



Software Group | Enterprise Networking Solutions

z/OS Communications Server Network Security Overview

Lin Overby
Chris Meyer

overbylh@us.ibm.com
meyerchr@us.ibm.com

Trademarks and notices

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

- ▶ Advanced Peer-to-Peer Networking®
- ▶ AIX®
- ▶ alphaWorks®
- ▶ AnyNet®
- ▶ AS/400®
- ▶ BladeCenter®
- ▶ Candle®
- ▶ CICS®
- ▶ DB2 Connect
- ▶ DB2®
- ▶ DRDA®
- ▶ e-business on demand®
- ▶ e-business (logo)
- ▶ e business (logo)®
- ▶ ESCON®
- ▶ FICON®
- ▶ GDDM®
- ▶ HiperSockets
- ▶ HPR Channel Connectivity
- ▶ HyperSwap
- ▶ i5/OS (logo)
- ▶ i5/OS®
- ▶ IBM (logo)®
- ▶ IBM®
- ▶ IMS
- ▶ IP PrintWay
- ▶ IPDS
- ▶ iSeries
- ▶ LANDP®
- ▶ Language Environment®
- ▶ MQSeries®
- ▶ MVS
- ▶ NetView®
- ▶ OMEGAMON®
- ▶ Open Power
- ▶ OpenPower
- ▶ Operating System/2®
- ▶ Operating System/400®
- ▶ OS/2®
- ▶ OS/390®
- ▶ OS/400®
- ▶ Parallel Sysplex®
- ▶ PR/SM
- ▶ pSeries®
- ▶ RACF®
- ▶ Rational Suite®
- ▶ Rational®
- ▶ Redbooks
- ▶ Redbooks (logo)
- ▶ Sysplex Timer®
- ▶ System i5
- ▶ System p5
- ▶ System x
- ▶ System z
- ▶ System z9
- ▶ Tivoli (logo)®
- ▶ Tivoli®
- ▶ VTAM®
- ▶ WebSphere®
- ▶ xSeries®
- ▶ z9
- ▶ zSeries®
- ▶ z/Architecture
- ▶ z/OS®
- ▶ z/VM®
- ▶ z/VSE

- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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

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

Agenda

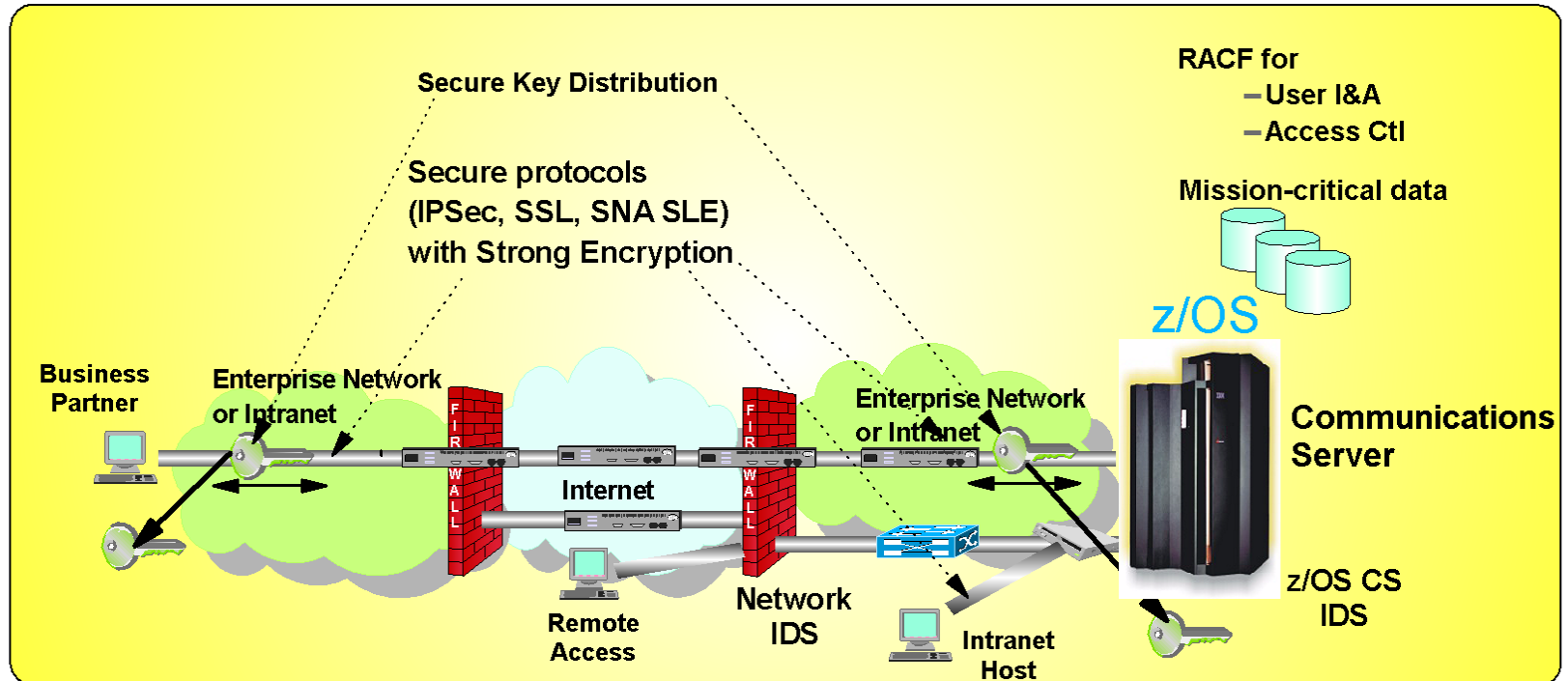
- z/OS Communications Server network security
 - ▶ Roles and objectives
 - ▶ Deployment trends and requirements

- 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 Communications Server
 - ▶ Enterprise Security Roles
 - Centralized Policy Agent
 - Network Security Services

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 System z 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

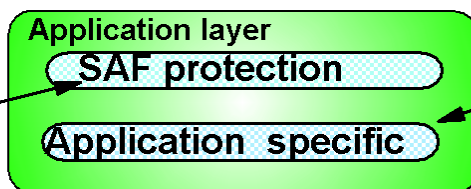
- Protecting the system from the network
 - ▶ Increased access requires focus on self protect
 - ▶ Defense in depth - no longer only perimeter based

- 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

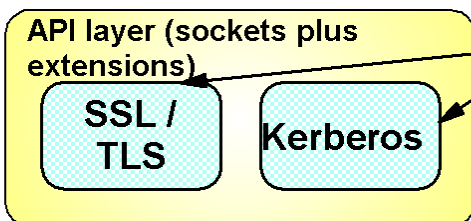
- Minimizing security deployment costs
 - ▶ Application transparent network security reduces application costs
 - ▶ Policy-based network security reduces deployment costs
 - ▶ GUI-based policy administration for ease of use

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..

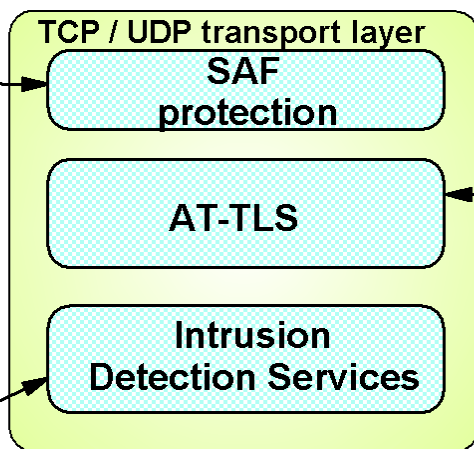


Protect data in the network
Examples of application protocols with built-in security extensions are SNMPv3, DNS, and OSPF.



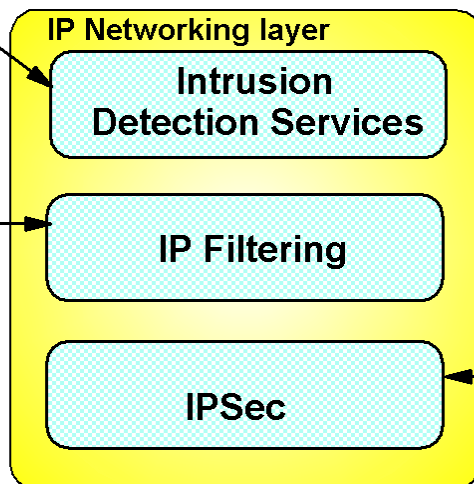
Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

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. These can be configured or can be applied dynamically.

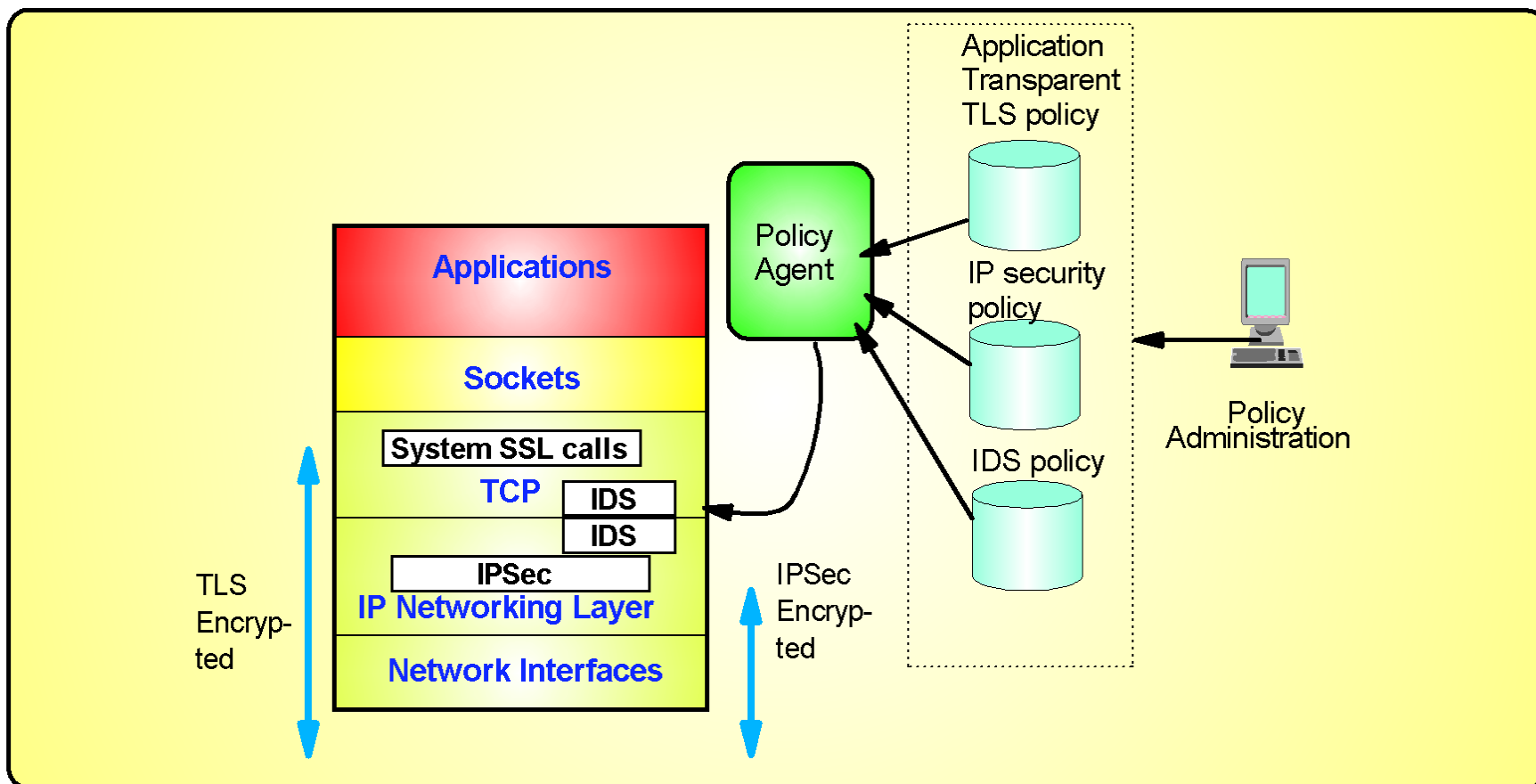
IPSec resides at the networking layer and is transparent to upper-layer protocols, including both transport layer protocol and application protocol.

