z/OS V1R9 Communications Server Security Updates

Session 10

Prepared by Patrick Kappeler
IBM Consulting IT Specialist
kappeler@fr.ibm.com

Redbooks
International Technical Support Organization

Trademarks

See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

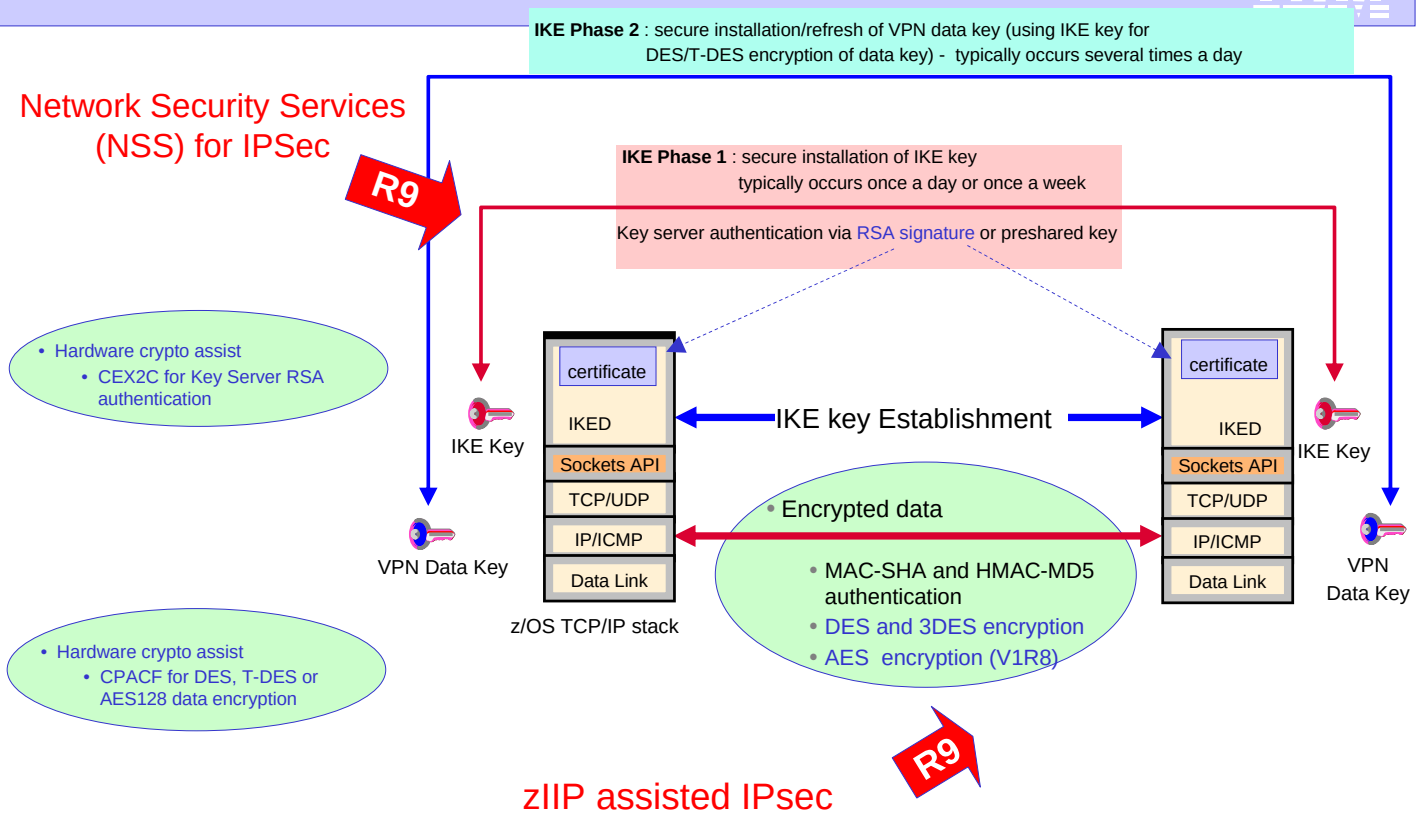
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- zIIP assisted IPSec
- IPsec network security services (NSS)
- AT-TLS enable the TN3270 server
- AT-TLS enable the FTP client and server
- FTP Kerberos single sign-on support

