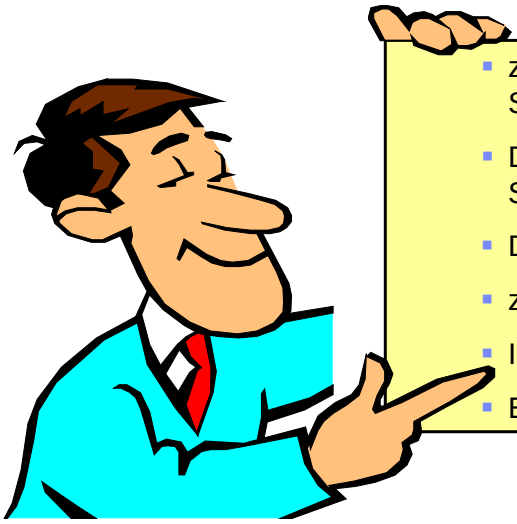
This presentation is an overview of the security enhancements for the Communications Server for z/OS V1R10.

Agenda - part one



- z/OS V1R9 Network Security Services (NSS) overview
- DataPower® integration with NSS SAF access service
- Defensive filtering
- z/OS Defense Manager overview
- IPSec RFC currency
- Enhanced port access control

This presentation includes security improvements in the Communications Server for z/OS V1R10. First it reviews z/OS V1R9 Network Security Services (NSS). Then the DataPower integration with NSS SAF access service, Defensive filtering, z/OS Defense Manager, IPSec RFC currency, and port access control enhancements are described.

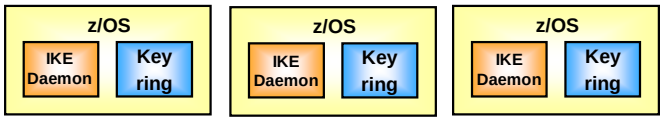
Agenda – part two

- Enhanced rpcbind application registration control
- FTP SSL/TLS enhancements
- SSL/TLS enablement for Load Balancing Advisor
- Autolog support for AT-TLS dependent applications
- Security options for Centralized Policy Server

The remainder of the security improvements include enhanced rpcbind application registration control, FTP SSL/TLS enhancements, SSL/TLS enablement for Load Balancing Advisor, Autolog support for AT-TLS dependent applications and security options for Centralized Policy Server.

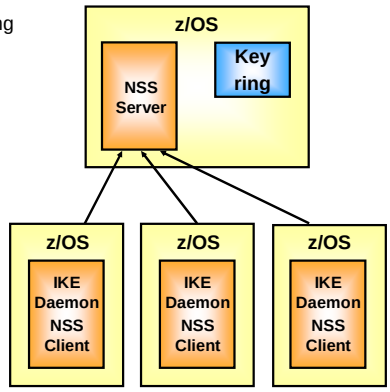
AT-TLS is the acronym for Application Transparent- Transport Layer Security (TLS) protocol.

Network Security Services (NSS) in z/OS V1R9 - Overview



Before z/OS V1.9 all z/OS CS IKE Daemons have their own key ring repository.

- Network Security Services is a z/OS V1R9 new feature
- IKE Daemon may be configured as a Network Security Client.



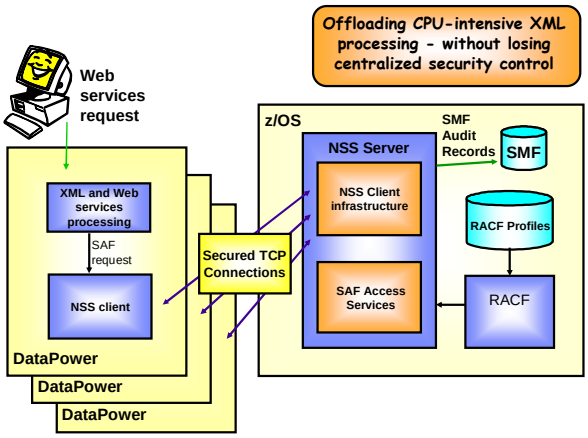
z/OS CS V1R9 IKE Daemons may have their IPSec certificates stored on a single system.

This slide describes Network security services (NSS) in z/OS V1R9. NSS provides centralized certificate and keyring management, centralized services that require access to private keys, and monitoring and management for IPSec security for z/OS systems within and across sysplexes.

When Internet Key Exchange (IKE) daemon is an NSS client, the configuration is on a per-stack basis. Each NSS-enabled stack will appear to the Network Security Server as an independent client. For TCP/IP stacks that are not configured to use Network Security Services, the IKE daemon will continue to manage certificates out of a local keyring.

DataPower integration with NSS SAF access service

- WebSphere DataPower SOA Appliances
  - *Integration Appliance XI50*
    - *XML Security Gateway XS40*
- CS V1R10 provides Integration of DataPower and NSS
  - Allows DataPower appliances to access SAF authentication services on z/OS (for example, RACF®)



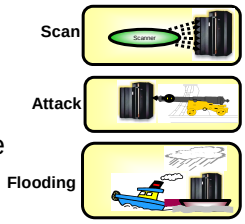
The Integration Applicance XI50 provides application message format transformation. The XML Security Gateway XS40 offloads XML and Web services security functions.

