

ibm.com



e-business

e-business security for z/OS 1.2

SecureWay Communications Server for z/OS 1.2 Security Enhancements



Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2001

CS for z/OS Network Security Technologies as of z/OS 1.1



Redbooks

International Technical Support Organization

Agenda

- **Network Access Control via Firewall Technologies**
- **Communication Security with the IPsec Virtual Private Networks**
- **Typical OS/390 Configuration**
- **Enhanced User Access Control to TCP/IP Resources**
- **Limitation of Inbound TCP Connection Requests**
- **Communication Security with the SSL protocol**

Introduction

• Security Threats

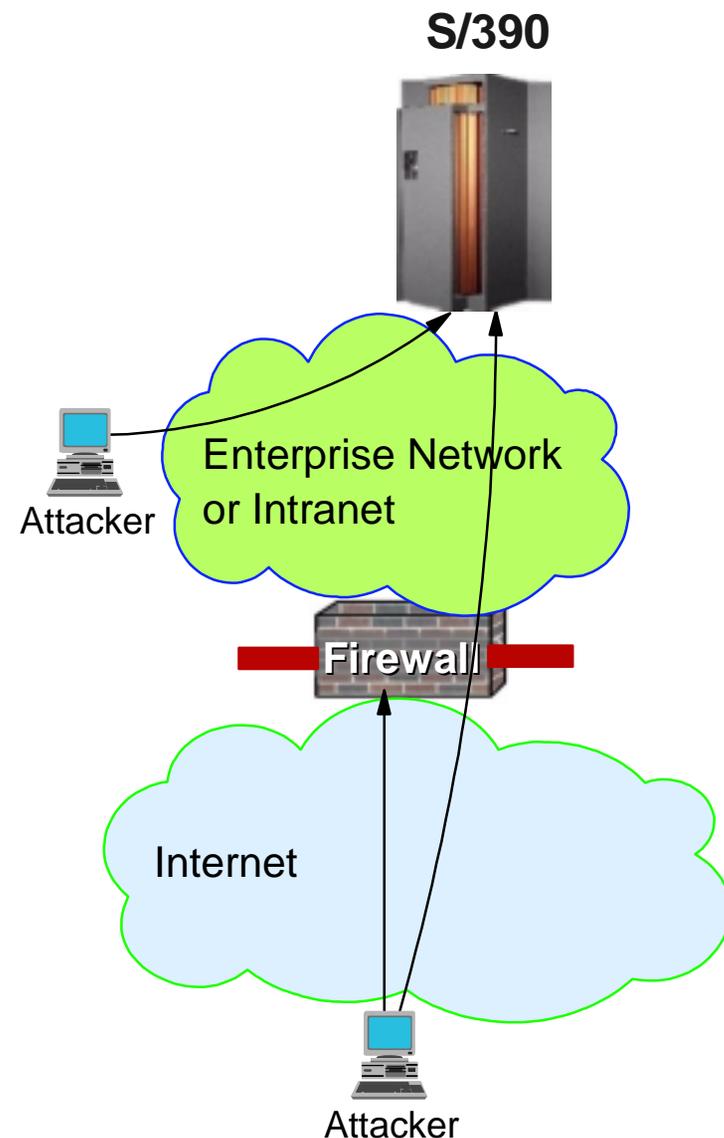
- **Eavesdropping/Impersonation/Theft** - On the network/on the host
 - Addressed by Encryption, Authentication, and Access Control
- **Denial of Service** - Attack on availability
 - ✓ Single Packet attacks - exploits system or application vulnerability
 - ✓ Multi-Packet attacks - floods systems to exclude useful work
 - Addressed by defensive well-written system code, firewalls, authentication techniques

• Attacks can occur from Internet or intranet

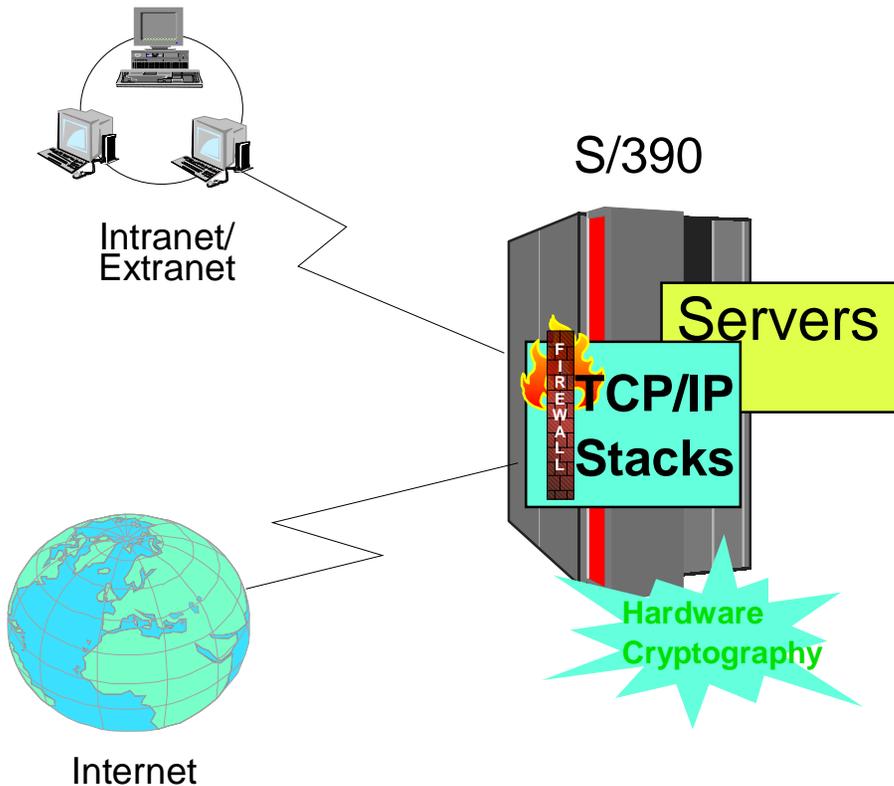
- **Firewall can provide some level of protection from Internet**
- **Perimeter Security Strategy *alone* may not be sufficient.**
 - Considerations:
 - ✓ Access permitted from Internet
 - ✓ Trust of intranet

• Enterprise Servers must be resistant against security breach

- **Secure platform is prerequisite**
- **Secure network and application infrastructure should be built on this base**



OS/390 - z/OS Firewall Technologie



• Firewall Technologies

– IP Filtering

- filters traffic based on source, destination, protocol, etc ..

– FTP Proxy server

- relays FTP communications between private network from external network, with insulation between networks

– SOCKS V4 server

- generic proxy (protocol independent)

– Network Address Translation (NAT)

- private network IP addresses are not disclosed to the external network

– IPSec Virtual Private Network (VPN)

- TCP/IP communications privacy and authentication via encryption

• Multiple TCP/IP Stacks in one OS/390 image

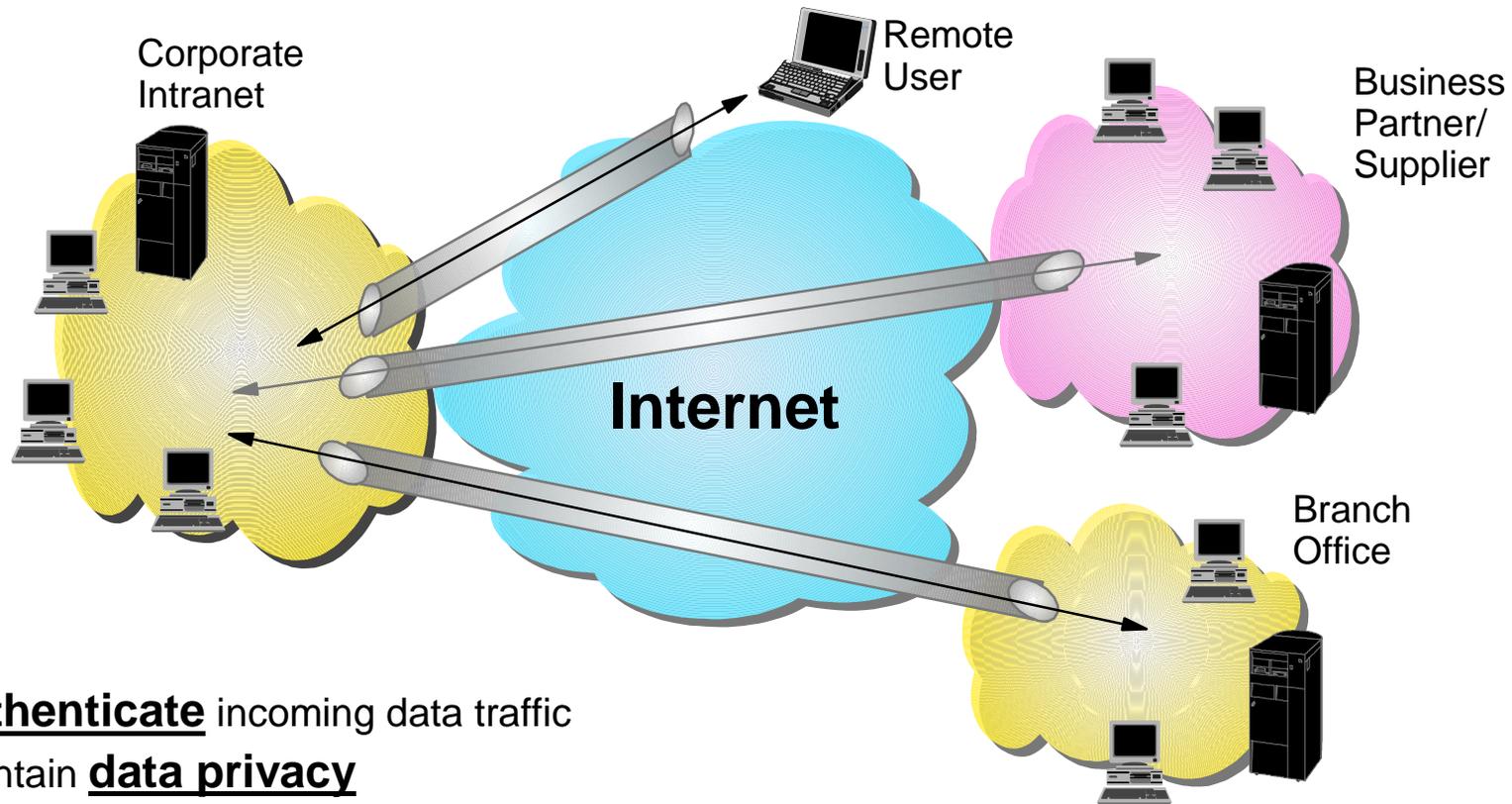
• The OS/390 HTTP server is also an HTTP proxy

z/OS Firewall Technology Deliverables...

- In OS/390 Security Server (licensed products)
 - FTP proxy server
 - Socks V4 server
 - Command Line Configuration (no Security Server license required)
 - Configuration Server (GUI) (OS/390 R7)
 - IPSec VPN Key server (dynamic tunnels) (OS/390 R8)
- In OS/390 Communications Server
 - IP filters
 - Real Audio Support
 - IPSec VPNs (manual tunnels)
 - Network Address Translation (N.A.T.)
 - Enhanced Syslog Daemon

Virtual Private Networks (IPSec)

Secure extension of your company's private intranet across a public network



Authenticate incoming data traffic

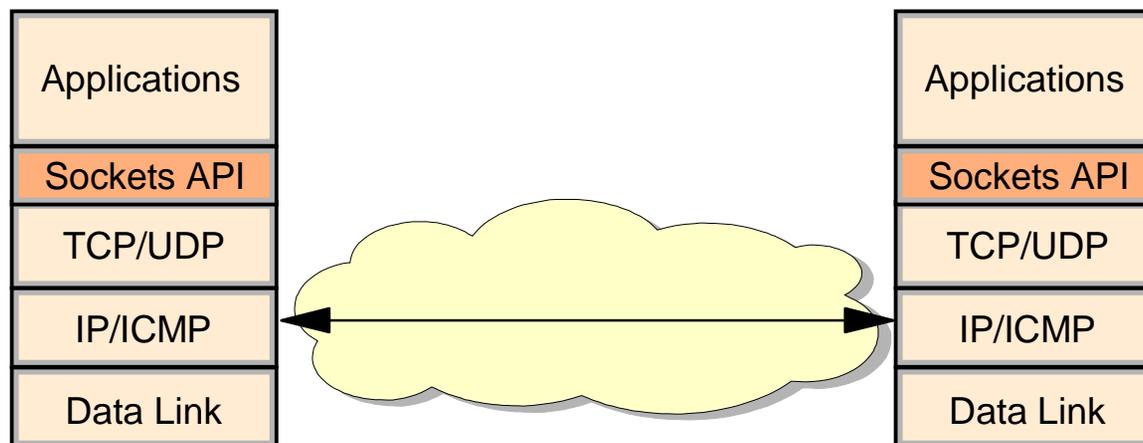
Maintain **data privacy**

Manage access as with private network

Security Association (secret key, ...)

