

Thomas Cosenza

tcosenza@us.ibm.com



AST 11 & 12 PART B

z/OS Communications Server Network

A Security Practitioner's Overview



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®
- DataPower®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e-business (logo)®
- ESCON®
- FICON®
- GDDM®
- GDPS®
- Geographically Dispersed Parallel Sysplex
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise™ System
- IMS
- InfiniBand®
- 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®
- POWER®
- POWER7®
- PowerVM
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x®
- System z®
- System z9®
- System z10
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9®
- z10 BC
- z10 EC
- zEnterprise
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

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

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

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- 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.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

Notes:

- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput a 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 data processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

z/OS Communications Server Network Security

- Overview
 - ▶ Roles and objectives
 - ▶ Deployment trends and requirements
- 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
 - ▶ Policy-based Network Security Componentry
- Enterprise-wide Security Roles
 - ▶ Centralized Policy Agent
 - ▶ Network Security Services

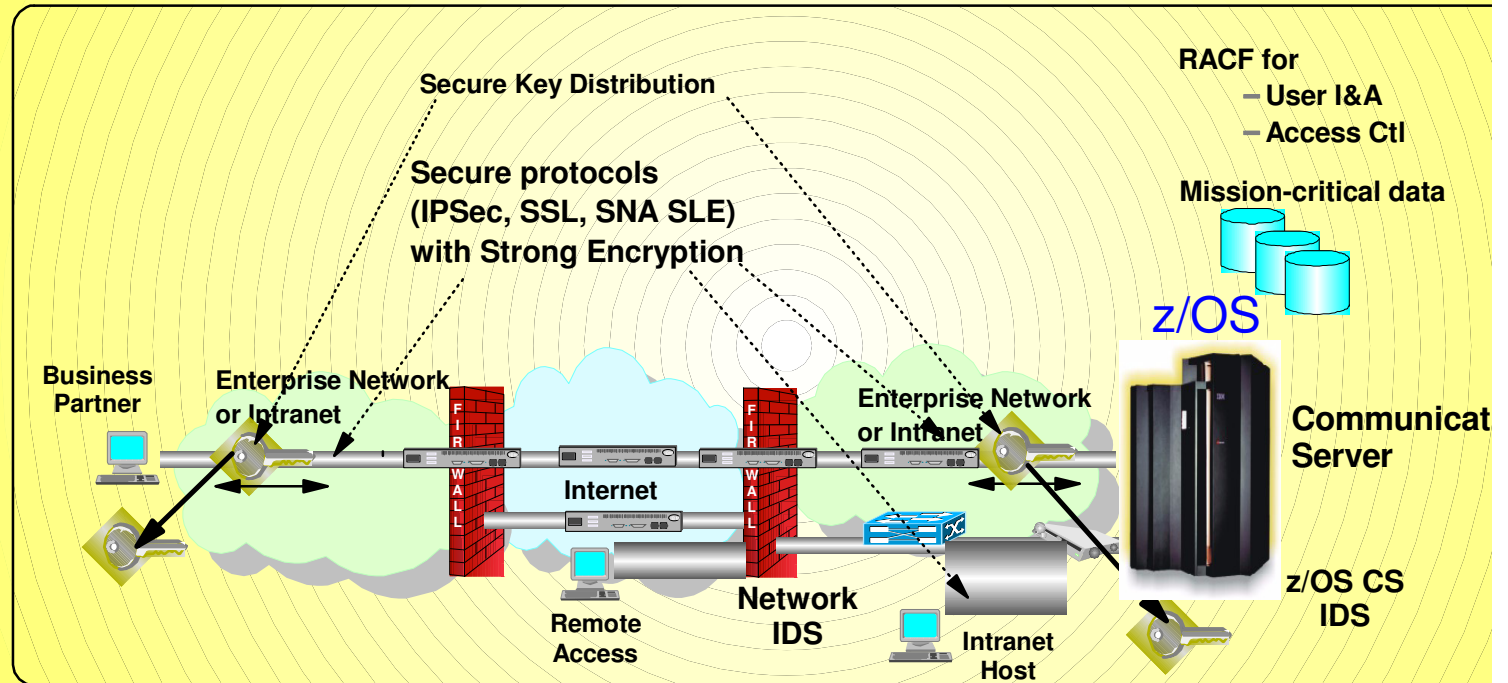
Agenda

z/OS Communications Server Network Security

- Overview
 - ▶ Roles and objectives
 - ▶ Deployment trends and requirements
- 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
 - ▶ Policy-based Network Security Componentry
- Enterprise-wide 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 from the network**

- **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 in the network using cryptographic security protocols**

- **Data endpoint authentication**
 - Verify who the endpoint claims to be
- **Data origin authentication**
 - Verify that data was originated by claimed :
- **Message integrity**
 - Verifv contents were unchanged in transit

Deployment Trends and Requirements

Self-protection will increase in importance and will evolve into the last layer deployed in a total defense depth strategy. The server (and client) will become the “new perimeter” as more security function is pushed into the endpoints, either because more security is required or because the endpoint is the only place the function can be performed.

- More “defense in depth” deployments
 - ▶ Security no longer perimeter based
 - ▶ Server is last layer in defense in depth

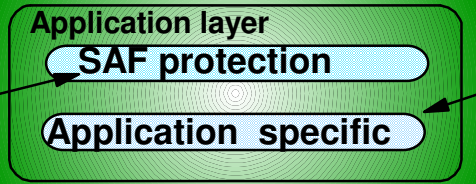
- Driven by regulatory compliance and more stringent IT security policies
 - ▶ Many new industry and government standards (PCI DSS, HIPAA, SOX, etc.)
 - ▶ Driving many enterprises to adopt new security practices
 - ▶ Data privacy is a common theme – drives end-to-end network crypto

- Increasing adoption of network security in servers
 - ▶ Seeing increasing deployment of both IPSec and TLS on z/OS
 - ▶ “Self-protect” features such as IP packet filtering (“personal firewall” on server), IDS

- Focus on minimizing security deployment costs
 - ▶ Application transparent network security reduces application costs

Protocol Stack View of TCP/IP Security Functions

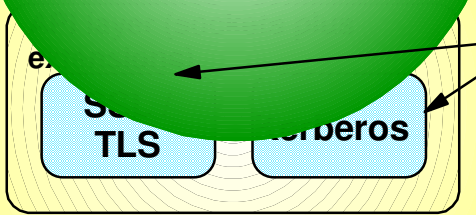
Protect the system
 z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources.



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

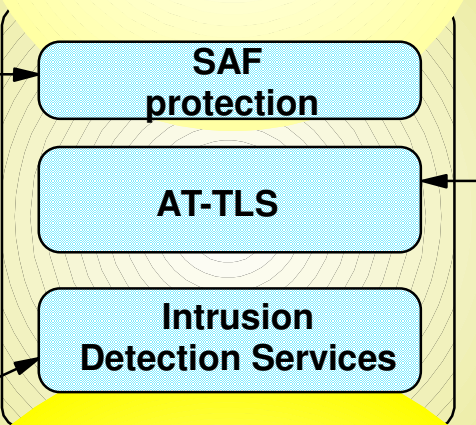
Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

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

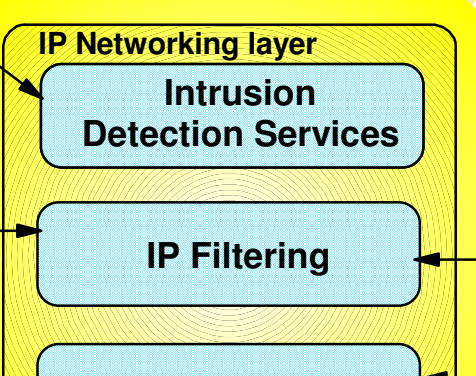


AT-TLS is TCP/IP stack service that provides SSL/TLS services at the TCP transport layer. It is transparent to upper-layer protocols. It is available to TCP applications in all programming languages except PASCAL.

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 system doesn't specifically permit. These can be configured or can be applied dynamically as "defensive filters."

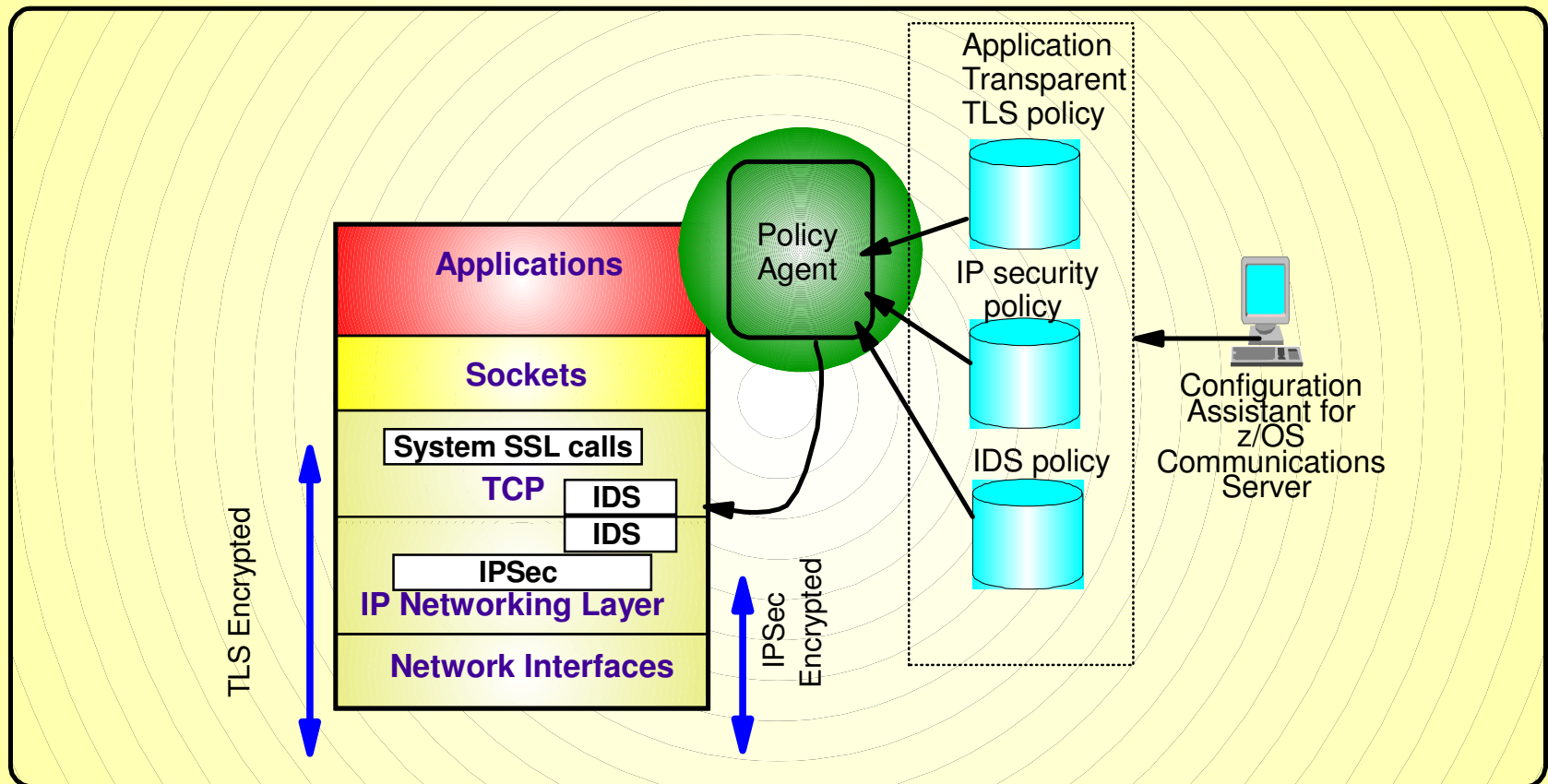


IP packet filters specify traffic that requires security. Sec resides at the networking layer and is transparent to upper-layer protocols, including