Using DataPower appliances enables offloaded XML and Web services security processing. Integration with z/OS Communications Server provides centralized management of SAF-based authentication and access control *across multiple hardware platforms.* DataPower includes an NSS Client. The z/OS NSS Server supports System Authorization Facility (SAF) Access Services.

The NSS Client-Server infrastructure includes basic operations for NSS Client-Server connections over secure TCP connections,SAF-based authentication of Web services request originators, and access control for XML objects enabled by way of a new parameter discipline (IPSec or XMLAppliance) on NssConfig. The new nssctl z/OS UNIX® command at NSS Server displays information about all connected NSS Clients. The NMsec_GET_CLIENTINFO NMI request/response was modified to distinguish IPSec NSS Clients from XMLAppliance NSS Clients.

Defensive filtering

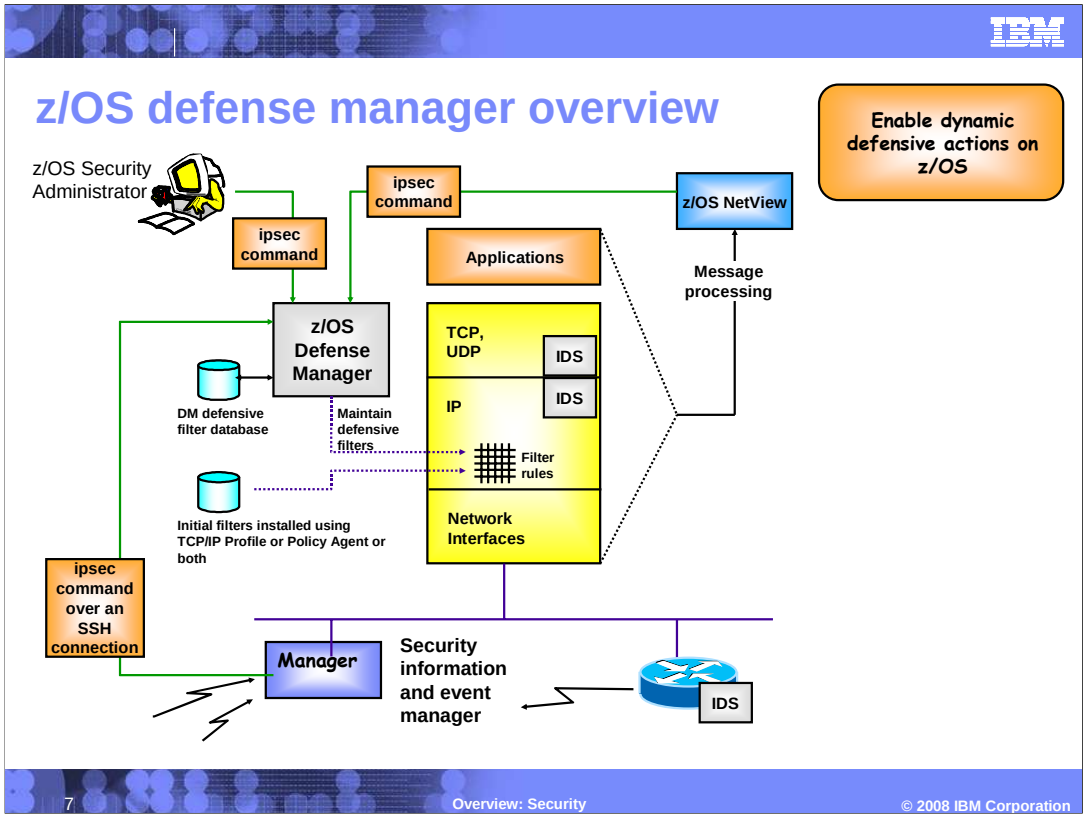
- Currently, z/OS IDS provides support for:
  - Scan detection and reporting
  - Attack detection, reporting, and prevention
  - Traffic regulation for TCP connections and UDP receive queues
- Primary focus for z/OS IDS has so far been detecting events, and to some limited extent, preventing intrusions
- The current z/OS IDS functions do not allow external security monitors or other IDS technologies to participate in the detection of intrusions or in the implementation of countermeasures
- In z/OS V1R10, a new z/OS Defense Manager component is added that will allow authorized components to dynamically install defensive filters



Current z/OS IDS support, when detecting attacks, can discard certain malformed IP packets. For traffic regulation, it can limit the number of TCP connections and limit the UDP receive queue size.

If they could participate, some of the non-z/OS monitors could in some cases cooperate with applications and detect intrusion events at an application layer - extending IDS monitoring beyond what the current z/OS IDS technology supports.

