Chris Meyer, CISSP – meyerchr@us.ibm.com
June, 2019

# z/OS Communications Server Network Security Overview

# Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and 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 remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including 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 results similar to those stated here.

# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

z/OS Encryption Readiness Technology (zERT)

SAF Protection of TCP/IP Resources – SERVAUTH class

Summary

# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

z/OS Encryption Readiness Technology (zERT)

SAF Protection of TCP/IP Resources – SERVAUTH class

Summary

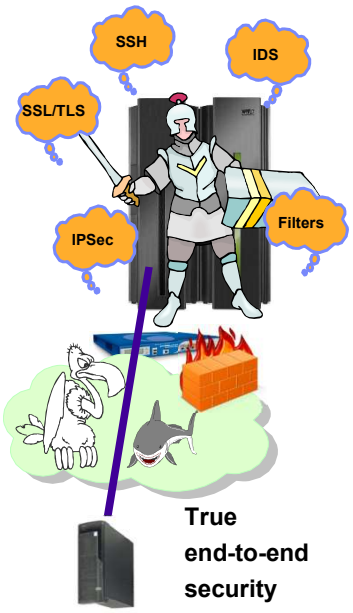
# Network security trends and requirements

- More “defense in depth”
  - Security is no longer perimeter-based
  - Server is the last layer of defense
- Regulatory compliance and tighter IT security policies
  - Corporate, industry and government standards (PCI-DSS, HIPAA, GDPR, etc.)
  - Driving many enterprises to adopt new security practices and understand existing security posture
  - Data privacy is a common theme – drives end-to-end crypto
- Increasing adoption of network security at the endpoint
  - TLS/SSL and IPSec deployments steadily increasing on z/OS
  - “Self-protect” features like IP packet filtering and IDS
- Focus on minimizing security deployment costs
  - Application transparent network security features and policy-based configuration reduce deployment costs
  - GUI-based policy administration for ease of use and faster deployment

# Role of network security on z/OS

- 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 cleartext 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**

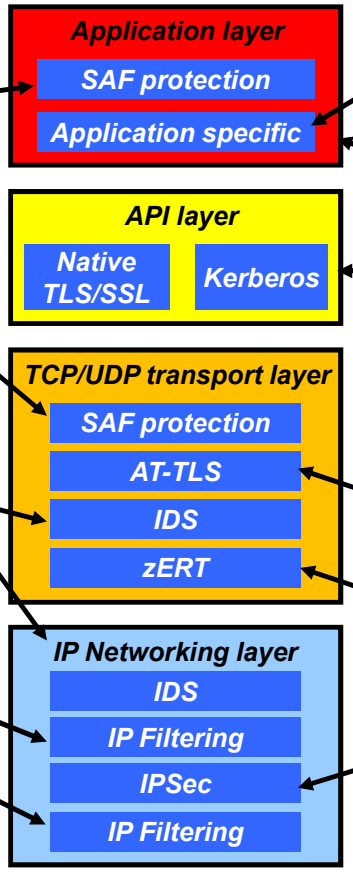
z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources.

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

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 filtering blocks IP traffic that this system doesn't specifically permit.

IP filtering is also used to control which traffic must use IPSec.




**Protect data in the network**

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

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

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

AT-TLS is a TCP/IP stack service that provides TLS/SSL services at the TCP transport layer and is transparent to applications.

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

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

# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

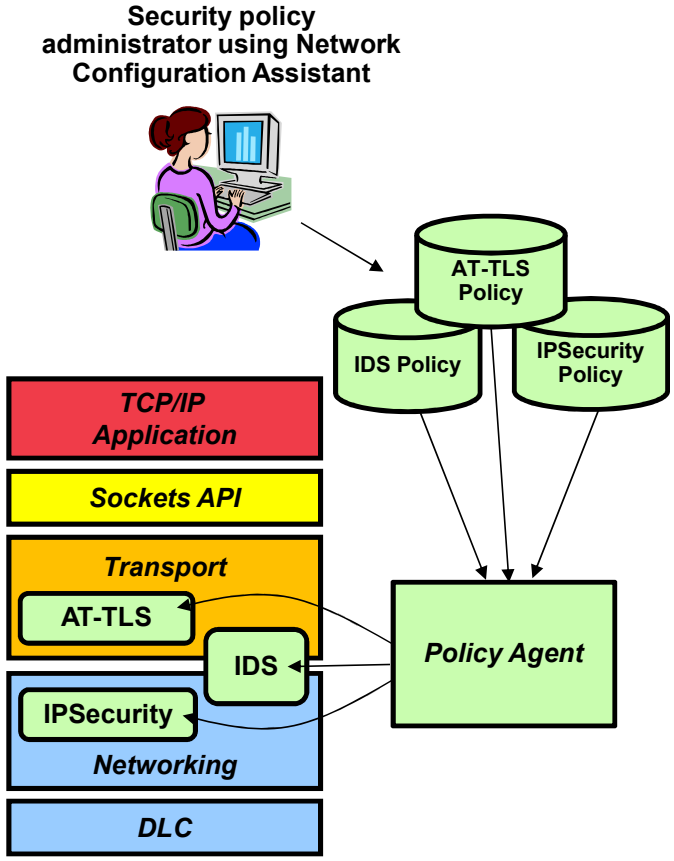
z/OS Encryption Readiness Technology (zERT)

SAF Protection of TCP/IP Resources – SERVAUTH class

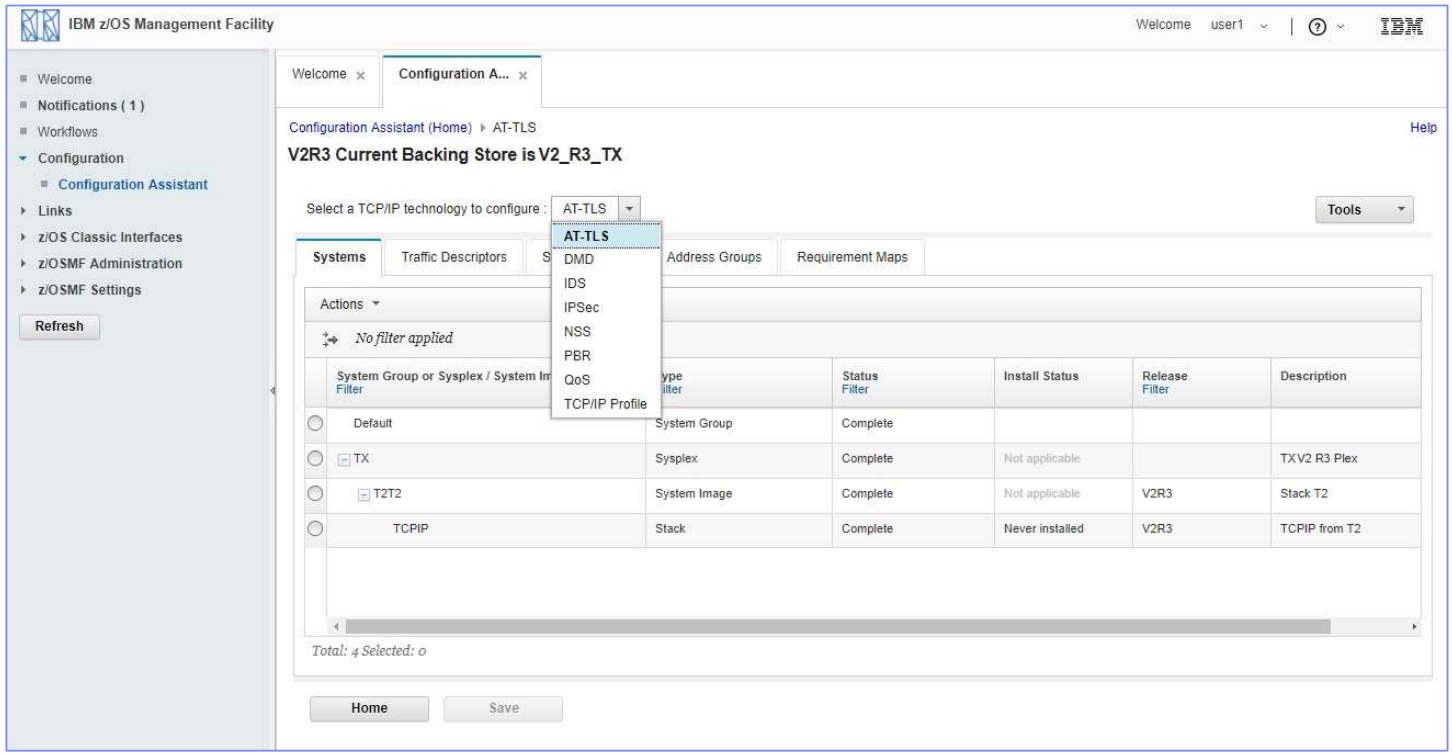
Summary

# Policy-based network security on z/OS

- Policy is created through Network Configuration Assistant for z/OS Communications Server
  - GUI-based tool
  - Configures each security discipline (AT-TLS, IP security and IDS) using consistent model
  - 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 and processes needed to enforce the policies (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 z/OS Communications Server




