



Software Group | Enterprise Networking and Transformation Solutions (ENTS)

# Overview of TCP/IP Security Features for z/OS Communications Server

## SHARE Session 3406

**Lin Overby**  
**[overbylh@us.ibm.com](mailto:overbylh@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:

- ▶ AIX<sup>7</sup>
- ▶ AnyNet<sup>7</sup>
- ▶ AS/400<sup>7</sup>
- ▶ Candle<sup>7</sup>
- ▶ CICS<sup>7</sup>
- ▶ CICSplex<sup>7</sup>
- ▶ CICS/ESA<sup>7</sup>
- ▶ DB2<sup>7</sup>
- ▶ DB2 Connect<sup>™</sup>
- ▶ DPI<sup>7</sup>
- ▶ DRDA<sup>7</sup>
- ▶ e business(logo)<sup>7</sup>
- ▶ ESCON<sup>7</sup>
- ▶ eServer<sup>™</sup>
- ▶ ECKD<sup>™</sup>
- ▶ FFST<sup>™</sup>
- ▶ GDDM<sup>7</sup>
- ▶ GDPS<sup>7</sup>
- ▶ HiperSockets<sup>™</sup>
- ▶ IBM<sup>7</sup>
- ▶ Infoprint<sup>7</sup>
- ▶ IMS<sup>™</sup>
- ▶ IP PrintWay<sup>™</sup>
- ▶ iSeries<sup>™</sup>
- ▶ Language Environment<sup>7</sup>
- ▶ MQSeries<sup>7</sup>
- ▶ MVS<sup>™</sup>
- ▶ MVS/ESA<sup>™</sup>
- ▶ NetView<sup>7</sup>
- ▶ OS/2<sup>7</sup>
- ▶ OS/390<sup>7</sup>
- ▶ Parallel Sysplex<sup>7</sup>
- ▶ PrintWay<sup>™</sup>
- ▶ PR/SM<sup>™</sup>
- ▶ pSeries<sup>7</sup>
- ▶ RACF<sup>7</sup>
- ▶ Redbooks<sup>™</sup>
- ▶ Redbooks (logo)<sup>™</sup>
- ▶ S/390<sup>7</sup>
- ▶ System/390<sup>7</sup>
- ▶ ThinkPad<sup>7</sup>
- ▶ Tivoli<sup>7</sup>
- ▶ Tivoli (logo)<sup>7</sup>
- ▶ VM/ESA<sup>7</sup>
- ▶ VSE/ESA<sup>™</sup>
- ▶ VTAM<sup>7</sup>
- ▶ WebSphere<sup>7</sup>
- ▶ xSeries<sup>7</sup>
- ▶ z/Architecture<sup>™</sup>
- ▶ z/OS<sup>7</sup>
- ▶ z/VM<sup>7</sup>
- ▶ zSeries<sup>7</sup>

- 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.

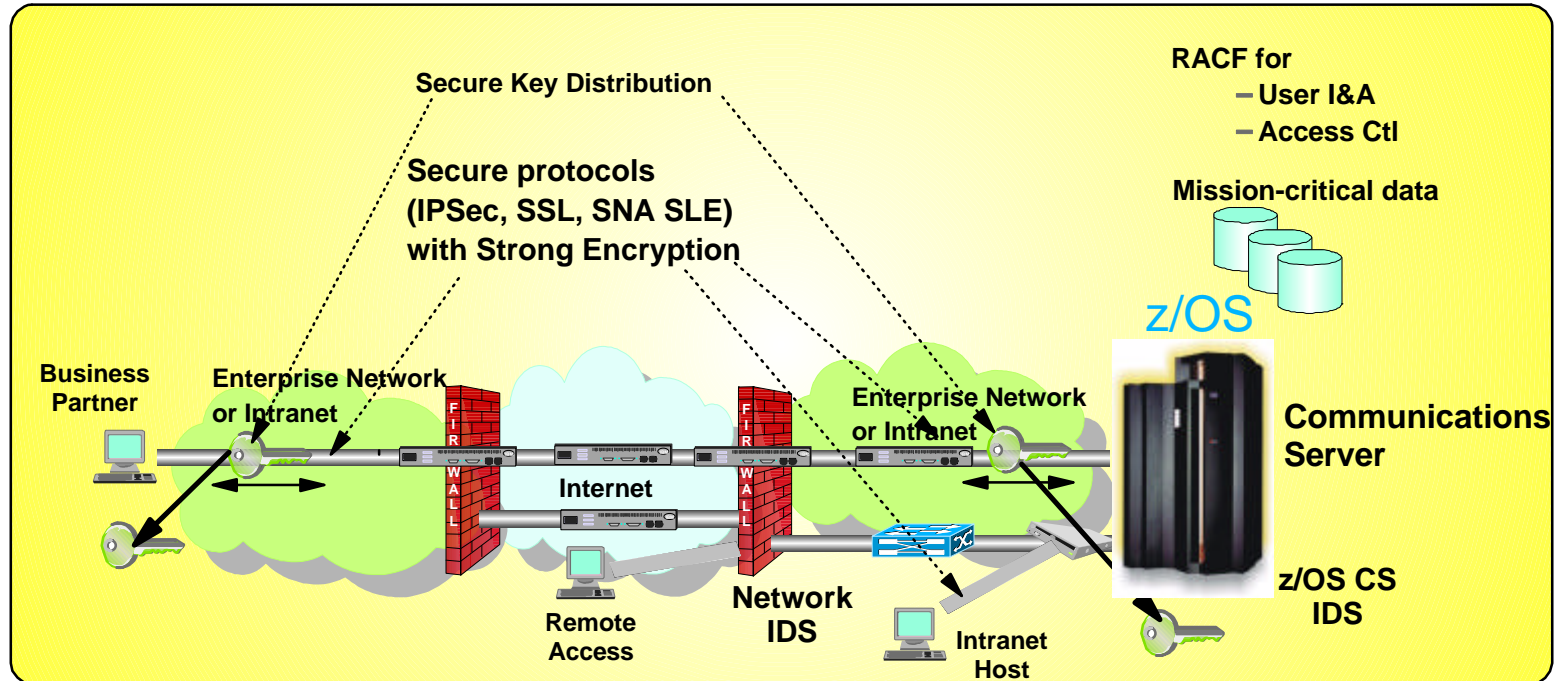
Refer to [www.ibm.com/legal/us](http://www.ibm.com/legal/us) for further legal information.

# Agenda

- z/OS Communications Server network security
  - ▶ Roles and objectives
  - ▶ Deployment trends and requirements
  
- Topic areas
  - ▶ Policy-based Network Security
    - IP security
      - IP Packet Filtering and IPSec
    - Application Transparent TLS
    - Intrusion Detection Services
  - ▶ Configuring Policy-based Network Security
    - Configuration Assistant for z/OS
  - ▶ Enterprise Security Roles
    - Centralized Policy Agent
    - Network Security Services for IPSec

# z/OS Communications Server Security Roles and Objectives

- ✓ Secure access to both TCP/IP and SNA applications
- ✓ Focus on end-to-end security and self-protection
- ✓ Exploit strengths of zSeries and system z9 hardware and software



- Protect data and other resources on the system
  - *System availability*
    - Protect system against unwanted access and denial of service attacks from network
  - *Identification and authentication*
    - Verify identity of users
  - *Access control*
    - Protect data and other system resources from unauthorized access

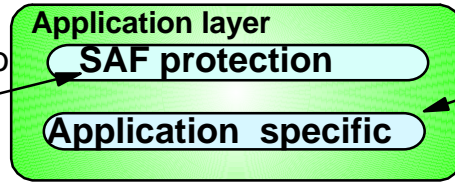
- Protect data in the network using cryptographic security protocols
  - *Data Origin Authentication*
    - Verify that data was originated by claimed sender
  - *Message Integrity*
    - Verify contents were unchanged in transit
  - *Data Privacy*
    - Conceals cleartext using encryption

# Deployment trends and requirements

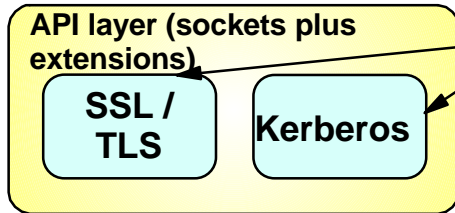
- Protecting the system from the network
  - ▶ Increased access requires focus on self protect
  - ▶ Defense in depth - no longer only perimeter based
- Focusing on end-to-end security
  - ▶ z/OS as the security endpoint
  - ▶ Observed increase of encryption endpoint deployments on z/OS
  - ▶ Pushes security traditionally deployed in network to server
    - Packet inspection techniques in network less effective
- Minimizing security deployment costs
  - ▶ Application transparent network security reduces application costs
  - ▶ Policy-based network security reduces deployment costs
  - ▶ GUI-based policy administration for ease of use

# Protocol stack view of TCP/IP Security Functions

**Protect the system**  
z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources..

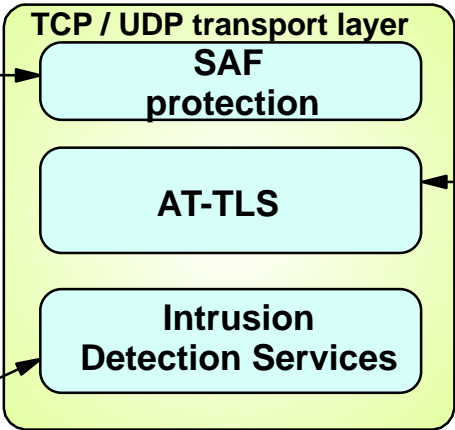


**Protect data in the network**  
Examples of application protocols with built-in security extensions are SNMPv3, DNS, and OSPF.



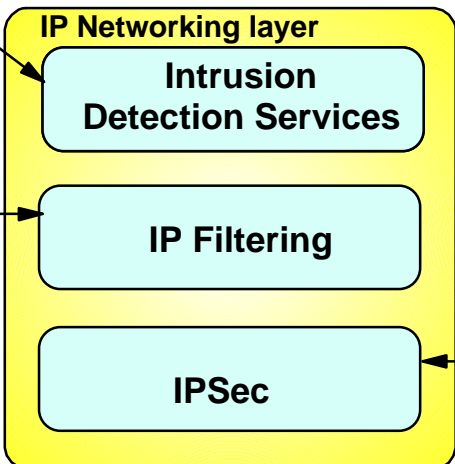
Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

The SAF SERVAUTH class is used to prevent unauthorized user access to TCP/IP resources (stack, ports, networks)



AT-TLS is TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to upper-layer protocols. It is available to TCP applications in all programming languages except PASCAL.

Intrusion detection services protect against attacks of various types on the system's legitimate (open) services. IDS protection is provided at both the IP and transport layers.



IP packet filtering blocks out all IP traffic that this systems doesn't specifically permit.

