Virtual Private Networks

By Rick Blum, Research Programs Manager, and Jeffrey M. Kaplan, Director, Strategic Marketing

Highlights

- Two-thirds of respondents indicate that VPNs will be very important to their overall IT strategy within12 months, and another quarter state that they will be somewhat important.
- Organizational issues, including processes and procedures, is most frequently cited as the biggest challenge in resolving VPN issues. Last year the top challenge was technological issues.
- The top barriers to improving VPN capabilities are lack/immaturity of products or services and the lack of experienced staff/staff training required.
- The single most important networking objective driving VPN strategies is to improve remote access networking capabilities. The most important business driver is providing remote access to mobile workers.
- By more than three to one, current VPNs are implemented internally, compared to externally managed VPNs. The ratio of internal solutions to external solutions drops to only 1.6 to 1 for respondents considering or evaluating future VPNs.
- A wide range of VPN types are being considered by respondents, from router-based to dedicated device to managed service. The top technologies to be implemented in these VPNs are IPSec for tunneling, digital certificates for access, and RADIUS for authentication.
- Eight-two percent of respondents are satisfied with the VPN products currently available. The greatest gap between importance and satisfaction of specific VPN features is for manageability, ease of integration, and quality of service.
- The top areas in which respondents need help in evaluating, implementing, or enhancing their VPN capabilities are designing (including vendor selection) and planning (including technology decisions).

NetCare®
The knowledge behind the network™

Lucent Technologies
Bell Labs Innovations

Contents

About Lucent Technologies NetCare

Lucent Technologies NetCare® is a global provider of network consulting and software solutions for the full lifecycle of a network, including planning and design, implementation, and operations. We maintain expertise in the most complex network technologies and multi-vendor environments. Through our VitalSoft division, Lucent NetCare offers industry-leading software solutions for managing and optimizing application-ready networks. Lucent Technologies is headquartered in Murray Hill, New Jersey, USA. The Lucent NetCare website is http://www.lucent.com/netcare.

For more information regarding Lucent NetCare network consulting and software solutions capabilities, call 1-800-4-NETCARE or e-mail: netcareinfo@lucent.com.

For further information regarding this survey, please contact:

Jeffrey M. Kaplan
Director, Strategic Marketing
(617) 376-2450, Ext. 236
E-mail: jeffkaplan@lucent.com

or

Rick Blum
Research Programs Manager
(617) 376-2450, Ext. 320
E-mail: rickblum@lucent.com

Introduction

Virtual private networks (VPNs) have become one of the hottest technologies in the last year, promising substantial reductions in wide-area networking costs and improved access for remote workers and branch offices, as well as for partners and customers. It is, however, a quickly evolving technology that bears constant attention in order to effectively implement the latest advances.

In November and December 1999, Lucent NetCare (formerly INS) conducted a Web-based survey on virtual private networks, which was completed by 175 network professionals. A previous survey on VPNs was conducted in September 1998. Together, these surveys yield valuable insight into the past, current, and future VPN strategies of network professionals, as well as the major trends in the adoption of VPNs and VPN technologies. They also identify the barriers and challenges that network professionals expect to encounter as they plan and implement VPN strategies. These results will assist networking organizations to assess their individual progress as compared to the industry, and identify opportunities for improvement. The complete results of both surveys are available at www.ins.com/surveys.

For this survey, virtual private network is defined as a computer network designed to use a shared wide-area network (WAN) infrastructure, such as the Internet or a managed network service, to transport data communications using Internet Protocol (IP). VPNs use tunneling, encryption, authentication, data integrity, and access control technologies to ensure secure transport. VPNs can be implemented internally with all VPN functionality residing outside the service provider network (WAN), or can be managed solutions provided by an external service provider, with the VPN capabilities ending at the WAN edge.

THE BOTTOM LINE

The demand for virtual private networks is being fueled by enterprises that need to improve their remote access capabilities – especially for mobile workers, but also to branch offices and business partners – while simultaneously lowering the cost of this access. Internally developed VPNs have led the early market charge, but managed VPN services will be considered more frequently as service providers are able to meet requirements for high security levels and availability. As network directors and managers ponder the many choices among technologies and VPN strategies, they should take the following into account:

- A shortage of experienced network professionals skilled in VPN technologies will remain for some time. Any evaluation of the advantages of an internal implementation versus a managed VPN service should take into account this factor, giving due consideration to the cost of acquiring and/or retaining VPN expertise while ultimate technological directions are still uncertain.
- VPN protocols and technologies for access and authentication are still evolving, as are the various options for implementing a VPN in software or hardware. Try to balance short-term needs for specific capabilities against long-term advantages of compatibility and interoperability when selecting among these options. The goal is to find a solution that will follow these tenets, and also provide scalability as VPN products mature.
- Technology will be only the starting point for a successful VPN strategy. In the earliest stages of planning, consider the organizational impact of the VPN. Then build into the over all plan the specific processes, procedures, and end-user training that will be required to smoothly transition to a VPN computing model.

Drivers of VPNs

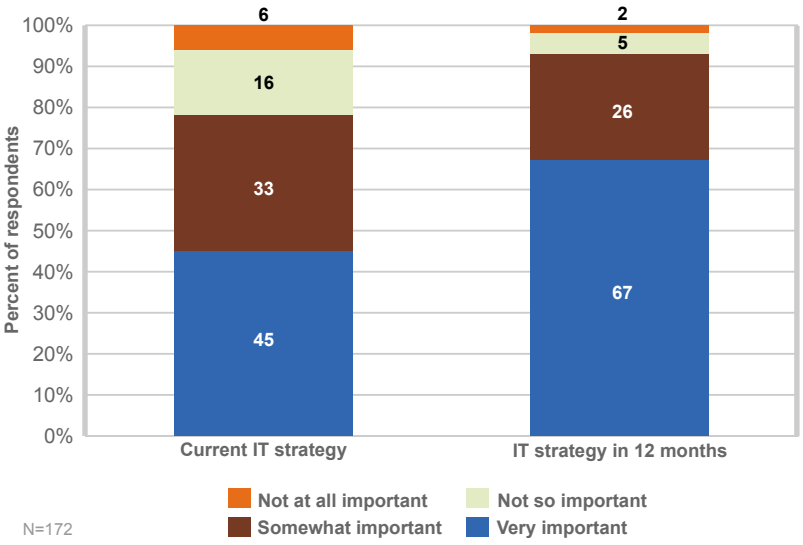
Many potential advantages to virtual private networks have been widely touted by vendors and service providers alike. While the technology is still evolving, many companies have already taken advantage of VPNs' potential, and still more are planning to do so in the coming year.

