Session 300

TCP/IP Security Controls on z/OS

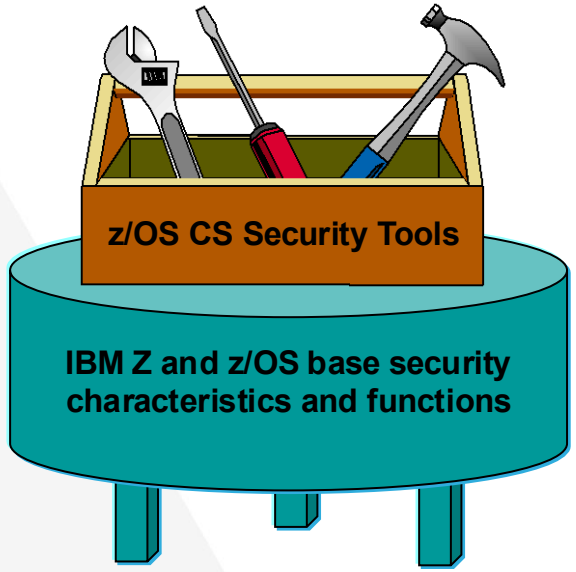
Navya Ramanjulu – navyaram@us.ibm.com
Edward Seidl – eseidl@us.ibm.com

Agenda

- z/OS Communications Server Overview
  - Roles and objectives
  - Policy-based networking

- Steps for protecting TCP/IP, related resources and data in transit
  1. Blocking unwanted traffic
  2. Protecting against attacks
  3. Protecting data in the network
  4. Audit trails: zERT and syslogd
  5. Controlling access to TCP/IP resources

- Summary



z/OS Communications Server provides a rich set of network security tools from which you can pick and choose

Agenda

- **z/OS Communications Server Overview**
  - **Roles and objectives**
  - **Policy-based networking**

- Steps for protecting TCP/IP, related resources and data in transit
  1. Blocking unwanted traffic
  2. Protecting against attacks
  3. Protecting data in the network
  4. Audit trails: zERT and syslogd
  5. Controlling access to TCP/IP resources

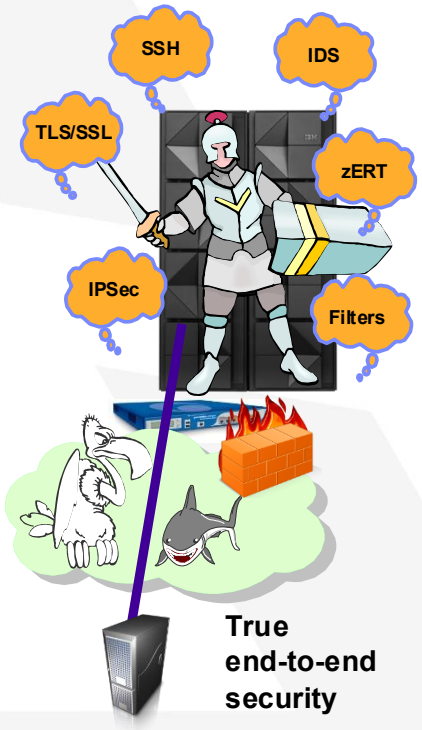
- Summary

Security roles and objectives

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

- **Protect data IN the network (cryptographically)**
  - *Data End Point Authentication*
    Verify who the secure end point claims to be
  - *Data Origin Authentication*
    Verify that data was originated by claimed sender
  - *Message Integrity*
    Verify contents were unchanged in transit
  - *Data Privacy*
    Conceal data payloads using encryption

Self protection:
z/OS itself is the last line of defense in an often hostile network environment!



z/OS CS security focus areas:
- **Self protection**
- **Provide secure access to both TCP/IP and SNA applications**
- **Exploit the strengths of System z hardware and software**
- **Provide audit trails for security functions**
- **Complement network-based security measures (firewalls, IDS/IPS, etc.)**
- **Minimize security deployment costs**

Communications Server security features by layer

Protect system from the network

syslogd provides event and error logging for a wide variety of Comm Server components and z/OS Unix applications

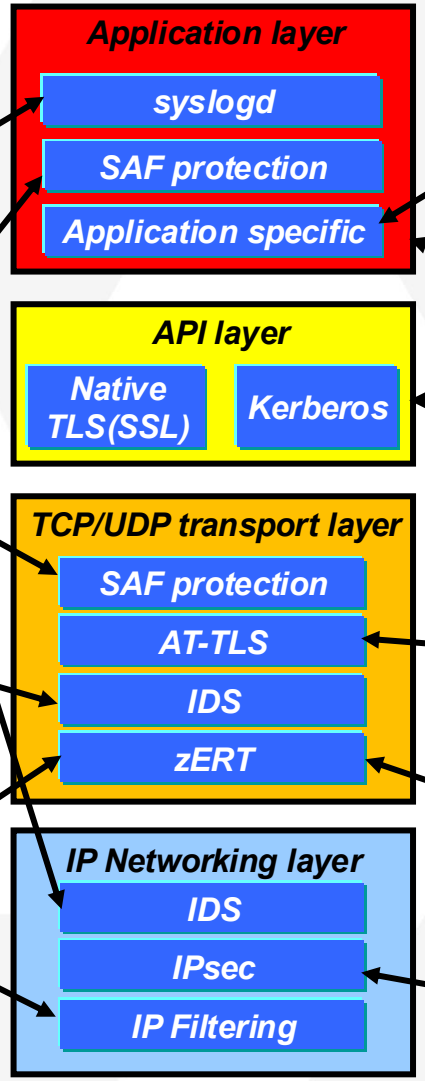
z/OS Comm Server TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources.

The SAF SERVAUTH class is used to prevent unauthorized access to a wide variety of TCP/IP resources.

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

z/OS Encryption Readiness Technology (zERT) policy-based enforcement allows for termination of TCP connections using insufficient cryptographic protection.

IP filtering blocks IP traffic that this system doesn't specifically permit. It also controls which traffic must use IPsec protection



Protect data in the network

Examples of application protocols with built-in security extensions are FTP, TN3270, SMTP, and OSPF.

SSH (not part of z/OS Comm Server) provides an umbrella of secure applications (secure shell access, secure file transfer, etc.)

Kerberos and TLS (neither part of z/OS Comm Server) provide cryptographic protection. Applications must be modified to use these functions. Both operate only on connection-based (TCP streaming) sockets (not UDP or raw sockets).

Application Transparent TLS is a TCP/IP stack service that provides TLS protection in the TCP transport layer to applications without requiring application changes.

z/OS Encryption Readiness Technology (zERT) provides detailed auditing of the cryptographic protection applied to all TCP and Enterprise Extender traffic.

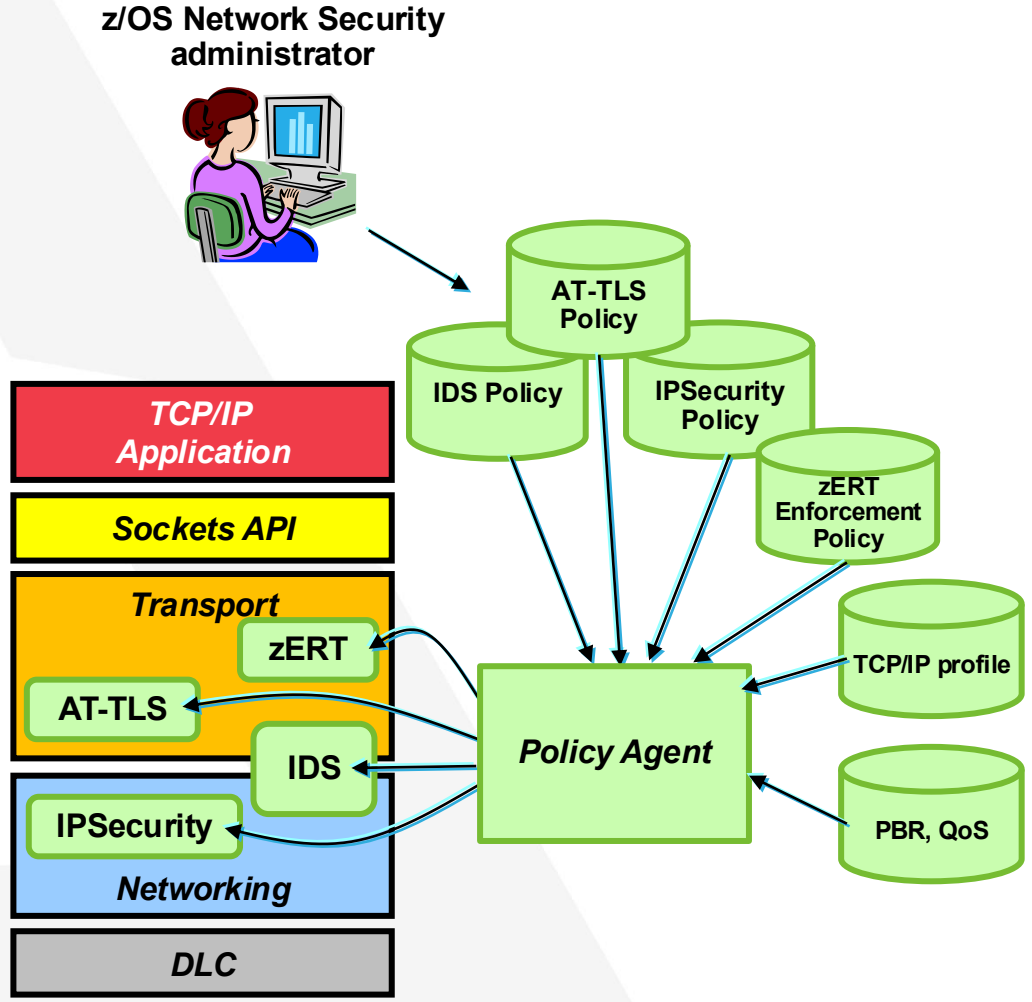
IPsec resides provides cryptographic protection of all IP traffic in the networking layer. It is transparent to upper-layer protocols and applications.

Audit and logging

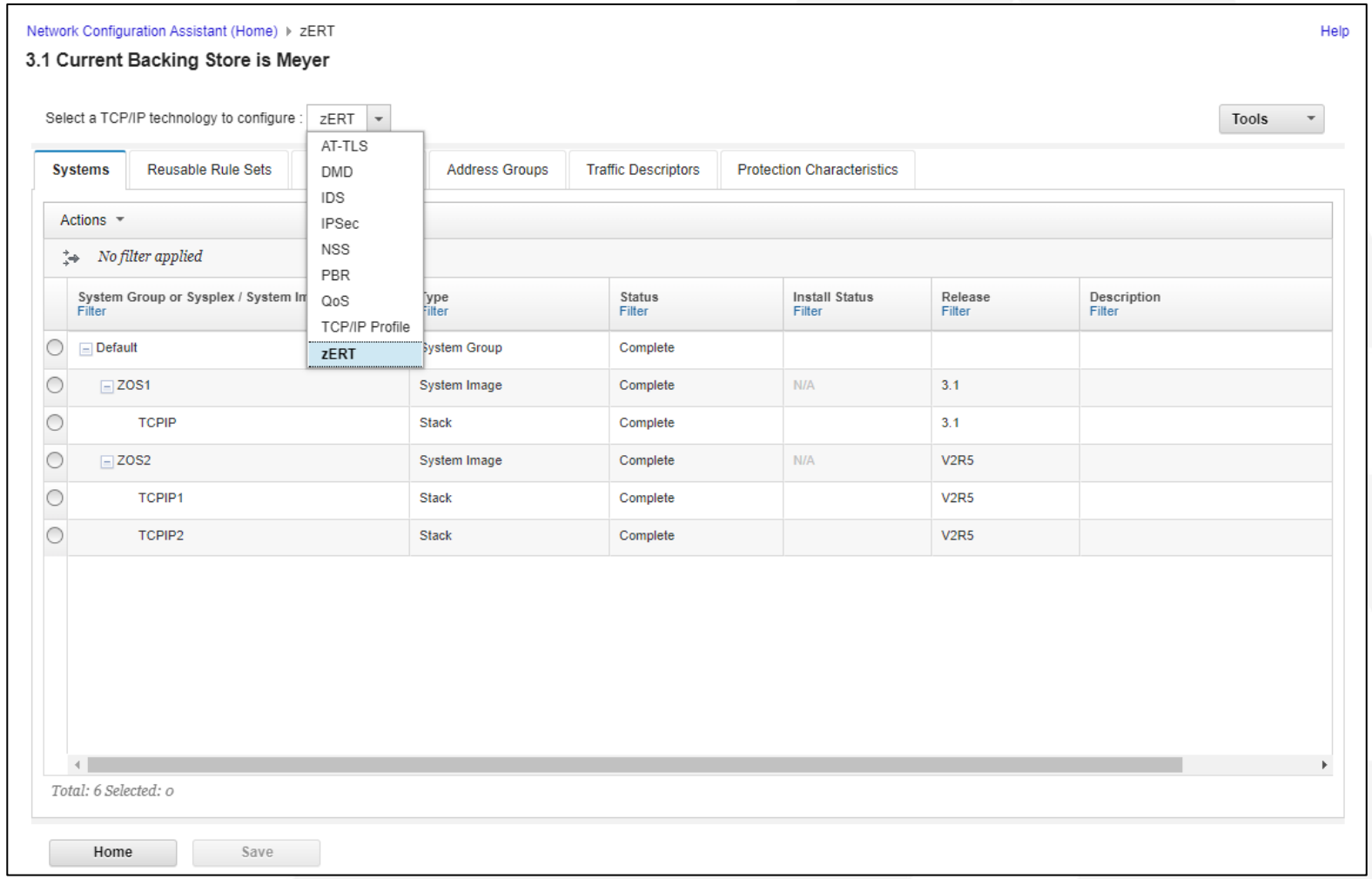
Comm Server applications and stack security features write appropriate SMF records and/or log messages

