Introduction to Using z/OS Communications Server Security Features

SHARE Session 3404

March 4, 2002

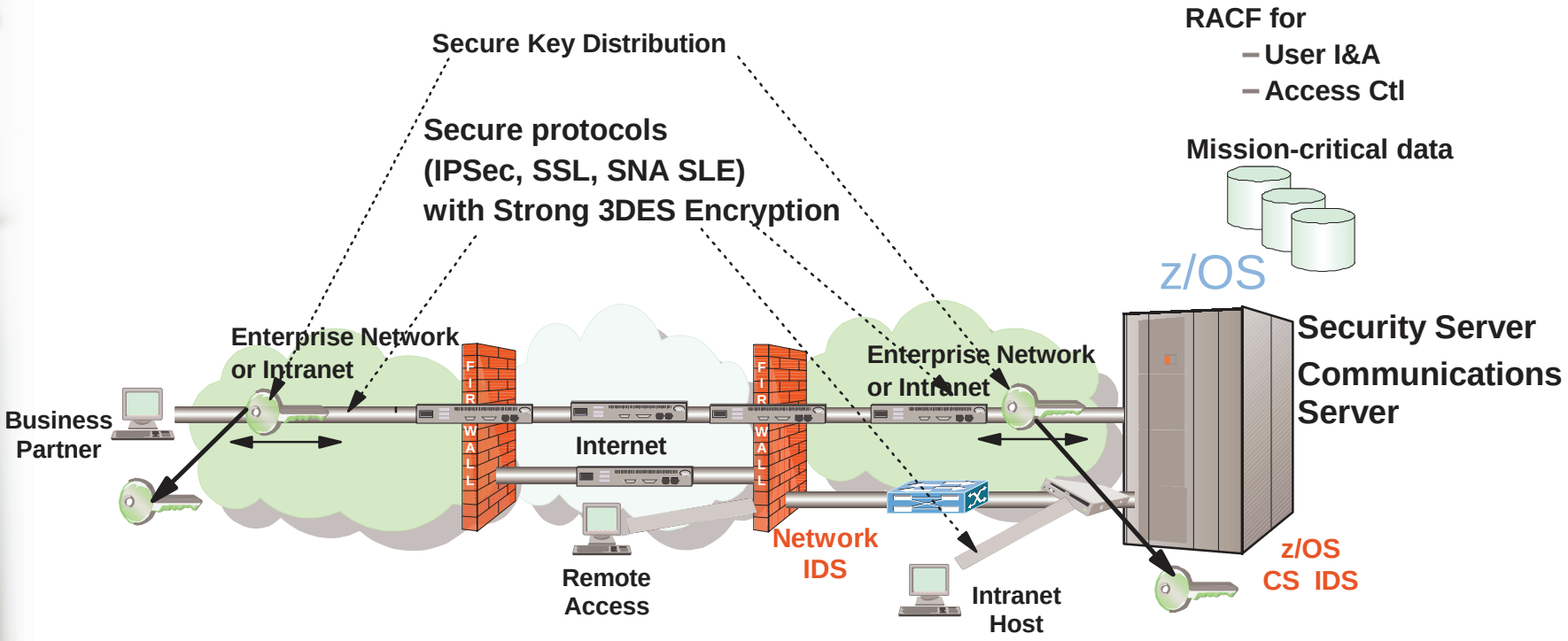
Lin Overby
WebSphere and eServer Networking Solutions
Strategy and Design
Internet: overbylh @ us.ibm.com

Topics

- **A quick review of security features through OS/390 V2R10**
  - TCP/IP Resource Protection
  - TCP/IP Application Security
  - Network Security
- **V1R2 Security Features**
  - Intrusion Detections Services
  - Built-in Application Security
    - SSL for FTP
    - Kerberos for FTP, telnetd, and rshd
    - OSPF Authentication
    - Secure DNS
  - Express Logon Feature
  - IPSec and VPN enhancements
  - FTP security enhancements
  - SMTP Exit Interface
  - Netstat output protection

z/OS Communication Server Enables e-business on z/900

- ✓ Secure access to both TCP/IP and SNA applications
- ✓ Focus on end-to-end security and self-protection
- ✓ Exploits strengths of S/390 and z900 hardware and software



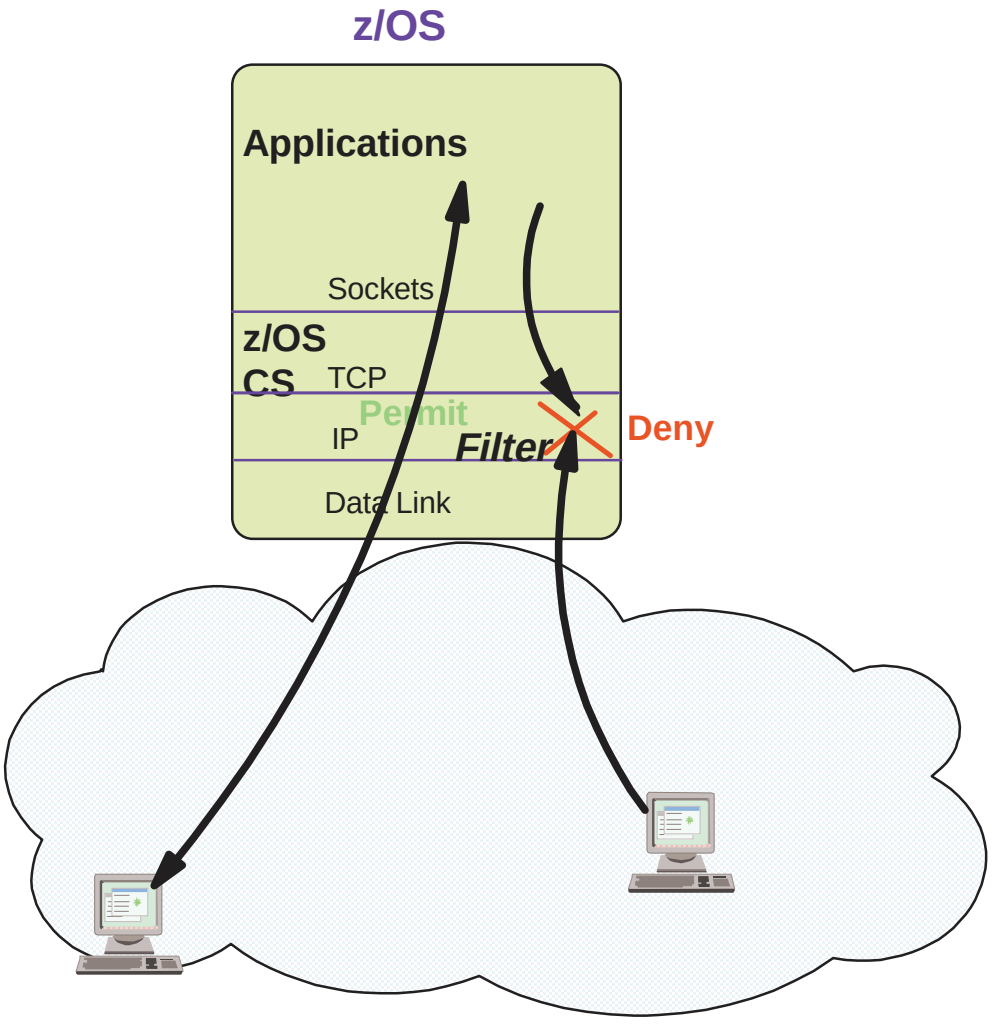
z/OS Communications Server Secures Mission-Critical Data

z/OS Communications Server Security Roles and Objectives

- **Protect data in the network using cryptographic security protocols**
  - ***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
- **Protect data and other resources on the system**
  - ***Identification and authentication***
    - Verify identity of users
  - ***Access control***
    - Protect data and other system resources from unauthorized access
  - ***System availability***
    - Protect system against denial of service attacks from network

IP Packet Filtering

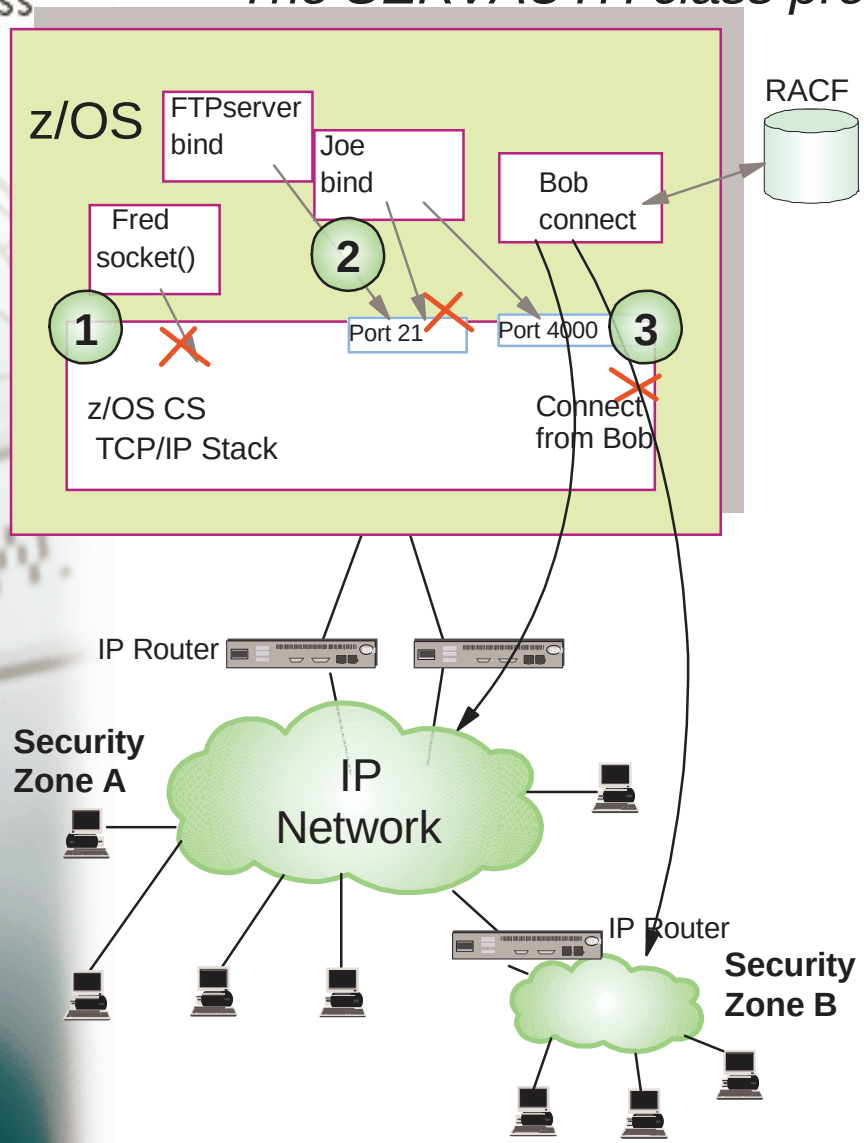
- **Packet filtering at IP Layer**
  - Filter rules defined to discard or permit packets based on:
    - IP source/dest address
    - IP protocol
    - Source/dest Port
    - Direction of flow
    - Time
  - Used to control
    - traffic being routed
    - access at destination host



- **Packaging (Firewall Technologies)**
  - Security Server
    - Configuration thru z/OS UNIX command line interface or Configuration GUI
  - Communications Server
    - Runtime IP packet filtering

