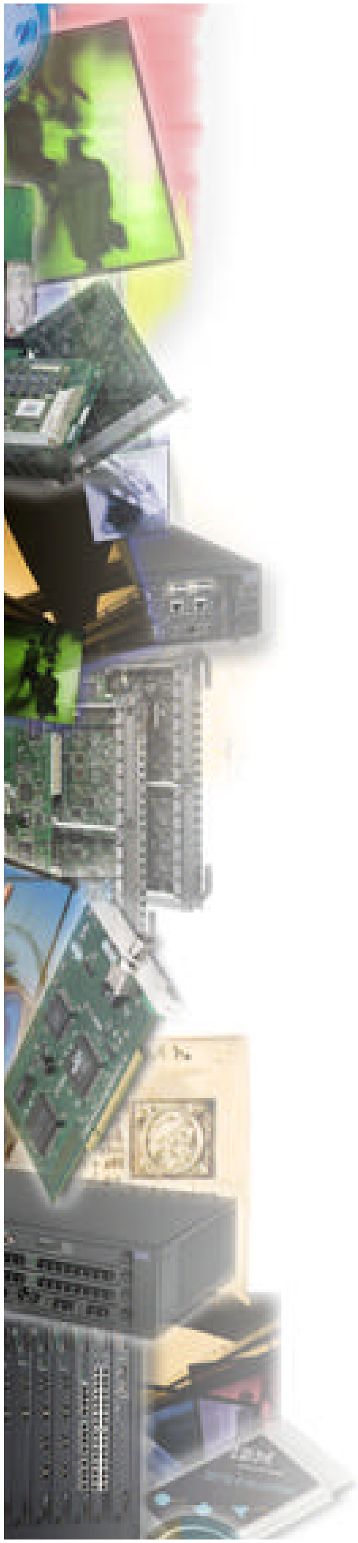
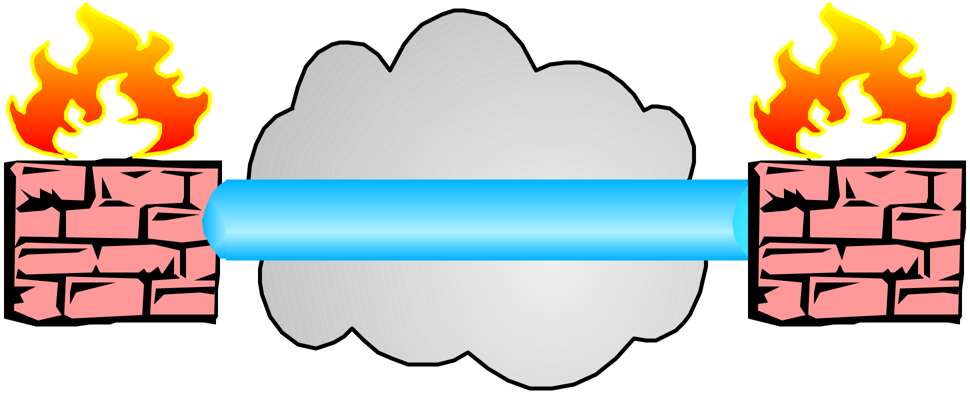
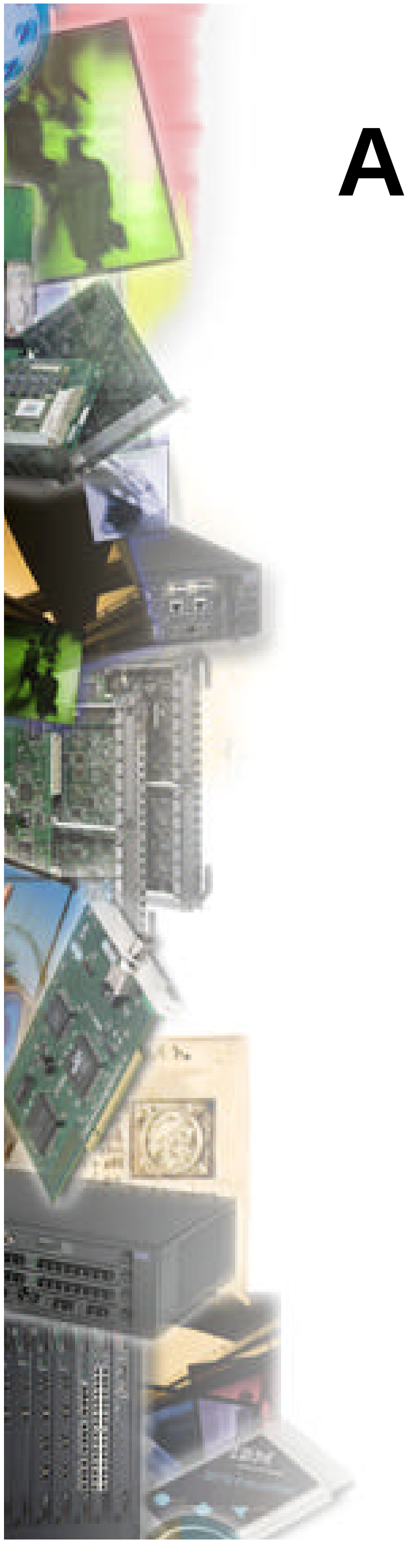


Inside the VPN Tunnel

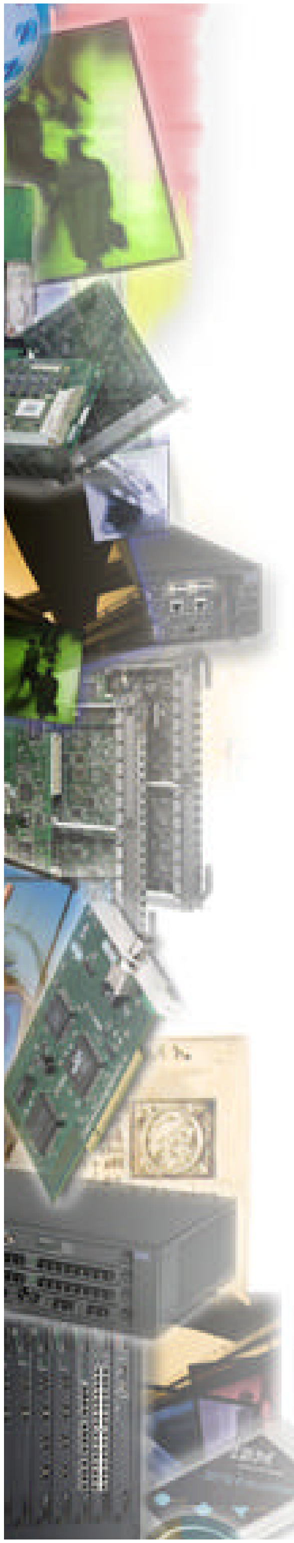
Jeff Crume
IBM Advanced Technical Support
crume@us.ibm.com



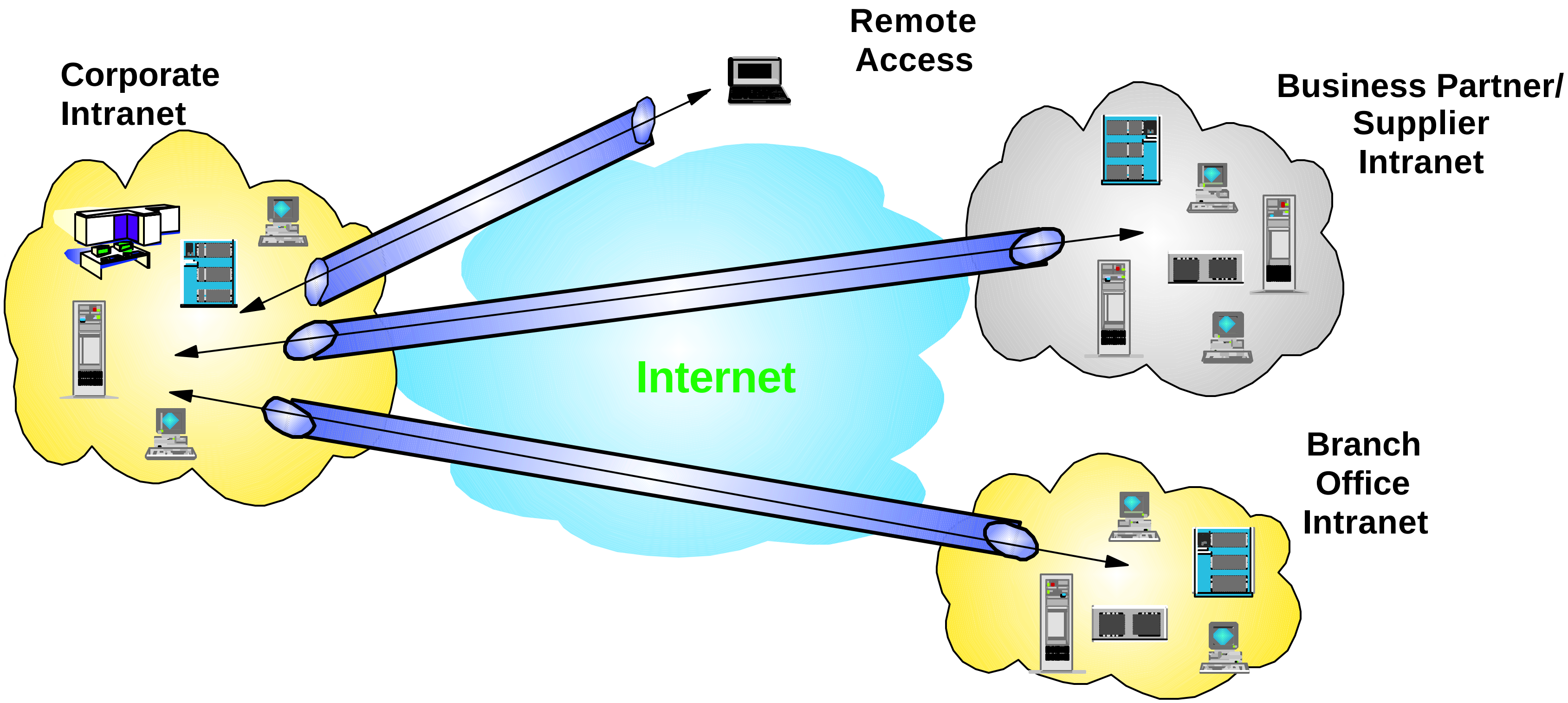


Agenda

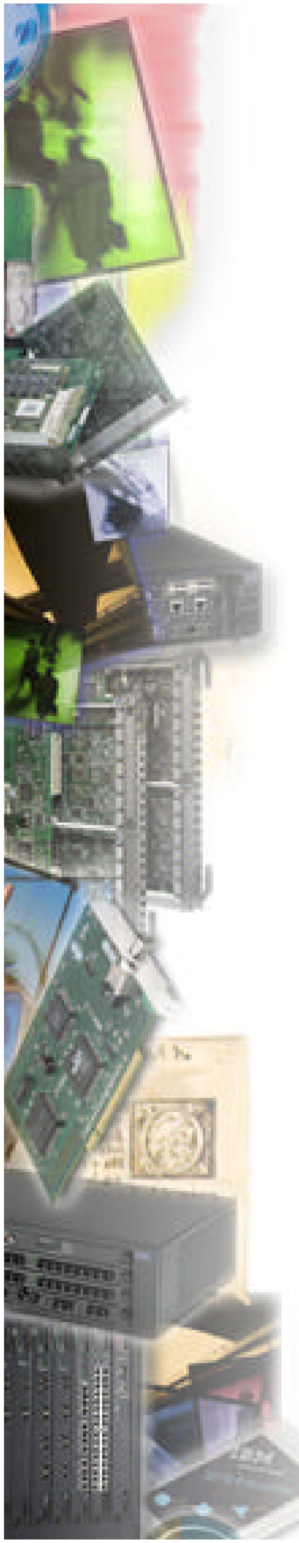
- Introduction
  - Why VPN's?
  - VPN Issues
- VPN Technologies
- IPSec Tutorial
  - IPSec components
  - Cryptography & Digital Certificates
  - IPSec options
- Interoperability
- VPN Management
- Summary



