

Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

Network Security Architecture



IBM Washington System Center
IBM Technical Sales Support

Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
 - **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
 - All other products may be trademarks or registered trademarks of their respective companies.
 - Refer to www.ibm.com/legal for further legal information.
-
- OSA-Express Features
 - There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express/Network Express features unless a specific OSA-Express feature is mentioned.

Agenda

- Why Do We Care about Security?
- Where to Protect Data
- Security Landscape: Security Architectures in General
- Security Architectures in IT Networking
- Cryptographic Landscape: One piece of the Security Landscape

Why Do We Care About Security?



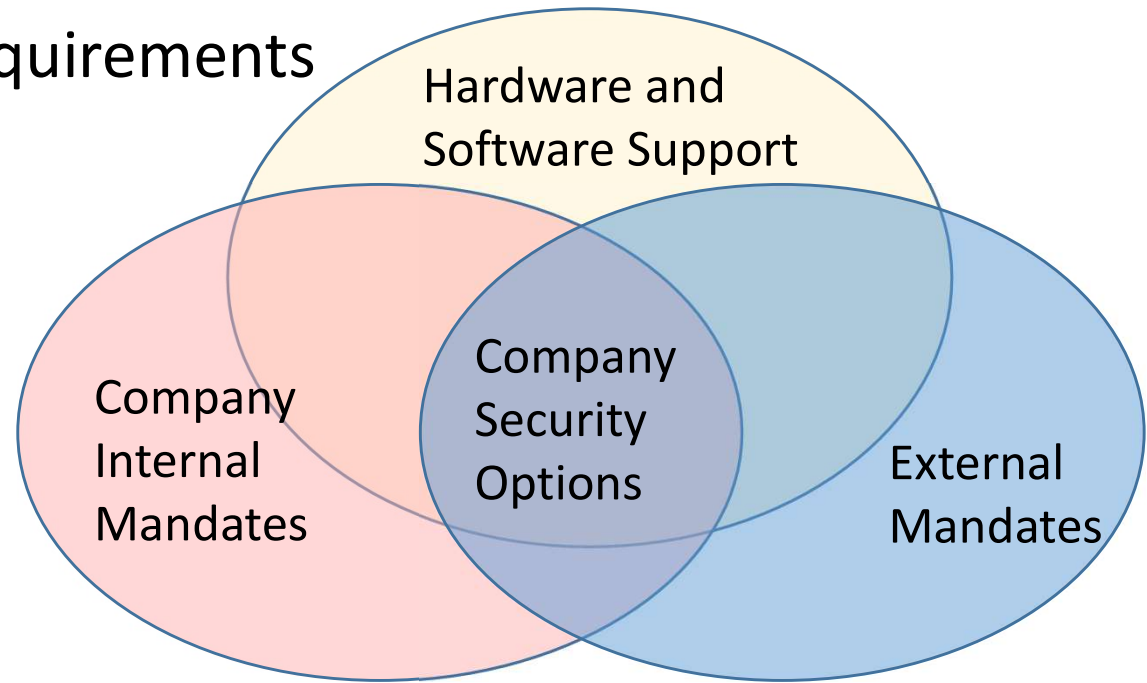
Data Breach

- Costly:
 - Penalties
 - Loss of Trust
 - Loss of Business
 - Loss of Data

Security Mandates

- Internal and External Requirements

- Encryption Protocols
 - IPsec IKEv1, IKEv2
 - TLS V1.0, V1.1, V1.2, V1.3
 - OpenSSL
- Encryption Algorithms
 - 3DES, AES, ECC
- Hash Algorithms
 - SHA1, SHA2
- Key Sizes
 - 1024, 2048
- External Mandates
 - GDPR – General Data Protection Regulation
 - PCI – Payment Card Industry
 - FIPS – Federal Information Processing Standards
 - HIPA – Health Insurance Portability and Accountability Act

