Implementing a Secure Virtual Private Network

WHITE PAPER

Virtual Private Networks (VPNs) are quickly becoming the most universal method for remote access. They enable you to take advantage of the power of the Internet by providing a private tunnel through the public cloud to realize cost savings and productivity enhancements from your remote access applications. But being private doesn't necessarily mean a VPN is secure. That's because a VPN is still often protected by nothing more than a weak password. This paper is designed to help you understand the nuts and bolts of VPNs as well as the choices that are available to enhance the security of a VPN.

RSA SECURITY® | Confidence Inspired™

TABLE OF CONTENTS

I. VPNS: THE OPPORTUNITY & THE RISK

Remote access is increasingly becoming standard business practice. It enables you to improve productivity and stay competitive in a fiercely competitive business environment that has already gone "electronic." Remote access is a business "must" that maximizes communication and interaction. It empowers mobile employees and remote users with access to critical information—any time, anywhere. It also enables organizations to extend their reach beyond employees to work effectively with contractors and consultants as well as customers, partners, and suppliers.

Remote access has traditionally been accomplished via leased line dial-up methods. Although effective, this method is typically plagued by slow transmission speeds and expensive network costs making it hard for you to provide the service levels your users need to do business effectively. But remote access has come a long way with the introduction and adoption of Virtual Private Network (VPN) technology. VPNs enable you to leverage the power of the Internet for remote access. That is, remote users dial into a local POP and connect to the corporate network through the Internet. The result is dramatic: significant cost reductions, increased productivity, improved service and anywhere, anytime access.

With all its power come risks too. After all, that VPN is tunneling right through the public network and opening your "network doors" to a wide range of users—users that you can't necessarily see or touch. These users are accessing valuable corporate data assets and conducting mission critical transactions. If the right people are accessing the right information, you couldn't find a more powerful business tool. But VPN remote access in the wrong hands could be devastating to your e-business.

II. VPN BASICS

An Overview of a VPN Implementation

In its simplest form, a VPN connects 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 your premises. The most important thing to note here is that you 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.

VPN SCENARIOS

There are several primary scenarios for using VPNs, each bringing you the benefits of reduced bandwidth charges, lower network operations costs, simplified administration, reduced capital expenditures, and increased scalability and flexibility. The key challenge for you 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 your 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.

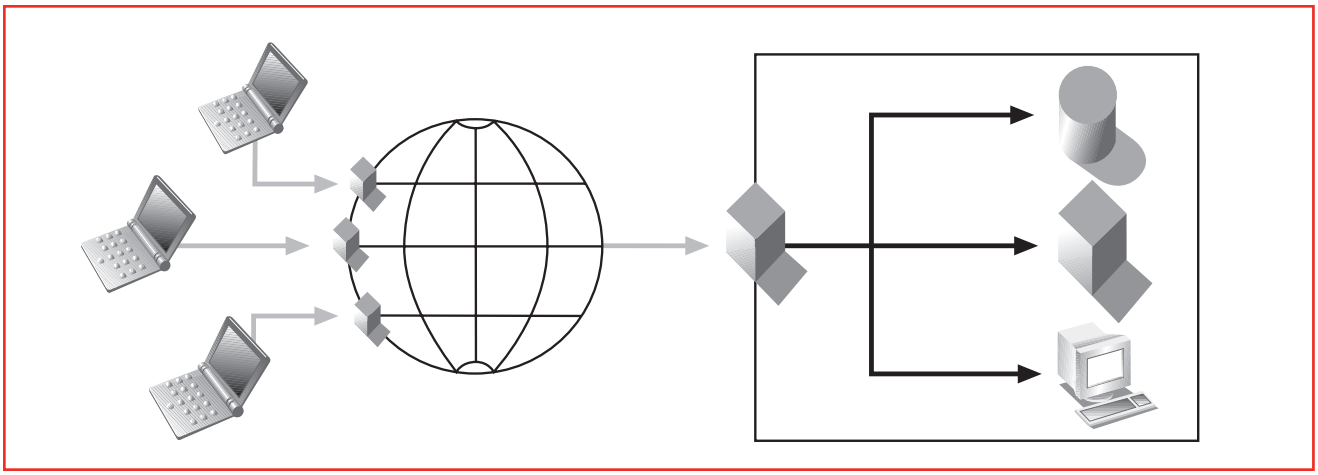
LAN-to-LAN Connectivity

This application reduces the requirement for expensive, leased line solutions. Remote offices consolidate LAN traffic onto a high-speed Internet connection, usually via a multi-protocol 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 you and your 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 require varying security levels, and you need the flexibility to dynamically assign multiple security levels.

