2400
1190_05_2000_c2   © 2000, Cisco Systems, Inc.   1

Introduction to VPNs

Extending the Classic WAN

Session 2400

2400
1190_05_2000_c2   © 2000, Cisco Systems, Inc.   2

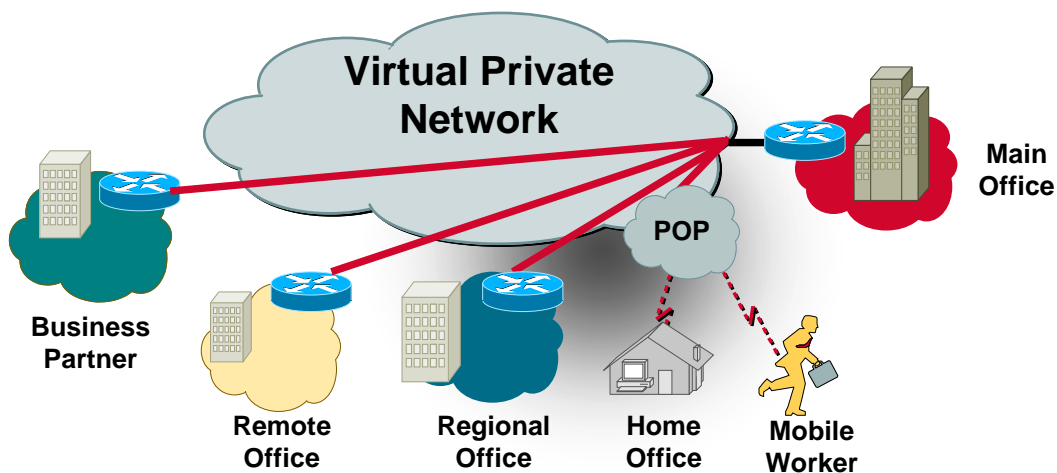# Agenda

- **VPN Choices—Choosing What's Right For You**

- **Understanding the Building Blocks of a VPN**

  Security

  Platforms

  Quality of Service

  Network and Service Monitoring

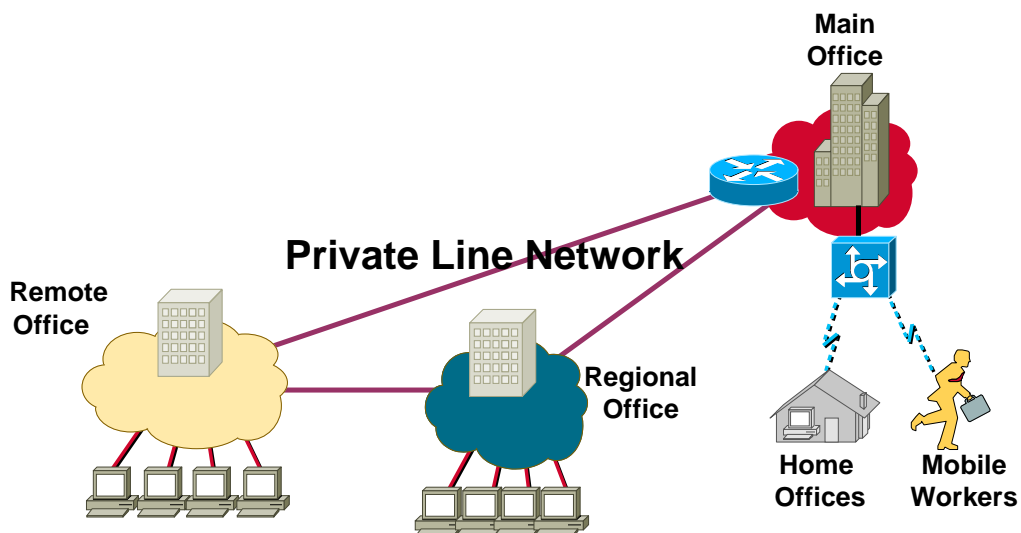- **Next Steps and Real World Deployments**

- **Q&A**

What Is a VPN?

Connectivity Deployed on a Shared Infrastructure with the Same Policies and 'Performance' as a Private Network
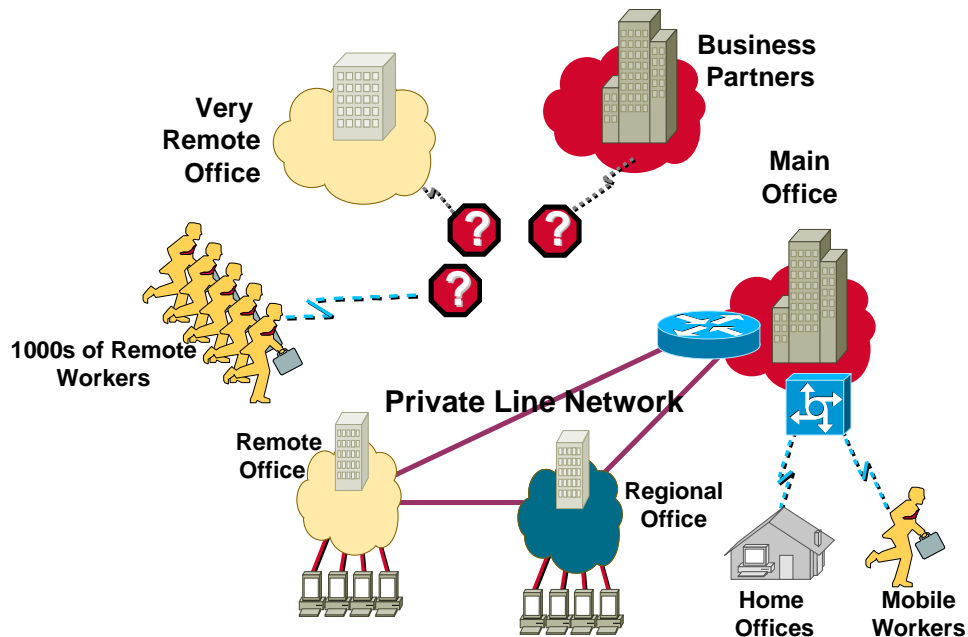
Virtual Private Network

POP

Main Office

Business Partner

Remote Office

Regional Office

Home Office

Mobile Worker

The VPN Timeline

1996	IETF IPSec Draft Standard
1997	IKE Reference Code
	Diffie/Hellman Patent Buyout
1998	Simple Certificate Enrollment Protocol (SCEP)
	Campus VPN
1999	Remote Access VPN
2000	IETF PKIX CMC
	Accelerated VPN Services
2001	Secure Streaming Services
	Audio/Video/Voice

Classic WAN

Main Office

Private Line Network

Remote Office

Regional Office

Home Offices

Mobile Workers

Classic WAN
Today's New Challenges

Very Remote Office

Business Partners

Main Office

1000s of Remote Workers

Private Line Network

Remote Office

Regional Office

Home Offices

Mobile Workers

VPNs Extend the Classic WAN

Very Remote Office

Business Partners

Main Office

1000s of Remote Workers

Private Line Network

Remote Office

Regional Office

Home Offices

Mobile Workers
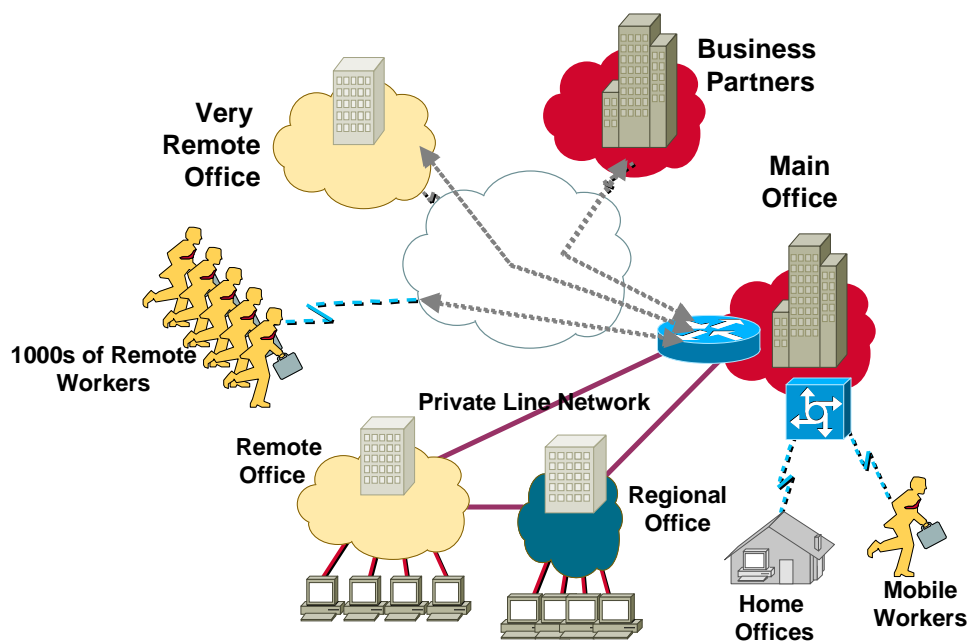
Enabling the Internet Economy

