OS/390 Security Server: Firewall Overview and Directions

SHARE Session 1744
July 27, 2000
Boston, Massachusetts

Dave Wierbowski
OS/390 Firewall Technologies Development
Endicott, New York

(607) 752-6739
wierbows@us.ibm.com

Trademarks

The following are trademarks of International Business Machines Corporation:

- CICS
- DB2
- IBM
- IMS
- OS/390
- AIX

The following are trademarks or registered trademarks of other companies or institutions:

Windows NT, 95, 98

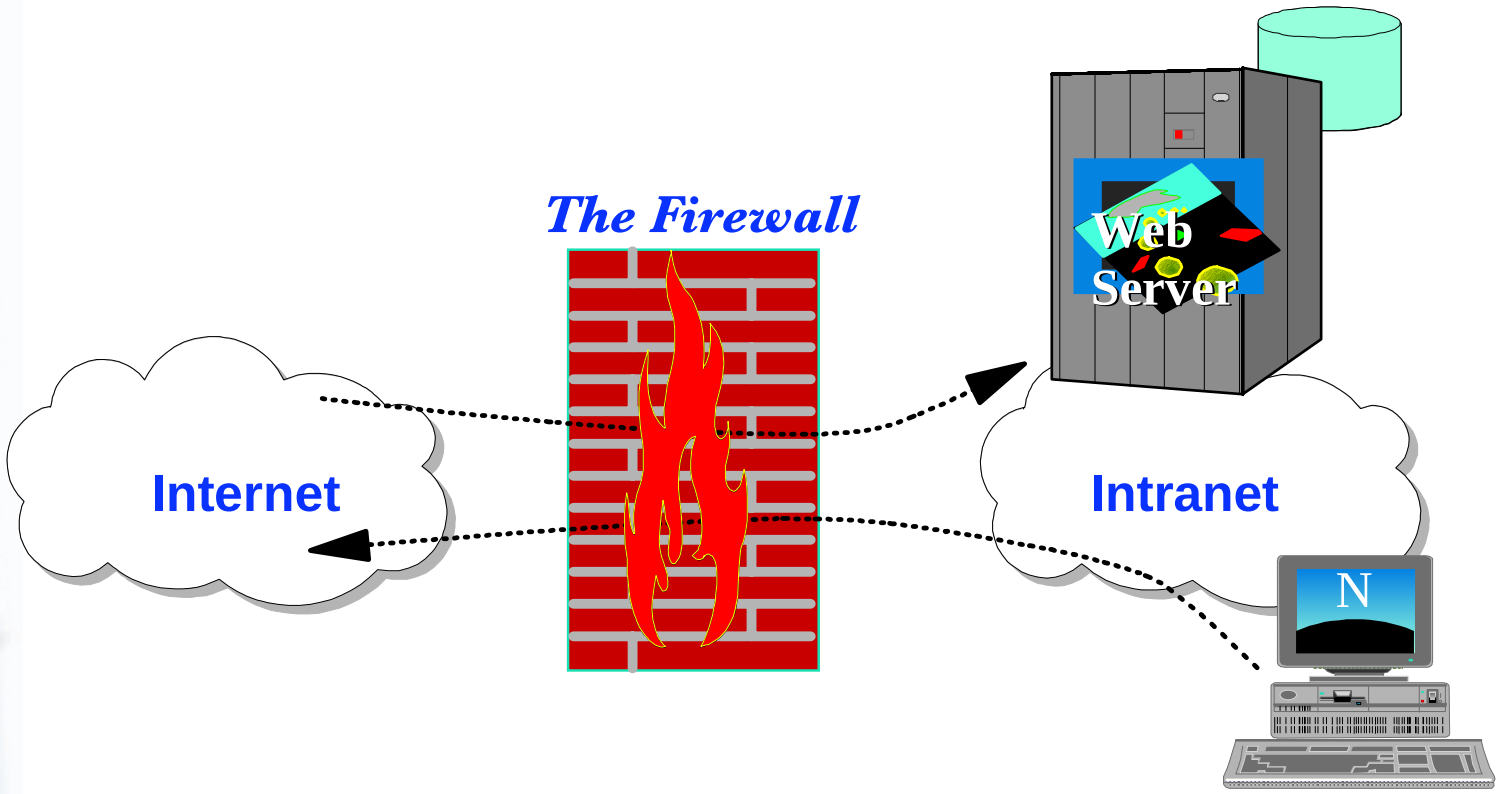
Session Objectives

- Provide an overview of Firewall Technologies shipped on OS/390
  - **Partially shipped in the Security Server**
  - **Partially shipped in the Communication Server**
- Identify how these technologies might be used
- Identify which technologies are shipped where
- Provide an release by release overview of Firewall content
- Provide insight into the future direction of Firewall Technologies on OS/390

Session Objectives

- Provide an overview of Firewall Technologies shipped on OS/390
  - **Partially shipped in the Security Server**
  - **Partially shipped in the Communication Server**
- Identify how these technologies might be used
- Identify which technologies are shipped where
- Provide an release by release overview of Firewall content
- Provide insight into the future direction of Firewall Technologies on OS/390

What is a Firewall?



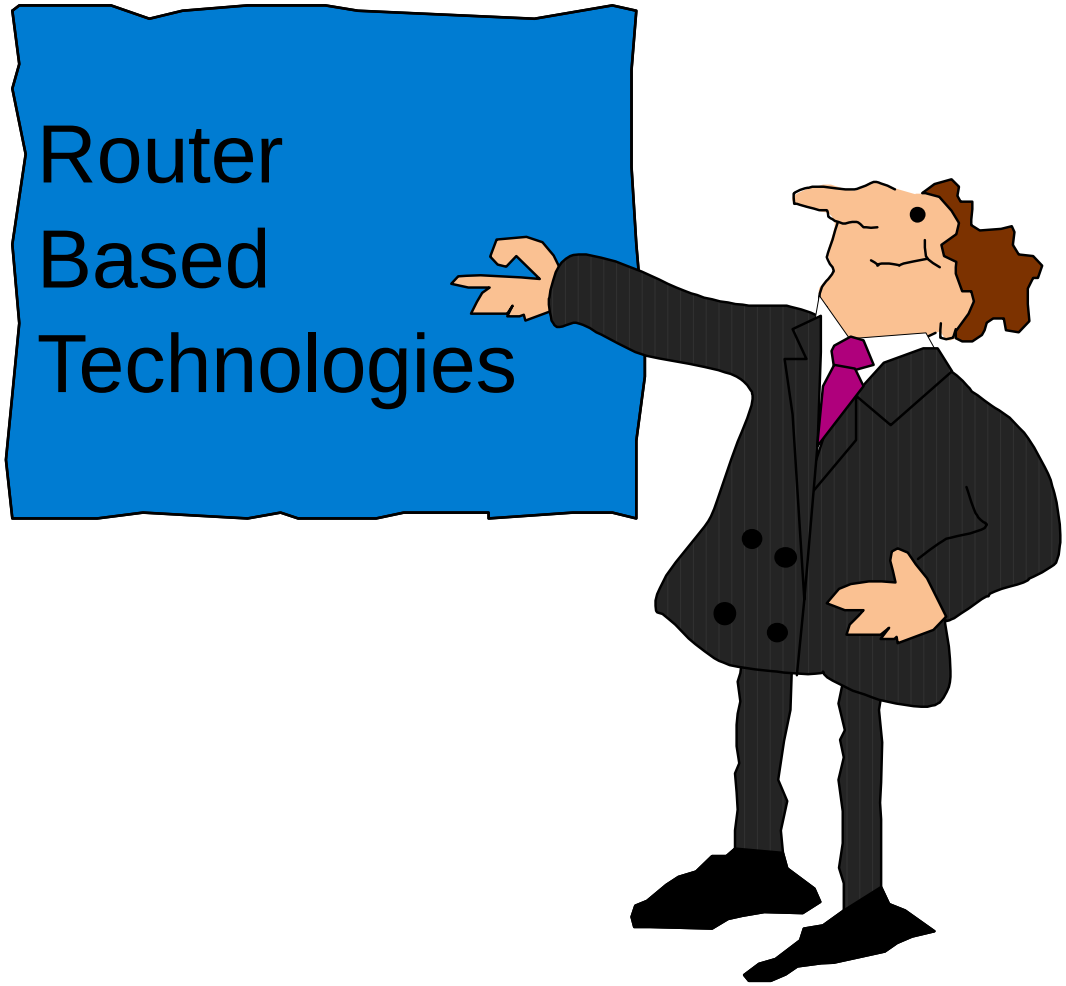
- A device used to separate a "safe" network from a "not-so-safe" network
- Allows selective access between the "safe" network and the "not-so-safe" network

