Patricia Seybold Group

Strategic Technologies, Best Practices, Business Solutions

The Internet Solution for Remote Access

Selecting an Internet Service and VPN Technology

By Michael A. Goulde

April 1999

Prepared for iPass Inc.

Table of Contents

Illustration and Table

The Internet Solution for Remote Access

Selecting an Internet Service and VPN Technology

By Michael A. Goulde
Prepared for iPass Inc. by the Patricia Seybold Group
April 1999

Executive Summary

The workforce is becoming increasingly mobile, and they are taking their computers and other devices along with them. Employees need to access corporate information resources while on the road. Traditional remote access solutions have relied on modem banks and long distance 800 numbers, but these entail an inordinately large cost and are completely lacking in scalability. Long distance dialing is also not robust enough for most needs. During the last 12 to 18 months there has been a major shift toward the Internet as the platform for remote access. Using the Internet addresses issues of cost, scalability, and reliability. This is possible because the Internet has become more reliable, and advances in security have made it a more secure network as well.

There are several approaches to providing remote access using the Internet. Companies can buy individual dial-up accounts from an Internet service provider (ISP) and distribute them to individuals. This is easy, but hard to manage and scale, and it doesn't provide adequate redundancy in the case of network outages. Another option is to outsource remote access to a managed service provider. Managed service providers can provide a complete solution but at a high cost and often with a loss in control over security and configuration. A third approach, which is gaining widespread acceptance, allows companies to internally manage the security and administration of remote access while still outsourcing the network infrastructure to the Internet. In each case, issues of service coverage and network redundancy should be considered. Not all ISPs and managed service providers have dial-up access in the required locations to ensure that remote users can connect to the Internet with a local call. When providers offer a global Internet roaming service, such as iPass, or use it to supplement their own offerings, they are able to address the need for widespread service coverage and network redundancy.

All of these approaches require security in order to prevent compromises of confidential data and strategic systems. Remote access over a virtual private network (VPN) provides a secure, cost-effective approach to giving people access to information resources. A VPN uses a combination of industry-standard networking protocols and data encryption to send

data securely between authenticated users and corporate networks. VPNs are primarily used by large companies that are outsourcing their Internet remote access or managing their own.

It is important to select the best Internet service and VPN technology for remote access based on a company's specific requirements and preferences. Selecting a solution must take into account issues of scalability, compatibility, security, cost, and manageability.

Introduction

The Mobile Workforce

Today's workforce is becoming increasingly mobile, working at home and on the road, which leads to increased productivity and flexibility. As a result, the demand for remote LAN access is growing tremendously. The Gartner Group conservatively estimates that by 2003 there will be more than 130 million people worldwide engaging in remote network access. People are able to work away from their offices because information and services constitute a growing part of the economy, and technology has made it straightforward to remotely access information. Businesses are redesigning their processes to incorporate mobile workers. With technology making it easier to travel and still connect to corporate networks, mobility is becoming an important part of more jobs. Remote network access allows employees to contribute from large distances. People from different organizations can collaborate. Information can be made available to people wherever they are, allowing them to make decisions on the spot. The consultant, the ultimate business nomad, can work interactively with clients wherever they are located. In general, remote access to corporate information resources helps eliminate delays and inefficiencies in work processes.

Identifying Needs and Requirements for Remote Access

The Need for Remote Access

The productivity of a mobile workforce depends on workers having access from anywhere to important information stored on corporate file servers, databases, and e-mail systems. They may need to access current price lists, review a contract or a proposal, update a project plan, update a customer record, or access myriad other key applications. E-mail is the leading application that requires remote access, but the list of other applications that people need to access is almost endless. The specific access requirements vary according to the organization. Among the factors that determine the nature and extent of remote access requirements are the number of employees traveling, the nature of the applications they will be accessing, the type and sensitivity of the data they will be accessing, and the locations from which employees will be connecting to the corporate LAN.

Remote Access Requirements

Many companies today have migrated to Internet-based remote access because of its many advantages over other solutions. The set of requirements that have to be met by any Internet-based remote access solution is fairly consistent. The objective is for IT departments and network administrators to be able to support remote users as well as local users. But supporting computer hardware and software remotely is hard. Many different types of devices have to be supported by staff who can't get their hands on them from a distance. Remote access introduces its own set of issues that must be addressed as well. The key issues fall into the following areas:

- **Security.** Protecting the network and protecting data
- **Cost.** Optimizing communication expenditures
- **Scalability.** Supporting large numbers of users
- **Quality of Service.** Providing the ability to access reliably with acceptable performance
- **Ease of Deployment, Management, and Use.** Making it easy for users and for managers to set up, maintain, and use

Security

Security is probably the most important requirement that IT departments and network administrators have for remote access. Security has to be airtight. The assumption has to be made that if security can be breached, somebody will breach it sometime. But security also has to be easy to administer, particularly when large numbers of remote users are involved. Security also has to be transparent to users or else they will try to find a way to bypass it. Managing security is complex because every resource on the corporate network must be protected: systems, information, application resources, and networks.

