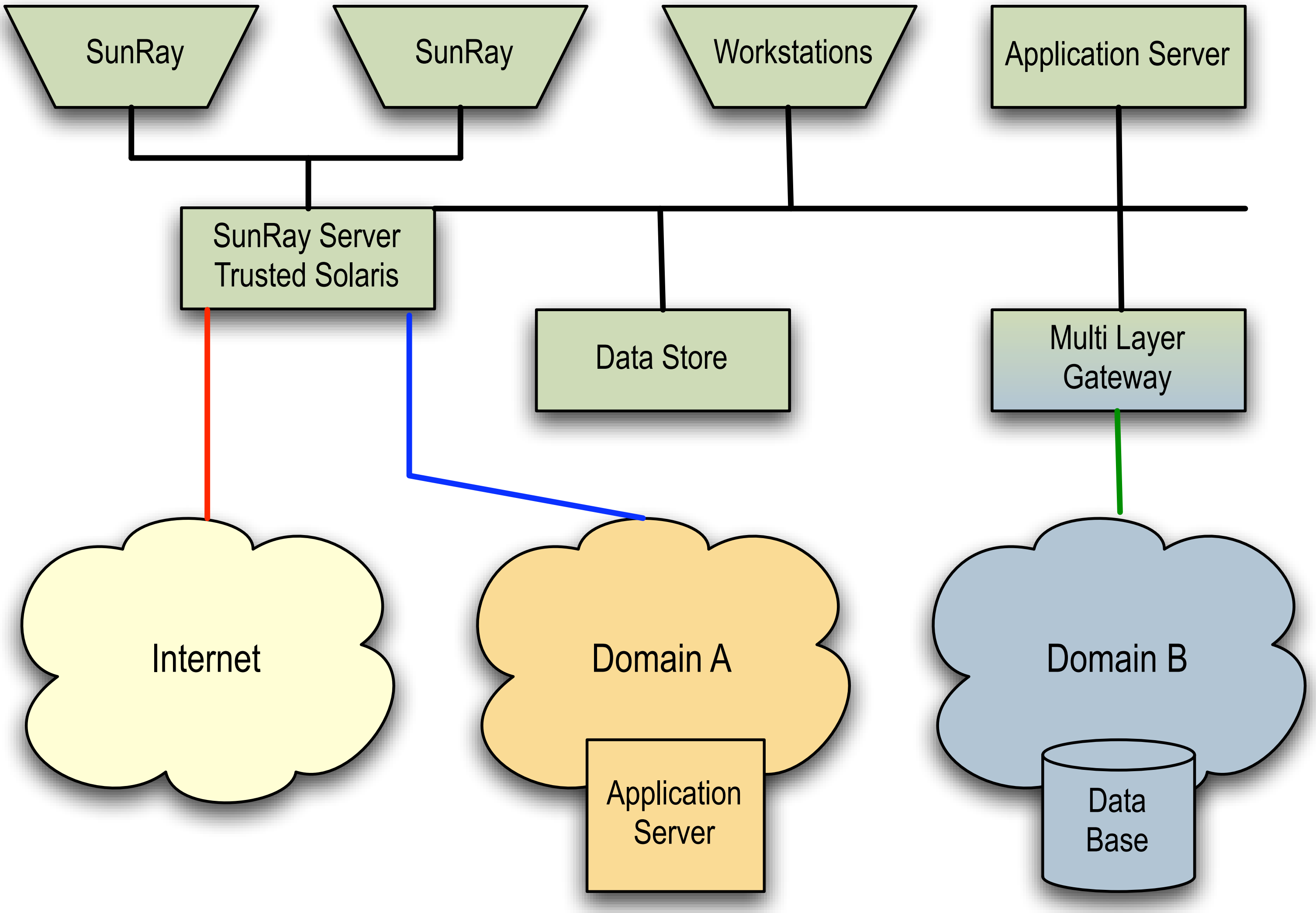
- Protection of Personally Identifiable Information
- Demanding results by very discriminating consumers
- Talented researchers and computer scientists
- Great IT people and process roadmaps
- Great IT fundamentals and infrastructure
- Multiple point solutions - engaged vendors (COE)
- A way to bring it all together

