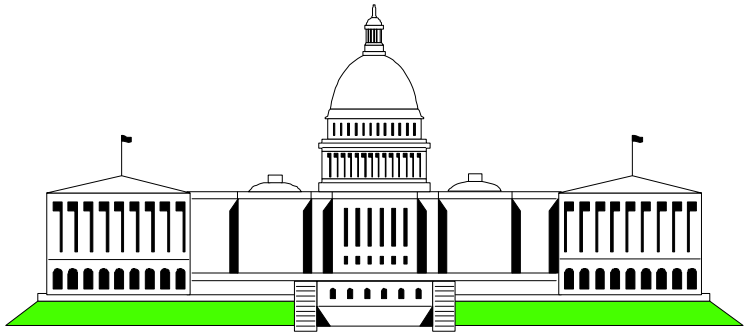
OS/390 Firewall Technology Overview



Washington System Center

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

Agenda

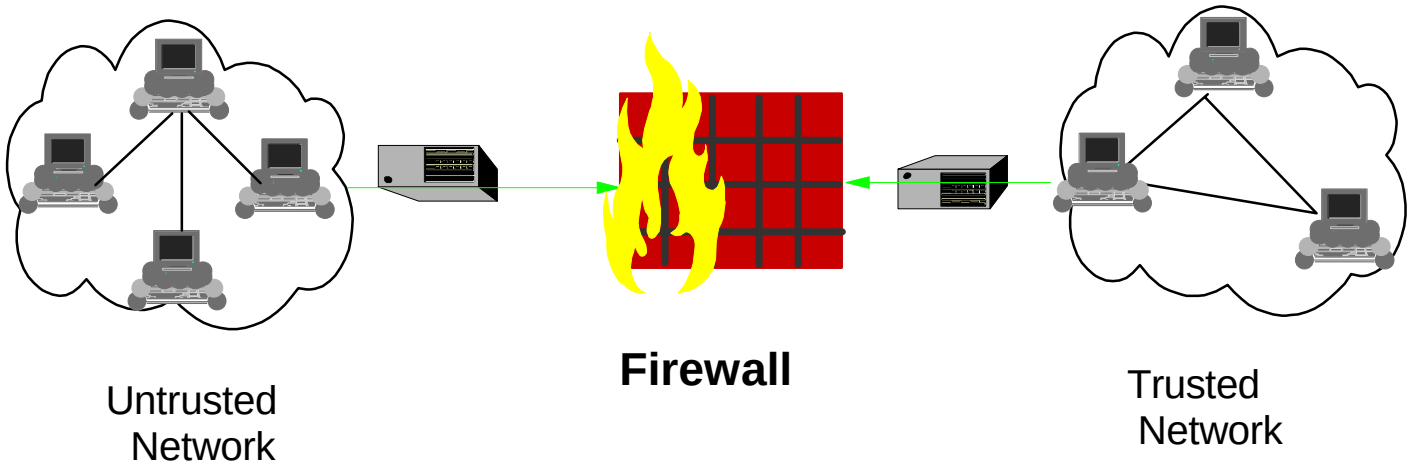
WSC
Advanced
Technical Support

- Basic Firewall strategies and design
- Hardware requirements
- Software requirements
- Components of OS/390 Firewall
- Enhancements in latest release of OS/390 Firewall

What is a Firewall

WSC
Advanced
Technical Support

- A solution that provides controlled access between a private (trusted) network, and an untrusted network such as the Internet
- A tool for enforcing your network security policy



Why Use a Firewall?

WSC
Advanced
Technical Support

??????????????????????????????????????

? ■ Limit access by persons within the secure network to selected resources in the non-secure network ?

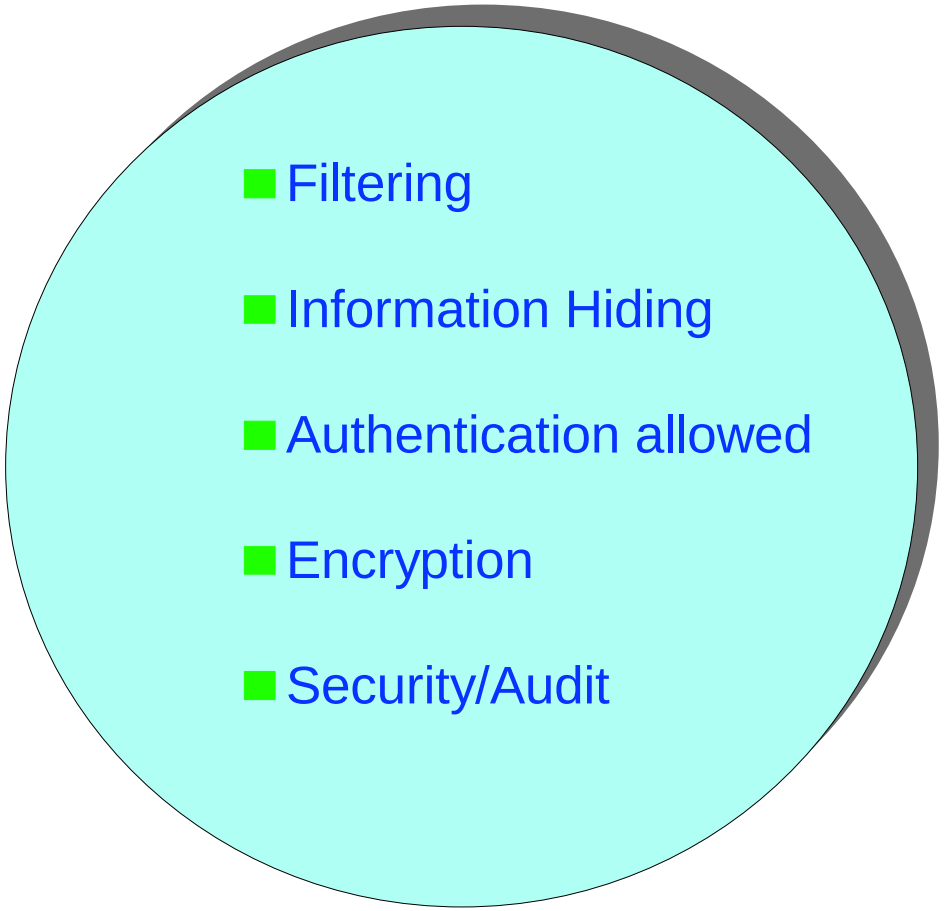
? ?

