



Software Group | Enterprise Networking Solutions

z/OS Communications Server Network Security Overview

SHARE Session 10820

Lin Overby **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:

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

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

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
- Wrap up

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
- Wrap up

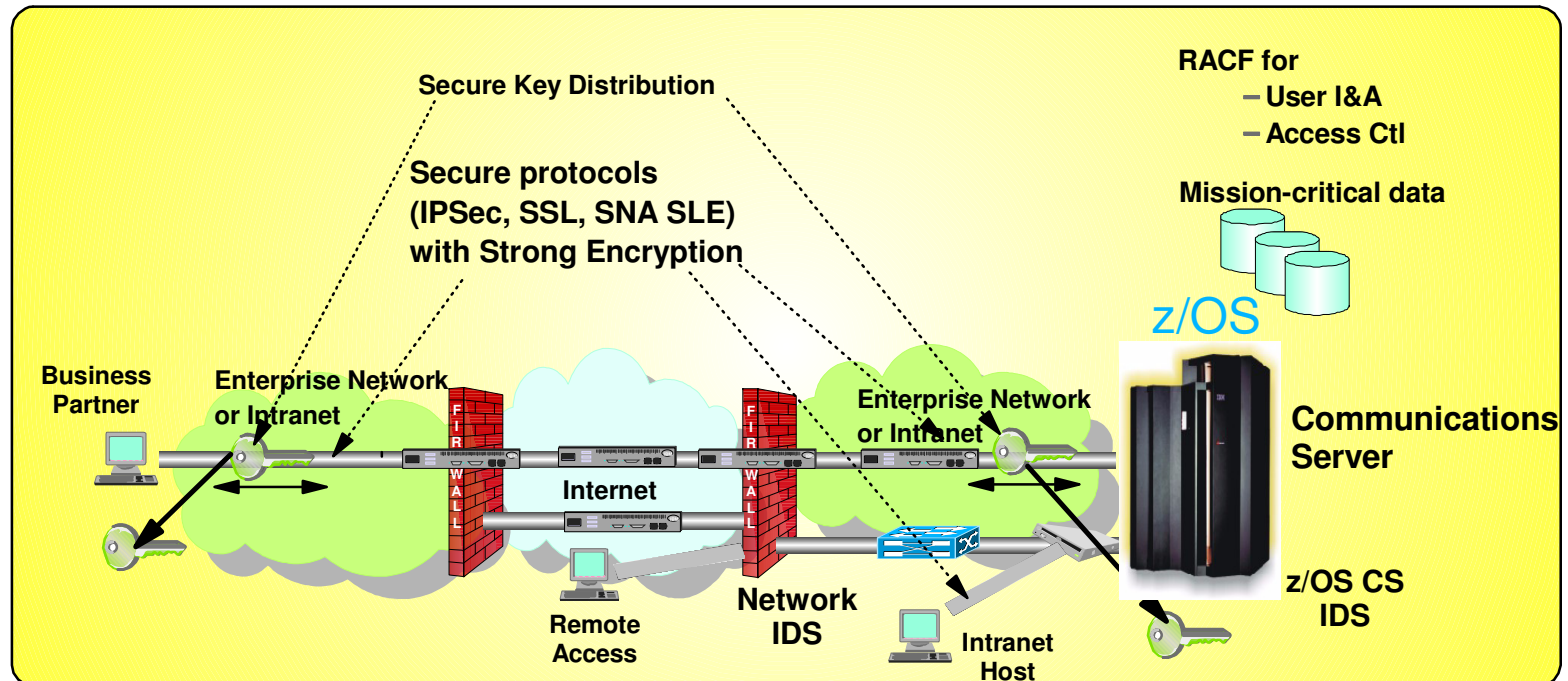
z/OS Communications Server

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

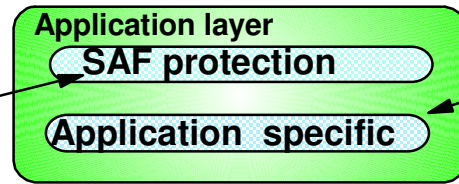
- Protecting the system from the network
 - ▶ Increased access requires focus on self protect
 - ▶ Defense in depth - no longer only perimeter based

- 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

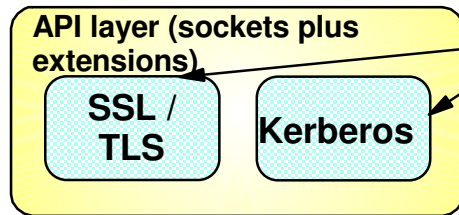
- Minimizing security deployment costs
 - ▶ Application transparent network security reduces application costs
 - ▶ Policy-based network security reduces deployment costs
 - ▶ GUI-based policy administration for ease of use

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.

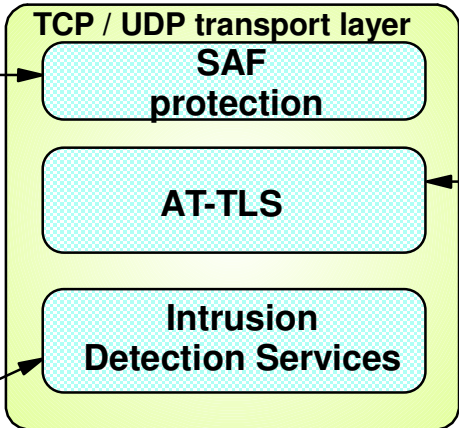


Protect data in the network
Examples of application protocols with built-in security extensions are SNMPv3 and OSPF.



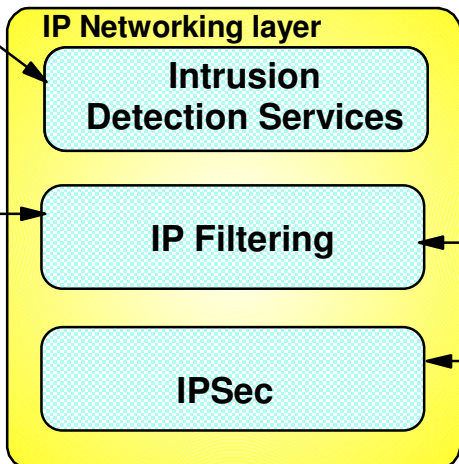
Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

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 as "defensive filters."

IP packet filters specify traffic that requires IPsec

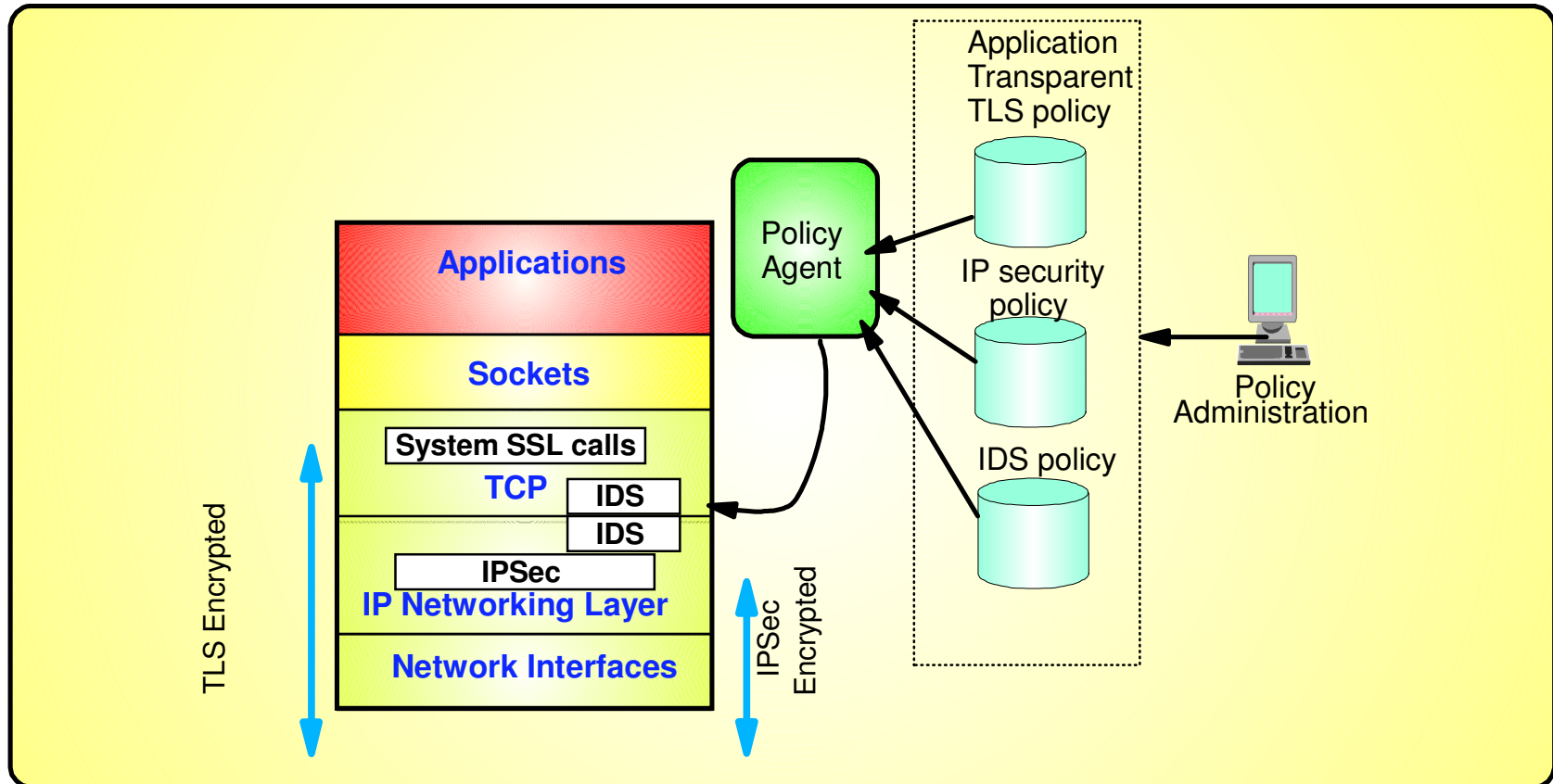
IPsec resides at the networking layer and is transparent to upper-layer protocols, including both transport layer protocol and application protocol.

