z/OS Firewall Technology Overview

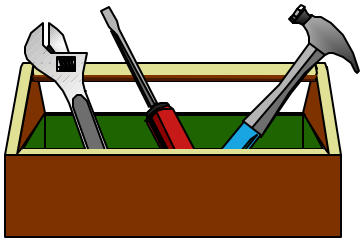
Mary Sweat
E - Mail: sweatm@us.ibm.com

Washington System Center

Firewall Technologies Tools

WSC
Advanced Technical Support

- Included with the OS/390 Security Server
  - Configuration Client (GUI)
  - Configuration Commands
  - Logging Server
  - 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 is not checked to see if there is a license for the Security Server.

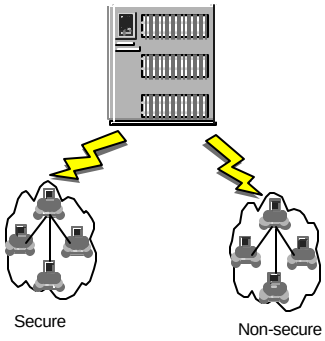
- Prior to OS/390 2.10 the Socks server, FTP proxy, ISAKMP server and Configuration client that comes with OS/390 Firewall Technologies can **only** be used if the customer has purchased the Security Server. The firewall checks and ensures a Security Server license exist before it allows the installation to utilize these features.

  As of OS/390 2.10 a customer can use ISAKMP and the Configuration Client without having a license provided they have the APAR OW47982 installed. A license is still required if configuring the FTP proxy or the Socks server.

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.
- SECURE adapter is the side of the firewall that allows data to flow in and out of the company's environment. The SECURE environment can be thought of as the company's intranet or an area which the company has control over the machines and can dictate what changes are allowed on those machines.
- The NONSECURE environment deals with the flow of traffic going to or coming from the Internet or any environment the company can not trust or does not control.
- The OS/390 Firewall Technology Virtual Private Network (often known as tunnels) can utilize the hardware crypto features on your CMOS machines. No other feature of the OS/390 Firewall uses this hardware.

  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
- 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)

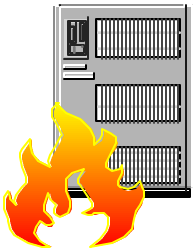
- System Secure Sockets Layer is required for the usage of the OS/390 Firewall GUI.
- OCSF and OCEP is required if dynamic tunnels (ISAKMP) are used.

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.

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

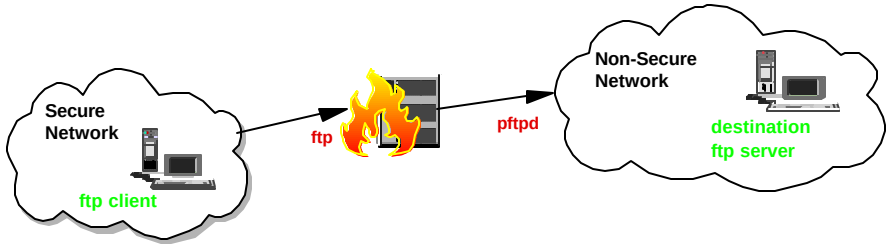
- Authorization to use and configure the firewall is checked via External Security Manager (eg. RACF). Must have explicit authorization to the GUI RACF profile ICF.CFGSRV even if you are a superuser.

