
# OS/390 Network Security Configurations

Paul de Graaff
IBM Field Technical Sales Specialist
E-mail: graaff@us.ibm.com

March 1 2001 - Session Number 1775
The Westin Hotel

# Abstract


This session shows some of the security challenges, we face when we move to deploy e-business solutions.

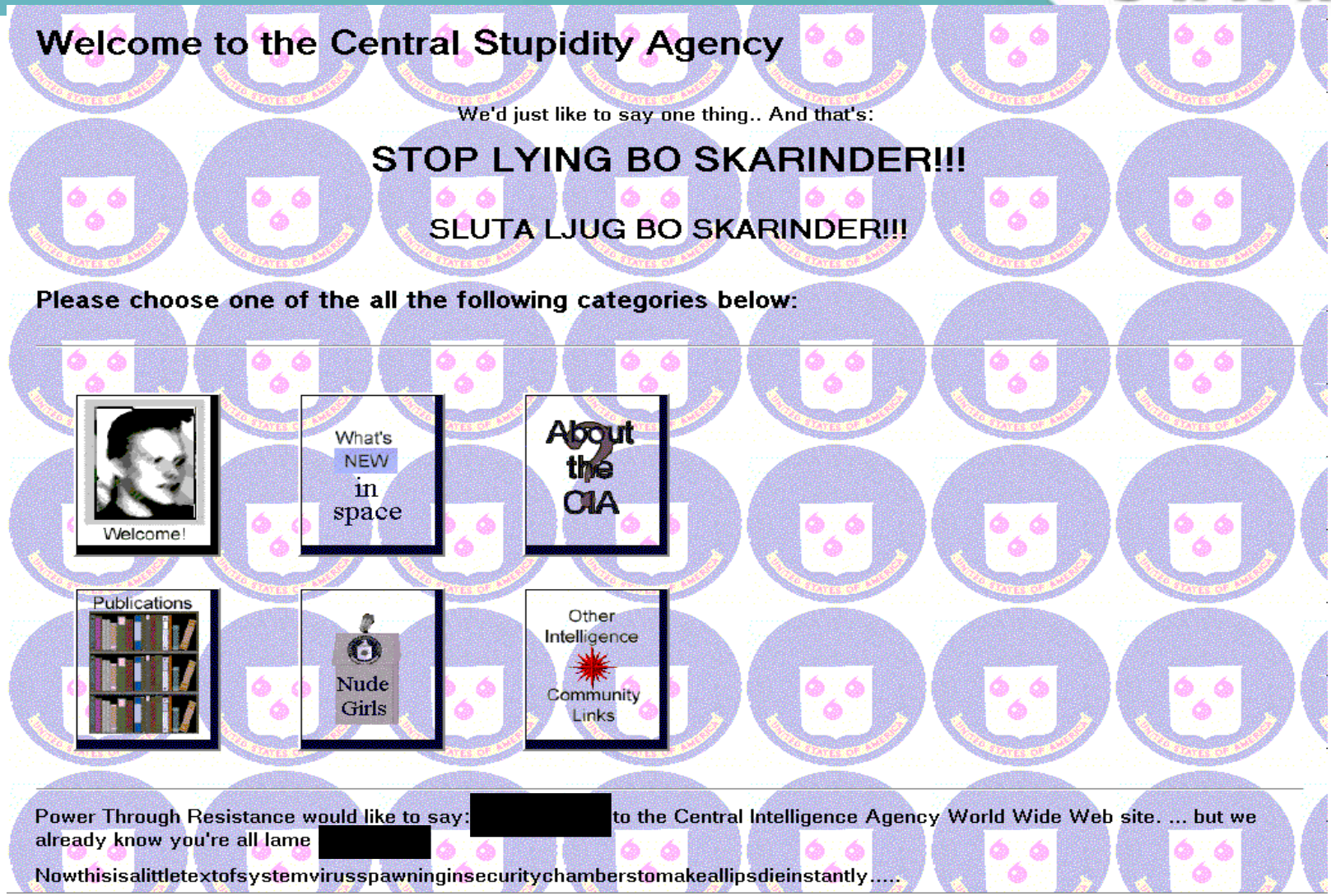
We will compare SNA and IP Security

Some Security Configurations for S/390 in the Internet World

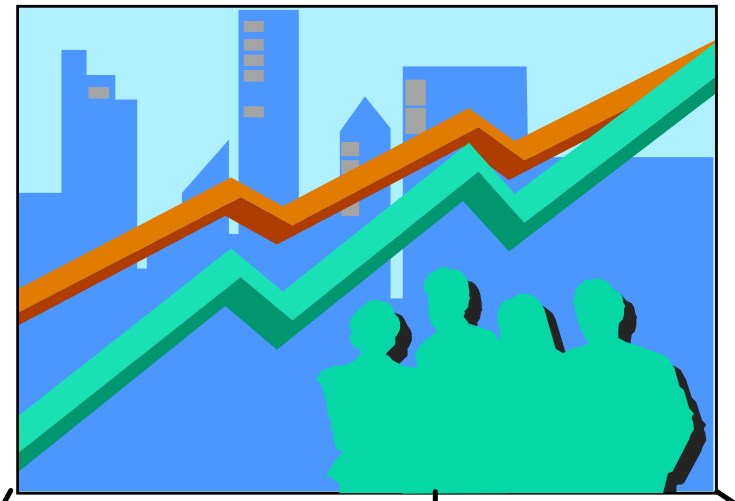
Last in this session we will take a look at some customer scenario’s


# Things to think about about !

# An example of why security is needed



# Customers



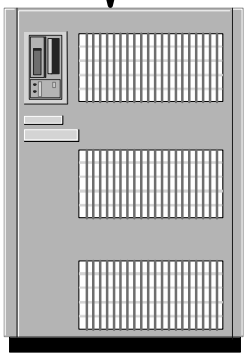
How many ?

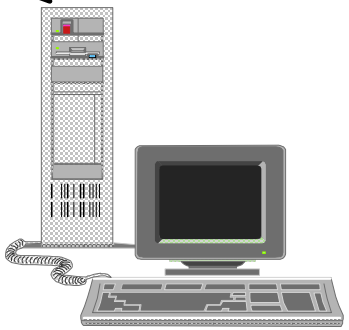
Millions ??

RACF, LDAP or PKI ?

Where are they ?

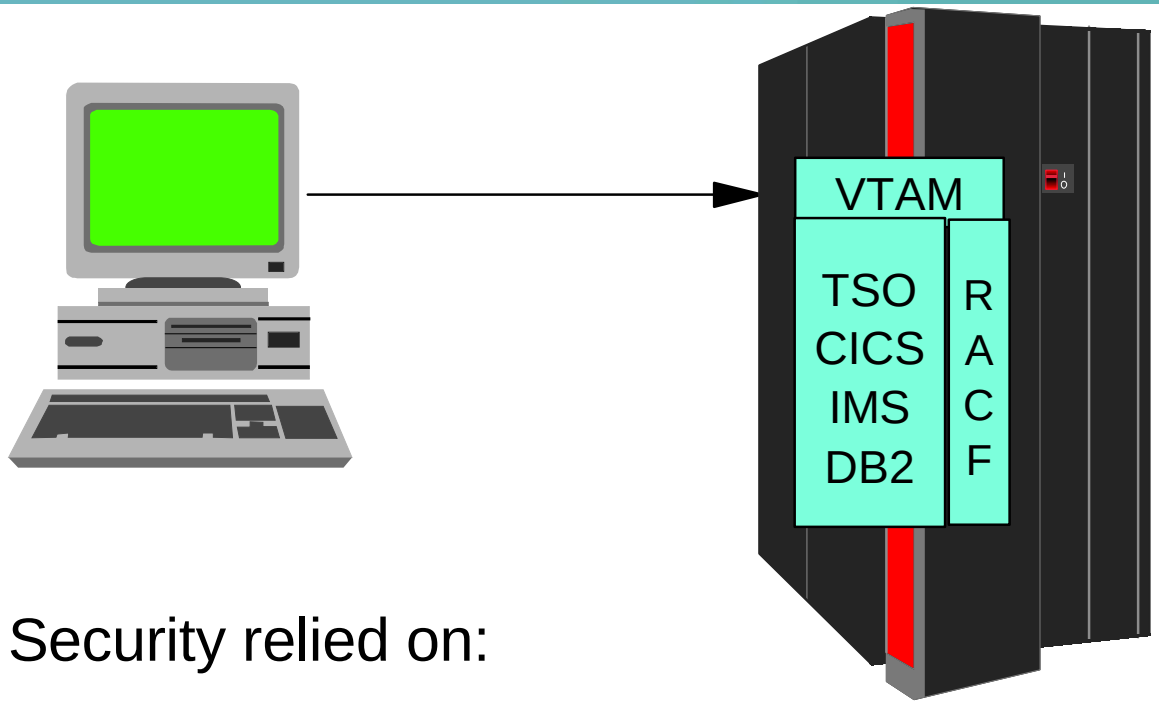
Probably anywhere !






# Protocols - SNA versus TCP/IP

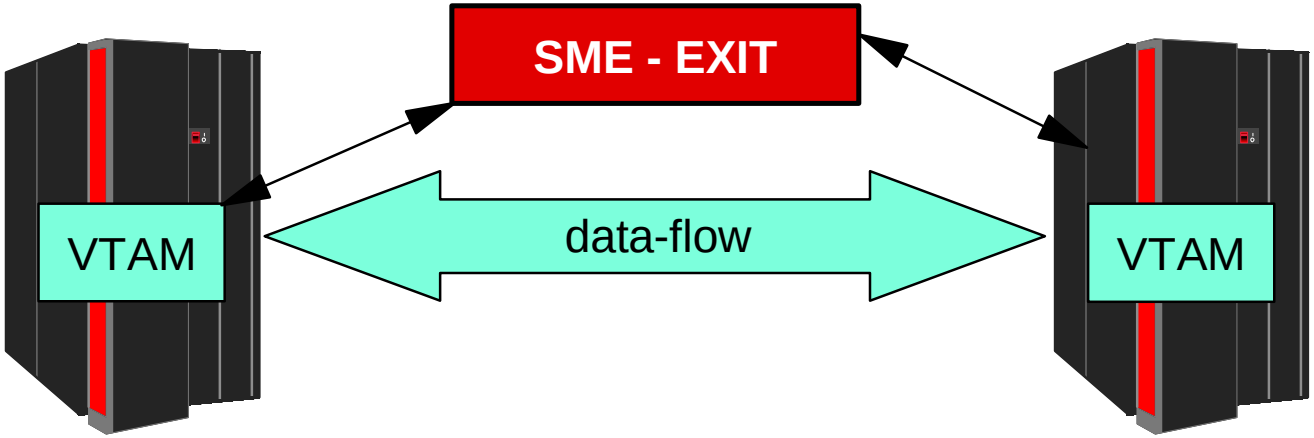
# Protocols - SNA/VTAM




Security relied on:

*User ID and password*
*VTAM Application Name*
*VTAM LU name (Terminal ID)*
*Private Network*

# Protocols - SNI Network



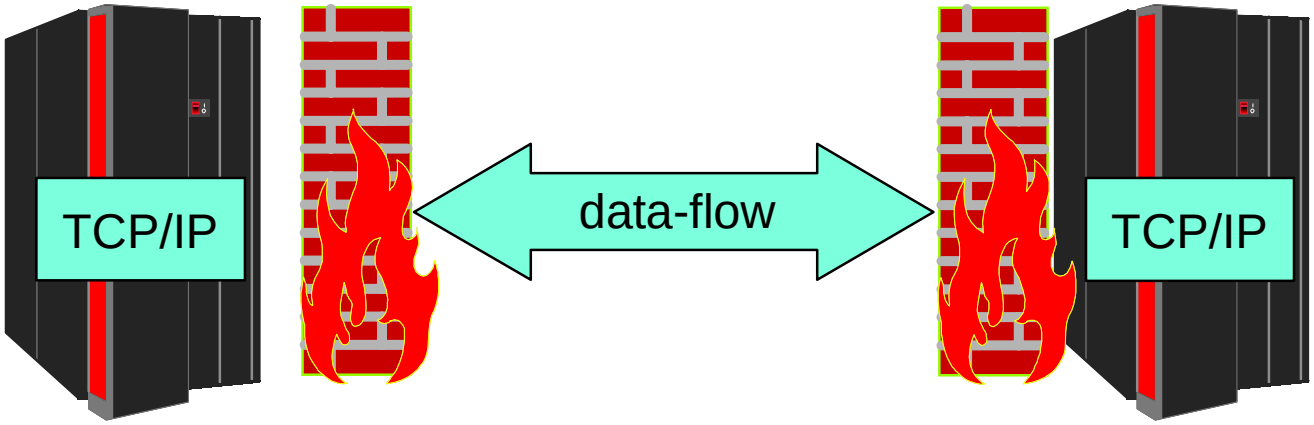

**Customer A** **Customer B**

Network Security relied on:

