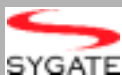


By
Steven Harris
Research Manager
International Data Corporation

Sponsored By:



Produced By:



Table of Contents

IP VPNs – An Overview for Network Executives By Steven Harris

Definition of IP VPN	2
The Business Case for IP VPNs	3
How IP VPNs Are Being Used	6
Implementation Types	6
IP VPN Providers	8
Conclusion	9



Steven Harris
Research Manager
ISP Markets/Business Network Services/IP VPNs
IDC

Steven Harris is research manager in IDC's ISP Markets, Business Network Services, and IP VPN research programs. Steven is responsible for IP telecommunications services and Internet Service Providers (ISPs), including company strategies, markets, and technologies. He is the author of "IP VPN Services: U.S. Market Forecast and Analysis, 2001-2006" and "IP VPN Services: A Demand-Side View, 2001."

Prior to joining IDC, Steven was an industry analyst with the U.S. Department of Commerce, where he was responsible for covering the data communications industry and promoting the sale of U.S. data products abroad. His work included tracking industry trends, helping government officials understand industry concerns/issues, and promoting exports through international trade shows and missions.

Steven graduated with a B.A. honor's degree in Economics and International Relations from the University of Wisconsin, Madison and a M.S. from the School of Foreign Service at Georgetown University, Washington, D.C., with a specialization in international business.

Steven can be reached at sharris@idc.com.

IP VPNs

An Overview for Network Executives

BY STEVEN HARRIS
RESEARCH MANAGER, INTERNATIONAL DATA CORPORATION

- Definition of IP VPN
- IP VPN usage
- Market Trends

Definition of IP VPN

Internet protocol (IP) virtual private networks (VPNs) are a collection of technologies that ensure the privacy of data over a shared IP network infrastructure. The two key points as to what constitutes an IP VPN are privacy and an IP network.

Privacy is accomplished in one of several ways. The most common forms of data privacy are through encryption or through the partitioning of data traffic for the customer.

Encryption used for IP VPNs is closely associated with the IP Security (IPSec) standard. IPSec is a reasonably well developed standard incorporated into the IP protocol. IPSec comes in two varieties: the Data Encryption Standard (DES), which uses a 56-bit key, or 3DES ("triple DES"), which applies the 56-bit key three times for stronger security.

Traffic partitioning used for IP VPNs is closely associated with Multi-protocol Label Switching (MPLS), which separates one customer's data traffic from that of other customers on the same shared network. Traffic partitioning is essentially the same type of privacy method used in frame relay networking.

IP VPNs require the use of an IP network. Data traffic that uses a frame relay or ATM network can be classified as a VPN, but not as an IP VPN.

Hybrid solutions that may be of interest to many users of traditional data services such as frame relay are available in the market. IP-enabled frame relay allows for the addition of many IP functions and features over a traditional frame relay infrastructure. IP-enabled frame relay is not considered an IP VPN, however, because an IP network is not being used for such a service.

Multiple terms and technologies are often associated with IP VPNs, including encryption, authentication, RADIUS, firewalls,

IPSec, tunneling, digital certificates, extranets, L2TP and MPLS. Some or all of these technologies, protocols and functions may or may not be part of an individual IP VPN implementation. Don't let their inclusion confuse you or their exclusion worry you. IP VPNs come in many flavors and varieties.

IP VPN Usage

IP VPN usage is growing rapidly and is well established, especially in the United States. International Data Corporation (IDC) conducts a survey (WAN Manager Survey) of 400 wide area network (WAN) managers of medium and large enterprises in various regions of the world each year. According to the 2001 survey, 48% of medium and large businesses in the United States are using IP VPNs now. In 2000 the figure was 30%.

The 48% of enterprises currently using IP VPNs include those that are trying the technology out in parts of their WAN or for remote access. IDC has not seen, and does not expect to see, wholesale replacement of traditional data networks by IP VPNs in large numbers of companies. IP VPNs will join other technologies as a mature WAN technology.



When VPN performance matters.

Internap's managed VPN service removes the uncertainties of VPN performance.

www.internap.com

INTERNAP™
The intelligent way through the Internet

[Internap Network Services Corporation](http://www.internap.com)

However, IP VPNs are growing both extensively (in the number of companies using IP VPNs and trying them out) as well as intensively (in the number of corporate sites or number of remote users connected via IP VPNs).