z/OS Communications Server Network Security

Policy-based Network Security

- IP Security
- Application Transparent TLS
- Intrusion Detection Services

Policy-based Network Security Overview



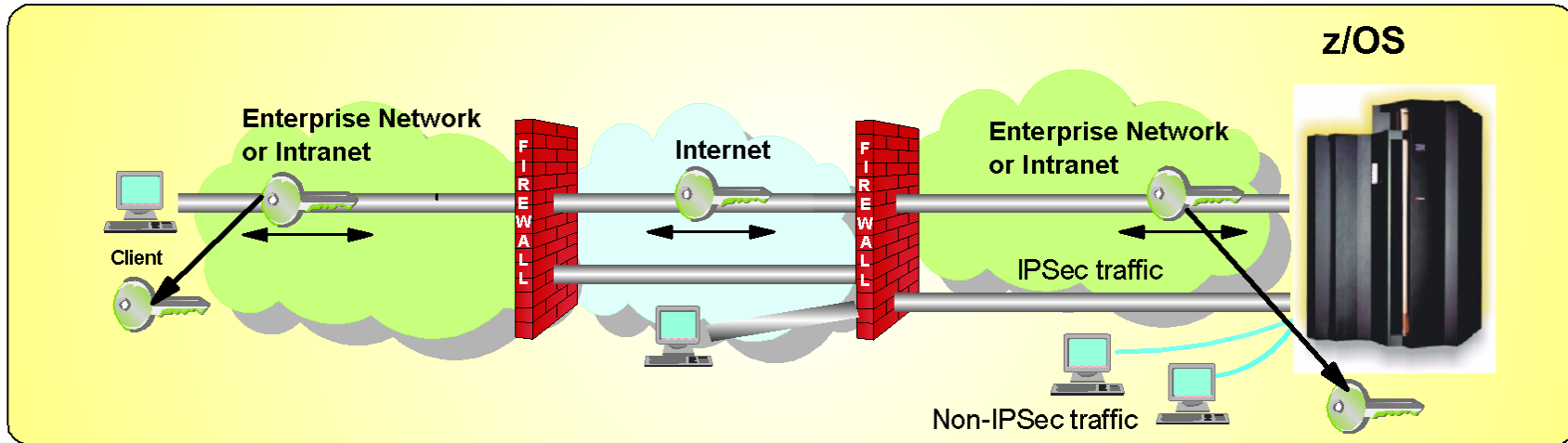
- Policy-driven using Communications Server Policy Agent
 - ▶ Configuration for each TCP/IP stack defines security requirements
- Network security without requiring application changes
 - ▶ Security services provided by the TCP/IP stack
 - AT-TLS, IP security, IDS
- Configure AT-TLS, IP security, IDS policy with a single, consistent administrative interface using Configuration Assistant for z/OS Communications Server
 - ▶ 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
- Starting in z/OS V1R8, Firewall Technologies is no longer available

z/OS Communications Server IP Security Features

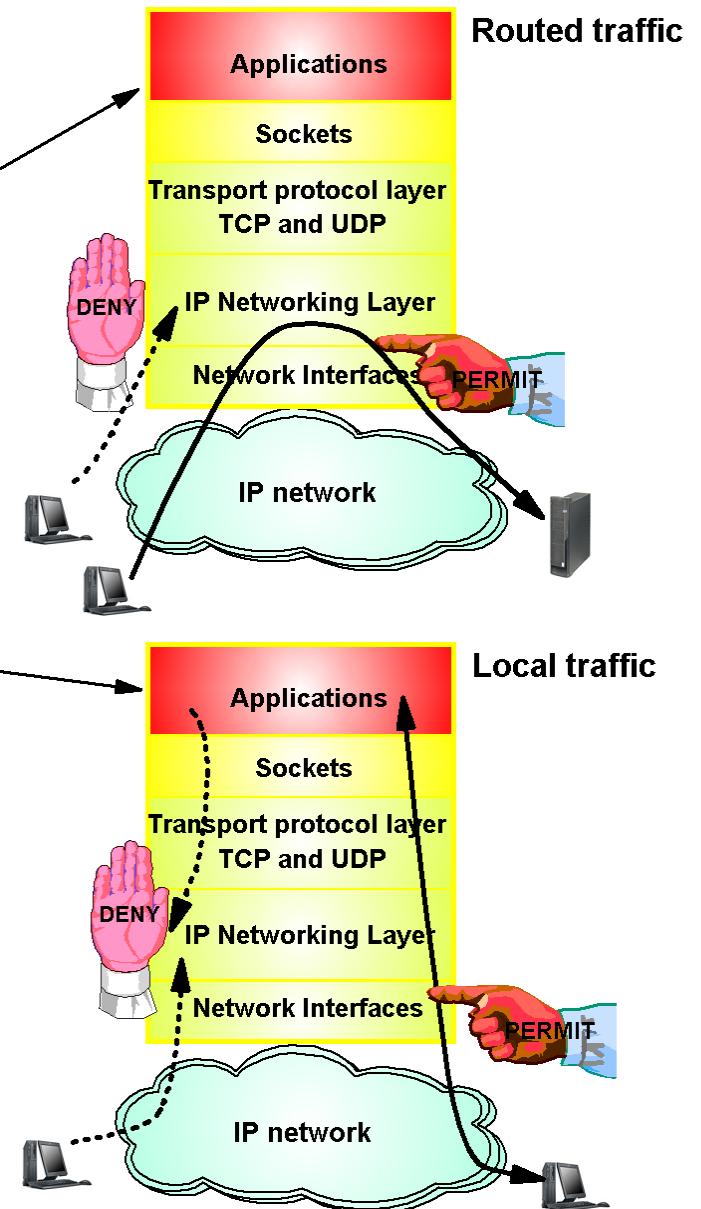
- **Configuration support**
 - ▶ Optimized for z/OS host-to-host and z/OS host-to-gateway (z/OS gateway still supported)
 - ▶ IPsec NAT Traversal support
 - IP address translation
 - Port translation
 - ▶ IPv4 and IPv6 support
- **Simplified configuration**
 - ▶ Configuration GUI for both new and expert 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
- **Cryptographic algorithms (** uses cryptographic hardware if available)**
 - ▶ HMAC-SHA (**) and HMAC-MD5 authentication
 - ▶ 3DES(**) and DES(**) encryption
 - ▶ AES (**) encryption
- **zIIP Assisted IPsec (Base V1R9 or V1R8 with z/OS Communications Server APAR PK40178)**
 - ▶ Moves most of the IPsec processing from the general purpose processors to the zIIPs
 - See Session 3942 for more information
- **IP Security Monitoring Interface (Base V1R9 or V1R8 with z/OS Communications Server APARs PK43352 and PK43353)**
 - ▶ IBM Tivoli OMEGAMON XE for Mainframe Networks monitors the use of IP filters and the performance of IPsec tunnels for the TCP/IP stacks on a z/OS system with this interface
 - See Session 3736 for more information

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

IP Packet Filtering Basics

Packet filtering at IP Layer

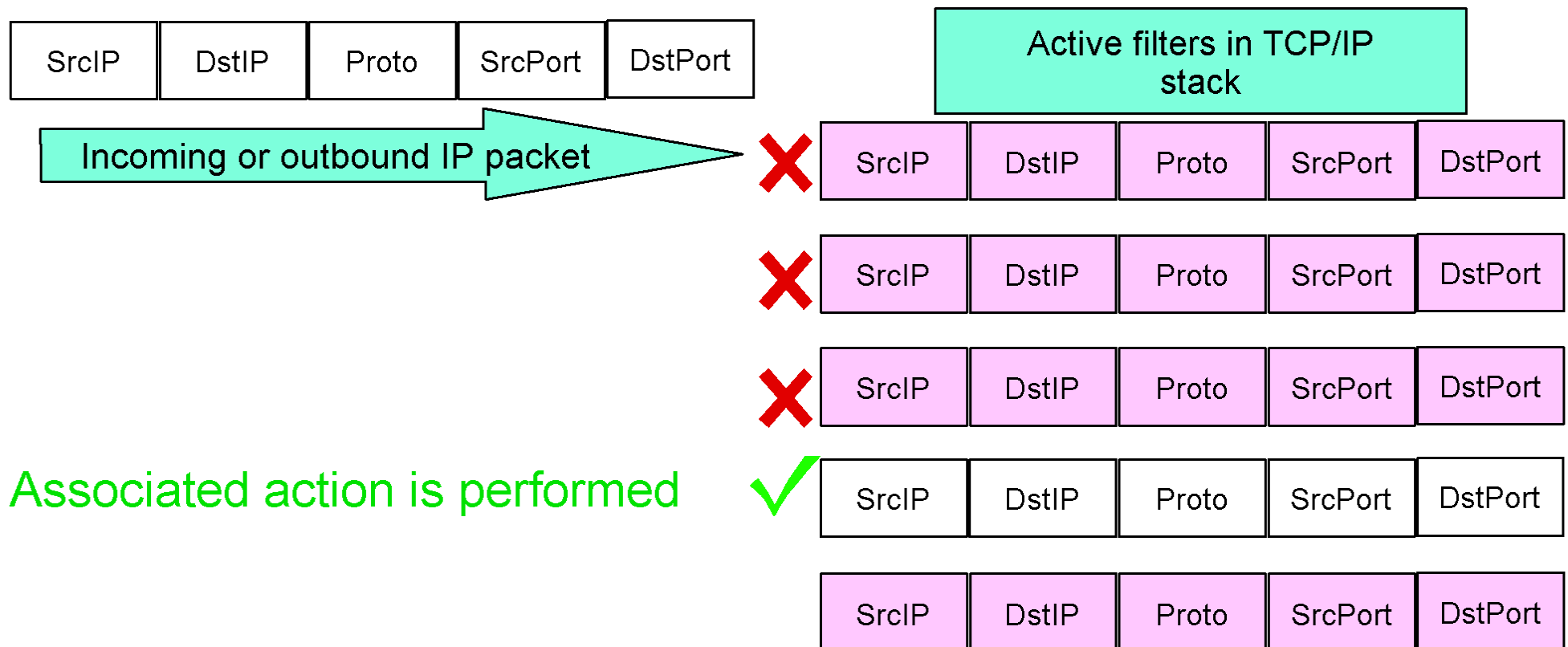
- Filter rules defined to match on inbound and outbound packets based on:
 - ▶ packet information
 - IP address, port, protocol
 - ▶ network attributes
 - direction, link security
 - ▶ time
- Used to control
 - ▶ traffic being routed
 - ▶ access at server
 - "Personal firewall" on z/OS
- Possible actions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



IP Filtering Concepts

Filter Matching

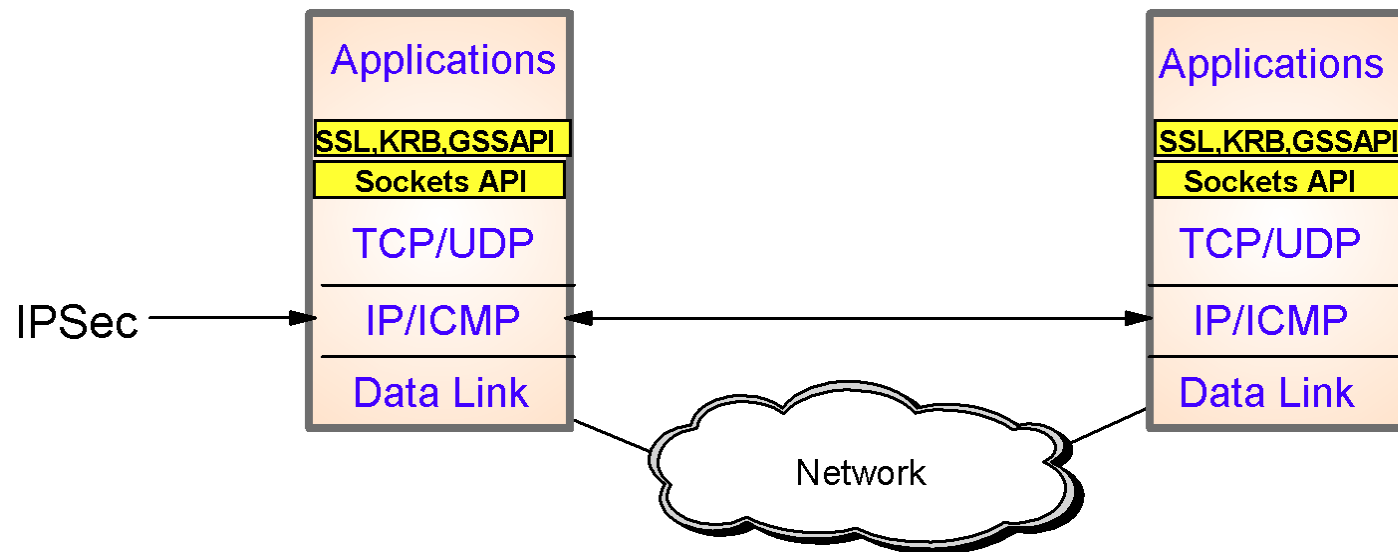
1. Filters are searched in the order they were configured
2. Each rule is inspected, from top to bottom, for a match
3. If a match is found, the search ends and the action is performed