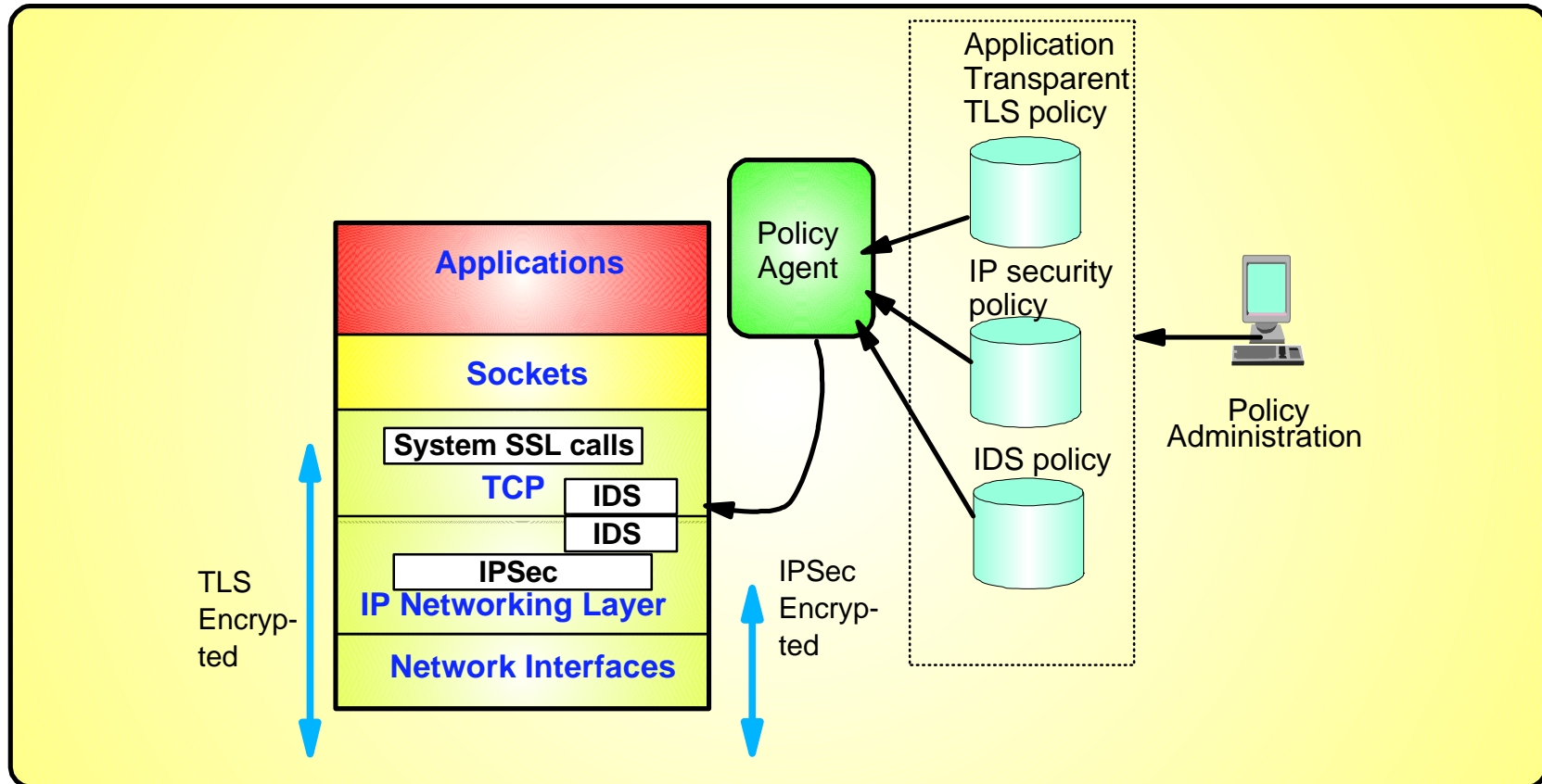
IPSec resides at the networking layer and is transparent to upper-layer protocols, including both transport layer protocol and application protocol.

# **z/OS Communications Server Network Security**

## **Policy-based Network Security**

- IP Security
- Application Transparent TLS
- Intrusion Detection Services

# Policy-based Network Security Overview



- Policy-driven using Communications Server Policy Agent
  - ▶ Configuration for each TCP/IP stack defines security requirements
- Network security without requiring application changes
  - ▶ Security services provided by the TCP/IP stack
    - AT-TLS, IP security, IDS
- Configure AT-TLS, IP security, IDS policy with a single, consistent administrative interface using Configuration Assistant for z/OS
  - ▶ Focus on what traffic to protect and how to protect
  - ▶ Less focus on low level details
    - (Though available on expert panels)

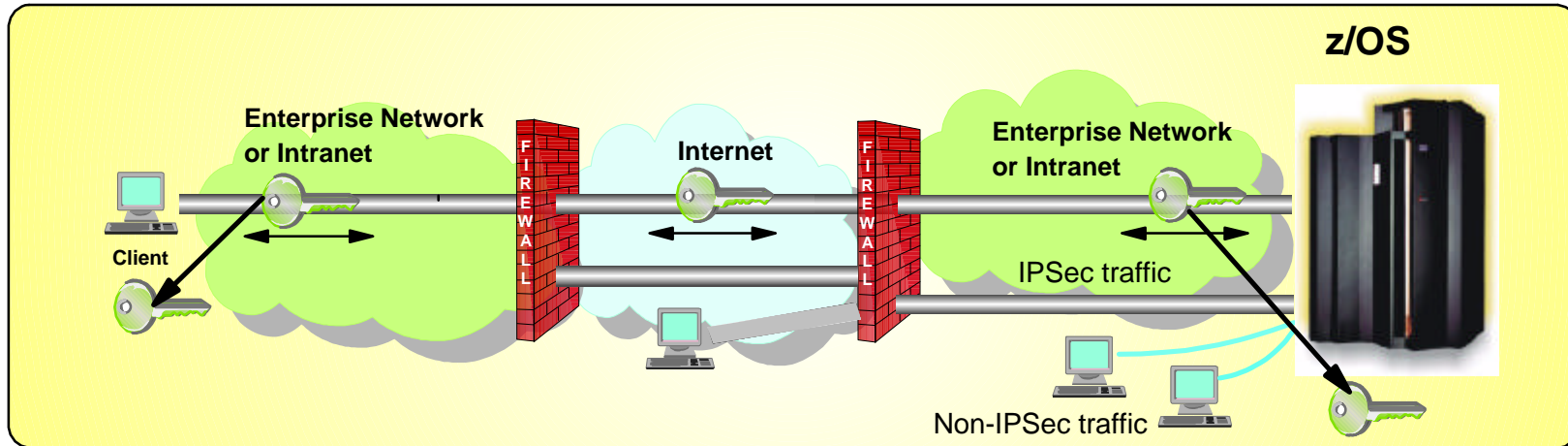


# z/OS Communications Server Network Security

## **IP Security**

- IP packet filtering
- IPSec

# z/OS IP security support



- Prior to z/OS V1R7, IP security packaged with Firewall Technologies
  - ▶ TCP/IP IPsec and IP filtering support
    - Communications Server
  - ▶ IKE daemon and configuration
    - Integrated Security Services
- In z/OS V1R7, complete IPsec, IP filtering, and IKE solution part of z/OS Communications Server
  - ▶ Alternative to Firewall Technologies
    - New IKE daemon and configuration
  - ▶ Services
    - IP filtering
    - Manual IPsec
    - Dynamic IPsec (IKE)
    - Filter directed logging to syslogd

# Firewall Technologies

- Starting in z/OS V1R8, Firewall Technologies is no longer available

## Announced Feb 15th, 2005

- z/OS V1.7 is the last z/OS release to include the Firewall Technologies component of the Integrated Security Services element.
- Many Firewall Technologies functions have been stabilized for some time and can be replaced using comparable or better functions provided by or planned for Communications Server, notably,
  - ▶ IPsec
  - ▶ IP packet filtering
  - ▶ In addition, a functionally rich downloadable tool is planned to replace the IPsec and IP Filtering configuration GUI support.
- The following functions will be removed without replacement:
  - ▶ FTP Proxy services
  - ▶ Socks V4 services
  - ▶ Network Address Translation (NAT)
  - ▶ RealAudio support

# z/OS Communications Server

## IP security features

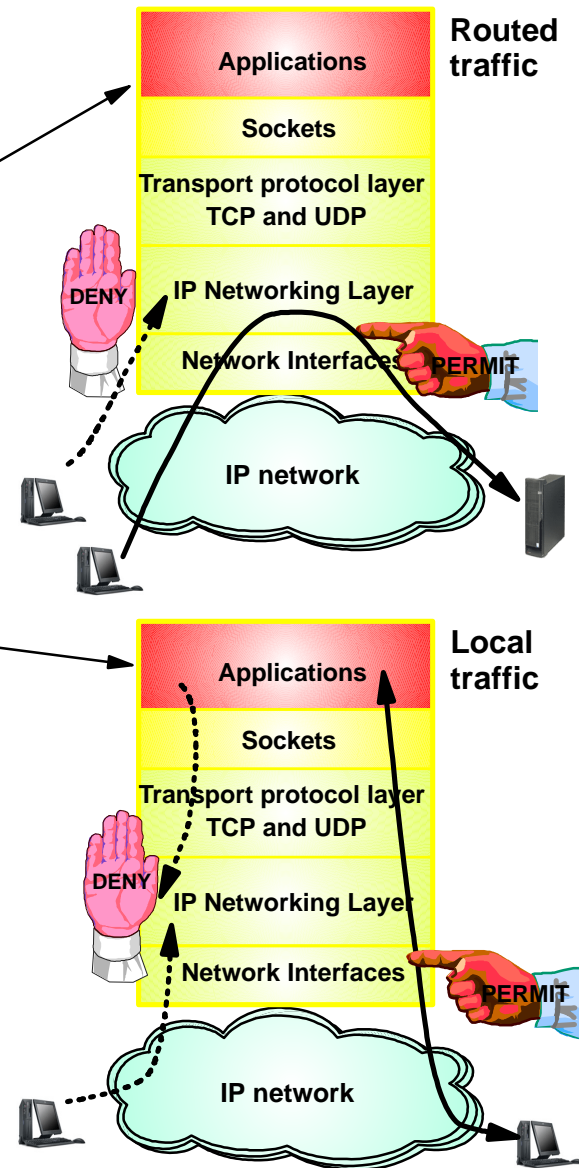
- **Configuration support**
  - ▶ Optimized for z/OS host-to-host and z/OS host-to-gateway (z/OS gateway still supported)
  - ▶ IPsec NAT Traversal support
    - IP address translation
    - Port translation (V1R8)
  - ▶ IPv4 and IPv6 support (IPv6 in V1R8)
- **Simplified infrastructure**
  - ▶ Eliminates need for FW Technologies daemons
  - ▶ Policy agent reads and manages IPsec and IKE policy
- **Simplified configuration**
  - ▶ New configuration GUI for both new and expert users
  - ▶ Direct file edit into local configuration file
  - ▶ Reduced definition, more "wildcarding"
- **Improved serviceability**
  - ▶ Improved messages and traces
- **Default filters part of TCP profile**
  - ▶ More granular control before policy is loaded
- **Administrative controls**
  - ▶ pasearch
  - ▶ ipsec command
- **Cryptographic algorithms (\*\* uses cryptographic hardware if available)**
  - ▶ DES(\*\*) and 3DES(\*\*) encryption
  - ▶ HMAC-SHA (\*\*) and HMAC-MD5 authentication
  - ▶ AES (\*\*) encryption (V1R8)

- 
- **z/OS Communications Server IP security covers:**
    - ▶ IP filtering
    - ▶ IPsec

# IP Packet Filtering Basics

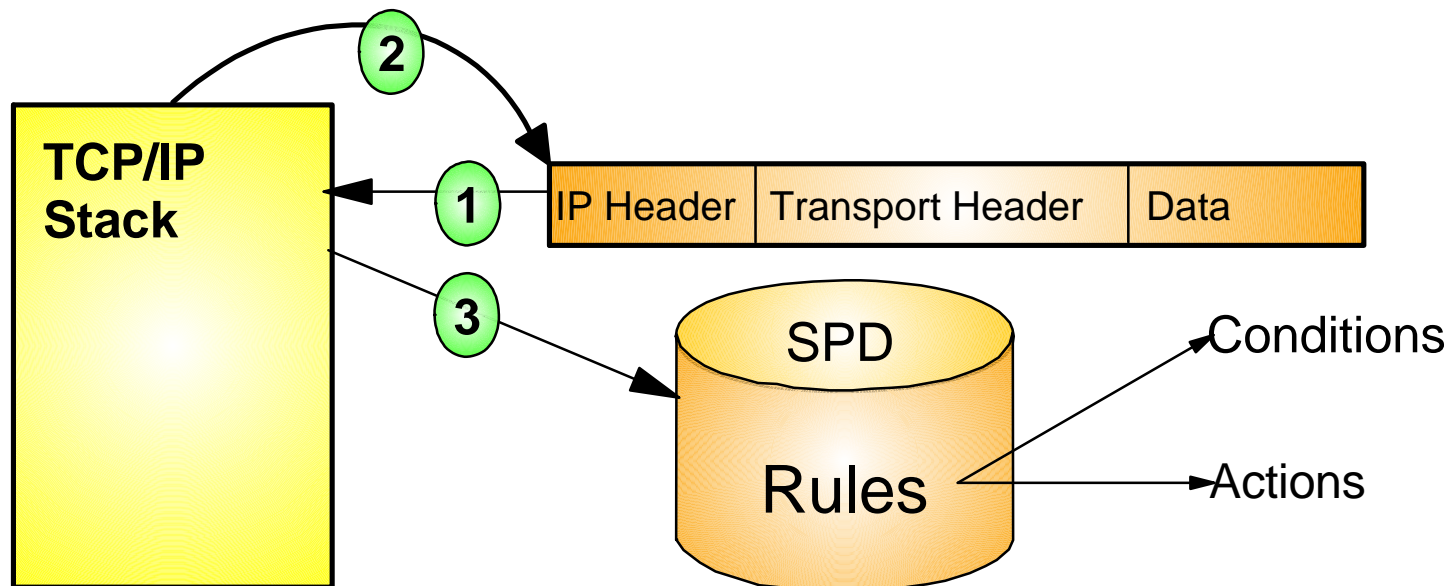
## Packet filtering at IP Layer

- Filter rules defined to match on inbound and outbound packets based on:
  - ▶ packet information
    - IP address, port, protocol
  - ▶ network attributes
    - direction, link security
  - ▶ time
- Used to control
  - ▶ traffic being routed
  - ▶ access at server
    - "Personal firewall" on z/OS
- Possible actions
  - ▶ 1. Permit
  - ▶ 2. Deny
  - ▶ 3a. Permit with manual IPsec
  - ▶ 3b. Permit with dynamic IPsec
  - ▶ Log
    - in combination with other actions



