

z/OS Network Security Roadmap

Alfred B Christensen – alfredch@us.ibm.com
IBM Raleigh, NC

Thursday 5-Aug-2010 - 9:30 AM to 10:30 AM



SHARE in Boston

z/OS Network Security Roadmap

Session number:	
Date and time:	Thursday 5-Aug-2010 - 9:30 AM - 10:30 AM
Location:	Room 302 (Hynes Convention Center)
Program:	Communications Infrastructure
Project:	Communications Server
Track:	Network Security, Network Security Management and Network Support and Management
Classification:	Technical
Speaker:	Alfred B Christensen, IBM
Abstract:	<p>This session will discuss how to address the increasing number of security compliance requirements IT organizations are facing. The session will introduce how z/OS CS can assist in protecting the operating system platform from malicious attacks through the IP network and how to secure the data that is transmitted over the network to/from IP applications running on the z/OS platform. Topics such as IPSec (secure Virtual Private Networks), IPSec on zIIP processors, IP filtering, Intrusion Detection and prevention (IDS), securing application access through authentication and encryption using SSL/TLS (including transparent SSL/TLS processing by the z/OS Communications Server) - will all be introduced.</p>

Trademarks, notices, and disclaimers

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

Refer to www.ibm.com/legal/us for further legal information.

Agenda



- ☐ Introduction
- ☐ z/OS Communications Server security roles and objectives
- ☐ System and resource protection
- ☐ Protecting data in the network
- ☐ Securing selected application workloads
- ☐ Summary



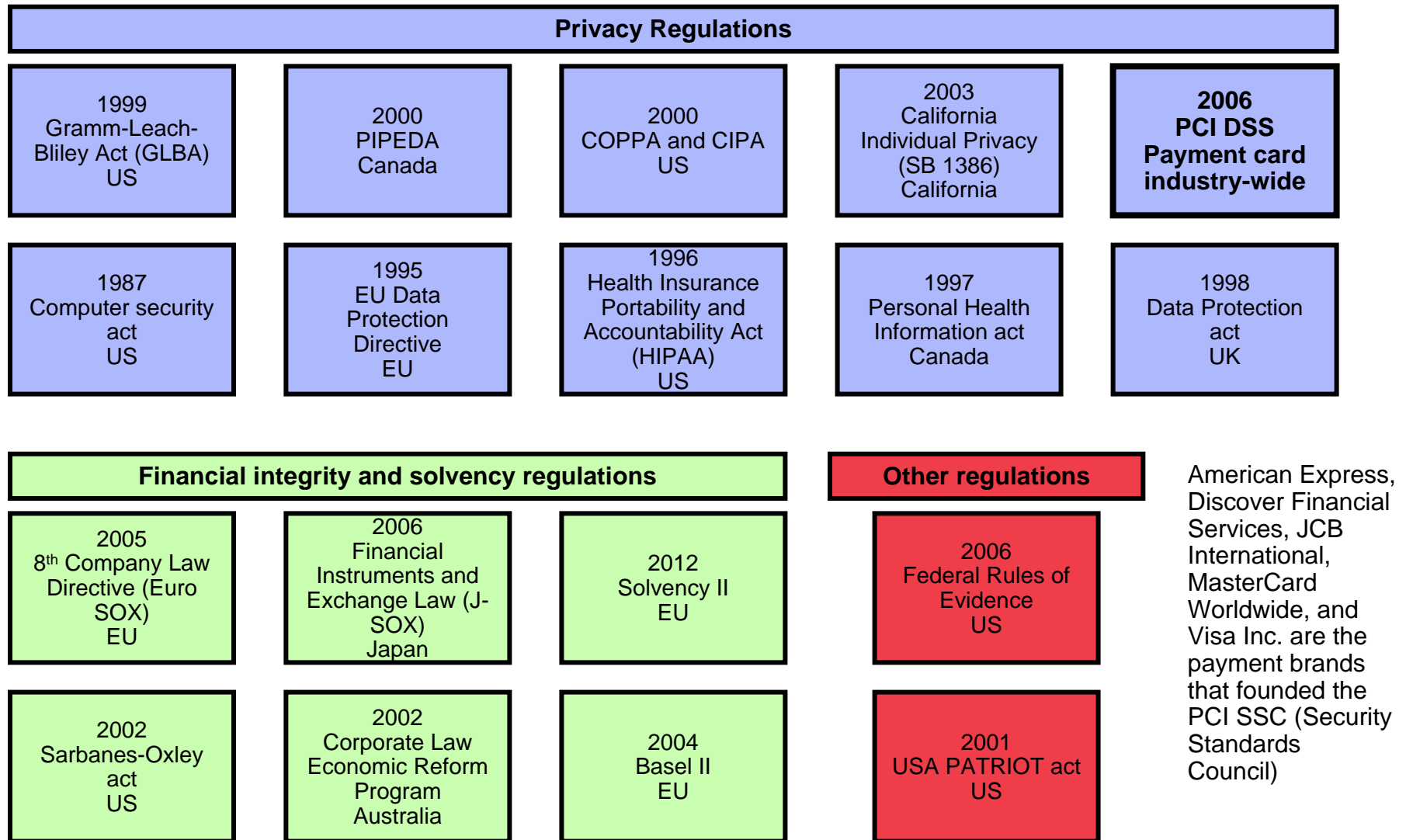
Disclaimer: All statements regarding IBM future direction or intent, including current product plans, are subject to change or withdrawal without notice and represent goals and objectives only. All information is provided for informational purposes only, on an “as is” basis, without warranty of any kind.

z/OS Network Security Roadmap

Introduction



It is not “just” the Payment Card Industry Data Security Standard (PCI DSS) your company needs to be concerned with!



Payment Card Industry Data Security Standard (PCI-DSS) – overview

Goals	Nbr.	PCI DSS Requirement
Build and maintain a secure network	1	Install and maintain a firewall and router configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5	Use and regularly update anti-virus software programs
	6	Develop and maintain secure systems and applications
Implement strong access control measures	7	Restrict access to cardholder data by business need-to-know
	8	Assign a unique ID to each person with computer access
	9	Restrict physical access to cardholder data
Regularly monitor and test networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an information security policy	12	Maintain a policy that addresses information security for employees and contractors

Source: PCI Quick Reference Guide – Understanding the Payment Card Industry Data Security Standard version 1.2
<https://www.pcisecuritystandards.org/index.shtml>

There are other standards related to security and/or IPv6, you also may need to consider:

- 1. FIPS Federal Information Processing Standards (primarily FIPS 140 standards)**
- 2. NIST National Institute of Standards and Technology (primarily IPv6)**
- 3. DoD Department of Defense (Primarily IPv6)**

Compliance with PCI-DSS

PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to organizations that store, process, or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. The council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the council, American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

Storing cardholder data	Data Element	Storage permitted	Protection required	PCI DSS Req. 3.4	PAN must be rendered unreadable anywhere it is stored.
Cardholder data	Primary account number (PAN)	Yes	Yes	Yes	
	Cardholder name ¹	Yes	Yes ¹	No	
	Service code ¹	Yes	Yes ¹	No	
	Expiration date ¹	Yes	Yes ¹	No	
Sensitive authentication data ²	Full magnetic stripe data ³	No	N/A	N/A	
	CAV2/CVC2/CVV2/CID	No	N/A	N/A	
	PIN/PIN block	No	N/A	N/A	

Notes:

1. These data elements must be protected if stored in conjunction with the PAN
2. Sensitive authentication data must not be stored after authorization (even if encrypted)
3. Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere

Source: PCI Quick Reference Guide – Understanding the Payment Card Industry Data Security Standard version 1.2

A few selected details from the PCI DSS requirements

- Firewalls between network security zones
- Description of groups, roles, and responsibilities for logical management of network components
- Do not allow internal addresses to pass from the internal network into the DMZ
- Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ
- Implement state-full inspection
- Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access
- Use strong cryptography and security protocols such as SSL/TLS or IPSec to safeguard sensitive cardholder data during transmission over open, public networks (the Internet, wireless networks, GSM networks, etc.)
- Never send unencrypted PANs by end-user messaging technologies (for example email, instant messaging, chat)
- Implement automated audit trails for all system components – including all actions taken by any individual with root or administrative privileges, and access to audit trails
- Secure audit trails so they cannot be altered
- Retain audit trail history for at least one year
- Run internal and external network vulnerability scans at least quarterly
- Plus many more – of which some that are not terribly relevant to a z/OS environment, such as anti-virus software.

Source: PCI Quick Reference Guide – Understanding the Payment Card Industry Data Security Standard - Requirements and Security Assessment Procedures – version 1.2.1 July 2009

Payment Card Industry Compliance for Large Computing Systems:
[http://www.atsec.com/downloads/white-papers/PCI_Compliance_for_LCS_\(version_1.0.1\).pdf](http://www.atsec.com/downloads/white-papers/PCI_Compliance_for_LCS_(version_1.0.1).pdf)

z/OS Network Security Roadmap

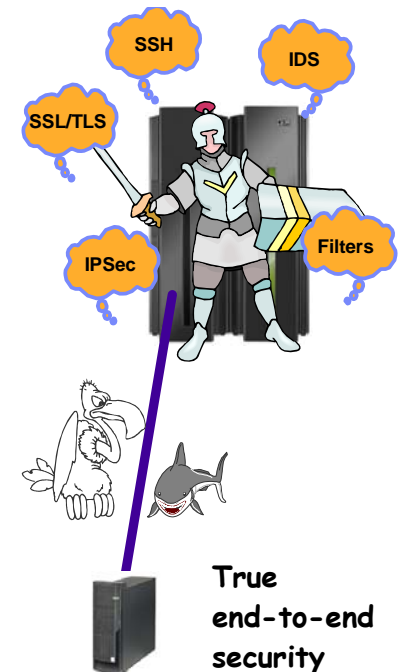
z/OS Communications Server security roles and objectives



z/OS general networking security objectives

- **Protect data and other resources on the system**
 - **System availability**
 - Protect the system against unwanted access, denial of service attacks, and other unwanted intrusion attempts from the network
 - **Identification and authentication**
 - Verify identity of users
 - **Access control**
 - Protect data and other system resources from unauthorized access
- **Protect data in the network using cryptographic security protocols**
 - **Data End Point Authentication**
 - Verify who the secure end point claims to be
 - **Data Origin Authentication**
 - Verify that data was originated by claimed sender
 - **Message Integrity**
 - Verify contents were unchanged in transit
 - **Data Privacy**
 - Conceal clear-text using encryption

**Self protection:
z/OS itself is the last line
of defense in a hostile
network environment!**

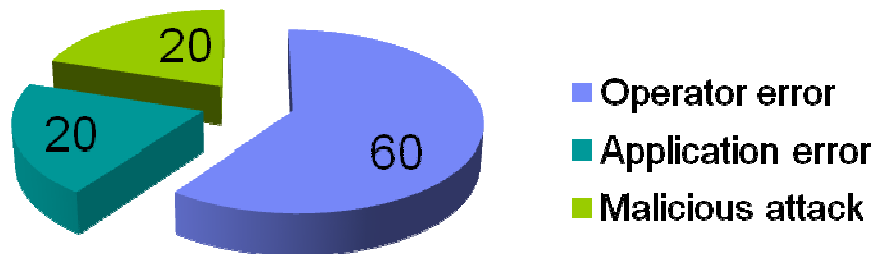


z/OS CS security focus areas:

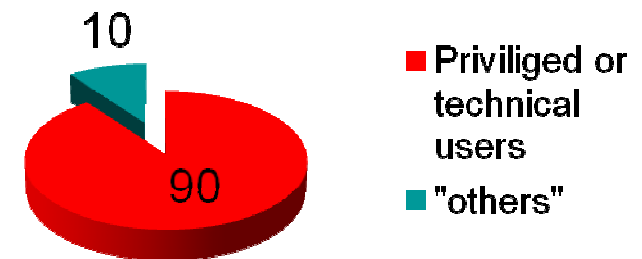
- Self protection
- Provide secure access to both TCP/IP and SNA applications
- Provide options for true end-to-end security and self-protection
- Exploit the strengths of System z hardware and software

Perimeter security alone is generally not enough: some statistics to consider

Categories of security-related incidents



Who is the “villain”?




Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005/6; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.

The enemy is most often ourself:

- **90% of insider incidents are caused by privileged or technical users**
- **Most are inadvertent violations of:**
 - Change management process
 - Acceptable use policy
 - Account management process
- **Others are deliberate, due to:**
 - Revenge (84%)
 - “Negative events” (92%)
- **Regardless, too costly to ignore:**
 - Internal attacks cost 6% of gross annual revenue or 9 dollars per employee per day

A suggested set of steps to provide some base protection of your z/OS system in a network environment

- 
- 1. Blocking unwanted traffic from entering deep into your z/OS system**
 - IP packet filtering on z/OS - potentially in combination with firewall solutions on network routers
 - 2. Protecting against malicious or accidental attacks on your system or your legitimate services**
 - In-context host intrusion detection services on z/OS
 - Potentially in combination with signature-based intrusion detection by IBM Internet Security System solutions (IBM ISS)
 - Potentially in combination with IBM DataPower as a secure gateway for Web Services workload
 - 3. Securing an audit trail for z/OS UNIX system services**
 - Syslogd setup, protection, and administration
 - 4. Controlling user access to TCP/IP resources on the system**
 - SAF SERVAUTH class protection using protection of SERVAUTH resources
 - 5. Protect end-to-end confidentiality and integrity of data in the network**
 - Numerous network security protocols and technologies to choose from:
 - IPSec VPN
 - SSL/TLS (including AT-TLS)
 - Kerberos
 - SSH
 - other application-specific security protocols (Secure DNS, SNMPv3 security, Web Services Security, etc.)

z/OS Communications Server security technology overview

Protect the system

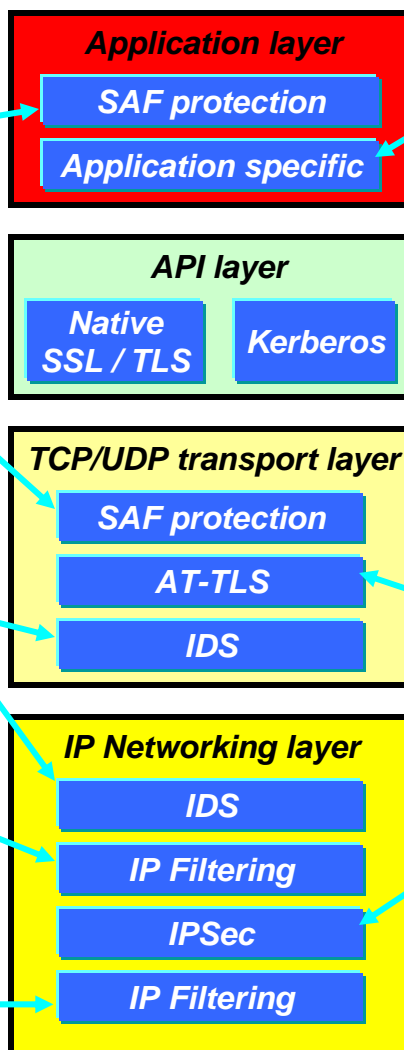
z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources.

The SAF SERVAUTH class is used to prevent unauthorized user access to TCP/IP resources (stack, ports, networks).

Intrusion detection services protect against attacks of various types on the system's legitimate (open) services. IDS protection is provided at both the IP and transport layers.

IP filtering blocks out all IP traffic that this systems doesn't specifically permit.

IP filtering is also used to control which traffic must use IPsec.



Protect data in the network

Examples of application protocols with built-in security extensions are SNMPv3, DNS, and OSPF.

SSH (not part of z/OS CS) provides an umbrella of secure applications (secure shell access, secure file transfer, etc.)

Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

AT-TLS is a TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to applications.

IPSec resides at the networking layer and is transparent to upper-layer protocols, including both transport layer protocol and application protocol.



z/OS Network Security Roadmap

System and resource protection



Step 1: blocking unnecessary/unwanted IP traffic at the front door through IP filtering

■ IP filtering at the z/OS IP Layer

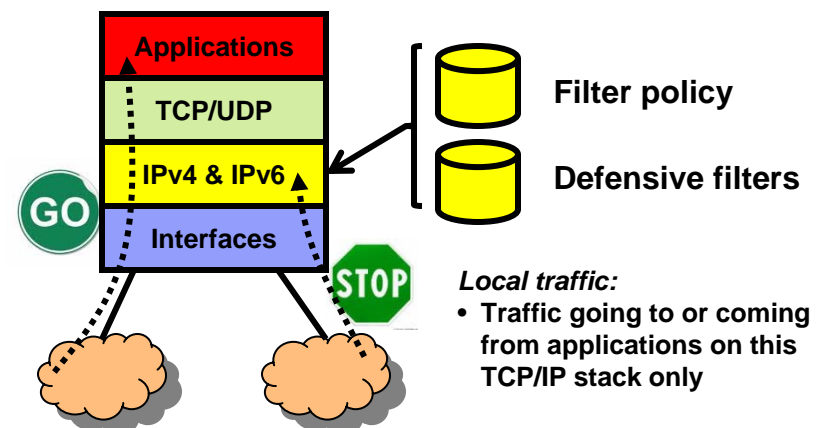
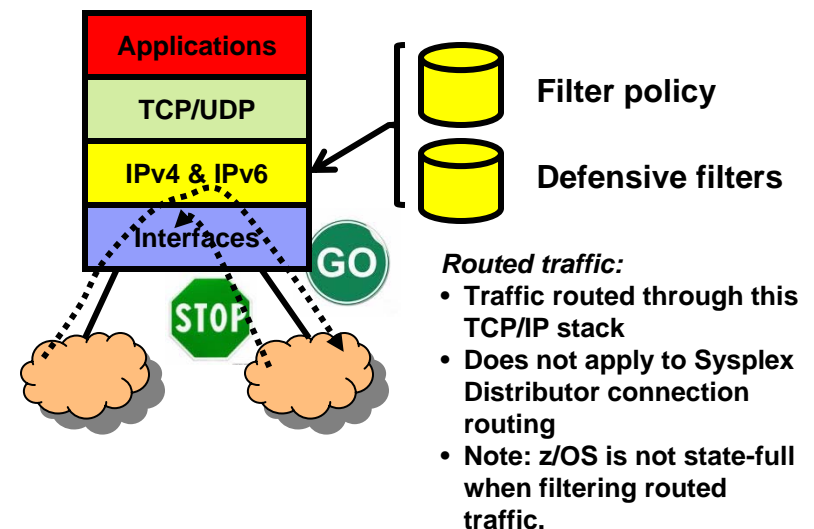
- Filter rules (sometimes referred to as access rules) defined to deny or permit IP packets based on:
 - IPv4 or IPv6 source/destination address
 - Protocol (TCP, TCP with ACK, UDP, ICMP, ?)
 - Source/destination Port
 - Direction of flow
 - Local or routed traffic
 - Time
 - Network interface
- Used to control
 - Traffic being routed
 - Access at destination host (local)
- When IP filtering is active, a default rule will deny all packets that are not specifically permitted

■ IP filtering is since z/OS V1R7 an integral part of z/OS Communications Server

- Defined and managed by z/OS Communications Server

■ Benefits for local traffic (self-protection):

- Early discard of potentially malicious packets
- Avoid wasting CPU cycles checking validity of packets for applications that are not supported on this system



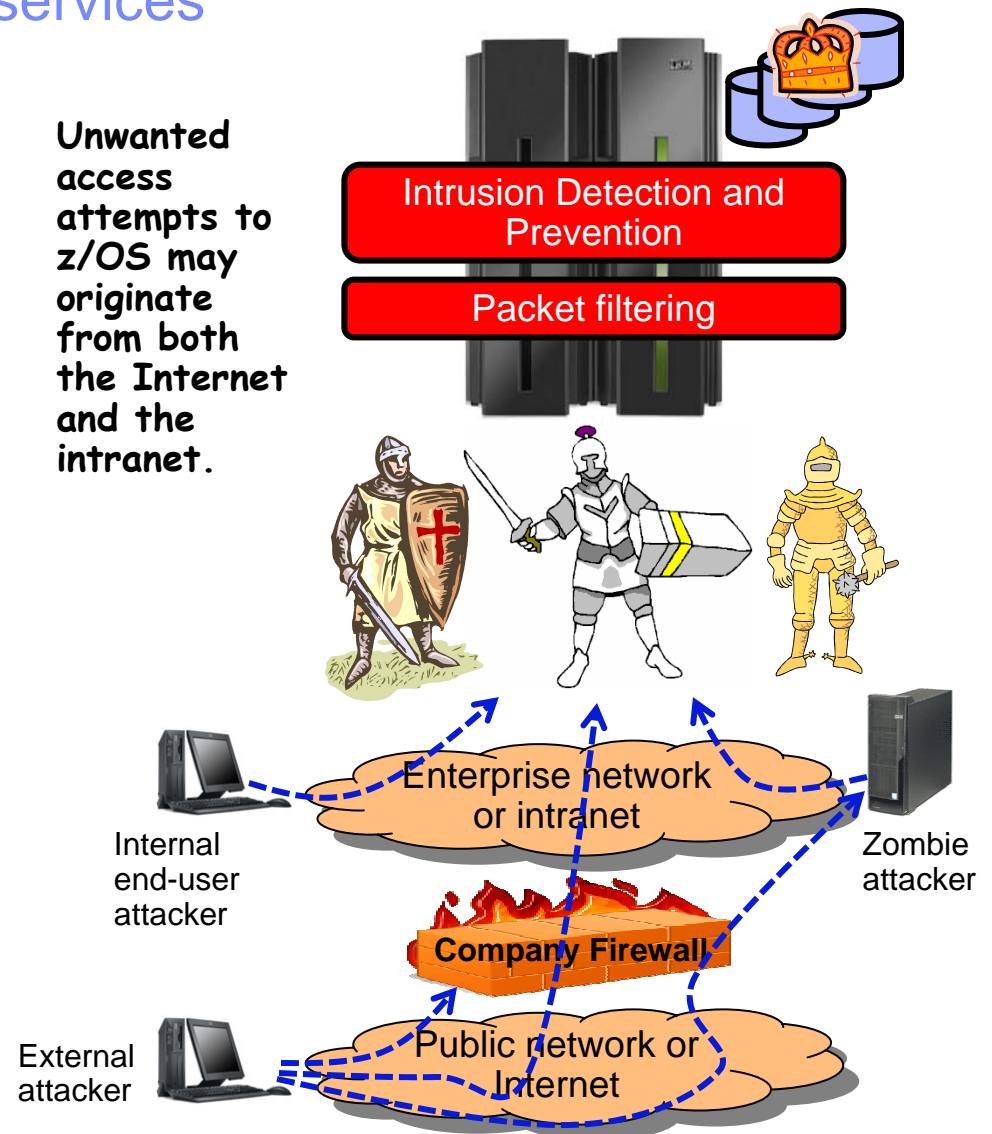
Step 2: Protecting against malicious or accidental attacks on your system or your legitimate (open) services

▪ What is an intrusion?