A remote access solution has to provide two levels of security. The first is user authentication, and the second is data encryption. It must be flexible, supporting a variety of user authentication methods so that existing authentication mechanisms in use in an enterprise can be used. Encryption must also be flexible, supporting a choice of whatever method a corporation chooses to adopt.

Cost

A remote access solution should not require an expense greater than necessary to achieve the goal of providing secure remote access from a large number of locations. Although giving every user a dedicated, leased line into the corporate network can provide guaranteed and secure access, the cost of such an approach is prohibitive. Low-cost solutions that do not compromise security are a must.

Scalability

A remote access solution must be able to support a large number of users without requiring a proportionate increase in expenditures for infrastructure or support. It needs to be able to support peak loads without requiring configuration with excess capacity that will be unused most of the time. The optimal remote access solution should also provide support for access from a large number of access points without increases in required infrastructure.

Quality of Service

Employees remotely accessing corporate network resources typically don't expect the same level of performance and reliability as they do when they are locally connected to their corporate network, but they do expect reliable services that allow them to access applications in a productive way. Dial-in attempts must provide successful connections at reasonable speeds, and they shouldn't get disconnected while downloading e-mail or accessing important information.

Ease of Deployment, Management, and Use

A remote access solution must easy to support, both on the LAN side of the connection and at the user end. Minimal software installation should be required and that software should be easy to install, configure, and use.

The Shift to the Internet for Remote Access

There are many different approaches to providing remote access to corporate LANs, but Internet-based approaches have come to dominate. Compared to leased lines, ISDN, and remote access servers, the Internet offers greater convenience, lower cost, and easier maintenance. Internet-based remote access uses the public Internet to provide the connection between the remote user and the corporate LAN. Internet-based remote access has become a mainstream option in a short period of time. In 1997, a Forrester Research survey found that 64 percent of network planners at Fortune 1000 companies would not consider the Internet for remote access. Sixteen months later, in August 1998, when Forrester Research conducted the same study, 86 percent of Fortune 1000 companies said they were already outsourcing or would consider outsourcing their remote access to the Internet. Issues of access, reliability, and security have largely been overcome, either in fact or in the perception that these were issues.

The Internet as a Viable Remote Access Alternative

Internet-based remote access has many benefits.

- The Internet can be accessed from nearly every city in the world.
- The Internet's architecture has built-in redundancy and fault tolerance, providing end-to-end reliability.
- Users are familiar with Internet access.

Security issues, long the strongest argument against Internet-based remote access, have largely been addressed through the use of the virtual private network (VPN). Briefly, VPNs require users to authenticate themselves in order to gain access to the corporate network. Authentication can be performed with various mechanisms, ranging from usernames and passwords to hardware-based security devices. Once connected, data exchanged between the user and the corporate network are encrypted, protecting them from being intercepted along the way.

The Internet itself has become more reliable as network providers continue investing billions of dollars in building a high-bandwidth, robust network backbone. Contrary to expectations a few years ago, the number of Internet Service Providers continues to increase, expanding the users' connection options.

Internet Advantages

Internet-based remote access has many benefits compared to those of traditional in-house modem bank solutions. Primary benefits of Internet-based options are:

- **Reduced Costs.** As a remote access platform, the Internet can reduce costs 50 to 80 percent over traditional modem bank solutions. Companies no longer have to purchase, set up, upgrade, and support in-house modem banks and leased lines. The Internet can also be accessed from all over the world with a local phone call through providers with broad-reaching networks or roaming services.

- **Scalable.** A company can immediately add hundreds or thousands of remote users when outsourcing to the Internet, as opposed to incrementally building out its own infrastructure to support these users.

- **Improved Reliability.** The Internet's architecture has built-in redundancy and fault tolerance, providing end-to-end reliability. Also, due to its widespread infrastructure, if a company should experience a rapidly growing remote user population, users are more likely to get connected through the Internet rather than by dialing into company modems that are overburdened with current users.

- **Ease of Use.** Most users are familiar with Internet access, so using the Internet to access corporate networks is easy with the appropriate client tools.

Exploring Internet-Based Options

A company can make use of the Internet to provide remote access in several ways. They are technically similar but differ in the business relationships that are established and in how easily they are managed.

Individual Dial-Up Accounts through an Internet Service Provider (ISP)

An Internet service provider (ISP) can be local, regional, or international. Most national ISPs offer roaming access to individual account users. The cost per month varies between $15 and $30. Set-up fees vary with each service. Each user has his own username and password and is billed monthly for the service. Access numbers are provided in the local city or in other cities where the provider offers service coverage, so a user can dial into and establish a connection to the Internet through the ISP. Each user has a username and password she uses to authenticate herself to the ISP.

Key Issues

The key issues for individual dial-up accounts are security, cost, manageability, and quality of service. The decision to use individual accounts is likely to be based on the expectation that the administrative effort involved is going to be relatively minimal. However, it does not take very many mobile employees accessing the corporate network with any degree of frequency before maintaining individual accounts is more trouble than another approach would be. Getting adequate support can be difficult, since the ISP may not know how to support the remote access VPN client the company has chosen for secure access. In addition, consideration has to be paid to the effort required to arrange for disabling the account when employees leave and establishing new accounts for new employees.

