



Module 12: Understanding Virtual Private Networks www.acit.in

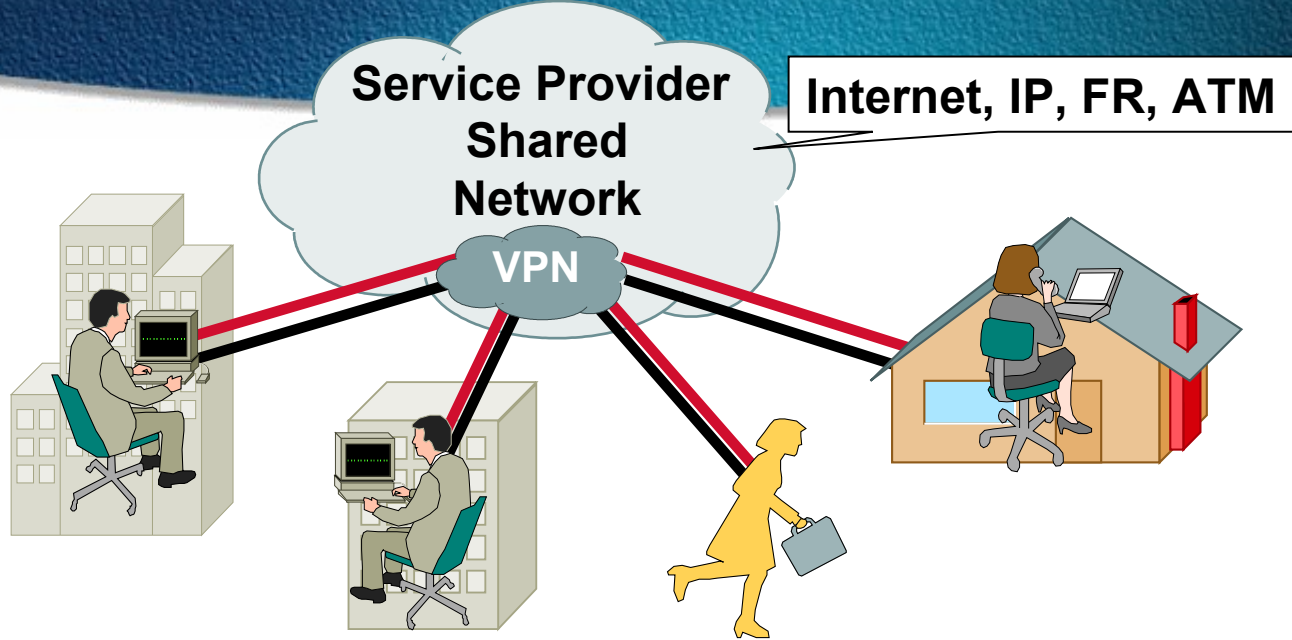


Agenda

- **What Are VPNs?**
- **VPN Technologies**
- **Access, Intranet, and Extranet VPNs**
- **VPN Examples**

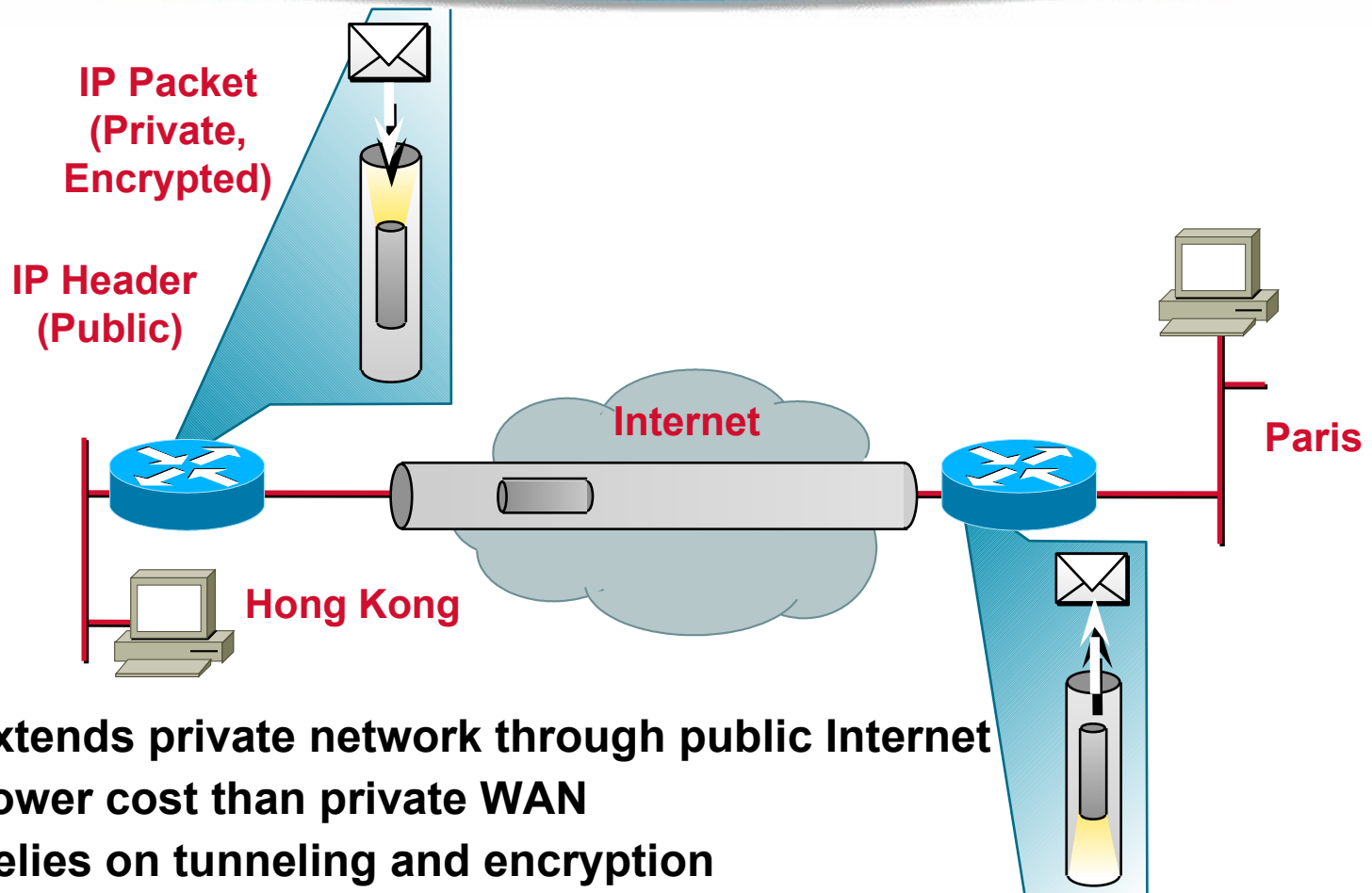


What Are VPNs?



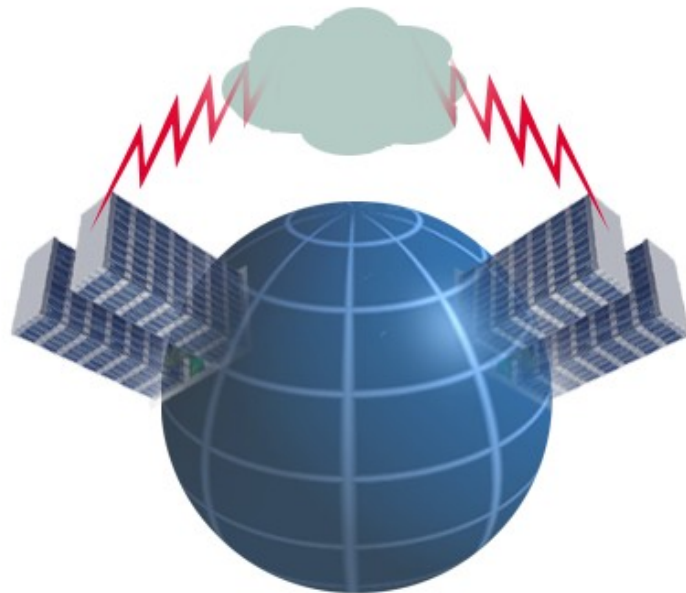
- **Virtual Private Networks (VPNs) extend the classic WAN**
- **VPNs leverage the classic WAN infrastructure, including Cisco's family of VPN-enabled routers and policy management tools**
- **VPNs provide connectivity on a shared infrastructure with the same policies and "performance" as a private network with lower total cost of ownership**

Virtual Private Networks



Why Build a VPN?

- **Company information secured**
- **Lower costs**
 - Connectivity costs
 - Capital costs
 - Management and support costs
- **Wider connectivity options**
- **Speed of deployment**



What's Driving VPN Offerings?

