

Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

Application Transparent – Transport Layer Security (AT-TLS)



IBM Washington System Center
IBM Technical Sales Support

Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
 - **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
 - All other products may be trademarks or registered trademarks of their respective companies.
 - Refer to www.ibm.com/legal for further legal information.
-
- OSA-Express Features
 - There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express features unless a specific OSA-Express feature is mentioned.

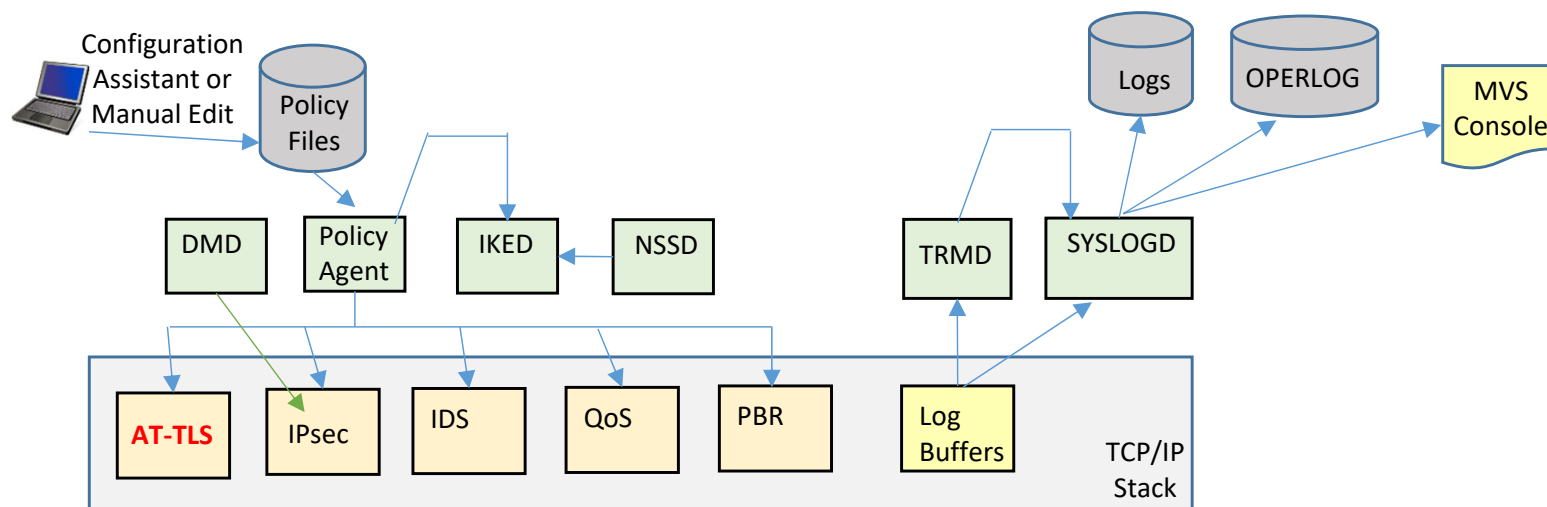
Agenda

- TLS Protocol
- Authentication and Encryption
- AT-TLS Usage
- Network Configuration Assistant for z/OS Communications Server
- Policy Rules and Policy Actions
- FIPS 140
- Error Codes and Commands

TLS Protocol

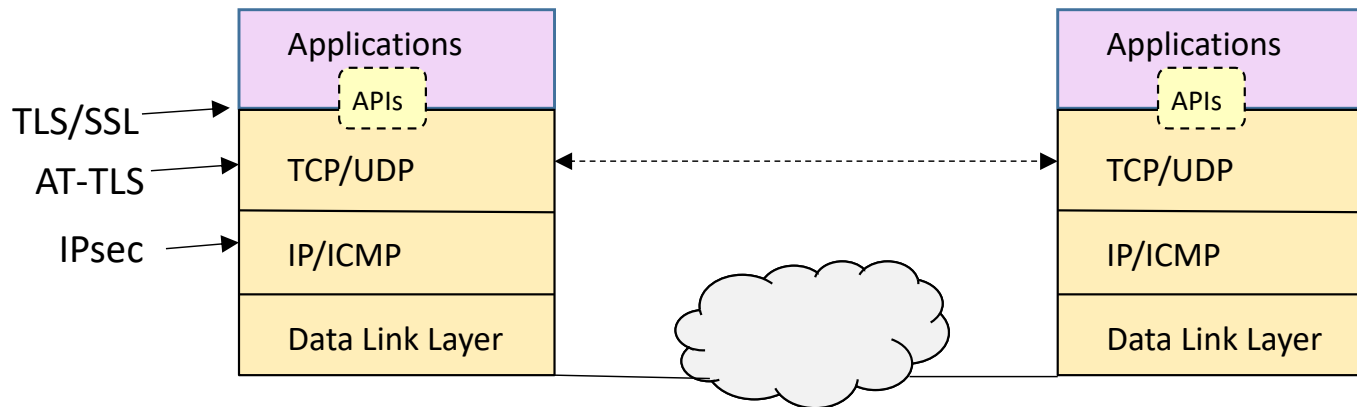


Lots of Different Policy Types and Started Tasks



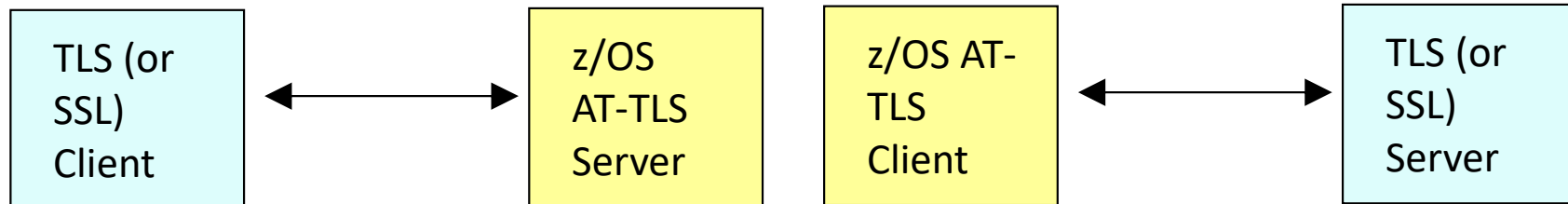
- Policy Agent
 - Installs Policies into the TCP/IP stack
- TCP/IP Stack
 - Enforces the Policies
- DMD (Defense Manager Daemon)
 - ipsec command can be used to install temporary IP Filter rules.
- IKED (Internet Key Exchange Daemon)
 - Required for IPsec Dynamic VPN (Virtual Private Network) Tunnels
- NSSD (Network Security Server Daemon)
 - Required for IKEv2
 - Provides central RACF certificate repository for remote IKED applications
 - Provides DataPower access to RACF
- TRMD (Traffic Regulation Management Daemon)
 - Required for log messages to syslogd for IP Filter, IPsec, and IDS
- SyslogD
 - Recommended for logging