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
- Wrap up

Policy-based Network Security Overview



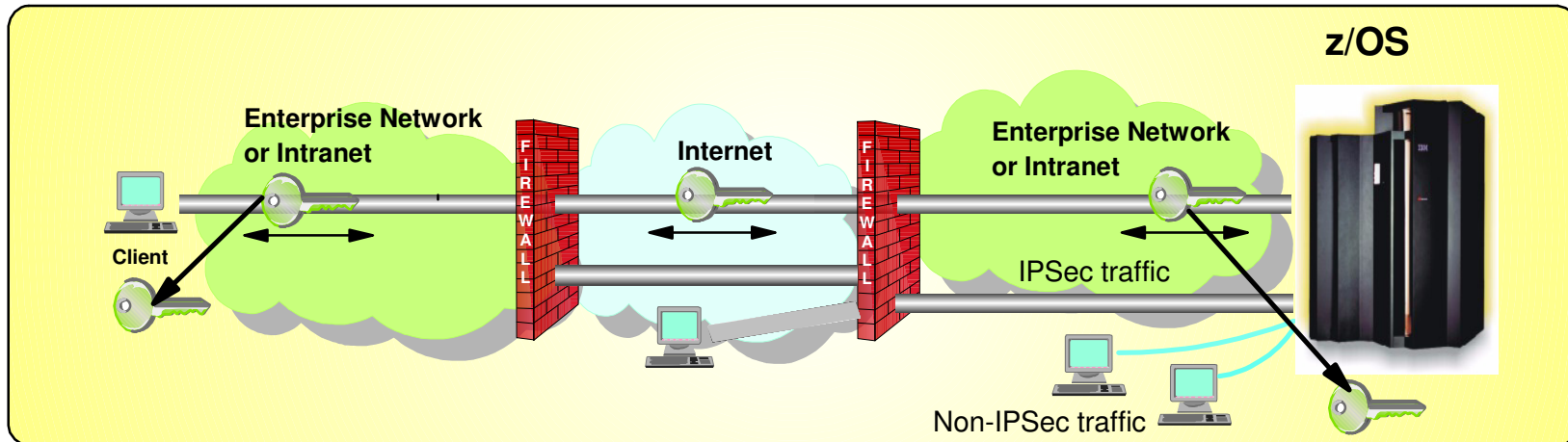
- Policy-driven using Communications Server Policy Agent
 - ▶ Configuration for each TCP/IP stack defines security requirements
- Network security without requiring application changes
 - ▶ Security services provided by the TCP/IP stack
 - AT-TLS, IP security, IDS
- Configure AT-TLS, IP security, IDS 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



A complete IP packet filtering, IPsec and Internet Key Exchange (IKE) solution built into z/OS Communications Server

- Protects the system from the network
 - ▶ IP filtering controls which packets enter the system
- Protects against data leakage from the system
 - ▶ IP filtering controls which packets can leave the system
- Cryptographically protects data in the network
 - ▶ Manual IPsec for statically defined security associations
 - ▶ Dynamic negotiation of IPsec security associations through IKE
- Filter directed logging of IP security actions to syslogd

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

- **Default filters in TCP profile provide basic protection before policy is loaded**

- **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

- **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)

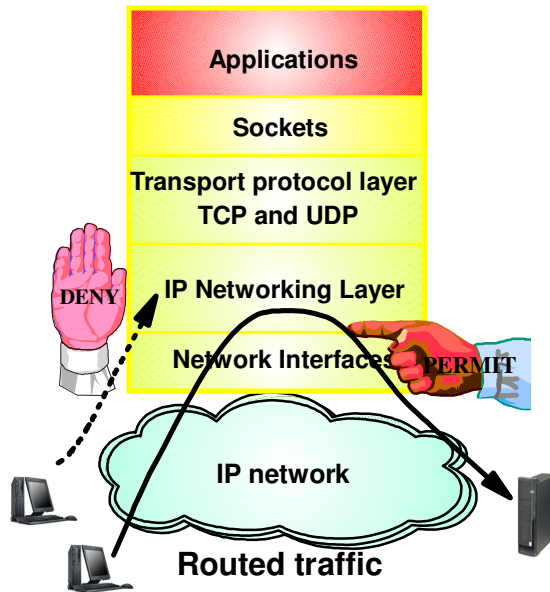
- **z/OS CommServer V1R12 successfully completed USGv6 interoperability testing including the IPsec, IKE, and ESP test suites**
 - <http://www.iol.unh.edu/services/testing/ipv6/usgv6tested.php>

**See sessions 10714 and 10718
for more information**

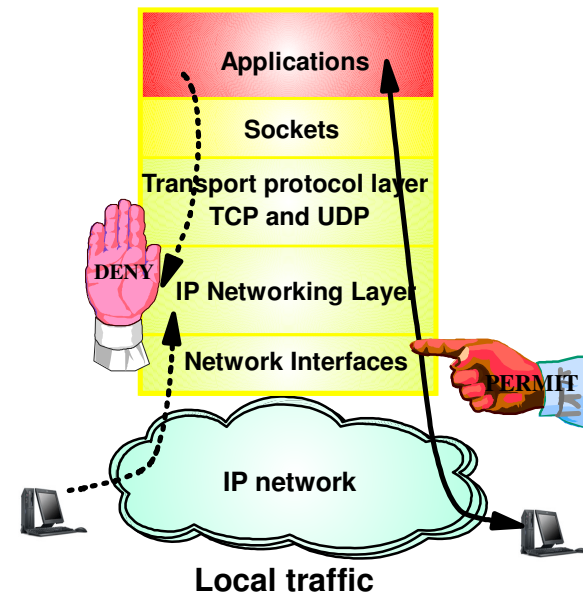
Basics of IP Packet Filtering

IP packet filtering used to control:

Traffic being routed



Access at source / destination host



- **Filter rules defined to match on inbound and outbound packets based on:**

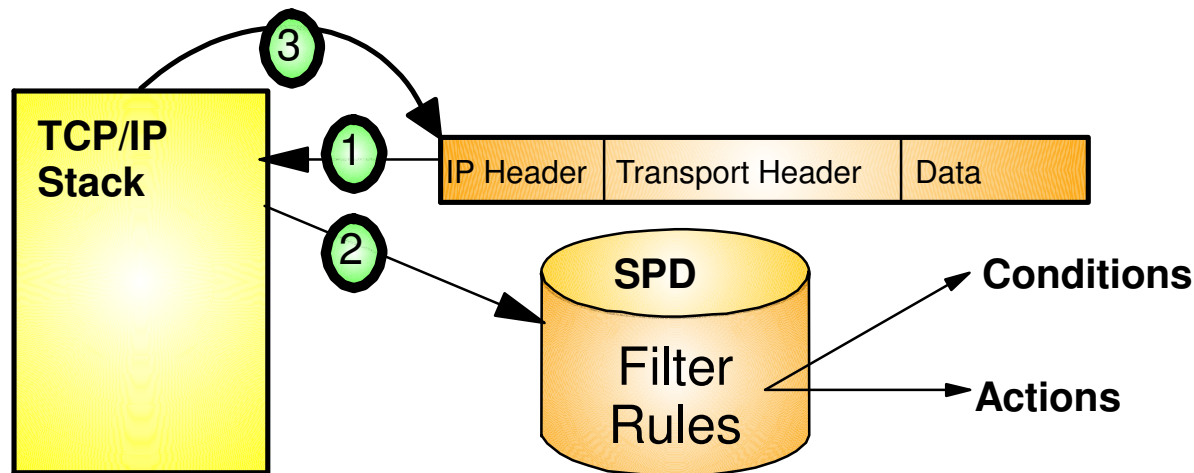
- ▶ packet information
- ▶ network attributes
- ▶ time

- **Possible actions**

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

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

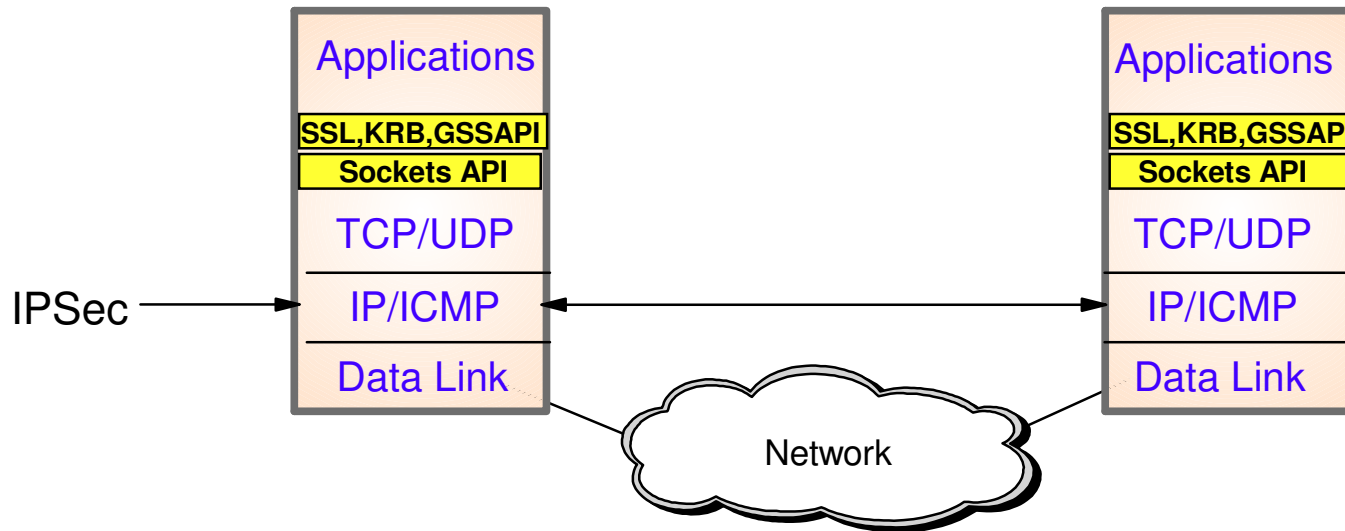


- Filter rules are searched in the order they were configured
- Each rule is inspected, from top to bottom, for a match
- If a match is found, the search ends and the action is performed

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
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 is sent/received.
Time condition	
Time, Day, Week, Month	Indicates when filter rule is active

IPSec Protocol Overview

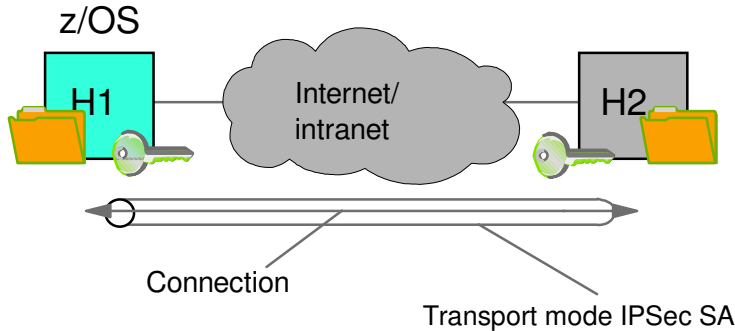


- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
 - ▶ IPSec security protocols
 - **Authentication Header (AH)** - provides data authentication / integrity
 - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional authentication/integrity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

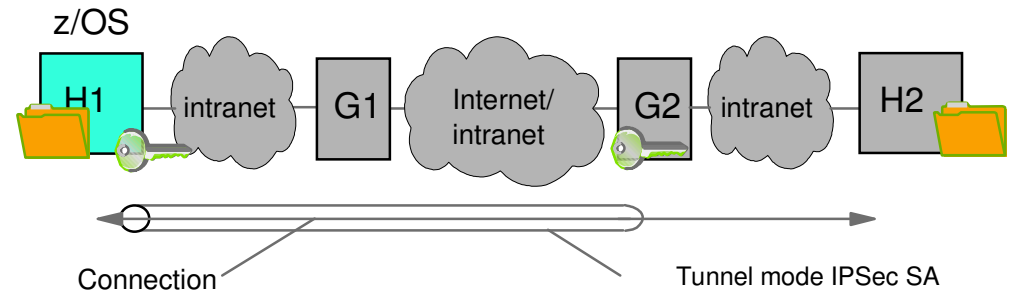
IPSec Scenarios and z/OS Roles

z/OS as Host (Data Endpoint)

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

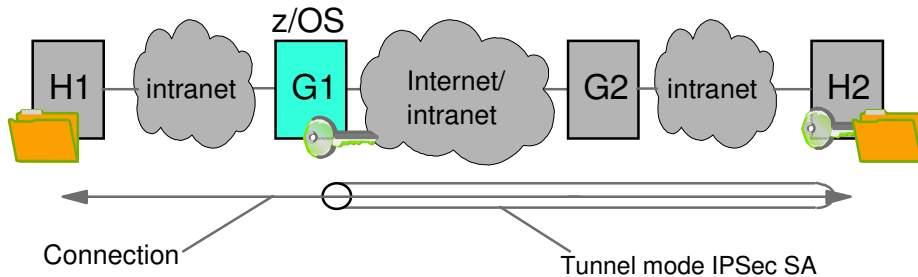


Host-to-gateway: Protect segment of data path

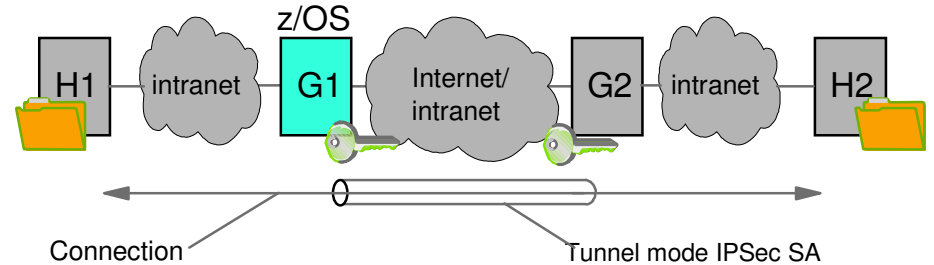


z/OS as Gateway (Routed Traffic)