? ■ Reduce network traffic outside the secure network ?

? ■ Improve performance within the secure network ?

??????????????????????????????????????

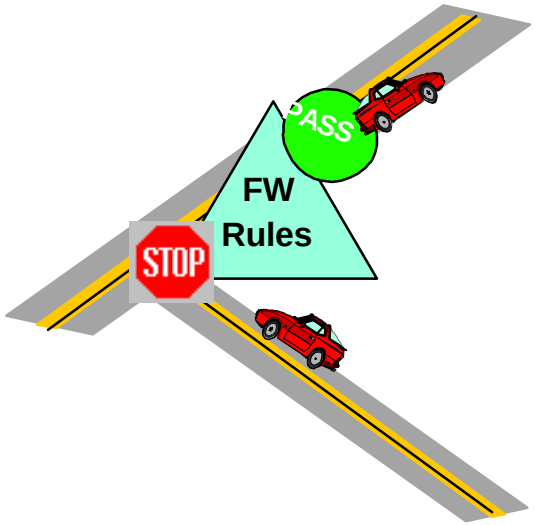
Firewall Strategies



Basic Design Decisions in a Firewall

WSC
Advanced
Technical Support

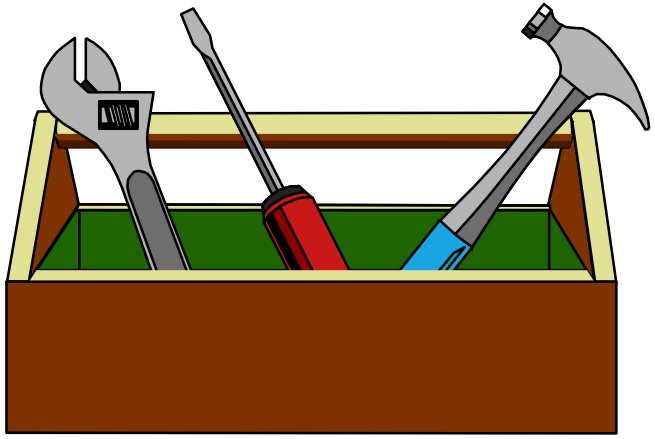
- Ensure physical security
- Configure the firewall by disallowing everything and then proceed by enabling those services defined in the security policy
  - Support only required applications and remove or disable others
- Security policy that defines how a firewall should function in cooperation with the security group/advisors
  - what type of traffic is allowed through the firewall and under what conditions
- Audibility



Firewall Technologies Tools

WSC
Advanced
Technical Support

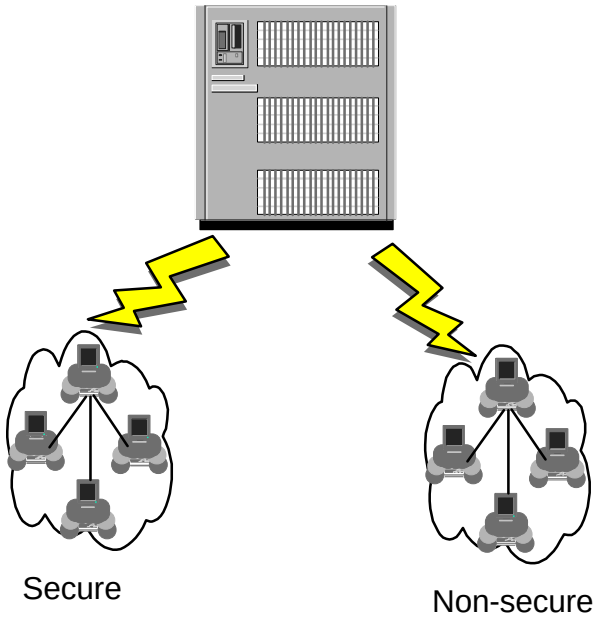
- Included with the OS/390 Security Server
  - Configuration Commands
  - Configuration Client (GUI)
  - Proxy FTP server
  - Socks Server
  - Logging Server
  - Real Audio Support



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

Hardware

- 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

- ICSF/MVS V2 R1.0 and Prog. Cryptographic Option
  - this is optional requirement as firewall can use software encryption

Software

WSC
Advanced
Technical Support

- OS/390 Security Server (RACF)
- OS/390 eNetwork Communications Server
- OS/390 Unix services (OpenEdition)
- OS/390 C/C++ Collection Cl. Lib.

