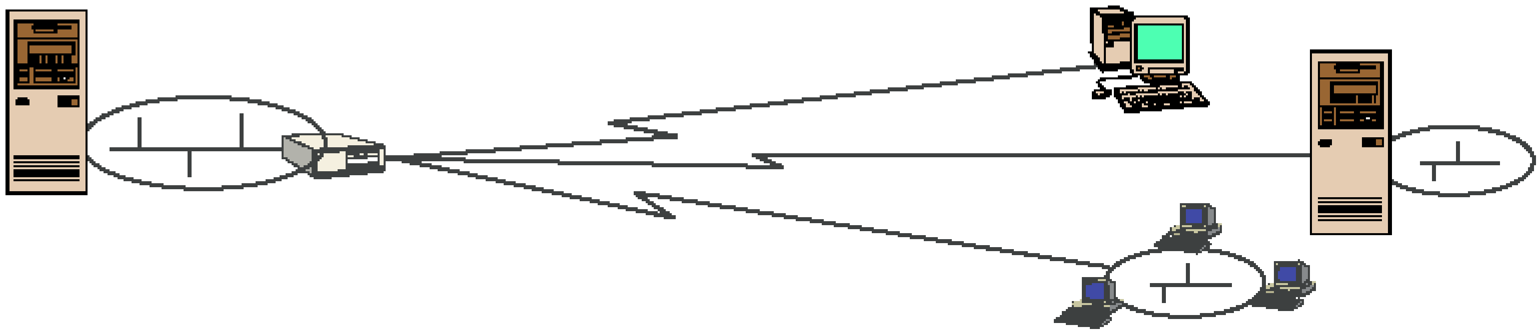
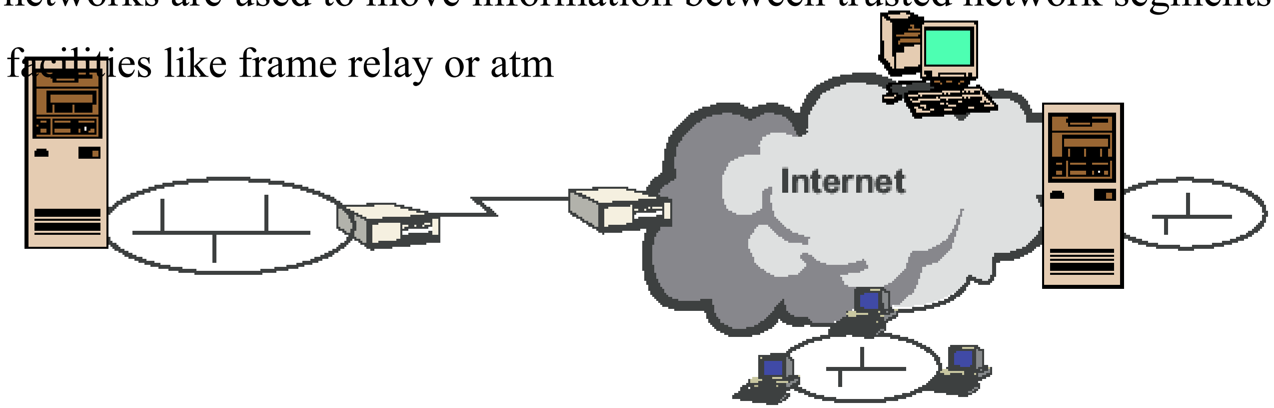
Virtual Private Networks

Fred Baker

What is a VPN



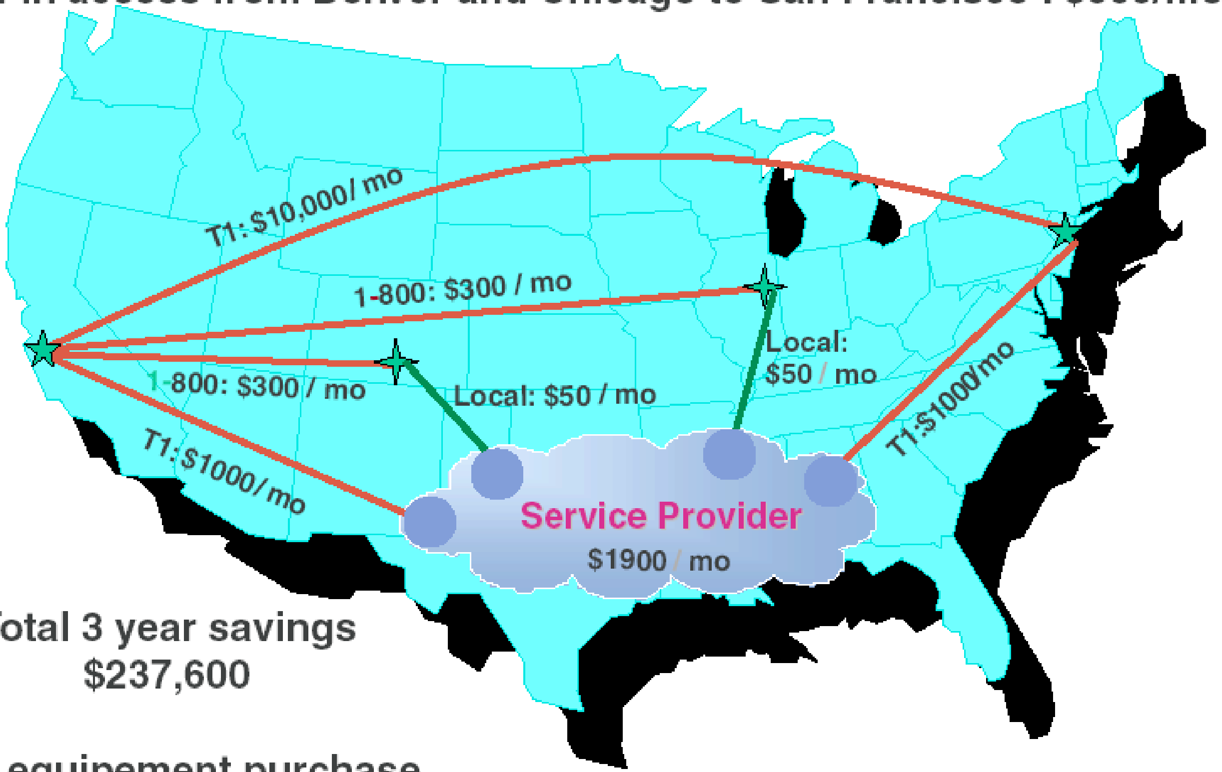
Public networks are used to move information between trusted network segments using shared facilities like frame relay or atm



A VIRTUAL Private Network replaces all of the above utilizing the public Internet
Performance and availability depend on your ISP and the Internet

Why?

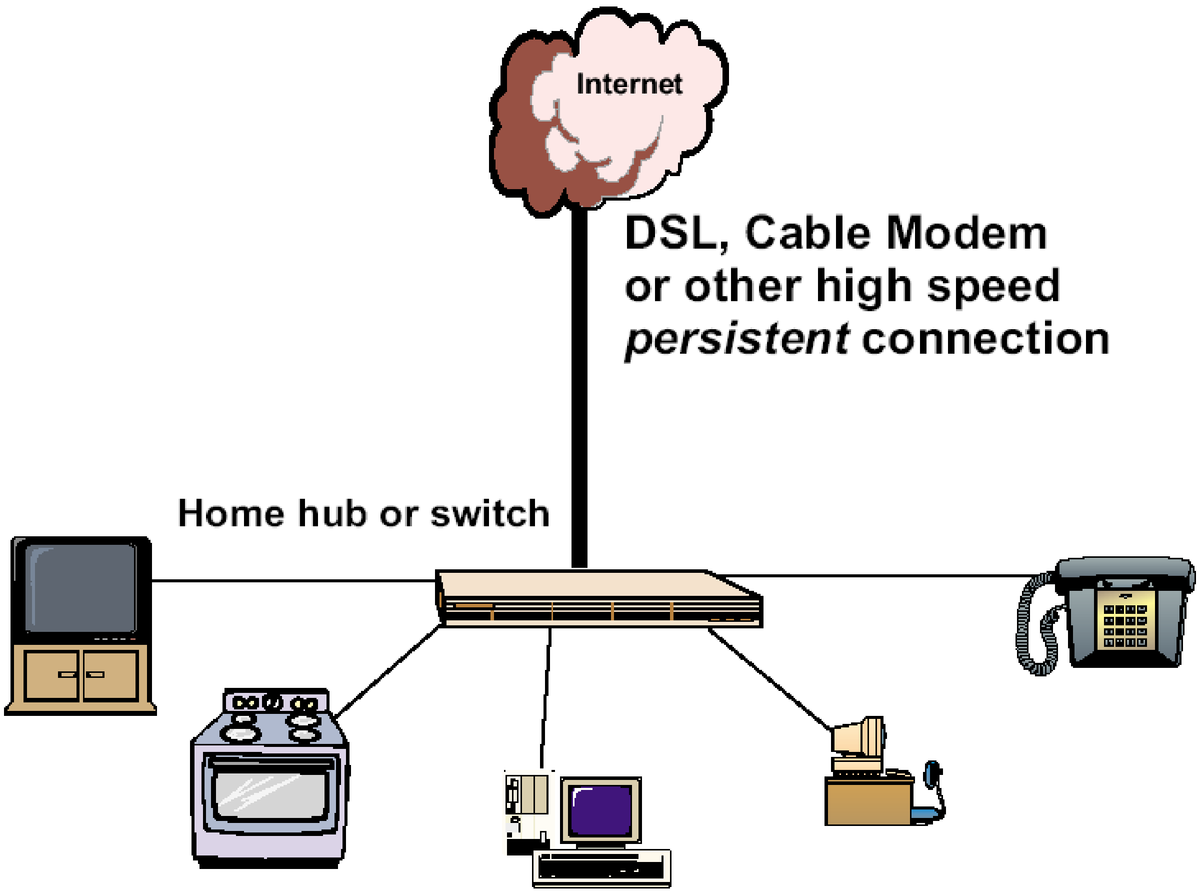
T1 connections between San Francisco and New York City : $10,000/mo
Dial-in access from Denver and Chicago to San Francisco : $600/mo



Total 3 year savings
$237,600

VPN equipement purchase
$7,800

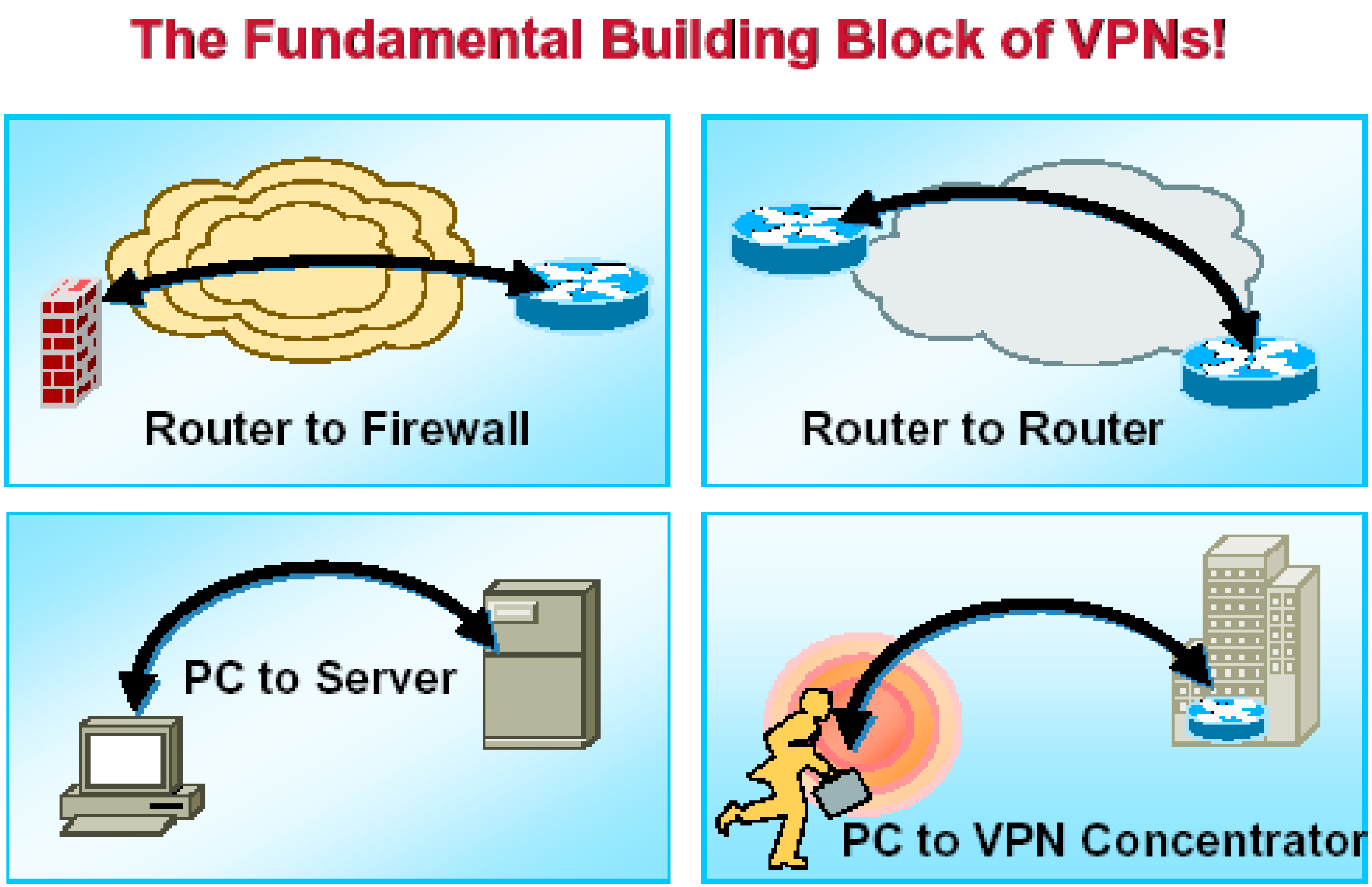
HomeNet to the office.



