STG LAB Services

ATS6
Protecting z/OS Data While in Flight

© 2012 IBM Corporation

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®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®
- GDDM®
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM (logo)®
- IBM®
- IMS
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x
- System z
- System z9
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

- 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.
- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- 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.

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.

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

© 2007 IBM Corporation

© 2007 IBM Corporation

Words to Live By

- **"The Security Perimeter is now at the End Point" Anonymous**

© 2007 IBM Corporation

Why Add Security

- ID theft is on the rise
- Meet both Public and Private standards
  - PCI standard (Session S1713)
  - European Common Standard
  - US regulations starting to come around
    - California SB 1386
- Keep the business off the BLOGs
  - Was the Front Page… but these days bad news travels a lot faster

© 2007 IBM Corporation

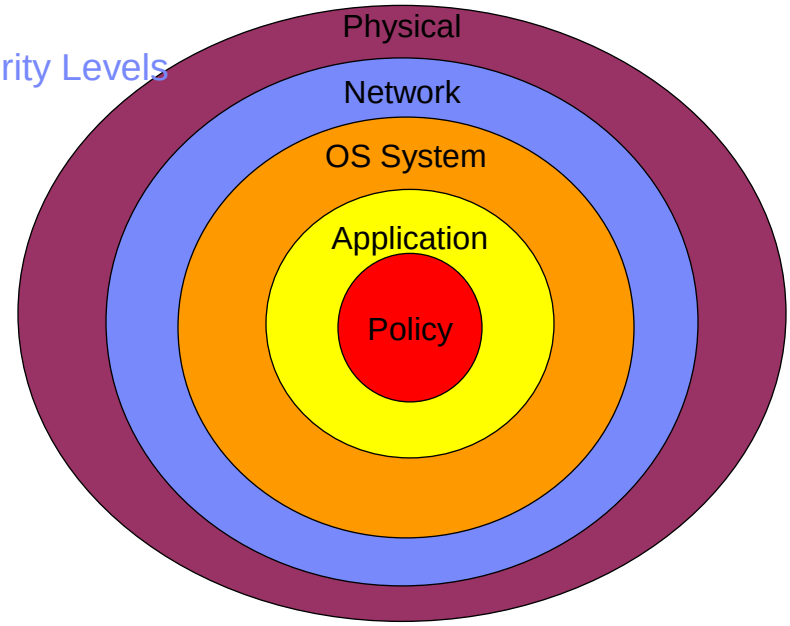
Business Unit or Product Name

Why Add Security

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

© 2007 IBM Corporation

Security Levels



© 2007 IBM Corporation

Most do a good Job protecting the Castle

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

© 2007 IBM Corporation

However what about the data you transmit

- User IDs and Passwords
- Employee Data
- Customer Data

© 2007 IBM Corporation

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 preforming man in the middle attacks

© 2007 IBM Corporation

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

© 2007 IBM Corporation

z/OS TCP/IP secure networking protocols

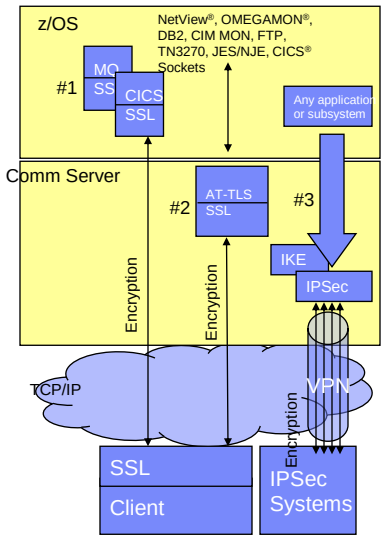
- **z/OS TCP/IP cryptographically protects network data in three ways:**

  #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

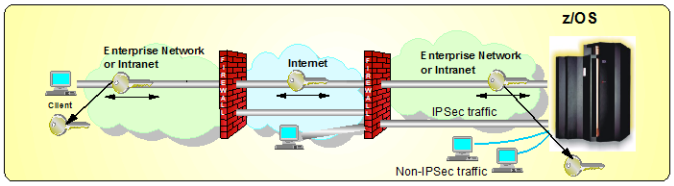
  #3 Virtual Private Networks using IP Security (IPSec) and Internet Key Exchange (IKE)
  - "Platform to platform" encryption
  - IPSec implemented at the IP layer as defined by policy
  - Wide variety (any to all) of traffic is protected
  - Completely transparent to application
  - IKE allows IPSec tunnels 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