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

FTP Proxy Support

WSC Advanced Technical Support

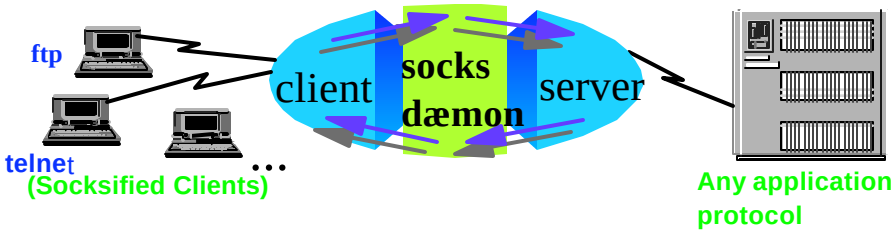
- OS/390 Firewall Technologies supply an FTP proxy server (**pftpd**)
  - access controlled on a user-by-user basis
    - to go out of the secure network
    - to come in from the non-secure world
  - local ***ftp*** commands disabled on the firewall
- Users **ftp** to the firewall and with valid authorizations, **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.
- The purpose of the FTP proxy is to act as middle man. Rather then the client connecting directly to the FTP server, the client will connect to the FTP proxy first. The proxy then ask the client where did it really want to go? The client responds with the information and the FTP Proxy performs the actual connection to the FTP server. When using this proxy the firewall address is what is sent to the FTP server rather then the clients address which is the norm. Therefore, the FTP proxy hides the client addresses.
- 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.
- Clients must be userid/passwords on the firewall system to use the FTP proxy. They do not need authority to logon to the system.
- Each proxy server is written for a specific application, in this case FTP.

Socks

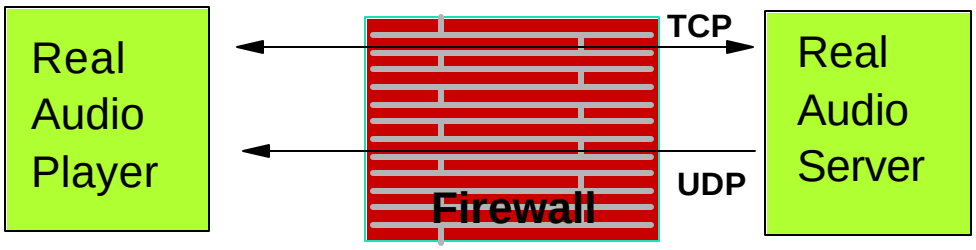
- A socks dæmon sits between the client and destination server
  - socks dæmon is generic
    - can handle traffic for multiple, different applications
- Socks replaces the IP address of the user with the address of the firewall



- A SOCKS server performs the same function as the FTP proxy with regards to keeping the client's address secret. However, a SOCKS server can be used by multiple application instead of the FTP proxy only working with FTP applications.
- To use the SOCKs server, application must be SOCKSIFIED, meaning the applications have be compiled to incorporate the SOCKS server library.
- SOCKS server uses rules to determine whether the request is authorized to pass to or from the protected network
- Authorization is rules-based, as opposed to a userid/password like the FTP proxy

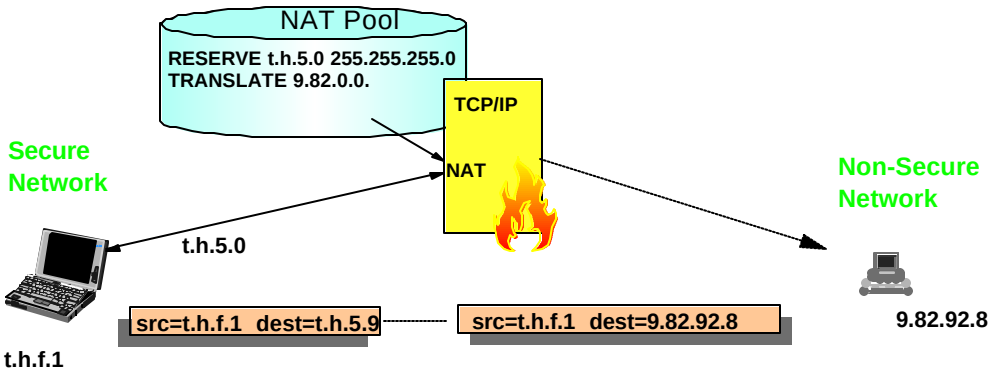
Real Audio Support

- 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)

- 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

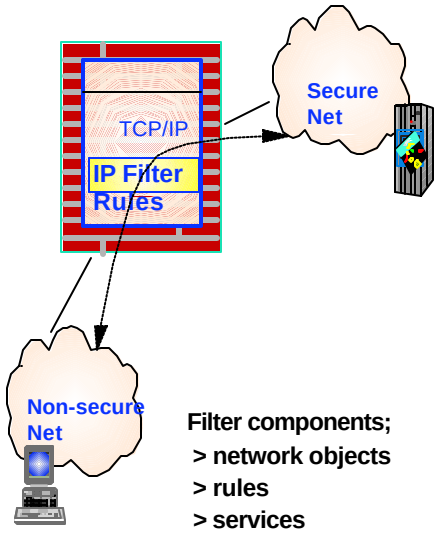
- NAT looks like a normal IP router that forwards IP packets between two network interfaces.

