SHARE in Orlando 2015

z/OS Communications Server Security Using Policy Agent

Session 17787

Thursday 8/13 Southern Hemisphere 5 at 3:15pm

Linda Harrison

lharriso@us.ibm.com

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AIX*
BladeCenter*
DB2*
Easy TIER*
IBM*
IBM i*
IBM logo*
Informix*
PartnerWorld *
Power*
POWER7*
Power Systems
PowerVM
PureApplication
PureFlex
PureSystems
Storwize*
System Storage*
System x*
System z*
Tivoli*
WebSphere *
zEnterprise*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Windows Server and the Windows logo are trademarks of the Microsoft group of countries.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

* Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

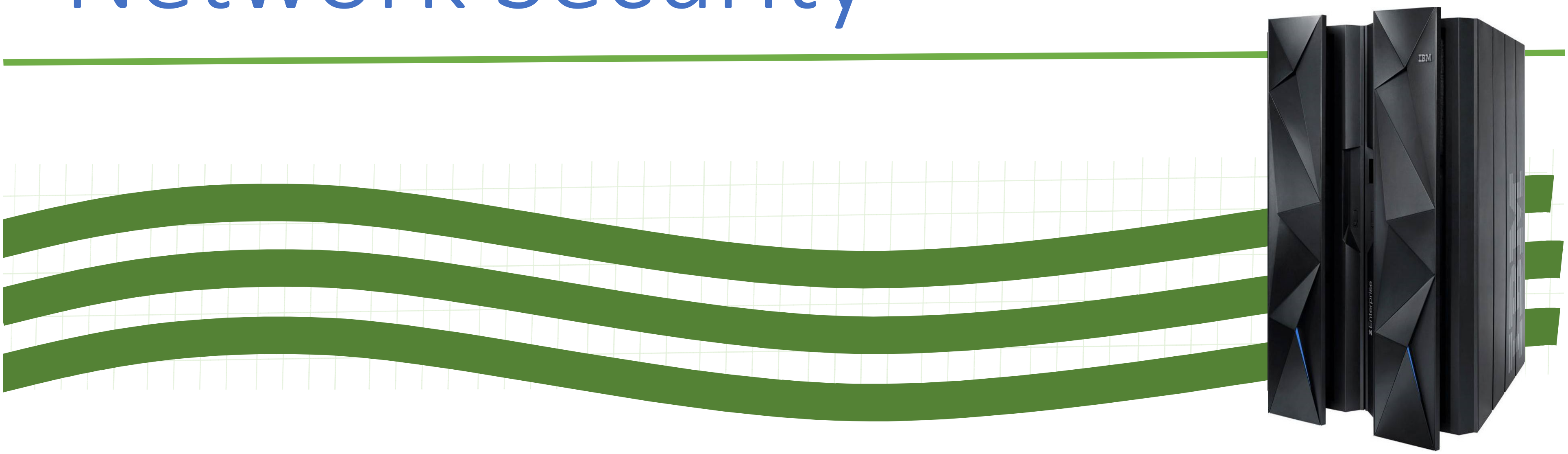
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- z/OS Communications Server Network Security
- Policy-based Network Security
- IPsec
- Application Transparent TLS
- Cryptographic Landscape: One piece of the Security Landscape
- Intrusion Detection Services
- Policy-based Routing (PBR)
- Configuration Assistant for z/OS
- Policy-based Network Security Components
- Enterprise Security Roles
- Centralized Policy Agent
- Network Security Services for IPSec
- Appendicies:
  - Why Do We Care about Security?
  - Where to Protect Data
  - Security Landscape: Security Architectures in General

z/OS Communications Server Network Security

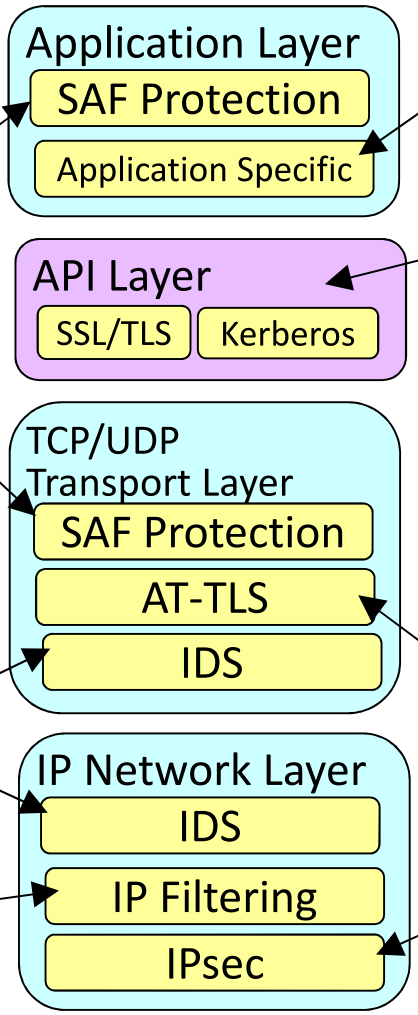


Protocol Stack View of TCP/IP Security Features

SAF SERVAUTH class to prevent unauthorized user access to resources.

Intrusion Detection Services (IDS) protects against attacks on the system's open services.

IP packet filtering blocks out all IP traffic that this system does not permit.



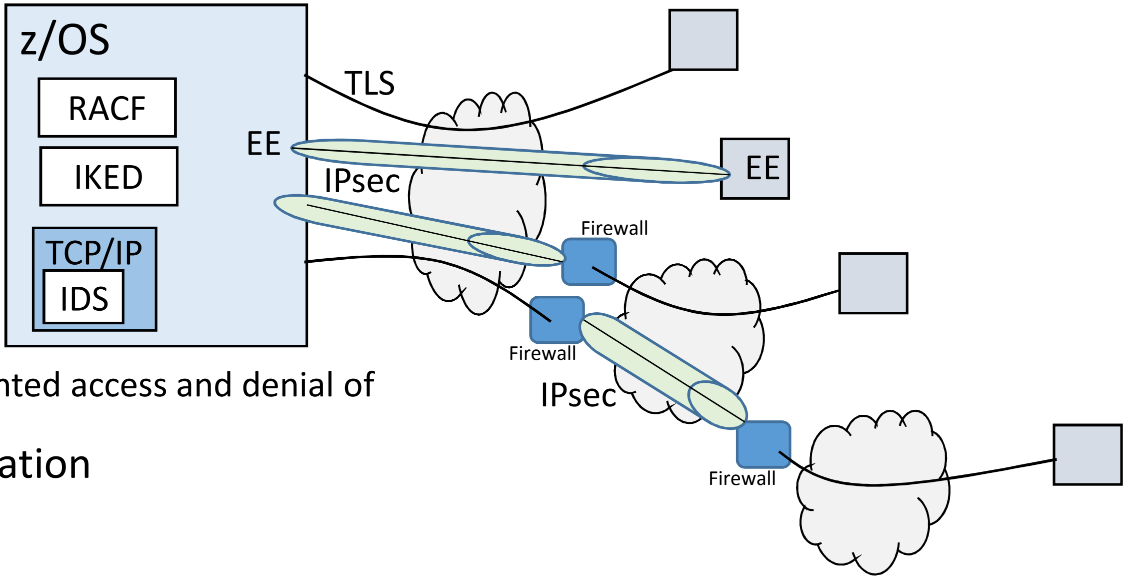
Applications with built-in security extensions, ie. SNMPv3, DNS, OSPF.

Both SSL/TLS and Kerberos are extensions to the sockets APIs and require application modification. So they are actually in the Application Layer and the Transport Layer. They are specific to TCP applications and do not support UDP.

AT-TLS provides SSL/TLS services and is available to TCP applications.

IPsec provides support for manual and dynamic VPN tunnels.

z/OS Communications Server Security Roles and Objectives



- Secure access to both TCP/IP and SNA applications
- Exploit strengths of System z hardware and software
- IDS & RACF protect data and other resources on the system
  - System availability
    - Protect system against unwanted access and denial of service attacks from network
  - Identification and authentication
    - Verify identity of users
  - Access control
    - Protect data and other system resources from unauthorized access
- TLS & IPsec Protect data in the network using cryptographic security protocols
  - Data Origin Authentication
    - Verify that data was originated by claimed sender
  - Message Integrity
    - Verify contents were unchanged in transit
  - Data Privacy
  - Conceals cleartext using encryption
- Focus on end-to-end security and self-protection

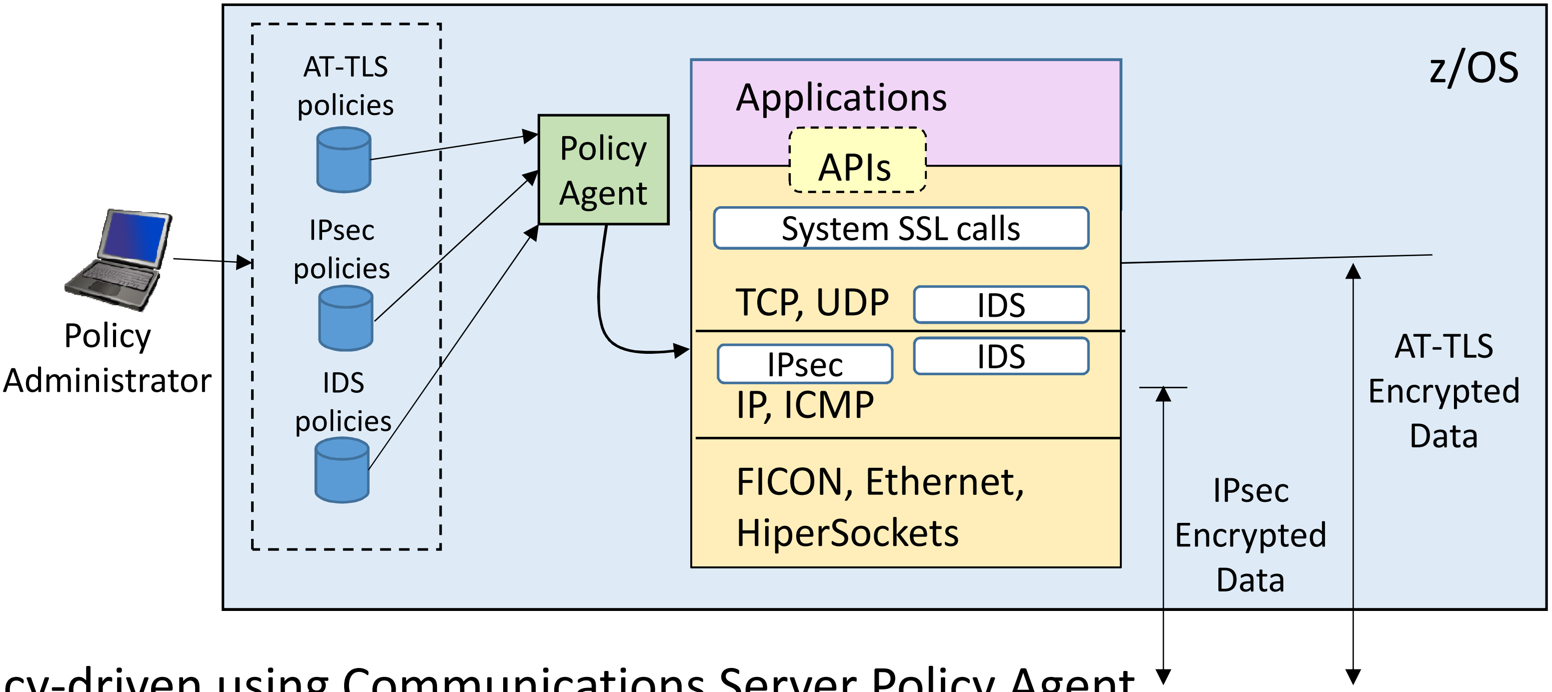
Deployment Trends and Requirements

- Protecting the system from the network
  - Observed increase in end-to-end security
    - z/OS encryption endpoint
    - Requires focus on self protect
    - z/OS IDS in addition to external Firewalls
      - Packet inspection techniques in network less effective
  - Minimizing security deployment costs
    - Application transparent network security reduces application costs
    - Policy-based network security reduces deployment costs
      - Numerous security types all implemented via Policy Agent
    - AT-TLS avoids separate TLS implementations in applications
    - Configuration Assistant for z/OS Communications Server to simplify customization

Policy-based Network Security

Application Transparent – Transport Layer Security (AT-TLS)
Defense Manager Daemon (DMD)
IP Filtering and IPsec
Intrusion Detection Services (IDS)
Network Security Services (NSS)
Quality of Service (QoS)
Policy Based Routing (PBR)
Central Policy Server

z/OS Communications Server Security Roles and Objectives

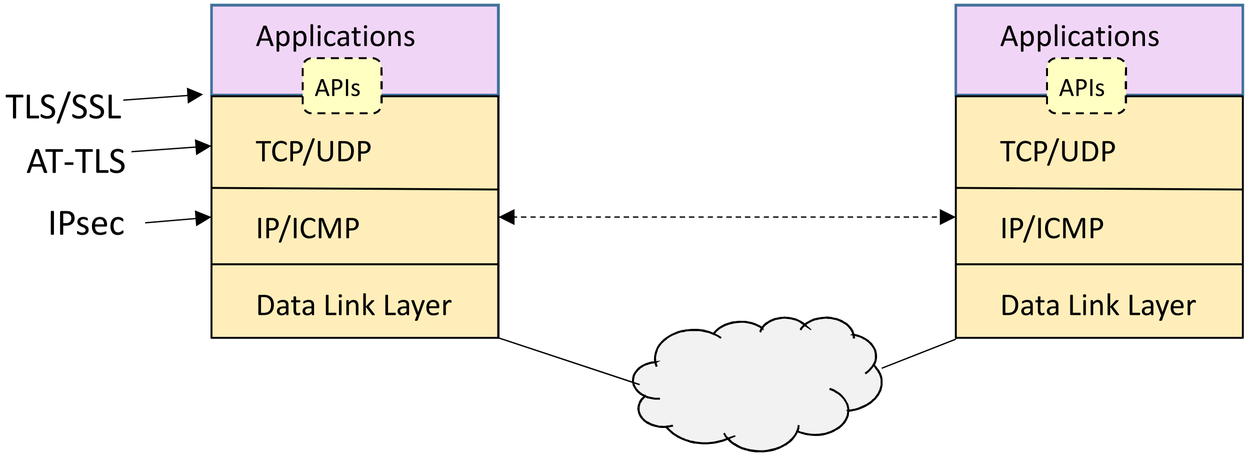


- Policy-driven using Communications Server Policy Agent
  - Network security without requiring application changes
- Security services provided by the TCP/IP stack
  - AT-TLS, IPsec, IDS, PBR
- Configure policies with a single, consistent administrative interface using Configuration Assistant for z/OS
  - Focus on what traffic to protect and how to protect
  - Less focus on low-level details
    - Details available on advanced panels