User Access Control to TCP/IP Resources Using RACF

The SERVAUTH class protects TCP/IP Resources



1. Stack Access Control

- Controls user ability to open socket
  - CS OS/390 TCP/IP stack is considered a resource
- Access to stack via TCP or UDP socket allowed if user permitted to new SAF resource (SERVAUTH class)
  - ✓ EZB.STACKACCESS.sysname.tcpname

2. Local Port Access Control

- Controls user access to a local TCP or UDP port
  - Port is considered a resource
- Function enabled
  - Via new SAF Keyword on PORT or PORTRANGE
- Access to port allowed if user permitted to new SAF resource (SERVAUTH class)
  - ✓ EZB.PORTACCESS.sysname.tcpname.SAFkeyword
- Access to port not permitted for any user
  - Via New RESERVED Keyword On PORT Or PORTRANGE

3. Network Access Control

- Controls local user access to network resources
  - Network considered a resource
    - ✓ Network/Subnet/Specific host
- Allows Management Of Security Zones
  - Via new NETACCESS statement In TCP/IP Profile
    - ✓ NETACCESS statement allows grouping of network resources
- Access to security zone allowed if user permitted to new SAF resource (SERVAUTH class)
  - ✓ EZB.NETACCESS.sysname.tcpname.zonename

Syslogd Data Integrity and Availability

Syslogd Isolation

Goals:

- Prevent loss of log records due to flooding
- Keep system log records separate from application log records

Protection between OS/390 users and jobs

- Ensure Segregation of Logs
  - **By specifying UserID and/or Jobname Rules as additional criteria along with syslogd facility and priority criteria**
  - **UserID/Jobname correlation can be traced in log**
- Verification of Client Credentials
  - **Syslogd uses USS-provided UserID and Jobname**

Protection from the network

- Syslogd configuration can turn off reception of log messages via UDP port
  - **Does Not Limit Ability To Send**
- IP filtering can be used to selectively receive syslogd messages from the network

z/OS CommServer Application Security Overview

- **RACF used by TCP/IP applications for**
  - Identification and authentication of users
  - Access control when files are accessed
- **Some applications have specific requirements and configuration for security**
  - Security extensions available with some applications for more control (e.g. FTP security exits)
- **Configuration options to control unauthenticated access**
  - Anonymous FTP, Remote Execution, TFTP

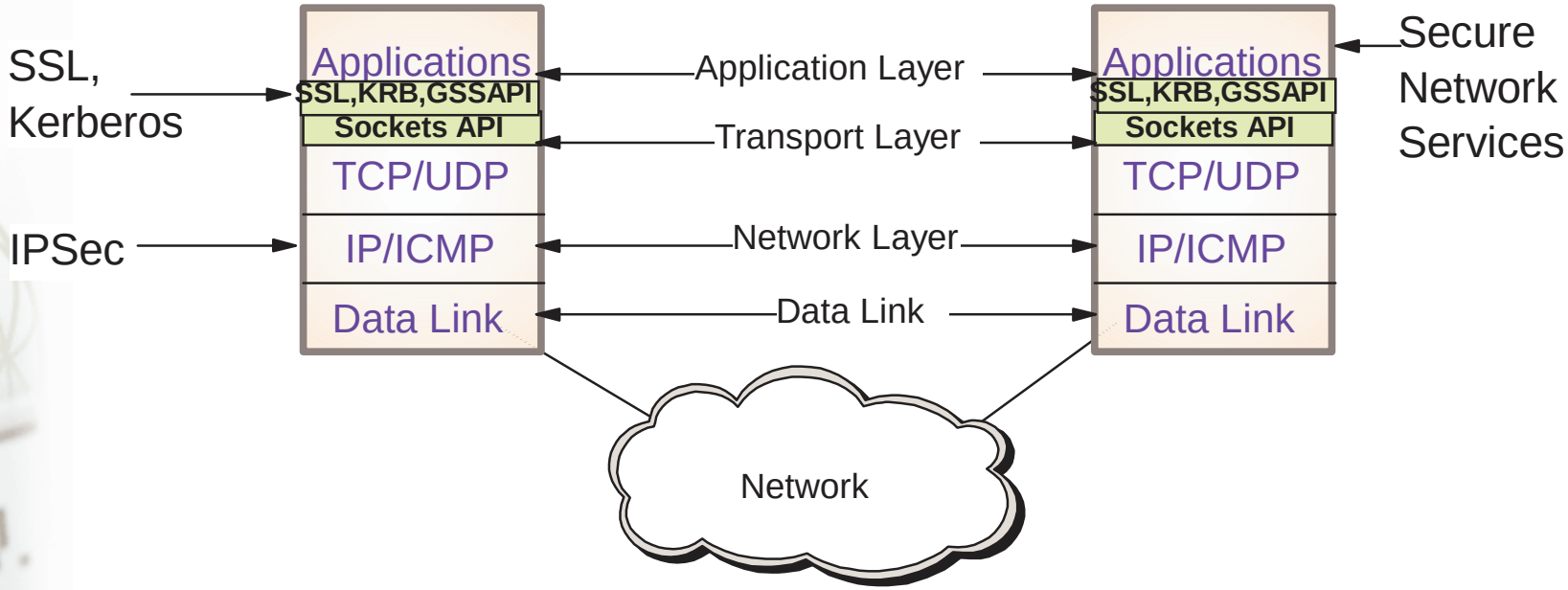
Application User Identification, Authentication, and Access Control

Server	End User Identification	Resource Access
FTP	Optional (1)	End user ID or configured anonymous user ID(2)
LPD	Optional (1)	Server user ID or end user ID
TFTP	No	Server user ID (2)
MVS REXECD	Required	End user ID
MVS RSHD	Required (password optional) (1)	Surrogate user ID or end user ID
UNIX REXECD	Required	End user ID
UNIX RSHD	Required (password optional) (1)	End user ID or Server user ID (exit routine to verify request)
UNIX Shell (telnet/rlogin)	Required	End user ID

(1) All optionals are installation controlled and all can be configured to require full end user identification

(2) Files accessible can be configured on a server basis to limit access

Workload-based Security Deployment



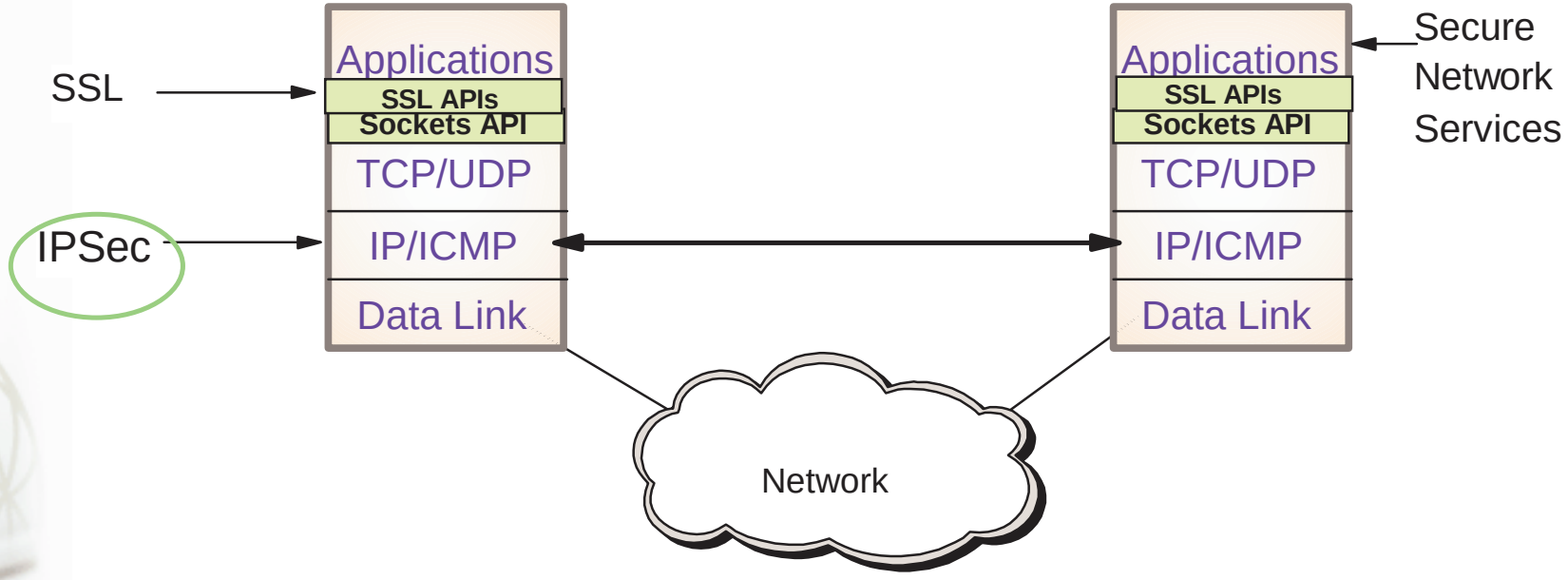
Existing Application Access over IP

- IPSec provides blanket protection for all applications
  - end-to-end or segment of data path
- SSL TN3270 securely extends reach of SNA applications over IP network
  - TN3270 client to TN3270 server data path secured

New Applications

- Build security into application (e.g. SSL enabled webserver)
- Secure, interoperable network services (e.g. SNMPv3)

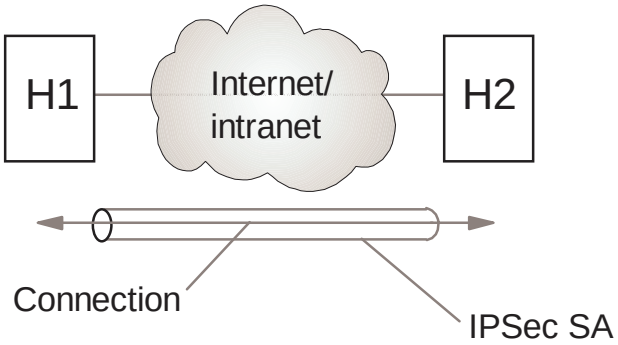
IPSec Overview



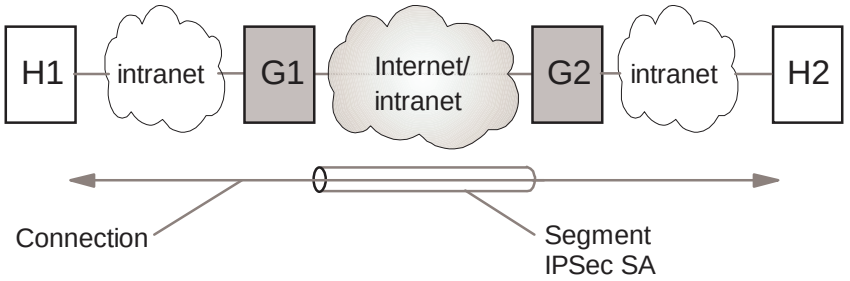
- Open network layer security protocol endorsed by IETF
- Provides authentication, integrity, and data privacy
  - IPSec security protocols
    - **Authentication Header (AH)** - provides authentication / integrity
    - **Encapsulating Security Protocol (ESP)** - provides privacy with optional authentication / integrity
- Allows secure tunnel between any two IP entities
  - Security Associations (SA)
- Management of crypto keys and security associations can be
  - manual
  - automated via key management protocol (IKE)
- Use of IPSec is transparent to upper layers including application
  - Blanket level protection for upper layer protocols