Filtering conditions

Criteria	Description
From packet	
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
Fragments	Fragmented TCP packets require special processing (V1R10)
Network attributes	
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.
Time condition	
Time, Day, Week, Month	Indicates when filter rule is active

IPSec Protocol Overview

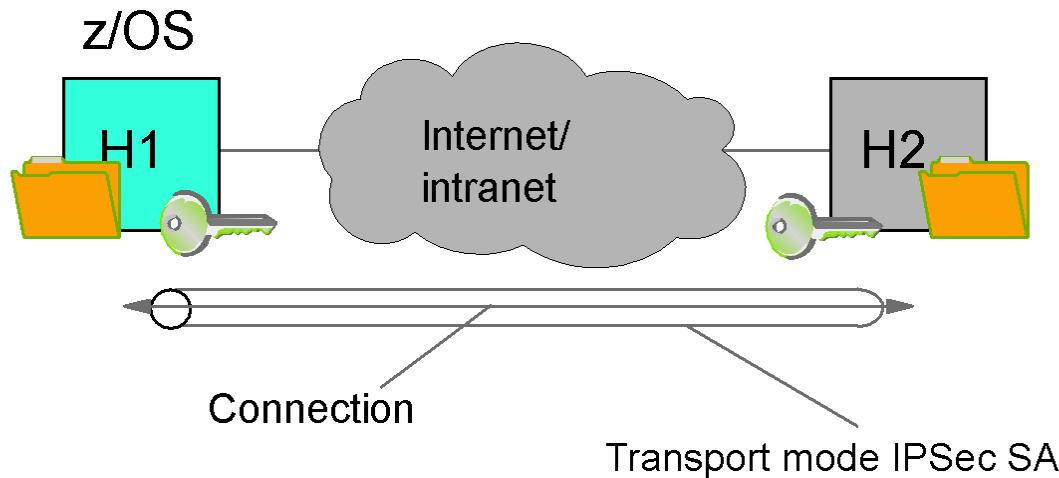


- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
 - ▶ IPSec security protocols
 - **Authentication Header (AH)** - provides data authentication / integrity
 - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional authentication/integrity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

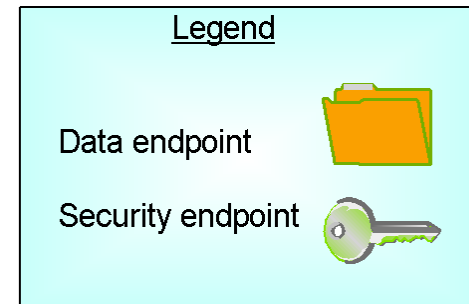
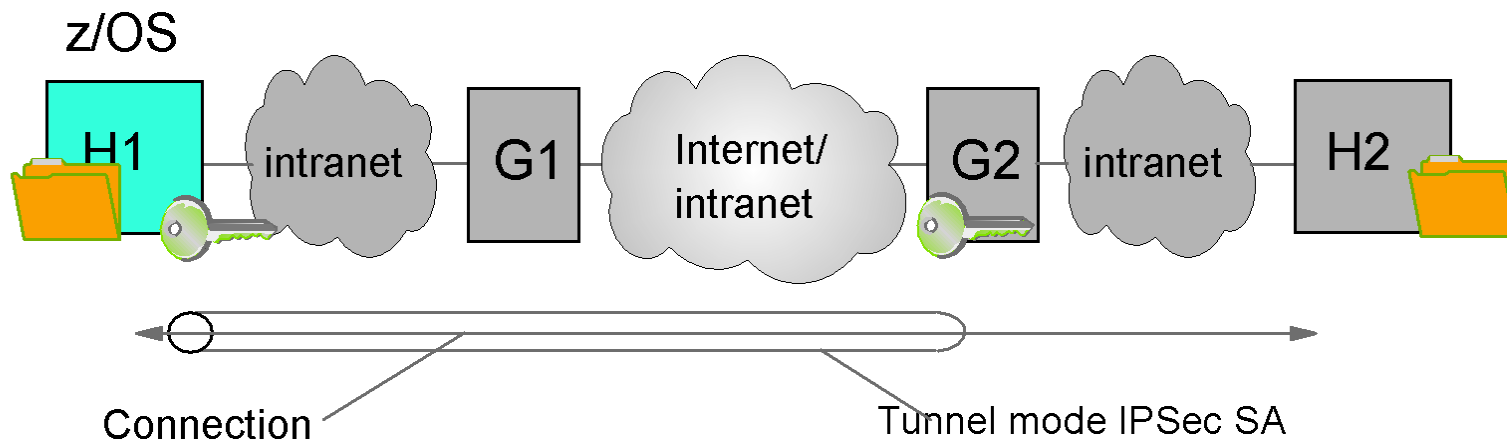
IPSec Scenarios

z/OS as Host (Data Endpoint)

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



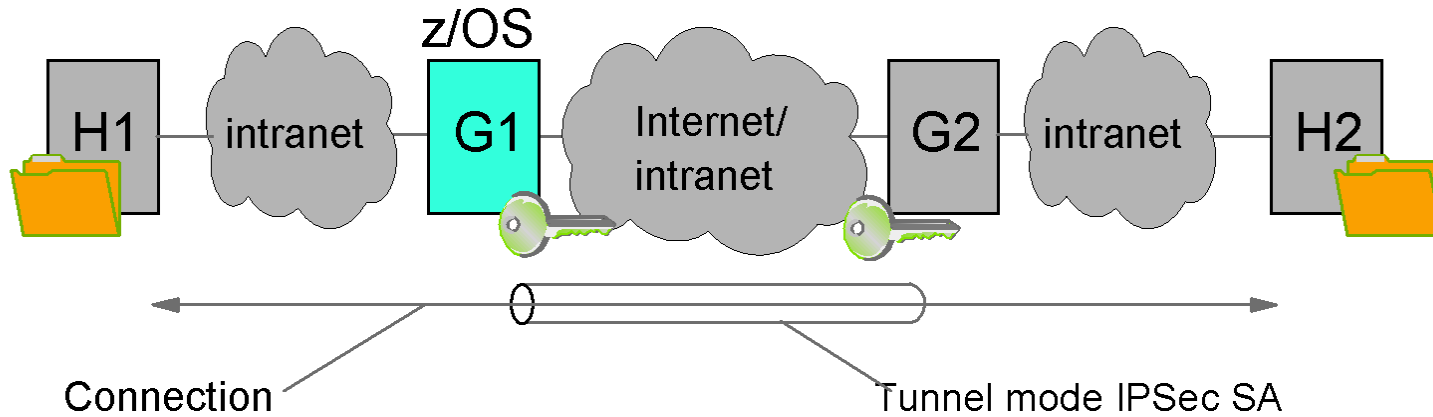
Host-to-gateway: Protect segment of data path



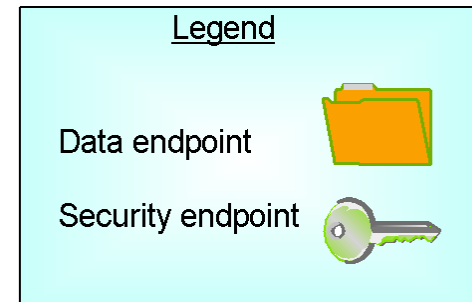
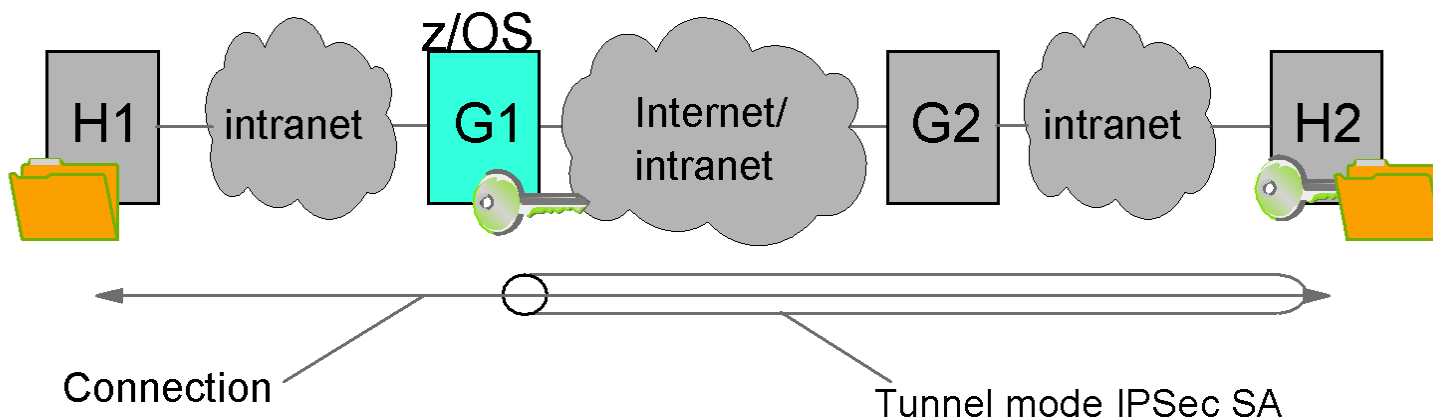
IPSec Scenarios

z/OS as Gateway (Routed Traffic)

Gateway-to-Gateway: Protection over Untrusted Network Segment



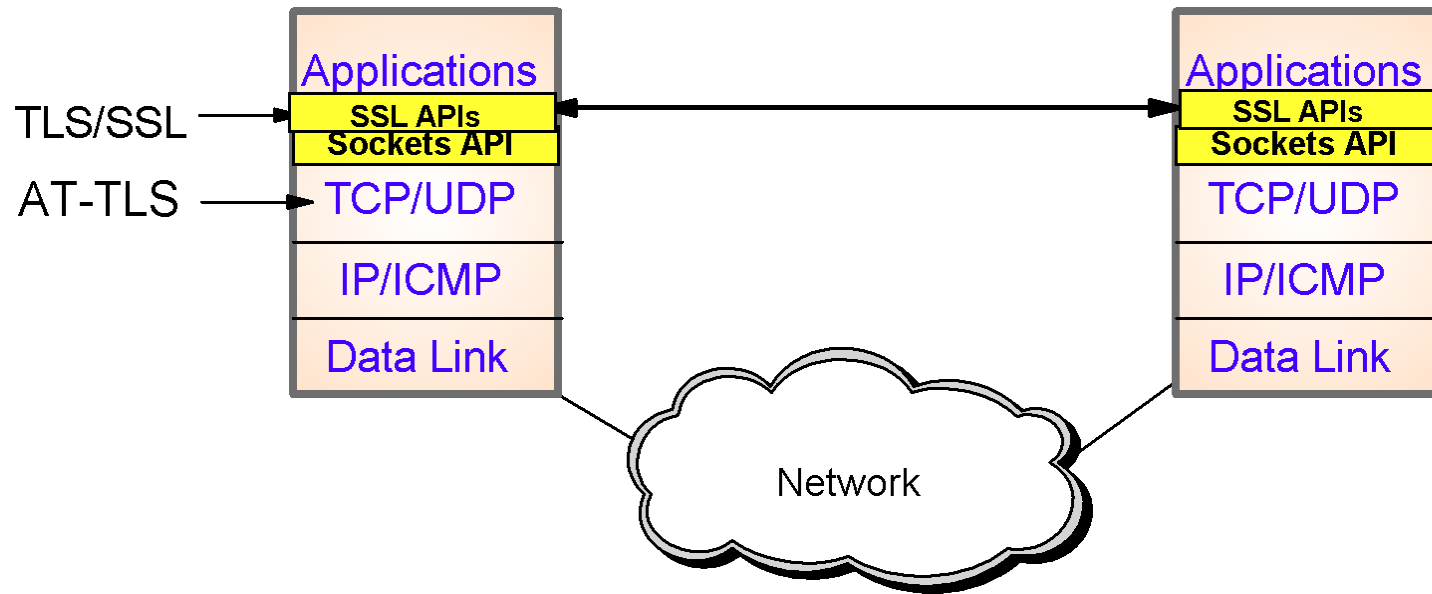
Gateway-to-Host: Protection over Untrusted Network Segment



