Virtual Private Networking

Richard J. Tobacco
NHD VPN Marketing Manager
rjt@us.ibm.com

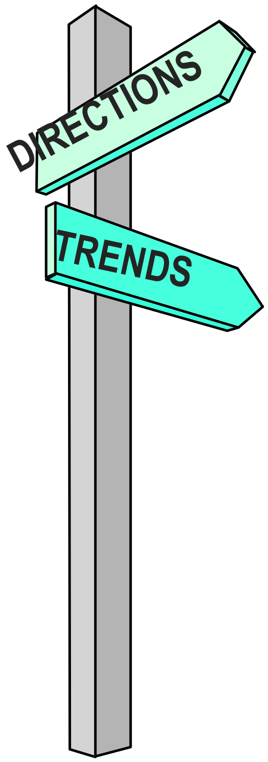
Designs for Implementation of Secure Communication

e-business VPN

Session abstract

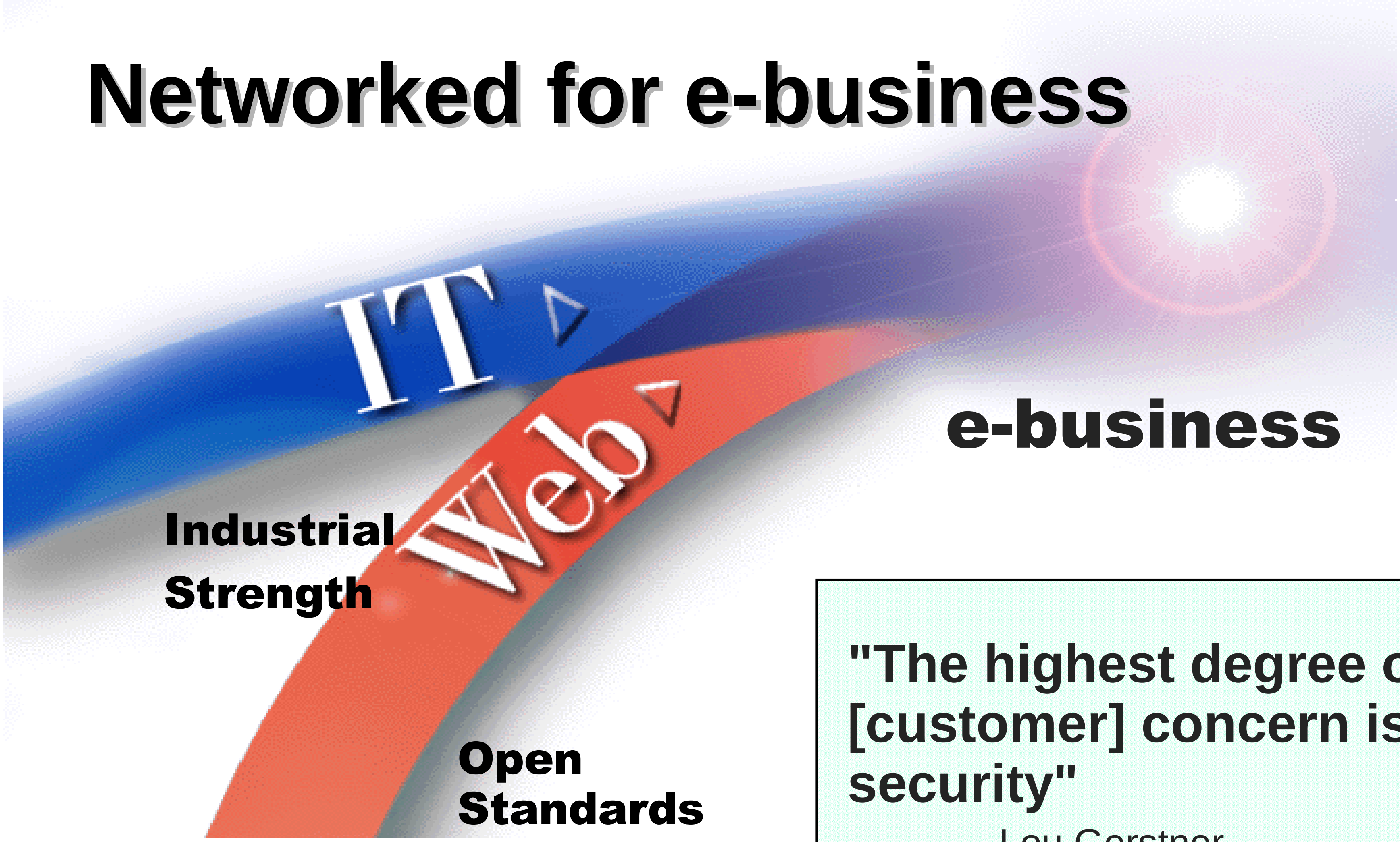
- Using the Internet to perform e-business can reduce network expense and increase business. However, the Internet is an insecure (or untrusted) transport and most business are unwilling to implement e-business solutions without first adding the security VPNs provide. Current solutions require VPN termination within network devices in addition to servers and clients.
  - This session will discuss the value of VPN functions
  - Features that are required for large VPN networks
  - What is (and will be) provided by IBM networking products

Implementation Intent



In order to fully appreciate specific feature and function currently available on our routing products, this presentation includes many statements regarding intent. These statements should not be construed as commitments by IBM. Products are not committed until they are announced.

Networked for e-business



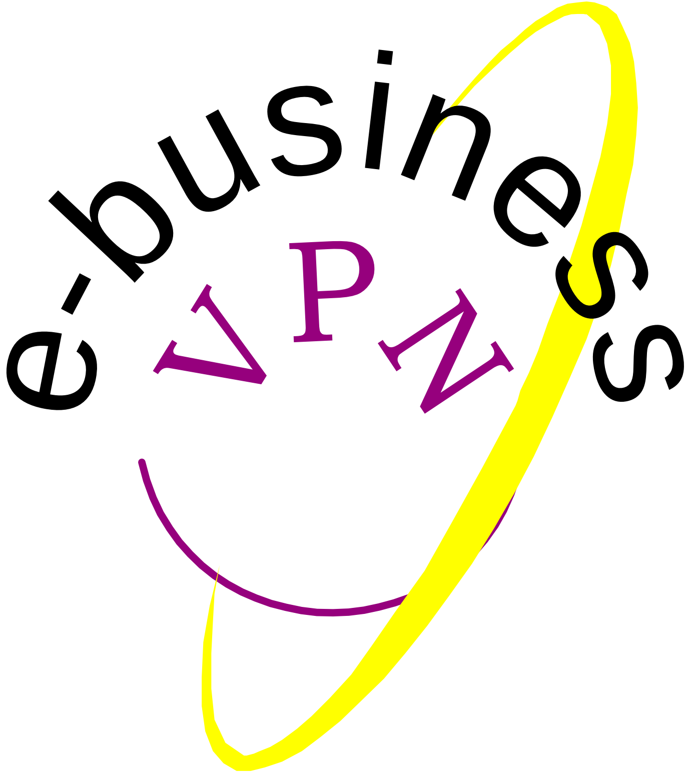
e-business

Industrial Strength

Open Standards

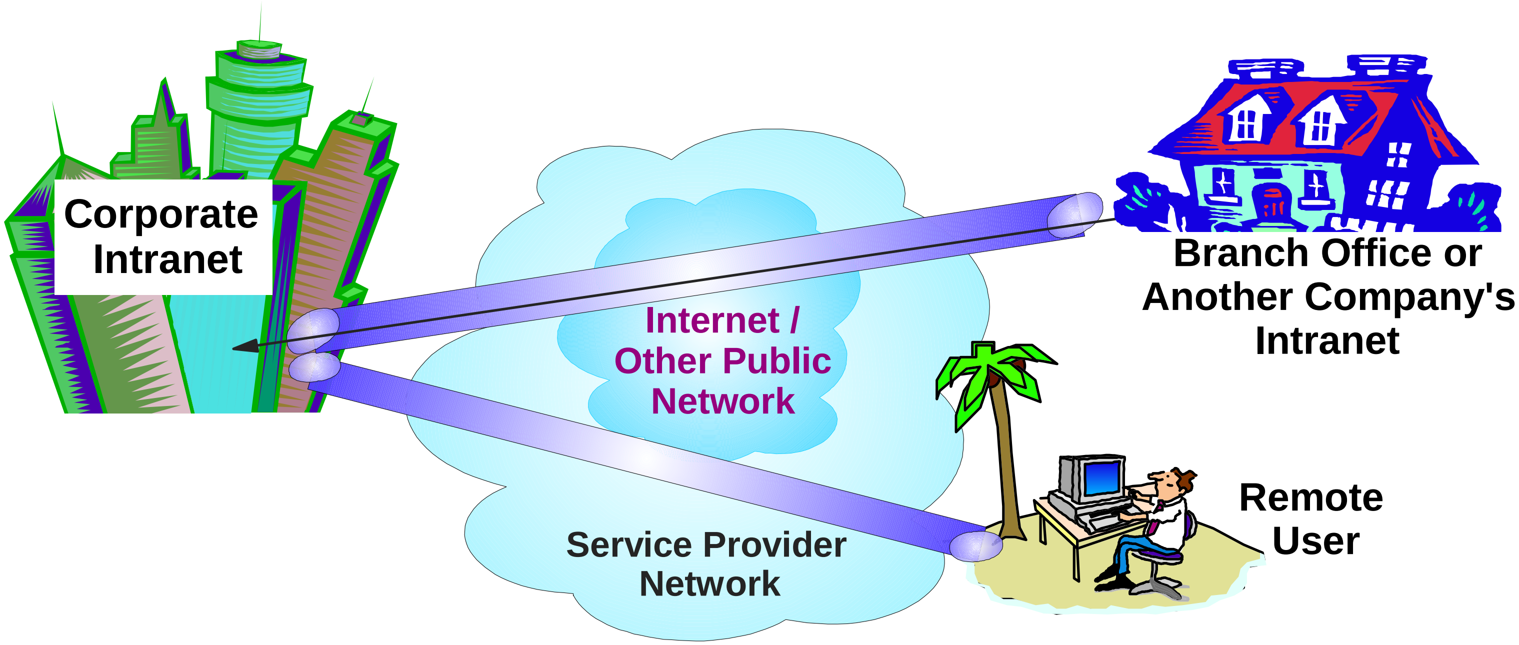
"The highest degree of [customer] concern is security"

