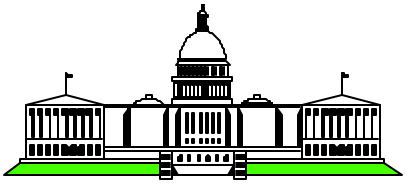
OS/390 Firewall Technology Overview



Mary Sweat
E - Mail: sweatm@us.ibm.com

Washington System Center

Agenda

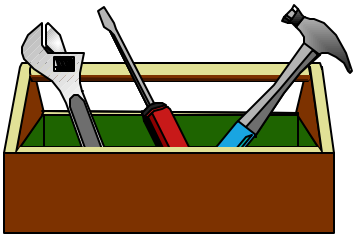
WSC
Advanced Technical Support

- OS/390 Firewall
  - OS/390 Firewall Features
  - Hardware requirements
  - Software requirements
- Firewall Examples

OS/390 Firewall Technologies Tools

WSC Advanced Technical Support

- Included with the OS/390 Security Server
  - Configuration Client (GUI)
  - Configuration Commands
  - Proxy FTP server
  - Socks Server
  - Real Audio Support
  - Internet Security Association Key Management Protocol (ISAKMP) Server



- Included with the eNetwork Communications Server for OS/390
  - Network Address Translation (NAT)
  - IP Filters
  - IP Tunnels (IPSec or Virtual Private Network)

- OS/390 Firewall Technologies is not a separate product. It is part of the OS/390 Security Server and eNetwork Communications Server for OS/390.

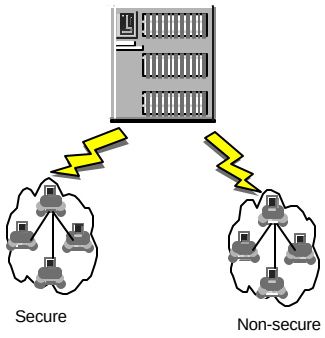
- If the Security Server has not been purchased the Configuration Commands can still be used because the Security Server code is shipped with the base OS/390 and the usage of Configuration Commands do not check to see if there is a license for the Security Server.

- The Socks server, FTP proxy and ISAKMP server that come with OS/390 Firewall Technologies can **only** be used if the customer has purchased the Security Server. Firewall checks and ensures a Security Server license exist before it allows the installation to utilize these features.

Firewall Hardware Requirements

WSC Advanced Technical Support

- Any communication hardware interface supported by the TCP/IP protocol stack to make the network connections
  - OSA, 3172, CTC, XCF, etc.
- At least two network interfaces;
  - one network interface connects the secure, internal network that the firewall protects
  - the other network interface connects to the nonsecure, outside network or internet
- Crypto Coprocessor
  - this is optional requirement as the OS/390 firewall can use software encryption (RSA BSAFE)
  - used with Integrated Cryptographic Service Facility (ICSF)



- By default all adapters defined are considered "non-secure" until the firewall administrator defines selected adapters as secure. You can have numerous adapters (max. 256) but you must have a minimum of 2 if you use the interfaces on both sides of the firewall.

- The OS/390 Firewall Technology can utilize the hardware crypto features on your CMOS machines. To exploit the hardware crypto functions, the TCP/IP Firewall stack needs to be authorized for the ICSF services via RACF class **CSFSERV**. ICSF services that can be exploited are;
  - clear key import callable service
  - decipher callable service
  - encipher callable service
  - random number generate callable services

Software Requirements

- OS/390 Security Server (RACF)
- OS/390 eNetwork Communications Server
- OS/390 Unix services (OpenEdition)
- OS/390 C/C++ Collection Cl. Lib.
- OS/390 System Secure Socket Layer (System SSL)
- Open Cryptographic Services Facility (OCSF)
- Security Server Open Cryptographic Enhanced Plug-ins (OCEP)

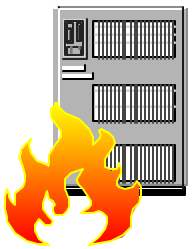
- System Secure Sockets Layer is required for the usage of the OS/390 Firewall GUI.
- OCSF and OCEP is required if dynamic tunnels are used.

