



Software Group | Enterprise Networking Solutions

Configuring TN3270 and FTP Workloads with Application Transparent TLS

Part 1 of 2

Lin Overby - overbylh@us.ibm.com

Alfred Christensen - alfredch@us.ibm.com

Trademarks and notices

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

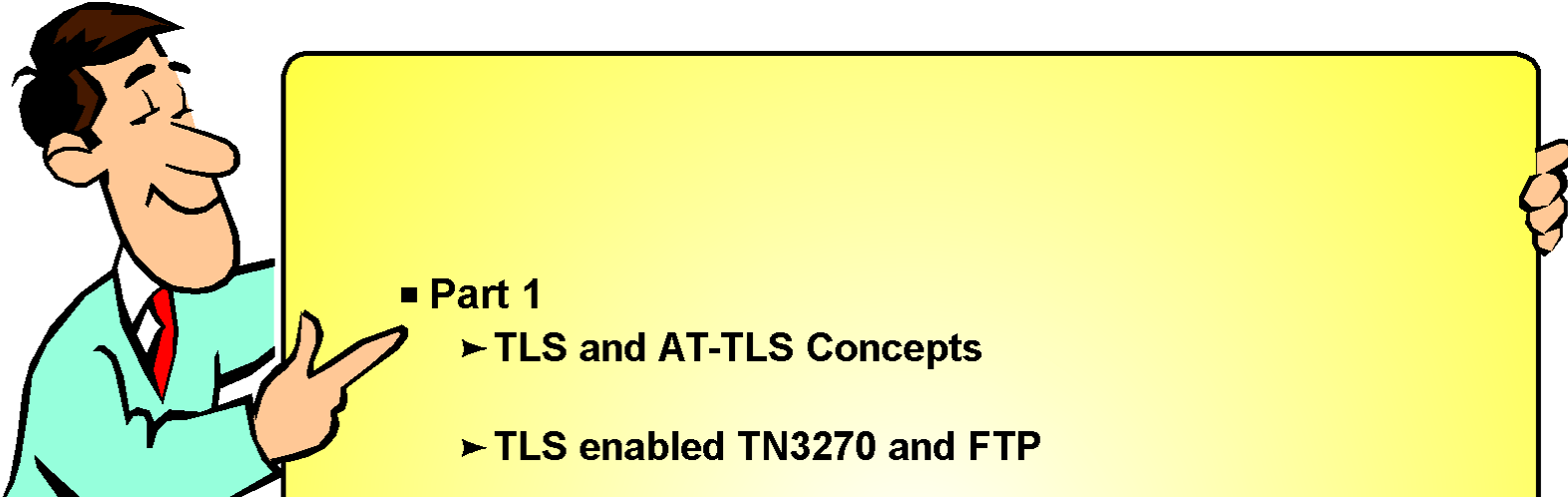
- ▶ Advanced Peer-to-Peer Networking®
- ▶ AIX®
- ▶ alphaWorks®
- ▶ AnyNet®
- ▶ AS/400®
- ▶ BladeCenter®
- ▶ Candle®
- ▶ CICS®
- ▶ DB2 Connect
- ▶ DB2®
- ▶ DRDA®
- ▶ e-business on demand®
- ▶ e-business (logo)
- ▶ e business (logo)®
- ▶ ESCON®
- ▶ FICON®
- ▶ GDDM®
- ▶ HiperSockets
- ▶ HPR Channel Connectivity
- ▶ 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.
- > All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

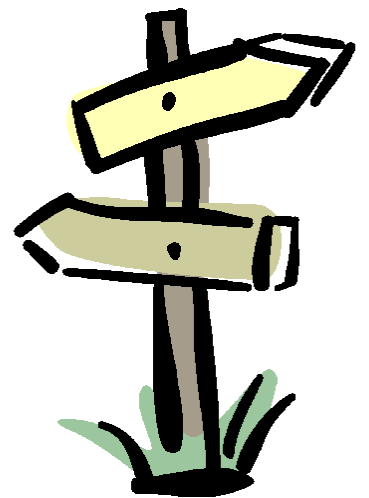
All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

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

Agenda



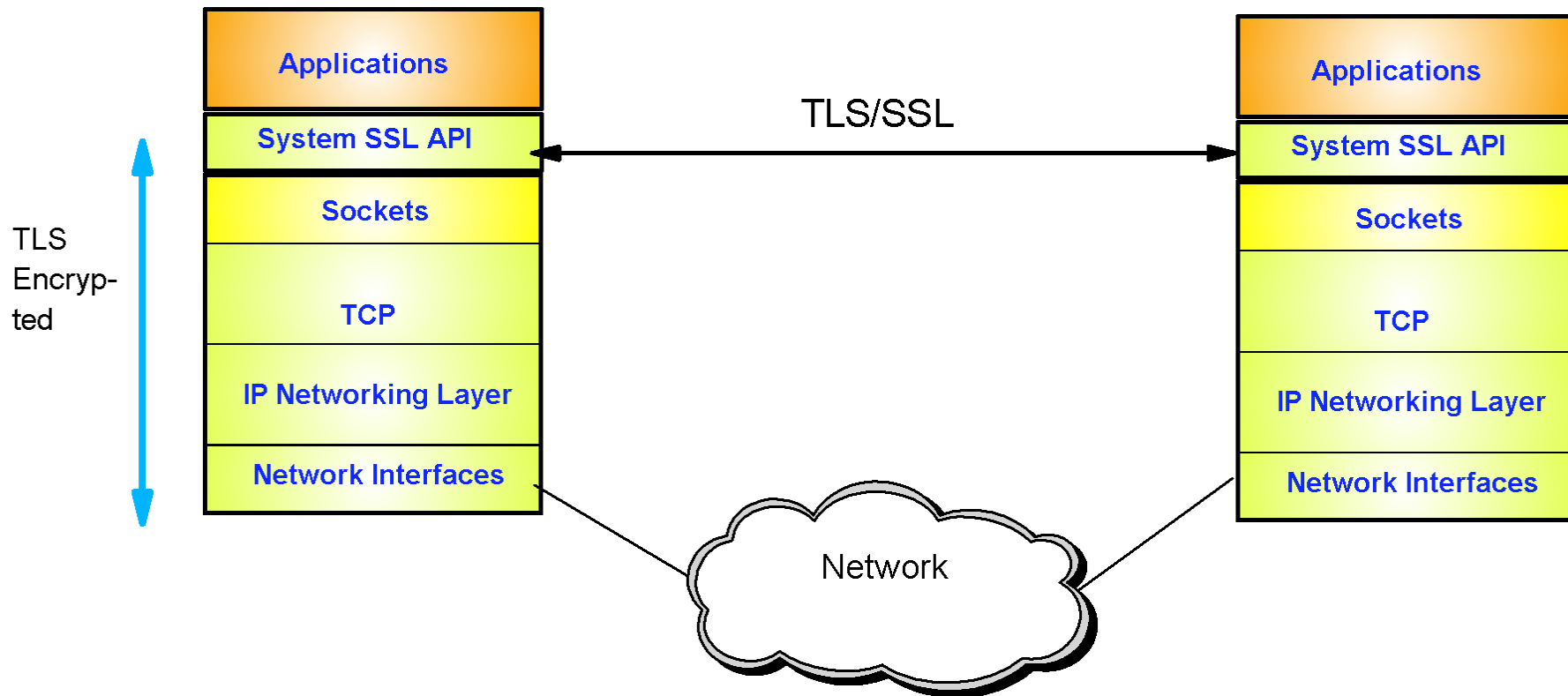
- Part 1
 - ▶ TLS and AT-TLS Concepts
 - ▶ TLS enabled TN3270 and FTP
 - ▶ AT-TLS enabled TN3270 and FTP
- Part 2
 - ▶ Configuring AT-TLS for TN3270 and FTP



