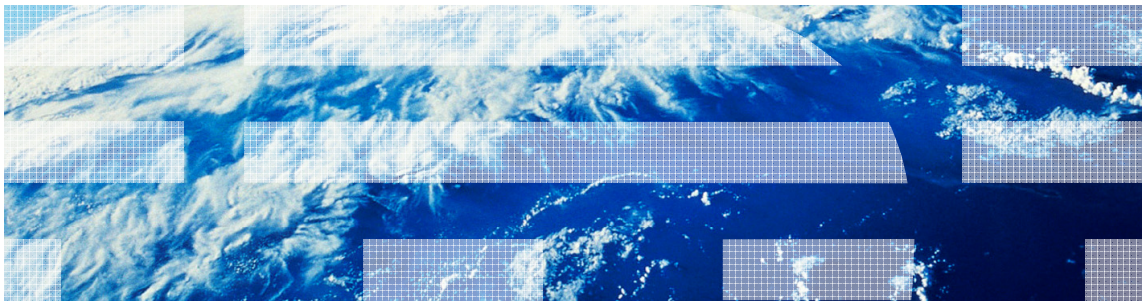
TCP/IP Security Controls on z/OS

Chris Meyer, CISSP – meyerchr@us.ibm.com
z/OS Communications Server

IBM Research Triangle Park, NC



June 21, 2011

Trademarks, notices, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DataPower®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®
- GDDM®
- GDPS®
- Geographically Dispersed Parallel Sysplex
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise™ System
- IMS
- InfiniBand ®
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- POWER®
- POWER7®
- PowerVM
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x®
- System z®
- System z9®
- System z10
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9®
- z10 BC
- z10 EC
- zEnterprise
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

* All other products may be trademarks or registered trademarks of their respective companies.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

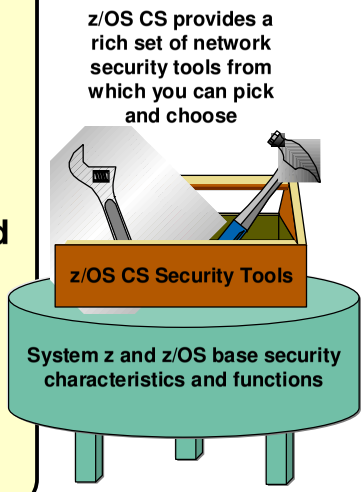
Notes:

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

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

Agenda

- **Communications Server security overview**
  - Trends and requirements
  - Roles and objectives
  - Policy-based network security
- **Steps for protecting TCP/IP, related resources and data in transit**
  1. Blocking unwanted traffic
  2. Protecting against attacks
  3. Protecting UNIX system services logs
  4. Controlling access to TCP/IP resources
  5. Protecting data in the network

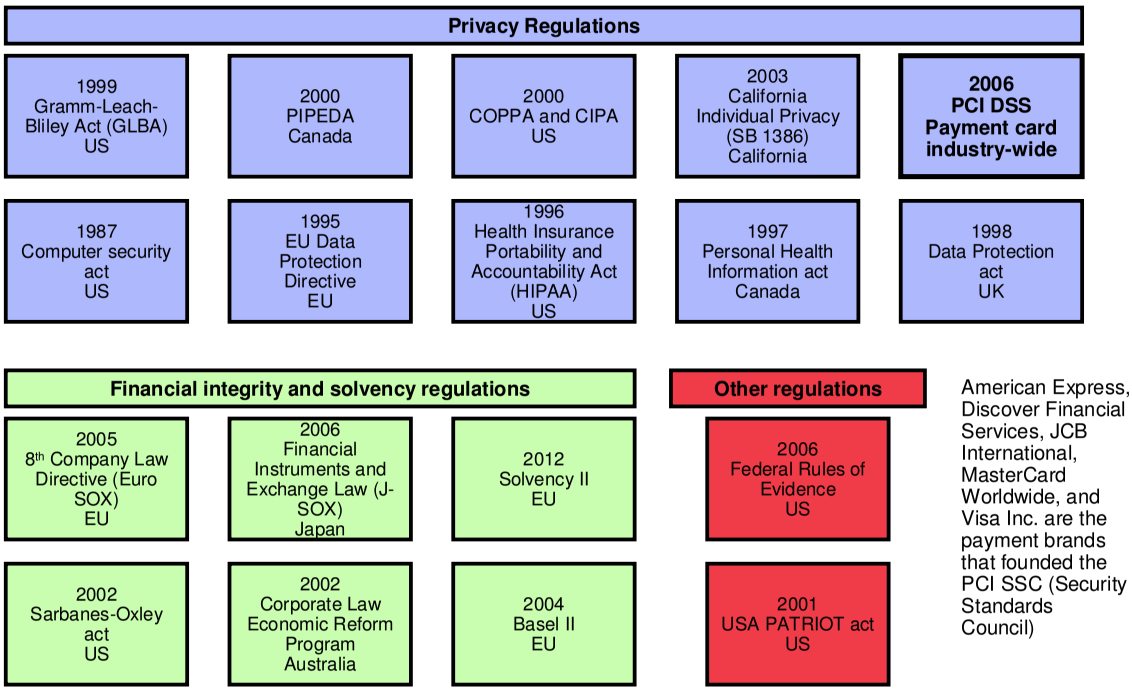


Disclaimer: All statements regarding IBM future direction or intent, including current product plans, are subject to change or withdrawal without notice and represent goals and objectives only. All information is provided for informational purposes only, on an "as is" basis, without warranty of any kind.

TCP/IP Security Controls on z/OS

Communications Server security overview

Trends and Requirements: It's not just PCI DSS*!