***Using a VTAM Session Management Exit to check:***
***VTAM Application Name***
***VTAM LU name and Network Name***

*Usually a private network*

# Protocols - TCP/IP Network




**Customer A** **Customer B**

Network Security relies on:

*May I pass the Firewall(s) with this IP address, this protocol and am I allowed to go to this TCP/IP port*

# Protocols - VTAM LU versus IPaddress

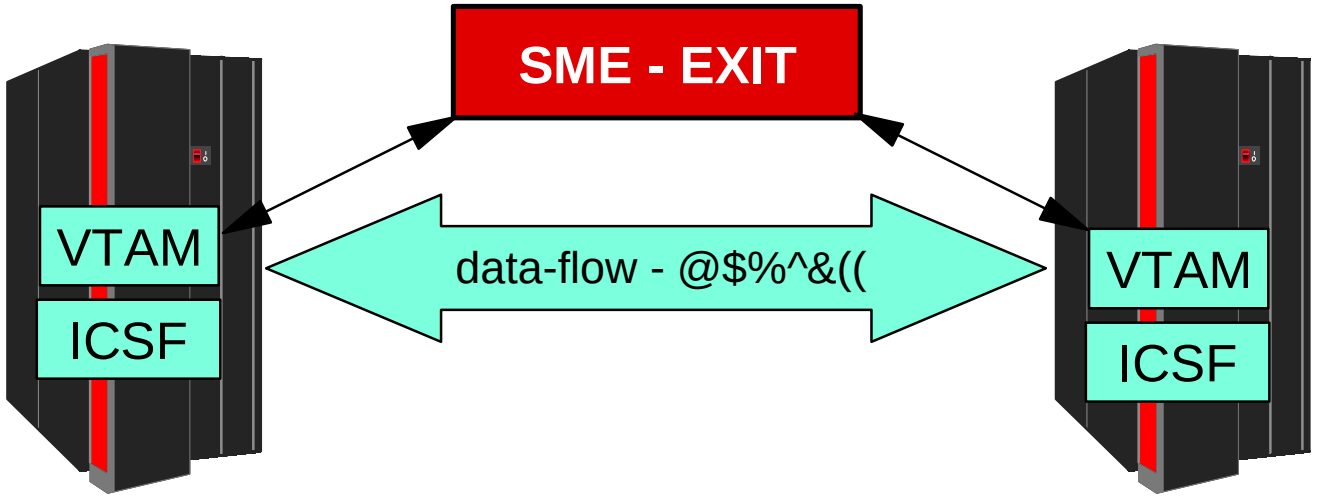

A lot of customers restricted access to applications based on a terminal id (VTAM LU) or groups of terminals

When moving from SNA to TCP/IP no longer is there a "logical Unit" that we potentially can trust or rely on.

IP addresses can be seen as terminals, and defined as terminal profiles, but IP addresses are dynamic, depending on where your customer/client is coming from. (e.g. what Internet Service Provider (ISP))

# Protocols - SNA - data encryption

When we had a need to encrypt data flowing over
an SNA network, we can use VTAM Session Level Encryption (SLE)

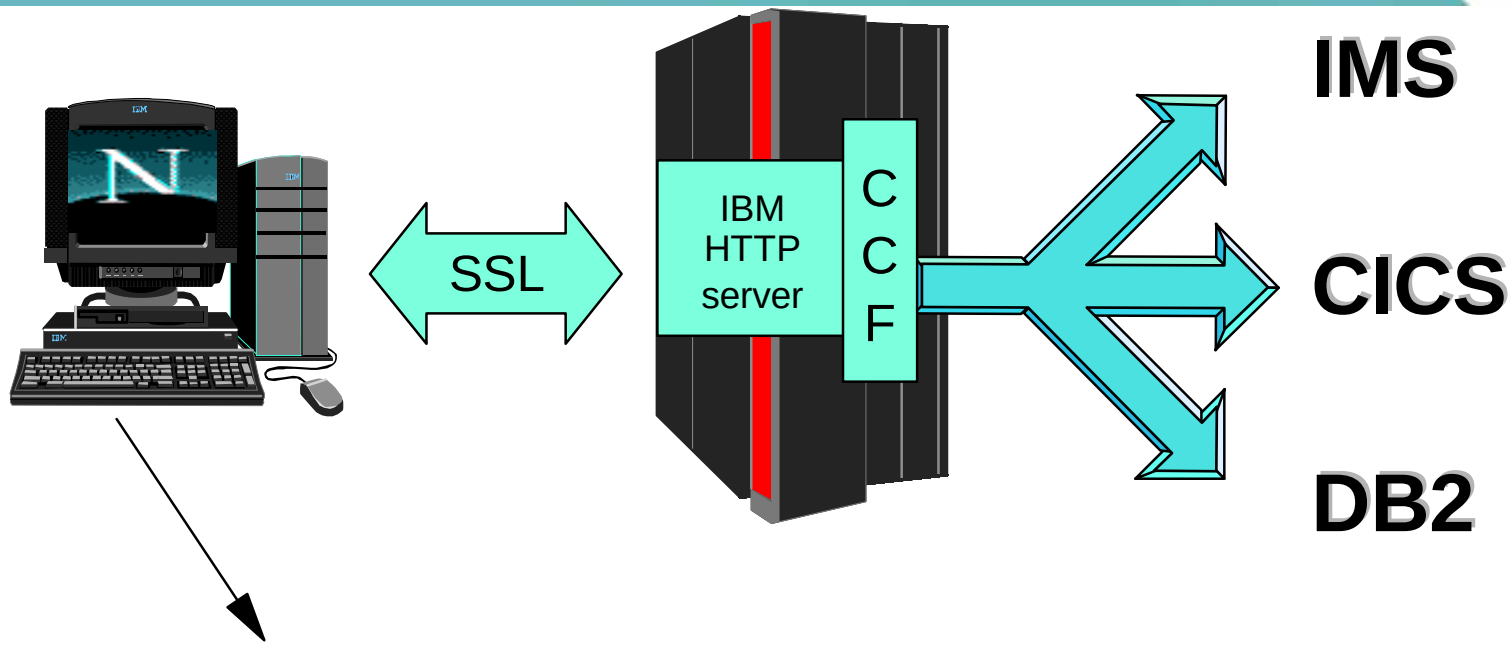


# Protocols - TCP/IP data encryption


Options available on OS/390 to encrypt the data flow over an TCP/IP network:

- Secure Sockets Layer (SSL) available for applications like:
  - IBM HTTP Server for OS/390 (IHS)
  - TN3270 Server (Telnet)
  - LDAP Server (Directory Services)
  - CICS Web Services (CWS)
- Virtual Private Networks (VPN) support using Internet Key Exchange (IKE)

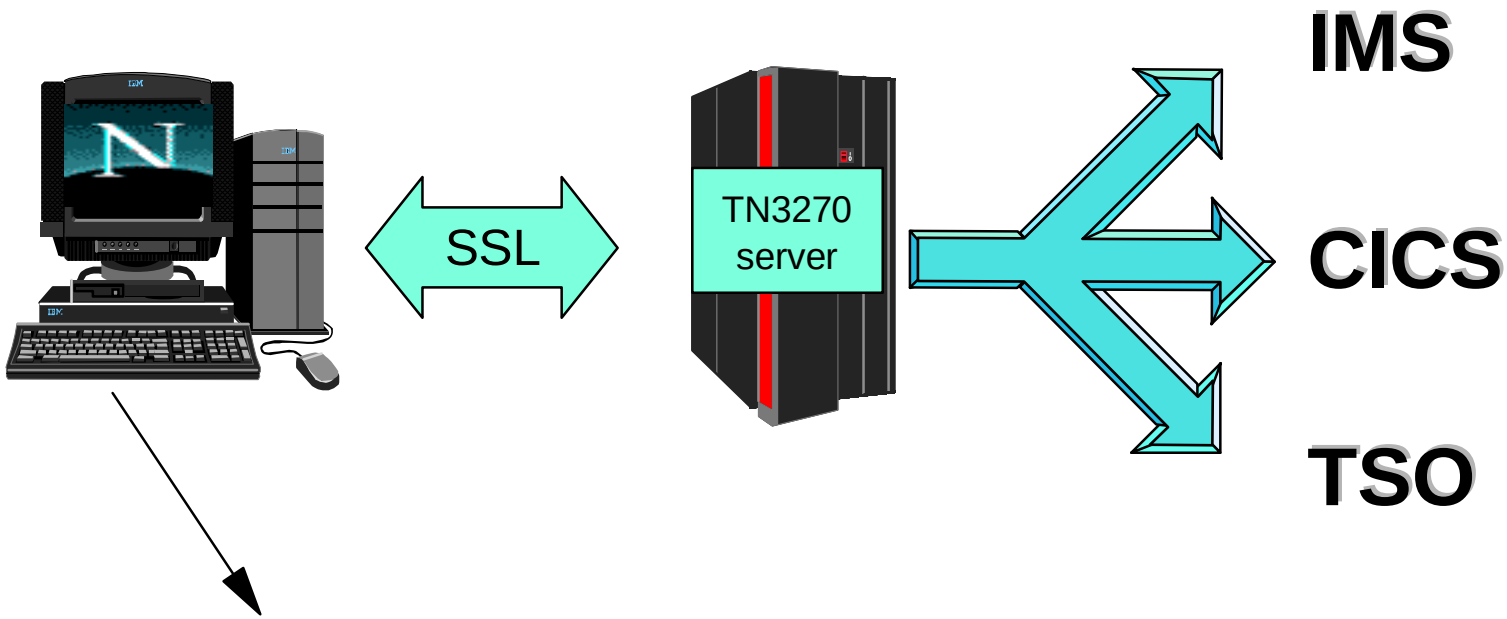
# Secure HTTP using SSL(Web Server)




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

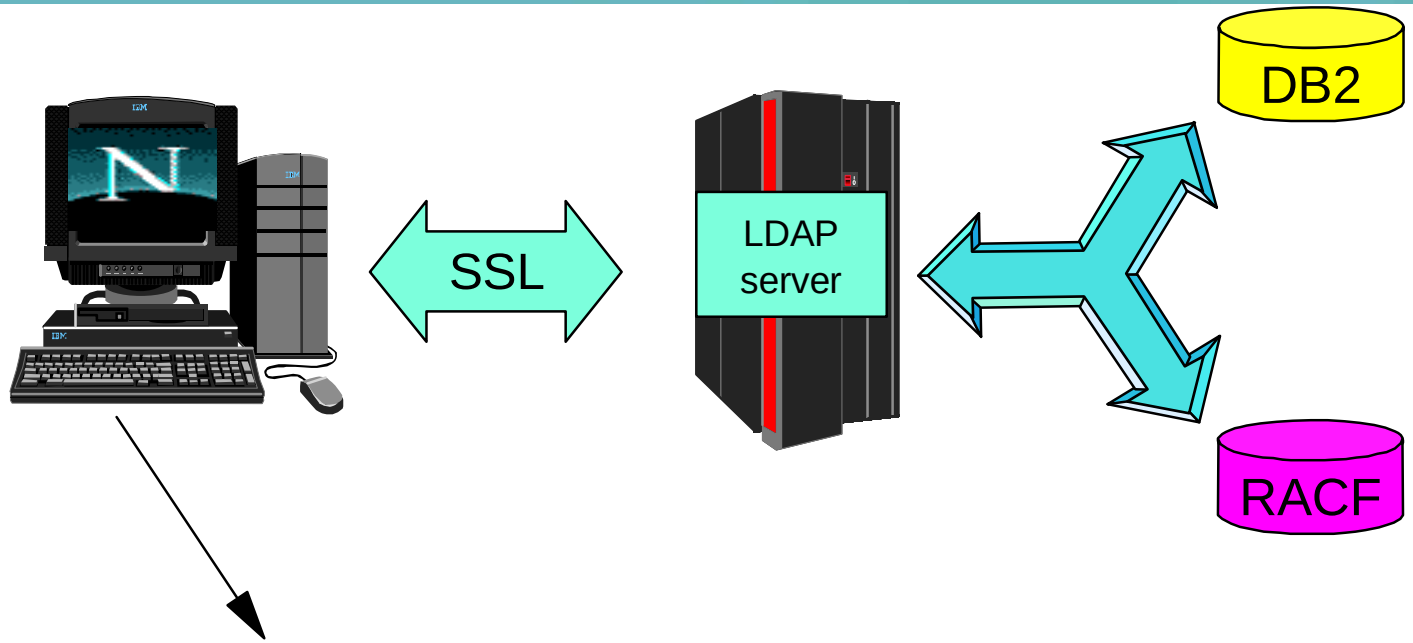
Encryption strength depends on encryption algorithm selected in SSL handshake between the browser and the server.