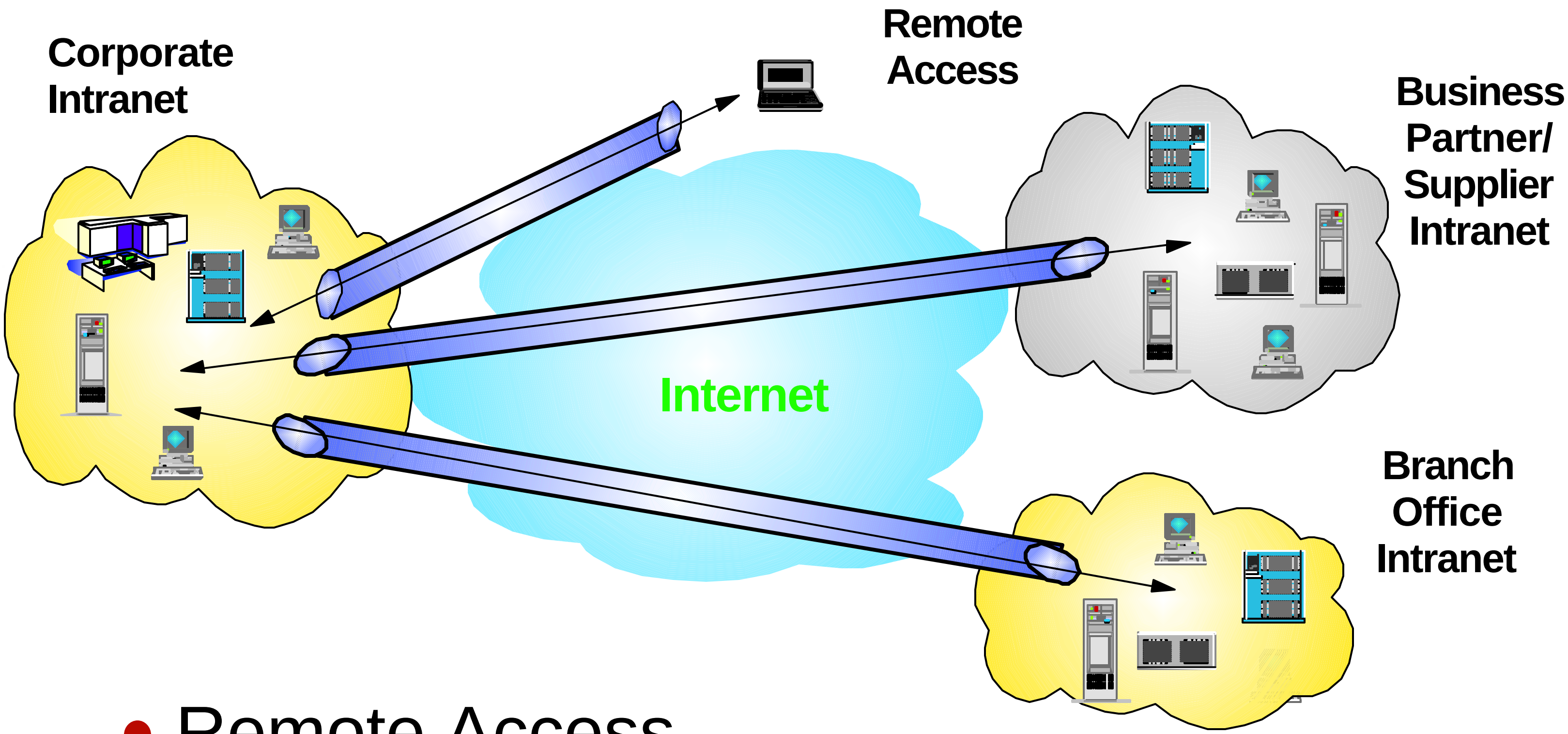
What is a VPN?



- A VPN (Virtual Private Network) is an extension of an enterprise's private intranet, across a public network (such as the Internet), through the creation of a ***secure***, authenticated and encrypted "tunnel"

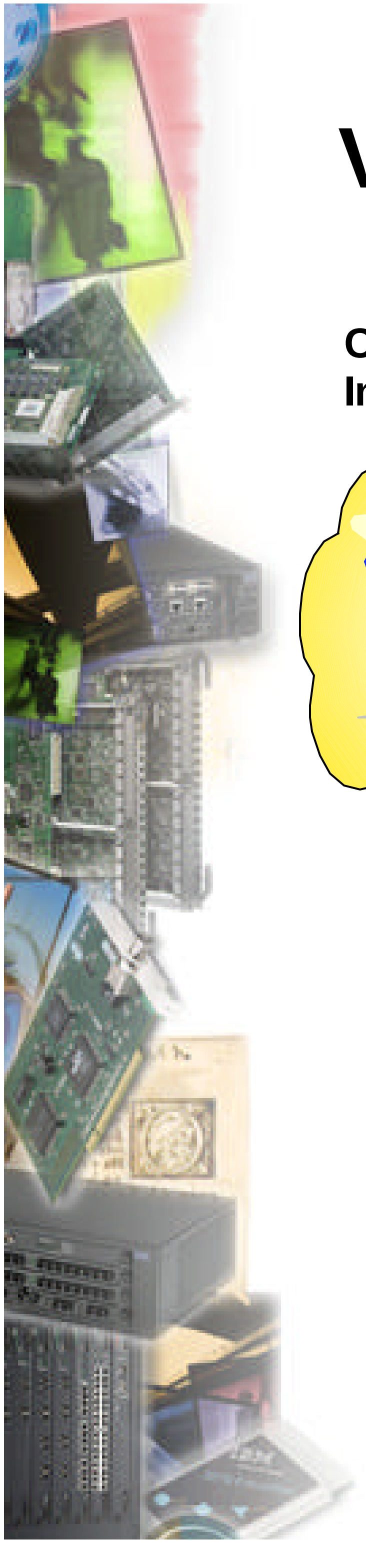


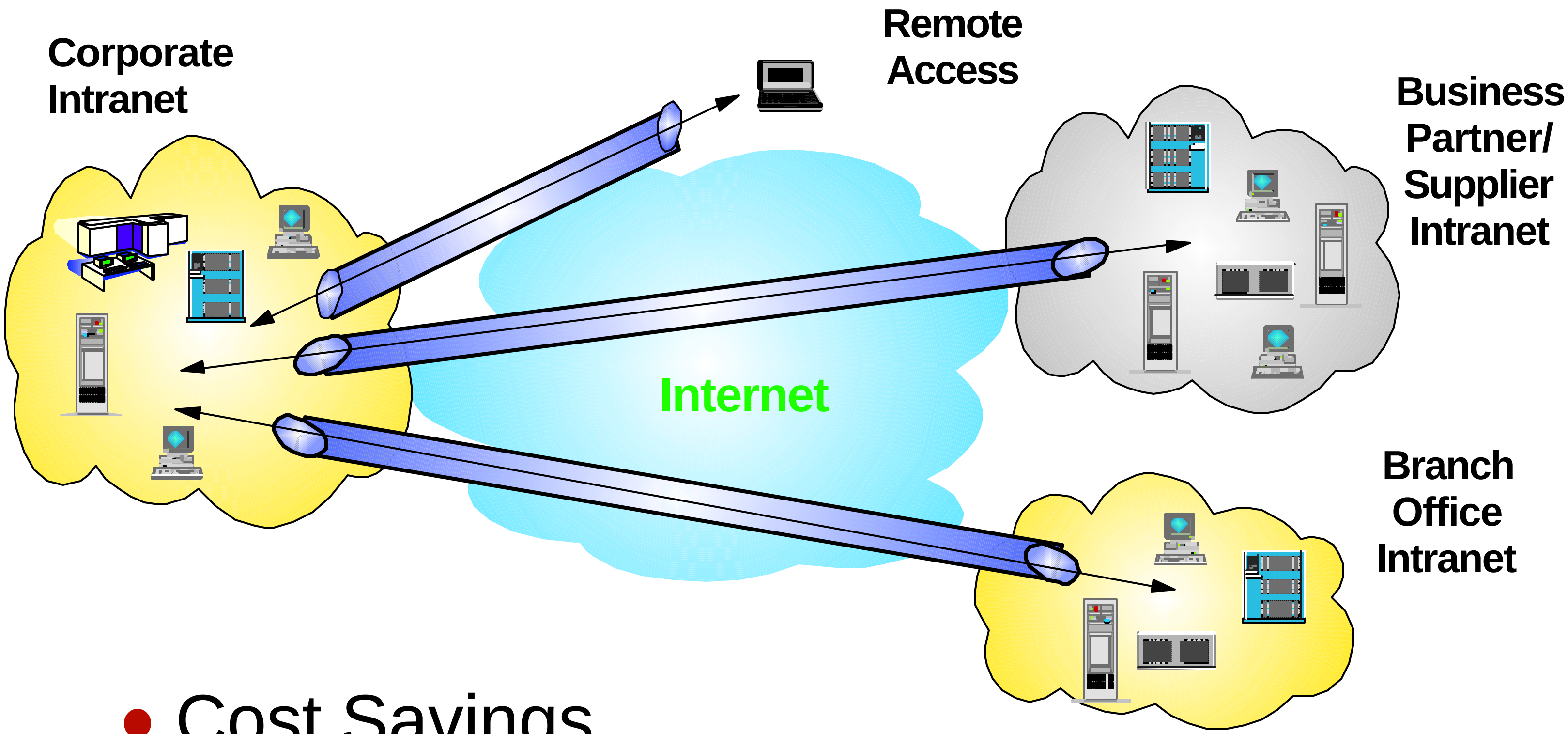
VPN Basic Applications



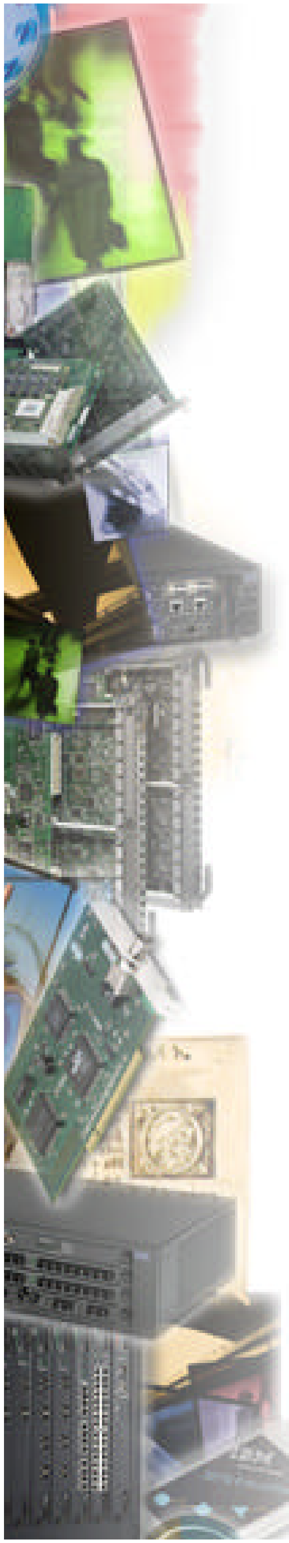
- Remote Access
- Site-to-Site Connectivity
- Extranet
- Internal Controls

