INS 1998 Survey Results:
Virtual Private Networks

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

Survey Introduction

As organizations become more geographically dispersed, virtual private networks (VPNs) have become increasingly attractive as a way to reduce communication expenses across the enterprise. The major business objectives in adopting this technology, according to our survey, are to reduce network costs, improve remote access control, and improve network capabilities. However, taking advantage of VPNs requires a combination of new technologies and specialized staff skills. In addition, organizations must choose between a growing array of VPN products and services aimed at helping them more effectively network their business operations.

CONTENTS

International Network Services (INS) recently conducted an industry survey to assess how organizations are addressing VPNs. This Web-based research project generated 69 survey responses, providing organizations with an opportunity to voice their opinions about VPN benefits and pitfalls.

Our intent in publishing the results of this survey is to help end-user organizations, vendors, and service providers determine the most effective approaches for implementing VPNs. The results can help companies compare their current and future VPN strategies and capabilities with those of other companies and provide valuable information about the benefits and pitfalls of implementing VPNs.

INTERNATIONAL NETWORK SERVICES

Survey Highlights

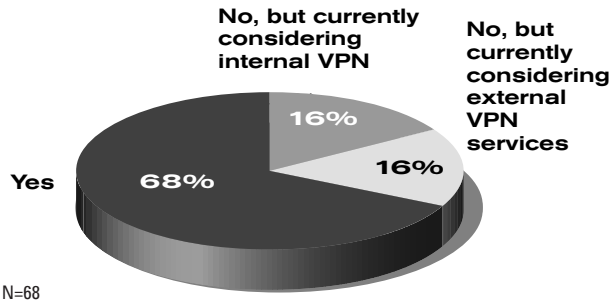
- Improving VPN capabilities is important to 89% of respondents.
- Inadequate product capabilities are the most frequent barrier to improving VPNs.
- Remote access for mobile workers is an important VPN concern for three-quarters of respondent organizations.
- Turnkey VPN solutions are a viable alternative for 50% of respondents.
- IP-based tunnels between sites that run over the public Internet infrastructure are the most often implemented VPN type as well as the most often planned for future implementation.
- Encryption, remote client software, and firewalls are the most important VPN elements. Respondents indicate that they are most likely to implement the following elements within six months:
  1. Firewall-to-firewall VPN capability
  2. Network perimeter firewalls with VPN capability
  3. Remote client VPN software

Profile of Current VPNs

Two-thirds of respondents have already implemented a VPN in their organization, an indication that our survey attracted network professionals in organizations with VPNs at a considerably higher rate than in the industry at large. Of the respondents without VPNs, half are considering an internal VPN and the other half are considering an external VPN service. The business objectives driving VPN deployment are fairly evenly distributed among reducing network costs, improving remote access control, and improving network capabilities. Greater management control is not an important factor in the growth of these networks.

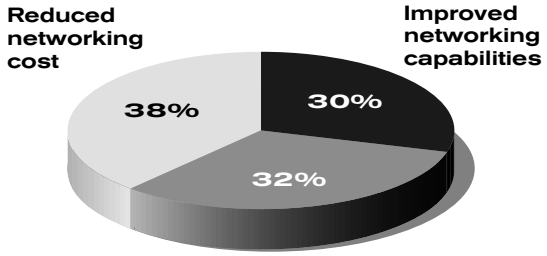
IP-based tunnels between sites that run over the public Internet infrastructure are the most frequently implemented type of VPN and also the most frequent type planned to be implemented (each by more than half of respondents). Service provider VPNs have not been implemented extensively to date, although more people plan to implement this type of VPN in the future. The vast majority of VPNs (78%) have encrypted IP protocols, although other types are also used with some regularity.

HAVE YOU IMPLEMENTED VPN CAPABILITIES IN YOUR ORGANIZATION, EITHER INTERNALLY OR USING AN EXTERNAL SERVICE PROVIDER?



