

## Implementing Secure Virtual Private Networks

Virtual Private Networks (VPNs) allow organizations to improve connectivity while reducing communications costs by providing remote access to enterprise network resources over the Internet. Remote workers, branch offices, subsidiary locations, and business partners can now “tunnel” calls over the Internet to reduce long distance charges and gain low-cost access to enterprise network resources. Security is critical to the successful deployment of VPNs. This whitepaper is intended to:

- > Define VPNs
- > Discuss the business value of VPNs
- > Demonstrate the business benefits of common VPN scenarios
- > Highlight the security implications of running business applications over the Internet
- > Present Security Dynamics solutions protecting business information traveling over the Internet

## TABLE OF CONTENTS

---

<b>INTRODUCTION</b>	<b>1</b>
<b>THE BUSINESS CASE FOR VPNs</b>	<b>3</b>
<b>VPN OVERVIEW</b>	<b>3</b>
<b>VPNs Reduce Costs and Simplify Scalability</b>	<b>4</b>
<b>VPNs Provide Competitive Advantages</b>	<b>5</b>
<b>Security Plays a Critical Role in VPN Adoption</b>	<b>6</b>
<b>VPN SCENARIOS</b>	<b>8</b>
<b>Remote User Access</b>	<b>8</b>
<b>LAN-to-LAN Connectivity</b>	<b>8</b>
<b>Extranets</b>	<b>8</b>
<b>TECHNOLOGY APPROACHES AND STANDARDS FOR SECURING VPNs</b>	<b>9</b>
<b>SECURITY DYNAMICS SECURVPN PROGRAM</b>	<b>11</b>
<b>Program Members</b>	<b>10</b>
<b>Partner Support Statements</b>	<b>11</b>
<b>ABOUT SECURITY DYNAMICS TECHNOLOGIES</b>	<b>14</b>
<b>GLOSSARY OF VPN TERMINOLOGY</b>	<b>14</b>

---

## THE BUSINESS CASE FOR VPNs

Information is a critical business asset and technology advances make it increasingly difficult to protect business applications. As users demand — and receive — more computing power and better access to critical business information, organizations realize increased productivity. Today, workers view “anywhere-to-anywhere” remote access as a birthright and expect online connectivity around-the-clock, seven-days-per-week.

### Remote Access Security and VPNs are Growing Rapidly

- Both Giga Information and International Data Corporation (IDC) project that use of strong authentication for remote access is growing at over 40% per year.
- Forrester Research predicts that most corporations will use VPNs to provide remote access services by 1999.
- Gartner Group predicts that by 2002, 90% of enterprises will use VPNs to provide switched services to remote workers and branch offices.
- IDC and Link Research predict that VPNs will continue to grow at a rate of 45% per year through 1999.
- In a recent LAN Times survey, 47% of respondents have plans to deploy VPNs to connect locations and/or mobile users.

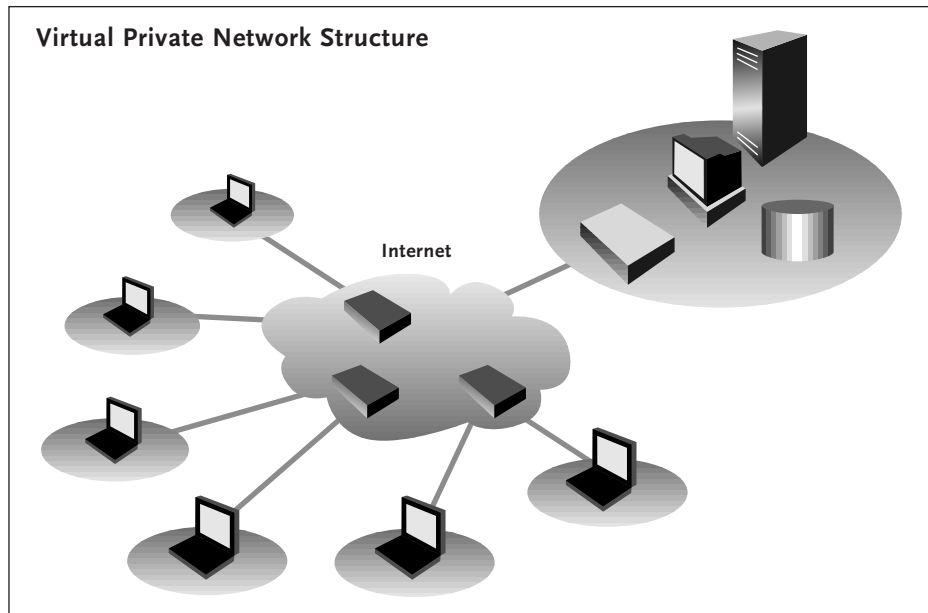
As organizations build remote access infrastructure, they realize the business value of eliminating costly, high-maintenance leased line connections between offices by tunneling high-speed connections over the Internet. Companies also realize the cost savings of connecting remote users and mobile professionals via the Internet to reduce long distance telephone charges. More business communications are now running over the Internet, creating potentially serious security risks if not managed properly.