Policy-based network security on z/OS

- Policy is created through Network Configuration Assistant for z/OS Communications Server
  - Generates and uploads policy files and related content to z/OS
- Policy Agent processes and installs policies into TCP/IP stack
  - Policies are defined per TCP/IP stack
  - Separate policies for each discipline
  - Policy agent also monitors and manages the other daemons (IKED, syslogd, trmd, etc.)
- Provides network security without requiring changes to your applications
  - Security policies are enforced by TCP/IP stack
  - Different security disciplines are enforced independent of each other



z/OSMF Network Configuration Assistant for Communications Server



- Focus on concepts, not syntax
  - what traffic to protect
  - how to protect it
  - De-emphasize low-level details (though they are accessible through advanced panels)
- Builds and maintains
  - TCP/IP profile
  - Policy files
  - Related configuration files
  - JCL procs and RACF directives
- Supports current z/OS release plus past two

Agenda

- z/OS Communications Server Overview
  - Trends and requirements
  - Roles and objectives
  - Policy-based networking
- **Steps for protecting TCP/IP, related resources and data in transit**
  1. Blocking unwanted traffic
  2. Protecting against attacks
  3. Protecting data in the network
  4. Audit trails: zERT and syslogd
  5. Controlling access to TCP/IP resources
- Summary

A suggested roadmap to securing z/OS in your network

1. **Blocking unwanted traffic from entering or leaving your z/OS system**
   - ☑ **Solution: IP packet filtering**

2. **Protecting against malicious or accidental attacks on your system**
   - ☑ **Solution: Intrusion Detection Services**

3. **Protect end-to-end confidentiality and integrity of data in the network**
   - ☑ **Solution: Various network security protocols (IPsec, TLS, SSH)**

4. **Audit trail**
   - ☑ **Solution: z/OS Encryption Readiness Technology**
   - ☑ **Solution: syslogd for secure logging**

5. **Controlling user access to TCP/IP resources on the system**
   - ☑ **Solution: SAF protection using SERVAUTH class resources**

Agenda

- z/OS Communications Server Overview
  - Trends and requirements
  - Roles and objectives
  - Policy-based networking

- Steps for protecting TCP/IP, related resources and data in transit
  1. **Blocking unwanted traffic: IP packet filtering**
  2. Protecting against attacks
  3. Protecting data in the network
  4. Audit trails: zERT and syslogd
  5. Controlling access to TCP/IP resources

- Summary

IP packet filtering: Basics

IP packet filtering is enabled in the TCPIP profile dataset:
IPCONFIG[6] IPSECURITY

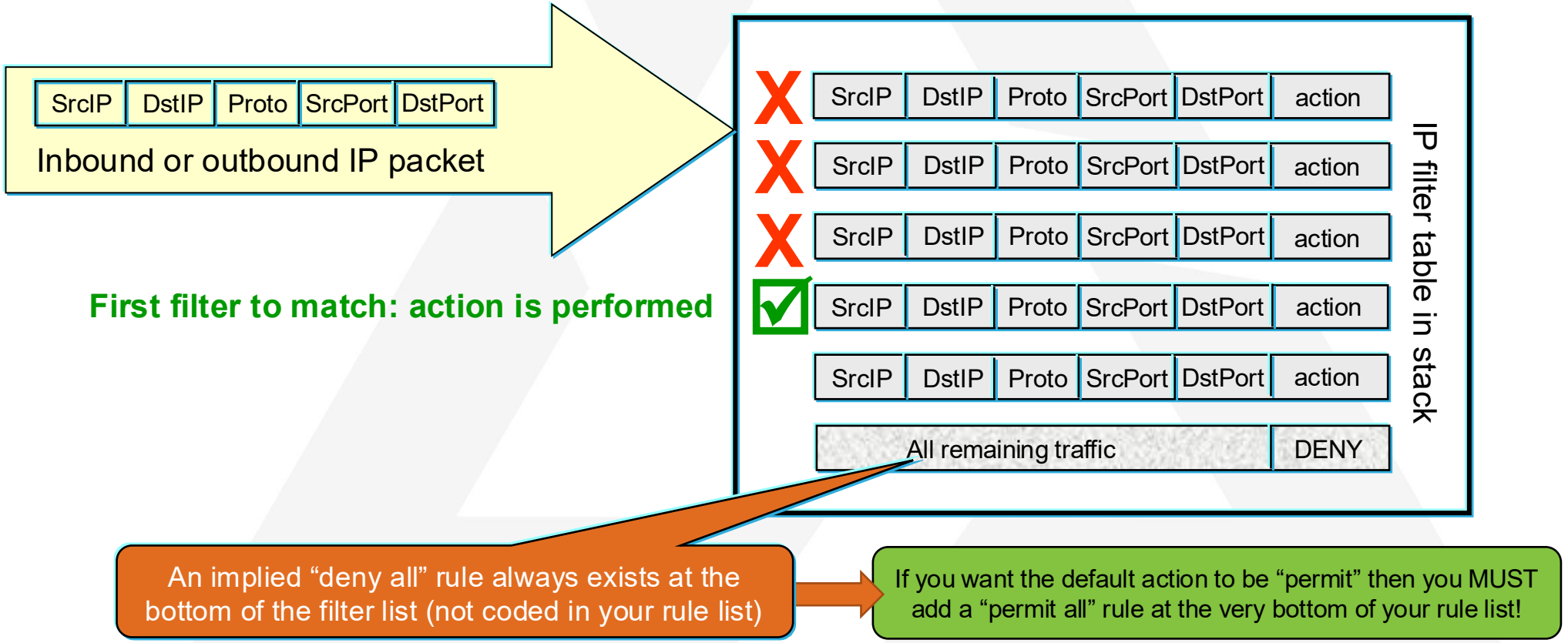
Filter rules:
- Rudimentary "default" rules can be configured in the TCPIP profile to allow specific traffic before policy agent initializes
- Configured in IPSecurity policy file - processed by Policy Agent
- Filter rules describe IP traffic based on relevant attributes
- Possible actions when a filter rule is matched:
  - Permit / Deny / Permit with IPsec (more on IPsec later)
  - Log (in combination with the above actions)

Benefits to local system:
- Early discard of potentially malicious packets
- Avoid wasting CPU on processing packets for non-existent applications
- Prevent outbound data leakage
- Can be used to enforce network segmentation

```
IpFilterRule InternalNetWeb
{
  IpSourceAddr 10.1.1.1
  IpDestAddrSet 10.1.1.0/24
  IpService
  {
    SourcePortRange 80
    DestinationPortRange 1024 65535
    Protocol tcp
    Direction bidirectional InboundConnect
    Routing local
    SecurityClass 0
  }
  IpGenericFilterAction
  {
    IpFilterAction permit
    IpFilterLogging no
  }
}
```

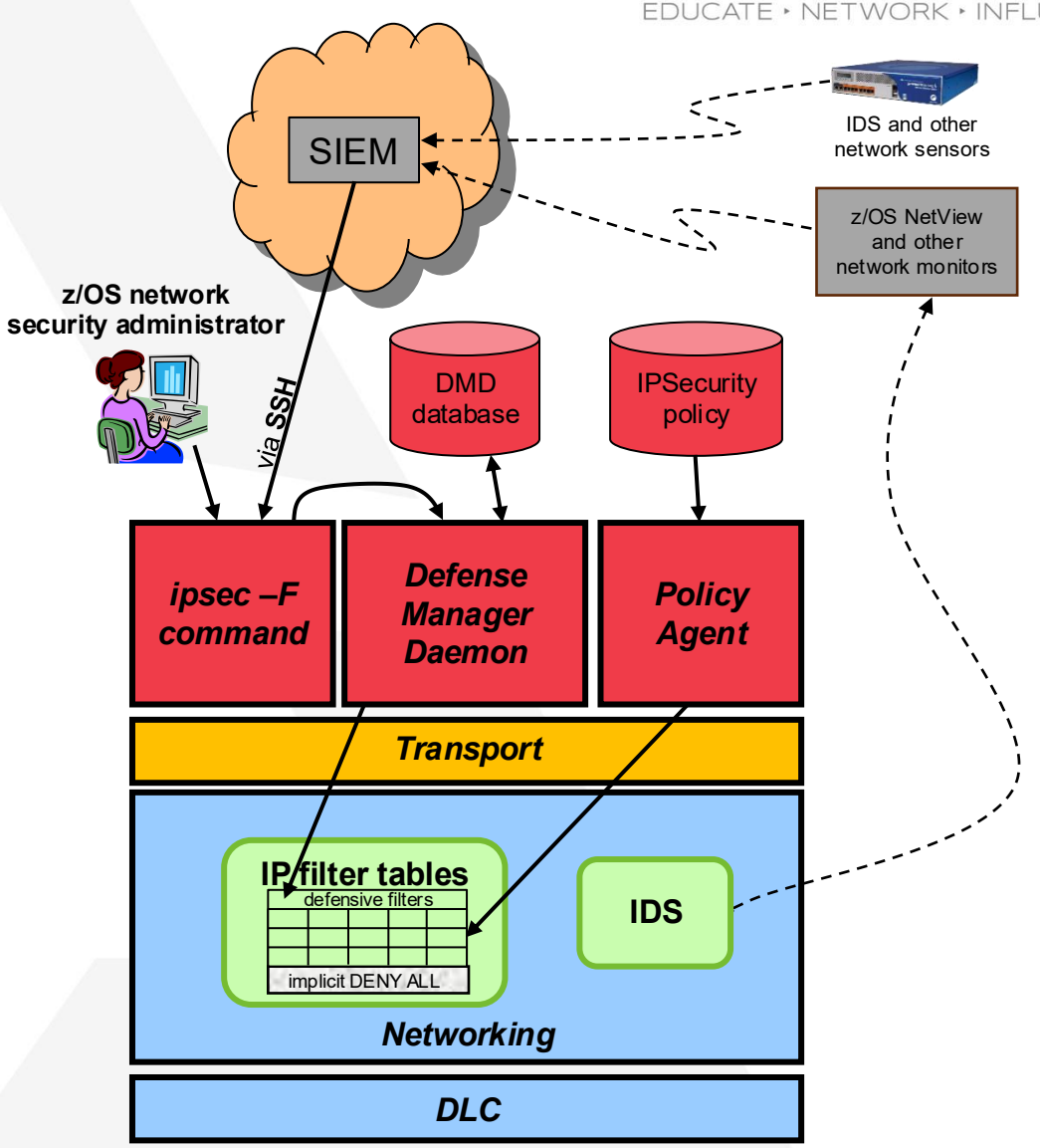
IP packet filtering: Filter matching

- Filters are searched in the order in which the were configured – **ORDER MATTERS**!
- Each rule is inspected, from top to bottom, for a match
- If a match is found, the search ends and that filter's action is applied
- As a result, rules with the most specific criteria should precede those that are more generalized



