Choosing a Virtual Private Network (VPN) Service Provider

Choosing a Virtual Private Network (VPN) Service Provider

Internet Virtual Private Networks (VPNs) offer enormous opportunities for any company looking to realize the Internet's economies of scale and global access, while maintaining the security of a private network. With a VPN, users can send and receive sensitive, business-critical data across the Internet, and feel confident that it will travel securely, unseen, unchanged, and intact. At the same time, VPNs are quick to set up and tear down, and accessible from anywhere in the world. As a result, VPNs are ideal for: 1) extranet applications, where they can enable on-demand, high-speed communications on a worldwide basis; 2) intranets, offering expanded deployment options; and 3) remote access for corporate users, where VPNs provide access to an organization's network over the Internet with just a local phone call to an ISP, thus providing dramatic cost advantages.

Although there is currently a lot of "buzz" about VPNs, they are actually not new at all. The first packet network VPN was created in 1975, when BBN Corporation, now known as GTE Internetworking, delivered the Private Line Interface (PLI) packet encryption devices used by the U.S. Navy to deploy a VPN for transmitting classified data over the ARPANET. More recently, with the explosive growth of the public Internet and increasing interest in linking critical business applications to the Web, the market for Internet VPNs has begun to grow dramatically, as vendors bringing varied technologies and resources have entered the scene. In fact, Frost & Sullivan predicts that IP-based VPN services will have a compounded annual growth rate of 87.7 percent between 1997 and 2004, achieving revenues of $13.59B in 2004.[1]

The good news is that enormous resources and talent are being dedicated to improving the security, service, and management of VPNs, resulting in more choices for customers. At the same time, the proliferation of vendors in the marketplace is creating an environment filled with hype and vendor value propositions that are so similar users can hardly tell them apart. Nowhere is this more apparent than among ISPs and carriers looking to provide managed VPN services to their customers. And the stakes are high for prospective users. According to Infonetics President Michael Howard, "VPNs are ultimately about partnerships, and the most important VPN partnership for many organizations will be the one they establish with their service provider."[2] Ideally, service providers should be well positioned to help customers eliminate technology risk, function as security and network experts, and ensure implementation success through their market experience and consulting/systems integration expertise. But they're not all the same!

How Do You Pick a Service Provider with Whom You Can Partner?

The reality is that it is difficult to pick a VPN service provider. Many service providers are new to Internet security, which is widely reported to be the key issue for corporate buyers and, according to GIGA Information Group, the number one most important VPN evaluation criterion.[3]

When it comes to security, most VPN providers are not yet offering the state of the art. For example, most are not yet using the latest hardware-based encryption devices, capable of encrypting and decrypting data faster and more reliably than software-based encryption. Few can provide digital certificates as part of their offering, a critical component for companies that need to have the highest level of assurance that senders and receivers are who they say they are. And most cannot combine these types of leading-edge security capabilities with equally high marks for business quality performance and reliability, as well as proven network management and monitoring. This white paper examines the criteria organizations should consider when making a VPN buying decision among a wide array of choices in this dynamic environment.

---

1 "U.S. Virtual Private Network Markets," Frost & Sullivan, 1998.

2 "Virtual Private Networks: A Partnership Between Service Providers and Network Managers," Infonetics Research Inc., 1997.

3 "Criteria for Evaluating Managed Internet-based VPN Providers," Giga Information Group Inc., 1998.

Outsourcing Is a Trusted Partnership

The traditional argument for outsourcing VPNs is well-documented, stemming from the common realities inside growth companies: the need for speed to market; a scarcity of internal labor resources and knowledge; the lack of experience deploying VPNs; a reluctance on the part of most companies to make significant capital investments in dynamically changing technologies; and the requirement for constant improvements in security, service, and support. Of course, the bottom-line reason for outsourcing VPNs is cost savings, made possible by the economies of scale enjoyed by service providers. But such factors in favor of outsourcing your VPN to a service provider are claims that can be made by all service providers. The key question then becomes, What separates the contenders from the pretenders — what critical features will transform your VPN initiative from an outsourced alternative to a trusted partnership? You can gain a foundation for valuable insights into your VPN provider by focusing your rigorous evaluation on five key categories:

