

# Protecting Your z/OS Data: Safe Flying Through Stormy Weather

*Thomas Cosenza*

*Systems Lab Services Security Consultant*

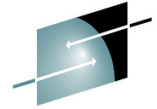
*tcosenza@us.ibm.com*



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



# Trademarks and Notices



The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

- |  |   |   |  |  |
|--|---|---|--|--|
| <ul style="list-style-type: none"> <li>• Advanced Peer-to-Peer Networking®</li> <li>• ADX®</li> <li>• alphaWorks®</li> <li>• AnyNet®</li> <li>• AS/400®</li> <li>• BladeCenter®</li> <li>• Candle®</li> <li>• CICS®</li> <li>• DataPower®</li> <li>• DB2 Connect</li> <li>• DB2®</li> <li>• DRDA®</li> <li>• e-business on demand®</li> <li>• e-business (logo)</li> <li>• e-business (logo)®</li> <li>• ESCON®</li> <li>• FICON®</li> </ul> | <ul style="list-style-type: none"> <li>• GDDM®</li> <li>• GDPS®</li> <li>• Geographically Dispersed Parallel Sysplex</li> <li>• HiperSockets</li> <li>• HPR Channel Connectivity</li> <li>• HyperSwap</li> <li>• i5/OS (logo)</li> <li>• i5/OS®</li> <li>• IBM eServer</li> <li>• IBM (logo)®</li> <li>• IBM®</li> <li>• IBM zEnterprise™ System</li> <li>• IMS</li> <li>• InfiniBand®</li> <li>• IP PrintWay</li> <li>• IPDS</li> <li>• iSeries</li> <li>• LANDP®</li> </ul> | <ul style="list-style-type: none"> <li>• Language Environment®</li> <li>• MQSeries®</li> <li>• MVS</li> <li>• NetView®</li> <li>• OMEGAMON®</li> <li>• Open Power</li> <li>• OpenPower</li> <li>• Operating System/2®</li> <li>• Operating System/400®</li> <li>• OS/2®</li> <li>• OS/390®</li> <li>• OS/400®</li> <li>• Parallel Sysplex®</li> <li>• POWER®</li> <li>• POWER7®</li> <li>• PowerVM</li> <li>• PR/SM</li> <li>• pSeries®</li> <li>• RACF®</li> </ul> | <ul style="list-style-type: none"> <li>• Rational Suite®</li> <li>• Rational®</li> <li>• Redbooks</li> <li>• Redbooks (logo)</li> <li>• Sysplex Timer®</li> <li>• System i5</li> <li>• System p5</li> <li>• System x®</li> <li>• System z®</li> <li>• System z9®</li> <li>• System z10</li> <li>• Tivoli (logo)®</li> <li>• Tivoli®</li> <li>• VTAM®</li> <li>• WebSphere®</li> <li>• xSeries®</li> <li>• z9®</li> <li>• z10 BC</li> <li>• z10 EC</li> </ul> | <ul style="list-style-type: none"> <li>• zEnterprise</li> <li>• zSeries®</li> <li>• z/Architecture</li> <li>• z/OS®</li> <li>• z/VM®</li> <li>• z/VSE</li> </ul> |
|--|---|---|--|--|
- \* All other products may be trademarks or registered trademarks of their respective companies.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Intel Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

## Notes

- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Refer to [www.ibm.com/legal/us](http://www.ibm.com/legal/us) for further legal information.



# Introduction

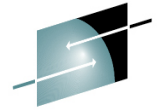


- Work for IBM for 17 years
- IBM Consultant for 11 years
- Working with customers in different business meeting their Network and Security needs

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



2014 was .....



**SHARE**  
Educate · Network · Influence

The Year of the HACK

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



## 2014 a Scary Look Back

- Hacking has gone into overdrive
- 2014 have seen an increase in every type of hacking
  - Denial of Service
  - Criminal
  - Hacktivism
  - Terrorism
  - State Sponsored Attacks

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

## Some Highlights

- Major US Retail Outlets
  - Point of Sales terminals Targeted
- US Banks
  - State Sponsored
  - 76 Million US Households effected
- SONY hack
  - Possibly State Sponsored
  - Hackers had months in their network
  - Demands shut down of a movie
    - So not all bad, I mean did you see it

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

## We need a new call to arms !!!

- “The Security Perimeter is now at the End Point”  
Anonymous
- SECURITY IS EVERYONES JOB!!!



Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

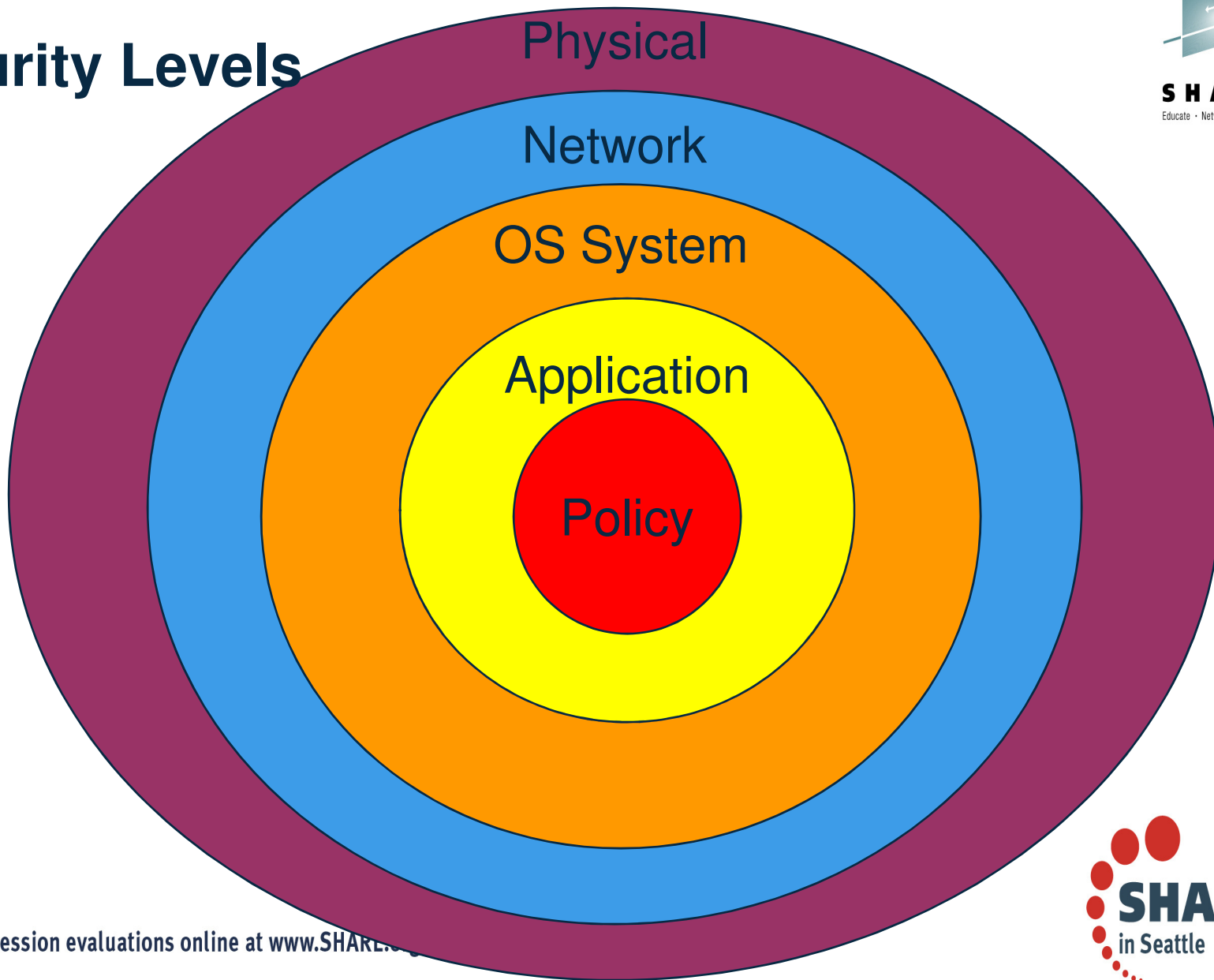
# Why Add Security

- Failure to Secure your business
  - Fines and penalties
  - Incidents from loss of data
    - Cost for forensics examinations
    - Liability for the losses
    - Dispute resolution costs
  - Stock Shares plummet
  - Loss of Customers

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# Security Levels



Complete your session evaluations online at [www.SHARE.org](http://www.SHARE.org)



# Most do a good Job protecting the Castle



- Use of SAF Profiles
- Encrypted DASD
- Dedicated fiber channels
- Firewalled zone where z/OS resides
- etc

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



## However

- STORM CLOUDS ARE GATHERING OUTSIDE YOUR WALLS!!!
- You no longer need to have physical access to hack your systems.
- This is more like chess than checkers
  - You have to think moves ahead of your opponent
  - Each layer of your enterprise needs to be strengthened
- Are the following secured with encryption??
  - User Logons
  - PI Data
  - Transactions

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

# You say we just transmit data within our intranet?



- A study that took 30 large companies has shown that the cost of cybercrime has been on average of \$5.9 Million
- Over 70% of successful cyber attacks occur within a companies intranet
- Criminal organizations have been shown to infiltrate network teams so they can dump information off of routers performing man in the middle attacks

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

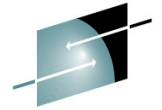


# CS for z/OS gives you two built in methods

- IPsec VPN
  - Layer 3 Protection
- TLS support
  - Application Based
  - AT-TLS
- Lets take a look at these methods



Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



SHARE

# z/OS TCP/IP secure networking protocols

- z/OS TCP/IP cryptographically protects network data in three ways:

## #1 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) through System SSL

- Application is explicitly coded to use these
- Per-session protection
- TCP only

## #2 Application Transparent TLS (AT-TLS)

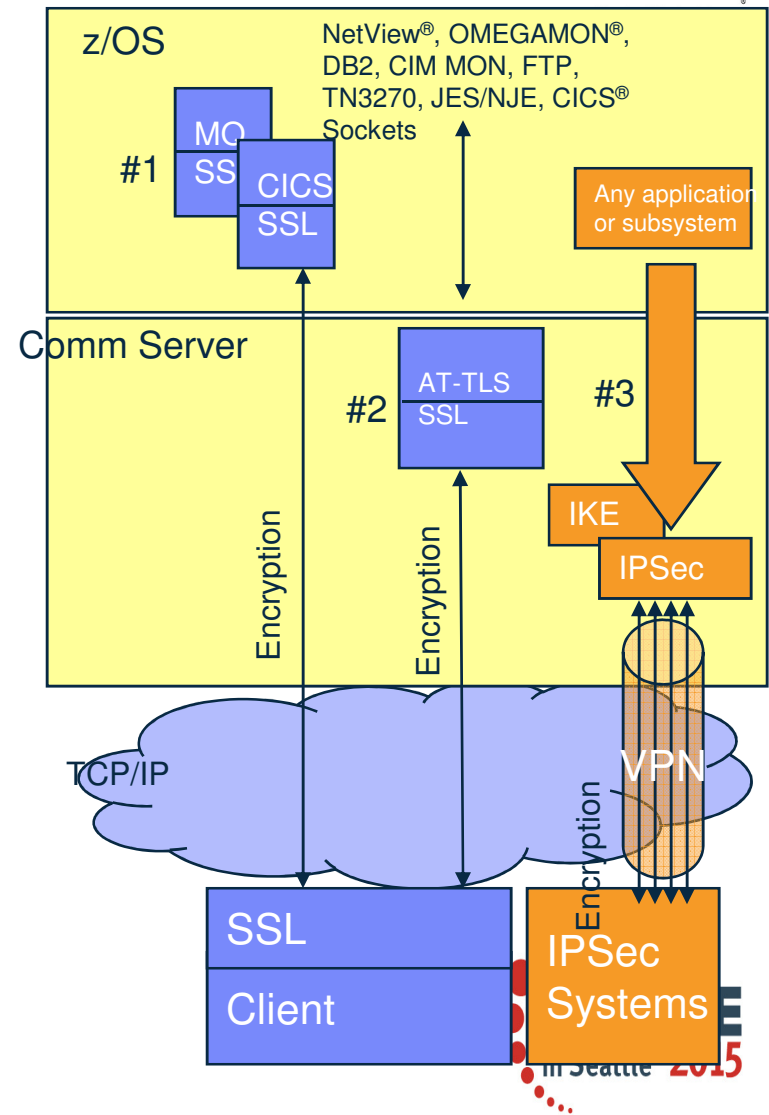
- TLS applied in transport layer (TCP) as defined by policy
- Typically applied transparently to application
- TCP/IP stack is user of System SSL services

## #3 Virtual Private Networks using IP Security (IPSec) and Internet Key Exchange (IKE)

- “Platform to platform” encryption
- IPSec implemented at the IP layer as defined by policy
- Wide variety (any to all) of traffic is protected
- Completely transparent to application
- IKE allows IPSec tunnels to be established dynamically

- When do you use one form versus another?
  - Depends on client, application, topology, performance requirements, and so forth.
  - Beyond scope of this presentation