In step with the trends toward easy-to-use, distributed applications and universal remote access, organizations must develop appropriate security measures to protect enterprise information. The stakes have never been higher for organizations trying to protect network access and information integrity.

In order to build remote access infrastructure to support traveling employees, telecommuters, contractors and after-hours workers, organizations are migrating applications from private networks to run over the Internet. The deployment of VPNs provides significant opportunities for organizations to improve network service and employee productivity while reducing long-distance line charges. However, to realize these business objectives, organizations must ensure the integrity of information traveling over public Internet connections.

## VPN OVERVIEW

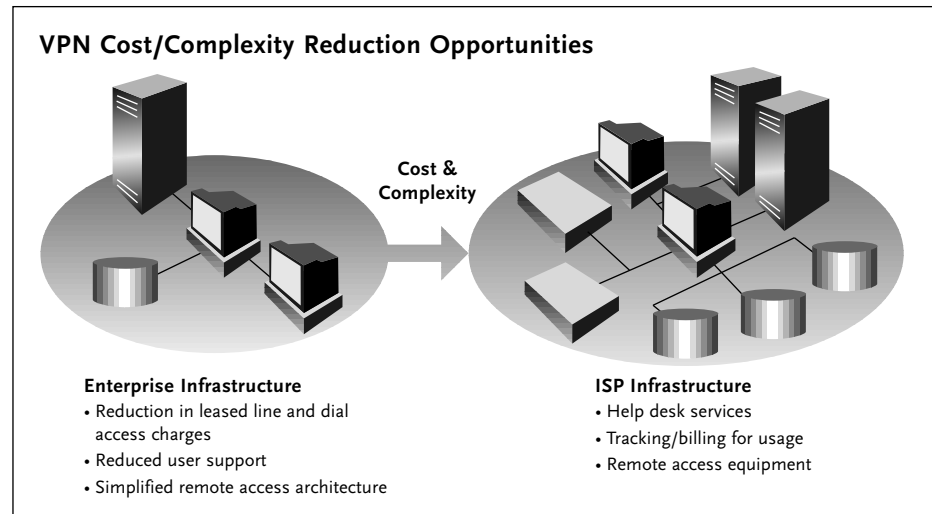
In their simplest forms, VPNs connect multiple remote users or remote offices to the enterprise network over the Internet. Whether in support of a traveling employee or a branch office, the approach is similar. The remote user places a call to the local Internet Service Provider (ISP) Point of Presence (POP). The call is then encrypted and tunneled through the Internet, and connected to the destination server on the customer premises. Branch offices can contract with an ISP for high-speed connections to the local POP, realizing the same benefits as expensive, dedicated connections — but without the long-distance charges.



The enterprise network pays only for the local calls and the ISP access fee. This allows them to take advantage of relatively low-cost Internet Protocol (IP) access services instead of distance-sensitive bandwidth charges. Considering that most ISPs offer flat-rate cost structures, phone access charges are dramatically reduced and can be budgeted for more reliably. Some technologies even provide support for roaming, which can allow a user to dial into an ISP anywhere to gain access to an encrypted VPN.

#### **VPNs Reduce Costs and Simplify Scalability**

Bandwidth charges are not the only cost savings afforded by VPNs. VPNs also reduce network complexity, resulting in lower network operations costs. Help desk calls, which traditionally focus on connecting the user to the network, are off-loaded to the ISP help desk and serviced as part of the monthly flat rate. This simplified architecture for connecting all users through one or more ISPs provides Information Technology (IT) executives a modular, virtually consistent architecture for all remote users, regardless of location or network need. Whether the remote connection is for a traveling sales representative connecting over a 56 Kbps modem or a branch office connecting at T1 speeds using a router, the architecture is similar and easily reproducible.