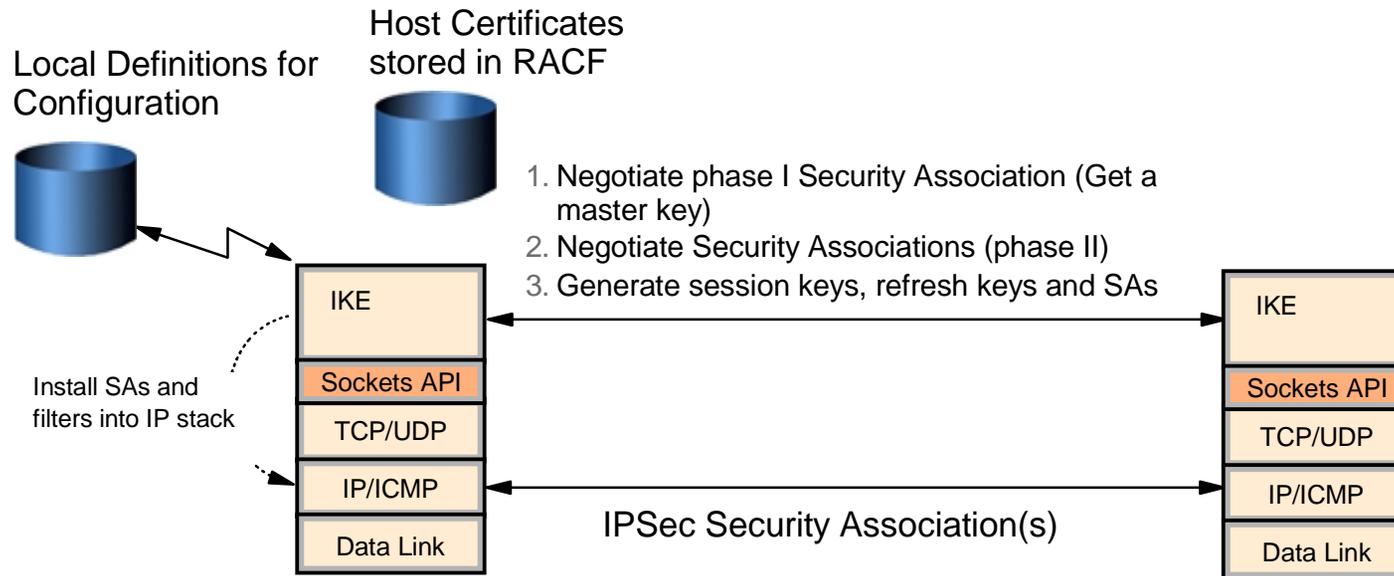
to be setup at both ends of the communication

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 Dynamic Tunnels in OS/390



• IKE Support (V2R8)

- Packaging

- ▶ ISAKMP daemon and configuration (Security Server)
- ▶ TCP/IP IKE Support (CS OS/390)

- Authentication methods

- ▶ Pre-shared key
- ▶ RSA signature (uses X.509 certificates for host-based authentication)

- Locally Configured

- ▶ Host certificates and Policy

• On-Demand Tunnels (V2R10)

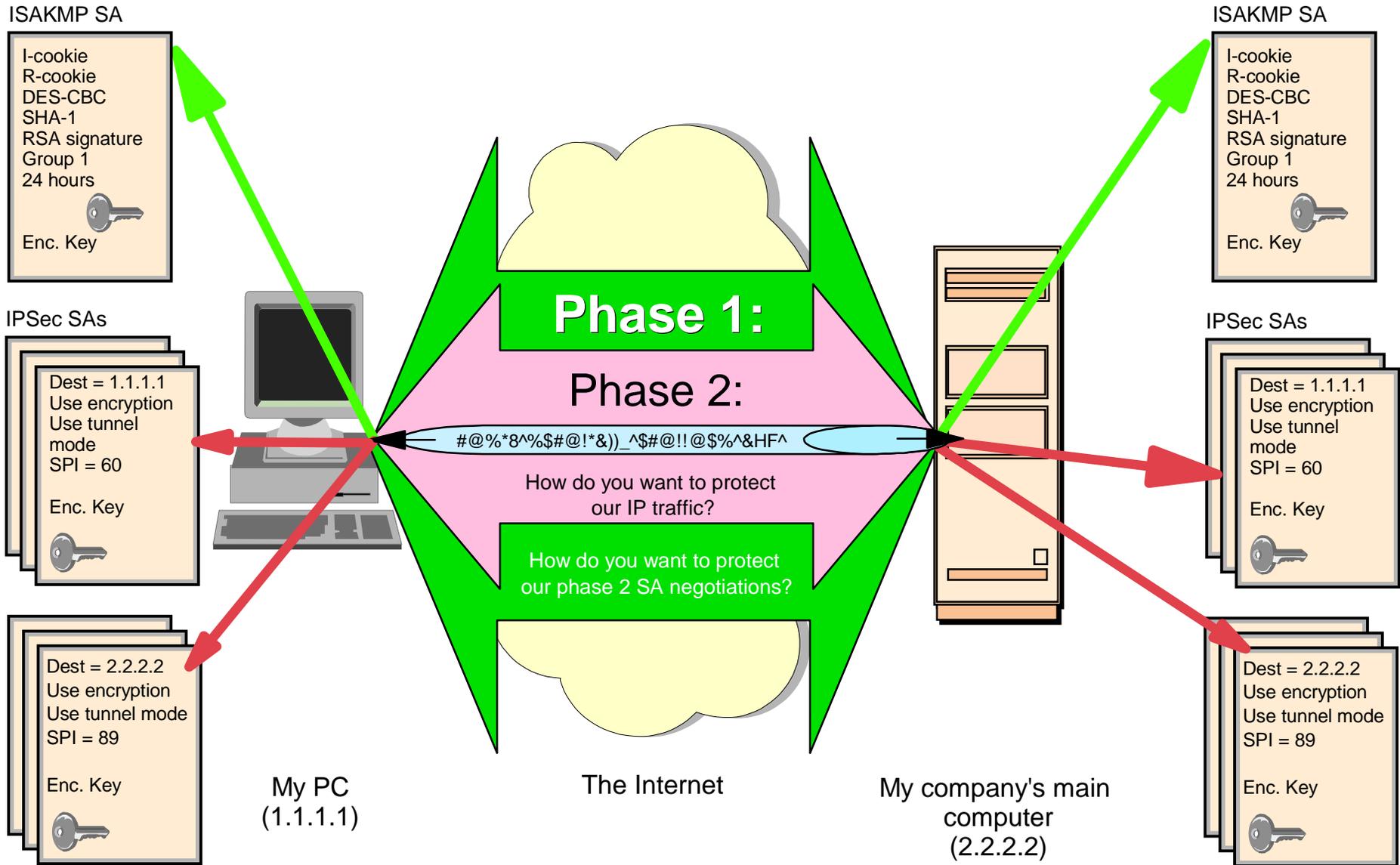
- Eliminates need to manually start SAs in advance for connections initiated outbound from S/390

- ▶ Allocate resources only when needed

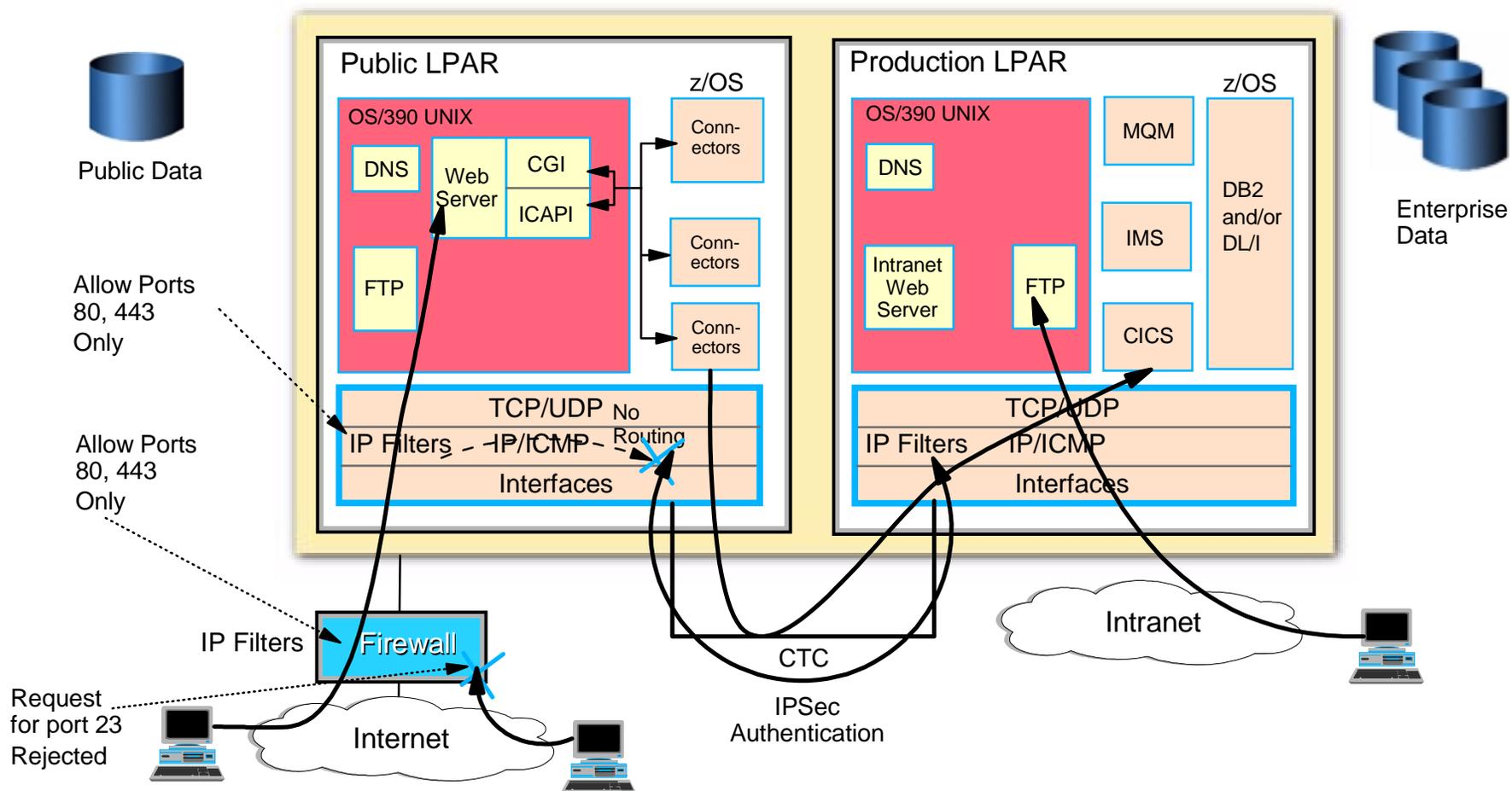
- Triggered when outbound data is sent, IPSec is required, and no SA exists

- ▶ Security Server configuration option provided to control use of function

Internet Key Exchange Protocol (OS/390 2.8)

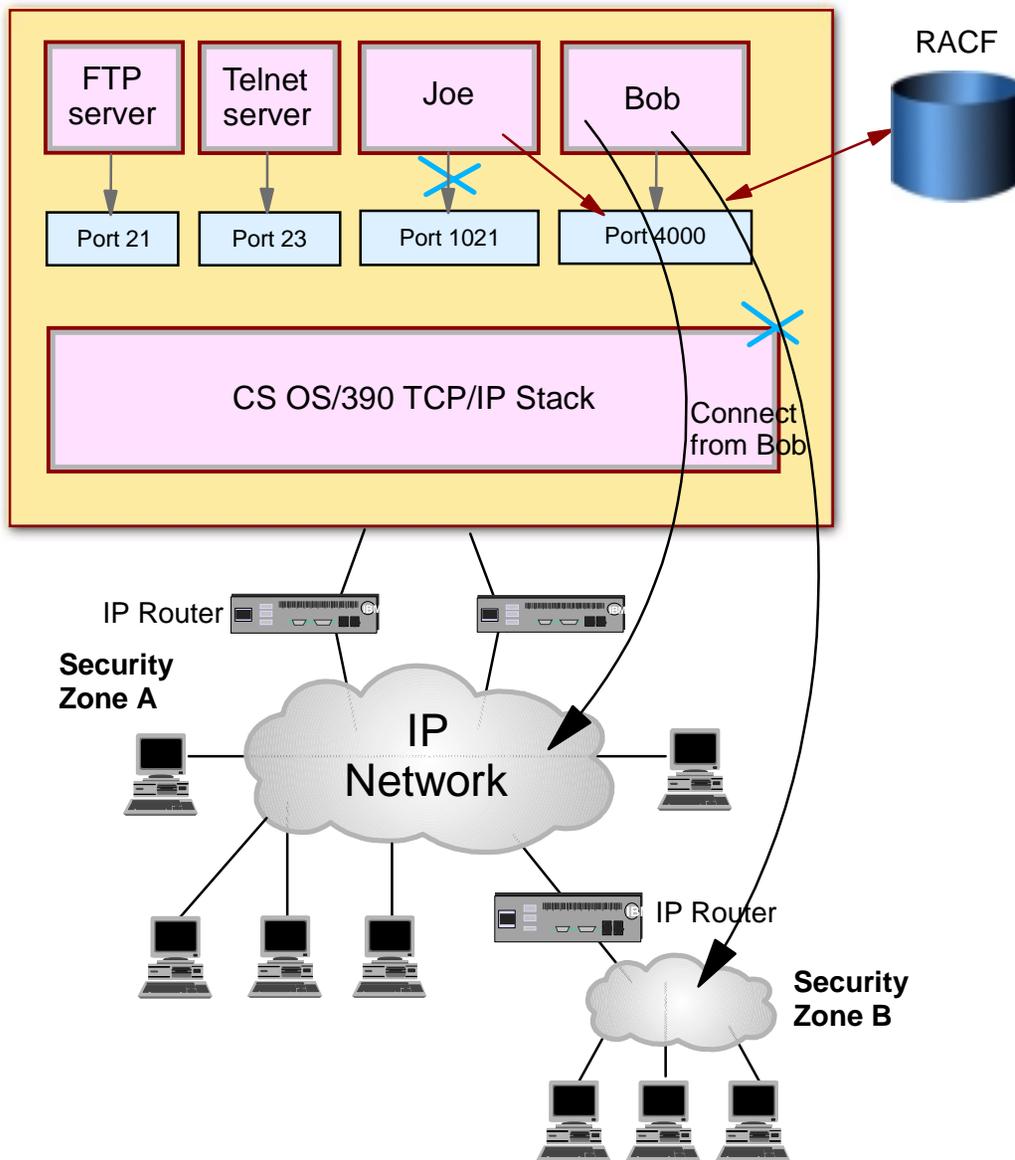


Typical OS/390 Configuration



- External Firewall can absorb cycles used to deflect unwanted incoming traffic
 - Based on destination port
 - Ex: Only allow Web / Deny all others
 - Insulate Public S/390 from Flooding Attacks
- Filtering used on Public S/390
 - Second line of defense

