

z Exchange – April 26, 2016

# End-to-end encryption options on z/OS

Chris Meyer, CISSP ([meyerchr@us.ibm.com](mailto:meyerchr@us.ibm.com))  
z/OS Communications Server design and architecture





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

- |                                     |   |                         |                   |                  |
|-------------------------------------|---|-------------------------|-------------------|------------------|
| • Advanced Peer-to-Peer Networking® | • FICON®                                    | • IPDS                  | • POWER7®         | • Tivoli®        |
| • AIX®                              | • GDDM®                                     | • iSeries               | • PowerVM         | • VTAM®          |
| • alphaWorks®                       | • GDPS®                                     | • LANDP®                | • PR/SM           | • WebSphere®     |
| • AnyNet®                           | • Geographically Dispersed Parallel Sysplex | • Language Environment® | • pSeries®        | • xSeries®       |
| • AS/400®                           | • HyperSockets                              | • MQSeries®             | • RACF®           | • z10®           |
| • BladeCenter®                      | • HPR Channel Connectivity                  | • MVS                   | • Rational Suite® | • z13®           |
| • Candle®                           | • HyperSwap                                 | • NetView®              | • Rational®       | • zEnterprise®   |
| • CICS®                             | • i5/OS (logo)                              | • OMEGAMON®             | • Redbooks        | • zSeries®       |
| • DataPower®                        | • i5/OS®                                    | • Open Power            | • Redbooks (logo) | • z Systems®     |
| • DB2 Connect                       | • IBM eServer                               | • OpenPower             | • Sysplex Timer®  | • z/Architecture |
| • DB2®                              | • IBM (logo)®                               | • Operating System/2®   | • System i5       | • z/OS®          |
| • DRDA®                             | • IBM®                                      | • Operating System/400® | • System p5       | • z/VM®          |
| • e-business on demand®             | • IBM zEnterprise™ System                   | • OS/2®                 | • System x®       | • z/VSE          |
| • e-business (logo)                 | • IMS                                       | • OS/390®               | • System z®       |                  |
| • e business (logo)®                | • InfiniBand®                               | • OS/400®               | • System z9®      |                  |
| • ESCON®                            | • IP PrintWay                               | • Parallel Sysplex®     | • System z10      |                  |
|                                     |   | • POWER®                | • Tivoli (logo)®  |                  |

\* 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 or 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, 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.

## Agenda

- What is end-to-end security?
- Network security protocols
  - The protocols
    - Transport Layer Security (TLS, also known as SSL)
    - IPsec
    - Secure Shell (SSH)
  - z/OS implementation options
  - Considerations for each option
- Protecting z/OS traffic
  - Common z/OS traffic types
    - TN3270
    - Enterprise Extender (EE)
    - FTP
    - SFTP (SSH file transfer)
    - Connect:Direct (aka NDM)
    - CSSMTP
    - CICS
    - MQ
    - IMS Connect
    - DB2
    - NJE
    - HTTP WebSphere
    - DNS
    - NFS, Portmapper
    - lpd
    - ICMP
  - Alternatives for protecting each

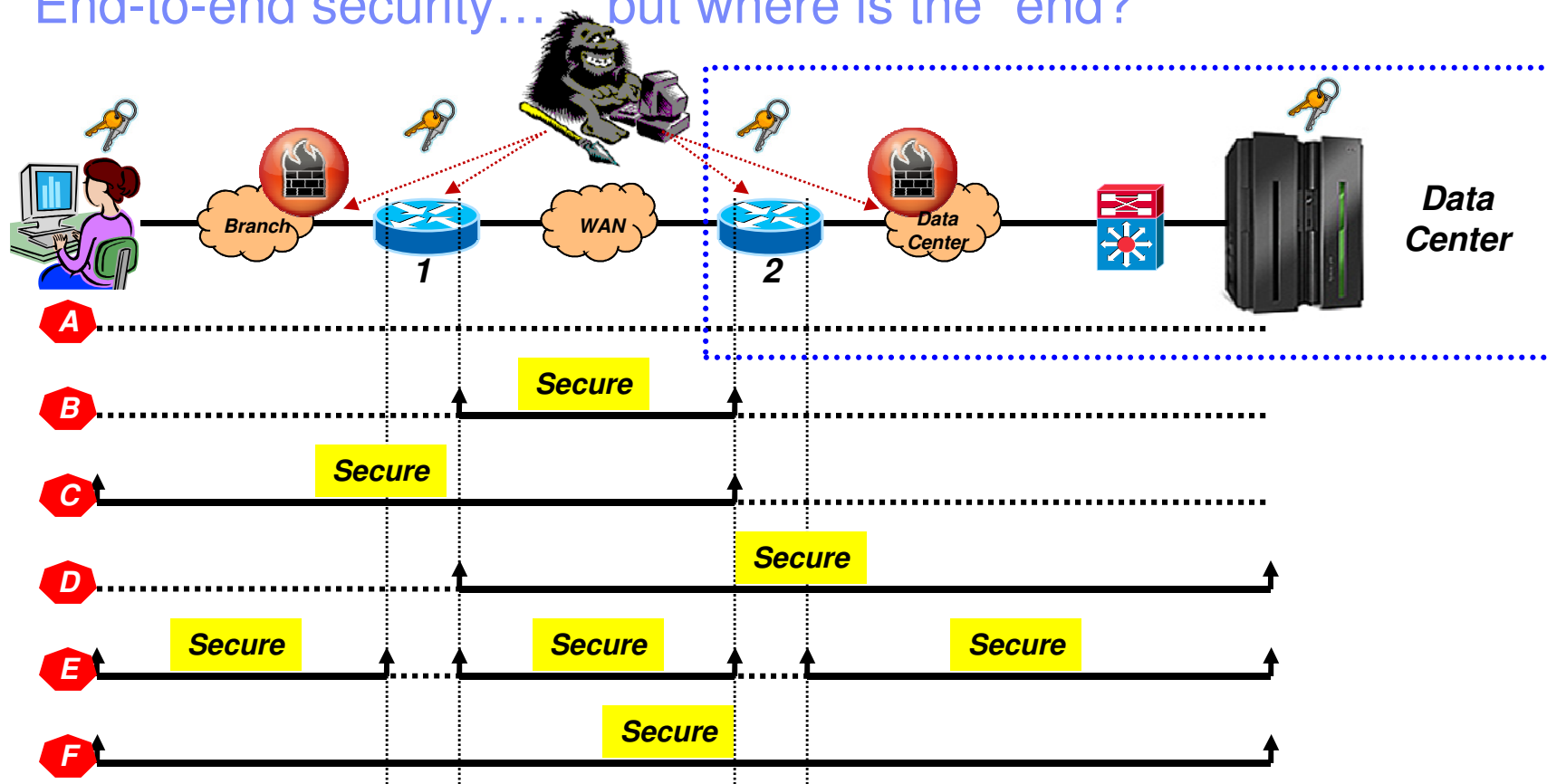


## Agenda

- What is end-to-end security?
- Network security protocols
  - The protocols
    - Transport Layer Security (TLS, also known as SSL)
    - IPsec
    - Secure Shell (SSH)
  - z/OS implementation options
  - Considerations for each option
- Protecting z/OS traffic
  - Common z/OS traffic types
    - TN3270
    - Enterprise Extender (EE)
    - FTP
    - SFTP (SSH file transfer)
    - Connect:Direct (aka NDM)
    - CSSMTP
    - CICS
    - MQ
    - IMS Connect
    - DB2
    - NJE
    - HTTP WebSphere
    - DNS
    - NFS, Portmapper
    - lpd
    - ICMP
  - Alternatives for protecting each



# End-to-end security... but where is the “end?”



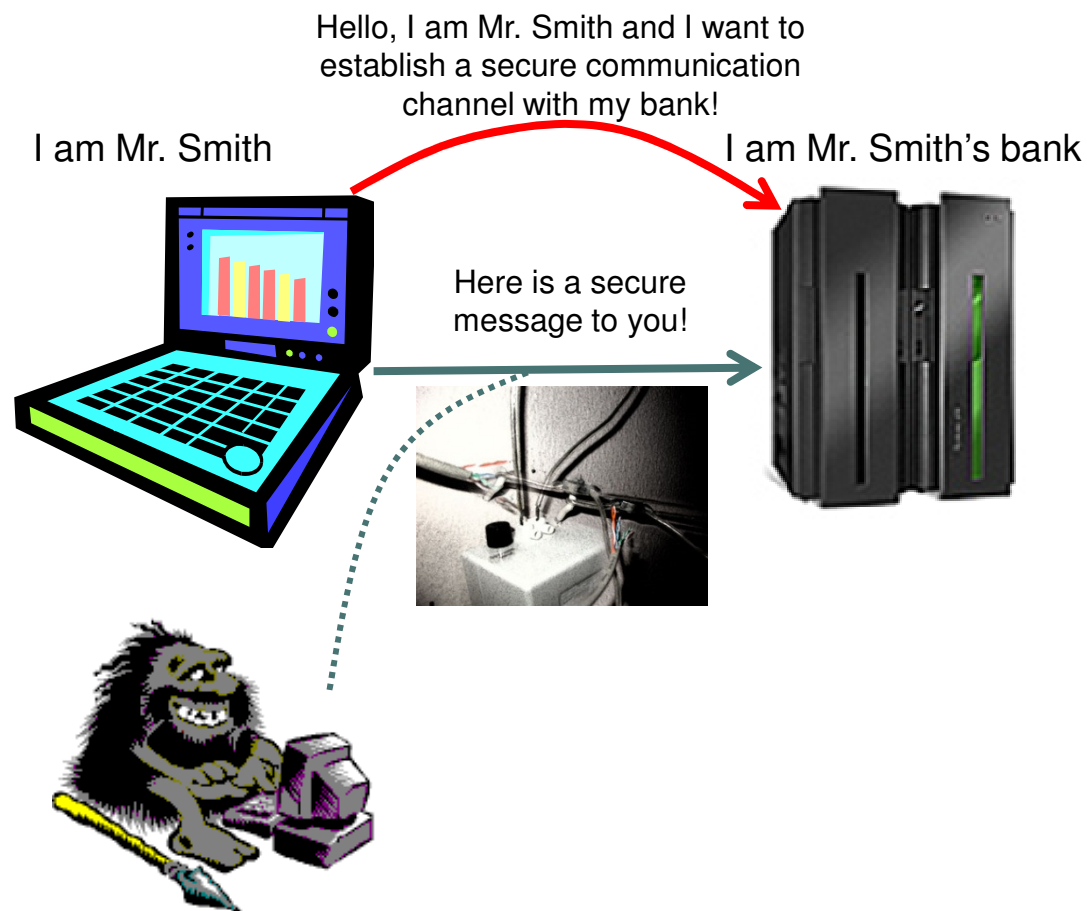
Secured segment	Partner authentication	Key management	Message authentication and integrity
A No security	None	None	None
B WAN only	Two WAN routers	On WAN routers	Between WAN routers
C Branch + WAN	Workstation – WAN router 2	On workstation and WAN router 2	Between workstation and WAN router 2
D WAN + data center	WAN router 1 – z/OS	On WAN router 1 and z/OS	Between WAN router 1 and z/OS
E Hop-by-hop security	Hop by hop	On all nodes, including WAN routers	Between all nodes, but not end to end (performance hit)
F End-to-end security	Workstation – z/OS	Workstation and z/OS	Between workstation and z/OS

