

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

Security Workshop

Security in z/OS Communications Server



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 features unless a specific OSA-Express feature is mentioned.

Agenda

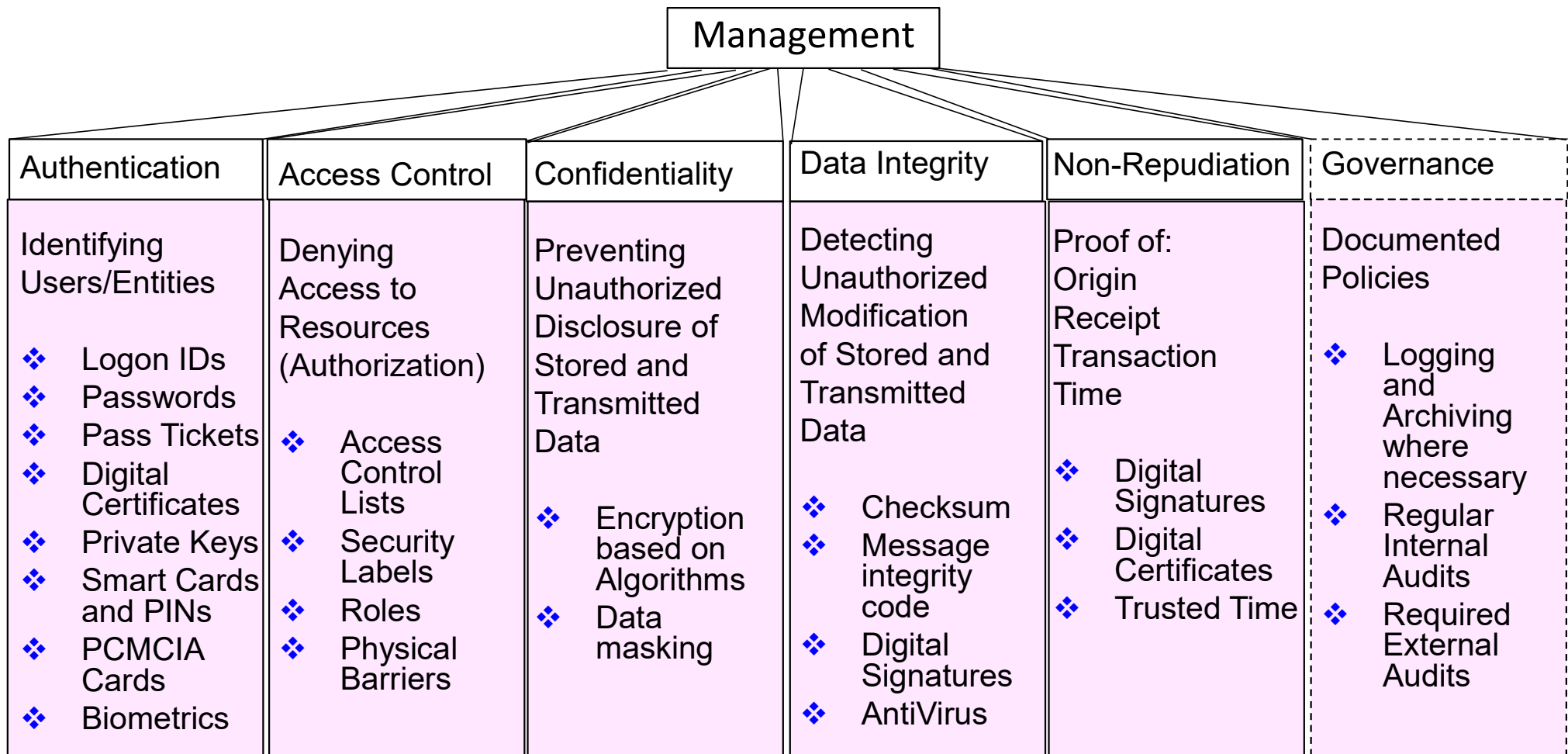
- z/OS Communications Server Network Security
- Policy-based Network Security
- IPsec
- Application Transparent – Transport Layer Security (AT-TLS)
- Intrusion Detection Services (IDS)
- Policy-based Routing (PBR)
- Quality of Service (QoS)
- Network Configuration Assistant for z/OS
- Policy-based Network Security Components
- Enterprise Security Roles
- Centralized Policy Agent
- Network Security Services for IPsec
- z/OS Communications Server Usage of Cryptographic Hardware
- Pervasive Encryption

z/OS Communications Server Network Security



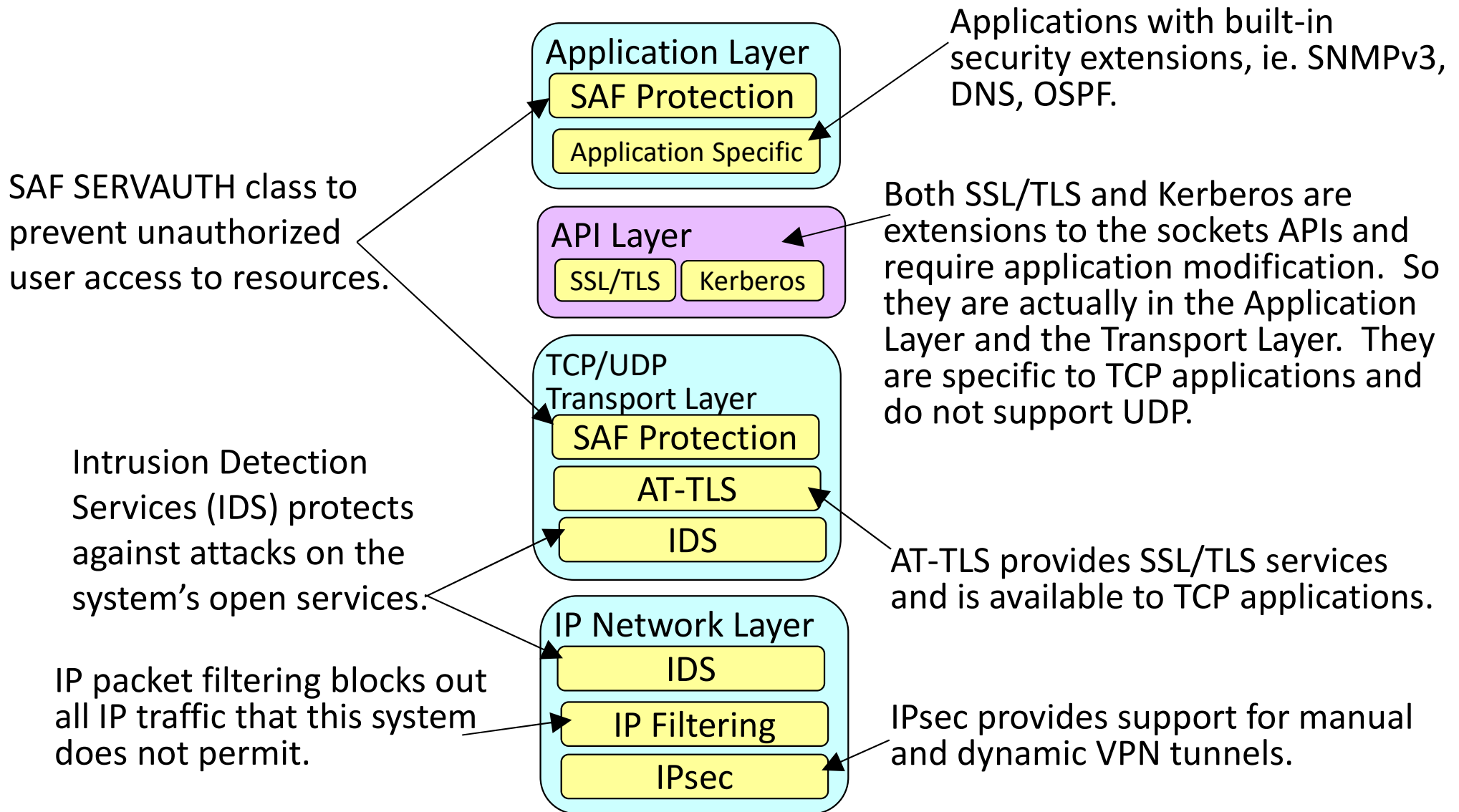
Security Architecture Role: How & Which Way to Protect

Security Services and Mechanisms



International Standard ISO 7498-2, "Security Architecture"

Protocol Stack View of TCP/IP Security Features

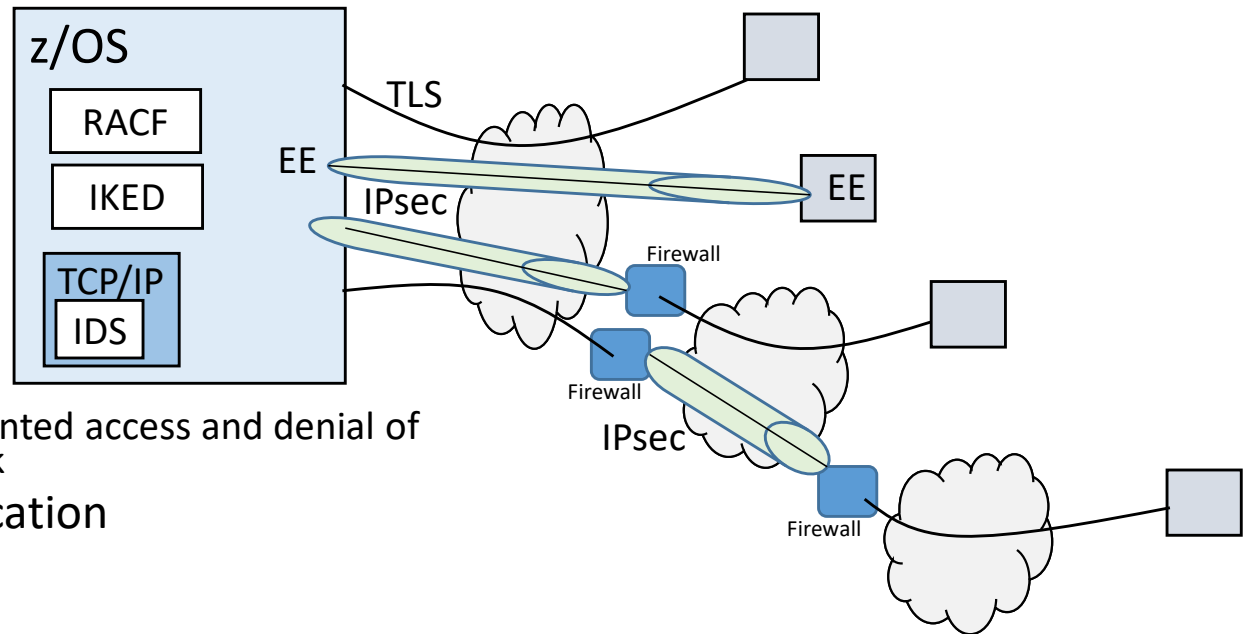


z/OS Communications Server Security Roles and Objectives

- 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
 - z/OSMF Network Configuration Assistant for z/OS Communications Server to simplify customization