Lou Gerstner,
Information Week
3/11/98



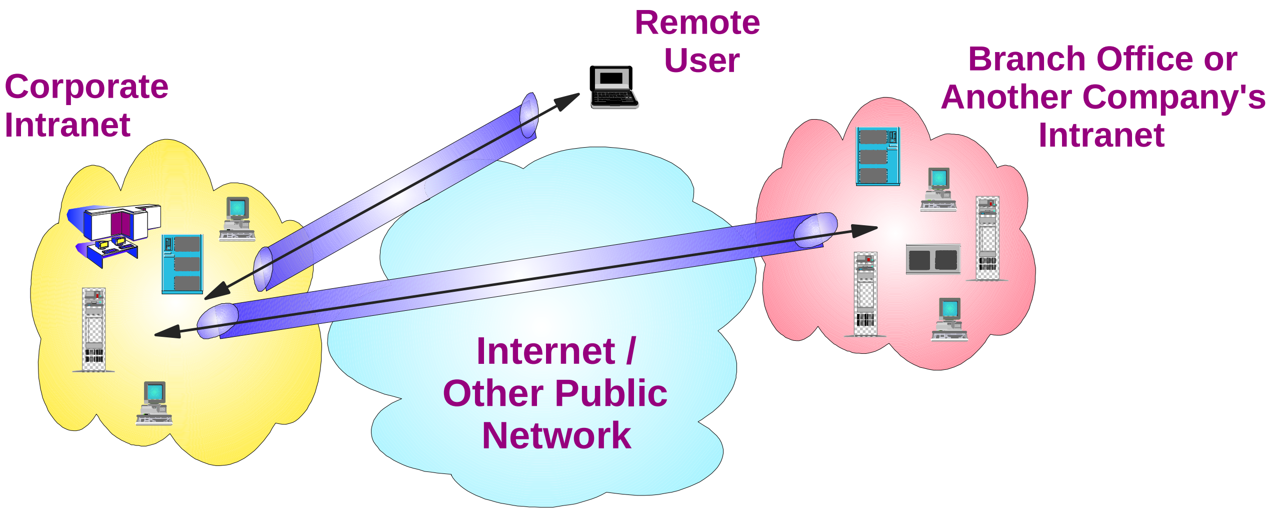
- Consumers and corporations embracing the Internet to transact business require protection of information
- Virtual Private Networks (VPNs) provide security that protects information when conducting e-business
- VPNs will be at the core of networks designed to conduct e-business

What is a VPN?


Corporate Intranet
Internet / Other Public Network
Branch Office or Another Company's Intranet
Remote User
Service Provider Network

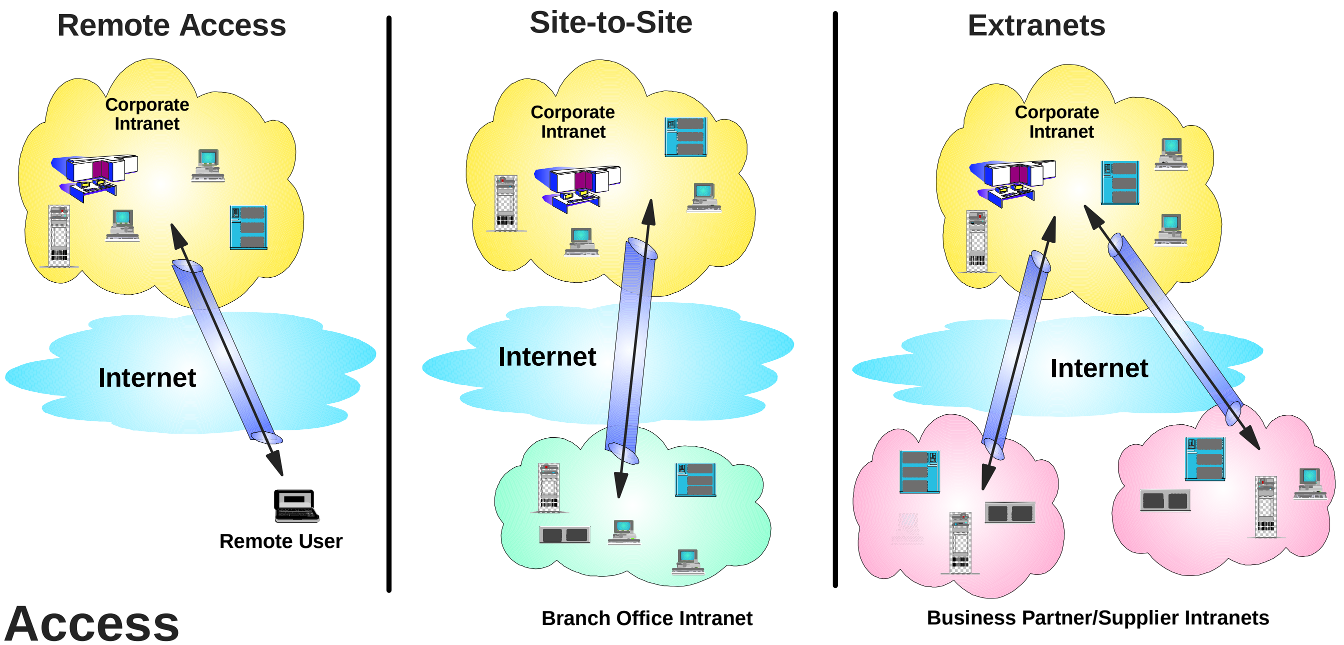
- A Virtual Private Network is a <u>secure</u> extension of a business' private intranet, across an untrusted public network (such as the Internet)
- VPNs essentially are private "tunnels" - created by the encapsulation of the original packets within new ones

What do VPNs Provide?



- ➢ Privacy for interchange of sensitive information
  - **Authorization** - *does the user have the right to this?*
  - **Authentication** - *are senders who they claim to be?*
  - **Accounting** - *are charges being applied to users?*
  - **Non-repudiation** - *can you prove the message origination?*
  - **Integrity** - *was the data changed during transit?*
  - **Confidentiality** - *can anyone else read it?.*
- ➢ Resource protection of information assets
  - *Hiding resource addresses.*
  - *Filtering out unwanted attempts to use the resource.*

Basic VPN Implementations



➤ Remote Access

- Problems: High administrative workload, expensive 800 or long distance costs
- Solutions: VPNs exploit worldwide ISP reach and lower connectivity and administrative costs

➤ Site-to-Site Connection

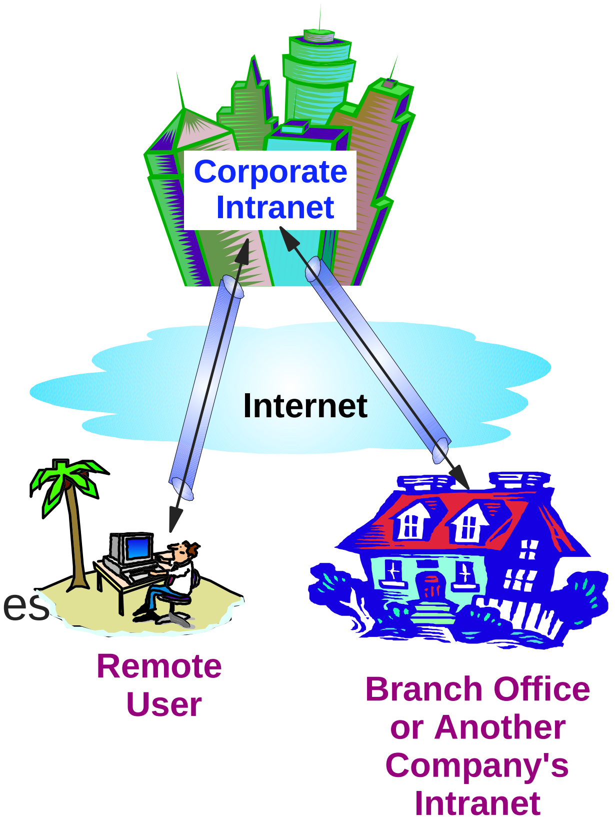
- Problems: Expensive leased line connections or part-time dial connections to home office
- Solutions: VPNs provide 24-hour real-time communication via inexpensive Internet links

➤ Extranets

- Problems: Set-up/operational costs prohibitively high for smaller business partners
- Solutions: VPNs provide global, secure, cost-effective, end-to-end intercompany communication