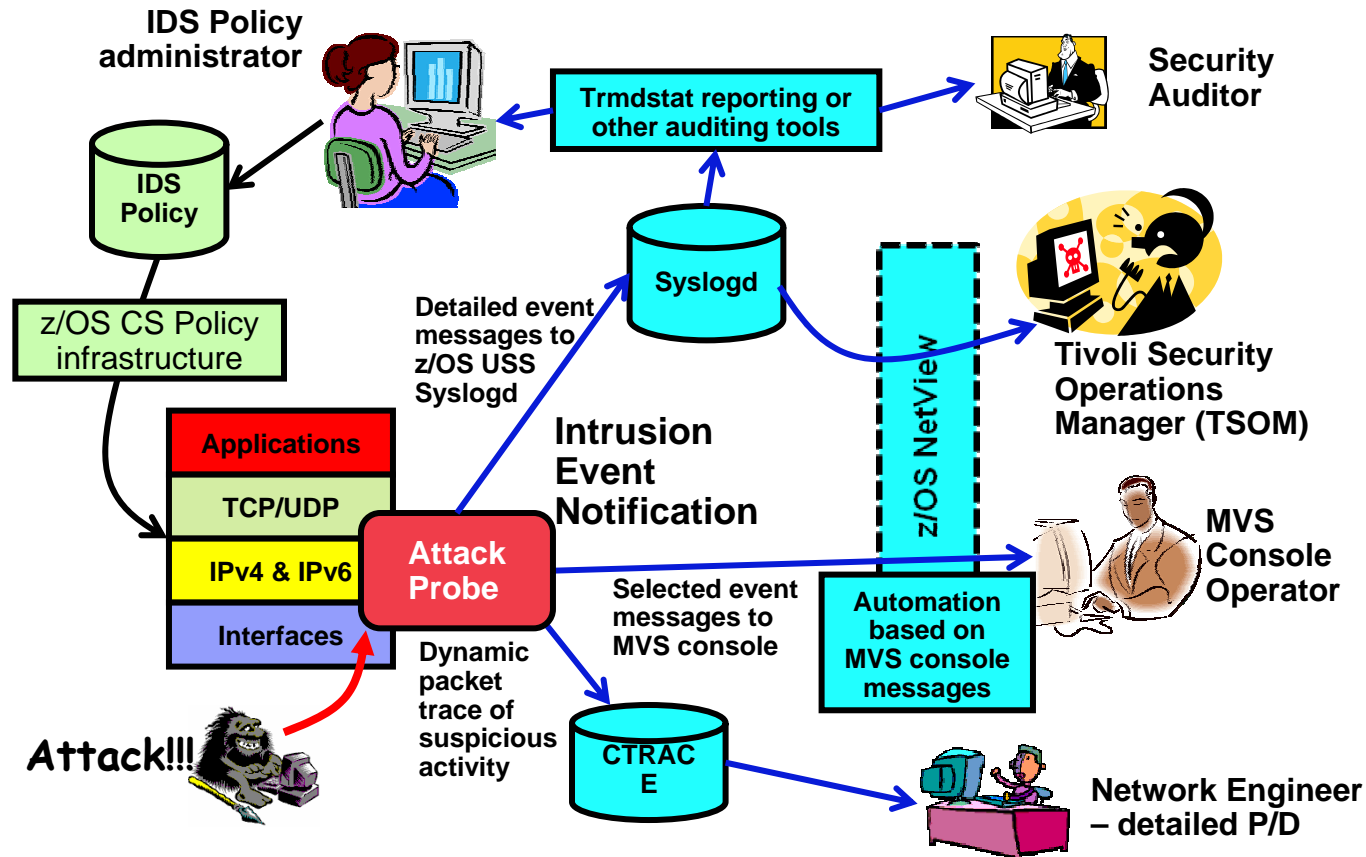
- Information Gathering
 - Network and system topology
 - Data location and contents
- Eavesdropping/Impersonation/Theft
 - On the network/on the host
 - Base for further attacks on others through Amplifiers, Robots, or zombies
- Denial of Service - Attack on availability
 - Single packet attacks - exploits system or application vulnerability
 - Multi-packet attacks - floods systems to exclude useful work

▪ Attacks can occur from Internet or intranet

- Company firewalls and Intrusion prevention appliances can provide some level of protection from Internet
- Perimeter security strategy alone may not be sufficient.
 - Some access is permitted from Internet – typically into a Demilitarized Zone (DMZ)
 - Trust of intranet
- Attacks can be deliberate with malicious intent, or they can occur as a result of various forms of errors on nodes in the network



Intrusion Detection and Prevention services on z/OS - overview



□ Events detected

- Scans
- Attacks against stack
- Flooding (both TCP and UDP)

□ Defensive methods

- Packet discard
- Limit connections

□ Reporting

- Logging
- Event messages to local console
- IDS packet trace
- Notifications to Tivoli NetView and Risk Manager

□ IDS Policy

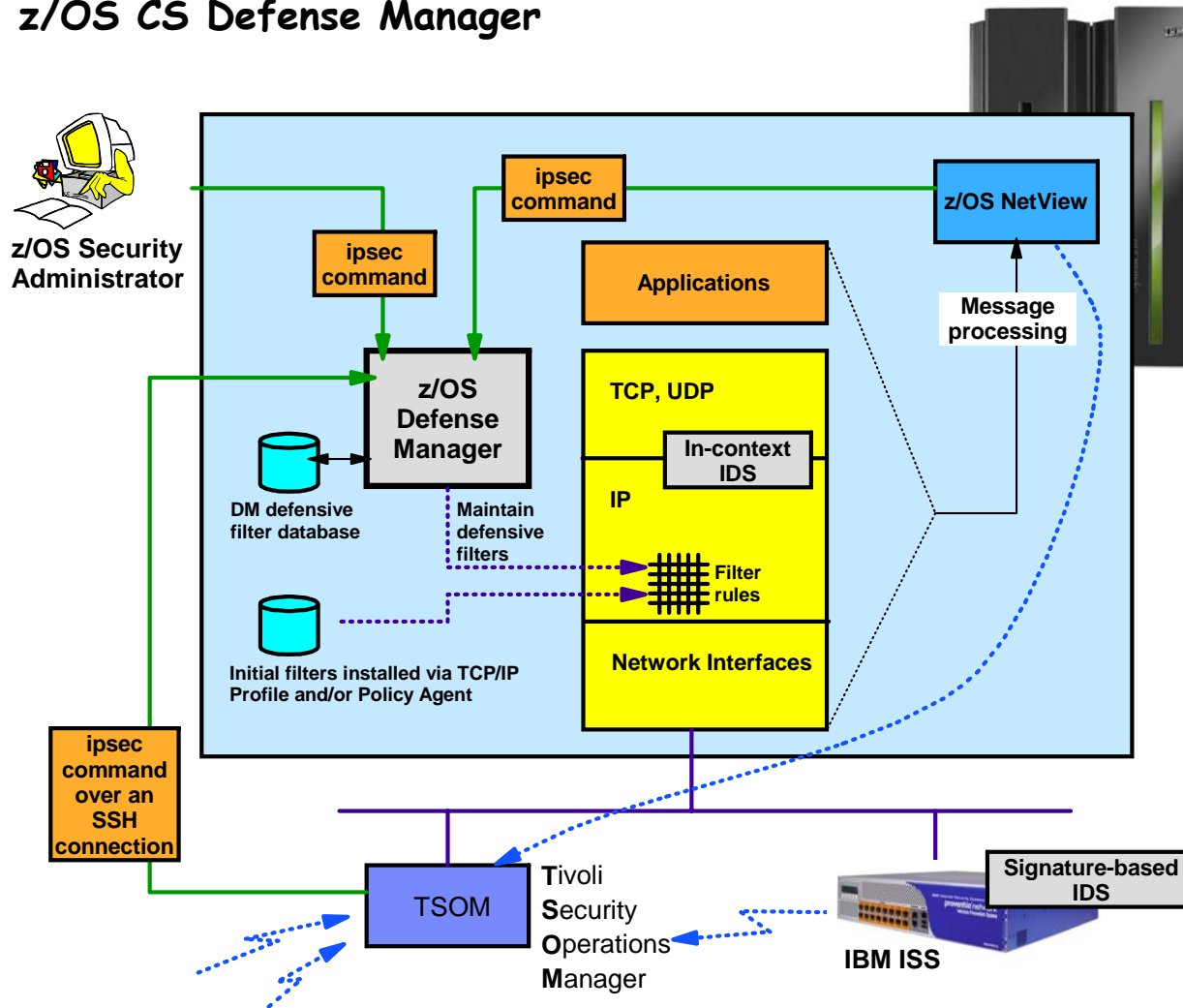
- Samples supplied with z/OS CS Configuration Assistant

▪ z/OS in-context IDS broadens overall intrusion detection coverage:

- In-context means as the communications end point, not as an intermediary
- Ability to evaluate inbound encrypted data - IDS applied after decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks - IDS policy checked after attack detected
- Detects statistical anomalies real-time - target system has state-full data / internal thresholds that generally are unavailable to external IDSs
- Policy can control prevention methods on the target, such as connection limiting and packet discard

Intrusion event action: install immediate defensive filter using the z/OS Defense Manager component

z/OS CS Defense Manager



- Use of ipsec command to display and control defensive filters is secured via SAF security profiles
- Defensive filters maintained on DASD for availability in case of DM restart or stack start/restart
- One Defense Manager per LPAR
- Defensive filters may be:
 - Global - all stacks on the LPAR where DM runs
 - Local - apply to a specific stack
 - Time-limited
 - Installed "in-front" of configured/default filters