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



in Seattle 2015

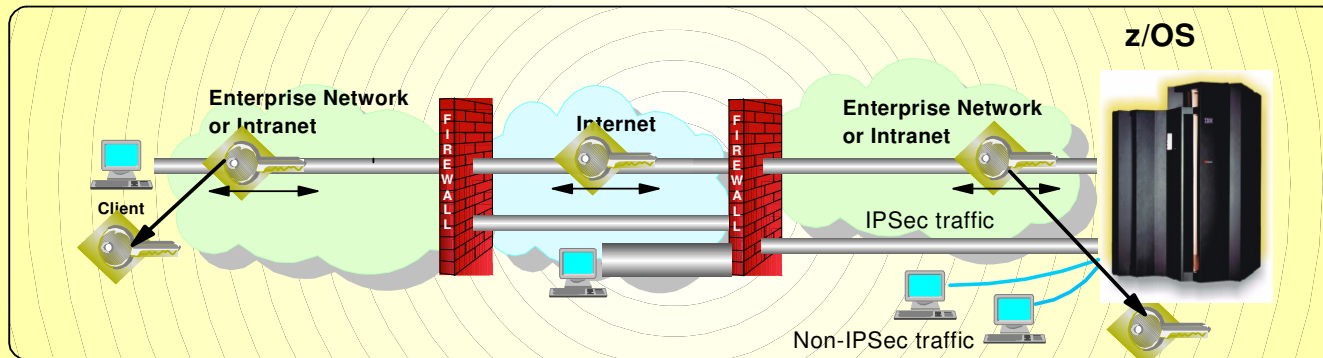
# z/OS Communications Server Network Security



## IPSec VPN

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



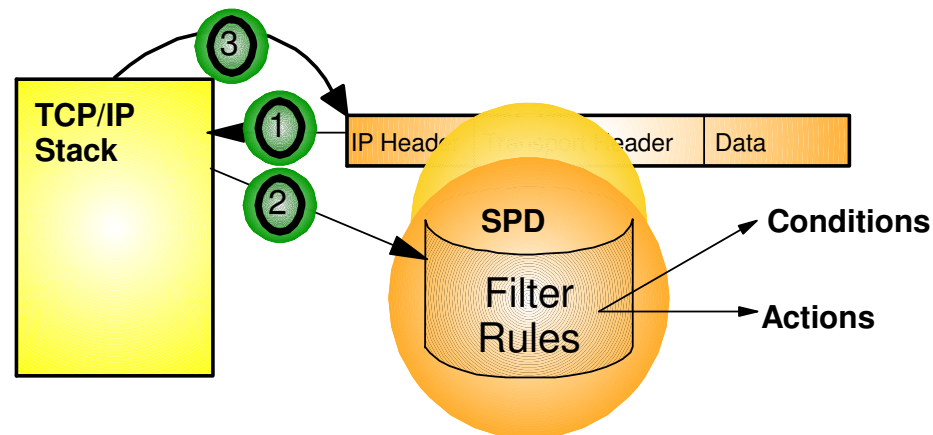


- Protection
  - ▶ IP filtering
- Cryptographic
  - ▶ Manual IPsec for static security associations
  - ▶ Dynamic negotiation of IPsec security associations through IKE
- Filter directed logging of IP security actions to syslogd



# IP Filtering Processing Overview

1. Inbound or outbound IP packet arrives
2. Consult set of filter rules in a filter rule table - Security Policy Database (SPD)
  - ▶ Rules have conditions and actions
3. Apply action of matching rule to packet
  - ▶ Deny
  - ▶ Permit
  - ▶ Permit with additional processing applied



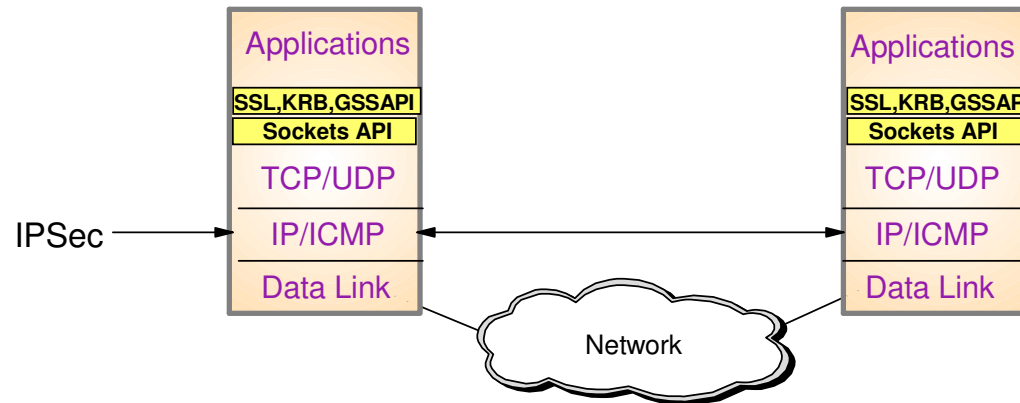
- Filter rules are searched in the order they were configured
- Each rule is inspected, from top to bottom, for a match
- If a match is found, the search ends and the action is performed

# Filtering Conditions

Criteria	Description
<b>From packet</b>	
Source address	Source IP address in IP header of packet
Destination address	Destination IP address in IP header of packet
Protocol	Protocol in the IP header of packet (TCP, UDP, OSPF, etc.)
Source port	For TCP and UDP, the source port in the transport header of packet
Destination port	For TCP and UDP, the destination port in the transport header of packet
ICMP type and code	For ICMP, type and code in the ICMP header of packet
OSPF type	For OSPF, type located in the OSPF header of packet
IPv6 Mobility type	For traffic with IPv6 mobility headers, MIPv6 type in header of packet.
Fragments Only	Matches fragmented packets only (applicable to routed traffic only)
<b>Network attributes</b>	
Direction	Direction of packet.
Routing	Packet is local if source or destination IP address exists on local host, otherwise it is routed
Link security class	A virtual class that allow you to group interfaces with similar security requirements. Non-VIPA addresses can be assigned a security class. Packets inherit the security class of the interface over which packet is sent/received.
<b>Time condition</b>	
Time, Day, Week, Month	Indicates when filter rule is active