IPSec Combinations

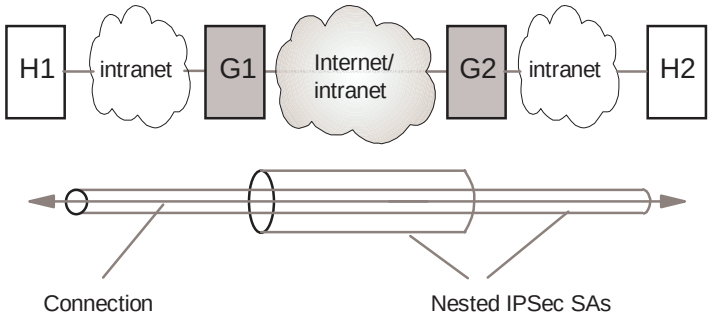
Case 1: End-to-End Security Association



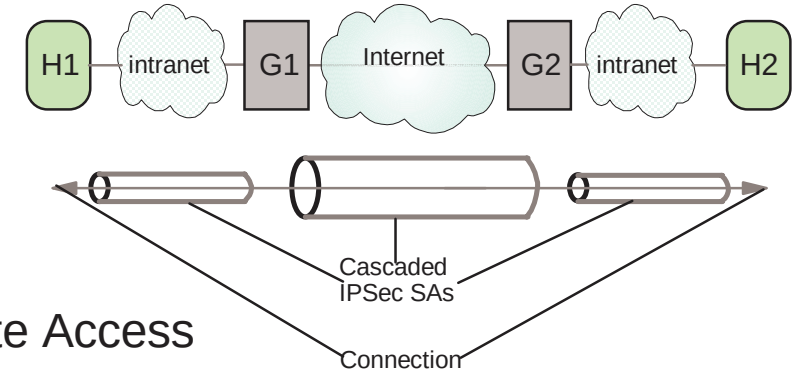
Case 2: Protection over Untrusted Network Segment



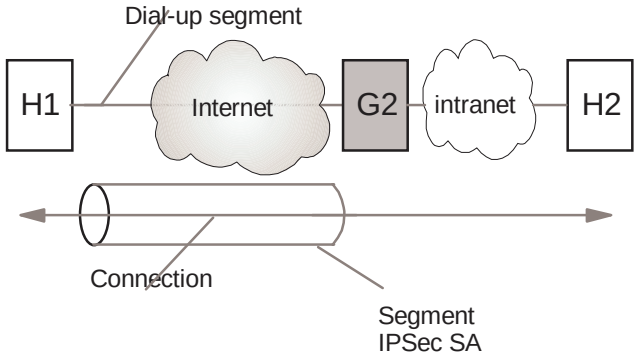
Case 3: End-to-End Security with Added Gateway Authentication



Case 4: End-to-End Security with Cascaded SAs

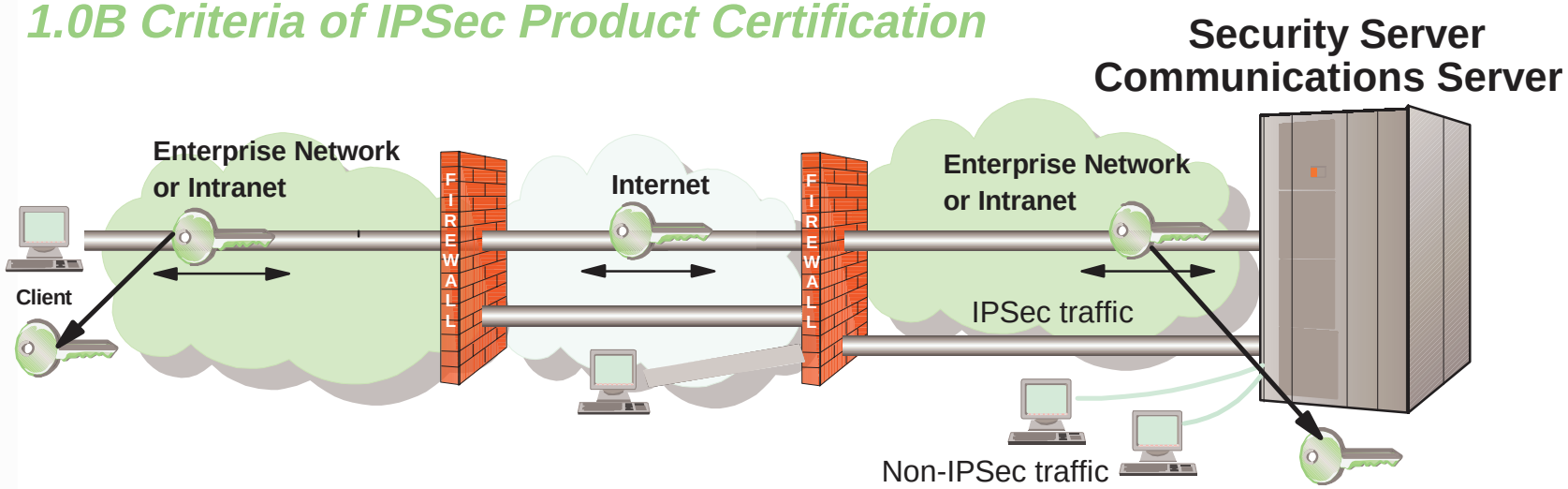


Case 5: Remote Access



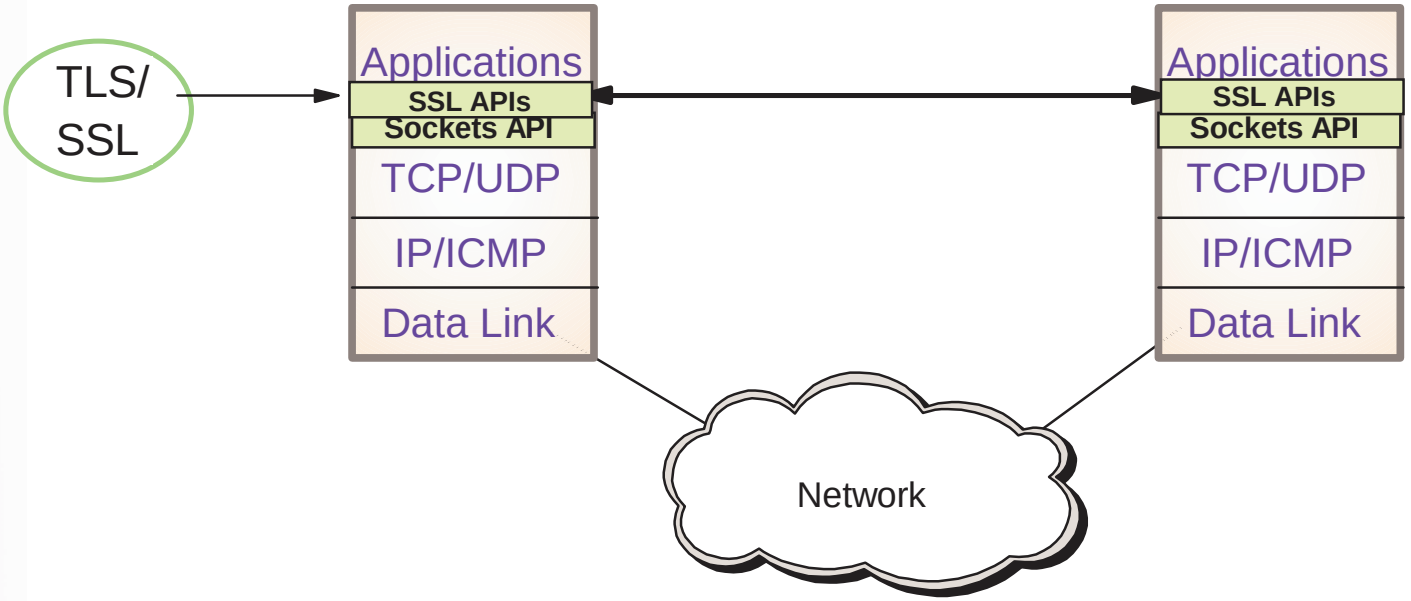
z/OS IPSec and VPN Support

OS/390 IPSec/IKE is Certified by ICSA under 1.0B Criteria of IPSec Product Certification



- **Supports latest IETF standards**
  - RFCs 2401-2406, 2409, 2410
    - Maintains interoperability with previous IPSec RFC levels (1825-1829)
- **Strong Crypto**
  - Triple DES encryption
    - Exploits hardware S/390 cryptographic coprocessor
  - Improved authentication algorithms (HMAC-MD5, HMAC-SHA)
- **IKE Support**
  - Authentication methods
    - Pre-shared key
    - RSA signature (uses X.509 certificates for host-based authentication)
  - Packaging (Firewall Technologies)
    - IKE daemon and configuration (Security Server)
    - TCP/IP IPSec & IKE Support (Communications Server)

Transport Layer Security Overview



- Transport Layer Security (TLS) is defined by the IETF
  - Based on Secure Sockets Layer (SSL)
    - SSL originally defined by Netscape to protect HTTP traffic
  - TLS defines SSL as a version of TLS for compatibility
    - TLS clients and server should drop to SSL V3 based on partner's capabilties
- Provides security services above the transport layer
  - Requires reliable transport layer
    - UDP applications cannot be TLS enabled
- z/OS applications can be TLS or SSL enabled with System SSL
  - z/OS Cryptographic Services

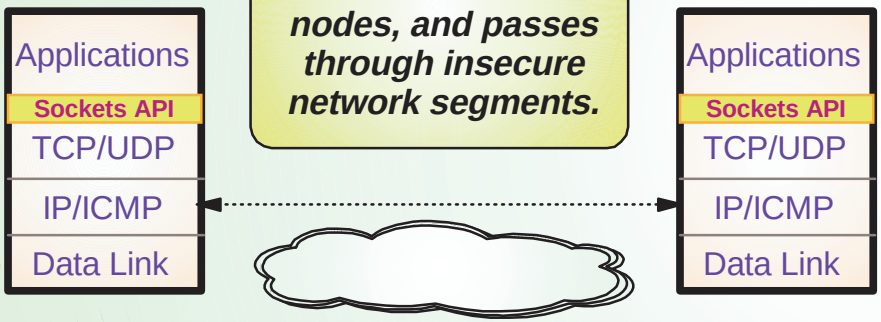
TLS Security Services

- **Protect data in the network using cryptographic security services**
  - ***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
- **Protocol includes**
  - **Negotiation of security parameters**
    - Based on ordered list of acceptable security services and algorithms
  - **Secure Key Exchange**
    - Public key cryptography based
  - **End user identification and authentication**
    - Server to client mandatory
    - Client to server optional