Policy-based Network Security

IP Filtering and IPsec

Application Transparent – Transport Layer Security (AT-TLS)

Intrusion Detection Services (IDS)

Defense Manager Daemon (DMD)

Policy Based Routing (PBR)

Quality of Service (QoS)

Central Policy Server

Network Security Services (NSS)

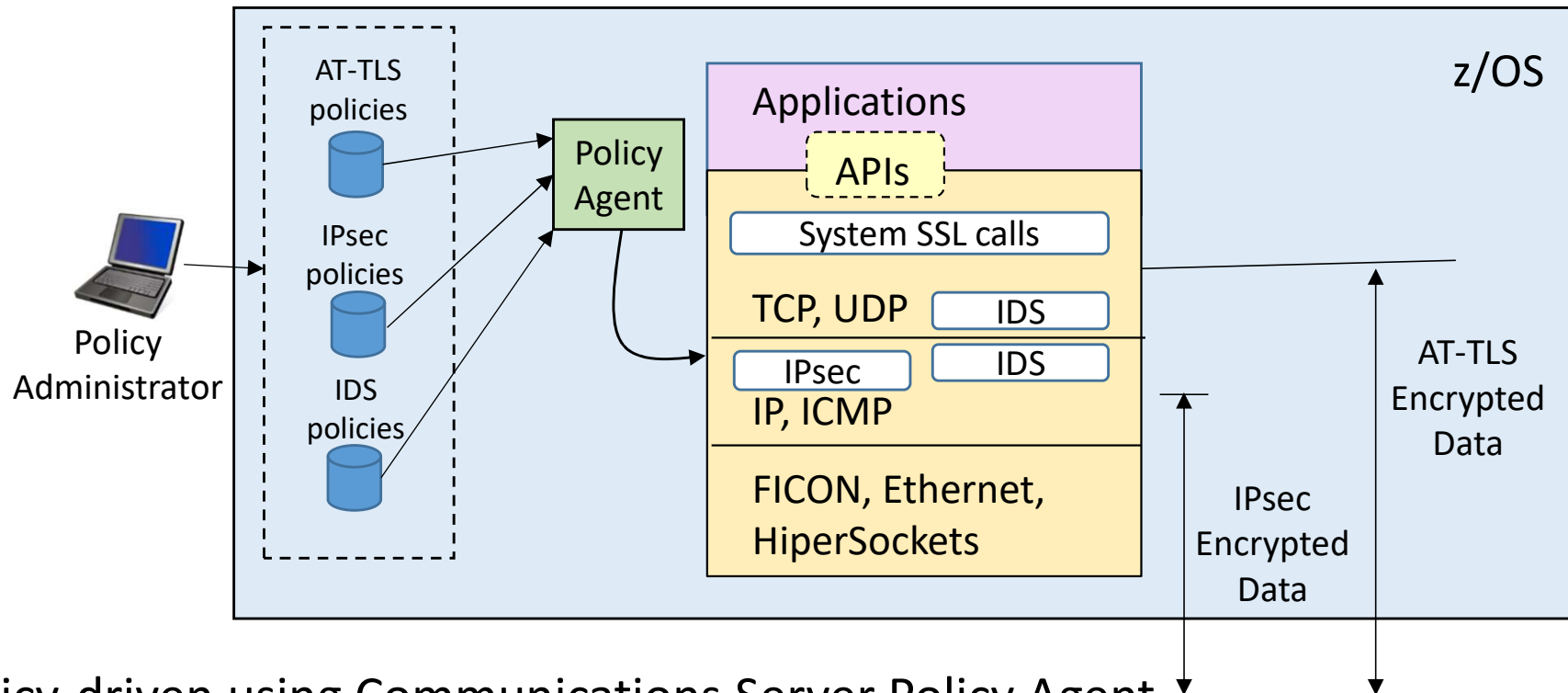
z/OS Encryption Readiness Technology (zERT)

TCP/IP Profile – z/OSMF Network Config but not part of Policy Agent

Cloud Configuration – z/OSMF Network Config but not part of Policy Agent



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, and IDS
- Configure policies with a single, consistent administrative interface using Network 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

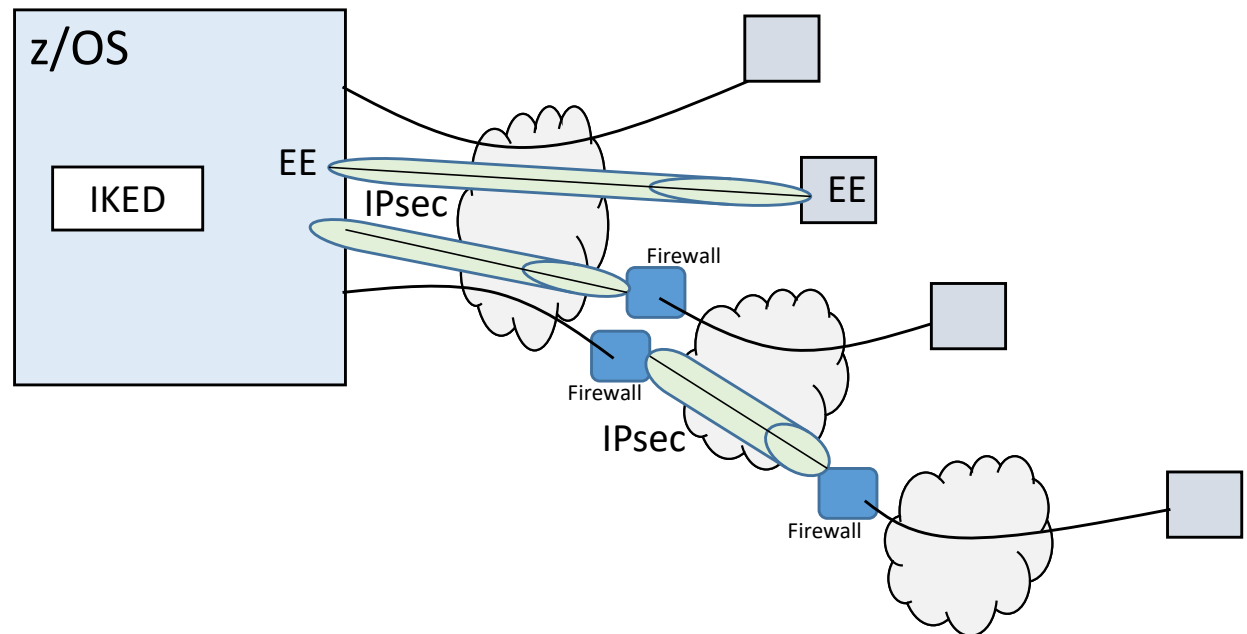
IPsec

IP Filtering
IPsec



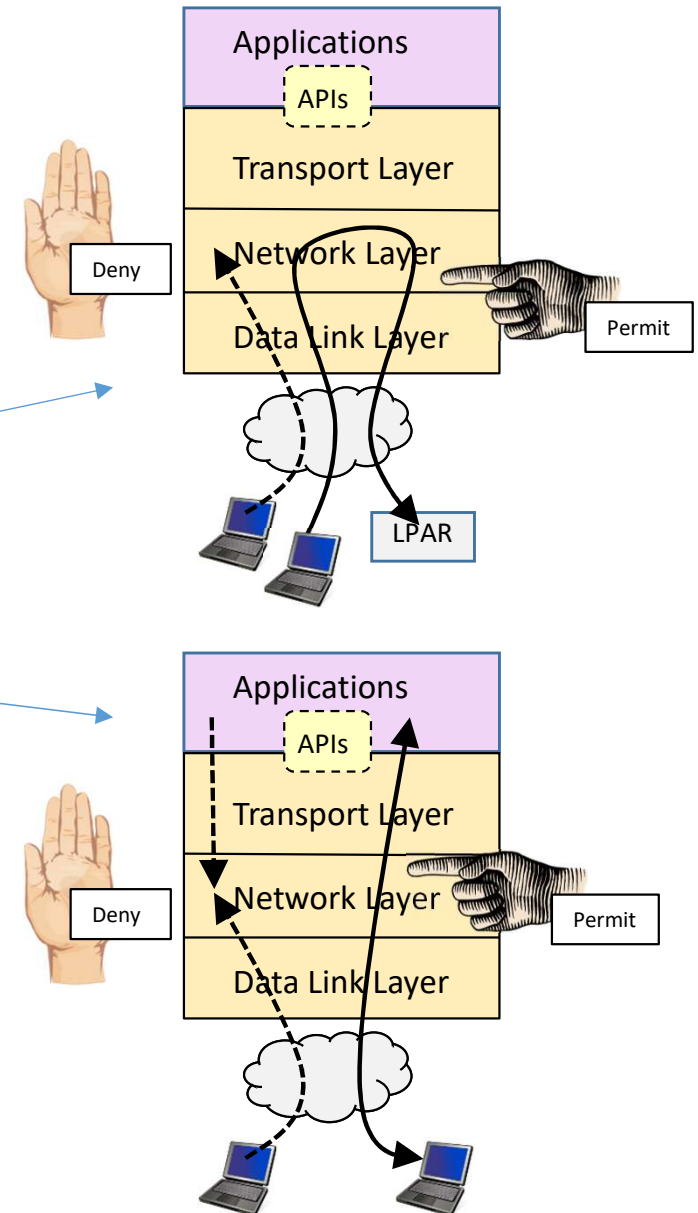
z/OS IPsec Support

- 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

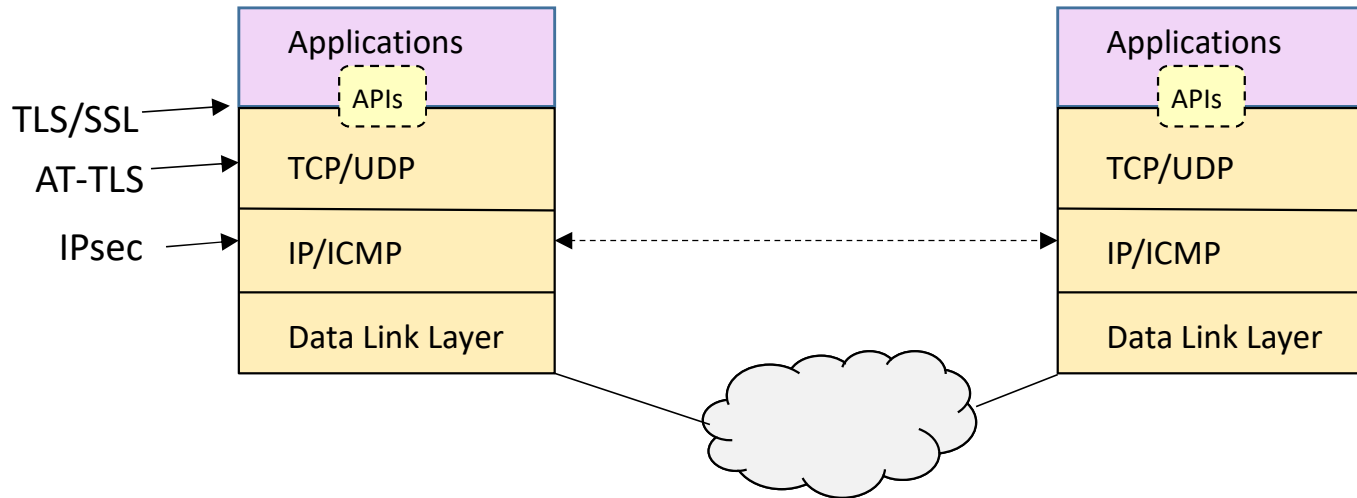


IP Packet Filtering Basics

- 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)