Enhanced User Access Control to TCP/IP Resources



1. Stack Access Control

- Controls user ability to open AF_INET 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

Limiting Inbound TCP Connection Requests

Prevention of overconsumption of system resources due to high volume of inbound connection requests

- **Intent not key**
 - Can be malicious user or unexpected peak in valid requests
- **Goal:**
 1. Keep system up
 2. Maximize ability to do useful work

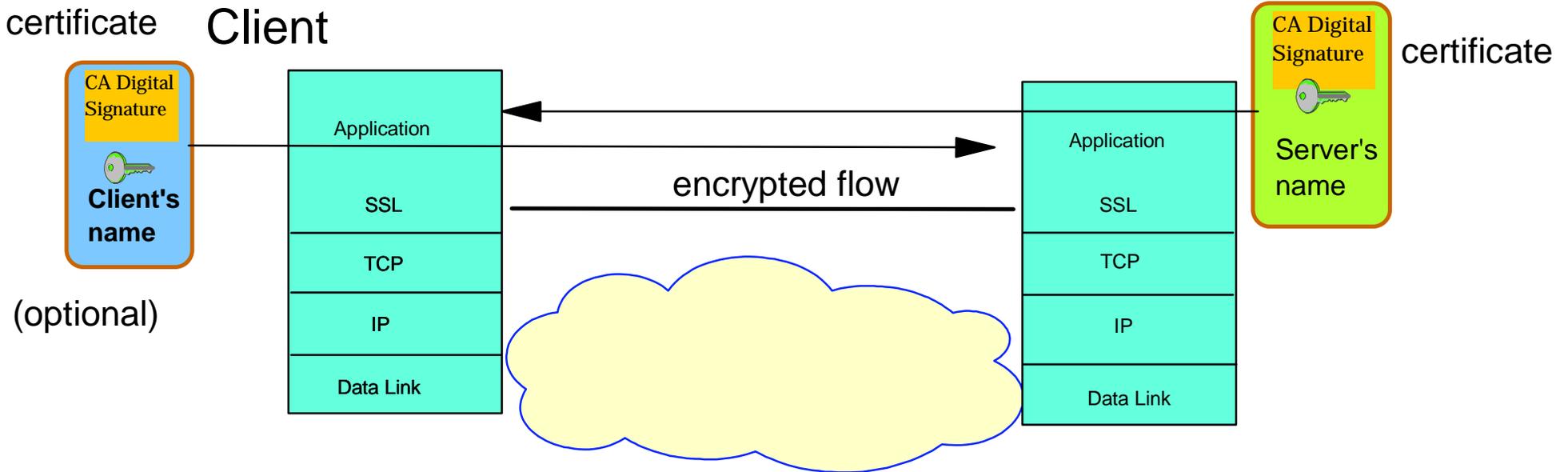
Differentiated Services (QoS) Policy (V2R7)

- **Provides control over number of inbound connections per QoS policy**
 - Specified as maximum number of connections for traffic that matches QoS policy filter

Traffic Regulation and Management Policy (V2R10)

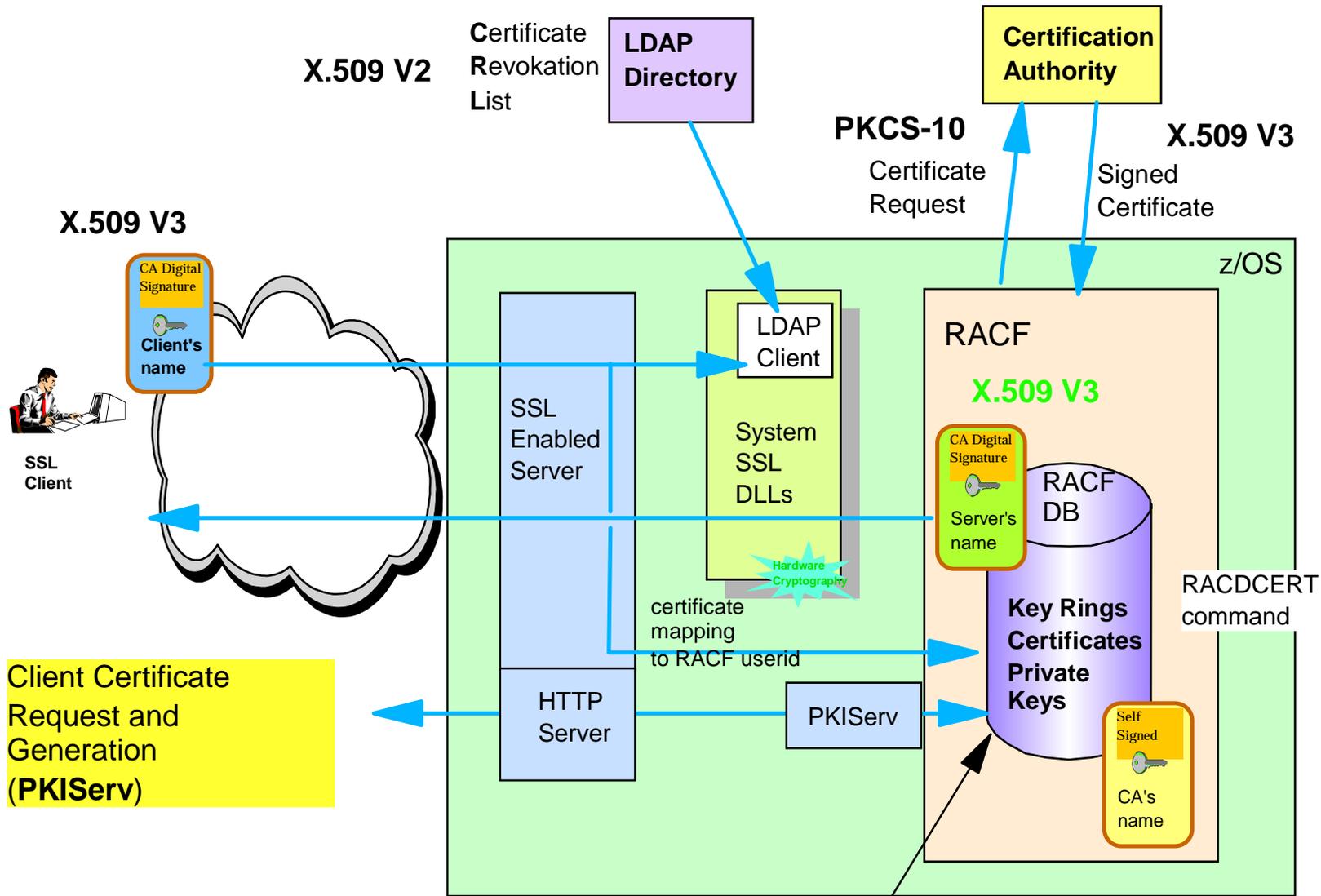
- **Provides control over number of inbound connections from a single host to a specified application port**
 - **Connection limit expressed as**
 - **Port Limit**
 - ✓ Total number for all connecting hosts
 - **Individual limit for a single host**
 - ✓ Connection within individual limit if single host connection total + new connection request \leq specified percentage of Available Connection Total
 - ✓ Available Connection Total = Total Connection Allowed - Total Connections Active

Secure Sockets Layer Overview



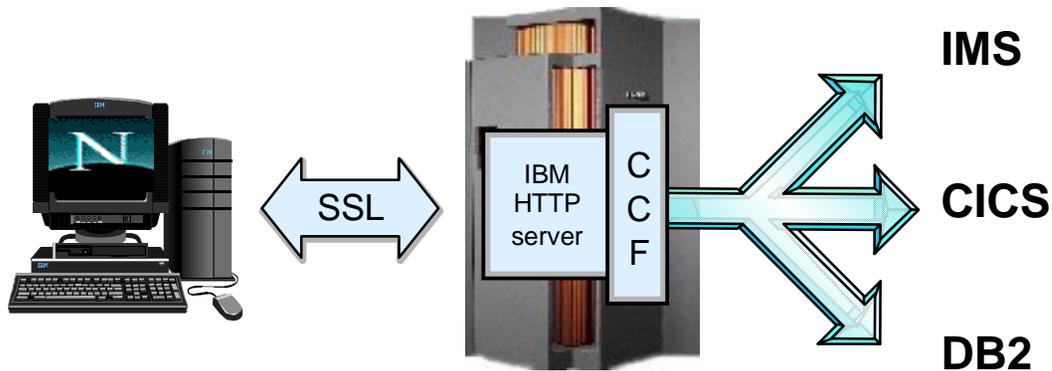
- Provides authentication, integrity, and data privacy above TCP layer.
 - Protocol includes key exchange using public key cryptography and negotiation of security parameters
- Applications must be changed to use SSL
- Applications that use SSL:
 - IBM HTTP Server, TN3270 Server, LDAP and CICS TS
- OS/390 provides a System SSL
 - Available to S/390 applications

SSL Support in z/OS 1.1



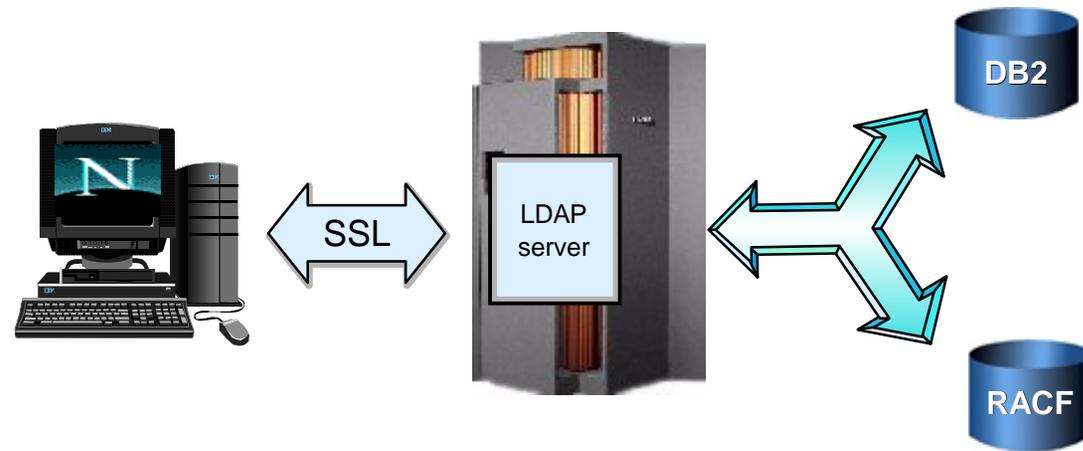
or in HFS file (initial implementation)

SSL enabled servers in z/OS 1.1



Browser(s) have built in support for SSL V2 and V3 invoked by HTTPS instead of HTTP

Encryption strength depends on encryption algorithm selected in SSL handshake between the browser and the server.