ADVANTAGES. The primary advantage of the individual dial-up account is that it is extremely easy and fast to set up for a few users. All that is typically needed is a telephone call to the ISP. Billing is generally to the user's credit card, and that is easy to manage. This makes it a scalable solution in the sense that everyone in a company could gain access through his or her own ISP. Software configuration is simple and rarely entails anything more complex than the Windows Dial-Up Networking client. End-user support is usually included as a part of the service.

DISADVANTAGES. Although individual accounts may be scalable, they are a management headache. It is hard to track accounts, and there are often multiple bills that have to be handled. Fixed-rate monthly accounts can also get expensive for large numbers of users. When averaged across many remote users, a usage-based plan is almost always more economical, since many users don't require remote access every month. Individual usage varies widely as well. Many have also found that it is very difficult to cancel an account when it is no longer needed. Often the monthly credit card charges can continue long after the request to stop service. Security is one of the major disadvantages with individual dial-up accounts, including both the lack of integration with corporate security systems and policies and the lack of encryption between the user and the corporate network. Users must set up their own security mechanisms or virtual private networks. (See "Making Access Secure: Selecting a VPN," page 13.)

Quality of service is another disadvantage, since the user only has one choice of telephone numbers to dial into. If that number is busy, out of service, or providing a poor connection, the user has few options.

Finally, users are assigned accounts by the ISP that do not reflect their corporate domains, which often leads to confusion in e-mail and other applications.

ADDITIONAL CONSIDERATIONS. Service coverage varies among ISPs, so coverage needs must be carefully matched to user travel patterns. Some ISPs offer only regional coverage, while others offer national coverage. Global coverage is offered by some through participation with a service such as the service provided by iPass.

High availability is a concern that needs to be addressed so users can still gain access during network failure or blackouts. Providers should have redundancy in the business centers where employees travel. Services such as iPass can allow providers to complement their offerings with access through multiple networks in the event of a single network failure.

Typical Customer Profile

The optimal customer for individual dial-up accounts is the small company that has relatively few employees who travel. Managing a few expense reports does not represent a burden for the small company. The vast majority of travel is likely to be only in those metropolitan areas served by the company's ISP and not overseas, where the ISP is unlikely to have access points.

This approach is satisfactory for a small number of users who are accessing only their e-mail or an intranet Web server, situations in which access can be controlled by the appropriate firewall configuration on the corporate network. It is not satisfactory, however, for a corporation trying to support large numbers of users securely accessing corporate applications. For companies that want to allow their remote users to securely access other corporate applications, this solution usually requires some internal IT resources to set up a VPN on the server and client side.

Outsourcing Remote Access to a Managed Service Provider

A service provider can manage user directories, permissions, authentication, and end-user support. The managed service provider uses either the public Internet or a private or closed user group network. In addition to the traditional managed service providers, other ISPs and system integrators are starting to get into this business by reselling dial-up services from larger network providers. Costs for these services vary but typically involve minimum fees for the number of users and for usage. Most provide consolidated and detailed billing for individuals. Users receive a dialer client for their machines with a list of access numbers or a built-in phone directory.

Key Issues

Outsourcing the remote access solution works well up to a point, and that point is where the number of accounts becomes large enough and the need to manage access privileges great enough to warrant consideration of a solution that is more cost-effective and more tightly integrated into the corporate network. Outsourcing approaches are attractive because they eliminate the necessity of having to maintain in-house expertise for supporting the service and end users. The outsourcing provider handles all of that at a predictable incremental cost as users are added. The trade-off is that the outsourced service is constrained in its flexibility because the same service has to be offered to many different customers in order to be offered at a competitive price. Also, the managed service provider is providing access to end users, not providing a solution that is integrated with internal corporate policies, systems, or user directories.

ADVANTAGES. Outsourcing remote access has advantages. It removes the significant administrative and management burden involved in supporting remote access services.

These services are easy to set up and minimal internal resources are required. This option is likely to be most attractive to companies that have been incurring a high cost in order to maintain a significant remote access infrastructure. The ongoing cost of maintaining and upgrading equipment and providing support will be quickly recouped with an outsourced approach. Consolidated billing and call detail records make auditing and administration straightforward.

DISADVANTAGES. There are significant drawbacks to using a managed service provider. Set-up fees and minimum commitments for users and usage may lead to a very expensive solution. Security options are limited and are not integrated with internal security mechanisms. Some use RADIUS proxy methods that expose the user names and passwords to interception by other members of the access group. Contrary to the belief of many companies, managed network services do not necessarily mean "secure" networks. If the provider is running a VPN then it should be secure. However, some providers refer to their network as "private," but, in many cases this just means a "closed" user group. Although some providers imply that a closed group of users on a private network is secure, many believe that having many companies with thousands of users utilizing the same private network is not any more secure than access and data transfer over the public Internet. Although supporting users on this problem falls in the lap of the service provider, the quality of support received varies, impacting the usability of the service and creating user dissatisfaction.

Managed service providers may require that the company purchase its dedicated Internet connection from them, further limiting a company's flexibility and choice.

In an environment where management flexibility and control is important, this approach offers little administrative control and is operated outside the realm of normal network operations. For example, user directories and permissions are maintained by the provider, a serious concern for security-conscious companies.