N=68

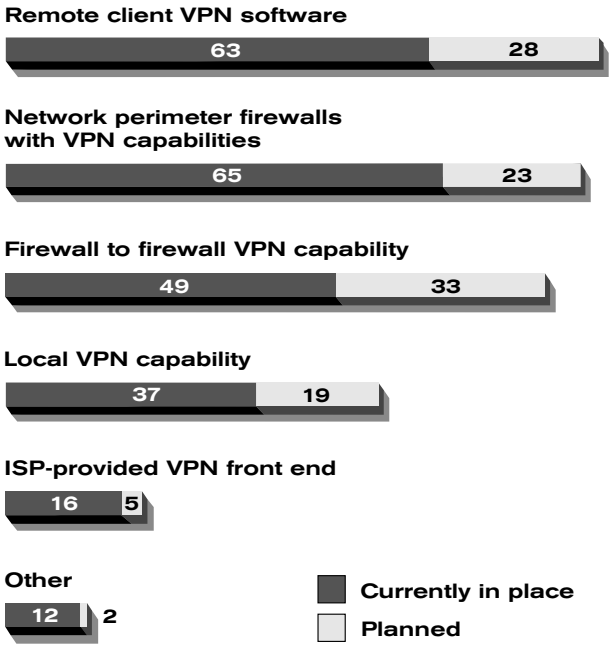
MOST IMPORTANT BUSINESS OBJECTIVE DRIVING DEPLOYMENT OF COMPANY VPN



N=68

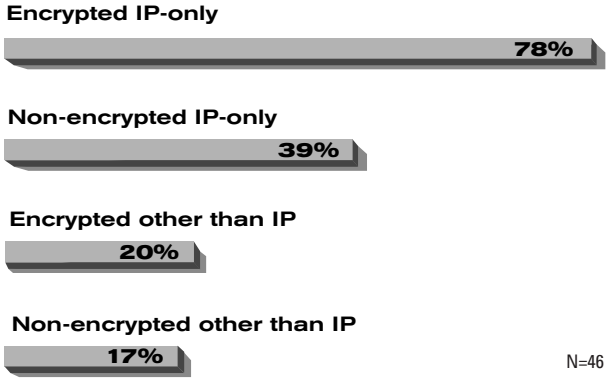
The majority of VPNs currently in place have network perimeter firewalls with VPN capability and/or remote client VPN software. Also frequently found in current VPNs is a firewall-to-firewall VPN capability. These are also the top three elements planned for implementation over the next six months.