VIRTUAL PRIVATE NETWORK INFRASTRUCTURE



You pay only for the local calls and the ISP access fee. This allows you 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.

III. THE BUSINESS CASE FOR VPNS

VPNs Reduce Costs and Simplify Scalability

Bandwidth charges are not the only cost savings afforded by VPNs. Equally important, 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 you with 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 the VPN infrastructure, since you can leverage ISP administrative systems to charge-back for usage. Capital costs are greatly reduced, because you only pay the ISP for access. The ISP is responsible for establishing the infrastructure for Internet connectivity. That means, you need only invest in the equipment to allow your 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 you are responsible only for the cost of access technologies.

VPNs Provide Competitive Advantages

A VPN is virtual in that you gain the benefits of a dedicated network connection which is available on-demand. You can therefore conduct business remotely using the Internet, rather than over costly private lines—empowering your employees in a highly competitive business environment. You can also achieve competitive advantages by relying on VPNs because they can evolve the network more rapidly and easily than any competitors with major investments in private networks. As business requirements for network connectivity change, there are no major changes required of your 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.

IV. SECURITY PLAYS A CRITICAL ROLE IN VPN ADOPTION

The Security Risk

While cost savings and simplified management are important VPN benefits, you can only gain competitive advantages from VPNs if you can guarantee the security of the information transmitted over the Internet.

Today, online business activity is not limited to inconsequential communication and harmless access to relatively public documents. You're doing everything online. You're accessing customer records, sales proposals, and corporate contracts. You're transmitting product specifications, purchase orders and legal documents. You're even closing deals and developing products on-line.

As a result, you need to know your VPN is secure. As you know, threats are everywhere. Hacking or other forms of cyber crime is no longer limited to computer experts. Now

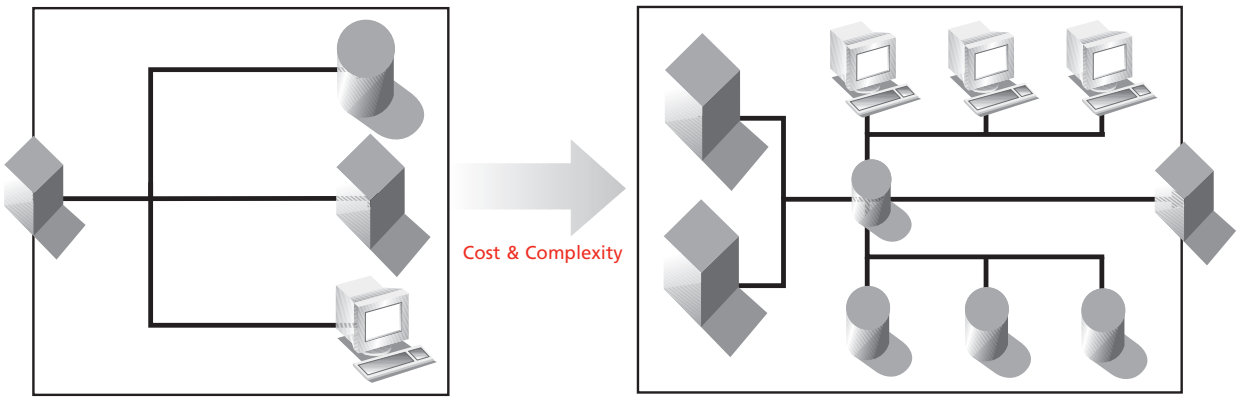
VPN COST / COMPLEXITY REDUCTION OPPORTUNITIES

Enterprise Infrastructure

- Reduction in leased line and dial access charges
- Reduced user support
- Simplified remote access architecture

ISP Infrastructure

- Help desk services
- Tracking / billing for usage
- Remote access equipment



anyone with a PC can download and use free tools to hack your network. And losses can pile up in many different ways: hackers stealing information, kids having fun, and even insiders looking to cause damage. No one is immune

It's also important to recognize that when it comes to cyber crime, the stakes are very high. In addition to financial loss, information is at risk—customer data, credit card information, corporate applications, product secrets, employee data and more. Information and other data assets are the lifeblood of your business. What's more, cyber crime jeopardizes your reputation and the trust you've earned. Once you've been breached, it's hard to recapture your good name.