ADDITIONAL CONSIDERATIONS. As in the case of ISPs, service coverage area is a major concern, and what is offered has to match the travel requirements of employees. Companies lose a great deal of productivity and dollars when their remote workers cannot achieve a successful connection to the corporate network, even if for just a short period of time.

Redundancy is another area of concern when a single network provider or closed group system is used. Although the Internet is known for its ubiquity, no single provider offers ubiquitous access. Even some of the largest managed network services that have a significant international presence fill in gaps in their service coverage with Points of Presence from other network providers. Some use services such as iPass, with global dial-up access points, to complete their remote access service offerings. This gives their customers the benefit of both widespread service and redundancy in major business centers through the multiple top-tier networks that are the foundation of the iPass service.

Typical Customer Profile

Companies that don't want to devote internal resources to managing remote access, typically small to medium-sized companies, find an outsourced solution easy and convenient. On the other hand, usage commitments and set-up charges make the managed service more attractive to larger companies. However, as security issues become more sensitive and as other options become available, larger companies are leaning toward internally managed solutions.

Internally Managing an Internet-Based Remote Access Solution

Finally, there is the option of internally managing a remote access solution that combines the ability to integrate corporate security policy and user authentication and management with the access provided by the global network of Internet access providers. This type of solution is offered today through some traditional Internet service providers as well as through value-added resellers and system integrators that have historically provided other telecommunications, networking, and security solutions to companies. In this approach, the company maintains and manages user directories, permissions, authentication, security, end-user support, client software, and telephone directories. Internet access is purchased through the company's provider of choice, using the Internet for remote access.

This approach uses existing internal authentication mechanisms to authenticate user access to a dial-in Point of Presence. Once users have been authenticated, they gain normal access to the Internet and the corporate network. This approach also provides the company with a consolidated remote access service bill and detailed usage records by individual, department, or group within the company.

By unifying access in this manner and integrating with a company's user directory and its authentication and security policy, this approach also makes it much easier to integrate a VPN solution so that data can be protected as they travel across the Internet.

Key Issues

Managing a remote access solution internally provides corporations with the ability to continue to manage their user directories, authentication, and security in-house, but to outsource the communications infrastructure. It also assumes that security and control are a high priority and that the company's strategy includes maintaining an internal IT staff. For companies trying to eliminate or significantly downsize IT departments, an internally managed solution eliminates maintaining user directories, authentication mechanisms, VPN, and management of end users, all of which require internal resource commitments.

This approach is most beneficial when a corporation has actually implemented a security policy and has an infrastructure that can support policy-based administration of security. If a company does not have an adequate security policy in place, then this approach cannot provide more security than is already provided on the corporate LAN. For example, if a company is lax in requiring passwords to meet certain requirements, the service cannot be responsible for stolen or guessed passwords. Similarly, even though a network of ISPs can provide redundant connection options in most cities, users will not experience any better or more reliable performance than the Internet backbone can provide at any point in time.

ADVANTAGES. Advantages of this approach are that it is easy to deploy, has minimal start-up and ongoing costs, and provides a high degree of flexibility and security to companies and their users. User directory management is kept in house, helping to ensure security. Security management, support, and configuration of resources to be accessed are all under corporate control. The company has a choice of authentication mechanisms and of the VPN to be used. The combination of a global network of ISPs and an integrated approach to security is powerful. It provides a higher quality of service, giving users multiple dial-in options in most cities. If an access number is unavailable or giving poor service, the user merely has to select a different number. Which ISP is providing the access is completely transparent to the user and the corporation. Pricing plans are flexible with both fixed-rate and usage-based options. Start up fees are minimal. Billing is provided on a consolidated basis, and call detail records can be provided to support internal accounting objectives. This approach is highly scalable, since any number of users can be supported with no additional infrastructure.

DISADVANTAGES. The disadvantages of internal management is that this type of solution requires internal IT resources to manage security policy, user directories, and permissions. It also requires that the company select and implement a VPN technology, although most of the service providers can now offer recommendations and some provide documentation on the configuration to make it much easier to get started.

ADDITIONAL CONSIDERATIONS. As with the other Internet-based approaches, service coverage and redundancy should be key considerations. iPass Corporate Access is an example of an internally managed, Internet-based remote access solution that aggregates the world’s top-tier telecom operators and network providers to offer a global network that provides network redundancy and that can be locally accessed from practically anywhere in the world. All access becomes a local call, significantly reducing connection costs. Providing multiple access points in most cities assures high network availability, and local calls ensure more reliable service than overseas calls. Integration with corporate authentication mechanisms ensures tight security. Support for industry-standard authentication protocols and VPN integration make secure communications straightforward. iPass’s settlement and clearinghouse platform allows it to provide companies with a single consolidated billing statement with call detail records down to the individual user level.

Typical Customer Profile

Any organization with internal IT resources, several remote users, and varying needs among users will benefit significantly from an internally managed, Internet-based remote access solution. Companies using this solution range from having a few heavy remote users to having tens of thousands of users. Since any internally managed option available today can include the iPass Corporate Access service, companies that have employees traveling the globe gain tremendous benefits from a global network with built-in network redundancy. Companies that want to retain administrative control over their remote users typically opt for this kind of an approach. The accompanying table compares remote access options.