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



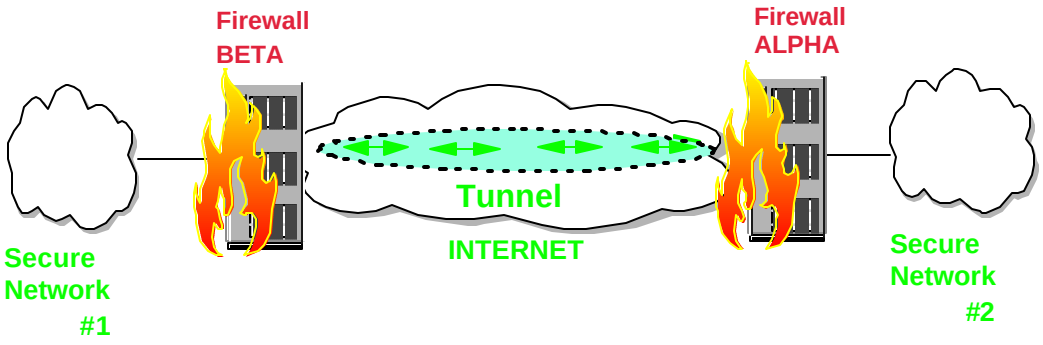
Filter components;
> network objects
> rules
> services
> connections

- Filter rules, or definitions specify what traffic is authorized to flow where, must be defined by the system administrator and activated

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.