z/OS Communications Server Network Security

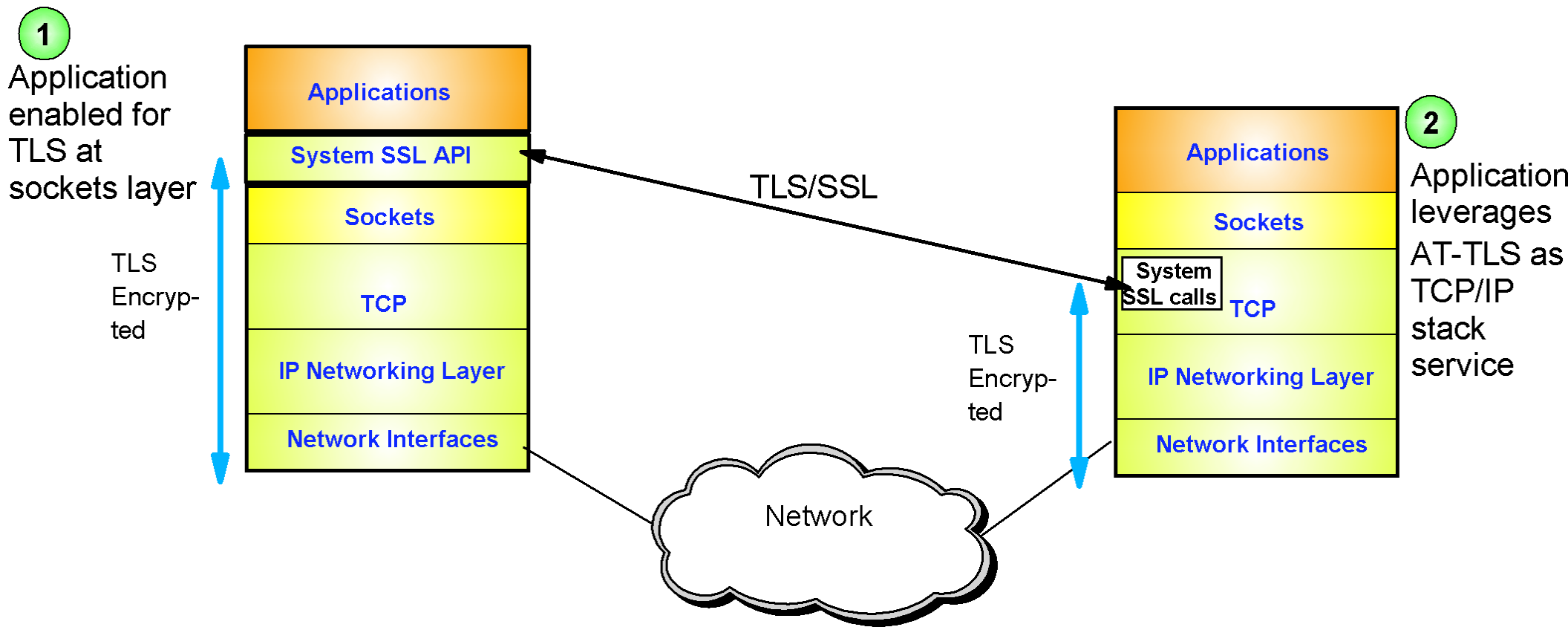
TLS and AT-TLS Concepts

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 capabilities
- Traditionally provides security services as a socket layer service
 - ▶ Provides secure session between TLS client and server
 - ▶ Requires reliable transport layer
 - UDP applications cannot be TLS enabled