Enable dynamic defensive actions on z/OS

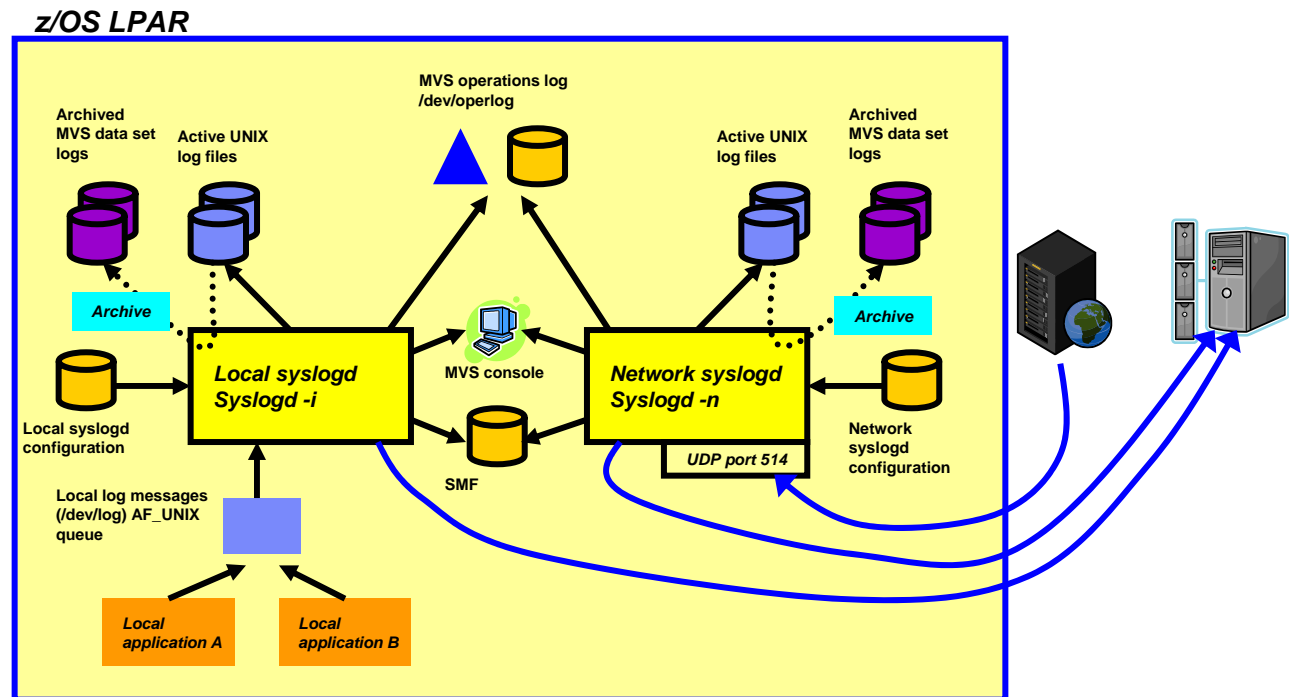
Step 3: Securing an audit trail for z/OS UNIX system services - Making sure log data is available when you need it to analyze past events

▪ Syslogd integrity and availability goals:

- Prevent loss of important system log records due to flooding
 - From network
 - From runaway or malicious applications
- Keep system log records separate from application log records
 - Ability to audit integrity of syslogd messages

▪ z/OS syslogd security controls provide:

- Protection from local z/OS users
 - Additional controls to direct syslogd messages to syslogd destinations based on Userid and/or Job name
 - UserID/Job name can be traced in log for audit
- Protection from the network
 - Syslogd configuration can turn off reception of log messages via UDP port
 - Does Not Limit Ability To Send
 - IP filtering can be used to selectively receive syslogd messages from the network
- z/OS V1R11 Communications Server delivered significant improvements in the area of syslogd management and use



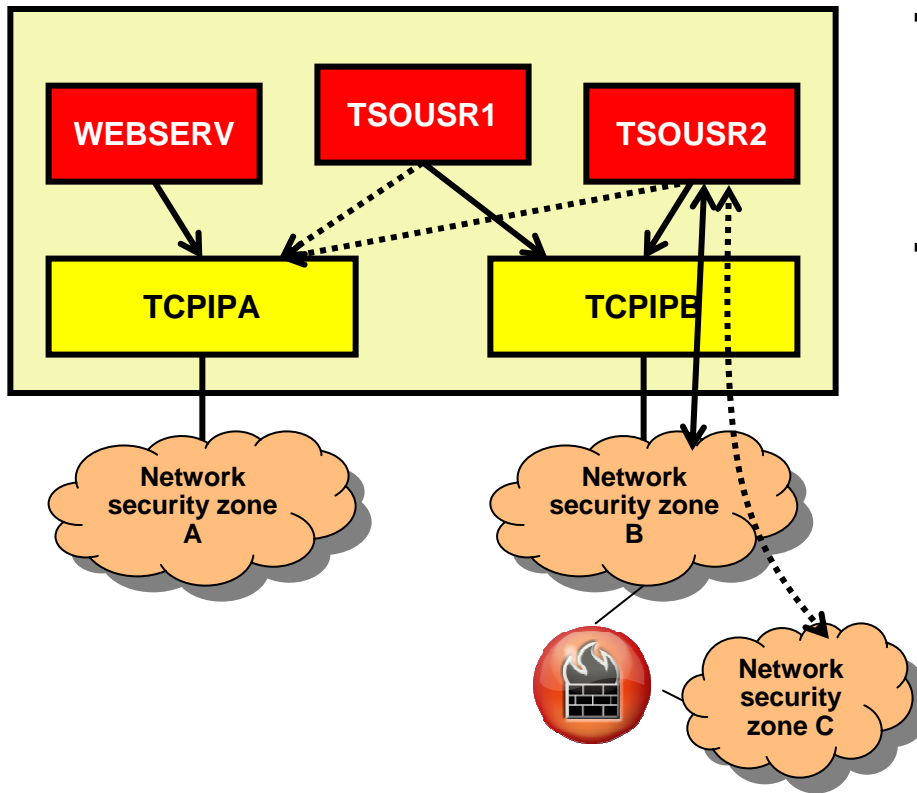
If anyone does not have SyslogD configured to capture, file, and archive log data - then you should go straight home and set it up!

Step 4: Extending SAF protection to TCP/IP-related resources on your z/OS system

- All the "traditional" SAF protection of datasets, authorized MVS and USS functions, etc. on a z/OS system applies to TCP/IP workload just as it applies to all other types of workload.
 - Be careful with anonymous services such as anonymous FTP or TFTP services that can be configured to allow unauthenticated users access to selected MVS data sets and/or HFS files.
 - The SERVAUTH resource class is used to specifically define and protect a number of TCP/IP unique resources
 - General SERVAUTH profile format:
 - **EZB.resource_category.system_name.jobname.resource_name**
- *EZB* designates that this is a TCP/IP resource
 - *resource_category* is capability area to be controlled e.g. TN3270, Stack Access, etc.
 - *system_name* is the name of the system (LPAR) - can be wild-carded (*)
 - *jobname* is the jobname associated with the resource access request - can be wild-carded (*)
 - optional *resource_name* - one or more qualifiers to indicate name of resource to be protected - can be wild-carded (*)
- To protect one of the supported TCP/IP resources, you define a SERVAUTH profile with universal access NONE and you then permit authorized user IDs to have READ access to the resource
 - If using OEM security packages, beware of the differences between defined/not defined resource actions
 - There are 30+ different possible TCP/IP-related resource types to protect
 - Careful use of these can provide a significant level of security administrator-based control over use of TCP/IP-related resources on z/OS

See IP Configuration Guide Chapter 3 for a complete list of SERVAUTH profiles

An example of use of SERVAUTH resources



EZB.STACKACCESS.*.TCPIPA

WEBSRV permitted, all others not

EZB.PORTACCESS.*.TCPIPA.WEBPORT

WEBSRV permitted, all others not

EZB.NETACCESS.*.TCPIPB.ZONEC

TSOUSR1 permitted, all others not

- **Stack Access Control in multi-stack LPARs**
 - Controls user ability to open socket (use of TCP/IP services)
 - Access to stack via sockets allowed if user permitted to SAF resource (SERVAUTH class: STACKACCESS)
 - TSOUSR1 and TSOUSR2 are not permitted to use TCPIPA
- **Local Port Access Control**
 - Controls whether a (started task) user ID can establish itself as a server on a given TCP or UDP port
 - Via SAF Keyword on PORT or PORTRANGE
 - Access to use port as a server allowed if user permitted to corresponding SAF resource (SERVAUTH class: PORTACCESS)
 - Only user ID WEBSRV is permitted to establish itself as the HTTP server (port 80) on stack TCPIPA
 - Access to a port not permitted for any user if the RESERVED Keyword is used on PORT Or PORTRANGE

Network Access Control

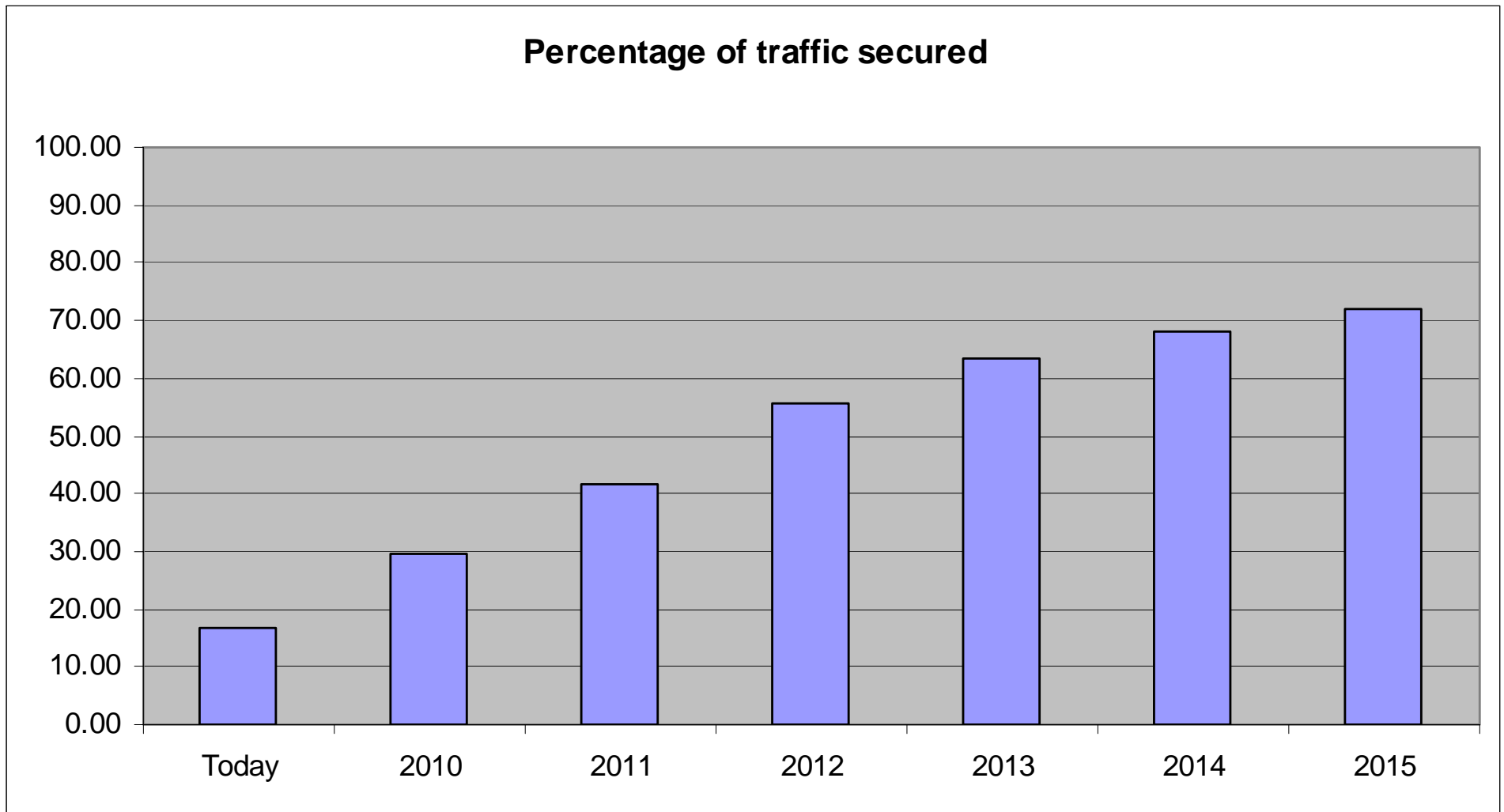
- Controls local user's access to network resources
 - A network segment considered a resource - Network/Subnet/Specific host
 - Network segment associated with SAF resource name in a NETACCESS statement in TCP/IP's Profile
 - Access defined as sending or receiving IP packets to/from a protected security zone
- Allows z/OS user-specific access to security zones
 - Firewalls cannot distinguish between individual users
- Access to security zone allowed if user permitted to SAF resource (SERVAUTH class: NETACCESS)
 - TSOUSR2 is not permitted to network security zone C