Secure access to directory services



Telnet client
(PCOMM or Host On Demand)
(optionally client authentication
PCOMM V5
and HOD V4)

TN3270 SSL Support for Internet Ready Access to SNA Applications

Secure TN3270 data exchange (V2R6)

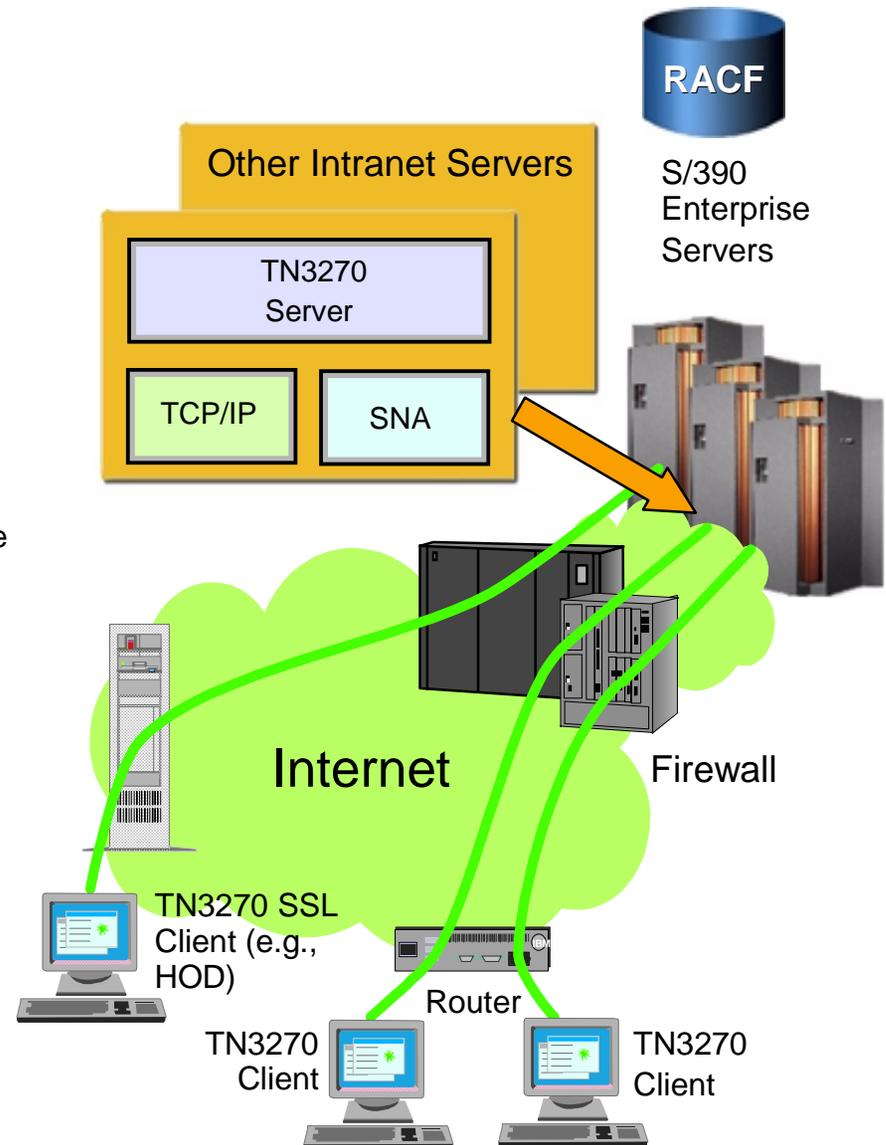
- SSL Server Side Authentication support using X.509 Certificates
- DES and Triple DES for data encryption
- Allows Multiple TN3270 Ports per Server
 - Basic Ports / SSL-Only
- Client Support
 - Host on Demand V2, PComm V4.3

Pre-Login Access Control using RACF digital certificate support (V2R8)

- Client credentials are validated before USSMSG (login 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

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 1.2

Communications Server Security Enhancements



Redbooks

International Technical Support Organization

Agenda

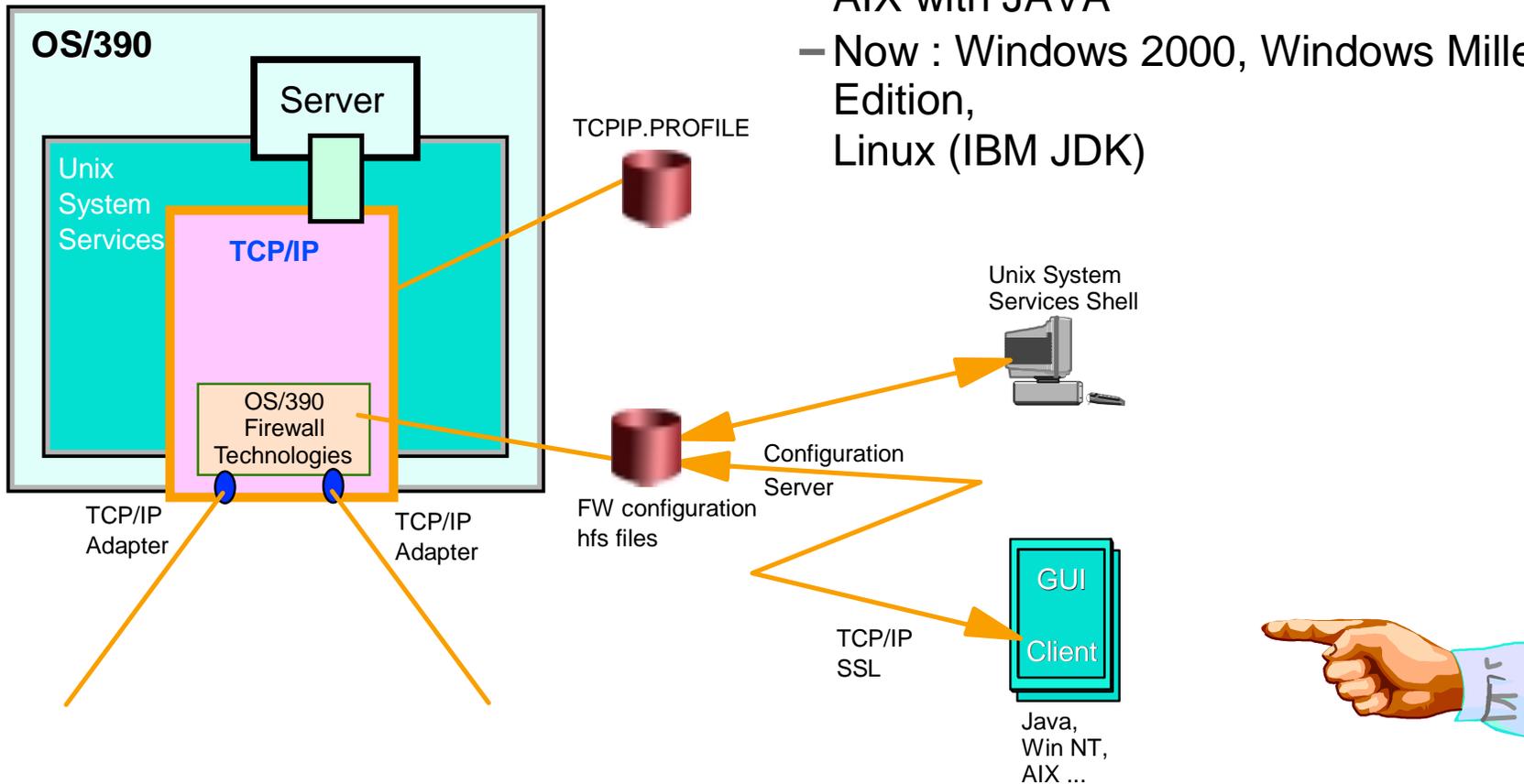
- **Firewall Technologies Enhancements**
- **Intrusion Detection System**
- **FTP Security Enhancements**
- **Unix Telnet, RSHD, Kerberos Support**
- **Express Logon Facility**
- **BIND DNS Upgrade**
- **IP Routing Authentication**

z/OS V1R2 Firewall Technologies - Overview

Line Item	Objective
GUI "Rewrite"	To maintain the serviceability of the GUI
Configuration Assistants	To reduce the initial learning curve required to configure IP filter rules, manual VPNs, and dynamic VPNs
Configuration Server Exploitation of Key Rings	To increase the security of the configuration server's private key
Commit Bit (ISAKMP Server)	To minimize "dropped packets" due to re-keying issues with the IKE protocol
VIPA Support (ISAKMP Server)	To facilitate the quicker usage of a Distributed VIPA by the ISAKMP server when it is moved from one stack to another
Always enable the ISAKMP and Configuration Servers	To maximize the number of potential exploiters of dynamic VPNs
Removal of DNS Configuration Support	To encourage the migration to the Communication Server's new DNS server
Migration	To facilitate the migration from previous releases to z/OS V1 R2

VPN Configuration GUI "Rewrite"

- Migrated from JAVA 1.1.8 runtime to JAVA 1.3
- Upgraded to the latest level of SSL light
- More consistent look with other IBM products
- Additional client platforms supported
 - Previously supported : Win 95/98/NT 4.0, AIX with JAVA
 - Now : Windows 2000, Windows Millennium Edition, Linux (IBM JDK)



Firewall Technologies Configuration Assistants

- Provide additional guidance for Firewalls Configuration
 - Created dialogs in the GUI that will guide one through the process of defining IP Filters, Manual VPNs, and Dynamic VPNs.
- Not intended to provide a shortened configuration process
 - Help the first time/occasional user by
 - Identifying configuration steps
 - Displaying text that describes each step
 - Help the experienced user by providing a fast path through the intermediate dialog panels
- Invoked by selecting the 'Configuration Assistant' folder on the GUI screen

Firewall Technologies Configuration Assistants

The screenshot displays the OS/390 Firewall Technologies Configuration Assistant for Dynamic VPN. The main window is titled "[dceimgud] Configuration Assistant: Dynamic VPN". The left pane shows a tree view of configuration options, with "AH Data Transform" selected under "Data Management Setup". The right pane, titled "Defining AH data transform templates", contains the following text:

The Authentication Header (AH) protocol can be used to provide:

- Authentication of the origin of an IPSec protected data packet
- Integrity of an IPSec protected data packet (i.e. ensure that it has not been modified)

The AH protocol cannot be used to provide privacy of the data contained with an IPSec protected data packet. The Encapsulating Security Payload (ESP) protocol must be used to obtain data privacy.

AH data transform templates are used to define a protection set that may be used when using the AH protocol to secure data being sent through a dynamic VPN tunnel. The information contained in this protection set consists of an encapsulation mode, an authentication algorithm, and a set of lifetime specifications. The lifetime specification indicates when a security association (SA) negotiated by the ISAKMP server should be expired. The ISAKMP server will automatically attempt to refresh SAs prior to the expiration of their lifetime.

AH data transform templates are referenced by data proposal templates. An AH data transform template can be referenced by multiple data proposals.

Click on 'Perform Add' if you need to configure an AH data transform template. You may repeat this step as frequently as desired to add multiple AH data transform templates.

Click on 'List Current' if you are unsure whether appropriate AH data transform templates have been previously configured.

The interface includes navigation buttons: "<<", "<", ">", ">>", "List Current", "Perform Add", and "Activate". At the bottom are "Close" and "Help ?" buttons.

Firewall Technologies

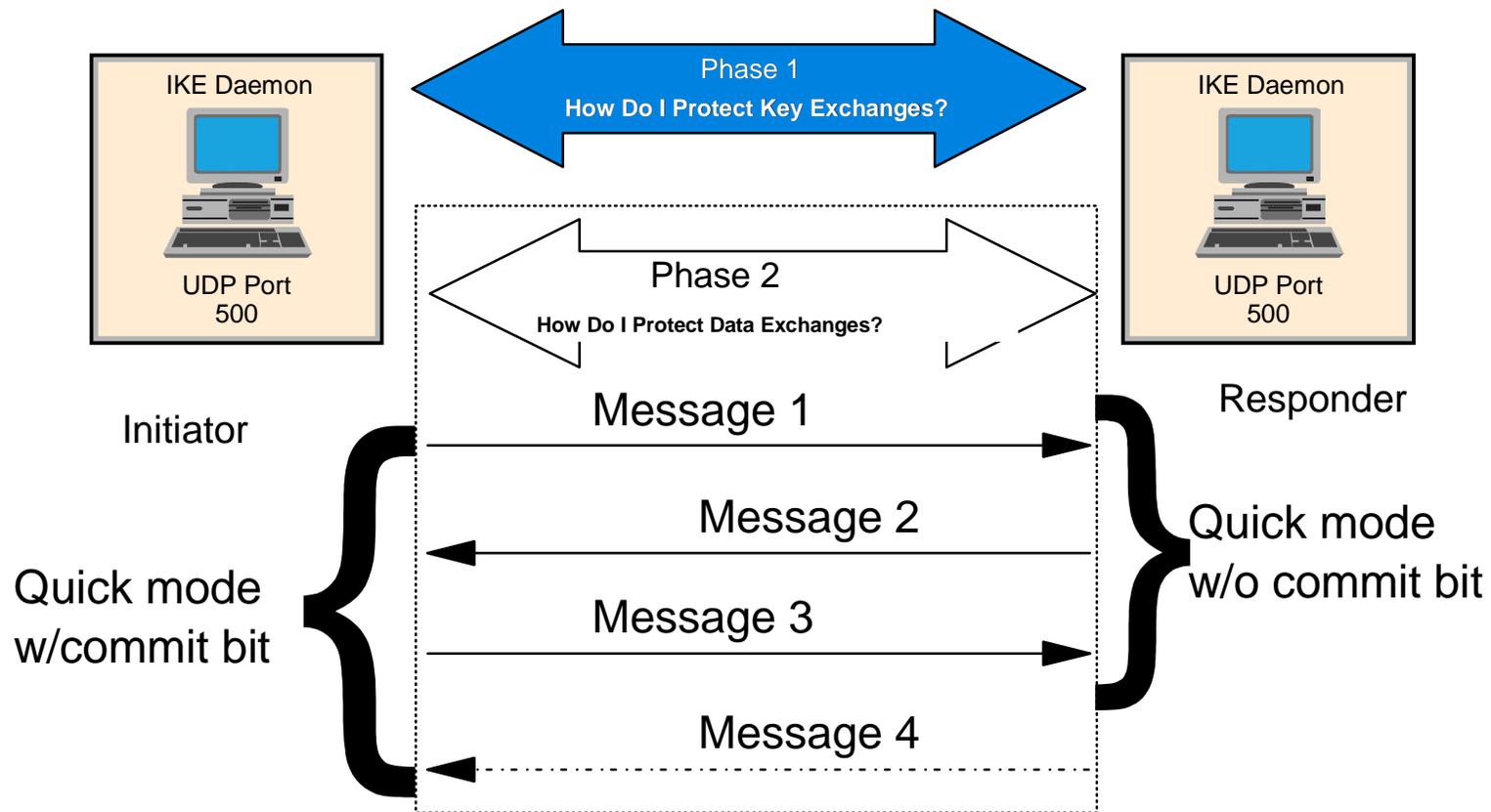
Configuration Server Exploitation of RACF Key rings