Agenda

z/OS Communications Server Network Security

- Overview
 - ▶ Roles and objectives
 - ▶ Deployment trends and requirements
- 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
 - ▶ Policy-based Network Security Componentry
- Enterprise-wide Security Roles
 - ▶ Centralized Policy Agent
 - ▶ Network Security Services

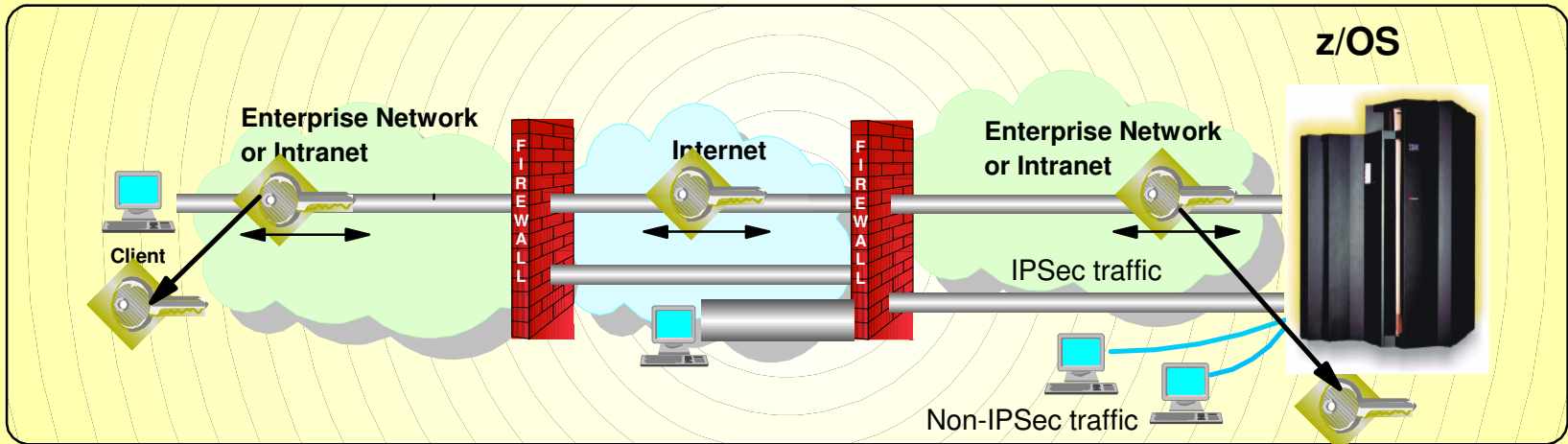


- Policy-driven using Communications Server Policy Agent
 - ▶ Configuration for each TCP/IP stack defines security requirements
- Network security without requiring application changes
 - ▶ Security services provided by the TCP/IP stack
 - AT-TLS, IP security, IDS
- Configure AT-TLS, IP security, IDS policy with a single, consistent administrative interface using Configuration Assistant for z/OS Communications Server

z/OS Communications Server Network Security

IP Security

- IP packet filtering
- IPSec



- Protection
 - ▶ IP filtering
- Cryptographic
 - ▶ Manual IPsec for...

z/OS Communications Server IP Security Features

■ Supports many configurations

- ▶ Optimized for role as endpoint (host), but also support routed traffic (gateway)
- ▶ IPSec NAT Traversal support (address translation and port translation)
- ▶ IPv4 and IPv6 support

■ Policy-based

- ▶ Configuration Assistant GUI for both new and expert users
- ▶ Direct file edit into local configuration file

■ Cryptographic algorithms

- ▶ RSA signature-based authentication
- ▶ ECDSA signature-based authentication
- ▶ HMAC-SHA-1, HMAC-MD5 authentication
- ▶ HMAC-SHA-2, AES-XCBC, AES-GMAC authentication
- ▶ AES-CBC, 3DES and DES encryption
- ▶ AES-GCM (128- and 256-bit) encryption
- ▶ Uses cryptographic hardware if available for most algorithms
- ▶ FIPS 140 mode

See session 12773 for more information

■ zIIP Assisted IPSec

- ▶ Moves most IPSec processing from general purpose processors to zIIPs

■ IP Security Monitoring Interface

- ▶ IBM Tivoli OMEGAMON XE for Mainframe Networks uses this interface

■ Support for latest IPSec RFCs

- ▶ RFCs 4301-4305, 4307-4308
- ▶ RFC 4306 (IKEv2)

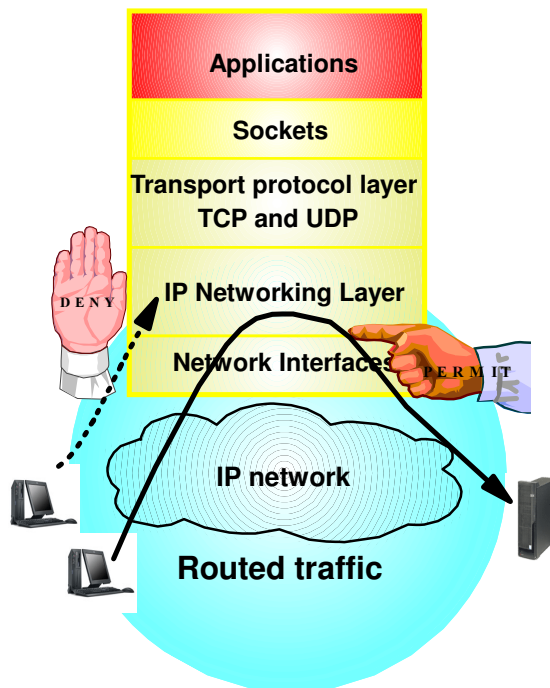
■ z/OS CommServer V1R12 successfully completed USGv6 interoperability testing including the IPSec, IKE, and ESP test suites

- ▶ <http://www.iol.unh.edu/services/testina/iov6/usav6tested.php>

Basics of IP Packet Filtering

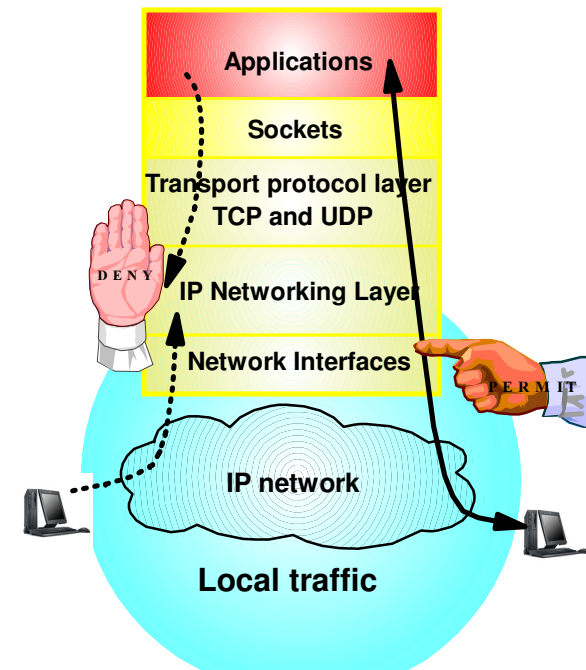
IP packet filtering used to control:

Traffic being routed



- Filter rules defined to match on inbound and outbound packets based on:
 - ▶ packet information
 - ▶ network attributes
 - ▶ time

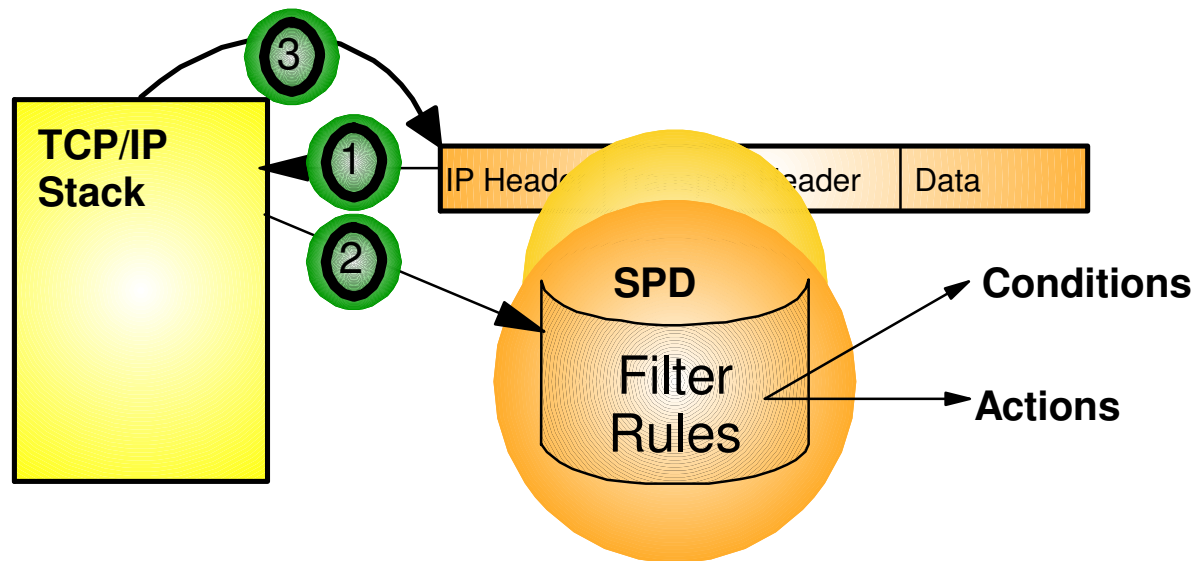
Access at source / destination host



- Possible actions
 - ▶ Permit
 - ▶ Deny
 - ▶ Permit with manual IPsec
 - ▶ Permit with dynamic IPsec
 - ▶ Log (in combination with other ac

IP Filtering Processing Overview

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

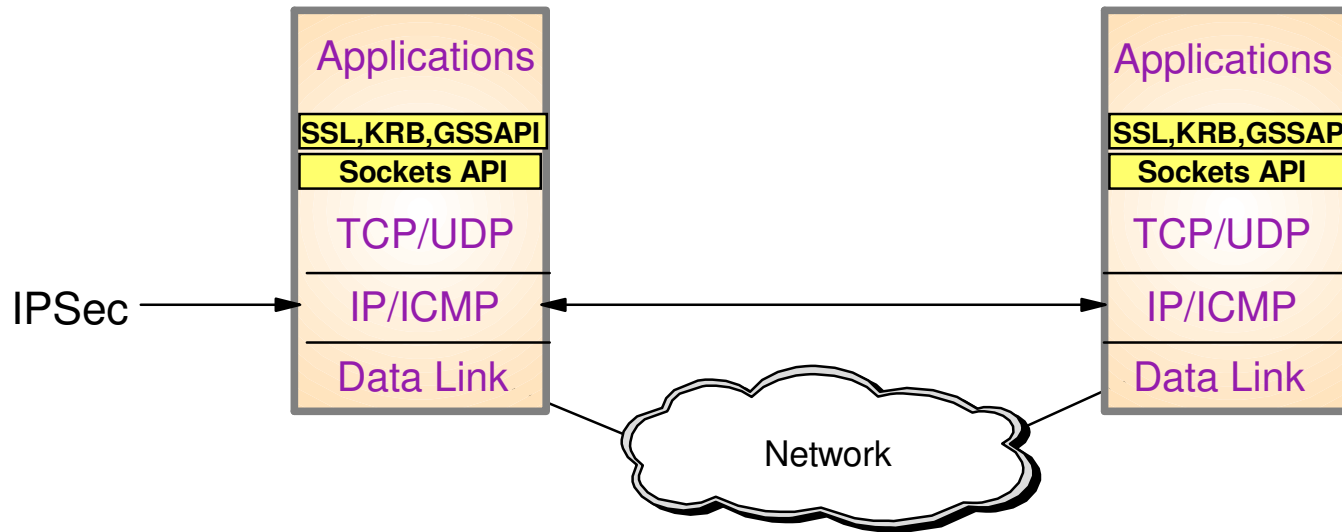


▪ Filter rules are searched in the order they were configured

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
IPv6 Mobility type	For traffic with IPv6 mobility headers, MIPv6 type in header of packet
Fragments Only	Matches fragmented packets only (applicable to routed traffic only)
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 sent/received.
Time condition	