- Security
- Performance/reliability
- Management and monitoring
- Consulting and integration services
- Provider stability and reach

Security Is Job One

How important is security to your company? For most companies looking to the Internet to deploy business applications, this is the fundamental issue. Many organizations cite security as the single greatest barrier to connecting with customers and partners over the Internet. Whether you're dealing with very valuable and sensitive data, or you just don't want to have people coming over the Internet to your internal servers, chances are you would not be considering a VPN if security were not of paramount importance, now or in the future. Certainly, as private intranet data merges with the world of e-commerce, security decisions will only become more challenging. This means you must first evaluate VPN providers on their ability to handle the security challenge.

The reality is, security expertise is a weak point for most VPN service providers. While a small number of service providers can claim years of security and networking experience, few can point to real-world applications for the world's most security-conscious users, such as banks and credit card companies or the government. Few will a have a track record in conducting security audits and developing and managing security policies and procedures. Most VPN providers cannot show how the products and services they utilize have been built from the ground up with security in mind, rather than having security bolted on as an extension. You can reduce a long list of potential partners to a short one by evaluating VPN service security based on four questions:

- What kind of security model is used?
- Which types of security standards does the service provider support?
- What kind of authentication does the service use?
- What kind of cryptography, if any, is employed?

Trust Is in the Security Model

VPN architectures differ widely, based on a few basic security models. Ask your potential partner which model they employ and whether data is ever in the clear or available to be tapped by outsiders. "In the cloud" security models encrypt data only when it is traveling on your provider's backbone, so that all local loop traffic is in the clear. POP to LAN security encrypts data at the ISP's POP and terminates at your premises, but the data is in the clear when traveling from the mobile user's desktop over PSTN line to the local POP. Finally, some vendors do not use encryption at all, instead employing closed user group schemes, which offer no data confidentiality, can be difficult to administer, and do not scale well.

What to look for: Only end-to-end security will provide true data protection. End-to-end privacy ensures that data is encrypted all the way from the mobile desktop or LAN through the "cloud," and back into the destination LAN. You need a managed VPN service that will provide this kind of robust security.

Security Interoperability: IPsec Required

There are many security protocols being used in VPN service implementations. It is important to understand what protocols are supported and what the issues are with some of these protocols. Many services support the Point-to-Point-Tunneling Protocol (PPTP). PPTP is integrated into Microsoft Dial Up Networking in Windows, but there are some significant security concerns associated with Microsoft's implementation of PPTP, from weak password-hashing algorithms to a design

flaw that can allow an attacker to masquerade as the PPTP server. Other services, particularly those that are router-based, use Layer 2 Forwarding (L2F). You should know that this protocol is being replaced by Layer 2 Tunneling Protocol (L2TP). L2TP has native multi-protocol support, but it has significant security weaknesses, such as weak data authentication, data integrity problems, and a lack of key management. In fact, L2TP is now looking to incorporate IPsec to address many of its security deficiencies.

What to look for: You need a VPN service that is in full IPsec compliance. IPsec is an IETF, open industry-supported standard. Adopting an IPsec-compliant VPN service will ensure interoperability as your network continues to expand.

Advanced Authentication: Experienced Certificate Provider Required

You need to know how your service provider plans to authenticate your users on the VPN service. Are they just using name and password-based authentication with its inherent management problems? Or will your users have to use challenge-response tokens that are costly and not very user friendly? If your provider is in full compliance with IPsec, they will be using digital certificates, which offer the highest level of authentication and provide customers with the most secure VPNs.

What to look for: VPN authentication via digital certificates is critical. In addition, for companies who do not already have a Public Key Infrastructure (PKI), or who need to manage thousands of digital certificates, it's essential that the VPN service be closely tied to a certification authority (CA). So selecting a VPN provider that is also a CA is the best choice: one provider for a complete solution, and no hidden costs for certificates.