Transport Layer Security (TLS) Protocol Overview



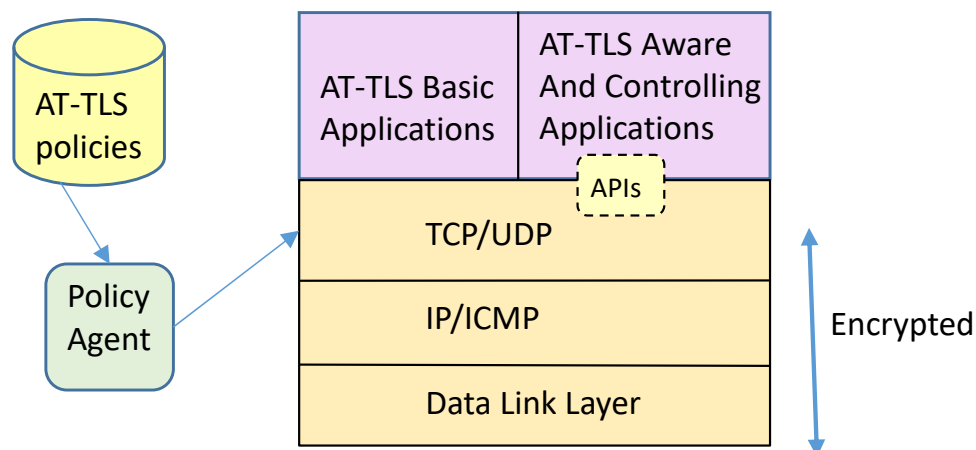
- Open standard transport layer security protocol defined by IETF in RFCs
- Provides authentication, integrity, and data privacy
- Based on Secure Sockets Layer (SSL)
- SSL originally defined by Netscape to protect HTTP traffic
- TLS defines SSL as a version of TLS for compatibility
 - TLS clients and server should drop to SSL V3 based on partner's capabilities
- TCP only
 - UDP, raw IP applications cannot be TLS enabled
- z/OS applications can be modified to support TLS
- Uses System SSL
 - System SSL is part of z/OS Cryptographic Services element
- TLS can be used with no application change by exploiting AT-TLS

AT-TLS is TLS



- AT-TLS happens to be “where” IBM has chosen to implement TLS for various reasons:
 - Consistency between different applications.
 - Support to applications that have not implemented TLS/SSL.
 - Saves development costs.
- AT-TLS is still just seen as a TLS Server or Client to the remote partner.
 - The remote partner sees z/OS as any other TLS or SSL partner.
 - The remote partner still needs to support TLS or SSL.
- TLS, AT-TLS, and SSL use System SSL Support
 - Without System SSL Security Feature Level 3
 - Connections across secure ports are protected only by way of MD5 or SHA hashing algorithms
 - With System SSL Security Feature Level 3
 - Encryption support by way of RC2, RC4, DES, triple DES, AES, etc.
- System SSL Security Feature Level 3
 - Part of z/OS Integrated Security Services element.
 - No charge item but separately orderable feature (export restrictions).
 - TCP/IP must have APF authorized access to the System SSL DLLs (in hlq.SGSKLOAD).

Application Transparent - Transport Layer Security (AT-TLS)



Application Specific TLS FTP.DATA Parameters	Application Specific TLS TN3270 Parameters	AT-TLS
Server Authentication TLSMECHANISM FTP	Server Authentication SECUREPORT	Basic Application FTP.DATA TLSMECHANISM ATTLS TN3270 Profile TTLSPT
Client Authentication SECURE_LOGIN REQUIRED	Client Authentication CLIENTAUTH SSLCERT	Basic Application
SECURE_LOGIN VERIFY_USER SECURE_PASSWORD OPTIONAL	CLIENTAUTH SAFCERT	Aware Application
SECURE FTP ALLOWED	CONNTYPE NEGTSURE CONNTYPE ANY	Controlling Application

- 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
- AT-TLS Basic applications
 - For Server Only Authentication or Server with “plain” Client Authentication there is no application change required.
- AT-TLS Aware applications
 - Applications can optionally exploit advanced features using SIOCTTLSCTL ioctl call.
 - Required for Client Authentication Advanced Features.
 - Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)
- AT-TLS Controlling applications
 - Required for a single port to concurrently connect to unsecure clients and secure clients
 - Control if/when to start/stop TLS, reset session/cipher

AT-TLS Advantages

- Reduces development costs for application TLS exploitation
 - Support of new System SSL functions without application changes
- Single, consistent AT-TLS policy system-wide vs. application specific policy
- Allows TLS-enablement of non-C sockets applications on z/OS (ie. CICS sockets, assembler and callable sockets, etc.)
- Exploits TLS features beyond what some TLS applications choose to support
 - Certificate Revocation List (CRL)
 - Multiple keyrings per server
 - System SSL cache
 - Support for non-DEFAULT certificate by use of LABEL name
 - TLS V1.1 and later
 - FIPS 140 mode
 - RFC 3820 certificate validation
 - RFC 3546 TLS extensions:
 - Truncated HMAC
 - Maximum SSL fragment size
 - Handshake server name indication
 - Ongoing performance improvements