American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. are the payment brands that founded the PCI SSC (Security Standards Council)

 * PCI DSS = Payment Card Industry Data Security Standard

Trends and Requirements: PCI DSS overview

Goals	Num	PCI DSS Requirement
Build and maintain a secure network	1	Install and maintain a firewall and router configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5	Use and regularly update anti-virus software programs
	6	Develop and maintain secure systems and applications
Implement strong access control measures	7	Restrict access to cardholder data by business need-to-know
	8	Assign a unique ID to each person with computer access
	9	Restrict physical access to cardholder data
Regularly monitor and test networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an information security policy	12	Maintain a policy that addresses information security for employees and contractors

Source: PCI Quick Reference Guide – Understanding the Payment Card Industry Data Security Standard version 1.2 https://www.pcisecuritystandards.org/index.shtml

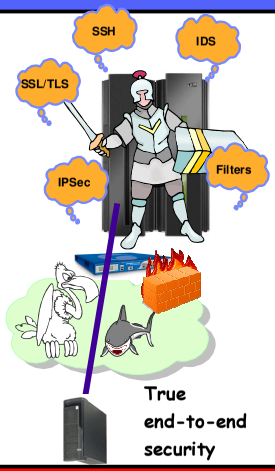
There are other standards related to security and/or IPv6, you also may need to consider:

1. **FIPS Federal Information Processing Standards (primarily FIPS 140 standards)**
2. **NIST National Institute of Standards and Technology (primarily IPv6)**
3. **DoD Department of Defense (Primarily IPv6)**

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 (cryptographic security protocols)**
  - ***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 clear-text using encryption

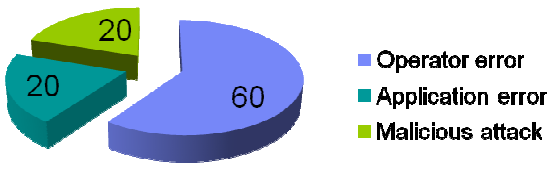
Self protection:
z/OS itself is the last line of defense in an often hostile network environment!



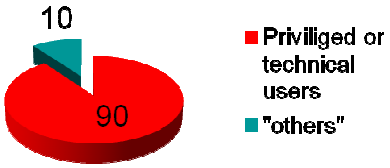
z/OS CS security focus areas:
- Self protection
- Provide secure access to both TCP/IP and SNA applications
- Exploit the strengths of System z hardware and software
- Complement network-based security measures (firewalls, IDS/IPS, etc.)
- Minimize security deployment costs

Roles and Objectives: Perimeter security alone is generally not enough

Categories of security-related incidents



Who is the "villain"?



Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005/6; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.

The enemy is most often ourselves:

- **90% of insider incidents are caused by privileged or technical users**
- **Most are inadvertent violations of:**
  - Change management process
  - Acceptable use policy
  - Account management process
- **Others are deliberate, due to:**
  - Revenge (84%)
  - "Negative events" (92%)
- **Regardless, too costly to ignore:**
  - Internal attacks cost 6% of gross annual revenue or 9 dollars per employee per day

Roles and Objectives: Communications Server security technologies

Protect the system

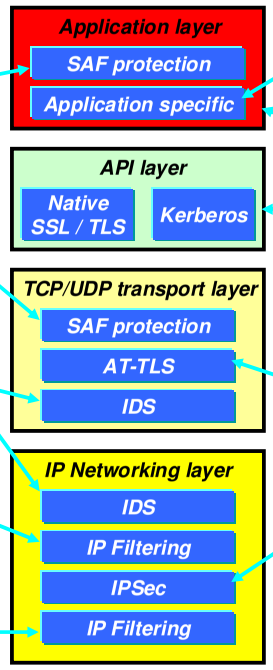
z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources.

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 filtering blocks out all IP traffic that this systems 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 CS) provides an umbrella of secure applications (secure shell access, secure file transfer, etc.)

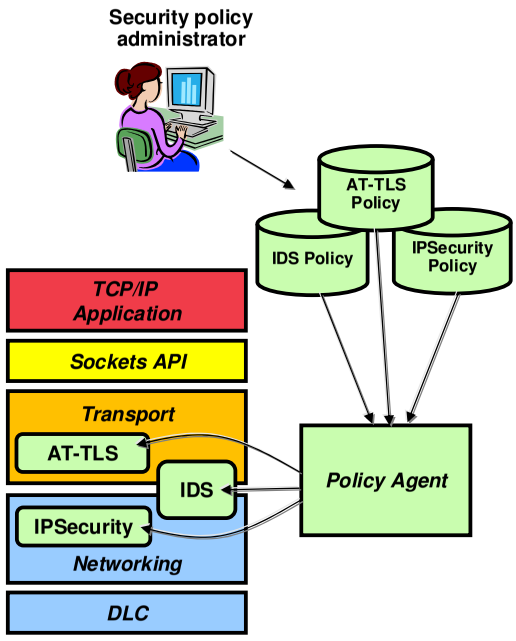
Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

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

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

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



Policy-based network security on z/OS: Configuration Assistant

Download the Windows version at http://tinyurl.com/cgoqsa

- **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 standalone Windows application**
- **Builds and maintains**
  - Policy files
  - Related configuration files
  - JCL procs and RACF directives
- **Supports import of existing policy files**

TCP/IP Security Controls on z/OS

Steps for protecting TCP/IP, related resources and data in transit

A suggested roadmap to protect your z/OS system in a network environment

1. **Blocking unwanted traffic from entering deep into your z/OS system**
   - ☑ **Solution: IP filtering**
2. **Protecting against malicious or accidental attacks on your system**
   - ☑ **Solution: Intrusion Detection Services**
3. **Securing an audit trail for z/OS UNIX system services**
   - ☑ **Solution: syslogd isolation**
4. **Controlling user access to TCP/IP resources on the system**
   - ☑ **Solution: SAF protection using SERVAUTH class resources**
5. **Protect end-to-end confidentiality and integrity of data in the network**
   - ☑ **Solution: Numerous network security protocols (IPSec, TLS, AT-TLS, etc.)**
   - ☑ **Solution: Application-specific security features**