# IP Packet Filtering Processing Overview

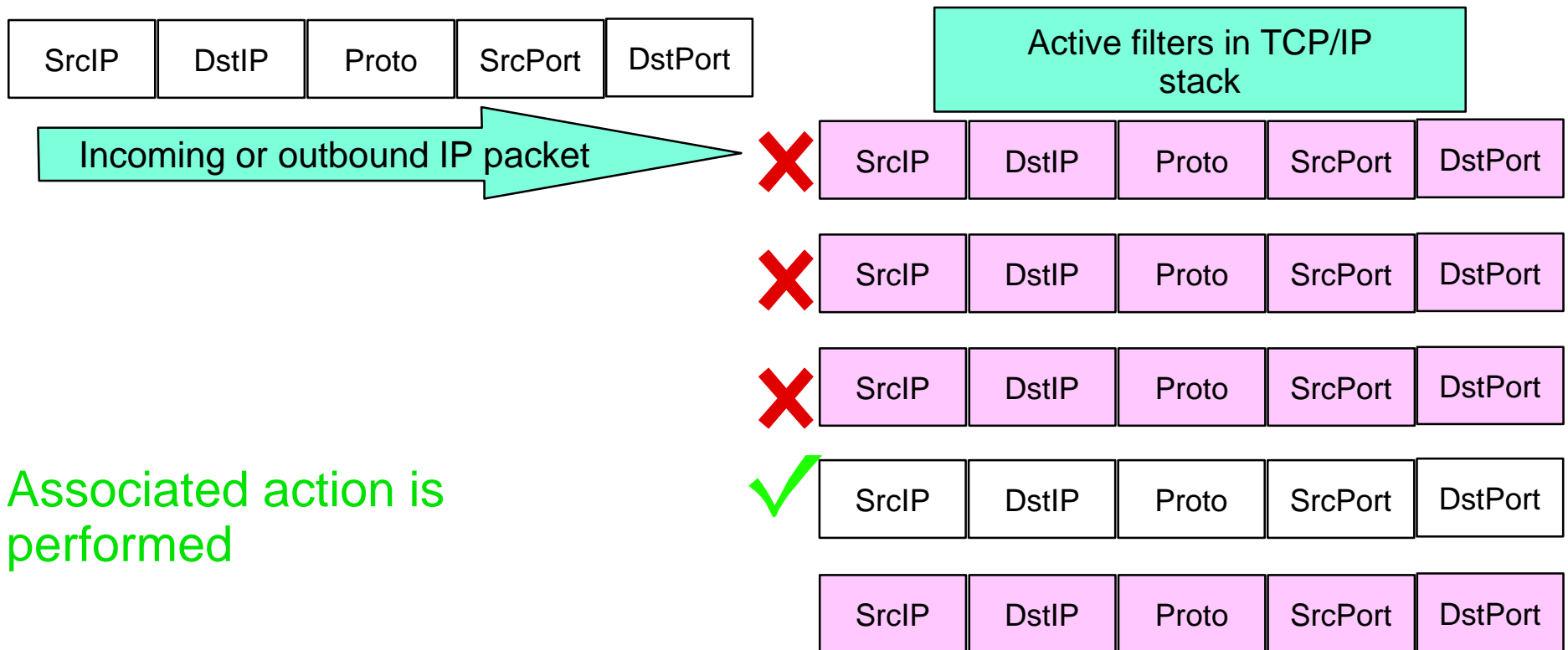
1. Inbound or outbound IP packet arrives
2. Consult filter rules in a Security Policy Database (SPD)
  - ▶ Rules have conditions and actions
3. Apply action of matching rule to packet
  - ▶ Deny
  - ▶ Permit
  - ▶ Permit with additional processing applied



# IP Filtering Concepts

## Filter Matching

1. Filters are searched in the order they were configured
2. Each rule is inspected, from top to bottom, for a match
3. If a match is found, the search ends and the action is performed

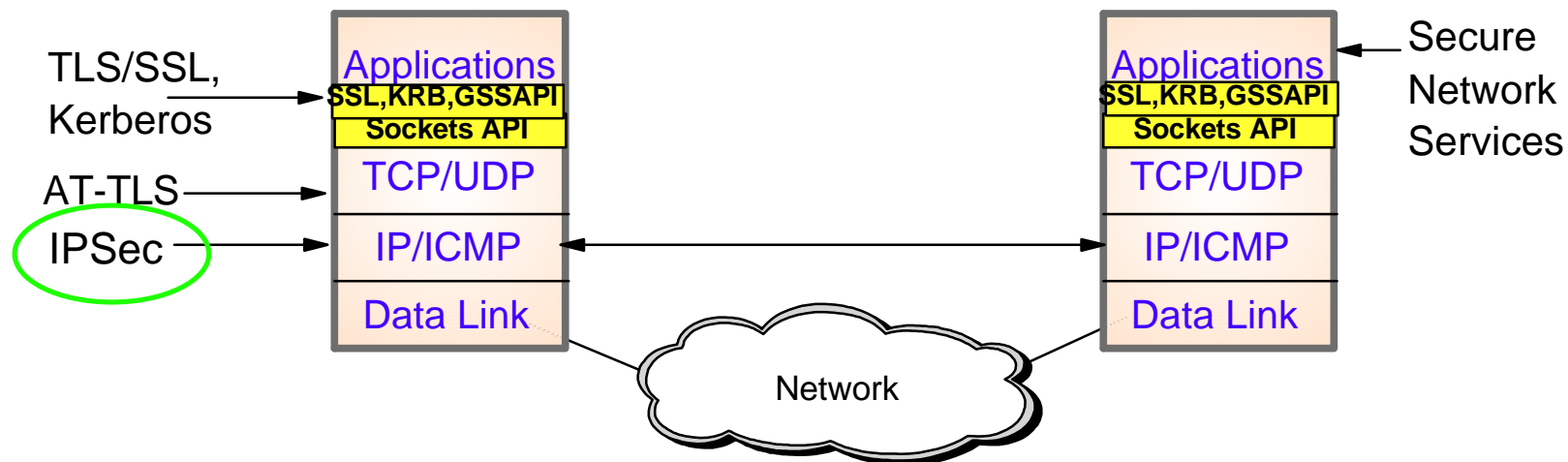


# Filtering conditions

Criteria	Description
<b>From packet</b>	
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
<b>Network attributes</b>	
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.
<b>Time condition</b>	
Time, Day, Week, Month	Indicates when filter rule is active



# IPSec Protocol Overview

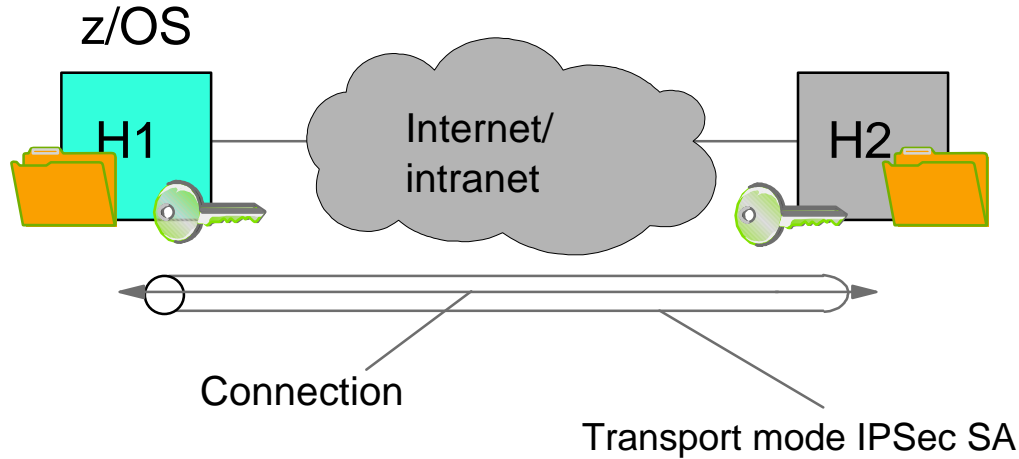


- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
  - ▶ IPSec security protocols
    - **Authentication Header (AH)** - provides authentication / integrity
    - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional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