Customers

Very Remote Sites

Partners

Telecommuters

Enterprise WAN Connectivity

SAP

BaaN

PEOPLE Soft

ORACLE

Multiservice/Voice
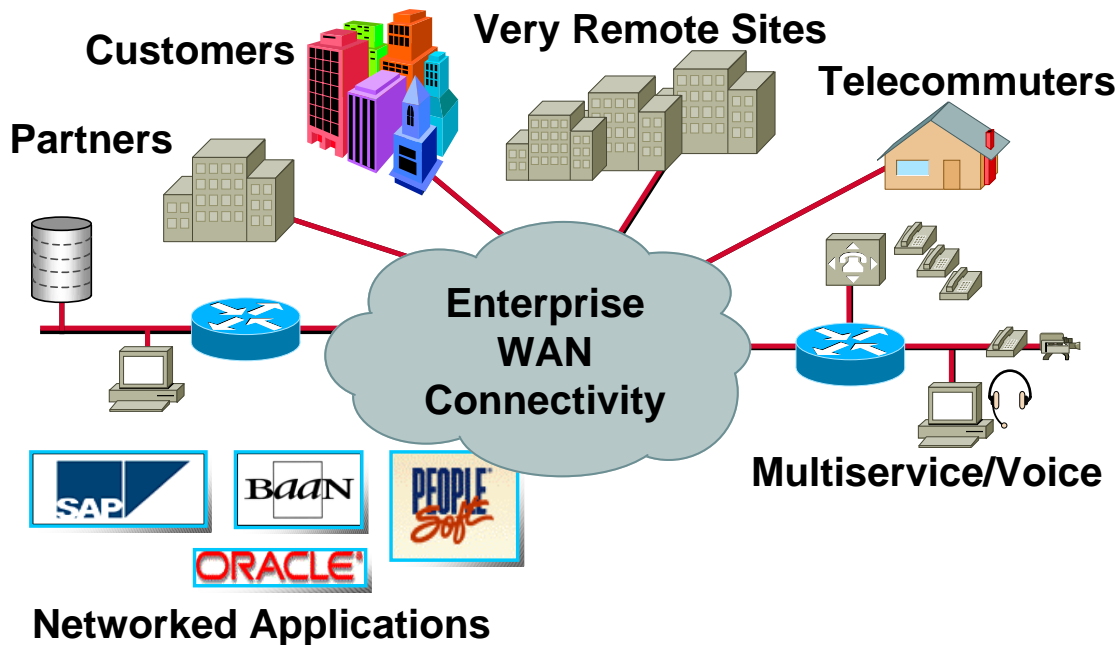
Networked Applications

Types of Virtual Private Networks

Intranet VPN

- Low cost, tunneled connections with rich VPN services, like IPSec encryption and QoS to ensure reliable throughput
- Cost savings over Frame Relay and leased lines

Home Office

Main Office

POP

VPN

Remote Office

POP

Extranet VPN

- Extends WANs to business partners
- Safe L3 security

Business Partner

Remote Access VPN

- Secure, scalable, encrypted tunnels across a public network, client software
- Cost savings over toll-free number expenditures

Mobile Worker
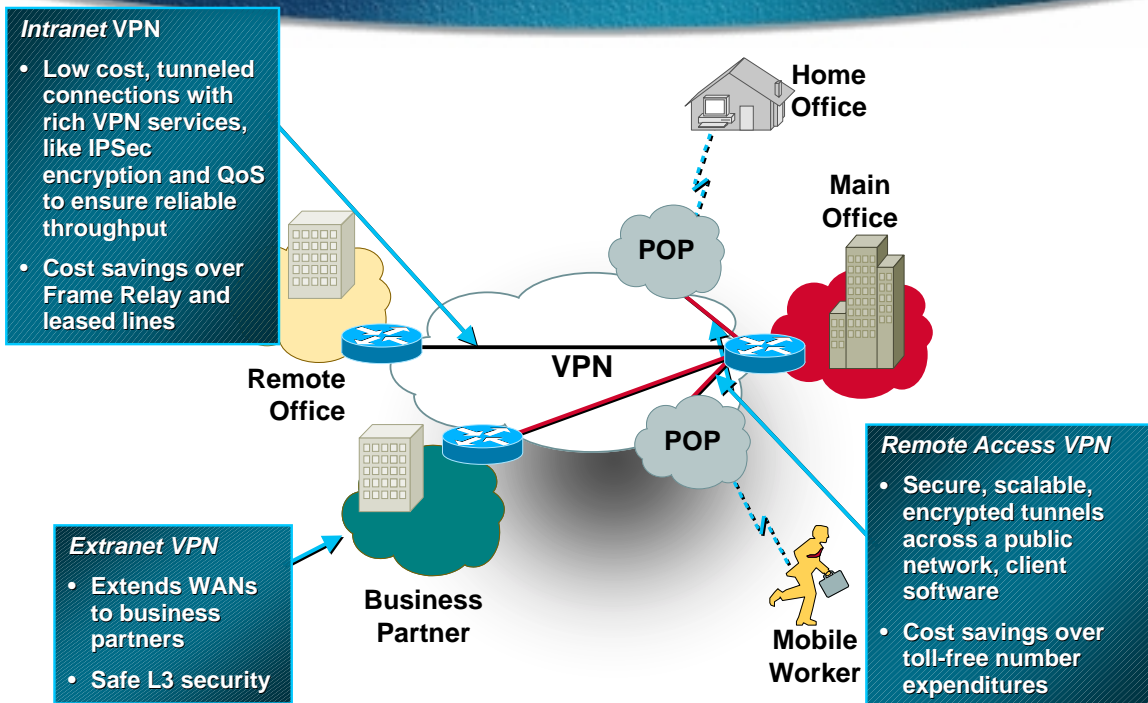
VPN Applications and Requirements

Extranet
Business-to-Business

Remote Access

DSL Cable

POP

VPN

Intranet

Central Site
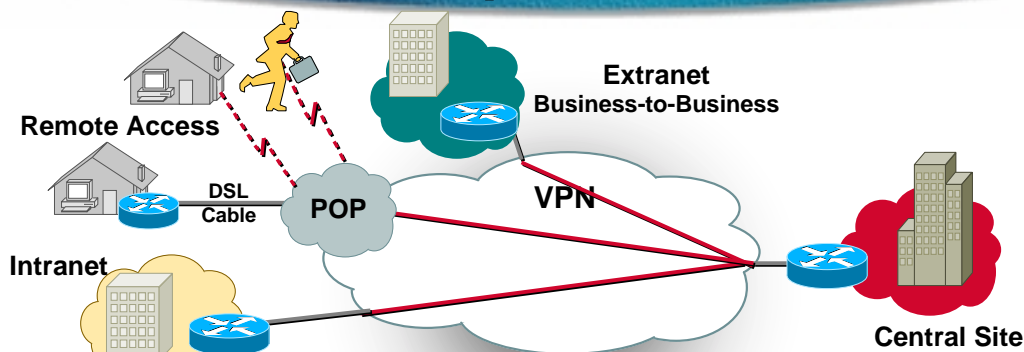
Remote Access

- **Extension of dial**
- **User manageability and deployment scalability**

Site-to-Site: Intranet and Extranet

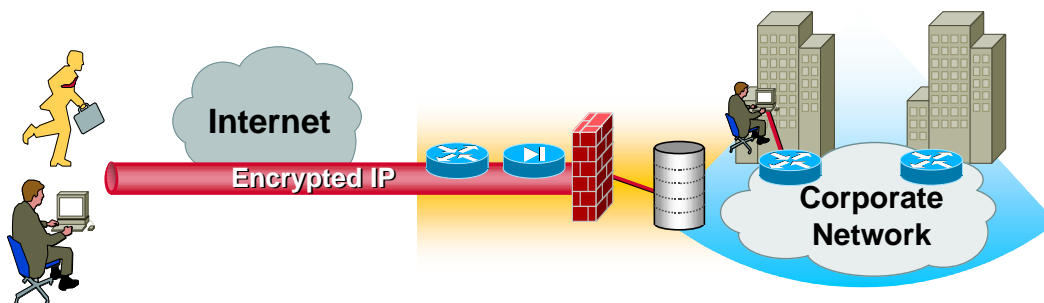- **Extension of classic WAN**
- **VPN services and scalable performance**

The Challenge **and** Opportunity of Broadband Access

Access VPN: Client Initiated

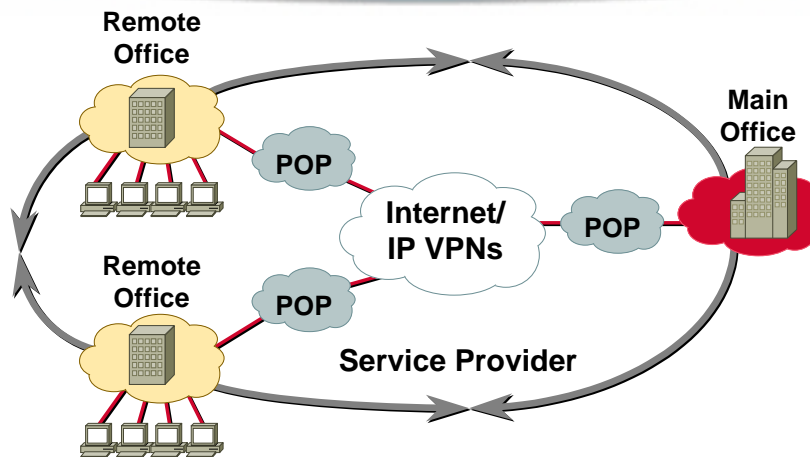**Internet**

Encrypted IP

Corporate Network

- **Encrypted tunnel from the remote client to the corporate network**
- **Independent of broadband access technology**
- **Standards compliant**
  - IPSec encapsulated tunnel
  - IKE key management
- **Fully interoperable**
  - Cisco IOS® and other IPSec-compliant systems