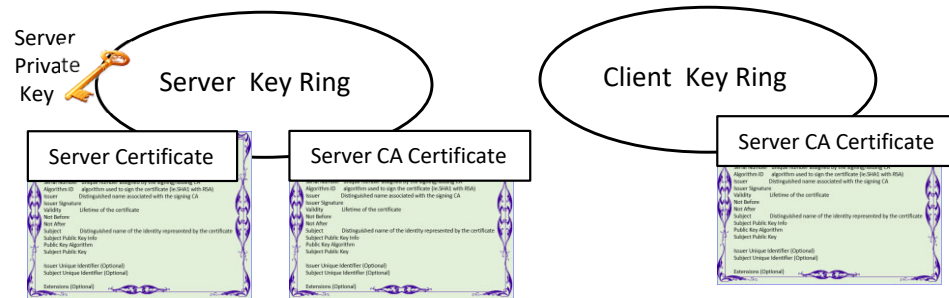
Authentication and Encryption



Key Ring Contents

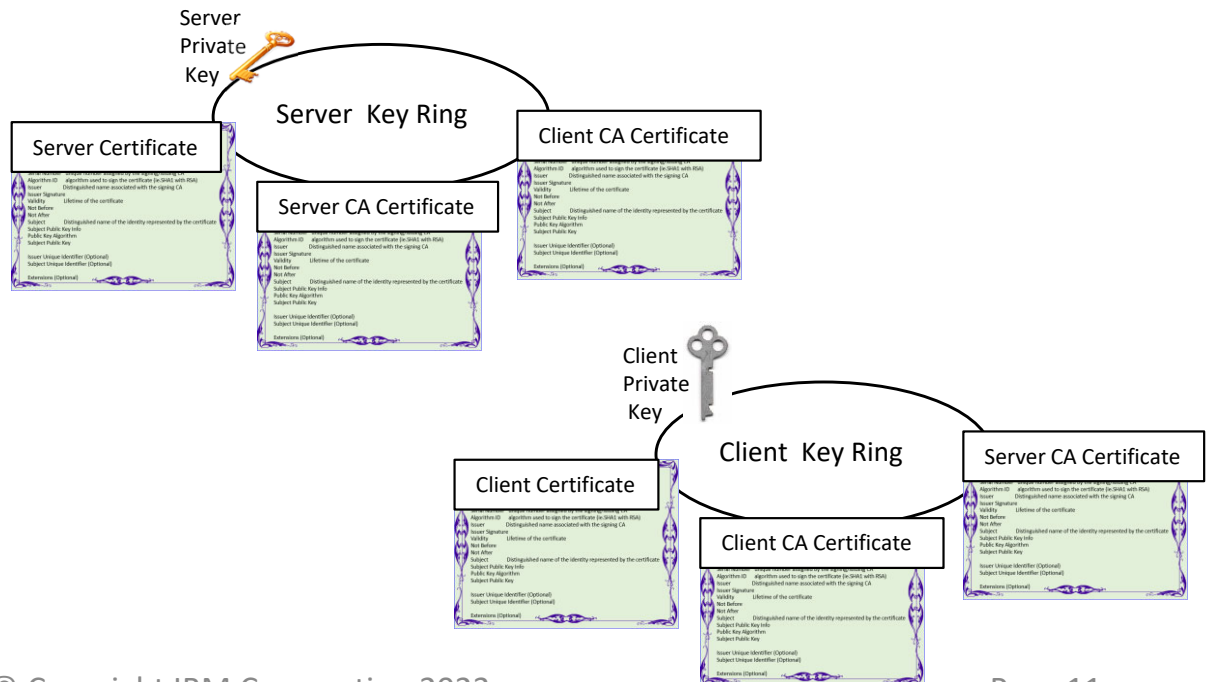
- AT-TLS Server Authentication is required.

- Server
 - Server Certificate
 - Server Private Key
 - Server CA Certificate
- Client
 - Server CA Certificate

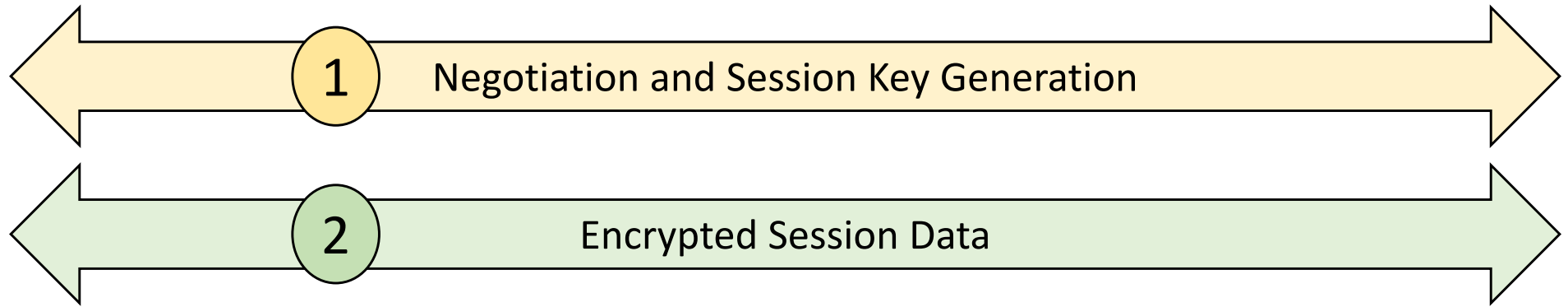


- AT-TLS Client Authentication is optional.

- Server
 - Server Certificate
 - Server Private Key
 - Server CA Certificate
 - Client CA Certificate
- Client
 - Client Certificate
 - Client Private Key
 - Client CA Certificate
 - Server CA Certificate



General Architecture of Encryption Flow



Encryption Flow	What Happens	SSL/TLS Terminology	IPsec Terminology	OpenSSH Terminology
Stage 1 Asymmetric Algorithms	Negotiation of Secure Connection: Authentication and Generation of and encrypted Transmit of Session Key	Handshake Layer	Phase I Phase II	No official terminology; just negotiation stage
Stage 2 Symmetric Algorithms	Encryption and Decryption of Data Payload (Session Data)	Record Layer	Phase II Tunnel	No official terminology, just data transfer stage

- Essentially all these security protocols use the same basic architecture:

- 1 Authenticate the partner; generate a symmetric key
 - Encrypt symmetric key with asymmetric algorithm and send
- 2 Encrypt session data with symmetric ("Session") key and transmit session data

- Two Stages

- Phase 1 Negotiation / Key Generation

- Handshake Layer

- Authenticates Server (and Optionally Client) and generates Session Key

- Uses ICSF or Crypto Card if available
 - Accelerator Card (Clear Key Mode)
 - Coprocessor Card (Secure Key Mode)