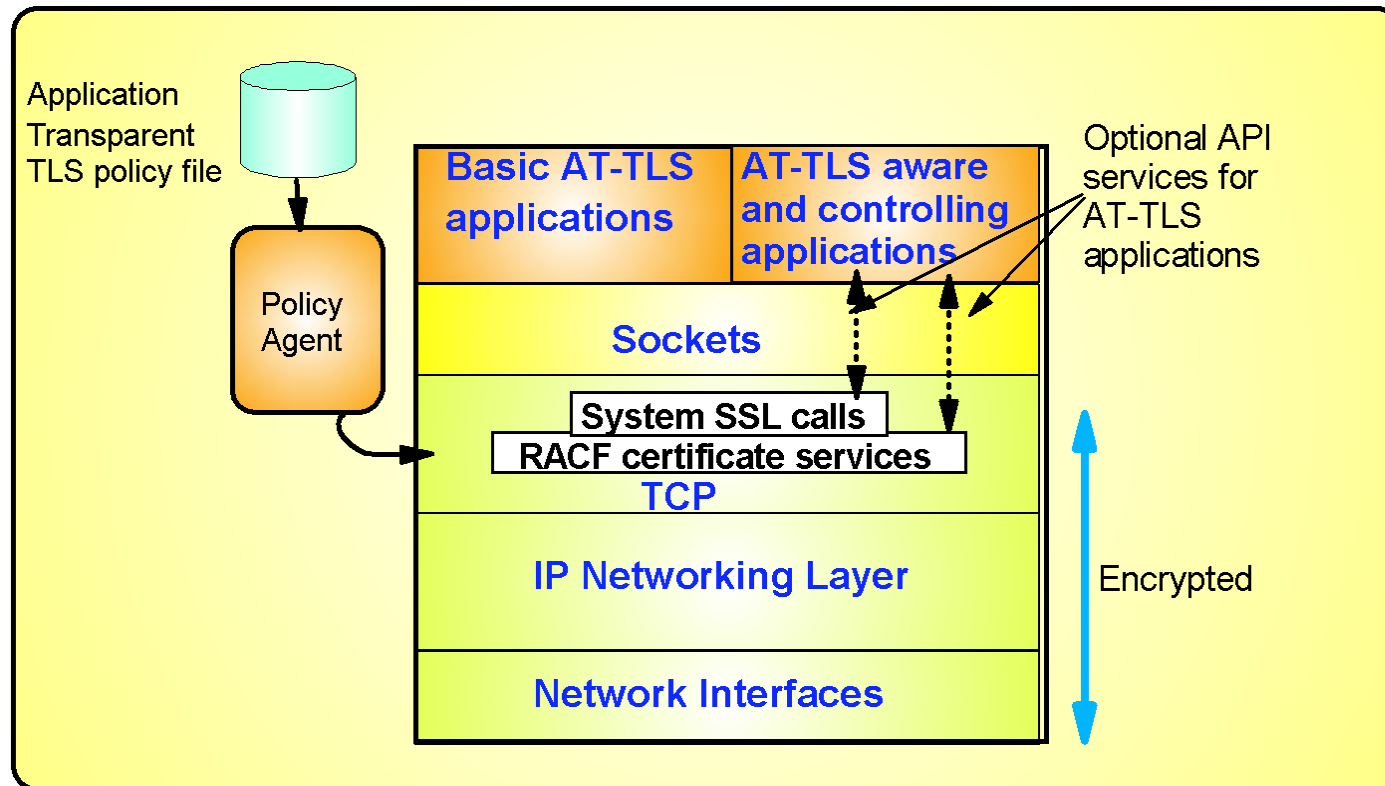
TLS Technology Choices on z/OS



Two methods for applications to receive TLS services on z/OS:

1. z/OS applications can be TLS enabled with System SSL
 - ▶ System SSL part of z/OS Integrated Security Services element
2. Starting in z/OS V1R7, TLS can be used with applications with no or minimal application change
 - ▶ Application Transparent TLS (AT-TLS)

AT-TLS Overview



- **AT-TLS performs TLS process at the TCP layer for the application**

- ▶ AT-TLS policy controls when and how to use AT-TLS

- AT-TLS policy managed by Policy Agent and configured by manual edit or Configuration Assistant for z/OS Communications Server

- **Most applications require no change to use AT-TLS**

- ▶ AT-TLS Basic applications

- **Applications can optionally exploit advanced features using new SIOCTTLSCTL ioctl call**

- ▶ AT-TLS Aware applications

- Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)

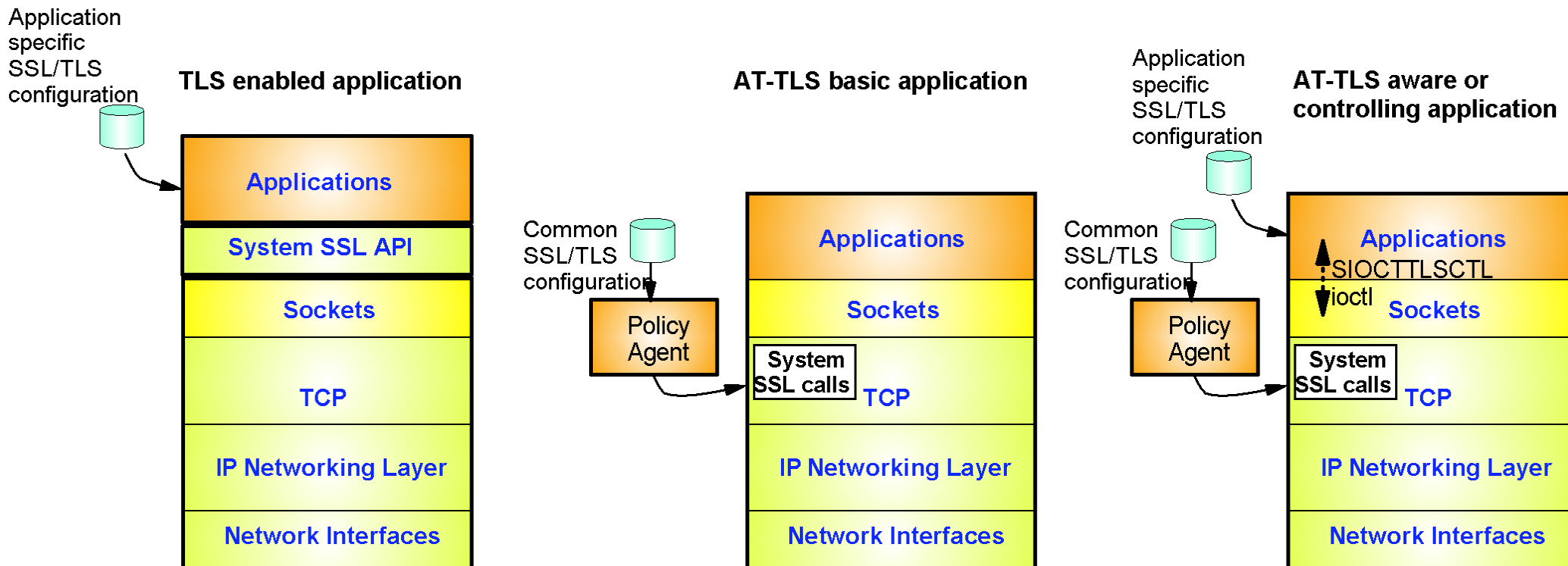
- ▶ AT-TLS Controlling applications

- Control if/when to start/stop TLS, reset session / cipher

AT-TLS Advantages

- Reduces development costs for application TLS exploitation
 - ▶ TLS system API invocations
 - ▶ TLS configuration controls
- AT-TLS provides SSL/TLS features above and beyond what most SSL/TLS applications choose to support:
 - ▶ Support for Certificate Revocation Lists (CRLs)
 - ▶ Multiple keyrings per server
 - ▶ Optional use of system SSL cache
- Support of new SSL/TLS functions can be added without application changes
 - ▶ ex: new ciphersuites
- Allows SSL/TLS-enabling non-C sockets applications on z/OS
 - ▶ ex: CICS Sockets, Assembler and Callable sockets, etc.
- Reduces administrative costs for AT-TLS configuration
 - ▶ Single, consistent AT-TLS policy system-wide vs. application specific policy

