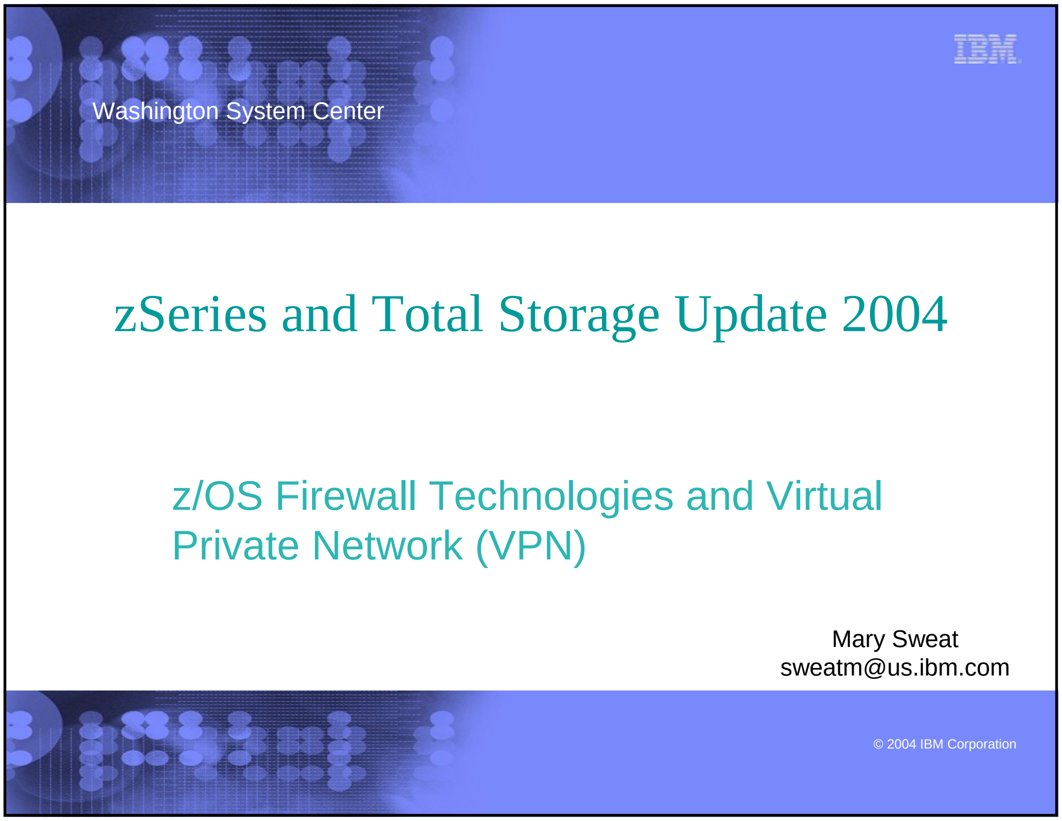
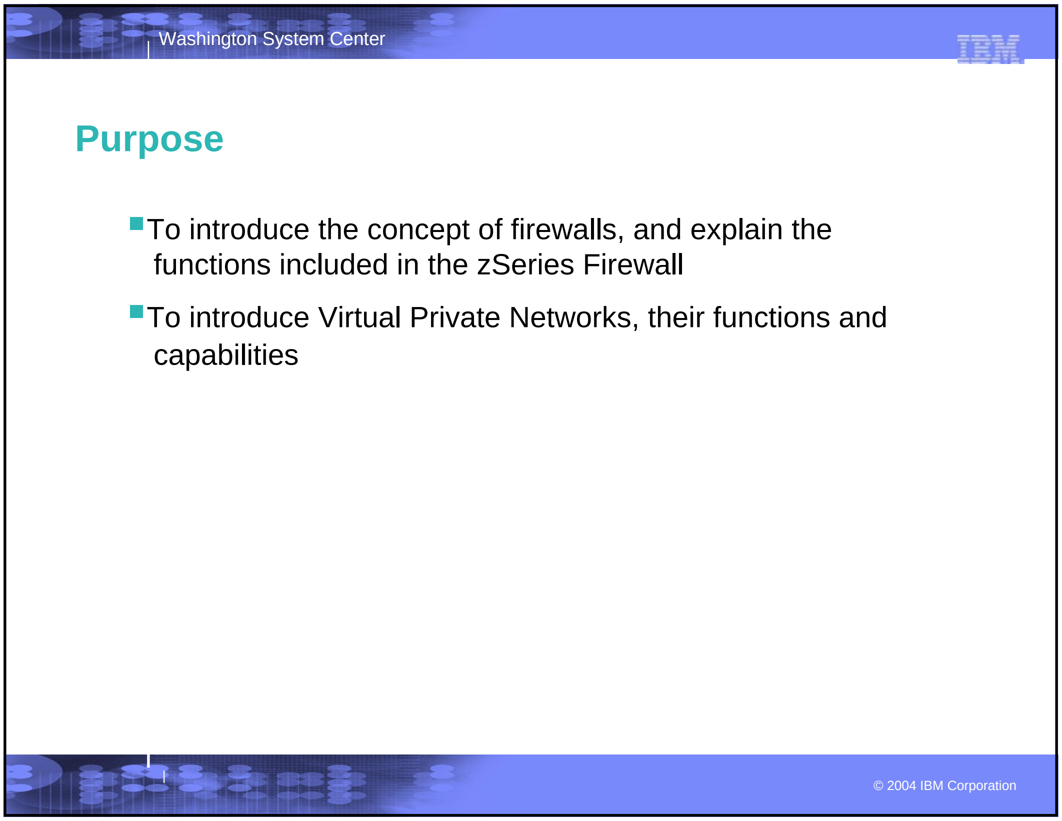


Washington System Center

zSeries and Total Storage Update 2004

z/OS Firewall Technologies and Virtual Private Network (VPN)

Mary Sweat
sweatm@us.ibm.com

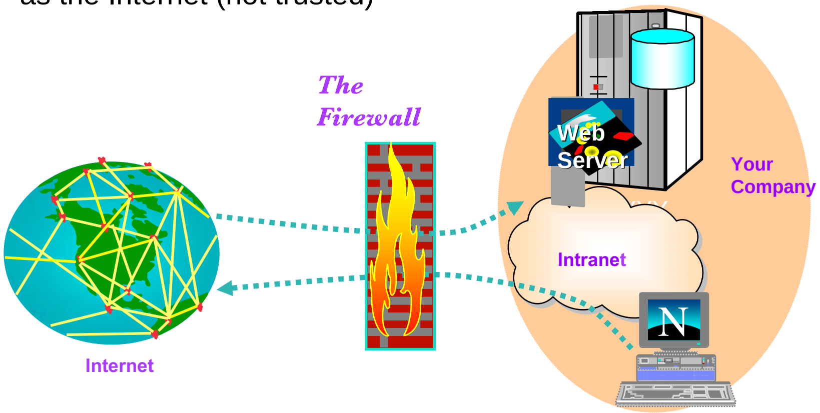


Purpose

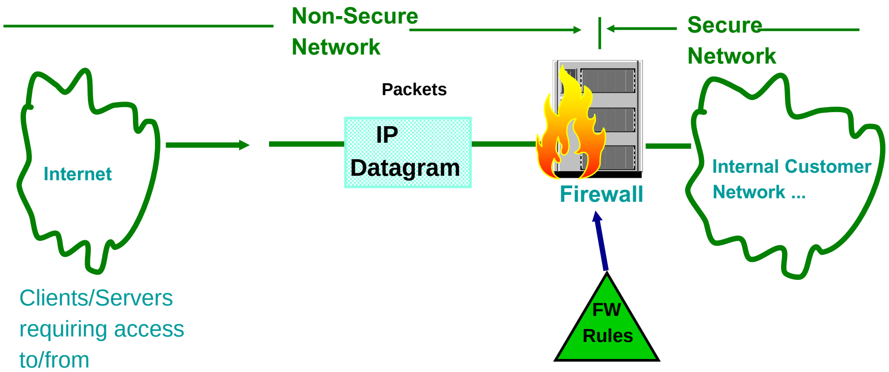
- To introduce the concept of firewalls, and explain the functions included in the zSeries Firewall
- To introduce Virtual Private Networks, their functions and capabilities

What is a Firewall?

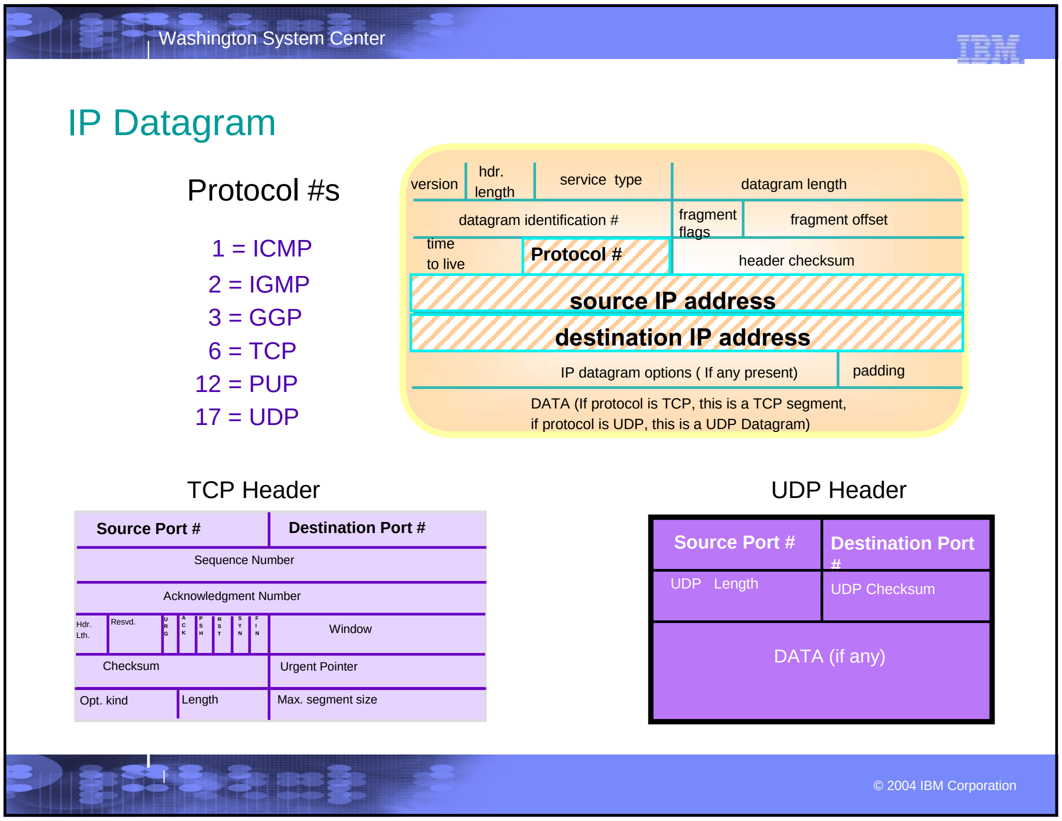
- A solution that provides controlled access between a private (trusted) network, and a network you have no control over such as the Internet (not trusted)



Theoretical Firewall Environment



Clients/Servers requiring access to/from Customer's network



IP Datagram

Protocol #s

1 = ICMP
2 = IGMP
3 = GGP
6 = TCP
12 = PUP
17 = UDP

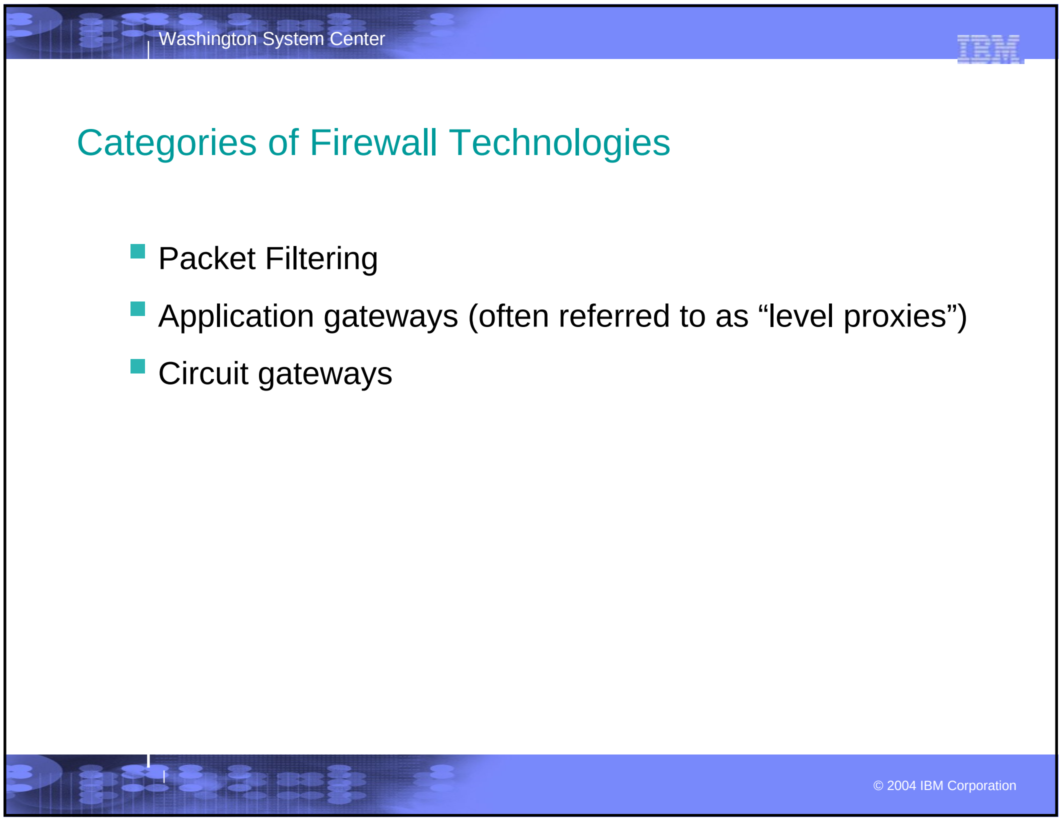
version	hdr. length	service type	datagram length	
datagram identification #			fragment flags	fragment offset
time to live		Protocol #	header checksum	
source IP address				
destination IP address				
IP datagram options (If any present)				padding
DATA (If protocol is TCP, this is a TCP segment, if protocol is UDP, this is a UDP Datagram)				