Cryptographic
Cards
(Accelerator or
Coprocessor)

CPACF

Software

GP
Processor

- Phase 2

- Record Layer

- Encrypts/Decrypts data

- Uses CPACF (clear key only) if available

CPACF

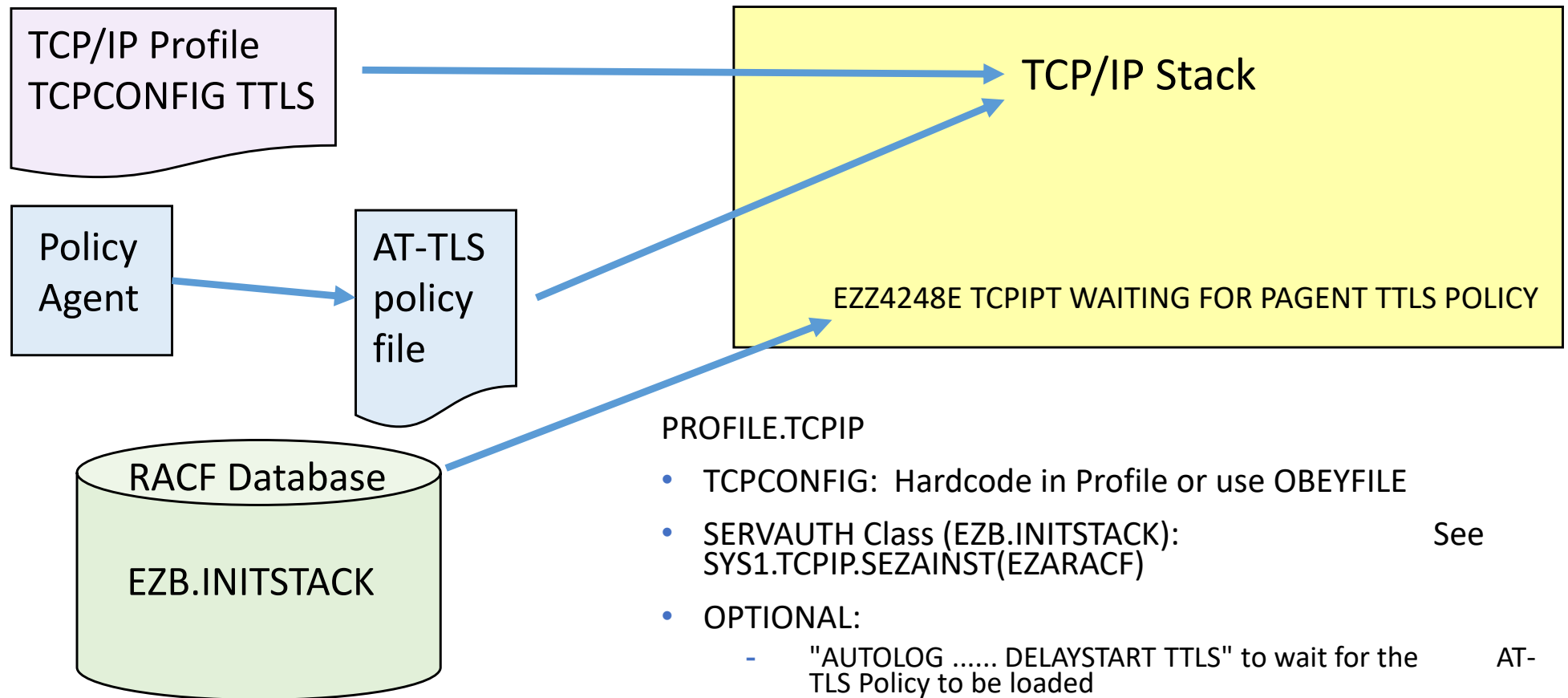
Software

GP
Processor

AT-TLS Usage



Enable TCP/IP Stack for AT-TLS



- Reduce AT-TLS overhead by adding this to the TCP/IP proc:

`//CEEOPTS DD * HEAPPOOLS64(ON)`

RACF Sample

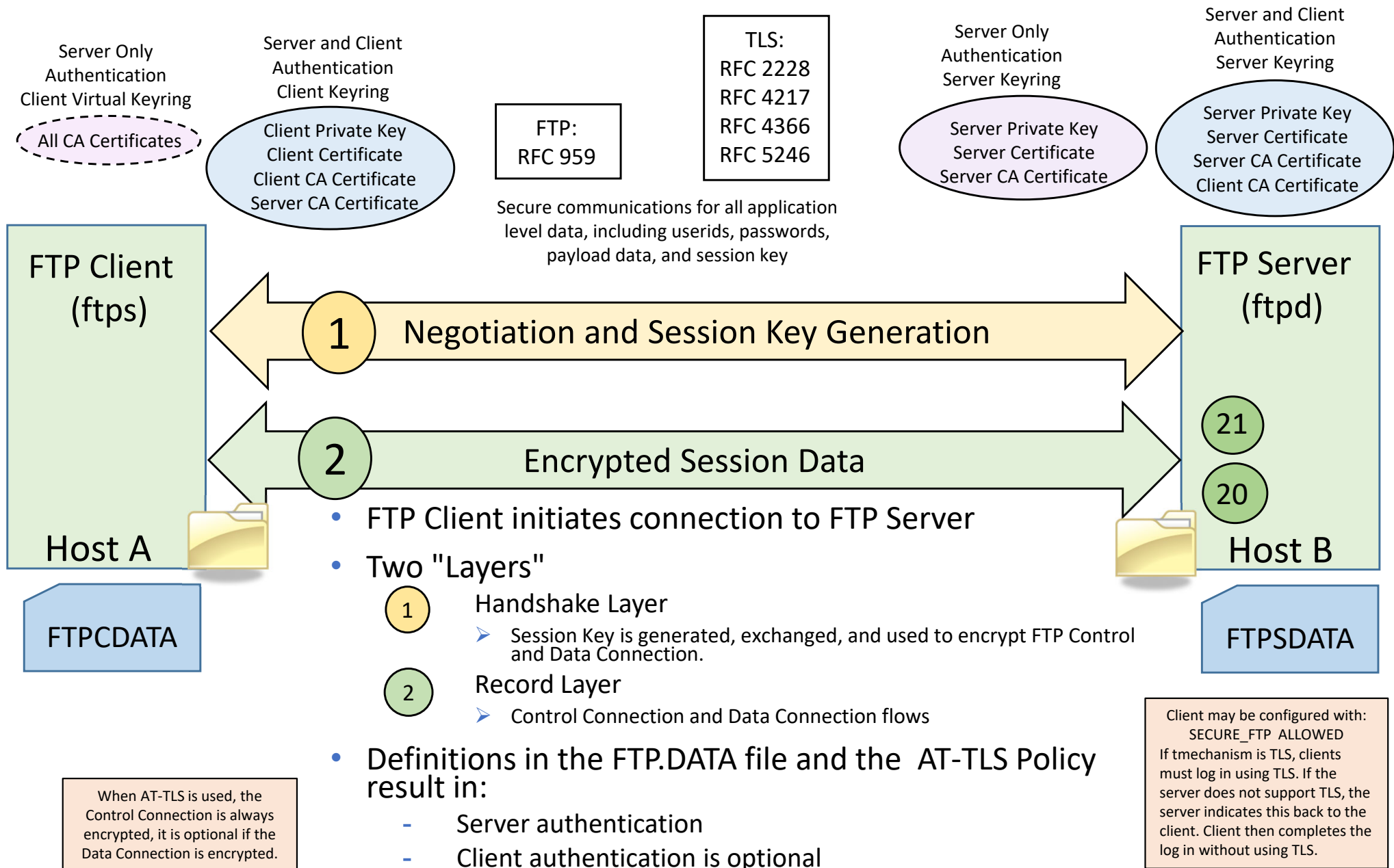
- SYS1.TCPIP.SEZAINST(EZARACF)

```
...
/*INITSTAC EXEC PGM=IKJEFT01
/*SYSTSPRT DD SYSOUT=*
/*SYSTSIN DD *
/* SETROPTS CLASSACT(SERVAUTH)
/* SETROPTS RACLIST (SERVAUTH)
/* SETROPTS GENERIC (SERVAUTH)
/* RDEFINE SERVAUTH EZB.INITSTACK.sysname.tcpprocname UACC(NONE)
/* PERMIT EZB.INITSTACK.sysname.tcpprocname -
/* CLASS(SERVAUTH) ID(PAGENT) ACCESS(READ)
/* PERMIT EZB.INITSTACK.sysname.tcpprocname -
/* CLASS(SERVAUTH) ID(OMPROUTE) ACCESS(READ)
/* PERMIT EZB.INITSTACK.sysname.tcpprocname -
/* CLASS(SERVAUTH) ID(OSNMPD) ACCESS(READ)
/* PERMIT EZB.INITSTACK.sysname.tcpprocname -
/* CLASS(SERVAUTH) ID(IOBSNMP) ACCESS(READ)
/* PERMIT EZB.INITSTACK.sysname.tcpprocname -
/* CLASS(SERVAUTH) ID(NAMED) ACCESS(READ)
/* PERMIT EZB.INITSTACK.sysname.tcpprocname -
/* CLASS(SERVAUTH) ID(IKED) ACCESS(READ)
/* SETROPTS GENERIC(SERVAUTH) REFRESH
/* SETROPTS RACLIST(SERVAUTH) REFRESH
/*
...
```

SETROPTS CLASSACT(SERVAUTH)
EZB.INITSTACK.sysname.tcpname
PERMIT EZB.INITSTACK.sysname.tcpname CL(SERVAUTH) ID(userid)
At a minimum, the following applications must be permitted to the profile:
Policy Agent
OMPROUTE
SNMP subagent

SERVAUTH class EZB.INITSTACK prevents TCP/IP stack access until after the Policy Agent has come up and installed the AT-TLS policies. PERMIT must be defined for the Policy Agent and any other applications that need access to the stack prior to policy load.

Secure FTP with TLS (and SSL and AT-TLS)

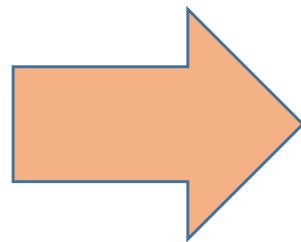
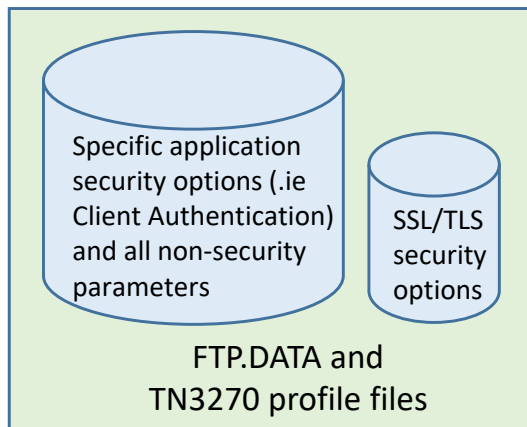


AT-TLS Enabling for TN3270 and FTP

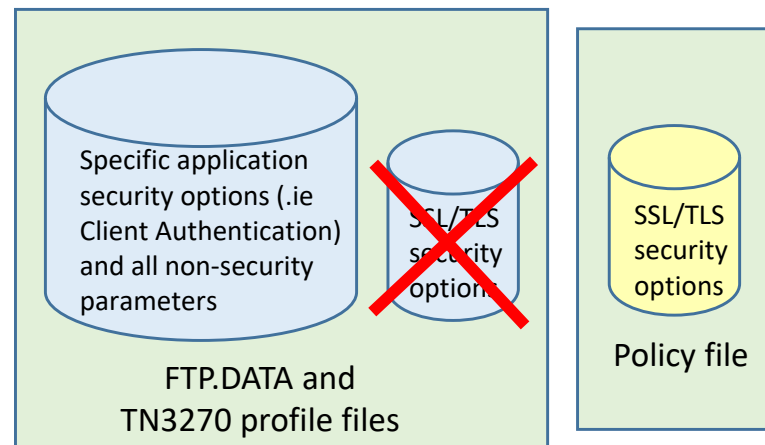
- Both the FTP server and client, and the TN3270 server on z/OS currently (and prior to AT-TLS) have “application specific” SSL/TLS support.
 - With the advantages of AT-TLS, it is desirable to migrate that SSL/TLS support to AT-TLS.
- FTP and TN3270 are enabled for AT-TLS to be AT-TLS “Aware” and “Controlling” applications.
- "Move" the SSL/TLS-specific configuration from FTP.DATA and TN3270 profile into the common AT-TLS policy format.
- Keep application-specific security options in FTP.DATA and TN3270 profile application configuration files.