Firewall Technologies

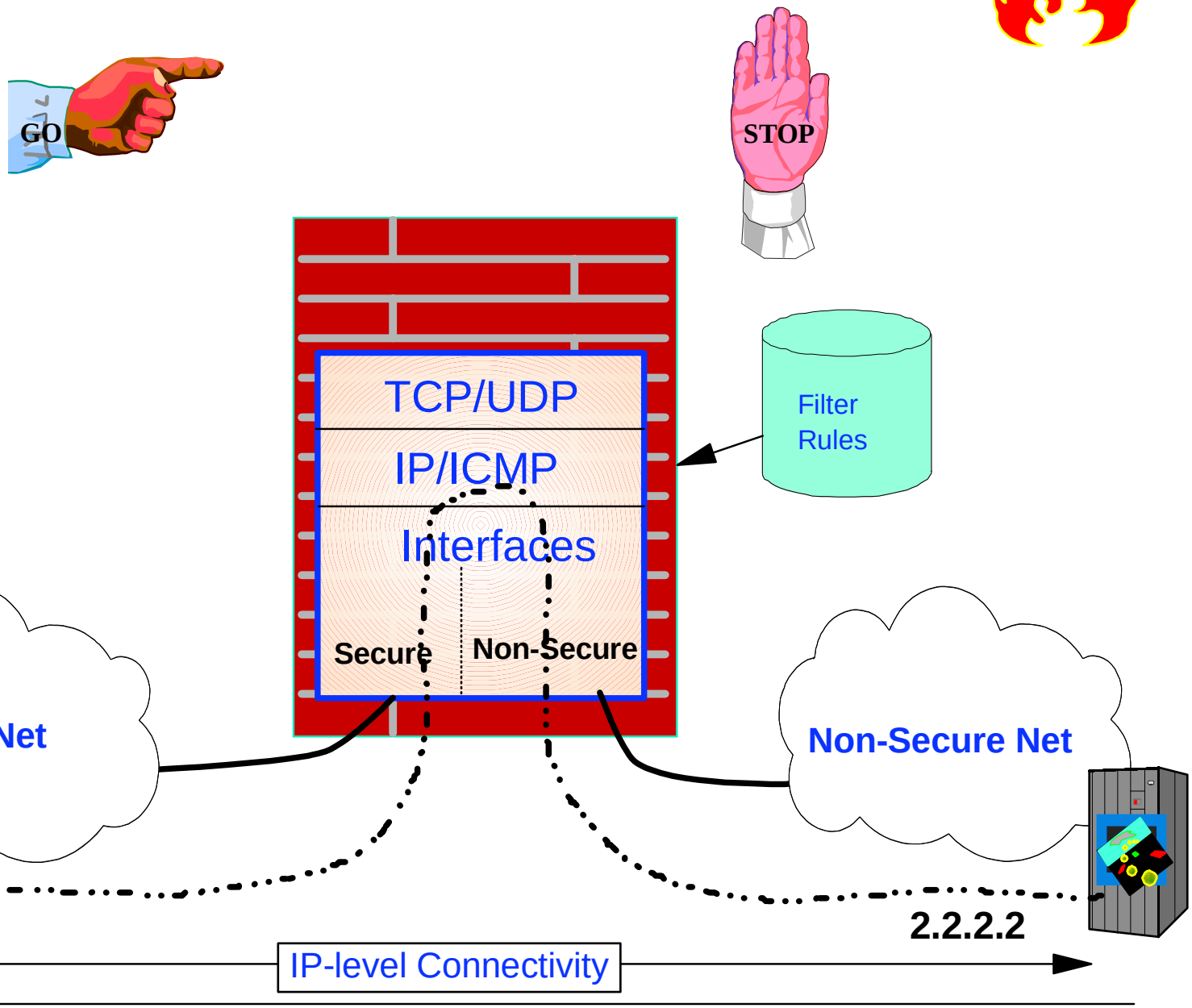
- Router Based
  - Gives the impression of a normal router
  - Analyzes packets to decide if it is allowed to be routed through the firewall
    - Also called a screening filter or a packet filter
  - May provide other functions such as address translation or IPSec
- Gateway Based
  - Designed to prevent the routing of IP traffic between the secure and non-secure network
  - Specialized - handles specific traffic
  - Communicates with both the secure and non-secure network
  - Two types
    - Application Level Gateway
    - Circuit Level Gateway
  - Also called bastion host

OS/390 Firewall Technologies

- Access Related
  - Router Based
    - IP Packet Filter
    - Real Audio Support
    - Network Address Translation (NAT)
    - Virtual Private Networks (VPN)
  - Gateway Based
    - FTP (Application Gateway) Proxy
    - SOCKS (Circuit Gateway) Server
- Management Related
  - Logs and Reports
  - Monitor and Detect
  - Administration GUI



IP Packet Filtering



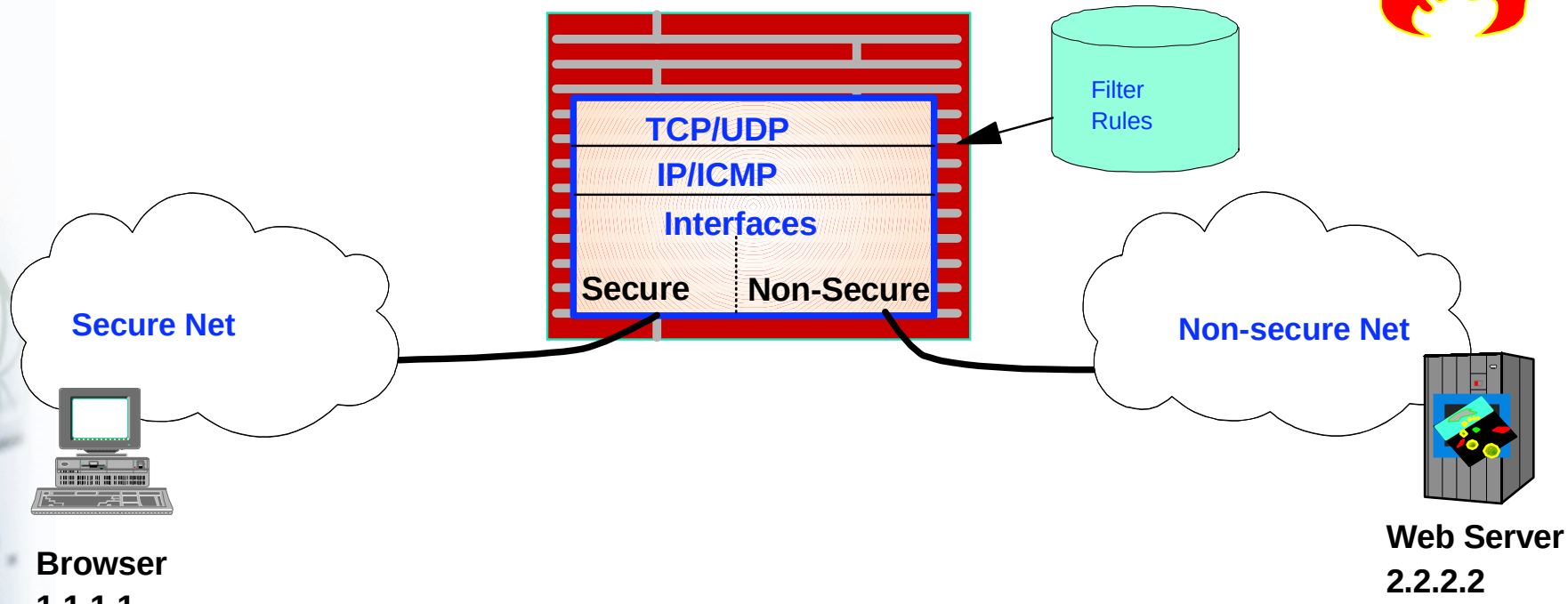
IP Packet Filter Selector Values

- Source:
  - IP Address
  - Port
- Destination:
  - IP Address
  - Port
- Protocol
- Interface
  - Secure/Non-secure/Both
- Direction:
  - Inbound/Outbound/Both
- Routing:
  - Local/Route/Both