Europe, Asia, and Latin America also show gains in IP VPN awareness and usage, albeit to a lesser extent than in the United States. However, IP VPNs are a global phenomenon that will continue to grow.

Market Trends

What is driving the growth of the IP VPN market?

- The need for remote access to the corporate LAN
- The potential for cost savings
- The increased deployment of IP-based applications
- The increase in better outsourcing options

Remote access is the main reason companies are deploying IP VPNs. According to the WAN Manager Survey, 83.5% of U.S. companies have deployed an IP VPN for use as a remote-access technology.

The reason that remote access is so popular for IP VPN usage is simply the lack of other good options. Telecommuters, employees who are traveling, or employees working at home on weekends or evenings can dial into the corporate LAN over the Internet without any security measures (simple dial access) or they can use security measures like IPsec encryption. Frame relay connections are not portable.

The Internet is ubiquitous and that is its primary selling point for corporations seeking to connect employees outside the office.

Cost savings are not necessarily inherent in IP VPN technology. A dedicated IP connection may or may not be cheaper than an equivalent frame relay connection. Whether IP or frame relay makes sense for connecting corporate sites on a WAN depends on multiple factors, including the degree of meshing needed between sites and the bandwidth speeds required.

Where IP VPNs demonstrate clear cost advantages is if two connections are currently being used at a corporate site and one of those can be eliminated by using an IP VPN.

For instance, nearly 99% of all medium and large U.S. businesses provide Internet access to some or all of their employees. As a result, an IP connection is present at most such locations. If companies are connecting their corporate locations via frame relay, then they have both an IP connection for Internet traffic and a frame relay connection for WAN traffic. If the WAN traffic can go over the IP connection using an IP VPN, then the frame

connection can be eliminated. While additional bandwidth may be needed on the IP connection to handle the additional traffic, the cost of a higher-speed connection is dramatically lower than a second WAN connection. The elimination of redundant site connections is where IP VPNs make the clearest cost sense.

The deployment of IP-based applications, including intranets, CRM, ERP and sales databases, has been another significant driver of IP VPNs. Applications that are IP do not need to be converted back and forth into various protocols while traversing the WAN. IP-based applications are IP on the headquarter's location's LAN, stay IP in the WAN, and end up IP on the branch office's LAN.

Why does this matter? It is considerably more efficient. Protocol conversion is easily done, but such a process adds complexity, and errors occur. Errors require retries, which cause delay. An IP VPN is a more efficient method of transport for IP-based applications.

Better outsourcing options are currently available than in the past for those wishing to deploy IP VPNs. In 1999, IT consultants and carriers were just getting their feet wet with IP VPNs, and the implementations that were available were relatively rudimentary and often came in a one-size-fits-all variety. Carriers have improved these services considerably and have multiple options available for different customer needs.

The Business Case for IP VPNs

Reasons to Deploy

Why bother with a relatively new and complex technology when there already exist many long-established WAN options in the marketplace today?

The only thing
more impressive
than the bite is the speed.

Deadly Fast VPN

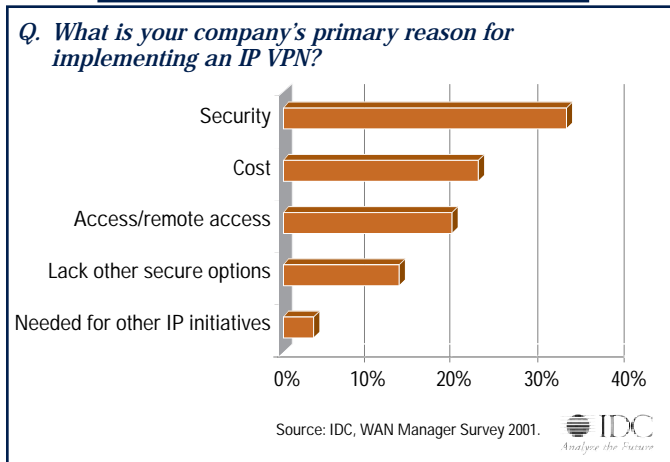
NETSCREEN
Scalable Security Solutions

Click to download the white paper
"Solving Business Problems With Virtual Private Networks!"