Data Handling Framework at ICURS Lab

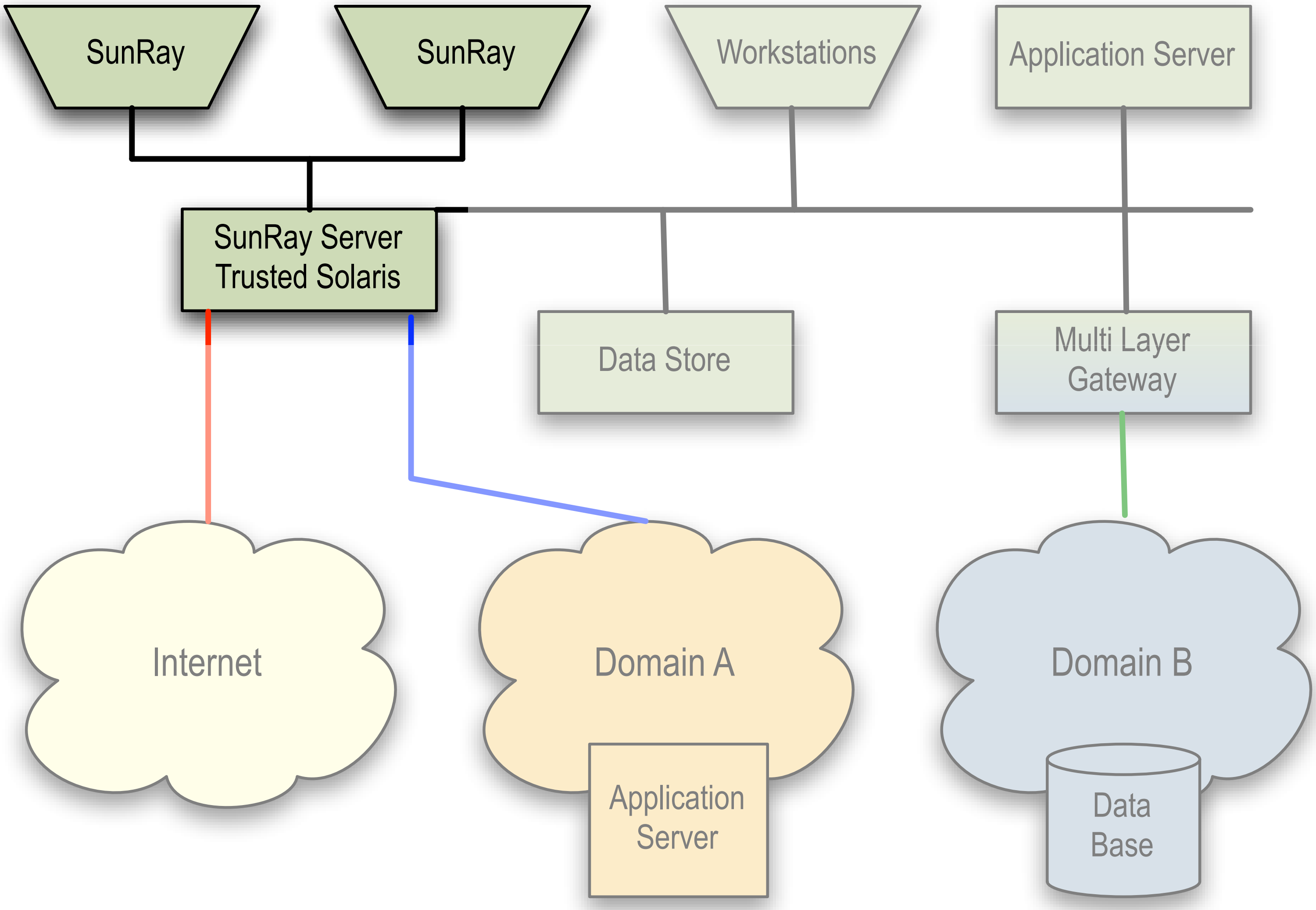
DHF

- Existing point solutions
  - Secure Network Access Platform - SNAP
  - Trusted Solaris and/or Solaris 10 with Trusted Extensions
  - Multi Layer Gateway
  - Data Store
- Case Study
- DHF approach for data interoperability

Data Handling Framework



DHF: SunRay with Trusted Solaris

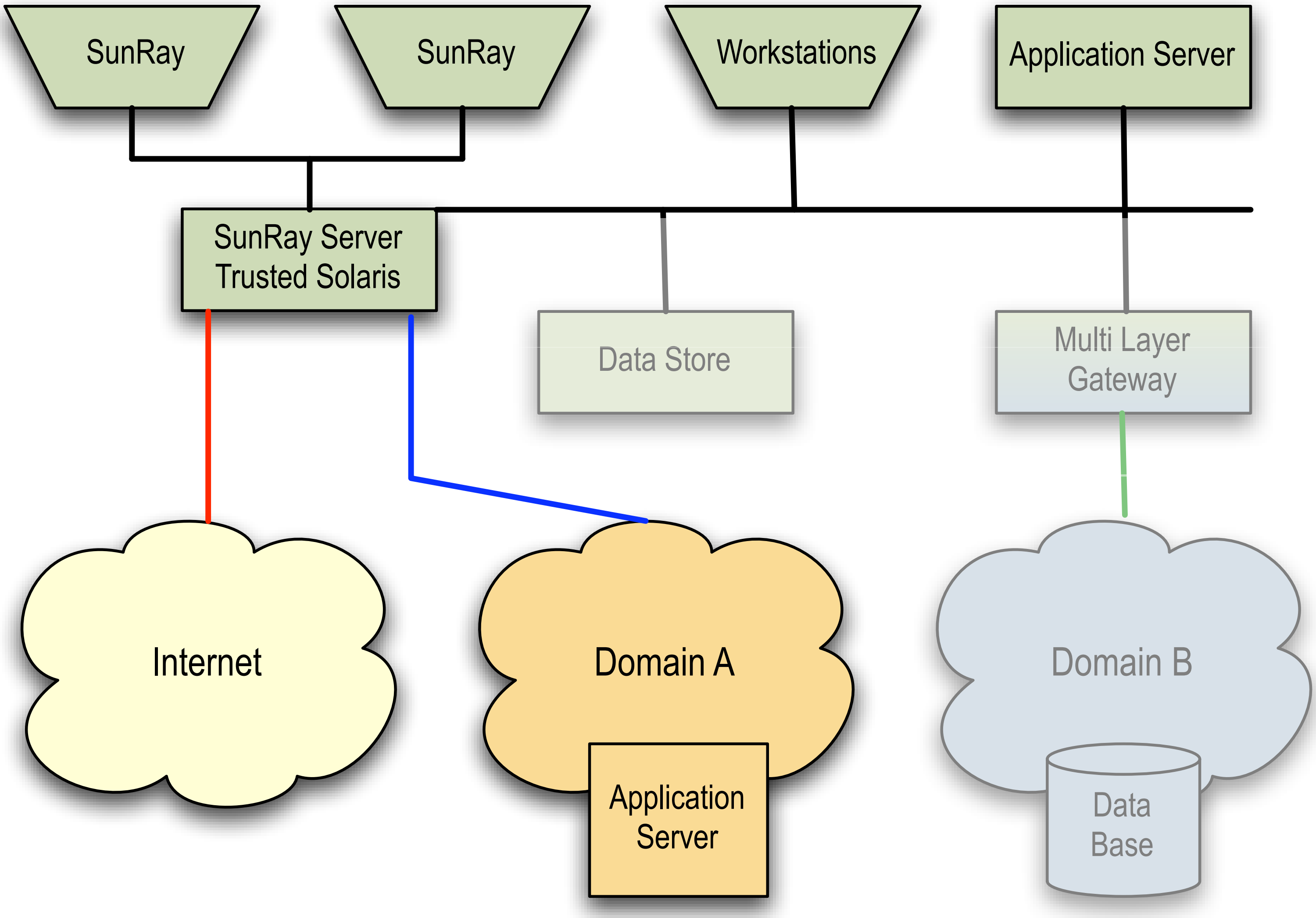


DHF: SunRay with Trusted Solaris

Trusted Solaris

- Orange Book B2 and ITSEC EAL 4
- Predicated on Bell LaPadula security model
  - write up read down - confidentiality
- Principle of Least Privilege
- Role Based Access Control (RBAC)
- Mandatory Access Control
  - Sensitivity Labels
  - Clearance Levels
- Discretionary Access Control