NetView® message automation as a result of analyzing IDS messages or other events, potential extensions to TSOM as a result of network-detected suspicious activity and a local security administrator as a result of information received about a pending threat are some examples of uses of Defense Manager.



Defense manager allows use of the ipsec command to display and control defensive filters is secured using SAF security profiles. The IPSec command can be used by an administrator, or provided over an SSH connection by a security information and event manager.

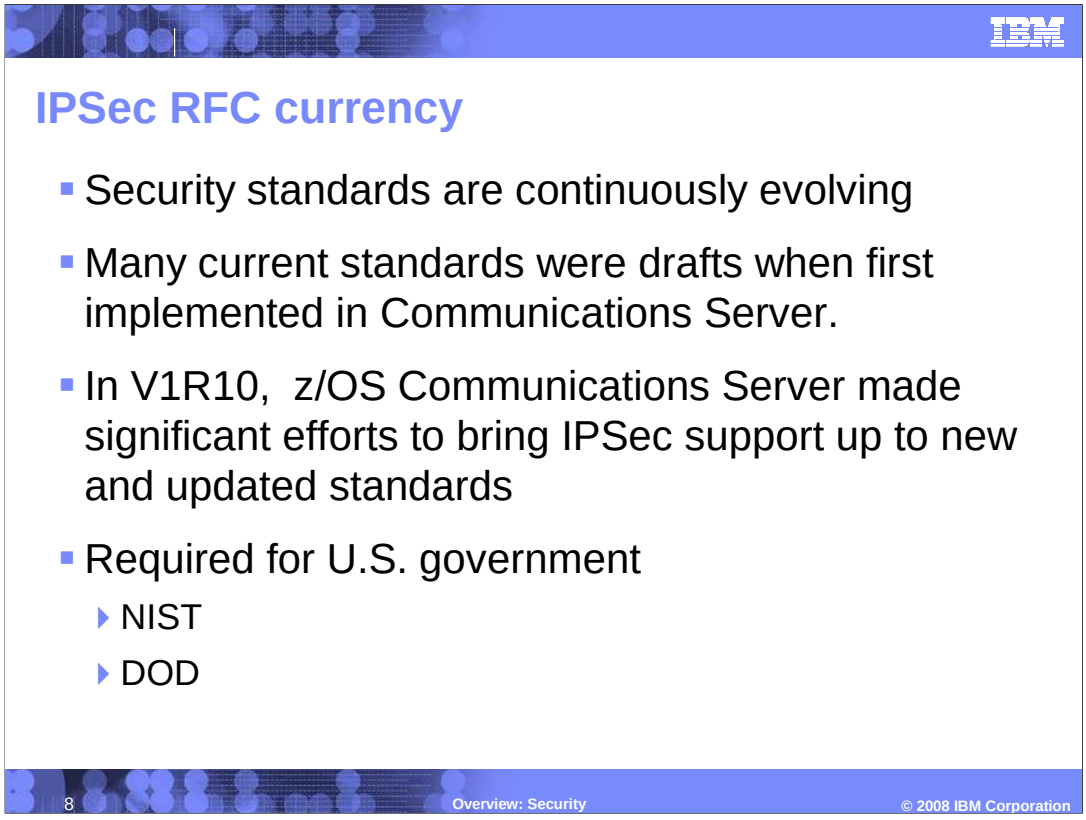
Defensive filters are maintained on DASD for availability in case of DM restart or stack start or restart.

There is one Defense Manager per LPAR.

Defensive filters can be Global and apply to all stacks on the LPAR where DM runs. They can be Local and apply to a specific stack. They are also Time-limited and apply to a period of time.

Defensive filters are installed "in-front" of configured or default filters and are therefore always searched first.

.



The NIST, National Institute of Standards and Technologies, sets standards in RFC compliance.

The DOD, Department of Defense, imposes additional, more stringent requirements for security standards compliance.