Description of the iPass Corporate Access Solution

iPass Corporate Access is an internally managed remote access solution. It gives mobile workers and telecommuters low-cost, secure access to the Internet, e-mail, and corporate networks (with a local call) through more than 3,000 access points throughout 150 countries.

Global Reach

The service delivers high-performance connectivity by combining the best-of-the-best networks such as UUNET Technologies, and CompuServe Network Services, (both now owned by MCI WorldCom), EQUANT, and top regional providers throughout the world, such as GTE Internetworking, NTT-PC, Hongkong Telekom, Deutsche Telekom, France Telecom, Argentina Telecom, and many others. By integrating several tier-one networks, iPass offers multiple access points, as well as network redundancy, in major business centers. The simple point-and-click interface of the iPass client software, with its automatically-updating international phone book, ensures easy, convenient connectivity worldwide.

Comparison of Remote Access Options

	Dial-Up Accounts	Externally Managed Solution	**Internally Managed Solution (iPass Corporate Access)
Global Coverage	*No	*Limited	Yes
Redundant Access in Major Business Centers	*No	*No	Yes
Rapid Deployment	Yes	Varies	Yes
Scalability for Management of Many New Users	No	Yes	Yes
Integration with Corporate Authentication Database	No	No	Yes
Secure Authentication	Varies	Varies	Yes
On-Site Control and Administration	No	Varies	Yes
Can Be Used with VPN for Secure Data Transfer	Yes	Yes	Yes
E-Mail Address Uses Corporate Domain	No	Yes	Yes
Provides Consolidated and Detailed Billing for All Users	No	Varies	Yes
Minimal Set-Up Fees	Yes	No	Yes
Fixed-Rate and Usage-Based Pricing Options	No	Varies	Yes

* ISPs and managed service providers that offer the iPass Internet Roaming service or use it to supplement their own offerings do have global service coverage and access point redundancy in most major business centers.

** All or almost all instances of internally managed services use iPass Corporate Access as the foundation of the offering.

Comprehensive Security

iPass Corporate Access uses 128-bit secure socket layer (SSL) encryption to secure user names and passwords during authentication. It also supports existing security systems on the corporate network, authenticating users with their corporate credentials and allowing the company to maintain control over user passwords and permissions. iPass Corporate Access can also be integrated with any VPN solution, ensuring that the user's session is secure and that data are protected. In some cases, iPass has worked with VPN vendors to bring a seamless integration to the user level, providing a "one-click" solution that connects remote users to the Internet and initiates the VPN client at the same time for a secure session.

Tremendous Cost Savings

The iPass service can save a company 50 to 80 percent compared to traditional solutions using in-house modem banks, long-distance numbers, and toll-free numbers. Administration is simplified; the service can be deployed in just a few hours, and it significantly reduces the administrative and support costs associated with maintaining modem banks and complicated client software. Companies can choose usage-based service plans, which provide the greatest savings when averaged over many users, or fixed-rate plans, which provide more predictability in monthly connectivity costs.

Based on the Leading Internet Clearinghouse

iPass is a leading Internet clearinghouse, providing authentication, authorization, settlement, and clearinghouse services between tier-one ISPs and businesses requiring remote access. This is similar to ATM networks, such as Cirrus, Plus, or Interlink, which allow people to get cash from the machines at participating banks even if they don't have a relationship with that bank. These systems provide the authentication and settlement between the participating banks, and they provide the means for the transaction to appear on the statement provided by the user's bank.

iPass acts as a clearinghouse just as an ATM network does. When a user dials into an iPass-enabled access point, iPass handles the authentication routing and settlement between the ISP and the company, paying the network provider for the use of its access point and billing the company for the use of the ISP's network. Billing information is collected by iPass and sent to the company as a single itemized bill for all employees, covering the service usage they have had during the billing period. It can show billing detail all the way down to a department or user level.

How iPass Corporate Access Works

In addition to the iPass Clearinghouse Platform, on which its Access Anywhere services are based, iPass Corporate Access comprises the iPass client software and the iPass RoamServer. The client software is installed on the mobile user's computer, and the iPass RoamServer software is installed on the corporate network. iPass RoamServer works in conjunction with the company's authentication database to allow users to connect to the

Internet through one of the iPass-participating network providers. (See illustration on page 15.)

Making Access Secure: Selecting a VPN

What Is a VPN?

The term *virtual private network* (VPN) is used in many different ways and can mean different things to different people. To best understand what a VPN is, it helps to also have a clear definition of both a private network and a public network relative to this paper.

A private network dedicates all network components (leased or owned) to a single customer.

A *public network* shares one or more network components among multiple customers.

A *virtual private network* (VPN**)** uses a public network, along with encryption, tunneling (encapsulation), and authentication, to achieve the same level of security and privacy as a private network.

Virtual private networks are used in two primary ways. First, VPNs can connect two networks. This is typically referred to as a LAN-to-LAN VPN or a site-to-site VPN. Second, a remote access VPN can connect a remote user to a network. This paper is focused only on the latter.