Logical IP Packet Filter Actions

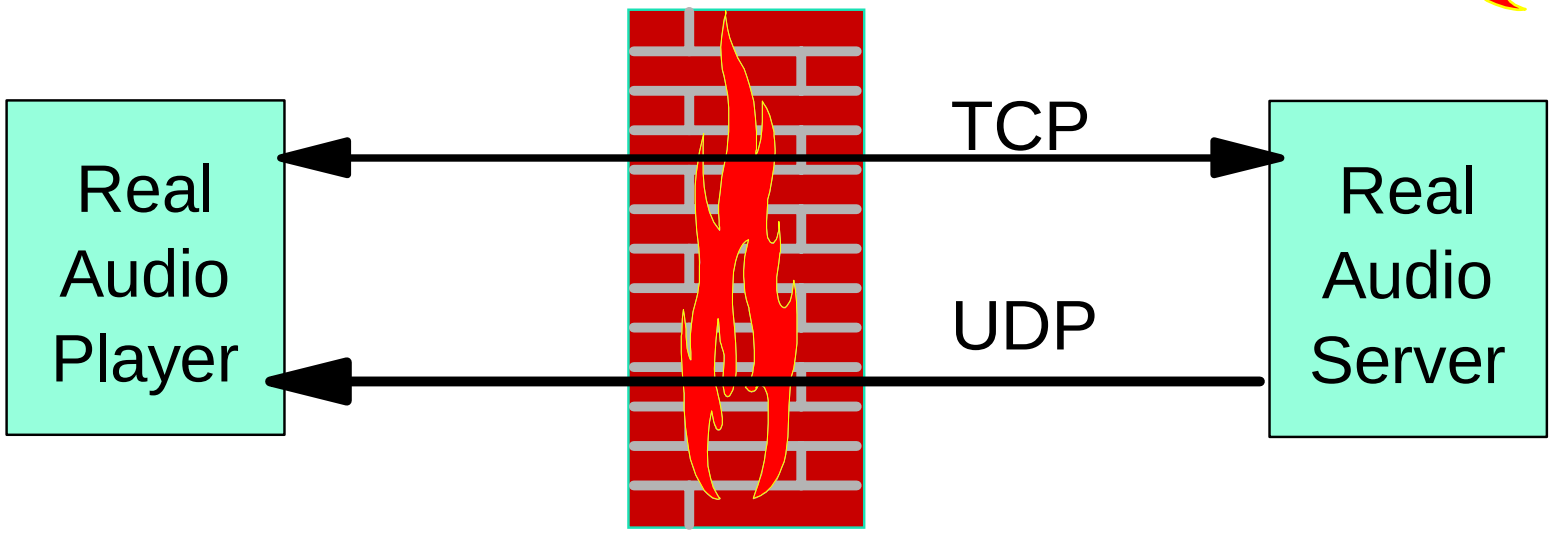
- Deny
- Permit
- Permit with IPSec
  - Implied for manual VPNs
  - Configured as action "Anchor" for dynamic VPNs

Web Server Example



Source IP	Source Port	Destination IP	Destination Port	Protocol	Direction	Interface	Routing
1.1.1.1	> 1023	2.2.2.2	80	TCP	Inbound	Secure	Route
1.1.1.1	> 1023	2.2.2.2	80	TCP	Outbound	Non-Secure	Route
2.2.2.2	80	1.1.1.1	> 1023	TCP/ACK	Inbound	Non-Secure	Route
2.2..2.2	80	1.1.1.1	> 1023	TCP/ACK	Outbound	Secure	Route

Real Audio Support

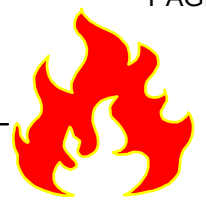


- Real Audio Protocol was developed by Progressive Networks
  - Uses a TCP connection between player and server
  - Optionally, server can establish a UDP channel back to the player
- OS/390 FW monitors Real Audio TCP connections
  - Dynamically manages the filter rule for UDP channel
- Still need to define filter rules for TCP connection

Network Address Translation

- Translates one IP address into another
- Allows internal IP addresses to be hidden from the non-secure network
- May wish to do this because of:
  - Security reasons
  - Using non-registered IP addresses
- Only applies to UPD and TCP traffic
  - Does not apply to ICMP
- NAT Configuration Keywords
  - RESERVE
  - TRANSLATE
  - EXCLUDE
  - MAP
- Outbound Traffic is filtered first, then NAT is applied
- Inbound Traffic applies NAT first, then filters

Network Address Translation (Continued)



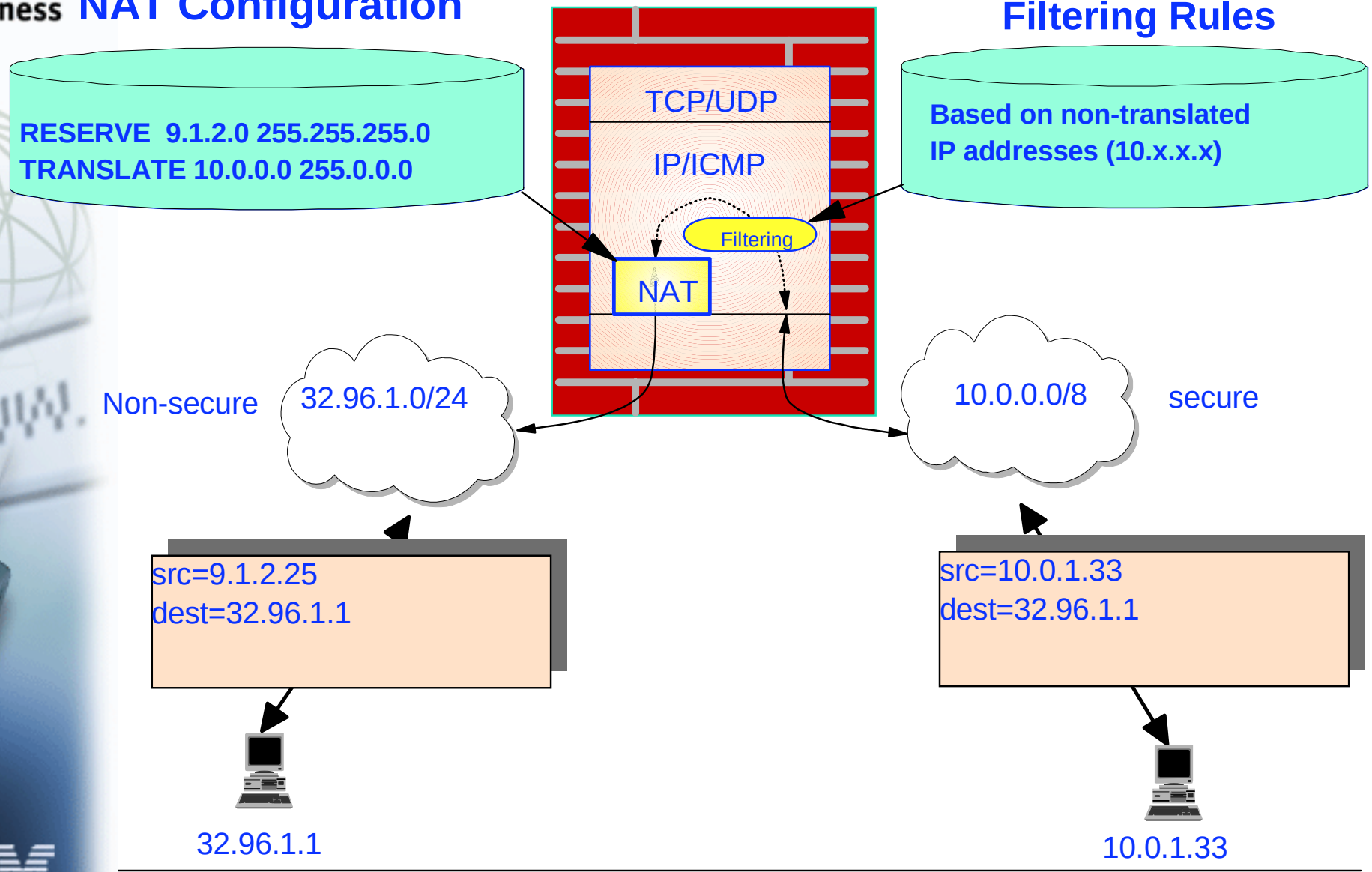
business

NAT Configuration

RESERVE 9.1.2.0 255.255.255.0
TRANSLATE 10.0.0.0 255.0.0.0

Filtering Rules

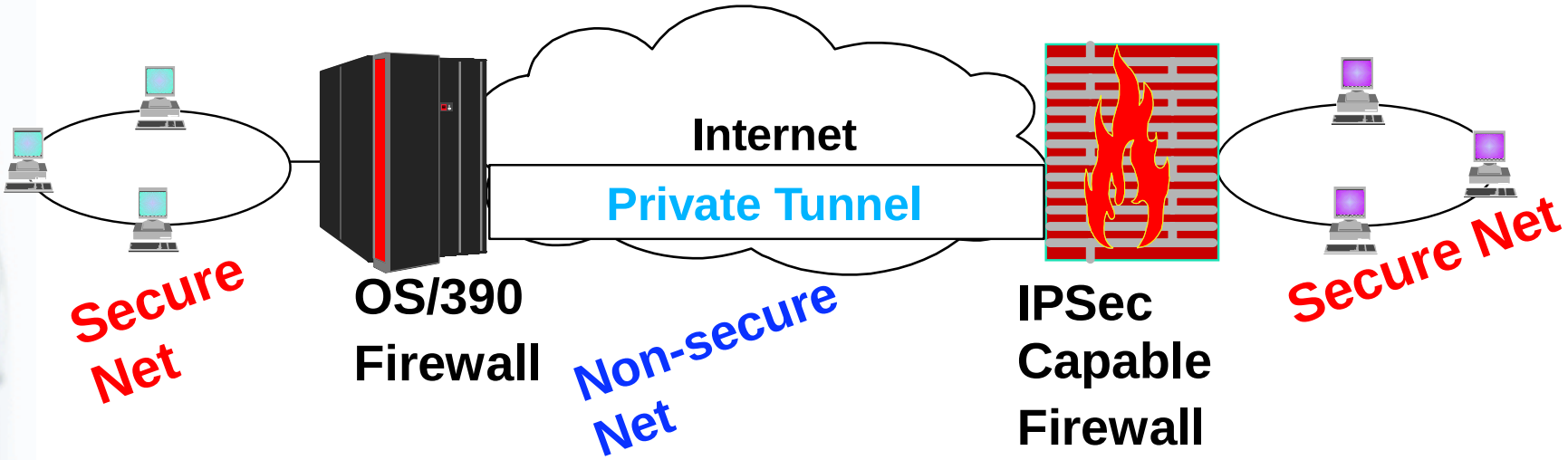
Based on non-translated IP addresses (10.x.x.x)



What is a VPN?