Enhanced Security for VPNs

For many IT organizations, security remains a primary obstacle to implementing VPNs. With a private network, you know you 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 employing enhanced security services to encrypt information and authenticate users for network access.

Encryption: Keeping Your Data Private

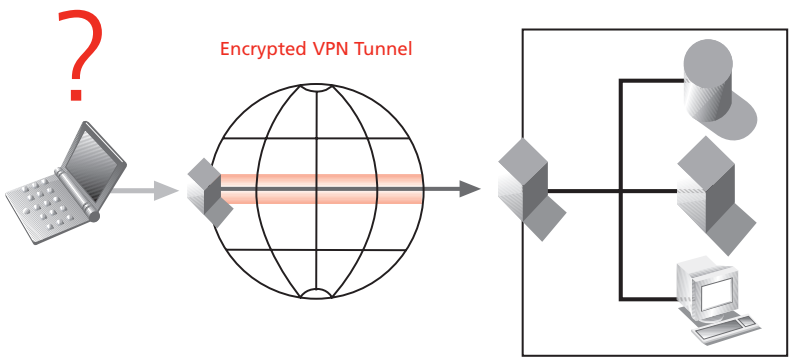
One layer of protection—ensuring the confidentiality and integrity of data you are sending, receiving and storing—can be easily achieved through the use of encryption technology.

Privacy of Data at Rest

All too often, credit card numbers, users' personal information, trade secrets, and confidential files are sitting on networked devices, unprotected. One of the easiest first steps to protecting this information is through the use of encryption technology. Encryption "scrambles" information so it is unintelligible if someone on the network gains access to this information.

Privacy of Data in Transit

For business to exist "at the speed of thought," data must be transmitted electronically across open and public networks—networks that cannot be trusted. Here again, one of the easiest first steps to securing this data is through the use of encryption technology that ensures that the information flowing across the public network is unintelligible to prying eyes.



The Cornerstone of VPN Security: User Authentication

Data integrity

Finally, the integrity of the data whether at rest or in transit is essential to any business process. An electronic order requesting 100,000 units is much different than an order for 1,000,000 units. You need to be confident that no one can get a hold of your confidential information and change it as you conduct your e-business across the public network. Encryption technologies offer you the ability to "booby trap" data, so you will know if it has been tampered with.

Authentication: Privacy vs. Security

What you've learned so far is that VPNs are private—the encrypted tunnel protects your data as it travels across the public network. But you must consider that privacy does not necessarily equal security. To be completely secure, there's still one more thing that you need to beware of: the authenticity of users. When a remote user accesses your corporate network, how do you know that he is who he says he is? Without enhanced security, you don't know—not for sure anyway.

In an attempt to identify users, many VPNs are protected merely by passwords. However, passwords alone cannot ensure secure remote access because they are a weak form of security. Passwords are easily guessed, stolen or otherwise compromised. And if a password is compromised you have no idea who is at the other end of your VPN.

VPN Authentication Choices

So now you've learned that the cornerstone to VPN security is authentication, the act of identifying and verifying the authenticity of users before they gain access to critical data assets and resources. You'll want to select from varying levels of authentication strength based on the value or sensitivity of the information that you're protecting, balanced against other considerations like usability, deployment, and budget. Let's consider the strength of various options.

Passwords

Passwords are the weakest, although most widely used, form of authentication. They help to identify users by requiring a single factor of identification—their secret code. This method of authentication is perceived to be easy to deploy and inexpensive. However, history has proven that these codes are easily guessed, stolen or otherwise compromised and are not as easy or inexpensive to maintain as you would think. Surprisingly, passwords are one of the most ineffective forms of authentication.

PASSWORD CRACKING TECHNIQUES

In many cases, VPN access is protected merely by passwords. Passwords offer a weak form of user authentication because they are easily guessed, stolen or otherwise compromised. And you don't have to be a computer expert to hack through password protection. VPNs are hacked every day by disgruntled ex-employees, thrill-seeking teens and competitive spies.

Password Cracking Tools
A variety of software tools, such as L0Phtcrack and NT Crack, automate the guessing of passwords through brute force and with extensive dictionaries of frequently used passwords. This approach is fostered by the fact that most users choose passwords that are predictable, such as "password" or children's names.