# Secure TELNET (TN3270)




Telnet client (PCOMM or Host On Demand)
(optionally client authentication)

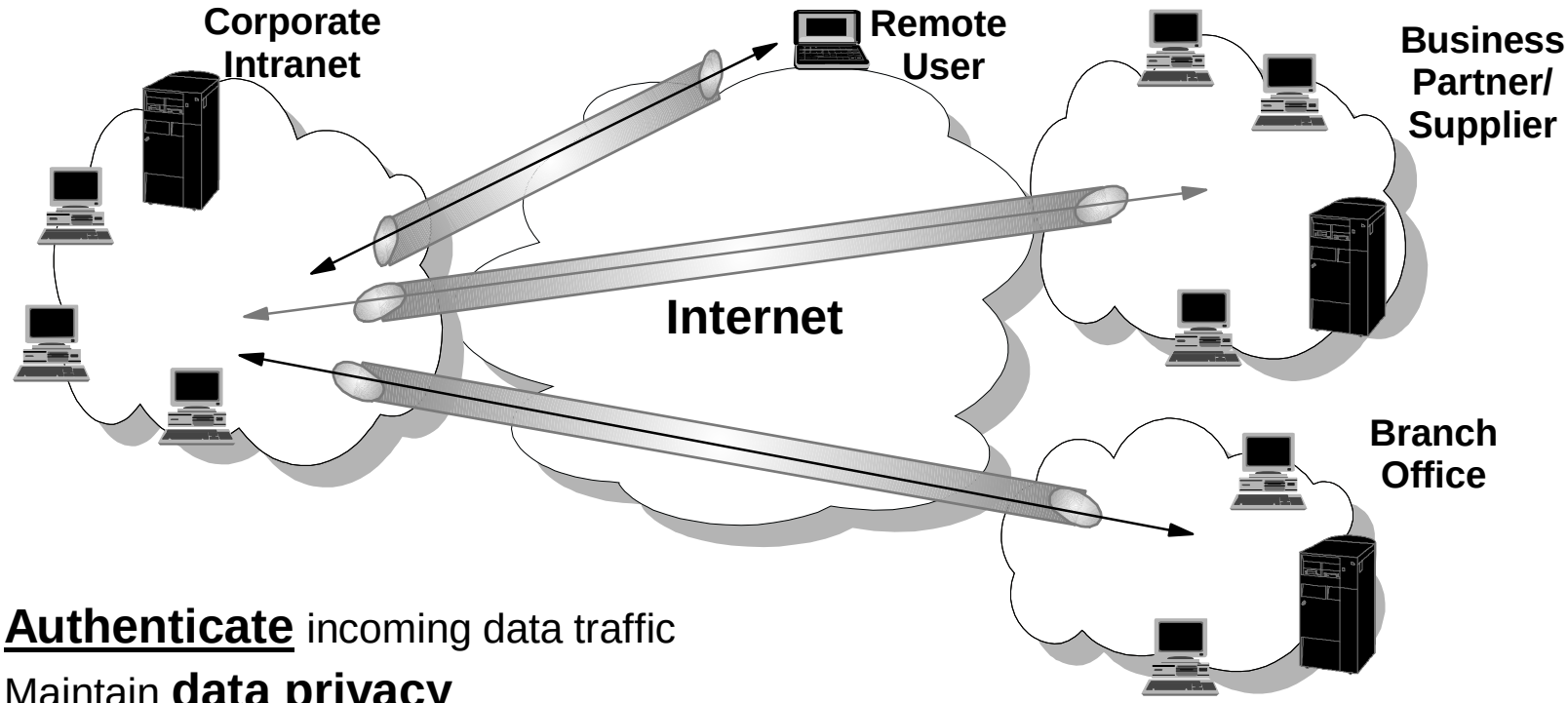
# Secure access to Directory Services(LDAP)




LDAP client (C, C++ or JAVA (jndi)

