May 28, 2003

Connecticut Office
803 Warrenville Road
Mansfield Center, CT 06250
860.429.0100

Texas Office
2208 Columbia Drive
Flower Mound, TX 75028
972.874.7791

Virginia Office
PO Box 17858
5 Paxton Road
Richmond, VA 23226
804.288.6864

www.telechoice.com

CB065034

IP-VPN Deployment Decisions and the Business Case for IP-VPN Managed Services

Prepared for: Nortel Networks

Introduction

Today’s enterprises have many needs that can vary due to their size and physical infrastructure. Single locations, multiple locations, mobile workers, telecommuters, etc. These enterprises all have one thing in common though: *They need to securely connect all of their workforce locations internally with each other and with the outside world.*

It’s not simple to securely connect everyone together. To consider how this requirement can quickly become complex, look at the following equation:

The need to support a wide variety of communications media
+
Highly distributed locations
+
Employees who expect access to corporate data no matter where they are (home, customer site, travel location)

All but the largest enterprises do not usually have in-house staff to support the technologies to meet these needs. Choices can be confusing and mistakes costly. Hardware or software? In-house or external IT skills? Which technology to use? Provider-managed or self-managed?

The wrong choice might not only be costly to your budget, but could also leave your organization’s data exposed and/or leave your firm unable to keep up with growth in your data networking needs.

A popular solution for an enterprise’s secure networking needs is a virtual private networking (VPN) solution. A VPN is defined as a network of virtual circuits that allows users to conduct private communications through public or shared infrastructure. VPNs are hot topics for most businesses. A survey of 436 users on VPN functionality by In-Stat/MDR (February, 2003) found that, of the respondents, 89% currently have or will have VPNs within the next two years. An IP-VPN is a virtual private network that uses the Internet Protocol (IP) for routing; IP represents the vast majority of data traffic in use today.

This paper will discuss the main enterprise applications that VPNs enable, the different VPN options available, and how these different VPN alternatives fit with resolution of the application requirements. (For the purposes of this paper, when we talk about VPNs, we’re talking about IP-VPNs exclusively.) The enterprises we will focus on in this paper are small and medium enterprises (or SMEs).

IP-VPN Solution Sets

When considering VPN deployment, there are four common solution sets that usually meet the needs of the enterprise:

1) Remote Access
2) Site-to-Site (Intranet) Connectivity
3) Extranet Applications
4) Security Solutions

A company might need one or all of the above in implementing their VPN.

Remote Access

For many enterprises, enabling remote access to corporate resources is a challenge due to the complexity and expense associated with traditional solutions — such as RAS (Remote Access Server)-based deployments — and the security concerns related to allowing individuals to gain access using their own personal dial-in accounts. Outsourcing remote access is a way to reduce the capital and operational expenses of their current in-house solutions, while at the same time boosting security of those connections.

Site-to-Site (Intranet) Connectivity

Branch office locations need access to all of the information available in the main headquarters location. Dedicated connectivity between sites can become a costly proposition for all but the largest enterprises. As employees connect to headquarters via different transport media, how does data stay secure? This is particularly true where more and more sites are using shared access mechanisms such as cable modems for their small business' Internet access.

Extranet Applications

As companies want to communicate with customers and partners in an expedited and secure fashion, the issues mentioned under site-to-site connectivity become exponentially more complex. You now have many more remote locations and transport media potentially involved in accessing your corporate data. Security issues are heightened when letting external users onto your network — keeping these users out of the private areas of your network while allowing them access to shared data and applications is paramount.

Security Solutions

Of course, security is key in all three scenarios mentioned above, as a means of ensuring that users only access information for which they have been approved. However, many enterprises require additional protection to further secure their networks and protect themselves against intruders who seek to gain control of a computer to launch additional attacks, extract private data, and/or masquerade as a legitimate user in order to perform other destructive activities across a network.

IP-VPN Deployment Options

There are basically four options available in the marketplace today for VPN solutions:

1) Customer-managed CPE

2) Provider-managed CPE

3) Network-hosted

4) Hybrid VPN solutions

In the past, customers have been predominantly focused on CPE-driven solutions. But today, companies will increasingly find that they may deploy both CPE and network-hosted solutions in their enterprise, customizing the VPN solution based on the needs of any particular division or site.

