Session abstract

z/OS Communications Server Network Security Overview

Traditionally, network security has been placed at the enterprise perimeter. Enterprise security deployments are increasingly implemented with multiple layers of defense to protect mission critical data systems. While perimeter-based network security is still in force, the additional enablement of network security function at the server provides a critical layer of protection in the security infrastructure. This session will describe how z/OS Communication Server 'self-protects' z/OS from a network security perspective. Topics covered are drivers of network security function deployment into the server endpoint, as well as the policy-based network security solutions that are available on z/OS. The solution focus areas for this session include IPSec, Application Transparent TLS, integrated intrusion detection services, SAF protection of TCP/IP resource, centralized control of Communications Server network security, and integration of DataPower with z/OS security using the Communications Server Network Security Server.
Agenda

• **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
• **Enterprise-wide Security Roles**
  – Centralized Policy Agent
  – Network Security Services
• **SAF Protection of TCP/IP Resources**
  – SERVAUTH profiles for TCP/IP
Agenda

• **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

• **Enterprise-wide Security Roles**
  – Centralized Policy Agent
  – Network Security Services

• **SAF Protection of TCP/IP Resources**
  – SERVAUTH profiles for TCP/IP
Role of network security on System z

- Secure access to both TCP/IP and SNA applications
- Focus on end-to-end security and self-protection
- Exploit strengths of System z hardware and software

- Protect data and other resources on the system from the network
  - System availability
    - Protect system against unwanted access and denial of service attacks from network
  - Identification and authentication
    - Verify identity of network users
  - Access control
    - Protect data and other system resources from unauthorized access

- Protect data in the network using cryptographic security protocols
  - Data endpoint 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
    - Conceals cleartext using encryption
Recent network security deployment trends and requirements

- **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
  - Policy-based network security reduces deployment costs
  - GUI-based policy administration for ease of use

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

Protocol layer view of TCP/IP security technologies

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.

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 packet filtering blocks out all IP traffic that this system doesn't specifically permit. These can be configured or can be applied dynamically as “defensive filters”.

Protect data in the network

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

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

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

IP packet filters specify traffic that requires IPSec.

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

• 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

• Enterprise-wide Security Roles
  – Centralized Policy Agent
  – Network Security Services

• SAF Protection of TCP/IP Resources
  – SERVAUTH profiles for TCP/IP
Policy-based network security on z/OS overview

- **Policy is created through Configuration Assistant for z/OS Communications Server**
  - GUI-based tool
  - Configures each security discipline (AT-TLS, IPSecurity and IDS) using consistent model
  - Generates and uploads policy files 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
Configuration Assistant for z/OS Communications Server

- **Configures:**
  - AT-TLS
  - IPSec and IP filtering
  - IDS
  - Quality of Service
  - Policy-based routing

- **Separate perspectives but consistent model for each discipline**

- **Focus on concepts, not details**
  - What traffic to protect
  - How to protect it
  - De-emphasize low-level details (though they are accessible through advanced panels)

- **z/OSMF-based web interface (strategic) or downloadable standalone Windows application**

- **Builds and maintains**
  - Policy files
  - Related configuration files
  - JCL procs and RACF directives

- **Supports import of existing policy files**
IP Security
z/OS IP Security support

- z/OS IP Security is a complete IP filtering, IPSec, and IKE solution and is part of z/OS Communications Server

- **Services**
  - Protect the system from the network
    - IP filtering to control which packets can enter the system
  - Protect against data leakage from the system
    - IP filtering to control which packets can leave the system
  - Cryptographic protection of data in the network
    - Manual IPSec (statically defined security associations)
    - Dynamic negotiation of IPSec security associations using Internet Key Exchange (IKE)
  - Filter directed logging of IP Security actions to syslogd
IP packet filtering overview

- **IP filtering at the z/OS IP Layer**
  - Filter rules defined based on attribute of IP packets:
    - IPv4 or IPv6 source/destination address
    - Protocol (TCP, TCP with ACK, 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 checking validity of packets for applications that are not supported on this system
IPSec overview