## Agenda

- What is end-to-end security?
- Network security protocols
  - The protocols
    - Transport Layer Security (TLS, also known as SSL)
    - IPsec
    - Secure Shell (SSH)
  - z/OS implementation options
  - Considerations for each option
- Protecting z/OS traffic
  - Common z/OS traffic types
    - TN3270
    - Enterprise Extender (EE)
    - FTP
    - SFTP (SSH file transfer)
    - Connect:Direct (aka NDM)
    - CSSMTP
    - CICS
    - MQ
    - IMS Connect
    - DB2
    - NJE
    - HTTP WebSphere
    - DNS
    - NFS, Portmapper
    - lpd
    - ICMP
  - Alternatives for protecting each



## Protocols: The four big questions



Each of the secure network communications protocols address these four basic questions, but in slightly different ways

### Who are you? (Partner authentication)

- How do I know that you really are who you claim to be and not some imposter?
- How do you know that I am who I say I am?

### Where did this message come from? (Message authentication)

- How do I know the secure message actually came from the partner I authenticated a little earlier?
- How do I know it wasn't injected into the network by someone else?

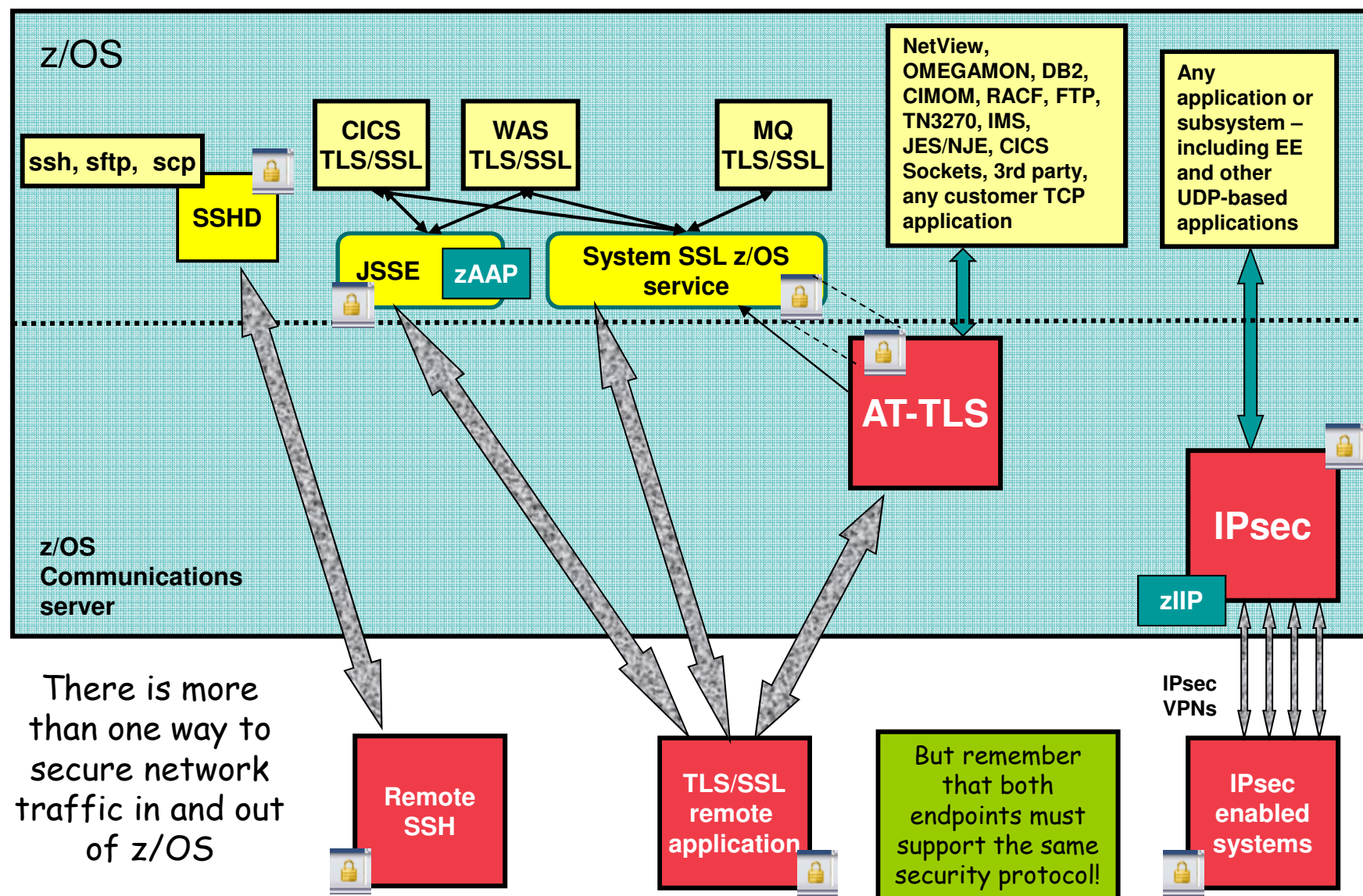
### Did anyone change this message? (Message integrity)

- How do I know that someone didn't modify the message since you sent it?
- How do I know that someone didn't duplicate an otherwise valid message?

### Can anyone else read this message? (Data Confidentiality)

- How do I know that no one could have intercepted this message and read it in an intelligible way when it was traversing the network?

# Protocols: z/OS Technology overview





# Protocols: What's encrypted and how are packet inspecting devices affected?

## What are “packet inspecting devices?”

- Many firewalls (especially those that are stateful)
- Intrusion detection devices (signature-based)
- Contents-based routers
- Protocol analyzers, tracers (sniffers), debuggers, etc.



*I am a packet inspecting device who wants to inspect those IP packets !*

**No encryption:**

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	50001	80	POST / HTTP/1.1 ... <soapenv:Envelope ...



**WSS encryption:**

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	50001	80	POST / HTTP/1.1 ... <soapenv:Envelope ... <xenc:EncryptedData ... ^%\$#\$#%#%#%



**SSH or TLS/SSL encryption:**

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	50002	443	@%\$#*&&^^!:"J)*GVM><



**IPSec encryption:**

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	>::"	*&hU\$\$\$\$	@%\$#dd*&&^s^!:"J)*bGVM> (*hgvvv<



**Your network engineer**

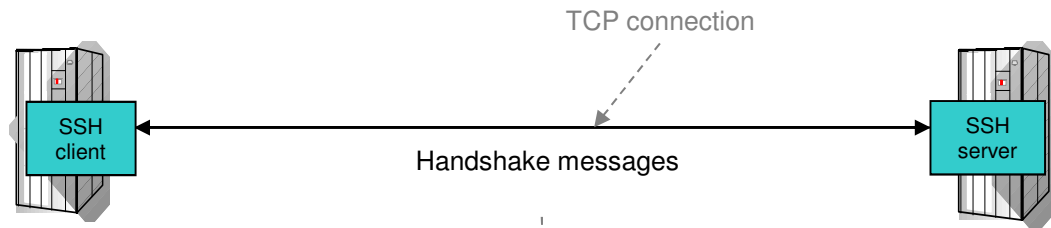
**Your security czar**

IP header encryption varies based on transport/tunnel mode, and AH/ESP protocol

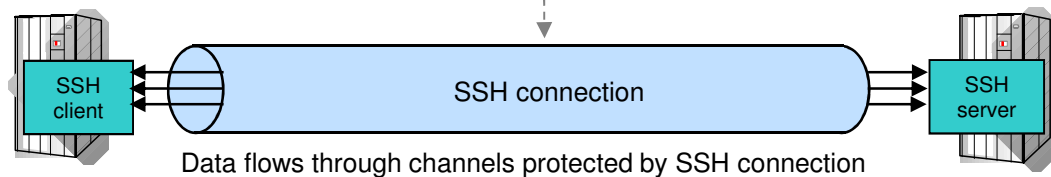
## Secure Shell (SSH)

- 1 SSH client program initiates a TCP connection to the SSH server. Once connected, a handshake occurs to authenticate the server and client to each other, negotiate cryptographic algorithms to use and exchange session keys.

Upon successful completion of the handshake, a secure connection exists between the client and the server.

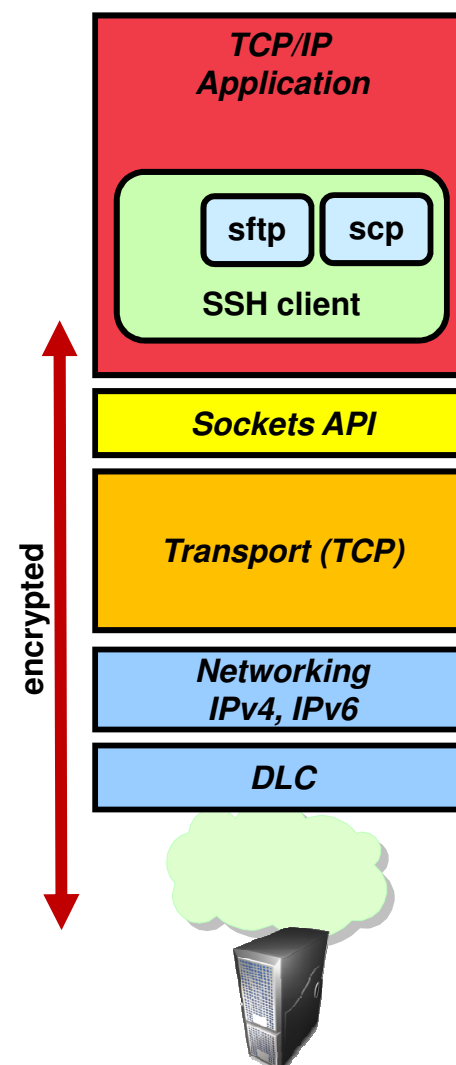


- 2 Data “channels” (e.g., login, sftp, scp, port forwarding etc.) are created and multiplexed under protection of the secure connection using symmetric encryption and message authentication negotiated during handshake




## SSH componentry

- **Application-layer**
  - SSH and its applications run completely at the application layer.
  - Even with port forwarding, traffic must pass through the SSH process in user space for encryption/decryption before it's forwarded to its ultimate destination
- **One SSH connection, multiple “channels”**
  - Each channel is a separate application stream (i.e., remote terminal, port forwarding, etc.)
  - However, in the most common case, command-line utilities (sftp, scp) invoke the SSH client such that a dedicated SSH connection is established for use by that command.