IP packet filtering: Defensive filters

- Defensive filters are **dynamically created** IP packet filters
- NOT policy-based: Rather, **created, managed and controlled through the `ipsec -F` command** and the Defense Manager Daemon (DMD)
- Installed “in front of” all other IP filters
- DENY only (but a "simulate mode" is available)
- Can be used by network management or SIEM automation to defend against intrusions or attacks from a specific IP address, subnet or network
- Limited lifetime (~2 weeks max)
- Maintained on DASD to protect restarted stacks from the time they come up
- Selectable scope:
  - Local – applies to a specific stack
  - Global – applies to all stacks on z/OS system
- One Defense Manager Daemon per z/OS system



Agenda

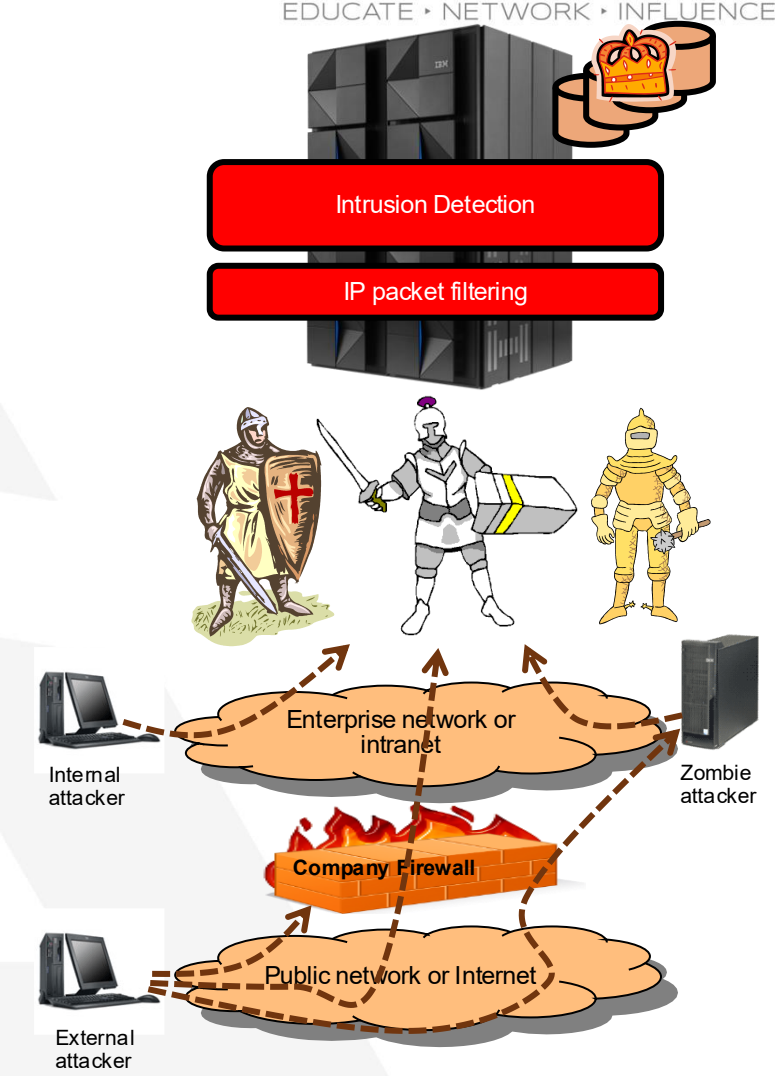
- z/OS Communications Server Overview
  - Trends and requirements
  - Roles and objectives
  - Policy-based networking

- Steps for protecting TCP/IP, related resources and data in transit
  1. Blocking unwanted traffic: IP packet filtering
  2. **Protecting against attacks: Intrusion Detection Services (IDS)**
  3. Protecting data in the network
  4. Audit trails: zERT and syslogd
  5. Controlling access to TCP/IP resources

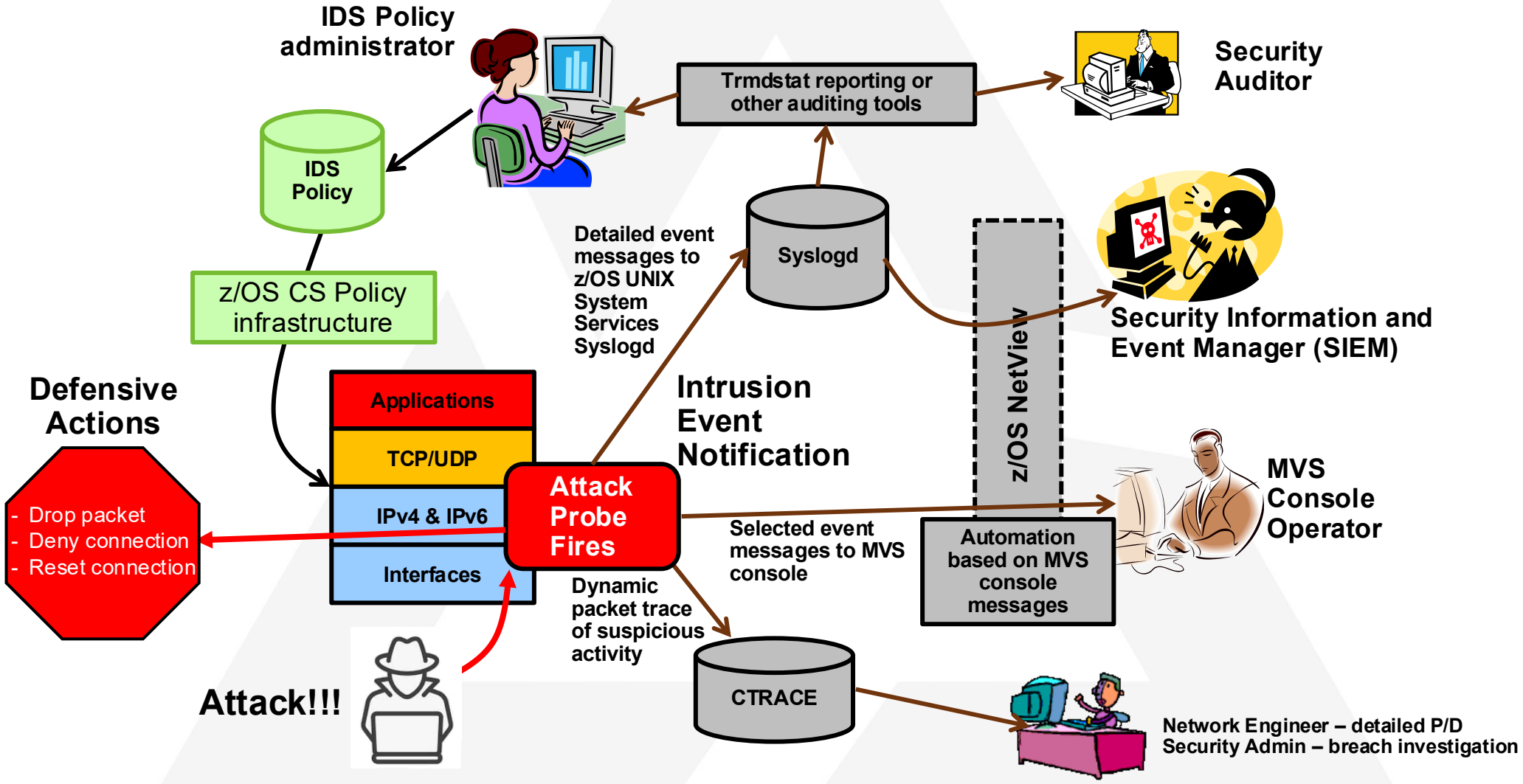
- Summary

IDS: Protecting against intentional and unintentional attacks

- What is an intrusion?
  - Information Gathering
  - Eavesdropping/Impersonation/Theft
  - 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 occur from Internet or intranet
  - Company firewalls and intrusion prevention appliances can provide some level of protection from Internet
  - Perimeter security strategy alone is typically not sufficient.
    - Some access is permitted from Internet – typically into a Demilitarized Zone (DMZ)
    - Trust of intranet and insiders
- Attacks can be intentional (malicious) but often occur as a result of errors on nodes in the network (config, application, etc.)



IDS: z/OS Communications Server IDS overview



IDS: z/OS TCP/IP IDS features

z/OS **in-context IDS** broadens overall intrusion detection coverage:

- **Not a replacement for network-based IDS – rather, z/OS IDS is complementary**
- In-context: IDS checks applied as part of communications endpoint processing, not as an intermediary
- Ability to evaluate inbound IPsec encrypted data - IDS applied after IPsec decryption on the endpoint system
- Detects statistical anomalies in realtime - endpoint system has stateful data / internal thresholds that generally are unavailable to external IDSs
- Policy can control prevention methods on the endpoint, such as connection limiting and packet discard

IDS Events

- **Scans – attempts by remote nodes to discover information about the z/OS system**

- **Attacks – numerous types**
  - **Malformed packets**
  - **IP option and IP protocol restrictions**
  - **Specific usage ICMP**
  - **Interface and TCP SYN floods**
  - **and so forth…**

- **Traffic Regulation**
  - **TCP - limits the number of connections any given client can establish**
  - **UDP – limits the length of data on UDP queues by port**

IDS Actions

- **Reporting**
  - Logging
  - Console messages
  - IDS packet trace
  - Notifications to external event managers (like IBM NetView)
- **Defensive actions**
  - Packet discard
  - Limit connections
  - Drop connections

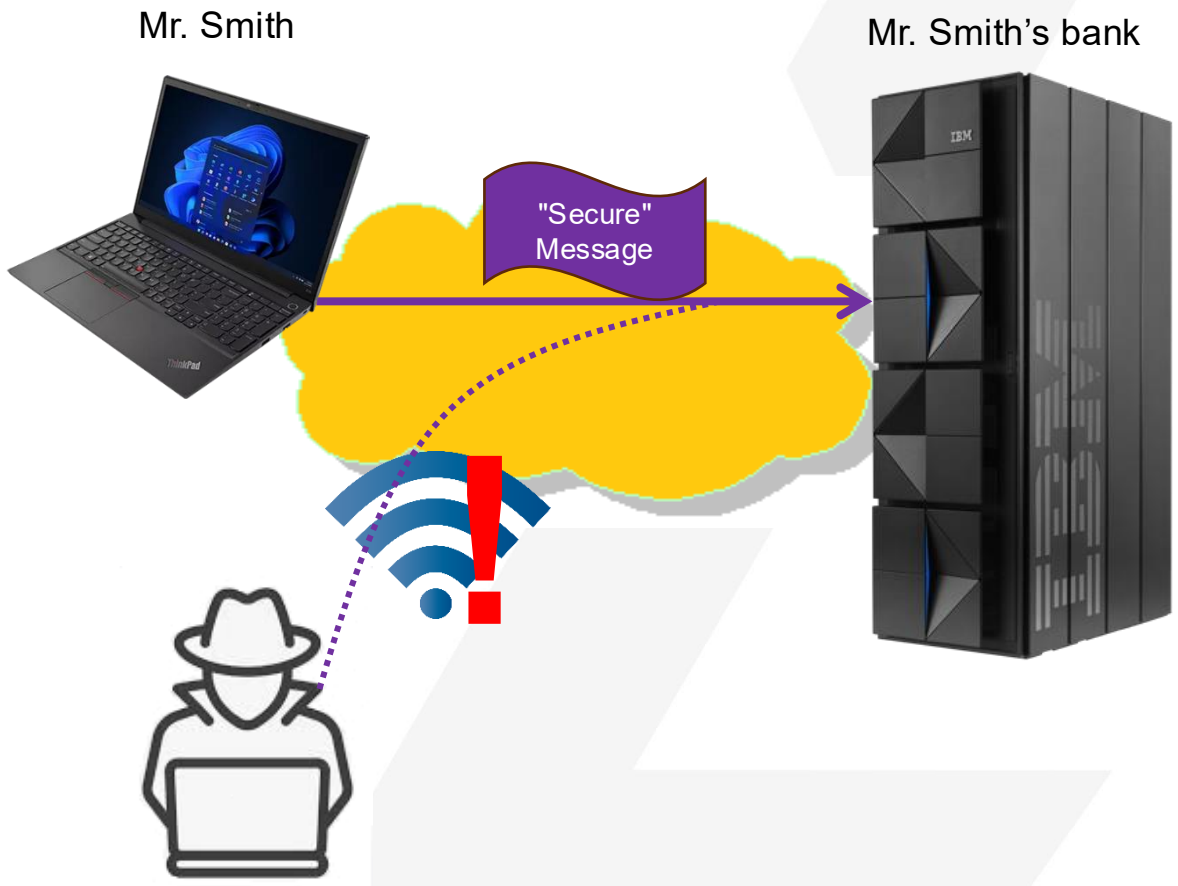
Agenda

- z/OS Communications Server Overview
  - Trends and requirements
  - Roles and objectives
  - Policy-based networking