Graphical User Interface

WSC Advanced Technical Support

GUI Client

SSL



Configuration Server (OS/390)

- Written in JAVA
- Installs / runs on Windows 95/NT & AIX
  - AIX
    - Java 1.1.4 or higher
    - AIX 4.2 or higher
    - Netscape 3.0.1
  - Windows 95 or Windows NT
    - web browser with Java and frames support
    - zip tool that handles long file names

- The GUI was available in 2.7, previous versions of S/390 Firewall only had a command line interface for configuring the firewall.

- SSL encrypts data flowing between GUI and Configuration Server. If SSL is not setup the GUI will not work.

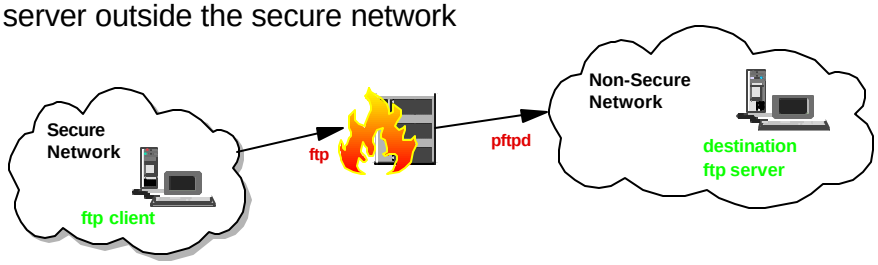
- Authorization to use and configure the firewall is checked via External Security Manager (eg. RACF). Must have explicit authorization to the GUI RACF profile ICF.CFGSRV even if you are a superuser.

- Benefits;
  > Provides ease of use
  > Defaults filled in
  > On-line help
  > Error checking
  > Dialog messages
  > English / Japanese

FTP Proxy Support

WSC Advanced Technical Support

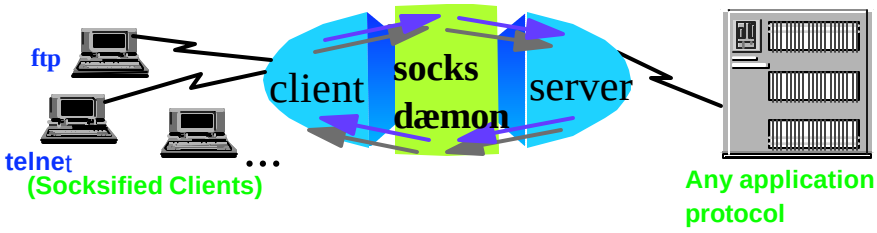
- OS/390 Firewall Technologies supply an FTP proxy server (**pftpd**)
  - access controlled on a user-by-user basis
    - to go out of the secure network
    - to come in from the non-secure world
  - local ***ftp*** commands disabled on the firewall
- Users **ftp** to the firewall and with valid authorizations, **pftpd** contacts FTP server outside the secure network



- File Transfer Protocol (FTP) is a TCP/IP service that transfers files from one network host to another.
- Once a connection is established, all commands the user enters, are forwarded to the remote host by the proxy. The proxy also returns all status messages for you.
- The proxy server makes the Internet connection, the Internet servers only see the Firewall IP address, thus hiding client address in the secure environment.
- Each proxy server is written for a specific application, in this case FTP.

Socks

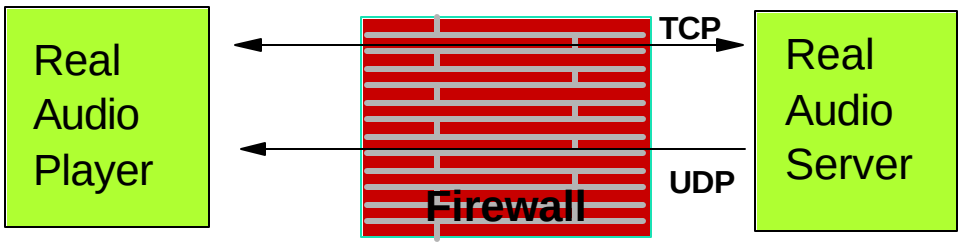
- A socks dæmon sits between the client and destination server
  - socks dæmon is generic
    - can handle traffic for multiple, different applications
- Socks replaces the IP address of the user with the address of the firewall