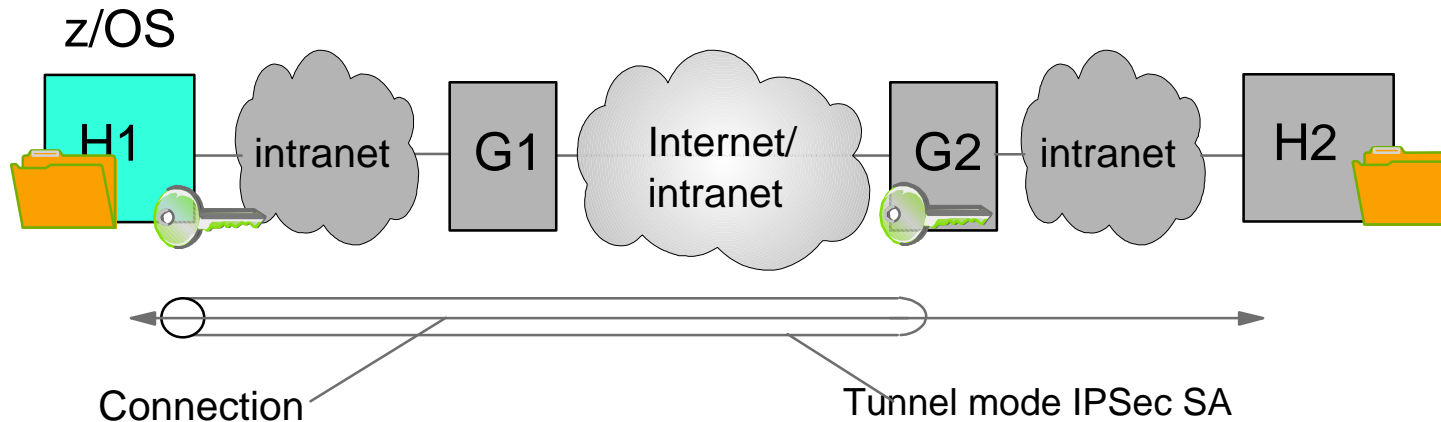
# IPSec Scenarios

## z/OS as Host



### Host-to-Host: End-to-End Security Association



### Host-to-gateway: Protect segment of data path



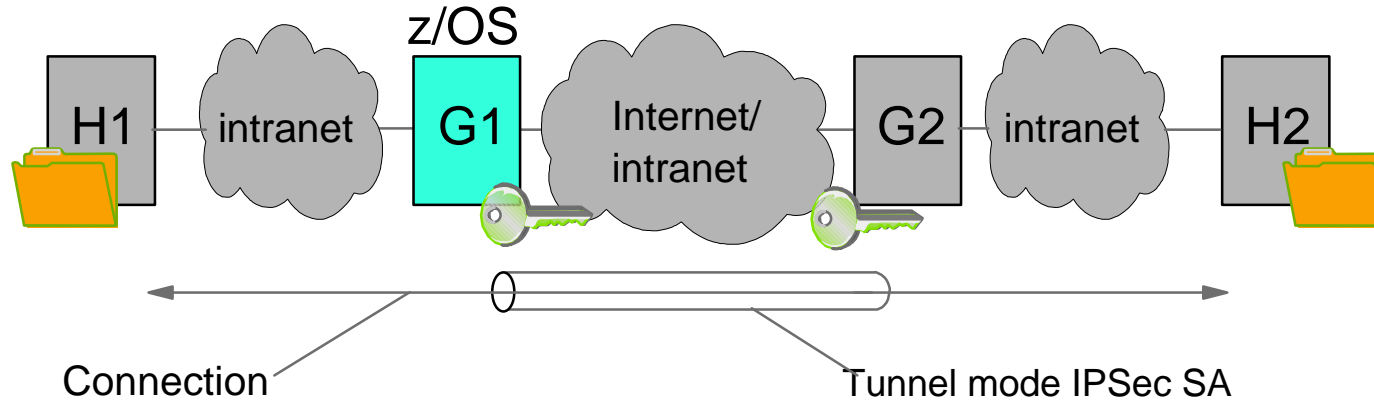
**Legend**

- Data endpoint 
- Security endpoint 

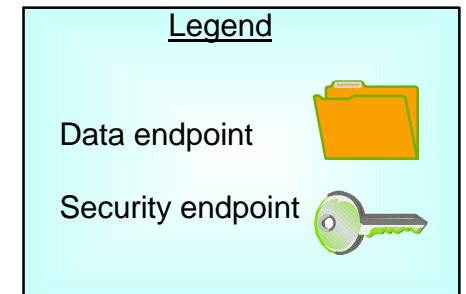
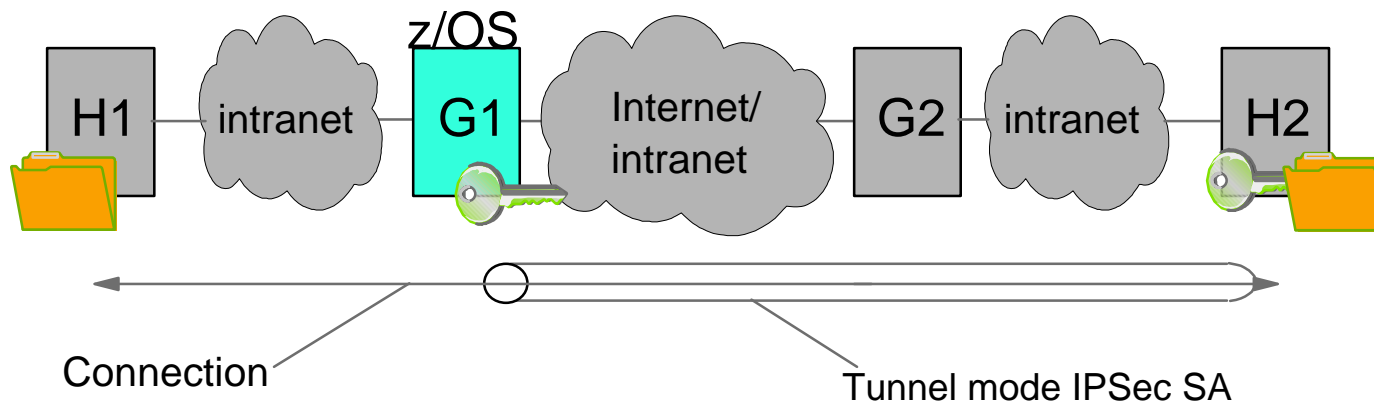
# IPSec Scenarios

## z/OS as Gateway

### Gateway-to-Gateway: Protection over Untrusted Network Segment



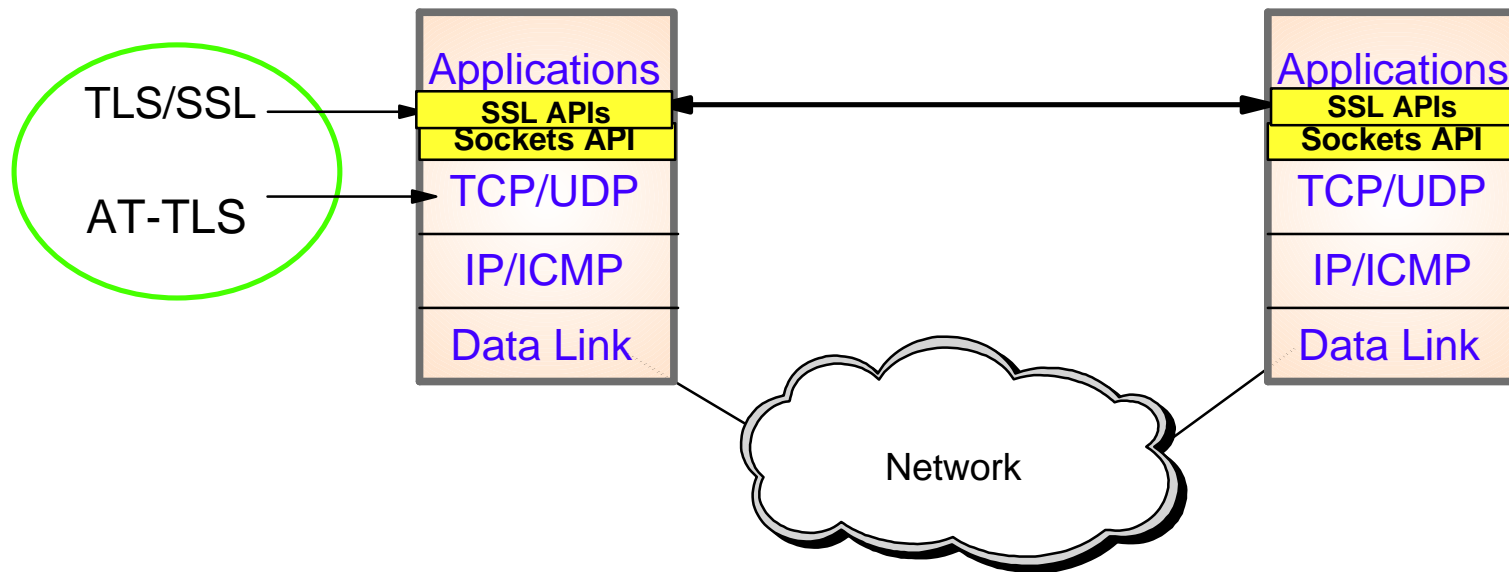
### Gateway-to-Host: Protection over Untrusted Network Segment



# **z/OS Communications Server Network Security**

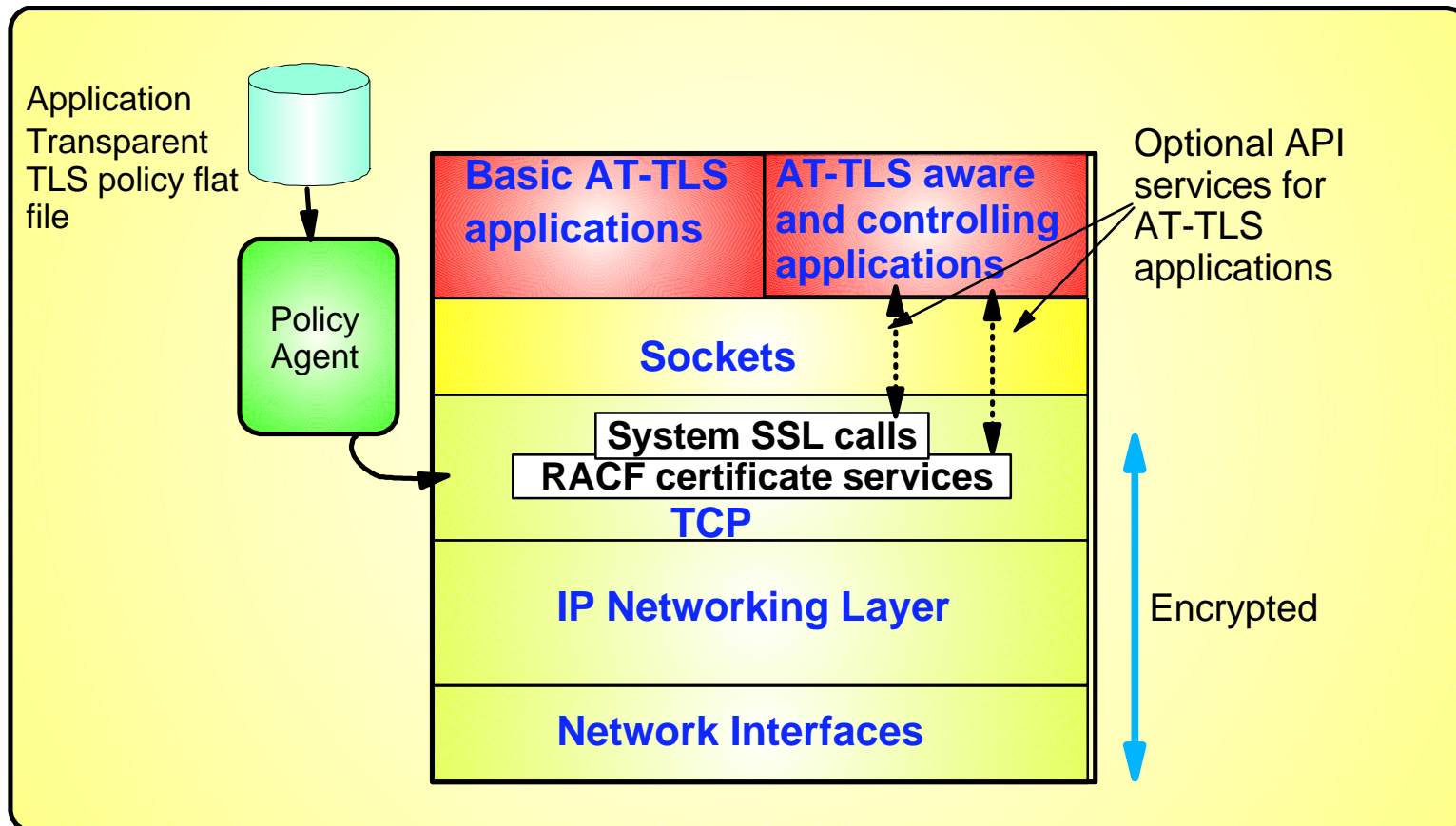
## **Application Transparent Transport Layer Security**

# 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
  - ▶ Requires reliable transport layer
    - UDP applications cannot be TLS enabled
- z/OS applications can be TLS enabled with System SSL
  - ▶ System SSL part of z/OS Integrated Security Services element
- 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



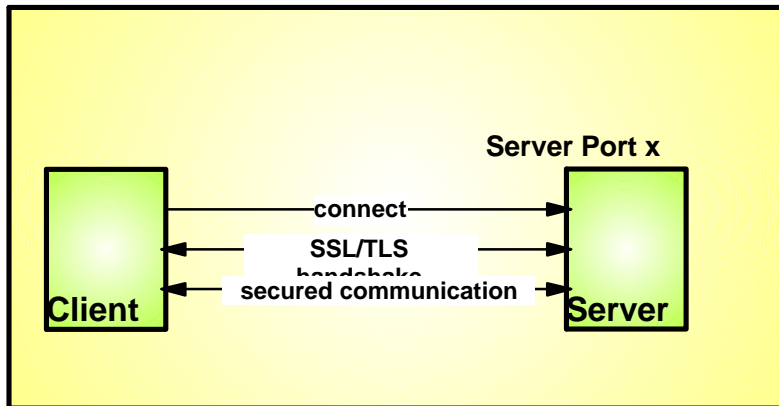
- **Most applications require no change to use AT-TLS**
  - ▶ AT-TLS Basic applications
- **Applications can optionally exploit advanced features using new SIOCTTLSCT ioctl call**
  - ▶ AT-TLS Aware applications
    - Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)
  - ▶ AT-TLS Controlling applications
    - Control if/when to start TLS. reset session / cipher

# AT-TLS Advantages

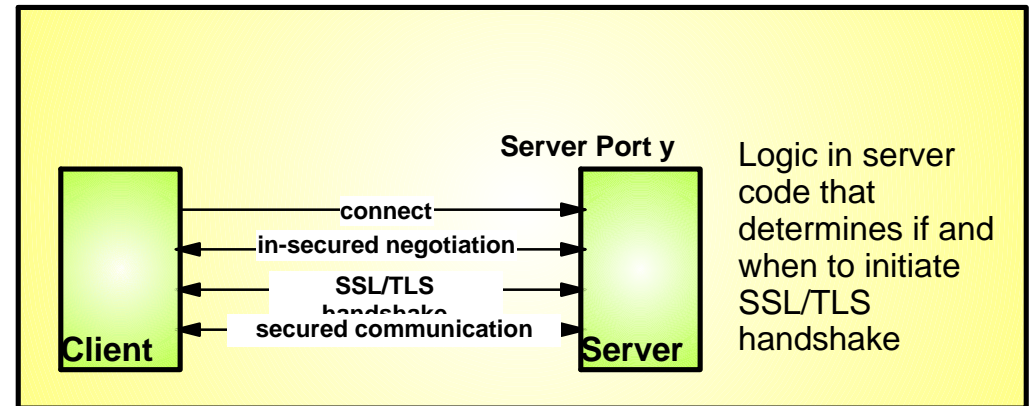
- AT-TLS provides SSL/TLS features above and beyond what most SSL/TLS applications choose to support -
  - ▶ Support for Certificate Revocation Lists (CRLs)
  - ▶ Multiple keyrings per server
  - ▶ Optional use of system SSL cache,
- AT-TLS uses an optimized SSL/TLS infrastructure that performs better than when SSL/TLS is implemented directly in the applications
  - ▶ FTP workload measurements show up to a 35% performance improvement
- 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.