TLS Configuration Cases



■ TLS enabled application

- Each application has its own configuration to control security policy and TLS functions

■ AT-TLS basic application

- All applications' security policy and TLS functions are governed by a single, consistent AT-TLS policy system-wide

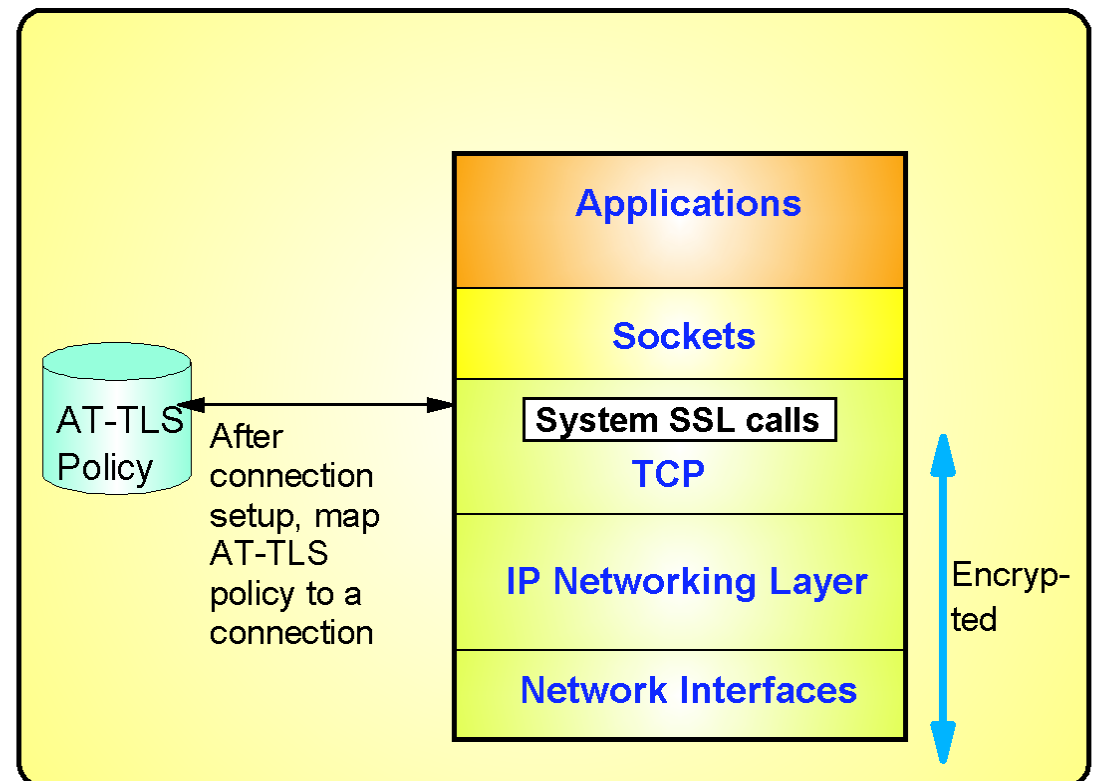
■ AT-TLS aware or controlling applications

- Application specific policy retained but reduced to what application needs for awareness or controlling functions
- AT-TLS policy continues to control overall AT-TLS function for the application

Mapping AT-TLS policy to a TCP Connection

- **An AT-TLS policy rule describes TLS requirements for a TCP connection**

- ▶ Policy rule is mapped to a connection based on policy condition
 - TCP/IP resource attributes
 - Connection type attributes
 - Local application attributes
- ▶ An AT-TLS policy rule is mapped to a connection at well defined points
 - Outbound Connect
 - First Select/Send/Receive
 - SIOCTLSCTL ioctl
- ▶ If a rule match is found, TCP/IP stack provides TLS protocol control based on the action
- ▶ Alternate method of mapping policy to a connection
 - Secondary Map



Secondary Connection Mapping

- **Alternate method of mapping policy to a connection**
 - ▶ Secondary Map
 - Used for applications that have one or more "secondary connections" and one "primary connection"
 - Used when it is difficult to write policy conditions for primary and secondary connections that match the same policy
- **Characteristic of these applications**
 - ▶ They use ephemeral or dynamically assigned ports for both ends of connections
 - ▶ Secondary connection is made after user identity has changed
 - e.g. forking applications such as FTP
- **Examples of application with secondary connections**
 - ▶ FTP
 - ▶ rsh, rexec, rlogin family of applications
- **For these applications write a policy condition for primary connection and designate that policy rule as "SecondaryMap".**
 - ▶ IP address pairs and the process ID for the active connection and policy rule priority are saved in a table when a policy rule with "SecondaryMap" is matched (during primary connection map)
 - ▶ If such a table of saved IP address pairs exist, it will be searched in addition to the normal policy search during policy map process
 - If two matches result, one with highest priority is used to map to policy for a secondary connection.

AT-TLS Policy Conditions

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

AT-TLS Policy Actions

Criteria	Description
TLS enablement	Specifies whether TLS is enabled for connection matching the policy rule
TLS/SSL versions allowed	SSLv2, SSLv3, TLSv1
Cipher suites	Set of potential cryptographic algorithms (in order of preference) that this TLS server or client will accept during the TLS handshake
Role	<ul style="list-style-type: none">• TLS client• TLS server• TLS server with client authentication
Client authentication type	<ul style="list-style-type: none">• Passthru (bypass checking)• Required• Full (Accepted if provided by client)• SAFCheck
Authentication information	<ul style="list-style-type: none">• Keyring identifier• Certificate label used for authentication• LDAP for certificate revocation list (CRL) processing
Data trace	Specifies whether to trace cleartext in datatrace or ctrace
AT-TLS trace levels	Specifies level of tracing
Handshake timeout	Time to wait for handshake to complete
Session key lifetime	When session key has been used this specified time period, a new session key must be created
Session ID requirements	Session ID cache size, Session ID timeout, Use sysplex-wide session ID cache
Secondary map used	Specifies whether a matching connection should be used as a "primary" connection in the "secondary policy mapping method"


z/OS Communications Server Network Security

AT-TLS Policy Configuration


Configuration Assistant for z/OS Communications Server



Configuration Assistant
for z/OS Communications Server
Version 1, Release 9



(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006, 2007. All Rights Reserved. U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.