- Steps for protecting TCP/IP, related resources and data in transit
  1. Blocking unwanted traffic: IP packet filtering
  2. Protecting against attacks: Intrusion Detection Services (IDS)
  3. **Protecting data in the network: Network cryptographic protocols**
  4. Audit trails: zERT and syslogd
  5. Controlling access to TCP/IP resources

- Summary

Protocols: The four big questions



Who are you?
(Partner authentication)

Who sent this message?
(Message authentication)

Was this message modified on its way to me? (Message integrity)

Who can read this message?
(Data Confidentiality)

Each of the cryptographic network protocols discussed here answer each of these questions - just in slightly different ways

Protocols: Cryptographic network protocols on z/OS

z/OS provides 4* mechanisms to protect TCP/IP traffic:

1. **TLS/SSL direct usage (TCP traffic)**
   - Application is explicitly coded to use these
   - Application layer, per-connection protection
   - TCP only

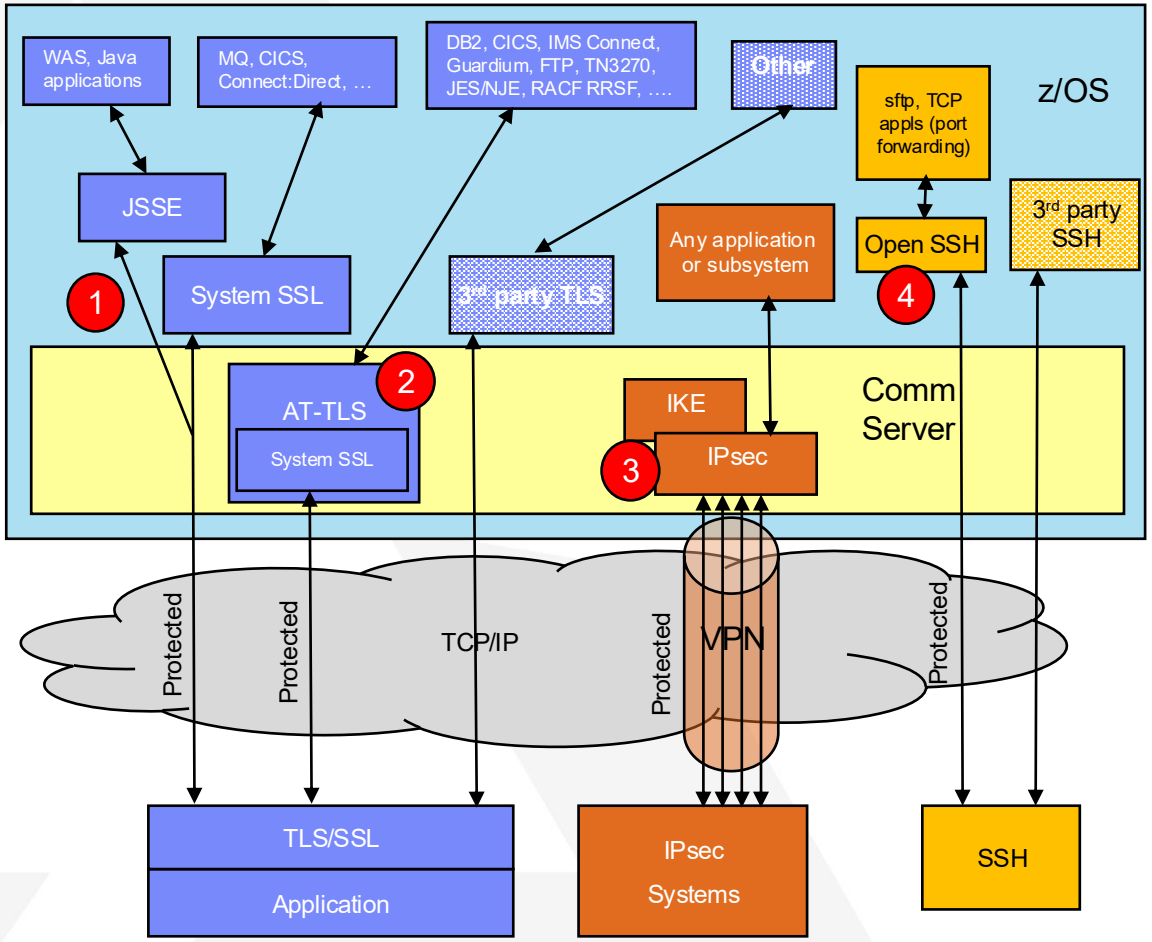
   (Can also have 3rd party TLS implementations like OpenSSL)

2. **Application Transparent TLS (AT-TLS) (TCP traffic)**
   - TLS/SSL applied in TCP layer as defined by policy
   - Configured in AT-TLS policy via Network Configuration Assistant
   - Typically, transparent to application
   - TCP/IP stack is user of System SSL services

3. **Virtual Private Networks using IPsec and IKE (IP traffic)**
   - "Node to node" encryption
   - IPsec implemented in IP layer as defined by policy
   - Completely transparent to application
   - Flexible scope of protection of traffic (wide to narrow)

4. **Secure Shell using z/OS OpenSSH (TCP traffic)**
   - Mainly used for sftp on z/OS, but also offers secure terminal access and TCP port forwarding
   - Configured in ssh configuration file and on command line

   (Can also have 3rd party SSH implementations)



* - z/OS also provides Kerberos support, but that is focused mainly on peer authentication

Protocols: Comparing TLS, IPsec (with IKE) and SSH

Attribute	TLS (SSL)	IPsec	SSH-2
Traffic covered	TCP connections	All IP traffic (TCP, UDP (incl EE), ICMP, etc.)	TCP connections
Provides true end-to-end protection	Yes	Yes	Yes
Provides network segment protection	No	Yes	No
Protection scope	Single TCP connection	Flexible (all traffic, by protocol, IP addrs, ports, etc)	One or more TCP sessions
Requires application layer changes	Yes (except basic AT-TLS)	No	No
Endpoints and authentication	Application to application	IP node to IP node	Host to Host
Auth credentials	X.509 certificates	X.509 certificates or pre-shared keys	public/private key
Auth frequency	Configurable	Configurable	Once at session startup
Session key refresh	Configurable based on time	Configurable based on data and time	Configurable based on data

Protocols: TLS, IPsec and SSH implementations on z/OS

SHARE
EDUCATE • NETWORK • INFLUENCE

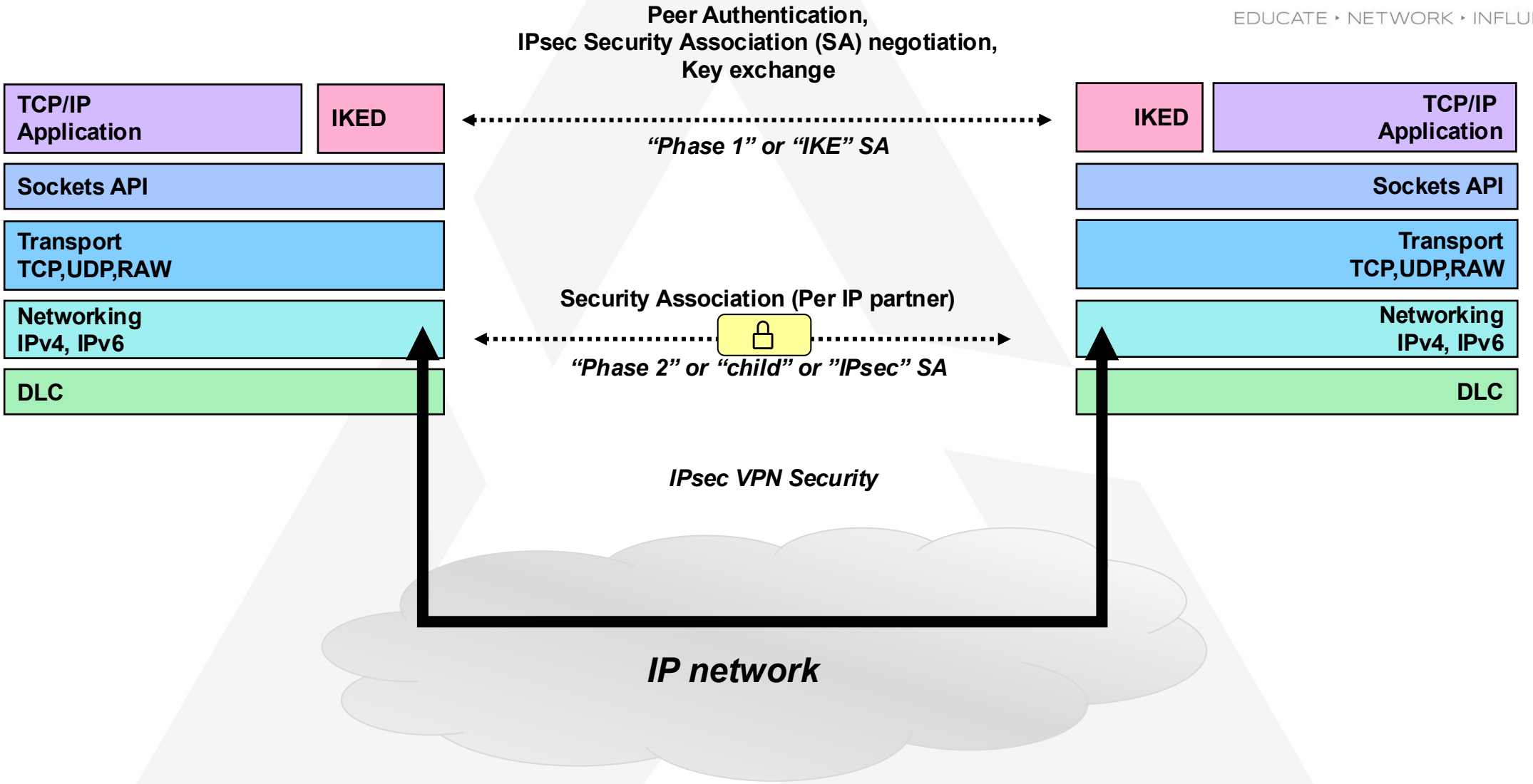
Attribute	TLS (SSL)	IPsec	SSH-2
Configuration	AT-TLS: Policy System SSL direct: per application JSSE: Java properties	Policy	OpenSSH configuration files as well as on command line invocation
Application transparency	AT-TLS: Yes (basic AT-TLS only) System SSL direct: No JSSE: No	Yes	Can be with port forwarding
SAF Keyrings	Yes	Yes	Yes (for keys only)
Secure Keys (CEX*n*)	Yes	Yes	No
Specialty engine (zIIP) support	JSSE only	Yes	No
System z hardware crypto	CPACF, CEX*n*	CPACF, CEX*n*	CPACF, CEX*n* (RNG)

