Managed VPN Services:

Marketing Opportunity and Paths for Implementation

A Guide for Enterprises and Service Providers
with Market Forecasts Provided by Infonetics Research

VPNet Technologies Inc.
www.vpnet.com

Table of Contents

Appendices

List of Figures

List of Tables

I. Introduction

Virtual private networks – or VPNs – have risen from relative obscurity to international celebrity status. Why all the excitement over VPNs? Are they just the fad of the month, or do VPNs truly represent a significant and lasting change in the way that businesses communicate? Are all VPNs the same? If not, how can we recognize the different types of VPNs and understand the applications, limitations, and issues associated with each? Many organizations are struggling with these questions as they map their strategies for supporting their business communications needs today and in the coming years. And while there are numerous topics of discussion and debate under the VPN umbrella, one thing is increasingly clear: VPNs have arrived and are here to stay.

According to a recent study conducted by Infonetics Research, worldwide expenditures by enterprises for VPN services are expected to top $10 billion in 2001, rising to over $29 billion in 2003. (See Appendix I for detailed data.) Such phenomenal growth can be readily understood when one considers the unusual “double benefits” that VPNs provide: Unlike many new technologies, VPNs enable organizations to immediately improve their effectiveness and competitiveness and reduce their operating costs at the same time.

VPNs clearly represent a significant opportunity. However, there are significant challenges facing both the enterprises that wish to profit from using VPNs, as well as the service providers who wish to profit by offering them. This paper is devoted to helping both enterprise network managers and service providers to better understand the VPN opportunity, the steps involved in implementing VPNs, and how to make the most-effective choices in planning and implementing VPN strategies.

II. A Brief Overview of VPNs

A. VPNs: An Alternative to Traditional WAN Infrastructures

Effective communications have become a necessity in today's networked economy, where timely access to business information is essential for companies to compete and serve customers. However, providing access to information at a reasonable cost has become more difficult as new communications requirements have outpaced the capabilities of traditional technologies for wide area networking (WAN). For example, leased line and frame relay services, which are well-suited to linking the offices of individual companies, are ill-suited to the needs of organizations that, in increasing numbers, need to exchange critical data with business partners as they implement outsourcing strategies. In addition, as markets are increasingly global, many companies are faced with unacceptably high costs whenever data cross international boundaries. At the same time, as more workers telecommute and travel, traditional remote access services have become too expensive and cumbersome to serve the needs of the increasingly dispersed and mobile workforce. These trends have put strains on traditional network infrastructures, especially as the once-clear distinction between the corporate LAN and the public WAN continues to blur.

What is needed to address the limitations of traditional WAN services is a low-cost, robust, worldwide data network that can connect anyone, at any time, to anywhere. Of course, such a network – in fact, many such networks – already exist in the form of the Internet "cloud" and the dedicated IP backbone networks maintained by dozens of network service providers. The Internet has clearly started a revolution based on the wide availability of low-cost, *adhoc* data communications. But despite the worldwide communications revolution created by the Internet, it is not an appropriate medium for business communications due to problems of guaranteeing reliability and quality of service (QoS), operational manageability, and security. However, a properly designed VPN can solve these problems, providing the end user with a greatly improved business communications infrastructure at a significantly reduced cost.

Specifically, VPNs allow:

- Network managers to cost-efficiently increase the span of the corporate network.
- Remote users to securely and easily access their corporate network.
- Corporations to securely communicate with business partners.
- Enterprises to outsource the hosting of servers and applications.
- Service providers to grow their businesses by providing substantial incremental bandwidth and value-added services.