Software for Configuration Client

WSC
Advanced
Technical Support

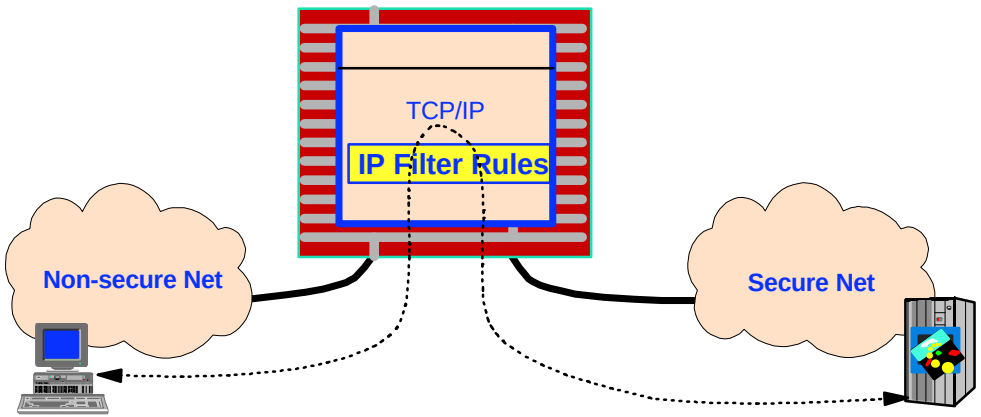
- AIX
  - Java.rte 1.1.4 or 1.1.6
  - AIX 4.2 or higher (as long as Java.rte level is supported)
  - Netscape nav.rte 3.0.0.1
- Windows 95 or Windows NT
  - Web browser with Java and frames support
  - Zip tool that handles long file names
    - WinZip32 tool in WinZip

IP Filters

WSC
Advanced
Technical Support

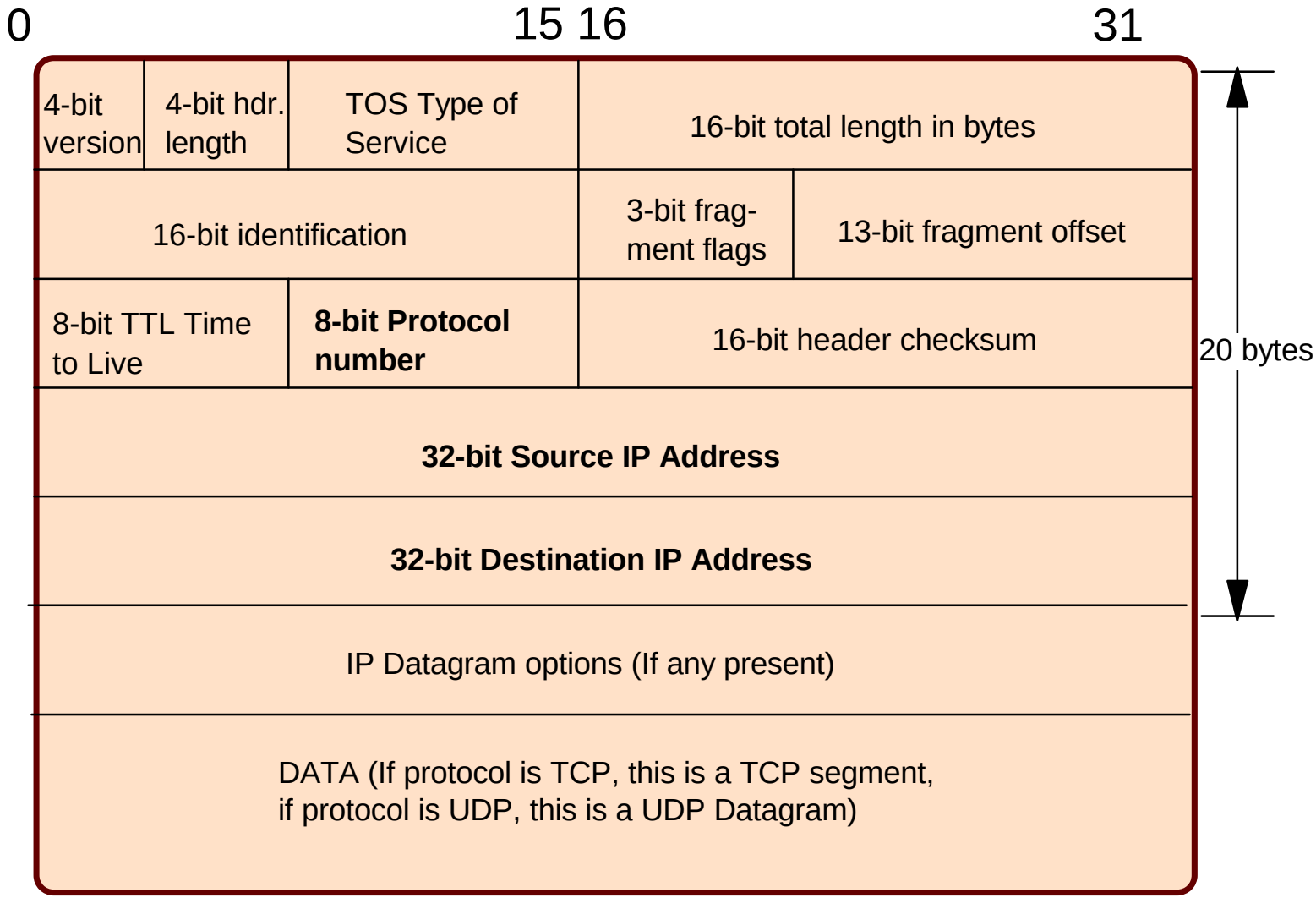
- Packet filtering looks at every packet coming into the IP stack, and determines whether the filter rules allow the packet to be sent to its destination.
- Filtering checks;

