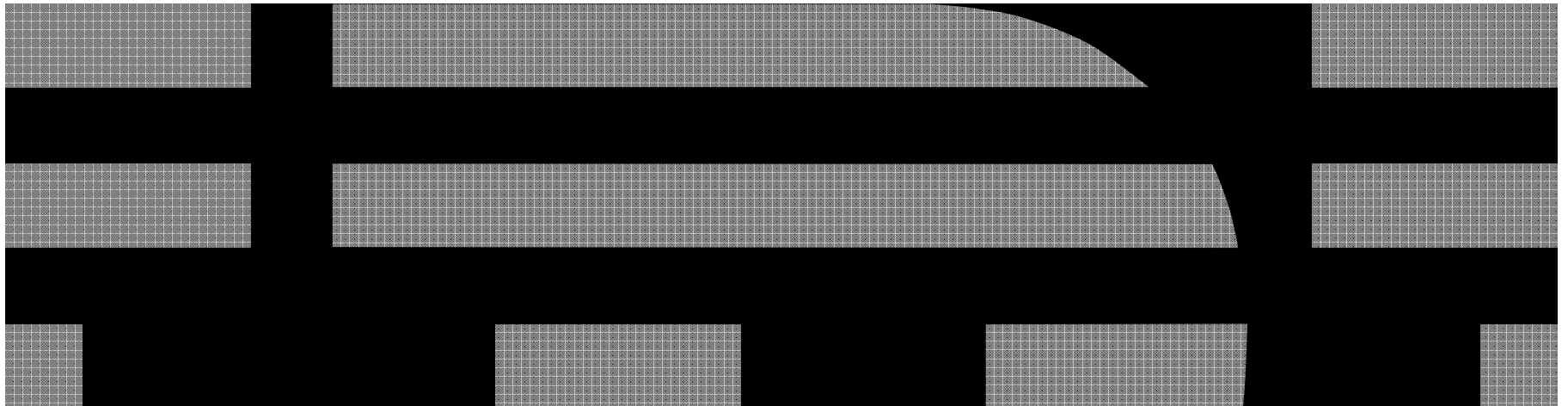Thomas Cosenza

tcosenza@us.ibm.com

IBM

FD6:
Section 4: Communication Server Security

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 regist⦙ trademarks of their ⦙ respective compani⦙

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 countrie⦙
- 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 ⦙ 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 ⦙ 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 th⦙ 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⦙ 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 s⦙ 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 produc⦙
- 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
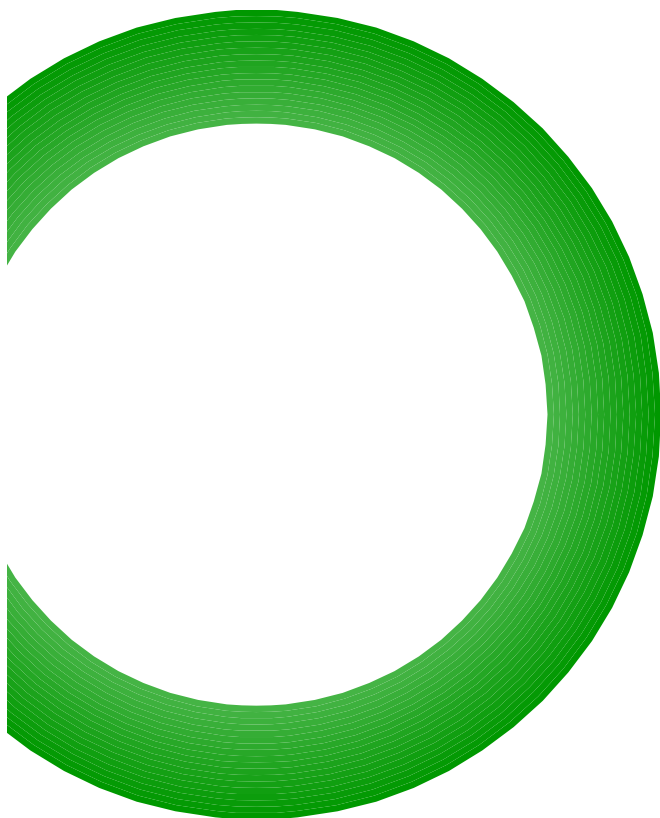
Deployment Trends and Requirements

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 pus into the endpoints, either because more security is required or because the endpoint is the only place t 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 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.

Application layer

- SAF protection
- Application specific
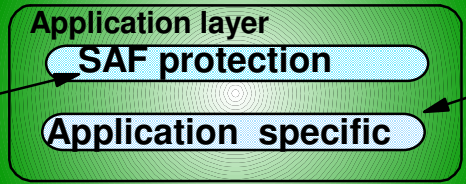
Protect data in the network

Examples of application protocols with built-in security extensions are SNMPv3 and OSPF.
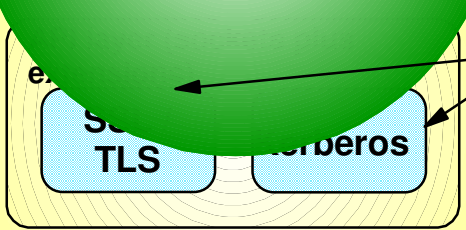
Both Kerberos and SSL/TLS are located a extensions to the sockets APIs and applica have to be modified to make use of these s functions. Both SSL/TLS and Kerberos are connection-based and only applicable to T (stream sockets) applications, not UDP.

SSL/TLS   Kerberos

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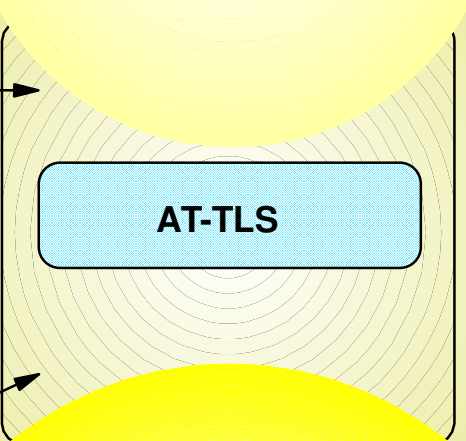
AT-TLS

AT-TLS is TCP/IP stack service that provid SSL/TLS services at the TCP transport lay is transparent to upper-layer protocols. It is avaliable to TCP applications in all progran 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.
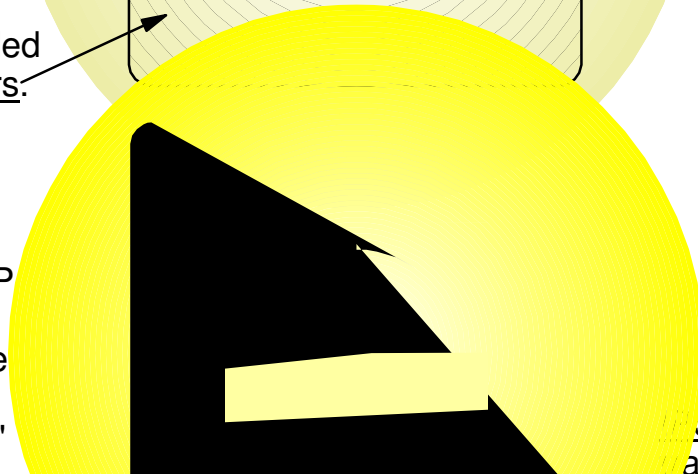
IP packet filtering blocks out all IP traffic that this systems doesn't specifically permit. These can be configured or can be applied dynamically as "defensive filters."