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)

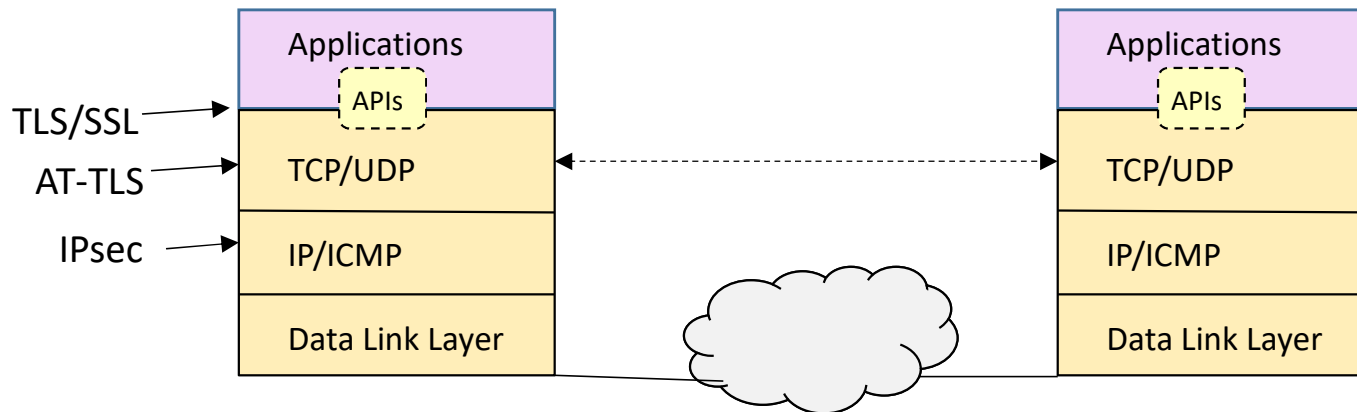
z/OS Communications Server IPsec Features

- 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
 - Network 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)

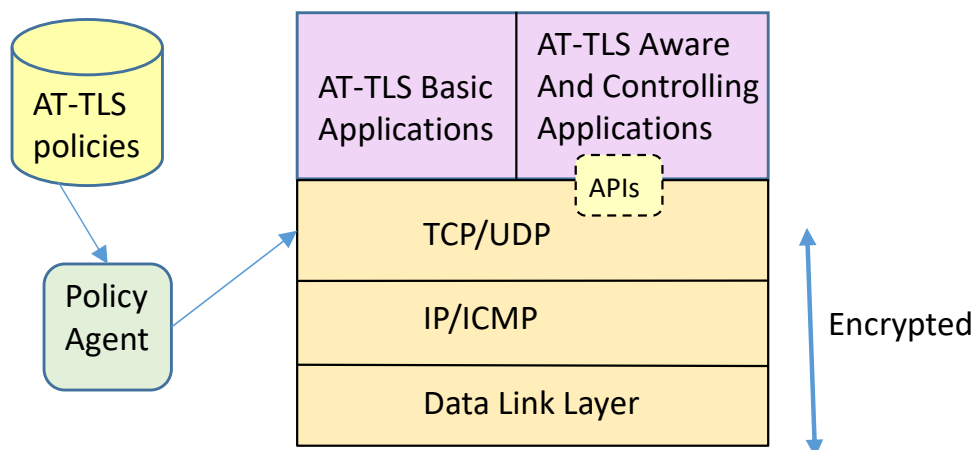


Transport Layer Security (TLS) Protocol Overview



- 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)



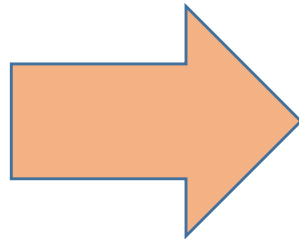
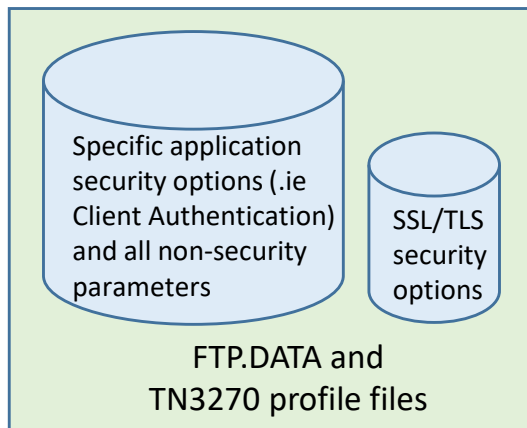
Application Specific TLS FTP.DATA Parameters	Application Specific TLS TN3270 Parameters	AT-TLS
Server Authentication TLSMECHANISM FTP	Server Authentication SECUREPORT	Basic Application FTP.DATA TLSMECHANISM ATTLS TN3270 Profile TTLSPT
Client Authentication SECURE_LOGIN REQUIRED	Client Authentication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

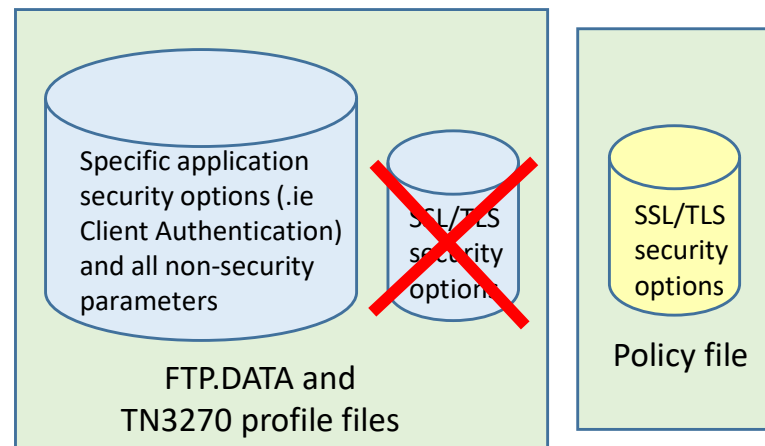
AT-TLS Enabling for TN3270 and FTP

- Both the FTP server and client, and the TN3270 server on z/OS currently (and prior to AT-TLS) have “application specific” SSL/TLS support.
 - Migrate SSL/TLS support to AT-TLS.
- FTP and TN3270 are enabled for AT-TLS to be AT-TLS “Aware” and “Controlling” applications.
- "Move" the SSL/TLS-specific configuration from FTP.DATA and TN3270 profile into the common AT-TLS policy format.
- Keep application-specific security options in FTP.DATA and TN3270 profile application configuration files.

“Application Specific” TLS Support



AT-TLS Support



IPsec and AT-TLS Comparison

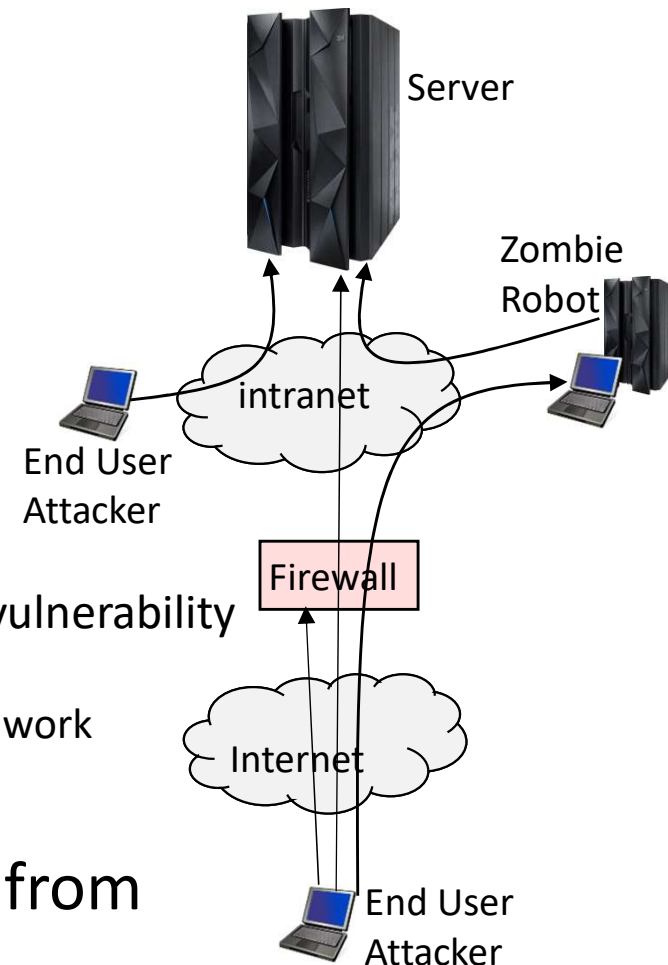
	IPsec	AT-TLS
Traffic protected with authentication and encryption	All protocols	TCP
End-to-end protection	Yes (transport mode)	Yes
Segment protection	Yes (tunnel mode)	No
Scope of protection	Security Association: 1. All traffic 2. Protocol 3. Single Connection	Single session
IPsec initiated	IPsec Policy: 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 negotiation. Dynamic VPN session key refreshed when timer expires. Manual VPN session key is not refreshed.	Session key generated in TLS negotiation. Session key refreshed when timer expires.