Gateway-to-Host: Protection over Untrusted Network Segment



Gateway-to-Gateway: Protection over Untrusted Network Segment



Legend

- Data endpoint 
- Security endpoint 

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

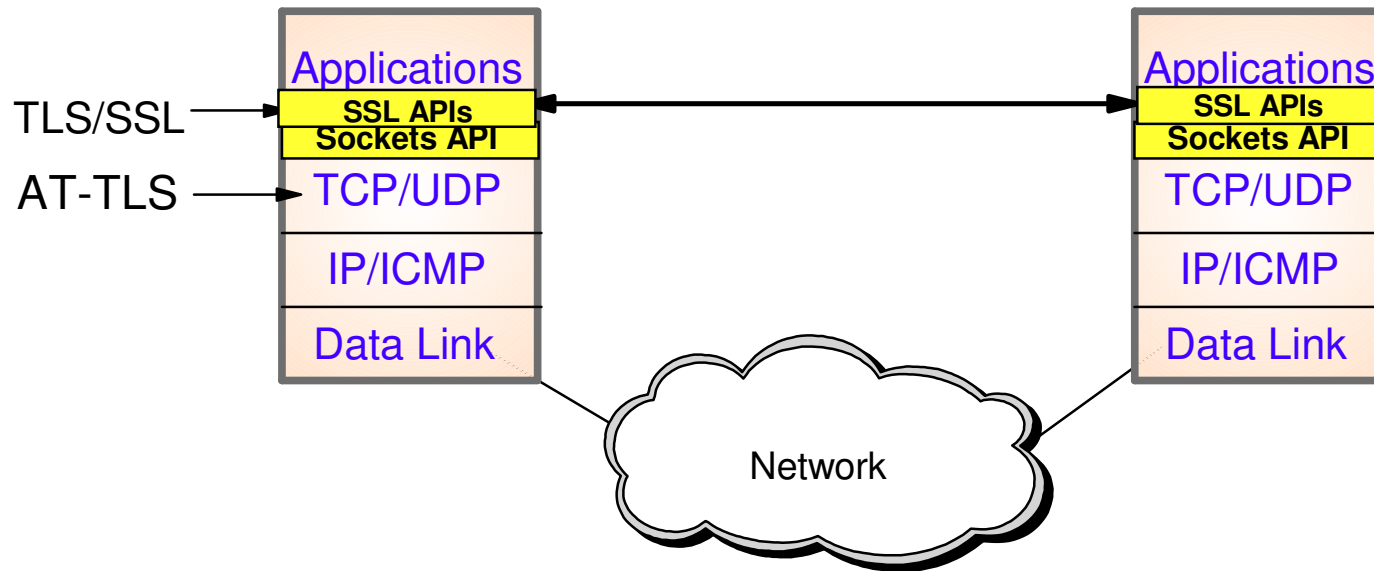
■ **Sysplex Wide Security Associations support for IKEv2**

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

z/OS Communications Server Network Security

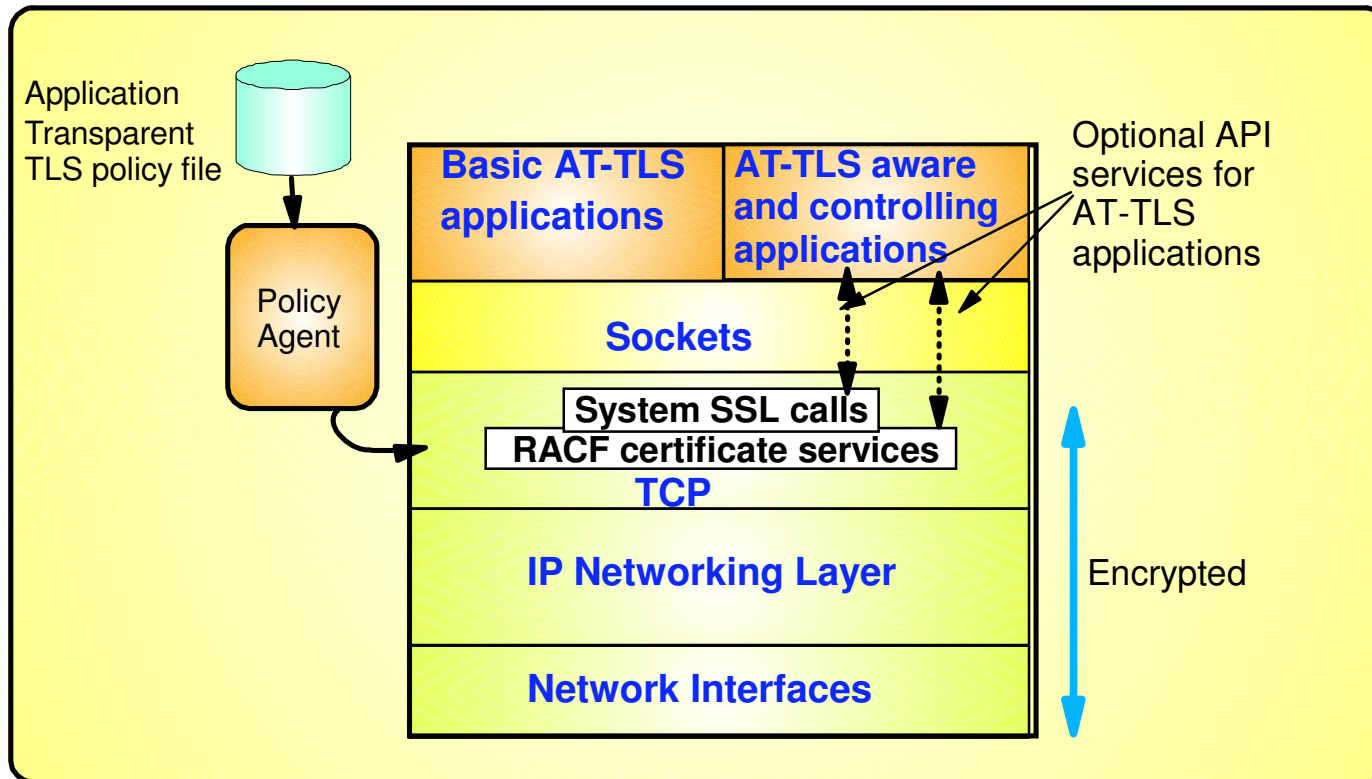
Application Transparent Transport Layer Security

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 (TCP only)
 - UDP, raw IP applications cannot be TLS enabled
- z/OS applications can be modified to support TLS using System SSL
 - ▶ System SSL part of z/OS Cryptographic Services element
- Application Transparent TLS (AT-TLS) lets you apply TLS protection through System SSL with zero or minimal application change

AT-TLS Overview



- **AT-TLS invokes System SSL TLS processing at the TCP layer for the application**
- **AT-TLS controlled through policy**
 - ▶ Installed through policy agent
 - ▶ Configured through Configuration Assistant GUI or by manual edit of policy files
- **Most applications require no change to use AT-TLS**
 - ▶ AT-TLS Basic applications
- **Applications can optionally exploit advanced features using 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

See session 10730 for more information

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.)

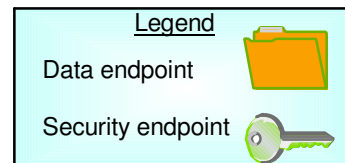
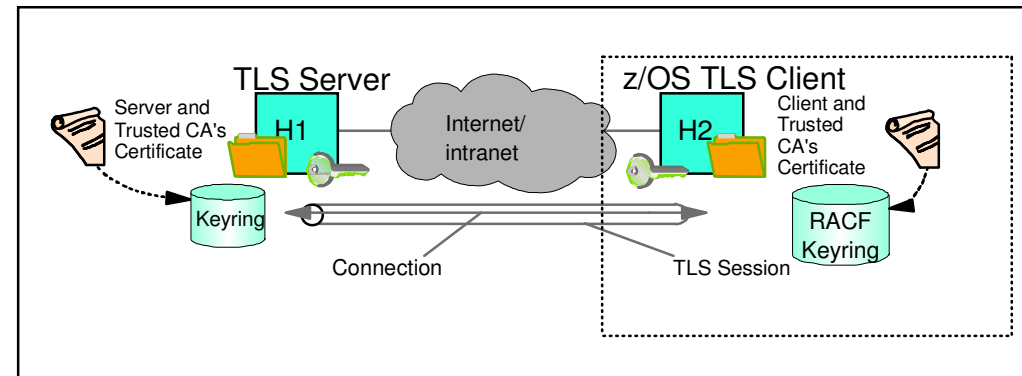
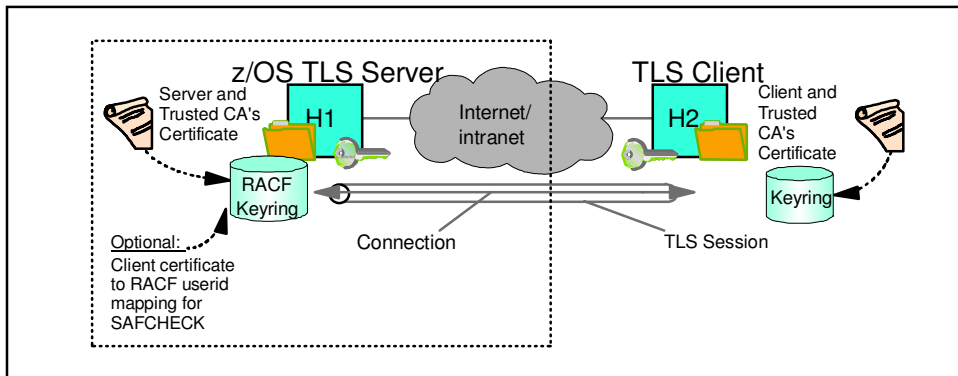
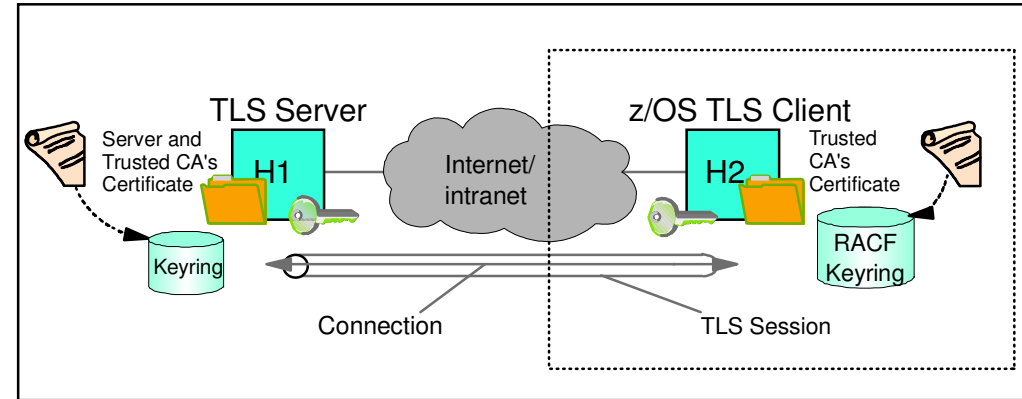
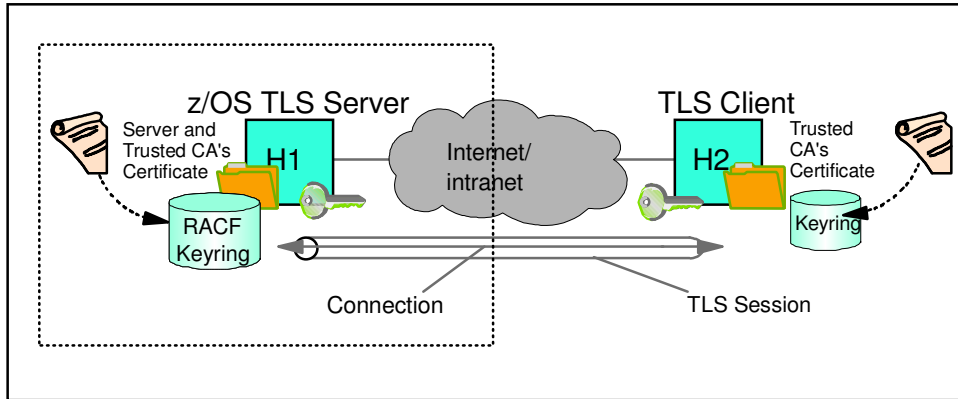
AT-TLS Policy Conditions