VPN Value

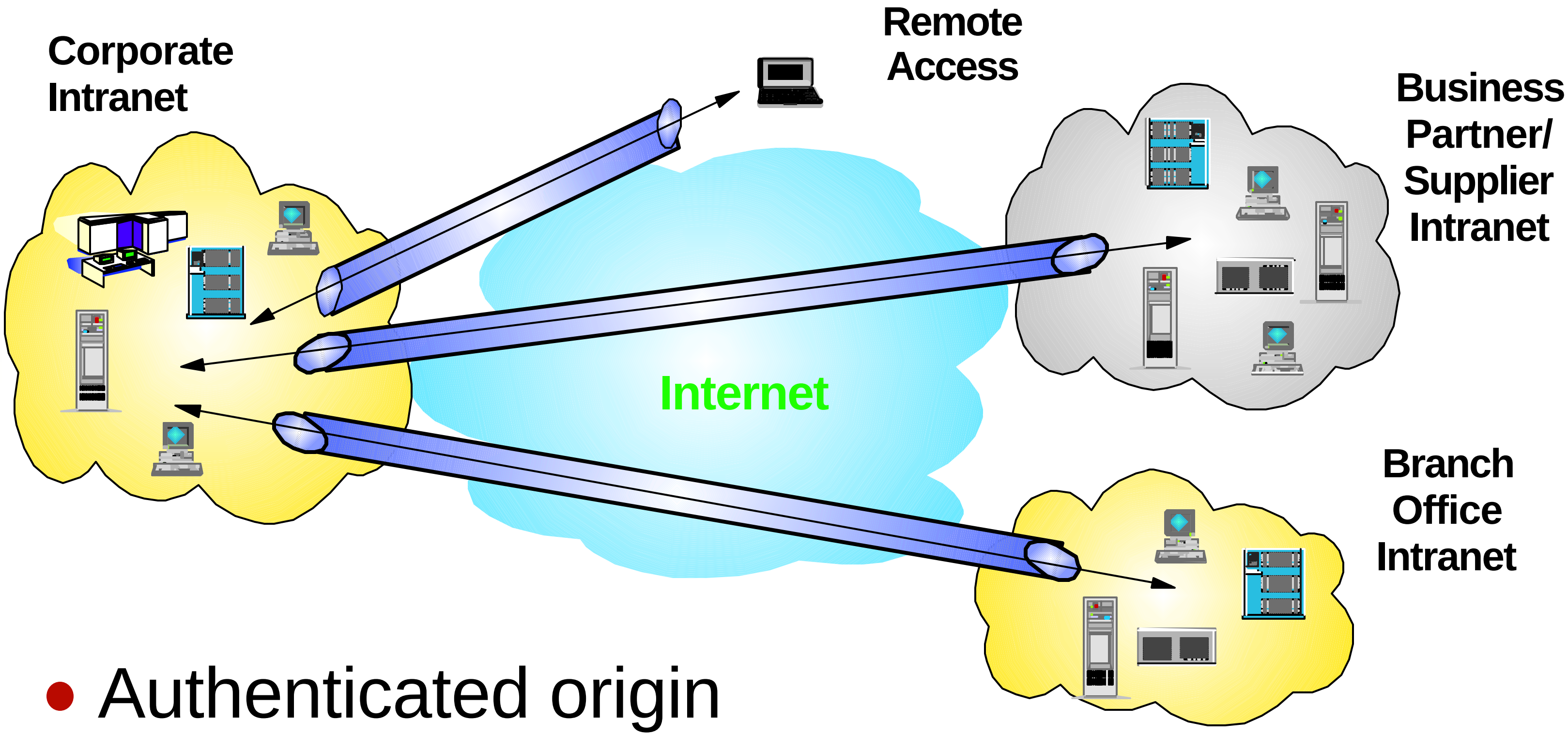




- Cost Savings
  - 20%-80% according to Infonetics Research study
- Easy, secure access to enterprise networks and resources
- Worldwide access



VPN Issues



Corporate Intranet

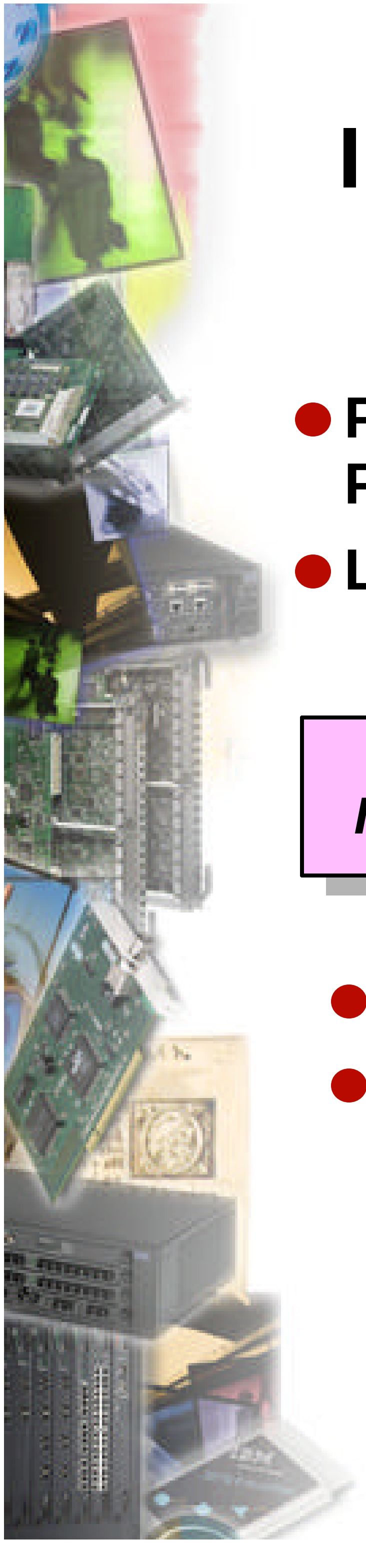
Remote Access

Business Partner/ Supplier Intranet

Internet

Branch Office Intranet

- Authenticated origin
  - Is the sender/receiver they claim to be?
- Data integrity
  - Was the data tampered with during transmission?
- Data confidentiality
  - Can anyone else read the message?
- Key management



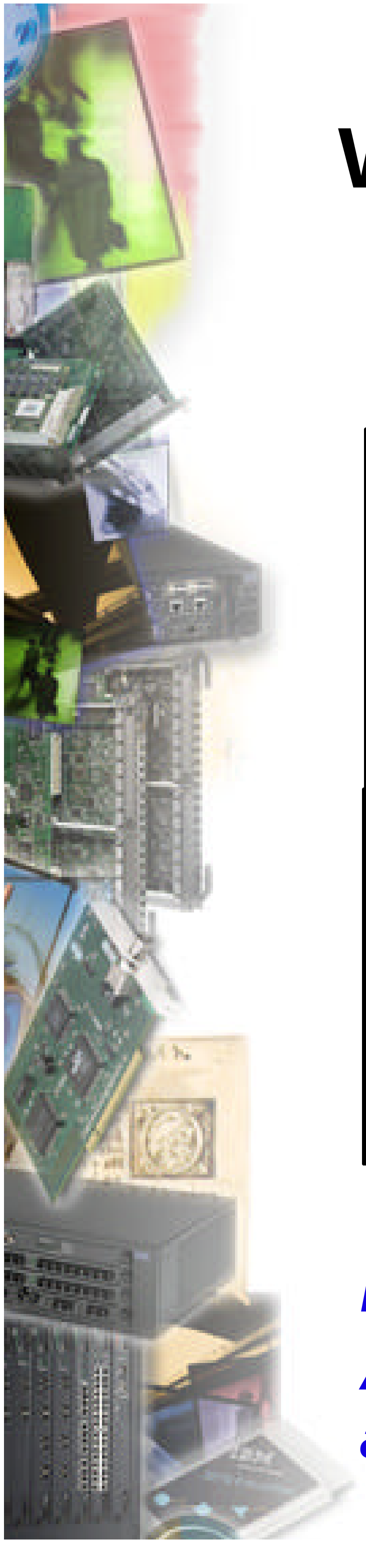
Internet *"VPN"* Technologies

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F)