VPN Values

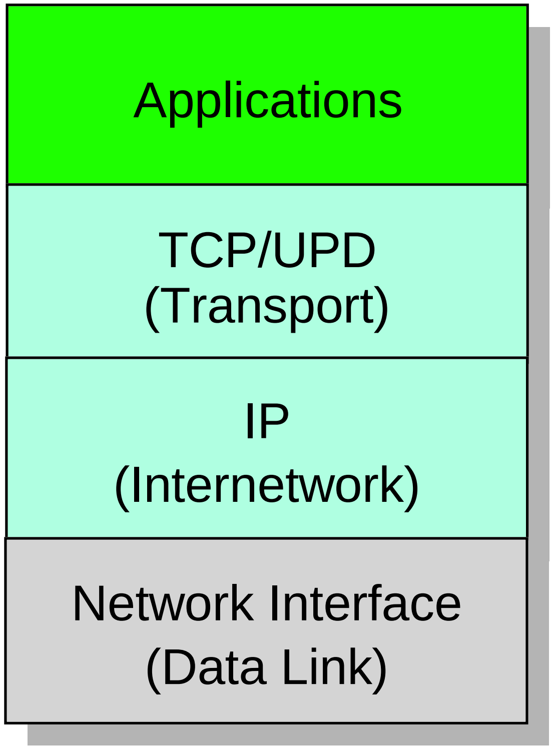
- ➢ Increased e-business opportunities
  - Promoting and selling products and services
  - Improved customer loyalty
  - Collaborating with business partners
    - reducing inventories
    - improved time-to-market
- ➢ Increased service opportunities
  - Rollout of VPNs to large enterprises
  - Extending VPN connectivity to small offices
  - Managed VPN provides services 'entry'
  - Standards leading offerings
- ➢ Improved communication effectiveness
  - Immediate worldwide reach & access
  - Positioned to leverage IP advancements
- ➢ Cost savings
  - Consolidating equipment needs
  - Minimizing network management responsibilities
  - Eliminating long-distance charges
    - Savings over private networks of up to 80% (Forrester Research, Infonetics Research)



Tunneling

Tunneling Protocols

TCP/IP Protocol Stack



Applications

TCP/UPD
(Transport)

IP
(Internetwork)

Network Interface
(Data Link)

VPN-Related Protocols

S-MIME, S-HTTP, PGP, SET
IPSec (IKE)

SOCKS V5
SSL

Packet filtering,
IPSec (AH, ESP)

L2TP, PPTP, L2F
CHAP, PAP, MS-CHAP

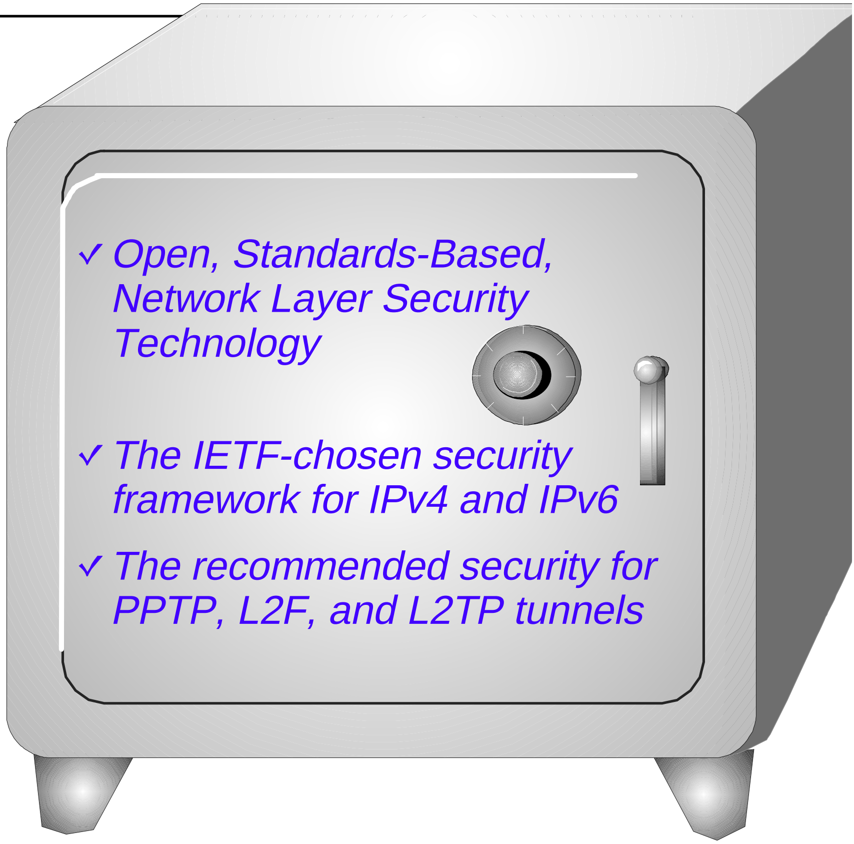
Although IPSec is the primary VPN tunneling protocol, higher and lower level security protocols will continue to exist.

IP Security Protocol

- Authentication Header (AH)
  - Data origin authentication (key based)
  - Data integrity (checksum)
  - Replay protection (sequence number)
- Encapsulating Security Payload (ESP)
  - Data origin authentication
  - Data integrity
  - Replay protection
  - ✓ Data Confidentiality (encryption)
- Internet Key Exchange (IKE)

  Previously: Security Association and Key Management Protocol (ISAKMP)
  - Framework to support negotiation of security associations (SA)

    Relevant information - party identities, keys, cryptographic algorithm, etc.
  - Mandatory key management protocol - Oakley



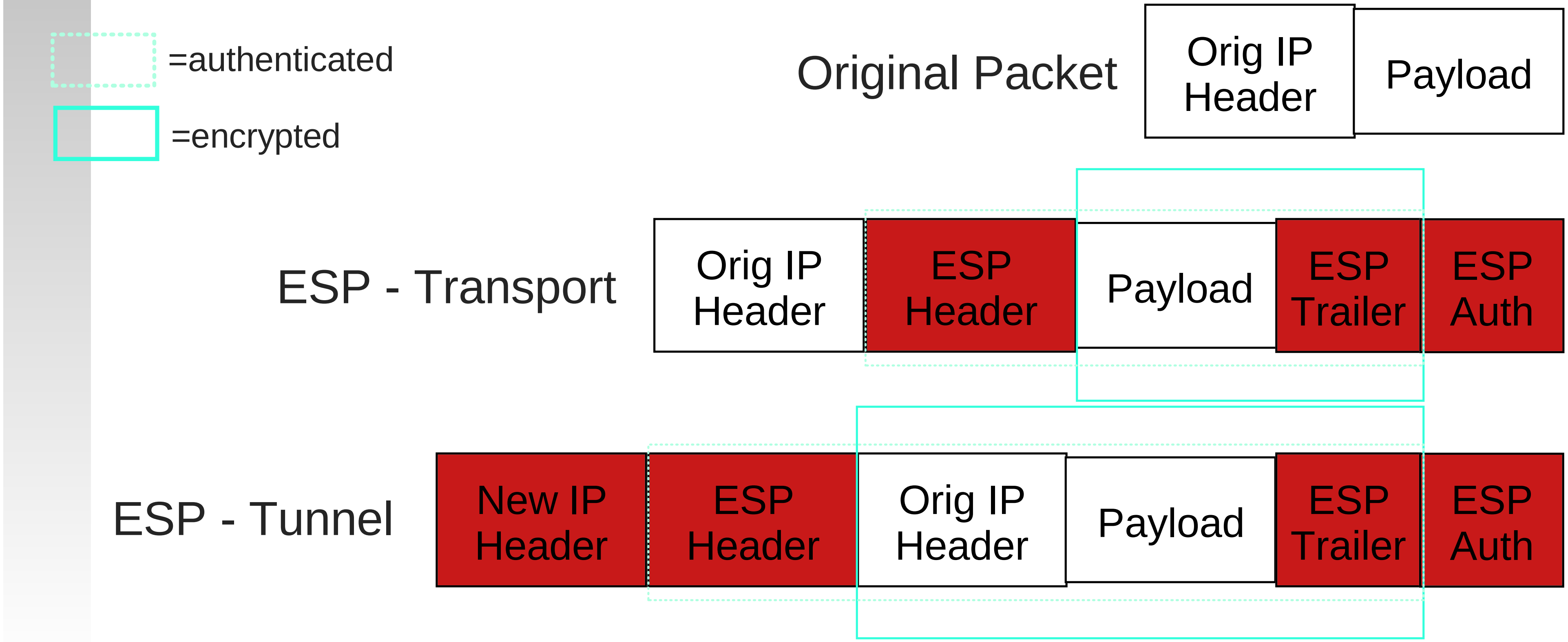
✓ Open, Standards-Based, Network Layer Security Technology

✓ The IETF-chosen security framework for IPv4 and IPv6

✓ The recommended security for PPTP, L2F, and L2TP tunnels

IPsec Encapsulating Security Payload (ESP)

- ✓ Provides data origin authentication, integrity protection, confidentiality (encryption) and optional replay protection on per-packet basis
- ✓ Protects either payload (transport) or original header+payload (tunnel)