Cost-containment and accountability is also enhanced by VPNs, since the enterprise network can leverage ISP administrative systems to charge-back for usage. Capital costs are greatly reduced, since the enterprise network is paying the ISP for access and the ISP is responsible for establishing the infrastructure for Internet connectivity. Enterprises need only invest in the equipment to allow their remote users local access to the ISP. This approach also reduces the cost of technology obsolescence, since the infrastructure capital costs are shifted to the ISP and the enterprise is responsible for the lower cost of access technologies.

### VPNs Provide Competitive Advantages

Organizations can achieve competitive advantages by relying on VPNs, because they can evolve the network more rapidly and easily than those companies with major investments in private networks. As business requirements for network connectivity change, there are no major changes required of enterprise infrastructure. This approach provides greatly improved scalability over the private network approach, since access equipment can easily be added and additional ISP connections can be provisioned to quickly accommodate the shift of additional applications to run over the Internet.

Forrester Research expects that, by 1999, most organizations will use the Internet for the bulk of their remote access needs, while maintaining dial-up infrastructure for backups and in case of failures. Dial infrastructure will remain the primary means of supporting local users as well. As security technologies increasingly guarantee the integrity of business communications over the Internet, more companies will be conducting electronic commerce over secure Extranets.

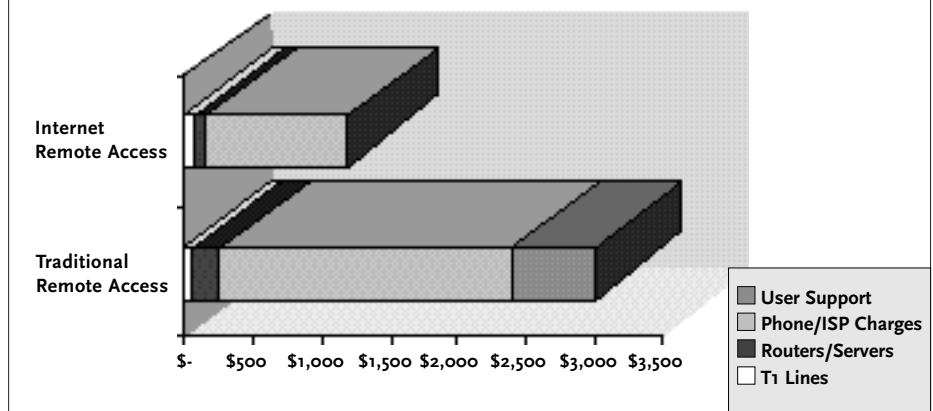
## Companies Realize Dramatic Cost Savings

The cost saving advantages of VPNs speak for themselves when compared to dial-up and private networks. Forrester Research estimates that VPNs offer the potential for a 60% overall reduction in remote access infrastructure costs.

In a 1997 analysis, they estimated the total costs associated with 2000-user remote access implementations. For a private remote access infrastructure, total annual costs were estimated at \$3.016 million. Telecommunications and User Support represented the largest percentage of costs at 72% (telecom) and 20% (user support) respectively. For an Internet-based remote access infrastructure, total annual costs were estimated at \$1.193 million. Telecommunications costs represented the largest percentage of costs at 90%. User Support costs, however, were eliminated by being completely offloaded to the ISP.

In this scenario, the VPN solution provides a “bottom line” savings of \$1.823 million per year.

Remote Access Cost Comparisons – Forrester Research 7/97 (\$000's)



It is important for IT executives to remember that a VPN is not completely *private*, since the Internet is something available to everyone. However, it is *virtual* in that organizations gain the benefits of a dedicated network connection which is available on-demand, and can therefore conduct business remotely using the Internet, rather than over costly private lines.

## Security Plays a Critical Role in VPN Adoption

While cost savings and simplified management are important VPN benefits, VPNs also represent opportunities for competitive advantage. However, companies can only gain competitive advantages from VPNs if they can guarantee the security of the information transmitted over the Internet. For many IT organizations, security remains a primary obstacle to implementing VPNs. With a private network, organizations know they control the flow of information and can establish and enforce security methods. However, secure remote access over VPNs can only be achieved for all business applications by combining several security technologies to authenticate users for network access and encrypt information traveling over the Internet.

## Encryption

Session encryption is essential to the deployment of VPNs, and vendors take different approaches to encryption depending on their product architectures and features. Application layer encryption, such as the Secure Multipurpose Internet Mail Extension (S/MIME), allows the creation of “Virtual Networks”, but it is the combination of

## Security Plays a Critical Role in VPN Adoption

- In a Forrester Research survey of Fortune 1000 companies, 32% cited “Security” as one of their biggest remote access challenges.
- In the same survey, 64% of respondents indicated no plans to use Internet-based remote access. Of these, 48% cited “Security Concerns” as the reason they will not use the Internet for remote access.

encryption and tunneling that ensures privacy and integrity of the information being transmitted over the VPN. This partially addresses the “P” in VPN. However, to implement a completely secure VPN, authentication of users in an essential VPN component.