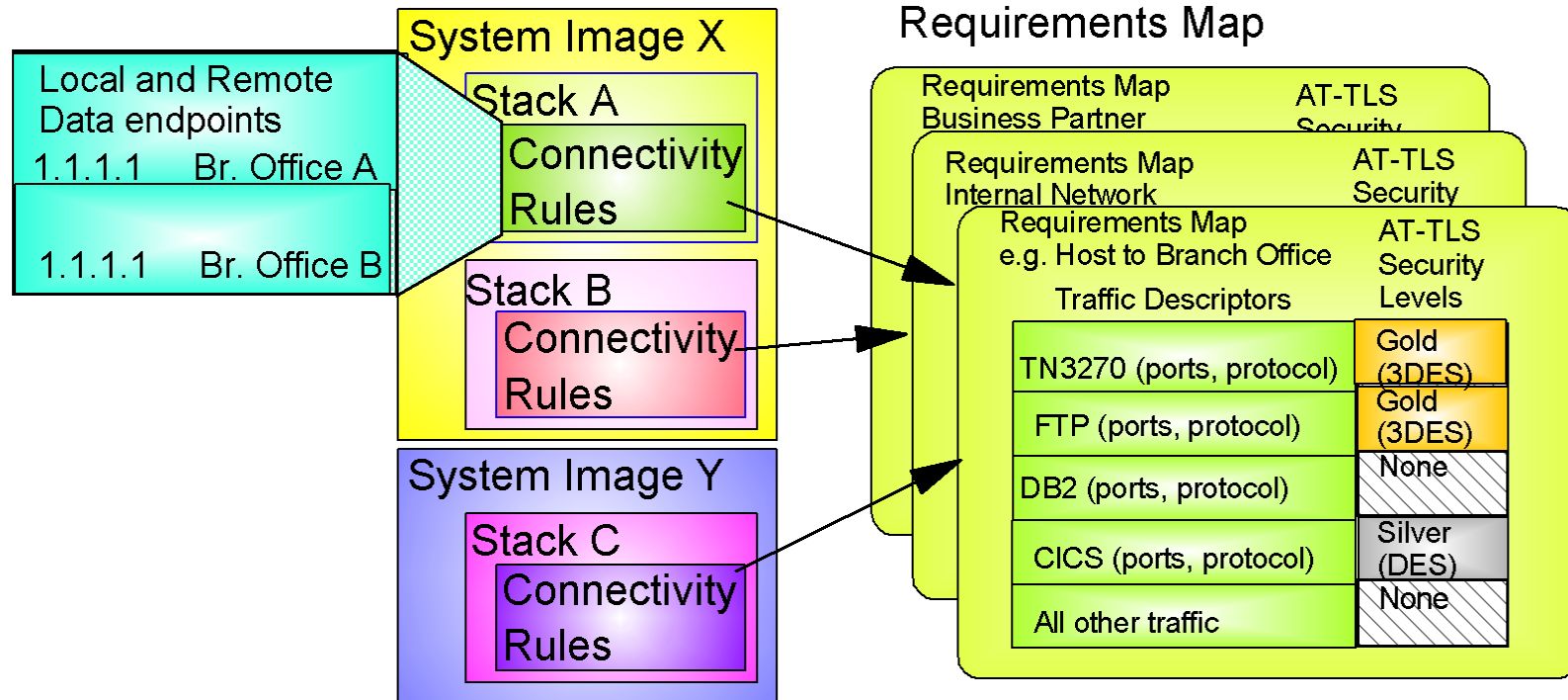
- ▶ **Policy Agent configuration tools are combined into one tool to manage policies for:**
 - ▶ AT-TLS
 - ▶ IPsec and IP filtering
 - ▶ IDS
 - ▶ QoS
 - ▶ Policy-based Routing (PBR) **(Added in V1R9)**
- ▶ **Common approach for all policy types:**
 - ▶ Master copy stored in binary file format on workstation, file server or, **added in V1R9**, on z/OS)
 - ▶ Text-based configuration files to be parsed by Policy Agent are created and transferred to z/OS

Downloadable policy configuration tool:

<http://www.ibm.com/software/network/commserver/zos/support/>

Configuration Assistant

Configuration Data Model



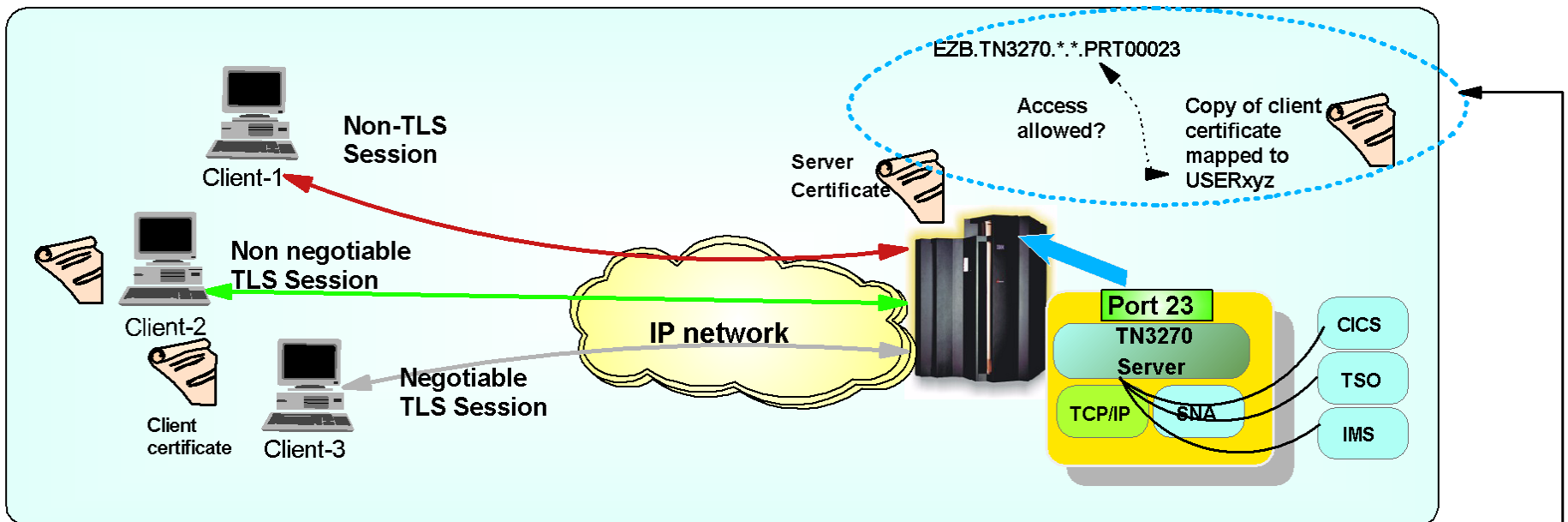
1. Define system images and TCP/IP stacks
2. Define security levels (reusable)
 - Protection suites (e.g. gold, silver, bronze)
3. Define traffic descriptors (reusable)
 - Represent applications and services
4. Define requirements map (reusable)
 - How to protect common scenarios (e.g. intranet, branch office, business partner)
 - Set of traffic descriptors linked to security level
5. Define connectivity rules
 - A complete security policy for all traffic between two endpoints
 - Specified data endpoints linked to a requirements map