TCP/IP Security Controls on z/OS

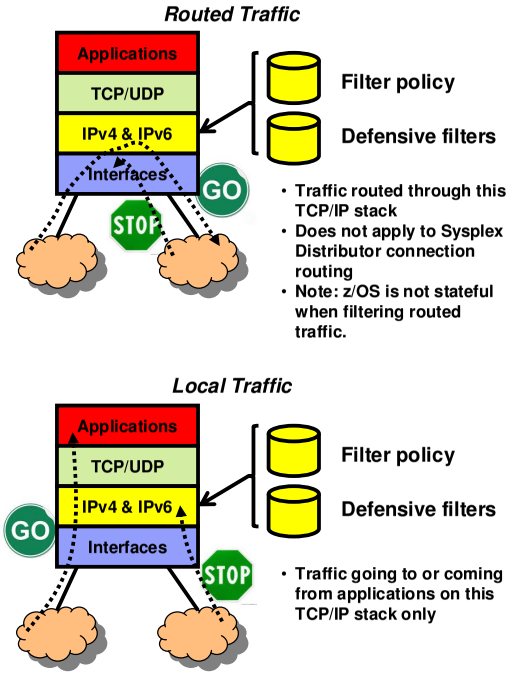
Steps for protecting…

Step 1: Blocking unwanted traffic

✓ IP filtering

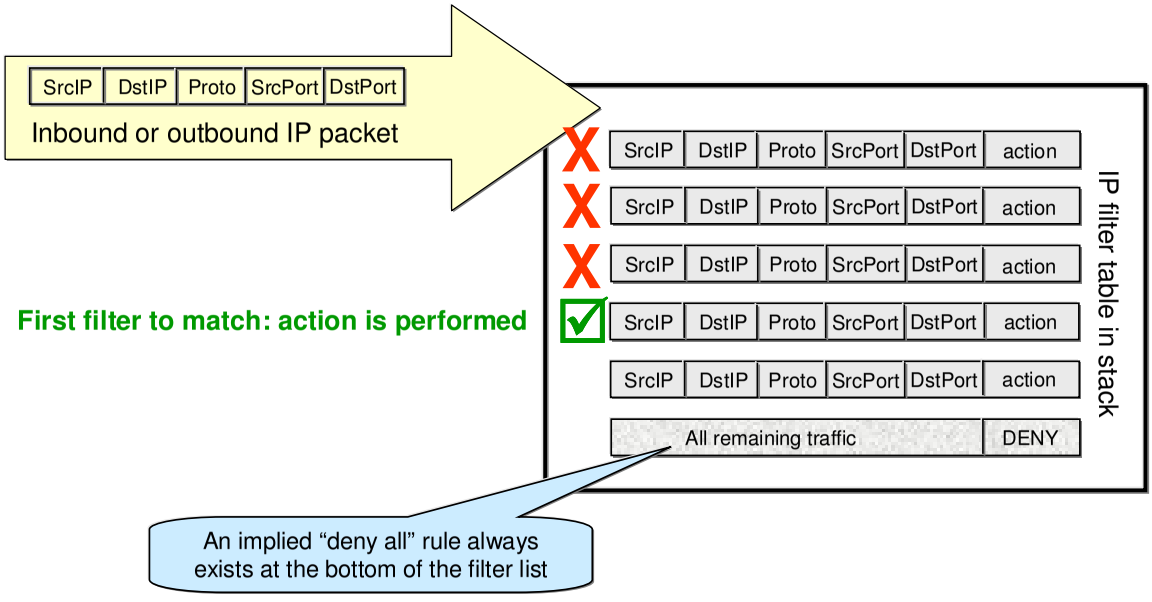
IP filtering: Basics

- **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



IP 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**



TCP/IP Security Controls on z/OS

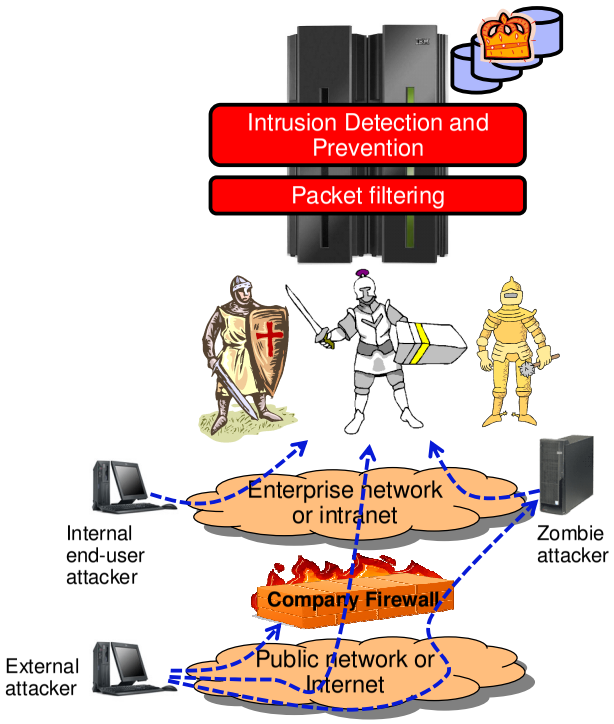
Steps for protecting…

Step 2: Protecting against attacks

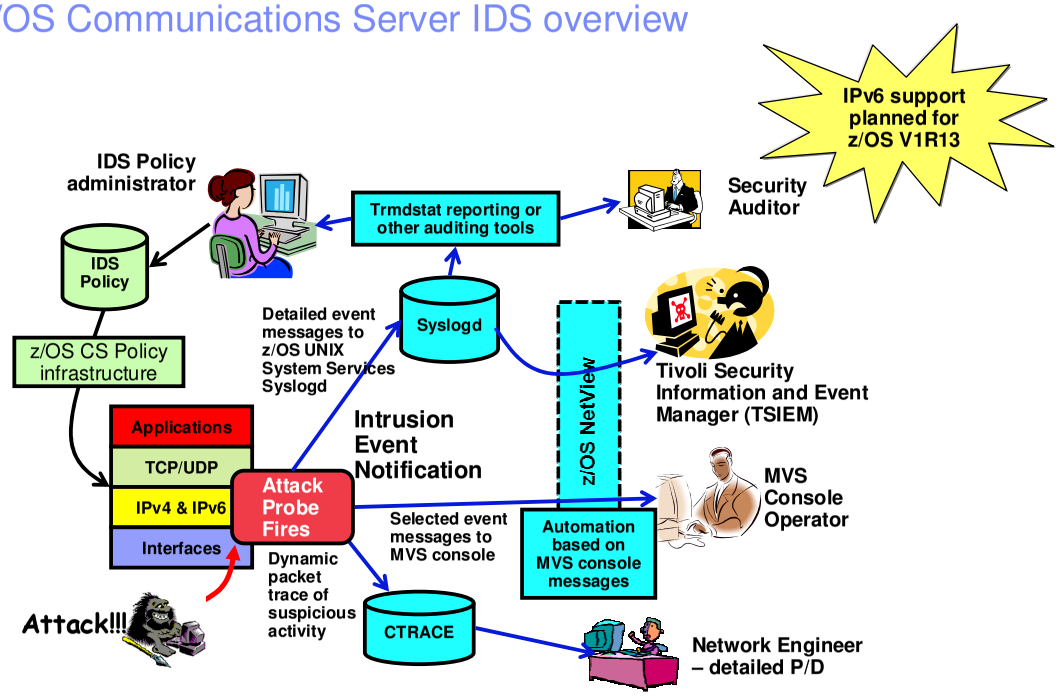
✓ Intrusion Detection Services

IDS: 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.)**



IDS: z/OS Communications Server IDS overview



IDS: zOS Communications Server 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… including several new attack types coming 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)