-- source and destination IP address & mask
-- source and destination port
-- direction of the data flow
-- IP protocol
-- type of interface (secure or nonsecure)
-- fragmentation
-- tunnel ID



IP Datagram - Unit of Data

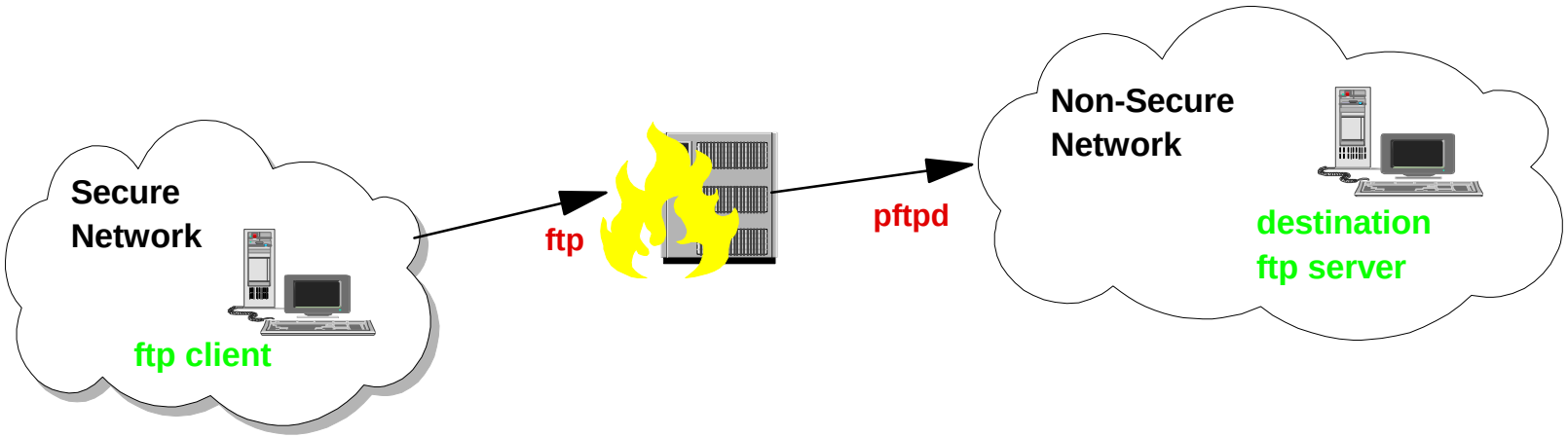
WSC
Advanced
Technical Support



FTP Proxy 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

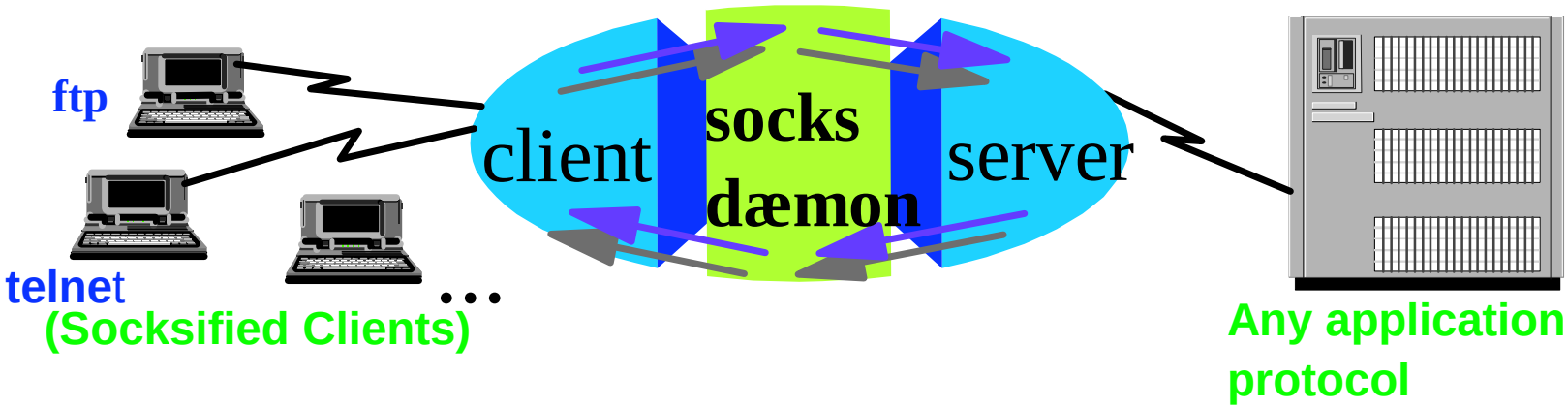
- Users **ftp** to the firewall and with valid authorizations, **pftpd** contacts FTP server outside the secure network