=authenticated

=encrypted

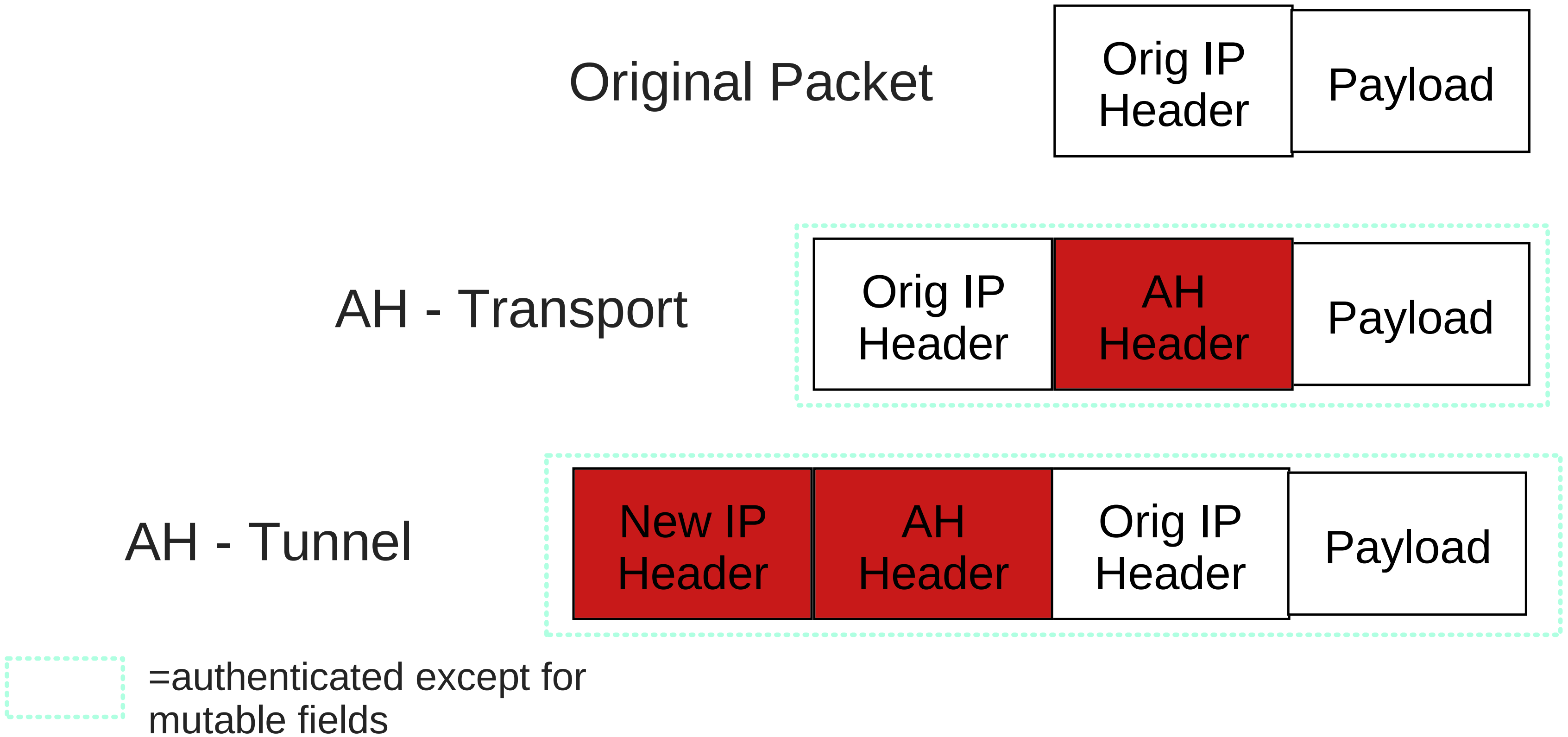
Original Packet: Orig IP Header | Payload

ESP - Transport: Orig IP Header | ESP Header | Payload | ESP Trailer | ESP Auth

ESP - Tunnel: New IP Header | ESP Header | Orig IP Header | Payload | ESP Trailer | ESP Auth

IP Authorization Header (AH)

- ✓ Supports data origin authentication and data integrity on a per-packet basis
  - optional replay protection
- ✓ Protects the integrity of the ENTIRE Packet
  - Header (except for mutable fields - e.g. IPv4 TTL, checksum)
  - Payload (still cleartext, not encrypted)



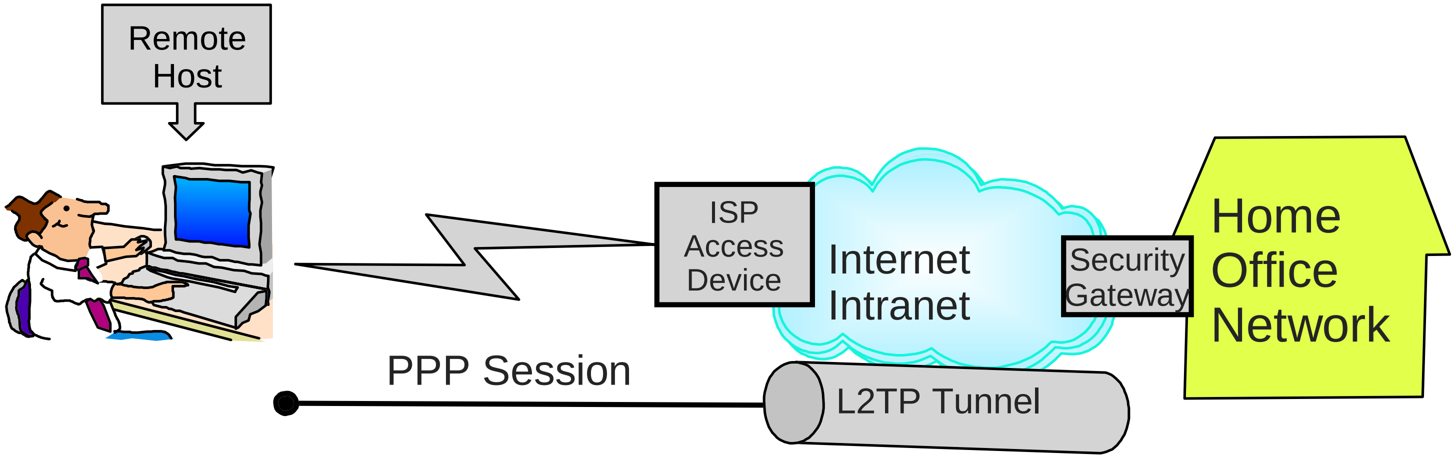
Original Packet: Orig IP Header | Payload

AH - Transport: Orig IP Header | AH Header | Payload

AH - Tunnel: New IP Header | AH Header | Orig IP Header | Payload

=authenticated except for mutable fields

L2TP



- Layer 2 Tunnel Protocol (L2TP)* extends the Point-to-Point Protocol (PPP) connection all the way to the corporate gateway
- Supports transport of legacy protocols (e.g., IPX)
- Combines with RADIUS, password & ID to provide:
  - Authorization, Authentication & Accounting
- L2TP lacks encryption exposing data to eavesdrop

* L2TP is a standards based combination of two proprietary layer 2 tunnel approaches

- Microsoft's Point-to-Point Tunnel Protocol (PPTP)
- Cisco's Layer 2 Forwarding (L2F)

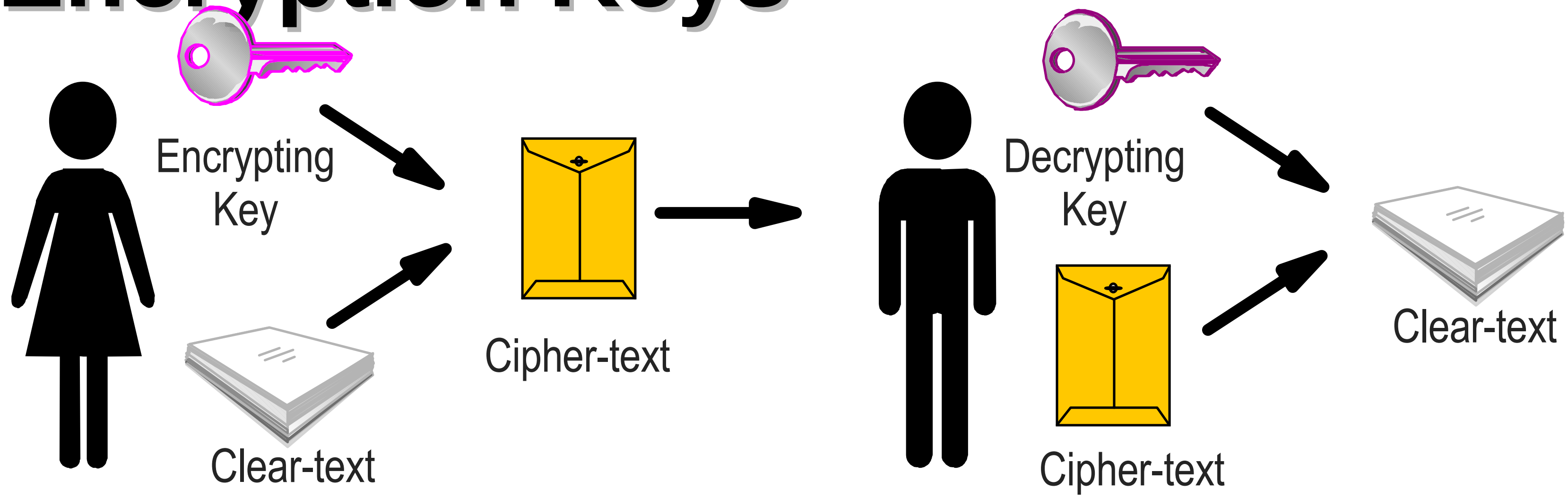
Encryption - Key management

Manual

Pre-shared

Internet Key Exchange

Encryption Keys



- Encryption converts data into a form unreadable by anyone other than the intended recipient
- Key management (e.g., exchange) is a basic VPN construct
  - Symmetric algorithms - Encryption and decryption keys the same - exchanged beforehand, for example by mail
  - Asymmetrical or public key algorithms - exchanged over an unsecured link