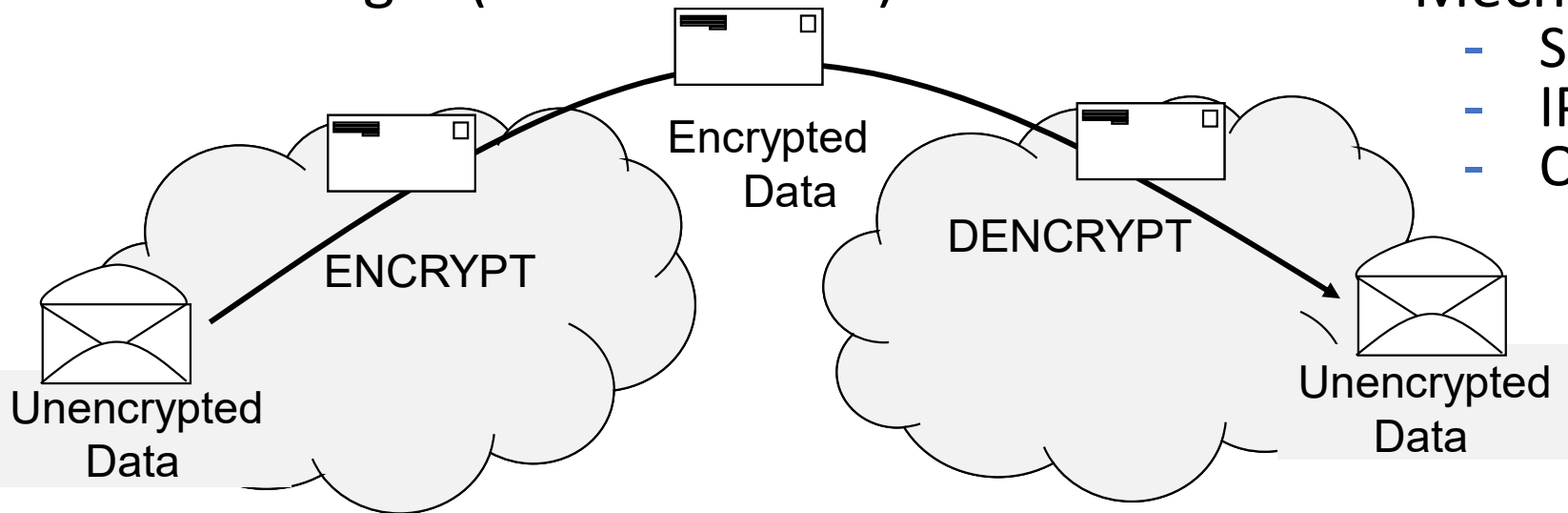


Where to Protect Data



Data in Flight

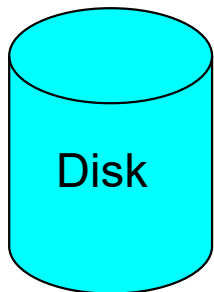
- Data in Flight (Data in Transit)



- Mechanisms:
 - SSL, TLS, AT-TLS
 - IPsec
 - OpenSSH

- Data at Rest (Archived Data)
- Data in Use (During Access for Processing)