z/OS Communications Server Network Security

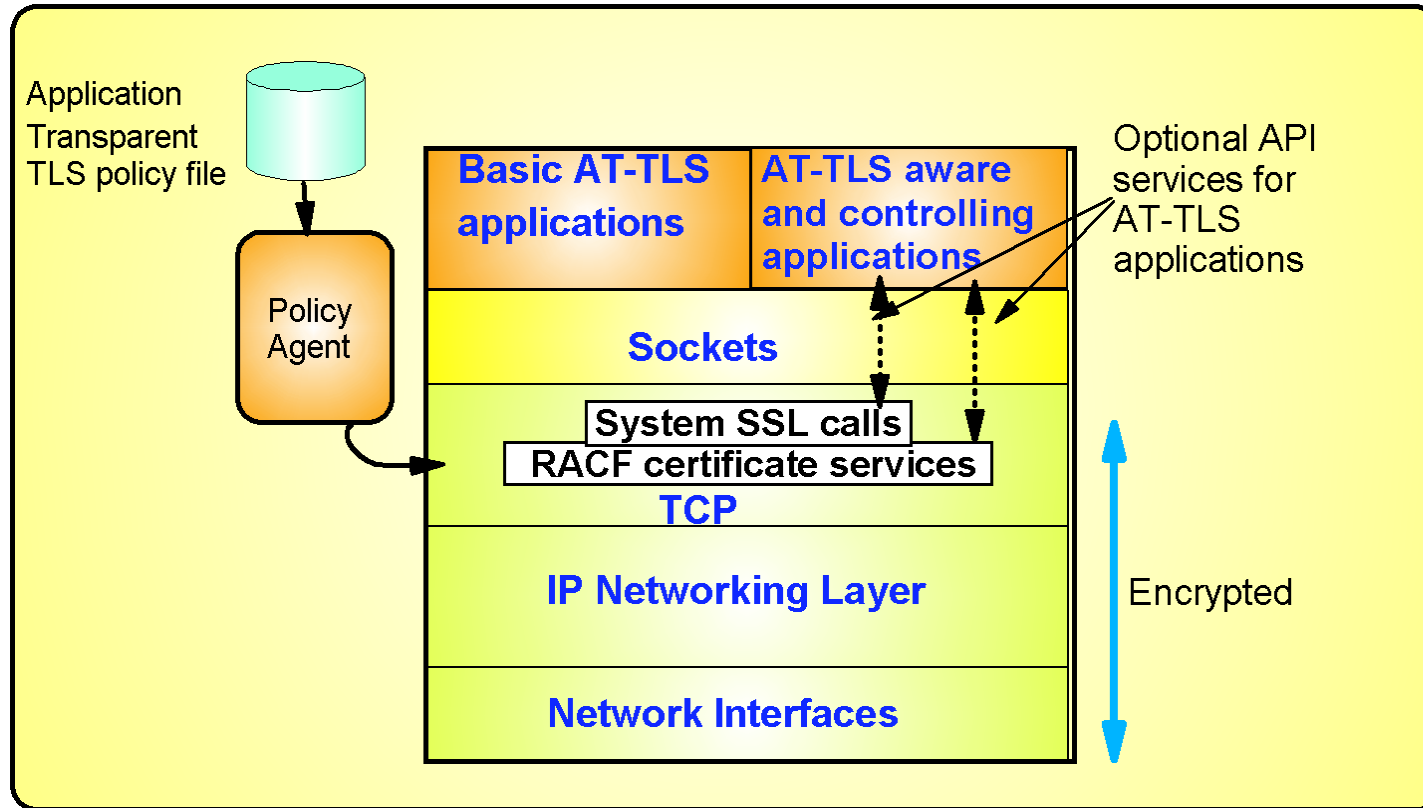
Application Transparent Transport Layer Security

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, raw IP 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



- **AT-TLS performs TLS process at the TCP layer for the application**
 - ▶ AT-TLS policy controls when and how to use TLS
 - AT-TLS policy managed by Policy Agent and configured by Configuration Assistant for z/OS Communications Server or by manual edit
- **Most applications require no change to use AT-TLS**
 - ▶ AT-TLS Basic applications
- **Applications can optionally exploit advanced features using new SIOCTLSCTL ioctl call**
 - ▶ AT-TLS Aware applications
 - Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)
 - ▶ AT-TLS Controlling applications
 - Control if/when to start/stop TLS, reset session/cipher

AT-TLS Advantages

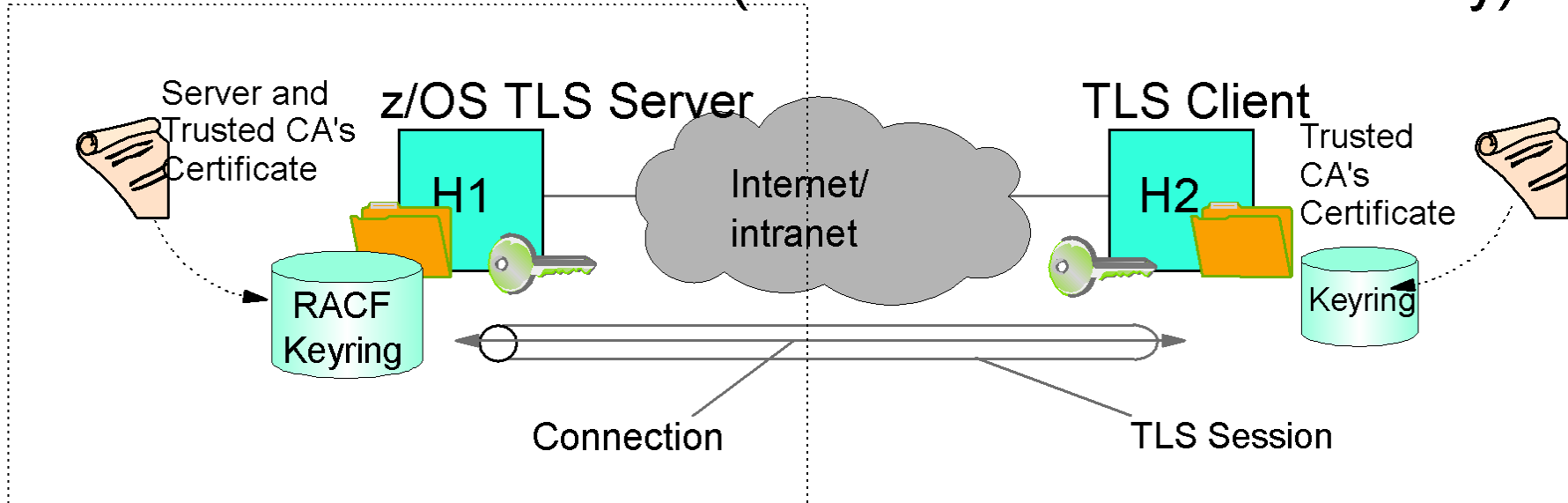
- Reduces development costs for application TLS exploitation
 - ▶ TLS system API invocations
 - ▶ TLS configuration controls
- AT-TLS provides SSL/TLS features above and beyond what most SSL/TLS applications choose to support -
 - ▶ Support for Certificate Revocation Lists (CRLs)
 - ▶ Multiple keyrings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

AT-TLS Policy Conditions

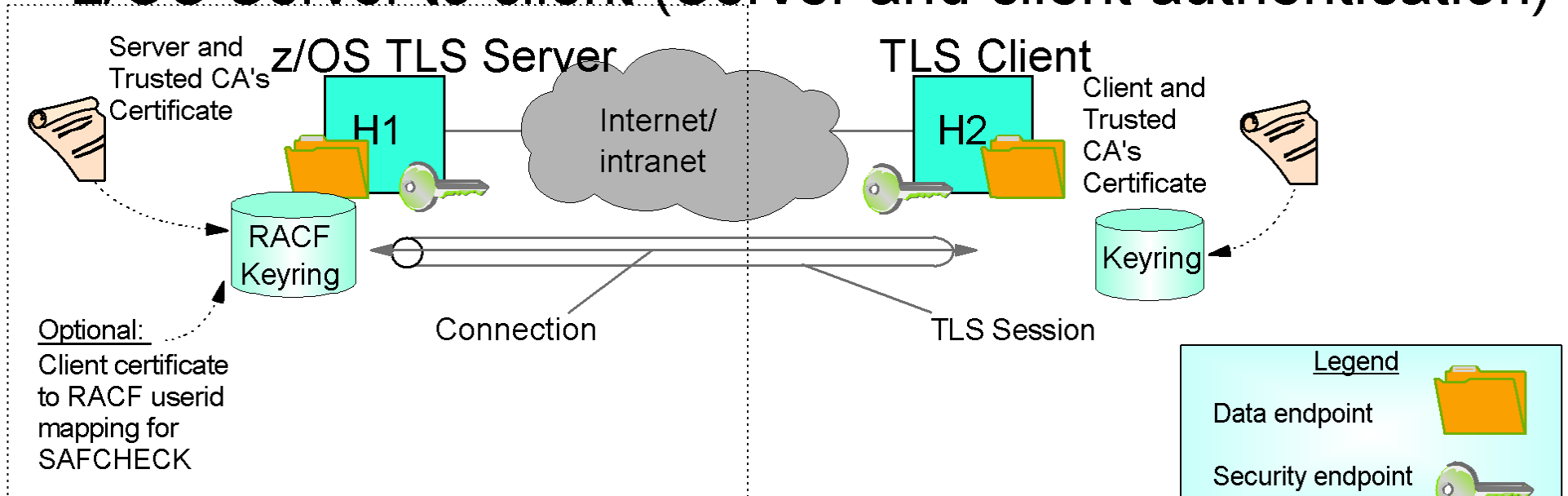
Criteria	Description
Resource attributes	
Local address	Local IP address
Remote address	Remote IP address
Local port	Local port or ports
Remote port	Remote port or ports
Connection type attributes	
Connection direction	<ul style="list-style-type: none">• Inbound (applied to first Select, Send, or Receive 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

z/OS AT-TLS Server Roles



z/OS Server to client (Server authentication only)