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



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

	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
Security endpoints	Device to device	Application to application
Type of authentication	Peer-to-peer	1)Server to client 2)Client to server (optional)
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 server
 - 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

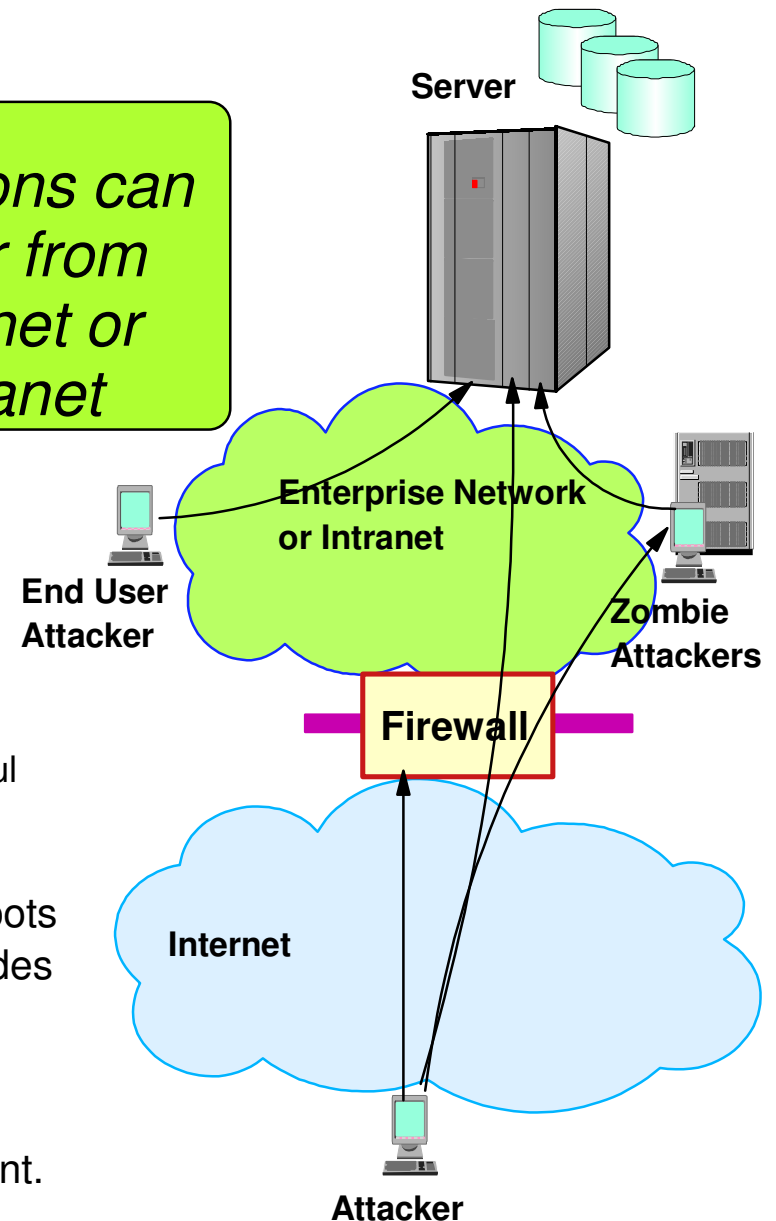
• Attacks can be deliberate or unintentional

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

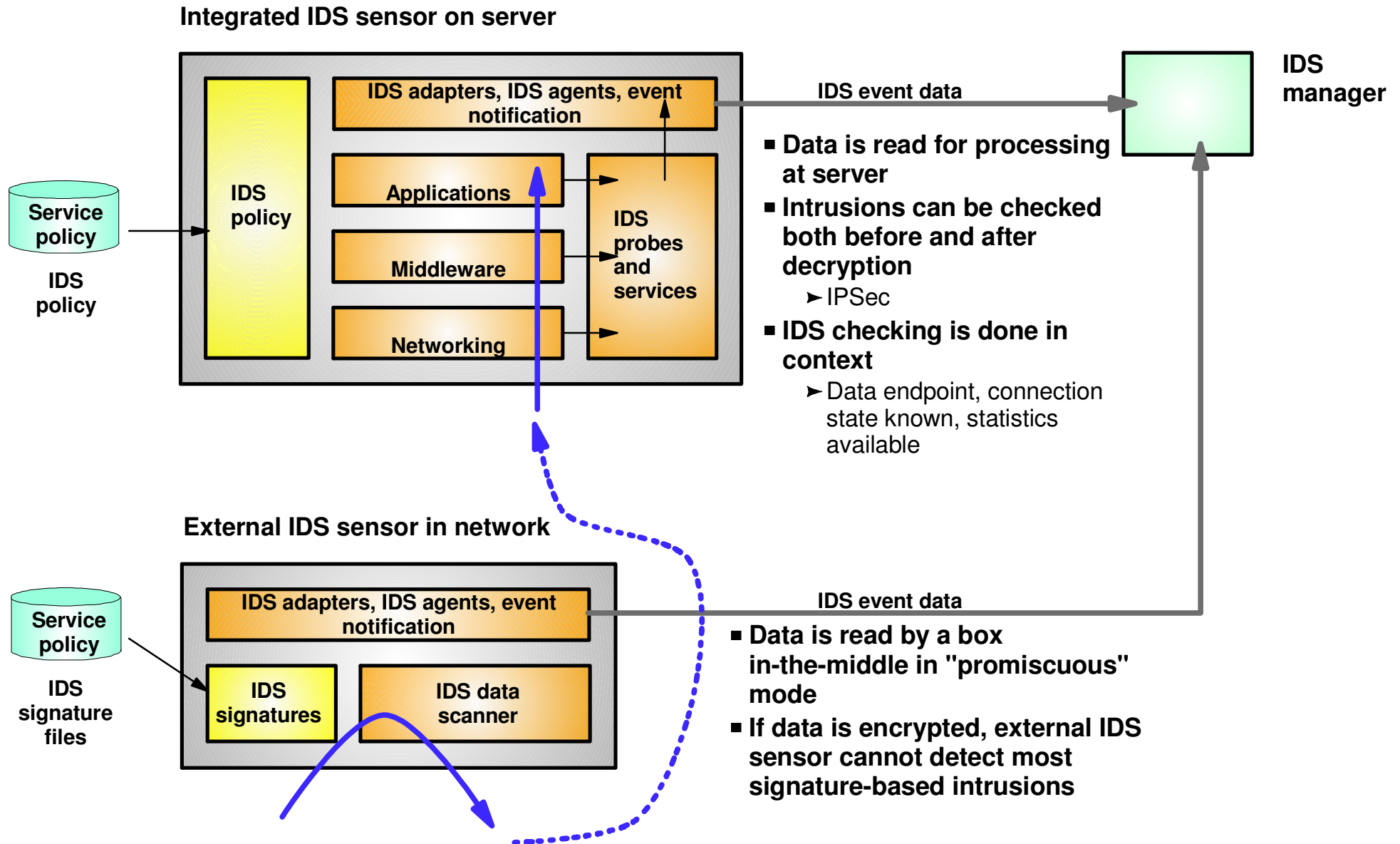
• Attacks can occur from Internet or intranet

- ▶ 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

Intrusions can occur from Internet or intranet

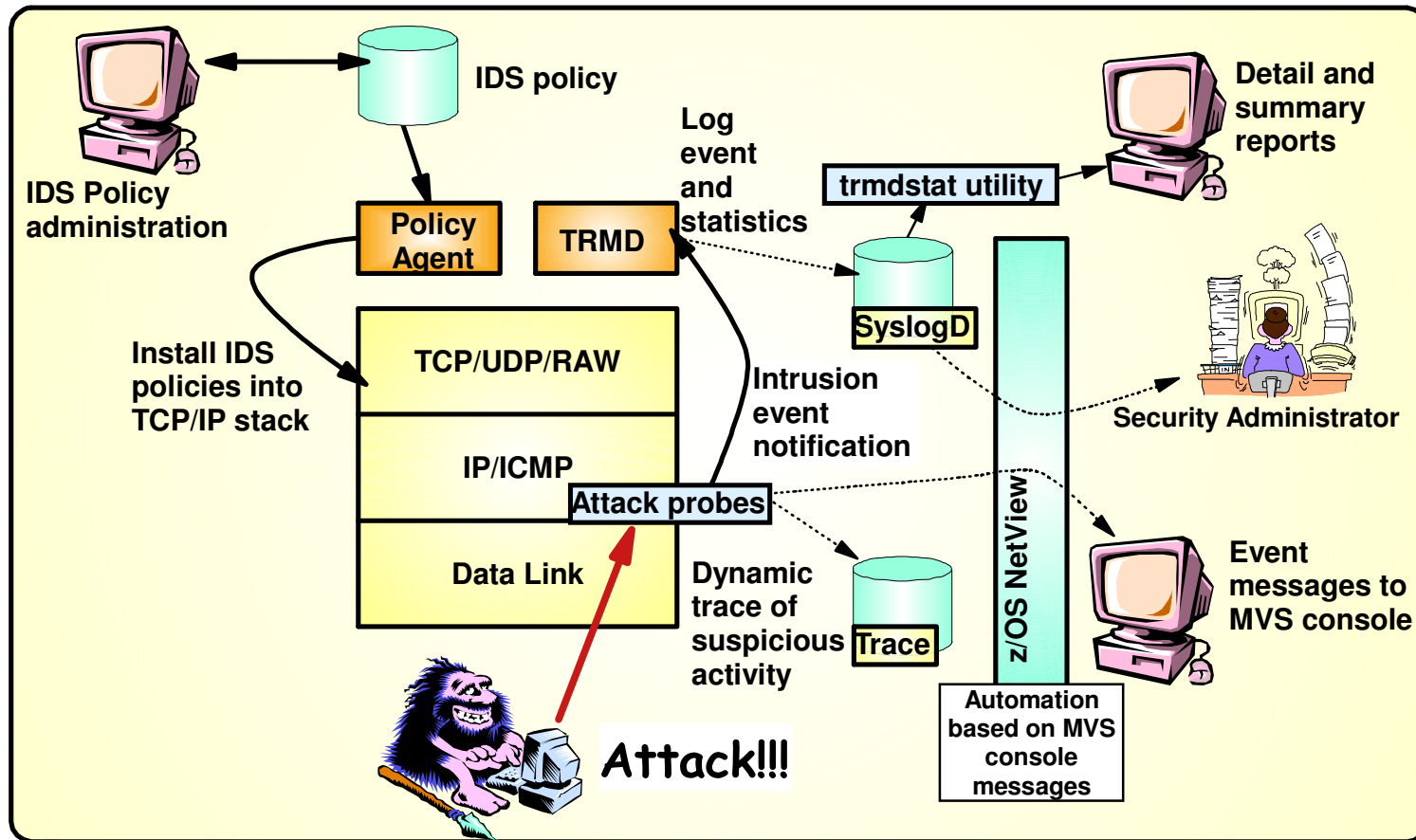


Integrated vs. External Intrusion Detection Concepts



Intrusion Detection Services Overview

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



Events detected

- Scans
- Attacks Against Stack
- Flooding

Defensive methods

- Packet discard
- Limit connections

Reporting

- Logging,
- Event messages to local console,
- IDS packet trace
- Notifications to Tivoli NetView

IDS Policy

- Samples provided with Configuration Assistant for z/OS Communications Server

z/OS IDS broadens intrusion detection coverage:

- Ability to evaluate inbound encrypted data - IDS applied after IPsec 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

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

See session 10829 for more information

Intrusion Event Types Supported

In V1R3 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 process when client connect to them should have a cap on the number of connections (FTP, otelnetd, etc.)

