So Your Customer Wants a VPN

Howard C. Berkowitz
Gett Communications
hcb@clark.net
(703)998-5819
Issues

• Understanding Requirements
• Managing Expectations
• Defining your Service
• Deployment Issues
Motivations
Customer Goals

- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money
- Saving money

- Enabling workforce distribution
- Building strategic alliances
- Improving operational flexibility
Customer Constraints

- Availability & Performance
- Security
- Compatibility
- Manageability
- Budget

Clue Factor
Common Customer Confusions

• VPN over IP = VPN over Internet
  – “whee! I can replace all my Frame Relay with $20 a month ISP connections!”

• VPN = “selling on the net”
  – Membership must be established before communication

• “The VPN does all my security”

• “I can get controlled QoS over the Internet”
Workforce Distribution

Telecommuter

Mobile User

Road Warrior

Satellite Office User

Source: Cisco University VPN Seminar
Special Challenges

• Voice
• Video
• Image retrieval
• Greater involvement with applications
High Speed Last Mile

• V.90, multiple modems (MLPPP)
• ISDN
• xDSL
• Fixed wireless
• Cable
• Fiber to the neighborhood/building
Network Commerce
Cost Savings

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>Cost Per Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>$0.80</td>
</tr>
<tr>
<td>Telephone</td>
<td>$0.40</td>
</tr>
<tr>
<td>ATM</td>
<td>$0.20</td>
</tr>
<tr>
<td>PC Banking</td>
<td>$0.00</td>
</tr>
<tr>
<td>Internet</td>
<td>$0.00</td>
</tr>
</tbody>
</table>

Department of Commerce, 5/98
Customer Financial Analysis
Cost Components

• Direct one-time costs
  – Access servers
  – Server routers
• Direct recurring costs
  – Dial charges
  – Line charges
  – Vendor support
• Indirect recurring costs
  – WAN Administrator time
  – Security/server administrator time
# Direct Cost Comparison

<table>
<thead>
<tr>
<th>Traditional Dial-Up</th>
<th>Access VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Set-up Costs</strong></td>
<td><strong>Number of Users</strong> 20</td>
</tr>
<tr>
<td>Number of Users</td>
<td><strong>Access Router, T1/E1, DSU/CSU, Firewall</strong> $4,600</td>
</tr>
<tr>
<td>Remote Access Server</td>
<td><strong>VPN Client Software</strong> $1,000 ($50 per user)</td>
</tr>
<tr>
<td>One-time-installation Fee—10 Phone Lines</td>
<td><strong>T1/E1 installation</strong> $5,000</td>
</tr>
<tr>
<td><strong>Recurring Costs</strong></td>
<td><strong>Central Site T1/E1</strong> $2,500</td>
</tr>
<tr>
<td>Monthly Long-Distance charges per minute $0.10</td>
<td><strong>Intranet Access</strong></td>
</tr>
<tr>
<td>Average use Per Day Per User in Minutes 90</td>
<td><strong>Monthly ISP access</strong> $400 ($20 per user)</td>
</tr>
</tbody>
</table>

Source: Cisco University VPN Seminar
Payback in Four Months!

- Payback: 4 months
- Annual savings: $30,000
- Capital outlay: $10,600

Source: Cisco University VPN Seminar
VPN Outsourcing Options

Increasing Enterprise Network Role

90%
Network Manager
Buys Products from
VPN Vendors and
Manages Network

SP Supplies
Basic Internet
Access

10%

50%
Network Manager
Provides Ongoing
Application and
Configuration
Management and Help
Desk Support

SP Supplies VPN
Equipment and Adds
QoS to Bandwidth
Offering

50%

10%
Net Manager
Administers
Security Server

SP Supplies Complete
VPN Solution, including Service,
Training, and Help
Desk

90%

Increasing Service Provider Role

Infonetics, 1997
Defining VPNs
What is it?

• 3Com white paper
  – "A VPN is a connection that has the appearance and many of the advantages of a dedicated link but occurs over a shared network." VPNs use tunneling
What is it?

• Ascend (3 related architectures)
  – Virtual Private Remote Networking (VPRN) with tunneling for remote LAN access
  – Virtual Private Trunking (VPT) to establish the equivalent of leased lines among major facilities
  – Virtual IP Routing (VIPR) to internetwork branch offices or establish extranets with closed user groups
What is it?

• Cisco
  – Customer connectivity deployed on a shared infrastructure with the same policies as a private network

• Ferguson & Huston
  – “A VPN is a private network constructed within a public network infrastructure, such as the global Internet.”
What is it?

• Infonetics
  – “VPNs use public networks to extend the reach of the enterprise network to remote sites, individual remote workers, and business partners.”