### **Firewall-based VPNs**

The use of firewalls is a common method of implementing VPNs today. Widely deployed at the boundaries of the network infrastructure, these VPNs provide encryption on UNIX or Windows NT servers, or even within network devices, such as routers. Firewalls provide protection of network information, and are most effective when implemented both at central and remote sites.

### **Authentication**

Password protection alone is not sufficient to ensure secure remote access. Users are forced to remember too many passwords. As a result, users often select passwords which are easily guessed or store them in places where they can be observed. Additionally, passwords are expensive to administer. In a VPN environment, authentication technology ensures that the remote user accessing the corporate network via the Internet is in fact, the authorized user.

**Two-factor authentication** provides exponential improvements over password protection and is required for truly secure VPNs. With two-factor authentication, users need a token and a personal identification number to gain access to network resources. Users must enter both a personal identification number and a single-use identification number which is issued by a security token or smart card.

SecurID® technology from Security Dynamics solves the problem of unauthorized access to the network. SecurID®’s strong, two-factor user authentication provides ‘crackproof’ protection against unauthorized access and substantially greater security than traditional password systems. SecurID® dynamically authenticates users via a randomly generated one-time code that automatically changes every 60 seconds.

At login, users simply enter their personal identification number (PIN), followed by the code displayed on their SecurID® token or smart card. Authorized users are able to gain easy access to the VPN. The SecurID® solution combines two factors for strong user authentication:

- Something the user has — a token card
- Something the user knows — a personal identification number

In a recent report, Mark Lobel, Manager of Information Technology Security Services for Coopers and Lybrand emphasized the corporate need for strong user authentication. “While there is a need for access control and authentication in our society, we have a special corporate need for strong user authentication,” he wrote. “Today, companies have many reasons for protecting assets, from legal requirements to guarding shareholder assets and value. Authentication cannot exist in a vacuum, it must be part of a security framework.”

## **VPN SCENARIOS**

There are several primary scenarios for using VPNs, each bringing IT executives the benefits of reduced bandwidth charges, lower network operations costs, simplified administration, reduced capital expenditures, and increased scalability and flexibility. The key challenge for the IT executive is to implement the optimal security solution for each application.

### **Remote User Access**

This approach allows remote users to tunnel calls over the Internet. The calls are aggregated onto a remote access server and provided with access to enterprise local area network (LAN) resources. Users can connect over analog modems or using Basic Rate ISDN (BRI) terminal adapters. They can be based in a fixed location — such as telecommuters or contractors — or they can be mobile — such as traveling executives or sales representatives. The security challenge in this application is to authenticate users to determine that they are indeed who they claim to be. Since many of the users are mobile, “call-back” techniques are not applicable, and the enterprise network must be protected from hackers and unauthorized users.

### **LAN-to-LAN Connectivity**

This application reduces the requirement for expensive, leased line solutions. Remote offices consolidate LAN traffic onto a high-speed Internet connection, usually via a multiprotocol router, which provides connectivity to other branch offices and to the enterprise network. The security challenge is to implement both two-factor authentication and session encryption. This approach allows each LAN to be validated for network access, while also allowing the virtual connection to be safely encrypted to protect from eavesdropping.

### **Extranets**

Communications between companies are being enhanced through the introduction of extranets, which provide LAN-to-LAN connectivity between a company and its business partners, customers, and even suppliers. Extranet applications allow organizations to improve productivity and achieve competitive advantages by streamlining supply chain management, improving customer service, and providing higher quality communications to the distribution channel. Production, order processing, sales and customer support applications are among the most commonly deployed extranet applications.

Extranets can create daunting security challenges, since diverse network technologies and architectures are integrated into a single logical network. Therefore, extranets require varying security levels, and IT executives need the flexibility to dynamically assign multiple security levels. For example, a company may offer product information to all of its partners, but restrict

pricing and availability data to resellers. These benefits can best be realized by implementing two-factor authentication, session encryption and flexible management tools to administer the complex security required to conduct business with third parties over the Internet.