** = New attack types added in V1R13

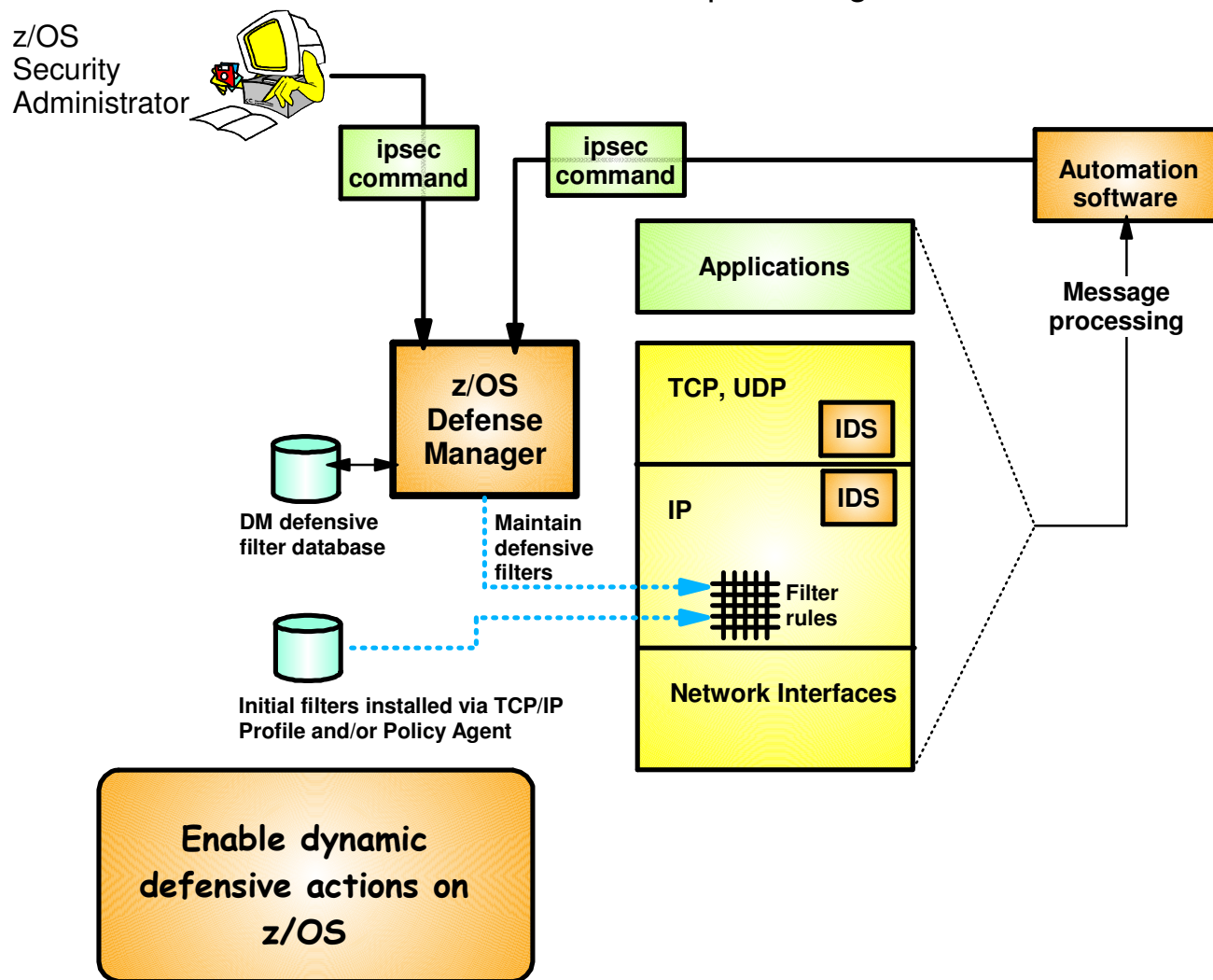
z/OS Defensive Filtering

- **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 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**

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
- Wrap up

Configuration Assistant for z/OS Communications Server



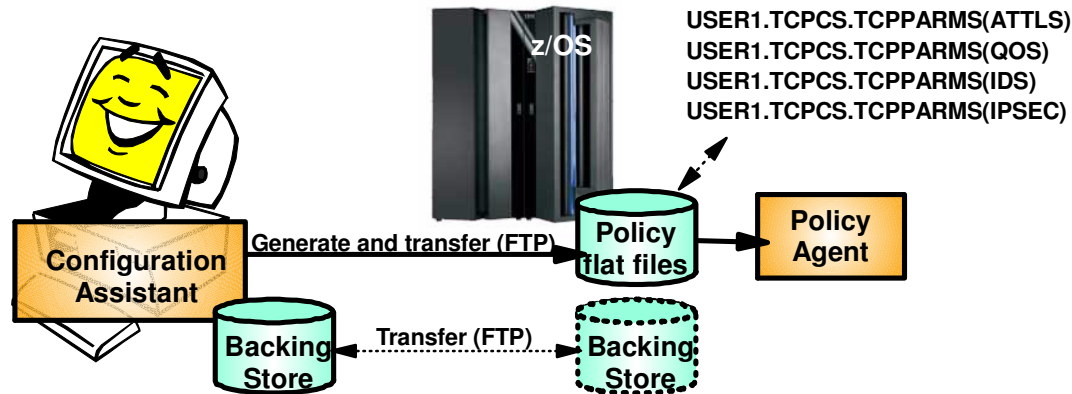
- **GUI-based approach to configuring multiple policy disciplines:**
 - ▶ IDS
 - ▶ AT-TLS
 - ▶ IPSec and IP filtering
 - ▶ QoS
 - ▶ Policy-based Routing (PBR)
- **Separate perspectives but consistent model for each discipline**
- **Focus on high level concepts vs. low level file syntax**
- **z/OSMF-based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

Download the Windows-based Configuration Assistant at: <http://tinyurl.com/cgoqsa>

Configuration Assistant for z/OSMF

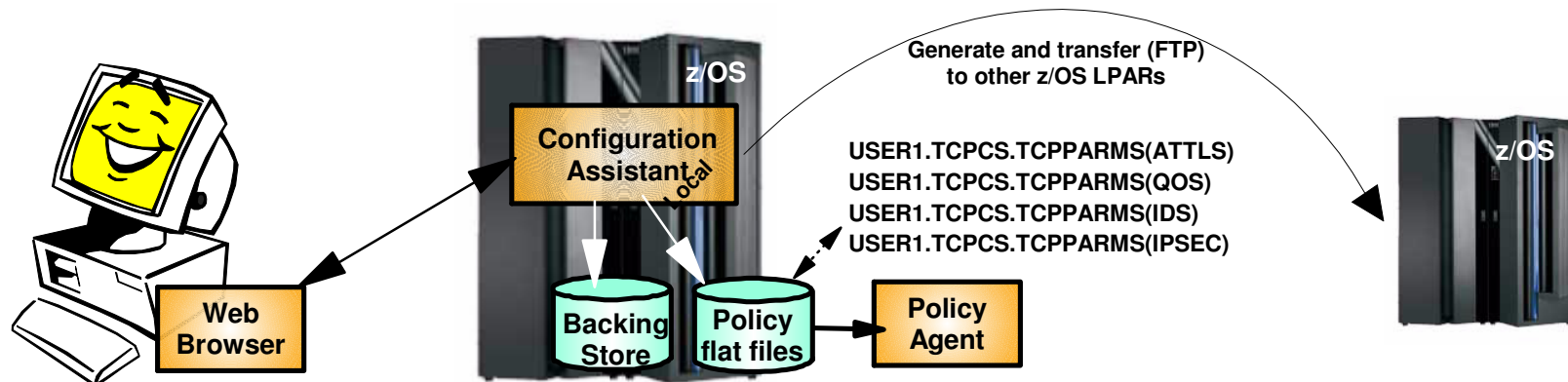
■ Originally, Configuration Assistant ran on Windows

- ▶ 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

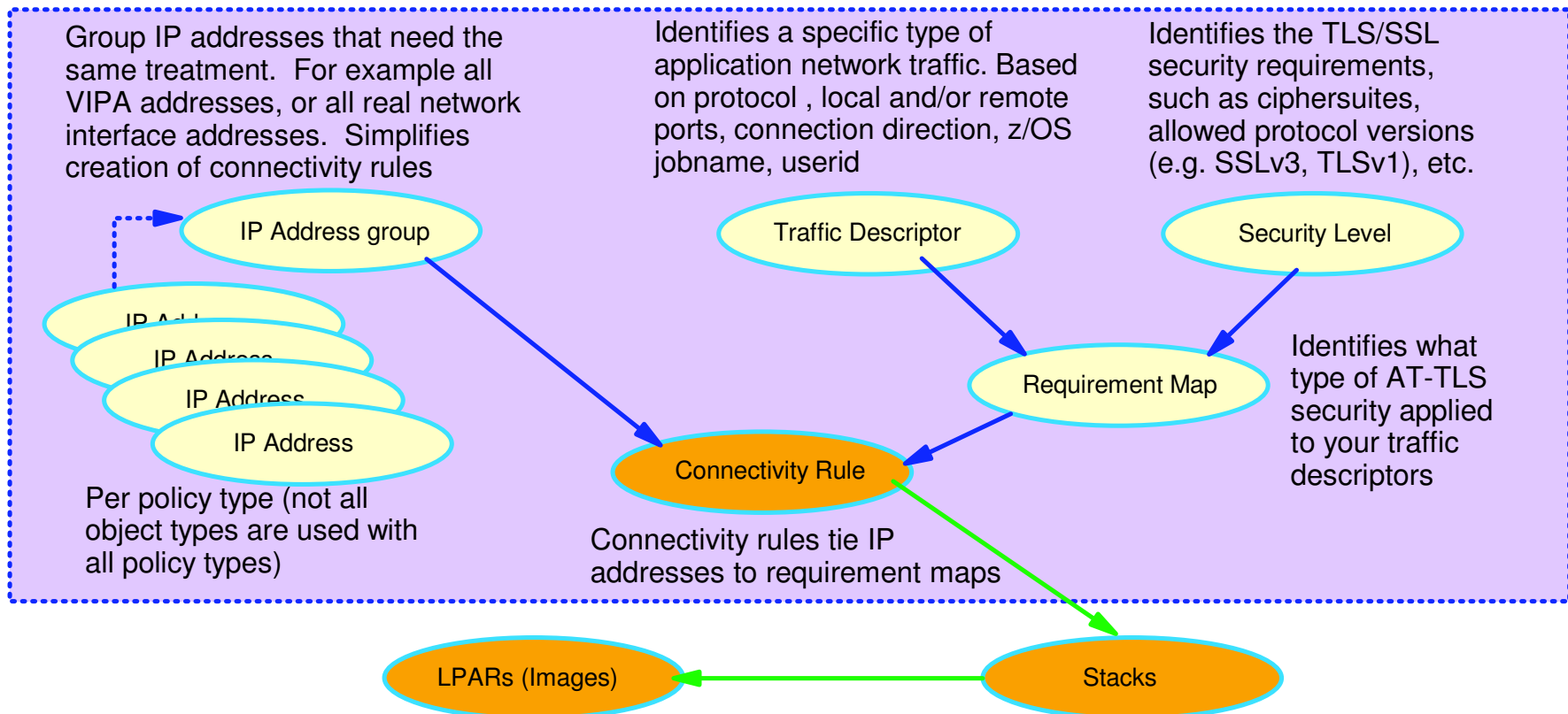


Configuration Assistant Policy Creation Approach

- 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 configured Requirement Map