Although VPNs are still in the early stages of market maturity, nearly half of all respondents (including those with no VPN plans) indicate that implementing or improving VPN capabilities is already very important to their overall IT strategy. A better indicator that the market is still in its early stages, however, is that two-thirds of these respondents state that VPNs will be very important to their overall IT strategy 12 months hence, and another quarter state that they will be somewhat important. Even many respondents with no VPN plans believe that this technology will be important to their organizations in a relatively short timeframe.

A little more than half of respondents in this year's VPN survey have either already implemented or are in the process of deploying a VPN. Another third of respondents do not have a VPN implemented or deployed, but are either considering or actively evaluating a VPN solution. Only 13% of respondents have no VPNs implemented currently, nor plans to consider a VPN solution at this time.[1]

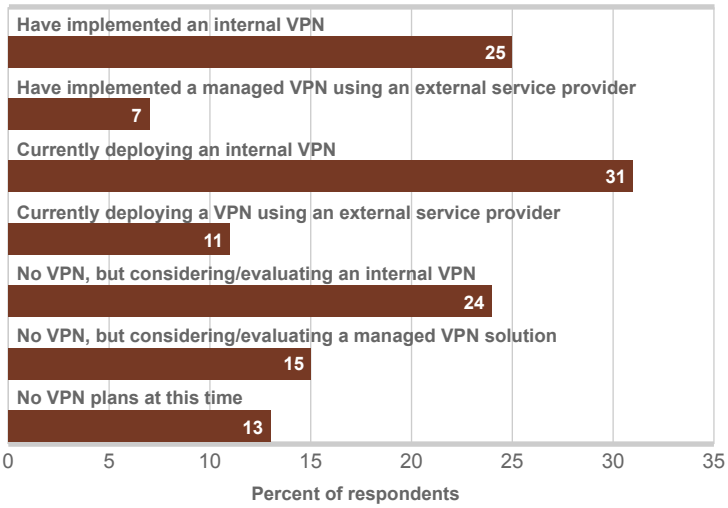
By more than three to one, currently implemented VPNs are done so internally, compared to managed VPNs, which are implemented using an external service provider.[2] For only respondents who are

Importance to IT Strategy of Implementing or Improving VPN



N=172

Current Status of VPN Deployment



N=169

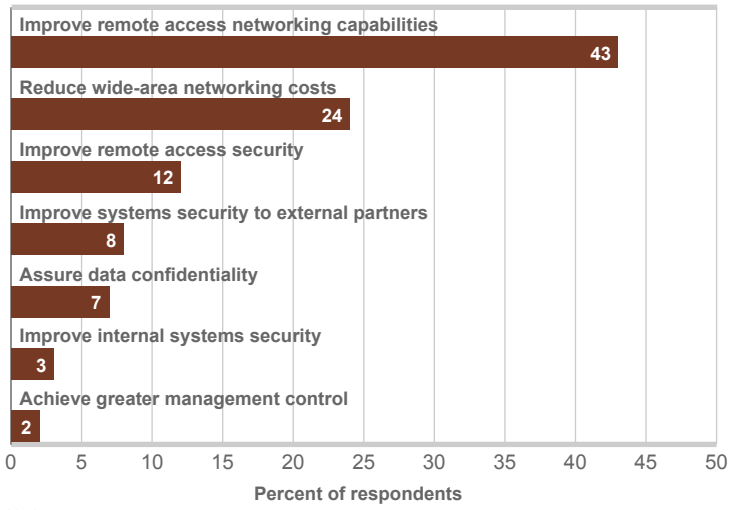
[1] *Respondents with no VPNs or VPN plans are not included in further data relating to VPNs. They are included in respondent demographics.*
[2] *Internal VPNs are implemented with all VPN functionality residing outside the service provider network (WAN). A managed VPN is provided by an external service provider, with VPN capabilities ending at the WAN edge.*

currently deploying a VPN, that ratio is slightly less than three to one. When we look at respondents who are considering or evaluating a VPN solution, the ratio of internal solutions to external solutions drops even more dramatically to only 1.6 to 1. This is a clear indication that as the VPN market continues to develop, enterprises will become more willing to look to external service providers for their VPN solution, rather than investing in the internal infrastructure (products and skills) necessary to add this capability to their networking strategy.

Networking organizations expect to achieve numerous objectives from implementing a VPN solution. When we asked them to name the single most important objective from a list of seven, nearly half (43%) listed *improve remote access networking capabilities.* This is an unambiguous result, indicating that remote access is the primary driver of the VPN market today. Remote access, however, is not the only driver, with nearly one-quarter of respondents' VPN strategies being driven by lowering the cost of wide-area networking. Coupled together, improving remote access while reducing costs will propel the VPN market for the next year or more.