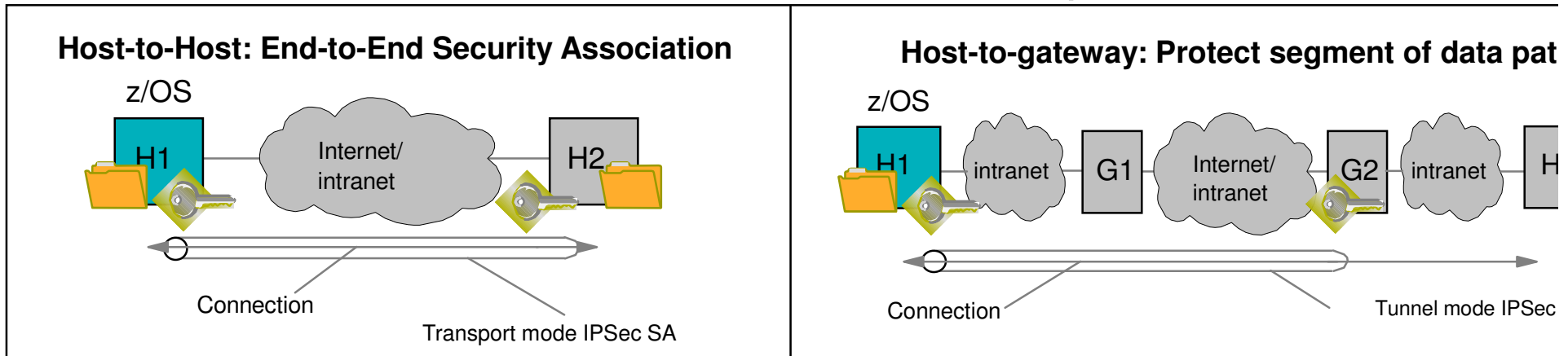
IPSec Protocol Overview



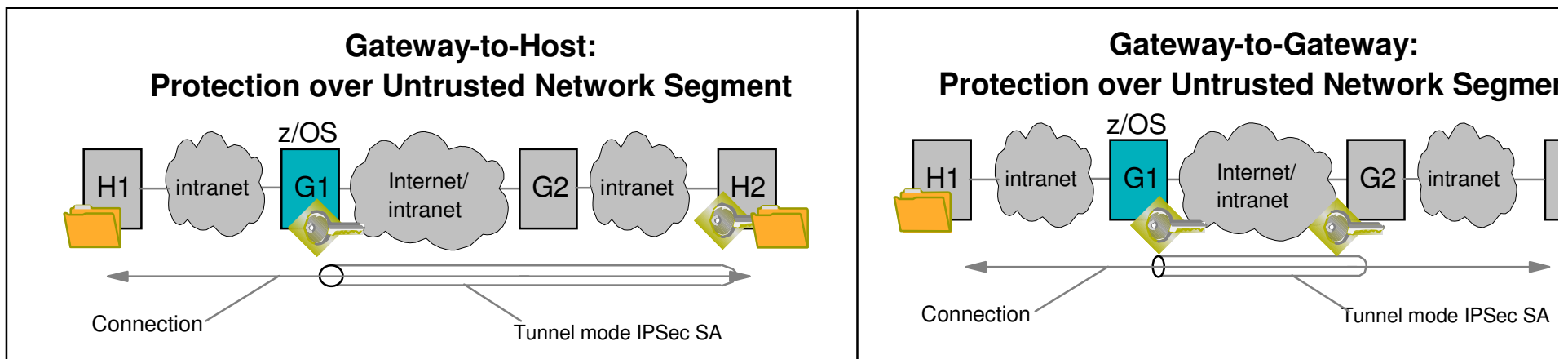
- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
 - ▶ IPSec security protocols
 - **Authentication Header (AH)** - provides data authentication / integrity
 - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional authentication/integrity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

IPSec Scenarios and z/OS Roles

z/OS as Host (Data Endpoint)



z/OS as Gateway (Routed Traffic)



Recent IP Security Enhancements Summary

z/OS Communications Server V1R12

■ **IKE version 2 support**

- ▶ IKE is used by peer nodes to perform mutual authentication and to establish and maintain security associations (SAs).
- ▶ IKEv2 is the latest version of the IKE protocol (RFC 4306)
- ▶ z/OS IKE daemon is enhanced to support IKEv2 protocol concurrently with IKEv1 protocol

■ **Advanced certificate support**

- ▶ Certificate revocation list (CRL)
 - CRLs may be retrieved via HTTP and consulted during IKEv1 or IKEv2 digital signature verification
- ▶ X.509 Certificate Trust Chains
 - The entire X.509 trust chain will be taken into consideration during IKEv1 or IKEv2 digital signature verification without requiring configuration of entire certificate trust chain

■ **IPSec support for cryptographic currency**

- ▶ Support for new encryption and authentication algorithms in IKED and IPSec
- ▶ IKE version 2 support for Elliptic Curve Digital Signature Algorithm (ECDSA)

■ **IPSec, IKE, and NSS support for FIPS 140-2 mode cryptographic modules**

z/OS Communications Server V1R13

■ **NAT Traversal support for IKEv2**

- ▶ IKEv1 support for NAT Traversal available in previous releases

■ **Sysplex Wide Security Associations support for IKEv2**

- ▶ IKEv1 support for Sysplex Wide Security Associations available in previous releases

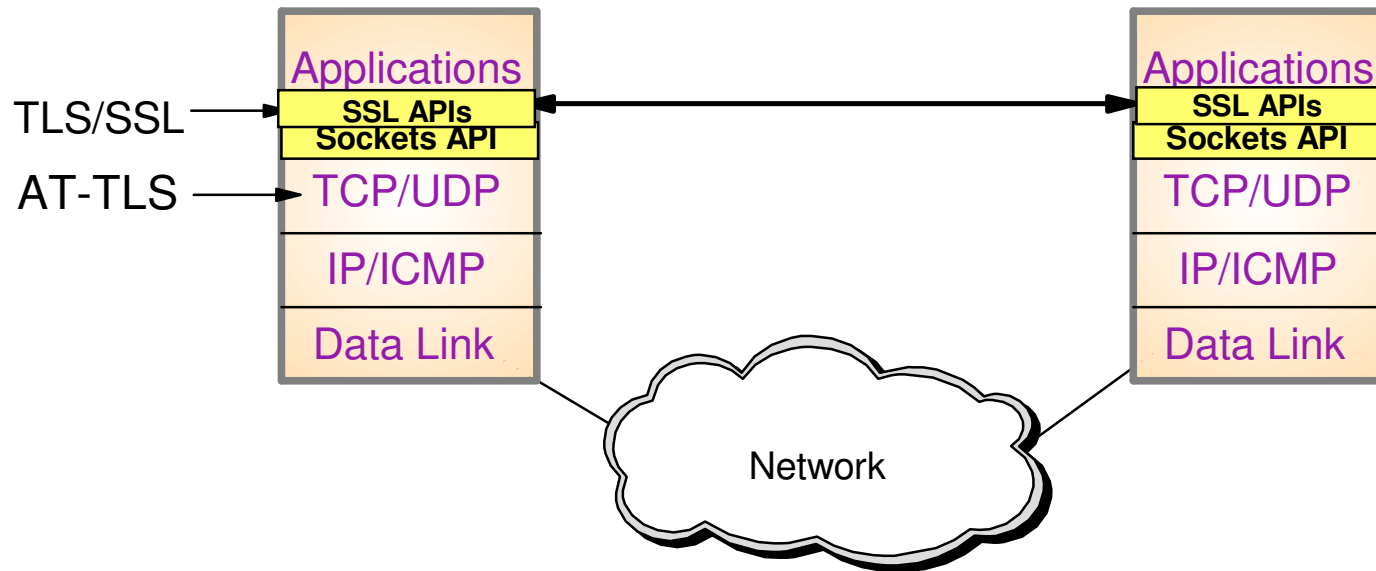
z/OS Communications Server V2R1

■ **Sysplex Wide Security Associations support for IPv6**

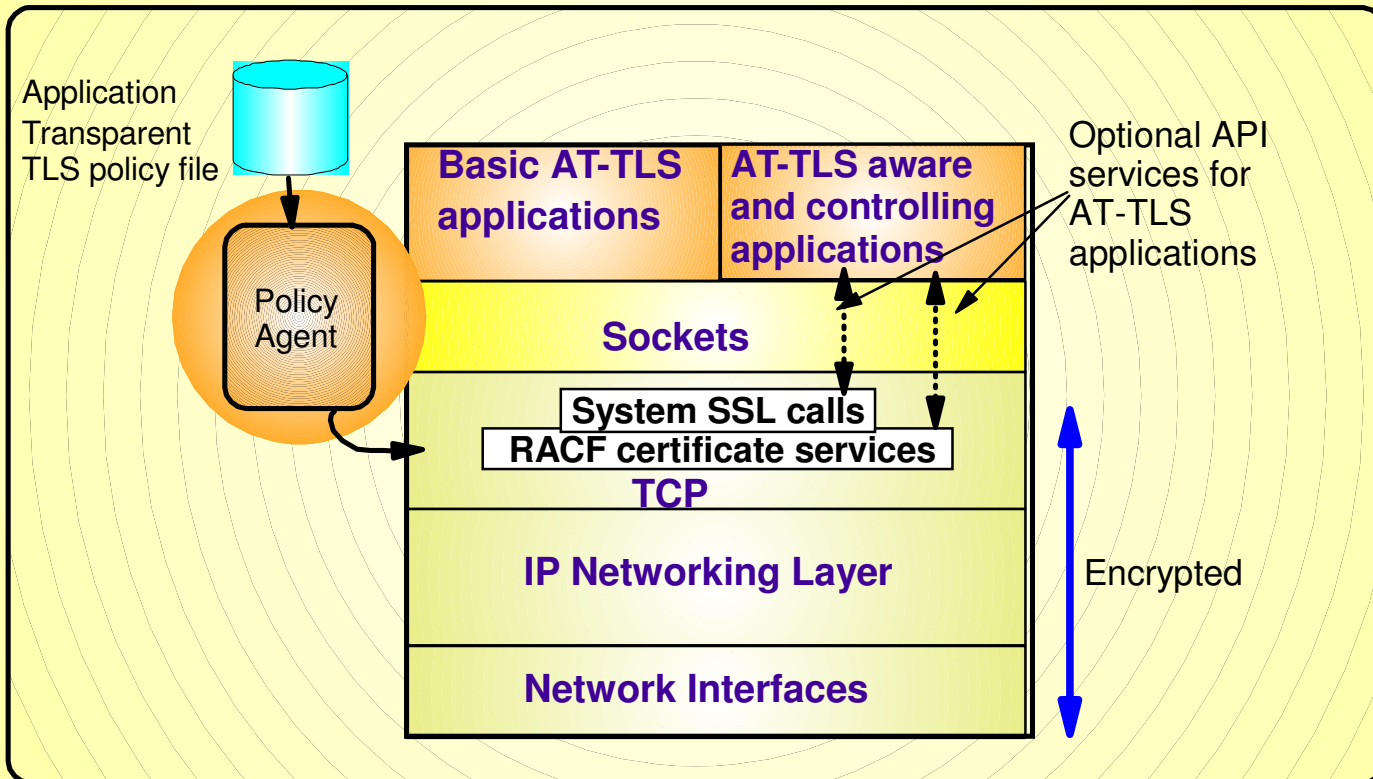
z/OS Communications Server Network Security