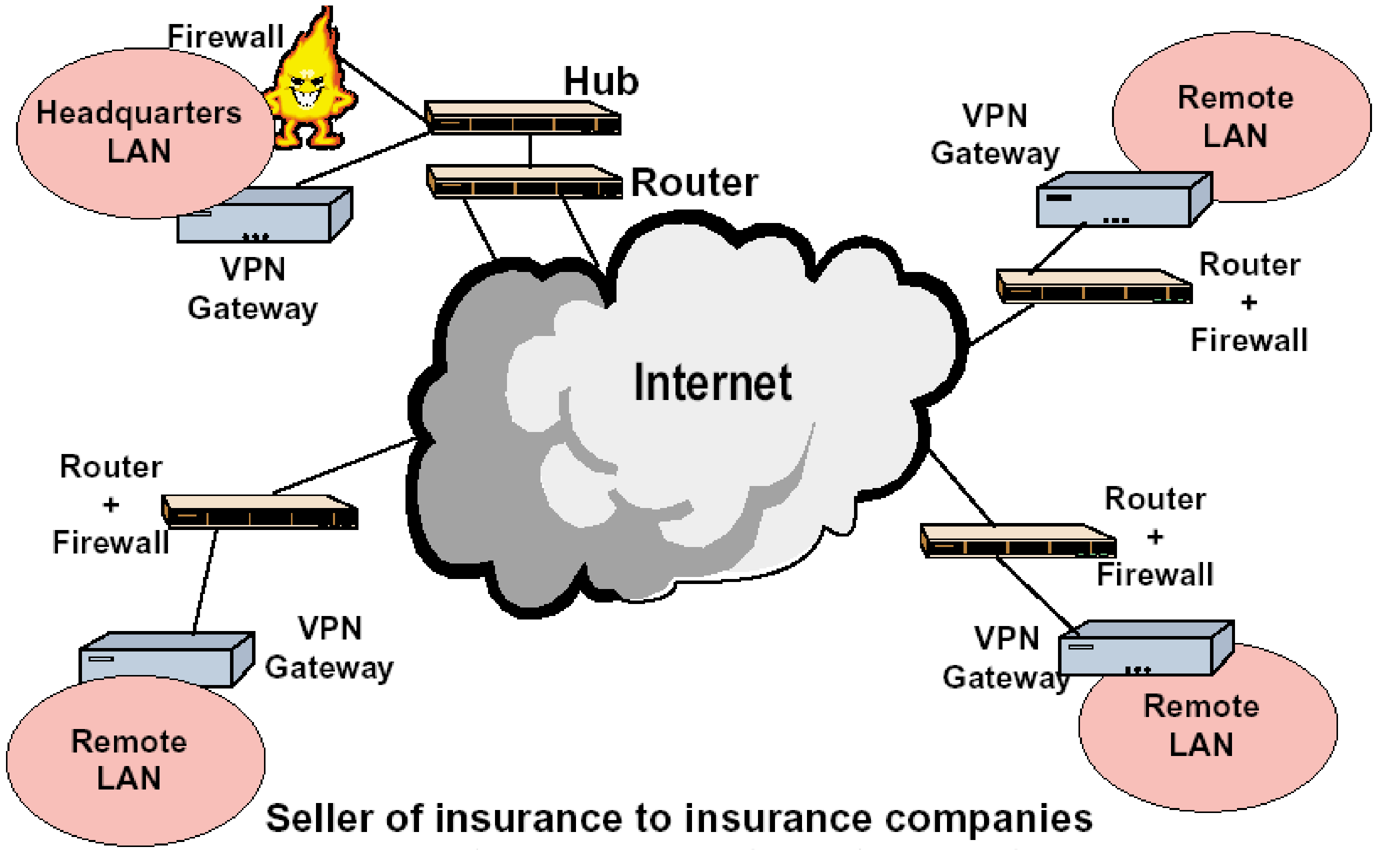
VPN Types

Use	Application	Alternative To	Benefits
Remote Access VPN	Remote Connectivity	Dedicated Dial ISDN	Ubiquitous Access Lower Cost
IntranetVPN	Site-to-Site Internal Connectivity	Leased Line	Extend Connectivity Lower Cost
ExtranetVPN	Business-to-Business External Connectivity	Fax, Mail, EDI	Facilitates E-Commerce

VPN Implementations



VPN as your Intranet

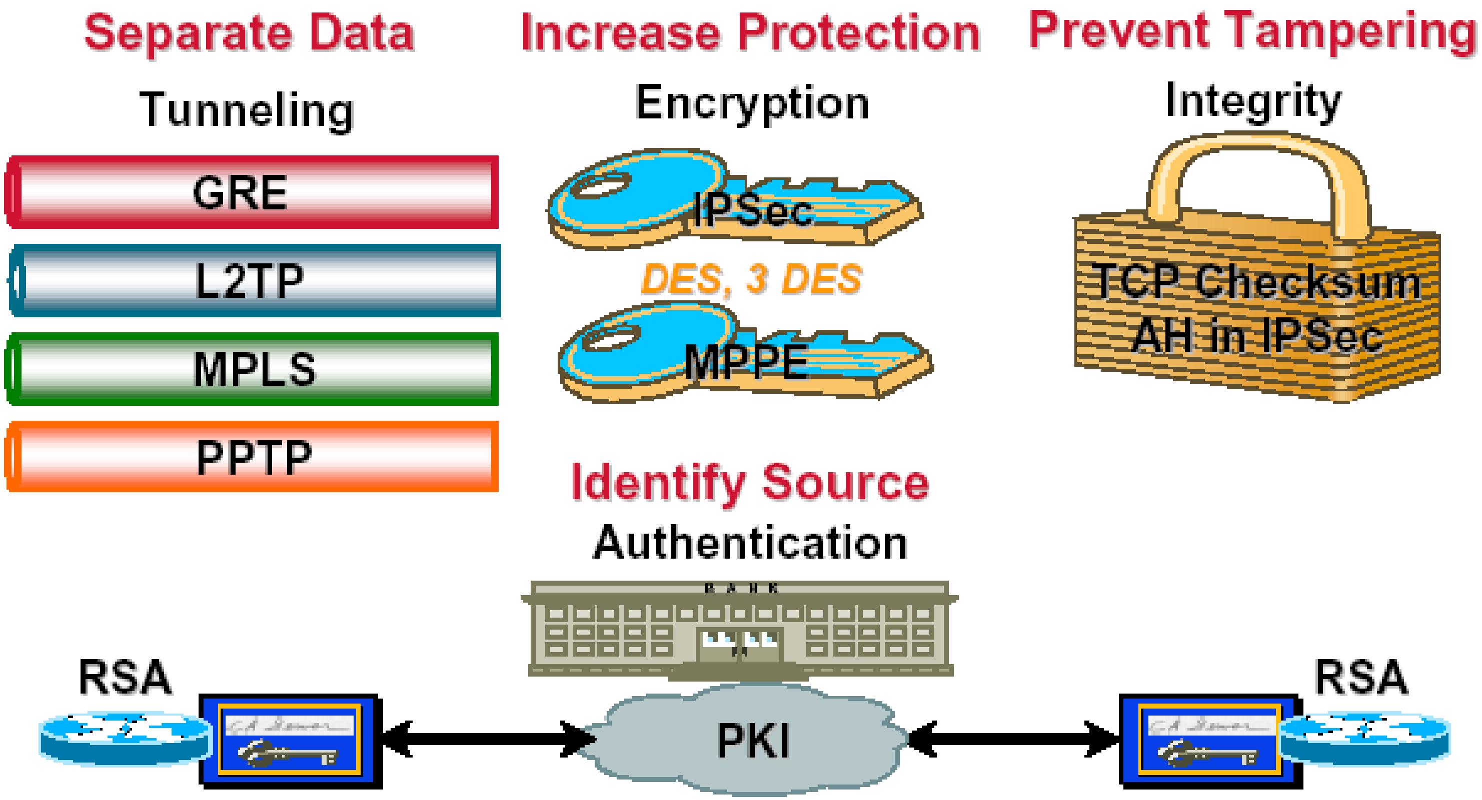


Seller of insurance to insurance companies
No legacy network allowed them to jump to VPN
VPN gateway has combined encryption and authentication

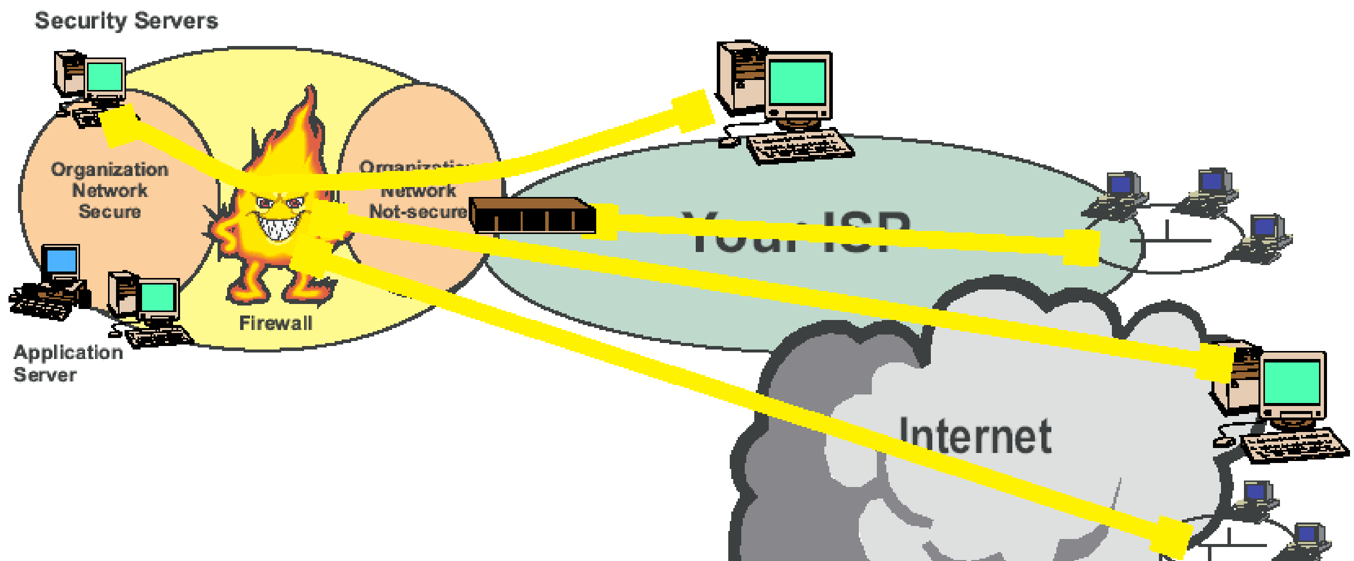
What a VPN needs

- VPNs must be encrypted
  - so no one can read it
- VPNs must be authenticated
- No one outside the VPN can alter the VPN
- All parties to the VPN must agree on the security properties