### TECHNOLOGY APPROACHES AND STANDARDS FOR SECURING VPNS

There are a variety of technologies and emerging standards associated with implementing security over VPNs. One of the most promising is the IP Security (IPSEC) specification being developed by the Internet Engineering Task Force (IETF). IPSEC provides network layer encryption and authentication at the IP level. It will become a part of IP Version 6 after it is finalized. The X.509 standard defining Digital Certificates is an important specification. Digital Certificates identify users to ensure the successful transfer of encrypted communications.

Most IT executives are already incorporating security technologies in existing networking solutions, so the challenge becomes how to optimize VPNs via the optimum combination of security technologies. Remote routers have the advantage of automatically authenticating themselves to the target routers upon connection, but it becomes difficult to authenticate users within each site. A new breed of specialized VPN devices are being introduced to provide the routing functionality required while also supporting both hardware-based encryption and firewall technology.

Software solutions are also available. The most common security technology for VPNs today is the implementation of firewalls to protect the enterprise network from direct Internet access and intrusion. Firewalls are deployed at the edge of the network, usually as software implementations on Windows NT or UNIX servers. Security protocol stacks implemented in software applications provide an alternative security technology. This approach has been particularly effective with remote users and servers. For example, the Point-to-Point Tunneling Protocol (PPTP) can be installed on any Windows client and any Windows NT Server to provide secure tunneling, and the L2TP specification can be used to provide secure connectivity between host and remote routers.

It is important to identify the key protocols that exist or are being put forward by vendors to address VPN security.

**PPP** — An implementation of TCP/IP that provides router-to-router and host-to-network connections.

**L2F** — Permits tunneling of the link layer of higher level protocols across the Internet. The L2F specification was developed by Cisco Systems.

**L2TP** — Combines the features of the L2F and PPTP protocols and permits tunneling of the link layer of PPP so privately addressed IP, IPX and AppleTalk packets can be carried across the Internet. It refers data security to the IPSEC Protocol, and has been put forward by Cisco Systems and Microsoft.

**IPSEC** — Internet Protocol Security. IPSEC provides network layer encryption and authentication of IP traffic. It will likely be finalized and approved as part of future releases of IP. There are differing proposals for managing the distribution of encryption keys. The Internet Security Access Key Management Protocol (ISAKEMP/Oakley) is proposed by Cisco Systems, and the Simple Key Management for Internet Protocols (SKIP) specification is proposed by Sun Microsystems for automated key management.

Secure VPNs deliver tremendous business value, but only if they provide the appropriate level of security to guarantee the privacy and integrity of corporate information for authorized users. Each VPN should provide the confidentiality required to prevent unauthorized viewing or eavesdropping on network traffic, two-factor authentication to verify each user for network access, and network integrity to prevent tampering with data as it passes through the Internet.

This requires a diverse and robust set of security tools. Through its SecurVPN Program, announced in August of 1997, Security Dynamics has worked with leading suppliers of VPN solutions to offer all the components needed for a complete, and fully secure VPN solution. Customers can rest assured that SecurID® and ACE/Server® will work with all major VPN solutions available in the marketplace today.

### SecurVPN™ Program Members

For more information on any of the SecurVPN partners listed below or our joint solutions, please visit our web site at <http://www.securitydynamics.com/solutions/SecurVPN>

Company	VPN Product Name
Ascend Communications	Secure Access and Pipeline 220
Aventail	Mobile VPN 2.0 and AutoSocks 2.1
Bay Networks	Baystream Dial VPN Products
Check Point Software Technologies Ltd.	FireWall-1 server and FireWall-1 SecuRemote client
Digital Equipment	AltaVista Tunnel 98 for Digital UNIX
Fortress Technologies	NetFortress VPN-1
IBM	IBM Firewall for AIX 3.2
InfoExpress	VTCP/Secure
New Oak	NOC 4000
Raptor Systems	EagleMobile VPN
TimeStep	Permit SVPN
Trusted Information Systems	Global Gauntlet VPN
V-ONE	SmartGate
VPNnet	VSU-1010

Livingston Enterprises, RedCreek Communications, Inc., Semaphore, Shiva and Sun Microsystems are all members of the SecurVPN program and have announced their intention to provide SecurID support when their respective VPN solutions are available. For more information on these partners and their VPN solutions please visit our web site at <http://www.securitydynamics.com/solutions/SecurVPN>

## SECURITY DYNAMICS SECURVPN™ PROGRAM

Security Dynamics, a leader in enterprise security solutions and RSA cryptographic technologies, introduced the SecurVPN Program in September of 1997. Program members have embedded, or plan to embed, Security Dynamics' ACE/Agent code in their VPN solutions, making it possible for companies to strongly authenticate users onto the VPN using SecurID authentication technology. Unlike other VPN solutions available on the market today, the solutions available through Security Dynamics' Program integrate session encryption technology with strong user authentication to create secure remote access solutions that protect against attacks by hackers or eavesdroppers.