Sec resides at the networking layer and i ansparent to upper-layer protocols, includ

Agenda

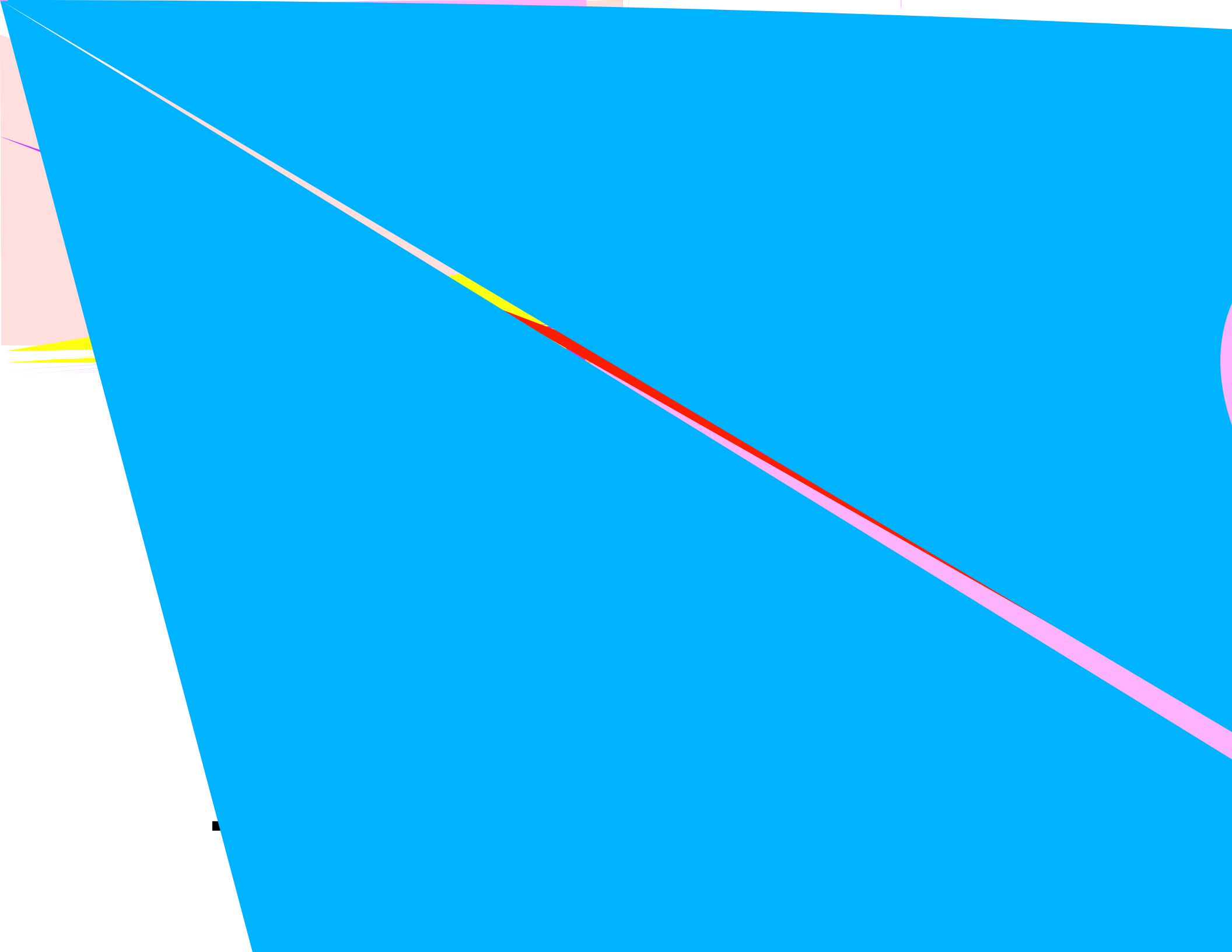z/OS Communications Server Network Security

- 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
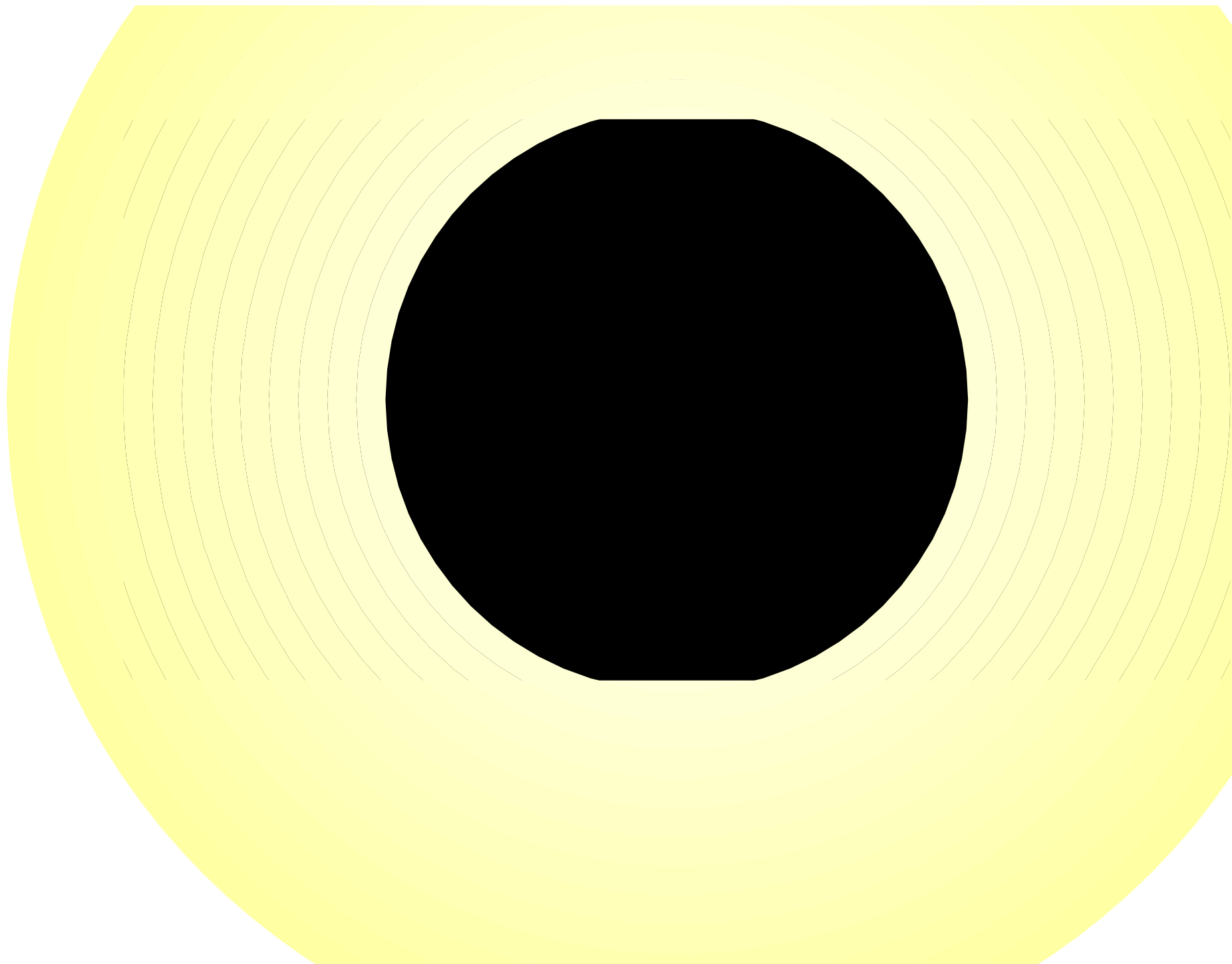
z/OS Communications Server Network Security