© 2007 IBM Corporation

z/OS IP Security Support



A complete IP packet filtering, IPSec and Internet Key Exchange (IKE) solution built into z/OS Communications Server

- Protects the system from the network
  - IP filtering controls which packets enter the system
- Protects against data leakage from the system
  - IP filtering controls which packets can leave the system
- Cryptographically protects data in the network
  - Manual IPSec for statically defined security associations
  - Dynamic negotiation of IPSec security associations through IKE
- Filter directed logging of IP security actions to syslogd

© Copyright International Business Machines Corporation 2011. All rights reserved.

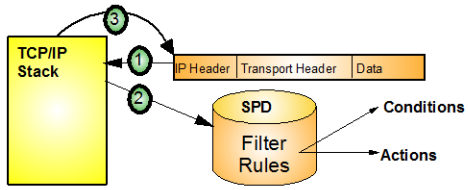
z/OS Communications Server IP Security Features

- **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 **(V1R12)**
  - HMAC-SHA-1, HMAC-MD5 authentication
  - HMAC-SHA-2, AES-XCBC, AES-GMAC authentication **(V1R12)**
  - AES-CBC, 3DES and DES encryption
  - AES-GCM (128- and 256-bit) encryption **(V1R12)**
  - Uses cryptographic hardware if available for most algorithms
  - FIPS 140 mode **(V1R12)**
- **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 **(V1R10)**
  - RFC 4306 (IKEv2) **(V1R12)**

© Copyright International Business Machines Corporation 2011. All rights reserved.

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

© Copyright International Business Machines Corporation 2011. All rights reserved.

© 2007 IBM Corporation

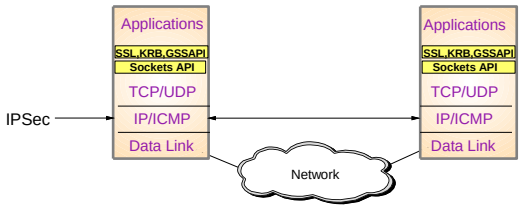
Filtering Conditions

Criteria	Description
From packet	
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)
Network attributes	
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.
Time condition	
Time, Day, Week, Month	Indicates when filter rule is active

© Copyright International Business Machines Corporation 2011. All rights reserved.

© 2007 IBM Corporation

IPSec Protocol Overview



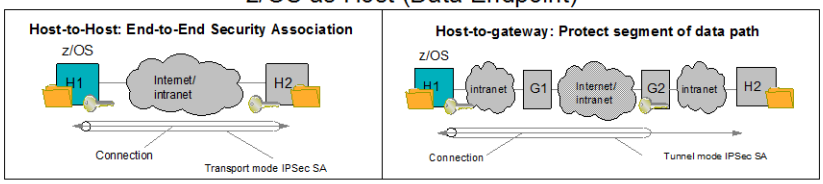
- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
  - IPSec security protocols
    - **Authentication Header (AH)** - provides data authentication / integrity
    - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional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

© Copyright International Business Machines Corporation 2011. All rights reserved.

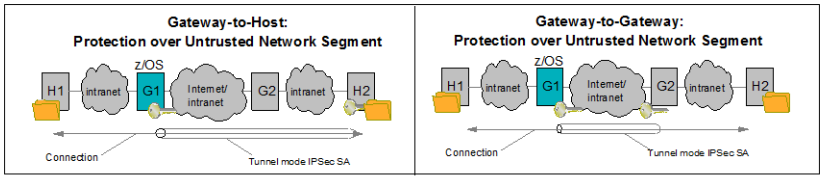
© 2007 IBM Corporation

IPSec Scenarios and z/OS Roles

z/OS as Host (Data Endpoint)



z/OS as Gateway (Routed Traffic)



© Copyright International Business Machines Corporation 2011. All rights reserved.