### Partner Support Statements

#### AltaVista

"The integration of the ACE/Agent technology into the AltaVista Tunnel coupled with the security offered by the strong RSA encryption makes AltaVista's solution the most secure method for performing remote access over the Internet. We look forward to continuing our work with Security Dynamics/RSA to uncover new and innovative ways to keep communication over the Internet secure" — *Raymond Suarez, marketing manager, Internet Security at AltaVista*

#### Ascend Communications

"The growth projections for the VPN market are strong for good reason. VPNs are an excellent way for corporations to maximize the cost benefits of the Internet. The combination of powerful encryption and authentication technologies in this solution provides a way for corporations to take advantage of the ubiquity of the Internet, while maintaining the utmost confidence in the security of their data. This bundled solution gives corporations the ability to verify the identity of remote users, secure information as it travels across the Internet, and ensure the identity of the intended recipient at the other end of the connection." — *Dave Dawson, General Manager, Ascend's Network Security Business Unit*

#### Aventail

"The combination of Aventail VPN and SecurID enables corporations to create a highly secure VPN that is ideal in building an extranet between 'un-trusted' networks. There is no other solution on the market that can ensure this level of privacy while effectively addressing ease of management and interoperability issues. Our products make secure extranets a reality today and into the future." — *Evan Kaplan, president and CEO of Aventail Corporation*

#### Bay Networks

"Realizing that VPN applications require a premium security solution, we designed BaySecure Access Control to be the primary component of a Bay Networks VPN that is 'SecurID-Ready.'" — *David Giglio, senior product manager for Remote Access Security at Bay Networks*

"Security Dynamics is showing real leadership in the fast growing VPN market by offering formal initiatives such as the SecurVPN program. Security is obviously the primary requirement in any VPN service offering. By integrating the SecurID APIs and agent code into our BaySecure Access Control Products, Bay Networks' VPN solution set is that much more robust security-wise." — *Jonathan Zarkower, senior product manager at Bay Networks responsible for Bay's cross-divisional IPVPN strategy*

<b>Check Point Software</b>	<p>“VPNs offer companies an enormous opportunity to provide their users with secure communication using the Internet, rather than expensive T-1 or leased lines, to reach company networks. ViPN offers the premier one-stop solution for remote access, providing a single package that enables simple and secure communication between sender and recipient.” — <i>Dr. Deborah Triant, president and CEO of Check Point Software Technologies, Inc</i></p>
<b>Fortress Technologies</b>	<p>“Simple passwords alone don’t provide effective security for remote access authentication. We immediately turned to Security Dynamics because most of our customers were already using SecurID cards. By joining Security Dynamics’ SecurVPN Program, we will be able to pair our NetFortress VPN-1 product with SecurID to meet our customers’ demands for a fast, simple and secure remote access solution.” — <i>Gary E. Brooks, vice president, marketing for Fortress Technologies</i></p>
<b>IBM</b>	<p>“A growing number of our customers are interested in using VPNs as a cost-effective, secure means of conducting business over the Internet. As an early supporter of Security Dynamics’ SecurID authentication products, and VPN solutions using IPSEC standards, the IBM Firewall, part of the IBM SecureWay &amp;trade; offerings, is well-positioned to meet the need.” — <i>Vijay Ahuja, product manager for the IBM firewall</i></p>
<b>InfoExpress</b>	<p>“Organizations can instantly add strong encryption and authentication to their fire software with SecurID, remote users can safely use the Internet to run their enterprise applications from anywhere in the world.” — <i>Stacey Lum, president of InfoExpress</i></p>
<b>Livingston Enterprises</b>	<p>“Livingston Enterprises has long recognized the important of strong authentication, particularly in protecting the endpoints of VPN sessions. Security Dynamics’ SecurID integrated with Livingston’s RADIUS authentication server offers superior security solution to static passwords, for protecting VPN sessions.” — <i>Alex Henthorn, senior technical product manager at Livingston Enterprises</i></p>
<b>New Oak</b>	<p>“Strong authentication is a key component to Extranet access. In addition to tunneling, encryption, filtering, authorization and accounting, two-factor authentication, like that offered by SecurID, is critical in building a scalable, secure and manageable Extranet access solution. New Oak is very pleased to be a member of the SecurVPN Program. We are committed to working with Security Dynamics to produce secure Extranet access solutions for customers.” — <i>Michael Feinstein, vice president of product marketing at New Oak Communications</i></p>
<b>Raptor Systems</b>	<p>“Security Dynamics’ technology has provided Raptor’s EagleMobile VPN client software with the strong user authentication needed to support dynamic IP address assignment by local ISPs. By joining Security Dynamics’ SecurVPN program, Raptor will be able to enhance EagleMobile’s support for Security Dynamics’ SecurID tokens and ACE/Server as well as smart cards in the near future. Raptor expects the SecurVPN program will provide additional features for what will become a family of EagleMobile products.” — <i>Lance Urbas, senior vice president of engineering and technical services at Raptor Systems, Inc.</i></p>
<b>Red Creek Communications</b>	<p>“RedCreek is pleased to be a member of the Security Dynamics SecurVPN program. The integration of the Security Dynamics’ SecurID with RedCreek’s Ravlin product family of fast IPsec encryption products offers customers strong user authentication for protecting the endpoints of secure VPN sessions.” — <i>Bill Wiedemann, founder and executive vice president of RedCreek</i></p>