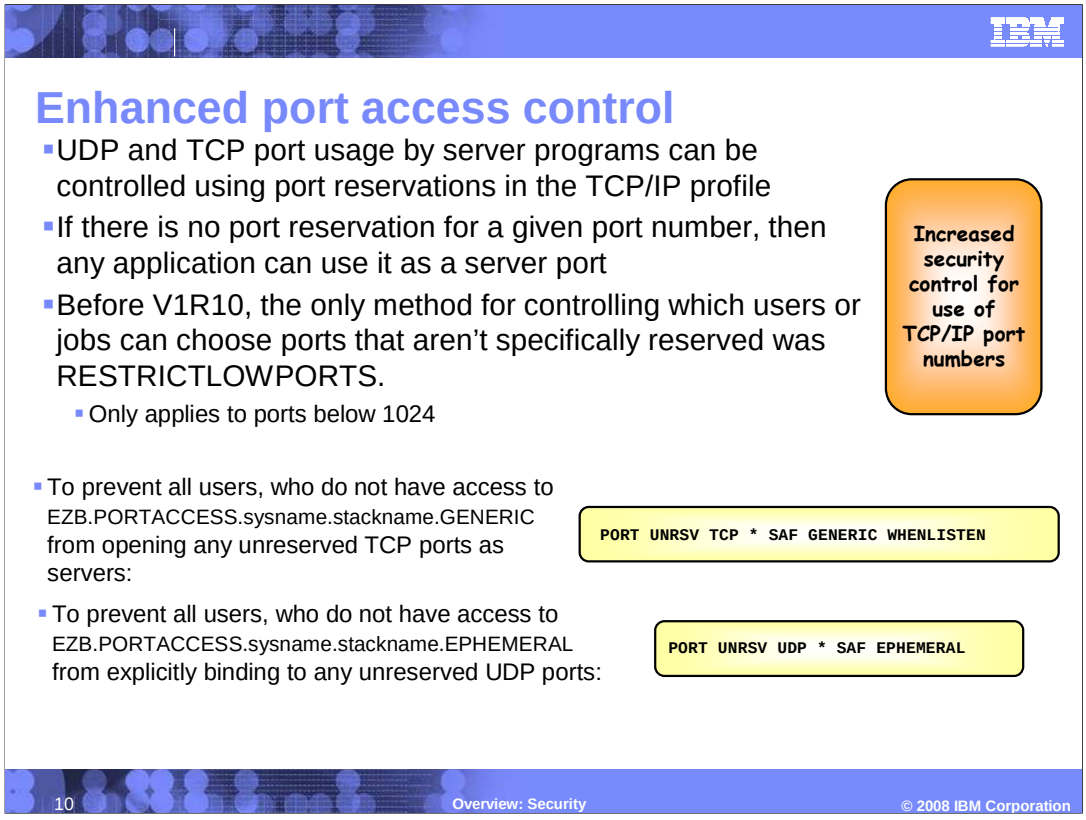
z/OS Communications Server for V1R10 made significant efforts to bring IPSec support up to new and updated standards.

z/OS CS IPSec RFC currency

Keeping up with the IPSec security standards

RFC	DOD Advanced UNIX Server Profile	NIST Host Profile	z/OS CS V1R10
2407 ISAKMP DOI	MUST	MUST	✓ (already supported)
2408 ISAKMP	MUST	MUST	✓ (already supported)
2409 IKE	MUST	MUST	✓ (already supported)
3948 UDP-encap ESP	N/A	MAY	✓ (already supported)
4109 IKE algorithms	MUST	MUST	✓ (already supported)
4301 IPsec	MUST	SHOULD+	✓ **(new in V1R10)**
4302 IP AH	MUST	MAY	✓ (already supported)
4303 IP ESP	MUST	MUST	✓ (already supported)
4304 ESN	SHOULD	MUST	✓ **(new in V1R10)**
4305 IPsec algorithms	SHOULD+	SHOULD+	✓ (already supported)
4308 Crypto suites	MUST	MAY	✓ **(new in V1R10)**

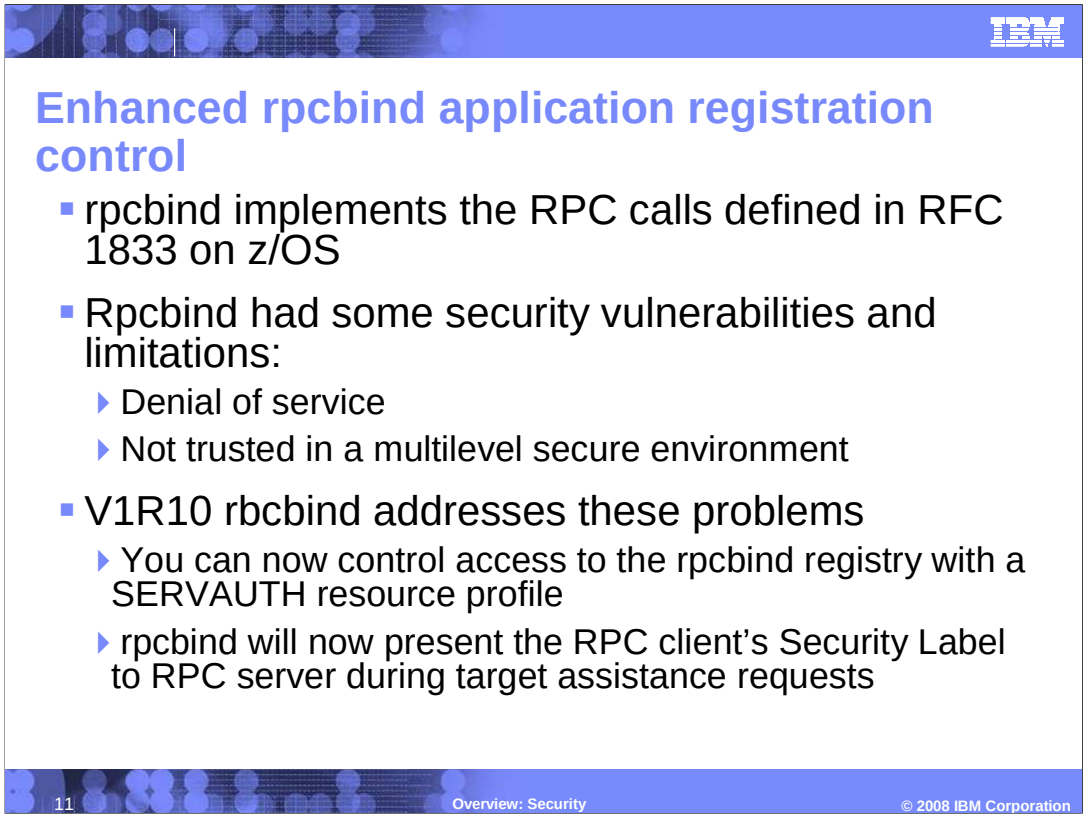
This chart shows an overview of the IPSEC RFC currency work done in V1R10. RFCs 4301 Ipsec, 4303 IP ESP and 4308 Crypto suites were implemented in V1R10. The z/OS Communications Server V1R10 supports all IPSec RFCs at levels currently required by DOD and NIST profiles.