IP Security

- IP packet filtering

- IPSec

z/OS Communications Server IP Security Featu

- **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 m information

- **zIIP Assisted IPSec**
  - ➤ Moves most IPSec processing from general purpose processors to zIIPs

- **IP Security Monitoring Interface**
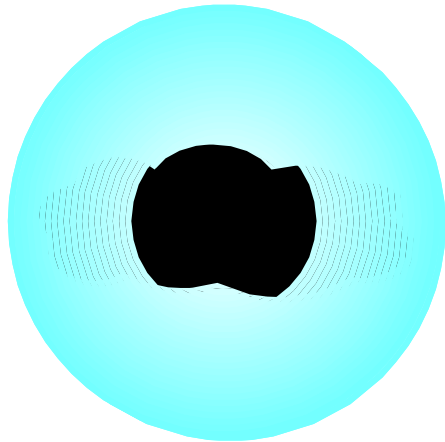 - ➤ IBM Tivoli OMEGAMON XE for Mainframe Networks uses this interface

- **Support for latest IPSec RFCs**
  - ➤ RFCs 4301-4305, 4307-4308
  - ➤ RFC 4306 (IKEv2)

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

Basics of IP Packet Filtering

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
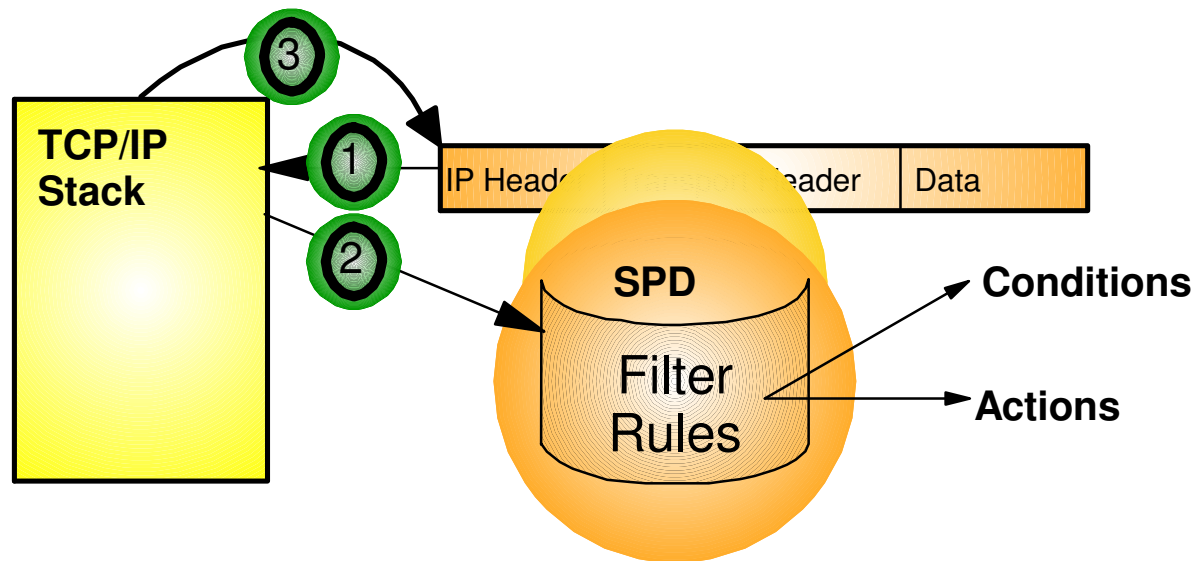
■ Filter rules are searched in the order they were configured

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 packe	
Destination port	For TCP and UDP, the destination port in the transport header of p	
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 packe	
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 ho otherwise it is routed	
Link security class	A virtual class that allow you to group interfaces with similar securit requirements. Non-VIPA addresses can be assigned a security cla Packets inherit the security class of the interface over which packet sent/received.	
Time condition		

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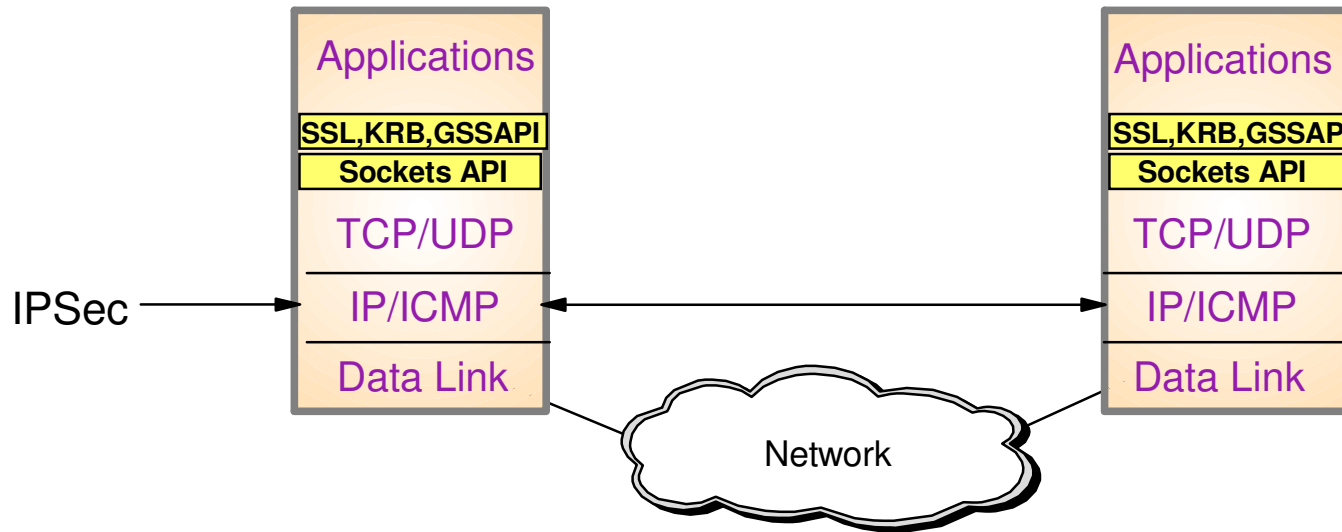
- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
  - IPSec security protocols
    - **Authentication Header (AH)** - provides data authentication / integrity
    - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional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