- A VPN is a:
  - **Virtual Private Network**
    - **Network**
      - **Two or more devices communicating with each other**
    - **Private**
      - **Confined to the members of the network**
    - **Virtual**
      - **Not really a private network, but has the essence of a private network**
- Something that provides security when two or more secure networks communicate across an unsecure network

Virtual Private Network Example



- Standard IPSec protocol
- Uses S/390 hardware CMOS Cryptographic Coprocessor
- VPNs do not have to be Firewall to Firewall
- OS/390 can act as a host in a VPN

VPNs on OS/390

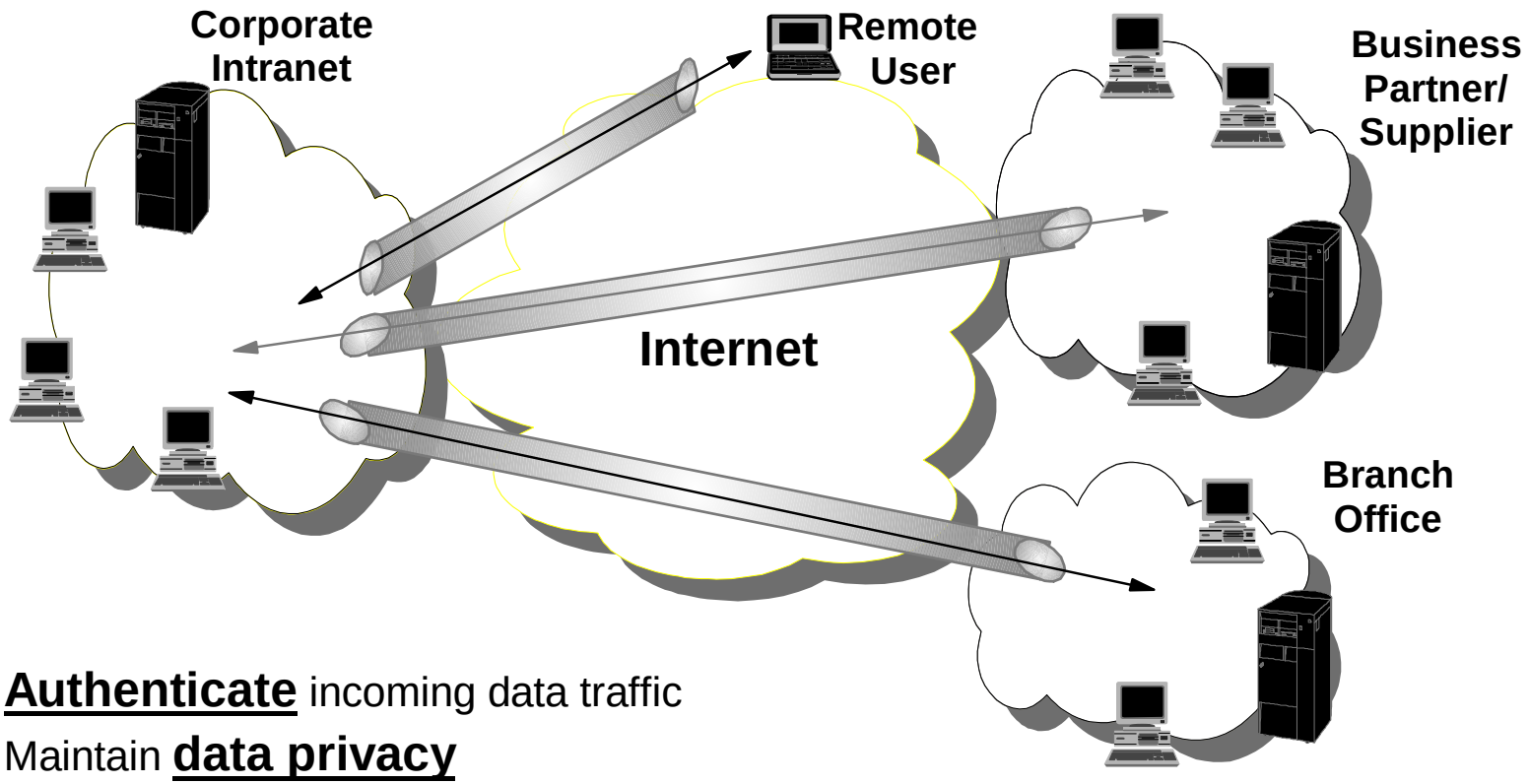
- Based on standards being defined in the Internet Engineering Task Force (IETF)
  - Standards to Protect data
    - AH Protocol
    - ESP Protocol
  - Standards to dynamically create keying material
    - ISAKMP
    - IKE
- Characteristics:
  - Data integrity (AH and ESP)
  - Authentication of data source (AH and ESP)
  - Privacy (ESP only)
  - Replay Protection (AH and ESP)

Types of VPNs on OS/390

- Manual VPNs
  - VPNs whose attributes and encryption keys must be managed by administrative procedures
  - First available via a kit in R4
- Dynamic VPNs
  - VPNs whose attributes and encryption keys are managed by the IKE protocol
  - First available in R8
  - Over the long run dynamic VPNs are easier to manage than manual VPNs, but initially dynamic VPNs have a steeper learning curve than manual VPNs

Customer's use of VPNs

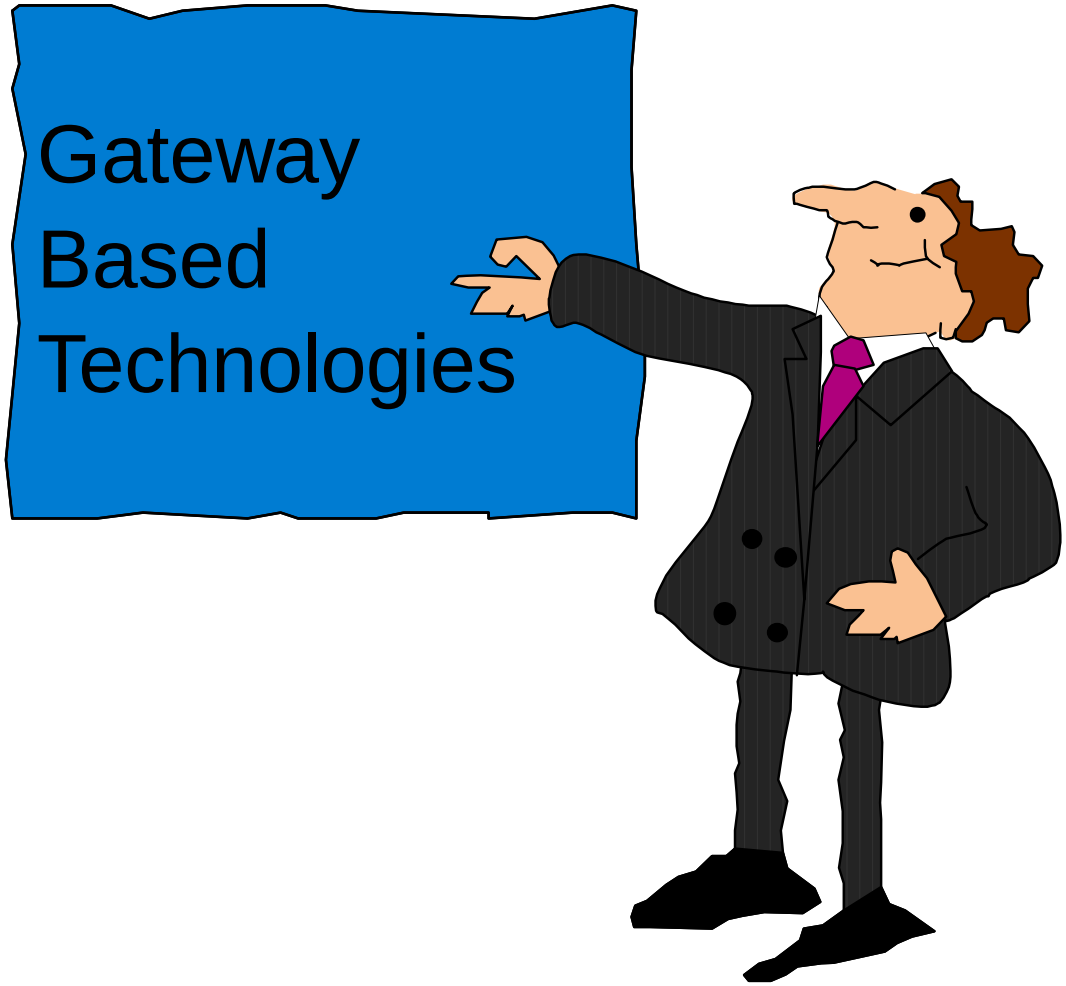
Secure extension of your company's private Intranet across a public network