IPSec and SSL/TLS Compared

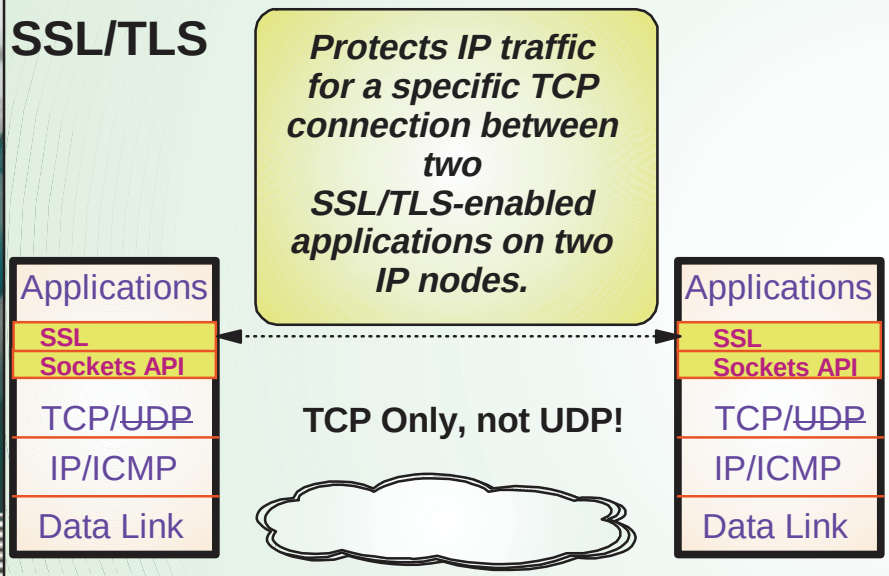
e-business

IPSec



- Provides authentication, integrity, and data privacy at IP layer
  - IKE protocol includes key exchange using public key cryptography and negotiation of security parameters
  - Mgmt of crypto keys and SAs can also be manual
- IP node authentication, not user authentication
- Use of IPSec is transparent to upper layers including application
  - Blanket level protection for upper layer protocols

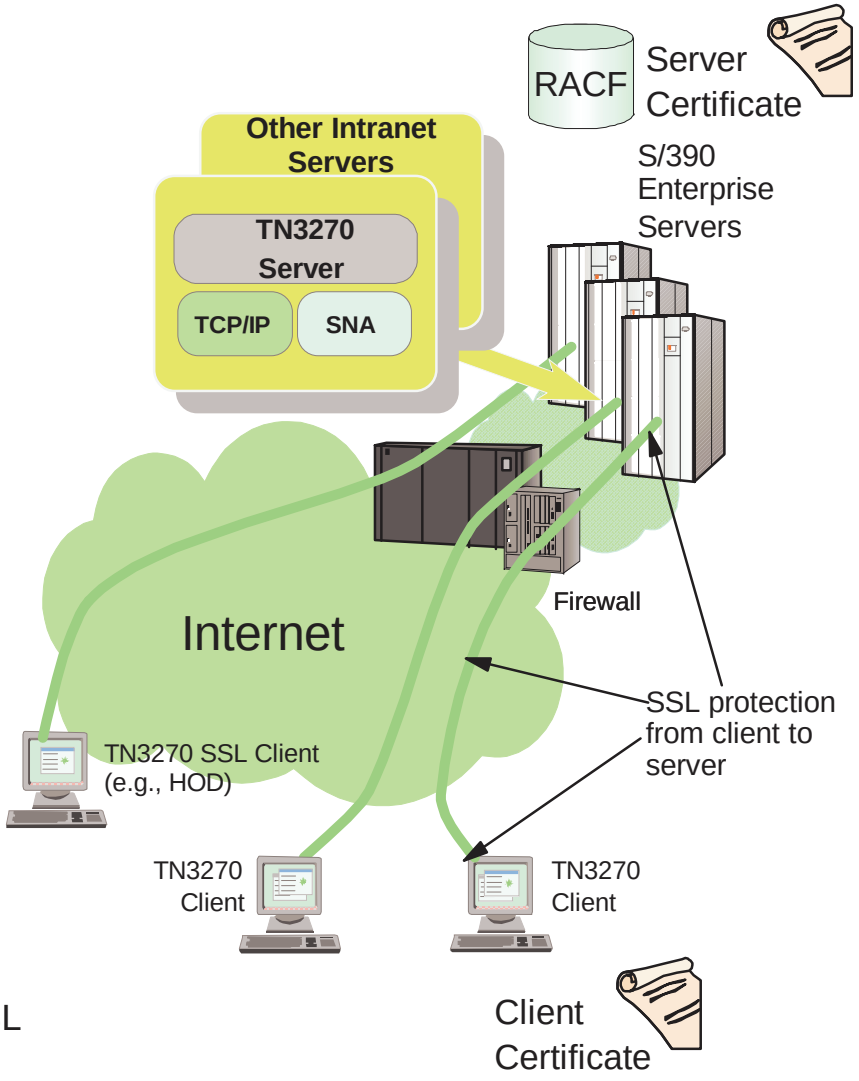
SSL/TLS



- Provides authentication, integrity, and data privacy above TCP layer.
  - SSL handshake protocol includes key exchange using public key cryptography and negotiation of security parameters
- User authentication if client certificates used
- Applications must be changed to use SSL

TN3270 SSL Support for Internet Ready Access to SNA Applications

1. **Secure TN3270 data exchange (V2R6)**
   - SSL Server Side Authentication support using X.509 Certificates
   - DES and Triple DES for data encryption
   - Allows Multiple TN3270 Ports per Server
     - Basic Ports / SSL-Only
   - Client Support
     - Host on Demand V2, PComm V4.3
2. **Pre-Login Access Control using RACF digital certificate support (V2R8)**
   - Client credentials are validated before USSMSG (logon screen) is sent
     1. Uses SSL Client Authentication with client certificate
     2. Access to port allowed if user represented by certificate permitted to SAF resource (SERVAUTH class)
        - EZB.TN3270.sysname.tcpname.portxxxx
   - Client Support
     - Host on Demand V4, PComm V5.0
3. **Negotiable SSL (V2R10)**
   - Uses new IETF defined Telnet Protocols to negotiate whether connection will be protected with SSL
     - SSL security levels negotiated based on policy
   - Simplifies client configuration
     - Allows use of a single port for SSL/non-SSL traffic
   - Client Support
     - Host on Demand V5



z/OS Communications Server

z/OS V1R2 Security Enhancements

- **Integrated Intrusion Detection Services**
- **Built-in Application Security**
  - TLS support for FTP
  - Application enablement for Kerberos
  - Secure network services
- **Express Logon Feature**
- **IPSec and VPN enhancements**
- **FTP Security Enhancements**
- **Netstat Command Access Control**
- **SMTP Exit Interface**

z/OS Communications Server Security

Integrated Intrusion Detection Services

What is an intrusion?

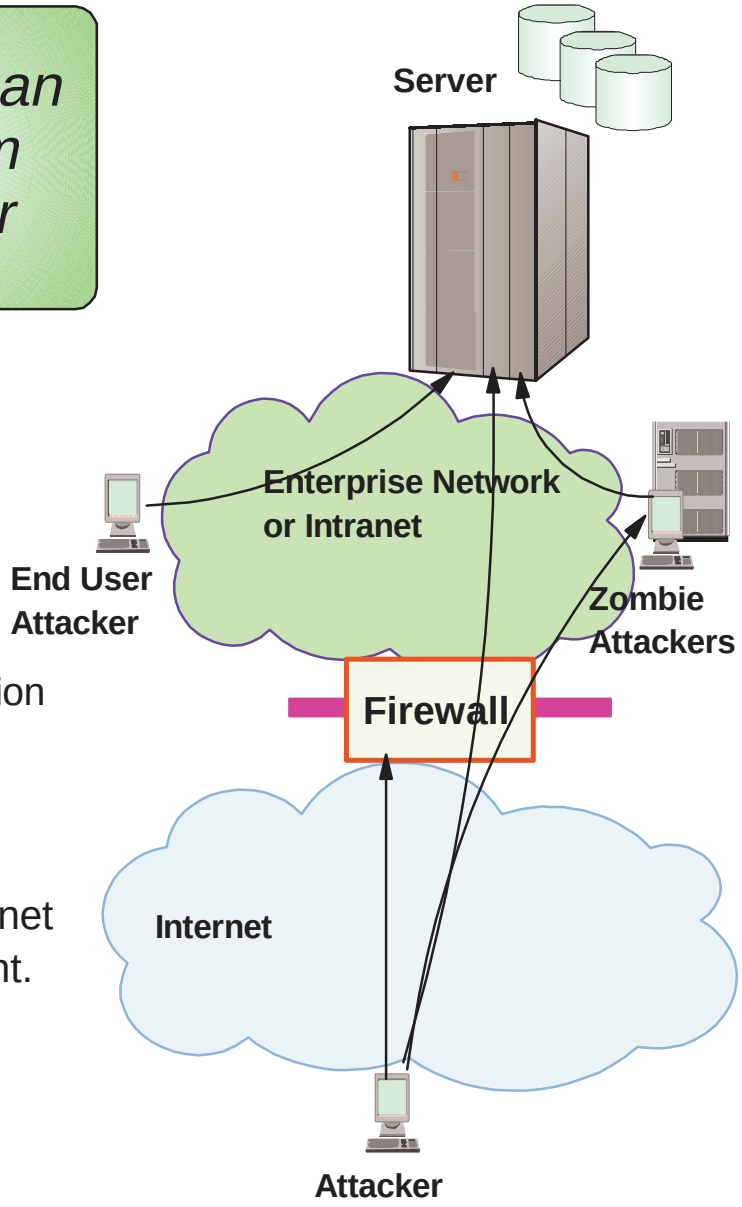
Intrusions can occur from Internet or intranet

Information Gathering
- Network and system topology
- Data location and contents

Unauthorized Usage
- Eavesdropping/Impersonation/Theft
  - On the network/on the host
- Base for further attacks on others
  - Amplifier
  - Robot or zombie