DHF: Secure Network Access Platform



Secure Network Access Platform

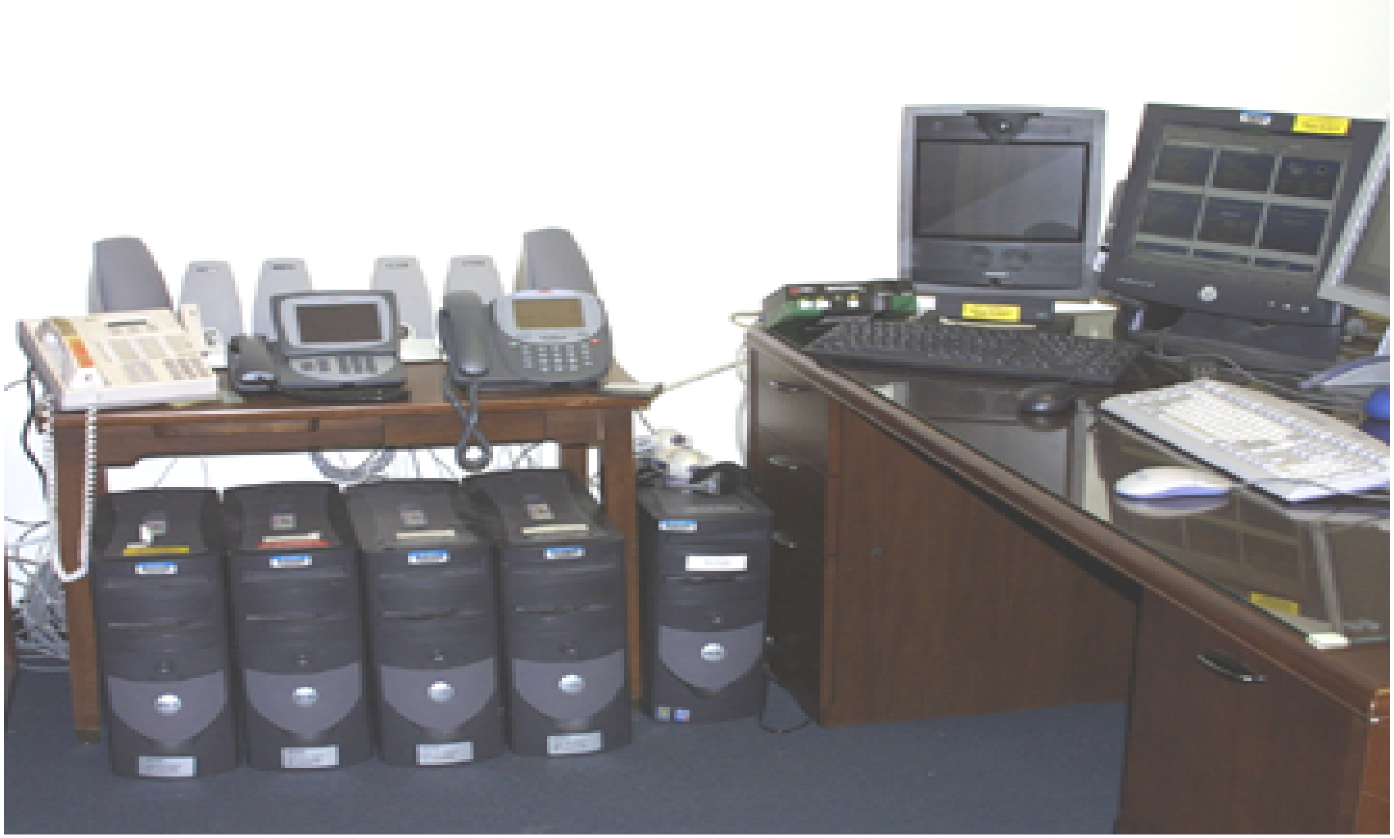
- The Secure Network Access Platform enables secure, multi-compartment access from a single, thin-client desktop system—while preserving network isolation
- Components include:
  - SunRay thin-clients
  - Javacards
  - SunRay server running on Trusted Solaris
  - Maintains network isolation

Case Study
Intelligence Analyst

System Requirements

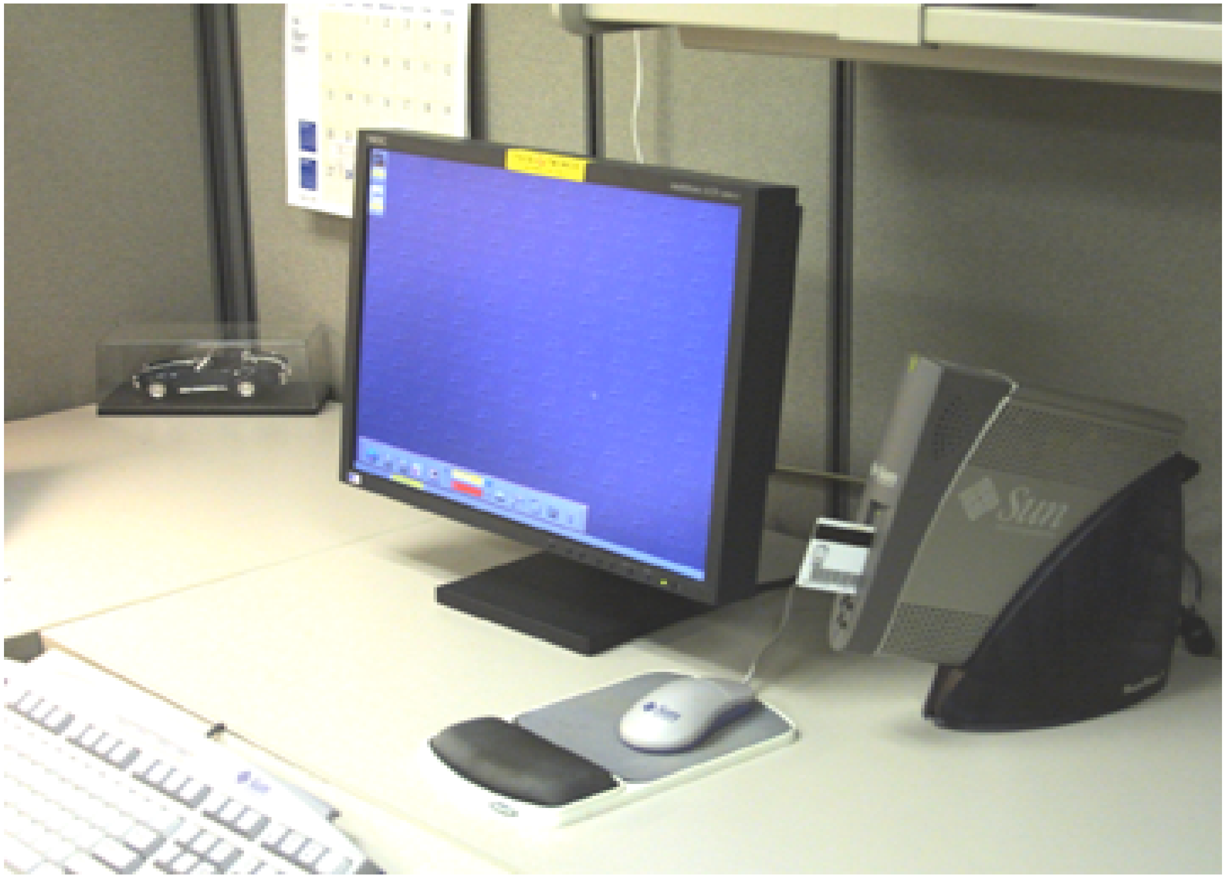
- Trusted Computing Solution
- Single Virtual Switch to Multiple Networks
  - Single desktop with connections to multiple security domains implemented as physically separated networks (without enabling intra-domain routing)
  - End-users have controlled access to domains based on security level (clearance)
- Secure Inter-Domain Data Transfer
  - Automated and manual auditing based on pre-defined policies and procedures
- Flexible Application Access
  - ICA®, RDP, X Windows, Browser