## SSH on z/OS

- In general, SSH on z/OS is used for remote access and file transfer between z/OS and \*IX systems.
- Because of this, we will focus mainly on TLS and IPsec
- Though available, TCP port forwarding is not heavily used on z/OS:
  - every packet must pass to the SSH application for encryption/decryption before being forwarded to its ultimate destination
  - not a very scalable solution
- IBM offers an OpenSSH implementation
  - V2R1 and earlier – part of IBM Ported Tools for z/OS
  - V2R2 – part of z/OS proper
  - supports CPACF (via ICSF), hardware random number generation and SAF keyrings for private keys
  - does not support MVS datasets or X.509 certificates
  -  in V2R2: FIPS 140-2 mode, Kerberos authentication and key exchange, zEnterprise Data Compression hardware support
- There are also some 3<sup>rd</sup> party SSH products that provide a some of the features that are not available in the z/OS OpenSSH implementation

## Transport Layer Security (and Secure Sockets Layer)

### Definitions:

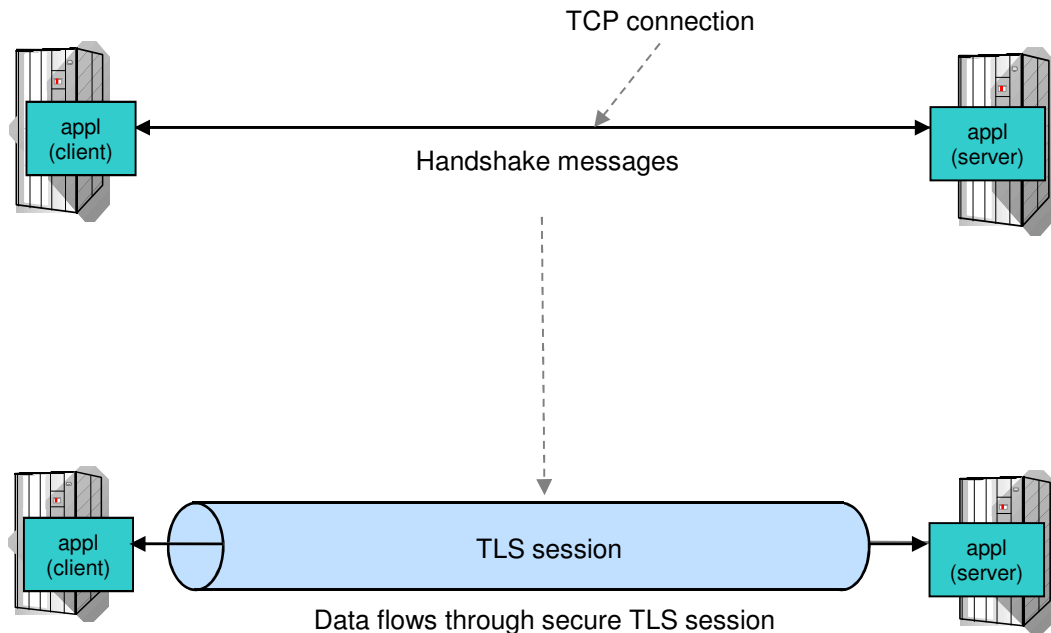
SSL = Secure Sockets Layer (an invention of Netscape). Final version was SSLv3.

TLS = Transport Layer Security (the IETF standardized version of SSL). TLS 1.0 is based on SSLv3.

**For our purposes, SSL and TLS are equivalent and one term implies the other**

- 1 Client application initiates TLS handshake which authenticates the server (and, optionally, client) and negotiates a cipher suite to be used to protect data

Upon successful completion of the handshake, a secure TLS session exists for the application partners

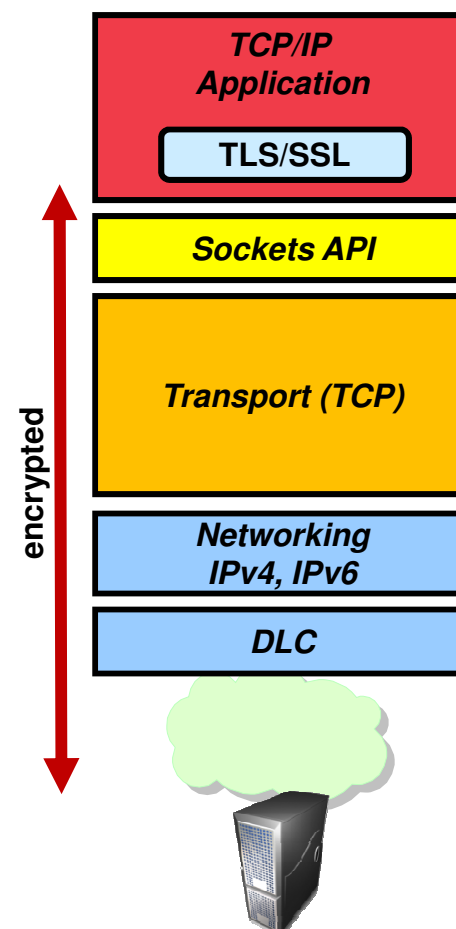


- 2 Data flows through secure session using symmetric encryption and message authentication negotiated during handshake

## Traditional TLS componentry

- **Application-layer**
  - The TCP application must call TLS functions to perform the handshake and later to protect each application message
  - In order to add protection to an existing application, that application must be modified (business logic, config, etc.)
  - On z/OS, System SSL and the Java JSSE provide the TLS functions
- **One connection, one TLS session\***
  - Each application maintains its own TLS sessions
  - Some implementations support “session reuse” to gain efficiency in the number of handshakes, but typically, a TLS session is associated with a single application connection

\* = in most cases!



## z/OS Application Transparent TLS

### ▪ IP stack-based TLS

- TLS process performed in TCP layer (via System SSL) without requiring any application change (transparent)
- AT-TLS policy specifies which TCP traffic is to be TLS protected based on a variety of criteria
  - Local address, port
  - z/OS userid, jobname
  - Remote address, port
  - Time, day, week, month
  - Connection direction

### ▪ Application transparency

- Can be fully transparent to application
- An optional API allows applications to inspect or control certain aspects of AT-TLS processing – “application-aware” and “application-controlled” AT-TLS, respectively

### ▪ Available to TCP applications

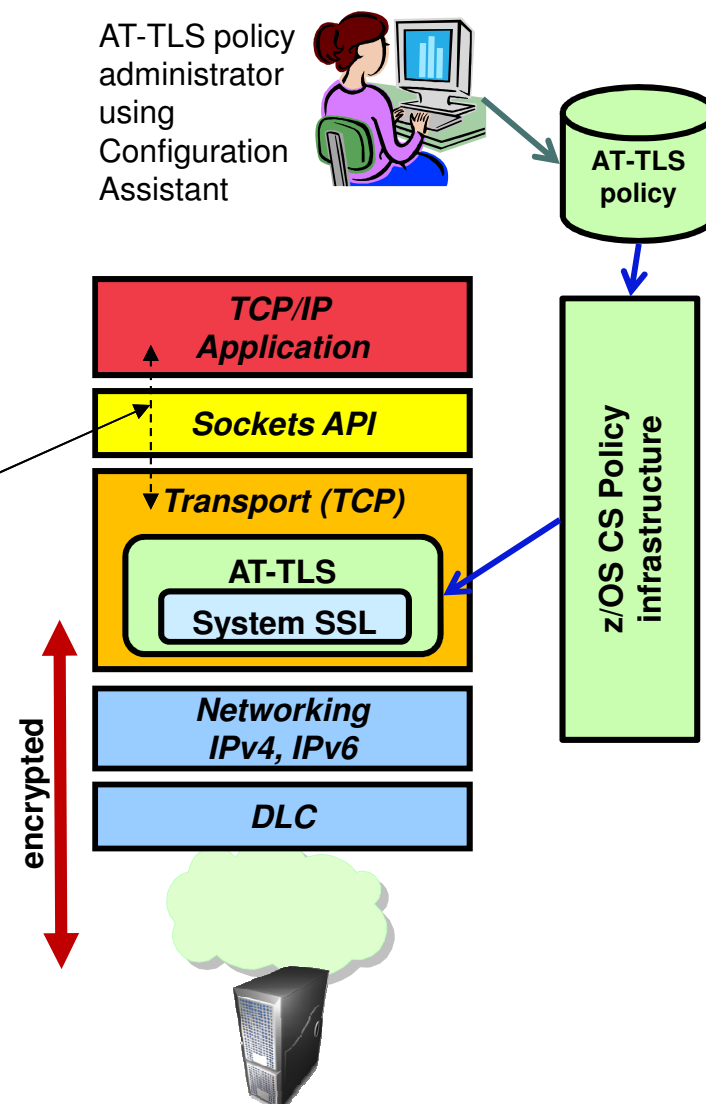
- Includes CICS Sockets
- Supports all programming languages except PASCAL

### ▪ Supports standard configurations

- z/OS as a client or as a server
- Server authentication (server identifies self to client)
- Client authentication (both ends identify selves to other)

### ▪ Uses System SSL for TLS protocol processing

- Remote endpoint sees an RFC-compliant implementation
- Interoperates with other compliant implementations



## Advantages of using AT-TLS

- **Reduce costs**

- Application development
  - Cost of System SSL integration
  - Cost of application's TLS-related configuration support
- Consistent TLS administration across z/OS applications
- Gain access to new features with little or no incremental development cost



- **Complete and up-to-date exploitation of System SSL features**

- AT-TLS makes the vast majority of System SSL features available to applications. For example,
  - V2R2 OCSP support and HTTP CRL retrieval
  - V2R1 TLSv1.2 support
- AT-TLS keeps up with System SSL enhancements – as new features are added, your applications can use them by changing AT-TLS policy, not code

- **Ongoing performance improvements**

Focus on efficiency in use of System SSL



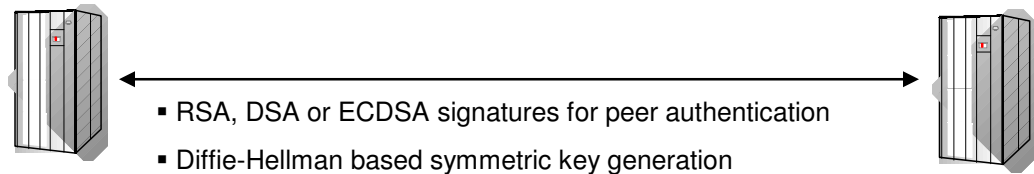
- **Great choice if you haven't already invested in System SSL integration**