IPSec VPN - Reminder



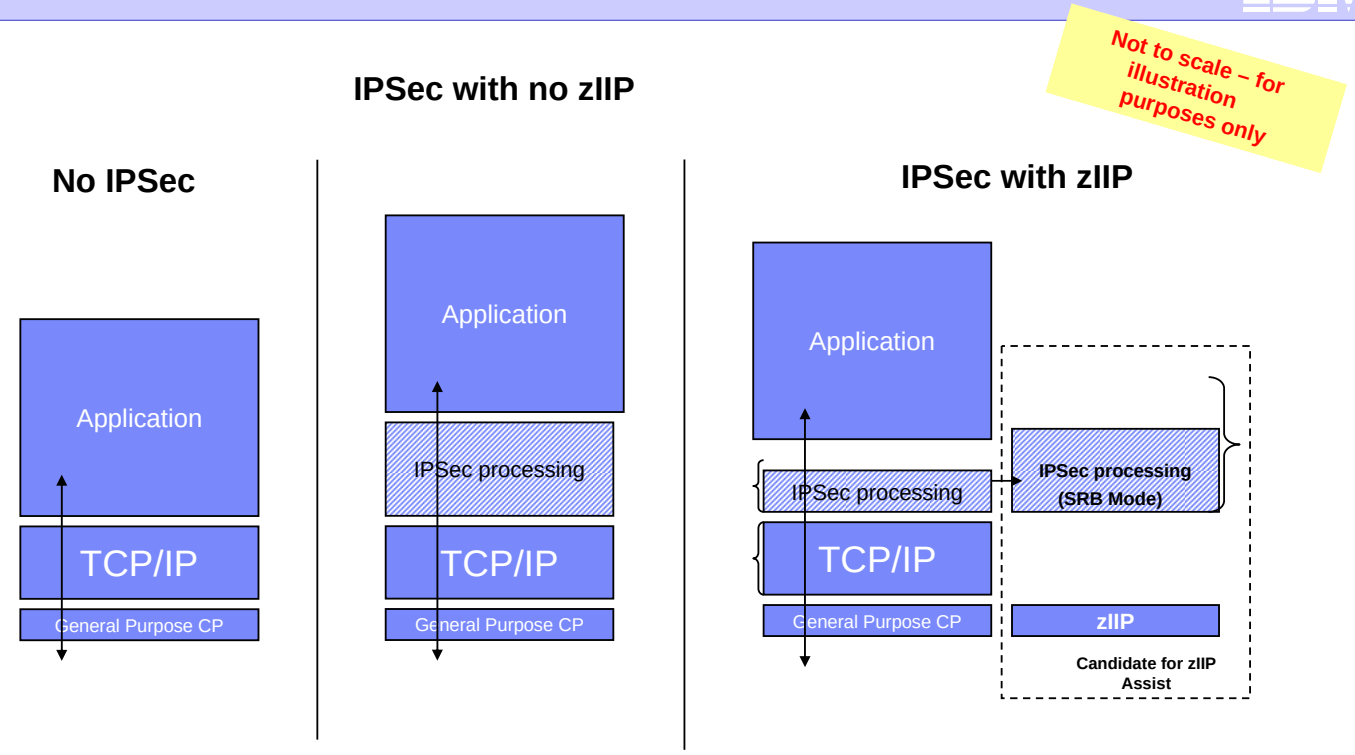
zIIP-Assisted IPSec

zIIP-Assisted IPsec

- zIIP-Assisted IPSec allows for the movement of a portion of Communications Server IPSec processing from general CPs to zIIPs
  - Encryption / decryption, message authentication, and IPSec header processing
- Can be used for IPSec protocol processing and shared with DB2 DRDA depending on workload
- Can lower CPU impact for network encryption workloads
  - zIIP supported on System z9 hardware or newer only
  - No IBM software charges on zIIPs
  - zIIPs priced lower than general purpose CPs
- zIIP is enabled by System z microcode and z/OS software
  - General purpose CPs and zIIPs can be in the same z/OS LPAR
- zIIP engine provides the same encryption acceleration (CPACF) as general purpose engines