Intrusion Detection Services (IDS)



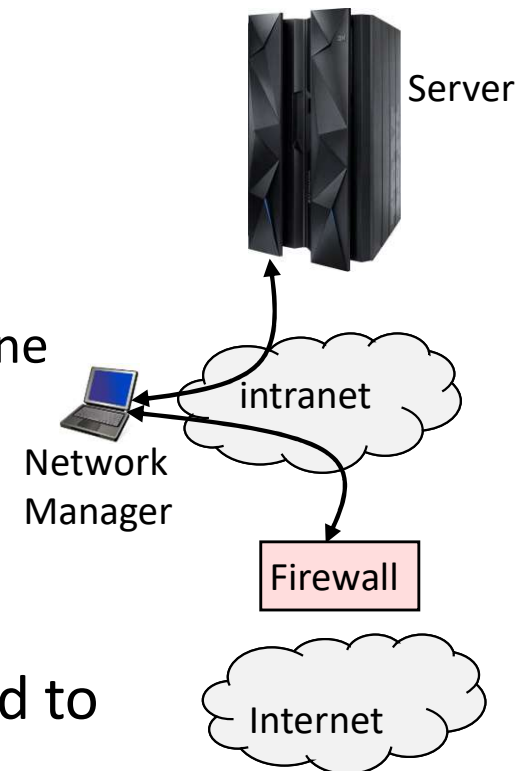
Intrusion Threat

- 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 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

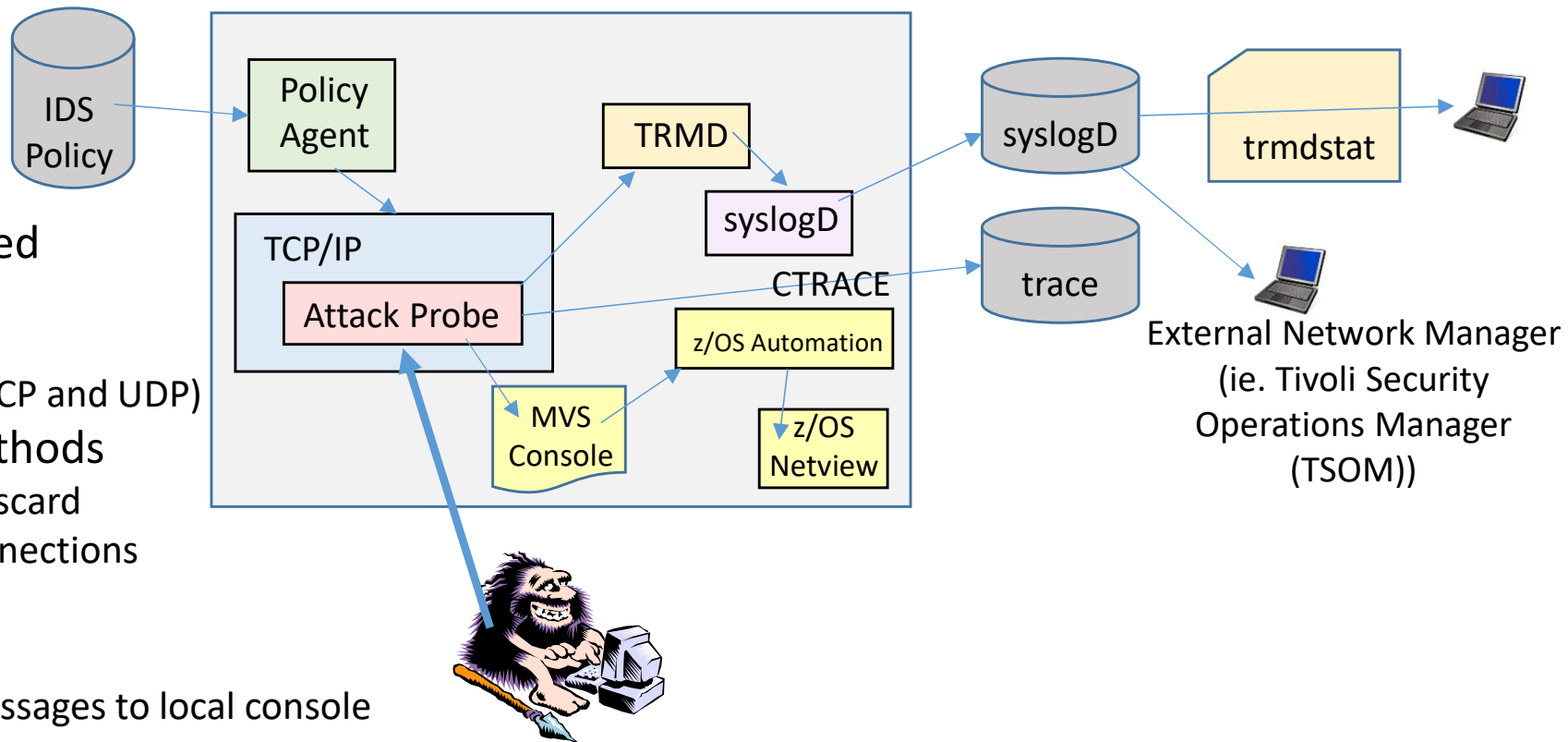


z/OS IDS versus External Firewall

- Not all problems perceived as Attacks are deliberate attacks by Hackers.
 - Deliberate: malicious intent from outside or internal bots
 - Unintentional: various forms of errors on network nodes
 - 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 concurrently.
 - ie. Tivoli Security Operations Manager



z/OS IDS Capabilities



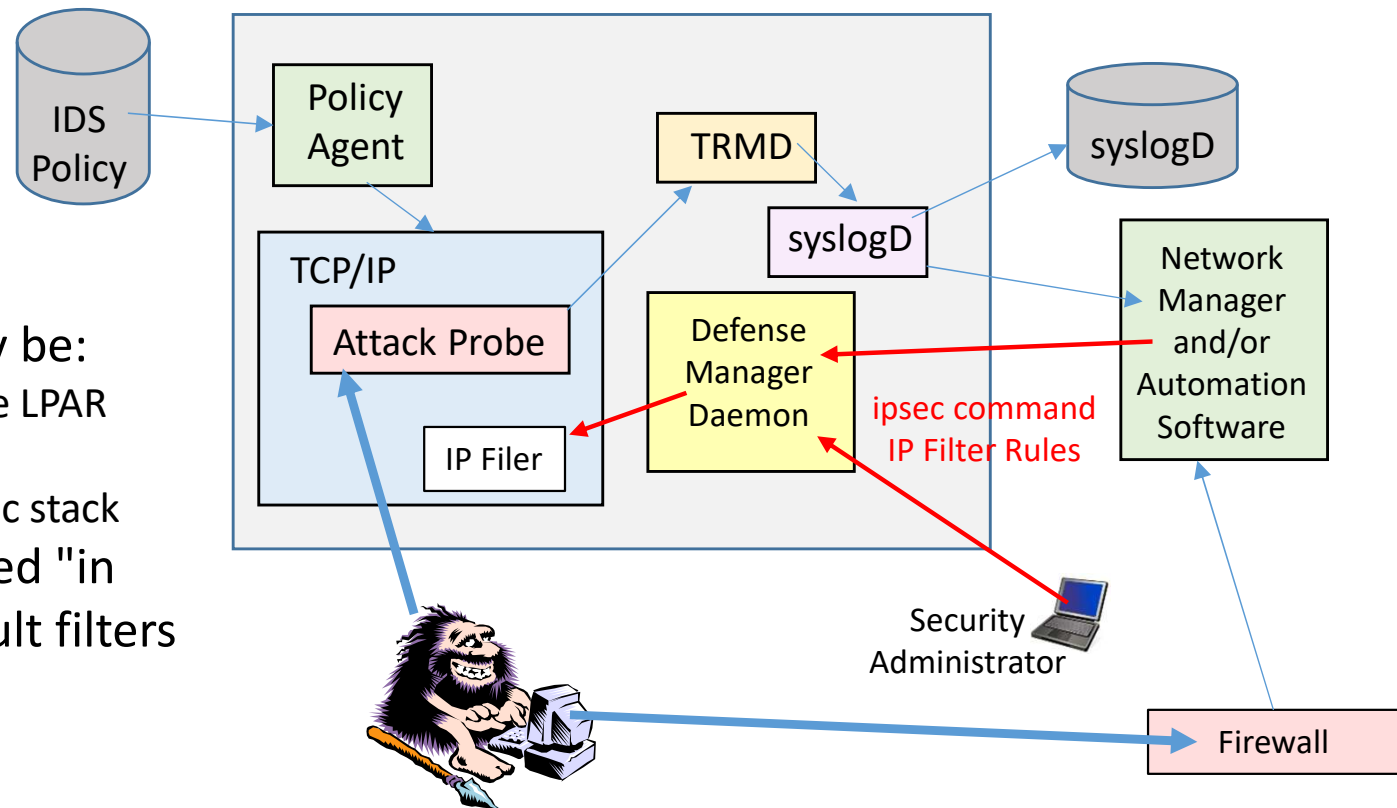
- Events detected
 - Scans
 - Attacks
 - Floods (TCP and UDP)
- Defensive methods
 - Packet discard
 - Limit connections
- Reporting
 - Logging
 - Event messages to local console
 - IDS packet trace
 - Notifications to Network Managers (ie. Tivoli NetView and Tivoli Security Operations Manager)
- z/OS 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 thresholds 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
 - Data Hiding
 - IPv6 Outbound Raw
 - IPv6 Destination Options
 - IPv6 Hop-by-Hop Options
 - IPv6 Next Header
 - TCP Queue Size
 - Global TCP Stall
 - Flood Attack (physical interface flood detection and synflood)
 - Perpetual Echo
 - IPv4 Protocols
 - IPv4 Options
 - ICMP Redirect
 - Malformed Packet
 - IPv4 Outbound Raw
 - IP Fragment
 - EE Malformed Packet
 - EE LDLC Check
 - EE Port Check
 - EE XID Flood
- 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

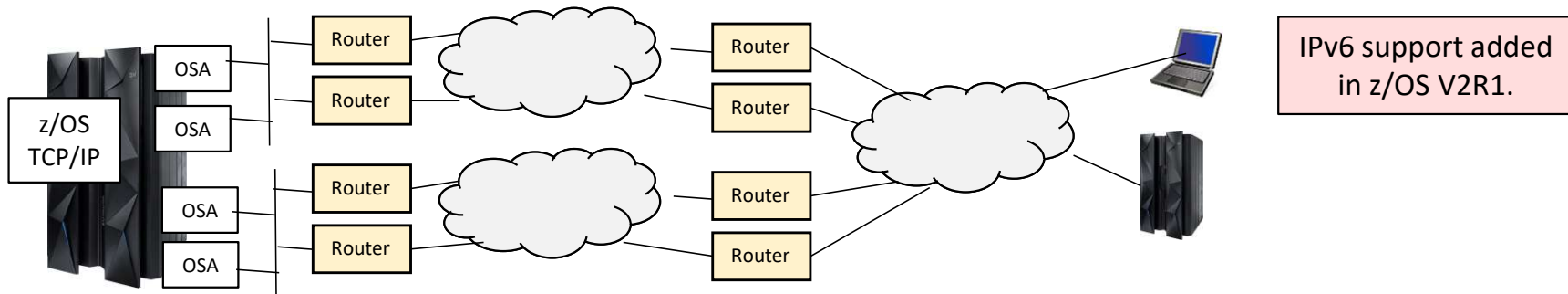
- Allows authorized users to dynamically install time-limited, defensive filters via ipsec command:
 - Security Administrator on z/OS
 - Automation
- Defensive filtering is an extension to IDS capabilities
- Requires minimal IPsec configuration to enable IP packet filtering
- Uses ipsec command to control 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

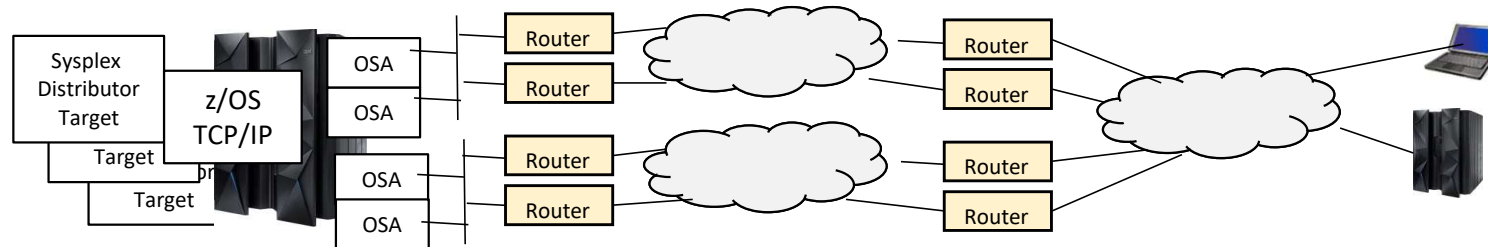


- z/OS IP Routing only effects Outbound Traffic – Data being sent FROM z/OS
 - First hop routers' routing tables determine Inbound Traffic – Data received by z/OS
 - Which of the OSAs is sent the traffic when there are multiple OSAs in the same subnet, etc.
- Whole Routing Table may include static routes 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.