Even if you have, consider the long-term cost of keeping up vs. short term cost of conversion

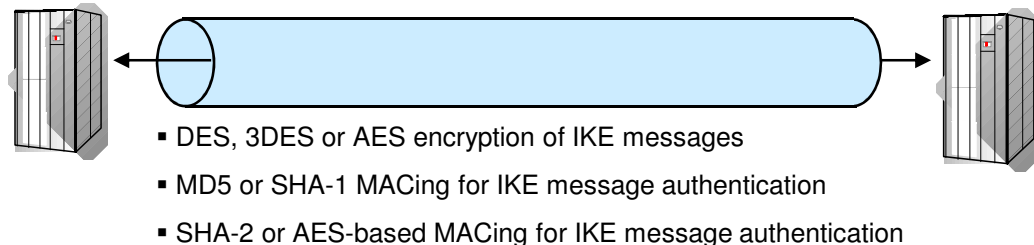


# IPSec using Internet Key Exchange (IKE)

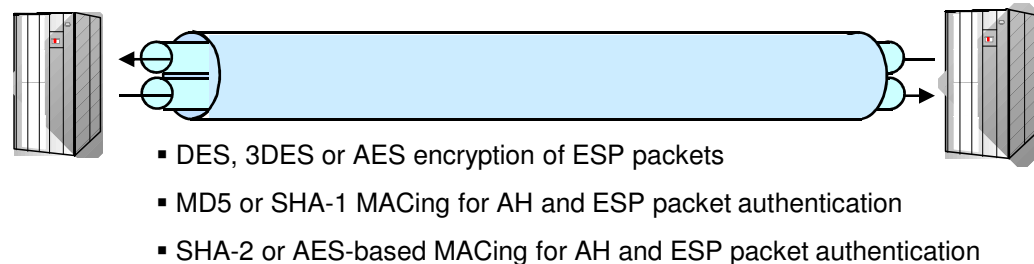
- 1 IKE peers negotiate an IKE ("phase 1") tunnel (one bidirectional SA) over an unprotected UDP socket.



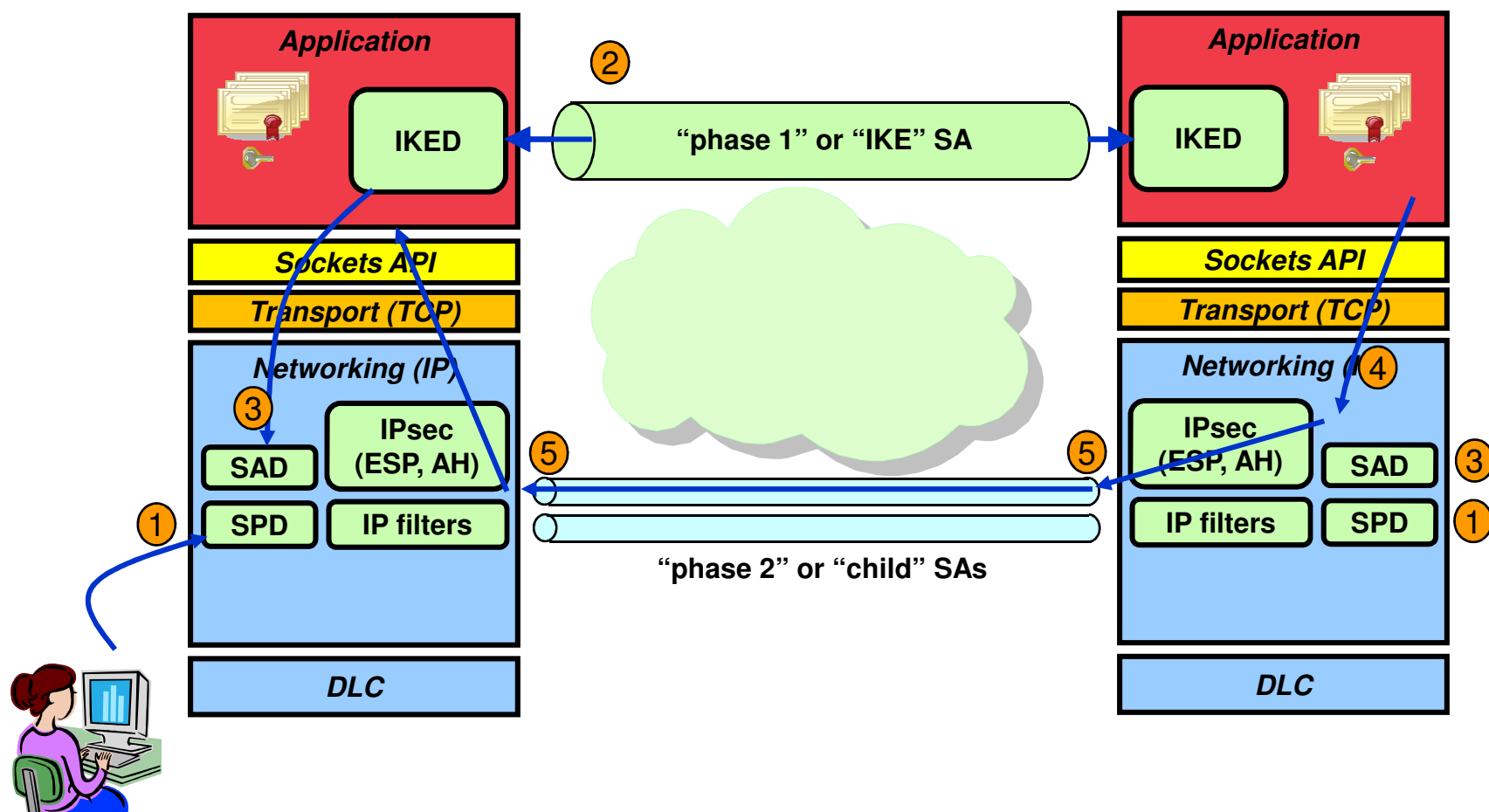
- 2 IKE peers negotiate IPSec ("phase 2") tunnel (two unidirectional SAs) under protection of the IKE tunnel



- 3 Data flows through IPSec tunnel using Authentication Header (AH) and/or Encapsulating Security Payload (ESP) protocol

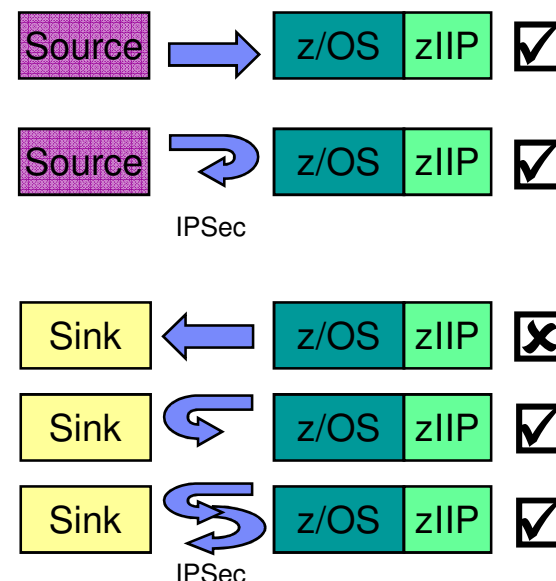


# IPsec components and basic interactions



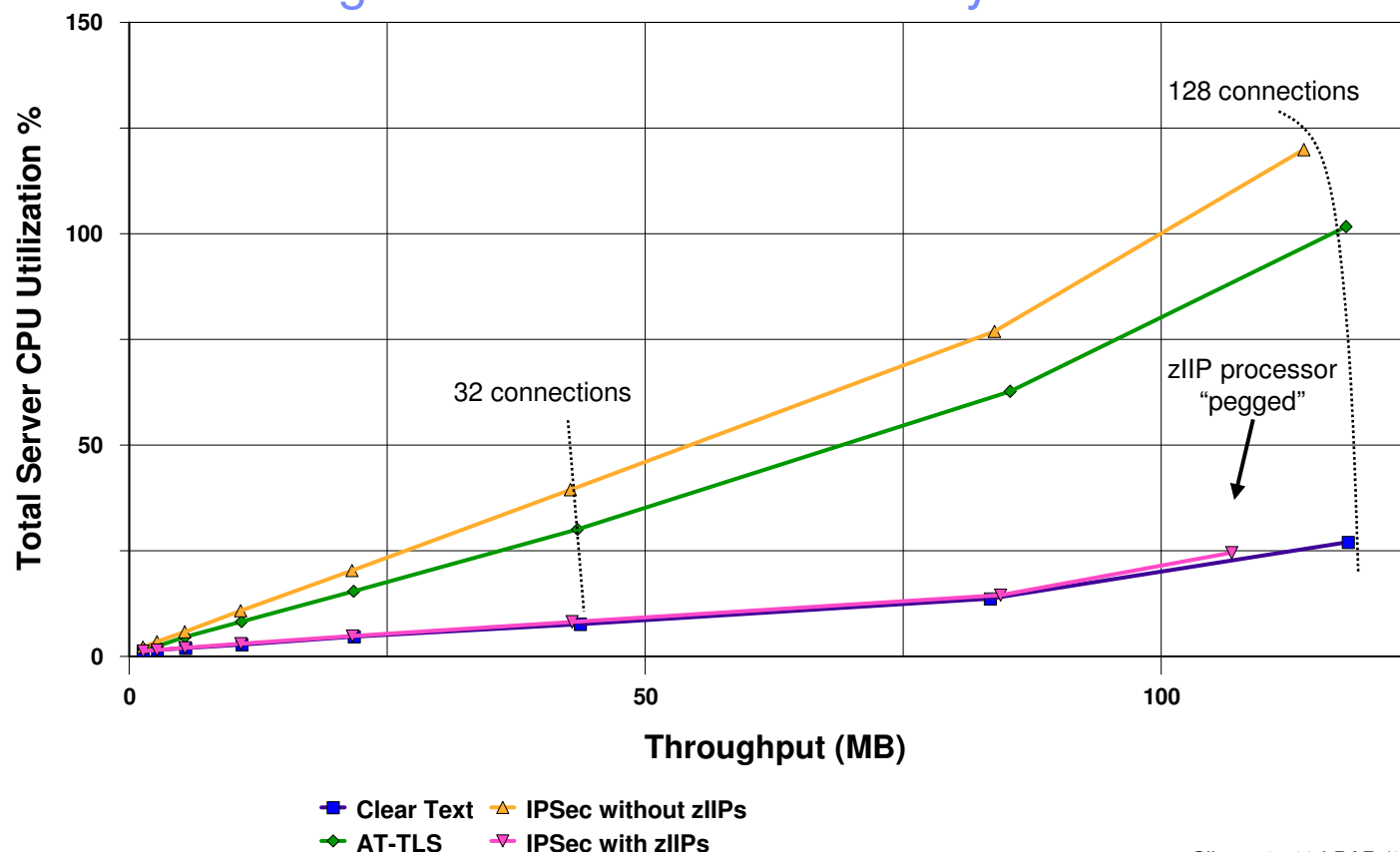
## IPSec use of System z Integrated Information Processor (zIIP)