**Reduced
Networking
Costs**



**Mobile Users
Telecommuters**

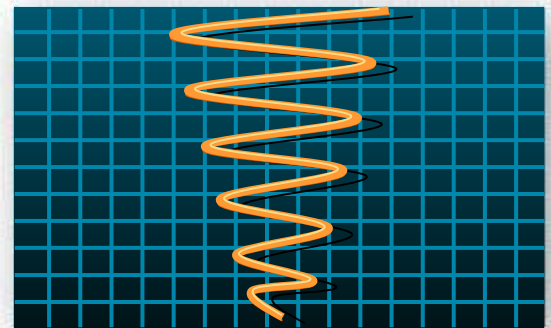
**Organizational
Changes**

**Mergers/
Acquisitions**

Extranets

Intranets

**Increased
Network
Flexibility**



Who Buys VPNs?

- **Organizations wishing to:**
 - Implement more cost-effective WAN solutions
 - Connect multiple remote sites
 - Deploy intranets
 - Connect to suppliers, business partners, and customers
 - Get back to their core business, and leave the WAN to the experts
 - Lower operational and capital equipment costs

Businesses with:

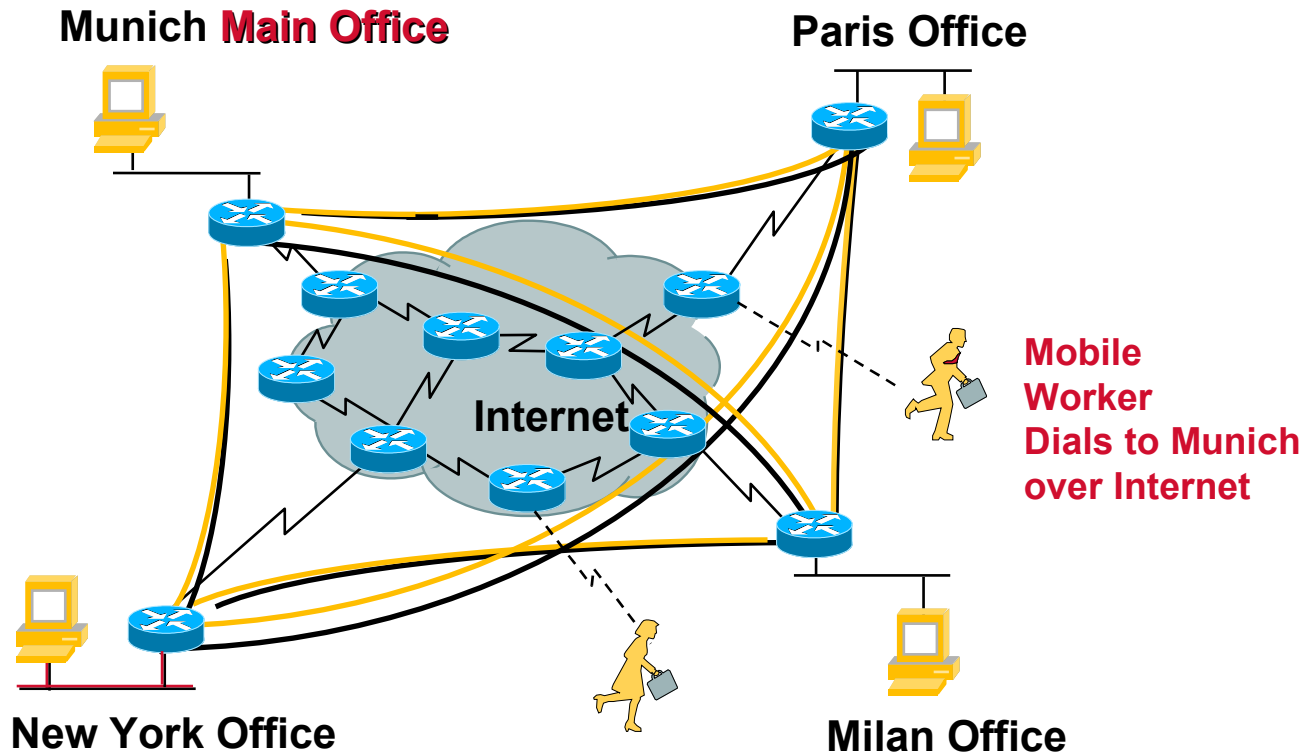
- Multiple branch office locations
- Telecommuters
- Remote workers
- Contractors and consultants

Networked Applications

- **Traditional applications**
 - E-mail
 - Database
 - File transfer
- **New applications**
 - Videoconferencing
 - Distance learning
 - Advanced publishing
 - Voice

Example of a VPN

- Private networking service over a public network infrastructure



A man in a white shirt and tie is climbing a large, curved, metallic structure, possibly a cable or pipe, against a blue background. The man is positioned in the upper right quadrant of the image, reaching up to grasp the structure. The structure is a thick, dark, curved line that arches across the top of the frame. The background is a textured, light blue surface with some darker, curved lines. The overall tone is blue and industrial.