Authenticate incoming data traffic

Maintain **data privacy**

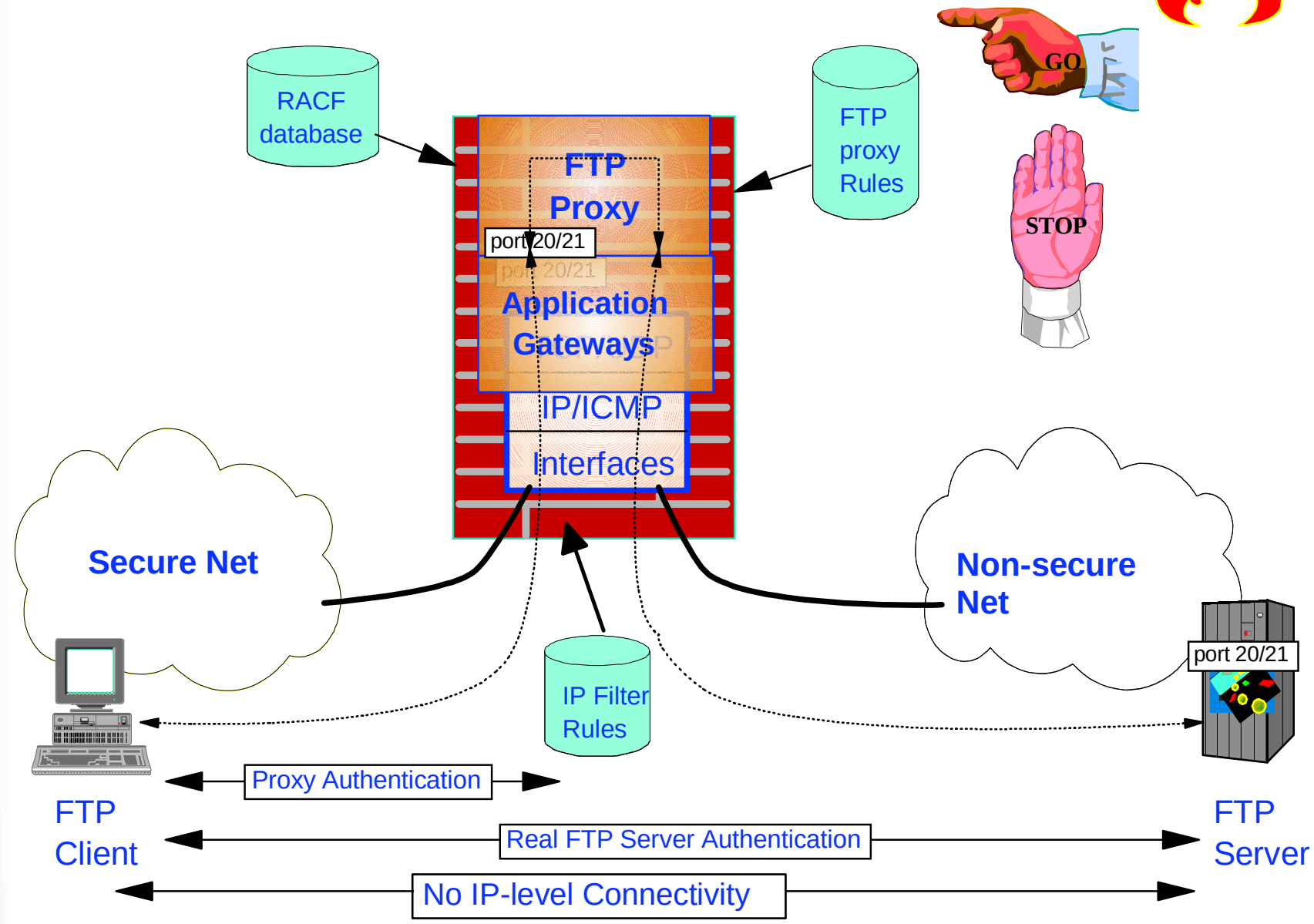
Manage access as with private network



FTP Proxy Server

- Used to issue ftp commands on behalf of another
- Application specific
  - Only addresses FTP
- Does not require a special ftp client
  - ftp client authenticates to the FTP Proxy Server
  - ftp client issues the "site" command to reach the desired FTP server
  - ftp client issues normal FTP commands
- IP Connection broken at FTP Proxy Server
  - FTP Server only knows about the FTP Proxy Server
  - Minimizes "holes" in firewall
- Clients can be on either the secure or non-secure network
  - Warning: user id and password to the proxy server flows in the clear

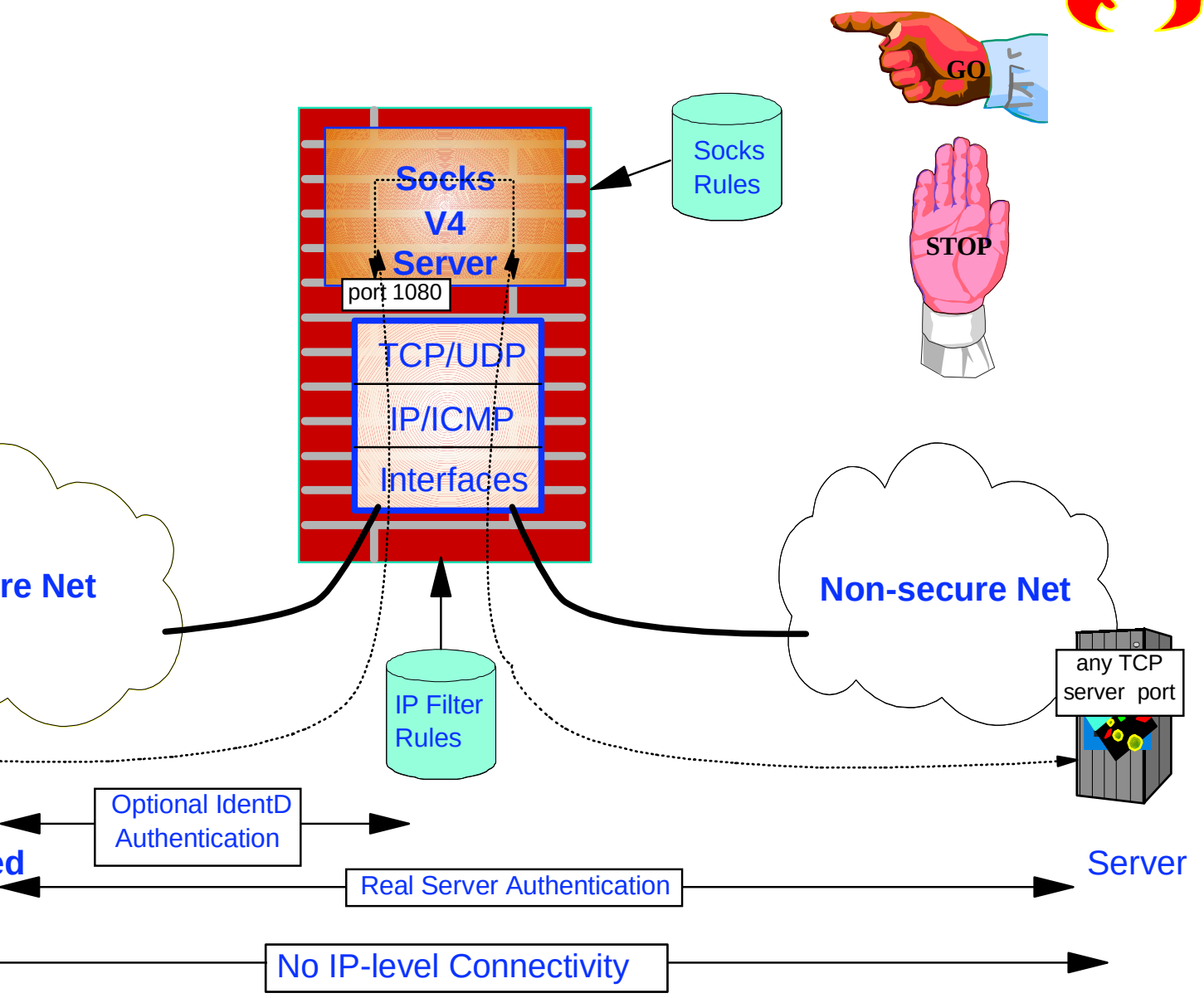
FTP Proxy Server (Continued)