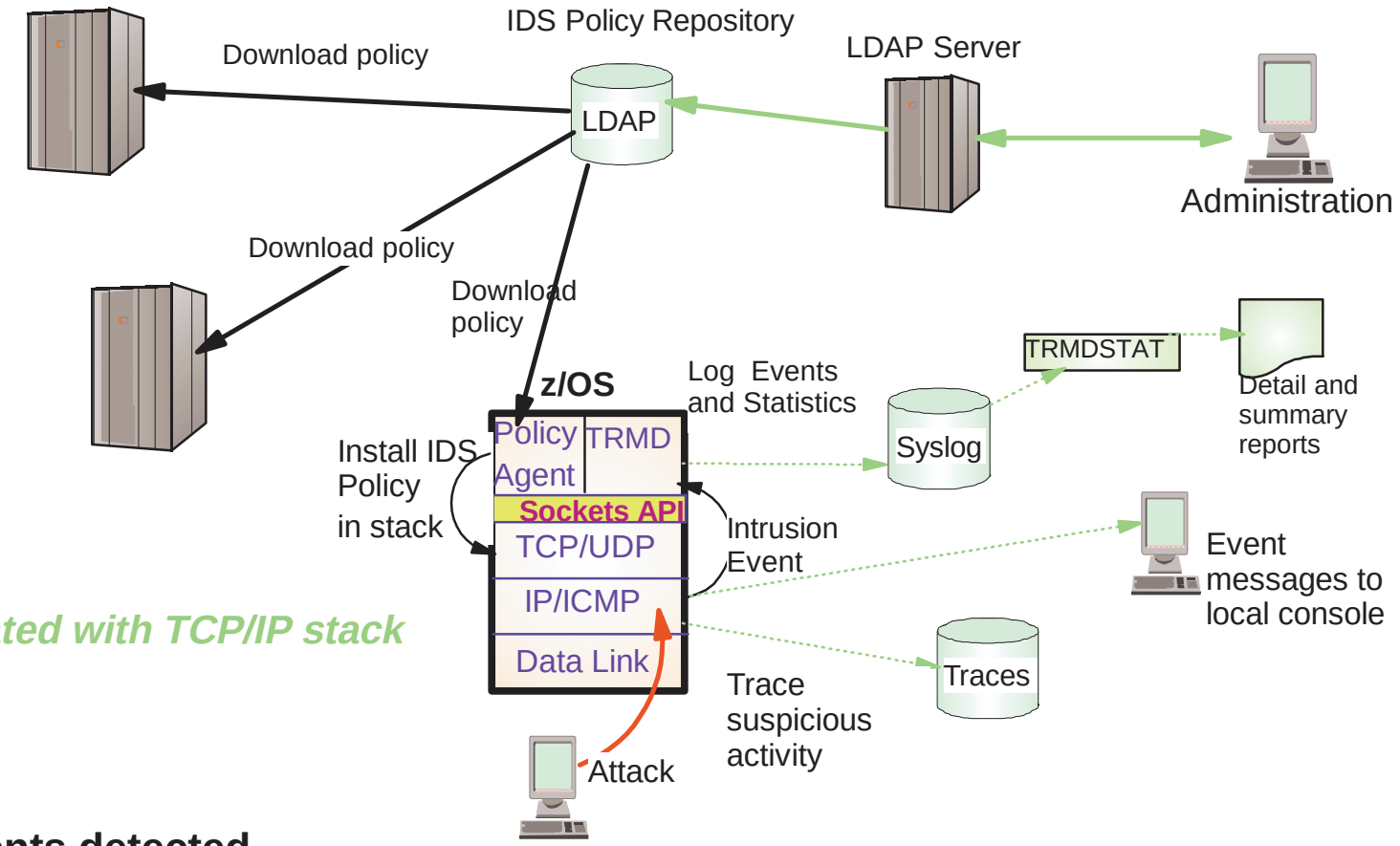
Denial of Service
- Attack on availability
  - Single Packet attacks - exploits system or application vulnerability
  - Multi-Packet attacks - floods systems to exclude useful work

Firewall can provide some level of protection from Internet
Perimeter Security Strategy *alone* may not be sufficient.
Consider:
- Access permitted from Internet
- Trust of intranet
  - Users
  - Ability of servers to withstand being taken over
    - ✓ Amplifiers, Robots, zombies



z/OS Intrusion Detection Services Overview

Integrated Intrusion Detection Services under policy control to identify, alert, and document suspicious activity



Integrated with TCP/IP stack

Events detected

- Scans, Attacks Against Stack, Flooding

Defensive methods

- Packet discard, limit connections

IDS Recording

- Event and statistics logging, event messages to local console, IDS packet trace

IDS Reporting

- trmdstat program for IDS reports

Intrusion Event Types Supported

- Scan detection and reporting
  - Intent of scanning is to map the target of the attack (Subnet structure, addresses, masks, addresses in-use, system type, op-sys, application ports available, release levels)
    - TCP port scans
    - UDP port scans
    - ICMP scans
      - ✓ Sensitivity levels for all scans can be adjusted to control number of false positives recorded.
- Attack detection, reporting, and prevention
  - Intent is to crash or hang the system (Single or multiple packet)
    - Malformed packet events
    - Inbound fragment restrictions
    - IP option restrictions
    - ICMP restrictions
    - SYNflood events
    - Outbound raw restrictions
    - UDP perpetual echo
- Traffic regulation for TCP connections and UDP receive queues
  - Could be intended to flood system OR could be an unexpected peak in valid requests
    - UDP backlog management by port
      - ✓ Packets discard
    - TCP total connection and source percentage management by port (R10)
      - ✓ Connection limiting

z/OS IDS defensive actions

Scan Events

- No defensive action defined

Attack Events

- Packet discard
  - Certain attack events always result in packet discard and are not controlled by IDS policy action
    - ✓ malformed packets
    - ✓ synflood
  - Some attack types controlled by IDS policy action
    - ✓ ICMP option restrictions
    - ✓ ICMP redirect restrictions
    - ✓ IP protocol restrictions
    - ✓ IP fragment
    - ✓ outbound raw restrictions
    - ✓ perpetual echo

Traffic Regulation Events

- Controlled by IDS policy action
  - TCP - Connection limiting
  - UDP - Packet discard

z/OS IDS recording actions

Recording options controlled by IDS policy action specification

- Recording suppression provided if quantity of IDS console messages reach policy-specified thresholds

Options

- Event logging
  - Syslogd
    - ✓ Number of events per attack subtype recorded in a five minute interval is limited
  - Local Console
- Statistics
  - Syslogd
    - ✓ Normal, Exception
- IDS packet trace
  - Activated after attack detected
    - ✓ Number of packets traced for multi-packet events are limited
    - ✓ Amount of data trace is configurable (header, full, byte count)

All IDS events recorded in syslog and console messages, and packet trace records have probeid and correlator

- Probeid identifies the specific event detected
- Correlator allows events to be matched with corresponding packet trace records

Using IDS Console Messages for Automation

- Console message can drive message automation
  - MPF message suppression can suppress message output to system console
- Example automation actions:
  - Route message to NetView console(s)
  - email notification to security administrator
  - Run trmdstat and attach output to email
- Selectors
  - Automate based on message number, other message content
    - e.g. event type, probeid

Message is multi-line WTO:

- **Always written**
  - **EZZ8761I IDS EVENT DETECTED** *nnn*
  - **EZZ8762I EVENT TYPE:** *eventtype*
  - **EZZ8763I CORRELATOR** *ccccc* **- PROBEID** *iiiiiiii*
- **Written if source IP address or port is present**
  - **EZZ8764I SOURCE IP ADDRESS** *sss.sss.sss.sss* **- PORT** *ppppp*
- **Written if destination IP address or port is present**
  - **EZZ8765I DESTINATION IP ADDRESS** *ddd.ddd.ddd.ddd* **- PORT** *ppppp*
- **Always written**
  - **EZZ8766I IDS RULE** *rulename*
  - **EZZ8767I IDS ACTION** *actionname*

NetView clists: http://www.tivoli.com/support/downloads/netview_390/tools/idsauto.html

Defining IDS Policy

e-business

Policy Object examples with
beie.a.aace.
eiitios.
slpptcpipsamples.

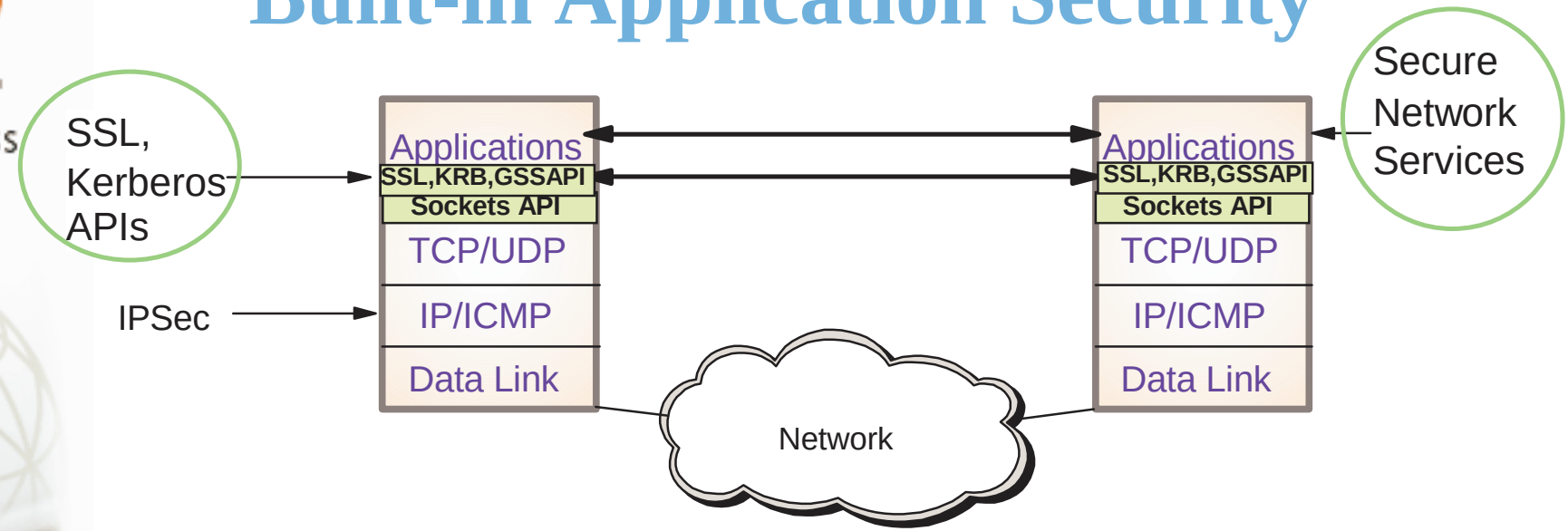
- pagent_starter_IDS.ldif
- pagent_advanced_IDS.ldif

1. Start with the samples
2. Consult the associated INFO APARS (II12498, II12499) to understand how to change the samples to fit your LDAP environment.
3. Consult the IP Configuration Guide and the IP Configuration Reference to understand and evaluate additional capabilities
4. Learn LDAP V3 Policy Schema syntax as needed

zIDSManager "as is" Web Tool: Coming Soon! to implement LDAP policies.
Will be available at:
http://www-3.ibm.com/software/network/commserver/downloads

Built-In Application Security

Built-in Application Security



TLS Enabled FTP Server and Client

- Secure file transfer by providing encryption, authentication, and message integrity for the FTP control and data connections
  - Strong authentication using X.509 Certificates (including client authentication)

Application Kerberization

- FTP Server and Client, Unix telnet daemon, Unix rsh daemon
  - Strong 3rd party authentication for client/server applications using secret key cryptography, encrypted data flows