VPN Technologies

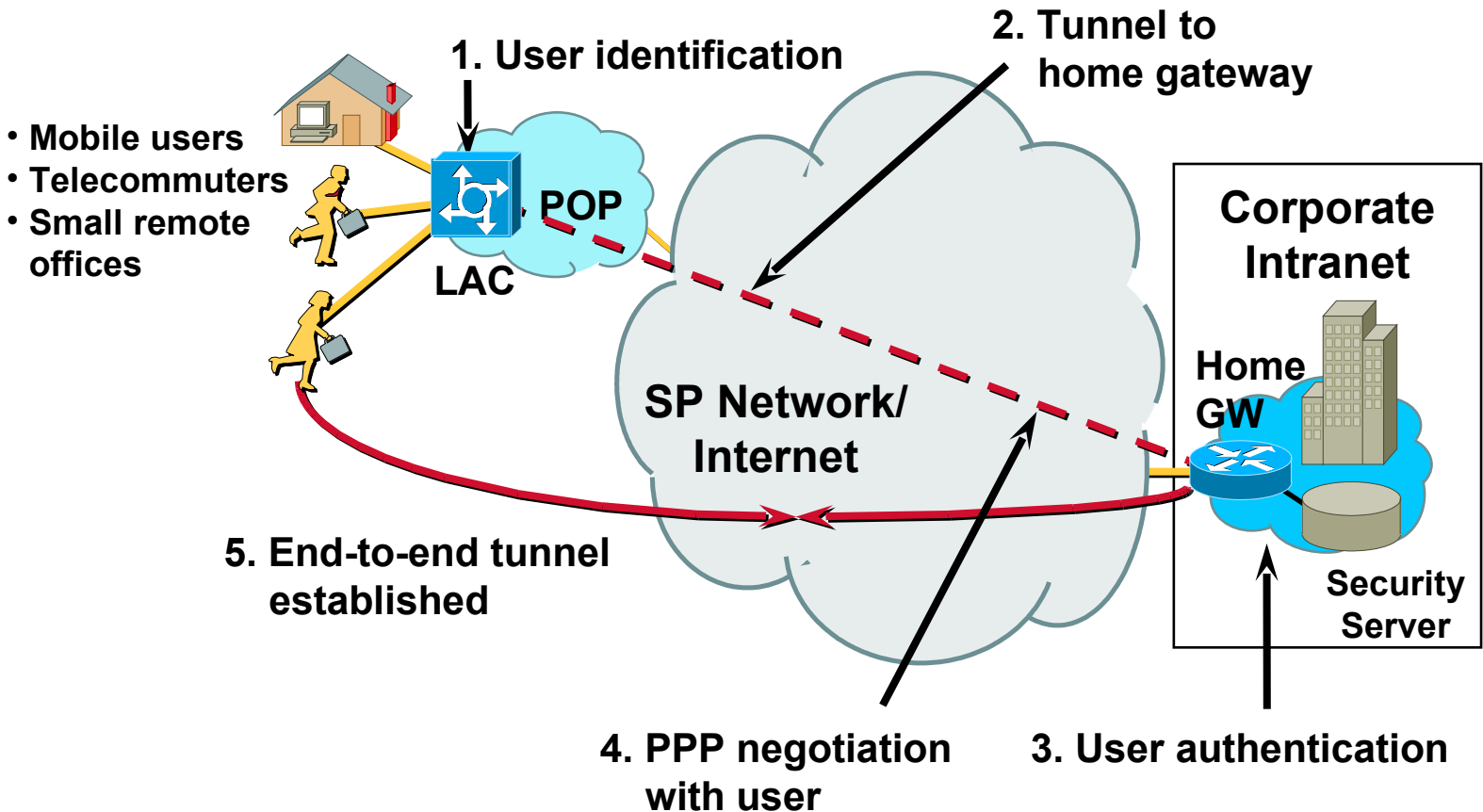
VPN Technology Building Blocks



Security

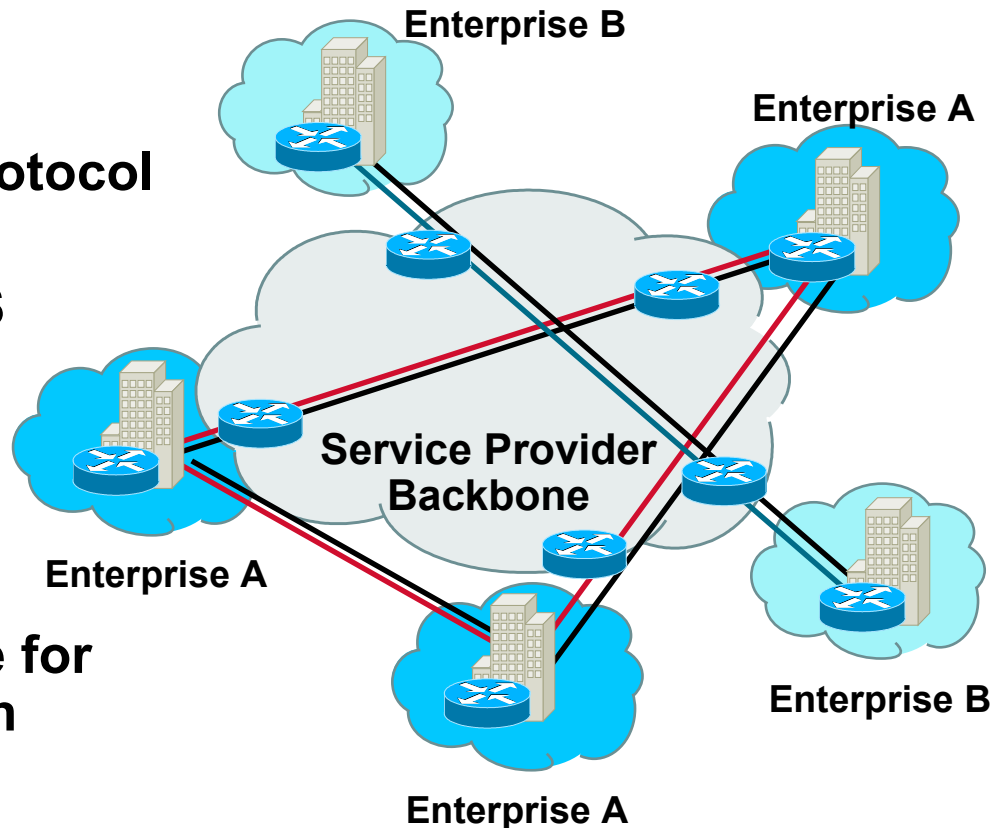
- **Tunnels and encryption**
- **Packet authentication**
- **Firewalls and intrusion detection**
- **User authentication**

Tunneling: L2F/L2TP



Tunneling: Generic Route Encapsulation (GRE)

- **Mesh of virtual point-to-point interfaces**
- **Encapsulates multiprotocol packets in IP tunnels**
- **Application-level QoS**
- **Value-added platform (new services)**
- **Encryption-optional tunneling**
- **Standard architecture for service providers with IP infrastructures**

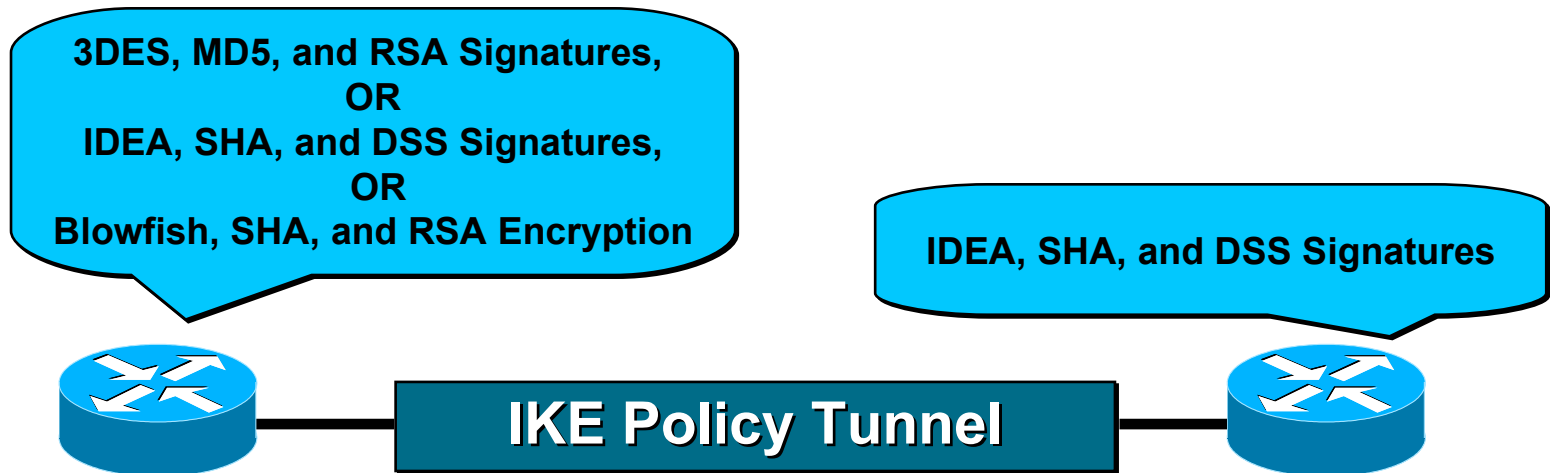


What Is IPSec?

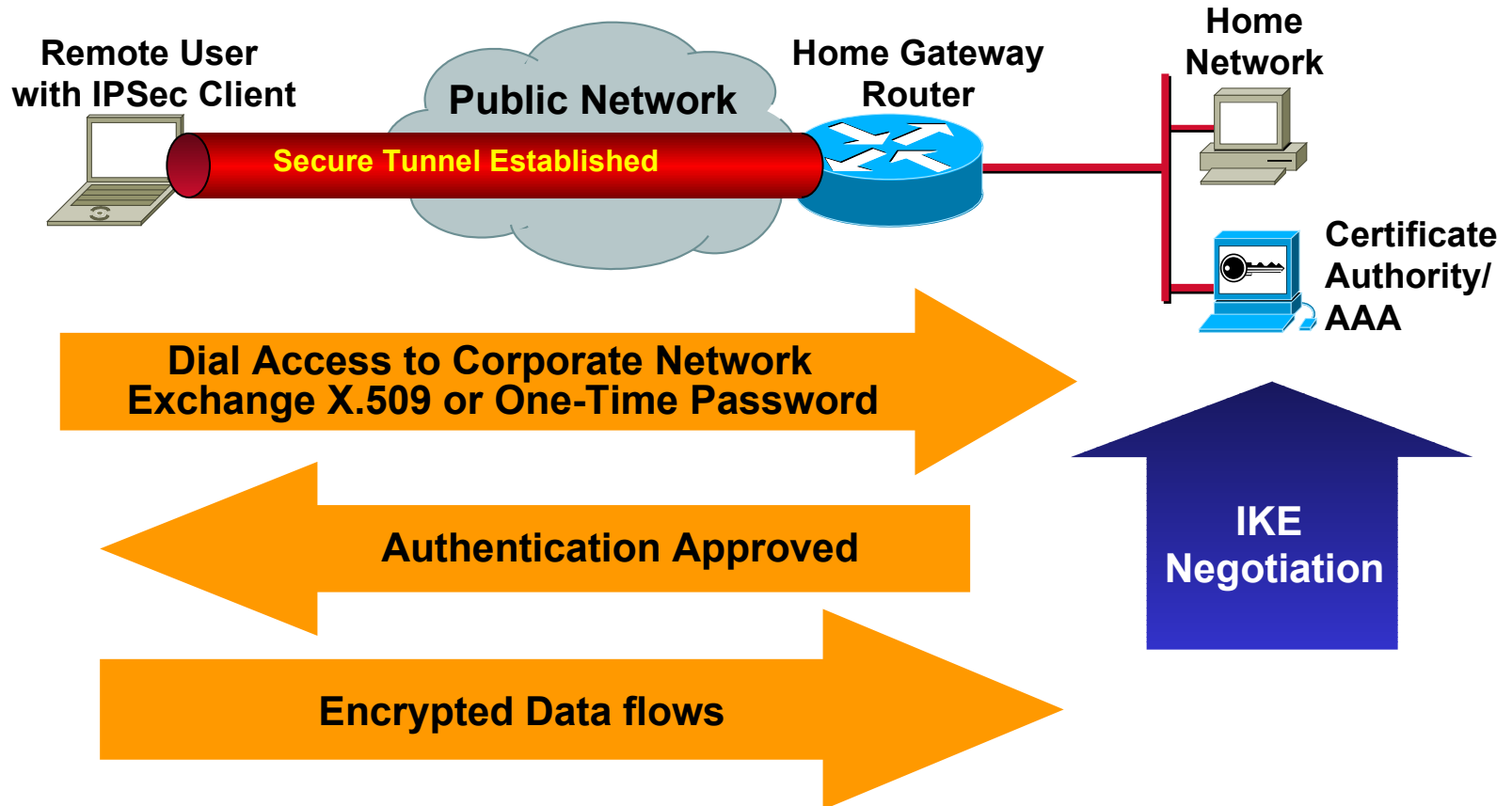
- **Network-layer encryption and authentication**
- **Open standards for ensuring secure private communications over any IP network, including the Internet**
- **Provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy**
- **Data protected with network encryption, digital certification, and device authentication**
- **Scales from small to very large networks**

What is Internet Key Exchange (IKE)?