[NetScreen Technologies](#)

There are various answers to this question. The results from IDC's WAN Manager Survey show a few of them, as shown in Figure 1.

FIGURE 1: Reasons for IP VPN deployment



Security tops the list. It is likely that many respondents have remote-access IP VPNs in mind when responding to this question, not only because remote access is the most popular use of IP VPNs but also because simple Internet dial-up is really the only remote-access option available to users.

That security scores highly in 2001 represents a big change from 2000, when most people associated IP VPNs with the Internet and hackers. It seems that the concept of IP VPNs is beginning to set in — that IP VPNs use the Internet in a secure way.

The one category where IP VPN did not show up as highly as expected was the last one: “needed for other IP initiatives.” IDC expected IP VPNs to be deployed because IP-based applications are proliferating throughout the enterprise. That may still be the case, but it did not score as highly as anticipated.

There were several “other” answers from the survey that allowed for short written answers. Although “other” was not popular, those that did offer this response listed “way of the world” and “management made the decision” as reasons for deployment.

These are terrible reasons to deploy an IP VPN. There are enough good, solid reasons why IP VPNs make sense — a company should not need to resort to following a trend or letting some CEO that read an article on IP VPNs decide on WAN options. A reasoned, empirical analysis of a company's site and remote user WAN needs may very well conclude that an IP VPN is the most effective WAN option for a wide variety of companies (see Figure 1).

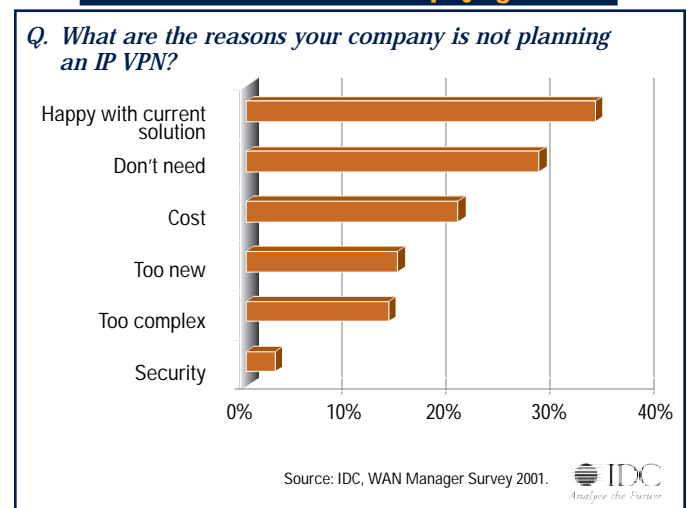
Reasons Not to Deploy

There also are reasons for why a company may not wish to deploy an IP VPN. The WAN Manager Survey indicates a few such reasons (see Figure 2).

The most consistent reason companies have not deployed or are not planning to deploy an IP VPN is that they are happy with their current WAN solution. For most companies, that WAN solution is frame relay.

Frame is a very established technology, and WAN managers have a great deal of experience with it. Carriers that offer frame relay are also very experienced, since the technology is a staple in WAN networking.

FIGURE 2: Reasons for Not Deploying IP VPNs



ZyXEL's
ZyWALL Series
AFFORDABLE
VPN
Security
Firewall
Gateway Routers
800-255-4101

ZyXEL

In 1999, IDC publicly stated that IP VPNs would not displace all other WAN technologies, and we were criticized for saying that frame relay was here to stay. Companies' comfort with traditional data technologies is a big part of the reason IDC believed frame would remain and why it does indeed remain. Very few WAN technologies ever die completely. Frame relay will have a place in corporate WANs for a long time to come. IP VPNs will grow faster, however.

In a related response, "don't need" IP VPNs was a popular reply. Some companies simply may not require the advantages that IP VPNs provide. If a company does not have secure remote-access needs, or extranet requirements, or if it has a good deal on frame relay for connecting corporate sites, then IP VPNs will be a relatively complex and unneeded WAN solution.

Security showed up as a reason not to deploy, but in much lower numbers in 2001 than in the past. Some respondents still associate IP VPNs with the dangerous and insecure Internet.