# AT-TLS application types

## Port-determined use of SSL/TLS



## Application-negotiated use of SSL/TLS



### ■ Characteristics:

- ▶ As soon as a connection has been established with the server, the SSL/TLS handshake starts
- ▶ Examples are the HTTPS port (443), and in some cases a TN3270 server port (Conntype Secure)

### ■ AT-TLS considerations:

- ▶ Can be done totally transparently to application code
  - This is referred to as an AT-TLS "Basic" application
- ▶ Optionally the application may query SSL/TLS attributes, such as client user ID (if client authentication is used, cipher suite in use, etc)
  - This is referred to as an AT-TLS "Aware" application

### ■ Characteristics:

- ▶ Application protocol includes verbs to negotiate security protocol and options
- ▶ Examples are FTP that uses the AUTH FTP command to negotiate use of SSL/TLS or Kerberos, and in some cases a TN3270 server port (Conntype NegtSecure)

### ■ AT-TLS considerations:

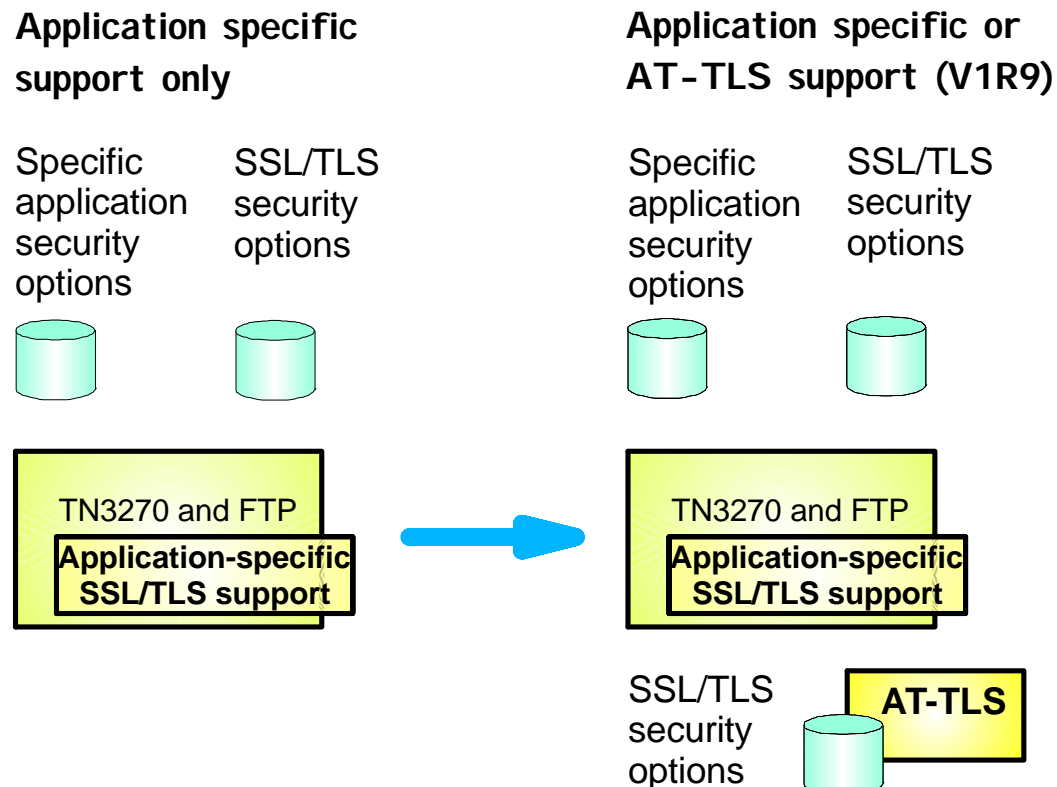
- ▶ Application needs to "tell" AT-TLS when to start the SSL/TLS handshake
  - This is referred to as an AT-TLS "Controlling" application
- ▶ Otherwise, use of AT-TLS is transparent to application
- ▶ Optionally the application may query SSL/TLS attributes, such as client user ID (if client authentication is used, cipher suite in use, etc)



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

## z/OS V1R9 Enhancement

- **Both the FTP server and client, and the TN3270 server 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, FTP and TN3270 are enabled to be AT-TLS aware and controlling**
- **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

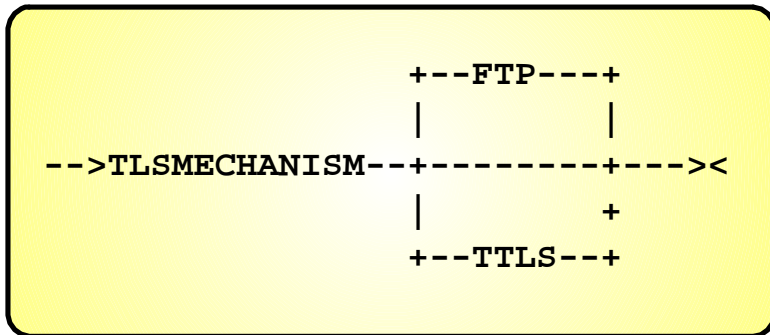


# AT-TLS enabling FTP

z/OS V1R9 Enhancement

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

- ▶ **TLSMECHANISM** (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-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)

- **FTP SSL/TLS security options**

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

# AT-TLS enabling TN3270

## z/OS V1R9 Enhancement

- **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**

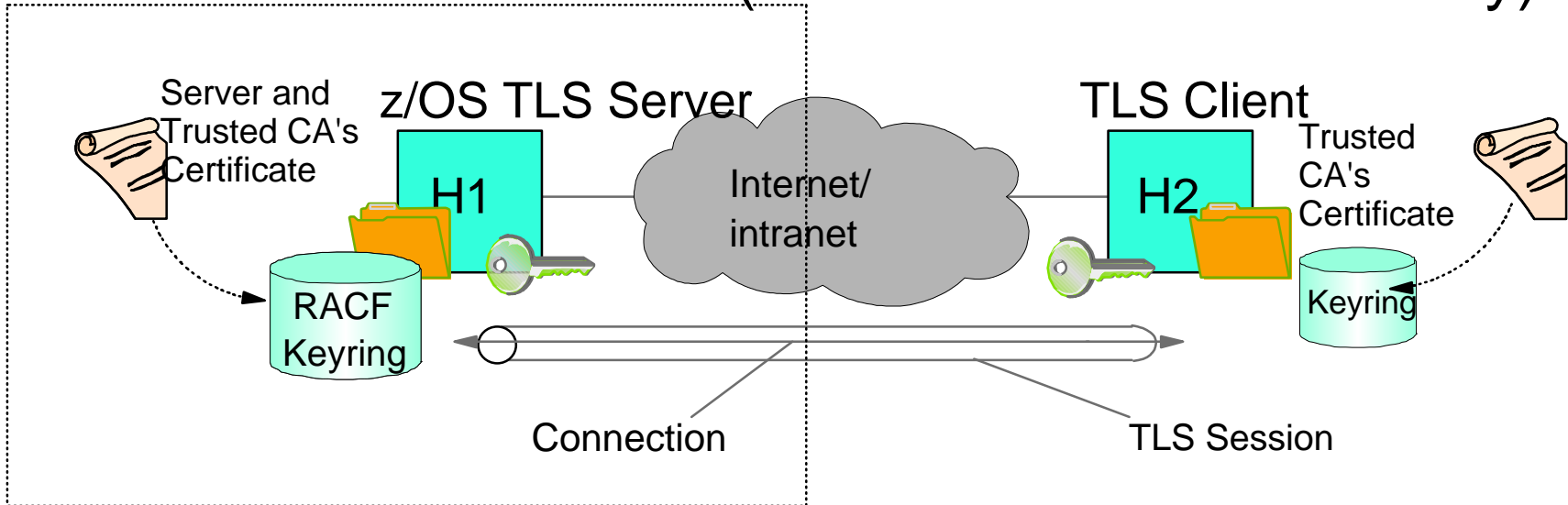
- ▶ **KEYRING**
- ▶ **CRLLDAPSERVER**
- ▶ **CLIENTAUTH**
  - SSLCERT
  - SAFCERT
- ▶ **ENCRYPTION**
- ▶ **SSLTIMEOUT**
- ▶ **SSLV2/SSLNOV2**

# AT-TLS Policy Conditions

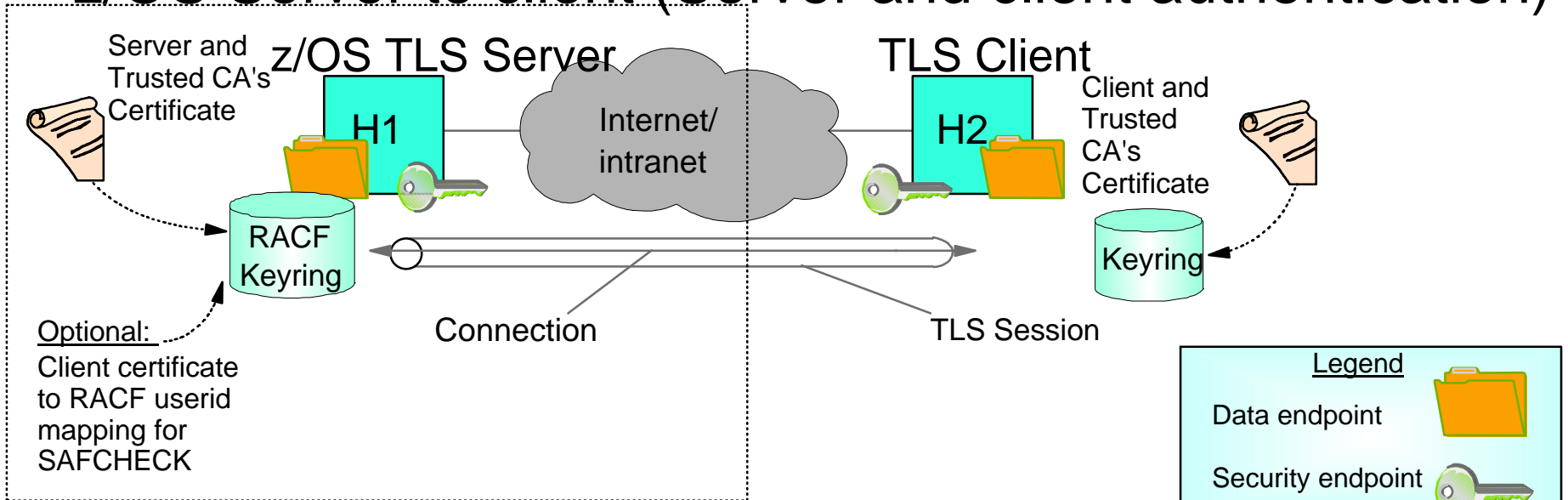
Criteria	Description
<b>Resource attributes</b>	
Local address	Local IP address
Remote address	Remote IP address
Local port	Local port or ports
Remote port	Remote port or ports
<b>Connection type attributes</b>	
Connection direction	<ul style="list-style-type: none"><li>• Inbound (applied to first Select,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