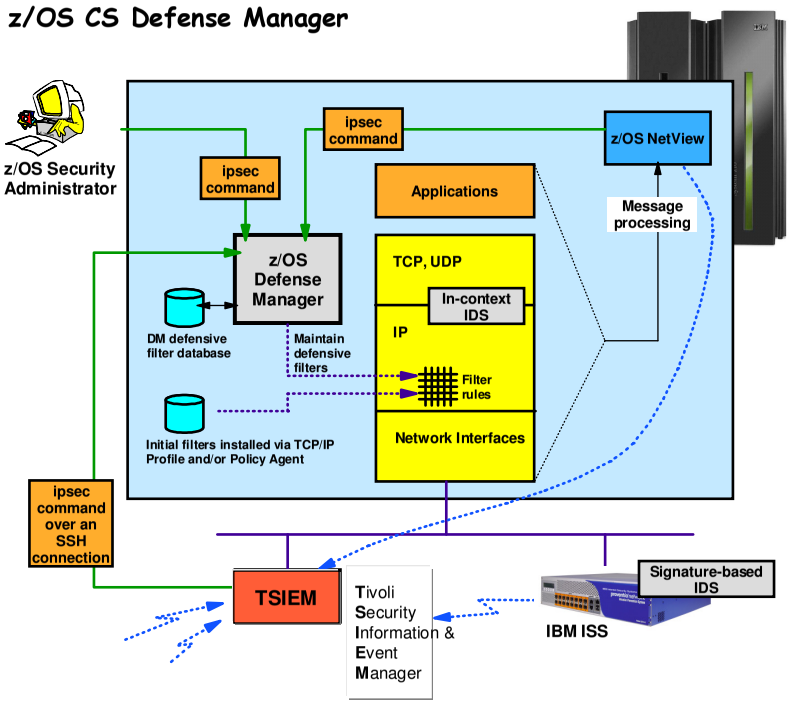
Reporting

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

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



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

Enables dynamic defensive actions on z/OS

TCP/IP Security Controls on z/OS

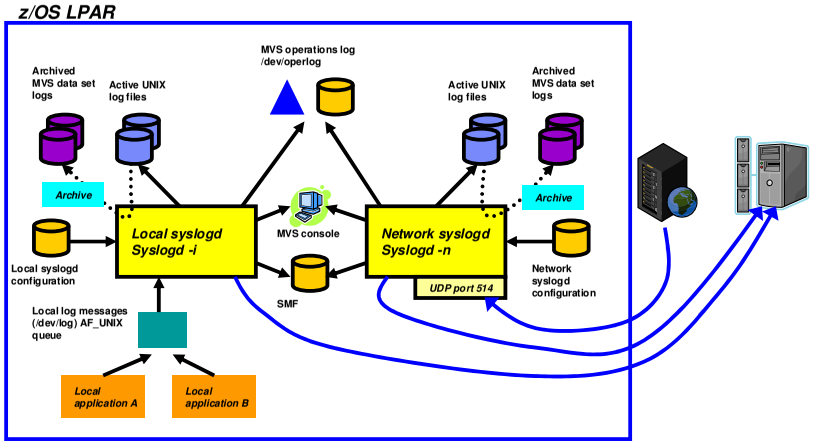
Steps for protecting…

Step 3: Securing z/OS UNIX system services audit trail

✓ **syslogd isolation**

syslogd isolation: Ensuring log data is available when you need it to analyze past events

- **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
    - Ability to audit integrity of syslogd messages

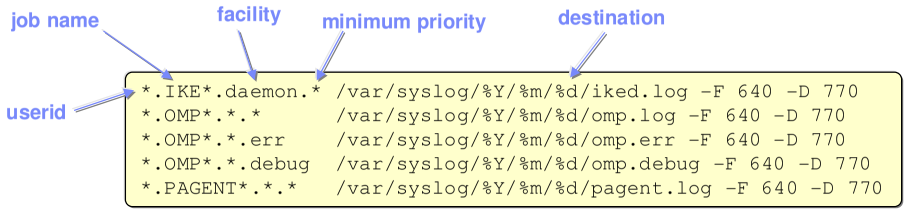


- **z/OS syslogd security controls provide:**
  - Protection from local z/OS users
    - Additional controls to direct syslogd messages to different destinations based on Userid and/or Job name
    - userid/jobname can be traced in log for audit
  - Protection from the network
    - Syslogd configuration can turn off reception of log messages via UDP port (while retaining the ability to send to other syslogd instances over UDP)
    - IP filtering can be used to selectively receive syslogd messages from the network
  - z/OS V1R11 Communications Server delivered significant improvements in the area of syslogd management and use

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

syslogd isolation: Controlling syslogd 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



See *IBM z/OS V1R12 Communications Server TCP/IP Implementation Volume 2: Standard Applications* for a good discussion on setting up syslogd. (http://www.redbooks.ibm.com/redpieces/pdfs/sg247897.pdf)

See *z/OS Communications Server IP Configuration Reference* for details on syslogd configuration statements

syslogd isolation: Key controls

- **Prevent or limit receipt of inbound syslogd message from remote nodes**
  - syslogd –i option prevents any inbound messages
  - Otherwise, use IP filters to control which remote addresses are permitted to send them to the local node

```
syslogd -i ...
```

- **Log userid and jobname for locally-generated syslog messages**
  - syslogd –u option
  - Valuable audit data
  - No way to record these for messages received over UDP

```
syslogd -u ...
```

- **Use appropriate UNIX permissions for log files and directories**
  - -F and –D options on the destination specification in syslog.conf
  - Prevents unauthorized viewing or alteration of audit logs

```
/var/syslog.../xyz.log -F 640 -D 770
```

- **Archive syslogd log files**
  - Variety of cron- and script-based approaches
  - V1R11 offers built-in archiving to z/OS data sets
    - Includes Generation Data Group support
    - Triggered by
      - ✓ Time of day
      - ✓ z/OS UNIX file system utilization (threshold percentage of capacity)

```
BeginArchiveParms
  DSNPrefix USER1.SYSLOG
  Unit SYSDA
EndArchiveParms
ArchiveThreshold 80
ArchiveTimeOfDay 02:01
```