- Transparent to the user
- Uses rules to determine whether the request is authorized to pass to or from the protected network
- Client must be "socksified", meaning it is a Socks-aware client
  > client uses a socksified TCP application
  > socksified Socket library
- Authorization is rules-based, as opposed to a userid/password like the FTP proxy

Real Audio Support

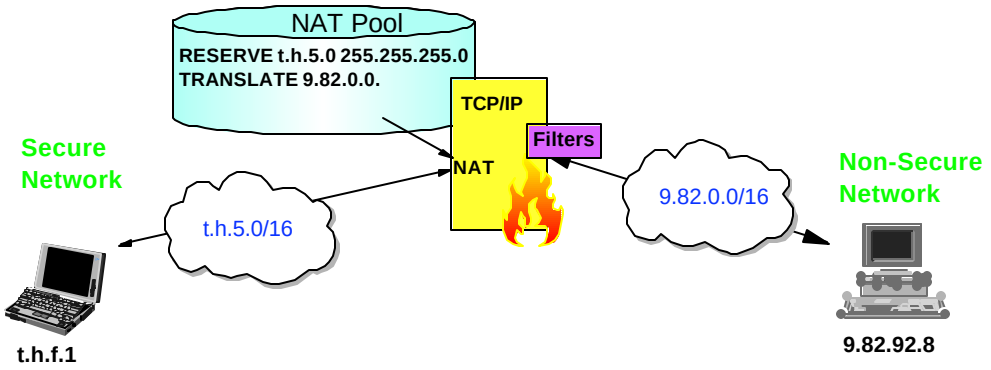
- Supports live and on-demand audio from the Internet
  - Special protocol developed by Progressive Networks
- OS/390 Firewall monitors and identifies RealAudio TCP connections
  - dynamic filter rule for a UDP packet is defined when a RealAudio connection is identified
  - rule is removed when the RealAudio TCP connection is closed



Network Address Translation (NAT)

WSC Advanced Technical Support

- Network Address Translation provides a translation from an internal (secure) IP address to an temporary external registered address



- Allows an installation to hide their internally-used IP addresses
  > to provide additional security
  > to externalize only registered IP addresses

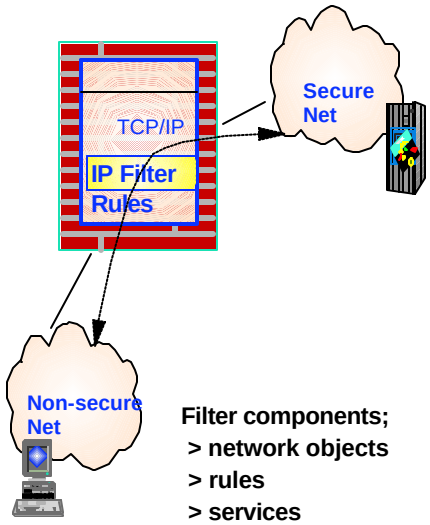
- NAT looks like a normal IP router that forwards IP packets between two network interfaces.

IP Filters

WSC Advanced Technical Support

- Basic control feature in firewalls
- Works at the IP layer of TCP/IP
- Determines what traffic is allowed to flow through
- Filters on;

-- source and destination IP address & mask
-- source and destination port
-- direction of the data flow
-- IP protocol
-- type of interface (secure or nonsecure)
-- date/time



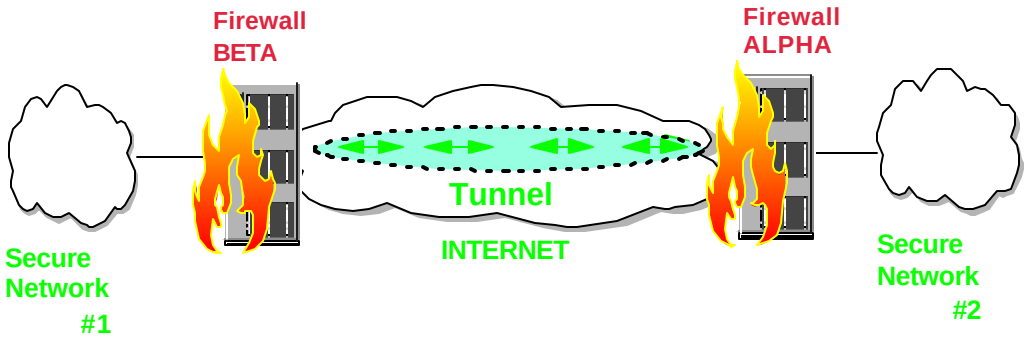
Filter components;
> network objects
> rules
> services
> connections

- Filter rules, or definitions specify what traffic is authorized to flow where, must be defined by the system administrator and activated
- TCP/IP is based on four layers and the IP layer equates to the Internetwork layer.