Rolled back to z/OS V1R8 – See the Appendix

zIIP-Assisted IPsec



Function is enabled via a new TCP/IP configuration keyword when zIIP hardware in place and pre-req software

zIIP-Assisted IPsec - Keywords

In the **GLOBALCONFIG** statement

`ZIIP IPSECURITY` = *eligible work is directed to zIIP*

`ZIIP NOIPSECURITY` *(default)*

New **IEAOPTxx** statement in PARMLIB
to control whether zIIP eligible IPSec (and DB2 DRDA) work can spill over to general CPs

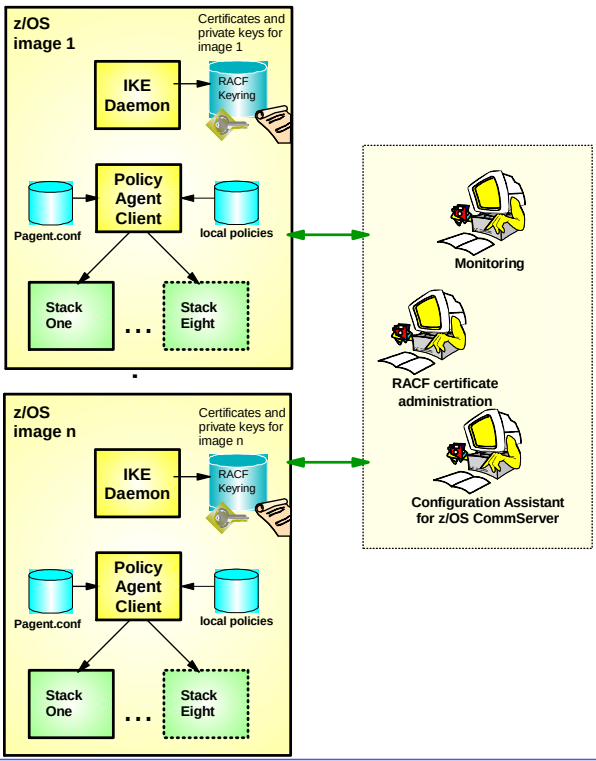
`IIPHONORPRIORITY=YES` *(default and recommended)*

`IIPHONORPRIORITY=NO` (*may result in throughput and/or response time degradation if zIIPs are heavily used*)

See pointers to resources in the appendix

Network Security Services (NSS)

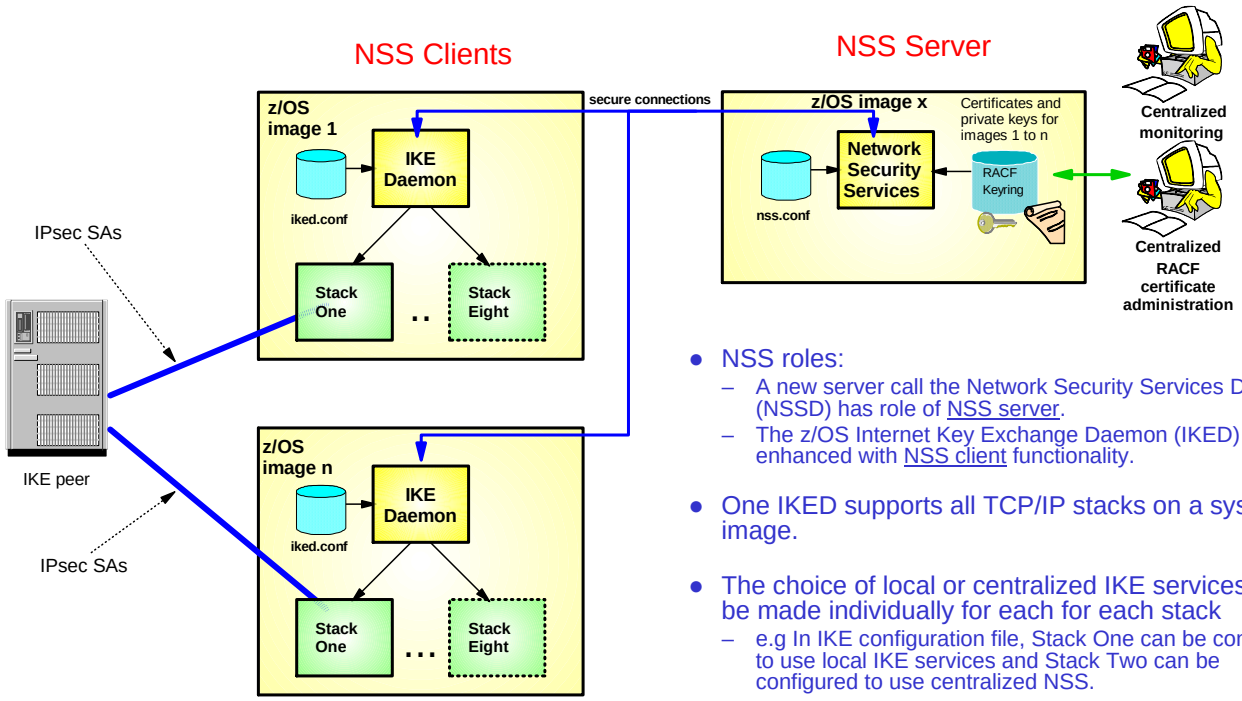
Network Security Services – IPSec Support