TCP/IP Security Controls on z/OS

Steps for protecting…

Step 4: Controlling user access to TCP/IP resources

✓ SAF protection using SERVAUTH class resources

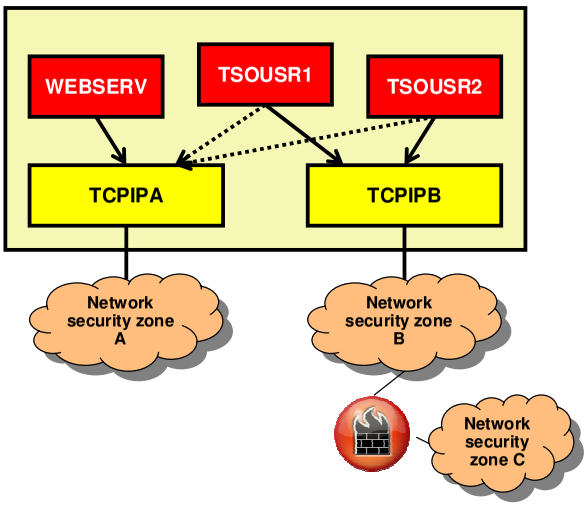
SAF Protection: Key TCP/IP-related resources

- **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**

SAF Protection: STACKACCESS



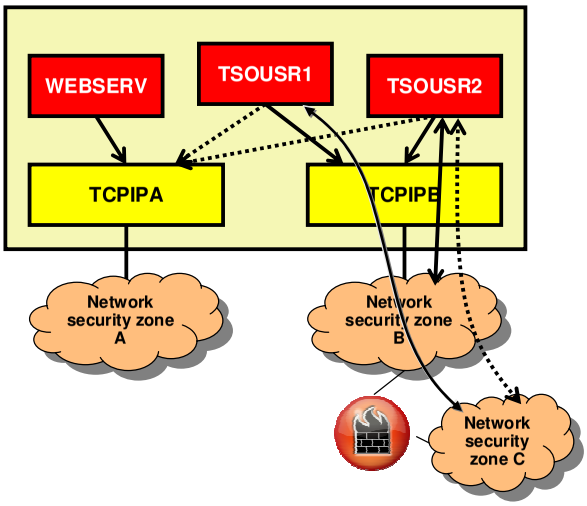
- **Limits local users' open sockets or use of TCP/IP stack services (e.g., get hostname, get hostid, etc.)**
- **Access to stack via sockets is allowed if the user has access to the following SERVAUTH class SAF resource:**

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

SAF Protection: 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:**

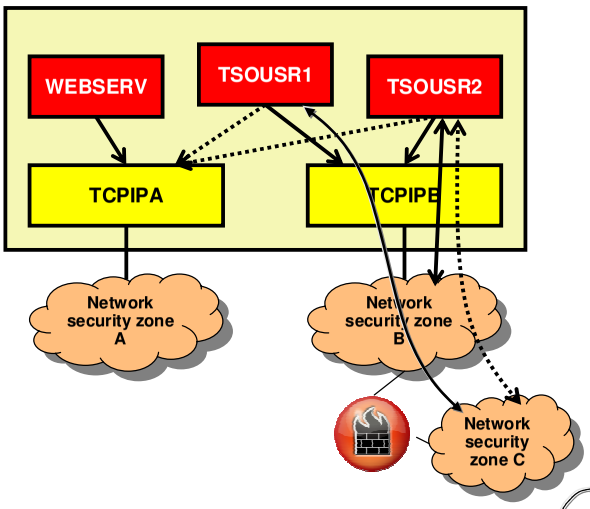
```
NETACCESS INBOUND OUTBOUND
  192.168.1.0     255.255.248.0 ZONEB
  192.168.0.0/16                ZONEC
  Default         0             WORLD
ENDNETACCESS
```

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

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

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

SAF Protection: 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
```

- **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**

```
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

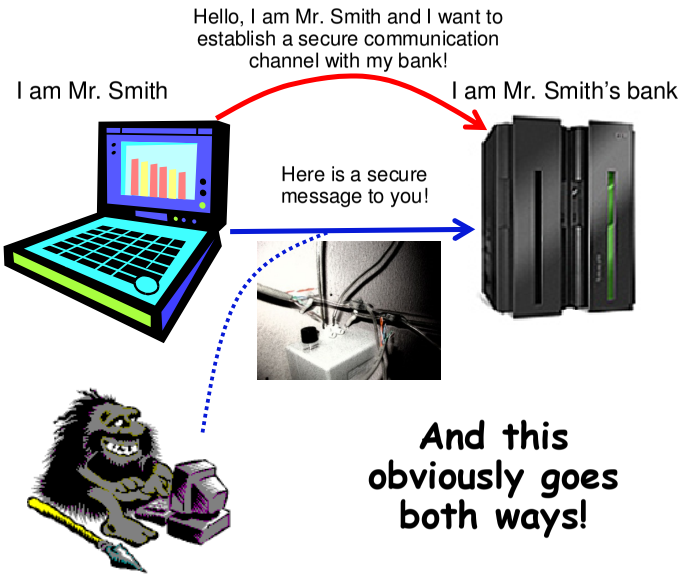
TCP/IP Security Controls on z/OS

Steps for protecting…

Step 5a: Protect data end-to-end

✓ Network security protocols

Protocols: The four big questions



Partner authentication
- How do I know that you really are who you claim to be and not some imposter?
- How do you know that I am who I say I am?

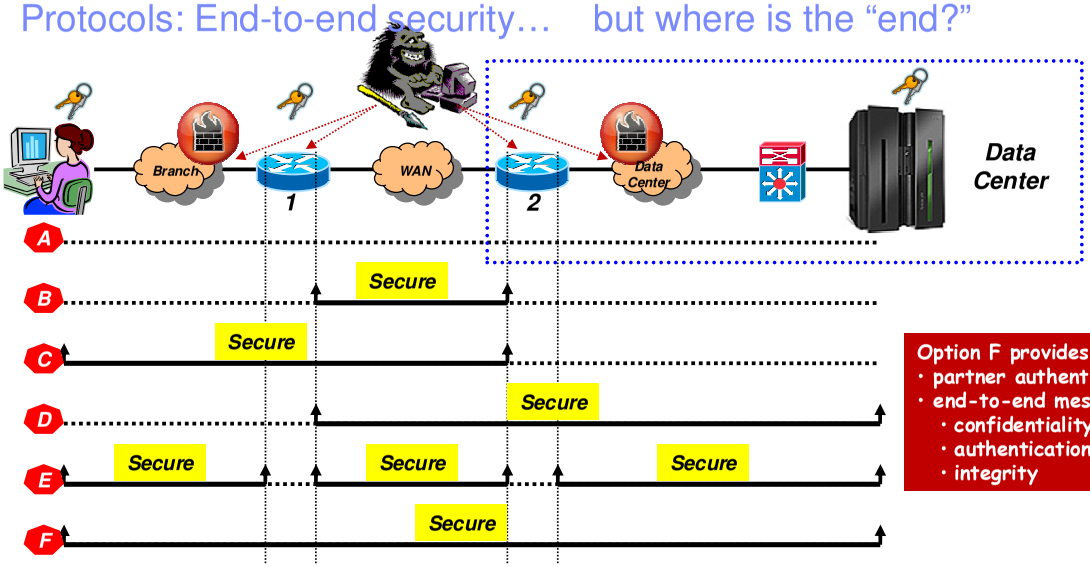
Message authentication
- How do I know the secure message actually came from the partner I authenticated a little earlier?
- How do I know it wasn't injected into the network by someone else?