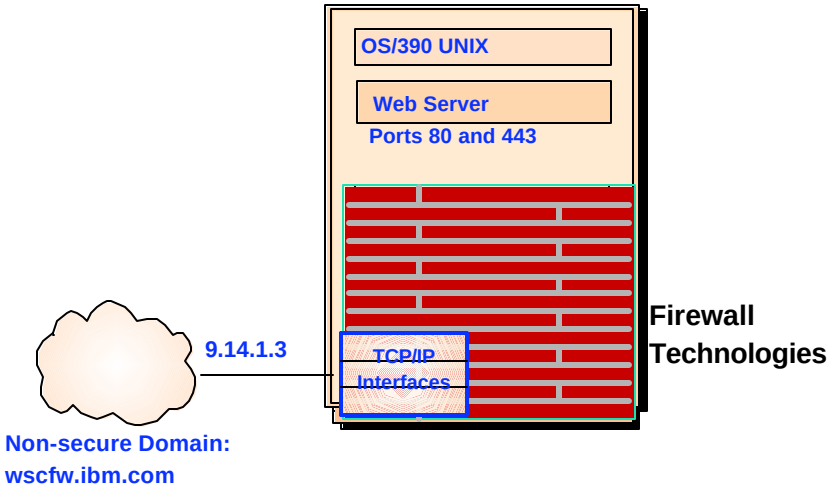
Tunnel Types

WSC Advanced Technical Support

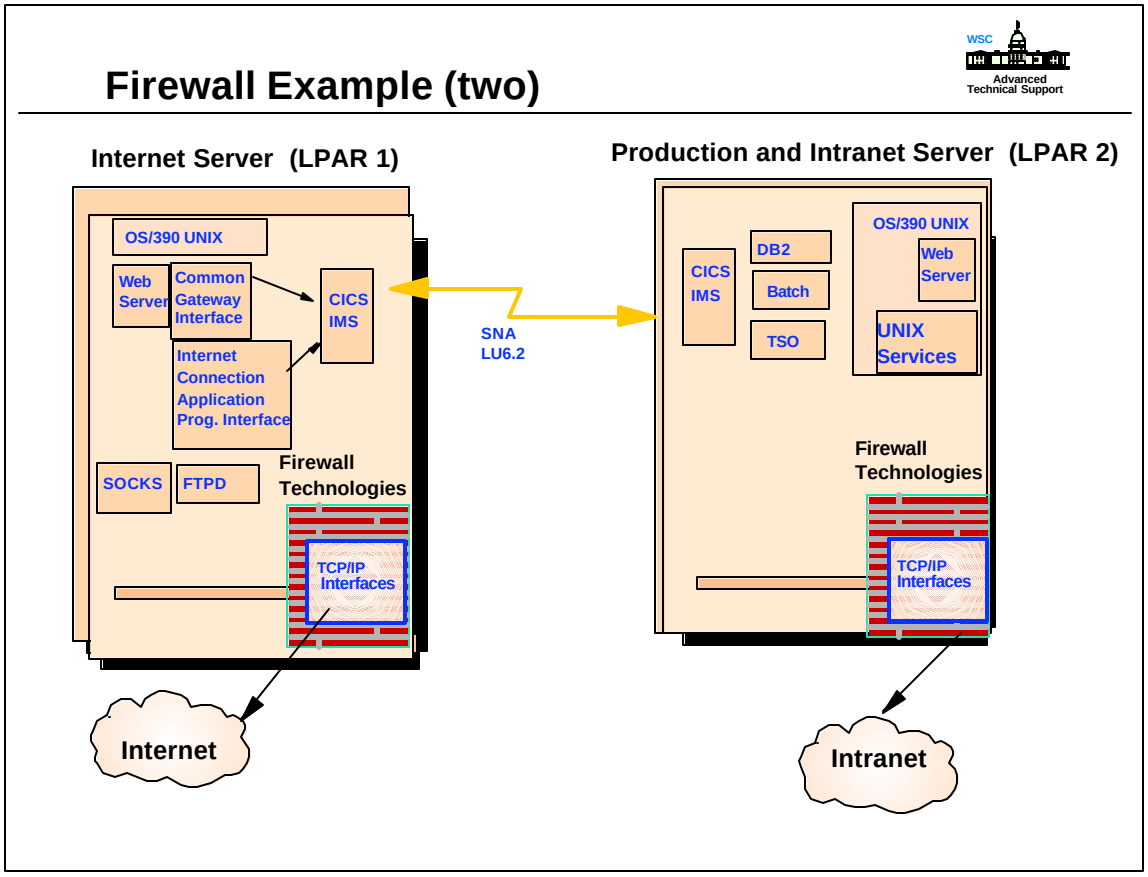
- Manual, keys are static
  - encryption & authentication keys are the same for the life of the tunnel
  - must be manually updated
  - has the widest choice of header and encryption options
- Dynamic tunnels (ISAKMP), keys are dynamic
  - based on Internet Security Association and Key Management Protocol (ISAKMP)
  - defines message formats and flows that will allow two devices to dynamically agree to the information shared between them
  - negotiate and refresh security parameters and exchange keys securely

- Ability to inter-operate with another OS/390 system or any other compatible IBM platforms is simplified by using export/import capability of the **fwtunn**l command or via the configuration client.
- For communicating with non-IBM platforms the tunnel information will have to be entered manually.