SHARE
EDUCATE • NETWORK • INFLUENCE

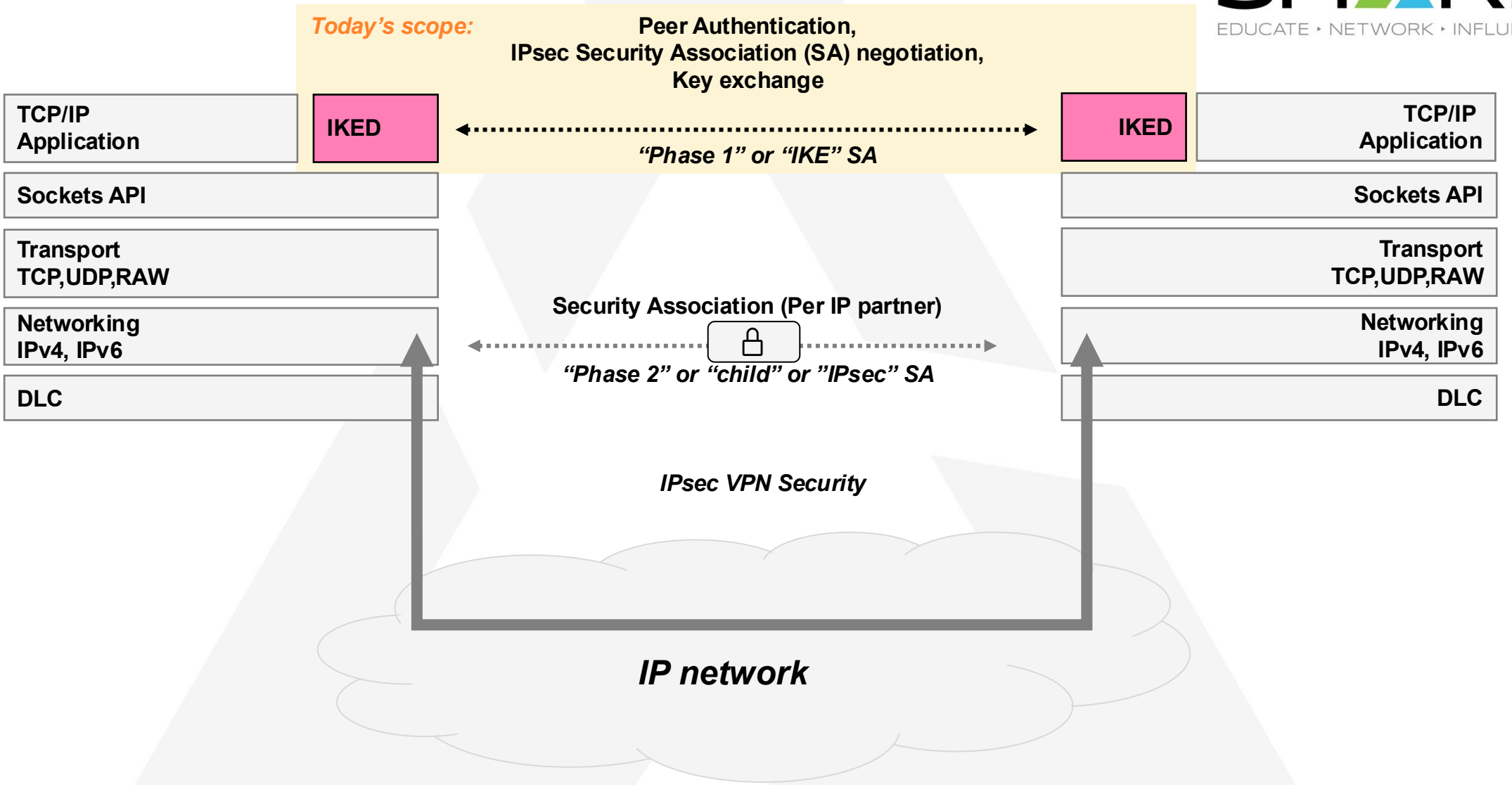
SHARE update:

Support for AES-GCM for IKEv2 SA

Background - IPSec



Background - IPSec



Support for AES-GCM for IKEv2 SA

- With **z/OS 3.2 and 3.1 APAR PH68240**, you can use Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) to protect IPSec using IKEv2 key exchanges.
  - Implements RFC 5282 - *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*
  - AES-GCM combines encryption and integrity into a single operation, referred to as a combined mode algorithm.
  - This algorithm has been long available as an option for IPsec/Child SA tunnels to protect TCP/IP data.
- **z/OSMF Network Configuration Assistant 3.2 and 3.1 APAR PH68902** provides new settings to configure use of AES-GCM for the IPSec discipline.

- Restrictions:
  - **IKEv2 only** – IKEv1 has been deprecated by the IETF with no new support
  - **Non-FIPS only** – When IKED is configured for FIPS-140, AES-GCM is not supported on the KeyExchangeOffer

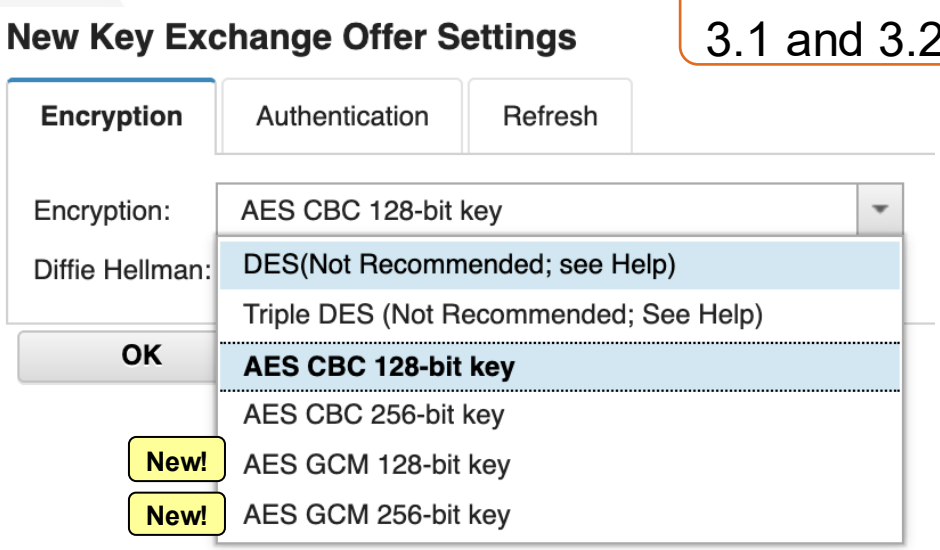
- This addresses the following open requirement:
  - ZOS-I-4518 - IKE Data Offer to add GCM blocking ciphers

Support for AES-GCM for IKEv2 SA – Network Configuration Assistant changes

- New dropdown options are added to the **Advanced** → **Key Exchange Offer Settings** panel for the IPSec *Connectivity* or *Reusable Rule*:
  - Encryption: AES GCM 128-bit key
  - Encryption: AES GCM 256-bit key

- Use of AES-GCM in **Encryption** tab will carry over dropdown setting to the **Authentication** tab's *IKEv2 Message Authentication* field
  - Remember, AES-GCM provide both encryption and message authentication function

NCA APAR PH6890
3.1 and 3.2



IKEv2 Advanced Key Exchange Offer Settings must be configured on a rule-by-rule basis to use AES-GCM for the IKEv2 key exchange proposal.

This configuration is not to be confused with the Security Level configuration used for specifying "phase 2" or "Child"/"IPSec" SA use of AES-GCM to protect IP data.

Support for AES-GCM for IKEv2 SA – Policy configuration

HowToEncrypt, **KeyExchangeOffer** parameter

- Encryption algorithm for protecting key exchanges
- New value: `AES_GCM_16 KeyLength keylen`

```
    .-HowToEncrypt--DES----------------------------.
|--+---------------------------------------------+--------->
   '-HowToEncrypt--+-DES------------------------+-'
                   +-3DES-----------------------+
                   +-AES------------------------+
                   +-AES_CBC KeyLength keylen----+
                   '-AES_GCM_16 KeyLength keylen-'
```

Support for AES-GCM for IKEv2 SA – Policy configuration

HowToVerifyMsgs, **KeyExchangeOffer** parameter

- Authentication algorithm for verifying message integrity of IKE version 2 key exchanges
- New value: `Null`
  - Only valid when `HowToEncrypt AES_GCM_16`
  - Required when `HowToEncrypt AES_GCM_16`

```
   .-HowToVerifyMsgs--HMAC_SHA1_96----------.
>--+-------------------------------------+------------------>
   '-HowToVerifyMsgs--+-Null--------------+-'
                      +-AES128_XCBC_96----+
                      +-HMAC_MD5_96-------+
                      +-HMAC_SHA1_96------+
                      +-HMAC_SHA2_256_128-+
                      +-HMAC_SHA2_384_192-+
                      '-HMAC_SHA2_512_256-'
```

Support for AES-GCM for IKEv2 SA
SMF and NMI updates

SMF:

- SMF type 119 subtype type 73 (IPSec IKE tunnel activation and refresh record)
- SMF type 119 subtype type 74 (IPSec IKE tunnel deactivation and expire record):
  - `SMF119IS_IKETunEncryptAlg:` new value **`SMF119IS_ENCR_AES_GCM_16 (20)`**
  - `SMF119IS_IKETunAuthAlg:` new value **`SMF119IS_AUTH_NULL (0)`**

Tip: Use `SMF119IS_IKETunEncryptKeyLength` to verify the AES-GCM key length.

NMI:

- Local IPSec NMI and Network Security Services (NSS) NMI: `Nmsec_GET_IKETUN`
  - `NMsIKETunEncryptAlg:` new value **`NMsec_ENCR_AES_GCM_16 (20)`**
  - `NMsIKETunPeerAuthMethod:` new value **`NMsec_AUTH_NULL (0)`**

Tip: Use `NMsIKETunEncryptKeyLength` to verify the AES-GCM key length

Support for AES-GCM for IKEv2 SA
zERT SMF and NMI reporting

zERT SMF and NMI data can also be used to verify use of AES-GCM!

SMF:

- SMF 119, subtype 11 (zERT connection detail record)
  - zERT connection detail IPSec protocol attributes section:
    - `SMF119SC_IPSec_IKETunEncAlg`
    - `SMF119SC_IPSec_IKETunAuthAlg`
- SMF 119, subtype 12 (zERT summary record)
  - zERT summary record IPSec protocol attributes section
    - `SMF119SS_IPSec_IKETunEncAlg`
    - `SMF119SS_IPSec_IKETunAuthAlg`

NMI:

- Real-time TCP network monitoring interface (NMI) available through **SYSTCPER** & **SYSTCPES** services.

Support for AES-GCM for IKEv2 SA – Important bug fix reminder

Bug fix: Support of AES-GCM proposal in the IKEv2 key exchange, even if you are not exploiting it.

If AES-GCM is configured as one of several proposals for the IKEv2 key exchange, action is required for any z/OS IKE peer(s) that do not have support for AES-GCM:

The z/OS IKE peers must have the PTF for APAR PH69019 installed. APAR PH69019 resolves a problem that causes an IKEv2 negotiation with an AES-GCM proposal to fail even when there is also an acceptable proposal.

Available for z/OS 3.2, 3.1, and 2.5.

To enable and use AES-GCM for the IKEv2 key exchange

The z/OS IKE peer must have 3.2 and 3.1 PTF for APAR PH68240 must be installed.

Available for z/OS 3.2 and 3.1.

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remain at our sole discretion.