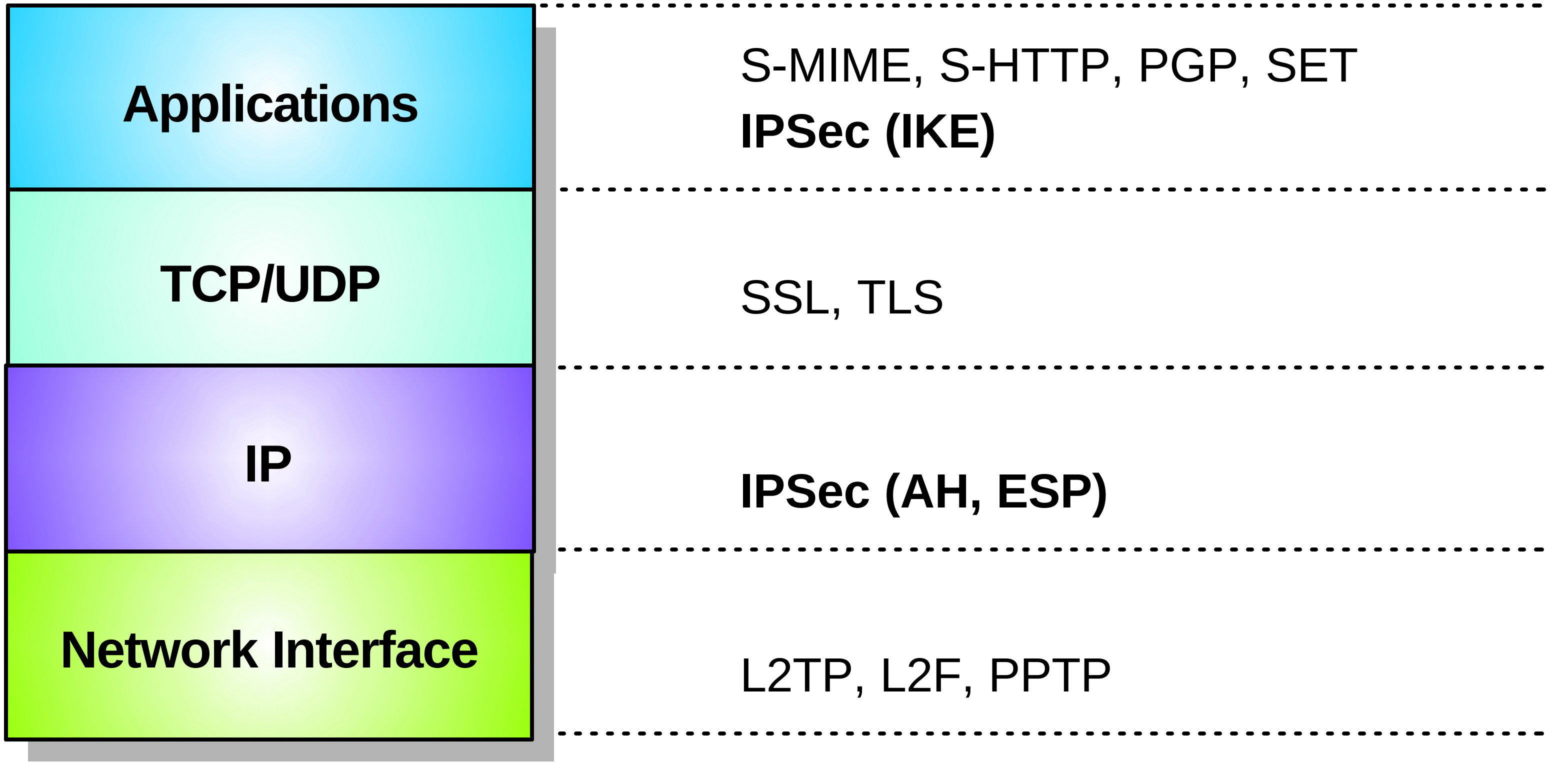
- Layer 2 Tunneling Protocol (L2TP)

The Above Technologies can transport Multiprotocol Data over the Internet, however they lack inherent Authentication and Encryption.

- SSL
- IP Security Protocol (IPSec)



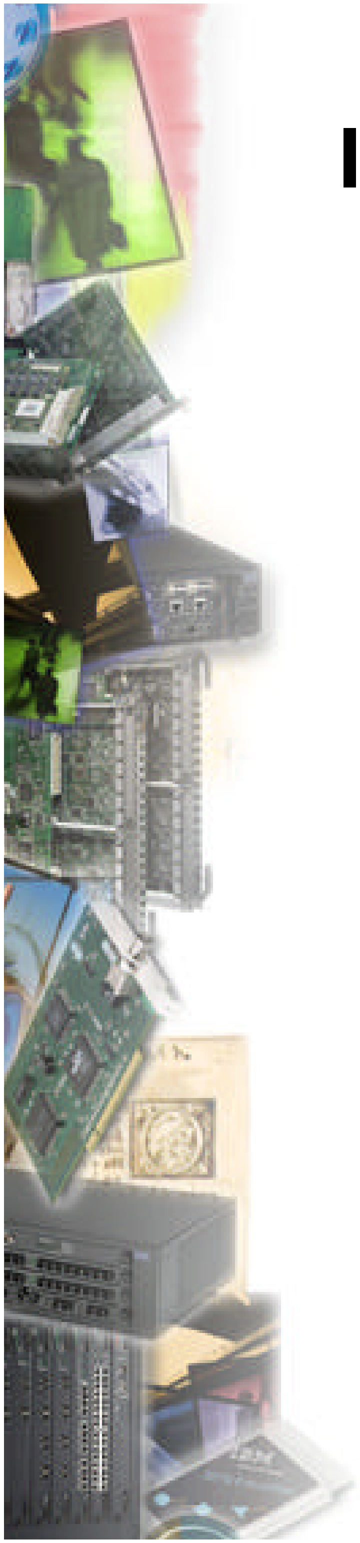
Where Does IPSec Fit?



TCP/IP Protocol Stack	VPN Protocols
Applications	S-MIME, S-HTTP, PGP, SET **IPSec (IKE)**
TCP/UDP	SSL, TLS
IP	**IPSec (AH, ESP)**
Network Interface	L2TP, L2F, PPTP

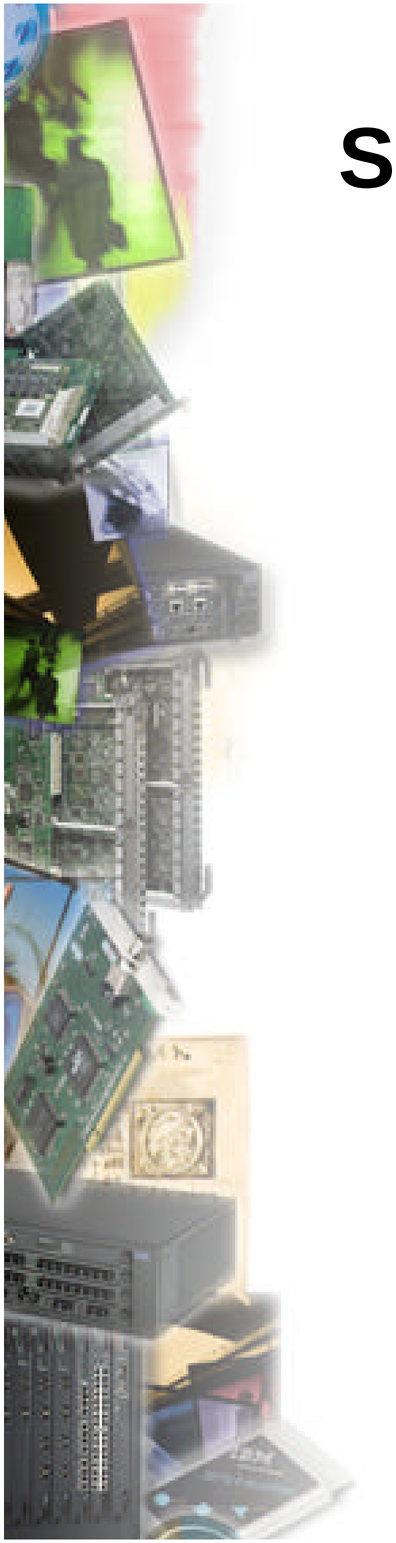
IP Layer (AH, ESP) protects user data

Application Layer (IKE) manages security associations



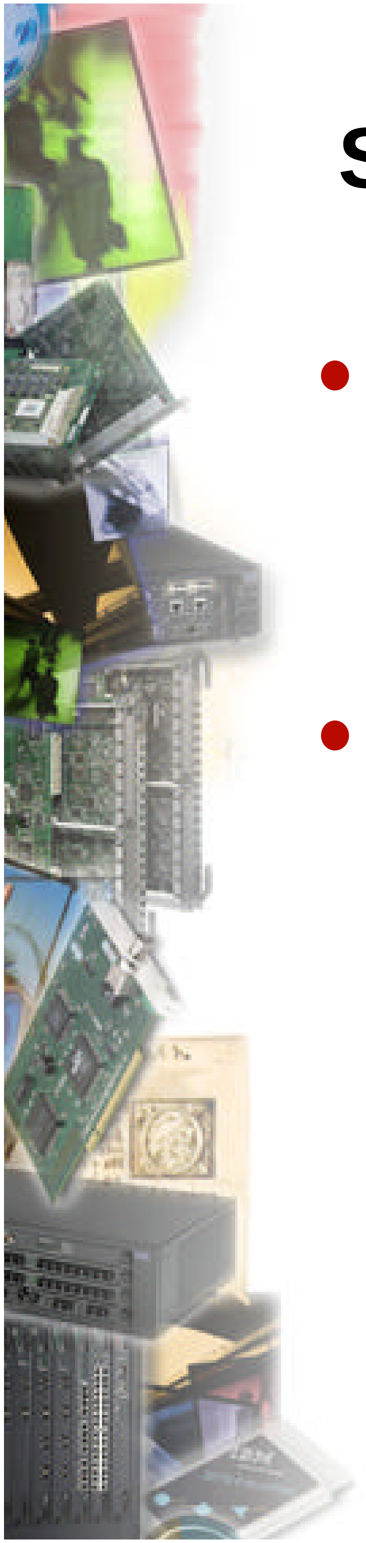
IPSec Features

- IPSec components
  - Authentication Header (AH) - authentication
  - Encapsulating Security Payload (ESP) - encryption
  - Internet Key Exchange (IKE) - key exchange
- IPSec allows for ...
  - authentication only
  - encryption & authentication
  - manual or automatic key exchange
  - tunnel or transport modes
  - nesting



Security Associations

- A *Security Association* (SA) consists of the following elements that define the details of an IPSec tunnel:
    - algorithms (encryption, authentication)
    - key lengths
    - lifetimes (how long until an SA expires)
    - peer identities (who is your partner)
    - nesting dependencies (inner or outer SA)
    - modes (tunnel or transport)



Symmetric Cryptography

- Uses a **single** key
  - a.k.a. secret key cryptography
  - encrypts and decrypts
- Examples
  - DES*: 56 bit key