IPsec

IP Filtering
IPsec

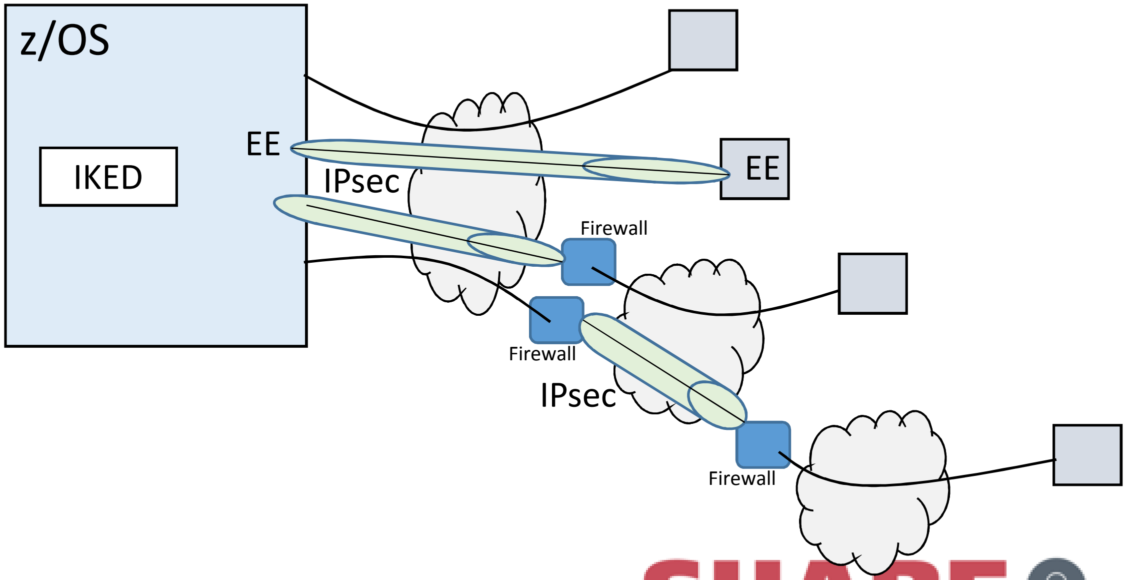
IPsec Protocol Overview



- Open standard network layer security protocol defined by IETF in RFCs
  - Provides authentication, integrity, and data privacy
- IPSec security protocols
  - Authentication Header (AH) - provides authentication / integrity
  - Encapsulating Security Protocol (ESP) - provides data privacy with optional authentication/integrity
- Implemented at IP layer
  - Requires no application change
  - Secures traffic between any two IP resources
  - Security Associations (SA)
- Management of crypto keys and security associations can be
  - Manual
  - Automated via key management protocol (IKE)

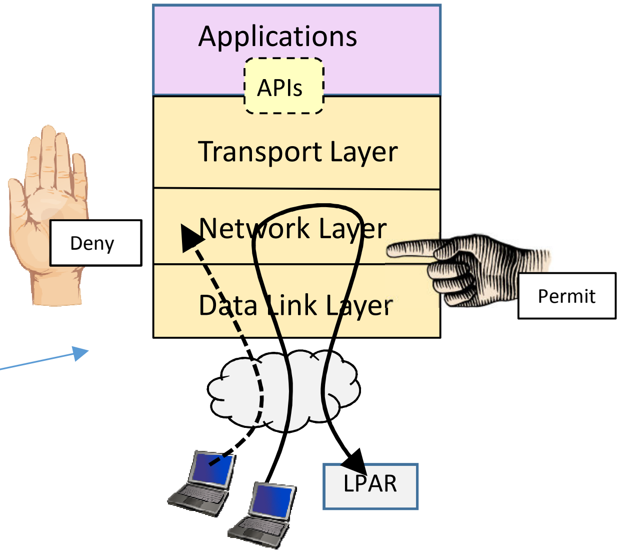
z/OS IPsec Support

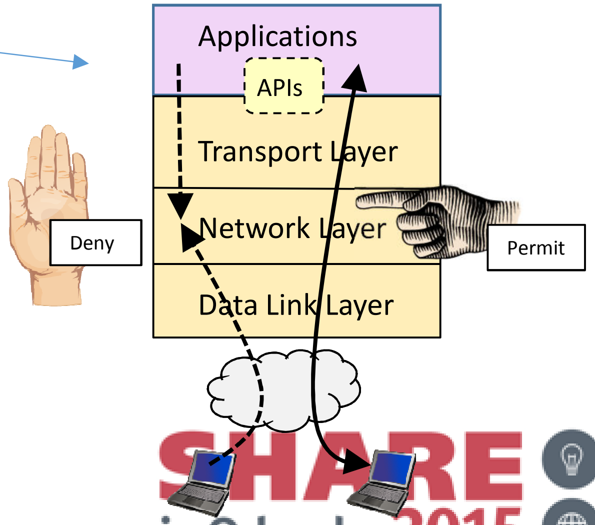
- Completely built into z/OS Communications Server:
  - IP filtering for permitting or denying packets
  - IPSec for permitting packets while authenticating, encrypting, performing data integrity checking, etc.
  - Internet Key Exchange (IKE) daemon for dynamic cryptographic key exchange and refresh over a secure "tunnel"
- Benefits:
  - Protects the system
  - Encrypts data to partners
  - Logging to syslogd based on administrator choices



IP Packet Filtering Basics

- Packet filtering at IP Layer
- Filter rules defined to match on inbound and outbound packets based on:
  - IP address, port, protocol
  - Direction, link security
  - Time
- Used to control
  - Traffic being routed
  - Local traffic
    - "Personal firewall"
- Possible actions
  - Permit
    - Without IPsec (in the clear)
    - With Manual IPsec
    - With Dynamic IPsec
  - Deny
  - Log (in combination with any other action)



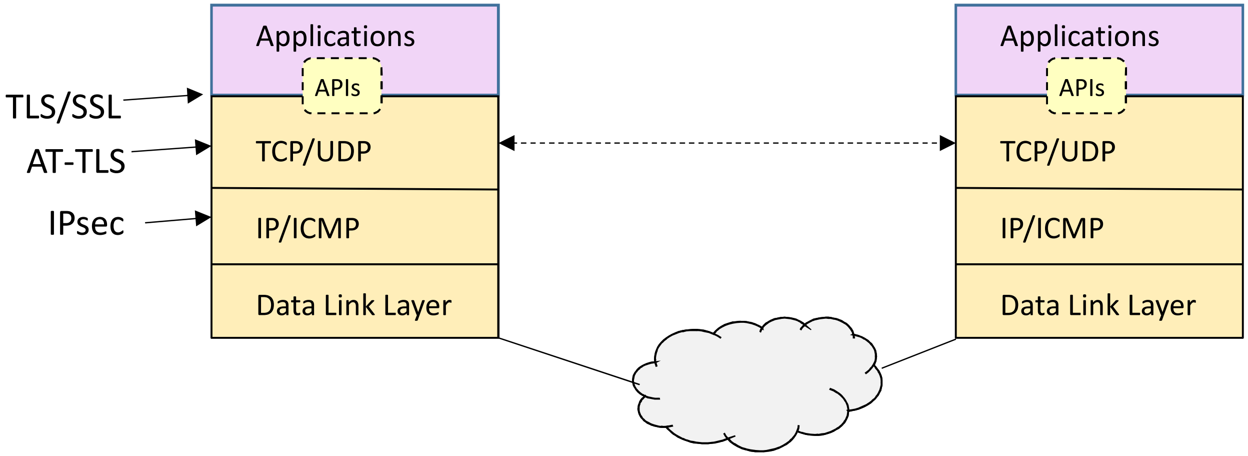


z/OS Communications Server IPsec Features

- Supports many configurations
  - Optimized for role as endpoint (host), but also support routed traffic (gateway)
  - IPSec NAT Traversal support (address translation and port translation)
  - IPv4 and IPv6 support
  - IKEv2 support in z/OS V1R12 (requires NSSD)
  - FIPS 140 Support added in z/OS V1R12
- Policy-based
  - Configuration Assistant
  - Direct file edit into local configuration file
- Default filters in TCP profile provide basic protection before policy is loaded
- Cryptographic algorithms
  - Uses cryptographic hardware (CPACF and Cryptographic Cards)
- zIIP Assisted IPSec
  - Moves most IPSec processing from general purpose processors to zIIPs
  - Additional V1R11 enhancements to optimize EE traffic over zIIP
- IP Security Monitoring Interface
  - IBM Tivoli OMEGAMON XE for Mainframe Networks uses this interface
- SMF Type 119 records
- Support for latest IPSec RFCs (added as they become approved)

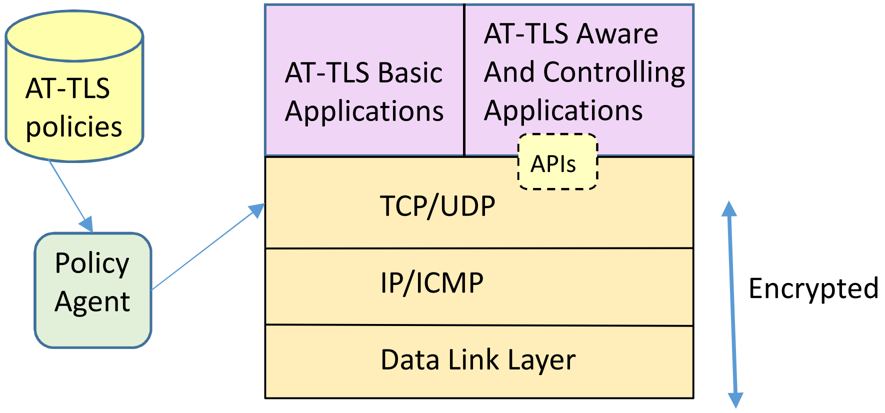
Application Transparent – Transport Layer Security (AT-TLS)

Transport Layer Security (TLS) Protocol Overview



- Open standard transport layer security protocol defined by IETF in RFCs
- Provides authentication, integrity, and data privacy
- Based on Secure Sockets Layer (SSL)
- SSL originally defined by Netscape to protect HTTP traffic
- TLS defines SSL as a version of TLS for compatibility
  - TLS clients and server should drop to SSL V3 based on partner's capabilities
- TCP only
  - UDP, raw IP applications cannot be TLS enabled
- z/OS applications can be modified to support TLS
- Uses System SSL
  - System SSL is part of z/OS Cryptographic Services element
- TLS can be used with no application change by exploiting AT-TLS

Application Transparent - Transport Layer Security (AT-TLS)



Application Specific TLS FTP.DATA Parameters	Application Specific TLS TN3270 Parameters	AT-TLS
Server Authentication TLSMECHANISM FTP	Server Authentication SECUREPORT	Basic Application FTP.DATA TLSMECHANISM ATTLS TN3270 Profile TTLSPORT
Client Authentication SECURE_LOGIN REQUIRED	Client Authentication CLIENTAUTH SSLCERT	Basic Application
SECURE_LOGIN VERIFY_USER SECURE_PASSWORD OPTIONAL	CLIENTAUTH SAFCERT	Aware Application
SECURE FTP ALLOWED	CONNTYPE NEGTSECURE CONNTYPE ANY	Controlling Application

- AT-TLS invokes System SSL TLS processing at the TCP layer for the application
- AT-TLS controlled through policy
  - Installed through policy agent
  - Configured through Configuration Assistant GUI or by manual edit of policy files
- AT-TLS Basic applications
  - For Server Only Authentication or Server with “plain” Client Authentication there is no application change required.
- AT-TLS Aware applications
  - Applications can optionally exploit advanced features using SIOCTTLSCTL ioctl call.
  - Required for Client Authentication Advanced Features.
  - Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)
- AT-TLS Controlling applications
  - Required for a single port to concurrently connect to unsecure clients and secure clients
  - Control if/when to start/stop TLS, reset session/cipher

IPsec and AT-TLS Comparison

	IPsec	**AT-TLS**
Traffic protected with authentication and encryption	All protocols	TCP
End-to-end protection	Yes (transport mode)	Yes
Segment protection	Yes (tunnel mode)	No
Scope of protection	Security Association: 1. All traffic 2. Protocol 3. Single Connection	Single session
IPsec initiated	IPsec Policy: 1. z/OS responds to IKE peer 2. z/OS initiates to IKE peer based on: - Outbound packet - IPsec command - Policy autoactivation	AT-TLS Policy: 1. Server TLS based on policy when server responds to client connection request 2. Client TLS based on policy when client initiates connection 3. Advanced function application
Application modification required	No	No, for server only authentication. Yes, for TLS Aware and TLS Controlling application support
Security endpoints	Peer (can be whole device or single application or in between)	Client or Server
Authentication options	Both sides authenticated always	Server only authentication or both sides authenticated (client authentication optional)
Endpoint identity	1. Preshared keys 2. X.509 certificates	X.509 certificates
Authentication credentials	Represents whole device or single application or in between	Represents application (server or client)
Session key generation and refresh	Session key generated in TLS negotiation. Dynamic VPN session key refreshed when timer expires. Manual VPN session key is not refreshed.	Session key generated in TLS negotiation.

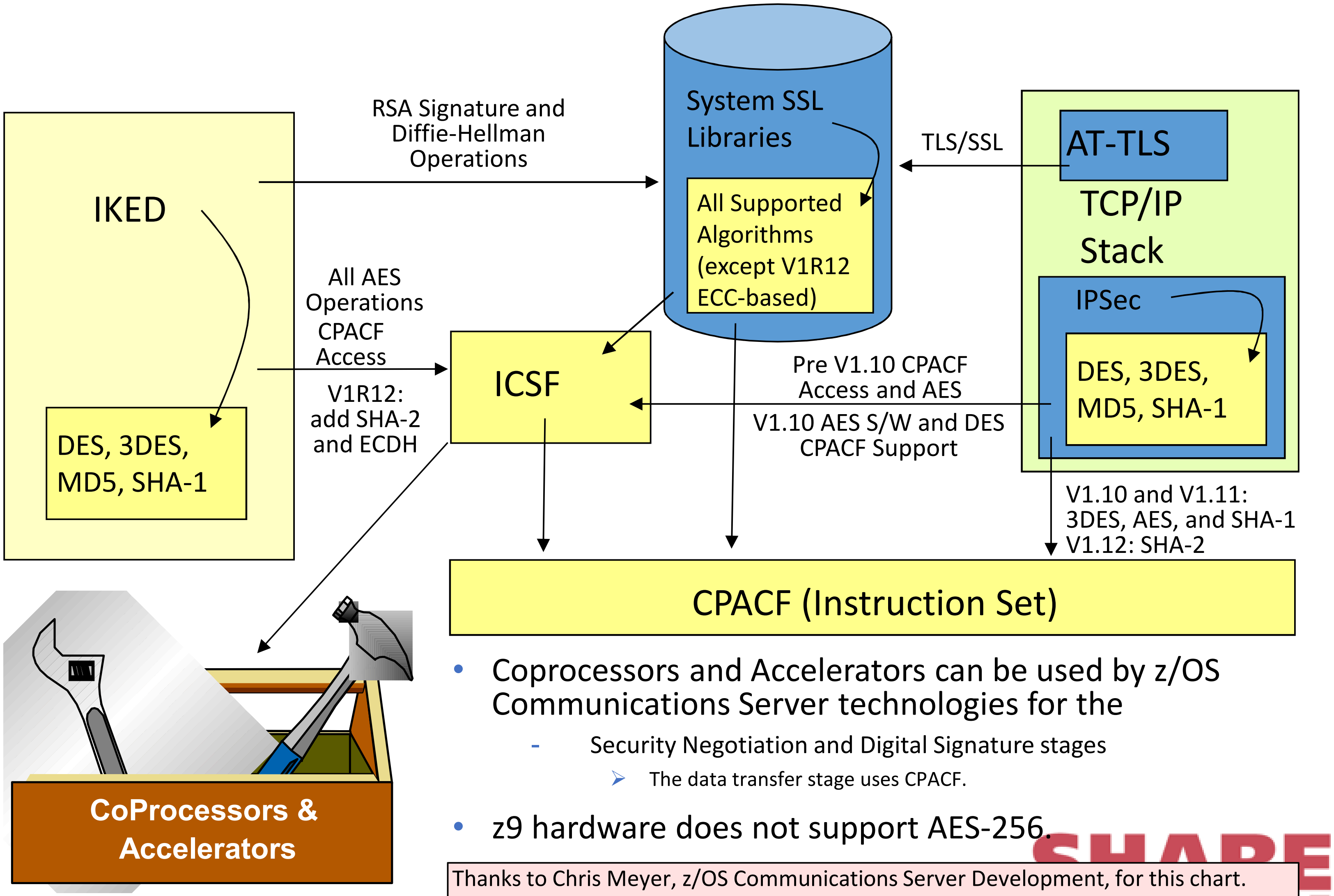
z/OS Communications Server Usage of Cryptographic Hardware

Performance numbers for Crypto Hardware:
ftp://public.dhe.ibm.com/common/ssi/ecm/en/zsw03170usen/ZSW03170USEN.PDF

Performance numbers for z/OS Communications Server with SSL/TLS/AT-TLS
http://www.ibm.com/support/docview.wss?rs=852&context=SSSN3L&uid=swg27005524

Performance numbers for offload of IPSec onto zIIP engine:
http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100988

z/OS TCP/IP Cryptographic Landscape without FIPS 140


IKED
DES, 3DES, MD5, SHA-1
RSA Signature and Diffie-Hellman Operations
All AES Operations CPACF Access
V1R12: add SHA-2 and ECDH
System SSL Libraries
All Supported Algorithms (except V1R12 ECC-based)
TLS/SSL
AT-TLS
TCP/IP Stack
IPSec
DES, 3DES, MD5, SHA-1
ICSF
Pre V1.10 CPACF Access and AES
V1.10 AES S/W and DES CPACF Support
V1.10 and V1.11: 3DES, AES, and SHA-1
V1.12: SHA-2
CPACF (Instruction Set)
CoProcessors & Accelerators

- Coprocessors and Accelerators can be used by z/OS Communications Server technologies for the
  - Security Negotiation and Digital Signature stages
    - The data transfer stage uses CPACF.
- z9 hardware does not support AES-256.