## IMPLEMENTING SECURE VIRTUAL PRIVATE NETWORKS

- Semaphore** “Semaphore recognizes the need for strong authentication in our VPN solution. We believe that the two-factor authentication provided by SecurID technology to be strategic to our success in the VPN marketplace.” — *Mark T. Vondenkamp, vice president and chief technical officer at Semaphore*
- Shiva Corporation** “Security remains a primary concern for customers when it comes to implementing virtual private networks. The combination of Security Dynamics’ SecurID technology and the powerful security features of Shiva’s VantagePath VPN technology will give our customers an unparalleled array of security options. This will enable our customers to reap the performance and cost benefits of VPNs without the security risks associated with putting sensitive corporate information onto the ultimate public network, the Internet.”  
— *Angelo Santinelli, senior vice president, worldwide marketing and business development at Shiva Corporation*
- Sun Microsystems** “Especially with the larger Virtual Private Networks, where end user authentication is increasingly important, adding SecurID support to our SunScreen VPN server products is being well received. With our installed base of Virtual Private Networks evolving from network-to-network to user-to-user communications, this type of authentication is important.”  
— *Chris Tolles, director of marketing at Sun’s Internet Commerce and Security Group*
- TimeStep** “The need for strong user authentication has never been more critical when providing access to the corporate network over the Internet. Because Security Dynamics can provide that level of authentication, TimeStep’s PERMIT VPN solution will support the ACE/Agent technology. As market leaders, the combination of the PERMIT and SecurID technologies will offer corporations a very powerful and comprehensive enterprise security solution.” — *Tim Hember, president and CEO of TimeStep*
- Trusted Information Systems** “The powerful encryption of TIS’ Gauntlet VPNs combined with SecurID authentication technology offer unbeatable protection to users relying on the Internet to access private networks. Information managers who are looking for proven ways to save money while enabling secure e-business can look to TIS for dependable global-VPN solutions.”  
— *Harvey L. Weiss, president of TIS’ commercial division*
- V-ONE** “V-ONE’s cornerstone philosophy has always been that networks and systems must be open and non-proprietary. Compatibility between SecurID and our VPN product SmartGate gives greater flexibility and strong security to our customers.” — *James F. Chen, president and CEO of V-ONE Corporation*
- VPNnet** “VPNnet was the first company to introduce a SecurID-Ready VPN solution, and we’re even more excited about the SecurVPN Program. Our recently announced VSU-1010 can eliminate long-distance remote access charges, support hundreds of simultaneous users, and deliver Triple-DES encryption, packet-level authentication, key management, and compression services at a full 10 Mbps. By integrating our solution with Security Dynamics’ SecurID and ACE/Server authentication technologies, we can offer customers the security and convenience of strong, two-factor user authentication, which is critical in many VPN applications. The result is a winning combination that delivers a new generation of business remote access.” — *Richard S. Kagan, vice president of marketing at VPNnet*

## ABOUT SECURITY DYNAMICS TECHNOLOGIES

Security Dynamics is a leading provider of security solutions for remote access to enterprise networks. Security Dynamics solutions help companies conduct business securely, protect corporate information assets and facilitate business-to-business electronic commerce. Security Dynamics' products employ patent-protected SecurID® token technology and ACE/Server® Communications or hardware access control products to authenticate the identity of users accessing networked or standalone computing resources. With 2 million users in 2,000 companies, Security Dynamics is the world leader in two-factor user identification and authentication. RSA Data Security Inc., a wholly owned subsidiary of Security Dynamics, is the world's brand name for cryptography, with more than 80 million copies of RSA encryption and authentication technologies installed and in use worldwide. Security Dynamics and RSA can be found on the World Wide Web at <http://www.securitydynamics.com/> and <http://www.rsa.com/>, respectively.