VPN Components

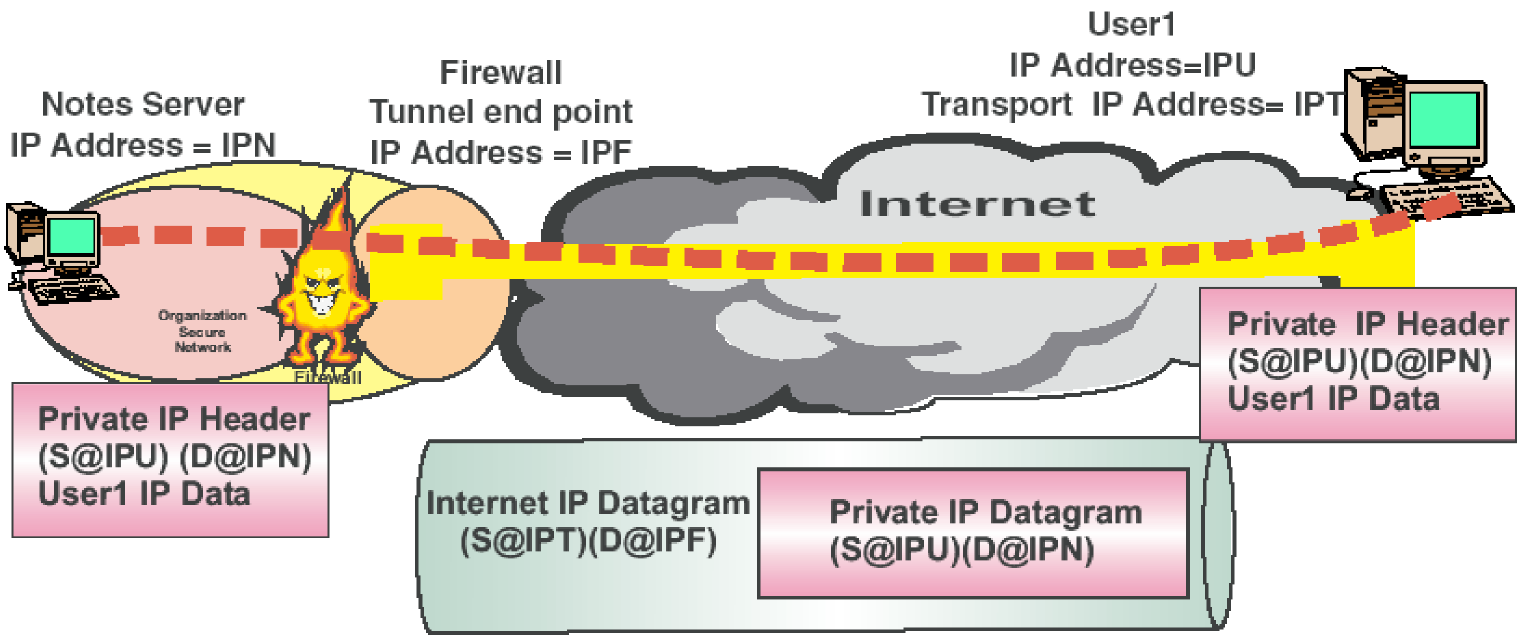


Parts of a VPN

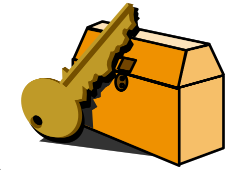


Physical connection to Internet/ISP
Building the tunnel
Security servers
Management
Provisioning
Quality of Service (QoS)

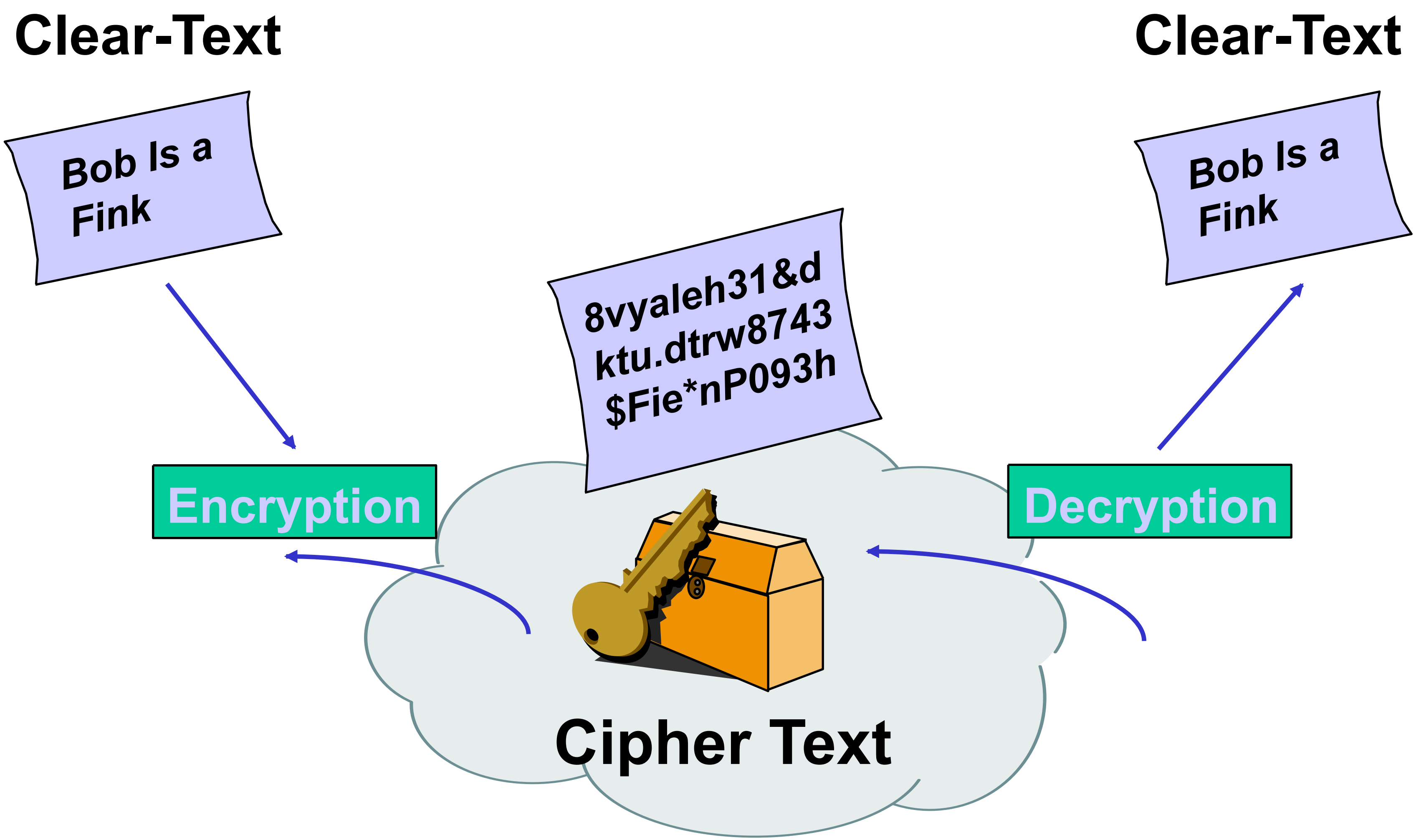
VPN works via crypto/Encapsulation



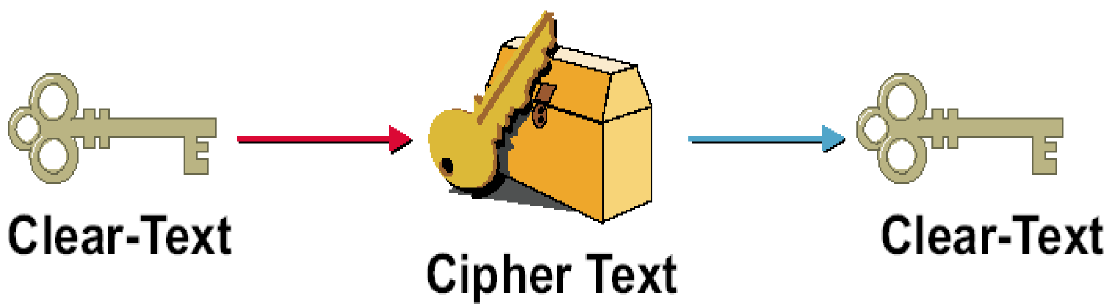
Tunneling includes
encapsulation
transmission
un-encapsulation



Encryption and Decryption



Basic Crypto – Keys are key



Components
- Keys
- Mathematical algorithms
- Message digest

Types
- Secret (symmetric)
- Public (asymmetric)

PKI
- Public Key Infrastructure

International politics

2 Kinds Key Systems

Secret Key - Symmetric

Same key used by
sender and receiver

Key used to encrypt
and decrypt data

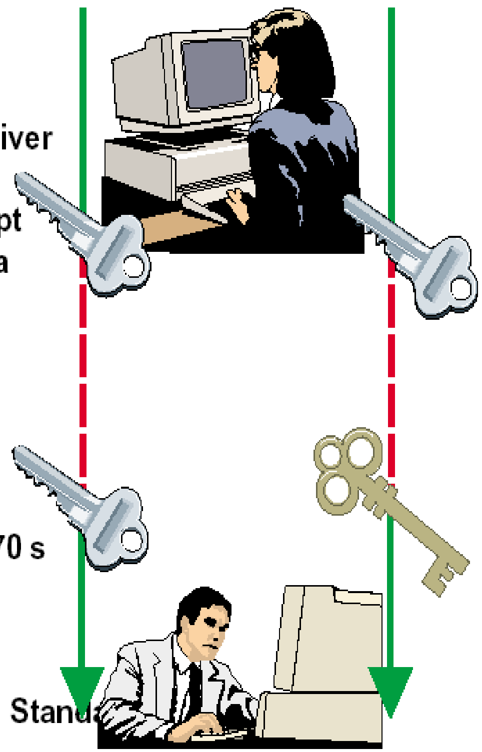
Rely on users to
protect the key

Very fast

Used since the 1970 s

Most popular
DES
(Data Encryption Stand

Most widely used today



Public Key - Asymmetric

Two keys
public and private

Public key known

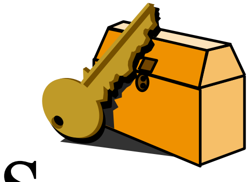
Private key kept
confidential by owner

Slower than symmetric key

More complex
- key distribution

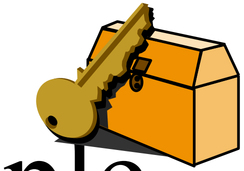
Most popular
RSA

Symmetric Key Algorithms

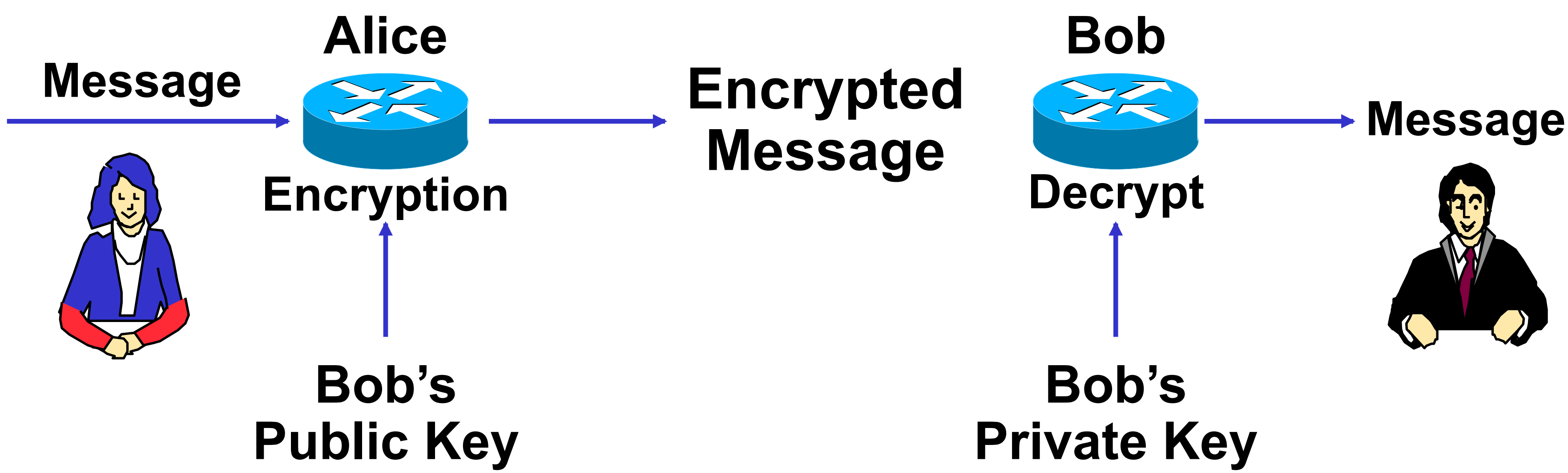


- DES—56-bit key
- Triple-DES—encrypt, decrypt, encrypt, using either two or three
  56-bit keys
- IDEA—128-bit key
- Blowfish—variable-length key, up to 448 bits