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

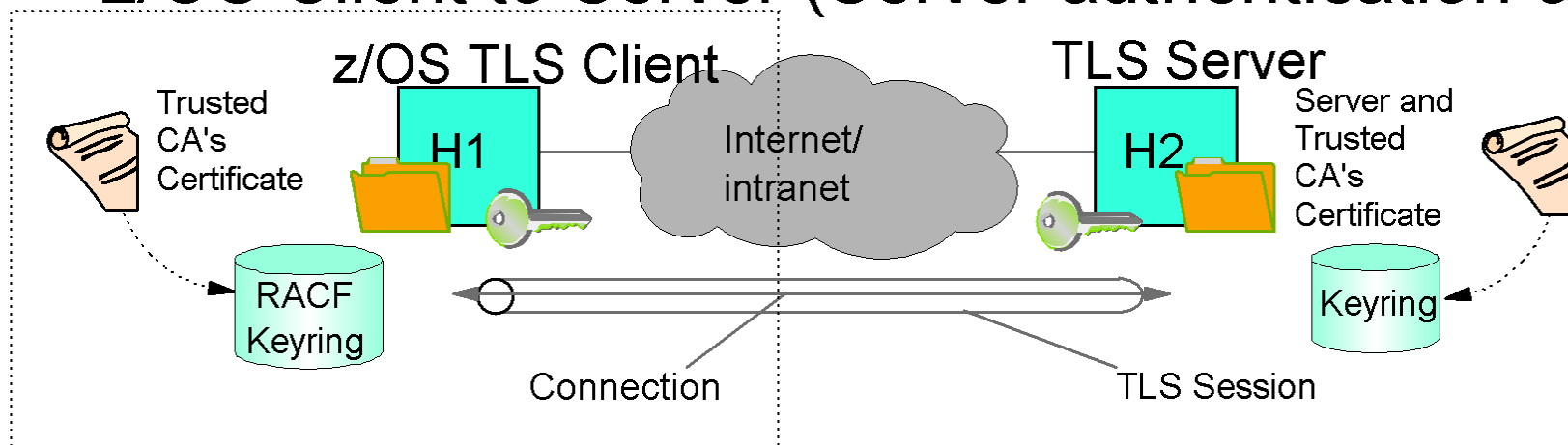


Legend

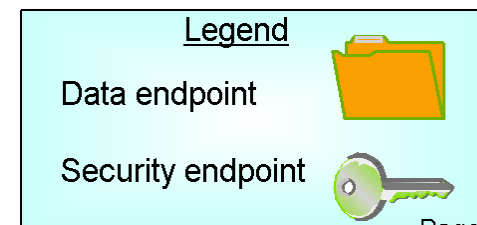
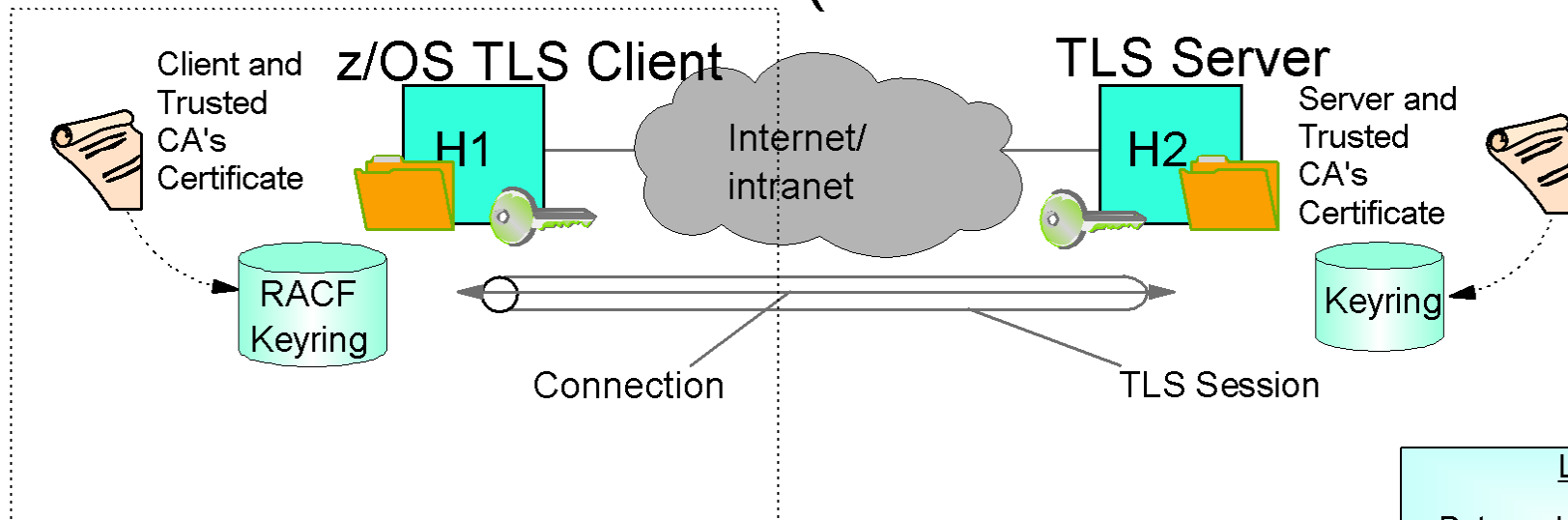
- Data endpoint 
- Security endpoint 

z/OS AT-TLS Client Roles

z/OS Client to Server (Server authentication only)



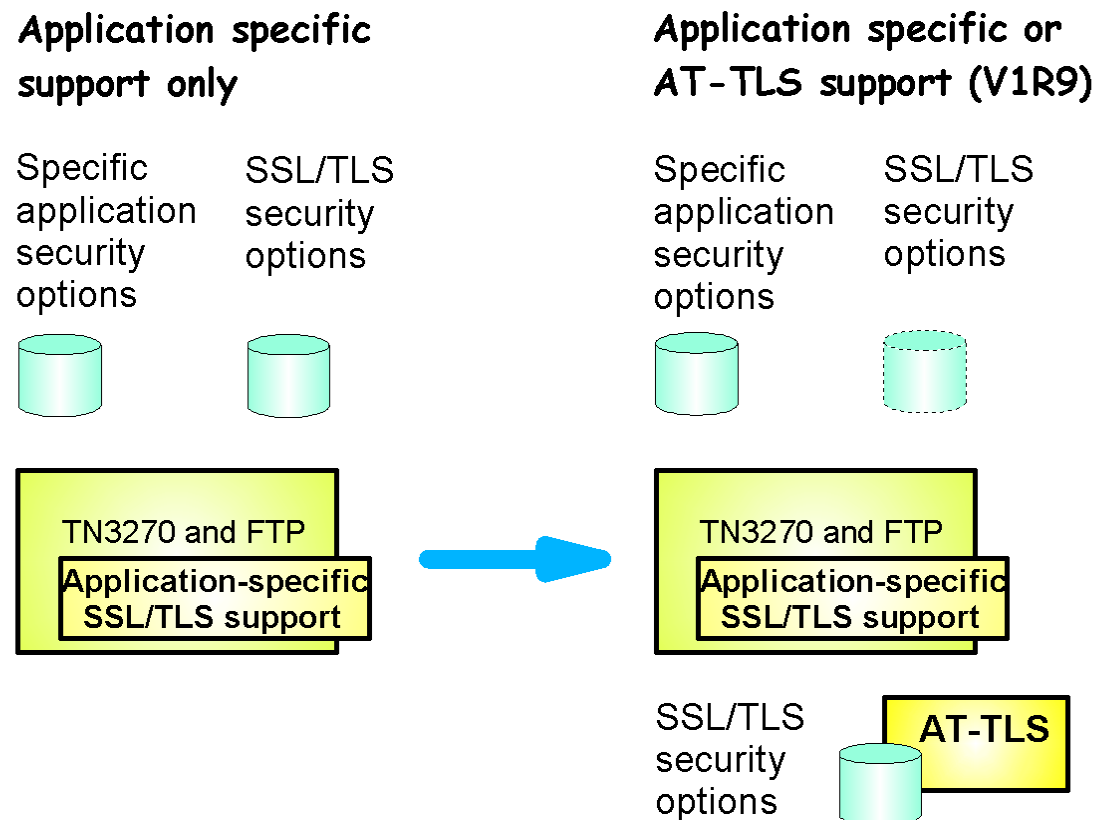
z/OS Client to Server (Server and client authentication)



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 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**

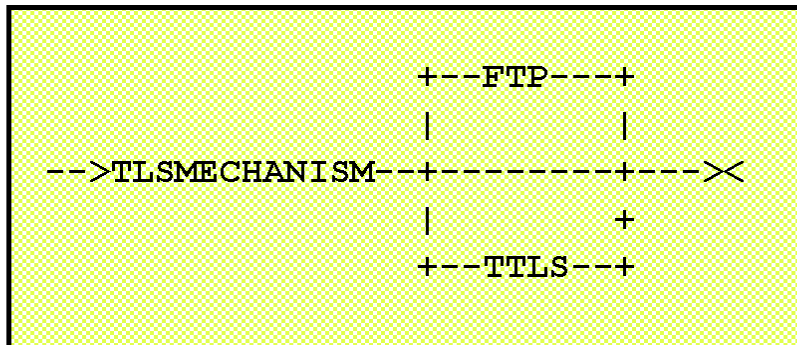
- ▶ **KEYRING**
- ▶ **CRLLDAPSERVER**
- ▶ **CLIENTAUTH**
 - SSLCERT
 - SAFCERT
- ▶ **ENCRYPTION**
- ▶ **SSLTIMEOUT**
- ▶ **SSLV2/SSLNOV2**

AT-TLS 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)

IPSec and AT-TLS Comparison

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

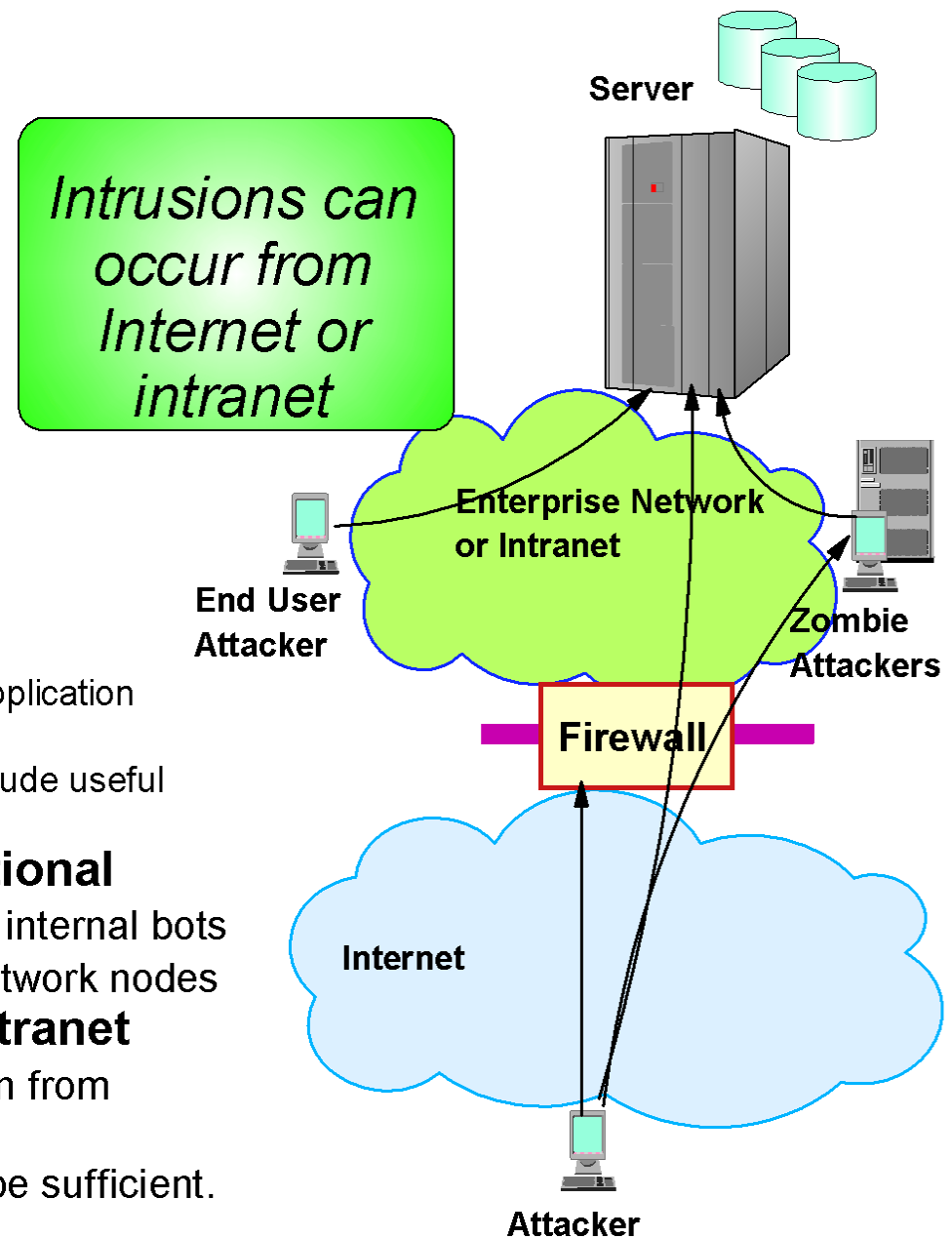
- ✓ Single Packet attacks - exploits system or application vulnerability
- ✓ Multi-Packet attacks - floods systems to exclude useful work

- **Attacks can be deliberate or unintentional**

- ▶ Deliberate: malicious intent from outside or internal bots
- ▶ Unintentional: various forms of errors on network nodes

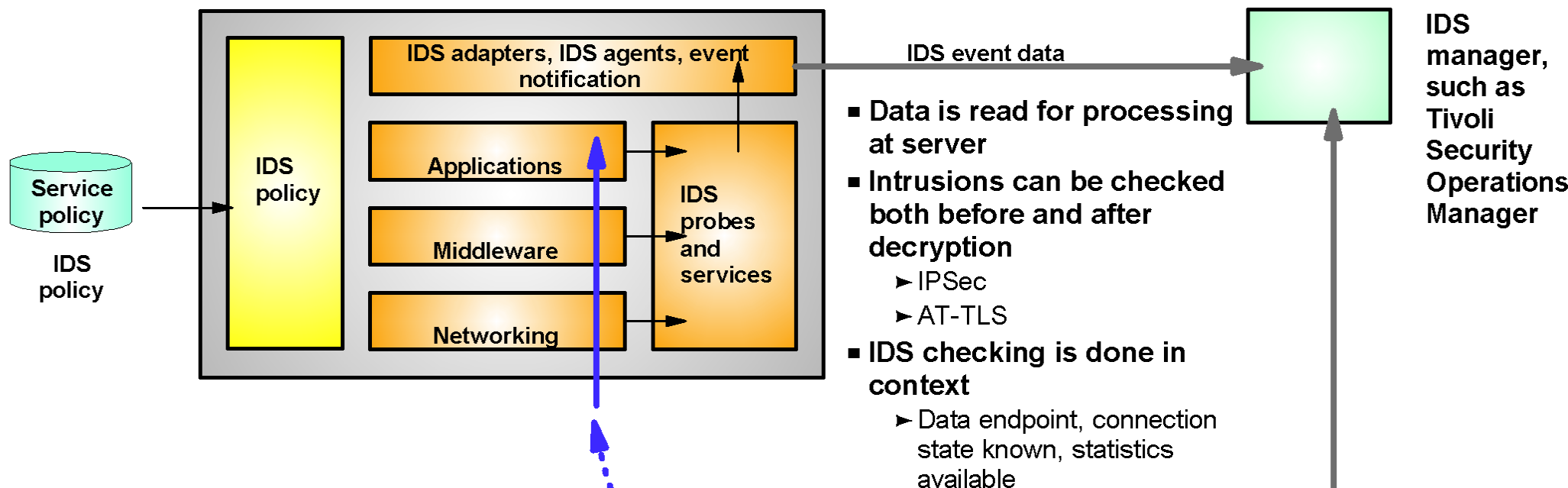
- **Attacks can occur from Internet or intranet**