Secure Network Services

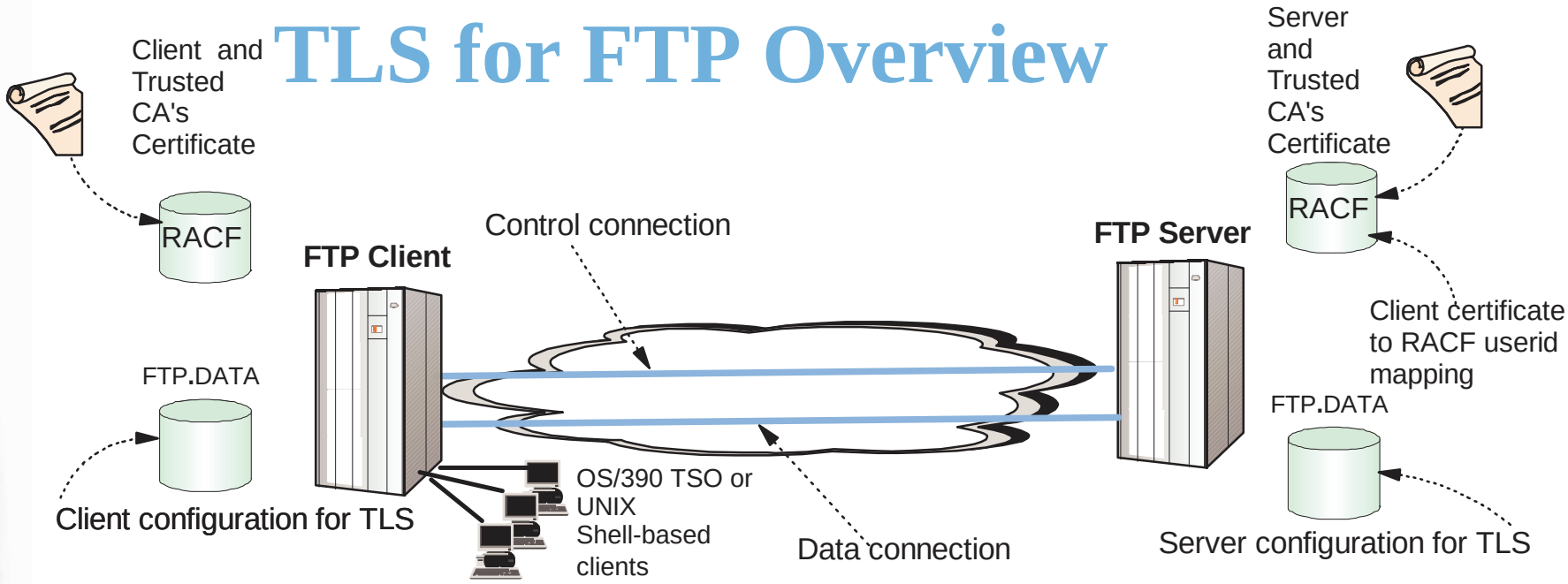
- Secure DNS
  - Ensures DNS query replies are authentic
- OSPF MD5 Authentication
  - Ensures routing table integrity
  - Uses MD5 authentication for routing messages (RFC 2328)

TLS Enablement for FTP

Both the z/OS FTP client and FTP server are enhanced to support Transport Layer Security (TLS). This support is based on three IETF definitions:

- The TLS Protocol (RFC 2246)
- Securing FTP with TLS (IETF draft)
- Subset of FTP Security Extensions (RFC 2228)

TLS for FTP Overview



- **Key features**
  - **Protection of data in the network**
    - Data origin authentication, data integrity, and privacy
  - **Server and client configuration provided to control security policy for TLS session**
    - TLS negotiation will find an agreeable policy or TLS setup will not proceed.
  - **Flexible selection of control and data connection protection**
    - Can choose to TLS protect just the control connection
    - TLS protection for the data connection can be turned on and off during life of the FTP session (i.e. life of the control connection)
  - **PKI based authentication of end users added. Options are:**
    - Basic - userid/password (always required)
    - TLS authentication of client certificate
    - Cross-checking of userid entered with userid associated with client certificate
  - **Key Ring Security**
    - Stored in RACF key ring using RACF digital certificate support
    - Stored in HFS file

How TLS is Requested

- **Unconditional TLS**
  - ➤ Uses separate protected ports for TLS (port 989 and 990)
    - – TLS for client and server assumed
- **Negotiable TLS**
  - ➤ Both TLS and non-TLS traffic share standard ports (20 and 21)
    - – Negotiation based on subset of the FTP security negotiation functions documented in RFC 2228
  - ➤ New FTP command to request negotiable mode TLS
    - – AUTH TLS | TLS-C | TLS-P | SSL
    - ✓ Server accepts all AUTH mechanisms, Client sends only TLS
  - ➤ Server must be configured to specify that the AUTH comand with TLS is supported
    - – EXTENSIONS statement with Auth_TLS
  - ➤ TLS can be specified as required or optional on the standard FTP ports

Securing FTP by Connection Type

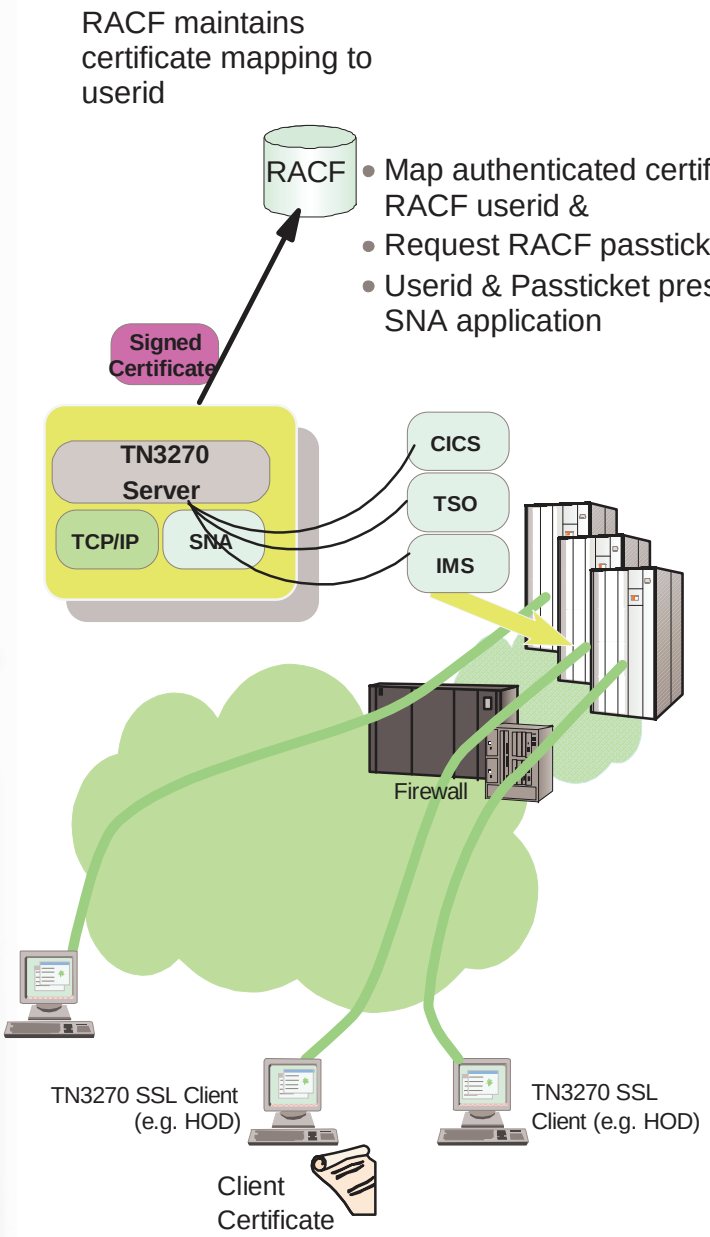
- **FTP has both a control and data connection. Possible combinations of TLS protection are:**
  - Control connection security only
  - Both control connection and data connection security
    - **Data connection security only not supported**
- **FTP server can be configured to specify security requirements for the data connection. Options are:**
  - Not allowed, Allowed, Required
- **New FTP command to request data connection protection levels**
  - PROTECT private
    - **TLS always uses data authentication and integrity / encryption is optional**
    - **Protection is based on ciphersuite negotiations**
    - **TLS session is negotiated for each data connection**
  - PROTECT clear
    - No TLS for the data connection

Express Logon Feature

Express Logon Feature for SNA Applications

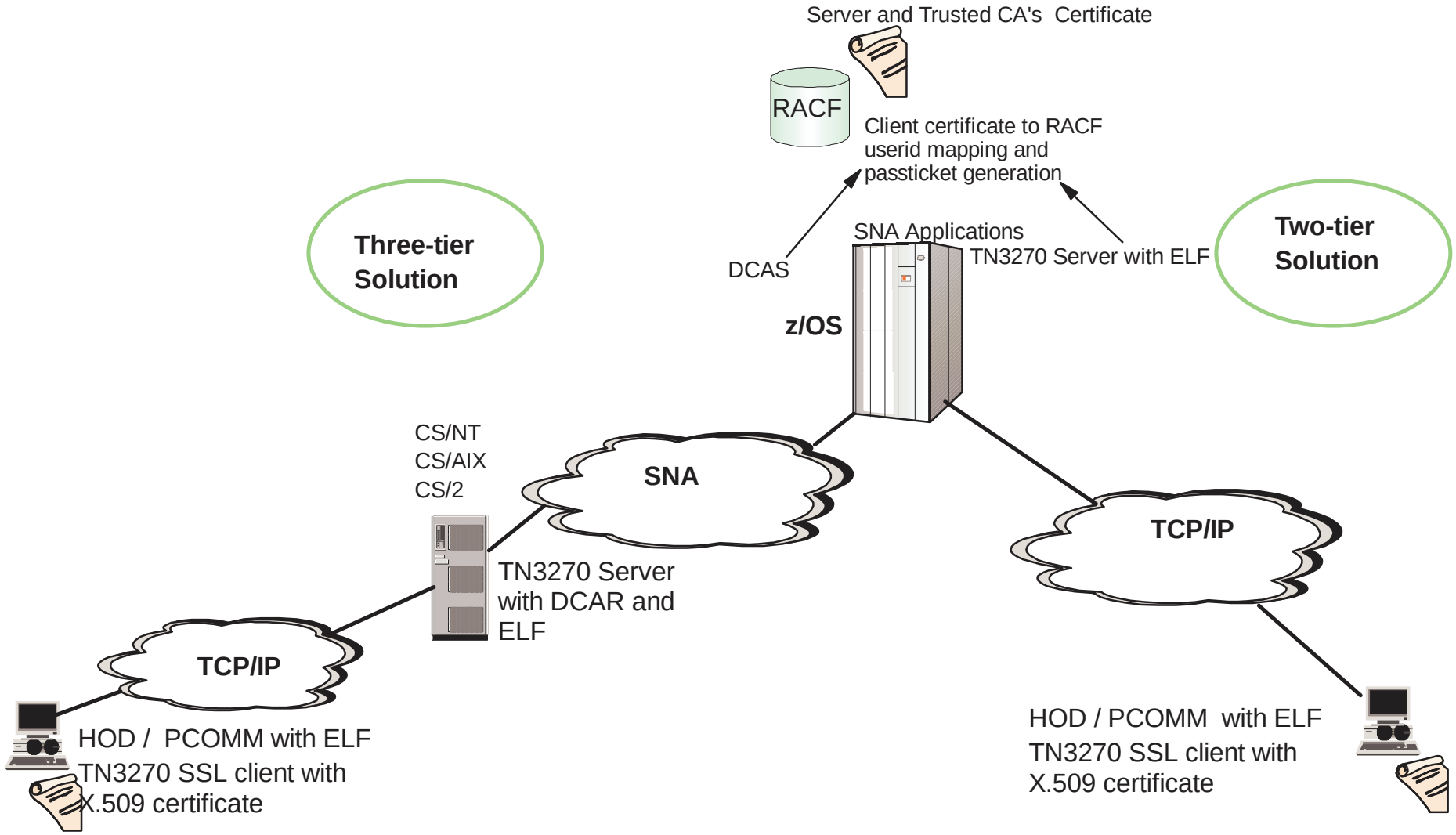
e-business

Simplifies userid and password administration



- **End user is not required to enter userid and password for SNA application signon**
  - ➤ No change to SNA application required
    - **TN3270 Server uses RACF Passticket support for application transparency**
      - ✓ **Passticket one-time password**
- **Uses Host On-Demand V5 or PComm V5.5 for login screen recognition and identification**
  - ➤ Administrator uses emulator's macro recording facility
    - **Captures the interaction sequence**
    - **and location on the panels of the userid and password**
- **TN3270 Server inserts userid and passticket into inbound datastream**
  - ➤ In place of symbolics inserted during emulator's macro playback
- **A single authenticated client certificate can be used for user identification to multiple SNA applications**
  - ➤ TN3270 Server application-qualifies certificate during certificate to userid mapping
    - **Applid provided by TN3270 client**