# Virtual Private Networks (IPSec)

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



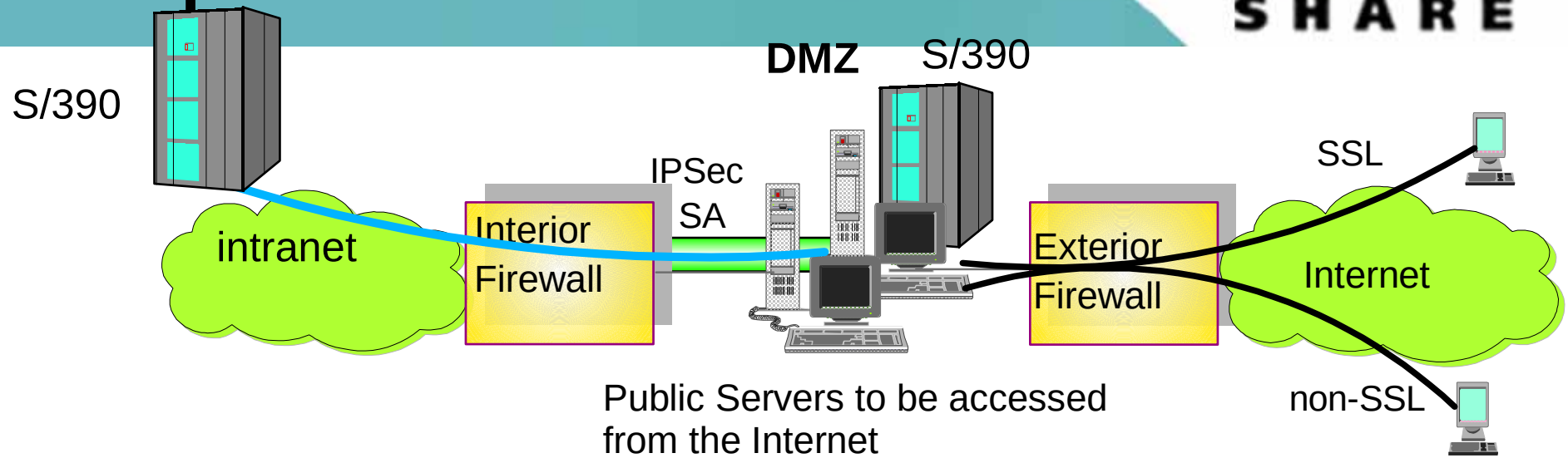

**Authenticate** incoming data traffic

Maintain **data privacy**

Manage access as with private network

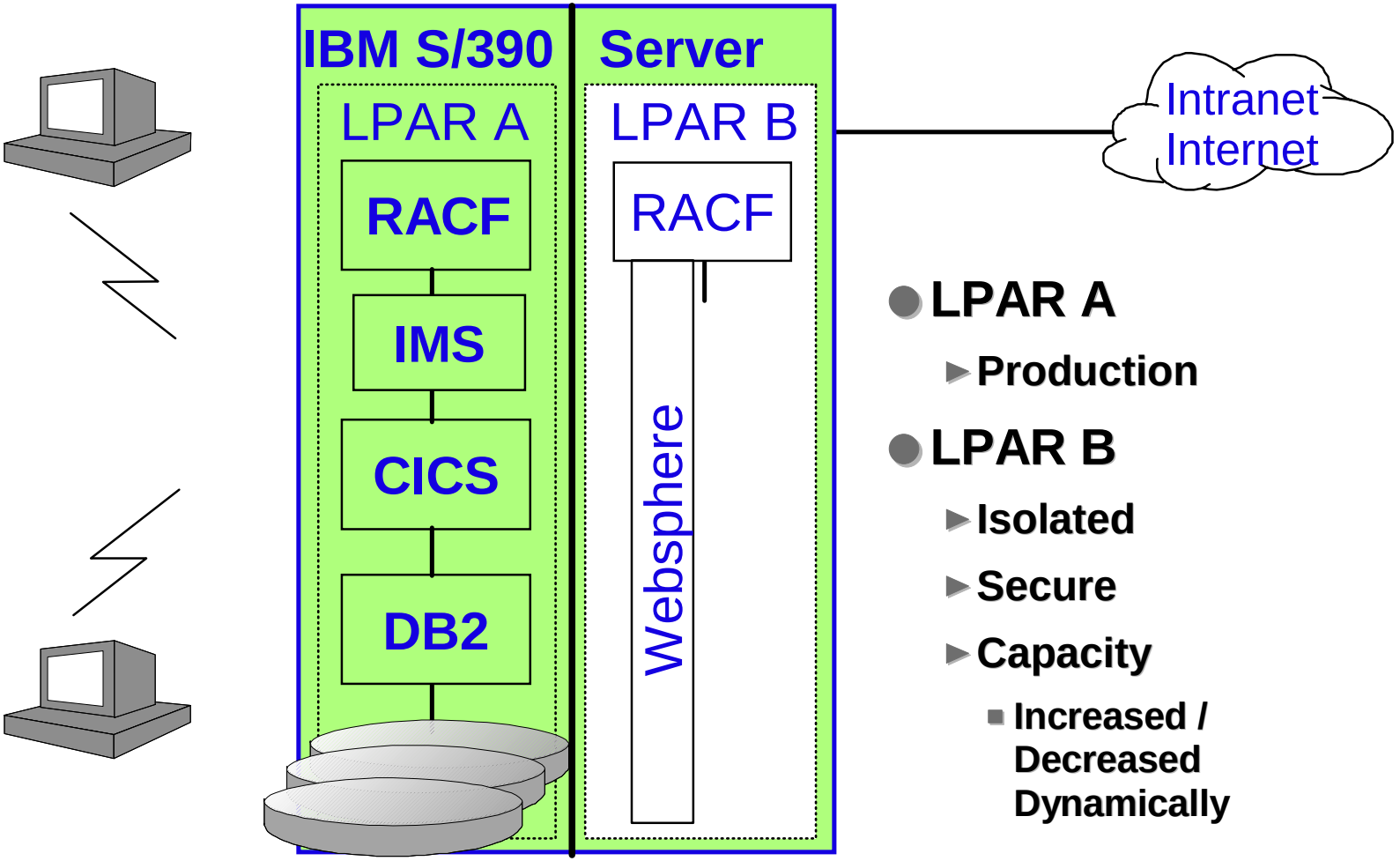

# S/390-Z-series and the Internet

# Demilitarized Zone (DMZ) Concept for Public Servers



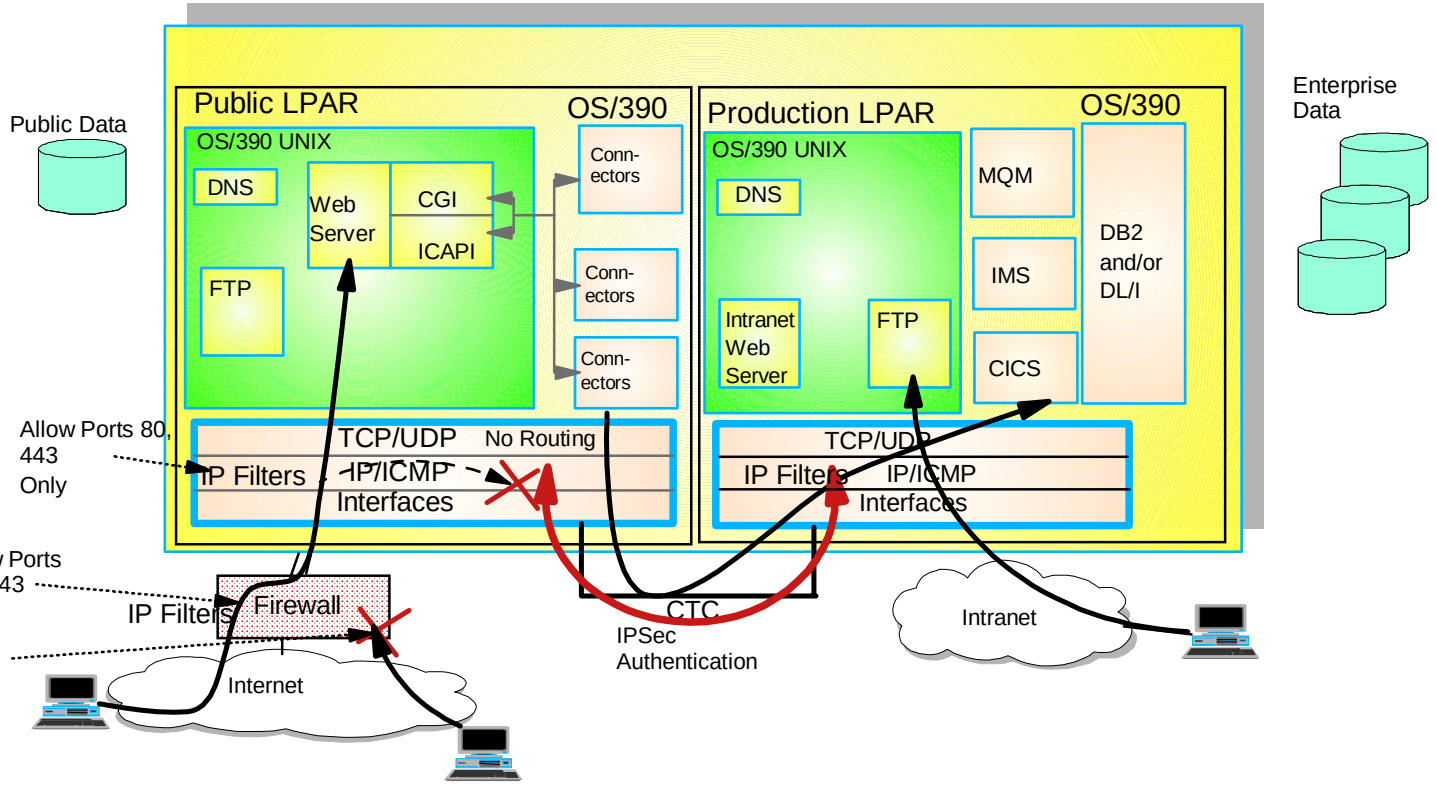

- **Exterior firewall allows only traffic to DMZ servers**
  - Traffic can be SSL or non-SSL depending on data sensitivity.
- **Data can be exchanged with DMZ servers and back-end hosts in the intranet through the interior firewall.**
  - Interior firewall allows only traffic from DMZ server
  - Traffic can be protected by security protocols as necessary
  - IPSec can be used to authenticate to interior firewall
- **The DMZ will require public IP addresses, because it is accessible at an IP level from the public network (i.e. the Internet)**

# Workload Isolation



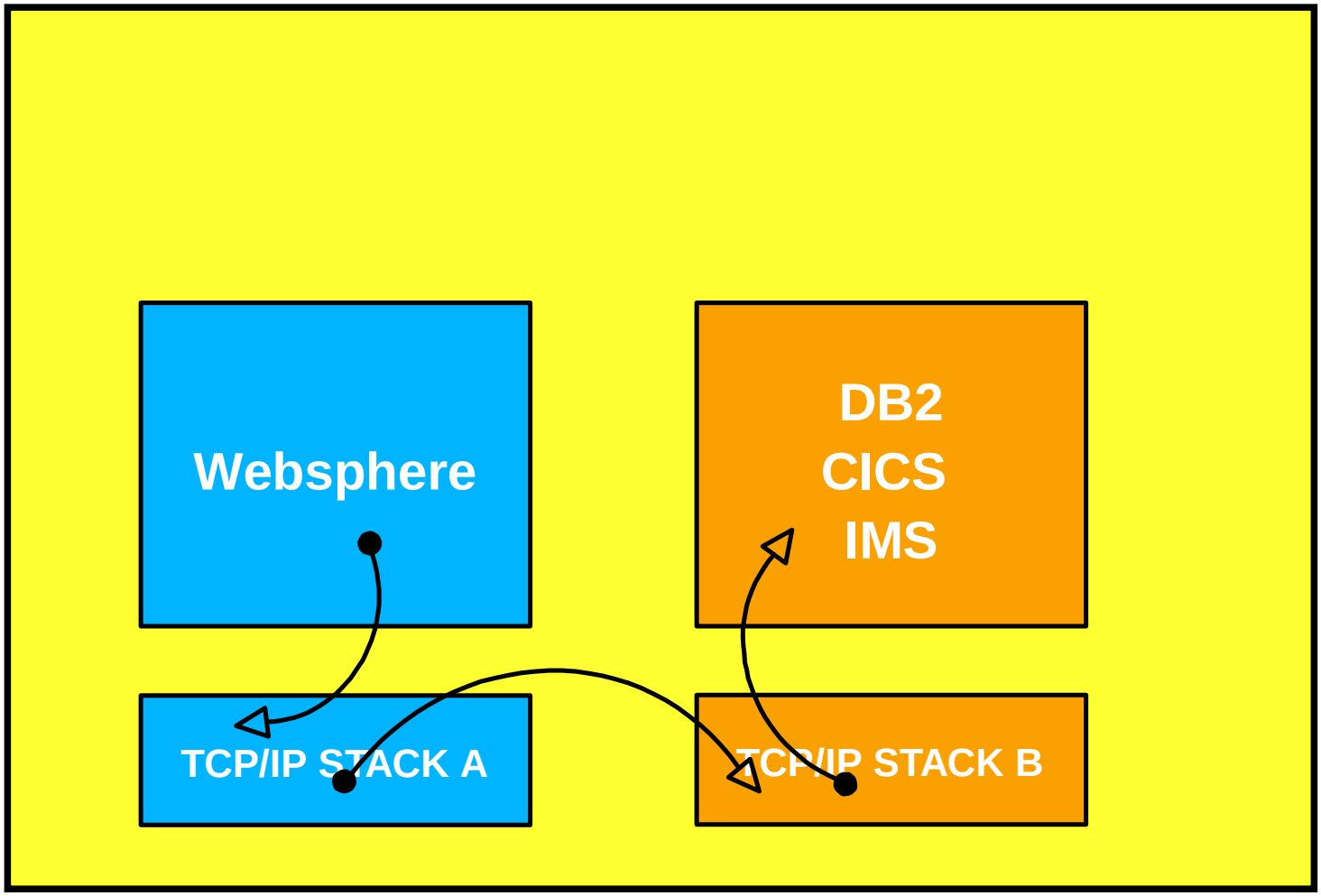

- **LPAR A**
  - **Production**
- **LPAR B**
  - **Isolated**
  - **Secure**
  - **Capacity**
    - **Increased / Decreased Dynamically**

# Public and Production Systems on Single S/390

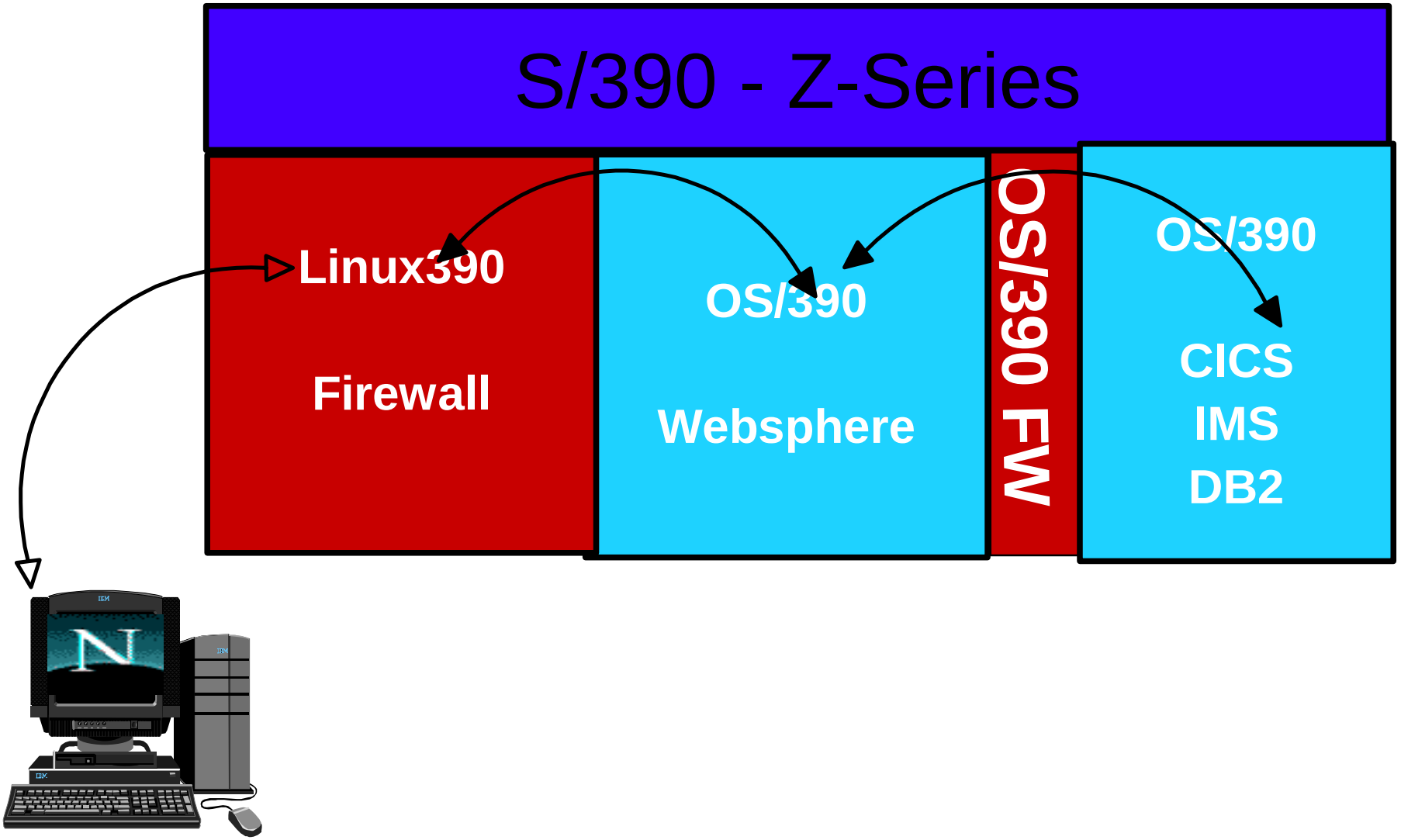



- **External Firewall can absorb cycles used to deflect unwanted incoming traffic**
  - Based on destination port
    - Ex: Only allow Web / Deny all others
  - Insulate Public Z900(S/390) from Flooding Attacks
- **Filtering used on Public Z900(S/390)**
  - Second line of defense