Comparing Figure 1 and Figure 2, you will notice that cost shows up both as a reason to deploy and a reason not to deploy an IP VPN. There are several explanations for this apparent anomalous result.

For some companies, IP VPNs may have dramatic cost savings (eliminating redundant data connections, for instance). Others may not save much if their frame relay network connections are not complex and they have good financial terms with their frame provider.

Another explanation revolves around what costs are included by survey respondents and what is in their minds when asked this survey question. No doubt some companies compare only the cost of frame relay to the cost of IP VPN connections. Some other respondents no doubt include the cost of transitioning to a new WAN technology. Still others may include IT staff time and training for IP VPN deployment.

Why Deploy an IP VPN?

- Cost
- Ease of use
- IP-based applications
- Remote access

So why does IDC think IP VPNs make sense for many companies? There are several reasons:

There may be significant cost savings for IP VPNs, depending upon a company's current WAN configuration. As mentioned

above, if a company can eliminate a redundant WAN connection, the cost advantages can be large.

It is not fair to say that IP VPNs are always much cheaper than frame relay and other data technologies. The price of frame is decreasing, and much anecdotal evidence exists to suggest that frame relay carriers cut their pricing significantly when existing frame customers talk about IP VPNs and imply they may jump to another carrier.

Some configurations of frame may also yield lower prices than some IP VPN configurations. The same holds for private lines. Multiple point-to-point private lines will surely cost more than an IP VPN solution. The degree of savings depends greatly on the individual customer's network and needs.

It is incorrect to say that IP VPNs always and everywhere cost less. IP VPNs are likely to reduce the overall cost of a WAN solution, but multiple factors are at play and no blanket statements can be made.

IP VPNs make changing WAN configurations easier. The number of IP VPN connections do not make as much of a difference to the complexity of the WAN as it would with a private line or frame relay solution. Customers do not need to worry as much about the number and location of various sites as they would for a meshed frame network.

IP VPNs make sense if a company is planning the deployment of IP-based applications like intranets or global sales databases.

Remote access is a particular problem for WANs, since there are few alternatives. The Internet is ideal for remote access, because it extends just about everywhere. Users can dial into local POPs from nearly anywhere they are likely to travel. Frame relay connections do not travel.

Make Open Networks Trustworthy

- Protect VPN Investment
- Enforce Personal Firewall & Antivirus
- Prevent Application Hijacking

SYGATE [click here](#)

[Sygate Technologies, Inc.](#)

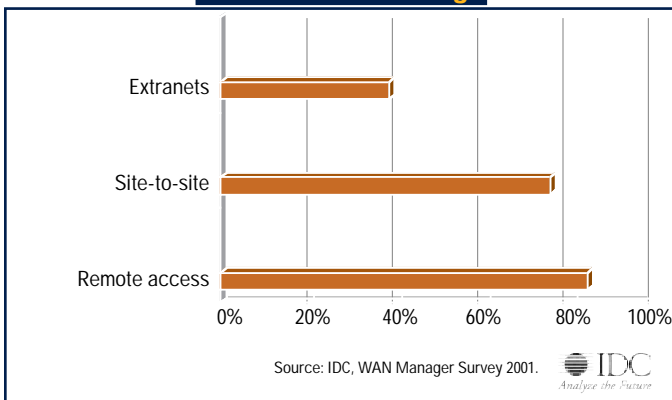
So the remote access options are Internet dial without security and IP VPNs with security. If the company is going to allow access to LAN resources, IP VPNs make definite sense.

How IP VPNs Are Being Used

There are basically three ways in which IP VPNs are being used: remote access, site-to-site connectivity, and extranets.

Figure 3 shows survey data on how IP VPNs are used and what they are used for. Multiple responses were allowed, and it is clear that IP VPNs are typically deployed in order to meet more than one of these connectivity needs.

FIGURE 3: IP VPN Usage



Of the companies currently using IP VPNs, 83.5% of them are using them for remote access. This result is not a surprise, since there are few other options for remote users. Site-to-site is also popular — 75% of the companies using IP VPNs use them for this purpose.