- z/OSMF-based web interface
- Configures all policy disciplines and TCP/IP profile
- Separate perspectives but consistent model for each discipline

- 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 import of existing profiles and policy files
- Supports current z/OS release plus past two
- Actively imports certain configuration information

# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

z/OS Encryption Readiness Technology (zERT)

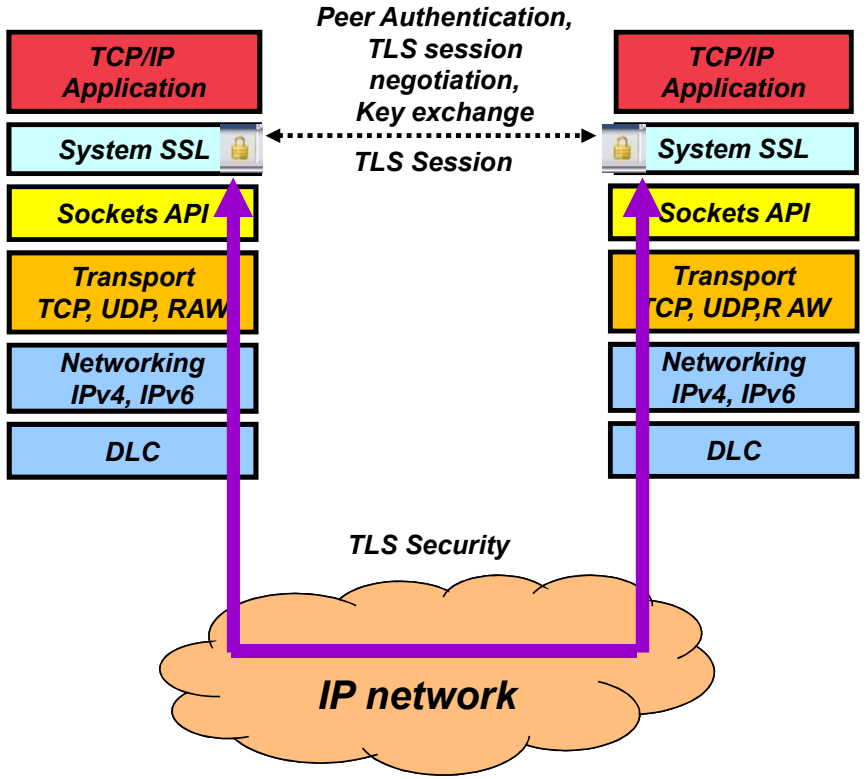
SAF Protection of TCP/IP Resources – SERVAUTH class

Summary

# AT-TLS: Traditional TLS/SSL

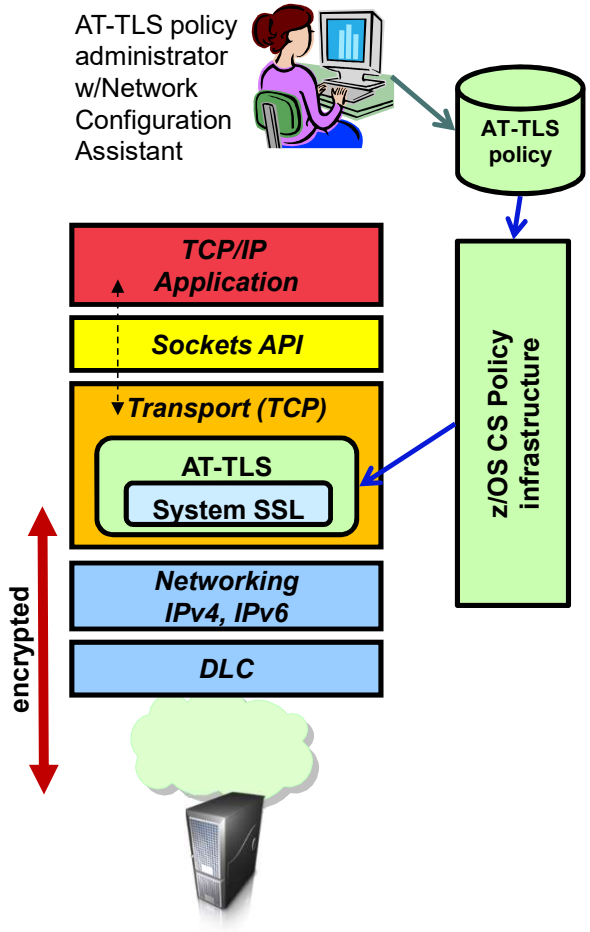
- Transport Layer Security (TLS) is an IETF standard based on Netscape's old proprietary Secure Sockets Layer (SSL) protocol
  - All new development of the protocol is under the IETF's domain and defined as new TLS versions.
  - The newest protocol version is TLSv1.3 – just approved in August, 2018 (RFC 8446)
- TLS traditionally provides security services as a socket layer service. Applications must be modified to call these services
- TLS requires a reliable transport protocol
  - Typically TCP
  - UDP applications cannot be enabled with TLS
- z/OS supports two complete TLS/SSL implementations:
  - z/OS Cryptographic Services System SSL provides an API library for C and C++ applications
  - Java Secure Sockets Extension (JSSE) provides classes for Java applications
- However, there is an easier way…

… Application Transparent TLS (AT-TLS)!



# AT-TLS: AT-TLS overview

- Policy-based TLS in the TCP/IP stack
  - TLS process performed in TCP layer (via System SSL) without requiring any application change (transparent)
  - AT-TLS policy specifies which TCP traffic is to be TLS protected based on a variety of criteria
    - Local address, port
    - Remote address, port
    - Connection direction
    - z/OS userid, jobname
    - Time, day, week, month
- Application transparency
  - Can be fully transparent to application
  - An optional API allows applications to inspect or control certain aspects of AT-TLS processing – “application-aware” and “application-controlled” AT-TLS, respectively
- Available to TCP applications
  - Includes CICS Sockets
  - Supports all programming languages except PASCAL
- Supports all standard configurations
  - z/OS as a client or as a server
  - Server authentication (server identifies self to client)
  - Client authentication (both ends identify selves to other)
- Relies on System SSL for TLS protocol processing
  - Remote endpoint sees an RFC-compliant implementation
  - Interoperates with other compliant implementations



# AT-TLS: Common workloads

- Communications Server applications
  - TN3270E Telnet server
  - FTP client and server
  - CSSMTP
  - Load Balancing Advisor
  - IKED (when operating as an NSS client)
  - NSS server
  - Policy Agent
  - DCAS server
- DB2 for z/OS
- IMS Connect
- InfoSphere Guardium S-TAP
- CICS Transaction Server 5.3+ (when operating as a server)
- IBM Multi-Site Workload Lifeline
- JES2 Network Job Entry
- RACF Remote Resource Sharing Facility
- z/OS CIM server
- IBM Security zSecure
- IBM Tivoli NetView applications
  - MultiSystem Manager
  - NetView Management Console
- IBM Tivoli Monitoring applications
  - Tivoli Enterpise Portal Server
  - Tivoli Enterprise Monitoring Server
- CICS Sockets applications
- 3rd Party applications
- Customer-written applications