## GLOSSARY OF VPN TERMINOLOGY

<b>BRI</b>	Basic Rate interface to ISDN allows remote user computers to access the Internet at speeds up to 128 Kbps.
<b>Digital Certificate</b>	An electronic certificate that identifies users to ensure the successful and authorized transfer of information.
<b>Encryption</b>	The transformation of data into a form unreadable by anyone without a decryption key. Encryption is a critical technology for securing information as it passes through the Internet.
<b>IP</b>	Internet Protocol (IP) is the standard protocol for sending information over the Internet. IP is also known as TCP/IP.
<b>IPSEC</b>	IPSEC provides network layer encryption and authentication of IP traffic. It will likely be finalized and approved as part of future releases of IP.
<b>ISDN</b>	Integrated Service Digital Network.
<b>ISP</b>	Internet Service Providers (ISPs) deliver access to Internet resources for both remote users and enterprise servers.
<b>L2F</b>	Permits tunneling of the link layer of higher level protocols across the Internet. It was developed by Cisco Systems.
<b>L2TP</b>	Combines the features of the L2F and PPTP protocols and permits tunneling of the link layer of PPP so privately addressed IP, IPX and AppleTalk packets can be carried across the Internet. L2TP has been put forward by Cisco Systems and Microsoft, and it refers data security to the IPSEC Protocol.

<b>Passwords</b>	The most basic security measure, which lacks the reliability of two-factor authentication. Passwords are easily guessed or hacked, providing limited security for remote access.
<b>POP</b>	The Point of Presence (POP) is located on the ISP's premises, and it provides access and egress for Internet traffic.
<b>PPP</b>	The Point to Point Protocol (PPP) is an implementation of TCP/IP that provides router-to-router and host-to-network connections.
<b>PPTP</b>	The Point-to-Point Tunneling Protocol (PPTP) is a Microsoft standard for encapsulating data for secure transmission over the Internet.
<b>PRI</b>	Primary Rate Interface to ISDN consists of 23 64 Kbps B channels in North America, and 30 channels in most of the rest of the world. It is the ISDN equivalent of a T1 or E1 circuit.
<b>RADIUS</b>	Remote Authentication Dial In User Service (RADIUS) is an Internet-standard protocol for managing the authentication and configuration of users dialing into networks. The IETF is working to strengthen the RADIUS standard with new support for the PPTP, L2F and IPSEC tunneling protocols, a move that would make it easier to establish virtual private networks (VPN) by ensuring that remote access and security could be managed from a single point with compatible hardware. Several vendors have already embraced RADIUS and are moving on their own into tunneling and proxy support. RADIUS tunneling will require new Tunnel Type, Tunnel Medium Type, Tunnel Client Endpoint, Tunnel Server Endpoint and Tunnel Connection ID standards attributes.
<b>Smart Card</b>	A plastic card similar in size and shape to a credit card which holds information in a small chip embedded into the card.
<b>Socks Version 5</b>	Socks is available as an open standard in an Internet RFC. Socks runs at the TCP layer of the stack and, unlike Winsock, is independent of the application. Socks proxies are different from application- or HTTP-layer proxies, because they simply pass packets through without knowing about the application. Version 5 features additional security, including Kerberos support.
<b>Token</b>	A credit card or calculator sized computer or software program that has the ability to authenticate users using a secret SEED number which gives the token a uniqueness allowing it to be differentiated from other tokens.
<b>Two-Factor Authentication</b>	The most effective means of identifying users and authorizing them to access the network. Users must enter both a personal identification number and the number assigned via a secure token.
<b>Tunneling</b>	Tunnels create a secure, logical connection between two end-points over the Internet.

*SecurVPN, Security Dynamics and the Security Dynamics logo are trademarks of Security Dynamics Technologies, Inc. All other trademarks are the property of their respective owners.*

©1997 Security Dynamics Technologies, Inc. All rights reserved.

C Printed on recycled paper.

SWP01

# SecurityDynamics