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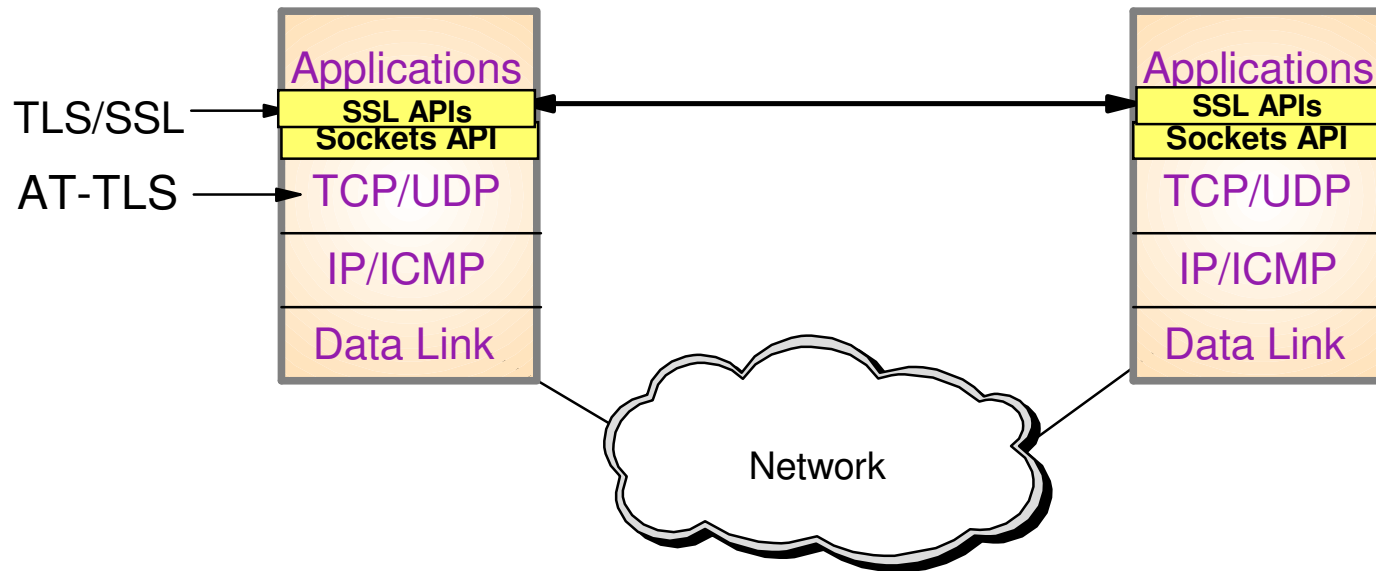 - ➤ IKEv1 support for Sysplex Wide Security Associations available in previous releases

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) whi defined by the IETF for unreliable transports
- On z/OS, System SSL (a component of z/OS Cryptographic Services) prov an API library for TLS-enabling your C and C++ applications
- Java Secure Sockets Extension (JSSE) provides libraries to enable TLS su for Java applications
- However, there is an easier way

- A
- A

- M

- A

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	• 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
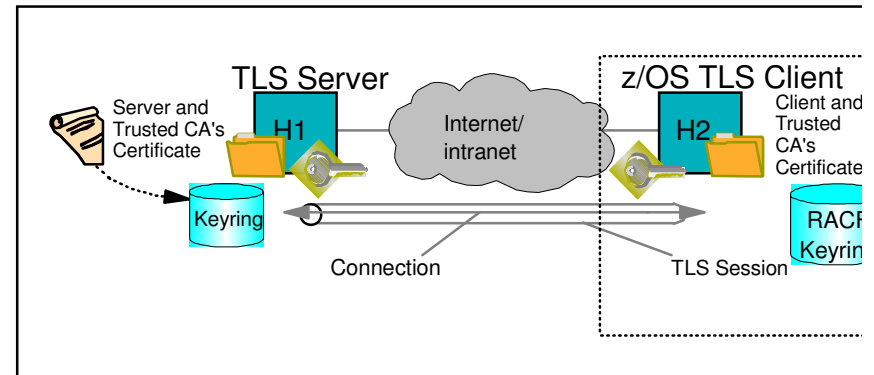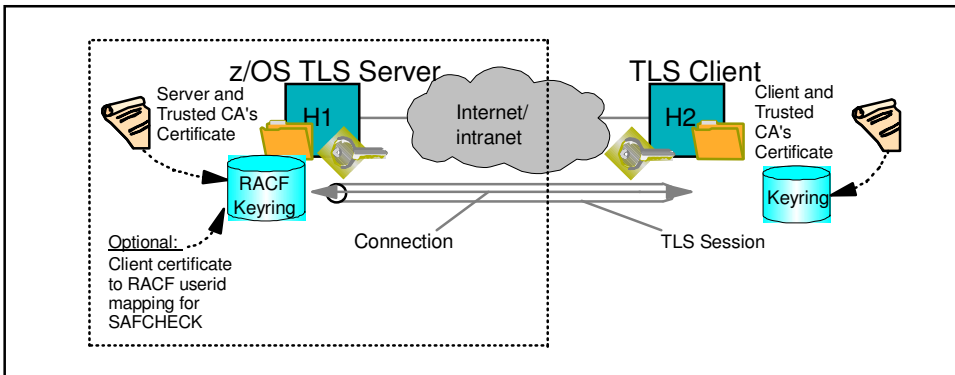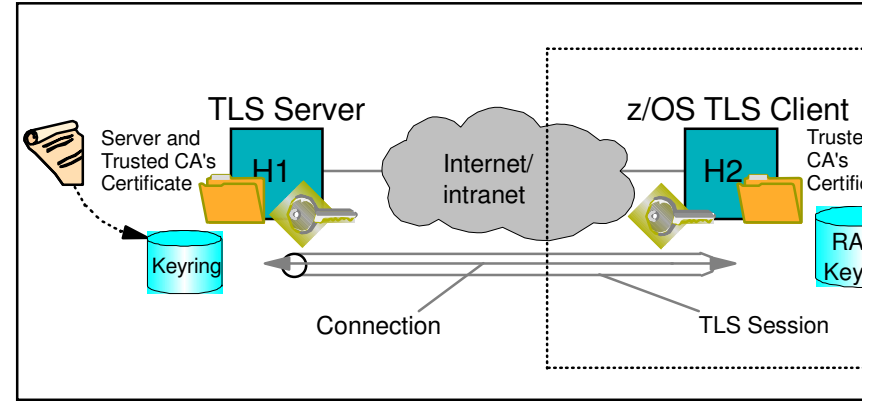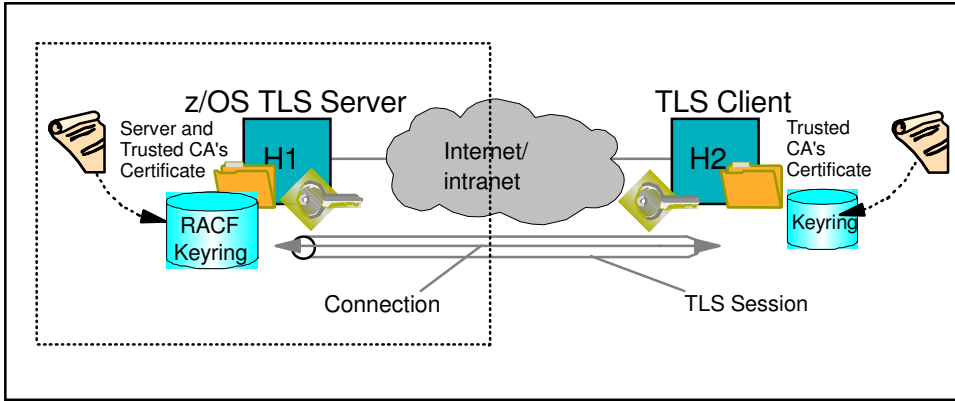
Some Applications That Use AT-TLS