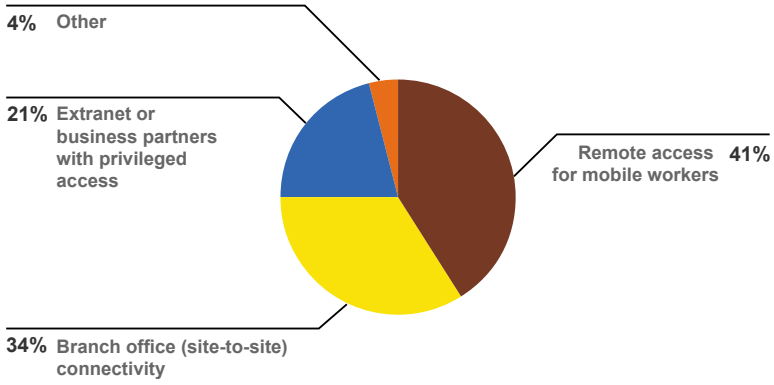
Given that improving remote access is the top networking objective for nearly half of respondents, we also asked which type of remote networking is the most important *business* driver of the VPN strategy. *Remote access for mobile networks* came out on top, selected by 41% of respondents. But *branch office connectivity* and *extranet or business partners with privileged access* each garnered a significant percentage of adherents. Businesses with a large number of mobile workers, such as sales people and service reps, are most likely to be driven by the need to get secure, reliable access to these workers from multiple locations. Other types of businesses might be more likely to focus on the benefits of branch office connectivity or connecting with business partners.

Most Important Networking Objective Driving VPN Strategy



N=147

Most Important Business Driver of VPN Strategy



N=146

VPN Type and Technology Profile

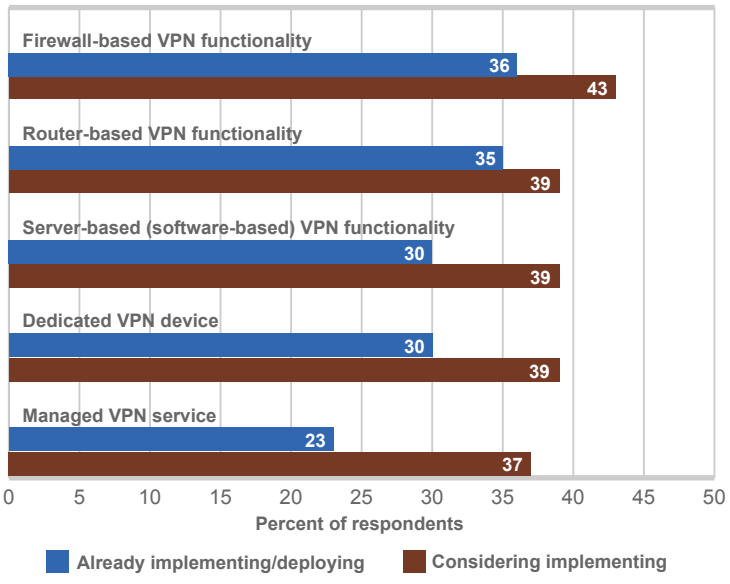
While we previously saw that internal VPNs are the most common type currently implemented, being deployed, or being considered/evaluated, managed VPN services will likely gain ground in the year ahead. Internal VPNs can be implemented in a number of different configurations, including:

- Firewall-based VPNs (VPN functionality is typically supported in the firewall software)
- Router-based VPNs (VPN functionality is supported in the router software)
- Server-based VPNs (VPN software is deployed in the network operating system residing on the network server, and connects to existing OS authentication services)
- Dedicated VPN device (VPN device, including hardware and software, that handles only the functions required for a VPN implementation, such as encryption and tunneling)

Again, reflecting the relative immaturity of the VPN market, no one internal VPN type is either implemented or being deployed significantly more — or less — often than any other, nor is any one type being considered for implementation significantly more or less often than the others. Respondents are showing a remarkably open mind about the type of VPN implementation that they will consider, including managed VPN services. In fact, the typical respondent is considering at least two implementation types.

Besides deciding on the type of VPN that is appropriate, network professionals must choose among a number of different VPN tunneling protocols and authentication and access technologies. Two VPN tunneling protocols are the favorites among respondents: Internet Protocol Security (IPSec) and Point-to-Point Tunneling Protocol (PPTP). IPSec has been implemented or is planned for implementation by nearly three-quarters of respondents, while PPTP is favored by slightly more than half of respondents. IPSec's backing as an international standard protocol could well have given it the boost to become the clear leader. PPTP, however, has the advantage of supporting both IP traffic and IPX traffic, which is not supported by IPSec. The reality is that respondents are considering multiple technologies — and will

VPN Types Implemented or Being Considered



N=128

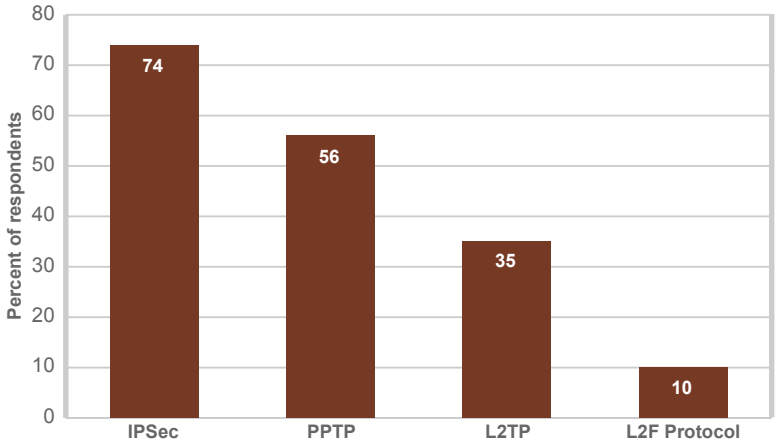
continue to do so for the near future — as is typical in a developing market.

VPNs must be able to verify the identity of and limit access to valid network users using a variety of authentication schemes, either alone or in combination. Two remote-access access services can typically be used: remote authentication dial-in user service (RADIUS) and terminal access controller access control system (TACACS). RADIUS is either implemented or likely to be implemented by twice as many respondents as TACACS. The public key infrastructure (PKI) security standard is favored by 44% of respondents for authentication, far ahead of token cards and Kerberos private key, encryption-based authentication.

Among centralized data stores, such as Microsoft® Active Directory™ and Novell® NDS®, Active Directory is preferred nearly two to one over NDS, even though it was not a released product at the time of the survey. Lightweight Directory Access Protocol (LDAP), which enables communications among X.509 directory services and access services, is being implemented or planned for implementation by 43% of respondents.