Before V1R10, you could use RESTRICTLOWPORTS to prevent users and jobs that are not authorized or UID(0) from choosing ports below 1024.

Port access can be controlled by server jobname or server userID access authorization to a SAF resource that is associated with the port.

This new function only controls application-specified ports. It does not affect generic binds or use of ephemeral ports (meaning, port number chosen by the stack).



RFC 1833 defines the lookup services provided by rpcbind. Binding protocols are the interface to request the services of rpcbind. These services enable a server to use any port, instead of a well known port. The port can change each time the server is started. An RPC server **registers** its transport address with rpcbind and RPC clients look up the transport address of the RPC server through rpcbind.

Rpcbind can be vulnerable to denial of service attacks because before V1R10, any application on the local host could register and deregister servers.

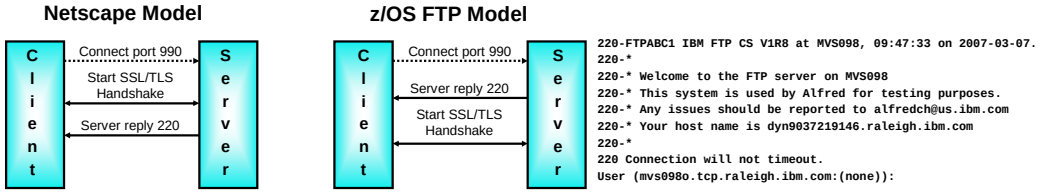
Rpcbind was not trusted in multilevel secure environment because the security Label of rpcbind server is presented as part of Port Of Entry for Target assistance requests. For example, an RPC server S thinks R originated with rpcbind.

Rpcbind is enhanced in this release to use a resource profile in the SERVAUTH class to control access to the rpcbind registry. Not only must registration requests and deregistration requests originate from the local host, the requesting RPC server must have read access to the SERVAUTH profile or rpcbind will reject the request.

In a multilevel secure environment, rpcbind will now switch to the RPC client's security label before it forwards a target assistance RPC to a registered RPC server. This will present correct port of entry credentials to the target server. That is, the request R will arrive at server S with the authority of the RPC client, not with the authority of rpcbind. The target server can correctly determine whether the request is authorized.

FTP enhancements (security – provide industry standard implicit SSL/TLS)

- There are two ways to indicate if an FTP session is to use SSL/TLS or not:
  - Explicit mode
  - Implicit mode



- z/OS FTP client was changed to optionally work according to the Netscape model using APAR PQ87711
- z/OS CS V1R10 adds similar support to the z/OS FTP server

Improved interoperability with other SSL/TLS-enabled FTP products

Using explicit mode, the FTP client connects to typical FTP server port 21 and sends an FTP subcommand (AUTH) to request use of SSL/TLS. This mode is defined in RFC 4217 and is the recommended mode according to the RFC standards.

Using implicit mode, the FTP client connects to an alternate FTP server port (for example, port 990). Then the client and server implicitly enter SSL/TLS mode as a result of the connection being established to that alternate port number. There are no RFC standards that govern how implicit mode FTP sessions are to be set up, so use of implicit mode FTP is generally based on how the original Netscape implementation worked.

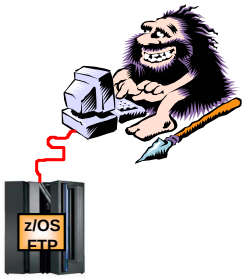
In V1R10, the FTP server is enhanced to optionally support the Netscape model, using the same SECUREIMPLICITZOS keyword that the client had been using.