Public Key Encryption Example



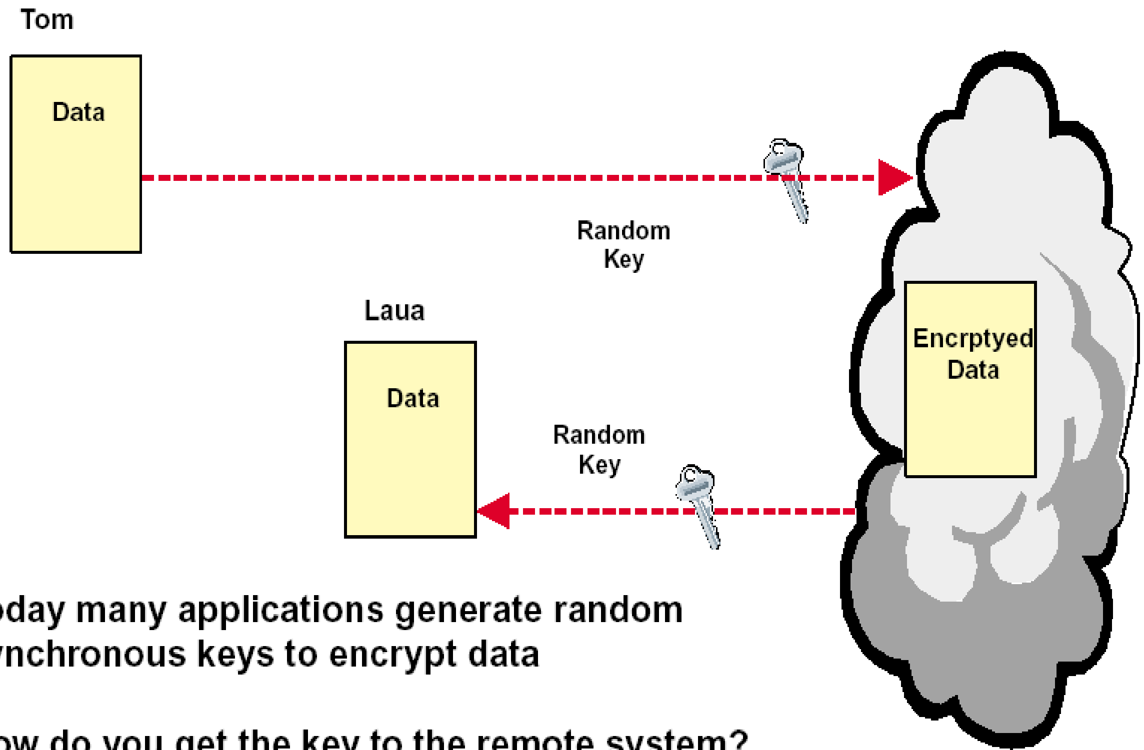
- Alice wants to send Bob encrypted data
  - Alice gets Bob's public key
  - Alice encrypts the data with Bob's public key
  - Alice sends the encrypted data to Bob
- Bob decrypts the data with his private key



PKI vs Symmetric Key

- PKI easier as you don’t have to manage keys on a per user basis
- But MUCH more compute intensive (up to 1000 times faster)
- Many systems do a combination I.e. PGP
  - –Use PKI to send a symmetric key
  - –Then use the symmetric key to crypto the data

Using Crypto in real life

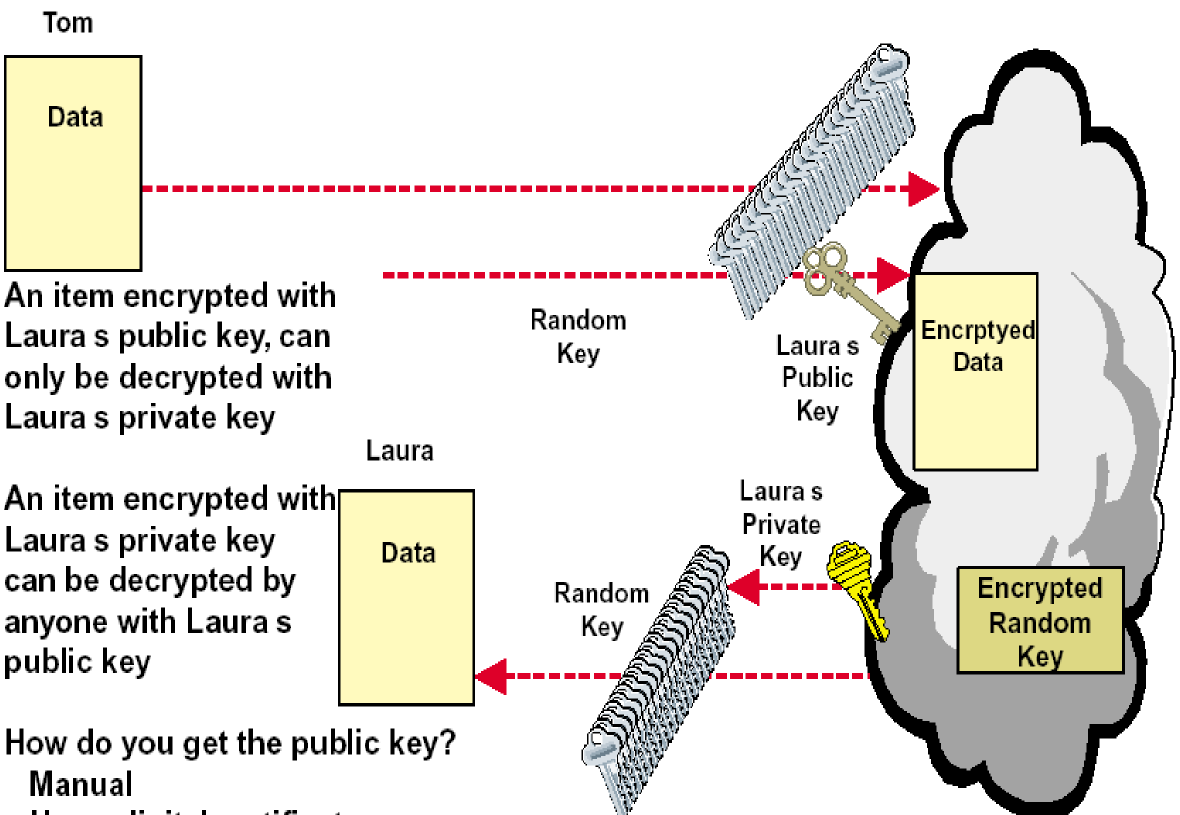


Today many applications generate random synchronous keys to encrypt data

How do you get the key to the remote system?

- Manual
- Using public/private keys

PKI to send Private Keys

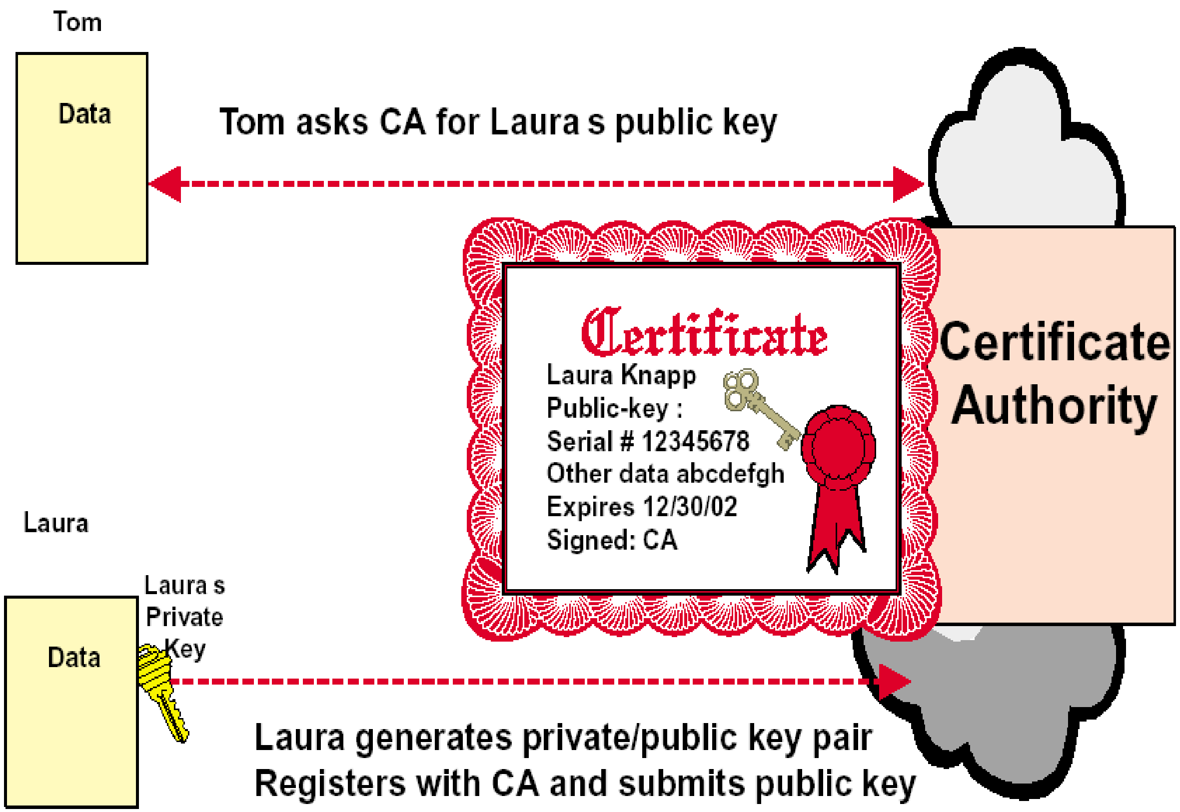


An item encrypted with Laura s public key, can only be decrypted with Laura s private key

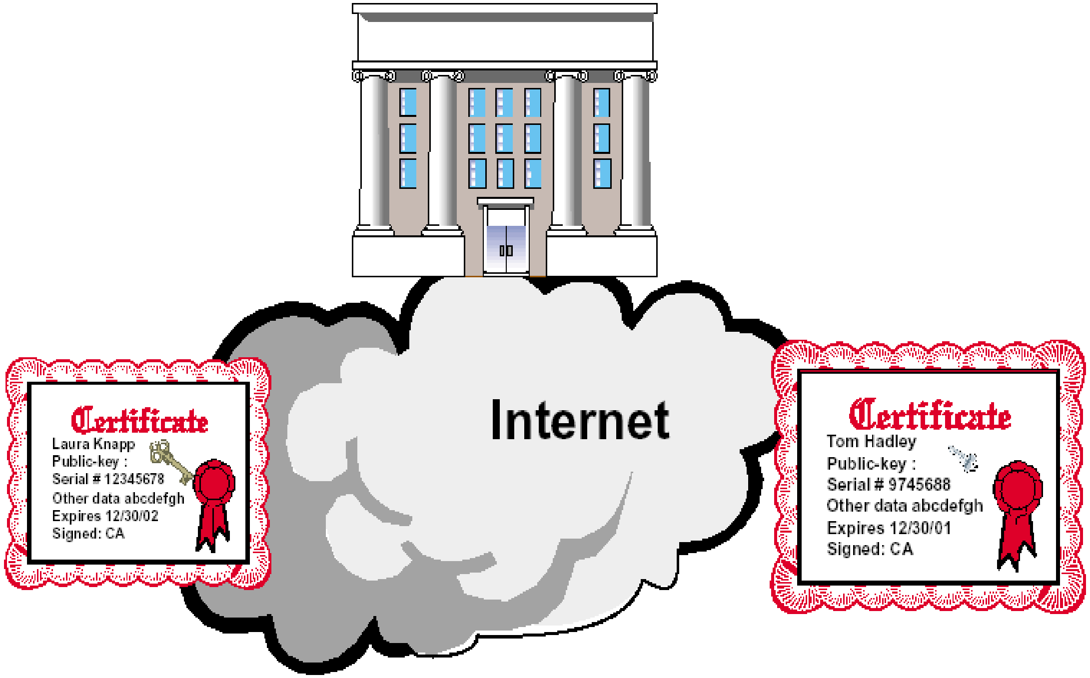
An item encrypted with Laura s private key can be decrypted by anyone with Laura s public key