Quality of Service (QoS)



Quality of Service (QoS)



- Quality of Service (Qos) includes:
 - Differentiated Services
 - TCP connection limits
 - Maximum and minimum TCP connection rates, TCP maximum delay
 - Token Bucket Traffic Shaping
 - Committed access bandwidth (mean rate and peak rate) control/enforcement
 - IPv4 type of service (ToS) byte or IPv6 traffic class setting
 - Sysplex Distributor target distribution
 - Integrated Services
 - Provided using the Resource Reservation (RSVP) protocol.

Inbound Blocking and Inbound Workload Queuing

```
• LCS (non-QDIO OSA OSE mode) and MPCIPA (QDIO OSA OSD mode) LINK

>>---LINK---link_name---+---ETHERNet-----+---link_num---device_name--->
                        +---802.3-----+
                        +---ETHEROR802.3---+
                        +---IPAQENET-----+

+---INBPERF---BALANCED-----+
>---+-----+-----> . . . . .
+---INBPERF---+---DYNAMIC-----+
+---MINCPU-----+
+---MINLATENCY---
```

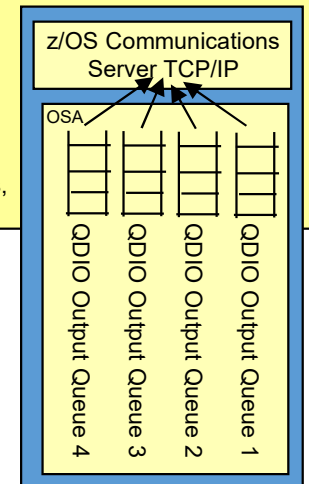
Inbound Workload Queuing (IWQ) INBPERF DYNAMIC WORKLOADQ

IWQ automatically provides unique input queues for:

- Sysplex Distributor traffic
- Bulk data (streaming) traffic
- Enterprise Extender (EE) traffic
- Default (Interactive)

Requires z196+ and z/OS V1.13+

Prevents inbound and outbound out of order packets, and the overhead that goes with it.



```
+---INBPERF---BALANCED-----+
+---INBPERF---DYNAMIC---WORKLOADQ-----+
>>---INTERFace---intf_name---DEFINE---+---IPAQENET-----+-----> . . . . .
                        +---IPAQENET6---+ +---INBPERF---DYNAMIC---NOWORKLOADQ---+
+---INBPERF---MINCPU-----+
+---INBPERF---MINLATENCY-----+
```

• INBPERF

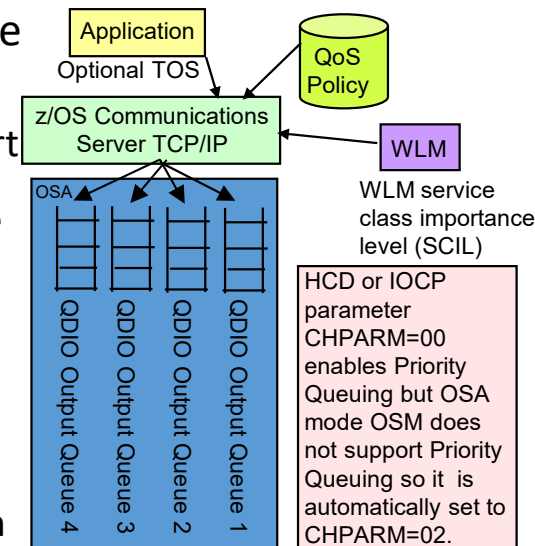
- Indicates how frequently the adapter should interrupt the host for inbound traffic.
- 3 Static Settings
 - MINCPU minimizes host interrupts without regard to throughput.
 - MINLATENCY minimizes delay, by more quickly passing packets to the host.
 - BALANCED achieves high throughput and low CPU consumption.
- 1 Dynamic Setting (z/OS V1.9+, PTFed back to V1.8)
 - DYNAMIC reacts to changes in inbound traffic patterns and sets interrupt-timing values to where throughput is maximized.
 - **DYNAMIC should outperform the other settings for most workload combinations.**
 - See 2098DEVICE Preventive Service Planning (PSP) buckets for hardware support.
 - DYNAMIC WORKLOADQ provides different queues for inbound traffic.
- INBPERF must match between LINK and INTERFACE for the same OSA.

Dynamic LAN Idle Support

LINK . . . INBPERF DYNAMIC
or INTERFACE . . . INBPERF DYNAMIC NOWORKLOADQ

Outbound Priority Routing Queues

- The Type of Service (ToS) byte in the IP header may be used by routers in the IP network to prioritize traffic (forward some types of traffic before others).
 - The most benefit is realized when the routers are all configured for this support
- TCP/IP uses the first three bits of the ToS byte in the IP header to determine the outbound priority value for a given datagram.
 - Optionally an application can specify the TOS for its traffic.
- z/OS CS TCP/IP supports four priority values in the range 1–4 for outbound QDIO traffic (with 1 being the highest priority).
 - TCP/IP will send packets using these four queues whether or not any routers in the network are configured to use the ToS settings.
- z/OS CS TCP/IP Policy Agent Quality of Service (QoS) may be used to override the default mapping of ToS values to priorities.
 - This may be used for devices without VLANs.
 - SetSubnetPrioTosMask statement
 - This may be used for devices with VLANs.
 - PriorityTosMapping parameter on the SetSubnetPrioTosMask statement may define VLAN priority-tagging.
- Enterprise Extender (EE) (SNA encapsulation over IP) automatically configures IP ToS.



Default mapping of ToS values to priorities:

ToS	Priority
000	4
001	4
010	3
011	2
100	1
101	1
110	1
111	1

WLM Service Class

```

+-----+
|
>>---GLOBALCONFig---V---+-----+-----><
|      +---NOWLMPRIORITYQ-----+      |
|      +-----+-----+-----+      |
|      |      +---default_control_values---+      |
|      +---WLMRIORITYQ---+-----+      |
|      +---IOPRIn control_values-----+      |
|      :      :      :      :      :      :
|      :      :      :      :      :      :

```

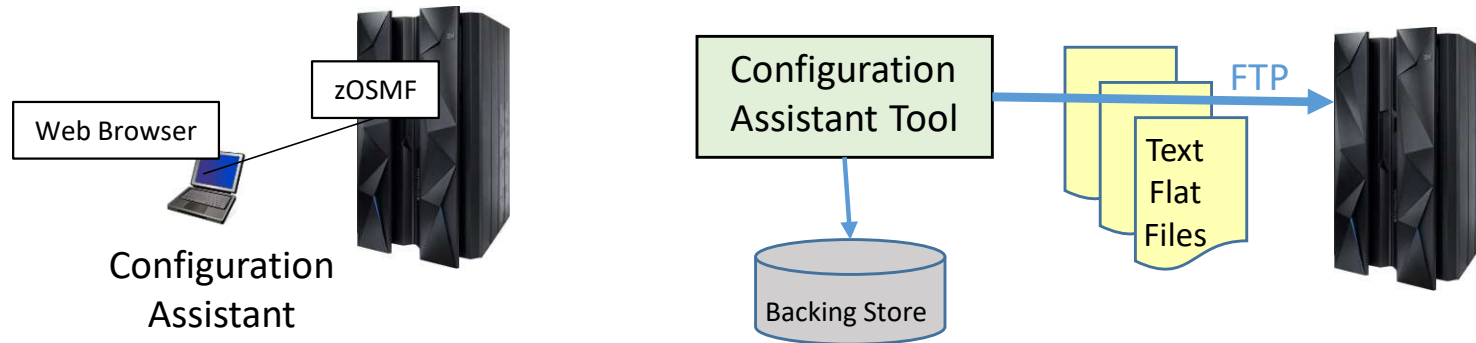
- WLM IO Priority Enhancement (z/OS V1.11+)
 - When the GLOBALCONFIG WLMRIORITYQ parameter is specified and a packet with a ToS or traffic class value 0 is sent over QDIO OSA port, TCP/IP sets the QDIO write priority of the packet based on the priority value provided by the WLM service class.

WLM Service classes	TCP/IP assigned control value	Default QDIO queue mapping
SYSTEM	n/a	Always queue 1
SYSSTC	0	Queue 1
User-defined with IL 1	1	Queue 2
User-defined with IL 2	2	Queue 3
User-defined with IL 3	3	Queue 3
User-defined with IL 4	4	Queue 4
User-defined with IL 5	5	Queue 4
User-defined with discretionary goal	6	Queue 4

Network Configuration Assistant for z/OS



IBM Network Configuration Assistant for z/OS Communications Server



- Runs on zOSMF (available since z/OS V1R11)
 - Rewritten at z/OS V2R1 to support new improved Liberty WebSphere
- Network Configuration Assistant configurations are stored in binary files
 - Named “Backing Store” files (also referred to as Persistent Data Store)
 - Only Network Configuration Assistant for z/OS Communications Server can use Backing Store files!
 - 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 the Network Configuration Assistant configurations the tool is used to send text files to z/OS
 - Network Configuration Assistant may use FTP to send the text files (FTP Server is required on z/OS)
 - Network Configuration Assistant may save the text files directly on the same LPAR
 - 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.)
- Older versions of Network Configuration Assistant Backing Store files may be upgraded to a later version.
- Starting at z/OS V2R4 the Policy Agent files can no longer be imported into the Network Configuration Assistant (NCA). Of course, the configuration may be recreated in the NCA tool.

Configuration Assistant Tool

The screenshot displays the IBM z/OS Management Facility Configuration Assistant tool. The main window shows the 'Welcome to z/OS' message and the 'Network Configuration Assistant' for z/OS Communications Server. The left sidebar contains a navigation menu with options like 'Welcome', 'Notifications', 'Workflow Editor', 'Configuration', 'Links', and 'z/OSMF Settings'. The main content area shows the 'Welcome to V2R3 Configuration Assistant for z/OS Communications Server' and a 'Select a TCP/IP technology to configure' dropdown menu. The dropdown menu is open, showing options: AT-TLS, DMD, IDS, IPsec (selected), NSS, PBR, QoS, and TCP/IP Profile. Below the dropdown, there is a table with columns: System Group or Sysplex / System ID, Type, Status, Install Status, and Release. The table shows one row with 'Default' in the System Group column, 'System Group' in the Type column, and 'Complete' in the Status column. The bottom of the window has 'Home' and 'Save' buttons.