- ▶ 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

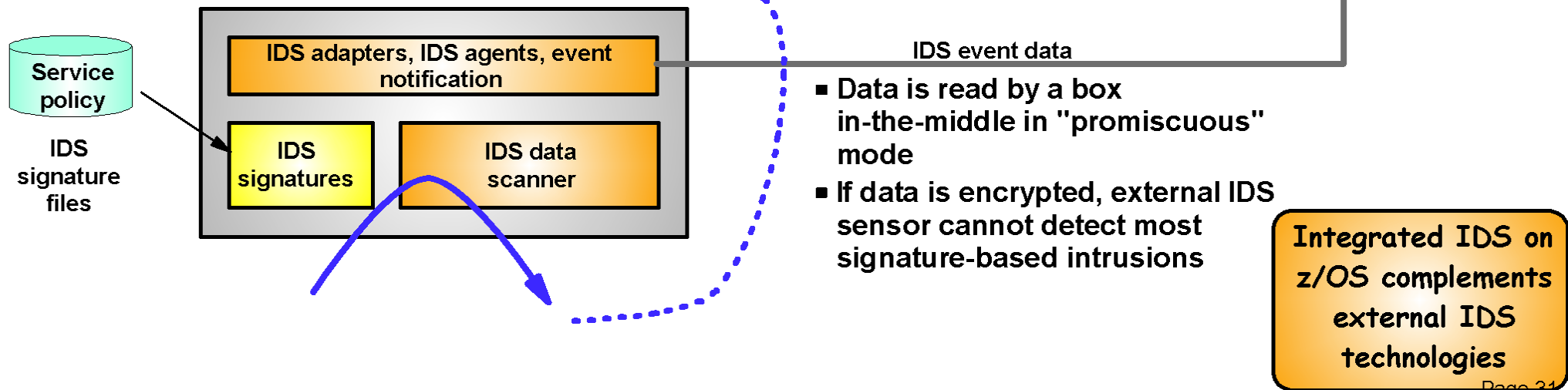


Integrated vs. External Intrusion Detection Concepts

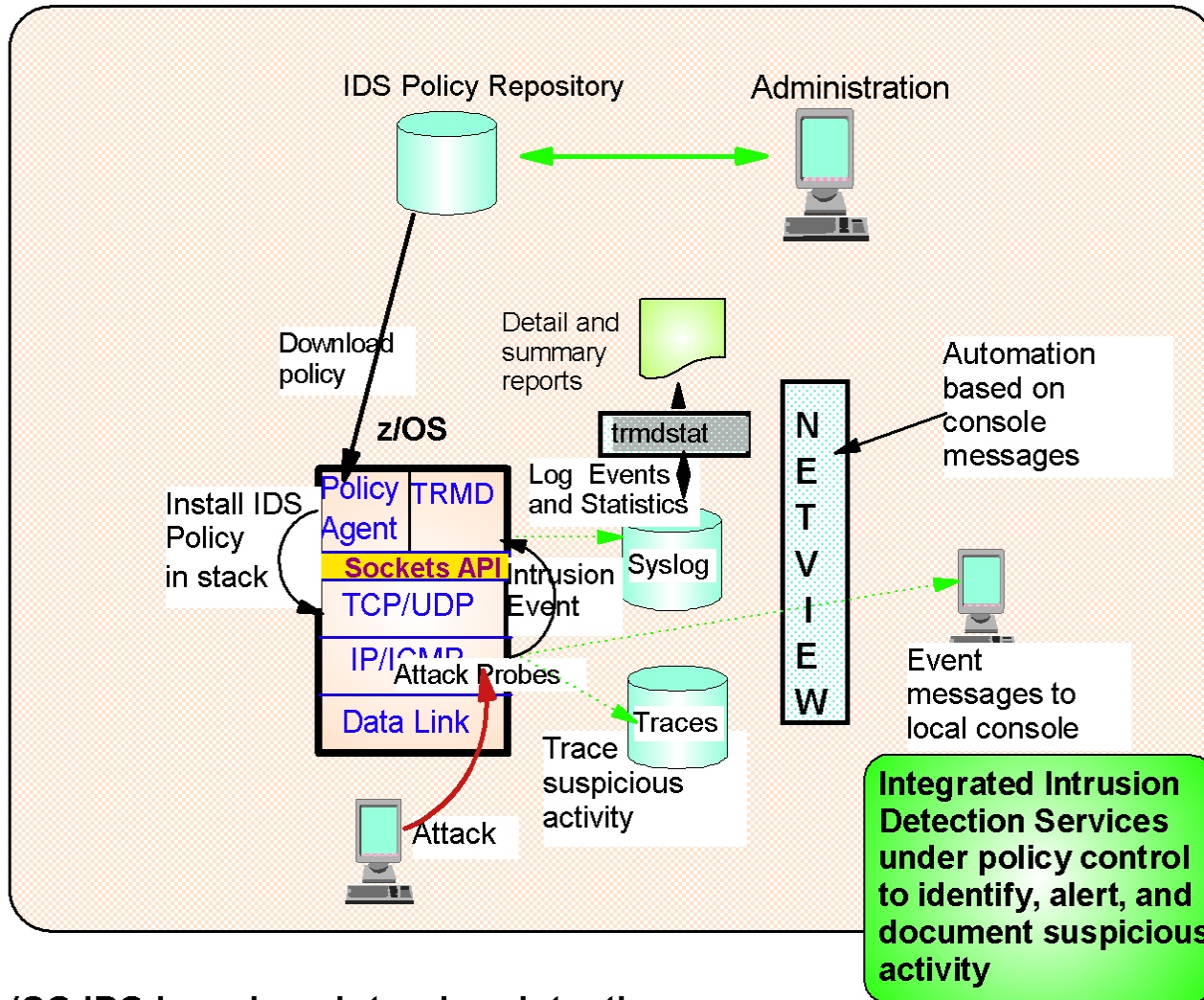
Integrated IDS sensor on server



External IDS sensor in network



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

- Flat file or LDAP

See Session 3931 for more information

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, OtelnetD, etc.)

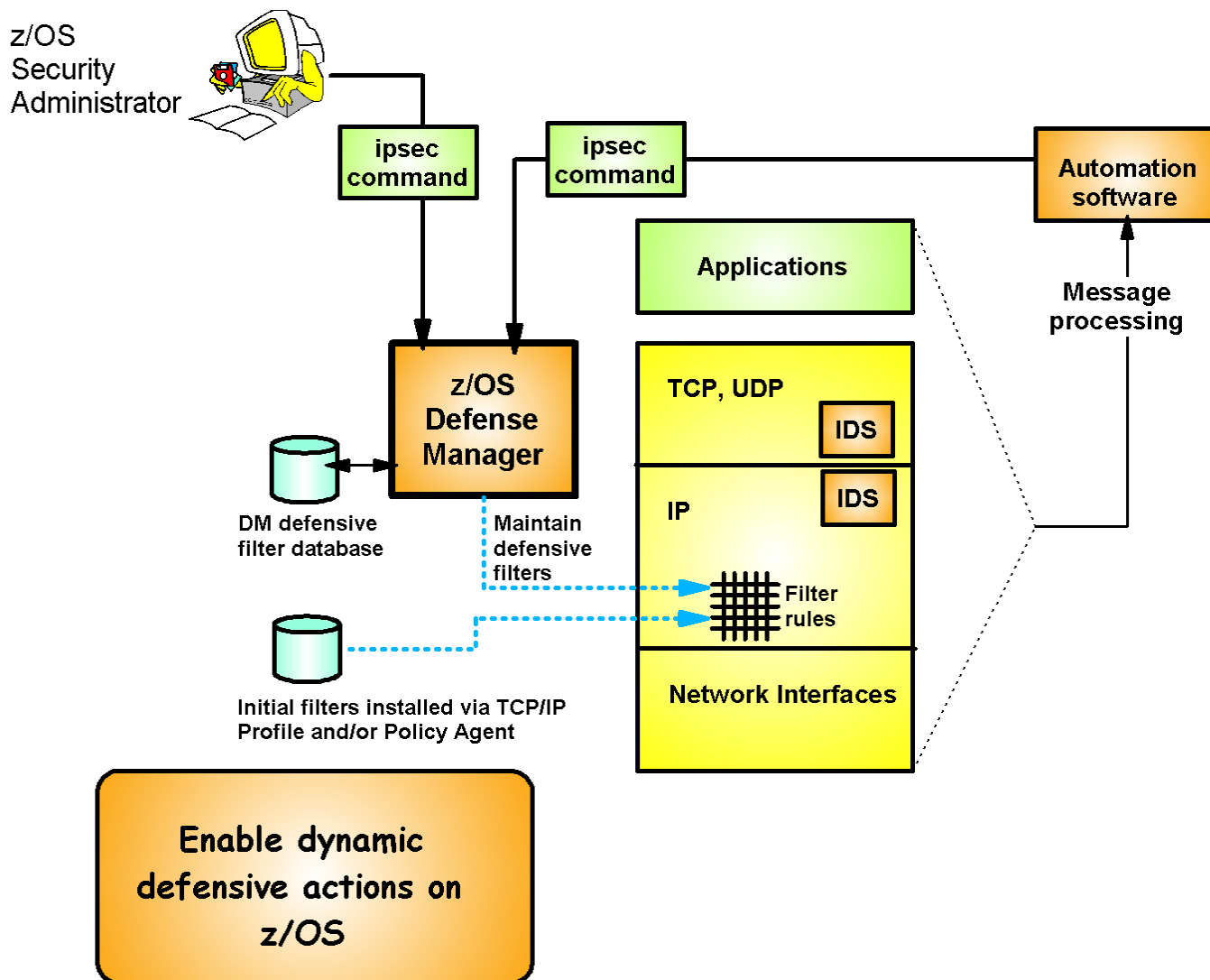
Tivoli Support for IDS Events

- 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 Defensive Filtering

z/OS V1R10 Enhancement

- A new z/OS Defense Manager component allows authorized users to dynamically install time-limited, defensive filters:
 - ▶ A local security administrator can install filters based on information received about a pending threat
 - ▶ Enables filter installation through automation based on analysis of current attack conditions
- Defensive filtering is an extension to IDS capabilities
 - ▶ Adds additional defensive actions to protect against attacks



- Requires minimal IP Security configuration to enable IP packet filtering function
 - ▶ Uses ipsec command to control and display defensive filters
- Defense Manager
 - ▶ Manages installed defensive filters in the TCP/IP stack
 - ▶ Maintains record of defensive filters on DASD for availability in case of DM restart or stack start/restart
- Defensive filter scope may be:
 - ▶ Global - all stacks on the LPAR where DM runs
 - ▶ Local - apply to a specific stack
- Defensive filter are installed "in-front" of configured/default filters

z/OS Communications Server Network Security

Configuring Policy-based Network Security

Configuration Assistant for z/OS Communications Server



Configuration Assistant
for z/OS Communications Server
Version 1, Release 10



(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006, 2008. All Rights Reserved. U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

