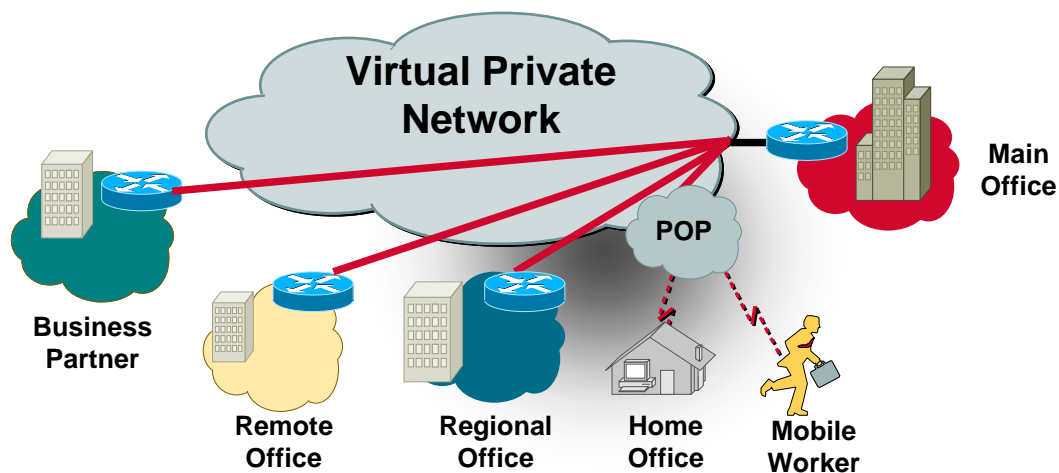


# Agenda

- **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?

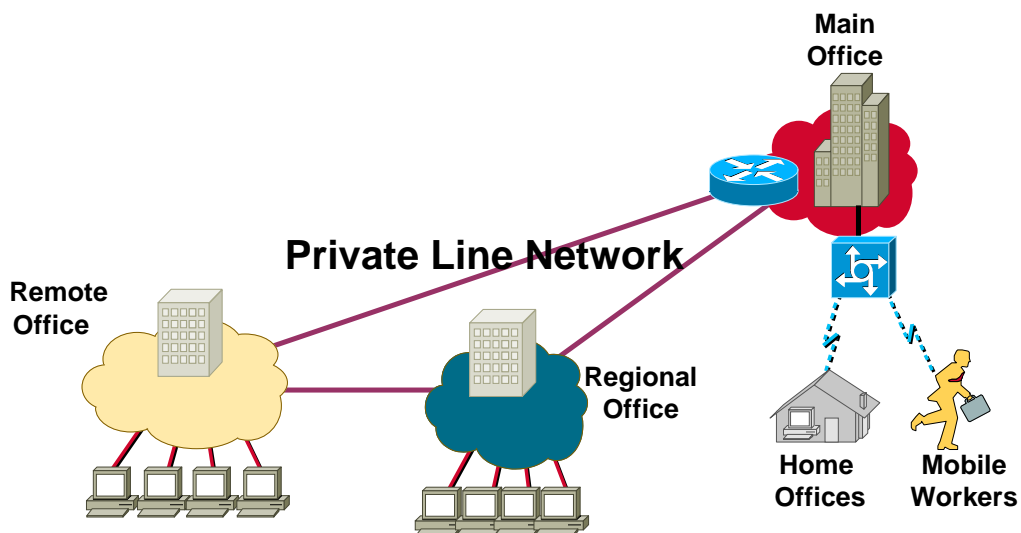
**Connectivity Deployed on a Shared Infrastructure with the Same Policies and 'Performance' as a Private Network**



# The VPN Timeline

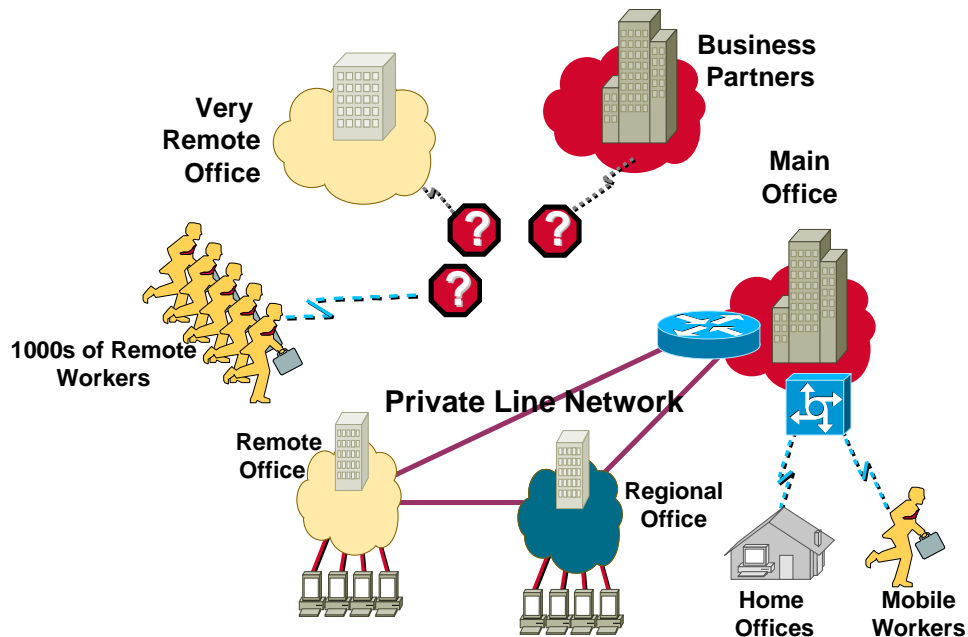
<b>1996</b>	<b>IETF IPsec Draft Standard</b>
<b>1997</b>	<b>IKE Reference Code</b> <b>Diffie/Hellman Patent Buyout</b>
<b>1998</b>	<b>Simple Certificate Enrollment Protocol (SCEP)</b> <b>Campus VPN</b>
<b>1999</b>	<b>Remote Access VPN</b>
<b>2000</b>	<b>IETF PKIX CMC</b> <b>Accelerated VPN Services</b>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

# Classic WAN



# Classic WAN

## Today's New Challenges

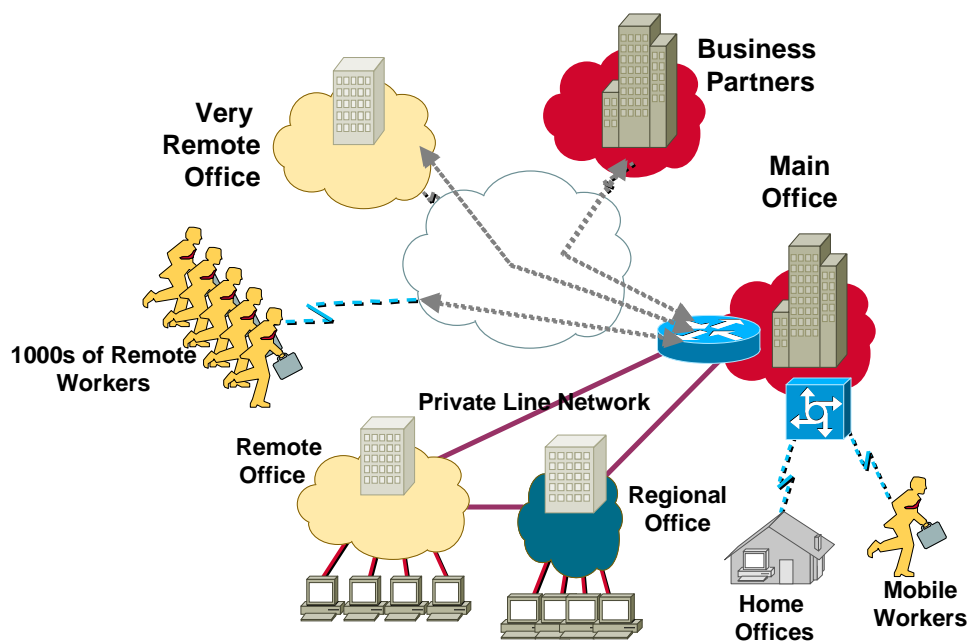


2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

7

# VPNs Extend the Classic WAN



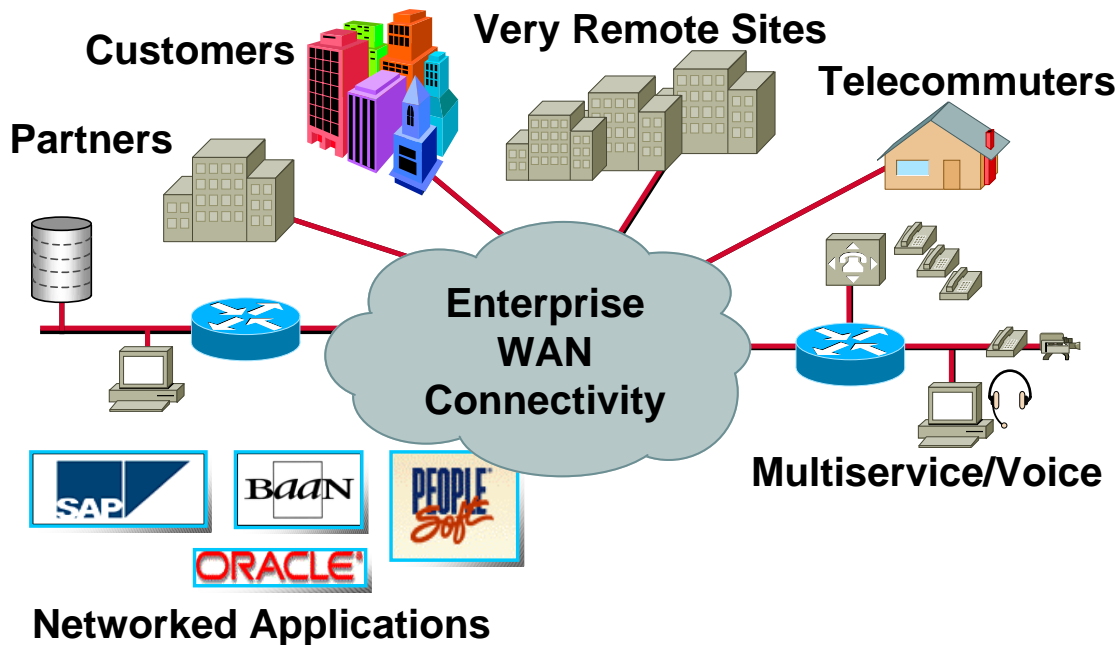
2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

8



# Enabling the Internet Economy

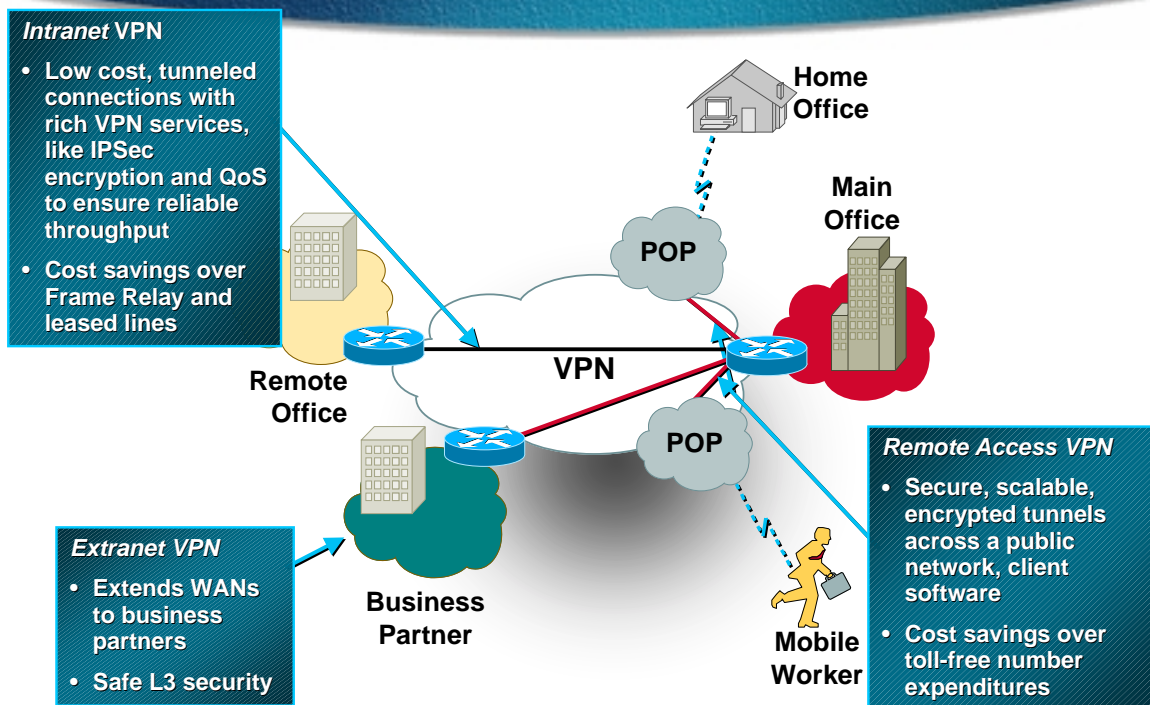


2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

9

# Types of Virtual Private Networks

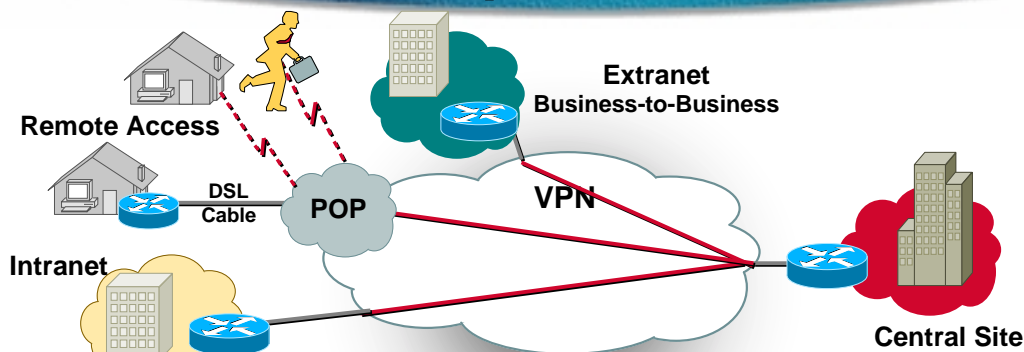


2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

10

# VPN Applications and Requirements



## 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

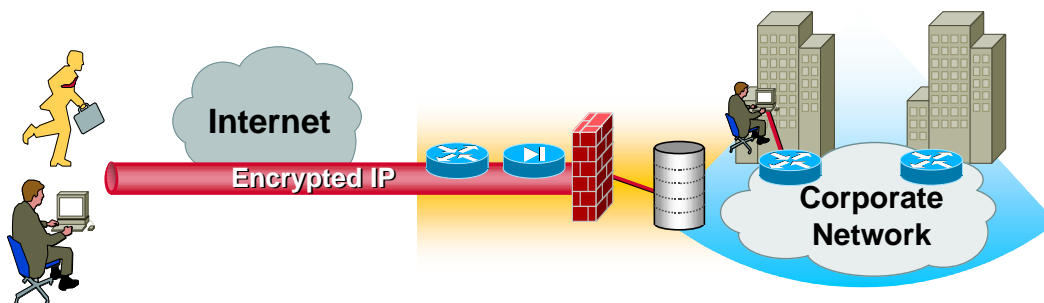
## The Challenge **and** Opportunity of Broadband Access

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

11

# Access VPN: Client Initiated



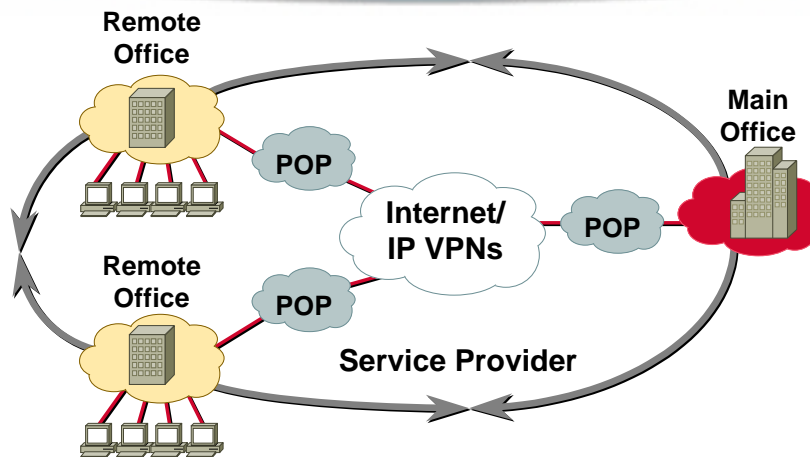
- Encrypted tunnel from the remote client to the corporate network
- Independent of broadband access technology
- Standards compliant
  - IPSec encapsulated tunnel
  - IKE key management
- Fully interoperable
  - Cisco IOS® and other IPSec-compliant systems

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

12

# VPN Types: Intranet VPN



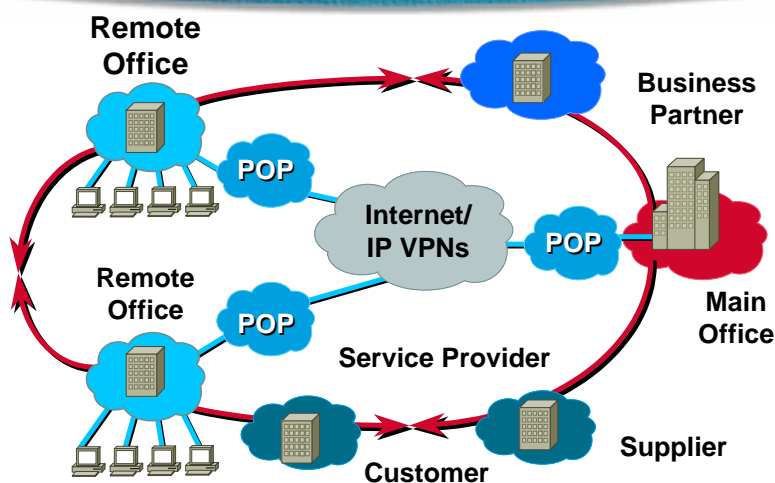
- **Extends the connectionless IP model across a shared WAN**

Reduces application development time

Reduces support costs

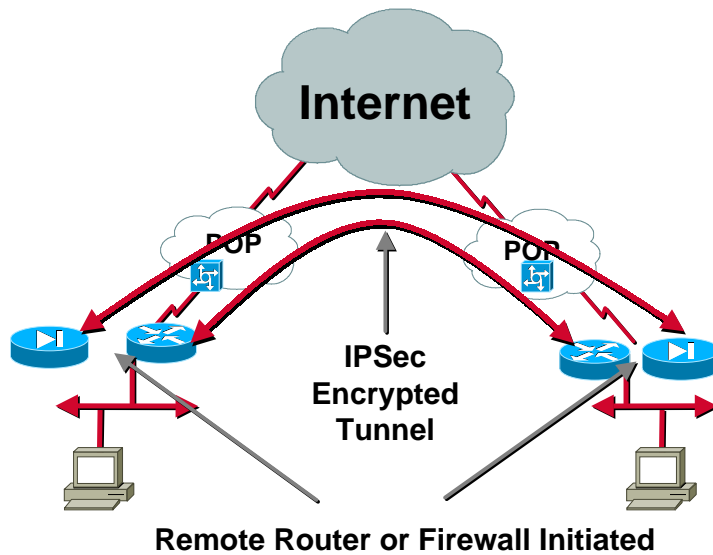
Reduces line costs

# VPN Types: Extranet VPN



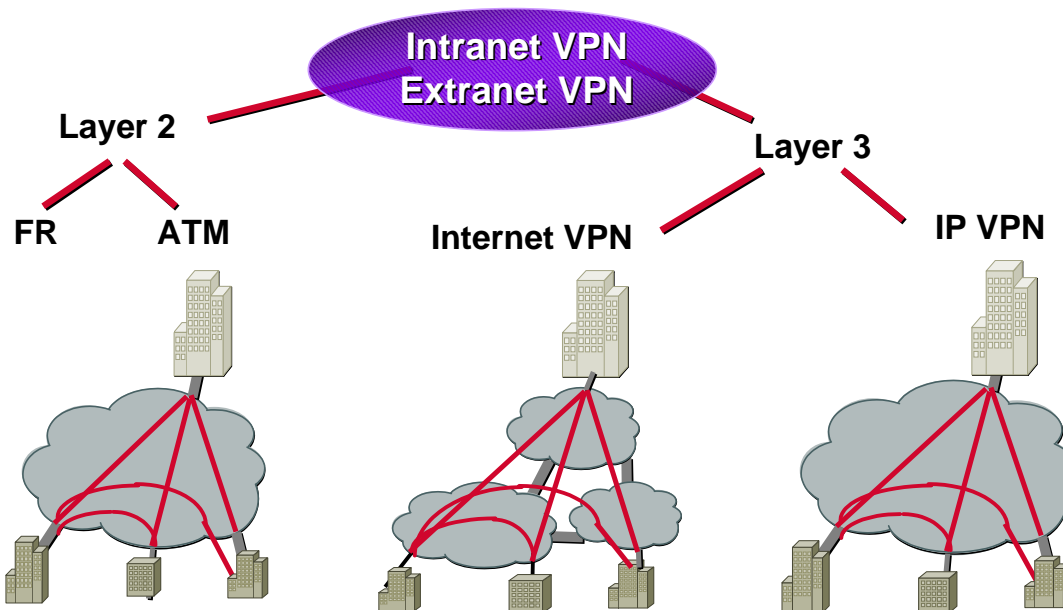
- **Extend connectivity to suppliers, customers, and business partners**
- **Over a shared infrastructure**
- **Using dedicated connections**
- **While ensuring proper level of authorized access**

# Router/Firewall-Initiated VPN



**For Site-to-Site Connectivity—Intranets and Extranets**

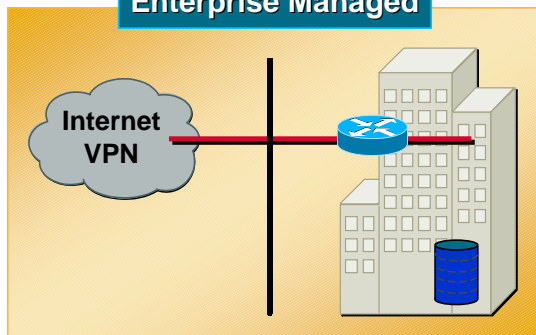
# VPNs Come in Many Flavors





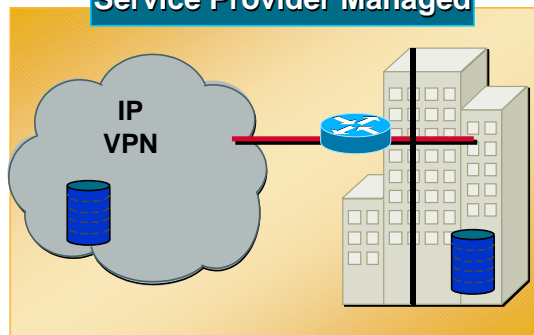
# VPNs—Who Does What

## Enterprise Managed



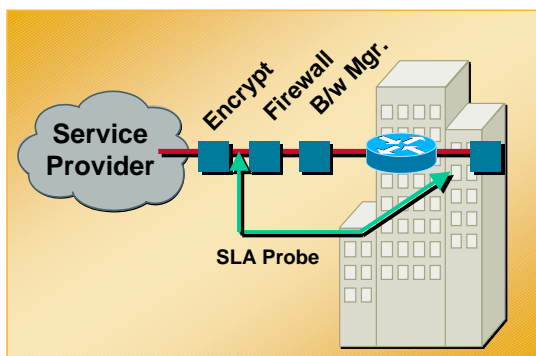
- Service Provider provides basic VPN connectivity
- Enterprise manages QoS, security, SLA, and configuration of VPN functions

## Service Provider Managed

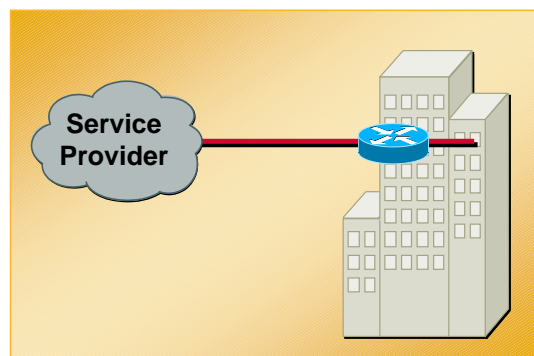


- Service Provider provides turnkey VPN
- Enterprise outsources design, provisioning and management
- Enterprise controls security

# VPN Equipment Options



- Multiple devices
- Separate management



- Integrated services
- Scalable performance
- Simplified provisioning

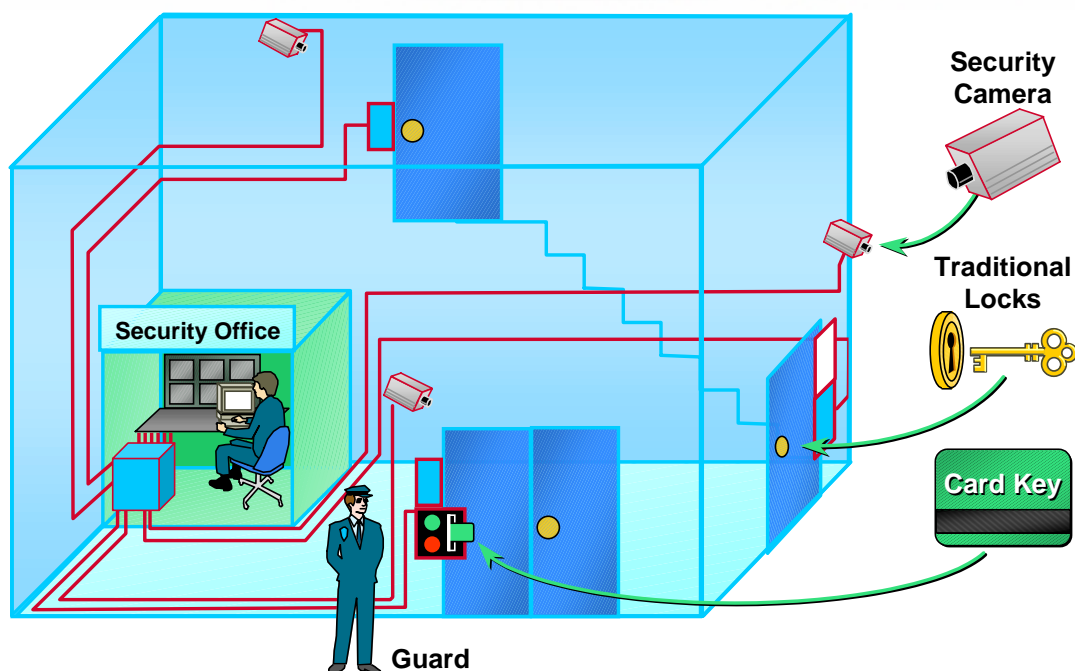
# VPN Security

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

19

## Security: A Physical Analogy



2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

20

# 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



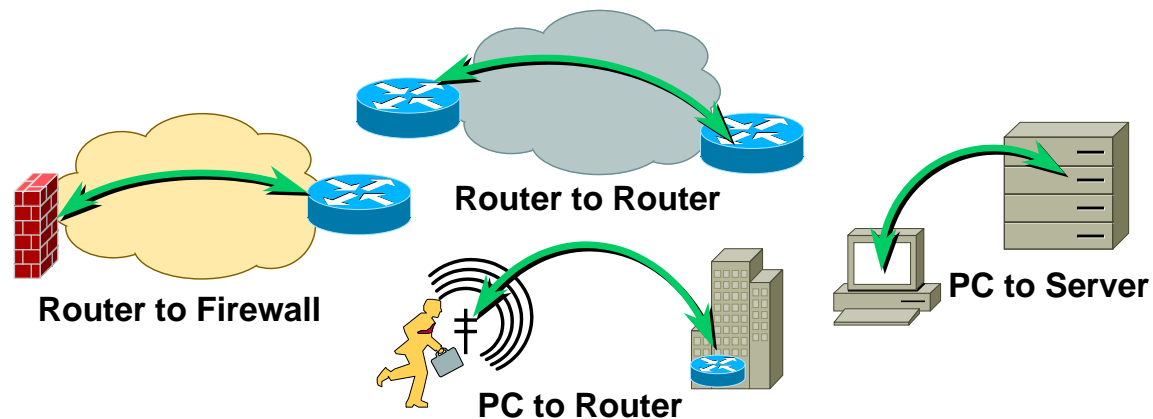
## Why VPN Security?

- **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



- 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

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

23

## IPSec Modes

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

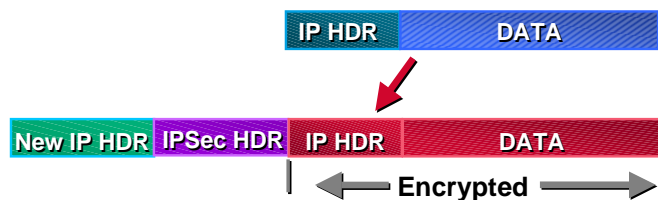
Outer IP header specifies  
IPSec processing  
destination

Inner IP header specifies  
ultimate packet destination

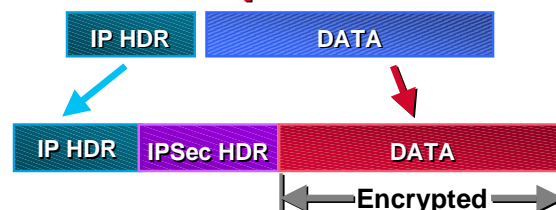
- **Transport mode:**  
between two hosts

Header after IP header,  
before TCP/UDP header

### Tunnel Mode



### Transport Mode



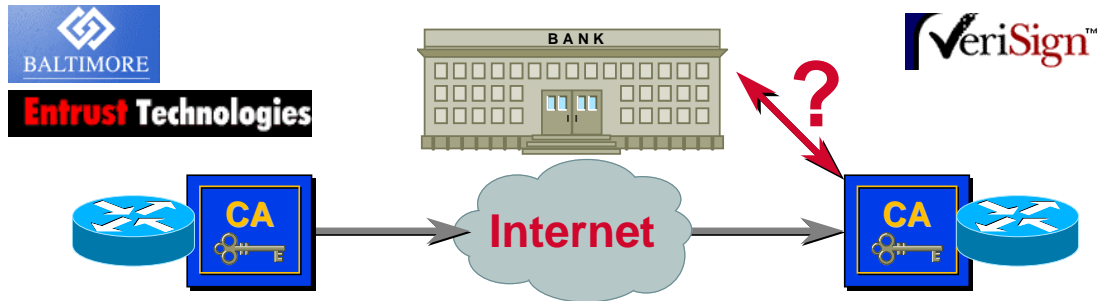
2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

24



# Public Key Infrastructure



- 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

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

25

# IPSec Linking Sites

## • Device authentication

Crypto devices obtain digital certificates from CAs

## • Authorization

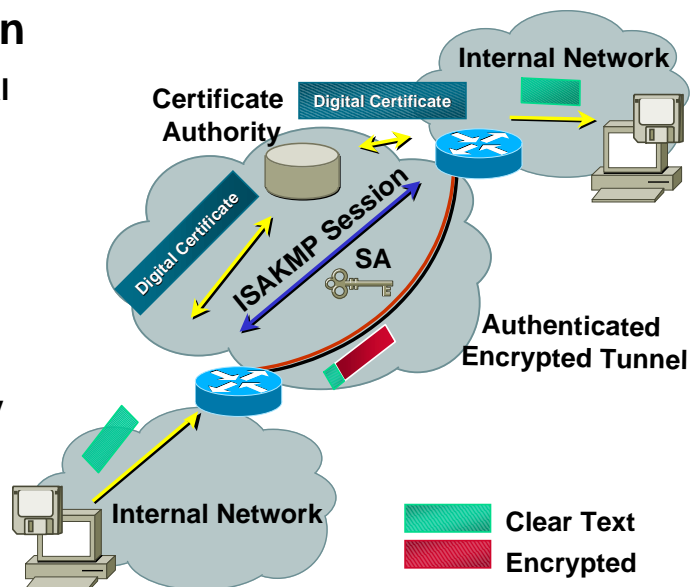
Packet selection via ACLs

Security Association (SA) established via IKE

## • Privacy and integrity

IPSec-based encryption and digital signature

## • Security Associations are a scarce resource

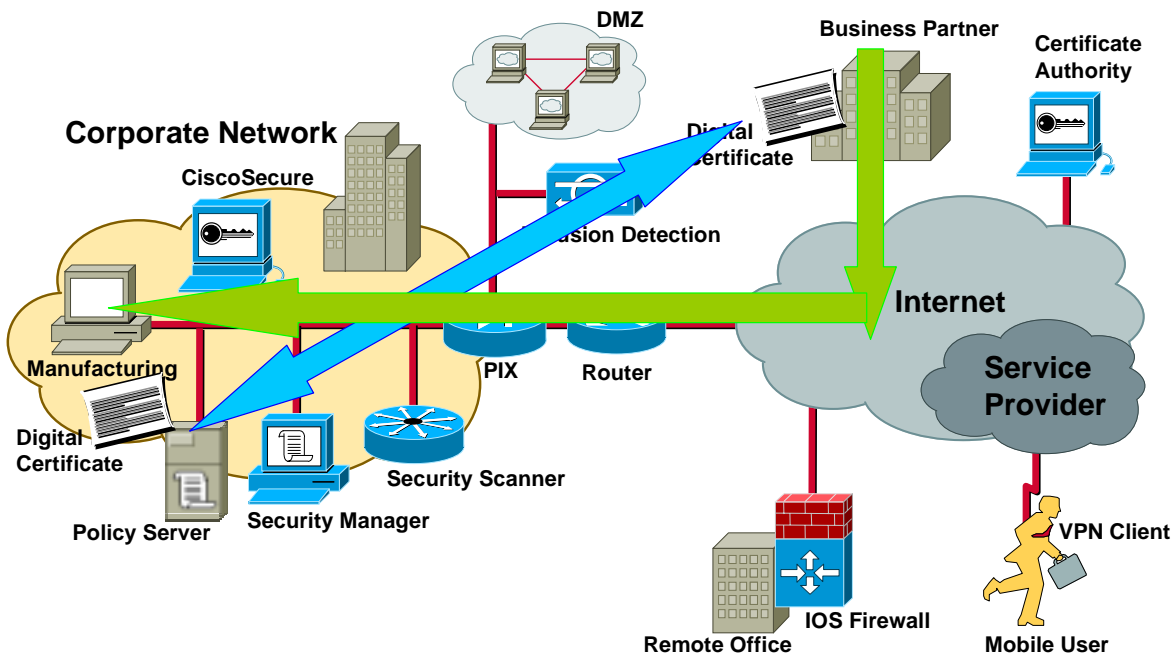


2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

26

# Secure VPN: Identity

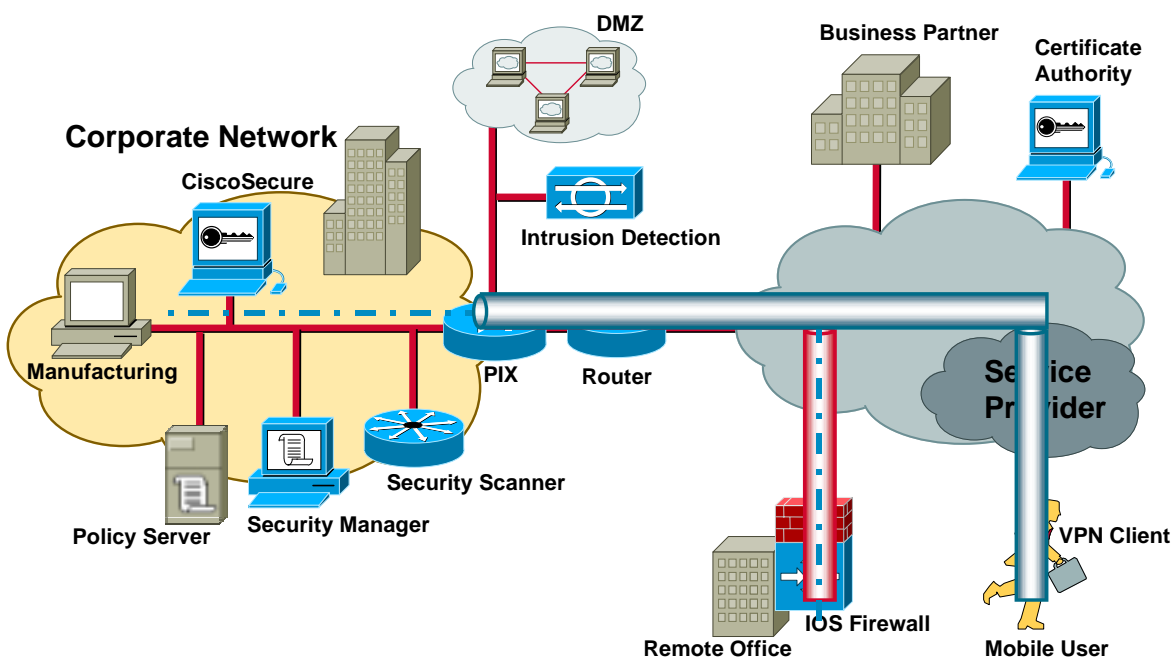


2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

27

# Secure VPN: Data Privacy

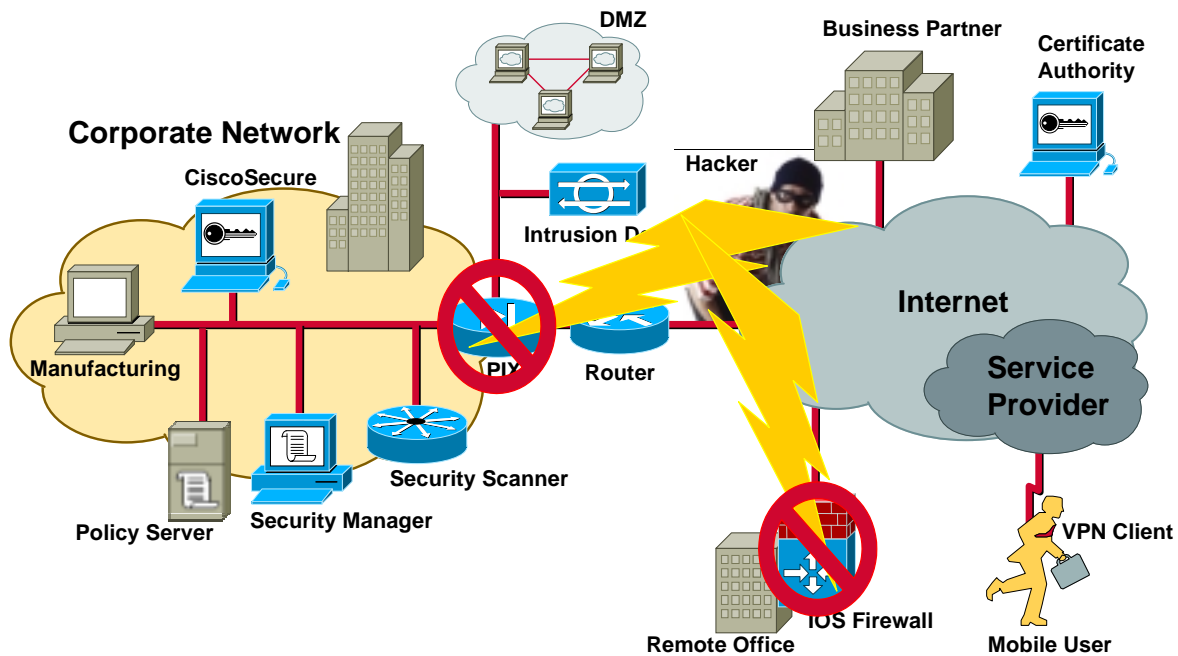


2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

28

# Secure VPN: Perimeter Security

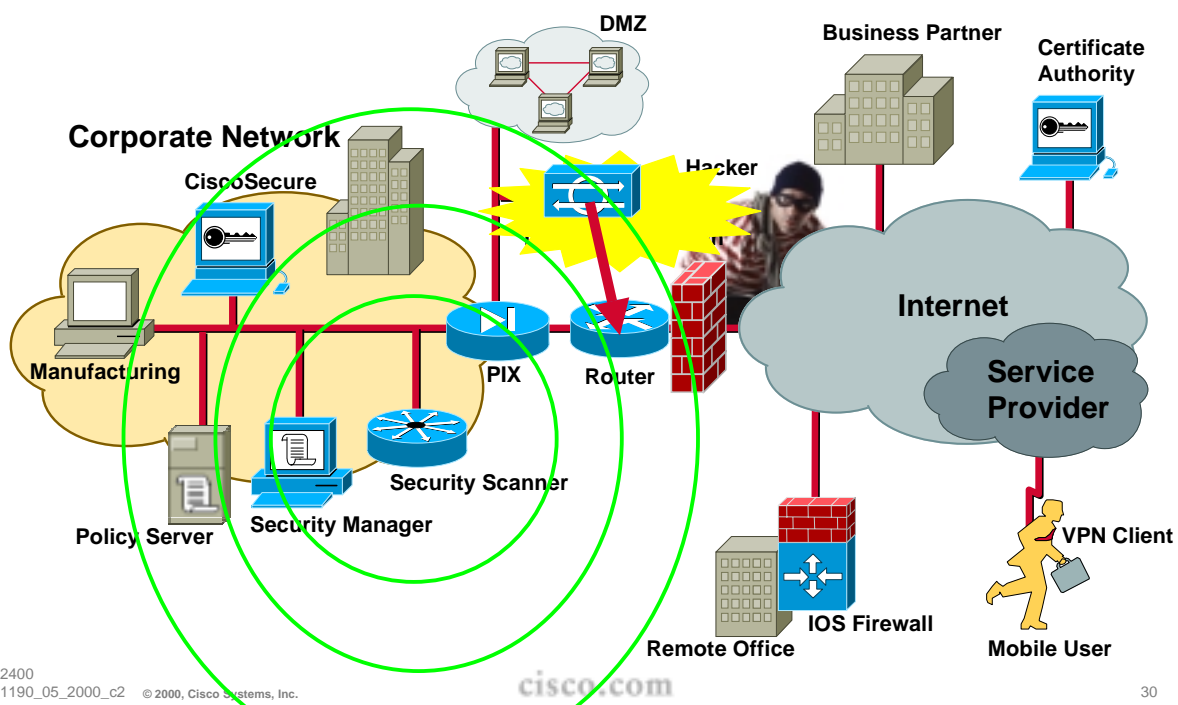


2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

29

# Secure VPN: Security Monitoring

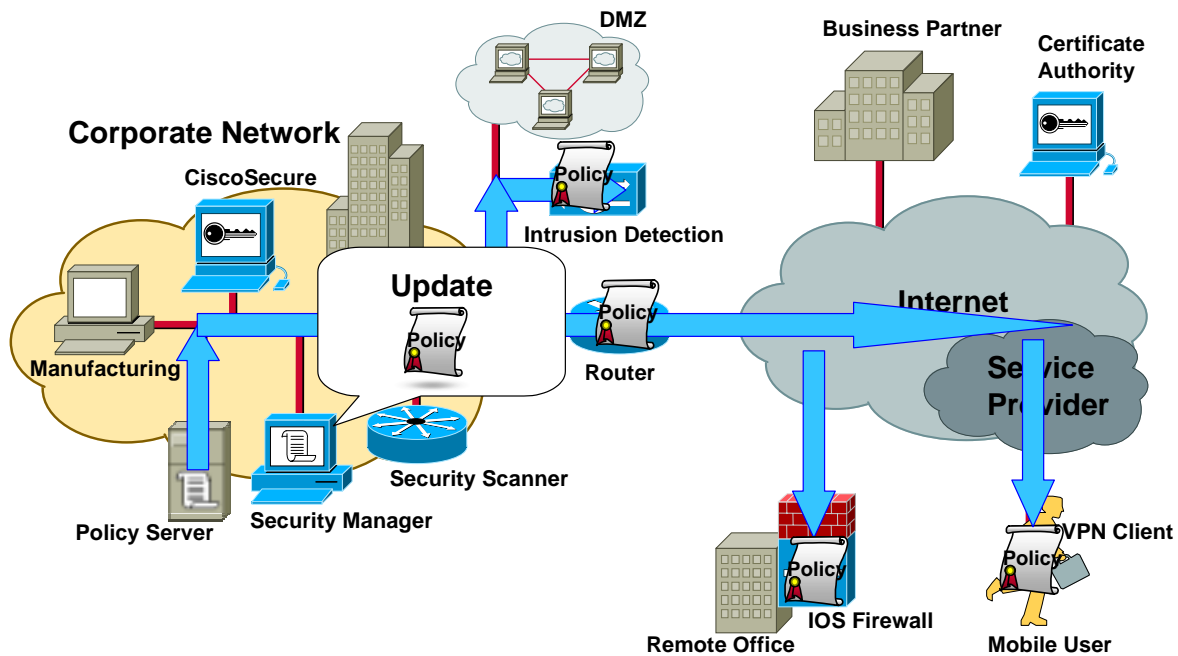


2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

30

# Secure VPN: Policy Management



2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

31

## E-VPN Platforms

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

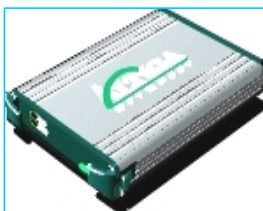
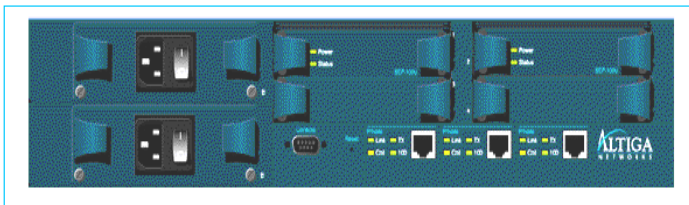
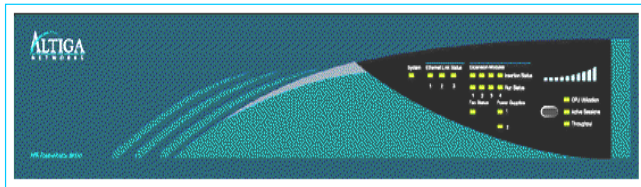
cisco.com

32



# Remote Access VPN

## Cisco VPN 3000 Concentrator Series



**Scalable  
Encryption  
Processor  
(SEP)**

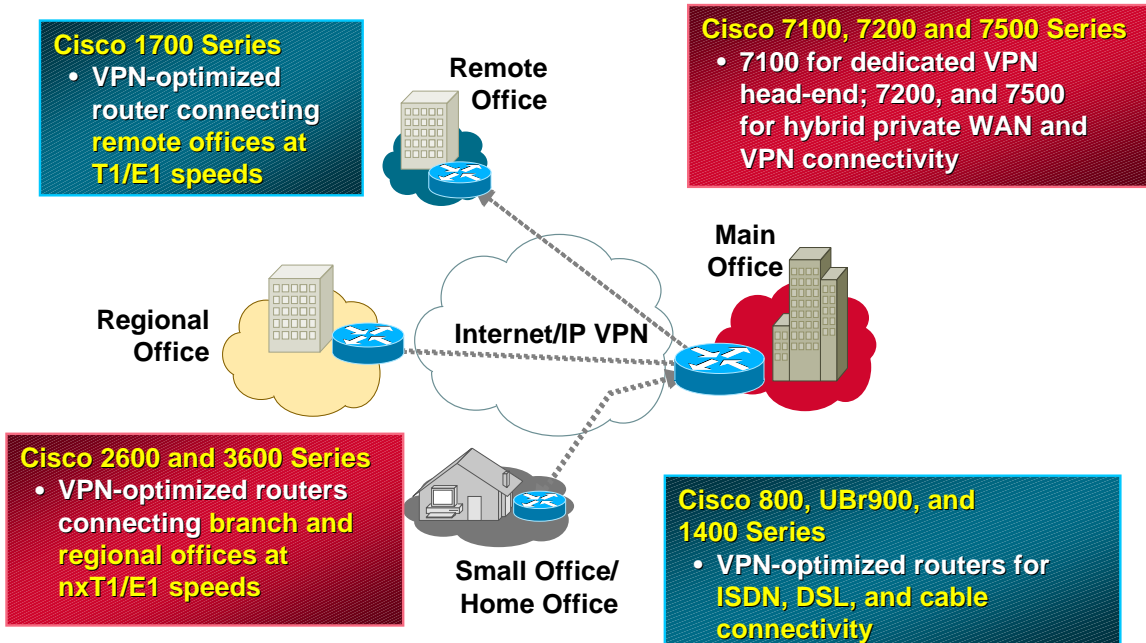
2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

33

# Cisco Site-to-Site VPN Solutions

## Scalability for Every Site



2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

34

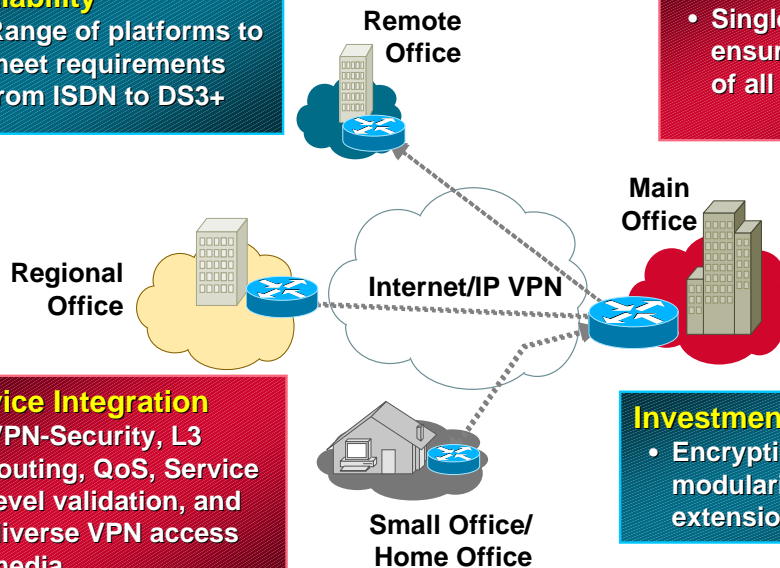
# Site-to-Site VPN Solutions

## Site-Specific Scalability

- Range of platforms to meet requirements from ISDN to DS3+

## Feature Interoperability

- Single device solution ensures interoperability of all VPN services



## Device Integration

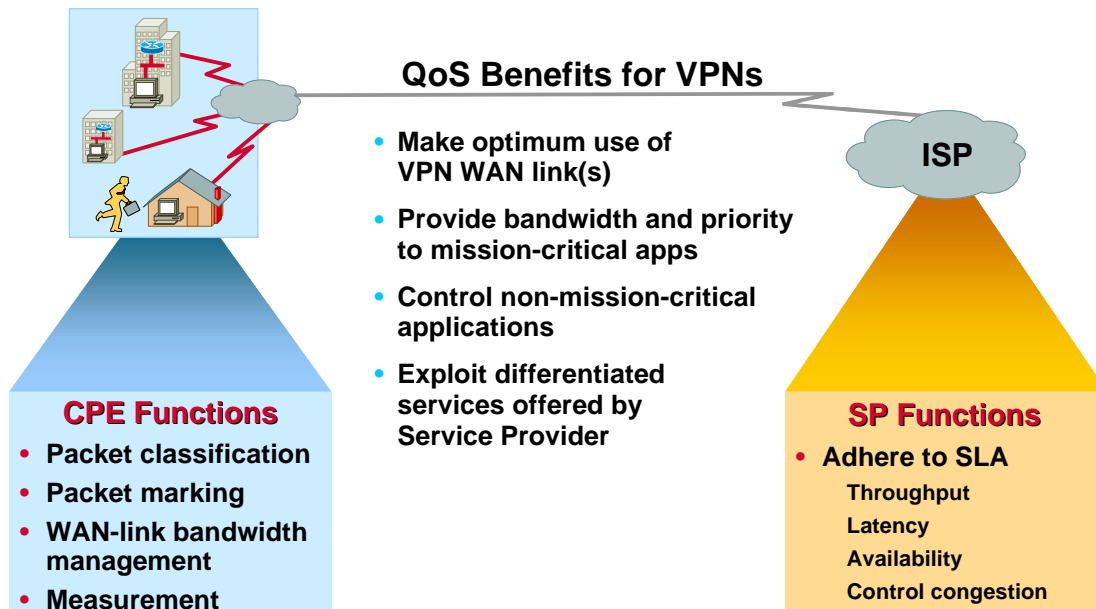
- VPN-Security, L3 routing, QoS, Service level validation, and diverse VPN access media

## Investment Protection

- Encryption acceleration modularity and software extensions

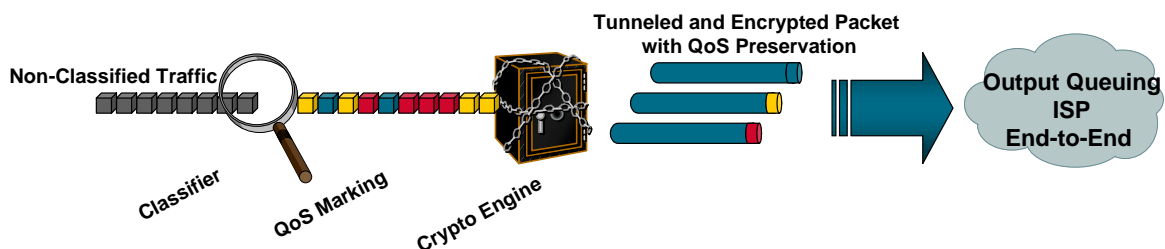
# E-VPN Services

# Quality of Service in a VPN



## IPSec TOS Preservation

- Enables classification for encrypted and tunneled VPNs
- Supports ISP Differentiated Services offerings
- Preserves QoS Signaling end-to-end





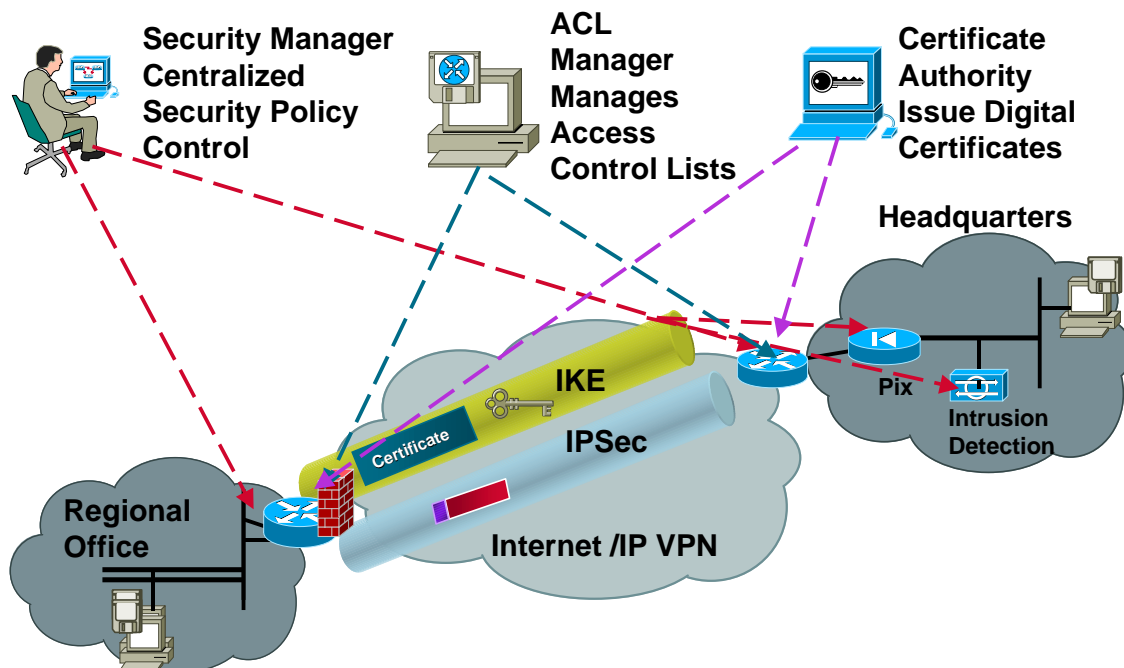
# E-VPN Management

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

39

## VPN Security Management



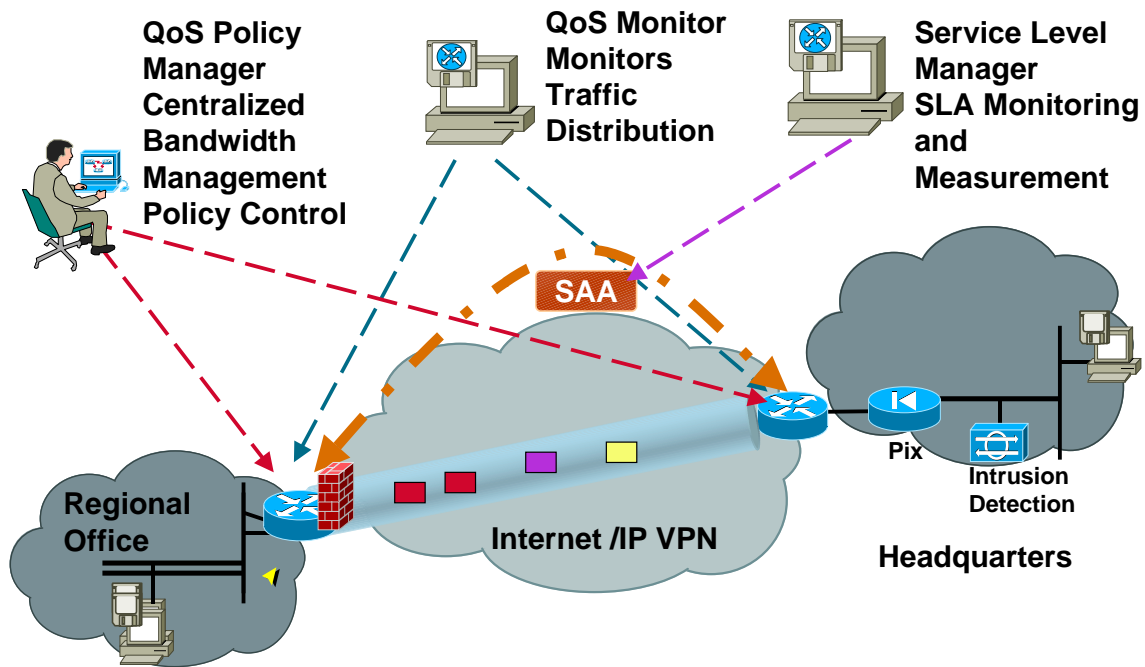
2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

40



# VPN Bandwidth Management



2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

41

## Next Steps

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

42

# Major VPN Challenges

- **Mobility**
- **Streaming services**
- **Voice, video, audio**
- **Scalable deployment**
- **Policy management**

## Non-Technology Challenges

**Role of  
Regulation**



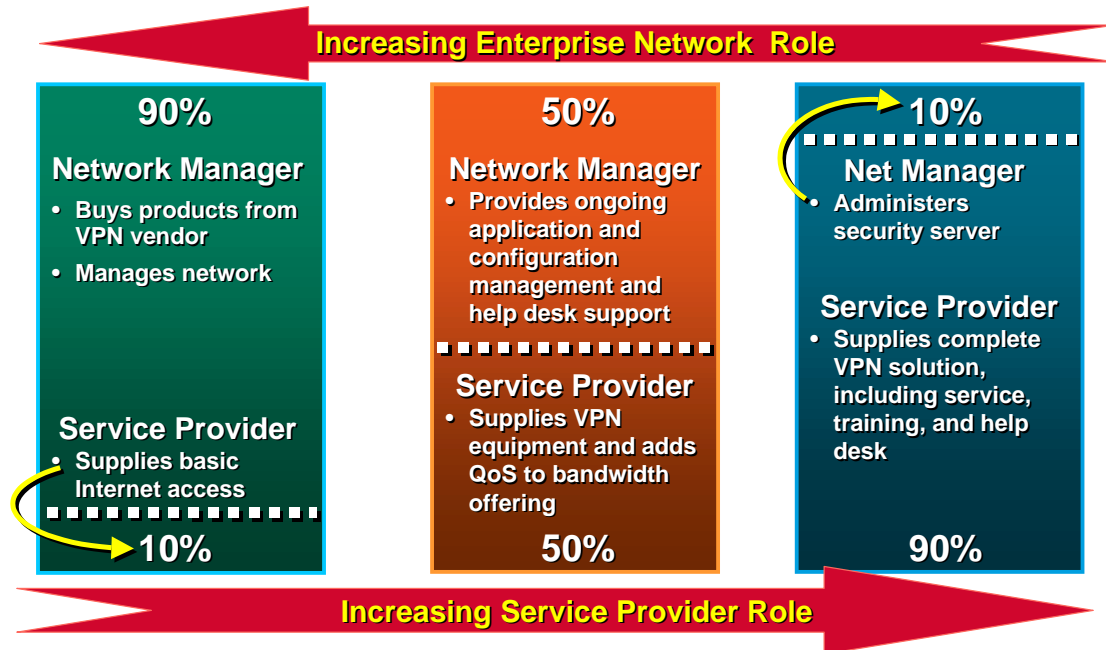
**Conflicting  
National  
Policies**



**Local Standards  
and Practices**



# VPN Deployment Options



## 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
<b>Totals:</b>	<b>\$2,907,000</b>	<b>\$1,800,000</b>	<b>\$1,107,000</b>
<b>Savings Based on VPN Solution (1000 Users)</b>			<b>38%</b>

\*Numbers are quoted on an annual basis for 1000 users.



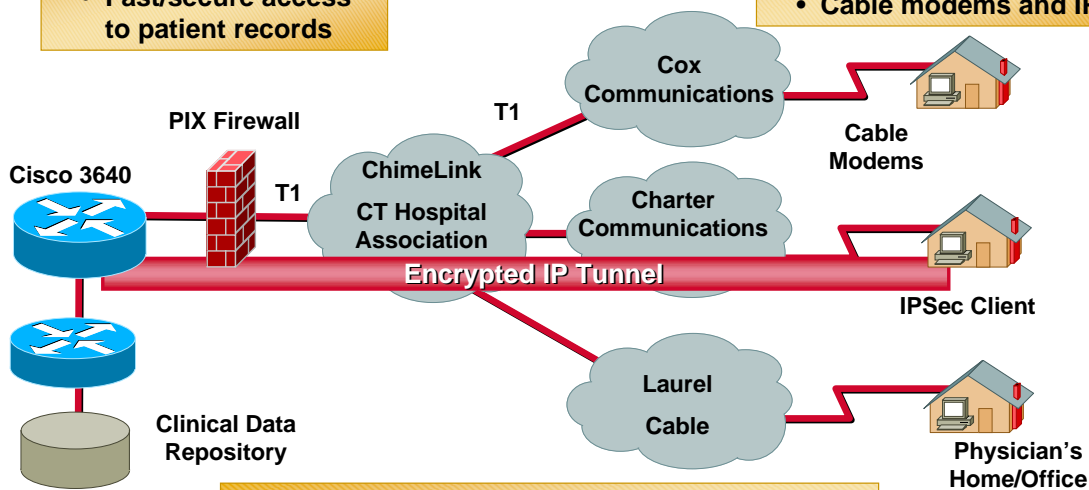
# Waterbury Hospital

## 1. Requirement

- Fast/secure access to patient records

## 2. Solution

- Extranet VPN Via
- Cable modems and IPSec



## 3. Benefit

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

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

47

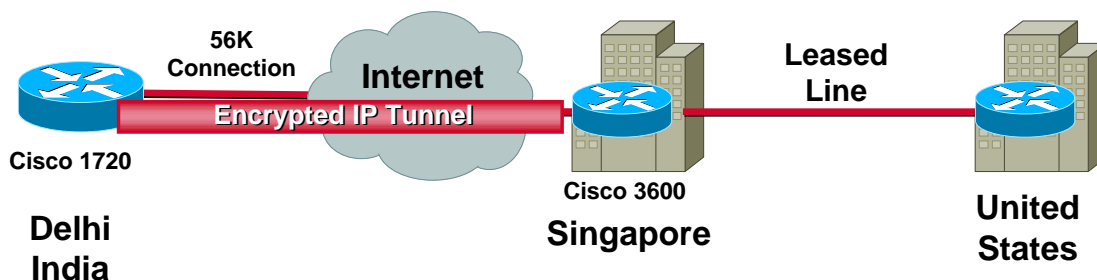
# Media Company

## 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



## 3. Benefit

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

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

48



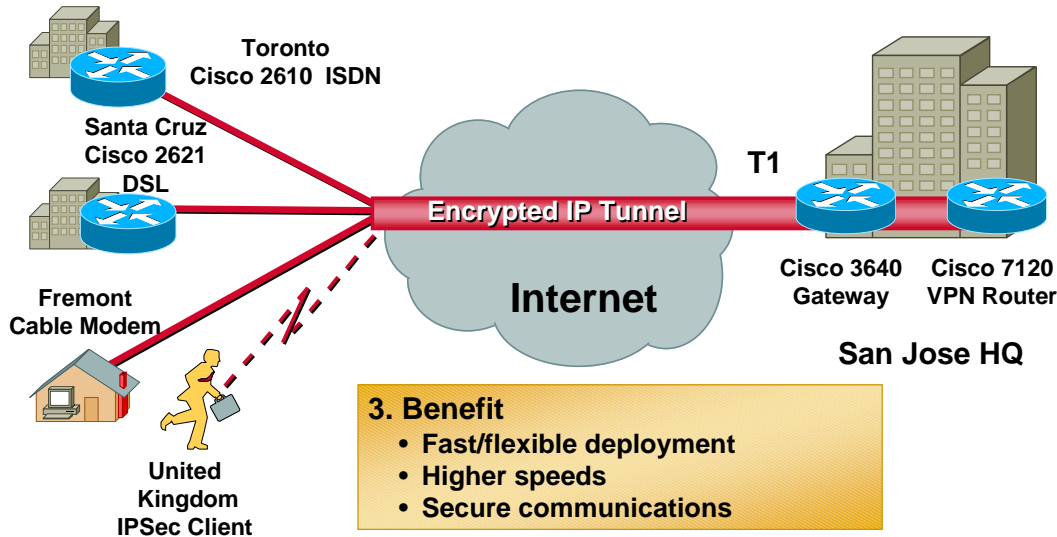
# Altera Semiconductor

## 1. Requirement

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

## 2. Solution

- Intranet and Remote Access
- VPN



## 3. Benefit

- Fast/flexible deployment
- Higher speeds
- Secure communications

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

49

# Additional Information

- [www.cisco.com/go/evpn](http://www.cisco.com/go/evpn)
- [www.cisco.com/go/security](http://www.cisco.com/go/security)
- [www.cisco.com/go/securityassociates](http://www.cisco.com/go/securityassociates)
- Networking Professionals Community

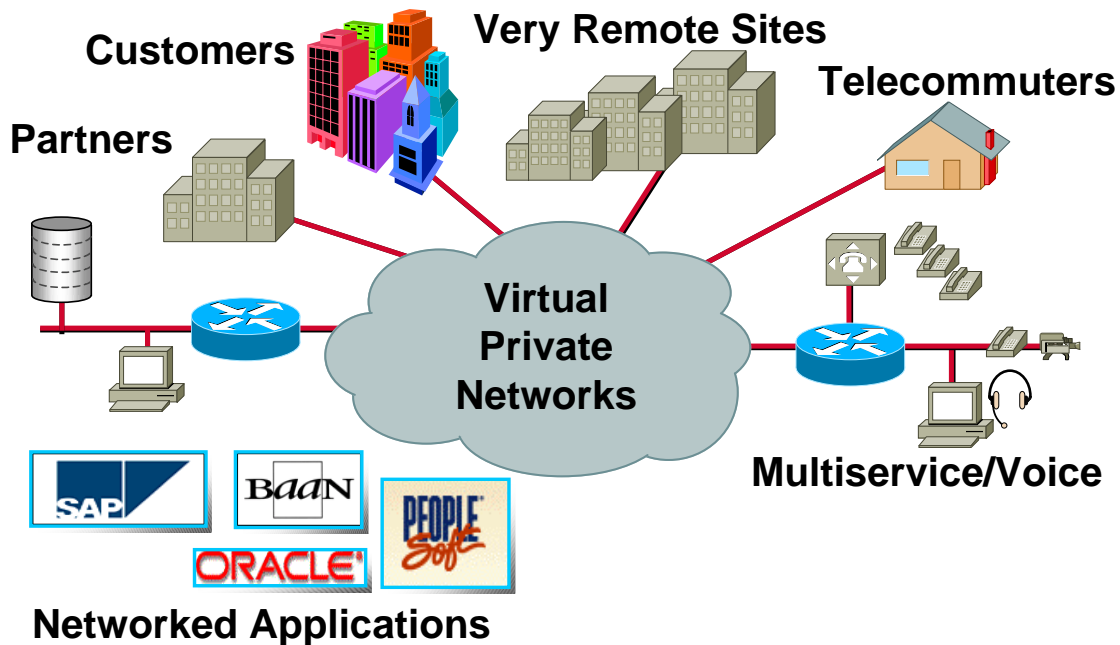
White Papers, ISPs with “Cisco Powered” VPN Services, Design Guides, Data Sheets, 3rd Party Solutions

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

50

# Are You Ready?



2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

cisco.com

51

## Introduction to VPNs

### Extending the Classic WAN

### Session 2400

2400  
1190\_05\_2000\_c2 © 1999, Cisco Systems, Inc.

cisco.com

52



# Please Complete Your Evaluation Form

## Session 2400

2400  
1190\_05\_2000\_c2 © 1999, Cisco Systems, Inc.

[cisco.com](http://cisco.com)

53

# CISCO SYSTEMS



## EMPOWERING THE INTERNET GENERATION<sup>SM</sup>

2400  
1190\_05\_2000\_c2 © 2000, Cisco Systems, Inc.

[cisco.com](http://cisco.com)

54