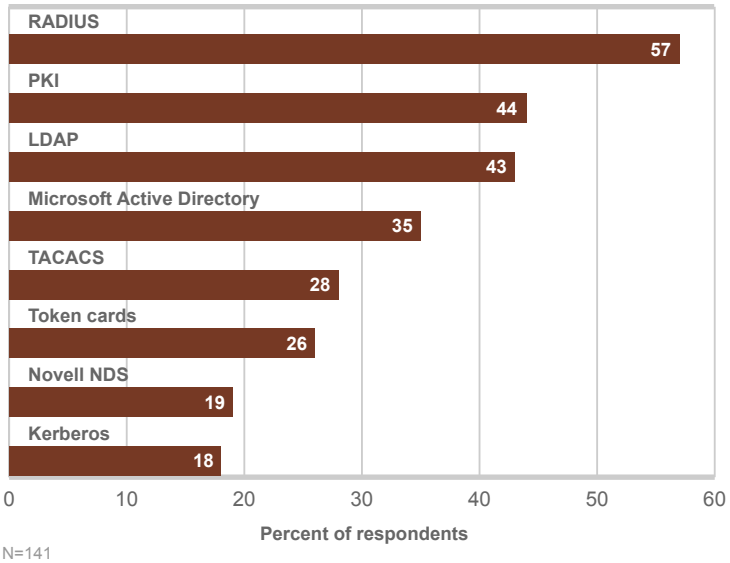
Like tunneling protocols, most network professionals are keeping their options open by looking at multiple authentication technologies.

VPN Tunneling Protocols Implemented or Planned to be Implemented



N=144

Authentication Technologies Implemented or Planned to be Implemented



N=141

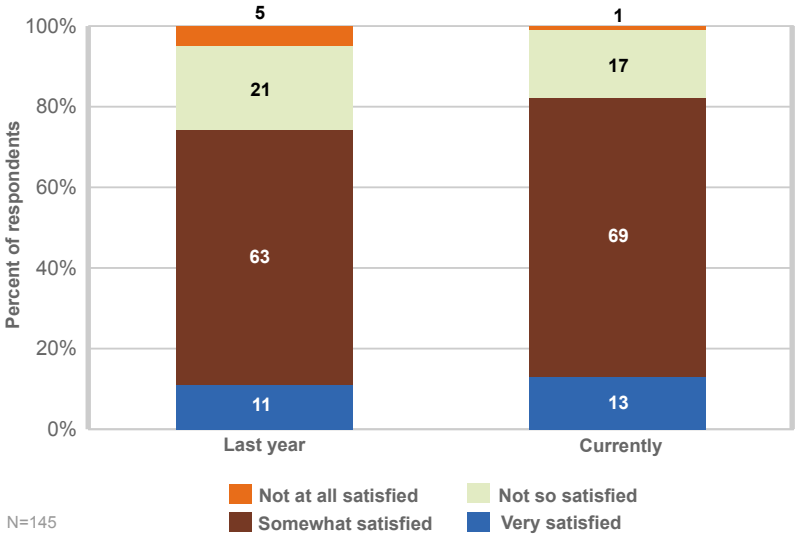
Importance and Satisfaction with VPN Products and Solutions

VPN products have been on the market for a number of years, and although new products are being introduced regularly, there has been ample time to measure satisfaction levels, both past and present. In this year's survey, overall VPN product satisfaction is higher than in last year's survey, although not by enough of difference to deem the change significant. The good news, however, is that the level of satisfaction last year was reasonably good, with 74% of respondents very or somewhat satisfied with VPN products. That satisfaction level has gone up to 82% this year. On a more cautious note, the percentage of respondents who are very satisfied with VPN products is still low, only 13% of respondents this year, which leaves ample room for product improvements.

Respondents are fairly demanding when it comes to evaluating a VPN solution, either an internally built solution or a managed service. Out of 15 factors they could take into account, the one rated lowest in importance, *reduce time to deploy new sites*, still garners a 3.2 rating on a scale of one to four, where one is not at all important and four is very important.

"…the percentage of respondents who are very satisfied with VPN products is still very low, only 13% of respondents this year…"

Satisfaction with VPN Products



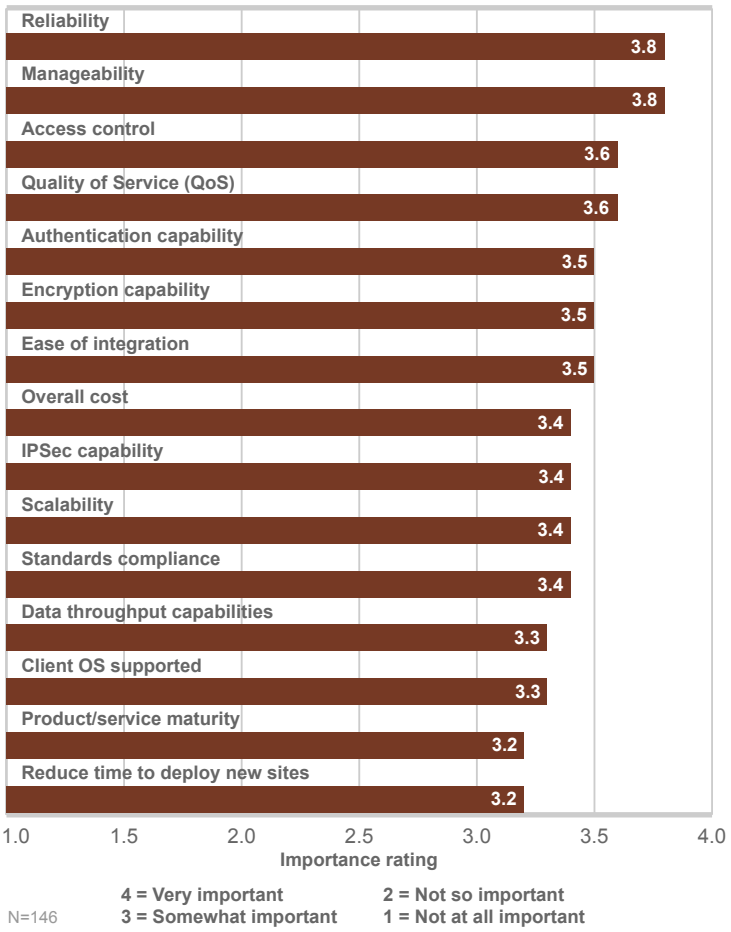
N=145

There is more differentiation among factors, however, if we look just at the *very important* ratings. On this measure, *reduce time to deploy new sites* is very important to only 37% of respondents, while *reliability* is very important to 86% of respondents. Factors that are very important to a majority of respondents are:

- Reliability 86%
- Manageability 75%
- Access control 69%
- Quality of service 64%
- Authentication capability 61%
- Encryption capability 57%
- Ease of integration 54%
- IPSec capability 50%

Clearly, network professionals most highly value characteristics that enable them to have a stable, controllable environment.

Importance of Factors for Evaluating VPN Solution (Internal or Managed Service)



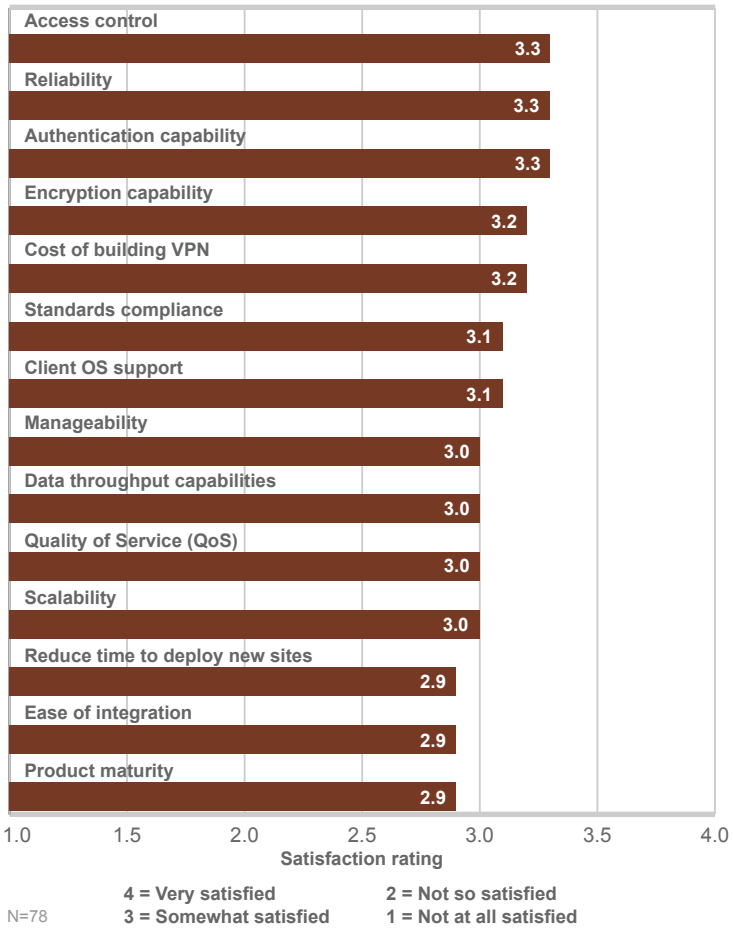
"…reliability is very important to 86% of respondents."

Respondents who have already implemented an internal VPN solution are fairly satisfied with the results. For every one of 14 factors affecting VPN satisfaction, at least 73% of respondents say they are very or somewhat satisfied. *Access control, reliability,* and *authentication capability* are tied for the highest satisfaction ratings. The difference between this top rating, however, and the bottom rated *product maturity, ease of integration* and *reduce time to deploy new sites* is relatively small – only 0.4.

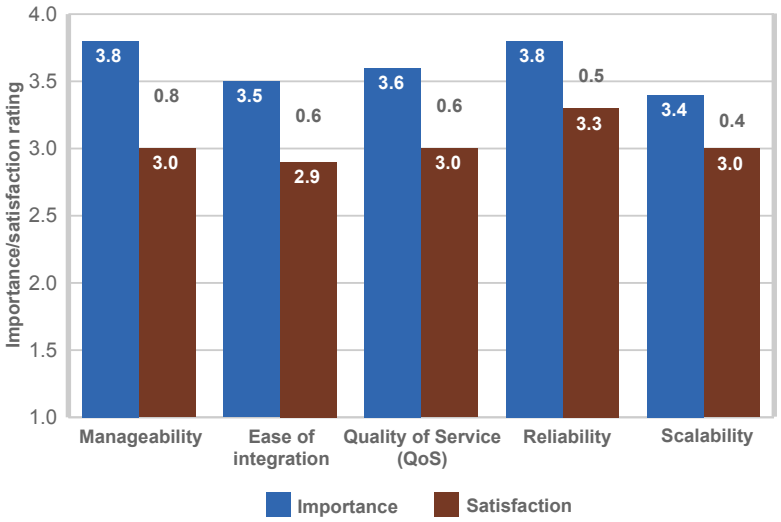
Although the satisfaction ratings are generally good, there are two concerns. The first is that on not a single factor are more than 41% of respondents very satisfied. The other concern is that all satisfaction ratings are lower than their equivalent importance ratings, which translates to an average importance rating of 3.5 versus an average satisfaction rating of 3.1. The top five factors with the greatest gap between importance and satisfaction are *manageability, ease of integration, quality of service (QoS), reliability,* and *scalability.* Vendors of both VPN products and managed services should read this list closely to use as a guide to areas that require

"…all satisfaction ratings are lower than their equivalent importance ratings…"