VPN ELEMENTS



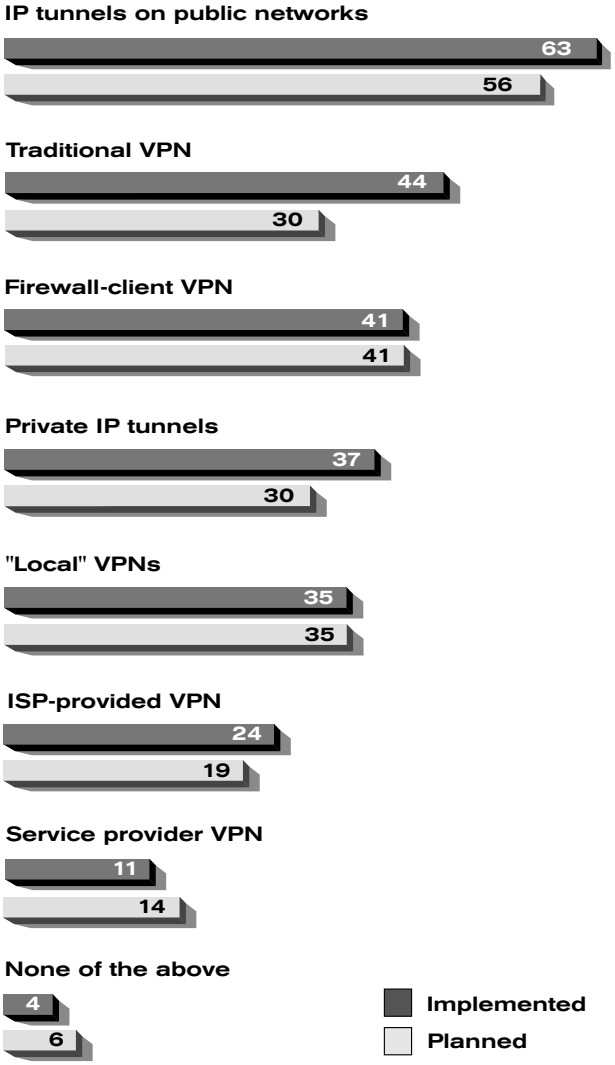
N=43

PROTOCOLS ON VPNS



N=46

VPN TYPES

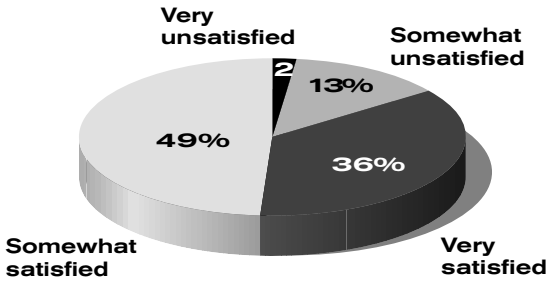


N=63

Satisfaction with VPN Capabilities, Platforms & Products

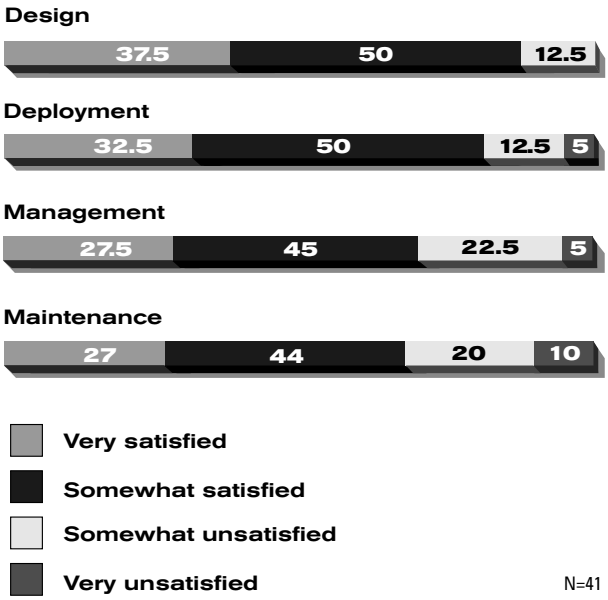
Overall, 85% of respondents are satisfied with the capabilities of their VPNs. At least 70% of respondents are satisfied with their enterprise operating system (EOS)-based VPN solution on four criteria (in order of highest satisfaction): design, deployment, management, and maintenance. Likewise, most respondents (74%) are satisfied with VPN products currently available.