# z/OS AT-TLS Server Roles



## z/OS Server to client (Server authentication only)



## z/OS Server to client (Server and client authentication)

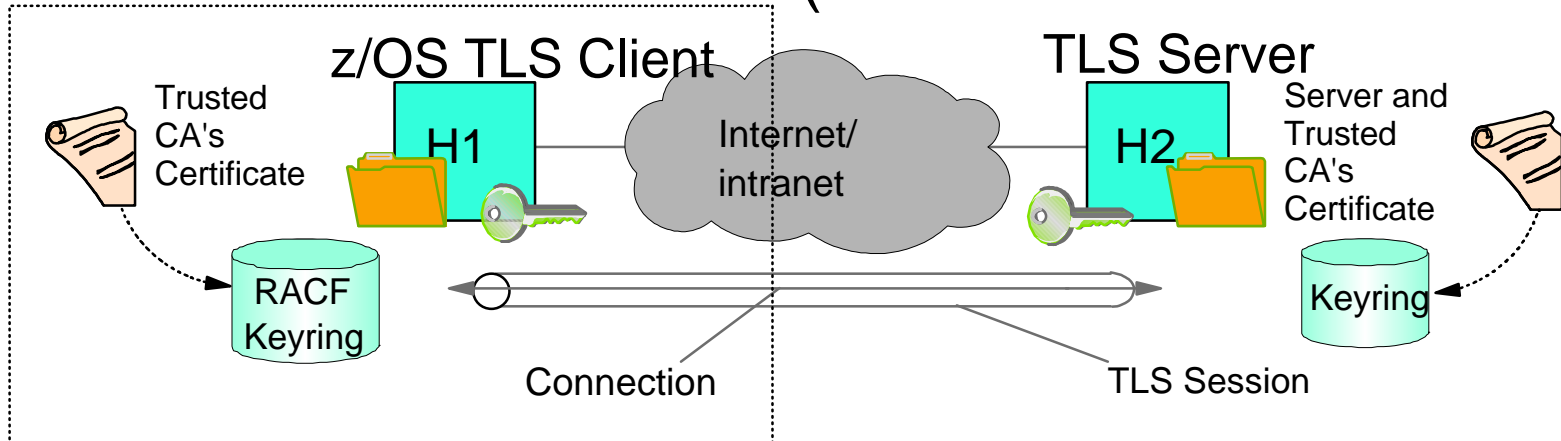


**Legend**

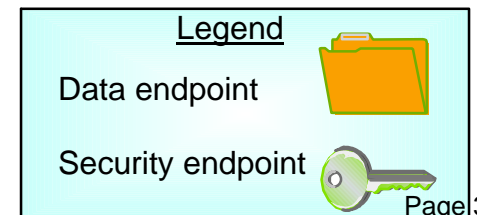
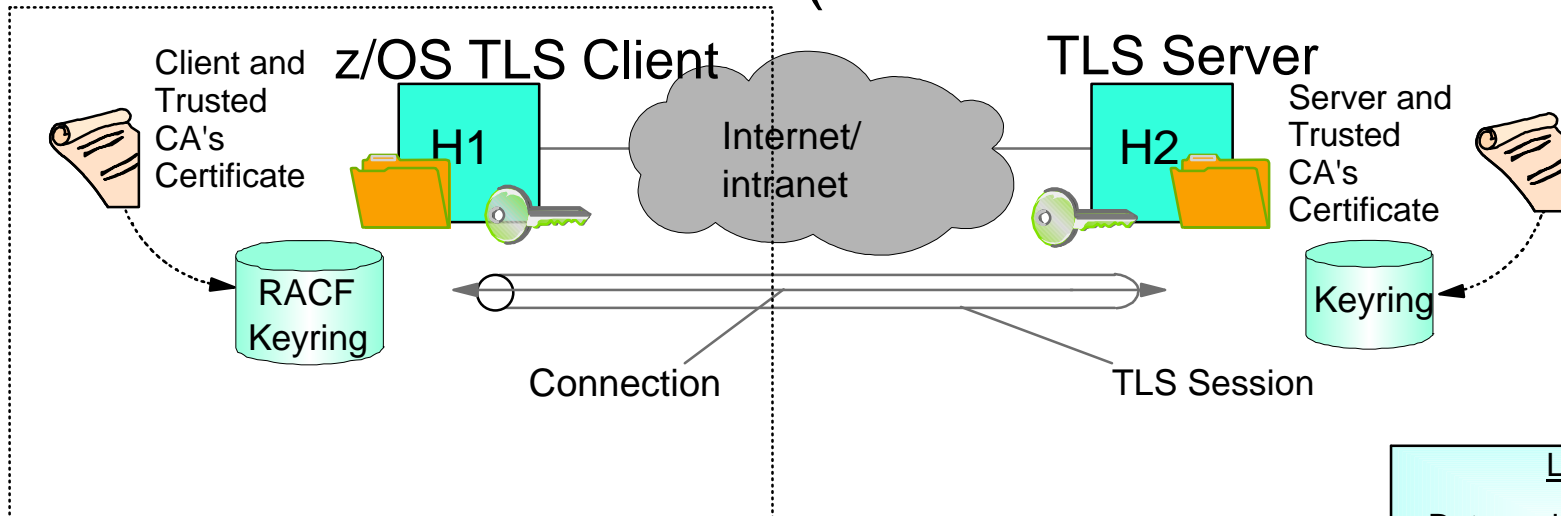
- Data endpoint 
- Security endpoint 

# z/OS AT-TLS Client Roles

## z/OS Client to Server (Server authentication only)



## z/OS Client to Server (Server and client authentication)



# IPSec and AT-TLS Comparison

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

# z/OS Communications Server Network Security

## **Intrusion Detection Services**



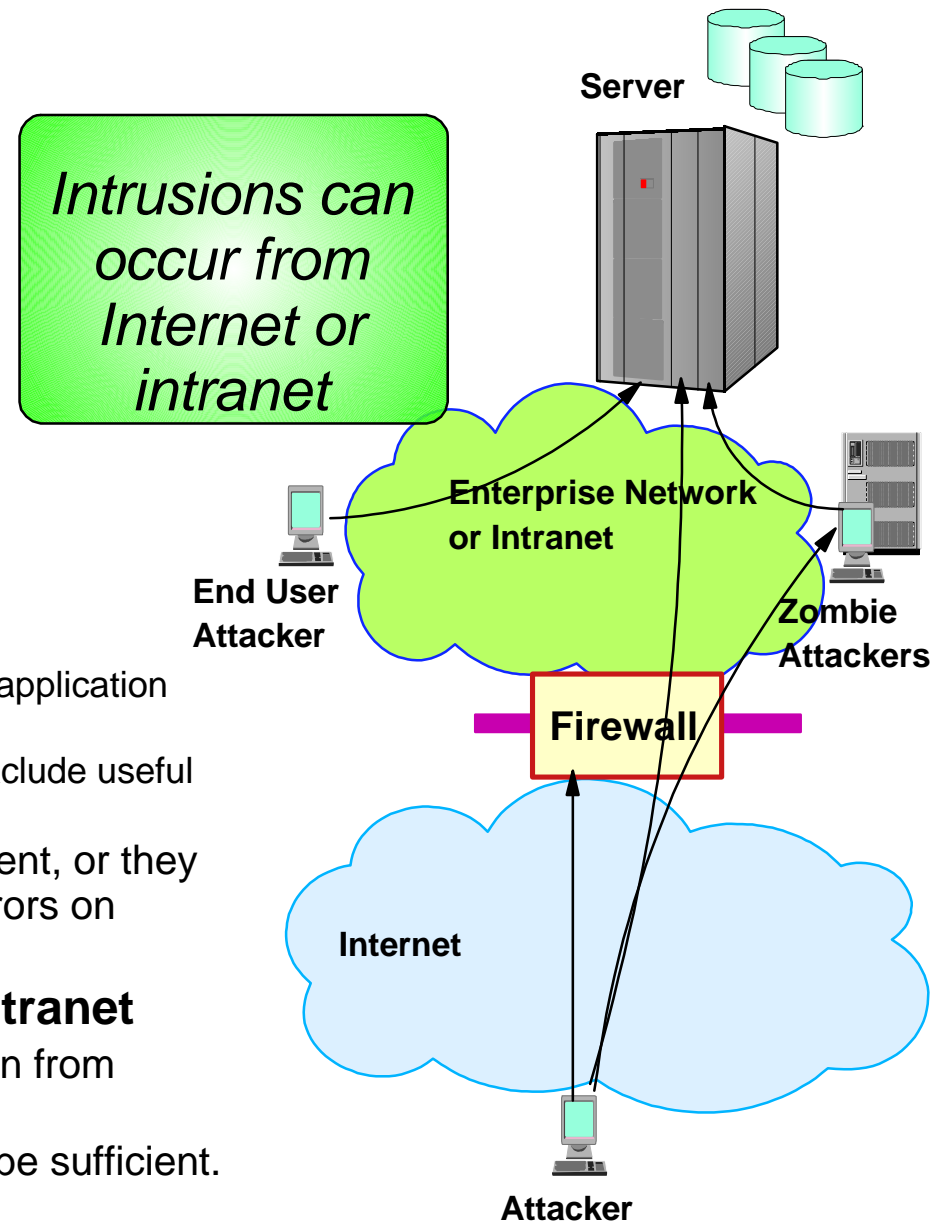
# The Intrusion Threat

## • What is an intrusion?

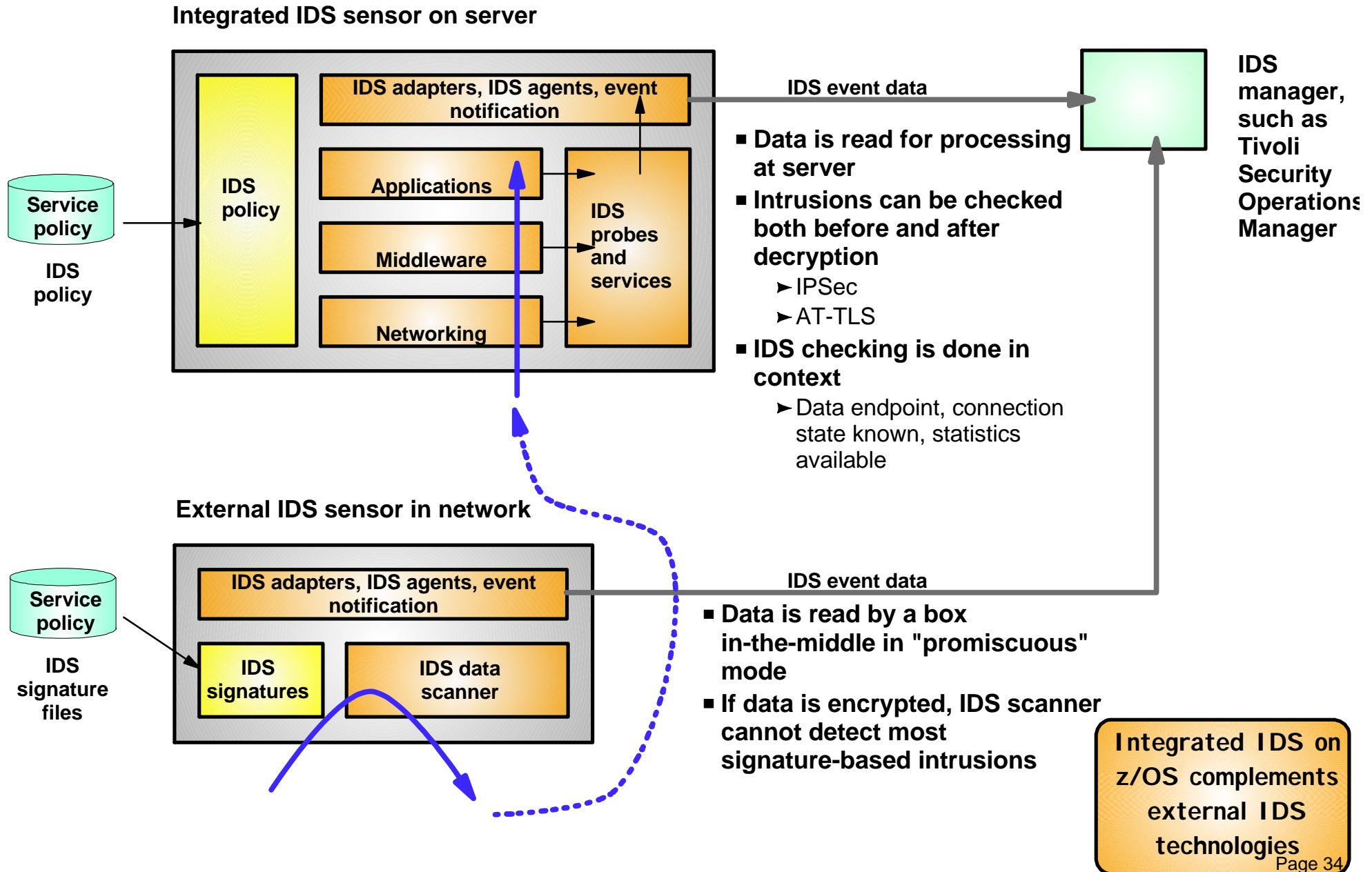
- ▶ Information Gathering
  - Network and system topology
  - Data location and contents
- ▶ Eavesdropping/Impersonation/Theft
  - On the network/on the host
  - Based for further attacks on others
    - ✓ Amplifiers
    - ✓ Robot or zombie
- ▶ Denial of Service
  - Attack on availability
    - ✓ Single Packet attacks - exploits system or application vulnerability
    - ✓ Multi-Packet attacks - floods systems to exclude useful work
- ▶ Attacks can be deliberate with malicious intent, or they can occur as a result of various forms of errors on nodes in the network