- 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

z/OS Communcations Server IDS, provides integrated intrusion detection and prevention for the networki
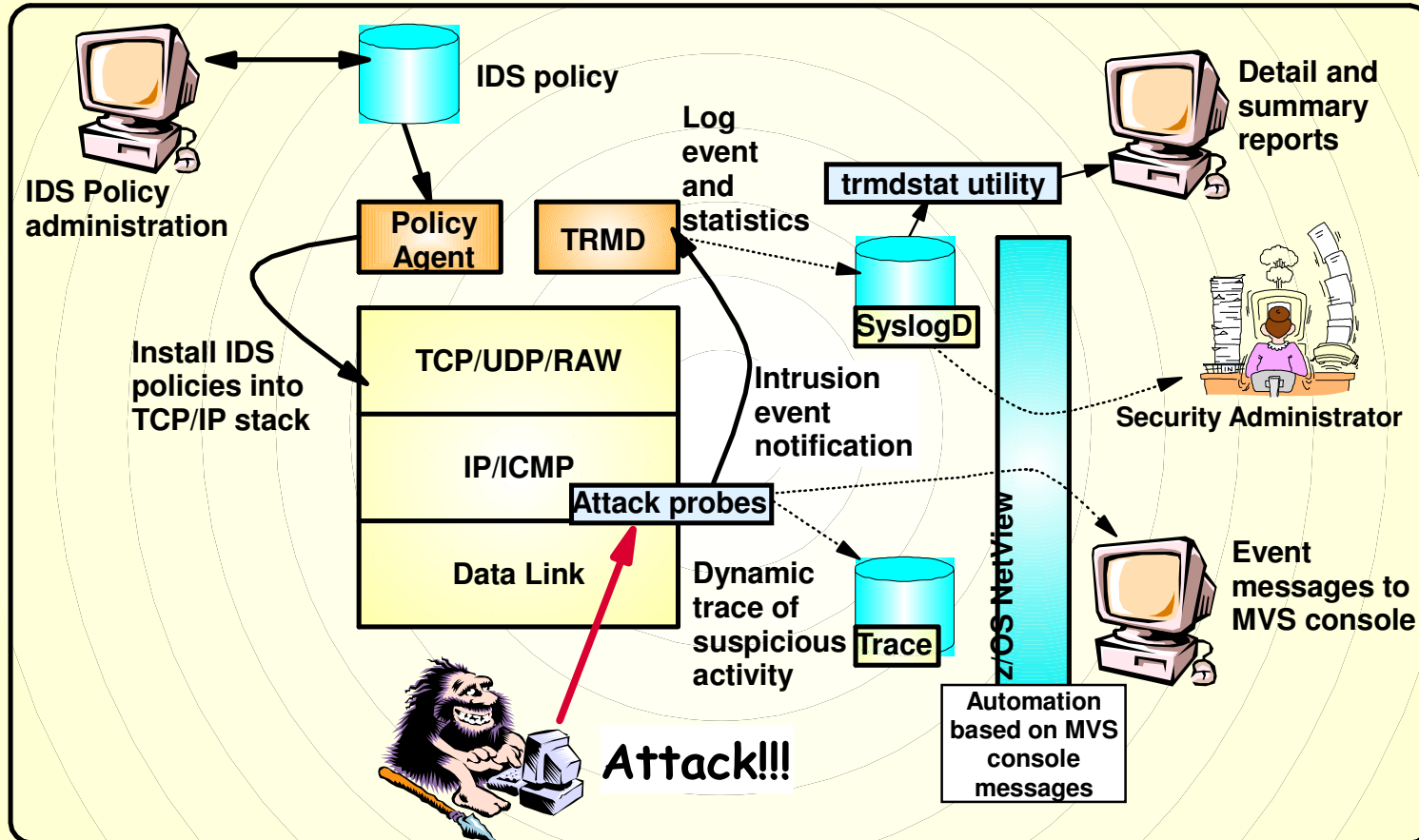
ents detected
- Scans
  Attacks Aga
  Stack
  Flooding
  ve method
  acket disc
  mit conne
  g
  ogging,
  vent mess
  cal consol
  DS packet
  Notifications
  Tivoli NetVie
  olicy
  Samples pr
  with Configu
  Assistant fo
  Communica
  Server

Integrated Intru
Detection Servi
under policy co
to identify, alert
document susp

internal
thre

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
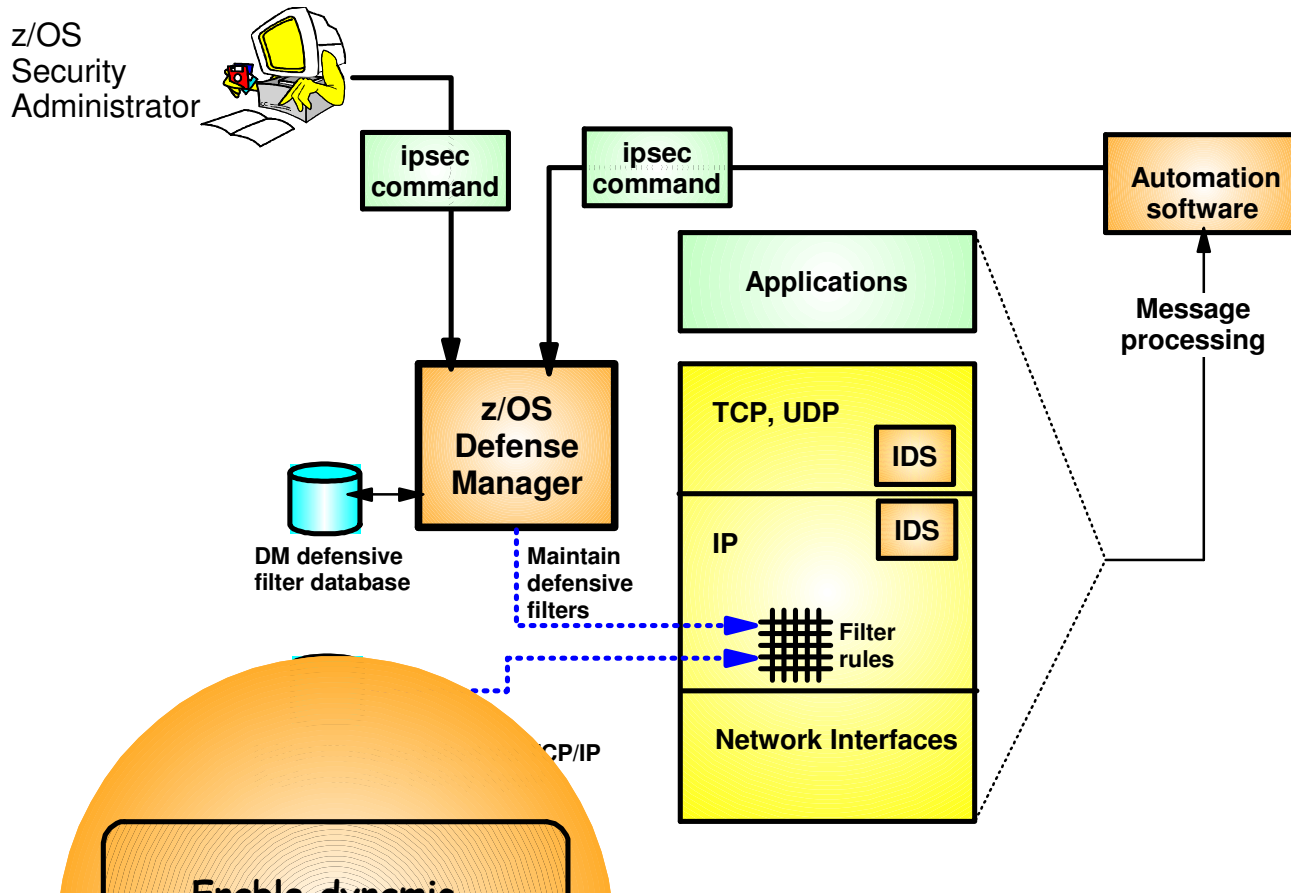- **Defensive filtering is an extension to IDS capabilities**
  - ➤ Adds additional defensive actions to protect against attacks