- The Configuration Server's certificate can now reside in a SAF (RACF) key ring instead of HFS
 - The IKE server and the Configuration Server can use the same SAF key ring, owned by FWKERN
 - a password stash file is no longer needed
 - Access to the private key is controlled using ESM security (e.g. RACF)
 - The private key could be stored in ICSF
- New options on the Configuration Server's daemonopt
 - k *keyring name*
 - l *Configuration Server certificate label*

```
fwdaemon cmd=change daemon=cfgsrv daemonopts="-k FirewallKeyRing -l cfgcert"
```

IPSec Commit Bit

- Reduces dropped packets that might occur during the re-keying of a dynamic VPN (IKE phase 2)
- increased interoperability



IPSec Commit Bit

- Commit bit logic implemented, based off of a post RFC 2409 draft of the Internet Key Exchange (IKE)
 - responder uses SA after message 3 is processed
 - initiator uses SA After Message 4 is processed or after Message 2 is processed and a packet using the SA is received from the peer
 - always set by the z/OS ISAKMP server when acting as a responder
- Enhanced the fwdynconns cmd=listactive command to:
 - Display all non-expired security associations
 - Display new commit bit related states
 - Pending
 - For use by inbound processing
 - For use by inbound and outbound processing

ISAKMP Server Dynamic VIPA Support

- Previous to z/OS 1.2, the ISAKMP server did not know of the deletion/addition of dynamic VIPA to the Firewall stack
 - local restart of the ISAKMP server is needed to take into account the change to DVIPA
- At z/OS .2 the running ISAKMP Server is informed when a dynamic VIPA is moved to a Firewall TCP/IP stack
 - The ISAKMP server will be able to immediately begin to listen on a UDP port 500 socket for the Dynamic VIPA
 - Dynamic VPN partners will be able to immediately negotiate security associations using the Dynamic VIPA

No more Security Server license for ISAKMP and Configuration Servers

- Non-Security Server customers can now:
 - Use the Configuration Server (and GUI) when configuring IP filtering, NAT, and VPNs
 - Use IPSec dynamic tunnels
- APAR OW47982 puts this line item back to OS/390 V2 R10

Miscellaneous ...

- Removal of Firewall DNS Configuration command
- fwmigrate command will add new predefined configuration objects to existing Firewall Configuration files
- Resources
 - SC24-5922 - z/OS SecureWay Security Server Firewall Technologies
 - z/OS Firewall Technologies web page
<http://www.ibm.com/servers/eserver/zseries/zos/firewall/>

z/OS 1.2 Intrusion Detection Services (IDS)



Redbooks

International Technical Support Organization

Intrusion Detection Services Interactions and Dependencies

- Host-based TCP/IP services under policy control, to identify, alert and document suspicious events and assist in later analysis.
 - Detect and record scanning, common attacks, and floods.
 - Recorded suspicious events to syslog, console, or packets trace.
 - Setup a policy to define preventative measures against attacks and flooding (i.e. queue limits and connection limits)
- Added to existing Security Plans and Procedures, Information and Application Access Controls, Firewalls and network-based IDS, for
 - detection of impending attacks
 - prevention of denial-of-service attacks
 - gathering of data for further legal actions

Intrusion Detection Functions

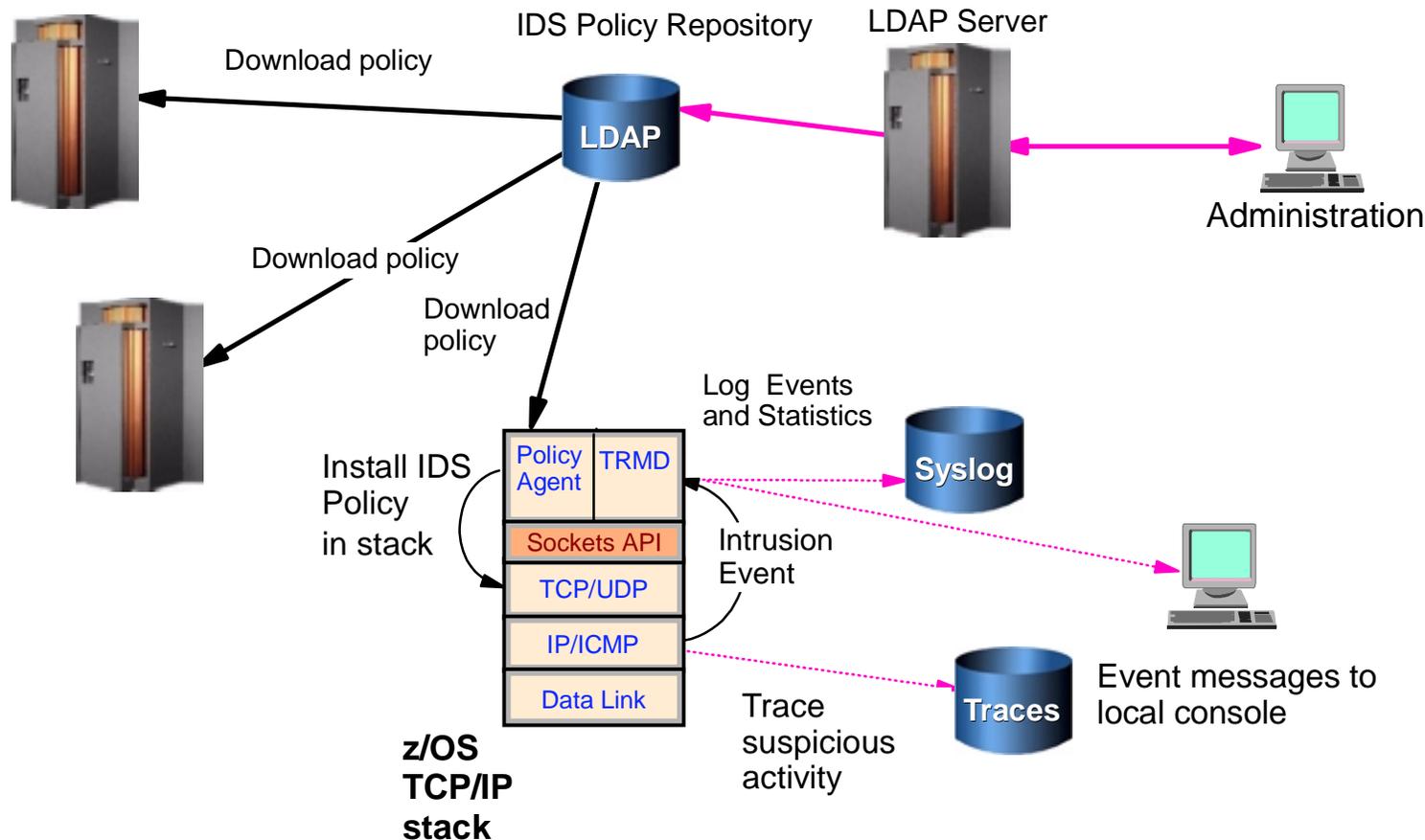
- **IDS events detected include:**

- Scan detection
 - 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
 - Malformed packet events
 - Outbound raw restrictions
 - Inbound fragment restrictions
 - IP option restrictions
 - ICMP restrictions
 - SYNflood events
 - UDP perpetual echo
- Traffic Regulation (Flood detection and prevention)
 - UDP backlog management by port
- Packets discard
 - TCP total connection and source percentage management by port (R10)
- Connection limiting

- **IDS Recording Options**

- Event logging
 - syslogd, local console
- Statistics
 - syslogd
 - normal, exception
- IDS packet trace after attack detected for offline analysis
 - Number of packets traced for multi-packet events are limited
- **Reports**
 - trmdstat produces reports from IDS syslogd records
 - Summary and detailed

Intrusion Detection Services

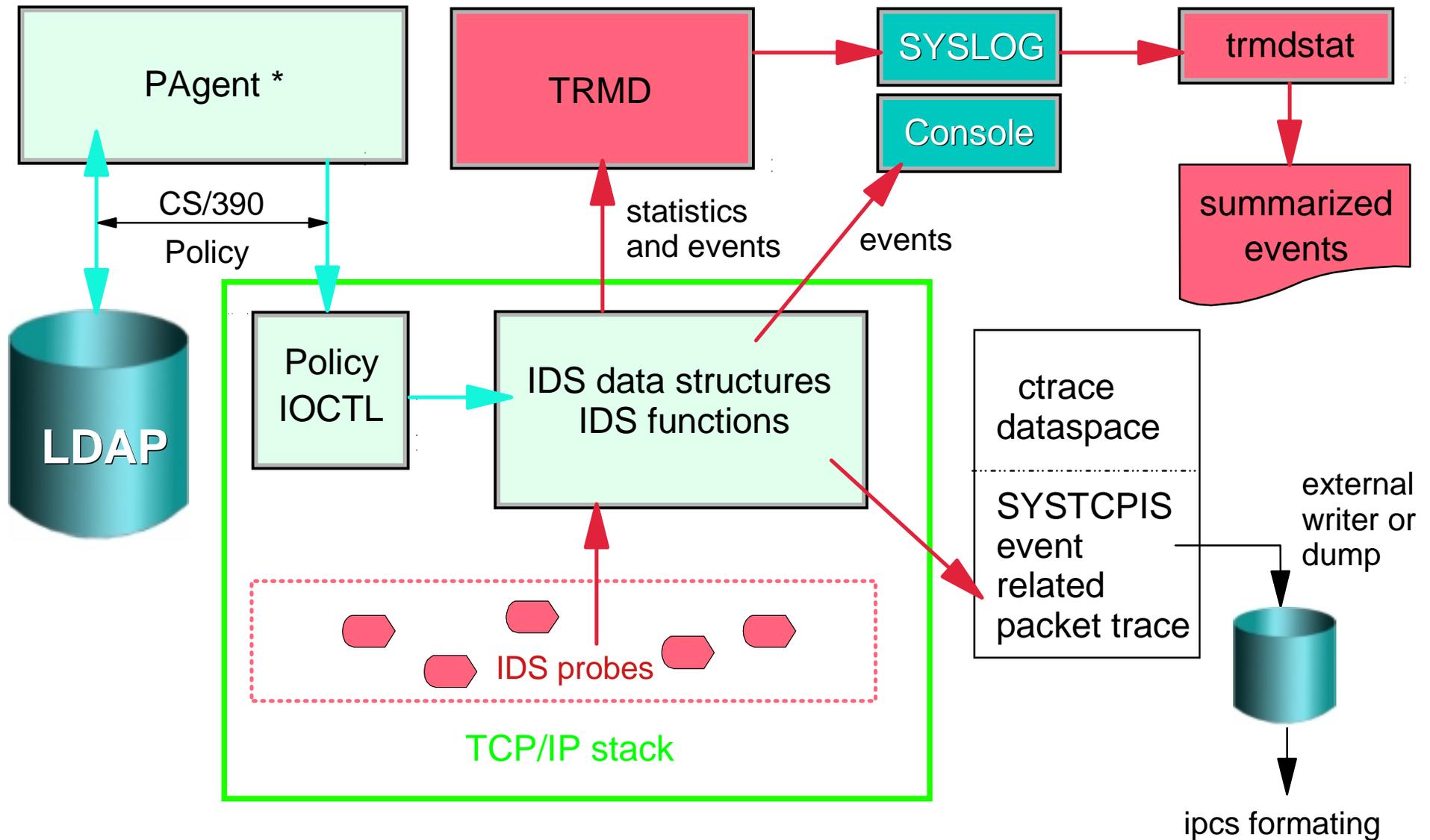


- **z/OS integrated IDS**

- Ability to evaluate inbound IPSec data
 - After decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks
 - IDS policy checked after attack detected
- Detects statistical anomalies real-time
 - Target system has stateful data / internal thresholds unavailable to external IDSs
- Policy can control prevention methods on the target
 - Connection limiting, packet discard

-

Intrusion Detection Services Overview



Intrusion Detection Services Invocation

- Activation of correct policies
 - check correct loading of policies into the LDAP directory (LDAP server logs)
 - Check the Policy Agent log file for errors while processing the policy
 - Use the psearch command to verify that the intended policies are active and have the expected attributes for the target stack
- Mapping of traffic to the correct policies
 - DISPLAY NETSTAT/onetstat IDS/-k SUMmary information for IDS policies mapping to attacks and scan
 - DISPLAY NETSTAT/onetstat IDS/-k PROTOcol TCP and IDS/-k PROTOcol UDP to check IDS policies mapping to the specified protocol
- Start TRMD as started task or from the OMVS shell
 - TRMD collects log record information issued by IDS Policies that include TypeAction:STATISTICS or TypeAction:LOG and Notification:SYSLOG
- The IDS report generator TRMDSTAT has to be run against the appropriate log files to produce reports on the area of interest.