TN3270 and FTP native TLS removed in z/OS V2.5.

“Application Specific” TLS Support



AT-TLS Support



Enabling FTP for AT-TLS

- FTP Server and Client

FTP.DATA

Some Security Statements Remain:

EXTENSIONS AUTH_TLS (Server only)
SECURE_CTRLCONN (Client and Server)
SECURE_DATACONN PRIVATE (Client and Server)
SECURE_FTP REQUIRED (Client and Server)
SECURE_HOSTNAME (Client only)
SECUREIMPLICITZOS (Client and Server)
SECURE_LOGIN (Server only)
SECURE_MECHANISM TLS (Client only)
SECURE_PASSWORD (Server only)
SECURE_PBSZ (Client and Server)
SECURE_SESSION_REUSE (Client and Server)
TLSMECHANISM ATTLS (Client and Server)
TLSPORT (Client and Server)
TLSRFCLEVEL RFC4217 (Client and Server)

Some Security Statements can be removed,
because they are defined in Policy:

CIPHERSUITE (Client and Server)
KEYRING (Client and Server)
TLSTIMEOUT (Client and Server)

Enabling TN3270 for AT-TLS

TN3270 Profile TELNETPARMS

PORT port_num or
SECUREPORT port_num must be changed to:
TTLSPORT port_num

Some Security Statements Remain:

CONNTYPE SECURE | NEGTCURE ...

DEBUG CONN DETAIL

EXPRESSLOGON

EXPRESSLOGONMFA

RESTRICTAPPL CERTAUTH

Some Security Statements can be removed,
because they are defined in Policy:

ENCRYPTION

KEYRING

TLSTIMEOUT, SSLTIMEOUT

CRLLDAPSERVER

CLIENTAUTH SSLCERT | SAFCERT

SSLV2 | NOSSLV2

SSLV3 | NOSSLV3

- TTLSPORT signifies AT-TLS for this port
 - You may use SECUREPORT on other ports
- When first testing, optionally enable DEBUG CONN
- BEGINVTAM remains unchanged.

Network Configuration Assistant for z/OS Communications Server



AT-TLS in Configuration Assistant

The screenshot displays the IBM z/OS Management Facility Configuration Assistant interface. The main window shows the 'New Connectivity Rule' configuration page, specifically the 'Data Endpoints' section. The breadcrumb navigation indicates the path: Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule. The 'Data Endpoints' section is divided into 'Local data endpoint' and 'Remote data endpoint'. Both sections have a radio button for 'Address group' (selected) and a dropdown menu set to 'All_IPv4_Addresses'. Below each, there is a radio button for '* IPv4 or IPv6 address, subnet, or range:' which is currently unselected. Examples of address formats are provided for both endpoints. The interface includes a left-hand navigation pane with categories like Welcome, Notifications, Workflows, Configuration, Links, Performance, z/OS Classic Interfaces, and z/OSMF Settings. A 'Refresh' button is visible at the bottom of the left pane. The top of the window shows the user 'zmfusr1' and a 'Log out' button. The browser window title is 'IBM z/OS Management Facility' and the URL is 'https://9.82.24.224/zosmf/'.

IBM z/OS Management Facility

Welcome zmfusr1

Log out IBM

Welcome x Configuratio... x

Help

Welcome to

Use this task to

Select a back

saveData

Learn more a

What's New

Getting Starte

Migrating to z

Tutorials

FAQs

Refresh

IBM z/OS Management Facility

Welcome harrisl

Log out IBM

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

Help

New Connectivity Rule

Data Endpoints

Requirement Map

Advanced Settings

* Connectivity rule name:

0

Select the address groups of the host endpoints of the traffic you want to protect.

Local data endpoint

Address group:

All_IPv4_Addresses

* IPv4 or IPv6 address, subnet, or range:

Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y
x::x, x::x/yyy, x::x-y::y

Remote data endpoint

Address group:

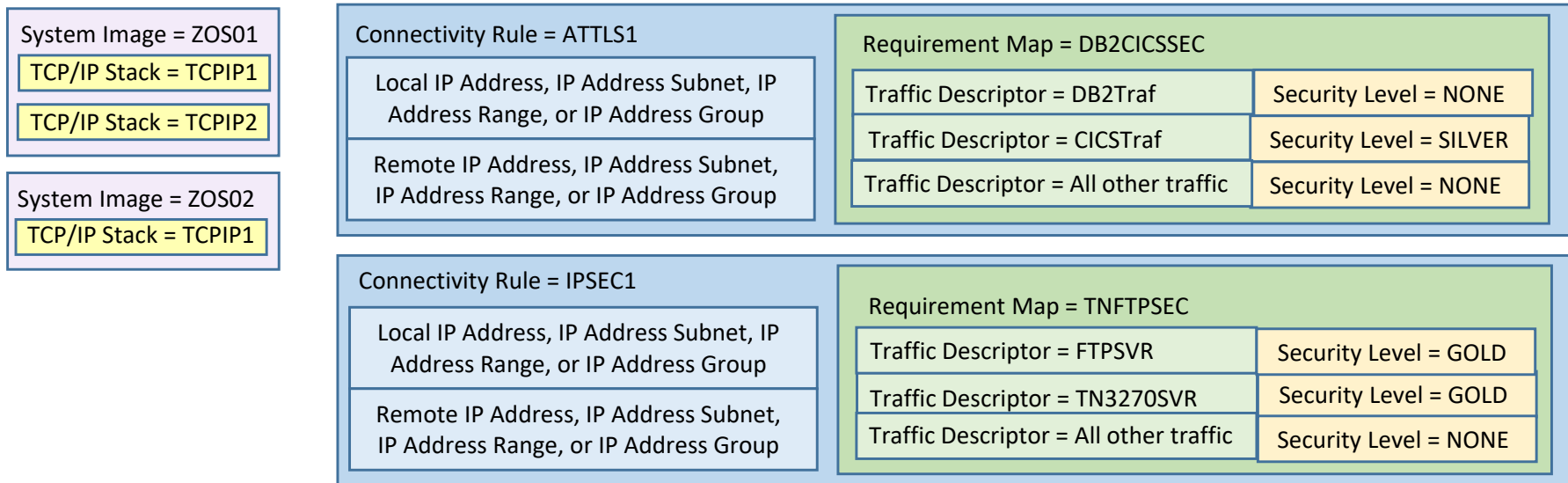
All_IPv4_Addresses

* IPv4 or IPv6 address, subnet, or range:

Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y
x::x, x::x/yyy, x::x-y::y

< Back Next > Finish Cancel

AT-TLS and IPsec



- 1 Define Sysplex Group or use the “Default” group
- 2 Define system images (z/OS systems) and TCP/IP stacks
- 3 Select Type of Policy (AT-TLS or IPsec)
 - Define connectivity rules
 - Complete security policy for all traffic between two endpoints
- 6 Specify IP Addresses for data endpoints (IP Address Groups Reusable)
- 7 Define Requirements maps (reusable)
 - Maps a set of Traffic Descriptors to Security Levels
- 4 Define Traffic Descriptors (reusable)
- 5 Define Security Levels (reusable)

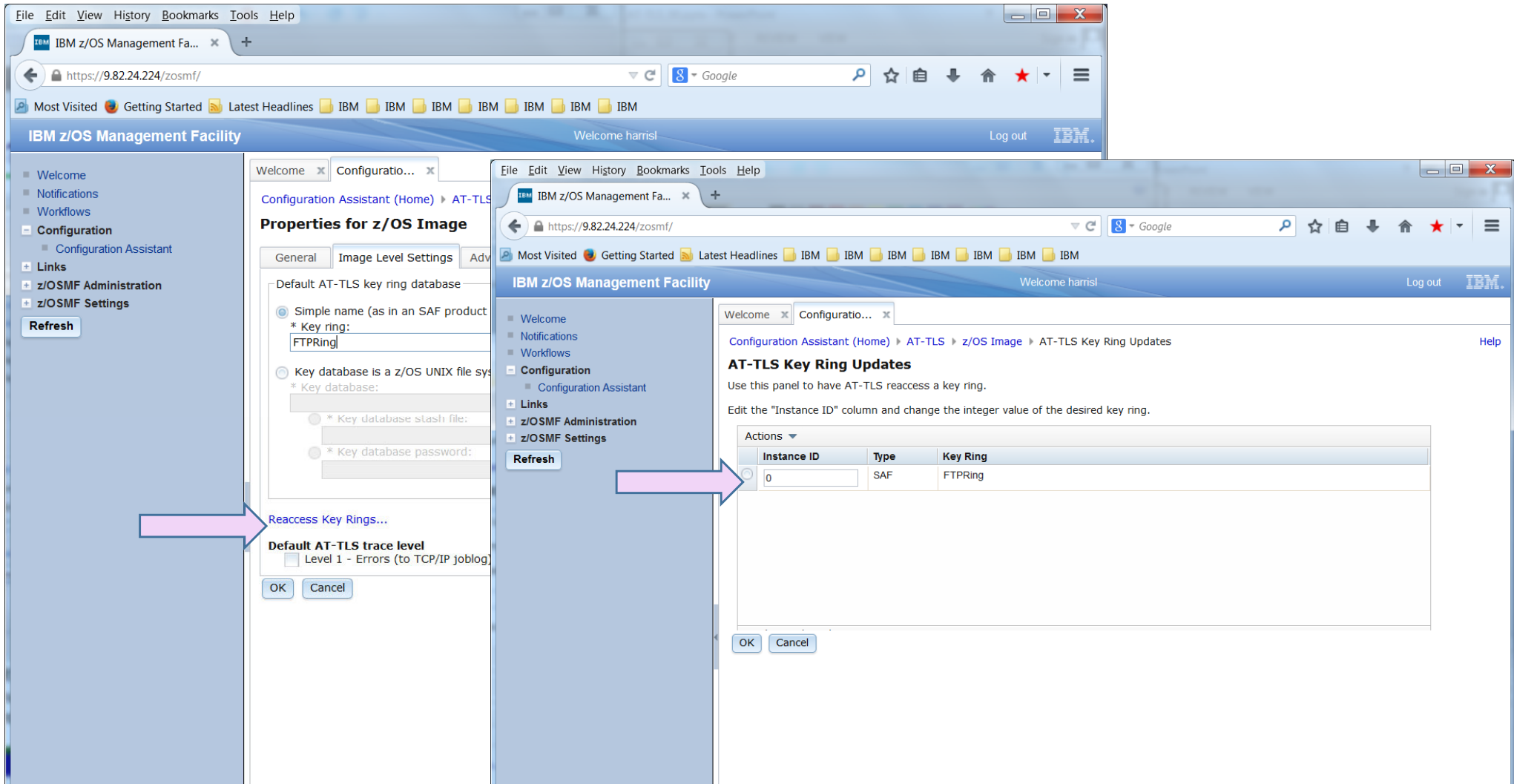
Policy Rules and Policy Actions



Policy Definition

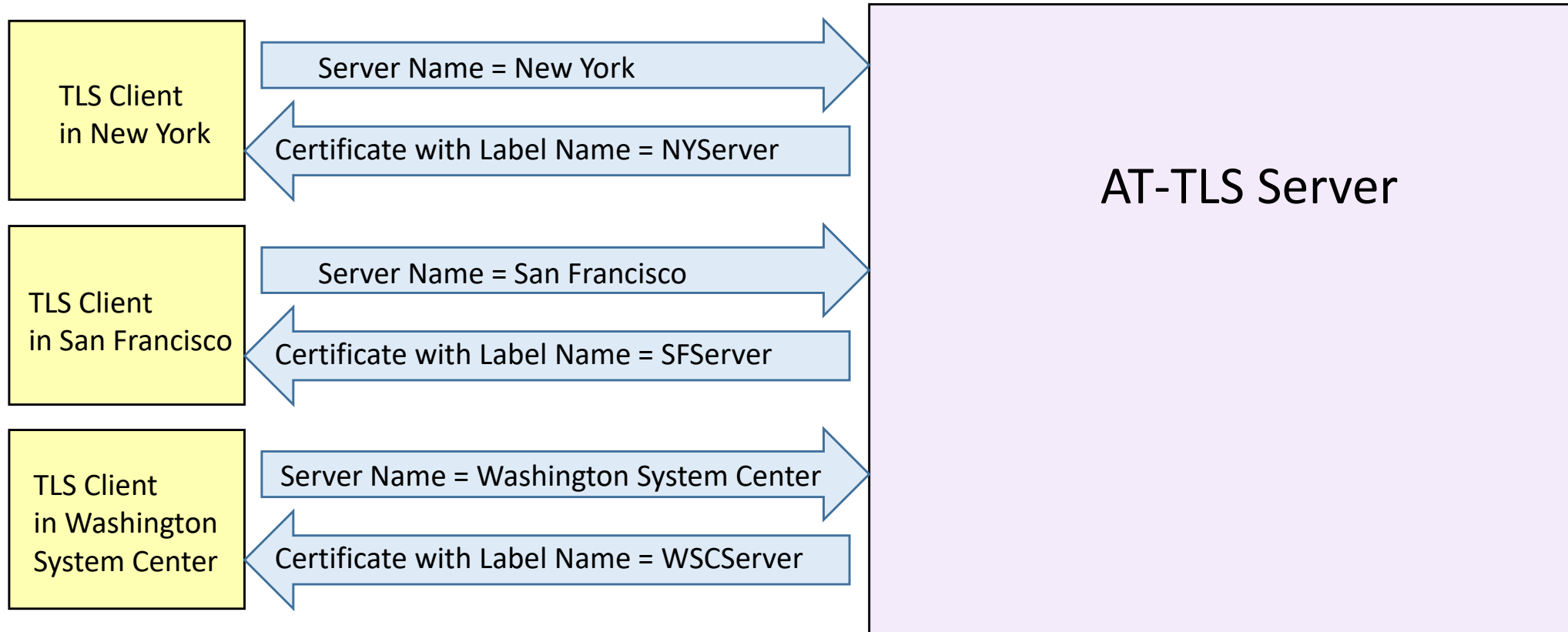
Criteria	Description
Resource Attributes	
Local address	Local IP Address
Remote address	Remote IP Address
Local port	Local Port
Remote port	Remote Port
Connection Type Attributes	
Connection direction	<ul style="list-style-type: none">• Inbound (applied to first Select, Send, or Receive after Accept)• 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.
Action	
Encryption Algorithm	Which encryption algorithm to use.
Hashing Algorithm	Which hashing algorithm to use.
Client Authentication	Designates whether Client Authentication is Required or Not

Keyring Changes



- Directly edit flat file:
 - TTLSEnvironment Action
 - EnvironmentUserInstance 7 <<<<<<<<<<(ie., changed from 6)

Server Name Indication



- The server matches the server name provided by the client with a certificate label and sends that certificate to the client (RFC4366).

FIPS 140



FIPS 140 Requirements

- You can configure AT-TLS to support FIPS 140.
 - Specify On for the FIPS140 statement of the TTLSGroupAction statement, or
 - Specify on a Configuration Assistant panel
- Understand System SSL Restrictions for FIPS 140
 - Consult z/OS System SSL Programming Guide
 - Restricted to specific encryption and hashing algorithms
 - No DES, no MD5, etc...
 - SSL V2 and SSL V3 are not supported.
 - System SSL requires Security Level 3 FMID (JCPT3C1)
 - Recommended: Initialize ICSF

System SSL Algorithm Support for FIPS 140

Non-FIPS					FIPS			