Typical Analyst’s Workspace



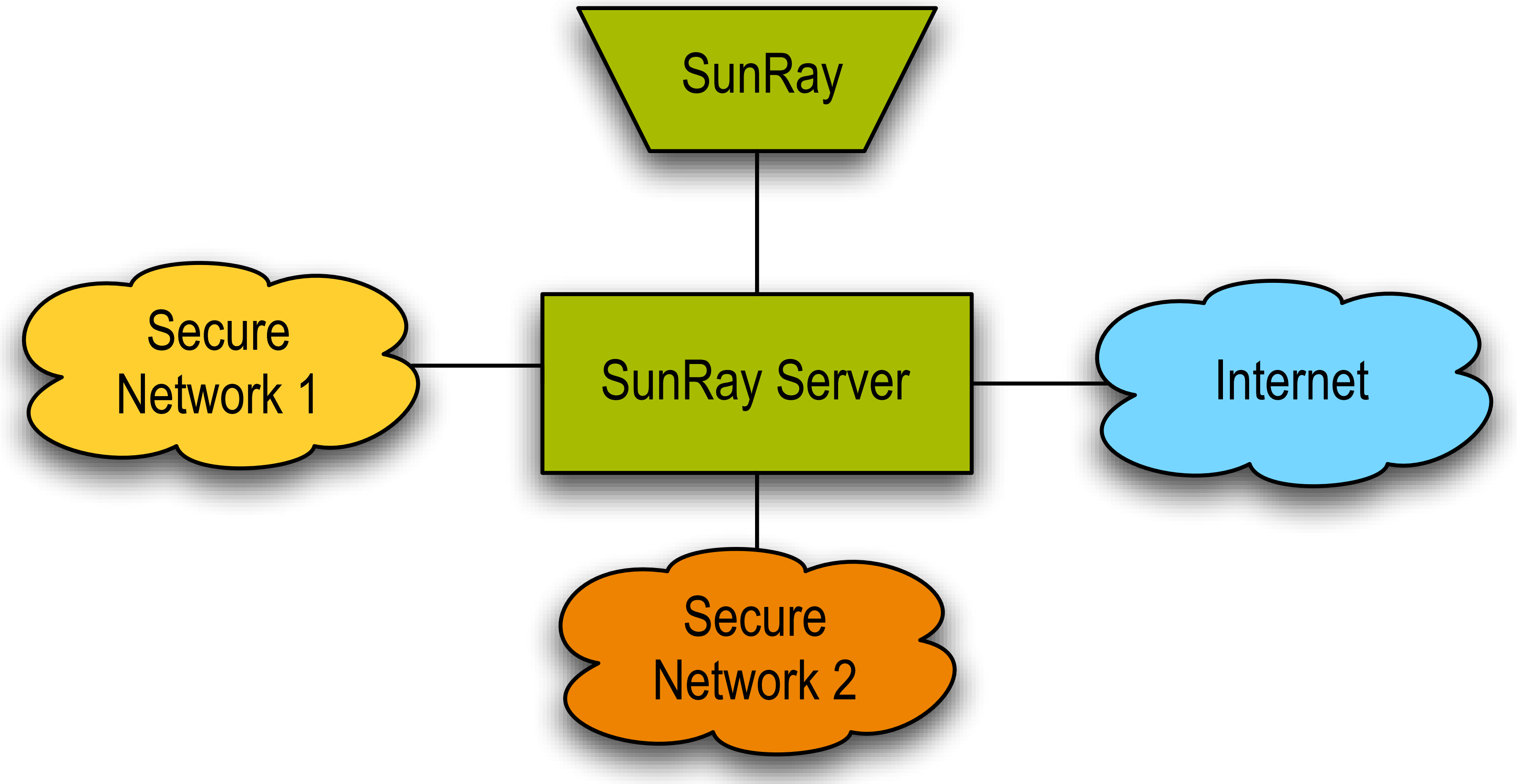
To ensure a high level of security physically isolated clients were deployed often resulting in up to 10 different PCs in a single office.

Analyst’s Workspace with SNAP

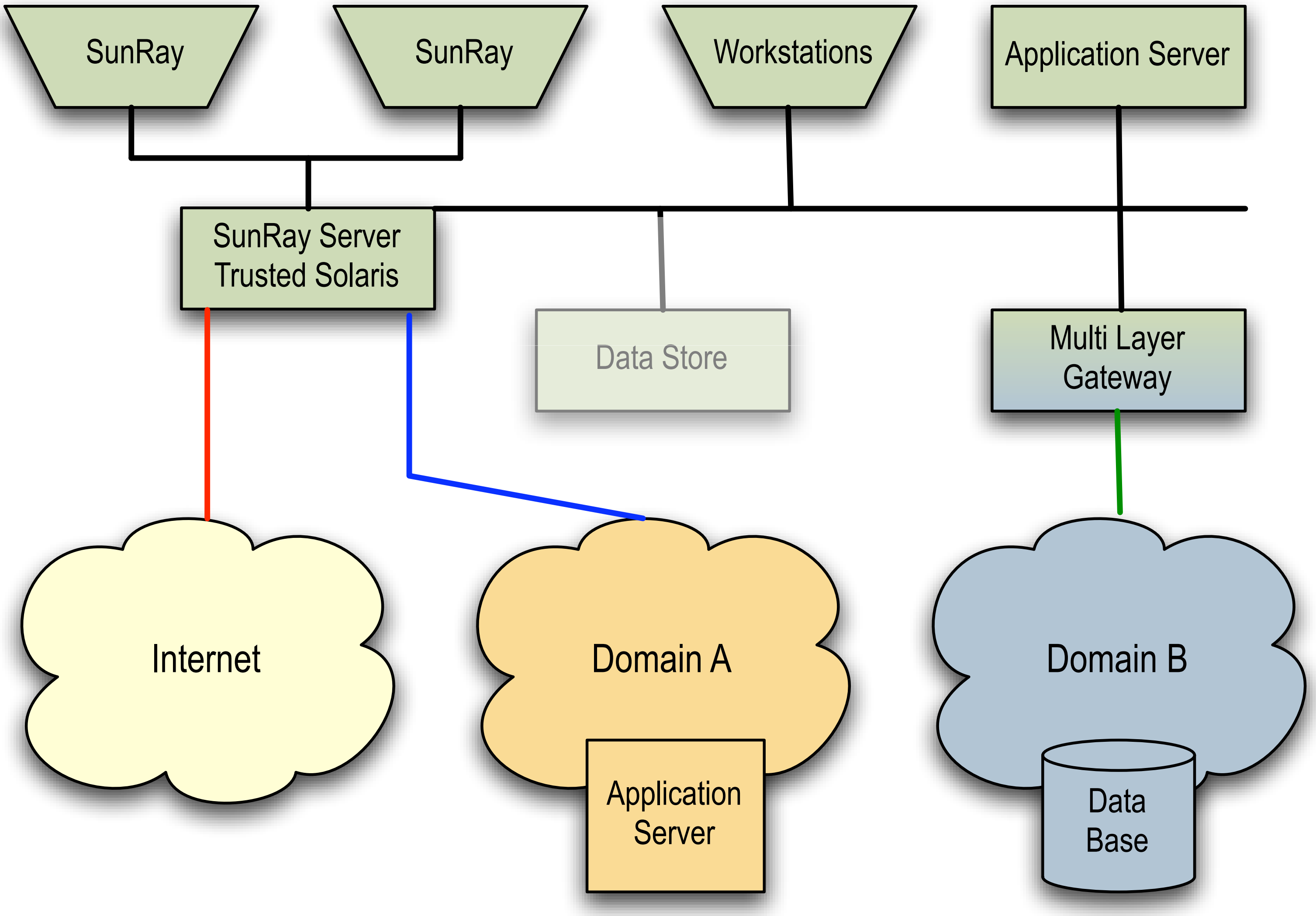


Full Session Mobility enabled by a single stateless Sun Ray(TM) front-end and protected by a Trusted Solaris(TM) based back-end