Extranets deserve special mention. The response rate for extranet usage is 38.4%, but this result is actually quite high compared to survey results from past years. Extranets are often discussed by some in the marketplace as a service in and of themselves. IDC views extranets as an increasingly common use of IP VPN technology, or as an additional benefit or reason to deploy site-to-site and remote-access IP VPN services.

The reason extranets are not ranking as high as remote access or site-to-site in usage is that extranets are often seen as an extra bonus in IP VPN deployments. Companies have few options for extranets. EDI is a tried-and-true technology but it is rather expensive. Extranet IP VPNs can be done with very little additional cost if an IP VPN is deployed for either remote access or site-to-site purposes.

While few companies will roll out an IP VPN only for use as an extranet, over one-third of companies using IP VPNs use them in part for extranets.

Implementation Types

- Network vs. customer premise equipment (CPE)
- Common device options
- Firewalls
- IP VPN-specific CPE
- Routers
- Servers/PCs
- Network-based

Network-based Versus CPE-based IP VPNs

The equipment and software to run an IP VPN service can either be located in the carrier's network or on the customer premise. It is the location of the equipment and where IP VPN functions are performed that determine if an IP VPN is network-based or CPE-based.

Network-based IP VPNs are closely associated with MPLS, which is a protocol that allows an IP network to switch various data technologies. MPLS also allows the first network router to determine the path of the first and all subsequent packets in a data stream. This functionality is very helpful for real-time applications like voice and video, in which the quality of the service is greatly impacted by the order in which packets are received. You want the first syllable of your word to reach the listener before the second syllable, of course.

These traffic-engineering capabilities are relevant for IP VPNs, because it is one way that data privacy is ensured. MPLS separates different customers' traffic on the network in a way that is very similar to frame relay permanent virtual circuits (PVCs). MPLS partitions customer traffic.

Thus, a carrier that has deployed MPLS in its network, by definition, makes all of its IP customers attached to it IP VPN customers, by virtue of the traffic-partitioning feature of MPLS.

MPLS has quality of service (QoS) capabilities that allow users to give packets various priorities. QoS ensures that time-sensitive



applications receive priority status over the IP connection and on the IP network.

While network-based IP VPNs are closely associated with MPLS, the two are not synonymous. Network-based IP VPNs can use the traffic-partitioning capabilities of MPLS, or the carrier can simply place IP VPN equipment in the network cloud, often in data centers on the carrier network.

Thus, a network-based IP VPN service could be based on firewalls in the carrier data center. This is one example of a network-based IP VPN that does not use MPLS.

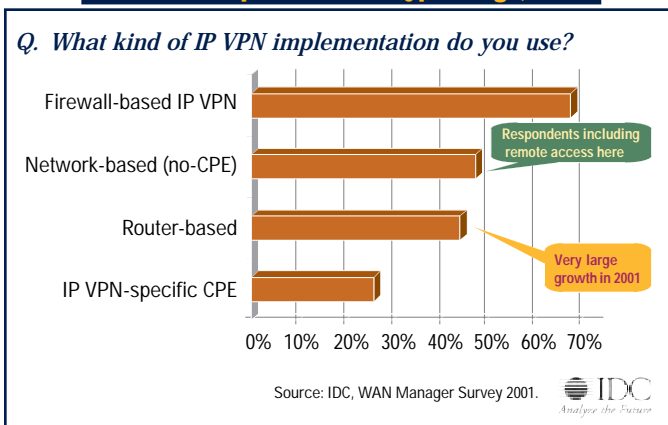
Device Options

Virtually any device with a microprocessor can perform IP VPN functions, such as creating tunnels and encrypting packets. These can be routers, servers or even PCs. Software, such as firewalls, can also perform IP VPN functions.

No one device or method is necessarily better than any other. The best implementation depends on the customer's needs, existing network devices, and cost considerations.

Figure 4 shows what implementations were used and in what intensity in 2001.

FIGURE 4: Implementation Type Usage, 2001



Firewalls are the most popular IP VPN service implementation (see Figure 4). The reasons, perhaps, are not surprising. Firewalls are often already present on the corporate site, many carriers already offer managed firewall services, and firewalls are already associated closely with security. Why not add IP VPN functions with their related security features right on a device or piece of software that handles this function already?