# AT-TLS: Advantages

- **Reduce costs**
  - Application development
  - Cost of System SSL integration
  - Cost of application's TLS-related configuration support
  - Consistent TLS administration across z/OS applications
  - Gain access to new features with little or no incremental development cost


- **Complete and up-to-date exploitation of System SSL features**
  - AT-TLS makes the vast majority of System SSL features available to applications
  - AT-TLS keeps up with System SSL enhancements – as new features are added, your applications can use them by changing AT-TLS policy, not code

- **Performance**

  Focus on efficiency in use of System SSL

- **Great choice if you haven't already invested in System SSL integration**

  … **and even if you have**, consider the long-term cost of keeping up vs. short term cost of conversion

# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

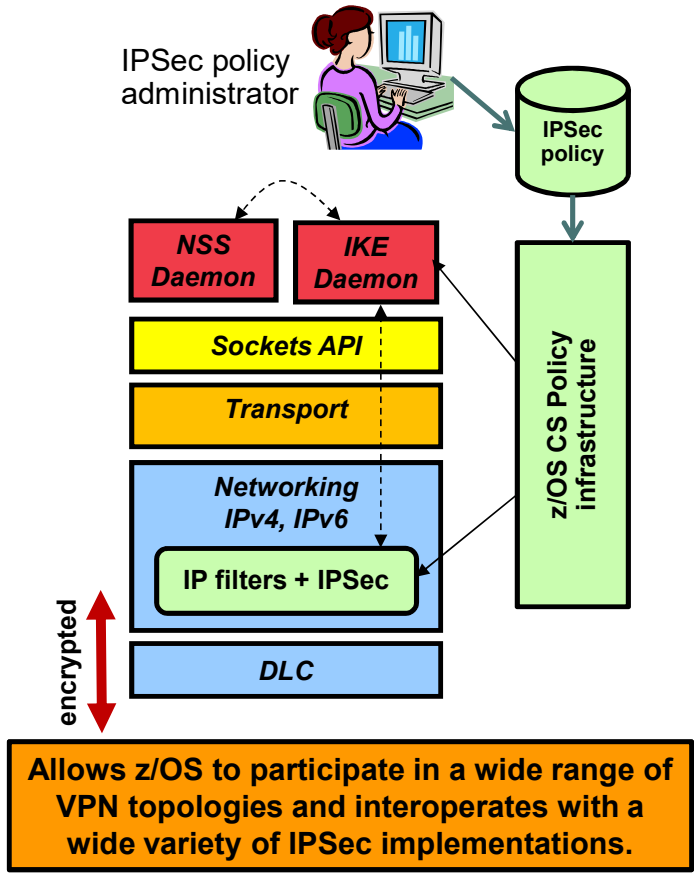
z/OS Encryption Readiness Technology (zERT)

SAF Protection of TCP/IP Resources – SERVAUTH class

Summary

# IP Security: Capabilities

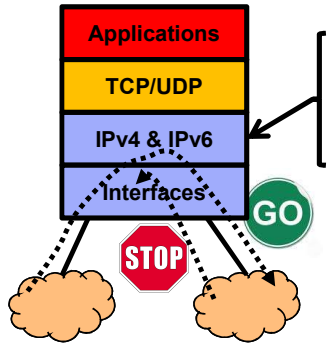
- A complete IP filtering, IPsec and IKE implementation
  - IP filtering controls which packets can enter or leave the system
  - Authentication Header (AH) and Encapsulating Security Payload (ESP) Security Associations (SAs)
  - Transport and Tunnel Mode
  - Supports host and gateway roles (optimized for host role)
  - IKE version 1 and version 2 (RFC 5996)
  - Filter-directed logging of security actions to syslogd
- Wide range of modern cryptographic algorithms including AES (multiple modes), SHA2, SHA1, RSA, ECDSA, etc.
- Complies with U.S. Government IPv6 profiles for IPsec, ESP and IKEv2
- zIIP assisted
  - Moves IPSec processing from general CPs to zIIPs
  - All inbound traffic and a good portion of outbound
- Supports NAT Traversal and NAPT for IPv4
- Sysplex-wide Security Associations allow IPsec SAs to be shared across the sysplex
- IP Security monitoring interface: IBM Tivoli OMEGAMON XE for Mainframe Networks



# IP Security: IP packet filtering

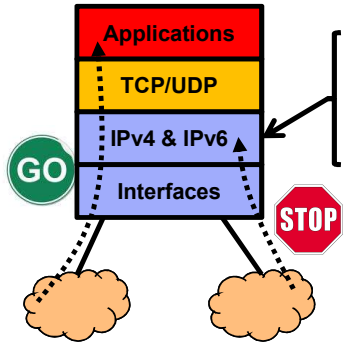
- IP filtering at the z/OS IP Layer
  - Filter rules defined based on relevant attributes :
    - IPv4 or IPv6 source/destination address
    - Protocol (TCP, UDP, ICMP, etc.)
    - Source/destination Port
    - Direction of flow
    - Local or routed traffic
    - Time
    - Network interface
  - Used to control
    - Traffic being routed
    - Access at destination host (local)
  - Possible actions when a filter rule is matched:
    - Permit
    - Deny
    - Permit with IPSec protection
    - Log (in combination with above actions)
- IP filter rules are defined within IPSecurity policy
  - This policy also controls IPSec if you choose to use it
  - Rudimentary “default rules” can also be defined in TCPIP profile to provide protection before policy agent initializes
- Benefits for local traffic (self-protection)
  - Early discard of potentially malicious packets
  - Avoid wasting CPU cycles on packets for applications that are not supported on this system
  - Prevent data leakage for outbound traffic

***Routed Traffic***




- Traffic routed through this TCP/IP stack
- Does not apply to Sysplex Distributor connection routing
- Note: z/OS is not stateful when filtering routed traffic.

