Virtual Private Networks (VPN)
MacWorld/Pro Conference
VPN Buyers Guide

Bill Vlahos
Network Services Engineer
OAO Corporation contracted to Jet Propulsion Laboratory
July 22, 1999

Objectives

- What is Remote Access?
- What is a VPN?
- Why do I want it?
- How do I choose it?
- When can I use it?
- Opportunities to lead using Macs
  - Most common VPN is Microsoft's built-in
**Introduction to Remote Access**

- Current situation
  - Dial up 56k v.90 or 128k ISDN
    - Multi-protocol
  - IP via Internet
    - IP only
    - IP address restriction on web & ftp servers
    - Clear text with little encryption

**Technology Direction**

- WEB and FTP information dissemination everywhere
- ISP services commonplace (with features you can't provide)
  - High Speed Internet services available
  - Wireless Internet access
  - International ISP services available
- Corporate business on web
  - Timecards
  - Order processing
- Off-site people
  - Telecommuters
  - Customers
  - Contractors

![Cable Modem vs Analog Modem Chart]
What is a VPN?

High-speed, secure, controlled connections from anywhere!

- Three forms
  - Client to server
    - Software solution plus authentication (often local)
  - Client to network (gateway)
    - Client software gateway software or hardware plus authentication server
  - Network to network (Gateway-gateway or LAN-LAN)
    - Hardware solution for stability and performance
Which type of VPN?

- Client-server
  - Complete encryption end to end
  - Doesn’t scale easily/how do you authenticate users
  - Performance and security issues
- Client-network
  - High performance
  - Scalable (can leverage existing infrastructure)
  - Requires client software
- Network-network
  - No client requirements (support all platforms)
  - Doesn’t go everywhere

The 3 Components of a VPN
Focus on Client-network

- VPN Gateway
  - External interface (IPSec only)
  - Internal interface (multi-protocol inside Company network)
- Authentication Server
- Client software
Features & Options

- Authentication Servers
  - RADIUS
  - TACACS
  - SecureID Card
  - PKI
- Type of Gateway
  - Appliance Box
  - Software application
- Performance Expectations
  - Simultaneous connections
  - Network throughput

Standards
- PPTP (Microsoft)
- L2TP (Microsoft & Cisco)
- IPSec (Ratified standard)

Services
- IP
- AppleTalk
- IPX
- NAT (Network Address Translation)
- Encryption levels (DES, 3DES, etc)

Macintosh Supported Vendors

<table>
<thead>
<tr>
<th>Vendor (Alphabetical)</th>
<th>IKE</th>
<th>SSL</th>
<th>RADIUS</th>
<th>PPTP</th>
<th>L2TP</th>
<th>IPSec</th>
<th>Vendor Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>AltairVista Tunnel/Compaq</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>S/W Unknown</td>
</tr>
<tr>
<td>Bay Networks/Novell</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Box User NTS Client</td>
</tr>
<tr>
<td>Cisco Systems</td>
<td>Yes</td>
<td>Yes</td>
<td>?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Both Uses Network Associates client</td>
</tr>
<tr>
<td>Compatible Systems</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Box Gateways some. Clients Limited</td>
</tr>
<tr>
<td>Internet Express</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>S/W No</td>
</tr>
<tr>
<td>Ifass</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Microsoft</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>S/W</td>
<td>Can use NTS client</td>
</tr>
<tr>
<td>Network Associates/PGPnet</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>S/W</td>
<td>Yes</td>
<td>S/W Yes</td>
</tr>
<tr>
<td>Network TeleSystems/NTS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Both Yes</td>
</tr>
<tr>
<td>Novell</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>S/W</td>
<td>No</td>
<td>S/W No</td>
</tr>
<tr>
<td>T FOREST</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Box</td>
<td>Some</td>
</tr>
<tr>
<td>V ONE</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>S/W</td>
<td></td>
</tr>
</tbody>
</table>