Cryptographic Security

Some managed VPN services do not provide data encryption at all. They might tell you that it's secure because the service uses closed user groups. This mechanism addresses only one element of security — access control. It does not ensure data confidentiality or integrity. These are very important elements when your data is traveling over shared networks. Encryption and cryptographic integrity mechanisms are essential to preventing unauthorized users from intercepting or changing your data.

What to look for: Make sure the VPN provider uses encryption. Triple DES represents the state of the art for commercial encryption, making the likelihood of successful interception exceedingly small. Check if your provider has or plans to put a key recovery mechanism in place so that you can use strong encryption internationally as well as domestically. In addition, look for a VPN provider that will work with you to determine what level of encryption is required for each location. This type of expertise and service is not part of most providers' solutions.

Once you feel assured that your VPN provider can meet security requirements, you can then evaluate their capabilities in the four additional areas: performance/reliability, management and monitoring, consulting and integration services, and provider stability and reach.

Performance: A Three-Part Harmony

Business-quality performance means guaranteed performance and reliability levels. It means your data will get where it's supposed to go, no matter where or when it is sent. Many Internet service providers have vastly improved their performance and reliability, and hopefully, VPN offerings will reflect these improvements. How can you tell if your VPN provider is one of the high performance contenders? Ask the tough questions, such as:

- What service level guarantees are offered, and how are you compensated if the provider does not meet the commitments?
- Is the VPN service using high-performance, dedicated hardware devices?
- What is the underlying structure and fabric of the provider's network infrastructure?

Service Guarantees

Today, any credible VPN service provider will commit to service level guarantees. If this is not a component of the service, you can stop your evaluation here. You need to review the commitment from three different perspectives: a) the actual guarantees, b) your recourse if the guarantees are not met, and c) how they are monitored and measured.

What to look for: Guarantees should be offered in four major areas. For your dedicated connections you should look for availability and latency guarantees. For your remote access connections you should look for call success rate and initial modem connect speed guarantees that meet or beat the industry average as measured by an independent third-party organization.

When it comes to service level agreements, providers should back up their guarantees with a proactive refund policy. This policy will indicate the confidence your provider has in its ability to meet or beat its service level commitments. As well, your provider should constantly monitor and gather data on their service levels (so that you don't have to catch them missing their service commitments) and provide you with online access to that information.

Specialized Hardware Devices

A good indicator of whether or not your VPN service will offer high performance is how the VPN is implemented. Some VPN service providers use software-based encryption, running on either a firewall or a router. Today, these are not good indicators of high performance. These devices were created to serve different purposes; attempting to use them to create a VPN will potentially overload these devices and decrease overall network performance.

What to look for: Only specialized VPN hardware devices are capable of delivering both the performance and functionality that a business quality VPN requires. Look for 10 Mbps growing to 100 Mbps throughput while encrypting, support for 500 to 1,000 simultaneous remote users per device, and the ability to handle over 1,000 simultaneous VPN tunnels per device. You need a service that uses such specialized VPN hardware devices.

Proven Network Infrastructure

Your VPN is only as reliable as the infrastructure that supports it. When reviewing providers, you should look at this from three perspectives: a) the technological prowess of the network, b) the current scope of the network, and c) the provider's commitment to investment and continuous improvement of their network.

What to look for: First, you need a Tier-1 provider that has a business-class IP backbone. In addition, you should expect that your provider will have concrete plans to upgrade their infrastructure with robust network technologies, such as integrated self-healing SONET OC-192 rings, frame relay, and ATM-layered architecture. The VPN service provider should also be able to provide you with access both domestically and internationally. Finally, ask the provider what they are investing in the future build-out of their network — this will give you a real indication of their commitment to providing an ongoing, robust, state-of-the-art network infrastructure.