Thanks to Chris Meyer, z/OS Communications Server Development, for this chart.

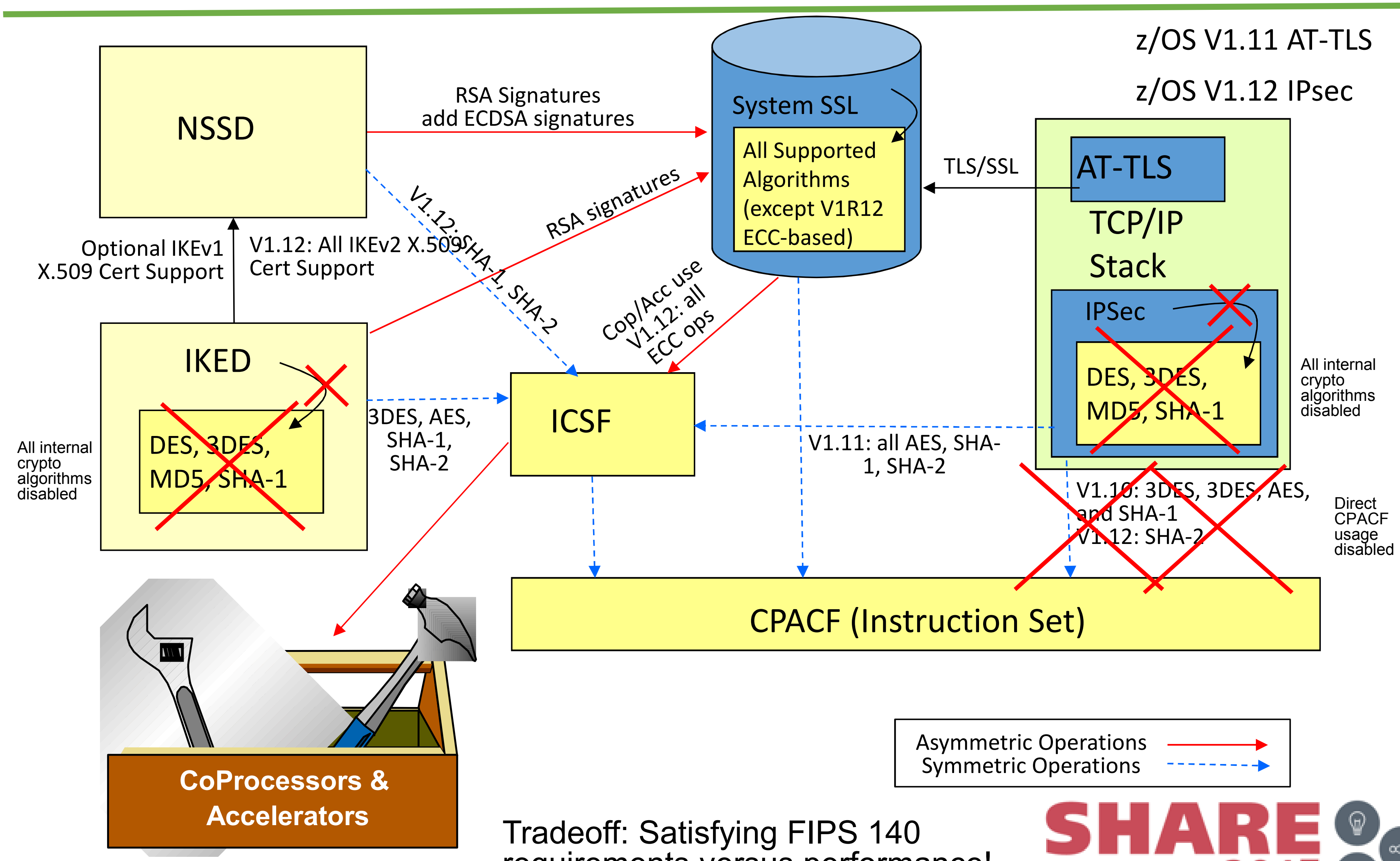
What is FIPS 140?

- Federal Information Processing Standards (FIPS) are written for a wide variety of information technologies:
  - From punched card codes to COBOL language standards to rules on the use of cryptographic technologies
  - Most of these standards are now focused on cryptography
- FIPS 140: “Security Requirements for Cryptographic Modules”
  - Originally written for hardware devices.
    - Later extended to software modules.
  - Applies only to “Cryptographic Modules” (Cryptographic Cards, Software libraries as with System SSL or ICSF)
    - Not whole systems or even applications
  - Covers:
    - Clearly defining and documenting the boundaries and interfaces of “cryptographic modules”
    - Ensuring integrity of crypto algorithms
      - signed binaries, self-test, environment, and so on
    - Limits supported algorithms
      - ie., MD5, DES, 512-bit RSA, some AES modes are not allowed
    - Ensures security of keys and key management
    - Personnel security roles, physical characteristics of hardware modules, and more
    - Current version is FIPS 140-2. FIPS 140-3 is out for review
  - The US government as well as others expect cryptographic modules to meet the FIPS 140 specifications.
    - Crypto-Express3 is certified at FIPS 140-2, Level 4

Security Levels of FIPS 140-2?

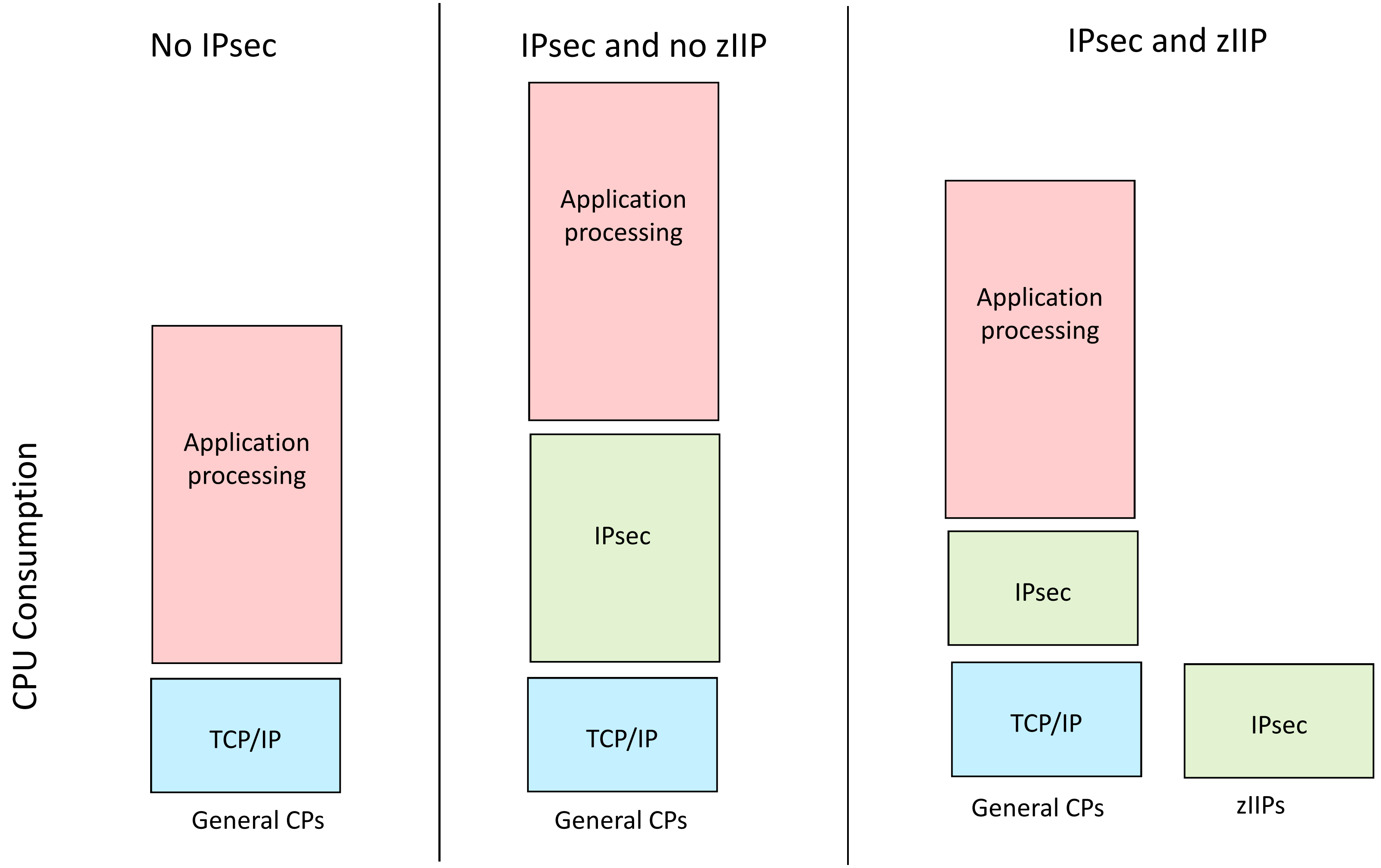
- Security Level 1:
  - Minimum level with one approved security function
- Security Level 2:
  - Adds tamper-evident detection for the security module
- Security Level 3:
  - Adds tamper-detection and tamper-protection/response to the security module
- Security Level 4:
  - Adds zeroing out of the security module if tampering is detected; also adds multi-factor authentication for operator authentication. Two of following required:
    - something known, such as a secret password,
    - something possessed, such as a physical key or token,
    - a physical property, such as a biometric.

Cryptographic Landscape with FIPS 140


z/OS V1.11 AT-TLS
z/OS V1.12 IPsec
NSSD
RSA Signatures
add ECDSA signatures
System SSL
All Supported Algorithms (except V1R12 ECC-based)
TLS/SSL
AT-TLS
TCP/IP Stack
IPSec
~~DES, 3DES, MD5, SHA-1~~
All internal crypto algorithms disabled
V1.12: SHA-1, SHA-2
RSA signatures
Optional IKEv1 X.509 Cert Support
V1.12: All IKEv2 X.509 Cert Support
Cop/Acc use V1.12: all ECC ops
IKED
~~DES, 3DES, MD5, SHA-1~~
All internal crypto algorithms disabled
3DES, AES, SHA-1, SHA-2
ICSF
V1.11: all AES, SHA-1, SHA-2
~~V1.10: 3DES, 3DES, AES, and SHA-1 V1.12: SHA-2~~
Direct CPACF usage disabled
CPACF (Instruction Set)
CoProcessors & Accelerators
Asymmetric Operations
Symmetric Operations

Tradeoff: Satisfying FIPS 140 requirements versus performance!

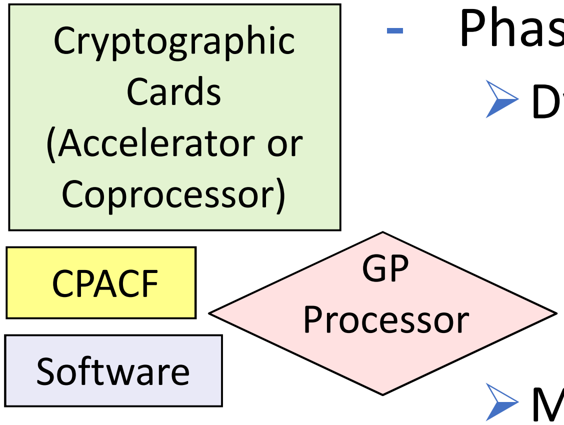
CPU Consumption for IPsec with zIIP Processor



- CPACF is exploited in the same manner on both the general CPs and zIIPs.
- Function enabled through a TCP/IP configuration keyword when zIIP hardware enabled.

IPsec

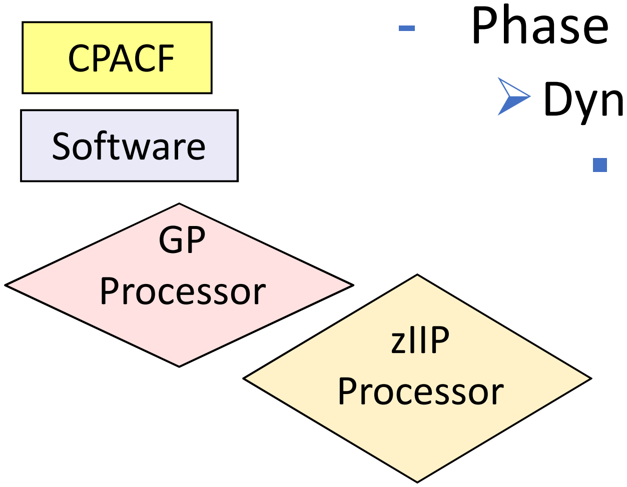
- Two Stages



  - Phase 1 Negotiation / Key Generation
    - Dynamic Tunnels IPsec IKED Phases 1 and 2
      - Authenticates Partners and generates SA Keys
        - Uses ICSF or Crypto Card if available

          Accelerator Card (Clear Key Mode)

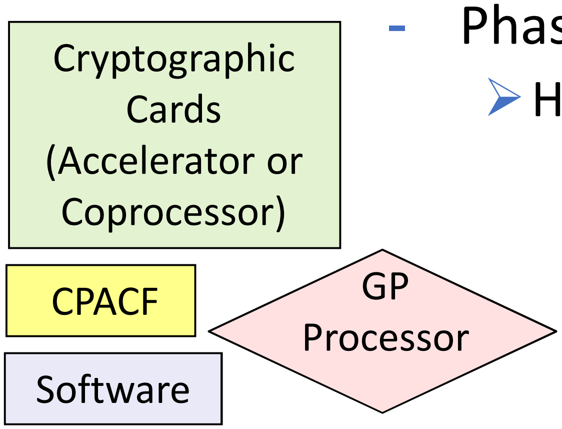
          Coprocessor Card (Secure Key Mode)
    - Manual (Static) Tunnels
      - Uses prior agreement instead of dynamic negotiation



  - Phase 2 Data Tunnel
    - Dynamic or Manual Tunnels
      - Encypts/Decrypts data
        - Uses CPACF (clear key only) if available

AT-TLS

- Two Stages



Cryptographic Cards (Accelerator or Coprocessor)

CPACF

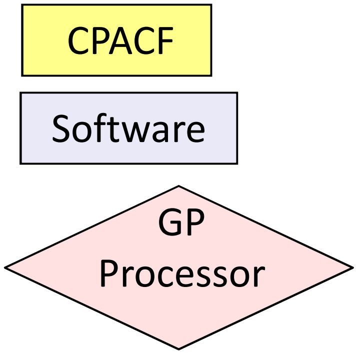
Software

GP Processor

- Phase 1 Negotiation / Key Generation
  - Handshake Layer
    - Authenticates Server (and Optionally Client) and generates Session Key
      - Uses ICSF or Crypto Card if available

      Accelerator Card (Clear Key Mode)

      Coprocessor Card (Secure Key Mode)



CPACF

Software

GP Processor

- Phase 2
  - Record Layer
    - Encypts/Decrypts data
      - Uses CPACF (clear key only) if available

Reasons for a Cryptographic Card for z/OS CS

- The z/OS Communications Server (CS) security implementations with SSL/TLS/AT-TLS and with IKE and IPSec rely exclusively on the CPACF hardware cryptography area of the System z processor for data payload encryption and decryption.
- CPACF does not help with any of the very expensive asymmetric operations involved in digital signatures used in the handshaking phases of SSL and IPSec.
- So WHAT might nevertheless justify the acquisition of a System z Crypto Card for such applications?
- If your needs approach more than 300 handshakes (SSL/TLS or AT-TLS) or negotiations (IKE with IPSec) per second and per CP assigned to the LPAR.
  - The acceleration function implemented by the Crypto Card in either accelerator mode or coprocessor mode would permit a much higher number of negotiations per second. (next page)
- If the savings in CPU provided with the use of the Crypto Card justifies the acquisition.
- If you are being required to use what is called Secured Key, which sets a Master Key for the hardware.
  - The coprocessor function of the Crypto Card provides the Secure Key function to establish this Master Key.
- If you are trying to minimize the frequency of Private Key changes associated with x.509 certificates or other security technologies as dictated by auditors for PCI, NIST, or other security mandates.
  - If you implemented Secure Key with Coprocessor mode, then only the master key that protects the Private Keys would need to be subjected to the more frequent key change intervals. You could avoid the renewing of Private Keys in most cases.
- If you are being required to comply with FIPS 140-2 levels 3 or 4, which provide tamper detection and response, and, in the case of level 4, even the zeroing out of the hardware cryptographic module.
- If you are unsure of future encryption requirements and it is budgetarily easier at this moment in time to order Cryptographic Cards rather than to wait.
- If you already have crypto cards for other types of applications that are already configured in accelerator or coprocessor mode and they have sufficient capacity to accommodate the added SSL or IKE operations.
- NOTES for Internet Key Exchange Daemon (IKED) and Network Security Services Daemon (NSSD)
  - If you are exploiting NSSD (Network Security Services Daemon), multiple crypto accelerator or coprocessor cards can help increase throughput when IKED is acting as an NSS client.
  - In contrast, IKED is single threaded and multiple crypto accelerator or coprocessor cards will not provide the same benefit as when IKED is an NSS client.
  - See the performance pages for Crypto on a your hardware version or consult next page.