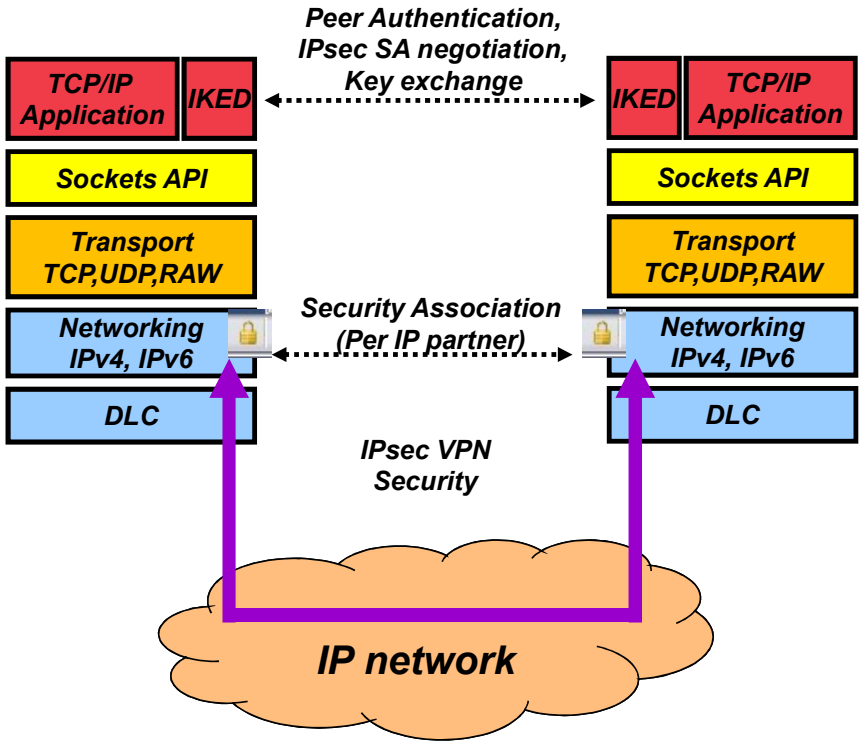
***Local Traffic***




- Traffic going to or coming from applications on this TCP/IP stack only

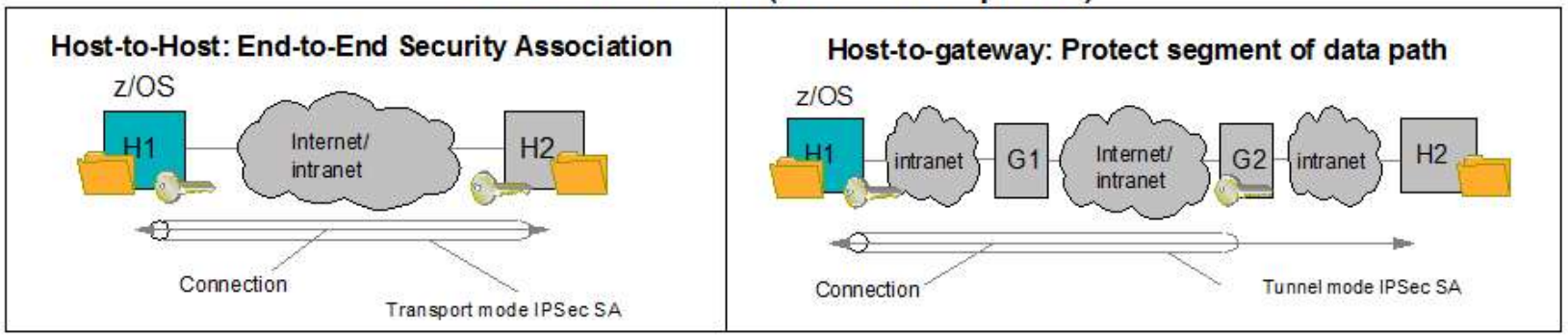
# IP Security: The IPsec protocol

- Implemented at the IP (network) layer
  - Completely transparent to application
  - Supports all IP traffic, regardless of higher-layer protocols
- Node-to-node protection via “Security Associations” (SAs)
- Data protection:
  - Authentication Header (AH) provides data authentication and integrity protection
  - Encapsulating Security Payload (ESP) provides data authentication, integrity and encryption
- Management of crypto keys and security associations:
  - Dynamic through Internet Key Exchange (IKE) protocol based on IPSecurity policy
  - Manual
- Partner authentication via digital certificates using IKE protocol

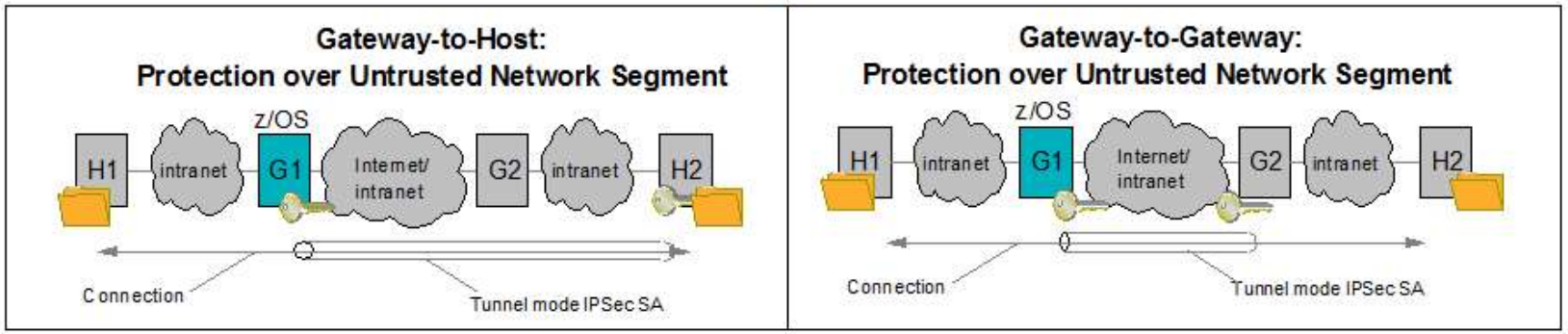


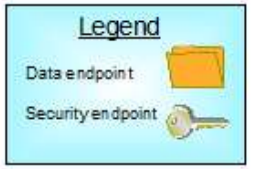
# IP Security: IPsec scenarios and z/OS roles

## z/OS as Host (Data Endpoint)




## z/OS as Gateway (Routed Traffic)



# IP Security: Common IPsec use cases

Enterprise Extender (SNA applications over an IP network)
- Since EE uses UDP/IP, TLS/SSL is not a viable option
- IPsec is used heavily and very successfully in the industry for protecting EE traffic
- IPSec protection can be set up for very specific EE traffic – even down to the specific EE ports if so desired

IBM Data Analytics Accelerator (IDAA)
http://www.ibm.com/support/docview.wss?uid=swg27047011&aid=1

Internet Control Message Protocol (ICMP and ICMPv6)
- These are their own IP protocols
- Used for things like neighbor discovery, path validation, etc.

…or most other IP-based prootcols

UDP-based protocols, such as:
- Domain Name System (DNS)
- Network File System (NFS), Remote Procedure Call (RPC) and Portmapper (can be run over UDP)
- Simple Network Management Protocol (SNMP)

TCP-based protocols whose implementations typically do not support TLS/SSL, such as:
- sendmail / SMTP
- Line Print Daemon (LPD)

Another excellent application of IPSec we have seen is blanket protection of all traffic between two nodes (especially within the data center)
- Example: encrypt everything between IP addr A and IP addr B
- True pervasive encryption of data in flight

# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

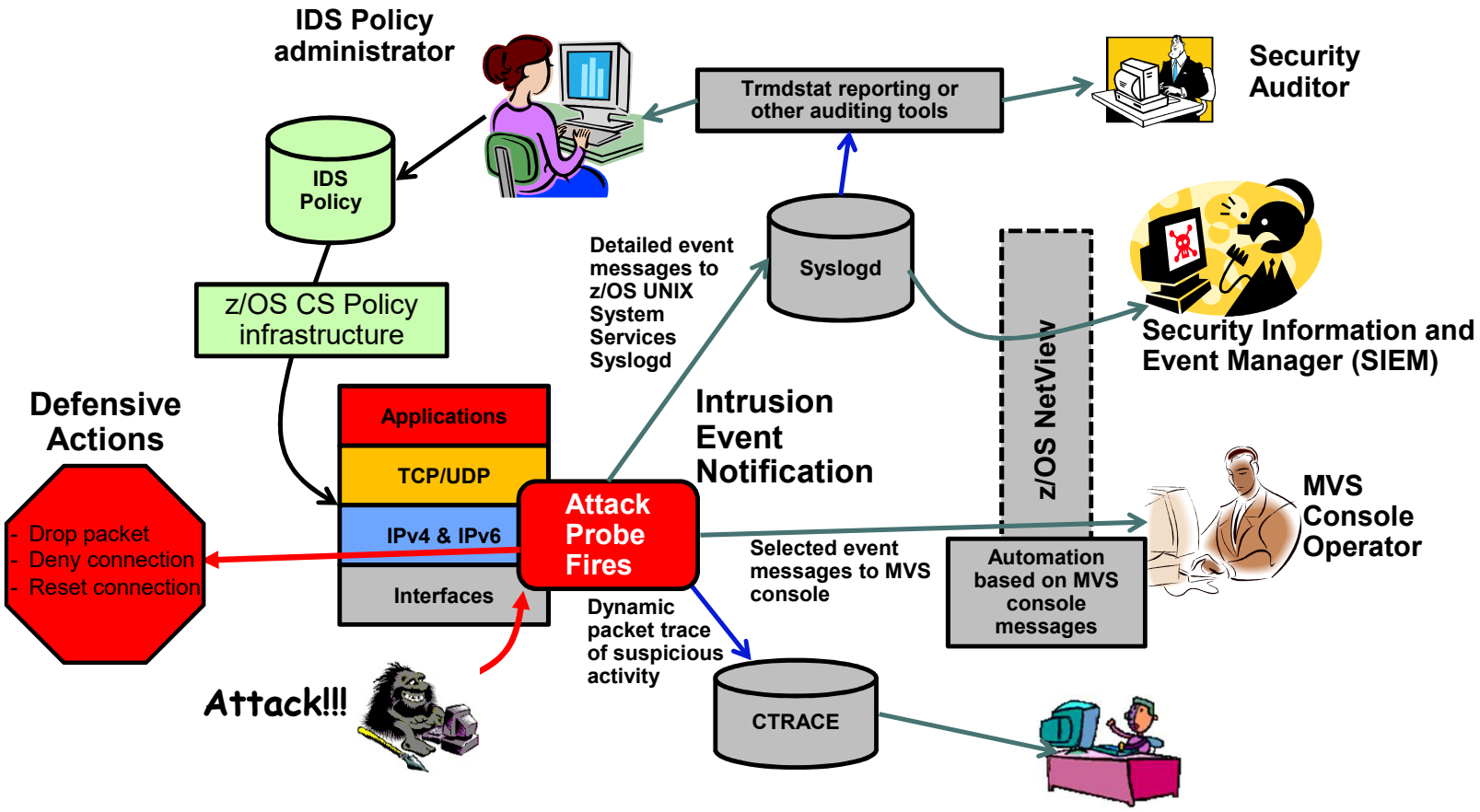
Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