Socks

- A socks dæmon sits between the client and destination server
  - socks dæmon is generic
    - can handle traffic for multiple, different applications

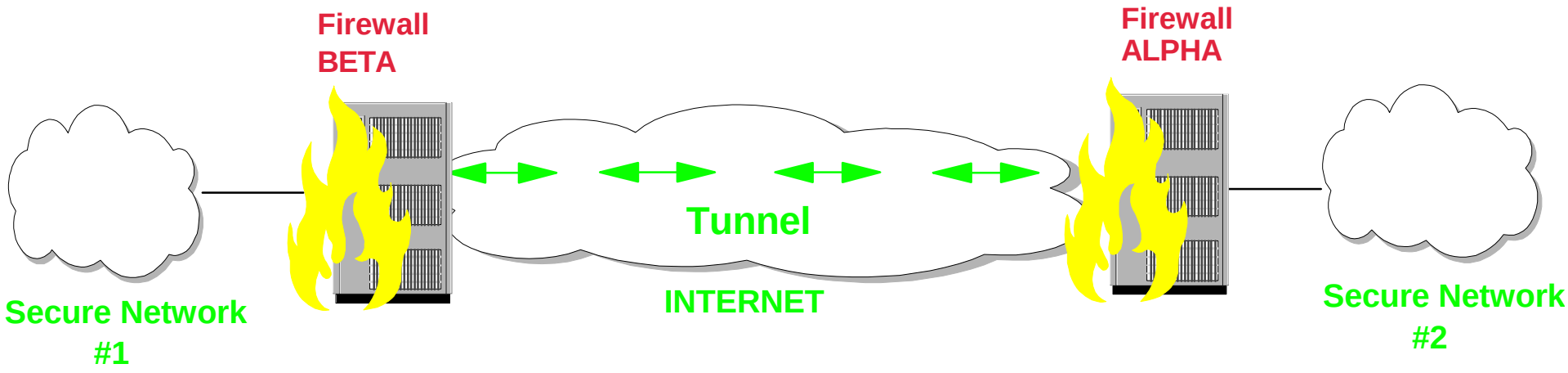
- Socks replaces the IP address of the user with the address of the firewall



Virtual Private Networks

WSC
Advanced
Technical Support

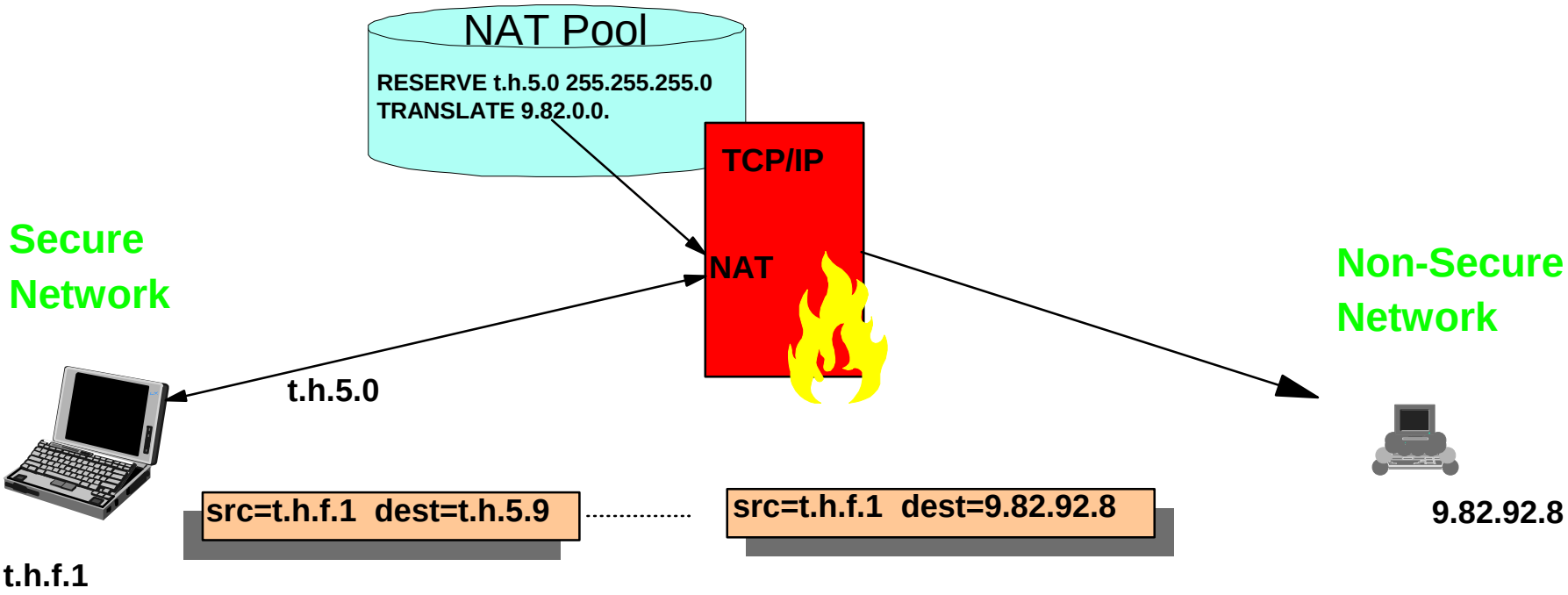
- Virtual Private Networking (VPN) allows secure communications between remote sites over a public network like the internet