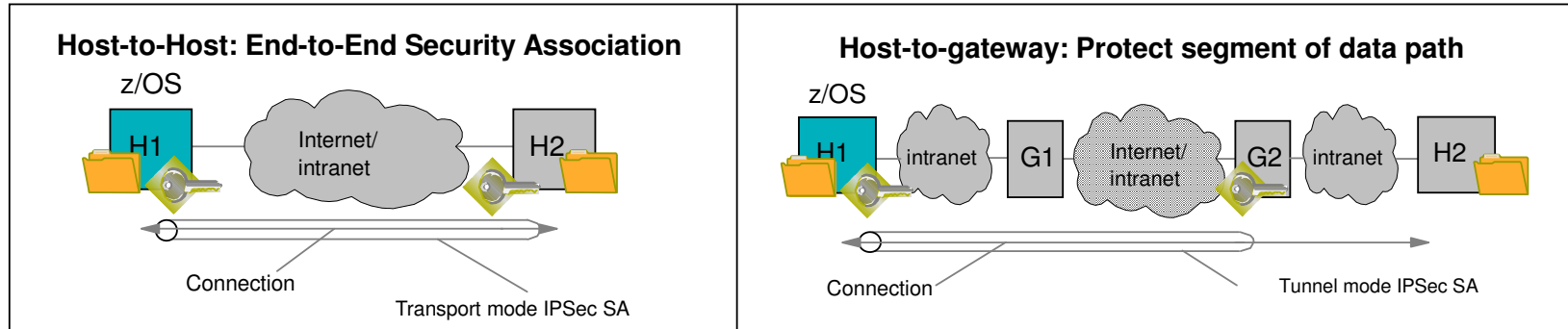
# IPSec Protocol Overview



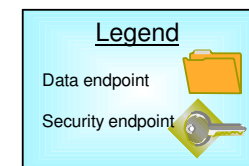
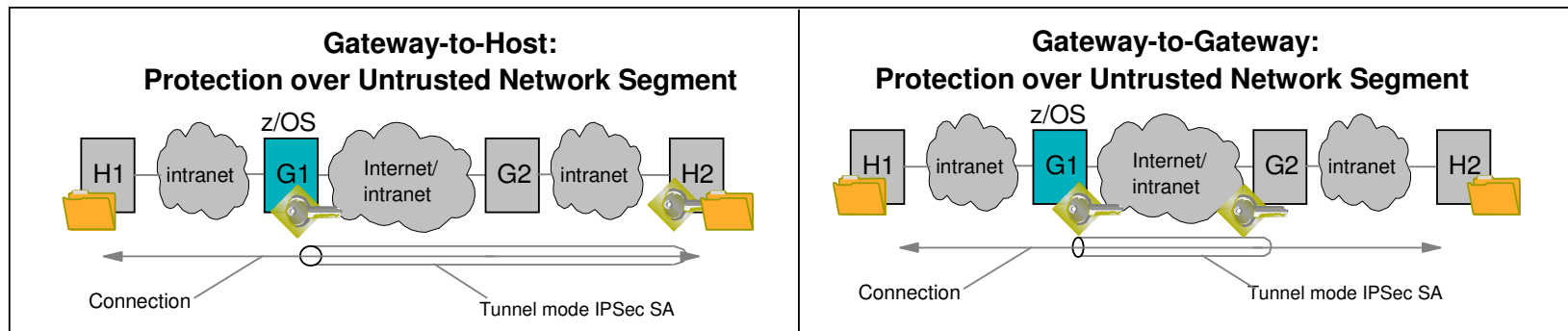
- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
  - ▶ IPSec security protocols
    - **Authentication Header (AH)** - provides data authentication / integrity
    - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional 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 (**Internet Key Exchange (IKE)**)

# IPSec Scenarios and z/OS Roles

## z/OS as Host (Data Endpoint)



## z/OS as Gateway (Routed Traffic)



# Stack hardware crypto usage (IPSec: AH, ESP): Non-FIPS 140 mode



- DES, 3DES, AES encryption of data traffic
- SHA-1 and MD5 HMACs for message authentication
- SHA-2 HMACs, AES-XCBC, and AES-GMAC MACs for message authentication (V1R12)
- Starting with V1R8 (APAR PK40178), all SRB-based processing in stack, *including these crypto operations*, can be offloaded to zIIP to reduce cost of IPSec protection.

Crypto Type	Algorithm	CPACF (stack doesn't use coproc'r or accel'r)
Symmetric Enc/Dec	DES	In CPACF (via ICSF)
	3DES	In CPACF
	AES-CBC-128	In CPACF
	AES-CBC-256 *	In software via ICSF on z9, CPACF in z10
	AES-GCM-128, -256 *	In software via ICSF
Symmetric Authentication	SHA-1	In CPACF
	SHA-256 *	In CPACF
	SHA-384, -512 *	In software via ICSF on z9, CPACF in z10
	AES-XCBC MAC and AES-GMAC-128, -256 *	In software via ICSF
	MD5	In software

Complete your session evaluations online at [www.SHARE.Ng/Seattle](http://www.SHARE.Ng/Seattle) for V1R12



# Stack hardware crypto usage (IPSec: AH, ESP): FIPS 140 mode (V1R12)



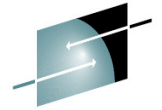
- 3DES, AES encryption of data traffic
- SHA-1 HMACs
- SHA-2 HMACs, AES-GMAC MACs for message authentication (V1R12)
- Note: FIPS 140 does not allow DES, MD5 or AES-XCBC
- All SRB-based processing in stack, *including these crypto operations*, can be offloaded to zIIP to reduce cost of IPSec protection.

Crypto Type	Algorithm	CPACF (stack doesn't use coproc'r or accel'r)
Symmetric Enc/Dec	3DES	In CPACF via ICSF **
	AES-CBC-128	In CPACF via ICSF **
	AES-CBC-256 *	In software on z9, CPACF in z10, all via ICSF **
	AES-GCM-128, -256 *	In software via ICSF **
Symmetric Authentication	SHA-1	In CPACF via ICSF **
	SHA-256 *	In CPACF via ICSF **
	SHA-384, -512 *	In software on z9, CPACF in z10, all via ICSF **
	AES-GMAC-128, -256 *	In software via ICSF **

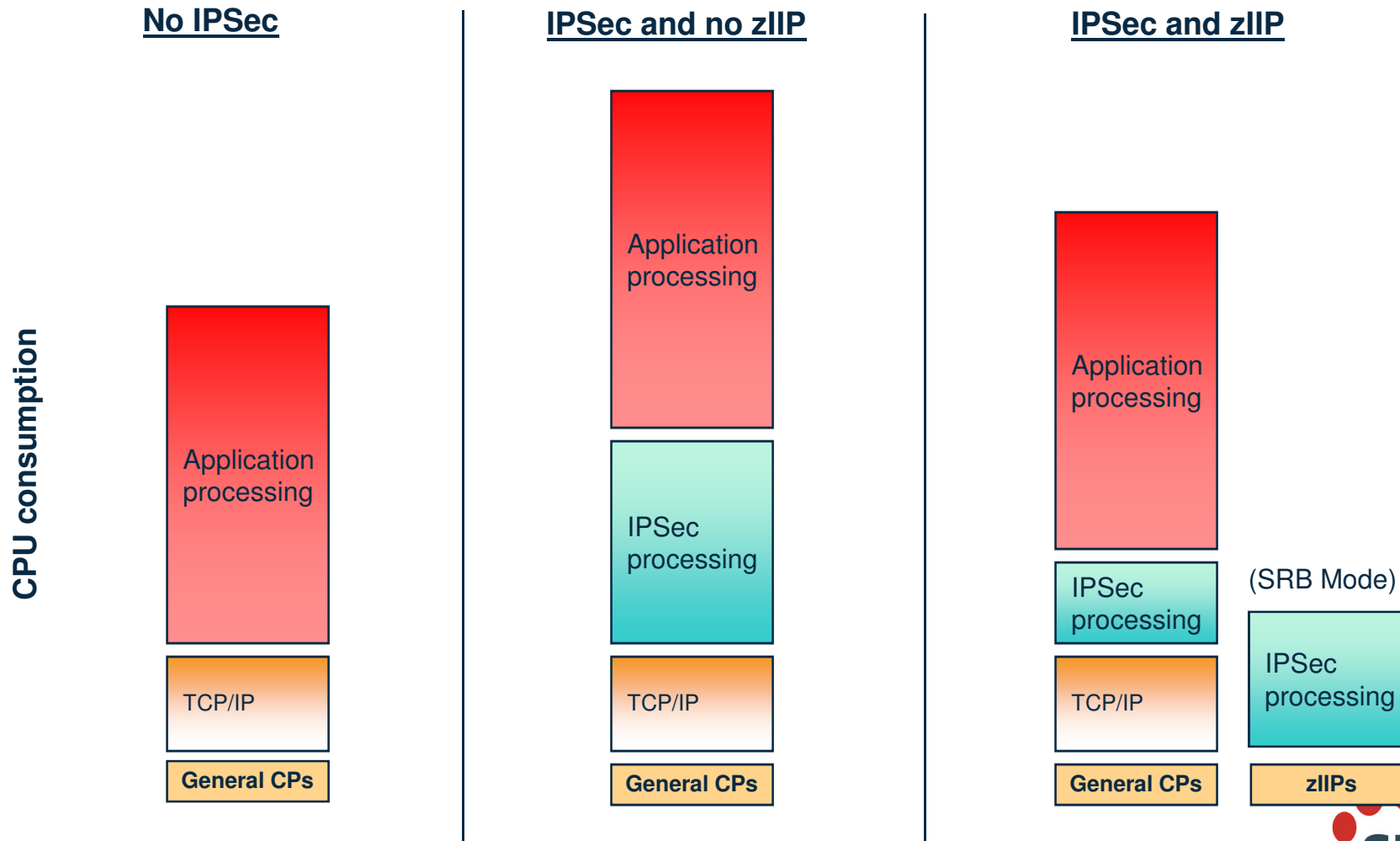
\* New algorithm for V1R12  
Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