z/OS
Security
Administrator

| ipsec command | | ipsec command | | Automation software |

Applications

Message processing

z/OS Defense Manager

DM defensive filter database

Maintain defensive filters

TCP, UDP

IDS

IP

IDS

Filter rules

Network Interfaces

CP/IP

Enable dynamic

- **Requires minimal IP Secu configuration to enable IP packet filtering function**
  - ➤ Uses ipsec command to c and display defensive filte
- **Defense Manager**
  - ➤ Manages installed defens filters in the TCP/IP stack
  - ➤ Maintains record of defens filters on DASD for availab case of DM restart or stac start/restart
- **Defensive filter scope may**
  - ➤ Global - all stacks on the where DM runs
  - ➤ Local - apply to a specific
- **Defensive filter are installe "in front of" configured/de 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

- **GUI-based approach to configuring multiple poli[c] disciplines:**
  - IDS
  - AT-TLS
  - IPSec and IP filtering
  - QoS
  - Policy-based Routing (PBR)
- **Separate perspectives bu[t] consistent model for eac[h] discipline**
- **Focus on high level conc[ept] vs. low level file syntax**
- **z/OSMF-based web interf[ace] (strategic) and standalon[e] Windows application**
- **Builds and maintains**
  - Policy files
  - Related configuration files
  - JCL procedures and RACF di[rectives]
- **Supports import of existi[ng] 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

z/OS

USER1.TCPCS.TCPPARMS(ATTLS)
USER1.TCPCS.TCPPARMS(QOS)
USER1.TCPCS.TCPPARMS(IDS)
USER1.TCPCS.TCPPARMS(IPSEC)

Configuration Assistant

Generate and transfer (FTP)

Policy flat files

Policy Agent

Backing Store

Transfer (FTP)
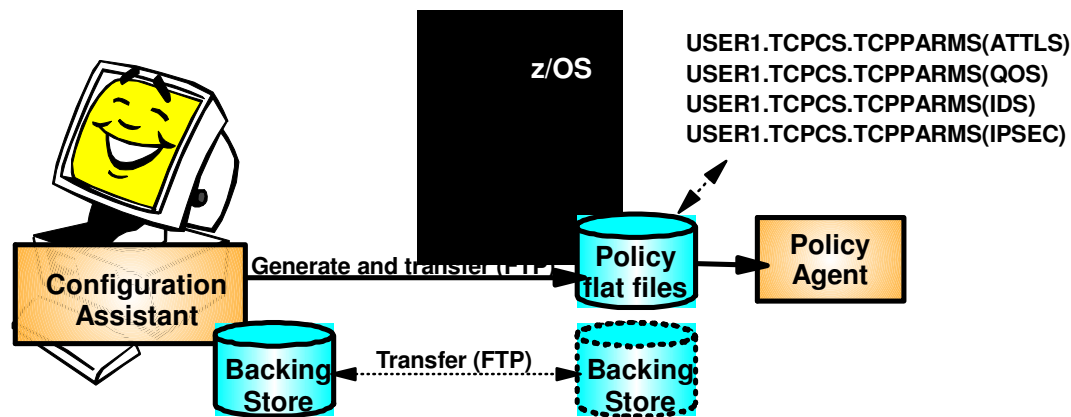
Backing Store

- **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

z/OS

Configuration Assistant
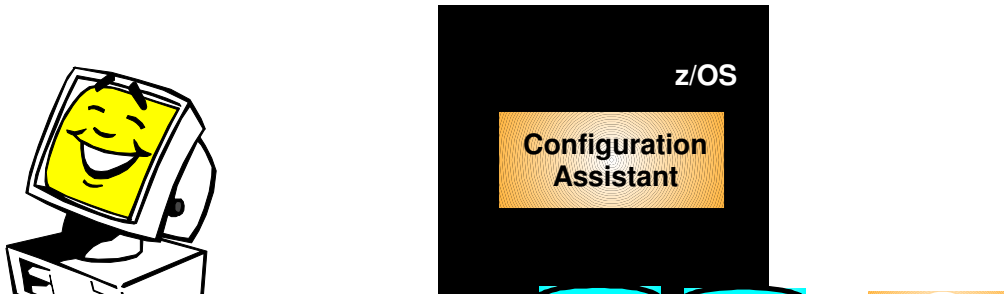
Configuration Assistant Policy Creation Approach

- 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)

Group IP addresses that need the same treatment. For example all VIPA addresses, or all real network interface addresses. Simplifies creation of connectivity rules

Identifies a specific type of application network traffic. Based on protocol , local and/or remote ports, connection direction, z/OS jobname, userid

Identifies the TLS/SSL security requirements, such as ciphersuites, allowed protocol versions (e.g. SSLv3, TLSv1), etc.

IP Address group

Traffic Descriptor

Security Level

IP Address
IP Address
IP Address
IP Address

Requirement Map

Identifies what type of AT-TLS security applied to your traffic descriptors

Per policy type (not all object types are used with all policy types)

Connectivity Rule

Connectivity rules tie IP addresses to requirement maps

LPARs (Images)

Stacks

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

Policy Creation Optimizations

- **One step requirement map creation for IPSec and AT-TLS**
  - ➤ Dialogs eliminate the step of creating requirement map objects before the creatio 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 immedia use.
  - ➤ Each rule defines an application with default port settings, key ring, and is associated with a default security level.