Network Monitoring
Also known as "sniffing," network monitoring is based on the fact that Ethernet routes all network traffic past individual user nodes, which normally capture only the messages meant specifically for them. Sniffing utilities allow you to reset your PC to "promiscuous" mode, thus monitoring without detection the contents of any message that streams by and flagging messages based on keywords, such as "login" or "password," in order to capture the desired information.

Brute Force Dialing
Programs like ToneLoc automate the process of locating modem telephone lines. When a line is found, it repeatedly attempts sign-on with various password alternatives. This approach is particularly effective with unauthorized modems attached to corporate phone lines, or in organizations where there is no monitoring of attempted dial-ins.

Abuse of Administrative Tools
Many tools that have been designed to control and improve networks can be misused for destructive purposes. For example, the software utility called S.A.T.A.N., a sinister acronym for System Administrator's Tool for Analyzing Networks, was designed to help managers strengthen their network security. However, it is widely used by hackers to identify and capitalize on network vulnerabilities.

Social Engineering
In contrast to the high-tech tools available to uncover passwords, some intruders use non-technical approaches to steal passwords. One well-known trick operates much like a classic con man swindle: Posing as an IT staffer, the hacker calls a new employee and offers to expedite the set-up of his system and the new employee volunteers the password, giving the hacker easy access.

Two-factor Authentication

This method of authentication is much stronger than passwords because it requires users to present two forms of identification before gaining access to protected resources. Much like a bank ATM, users must both know their PIN and possess their authentication device (token or smart card). The combination proves that users are who they say they are.

RSA SecurID® Hardware Tokens

RSA SecurID time-synchronous tokens provide strong two-factor authentication by requiring users to present something they know and something they have. These tokens are designed as an easy-to-use and deploy option for replacing passwords—a weak form of authentication that can easily be guessed or compromised.

Digital Certificates

The use of digital certificates as a form of authentication is quickly becoming more widespread with the growth of Internet transactions. Digital certificates help identify users by requiring access to digital credentials that should only be used by the rightful owner. Digital certificates offer strong two factor authentication through the ability to be pass-phrase protected in the Web browser credential store.

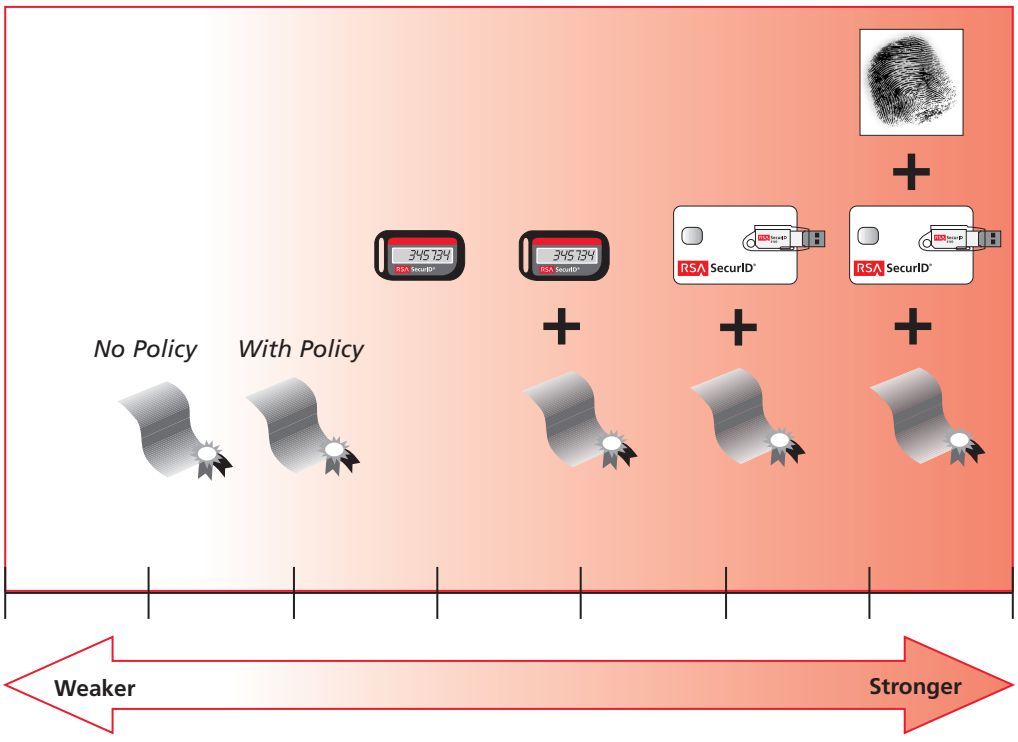
Smart Cards, USB Tokens and Certificates