Network Address Translation (NAT)

WSC
Advanced
Technical Support

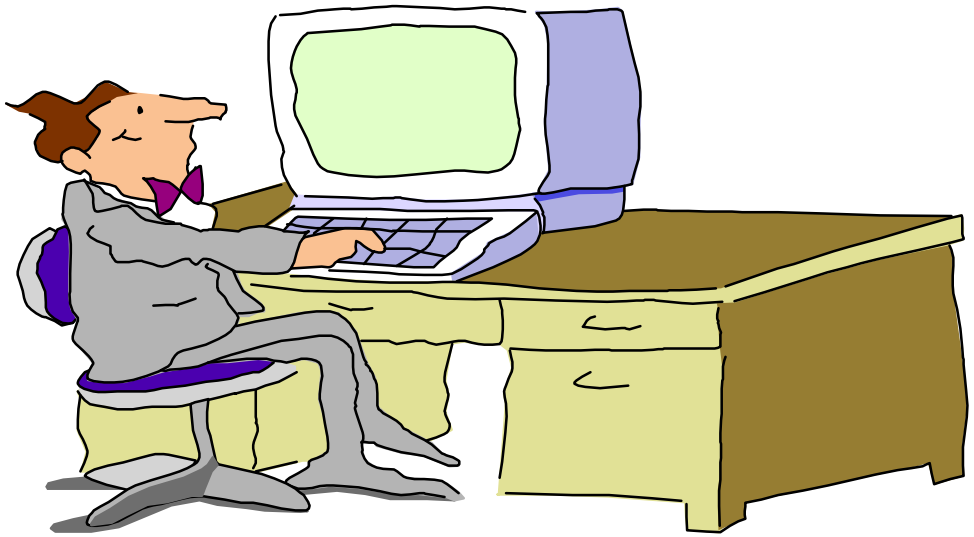
- Network Address Translation provides a translation from an internal (secure) IP address to an temporary external registered address