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
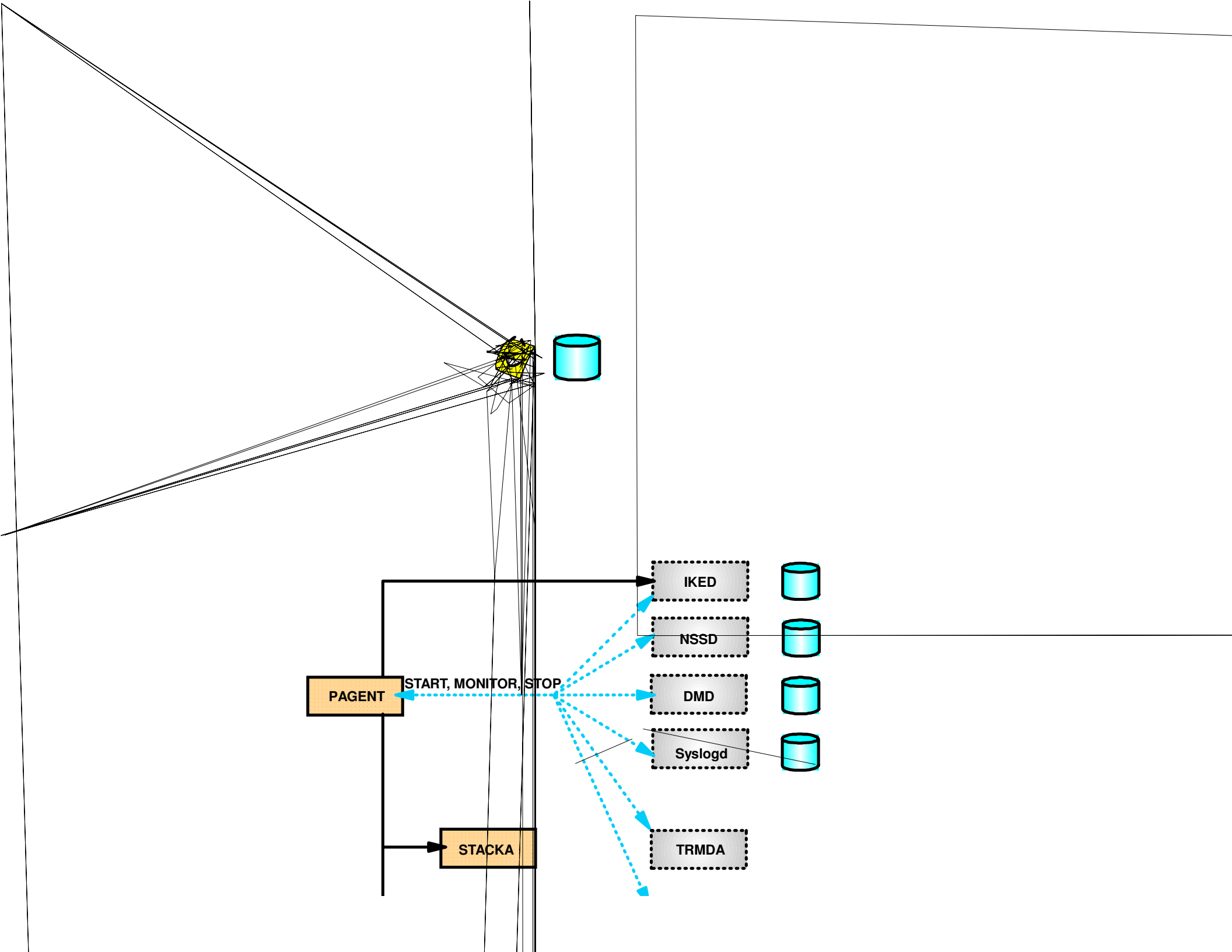
IKED

NSSD

START, MONITOR, STOP
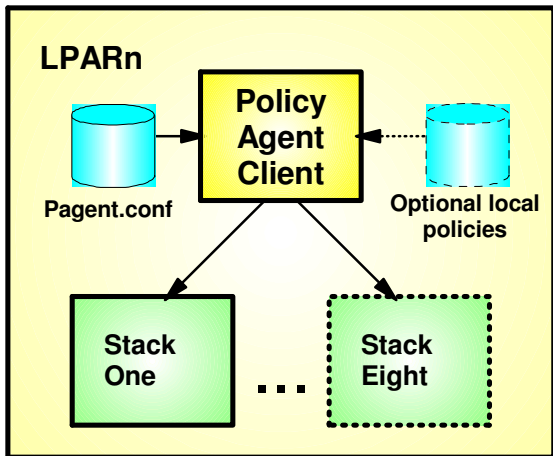
PAGENT

DMD

Syslogd

STACKA

TRMDA

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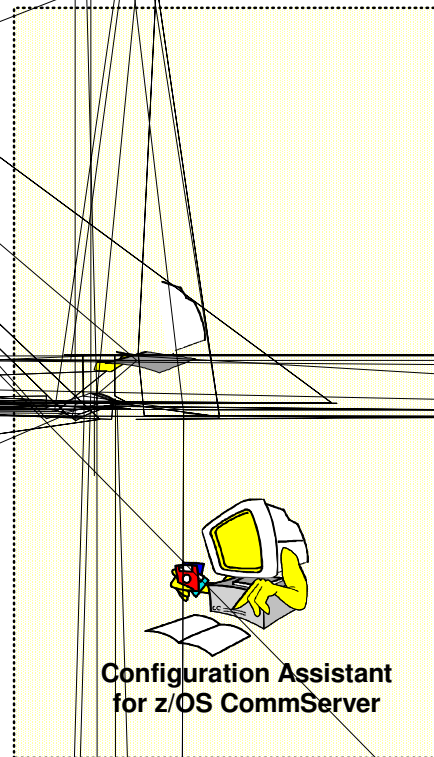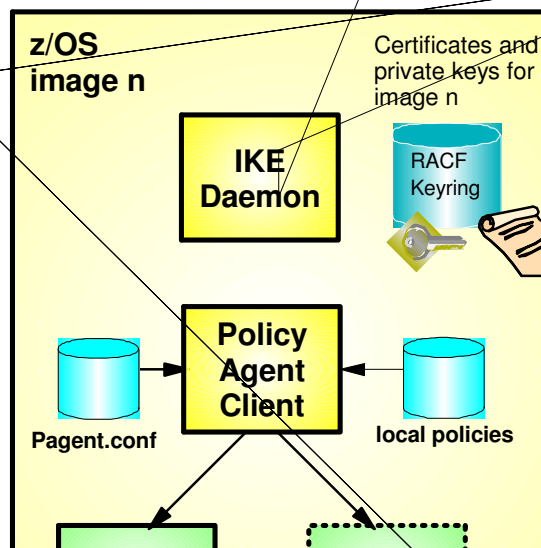
- **Each z/OS system locally admini**
  - ➤ RACF certificate administration
  - ➤ Policy configuration
  - ➤ Monitoring
- **Connectivity required between administration and each manage platform**
  - ➤ Monitoring application has advanc knowledge of each managed node
  - ➤ Coordination required to push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