OVERALL SATISFACTION WITH CURRENT VPN CAPABILITIES



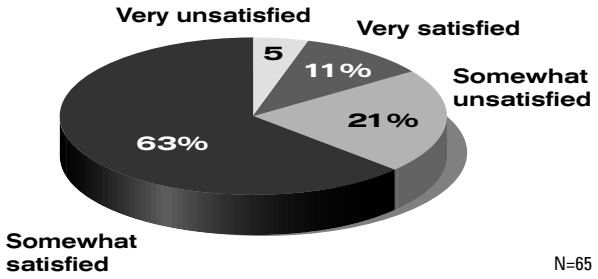
N=45

SATISFACTION WITH ENTERPRISE (EOS)-BASED VPN SOLUTIONS IN YOUR ENVIRONMENT



N=41

SATISFACTION WITH THE VPN PRODUCTS CURRENTLY AVAILABLE ON THE MARKET

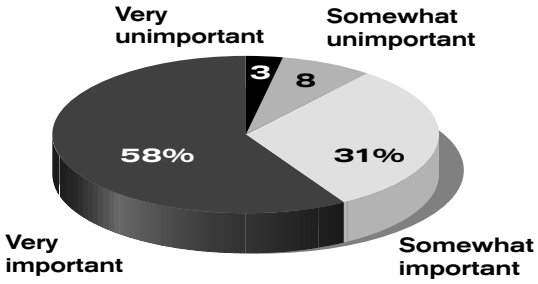


N=65

Importance of VPN Capabilities and Elements

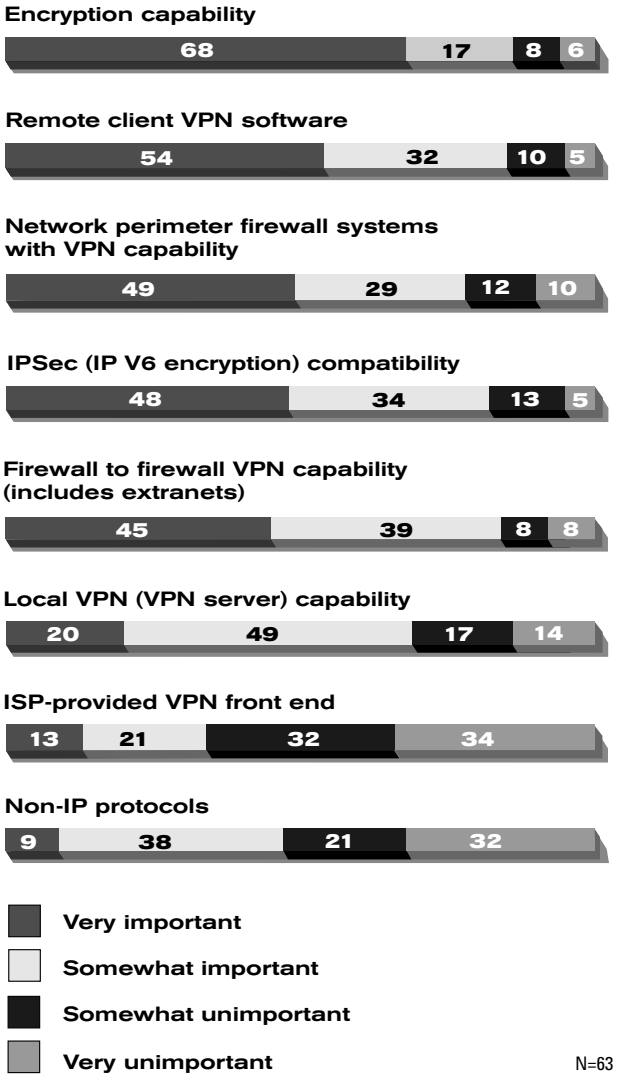
Despite the fact that most respondents with VPNs are satisfied with their current VPN capabilities, 89% of all respondents believe that it is important to improve VPN capabilities in their environment. The VPN elements most often rated somewhat or very important are encryption capability (86%), remote client VPN software (86%), firewall-to-firewall VPN capability, including intranets (84%), and IPSec (IP V6 encryption) (82%).

IMPORTANCE OF IMPROVING VPN CAPABILITIES IN YOUR ENVIRONMENT



N=65

NETWORK SECURITY ELEMENTS

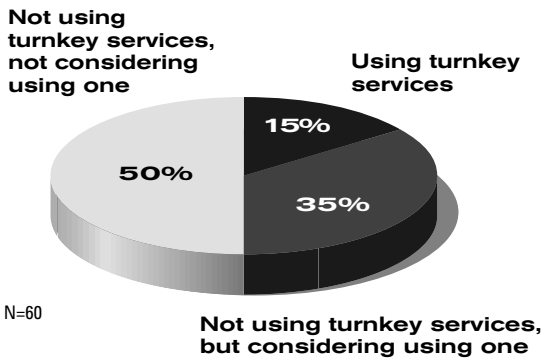


N=63

Turnkey VPN Services

Turnkey services, as defined for this survey, are packaged VPN services available on a subscription basis. Only 15% of respondent organizations are currently using a turnkey VPN service, and most of these respondents are satisfied with that service. Another 35% of respondents would consider using a turnkey VPN service at some time in the future. However, the remaining 50% of respondents neither use nor would consider using a turnkey service for implementing a VPN.