**Application Transparent
Transport Layer Security**

Transport Layer Security Protocol Overview



- TLS traditionally provides security services as a socket layer service
 - ▶ TLS requires reliable transport layer,
 - Typically TCP (but architecturally doesn't have to be TCP)
 - ▶ UDP applications cannot be enabled with traditional TLS
 - There is now a TLS variant called Datagram Transport Layer Security (DTLS) which is defined by the IETF for unreliable transports
- On z/OS, System SSL (a component of z/OS Cryptographic Services) provides an API library for TLS-enabling your C and C++ applications
- Java Secure Sockets Extension (JSSE) provides libraries to enable TLS support for Java applications
- However, there is an easier way



- AT-TLS
- AT-TLS
 - ▶ Installed
 - ▶ Configured
- Most applications
 - ▶ AT-TLS Basic app
- Applications can optionally use `IOCTLSSLCTL ioctl call`
 - ▶ AT-TLS Aware applications
 - Extract information (policy, handshake results, X.509 client certificate, userid associated with certifi
 - ▶ AT-TLS Controlling applications

AT-TLS Advantages

- Reduces cost
 - ▶ Application development
 - Cost of System SSL integration
 - Cost of application SSL-related configuration support
 - ▶ Consistent TLS administration across z/OS applications
 - Single, consistent AT-TLS policy system-wide vs. application specific policy
- Exploits SSL/TLS features beyond what most SSL/TLS applications choose to support
 - ▶ CRLs, multiple keyrings per server, use of System SSL cache, etc.
- Support of new System SSL functions without application changes
 - ▶ AT-TLS makes vast majority of System SSL features available to applications
 - ▶ As System SSL features are added, applications can use them by administrative change to AT-TLS policy
- Allows SSL/TLS-enablement of non-C sockets applications on z/OS (e.g., CICS sockets, assembler and callable sockets, etc.)

Recent AT-TLS Enhancements Summary

z/OS Communications Server V2R1

- **Transport Layer Security (TLS) Renegotiation Extension (RFC 5746):**
 - ▶ Provides a mechanism to protect peers that permit re-handshakes
 - ▶ When supported, it enables both peers to validate that the re-handshake is truly a continuation of previous handshake

- **Support Elliptic Curve Cryptography (ECC)**
 - ▶ Twenty new ECC cipher suites
 - ▶ ECC cipher suites for TLS (RFC 4492)

- **TLS Protocol Version 1.2 (RFC 5246):**
 - ▶ Twenty-one new cipher suites
 - 11 new HMAC-SHA256 cipher suites
 - 10 new AES-GCM cipher suites

- **Support for Suite B cipher suites**
 - ▶ TLS is required
 - ▶ All cipher suites use ECC
 - ▶ Suite B has two levels of cryptographic strength that can be selected
 - 128 or 192 bit

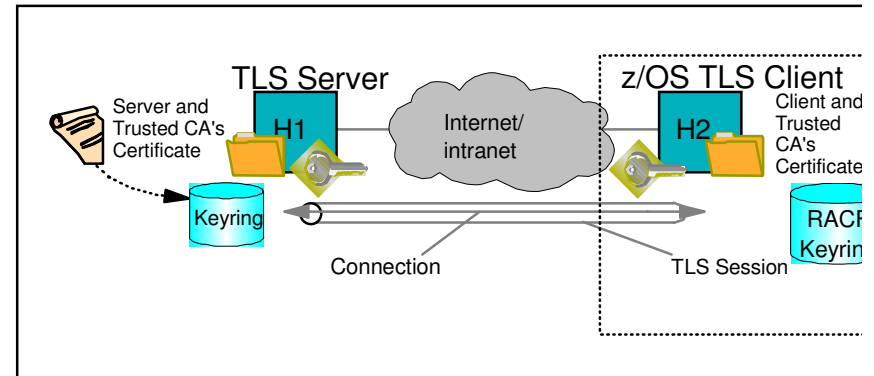
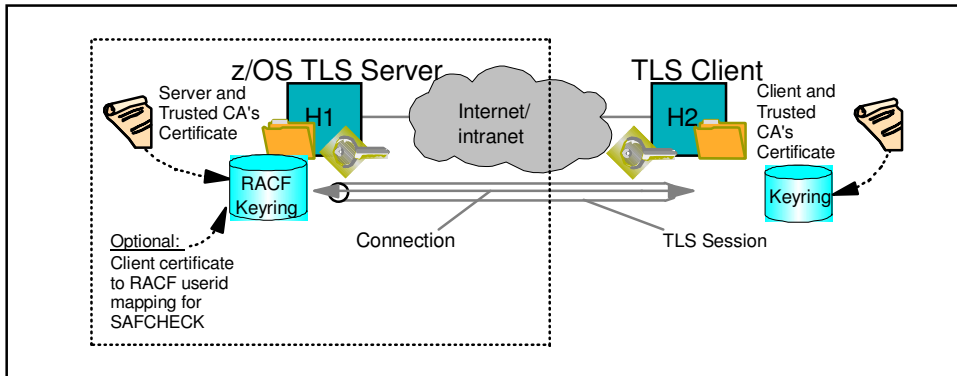
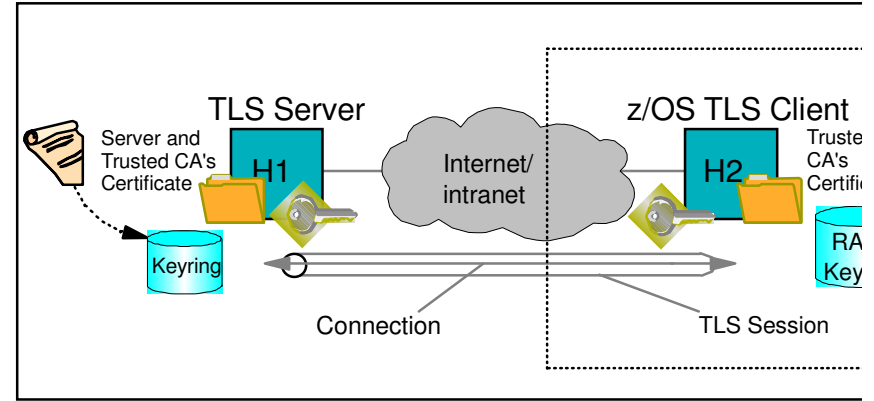
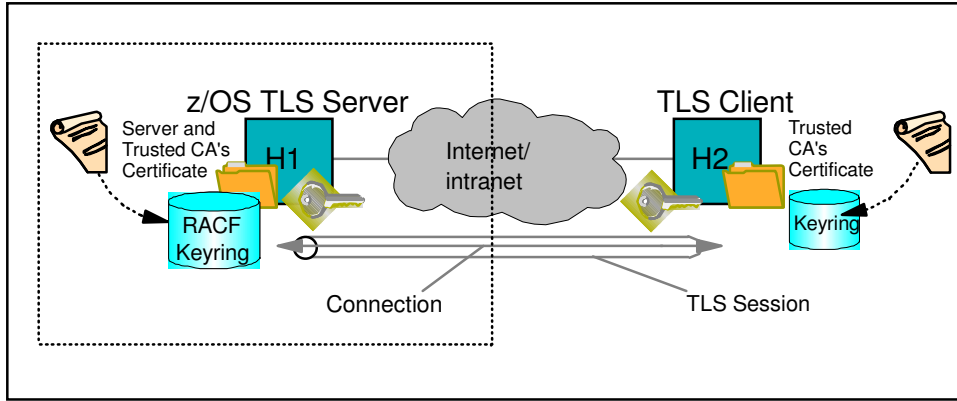
AT-TLS Policy Conditions


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 Supported Roles

z/OS as Server

z/OS as Client



Legend 

Server authentication only

Server + client authentication

Some Applications That Use AT-TLS

- CommServer applications
 - ▶ TN3270 Server
 - ▶ FTP Client and Server
 - ▶ CSSMTP
 - ▶ Load Balancing Advisor
 - ▶ IKE NSS client
 - ▶ NSS server
 - ▶ Policy agent
- DB2 DRDA
- IMS-Connect
- JES2 NJE
- Tivoli Netview applications
 - ▶ MultiSystem Manager
 - ▶ NetView Management Console
- RACF Remote Sharing Facility
- CICS Sockets applications
- 3rd Party applications
- Customer applications

IPSec* and AT-TLS Comparison

Attribute	IPsec	AT-TLS
Traffic covered	All IP traffic (TCP, UDP, ICMP, etc.)	TCP connections
Provides true end-to-end protection	Yes	Yes
Provides network segment protection	Yes	No
Protection scope	Flexible (all traffic, single protocol, single or range of connections, etc.)	Single TCP connection
Requires application modifications	No	No, unless advanced function needed
Endpoints and authentication	IP node to IP node	Application to application
Auth credentials	(dynamic tunnels only) X.509 certificates or pre-shared keys	X.509 certificates
Session key refresh	Configurable based on data and time.	Configurable based on time.