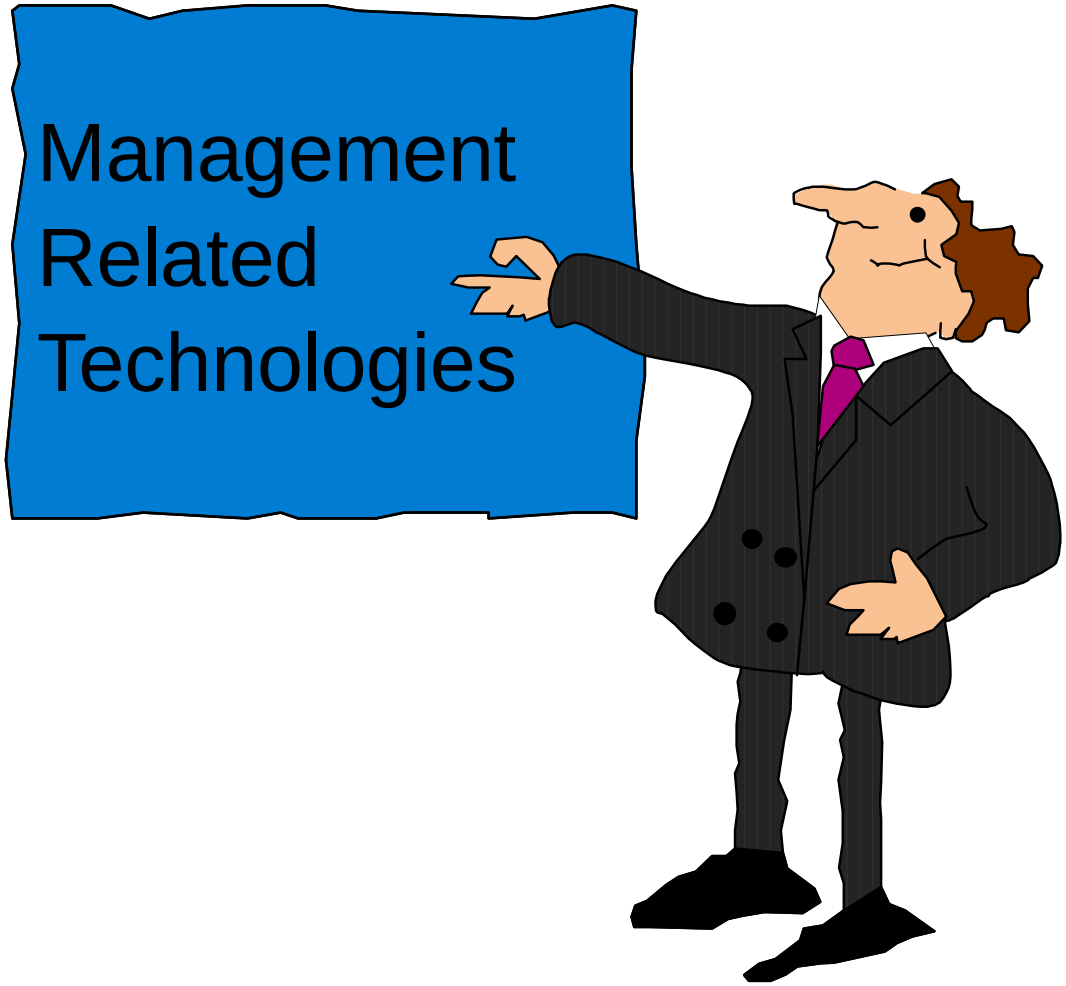


Socks Server

- Based on SOCKS V4
- Used to forward TCP packets on behalf of another
- Works with all TCP based applications
  - No changes required to application server
  - Requires clients to become "sockified"
    - Stack level
    - Application level
- IP Connection broken at SOCKS Server
  - Application server only knows about the SOCKS Server's IP address
  - Minimizes "holes" in firewall
- Application server authenticates client, not socks server
- Clients can be on the secure or non-secure network
- Optional IdentD client authentication at SOCKS Server

Socks Server (Continued)





Logging & Reporting

- Enhanced SYSLOG Daemon
- Logs Firewall events to either:
  - HFS log files
    - Archiving support
    - Log formatting support
  - SMF records (TYPE 109)
  - A SYSLOG Daemon on another host
  - A user id

Monitor and Detect

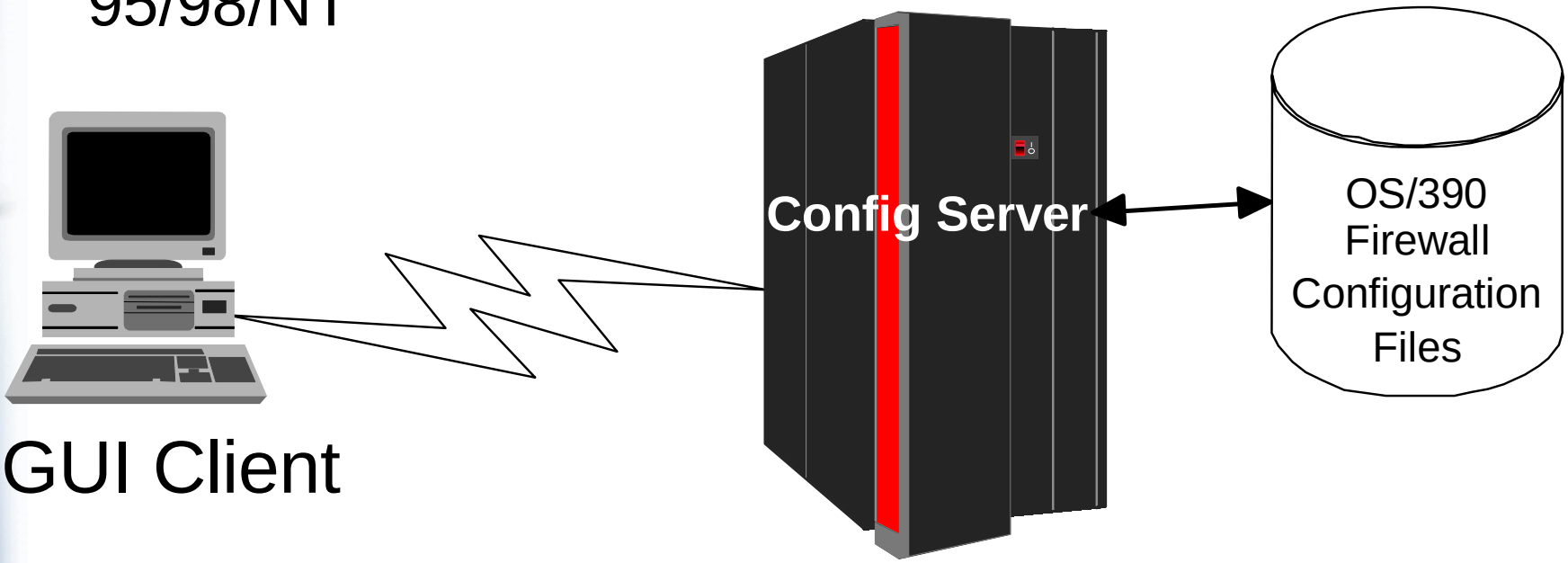
- Logging can be directed to the system log
- System log can be scanned by Netview and Alerts can then be generated based upon thresholds set by customer !
- This does not come out of the box !
- Customer has to do that himself !