## • Attacks can occur from Internet or intranet

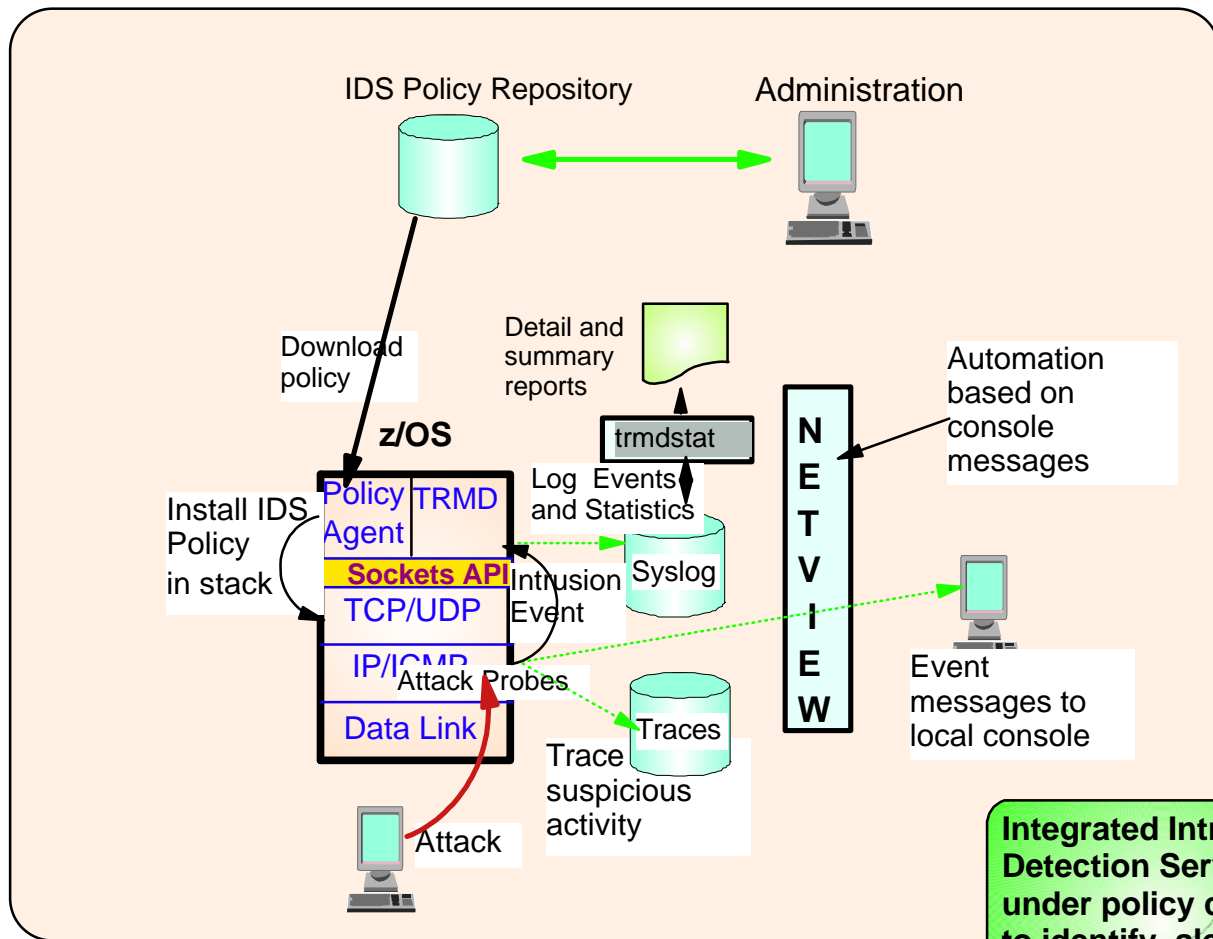
- ▶ Firewall can provide some level of protection from Internet
- ▶ Perimeter Security Strategy *alone* may not be sufficient.
  - Considerations:
    - ✓ Access permitted from Internet
    - ✓ Trust of intranet



# Integrated vs. External Intrusion Detection Concepts



# Z/OS Intrusion Detection Services Overview



## Events detected

- Scans
- Attacks Against Stack
- Flooding (both TCP and UDP)

## Defensive methods

- Packet discard
- Limit connections

## Reporting

- Logging,
- Event messages to local console,
- IDS packet trace
- Notifications to Tivoli NetView and Tivoli Security Operations Manager

## IDS Policy Repositories

- LDAP
- Flat file support as LDAP alternative

▶ **New in V1R8**

## z/OS IDS broadens intrusion detection coverage:

- Ability to evaluate inbound encrypted data - IDS applied after decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks - IDS policy checked after attack detected
- Detects statistical anomalies real-time - target system has stateful data / internal thresholds unavailable to external IDSs
- Policy can control prevention methods on the target, such as connection limiting and packet discard

# Intrusion Event Types Supported

## ■ Scan detection and reporting

▶ Intent of scanning is to map the target of the attack (Subnet structure, addresses, masks, addresses in-use, system type, op-sys, application ports available, release levels)

- TCP port scans
- UDP port scans
- ICMP scans

✓ Sensitivity levels for all scans can be adjusted to control number of false positives recorded.

## ■ Attack detection, reporting, and prevention

▶ Intent is to crash or hang the system (Single or multiple packet)

- Malformed packet events
- Inbound fragment restrictions
- IP option restrictions
- IP protocol restrictions
- ICMP redirect restrictions
- Flood events (physical interface flood detection and synflood)
- Outbound raw restrictions
- UDP perpetual echo

## ■ Traffic regulation for TCP connections and UDP receive queues

▶ Could be intended to flood system OR could be an unexpected peak in valid requests

- UDP backlog management by port
- TCP total connection and source percentage management by port

✓ All TCP servers that use a UNIX process model to create new process when client connect to them should have a cap on the number of connections (FTP, OtenetD, etc.)

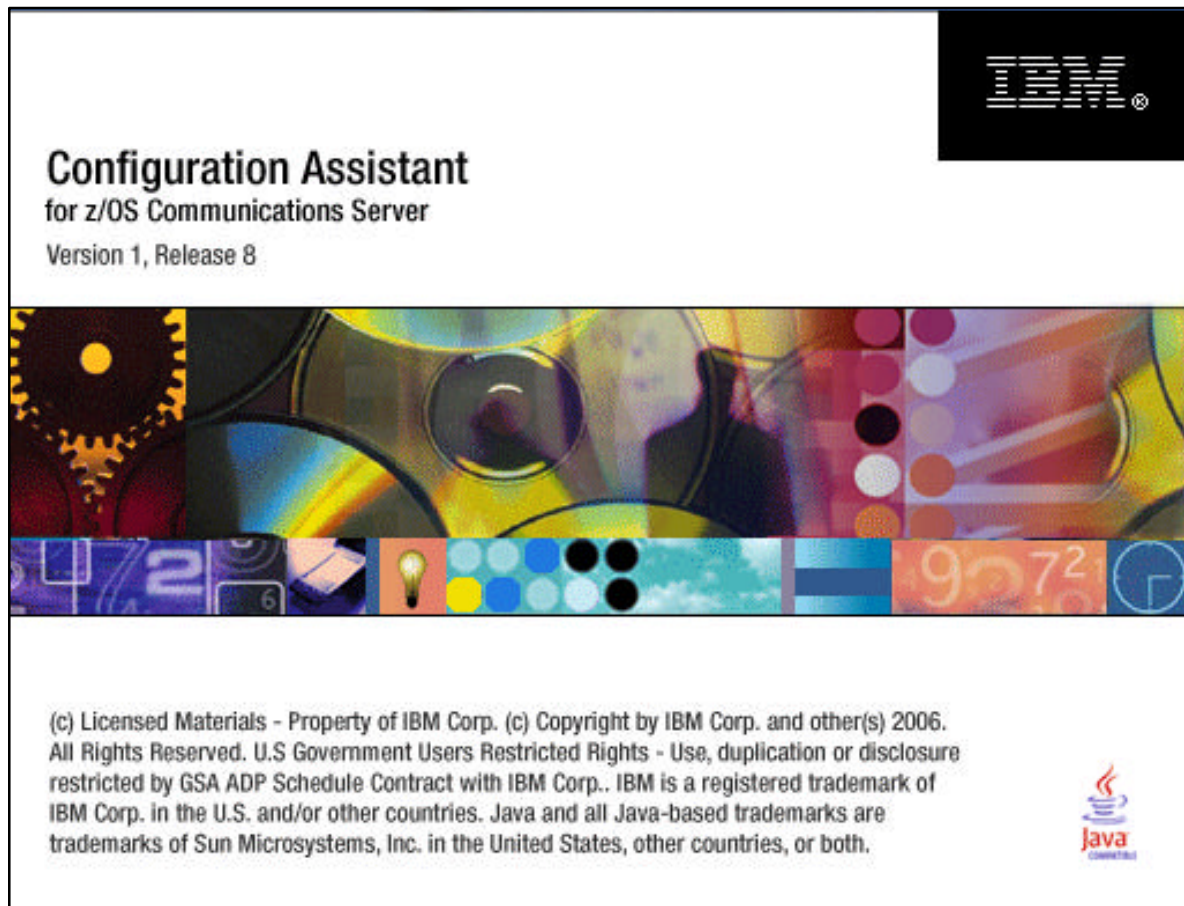
# Tivoli Support for IDS Events

- Tivoli NetView z/OS V5R1, PTF UA11043, provides local z/OS management support for IDS
  - ▶ NetView provides ability to trap IDS messages from the system console or syslog and take predefined actions based on IDS event type such as:
    - Route IDS messages to designated NetView consoles
    - email notifications to security administrator
    - Run trmdstat and attach output to email
    - Issue pre-defined commands
- Tivoli Security Operations Manager provides enterprise-wide management support for IDS
  - ▶ Automated aggregation and correlation of events, logs, and vulnerabilities
    - Broad device support for multi-vendor environments, including security, network, host, and applications
    - Support includes processing for z/OS Communications Server syslog messages for IDS events
  - ▶ Automates policy and regulatory compliance
    - Policy and Regulatory based policy monitoring and reporting

# z/OS Communications Server Network Security

## Configuring Policy-based Network Security

# Configuration Assistant for z/OS Communications Server

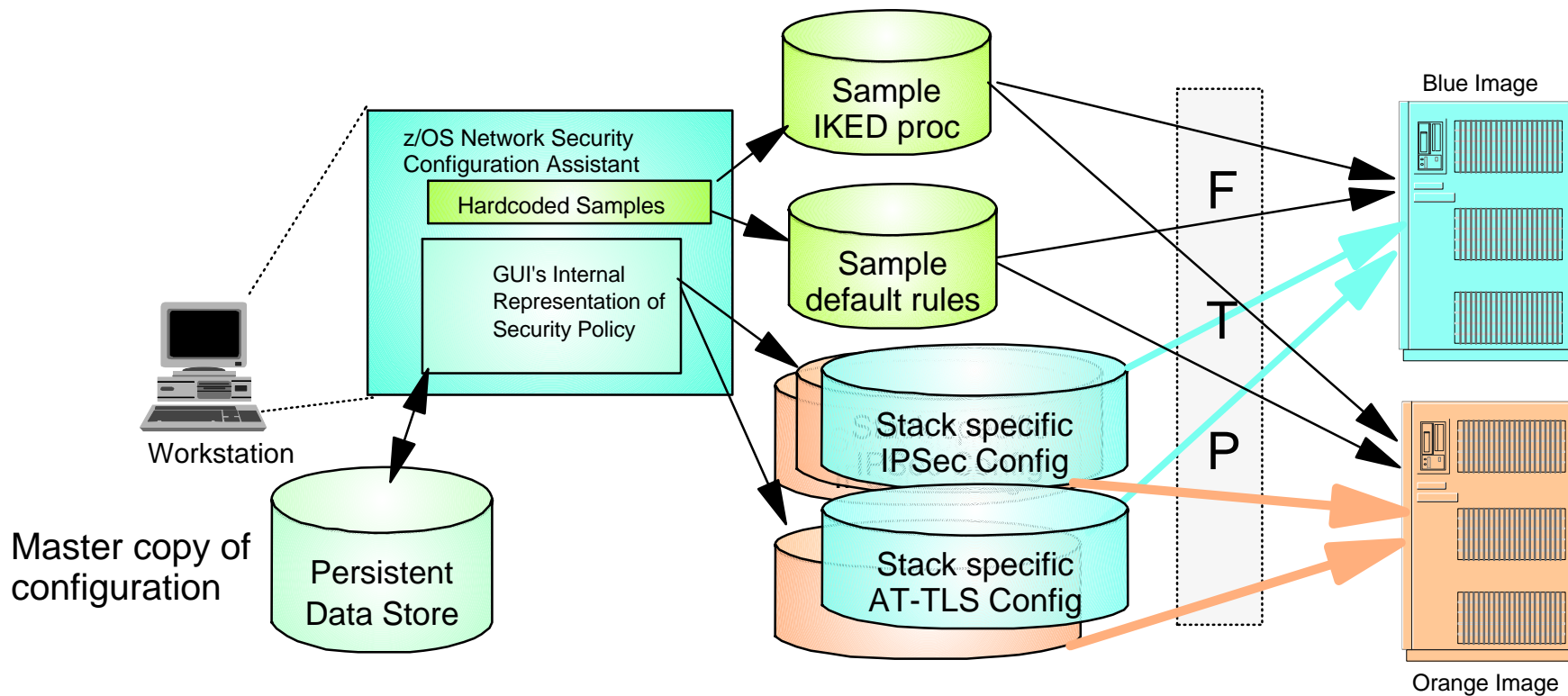


- ▶ In z/OS V1R8 the Policy Agent configuration tools are combined into one tool to manage policies for:
  - ▶ AT-TLS
  - ▶ IPsec and IP filtering
  - ▶ IDS
  - ▶ QoS
- ▶ **Common approach for all policy types:**
  - ▶ Master copy stored in binary file format (on workstation or file server)
  - ▶ Text-based configuration files to be parsed by Policy Agent are created and transferred to z/OS