\*\* New with V1R12 FIPS 140 support





# IPSec processing using zIIP



- CPU is exploited in the same way on both the general CPs and the zIIPs
- Function enabled through a TCP/IP configuration keyword when zIIP hardware and pre-req software is in place

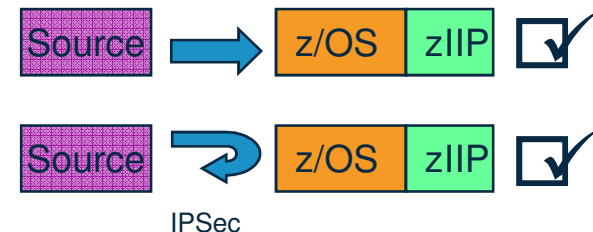
# What IPSec workload is eligible for zIIP?



- The zIIP assisted IPSec function is designed to move most of the IPSec processing from the general purpose processors to the zIIPs
- 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

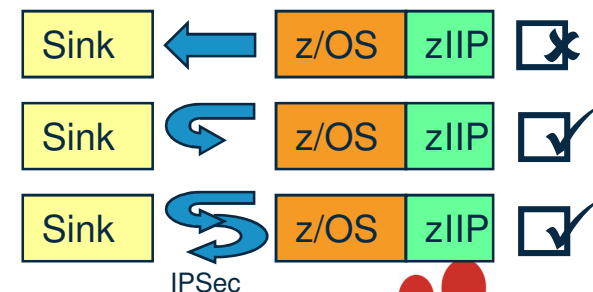
## – Inbound operation (not initiated by z/OS)

- All inbound IPSec processing is dispatched to enclave SRBs and is eligible for zIIP
- All subsequent outbound IPSec responses from z/OS are dispatched to enclave SRB. This means that all encryption/decryption of message integrity and IPSec header processing is sent to zIIP



## – Outbound operation (initiated by z/OS)

- Operation which starts on a TCB is not zIIP eligible
- BUT... any inbound response or acknowledgement is SRB-based and therefore zIIP eligible
- AND... all subsequent outbound IPSec responses from z/OS are also zIIP eligible



Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)





# z/OS Communications Server IP Security 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
- **Policy-based**
  - Configuration Assistant GUI for both new and expert users
  - Direct file edit into local configuration file
- **Default filters in TCP profile provide basic protection before policy is loaded**
- **Cryptographic algorithms**
  - RSA signature-based authentication
  - ECDSA signature-based authentication
  - HMAC-SHA-1, HMAC-MD5 authentication
  - HMAC-SHA-2, AES-XCBC, AES-GMAC authentication
  - AES-CBC, 3DES and DES encryption
  - AES-GCM (128- and 256-bit) encryption
  - Uses cryptographic hardware if available for most algorithms
  - FIPS 140 mode
- **zIIP Assisted IPSec**
  - Moves most IPSec processing from general purpose processors to zIIPs
- **IP Security Monitoring Interface**
  - IBM Tivoli OMEGAMON XE for Mainframe Networks uses this interface
- **Support for latest IPSec RFCs**
  - RFCs 4301-4305, 4307-4308
  - RFC 4306 (IKEv2)

# More updates

## *z/OS Communications Server V1R13*

### ▪ **NAT Traversal support for IKEv2**

- ▶ IKEv1 support for NAT Traversal available in previous releases

### ▪ **Sysplex Wide Security Associations support for IKEv2**

- ▶ IKEv1 support for Sysplex Wide Security Associations available in previous releases

## *z/OS Communications Server V2R1*

### ▪ **Sysplex Wide Security Associations support for IPv6**

### ▪ **QDIO Acceleration coexistence with IP Packet Filtering**

- ▶ V2R1 will allow QDIOACCELERATOR function with IPSECURITY in the TCPIP profile if all routed traffic is explicitly permitted, otherwise routed traffic will be processed by the IP layer

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

# z/OS Communications Server Network Security

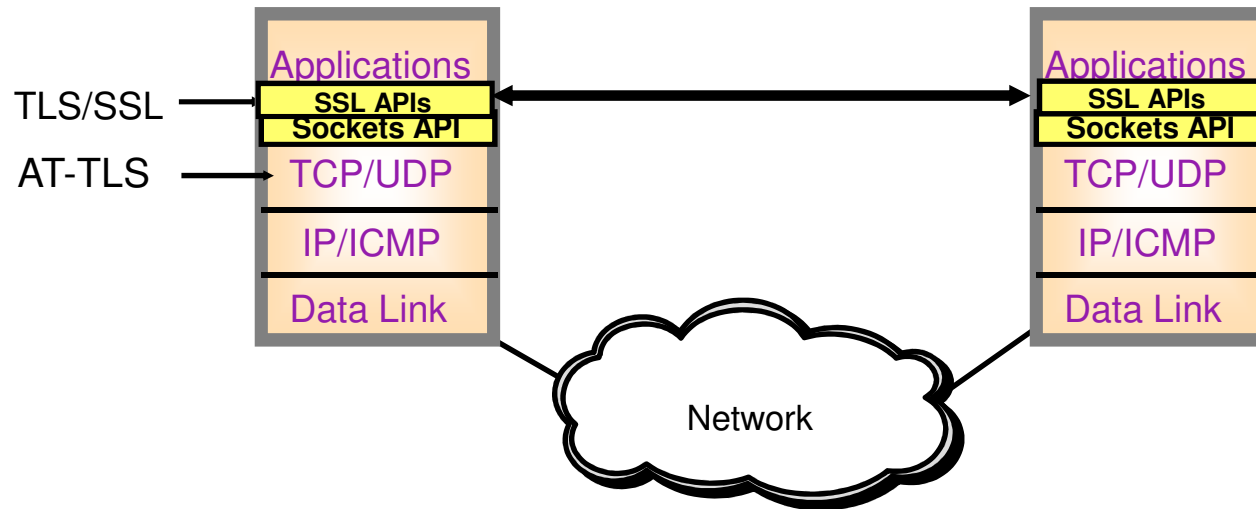


## Application Transparent Transport Layer Security

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# Transport Layer Security Protocol Overview