- 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



## What about performance?

### FTP Server CPU usage with and without security

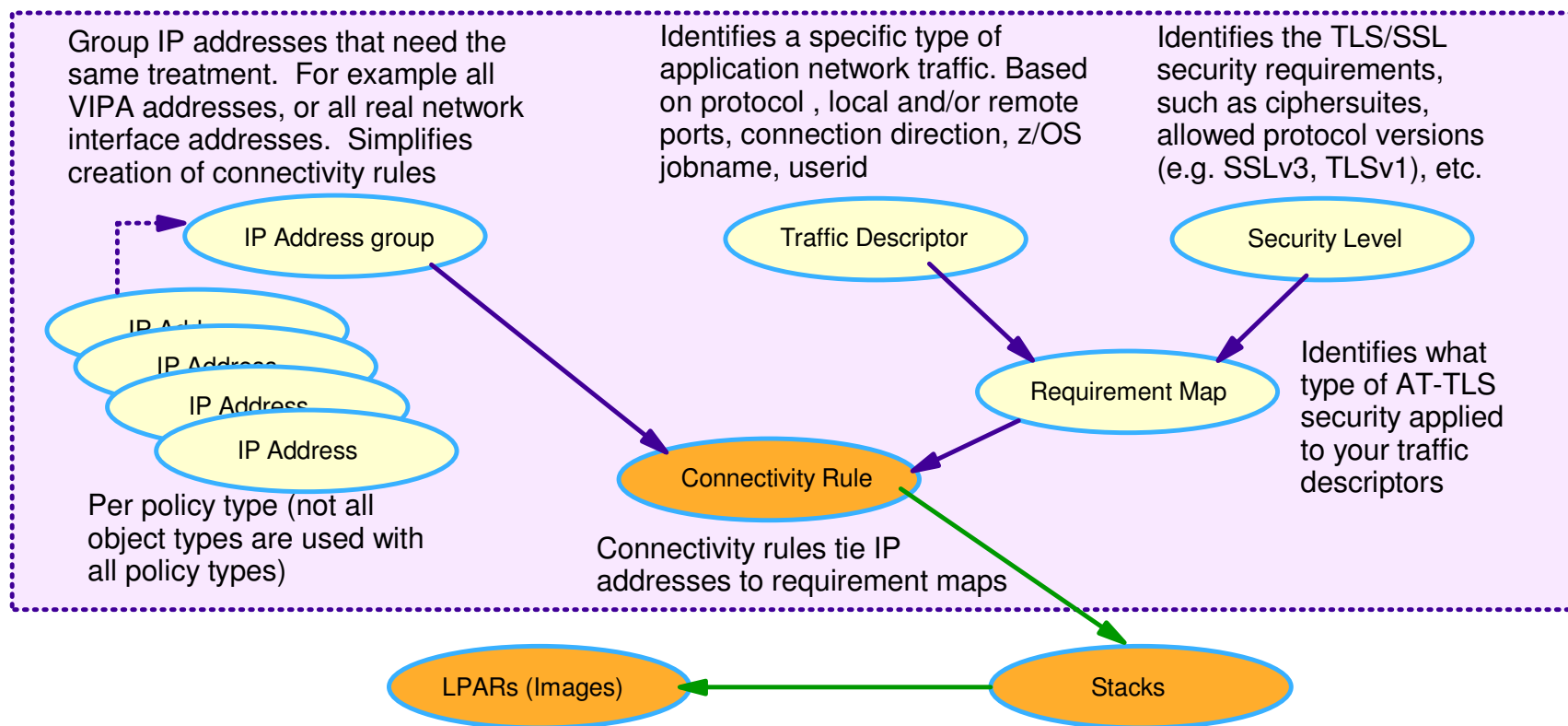


All measurements done with z/OS V1R12  
 Outbound Data (Gets) to an MVS client  
 3DES encryption with SHA authentication  
 From 1 to 128 parallel connections  
 Highest throughput numbers obtained with 0 think-time

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

Client: 1 z10 LPAR (3 dedicated CPs)  
 Server: 1 z10 LPAR (4 dedicated CPs)  
 Connectivity: OSA-E3 10 GbE  
 Encryption/Authentication: 3DES/SHA  
 Transaction: 1 byte / 2 MB  
 Target data sets: MVS data sets on 3390 DASD  
 Think time: 1500 ms  
 Number of connections: 1 to 128  
 Driver tool: AWM

## Configuration Assistant: Reusable object model



1. Create system image and TCP/IP stack image
2. Create one or more Requirement Maps to define desired security for common scenarios (e.g. intranet, branch office, business partner)
  - Create or reuse Security Levels to define security actions
  - Create or reuse Traffic descriptors to define application ports to secure
3. Create one or more Connectivity Rules between Data Endpoints (IP addresses) and associate with a configured Requirement Map

# Configuring IPsec and AT-TLS on z/OS: Configuration Assistant

IBM z/OS Management Facility

Welcome user1

IBM

- Welcome
- Notifications
- Workflows
- Configuration
  - Configuration Assistant
- Links
- Software
- z/OS Classic Interfaces
- z/OSMF Administration
- z/OSMF Settings

Refresh

Welcome x Configuration A... x

Configuration Assistant (Home) > AT-TLS

V2R2 Current Backing Store is Meyer

Select a TCP/IP technology to configure:

AT-TLS

AT-TLS

DMD

IDS

IPSec

NSS

PBR

QoS

TCP/IP Profile

Tools

Systems

Traffic Descriptors

Address Groups

Requirement Maps

Actions

System Group or Sysplex / System Im	Type	Status	Install Status	Release	Description
<input type="radio"/> Default	System Group	Complete			
<input type="radio"/> ZOS1	System Image	Complete		V2R2	
<input type="radio"/> STACK1	Stack	Complete	Never installed	V2R2	

Total: 3 Selected: 0

Home

Save

# Configuration Assistant: AT-TLS stack view

IBM z/OS Management Facility

Welcome user1

?

IBM

Welcome

Notifications

Workflows

Configuration

Configuration Assistant

Links

Software

z/OS Classic Interfaces

z/OSMF Administration

z/OSMF Settings

Refresh

Welcome x Configuration A... x

Configuration Assistant (Home) > AT-TLS > TCP/IP Stack

Connectivity Rules for System Image ZOS1, Stack STACK1

Actions

Move Up

Move Down

No filter applied

	Status	Rule Name	Application / Requirement Map	Key Ring
<input type="radio"/>	Disabled	Default_DB2-Requester	DB2-Requester	tlsKeyring
<input type="radio"/>	Disabled	Default_DB2-Server	DB2-Server	tlsKeyring
<input type="radio"/>	Disabled	Default_Central_PolicySvr	Centralized_Policy_Server	tlsKeyring
<input type="radio"/>	Disabled	Default_CICS	CICS	tlsKeyring
<input type="radio"/>	Disabled	Default_CIMServerInBound	CIMServerInBound	tlsKeyring
<input type="radio"/>	Disabled	Default_CIMServerOutBound	CIMServerOutBound	tlsKeyring
<input type="radio"/>	Disabled	Default_CSSMTP	CSSMTP	tlsKeyring
<input type="radio"/>	Disabled	Default_DefaultDCASConnect	DefaultDCASConnect	tlsKeyring
<input type="radio"/>	Disabled	Default_FTP-Client	FTP-Client	tlsKeyring
<input type="radio"/>	Disabled	Default_FTP-Server	FTP-Server	tlsKeyring
<input type="radio"/>	Disabled	Default_IMS-Connect	IMS-Connect	tlsKeyring
<input type="radio"/>	Disabled	Default_JES-Client	JES-Client	tlsKeyring
<input type="radio"/>	Enabled	Default_JES-Server	JES-Server	tlsKeyring

Total: 25 Selected: 0

Close

## Comparing TLS, IPsec\* and SSH protocols

Attribute	TLS (SSL)	IPsec	SSH-2
Traffic covered	TCP connections	All IP traffic (TCP, UDP, ICMP, etc.)	TCP connections
Provides true end-to-end protection	Yes	Yes	Yes
Provides network segment protection	No	Yes	No
Protection scope	Single TCP connection	Flexible (all traffic, single protocol, single or range of connections, etc.)	One or more TCP sessions
Requires application layer changes	Yes (except basic AT-TLS)	No	No
Endpoints and authentication	Application to application	IP node to IP node	Host to Host
Auth credentials	X.509 certificates	(dynamic tunnels only) X.509 certificates or pre-shared keys	public/private key, OpenSSH certificates
Auth frequency	Configurable	Configurable	Once at session startup
Session key refresh	Configurable based on time	Configurable based on data and time	Configurable based on data

\* - using IKE to establish IPsec tunnels dynamically



## Comparing TLS, IPsec and SSH implementations on z/OS

Attribute	TLS (SSL)	IPsec	SSH-2
Configuration	AT-TLS: Policy System SSL direct: per application JSSE: Java properties	Policy	OpenSSH configuration files as well as on command line invocation
Application transparency	AT-TLS: Yes* System SSL direct: No JSSE: No	Yes	Can be with port forwarding
SAF Keyrings	Yes	Yes	Yes (keys only)
Secure Keys (CryptoExpress)	Yes	Yes	No
FIPS 140-2 mode	Yes	Yes	Yes (new in V2R2)
Specialty engine support	AT-TLS and System SSL direct: No JSSE: Yes	Yes	No
System z hardware crypto	CPACF, CryptoExpress	CPACF, CryptoExpress	CPACF, CryptoExpress (RNG)

\* - can be as transparent as the application wants it to be

## Some considerations in selecting a security protocol (1 of 2)

1. Does corporate security policy dictate a specific technology or requirement?
  - ☐ Technology example: “All file transfers must be protected by TLS version x.x”
  - ☐ Requirement example: “All customer financial data must be encrypted, end-to-end, as it traverses the network”
2. What are the capabilities of the hosts and network equipment? Both endpoints of a secure connection must support the same...
  - ☐ Network security protocols and versions
  - ☐ Cryptographic algorithms and key lengths
3. How do your company’s firewall , deep packet inspection and network security policies fit in with the options?
  - ☐ Can you use the protocol within the firewall policies?
  - ☐ How will encryption affect your deep packet inspection devices (IDS/IPS, etc.)?
  - ☐ Are you using NATs? If so, look closely at the way you want to use IPsec
4. What is your communication partner willing to use?
  - ☐ Different enterprises have different standards and infrastructure (e.g., you may use IPsec, but they may not)
  - ☐ Many \*IX users won’t touch anything but SSH for file transfer
5. Are relative security infrastructures already in place?
  - ☐ Is there already an Public Key Infrastructure (PKI) in place?
  - ☐ Is TLS or IPSec already deployed anywhere in the network?
  - ☐ What method will you use to distribute public keys for SSH?