SNAP Logical Diagram



DHF: Multi Layer Gateway



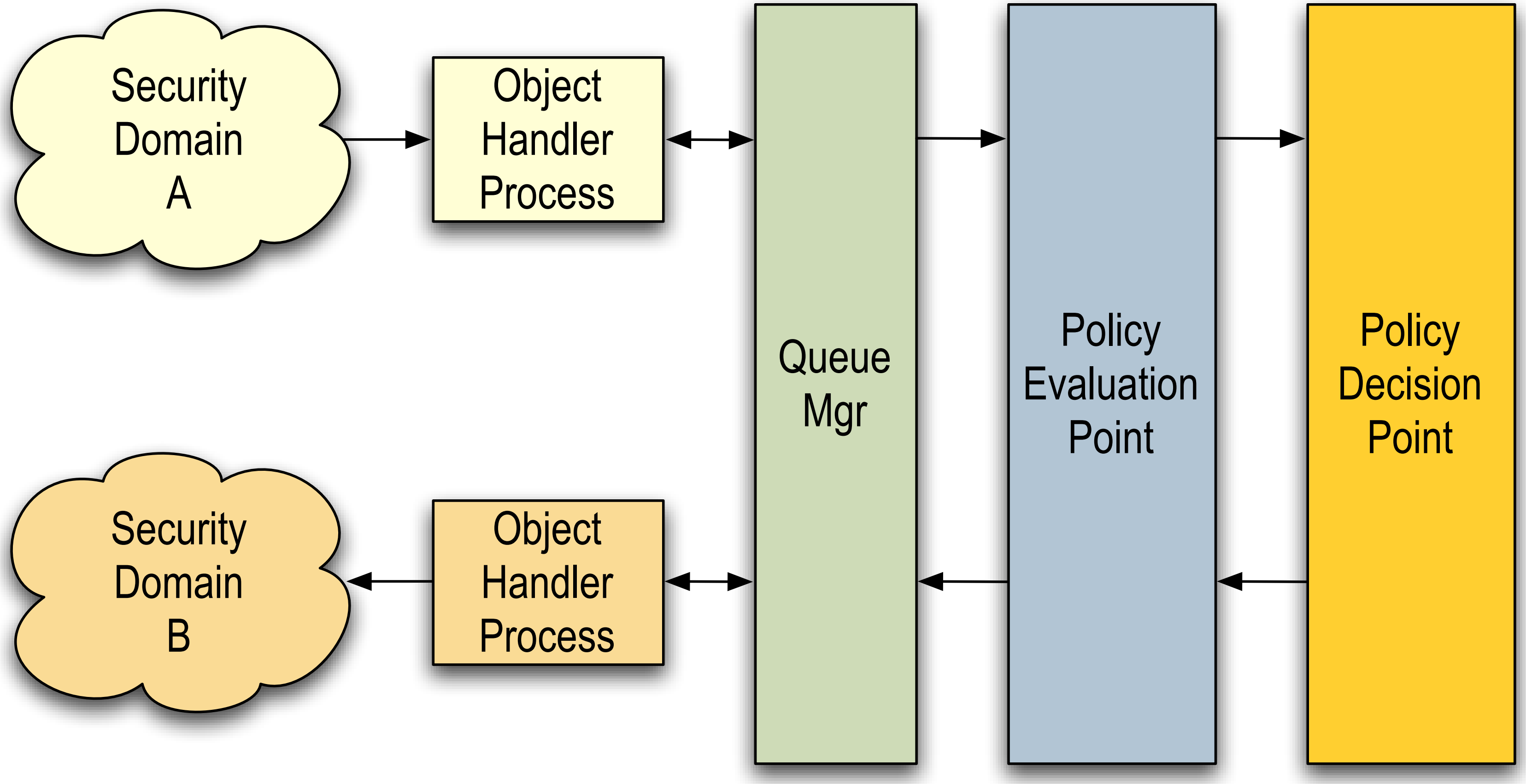
Multi-Layer Gateway

- Built on Trusted Solaris
- Everything is labeled (either directly or implied)
- Uses the two-person rule:
  - One person creates policy
  - Second person instantiates policy
- Policy consists of actions, rules and obligations that effect data
- Successful results allow data to pass
- Failure quarantines the data
- Strong audit trail