VPN Types: Intranet VPN

Remote Office

Main Office

POP

Internet/ IP VPNs

POP
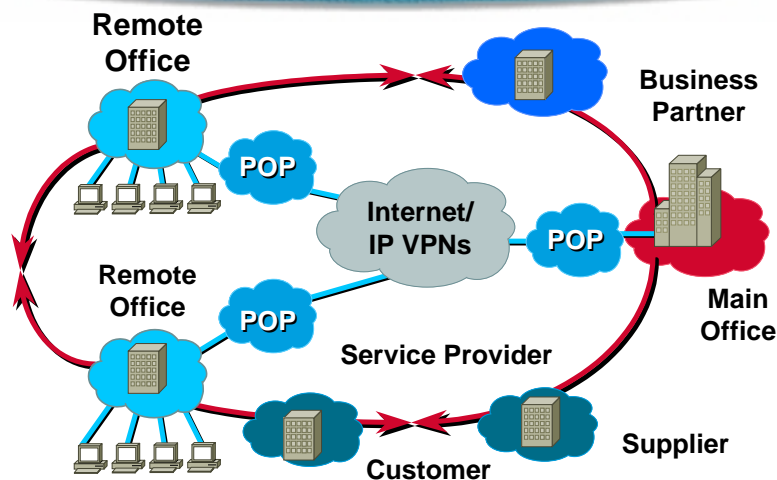
Remote Office

POP

Service Provider

- **Extends the connectionless IP model across a shared WAN**
  - **Reduces application development time**
  - **Reduces support costs**
 - **Reduces line costs**

VPN Types: Extranet VPN

Remote Office

Business Partner

POP

Internet/ IP VPNs

POP

Remote Office

POP

Main Office

Service Provider

Customer

Supplier

- **Extend connectivity to suppliers, customers, and business partners**
- **Over a shared infrastructure**
- **Using dedicated connections**
- **While ensuring proper level of authorized access**
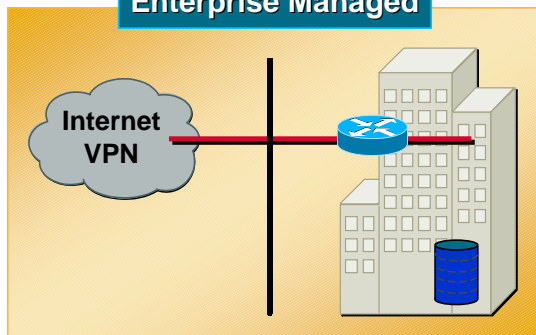
Router/Firewall-Initiated VPN

Internet

POP   POP

**IPSec
Encrypted
Tunnel**

Remote Router or Firewall Initiated
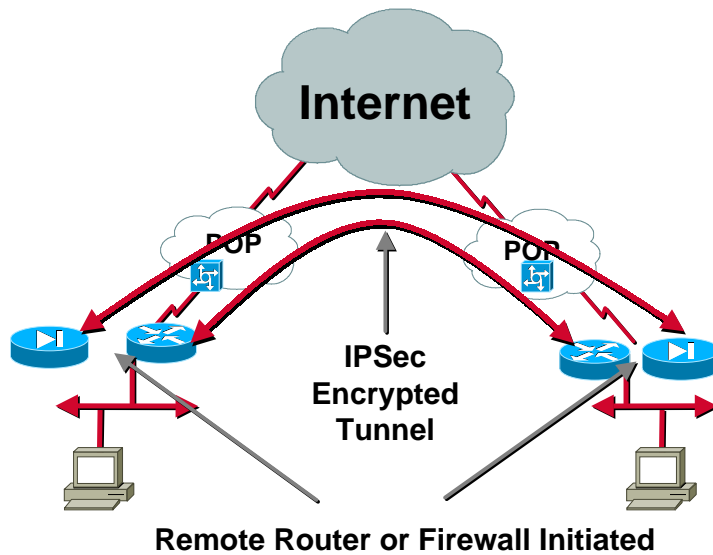
For Site-to-Site Connectivity—Intranets and Extranets

VPNs Come in Many Flavors

**Intranet VPN
Extranet VPN**

Layer 2   **Layer 3**

FR   **ATM**   **Internet VPN**   **IP VPN**
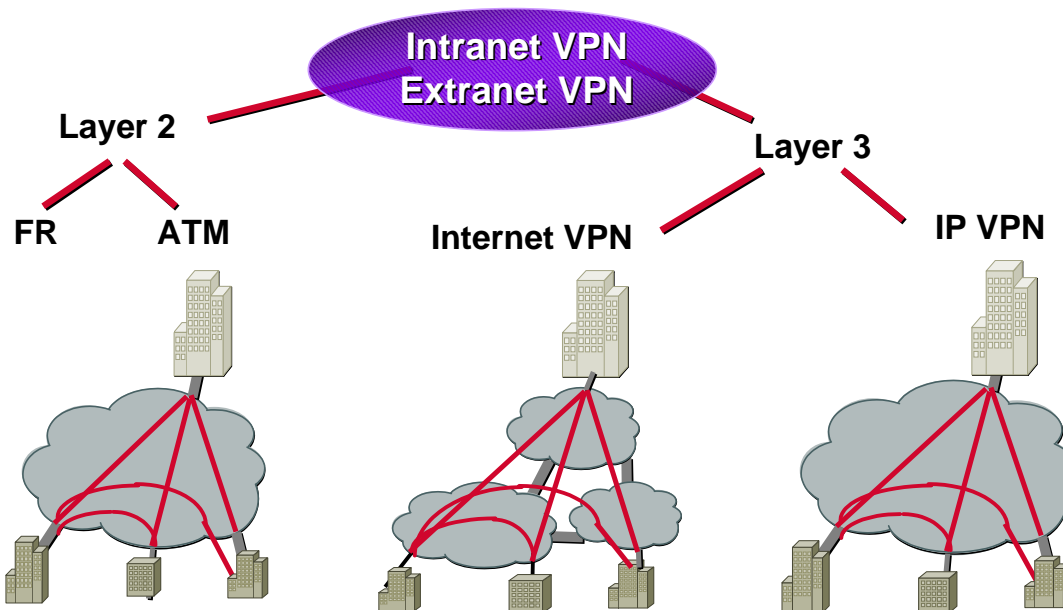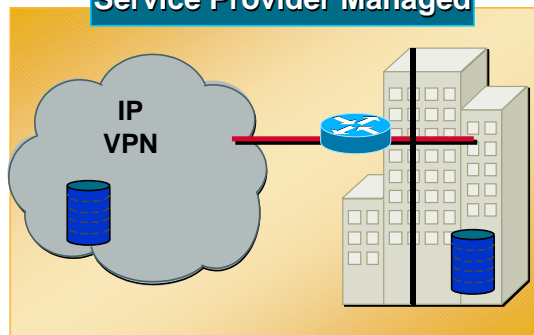
VPNs—Who Does What

Enterprise Managed

Internet VPN

- Service Provider provides basic VPN connectivity
- Enterprise manages QoS, security, SLA, and configuration of VPN functions
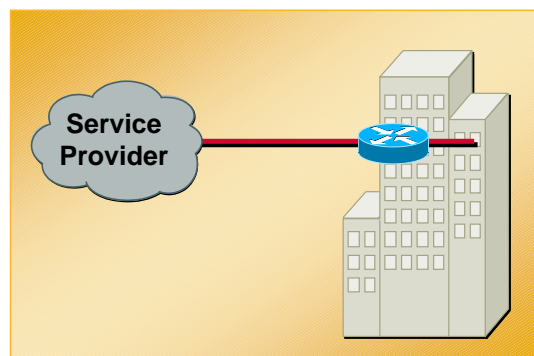
Service Provider Managed

IP VPN

- Service Provider provides turnkey VPN
- Enterprise outsources design, provisioning and management
- Enterprise controls security

VPN Equipment Options

Service Provider — Encrypt, Firewall, B/w Mgr., SLA Probe

Service Provider
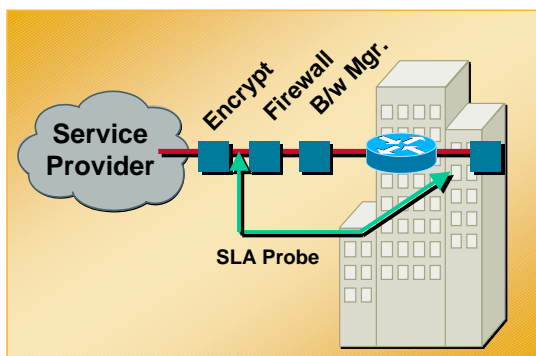
- **Multiple devices**
- **Separate management**

- **Integrated services**
- **Scalable performance**
- **Simplified provisioning**

VPN Security

   cisco.com

Security: A Physical Analogy

Security Camera

Traditional Locks

Security Office

Card Key

Guard
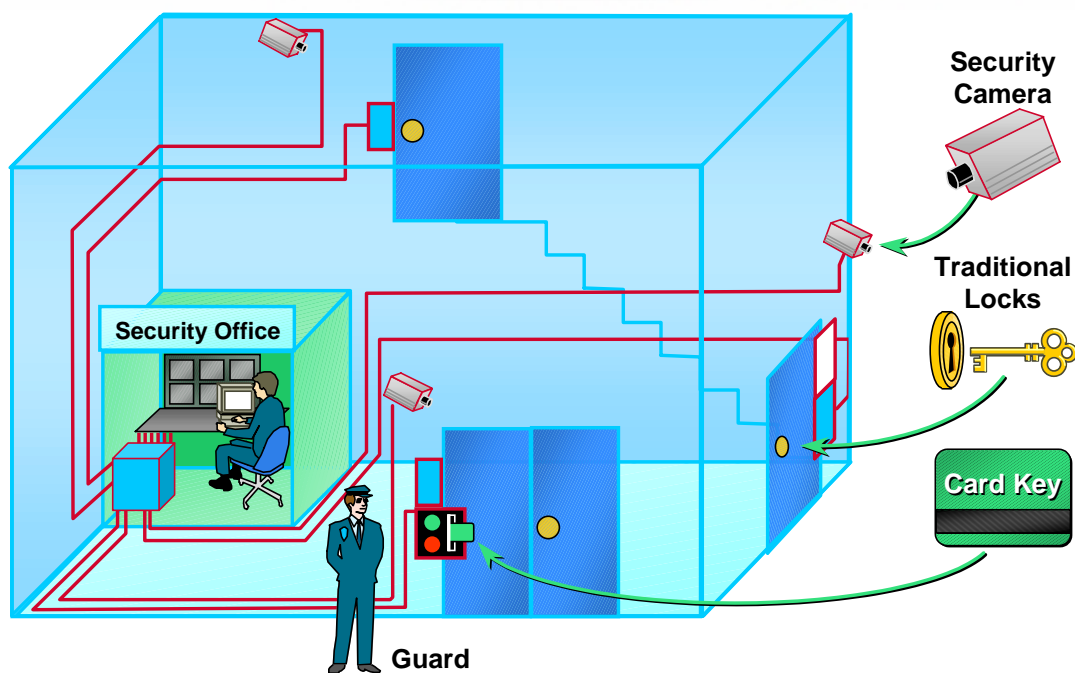
   cisco.com

Elements of Network Security

- **Corporate security policy**
- **Secure**
    - **Identification**
        - **Provide authentication services**
    - **Perimeter control**
        - **Restrict and manage access to network resources**
        - **Protect against denial-of-service attacks, etc.**
    - **Data privacy—VPN**
        - **Ensure data confidentiality**
- **Security monitoring**
    - **Detect and react to intruders**
- **Test**
    - **Recognize network vulnerabilities**
- **Policy Management**
    - **Centralized control of security services**
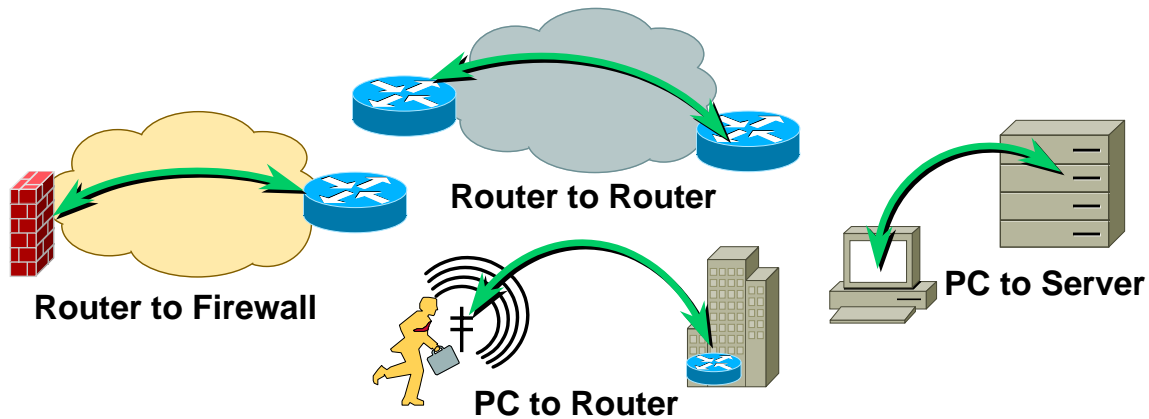

Why VPN Security?

- **VPNs are shared IP networks (untrusted)**

- **VPNs need robust security like classic WANs**

    - **Authentication**

    - **Integrity and confidentiality**

- **VPNs need auditing/monitoring: How do you know your VPN is secure?**

IPSec Technology Review

Router to Router

PC to Server

Router to Firewall

PC to Router

- **IETF standard enables encrypted communication between users and devices**
  - Implemented transparently into the network infrastructure
  - Scales from small to very large networks

- **Open standard enables multivendor interoperability**

- **Included in Cisco IOS 11.3 and later**
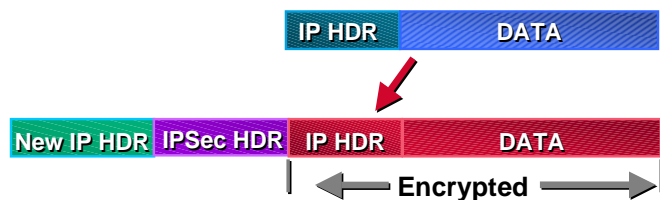

IPSec Modes

- **Tunnel mode: applied to an IP tunnel**

  Outer IP header specifies IPSec processing destination

  Inner IP header specifies ultimate packet destination

Tunnel Mode

IP HDR	DATA

New IP HDR	IPSec HDR	IP HDR	DATA

← Encrypted →

- **Transport mode: between two hosts**

  Header after IP header, before TCP/UDP header

Transport Mode

IP HDR	DATA

IP HDR	IPSec HDR	DATA

← Encrypted →
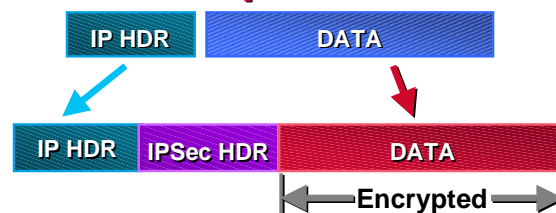
Public Key Infrastructure

BALTIMORE

Entrust Technologies

BANK

VeriSign™

?

CA

Internet

CA
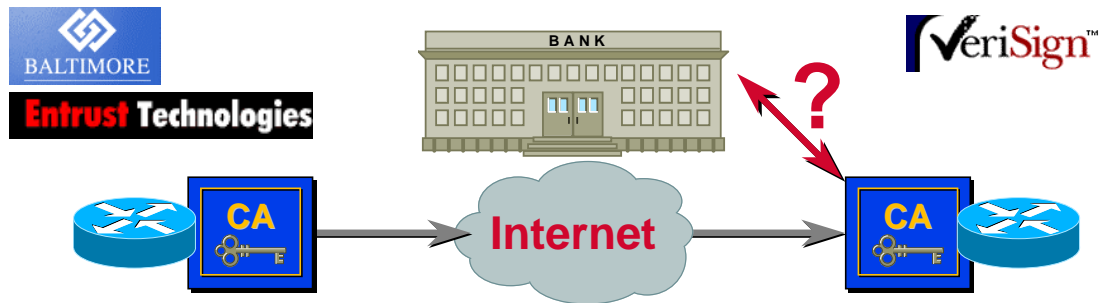
- **Digital certification identity mechanism for users and devices (electronic ID card)**

- **Certificate Authority (CA) verifies identity and signs digital certificate, and deals with certificate creation, storage, distribution, revocation, recovery**

- **Certificate Authorities help provide scalability**

- **Cisco IOS interoperates with:**

  Verisign Onsite for IPSec, Entrust VPN Connector, Baltimore Technologies, Microsoft

---

IPSec Linking Sites

- ### Device authentication

  Crypto devices obtain digital certificates from CAs

- ### Authorization

  Packet selection via ACLs

  Security Association (SA) established via IKE

- ### Privacy and integrity

  IPSec-based encryption and digital signature

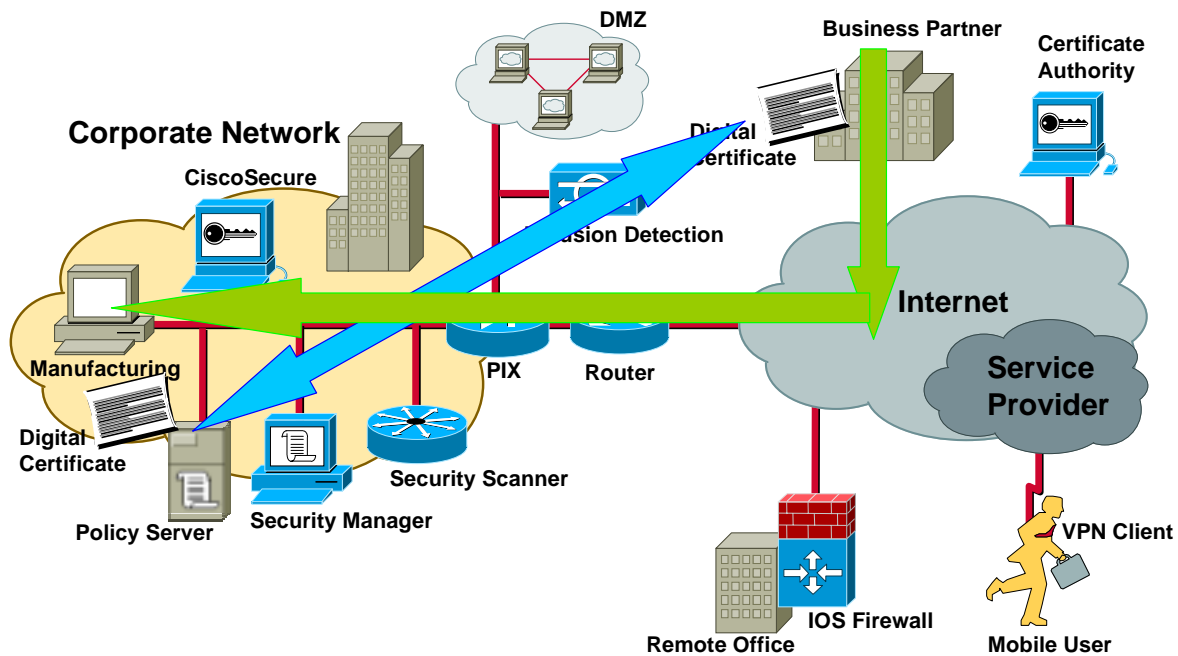- ### Security Associations are a scarce resource
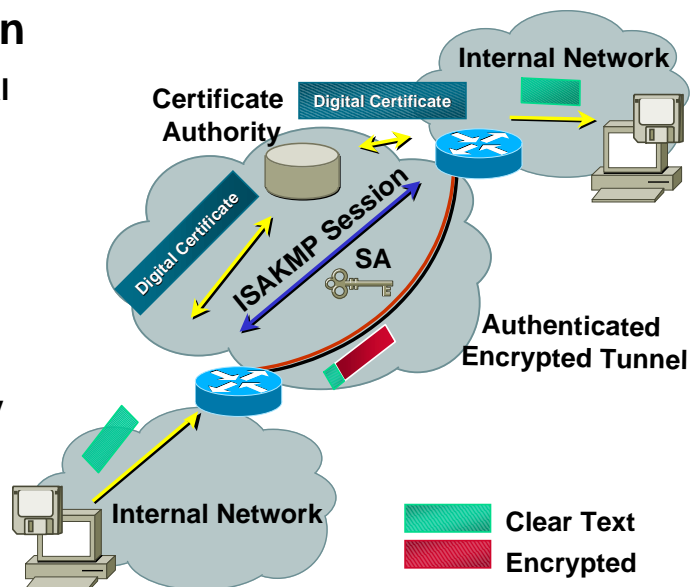
Internal Network

Certificate Authority

Digital Certificate

Digital Certificate

ISAKMP Session

SA

Authenticated Encrypted Tunnel

Internal Network

Clear Text

Encrypted

Secure VPN: Identity

DMZ

Business Partner

Certificate Authority

Corporate Network

CiscoSecure

Digital Certificate

Intrusion Detection

Internet

Service Provider

Manufacturing

PIX

Router

Digital Certificate

Security Scanner

Policy Server

Security Manager

VPN Client

IOS Firewall

Remote Office

Mobile User

Secure VPN: Data Privacy

DMZ

Business Partner

Certificate Authority

Corporate Network

CiscoSecure

Intrusion Detection

Manufacturing

PIX

Router

Service Provider

Security Scanner

Policy Server

Security Manager

VPN Client

IOS Firewall

Remote Office

Mobile User
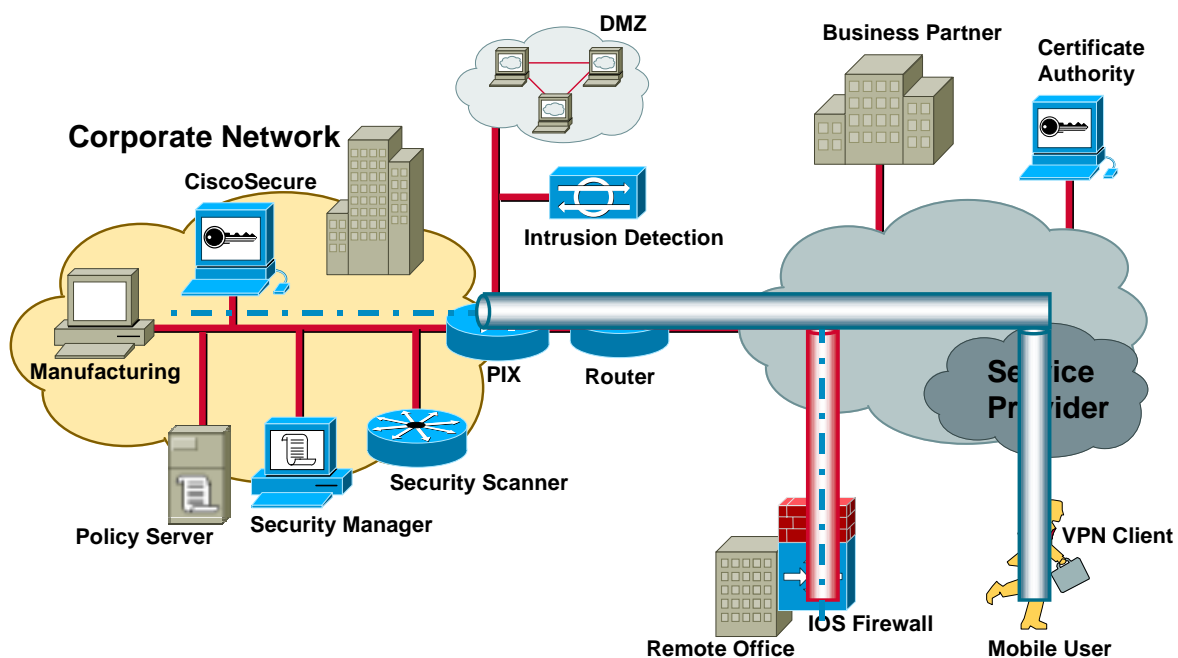
Secure VPN: Perimeter Security

DMZ

Business Partner

Certificate Authority

Corporate Network

CiscoSecure

Hacker

Intrusion D

Internet

Manufacturing

PIX

Router

Service Provider

Security Scanner

Policy Server

Security Manager

VPN Client

IOS Firewall

Remote Office

Mobile User
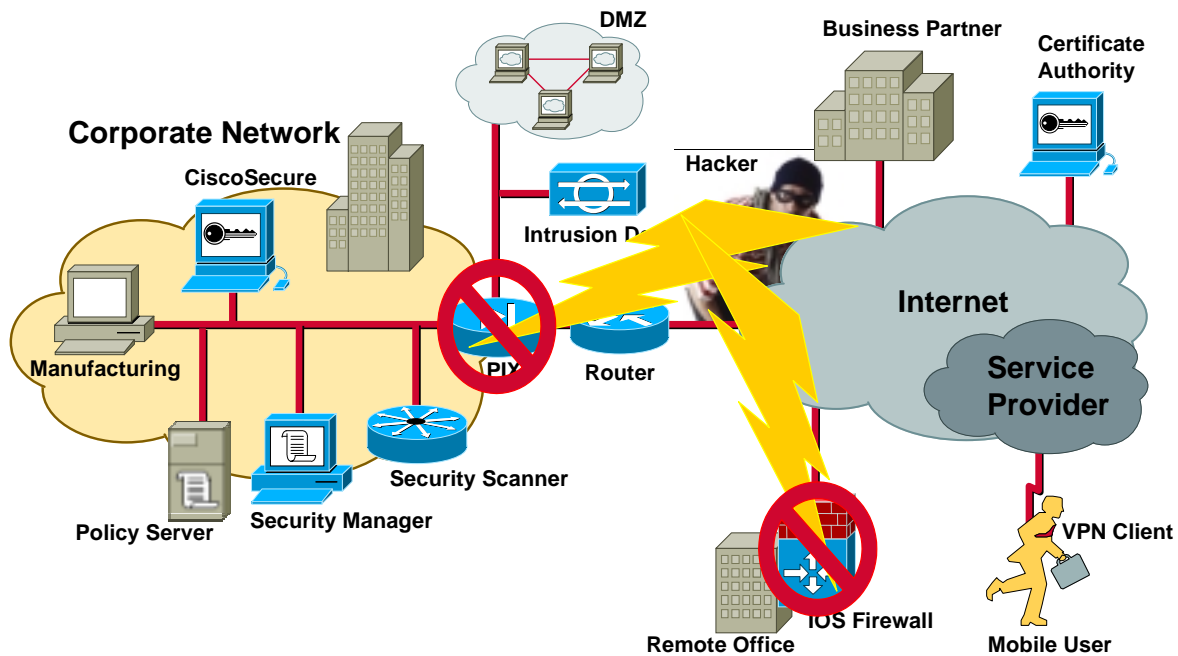
Secure VPN: Security Monitoring

DMZ

Business Partner

Certificate Authority

Corporate Network

CiscoSecure

Hacker

Internet

Manufacturing

PIX

Router

Service Provider

Security Scanner

Policy Server

Security Manager

VPN Client

IOS Firewall

Remote Office

Mobile User
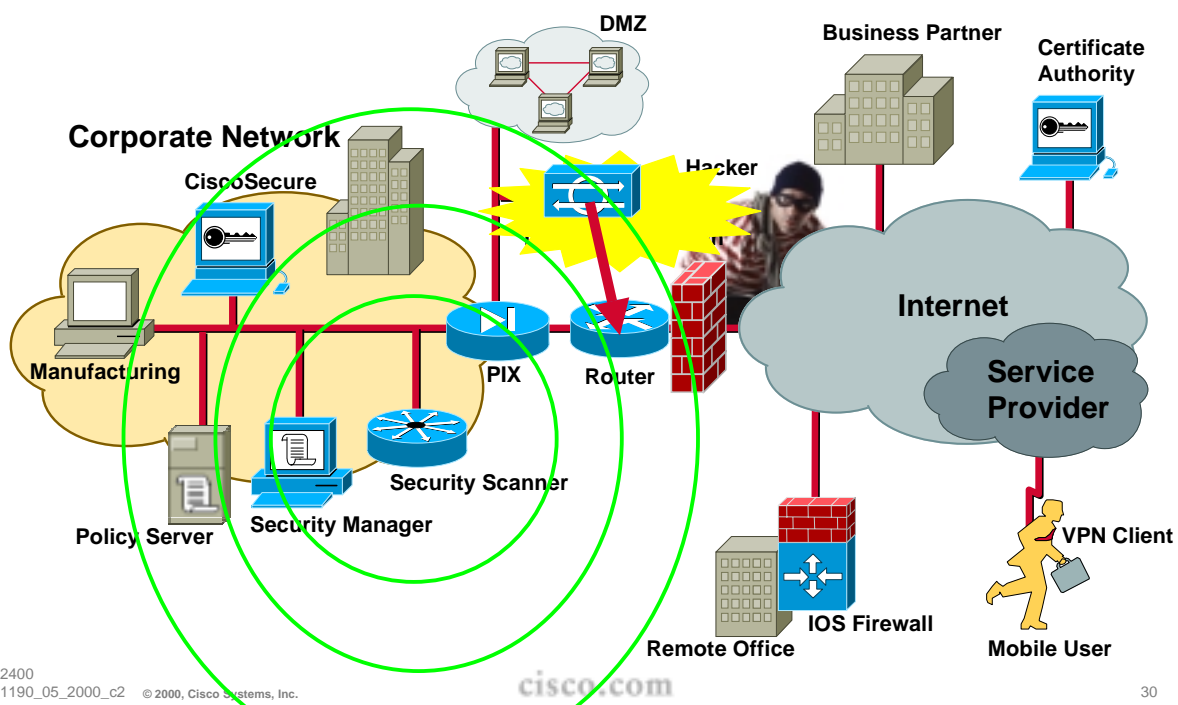
Secure VPN: Policy Management
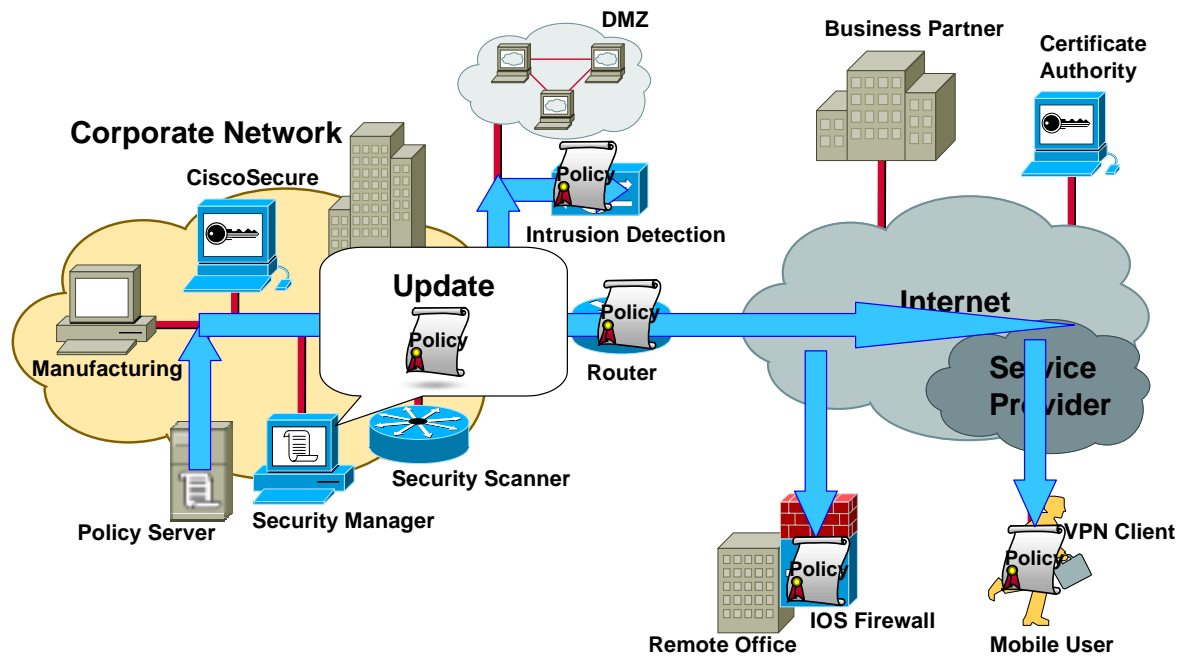
DMZ

Business Partner

Certificate Authority

Corporate Network

CiscoSecure

Policy

Intrusion Detection

Update
Policy

Internet

Manufacturing

Policy

Router

Service Provider

Security Scanner

Policy Server

Security Manager

Policy

IOS Firewall

Remote Office

VPN Client

Policy

Mobile User

E-VPN Platforms

Remote Access VPN
Cisco VPN 3000 Concentrator Series
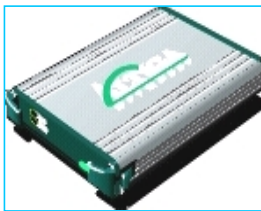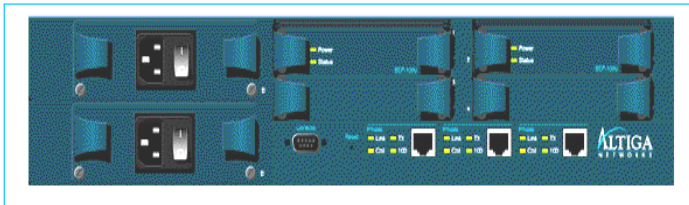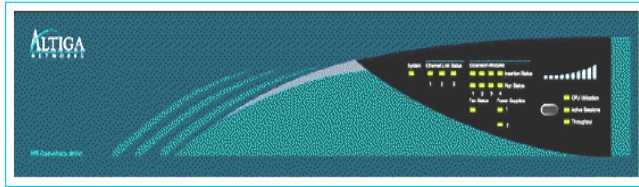
Scalable Encryption Processor (SEP)

Cisco Site-to-Site VPN Solutions
Scalability for Every Site

Cisco 1700 Series
- VPN-optimized router connecting remote offices at T1/E1 speeds

Remote Office

Cisco 7100, 7200 and 7500 Series
- 7100 for dedicated VPN head-end; 7200, and 7500 for hybrid private WAN and VPN connectivity

Regional Office

Internet/IP VPN

Main Office

Cisco 2600 and 3600 Series
- VPN-optimized routers connecting branch and regional offices at nxT1/E1 speeds

Small Office/ Home Office

Cisco 800, UBr900, and 1400 Series
- VPN-optimized routers for ISDN, DSL, and cable connectivity

Site-to-Site VPN Solutions

Site-Specific Scalability
- Range of platforms to meet requirements from ISDN to DS3+

Feature Interoperability
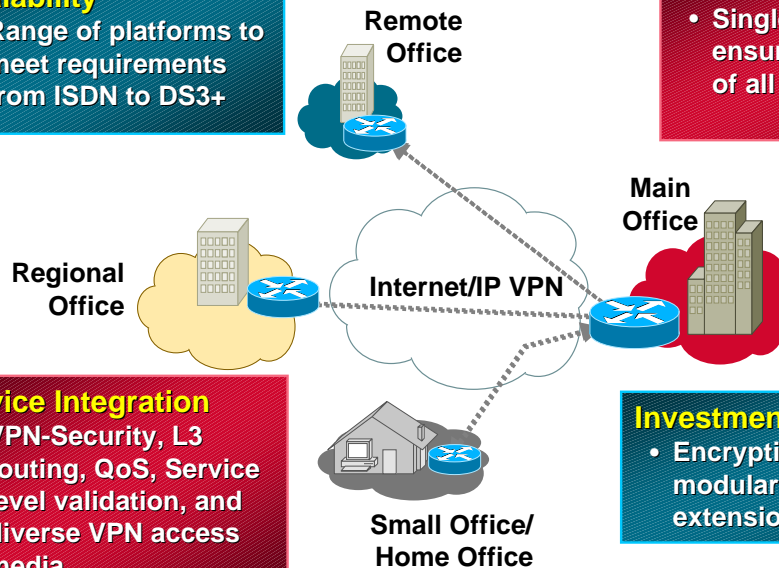- Single device solution ensures interoperability of all VPN services

Remote Office

Regional Office

Internet/IP VPN

Main Office

Device Integration
- VPN-Security, L3 routing, QoS, Service level validation, and diverse VPN access media

Small Office/ Home Office

Investment Protection
- Encryption acceleration modularity and software extensions

E-VPN Services

Quality of Service in a VPN

QoS Benefits for VPNs

- **Make optimum use of VPN WAN link(s)**
- **Provide bandwidth and priority to mission-critical apps**
- **Control non-mission-critical applications**
- **Exploit differentiated services offered by Service Provider**

ISP

CPE Functions
- **Packet classification**
- **Packet marking**
- **WAN-link bandwidth management**
- **Measurement**

SP Functions
- **Adhere to SLA**
  - **Throughput**
  - **Latency**
  - **Availability**
  - **Control congestion**

IPSec TOS Preservation

- **Enables classification for encrypted and tunneled VPNs**

- **Supports ISP Differentiated Services offerings**
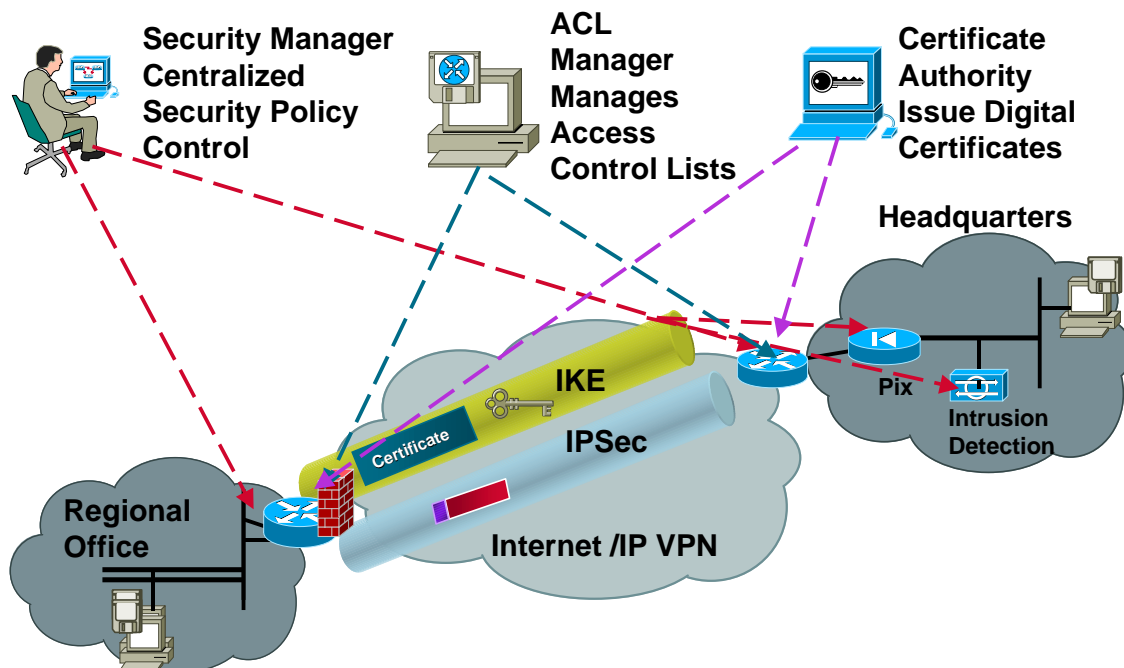
- **Preserves QoS Signaling end-to-end**

Tunneled and Encrypted Packet with QoS Preservation

Non-Classified Traffic

Output Queuing ISP End-to-End

Classifier

QoS Marking

Crypto Engine
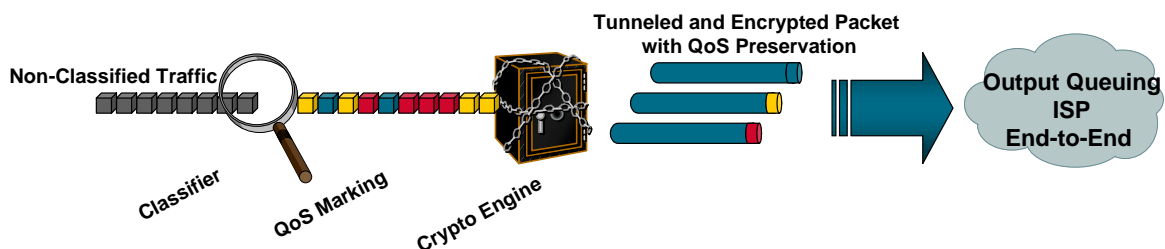
E-VPN Management

VPN Security Management

Security Manager Centralized Security Policy Control

ACL Manager Manages Access Control Lists

Certificate Authority Issue Digital Certificates

Headquarters

IKE

Certificate

IPSec

Pix

Intrusion Detection

Regional Office

Internet /IP VPN

VPN Bandwidth Management

QoS Policy Manager Centralized Bandwidth Management Policy Control

QoS Monitor Monitors Traffic Distribution

Service Level Manager SLA Monitoring and Measurement

SAA

Regional Office

Internet /IP VPN

Pix

Intrusion Detection

Headquarters
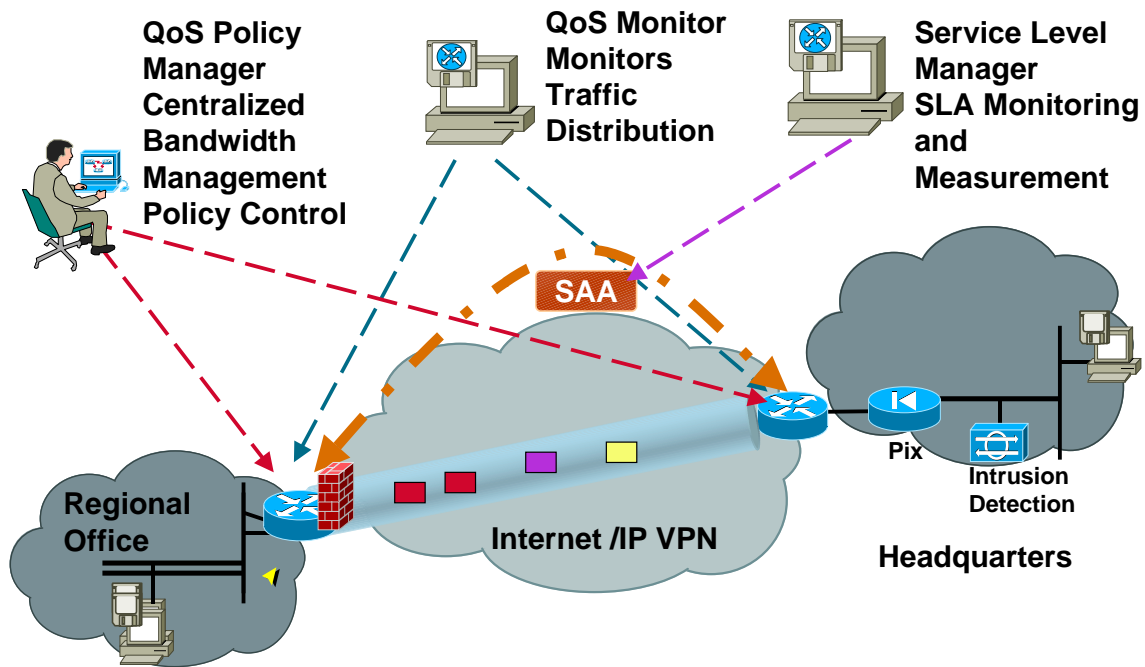
Next Steps

Major VPN Challenges

- **Mobility**

- **Streaming services**

- **Voice, video, audio**

- **Scalable deployment**

- **Policy management**
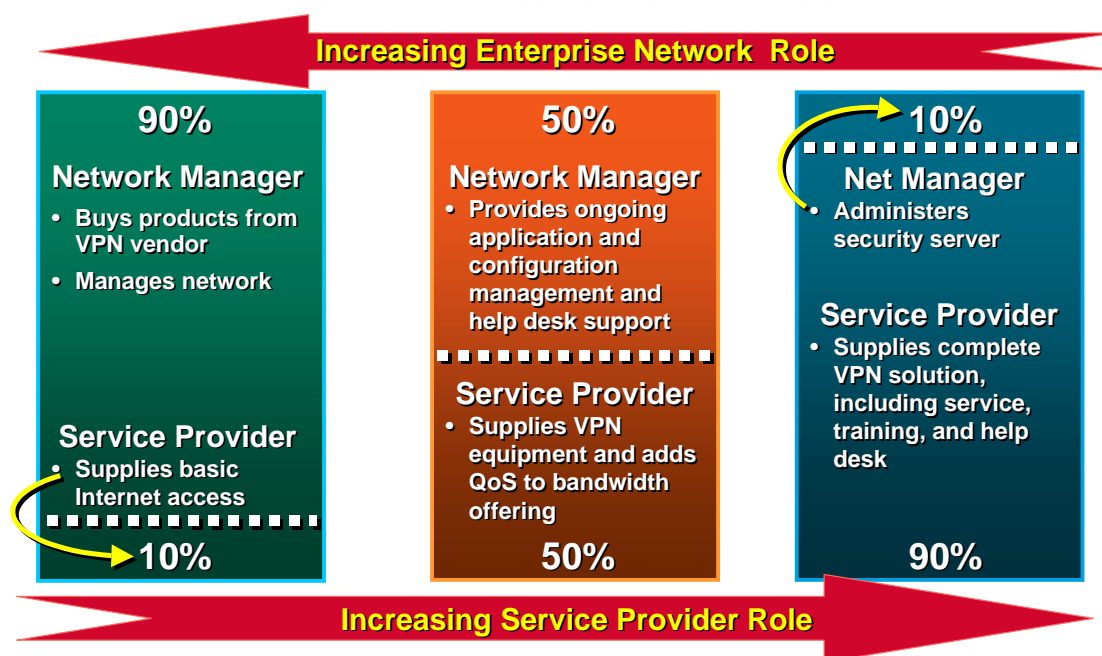

Non-Technology Challenges

Role of Regulation

Conflicting National Policies

Local Standards and Practices

VPN Deployment Options

Increasing Enterprise Network Role

90%

Network Manager
- Buys products from VPN vendor
- Manages network

Service Provider
- Supplies basic Internet access

10%

50%

Network Manager
- Provides ongoing application and configuration management and help desk support

Service Provider
- Supplies VPN equipment and adds QoS to bandwidth offering

50%

10%

Net Manager
- Administers security server

Service Provider
- Supplies complete VPN solution, including service, training, and help desk

90%

Increasing Service Provider Role

Cost-Effectiveness of VPN Remote Access*

	In-House	VPN	Savings
Ports and Tollfree Access	$957,000	$700,000	$257,000
Network Backbone	$500,000	$450,000	$50,000
Staffing	$440,000	$0	$440,000
Security	$185,000	$100,000	$85,000
24 x 7 Help Desk	$750,000	$550,000	$200,000
Network Management	$75,000	$0	$75,000
Totals:	$2,907,000	$1,800,000	$1,107,000

Savings Based on VPN Solution (1000 Users) **38%**
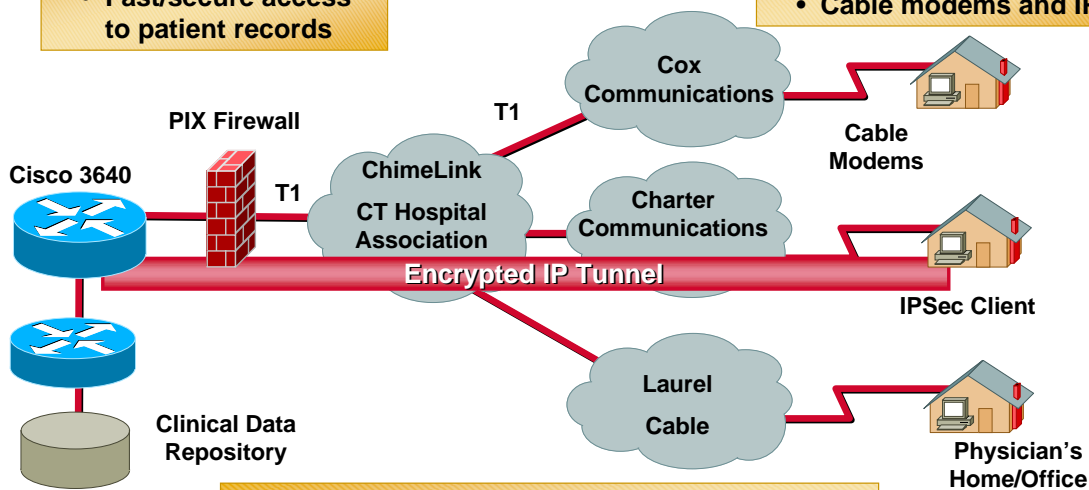
*Numbers are quoted on an annual basis for 1000 users.

Waterbury Hospital

1. Requirement
- Fast/secure access to patient records

2. Solution
- Extranet VPN Via
- Cable modems and IPSec

Cox Communications

T1

Cable Modems

PIX Firewall

Cisco 3640

T1

ChimeLink
CT Hospital Association

Charter Communications

IPSec Client

Encrypted IP Tunnel

Clinical Data Repository

Laurel Cable

Physician's Home/Office

3. Benefit
- High speed access to new applications
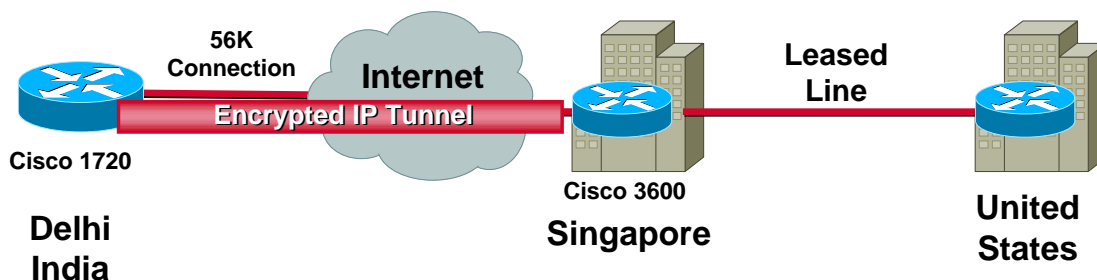- More detailed patient information for doctors

---

Media Company

1. Requirement
- Reliable/low-cost
- Access from remote office

2. Solution
- Intranet VPN Via
- From Delhi to Hong Kong
- Lease line From Hong Kong to US HQ

56K Connection

Internet

Encrypted IP Tunnel

Cisco 1720

Leased Line

Cisco 3600

Delhi India

Singapore

United States

3. Benefit
- 10x cost savings over Frame Relay
- Deployment in 3 weeks vs 6 months
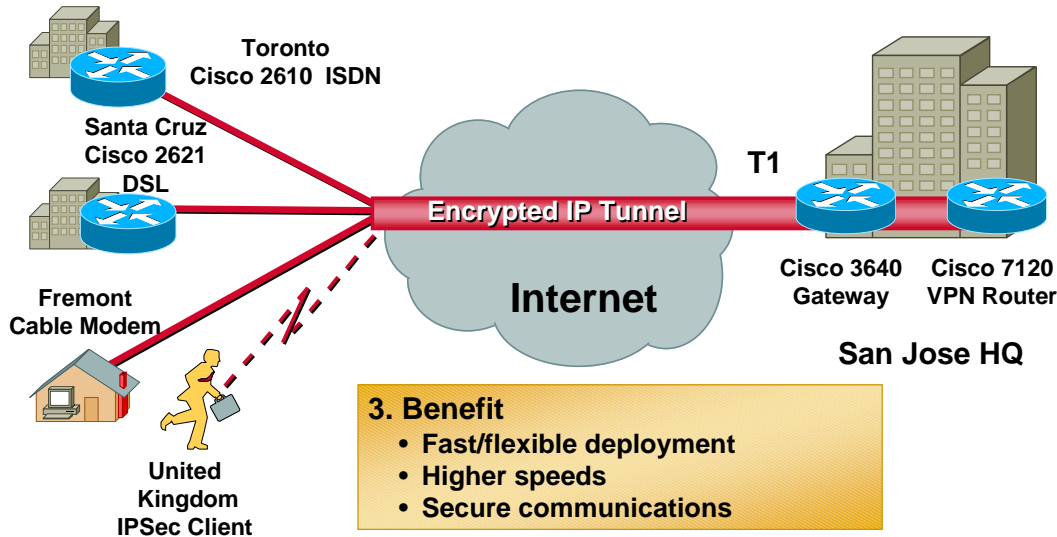- Expanding VPN to other remote sites around world

Altera Semiconductor

1. Requirement
- Reliable/low-cost/secure
- Connections to remote offices and telecommuters

2. Solution
- Intranet and Remote Access
- VPN

Toronto
Cisco 2610 ISDN

Santa Cruz
Cisco 2621
DSL

Fremont
Cable Modem

United
Kingdom
IPSec Client

Encrypted IP Tunnel

Internet

T1

Cisco 3640
Gateway

Cisco 7120
VPN Router

San Jose HQ

3. Benefit
- Fast/flexible deployment
- Higher speeds
- Secure communications

Additional Information

- **www.cisco.com/go/evpn**

- **www.cisco.com/go/security**

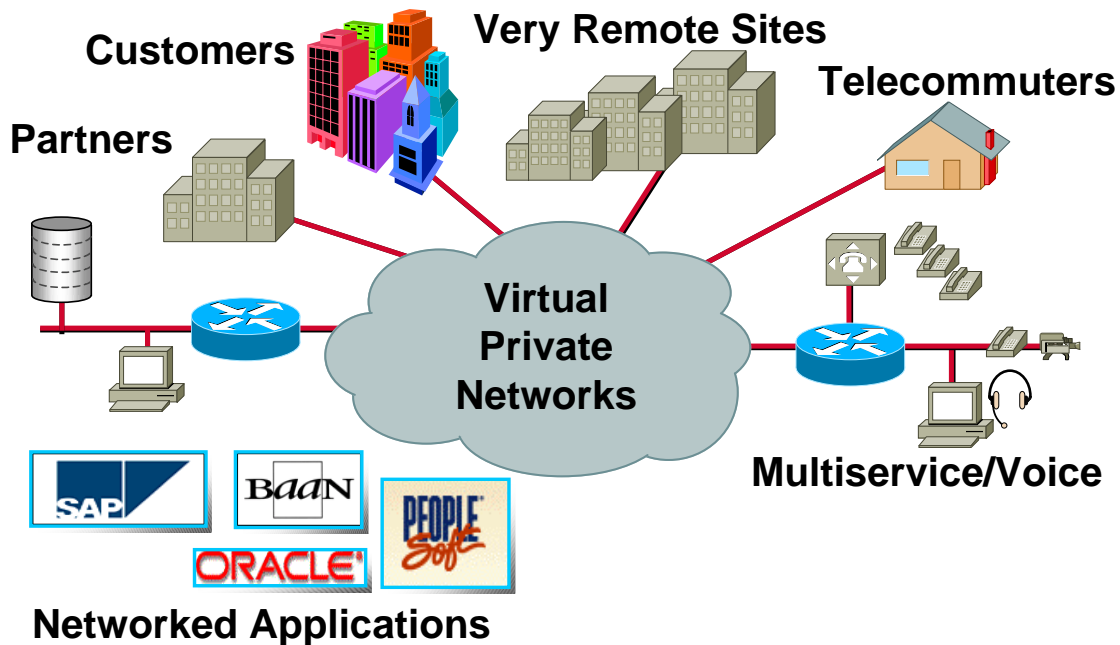- **www.cisco.com/go/securityassociates**

- **Networking Professionals Community**

  White Papers, ISPs with "Cisco Powered" VPN Services, Design Guides, Data Sheets, 3rd Party Solutions

Are You Ready?

Customers

Partners

Very Remote Sites

Telecommuters

Virtual Private Networks

Multiservice/Voice

SAP   BaaN   PEOPLE Soft

ORACLE

Networked Applications

Introduction to VPNs

Extending the Classic WAN

Session 2400

Please Complete Your Evaluation Form

Session 2400

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION℠