A remote access VPN replaces the need for a private network. In a VPN, one organization’s data travel over the same Internet as everyone else’s–no virtual network is created. But, because the data is encrypted and only authenticated and authorized users can access the data, a virtual network that is private and secure exists. In fact, VPNs on the Internet are thought by some to be more secure than WANs that do not employ data encryption.

VPNs: Critical to Remote Access

The key to cost-effective, secure remote access over the Internet is having a virtual private network in place. The Internet is the most ubiquitous and least expensive public data network and is the optimal foundation for a VPN. An Internet-based VPN is virtual because it appears to be a dedicated private network with exclusive use of the infrastructure that constitutes it, even though the infrastructure is anything but dedicated. Because users see only their own traffic, which is routed to them, it appears that the network is private.

A VPN solution must provide the security necessary in order for private data traffic to be sent over the Internet’s public data network with guarantees of privacy. VPNs can link all of an organization's offices, traveling employees, telecommuters, and even customers and suppliers. Because of the Internet's ubiquity, individual users anywhere can connect with a local phone call. Some estimates are that VPNs can provide a cost saving of as much as 90 percent over private networks.

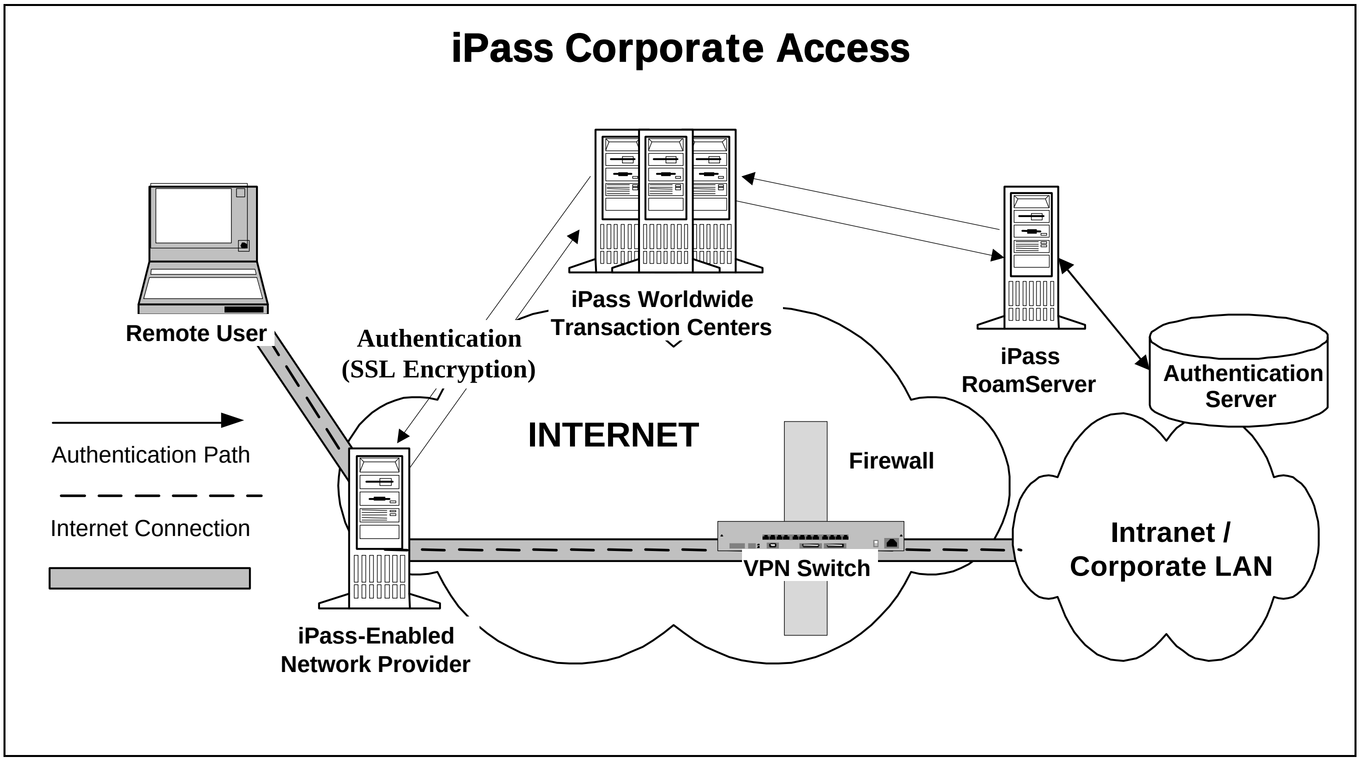

Illustration. A remote user dials into a local iPass-enabled network provider. The user's logon credentials are encrypted and passed over the Internet to the nearest iPass Transaction Center, which routes the request to the iPass RoamServer at the corporate site for authentication. RoamServer checks the corporate authentication database to determine if the user should be granted access. Depending upon the response sent back, the iPass-enabled network provider either grants or denies the user access to the Internet and any application outside of the company's firewall. To access resources behind the company's firewall, the remote user initiates the VPN client and enters a password to get authorized for access to the corporate network. Once the user is authorized, the VPN creates a tunnel between the user and the corporate network to allow encrypted data to travel securely over the Internet. The iPass Transaction Center logs the time users are online so iPass can pay the network provider and can provide the company with call detail reports.

