

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

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 3

z/OS Communications Server Network Security

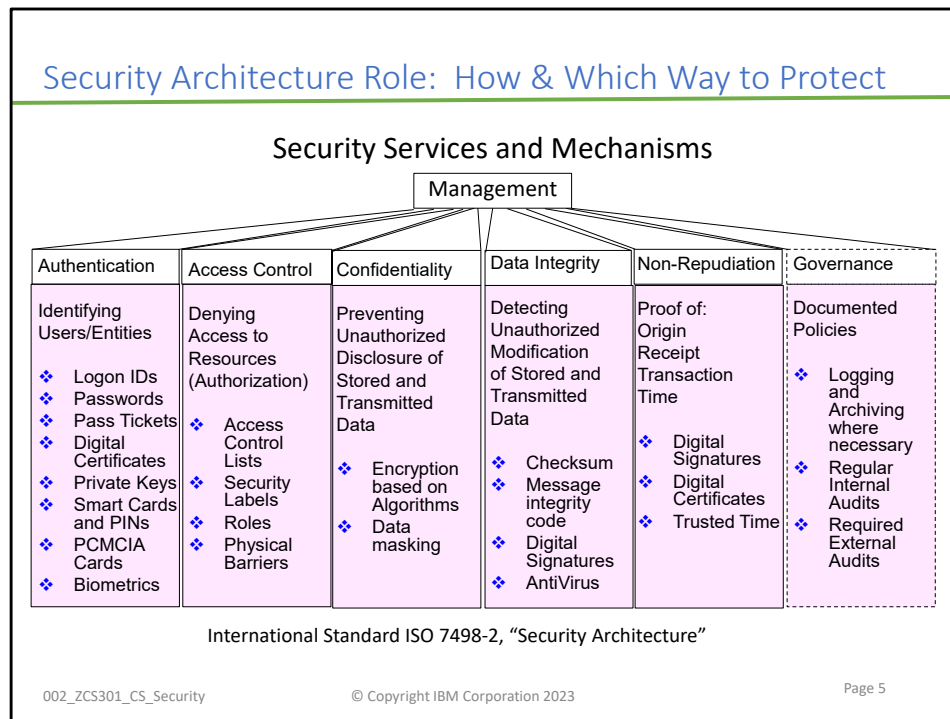


002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 4

Security Architecture Role: How & Which Way to Protect



You have seen the "Essential Questions for Planning Security":

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

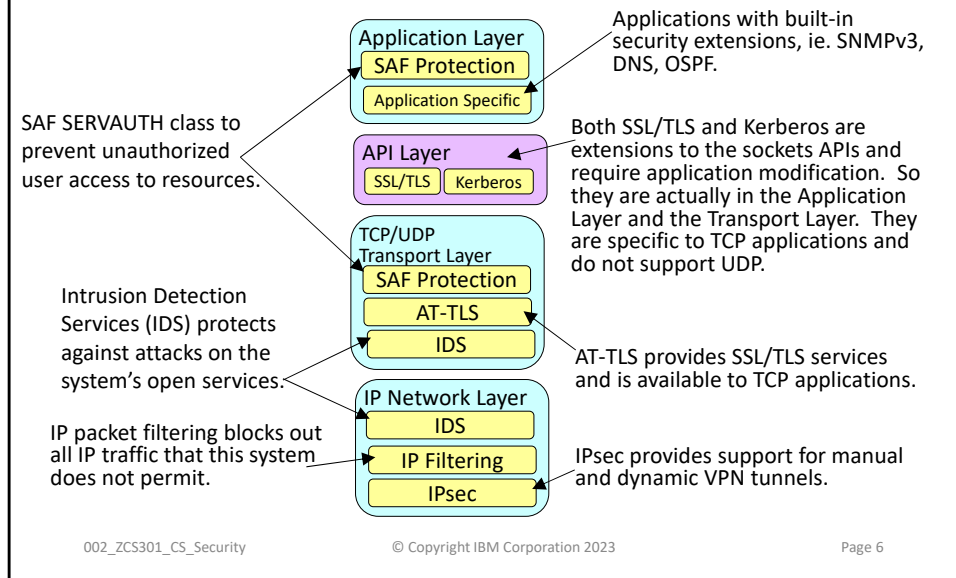
The ISO 7498-2 model -- depicted here -- addresses the second and third sub-bullets above: "How should you protect," and "Which mechanisms or technologies should you use to protect?"

This is an older version of the ISO security model. Note the entry for "Governance" and "Logging." This is not part of the ISO model, but it is nevertheless integral for any security implementation. We have added it here to show its importance.

SUMMARY: You have now seen a couple of architectures for security. What is the difference?

- The IBM Security Framework describes WHAT needs to be protected in an IP installation.
- This ISO Security architecture describes:
 - HOW to protect the data (i.e., which Services should be used to protect data and resources)
 - WHICH ways to protect the data (i.e., which security mechanisms could be used to protect the data and resources)

Protocol Stack View of TCP/IP Security Features



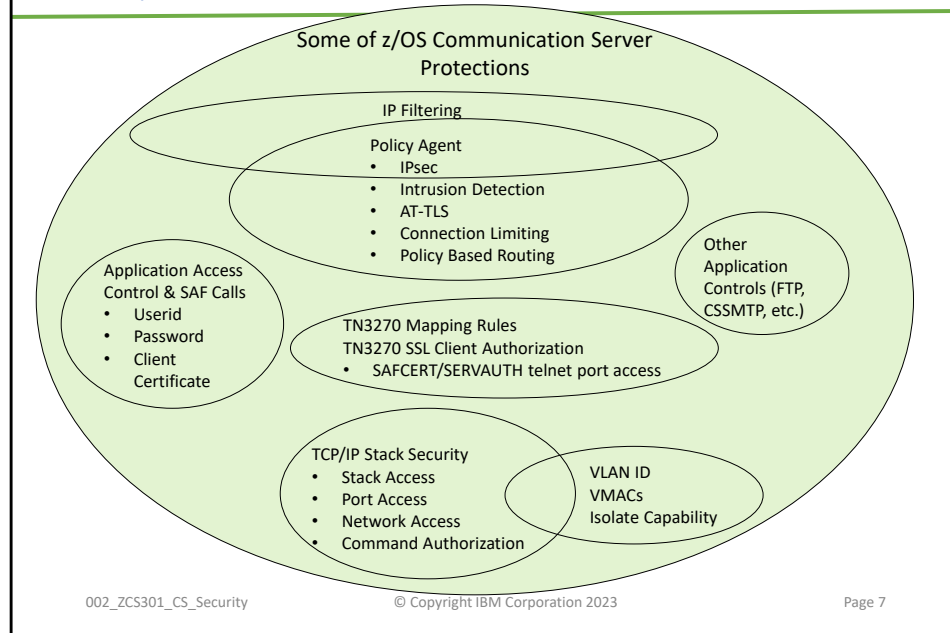
This protocol stack view of the TCP/IP architecture shows you that z/OS Communications Server addresses security at every level of the architecture.

At the Application Layer, an application itself can have built-in security mechanisms for access control and can also make API calls to security technologies like RACF, ACF2, Top Secret, etc for the purposes of access control or authentication.

At the Transport Layer, protection can be invoked with API calls to a Security Access Facility (SAF) for authorization, with calls to encryption technologies through Secured Sockets Layer (SSL), Transport layer Security (TLS), or Application-Transparent TLS (AT-TLS). These related technologies provide authentication, data integrity checking, and encryption. At this layer, layer 4, we can also implement Intrusion Detection or Prevention Services or Systems (IDS or IPS) to warn and obstruct intrusions into the networking nodes and their applications.

At the Networking Layer, layer 3, IDS or IPS can be invoked as at layer 4. In addition, we may implement a Virtual Private Network (VPN) endpoint to set up a secure tunnel between authenticated partners for authentication, data integrity checking, and encryption by means of IP Security (IPSec). IP Filtering can be used to permit or deny traffic into the stack or out of the stack. Even routing can be invoked at this layer to force traffic over secured or unsecured paths using a Policy built with the IBM z/OS Configuration Assistant. This procedure is called "Policy-based Routing."