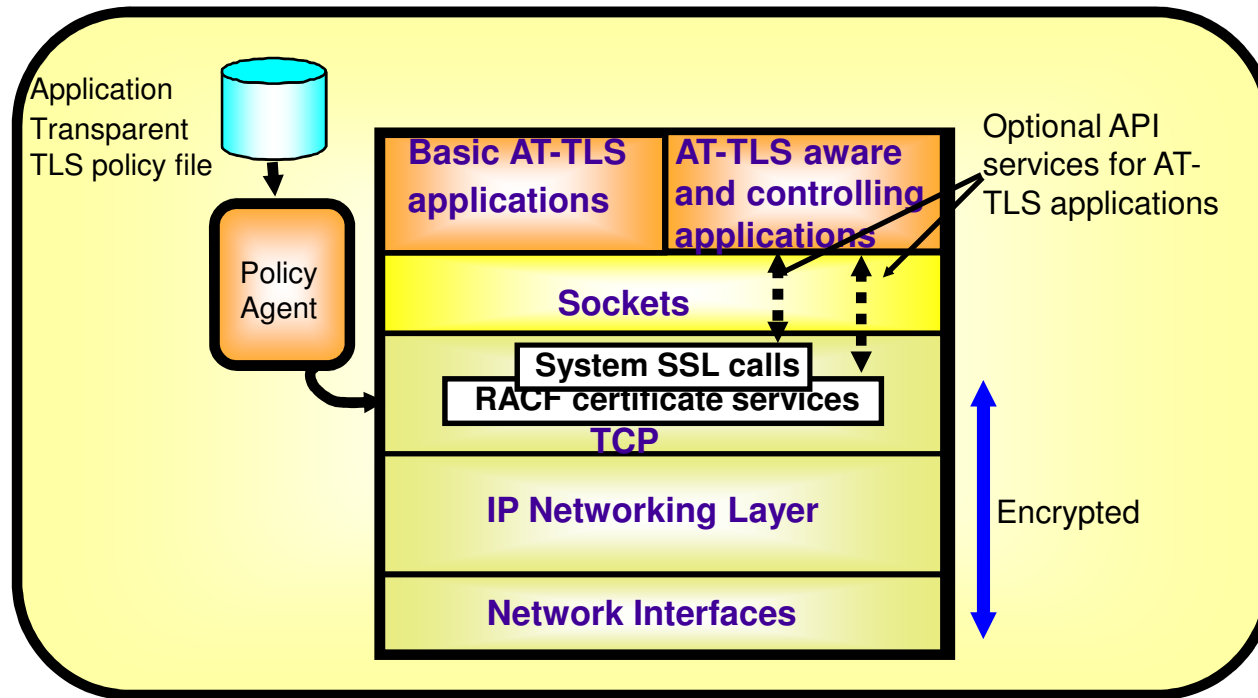


- TLS traditionally provides security services as a socket layer service
  - ▶ TLS requires reliable transport layer,
    - Typically TCP (but architecturally doesn't have to be TCP)
  - ▶ UDP applications cannot be enabled with traditional TLS
    - There is now a TLS variant called Datagram Transport Layer Security (DTLS) which is defined by the IETF for unreliable transports
- On z/OS, System SSL (a component of z/OS Cryptographic Services) provides an API library for TLS-enabling your C and C++ applications
- Java Secure Sockets Extension (JSSE) provides libraries to enable TLS support for Java applications
- However, there is an easier way...
  - ... Application Transparent TLS!

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# AT-TLS Overview



- **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
- **Most applications require no change to use AT-TLS**
  - ▶ AT-TLS Basic applications
- **Applications can optionally exploit advanced features using SIOCTLSCTL ioctl call**
  - ▶ AT-TLS Aware applications
    - Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)
  - ▶ AT-TLS Controlling applications
    - Control if/when to start/stop TLS, reset session/cipher

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# AT-TLS Advantages



- Reduces cost
  - ▶ Application development
    - Cost of System SSL integration
    - Cost of application SSL-related configuration support
  - ▶ Consistent TLS administration across z/OS applications
    - Single, consistent AT-TLS policy system-wide vs. application specific policy
- Exploits SSL/TLS features beyond what most SSL/TLS applications choose to support
  - ▶ CRLs, multiple keyrings per server, use of System SSL cache, etc.
- Support of new System SSL functions without application changes
  - ▶ AT-TLS makes vast majority of System SSL features available to applications
  - ▶ As System SSL features are added, applications can use them by administrative change to AT-TLS policy
- Allows SSL/TLS-enablement of non-C sockets applications on z/OS (e.g., CICS sockets, assembler and callable sockets, etc.)

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# Recent AT-TLS Enhancements Summary



## *z/OS Communications Server V2R1*

### ▪ **Transport Layer Security (TLS) Renegotiation Extension (RFC 5746):**

- ▶ Provides a mechanism to protect peers that permit re-handshakes
- ▶ When supported, it enables both peers to validate that the re-handshake is truly a continuation of the previous handshake

### ▪ **Support Elliptic Curve Cryptography (ECC)**

- ▶ Twenty new ECC cipher suites
- ▶ ECC cipher suites for TLS (RFC 4492)

### ▪ **TLS Protocol Version 1.2 (RFC 5246): (available in V1R13 with APAR)**

- ▶ Twenty-one new cipher suites
  - 11 new HMAC-SHA256 cipher suites
  - 10 new AES-GCM cipher suites

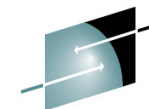
### ▪ **Support for Suite B cipher suites**

- ▶ TLS is required
- ▶ All cipher suites use ECC
- ▶ Suite B has two levels of cryptographic strength that can be selected
  - 128 or 192 bit