- Wizards and dialogs guide you through a top-down approach to configuration
 - ▶ Navigational tree supports a bottom-up approach to allow an experienced user to bypass wizard screens

z/OS Communications Server Network Security

TLS Support for TN3270 and FTP

TLS-enabled TN3270



- **Protection of data in the network**

- ▶ Protects IP portion of data path ... from client into z/OS TN3270 server
- ▶ If needed, SNA portion of data path can be protected using SNA session level encryption (SLE)

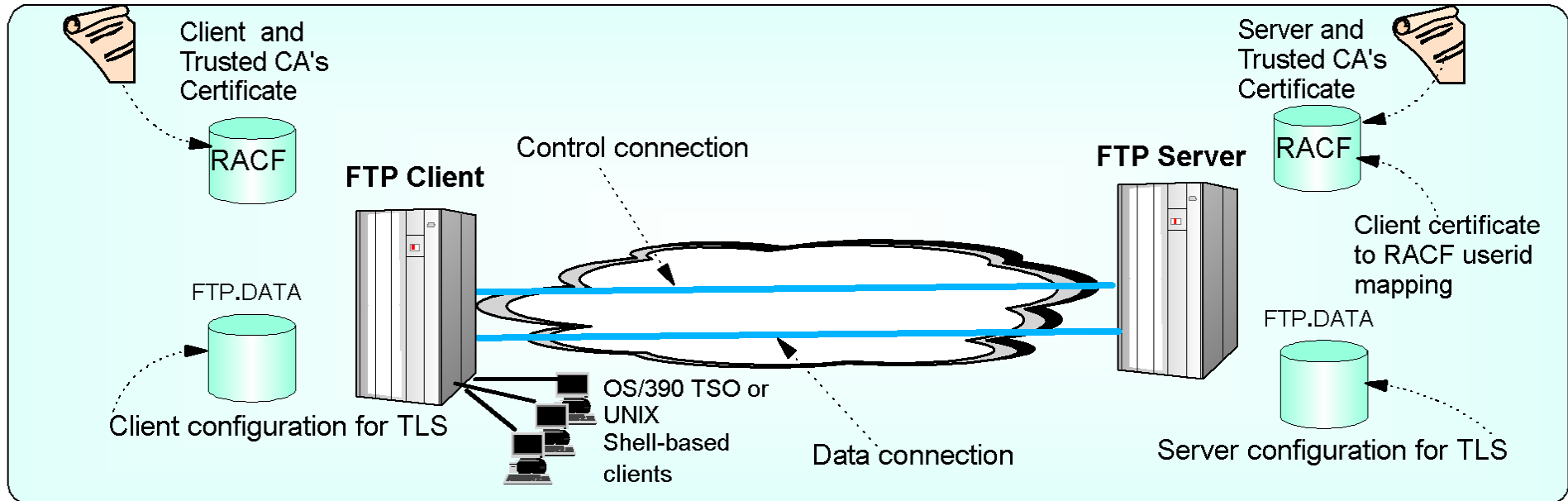
- **Optional levels of authentication based on TN3270 client certificate**

- ▶ TLS authentication of client certificate
- ▶ SAF verification of userid associated with client certificate authorized to access TN3270 port
 - Uses SERVAUTH class - Profile EZB.TN3270.sysname.tcpname.portxxx
- ▶ Use certificate for logon into SNA application without requiring userid/password
 - Express Logon Feature from PCOMM or HOD

- **Telnet profile configuration controls security policy for SSL session:**

- ▶ The PARMSGROUP and PARMSMAP statements controls which clients must use TLS, which clients may use TLS, and which clients are not allowed to use TLS at all.
- ▶ Whether unconditional or negotiable (or both) methods of TN3270 TLS are allowed
- ▶ Controls which ciphersuites are acceptable to TN3270 server.

TLS-enabled FTP



■ Key features

➤ Protection of data in the network

- Data origin authentication, data integrity, and privacy
- Can TLS protect control and data connection OR control connection alone
 - Data connection cannot be protected without control connection

➤ PKI based authentication of end users added. Options are:

- Basic - userid/password
- TLS authentication of client certificate
- SAF verification of userid associated with client certificate authorized to access FTP port
 - Uses SERVAUTH class - Profile EZB.FTP.sysname.ftpdemonname.portxxx
 - Cross-checking of userid entered with userid associated with client certificate
- Use certificate for logon without requiring password

➤ FTP.DATA configuration (server and client) controls security policy for TLS session

- TLS negotiation will find an agreeable policy or TLS setup will not proceed.
- Whether unconditional or negotiable methods of FTP TLS are allowed
- Controls which ciphersuites are acceptable to FTP server