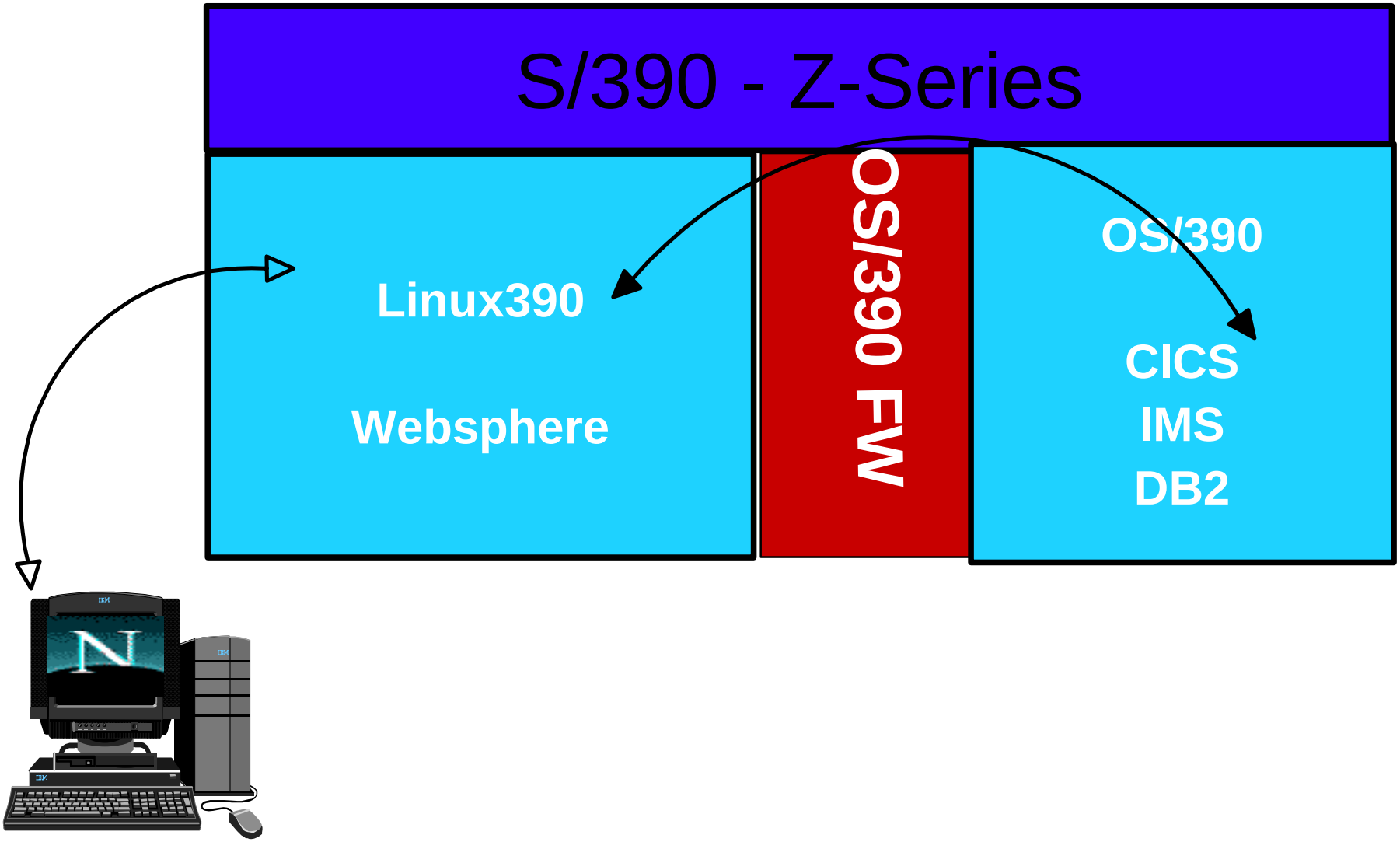
# TCP/IP Stack Seperation



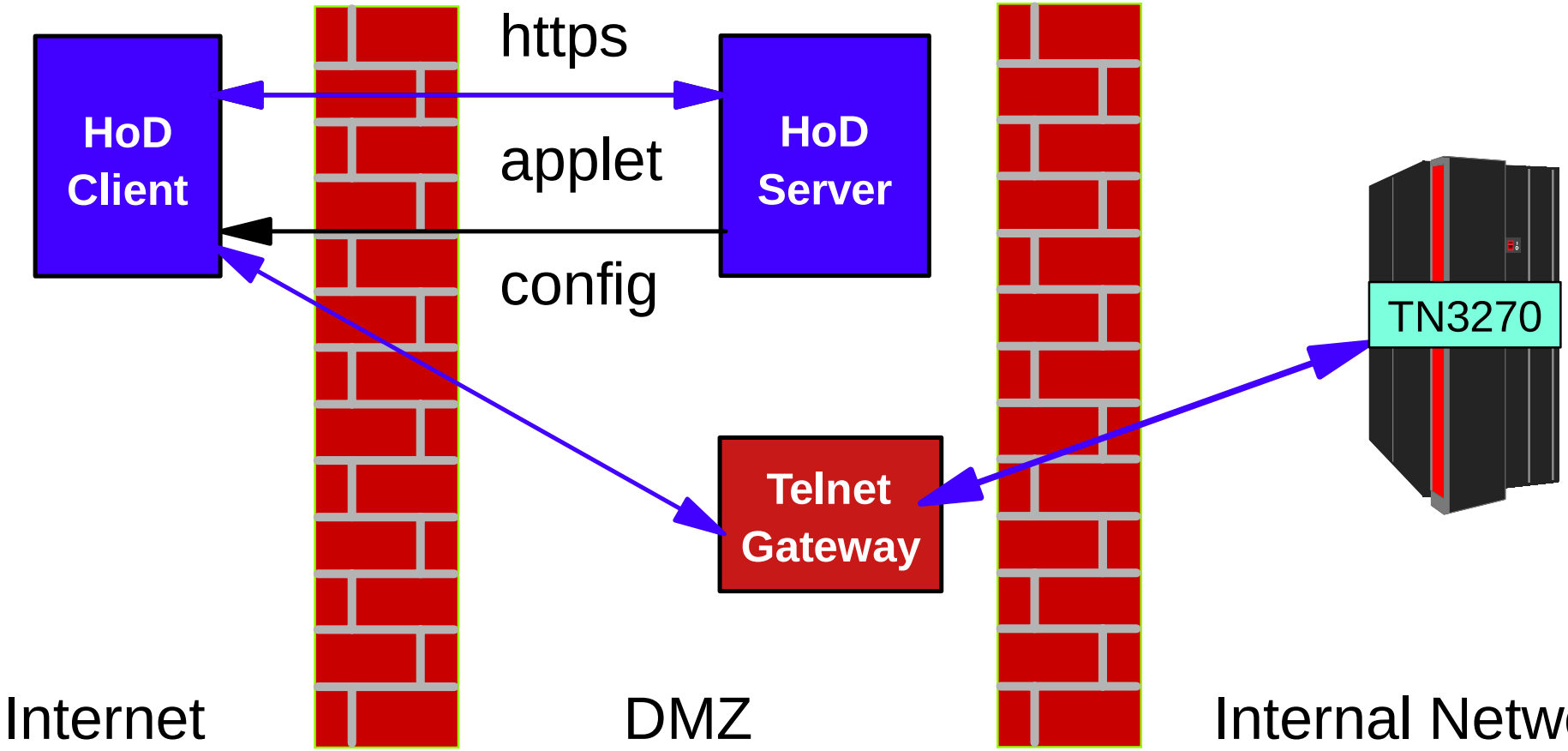
# Firewall support on Linux/390



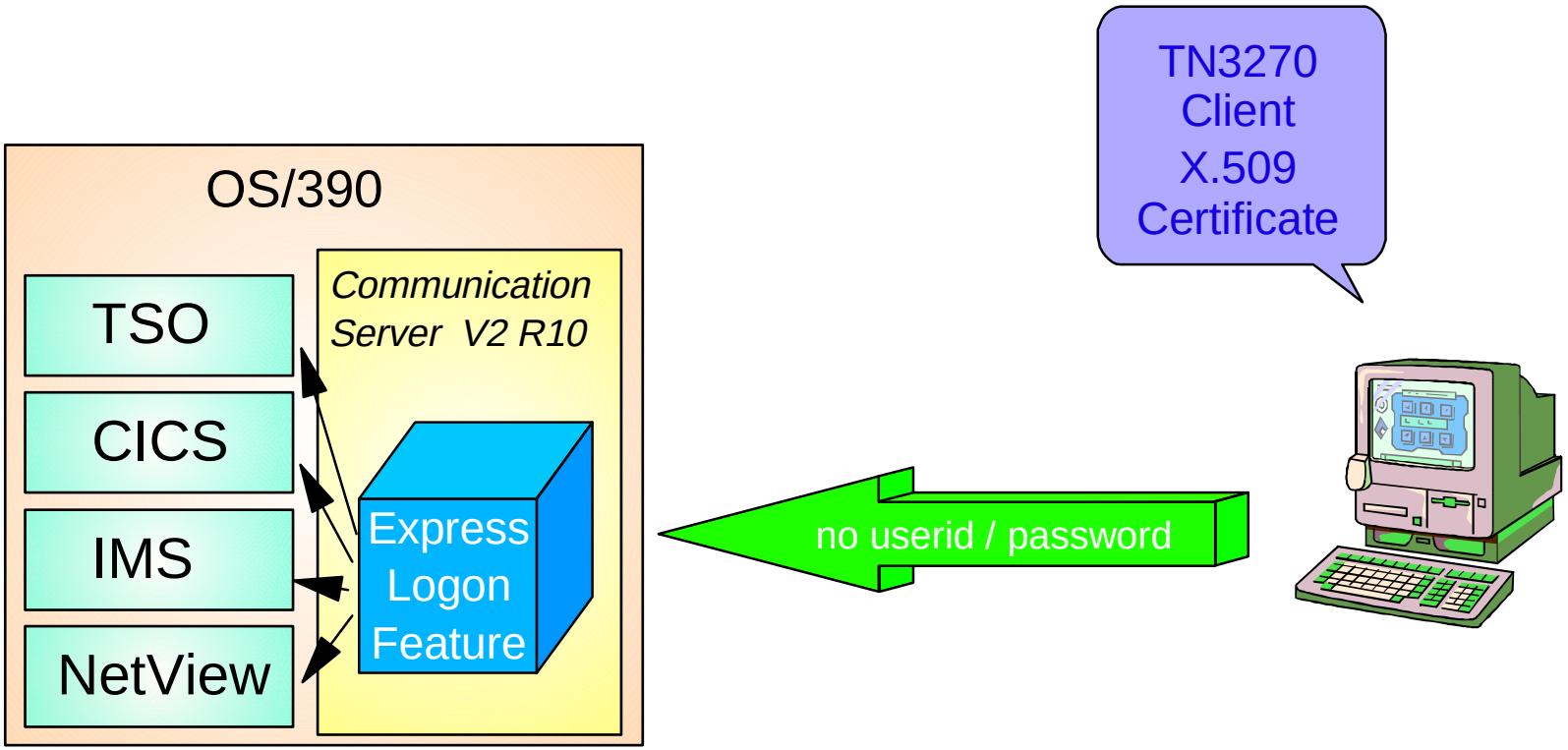
# Websphere AE on Linux/390



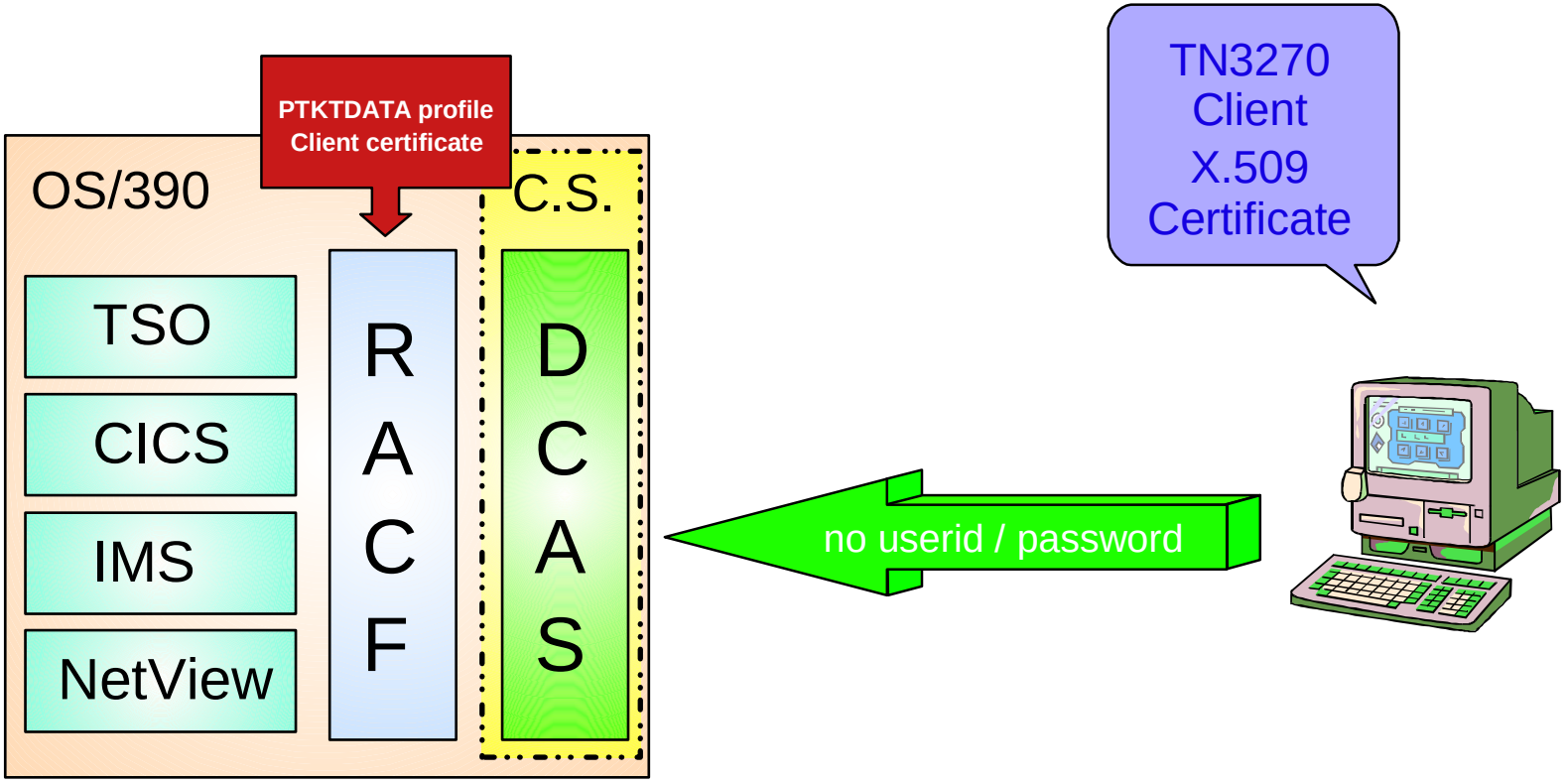
# Host on Demand (HoD)



# Express Logon Feature overview

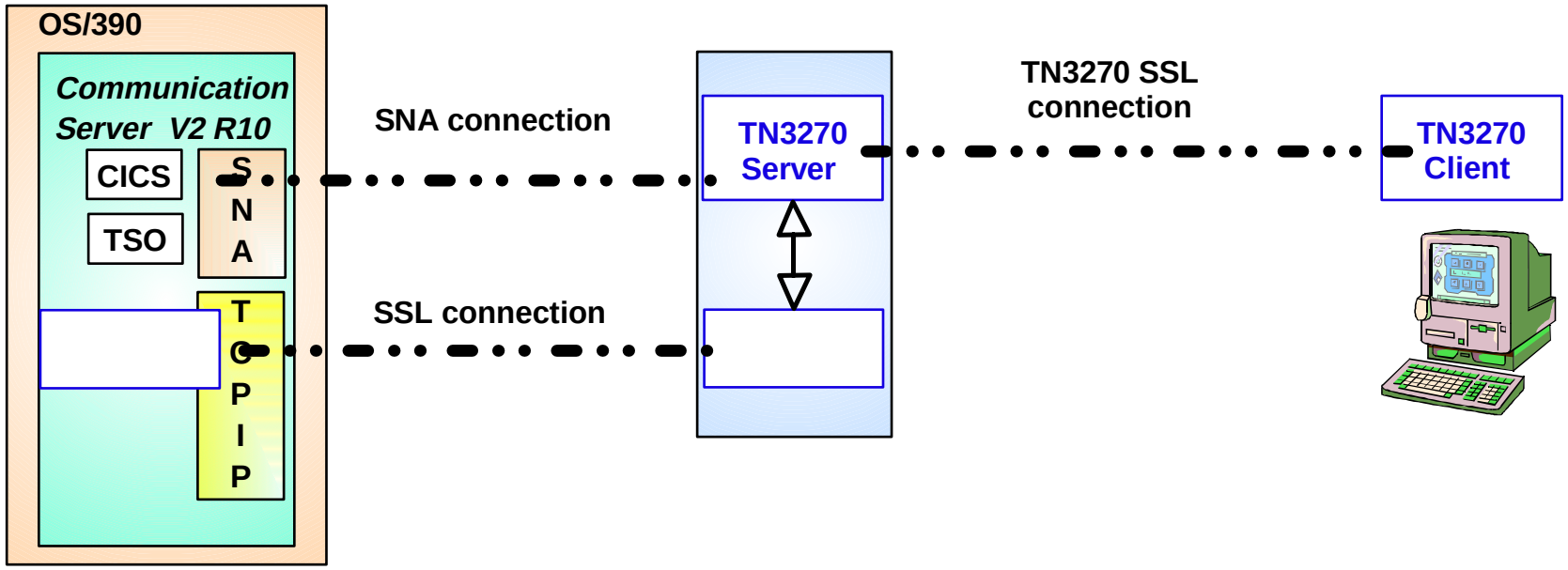