z/OS Network Security Roadmap

Step 5: Protect end-to-end confidentiality and integrity of data in the network

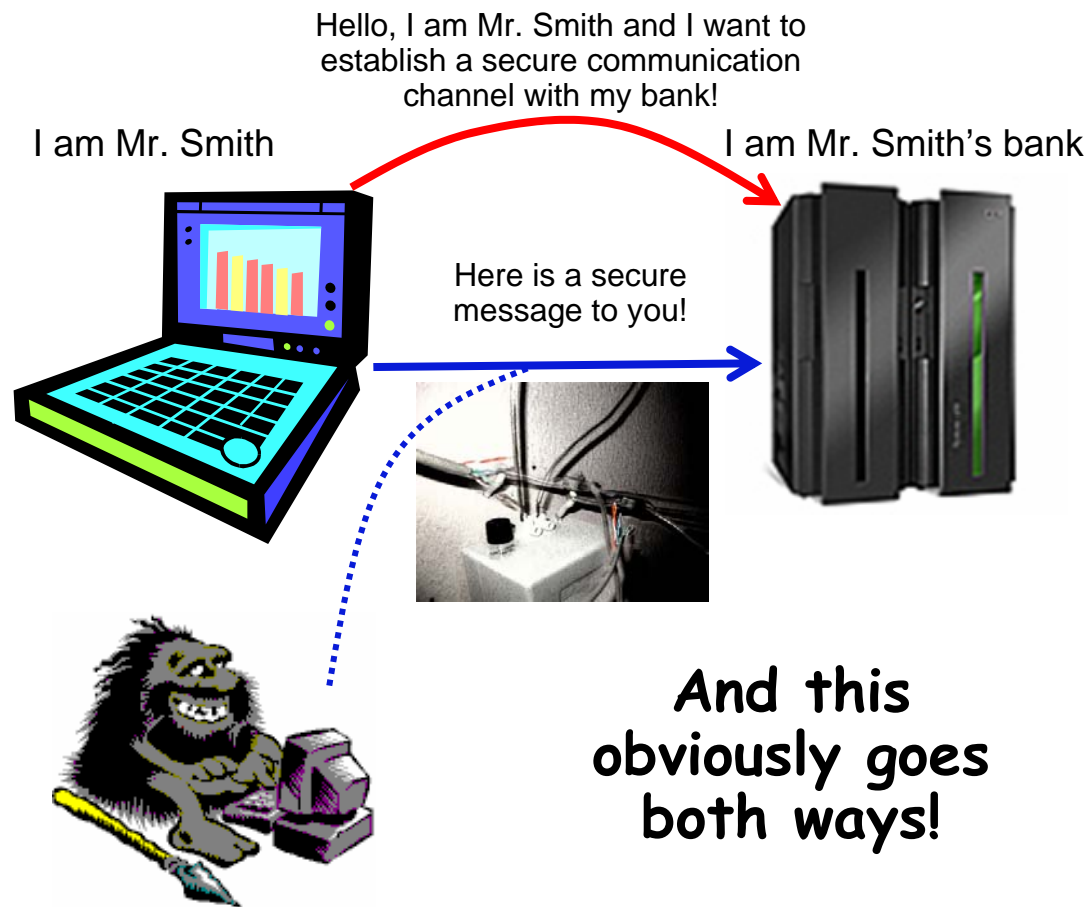


z/OS customer expectations to amount of secured traffic



Source: z/OS Communications Server CAP customer survey early 2009.

The four big questions for secure network communication



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

Partner authentication

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

Message authentication

- How can I trust that the secure message indeed came from the partner, who I authenticated a little earlier?
- How can I know it wasn't injected into the network by someone else?

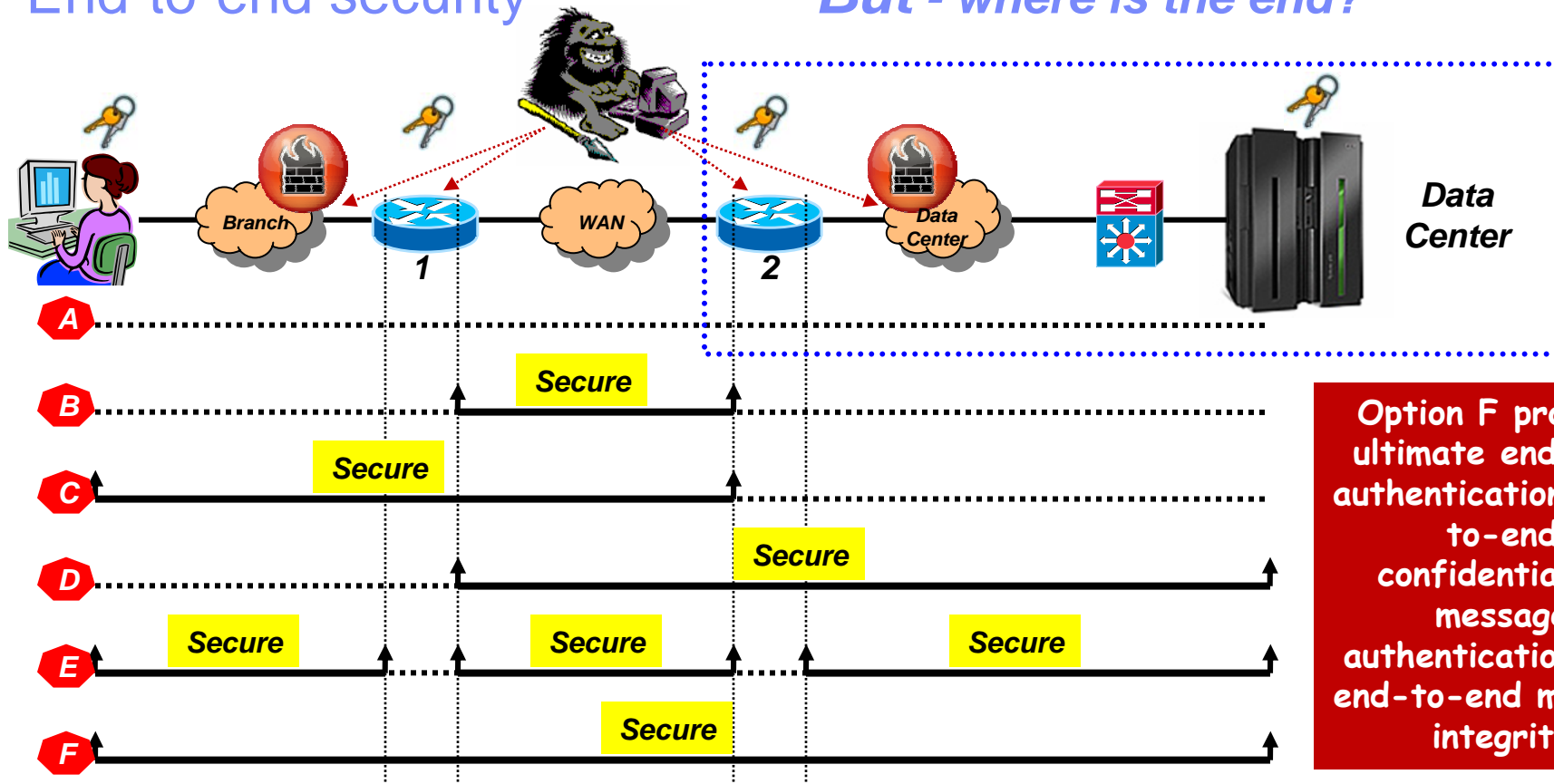
Message integrity

- How can I trust that someone didn't modify some of the data in the message since you sent it onto the network, or that someone didn't duplicate an otherwise valid message?