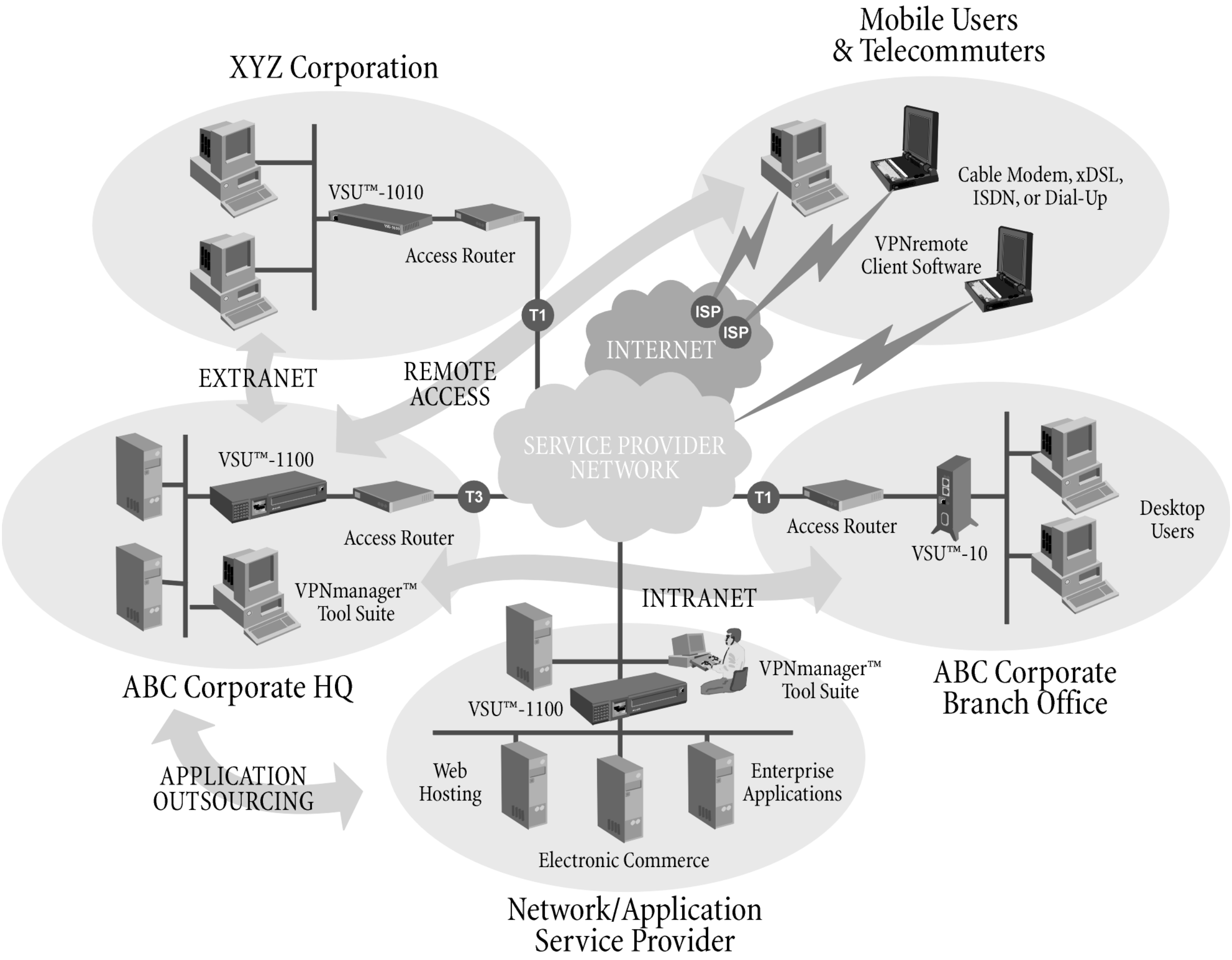

Figure 1. VPN Application of Intranet, Extranet, Remote Access, and Hosting

When compared with current alternatives, VPNs offer significantly improved capabilities at a reduced cost. VPN-based intranets enable companies to save money by avoiding the high recurring line charges and labor costs associated with leased lines, and VPNs are more flexible than frame relay services. VPNs also allow remote access for the cost of a local call, which is often free—or at least much less expensive than dialing in at long distance rates. According to numerous studies and reports from end users, companies can quickly save 20 to 40 percent on site-to-site domestic networks and much more internationally. Savings range from 60 to 80 percent for traveling and telecommuting employees connecting to the home office via a VPN. In addition, VPN connections can be set up and taken down in minutes -- compared with the days and weeks typically associated with adding or changing leased line or frame relay services.

Most importantly, from a strategic view, VPNs enable rich, flexible communications with customers, suppliers, and business partners over extranets. These allow users to establish secure interactive links with every business partner—not just a few. Expensive, dedicated WAN facilities are no longer a necessity. Instead, VPN technology creates a secure communications cloud that members may join with ease. VPN extranets provide a cost-effective, manageable, and secure means for building closer business relationships. They enable improved service and support while increasing revenues and enhancing customer loyalty, by including customers as an extension of the corporate network. VPNs have major strategic implications because of their unique ability to reach across traditional and arbitrary barriers and change the ground rules of business communications. Put another way, with VPNs, *the WAN is the LAN*.

B. VPN Implementation Challenges

While VPNs can be simple to implement, they frequently require the use of new and often unfamiliar technologies compared with frame relay, leased line, or enterprise-based remote access services. The primary reasons that VPNs are more challenging are illuminated by considering the technical scope and geographic breadth required for VPN services.

Traditional Services are Predictable

While traditional leased line and frame relay services are rather limited and inflexible, they do provide the benefits of predictability. For example, leased line connections are simple point-to-point links that are pre-engineered to exhibit well-controlled performance characteristics. Security is not a concern in leased line networks except in the cases where the data are of extraordinary value, such as government secrets or large bank transactions. As such, there is no need to validate the origin of data that emerge from a leased line; the data must have come from the other end of the link. Nor is there a need to scramble data to render it unreadable to unintended recipients. Service level management is also not a major concern, because service providers can tightly manage a leased line's throughput and delay. Frame relay links, although they offer greater flexibility than leased lines (i.e., point-to-multipoint capability) and sacrifice fully guaranteed performance, are generally similar to leased lines in perceived security and service level.

VPNs are Policy Based Networks

VPNs, especially those that use or provide access to the public Internet, provide great flexibility compared with traditional services, but generally do so at the expense of predictability. For example, one cannot assume anything about the origin of a data packet emerging from a link to a public VPN. It may have come from a remote company site or a telecommuter, or from a business partner, or from a public web site – or from a would-be intruder.

In addition, unless all of those connected to a VPN use a single service provider's network, it is generally not possible today to predict, much less guarantee, performance. As such, VPNs require each data stream to be processed as it enters and exits the public WAN to ensure security and to optimize performance and manageability. The collection of services which is applied to each data stream in a VPN is a policy. Generally, policies apply to individual users or groups of users (e.g. senior management, sales personnel, specific business partners, etc.), and include specific security, quality of service, and management features. A list of such VPN features, along with the related technologies and key standards is presented in Table 1.

TABLE 1. TECHNOLOGIES AND STANDARDS USED TO IMPLEMENT VPN POLICIES

VPN Requirement	Related Technologies	Common/Standard Implementations
Secure data over the public IP network	Encryption, packet authentication, key management	IPSEC, DES, 3DES, IKE
Verify user identity	User authentication	PKI (x.509), tokens, RADIUS
Generate VPNs policy	Directory services	LDAP, NDS
Access control/ network protection	Firewall, intrusion detection, virus checking	Packet filtering, stateful inspection, appplication proxy, content filtering
Connect private LANs over public IP network	Network Address Translation (NAT)	RFC 1631
Maximize available bandwidth	Compression	STAC, LZS
Match available bandwidth to business priorities	Bandwidth management	CBQ, Rate control
Manage business traffic using policies	QoS, Service level management	Diff-Serv, COPS, MPLS, etc.

Security and user authentication features are used in essentially all IP VPNs. Nonetheless, there is considerable variation in VPN implementations, especially in view of the many permutations and combinations of features, technologies, and standards available. This issue will be revisited later in this paper when we classify VPNs into 5 classes, ranging from the simplest to the most complex applications. For now, what is most important to note is that *very few (if any) of the technologies listed above are typically needed or used in traditional frame relay, leased line, or remote access services*. For those not already experienced in deploying policy-based networks, VPNs require the acquisition and mastery of new skills.

VPN Implementation Challenges: Technical Scope and Geographic Reach

As with any sophisticated technology, successful VPN implementation demands careful coordination of a set of interrelated tasks, as shown in Table 2, from the initial design requirements through the day-to-day operations and support.

TABLE 2. MAJOR TASKS REQUIRED TO DEPLOY A VPN

VPN Implementation Tasks	Key Elements
Network Design	Existing network and applications audit Identification of VPN applications (intranet, extranet, remote access, hosting) Determination of bandwidth and QoS policies Service Level Agreement definition Determination of public & private addressing schemes, translations, & naming services Identification of VPN device placement relative to existing routers, firewalls, etc.
Security Design	Security analysis and audit Security policy definition and review Determination of encryption, authentication, key management, access control, and filtering policies Determination of user authentication and Public Key Infrastructure requirements
Network and Security Integration	Initial installation and configuration of devices: Routers, VPN service units, firewalls, bandwidth management devices, authentication servers, directory servers, etc. Verification and check-out
Operations and Support	VPN activity and performance monitoring Security monitoring and reporting Certificate authority management Remote site and user support Change management Capacity planning

In addition to the technical and logistical challenges mentioned above, VPNs tend to be geographically dispersed, and are often international in scope. This is not surprising, as VPN cost savings are usually the greatest when international borders are crossed (compared with traditional WAN services). As such, many organizations planning to use or offer VPNs find themselves faced with a need to deploy the services in far-flung locations from the outset.