Message integrity
- How do I know that someone didn't modify the message since you sent it?
- How do I know that someone didn't duplicate an otherwise valid message?

Data Confidentiality
- How do I know that no one could have intercepted this message and read it in an intelligible way when it was traversing the network?

Each of the secure network communications protocols address these four basic requirements, although in slightly different ways

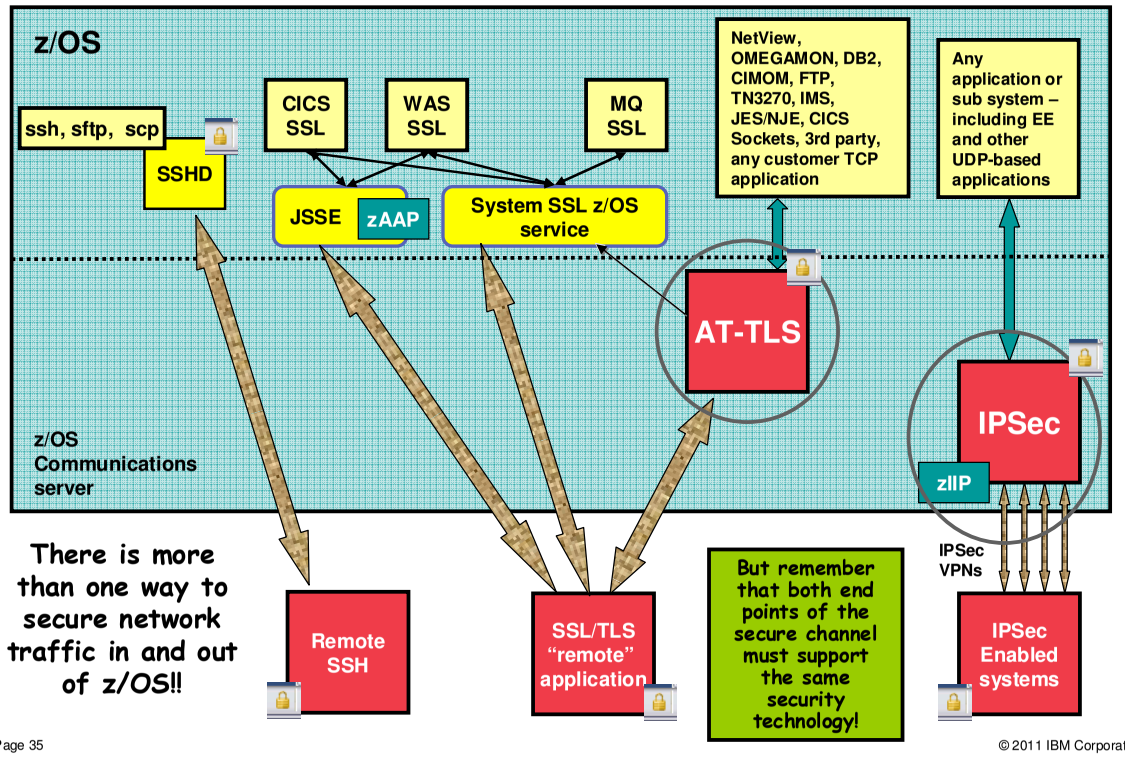
Protocols: End-to-end security… but where is the "end?"



Option F provides best
- partner authentication
- end-to-end message
  - confidentiality
  - authentication
  - integrity

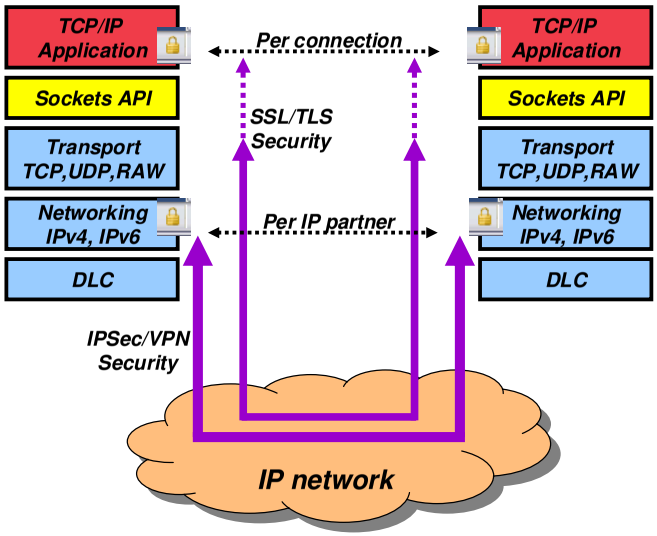
Topology	Partner authentication	Key management	Message authentication and integrity
A No security	None	None	None
B WAN only	Two WAN routers	On WAN routers	Between WAN routers
C Branch + WAN	Workstation – WAN router 2	On workstation and WAN router 2	Between workstation and WAN router 2
D WAN + data center	WAN router 1 – z/OS	On WAN router 1 and z/OS	Between WAN router 1 and z/OS
E Hop-by-hop security	Hop by hop	On all nodes, including WAN routers	Between all nodes, but not end to end (performance hit)
F End-to-end security	Workstation – z/OS	Workstation and z/OS	Between workstation and z/OS

Protocols: Technology overview



Protocols: Some key differences between SSL/TLS and IPSec

- **SSL/TLS**
  - Each session protects one TCP connection
  - Does not support UDP
  - Application-to-application
  - Often a designated TCP port for secure connections (such as 443)
  - AT-TLS can make it transparent to applications on z/OS
    - Else requires app awareness
  - Partner authentication via X.509 certificates
- **IPSec VPN**
  - Supports all transport layer protocols (TCP, UDP, raw)
  - One session can protect multiple application connections/streams
  - IP layer to IP Layer
  - Transparent to all applications
  - Partner authentication via pre-shared key or X.509 certificates
  - IPSec on z/OS can use zIIP