IBM z/OS Management Facility

Learn More NEED HELP?

Welcome to z/OS

The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe

IBM z/OS Management Facility

Welcome user72

Configuration Assistant (Home) > IPsec

V2R3 Current Backing Store is Team72

Select a TCP/IP technology to configure:

- AT-TLS
- DMD
- IDS
- IPsec**
- NSS
- PBR
- QoS
- TCP/IP Profile

System Group or Sysplex / System ID	Type	Status	Install Status	Release
Default	System Group	Complete		

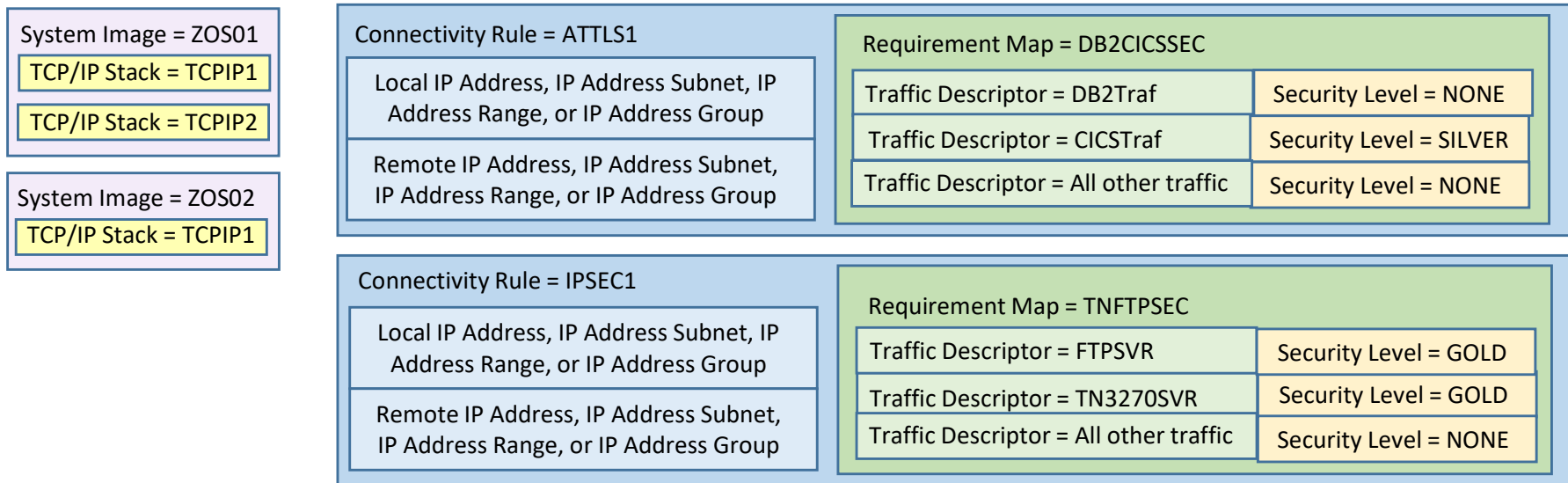
Total: 1 Selected; 0

Home Save

Configuration Assistant Tool Usage

- As you can see on the previous foil, the Network Configuration Assistant (CA) tool may be used to configure:
 - z/OS Cloud – not covered in this class (see CA tutorial for more info)
 - IPSec
 - AT-TLS
 - IDS
 - DMD
 - PBR - not covered in this class other than in this presentation
 - QoS - not covered in this class other than in this presentation
 - NSS
 - TCP/IP Profile – not covered in this class (may be used to customize a profile file for a TCP/IP stack)

AT-TLS and IPsec

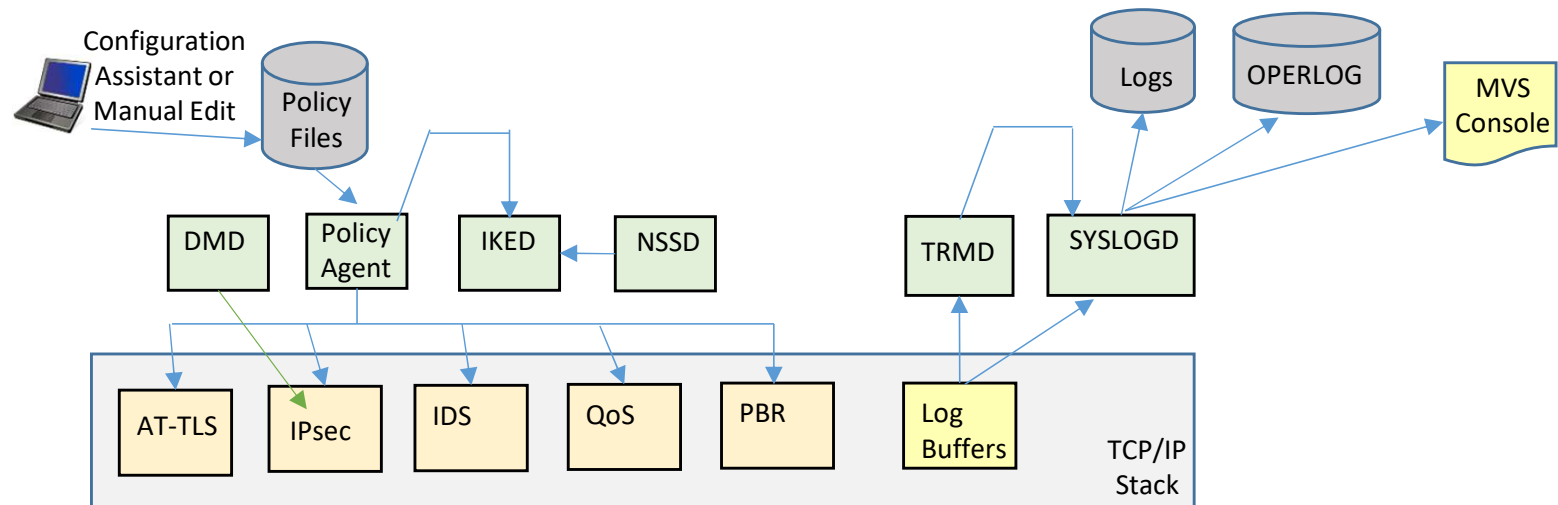


- 1 Define Sysplex Group or use the “Default” group
- 2 Define system images (z/OS systems) and TCP/IP stacks
- 3 Select Type of Policy (AT-TLS or IPsec)
 - Define connectivity rules
 - Complete security policy for all traffic between two endpoints
- 6 Specify IP Addresses for data endpoints (IP Address Groups Reusable)
- 7 Define Requirements maps (reusable)
 - Maps a set of Traffic Descriptors to Security Levels
- 4 Define Traffic Descriptors (reusable)
- 5 Define Security Levels (reusable)

Policy-based Network Security Components



Lots of Different Policy Types and Started Tasks

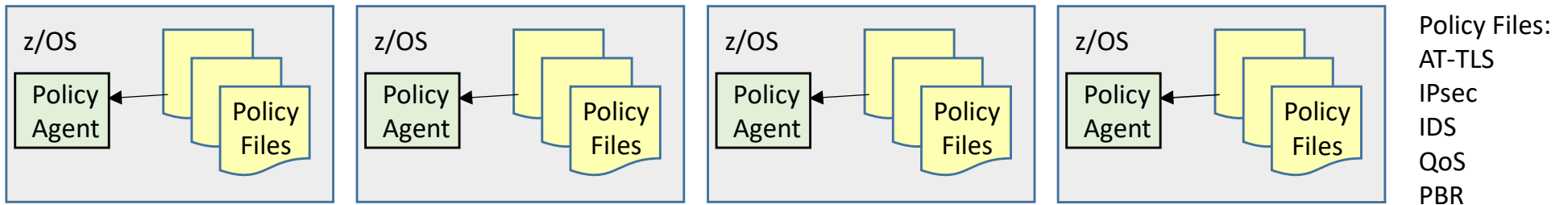


- **Policy Agent**
 - Installs Policies into the TCP/IP stack
- **TCP/IP Stack**
 - Enforces the Policies
- **DMD (Defense Manager Daemon)**
 - ipsec command can be used to install temporary IP Filter rules.
- **IKED (Internet Key Exchange Daemon)**
 - Required for IPsec Dynamic VPN (Virtual Private 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 IP Filter, IPsec, and IDS
- **SyslogD**
 - Recommended for logging

Policy Server

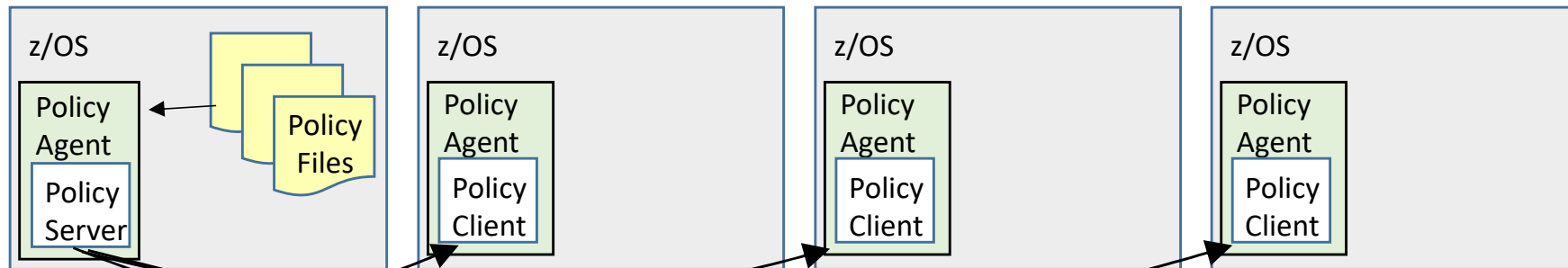


No Central Location for Policies



- 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



- 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).