Data Confidentiality

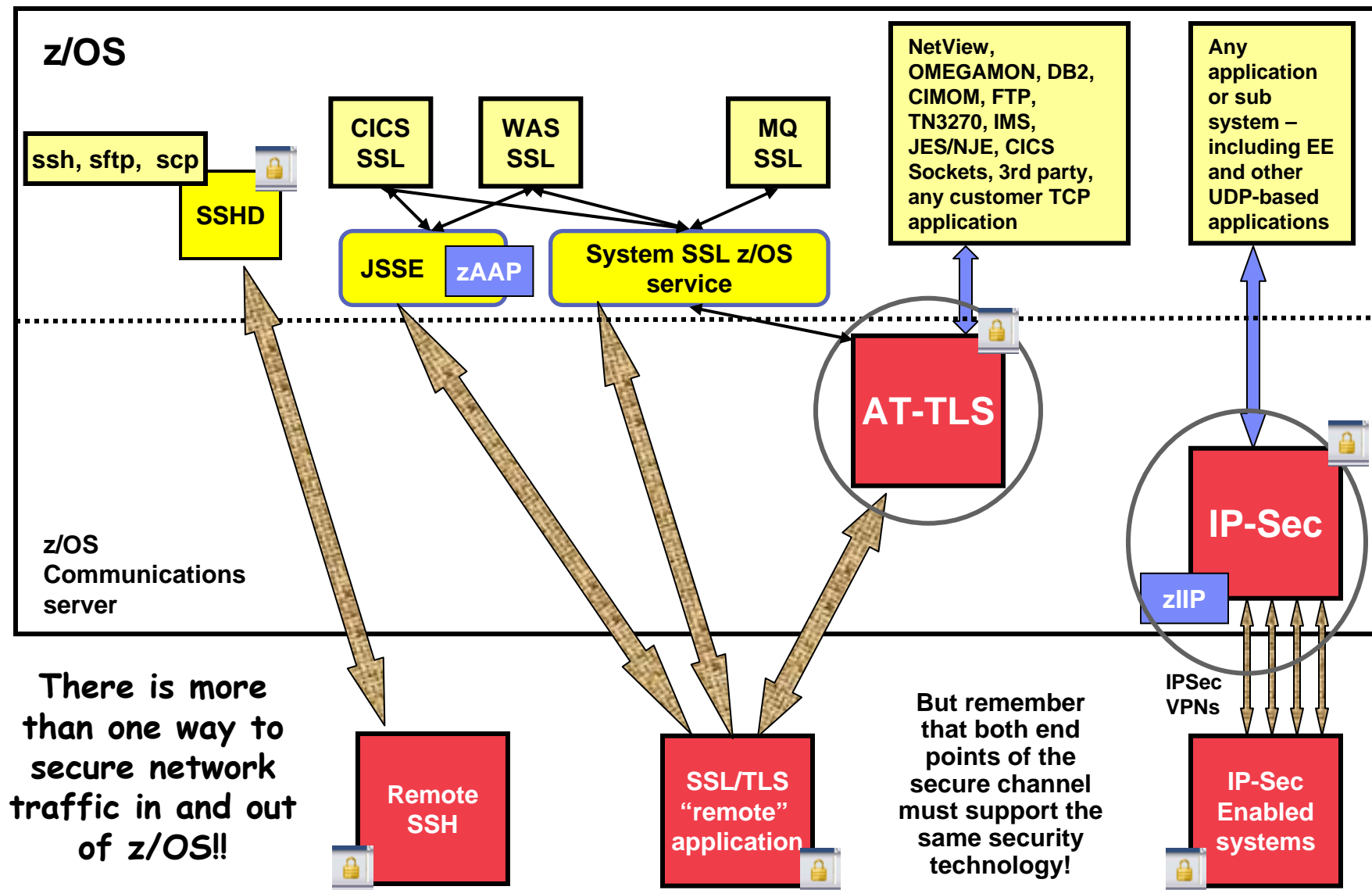
- How can I trust that no one could have snapped this message up and read it in an intelligible way since it was sent by you?

End-to-end security

But - where is the end?

Topology	Partner authentication	Key management	Message 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

Protect the data in the network: technology overview



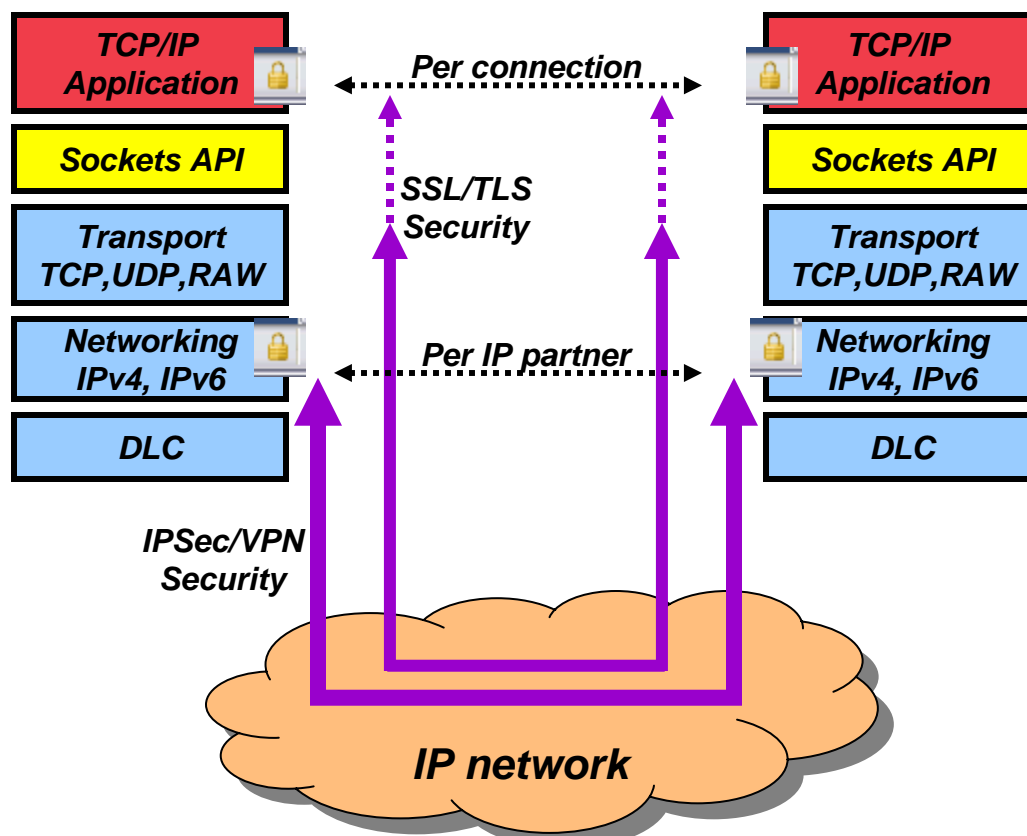
Some key differences between SSL/TLS and IPSec

■ SSL/TLS

- Per individual TCP connection
- Does not support UDP
- Application (ATTLS layer) to application (ATTLS layer) protection
- Often a designated TCP port for secure connections (such as 443)
- Transparent to applications on z/OS if ATTLS is used
 - Otherwise not
- Partner authentication via X.509 certificates

■ IPSec/VPN

- Supports all transport layer protocols (TCP, UDP, RAW)
- Can tunnel traffic from multiple applications over a single secure tunnel
- IP layer to IP Layer protection
- Always transparent to all applications
- Partner authentication via pre-shared key or X.509 certificates
- IPSec on z/OS can use zIIP

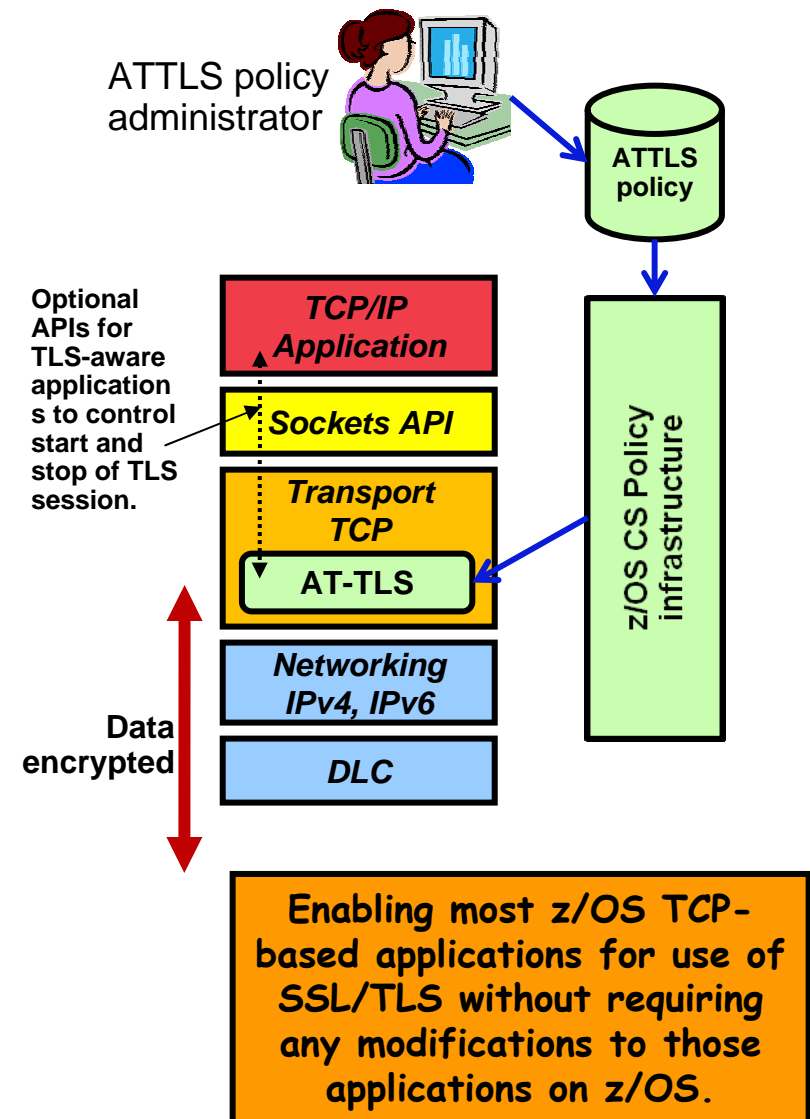


Some common characteristics:

- Both use CPACF and Crypto Express if available
- Both support most common encryption and authentication algorithms (3DES, AES, SHA, MD5, etc.)
- Both can use RACF and ICSF key-rings

z/OS application transparent SSL/TLS overview

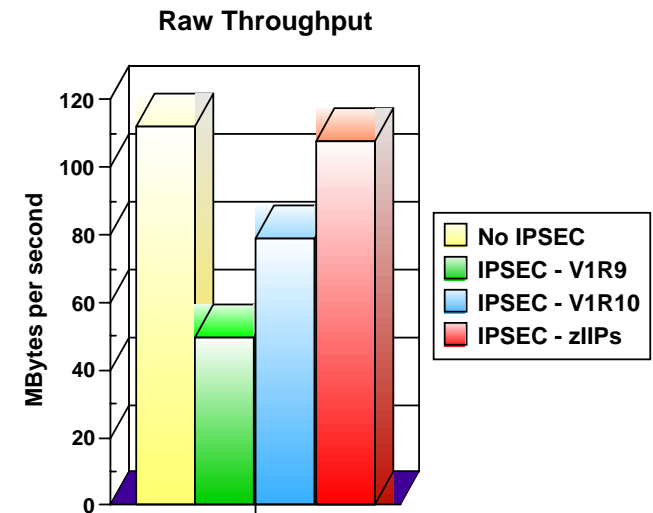
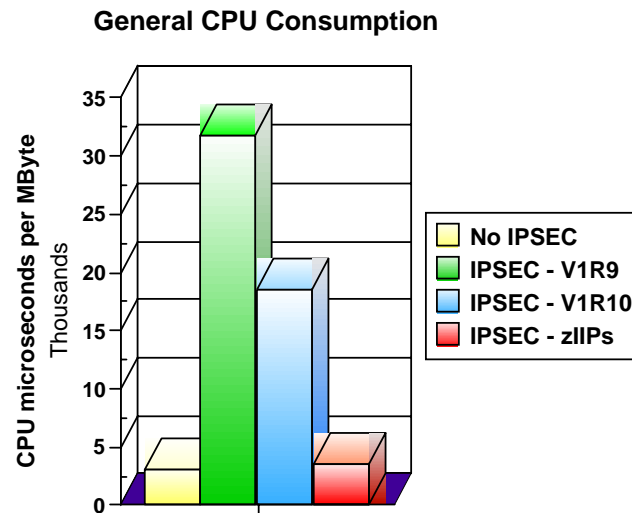
- **Basic TCP/IP stack-based SSL/TLS**
 - SSL/TLS process performed at TCP layer without requiring any application change (transparent)
 - All connections to specified port are designated as SSL/TLS required
 - Can be further qualified by source/destination IP addresses
 - AT-TLS policies managed via Policy Agent
- **Available to TCP applications**
 - Includes CICS Sockets
 - All programming languages except PASCAL supported
- **Application transparency**
 - Can be fully transparent to application
 - Application can control certain aspects of ATTLS processing - known as application-controlled ATTLS (TN3270, FTP, and NJE/IP use of ATTLS is application-controlled)
- **TCP/IP stack-based SSL/TLS with client identification services for application**
 - Application issues TLS API calls to receive user identity information based on X.509 client certificate
- **AT-TLS implements the standard SSL/TLS protocols**
 - Remote connection end point may use any SSL/TLS APIs to implement SSL/TLS