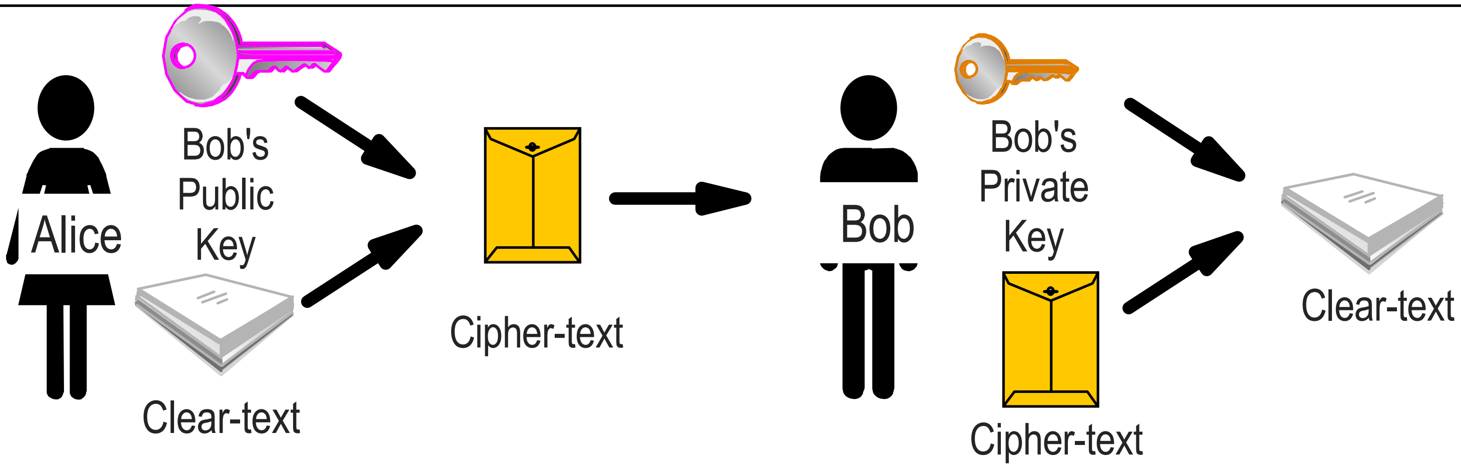
Symmetric or Secret Key Algorithms

Encrypting Key

Decrypting Key

- Conventional cryptographic algorithms where the sender and receiver must agree on the key before any secured communication can take place
  - Key exchanged via alternate (secure) communication
  - Key exchanged after public key algorithms secure session
- Symmetric algorithms are efficient and can easily be implemented in hardware
- Well known algorithms (ciphers) include:
  - Data Encryption Standard (DES), developed by IBM, with a 56 bit key length
    - Triple DES (3DES) with a 128 bit key length
  - International Data Encryption Algorithm (IDEA), with a 128 bit key length
    - Stronger and faster than DES, but lacking widespread acceptance

Public Key Algorithms



- ✓ Public - private key ciphers that enable secure transmission over an unsecure link
  - Encryption: Message sent with <u>recipient's public</u> key
    Readable only by intended <u>recipient' private</u> key
  - Authentication: Identification sent with <u>senders private</u> key
    Receiver verifies authenticity with <u>senders public</u> key
- ✓ Asymmetric algorithms are process intensive and often only used at session initiation to exchange symmetric or secret keys
- ✓ Well known algorithms (ciphers) include:
  - The de-facto standard RSA based on very large prime numbers
  - Diffie-Hellman used for key-exchange (does not authenticate)

Authentication

1. Something you know:
   Passwords, shared secrets
2. Something you have:
   Certificate, tokens, smart cards
3. Something you are:
   Biometrics: voice recognition, fingerprint, eye scan

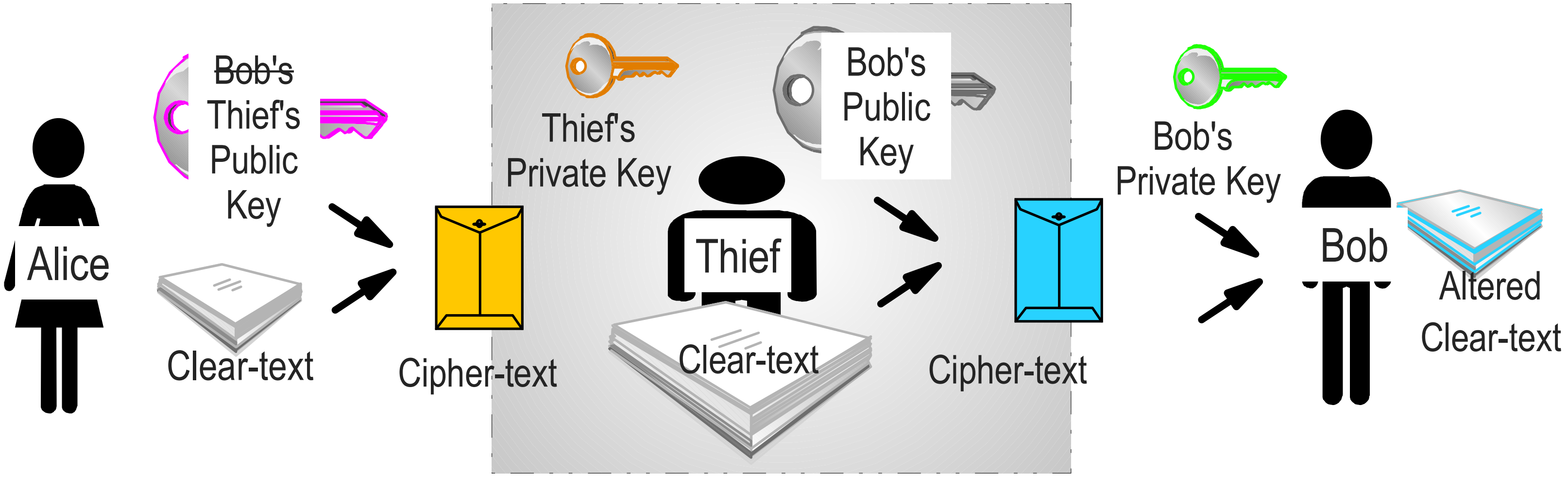
Comparing Authentication Alternatives

	High Security	Scaleability	Ease-of-Use and Management	Few client upgrades needed	Low Cost
Passwords			X	X	X
Shared Secrets				X	X
Tokens	X				
Smart Cards	X		X		
Biometrics	X		X		
Certificates(PKI)	X	X	X	X	X

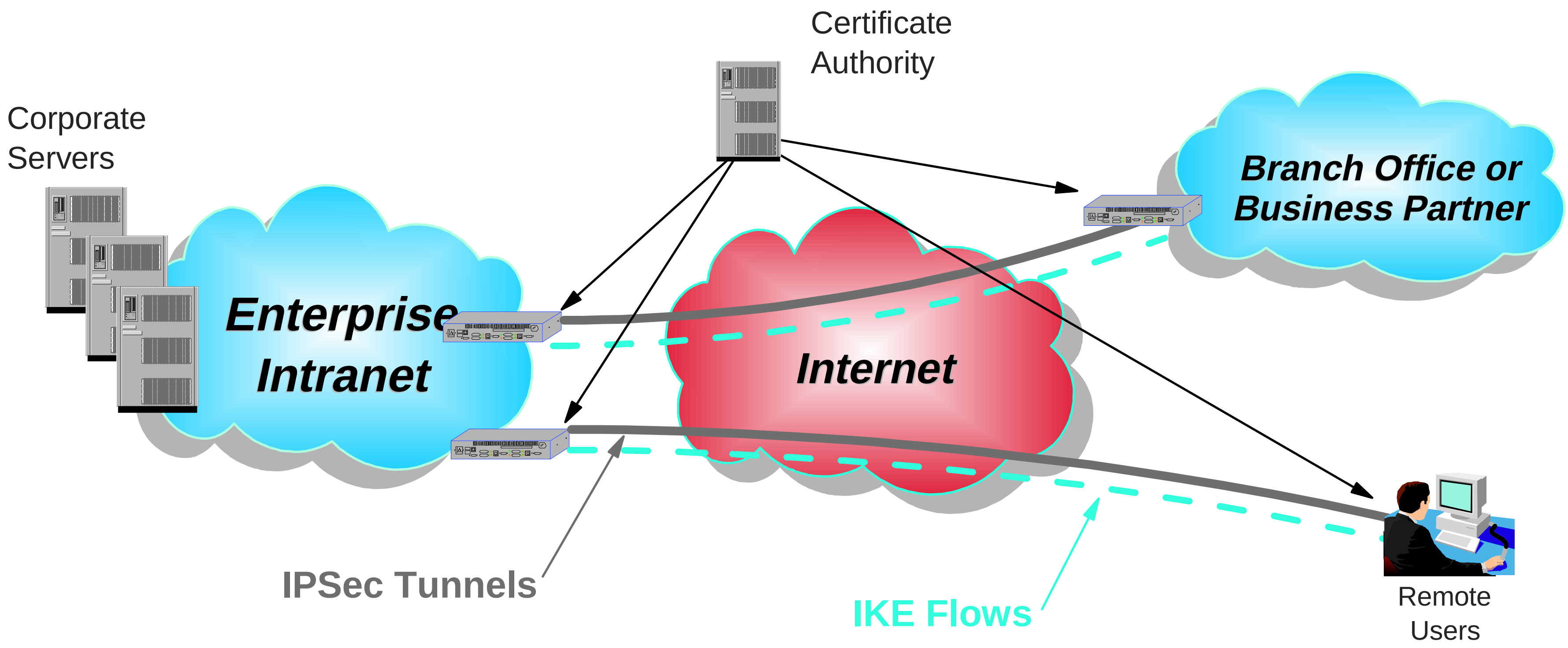
Source: Forrester Research, IBM

Digital Certificates - Certificate Authorities

- Digital certificates prevent message interception and impersonation
  - Thieves cannot represent their public keys as someone else's
  - A digital certificate is a file that binds an identity to a public key
- This bind is validated by a trusted third party, the certificate authority
  - The CA verifies the applicant and signs the digital certificate with their private key
  - X.509 is an international standard for digital certificates