This combination of great geographic reach and technical scope is unique to VPNs. Compared with traditional telephone services, leased line and frame relay services, and even Internet access, VPNs are more challenging, as they demand skills that cover a wide range of new, often unfamiliar technologies, along with the need to do so in many locations at once.

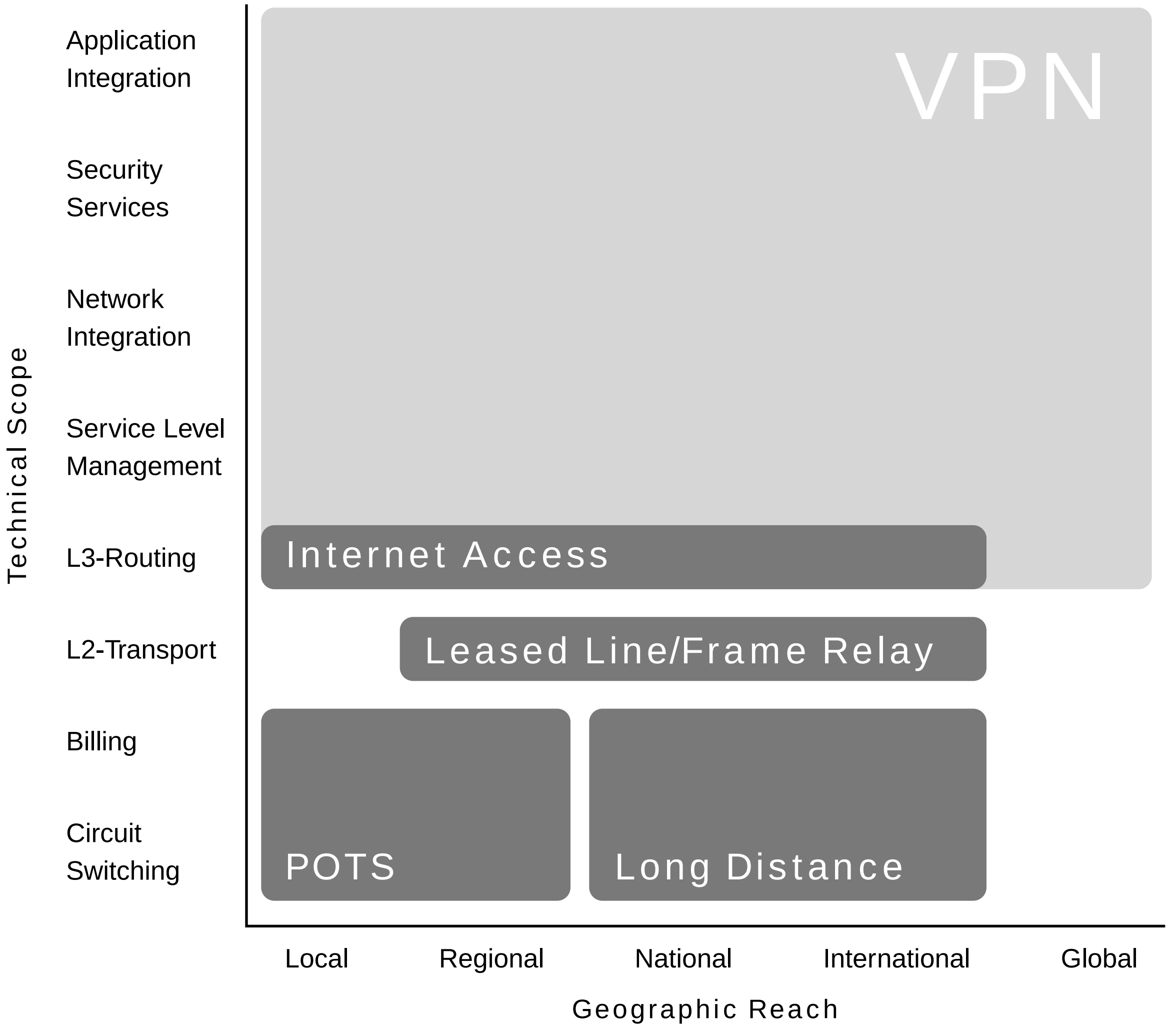

Figure 2. VPNs Provide Greater Geographic Reach and Technical Scope than Traditional WANs

The unique challenges of VPNs call for carefully planned implementation strategies. A number of such strategies are discussed in the next section.

III. Outsourcing as a VPN Strategy

A. VPN Outsourcing for Enterprises

End users essentially have two choices when it comes to launching a VPN:

1. Purchase bandwidth from a network service provider and perform the remaining tasks using in-house or outsourced resources; or

2. Purchase a turn-key VPN service from a service provider who offers managed VPN services

Whether large or small, all companies are facing a worldwide scarcity of qualified IT and networking talent. In fact, most IT departments are stretched to capacity, dealing with network growth, new applications, Y2K problems, and the like. This scarcity of key personnel is expected to not only persist into the foreseeable future but to get worse. Not surprisingly, therefore, many enterprises have already turned to outsourcing to fulfill all or part of their current IT requirements. The emergence of VPNs, with their combined challenges in terms of technical skills and international scope, only heightens the need for IT and WAN service outsourcing. Indeed, according to the data in Appendix I, fully 65 percent of VPN revenues are expected to be generated by enterprises that outsource some or all of their VPN needs to their service provider – a market worth over $19 billion annually in 5 years.

In general, only the largest corporations possess the depth and breadth of skills needed to implement and manage VPNs. These companies also express the greatest reluctance to share the responsibility for their security controls with their IP service providers. As such, a number of large companies will be the most likely to purchase “unbundled” bandwidth from their service providers. According to Infonetics, such purchases of unmanaged IP bandwidth for VPNs will represent $10.4 billion in revenue in 2003, representing just over one third of the VPN services market. Of course, many if not most of the companies who purchase unmanaged bandwidth are also expected to utilize network and system integrators to assist them with the design, implementation, and management tasks.

B. Outsourcing for Service Providers

Service providers who plan to offer VPN services face many of the same challenges as their enterprise customers: They need to support a variety of new technologies, and to provide installation and support services worldwide in order to be successful. Service providers also face a slew of additional challenges. In particular, they must:

1. Determine the segments of the market in which they’ll compete, e.g.
   - Large, medium, or small companies
   - Regional, national, or international coverage
   - Intranets, extranets, remote access, or hosting services
   - Bandwidth only, network services, security services, full turn-key, etc.