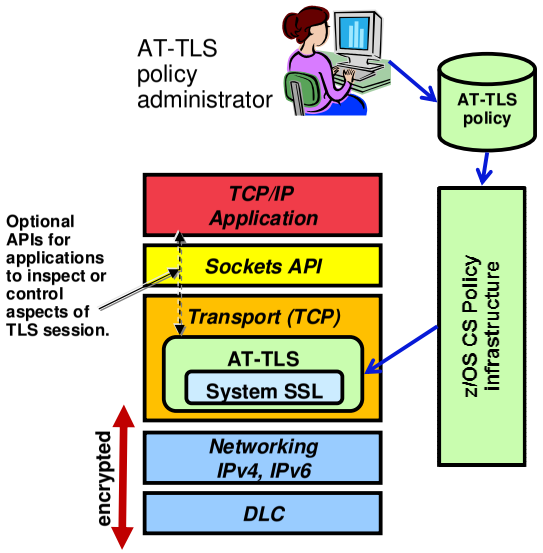


Some common characteristics:

- Both use CPACF and Crypto Express if available
- Both support most common encryption and authentication algorithms (AES, 3DES, SHA, MD5, etc.)
- Both can use RACF keyrings and ICSF secure keys

Protocols: z/OS Application Transparent TLS overview

- **Basic TCP/IP stack-based SSL/TLS**
  - SSL/TLS process performed at TCP layer (via System SSL) without requiring any application change (transparent)
  - AT-TLS policy specifies which TCP traffic is to be SSL/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
  - Application has option to inspect or control certain aspects of ATTLS processing – "application-aware" and "application-controlled" ATTLS, respectively
- **Available to TCP applications**
  - Includes CICS Sockets
  - All programming languages except PASCAL supported
- **Supports both client and server roles**
- **Supports both server and client authentication**
- **Uses System SSL for SSL/TLS protocol processing**
  - Remote connection end point may use any SSL/TLS APIs to implement SSL/TLS



Enabling most z/OS TCP-based applications for use of SSL/TLS without requiring any modifications to those applications on z/OS.

Protocols: AT-TLS benefits

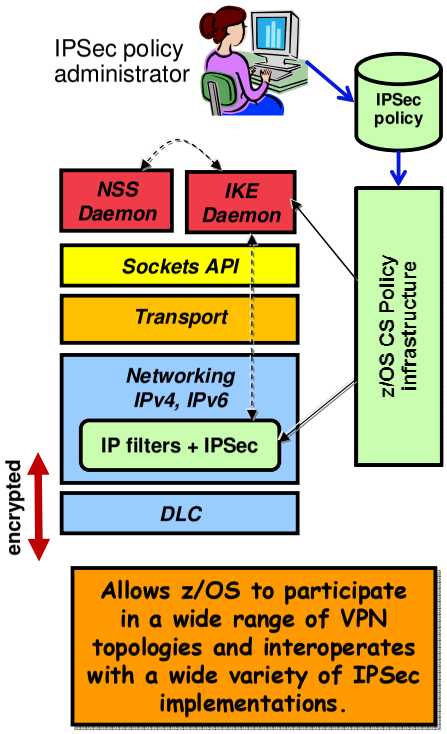
- **Reduce costs**
  - Application development
    - Cost of System SSL integration
    - Cost of application SSL-related configuration support
  - Consistent TLS administration across z/OS applications

- **Complete and up-to-date exploitation of System SSL features**
  - AT-TLS makes 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**

- **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

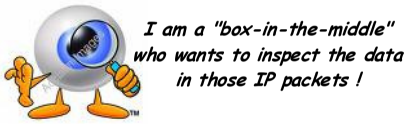
Protocols: z/OS IPSec overview

- **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.**
- **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 SAs to be shared across the sysplex**
- **IP Security monitoring interface: IBM Tivoli OMEGAMON XE for Mainframe Networks**



Protocols: What is encrypted and how are "boxes-in-the-middle" affected?

- ***What are "boxes-in-the-middle"?***
  - Many firewalls (especially those that are stateful)
  - Intrusion detection devices (signature-based)
  - Contents-based routers
  - Protocol analyzers, tracers (sniffers), debuggers, etc.



No encryption:

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	50001	80	POST / HTTP/1.1 ... <soapenv:Envelope ...

WSS encryption:

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	50001	80	POST / HTTP/1.1 ... <soapenv:Envelope ... <xenc:EncryptedData ... ^%$$##%%%%

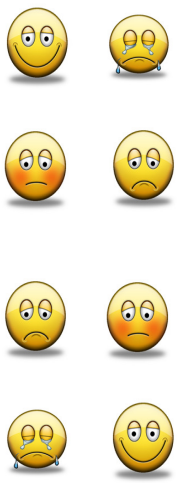
SSH or SSL/TLS encryption:

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	50002	443	@%$#*&&^^!:"J)*GVM><

IPSec encryption:

SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	>::"	*&hU$$$	@%$#dd*&&^s^!:"J)*bGVM> (*hhgvvv<

IP header encryption varies based on transport/tunnel mode, and AH/ESP protocol



Protocols: Some considerations in selecting a security protocol

1. **Does corporate security policy dictate a specific technology or requirement?**
   - **Technology example: "All file transfers must be protected by TLS"**
   - **Requirement example: "All customer financial data must be encrypted, end-to-end, as it traverses the network"**
2. **What are the capabilities of the hosts and network equipment? Both endpoints of a secure connection must support the same…**
   - **Network security protocol**
   - **Cryptographic algorithms**
3. **Are relative security infrastructures already in place?**
   - **Is there already an Public Key Infrastructure (PKI) in place?**
   - **Is TLS or IPSec already deployed anywhere in the network?**
4. **Do the security protocols support the transport protocols?**
   - **TLS works great for TCP, but nothing else**
   - **IPSec protects any IP traffic, regardless of transport protocol**
5. **Is the application already enabled for network security?**
   - **TLS, Kerberos, secure network services**
   - **If so, then see 3 above**
   - **If not, consider application-transparent technologies**

6. **What do you want to authenticate?**
   - **Application/user identity: TLS authentication is visible to the application, IPSec is not**
   - **Host identity: IPSec authenticates at the host level**