z/OS Encryption Readiness Technology (zERT)

SAF Protection of TCP/IP Resources – SERVAUTH class

Summary

# IDS: z/OS TCP/IP IDS overview



# IDS: z/OS TCP/IP IDS features

**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**

**Defensive actions**

- Packet discard
- Limit connections
- Drop connections

**Reporting**

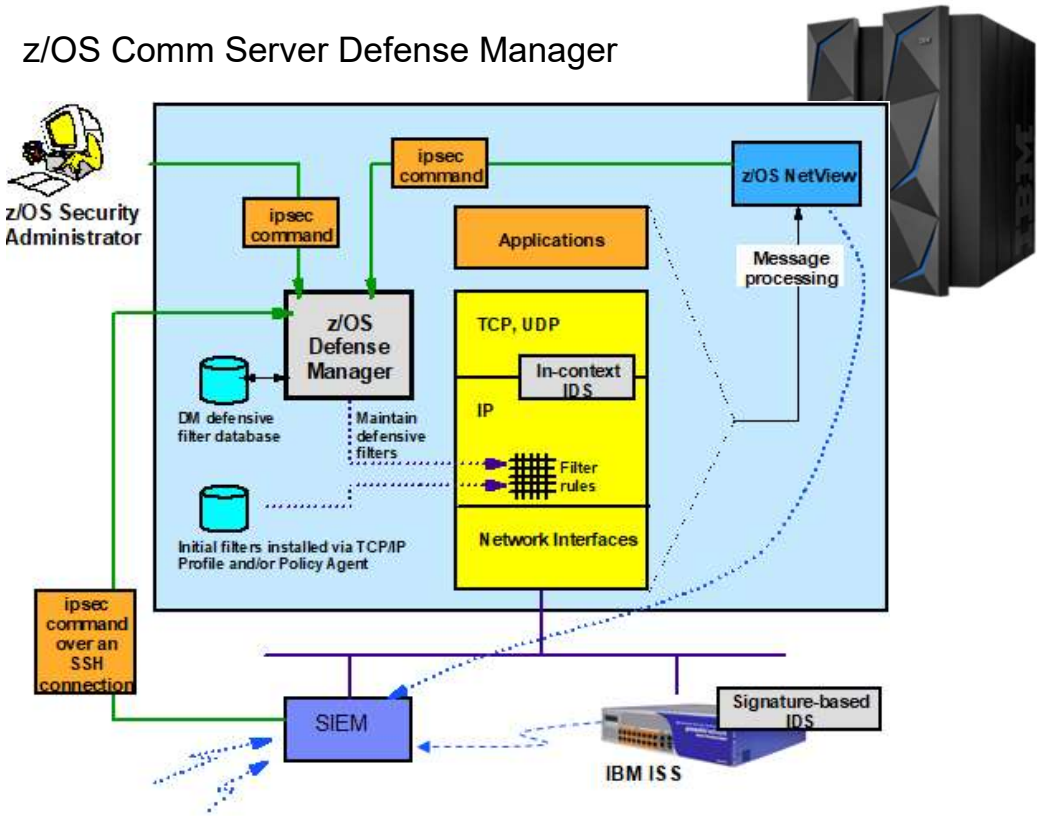
- Logging
- Console messages
- IDS packet trace
- Notifications to external event managers (like Tivoli NetView and SIEMs)

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

- In-context means as the communications end point, not as an intermediary
- Ability to evaluate inbound encrypted data - IDS applied after decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks - IDS policy checked after attack probe fires
- Detects statistical anomalies realtime - target system has stateful data / internal thresholds that generally are unavailable to external IDSs
- Policy can control prevention methods on the target, such as connection limiting and packet discard

# IDS: Defensive filtering with the Defense Manager Daemon (DMD)

- Defensive filters enable dynamic defensive actions in case of attack
- NOT policy-based, but created, managed and controlled through the ipsec command
- NOT part of IDS, but can be used within automation for IDS event processing
- DENY only (but also “simulate mode”)
- Installed “in front of” all other IP filters
- Maintained on DASD to protect restarted stacks from the time they come up
- Limited lifetime (~2 weeks max)
- Selectable scope:
  - Local – applies to a specific stack
  - Global – applies to all stacks on LPAR
- One Defense Manager Daemon per LPAR



# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

z/OS Encryption Readiness Technology (zERT)

SAF Protection of TCP/IP Resources – SERVAUTH class

Summary

# zERT: Cryptographic network protection on z/OS

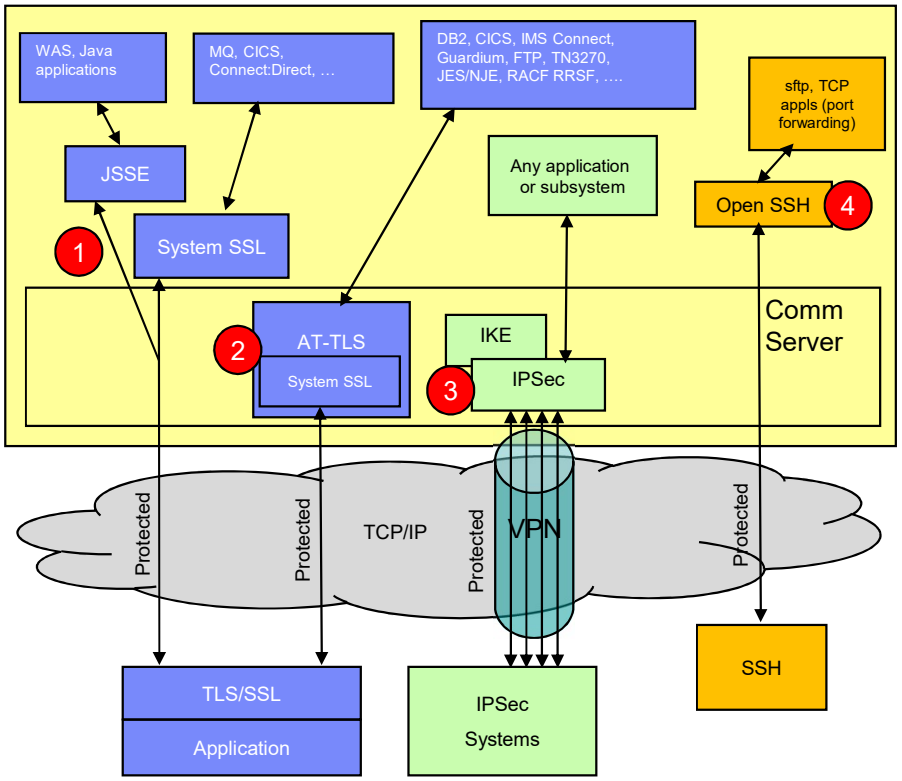
**z/OS provides 4* main mechanisms to protect TCP/IP traffic:**