How do you get the public key?
- Manual
- Use a digital certificate

PKI Certs a way to authenticate

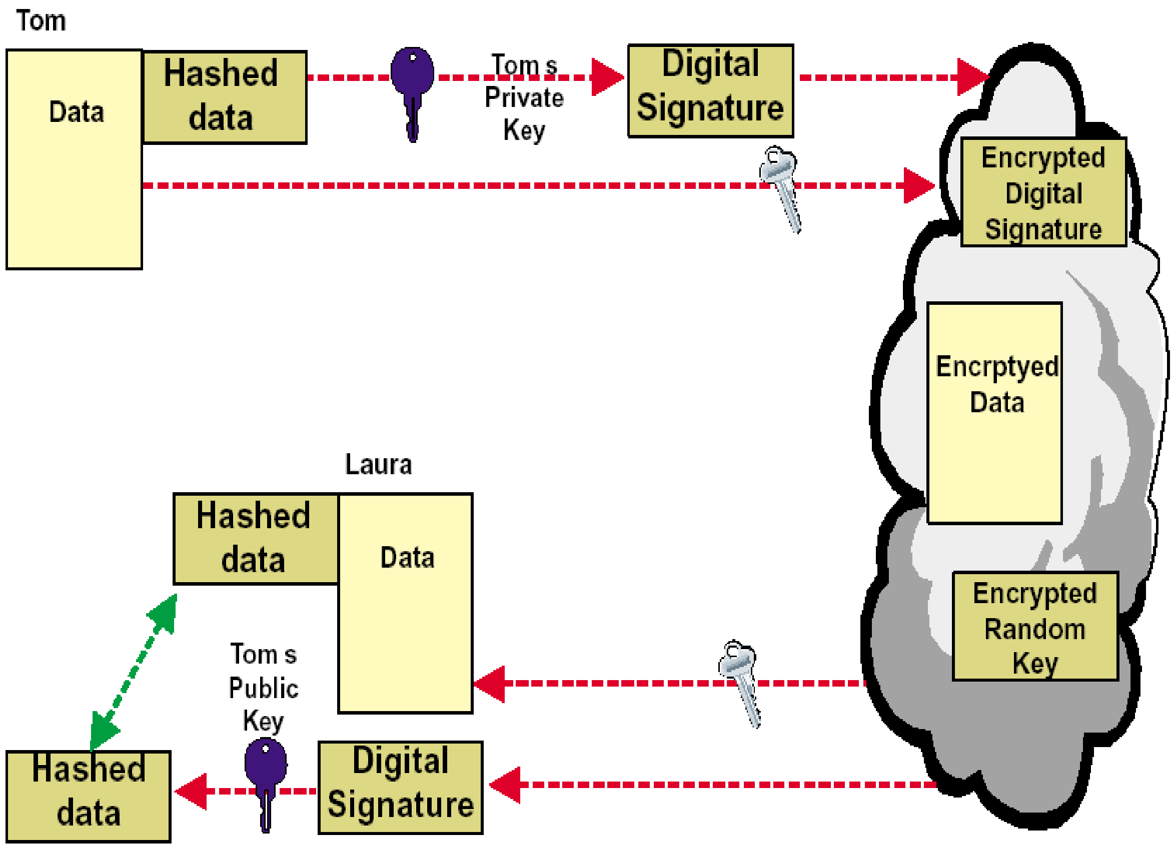


Prove the user cert Certificates of authority

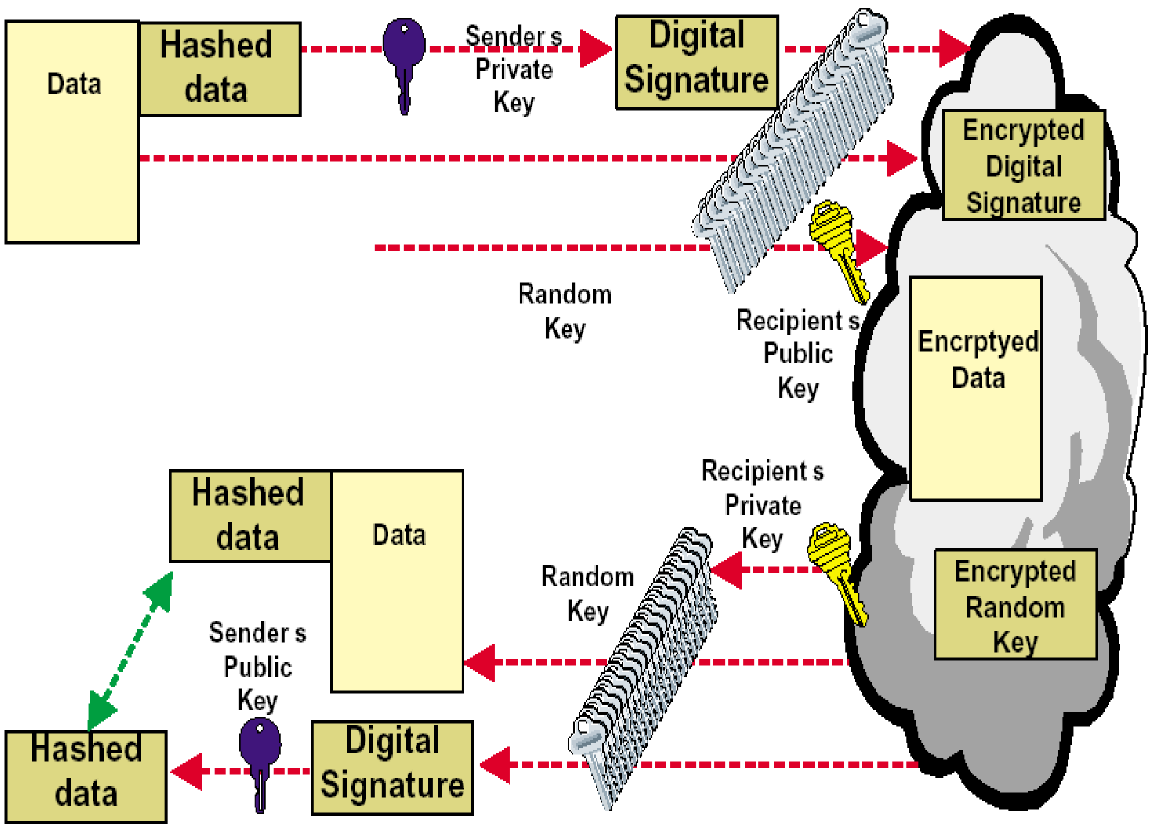


Certificate Authority (CA) verifies identity
CA signs digital certificate containing public key
Certificate equivalent to an ID card

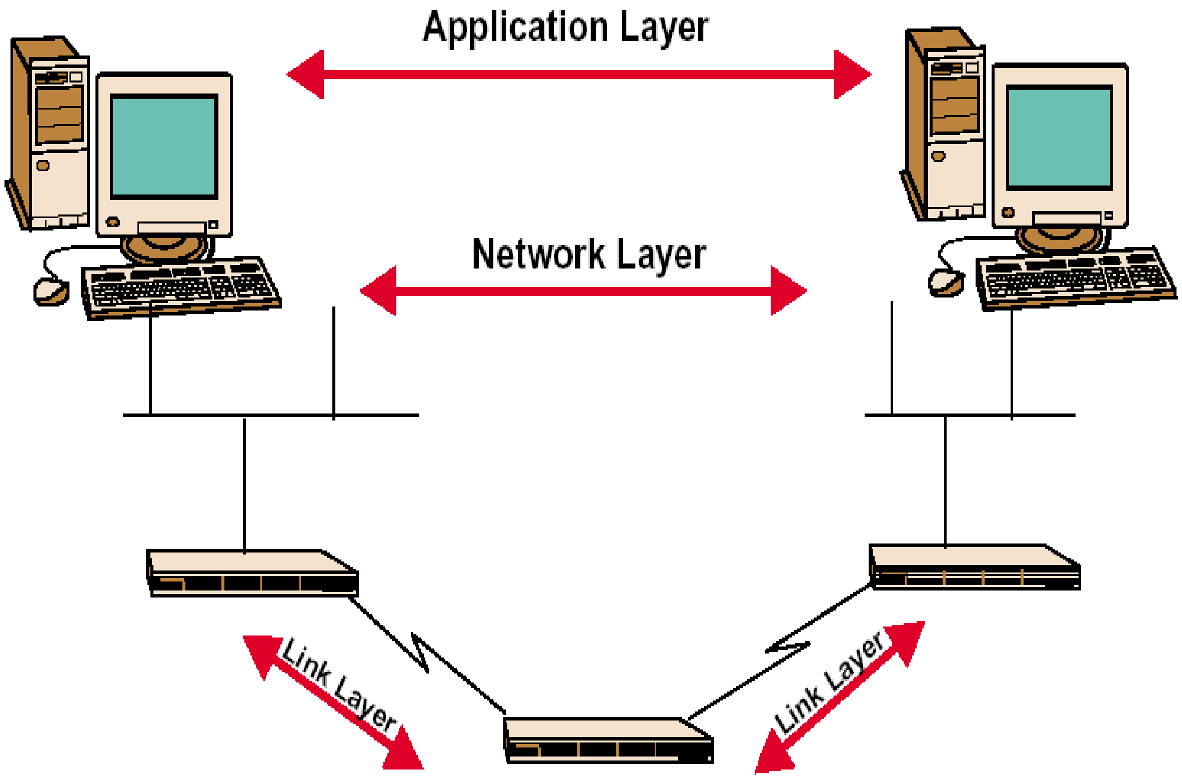
Digital Signature to verify data not changed in transit



PKI the full picture



Where you do Crypto

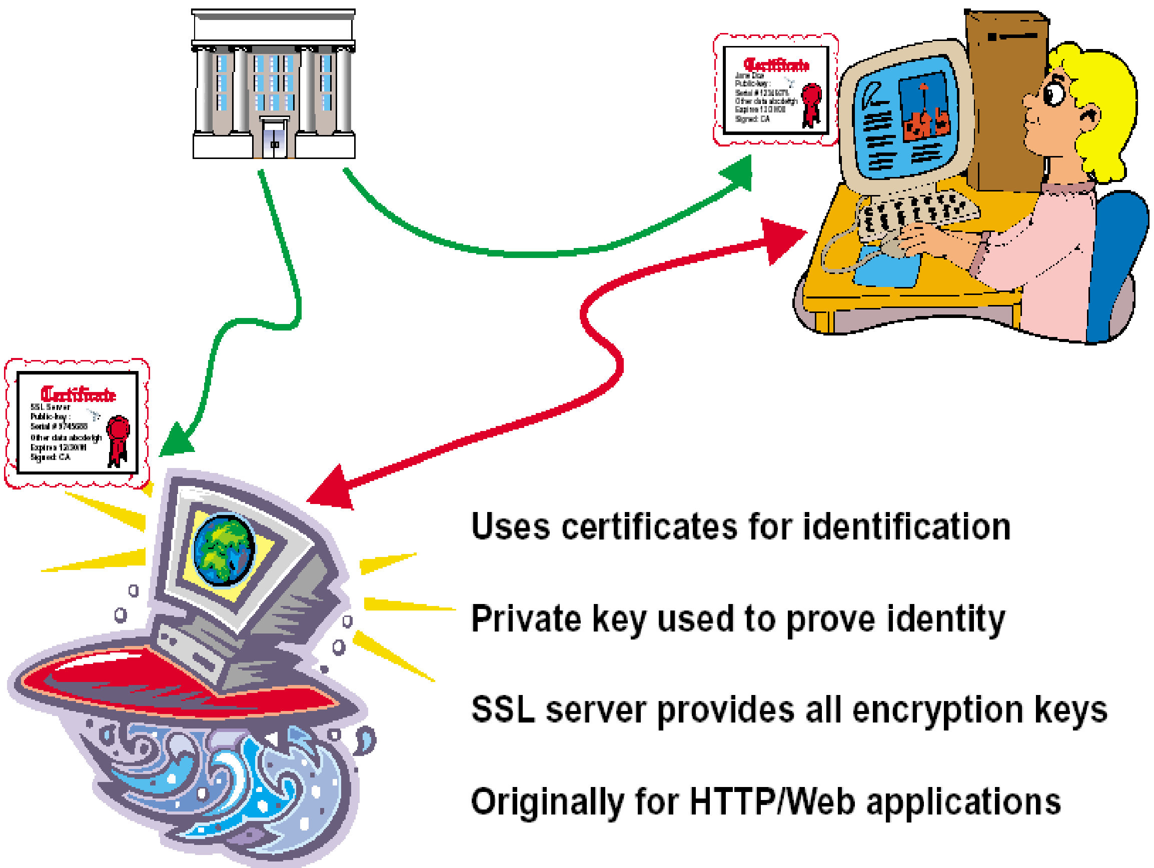


Technologies

	Simplicity Low cost	Advanced Security
Application to Application	SSL	
End to End	IPSec Transport Mode	
Gateway to Gateway	PPTP	L2TP/IPSec IPSec Tunnel Mode
Client to Gateway	PPTP	L2TP/IPSec

PPTP - Point to Point Tunneling Protocol - Layer 2 - Multiprotocol
L2TP/IPSec - Layer 2 Tunneling Protocol - Multiprotocol - Encryption and Authentication
IPSec - IP Security - Layer 3 - IP protocol - Encryption and Authentication
SSL - Secure Sockets Layer - Layer 6/7 - Application - Encryption and Authentication

Application Layer: SSL



Uses certificates for identification

Private key used to prove identity

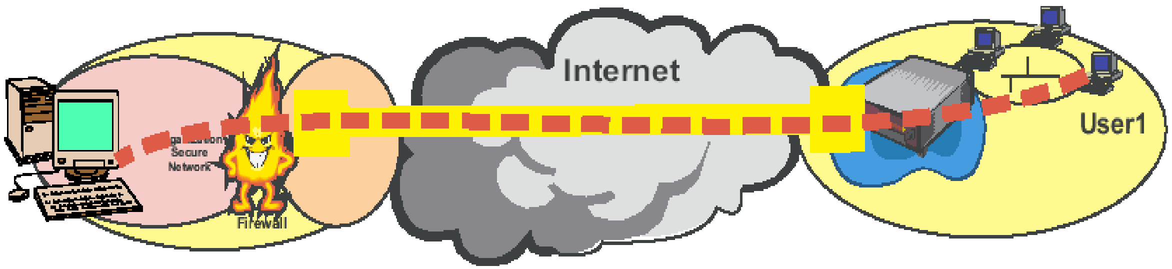
SSL server provides all encryption keys

Originally for HTTP/Web applications

Transport Layer: IPSEC

- A standard
- is composed of:
  - Diffie-Huffman key exchange
  - PKI for the DH exchanges
  - DES and other bulk encryption
  - Hash to authenticate packets
  - Digital Certificates to validate keys