Virtual Private Networks

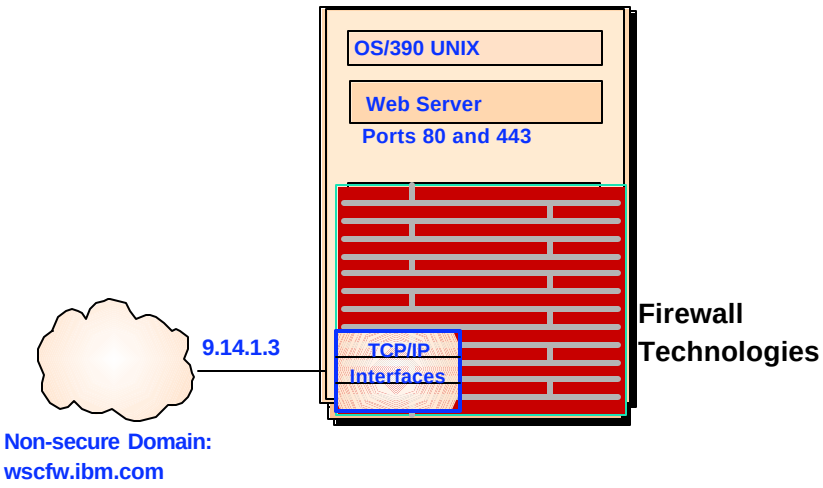
WSC Advanced Technical Support

- Virtual Private Networking (VPN) allows secure communications between remote sites over a public network like the internet
- Secures data traffic at the IP layer
  - secure traffic for all applications, without modifications to applications



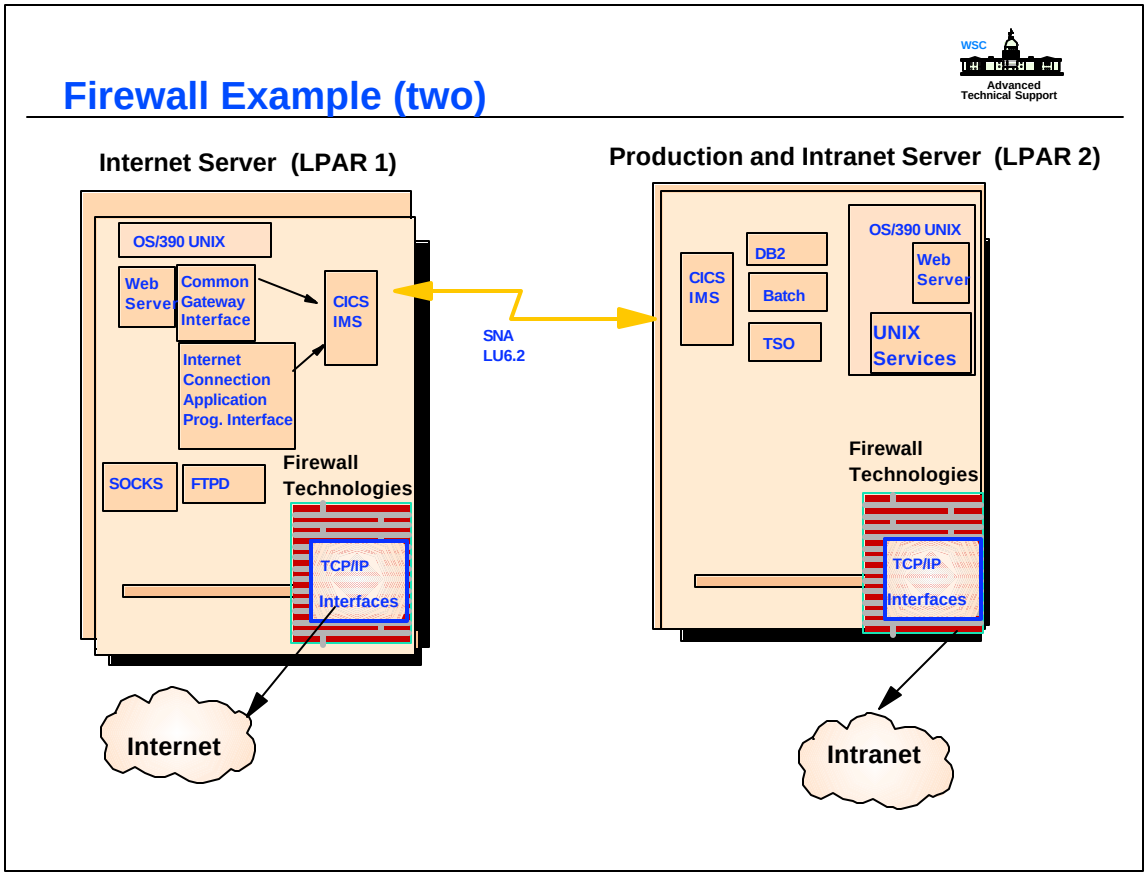
- Illustrated is a tunnel between two firewall hosts across the Internet. The two secure networks are in effect combined into a Virtual Private Network and it allows secure communications between the two hosts.