1. **TLS/SSL direct usage**
   - Application is explicitly coded to use these
   - Configuration and auditing is unique to each application
   - Per-session protection
   - TCP only

2. **Application Transparent TLS (AT-TLS)**
   - TLS/SSL applied in TCP layer as defined by policy
   - Configured in AT-TLS policy via Configuration Assistant
   - Auditing through SMF 119 records
   - Typically transparent to application
   - TCP/IP stack is user of System SSL services

3. **Virtual Private Networks using IPSec and IKE**
   - “Platform to platform” encryption
   - IPSec implemented in IP layer as defined by policy
   - Auditing through SMF 119 records – tunnel level only
   - Completely transparent to application
   - Wide variety (any to all) of traffic is protected
   - Various topologies supported (host to host, host to gateway, etc.)
   - IKE negotiates IPSec tunnels dynamically

4. **Secure Shell using z/OS OpenSSH**
   - 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
   - Auditing via SMF 119 records
   - TCP only




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

# zERT: Why zERT?

- Given all of the workloads, crypto protocols, and variation in configuration and auditing on z/OS, how can you tell…
  - Which traffic is being protected (and which is not)?
  - How is that traffic being protected?
  - Who the traffic belongs to?
  - Whether existing and new configurations adhere to my company's security policies?

- zERT is design specifically to answer the above questions
  - Positions the TCP/IP stack as a central collection point and repository for cryptographic protection attributes of all:
    - **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:
    - TCP stream observation (for TLS, SSL and SSH) for all TCP connections
    - Advice of the cryptographic protocol provider (System SSL, ZERTJSSE, OpenSSH, z/OS IPsec support)
  - Reported through new **SMF 119 records** (through SMF or real-time services)
  - Provides a **web-based UI** (the zERT Network Analyzer) to analyze those records
  - Several IBM and ISV products have integrated support for zERT SMF data

# zERT: Functions

- zERT **Discovery**
  - **SMF 119 subtype 11 "zERT Connection Detail" records**
  - These records **describe the complete cryptographic protection history of each TCP and EE connection**
  - Writes at least one zERT Connection Detail record for every local TCP and EE connection
  - Covers all recognized cryptographic protocols in one record
  - Depending on your z/OS network traffic, these could be generated in very high volumes

- zERT **Aggregation** – available via V2R3 new function APAR PI83362
  - **SMF 119 subtype 12 "zERT Summary" records**
  - These records **describe the repeated use of security sessions over time**
  - Since the focus is a security session, each record is focused on a single cryptographic protocol
  - Writes one zERT Summary record at the end of each SMF interval for each security session that was active during the SMF interval
  - Can greatly reduce the volume of SMF records (over Discovery) while providing the same level of cryptographic detail

- zERT **Network Analyzer** - available via V2R3 new function APAR PH03137
  - **Web-based (z/OSMF) UI** to query and analyze zERT Summary (subtype 12) records
  - Intended for z/OS network security administrators (typically systems programmers)

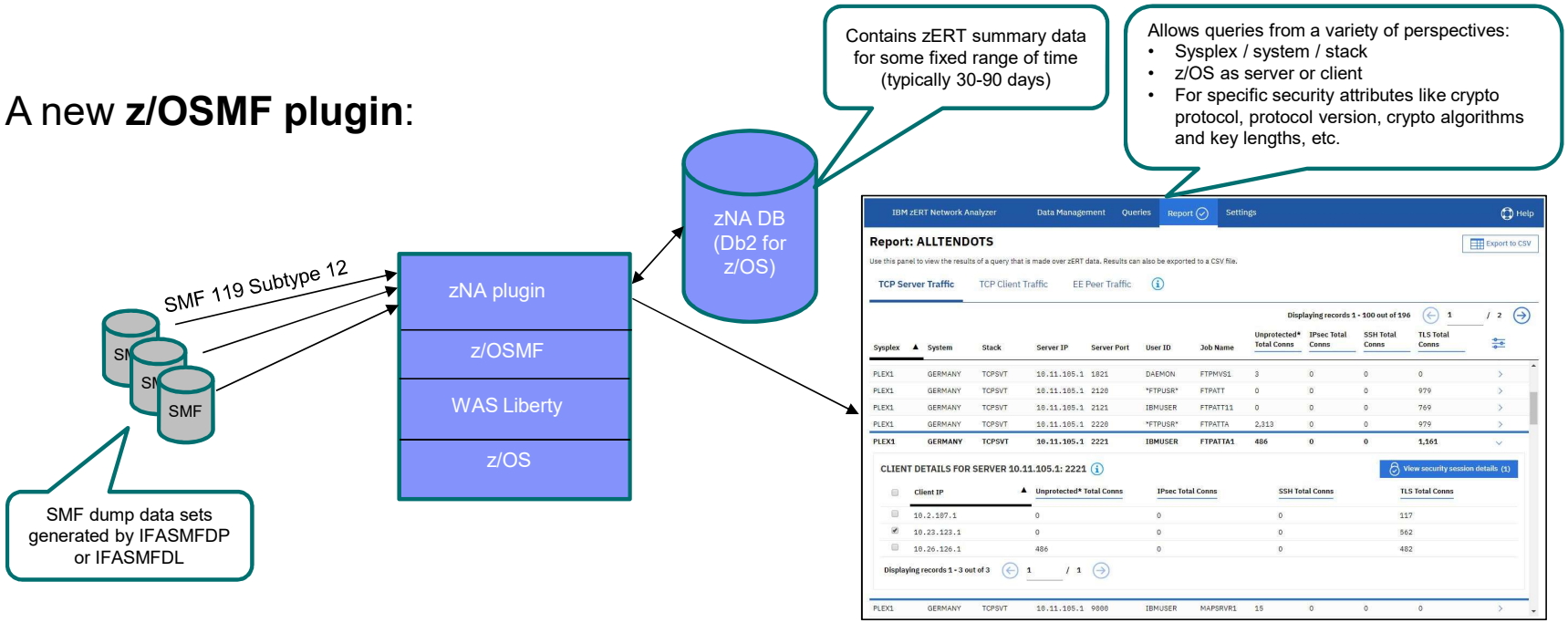
# zERT: What data is collected?

- Attributes of the connection and its security sessions
  - **Significant attributes**
    - Identifying attributes like IP addresses, ports, jobname, userid, etc.
    - Protection attributes like protocol version, cryptographic algorithms, key lengths, etc. Changes in these cause a protection state change record to be written if they change
  - **Informational attributes** like protocol session identifiers, session or certificate expiry data and certificate serial numbers are recorded for informational purposes only. When recorded, the values of such attributes are taken at the time the SMF record is written. Changes in these attributes do not constitute a significant change and will not result in the creation of a change event record
- **zERT does not collect, store or record the values of secret keys, initialization vectors, or any other secret values that are negotiated or derived during cryptographic protocol handshakes**

See the z/OS Communications Server IP Programmer's Guide for all the details

# zERT: Network Analyzer overview

- A new **z/OSMF plugin**:




- **Web UI** makes zERT data consumable for **z/OS network security administrators** (typically systems programmers)
- **Access to UI controlled through SAF** resource IZUDFLT.ZOSMF.ZERT_NETWORK_ANALYZER in the ZMFAPLA class
- Used primarily to investigate specific network encryption questions (but could also be used for periodic report generation)
- The IBM zERT Network Analyzer is available via **new function APAR PH03137**

# zERT: Network Analyzer – what data is available? (TLS and SSH)

**TLS Cryptographic Details**

- [x] Client IP
- [ ] Session ID
- [x] Protocol Version
- [x] Negotiated Cipher
- [x] Key Exchange Algorithm
- [x] Symmetric Encryption Algorithm
- [x] Message Authentication Algorithm
- [ ] ETM
- [ ] Source