Intrusion Detection Services Invocation

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

Intrusion Detection Services Invocation

IDS Packet Trace

- PARMLIB member
CTIIDS00
- Dump TCP/IP data space
TCPIPDS1
- CTRACE writer
- Format with IPCS
- Associate traced packets with events
PROBEID
CORRELATOR

Attack Policy Example

ibm-idsConditionType:ATTACK
ibm-idsAttackType:MALFORMED

Attack Type

ibm-idsTypeActions:EXCEPTSTATS
ibm-idsTypeActions:STATISTICS
ibm-idsStatInterval:n

To get statistics

ibm-idsTypeActions:LOG
ibm-idsNotification:CONSOLE
ibm-idsNotification:SYSLOG
ibm-idsLoggingLevel:n
ibm-idsMaxEventMessage:n

To get a message logged
whan an attack is detected

ibm-idsTraceData:HEADER
ibm-idsTraceData:RECORDSIZE
ibm-idsTraceRecordSize:xx
ibm-idsTraceData:FULL
ibm-idsTraceData:NONE

To request that a packet be
traced when an attack is
detected

ibm-idsTypeActions:LIMIT

To request that a packet be
discarded when it is detected as
an attack

Attack Detail Report Example

This report will be displayed when the -A and -D options are specified on the trmdstat command.
It will display the contents of attack event records.

```
trmdstat -A -D /tmp/tstlog.log
```

```
trmdstat for Z/OS CS V1R2          Wed Nov  8 09:55:36 2000
```

```
Log Time Interval      : Aug 21 08:32:09 - Aug 21 10:32:09
```

```
Stack Time Interval   : Aug 21 14:32:09 - Aug 21 14:32:09
```

```
TRM Records Scanned  : 71
```

```
Port Range           : ALL
```

ATTACK Events

Packets Discarded

Attack	Date and Time	Dst IpAddr	Src IpAddr	Dst Port	Src Port	Correlator	ProbeID
Malf	8/21/2000 14:32:9.53	51.52.53.54	41.42.43.44	0	0	82334	04010009
IPFr	8/21/2000 14:32:9.53	51.52.53.54	41.42.43.44	0	0	82336	04030001
IPOP	8/21/2000 14:32:9.53	51.52.53.54	41.42.43.44	0	0	82338	04050001
PRTO	8/21/2000 14:32:9.53	51.52.53.54	41.42.43.44	0	0	82339	04060001
Perp	8/21/2000 14:32:9.53	51.52.53.54	41.42.43.44	13001	10001	82342	04080001
ICMP	8/21/2000 14:32:9.53	51.52.53.54	41.42.43.44	12001	10001	82337	04040009

Packets would have been Discarded

Attack	Date and Time	Dst IpAddr	Src IpAddr	Dst Port	Src Port	Correlator	ProbeID
ORAW	8/21/2000 14:32:9.54	41.42.43.44	71.72.73.74	0	0	87999	04020001

TRMD Started : Aug 21 10:32:09

z/OS Intrusion Detection Services Resources

- z/OS Communications Server IP Configuration Guide
SC31-8775-01
- z/OS Communications Server IP Configuration Reference
SC31-8776-01
- z/OS Communications Server IP System Administrator 's
Commands - SC31-8781-00

z/OS 1.2 FTP Security Enhancements



Redbooks

International Technical Support Organization

FTP Security Enhancements

- Implement RFC 2577 to protect the FTP server against bounce attacks
- Use RACF surrogate support so that password is not required to be coded in FTP.DATA
- Check RACF authorization before returning contents of catalog
- Support TLS for FTP client and server
- Support Kerberos for FTP client and server
- Socksified FTP client

FTP Security Enhancements Invocation

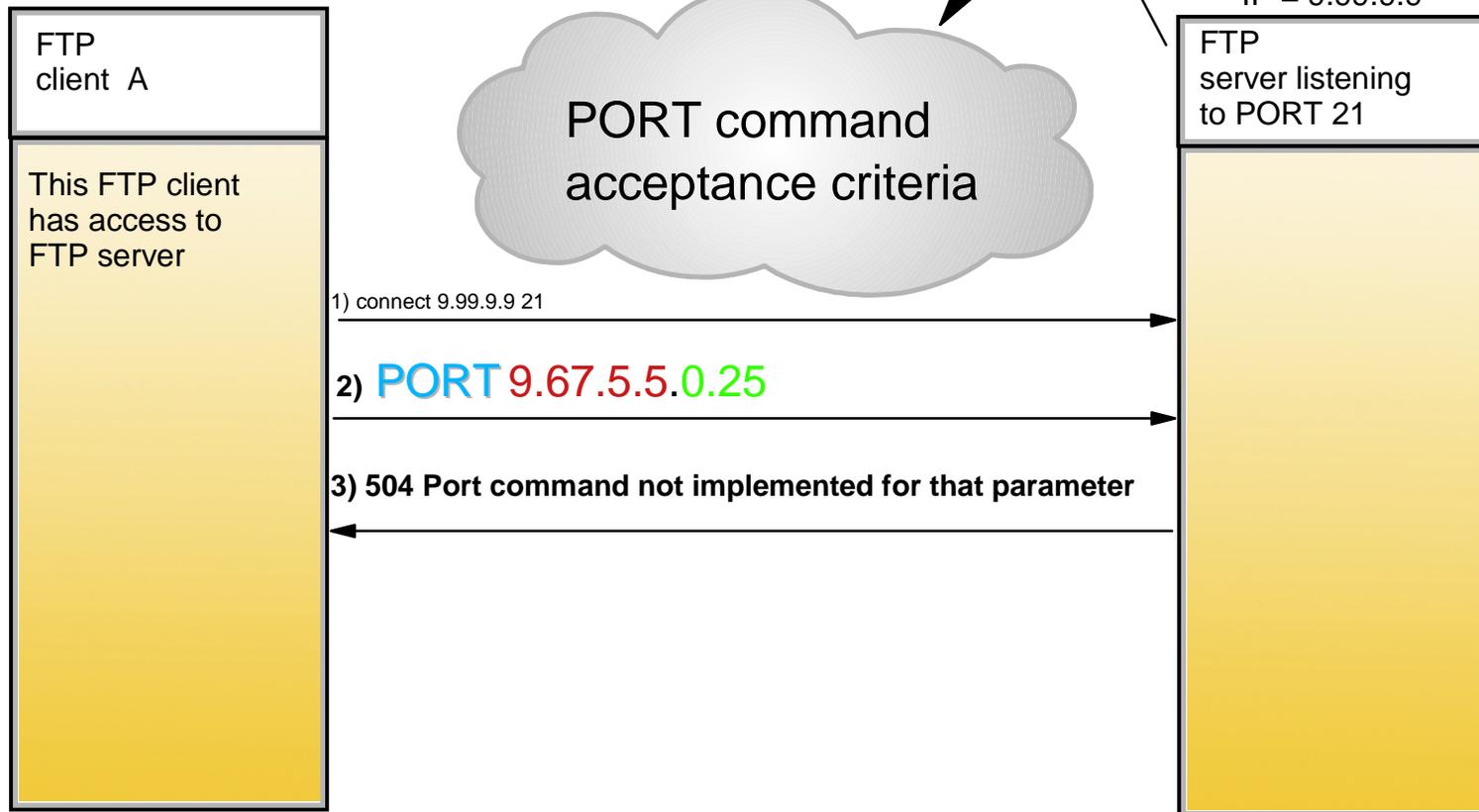
Protect Against Bounce Attacks

- Limit the use of the PORT command sent from clients to protect the server from being used in a bounce attack in FTP.DATA
 - ▶ PORTCOMMAND ACCEPT/REJECT
 - the FTP server accepts PORTCOMMAND or not
 - ▶ PORTCOMMANDIPADDR UNRESTRICTED/NOREDIRECT
 - accepts PORT command with IP address that is different from the IP address of the FTP client
 - ▶ PORTCOMMANDPORT UNRESTRICTED/NOLOWPORTS
 - accepts PORT command with a PORT number that is less than 1024.

FTP Security Enhancements Invocation

Protect Against Bounce Attacks

- 1) ftp server X port 21
- 2) PORT 25
- 3) STOR A



FTP Security Enhancements Invocation

Surrogate RACF Support

- In FTP.DATA
ANONYMOUS=*user_id/password* in FTP.DATA

can be replaced by

ANONYMOUS=*user_id/SURROGATE* in FTP.DATA

If a RACF surrogate profile has been defined for *user_id* and the FTP server is permitted to the profile

```
SETROPTS CLASSACT(SURROGAT)
RDEFINE SURROGAT BPX.SRV.user_id UACC(NONE)
PERMIT BPX.SRV.user_id CLASS (SURROGAT) ID(FTPD) ACCESS(READ)
```

- ANONYMOUSLEVEL must be ≥ 3

FTP Security Enhancements Invocation

Restrict DIR Output

- Prevent users that are not authorized from seeing the contents of a catalog
 - ✓ Assuming that user access is restricted to a group which does not have access to EXAMPLE.*

Prior to z/OS 1.2

```
DIR 'EXAMPLE.*'  
EZA2284I Volume Unit      Referred Ext  ... BlkSz Dsorg Dsname  
EZA2284I CPDLB0 3390    2000/10/05  1  ...   256  PS 'EXAMPLE.RESTART.TMP4.SHOE.BANNER'  
EZA2284I CPDLB1 3390    2001/02/07  1  ...    80  PS 'EXAMPLE.RESTART.TMP5.BANNER'  
EZA2284I CPDLB1 3390    2001/02/07  1  ...    80  PS 'EXAMPLE.TMP.BANNER'  
EZA2284I CPDLB3 3390    2001/02/07  1  ...  6233  PS 'EXAMPLE.TMP2.BANNER'  
EZA2284I CPDLB3 3390    2001/02/07  1  ...  6233  PS 'EXAMPLE.TMP2.BANNER'  
EZA2284I CPDLB3 3390    2001/02/07  1  ...  6233  PS 'EXAMPLE.TMP3.BANNER'
```

At z/OS 1.2

```
DIR 'EXAMPLE.*'  
550 No data sets found.
```

FTP Security Enhancements Invocation

TLS for FTP

- Protect FTP traffic using authentication and/or encryption
- Note: Proxy open is not supported with security mechanisms
- New FTP commands
 - ▶ AUTH Authentication/Security Mechanism
 TLS, TLS-C, TLS-P, SSL, GSSAPI (Kerberos)
 - ▶ PBSZ maximum size of encoded data block
 - ▶ PROT Data Connection Protection Level
 CLEAR/PRIVATE
- The Control Connection is always protected (private)