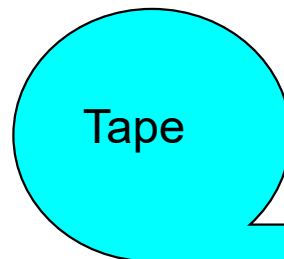
Encrypted
Data



Encrypted
Data



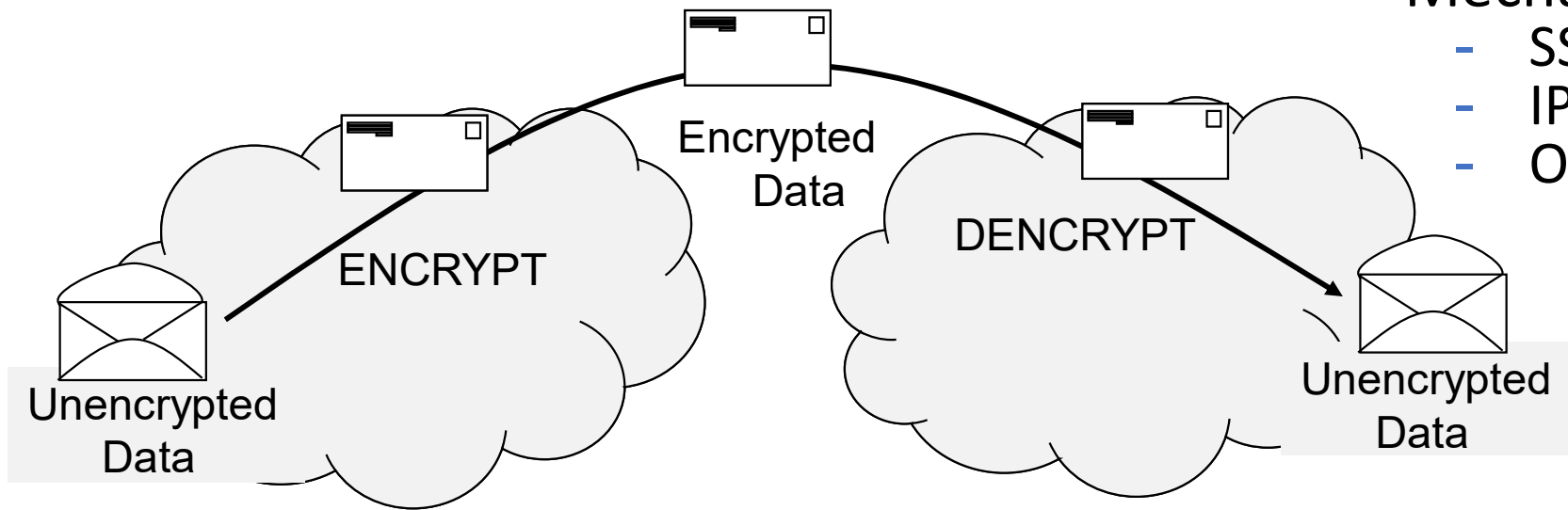
Encrypted
Data



- Mechanisms:
 - IBM Tape and Disk Encryption
 - Encryption Facility for DB2 and IMS
 - z/OS Encryption Facility
 - ICSF Programming
 - VSAM Encryption

Security Checks Performed for Data in Flight

- Data in Flight (Data in Transit)



- Mechanisms:
 - SSL, TLS, AT-TLS
 - IPsec
 - OpenSSH

- Authenticate the partner in the connection
 - Is this the connection partner we are supposed to be communicating with?
- Verify the integrity of the transmission
 - Has the data been altered in transit?
- Encrypt the data in transit
 - Is anyone unauthorized able to intercept the transmission and understand the contents?
 - Have we made the contents of the transmission private while it is traversing the network?