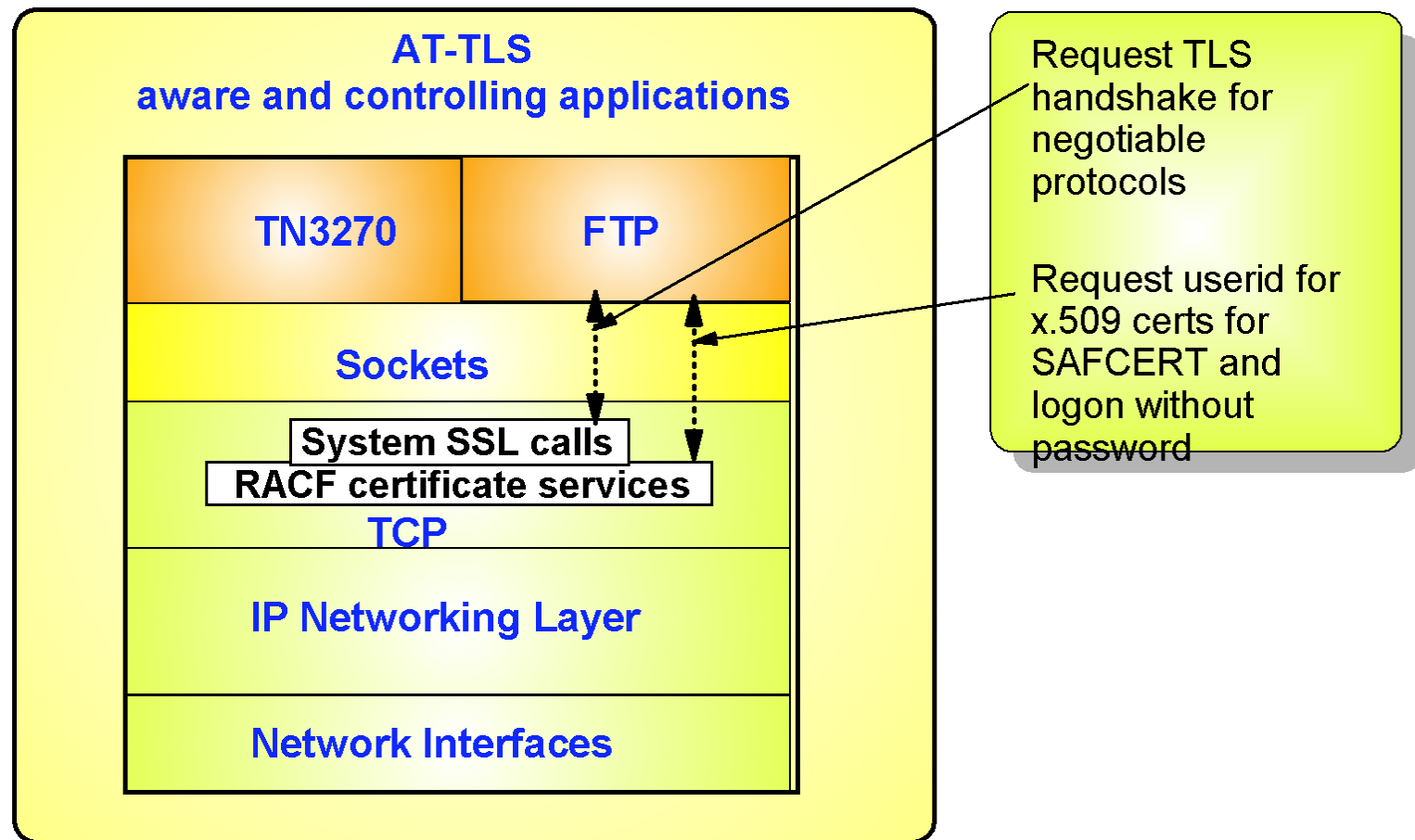
z/OS Communications Server Network Security

AT-TLS Enablement Support for TN3270 and FTP

AT-TLS enabling the TN3270 server and the FTP client and server

z/OS V1R9 Enhancement

- Both the TN3270 server, and the FTP server and client on z/OS have in the past implemented SSL/TLS support
 - ▶ With the advantages of AT-TLS, it is desirable to migrate that SSL/TLS support to AT-TLS
- In z/OS V1R9, TN3270 and FTP are enabled to be AT-TLS aware and controlling

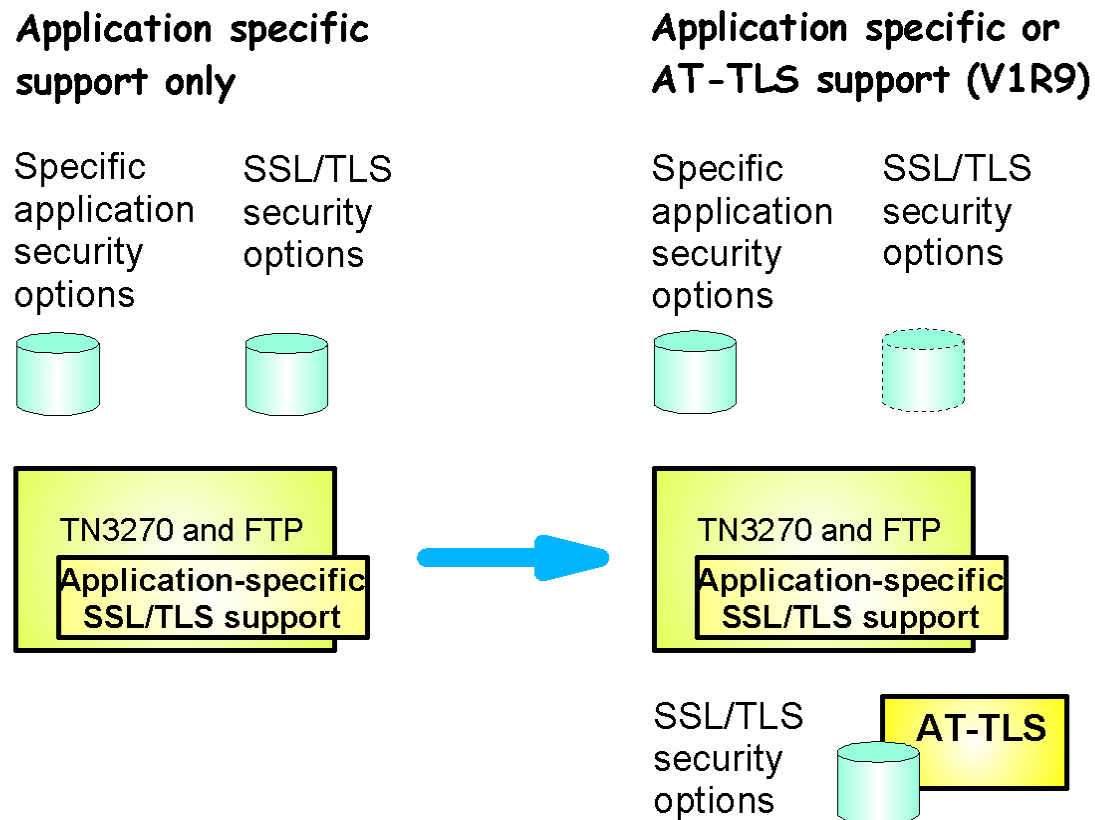


AT-TLS enabled TN3270 / FTP Benefits

- **By enabling TN3270 and FTP as AT-TLS aware and controlling applications, they automatically picks up new TLS functionality through AT-TLS:**
 - ▶ Support keyring refresh without stopping/starting server
 - ▶ Allow multiple keyrings per server
 - ▶ Allow specification of certificate labels other than the default certificate
 - ▶ Support multiple Certificate Revocation List (CRL) LDAP server specification
 - ▶ Support new ciphers added
 - ▶ Support sysplex-wide Session ID caching