FTP Security Enhancements Invocation

TLS for FTP

For the server, in FTP.DATA

EXTENSIONS AUTH_TLS

used to specify that the TLS authentication is supported

SECURE_FTP REQUIRED|ALLOWED

to specify whether authentication is required

SECURE_LOGIN VERIFY_USER|REQUIRED|OPTIONAL

to specify client authentication using client certificate

SECURE_PASSWORD REQUIRED|OPTIONAL

to specify password prompt

SECURE_DATACONN NEVER|CLEAR|PRIVATE

to specify protection of the data connection

KEYRING *keyring*

HFS key database or RACF keyring

CIPHERSUITE *name*

list of supported TLS CipherSuite

TLSTIMEOUT *seconds*

maximum time allowed for TLS negotiation

FTP Security Enhancements Invocation

TLS for FTP

For the client in FTP.DATA

SECURE_MECHANISM TLS|TLS-P

to specify use of TLS and protection of data connection

SECURE_FTP REQUIRED|ALLOWED

to specify requirement for authentication

SECURE_DATACONN NEVER|CLEAR|PRIVATE

to specify protection of the data connection

KEYRING *keyring*

HFS key database or RACF keyring

CIPHERSUITE name

list of supported TLS CipherSuite

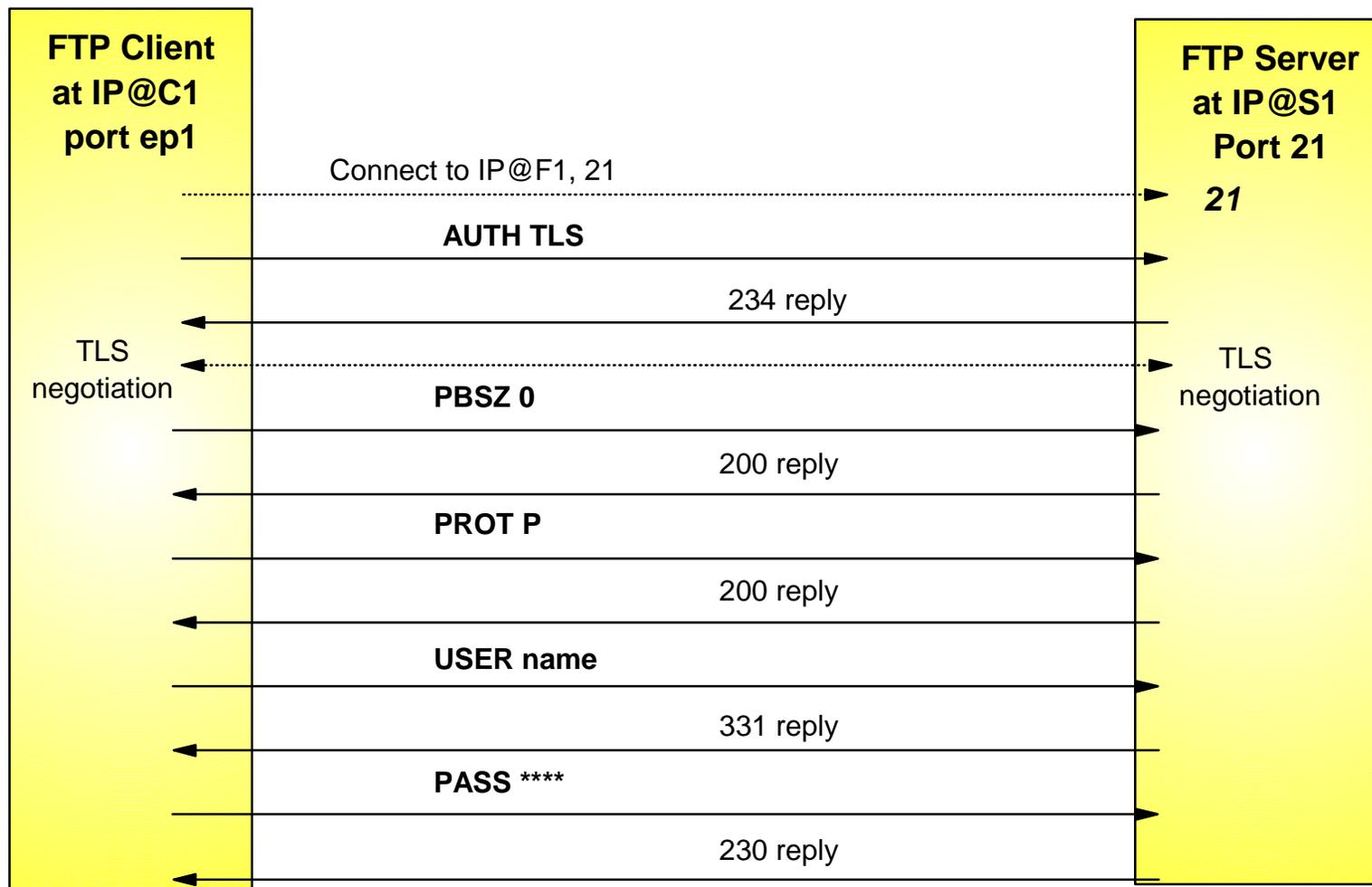
TLSTIMEOUT seconds

maximum time allowed for TLS negotiation

FTP Security Enhancements Invocation

TLS for FTP

Establish a protected session using port 21



FTP Security Enhancements Invocation

Kerberos Support

For the server, in FTP.DATA

EXTENSIONS AUTH_GSSAPI

used to specify that the Kerberos authentication is supported

SECURE_FTP REQUIRED|ALLOWED

to specify whether authentication is required

SECURE_LOGIN VERIFY_USER|REQUIRED|OPTIONAL

to specify client authentication using Kerberos principal name

SECURE_PASSWORD REQUIRED|OPTIONAL

to specify password prompt

SECURE_CTRLCONN CLEAR|SAFE|PRIVATE

to specify integrity and privacy protection of the command channel

SECURE_DATACONN NEVER|CLEAR|PRIVATE

to specify protection of the data connection

SECURE_PBSZ *size*

maximum size of encoded data block

FTP Security Enhancements Invocation

Kerberos Support

For the client, in FTP.DATA

EXTENSIONS AUTH_GSSAPI

used to specify that the Kerberos authentication is supported

SECURE_FTP REQUIRED|ALLOWED

to specify whether authentication is required

SECURE_CTRLCONN CLEAR|SAFE|PRIVATE

to specify integrity and privacy protection of the command channel

SECURE_DATACONN NEVER|CLEAR|PRIVATE

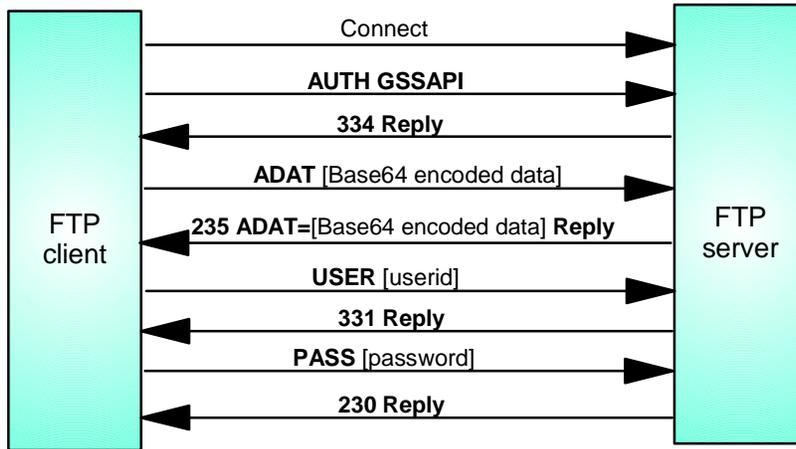
to specify protection of the data connection

SECURE_PBSZ *size*

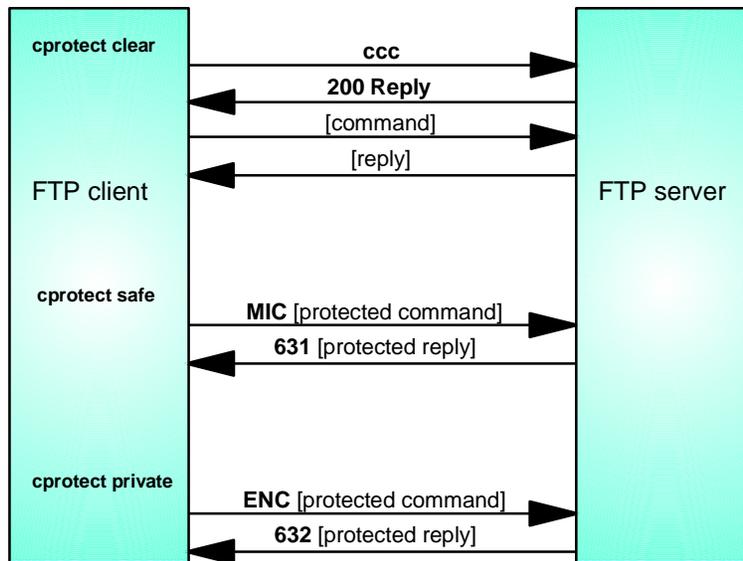
maximum size of encoded data block

FTP Security Enhancements Invocation

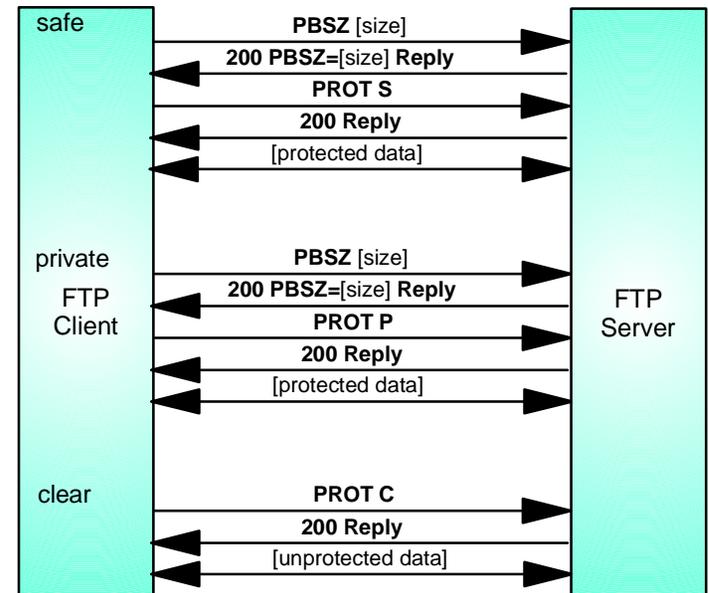
Kerberos Support



Control connection protection



Data connection protection



FTP Usability Enhancements Invocation

Socksify FTP Client

- SOCKSCONFIGFILE statement in the client's FTP.DATA
 - ▶ SOCKSCONFIGFILE can be HFS or MVS.
 - ▶ No default value is used for SOCKSCONFIGFILE if the statement is absent or invalid.
 - ▶ The locstat subcommand can be used to identify the SOCKSCONFIGFILE in use
- Sample SOCKSCONFIGFILE configuration

```
; This is my socks configuration
```

```
;
```

```
direct 9.0.0.0 255.0.0.0 ; Internal net
```

```
direct 127.0.0.1 255.255.255.255 ; Loopback
```

```
sockd4 @=9.1.2.3 192.168.1.0 255.255.255.0 ; Test net
```

```
sockd5 @=9.1.2.4 0.0.0.0 0.0.0.0 ; Anything else
```

FTP Security Enhancements Resources

- z/OS Communications Server IP Configuration Guide
SC31-8775-01
- z/OS Communications Server IP Configuration Reference
SC31-8776-01
- z/OS Communications Server IP System Administrator 's
Commands - SC31-8781-00
- FTP Security Extensions RFC 2228
- The TLS Protocol RFC 2246
- RFC 1510 describes Kerberos Version 5
- RFC 1964 describes GSS-API

z/OS 1.2 Telnet/RSHD Kerberos Support



Redbooks

International Technical Support Organization

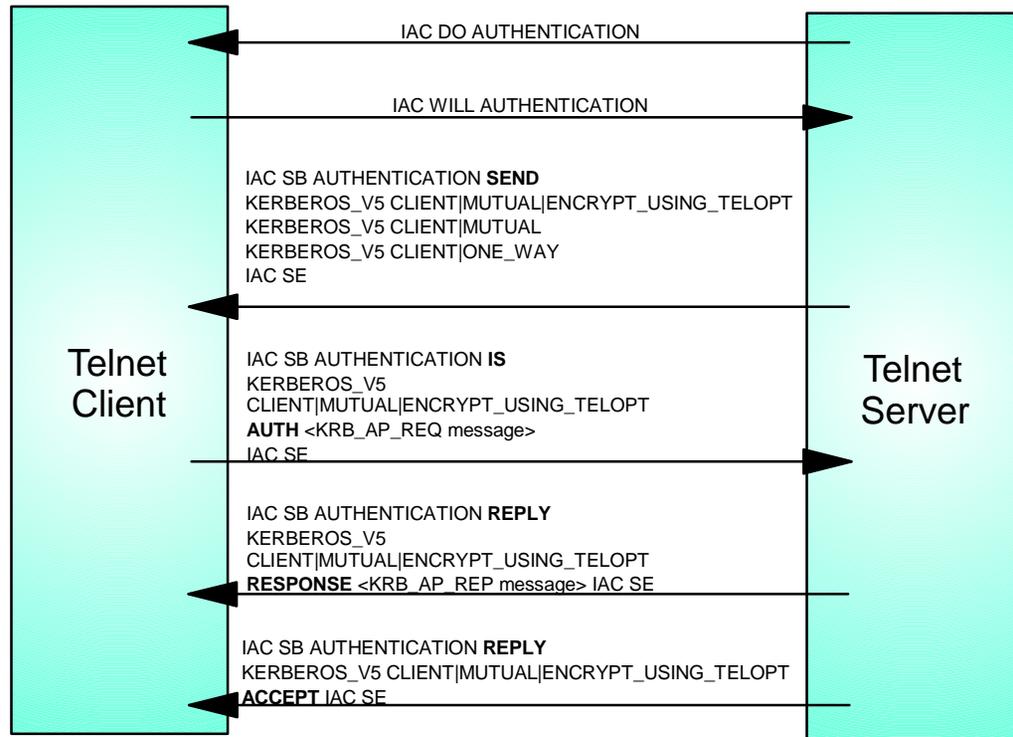
Unix TelnetD/RSHD Kerberos Support Overview

- To logon to the Unix telnet daemon or the rsh daemon using the kerberos authentication mechanism