Security Mechanisms in z/OS Communications Server



Note how Communications Server in z/OS provides many ways to secure data, the network, and the nodes and processes in the network.

At Layer 5 many applications have built-in security processes:

- Access Control Lists (ACLs)
- Requests for userid and password during login
- Requests for Client Certificates

Other applications, like TN3270, have "mapping rules" that limit who is allowed to access which IP addresses or SNA Logical Unit Names or even SNA applications reached through TN3270.

We also have types of security that can filter who is allowed to connect to a stack, to an application port, or to a specific network in the TCP/IP stack.

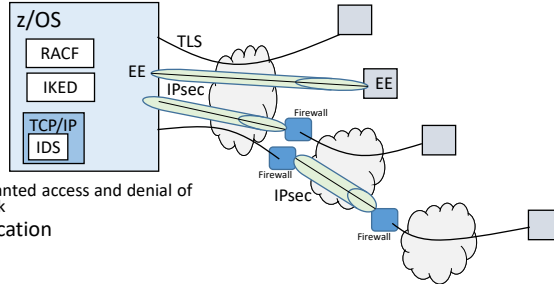
Policy Agent performs several services that are relevant to security, some of which you will hear more about in this course.

- Limiting & Blocking Connections with QoS Policies
- Intrusion Detection Services (IDS) at Layer 4 and Layer 3
 - IDS provides Host-based TCP/IP services under policy control, to identify, alert and document suspicious events and assist in later analysis. IDS should be added to existing Security Plans and Procedures, Information and Application Access Controls, Firewalls and network-based IDS. It should not be seen as the sole means of protecting the company from intruders.
 - IDS also assists with REPORTING on suspicious activity.
- IP Filtering at Layer 3
- IP Security (IPSec) at Layer 3 which provides security through authentication, data integrity services, and encryption from the IP layer on one node to the IP layer on another node.
- Application-Transparent Transport Layer Security (AT-TLS) at Layer 4 which provides security through authentication, data integrity services, and encryption from the Sockets layer (Transport Layer) on one node to the Sockets layer (Transport Layer) on another node.

CS also provides security at Layer 2 through the use of VLAN IDs, VMACs, and the OSA Connection Isolation Feature.

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



002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 8

Prior to z/OS V1R7, IP security packaged with Firewall Technologies.

In z/OS V1R7, complete IPsec, IP filtering, and IKE solution are part of z/OS Communications Server.

- Alternative to Firewall Technologies
- Intrusion Detection Services (IDS)
- IP filtering
- Manual IPsec
- Dynamic IPsec (IKE)
- Filter directed logging to syslogd

Beginning in z/OS V1R8 Firewall Technologies no longer available.

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

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 9

External Firewalls are no longer able to apply Intrusion Detection Services (IDS) to traffic because traffic is being encrypted all the way to z/OS instead of being unencrypted by the external Firewalls.

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
Cloud Configuration

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 10



Policy-based Network Security exploits many technologies.

In this class we focus on encryption and IDS:

- AT-TLS
- IP Filtering and IPsec
 - IPsec with Manual "tunnels"
 - IPsec with Dynamic "tunnels" using Internet Key Exchange Daemon (IKED)
- Intrusion Detection Services (IDS)

We mention most of the rest of the listed technologies but we refer you to the IP Configuration Guide for more information on:

Defense Manager Daemon (DMD)

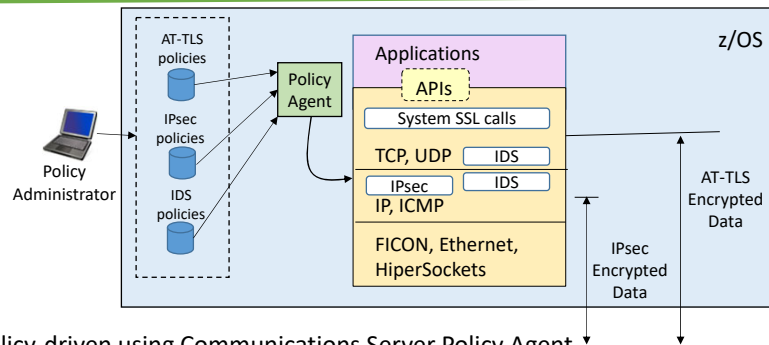
Network Security Server (NSS)

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, 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

002_ZCS301_CS_Security

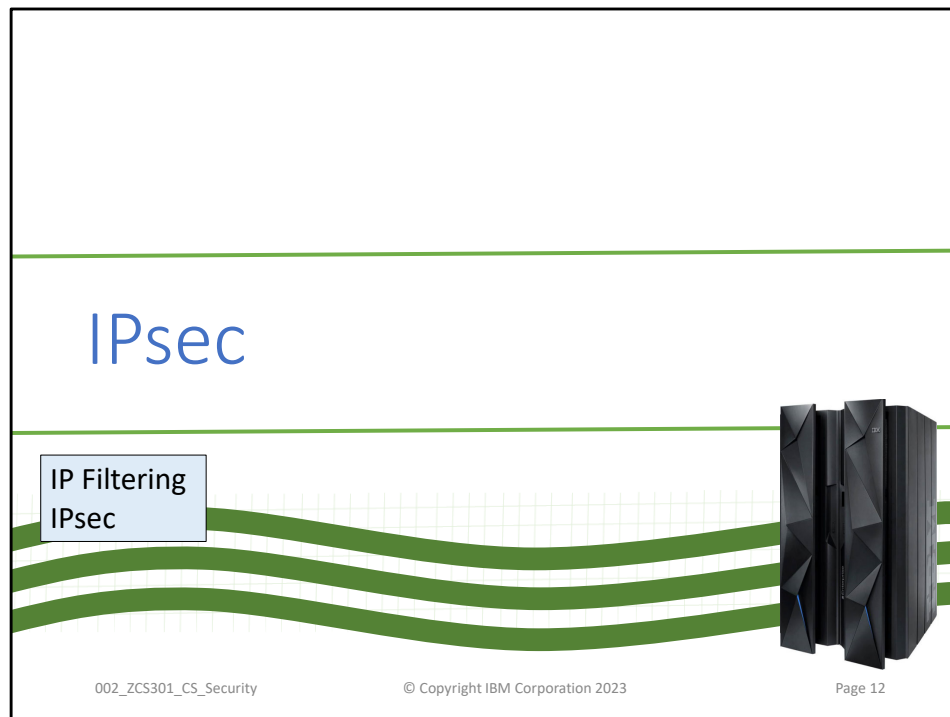
© Copyright IBM Corporation 2023

Page 11

IPsec traffic is encrypted and unencrypted at the Network Layer (Layer 3).

AT-TLS traffic (and TLS and SSL) is encrypted and unencrypted at the Transport Layer (Layer 4).

The applications are always sending and receiving unencrypted data.

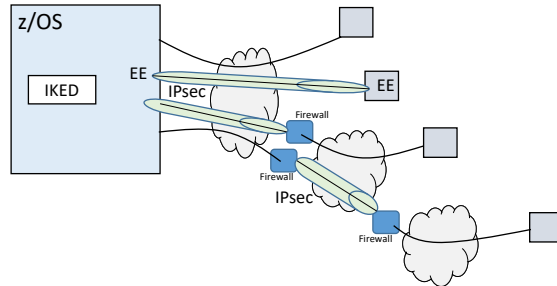


IPsec is a standard protocol. IP Filtering is not part of the IPsec protocol, however IP Filtering is part of the IPsec implementation on z/OS. IP Filtering is required to implement IPsec on z/OS.

- On z/OS it is possible to implement IP Filtering without IPsec but it is not possible to implement IPsec without IP Filtering.