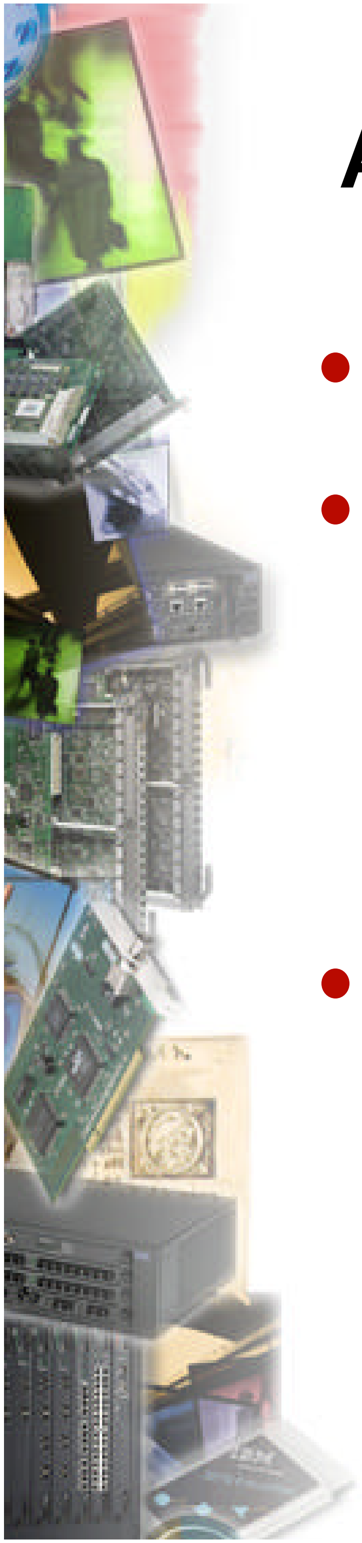
    developed by IBM in 1976

    adopted by NIST in 1978
  - Triple DES, RC2, RC4, RC5, IDEA

✓ Very fast - good for bulk encryption

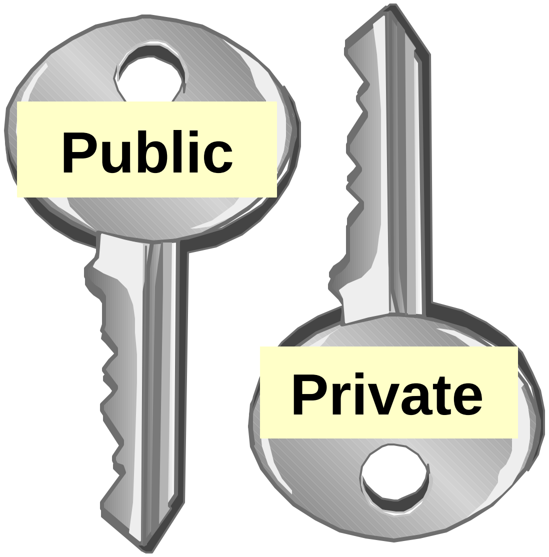
✗ Requires key to be sent between users

* Data Encryption Standard



Asymmetric Cryptography

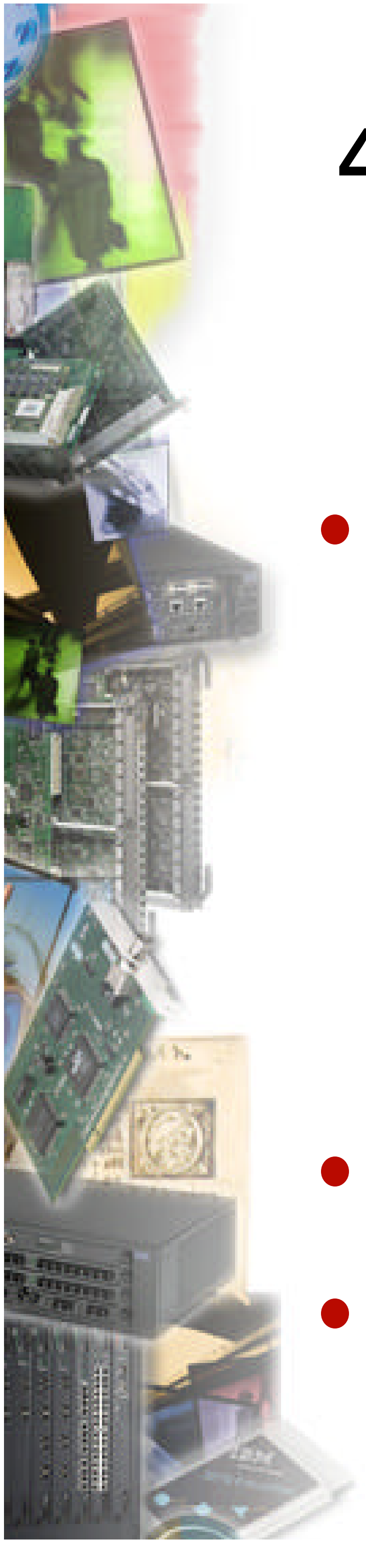
- a.k.a. public key cryptography
- Uses public key & private key
  - mathematically related
  - data encrypted with one can only be decrypted with the other
  - freely distribute public key
- Example
  - RSA, Elliptic Curve



✓ Can authenticate sender & receiver

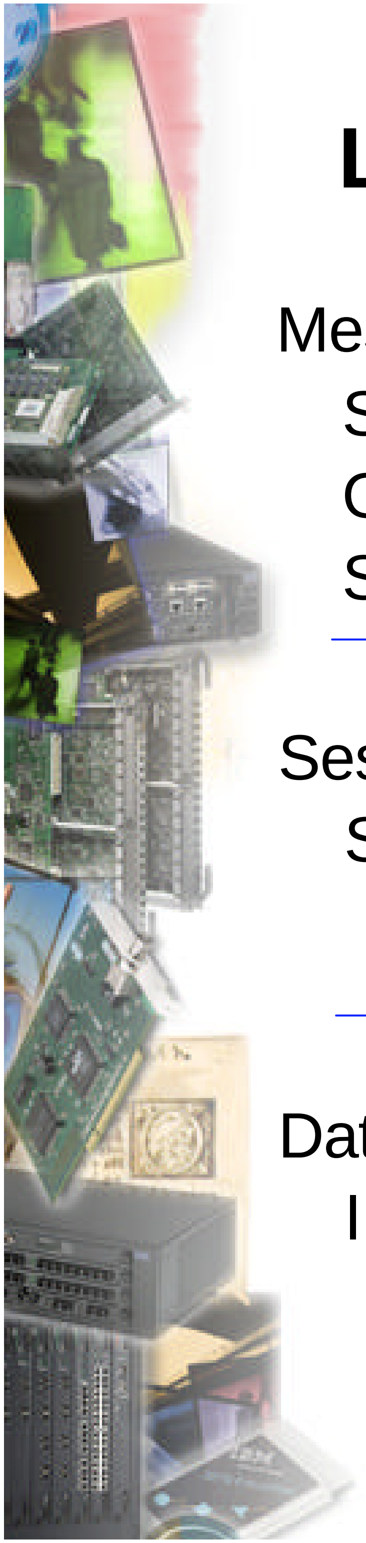
✗ Very slow

- 100-1000 times slower than symmetric



4758 PCI Crypto Coprocessor

- Improves security
  - tamper-sensing & tamper-responding
    - detects physical attacks (penetration, radiation, voltage, excessive cold/heat)
    - device is "zeroed"
  - first to receive FIPS 140-1 level 4
- Increases speed of crypto ops
- AIX, NT, & OS/2 supported



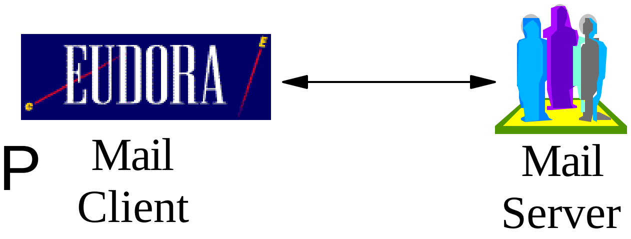
Levels of Encryption

Message

S-MIME

OpenPGP

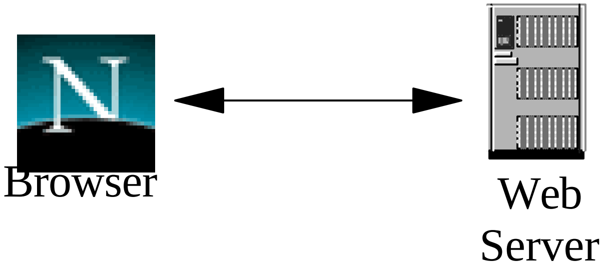
SET™



- asynchronous
- self-contained
  - atomic units

Session

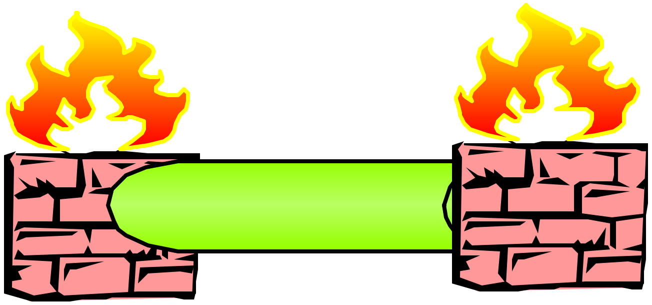
SSL



- unlimited destinations
  - widely deployed
- ubiquitous client
  - browser
- spontaneous connection

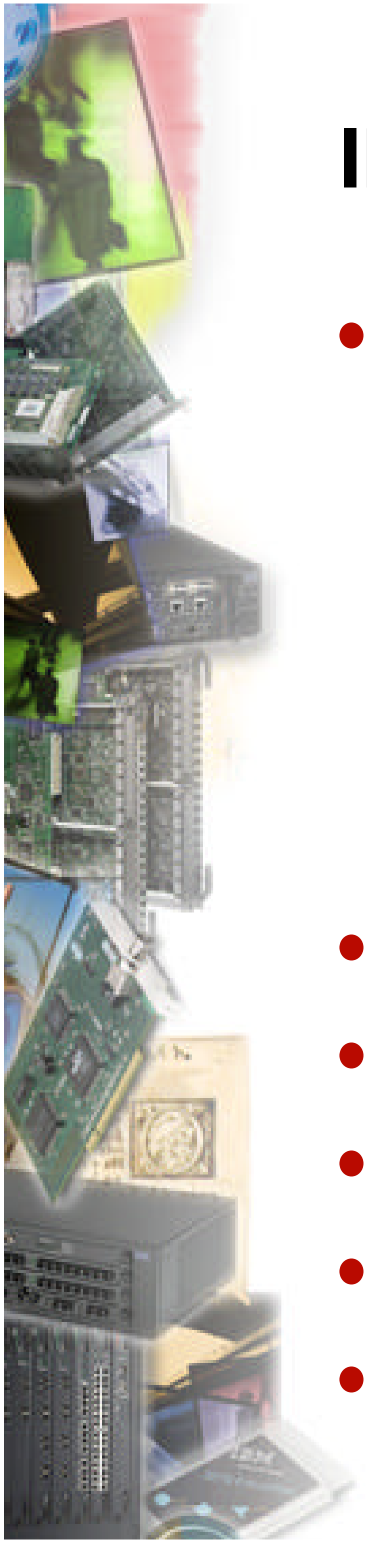
Datagram

IPSec



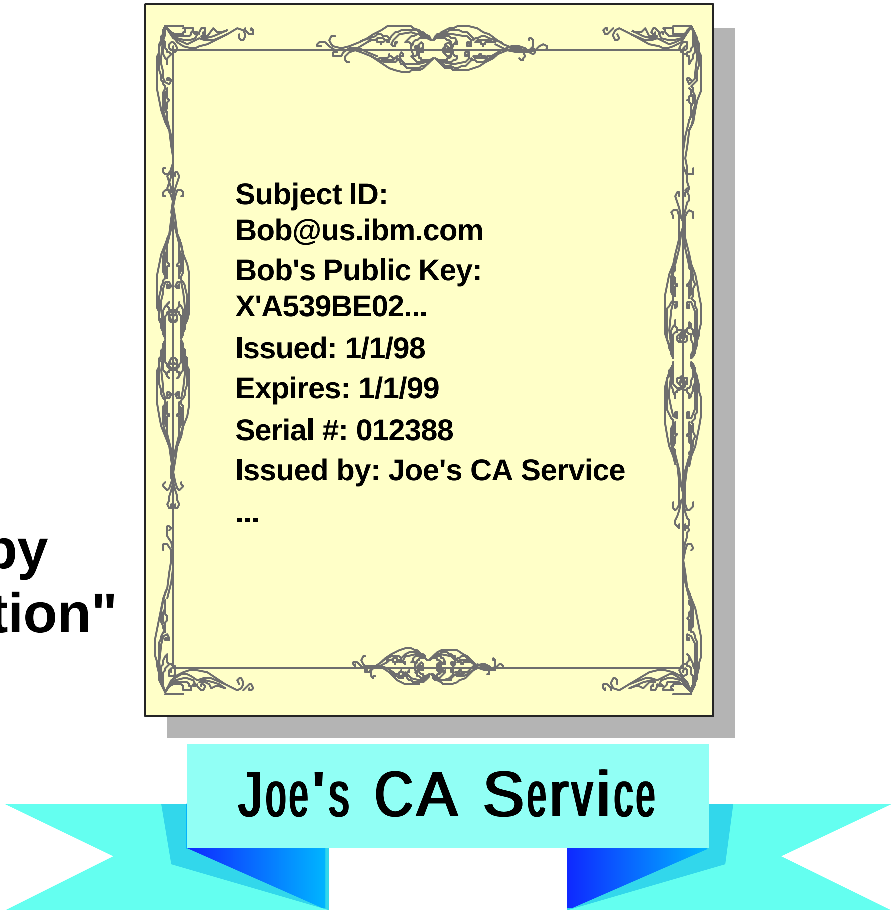
- minimizes overhead
- handles all IP traffic
- no impact to apps
- can hide net details

SET™ is a trademark of SETCo.