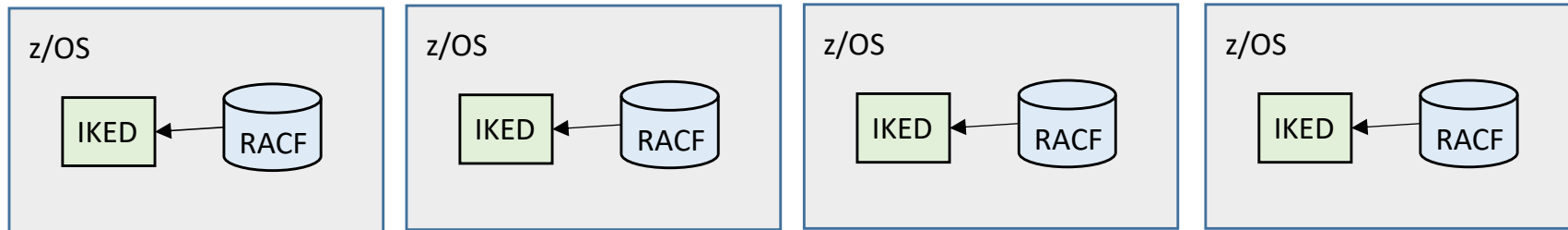
Policy Files:
AT-TLS
IPsec
IDS
QoS
PBR

Network Security Services for IPsec

NSSD is required for IKEv2

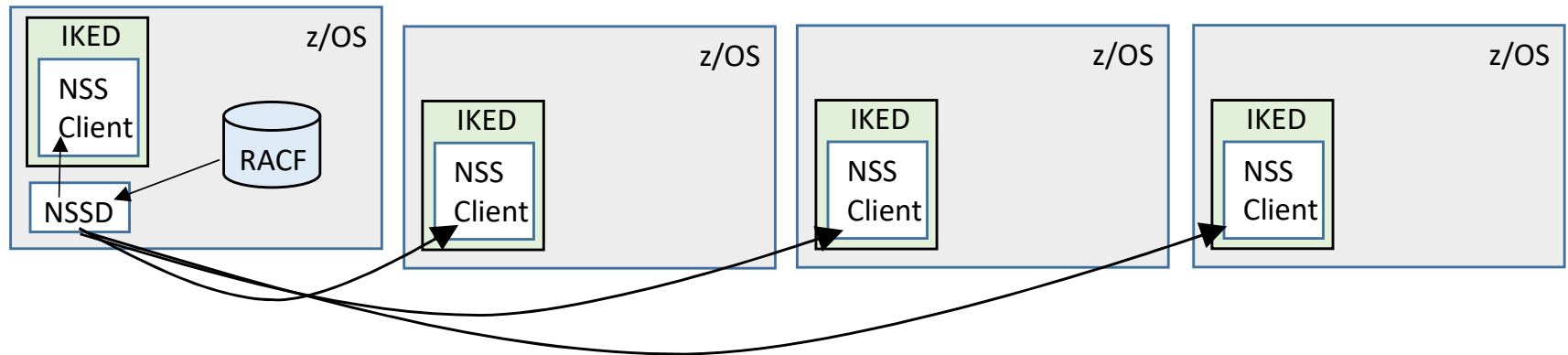


No Central Location for Certificates and Keyrings



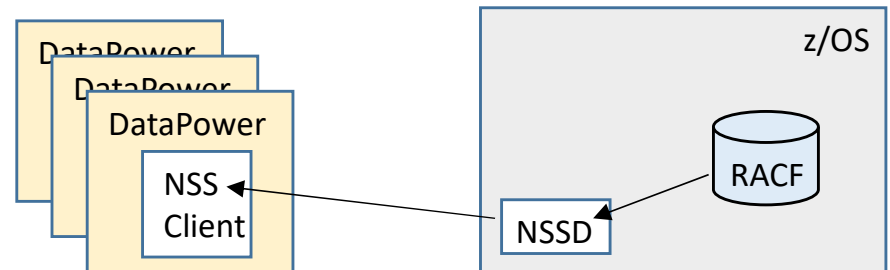
- Each z/OS system IKED may have their own certificate and keyring repository locally.
- Certificate and Keyring Administration may be from a single location
 - Configuration and monitoring can be done from a single location (administrator computer).

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
 - <https://www.ibm.com/products/datapower-gateway>
- 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

z/OS Communications Server Usage of Cryptographic Hardware

Performance numbers for Crypto Hardware:

<https://www.ibm.com/downloads/cas/6K2653EJ>

Performance numbers for z/OS Communications Server with SSL/TLS/AT-TLS

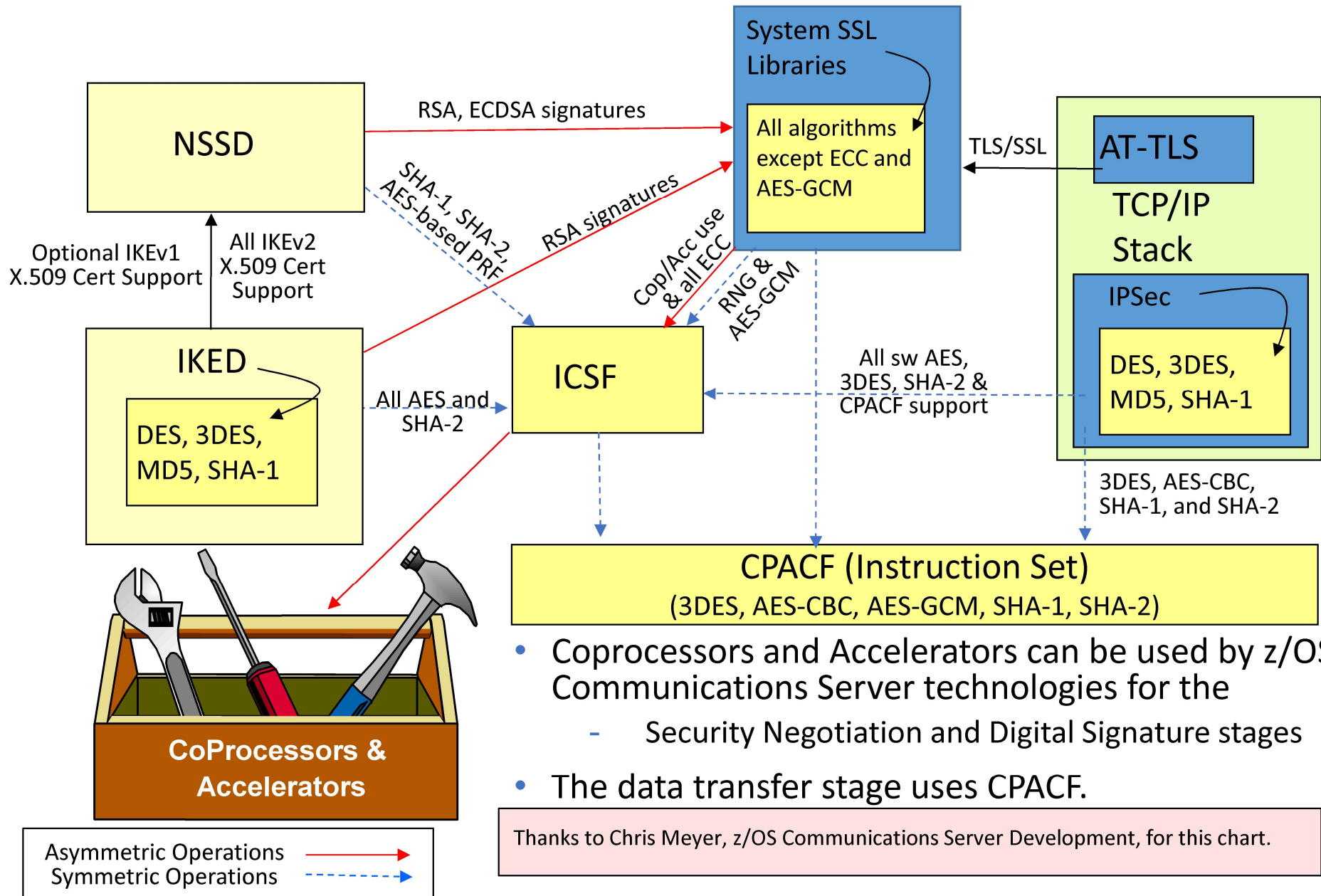
<http://www.ibm.com/support/docview.wss?rs=852&context=SSSN3L&uid=swg27005524>

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



- 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.

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

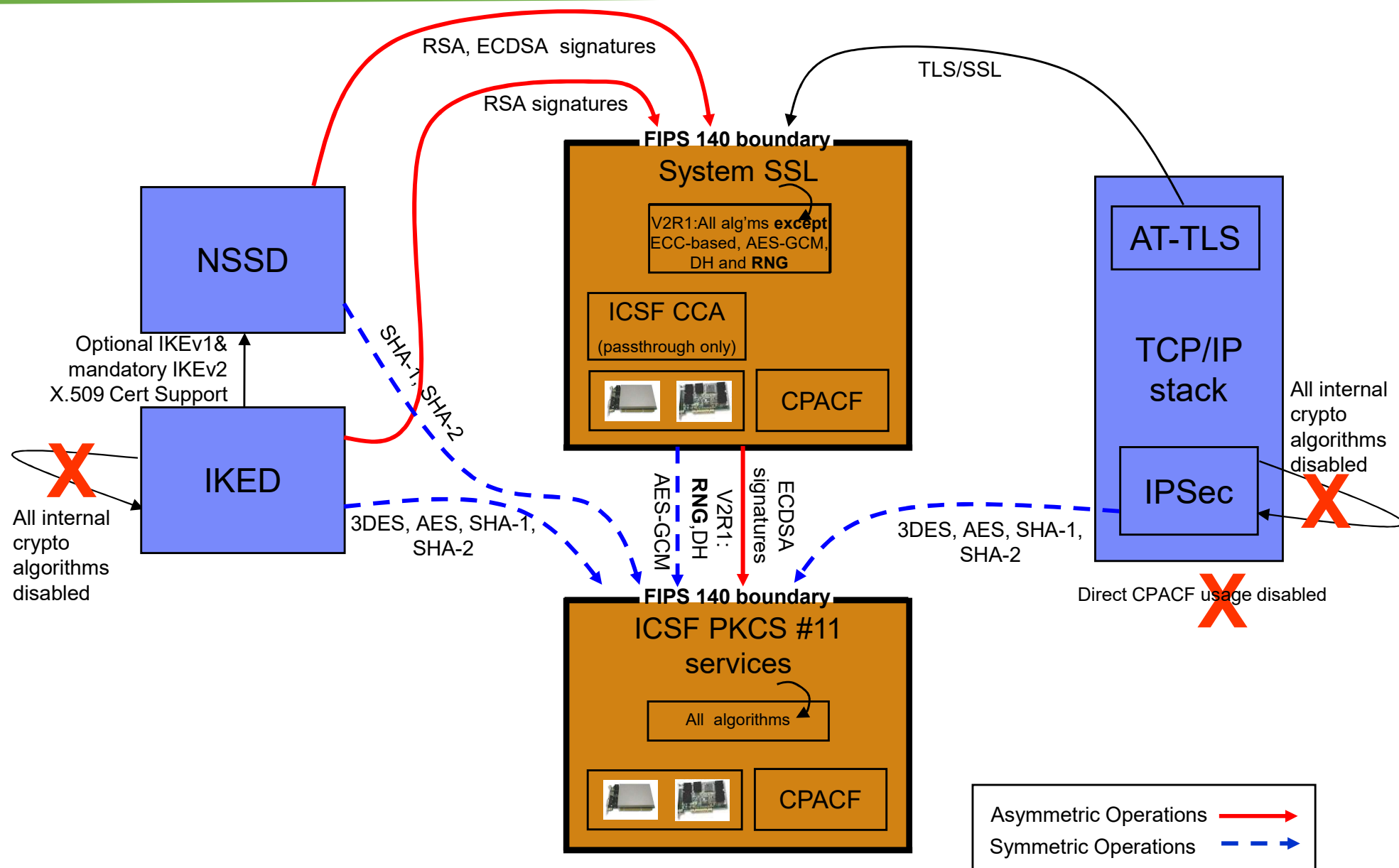
What is FIPS 140?