## Some considerations in selecting a security protocol (2 of 2)

6. Do the security protocols support the transport protocols?
  - ☐ TLS works great for TCP, but nothing else
  - ☐ IPSec protects any IP traffic, regardless of transport protocol
7. Is the application already enabled for network security?
  - ☐ TLS-enabled applications may offer features based on the TLS integration
  - ☐ If not, consider application-transparent technologies
8. What do you want to authenticate?
  - ☐ Application/user identity (TLS authentication is visible to the application, IPSec is not)
  - ☐ Host identity (IPSec authenticates at the host level)
9. How are the different technologies implemented on the platforms involved?
  - ☐ Performance optimization: Hardware crypto and other acceleration technologies
  - ☐ Exploitation of other platform-specific features (secure key, SAF, etc.)
10. There will be others



## Agenda

- What is end-to-end security?
- Network security protocols
  - The protocols
    - Transport Layer Security (TLS, also known as SSL)
    - IPsec
    - Secure Shell (SSH)
  - z/OS implementation options
  - Considerations for each option
- Protecting z/OS traffic
  - Common z/OS traffic types
 

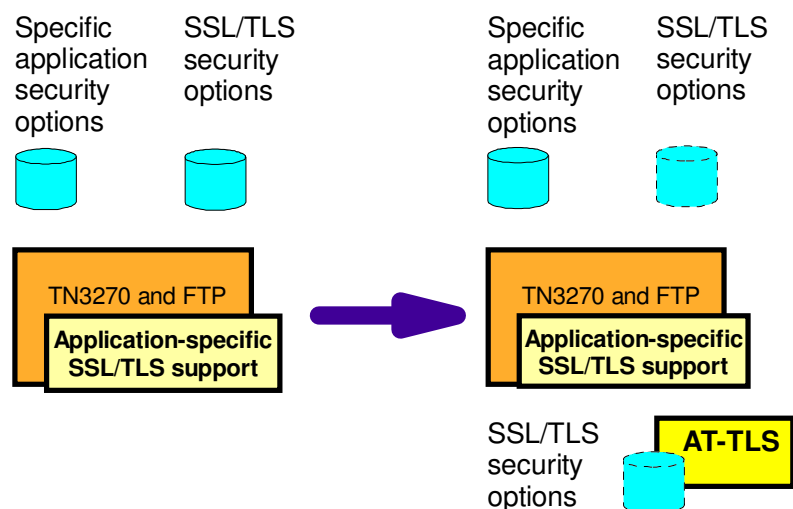
<ul style="list-style-type: none"> <li>• TN3270</li> <li>• Enterprise Extender (EE)</li> <li>• FTP</li> <li>• SFTP (SSH file transfer)</li> <li>• Connect:Direct (aka NDM)</li> </ul>	<ul style="list-style-type: none"> <li>• CSSMTP</li> <li>• CICS</li> <li>• MQ</li> <li>• IMS Connect</li> <li>• DB2</li> <li>• NJE</li> </ul>	<ul style="list-style-type: none"> <li>• HTTP WebSphere</li> <li>• DNS</li> <li>• NFS, Portmapper</li> <li>• lpd</li> <li>• ICMP</li> </ul>
---	---	---
  - Alternatives for protecting each



## TN3270

- Tight integration with AT-TLS
  - TN3270 is an AT-TLS-controlling or -aware application (depending on setting of CONNTYPE parameter)
  - Provides access to the latest features of System SSL
  - Tested with tens/hundreds of thousands of concurrent connections
  - CONNTYPE supports a few modes in how TLS protection is applied:
    - SECURE – use TLS immediately at client connect time
    - NEGOTSECURE – use a TN3270 negotiation with client to see if client is willing to use TLS protection. If not, the connection is closed.
    - ANY – Try the TLS handshake – if the client doesn't support it, allow the cleartext connection
    - BASIC – no security, just cleartext
    - NONE – don't allow any client connections
  - There's also a deprecated direct integration with System SSL - no longer being updated and is not recommended
- IPsec is also an option
  - In this case, TN3270 “thinks” it's running in cleartext mode
  - Traffic is secure, but you won't have visibility to client certificates through usual TN-related displays
  - Provides the benefit of zIIP offload

## Configuring TN3270 to use AT-TLS protection



- To specify whether TN3270 should use AT-TLS instead of the TN3270 server's own system SSL calls, use the following TN3270 configuration parameter:
  - TTLSPORT
    - CONNTYPE retains its current meaning for a TTLSPORT
- When TTLSPORT is used for a TN3270 server port:
  - The TN3270 server becomes an AT-TLS controlling and AT-TLS aware application
  - All the TN3270-specific security options will continue to impact how TN3270 operates
  - Any TN3270 server TLS/SSL security options will be ignored.
    - Matching AT-TLS policies need to be defined before enabling AT-TLS support for the TN3270 server

- **TN3270-specific security options:**

- SECUREPORT (use of this option will indicate to TN3270 that it is to use its existing application-specific TLS/SSL support, and not AT-TLS for the specified port number)
- CONNTYPE
  - SECURE
  - NEGOTSECURE
  - ANY
  - BASIC
- EXPRESSLOGON
- RESTRICTAPPL CERTAUTH

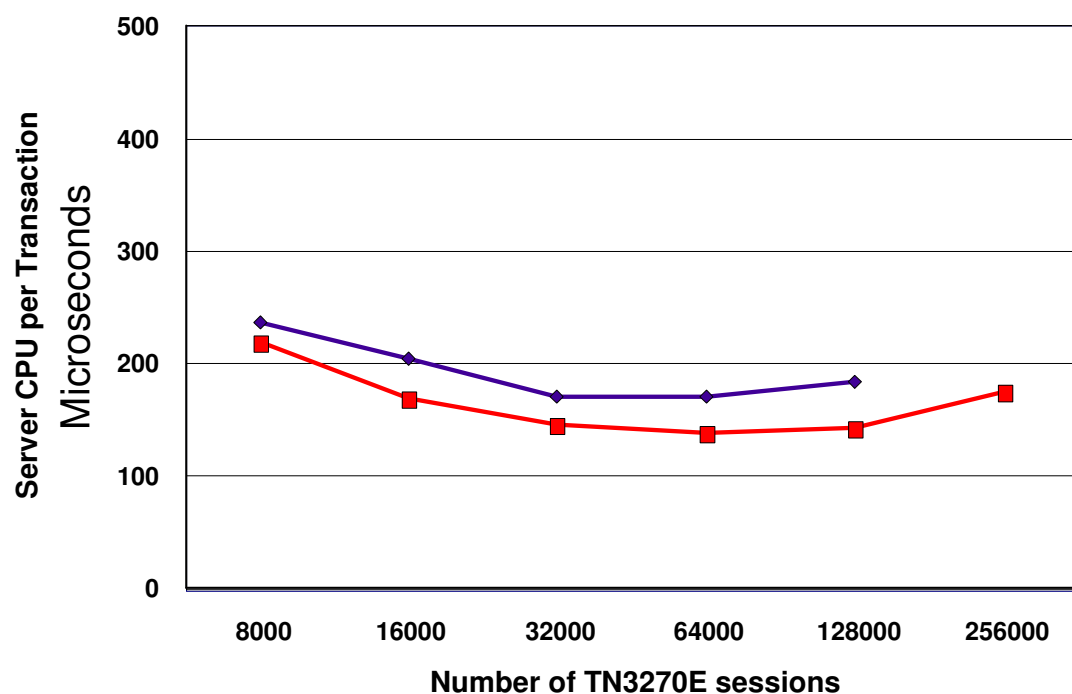
- **TN3270 TLS/SSL security options**

- KEYRING
- CRLLDAPSERVER
- CLIENTAUTH
  - SSLCERT
  - SAFCERT
- ENCRYPTION
- SSLTIMEOUT
- SSLV2/SSLNOV2

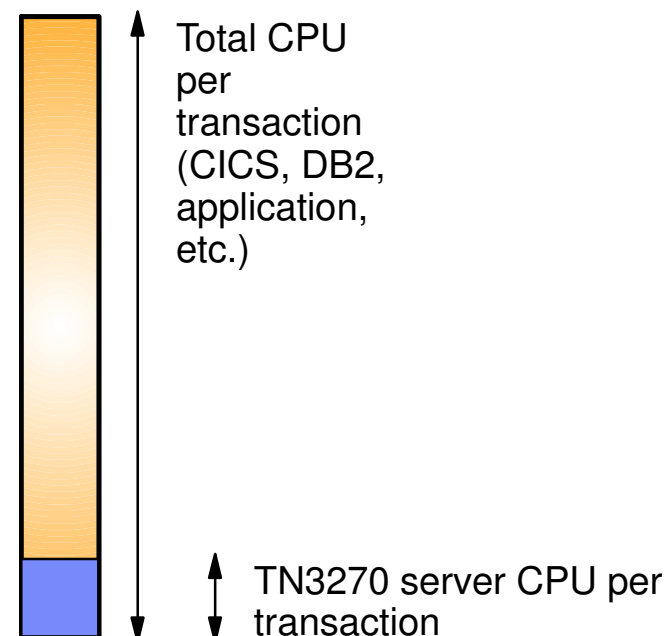
## z/OS V1R9 Communications Server TN3270E AT-TLS Security Performance (TN3270 Server, Steady State, CPU per Transaction)

### IPv4 TN3270E Server CPU Scalability

z/OS CS V1R9 AT-TLS vs. Clear Text  
2 TN servers with 1 Port each



TN3270 server and application server: 4-way 2094-S38



- The TN3270 server CPU portion of the total CPU usage per transaction is very small.
- If you increase the TN3270 server CPU usage with 20%, the total transaction percentage CPU increase is significantly lower.