# General requirements (cont'd)

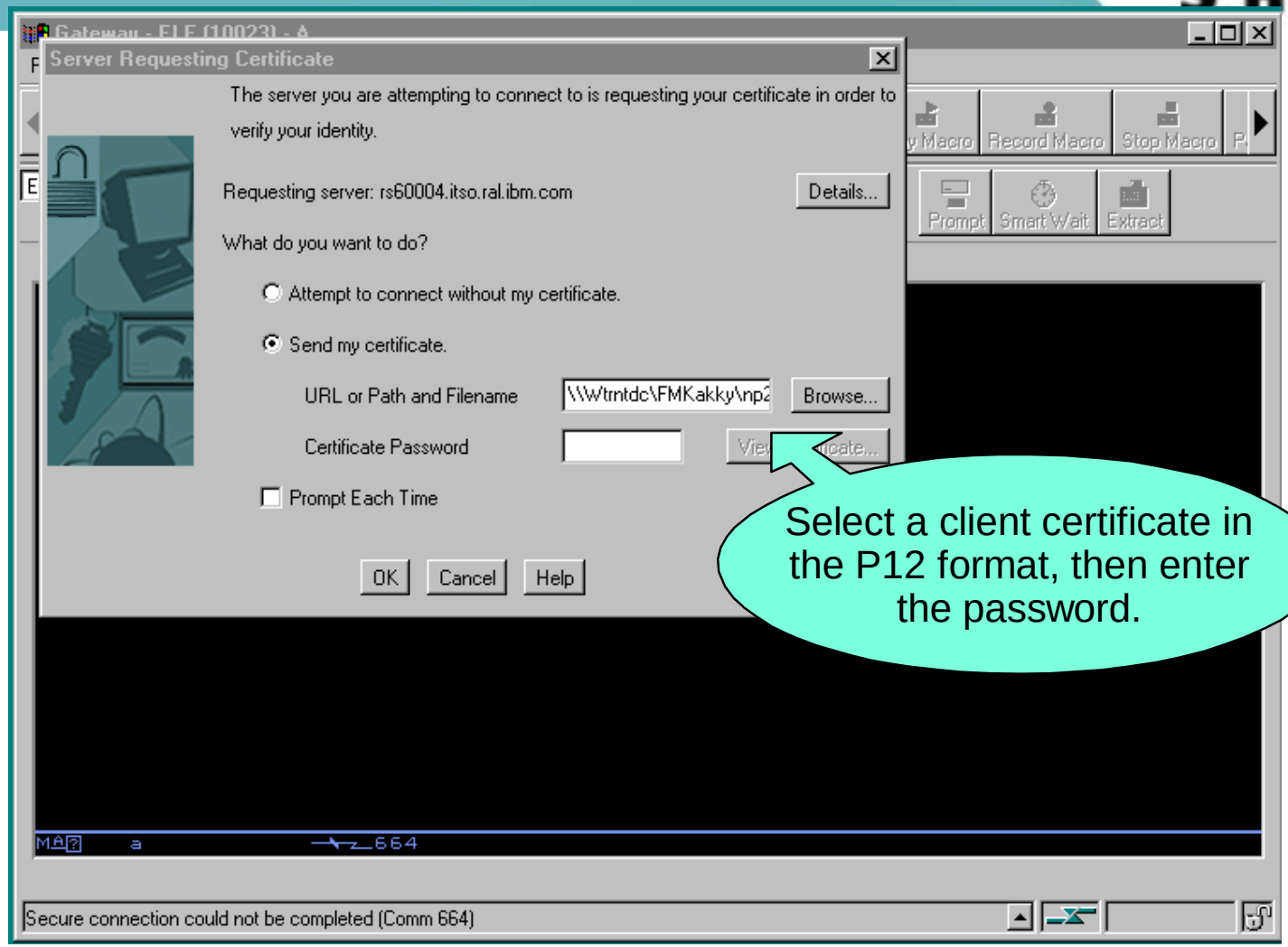


# Three-tier network design

- OS/390
  - IBM CS for OS/390 R10
  - RACF
  - DCAS
  - SNA Application
- Middle-tier server
  - TN3270 Server
  - Digital Certificate Acces Requester (DCAR)
- Workstation
  - TN3270 client
  - SSL with X.509 Certificate