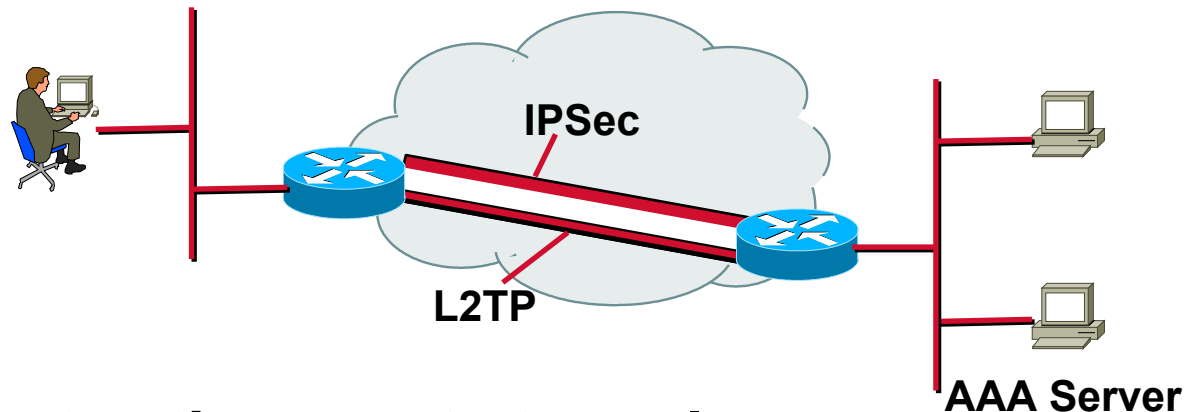
- Automatically negotiates policy to protect communication
- Authenticated Diffie-Hellman key exchange
- Negotiates (possibly multiple) security associations for IPSec



IPSec VPN Client Operation



L2TP and IPSec Are Complementary



- **IPSec creates the remote tunnel**
- **L2TP provides tunnel end-point authentication**
- **IPSec maintains encryption**
- **L2TP provides tunnels for non-IP traffic**
- **AAA services and dynamic address like DHCP**

Encryption: DES and 3DES

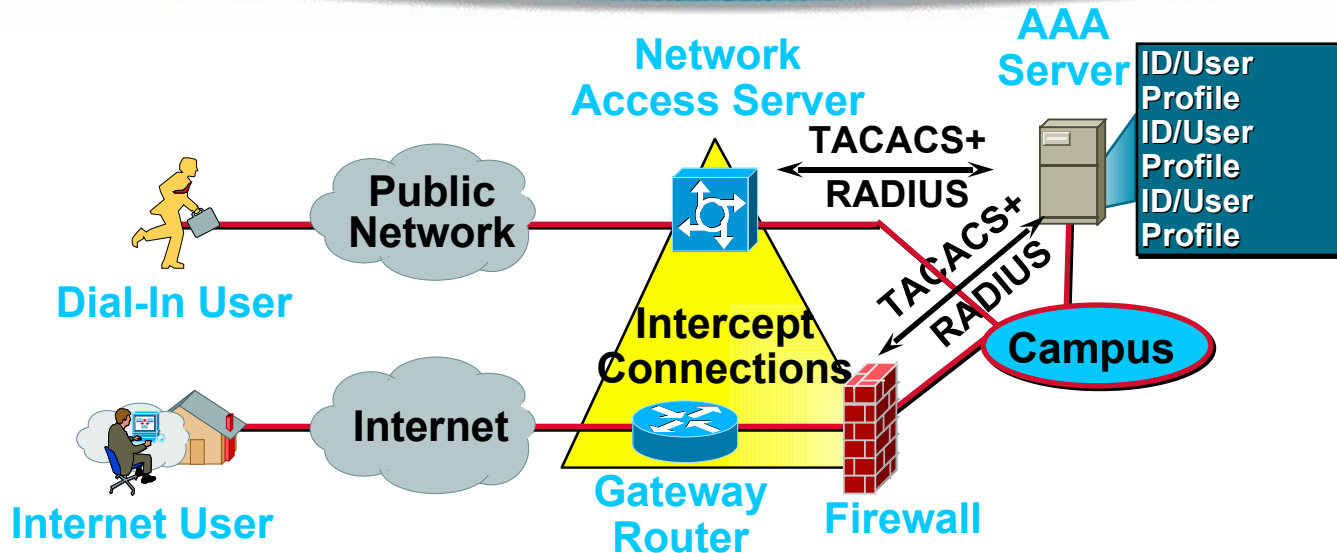
- Widely adopted standard
- Encrypts plain text, which becomes **cyphertext**
- DES performs 16 **rounds**
- Triple DES (3DES)
 - The 56-bit DES algorithm runs three times
 - 112-bit triple DES includes two keys
 - 168-bit triple DES includes three keys
- Accomplished on a VPN client, server, router, or firewall

Firewalls



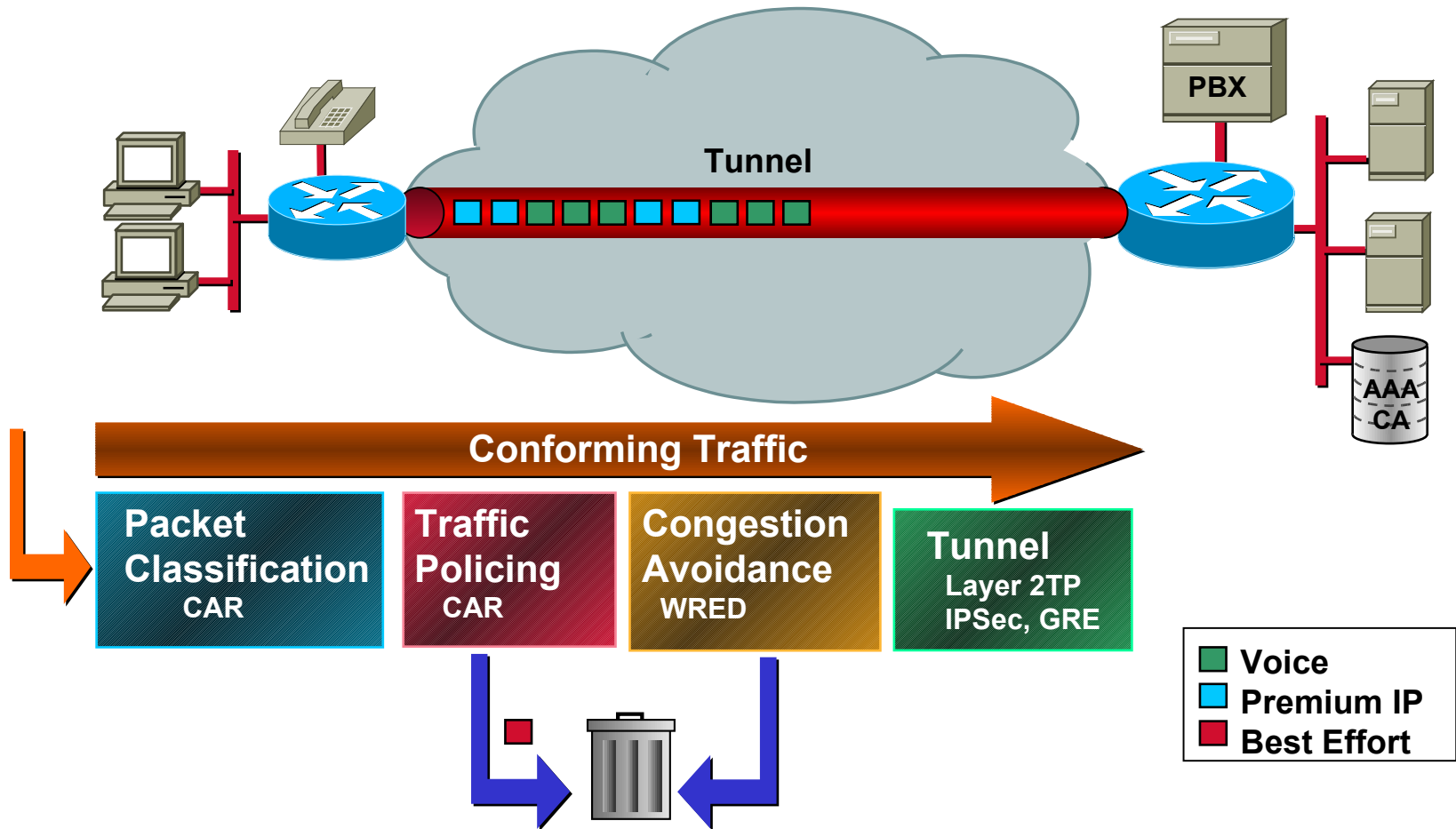
- **All** traffic from inside to outside and vice versa must pass through the firewall
- Only **authorized** traffic, as defined by the local security policy, is allowed in or out
- The firewall itself is immune to penetration