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



002_ZCS301_CS_Security

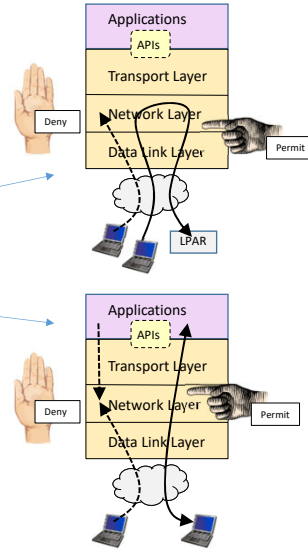
© Copyright IBM Corporation 2023

Page 13

Protects the system from the network.
IP filtering controls which packets enter the system.
IP filtering controls which packets can leave the system.
Cryptographically protects data in the network.
Manual IPSec for statically defined security associations.
Dynamic negotiation of IPSec security associations through IKE.
Filters directed logging of IP security actions to syslogd.
Administrator controls which types of log messages are written to syslogd.

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)



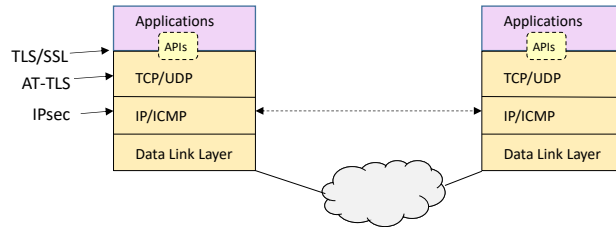
002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 14

IP Filtering may be defined for Local traffic, Routed traffic, or both.

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)

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 15

IPsec protocol supports all upper level protocols.

- TCP and UDP

A Security Association (SA) includes the security algorithms decided upon in the negotiation between both sides.

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)

002_ZCS301_CS_Security

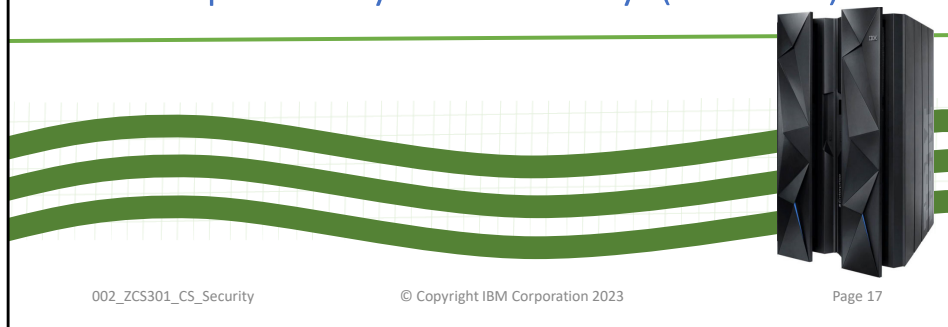
© Copyright IBM Corporation 2023

Page 16

When z/OS is the security endpoint (encryption endpoint) as well as the data endpoint, then z/OS is configured as an IPsec Host. When z/OS is the security endpoint (encryption endpoint) but the data endpoint is on some other system, then z/OS is configured as an IPsec Gateway.

Network Security Services Daemon (NSSD) is required for IKEv2 support.

Application Transparent – Transport Layer Security (AT-TLS)

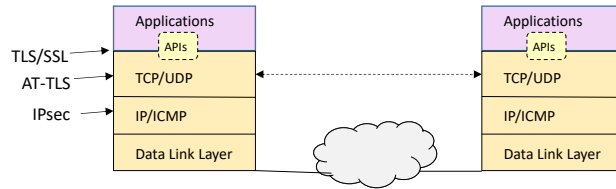


002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 17

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

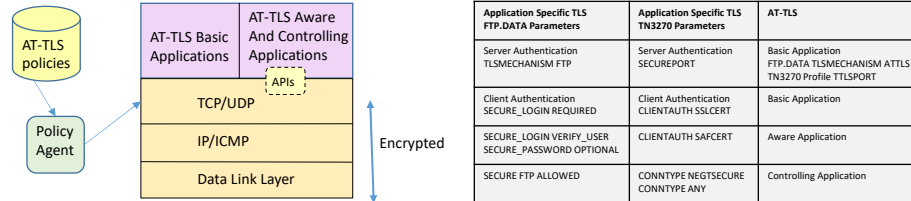
002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 18

If encryption for UDP is desired then IPsec should be used instead of AT-TLS.

Application Transparent - Transport Layer Security (AT-TLS)



- 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 SIOCTTLSCCTL 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

002_ZCS301_CS_Security

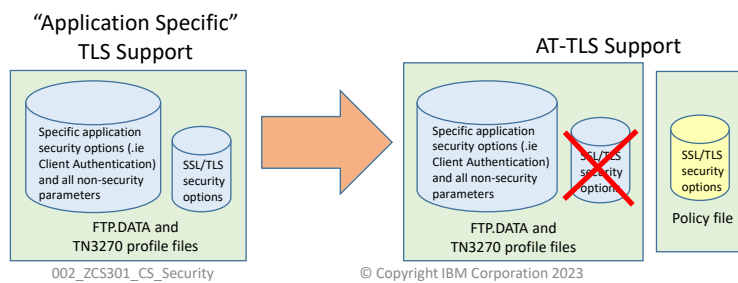
© Copyright IBM Corporation 2023

Page 19

AT-TLS is just standard TLS. It is only named AT-TLS to differentiate it from previous TLS support that already existed in FTP and TN3270 and to indicate that it can be implemented without application change for Server Only authentication or Server with “plain” Client Authentication.

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.



FTP and TN3270 should be migrated from “application specific” TLS support to AT-TLS.

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)



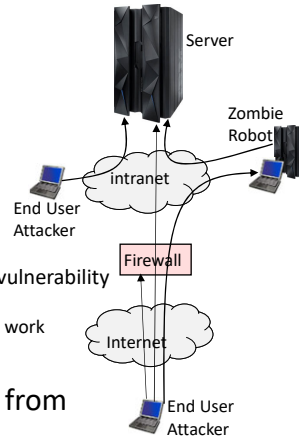
002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 22

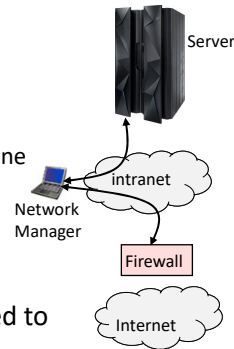
Intrusion Threat

- 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 information concurrently.
 - ie. Tivoli Security Operations Manager

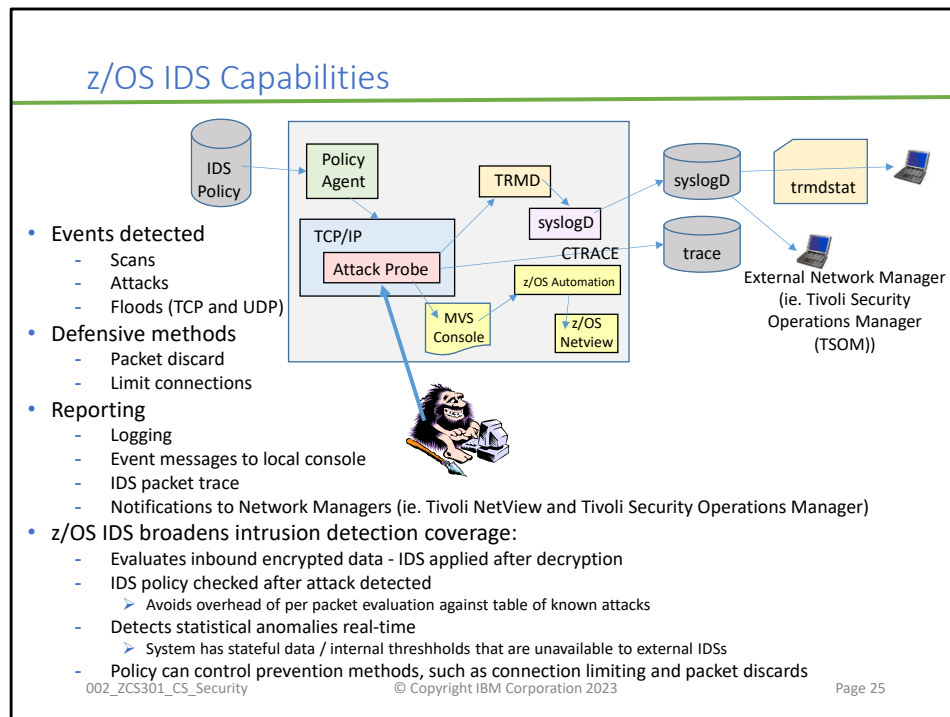


002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 24

We are not saying to get rid of external Firewalls. They are still serving their original purpose. What we are saying is that the z/OS IDS is a useful tool in addition to all external Firewalls.