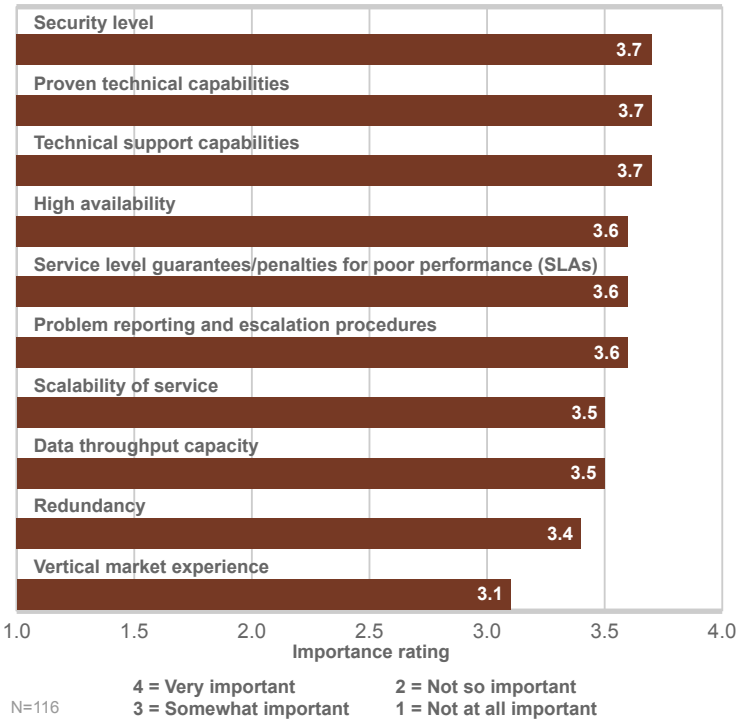
Satisfaction with Internal VPNs



Factors with Greatest Gap Between Importance and Satisfaction



Importance of Factors When Evaluating a Managed VPN Service



immediate improvements, and can provide the highest payback.

When selecting a managed VPN service, there are additional factors that network professionals should take into account. Again, respondents prove to be very demanding, as they universally consider 10 different factors important to consider. And, except for *vertical market experience* and *redundancy,* all are considered very important by more than half of respondents. As we saw earlier, there appears to be a growing interest in managed VPN services, but the bar that respondents set for VPN service providers is a high one indeed.

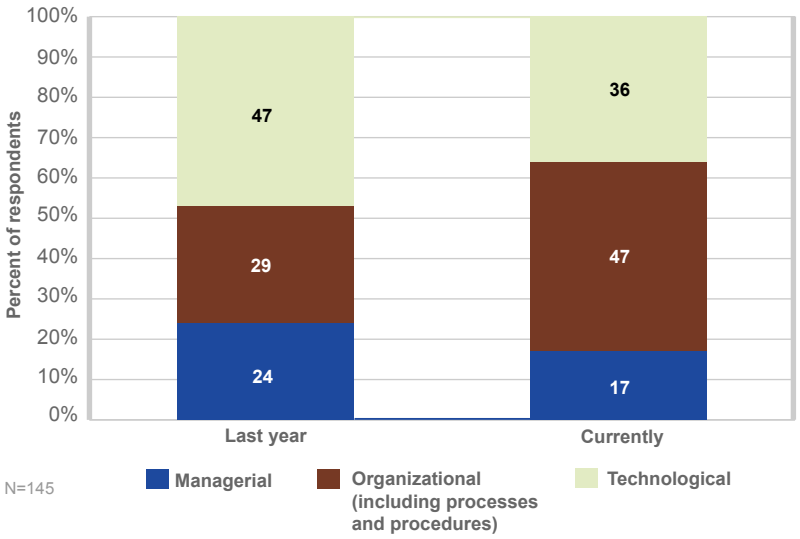
VPN Challenges and Barriers

Being a relatively new technology, it would be reasonable to expect that technological issues would be foremost on most network professionals' lists of challenges for resolving VPN issues. And that was true last year when 47% designated technological issues as their biggest challenge. But this year is quite different. While technological issues are still the top challenge for 36% of respondents, organizational issues, which include processes and procedures, are now the top challenge for 47% of respondents. Managerial issues are the top challenge for 17% of respondents, down from 24% last year.

This reversal in the order of biggest challenge is not unusual. As technologies mature and are implemented more widely, the technological issues lessen while, simultaneously, operational issues increase. Network professionals are all too familiar with technologies that fail because proper processes and procedures are not followed. We expect that organizational issues will continue to grow in importance as VPNs become more integrated into the network infrastructure.

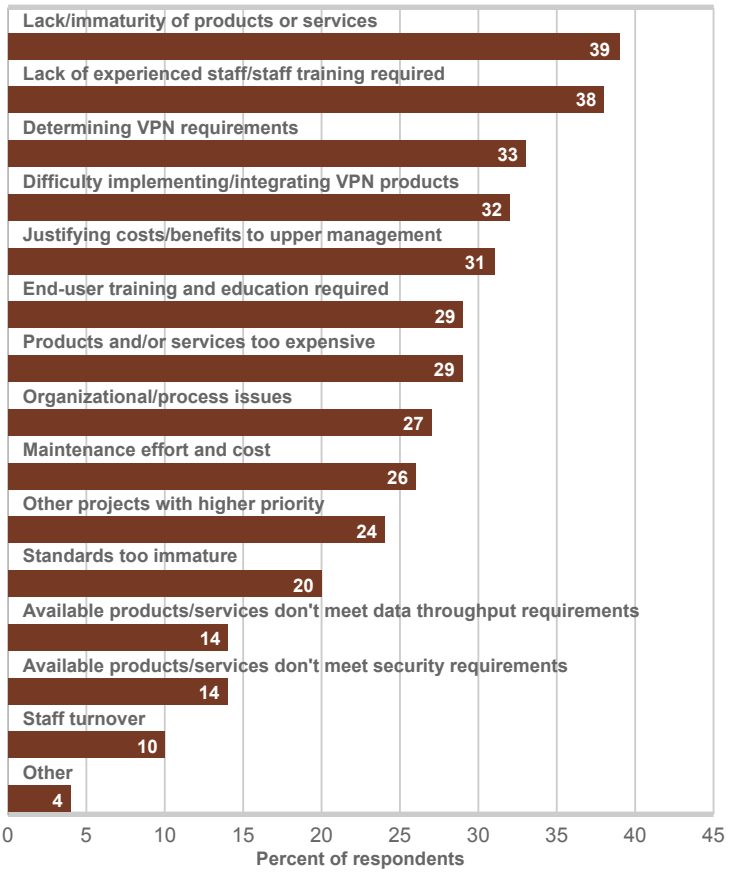
Network professionals recognize many of the challenges that lie ahead in implementing VPNs. They also recognize that there are many potential barriers to be overcome. Even though they understand that organizational issues are going to take a high level of priority, 39% of respondents still