**TLS Certificate Details**

- [x] Client IP
- [ ] Session ID
- [x] Server Certificate Signature Method
- [x] Server Certificate Asymmetric Encryption Algorithm
- [x] Server Certificate Digest Algorithm
- [x] Server Certificate Key Length
- [ ] Server Certificate Key Type
- [x] Client Certificate Signature Method
- [x] Client Certificate Asymmetric Encryption Algorithm
- [x] Client Certificate Digest Algorithm
- [x] Client Certificate Key Length
- [ ] Client Certificate Key Type

**TLS Distinguished Name Details**

- [x] Client IP
- [ ] Session ID
- [x] Server Certificate Issuer Distinguished Name
- [x] Server Certificate Subject Distinguished Name
- [x] Client Certificate Issuer Distinguished Name
- [x] Client Certificate Subject Distinguished Name

**TLS Traffic Details**

- [x] Client IP
- [ ] Session ID
- [x] Total Connections
- [x] Partial Connections
- [x] Bytes In
- [x] Bytes Out
- [x] Segments In
- [x] Segments Out

**SSH Cryptographic Details**

- [x] Client IP
- [ ] Session ID
- [x] Protocol Version
- [x] Key Exchange Algorithm
- [x] Symmetric Encryption Algorithm In
- [x] Symmetric Encryption Algorithm Out
- [x] Message Authentication Algorithm In
- [x] Message Authentication Algorithm Out
- [x] Authentication Method
- [ ] Authentication Method 2
- [x] Server Key Length
- [ ] Server Key Type
- [x] Client Key Length
- [ ] Client Key Type
- [ ] ETM In
- [ ] ETM Out
- [ ] Source

**SSH Certificate Details**

- [x] Client IP
- [ ] Session ID
- [x] Server Certificate Signature Method
- [x] Server Certificate Asymmetric Encryption Algorithm
- [x] Server Certificate Digest Algorithm
- [x] Server Certificate Key Length
- [ ] Server Certificate Key Type
- [x] Client Certificate Signature Method
- [x] Client Certificate Asymmetric Encryption Algorithm
- [x] Client Certificate Digest Algorithm
- [x] Client Certificate Key Length
- [ ] Client Certificate Key Type

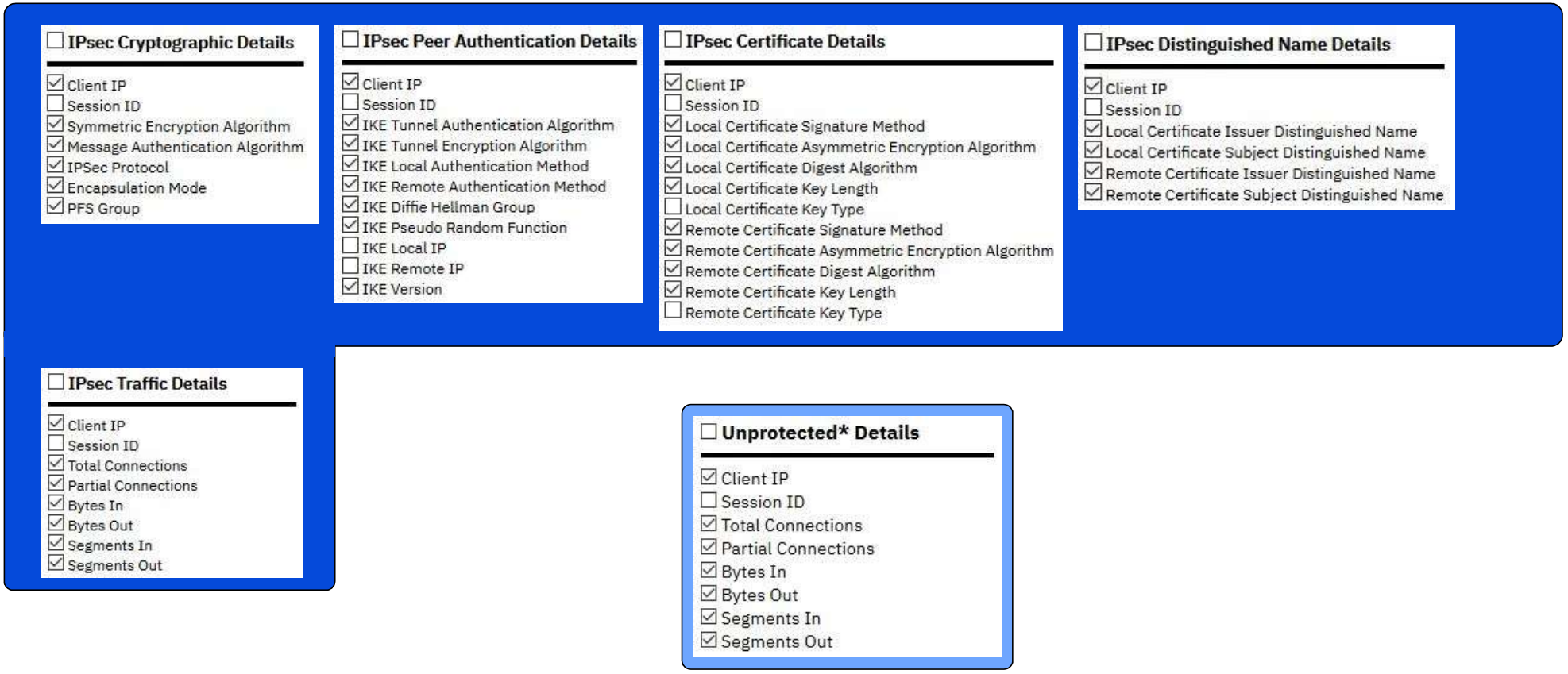
**SSH Distinguished Name Details**

- [x] Client IP
- [ ] Session ID
- [x] Server Certificate Issuer Distinguished Name
- [x] Server Certificate Subject Distinguished Name
- [x] Client Certificate Issuer Distinguished Name
- [x] Client Certificate Subject Distinguished Name

**SSH Traffic Details**

- [x] Client IP
- [ ] Session ID
- [x] Total Connections
- [x] Partial Connections
- [x] Bytes In
- [x] Bytes Out
- [x] Segments In
- [x] Segments Out

# zERT: Network Analyzer – what data is available? (IPsec and unprotected*)




* “Unprotected” means no recognized cryptographic protection was identified

# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

z/OS Encryption Readiness Technology (zERT)

SAF Protection of TCP/IP Resources – SERVAUTH class

Summary

# SAF protection: SERVAUTH class resources

- The SERVAUTH resource class is used to specifically define and protect a number of TCP/IP unique resources
- General SERVAUTH profile format:

**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.

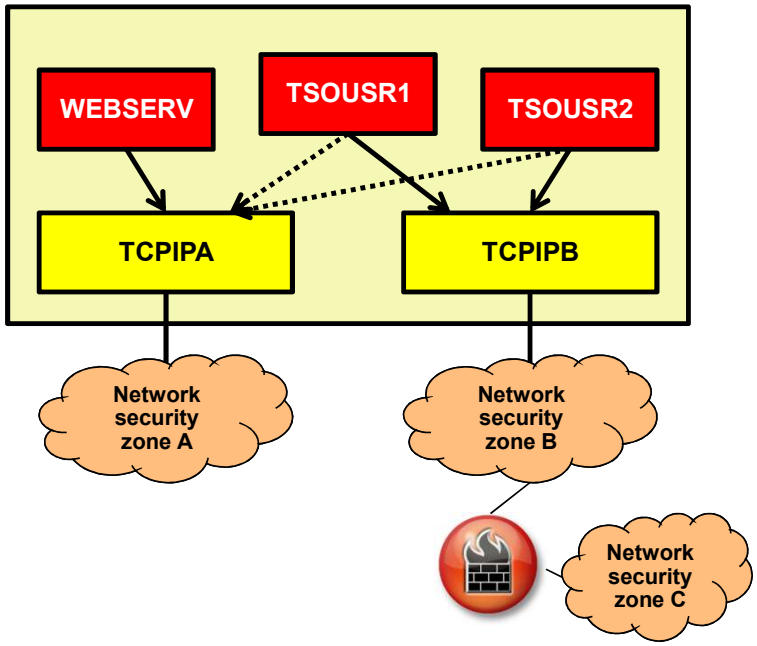
– system_name is the name of the system (LPAR) - can be wild-carded (*)

– 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 (*)

- To protect one of the supported TCP/IP resources, 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.
- Be careful with anonymous services such as anonymous FTP or TFTP services that can be configured to allow un-authenticated users access to selected MVS data sets and/or HFS files.