IPSec VPNs Administration at z/OS V1R8

- Each z/OS system locally administered
  - Monitoring
  - RACF certificate administration
  - Policy configuration
- Connectivity required between administration and each managed platform
  - Monitoring application has advance knowledge of each managed node
  - Coordination required to push policy out to each system for deployment

Network Security Services – z/OS V1R9 IPSec Support



- NSS roles:
  - A new server call the Network Security Services Daemon (NSSD) has role of NSS server.
  - The z/OS Internet Key Exchange Daemon (IKED) is enhanced with NSS client functionality.
- One IKED supports all TCP/IP stacks on a system image.
- The choice of local or centralized IKE services can be made individually for each for each stack
  - e.g In IKE configuration file, Stack One can be configured to use local IKE services and Stack Two can be configured to use centralized NSS.
- Backup NSSD can be specified in IKE configuration file.

Network Security Services – z/OS V1R9 IPSec Support

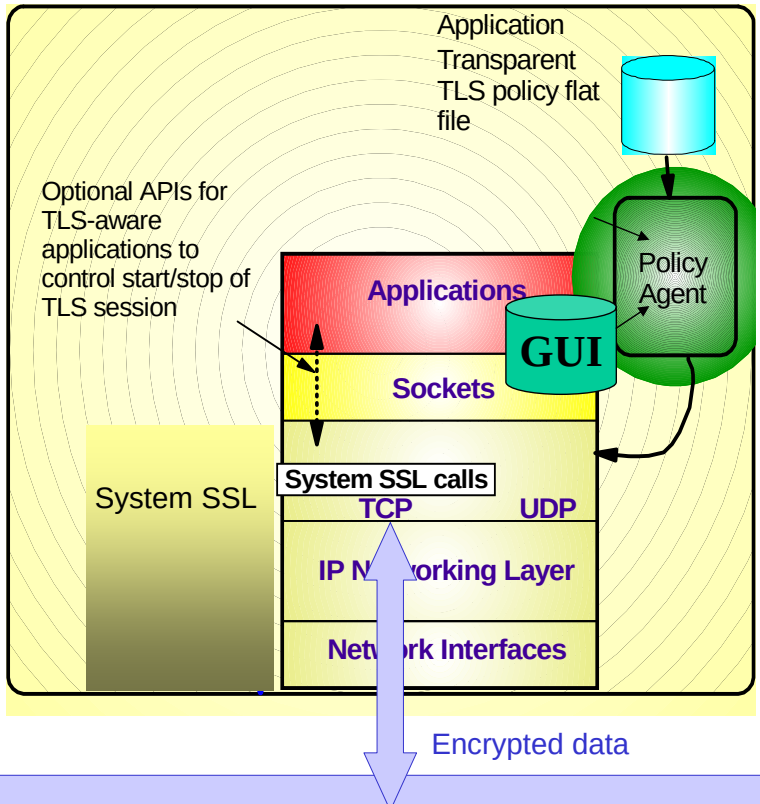
- Optional centralized network security services for a set of z/OS images
  - Images can be non-sysplex, within sysplex or cross sysplex
  - Configure NSS client and NSS server usage parameters for each stack
  - SAF profiles for thorough access control to commands and facilities
- Centralize and reduce configuration complexity and deployment
  - Eliminates need to distribute IKE certificates and keys to the endpoint
- NSS RSA signature services
  - Allows central administration of RACF certificates and private keys
    - Sign and verify during runtime IKE negotiations
- NSS monitoring interfaces
  - Allows selection of single focal point as IPsec management hub
    - ipsec command for administrator
    - Network Monitor Interface (NMI) for management application