IKE & Certificate Authorities

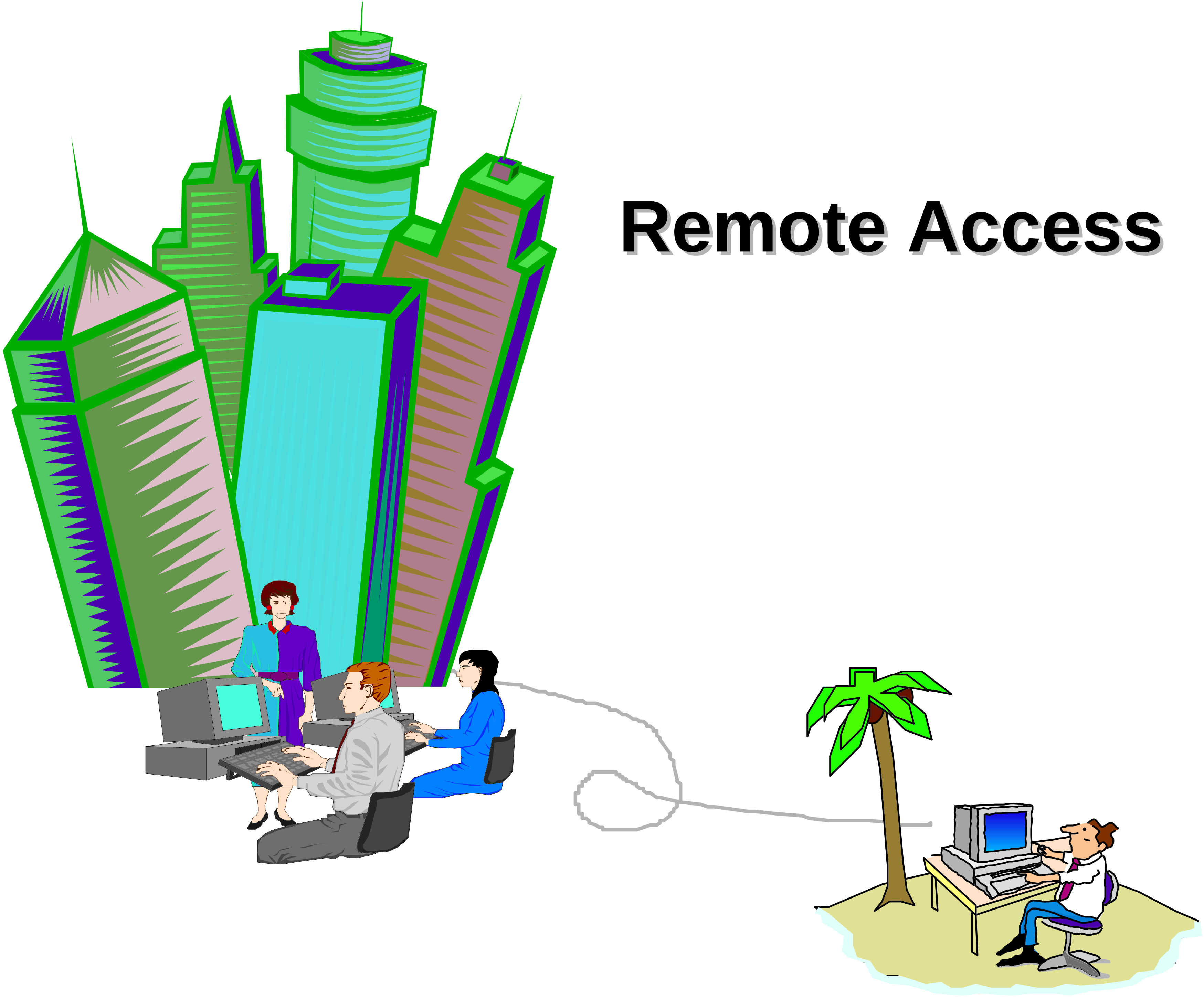


Linear scale - key to large scale networks

- Only requirement is to trust CA
- Passwords require knowledge of all partners

  (Scale expodentially)

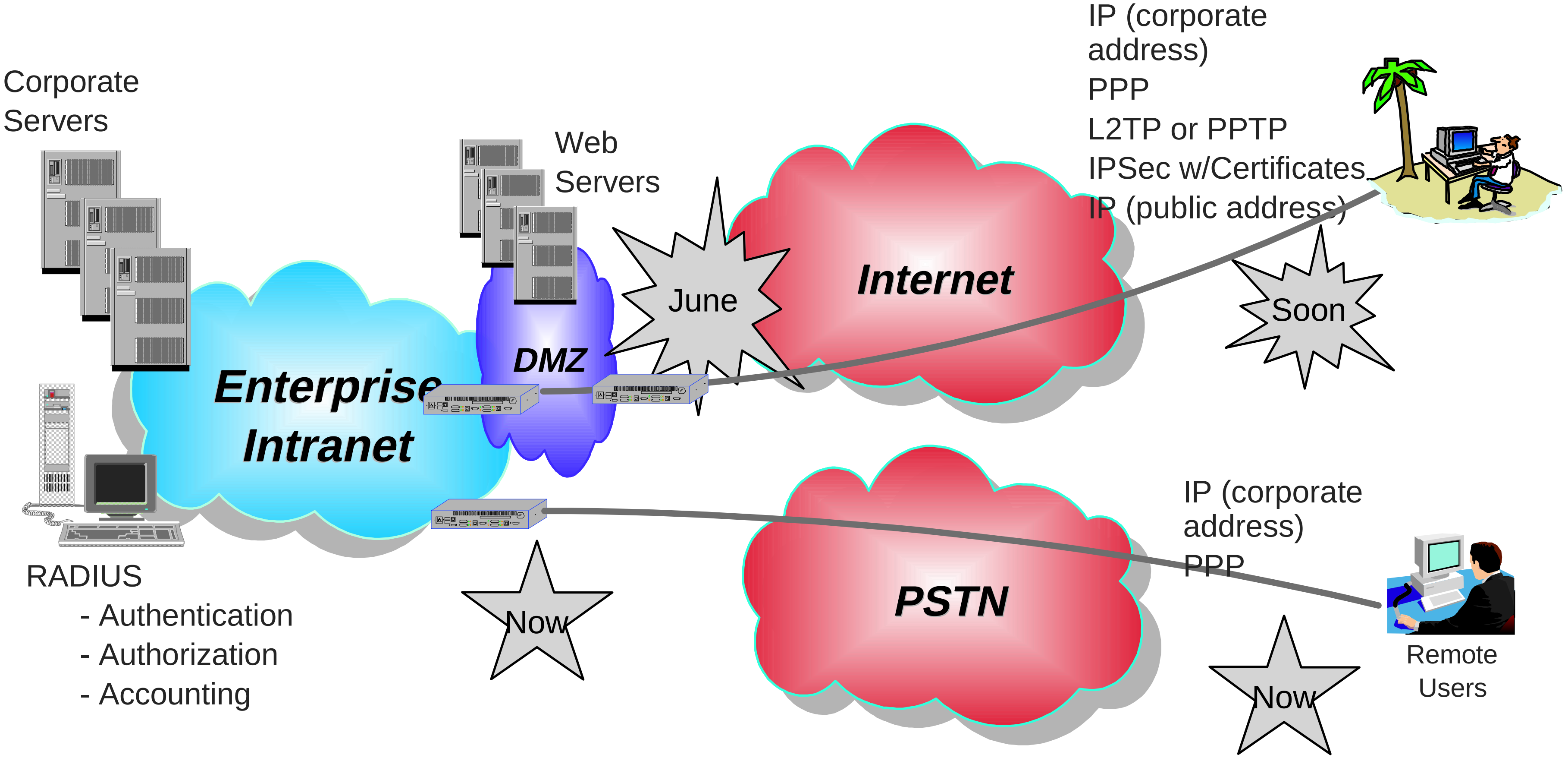
Remote Access



Comparing VPN Remote Access

	High Security	Perimeter Integration: AAA	Perimeter Integration: IP Address	Multi-protocol Transport	Low Cost
IPSec w/Certificates	X				X
L2TP (w/PPP ID & PW, RADIUS)		X	X	X	X
IPSec + L2TP (or IPSec + PPTP or IPSec + L2F)	X	X	X	X	X

VPN Remote Access



Corporate Servers

Web Servers

IP (corporate address)
PPP
L2TP or PPTP
IPSec w/Certificates
IP (public address)

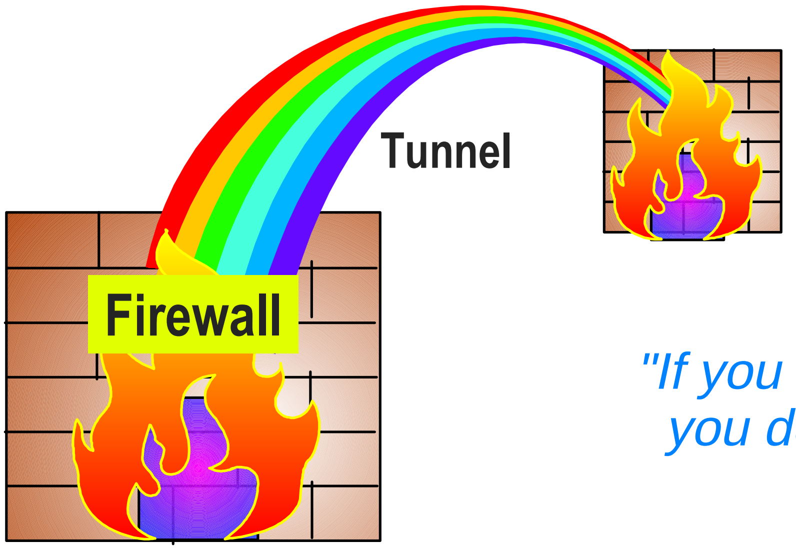
IP (corporate address)
PPP

RADIUS
- Authentication
- Authorization
- Accounting

Resource protection
Firewall filtering

How do I keep my customer from viewing confidential data?