© 2007 IBM Corporation

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

*** New algorithm for V1R12**

© 2007 IBM Corporation

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

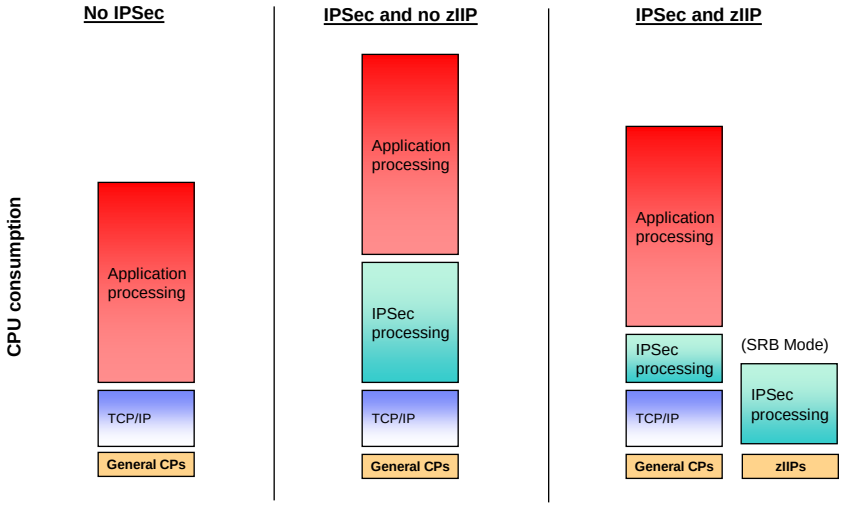
- **3DES, AES encryption of data traffic**
- **SHA-1 HMACs**
- **SHA-2 HMACs, AES-GMAC MACs for message authentication (V1R12)**
- **Note: FIPS 140 does not allow DES, MD5 or AES-XCBC**
- **All SRB-based processing in stack, *including these crypto operations*, can be offloaded to zIIP to reduce cost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

© 2007 IBM Corporation

IPSec processing using zIIP

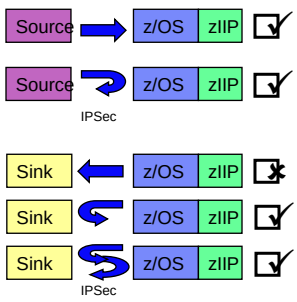


- CPACF is exploited in the same manner on both the general CPs and the zIIPs
- Function enabled through a TCP/IP configuration keyword when zIIP hardware and pre-req software is in place

© 2007 IBM Corporation

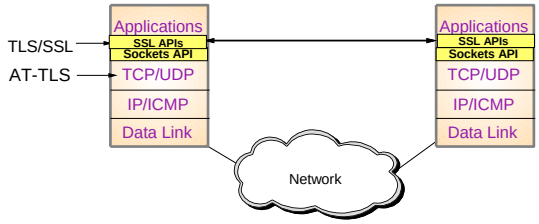
What IPSec workload is eligible for zIIP?

- **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



© 2007 IBM Corporation

Transport Layer Security Protocol Overview

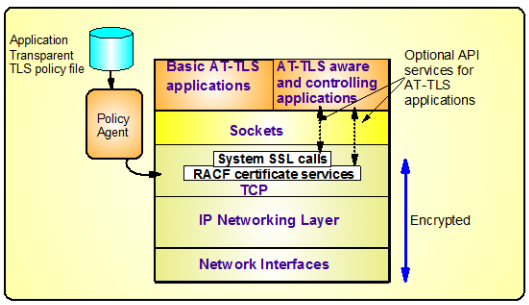


- Transport Layer Security (TLS) is defined by the IETF
  - ➤Based on Secure Sockets Layer (SSL)
    - –SSL originally defined by Netscape to protect HTTP traffic
  - ➤TLS defines SSL as a version of TLS for compatibility
    - –TLS clients and server should drop to SSL V3 based on partner's capabilties
- Traditionally provides security services as a socket layer service
  - ➤ Requires reliable transport layer (TCP only)
    - –UDP, raw IP applications cannot be TLS enabled
- z/OS applications can be modified to support TLS using System SSL
  - ➤ System SSL part of z/OS Cryptographic Services element
- Application Transparent TLS (AT-TLS) lets you apply TLS protection through System SSL with zero or minimal application change

© Copyright International Business Machines Corporation 2011. All rights reserved.