TCP Header

Source Port #							Destination Port #	
Sequence Number								
Acknowledgment Number								
Hdr. Lth.	Resvd.	URG	ACK	PSH	RST	SYN	FIN	Window
Checksum							Urgent Pointer	
Opt. kind	Length						Max. segment size	

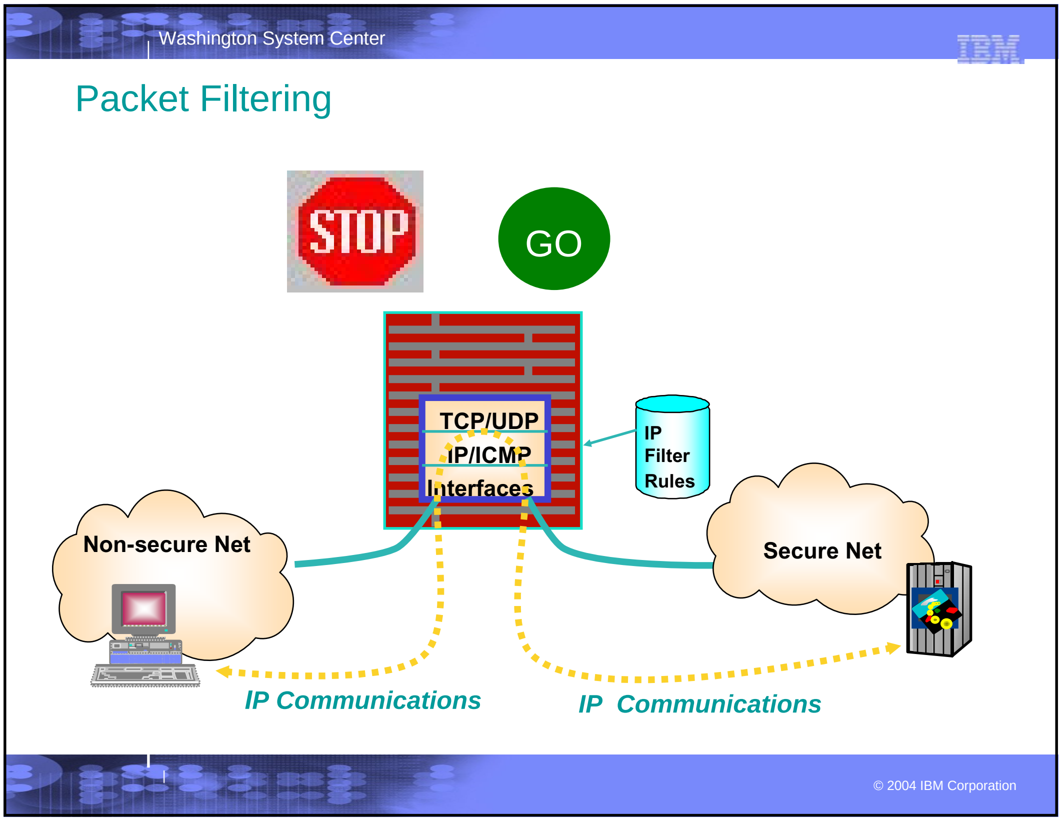
UDP Header

Source Port #	Destination Port #
UDP Length	UDP Checksum
DATA (if any)	

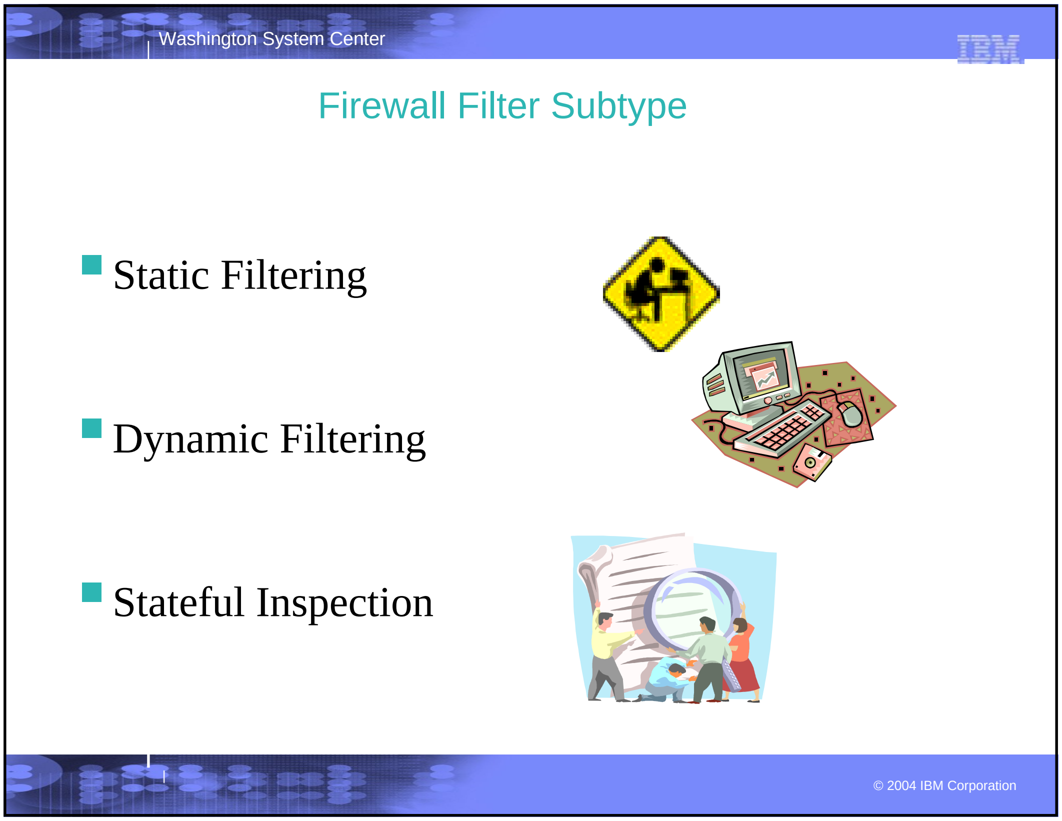


Categories of Firewall Technologies

- Packet Filtering
- Application gateways (often referred to as “level proxies”)
- Circuit gateways