**3DES and SHA**

**100 bytes in/800 bytes out**

**Think time 30 seconds**

## Detailed AT-TLS netstat report for AT-TLS secured TN3270 connection

### NETSTAT TTLS CO 000016AF DETAIL TCP TCPCS

```

ConnID: 000016AF
  JobName:      TN3270A
  LocalSocket:  ::ffff:9.42.105.45..2025
  RemoteSocket: ::ffff:9.65.253.59..1266
  SecLevel:     TLS Version 1
  Cipher:       0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
  CertUserID:   N/A
  MapType:      Primary
  FIPS140:      Off
TTLRule: ABC_TN3270-Server_2025~3
  Priority:     253
  LocalAddr:    All
  LocalPort:    2025
  RemoteAddr:   All
  RemotePortFrom: 1024      RemotePortTo: 65535
  Direction:    Inbound
  TTLGrpAction: gAct1
    GroupID:      00000001
    TTLEnabled:    On
    Envfile:       /etc/attls.env
    CtraceClearText: Off
    Trace:         6
    SyslogFacility: Daemon
    SecondaryMap:   Off
    FIPS140:       Off

```

```

TTLSEnvAction: eAct1
  EnvironmentUserInstance: 0
  HandshakeRole:           Server
  Keyring:                 TLSRING
  SSLV2:                   Off
  SSLV3:                   On
  TLSV1:                   On
  TLSV1.1:                 On
  ResetCipherTimer:        0
  ApplicationControlled:    Off
  HandshakeTimeout:        10
  TruncatedHMAC:           Off
  ClientMaxSSLFragment:     Off
  ServerMaxSSLFragment:     Off
  ClientHandshakeSNI:       Off
  ServerHandshakeSNI:       Off
  ClientAuthType:          Required
  CertValidationMode:       Any
TTLSConnAction: cAct3~TN3270_2025
  HandshakeRole:           Server
  V3CipherSuites:          2F TLS_RSA_WITH_AES_128_CBC_SHA
                           0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
  CtraceClearText:         Off
  Trace:                   6
  ApplicationControlled:    On
  SecondaryMap:             Off

```



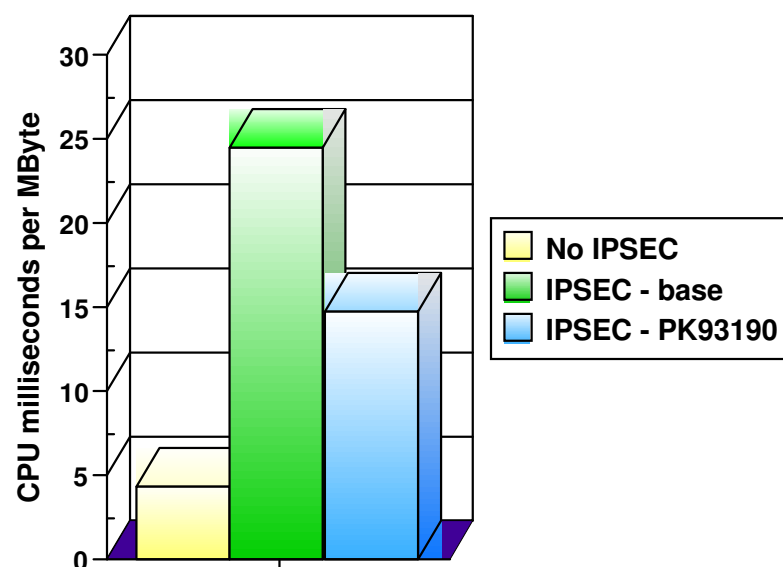
## Enterprise Extender

- Since EE uses UDP/IP, TLS/SSL is not a viable option
- IPsec is used heavily and very successfully in the industry for protecting EE traffic
- As with all applications, IPsec is completely transparent to EE traffic
- Configuration can be very narrow – down to the specific EE ports if so desired
- EE over IPsec performance has seen dramatic improvements in past releases. Examples:
  - Improved performance for EE over IPsec
    - The “bursty” nature of HPR traffic can cause significant performance degradation when it is carried over IPsec tunnels.  
Smaller bursts frequently get encrypted and sent before larger bursts. This results in out-of-order segments that are dropped at the other end of the IPsec tunnel, forcing retransmits.
    - V1R11 breaks large bursts into batches of smaller bursts
    - PTFed back to V1R10 – APAR PK93190
  - Improved support for EE over IPsec when IPsec processing offloaded to a zIIP
    - Support for offloading outbound EE over IPsec traffic to a zIIP processor. Previously only inbound traffic was processed on the zIIP.

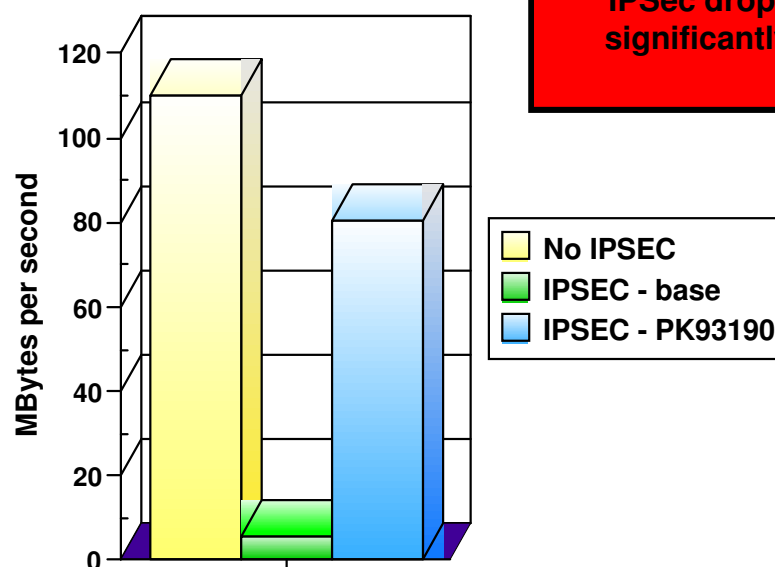
## EE over IPsec performance (z/OS V1R10 and V1R11)

### 1 bulk session retrieving 20MB

General CPU Consumption



Raw Throughput



Test did not include the benefits of zIIP. With zIIP, the amount of general CPU resources used for EE over IPsec drops significantly.

#### ■ With PK93190

- Networking CPU is reduce from a 466% increase to a 242% increase compared to non-secure
- Throughput rate reduction improves from a 95% decrease to a 27% decrease compared to non-secure

Note: The performance measurements discussed on this page were taken z/OS V1R11 Communications Server and were collected using a dedicated system environment. The results obtained in other configurations or operating system environments may vary.

## File transfer protocols... let's clear up some common confusion...



### ▪ **FTP (File Transfer Protocol):**

RFC959  
FTP

- Also referred to as RFC959 FTP or “normal” FTP
- The FTP protocol we all know and have used for years.
- Has been extended numerous times since RFC 959 was issued in 1985
- An RFC959 FTP client talks to an RFC959 FTP server - not an sftp server
- What the z/OS CS FTP client and server have supported through many years

### ▪ **sftp (Secure Shell File Transfer Protocol):**

Secure  
Shell  
FTP

- A sub-protocol of SSH (Secure Shell)
- Supported on z/OS by "IBM Ported tools for z/OS" and at least two ISV products
- Has nothing to do with RFC959 FTP - incompatible protocols
- An sftp client talks to an sftp server - not an RFC959 FTP server

### ▪ **FTPS (File Transfer Protocol Secure):**

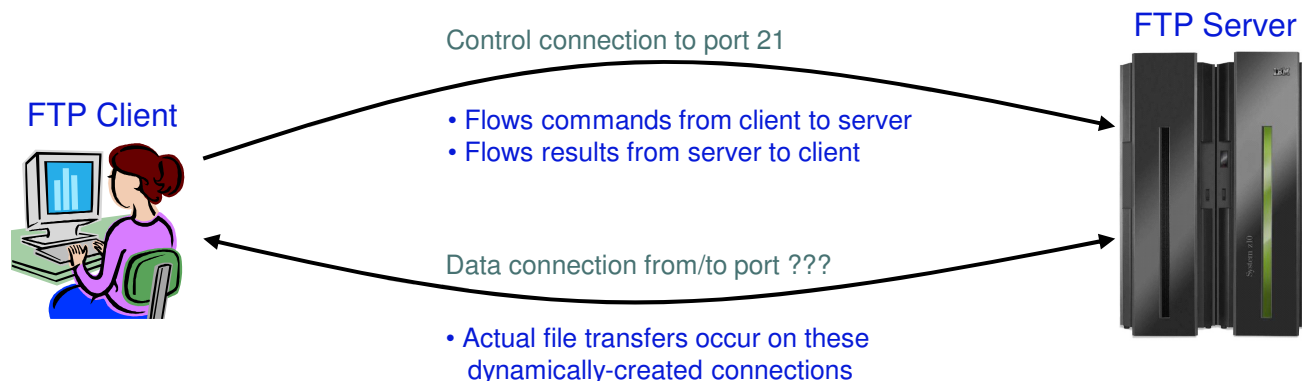
RFC4217  
FTP

- Also referred to as FTP – SSL, RFC4217 FTP, FTP AUTH-TLS, FTP AUTH-SSL
- RFC959 FTP but extended with full network security (authentication, data integrity, and data privacy) using a standard security mechanism, such as Kerberos or TLS/SSL
  - TLS/SSL protection specified by RFC4217 "Securing FTP with TLS"
- Both control connection and data connection can be secured
  - No user IDs or password flowing in the clear

## A basic FTP protocol overview

- TCP-based protocol (default is port 21)
- Client initiates session (a “control connection”) to FTP daemon on server
- FTP daemon spawns a new FTP server process to handle the client’s session
- Client sends commands to server and receives replies on control connection. For example:

LIST – list contents of current directory	USER – identify userid under which to log in
RETR – retrieve a file from the server	PASS – specify login password
STOR – store a file on the server	TYPE – indicate data transfer type (binary/text)
CWD – change working directory	...and lots more!
- RETR, STOR and other commands cause a separate “data connection” to be established on a different set of ports between the server process and the client:
  - Active mode: server initiates data connection to the client
  - Passive mode: client initiates data connection to server



## Securing selected z/OS file transfer technologies: A comparison

	<b>FTP</b> With no security RFC959	<b>FTPS</b> FTP w. TLS/SSL RFC959 + RFC4217	<b>FTP</b> FTP w. IPSec Any RFC level	<b>SFTP</b> As implemented by IBM Ported Tools
User ID and password protection	No	Yes	Yes	Yes
Data protection (the file being transferred)	No	Yes	Yes	Yes
z/OS UNIX file support	Yes	Yes	Yes	Yes
z/OS MVS data set support	Yes	Yes	Yes	No (but add-on products do exist*)
Use of System z hardware encryption technologies	n/a	Yes	Yes	Yes (CPACF & random number generation)
Partner authentication via locally stored copies of public keys	n/a	No	Yes (pre-shared key)	Yes
Partner authentication via X509 certificates	n/a	Yes	Yes	No
Use of SAF key rings and/or ICSF	n/a	Yes	Yes	Yes
FIPS 140-2 mode	n/a	Yes (z/OS V1R11)	Yes (z/OS V1R12)	No
Mutual authentication supported	n/a	Yes	Yes (at an IP address level)	Yes