*Planned
Contacting Vendors

AltaVista Tunnel /Compaq http://altavista.software.digital.com/tunnel/
Bay Networks/NorTel http://www.nortelnetworks.com
Cisco Systems http://www.cisco.com
Compatible Systems http://www.compatible.com
InfoExpress http://www.infonet.com
*i Pass http://www.centralhouse.com/ippass/service_overview.html
Network Associates(PGPnet) http://www.nai.com/
PGPnet from MIT (Freeware) http://web.mit.edu/network/pgp.html
Network TeleSystems(NTS) http://www.nts.com/
TimeStep http://www.timeset.com
V-ONE http://www.v-one.com/smargate.htm

Authentication Servers

- MacRADIUS http://www.cyno.com
  - IETF Standards based RADIUS (Remote Authentication Dial-in User Service) server with extensive AppleScript support.
- HandyTACACS http://www.arithmetic.ch/HandyTacacs/index.shtml
  - TACACS (Terminal Access Controller Access Control System)
- Accounts on the Gateway
  - Not scalable
- Public Key Infrastructure (PKI) - not Mac based
  - Entrust http://www.entrust.com/
  - Verisign http://www.verisign.com/
  - x.509 Certificates
Sample Requirements for VPNs
your mileage may vary

- Encryption (IPSec)
- smart tunnel (appropriate use)
- NAT (Network Address Translation)
- log source and NAT IP addresses
- log traffic indicator
- RADRS
- IKE/PKI Enroll (in future)
- Y2K
- Encryption key rotation
- IP
- AppleTalk
- IPX
- failover & redundancy

- Connection (Client gateway, gateway, gateway at edge of intranet)
- Maj. Wintel/NT
- client sw exportable
- application independent
- 500 simultaneous connections
- 27 Mbps throughput
- load balancing
- password protected
- Console port protected
- passwords changeable
- NSP monitoring
- vendor replacement

Cost per user for 3 years

VPN Cost per User Comparison

Users Supported

- Client/Server
- Client/Server
- Client/Server
- Client/Server
- ISP (9 Speed)
- [Typical network (20 users/week)]
- [LAN/VPN (20 users/week)]
- [Commercial VPN (VPN subscriber model) (20 users/week)]
- [ISP Provider Network]
**Client-Gateway VPN**

- **Advantages**
  - All network services automatically protected
  - Ubiquitous Internet access
  - ISP & technology independent
  - Traffic is encrypted before it leaves computer
  - User is authenticated at connection time
  - Smart tunnel feature assures “appropriate usage”
  - Standards based (IPSec)
  - Leverage current infrastructure (authentication, etc.)
  - No changes to existing services

- **Disadvantages**
  - Software installed on remote client computer

---

**Gateway-Gateway VPN**

- **Advantages**
  - Does not require client installs on remote computers
  - Supports all computer platforms
  - ISP independent. Gateway(s) can be anywhere on the Internet
  - Smart tunnel feature assures “appropriate usage”
  - “Always-on” connection

- **Disadvantages**
  - Difficult to control who is on the remote network
So does it work?

- Yes!
- How well do you ask?...

VPN Performance Impact
High-speed cable modem

- We expected to see some degradation but did not find any.
VPN Performance Impact
Analog Modems

- Good line conditions
  Small penalty (17%)

- Poor line conditions
  No consistent penalty

Challenges for deployment

- Remote site firewalls
- Support of computers owned by other institutions
- Who will support outside users
- IPSec ratified Nov. '98. Will take time to stabilize
- Cross-vendor compatibility not good
Additional Information

- IPSec (IPSec) RFC 2409 (IKE (Internet Key Exchange)) and RFC 2407 (ISAKMP (Internet Security Association and Key Management Protocol)).
  http://www.ietf.org/html.charters/ipsec-charter.html
- RADIUS (Remote Authentication Dial In User Service) RFC 2058 (Authentication) and RFC 2059 (Accounting)
- My email address: bvlahos@jpl.nasa.gov