- Provides authentication, integrity, and data privacy via IPSec security protocols
  - Authentication Header (AH) - provides authentication / integrity
  - Encapsulating Security Protocol (ESP) - provides data privacy with authentication / integrity
- Implemented at the 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
  - Dynamically negotiated via Internet Key Exchange (IKE) based on IP security policy
z/OS IPSec security features

- **A complete IPSec implementation**
  - 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)

- **Wide range of modern cryptographic algorithms including AES (multiple modes), SHA2, SHA1, RSA, ECDSA, etc.**

- **zIIP assisted**
  - Moves IPSec processing from general CPs to zIIPs
  - All inbound IPSec traffic and a good portion of outbound IPSec traffic is processed on a zIIP processor

- **Supports NAT Traversal and NAPT for IPv4**

- **Sysplex-wide Security Associations allow SAs to be shared across the sysplex**

- **IP Security monitoring interface: IBM Tivoli OMEGAMON XE for Mainframe Networks**

Allows z/OS to participate in a wide range of VPN topologies and interoperates with a wide variety of IPSec implementations.
IPSec Scenarios and z/OS Roles

z/OS as Host (Data Endpoint)

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

Host-to-gateway: Protect segment of data path

z/OS as Gateway (Routed Traffic)

Gateway-to-Host: Protection over Untrusted Network Segment

Gateway-to-Gateway: Protection over Untrusted Network Segment
Application Transparent TLS
 TLS traditionally provides security services as a socket layer service
  – TLS requires reliable transport layer,
    • Typically TCP (but architecturally doesn’t have to be TCP)
  – UDP applications cannot be enabled with traditional TLS
    • There is now a TLS variant called Datagram Transport Layer Security (DTLS) which is defined by the IETF for unreliable transports

• On z/OS, System SSL (a component of z/OS Cryptographic Services) provides an API library for TLS-enabling your C and C++ applications
• Java Secure Sockets Extension (JSSE) provides libraries to enable TLS support for Java applications
  – However, there is an easier way…

... Application Transparent TLS!
z/OS Application Transparent TLS overview

- **Stack-based TLS**
  - 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
  - Applications have option 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 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)

- **Uses System SSL for TLS protocol processing**
  - Remote endpoint sees an RFC-compliant implementation
  - Interoperates with other compliant implementations
Some z/OS applications that use AT-TLS

- **Communications Server 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**
Advantages of using AT-TLS

- **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

- **Ongoing performance improvements**
  Focus on efficiency in use of System SSL

- **Great choice if you haven’t already invested in System SSL integration**
  Even if you have, consider the long-term cost of keeping up vs. short term cost of conversion
z/OS AT-TLS Supported Roles

z/OS as Server

z/OS as Client

Server authentication only

Server + client authentication

System z security for today ... and tomorrow
## IPSec* and AT-TLS comparison

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

* - using IKE to establish IPsec tunnels dynamically
Intrusion Detection Services
Protecting against intentional and unintentional attacks on your system

• **What is an intrusion?**
  – Information Gathering
    • Network and system topology
    • Data location and contents
  – Eavesdropping/Impersonation/Theft
    • On the network/on the host
    • Base for further attacks on others through Amplifiers, Robots, or Zombies
  – 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 may not be sufficient.
    • Some access is permitted from Internet – typically into a Demilitarized Zone (DMZ)
    • Trust of intranet

• **Attacks can be intentional (malicious) but often occur as a result of errors on nodes in the network (config, application, etc.)**
z/OS Communications Server IDS overview

IDS Policy administrator

z/OS CS Policy infrastructure

Applications
TCP/UDP
IPv4 & IPv6
Interfaces

IDS Policy

Security Auditor

Syslogd

Security Administrator

MVS Console Operator

Network Engineer – detailed P/D

Defensive Actions
Discard packet
Deny connection
Reset connection

CTRACE
Dynamic packet trace of suspicious activity

Trmdstat reporting or other auditing tools

Intrusion Event Notification Actions

Selected event messages to MVS console messages

Detailed event messages to z/OS UNIX System Services Syslogd

Attack Probe Fires

Attack!!!
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… including several new attack types introduced in V1R13

- **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 (V1R13)

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

z/OS in-context IDS broadens overall intrusion detection coverage:
- Ability to evaluate inbound encrypted data - IDS applied after IPSec decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks - IDS policy checked after attack 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
Defense Manager enables dynamic defensive actions