Handshakes per Second

- Information below extracted from:
  - –http://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=ZSL03211USEN
  - –3.4.2. SSL Performance - System SSL with z/OS V1.13 and Cryptographic Support for z/OS V1R12-R13 (ICSF FMID HCR77A0)
  - –zEC12 Model 2827-HA1 (4 Central Processors)

Caching SID	Handshake	Client Auth	ETR	CPU Util %	Crypto Util %
100%	Avoided	no	24,808	98.44	N/A
no	Software	no	1,378	100	N/A
no	4CEX4C	no	9,003	56.29	99.4
no	4CEX4A	no	17,493	98.34	87.8
no	4CEX4A	yes	11,477	98.61	79.1

- The first row of the table shows the transaction rate when the client SSL session identifier is cached in the server resulting in the majority of the SSL handshake processing being avoided.
- The next four rows show the transaction rates when the client SSL session identifier is not cached in the server resulting in a full SSL handshake for each client connection.
- Using the CEX4C cryptographic hardware compared to using System SSL Software (second and third rows in the above table) produces an increase in throughput (number of SSL handshakes per second) of 6.5 times and reduces the CP utilization by 44%. The CP utilization of this measurement only reached 56.29% because the 4 CEX4C cards were fully utilized at 99.4% and limited the throughput capacity of this configuration. Adding additional CEX4C cards to this environment would allow for a higher ETR.
- The fourth row shows that a higher ETR can be achieved with the same 4 CEX4S adapters configured in Accelerator mode. In this measurement the average utilization of the CEX4A adapters was 87.8%, indicating that the 4 CEX4A adapters could process more than 19,000 SSL handshakes before reaching 100% utilization. The 17,493 ETR represents close to the maximum number of SSL handshakes that can be supported with this configuration because the 4 Central Processors are 98% utilized.
- If Client authentication is required the throughput of the server is considerably reduced, as shown in row 5 of the above table.

Displaying Cryptographic Capabilities with System SSL

```
System SSL: SHA-1 crypto assist is available
System SSL: SHA-224 crypto assist is available
System SSL: SHA-256 crypto assist is available
System SSL: SHA-384 crypto assist is available
System SSL: SHA-512 crypto assist is available
System SSL: DES crypto assist is available
System SSL: DES3 crypto assist is available
System SSL: AES 128-bit crypto assist is available
System SSL: AES 256-bit crypto assist is available
System SSL: ICSF FMID is HCR7770
System SSL: PCI cryptographic accelerator is not available
System SSL: PCIX cryptographic coprocessor is available
System SSL: Public key hardware support is available
System SSL: Max RSA key sizes in hardware - signature 4096, encryption 4096
```

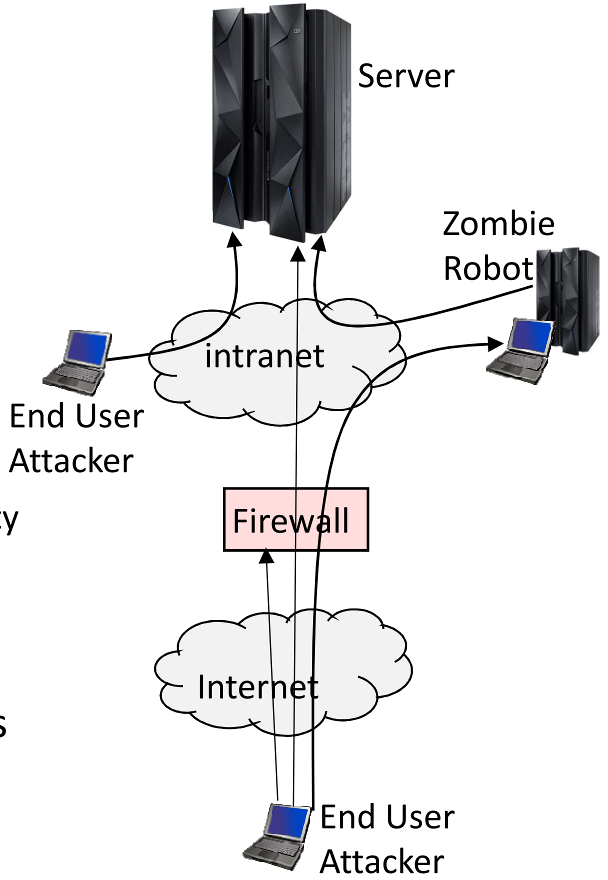
or

```
...
System SSL: PCIX cryptographic coprocessor is not available
System SSL: Public key hardware support is not available
```

Intrusion Detection Services (IDS)

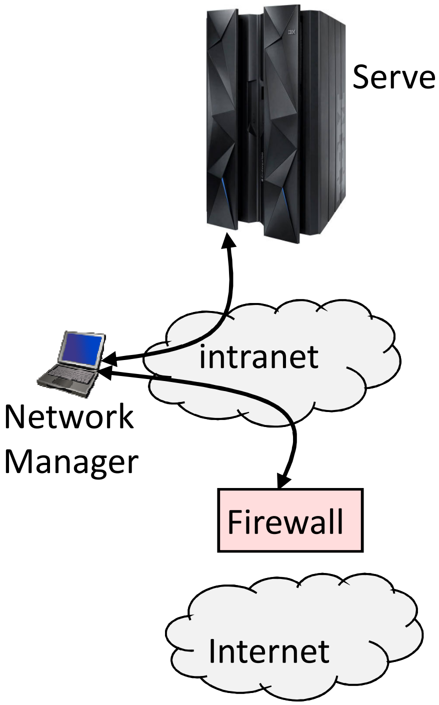
Intrusion Threat

- What is an intrusion?
  - Scan is Information Gathering
    - Basis for future attack
    - Network and system topology
    - Data location and contents
  - Eavesdropping/Impersonation/Theft
    - On the network/on the host
  - Amplifiers, Robot, or zombie installation
  - Attacks
    - Single Packet attacks - exploits system or application vulnerability
    - Denial of Service
      - Multi-Packet attacks - floods systems to exclude useful work
- Attacks can be deliberate or unintentional
  - Deliberate: malicious intent from outside or internal bots
  - Unintentional: various forms of errors on network nodes
- Attacks can occur from Internet or intranet
- Firewall can provide some level of protection from Internet
- Perimeter Security Strategy alone may not be sufficient.
  - Access permitted from Internet
  - Trust of intranet

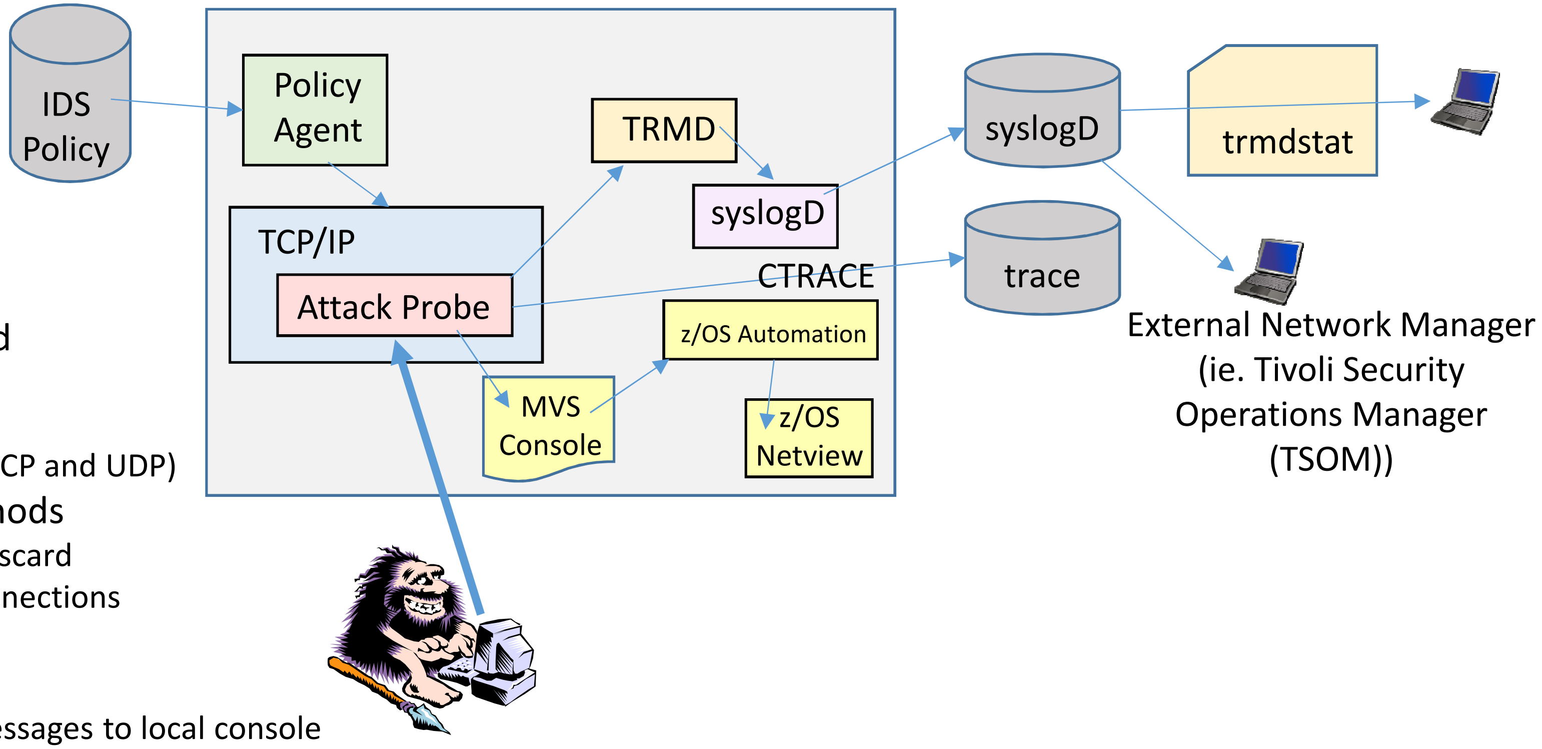


z/OS IDS versus External Firewall

- Not all problems perceived as Attacks are deliberate attacks by Hackers.
  - Hardware/Software bug may cause rogue machine
- Do you trust all intranet users?
  - Disgruntled employee
- When z/OS is encryption endpoint
  - Firewall IDS policies are not able to be applied to encrypted data.
- Network Managers may use external Firewall and z/OS IDS information concurrently.
  - ie. Tivoli Security Operations Manager



z/OS IDS Capabilities



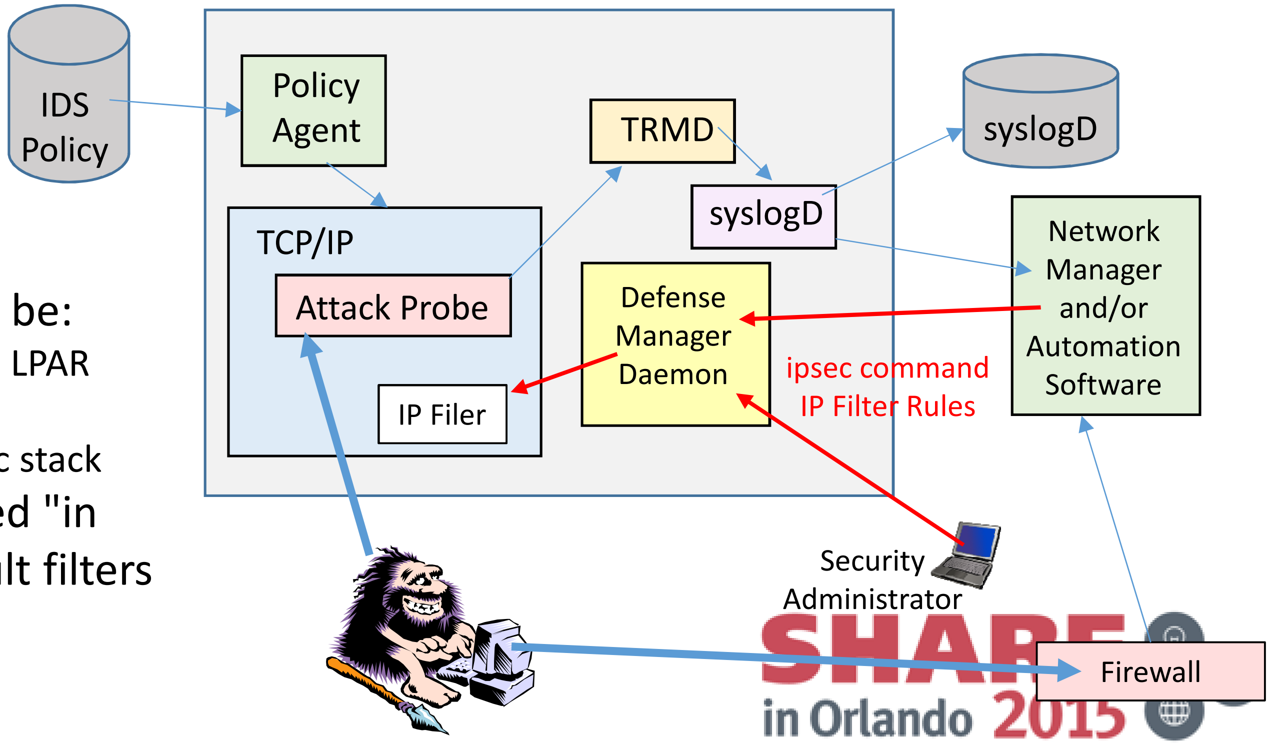
- Events detected
  - Scans
  - Attacks
  - Floods (TCP and UDP)
- Defensive methods
  - Packet discard
  - Limit connections
- Reporting
  - Logging
  - Event messages to local console
  - IDS packet trace
  - Notifications to Network Managers (ie. Tivoli NetView and Tivoli Security Operations Manager)
- z/OS IDS broadens intrusion detection coverage:
  - Evaluates inbound encrypted data - IDS applied after decryption
  - IDS policy checked after attack detected
    - Avoids overhead of per packet evaluation against table of known attacks
  - Detects statistical anomalies real-time
    - System has stateful data / internal threshholds that are unavailable to external IDSs
  - Policy can control prevention methods, such as connection limiting and packet discards

IDS Event Types

- Scans
  - TCP port scans
  - UDP port scans
  - ICMP scans
  - Sensitivity levels for all scans can be adjusted to control number of false positives recorded.
- Attacks
  - Malformed packet events
  - Inbound fragment restrictions
  - IP option restrictions
  - IP protocol restrictions
  - ICMP redirect restrictions
  - Flood events (physical interface flood detection and synflood)
  - Outbound raw restrictions
  - UDP perpetual echo
  - etc.
- Traffic Regulation
  - UDP backlog limit - management by port
  - TCP total connection and source percentage management by port
  - All TCP servers that use a UNIX process model to create a new process when a client connects to them should have a cap on the number of connections (FTP, otlenetD, etc.)