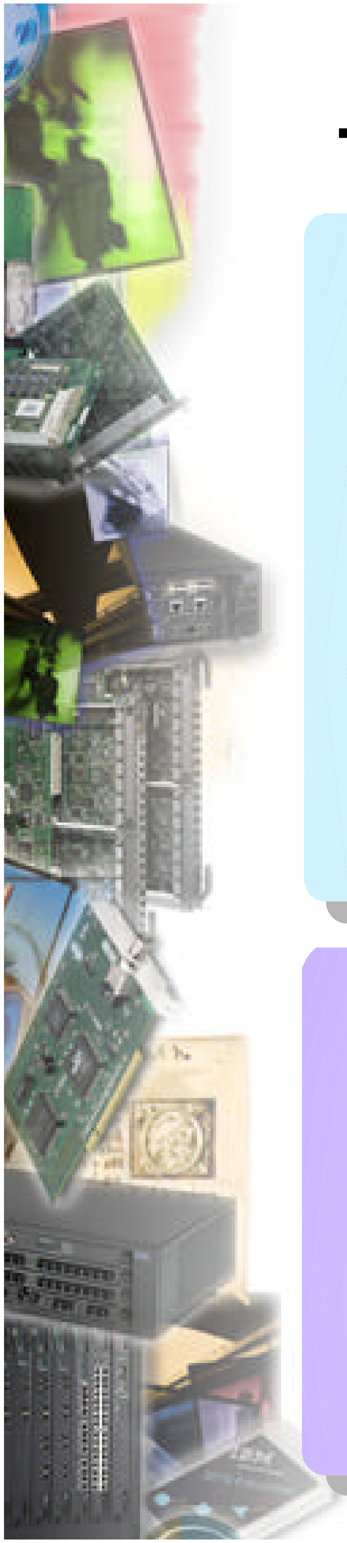
IPSec Certificates

- Named "subject"
  - **IP address/range**
  - **Subnet address**
  - **Domain Name**
  - **Distinguished Name**
  - **Text string**
  - **...anything else allowed by IP "Domain of Interpretation"**
- Public Key for "Subject"
- Date of issue
- Expiration date
- Miscellaneous info from issuing CA (serial #...)
- Issuing CA's digital signature on information above

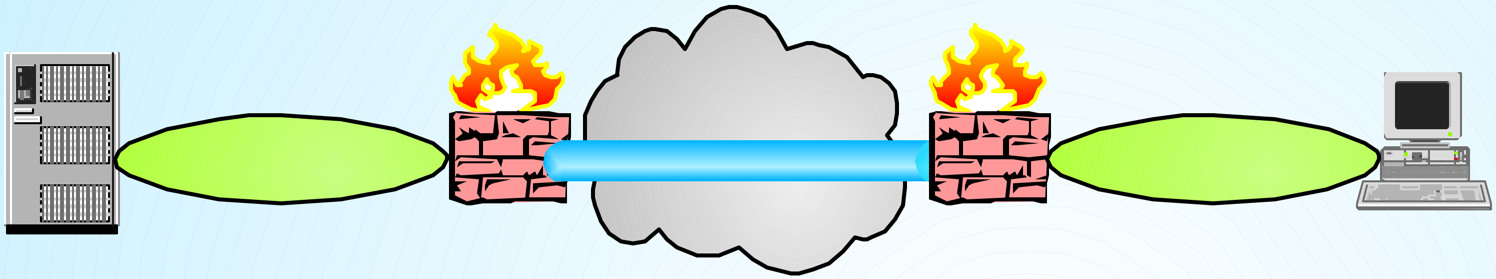


Subject ID:
Bob@us.ibm.com
Bob's Public Key:
X'A539BE02...
Issued: 1/1/98
Expires: 1/1/99
Serial #: 012388
Issued by: Joe's CA Service
...

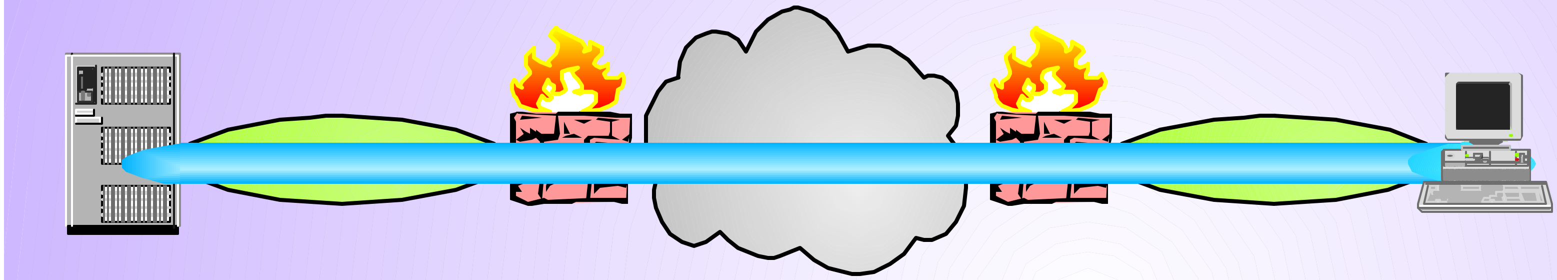
Joe's CA Service



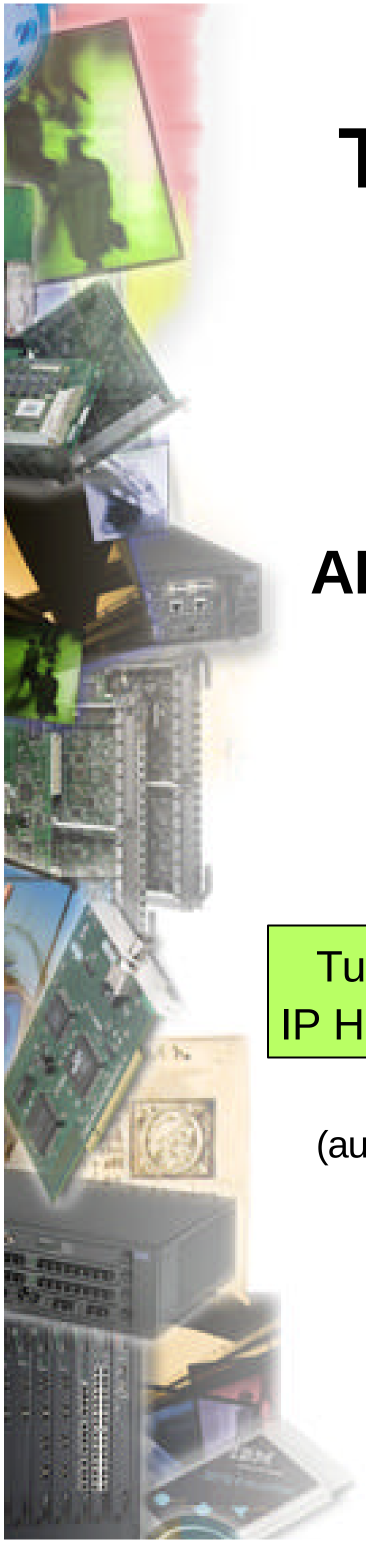
Terminating the Tunnel



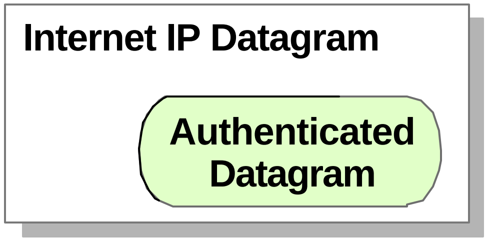
- In the middle
  - no impact to clients, servers
  - easier to setup, admin, manage
  - lower cost



- End-to-End
  - maximum security



Tunnel vs. Transport Modes



AH-Authentication Header

src@/dest@	Payload

Original Datagram

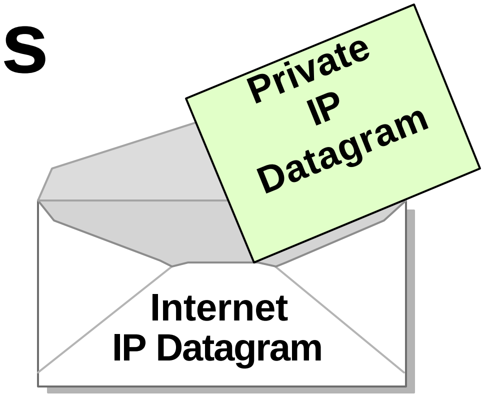
Tunnel IP Header	AH	src@/dest@	Payload

AH-Tunnel

(authentication at an intermediate gateway)

src@/dest@	AH	Payload

AH-Transport



ESP-Encapsulating Security Payload

src@/dest@	Payload

Original Datagram

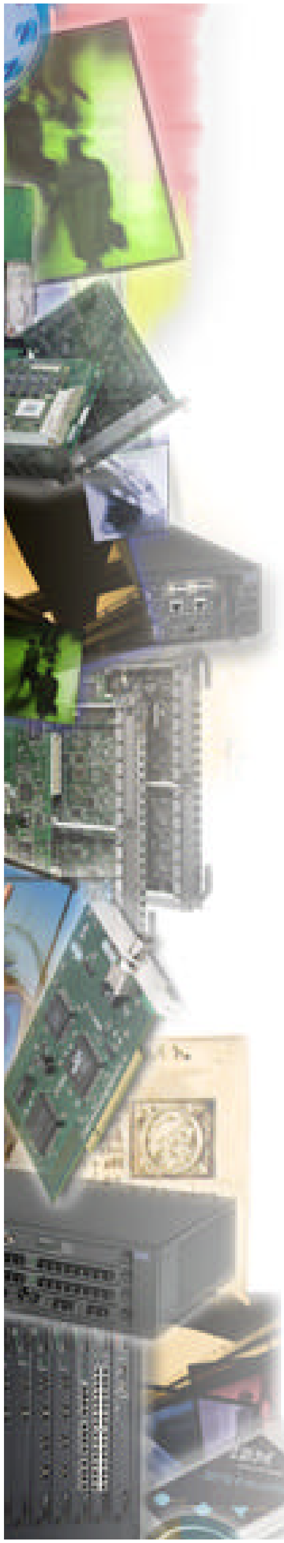
Tunnel IP Header	ESP	src@/dest@	Payload	ESP