Transport Layer: IPSEC VPNs
3 parts



Builds the tunnel

Integrated security technologies

ESP = Encapsulating Security Payloads - encrypts IP datagram

- DES and 3DES are most common encryption mechanisms used
- May provide confidentiality, authentication, integrity, non-repudiation, replay protection, and traffic analysis protection
- Does everything AH does

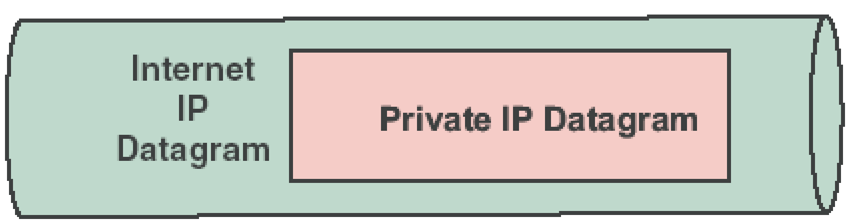
AH = Authentication Header - validates sender and indicates data integrity

- MD5 and SHA1 are most common authentication mechanisms used
- Provides integrity and authentication but not confidentiality

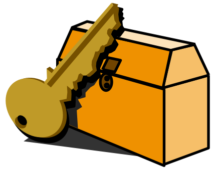
IKE - Internet Key Exchange (aka:ISAKMP/Oakley) Protocol

Tunnel vs Transport

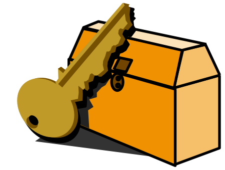
- Transport
  - Implemented by the end point systems
  - Real address to real address
  - Cannot ‘go through’ other networks
- Tunnel
  - Encapsulation of the original IP packet in another packet
  - Can ‘go through’ other networks
  - End systems need not support this
  - Often PC to a box on the ‘inside’



Diffie-Hellman Key Exchange (1976)



- By openly exchanging non-secret numbers, two people can compute a unique shared secret number known only to them



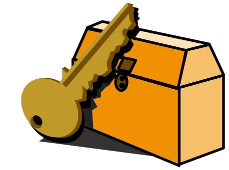
Modular Exponentiation

Both g and p Are Shared and Well-Known

- **Generator, g**
- **Modulus (prime), p**
- **$Y = g^X \bmod p$**

2^237276162930753723 mod 79927397984597926572651

Diffie-Hellman Public Key Exchange



Alice

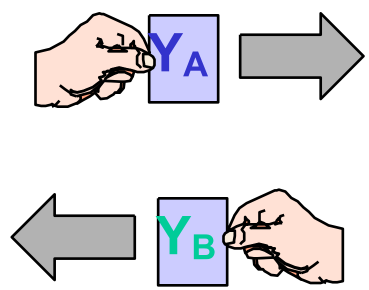
Private Value, X_A
Public Value, Y_A

$$Y_A = g^{X_A} \text{ mod } p$$

Private Value, X_B
Public Value, Y_B

Bob

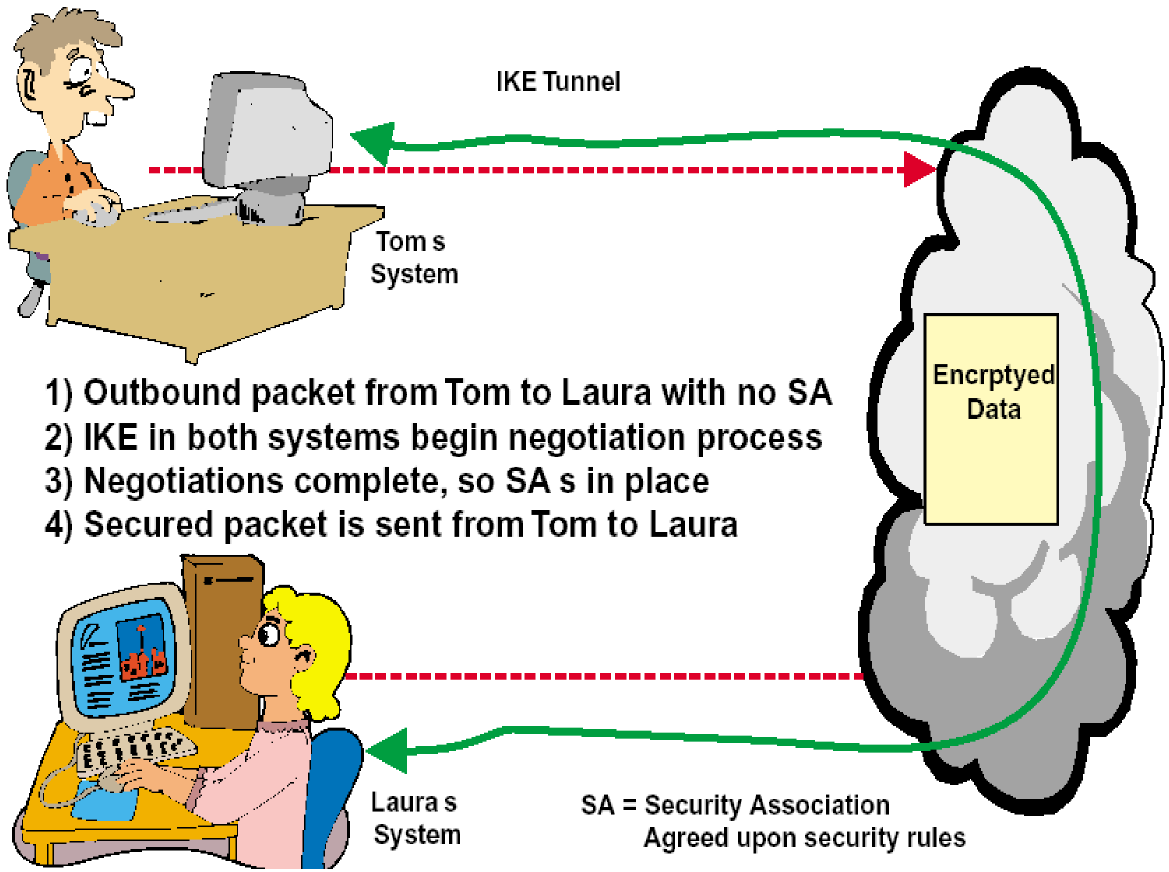
$$Y_B = g^{X_B} \text{ mod } p$$



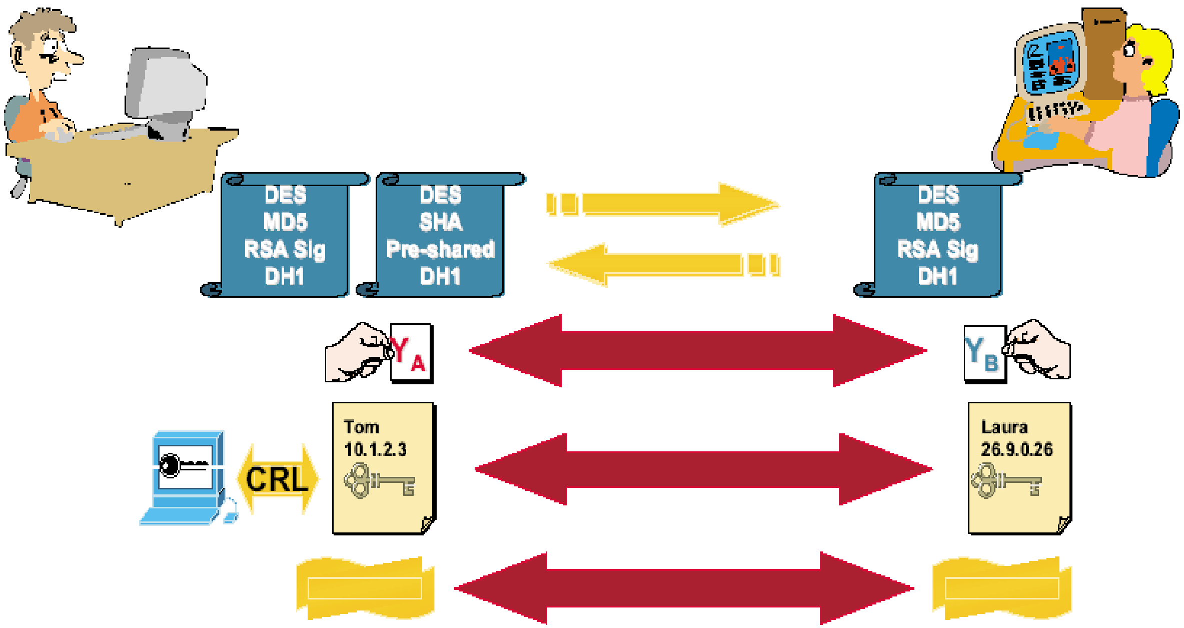
$$Y_B^{X_A} \text{ mod } p = g^{X_A X_B} \text{ mod } p = Y_A^{X_B} \text{ mod } p$$

(shared secret)

Security Association is the agreement on how to secure

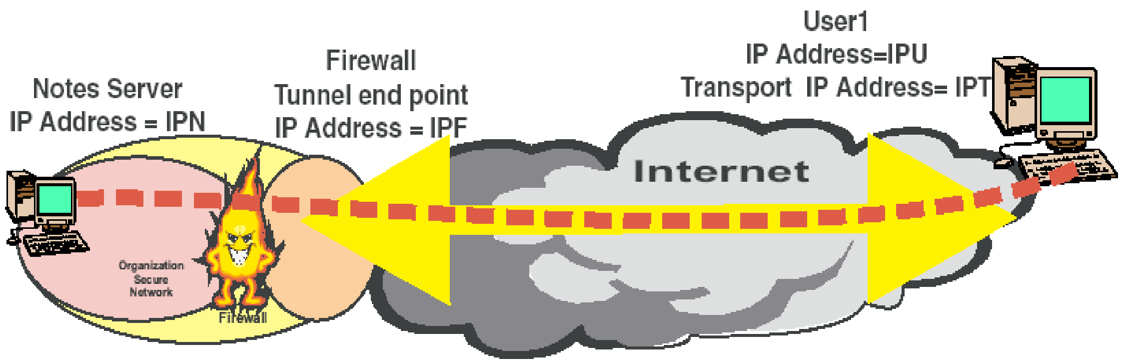


create the ISAKMP SA
(Internet Security Association Key Management Protocol)



Negotiate IKE parameters
Exchange public keys
Exchange certificates and check Certificate Revocation List (CRL)
Exchange signed data for authentication

IPSEC Key Exchange (IKE)



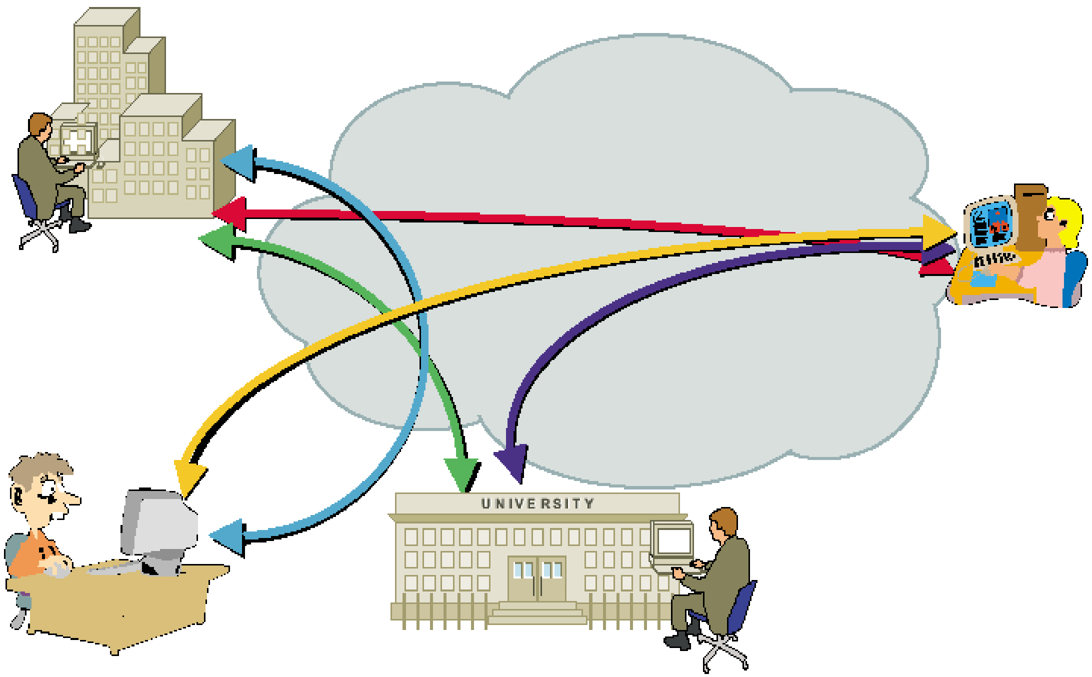
Agree on parameters
Exchange keys
Use encrypted tunnels