Packet Filtering

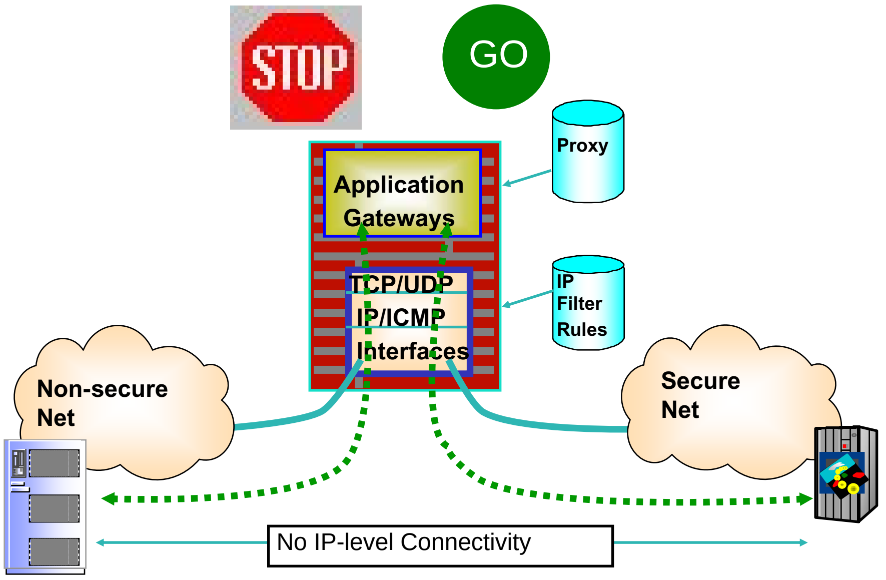


Firewall Filter Subtype

- Static Filtering
- Dynamic Filtering
- Stateful Inspection

Washington System Center

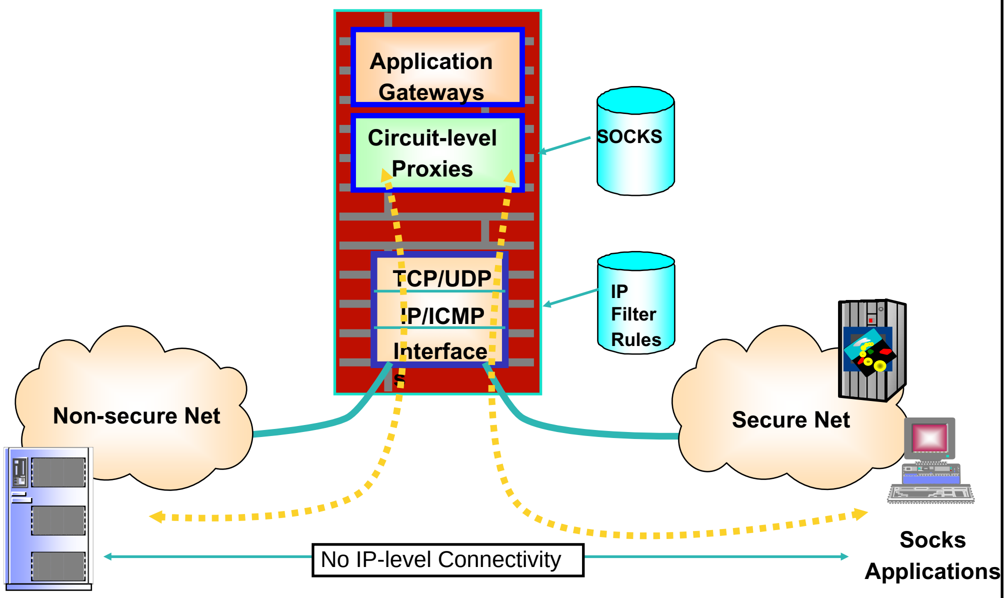
Application Gateway Firewall



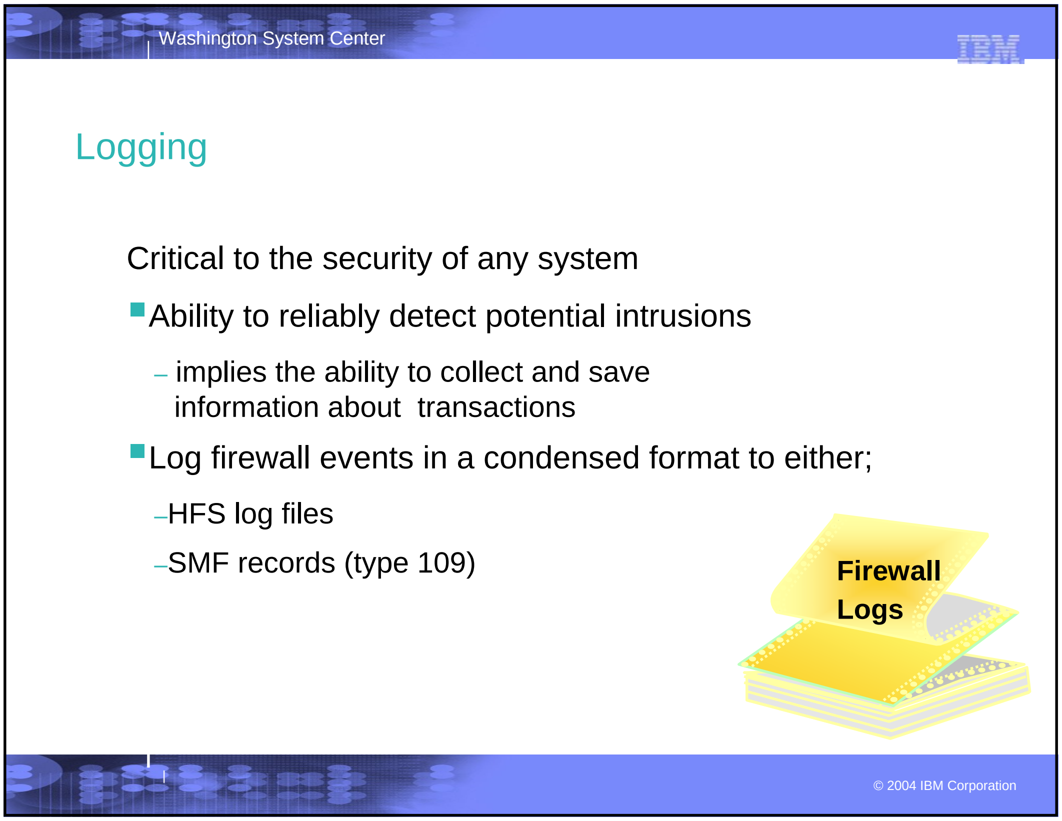
© 2004 IBM Corporation

Washington System Center

Circuit-level Proxies



© 2004 IBM Corporation

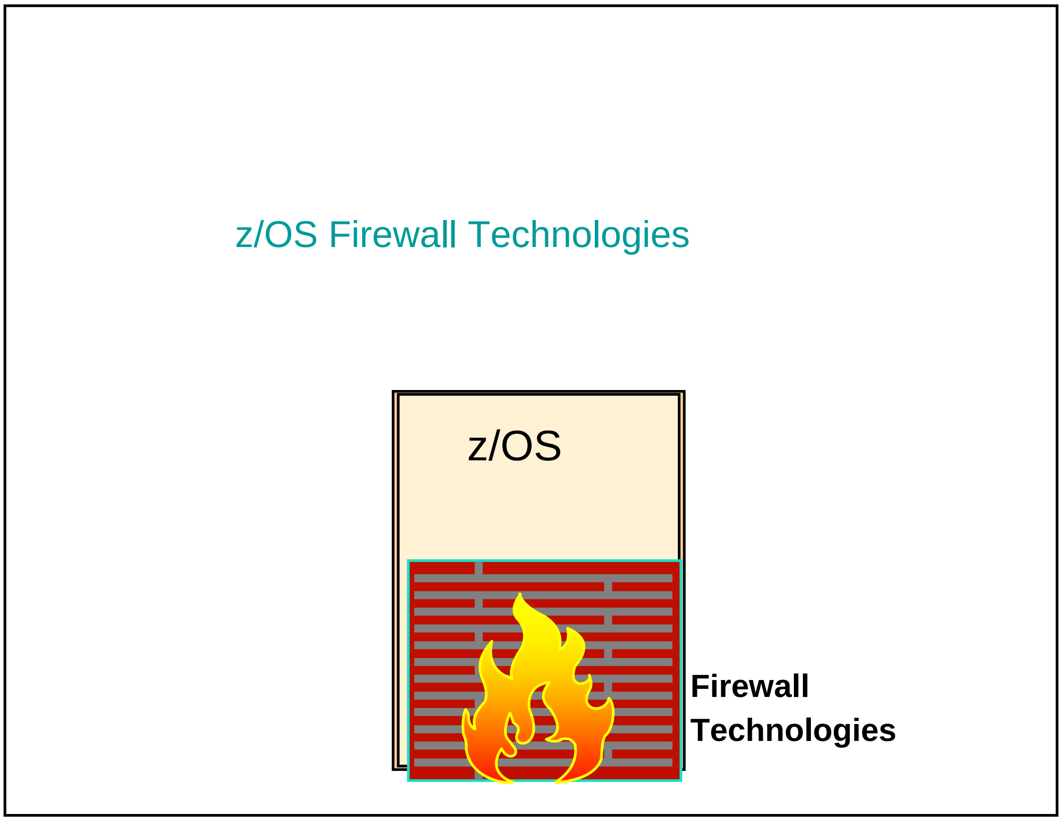


Logging

Critical to the security of any system

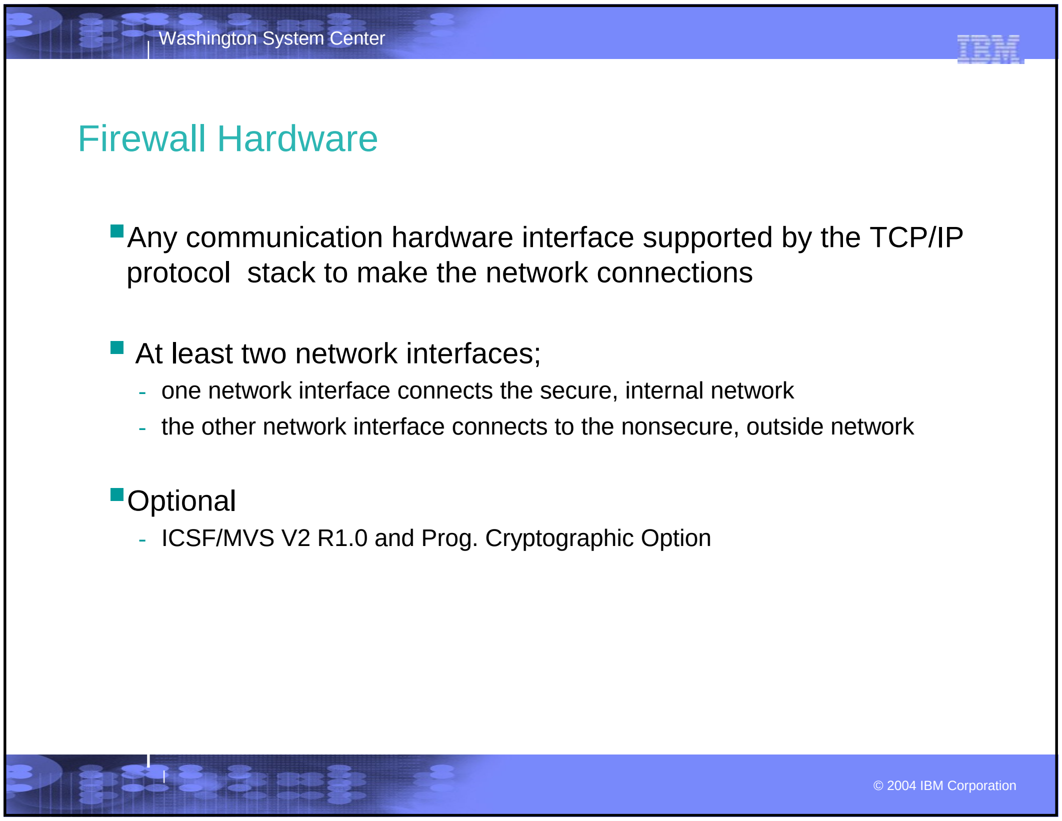
- Ability to reliably detect potential intrusions
  - implies the ability to collect and save information about transactions
- Log firewall events in a condensed format to either;
  - HFS log files
  - SMF records (type 109)

Firewall
Logs



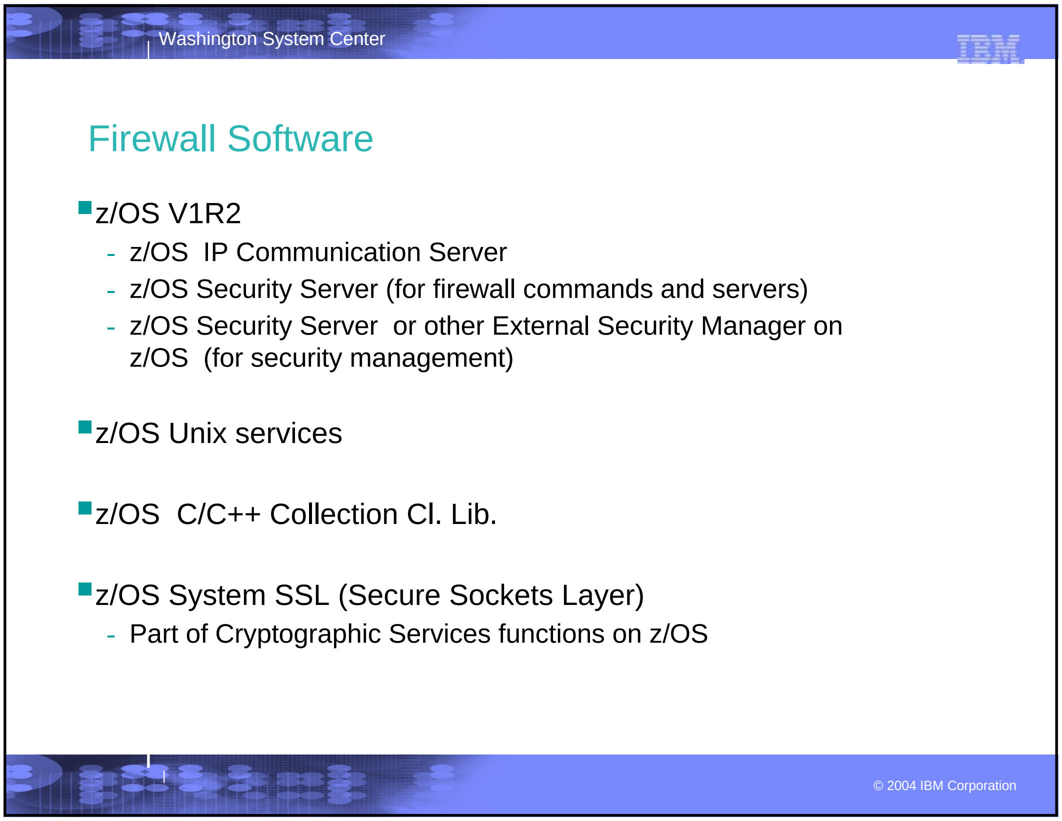
z/OS Firewall Technologies

z/OS
Firewall
Technologies



Firewall Hardware

- Any communication hardware interface supported by the TCP/IP protocol stack to make the network connections
- At least two network interfaces;
  - one network interface connects the secure, internal network
  - the other network interface connects to the nonsecure, outside network
- Optional
  - ICSF/MVS V2 R1.0 and Prog. Cryptographic Option



Firewall Software

- z/OS V1R2
  - z/OS IP Communication Server
  - z/OS Security Server (for firewall commands and servers)
  - z/OS Security Server or other External Security Manager on z/OS (for security management)
- z/OS Unix services
- z/OS C/C++ Collection Cl. Lib.
- z/OS System SSL (Secure Sockets Layer)
  - Part of Cryptographic Services functions on z/OS

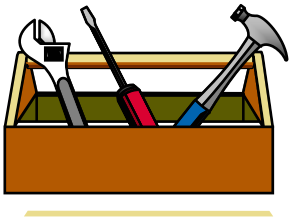
Software for Configuration Client

- 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

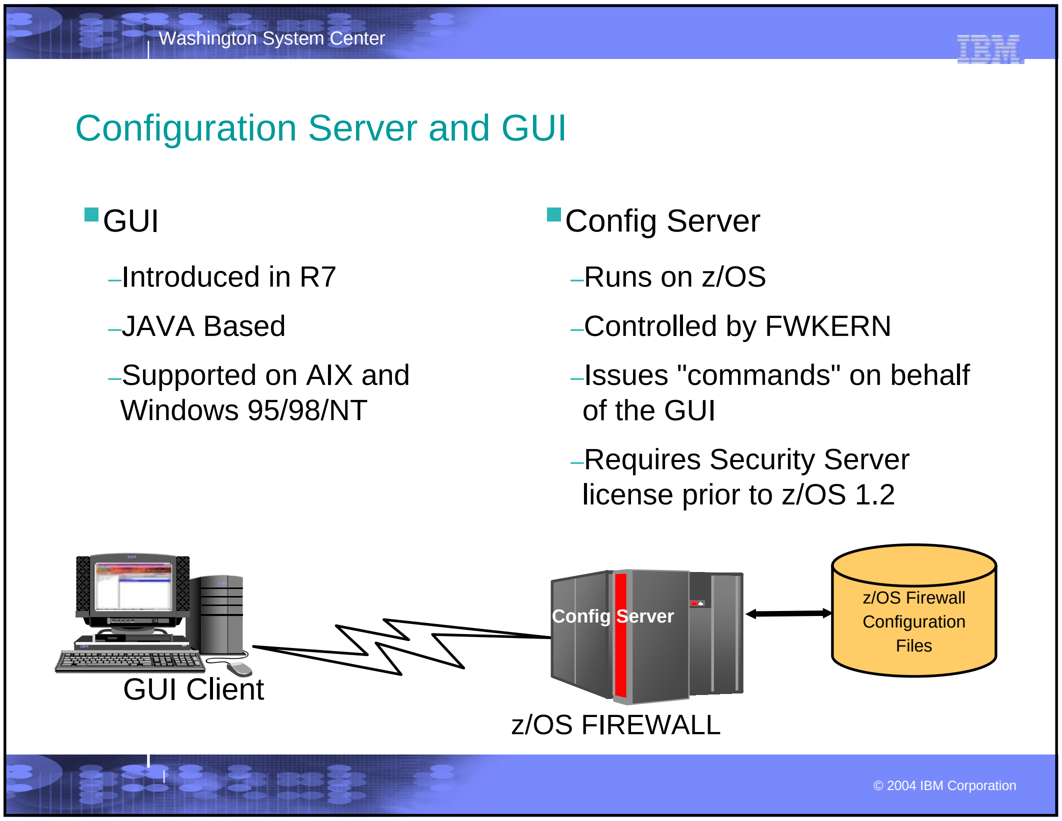
- Windows 95 or Windows NT
  - Web browser with Java and frames support
  - Zip tool that handles long file names
    - WinZip32 tool in WinZip

Firewall Technologies Tools

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

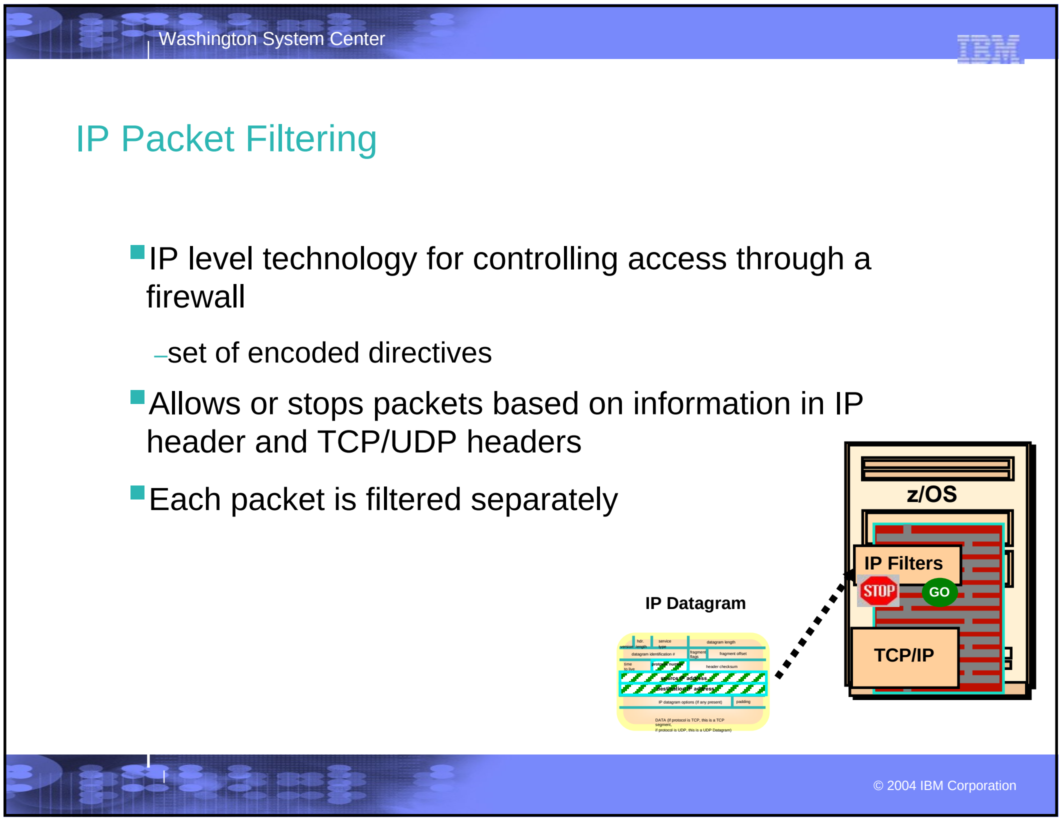


- Included with the eNetwork Communications Server for z/OS
  - Network Address Translation (NAT)
  - IP Filters
  - IP Tunnels (IPSec or Virtual Private Network)



Configuration Server and GUI

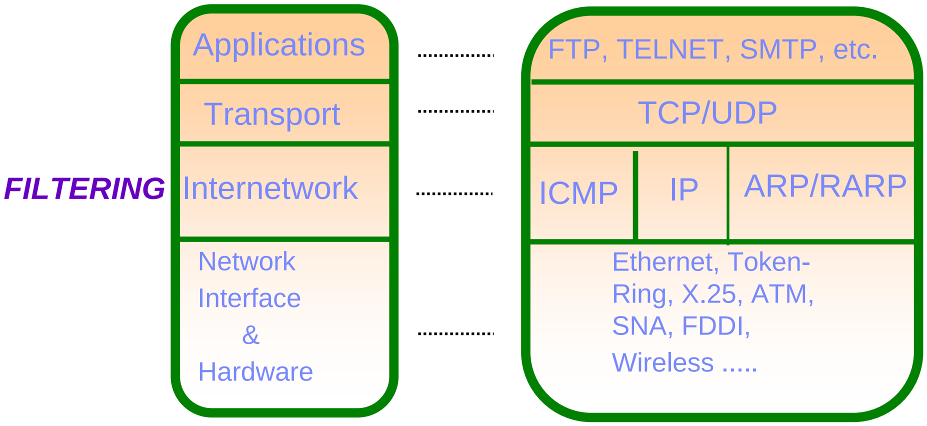
- GUI
  - –Introduced in R7
  - –JAVA Based
  - –Supported on AIX and Windows 95/98/NT
- Config Server
  - –Runs on z/OS
  - –Controlled by FWKERN
  - –Issues "commands" on behalf of the GUI
  - –Requires Security Server license prior to z/OS 1.2



IP Packet Filtering

- IP level technology for controlling access through a firewall
  - –set of encoded directives
- Allows or stops packets based on information in IP header and TCP/UDP headers
- Each packet is filtered separately

TCP/IP Layers and IP Filters


FILTERING
Applications
Transport
Internetwork
Network Interface & Hardware
FTP, TELNET, SMTP, etc.
TCP/UDP
ICMP
IP
ARP/RARP
Ethernet, Token-Ring, X.25, ATM, SNA, FDDI, Wireless .....

Packet Filter Rule Contents

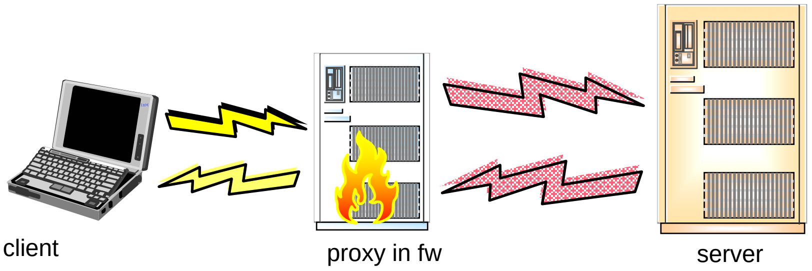
- **Selector Values**
  - Source:
    - IP Address Specification
    - Port
  - Destination:
    - IP Address Specification
    - Port
  - Protocol
- **Actions Types**
  - Deny
  - Permit
  - Anchor
- **Interface**
  - secure/non-secure/both
- **Direction**
  - Inbound/outbound/both
- **Routing**
  - local/route/both
- **Control Information**
  - logging
  - time filters
  - tunnel (vpn information)

```
type                  =   permit
source address        =   9.12.14.128
source masking        =   255.255.255.255
destination address = 10.12.14.247
destination mask      =   255.255.255.255
protocol              =   tcp
source operation code  =    gt
source port           =   1023
destination operation code =   eq
destination port           =   23
interface             =   nonsecure
routing               =   local
direction             =   both
logging               =   y
```

Washington System Center

File Transfer Protocol Proxy

- ***FTP proxy is a TCP/IP service that transfers files from one network host to another***
- ***FTP proxy server (pftpd) in the firewall checks authorizations to go out of the secure network***
- ***With valid authorizations,* pftpd *contacts FTP server outside the secure network***



Washington System Center

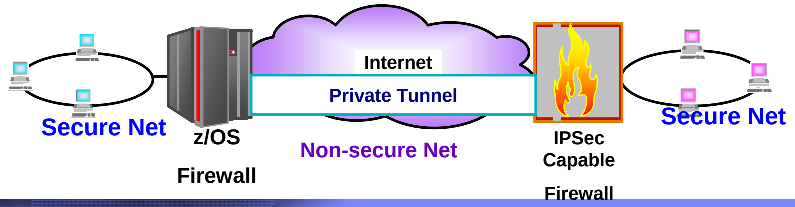
Summary

- Single most important factor affecting your firewalls security is how you configure it
  - how are firewalls access control rules defined
    - wide-open
    - nothing at all gets through
- Firewalls can provide only limited protection against attacks carried in data you're allowing into your network

Virtual Private Networks

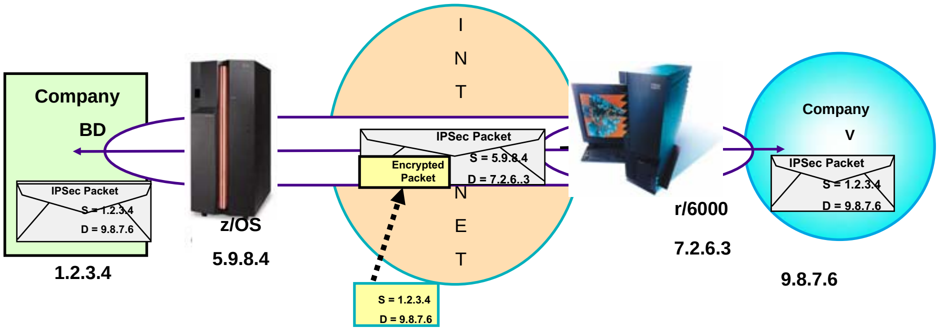
What is a Virtual Private Network

- **A Virtual Private Network consists of two or more sub-networks connected by one or more tunnels**
- **A tunnel is a mechanism for securing data between two sub-networks**
  - **authenticates**
    - data origin
    - data integrity
    - replay protection
  - **provides data privacy via encryption**



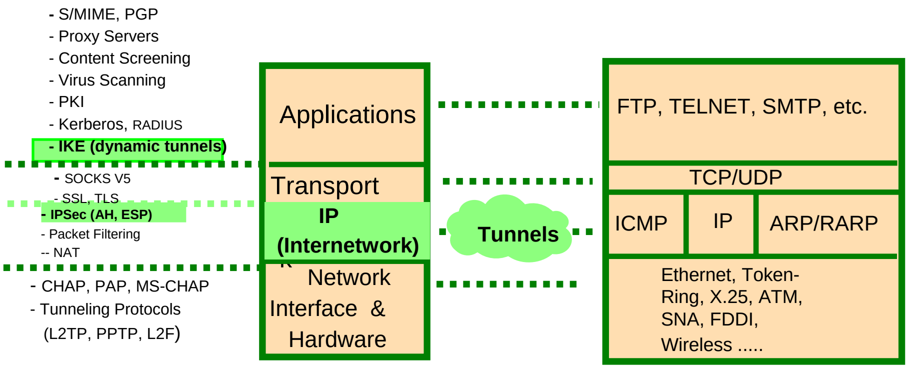
VPN Data

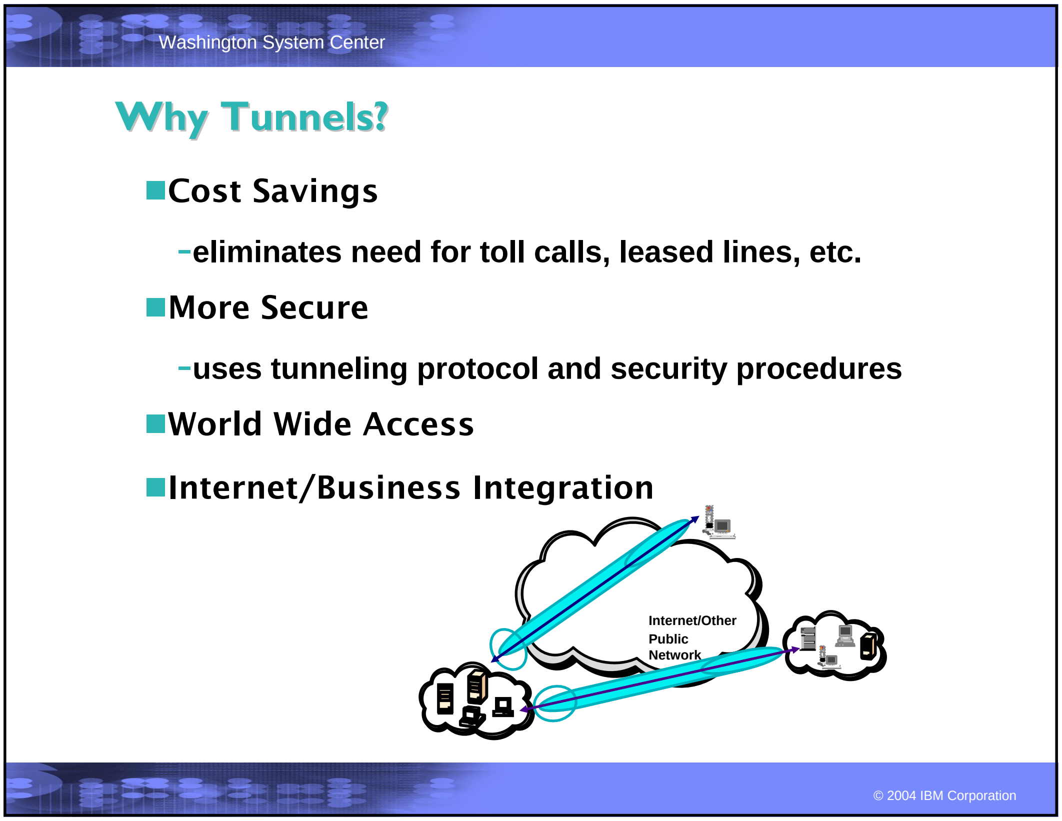
- Data sent in packets from one secure location to another are;
  - encrypted and/or authenticated at the source
  - sent in a new IP packet to the destination



TCP/IP Layers

- VPNs use IPSec (AH and ESP) protocols
- Dynamic tunnels use IPSec (ISAKMP) protocol
- Operates at the IP layer
- use of IPSec is transparent to upper layers including applications



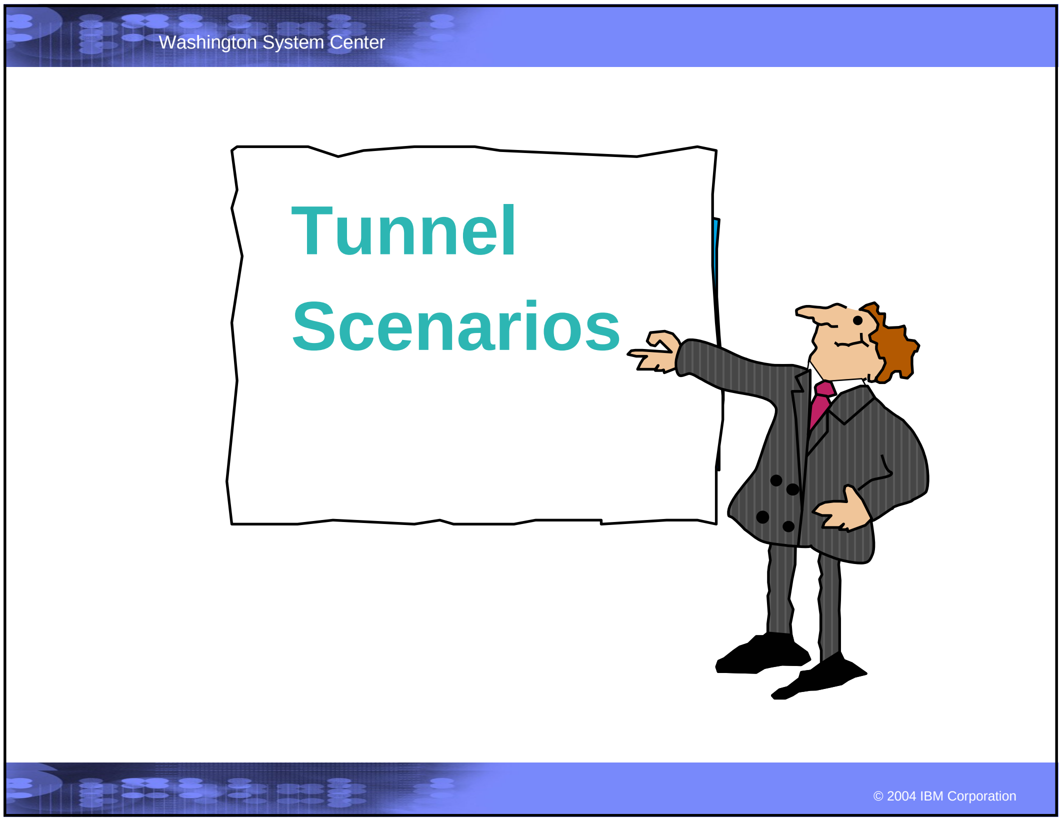


Washington System Center

Why Tunnels?

