

# Playing the Remote Access Game: Will IPSec or SSL VPNs fit your needs?

Enterprises currently face two seemingly opposed imperatives in the quest to improve productivity, increase profits, and mitigate risk. One requirement is the growing need to provide a variety of audiences, from employees to contractors and from business partners to customers, with “anywhere/ anytime” access to information. The creation of virtual private network (VPN) technology made it possible to extend information outside the enterprise in a cost-effective fashion. The evolution of both network-layer (IPSec) and application-layer (SSL) VPNs has now made connections from site-to-site and from user-to-site very easy and efficient.

The other mission critical need faced by today’s enterprise, which is growing in proportion to the need to provide access, is to secure internal resources as access becomes more pervasive. Well-publicized stories of hackings and information and identity theft, coupled with today’s strict regulatory environment, are forcing companies to protect electronically stored information from unauthorized access. And the fact is that in many instances, it’s not much harder for a hacker to gain access to a company’s network than it is for an authorized user.

RSA SecurID® authentication software enables companies to provide secure access to networks using both SSL VPNs and IPSec VPNs. This paper will focus on the differences between the two and the particular benefits of implementing RSA SecurID two-factor authentication with SSL VPNs.



Confidence Inspired™



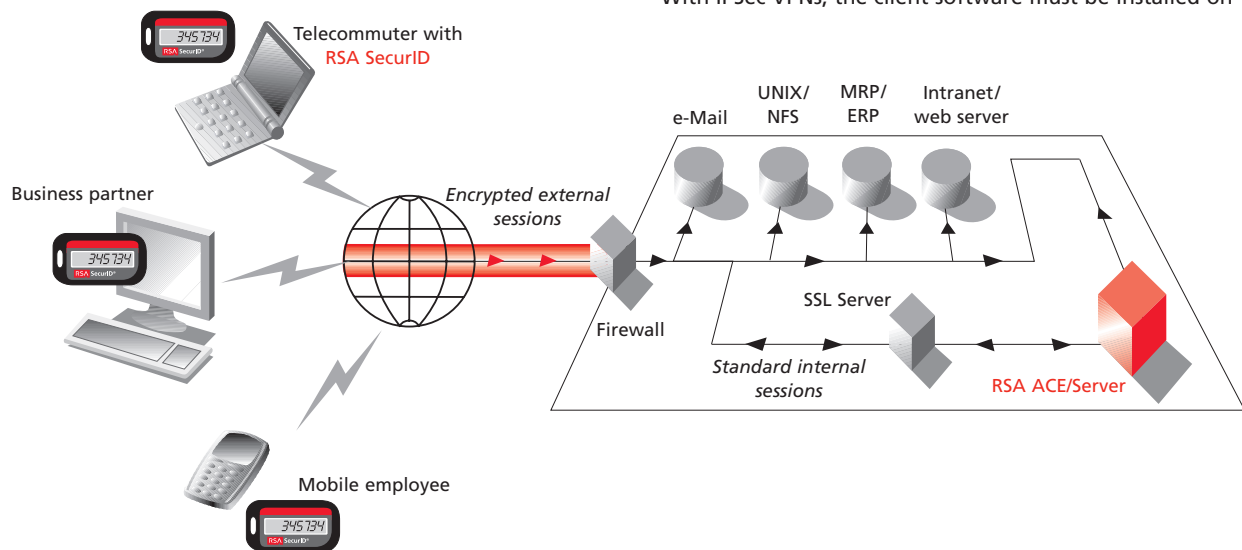
TABLE OF CONTENTS

I. INTRODUCTION	PAGE 1
The Emergence of SSL VPNs	
The Issue of Security	
II. SSL VS. IPSEC: IS ONE "BETTER" THAN THE OTHER?	PAGE 2
Cost and Management	
Flexibility	
III. RSA SECURID TECHNOLOGY VS. PASSWORDS: FOR STRONG SECURITY, ONE IS CLEARLY BETTER THAN THE OTHER	PAGE 3
The Problems with Passwords	
IV. CONCLUSION	PAGE 4
ABOUT RSA SECURITY INC.	
ABOUT JUNIPER NETWORKS.	

## I. INTRODUCTION

With growing numbers of mobile and remote workers—and the need for them to maintain their productivity outside the enterprise—organizations have tried to seamlessly, securely and cost-effectively connect these users to network applications and resources. The original solution—dialing up on dedicated lease lines connecting office-to-office—was slow and expensive. In the early 1990s, virtual private networks (VPNs) changed that paradigm by providing a way to transport private data using the public Internet infrastructure. Network-layer VPNs use peer negotiation software like IPSec, installed on the client PC, to encapsulate the data being transferred. The data is then transferred across the Internet in this IP “wrapper,” which is then “unwrapped” at the other end. Traffic received by the VPN gateway is routed as if it came from within the enterprise, which allows IPSec VPNs to provide an “on-the-LAN” experience. IPSec VPNs remain ideal for office-to-office connections. They are also a workable solution if an organization has only a small, trusted audience to which they want to extend access. Limitations to this approach for widespread remote access include the following:

- The deployment, installation, configuration and management of software on every client PC can be cumbersome,
- Users must use a corporate PC to access information, which can be inconvenient and
- Because IPSec VPNs enable full LAN (or VLAN) access, users can get access to sensitive internal information.