With the APAR, the method used can be specified with FTP.DATA client keywords, SECUREIMPLICITZOS=[TRUE/FALSE]. Support is for levels z/OS V1R4 and above.

FTP enhancements (security: provide a SAF-based mechanism to control access to the z/OS FTP server)

- Basically, any user who has a valid z/OS user ID can log on and use the z/OS FTP server
- There are some pre-existing ways to restrict access to the z/OS FTP server:
  - FTCKPWD exit routine
  - SSL/TLS
- z/OS CS V1R10 optionally extends the check of the already existing SERVAUTH resource to all users who log on to the FTP server
- A new FTP.DATA server option is used to indicate this new behavior:
  - VERIFYUSER=[TRUE/FALSE]

Increased protection of the z/OS FTP server in general

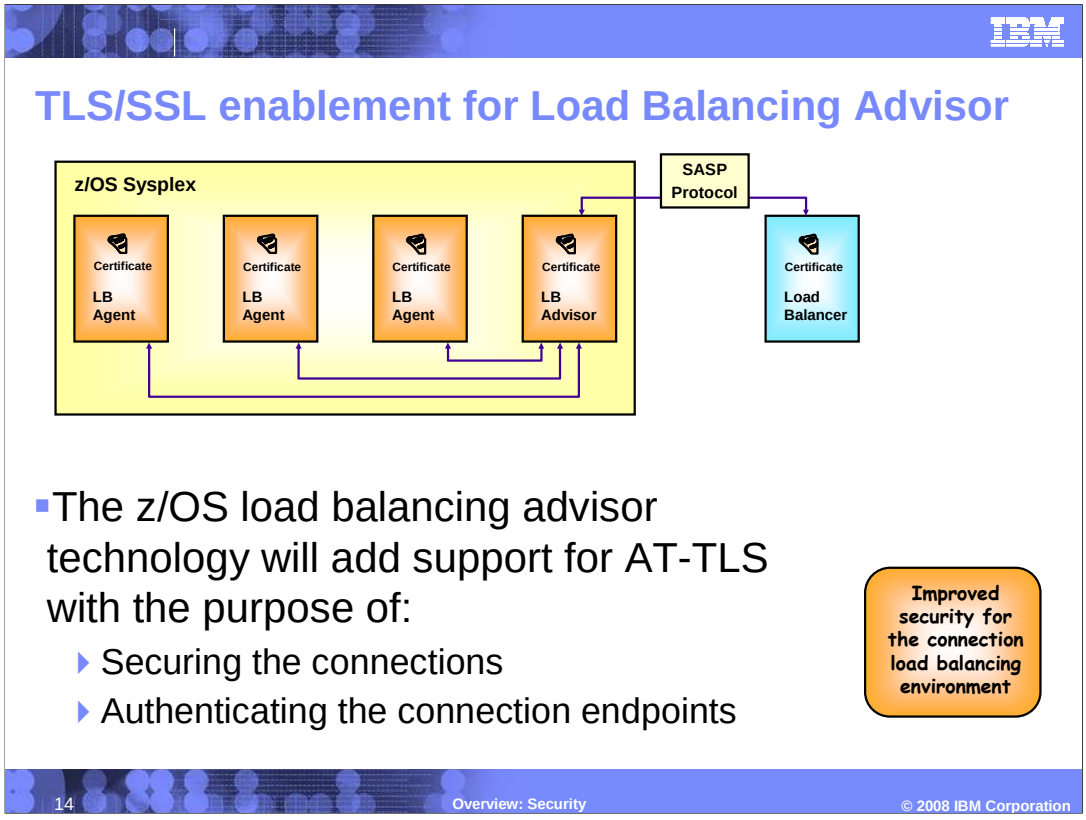


Before V1R10, user restrictions to the FTP server restrictions could be implemented in general by coding an FTP server password check exit routine (FTCHKPWD), but many installations no longer have the skills to implement exit routines.

If users log on using SSL/TLS and the SECURE_LOGIN option is set to VERIFY_USER, the FTP server will check if the user has READ access to EZB.FTP.<systemname>.<ftpdaemonname>.PORTxxxx SERVAUTH resource.

If users do not use SSL/TLS or the VERIFY_USER option is not set as above, no checking of the SERVAUTH resource is done before V1R10.

Now with V1R10, installations have an easy way to limit use of the FTP server functions in general. The new VERIFYUSER keyword can be coded to require users to have access to the SSL/TLS SAF resource even if SSL/TLS is not being used. They can define the EZB.FTP.<systemname>.<ftpdaemonname>.PORTxxxx SERVAUTH SERVAUTH resource with universal access set to NONE. An alternate method is to permit those users who are allowed to use the FTP server with READ access to the SERVAUTH resource.