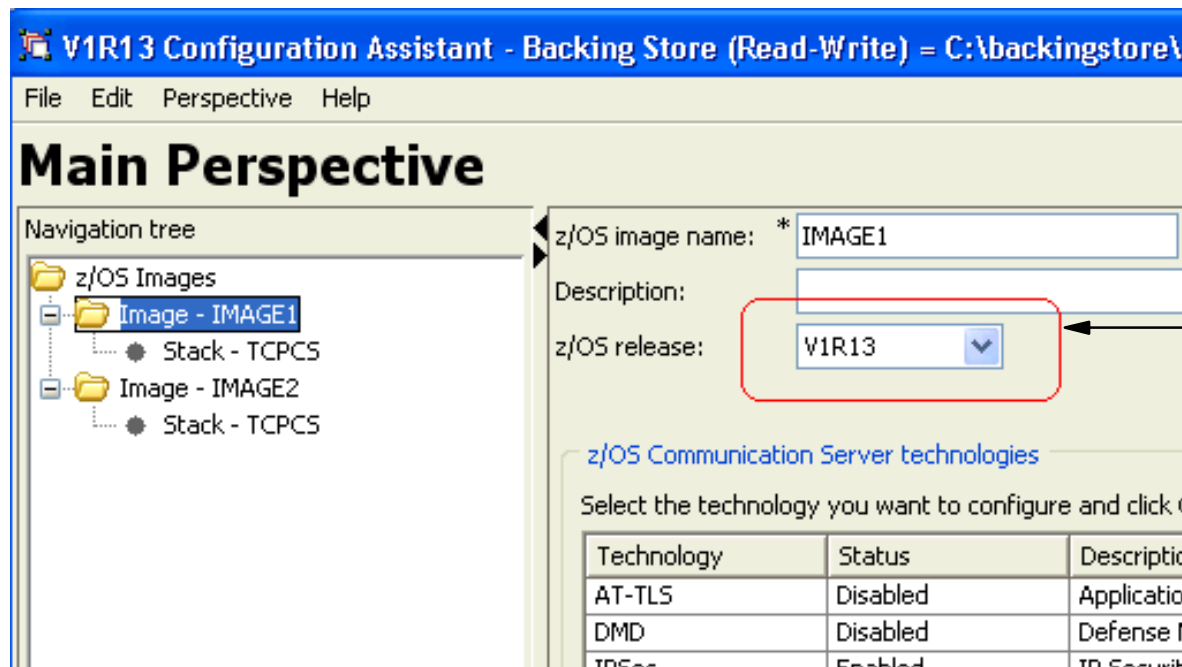
Policy Creation Optimizations

- **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.

Multiple Release Support

- Beginning in V1R13, Configuration Assistant makes it easier to manage a diverse configuration by supporting the configuration of multiple z/OS Communications Server releases.
 - You no longer have to maintain multiple installations of z/OSMF in order to manage multiple releases.
- In V1R13, a single Configuration Assistant concurrently supports both V1R13 and V1R12 configuration.



Can change release level at any time

Common Configuration for Multiple Stacks

- Beginning in V1R13, the Configuration Assistant supports common configuration of multiple stacks.
 - ▶ New reusable object called "rules".
 - Reusable rules are created a single time and assigned to TCP/IP stacks.
 - If a reusable rule needs to be updated, only a single rule needs to be modified and the changes are propagated to all stacks.
 - ▶ New variable names for local IP addresses and IKE identities
- Reusable rules can reference variable names for both local IP addresses and IKE identities, and these names can be assigned specific values for each stack.

Navigation tree

- IPSec
 - Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Address Groups
 - Requirement Maps
 - Rules
 - z/OS Images
 - Image - IMAGE1
 - Stack - TCPCS
 - Image - IMAGE2
 - Stack - TCPCS

Connectivity Rules Local Identity Stack Settings NSS Local Addresses IKE Symbols

TCP/IP stack name: * TCPCS

Description:

z/OS release: V1R12

Click the Add... button for each connectivity rule you want to add to this stack.

Local/Source	Remote/Destination	Requirement Map	Topology	Status	Name
%osa	8.8.8.8	CICS	Host to Host	Enabled	(R) ToBranchOffice
1.1.1.1	2.2.2.2	CICS	Host to Host	Enabled	(R) 0
1.2.3.4	9.9.9.9	CICS	Host to Gateway	Enabled	1
All_IPv	addresses	gw	Gateway to Host	Enabled	2
All_IPv	addresses	gw	Gateway to Gateway	Enabled	3
%osa	8.9.7.6	Filtering	Filtering - Host	Enabled	4
8.9.7.6	addresses	gw_fil	Filtering - Gateway	Enabled	5
8.2.5.2	addresses	gw_fil	Filtering - Either	Enabled	6
%subn		man	Host to Host	Enabled	7
All_IPv	addresses	CICS	Host to Host	Enabled	8

Context menu options: Add..., Modify..., Modify Wizard..., Copy..., Delete, Cut, Paste, Move Up, Move Down, View Details..., Enable Rule, Disable Rule, Make Reusable..., Make Stack Specific

Buttons: Modify Basics..., Delete, View Details..., Move Up, Health Check..., Modify Wizard..., Move Down

Main Perspective Apply Changes OK Cancel Help ?

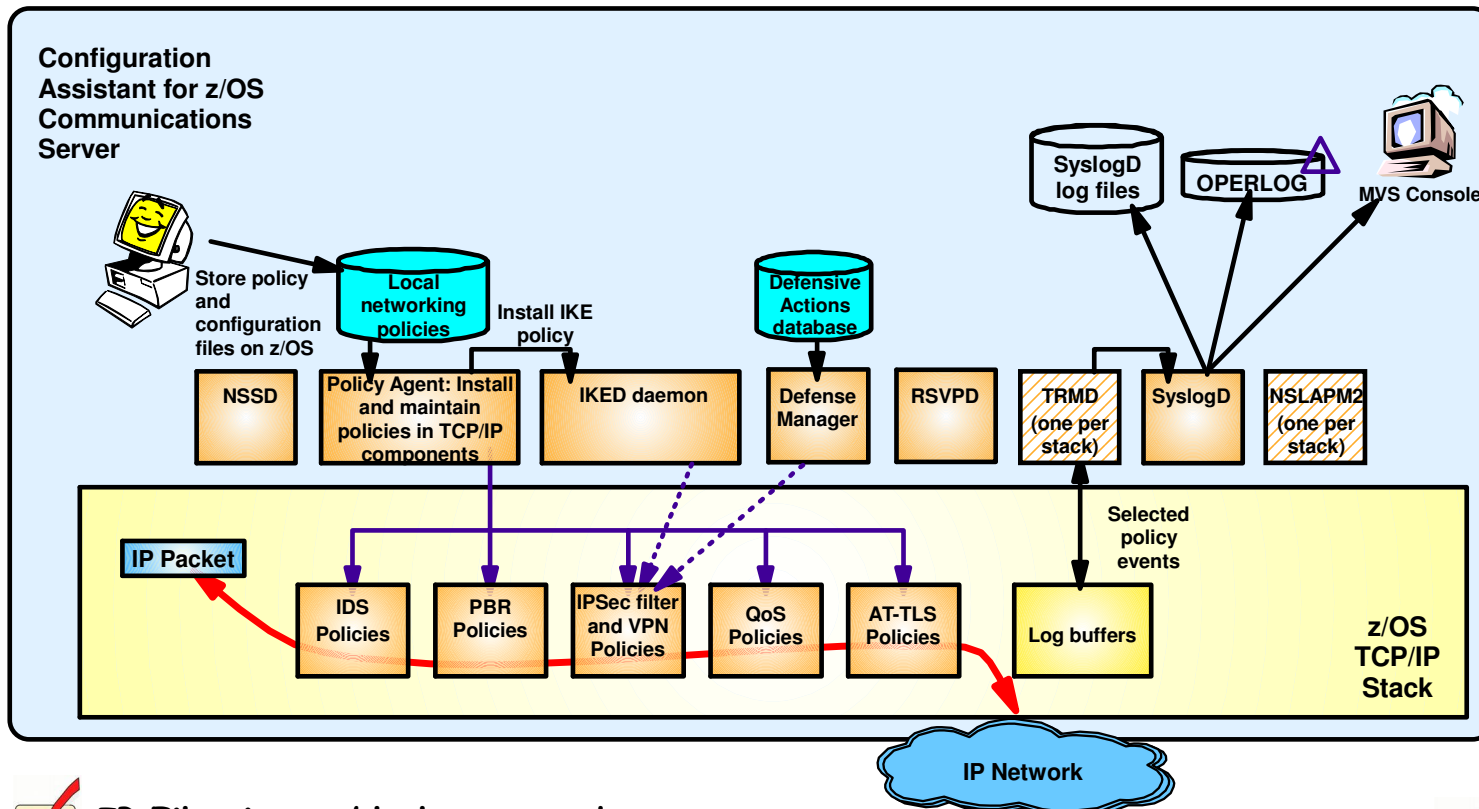
Discovery of TCP/IP stack IP addresses

- Beginning with V1R13, the Configuration Assistant supports the discovery of IP addresses for each stack.
 - ▶ Can help reduce manual entry of IP addresses
- The discover function is only available on z/OSMF.
 - ▶ Not available in the Windows-based Configuration Assistant
- Initiate the discovery process from the Local Addresses tab for a stack by choosing the Discover action

The screenshot shows the Configuration Assistant interface with the 'Local Addresses' tab selected. A context menu is open over the 'Local Addresses' tab, and the 'Discover...' option is highlighted. A red box highlights the 'Discover...' option, and a blue arrow points from the 'Discovered Information' column header in the table below to the 'Discover...' option in the menu.

Select	IP Address	Name	Discovered Information
<input type="radio"/>	2001:db8:10::92:1:1	VIPA6921	Type=Dynamic VIPA Define, Name=VIPA6921
<input type="radio"/>	2001:db8:10::91:1:1	VIPA6911	Type=Dynamic VIPA Define, Name=VIPA6911
<input type="radio"/>	10.71.0.0/16		Type=Dynamic VIPA Range
<input type="radio"/>	10.91.3.3		Type=Dynamic VIPA Backup, backup rank=100
<input type="radio"/>	10.93.1.1/24		Type=Dynamic VIPA Define
<input type="radio"/>	10.92.1.1/24		Type=Dynamic VIPA Define
<input type="radio"/>	10.91.1.1/24		Type=Dynamic VIPA Define
<input type="radio"/>	::14:0	LOOPBACK6	Type=Loopback, Name=LOOPBACK6
<input type="radio"/>	2001:db8::/64	MPC1IPV6	Type=MPC, Name=MPC1IPV6
<input type="radio"/>	2001:db8:172::16:2:1	QDIO6201	Type=OSAD, Name=QDIO6201
<input type="radio"/>	2001:db8:172::16:1:1	QDIO6101	Type=OSAD, Name=QDIO6101

Policy-Based Networking Componentry



- ▶ Many components to manage and operate
 - Some initial setup cost
 - Lots of valuable function!
- ▶ V1R11 simplifies overall setup and operation of networking policy infrastructure, making it easier and less costly to 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

Configuration Assistant Policy Installation Simplification

Configuration Assistant now generates...