Logging/Configuration/Administration

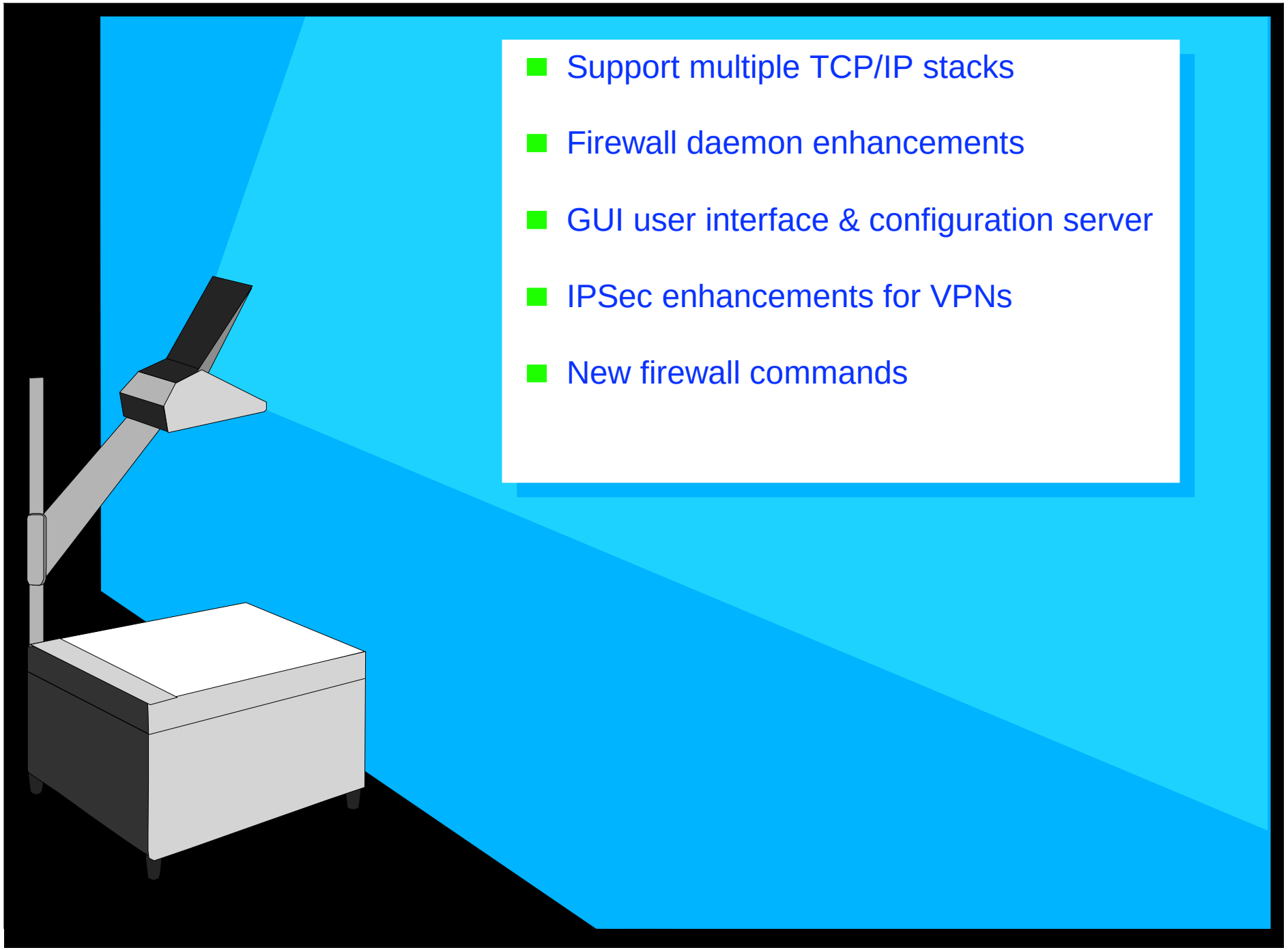
WSC
Advanced
Technical Support

- Logging
  - Critical to the security of any system
  - Ability to reliably detect potential intrusions
    - implies the ability to collect and save information about transactions
- GUI/Commands are used to configure and administer the firewall technologies
  - define secure and non-secure adapters
  - set logging parameters
  - define rules for packet filtering and socks
  - define VPN



Firewall enhancements in latest release (R7)

WSC
Advanced
Technical Support

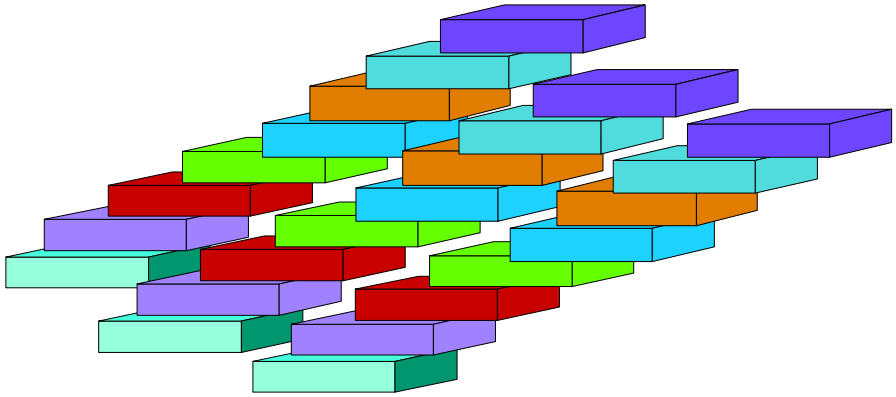


- Support multiple TCP/IP stacks
- Firewall daemon enhancements
- GUI user interface & configuration server
- IPSec enhancements for VPNs
- New firewall commands

Multi-Stack

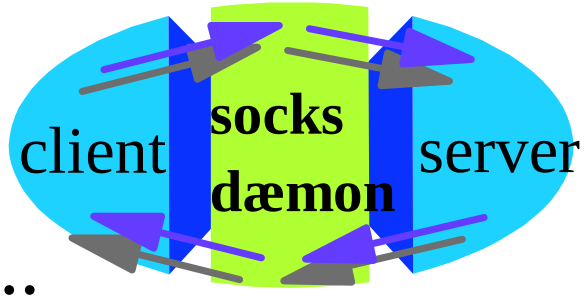
- 8 Firewalls can now run simultaneously
  - in prior releases, system was restricted to one
  - utilizes TCP/IP stack (OS/390 supports 8)

- Firewall configuration commands made "stack-aware"
  - new commands associate firewall functions with particular stack
  - each firewall could have a potentially different configuration