Customers are increasingly comfortable with having their carrier more closely involved with their security solution, either by managing CPE or by hosting the VPN in the network. Of those enterprises currently having VPNs in place, a whopping 74% would consider switching to provider-managed services, according to In-Stat/MDR (February 2003). Within this same group, 72% would be interested in a service that allows for class of service to be implemented to support their VPN traffic. In-Stat/MDR outlined the main drivers for those who are thinking of migrating from a do-it-yourself to a provider-managed solution: 1) the ability to reduce ongoing operating costs, 2) reduce IT headcount, 3) collapse multiple networks and 4) reduce the number of access circuits required.

Parks Associates in a March of 2003 study also found a great willingness in the SME market to utilize managed services. About half of the companies reviewed were already using some form of managed services. Managed security services ranked second of those already in use, with managed VPN services following at fourth.

Customers in certain market verticals are more prone towards managed CPE and network-hosted solutions than others. Research by TeleChoice (2003) found that SMEs in market segments with lower security risk exposure were very interested in carrier-driven solutions. Conversely, Financial and Healthcare organizations – two groups where security and privacy issues are paramount – were very focused in retaining hands-on control of their connectivity solutions due to the consequences to their companies if there were a breach of this data.

Customer-managed CPE Solutions

In a CPE-based solution, all functionality and equipment is deployed by the enterprise. The enterprise will also manage and monitor the VPNs in this scenario. The enterprise’s management or IT staff needs to stay aware of the current market options, stay abreast of the best solution to fit their needs, and evolve the solution to match growth and organizational change. Quite often, this is only a fit for the larger enterprise organizations with a knowledgeable in-house IT staff.

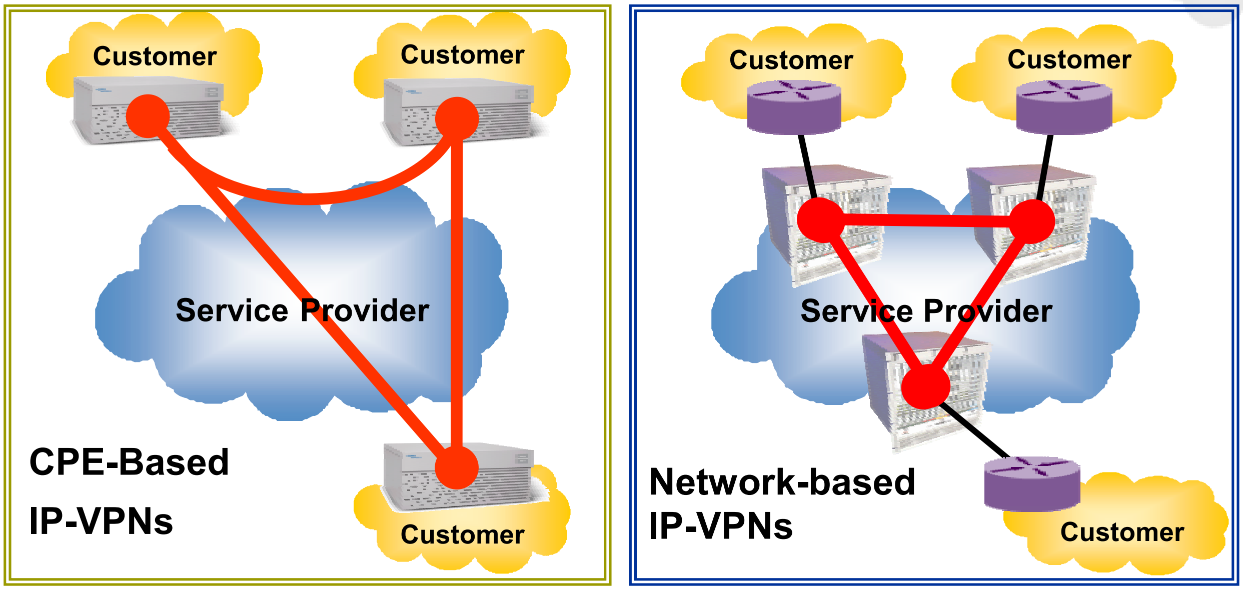

Diagram 1: IP VPN Options

Provider-managed CPE Solutions

The network architecture for provider-managed CPE solutions is quite similar to that of the customer-managed CPE solutions. The difference lies in where the responsibility lies regarding the management of the CPE and connectivity between locations. With provider-managed CPE solution, the carrier is responsible for both the management of the connectivity between locations, as well as for the CPE on the customer premises that enables the VPN functionality. This CPE might be owned by the customer or provided as part of the provider-managed service.