Security is more than information tunneling

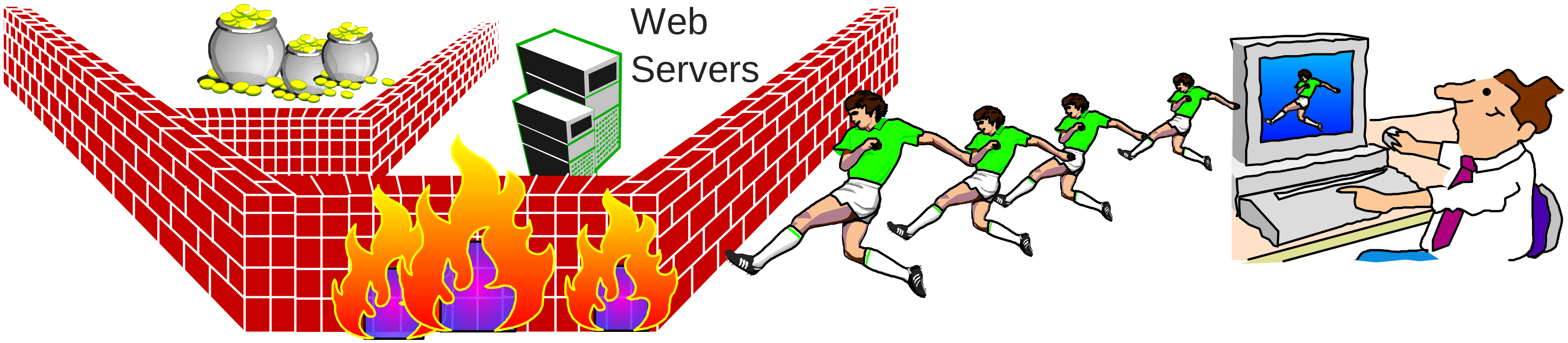


Firewalls

*"If you don't have security **everywhere**,
you don't have security **anywhere**". .*

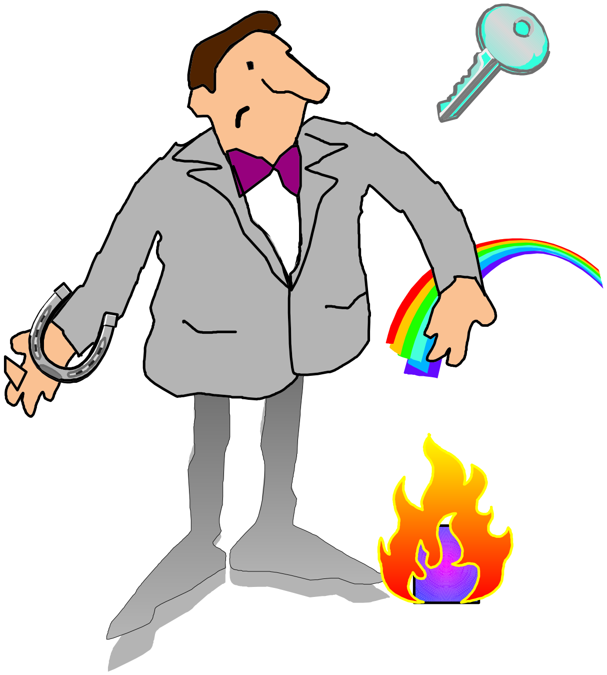
- A firewall passes only authorized traffic for trusted users
- Firewall solutions should:
  - Be integrated within remote access equipment to preserve cost-effectiveness
  - Have low-cost (e.g., software-only) versions for remote users
  - Adopt a strict policy of denying anything not expressly permitted
  - Optionally have an unprotected DMZ where Web and other public servers exist
  - Be certifiable by the International Computer Security Association

Firewall Defense



- ➢ DMZs cordon off resources available to select individuals or companies
  - ✓ Firewalls separate public information resources from confidential resources
  - ✓ VPN tunnels typically terminate at entry gateway
- ➢ Websites are generally placed in DMZs - for example
  - ✓ Product information made available to all
  - ✓ Software updates only available to licensed customers

Policy Management



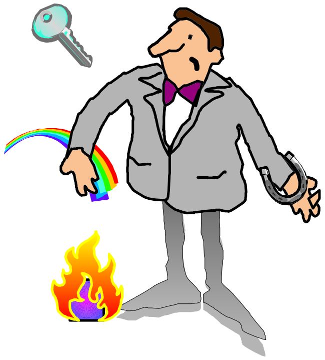
When
Where
How

- ✓VPNs are a significant part of policy
- ✓VPNs must coexist with other service level attributes such as QoS

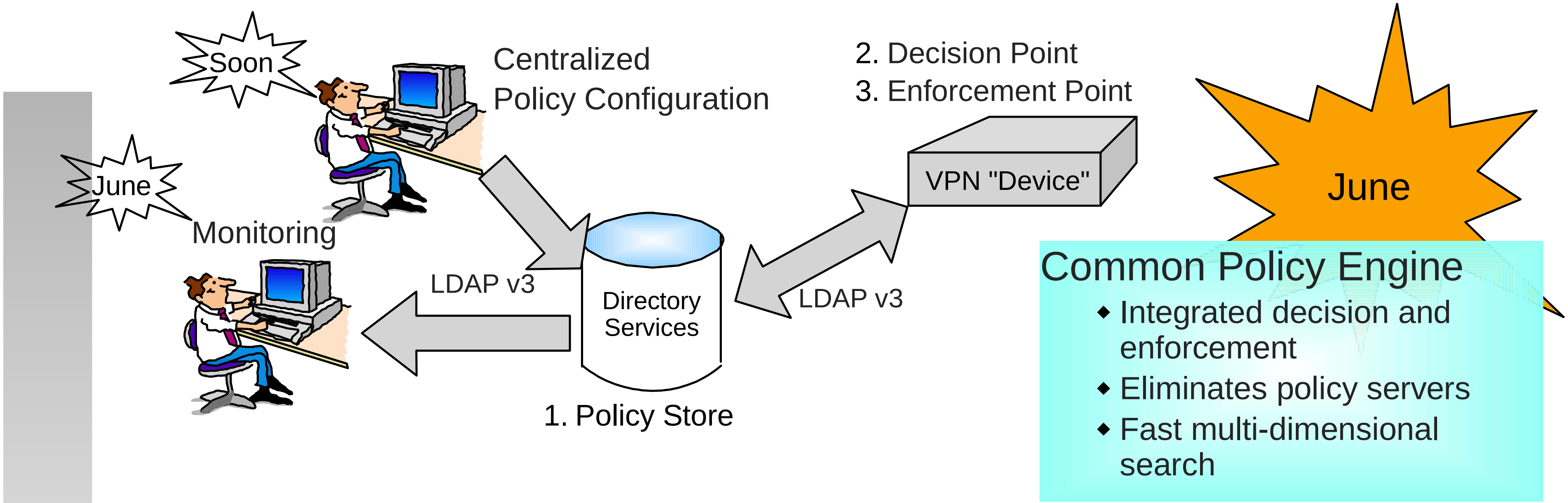
Policy Initiative

"Specific applications performing at specific levels for specific users at specific times"

- Policy Configuration: The ability to uniformly specify and distribute corporate policies to network devices
  - Which *users* can access *applications* and *servers* from *where, when*, and *how*?
  - Which *users* and *applications* have highest priority for network or server resources *when*?
- Policy Enforcement: The ability to enforce corporate directives on network behavior
- Defining Policy
  - By users: Source and destination IP address
  - By application: Source and destination ports, protocol
  - By interfaces: Inbound and outbound interface
  - May use wildcards



Rapid Packet Classification



Common Policy Engine

- Integrated decision and enforcement
- Eliminates policy servers
- Fast multi-dimensional search