• V--One
  – "the security technology that will enable companies to leverage the Internet as private enterprise backbone infrastructure."
IETF Work

• No WG yet. BOF last met in Orlando (December)
• Many working drafts at http://www.ietf.org/internet-drafts/xxx
  – draft-gleeson-vpn-framework-01.txt
  – draft-rosen-bgp-mpls-0x.txt
  – draft-berkowitz-vpn-tax-00.txt
  – draft-fox-vpnid-00.txt
Scope and Function

Source: VPNet Technologies [http://www.vpn.com/services/vpnsure.htm]
More Formally, a VPN has...

- Core User Capabilities
- Optional user capabilities
- Administrative model
- Mapping methods
- Transmission infrastructure
Core User Capabilities

• User Scope
  – Intranet via provider
  – Extranet via provider
  – Hybrid/bypass
• Set of users and servers
• Security policy
• Availability policy
• Addressing & Naming Model
• VPN ID (which may be null)
Optional User Capabilities

- Security mechanisms
- QoS Mechanisms
- Billing
- Addressing & naming services
- Non-IP support
Operational Model

• Responsibility for premises routers
  – WAN
  – LAN
• Responsibility for user support
• Responsibility for security
• Responsibility for QoS

• Help desk
• Adds and changes
• QoS
  – Engineering
  – Measurement
  – Compliance
• Security
  – Policy
  – Enforcement
  – Response to events
Mapping Functions

- Tunnels
- Virtual circuits
- Real on-demand circuits
- Real dedicated lines
Transmission Infrastructures

- Dial networks
  - local loop alternatives: xDSL, cable, etc
- Frame relay, ATM, other VC services
- Routed IP clouds
- MPLS
- Dedicated lines
- RFC 1149
Core Capabilities
Membership

• Has to be defined by customer
• Endpoint may belong to:
  – More than one VPN
    • Intranet
    • Extranet
  – Public Internet
• Provider has to track multiple VPNs
Security Policy (distinct from plan)

• Who is authorized to use what
  – Time of day, other qualifiers

• Kinds of users
  – Operations, inside, partners, public

• Enforcement policy
  – Something backed by top management

• Good policy is 1-2 pages
A Secure Communication may have:

- **Authenticity**
  - User/client, server

- **Integrity**
  - Unitary vs. sequential
  - Non-Repudiation

- **Confidentiality**
  - Lightweight, middleweight, strong

- **Availability**
  - Network failures, denial of service attacks
Addressing & Naming Model

• Issues
  – Private vs. public space
  – PI vs PA
  – Multihomed routing
  – Routing registries
  – NAT
    • Application transparency
    • End-to-end assumption traceability
  – Other addressing & naming manipulation
NHS Architecture

Customer Core

Frame Relay Core VCs

VPN

Network Mgt

Customer Distribution

Data Ctr

ISP 1

ISP 2

Clinic

Data Ctr Local

Trans.

Clinic address space

may be private or registered

registered

Arbitrary registered space -- transcriptionist addresses
Clinic Site

ISP Access

Router

NAT

Frame

IPsec 3DES

Dial/ISDN Interface

Voice Server

Printer

Management Port

Switch

Clinic network

PC

Clinic Network
Non-IP Services

• Issues
  – Does the ISP really understand these?
  – Transition planning
  – Performance expectations
Trust Models

- End-to-end
- Security gateway
- ISP-centric
Application Models
# Access VPN

<table>
<thead>
<tr>
<th>Core</th>
<th>Central Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VPN Service</strong></td>
<td></td>
</tr>
<tr>
<td>Remote Users</td>
<td>Central Site Clients</td>
</tr>
</tbody>
</table>

5/22/1999 5:55 PM
VPN Distribution Tier

- Internet Router
- Provider Network
- Network Access Servers
- VPN Router
- Access Control
# Dual VPN access

<table>
<thead>
<tr>
<th>Core</th>
<th>Internet Access</th>
<th>VPN Service</th>
<th>Central Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Remote Users</td>
<td></td>
<td>Central Site Clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Central Servers</td>
</tr>
</tbody>
</table>
VPN service organization

Ent. 1

Ent. 2

Ent. 3

Ent. 4

Service Organization
Hybrid VP N

Ent. 1

Ent. 2

Ent. 3

Ent. 4

Service Organization
VPN bypass

Ent. 1

Ent. 2

Ent. 3

Ent. 4

Service Organization
Need for Policy Routing

Ent. 1

Ent. 2

Ent. 3

Ent. 4

Service Organization
Optional User Capabilities
Security Services

• Components
  – Host
  – Customer firewall
  – Network
  – Service provider firewall
  – Certificate Authority
  – Identification servers
  – Log servers

• Activities
  – User IDs
  – Certificates
  – Key management
  – Attack detection
  – Attack response
Who is Responsible?