**Note:** IDS policies may now be stored in a text file, just as the other policy types. There is no requirement for LDAP.

- V1R7 - Network Security Configuration Assistant
  - ▶ Configured policy for IPsec and AT-TLS
- V1R8 - (Name change) Configuration Assistant for z/OS Communications Server
  - ▶ Adds policy configuration support for IDS and QoS

# Configuration Assistant Overview



- Downloadable policy configuration tool runs on workstation
  - ▶ <http://www-1.ibm.com/support/docview.wss?rs=206&uid=swg21181698>
- Allows policy definition to be performed at higher level of abstraction than policy file statements
  - ▶ Define policy for both CS IP security and AT-TLS as a single administrative task
    - Generates separate policy files for CS IP security and AT-TLS
  - ▶ Files created are transferred to z/OS image
- **In V1R9**, new file management improvements
  - ▶ Persistent data store can be stored on z/OS
  - ▶ Locking support at the persistent data store level to prevent inadvertent loss of data

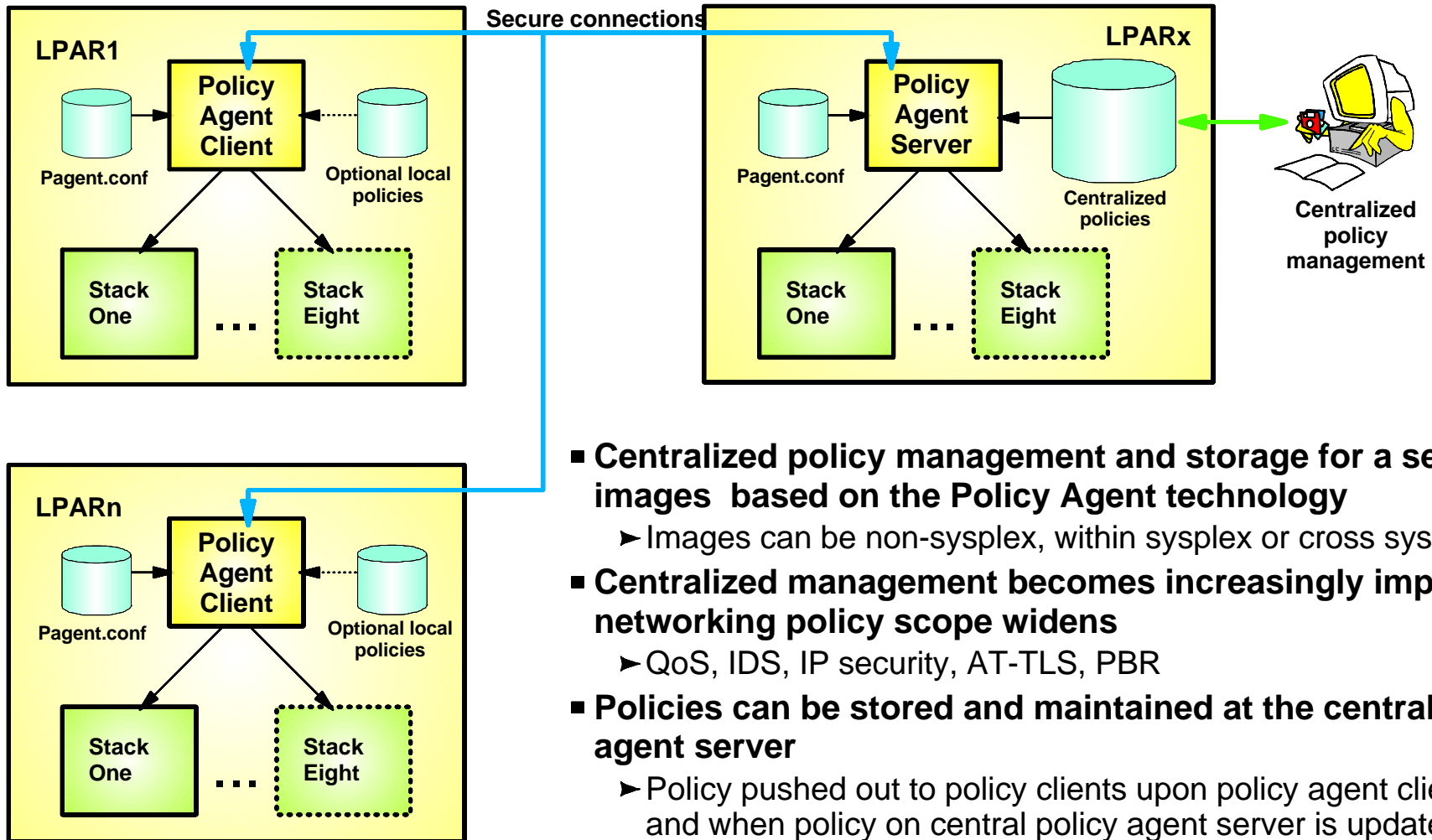


# z/OS Communications Server Network Security

## Enterprise Wide Security Roles

# Centralized networking policy management

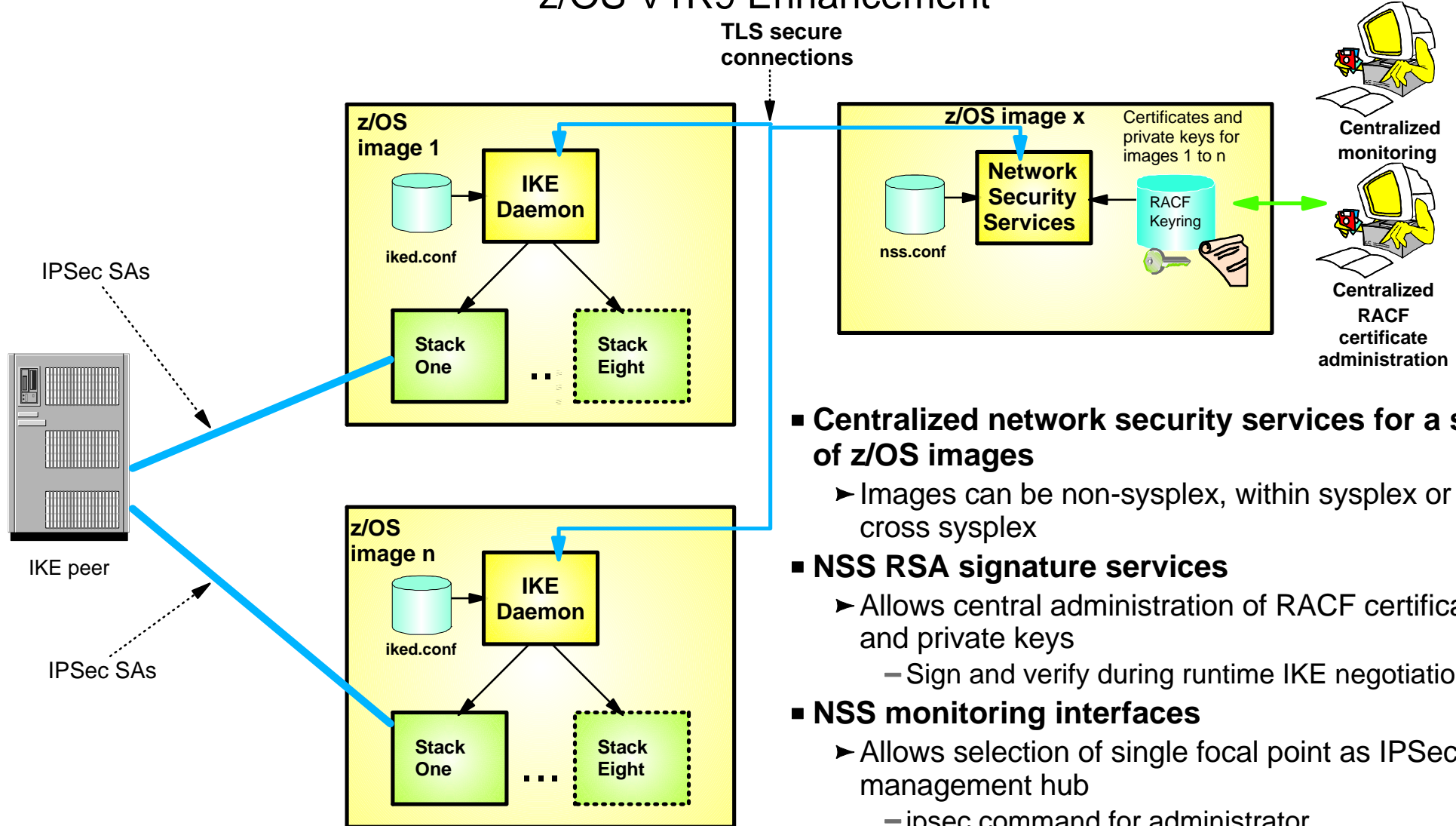
z/OS V1R9 Enhancement



- **Centralized policy management and storage for a set of z/OS images based on the Policy Agent technology**
  - ▶ Images can be non-sysplex, within sysplex or cross sysplex
- **Centralized management becomes increasingly important as networking policy scope widens**
  - ▶ QoS, IDS, IP security, AT-TLS, PBR
- **Policies can be stored and maintained at the central policy agent server**
  - ▶ Policy pushed out to policy clients upon policy agent client request and when policy on central policy agent server is updated.
- **Availability options**
  - ▶ Backup NSS can be specified
- **Policy can be configured with manual edit or with Configuration Assistant for z/OS**

# Network Security Services for IPSec

## z/OS V1R9 Enhancement



- **Centralized network security services for a set of z/OS images**
  - ▶ Images can be non-sysplex, within sysplex or cross sysplex
- **NSS RSA signature services**
  - ▶ Allows central administration of RACF certificate 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 for management application
- **Availability options**
  - ▶ Backup NSS can be specified

# z/OS V1R8 Communications Server Security Enhancements Summary

- IPsec
  - ▶ AES support added
  - ▶ IPv6 supported added
  - ▶ NAT traversal for port translation support added
- Intrusion Detection Services
  - ▶ Policy can reside in a file or data set as an alternative to LDAP repository
- Configuration Assistant
  - ▶ Adds support for IPv6 configuration of AT-TLS and IPsec
  - ▶ Adds support for NAT traversal / AES for IPsec
  - ▶ New IDS support added for simpler configuration of IDS policies
  - ▶ New QoS support added

# z/OS V1R9 Communications Server Security Enhancements Summary

- AT-TLS enablement
  - ▶ AT-TLS enablement for FTP and TN3270
- Configuration Assistant
  - ▶ Support Policy-based routing (PBR) policy
  - ▶ File management
    - Store configuration assistant files on z/OS
    - Lock management
- Enterprise Wide Security
  - ▶ Centralized policy agent
  - ▶ Network security services for IPSec

# For More Information...

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