Tivoli NetView z/OS V5R1, PTF UA11043

- Provides local z/OS management support for IDS

Tivoli Security Operations Manager

- Provides enterprise-wide management support for IDS

NetView provides ability to trap IDS messages from the system console or syslog and take predefined actions based on IDS event type such as:

- Route IDS messages to designated NetView consoles
- email notifications to security administrator
- Run trmdstat and attach output to email
- Issue pre-defined commands

Automated aggregation and correlation of events, logs, and vulnerabilities

- Broad device support for multi-vendor environments, including security, network, host, and applications
- Support includes processing for z/OS Communications Server syslog messages for IDS events

Automates policy and regulatory compliance

- Policy and Regulatory based policy monitoring and reporting

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, ottenetD, etc.)

002_ZCS301_CS_Security

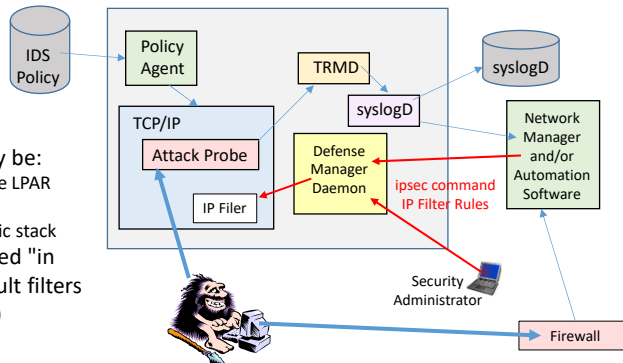
© Copyright IBM Corporation 2023

Page 26

A complete list of Attack types is listed in the IDS specific presentation.

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)

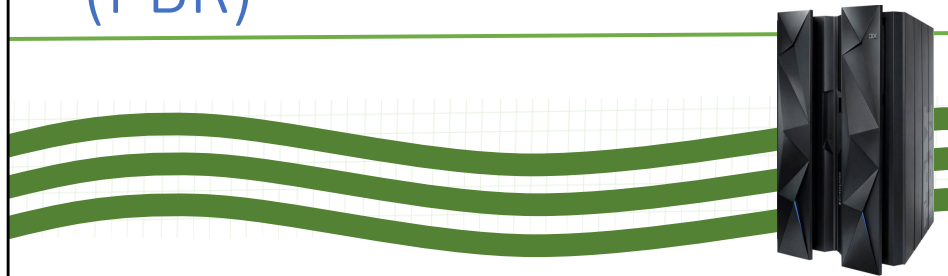


002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 27

Policy Based Routing (PBR)

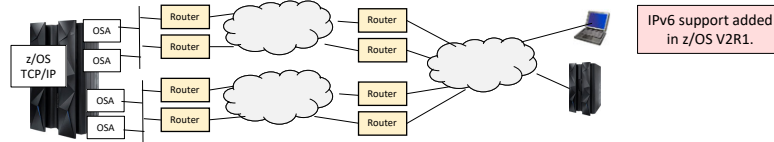


002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 28

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.

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 29

Choose first hop router, outbound network interface (including VLAN), and MTU.

Choice can be based on more than the usual destination IP address/subnet.

With PBR, the choice can be based on source/destination IP addresses, source/destination ports, TCP/UDP, etc.

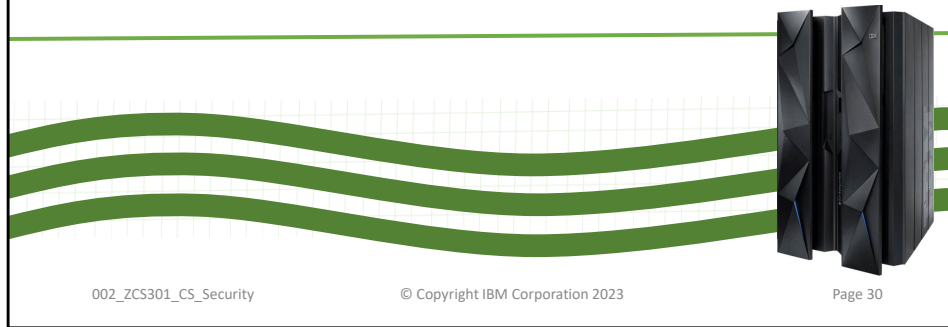
Allows an installation to separate outbound traffic for specific applications to specific network interfaces and first-hop routers:

- Security related
- Choice of network provider
- Isolation of certain applications
 - EE traffic over one interface
 - TN3270 traffic over another interface

PBR policies will identify one or more routes to use.

If none of the routes are available, options to use any available route or to discard the traffic are provided.

Quality of Service (QoS)

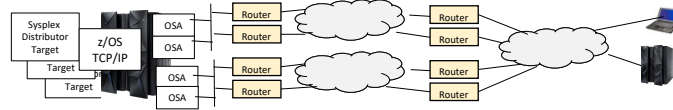


002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 30

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.

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 31

Choose first hop router, outbound network interface (including VLAN), and MTU.

Choice can be based on more than the usual destination IP address/subnet.

With PBR, the choice can be based on source/destination IP addresses, source/destination ports, TCP/UDP, etc.

Allows an installation to separate outbound traffic for specific applications to specific network interfaces and first-hop routers:

- Security related
- Choice of network provider
- Isolation of certain applications
 - EE traffic over one interface
 - TN3270 traffic over another interface

PBR policies will identify one or more routes to use.

If none of the routes are available, options to use any available route or to discard the traffic are provided.

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--->
+---S02.3-----+
+---ETHER0802.3---+
+---IPAQUENET-----+

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

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+---INDEF---BALANCED---DYNAMIC---WORKLOAD---+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
>---INTERFACE---INTF_NAME---DEFINE---IPACNET6---+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+---INDEF---DYNAMIC---NOWORKLOAD---+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+---INDEF---MINCPU---+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+---INDEF---MINLATENCY---+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

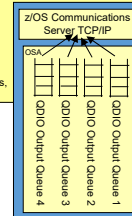
Inbound Workload Queuing (IWQ)

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

- 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 Z098DEVICE 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 Settings**

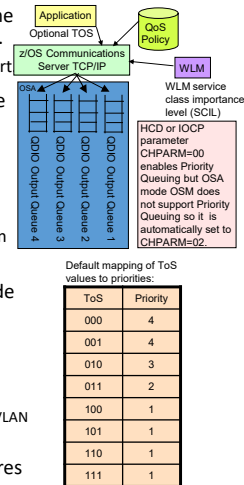
LINK ... INBPERF DYNAMIC
or INTERFACE ... INBPERF DYNAMIC

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.



Network Configuration Assistant for z/OS

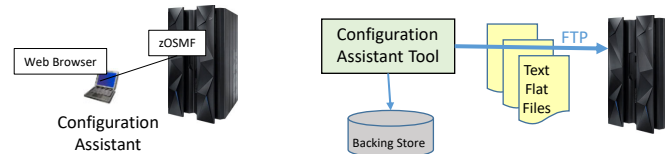


002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 35

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.

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 36

Allows policy definition to be performed at higher level of abstraction than policy file statements.