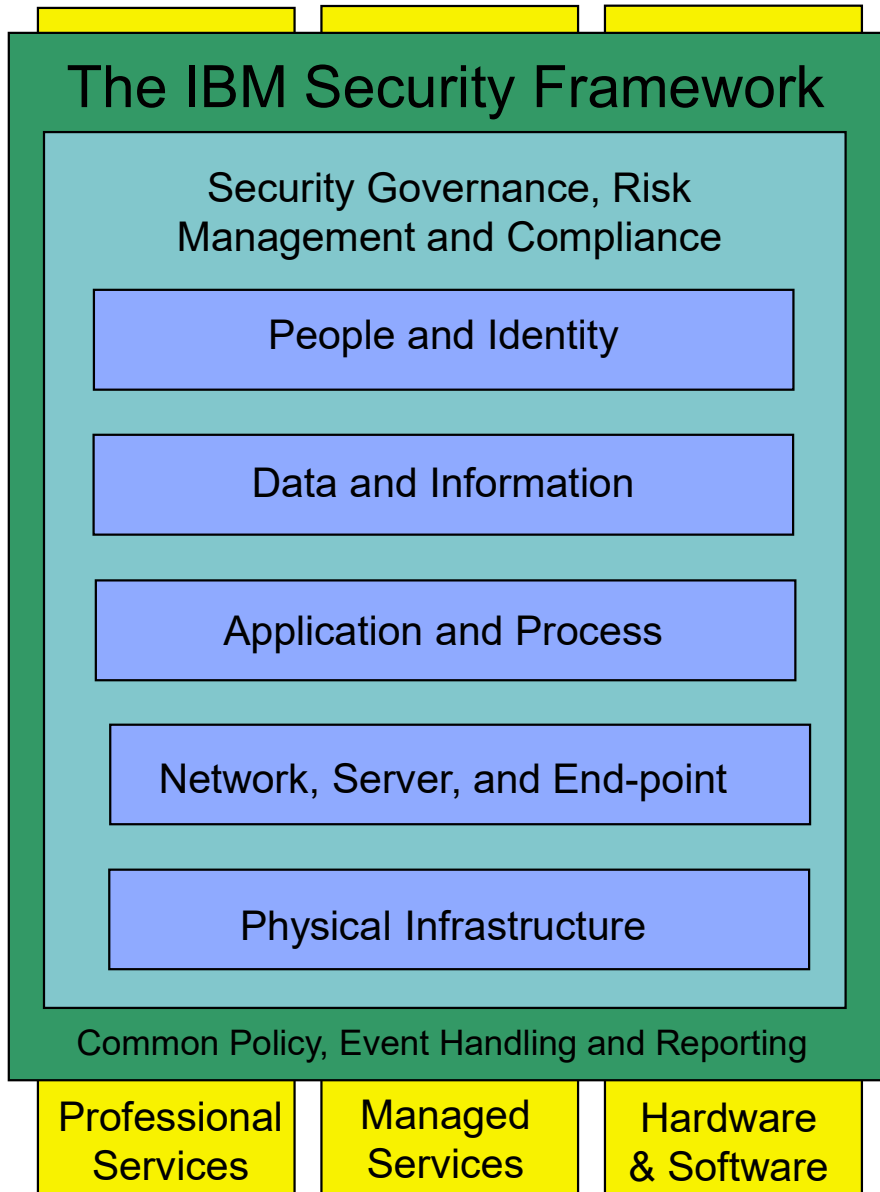
The Security Landscape: Security Architecture in General

Questions for Planning Security:

- **What** needs protecting?
- **How** should you protect?
- **Which** mechanisms or technologies should you use to protect?