## The Emergence of SSL VPNs

IPSec VPNs are a good solution for a contained number of trusted users accessing the LAN from managed corporate PCs. Increasingly, however, a significant number of users are more likely to be in different locations (homes, customer sites or hotels), use different devices (laptops, PDAs and web-enabled cellular phones) and come from different types of audiences (employees, contractors, business partners or customers.) In such instances—as well as when an organization has hundreds or thousands of remote users, or where an organization doesn't have control of the user's desktop (such as with business partners)—to install client software on remote users' PCs is expensive, difficult to manage and all but impractical.

Because of these challenges, a new kind of VPN emerged: the SSL VPN. SSL VPNs use the Secure Sockets Layer protocol, which is part of all standard web browsers, to provide secure transport over the Internet instead of individual client software. Because SSL VPNs require only a web browser and Internet connection, they are a highly flexible remote access solution. They are not, however, an ideal solution for site-to-site connections, where an on-the-LAN experience is essential.

## The Issue of Security

Because VPNs are designed to provide access to internal information, security and access control are major issues. Both IPSec and SSL VPNs provide encryption to ensure the confidentiality and integrity of data in transit across the Internet itself. This answers the question of data integrity, in that the information sent will be the information received, but it does not address the greater question of the user's identity in an SSL or IPSec VPN environment. With IPSec VPNs, the client software must be installed on

the PC. The step of installing software on each client PC has led to the impression that IPsec VPNs are more “trusted,” though this impression may not be completely valid with the proliferation of free, easily downloaded client software and the increasing sophistication of hackers. SSL VPNs can provide access to a much broader audience that is inherently less well known because there is no need to install software on the PC client. The fact remains, however, that any access solution requires a strong two-factor authentication solution such as RSA SecurID technology.

## II. SSL VS. IPSEC: IS ONE “BETTER” THAN THE OTHER?

Both SSL and IPsec VPNs are highly effective remote access solutions that use field-tested protocols and methodologies. They offer roughly the same performance bandwidth, and the same level of encryption. Furthermore, IPsec and SSL VPNs are not mutually exclusive; they can be, and often are, deployed within the same enterprise. Each, however, has strengths that make it most suitable for particular situations. For example, IPsec VPNs are considered ideal for static, long-term connections between offices, whereas SSL VPNs are the best choice for providing access for large numbers of mobile employees and for business partner extranet environments. A side-by-side comparison in two key areas—cost and management, and flexibility—follows.

### Cost and Management

Because they provide a transparent, “on-the-LAN” experience, IPsec VPNs remain the access method of choice for site-to-site connections. IPsec VPNs are also effective for user remote access, but require that a software client be installed and configured—and, as necessary, upgraded—on each user’s PC. For small, finite user populations, such as a defined group of remote employees, this can be managed. However, organizations that need to provide remote access to large numbers of mobile users in disparate locations would need to deploy, configure and manage client software on each user’s PC, which would prove an administrative and financial burden. When providing access to audiences such as business partners or customers, deploying client software is not even an option. In such situations, where the organization cannot manage user PCs, an SSL VPN may be a better choice. With an SSL VPN, users don’t need to have client software installed on their PCs (or PDAs, or mobile phones) in order to gain access, so there is virtually no cost or management required on a per-user basis. In addition, with SSL VPNs the link between the user and the enterprise resources occurs at the application

level, making the SSL VPN operating system independent. Therefore, if the OS changes on a user PC in an SSL environment, nothing needs to be done—while with IPsec, the client software would need to be upgraded and reconfigured. Because there is no client software to configure and maintain, SSL VPNs can offer an overall lower cost of deployment, and lower total cost of ownership, for organizations serving large numbers of diverse users.

### Flexibility

By eliminating the need for expensive leased lines in favor of the public Internet as a connection vehicle, IPsec VPNs represented an improvement in flexibility. IPsec VPNs deployed in a site-to-site configuration retain the same basic functionality as those dedicated connections, at a much lower cost. For remote users, however, IPsec VPN connectivity is limited to those PCs on which the client software has been installed and configured. Therefore, if the enterprise has control of the user desktops, IPsec is a feasible solution, though it becomes harder to manage as the audience grows. When IT personnel do not have control of the PC, such as with business partners and mobile employees, SSL is a more flexible choice. With SSL, the “client” is the browser itself, which is ubiquitous—not only on virtually all PCs, but also on Internet kiosks, PDAs and many mobile phones.