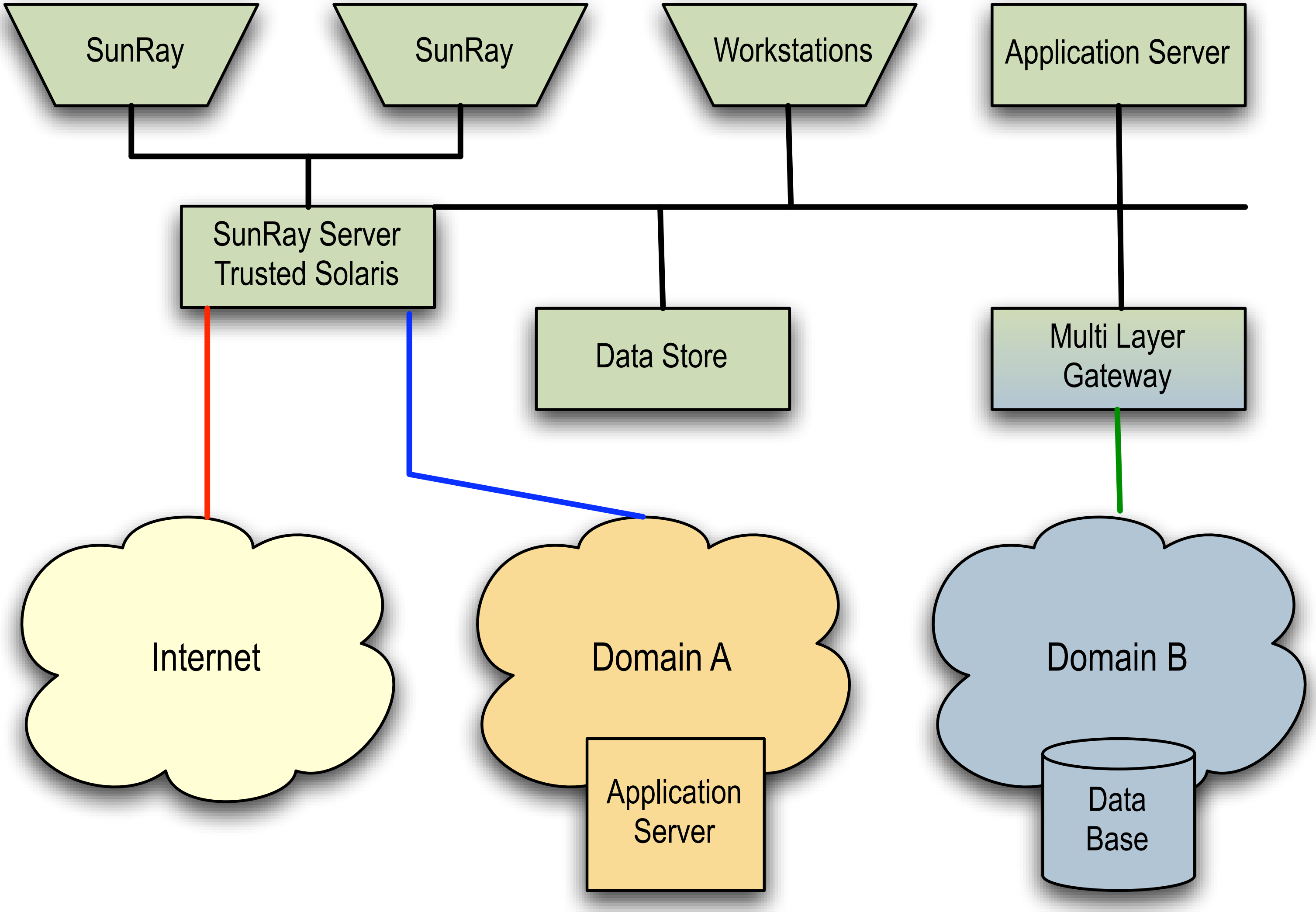
Multi-Layer Gateway

- Functionality includes
  - transferring data from one sensitivity to another
  - transferring data from one clearance to another
  - labeling unclassified data
  - redact data
    - de-identification of PI or PHI with masking
    - removal of fields from SQL queries
    - codework masking
  - dirty word quarantine (codeword)
  - tearline reporting
  - allows for other security model (Biba or Clark Wilson)

Multi-Layer Gateway: Logic



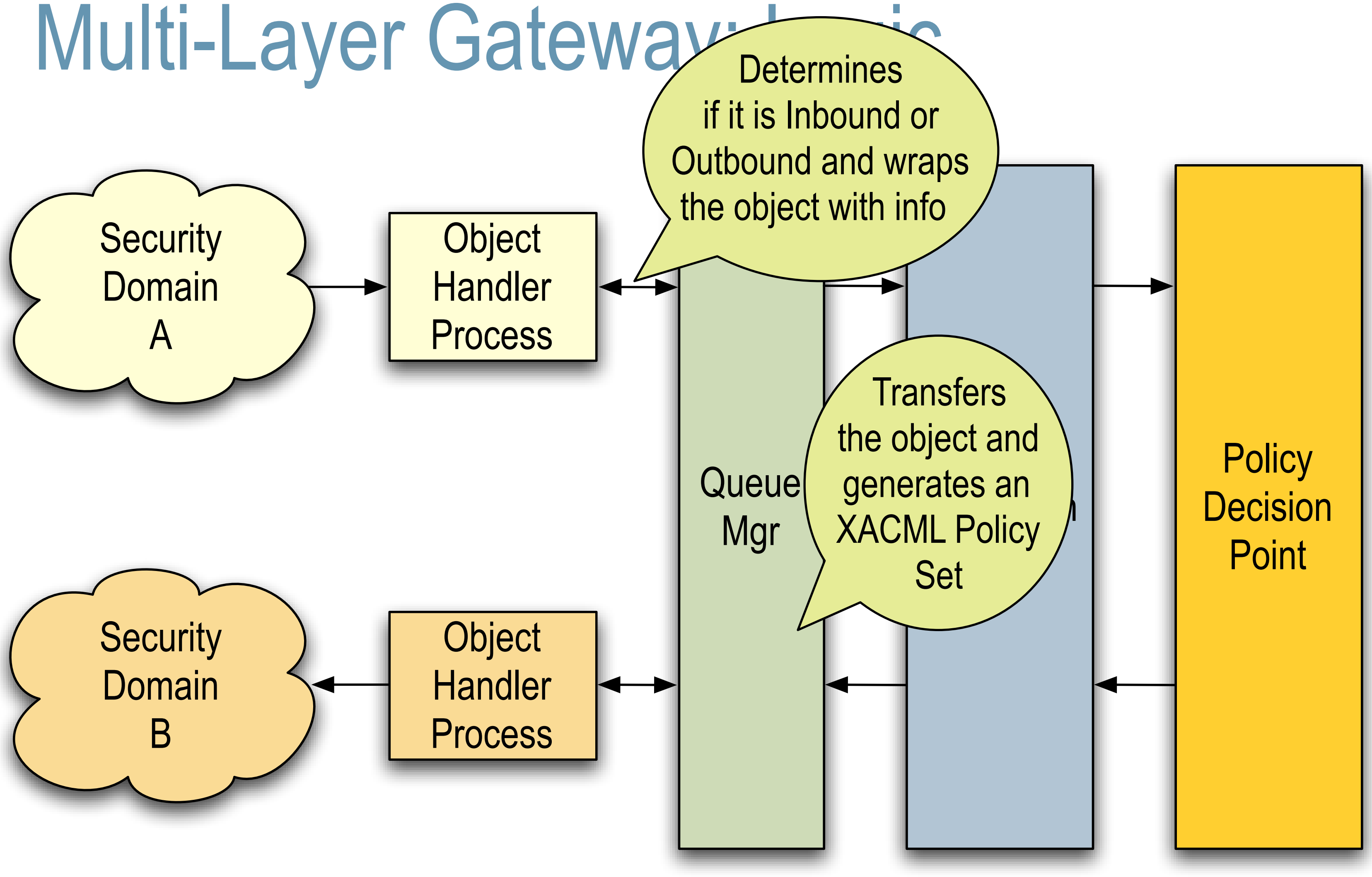
DHF: Secure Data Store



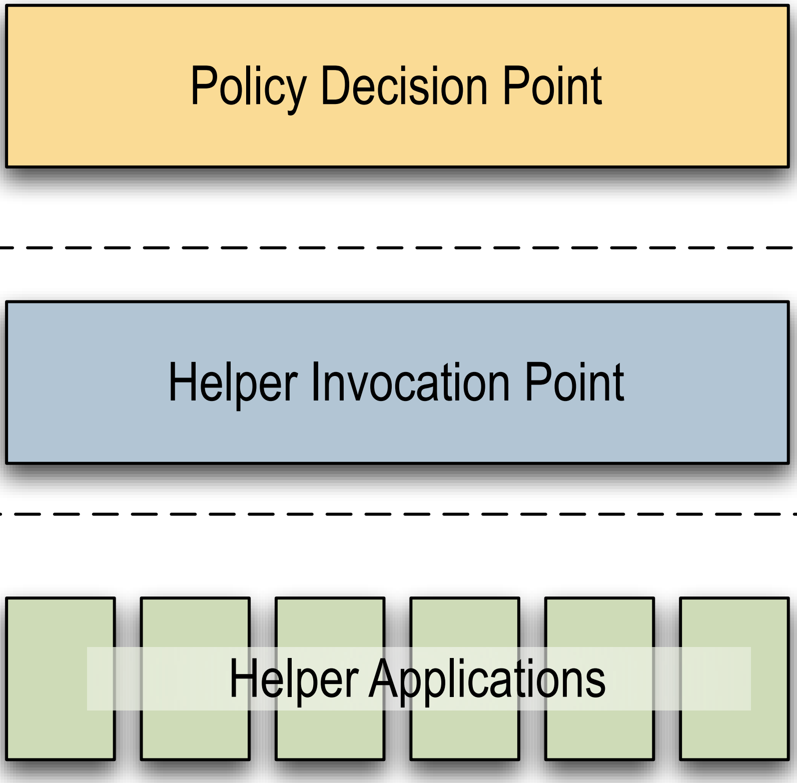
Secure Data Store

- Built on Trusted Solaris - similar to MLG
- Users check data out and check data in - RCS
- Rules driven framework
  - Allows for different rules for different security domains
  - Allows for rules to evolve over time
  - Highly adaptable
- Pluggable framework
  - New rules? Add to rules base, add helper to platform
  - Allows for stricter checking by modify helpers leaving the rules base unchanged
- Strong audit trail