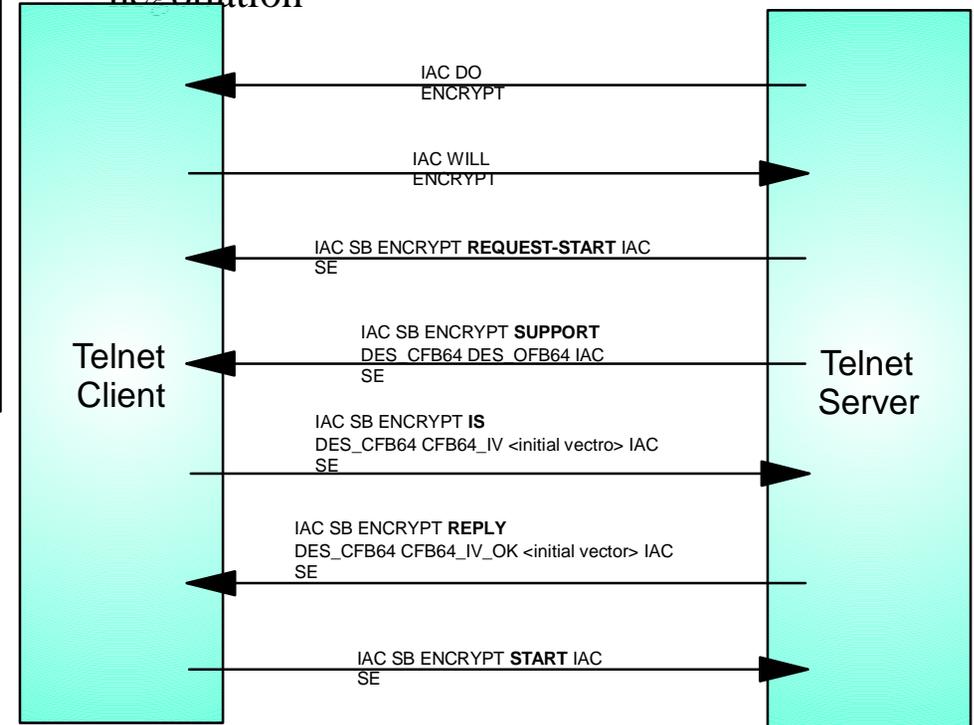
- New parameters for the otelnetd server
 - ▶ -a [authentication-level]
none, valid, other, user, or off
 - ▶ D [debug-type]
authentication or encryption
 - ▶ -s
to indicate that RACF Kerberos KDC is to be used
 - ▶ -X [authentication-mechanism]
KERBEROS_V5

Unix TelnetD/RSHD Kerberos Support Overview

Example Telnet Authentication option negotiation



Example Telnet Encryption option negotiation



Unix TelnetD/RSHD Kerberos Support Overview

New command line parameters for the orshd server:

-k [authentication-mechanism]

KRB5 or GSSAPI

-e encryption must be used on the connection with the client

-t indicates that the RACF Kerberos KDC must be used

-m Kerberos clients must present checksum of initial connection information

-i ignore Kerberos clients authenticator checksums

Unix TelnetD/RSHD Kerberos Support Resources

- z/OS Communications Server IP Configuration Guide
SC31-8775-01
- z/OS Communications Server IP Configuration Reference
SC31-8776-01
- z/OS Communications Server IP System Administrator 's
Commands - SC31-8781-00
- Telnet Kerberos RFCs
 - RFC 2941 Telnet Authentication Option
 - RFC 2942 Telnet Authentication: Kerberos Version 5
 - RFC 2946 Telnet Data Encryption Option
 - RFC 2952 Telnet Encryption: DES 64 bit Cipher Feedback
 - RFC 2953 Telnet Encryption: DES 64 bit Output Feedback

z/OS 1.2 TN3270E Express Logon Facility

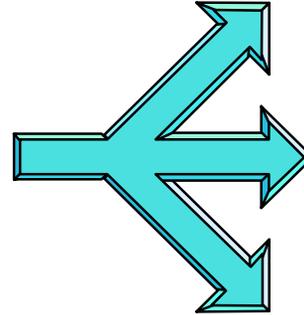
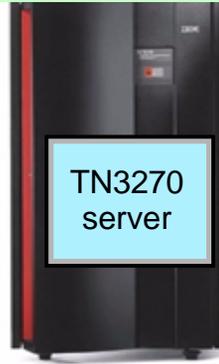


Redbooks

International Technical Support Organization

Express Logon - Extend Client Certificate to SNA Logon

SSL support parameters
in TCPIP.PROFILE



IMS

CICS

TSO

Optional SSL V3 Client authentication to the secure port (OS/390 2.8)

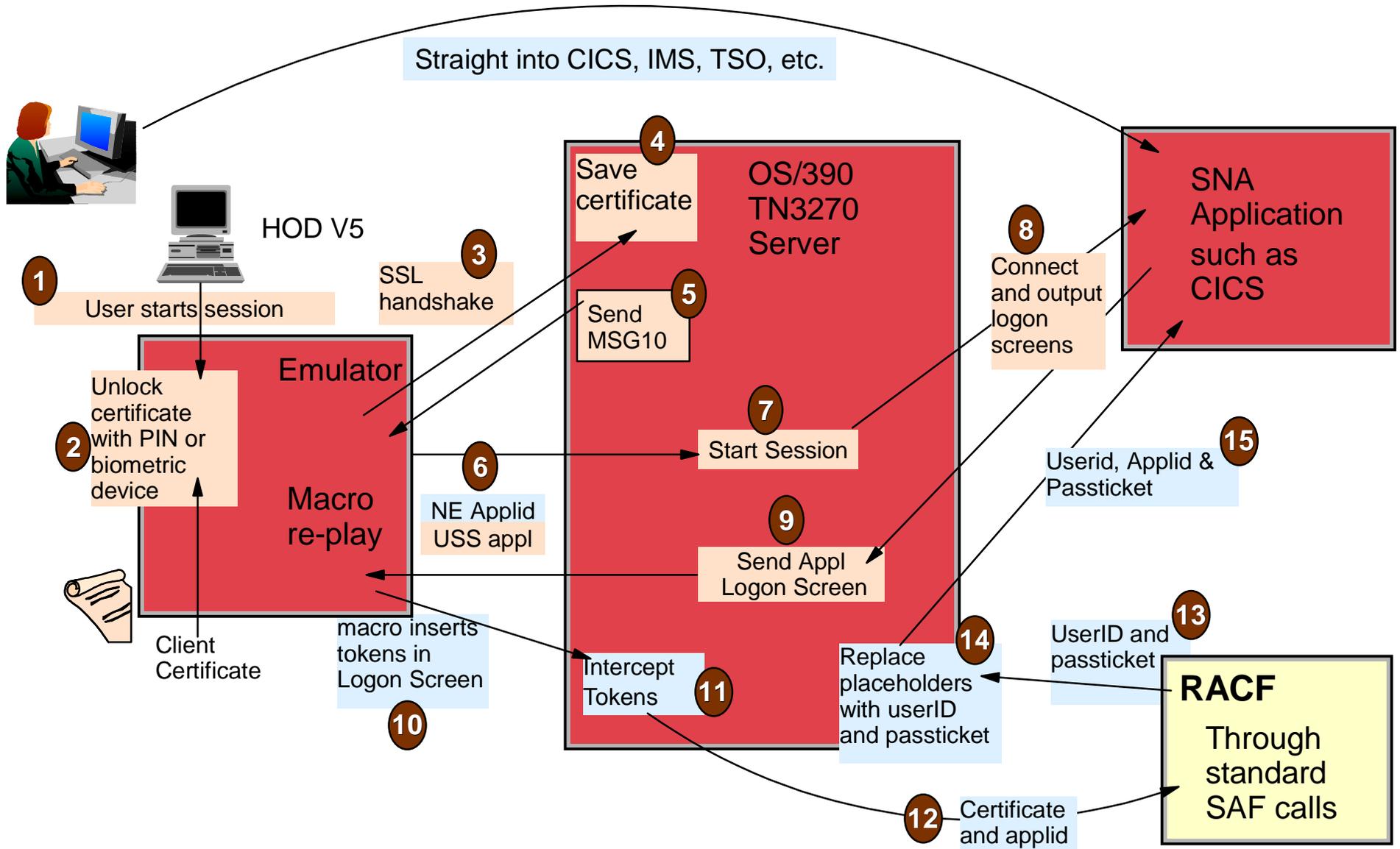
Optional SSL V3 Client authentication to the backend application (Express Logon Facility with HOD V5, OS/390 2.10, z/OS 1.2)

Telnet client
(PCOMM or Host On Demand)
(optionally client authentication PCOMM V5 and HOD V4)

Express Logon - Extend Client Certificate to SNA Logon

- Allow TN3270E clients using SSL to logon without having to enter a userid and password
- Function externals
 - ▶ ExpressLogon/NoExpressLogon, in TelnetGlobals, TelnetParms, ParmsGroup
 - ▶ Client Capable of New Environment Negotiation & Scripted Macros
 - Host On Demand V5
 - ▶ RESTRICTAPPL *application* CERTAUTH USER=*user_id*
- Prerequisites for installation
 - ▶ Macro must be configured on client to
 - send an application name under the New Environment Telnet Option
 - enter the tokens \$usr.id\$ and \$pass.wd\$ in the logon screen
 - ▶ PTKTDATA profiles in place for backend application

Express Logon - Extend Client Certificate to SNA Logon



Express Logon Facility Resources

- z/OS Communications Server IP Configuration Guide
SC31-8775-01
- z/OS Communications Server IP Configuration Reference
SC31-8776-01
- z/OS Communications Server IP System Administrator 's
Commands - SC31-8781-00
- Telnet New Environment Option - RCF 1572

z/OS 1.2 SNMP Enhancements



Redbooks

International Technical Support Organization

SNMP Security Enhancement

- SNMPv3 already supported data integrity, authentication and confidentiality
- At z/OS 1.2 : provides RACF authorization to control which SNMP subagents userIDs can connect to the SNMP agent using TCP
 - subagents userIDs must be permitted to the RACF profile in the SERVAUTH class
 - **EZB.SNMPAGENT.sysname.tcprocname**
- One profile per TCP/IP stack per z/OS image
 - remote subagents cannot connect to the SNMP agent from other z/OS images
 - subagents cannot connect to agents associated with another TCP/IP stack

z/OS 1.2 BIND DNS Upgrade



Redbooks

International Technical Support Organization

BIND DNS Upgrade Highlights

- Add BIND 9-base DNS to z/OS
 - future replacement for current BIND 4.9.3 DNS
 - up-to-date industry standard
 - provides enhanced security functions
 - includes support for IPV6 addresses
 - improved scalability on S/390-zSeries
- For the time being, does not support
 - DNS/WLM load balancing
 - DDNS functions of prior Communications Server releases
- BIND 4.9.3 DNS still provided

BIND DNS Upgrade Highlights

- BIND 9 Security
 - Support for DNSSEC
Cryptographic authentication of DNS information ('signed zones')
 - Support for TSIG (Transaction SIGNature)
BIND Server to BIND server communications have authentication and integrity check via shared secret key
 - Access Control Lists
who can query the server, receive zone transfers, dynamically update the zone
 - Enhanced auditability
 - split DNS (firewall DNS) support
- Unix System Services tools
 - dnssec-keygen (for v9 DNSSEC and TSIG)
 - dnssec-makekeyset (for DNSSEC)
 - dnssec-signkey (for DNSSEC)
 - dnssec-signzone (for DNSSEC)

BIND DNS Upgrade Highlights

Main elements of named.conf

acl	defines a named IP address matching list, for access control and other uses.
controls	declares control channels to be used by the 'rndc' utility.
include	includes a file.
key	specifies key information for use in authentication and authorization using TSIG.
logging	specifies what the server logs, and where the log messages are sent.
options	controls global server configuration options and sets defaults for other statements.
server	sets certain configuration options on a per-server basis.
trusted-keys	defines trusted DNSSEC keys.
view	defines a view. A subset of data visible to specific clients/servers
zone	defines a zone. data for a domain

BIND DNS Security Resources

- z/OS Communications Server IP Configuration Guide
SC31-8775-01
- z/OS Communications Server IP Configuration Reference
SC31-8776-01
- z/OS Communications Server IP System Administrator 's
Commands - SC31-8781-00
- DNS Security RCF 2535

z/OS 1.2 IP Routing Authentication



Redbooks

International Technical Support Organization

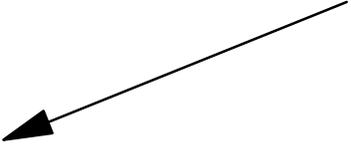
IP Routing Enhancements - MD5 Authentication

- Support MD5 authentication for OSPF packets (Cisco compatible)
- Two new keywords for OSPF_INTERFACE and VIRTUAL_LINK
 - Authentication_Type values: none, password, or MD5
 - Authentication_Key_ID : an integer from 0-255
- One keyword enhanced:
 - Authentication_key : can now specify a hexadecimal MD5 key

```
OSPF_INTERFACE
  ip_address = 9.67.101.3
  subnet_mask = 255.255.255.0
  authentication_type = MD5
  authentication_key_id = 124
  authentication_key = 0x1234567890ABCDEF0123456789ABCDEF
  .....i
```

```
Virtual_Link
  Virtual_Endpoint_RouterID=7.7.7.7
  Links_Transit_Area=1.1.1.1
  authentication_type=MD5
  AUTHENTICATION_KEY_ID=4
  authentication_key=0xfedcba9876543210fedcba0987654321;
```

MD5 key shared by
all routers
attached to the
subnet



IP Routing Enhancements - MD5 Authentication

- The PWTOKEY is provided for SNMP as a utility to generate MD5 keys from text passwords and SNMP parameters
- PWTOKEY simplified version for use with OMPROUTE
 - can generate a key with only a password input
 - There is no "official" method for generating MD5 keys -- this utility is provided as a convenience, users can use any methods they like to generate the 16-byte keys