How a VPN Works

A VPN uses a combination of authentication, data encryption, and tunneling to create a secure channel between a user and a corporate network or between two networks. In a remote access situation, the users dial in to the local access provider's POP, establish a connection to the Internet, and then identify themselves to the corporate VPN's authentication system. The VPN verifies the identity of a user either on the basis of username and password, a hardware token and PIN number, or some other mechanism. Upon successful authentication, tunneling and/or encryption is set up for all traffic between the VPN client and VPN server.

Selecting a VPN Solution

A VPN solution has four key requirements: compatibility, security, availability, and interoperability.

Compatibility

When choosing an Internet service for a VPN, 77 percent of the respondents in one survey said they seek compatibility with their existing equipment. In order to use the Internet for a VPN, the corporate network must be made compatible with the Internet Protocol (IP). Many private networks use nonstandard IP addressing schemes; these cannot be used directly with the Internet. Other private networks are non-IP based, and they too must be made IP compatible. In order for these networks to be used with an Internet VPN, they must either be converted to standard Internet addressing, have IP gateways installed, or employ tunneling techniques. Determining which solution is appropriate is beyond the scope of this paper, but, in any case, there must be a match between the selected approach and the VPN solution that is used.

Security

Security is vital to a virtual private network. Privacy is assumed, often mistakenly, on private networks. The key is to employ a VPN solution that is as private as the private network should be. With appropriate security, the Internet can achieve a high degree of privacy. The key concern is to ensure that information privacy is maintained while it is in transit between servers and clients. Protecting data requires that they be encrypted while traveling over the Internet. There are many algorithms; TripleDES is currently popular among companies. Tunneling, also known as encapsulation, can be used to transport non-IP protocols, such as NetBEUI and IPX.

Availability

VPNs need to be highly available and to provide high throughput. High availability is a function of the network, the VPN software, and the system on which it is running. The Internet does not guarantee performance levels, but it is a highly resilient network, providing more robust end-to-end redundancy and resiliency than a typical private network. In terms of performance, early VPN solutions suffered poor performance because of the amount of processing necessary to encrypt and decrypt packets. More powerful notebook computers, encryption co-processors, and faster algorithms have helped to alleviate the performance bottlenecks.

Interoperability

Although standards exist for providing VPN compatibility, various factors, including differences in the implementation of those standards, limit multivendor interoperability today. In addition, many standards for tunneling, authentication, and encryption are new or are just emerging. Care must be taken to ensure that the VPN solution selected adequately provides end-to-end compatibility and interoperability. This often means selecting a single-vendor solution. Nevertheless, the solution should be one that supports, or intends to support, industry standards.

Debunking Myths about Internet-Based Remote Access

Many network administrators have their reasons for being reluctant to implement a remote access solution. Although many of these reasons may have been valid in the past, a variety of solutions and services on the market today have addressed many longstanding concerns.

Myth #1: "If I open up my network to people for remote access, hackers will be able to gain access."

A chain is only as strong as its weakest link. There are a variety of solutions on the market today that make it extremely difficult, if not impossible, for someone to gain unauthorized access to an Internet-connected network. Products such as firewalls, security tokens, and strong encryption go a long way toward closing potential access holes to unauthorized users. However, these technologies are of no use if an adequate security policy isn't in place on the corporate LAN, whether or not remote access is enabled. The most serious threat to information resources has proved to be from internal sources. Until systems are adequately protected from employees gaining improper access from the internal LAN, worrying about insecure access from outside is fruitless.

Myth #2: "Sending important information via the Internet is not secure and is unreliable."

Security is certainly a risk if data are sent as clear text. However, virtual private networks can ensure that data being sent and received are securely encrypted and that their cost per user is affordable and justifiable in terms of productivity and supporting people in the field. Reliability is an application design issue more than a remote access issue. Applications need to be designed to fail gracefully, either rolling back incomplete transactions or timing out after a preset period if there is no response from the user. Applications that crash because a connection is lost shouldn't be on a corporate LAN, let alone any other network.

Myth #3: "Managed network services offer a "private" network and ensure secure data transfer."

In most cases, the "private" network is really just a closed user group, providing no tunneling or encryption of data. Since this closed user group could include hundreds of companies and thousands of users, in many ways it really isn't any more private than the public Internet. If companies want secure data transfer, they must be sure to request a VPN service on top of the managed network service or they should implement their own VPN. In addition to secure data transfer, user authentication must be secure. Often, these services use RADIUS proxies over these networks to route user authentication and authorization requests in clear text. If these usernames and passwords are not encrypted, they can easily be intercepted by other users in a "closed user group." Remember, the majority of security breaches are internal.

Myth #4: "Service-level agreements (SLAs) ensure that you get a highly reliable and defined service level."