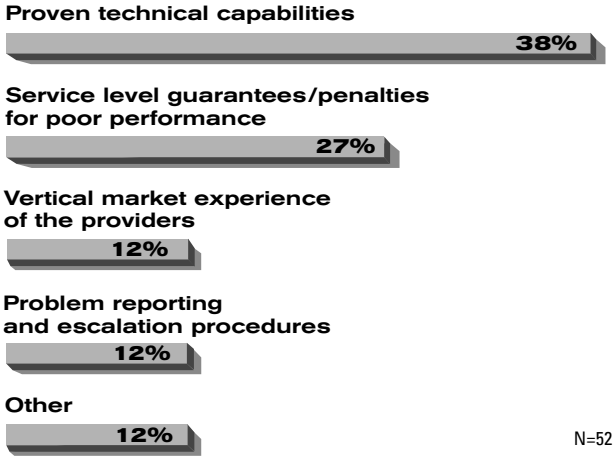
USE OF TURNKEY VPN SERVICES



N=60

Thirty-eight percent of respondents rank "proven technical capabilities" as their most important issue when considering turnkey VPN services. "Service level guarantees/penalties for poor performance" is ranked most important by 27%.

VPN ISSUES WHEN CONSIDERING A TURNKEY SERVICE



N=52

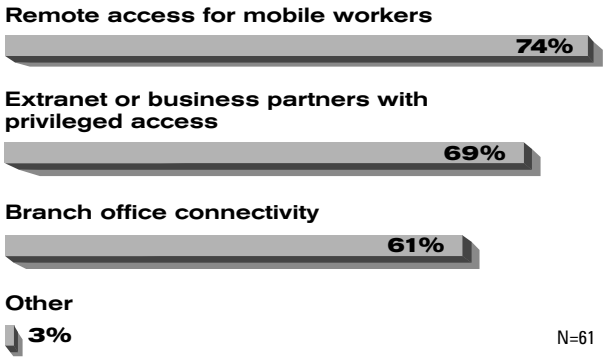
Concerns, Challenges & Barriers

At least two-thirds of respondents have concerns about remote access for mobile workers, the extranet (or business partners with privileged access) and/or branch office connectivity in regard to VPNs. The challenges to resolving VPN issues are more often technological (47%), but organizational (29%) and managerial (24%) challenges are also frequently mentioned.

Although three-quarters of respondents are satisfied with currently available VPN products, nearly half (47%) indicate that inadequate product capabilities versus requirements are among the greatest barriers to improving their VPN capabilities. Clearly, a gap remains between the capabilities of VPN products currently on the market and user requirements for VPNs. While this gap remains, respondents who need help implementing or enhancing their VPNs are looking for assistance in the following areas:

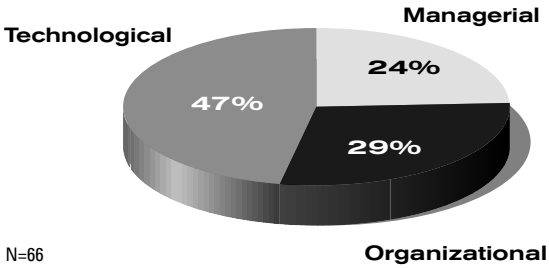
- ▲ Design and vendor selection (68%)
- ▲ Planning and technology recommendations (60%)
- ▲ Implementation (52%)
- ▲ Operations (44%)