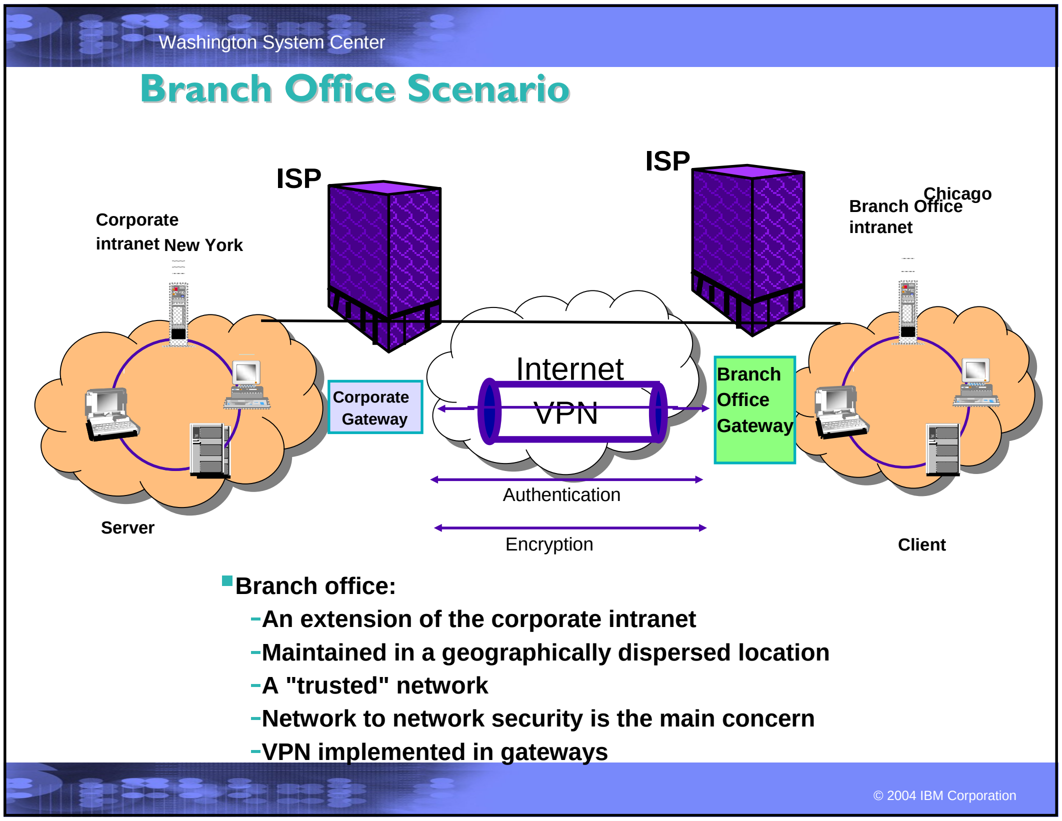
- Cost Savings
  - eliminates need for toll calls, leased lines, etc.
- More Secure
  - uses tunneling protocol and security procedures
- World Wide Access
- Internet/Business Integration

Internet/Other
Public
Network



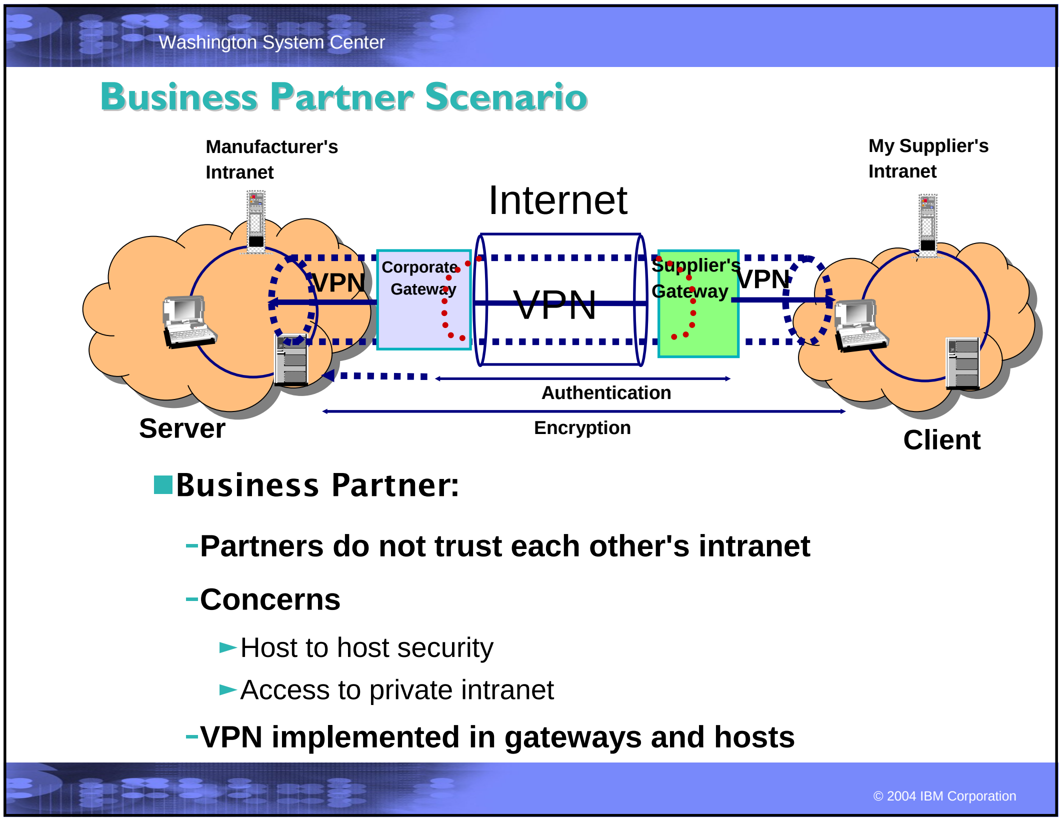
Washington System Center

Tunnel Scenarios



Branch Office Scenario

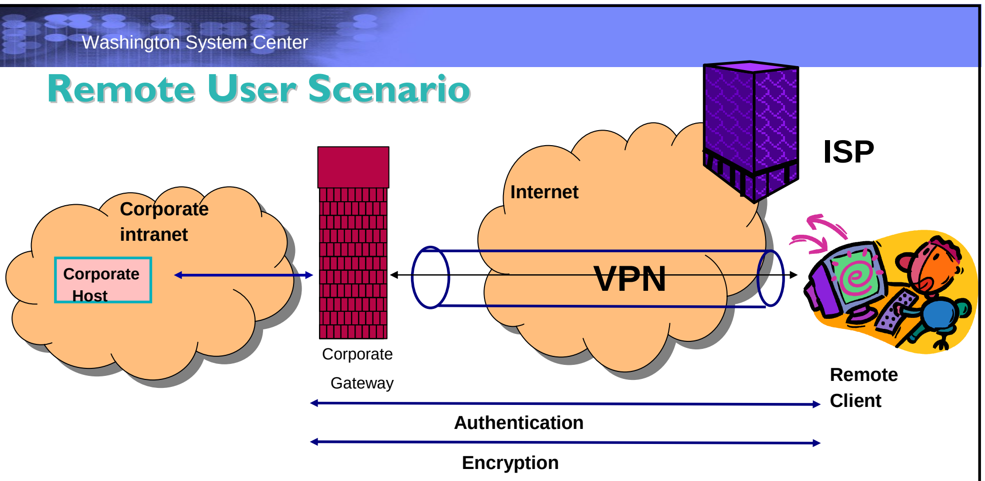
- Branch office:
  - An extension of the corporate intranet
  - Maintained in a geographically dispersed location
  - A "trusted" network
  - Network to network security is the main concern
  - VPN implemented in gateways



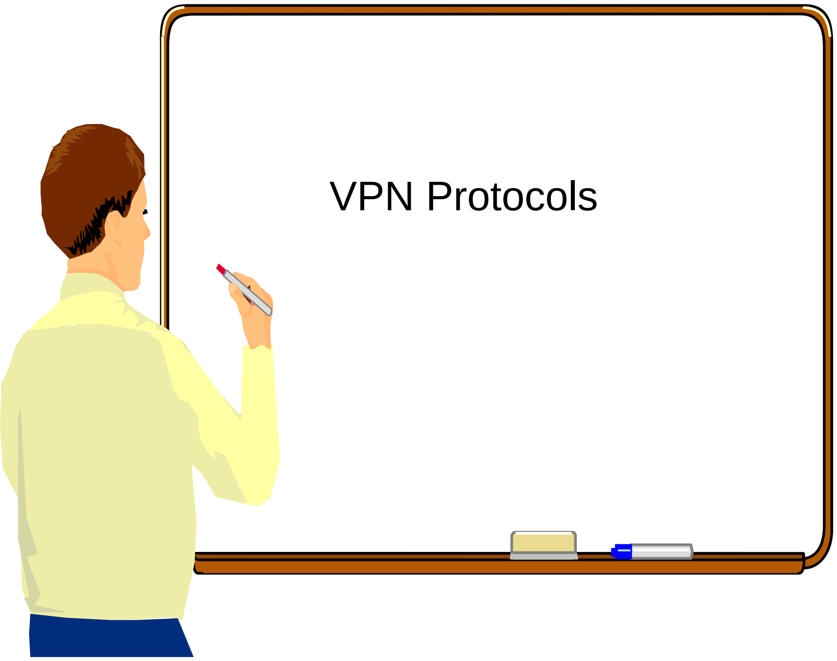
Business Partner Scenario

- Business Partner:
  - Partners do not trust each other's intranet
  - Concerns
    - Host to host security
    - Access to private intranet
  - VPN implemented in gateways and hosts

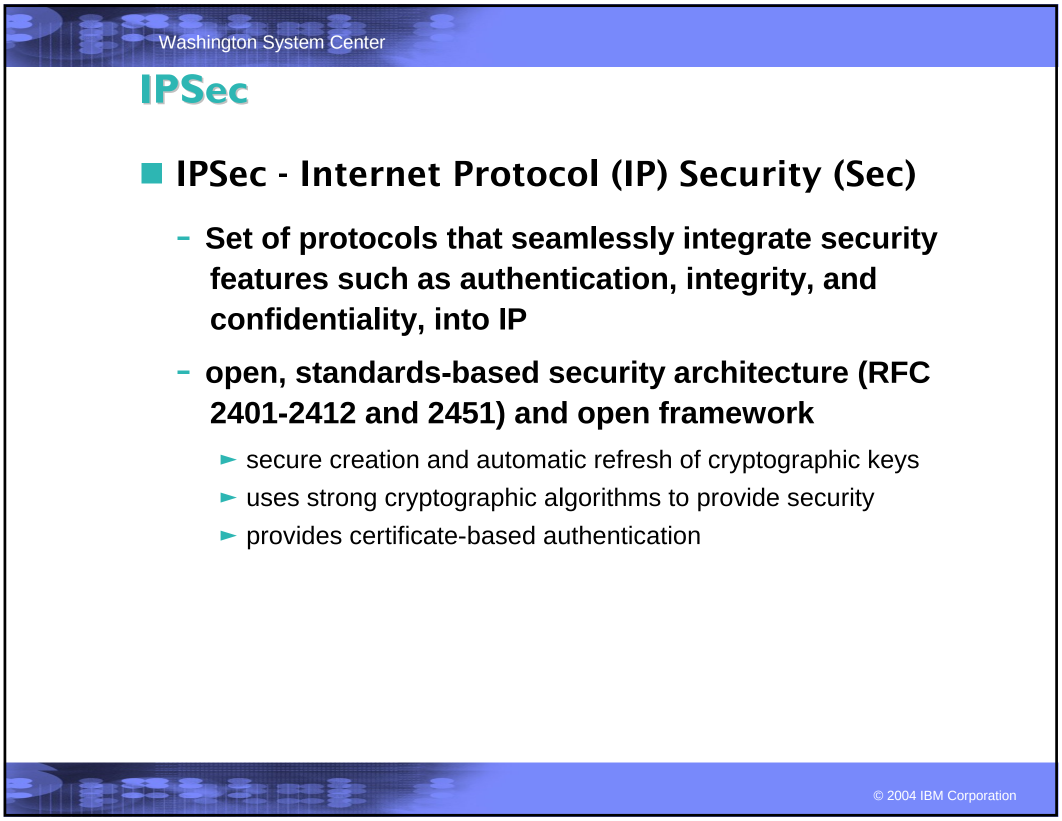
Remote User Scenario



- **Remote User:**
  - **An extension of the corporate intranet**
  - **A "trusted" user, not IP address**
  - **Internet Service Provider may not be trusted**
  - **VPN implemented in corporate gateway and remote user's host**

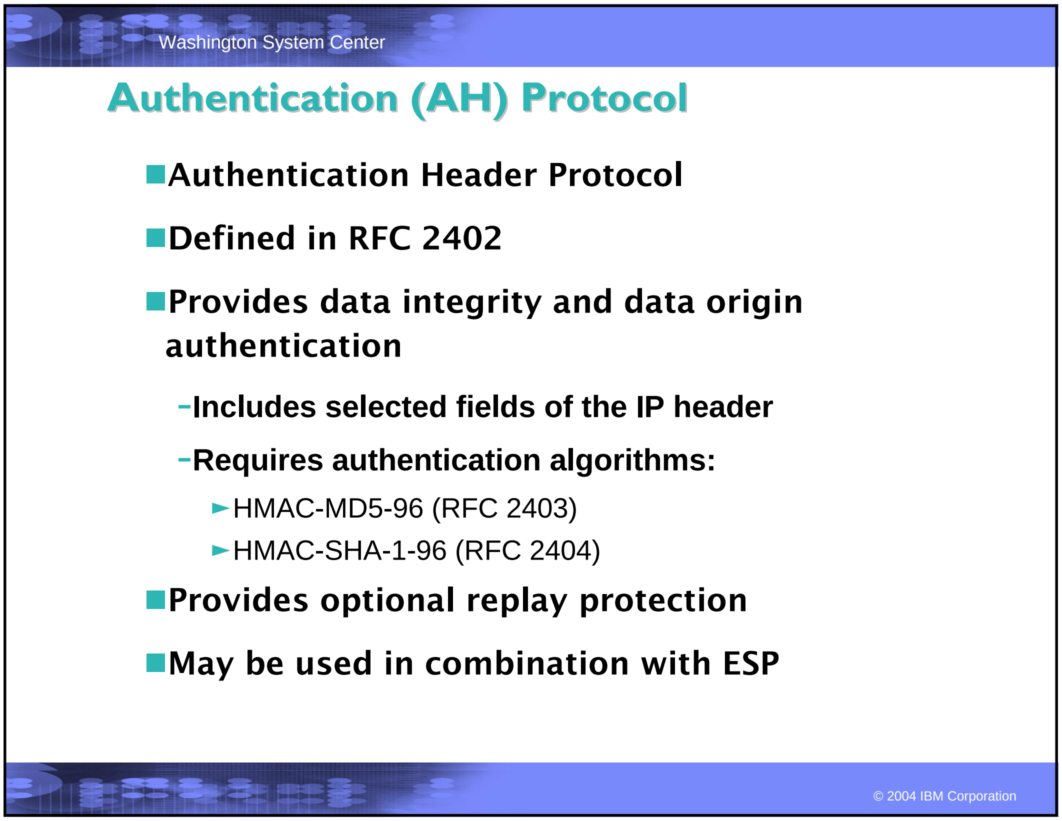


VPN Protocols



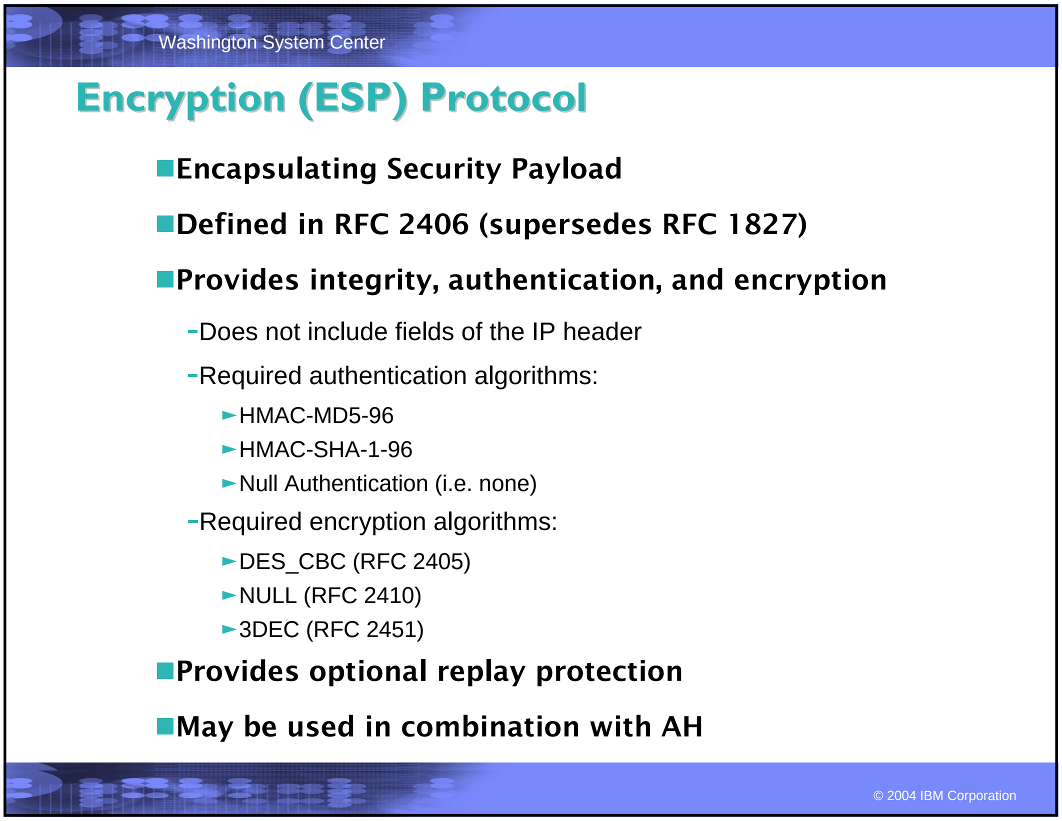
IPSec

- IPSec - Internet Protocol (IP) Security (Sec)
  - Set of protocols that seamlessly integrate security features such as authentication, integrity, and confidentiality, into IP
  - open, standards-based security architecture (RFC 2401-2412 and 2451) and open framework
    - ► secure creation and automatic refresh of cryptographic keys
    - ► uses strong cryptographic algorithms to provide security
    - ► provides certificate-based authentication



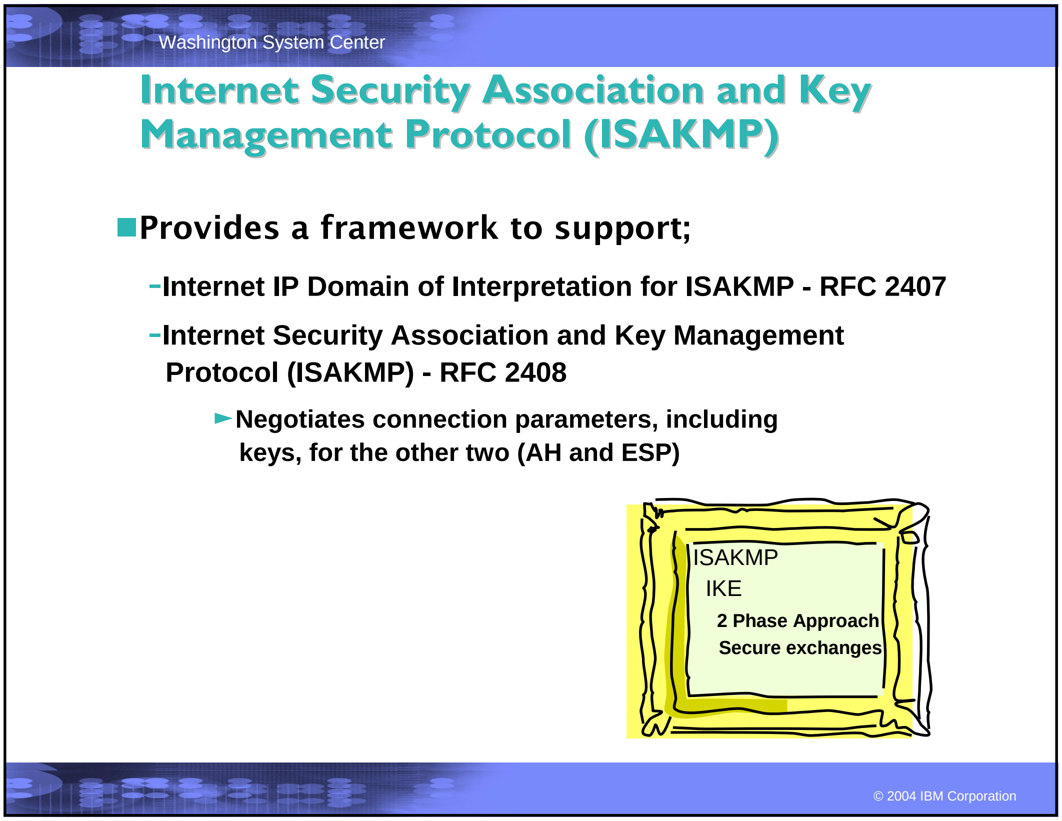
Authentication (AH) Protocol

- Authentication Header Protocol
- Defined in RFC 2402
- Provides data integrity and data origin authentication
  - Includes selected fields of the IP header
  - Requires authentication algorithms:
    - ►HMAC-MD5-96 (RFC 2403)
    - ►HMAC-SHA-1-96 (RFC 2404)
- Provides optional replay protection
- May be used in combination with ESP



Encryption (ESP) Protocol

- Encapsulating Security Payload
- Defined in RFC 2406 (supersedes RFC 1827)
- Provides integrity, authentication, and encryption
  - Does not include fields of the IP header
  - Required authentication algorithms:
    - HMAC-MD5-96
    - HMAC-SHA-1-96
    - Null Authentication (i.e. none)
  - Required encryption algorithms:
    - DES_CBC (RFC 2405)
    - NULL (RFC 2410)
    - 3DEC (RFC 2451)
- Provides optional replay protection
- May be used in combination with AH



Internet Security Association and Key Management Protocol (ISAKMP)

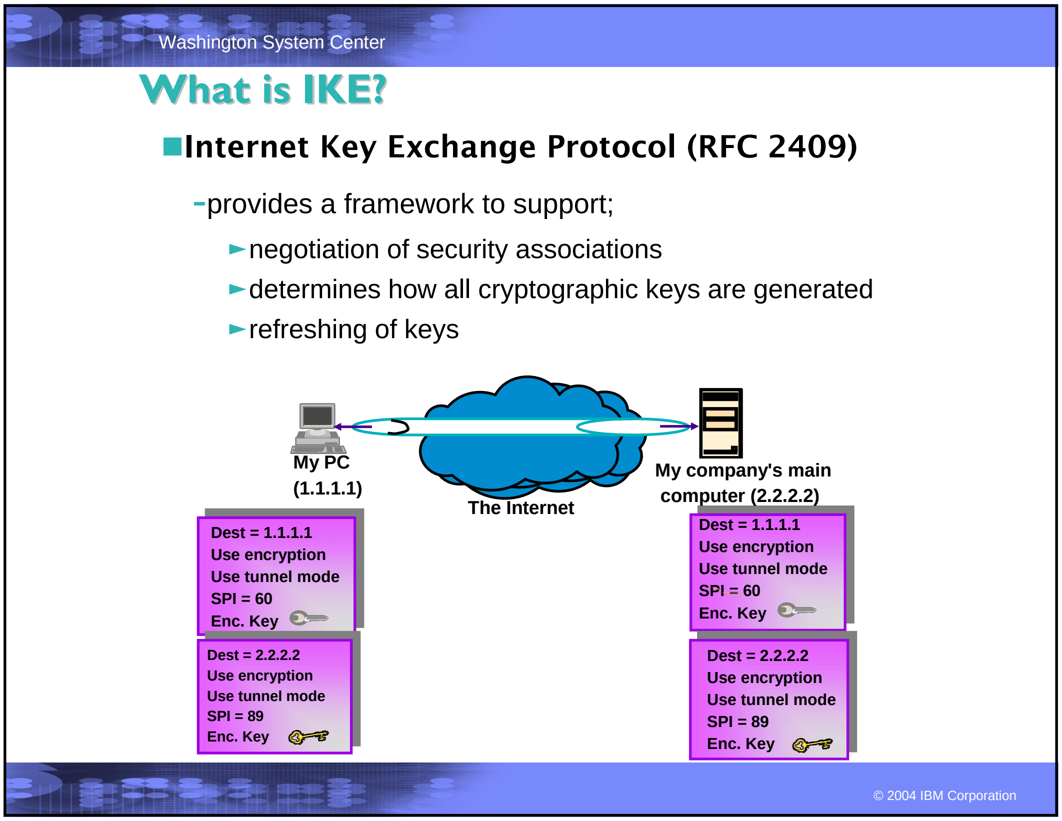
- Provides a framework to support;
  - Internet IP Domain of Interpretation for ISAKMP - RFC 2407
  - Internet Security Association and Key Management Protocol (ISAKMP) - RFC 2408
    - Negotiates connection parameters, including keys, for the other two (AH and ESP)

ISAKMP

IKE

2 Phase Approach

Secure exchanges



Washington System Center

What is IKE?

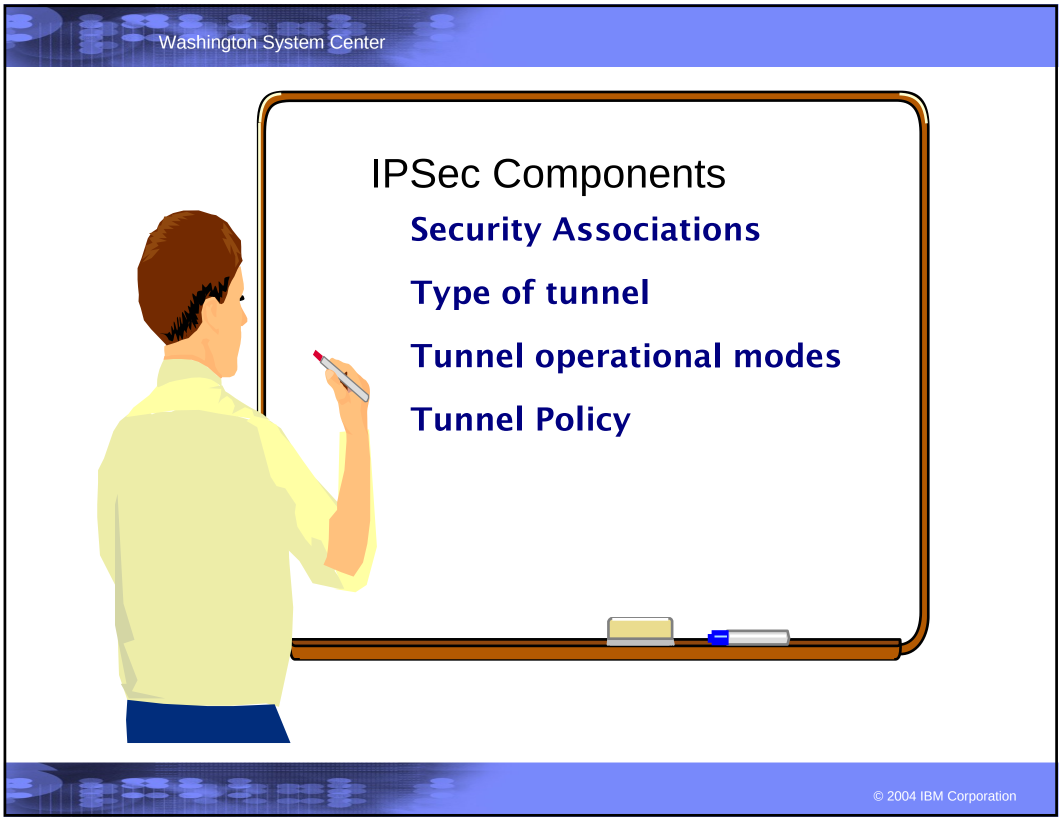
- Internet Key Exchange Protocol (RFC 2409)
  - provides a framework to support;
    - negotiation of security associations
    - determines how all cryptographic keys are generated
    - refreshing of keys

Dest = 1.1.1.1
Use encryption
Use tunnel mode
SPI = 60
Enc. Key

Dest = 2.2.2.2
Use encryption
Use tunnel mode
SPI = 89
Enc. Key

Dest = 1.1.1.1
Use encryption
Use tunnel mode
SPI = 60
Enc. Key

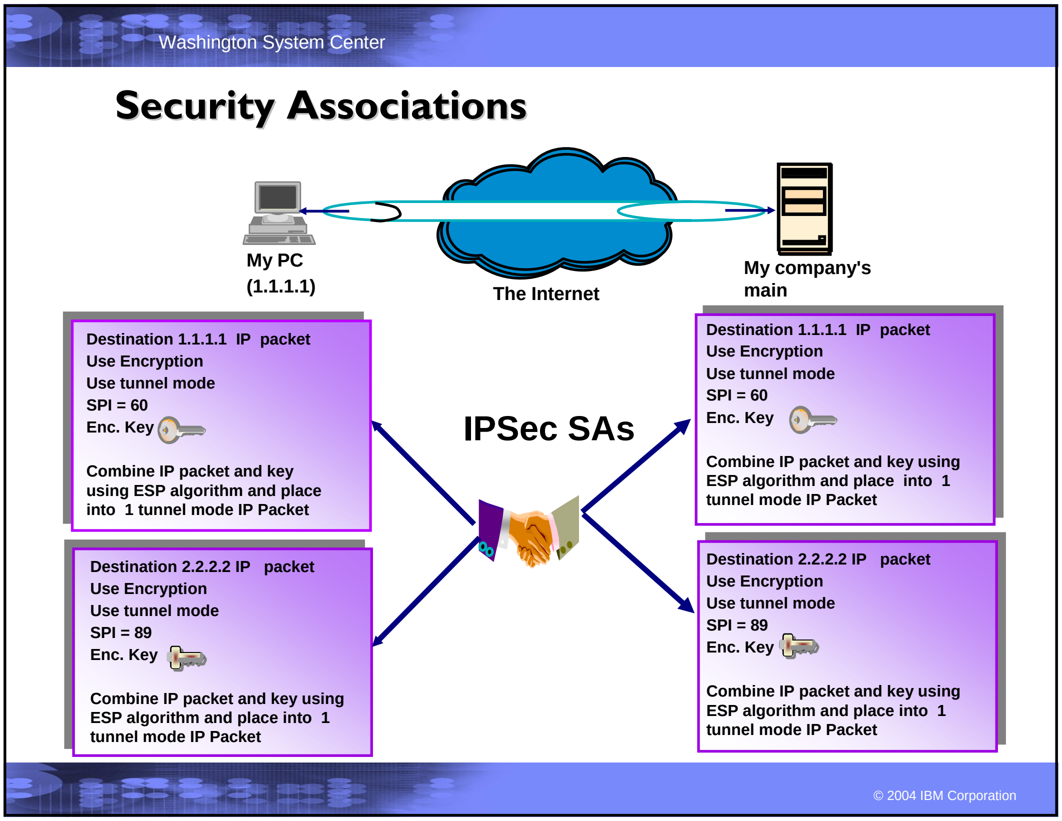
Dest = 2.2.2.2
Use encryption
Use tunnel mode
SPI = 89
Enc. Key



Washington System Center

IPSec Components

- Security Associations
- Type of tunnel
- Tunnel operational modes
- Tunnel Policy



Security Associations

Destination 1.1.1.1 IP packet
Use Encryption
Use tunnel mode
SPI = 60
Enc. Key

Combine IP packet and key using ESP algorithm and place into 1 tunnel mode IP Packet

Destination 2.2.2.2 IP packet
Use Encryption
Use tunnel mode
SPI = 89
Enc. Key

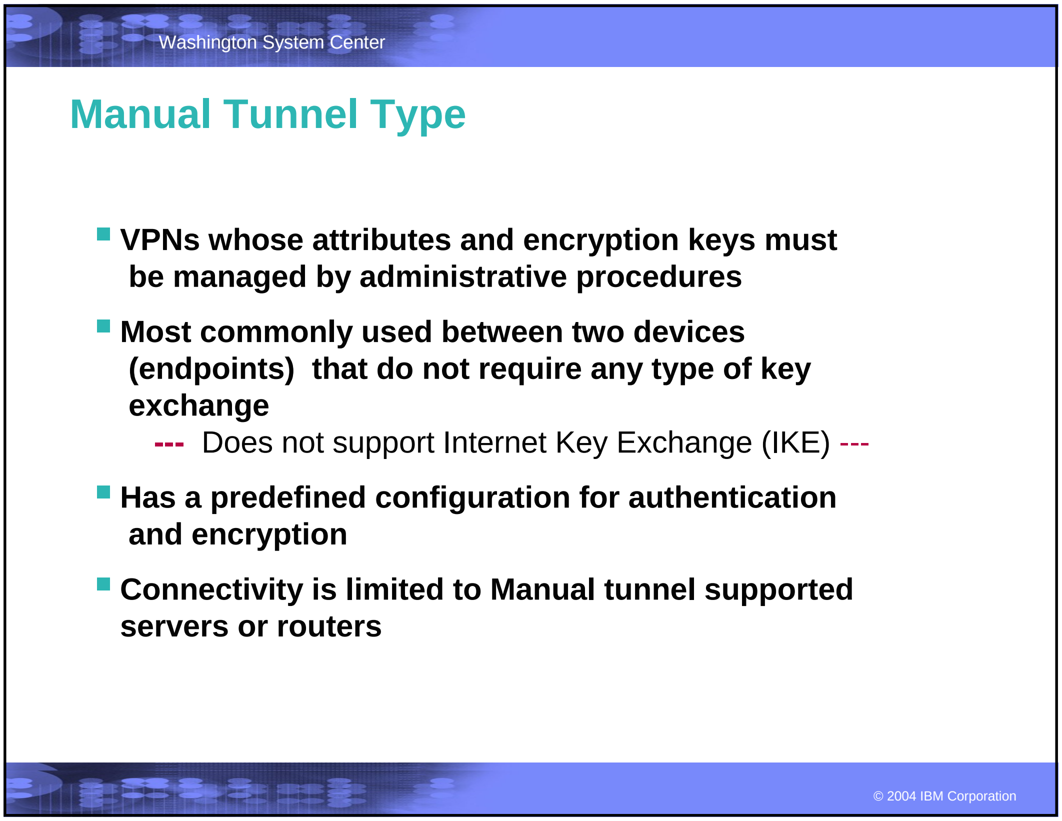
Combine IP packet and key using ESP algorithm and place into 1 tunnel mode IP Packet

Destination 1.1.1.1 IP packet
Use Encryption
Use tunnel mode
SPI = 60
Enc. Key

Combine IP packet and key using ESP algorithm and place into 1 tunnel mode IP Packet

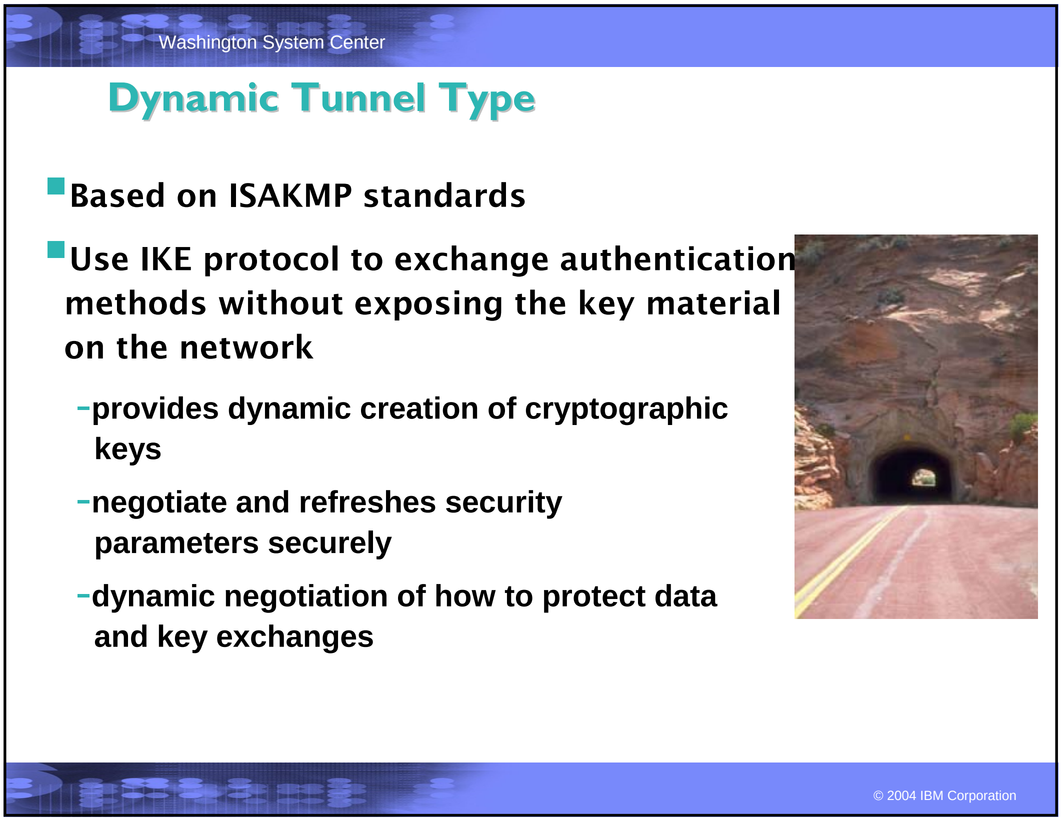
Destination 2.2.2.2 IP packet
Use Encryption
Use tunnel mode
SPI = 89
Enc. Key

Combine IP packet and key using ESP algorithm and place into 1 tunnel mode IP Packet



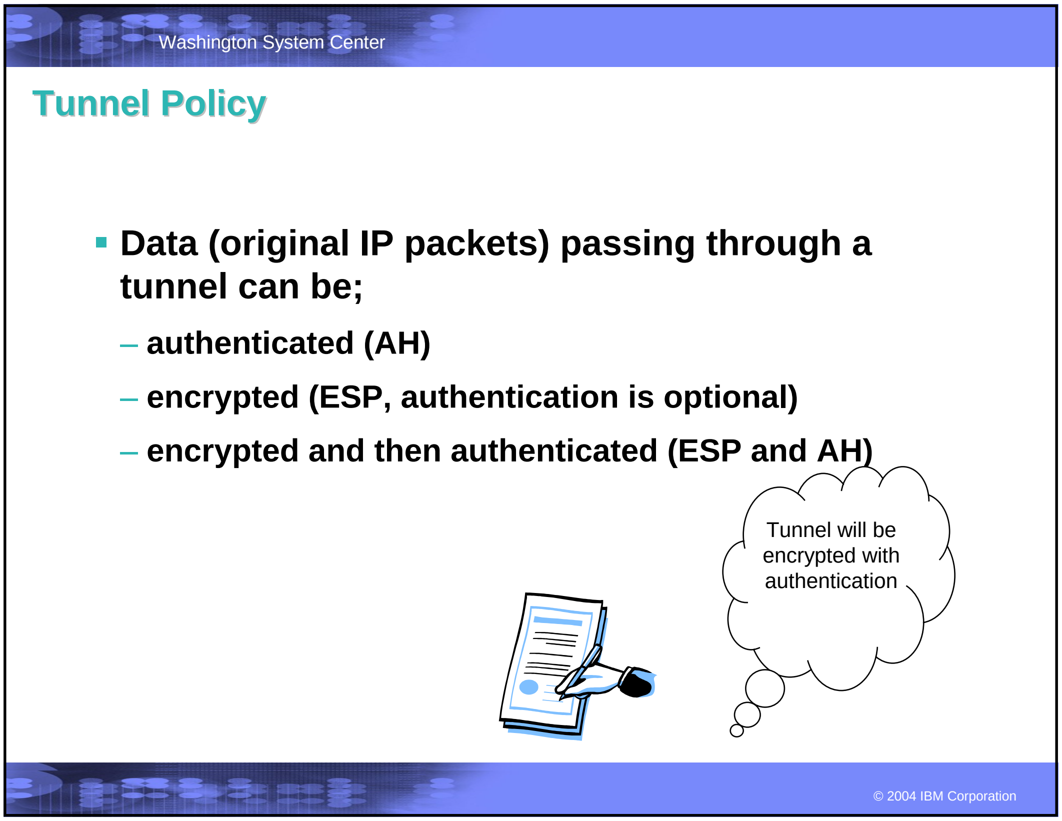
Manual Tunnel Type

- VPNs whose attributes and encryption keys must be managed by administrative procedures
- Most commonly used between two devices (endpoints) that do not require any type of key exchange
  --- Does not support Internet Key Exchange (IKE) ---
- Has a predefined configuration for authentication and encryption
- Connectivity is limited to Manual tunnel supported servers or routers



Dynamic Tunnel Type

- Based on ISAKMP standards
- Use IKE protocol to exchange authentication methods without exposing the key material on the network
  - provides dynamic creation of cryptographic keys
  - negotiate and refreshes security parameters securely
  - dynamic negotiation of how to protect data and key exchanges



Tunnel Policy

- Data (original IP packets) passing through a tunnel can be;
  - authenticated (AH)
  - encrypted (ESP, authentication is optional)
  - encrypted and then authenticated (ESP and AH)

Tunnel will be encrypted with authentication

Tunnel Operational Modes

- Original packet

IP Header	TCP Hdr	Data

- Transport mode

IP Header	IPSec Header	TCP Hdr	Data

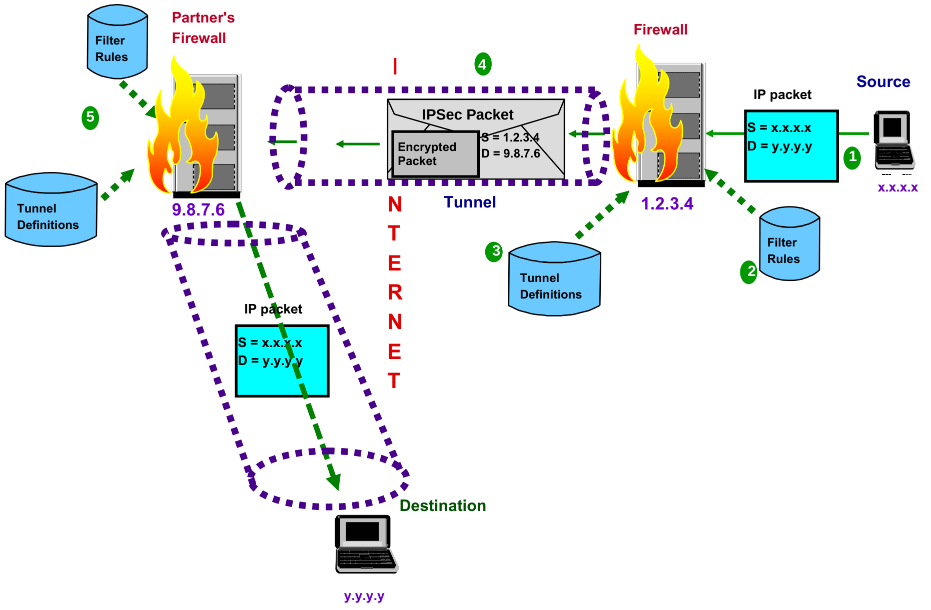
  - original data is protected but certain header fields are not