Administration & Configuration

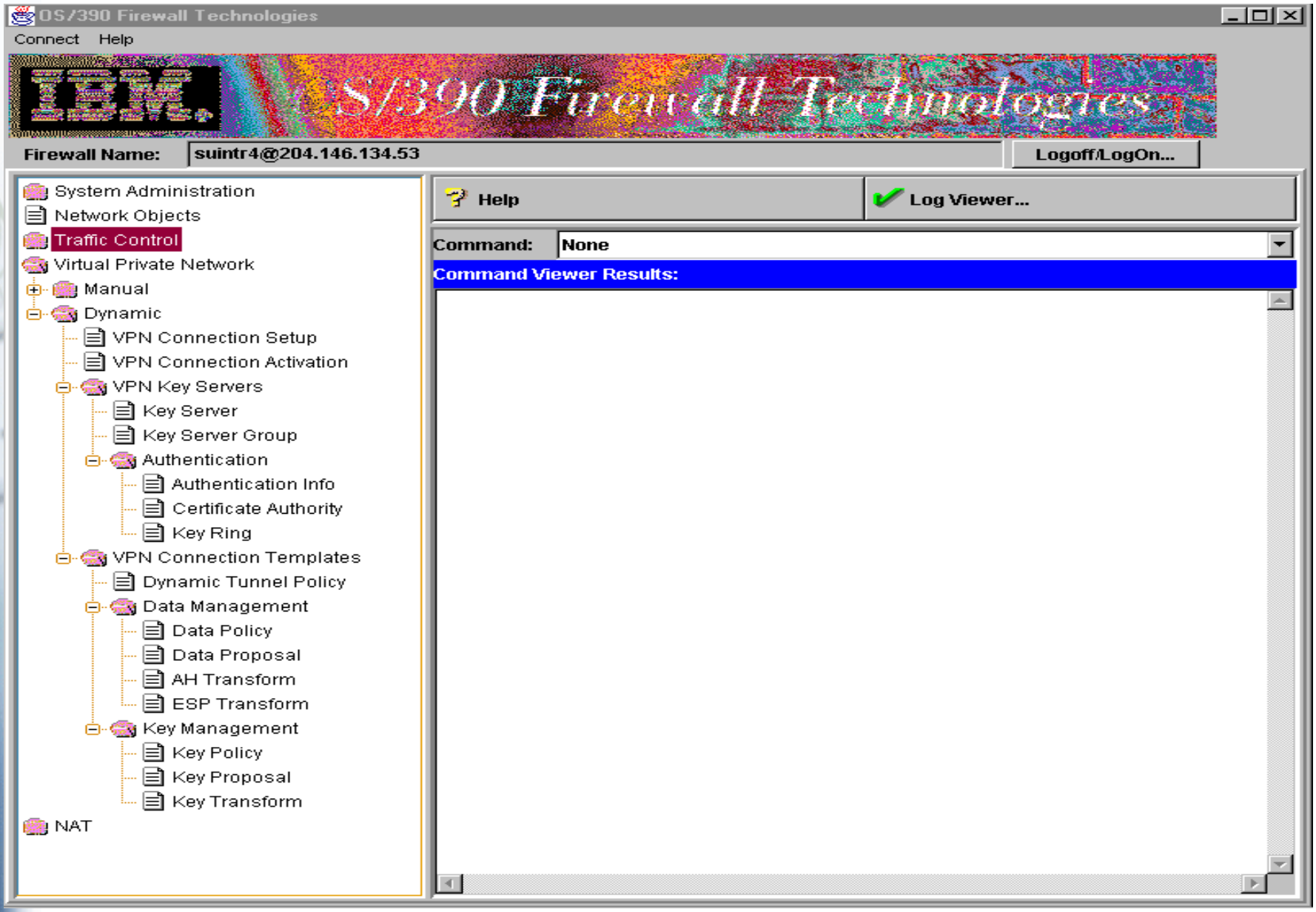
- Command line interface
  - Through the UNIX System Services
- GUI Interface and Firewall Configuration Sever
- Firewall configuration files comes with predefined objects
- Migrate utility to assist in the move from any release to the current release

Configuration Server and GUI

- GUI
  - Introduced in R7
  - JAVA Based
  - Supported on AIX and Windows 95/98/NT
- Config Server
  - Runs on OS/390
  - Controlled by fwkern
  - Issues commands on behalf of the GUI



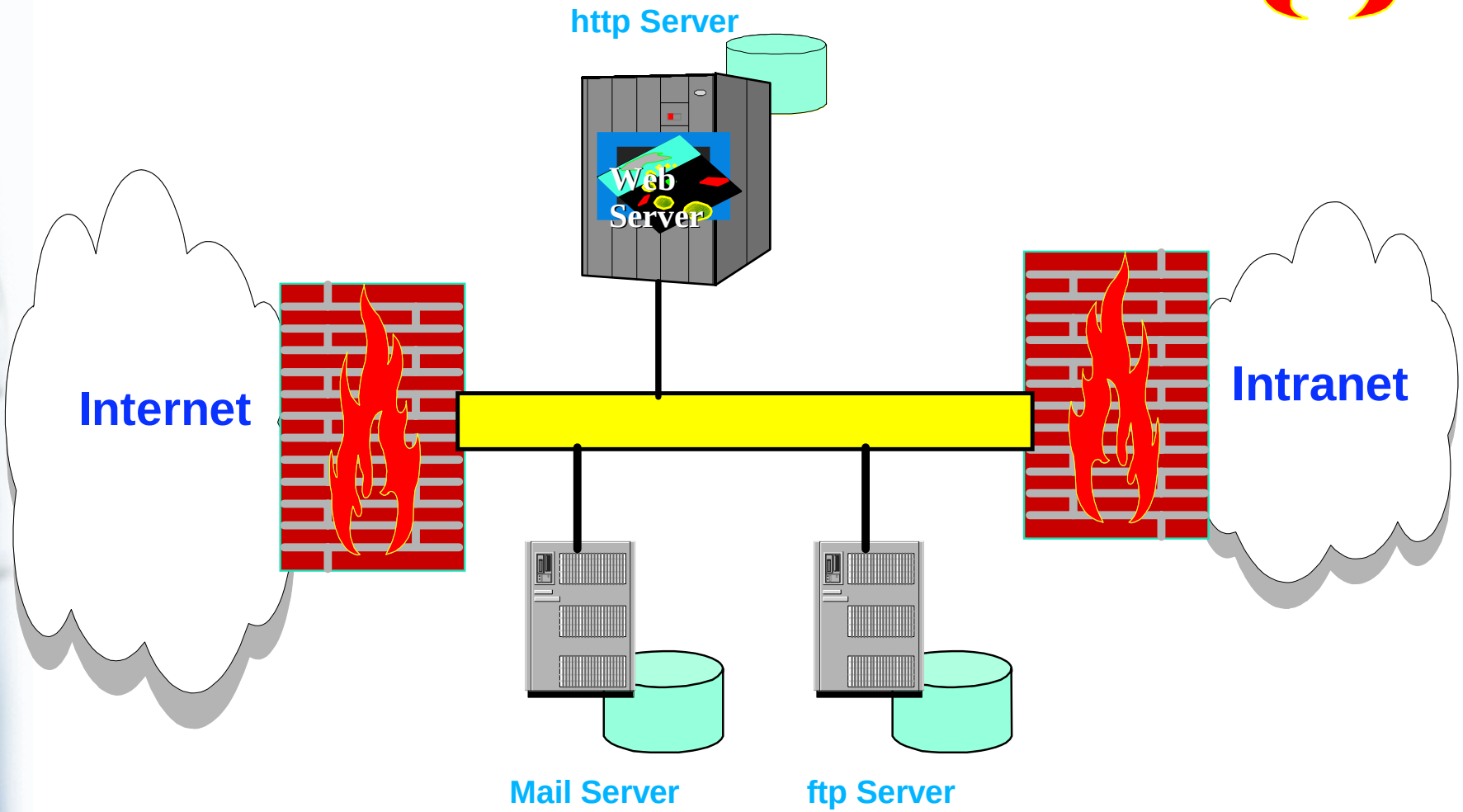
JAVA GUI



Session Objectives

- Provide an overview of Firewall Technologies shipped on OS/390
  - Partially shipped in the Security Server
  - Partially shipped in the Communication Server
- Identify how these technologies might be used
- Identify which technologies are shipped where
- Provide an release by release overview of Firewall content
- Provide insight into the future direction of Firewall Technologies on OS/390

Demilitarized Zone (DMZ)