Area That is Biggest Challenge to Resolving VPN Issues



N=145

Significant Barriers to Improving VPN Capabilities



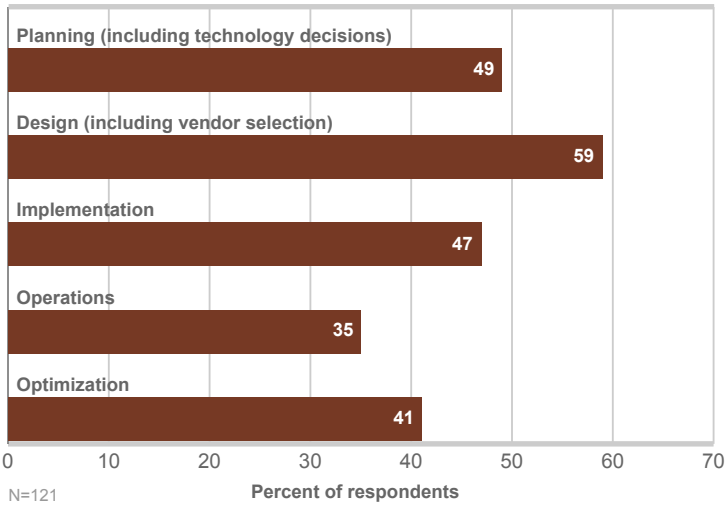
N=144

recognize that the immaturity of VPN products or services will be a barrier. However, this percentage is down from 47% on last year's survey, echoing the decline in technological issues as their biggest challenge.

Nearly as often a barrier as product immaturity is the lack of experienced staff and the amount of staff training required, a barrier to 38% of respondents. Being a relatively new technology, it is reasonable to expect that these would be hurdles for a high percentage of network organizations. However, it is somewhat surprising that last year this was a barrier to only 20% or respondents, reflecting, perhaps, a much higher level of VPN activity in the past year.

The typical respondent chose three to four barriers to improving the VPN capabilities in their organization. Some may feel that they can overcome these barriers internally, but most recognize that they require assistance in one or more aspects of the network lifecycle to successfully execute their VPN strategies. Of those respondents who recognize the need for this assistance, the majority point to VPN design (including vendor selection) as an area in which they need help. But VPN planning (including technology decisions) and implementation are also areas in which a large percentage of respondents need help. As more network organizations move through the VPN lifecycle, we'd expect to see a shift toward higher assistance requirements in operations and optimization.

Areas in Which Help is Needed to Evaluate, Implement, or Enhance VPN Capabilities



"The typical respondent chose three to four barriers to improving the VPN capabilities in their organization."

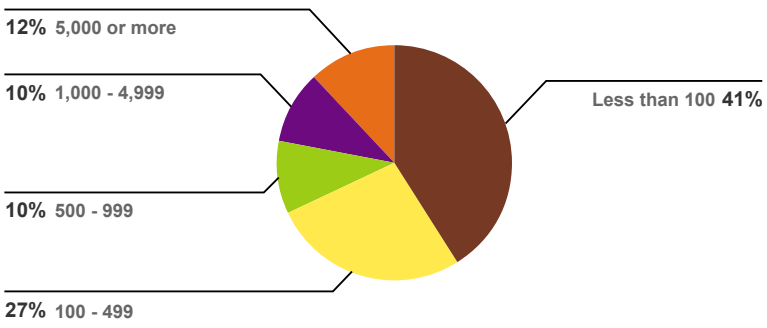
Respondent Demographics

VPNs can support a wide range of simultaneous users, from small VPNs supporting less than 100 users, to the largest implementations supporting more than 5,000 users. Most respondents either currently support or plan to support VPNs of less than 500 users. But a significant percentage of respondents in the survey have much more ambitious plans: 12% have or will have VPNs supporting more than 5,000 users.

Survey respondents are primarily from North America (81%), with Europe (9%), Asia (5%), and South and Central America (2%) also well represented. Other locations from which responses were received include New Zealand and Kenya.

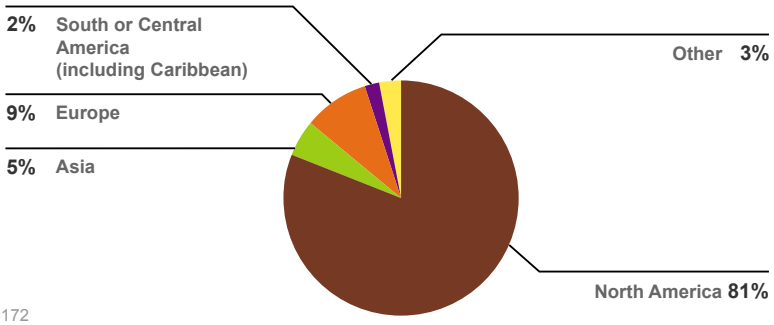
"Most respondents either currently support or plan to support VPNs of less than 500 users."