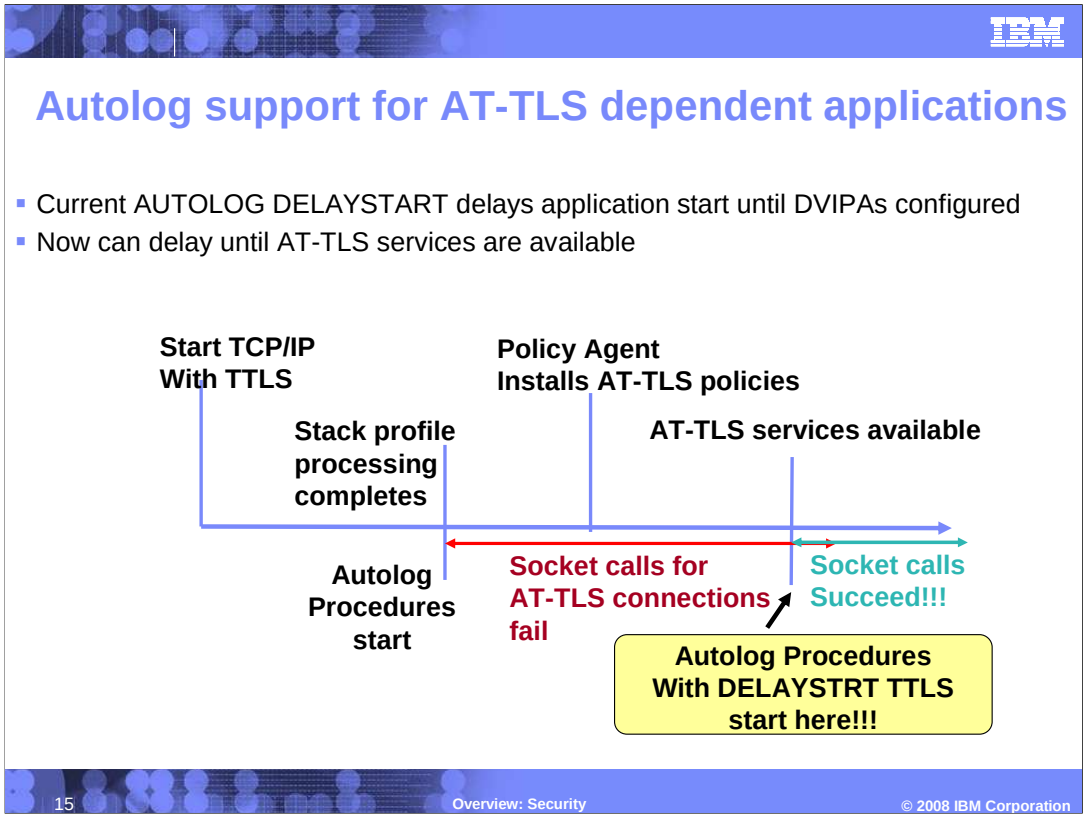


The SASP protocol is defined in *"Server/Application State Protocol v1"*, RFC 4678. This RFC recommends that security is addressed by using SSL/TLS on the SASP connection. IBM's other SASP implementation, EWLM, already supports SSL/TLS on the SASP connections.

Load balancing advisor support of AT-TLS will enable securing the connections between the agents and the advisor, and between the advisor and the external load balancer, where the external load balancer supports SSL/TLS at its endpoint.

It will also enable authentication of connection endpoints. Before z/OS V1R10, authentication of agents and external load balancer is done using pre-configured IP addresses and port numbers. However, this method is cumbersome to configure and provides limited security.

With AT-TLS support, such authentication can be done based on client authentication (certificates at both endpoints of the connections)

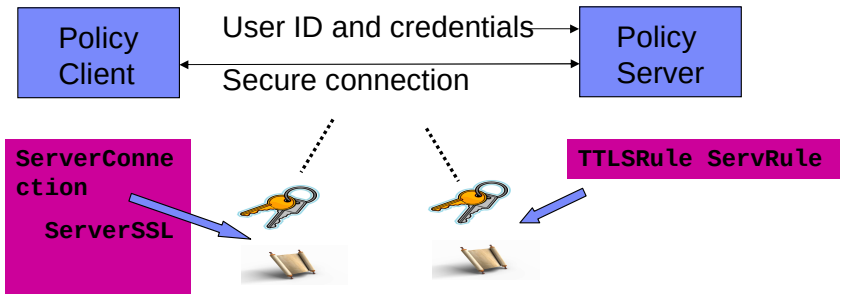


Current AUTOLOG DELAYSTART is used so that AUTOLOG procedures that bind to a DVIPA will not start until the DVIPA has been configured (after the stack has joined the sysplex group)

DELAYSTART is needed when DELAYJOIN is specified on the GLOBALCONFIG profile statement. When DELAYJOIN is specified, TCP/IP will not join the sysplex group and process the stack's dynamic VIPA configuration until OMPROUTE is active and ready to advertise dynamic VIPAs when they are created on this stack. Having both DELAYJOIN and DELAYSTART prevents scenarios during Sysplex Distributor Takeback where a distributor needs OMPROUTE active and the DVIPAs configured to take back ownership of the DVIPAs.