AT-TLS Enablement For TN3270 And FTP

Application Transparent TLS (AT-TLS)

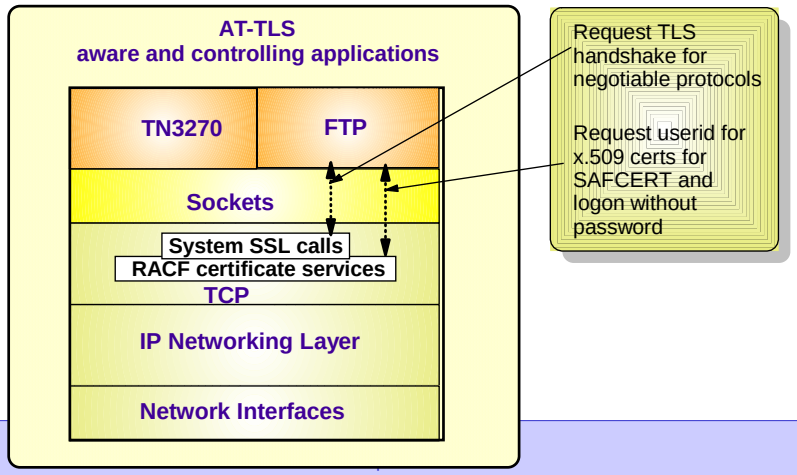
Introduced in z/OS V1R7

- TCP/IP stack performs TLS
  - No application changes required
  - Take advantage of z/OS unique encryption
- TLS Configuration through system wide policies
- GUI supplied to ease configuration
- Optional API for applications that wish to be “aware” or control TLS information



AT-TLS - TN3270 And FTP Enablement

- Both the TN3270 server, and the FTP server and client on z/OS have in the past implemented SSL/TLS support. They are now constrained regarding the set of options supported today by System SSL (see appendix)
- AT-TLS is exploiting the full set of System SSL options - It is desirable to migrate the FTP and TN3270 SSL/TLS support to AT-TLS
- In z/OS V1R9, TN3270 and FTP are enabled to be AT-TLS aware and controlling



AT-TLS - TN3270 And FTP Enablement

- New keywords

  `TTLSPORT nnnnn` in TN3270 Security options

  `TLSMECHANISM FTP|TTLS` in FTP.DATA

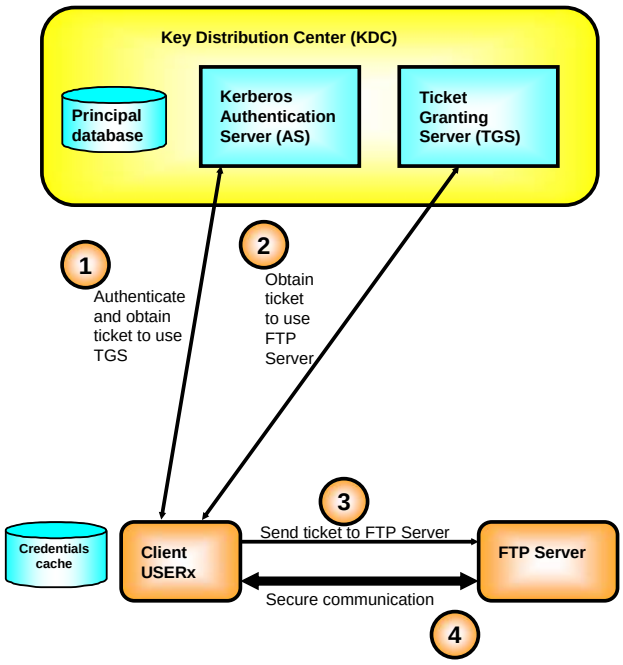
- By enabling TN3270 and FTP as AT-TLS aware and controlling applications, they automatically picks up new TLS functionality through AT-TLS:
  - Support keyring refresh without stopping/starting server
  - Allow multiple keyrings per server
  - Allow specification of certificate labels other than the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