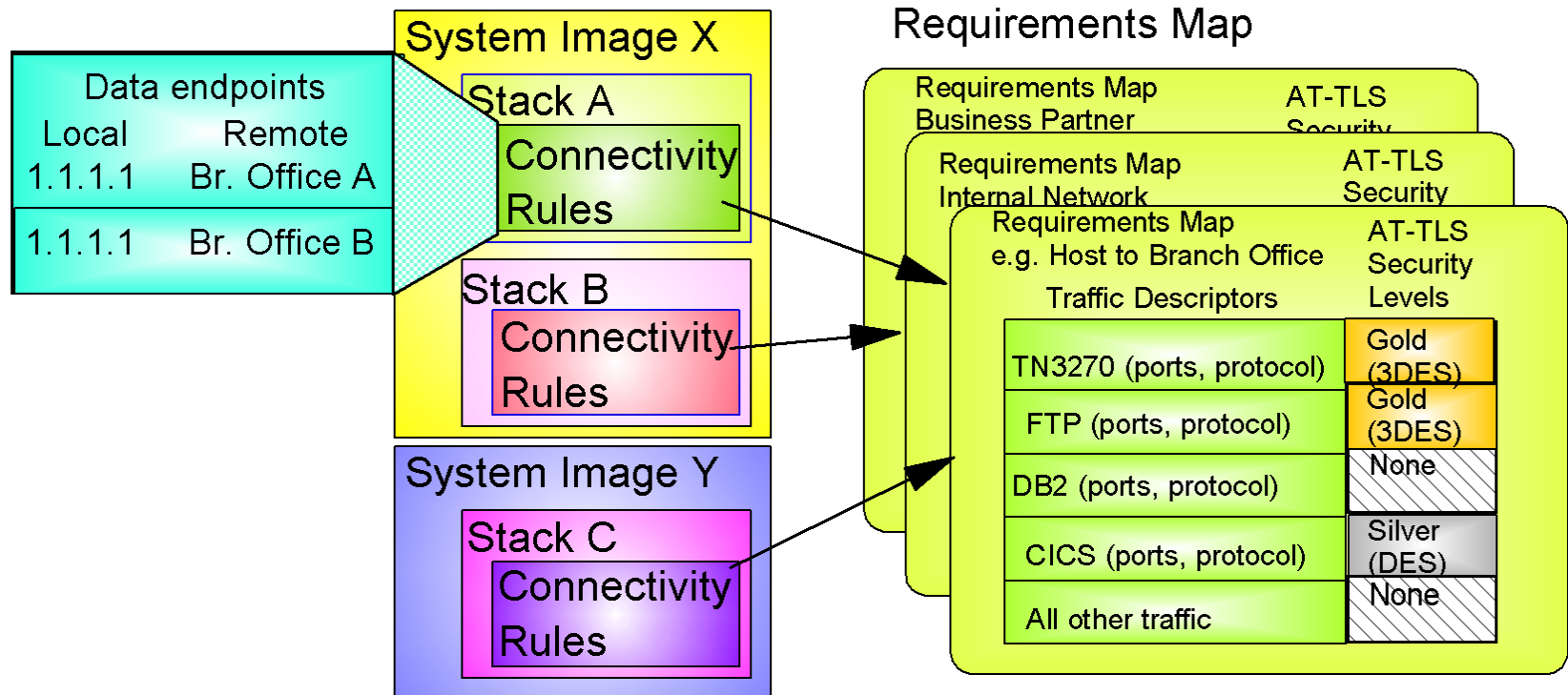


- **Policy Agent configuration tools are combined into one tool to manage policies for:**
 - ▶ AT-TLS
 - ▶ IPsec and IP filtering
 - ▶ IDS
 - ▶ QoS
 - ▶ Policy-based Routing (PBR)
(Added in V1R9)
- **Common approach for all policy types:**
 - ▶ Master copy stored in binary file format on workstation,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

Downloadable policy configuration tool:

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

Configuration Assistant Configuration Data Model



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

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

IP Address Group Support in the Configuration Assistant

z/OS V1R10 Enhancement

- In an effort to simplify the policy configuration files that are created by the Configuration Assistant, z/OS V1R10 adds support for IP address groups
 - ▶ Policy configuration flat file syntax already supports IP address groups
 - ▶ Can significantly reduce the number of Connectivity Rules required
 - Also reduces the number of IP filter rules that are generated by the Configuration Assistant

Configuration Assistant - TCP/IP Stack Settings

File Edit Perspective Help

IPSec Perspective z/OS V1R9 Configuration Assistant

Configuration Assistant Navigation Tree

- IPSec
 - Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
 - Work with z/OS Images
 - Image - MVS098
 - Stack - TCPCS
 - Stack - TCPCS2

Connectivity Rules Dynamic Tunnel Local Identity Stack Level Settings Client NSS settings

TCP/IP Stack Information:

Enter the name of the TCP/IP Stack: TCPCS

Enter a description: Default stack on MVS098

Click the Add... button for each Connectivity Rule you want to add to this Stack.

Local/Source	Remote/Destination	Requirement Map	Topology	Status	Name
All IP V4	All IP V4	Filtering	None	Disabled	ABC-allIPv4
9.42.105.159	All IP V4	ABC-Permit	None	Enabled	DVIPA1
9.42.104.161	All IP V4	ABC-Permit	None	Enabled	Static-VIPA1
192.168.101.1	All IP V4	ABC-Permit	None	Enabled	DVIPA2
9.42.105.45	All IP V4	ABC-Permit	None	Enabled	QD104
9.42.103.11	All IP V4	ABC-Permit	None	Enabled	TR1
192.168.5.1	All IP V4	ABC-Permit	None	Enabled	DynXCF
224.0.0.0/8	All IP V4	ABC-Permit	None	Enabled	Multicast

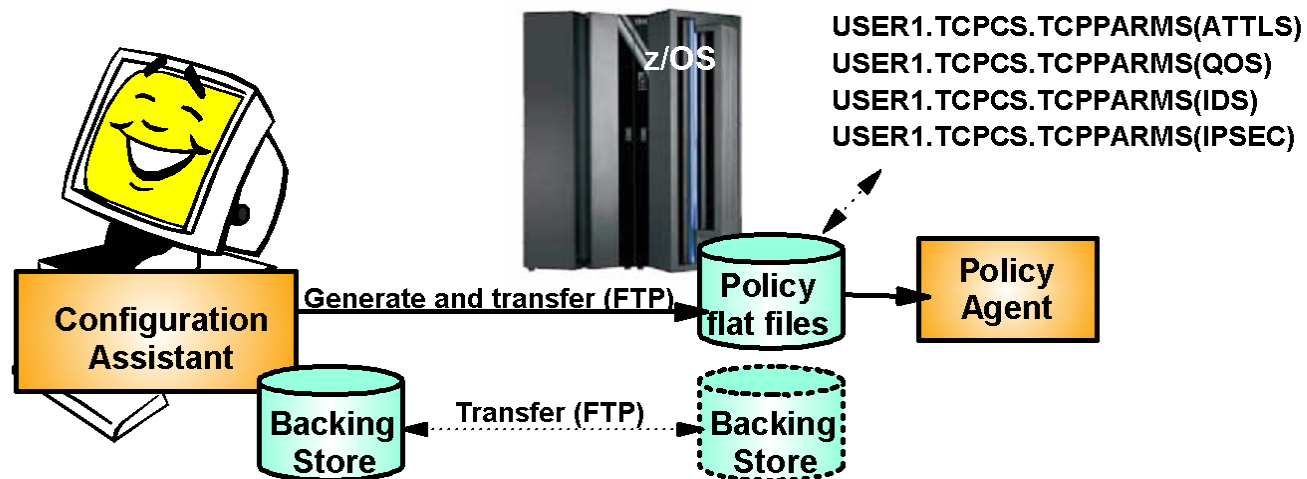
Add... Copy... Modify Basics... Delete View Details... Move Up Health Check...
Modify Wizard... Move Down

Main Perspective Apply Changes OK Cancel Help ?

In this example, most of the local IP addresses could have been grouped into a single group and covered by a single connectivity rule

- ▶ Prior to V1R10, a connectivity rule must be configured per IP address in the HOME list.
- ▶ For each connectivity rule, an IP filter rule per traffic descriptor in the associated requirement map is generated in the policy file
- ▶ With IP address group support, the number of connectivity rules can be reduced, and hence the number of generated IP filter rules in the policy file.

Configuration Assistant Policy File Handling

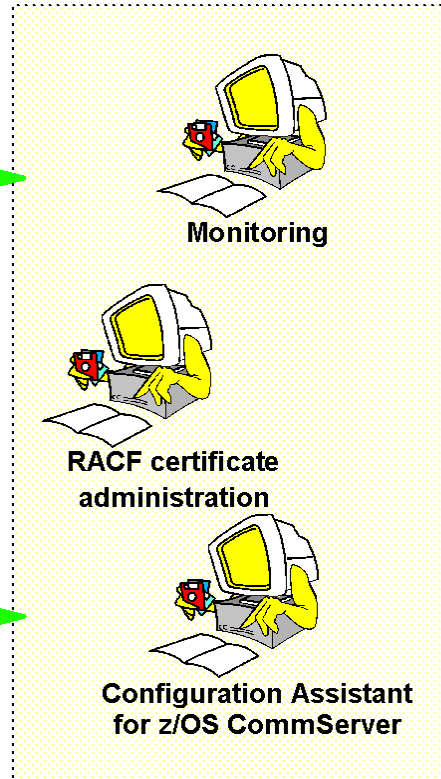
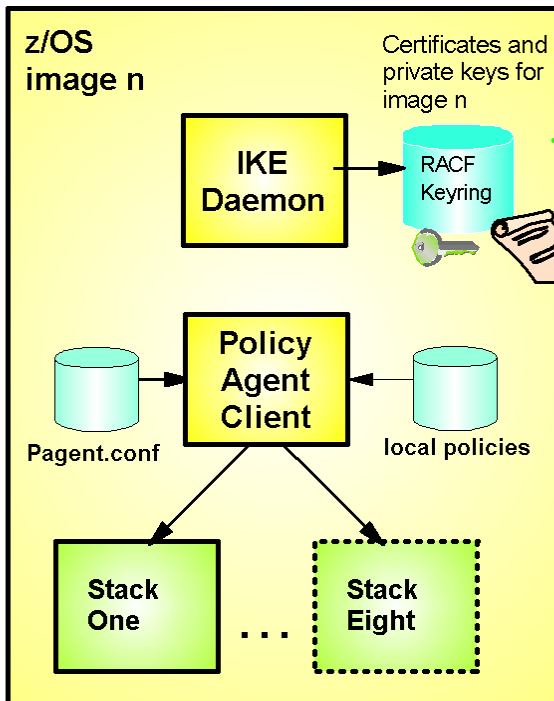
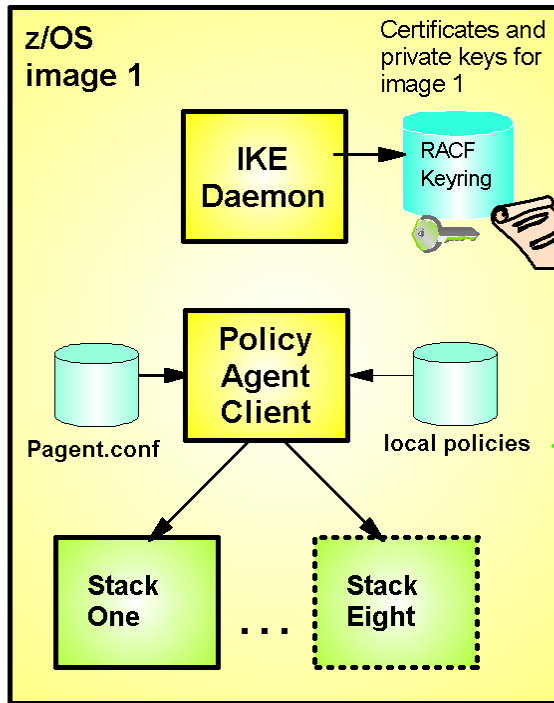


- **Downloadable policy configuration tool runs on workstation**
- **Allows policy definition to be performed at higher level of abstraction than policy file statements**
 - ▶ Configuration Assistant stores and works with an internal representation of policy (backing store)
 - ▶ Generates and transfers policy files to z/OS for runtime enforcement
- **In V1R9, file management improvements**
 - ▶ Backing store can be stored on z/OS
 - ▶ Locking support at the backing store level to prevent inadvertant loss of data
- **In V1R10, a policy flat file import function is added**
 - ▶ Changes to policy flat file made via an editor can now be picked up by the Configuration Assistant
 - ▶ Existing manually created policy flat files can be imported into the Configuration Assistant and changes can from now on be implemented using the Configuration Assistant
 - ▶ z/OS V1R10 will support import of most, but not all, of the policy configuration files:
 - Supported: IPsec, AT-TLS, PBR, IDS
 - Not supported: QoS, non-policy config files (NSS, IKED)

z/OS Communications Server Network Security

Enterprise Wide Security Roles

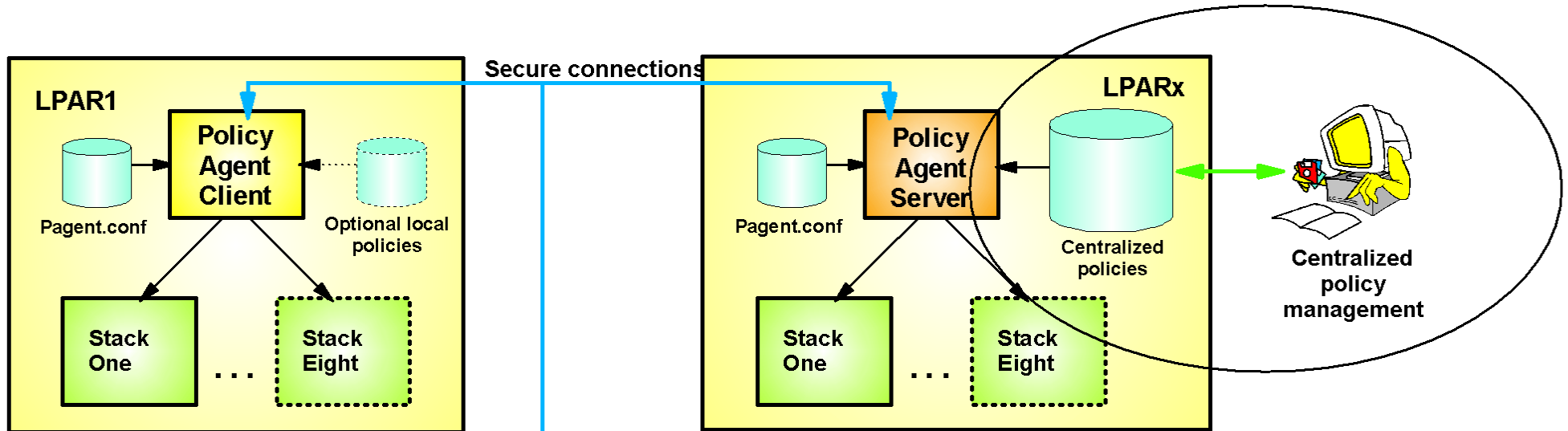
Network Security Administration - Prior to z/OS V1R9