Express Logon Network Designs



Three Tier Support

Middle Tier TN3270 Support - via PTFs on CS2 6.1, CS/NT 6.1.1, CS/AIX 6.0.0.1 via PTF

TN3270 Client - Host On-Demand V5.0, PComm V5.5

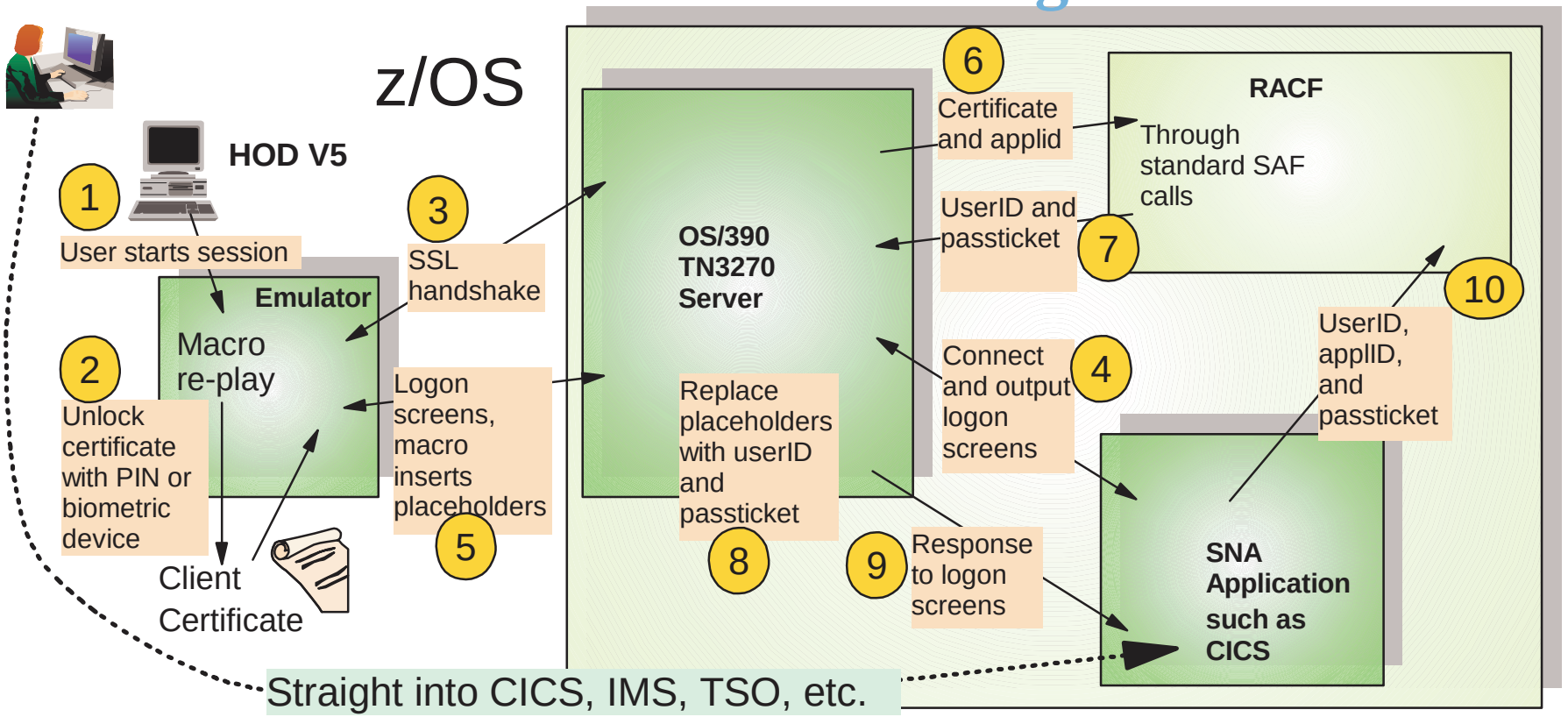
DCAS - CS OS/390 V2R10 PTF

Two Tier Support

TN3270 Server - z/OS CS V1R2 (Rollback to CS OS/390 V2R10 via PTF (UQ55691))

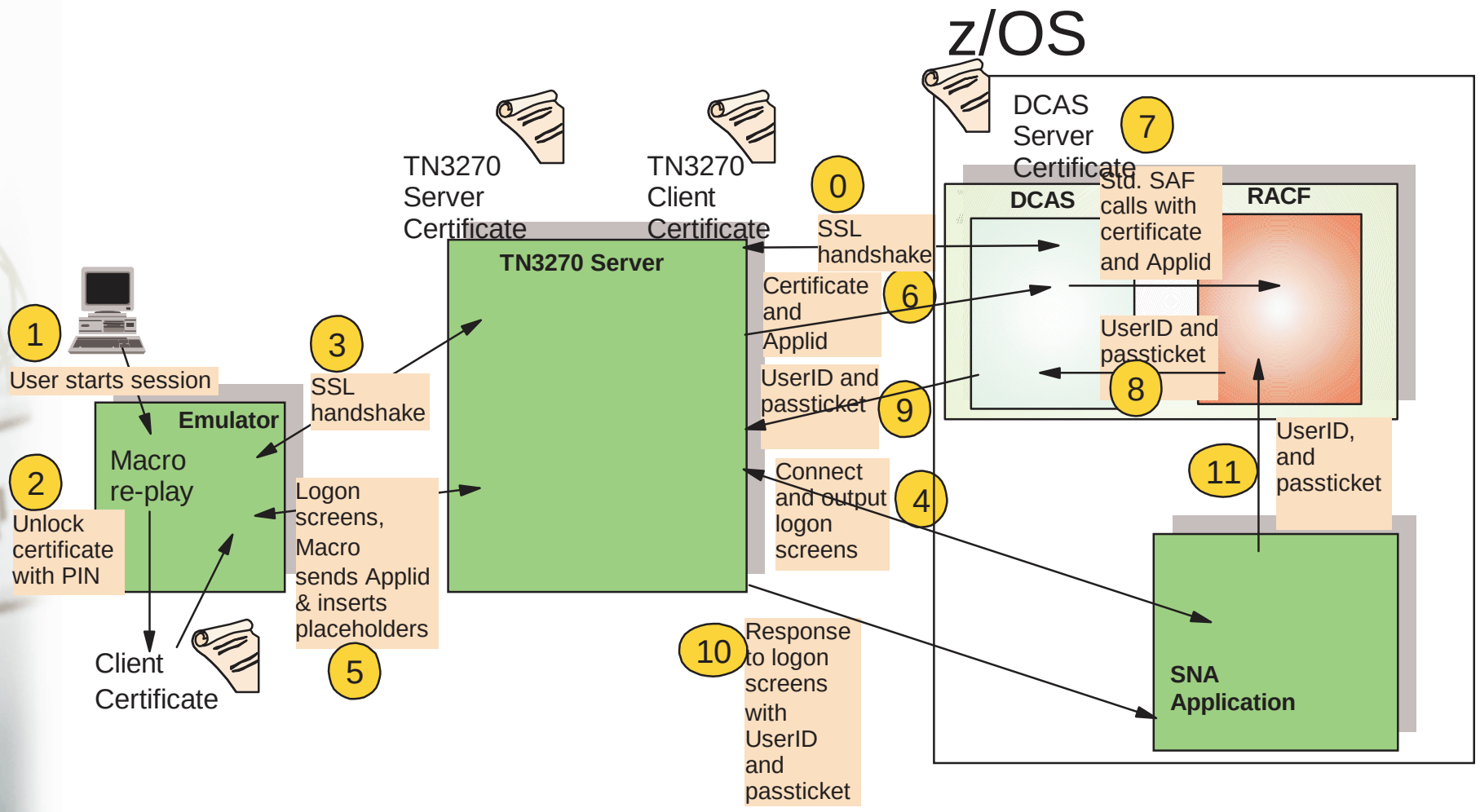
TN3270 Client - Host On-Demand V5.0, PComm V5.5

Express logon in z/OS V1R2 - extend client certificate to SNA logon
Two Tier Design



- Administrator would use emulator's macro recording facility to capture the interaction sequence and location on the panels of the userid and password
- The solution does not require changes in the TN3270 protocol but does require cooperation by the client software
  - During SSL handshake, the passticket capabilities are negotiated via the "Telnet New Environment Option" as defined in RFC1572 - environment options used are: PASSTICKET and APPLID.
  - The client must identify which application to use on the APPLID environment option.
- When the macro sends the generated response to the logon screen, it inserts placeholders where the userID and password should be; the TN3270 server intercepts these, obtains a userID and passticket, fills them in and forwards the logon screen input to the application, which then does normal SAF calls to verify the user's identity.

Express Logon Feature Process Steps
Three Tier Solution



- TN3270 Server on middle tier performs insertion of userid and passticket into inbound logon screen
- TN3270 Server request RACF services on z/OS in order to obtain userid and passticket
  - z/OS CS Digitial Certificate Access Server (DCAS) provides this information to Middle Tier TN3270
  - Middle Tier TN3270 must use SSL when communicating with DCAS
  - TN3270 Server must supply a client certificate for SSL session to DCAS
  - DCAS converts TN3270 Server client certificate to userid and verifies that the userid representing the requesting TN3270 server is authorized to access DCAS services
  - SSL session can be long running