- ▶ configuration files
- ▶ started task JCL procedures
- ▶ RACF directives

...for each of the relevant daemons and servers (Pagent, IKED, TRMD, Syslogd, etc.) as required by the configured policy.

▶ New dialogs walk the user through each of the required setup tasks in the proper order. These dialogs are available for each configured feature.

▶ All generated configuration material can be installed from the setup tasks dialogs.

The screenshot displays the IBM Help System interface. The main window shows the title "RACF Directives for SYSLOGD startup" and a note: "You must authorize the Syslog daemon to access appropriate system resources." Below this, there is a "NOTE" section and a "Before you begin" section with a numbered list: "1. The sample setu daemon applica occurrences wh". An "Install Files to Remote Host" dialog box is open in the foreground, showing the "Install file:" field with the path "/etc/cfgasst/v1r11/MVSPROD/rsyslogd". The "FTP login information" section includes fields for "Host name:" (MVSPROD), "Port number:" (21), "User ID:" (adm0034), and "Password:" (*****). There is a "Save password" checkbox which is checked, and a "Use SSL" checkbox which is unchecked. The "Data transfer mode" section has radio buttons for "Default" (selected), "Passive", and "Active". At the bottom of the dialog are "Go", "Close", "View FTP Log", and "Help" buttons. In the background, a "Task: RACF Directiv" dialog is partially visible, with "Instructions" and "Install File..." buttons circled in red. A "Task Details..." button is also circled in red in the bottom left of the background dialog. The IBM Help System search bar and navigation icons are visible at the top of the main window.

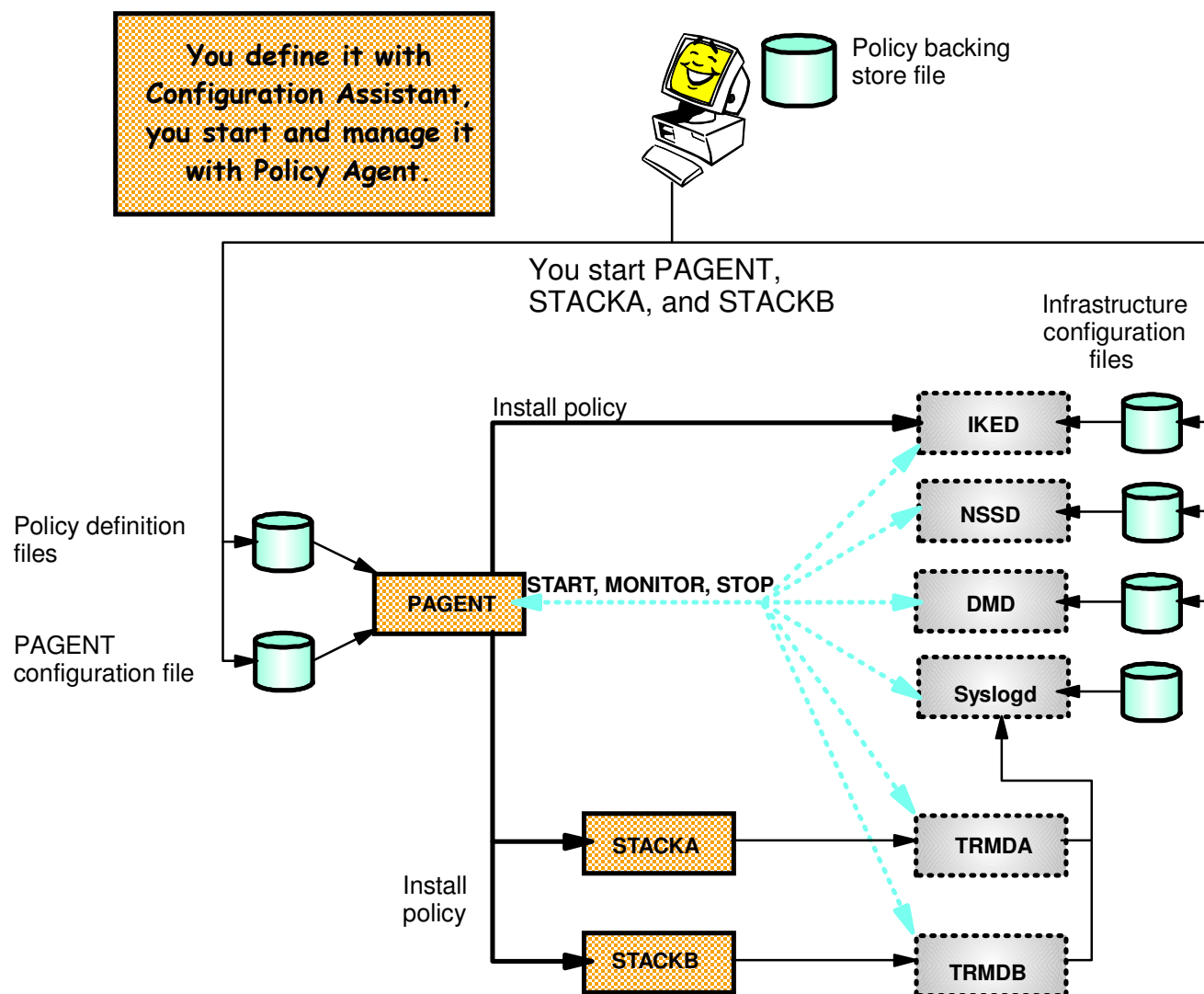
Infrastructure Management Overview

- Prior to z/OS V1R11, the various policy infrastructure components are independently managed:

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

- z/OS V1R11, Policy Agent is enhanced to start, stop, and monitor most policy infrastructure components

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

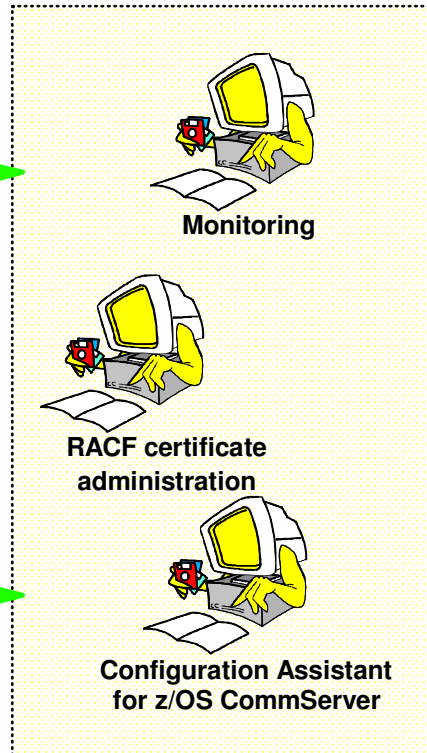
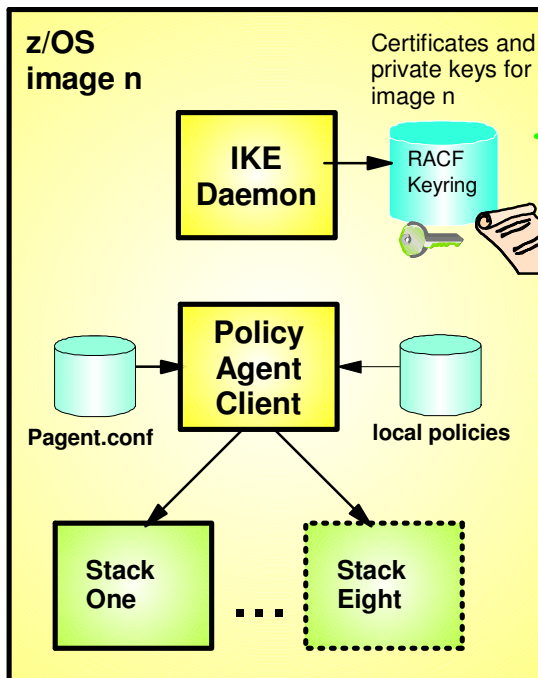
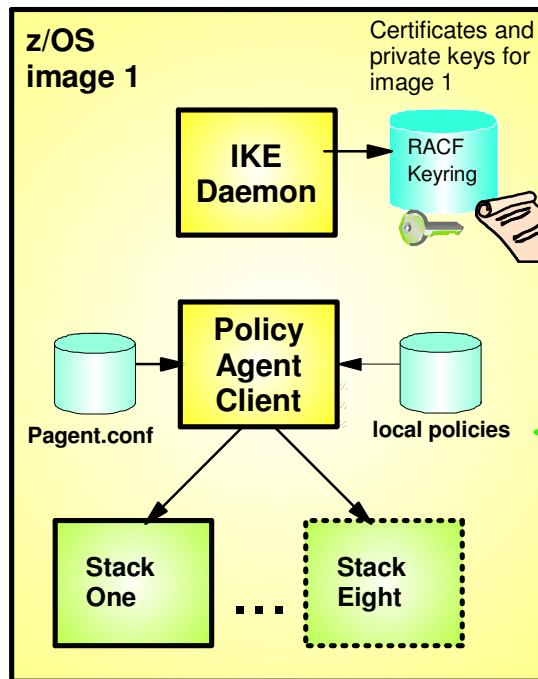


Agenda

z/OS Communications Server Network Security

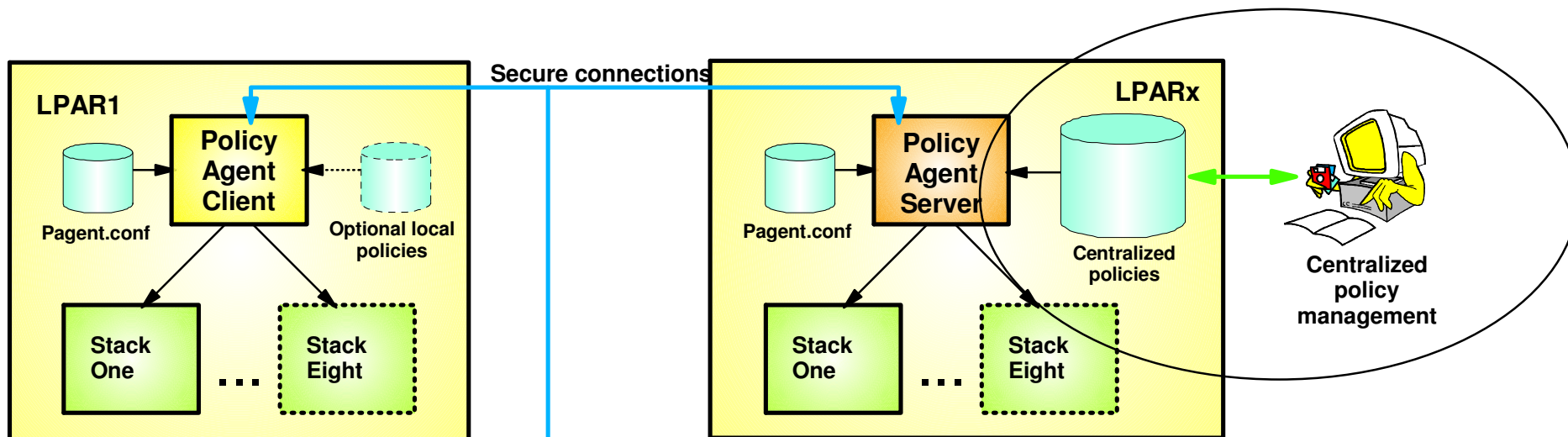
- Overview
 - ▶ Roles and objectives
 - ▶ Deployment trends and requirements
- Policy-based Network Security
 - ▶ IP security (IP packet filtering and IPSec)
 - ▶ Application Transparent TLS
 - ▶ Intrusion Detection Services
- Configuring Policy-based Network Security
 - ▶ Configuration Assistant for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

