



WHITE PAPER

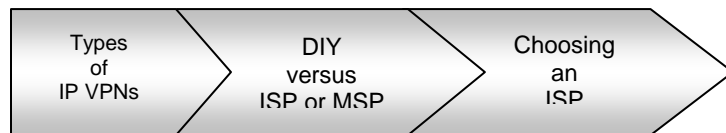
Implementing an IP VPN

Introduction

This White Paper is intended for those who have already assessed their WAN requirements and determined that they would be best served by an IP VPN solution. This decision may be due to any number of factors, including the ability to:

- Keep their data private and protect IT resources from malicious attacks
- Leverage the Internet to reach numerous locations throughout the U.S. or around the world
- Use an efficiently meshed topology to facilitate direct communication among sites
- Allow remote users/sites to access the network via their local ISP (dial-up, cable or DSL)
- Deploy an Extranet that business partners can access via their existing Internet connection
- Provide branch offices with direct access to the Internet and the WAN over a single circuit
- Provision higher bandwidth for demanding applications like remote data storage
- Accommodate bursty applications without compromising performance
- Converge a variety of applications over a single WAN infrastructure for greater efficiency

Now, it is just a matter of deciding which *type* of IP VPN best suits your needs, *how* to deploy these various types of IP VPNs, and *which* IP VPN service provider to choose. Once you know these answers, you'll be able to implement the IP VPN solution that's right for your business.



Types of IP VPNs

There are two general categories of IP VPNs, CPE-based and Network-based, but for each of these there are a variety of technologies and numerous ways that they can be implemented.

CPE-based IP VPNs

The original approach to building a CPE-based IP VPN was to deploy Firewalls with VPN capability at each location, using IP Security (IPSec) to encrypt the data from site-to-site. For this approach, companies typically used a software based Firewall/VPN, such as Check Point, running on a standard Unix server or purpose-built appliance. More recently, however, Firewall/VPN appliances have been introduced with Application Specific Integrated Circuits (ASICs) that encrypt/decrypt data much faster than software. A more

recent approach has been to integrate the VPN encryption functionality into the router. Since each location needs a router, this “single-box” approach tends to be much more cost-effective and is easier to manage.

Advantages

The primary advantage of using a CPE-based approach is that it encrypts/decrypts data at the customer premise, thereby ensuring the highest level of protection across the entire WAN. As a result, one can even send data across the public Internet with the comfort of knowing that even if someone intercepted it, they would have an extremely difficult time decrypting and exposing the information and/or using it to compromise the sender and destination sites.

This ability to use the public Internet makes the CPE-based approach an ideal solution for sites that are connected to the Internet via different ISPs, such as business partners of autonomous corporate divisions (e.g., as a result of an acquisition). It is also an efficient solution for providing access to telecommuters and mobile workers, since most VPN equipment include VPN client software for these remote users. This software, running on the individual's PC, may be somewhat slower at encrypting/decrypting data than would a separate appliance or server, but deploying a VPN appliance each individual's location would not be economical or, in some cases, even practical (e.g., 'on the road'). It also would allow any user at the site (i.e., their home) to access the corporate network. Since many teleworkers have family members or other potential users at their home who should not have access to the corporate network, using a VPN appliance is not advised.

Another instance where a CPE-based approach makes sense is where the company has offices in distant locations around the world, all of which are not served well by a single provider or where using the local ISP can be much more cost-effective than a single provider. In these cases, as with any CPE-based VPN, there is no additional technology necessary or modification required to the service provider's network making it feasible to extend one's VPN to virtually anywhere one has access to the Internet.

Disadvantages

The primary disadvantages of a CPE-based IP VPN are the cost and time associated with deploying and managing the CPE and Hub site equipment, and administering the site-to-site VPN tunnels. Naturally, the more sites one has, the more equipment one needs to purchase, deploy and manage. While some CPE manufacturers offer software to manage all of one's VPN devices from a single interface, this software is usually quite expensive. In fact, it is designed for service providers, who are, for this reason, typically called upon to manage large CPE-based IP VPNs. Some service providers will bundle the cost of the equipment into a single monthly service charge. And, of course, most service providers will facilitate deployment by pre-

configuring and shipping the equipment to each site and then provide the ongoing management service – saving the user considerable time effort.

Managing CPE-based VPNs can consume considerable time and effort, especially for those that require a high degree of site-to-site connectivity, or “meshing,” particularly if these virtual connections, or “tunnels,” change frequently. Such frequent changes may be due to sites being added/removed from the network or because of the dynamics of one’s business. The issue here is that with the CPE-based approach one needs to set up each site-to-site tunnel by configuring both the equipment at both locations. This makes it extremely time consuming to add a new location to a large meshed network, since it means you update the configuration at all of the other recipient. So, the economics of deploying and managing a CPE-based approach are unfavorable for large or growing WANs. CPE-based IP VPNs also typically do not provide the level of performance associated with a network-based IP VPN because data traverses the public Internet versus residing on a single provider’s network.

Network-based IP VPNs

Network-based IP VPNs perform all of the site-to-site VPN functionality within the service provider’s network using either IPsec encryption or Multi-protocol Label Switched routing (MPLS). To offer IPsec network-based IP VPNs, service providers place equipment in their POPs that encrypts/decrypts customer traffic as it enters/leaves their network. This technology may also enable the service provider to provide certain network-based firewall services. To offer MPLS network-based IP VPNs, service providers run MPLS on the routers in their POPs to build Label-Switched Paths (LSPs) across their network. Each customer’s traffic is logically separated within the network, to provide similar privacy as Layer 2 technologies, like Frame Relay and ATM. This approach also enables the service provider to manage the traffic on its network more effectively and prioritize certain types of traffic over others. As a result, the ISP can offer customers distinct Classes of Service (CoS) with aggressive Service Level Agreements (SLAs) designed to support performance-sensitive applications (e.g., voice/video). The latter capability makes MPLS network-based IP VPNs the ideal choice for companies that want to converge voice and data over a single network, and have business critical applications (e.g., ERP/CRM).

In each case, network-based IP VPNs rely on the inherent security of the access technology to protect customer data en-route between the customer site and the service provider’s network. For this reason, only certain access technologies will suffice. Namely, the site should be connected via a dedicated T1/T3 local loop or a Layer 2 technology like ATM over DSL. Access technologies that do not isolate each customer’s traffic, such as Cable Internet access, do not provide sufficient protection and therefore should not be used without encryption.

If the customer wants to provide secure access for remote users, this can be achieved in several ways with a network-based IP VPN. Rather than incurring the long-distance charges of having the remote users dial in to a RAS server, as is typically done with traditional WANs, companies have their remote users access the network via the public Internet using dial-up, cable or DSL access and use VPN client software to encrypt their data, as with a CPE-based IP VPN approach. In the case of IPSec network-based IP VPNs, the equipment the service provider has in their POPs to terminate IPSec tunnels from CPE can also terminate IPSec tunnels from software-based VPN clients.

Advantages

The general advantage of network-based IP VPNs is that they require much less capital expenditure for the customer than the CPE-based approach and they limit the number of VPN tunnels that need to be managed; the maximum number of VPN tunnels is based on the number of POPs the service provider has (maximum tunnels= $n*(n-1)/2$, where n =POPs). This is particularly relevant for large, fully meshed IP VPNs, for which using a CPE-based approach would require VPN tunnels between each pair of sites.

However, the most significant advantage of an MPLS network-based IP VPN is the enhanced performance and the associated Classes of Service the service provider can offer for site that are connected via dedicated T1/T3 or Layer 2 DSL access. This capability enables customers to converge all of their data communications onto a single network infrastructure for on-net/off-net sites *and* remote users (one router, one local loop, one access port, etc.) and assign different Classes of Service to each application or source/destination address. Rationalizing network resources in this fashion minimizes capital costs, network expenses and management costs through more efficient use of personnel, equipment, and bandwidth, and enables the customer to realize tremendous economies of scale.

Disadvantages

IPSec and MPLS network-based IP VPNs each have certain minor shortcomings depending on network topology and the range of services desired. For instance, an MPLS network-based IP VPNs are limited to those sites that can be reached by dedicated or Layer 2 access technologies (dedicated T1/T3s, frame relay or Layer 2 DSL). CPE-based network VPNs, on the other hand, can reach any site that has Internet access. This is particularly advantageous for hard-to-reach locations and sites that are owned by customers or suppliers of the company deploying the network (i.e., extranet partners). Also, finally, with a CPE-based network VPN, the encryption can degrade performance and, unlike with MPLS, there is no bi-directional Class of Service capability available; performance-sensitive applications can be prioritized only in the outbound direction.

Single vs. Combined Solutions

Customers will more than likely combine various types of IP VPN technologies to address their specific WAN requirements. Only in certain cases will a single approach suffice.

Single Technology IP VPNs

Here are a few instances where it may make sense to deploy a single type of IP VPN:

CPE-based IP VPN

- Small number of sites with no meshing and no performance-sensitive applications
- All sites are located in globally diverse locations and are better served by local ISPs
- Sensitive information requires site-to-site encryption

Network-based IP VPN

- Large number of sites serviceable by one service provider
- Many sites that need to communicate with each other (meshed topology)
- Certain applications that require high performance (MPLS only)

Combined Technology IP VPNs

A combination approach allows one to address each need with the appropriate IP VPN technology and thereby create a tailored solution.

Network-based IP VPN

- Intranet connects branch offices within service provider's service area (MPLS for companies that have performance-sensitive applications)
- Centralized remote access and Internet access can be at a hub location(s)

CPE-based IP VPNs

- Extranet connects off-net business partners
- Intranet is extended to those locations outside of primary service providers' service area
- Provide site-to-site encryption for those sites with sensitive information

In cases where companies need both site-to-site encryption and enhanced performance, they may use both a CPE-based and an MPLS network-based IP VPN to connect each location.

DIY Versus ISP or MSP

If you have a small number of sites and the expertise on staff, you can deploy, configure and manage a CPE-based IP VPN without too much difficulty. However, as the number sites increase, or your network topology is meshed and changes frequently, a CPE-based IP VPN becomes difficult to manage without the appropriate software tools and resources. Add to this the level of expertise that's required to manage a large, complex network, and it becomes apparent why many medium-sized and large companies outsource this function to an Internet Service Provider (ISP) or a Managed Service Provider (MSP).

The difference between an ISP and an MSP is that, in addition to Internet access and VPNs, the latter provides a wide range of sophisticated security management and consulting services, including Managed Firewall, Intrusion Prevention, Anti-virus and Web Filtering. Most MSPs will manage CPE-based VPNs, but not all have the MPLS network infrastructure to provide network based IP VPNs. So, if you have decided on a network-based IP VPN – or a combination CPE/Network – then the choice is simple, since only an MSP can offer this service.

Choosing a Service Provider

Once you know what type(s) of IP VPN you want, and whether you want to have your service provider manage it, then you can begin evaluating them. If you plan to implement a CPE-based IP VPN yourself or with an MSP, then your choice of service provider only need be based on basic aspects of Internet service delivery.

- Ability to reach all of your locations with cost-effective access technologies
- Network reliability and performance (SLAs)
- Scope of communication services offered
- Customer support and managed services capabilities
- Value-added services, such web-based network performance monitoring

If you plan to have your service provider implement a CPE-based IP VPN (standalone or as a complement to a network-based IP VPN), then you need to consider the candidates' ability in this area. Start by narrowing the field to those service providers that support the type of VPN equipment you want to use (software and/or VPN router) and that have a strong relationship with the leading vendors in that market segment. These service providers are likely to be more knowledgeable about the latest technology, carry a more complete line of their products and have full access to the vendor's engineers for better support and services. As with any service, make sure that the service provider you choose is capable of providing the level of support you

require; if you desire, they should be able to configure, install and repair/replace your equipment on-site and monitor/manage it 24x7x365.

Companies that are looking for the enhanced scalability and lower capital cost of a network-based IP VPN must consider which technology to use, IPSec or MPLS. If enhanced performance is not a critical requirement and so you've settled on using an IPSec network-based IP VPN, you must evaluate the technology used to provide network-based remote access and firewall services. If you do plan to run performance-sensitive applications across your IP VPN, then you should limit your selection to service providers that offer MPLS network-based IP VPNs. Again, you should be sure that the service provider is using a leading equipment vendor to deliver this service, has a close relationship with that vendor and has a high level of expertise building and managing complex networks. If you require remote access, you must also consider how the service provider supports this aspect of the service (vendor, support, etc.). Finally, the key to evaluating MPLS network-based IP VPN services is a careful review of the SLAs to make sure they support your business requirements.

For reasons explained above, most medium-to-large companies are best served by a combination of CPE and network-based IP VPNs. If this describes your situation, then use the selection criteria above to choose a service provider that can deliver in both areas. If you plan to use a CPE-based IP VPN to reach business partners (i.e., an Extranet), make sure that the service provider will support locations that are off-net. Most importantly, make sure that the service provider has the technical resources and expertise to handle your growing needs.

Once you've created your 'short list' of service providers that can deliver the type of IP VPN you desire, then revisit the list of service delivery criteria above. Also, consider which offers the best value-added services. One value-added service that's particularly useful is having access to a web-based customer portal. It should show the status of each site/user throughout the provisioning process, report the availability of existing sites, and provide visibility into of trouble tickets and billing systems – this is particularly useful for large-scale deployments.

Conclusion

By now you are well aware of the vast potential an IP VPN can offer your business and recognize the importance of selecting the right platform and service provider for deploying this technology. You should also be better prepared to make this selection using the criteria outlined above. Of course, one other important consideration is price – or, rather, "cost." That is, the price service providers charge for each type of IP VPN technology will not have as great an impact on your overall cost as will selecting the right type of

IP VPN and choosing a service provider that can save you time and money by deploying it and managing it effectively.

©2005 MegaPath Communications. All trademarks and service marks are property of their respective owners.

V1106