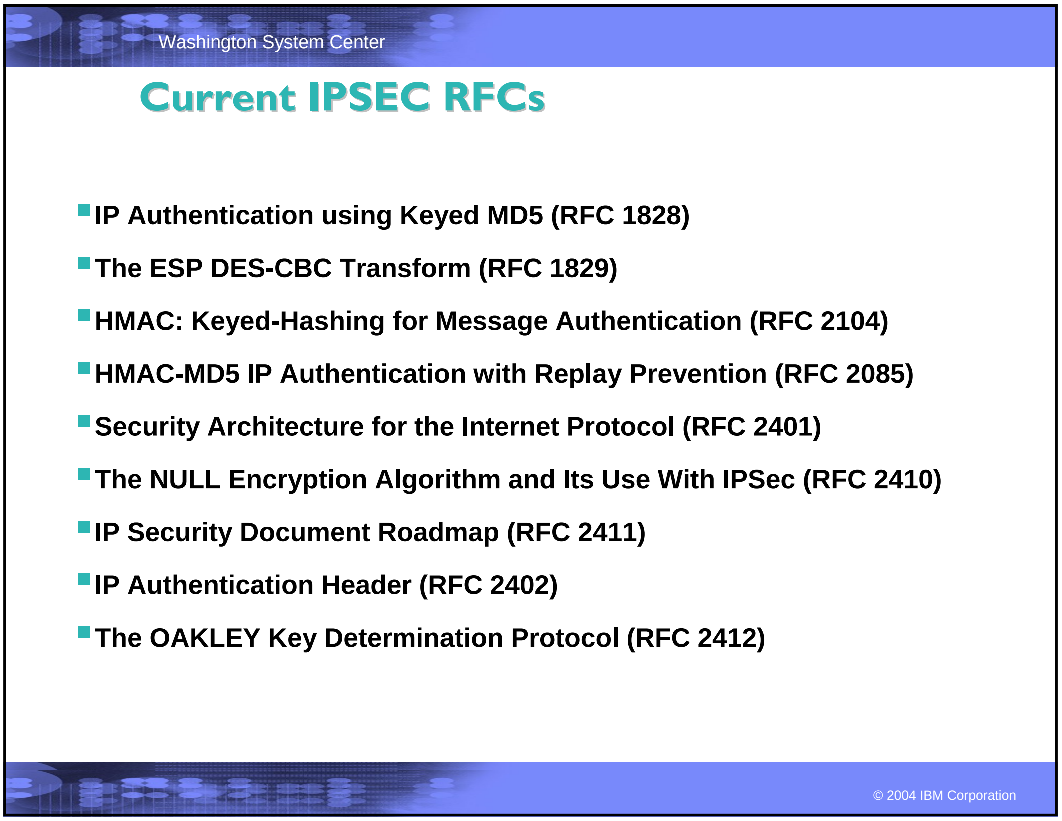
- Tunnel

New IP Hdr	IPSec Header	IP Header	TCP Hdr	Data

  - protects the entire IP packet
  - a new IP header and IPSec header are placed in front of the original IP packet

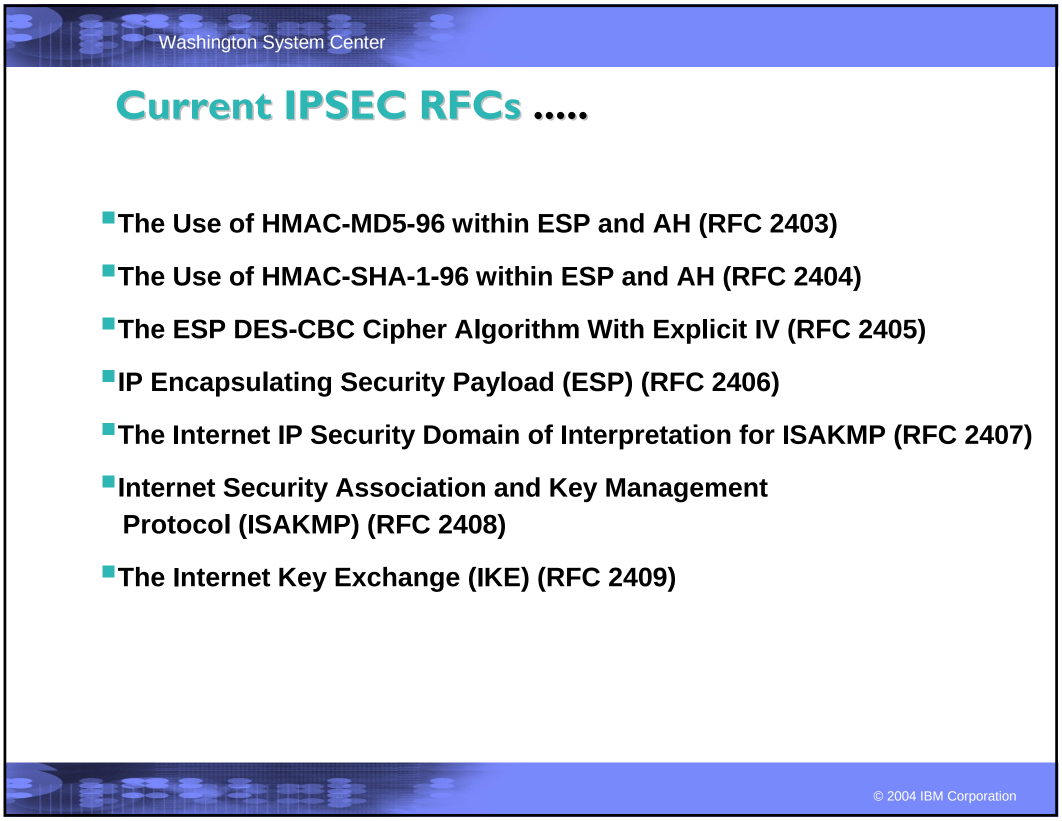
Secure IP Tunnels





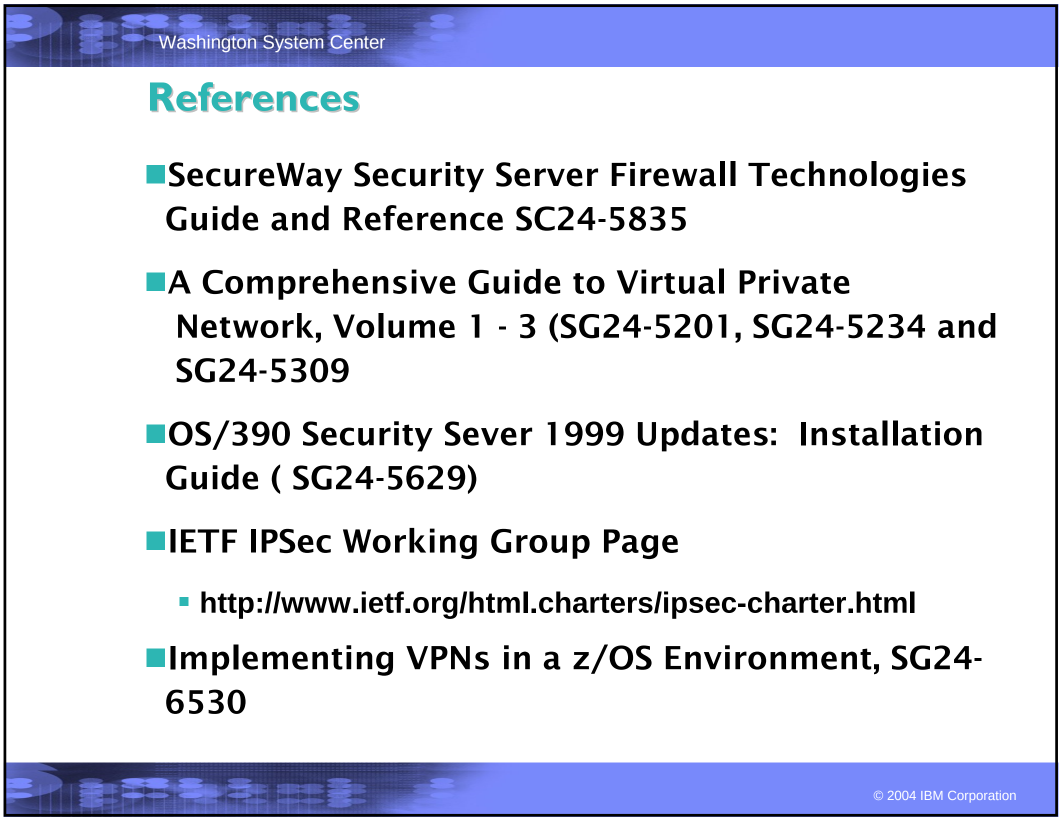
Current IPSEC RFCs

- IP Authentication using Keyed MD5 (RFC 1828)
- The ESP DES-CBC Transform (RFC 1829)
- HMAC: Keyed-Hashing for Message Authentication (RFC 2104)
- HMAC-MD5 IP Authentication with Replay Prevention (RFC 2085)
- Security Architecture for the Internet Protocol (RFC 2401)
- The NULL Encryption Algorithm and Its Use With IPSec (RFC 2410)
- IP Security Document Roadmap (RFC 2411)
- IP Authentication Header (RFC 2402)
- The OAKLEY Key Determination Protocol (RFC 2412)



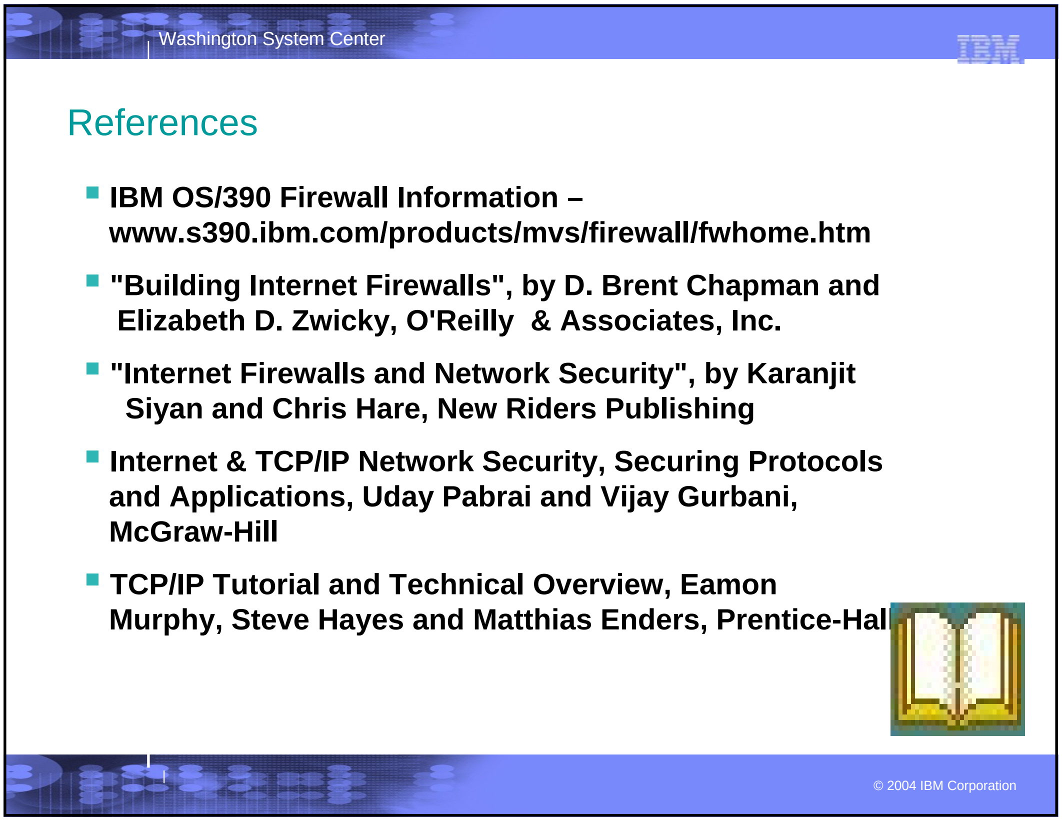
Current IPSEC RFCs .....

- The Use of HMAC-MD5-96 within ESP and AH (RFC 2403)
- The Use of HMAC-SHA-1-96 within ESP and AH (RFC 2404)
- The ESP DES-CBC Cipher Algorithm With Explicit IV (RFC 2405)
- IP Encapsulating Security Payload (ESP) (RFC 2406)
- The Internet IP Security Domain of Interpretation for ISAKMP (RFC 2407)
- Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
- The Internet Key Exchange (IKE) (RFC 2409)



References

- SecureWay Security Server Firewall Technologies Guide and Reference SC24-5835
- A Comprehensive Guide to Virtual Private Network, Volume 1 - 3 (SG24-5201, SG24-5234 and SG24-5309
- OS/390 Security Sever 1999 Updates: Installation Guide (SG24-5629)
- IETF IPSec Working Group Page
  - http://www.ietf.org/html.charters/ipsec-charter.html
- Implementing VPNs in a z/OS Environment, SG24-6530



References

- IBM OS/390 Firewall Information – www.s390.ibm.com/products/mvs/firewall/fwhome.htm
- "Building Internet Firewalls", by D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates, Inc.
- "Internet Firewalls and Network Security", by Karanjit Siyan and Chris Hare, New Riders Publishing
- Internet & TCP/IP Network Security, Securing Protocols and Applications, Uday Pabrai and Vijay Gurbani, McGraw-Hill
- TCP/IP Tutorial and Technical Overview, Eamon Murphy, Steve Hayes and Matthias Enders, Prentice-Hall

References ....

- ***Secure e-business in TCP/IP Networks on OS/390 and z/OS***
  (SG24-5383)

- ***IBM Communications Server for OS/390 V2R10 TCP/IP***

- ***Implementation Guide Volume 1: Configuration and Routing (SG24-5227)***

- ***SecureWay Security Server Firewall Technologies Guide and Reference,*** **SC24-5835**