Management and Monitoring

Most VPN service providers will provide some flavor of 24x7x365 remote monitoring and management. But there is management, and then there is management. Most providers are using the management tools that are part of the VPN vendor's system. These tools are immature and not created for use as part of a managed service designed to support hundreds or thousands of customers. Few providers offer what is required to provide truly mission-critical managed IP services, particularly when it can mean reporting on their own performance and inability to meet service level agreements. Also, you need to understand how easy the service provider will make it for you to make changes to your VPN, add and delete users, update security policies, and change remote configurations. Many industry experts believe management and monitoring capabilities will define the successful VPN service providers.

What to look for: You need a provider that has a dedicated VPN network operations center with trained professionals who are using the state-of-the-art VPN management tools. Ask the provider what they use for management tools. You need a provider that can provide you with real-time and historical reports so that you can see how your VPN is being used and how it is performing. You need a provider that will analyze this data and actively work with you to calibrate your VPN for the best possible performance.

Consulting and Integration Services

Here is another area where the VPN service providers differ widely. Companies embarking on a VPN need to reduce networking costs, minimize risks, and accelerate the time it takes to get their VPN up and running to their satisfaction and the satisfaction of their users. And they need readily available assistance and proven expertise. Often, the first step is determining an overall game plan for the VPN: what performance levels are needed; which applications are best suited; what security is required; whether staging and integration services are needed. Most VPN providers cannot offer a track record for these types of services.

What to look for: Look for a VPN provider with a full range of network security, consulting, and integration services, including experience in network and security assessment, design, policies and procedures, penetration testing, and staging and integration.

Provider Stability and Reach

There are lots of questions you should ask any potential service provider to determine provider viability, stability, and experience in order to separate those with in-market expertise, versus the relative newcomers to managed services. Begin by checking the industry reports on what makes a good ISP.[3] This will help you determine which providers have the best service offerings, support track records, and security expertise. There are many second-tier ISPs that will not be able to meet the needs of most VPN customers. Many, for example, cannot provide global access or demonstrate that they are making the investments in a VPN architecture required to support global customers. Many cannot provide the flexibility and guarantees required because they do not own or manage their own IP backbone networks. Others will not be able to show scalability for very large, secure implementations.

What to look for: Proven engineering experience building and managing complex networks, hosting mission-critical sites, and deploying applications; 24x7 monitoring with end-to-end systems management; high industry ratings for performance, reliability, and bandwidth; significant future investments in global network infrastructure. Finally, you should ask if your VPN provider's management and service capabilities are available across other service provider networks — this is especially important if you plan to expand your VPN to partners and customers who may use a different Internet service provider.

Summary

It seems there is a press release every day about a new VPN service offering. The feeding frenzy atmosphere shows just how quickly the market is evolving. Yet, among the majority of the VPN service providers, there appears to be little differentiation. With security as the driving force behind corporate VPN deployment, it is critical for VPN providers to focus on this core capability. And while most VPN providers will claim security expertise, few can withstand critical evaluation based on security as the paramount concern of customers. Companies adopting the Internet for secure business applications simply cannot afford a tactical choice that may result in changing VPN service partners later, because of provider security difficulties or inability to meet customer requirements. Unless security is the initial focus, organizations may just as well link their critical applications to the public Internet and forego the secure communications Internet-based VPNs are designed to provide. At the same time, VPN service providers must score high on a detailed assessment of performance, management and monitoring, consulting and integration services, as well as overall vendor stability and reach. With these key criteria in mind, it is possible to pick a managed VPN service winner.

Managed Connectivity
GTE Internetworking offers a wide range of connectivity options, including dedicated lines from 56 Kbps to 45 Mbps (T3) and frame relay access domestically, and 64 Kbps to 2 Mbps (E1) bandwidth internationally. Managed connectivity comes with around-the-clock network management, monitoring, and problem resolution, including 24x7 line monitoring by the GTE Internetworking Network Operations Center. Enhanced features include Internet domain name service administration, network news feeds, packet filtering, and network usage reporting. GTE Internetworking can also provide routers and other hardware for full Internet access.