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# AT-TLS Policy Conditions



**SHARE**  
Educate · Network · Influence

Criteria	Description
<b>Resource attributes</b>	
Local address	Local IP address
Remote address	Remote IP address
Local port	Local port or ports
Remote port	Remote port or ports
<b>Connection type attributes</b>	
Connection direction	<ul style="list-style-type: none"> <li>•Inbound (applied to first Select, Send, or Receive after Accept)</li> <li>•Outbound (applied to Connect)</li> <li>•Both</li> </ul>
<b>Application attributes</b>	
User ID	User ID of the owning process or wildcard user ID
Jobname	Jobname of the owning application or wildcard jobname
<b>Time condition</b>	
Time, Day, Week, Month	When filter rule is active

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

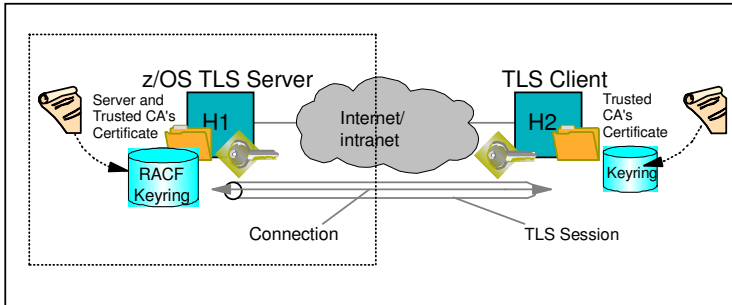




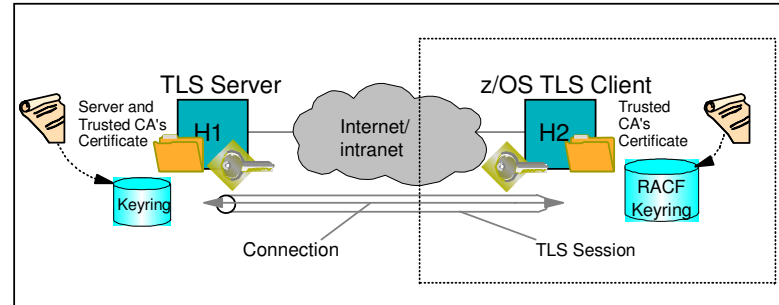
# z/OS AT-TLS Supported Roles

Server authentication only

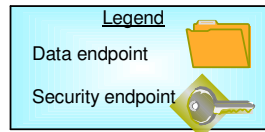
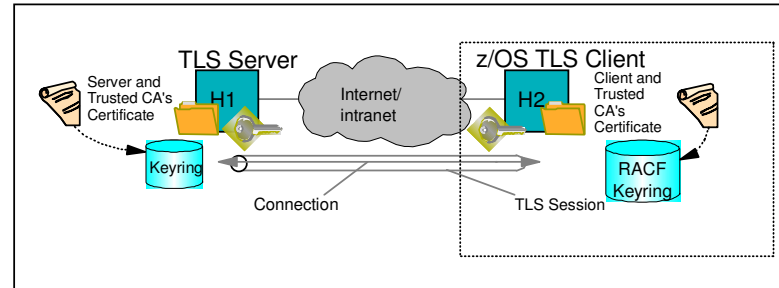
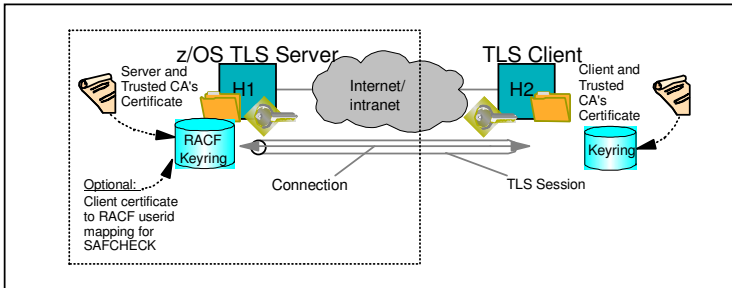
z/OS as Server

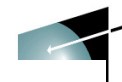


z/OS as Client



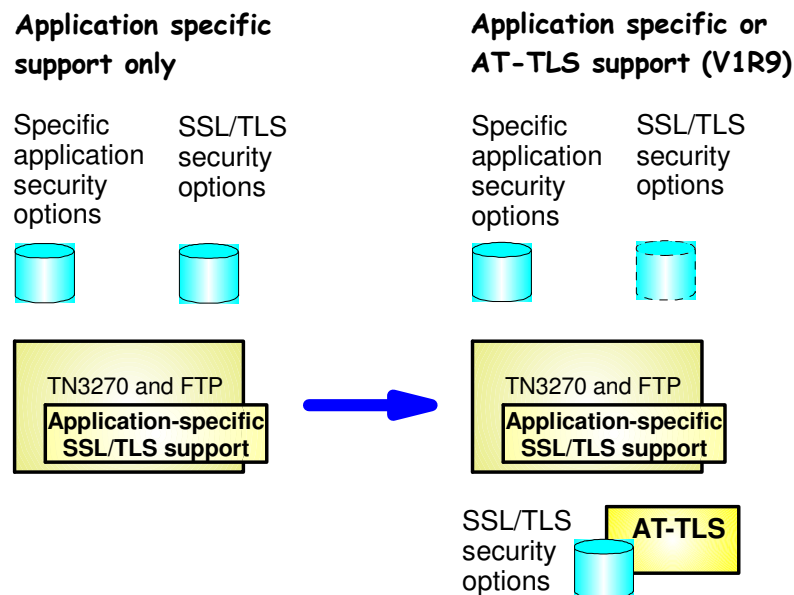
Server + client authentication





# AT-TLS Enabling TN3270 and FTP

- **Both the FTP server and client, and the TN3270 server on z/OS originally were SSL/TLS enabled with System SSL**
  - ▶ With the advantages of AT-TLS, it is desirable to migrate that SSL/TLS support to AT-TLS
- **Subsequently, FTP and TN3270 were enabled for AT-TLS awareness and control**
  - ▶ May need certificate and there are negotiating protocols prior to the TLS handshake
- **Approach used for enabling FTP and TN3270 for AT-TLS**
  - ▶ "Move" the SSL/TLS-specific configuration into the common AT-TLS policy format
    - One common policy format where new options can be added without changes to all applications
  - ▶ Keep application-specific security options in application configuration



# SSL/TLS (and AT-TLS) hardware crypto usage

Crypto Type	Algorithm	CPACF available only	CPACF + Coprocessor/Accelerator
Asymmetric Encrypt/Decrypt	RSA signature generation	In software	In coprocessor mode only (non-FIPS mode only). Otherwise in software (accelerator does not support this operation).
	RSA signature verification	In software	In coprocessor/accelerator.
	PKA encrypt/decrypt for handshake	In software	In coprocessor/accelerator
Symmetric Encrypt/Decrypt	DES	CPACF (non-FIPS mode only: DES not allowed in FIPS mode)	
	3DES	CPACF	
	AES-CBC-128	CPACF	
	AES-CBC-256	In software on z9, CPACF in z10	
Symm Auth	SHA-1	CPACF	
	MD5	In software (non-FIPS mode only: MD5 not allowed in FIPS mode)	