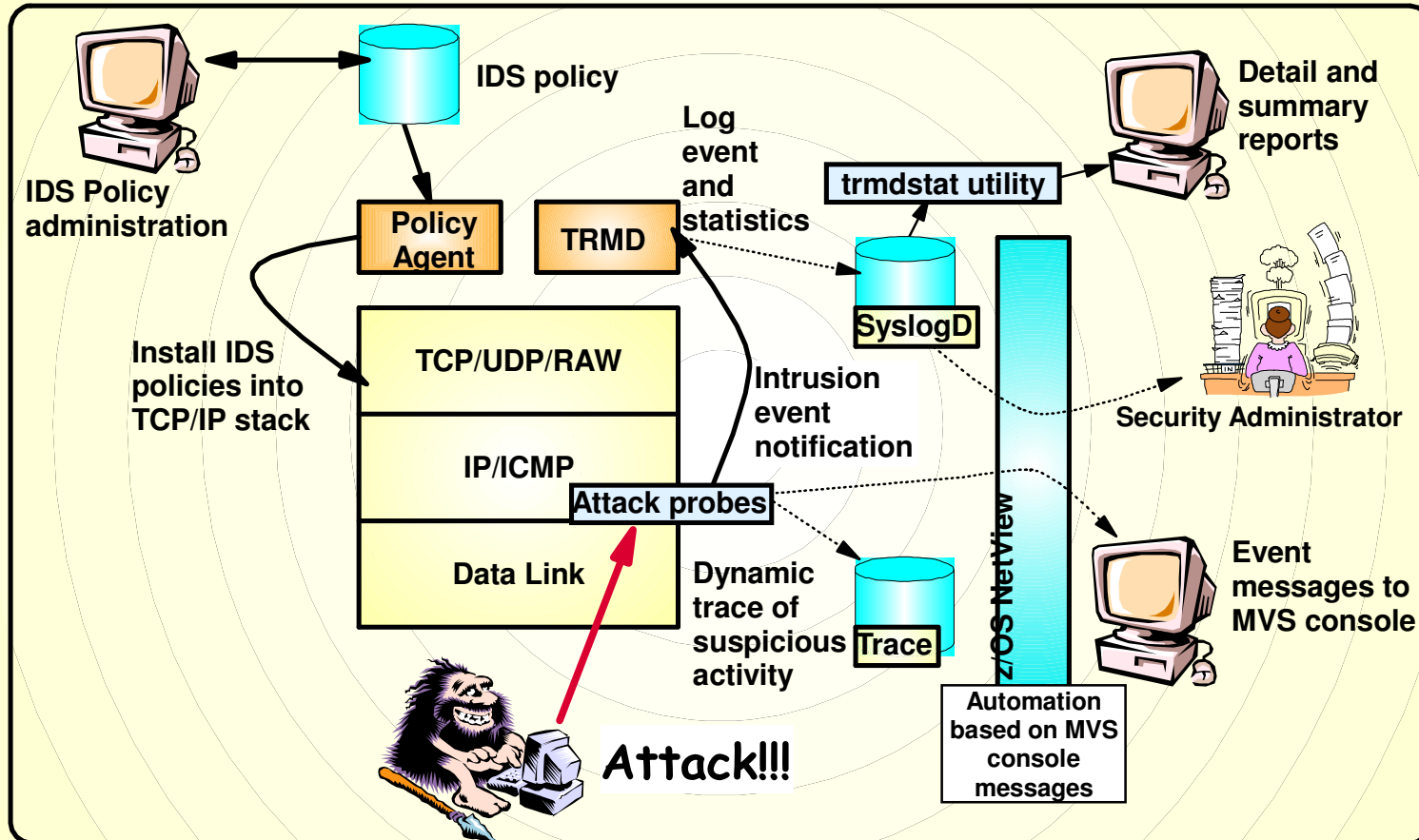
* using IKE to establish IPsec tunnels dynamically

z/OS Communications Server Network Security

Intrusion Detection Services

Overview

z/OS Communications Server IDS, provides integrated intrusion detection and prevention for the network



Events detected

- Scans
- Attacks Against Stack
- Flooding
- Denial of Service methods
- Packet discarding
- Permit connections
- Logging
- Event messages to console
- OS packet notifications
- Tivoli NetView

Policy

Samples provided with Configuration Assistant for Communications Server

Integrated Intrusion Detection Service under policy control to identify, alert and document suspicious activity

through

internal

Intrusion Event Types Supported

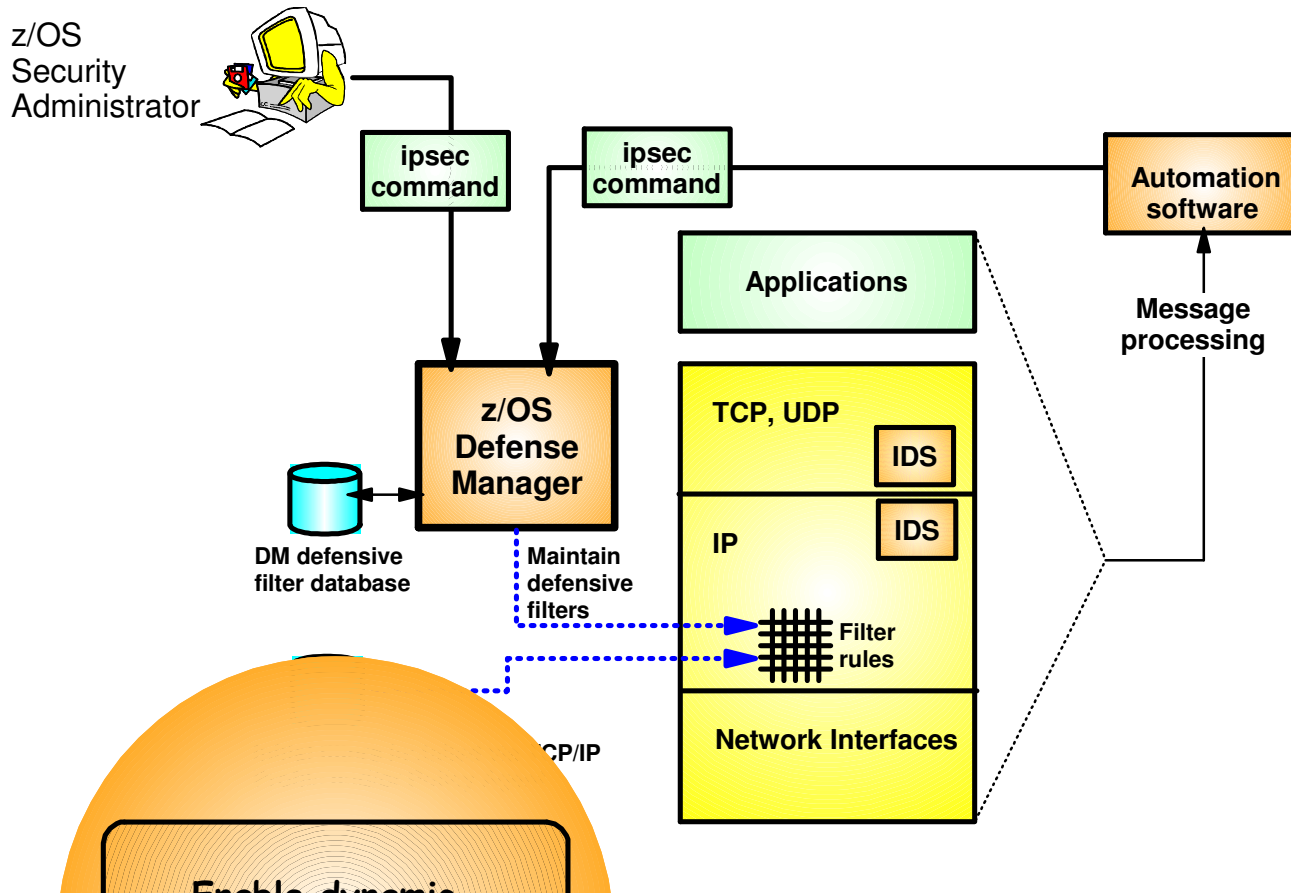
In V1R13 all IDS event types are updated to support IPv6

- 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
 - Outbound raw restrictions
 - UDP perpetual echo
 - Flood events (physical interface flood detection and synflood)
 - Data hiding **
 - TCP queue size **
 - Global system stall **
 - Enterprise extender protection **
- 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 processes when client connect to

z/OS Defensive Filtering

- The 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 create 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 vary**
 - ▶ Global - all stacks on the system where DM runs
 - ▶ Local - apply to a specific stack
- Defensive filters are installed "in front of" configured/default filters**

Agenda

z/OS Communications Server Network Security

- Overview
 - ▶ Roles and objectives
 - ▶ Deployment trends and requirements
- 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
 - ▶ Policy-based Network Security Componentry
- Enterprise-wide Security Roles
 - ▶ Centralized Policy Agent
 - ▶ Network Security Services

Configuration Assistant for z/OS Communications Server



The screenshot shows the title page of the Configuration Assistant for z/OS Communications Server. At the top right is the IBM logo. The main title is "Configuration Assistant for z/OS Communications Server" with "Version 1, Release 13" below it. A central banner features a collage of colorful, abstract images including gears, a lightbulb, and various geometric shapes. At the bottom left, there is a copyright notice, and at the bottom right, the Java logo is visible.

IBM

Configuration Assistant
for z/OS Communications Server
Version 1, Release 13

(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006, 2011. 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.

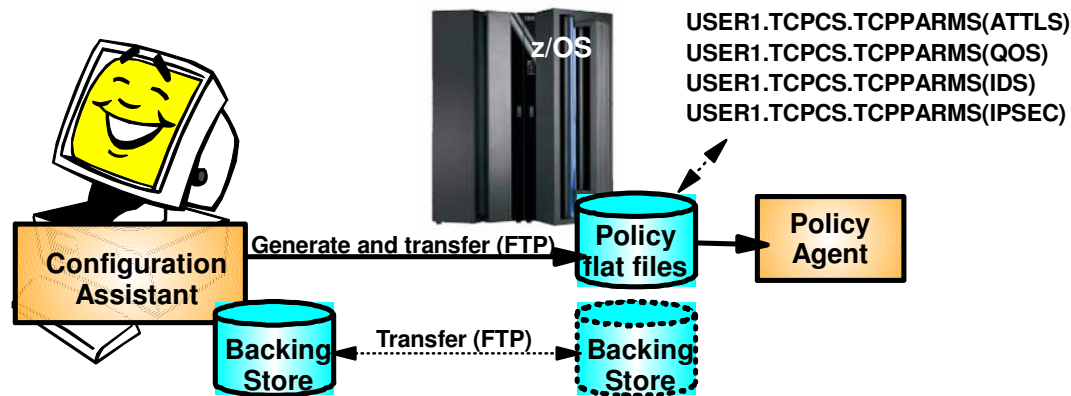
Java

- **GUI-based approach to configuring multiple policy disciplines:**
 - ▶ IDS
 - ▶ AT-TLS
 - ▶ IPSec and IP filtering
 - ▶ QoS
 - ▶ Policy-based Routing (PBR)
- **Separate perspectives but consistent model for each discipline**
- **Focus on high level concepts vs. low level file syntax**
- **z/OSMF-based web interface (strategic) and standalone Windows application**
- **Builds and maintains**
 - ▶ Policy files
 - ▶ Related configuration files
 - ▶ JCL procedures and RACF definitions
- **Supports import of existing policy files**

Configuration Assistant for z/OSMF

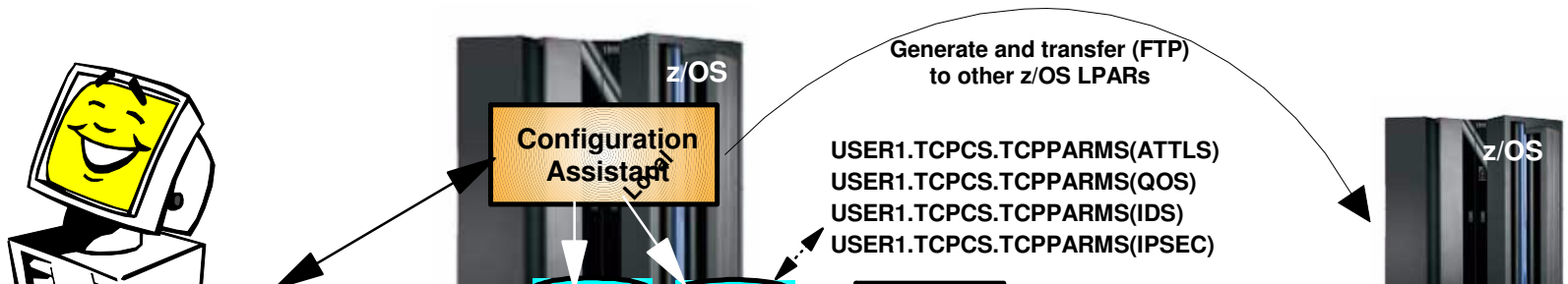
■ Originally, Configuration Assistant ran on Windows