2. Determine how VPN services will be positioned relative to other services they may currently offer (such as leased line, frame relay, or other services)

3. Establish the network infrastructure necessary to offer IP services, directly or through arrangements with other service providers

4. Determine the types of access services and data rates to be supported
   - Dial, ISDN, DSL, T1, DS3, OC3, etc.

5. Establish parameters for offering service level agreements and non-performance penalties
   - Throughput, latency, availability, etc.
   - Measurement and validation methods

6. Establish processes for managing and delivering committed service levels

7. Determine the types of security services to be provided
   - Assessment, audit, design
   - Encryption, user authentication, tunneling, key management
   - Firewall, filtering, content inspection, virus detection
   - Public key infrastructure
   - Monitoring and reporting
   - Change management

8. Determine which services will be delivered at the customer premises vs. those delivered within the service provider's core infrastructure

9. Integrate VPN services into their order administration, provisioning, and operations systems

10. Determine how to bill for VPN services

11. Establish facilities for monitoring and troubleshooting customer problems and network problems

12. Evaluate and choose VPN hardware and software products

13. Establish processes and resources for VPN design, installation, and support

14. Train sales and support staff

15. Launch and promote the service

Given the formidable list of tasks to be addressed by service providers, it is not surprising that they, like their enterprise customers, are turning to outsourcing to supplement their technical capabilities and geographic reach. However, both service providers and enterprise managers need tools to help them sort through the many issues and focus on those most relevant to their specific needs and goals. The next section provides a basis for classifying VPNs and identifying those issues that are of concern to implementers and users of the various VPN types.

IV. A Guide to VPN Classification

All VPNs are not the same. They vary in purpose, size, scope, and complexity. There are no clear, “hard and fast” rules by which to classify VPNs. The classification scheme detailed in Table 3 is intended to help users and service providers to quickly determine the types of VPN technologies they’ll need to deploy based on the applications they intend to support, the VPN services to be provided, and the size and scale of the network.

TABLE 3. VPN CLASSIFICATION GUIDE

VPN Class	Typical Users	Typical Information Needs	Scalability & Bandwidth Needs	Technologies/Products	Pros/Cons
Class 0	Small companies with remote workers (small manufacturing, services, etc.)	• Email • Internal database • File access	• 1 site • Up to 50 remote users • Internet access at site via DSL or FT1 • Dial access for remote sites	• PPTP • Windows 95/98/NT • Software VPN solutions on standard PC platforms • Packet filtering	+ Simplest and lowest cost to implement + Good way to “trial” remote access - No site-to-site - Inflexible (point to point) - Longest meantime-to-repair (if server fails)
Class 1	Small to mid size companies with multiple locations (small to mid-sized manufacturers, services, etc.)	• Email • Internal database • File access	• 2 to 10 sites • Up to 250 remote users • Internet access at site up to T1 • Dial access for remote sites	• IPSec (DES, IKE) • Password user authentication • Hardware VPN gateway (wirespeed T1 with 250 sessions) • Remote access client software • Simple firewall or packet filtering	+ Easy to design & install + Low cost + Site-to-site & remote access + Hardware gives security without performance loss - Extranets not supported if IPSec is not interoperable
Class 2	Medium size companies with high-value intellectual property; (design services, media, etc.)	• Email, internal database & file access • Product design • Project plans	• Up to 10 sites • Up to 500 remote users • Up to T1/multi-T1 at main site • Up to T1 for branch sites • Dial access for remote sites	• IPSec, (3DES, IKE) • Network Address Translation • Strong user authentication (eg.,soft tokens) • Firewall at main site • RADIUS server • Hardware VPN gateways at multiple performance levels (wirespeed T1, wirespeed multi-T1 with 500 sessions) • Remote access client software	+ Higher security + Manageable cost + Site-to-site & remote access - Additional administration (RADIUS, Firewall, etc.) - No extranets (requires interoperability) - No real-time applications

Class 3	Medium to large companies with their business partners & customers (medical, manufacturing, insurance, e-commerce)	• Email, internal database & file access • Design information • Supply chain info & transactions • e-commerce	• 100's of sites • 1,000's of remote users • FT1 to multi-T1 at branches • Multi-T1/T3 at main site • QoS/SLAs for intra-company sites • Dial, ISDN, xDSL, or cable modem access for remote users	• Certified interoperable IPSec (3DES, IKE) • Network Address Translation • Strong user authentication (smart cards, tokens) • Firewall at main site and large branches • LDAP directory server • Certificate services (PKI) • Hardware VPN gateways at multiple performance levels (wirespeed T1, wirespeed multi-T1, wirespeed T3 with 1000+ sessions) • Remote access client software with automatic policy distribution	+ Support extranets + Support time-sensitive e-commerce transactions - Requires corporate security policy - Requires sophisticated design skills - Requires significant ongoing administration & management
Class 4	Large multi-national companies with extended business partner chain and high degree of outsourcing (medical, insurance, government, financial, etc.)	• Email, internal database & file access • Supply chain info & transactions • e-commerce • Voice & video	• 1000's of sites • 10,000's of remote users • FT1 to Multi-T1 at branches • f-T3 to OC3 at main site • QoS/SLAs for intra-company. sites • Dial, ISDN, xDSL, or cable modem access for remote users	• Certified interoperableIPSec (3DES, IKE) • Network Address Translation • Strong user authentication (smart cards, tokens) • Firewall at main site and large branches • LDAP directory • Certificate services (PKI) • Hardware VPN gateways at multi performance levels (wirespeed T1, wirespeed multi-T1, wirespeed T3 or OC3 with 5000+ sessions) • Bandwidth management • Multi VPN service levels • Real time QoS & SLAs • Remote client software with auto- policy distribution	+ Supports extranets + Highest security + Supports real-time voice & video + Supports e-commerce transactions + Scalable admin + Multiple partner relationships - Most complex & expensive - Requires extensive network & security skills, - Significant ongoing management effort

Class 0 VPNs are only for small companies with a single site and limited remote workers. They are the simplest and least expensive VPNs to implement, offering Point-to-Point Tunneling Protocol (PPTP) and packet filtering for intranets. At a minimum, all that is required is the installation of Windows NT, or for slightly more security, a VPN software solution installed on a server. The Class 0 VPN provides for email and internal database access at a single site, and file access for up to 50 remote users, through dial-up connections. The Internet access at the main site can be over an SDL or fractional T1. These most basic of VPNs are the simplest and cheapest to implement, and they offer an easy way to test remote-access applicability. The downsides are site-to-site inflexibility and the longest mean-time-to-repair, if VPN software is residing on a server that fails.