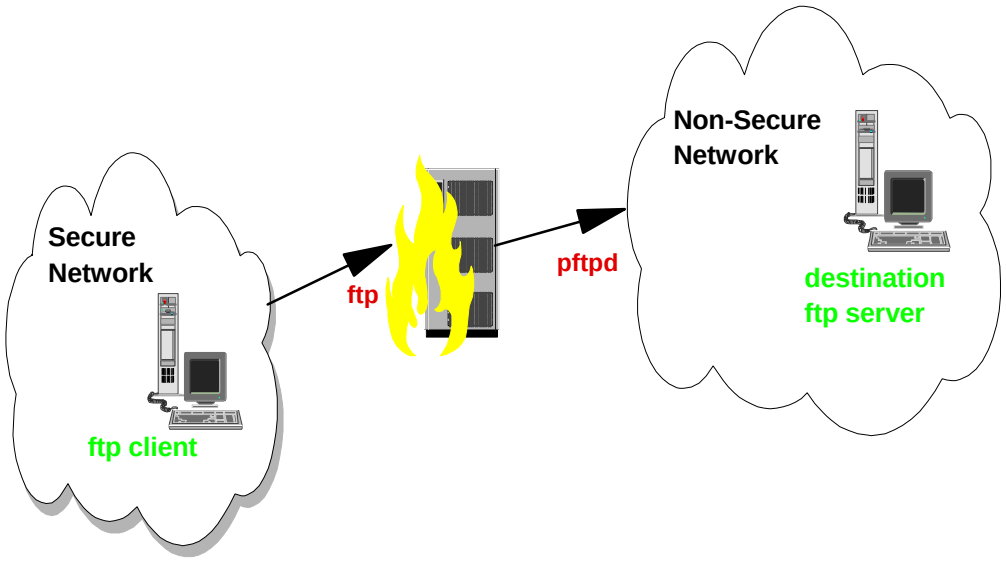


FTP & SOCKS

- Enhancements
  - Number of connections allowed is vastly increased
  - Administrator can determine number of connections allowed

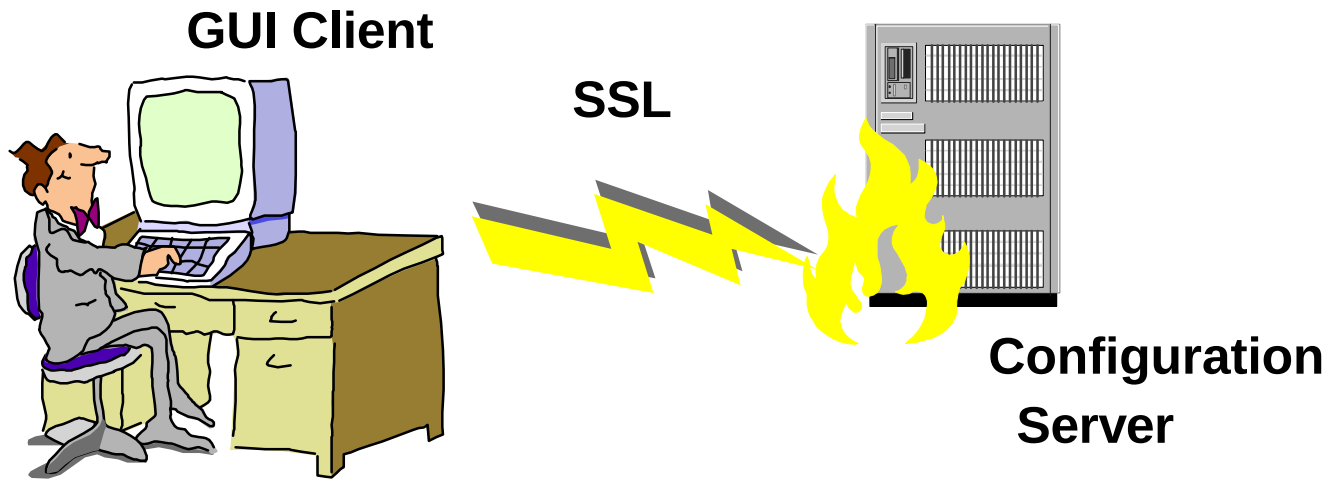


...



Graphical User Interface

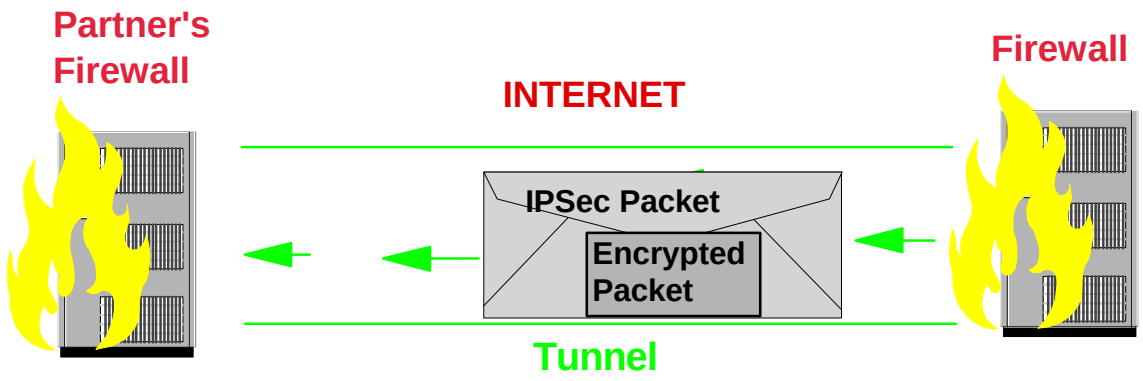
- Graphical User Interface (GUI)
  - written in JAVA
  - installs / runs on Windows 95/NT & AIX
- Configuration Server runs on OS/390
- GUI Security uses Secure Sockets Layer (SSL)



IPSec Enhancements for VPNs

WSC
Advanced
Technical Support

- Uses upgraded IPSec that supports new standards
  - triple DES
  - replay prevention
  - new authentication processes
  - encryption standard contains ability to also authenticate



QUESTIONS