Additional Security Enhancements

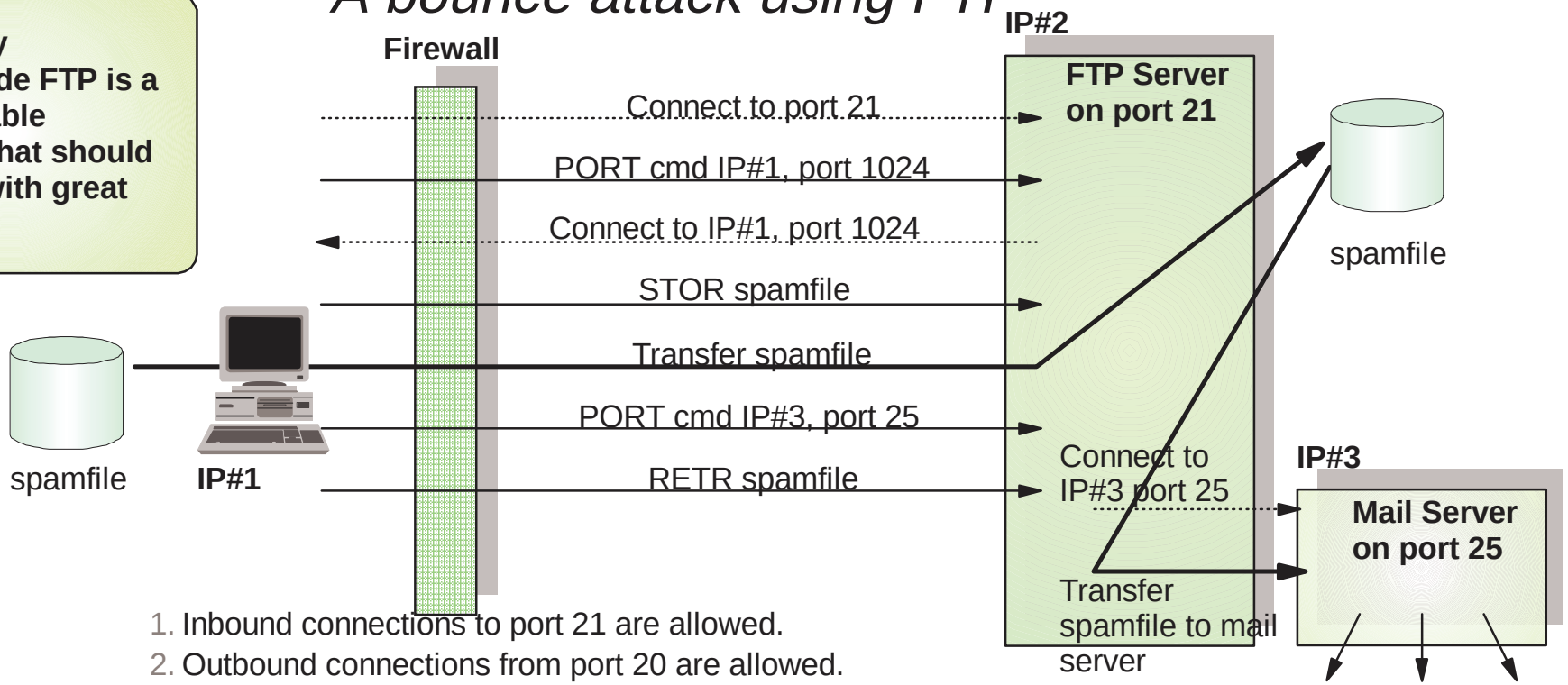
VPN Enhancements

- Remove requirement for Security Server license for IKE and Configuration Server
  - **Available back to OS/390 V2R10 with APAR OW47982**
- New Configuration Assistant to Configuration GUI
  - **Combination Wizard and Help**
  - **Simplifies configuration by guiding administrator through the configuration steps for:**
    - Filter rules
    - Manual security associations (SA)
    - Dyanmic SAs
- Commit bit processing
  - **Guarantees SA active on both IPSec hosts before SA is used**
- Configuration Server exploitation of RACF key rings
  - **Previously private key kept in HFS file**
- IKE performance improvements
  - **Internal dispatching scheme improved to support more concurrent IKE SA negotiations**
- IPSec performance improvements
  - **Path MTU Discovery supported with IPSec**
    - Allows larger segments without fragmentation in network
  - **Improved use of Crypto Coprocessor to get better use of multiprocessors**
    - Adjust breakpoints for hardware / software encryption and authentication
    - Track IPSec queue depth for hardware and use software if queue depth threshold exceeded
    - After hardware crypto ops, end SRB and redispatch to reduce execution time on CP system

FTP Port Command Restrictions
Prevents "bounce" attack

A bounce attack using FTP

Three-way proxy-mode FTP is a questionable function that should be used with great caution!



1. Inbound connections to port 21 are allowed.
2. Outbound connections from port 20 are allowed.
3. Everything else is disallowed.

Without breaking firewall rules, the malicious user managed to create a spam mail attack inside the firewall from outside the firewall!

z/OS V1R2 FTP Server enhanced to allow restrictions on use of PORT command

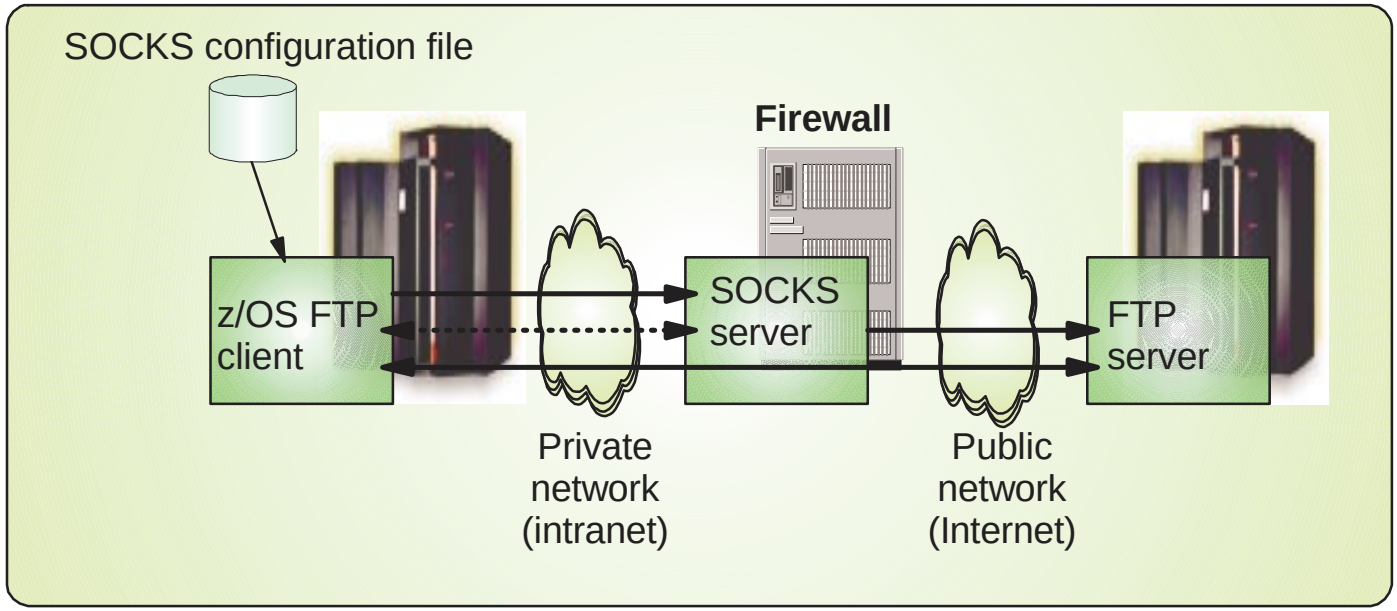
- **New configuration in FTP.DATA support these possible actions:**
  - **Accept or Reject all PORT commands**
  - **Reject all PORT commands that contain a well-known port**
  - **Reject all PORT command that contain IP address that's different than FTP client IP address**

FTP Command Security Exit can also be used to control use of PORT command (Available prior to V1R2)

Socksified FTP client in z/OS V1R2

- SOCKS is a very common relay server on firewalls.
- SOCKS allow TCP connections to be relayed on a firewall in such a way that intranet IP addresses are not revealed to the public network - it is an application-layer gateway type of firewall technology.
- Clients that connect through a SOCKS server must have specific support for doing so (to be socksified).
- Servers that are being used through a SOCKS server do not need any modifications.

- The SOCKS configuration file instructs the FTP client which destinations (IP address ranges) can be reached directly and which require use of a SOCKS server.
- Intranet destinations directly; everything else via a SOCKS server at a given intranet IP address.



No longer a need to stage data on a workstation if you need to transfer data sets or files directly to/from z/OS to/from an Internet destination. One example is when transferring data to/from the IBM support site.

Additional Security Enhancements...

- Netstat command access control using RACF
  - Ability to restrict Netstat usage
    - Can now define access control at Netstat option level
      - ✓ EZB.NETSTAT.sysname.tcpname.netstat_option
- New SMTP exit interface
  - Allows installation to provide exit that can control how mail is processed
    - Can be used to implement installation's policy regarding spam control
    - The exit receives control for most SMTP data flows
      - ✓ SMTP command processing
      - ✓ Access to actual incoming data
    - Exit can decide whether mail is accepted or not
  - Exit sample provided

Communications Server Security Features

- **Protecting system resources and data from the network**
  - RACF protection of z/OS resources *
    - z/OS CS application access to data sets and files
    - Local user access to TCP/IP system, TCP and UDP ports
  - Protect system availability
    - Built in protection against Denial of Service attacks
    - IP packet filtering
    - Syslogd integrity and availability
    - Connection limiting
- **Protecting mission critical data in the network**
  - Strong encryption with Triple DES
    - Using hardware assist from crypto coprocessor
  - Transparent Application Security
    - IPSec for TCP/IP applications
      - *ICSA Certified at 1.0B Criteria for IPSec Product Certification*
    - Internet-ready access to SNA applications with TN3270 SSL
    - Express Logon Feature *
  - Built-in Application Security *
    - SSL-enabled FTP, Kerberized FTP, rsh, telnet
  - Secure network services
    - SNMPv3, Secure OSPF Authentication *, Secure DNS *
- **Recording security events**
  - Access control events
    - RACF audit records, filter rule event logging
  - Integrated Intrusion Detections Services *
    - Detects and records scans, stack attacks, flooding

* *New in z/OS V1R2*

Index to Functions by Release

OS/390 V2R5

- VPN
  - IPSec (RFCs 1825-1829)
  - Tunnel mode IPSec
- IP Filtering
- Secure network services
  - Secure dynamic DNS

OS/390 V2R6

- VPN
  - Transport mode IPSec
- TN3270 SSL
  - Server Auth

OS/390 V2R7

- VPN
  - IPSec RFC Upgrade (2401-2406,2410)
  - 3DES
- Secure network services
  - SNMPv3
- System Resource Protection
  - Limiting Inbound TCP connections
    - QoS Connection Limits (limits on QoS policy basis)

OS/390 V2R8

- VPN
  - IKE and dynamic tunnels
  - *ICSA Certified at 1.0B Criteria for IPSec Product Certification*
    - *IPSec and IKE*
- TN3270 SSL
  - Client Authentication
  - Pre-login Access Control using RACF
- 3DES for SNA SLE

OS/390 V2R10

- VPN
  - On Demand Tunnels
- TN3270 SSL
  - Negotiable SSL
  - RACF Key Ring support
- System Resource Protection
  - RACF access control for TCP resources
    - Stack Access Control
    - Port Access Control
    - Network Access Control
  - Limiting Inbound TCP Connections
    - Traffic Regulation Manager (fair share limiting)
  - Syslogd Isolation

z/OS V1R2

- Integrated Intrusion Detection Services
- Secure network services
  - Secure DNS
  - OSPF Authentication
- Built-in Application Security
  - FTP SSL (Client and Server)
  - Kerberos
    - FTP Client and Server
    - Unix telnet
    - Unix rsh
- TN3270 SSL
  - Express Logon Feature
- System Resource Protection
  - FTP Security Enhancements
  - SMTP Exit Interface
  - Restrict Netstat Access using RACF

For More Information....

URL	Content
http://www.ibm.com/servers/eserver/zseries	IBM Enterprise Servers (z900 & S/390)
http://www.ibm.com/servers/eserver/zseries/networking	z900 Networking
http://www.ibm.com/servers/eserver/zseries/networking/technology.html	Networking White Papers and Information
http://www.ibm.com/software/network	Networking & Communications Software
http://www.ibm.com/software/network/commserver	Communications Server
http://www.ibm.com/software/network/commserver/library	CS White Papers, Product Doc, etc.
http://www.redbooks.ibm.com	ITSO Redbooks
	Security in OS/390-based TCP/IP Networks (SC24-5383)
	A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Server, and Client Solutions (SC24-5201)
	A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key an Policy Management (SC24-5309)
http://www.ibm.com/support/techdocs/	Advanced Technical Support (Flashes, Presentations, White Papers, etc.)