Service-level agreements (SLAs) are not absolute guarantees of performance levels. Initially designed to make companies feel more confident about the service reliability, SLAs often provide financial compensation to companies when the terms of the SLA are not met. Typically, they can measure only the overall service levels of their networks and cannot measure service performance for a particular customer. In many instances it is not even possible for a company to verify whether its service level is being met. The bottom line is that the financial incentives do not make up for the lost productivity and opportunity when remote employees can't gain network access. SLAs can make a company feel better about its service provider's commitment to providing reliability, but, if a company believes that downtime will be extremely costly, it really should look for services that provide access point redundancy in the service areas where employees travel most frequently. In addition to general redundancy, multi-service provider approaches, such as iPass, offer access point coverage across multiple networks so that, if one network provider has a temporary outage, remote users can gain access through a different provider.

Myth #5: "Large enterprises should outsource their remote access to the large managed network providers."

Traditionally this was true because it was the only way to get broad coverage. But now there are more options available that provide both coverage and the additional advantage of managing security in house. The largest companies and those most concerned about security prefer the new internally-managed service options. Some of these options allow companies that wish to handle all of their security in-house to internally manage user authentication and directories. Today, it is typically the smaller companies, which don't have internal IT managers or enough internal IT support, that tend to want to outsource everything to a service provider, including user directories, authentication, security, and support.

Myth #6: "The traditional managed network providers all own and operate their own networks, ensuring the best quality of service to companies."

First, many of the traditional managed network providers do not entirely own and operate their networks. For example, CompuServe Network Services, now owned by WorldCom, provides network access through multiple network providers as part of its managed network service to enterprises. Secondly, just because a provider owns and operates its own network does not mean that it provides a better quality of service. Multi-service provider solutions, like iPass, for example, can consistently provide higher network availability by offering access point redundancy in major business centers throughout the world. In iPass's case, network access is available through providers such as CompuServe Network Services, EQUANT, UUNET, and top regional providers throughout the world, such as GTE Internetworking, NTT-PC, Hongkong Telekom, Singapore Telekom, Deutsche Telekom, and France Telecom.

Myth #7: 'Multi-service-provider solutions, such as iPass, can't control service reliability because there are hundreds of ISPs in their alliance."

Although iPass has over 600 Internet service providers selling its Access Anywhere services to businesses and mobile Internet users, very few (currently 150) actually provide network access for iPass global access services. iPass uses stringent quality-of-service requirements that must be met for network providers to participate in its global access service. The large percentage of iPass network access is supplied by the world's tier-one network providers, with smaller regional providers "filling in" service coverage where the large national providers don't have coverage. This approach is a key part of the company's strategy for providing a high quality of service and garnering a high level of customer satisfaction.

Myth #8: "The biggest cost savings a company experiences when using the Internet for remote access is the elimination of long-distance and toll-free connection charges."

Although the long-distance and toll-free connection charges with traditional in-house modem bank solutions are typically extremely high, the overall cost to purchase, install, maintain, and support in-house modem banks and leased lines can be a huge "hidden" cost center to a company. Companies should be sure that the service provider they select provides local access points in the locations where employees will most frequently travel. Many service-provider offerings are not truly global, requiring long distance calls by employees for remote access from many locations.

Myth #9: "Flat-Rate Internet access usage plans are more economical than usage-based services."

Although intuitively it appears that a flat-rate monthly service charge for Internet access would be less expensive than "pay-as-you-go" services, in reality, when usage is averaged across all mobile workers in a company, a usage-based or "pay-as-you-go" service is usually far more economical. Flat-rate usage plans are primarily designed for telecommuters and heavy remote users, and more importantly, for those companies who are willing to pay for predictability in their monthly service costs.

Myth #10: "The largest network providers always provide the best services with the broadest service coverage."

Typically, the largest network providers do offer some of the broadest offerings. However, there are significant differences between these providers and a number of other emerging service providers that have already proved to offer some of the best services to enterprises.

Although some providers have expanded internationally, none of these providers can offer true "global" access on their own. The ones that have the broadest network reach are those that use a clearinghouse service, such as iPass, to fill in gaps in their service coverage in order to give their customers a more comprehensive offering. There is a new class of emerging providers, companies that have traditionally offered security and networking products and are now offering remote access consulting and VPN services to enterprises. These companies offer customized, flexible solutions, and can often deliver more personalized support services to businesses than the largest network providers.

Summary

Mobile workers are rapidly reaching the point where they assume that they will be able to access their e-mail, files, and other resources on their corporate networks. They want this access to be easy and to be possible from any location in the world. At the same time, IT organizations and network administrators want remote access solutions that are secure, easy to support, and cost-effective.

Putting an Internet-based remote access solution in place makes sense for most companies. But this must be done with forethought and planning, particularly around security issues. Local security policy must be well defined before remote access can be turned on.

Companies with just a few remote users may want to consider purchasing individual dial-up accounts for their remote users. Small to mid-sized companies with minimal internal IT resources should consider a complete outsourced solution by a managed service provider. In both cases, companies should understand their service coverage needs, and if they are wide-ranging, companies must be sure that the service provider offers widespread coverage and redundancy in the locations required.

For mid-sized to large enterprises or for those companies with many remote users and internal IT resources, an internally managed solution such as iPass Corporate Access meets all of the key requirements for a secure remote access solution, including on-site control and integration with existing user directories, authentication mechanisms, and a VPN solution. An additional benefit is the nearly universal access and network redundancy that iPass offers as a result of its worldwide network of cooperating network access providers.