The IBM Security Framework: What to Protect

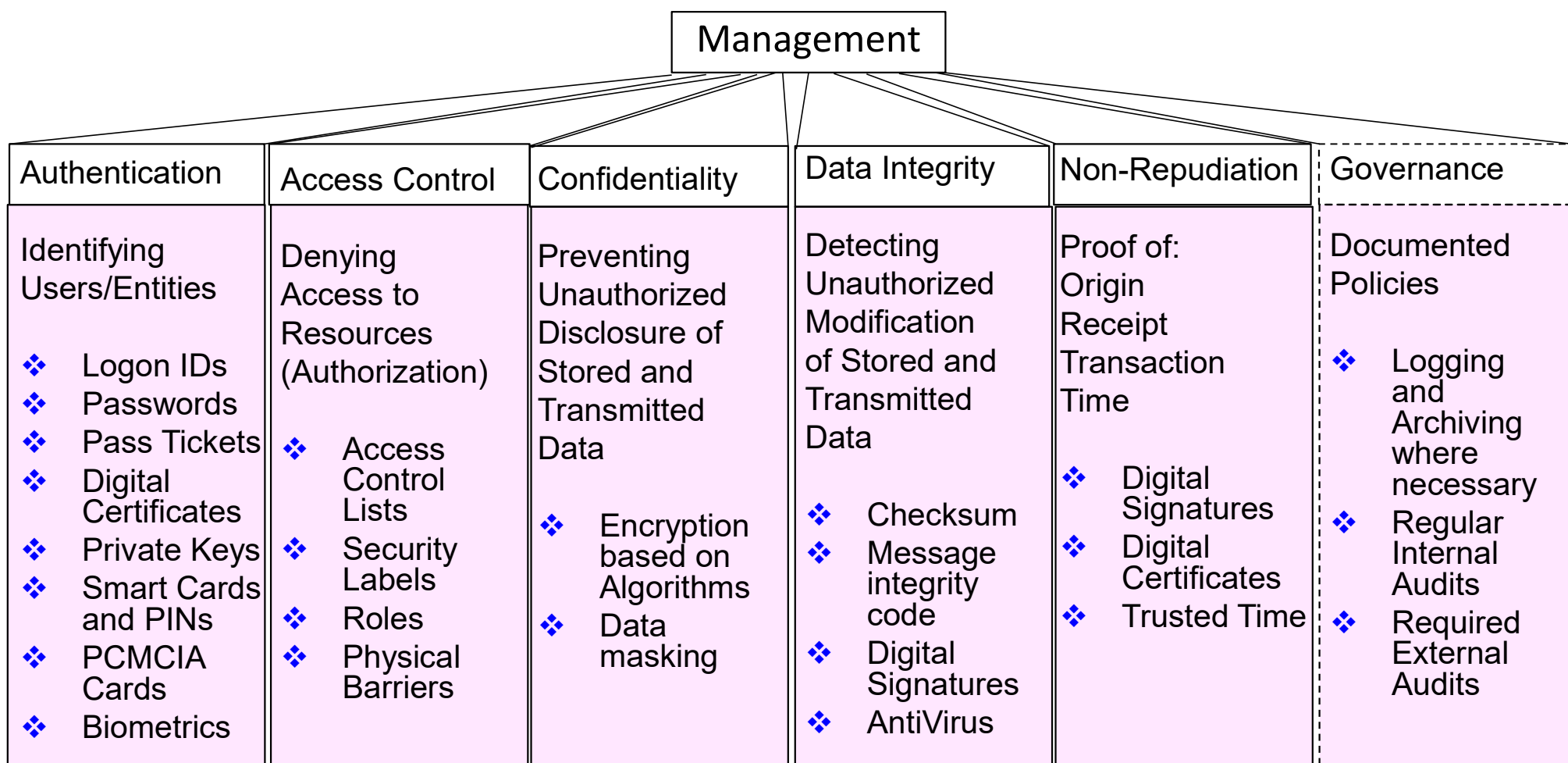


- IBM Solutions:

- Security Compliance
 - Demonstrate policy enforcement aligned to regulations
- Identity and Access
 - Controlled and secure access to information, applications, and assets
- Data Security
 - Protect and secure data and assets
- Application Security
 - Manage, monitor, audit
- Infrastructure Security
 - Threat management across networks, servers, end-points