- User identification & authorization
  - Password/key management
  - Per-user access lists
- End-to-end encryption
  - Client distribution
  - Key management
- Network security
  - Customer routers/firewalls
  - Provider devices
  - Key management
  - Intrusion detection & response
Encryption Performance Tradeoffs

• Clients
  – IPsec
  – SOCKS/SSL

• Application Servers
  – Software encryption
  – Coprocessor

• Router
  – Software encryption
  – Coprocessor

• Encryption server
• Firewall
• Access server
  – Proxy
  – L2TP + IPsec

• Keys
  – Key size
  – Pregeneration
  – Change frequency
  – Revocation
QoS Deployment

• Prerequisites
  – Policy
  – Means of identifying and marking priority traffic
  – Workload assumptions

• KISS mechanisms
  – Dedicated media
  – VCs with good SLA

• Advanced
  – RSVP
  – WFQ, WRED, etc.

• Bleeding edge
  – Multiprovider QoS
Addressing & Naming Services

• Mechanisms
  – DNS
    • inside & outside?
    • who runs?
  – Dynamic addressing
    • DHCP inside
    • PPP (static inside, NAS pools, AAA server, DHCP proxy)
  – Address management for infrastructure
  – Addressing & Naming Manipulation
    • Caches, load-sharing mechanisms
Non-IP services

• Mechanisms
  – Tunneling
  – Translation
  – Proxies
Operational Responsibilities
Control Points

• Customer router
• ISP router at customer site
• NAS
Help Desks

• Customer-operated single point
• ISP-operated single point
• Separate network & application
Adds, Moves, & Changes

• Models
  – User to ISP
  – Customer admin to ISP

• Coordination between customer and ISP
Mapping Functions & the User
NATs and Proxies

Application Caches

Load Sharing NAT

PAT/NAPT

Classic NAT

Load Aware DNS

Content-Aware Proxy

Traffic-Aware Proxy

Application Proxy

Circuit Proxy

Stateful Packet Filter

Packet Filter

Frame Filter

IPsec

Tunneling
What has to happen?

<table>
<thead>
<tr>
<th>Application Data</th>
<th>Transport Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Data</td>
<td>Transport Checksum</td>
</tr>
<tr>
<td>Source Port</td>
<td>Dest. Port</td>
</tr>
<tr>
<td>IP Checksum</td>
<td>Source Address</td>
</tr>
<tr>
<td></td>
<td>Dest. Address</td>
</tr>
</tbody>
</table>

NAT

<table>
<thead>
<tr>
<th>Application Data</th>
<th>Transport Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Checksum</td>
<td></td>
</tr>
<tr>
<td>Source Port</td>
<td>Dest. Port</td>
</tr>
<tr>
<td>IP Checksum</td>
<td>Source Address</td>
</tr>
<tr>
<td></td>
<td>Dest. Address</td>
</tr>
</tbody>
</table>
Layer 3/4 Tunnels

- IPsec (provides security)
- GRE (carries security or runs over trusted network)
  - PPTP
  - X9.17, etc.
  - Host IPsec with bogus addresses
  - Other encryption
Layer 2 Tunnels

- Proxy remote access service
- Upper layer protocol independent
- Potential for roaming
**Basic Tunnel**

![Diagram of Basic Tunnel]

- **Payload packet**
- **Layer 2 Of payload**
- **Tunnel header**
- **Delivery**

Present only when tunneling nonroutable protocols.
Tunneling Traceroute
Tunneling MTU Issues

Host
(MTU=1500)

Payload packet

Ingress Router
(all interfaces MTU=1500)

Tunnel header +8

Delivery +20
Secure Paths

- Multiplexed
- Routed
- Encrypted

<table>
<thead>
<tr>
<th>Trusted provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Untrusted provider</td>
</tr>
</tbody>
</table>
IPsec scope

- End-to-end
- Gateway-to-Gateway
- Host-to-Gateway
- Host-to-Gateway
IPsec packets

Tunnel Mode

Transport

IPsec Processing

Payload

AH/ESP

Payload

AH/ESP

Payload

5/22/1999 5:55 PM
Combined Tunnels--ISP security
Combined Tunnels -- user security

[Diagram showing user security with IPsec and L2TP]
Transmission Infrastructure Constraints
Basic Criteria

• Adequate bandwidth?
  – Dedicated
  – On-Demand

• Trust?
Additional Criteria

• Fault tolerance

• Quality of Service
  – Service contract (ATM)
  – Dedicated facility
  – Traffic engineered routing
    • RSVP
    • Emerging QOSR
Routed Infrastructure

• Convergence
• Policy/special considerations
• Inter-provider coordination
**Conclusions**

- **VPNs are a valuable approach to design**
  - Even if we aren’t quite sure what they are

- **Challenges for ISPs**
  - Understanding customer
    - requirements
    - perceptions and beliefs
  - Managing expectations & responsibilities
  - Use deployable technologies