Provider Network-hosted Solutions

A network-hosted solution can be offered where all functionality is hosted in the carrier's network on powerful carrier-grade platforms, which can be rich in IP service capabilities. By utilizing functionality deployed in the carrier's network, customers can take advantage of solutions deployed to serve thousands of users. This can increase the number of advanced services available to them, decrease the time for implementation of these services, and potentially reduce costs.

Hybrid VPN Solutions

In a hybrid solution, a combination of functionality is utilized. Some of this functionality is based in the carrier's network while additional functionality remains at the customer premises. This functionality is networked together, acts in tandem, and is typically managed by the carrier.

Provider-Managed IP VPN Services

Although customer-based VPN solutions have been around for quite a few years, their users are often faced with challenges related to cost, scalability, and manageability. Provider-managed IP VPN solutions provide a similar level of security without many of these same challenges.

As mentioned earlier in the document, there are two options available with provider-managed solutions:

1. *Provider-managed CPE*, where the carrier is managing VPN CPE placed on the customer premises and — most likely — the connectivity between the CPE and the carrier network. The CPE might be owned by the enterprise or provided by the carrier as part of a managed service.

2. *Provider network-hosted*, where all functionality is provided from within the service provider's network.

People often are concerned about moving towards a provider-managed solution because they automatically think it will be more expensive. Indeed, pricing is structured differently under managed services, with an emphasis on monthly and annual fees as opposed to the mostly one-time fee under customer-driven CPE solutions. But other operational costs and ongoing management costs creep in when you are managing it yourself, and before you know it, you are spending a lot more time on your VPN applications than you thought you would be — and we all know that time is money. Indeed, it was this user experience that prompted the development of provider-based VPN services to begin with.

So when evaluating these provider-based solutions, don't just focus on the cost of the solutions, but give equal treatment to understanding the versatility of these solutions and how they offload a lot of the ongoing aspects of VPN capability and management. Oftentimes, this versatility is where you find the greatest substantial business value.

Exact service descriptions from carriers will vary depending on what services they offer, the types of managed CPE they offer, the degree to which this is bundled with other services offered by the carriers, etc. In general, though, with provider-managed CPE services, the provider is acting as your outsourced staff and coordinating all your configuration and ongoing management of your equipment, access lines, and network services to support your VPN application. With the provider hosted-network services, it is much the same except the CPE may be totally or partially subsumed by network capabilities.

These relieve the enterprise of the responsibility for securing the appropriate access technology to each location enabled with IP VPN support, for acquiring and pre-configuring CPE for each location, for managing upgrades and daily chores, and for the overall hardware, software, and network infrastructure associated with the application.

The Benefits of Provider Managed and Hosted Solutions

When deciding which type of VPN solution best fits your enterprise's needs there are some key criteria to keep in mind among the options we have mentioned to so far — provider network-hosted, provider-managed CPE, or customer-managed CPE-based do-it-yourself solutions. The benefits of a provider-managed CPE or provider network-hosted solution are detailed below:

- ✓ *Operational Cost Savings* — By utilizing functionality deployed in the service provider's network, you are basically able to outsource this requirement for a single monthly fee. This reduces the ongoing internal requirements other solutions would require for the in-house personnel to install, maintain, and manage this functionality.

- ✓ *Capital Cost Savings* — In line with reduced operational costs, the up-front capital requirements to get VPN functionality up and running are reduced relative to a do-it-yourself solution. Even a provider-managed CPE solution could include all or a portion of the required equipment in your monthly fee.

- ✓ *Scalability* — With provider-managed solutions, the addition of new users, locations or policies just requires a phone call to your carrier. The need to determine the hardware and software requirements to support these users no longer falls on the enterprise's shoulders. New Web-based interfaces are making it easier for you to manage your own VPN settings as well.

- ✓ *Centralized Policy Control and Management* — The service provider is able to manage all of your policy requirements in one location and apply them across all users, locations and applications that apply to your enterprise's needs. The virtual routing or virtual forwarding function in the carrier's network will conduct all of the policy management required in order to allow for specific performance levels of applications and user traffic, based on those policies set by the enterprise.

- ✓ *Security Management* — In addition to these policy management functions, the carrier can also provide additional security solutions via their network infrastructure. These might include firewall, virus scanning and intrusion detection, to name just a few examples. Authentication, encryption and tunneling functions can be managed either in the network or in the CPE, depending on the approach.

- ✓ *Adaptability* — Carriers can expand the VPN network quickly and economically versus the enterprise having to buy new equipment and re-configure their network to react to growth, mergers and acquisitions, organizational changes, etc.

- ✓ *Network QoS control* — Carriers can supply and guarantee performance on their network.

- ✓ *Risk Reduction* — The enterprise can reduce their risk by allowing the carrier to determine the appropriate evolution path for their VPN requirements as their organization evolves.

The ability to utilize provider-managed VPN solutions can allow a SME to present itself to the world as a larger enterprise. By utilizing assets deployed in the carrier's network, a business can take advantage of advanced services they could never afford to deploy on a do-it-yourself basis with a limited budget.

Let's not forget that there are also some challenges associated with provider-managed solutions that the enterprise should be aware of:

- ✓ *Ensuring End-to-End Security* —CPE solutions inherently provide end-to-end encryption of data packets, which is not typically the case with network-hosted solutions. The trade off to consider here is the hardware and personnel requirements necessary to provide this higher level of end-to-end security.

- ✓ *CPE Still A Requirement* — Some solutions will still require additional CPE in order to ensure an adequate solution — for example, intrusion detection services may require installation of CPE devices.

Indeed, the In-Stat/MDR survey noted earlier found that those who are still hesitant about the provider-managed scenario have concerns that mostly relate to the ability to control security features and a general need for control on the part of some users. So CPE solutions will probably continue to be part of the VPN in some enterprises.

Table 1: Deciding Among IP-VPN Deployment Options

Issues to Consider	Key Factors	Do-It-Yourself CPE	Provider-Managed CPE	Network -Hosted
Costs (trying to do more with less)	▪ Reduce monthly outflow of operational dollars	✓		
	▪ Reduce capital asset purchase requirements		✓	✓
Headcount (in-house skill set)	▪ Requirement for in-house IT staff to maintain and manage VPN solutions	✓		
Control	▪ How much control is required over VPN solutions	✓	✓	✓
Quality of Service	▪ Different levels of guaranteed performance may be required o By application o By user o By location o By time of day o By destination/ origination			✓
Network Support	▪ 24x7 technical support		✓	✓
	▪ Ease of scalability		✓	✓
Level of comfort with technology risks	▪ Reduce the risk of owning a solution that fails to keep pace with your needs		✓	✓

IP-VPN Business Solution Case Studies

In the sections that follow, we will discuss three potential solutions that address enterprise requirements in today's business environment.

1. IP-VPN Security Solution
2. IP-VPN Remote Access Solution
3. IP-VPN Site-to-Site (Intranet and Extranet) Solution

We then follow with a section summarizing the conclusions that can be drawn from the use of provider-managed solutions to solve these problems, and then provide business case comparisons to help highlight the differences in costs among the among customer-managed do-it-yourself, provider-managed CPE, and provider network-hosted solutions. In the Appendix, we provide financial comparisons drawn from the Nortel IP-VPN Business Case Model that help you understand the bottom line costs of the different approaches to IP virtual private networking.

Business Case Study #1: Security Solutions

SMEs continue to rapidly adopt broadband Internet access for conducting business, researching/collecting information, and communicating, for both intra-company as well as with external customer and partner communication. With this increased use of the Internet comes added concern for the security of business information. Although many SMEs have already thought about virus scanning, control software, and manual configuration steps to help keep PCs clean of undesirable items, many companies require additional protection to further protect and prevent against intruders who seek to gain control of a computer to launch additional attacks, extract private data, and/or masquerade as a legitimate user in order to perform other destructive actions across a network.

The many techniques hackers can use to compromise a PC make it particularly difficult for the enterprise to ensure protection on its own. This challenge results in an increasing need and demand for outside assistance in order to keep up with the current requirements for protection as technology continues to evolve. The key functionality an enterprise may choose to add to their basic IP VPN service could include firewall, virus scanning, intrusion detection, denial of service and anti-spoofing. The definitions for each of these security solutions are as follows:

- ✓ *Firewall (basic or managed)* — A firewall keeps traffic from entering your network that should not enter your network. A basic firewall uses simple, static rules to allow certain forms of traffic and denying inbound traffic initiated externally. A managed firewall would allow for additional firewall policy control and greater granularity over what is allowed onto the network by the basic firewall.
- ✓ *Virus Scanning* — Virus scanning checks any inbound email, Instant Messaging, or other inbound traffic to look for harmful viruses. Any infected traffic would be isolated until the virus is resolved.
- ✓ *Intrusion Detection* — Intrusion detection (and more recently prevention) is aimed at enterprise users who require a level of security above the basic or managed firewall solutions.

- ✓ *Denial of Service (DoS) Attack Protection* — This protects your enterprise from hackers who utilize DoS attacks to disable a server or network connection.
- ✓ *Anti-Spoofing* — Spoofing is another common technique used to masquerade as a legitimate IP address, but actually direct traffic to an insecure location.

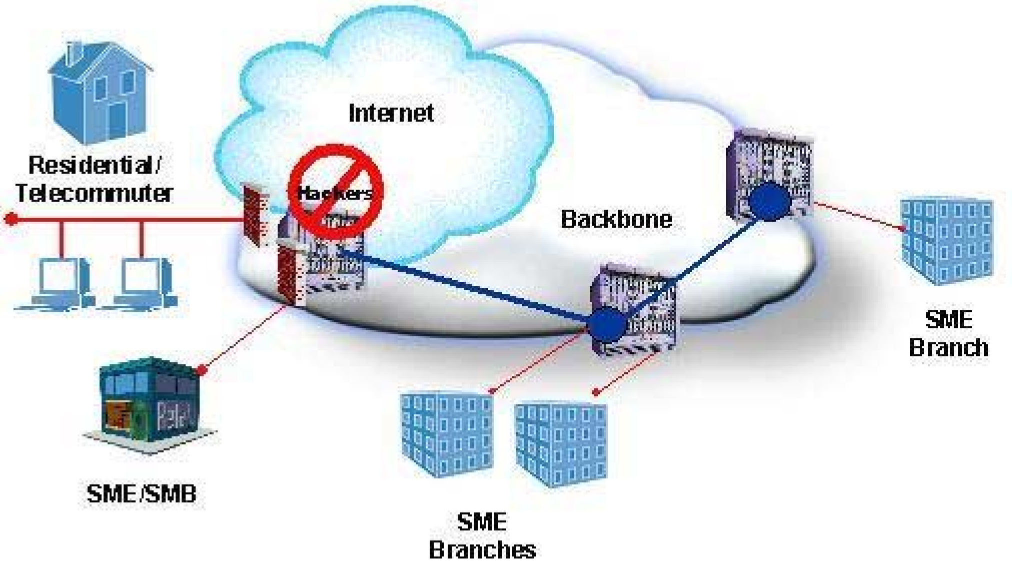

Diagram 2: Security Solutions

Business Case Study #2: Remote Access Solutions

As more SMEs enable external remote access to corporate resources, they find they are challenged due to the complexity and expense associated with traditional solutions — such as RAS (Remote Access Server) — and the security concerns of allowing individuals to gain access on their own through personal ISP accounts. Remote access solutions can become a part of your overall IP VPN solution set to help link security with connectivity.

When an enterprise looks to resolve remote access functionality there are three main categories which need to be addressed — how dial-up users will be supported, how broadband users will be supported, and how all users will be authenticated.

- ✓ *Dial-Up Access* — Accomplished via a software client residing on the user's PC, access to local dial Internet connectivity, and centralized management and policy enforcement.
- ✓ *Broadband Access* — Basically accomplished via the same provider-managed solution as the Dial-Up Access user.
- ✓ *Authentication* — Supported via a two-level authentication mechanism, including username and password authentication of remote users via RADIUS from within its network-based solution.

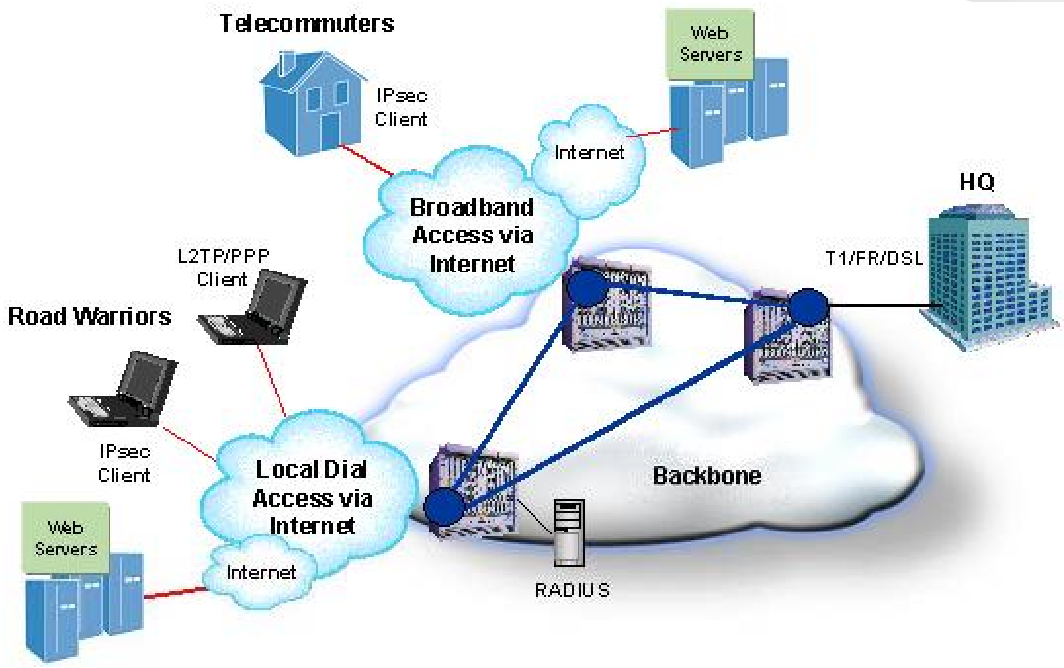

Diagram 3: Remote Access Solutions

Business Case Studies #3: Site-to-Site (Intranet and Extranet) Solutions

In addition to remote access solutions that allow mobile employees and telecommuters to securely reach corporate data, there are scenarios where branch or regional office locations need to be connected to the corporate LAN in order to access Intranet applications. This same type of functionality can be extended to partners, suppliers and customers who wish to conduct Extranet applications.

Provider-managed solutions resolve site-to-site connectivity needs on a per site or a per subscriber basis. Some of the functionality offered by a provider-managed solution includes:

- ✓ *Access* — Ethernet, DSL, cable, wireless, ATM, frame relay, and private line.
- ✓ *IP VPN Port* — This port is the connection point to the carrier's backbone network. Provider-managed solutions are able to customize the way traffic is delivered from a bandwidth management perspective via enhanced capabilities such as rate limiting, queuing, traffic shaping and policing capabilities based on application type, TCP port number, source/destination, or IP address.
- ✓ *IP-VPN transport* — IP VPN Transport comes in two flavors:
    - o Encrypted (typically with IPSec; used when data is traversing a non-trusted network)
    - o Unencrypted (traversing MPLS or various layer 2 carrier networks which are considered trusted, much the way Frame Relay networks are trusted)
- ✓ *Direct Internet access* — Direct Internet access not only delivers better connection performance to the individual locations, but also results in the off-load of such traffic from having to traverse corporate WAN links, resulting in more efficient bandwidth utilization.

✓ *NAT/PAT (Network/Port Address Translation)* — NAT/PAT is an Internet-standard means of hiding internal network addresses from would-be attackers while providing a public address for legitimate users/applications to inter-operate with your network.

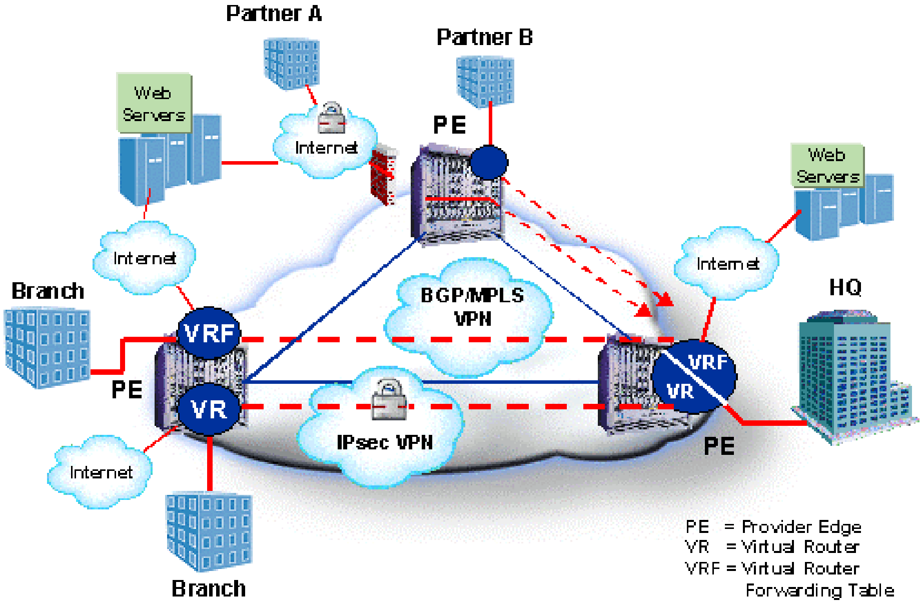

Diagram 4: Site-to-Site Solutions

Conclusions from Business Case Studies

In weighing the pros/cons of solutions provided by a carrier, there are many items to consider. First and foremost is that all functionality is enabled from the carrier's network or from provider-managed CPE. This eliminates a great deal of complexity on the part of the enterprise and reduces upfront and ongoing costs of providing the functionality. This also allows your IT staff to focus on other important functions essential to your business. A single point of contact is available for enterprise service components and that contact is available 24x7.

On the flip side it must also be considered that managed CPE solutions (provider- or customer-based) will also carry a higher level of security than network-hosted solutions, but may also carry a much higher cost. Customers also do not have to work with a third party when they want to make changes to their own customer-managed solutions. Finally, with customer-managed solutions, there is greater flexibility to change network elements since you are network-carrier agnostic.

Presented below is a table representing the key drivers influencing the business case between customer-managed CPE, provider-managed CPE, and network-hosted solutions. The scenarios presented include the firewall piece of a security solution, remote access plus VPN functionality and site-to-site solutions to support Intranet and Extranet functionality.

Table 2: Key Business Case Cost Factors

IP VPN Components	Customer-Managed CPE IP VPN Service	Provider-Managed CPE IP VPN Service	Network-Hosted IP VPN Service
Capital Considerations	$3,000 one time charge (per site)	$300 per month lease (per site)	$0
Installation Considerations	$2,400 one time charge (per site)	$1,500 one time charge (per site)	$600 one time charge (per site)
Monthly Service Provider Fee Considerations (Includes access, transport, management and maintenance charges)	$3,100 per month (HQ) $80 per month (per user location)	$2,100 per month (HQ) $130 per month (per user location)	$2,100 per month (HQ) $130 per month (per user location)

Presented in an appendix following the conclusion section of this document are more details from the high-level business cases that support these analyses.

Final Thoughts

SMEs have many choices in their deployment of a corporate VPN, across a rich spectrum of in-house and provider-managed alternatives. In this paper, we’ve seen some compelling arguments for the provider-managed alternatives, both provider-managed CPE and fully network-hosted solutions. Throughout this paper you have seen cost concerns come to the forefront of the list of reasons an enterprise might consider the adoption of solutions other then customer-managed CPE options. Cost is certainly important in the current economic climate, but features and functionality should not be overlooked. The ability to streamline electronic communications both internal to and external to your organization can add substantial improvements in productivity, which also rolls to the bottom line. The ability to offer partners, suppliers, and customers more advanced options for interaction can allow you to present your organization as a larger, more sophisticated one to the external marketplace. This ability to more fully and securely interoperate with external organizations may in turn open up opportunities you may not have had access to otherwise. The reduction of risk associated with VPN requirements is also important. As your enterprise evolves, the carrier can supplement your scarce IT resources to ensure an adequate solution for your needs.

In the past, many IT managers have stayed away from provider-managed solutions because they felt it deprived them of their hands-on, value-add to the organization. Now, however, IP-VPN solutions have evolved to provide managers with a deep degree of control so they can still control their security solutions, while benefiting from the scale and reliability of provider-based solutions. As shown in this discussion, provider-managed IP VPN services can truly change the business model for SMEs and should be strongly considered when setting up or enhancing your communications solutions.

Business Case Appendix

Firewall Security

IP VPN Components (per site)	Customer-Managed CPE Hardware Firewall (per site)	Provider-Managed Hardware Firewall (per site)	Provider-Hosted Managed Firewall (per site)
Monthly cost of IP transport and access (Business Class DSL or fractional T-1)	$500 per month	$500 per month	$500 per month
Cost of Firewall CPE (e.g., NetScreen)	$600 one time	$50 per month (Recurring lease expense)	$0
Installation and initial set-up cost.	$800 one time Based on 8 hours per site at $100 per hour (fully loaded technician costs)	$500 one time	$200 one time Configured via portal interface or remote management facility by the service provider
Customer costs of management and maintenance of firewall CPE ($100/ hour @ 3 hours per month)	$300 per month ($100/hour @ 3 hours per month)	$0	$0
Monthly service provider fee for managed IP VPN service	$0	$150 per month	$150 per month
One-time costs (per site)	$1,400	$500	$200
Monthly costs per site	$800 per month	$700 per month	$650 per month
Total 1st Year Costs per site	$11,000	$8,900	$8,000
Total 1st year savings from managed security services based on 5-site network		**$10,500**	**$15,000**

VPN plus Remote Access

IP VPN Components (per site)	Customer-Managed CPE IP VPN Remote Access (per site)	Provider-Managed CPE-based Remote Access (per site)	Network-Hosted IP VPN Remote Access Service (per site)
Monthly cost of IP transport and access (T-1 for main site, SOHO DSL for remote)	$500 per month for main site, $80 per month for remote SOHO users	$500 per month for main site, $80 per month for remote SOHO users	$500 per month for main site, $80 per month for remote SOHO users
Cost of VPN CPE (e.g., NetScreen)	$1,200 one time	$125 per month recurring lease expense	$0
Installation and initial set-up cost.	$800 one time Based on 8 hours per site at $100 per hour (fully loaded technician costs)	$500 one time	$200 one time Configured via portal interface or remote management facility by the service provider
Customer costs of management and maintenance of VPN CPE	$900 per month ($100/ hour @ 4 hours per month for main site, .5 hour per remote user supported)	$0	$0
Monthly service provider fee for managed IP VPN remote access	$0	$700 per month ($200 per month, $50 per remote user)	$700 per month ($200 per month, $50 per remote user)
One-time costs (per site)	$2,000	$500	$200
Monthly costs per site	$1,400 per month main site, $80 per remote	$825 per month main site, $130 per remote	$700 per month main site, $130 per remote
Total 1st Year Costs main site plus 10 remote access	$28,400	$26,000	$24,200
Total 1st year savings from VPN and remote access services based on 10 remote access users		**$2,400**	**$4,200**

Firewall plus Site-to-Site IP VPN Services

IP VPN Components (per site)	Customer-Managed CPE IP VPN Service (per site)	Provider-Managed CPE IP VPN Service (per site)	Network-Hosted IP VPN Services (per site)
Monthly cost of IP transport and access (Business Class DSL or fractional T-1)	$500 per month	$500 per month	$500 per month
Cost of VPN CPE (e.g., NetScreen)	$1,200 one time	$125 per month recurring lease expense	$0
Installation and initial set-up cost.	$800 one time Based on 8 hours per site at $100 per hour (fully loaded technician costs)	$500 one time	$200 one time Configured via portal interface or remote management facility by the service provider
Customer costs of management and maintenance of VPN CPE ($100/ hour @ 4 hours per month)	$400 per month ($100/hour @ 4 hours per month)	$0	$0
Monthly service provider fee for managed IP VPN service	$0	$250 per month	$250 per month
One-time costs (per site)	$2,000	$500	$200
Monthly costs per site	$900 per month	$875 per month	$750 per month
Total 1st Year Costs per site	$12,800	$11,000	$9,200
Total 1st year savings from managed security and VPN services based on 5-site VPN		**$9,000**	**$18,000**

Notes