SSL VPNs, therefore, are highly scalable, providing the fully portable environment required for anytime, anywhere access. The most important benefit of SSL VPNs may be that they support not only remote employees, but also business partners and mobile employees—helping to sustain productivity and enhance customer service and sales activities.

### Conclusion: Both are Effective and Complementary

IPsec and SSL VPNs are effective and efficient means of providing network access to remote users and from site-to-site. Each excels in different scenarios, and many complex organizations could see reason to use both. One is not, therefore, “better” than the other; they are each ideal for what they do best. Because both methods secure data in transit, a key consideration is how to provide effective authentication ensuring that the user is who they say that they are.

### III. RSA SECURID TECHNOLOGY VS. PASSWORDS: FOR STRONG SECURITY, ONE IS CLEARLY BETTER THAN THE OTHER

For all the convenience of VPNs, there also are security risks. IPSec VPNs are designed to enable a virtual extension of the corporate LAN. A routed tunnel between the client machine and the VPN gateway effectively places the client machine on the network. Therefore, if a remote computer on an IPSec network becomes infected with a worm or virus, the network and servers are vulnerable to infection. Yet because SSL connects at the application layer, the network would never be similarly exposed.

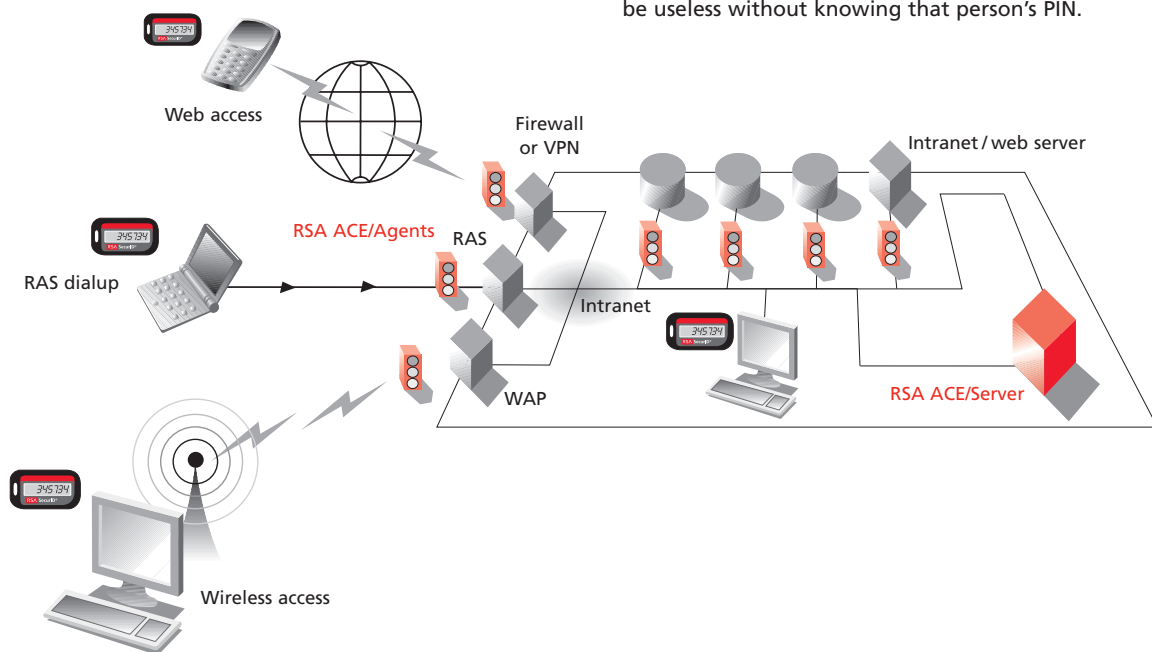
However, SSL VPNs are also vulnerable for the simple reason that the Internet is vulnerable. While SSL provides encryption to protect the data, there is usually nothing other than a password to prevent unauthorized users from gaining access to the network.

#### The Problems with Passwords

Password protection is the most commonly implemented authentication method for securing VPNs, yet passwords alone are a weak solution. There are many reasons for this, such as:

- Passwords can easily be lost, forgotten or shared/overheard,
- Passwords can be guessed or hacked,
- Using the same password for entry to the VPN that is also used for other resources gives the keys to the kingdom to unauthorized users,
- Weak password policies (i.e., those that do not require regular password changes or mandate use of both numerals and letters) do not pass security audits and
- Strong password policies have the unintended consequences of promoting unsafe practices (such as writing down passwords) and increasing help desk costs when employees inevitably forget their passwords.