Security Architecture Role: How & Which Way to Protect

Security Services and Mechanisms

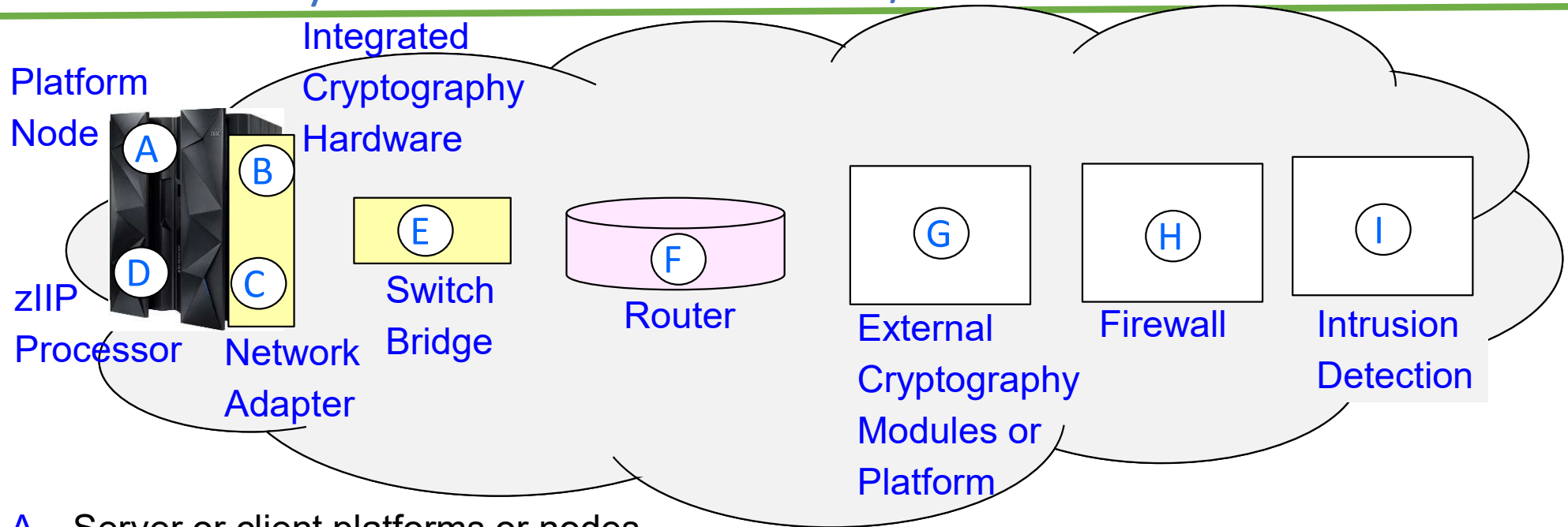


International Standard ISO 7498-2, "Security Architecture"

Network Security Components



Security Hardware in a TCP/IP Network



A. Server or client platforms or nodes

- On System Z: Control over sharing of Channel Subsystems through IOCP

B. Integrated Crypto Hardware

C. Networking adapter: Serial or Local Area Network Ports

D. On System z: zIIP processor to offload CPU expended on IPSec

E. Switch: Interconnects multiple segments on same network

F. Router: Interconnects separate network segments

G. External Crypto Modules or Platforms

H. Firewall: Examines information flow to determine whether to permit or deny it

I. Intrusion Detection: Detect and report on suspicious data flowing to nodes on network

RACF

- IBM Resource Access Control Facility (RACF)
 - Uses z/OS System Authorization Facility (SAF) to control access to resources:
 - Data Sets, MVS Commands, Networks, Network Services
 - SAF = high level MVS interface for plugging into any SAF-compatible security product.
 - Keeps a record of all the resources that it protects in the RACF database.
 - A resource can be a data set, a program, and even a subnetwork.
 - Identification of users and Authentication of user IDs and passwords
 - When a user tries to access a resource, RACF checks its database for User ID and password and permits or denies access to the resource.
 - It displays an ICH408I message if the access is denied.

```
ICH408I  USER(UTSM)  GROUP(MTSM)  NAME(TSOMON  STC-USERID)
EZB.PORTACCESS.SX00.TCP2.SAPSYS  CL  (SERVAUTH)
INSUFFICIENT ACCESS AUTHORITY FROM EZB.PORTACCESS.*.*.SAPSYS  (G)
```
 - Protection of Application Programs
 - Robust protection of its programs from unauthorized alteration.
 - Makes the z/OS platform effectively immune to computer viruses.
 - Protection of Network Resources with SERVAUTH resource class
 - Uses the SERVAUTH resource class to protect most TCP/IP resources:
 - Ports, Networks, IP Stacks.
 - Protection of Network Resources with Multi-level Security (MLS)
 - Uses Security Labels (SECLABELs)
 - A security category such as PAYROLL, PERSONNEL, or RESEARCH
 - A security level such as CONFIDENTIAL, SENSITIVE, or TOP-SECRET
 - Access to Resource is permitted only if User's SECLABEL is greater than or equal to the SECLABEL of resource