For more on TLS

Session 298 “AT-TLS Hints and Tips”
at 3:45 PM on Wednesday, 2/25 in Salon 20

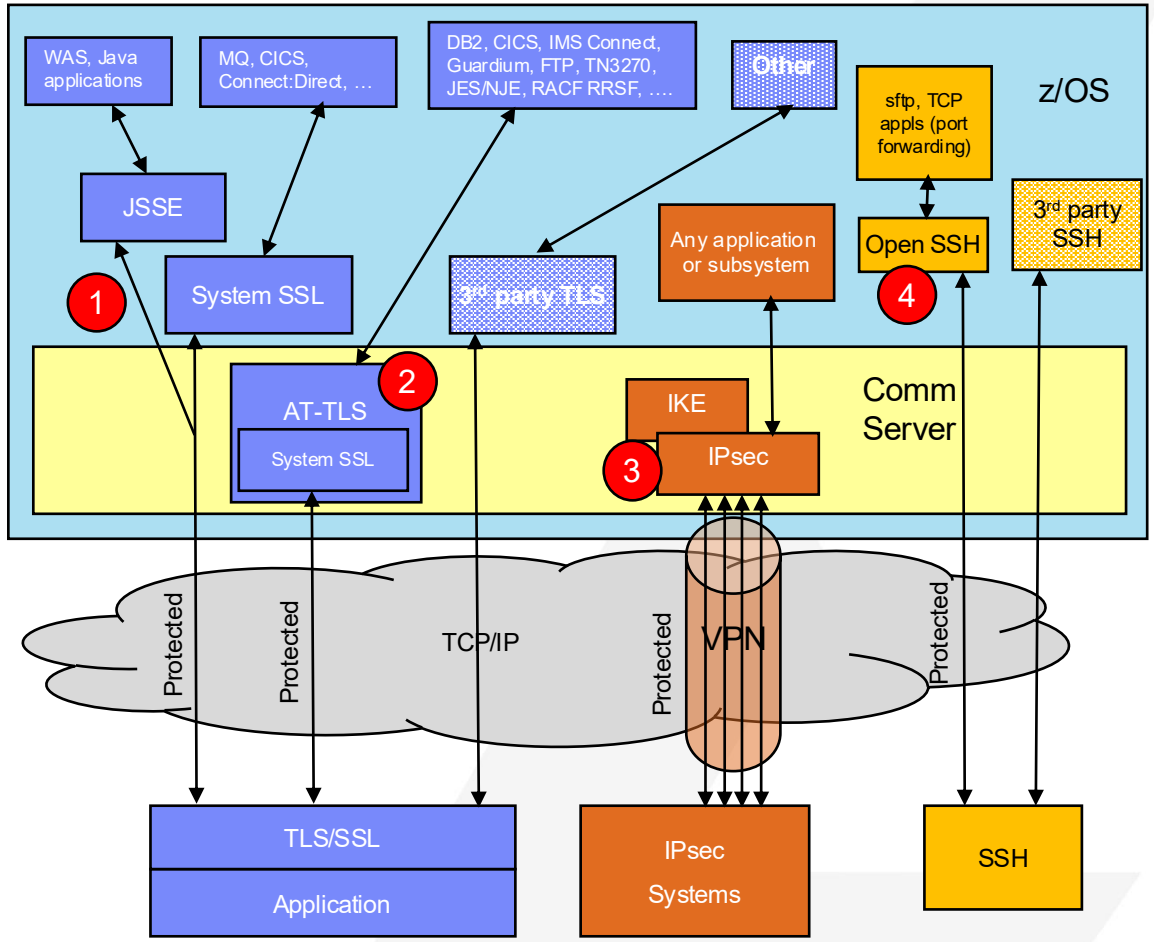
Agenda

- z/OS Communications Server Overview
  - Trends and requirements
  - Roles and objectives
  - Policy-based networking

- Steps for protecting TCP/IP, related resources and data in transit
  1. Blocking unwanted traffic: IP packet filtering
  2. Protecting against attacks: Intrusion Detection Services (IDS)
  3. Protecting data in the network: Network cryptographic protocols
  4. **Audit trails: zERT and syslogd**
  5. Controlling access to TCP/IP resources

- Summary

zERT: Remember all those crypto protocols & mechanisms?



With all this complexity, how can you tell…

Which traffic is being protected? Which is not?

How is the traffic being protected?

Who does the traffic belong to?

Do existing and new configurations adhere to your company's security policies?

zERT: Why zERT?

zERT is design specifically to help answer the preceding questions

- Positions the **TCP/IP stack** as a central collection point of cryptographic protection attributes for:
  - **TCP** connections that are protected by **TLS, SSL, SSH, IPsec** or are **unprotected***
  - **Enterprise Extender** connections that are protected by **IPsec** or are **unprotected***
- Two methods for discovering the security sessions and their attributes:
  - **Stream observation** (for TLS, SSL and SSH) – the TCP/IP stack observes the protocol handshakes as they flow over the TCP connection
  - **Advisory observation** by the cryptographic protocol provider (**System SSL, ZERTJSSE provider, z/OS OpenSSH, and z/OS IPsec** are enabled for zERT advisory observation)
- Reported through **SMF 119 records** via:
  - **SMF** and/or
  - **Real-time** network management interfaces (NMIs)

unprotected* = no protection that zERT recognizes

zERT features

z/OS Encryption Readiness Technology (zERT)

zERT Discovery
(z/OS Communications Server)

Generates **SMF Type 119 subtype 11 "zERT Connection Detail" records**

- These records describe the complete **cryptographic protection history** of each TCP and EE connection
- **At least 1 record is written for each connection** - and each describes all cryptographic protection for that connection
- Well suited for **real-time monitoring** applications
- Often generated in very high volumes

zERT Aggregation
(z/OS Communications Server)

Generates **SMF 119 Type 119 subtype 12 "zERT Summary" records**

- These records describe the repeated use of security sessions over time
- Writes **1 zERT Summary record at the end of each recording interval for each security session** active during the interval
- Well suited for **reporting and analysis**
- Can greatly reduce the volume of SMF records (over Discovery) while providing the same level of cryptographic detail

zERT Network Analyzer
(z/OSMF)

Web-based (z/OSMF) UI to query and analyze zERT Summary (subtype 12) records.

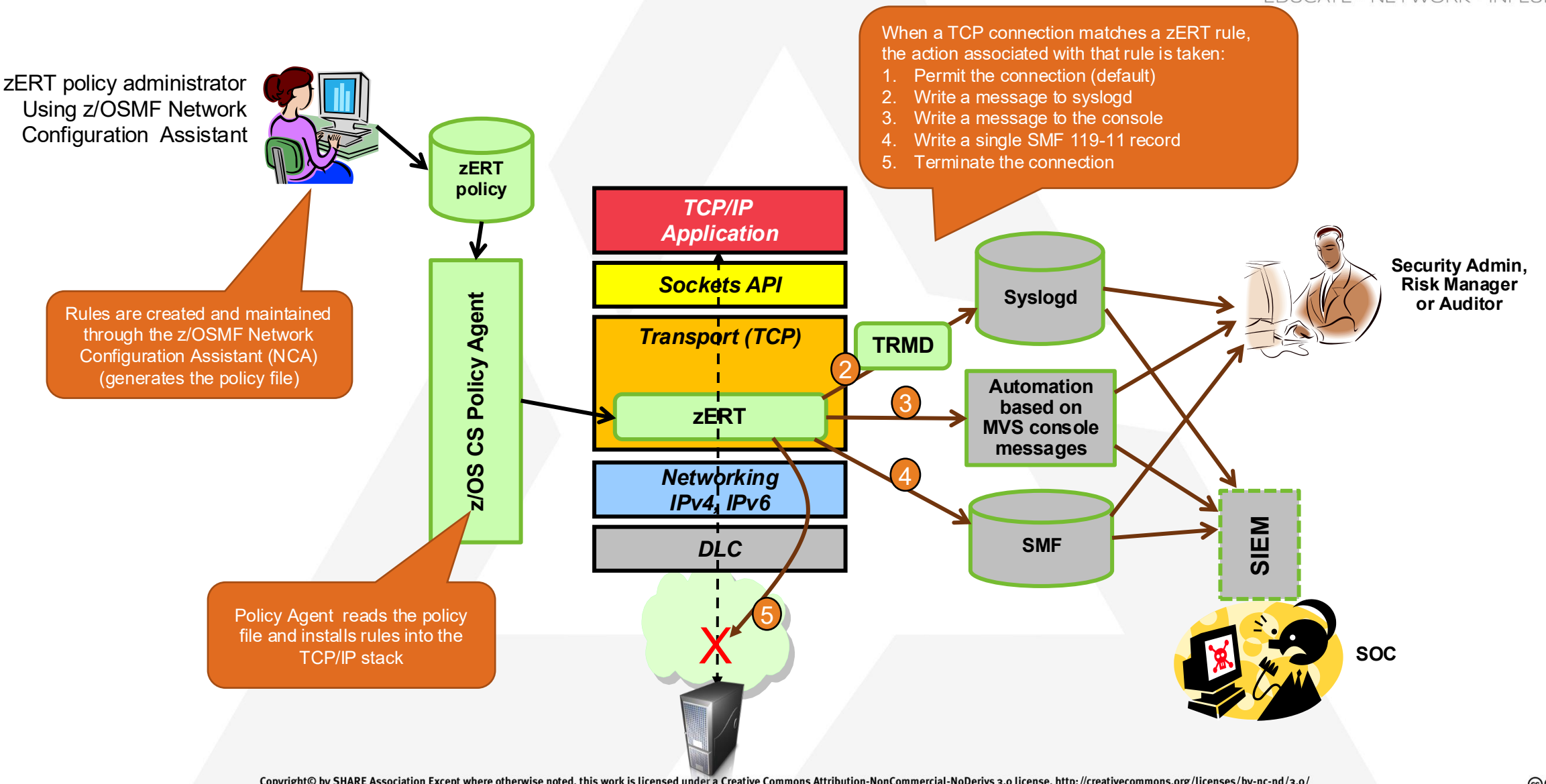
- The latest network analyzer PTF always contains an up-to-date fresh install image
- Intended for z/OS network security administrators (typically systems programmers)
- Comes with z/OS Communications Server at no extra charge, but **relies on Db2 for z/OS**

zERT Policy-based Enforcement
(z/OS Communications Server)

Real-time monitoring based on user-written policy rules

- Provides **notification or even defensive actions** when insufficient cryptographic protection is recognized
- z/OSMF Network Configuration Assistant used to create rules

zERT: Enforcement architecture



zERT: Products that consume zERT SMF data

The zERT Network Analyzer is NOT the only way to view zERT data!

IBM is aware of the following products that have shipped support for zERT data. Note that this **should not be considered to be a comprehensive list** as there may be others of which IBM is currently unaware:

Vendor & Product	119-11	119-12	Notes
IBM zSecure Audit	X	X	
IBM QRadar SIEM	X	X	Supports what zSecure feeds it
IBM IntelliMagic Vision		X	
IBM Z Common Data Provider	X	X	
IBM NetView Version	X		Through NMI
IBM Omegamon for Networks on z/OS	X		Through NMI
IBM Z Performance and Capacity Analytics	X	X	
Merril Technologies MXG	X	X	Feeds into SAS
Broadcom NetMaster Network Management for TCP/IP	X		Through NMI
Broadcom Compliance Event Manager	X		
Vanguard Advisor	X		
Pacific Systems Group's Spectrum SMF Writer	X	X	
Black Hill Software EasySMF	X	X	
Vertali zTrust for Networks	X	X	Uses SMF records for discovery Can also use zERT Enforcement
EPS Pivotor	X	X	

SHARE
EDUCATE • NETWORK • INFLUENCE

SHARE update:

zERT monitoring enhancements

zERT monitoring and recording deficiencies

- z/OS 3.2 Communications Server has enhanced zERT to easily distinguish between TLS/SSH connections (successful and failed) and unprotected connections and provide all the information necessary to ensure that the network traffic is protected per network policy.