Local Network Security Administration



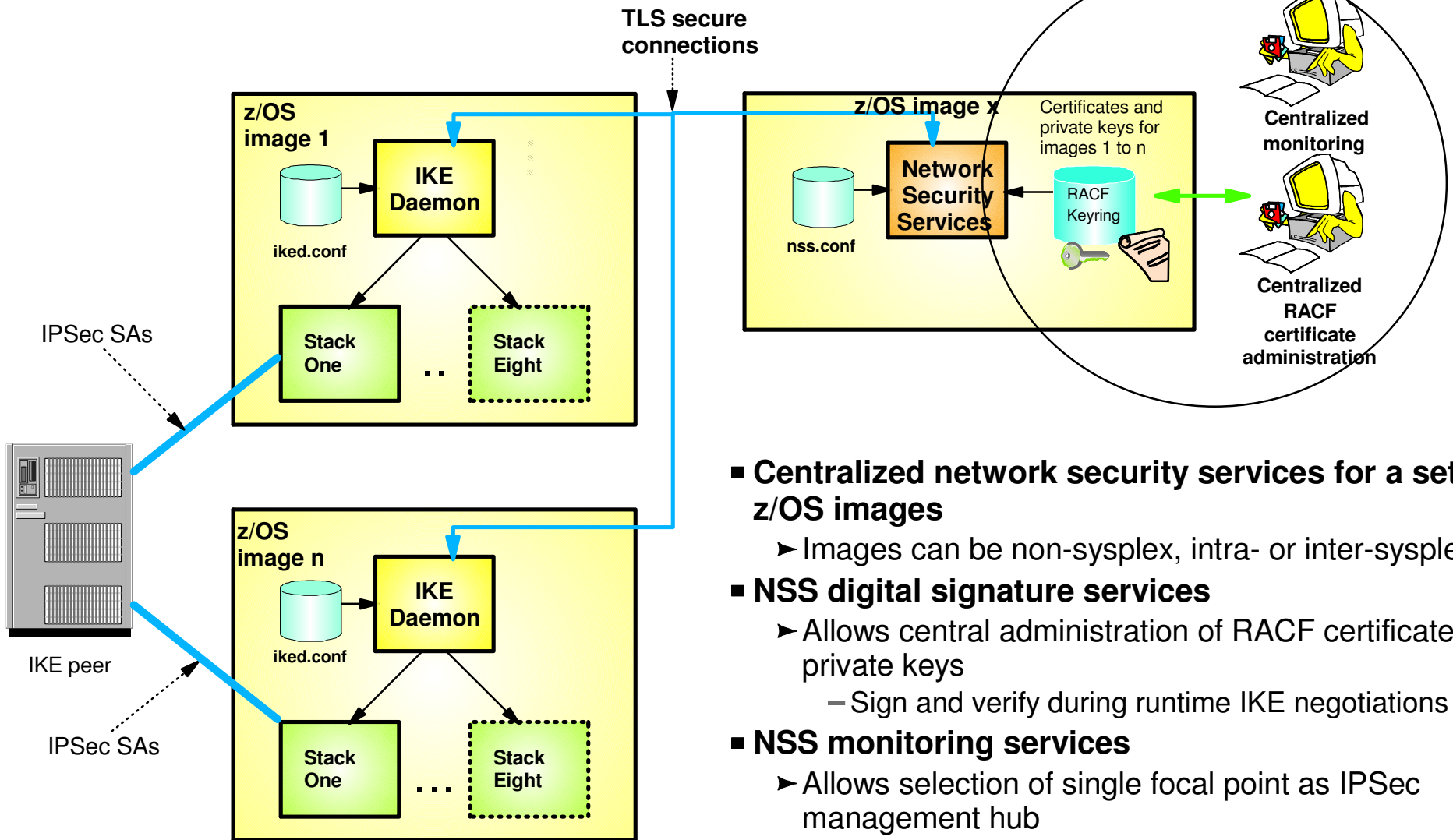
- **Each z/OS system locally administered**
 - ▶ RACF certificate administration
 - ▶ Policy configuration
 - ▶ Monitoring
- **Connectivity required between administration and each managed platform**
 - ▶ Monitoring application has advance knowledge of each managed node
 - ▶ Coordination required to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

Centralized Network Policy Management



- **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



- **Centralized network security services for a set of z/OS images**

- ▶ Images can be non-sysplex, intra- or inter-sysplex

- **NSS digital signature services**

- ▶ Allows central administration of RACF certificates and private keys
 - Sign and verify during runtime IKE negotiations

- **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 role in z/OS V1R12

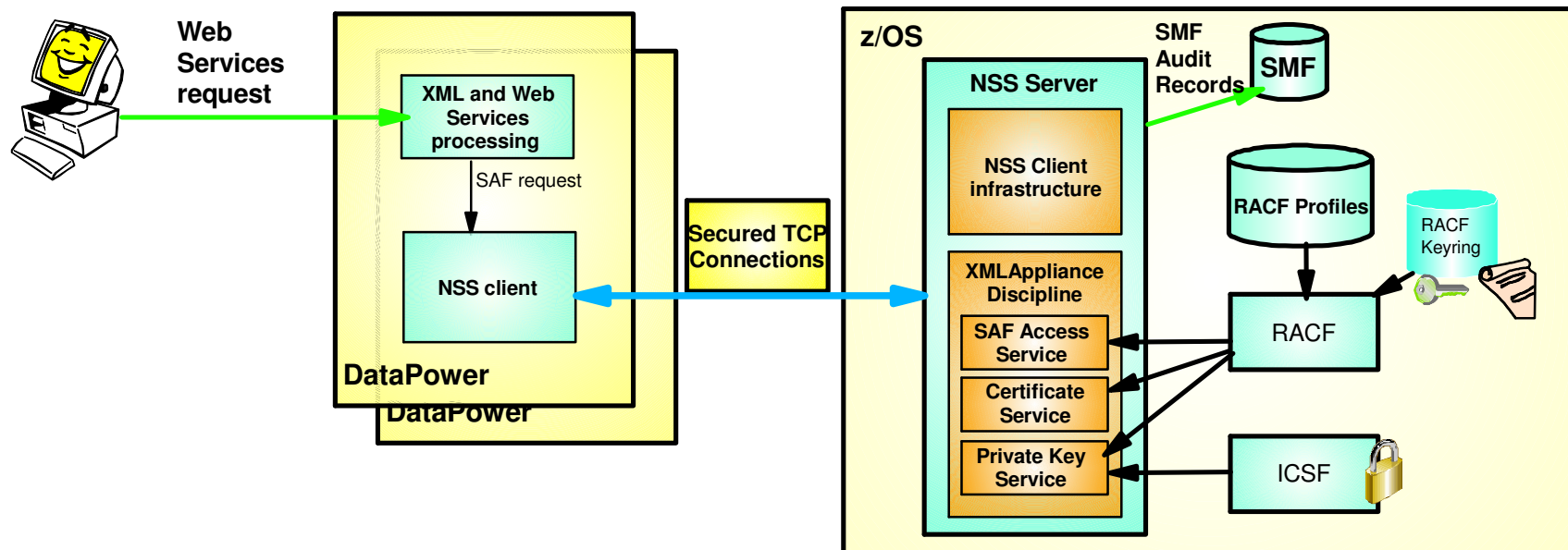
- NSS is required for z/OS V1R12 advanced certificate support
 - ▶ Certificate Revocation List
 - ▶ Certificate Trust Chain
- NSS is required for ALL IKEv2 certificate services

Extending NSS - Integrating DataPower with z/OS Security

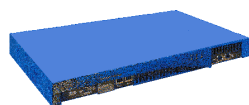
WebSphere DataPower SOA Appliances:

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

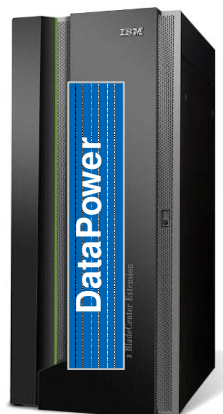
Offloading CPU-intensive XML processing - without losing centralized security control



DataPower Appliance (logical integration)



DataPower XI50z Integrated Blade (physical integration)



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

Agenda

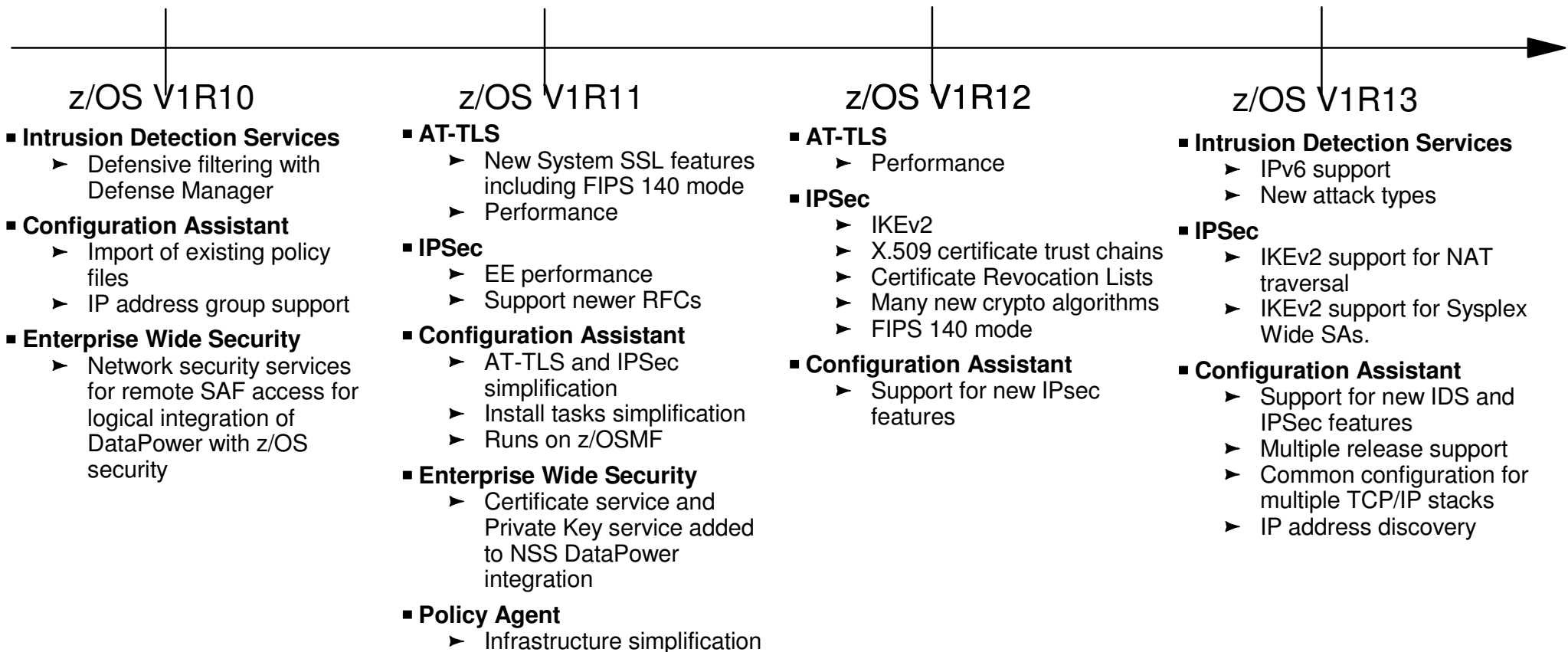
z/OS Communications Server Network Security

- 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
- **Wrap up**



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