Manual Key Management
- Administrator sets up keys at both ends
- Not scalable

Automated Key Managment
- On-demand creation of keys
- Complex to configure
- Scalable

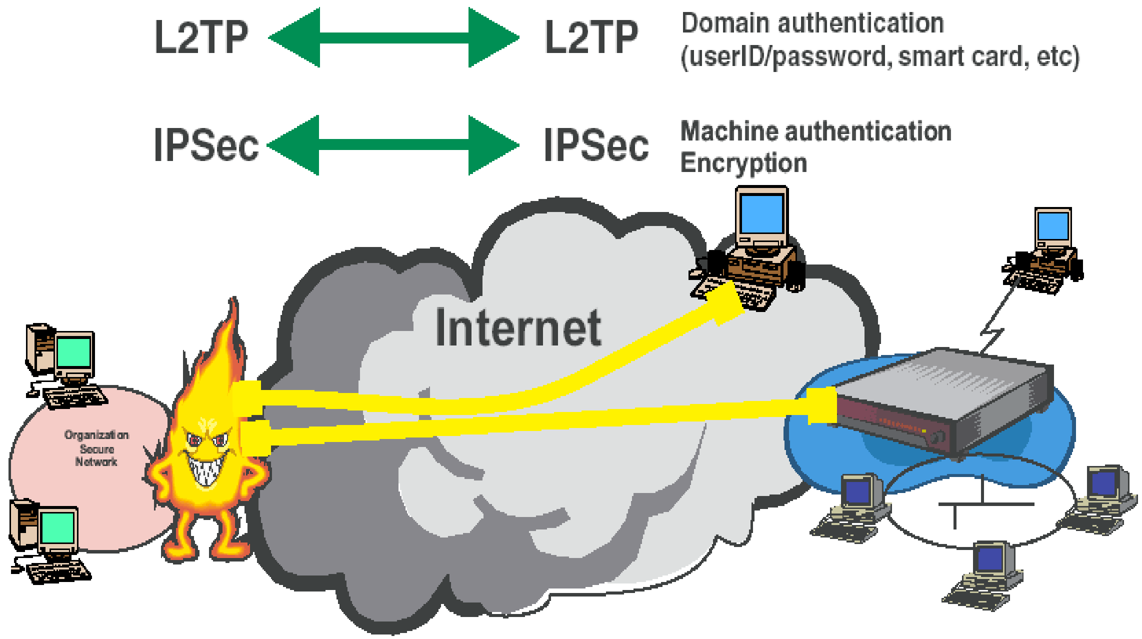
Two parties negotiate
- Encryption algorithm
- Hash digests
- Authentication
- Key strength
- Security association lifetimes

IKE allows scale as I do not need to hard code passwords for each pair



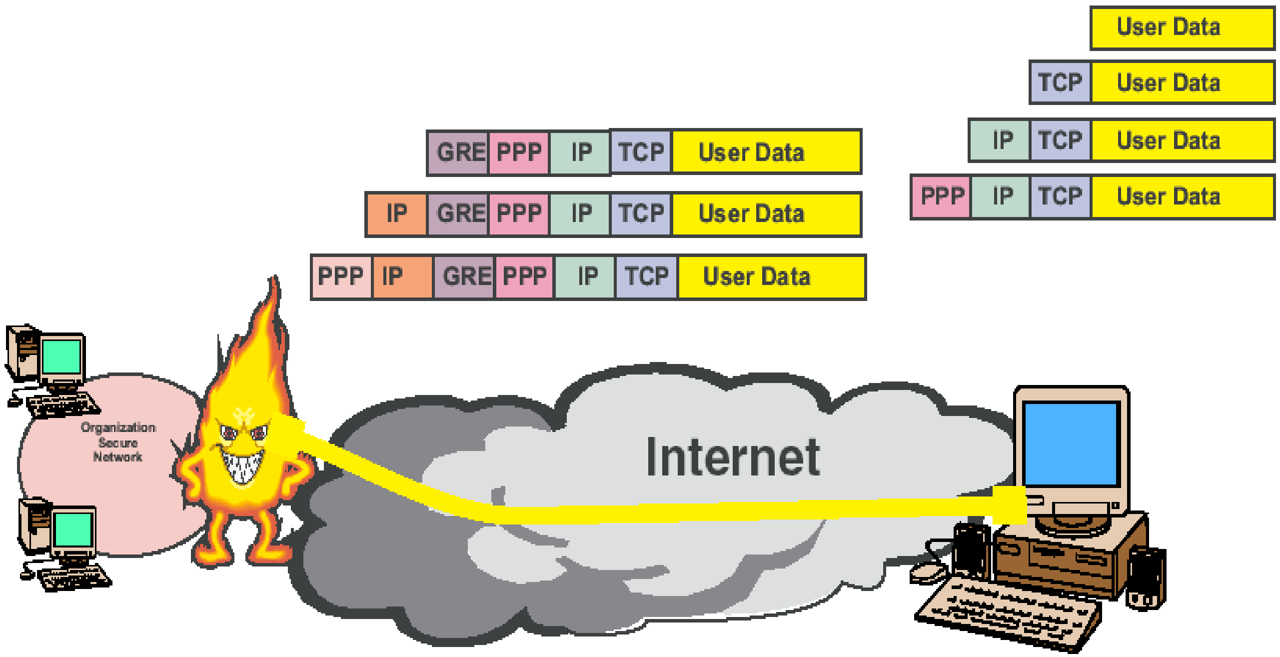
Ensure confidential communications in an unsecured network
Also known as the Key Management Nightmare !!!!!

Link Layer: L2TP for VPDN (Vir Pvt Dial Net)



IPSec IKE negotiation
Establish IPSec ESP for L2TP UDP port 1701
L2TP tunnel setup, management over IPSec
User authentication to domain

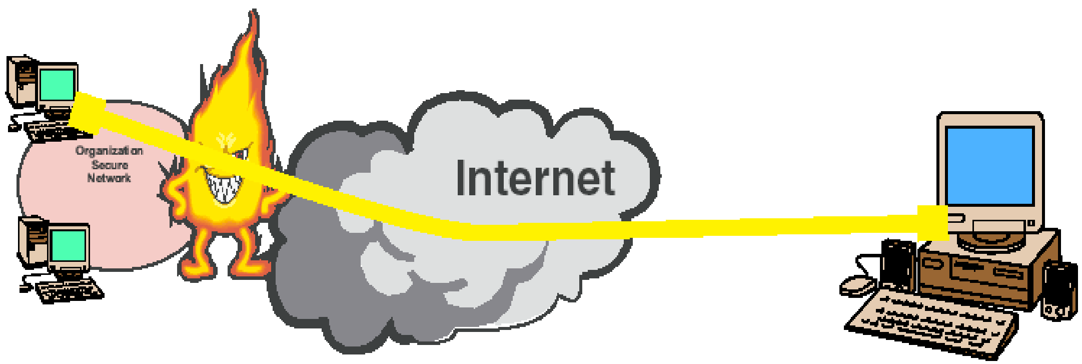
PPTP: Free from Microsoft



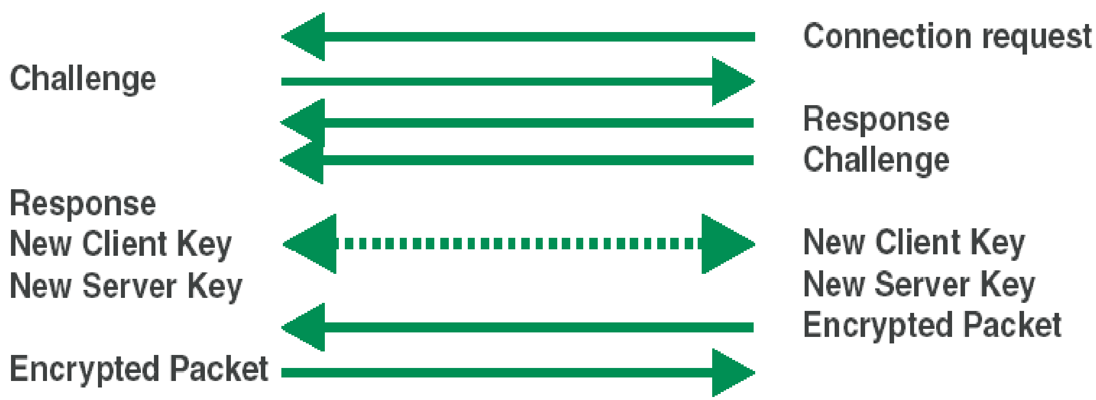
PPTP

- PPoE is Point-Point protocol over Ethernet
- Single tunnel between end-points : single device support (GRE = generic routing encapsulation)
- 6 bytes of overhead when compression used
- No tunnel authentication
- With RADIUS server supports authentication and accounting
- CHAP V2 fixes password, masquerading, and encryption weakness
- 40 or 128 bit RC4 packet encryption

PPTP: Security



CHAP V2 Authentication with 40 or 128 bit RC4 encryption

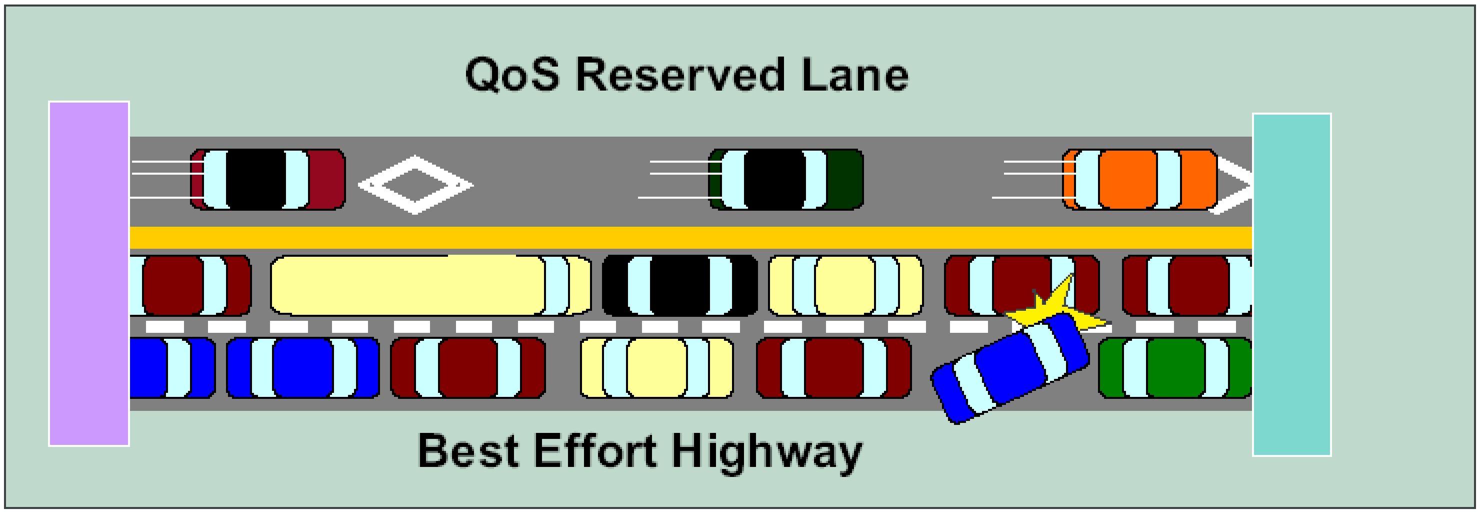


VPN Comparisons

	L2TP/IPSec	IPSec	PPTP	SSL
Mode	Client/server	Host-host	Client/server	Client/server
Layer	2	3	2	7
Protocols	Multiprotocol	IP	Multiprotocol	IP
Security				
User Authentication	PKI		PKI	Log-in
Machine Authentication		PKI		
Packet Authentication		X	X	
Packet Encryption	DES, 3DES, PGP	DES, 3DES	X	
Key Management	IKE	IKE	PKI	Private Key