Multi-Layer Gateway: Logic


Security Domain A
Object Handler Process
Security Domain B
Object Handler Process
Queue Mgr
Policy Decision Point
Determines if it is Inbound or Outbound and wraps the object with info
Transfers the object and generates an XACML Policy Set

Secure Data Store: Basic Architecture



Unprivileged

In separate compartment / zone

Policy Decision Point

Unprivileged

In separate compartment / zone

Helper Invocation Point

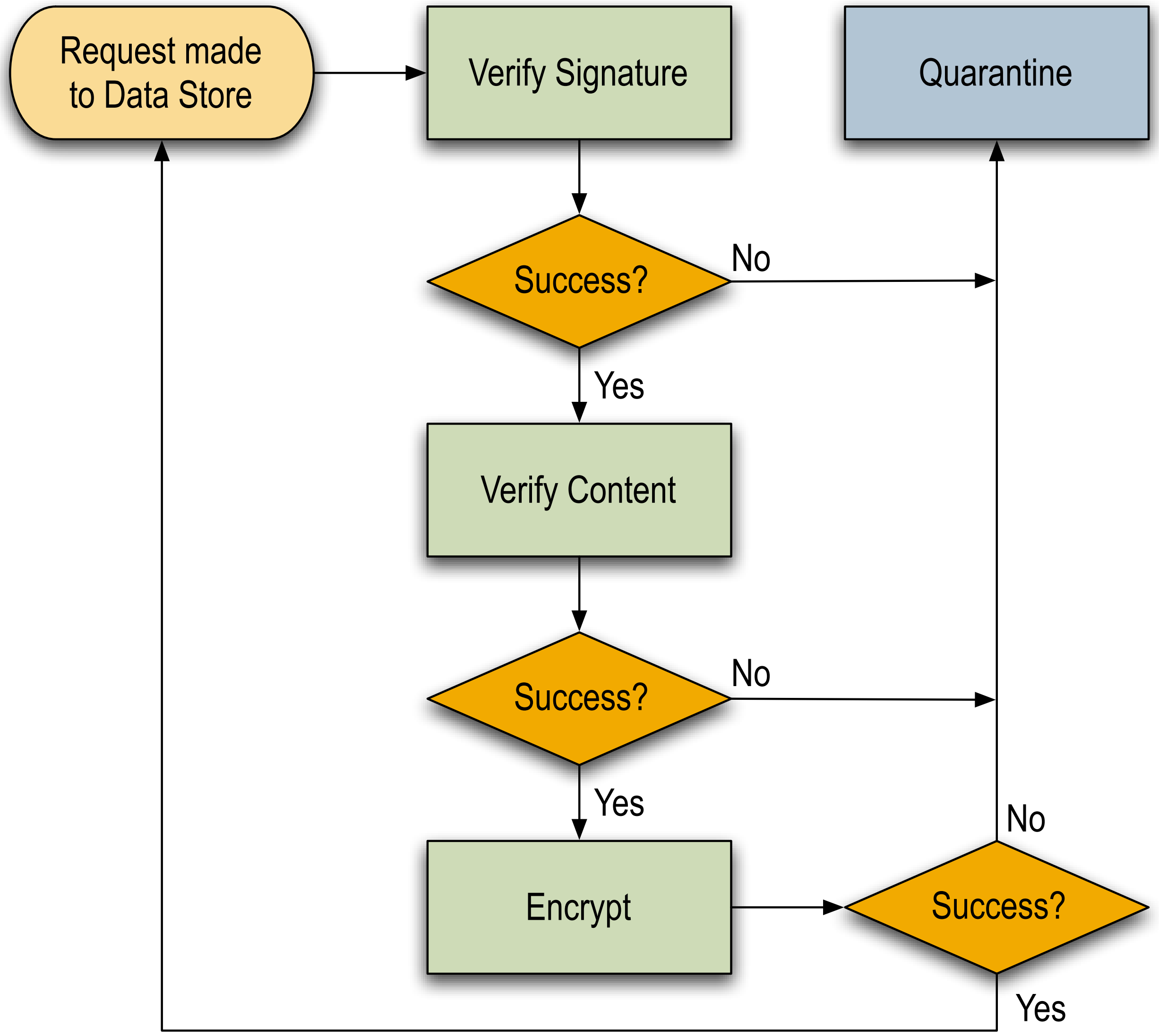
Privileged as necessary

In separate compartment / zone

Helper Applications

Process success / failure is action action success / failure

Secure Data Store: Example



Case Study
JICPAC

JICPAC Case Study

Organization:

- Joint Intelligence Center Pacific (JICPAC)
- Combined military intelligence center supporting all four military branches in the Pacific Command

- Collaboration between multiple disparate intelligence and military agencies
- JICPAC users require simultaneous access to applications residing in multiple secure domains