Firewall Example (one)



- OS/390 system, running a web server , connected to the Internet.

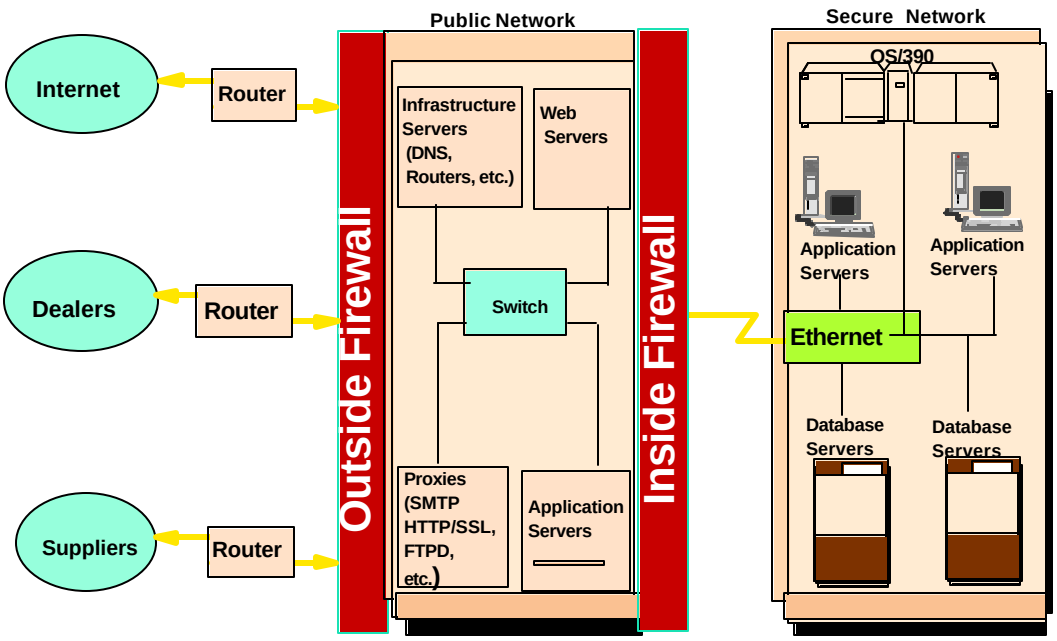
Firewall Example (two)



- Internet Connection Application Programming Interface (ICAPI) and Common gateway Interface (CGI) are standards for interfacing external applications with information servers, such as HTTP or Web servers. These programs are executed in real time, so they can output dynamic information.

- Example: A program that a web daemon will execute and transmit information to a data base, receives the results back and display them to the client that executed the program.

Firewall Example (three)



- Each box in the public network represents multiple machines providing the services depicted.

References

WSC Advanced Technical Support

- OS/390 Security Server 1999 Updates Technical Presentation Guide (SG24-5627-00)
  - located at www.redbooks.ibm.com
- Security in OS/390-based TCP/IP Network (SG24-5383)
- SecureWay Security Server Firewall Technologies Guide and Reference (SC24-5835-05)