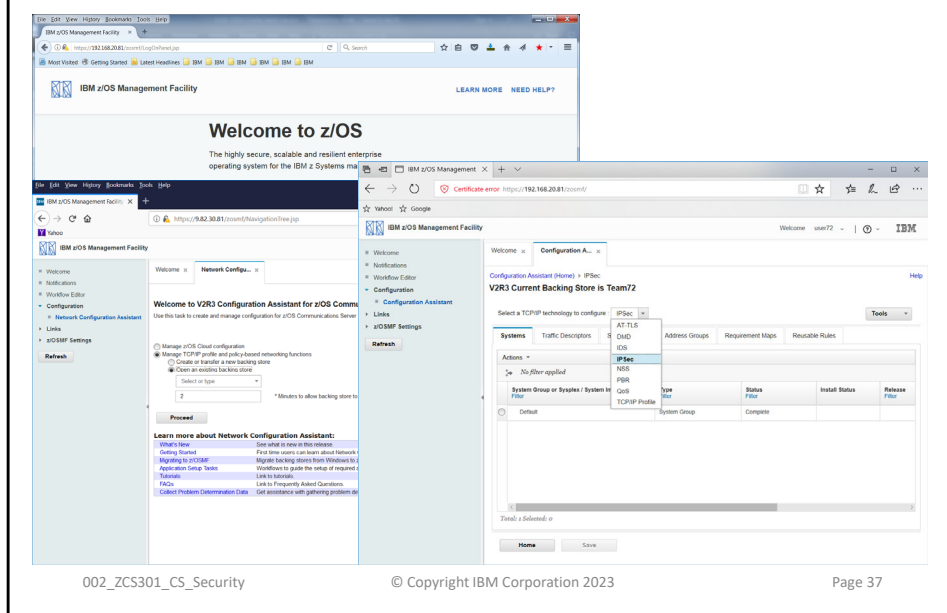
Locking support at the persistent data store to prevent inadvertent loss of data.

- When file is being edited and another person tries to open the file they will get a message that it is already in use.

If z/OS policies are imported into the Configuration Assistant, it is recommended to do the import only once, or as few times as possible.

- Internal names are created by the tool so the text files do not match the original policy files on z/OS, but the policy execution is the same.

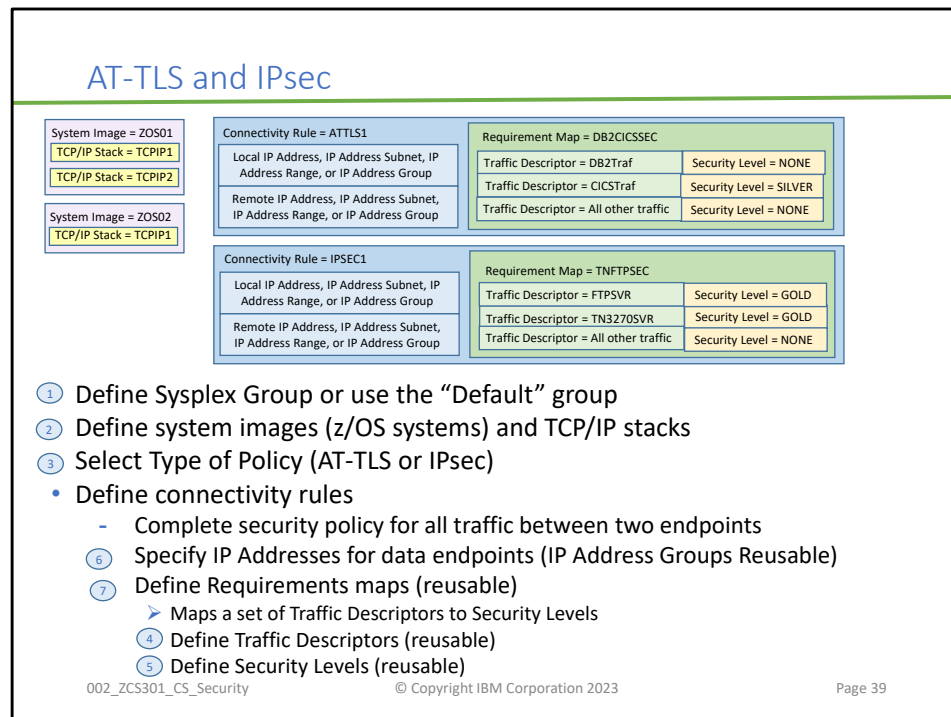
Configuration Assistant Tool



Another way to download the GUI executable is from the following web page:
<http://www.ibm.com/software/network/commserver/zos/support/>
then select "Download" from the bottom of the page and search for Configuration Assistant.

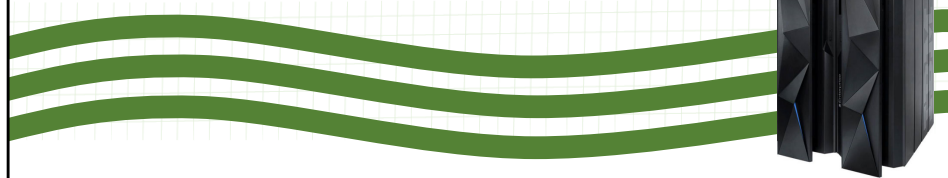
Configuration Assistant Tool Usage

- 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)



There are Wizards that start for each section with a set of panels that must be completed to create the selected item. Wizards and dialogs guide you through a top-down approach to the configuration. The order depicted on the chart above. Navigational tree supports a bottom-up approach to allow an experienced user to bypass wizard screens. Navigational tree appears on the left hand side of the Window.

Policy-based Network Security Components

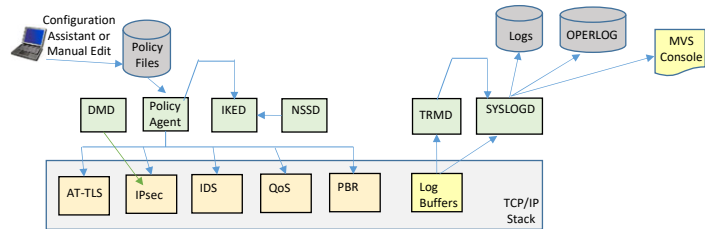


002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 40

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

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 41

Configuration Assistant can really help getting the whole environment setup.

Policy Server

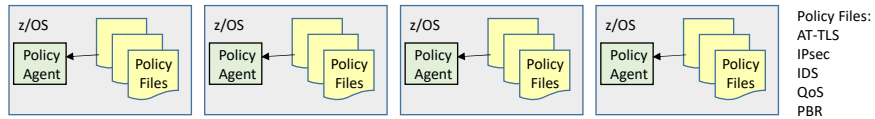


002_ZCS301_CS_Security

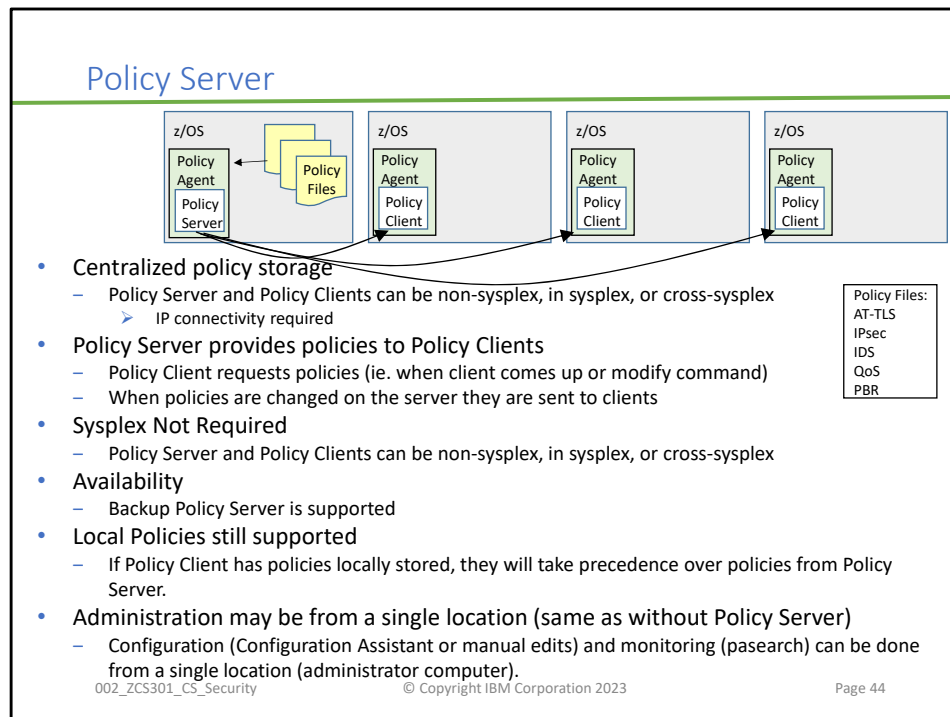
© Copyright IBM Corporation 2023

Page 42

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).