Many of the do-it-yourself implementations use the firewall method. It's a relatively inexpensive and easy-to-implement solution, and corporate LAN administrators already use and operate firewalls.

However, firewalls were not originally designed for IP VPN functionality, and new features have had to be added to make them IP VPN ready. Most firewall vendors have done this, recognizing the market demand and the logical fit between firewall security and IP VPN security features.

IP VPN-Specific Devices

A common method of implementing an IP VPN from a carrier is to use a device specifically designed just for this purpose.

These devices have the advantage that they are designed specifically for IP VPNs. The devices do not tap the resources of other devices that have functions other than that of a VPN, such as routing or protecting the corporate network from intrusion.

A disadvantage of these devices is that they represent one more box that needs to be placed somewhere at the corporate location or in the network. And since other, already existing devices at the corporate site can perform these same VPN functions, a VPN-specific device may become just one more piece of hardware taking up space.

Routers

Several carriers have IP VPN implementations that include a router implementation. Routers will inevitably be a common implementation for the do-it-yourself market, which will run IP VPNs on their existing routers at corporate sites.

The major advantage of this choice is that the corporate site probably already has a router existing at the location and routers exist in the carrier networks. A major disadvantage is that many routers are already fully tasked with important functions, and adding VPN tasks may reduce the performance of the routers for routing traffic — in theory their primary function. Router vendors often offer acceleration cards that will speed processing power to perform IP VPN tasks more efficiently without additionally taxing the router's processing resources.

Servers/PCs

Any computer can be made to perform VPN functions. This implementation is typically done on a server running software such as a firewall. However, even a simple PC can perform functions for VPN implementations that are not too complex.

PCs and servers may be very popular with do-it-yourself customers because special equipment is not needed and cus-



tomers will most likely not need to make special capital investment in equipment. Also, IT departments are very familiar with PCs and may not be as intimidated as by an IP VPN-specific device with which they have little or no experience.

Network-Based VPNs

Perhaps the most logical IP VPN implementation for a carrier is the network-based IP VPN. All IP VPN functionality is located in the "cloud," or the hub, point of presence (POP), or data center. Several carriers offer a network-based IP VPN service in which all dial-user authentication is done by RADIUS servers in the carrier network, and all encryption and tunneling is done once the IP traffic hits the carrier network.

The advantages of a network IP VPN are that no new CPE is required, it's relatively easy and painless for the customer to establish it and get it up and running, and it can be a very cost-effective solution compared with managing CPE internally by already-stretched IT staff.

Also, numerous equipment options are typically available, with all the equipment residing in the carrier network.

The biggest disadvantage of a network IP VPN is that encryption and decryption are done in most cases once the IP traffic hits the carrier network. Thus, traffic on the last mile is not encrypted or secured. This may not be as huge a security breach as it may seem, since that local loop is dedicated to that particular customer, but given the human traffic in regional Bell operating company (RBOC) central offices and the fact that the loop cannot be completely secured from a determined data thief, this solution may not be adequate for customers that have very stringent security requirements.

Another advantage (or disadvantage, depending on one's perspective) of a network IP VPN is that configuration changes and maintenance, by necessity, are executed by the carrier and not on the customer premises. Some overworked WAN managers (or those less at ease with the complex technologies underlying an IP VPN service) may be very happy to inform the carrier of configuration changes that are needed and let the carrier's staff alter the IP VPN service as specified.

Other more controlling, or paranoid, WAN managers (or those very experienced with the various IP VPN technologies involved) may well want to be able to see and reach IP VPN equipment at a moment's notice, or simply sleep better knowing it is within their reach. So the lack of CPE is either a big advantage or big disadvantage depending upon the customer's needs and on the carrier and its range of IP VPN service implementation options.

IP VPN Providers

Do-It-Yourself (DIY)

DIY is still the biggest IP VPN service provider in the United States. An increasing number of companies are choosing a carrier-provided IP VPN solution, but DIY is still the most popular IP VPN provider. The reasons are many and varied, but IDC believes the following are the main reasons:

- **Cost.** IP VPNs are being implemented primarily because of the perceived cost savings of this WAN alternative. What could be less expensive than doing it yourself? But the WAN Manager Survey results show that carrier implementations are growing in importance. IDC believes that many companies have tried IP VPNs on their own and either failed to realize cost savings (when the cost of personnel time is included), or the technologies proved too cumbersome to administer with relative ease.