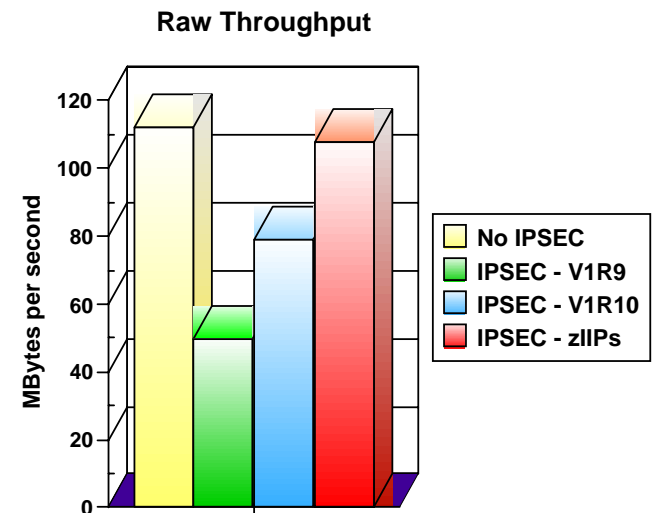
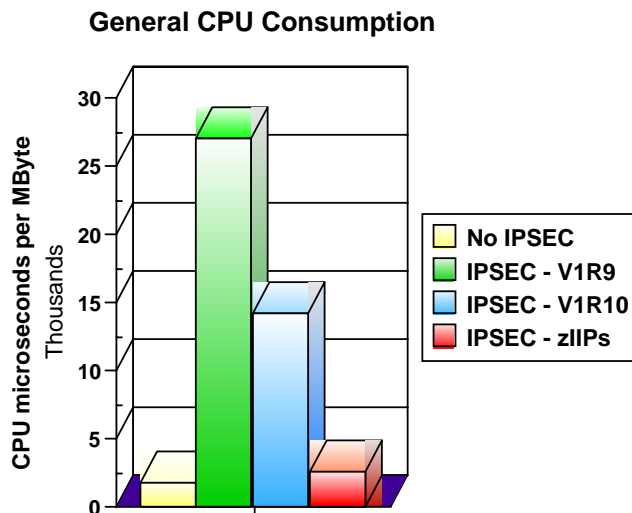
z/OS IPsec with zIIP: streaming (file transfer) workload performance

10 concurrent streaming sessions using AES encryption and SHA authentication

Inbound streaming



Outbound streaming



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.

What is encrypted and what are the impacts to “boxes-in-the-middle”?

What are “boxes-in-the-middle”?

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



*I am a “box-in-the-middle”
who wants to inspect the data
in 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
SSL/TLS
encryption:

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



IPSec
encryption:

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



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

*Your
network
engineer!*

*Your
security
czar!*

z/OS Network Security Roadmap

Securing selected application workloads



Why use AT-TLS for TN3270?

- TN3270 can be set up to use native System SSL or AT-TLS
 - TN3270 traffic is typically the first application workload to protect in order to secure RACF passwords that are typed in when logging in to TSO, CICS, or various session monitors
- Using AT-TLS instead of native System SSL has several advantages:
 - AT-TLS provides SSL/TLS features above and beyond what most SSL/TLS applications choose to support - such as, support for Certificate Revocation Lists (CRLs), multiple key-rings per server, optional use of system SSL cache, etc.
 - AT-TLS uses an optimized SSL/TLS infrastructure that in most cases performs better than when SSL/TLS is implemented directly in the applications
 - Performance enhancements in z/OS V1R12
 - Support of new SSL/TLS functions, such as new cipher-suites, can be added without application changes
 - New functions were added to AT-TLS in z/OS V1R11 - such as support for TLSv1.1
 - Addressing FIPS 140-2 requirements
 - Allows SSL/TLS-enabling non-C sockets applications on z/OS, such as CICS Sockets, Assembler- and Callable sockets, etc.



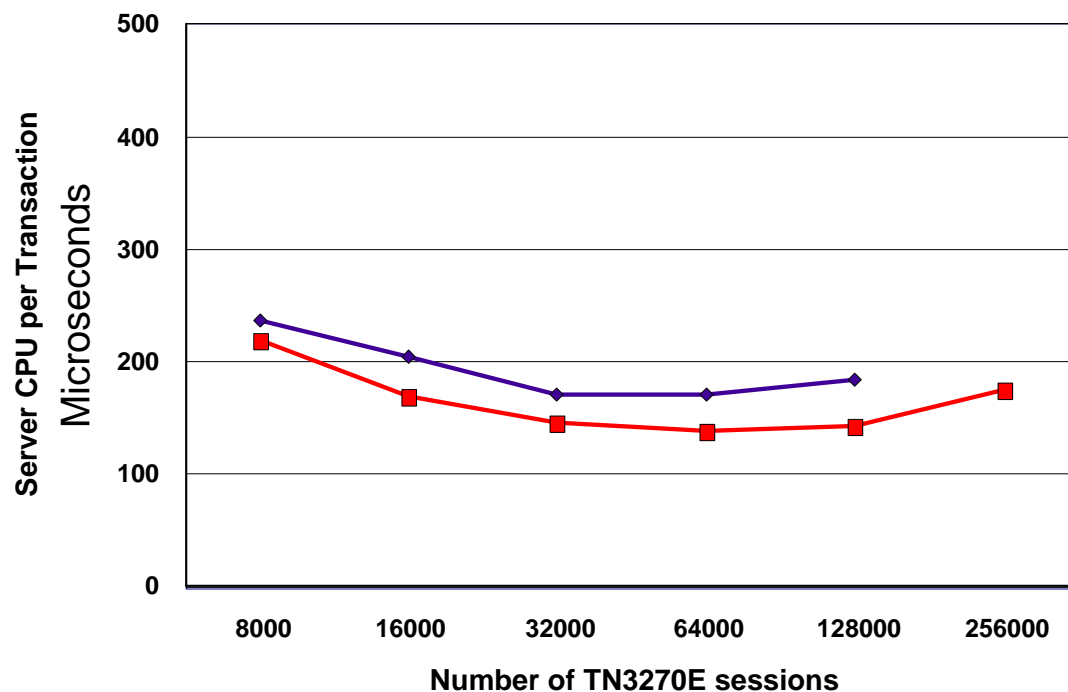
***We want
you to use
AT-TLS !!***

***Not (just) because (Uncle) Sam tells you
to, but because it is the smart thing to do!***

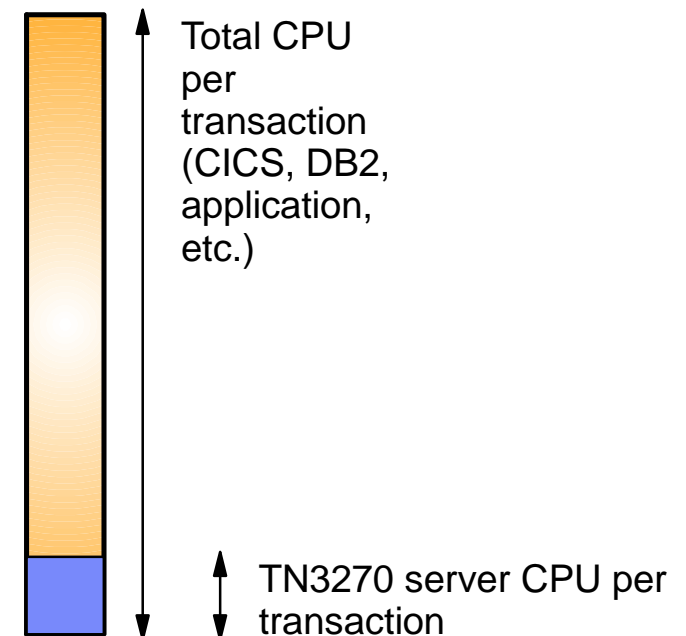
z/OS V1R9 Communications Server TN3270E AT-TLS Security Performance (TN3270 Server, Steady State, CPU per Transaction)