Number of Simultaneous Users Supported by Current or Planned VPN



N=146

Respondents' Location

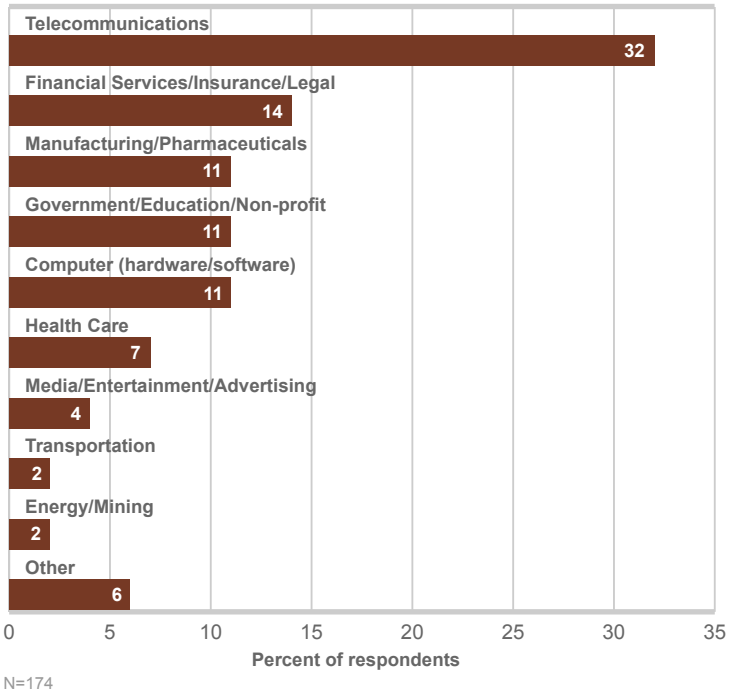


N=172

Survey respondents represent a cross-section of industries led by telecommunications, which represent nearly one-third of respondents. Other industries well represented include financial services/insurance/legal (14%), manufacturing/pharmaceuticals (11%),government/education/non-profit (11%), and computer hardware and software vendors (11%).

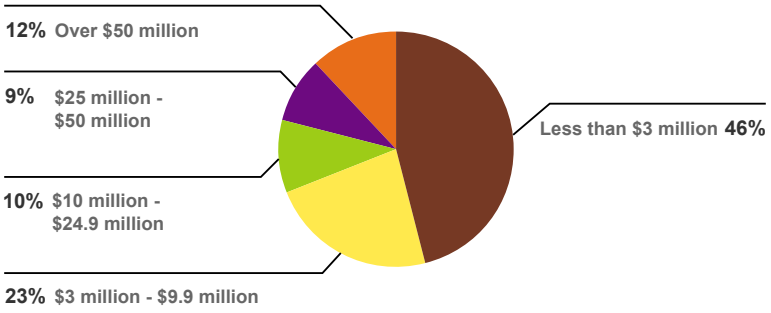
The size of the respondents' company's data networking budget ranges from less than $3 million to more than $50 million.

Respondents' Industry



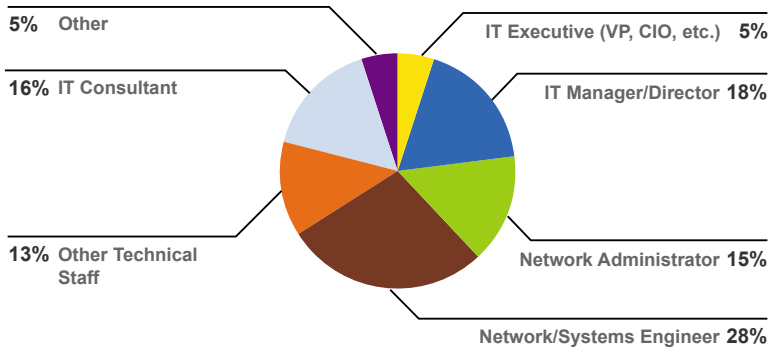
N=174

Respondents' Companies' Data Networking Budget



Respondent job functions are led by network/systems engineers (27%), followed by IT manager/directors (18%), IT consultants (16%), and network administrators (15%). Nearly one-quarter of respondents hold executive or management positions.

Respondents' Job Function



N=173

Comments

- *Client privacy and confidentiality are the absolutely most important criteria for us. We are a children's mental health provider and need to share confidential data between branch offices.*
- *Too many VPN products are not optimized for managing users. They're also crudely integrated with the Token and PKI systems, which themselves have extremely poor management applications.*
- *We are taking a first look at VPNs and have (identified) a few applications where the financial savings would be impressive.*

Methodology

This Virtual Private Networks survey was conducted over the World Wide Web in conjunction with a number of network-oriented organizations. Lucent NetCare would like to thank those organizations for their cooperation and support of this research project.

The survey was conducted from November 1–December 6, 1999, at:

http://www.ins.com/surveys

All Web survey responses were automatically collected into a survey tool. Any questions skipped or incorrectly answered by survey respondents were not included in the tabulations. Not-applicable responses were also not included in the tabulations. Each chart includes the number of valid responses for that particular question (e.g., N=100 indicates 100 responses). Percentages shown in charts may not equal 100% due to rounding.

About Lucent NetCare Network Industry Surveys

Lucent Technologies NetCare conducts monthly industry survey projects intended to provide IT managers with insight into key issues impacting the ability to develop and deploy network-centric business applications. Previous survey topics include:

- Network Operations Centers
- Enterprise Performance Management
- Enterprise Operating Systems and Directory Services
- Voice/Data Convergence
- New World Service Providers
- Management Intranets
- Service Level Management
- Network Professionals' Job Satisfaction
- Network and Systems Management Total Cost-of-Ownership
- Performance Management
- Virtual Private Networks
- Network Security
- Web/Java™-based Management
- Remote Access Services

To see the results of these surveys or participate in the latest Lucent NetCare network industry survey, see our website at:

http://www.ins.com/surveys

If you would like to learn how Lucent NetCare can help you implement or improve your VPN capabilities, please call us at 800-4-NETCARE, or email: netcareinfo@lucent.com.

For additional information, please contact your Lucent Technologies Sales Representative.

You can also visit our website at http://www.lucent-netcare.com/surveys or call 1-800-4-NETCARE (1-800-463-8227) or 1-727-217-2303

Lucent Technologies Inc.
Marketing Communications
6605 DLA 12/99
SR.GN.VPN.0100

1213 Innsbruck Drive
Sunnyvale, CA 94089