ESP-Tunnel

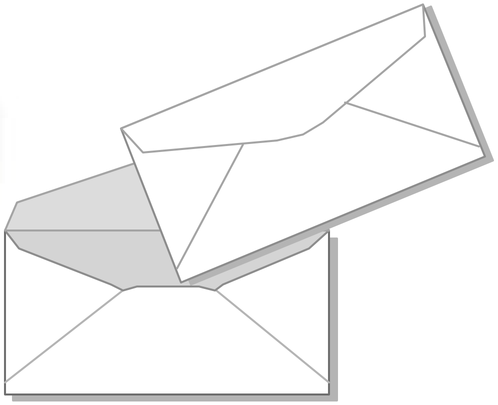
(hides endpoint addrs)

src@/dest@	ESP	Payload	ESP

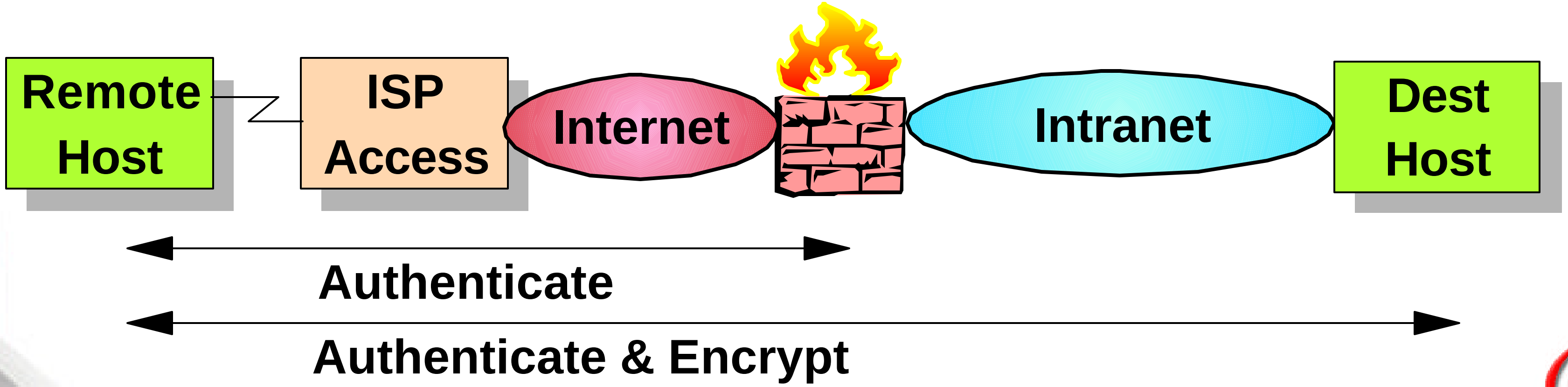
ESP-Transport

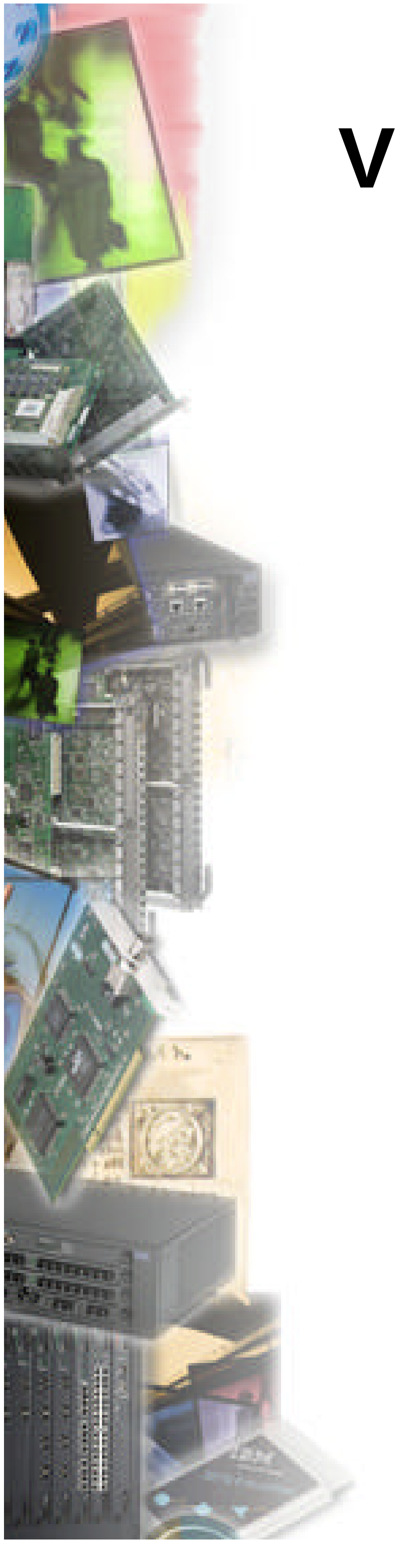


Nesting IPSec Protocols



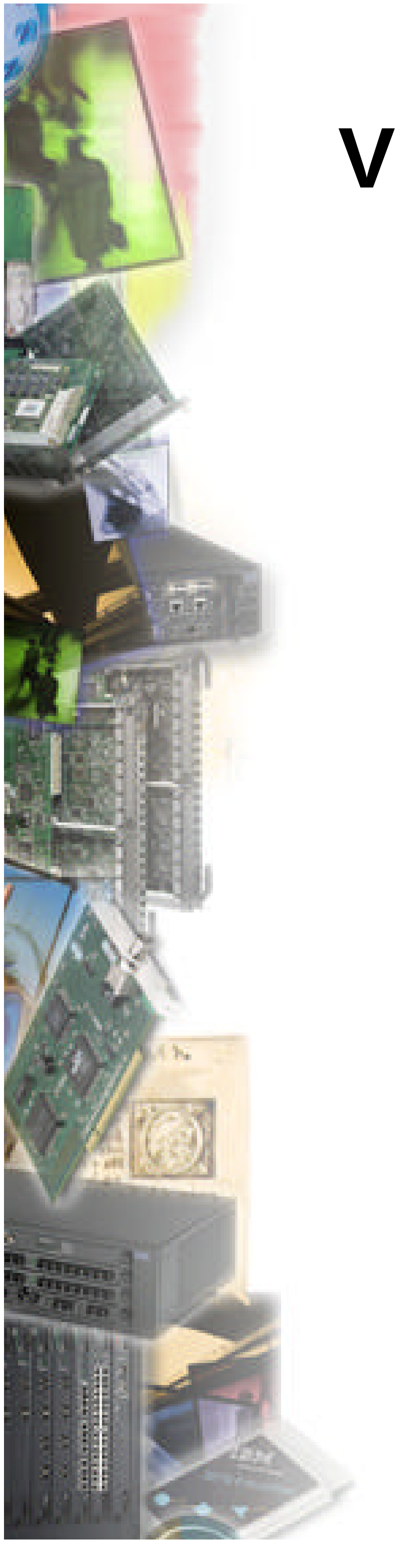
- Multiple security levels:
  - For end-to-end encryption and authentication, use ESP-transport mode with optional authentication
  - For host-to-firewall authentication, use AH-tunnel mode
  - Nest the ESP-transport inside the AH-tunnel





VPN Interoperability

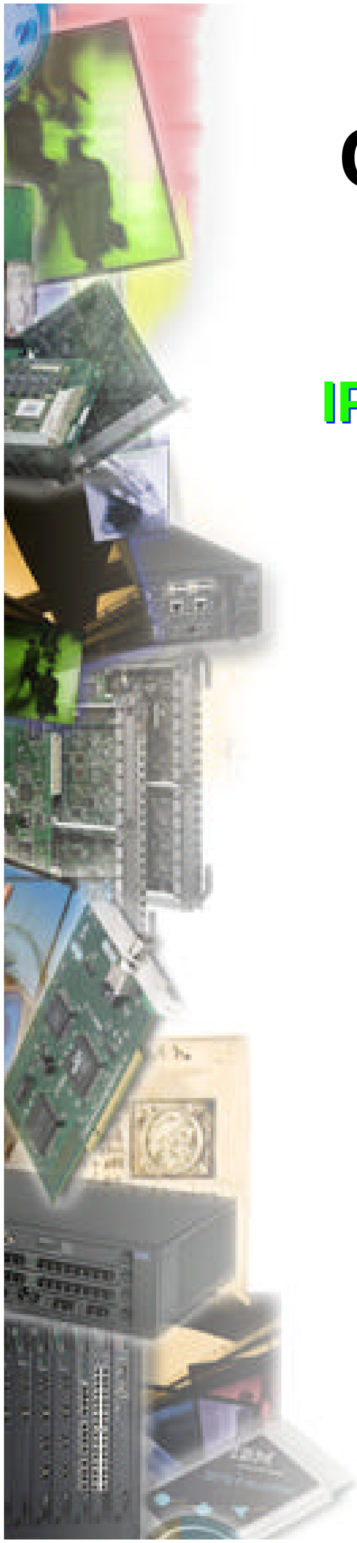
- ICSA Certification
  - testing against a reference implementation
  - "VPN certification" (fewer reqmts)
  - "IPSec certification" must support:
    - AH, ESP, & IKE
    - tunnel & transport modes
    - interaction with a CA (e.g. RSA signatures, CRL, MD5-HMAC & SHA-1-HMAC)
    - preshared keys
    - RSA, DES (3DES is "recommended" but not required)
- ANX Workshops
  - testing against other vendor's products
  - IBM hosted 4Q98 event
  - 50+ vendors
    - Networking: 3COM, Bay, Cabletron, Cisco, Lucent, Shiva
    - Security: Baltimore Technologies, Checkpoint, Entrust, ICSA, Network Associates, Redcreek, Verisign
    - Others: Intel, Microsoft, NIST