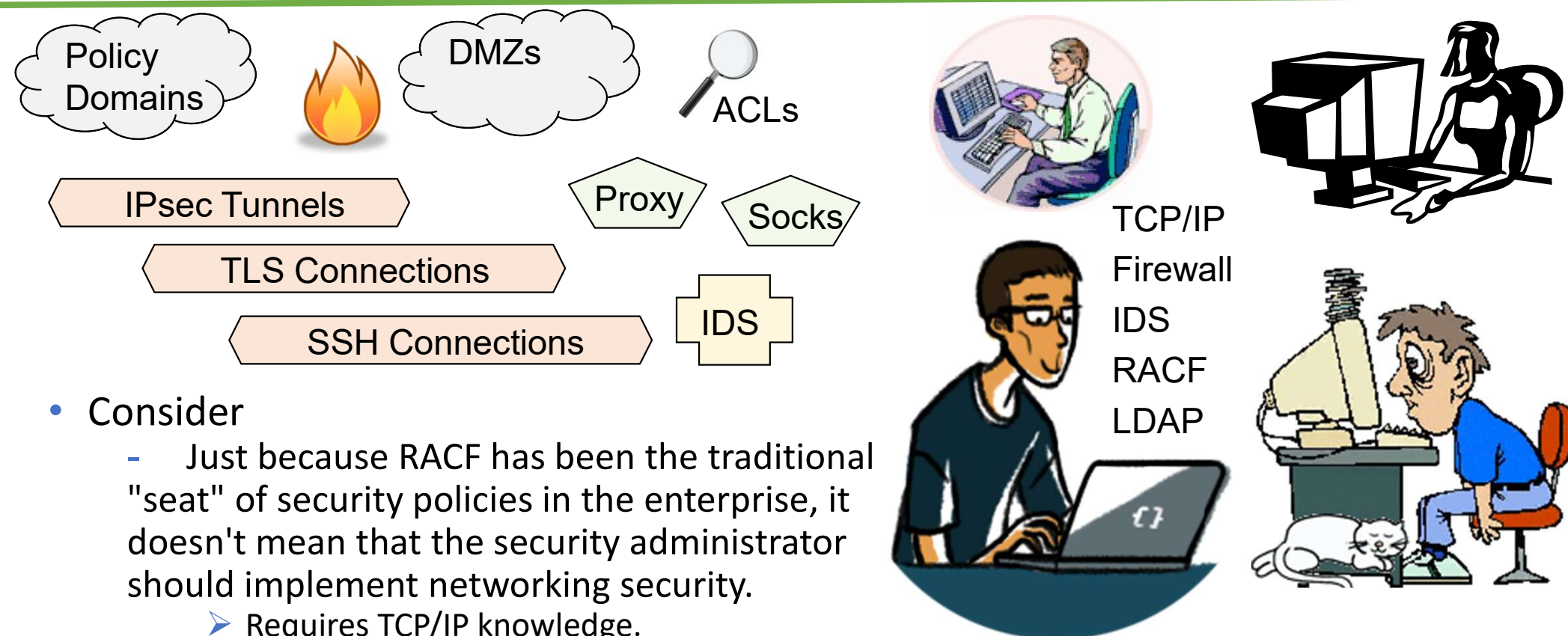
Hardware and Software on System z

- z/OS Cryptographic Services
 - CP Assist for Cryptographic Function (CPACF)
 - IBM Z hardware feature 3863
 - No cost feature that is enabled by default in most countries (no Started Procedure)
 - Provides APIs to encrypt or decrypt user data
 - Integrated Cryptographic Service Facility (ICSF)
 - z/OS component that provides secure, high-speed crypto services (Started Procedure must be up)
 - A variety of cryptographic primitives
 - Application access to z/OS hardware crypto features (CPACF, Crypto Coprocessor card, and Crypto Accelerator card)
- System SSL
 - z/OS component that provides SSL, TLS implementations (Started Procedure available but not required)
 - Also provides certificate-related APIs, including RSA signature generation and validation
 - Contains own software implementations of all crypto algorithms
 - Makes use of hardware crypto facilities to varying degrees
- z/OS Communications Server
 - TCP/IP stack implements
 - Application Transparent - TLS and IPSec including Internet Key Exchange daemon (IKED)
 - Both contain software implementations of most cryptographic algorithms
 - Both use hardware crypto facilities to varying degrees
 - Intrusion Detection Services
- OpenSSH
 - Uses OpenSSL for cryptographic algorithms
 - Uses hardware crypto facilities to varying degrees

Other System z

- Selected Other Software Offerings:
 - z/OS Encryption Facility, Encryption Facility for IMS and DB2, etc.
 - OPTIM Data Privacy Solution
 - Rational APPScan
 - Tivoli Identity Management, etc.
 - Proventia Firewall for Linux on z
 - IBM zSecure
 - <https://www.ibm.com/security/mainframe-security/zsecure>