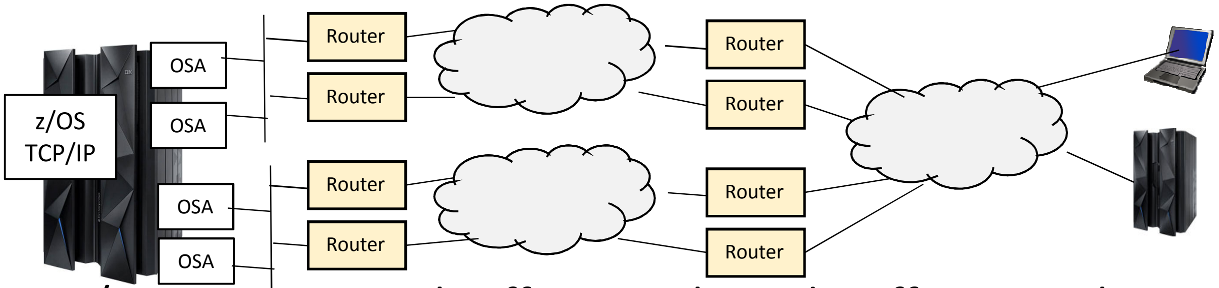
z/OS Defense Manager Daemon

- Allows authorized users to dynamically install time-limited, defensive filters via ipsec command:
  - Security Administrator on z/OS
  - Automation
- Defensive filtering is an extension to IDS capabilities
- Requires minimal IPsec configuration to enable IP packet filtering
- Uses ipsec command to control and display defensive filters
- Maintains record of defensive filters on DASD for availability in case of DMD restart or stack start/restart
- Defensive filter scope may be:
  - Global - all stacks on the LPAR where DMD runs
  - Local - apply to a specific stack
- Defensive filter are installed "in front of" configured/default filters (from policies and profile)



Policy Based Routing (PBR)

PBR Outbound Routing

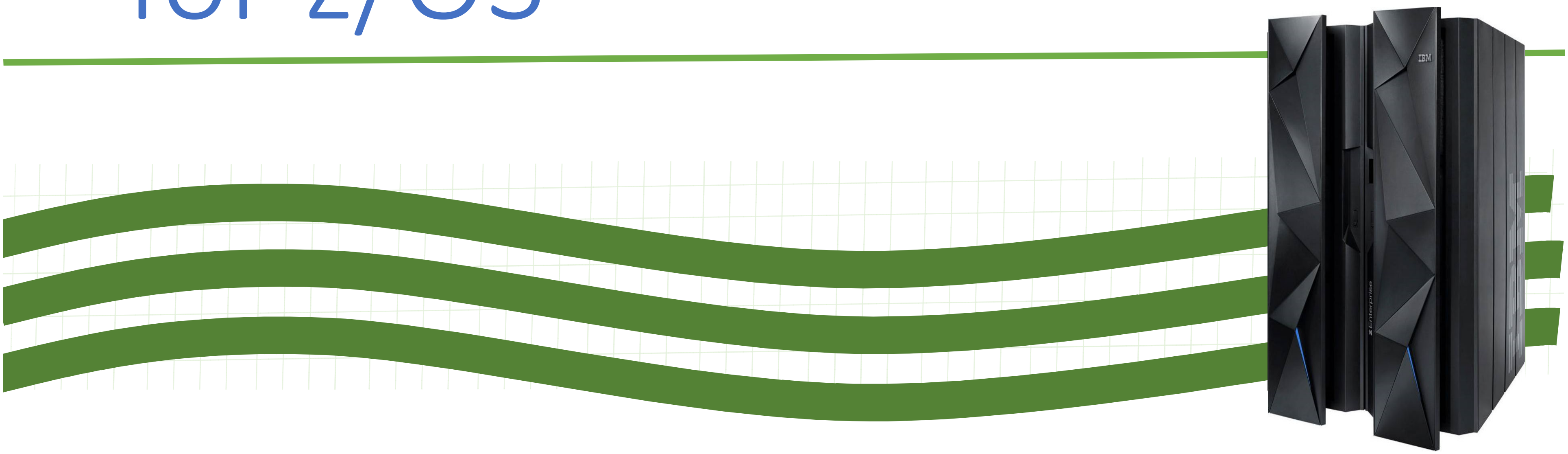


IPv6 support added in z/OS V2R1.

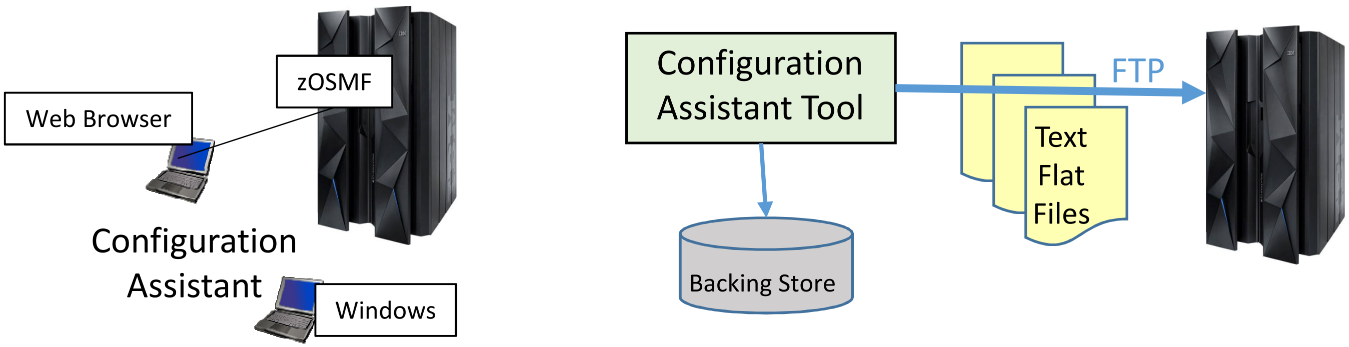
PBR is a great companion to VLAN for separation of traffic.

- z/OS IP Routing only effects Outbound Traffic – Data being sent FROM z/OS
  - First hop routers' routing tables determine Inbound Traffic – Data received by z/OS
    - Which of the OSAs is sent the traffic when there are multiple OSAs in the same subnet, etc.
- Whole Routing Table may include static routes and dynamic routes.
- PBR enables defining:
  - Types of traffic
  - Subsets of the Whole Routing Table
- Types of Traffic are defined by:
  - Protocol
  - IP Addresses (Local and Remote)
  - Ports (Local and Remote)
  - Job Name
- When Outbound Traffic matches PBR policy rule then action(s) define which subset(s) of Whole Routing Table to use for sending the traffic.
  - If a route is not found after searching the defined subset(s), the PBR rule also defines if the traffic should be sent using the Whole Routing Table or be discarded.

Configuration Assistant for z/OS

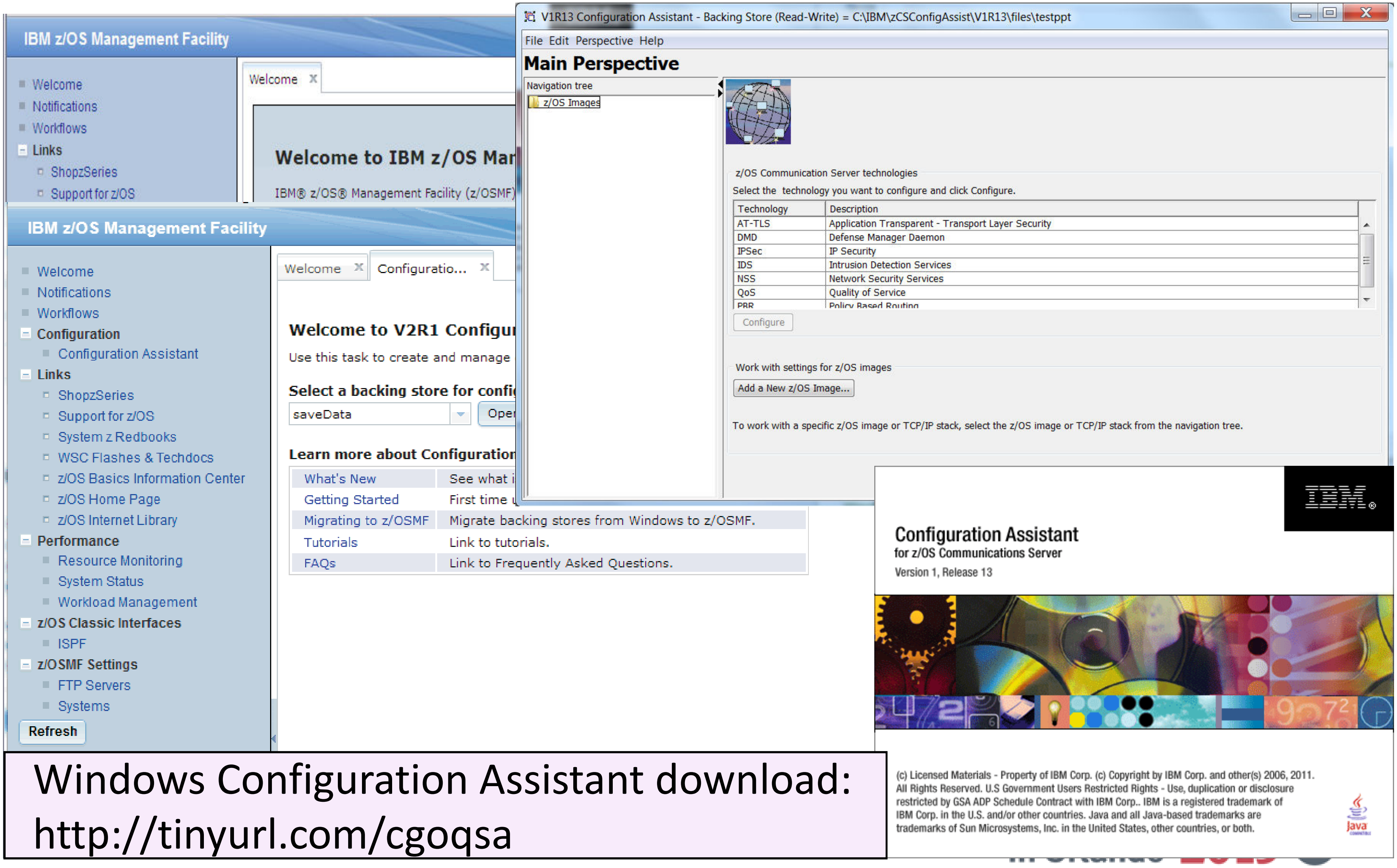


IBM Configuration Assistant for z/OS Communications Server



- Runs on Windows (prior to z/OS V2R1)
- Runs on zOSMF (available since z/OS V1R11)
  - Rewritten at z/OS V2R1 to support new improved Liberty WebSphere
- Configuration Assistant configurations are stored in binary files
  - Named “Backing Store” files (also referred to as Persistent Date Store)
  - Only Configuration Assistant for z/OS Communications Server can use Backing Store files!
  - Windows Tool can save Backing Store files on Windows, LAN Network drive, or z/OS
  - zOSMF Tool saves Backing Store files on z/OS
    - ➢ Auto-backup to protect against loss of changes due to web browser session interruptions
- To use Configuration Assistant configurations the tool is used to send text files to z/OS
  - Configuration Assistant uses FTP to send the text files (FTP Server is required on z/OS)
  - Many different text files can be generated by the Configuration Assistant
    - ➢ Separate policy file for each policy type (AT-TLS, IPsec, IDS, QoS, PBR)
    - ➢ Application setup files (IKED, NSSD, DMD, etc.)
- Existing z/OS policies may be imported into the Configuration Assistant
- Older versions of Configuration Assistant Backing Store files may be upgraded to a later version.

Configuration Assistant Tool



Welcome to V2R1 Configu

Use this task to create and manage

Select a backing store for confi

saveData

Oper

Learn more about Configuration

What's New	See what i
Getting Started	First time u
Migrating to z/OSMF	Migrate backing stores from Windows to z/OSMF.
Tutorials	Link to tutorials.
FAQs	Link to Frequently Asked Questions.

z/OS Communication Server technologies

Select the technology you want to configure and click Configure.

Technology	Description
AT-TLS	Application Transparent - Transport Layer Security
DMD	Defense Manager Daemon
IPSec	IP Security
IDS	Intrusion Detection Services
NSS	Network Security Services
QoS	Quality of Service
PBR	Policy Based Routing

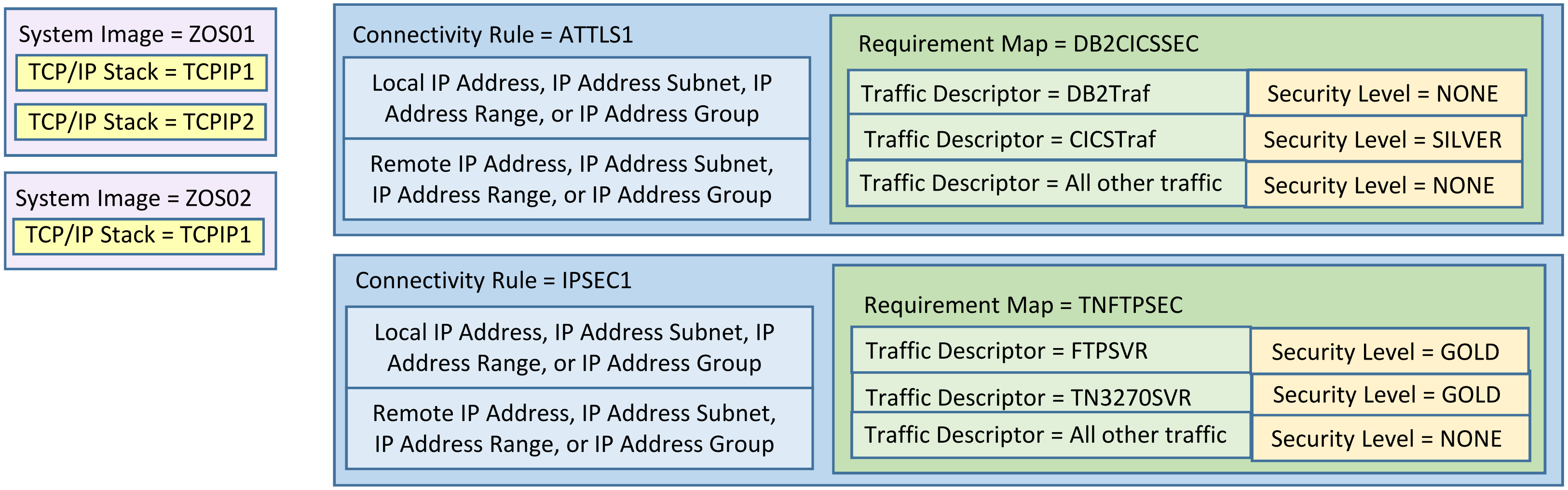
Work with settings for z/OS images

To work with a specific z/OS image or TCP/IP stack, select the z/OS image or TCP/IP stack from the navigation tree.