- Each z/OS system locally administered
 - ▶ RACF certificate administration
 - ▶ Policy configuration
 - ▶ Monitoring
- 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

Centralized networking policy management

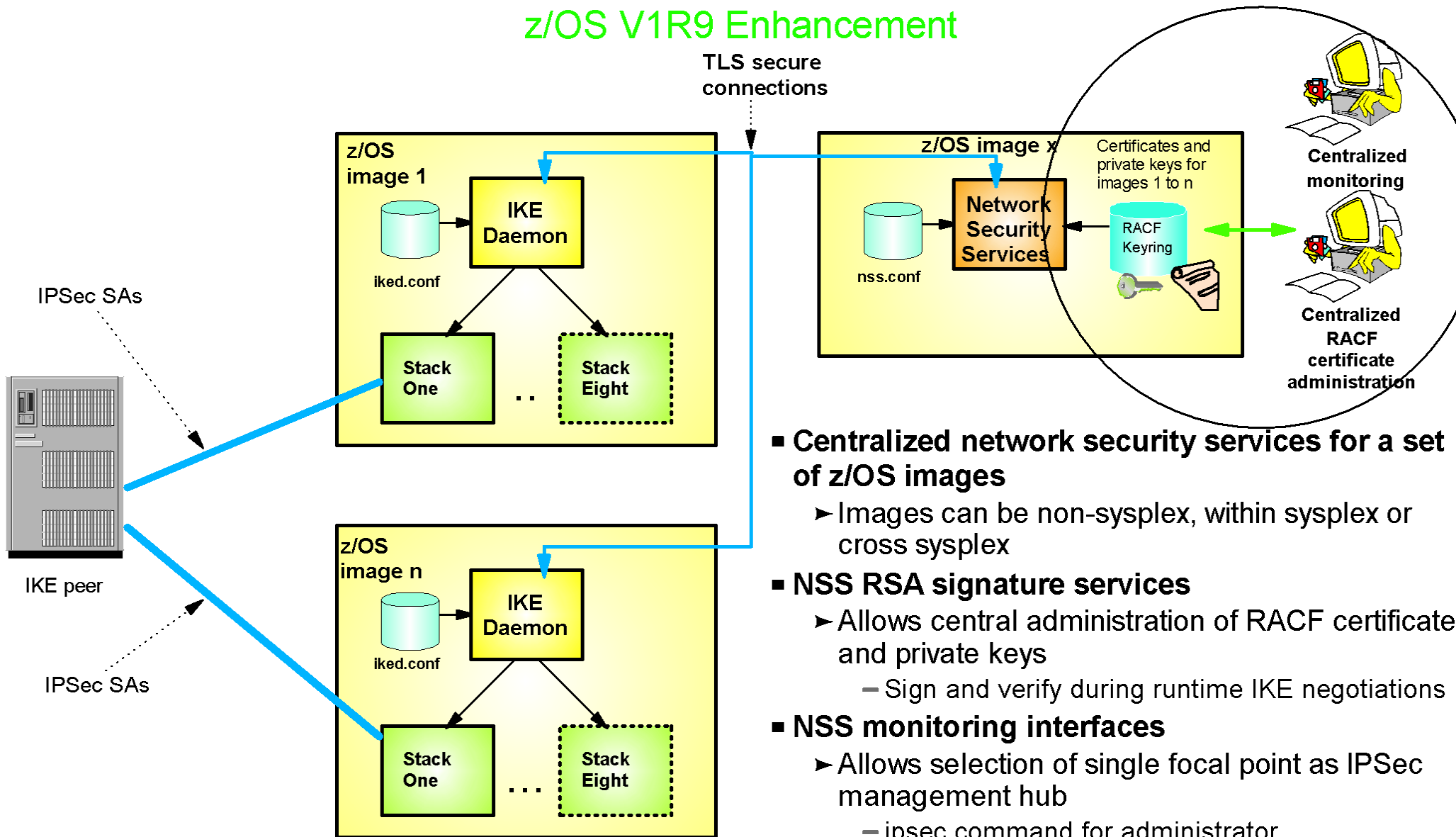
z/OS V1R9 Enhancement



- **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 policy agent can be specified
- **Policy can be configured with Configuration Assistant for z/OS Communications Server or with manual edit**

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 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 Management Interface for management application

- **Availability options**

- ▶ Backup NSS can be specified

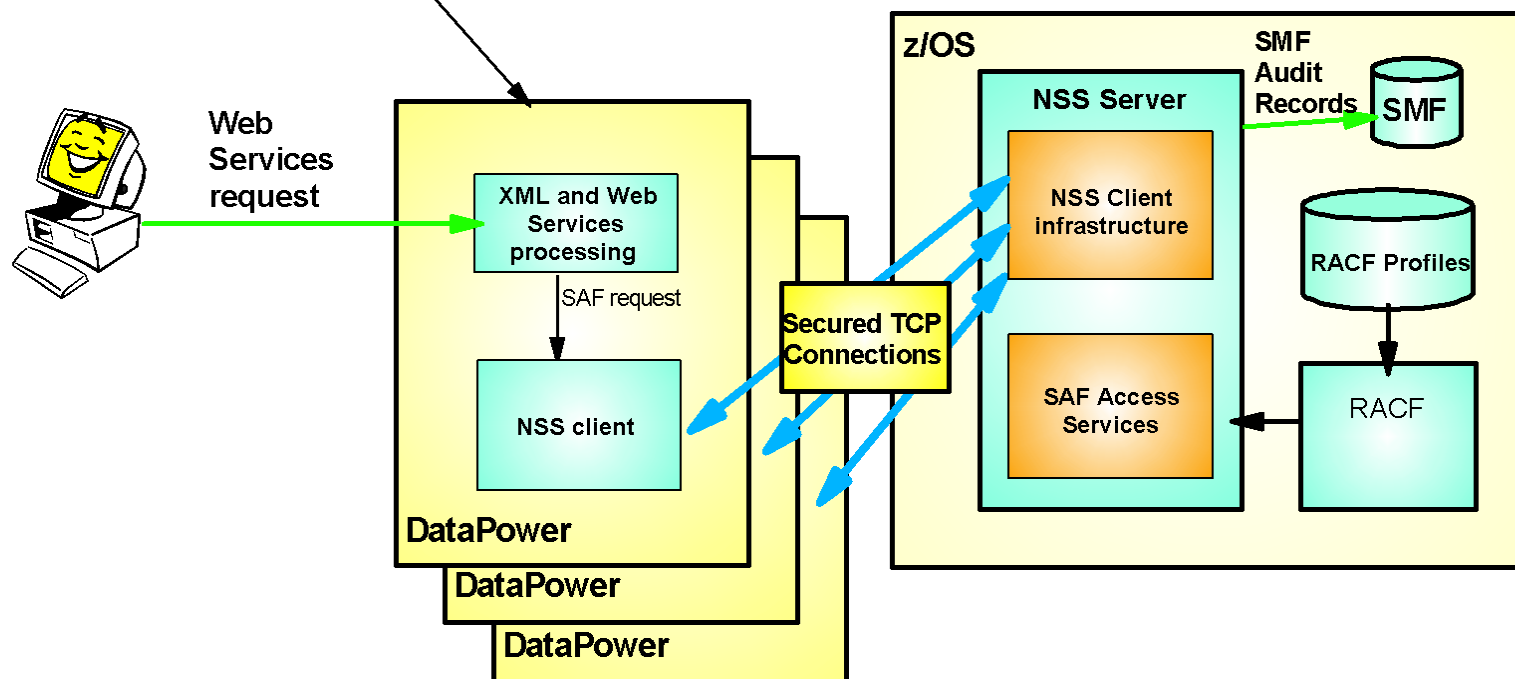
Extending NSS - Integrating DataPower with z/OS Security

z/OS V1R10 Enhancement

■ WebSphere DataPower SOA Appliances:

- ▶ Application message format transformation
- ▶ Offloads XML and Web Services security functions

Offloading CPU-intensive XML processing - without losing centralized security control



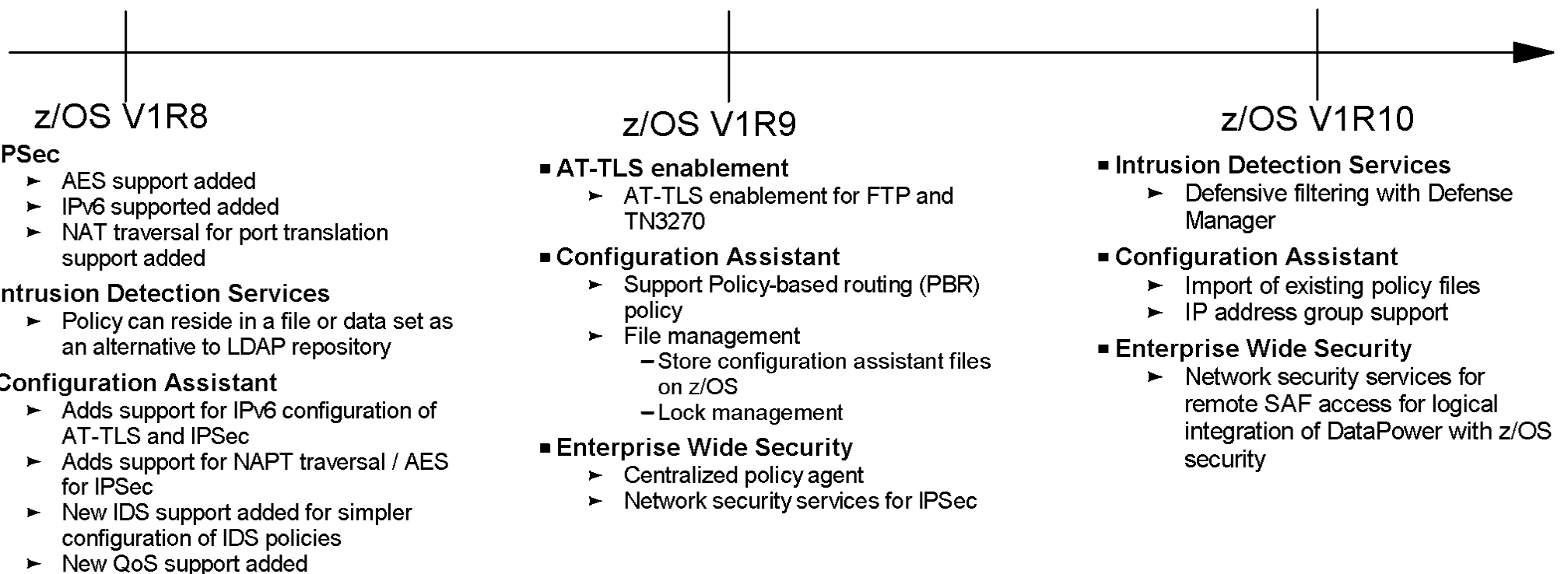
■ NSS is extended to provide logical integration of DataPower and z/OS security:

- ▶ Centralized management of SAF-based authentication and access control *across multiple hardware platforms*
 - DataPower will include an NSS Client
- ▶ z/OS NSS Server will support SAF Access Service
 - User identification and authentication for DataPower users
 - Access control for DataPower resources
 - Audit records for DataPower SAF access written to SMF
- ▶ Monitoring services for DataPower appliances using SAF Access Services
 - nssctl command displays information about all connected clients for administrator
 - Network Management Interface for management applications

z/OS Communications Server

Policy-based Network Security Enhancements Summary

- Recent Policy-based security functions by release:
 - ▶ Enhancement made to following areas:
 - IP Security
 - Application Transparent TLS
 - Intrusion Detection Services
 - Configuration Assistant for z/OS Communications Server
 - Enterprise Wide Security



For More Information...

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