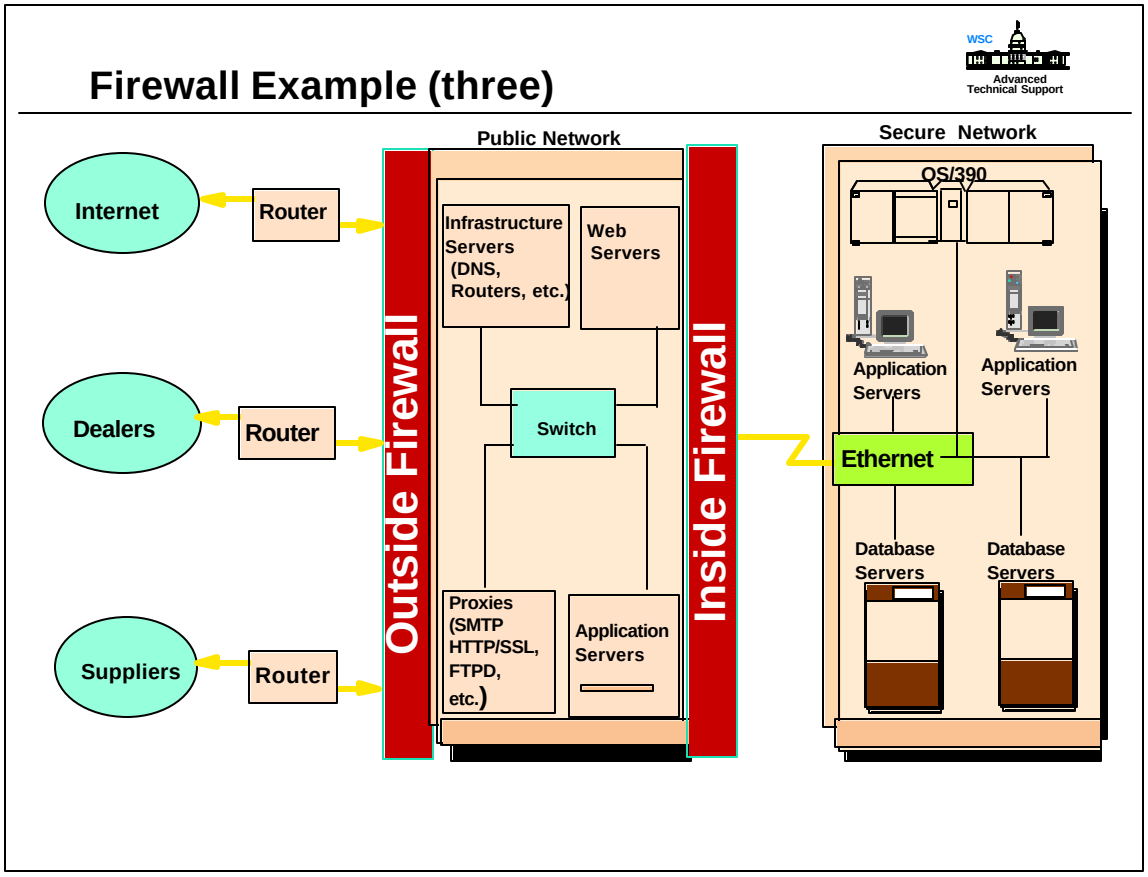
Firewall Example (one)



- OS/390 system, running a web server , connected to the Internet. A firewall is setup on this host to ensure that only traffic destined for the Web server are allowed in. All other data is denied access.



- A second example of using the OS/390 Firewall is to place one on the LPAR that deals with the public (Internet). This firewall controls traffic inbound from the Internet and the response back.
- The production LPAR also has a firewall. This firewall controls company employees coming from the Intranet.
- Any communication between the two LPAR's is performed via SNA.



- Each box in the public network represents multiple machines providing the services depicted.
- A firewall on a platform other then OS/390 is setup in front of the public environment. This firewall handles all incoming requests from the Internet.
- Behind the public network another firewall is placed (OS/390 Firewall). This firewall is there to have another layer of security in place of the critical data residing on the OS/390.

IPSec Standard References

WSC
Advanced Technical Support

- Request for Commends (RFCs)
  - located at www.ietf.org
    - 1825 Security Architecture for Internet Protocol
    - 1826 IP Authentication Header
    - 1827 IP Encapsulating Security Payload
    - 1828 IP Authentication Using Keyed MD5
    - 1829 The ESP DES_CBC Transform
    - 2401 Security Architecture for Internet Protocol
    - 2402 IP Authentication Header
    - 2403 HMAC-MD5-96 within ESP and AH
    - 2404 HMAC-SHA-1-96 within ESP and AH
    - 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
    - 2406 IP Encapsulating Security Payload
    - 2407 Internet IP Domain of Interpretation for ISAKMP
    - 2408 Internet Security Association and Key Management Protocol (ISAKMP)
    - 2409 Internet Key Exchange
    - 2410 NULL Encryption Algorithm and Its Use With IPSec

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)