(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006, 2011. All Rights Reserved. U.S Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Windows Configuration Assistant download:
http://tinyurl.com/cgoqsa

AT-TLS and IPsec



System Image = ZOS01

TCP/IP Stack = TCPIP1

TCP/IP Stack = TCPIP2

System Image = ZOS02

TCP/IP Stack = TCPIP1

Connectivity Rule = ATTLS1

Local IP Address, IP Address Subnet, IP Address Range, or IP Address Group

Remote IP Address, IP Address Subnet, IP Address Range, or IP Address Group

Requirement Map = DB2CICSSEC

Traffic Descriptor = DB2Traf	Security Level = NONE
Traffic Descriptor = CICSTraf	Security Level = SILVER
Traffic Descriptor = All other traffic	Security Level = NONE

Connectivity Rule = IPSEC1

Local IP Address, IP Address Subnet, IP Address Range, or IP Address Group

Remote IP Address, IP Address Subnet, IP Address Range, or IP Address Group

Requirement Map = TNFTPSEC

Traffic Descriptor = FTPSVR	Security Level = GOLD
Traffic Descriptor = TN3270SVR	Security Level = GOLD
Traffic Descriptor = All other traffic	Security Level = NONE

1 Define system images (z/OS systems) and TCP/IP stacks

2 Select Type of Policy (AT-TLS or IPsec)

3 Define connectivity rules

- Complete security policy for all traffic between two endpoints

4 Specify IP Addresses for data endpoints (IP Address Groups Reusable)

5 Define Requirements maps (reusable)

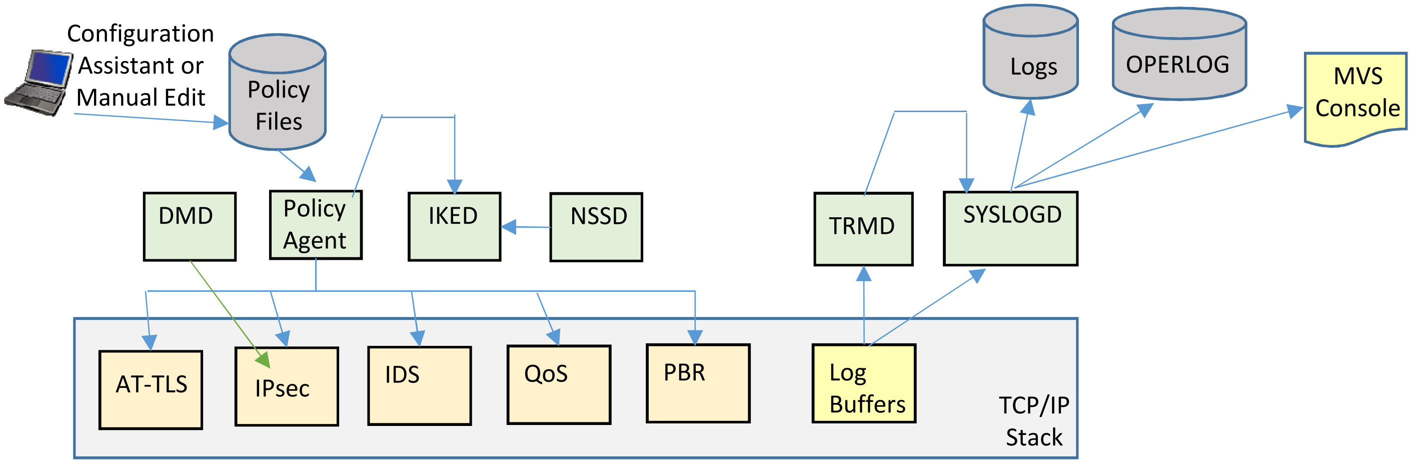
➢ Maps a set of Traffic Descriptors to Security Levels

6 Define Traffic Descriptors (reusable)

7 Define Security Levels (reusable)

Policy-based Network Security Components

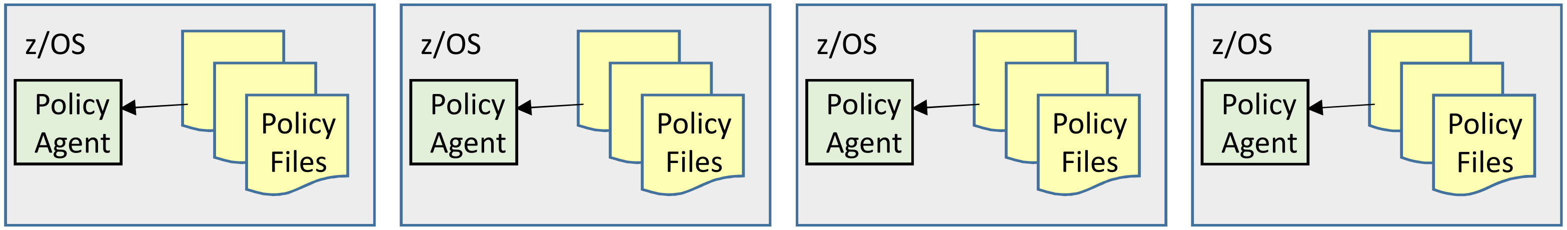
Lots of Different Policy Types and Started Tasks



- Policy Agent
  - Installs Policies into the TCP/IP stack
- TCP/IP Stack
  - Enforces the Policies
- DMD (Defense Manager Daemon)
  - ipsec command can be used to install temporary IP Filter rules.
- IKED (Internet Key Exchange Daemon)
  - Required for IPsec Dynamic VPN (Virtual Private Network) Tunnels
- NSSD (Network Security Server Daemon)
  - Required for IKEv2
  - Provides central RACF certificate repository for remote IKED applications
  - Provides DataPower access to RACF
- TRMD (Traffic Regulation Management Daemon)
  - Required for log messages to syslogd for IPsec and IDS
- SyslogD
  - Recommended for logging

Policy Server

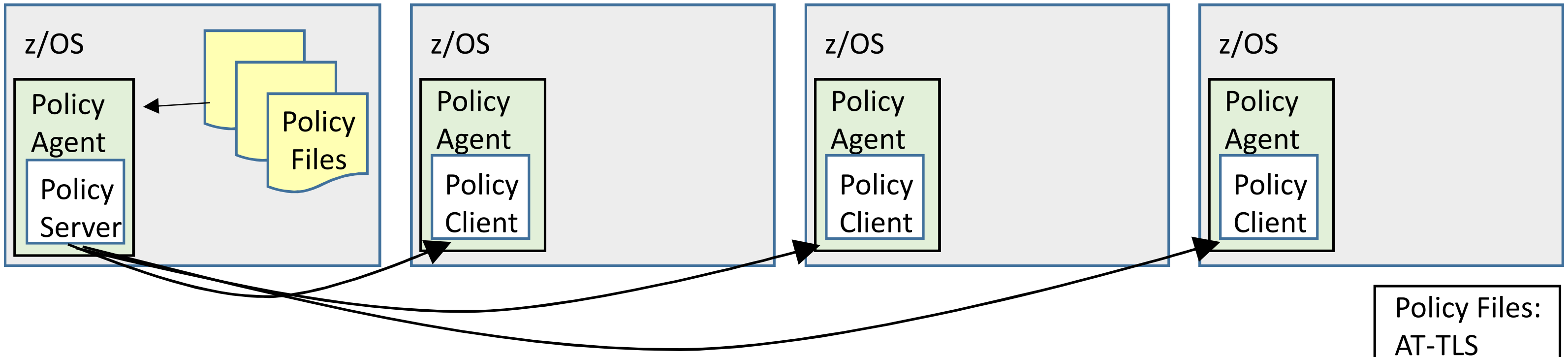
No Central Location for Policies



Policy Files:
AT-TLS
IPsec
IDS
QoS
PBR

- Each z/OS system Policy Agent may have their own Policy files stored locally.
- Policy Administration may be from a single location
  - Configuration (Configuration Assistant or manual edits) and monitoring (pasearch) can be done from a single location (administrator computer).

Policy Server



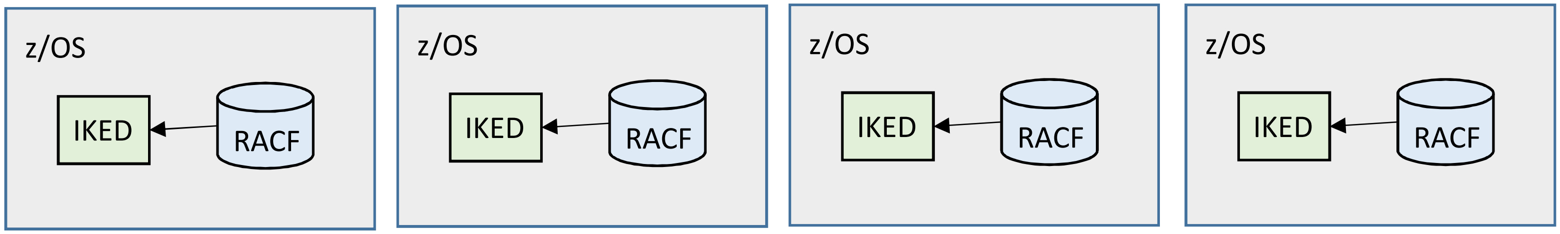
Policy Files:
AT-TLS
IPsec
IDS
QoS
PBR

- Centralized policy storage
  - Policy Server and Policy Clients can be non-sysplex, in sysplex, or cross-sysplex
    - IP connectivity required
- Policy Server provides policies to Policy Clients
  - Policy Client requests policies (ie. when client comes up or modify command)
  - When policies are changed on the server they are sent to clients
- Sysplex Not Required
  - Policy Server and Policy Clients can be non-sysplex, in sysplex, or cross-sysplex
- Availability
  - Backup Policy Server is supported
- Local Policies still supported
  - If Policy Client has policies locally stored, they will take precedence over policies from Policy Server.
- Administration may be from a single location (same as without Policy Server)
  - Configuration (Configuration Assistant or manual edits) and monitoring (pasearch) can be done from a single location (administrator computer).

Network Security Services for IPsec

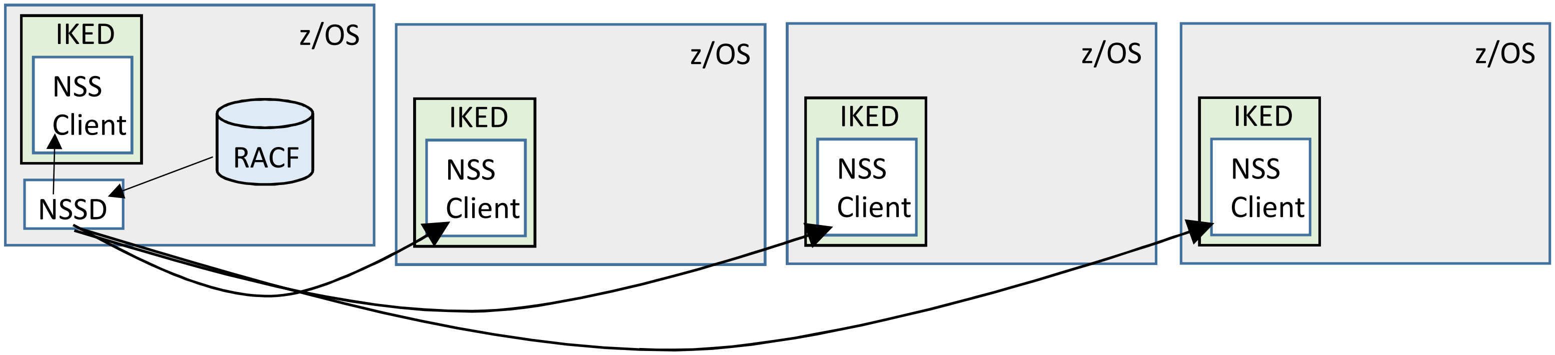
NSSD is required for IKEv2

No Central Location for Certificates and Keyrings



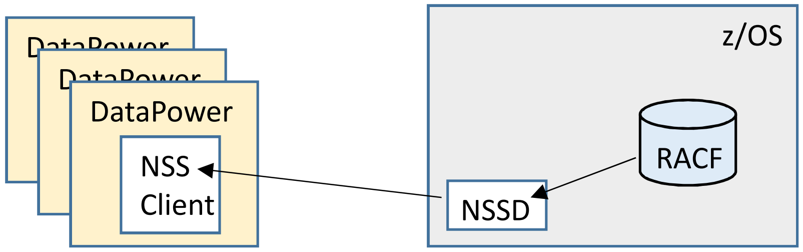
- Each z/OS system IKED may have their own certificate and keyring repository locally.
- Certificate and Keyring Administration may be from a single location
  - Configuration and monitoring can be done from a single location (administrator computer).

Network Security Services Daemon (NSSD)



- Centralized certificate and keyring repository
  - NSSD and IKED NSS Clients can be non-sysplex, in sysplex, or cross-sysplex
- NSSD provides certificate and keyring items to IKED NSS Clients
  - IKED NSS Clients requests policies (ie. when application starts or policy instance number changes)
- Sysplex Not Required
  - NSSD and IKED NSS Clients can be non-sysplex, in sysplex, or cross-sysplex
- Availability
  - Backup NSSD is supported
- Certificate and Keyring Administration may be from a single location (same as without NSSD)
  - Configuration and monitoring can be done from a single location (administrator computer).

NSSD DataPower Support

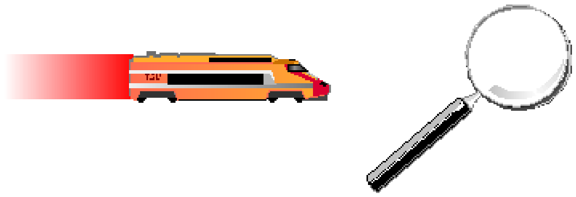


- WebSphere DataPower SOA Appliances:
  - Offloads XML translation for Web Traffic
- NSSD provides access to RACF certificates and keyrings for DataPower:
  - SAF-based authentication
  - Retrieval of RSA certificates from a SAF keyring
  - Private RSA key retrieval (clear key only)
  - RSA signature and decryption operations (secure key only)
- Monitoring:
  - nssctl command
  - Programmatically via Network Management Interface

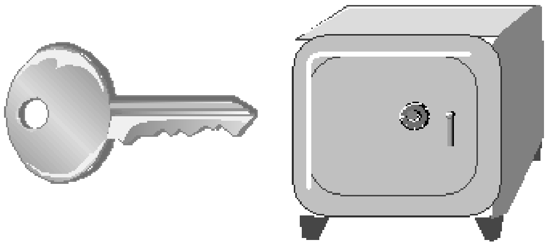
Appendix: Why Do We Care About Security?