Policies for multiple z/OS systems can be stored on a single z/OS system.

Network Security Services for IPsec

NSSD is required for IKEv2



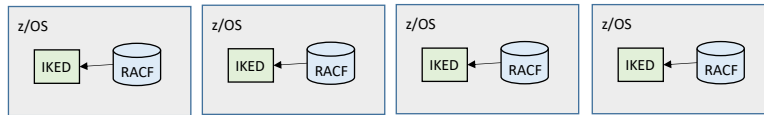
002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 45

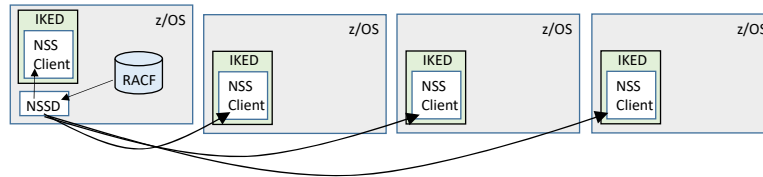
Network Security Services Daemon is required for IKEv2 support.
IKEv2 also requires z/OS V1R12 or later.

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).

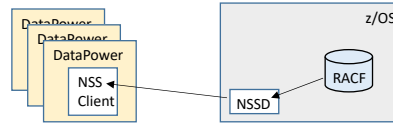
002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 47

Policies for multiple z/OS systems can be stored on a single z/OS system.

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

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 48

NSSD DataPower support has nothing to do with IPsec.

Because NSSD provides access to RACF, DataPower can now take advantage of that same RACF 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>

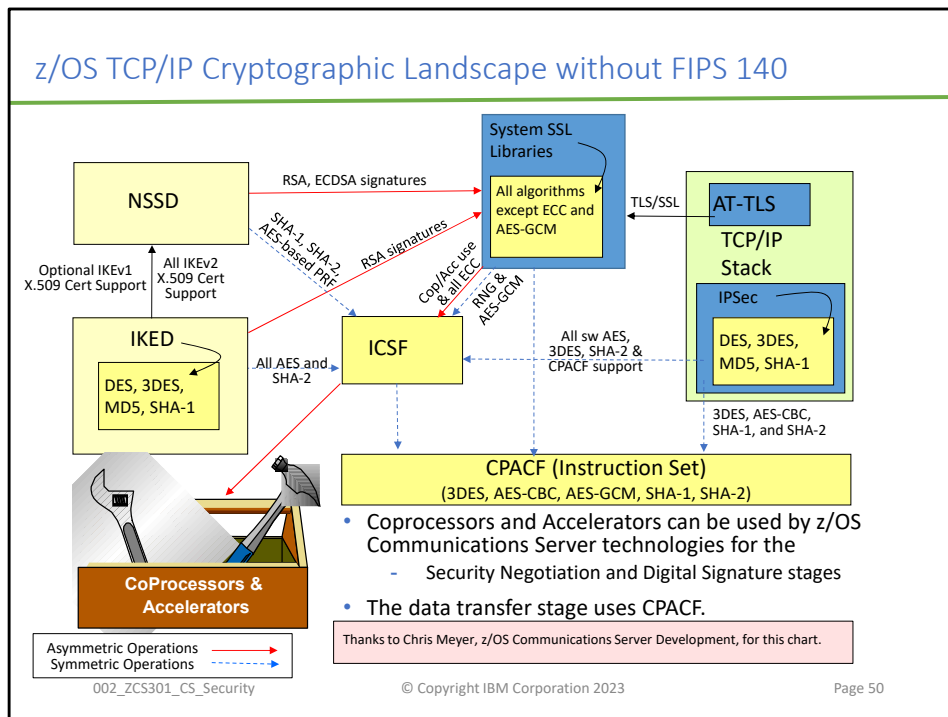
Performance numbers for offload of IPSec onto zIIP engine:
<http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100988>

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 49

You have now explored the entire Security Landscape ... next we show you how one component of security -- data privacy -- is assisted by software and hardware features in z/OS Communications Server. In other words, cryptography is only one small part of the security landscape. Never confuse "Cryptography" with "Security"!



Cryptographic coprocessors and accelerators are available for an extra charge on the System z processors.

CPACF is also available on the System z processors, but it carries no charge. However, you must order it and have the IBM CE enable it for you.

If the customer does not have CPACF enabled in the processor, they have to ask the IBM rep to order the following feature code. It is microcode that is enabled by the CE, it is not something that the customer can enable.

FC3863 CPACF Enablement Lic (License Internal Code)

Pre-V1R10, IPsec uses ICSF to employ AES encryption or for access to CPACF.

However, IPsec prior to z/OS V1R10 had software implementations for DES, 3DES, MD5, and SHA-1 and did not use CPACF at all for these operations. The stack did not even call ICSF for access to CPACF unless the buffer size warranted the extra path length. Starting with V1R10, the z/OS TCP/IP stack changed so that IPsec could directly access CPACF for 3DES, AES, and SHA-1. But, for DES, the TCP/IP stack still needs to use ICSF for access to CPACF on behalf of DES, or the stack can continue to perform DES operations without CPACF.

The z10EC can exploit AES in CPACF; the z10BC cannot; neither can a z9.

AT-TLS uses System SSL for the cryptographic support. The only reason that System SSL might need ICSF is for the Cryptographic processors support.

Note: Consult the System SSL PROGRAMMING GUIDE to discover which ciphers are exploited on a particular hardware platform and where. For example, the z9 and its CPACF do not support AES256 in SSL, but the z10 (both EC and BC) does.

To see which algorithms are available and whether CPACF is enabled on a System z, enable ATTLS in the IP Stack and then examine the JOBLIST of the IP Stack. It tells you what is being supported with System SSL on your hardware platform. Or you can start the GSKSRVR of System SSL and issue a DISPLAY CRYPTO command.

Note that only the System SSL libraries are required for IPsec, IKED, and AT-TLS; there is no need to start the System SSL task named GSKSRVR to obtain these functions.

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

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 51

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 140-2 defines the Security Requirements for Cryptographic Modules. It is published by the National Institute of Standards and Technology (NIST). (See the National Institute of Standards and Technology (NIST) Web site at <http://csrc.nist.gov/publications/PubsFIPS.html> for the most recent info on FIPS 140). Security products must be certified and verified against this standard. These criteria have restrictions on the cryptographic algorithms, protocols and key sizes used when securing connections with SSL or IPSec.

System SSL provides an API for applications to invoke System SSL as FIPS 140-2 compliant. AT-TLS has been updated to support a configuration option to allow AT-TLS to be configured as FIPS 140-2 compliant or not. IPSec also has configuration options for FIPS compliance.

Some examples of the FIPS restrictions are:

- Cryptographic algorithms and keys must be contained within a cryptographic module and accessed through a well defined cryptographic boundary.
- Use of weaker cryptographic algorithms (for example, DES and MD5) is not allowed.
- Use of weaker asymmetric key lengths (for example, RSA digital signature operations using key lengths less than 1024 bits) is not allowed.
- Use of Diffie-Hellman groups with weaker key lengths (key lengths less than 2048 bits) is not allowed. This restriction applies to groups 1, 2, and 5.