- **Control.** The desire to maintain tight control over the IP VPN was also a strongly cited reason for a DIY implementation. WAN managers and LAN administrators are not known for their ability to trust others. These individuals tend to like to have a maximum amount of control over their networks, even if their systems become so complex that control is an illusion. The perception that keeping the IP VPN in house gives the organization the greatest amount of control is a powerful one in favor of DIY.

- **Slow rollout of carrier services.** Many carriers came out with IP VPN services around mid-1999 (with some exceptions) and robust offerings in late 1999. Even in 2001, carriers are implementing new IP VPN services, adding functions and multiple service choices. Large-scale, robust and cost-effective IP VPN services from carriers have not been particularly rapid in coming. As a result, companies that in the past had looked for an IP VPN that met their particular specifications often found that one was not available from carriers at the time. Carrier IP VPN services, however, are considerably more mature in 2002.

Carriers

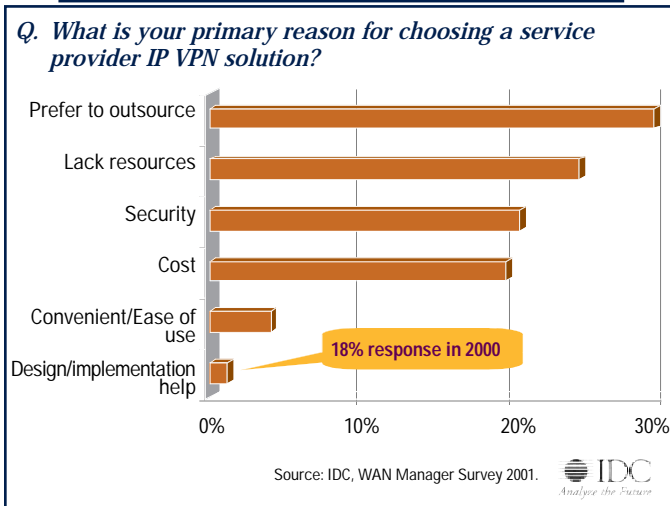
Why would a company go with a carrier when they can do it by themselves? Lots of reasons.

Figure 5 shows survey data as to why companies chose to use a carrier's IP VPN solution.



A preference for outsourcing (a combined category from multiple individual answers) is the biggest reason. This is not the slightest bit surprising.

FIGURE 5: Reasons for Carrier IP VPN Solutions



Most WAN managers deal with frame relay and other data services providers. In a frame relay WAN, for instance, WAN managers are not setting authentication policies or making configuration changes on their own. They have their provider make those changes for them as part of the service.

A carrier-managed IP VPN frees up the WAN manager to manage the WAN and not force him/her to run the WAN. Most WAN managers and LAN administrators are not very familiar with WAN operational issues and may not feel comfortable with their ability to manage it well themselves.

Traditional WAN technologies are run and managed day to day by a carrier, and many WAN managers may want a similar management solution for an IP VPN.

The second-most-popular reason given in the WAN Manager Survey for using a carrier was lack of internal resources. Even if WAN managers or LAN administrators are capable of running an IP VPN on their own, they may lack the time to do so.

What to Look for in a Carrier Solution

There are several criteria any potential IP VPN customer should use in evaluating carrier options. Some of the items here may be of less importance to some users, and some users may have additional criteria. The essentials are listed here.

- **Financial security.** Will the carrier be around in 2003? An IP VPN implies that the connection is mission-critical. You don't want to outsource a mission-critical element to a carrier that may shut you off if its business model fails.

- **Coverage.** Does the carrier you are considering provide access in all locations where your company does business? If you plan a remote-access IP VPN, does the carrier have local-access numbers in all the locations where your employees will travel? If not, you will end up paying long-distance charges if the carrier does not have its own network or a roaming agreement with a carrier that does have local access in all those areas.