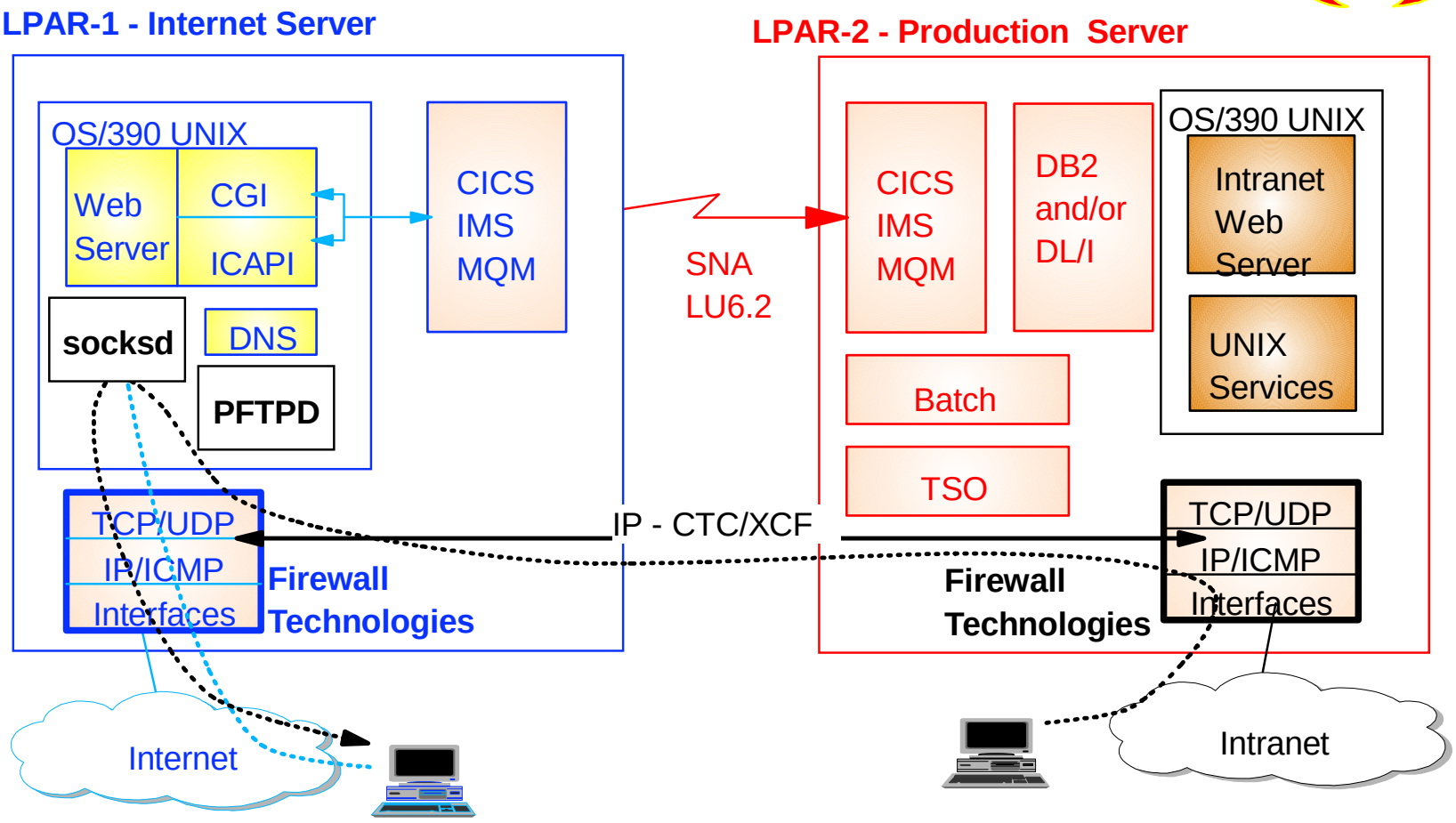


- A network between a secure and an unsecure network
- Logical an extension of the secure network
- Used to fence off access to the secure network

OS/390's Role

- The OS/390 Firewall Technologies could be used as:
  - **The firewall between the Internet and the DMZ**
  - **The firewall between the Intranet and the DMZ**
  - **A technology to harden a server within the DMZ**
  - **A technology to harden a server within the Intranet**
- To date, there has been some interest in using OS/390 as the firewall to the Internet
- The perceived value of the Firewall Technologies on OS/390 is:
  - **Its ability to harden servers running in the DMZ**
  - **Its ability to serve as the firewall between the DMZ and the Intranet**

Sample Scenario Options



Option 1: Web Server connected to Internet

Option 2: Option 1 plus non-IP interactions with backend systems

Option 3: Option 2 plus internal access to Internet

VPN Usage on OS/390

- To secure IP based applications that can't take advantage of SSL (i.e. UPD) or have yet to be SSL-ized
  - To date, the biggest interest in VPNs on OS/390 has been to perform "secure" ftp transfers
  - Both Internet and Intranet scenarios
- Business to business (B2B) environments where host to host security is deemed critical
  - Business Partner Scenarios
  - Medical Records
  - Financial Information
  - Human Resource Information
- Remote user access

Session Objectives

- Provide an overview of Firewall Technologies shipped on OS/390
  - Partially shipped in the Security Server
  - Partially shipped in the Communication Server
- Identify how these technologies might be used
- Identify which technologies are shipped where
- Provide an release by release overview of Firewall content
- Provide insight into the future direction of Firewall Technologies on OS/390

Software Requirements

OS/390 Version 2 Release 4

- OS/390 V2R4 eNetwork Communication Server IP, with the DNS w/WLM KIT SK2T-6136
- OS/390 Security Server
- OS/390 Firewall Technology Toolkit (no longer available)

OS/390 Version 2 Release 5 and Beyond

- Firewall Technology integrated into :
  - OS/390 Security Server
  - OS/390 eNetwork Communication Server

OS/390 Firewall Technology Delivery

OS/390 Security Server

- FTP proxy server, Socks server
- Enhanced Syslog daemon
- Configuration Server (as of V2R7)
- Configuration GUI
- IKE daemon
- Administration/configuration commands

OS/390 eNetwork Communication Server

- IP filters
- IPsec (tunnels, VPN)
- Network Address Translation (NAT)

But I Don't Have a Security Server License!

- Can't use:
  - FTP proxy server, Socks server
  - Enhanced Syslog daemon
  - Configuration Server (as of V2R7)
  - Configuration GUI
  - IKE daemon
- Can use:
  - Administration/configuration commands
    - Although shipped with the Security Server, the commands can be installed and used without a license
  - IP filters
  - IPsec (tunnels, VPN)
    - Manual mode only
  - Network Address Translation (NAT)

Session Objectives

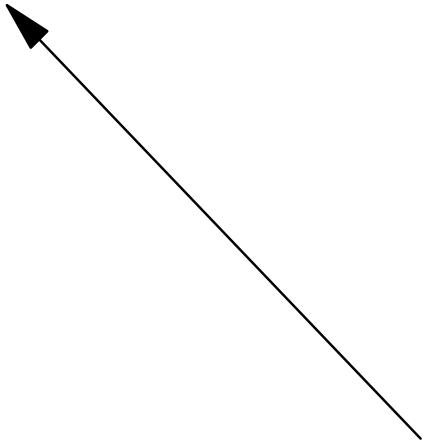
- Provide an overview of Firewall Technologies shipped on OS/390
  - Partially shipped in the Security Server
  - Partially shipped in the Communication Server
- Identify how these technologies might be used
- Identify which technologies are shipped where
- Provide an release by release overview of Firewall content
- Provide insight into the future direction of Firewall Technologies on OS/390

Support in R5 (also in R4 Kit)

- FTP Proxy
- Socks V4 Server
- Network Address Translation
- IP Packet Filtering
- Real Audio Support
- Manual VPN Support
  - Support for RFCs 1825-1829
- Firewall Syslog Server (syslogd)
- Command Line Configuration

Support Introduced in R6

- Manual VPN
  - Added support for transport mode



OS/390 can act as a VPN Host, not just a VPN Firewall!!!!

Support Introduced in R7

- Manual VPN
  - ►Support for RFCs 2401-2406 and 2410
- Configuration Server
- Configuration GUI
- Multiple Stack Support
  - ►Introduced fwstackd server
- Server Scalability

►Command Line and GUI configuration

Support Introduced in R8

- Dynamic VPN Support:
  - Support for RFCs 2401-2406 and 2410
  - Support for RFCs 2407-2409

- **No new Firewall support was introduced in R9!**

Session Objectives

- Provide an overview of Firewall Technologies shipped on OS/390
  - Partially shipped in the Security Server
  - Partially shipped in the Communication Server
- Identify how these technologies might be used
- Identify which technologies are shipped where
- Provide an release by release overview of Firewall content
- Provide insight into the future direction of Firewall Technologies on OS/390

Future Direction

- Emphasis will be on VPN enhancements rather than traditional firewall features
- Potential enhancements
  - Support to maintain currency with the IPSec RFCs
  - Ease of VPN activation
  - Ease of VPN configuration
  - Support to quickly relocate VPNs in case of a system outage
  - Support for centralized management of VPN Policy
- If you have suggestions, let me know!

Where to Find More Information

- The OS/390 Firewall Technologies Resource Web page
  - http://www.s390.ibm.com/products/mvs/firewall/resources.html
    - See our OS/390 FIREWALL TECHNOLOGIES GUIDE AND REFERENCE
      - R4, R5, R6, R7, and R8 versions available
        - html format
        - pdf format
    - See the following Freelance presentations:
      - OS/390 CONFIGURING VPNS ON OS/390
      - GETTING STARTED: IPSEC WITH CS FOR OS/390
        - Concentrates on actual configuration
      - GETTING STARTED: IPSEC WITH CS FOR OS/390 (Boston)
        - Concentrates on gathering information for configuration
      - FIREWALL OVERVIEW AND DIRECTIONS
        - This presentation
      - GETTING STARTED USING THE FIREWALL

Questions

???????