User Authentication



- Centralized security database (AAA services)
- High availability
- Same policy across many access points
- Per-user access control
- Single network login
- Support for: TACACS+, RADIUS (IETF), Kerberos, one-time password


VPNs and Quality of Service



A man in a white shirt and tie is climbing a large, curved, metallic structure, possibly a cable or pipe, against a blue background. The man is positioned near the top of the curve, reaching up with his arms. The structure is dark and metallic, with a bright light source creating a strong lens flare effect on the left side of the image. The background is a textured blue surface.

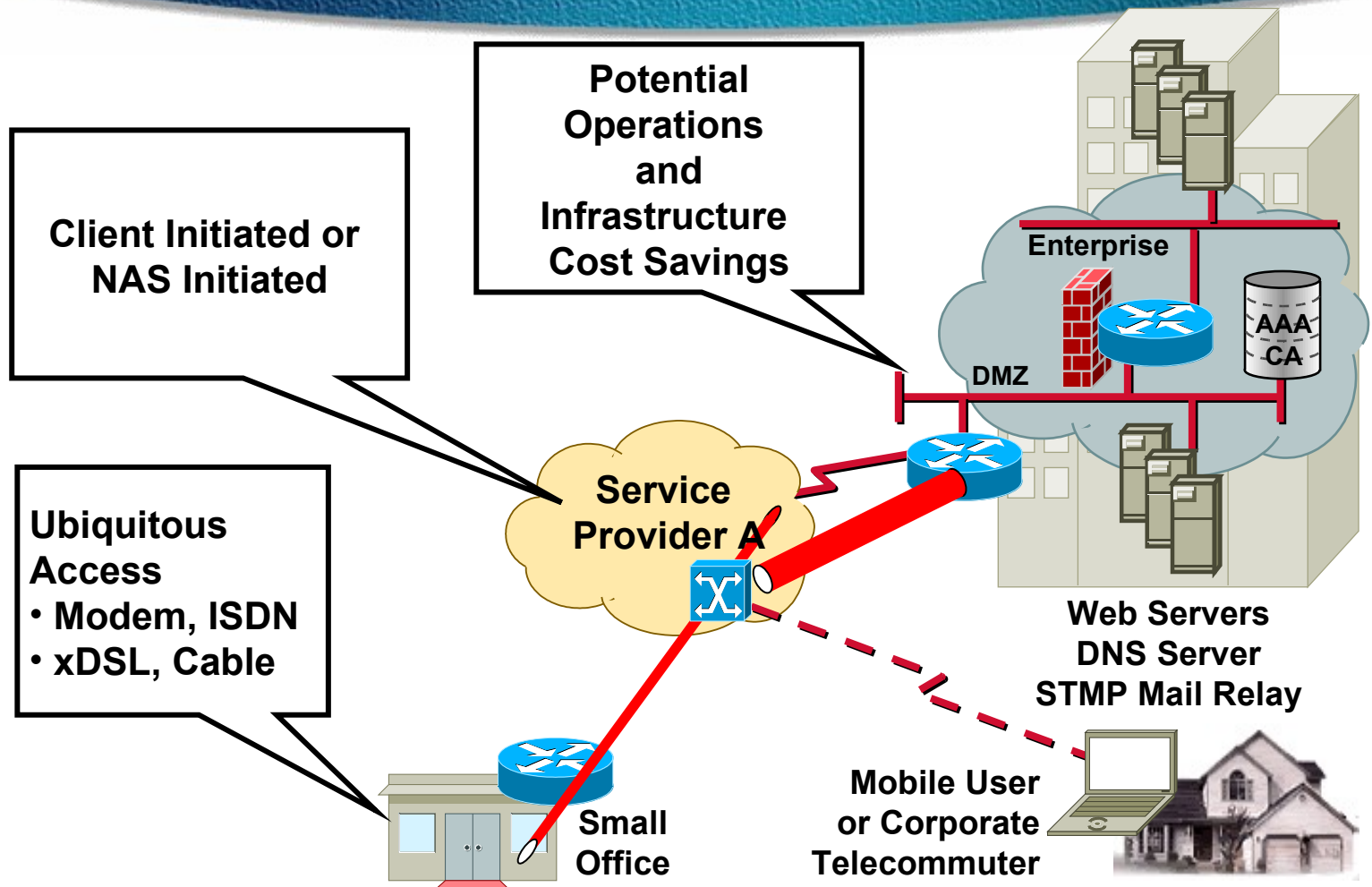
Access, Intranet, and Extranet VPNs

Three Types of VPNs

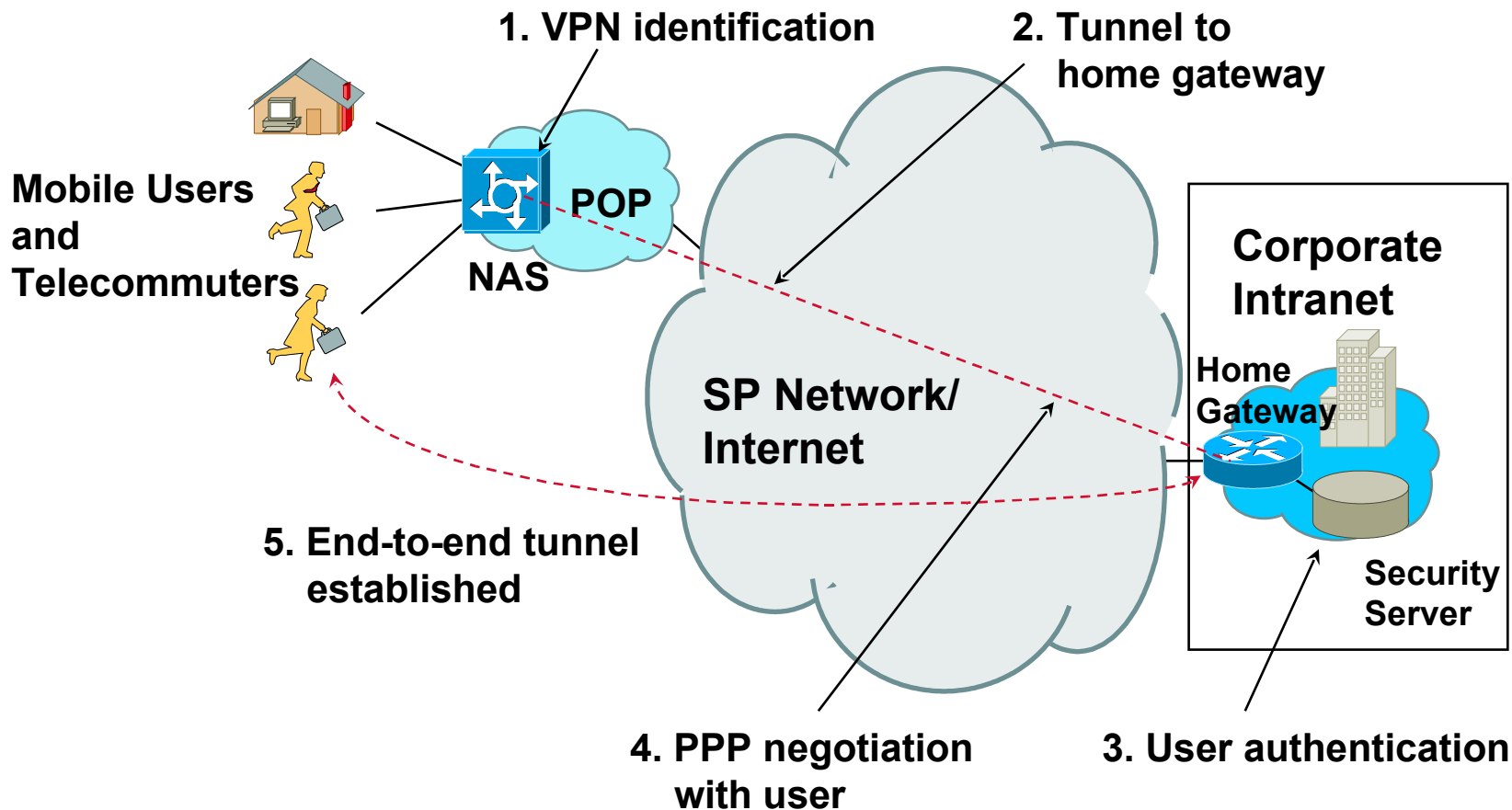


Time	Type	Application	Alternative To	Benefits
	Remote access VPN	Mobile users Remote connectivity	Dedicated dial ISDN	Ubiquitous access, lower cost
	Intranet VPN	Site-to-site Internal connectivity	Leased line	Extend connectivity, lower cost
	Extranet VPN	Business-to-business External connectivity	Fax Mail EDI	Facilitates e-commerce

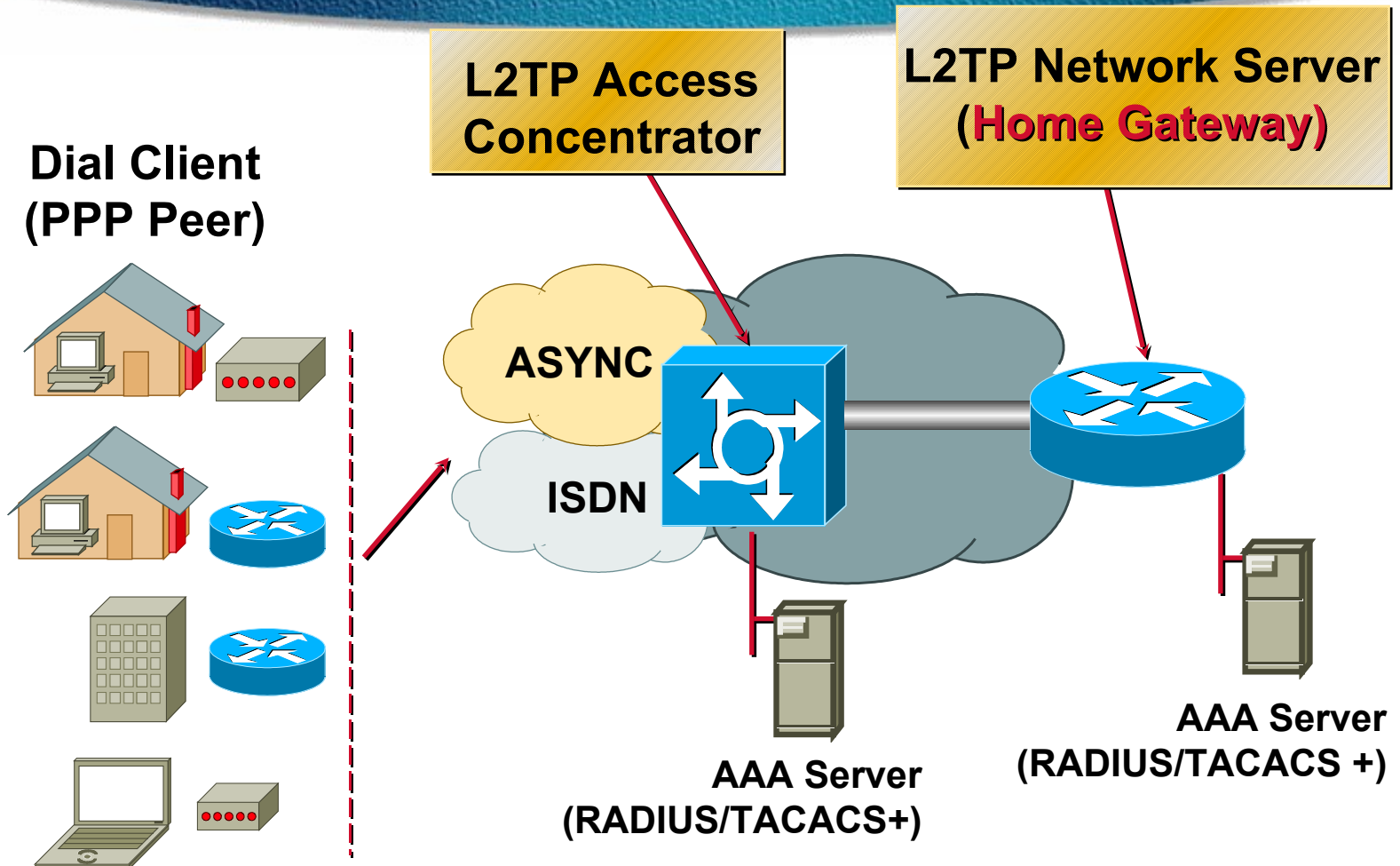
Access VPNs



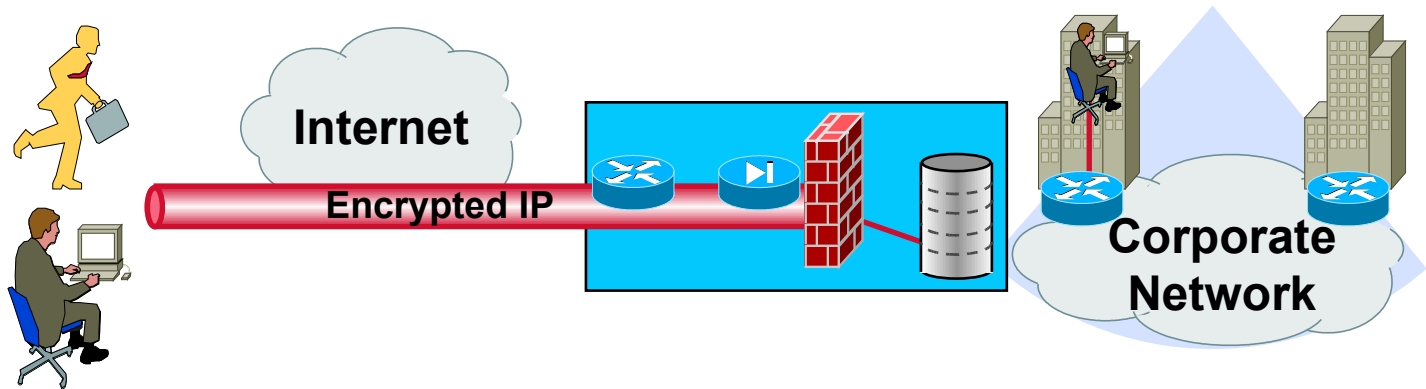
Access VPN Operation Overview



Access VPN Basic Components



Client-Initiated Access VPN

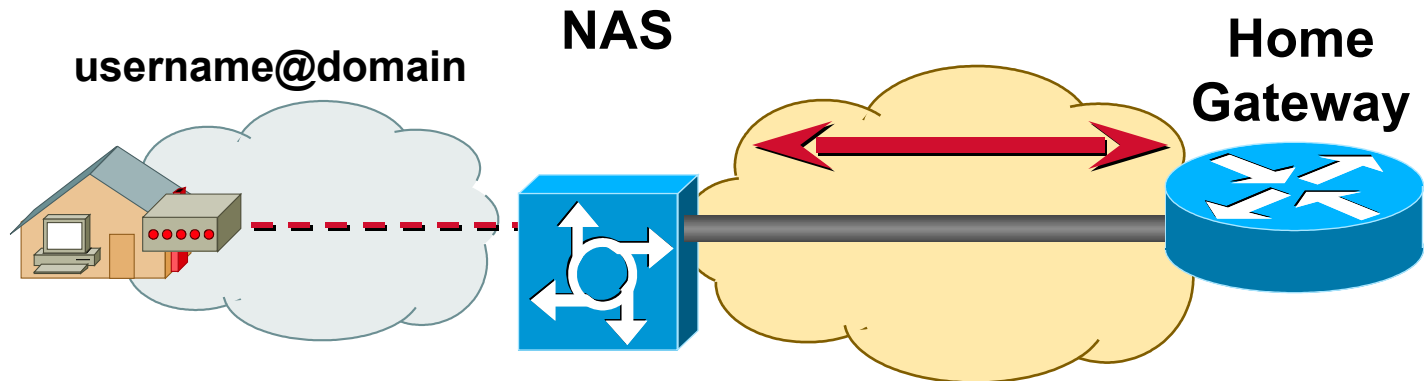


- **Encrypted tunnel from the remote client to the corporate network**
- **Independent of access technology**
- **Standards compliant**
 - IPsec encapsulated tunnel
 - IKE key management

Client-Initiated VPNs

- **Pros:**
 - Use same hardware for dedicated access
 - Dedicated encryption hardware in firewall for performance
- **Cons:**
 - Management of IPSec PC client
 - Security must be initiated by user

NAS-Initiated Access VPN



NAS-Initiated VPNs

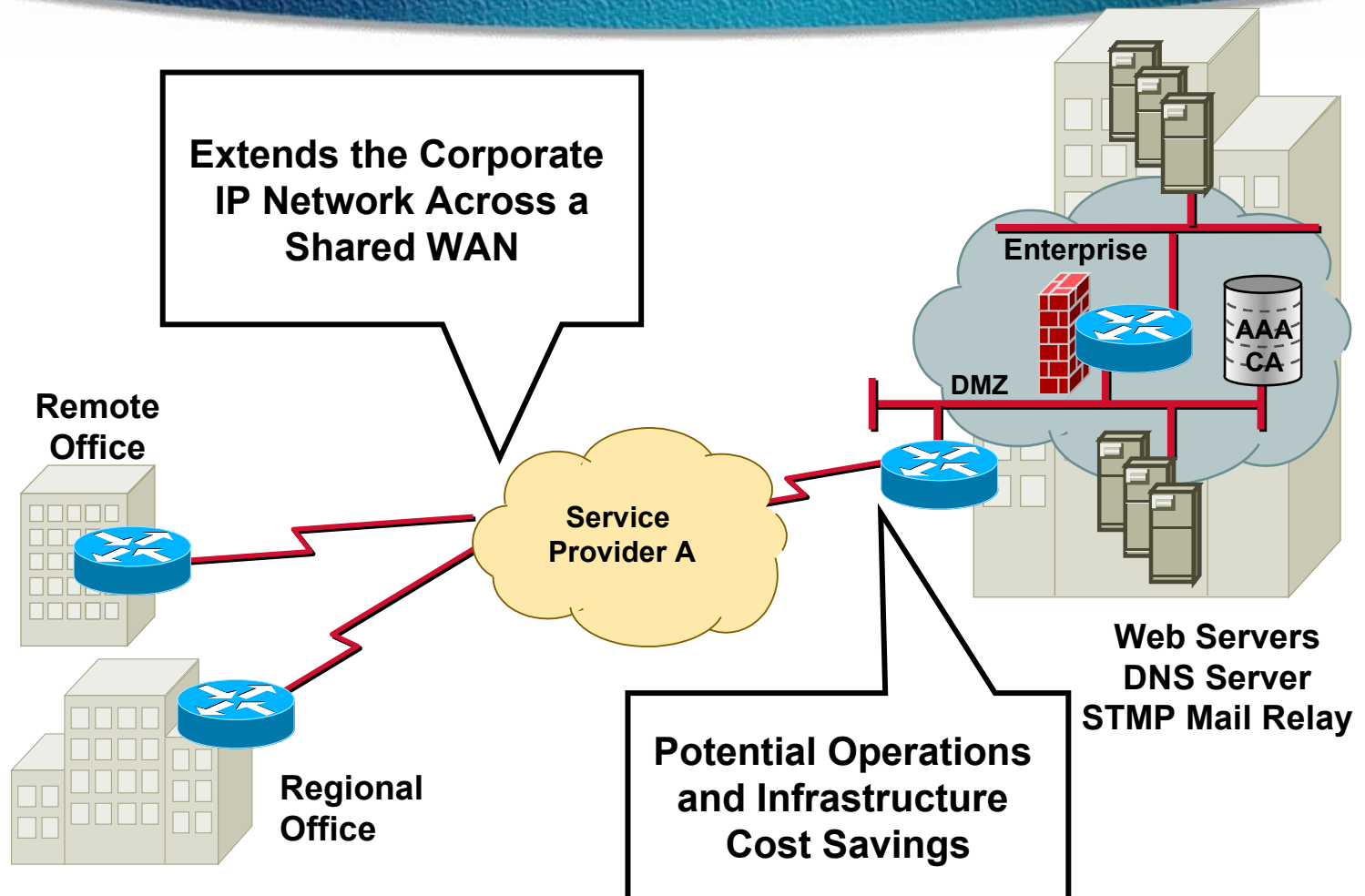
- **Pros:**

- No PC client software to manage
- Premium services
- VPN and Internet access at the NAS
- More scalable and manageable

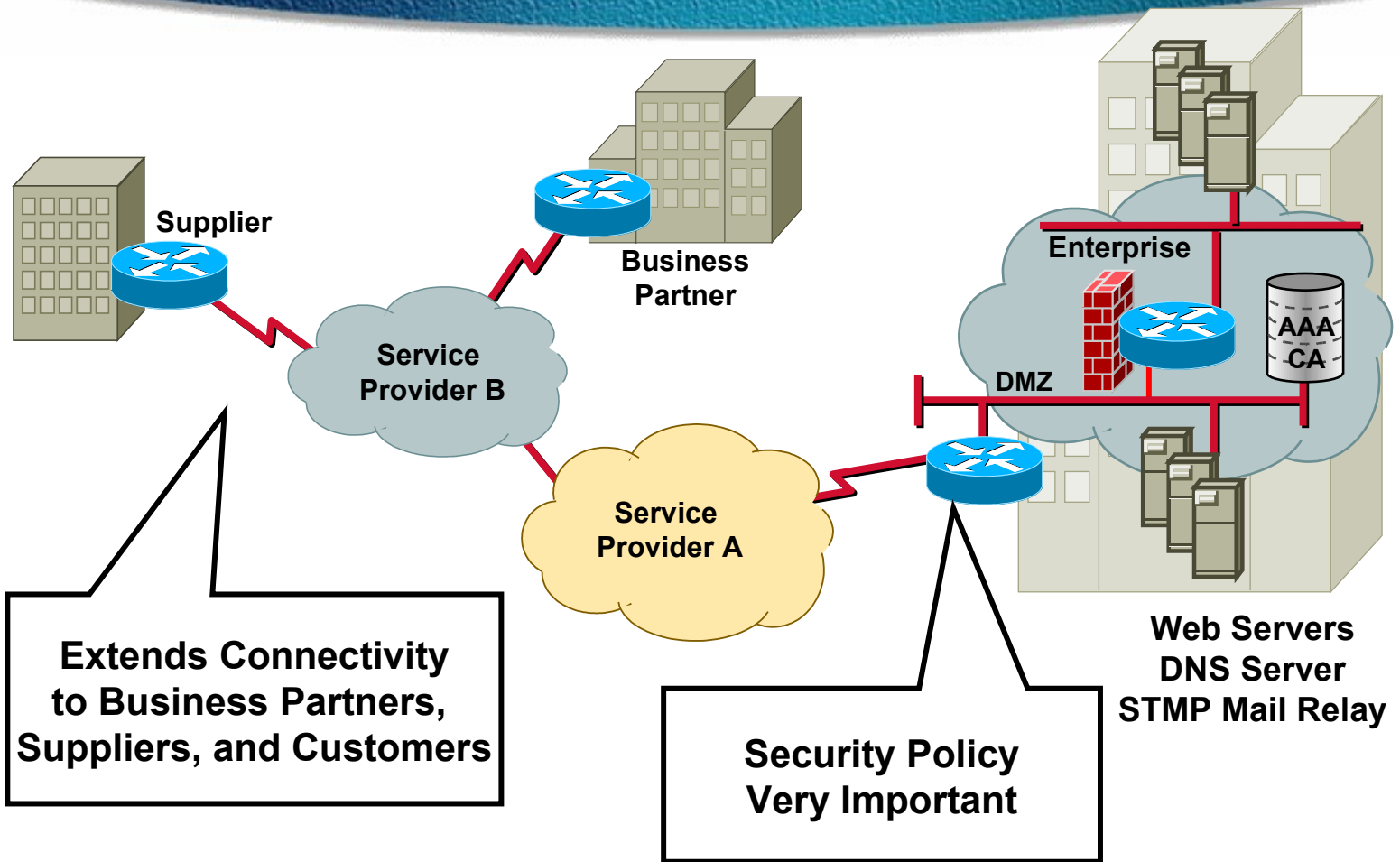
- **Cons:**

- Users can connect only to certain POPs

The Intranet VPN



The Extranet VPN



Intranet and Extranet VPNs

- **Multiple users, multiple sites, and potentially multiple companies or multiple communities of interest**
- **Dedicated connections**
- **Flexible architecture options**
 - **IP tunnels with IPSec or GRE**
 - **Managed router service with Frame Relay or ATM virtual circuits**
 - **Tag Switching/MPLS**

Comparing the Types

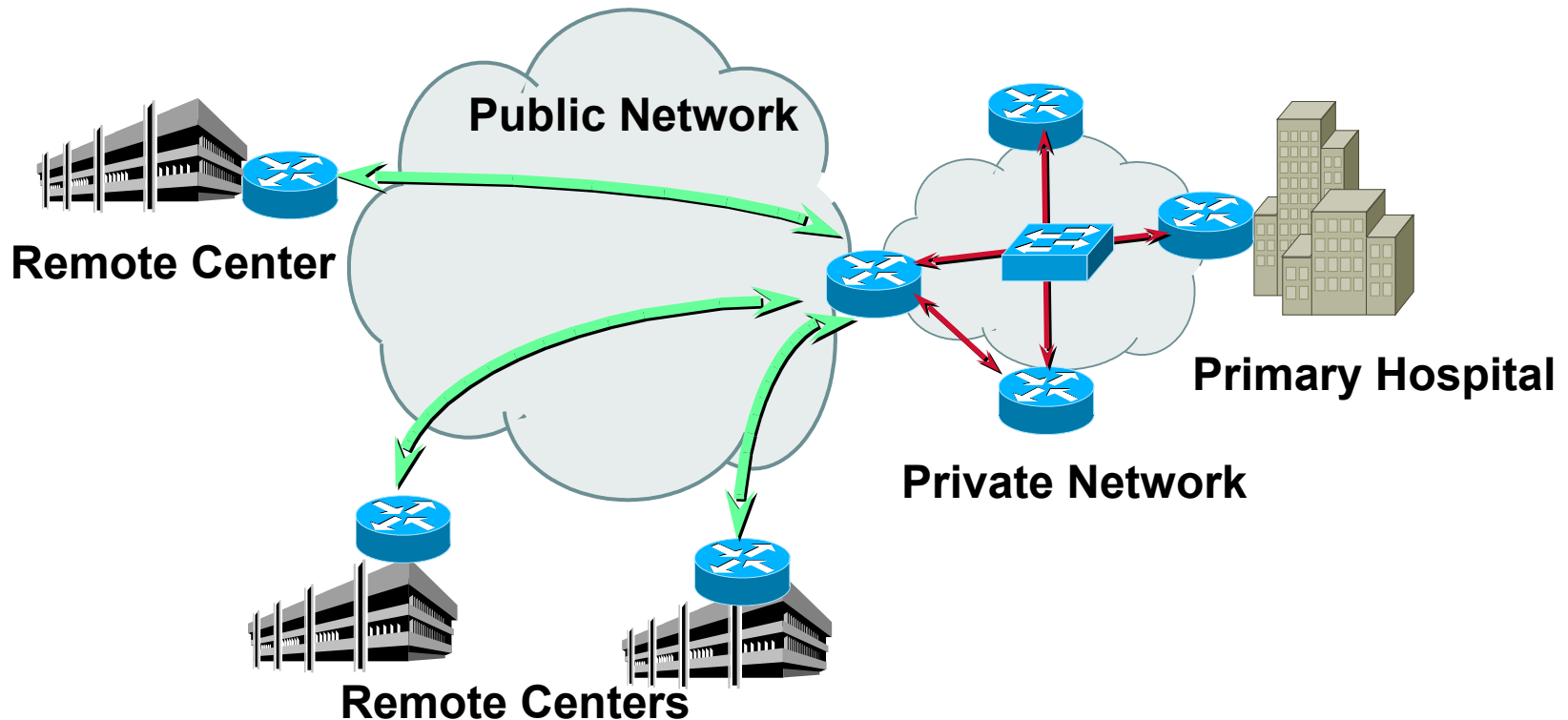
Type	Access VPN	Intranet	Extranet
NAS-Initiated	X	X	X
Client-Initiated	X	X	X
Router-Initiated		X	X

A man in a white shirt and tie is climbing a large, curved, metallic structure, possibly a cable or pipe, against a blue background. The man is positioned in the upper right quadrant of the image, reaching up to grasp the structure. The structure is a thick, curved cable or pipe that arches across the frame. The background is a textured, blue surface with some vertical lines on the left side.

VPN Examples

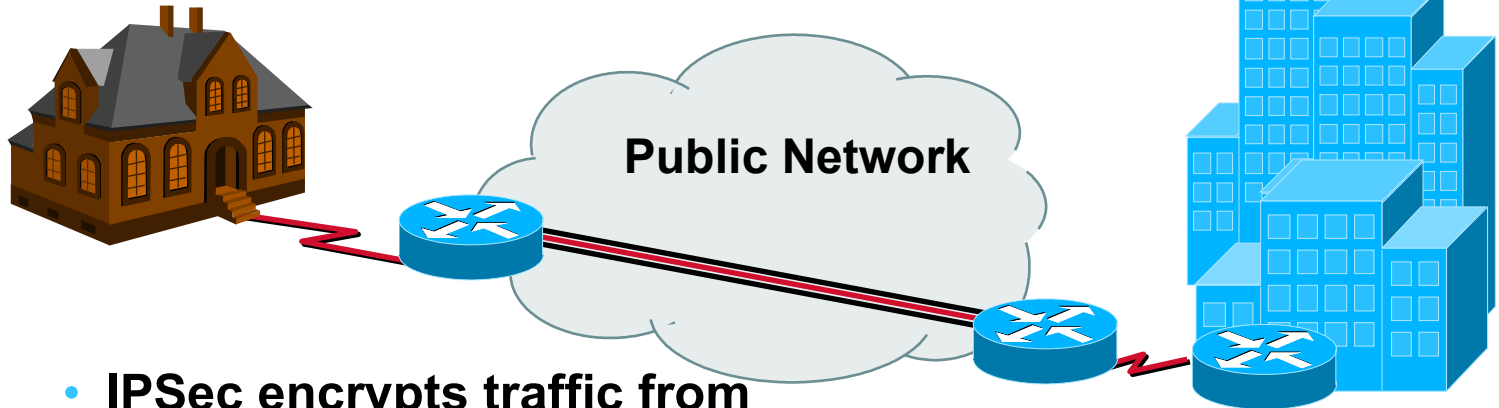
Health Care Company Intranet Deployment

**Challenge—Low-cost means for connecting
remote sites with primary hospital**



Branch Office or Telecommuters

Challenge—Cost-effective means for connecting branch offices and telecommuters to the corporate network



- **IPSec encrypts traffic from remote sites to the enterprise using *any* application**
- **IPSec may be combined with other tunnel protocols, e.g., GRE**
- **Telecommuters can gain secure, transparent access to the corporate network**

Traditional Dialup Versus Access VPN

Traditional Dialup		Access VPN	
Number of users	20	Number of users	20
Remote access server	\$3,000	Access router, T1/E1, DSU/CSU, firewall	\$4,600
One-time installation fee: 10 phone lines	\$1,000	VPN client software (\$50/user)	\$1,000
		T1/E1 installation	\$5,000
Monthly long-distance charges per minute	\$0.10	Central site T1/E1 Intranet access	\$2,500
Avg. use per day, per user (min)	90	Monthly ISP access (\$20/user)	\$400

Traditional Dialup Versus Access VPN

Traditional Dial-Up		Access VPN	
Number of users	20	Number of users	20
Remote access server	\$3,000	Access router, T1/E1, DSU/CSU, firewall	\$4,600
One-time installation fee-10 phone lines	\$1,000	VPN client software (\$50/user)	\$1,000
		T1/E1 installation	\$5,000
One-time capital cost	\$4,000	One-time capital cost	\$10,600
Monthly long distance charges per minute	\$0.10	Central site T1/E1 Intranet access	\$2,500
Avg. use per day per user (min)	90	Monthly ISP access (\$20/user)	\$400
Recurring cost	\$5,400	Recurring cost	\$2,900

VPN Payback

Total Cost

\$80,000

\$60,000

\$40,000

\$20,000

0

1

2

3

4

5

6

7

8

9

10

11

12

Month

Traditional

VPN

Payback in 3 months!!

Summary

- **VPNs reduce costs**
- **VPNs improve connectivity**
- **VPNs maintain security**
- **VPNs offer flexibility**
- **VPNs are reliable**

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATIONSM