IBM eNetwork Software White Paper
eNetwork VPNs--IBM's Virtual Private Network Solutions

Abstract

In this paper, we begin by defining a virtual private network (VPN) and explaining the benefits that customers can achieve from their implementation. We then describe the IBM eNetwork(TM) VPN solutions, with a focus on VPN security. The advantages of an IBM eNetwork VPN solution are then described through the detailed explanation of three VPN customer scenarios--business partner/supplier network, branch office connection network, and remote access.

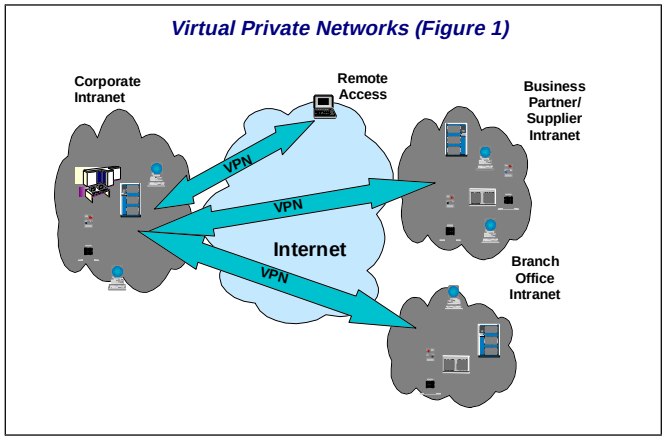
Introduction

With the explosive growth of the Internet, companies are beginning to ask: "How can I best exploit the Internet for *my* business?" Initially, companies were using the Internet to promote their company's image, products, and services by providing World Wide Web access to corporate Web sites. Today, however, the Internet potential is limitless, and the focus has shifted to e-business--using the global reach of the Internet for easy access to key business applications and data that reside in traditional I/T systems. Companies can now securely and cost-effectively **extend the reach** of their applications and data across the world through the implementation of virtual private network (VPN) solutions.

VPN description and benefits

A virtual private network (VPN) is an extension of an enterprise's private intranet across a public network such as the Internet, creating a secure private connection, essentially through a private "tunnel." VPNs securely convey information across the Internet, connecting remote users, branch offices, and business partners/suppliers into an extended corporate network, as shown in Figure 1. Internet service providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive leased lines, long-distance calls, and toll-free telephone numbers. A 1997 VPN Research Report, by Infonetics Research, Inc., estimates savings from 20% to 47% of wide area network (WAN) costs by replacing leased lines to remote sites with VPNs. And, for remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs. Additionally, Internet access is available worldwide where other connectivity alternatives may not be available.

Virtual Private Networks (Figure 1)



The technology to implement these virtual private networks, however, is just becoming standardized. Some networking vendors today are offering non-standards-based VPN solutions

that make it difficult for a company to incorporate all its employees and/or business partners/suppliers into an extended corporate network. However, VPN solutions based on Internet Engineering Task Force (IETF) standards will provide support for the full range of VPN scenarios, with more interoperability and expansion capabilities.

The key to maximizing the value of a VPN is the ability for companies to evolve their VPNs as their business needs change and to easily upgrade to future TCP/IP technology. Vendors who support a broad range of hardware and software VPN products provide the flexibility to meet these requirements. VPN solutions today run mainly in the IPv4 environment, but it is important that they have the capability of being upgraded to IPv6 to remain interoperable with your business partner's and/or supplier's VPN solutions. Perhaps equally critical is the ability to work with a vendor who understands the issues of deploying a VPN. The implementation of a successful VPN involves more than technology. The vendor's networking experience plays heavily into this equation.

IBM eNetwork VPN solutions

IBM has many years of experience in delivering industrial-strength networking solutions that use the latest technologies. We are committed to having the **broadest support** of VPN technology and the **widest breadth of offerings** in the industry-- including firewalls, clients, servers, routers, controllers, ISP services, and consulting services. These solutions are backed by **IBM's world-class security expertise** in leading-edge Internet security technologies, such as DES (Data Encryption Standard) and HMAC (Hashed Message Authentication Code), which were invented by IBM developers, and SET (Secure Electronic Transactions). We are also committed to the development of open, IETF-based technology, so companies can incorporate other vendors' products into their eNetwork VPN solution if they so choose.

IBM added-value

While many VPN solutions today consist only of firewalls, IBM eNetwork VPN solutions will also encompass multi-platform VPN-enabled clients and servers, routers, and management functions. The advantages of IBM VPN solutions are: scalability; flexibility of VPN function placement; and the ability to have secure IP tunnels all the way from the client to IBM servers, where the majority of critical corporate data resides today. This can be done without any changes to your existing applications and with easy-to-use eNetwork VPN management functions to manage your VPN environment.

IBM was one of the earliest providers of VPN offerings, delivering VPN capability in our AIX(R) Firewall in 1995. The AIX Firewall VPN capabilities were enhanced in 1996 to include IPSec, an IETF industry security standard. Other IBM VPN-enabled products available today are Windows 95 LAN/dial-up clients (through IBM eNetwork Communications Suite), OS/2(R) clients, AIX clients and servers, OS/390 (TM) servers with integrated firewall capabilities, ISP services (provided by IBM Global Services), and consulting services.

Throughout 1998, we will be extending our VPN coverage by offering the widest breadth of integrated, scalable, open, comprehensive IBM eNetwork VPN solutions in the industry. Our server offerings will be expanded to include VPN-enabled OS/400(R) servers, with integrated

firewall functionality and IPSec security. We will also offer routers and controllers with imbedded IPSec, L2TP and firewall technology.

In addition, we will incorporate VPN management capabilities--such as policy, certificate, IP address, and key management--into our solutions, as well as "future-proof" our offerings by adding critical functionality such as IPv6 to all our products. We will also offer support for service level agreements with our VPN solutions, giving customers the ability to provide levels of service and improved availability to their end users. In essence, we plan to offer customers all the components of a successful VPN solution-- the hardware, the software, the ISP services, and the consulting services (design, installation, and maintenance)--for one-stop VPN shopping, including a complete outsourcing of the VPN solution, if desired.

Through the implementation of IBM eNetwork VPN solutions, customers can **extend the reach** of their intranet, securely and cost-effectively. Companies need to communicate among their geographically dispersed locations; manufacturers and their suppliers need access to shared databases; and remote users need to reach applications and servers in their corporate intranet. IBM eNetwork VPN solutions support all of these scenarios, and many others, just as securely as if they were being run over dedicated private lines.

IBM recognizes that individual companies require different levels of security strength and administrative control. Our VPN solutions can be customized to be as secure or as flexible as required. The key is that IBM will offer eNetwork VPN solutions to meet the needs of your company--today *and* tomorrow--and we will offer all the products and services that you will need to design and deploy a VPN solution appropriate for the needs of *your* business.

Security

IBM uses IPSec--an open, IETF-standard security technology--as an integral element in our eNetwork VPN solutions. IPSec provides cryptography-based protection of all data at the IP layer of the communications stack. It provides secure communications transparently, with no changes required to existing applications. IPSec is the IETF-chosen, industry-standard network security framework for use in both the IPv4 and IPv6 environments. It is also currently the technology of choice for more than a dozen networking vendors, such as Sun, Attachmate, and Bay Networks.

IPSec protects your data traffic in three ways, using robust cryptographic techniques:

1. *Authentication*: The process by which the identity of a host or end point is verified
2. *Integrity checking*: The process of ensuring that no modifications were made to the data while in-transit across the network
3. *Encryption*: The process of "hiding" information while in-transit across the network in order to ensure privacy

In addition, as described below, IPSec can address the security requirements of *all* key VPN business scenarios and provides a growth path covering VPN expansion and security requirement

changes. In 1997, the IETF Security Working Group completed the initial work on IPSec extensions that provide *automated* Internet Security Association and Key Management Protocol (ISAKMP) capabilities combined with a key distribution protocol (Oakley). This solution includes both a mechanism for negotiating Security Associations to achieve the degree of protection you need (enabling automated tunnel setup) and a mechanism for automated secure distribution and refresh of strong cryptographic keys. By supporting IPSec with ISAKMP/Oakley, IBM eNetwork VPN offerings will minimize manual configuration and thus provide a more robust, user-friendly, maintenance-free solution.

At the April 1998 IETF meeting, the IPSec Working Group agreed to advance all of the base IPSec documents to "proposed standards". Having completed work on the base IPSec functions (authentication, encryption, integrity, key management and security association management), the IPSec working group will now turn its attention to developing new protocols to complement the base set. For example, it will consider ease-of-use issues such as VPN Policy databases, extended authentication methods for use with ISAKMP/Oakley, and interoperability across several Certificate Authorities.

IPSec can also be used in conjunction with security protocols that may already exist in other layers of the communications stack. Today, IBM supports the Secure Electronic Transaction protocol (SET), Secure Sockets Layer (SSL), and a variety of other security technologies that can be incorporated into your IPSec-based VPN solution. Object-layer security such as SET can be used to secure electronic payment transactions over the Internet, and SSL technology can be used to secure your specific applications. However, independent of whether any application-level security such as SSL has been implemented, IPSec can provide an authenticated and encrypted tunnel that protects *all* your IP traffic.

IPSec can also provide robust security in conjunction with other tunneling protocols, such as the Layer 2 Tunneling Protocol (L2TP) used in remote access dial-up configurations. L2TP, which is also an IETF standard, has the capability of establishing dial-up connections from clients using the point-to-point protocol (PPP). In addition, L2TP can be used to carry multiprotocol traffic, such as NetBIOS. But, L2TP lacks strong security properties. Thus, the March 1998 IETF Draft titled “Securing L2TP using IPSEC” discusses how L2TP can utilize IPSEC to provide for tunnel authentication, privacy protection, integrity check and replay protection. When IPSec is used in conjunction with L2TP, cryptographically strong access control is provided. IPSec will provide authentication, integrity checking, and encryption for *each* packet transmitted. It also provides automated key management functions and can protect data all the way to the target server.

VPN customer scenarios

IBM eNetwork VPN offerings are designed to allow companies to easily construct solutions that meet their business needs. We will look at three business scenarios well suited to the implementation of a VPN solution:

1. Business partner/supplier network
2. Branch office connection network
3. Remote access network

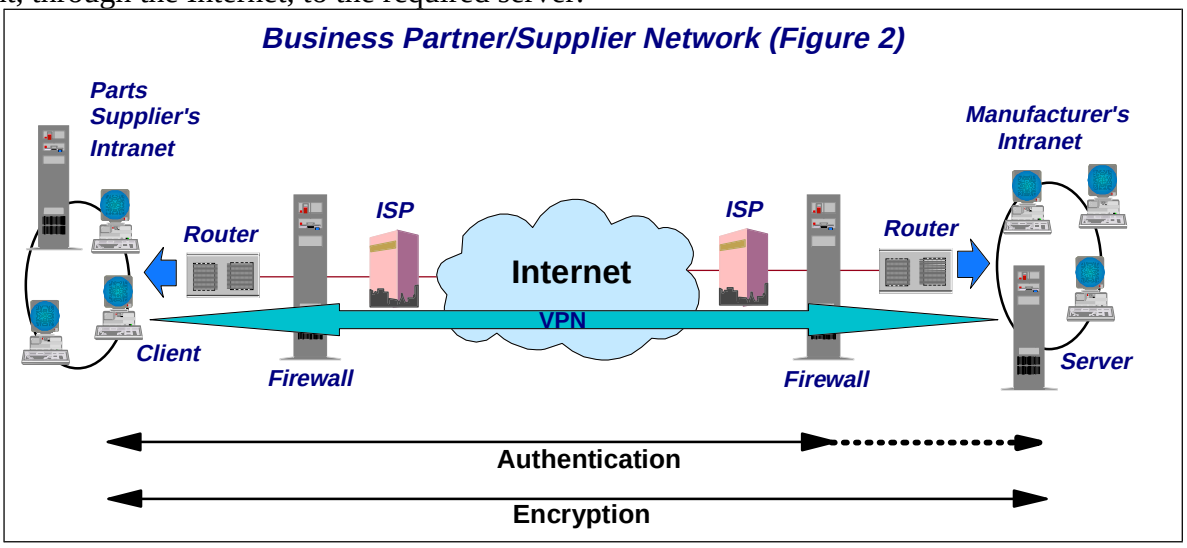
Business partner/supplier network

Industry-leading companies will be those that can communicate inexpensively and securely to their business partners, subsidiaries, and vendors. Many companies have chosen to implement frame relay and/or purchase leased lines to achieve this interaction. But this is often expensive, and geographic reach may be limited. VPN technology offers an alternative for companies to build a private and cost-effective extended corporate network with worldwide coverage, exploiting the Internet or other public network.

Suppose you are a major parts supplier to a manufacturer. Since it is critical that you have the specific parts and quantities at the exact time required by the manufacturing firm, you always need to be aware of the manufacturer's inventory status and production schedules. Perhaps, you are handling this interaction manually today, and have found it to be time consuming, expensive, and maybe even inaccurate. You'd like to find an easier, faster, and more effective way of communicating. However, given the confidentiality and time-sensitive nature of this information, the manufacturer does not want to publish this data on their corporate Web page or distribute this information monthly via an external report.

To solve these problems, the parts supplier and manufacturer can implement an eNetwork VPN, as shown in Figure 2. A VPN can be built between a client workstation, in the parts supplier's intranet, directly to the server residing in the manufacturer's intranet. The clients can authenticate themselves either to the firewall protecting the manufacturer's intranet, directly to the manufacturer's server (validating that "they are who they say they are"), or to both, depending on your security policy. Then, a tunnel could be established, encrypting all data packets from the

client, through the Internet, to the required server.



With the establishment of this VPN, the parts supplier can have global, online access to the manufacturer's inventory plans and production schedule at all times during the day or night, minimizing manual errors and eliminating the need for additional resources for this communication. In addition, the manufacturer can be assured that the data is securely and readily available to only the intended parts supplier(s).

One way to implement this scenario is for the companies to purchase Internet access from an Internet service provider (ISP), such as IBM Global Services. Then, given the lack of security of the Internet, either an IPSec-enabled IBM firewall or an IBM server with firewall functionality can be deployed as required to protect the intranets from intruders. If end-to-end protection is desired, then both the client and server machines need to be IPSec-enabled as well.

Through the implementation of this VPN technology, the manufacturer would easily be able to **extend the reach** of their existing corporate intranet to include one or more parts suppliers--essentially building an extended corporate network--while enjoying the cost-effective benefits of using the Internet as their backbone. And, with the flexibility of open IPSec technology, the ability for this manufacturer to incorporate *more* external suppliers is limitless.

Yet, inherent in network expansion are concerns of manageability. Tools should be implemented to ensure your network remains easy to maintain. Management functions to be included in eNetwork VPN solutions are: policy management, automated ISAKMP/Oakley key management capabilities (previously mentioned), certificate management, secure domain name server (DNS), and lightweight directory access protocol (LDAP) support. When implementing a VPN, a set of security configuration criteria must be established. Decisions such as which security algorithms are to be used by each IPSec-enabled box and when the keys are to be refreshed are all aspects of policy management. And, with respect to "key" technology, almost all of today's currently popular security protocols begin by using public key cryptography. Each user is assigned a

unique public key. Certificates, in the form of digital signatures, validate the authenticity of your identity and your encryption key. These certificates can be stored in a public key database, such as a secure domain name server (secure DNS), that can be accessible via a simple protocol, such as the lightweight directory access protocol (LDAP).

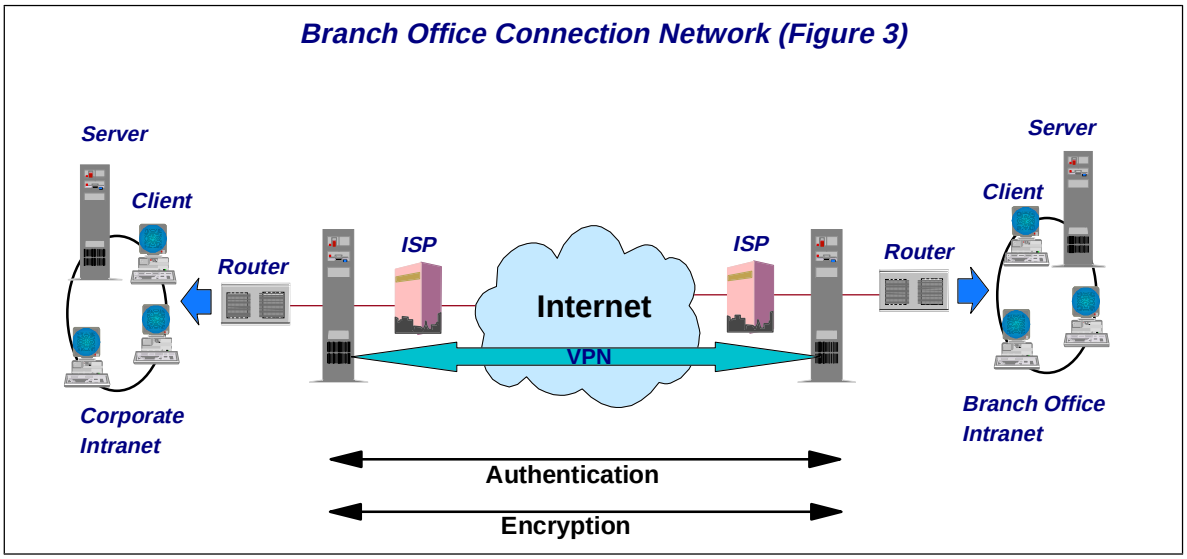
An automated IP address management system is especially important for VPNs in order to assign and manage your network's IP addresses. Thus, on March 16, 1998, IBM and Quadritek Systems, Inc, a market-leading IP address management company, announced an agreement to advance total product solutions for centralized, enterprise-scaleable IP name and address management. Together, IBM and Quadritek will offer highly centralized control of all network devices in your entire extended intranet. Also, along the lines of managing your IP addresses, network address translation (NAT), available today in IBM AIX Firewall, allows you to use a globally unique (public) address on the Internet, while enabling you to use private IP addresses within your intranet.

IBM will be incorporating all of these VPN management tools into our eNetwork VPN solutions, which can easily be implemented to meet the needs of your existing and future networking environment. Consultations with IBM networking and security experts will help you establish the VPN solution that best meets the needs of *your* company.

Branch office connection network

The branch office scenario, unlike the business partner/supplier network scenario, securely connects two *trusted* intranets within your organization. This is a key difference, since your security focus is on both protecting your company's intranet against external intruders and securing your company's data while it flows over the public Internet. This differs from the business partner/supplier network, where the focus is on enabling your business partners/suppliers access to data in your corporate intranet.

For example, suppose a corporate headquarters wants to minimize the costs incurred from communicating to and among its own branches. Today, the company may use frame relay and/or leased lines, but wants to explore other options for transmitting their internal confidential data that will be less expensive, more secure, and globally accessible. By exploiting the Internet, branch office connection VPNs can easily be established to meet the company's needs.



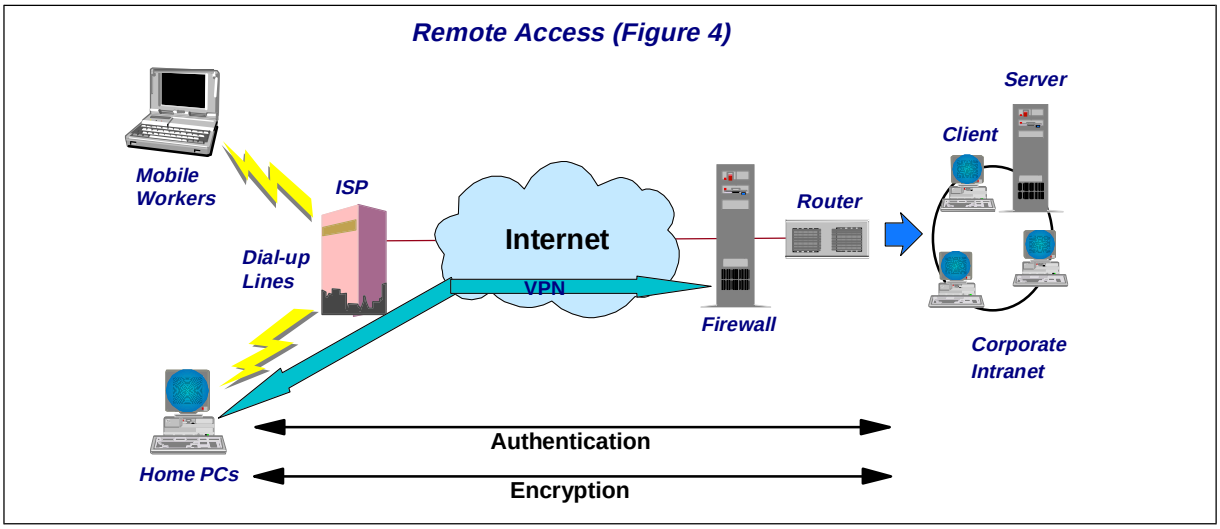
As shown in Figure 3, one way to implement this VPN connection between the corporate headquarters and one of its branch offices is for the company to purchase Internet access from an ISP, such as IBM Global Services. IBM eNetwork firewalls, or routers with integrated firewall functionality, would be placed at the boundary of each of the intranets to protect the corporate traffic from Internet hackers. With this scenario, the clients and servers need not support IPSec technology, since the IPSec-enabled firewalls (or routers) would be providing the necessary data packet authentication and encryption. With this approach, the inventory and pricing information would be hidden from *untrusted* Internet users, with the firewall denying access to potential attackers. And, as previously described in the VPN business partner/supplier network scenario, eNetwork VPN management functions can also be used to manage your VPN branch office connection network.