Passwords are a single-factor solution; in other words, a user just needs to furnish the correct password in order to gain access. Far more robust and secure is a two-factor solution, which combines a password or PIN with another authentication method. RSA SecurID technology, for example, works with an authenticator (or “token”) to provide two-factor authentication. When users attempt to access the SSL VPN, they will be prompted for their PIN and the random digital “token code”—which changes automatically every 60 seconds—that appears on their token. Only with both factors correctly employed can a user gain access to the VPN. That way, someone could learn a user’s PIN but not be able to steal his or her identity without also gaining possession of the token. And if someone were to find or steal a person’s token, it would be useless without knowing that person’s PIN.



## RSA SECURID AUTHENTICATION KEEPS CATHOLIC HEALTH SYSTEMS' SSL VPN SECURE

Formed in 1998, the Catholic Health System (CHS) provides health care services to 200,000 people across western New York. One of the two largest providers in the region, CHS encompasses more than 40 sites, employs 8,000 people and is affiliated with 1,200 physicians. CHS had two challenges: implement a scalable, extensible remote access solution for its widely dispersed physicians; and comply with the federal Health Information Portability and Accountability Act (HIPAA).

"We have both an ethical and a legal obligation to safeguard the confidentiality of patient information," says Doug Torre, director of networking and technical services at CHS. "We wanted to provide physicians with remote access to patient data, including x-ray images, lab results and transcribed reports so they could respond to patient needs at any time, even when they were off-site."

Initially, CHS installed an IPSec VPN but found it too cumbersome and expensive to deploy and support—chiefly because it required configuration of remote PCs. Then the organization decided on an SSL VPN solution comprising the Neoteris Instant Virtual Extranet (offered by NetScreen, which was recently acquired by Juniper Networks), along with RSA SecurID authentication software. To access CHS resources via the extranet, users must have an RSA SecurID authenticator (in the form of a convenient key fob). "This gives us a high degree of certainty that people coming into our applications are, in fact, who they claim to be," says Torre.

CHS started with a pilot rollout to 10 users and the solution has since been scaled to 200 users. Best of all, implementing RSA SecurID two-factor authentication has helped CHS achieve compliance with HIPAA 45 164.312D, which mandates the use of authentication procedures to verify the identity of individuals seeking access to health information.

## CONCLUSION

RSA SecurID technology is effective, flexible and proven for strong authentication; passwords are simply no match for RSA SecurID technology. RSA SecurID hardware and software authenticators have been deployed to 15 million users worldwide. Their portability and device-independence make them a perfect match for the flexibility of the SSL VPN environment, yet strong two-factor authentication, should not be limited for use to only SSL VPNs when the security benefit is readily recognizable for an IPSec VPN environment as well. Hardware tokens are available in key fob, card and PINPad formats. Software tokens are available for Microsoft® Windows® workstations, Pocket PC, Palm handhelds and Blackberry handhelds.

In addition, a number of leading SSL VPN vendors have designed their products to interoperate with RSA SecurID authentication. To date, they include:

- Juniper Networks,
- Aventail,
- Cisco,
- CheckPoint
- Netilla and
- Whale Communication.

## ABOUT RSA SECURITY

RSA Security helps organizations protect private information and manage the identities of people and applications accessing and exchanging that information. RSA Security's portfolio of solutions—including identity & access management, secure mobile & remote access, secure enterprise access and secure transactions—are all designed to provide the most seamless e-security experience in the market. Our strong reputation is built on our history of ingenuity, leadership, proven technologies and our more than 14,000 customers around the globe. Together with more than 1,000 technology and integration partners, RSA Security inspires confidence in everyone to experience the power and promise of the Internet. For more information, please visit [www.rsasecurity.com](http://www.rsasecurity.com).

## ABOUT JUNIPER NETWORKS

Juniper Networks transforms the business of networking by creating competitive advantage for our customers with superior networking and security solutions. Juniper Networks is dedicated to customers who derive strategic value from their networks, including global network operators, enterprises, government agencies and research and educational institutions. Juniper Networks' portfolio of networking and security solutions supports the complex scale, security and performance requirements of the world's most demanding mission critical networks. Additional information can be found at [www.juniper.net](http://www.juniper.net).



RSA Security Inc.  
[www.rsasecurity.com](http://www.rsasecurity.com)

RSA Security Ireland Limited  
[www.rsasecurity.ie](http://www.rsasecurity.ie)

RSA Security, the RSA logo and SecurID are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and/or other countries. NetScreen-5GT, J-series and JUNOS are trademarks of Juniper Networks, Inc. Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.

**SSLVPN WP 0604 JUNIPER**