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

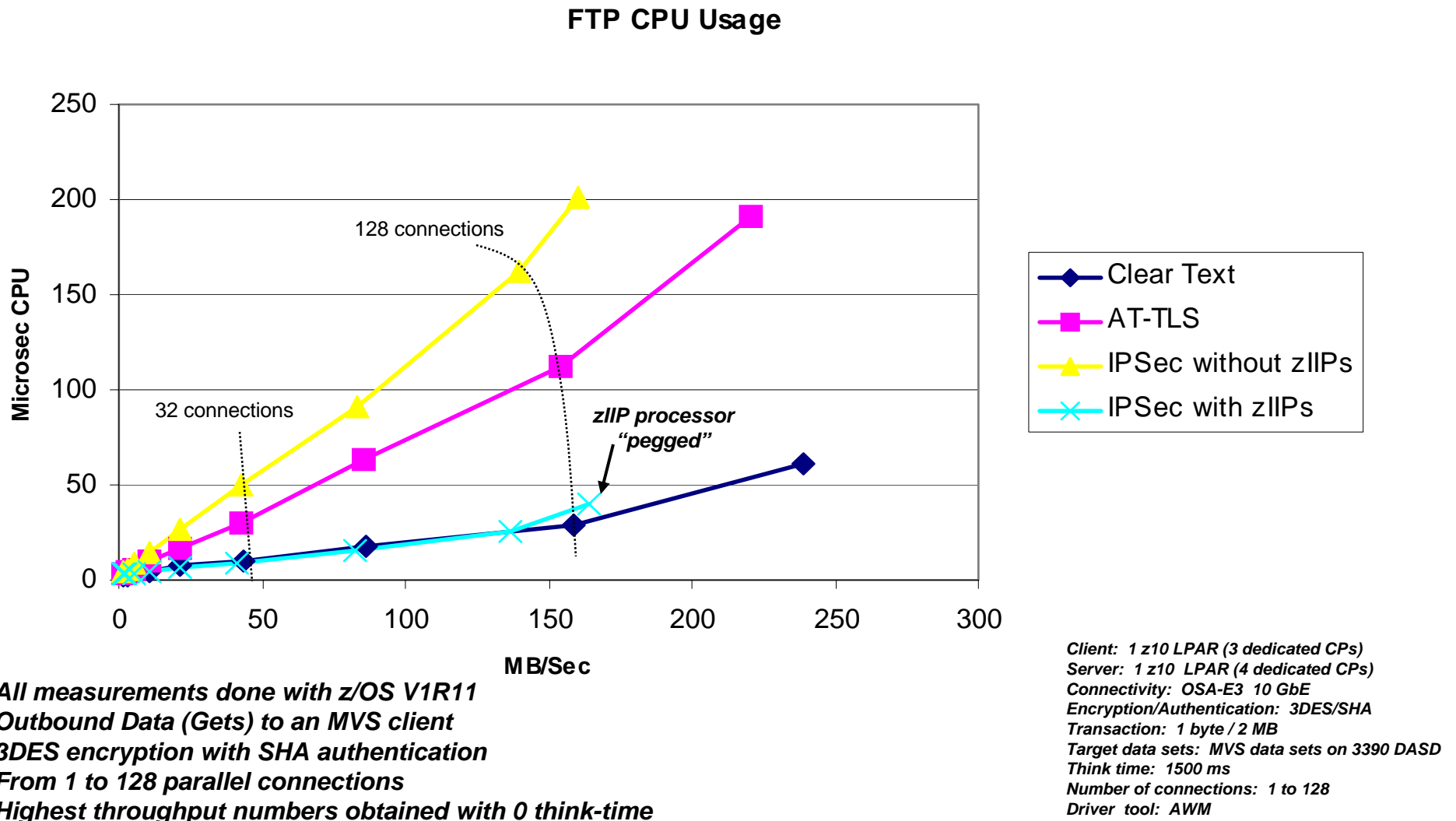
100 bytes in/800 bytes out

Think time 30 seconds

A quick comparison of selected z/OS file transfer technologies from a security perspective

	FTP With no security RFC959	FTPS FTP w. SSL/TLS RFC959 + RFC4217	FTP FTP w. IPSec Any RFC level	SFTP 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
Use of System z hardware encryption technologies	n/a	Yes	Yes	No
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	No
FIPS 140-2 mode	n/a	Yes (z/OS V1R11)	No	No
Mutual authentication supported	n/a	Yes	Yes (at an IP address level)	Yes

Comparing FTP Server CPU usage with and without security

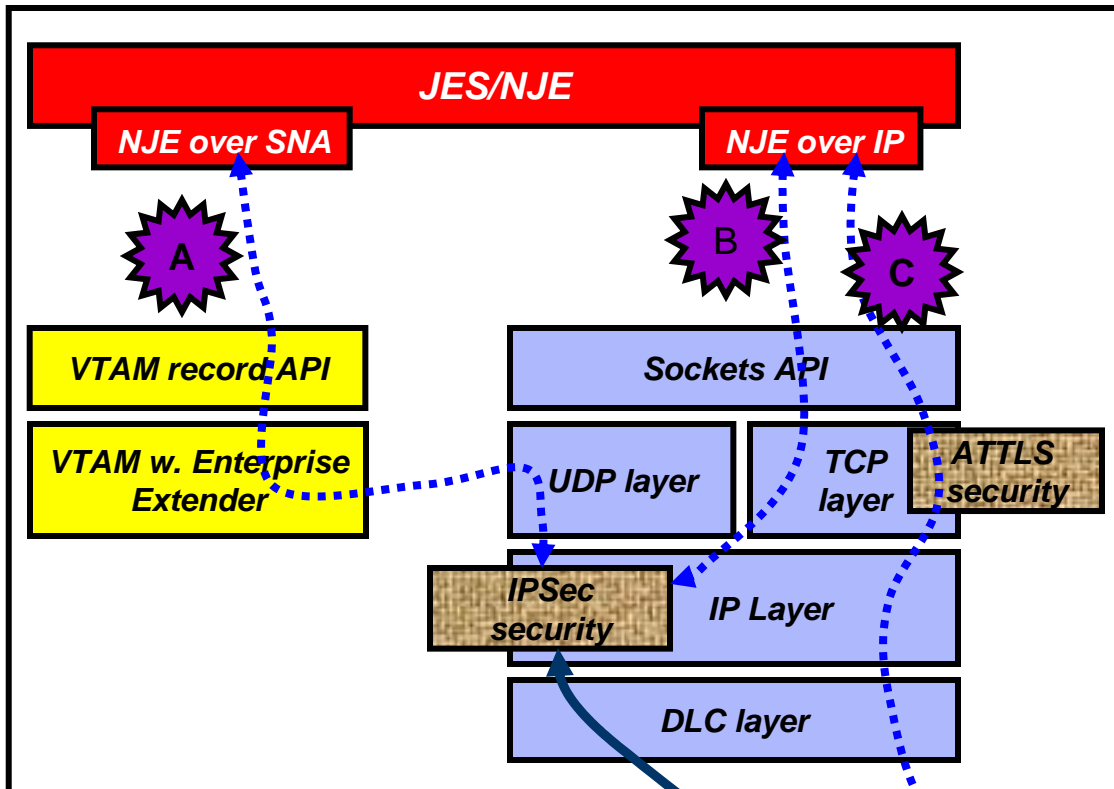


All measurements done with z/OS V1R11
Outbound Data (Gets) to an MVS client
3DES encryption with SHA authentication
From 1 to 128 parallel connections
Highest throughput numbers obtained with 0 think-time

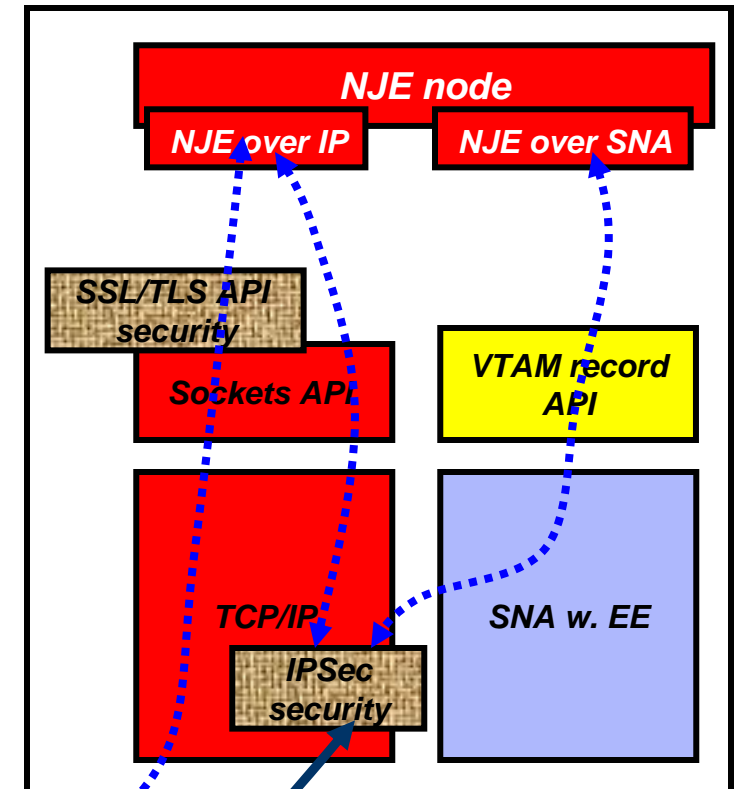
All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

Securing NJE traffic over an IP network

z/OS



Some other NJE node



NJE traffic
protected using
IPSec/VPN

NJE traffic
protected
using SSL/TLS

IPSec/VPN secure tunnel

Choosing networking security technology for NJE traffic

	NJE/SNA using EE and IPSec	NJE/IP using IPSec	NJE/IP using AT-TLS
JESPARM changes	None	None (if already using NJE/IP)	Define secure port
Performance (throughput)	Acceptable (Improvements in z/OS V1R11)	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	SSL/TLS
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	SSL/TLS setup
Addressing FIPS 140-2 compliance	Yes (z/OS V1R12)	Yes (z/OS V1R12)	Yes (z/OS V1R11)
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

SSL/TLS enabling 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	Yes	Yes	(Yes)	
All TCP applications			(Yes)	

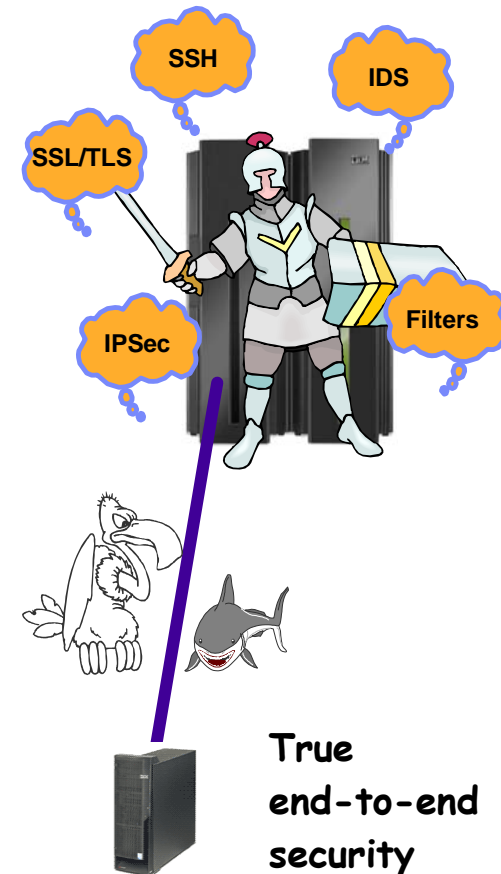
z/OS Network Security Roadmap

Summary



z/OS CS security aspects sum-up



- Protecting system resources and data from the network
 - Integrated Intrusion Detections Services
 - Detects, records, and defends against scans, stack attacks, flooding
 - Protect system availability
 - Built in protection against Denial of Service attacks
 - IP packet filtering
 - Syslogd integrity and availability
 - Sysplex Wide Security Associations
 - SAF protection of z/OS resources
 - z/OS CS application access to data sets and files
 - SERVAUTH class protection
 - Ex: Local user access to TCP/IP system, TCP and UDP ports
 - Multilevel security
- Protecting mission critical data in the network
 - True end-to-end security with security end-point on z/OS
 - Strong encryption with Triple DES and AES
 - Using hardware assist from crypto coprocessor and CP assist instruction
 - Transparent Application Security
 - IPSec for TCP/IP applications
 - Application-Transparent TLS support
 - Internet-ready access to SNA applications with TN3270 SSL
 - SSH port forwarding or tunneling
 - Built-in Application Security
 - SSL-enabled FTP, Kerberized FTP, rsh, telnet, ssh, sftp, scp
 - Secure network services
 - SNMPv3, Secure OSPF Authentication, Secure DNS



You will likely end up using a combination of technologies to meet all your security requirements.

For more information



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

For pleasant reading