With the establishment of branch office connection VPNs, the company's corporate headquarters will be able to communicate securely and cost-effectively to its branches, whether located locally or miles away. Through VPN technology, each branch can also extend the reach of its existing intranet to incorporate the other branch intranets, building an extended, enterprise-wide corporate network. And, as in the business partner/supplier network scenario, this company can easily expand this newly created environment to include its business partners, suppliers, and remote users--through the use of open IPSec technology.

Remote access network

A remote user, whether at home or on the road, wants to be able to communicate securely and cost-effectively back to his/her corporate intranet. Although many still use expensive long-distance and toll-free telephone numbers, this cost can be greatly minimized by exploiting the Internet. For example, you're at home or on the road, but need a confidential file on a server within your intranet. By obtaining Internet access in the form of a dial-in connection to an ISP such as IBM Global Services, you can communicate with the server in your intranet and access the required file.

One way to implement this scenario is to use an eNetwork VPN IPSec-enabled remote client and firewall, as shown in Figure 4. The client accesses the Internet via dial-up to an ISP, and then establishes an authenticated and encrypted tunnel between itself and the firewall at the intranet boundary. By applying IPSec authentication between the remote client and the firewall, you can protect your intranet from unwanted and possibly malicious IP packets. And by encrypting traffic that flows between the remote host and the firewall, you can prevent outsiders from eavesdropping on your information. Once again, the previously described eNetwork VPN management capabilities can also be utilized.



Summary

We have briefly outlined the concepts behind the definition and the implementation of a VPN and described the value of IBM eNetwork VPN solutions based on IPSec. However, given the multitude of network environments and business needs, all scenarios have not been addressed in this paper. It is quite possible, for example, that a company may require elements of all three VPN scenarios that were described above. For example, what if you need to run multiple VPNs--one for your company's internal communications (e.g., the branch office connection scenario) and another for your external business communications (e.g., the business partner/supplier network scenario)? Or, what if you want to incorporate remote users into your supplier network? Or, what if you are a smaller business and need only a "small firewall" to protect your employees from Internet hackers? Or, when might you require VPN-enabled routers in your network?

These are all complex questions that should be discussed with experienced networking and security experts from IBM. With years of experience in these areas, IBM specialists can address these questions and determine the eNetwork VPN solution that will meet the needs of your business.

IBM eNetwork VPN solutions provide capabilities that can link your I/T assets with Web technology to build secure e-business solutions. With the implementation of an IBM eNetwork VPN solution, you can cost-effectively **extend the reach** of your network, your applications, and

your data. You can easily incorporate your business partners and suppliers, your remote branch offices, and your remote users--enabling improved communication and enhanced business processes. You can reduce business expenses both by exploiting the Internet or other public networks--instead of expensive private leased lines, dial-up lines, or toll-free telephone numbers--and by using IBM VPN management capabilities to minimize your VPN maintenance costs.

With IBM eNetwork VPN solutions, which encompass a comprehensive, flexible, open, scalable set of VPN products (clients, servers, firewalls, routers, and controllers) and ISP services and consulting services (design, implementation, and maintenance), IBM can build an extended, enterprise-wide, globally connected corporate intranet, tailored to the needs of *your* company.

For more detailed information about IBM eNetwork VPN solutions, please contact your IBM sales or marketing representative.