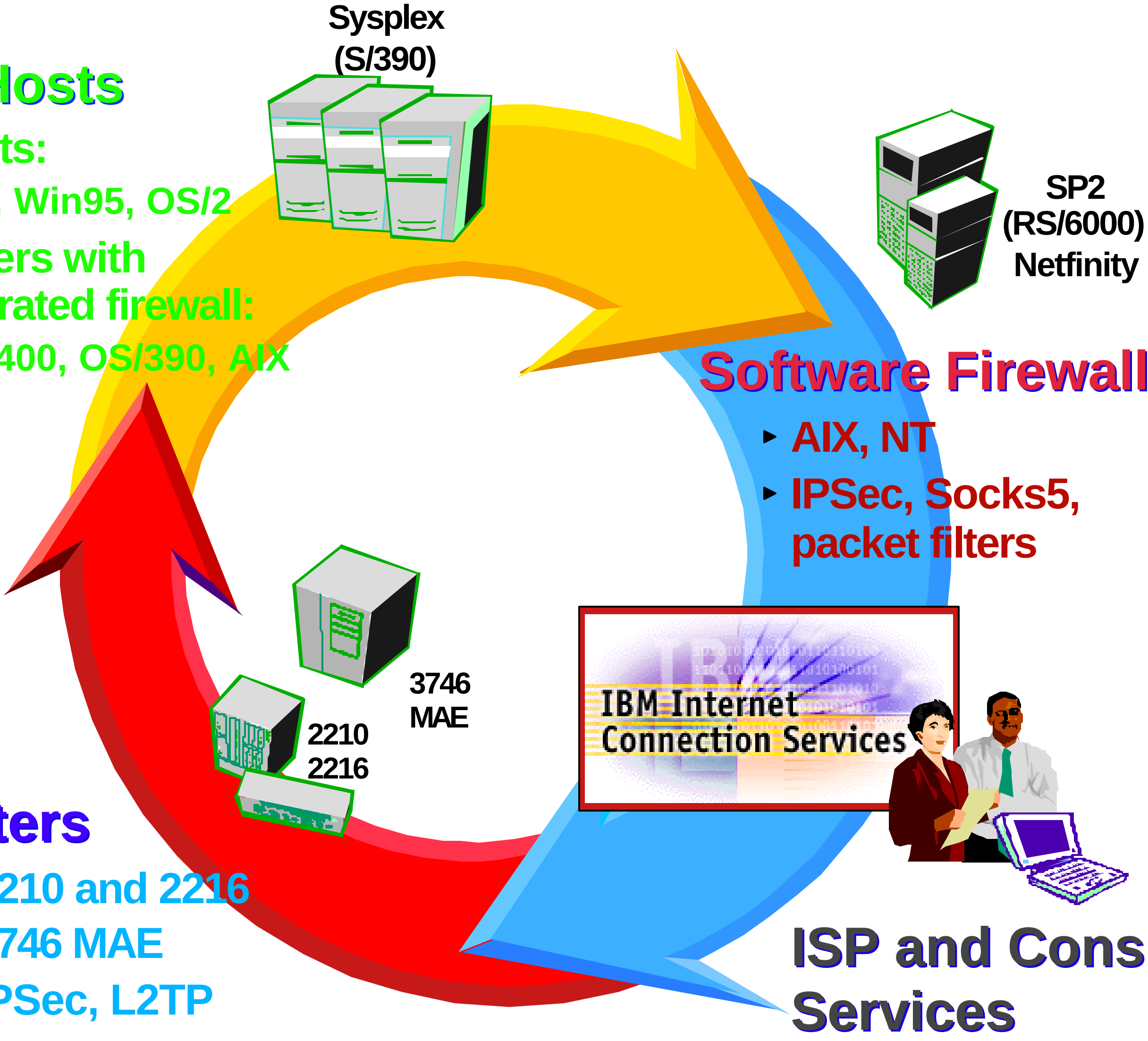


VPN Management

- LDAP
  - Lightweight Directory Access Protocol
  - basis for common directory facility
    - storage and lookup
- IBM's Application Driven Networking Architecture
  - 1st product delivery - Common Policy Engine
    - rapid packet classification technology
    - integrated LDAP client
    - interpret and enforce QOS, **VPN**, and filtering policies (from LDAP directory)
    - software upgrade to 2210, 2212, 2216, & Network Utility

Comprehensive Offerings





IPSec Hosts

- Clients:
  AIX, Win95, OS/2
- Servers with integrated firewall:
  OS/400, OS/390, AIX

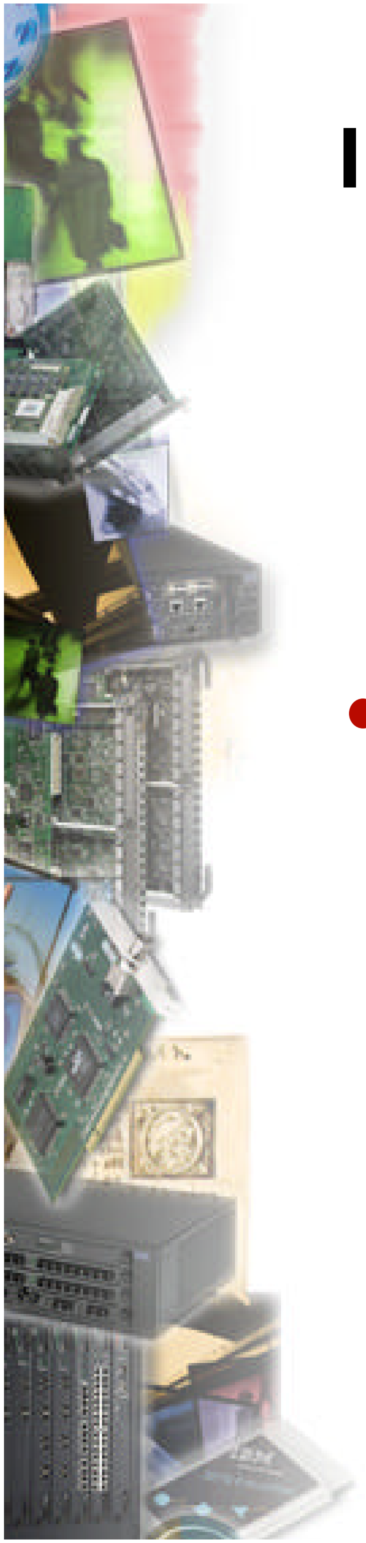
Software Firewalls

- AIX, NT
- IPSec, Socks5, packet filters

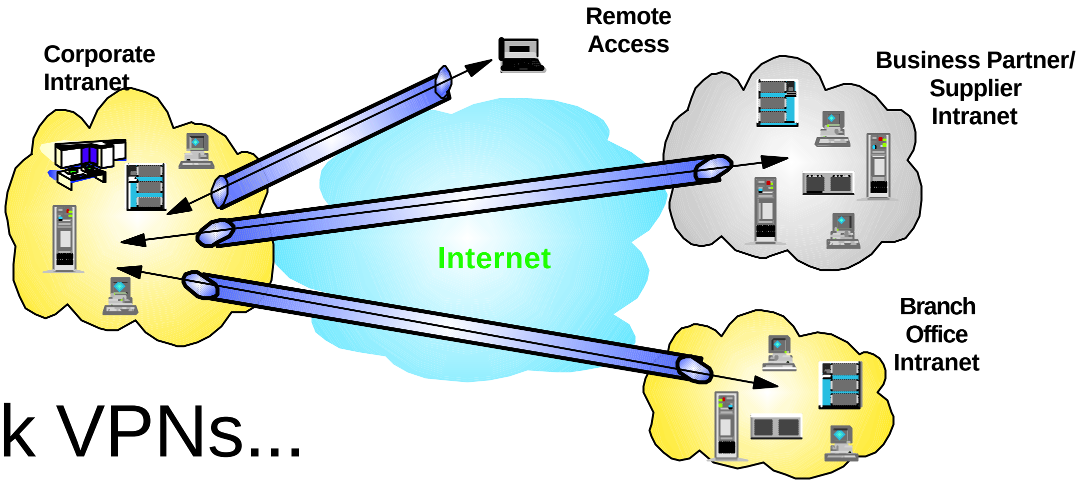
Routers

- 2210 and 2216
- 3746 MAE
- IPSec, L2TP

ISP and Consulting Services



IBM eNetwork Virtual Private Networks

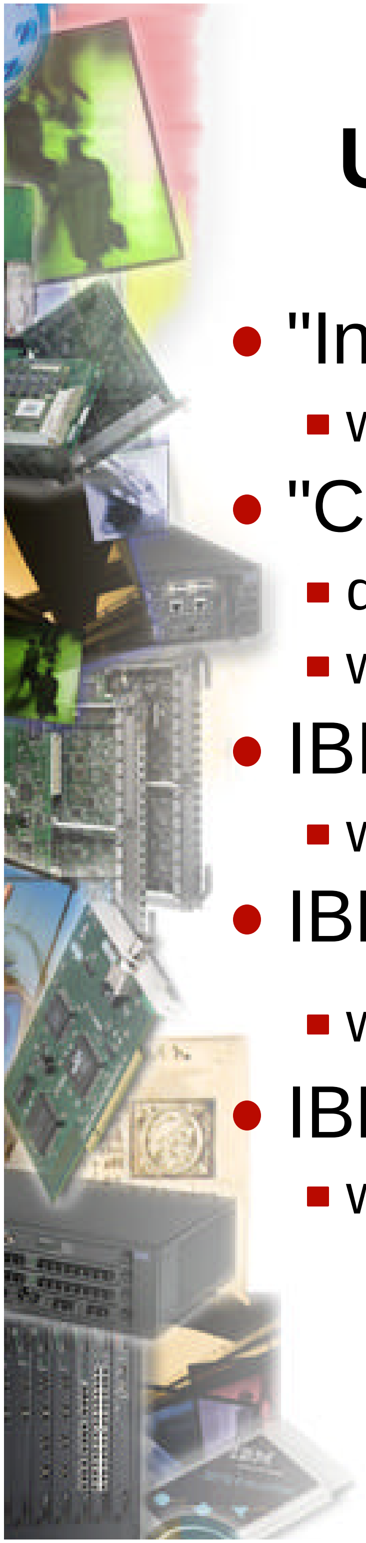


- IBM eNetwork VPNs...
  - Extend the Reach of Your Network, Applications & Data
  - Enable Secure e-business Communications

IBM Virtual Private Network Information:

eNetwork VPN Solutions: www.software.ibm.com/enetwork/technology/vpn

IBM Routers:	www.networking.ibm.com
IBM Firewall:	www.software.ibm.com/enetwork/firewall
IBM S/390:	www.s390.ibm.com/marketing/g3263036.html
IBM AS/400:	www.as400.ibm.com/usa/TRENDS/html
AIX Server:	www.rs6000.ibm.com/resource/features/1998/aixrite/choose_aix431.html
SecureWay:	www.ibm.com/security



URL's

- "Inside the VPN Tunnel" article
  - www-1.ibm.com/support/tcp/fall98/vpntunel.html
- "Cryptography and SET: Safe Surfing?" article
  - d02xdgcl01.southbury.ibm.com/support/tcp/assets/pdf/setwebpa.pd
  - www.software.ibm.com/commerce/payment/cryptset.html
- IBM SecureWay home page
  - www.ibm.com/Security
- IBM Security Services
  - www.ibm.com/security/html/consult.html
- IBM eNetwork Firewall
  - www.software.ibm.com/enetwork/firewall