# SAF protection: STACKACCESS



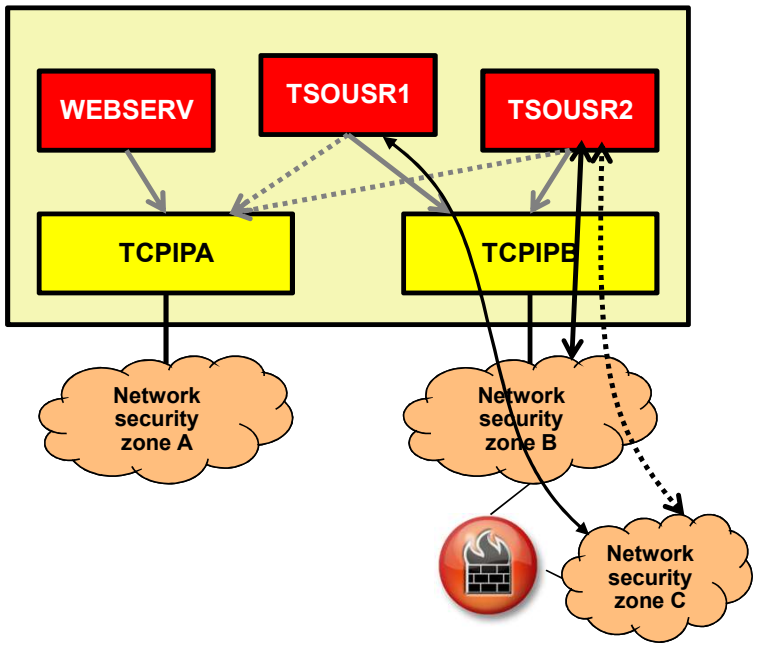

```
EZB.STACKACCESS.*.TCPIPA
```
WEBSRV permitted, all others not

- **Limits local users' open sockets or use of TCP/IP stack services (e.g., get hostname, get hostid, etc.)**
- **Access to stack via sockets is allowed if the user has access to the following SERVAUTH class SAF resource:**

**EZB.STACKACCESS.*sysname.stackname***

- **Define stack profile with UACC(NONE) and permit groups or individual users to allow them access to the stack**
- **In the example, TSOUSR1 and TSOUSR2 are not permitted to use TCPIPA**

# SAF protection: NETACCESS




```
EZB.STACKACCESS.*.TCPIPA
      WEBSRV permitted, all others not

EZB.NETACCESS.*.TCPIPB.ZONEC
      TSOUSR1 permitted, all others
```

- **Controls local user's access to network resources**
  - bind to local address
  - send/receive IP packets to/from protected zone
  - Network
  - Subnet
  - Individual host

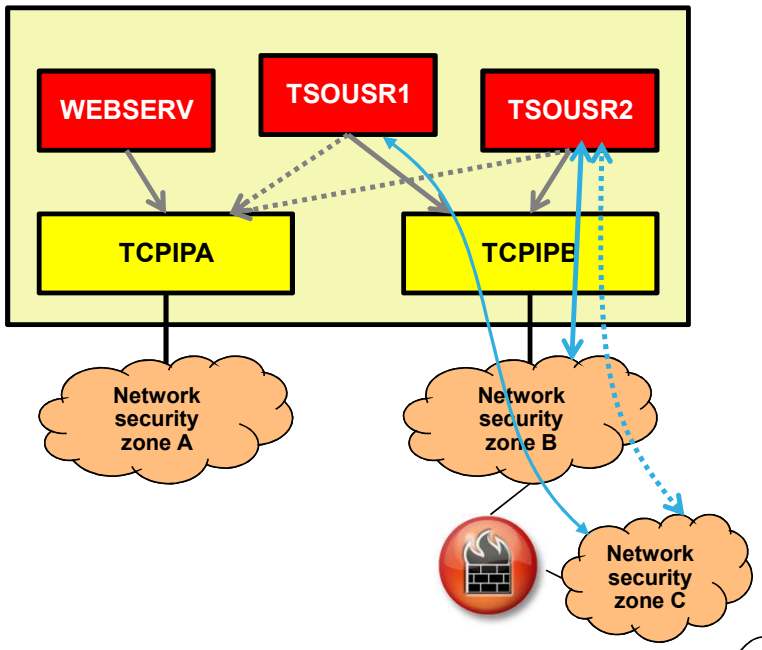
  **(Note that firewalls can't distinguish between individual users)**
- **Access to security zone is allowed if the user has access to the SERVAUTH class SAF resource associated with the zone:**

  **EZB.NETACCESS.*sysname.stackname.zonename***
- **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
```

- **In the example, TSOUSR2 is not permitted to network security zone C**

# SAF protection: PORTACCESS




```
EZB.STACKACCESS.*.TCPIPA
      WEBSRV permitted, all others not
EZB.PORTACCESS.*.TCPIPA.WEBPORT
      WEBSRV permitted, all others not
EZB.NETACCESS.*.TCPIPB.ZONEC
      TSOUSR1 permitted, all others
```

- **Limits local users' access to *non-ephemeral* ports**
- **Controls whether a started task or userid can establish itself as a server on a given TCP or UDP port.**
- **Access to use port is allowed if the user has access to the following SERVAUTH class SAF resource:**

```
EZB.PORTACCESS.sysname.stackname.SAFname
```

- **SAF keyword on PORT or PORTRANGE statement in TCP/IP profile defines SAF resource name. For example, stack A may have:**

```
PORT 80 TCP * SAF WEBPORT
```

- **RESERVED keyword on PORT or PORTRANGE statement prohibits access for all users.**
- **In the example, only userid WEBSRV is permitted to establish itself as a server on port 80 on stack TCPIPA**

# SAF protection: Other SERVAUTH resources

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
  - broadcast socket options
  - IPv6 advanced socket APIs
  - NSS certificate, service, client access
  - FTP port, command access and HFS access
  - DCAS access
- Other resource restrictions
  - Fast Response Cache Accelerator (FRCA) page load
  - SNMP subagent access
  - DVIPA modification control

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

# Agenda

Overview
- Roles and objectives
- Deployment trends and requirements

Policy-based Network Security
- Application Transparent TLS
- IP security (IP packet filtering and IPSec)
- Intrusion Detection Services (IDS)

z/OS Encryption Readiness Technology (zERT)

SAF Protection of TCP/IP Resources – SERVAUTH class

Summary

# Summary

**Protecting system resources from the network**

- Integrated Intrusion Detection Services detects, records, and defends against scans, stack attacks, flooding
- Protect system availability
  - Built in protection against Denial of Service attacks
  - IP packet filtering
  - Syslogd integrity and availability
  - Sysplex Wide Security Associations
- SAF protection of z/OS resources
  - z/OS CS application access to data sets and files
  - SERVAUTH class protection

**Protecting data in the network**

- True end-to-end security with security endpoint on z/OS
- Strong cryptographic algorithms using IBM Z hardware crypto features
- Transparent Application Security
  - IPSec for TCP/IP applications
  - Application-Transparent TLS support
  - Internet-ready access to SNA applications with TN3270 TLS/SSL
- Built-in Application Security
  - Kerberized FTP, rsh, telnet,
  - SNMPv3, Secure OSPF Authentication
- Complete auditing of network cryptographic protection through zERT


# Thank you!

# Notices and disclaimers (1 of 2)



**U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

**Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those

customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

# Notices and disclaimers (2 of 2)

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of 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. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

.