AT-TLS common policy and application specific configuration handling

- Approach used for enabling TN3270 and FTP 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



AT-TLS enabling TN3270

- A new TN3270 server option to indicate use of AT-TLS instead of the TN3270 server's own system SSL calls is being implemented:

- ▶ 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 SSL/TLS 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 SSL/TLS support, and not AT-TLS for the specified port number)
- ▶ CONNTYPE
 - SECURE
 - NEGTSURE
 - ANY
 - BASIC
- ▶ EXPRESSLOGON
- ▶ RESTRICTAPPL CERTAUTH

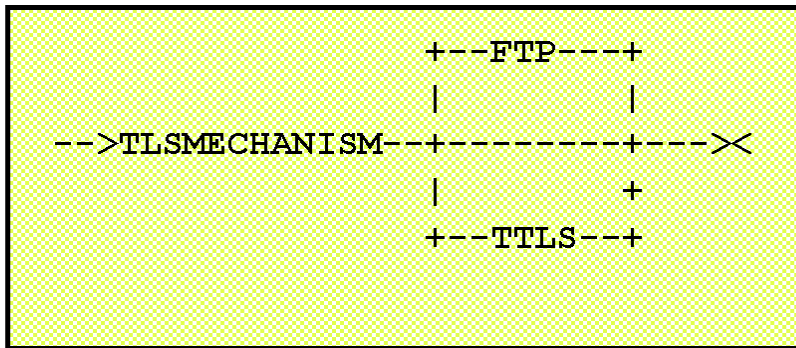
- TN3270 SSL/TLS security options

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

AT-TLS enabling FTP

- A new **FTP.DATA** option to instruct the FTP server or client to use AT-TLS instead of FTP's own system SSL calls are implemented:

- ▶ **TLSMECHANISM** (Client and Server)



■ FTP-specific security options:

- ▶ **EXTENSIONS AUTH_TLS** (Server)
- ▶ **SECURE_CTRLCONN** (Client and Server)
- ▶ **SECURE_DATACONN** (Client and Server)
- ▶ **SECURE_FTP** (Client and Server)
- ▶ **SECURE_HOSTNAME** (Client)
- ▶ **SECURE_LOGIN** (Server)
- ▶ **SECURE_MECHANISM** (Client)
- ▶ **SECURE_PASSWORD** (Server)
- ▶ **SECUREIMPLICITZOS** (Client)
- ▶ **TLSPORT** (Client and Server)

■ When TTLS is specified as TLS mechanism:

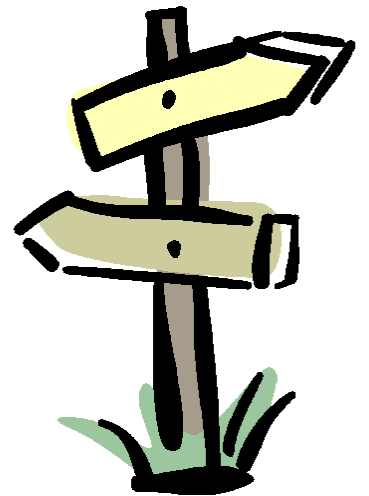
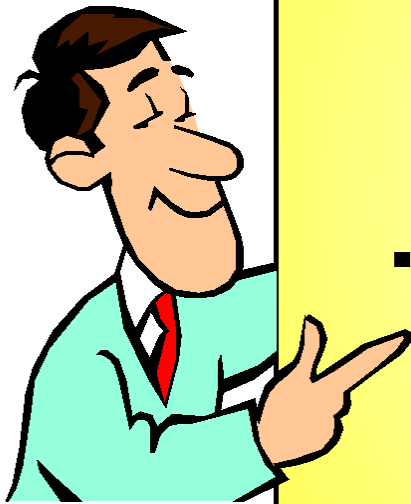
- ▶ FTP becomes an AT-TLS controlling and AT-TLS aware application
- ▶ All the FTP-specific security options will continue to impact how FTP operates
- ▶ The SSL/TLS security options in **FTP.DATA** will be ignored.
 - Matching AT-TLS policies need to be defined before enabling AT-TLS support in FTP

■ FTP SSL/TLS security options

- ▶ **CIPHERSUITE** (Client and Server)
- ▶ **KEYRING** (Client and Server)
- ▶ **TLSTIMEOUT** (Client and Server)

Agenda

- Part 1
 - ▶ TLS and AT-TLS Concepts
 - ▶ TLS enabled TN3270 and FTP
 - ▶ AT-TLS enabled TN3270 and FTP
- Part 2
 - ▶ Configuring AT-TLS for TN3270 and FTP



For More Information...

URL	Content
http://www.ibm.com/servers/eserver/zseries	IBM eServer zSeries Mainframe Servers
http://www.ibm.com/servers/eserver/zseries/networking	Networking: IBM zSeries Servers
http://www.ibm.com/servers/eserver/zseries/networking/technology.html	IBM Enterprise Servers: Networking Technologies
http://www.ibm.com/software/network/commserver	Communications Server product overview
http://www.ibm.com/software/network/commserver/zos	z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin	Communications Server for Linux on zSeries
http://www.ibm.com/software/network/ccl	Communication Controller for Linux on zSeries
http://www.ibm.com/software/network/commserver/library	Communications Server products - white papers, product documentation, etc.
http://www.redbooks.ibm.com	ITSO redbooks
http://www.ibm.com/software/network/commserver/support	Communications Server technical Support
http://www.ibm.com/support/techdocs/	Technical support documentation (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)
http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp	IBM Education Assistant