Dial-Up Access
GTE Internetworking's DiaLinx℠ remote access service provides businesses and organizations with dial-up access to their intranets, extranets, and the Internet from nearly 600 local calling locations in the United States and approximately 150 countries around the world. For small businesses and consumers, GTE offers analog and ISDN Internet access from more than 550 local dial-in numbers available nationwide and provides 24x7 customer service and technical support.

Managed Internet Security
Site Patrol℠ is an Internet security service, available on a global basis, designed for companies that seek secure, reliable communications across the Internet, along with reduced exposure to network security breaches through their firewall. The solution includes firewall hardware, software, and installation, field-tested operational policies and procedures, configuration management, security updates, 24-hour proactive monitoring, and appropriate rapid response by GTE Internetworking's Network Operations Center. Site Patrol works on any ISP network. GTE Internetworking Site Scan Service provides an effective means for identifying vulnerabilities, risk factors, and recommended remedies in a proactive manner to address security vulnerabilities.

Certificate Management Systems
GTE Internetworking's CyberTrust® Security Family provides Certification Authority (CA) products and CA hosting services to support secure Web access, Internet-based communication, and electronic transactions. It includes a wide range of public key infrastructure (PKI) solutions used worldwide for electronic commerce by financial institutions, corporate enterprises, and government agencies. The CyberTrust Security Family is scalable to meet the highest assurance security requirements of individual enterprises and national certification authorities.

Web Hosting
By offering a full spectrum of Web hosting services, GTE Internetworking provides organizations with high-performance, high-bandwidth, highly reliable, and scalable Web sites. Services include shared, dedicated, custom, and collocated hosting, designed to meet specific needs for a professionally managed and monitored Web site. GTE Internetworking can help clients grow from simple marketing Web sites to large-scale, integrated transaction environments. GTE Internetworking's hosting infrastructure includes Hopscotch™, a unique load-balancing technology, and secure distributed data centers strategically located at key network exchange points throughout the world.

Web Applications
GTE Internetworking offers a full suite of value-added, Web-based applications and integration services that enable organizations to migrate their businesses to the Web, moving from the simple exchange of information to true e-commerce. The Re@ch Enterprise suite offers a full-featured e-commerce solution, including an electronic catalog with payment and delivery options, which leverages our industry-leading Web hosting, project management, implementation support, consulting, and training services.

Consulting Services
GTE Internetworking offers consulting services based on a unique depth and breadth of network and security experience. GTE Internetworking's consulting services include a seasoned team of highly qualified and widely respected internetworking consultants, researchers, practitioners, and technology analysts. Offers include assessments, design, migration, implementation, and distributed application services, as well as advanced scheduling capabilities.

About GTE Internetworking

GTE Internetworking, a unit of GTE Corporation (NYSE:GTE), offers customers, from consumers to Fortune 500 companies, a full spectrum of integrated Internet services using IP networking technologies. GTE Internetworking delivers complete network solutions, including dial-up and dedicated Internet access, high-performance Web hosting, managed Internet security and Virtual Private Networks, enhanced IP services, network management, systems integration, and the enabling technologies for electronic commerce. GTE Internetworking has 12 global data centers, a unique load-balancing technology for Web hosting, and seamless dedicated access in more than 65 countries. The company also develops advanced technologies through funded research and development at its BBN Technologies division.

For more information, contact us at:

GTE Internetworking
3 Van de Graaff Drive
P.O. Box 3073
Burlington, MA 01803

Tel: 800.472.4565(toll-free from U.S. or Canada)
or +1 781.262.2905
Fax: +1 781.262.2310
URL: http://www.bbn.com
E-mail: net-info@bbn.com

GTE Internetworking International
Centro Direzionale Milano Oltre
Palazzo Tintoretto
Villa Cassanese 224
20090 Segrate (Milano), Italy

Tel: +39-02-2692-6142
Fax: +39-02-2692-2101
URL: http://www.bbn.com
E-mail: net-info@bbn.com

GTEI/0064/1.99/VPN/WP/8K