Algorithm	Sizes	System SSL software	Direct calls to CPACF	Support through ICSF	Sizes	System SSL software	Direct calls to CPACF	Support through ICSF
3DES	168	X	X		168	X	X	
AES	128 and 256	X	X		128 and 256	X	X	
AES-GCM	128 and 256			X	128 and 256			X
DES	56	X	X					
DH	512-2048	X			2048			X
DSA	512-2048	X			1024-2048	X		
ECC Brainpool	160-521			X				
MD5	48	X						
NIST ECC	192-521				192-521			X
RC2	40 and 128	X						
RC4	40 and 128	X						
RSA	512-4096	X		X	1024-4096	X		X
RSASSA-PSS	2048-4096			X	2048-4096			X
SHA-1	160	X	X		160	X	X	
SHA-2	224, 256, 384, and 512	X	X		224, 256, 384, and 512	X	X	

See z/OS Cryptographic Services System Secure Sockets Layer Programming, SC14-7495, for the latest support.

Error Codes and Commands



AT-TLS Error Codes

- Return codes between 5001 and 5999 describe AT-TLS errors that can be corrected by the user.
- Return codes between 6001 and 6999 describe internal AT-TLS errors.
- Table 53 lists some common System SSL return codes and possible causes.

Table 53 Common System SSL return codes

Return code	Event	Possible cause and solution
202	Environment Init	<p>The key ring cannot be opened because the user does not have permission. Check the following:</p> <ul style="list-style-type: none">- Look at message ESD1281 to verify the user ID being used for this connection and the TTLSEnvironmentAction statement mapped to this connection. If you are configuring using the z/OS Configuration Assistant for z/OS Communications Server, you can specify the key ring on either the AT-TLS Image Level Settings panel or on each Traffic Descriptor.- Ensure that the correct key ring has been specified.- If using RACF key ring, verify that all the steps in z/OS Communications Server: IP Configuration Guide have been followed for this user ID.

- Consult IP Diagnosis for z/OS (GC27-3652)
 - Lists common SSL/TLS Error Codes
- Consult Cryptographic Services Secure Sockets Layer Programming for z/OS
 - Lists all the SSL/TLS Error Codes

Commands for AT-TLS

- UNIX commands
 - pasearch -t
- MVS Commands
 - D TCPIP,,N,TTLS
 - D TCPIP,<tnproc>,T,PROF,DETAIL
 - D TCPIP,<tnproc>,T,CONN
 - D TCPIP,<tnproc>,T,CONN,CONN=<connection number>
 - D TCPIP,<tnproc>,T,CONN,CONN=<connection number>,DETAIL

End of Topic