Introducing smart cards or USB tokens to protect digital certificates is one of the strongest levels of authentication service. Not only is access to the smart card protected with two-factor authentication, but key pairs can also be generated and stored on the smart card or USB token. In fact, the private key never leaves the card or token, so it can never be accessed by unauthorized users or copied to a server.

Smart Cards, USB Tokens, Certificates and Biometrics

By introducing a third factor, such as biometrics, into your procedures, you can achieve the strongest available level of authentication. Biometrics refers to a characteristic that is unique to a user. This measurement is achieved through approaches like fingerprinting, retinal scanning and voice printing. This third authentication factor, combined with certificates stored on a smart card or USB token, is impenetrable.

AUTHENTICATION CHOICES CONTINUUM



V. CONCLUSION

Get Yourself a Strategic e-Security Partner

VPNs have emerged as the primary technology to reduce remote access costs and provide private transactions through the Internet. VPNs deliver tremendous business value, but only if they provide the appropriate level of security to guarantee the privacy and integrity of corporate information accessed only by authentic users. Each VPN should provide the security required to prevent unauthorized viewing or eavesdropping on network traffic as well as strong authentication to positively identify each user and network integrity to prevent tampering with data as it passes through the Internet.

Keep in mind that you don't have to go with an "all or nothing" approach. You may discover that you have disparate e-business initiatives that require different levels of security—in which case you may opt to use a mixed approach. That is, you deploy a digital certificate management solution protected with two-factor authentication for high-value resources, but rely on simple passwords for non-critical applications. You may even decide to take a phased approach to your e-security plan if time-to-market, budget and human resources are an issue. Here you might start by replacing weak passwords with certificates and add two-factor authentication to bring user identification to a higher level as resources become available.

All of this requires a diverse and robust set of security tools. So when you look for a strategic partner to help you secure your VPN, look for a vendor with choices—only then will you be able to choose the right level of security for your unique VPN requirements. It's all about options and the right strategic e-security partner will be able to offer you a full range of choices. And in the end, you'll have a security solution that's just right for your business. achieved through approaches like fingerprinting, retinal scanning and voice printing. This third authentication factor, combined with certificates stored on a smart card or USB token, is impenetrable.

ISVPN WP 0104

RSA SECURITY®

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

IPSEC IN VPN IMPLEMENTATIONS

Internet protocol security (IPSec), developed by the Internet Engineering Task Force (IETF) IPSec Working Group, defines the standard for providing network layer authentication, access control, encryption, message integrity, and replay protection for securing communications between network devices and applications. IPSec analyzes IP packets sent to and from a network interface, allowing those that match the configured security policy to pass. Those that do not match the policy are discarded.

IPSec offers two modes of operation: transport and tunnel. With transport mode, the security endpoints correspond with the communication endpoints (i.e., sender and recipient), providing end-to-end security for traffic that passes across a multi-segment network, such as the Internet. In tunnel mode, security is applied on one or more network segments between the sender and recipient (neither need be IPSec-aware) resulting in security that is transparent to the communication endpoints.

It is important to note that IPSec supports the use of Industry standard X.509 digital certificates as one of its methods of authentication. When managed by a digital certificate management solution, digital certificates allow you to validate devices on both the client side and the server side. In a typical VPN environment, device identification is performed through the exchange of a single, shared secret. In contrast, managed digital certificates use a unique key pair (one public and one private) that each VPN client shares with the VPN gateway to ensure the authenticity of a device.

The use of digital certificates in an IPSec-compliant VPN environment is particularly appealing for businesses that have already invested in a digital certificate management solution as they are able to extend the benefits of their existing investment across multiple applications. The use of digital certificate management in an IPSec-compliant VPN environment also expands interoperability, allowing companies to expand VPN use beyond the enterprise (for example, VPN remote access for partners, customers and contractors) without vendor interoperability issues.