GREATEST VPN CONCERNS



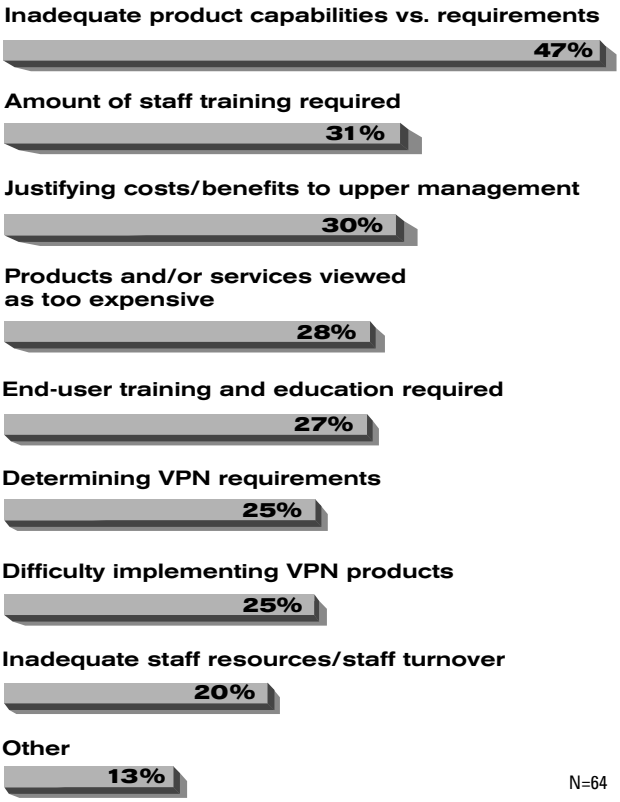
N=61

MOST IMPORTANT OVERALL CHALLENGE IN RESOLVING VPN ISSUES



N=66

GREATEST BARRIERS TO IMPROVING VPN CAPABILITIES



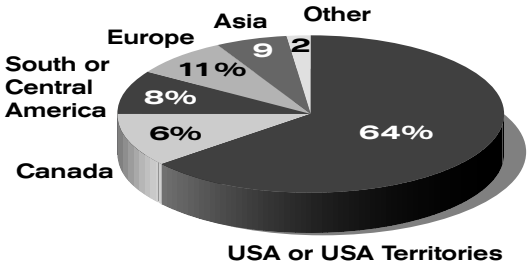
N=64

Demographics

Sixty-nine survey responses were received during the survey collection period from September 1 to October 5, 1998. Survey responses were primarily received from the United States (64%), with significant representation from Europe (11%), Asia (9%) and South/Central America (8%). Survey respondents represent a cross-section of end users, network service providers, product vendors, and consulting/integration organizations. Industry representation is widely distributed, with computers/software comprising the largest segment (30%). Respondent job functions are also well distributed, primarily among consultants (27%), network administrators (22%), and managers/directors (21%).

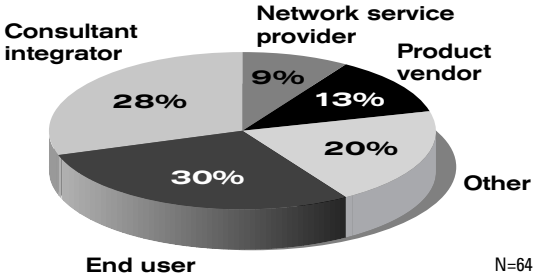
The estimated annual budget (capital, expenses, and staff) for data networking in respondent organizations ranged from less than $3 million to greater than $50 million. Of those respondents who could provide an estimate, approximately 40% have an annual data networking budget of greater than $10 million.

COUNTRY DISTRIBUTION



N=64

COMPANY TYPES

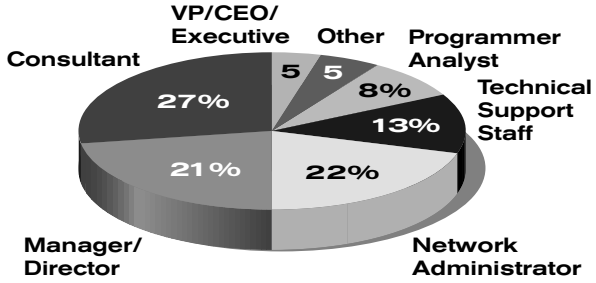


N=64

INDUSTRY DISTRIBUTION

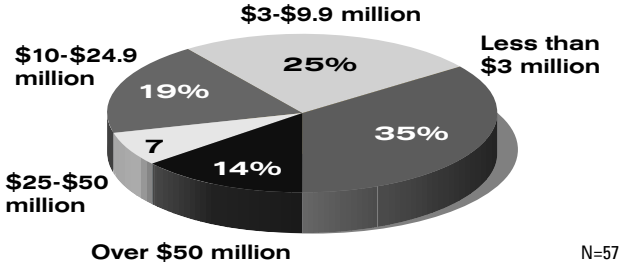
N=64

RESPONDENT TITLES



N=63

ESTIMATED ANNUAL BUDGET ($US) FOR DATA NETWORKING ORGANIZATION



N=57

Survey Comments

A number of survey respondents included comments in their responses. The following quotes are indicative of respondents' views:

- Nearly all remote-access style VPNs are missing client firewalling capabilities, which I view as being pretty critical.
- The VPN endpoints are the most commonly over looked and most critical pieces of a VPN. Regardless of the strength of the encryption between the endpoints, if I can break into an end point, the information is not safe.
- VPNs are very powerful tools, however some companies are deploying them on top of frame relay networks in order to "save money." This is simply rubbish. Intracompany communications with VPNs make sense to connect continents via VPN, but not within North America. The port charges that are being paid . . . are doubling companies infrastructure costs, not to mention the costs of the appliances that make this technology work.
- Personal VPNs are very important in making a spread-out organization connected. Being able to sit anywhere connected to the Internet and log in to your local network is a huge benefit. However, most managers would rather pay long-distance charges and have users dialing to a modem bank, when (instead) they could pay a fee to dialup a national/ international internet provider and really reduce the costs of having employees in remote locations.

Survey Conclusions

VPNs are becoming a significant technology for companies both to improve their networking capabilities and remote access security and to reduce networking costs. Satisfaction with currently implemented VPNs is high, indicating the continuation of their growth in the enterprise networking sphere. However, vendors should not be complacent. Nearly all respondents want to improve their VPN capabilities, and while most users appear satisfied with current VPN products, a large gap remains between current and desired product capabilities. Identification of these "gap" needs should guide future product development, particularly in the areas of encryption, remote client software, and network perimeter firewall systems.

A VPN solution need not be internally developed. Half of respondents are either using or willing to consider using a turnkey VPN solution, presenting a large opportunity for vendors with the expertise to package VPN products and technologies that will enable guaranteed performance for a broad range of VPN needs, including remote access for mobile workers, extranets, and branch office connectivity.

For companies that continue to develop VPNs internally, staff training and cost justification are significant barriers. Generally, respondents need help across the full lifecycle of VPN development, but more so in the initial planning and design stages. They are most often planning to build IP tunnels on public networks, firewall-client VPNs, and "local" VPNs. Building expertise in these areas should prove rewarding to product vendors and service providers alike.

Survey Methodology

The 1998 INS Virtual Private Network (VPN) Survey was conducted over the Internet in conjunction with a number of network-oriented organizations. INS would like to thank those organizations for their cooperation and support of this research project. The survey was conducted from September 1 to October 5, 1998 via the World Wide Web at:

http://www.ins.com/surveys

All survey responses were automatically collected into a survey tool that generated statistical results used as the basis for this report.

Any questions that were skipped or incorrectly answered by survey respondents were not included in the findings of this report. Not-applicable responses were also not included in the findings. Each graph includes the number of responses for that particular question (e.g., N=100 indicates 100 responses). Percentages shown in graphs may not equal 100% due to rounding.

About INS Network Surveys

International Network Services has conducted 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 Security
- Service Level Management
- Network Performance Management
- Remote Access
- Network Operations Centers
- Network Job Satisfaction
- Network and Systems Management
  Total Cost-of-Ownership
- Web/Java-based Management

To see the results of these surveys or participate in INS' latest monthly survey, please contact INS via the World Wide Web at:

http://www.ins.com/surveys

About INS

International Network Services (INS) is a global provider of solutions for complex enterprise networks. INS provides professional services for the full lifecycle of a network, including planning, design, implementation, operations and optimization, and maintains expertise in the most complex network technologies and multi-vendor environments. INS "Network Wizards" are recognized for their in-depth expertise and hands-on experience that enable them to quickly and effectively solve our clients' most challenging networking problems. Through its INSoft Division, INS also offers industry leading software solutions for managing and optimizing application-ready networks.

As of September 30, 1998, INS had 1,562 employees and provided service from 36 locations. INS' headquarters are located at 1213 Innsbruck Drive, Sunnyvale, CA 94089. The INS Web site is located at http://www.ins.com. INS is a public company, trading under the Nasdaq symbol INSS.

For further information regarding this survey, please contact:

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

or

Rick Blum
Research Programs Manager
(781) 221-2230, Ext. 477
Email: rick_blum@ins.com

INTERNATIONAL NETWORK SERVICES

*The knowledge behind the network.*SM

For more information call INS: 1-888-INS-8100
or visit our Web site at: www.ins.com