\* MVS data set support example: Dovetailed Technologies' Co:Z SFTP

## Connect:Direct (formerly known as Network Data Mover (NDM))

- TCP-based application infrastructure
- Very good built-in TLS support
  - Direct integration with System SSL
  - Offloads TLS operations to zIIP
  - Also offloads compression operations to zIIP
- AT-TLS will also work but you don't get the zIIP exploitation
- IPsec is also an option – we know of at least one customer using IPsec to protect their Connect:Direct traffic. Again, Connect:Direct thinks it's running in cleartext mode

## TLS/SSL options for z/OS applications

	JSSE	Native System SSL	AT/TLS	AT/TLS – aware / controlled
TN3270		(Yes)	Yes	Yes
FTP (server and client)		(Yes)	Yes	Yes
DB2 DRDA			Yes	Yes
NJE over IP			Yes	Yes
MQ		Yes	(Yes)	
CSSMTP			Yes	Yes
CICS Sockets			Yes	Yes
CICS TS	(Yes)	Yes	(Yes)	
IMS Connect			Yes	Yes
WebSphere Application Server and Java appls	Yes	Yes	(Yes)	
All TCP applications			Yes*	

\* Need to evaluate each, but for applications that are not SSL-enabled, AT-TLS is a good choice

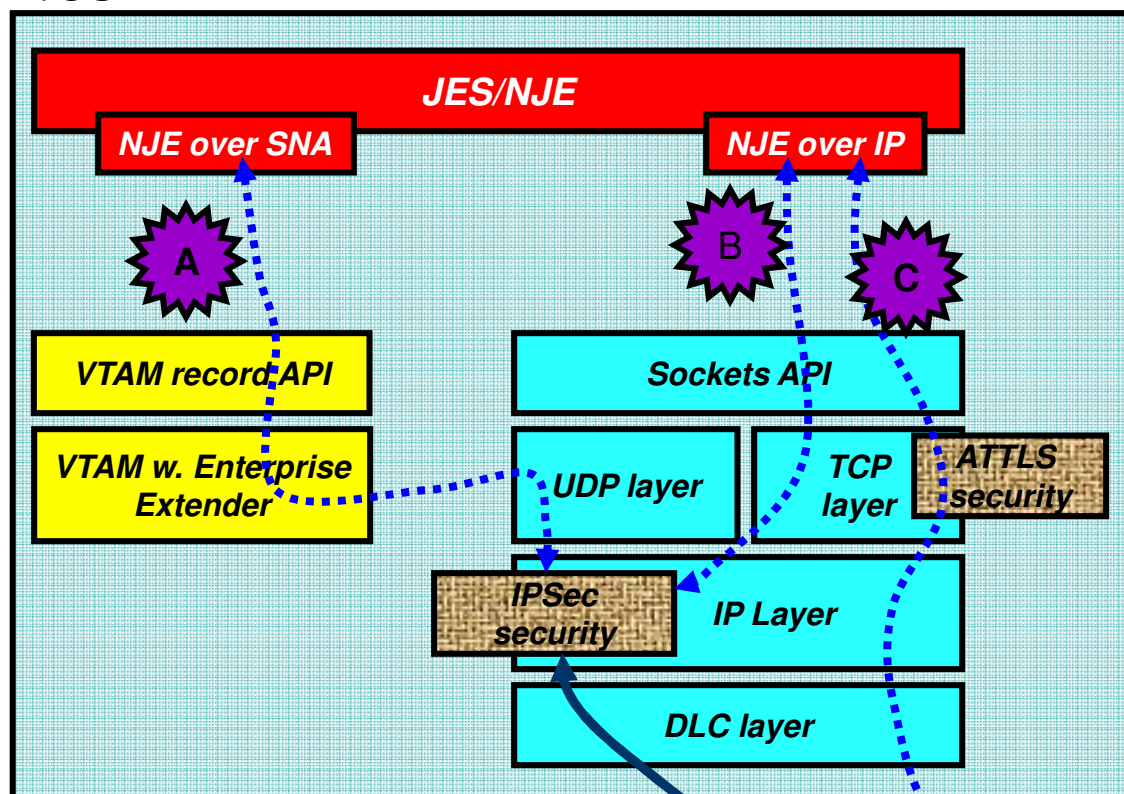
## Other common z/OS traffic – good IPsec candidates

- Internet Control Message Protocol (ICMP and ICMPv6)
  - These are their own IP protocols
  - Used for things like neighbor discovery, path validation, etc.
- UDP-based protocols:
  - Enterprise Extender (as previously discussed)
  - Domain Name System (DNS)
  - Network File System (NFS), Remote Procedure Call (RPC) and Portmapper can all run over UDP
  - Simple Network Management Protocol (SNMP)
- TCP-based protocols whose implementations typically do not support TLS/SSL
  - sendmail / SMTP
  - Line Print Daemon (LPD)
  - ...and others

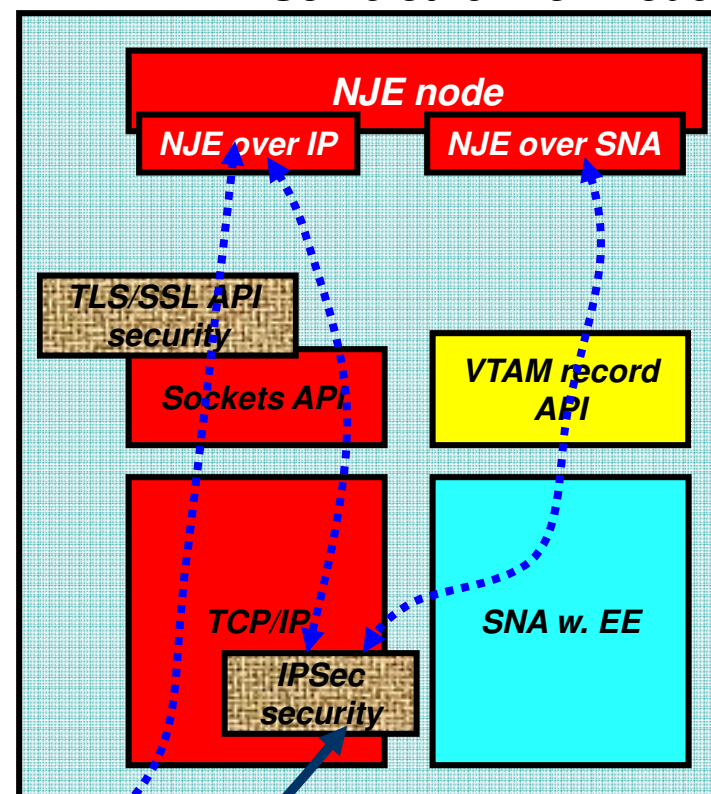


# Securing NJE traffic over an IP network

z/OS

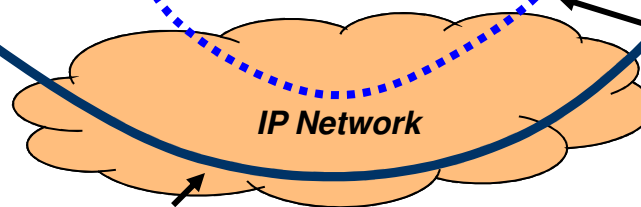


Some other NJE node



NJE traffic protected using IPSec/VPN

NJE traffic protected using TLS/SSL



IPSec/VPN secure tunnel

## Choosing networking security technology for NJE traffic

	NJE/SNA using EE and IPSec	NJE/IP using IPSec	NJE/IP using TLS/SSL
JESPARM changes	None	None (if already using NJE/IP)	Define secure port
Performance (throughput)	Acceptable	Good	Best
Can security overhead be offloaded to zIIP on z/OS?	Yes	Yes	No
Firewall traversal sensitivity	High (UDP and IPSec)	Medium (IPSec)	Low
Non-z/OS node support requirements	EE and IPSec	IPSec	TLS/SSL
z/OS enablement	Policy definition (IPSec policy)	Policy definition (IPSec policy)	Policy definition (ATTLS policy)
Non-z/OS enablement	EE and IPSec setup	IPSec setup	TLS/SSL setup
Addressing FIPS 140-2 compliance	Yes	Yes	Yes
End-point authentication by security protocol	IP address	IP address	User ID associated with JES started task and remote process
General ease of implementation and use	Medium	Medium	Simplest

## What tools are available for identifying traffic and endpoints?





- IP filters
  - Only identifies the traffic – not the application endpoints
  - Turn on a “permit all” rule with logging enabled. Note that this will generate a LOT of syslogd traffic and output!
  - Analyze the log records to identify unique IP traffic (this can be quite a bit of work – IBM services team can help here)
- SMF records
  - Type 119, subtype 1 – TCP Connection Initiation
    - Useful for identifying TCP application endpoints
    - Written any time a TCP connection is opened
    - Contains jobname of the local application using the connection
  - Type 119, subtype 73 – IPsec IKE Tunnel Activation
    - Useful for identifying remote nodes that are IPsec tunnel endpoints
    - Contains IKE identity of peer
    - Does not link to a local jobname
  - Type 119, subtype 75 – IPsec Dynamic Tunnel Activation
    - Useful for identifying remote ports that are IPsec tunnel endpoints
    - Contains local/remote IP addresses, ports and IP protocol
    - Does not link to a local jobname

## Summary

- z/OS supports three robust end-to-end security protocols
  - Transport Layer Security (TLS, also known as SSL)
  - IPsec
  - Secure Shell (SSH)
- Each has its place and is suited for different types of traffic
- Which protocol you select to protect each type of application traffic will depend on a number of different factors
- In most cases, you'll have a choice of protocols for any given application type



## For more information

URL	Content
<a href="http://www.twitter.com/IBM_Commserver">http://www.twitter.com/IBM_Commserver</a>	IBM Communications Server on 
<a href="http://www.facebook.com/IBMCommserver">http://www.facebook.com/IBMCommserver</a>	IBM Communications Server on 
<a href="http://www.youtube.com/user/zOSCommServer">http://www.youtube.com/user/zOSCommServer</a>	IBM Communications Server on 
<a href="http://tinyurl.com/zoscsblog">http://tinyurl.com/zoscsblog</a>	IBM Communications Server blog 
<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/ccl/">http://www.ibm.com/software/network/ccl/</a>	IBM Communication Controller for Linux on System z
<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.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



**Thank you!**