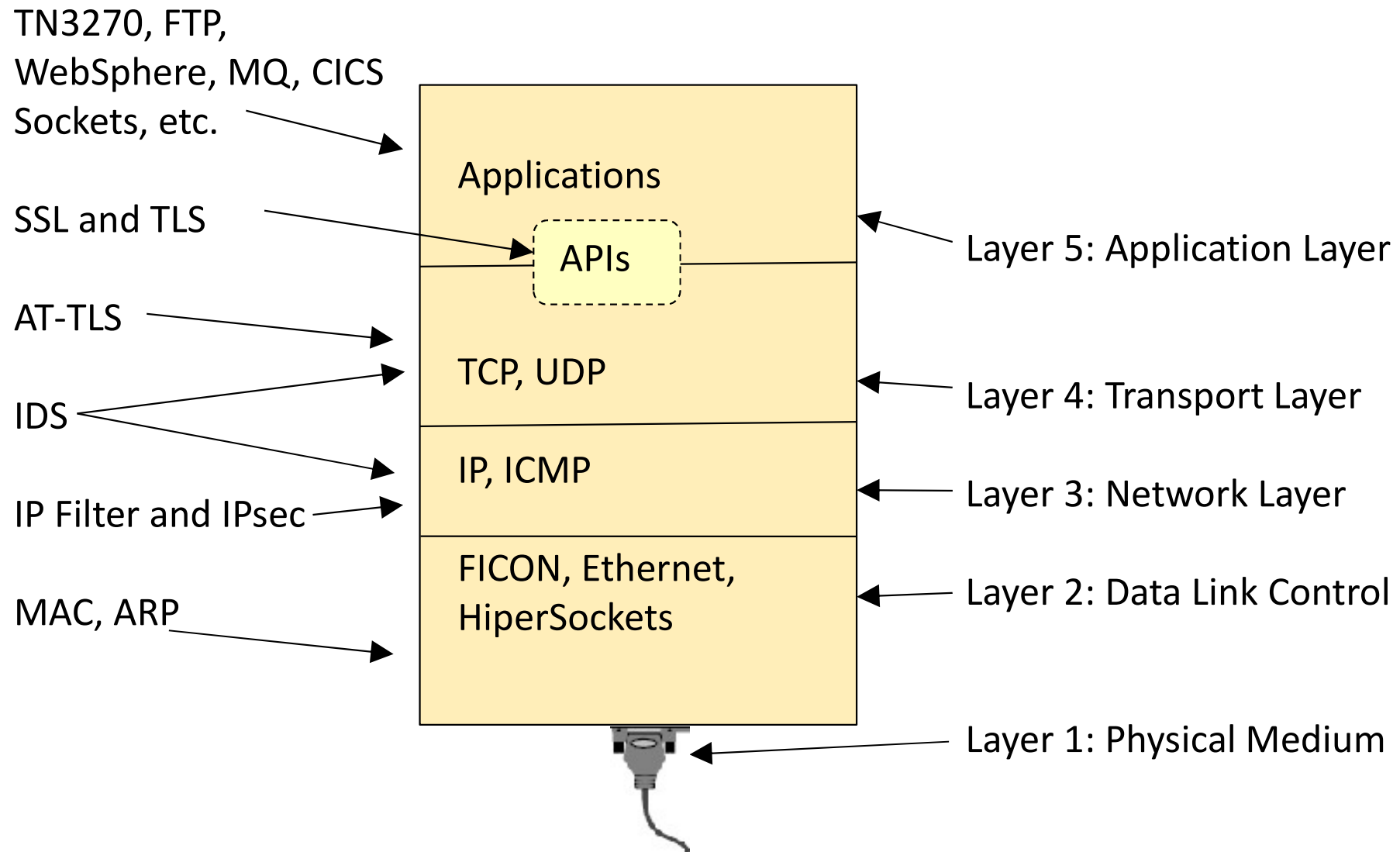
Best Practices: Security Teaming – Multiple Departments



- Consider

- Just because RACF has been the traditional "seat" of security policies in the enterprise, it doesn't mean that the security administrator should implement networking security.
 - Requires TCP/IP knowledge.
 - Requires understanding of the IDS options and parameters that are meaningful for your environment.
 - Requires analysis of what the samples (ldif and xml) provide you and what you may want to change in them.
- Advise the Firewall and the external IDS technical crew of all your findings.
 - Work with them to enhance their policies and rules.
- Always use Internal IDS as a second or third line of defense.

Security and Other Protocols in a TCP/IP Network



End of Topic