Configuration Assistant for z/OS CommServer

z/OS image n

Certificates and private keys for image n

IKE Daemon

RACF Keyring

Policy Agent Client

Pagent.conf

local policies

LPAR1

Policy Agent Client

Pagent.conf

Optional local policies

Stack One

Stack Eight

LPARn

Policy Agent Client

Pagent.conf

Optional local policies

Stack One

Stack Eight
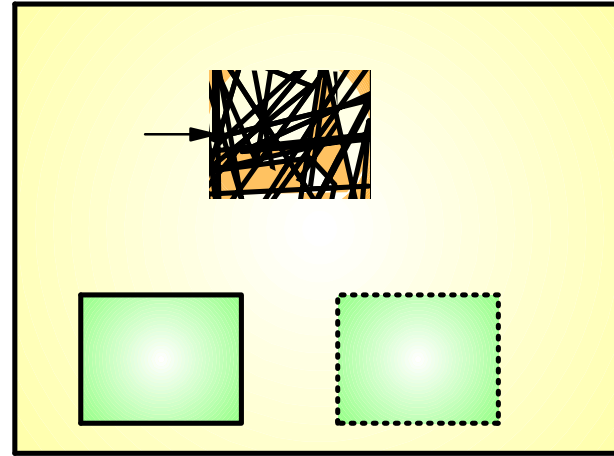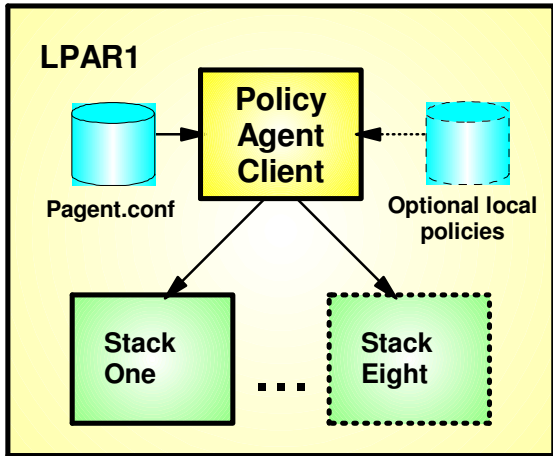
Network Security Services for IPSec
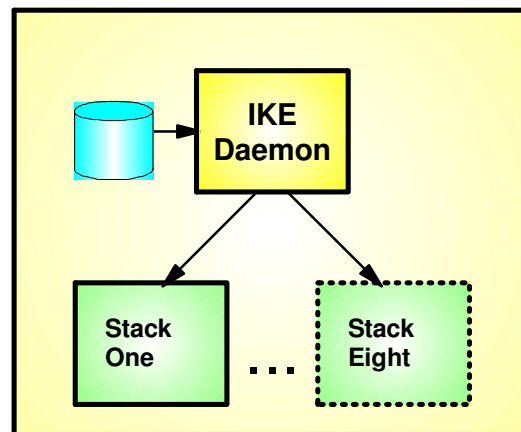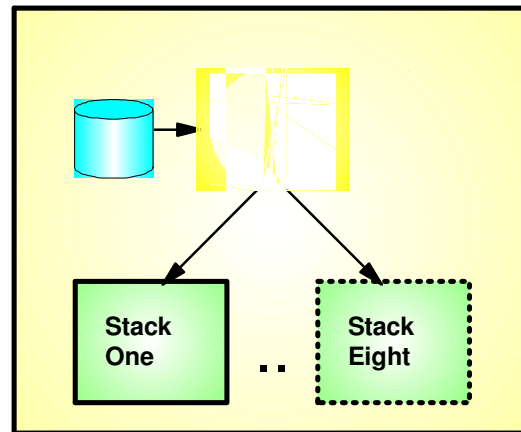
- **Centralized network security services for a z/OS images**
  - ➤ Images can be non-sysplex, intra- or inter-sys
- **NSS digital signature services**
  - ➤ Allows central administration of RACF certific private keys
    - – Sign and verify during runtime IKE negotiatic
- **NSS monitoring services**
  - ➤ Allows selection of single focal point as IPSe management hub
    - – ipsec command for administrator
    - – NMI API for management applications
- **Availability options**
  - ➤ Backup NSS can be specified
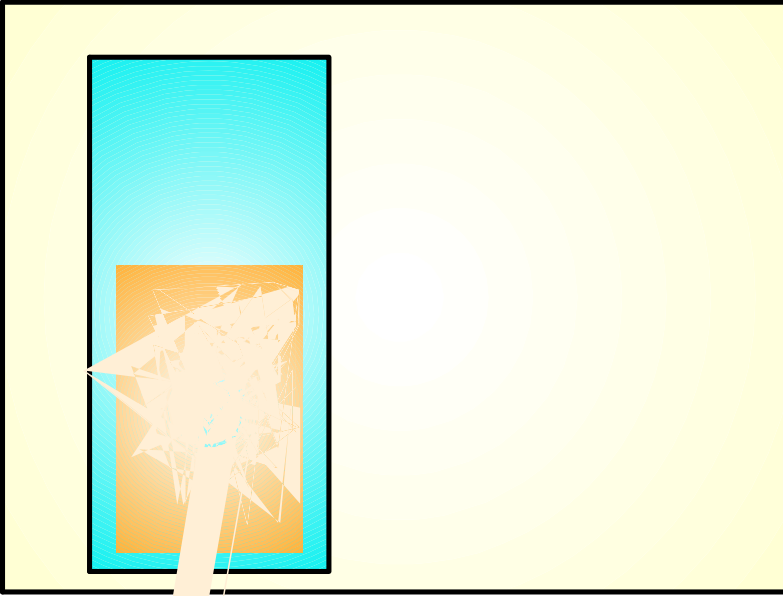
Agenda

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 Summar

- ■ 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

---

z/OS V1R12

- ■ **AT-TLS**
  - ➤ Performance
- ■ **IPSec**
  - ➤ IKEv2
  - ➤ X.509 certificate trust chains
  - ➤ Certificate Revocation Lists
  - ➤ Many new crypto algorithms
  - ➤ FIPS 140 mode
- ■ **Configuration Assistant**
  - ➤ Support for new IPsec features

z/OS V1R13

- ■ **Intrusion Detection Services**
  - ➤ IPv6 support
  - ➤ New attack types
- ■ **IPSec**
  - ➤ IKEv2 support for NAT traversal
  - ➤ IKEv2 support for Sysplex Wide SAs.
- ■ **Configuration Assistant**
  - ➤ Support for new IDS and IPSec features
  - ➤ Multiple release support
  - ➤ Common configuration for multiple TCP/IP stacks
  - ➤ IP address discovery

z/OS V2R1

- ■ **AT-TLS**
  - ➤ TLS Renegotiation Extension 5746)
  - ➤ Elliptic Curve Cryptography s
  - ➤ TLS V1.2 (RFC 5246)
  - ➤ Suite B cipher suite support
- ■ **IPSec**
  - ➤ IPv6 support for Sysplex Wid
  - ➤ QDIO accelerator coexistenc IP packet filtering
- ■ **Intrustion Detection Services**
  - ➤ Limit defense filter logging
- ■ **Configuration Assistant**
  - ➤ Support for new IPsec and A features

For more information ...

URL	Content
http://www.twitter.com/IBM_Commserver twitter	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/atsmastr.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