TCP/IP Security Controls on z/OS

Steps for protecting…

Step 5b: Protect data end-to-end

✓ Application-specific secure network services

App-specific: Overview of built-in application security

Socket-based security

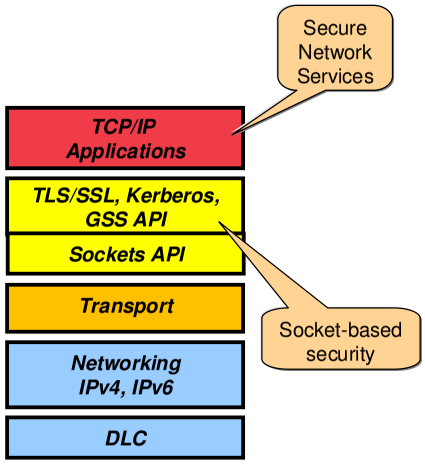
- **TLS-enabled applications**
  - FTP server and FTP client
  - TN3270 server
  - DCAS server
  - CSSMTP server

  Partner authentication and message protections as described earlier
- **"Kerberized" applications**
  - FTP server and client
  - Unix telnet daemon
  - Unix rsh daemon

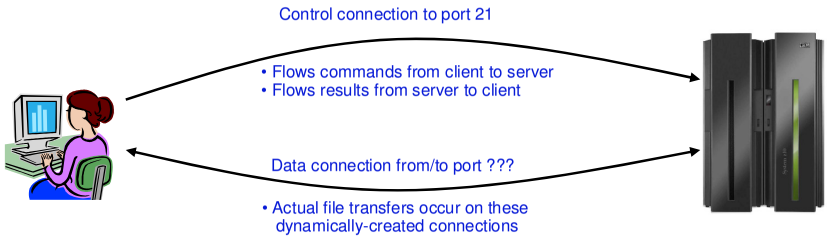
  Provides strong third-party authentication for client/server applications using secret key cryptography and encrypted data flows

Secure Network Services

- **SNMPv3**
  - Authentication, data integrity and privacy for SNMP messages
  - Access controls for MIB objects
- **Secure DNS**
  - Ensures DNS query replies are authentic
- **OSPF MD5 Authentication**
  - Ensures routing table integrity
  - Uses MD5-based authentication for routing messages (RFC 2328)
- **SSH**
  - ssh, sftp, scp
  - via IBM Ported Tools for z/OS or vendor products

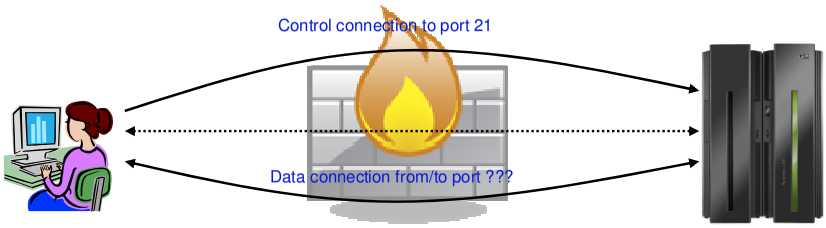


App Specific: TLS-protected FTP



- **TLS protection can be applied to both the control and data connections**
  - Control connection protection can be "turned on and off" using CCC command
  - Data connection protection is applied for the life of the connection
- **Control connections**
  - Wide variety of commands flow over this connection
  - Some of these commands have a direct effect on the state of the control and/or data connections
- **Data connections**
  - Often established using ephemeral ports
  - Two ways to establish these connections
    - "active" - the server connects out to the client
    - "passive" – the client connects out to the server

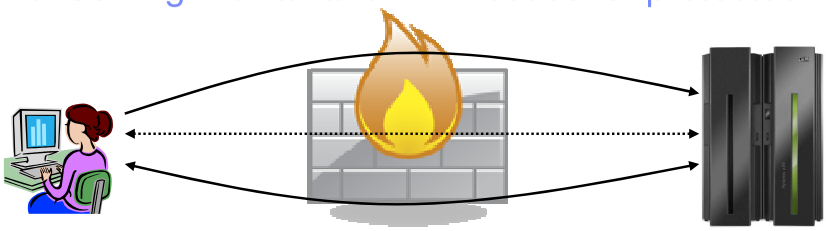
App Specific: Firewalls and FTP



- **Port-based filter rules – in particular dynamic port rules**
  - FTP control connection is no problem - pre-defined server port number (default 21)
  - Data connection port number (or direction) is not pre-defined, but dynamically negotiated between the FTP client and server
    - The firewall does "deep inspection" (peeks into) the FTP control connection to learn about the negotiated ports and the direction for the data connection
- **NAT**
  - FTP control connection is no problem – only IP headers need translation
  - PORT command and PASV reply refers to local (intranet) IP addresses
    - Firewall needs to do "deep inspection" of the FTP control connection to locate and modify the IP address information in the PORT command and the PASV reply

Deep inspection and data modification is impossible when the data on the FTP control connection is secured through encryption and message integrity checking at the end points.

App Specific: Solving firewall and NAT issues for protected FTP



<shameless plug>

Come see how in session AST8:

Safe and Secure Transfers with z/OS FTP

On Wednesday, June 22!!

</shameless plug>

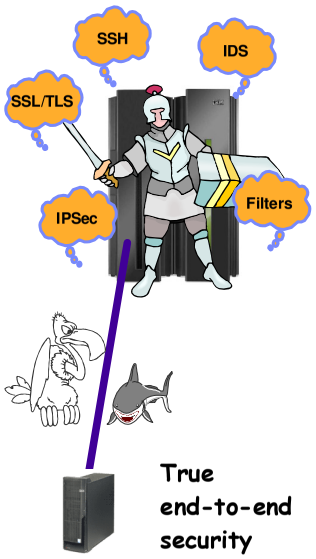
z/OS Network Security Roadmap

Summary

Summary

- **Protecting system resources and data from the network**
  - Integrated Intrusion Detections 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
    - SSH port forwarding or tunneling
  - Built-in Application Security
    - SSL-enabled FTP, Kerberized FTP, rsh, telnet, ssh, sftp, scp
  - Secure network services
    - SNMPv3, Secure OSPF Authentication, Secure DNS



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.twitter.com/IBM_Commserver	IBM Communications Server Twitter Feed
http://www.facebook.com/IBMCommserver	IBM Communications Server Facebook Fan Page
http://www.ibm.com/systems/z/	IBM System z in general
http://www.ibm.com/systems/z/hardware/networking/	IBM Mainframe System z networking
http://www.ibm.com/software/network/commserver/	IBM Software Communications Server products
http://www.ibm.com/software/network/commserver/zos/	IBM z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	IBM Communications Server for Linux on System z
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library/	IBM Communications Server library
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/zos/support/	IBM z/OS Communications Server technical Support – including TechNotes from service
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)
http://www.ibm.com/systems/z/os/zos/bkserv/	IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server