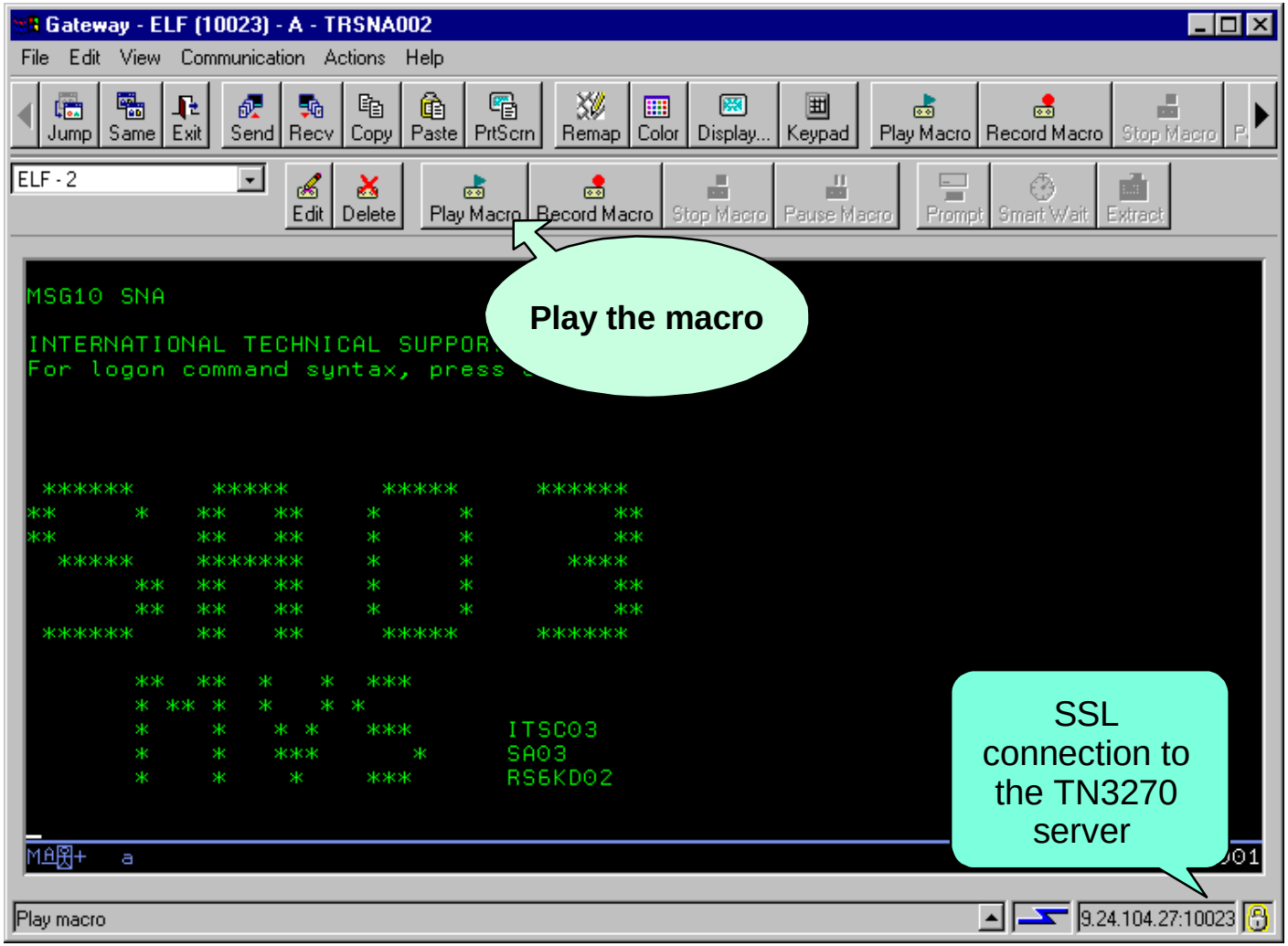


# HoD V5 - select client certificate

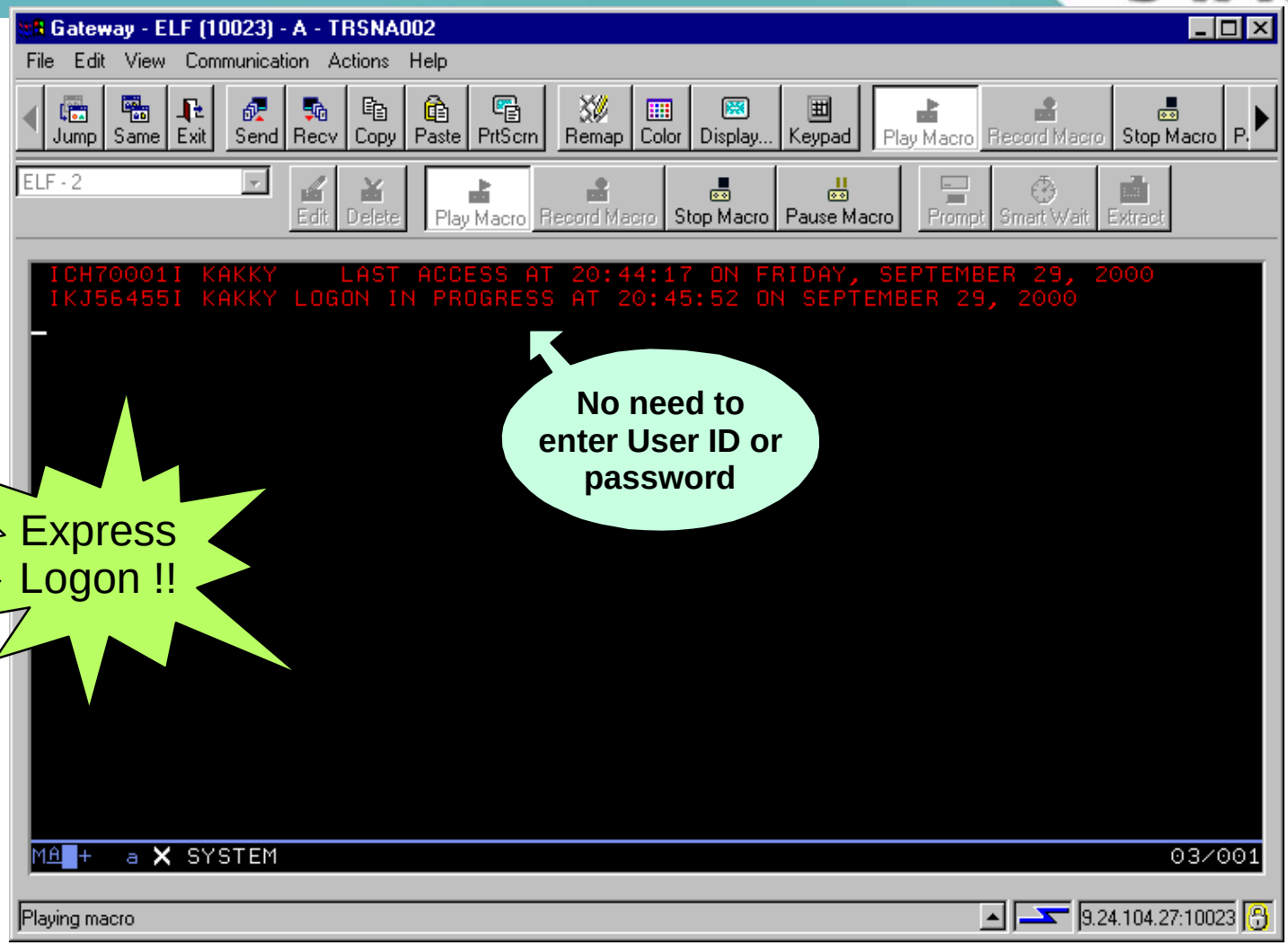



Select a client certificate in the P12 format, then enter the password.

# HoD V5 - MSG10 message



# HoD V5 - express logon




# Customer Scenario’s

# Customer Scenario I


Financial Customer

- Traditional S/390 Customer, CICS/DB2 oriented
- Merged recently, now have a SUN Web environment as well

Challenges

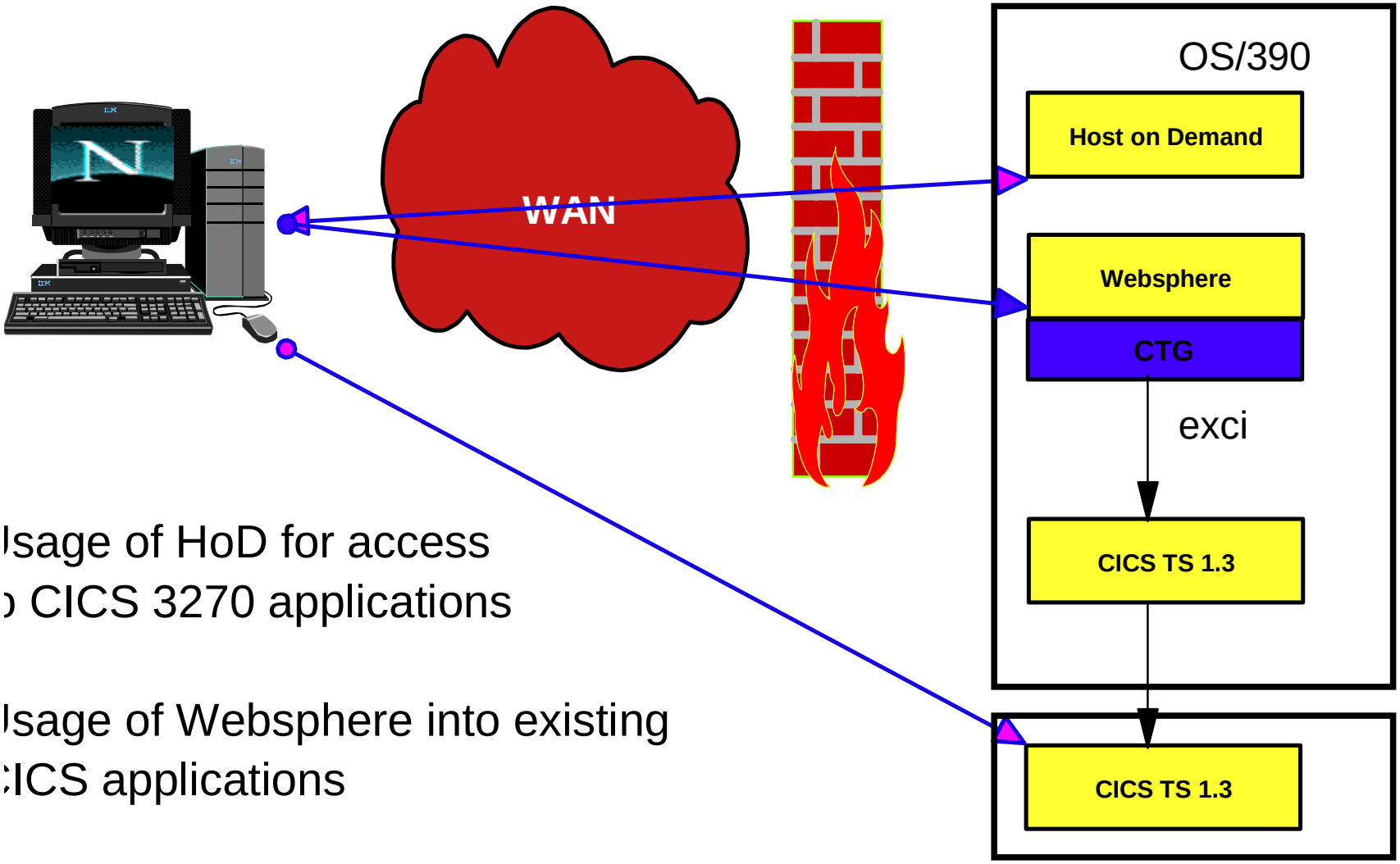
- Security flows between systems
- "dual" authentication requirement

# Customer Scenario I ...


The new application had to meet the following design considerations:

- Existing applications accessible via Web browsers
- Ease of use by traders with little computing knowledge
- Ability to provide an audit trail of the authentication of every transaction performed
- Ability to scale the system with increased usage
- Available quickly and without modification of the existing client workstations

# Customer Scenario I .....




lsage of HoD for access
› CICS 3270 applications

lsage of Websphere into existing
:ICS applications

# Customer Scenario I ...

## Security Challenges

- Dual Authentication
  - Every client will get a digital Certificate and has a RACF User ID and PW and they are linked together.
  - The HTTP server allows for both a certificate and a RACF User ID/pw, but do not need to be "linked" together.
  - Needed a HTTP Server exit to accomplish that.

# Customer Scenario I ...

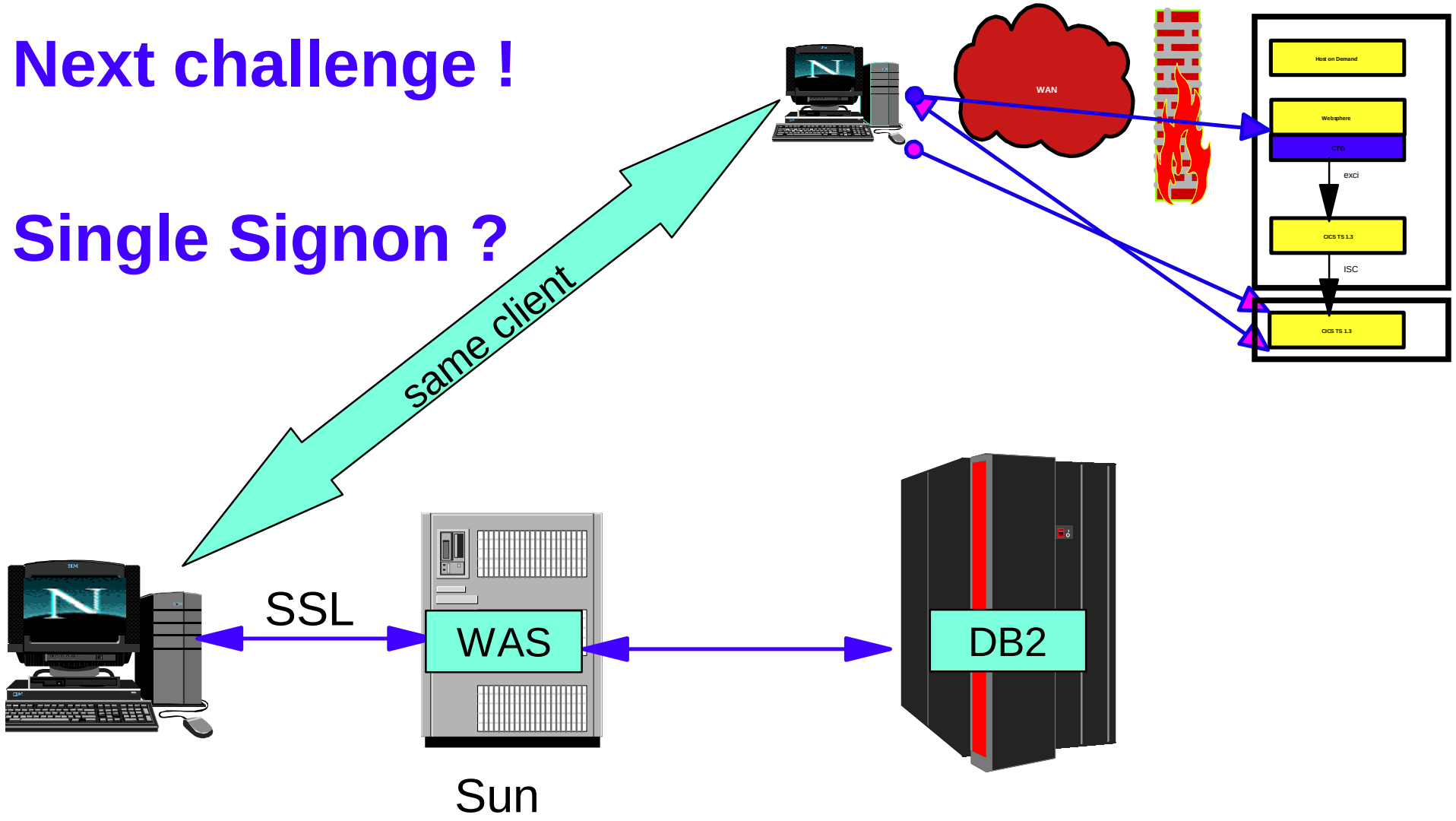
## Security Challenges

- Customer became their own Certificate Authority (CA) using Tivoli PKI (initially used IBM's Vault Registry)
  - SSL Client Authentication caused headaches for both IBM and Customer, HoD and CTG required certs in different formats (PKCS#12 and JAVA keyring) because no access to browser's keyring
  - Browser's support for certs left something to be desired
  - Netscape (prior to 4.7) had a SSL handshake bug !
  - Internet Explorer times out the SSL session after ten seconds !