- **Remote access, site-to-site, extranets.** Does the carrier support all your IP VPN needs? If you are only planning a remote-access or only a site-to-site IP VPN, you will have more options. But if you plan both types, the carrier should offer both as a standard service. And if you plan to connect customers or suppliers to your IP VPN to form an extranet, make certain the carrier does not require those customers or suppliers to have that same carrier's connectivity to reach your IP VPN. It may be easier to force your suppliers to change IP carriers, but don't try to tell your customers they need to change providers.

- **Service level agreements (SLAs).** Are the carrier's SLAs comprehensive, with monitoring and credits with teeth? SLAs are very technical and legal documents, and it is important to read them carefully. Does the carrier offer competitive SLAs that allow you to monitor performance? Does the carrier proactively notify you if a credit is missed, or do you need to catch it yourself and file a trouble ticket to get credit? Do the SLAs have credits with real penalties for the carrier if missed, or do they have clauses that require the carrier to miss the credit for two consecutive months in order for the credit to be issued? Do the SLAs include a provision to allow you to cancel the contract at no penalty should the SLAs be badly missed? Credits are needed in SLAs, but you should find a carrier that has strong credits on which they never pay credits. If your connection is mission critical, the credit amount will not make up for downtime or poor performance.

- **QOS.** If you are running or planning to run real-time applications over your IP VPN, does your carrier have QOS capabilities with MPLS, DiffServ or other protocols to ensure that they perform as needed?

Conclusion

IP VPNs are a collection of technologies brought together to ensure the privacy of WAN data over IP networks. IP VPNs are



growing in popularity — nearly half the medium and large enterprises in the United States use them.

IP VPNs are growing so rapidly because they are meeting the needs of businesses. IP VPNs allow for secure remote access for traveling or telecommuting employees. Site-to-site IP VPNs can offer a cost advantage over traditional data technologies and also allow for the addition of added features like extranets, as well as the relatively easy deployment of advanced IP services.

IP VPNs can function on the customer premise or in the carrier's network, and both types can use numerous devices and technologies to accomplish IP VPN functions. What particular implementation is best depends greatly on each company's unique business needs.

IP VPNs can be done in-house or purchased as a fully managed option from a carrier. While do-it-yourself is still the largest provider in the United States, that position will be eroded over time as carriers expand and improve their offerings and as more companies choose to leave WANs to the service providers with expertise in day-to-day WAN management.

Finally, the growth of IP VPNs is not a fad or pie-in-the-sky idea, like ubiquitous fiber to the curb or renting Excel from an ASP per use. Rather, IP VPNs make a lot of sense for most companies because they are flexible, cost effective, and enable numerous additional technologies and services that help meet today's business needs.

Steven Harris is research manager in IDC's ISP Markets, Business Network Services, and IP VPN research programs. Steven can be reached at sharris@idc.com.

Additional VPN & IP VPN resources on the Network World Fusion Web site — www.nwfusion.com

Network World on VPNs newsletter

Offers everything from how-to tips to analysis of the latest vendor and carrier offerings to make VPNs easier to understand and build.

<http://www.nwfusion.com/newsletters/vpn/index.html>

VPN research page

Get up to speed on VPN issues, including wireless VPNs, secure VPNs, MPLS, QoS and more.

<http://www.nwfusion.com/research/vpn.html>

Breaking VPN news

Keep up to date on the latest vendor, technology and product news.

<http://www.nwfusion.com/topics/vpn.html>

VPN audio primer

In this 6-minute primer, learn how VPNs work, as well as if they are right for your remote access needs.

<http://www.nwfusion.com/primers/vpn/vpnprimer.html>

Crafting service-level agreements for IP VPNs

Outlining key elements that are essential to include in every SLA.

Network World, 11/19/01.

<http://www.nwfusion.com/columnists/2001/1119eye.html>

Know what you are getting with your IP VPN

IP VPNs have advantages, particularly flexibility, dynamic bandwidth and the ability to provide secure connectivity to outside organizations. But not all IP VPNs are created equal.

Network World, 11/05/01.

<http://www.nwfusion.com/columnists/2001/1105eye.html>

VPNs: IP adds a new twist

IP VPNs are the latest wave in site-to-site connectivity, but not the least painful.

Network World, 09/24/01.

<http://www.nwfusion.com/buzz2001/ipvpn/>