FTP Security Enhancements

FTP Kerberos Single Sign-On Support

- **One of the main benefits, and often the main reason why people use Kerberos, is the single sign-on capability:**
  - Users sign on to the Kerberos Authentication Server
  - Users are then granted access to other servers through a "ticket" approach
  - When connecting to a Kerberos-enabled server and presenting the user's "ticket", the user may be signed on implicitly
- **FTP on z/OS was Kerberos-enabled in z/OS V1R2, but continued to always require both a user ID and password.**
- **FTP protocol prevents us from bypassing the request for a user ID.**
- **If the entered FTP user ID matches the user ID in the Kerberos ticket, the prompt for an FTP password will be bypassed**
  - New FTP server configuration option to control this behavior:

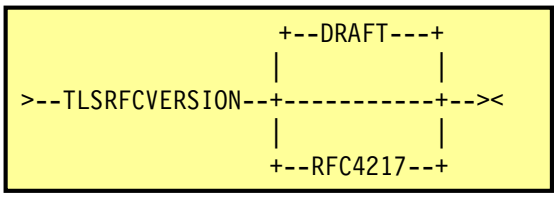
```
SECURE_KERBEROS_PASSWORD {REQUIRED/OPTIONAL}
```



Enables easier use of z/OS FTP Server in a Kerberos-based single sign-on environment.

FTP – Latest SSL/TLS IETF Standards

- FTP was originally enabled for SSL/TLS back in z/OS V1R2
  - Based on a draft RFC that described how the FTP protocol were to work with SSL/TLS
- That draft RFC has since that time undergone several revisions and has now made it into official RFC status
  - RFC 4217 "Securing FTP with TLS"



Default is to use the current default (DRAFT).

To use the RFC4217 level, this option must be specified in the FTP client FTP.DATA or set by a LOCSITE command for the client - and in FTP.DATA for the server (no SITE command support).

Thank You

Any Questions ?

Appendix

zIIP-Assisted IPsec - Resources

- What are the pre-requisites for zIIP assisted IPSec?
  - **z/OS 1.8 Communications Server PTF (APAR PK40178)**
  - **z/OS 1.8 PTF (APAR OA20045) (coreq for APAR PK40178)**
  - **System z9 with zIIPs**
- z/OS Communications Server ibm.com**/software/network/commserver/zos/security/**
- zIIP page ibm.com**/systems/z/ziip/**
- Redbooks® – z/OS Network Security
  - www.redbooks.ibm.com**/redbooks/pdfs/sg247342.pdf**
- White paper "Capacity Planning for zIIP-Assisted IPSec"
  - ibm.com**/support/techdocs/atsmastr.nsf/WebIndex/WP100988**
  - ibm.com**/support/docview.wss?rs=852&uid=swg27009459**
- Techdocs
  - **#PRS2745 WSC Experiences with IPSec on the zIIP Processor**
  - **#WP100988 Capacity Planning for zIIP-Assisted IPSec**
  - **#TD103516 Specialty Engine zIIP and zAAP Software Update**

AT-TLS Support In FTP And TN3270

FTP at z/OS V1R8 uses System SSL, but does not implement all the options

- Does not use LDAP servers
- Unable to specify label for certificate
- Unable to refresh session key

TN3270 at z/OS V1R8 does not support

- Key ring refresh without stopping/starting ports
- Allowing multiple key rings per server
- Specifying certificate label other than the default certificate
- Multiple CRL LDAP server specification
- New ciphers added
- Session ID caching (Reset session/cipher)

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)