# Customer Scenario I .....

## Next challenge !

## Single Signon ?



# Customer Scenario II

Financial Customer

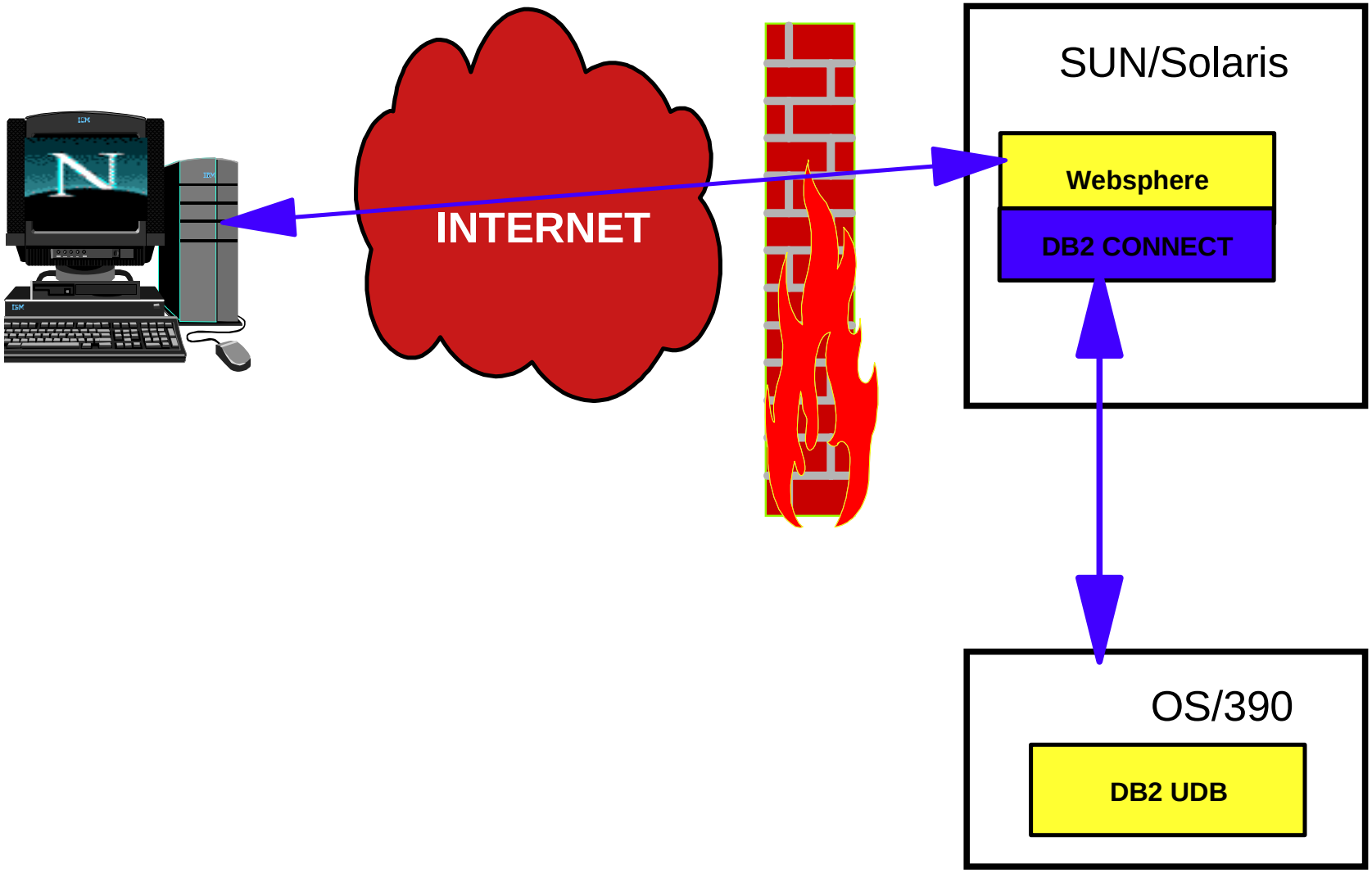
- Mixed vendor environment
- Web deployment on SUN/Solaris
- Data resides on S/390 and DB2 databases

# Customer Scenario II ...


The new application had to meet the following design considerations:

- Time to market crucial
- Ease of use for customers (you and me)
- Security should not be an inhibitor

# Customer Scenario II .....



# Customer Scenario II ...


## Security Challenges

- Authentication
  - SSL used but no "SSL Client Authentication"
  - User ID and PIN used to access application (existing directory)
  - Hardcoded RACF User ID and password in the application !
  - Audit trail !

# Customer Scenario II ...


## Security Challenges

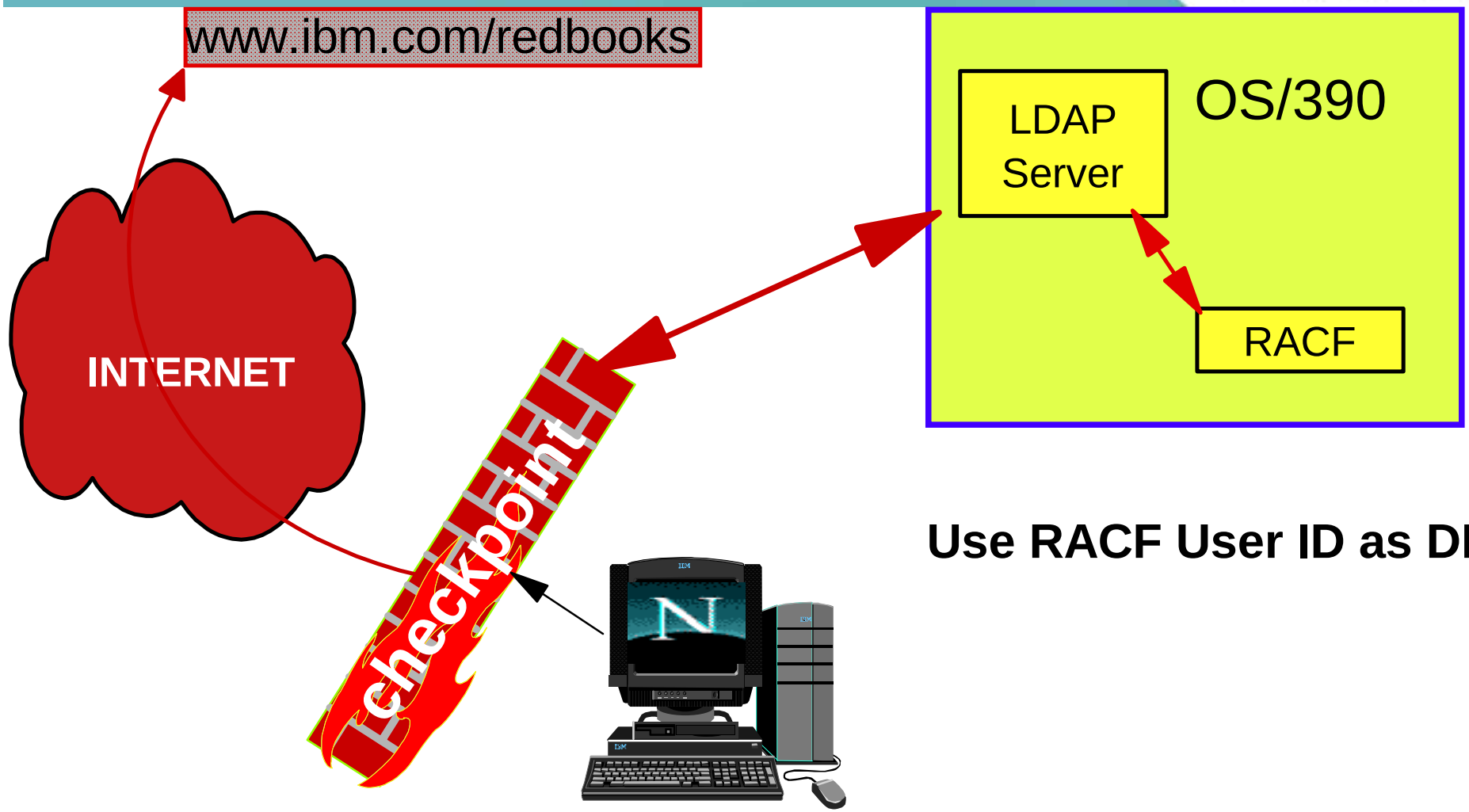
- OS/390 Security Implementation additions:
  - Implemented OS/390 Firewall Technologies IP filters to ensure the right server is talking to the right server !
  - Because of hardcoded ID/PW we wanted to restrict access to DB2 UDB based on TCP/IP port, to prevent access internally using DB2 Connect

# Customer Scenario III

Insurance and Securities Company

- Mixed vendor environment
- Struggling with password synch across systems
- Used Checkpoint firewall to allow internal personnel access to the Internet using a Netscape Directory (another one !)
- Wanted to exploit OS/390 LDAP - RACF interface

# Customer Scenario III ....




**Use RACF User ID as DN**

# Customer Scenario III ...

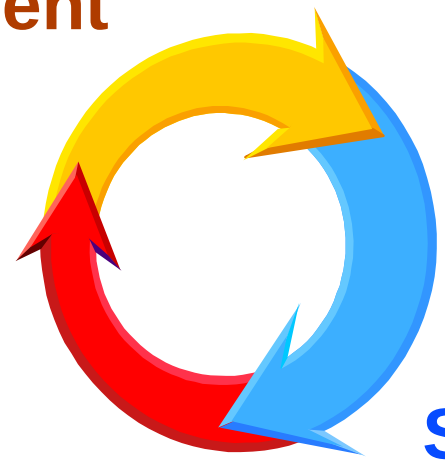
## Security Challenges

- Checkpoint supported LDAP but did not distinguish between the LDAP bind and the LDAP lookup for "entitlements"
- Checkpoint currently does not support user written authentication
- OS/390 LDAP development is working on "native authentication"
- Allows a indicator in the LDAP schema to indicate this User can be verified locally using the UNIX callable service (__passwd).
- Use OS/390 LDAP interface to RACF requires OMVS segments !

# The Cost of Coffee

## A Catch-22

More money spent on Coffee than Security



Security Problem Occurs

Sharp Increase in Security Resources

Security Hours Increase to Resolve Problem

# Recommended reading


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 and Policy Management,SC24-5309

OS/390 Security Server 1999 Updates; Technical Presentation Guide, SG24-5627

OS/390 Security Server 1999 Updates; Installation Guide, SG24-5629

SecureWay Host on Demand Version 4, SG24-2149

Millennium proof security for OS/390, SG24-5675 (redpiece, soon !)