Security as a Component of High Availability

- Redundancy



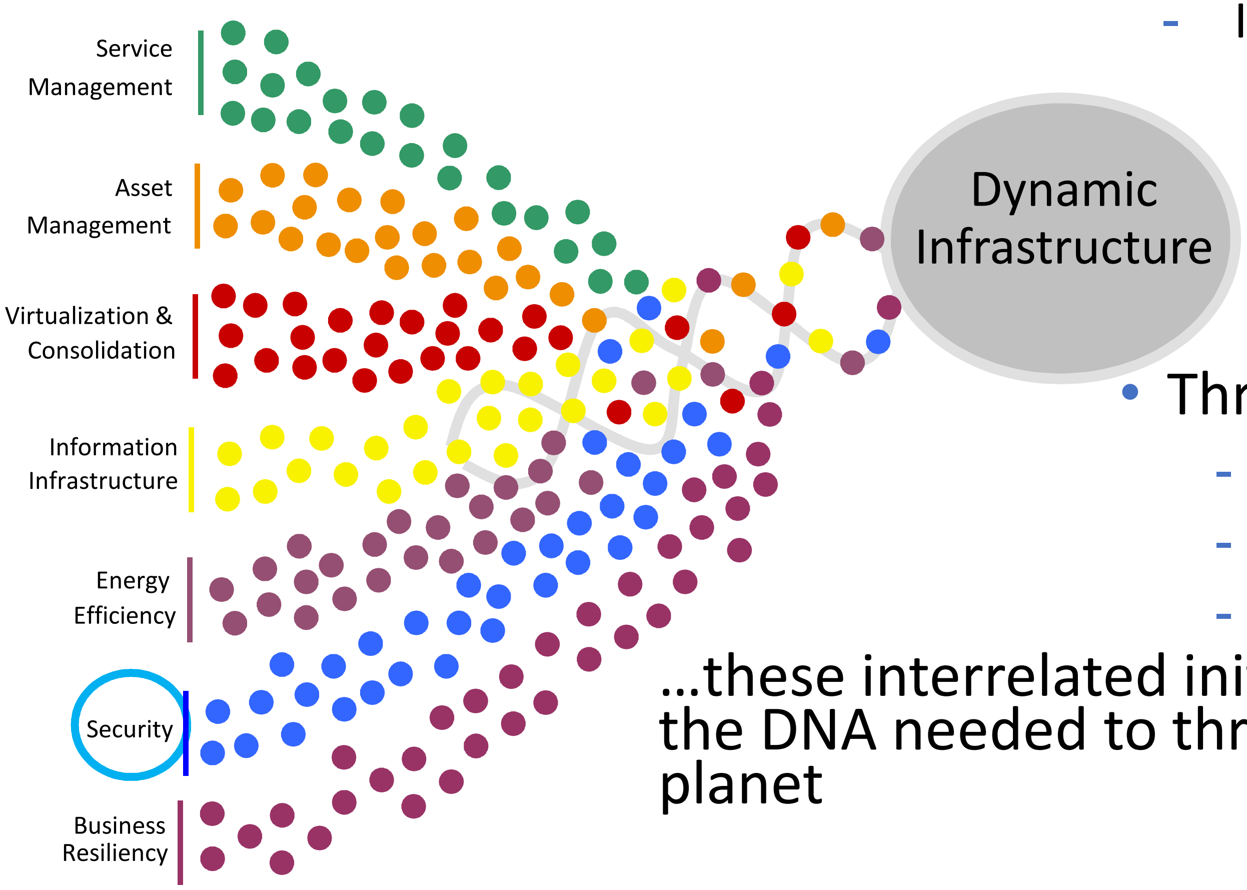
- Performance



- Security

Smarter Planet, Dynamic Infrastructure to Manage Risk

- New Possibilities:
  - Breakthrough productivity
  - Accelerated value creation
  - Increased velocity

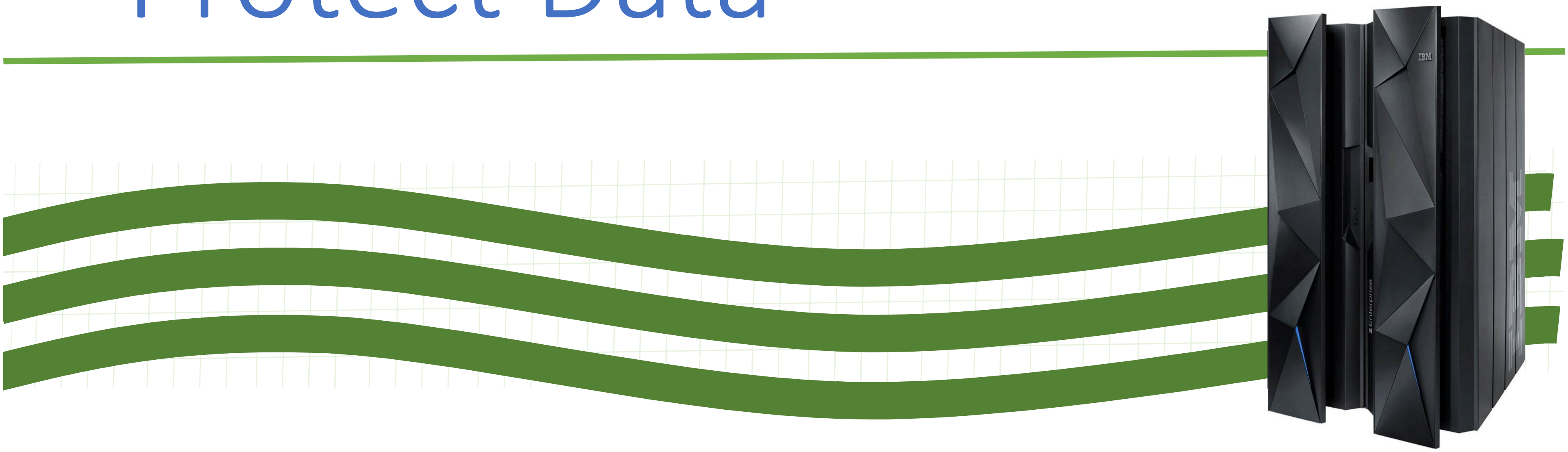


- Three client imperatives:
  - Improve Service
  - Manage Risk
  - Reduce Cost

…these interrelated initiatives can provide the DNA needed to thrive in a smarter planet

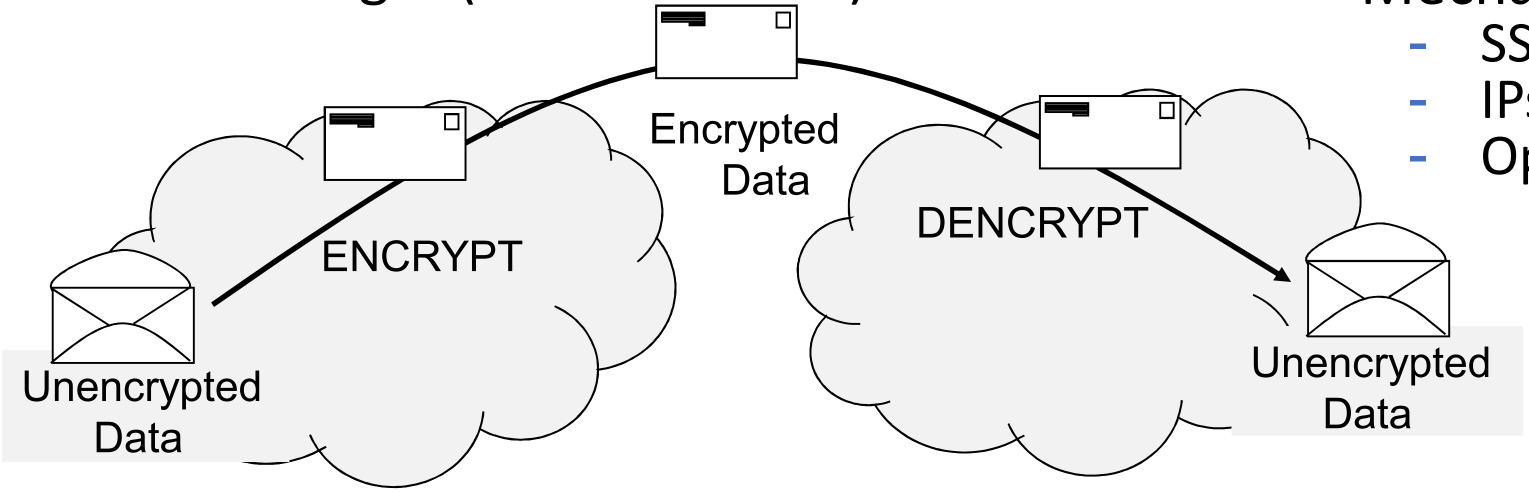
SHARE in Orlando 2015

Appendix: Where to Protect Data



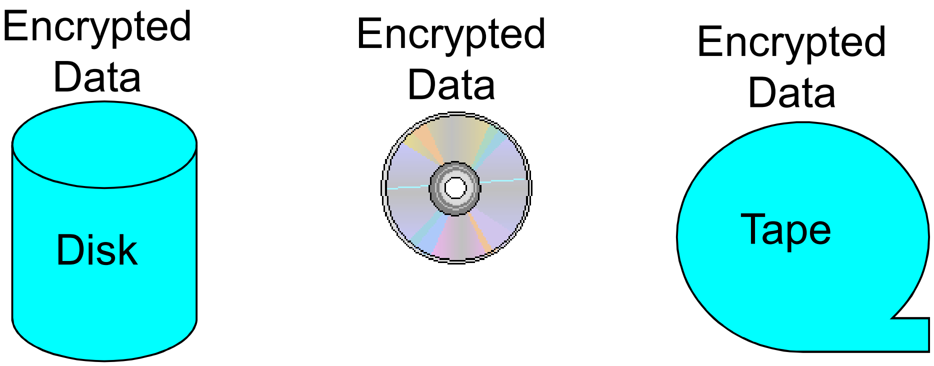
Data in Flight

- Data in Flight (Data in Transit)



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

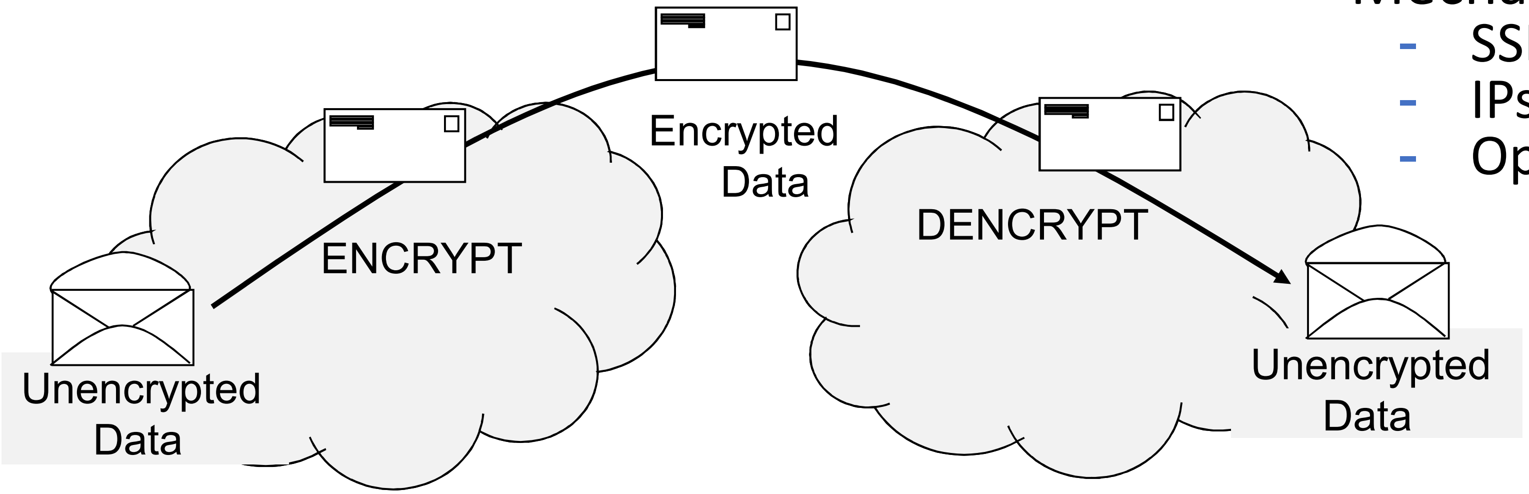
- Data at Rest (Archived Data)
- Data in Use (During Access for Processing)



- 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

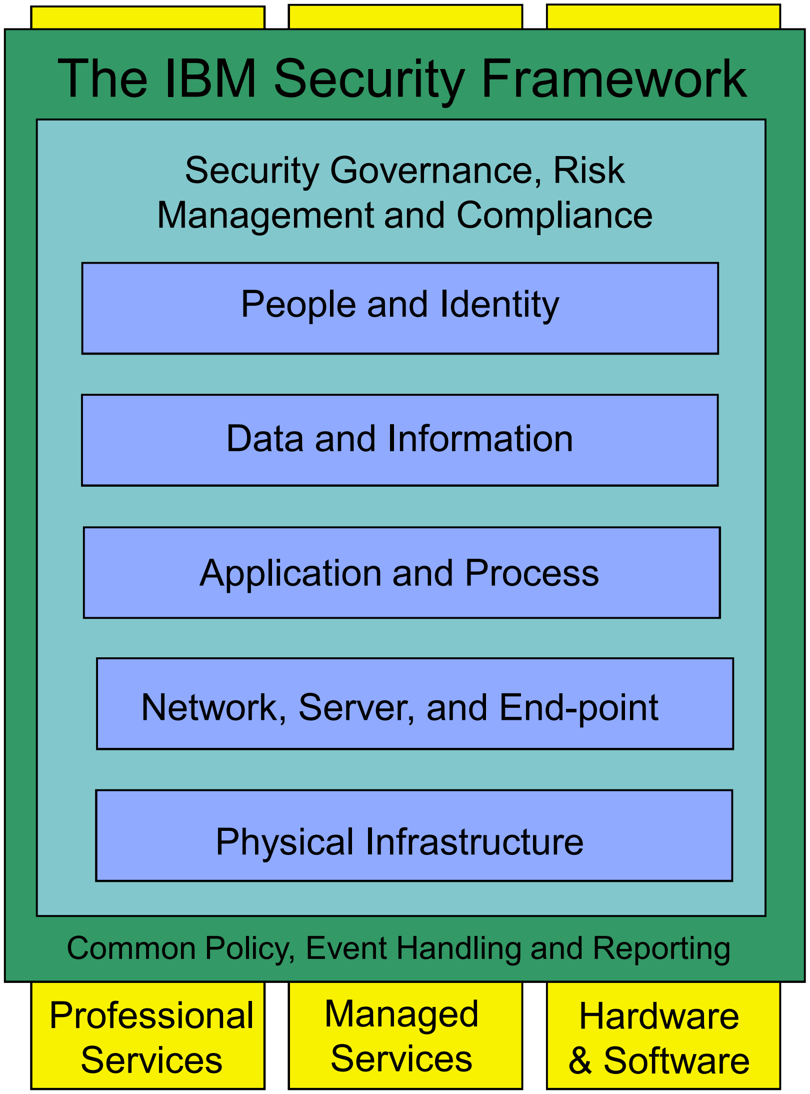
- Authenticate the partner in the connection
  - Is this the connection partner we are supposed to be communicating with?
- Verify the integrity of the transmission
  - Has the data been altered in transit?
- Encrypt the data in transit
  - Is anyone unauthorized able to intercept the transmission and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

Appendix: The Security Landscape: Security Architecture in General

Questions for Planning Security:

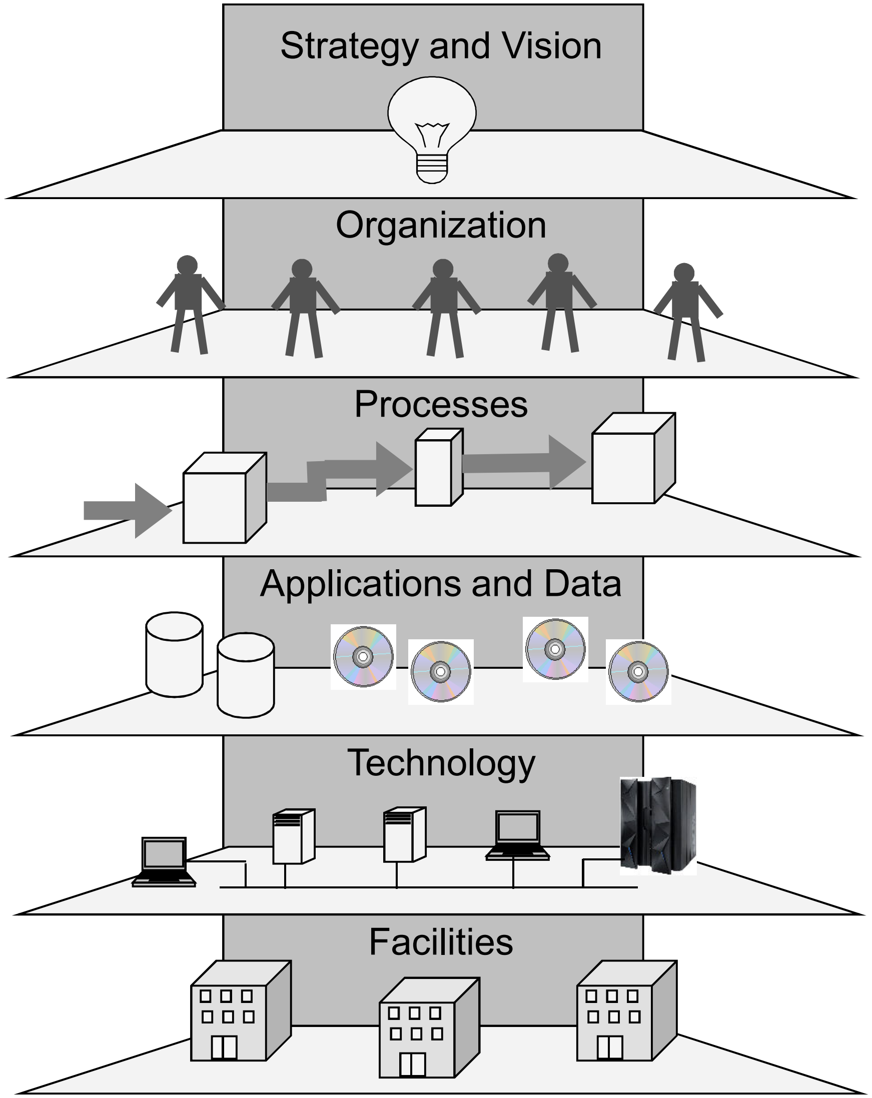
- **What** needs protecting?
- **How** should you protect?
- **Which** mechanisms or technologies should you use to protect?