- ▶ Maintains and operates on an internal representation of policy called a "backing store"
- ▶ Generated policy files are uploaded to z/OS for runtime enforcement via built-in FTP client
- ▶ Several enhancements and improvements to file management in V1R10



■ In V1R11, Configuration Assistant runs on z/OSMF

- ▶ Web-based UI that runs on z/OS
- ▶ Functionally equivalent to Windows-based tool (plus has support for IP address discovery V1R13)
- ▶ Backing store maintained on z/OS
- ▶ Windows-based Configuration Assistant still available for download through V1R13
- ▶ Starting in z/OS V2R1, Configuration Assistant is available only through z/OSMF

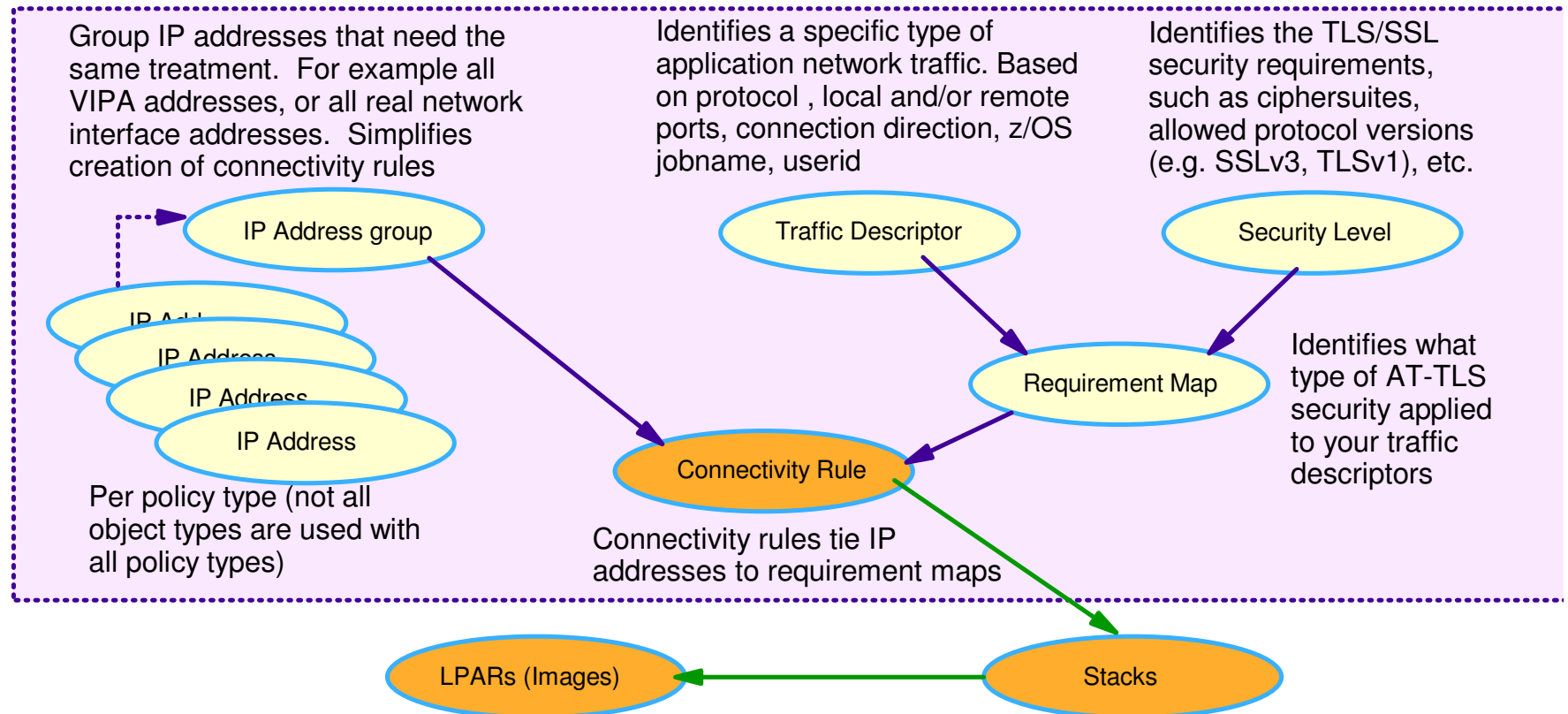


Configuration Assistant Policy Creation Approach

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

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

Configuration Assistant Model - Leveraging reusable objects (AT-TLS example)



1. Create system image and TCP/IP stack image
2. Create one or more Requirement Maps to define desired security for common scenarios (e.g. intranet, branch office, business partner)
 - ▶ Create or reuse Security Levels to define security actions
 - ▶ Create or reuse Traffic descriptors to define application ports to secure
3. Create one or more Connectivity Rules between Data Endpoints (IP addresses) and associate with a

Policy Creation Optimizations

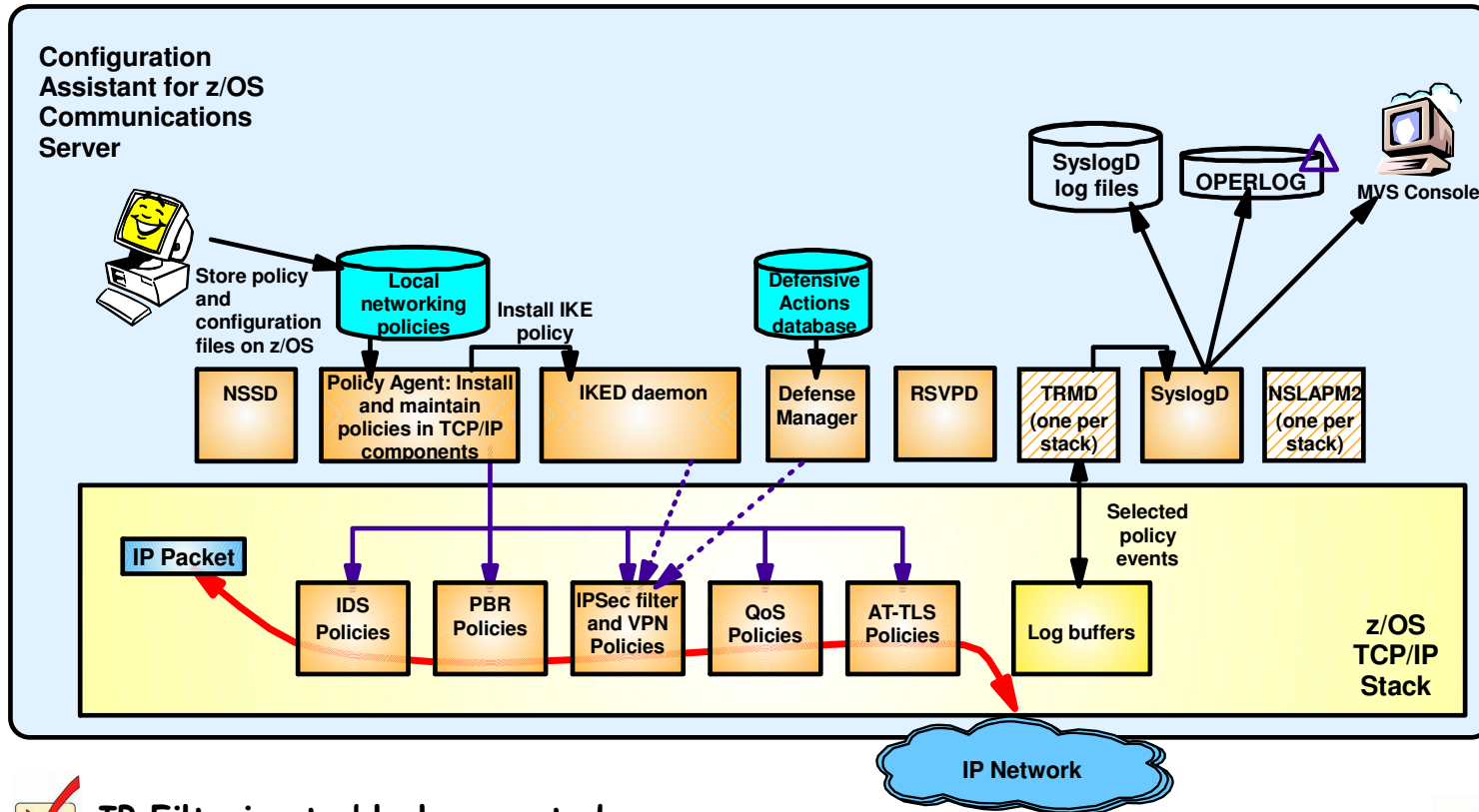
■ **One step requirement map creation for IPSec and AT-TLS**

- ▶ Dialogs eliminate the step of creating requirement map objects before the creation of the connectivity rules.
- ▶ New requirements maps are created seamlessly using the connectivity rule dialogues.
- ▶ Requirement maps created in this dialogue are reusable for subsequent connectivity rule dialogues .

■ **AT-TLS default connectivity rules for common applications**

- ▶ AT-TLS enabled for applications by selection of pre-defined connectivity rules
 - Useful when IP address selectivity not needed
- ▶ In most cases, these rules need no modification and can be enabled for immediate use.
- ▶ Each rule defines an application with default port settings, key ring, and is associated with a default security level.

Policy-Based Networking Componentry



- ▶ Many component manage and oper
 - Some initial set
 - Lots of valuable function!
- ▶ V1R11 simplifies setup and operati networking policy infrstructure, mak easier and less cc gain benefits.

✓ IP Filtering to block unwanted traffic from entering or leaving your z/OS system

✓ Connection-level security for TCP applications without application changes

✓ Making sure high-priority applications also get high-priority processing by the network

✓ Application-specific selection of outbound interface and route (Policy-based routing PBR)