- 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?

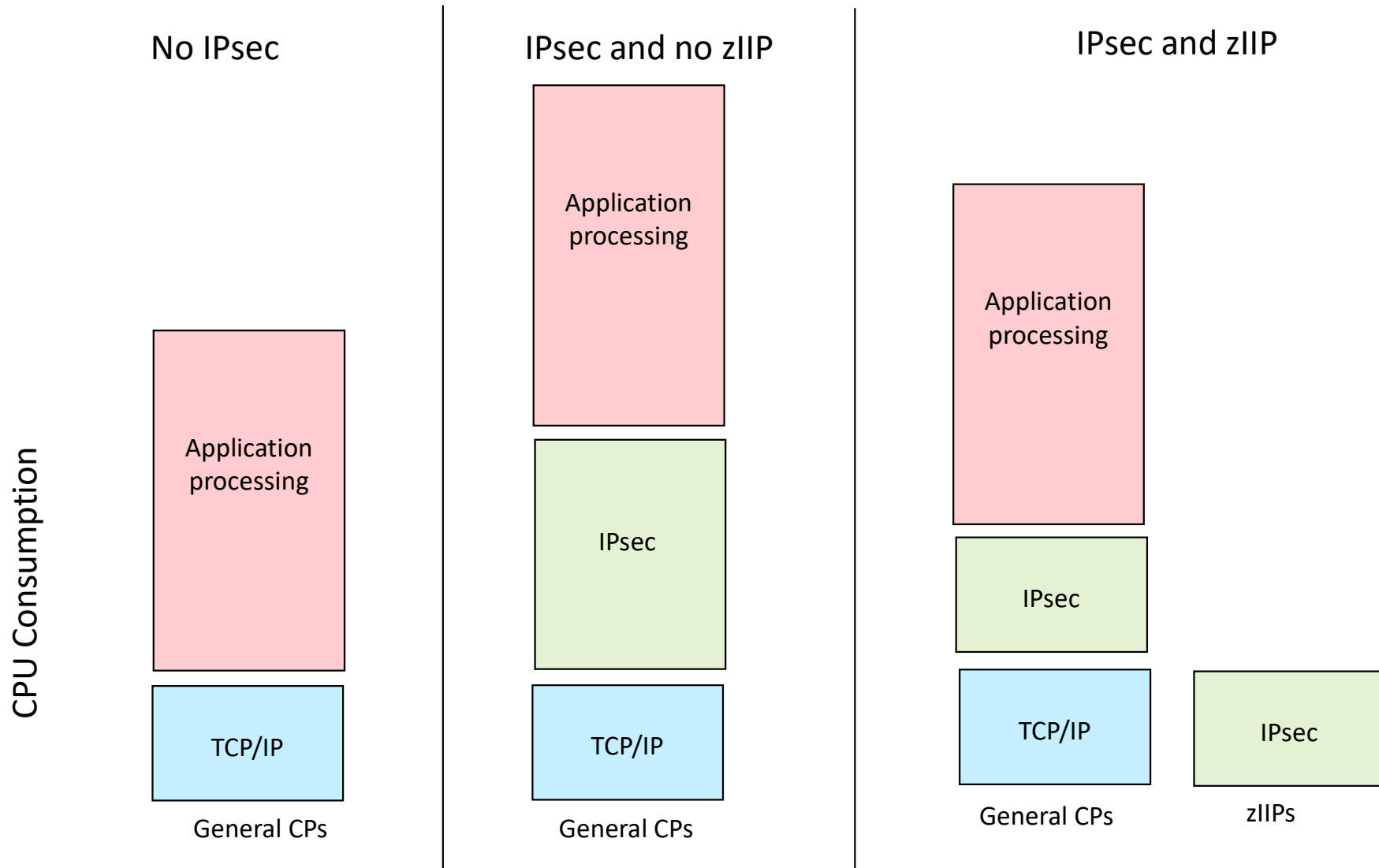
- Security Level 1:
 - Minimum level with one approved security function
- Security Level 2:
 - Adds tamper-evident detection for the security module
- Security Level 3:
 - Adds tamper-detection and tamper-protection/response to the security module
- Security Level 4:
 - Adds zeroing out of the security 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



Tradeoff: Satisfying FIPS 140 requirements versus performance!

CPU Consumption for IPsec with zIIP Processor



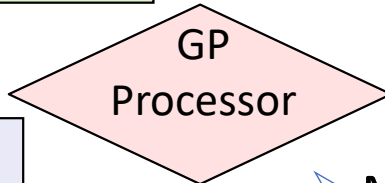
- CPACF is exploited in the same manner on both the general CPs and zIIPs.
- Function enabled through a TCP/IP configuration keyword when zIIP hardware enabled.

- Two Stages

Cryptographic Cards
(Accelerator or Coprocessor)

CPACF

Software



- 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

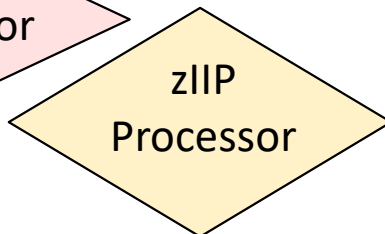
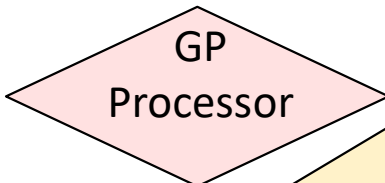
- Dynamic or Manual Tunnels

- Encrypts/Decrypts data

- Uses CPACF (clear key only) if available

CPACF

Software



- Two Stages

- 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)

Cryptographic
Cards
(Accelerator or
Coprocessor)

CPACF

Software

GP
Processor

- Phase 2

- Record Layer

- Encrypts/Decrypts data

- Uses CPACF (clear key only) if available

CPACF

Software

GP
Processor

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:
 - IBM z15 Performance of Cryptographic Operations
 - <https://www.ibm.com/downloads/cas/6K2653EJ>
 - 3.5.2 System SSL with z/OS V2R4 and Cryptographic Support for z/OS V2R1-V2R4 (ICSF FMID HCR77D1)
 - z15 Model 8561-770 (4 Central Processors)

Caching SID	Handshake	Client Auth	ETR	CPU Util %	Crypto Util %
100%	Avoided	no	38098	99.01	N/A
no	Software	no	255	100.00	N/A
no	1 CEX7C	no	10847	44.40	99.0
no	1 CEX7A	no	13456	55.32	98.6
no	2 CEX7A	yes	14471	91.50	100

- The first row of the table shows the transaction rate when the client SSL/TLS session identifier was cached in the server resulting in most of the SSL/TLS handshake processing being avoided.
- The next four rows show the transaction rates when the client SSL/TLS session identifier was not cached in the server resulting in a full SSL/TLS handshake for each client connection.
- Using the CEX7C cryptographic hardware compared to using System SSL software (second and third rows in the above table) produced an increase in throughput (number of SSL/TLS handshakes per second) of 42.5 times and reduced the CP utilization by 55%. The CEX7
- Coprocessor was 99.0% utilized. This demonstrates how off-loading the compute intensive processing associated with an SSL/TLS protocol handshake increased system capacity and reduced CP Utilization. Adding additional CEX7 Coprocessors to this environment would allow for a higher ETR as there was plenty of CPU available to handle additional workload.
- The fourth row shows that a higher ETR can be achieved by configuring the CEX7S adapter in Accelerator mode. In this measurement the utilization of the CEX7S Accelerator was 98.6%. Adding additional CEX7 Accelerators to this environment would allow for a higher ETR as there was plenty of CPU available to handle additional workload.
- If client authentication is required, the additional cryptographic operations necessary to authenticate the client reduced the throughput capacity of the server, as shown in row 5 of the table. A second CEX7 Accelerator was added to the system configuration for this measurement. The average utilization of the 2 Accelerators was 100%.

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

Pervasive Encryption



IBM Z Pervasive Encryption

- Pervasive Encryption is not a single product but more a set of z Hardware and Software Capabilities:
 - Provide Comprehensive Encryption Support
 - Provide encryption for “data at rest” and “data in flight”
 - Simplify encryption implementation
 - Improve encryption performance / Reduce encryption cost
- Only Some of the Pervasive Encryption Support is **New in V2R3**
 - Full Disk Encryption (Not New)
 - Integrated Crypto Hardware (Not New)
 - Continuously enhanced
 - **Performance enhancements in z/OS V2R3**
 - Network Encryption (Not New)
 - Continuously enhanced
 - **zERT audit capability and zERT Analyzer added in z/OS V2R3**
 - Data Set Encryption (**New in z/OS V2R3**)
 - No application changes
 - Granular access to encryption information
 - Coupling Facility (**New in z/OS V2R3**)
 - Secure Service Container (**New in z/OS V2R3**)
- For more information about Pervasive Encryption please visit
 - <https://www.ibm.com/support/z-content-solutions/pervasive-encryption/>
 - <https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSQ03116USEN>

Network Encryption

- z/OS already provided encryption for “data in flight” prior to the umbrella term “Pervasive Encryption”.
 - TLS/SSL application specific support
 - Application Transparent – TLS (AT-TLS)
 - Virtual Private Networks (VPNs) using IPsec and Internet Key Exchange (IKE)
 - Secure Shell using z/OS OpenSSL (not part of z/OS Communications Server)
- z/OS Encryption Readiness Technology (zERT) was New in z/OS V2R3
 - Generates new SMF records that include network encryption attributes for TCP and Enterprise Extender traffic
 - Supports all encryption listed above
 - Includes data about traffic that is not encrypted
 - SMF 119 record subtype 11 (also supported by SYSTCPER real-time NMI server)
 - SMF 119 record subtype 12 summary records (APAR PI83362)
 - z/OSMF zERT Analyzer may be used to view reports (requires DB2)
 - zERT Enforcement provides logging and policy-based enforcement capabilities (new in z/OS V2.5)

System z Lab Services Security Offerings

Is the client's System z environment secure enough considering their business, policy, or regulatory requirements?	System z security review and enhancement services	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?
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			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.
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?	Enterprise encryption certificate creation and management services	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?
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.			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
Has the client purchased IBM System z cryptographic hardware and expressed concerned with centralized encryption key management and exploitation?	System z encryption hardware exploitation services	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?
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			Lab Services consultants assist customers in meeting security regulatory (ie HIPAA, 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.
Is the client planning to have System z be compliant with PCI, HIPAA, FIPS 140-2, or other security regulations?	PCI and other security standard compliance for System z services	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?
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.			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.

End of Topic