A similar ability to "delay start" of applications is needed for applications using AT-TLS services. Without this, applications using AT-TLS can start but have all their connections fail until Policy Agent installs the AT-TLS policies and all AT-TLS services are available. A new AUTOLOG DELAYSTART parameter TTLS is added to postpone automatically starting an application until AT-TLS services are available. A new parameter DVIPA is also added for customers desiring the current support of delaying application start until DVIPA configuration completes. Either TTLS or DVIPA or both may be specified for an AUTOLOG applications.

Security options for Centralized Policy Server



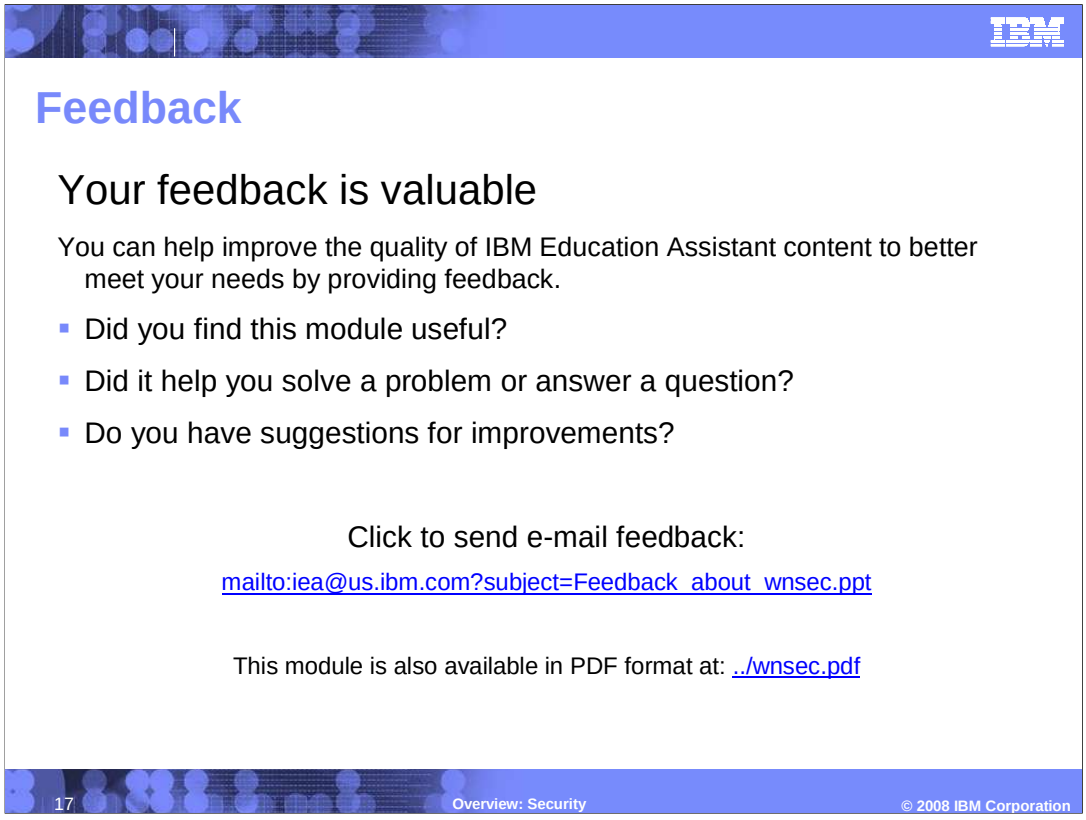
- V1R9 Centralized Policy Services require:
  - SSL/AT-TLS
  - User ID and Credentials
- SSL/AT-TLS is now optional
  - Note sensitive info (like passwords, certificate labels, IPSEC keys) will flow “in the clear”

In V1R9 you are required to set up secure connections between policy clients and the policy server for the Centralized Policy Services function. You are also required to set up a user ID and credentials (password or PassTicket) for each policy client. The secure connections use SSL on the policy client and AT-TLS policy on the policy server to point to the appropriate keyrings containing the certificates used to establish secure connections.

The solution is to make the SSL configuration on the policy client optional. Note that a user ID and credentials are still required. The use of user ID and credentials without SSL provides authentication without encryption.

You are still responsible for setting up (or not) the AT-TLS policies on the policy server. If none of the policy clients are using SSL you don’t need any AT-TLS policies to protect any policy client connections. If you’re not using AT-TLS for anything else you also don’t need to configure the TCP/IP stack for AT-TLS.

Be aware that sensitive information such as the password used to authenticate with the policy server, and any policy information retrieved from the policy server, flows in the clear without the use of SSL/AT-TLS.



You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, copyrights, and disclaimers

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

DataPower IBM NetView RACF WebSphere z/OS

A current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

UNIX is a registered trademark of The Open Group in the United States and other countries.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance 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 or performance improvements equivalent to the ratios stated here.