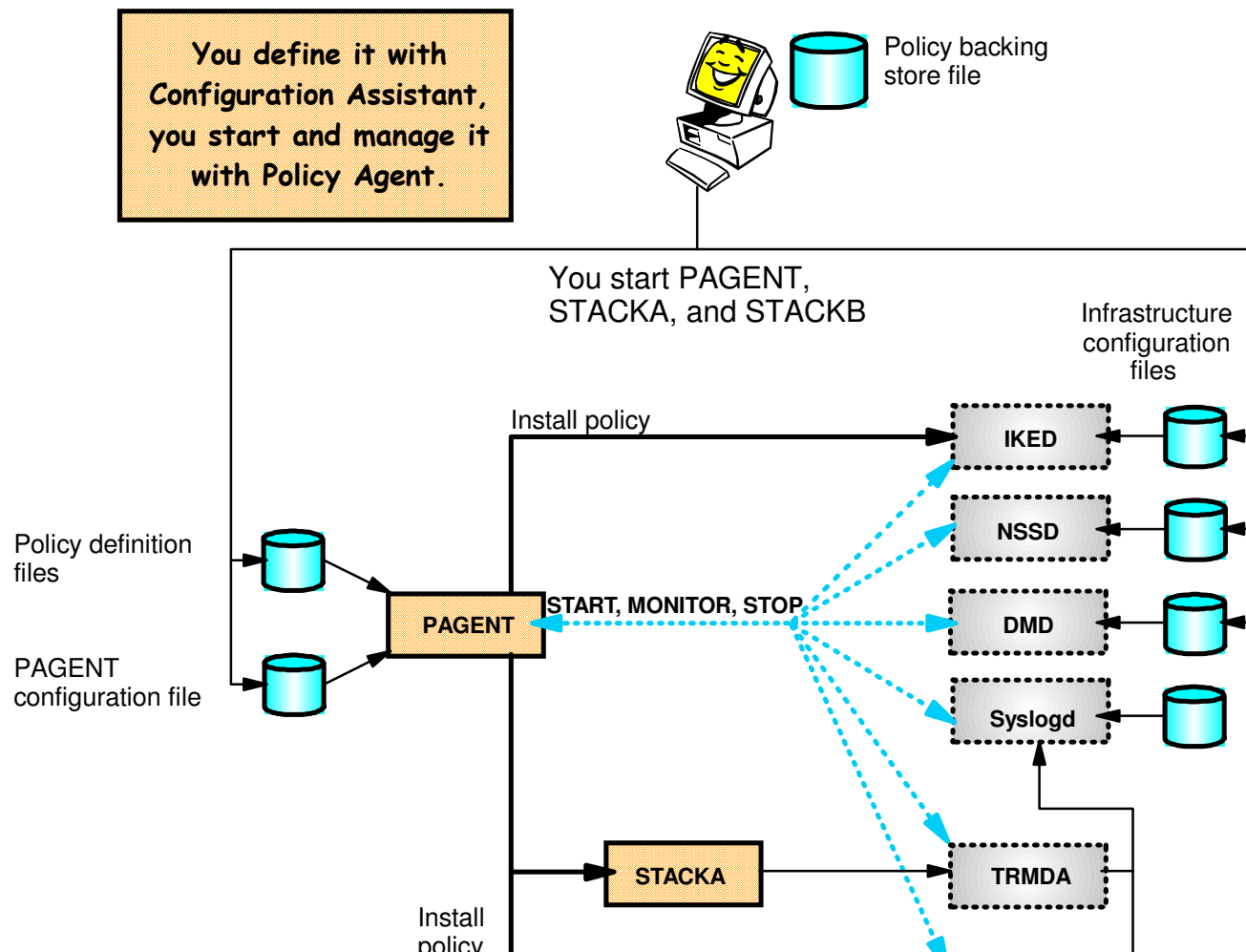
✓ Providing secure end-to-end IPsec SAs on z/OS

✓ Protection against "bad guys" trying to attack your z/OS system

Infrastructure Management Overview

- Originally, the various policy infrastructure components are independently managed:

- Start and stop applications
- Interact with applications using operator commands



- Now the Policy Agent starts, stops, and monitors most policy infrastructure components

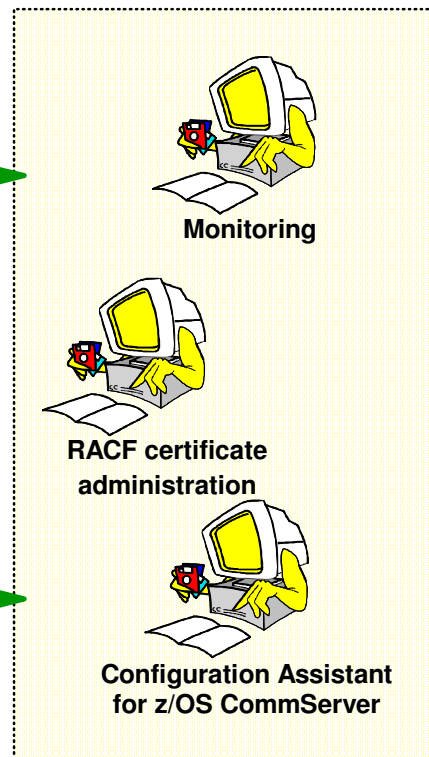
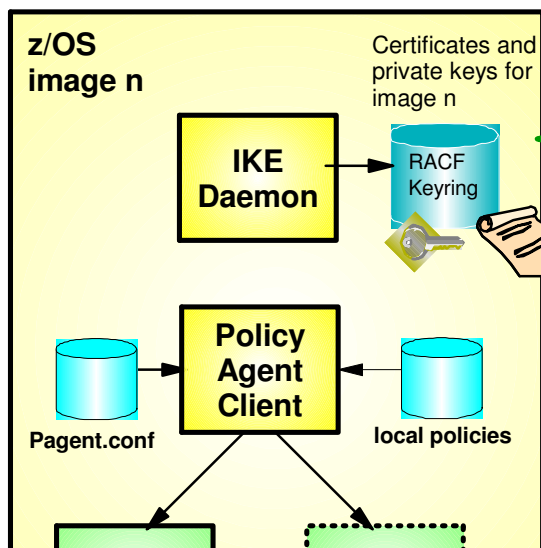
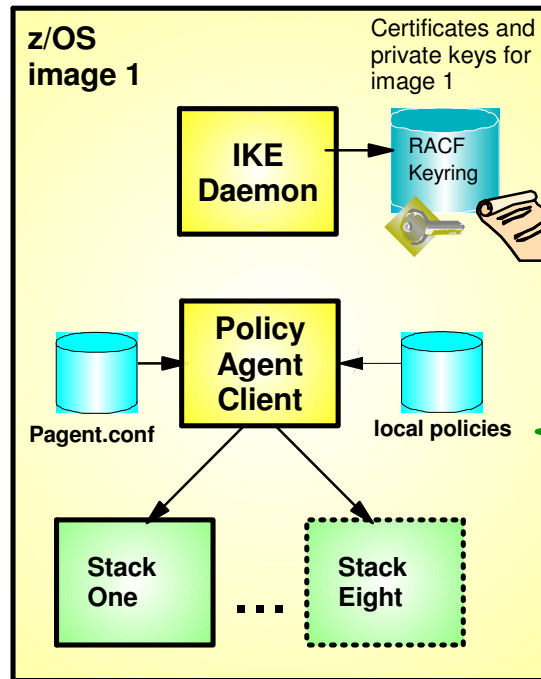
- Syslog daemon (syslogd)
- Traffic Regulation Management daemon (TRMD)
- Internet Key Exchange daemon (IKED)
- Network Security Server daemon (NSSD)
- Defense Manager daemon (DMD)

Agenda

z/OS Communications Server Network Security

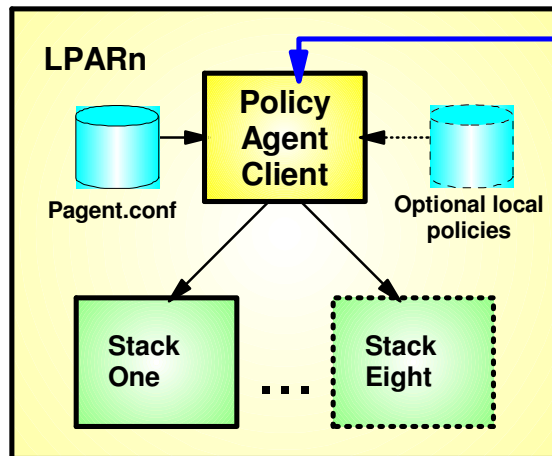
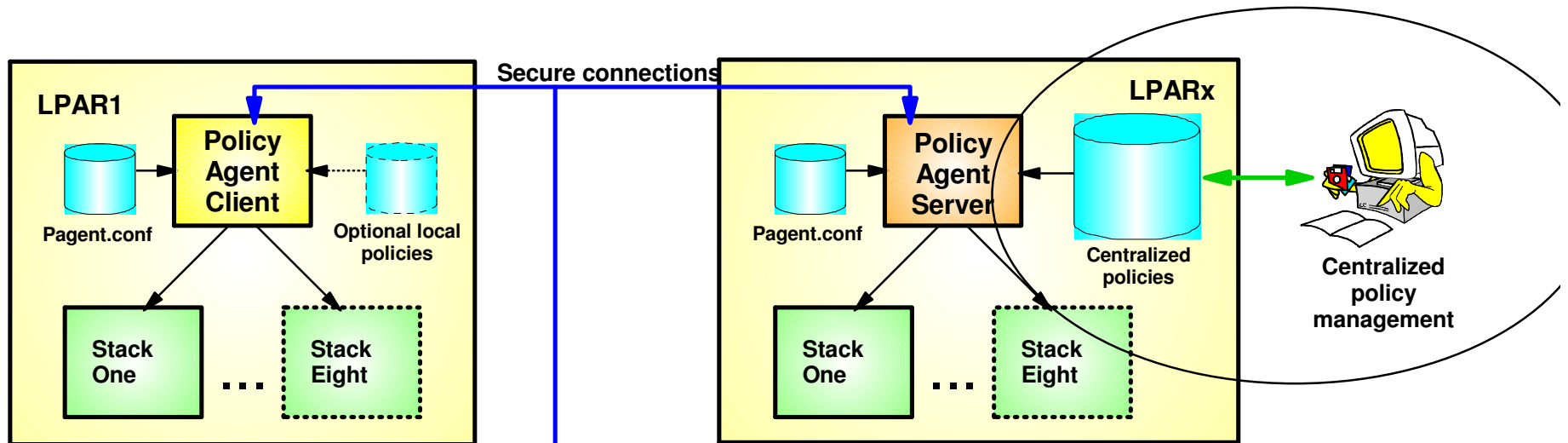
- Overview
 - ▶ Roles and objectives
 - ▶ Deployment trends and requirements
- Policy-based Network Security
 - ▶ IP security (IP packet filtering and IPSec)
 - ▶ Application Transparent TLS
 - ▶ Intrusion Detection Services
- Configuring Policy-based Network Security
 - ▶ Configuration Assistant for z/OS Communications Server
 - ▶ Policy-based Network Security Componentry
- Enterprise-wide Security Roles
 - ▶ Centralized Policy Agent
 - ▶ Network Security Services