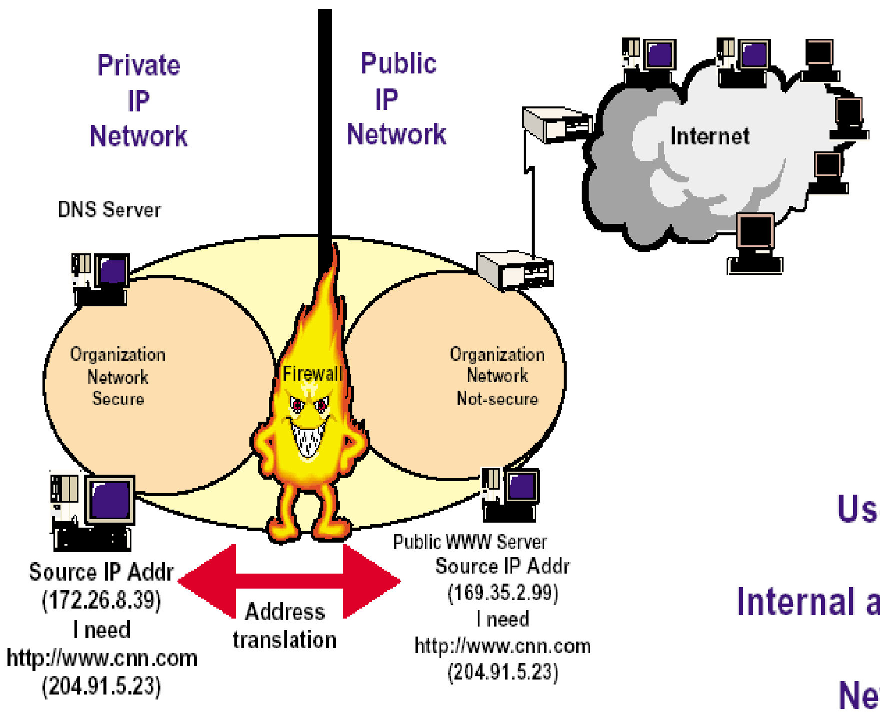
*Provided outside of specification

So why have a private network: QOS not fully cooked



- Very dependent on your ISP
- Real hard to do across ISPs
- So no guarantee of performance

Other Issues



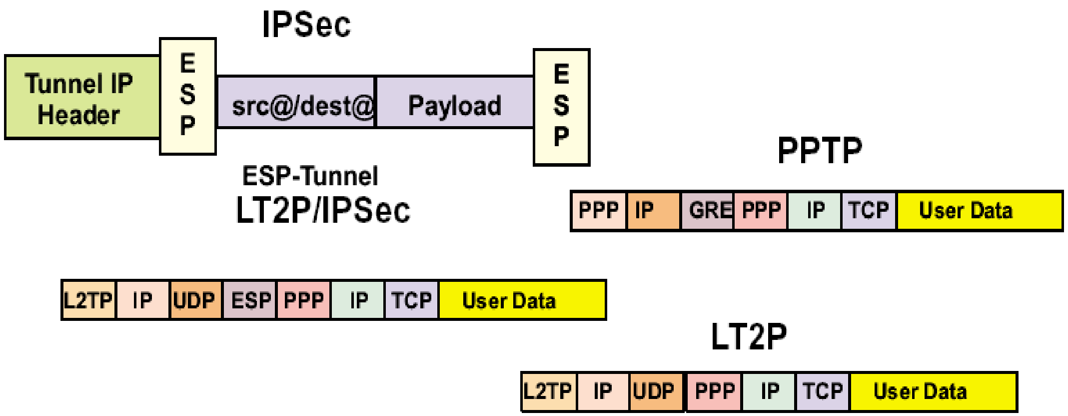
Use of NAT servers

Internal and external DNS

Newer applications

ISPs that change IP address in flight

Like Nat



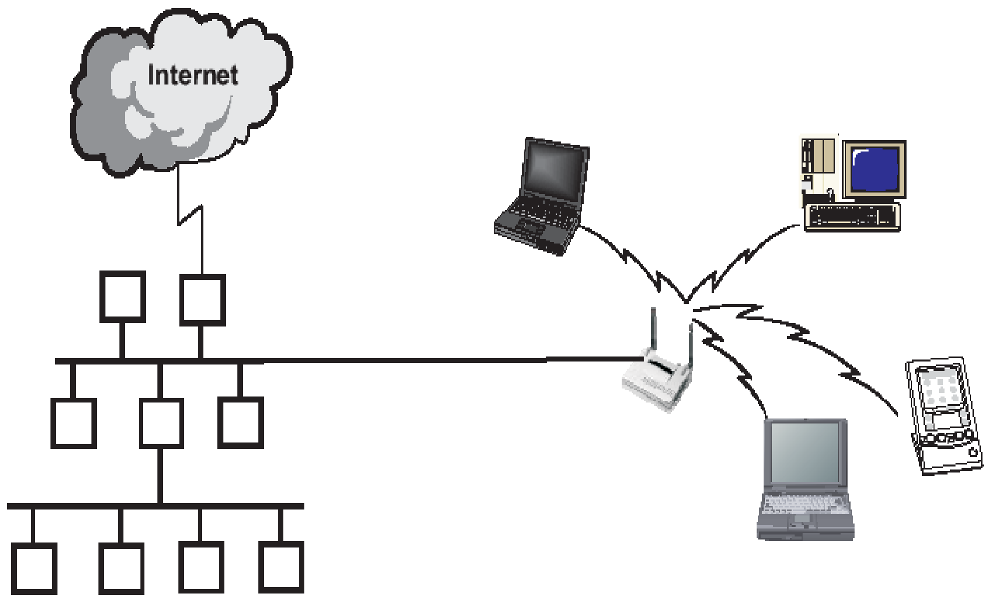
Can NAT work with all VPN protocols?
Need to access IP and TCP checksums, so these cannot be encrypted

You loose end-end traceability

VPNs make NAT very complex and therefore a vulnerable part of your network

New solutions coming out of IETF to solve several of these issues
Will your supplier support these........and how fast!

Wireless: a new big driver, WAS (Work At Starbucks)



An access point (AP) is a shared device
Remember the performance issues of shared hubs
Bridges and other devices allow for interconnection
Protocols and applications work seamlessly

Many security protocols, depends on deployer

SSID - Set Service ID

MAC ID - Media Access Control ID

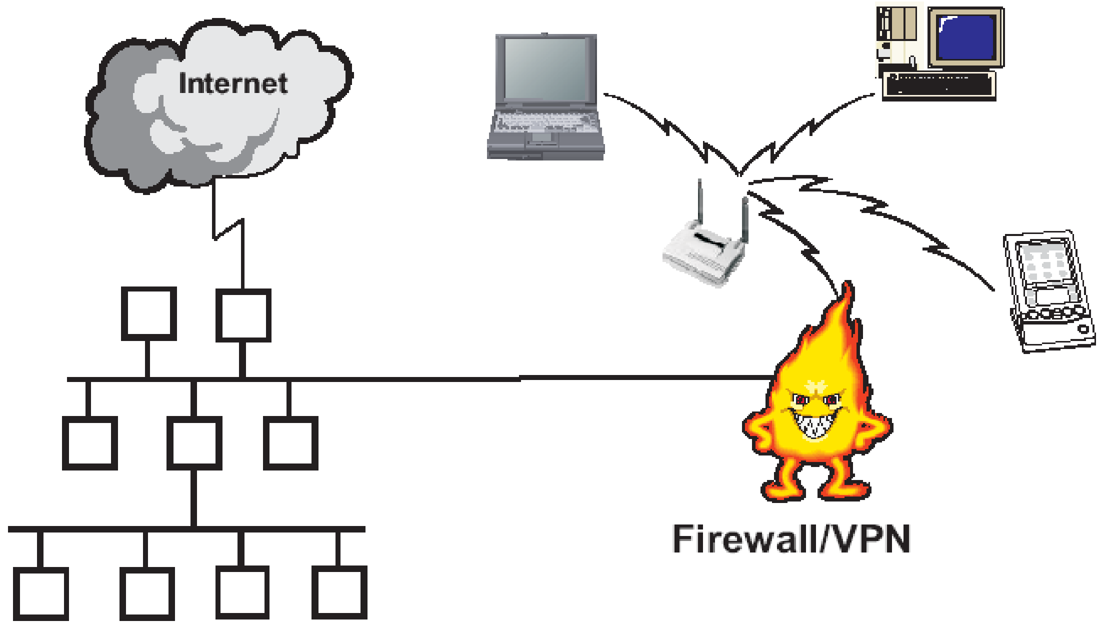
WEP - Wired Equivalent Privacy

802.1x - IEEE 802.1x standard

VPNs - Virtual Private Networks

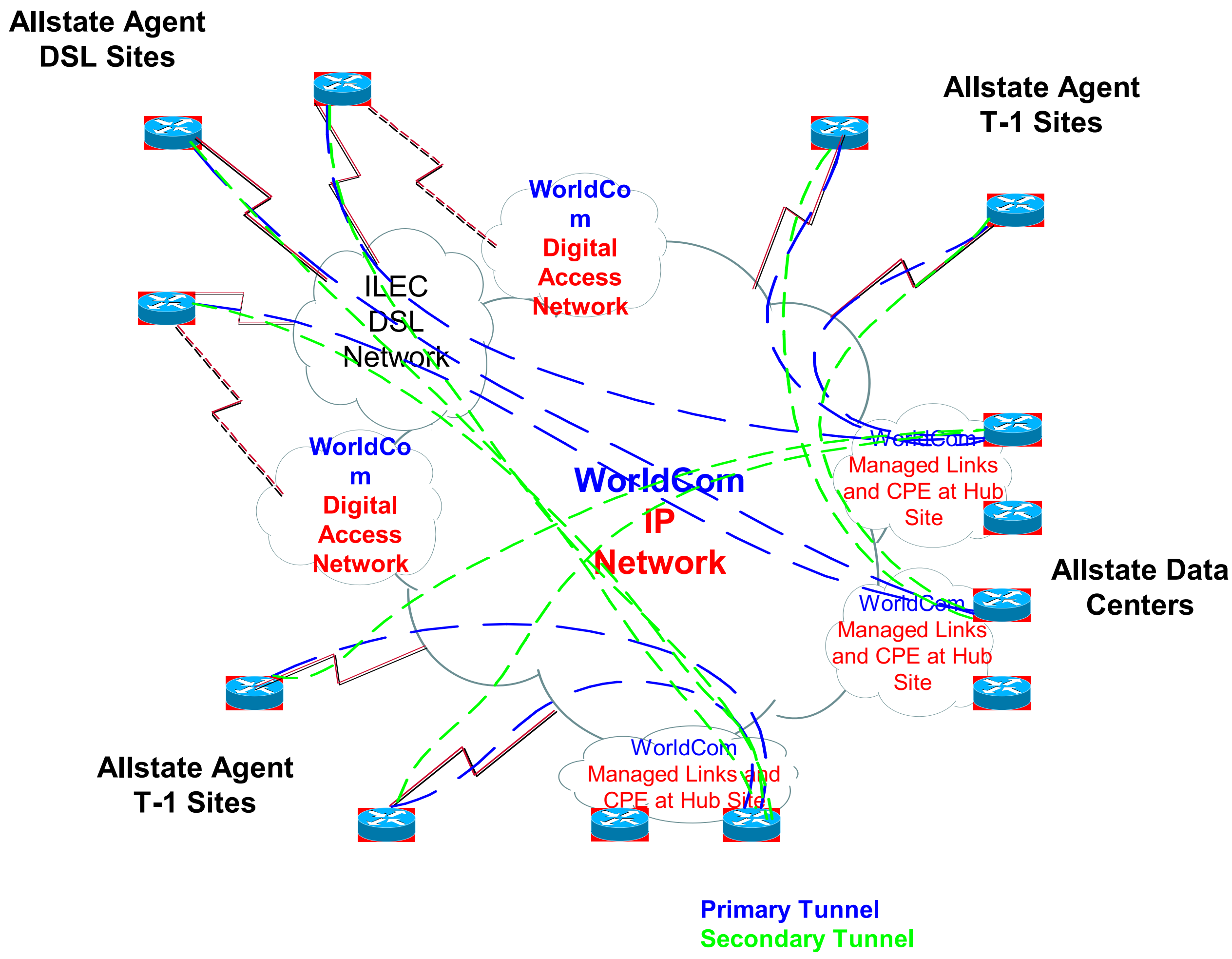
VLANs - Virtual Local Area Networks

VPN means I don't care how you connect



Scalable authentication and encryption solution
Requires end user configuration and VPN software
Requires end user knowledge of VPN technology
User re-authenticates if roaming

Example



Allstate Agent DSL Sites
Allstate Agent T-1 Sites
WorldCom Digital Access Network
ILEC DSL Network
WorldCom Digital Access Network
WorldCom IP Network
WorldCom Managed Links and CPE at Hub Site
WorldCom Managed Links and CPE at Hub Site
Allstate Data Centers
Allstate Agent T-1 Sites
WorldCom Managed Links and CPE at Hub Site
Primary Tunnel
Secondary Tunnel

So what could be wrong?

- VPN clients hit the network stack
- May not play well with personal firewalls
- Or other software
- May not need full access to the target network just encrypted access

One answer: clientless VPN

- Use SSL as the transport protocol to an appliance
- Can add NT authentication to the appliance
- Clientless mode: Use web enabled applications over the Internet, the appliance SSLifies web sites
- Java Applet: Use an downloadable applet to send traffic over SSL, get more support for applications.
- Can work well if you want to have encrypted web based apps without redoing the application
  - to use SSL you need certs and have to change EVERY link to HTTPs
  - Also big hit on the server cpu

Summary: VPNs

- Very big in the work access space
  - Exploit High speed
- Wireless
  - in the office
  - public ‘hot spots’ like Borders
- Replaces direct dial into the work network
- Replace dedicated Business partners
- May replace the corporate WAN