1. Policy Store

   Data store that handles replication, contains schema

2. Policy Decision Point

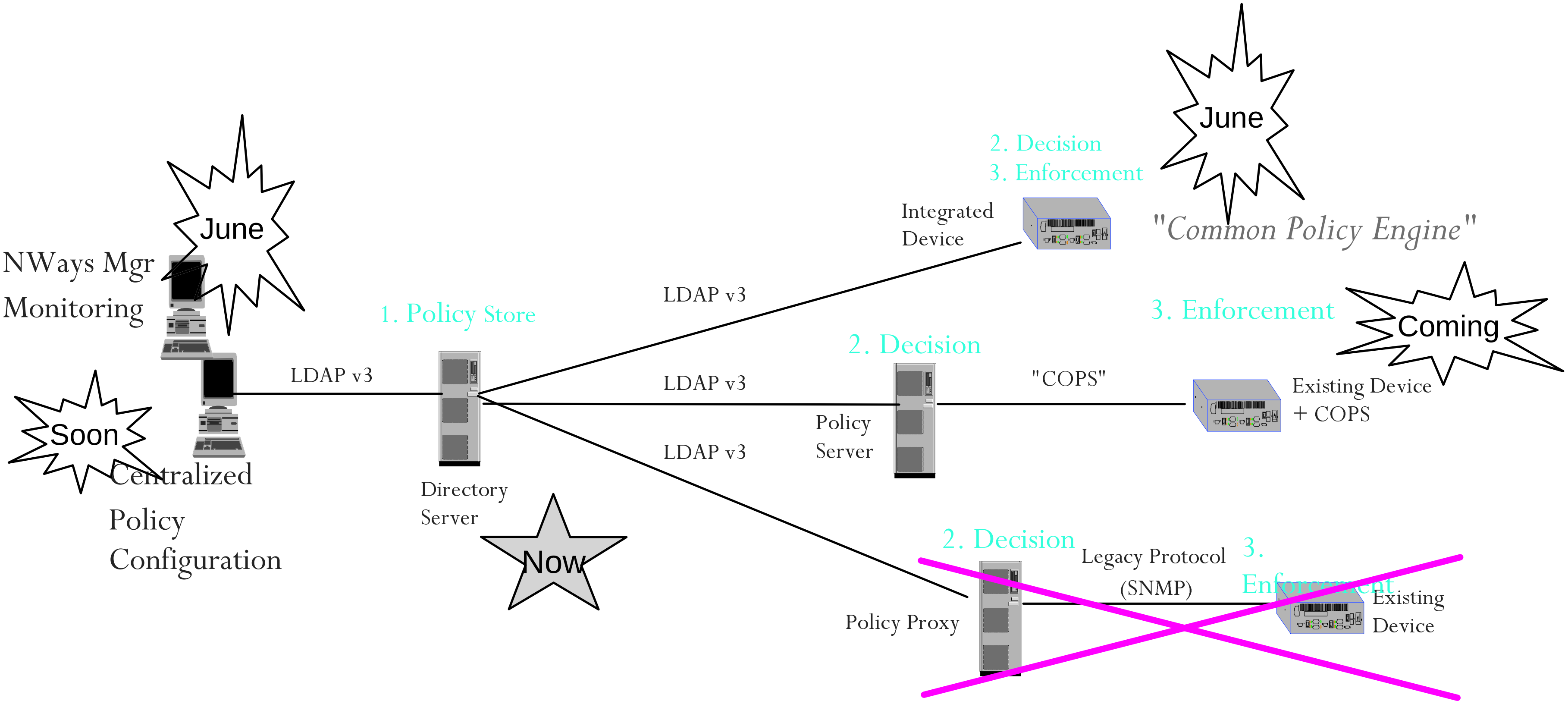
   Evaluates the resource request and makes policy decision

3. Policy Enforcement Point

   Ensure the policy is realized via packet filtering, traffic prioritization, encryption, authentication, bandwidth reservation and load balancing

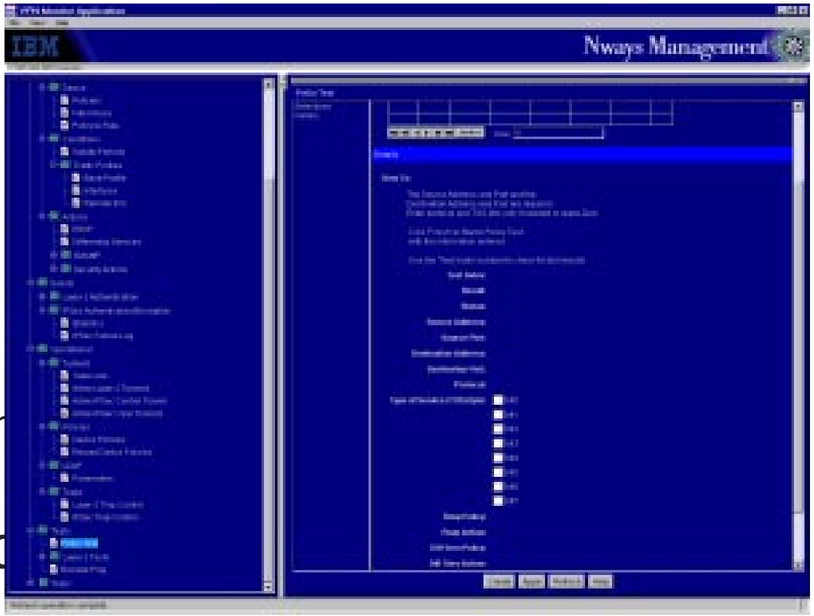
Scalable Policy Architecture

- Improved Scaleability
- Reduced bandwidth overhead
- Lower costs



Nways VPN Manager

- Monitors* VPN and IPSec policies
  - -Layer 2 Response Time Test** monitors the performance of active sessions
  - -Layer 2 Connectivity Test** verifies connectivity of proposed VPNs before implementation
- Policy Test** verifies correctness
  - -Simulates the effects of a policy in the client
  - -Compares the defined policy with the decision-tree actions that the client will take
  - -Verifies that a policy will work as expected when implemented
- Clients refresh policy when prompted by Nways VPN Manager
- Supported on AIX, HP/UX, HP OpenView, and Windows NT



Nways VPN Manager tests policies to verify correctness

* Preview

** Patent pending

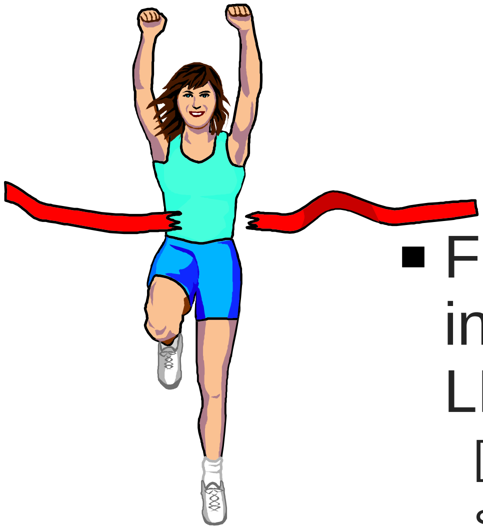
Differentiated Services for Standards based QoS

Transmission rate and latency guaranteed for policy-selected frame relay or PPP IPv4 packets

- Interprets the industry pre-standard schema for DiffServ policy
- Performs rapid packet classification based upon 8 slectors
  - Allows use the DiffServ field as a classifier (e.g., place traffic into a VPN tunnel based upon the DiffServ setting)
- Enforces DiffServ marking based upon policy
  - Including remarking of proprietary TOS implementations to industry standard DiffServ

Where we've been
Where we are going

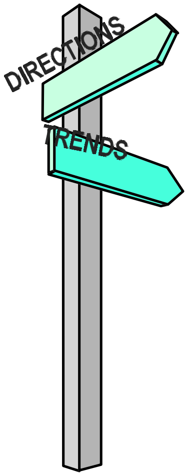
IBM's Key implementation elements



- First routers with integrated LDAP client using industry standard policies directly from the LDAP Directory Server

  [eNetwork LDAP Directory (OS/390,AIX,OS/400), Novell Directory Services*, Netscape Directory*]

- Interpretation of industry standard schema for VPN and QoS
- IBM research innovation - rapid classification algorithms - enforces Security (VPN) and Quality of Service (Diffserv) policies 25X faster than competing approaches
- Patent pending policy test and monitoring in Nways Manager

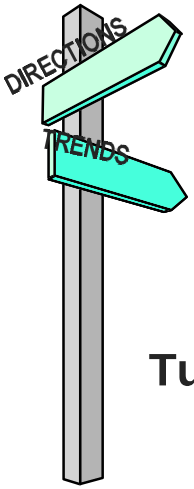


IBM Network Products - Scalable VPNs

- Scaleable authentication (certificates)
- Automatic key generation and distribution (IKE)
- Centralized monitoring and management
- Scaleable policy enforcement architecture
- Service Level Agreements (SLAs)
- Hardware encryption assist
- Centralized network policy configuration
  - Point & click policy application
  - Tool performs consistency checking
- Hardware key generation assist

IPSec Implementation

- Currently shipping (2210, 2212, 2216, NetUtility)
  - NAT, Filtering (firewall)
  - IPSec
  - Manual Keys
  - Integrated IPSec & L2TP
- Scheduled (2210, 2212, 2216, NetUtility, Switches, Other)
  - IKE
  - Certificates (PKI)
  - LDAP client (DEN Enablement)
  - Improved Scaleability
  - Policy Infrastructure
  - Centralized Configuration
  - Integrated IPSec & {L2TP, L2F, PPTP}
  - IPSec Client for Remote Access (Single User Dial-in)
  - Hardware Assists



VPN Functions

Tunneling Protocols

- PPTP, including compression
- L2TP, L2F, IPSec

Authentication Services

- PKIX, LDAP (internal & external)
- X.509 digital certificates
- RADIUS, TACAS+, PAP/CHAP

Encryption

- Up to 128 bit keys
- DES, Triple-DES

Integrity

- HMAC-MD5, HMAC-SHA-1

Key Management

- Shared secret
- IKE (ISAKMP/Oakley)

Accounting

- RADIUS interface
- Event, system, security and configuration

Management

- Centralized monitoring
- Centralized management

Firewall

- Individual user or user group
- Flexible filtering
    - Source and destination IP address
    - Port, service and protocol type

Dial-in Client

- IPSec, L2TP
- Windows 95 or Windows NT (or later)

- Providing corporate network integrity to e-business transactions
  - ✓ Leveraging 35+ years of corporate networking experience to IP networks
    - ➤ Integrated VPN and Diff Serve policy - linking RSVP to DS
    - ➤ IPSec and L2TP combined for multiprotocol support
  - ✓ Provide scaleable, manageable and secure networking
    - ➤ Integrated policy engine
    - ➤ Tunnel management using 'pre-standard' MIBs
    - ➤ Development of an inventive management approach with unlimited scaleability
- Offering complete user-to-application (end-to-end) security solutions
  - ✓ Providing global office-to-office integrity across the Internet
    - ➤ Routing product support for IPSec, L2TP, X.509, RSA, filtering etc.
    - ➤ S/390 & AS/400 server support of VPN
    - ➤ Firewall support of VPN
  - ✓ Migrating direct dial customers to VPN
    - ➤ Development of remote client with IPSec and L2TP support