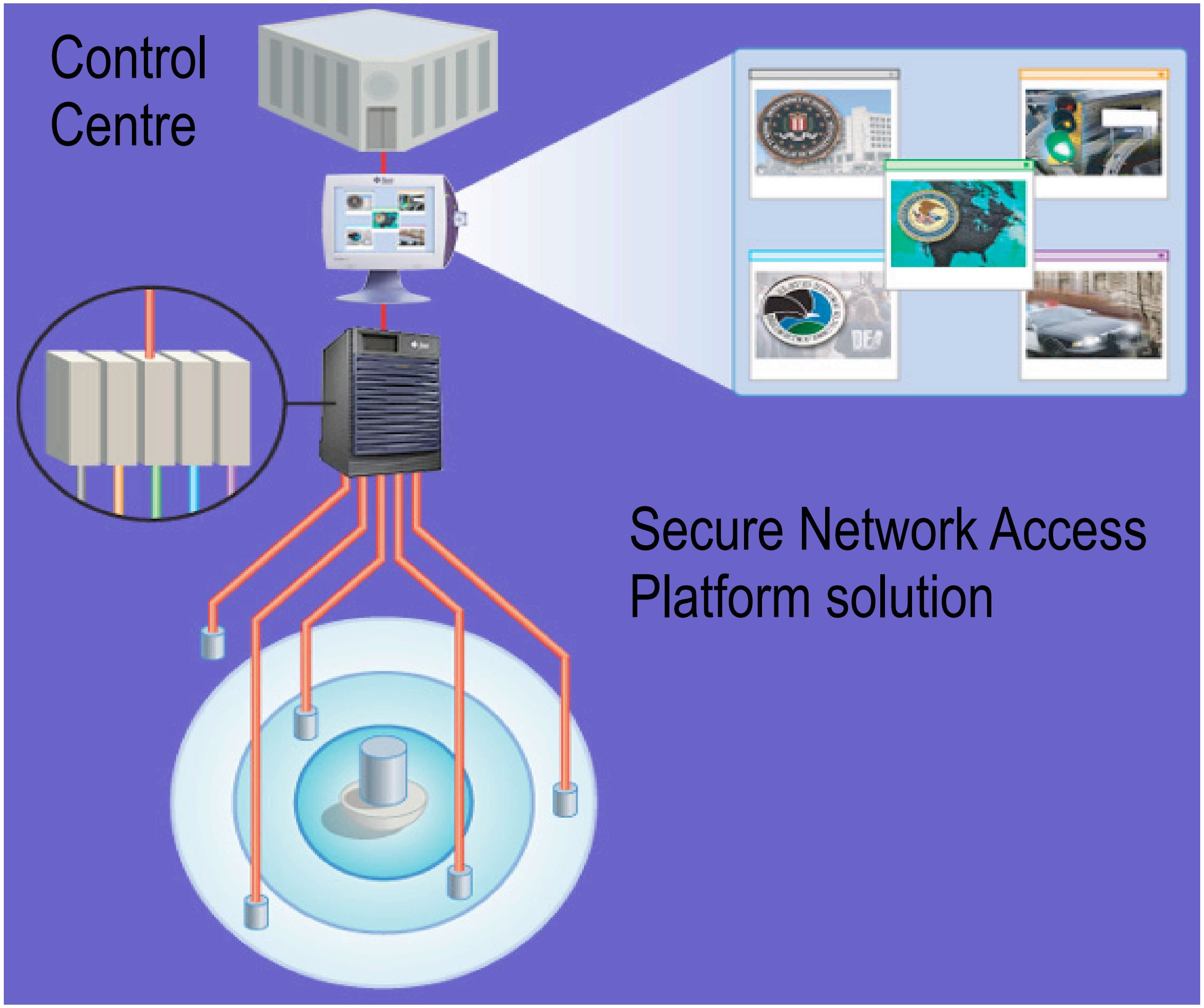
JICPAC Case Study

- JICPAC requirement to maximize productivity while minimizing the cost
- Supported Solution based on COTS products
- Scalable to meet JICPAC operational requirements

JICPAC Case Study

11/0700Z
BSD 03-05
US Forces in AOR must remain in FPCON CHARLIE as previously directed
CNN
Changes

JICPAC Case Study

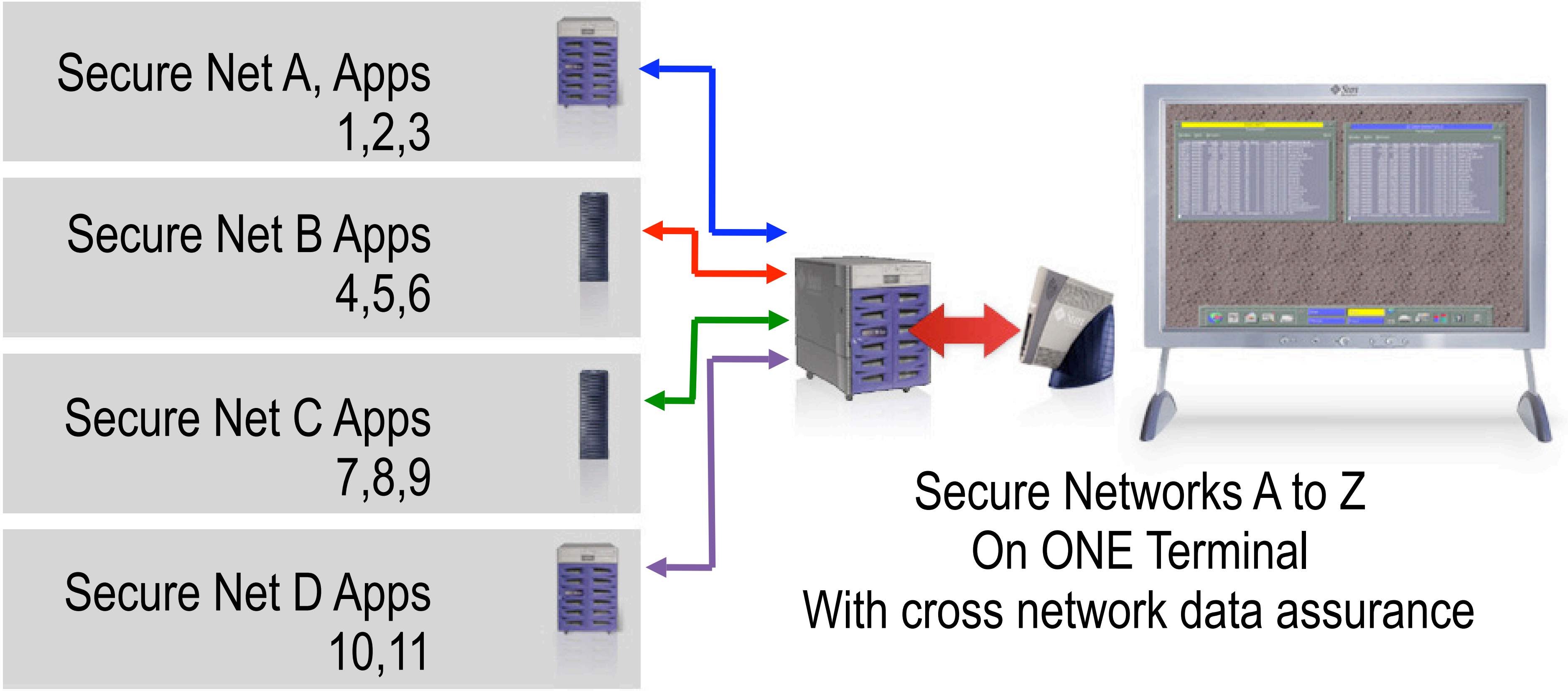


Control Centre

Secure Network Access Platform solution

JICPAC Case Study

Single-point for info assurance



Secure Net A, Apps 1,2,3

Secure Net B Apps 4,5,6

Secure Net C Apps 7,8,9

Secure Net D Apps 10,11

Secure Networks A to Z
On ONE Terminal
With cross network data assurance

JICPAC Case Study

- 24/7 Operation
- Intelligence Center for the Pacific Command
- 600 seats, with growth to thousands
- Expecting an order of magnitude in cost reduction over 5 years
- Meets highest levels of DOD Trusted Computing Deployment Criteria
- Maximize Operation Efficiency

Conclusions:

- Data Interoperability is difficult
- There are many challenges in Federating (info in datasets, trusted users, data, audit and info about the info)
- Excellence in people, process and technologies
- Innovation is the key - new paradigms
- Sun Microsystems is one of the best kept secrets in the data interoperability world - data handling framework is one of many micro-architectures being brought to solve security and privacy.

Questions & Answers

Robin T. Wakefield

robin.wakefield@sun.com

www.robinwakefield.com