- The z/OS Communications Server 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

Defensive filters...
- DENY only
- Limited lifetime (max ~2 weeks)
- Installed "in-front" of configured/default filters
- Maintained on DASD for availability in case of DM restart or stack start/restart
- Scope may be:
  - Global - all stacks on the LPAR where DM runs
  - Local - apply to a specific stack
- One Defense Manager per LPAR
- Use of ipsec command to display and control defensive filters is secured via SAF security profiles
Centralized Policy Agent
and
Network Security Services
Network Security Administration and Monitoring at Each System

- Each z/OS system locally administered
  - Monitoring
  - RACF certificate administration
  - Policy configuration

- Connectivity required between administration and each managed platform
  - Monitoring application has advance knowledge of each managed node
  - Coordination required to push policy out to each system for deployment
Centralized networking security policy management

- **Network security policy governs actions by security enforcement points**
  - IPSec, TLS, IDS/IPS

- **Policy agent roles**
  - Centralized policy service provided by policy agent that has role of **policy server**
  - Policy agents that obtain policy from policy server have role of **policy client**
  - A single policy agent can be a policy client or policy server but not both
Centralized Network Security Services for IPSec

- **Centralized IPSec network security services for a set of z/OS images**
  - Images can be non-sysplex, within sysplex or cross sysplex
- **NSS digital signature services**
  - Allows central administration of SAF certificates and private keys
    - Sign and verify during runtime IKE negotiations
- **NSS monitoring interfaces**
  - Allows selection of single focal point as IPsec management hub
    - `ipsec` command for administrator
    - Network Monitor Interface (NMI) for management application

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

NSS is required for ALL IKEv2 certificate services
Extending NSS – Integrating DataPower with z/OS security

**WebSphere DataPower Appliances**
- Performs advanced WebServices operations
- Message format transformation for traditional z/OS applications
- Offloads XML and WebServices security function

**NSS XMLAppliance discipline** enables both logical and physical integration between DataPower and z/OS security.

- **DataPower accesses centralized SAF services via z/OS NSS for:**
  - **SAF access service**: Provides SAF-based authentication (of DP users) and access control (of DP resources) with SMF auditing
  - **Certificate service**: Provides retrieval of RSA certificates from a SAF keyring
  - **Private key service** provides:
    - Private RSA key retrieval (clear key only)
    - RSA signature and decryption operations (secure key only)

- **z/OS security administered through z/OS security facilities such as RACF (SAF), ICSF**
Agenda

• **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
• **Enterprise-wide Security Roles**
  – Centralized Policy Agent
  – Network Security Services
• **SAF Protection of TCP/IP Resources**
  – SERVAUTH profiles for TCP/IP
SERVAUTH Protection for TCP/IP

- 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.
- 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 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, you define a SERVAUTH profile with universal access NONE and you then permit authorized user IDs to have READ access to the resource
- If using OEM security packages, beware of the differences between defined/not defined resource actions
STACKACCESS

- 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 resource 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

**EZB.STACKACCESS.*.TCPIPA**

- WEBSRV permitted, all others not
NETACCESS

- 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

---

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

EZB.NETACCESS.*.TCPIPB.ZONEC
TSOUSR1 permitted, all others not
PORTACCESS

- 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

- In the example, only userid WEBSRV is permitted to establish itself as a server on port 80 on stack TCPIPA

```
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 not
```
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 z/OS Communications Server IP Configuration Guide chapter 3 for a complete list of SERVAUTH profiles
Summary
Summary

• **Protecting system resources and data 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 mission critical data in the network**
  - True end-to-end security with security endpoint on z/OS
  - Strong encryption with AES and Triple DES
    • Using hardware assist from crypto coprocessor and CP assist instruction
  - Transparent Application Security
    • IPSec for TCP/IP applications
    • Application-Transparent TLS support
    • Internet-ready access to SNA applications with TN3270 SSL
  - Built-in Application Security
    • Kerberized FTP, rsh, telnet,
  - Secure network services
    • SNMPv3, Secure OSPF Authentication, Secure DNS
Thank you