Class 1 VPNs are optimum for small to mid-sized companies, with multiple branch locations, accessing the Internet over T1 connections, with up to 250 remote users. Class 1 VPNs offer basic IPSec security with DES encryption, and password authentication for remote access to email and access to internal databases and files. These VPNs are implemented through a hardware VPN gateway with associated client software for IPSec remote access. The benefits are comparatively easy design and installation, low cost, both site-to-site and remote access, and greater security without performance degradation. However, extranets are not supported unless the IPSec implementation used has been certified for interoperability.

Class 2 VPNs are applicable for medium companies with up to 500 remote users and up to 10 corporate sites, such as engineering firms or advertising and marketing agencies that have high-value intellectual property. Branch office connections can be provided by T1 or FT1 links; main-site connections can be provided by single or mulitple T1 lines. Class 2 VPNs offer higher security, with 3DES encryption and strong (two-factor) user authentication, using a method such as software tokens. Scalability can be enhanced through the use of RADIUS servers to manage the user names, passwords, and policies. The Class 2 VPNs can coexist with firewalls and offer network address translation (NAT) to allow privately addressed sites to be linked together without requiring changes to the existing LAN addressing schemes. The benefits of Class 2 VPNs are higher security, manageable cost, and provision for site-to-site communications as well as remote access. The weaknesses are lack of support for extranets and real-time applications.

Class 3 VPNs support medium to large companies with thousands of remote users and hundreds of sites, including those of business partners and customers, to send and receive customer account status, supply chain transactions, and e-commerce transactions. Such users could be medical providers, insurance companies, manufacturers, or companies that are part of an extended supply chain. Branch-office connections are typically over fractional T1, full T1, or multiple T1 lines. Main-site connections could be over multiple T1, fractional T3, or full T3 links. Remote users can have access over xDSL or cable modem connections, as well as dial access. Class 3 VPNs use a service provider that offers QoS and service level agreements to support guaranteed response times for critical applications running between company sites connected to the provider’s backbone. The use of certified interoperable IPSec devices enables extranets with users on different networks with different equipment. The addition of user-level authentication capabilities, such as two-factor authentication tokens or smart cards, supports secure remote access, and enables user-level usage reporting and billing. For scalable administration, Class 3 VPNs employ directory services for storing and retrieving policies, as well as for storing digital certificates used for authentication. Correspondingly, an in-house certificate authority, outsourced certificate service, or some method of managing a public key infrastructure (PKI) is required. As such, implementation of these VPNs requires sophisticated design skills and ongoing management with concomitant time and resource requirements. In addition, implementation of sophisticated policies for employee and partner access necessitates the development, implementation, and management of a comprehensive corporate security policy.

Class 4 VPNs are the most secure, flexible, and scalable. They support secure transactions for large, multi-national enterprises, with more than 10,000 users and thousands of sites, that have extended chains of business partners and needs for a high-degree of outsourcing, such as government agencies and financial institutions. The branch sites can be connected over fractional T1/E1, full T1/E1, or multiple T1/E1 links, and the main sites can be linked over fractional T3, full T3, or OC3 lines. The full range of remote access options, from dial to xDSL and cable modem are supported. Use of a service provider network that offers real-time QoS and SLAs in conjunction with bandwidth management supports convergence applications such as voice over IP and IP video conferencing. Class 4 VPNs make extensive use of directory services and PKI technologies to manage policy and verification of user identity and role. These VPNs support sophisticated extranet relationships involving multiple partners and multiple, independent PKI systems. Class 4 VPNs are comparatively complex and expensive to implement, and require significant ongoing management.

V. VPN Service Planning and Implementation Tools

With an understanding of the information presented thus far, establishing a VPN implementation strategy is fairly straightforward. We have identified the key VPN implementation tasks, and classified VPNs according to the supported applications and their required technologies and services. We've also identified the potential for outsourcing to play a key role in dealing with the technical scope and geographic breadth of VPNs. What remains is for each organization to examine their own objectives, requirements, and capabilities, and to determine a course of action. In short, the key questions to identify are these:

1. WHAT are the VPN technologies and services that will be required?
2. WHO will perform each of the key implementation tasks?
3. WHERE will each function be performed?

In the remainder of this paper, we present a number of tools than can be used respectively by enterprise IT managers and by service providers to plan and execute their VPN strategies. The first tool, in Appendix II, is an "Enterprise VPN Checklist" that establishes the VPN class required and identifies WHO will perform each of the key tasks for an enterprise VPN project. The second tool, in Appendix III, is a "Service Provider VPN Checklist." This tool lists the additional tasks required for service providers to define and launch VPN services, and also provides a place to identify WHAT will be provided and WHO will handle each task.

The next section addresses Item 3 above, which concerns WHERE key VPN services are deployed. This topic, a subject of much discussion, requires very careful consideration by both the enterprise user and the service provider.

VI. Where to Locate VPN Services

A. To CPE or not to CPE

As discussed earlier, VPNs add security, quality of service, and manageability features to data streams as they travel from a private LAN, or remote user, to a public WAN--and again upon exiting the WAN and entering another private LAN. To date, the vast majority of VPNs have been implemented using hardware and software deployed at or near the point at which the enterprise LAN physically connects to the WAN access link, using customer premises equipment, or "CPE." There are however a number of vendors and service providers who are promoting the idea of implementing VPNs wholly within the service provider's WAN infrastructure, entirely without the use of CPE. This has led to an interesting industry debate which will no doubt persist for some time. As the decision to implement a VPN with or without CPE is significant, this subject is discussed briefly here.

B. Pros and Cons of CPE-Based VPNs

The primary benefits of CPE-based VPNs are as follows:

- The enterprise user retains physical possession of the devices that contain the most sensitive security information, such as user passwords, encryption keys, etc.
- Security is "end-to-end," from the user's location to the end destination: The data are secured prior to exiting the customer's premises, limiting security exposures on the link(s) between the access provider(s) and the VPN provider.
- The customer premises is the natural (and only) location at which to apply bandwidth management functions to LAN-based application traffic. Once data leave the enterprise LAN and enter the WAN access link, it is too late to apply policy in order to prioritize one type of traffic over another.
- CPE-based VPN services can be implemented in conjunction with many different IP service providers, and are not tied to proprietary features that may be implemented only by one or a few providers.

The primary drawback of CPE-based VPNs is as follows:

- CPE-based VPNs may require the expense of one or more VPN service devices, each of which must be adequately housed and maintained.

C. Pros and Cons of Service Provider Core-Based VPNs

Core-based VPN services do not require the deployment of any customer premises equipment beyond that required for basic access (i.e. either stand-alone or integrated DSU/CSU and access router). All of the VPN services are provided by equipment located within the service provider's core infrastucture. The primary benefits of such core-based VPNs are:

- The customer is not required to invest in or maintain VPN equipment.
- The service provider can more easily provide high availability using highly redundant, "carrier-class" equipment.
- The service provider can more readily diagnose and repair VPN problems without dispatching personnel to the customer's location.
- The service provider can more closely integrate the VPN service with their core network QoS capabilities.

The primary drawbacks of core-based VPNs are:

- The customer must trust the service provider to properly protect sensitive security information, including passwords and encryption keys, held by the service provider.
- The path between the customer premises and the service provider's core-based VPN equipment, which includes the WAN access link and any intervening links between the access provider and the VPN provider, is not secured.
- It is not possible to apply bandwidth management services to LAN-based application traffic. Once the data pass from the enterprise LAN to the WAN access link, it is no longer possible to prioritize access to the more scarce (i.e. WAN access link) bandwidth.

D. And the Winner is...The Customer

To summarize the pros and cons listed above, CPE-based VPN solutions have the most benefits for the customer, e.g., they offer the greatest security, the most flexibility, and the most complete feature set, at the expense of additional equipment for the user and additional integration and service headaches.

Core-based solutions offer the most significant benefits for the service provider, e.g., they provide ease of deployment and maintenance, economies of scale, and a stronger hold on the customer, at the expense of security and functionality (such as bandwidth management). In the end, one would expect that in such a hotly contested and competitive market, the customer will ultimately dictate the result. As the market data in Appendix I indicate, there will be a market for both core-based and CPE-based VPN services: CPE-based managed VPN services are expected to account for approximately 74 percent of the total managed services market in 2003, with core-based VPN solutions expected to comprise the remaining 26 percent.

VII. Where to Locate a VPN Partner

VPNet has been a pioneer in the emerging VPN market, and was the first company to focus exclusively on delivering Virtual Private Networks Without Compromise™. VPNet has been recognized for its industry-leading VPNware™ Systems, which provide a complete range of hardware devices and software tools needed to configure and implement VPN security, quality of service, and management policies. VPNet has extensive VPN experience and expertise, with a customer base that includes major service provider and end user organizations in over 25 countries.

Recognizing the enormous need for both enterprises and service providers to outsource the design, implementation, and management of their VPNs, VPNet has created the VPNsureSM Managed Services Program. The VPNsure Program provides a range of services, on a global scale, to assist customers with the full range of VPN tasks. Either directly or through a network of VPNsure Alliance Partners, the VPNsure Program provides VPN planning, design, installation, monitoring, management, and maintenance services worldwide.

VPNsure Alliance Partners include local and regional specialist organizations, as well as global organizations such as IBM Global Services. Working together, VPNet and the VPNsure Alliance Partners make it easy for end users and service providers to quickly gain the benefits of using and offering VPN services.

To learn more about VPNet, VPNware Systems, and the VPNsure Programs, see the relevant sections of VPNet’s web site at www.vpnet.com, or call 1-888-VPNET-88 in the US or +1-408-445-6600 internationally.

Appendix I. VPN Services Market Projections from Infonetics Research

The forecasts below cover calendar years 1999 through 2003 and include intranet (within a single organization) and extranet (organization-to-organization) VPNs. The forecasts are presented in worldwide service provider revenues for all types of service providers (IXCs, ILECs, CLECs, ISPs, Next Generation Telcos, integrators, and VARs). Each forecast breaks the total worldwide VPN services opportunity into a different group of categories, and some categories in one forecast may overlap with categories in the other forecasts.

All forecasts are derived using the following:

1. Infonetics Research demand-side study data gathered from end-users and service provider
2. Supply-side information provided by VPN product manufacturers and service providers
3. Publicly available documents, including annual reports, public market research data, and other forecasts
4. Infonetics Research's expert opinion

All forecasts use information from the following Infonetics Research, Inc. studies, where applicable: The Medium Business Networking Opportunity 1997, User Plans for VPN Products and Services 1998, The ISP Opportunity Annual Service 1998, Access in the US 1999: the Big Picture, and The Local/Regional ISP Opportunity 1999.

For the purposes of these forecasts, VPNs are defined as secure private data networks that use the Internet and other public IP networks for transport. VPNs require tunneling and encryption technologies such as IPSec, PPTP, L2TP, DES, and Triple DES.

A. VPN Service Revenue

Table 4 and Figure 3 provide forecasts by VPN service types: unmanaged, managed customer premise equipment (CPE), and managed cloud.

1. Unmanaged VPNs include revenues for services such as design and integration, but not operations and support of the VPN.
2. Managed CPE-based VPNs, in which VPN tunnels are initiated at the organization's site(s), include revenues for services such as design, integration, and ongoing management.
3. Managed service provider cloud VPNs, in which VPN tunnels are initiated and terminated inside the service provider's cloud, include revenues for services such as design, integration, and ongoing management.

TABLE 4. VPN SERVICE TYPE REVENUE PROJECTIONS

VPN Types	Millions ($000,000)				
	1999	2000	2001	2002	2003
Unmanaged	$1,414	$3,018	$5,460	$8,793	$10,416
Managed CPE	$541	$1,688	$4,068	$8,011	$14,285
Managed cloud	$125	$409	$1,178	$2,736	$5,059
Total	$2,080	$5,115	$10,705	$19,540	$29,760
Total growth		146%t	109%t	83%t	52%

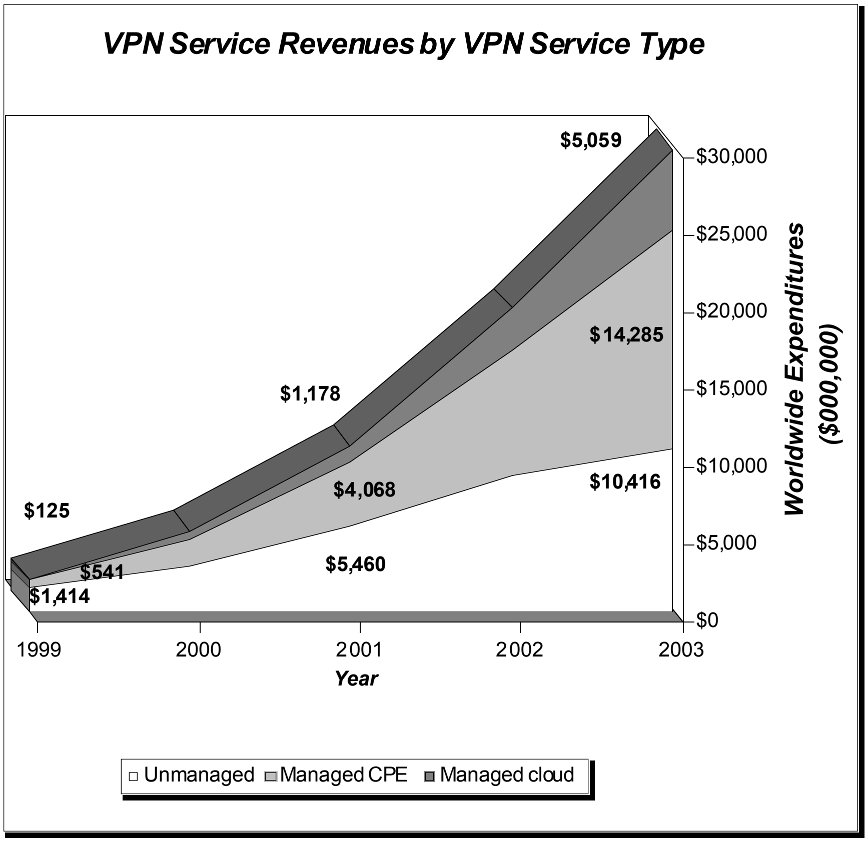

Figure 3. VPN Service Revenues by VPN Service Type

B. VPN Service Revenue Forecast by VPN Type

Table 5 and Figure 4 provide revenue forecast by VPN type.

1. Individual remote access VPNs for telecommuters, day extenders, and mobile workers include revenues for services such as design, integration, operations and support, and standalone bandwidth for individual remote access VPNs.
2. Site-to-site VPNs for connecting sites with multiple VPN users include revenues for services such as design, integration, operations and support, and standalone bandwidth for site-to-site VPNs.
3. Service provider hosted VPNs for connecting individuals or sites to servers, applications, or content hosted inside the service provider's network include revenues for services such as design, integration, operations and support, and standalone bandwidth for service provider hosted VPNs.

TABLE 5. VPN TYPE REVENUE PROJECTIONS

VPN Types	Millions ($000,000)				
	1999	2000	2001	2002	2003
Remote access	$1,352	$2,916	$5,138	$7,816	$9,523
Site-to-site	$624	$1,841	$4,496	$9,379	$15,773
Hosted	$104	$358	$1,071	$2,345	$4,464
Total	$2,080	$5,115	$10,705	$19,540	$29,760
Total growth		146%t	109%t	83%t	52%t

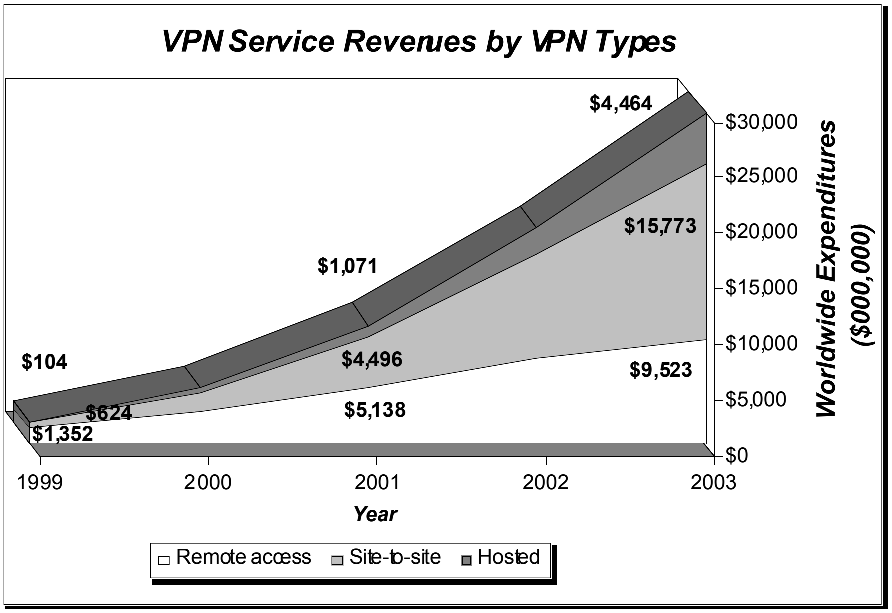

Figure 4. Revenue Forecast by VPN Type

C. VPN Service Revenue Forecast by Task

Table 6 and Figure 5 provide revenue forecasts by VPN tasks.

1. VPN design includes revenues for network assessment and design services, such as determining network bandwidth and transport technology requirements.

2. VPN integration includes revenues for network integration services such as initial installation and configuration of network hardware and software supporting VPNs.

3. VPN operations/support/bandwidth includes revenues for ongoing management of the network aspects of VPNs, such as monitoring network activity, configuring hardware and software, future network planning, ongoing charges for both dial-up and dedicated bandwidth, and supporting end-users.

4. VPN security design, integration, operations, and support include revenues for design, integration, and operations and support of the security aspects of VPNs, such as defining and maintaining security policies, managing user authentication, installing and managing firewalls, installing a public key infrastructure, and operating a certificate authority.

5. Standalone VPN bandwidth purchase includes revenues for dial-up and dedicated bandwidth and QoS related to that bandwidth, sold for VPN use to organizations deploying CPE-based VPNs and handling their own network and security design, integration, and operations and support.

TABLE 6. VPN TASK REVENUE PROJECTIONS

Tasks	**Millions ($000,000)**				
	1999	**2000**	**2001**	**2002**	**2003**
Design	$42	$102	$321	$782	$1,190
Integration	$125	$384	$1,071	$1,954	$3,274
Operations/ support/ bandwidth	$541	$1,611	$3,747	$8,011	$13,690
Security	$229	$716	$1,606	$3,322	$5,357
Standalone bandwidth	$1,144	$2,302	$3,961	$5,471	$6,250

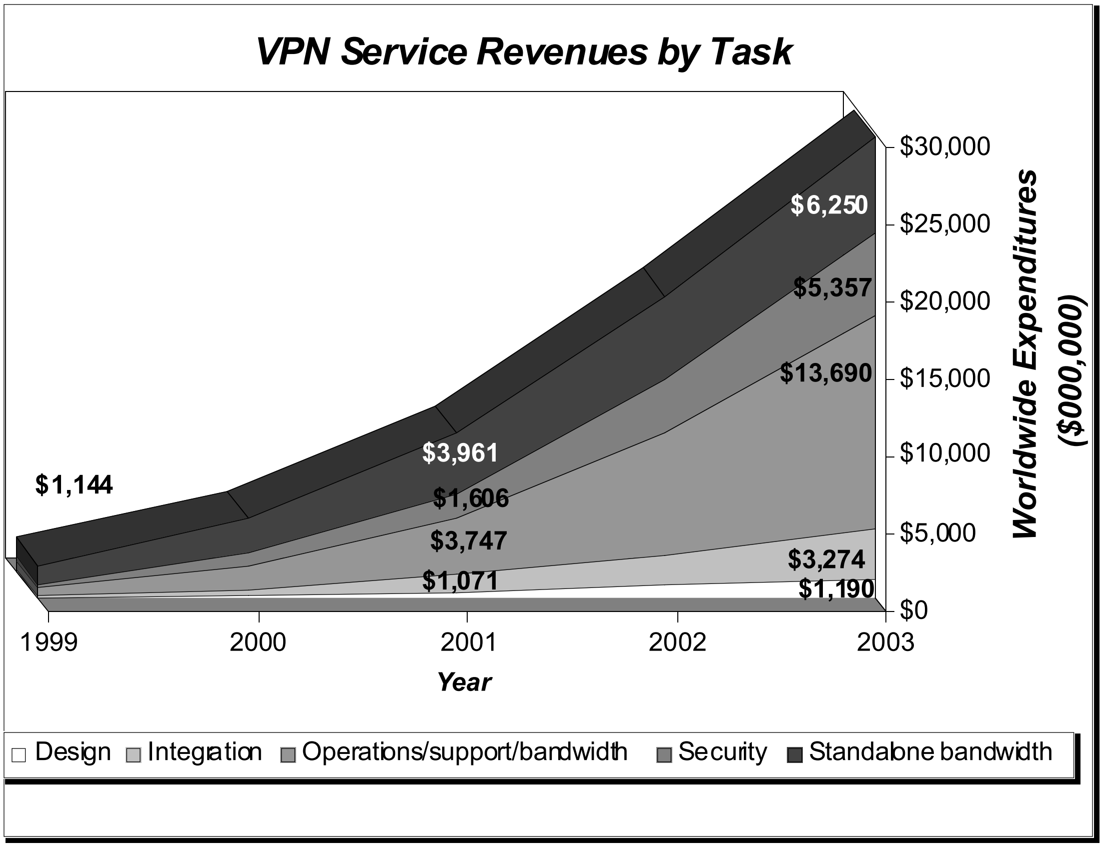

Figure 5. VPN Service Revenues by Task

Appendix II. Enterprise VPN Checklist

Use this checklist to identify the VPN class which best fits your needs, and to identify the resources you'll use for planning, design, installation, and ongoing monitoring, maintenance, and support. Be sure to consider anticipated growth over the next 2 to 3 years in addition to today's needs, and be sure that your VPN can grow and expand while preserving initial investments.

ENTERPRISE VPN CHECKLIST

Number of Intranet Sites (Domestic/Int’l) *(If 1 site only, consider Class 0 VPN; For 2-10 sites, consider Class 1; Less than 100 sites, Class 2; 100’s of sites, Class 3; 1000’s of sites, Class 4; If international sites, note potential export issues)*	Year 1	Year 2	Year 3
Number of Remote Users *(If <50 users, consider Class 0 VPN;50-250 users, Class 1; 250-500 users, Class 2; 1000’s of users and/or xDSL/cable modem access, Class 3; 10,000’s, Class 4)*	Year 1	Year 2	Year 3
High Value Information? *(If YES, consider Class 2 or above)*	Type of Information:		
Extranet Partners? *(If YES, consider Class 3 or above; If many partners with their own PKI, consider Class 4)*	Extranet Partners:		
Time-Sensitive Applications? *(If YES, consider Class 3)*	Applications and round-trip latency guarantee required:		
Voice or Video Applications? *(If YES, consider Class 4)*	Amount of voice and video traffic (avg./peak)		

VPN Design/Implementation Task	**Resource(s) Employed**	
	Insource (Who)	**Outsource (Who)**
VPN Architecture		
Network Analysis/Audit		
Network Design		
Security Analysis/Audit		
Security Policy Assessment/Design		
Network Installation/Integration (Local/Domestic)		
Network Installation/Integration (Remote/Int’l)		
Security Installation/Integration (Local/Domestic)		
Security Installation/Integration (Remote/Int’l)		
On-site N/W Support/Maintenance (Local/Dom)		
On-site N/W Support/Maintenance (Rem/Int’l)		
On-site Security Support/Maint (Local/Dom)		
On-site Security Support/Maint (Rem/Int’l)		
Network Monitoring Services		
Security Monitoring Services		

Appendix III. Service Provider VPN Checklist

There are two parts to this checklist: Part 1 identifies key characterictics of the planned VPN offerings. Part 2, on the following page, identifies the resources that will be used to implement the service.

SERVICE PROVIDER CHECKLIST – PART 1: SERVICE DEFINITION
Classe(s) of VPNs offered:
Year 1
Year 2
Year 3
CPE-based services (Yes/No/Types):
Core-based services (Yes/No/Types):
Positioning of VPN offerings vs. current services:
Leased Line:
Frame Relay:
800 RAS:
Other:
Access services supported: (Dial, ISDN, xDSL, Cable, FT1, T1, Multi-T1, DS3, OC3, OC12, OC48, OC96)
SLA parameters (throughput, latency, availability, security):
SLA validation metrics:
SLA geographic coverage:
Bandwidth Management Services:

SERVICE PROVIDER CHECKLIST – PART 2: RESOURCE IDENTIFICATION

Key: I = Insource; O = Outsource; C = Provided by Customer

Network Services:

Network assessment/audit service (I/O/C, in current service area):

Network assessment/audit service (I/O/C, outside current service area):

Network design service (I/O/C, in current service area):

Network design service (I/O/C, outside current service area):

Network installation & maintenance service (I/O/C, in current service area):

Network installation & maintenance service (I/O/C, outside current service area):

Network monitoring & management service (I/O/C, in current service area):

Network monitoring & management service (I/O/C, outside current service area):

Sell CPE (Y/N):

Bundle CPE into offering (Y/N):

Security Services:

Security assessment/audit service (I/O/C, in current service area):

Security assessment/audit service (I/O/C, outside current service area):

Security design service (I/O/C, in current service area):

Security design service (I/O/C, outside current service area):

Security installation & maintenance service (I/O/C, in current service area):

Security installation & maintenance service (I/O/C, outside current service area):

Security monitoring & management service (I/O/C, in current service area):

Security monitoring & management service (I/O/C, outside current service area):

Sell CPE (Y/N):

Bundle CPE into offering (Y/N):

Support Services:

Help desk (I/O/C, site-to-site, in service territory):

Help desk (I/O/C, site-to-site, outside service territory):

Help desk (I/O/C, remote access, in service territory):

Help desk (I/O/C, remote access, outside service territory):

Billing:

Billing basis (site-to-site):

Billing basis (remote access):

Billing basis (extranet):

Billing basis (hosting):

Billing variables (time of day, class of service, other):

Usage statistics required from CPE:

Service Launch:

Sales training (I/O):

Technical training (I/O):