The IBM Security Framework: What to Protect


The IBM Security Framework
Security Governance, Risk Management and Compliance
People and Identity
Data and Information
Application and Process
Network, Server, and End-point
Physical Infrastructure
Common Policy, Event Handling and Reporting
Professional Services
Managed Services
Hardware & Software

- 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

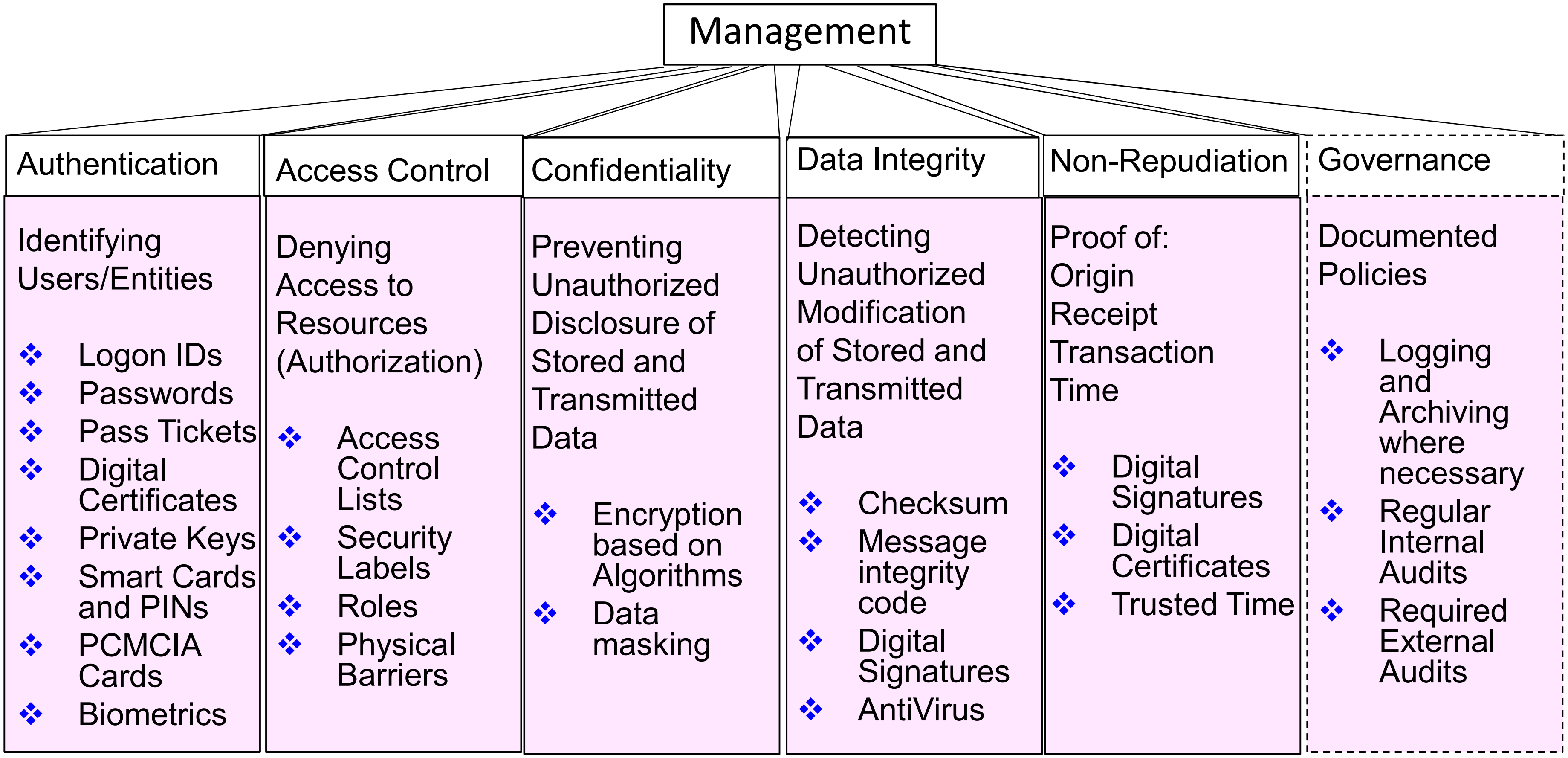
The IBM Security Framework: What to Protect



- Strategy and Vision:
  - Day to day activities for continuous operation.
- Organization
  - Communication channels, skills of people, training
- Processes
  - Accounts receivable and payable, Change management, incident management
- Applications and Data
  - Customer relationship management, enterprise resource management, database and transaction processing applications
- Technology
  - Hardware, software, networking protocols
- Facilities
  - Physical plant

Security Architecture Role: How & Which Way to Protect

Security Services and Mechanisms



Management

Authentication

Identifying Users/Entities

- Logon IDs
- Passwords
- Pass Tickets
- Digital Certificates
- Private Keys
- Smart Cards and PINs
- PCMCIA Cards
- Biometrics

Access Control

Denying Access to Resources (Authorization)

- Access Control Lists
- Security Labels
- Roles
- Physical Barriers

Confidentiality

Preventing Unauthorized Disclosure of Stored and Transmitted Data

- Encryption based on Algorithms
- Data masking

Data Integrity

Detecting Unauthorized Modification of Stored and Transmitted Data

- Checksum
- Message integrity code
- Digital Signatures
- AntiVirus

Non-Repudiation

Proof of:
Origin
Receipt
Transaction
Time

- Digital Signatures
- Digital Certificates
- Trusted Time

Governance

Documented Policies

- Logging and Archiving where necessary
- Regular Internal Audits
- Required External Audits

International Standard ISO 7498-2, “Security Architecture”

Web Pages

- URLs for Publications
  - http://www.ibm.com/systems/z/os/zos/bkserv/index.html
  - http://www.redbooks.ibm.com
- URLs for z/OS Communications Server and GUI Download
  - http://www.ibm.com/software/network/commserver/zos/support/
  - http://www.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=DB530&dc=D430&dc=D410&dc=D420&dc=DB510&dc=DB550&q1=Configuration+Assistant&uid=swg24013160&loc=en_US&cs=utf-8&lang=en
  - or better:
    - ➢ http://www.ibm.com/software/network/commserver/zos/support/
    - ➢ then select "IBM Configuration Assistant for z/OS Communications Server" in "Download" section of the page
- Main Security Web Pages:
  - https://www.pcisecuritystandards.org/
  - http://www.iss.net/
  - http://www.ibm.com/servers/eserver/zseries/zos/security
  - http://www.ibm.com/systems/z/security/
- IBM Mainframe Servers
  - http://www.ibm.com/servers/eserver/zseries
- IBM zEnterprise Servers Network Technologies
  - http://www.ibm.com/servers/eserver/zseries/networking/technology.html
- z/OS Communications Server
  - http://www.ibm.com/software/network/commserver/zos/

Web Pages (cont.)

- Communications Server for Linux on System z
  - http://www.ibm.com/software/network/commserver
  - http://www.ibm.com/software/network/commserver/library
- Communication Controller for Linux on System z
  - http://www.ibm.com/software/network/ccl
- PKI Services web site:
  - http://www.ibm.com/servers/eserver/zseries/zos/pki
- PKI Services Red Book:
  - http://www.redbooks.ibm.com/abstracts/sg246968.html
- ITSO Redbooks
  - http://www.redbooks.ibm.com
- RACF web site:
  - http://www.ibm.com/servers/eserver/zseries/zos/racf
- IBM Washington Systems Center Technical Sales Support
  - http://www.ibm.com/support/techdocs/
- Request for Comment (RFC)
  - http://www.rfc-editor.org/rfcsearch.html
  - http://www.rfc-editor.org/
- Online Courses (search for cryptography)
  - http://coursera.org

IBM Manuals

- IBM z/OS and z/OS Communications Server Manuals
  - z/OS Communications Server IP Configuration Guide (z/OS V1.13 SC31-8775, z/OS V2.1+ SC27-3650)
  - z/OS Communications Server IP Configuration Reference (z/OS V1.13 SC31-8776, z/OS V2.1+ SC27-3651)
  - z/OS IP Diagnosis Guide (z/OS V1.13 GC31-8782, z/OS V2.1+ GC27-3652)
  - z/OS IP System Administrator Commands (z/OS V1.13 SC31-8781, z/OS V2.1+ SC27-3661)
  - z/OS Four Volumes of IP Messages (z/OS V1.13 SC31-8783, SC31-8784, SC31-8785, SC31-8786, z/OS V2.1+ SC27-3654, SC27-3655, SC27-3656, SC27-3657)
  - z/OS Migration Manual (z/OS V1.13 GA22-7499, z/OS V2.1+ GA32-0889)
  - z/OS System SSL Programming Guide (z/OS V1.13 SC24-5901, z/OS V2.1+ SC14-7495)
  - z/OS Integrated Cryptographic Services (ICSF) System Programmer Guide (z/OS V1.13 SA22-7520, z/OS V2.1+ SC14-7507)
  - z/OS Cryptographic Services PKI Services Guide and Reference (z/OS V1.13 SA22-7693, z/OS V2.1+ SA23-2286)
  - z/OS Security Server RACF Security Administrator's Guide (z/OS V1.13 SA22-7683, z/OS V2.1+ SA23-2289)
  - z/OS Security Server RACF Command Language Reference (z/OS V1.13 SA22-7687, z/OS V2.1+ SA23-2292)
  - z/OS UNIX System Services Planning (z/OS V1.13 GA22-7800, z/OS V2.1+ GA32-0884)
  - z/OS UNIX System Services User's Guide (z/OS V1.13 SA22-7801, z/OS V2.1+ SA23-2279)
  - z/OS UNIX System Services Command Reference (z/OS V1.13 SA22-7802)
- RACF Command Samples for TCP/IP on z/OS
  - SYS1.TCPIP.SEZAINST(EZARACF)

IBM Manuals (cont.)

- IBM RedBooks
  - Communications Server for z/OS V1R11 TCP/IP Implementation
    - Volume I: Base Functions, Connectivity, and Routing (SG24-7798)
    - Volume II: Standard Applications (SG24-7799)
    - Volume III: High Availability, Scalability, and Performance (SG24-7800)
    - Volume IV: Security and Policy-based Networking (SG24-7801)
  - Communications Server for z/OS V1R12 TCP/IP Implementation
    - Volume I: Base Functions, Connectivity, and Routing (SG24-7896)
    - Volume II: Standard Applications (SG24-7897)
    - Volume III: High Availability, Scalability, and Performance (SG24-7898)
    - Volume IV: Security and Policy-based Networking (SG24-7899)
  - Communications Server for z/OS V1R13 TCP/IP Implementation
    - Volume I: Base Functions, Connectivity, and Routing (SG24-7996)
    - Volume II: Standard Applications (SG24-7997)
    - Volume III: High Availability, Scalability, and Performance (SG24-7998)
    - Volume IV: Security and Policy-based Networking (SG24-7999)
  - Communications Server for z/OS V2R1 TCP/IP Implementation
    - Volume I: Base Functions, Connectivity, and Routing (SG24-8096)
    - Volume II: Standard Applications (SG24-8097)
    - Volume III: High Availability, Scalability, and Performance (SG24-8098)
    - Volume IV: Security and Policy-based Networking (SG24-8099)

System z Lab Services Security Offerings

System z security review and enhancement services

Is the client's System z environment secure enough considering their business, policy, or regulatory requirements?

Consultants recommend how to mitigate weaknesses and enhance security protections leveraging the security architecture analysis, the z/OS security manager analysis, or the specific components' configuration security analysis

Enterprise encryption certificate creation and management services

Does the client currently pay an external vendor for signed certificates and is the client concerned with year-to-year costs? Has the client considered centrally managed certificates?

Stop paying someone else and become your own certificate authority using the tools you already own. Running a Certificate Authority (CA) on z/OS and leveraging PKI Services for z/OS to sign certificates used internally can save money, reduce turnaround time for certificate fulfillment and improve overall enterprise security.

System z encryption hardware exploitation services

Has the client purchased IBM System z cryptographic hardware and expressed concerned with centralized encryption key management and exploitation?

System z provides exceptional performance and function via cryptographic coprocessors and accelerators. Related software products such as ICSF, EKMF, ACSP can unleash the hardware's functionality. Lab Services consultant assist with designing, deploying and configuring these cryptographic solutions with best practices for secured key management

PCI and other security standard compliance for System z services

Is the client planning to have System z be compliant with PCI, HIPAA, FIPS 140-2, or other security regulations?

This offering provides technical assistance to prepare your client's System z environment to be compliant with requirements from security standards such as PCI DSS, HIPAA, ISO/IEC 27000- series, Sarbanes–Oxley. Consultants also have the breath of experience to discuss security solutions beyond these standards to fit the client business needs.

Enterprise LDAP identify directory on z/OS enablement services

Is the client looking for a stable high performance directory server and/or could the client benefit from centralized identities across z/OS and distributed platforms?

Tivoli Directory Server for z/OS (TDS z/OS) is an identity directory server following Lightweight Directory Access Protocol (LDAP) for LDAP-compliant enterprise middleware platforms. Allow your enterprise to take your identities into a centralized repository while benefiting from the inherent high scalability, availability and security that comes with z/OS.

Cloud on System z Security services

Is the client concerned with security enforcement in their Cloud on System z solution? Does the client need to secure virtual environments based on Linux on System z and z/VM?

This offering provides: the security expertise required to assess, design and implement a secure Cloud solution on System z ensuring all infrastructure layers to the O.S. and middleware are secure. It also addresses data segregation, multi-tenant security, standards compliance, and the secure integration between System z and the Cloud management platform

Enterprise System z network security audit compliance services

Is the client looking to secure z/OS or Linux network communications or resources? Does the client want to achieve a secure environment through new or existing z/OS Communications Server functions?

Lab Services consultants assist customers in meeting security regulatory (ie HIPPA, PCI) and risk mitigation goals for their Enterprise System z network. This offering provides a recommended design and implementation of System z network security features to comply with your security policy and to meet regulatory audit compliance.

Storage encryption key management centralization services

Does the client's environment: need centralized key management for device based encryption solutions or need to share encrypted data with business partners or their customers?

Leveraging encryption of data on disk or tape is a valuable direction for clients to proceed. In many instances, it is a statutory mandate as well. Lab Services can assist clients with design, implementation and installation of centralized key management servers for device based encryption such as tape or disk encryption.

Contact: stgls@us.ibm.com

Visit: ibm.com/systems/services/systemz

End of Topic