- **zERT monitoring enhancements are also available on z/OS V2R5 and z/OS 3.1 via APAR PH63197.**

- This addressed several open requirements:
  - Idea ZOS-I-3371 – Enable zERT to Detect Partial/Failed Secure Handshakes
  - Idea ZOS-I-339 – Certificate details, particularly serial and expiry date, on SMF119-12
  - Idea ZOS-I-3963 – Add Client/Server role indicator into ZERT SMF 119 Subtype 11 Records

zERT monitoring enhancements (1 of 3)

zERT monitoring is enhanced to take additional factors into account when deciding to write SMF records (SMF119-11 and 12):

1) Failed TLS / SSH handshakes

- Report TLS/SSH failed handshakes as TLS/SSH records with a flag/count that indicates the handshake failed
  - Easily distinguish between TLS/SSH connections (successful and failed) and unprotected connections
  - SMF 119-11 (zERT connection detail record) – new flags to indicate TLS/SSH handshake failed
  - SMF 119-12 (zERT summary record) – new counts of failed handshakes for the life of the security session at the beginning and end of the intervals
    - Note: When either of these fields is > 0, all the fields in the corresponding security session (TLS or SSH) section will contain binary zeroes or blanks except SMF119SS_TLS_Source and SMF119SS_TLS_Neg_Cipher (when TLS) or SMF119SS_SSH_Source (when SSH).

zERT monitoring enhancements (2 of 3)

2) Reduce the number of SMF 119-11 unprotected records that result from transient or unusual conditions

- **Handshake in progress**
  - If zERT has detected the beginnings of a handshake within the first 10 seconds, zERT will wait and not write a record until the handshake completes successfully / fails

- **TLS session ending and TCP connection is not terminated within 1 second**
  - When a TLS session is terminated, zERT will not write a record until the TCP connection is terminated (term or short-term record) or data flows on the TCP connection in the clear (protection state change record)

zERT monitoring enhancements (3 of 3)

3) Additional important security information

- Flag to indicate the **role of the local TCP socket** in SMF 119-11 “zERT Detail” records
- **Report end-entity certificate serial number and expiry information** in SMF 119-12 "zERT Summary" records (similar to what we do in SMF 119-11).

```
SMF119SS_<proto>_<x>Cert_Serial_Len
SMF119SS_<proto>_<x>Cert_Serial
SMF119SS_<proto>_<x>Cert_Time_Type
SMF119SS_<proto>_<x>Cert_Time
```

<proto> is either **IPSec** or **TLS**, while **<x>** can be one of

S for server certificate information

C for client certificate information

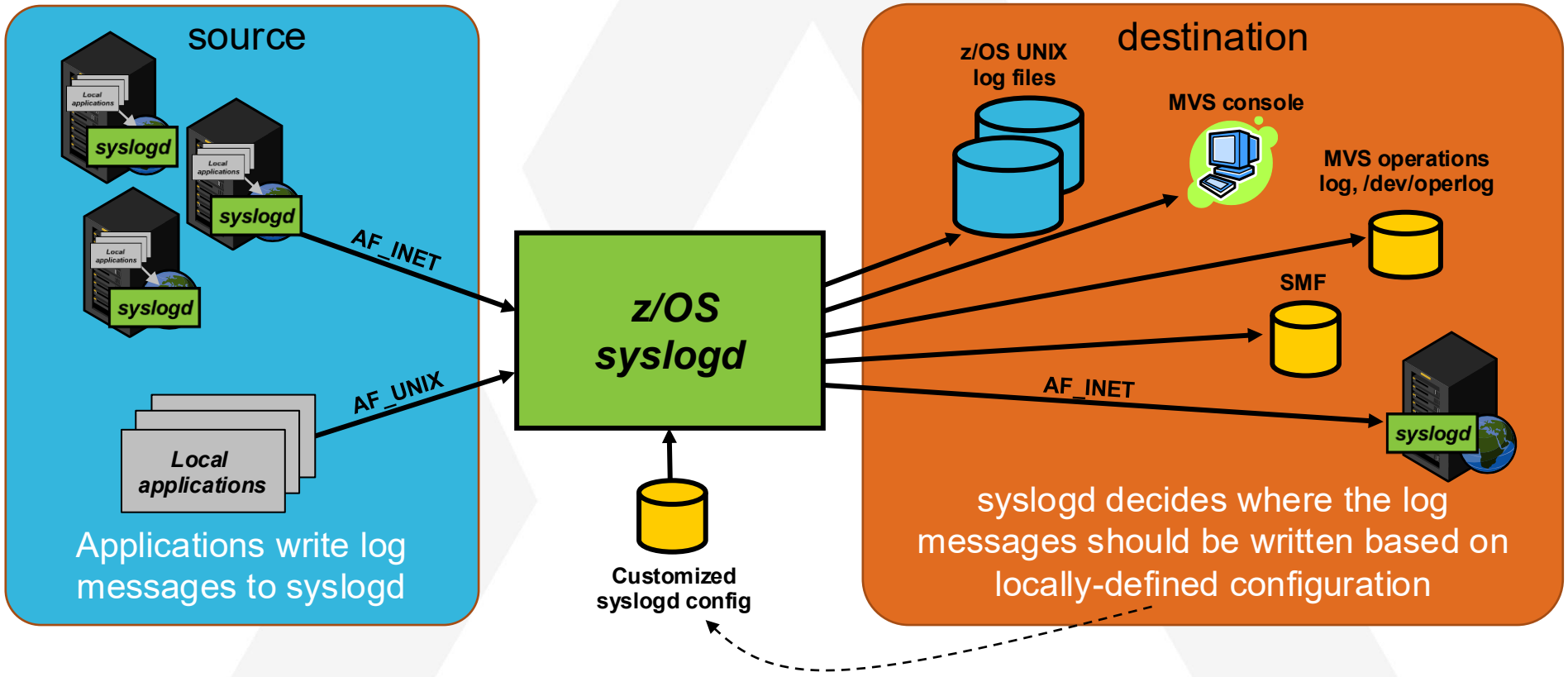
Lcl for IKE Local certificate information

Rmt for IKE Peer certificate information

For more on zERT…

Visit Things you should know about zERT on IBM Community and discover event information, video, product documentation, presentations and blogs about zERT.

Syslogd: Overview



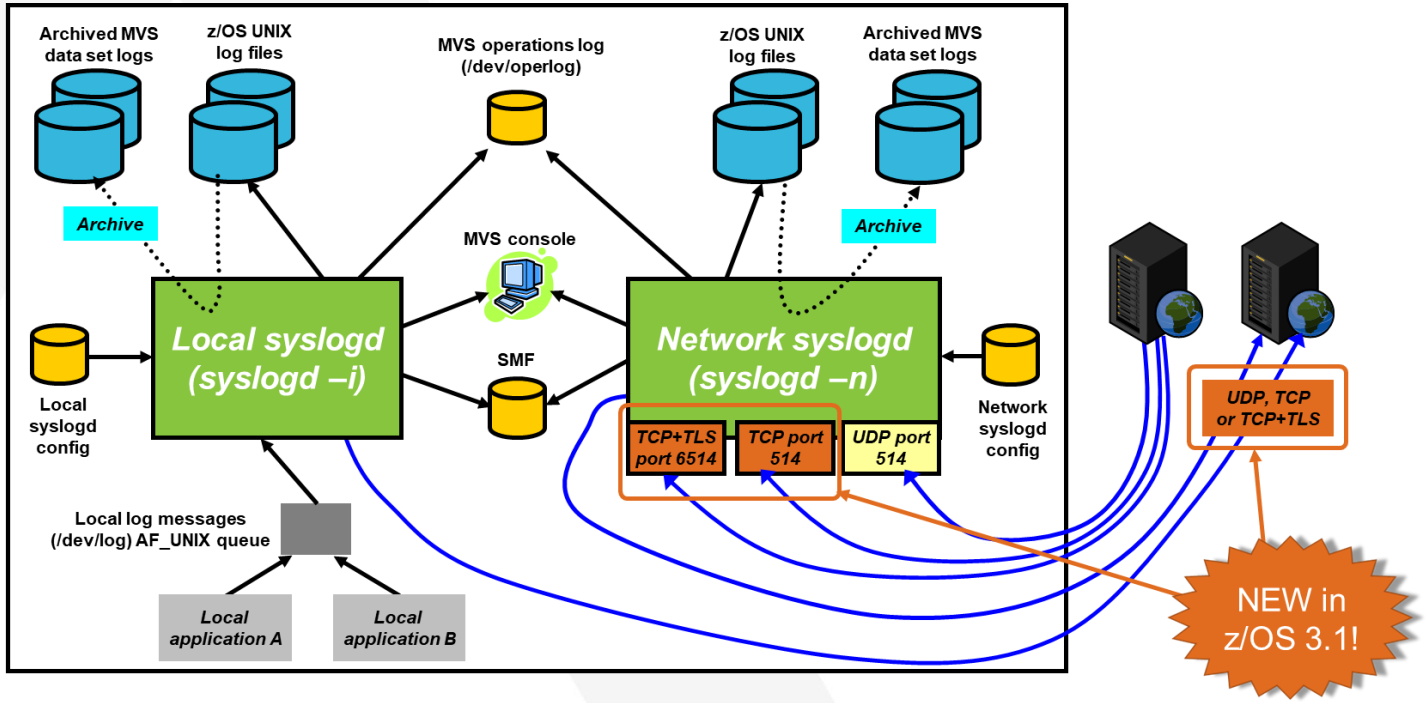
Some common z/OS Communications Server users of syslogd:

- FTP server and client
- AT-TLS
- Policy Agent
- CSSMTP (mail)
- Intrusion Detection Services (IDS)
- IP Security (IPsec, IKED, NSSD)
- OMPROUTE
- Several others

syslogd is an important part of your z/OS network security infrastructure!

Syslogd isolation: Ensuring availability of your log data

- **Syslogd integrity and availability goals**:
  - Prevent loss of important system log records due to flooding
    - From network
    - From runaway or malicious applications
  - Keep system log records separate from application log records
  - Automatically archive logs for long-term access

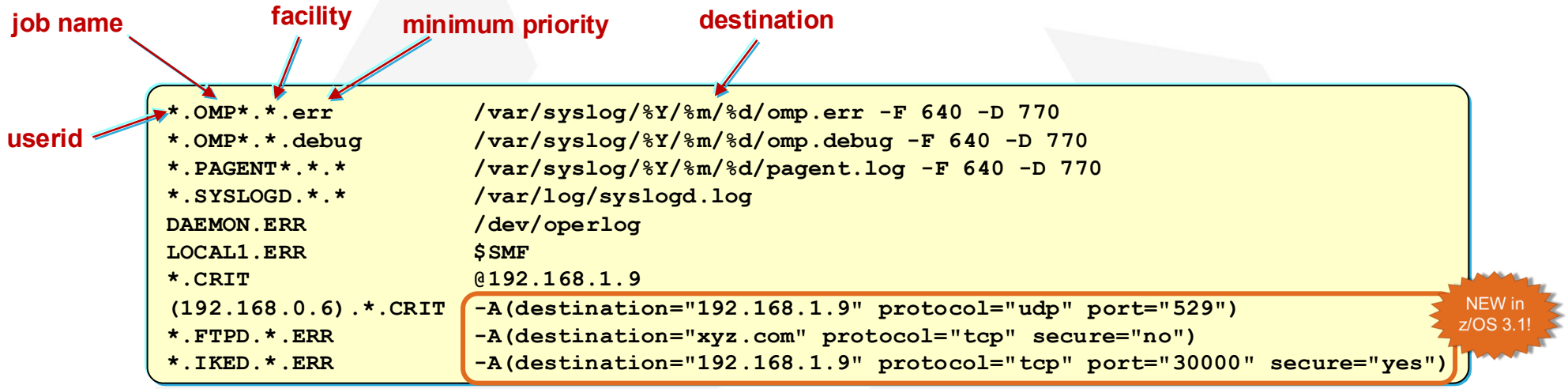


- **z/OS syslogd security controls provide:**
  - Protection from local z/OS users
    - Configuration directs syslogd messages to different destinations based on facility, priority, z/OS userID and/or jobname
    - userid/jobname can be logged for audit purposes
    - Configuration controls UNIX file permissions of created files and directories
  - Protection from the network
    - Encrypted connections to other syslogds over TCP with TLS protection
    - Configuration can disable reception of log messages over the network (while retaining the ability to send to other syslogd instances over the network)
    - IP packet filtering can be used to control which remote syslogds can connect to the local one

If you don't have syslogd configured to capture, file, and archive log data, then you should set it up as soon as you can!