Regarding the statement: "Ensuring integrity of crypto algorithms (signed binaries, self-test, environment, and so on)"

- Self-Test: Part of the FIPS 140-2 requirements are the inclusion of "known answer tests" -- essentially, when you load the module, it needs to test its algorithms with these tests -- with known input parameters to ensure that the algorithms generate the "right" (known) answer.
- Signed Binaries: This means that the System SSL DLL is actually signed and the signature is verified when the library is loaded. ICSF must do the same thing.
- Environment really refers to the maintenance of well-defined APIs and the FIPS 140 boundary.

The standard provides four increasing, qualitative levels of security: Security Level 1, Security Level 2, Security Level 3 and Security Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed.

On z/OS systems, Integrated Cryptographic Services Facility (ICSF) and System SSL provide cryptographic services. z/OS Communications Server uses ICSF and System SSL in addition to its own cryptographic algorithms in some of its networking security functions, such as AT-TLS and IPSec. The Crypto-Express3 cards are assigned a security level of 4. (Banks require security levels of 3 and Military requires security level of 4.)

You can configure ICSF, System SSL, and the z/OS Communications Server networking security functions in FIPS 140 mode, in which they will enforce FIPS 140 restrictions.

Note: We recommend initializing ICSF in any case as it is sometimes time-consuming to determine whether or not a specific algorithm or operation will require ICSF access even if hardware cryptographic cards are not installed on the processor.)

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.

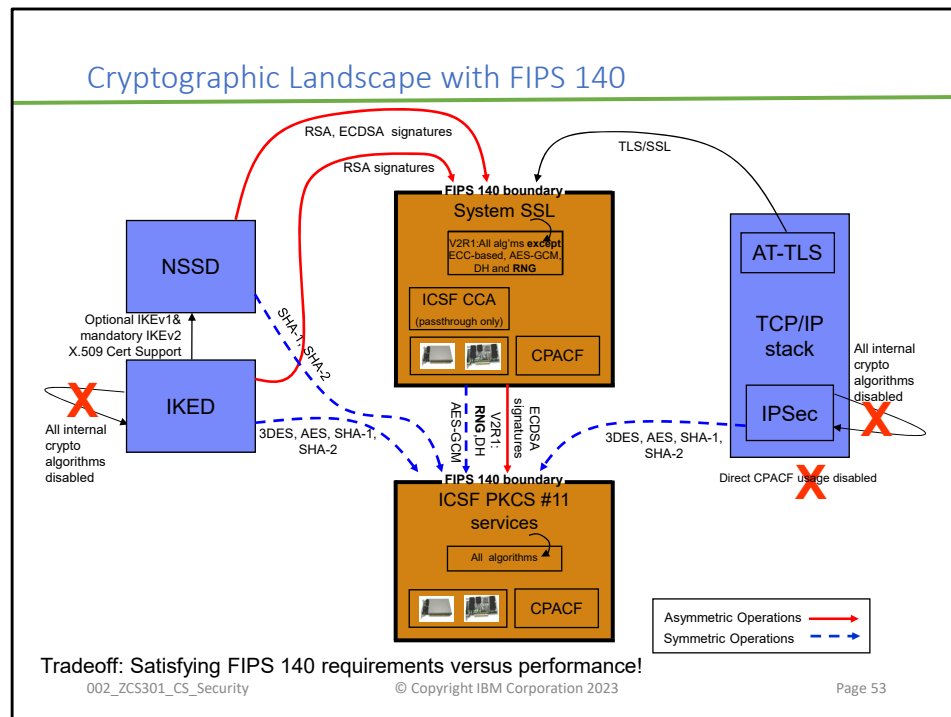
002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 52

4 Levels of compliance for FIPS 140-2:

- Security Level 1: Security Level 1 provides a minimum set of assurance requirements. At a minimum, at least one Approved security function must be implemented in an Approved mode of operation. The module does not provide protection of Critical Security Parameters (CSPs) used or generated by the module. Security Level 1 allows the software components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system.
- Security Level 2: Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals, or for pick-resistant locks on removable covers or doors of the module.
- Security Level 3: In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 provides requirement to mitigate the unauthorized access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at direct physical access, and use or modification of the cryptographic module and probing through ventilation holes or slits.
- Security Level 4 provides the highest level of security in the standard. This level includes all the appropriate security features of the lower levels, as well as extended features.
- At Security Level 4, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments. Security Level 4 introduces the multi-factor authentication requirement for operator authentication. At minimum, this requires two of the following three attributes:
 - something known, such as a secret password
 - something possessed, such as a physical key or token
 - a physical property, such as a biometric



This slide shows the z/OS Communications Server cryptographic landscape under the new FIPS 140 cryptographic mode for IPsec and SSL.

The FIPS 140 enablement can be addressed with parameters that you code in the IPsec and AT-TLS security policies. The IPsec, IKED, and AT-TLS enablement relies on prerequisite enablement in ICSF, in System SSL, etc. as described in the z/OS Communications Server IP Configuration Guide.

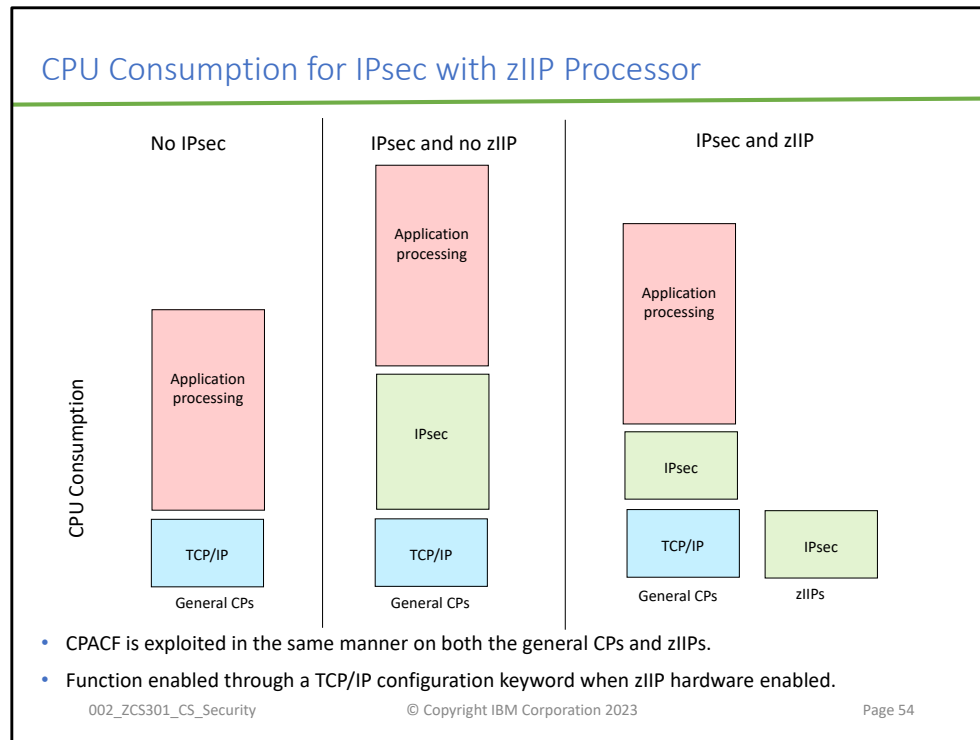
A logical cryptographic boundary is introduced that separates the cryptographic operation requestors from the cryptographic operation providers.

All cryptographic operations must be performed inside the boundary, and be initiated by cryptographic modules in FIPS 140 modes of operation.

- When z/OS IPsec is operating in FIPS 140 mode, only cryptographic methods and modules that are contained inside a logical FIPS 140 cryptographic boundary are used
- When cryptographic operation requests cross this boundary, they must only do so by using interfaces with FIPS 140 certified cryptographic modules
 - As mentioned in a previous slide, the cryptographic modules used by z/OS IPsec are System SSL and optionally ICSF. (Note: We recommend initializing ICSF in any case as it is sometimes time-consuming to determine whether or not a specific algorithm or operation will require ICSF access even if hardware cryptographic cards are not installed on the processor.)
 - The cryptographic modules either provide cryptographic operations themselves, or make internal (to the cryptographic boundary) calls to other cryptographic operation providers.

Tradeoff: Satisfying FIPS 140 requirements versus performance

- The tradeoff being made is meeting requirements of a stringent security standard at the cost of increased use of system resources.
- The use of FIPS 140 mode will impact system resource utilization. This is due to the use of FIPS 140 mode interfaces instead of the most optimized software routines and direct hardware paths.
 - For example, the Disablement of optimized routines and interfaces
 - For example, Direct hardware instructions are not permitted



The performance document is at <http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100988>

The zIIP assisted IPsec function is designed to move most of the IPsec processing from the general purpose processors to the zIIPs. CPACF is available on zIIPs as well as general CPs, so when the IPsec processing moves to a zIIP, it will use CPACF on that zIIP to do its symmetric encrypt/decrypt as well as SHA hashing operations.

z/OS CS TCP/IP recognizes IPsec packets and routes a portion of them to an independent enclave SRB.

- This workload is eligible for the zIIP

The zIIP IPSECURITY design allows Communication Server to interact with z/OS Workload Manager to have a portion of its enclave Service Request Block (SRB) work directed to zIIP. Within CommServer starting with z/OS V1R8, much of the processing related to security routines (Encryption and Authentication algorithms) runs in Enclave

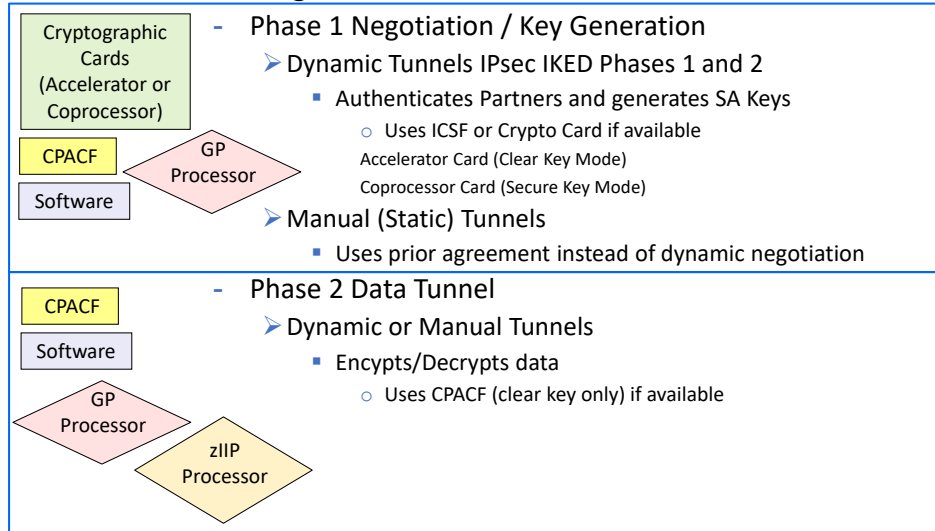
SRBs. In z/OS V1R8, this Enclave SRB workload can be directed to available zIIPs. A single configuration statement within the TCP/IP profile triggers CommServer to request z/OS to direct this IPsec Enclave SRB processing to available zIIPs.

- GLOBALCONFIG ZIIP IPSECURITY

It is possible for IPsec workload performance (response time and/or aggregate throughput) to be improved when zIIPs are added to the configuration. Such Response Time/Throughput improvement is likely if your network performance is currently being constrained by high CPU utilization, and addition of zIIP(s) relieves this constraint.

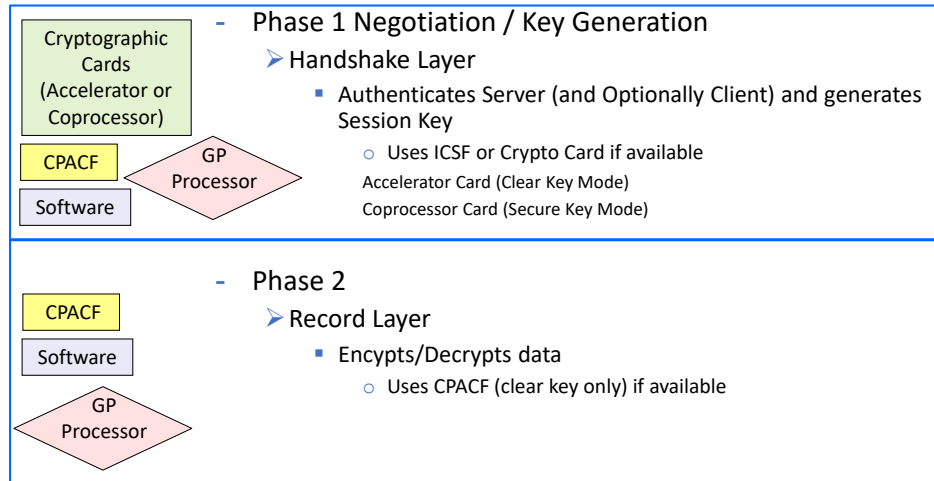
IPsec

- Two Stages



AT-TLS

- Two Stages



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%.

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 58

If a crypto card is implemented in Accelerator mode only, ICSF must be available to exploit it.

If a crypto card is implemented in Coprocessor mode, ICSF must be available, but in addition the x.509 certificates must indicate that secured key will be used if available.

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

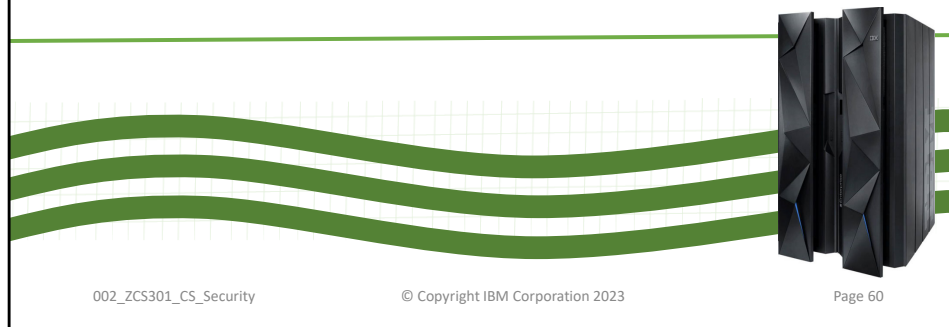
...
System SSL: PCIX cryptographic coprocessor is not available
System SSL: Public key hardware support is not available

These are displays from System SSL that are contained in the TCP/IP Job Log. Similar information is available with displays from the System SSL server ("GSKSRVR").

You can start the GSKSRVR task and then issue the console display command:

'F GSKSRVR,D CRYPTO '

Pervasive Encryption



002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

Page 60

Network Security Services Daemon is required for IKEv2 support.
IKEv2 also requires z/OS V1R12 or later.

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>

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

61

External Firewalls are no longer able to apply Intrusion Detection Services (IDS) to traffic because traffic is being encrypted all the way to z/OS instead of being unencrypted by the external Firewalls.

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 SYSTCPCER 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)

002_ZCS301_CS_Security

© Copyright IBM Corporation 2023

62

External Firewalls are no longer able to apply Intrusion Detection Services (IDS) to traffic because traffic is being encrypted all the way to z/OS instead of being unencrypted by the external Firewalls.

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 ICSP, EKMF, ACSF 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 <i>transit</i> or <i>at rest</i> encryption.

002_ZCS301_CS_Security

Contact: stgls@us.ibm.com
Visit: ibm.com/systems/services/systemz

Page 63

End of Topic