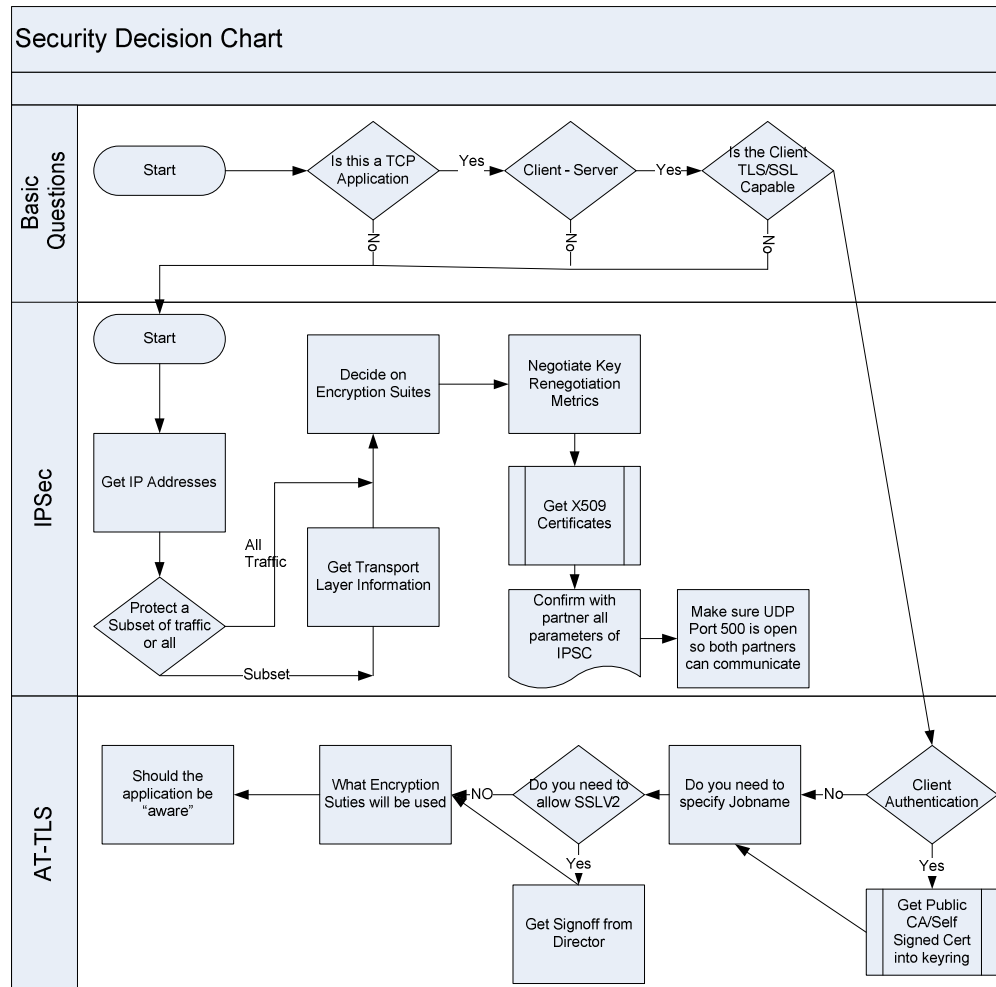
Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# IPSec and AT-TLS Comparison

	<b>IPSec</b>	<b>AT-TLS</b>
<b>Traffic protected with data authentication and encryption</b>	All protocols	TCP
<b>End-to-end protection</b>	Yes (transport mode)	Yes
<b>Segment protection</b>	Yes (tunnel mode)	No
<b>Scope of protection</b>	<u>Security association</u> 1)all traffic 2)protocol 3)single connection	<u>TLS session</u> 1)single connection
<b>How controlled</b>	<u>IPSec policy</u> 1)z/OS responds to IKE peer 2)z/OS initiates to IKE peer based on outbound packet, IPSec command, or policy autoactivation	<u>AT-TLS policy</u> 1)For handshake role of server, responds to TLS client based on policy 2)For handshake role of client, initializes TLS based on policy 3)Advanced function applications
<b>Requires application modifications?</b>	No	No, unless advanced function needed 1)Obtain client cert/userid 2)Start TLS
<b>Security endpoints</b>	Device to device	Application to application
<b>Type of authentication</b>	Peer-to-peer	1)Server to client 2)Client to server (optional)
<b>Authentication credentials</b>	1)Preshared keys 2)X.509 certificates	X.509 certificates
<b>Authentication principals</b>	Represents host	Represents user
<b>Session key generation/refresh</b>	Yes with IKE No with manual IPSec	TLS handshake



# So how do you decide what to use



Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

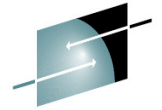
## For more information



URL		Content
<a href="http://www.twitter.com/IBM_Commserver">http://www.twitter.com/IBM_Commserver</a>		IBM Communications Server Twitter Feed
<a href="http://www.facebook.com/IBMCommserver">http://www.facebook.com/IBMCommserver</a>		IBM Communications Server Facebook Fan Page
<a href="http://www.ibm.com/systems/z/">http://www.ibm.com/systems/z/</a>		IBM System z in general
<a href="http://www.ibm.com/systems/z/hardware/networking/">http://www.ibm.com/systems/z/hardware/networking/</a>		IBM Mainframe System z networking
<a href="http://www.ibm.com/software/network/commserver/">http://www.ibm.com/software/network/commserver/</a>		IBM Software Communications Server products
<a href="http://www.ibm.com/software/network/commserver/zos/">http://www.ibm.com/software/network/commserver/zos/</a>		IBM z/OS Communications Server
<a href="http://www.ibm.com/software/network/commserver/z_lin/">http://www.ibm.com/software/network/commserver/z_lin/</a>		IBM Communications Server for Linux on System z
<a href="http://www.ibm.com/software/network/ccl/">http://www.ibm.com/software/network/ccl/</a>		IBM Communication Controller for Linux on System z
<a href="http://www.ibm.com/software/network/commserver/library/">http://www.ibm.com/software/network/commserver/library/</a>		IBM Communications Server library
<a href="http://www.redbooks.ibm.com">http://www.redbooks.ibm.com</a>		ITSO Redbooks
<a href="http://www.ibm.com/software/network/commserver/zos/support/">http://www.ibm.com/software/network/commserver/zos/support/</a>		IBM z/OS Communications Server technical Support – including TechNotes from service
<a href="http://www.ibm.com/support/techdocs/atmastr.nsf/Web/TechDocs">http://www.ibm.com/support/techdocs/atmastr.nsf/Web/TechDocs</a>		Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
<a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a>		Request For Comments (RFC)
<a href="http://www.ibm.com/systems/z/os/zos/bkserv/">http://www.ibm.com/systems/z/os/zos/bkserv/</a>		IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

 in Seattle 2015



**SHARE**  
Educate · Network · Influence

# DON'T FORGET YOUR EVALS



Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