Local Network Security Administration



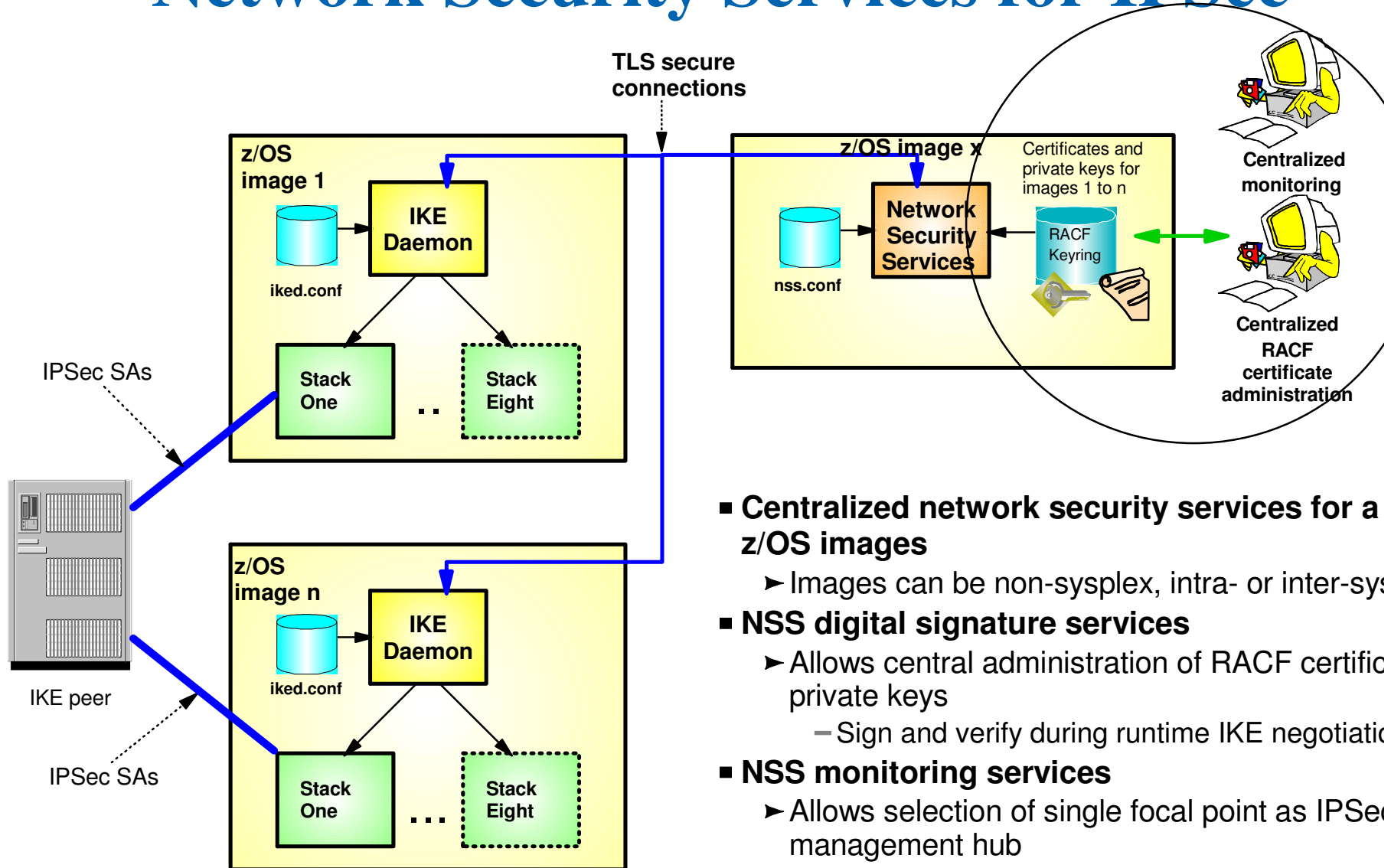
- **Each z/OS system locally admini**
 - ▶ RACF certificate administration
 - ▶ Policy configuration
 - ▶ Monitoring
- **Connectivity required between administration and each manage platform**
 - ▶ Monitoring application has advan knowledge of each managed nod
 - ▶ Coordination required to push pol to each system for deployment

Centralized Network Policy Management



- **Centralized policy management and storage for a set of z/i images based on the Policy Agent technology**
 - ▶ Images can be non-sysplex, within sysplex or cross sysplex
- **Centralized management becomes increasingly important 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

Network Security Services for IPsec



Extending NSS role in z/OS V1R12

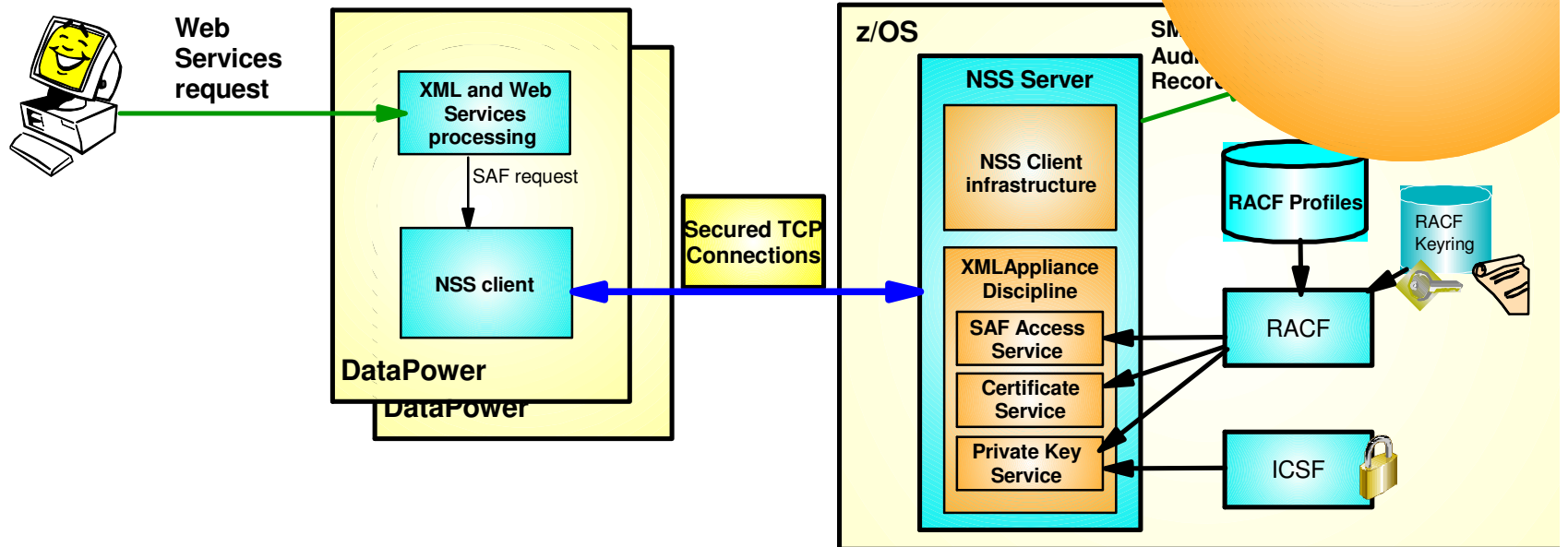
- NSS is required for z/OS V1R12 advanced certificate support

- **Centralized network security services for a z/OS images**
 - ▶ Images can be non-sysplex, intra- or inter-sysplex
- **NSS digital signature services**
 - ▶ Allows central administration of RACF certificate private keys
 - Sign and verify during runtime IKE negotiation
- **NSS monitoring services**
 - ▶ Allows selection of single focal point as IPsec management hub
 - ipsec command for administrator
 - NMI API for management applications
- **Availability options**
 - ▶ Backup NSS can be specified

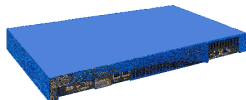
Extending NSS - Integrating DataPower with z/OS

WebSphere DataPower SOA Appliances:

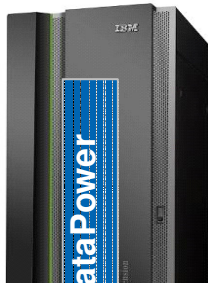
- ▶ Application message format transformation
- ▶ Offloads XML and Web Services security functions



DataPower Appliance (logical integration)



DataPower XI50z Integrated Blade (physical)



NSS XMLAppliance discipline enables both logical and physical integration between DataPower and z/OS security with centralized management across multiple hardware platforms:

- ▶ **SAF Access service** provides SAF-based authentication (of DP users) ; access control (of DP resources) with SMF auditing
- ▶ **Certificate service** provides for retrieval of RSA certificates from a SAF
- ▶ **Private Key service** provides:
 - Private RSA key retrieval (clear key only)
 - RSA signature and decryption operations (secure key only)

Agenda

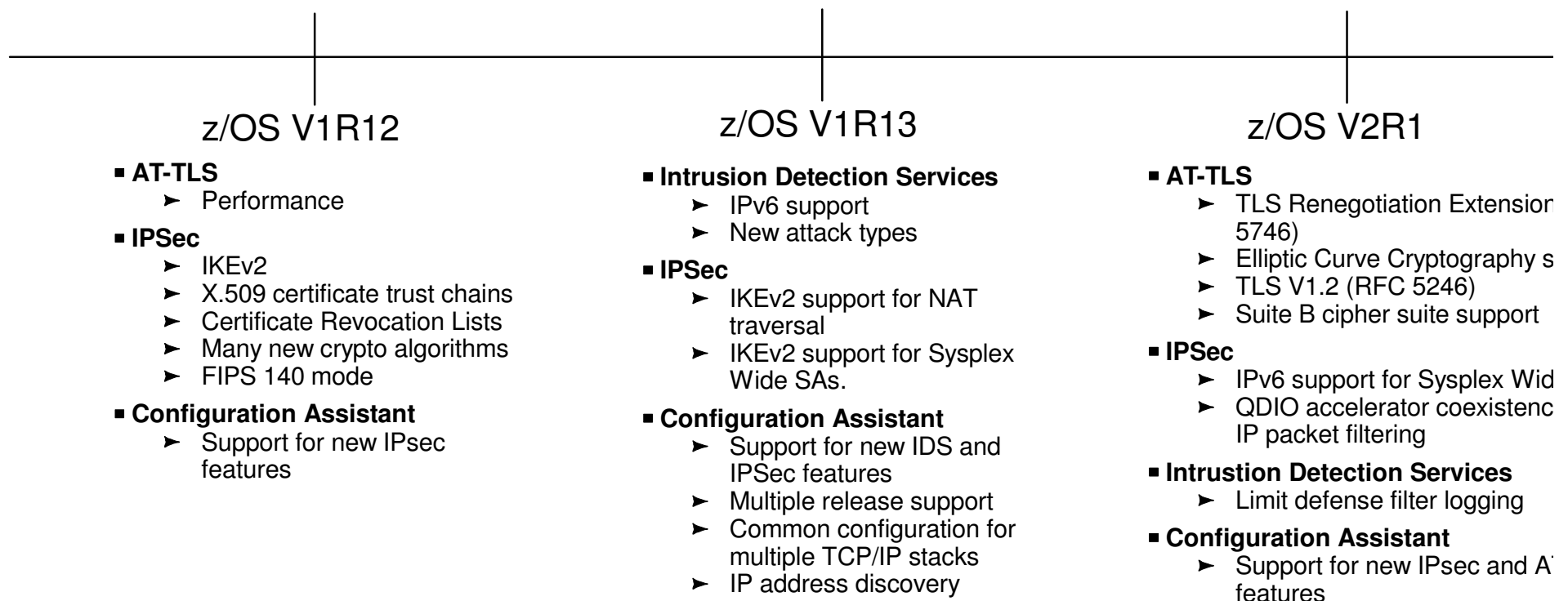
z/OS Communications Server Network Security

- Overview
 - ▶ Roles and objectives
 - ▶ Deployment trends and requirements
- 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
 - ▶ Policy-based Network Security Componentry
- Enterprise-wide Security Roles
 - ▶ Centralized Policy Agent
 - ▶ Network Security Services



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
 - Enterprise Wide Security
 - Policy Agent
 - Configuration Assistant for z/OS Communications Server



For more information ...

URL		Content
http://www.twitter.com/IBM_Commserver		IBM Communications Server Twitter Feed
http://www.facebook.com/IBMCommserver		IBM Communications Server Facebook Fan Page
http://www.ibm.com/systems/z/		IBM System z in general
http://www.ibm.com/systems/z/hardware/networking/		IBM Mainframe System z networking
http://www.ibm.com/software/network/commserver/		IBM Software Communications Server products
http://www.ibm.com/software/network/commserver/zos/		IBM z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/		IBM Communications Server for Linux on System z
http://www.ibm.com/software/network/ccl/		IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library/		IBM Communications Server library
http://www.redbooks.ibm.com		ITSO Redbooks
http://www.ibm.com/software/network/commserver/zos/support/		IBM z/OS Communications Server technical Support including TechNotes from service
http://www.ibm.com/support/techdocs/atmastr.nsf/Web/TechDocs		Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html		Request For Comments (RFC)
http://www.ibm.com/systems/z/os/zos/bkserv/		IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server