© 2007 IBM Corporation

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 SIOCTTLSCTL 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

© 2007 IBM Corporation

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.)

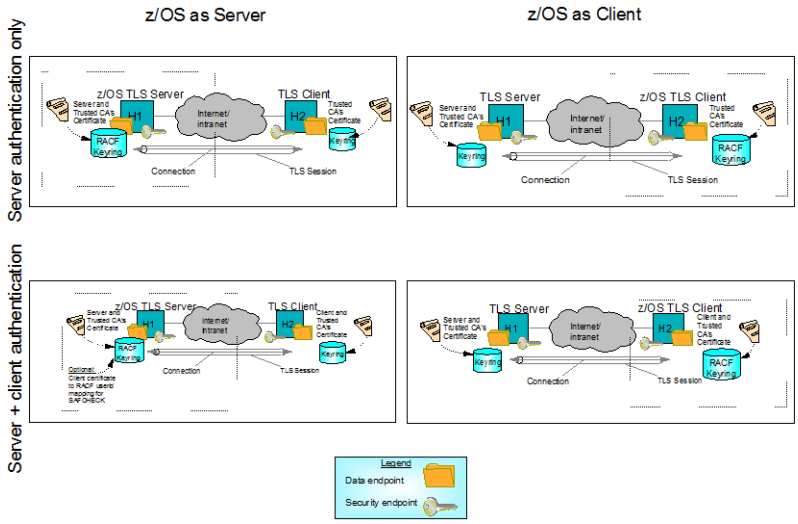
© Copyright International Business Machines Corporation 2011. All rights reserved.

AT-TLS Policy Conditions

Criteria	Description
Resource attributes	
Local address	Local IP address
Remote address	Remote IP address
Local port	Local port or ports
Remote port	Remote port or ports
Connection type attributes	
Connection direction	• Inbound (applied to first Select, Send, or Receive after Accept) • Outbound (applied to Connect) • Both
Application attributes	
User ID	User ID of the owning process or wildcard user ID
Jobname	Jobname of the owning application or wildcard jobname
Time condition	
Time, Day, Week, Month	When filter rule is active

© Copyright International Business Machines Corporation 2011. All rights reserved.

z/OS AT-TLS Supported Roles

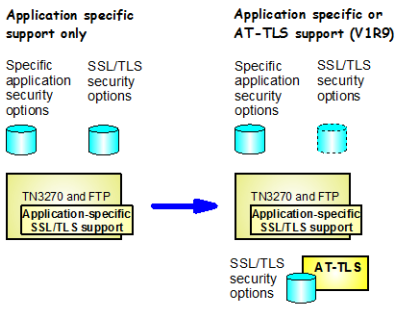


© Copyright International Business Machines Corporation 2011. All rights reserved.

© 2007 IBM Corporation

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 TN3720 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



© Copyright International Business Machines Corporation 2011. All rights reserved.

© 2007 IBM Corporation

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)	

© 2007 IBM Corporation

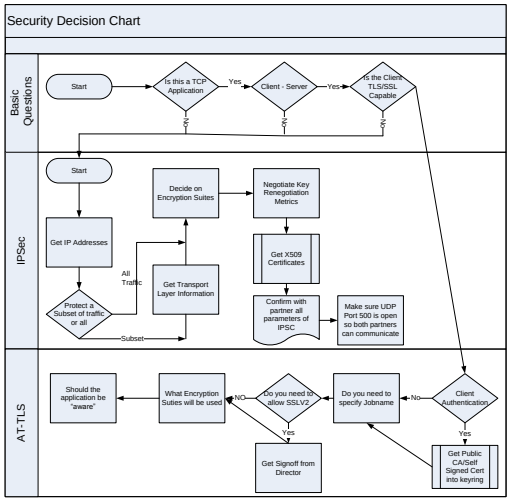
IPSec and AT-TLS Comparison

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

© Copyright International Business Machines Corporation 2011. All rights reserved.

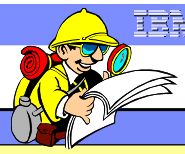
© 2007 IBM Corporation

So how do you decide what to use



© 2007 IBM Corporation

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

© 2007 IBM Corporation