Syslogd isolation: Controlling access and destinations

- syslogd processing is controlled through configuration file named /etc/syslog.conf
  - Defines logging rule conditions and output destinations
  - **Each destination has a dedicated thread**, so isolation improves throughput and reliability
- Logging rule conditions
  - facility, priority (provided by the application)
  - userid, jobname (provided by system for local logging)
  - hostname or IP address (provided by system for messages received from network)
- Logging rule destinations
  - Several types supported (z/OS UNIX file, a remote syslogd, console, SMF type 109 record, etc.)
  - Most common type is a local z/OS UNIX file



Agenda

- z/OS Communications Server Overview
  - Trends and requirements
  - Roles and objectives
  - Policy-based networking

- Steps for protecting TCP/IP, related resources and data in transit
  1. Blocking unwanted traffic: IP packet filtering
  2. Protecting against attacks: Intrusion Detection Services (IDS)
  3. Protecting data in the network: Network cryptographic protocols
  4. Audit trails: zERT and syslogd
  5. **Controlling access to TCP/IP resources: SAF SERVAUTH class**

- Summary

SAF protection: SERVAUTH class resources (1 of 2)

- The SERVAUTH resource class is used to protect a wide variety of TCP/IP unique resources

`EZB.resource_category.system_name.jobname.resource_name`
  - EZB designates that this is a TCP/IP resource
  - *resource_category* is a capability area to be controlled e.g. TN3270, Stack Access, etc.
  - *system_name* is the name of the system (LPAR) - can be wild-carded (*)
  - *jobname* is the jobname associated with the resource access request - can be wild-carded (*)
  - optional *resource_name* - one or more qualifiers to indicate name of resource to be protected - can be wild-carded (*)

- Define a SERVAUTH profile with universal access NONE and then permit authorized user IDs to have READ access to that profile
  - If using OEM security packages, beware of the differences between defined/not defined resource actions
- All the "traditional" SAF protection of datasets, authorized MVS and z/OS UNIX functions, etc. on a z/OS system applies to TCP/IP workload just as it applies to all other types of workload

SAF protection: SERVAUTH class resources (2 of 2)

There are 30+ different possible TCP/IP-related resource types to protect. Careful use of these can provide a significant level of security administrator-based control over use of TCP/IP-related resources on z/OS

- Command protection
  - ipsec
  - nssctl
  - pasearch
  - netstat
- Network management APIs
  - packet trace
  - realtime SMF data
  - connection data
- Application control
  - specific socket options and special-purpose APIs
  - NSS certificate, service, client access
  - FTP port, command access, HFS and JES access
  - TN3270 and DCAS access
  - Ability to register listening port with RPCBIND
- Other resource restrictions
  - Fast Response Cache Accelerator (FRCA) page load
  - SNMP subagent access
  - DVIPA controls

See z/OS Communications Server IP Configuration Guide chapter 3 for a complete list of SERVAUTH resources

SAF protection: Example: FTP JES mode control

The z/OS FTP server provides several operational modes:

- **SEQ** mode – for accessing MVS data sets
- **HFS** mode – for accessing the z/OS Unix file system
- **SQL** mode – to access Db2
- **JES** mode – to submit jobs and interrogate job output

JES mode has been noted by z/OS penetration testers as a way to introduce malware to an unprotected z/OS system.

APAR PH42618 (for V2R3, V2R4 and V2R5) adds a new SAF resource to easily and explicitly control access to FTP JES

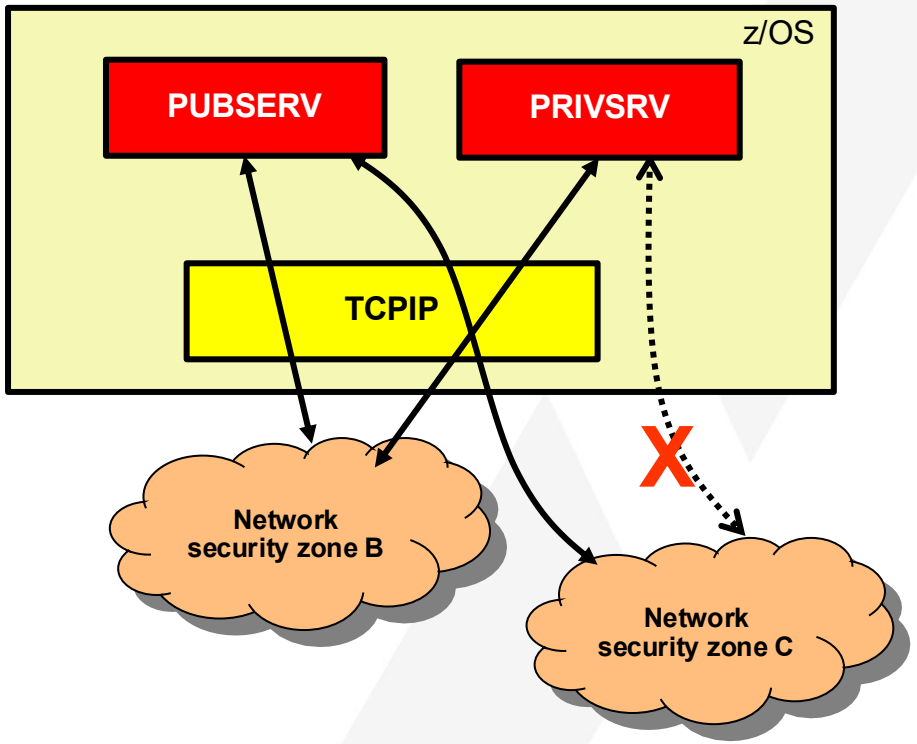
```
EZB.FTP.sysname.ftpdaemonname.ACCESS.JES
```

Users with access to this resource may enter JES mode. Without it, any attempt to enter JES mode is rejected:

```
200 - User username is not allowed to use FILETYPE=JES
```

Note: This resource is **NOT a replacement for the JESJOBS or JESSPOOL classes!** Those classes (and FTP JESINTERFACELEVEL 2) should still be implemented as they control JES access well beyond FTP.

SERVAUTH class: Example: NETACCESS controls




```
EZB.NETACCESS.*.TCPIPB.ZONEB
   All users permitted
EZB.NETACCESS.*.TCPIPB.ZONEC
   Only PUBSRV permitted
```

- Controls local user's access to network resources
  - bind to local address
  - send/receive IP packets to/from protected zone
  - Network
  - Subnet
  - Individual host
- NETACCESS statement in TCP/IP profile defines security zones. For example, stack B may have:

```
NETACCESS INBOUND OUTBOUND
  192.168.1.0     255.255.248.0 ZONEB
  192.168.0.0/16                ZONEC
  Default         0             WORLD
ENDNETACCESS
```

- Access to security zone is allowed if the user has access to the SERVAUTH class SAF resource associated with the zone:

  EZB.NETACCESS.*sysname.stackname.zonename*

  (Note that firewalls can't distinguish between individual users)

- In the example, PRIVSRV is not permitted to network security zone C

Agenda

- z/OS Communications Server Overview
  - Trends and requirements
  - Roles and objectives
  - Policy-based networking

- Steps for protecting TCP/IP, related resources and data in transit
  1. Blocking unwanted traffic: IP packet filtering
  2. Protecting against attacks: Intrusion Detection Services (IDS)
  3. Protecting data in the network: Network cryptographic protocols
  4. Audit trails: zERT and syslogd
  5. Controlling access to TCP/IP resources: SAF SERVAUTH class

- **Summary**

Summary

- Protect system resources FROM the network
  - IP packet filtering
  - Integrated Intrusion Detections Services
  - Built-in self-defense protection
  - SAF protection of z/OS resources
  - Auditability
- Protect data IN the network (cryptographically)
  - Cryptographic network protocols
  - Strong cryptography using IBM Z hardware crypto features
  - Integrated Intrusion Detection Services
  - SAF protection of z/OS resources
- Audit and logging across security functions

You will likely end up using a combination of technologies to meet all your security requirements.

Start today - don't wait for the first security disaster to happen!

For more information

URL	Content
http://www.youtube.com/user/zOSCommServer	IBM Communications Server on YouTube
http://tinyurl.com/zoscsblog	IBM Communications Server blog
https://www.ibm.com/docs/en/zos/3.1.0?topic=zos-communications-server	IBM Communications Server library

Digital Badges & Online Courses

Start your free z/OS online learning and earn IBM open badges!

Networking on z/OS - Foundations

Foundational understanding of networking on z/OS.

- **IBM Open Badge:** https://ibm.biz/zosnetworkingbadge
- **Online course:** https://ibm.biz/zosnetworkingcourse

z/OS TCP/IP Configuration with NCA

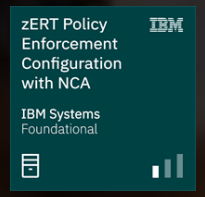
Use the IBM Configuration Assistant for z/OS Communications Server (NCA) to create and manage TCP/IP profiles.

- **IBM Open Badge:** http://ibm.biz/NCAbadge
- **Online course:** http://ibm.biz/NCATCPIPcourse

z/OS Network Security - Foundations

Knowledge and foundational understanding of z/OS network security.

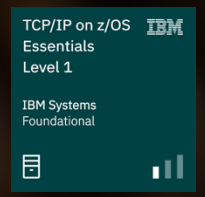
- **IBM Open Badge:** http://ibm.biz/zosnetsecuritybadge
- **Online course:** http://ibm.biz/zosnetsecuritycourse



zERT Policy Enforcement Configuration with NCA

Configure zERT Policy Enforcement using the IBM Configuration Assistant for z/OS Communications Server (NCA)

- **IBM Open Badge:** http://ibm.biz/NCA_zERTbadge
- **Online course:** http://ibm.biz/NCA_zERTcourse



TCP/IP on z/OS Essentials - Level 1

General knowledge and understanding of TCP/IP on z/OS, including network layers, protocols at each layer, and the hardware that facilitates the transport of data.

- **IBM Open Badge:** http://ibm.biz/tcpipl1badge
- **Online course:** https://ibm.biz/tcpipl1course

Experience more with IBM

Visit us at the IBM Booth #113

After a full day of technical sessions, take a break with us!

Connect with our experts, snap a photo with the z17 Plexi or the latest Telum II, and get an up-close look at our Spyre Accelerator.

Come back each day for fresh topics and demos at our expert stations.

Think 2026

Join 5000+ senior business and technology leaders who are seizing the AI revolution to unlock unprecedented growth and productivity at Think 2026.

Find out more information using the QR code below.

IBM Digital Asset Haven

IBM Digital Asset Haven is the operational backbone for financial institutions and regulated enterprises entering the digital asset economy.

Find out more information using the QR code below.

Want to attend an in-person IBM z/OS Academy?

Learn, **Interact** and **Network** with IBMers and peers

May 5th- 7th, 2026	**Fall 2026**
IBM Tech Campus	**IBM US**
Ehningen, Germany	**New York, USA**

These **free** events are designed for early tenure z/OS system programmers (2-10 years), but all are welcome!

Training and presentations include topics on new z/OS capabilities, best practices, career tips, and **much more!**
Subscribe to the community page today to stay informed about future events!

Register now for Ehningen/ Germany:

Join our IBM Community: https://ibm.biz/zOSAcademy
Questions? Contact us at zOS.Academy.USA@us.ibm.com **or** zOS.Academy.Europe@de.ibm.com

SHARE Security Warrior Digital Badge

- Explore all eligible sessions in the technical agenda
  - Filter ‘Digital Badge’ for ‘Security Warrior’

- Earn a Security Warrior digital badge
  - Attend **10** eligible sessions
  - Submit a Security Warrior badge form (more information available here)
  - Claim your badge via email from SHARE HQ

Session 300 – TCP/IP Security Controls

Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation