Introduction to VPNs
Extending the Classic WAN
Session 2400
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

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

Regional Office

Home Offices

Mobile Workers

Remote Office
Enabling the Internet Economy

Customers

Very Remote Sites

Partners

Telecommuters

Networked Applications

Enterprise WAN Connectivity

Multiservice/Voice

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

Extranet VPN
- Extends WANs to business partners
- Safe L3 security

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

Main Office
Main Office

Business Partner
Business Partner

Mobile Worker
Mobile Worker

Home Office
Home Office

POP
POP

Remote Office
Remote Office

VPN
VPN
VPN Applications and Requirements

Remote Access
- Extension of dial
- User manageable 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

- 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

- 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

Security: A Physical Analogy

- Security Office
- Guard
- Security Camera
- Traditional Locks
- Card Key
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

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**

```
| IP HDR | DATA |
```

```
<table>
<thead>
<tr>
<th>New IP HDR</th>
<th>IPSec HDR</th>
<th>IP HDR</th>
<th>DATA</th>
</tr>
</thead>
</table>
```

Encrypted

**Transport Mode**

```
| IP HDR | IPSec HDR | DATA |
```

```
| IP HDR | IPSec HDR | DATA |
```

Encrypted
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 inter-operates 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
Secure VPN: Identity

- Corporate Network
- CiscoSecure
- DMZ
- Business Partner
- Certificate Authority
- Internet
- Service Provider
- PIX
- Router
- Mobile User
- VPN Client
- Intrusion Detection
- Security Scanner
- Security Manager
- Policy Server
- Manufacturing
- Digital Certificate

Secure VPN: Data Privacy

- Corporate Network
- CiscoSecure
- DMZ
- Business Partner
- Certificate Authority
- Internet
- Service Provider
- PIX
- Router
- Mobile User
- VPN Client
- Intrusion Detection
- Security Scanner
- Security Manager
- Policy Server
- Manufacturing
- Digital Certificate
Secure VPN: Policy Management

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

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

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

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

Main Office
Remote Office
Regional Office
Internet/IP VPN
Small Office/Home Office
Site-to-Site VPN Solutions

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

**Remote Office**

**Regional Office**

**Internet/IP VPN**

**Small Office/ Home Office**

**Main Office**

**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

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

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

Non-Classified Traffic
Classifier
QoS Marking
Crypto Engine

Tunneled and Encrypted Packet with QoS Preservation

Output Queuing
ISP End-to-End
E-VPN Management

VPN Security Management

- Security Manager: Centralized Security Policy Control
- ACL Manager: Manages Access Control Lists
- Certificate Authority: Issue Digital Certificates
- Headquarters
- Regional Office
- Internet/IP VPN
- IPSec
- IKE
- Intrusion Detection
- PIX
- Certificate

ACL Manager

Security Manager

Centralized Security Policy Control

Manages Access Control Lists
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

**50% Network Manager**
- Provides ongoing application and configuration management and help desk support

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

**10% Net Manager**
- Administers security server

**Increasing Service Provider Role**
- **90%**
  - Service Provider supplies complete VPN solution, including service, training, and help desk

---

### Cost-Effectiveness of VPN Remote Access*

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

**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 Cox Endeavor Communicators and IPSec

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

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

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
Introduction to VPNs
Extending the Classic WAN
Session 2400
Please Complete Your Evaluation Form

Session 2400