



# SSL VPN: Improving the ROI of Remote Access

## Secure Authentication and Access to your Critical Resources

---

### Overview

Every day thousands of people type “SSL VPN” in Google to search for relevant material on this new technology. SSL VPN is one of the fastest growing remote access categories, yet most organizations are not really that familiar with the value, history, or what this new type of remote access product really can deliver. Key questions like: All this hype around SSL VPNs, is it warranted? What is an SSL VPN and why do I need one ? Will it make me a savior to management and the business constituents or end my career? When should I use an SSL VPN vs. and IPSec VPN ?

As the ability to access corporate information has moved from RAS dial up servers and leased lines to broadband, the need to secure the information has grown substantially. This need is primarily driven by the inherent weaknesses of the Internet because of its open architecture. Justification for remote access security continues to be a plaguing problem. Demonstrating ROI primarily comes back to improved partner access, a reduction in downtime, and the cost of patching security holes after they are opened up. The PR from a security breach continues to be deadly. This all leads back to fundamental questions like: How can we open up our systems to more remote employees and business partners without creating security vulnerabilities? At the same time, how can we make this security not overly intrusive to users? These questions and the ultimate goal of providing a high degree of access to critical information, without pain will be answered within.

### Evolution

As applications have moved to the Web, the challenge that organizations face is how to deliver access from any PC securely without being intrusive on the end-user. For the last 20 years, users and management have constantly heard that they are not allowed to access applications outside of the office because of security reasons. In the 1970s the concept of remote access was accessing an application from a remote office. This required WAN and leased line connections.

During the 1980s a limited group of users could use a modem and dial directly into modem banks or their own PC, but this was extremely costly and limited to a select group. Personal computers were just becoming mainstream at work and the demand for remote access was not as great. Workers lead a more serene “work stays at the office” life unless you wanted to drag a plethora of paperwork home, which many did. As the 1990s rolled around, laptops started emerging as well as the home PC. Executives and sales representatives started traveling with their

computer and needing access to information real time. Site-to-Client IPSec VPNs came into being to protect this access. Site-to-Client VPNs provided the needed security, but presented challenges when users needed access from different locations. Any changes in the PC might disable the VPN. End users put up with these nuances and ongoing access headaches because they didn't have a choice. From the IT side, rolling out an IPSec VPN was not only about installing and maintaining the client, but about the change needed for the infrastructure. If an IT department has complete control of the infrastructure from the back-end to the client this was one degree of complexity. If the IT group did not have control, the degree of complexity went up a number of times. Imagine that users want to use their own home computers or if a partner wants access. Deploying a VPN client to a computer that you don't own or control can be very difficult. The same principal applies for local NATing and firewalls at the partner, home, or other sites such as hotels.

Today, organizations are starting to look at what their options are for secure remote access. IPSec VPNs and leased WAN lines are a perfect fit for static connections that don't change frequently. Companies started looking at SSL as a protocol that would ride on the Internet backbone. SSL was and is a common method for encrypting traffic over the Internet and many organizations moved to implement SSL for their Extranets and Intranets. Access control was limited though and SSL VPNs evolved. Organizations also realize that if traveling users only need access to limited applications that are primarily web-based, then, an SSL VPN is ideal. Full network access still would require an IPSec VPN, but many groups of users don't require this level of connectivity.

## **SSL VPN Defined**

SSL VPNs evolved to complement existing SSL implementations and increase the level of access control and web security that an organization implements. SSL VPNs also address the challenge that organizations have because the native security in application access has decreased. Dial-up by nature is relatively secure because there are only specific phone lines that can authenticate the user. Client Server and IPSec VPNs themselves have a certain amount of security because client software needs to be installed. At the same time, the risks of fraud, threats, and hacks are only increasing. Now that our applications and access is potentially available to anyone with a browser, the nature of security has changed.

SSL VPNs take the ease of use that SSL provides and implement the level of data security and access control that an IPSec VPN uses. SSL VPN is a phrase that was developed by the market a few years ago. Everyone understands what the acronym SSL and VPN means independently, but what does this new phrase mean together? At an academic and business level, it can be misconstrued to be an oxymoron because of what they stand for:

**SSL** secures data over the Internet with encryption that is automatically enabled in every browser. A certificate is needed for the web server, but other than the few days you wait for your credit card to clear buying your certificate, turning on SSL is relatively straightforward for an application. If the application does not natively support SSL, then changing some links might be needed, but this depends solely on the application. For larger loads of traffic, SSL acceleration is recommended to alleviate any bottlenecks, but this is a plug and play implementation.

**VPNs** on the other hand are focused around virtually connecting networks. The “Private” part of VPN ensures privacy of the data and a certain level of access control. VPNs are always associated with IPSec because it is the de facto protocol used to encrypt traffic for VPNs. IPSec VPNs are used to connect two networks or end points. These are then closed end points or connections. This is done with a physical client that is installed on a users machine. IPSec also operates at a network layer for this connection.

So, how do SSL and VPN collide? One school of thought can be convenience of describing the ubiquity of SSL and the security or perception of security that a VPN provides for secure remote access. SSL VPNs are the best description for the technology that is used to solve the business problem of easily and securely connecting end users to critical corporate data. SSL provides an easy to use avenue to access information, replacing the difficult to use VPN client. Any machine with a browser can use SSL VPNs, where with a traditional VPN; a physical client needs to be installed on every machine that is used for access. Because SSL is embedded in browsers, the need for a client disappears. This is especially important when users have several machines (home, work, client site) they use to connect to information. VPN is a common term for describing secure remote access tunnels. At an academic level SSL VPN might seem like a contradiction, but really it is a clarification on the next generation of secure remote access properties.

## **Why SSL VPN**

SSL VPNs are attractive to organizations with heavy remote access needs for a number of reasons. As more organizations struggle with the right balance of access control, security, and overall end user acceptance, SSL VPNs provide a perfect fit. In a June 12th Infonetics Research article, they stated, “By 2005, 74% of mobile workers will use VPNs, up from 59% in 2003; this increase is due in large part to the fact that SSL offers an alternative to IPSec that avoids the headaches of deploying and managing client software.”

John Girard, vice president and research director at Gartner, Inc in an April 8<sup>th</sup>, 2003 report, best describes the value of SSL VPNs:

*“Enterprises that want easier and more flexible ways to deploy secure remote access should consider SSL VPNs for new investments, and as upgrades for legacy VPNs. Many enterprises implement complete VPNs where simpler, easier, less expensive private access could be created by using SSL-based solutions.”*

The value of an SSL VPN comprises multiple areas. The key areas are improved access control, web security, ease of use and the return on investment.

**Access Control** is more efficiently implemented with an SSL VPN because different users can be centrally managed. All remote access is controlled through the SSL VPN console to more effectively monitor the privileges and rights of users. These users can be employees, business partners, and clients. Access is restricted at the application layer and can be granted down to a URL or even file level. With an IPSec VPN, security is enforced at the network layer.

SafeNet’s SafeEnterprise™ SSL iGate offers integrated two factor authentication that enforces the security from the specific user in addition to locking down the application level. This is the last area that future of secure remote access because user logs and audits ensure a greater level of trust.

**Web Security** is enforced and more comprehensively managed through hardened, appliance-based SSL VPNs. Data integrity is upheld by ensuring only users with their vested rights can access critical data. All traffic goes through the Web ports that you already have open for traffic. Other ports or “holes” in your firewall don’t need to be created. The risks that exist from vulnerabilities with Web servers are mitigated because the SSL VPN appliance proxies the web servers in effect hiding the web server DNS information. The major security concerns that IPSec VPNs create are that they bridge networks, where an SSL VPN terminates sessions between it and the client side applications.

**Ease of Use** is one of the most important reasons why clients choose an SSL VPN. The average user wants to leverage the freedom that Web-Based applications offer and a full client VPN limits the ability to access corporate data from PCs where the client is not installed. From initial installation through ongoing maintenance, the value that SSL VPNs provide is the ability for deployment of an application without having “control of the desktop”. Remote sales executives can access their CRM system securely through only a browser from their home or client computer when their IPSec VPN is most likely not installed.

Because SSL VPNs can be implemented without deploying a VPN client, expanding secure access to non-employees securely is now possible. Business partners that need access to systems such as Supply Chain and CRM can now access them via only a browser, where before they might never have been given access. The critical factor is how easy it is for end users because if the technology is too difficult, then users won’t use it.

Most SSL VPNs offer the ability to protect Web and legacy applications through their proxy technology. SSL VPNs can securely move almost any protocol over SSL by using a local applet to interpret the data calls to the backend. Instead of a local client talking POP to the server for example, the local client talks POP to the local applet, which then wraps it in SSL and sends it securely over the Internet to the SSL VPN appliance. The SSL VPN appliance then forwards the POP data to the back-end server.

Examples of this are mail (POP, IMAP), file sharing (FTP), and other legacy applications such as Telnet. The value from this support is that organizations don’t have multiple holes in their firewall to allow various ports to move through. All access is done through the SSL VPN proxy over SSL.

**Return on Investment (ROI)** is one of the most critical areas to look at when analyzing an SSL VPN. The ROI for an SSL VPN can be broken into a few categories:

Telecommunication costs can be reduced because companies can use the Internet backbone directly instead of relying on dial-up connections for remote users. Many users could not leverage the high-speed Internet connection available in remote offices and hotel rooms because their VPN client would not always function.

Initial Implementation costs will be reduced several fold with an SSL-based VPN because SSL doesn’t require any changes to the corporate or client infrastructure. SSL can be implemented on the back-end in a matter of hours, The majority of implementation costs occur with the clients because VPN clients need to be installed on every desktop. This can take several hours per client machine because the TCP/ IP protocol stack needs to be modified and varies depending on the client

settings. With an SSL VPN, the implementation is minutes because the user just fires up a browser.

Operational Costs are really where an SSL VPN shines because the browser doesn't need to be updated on every revision and the browser doesn't interfere with other applications. SSL is built into every browser. With an SSL VPN, the Internet connection needs to work and that's all.

Web Security can be an important financial driver as organizations weigh the costs of protecting their core applications. Proactively monitoring and patching applications as new vulnerabilities arise can be resource intensive. SSL VPNs proxy web servers and provide an additional level of authentication because users must first authenticate to the SSL VPN appliance before they are passed on to the application. Users that are not part of an already trusted group will not even be allowed to see the web servers. The need for aggressive patching is reduced because of this additional security layer. Wireless access can be securely managed by restricting use to applications and ensuring encryption and authentication are properly implemented.

Because SSL VPNs are easy to manage and less expensive, corporations can extend the reach of remote access to more employees. The solution is ideal for corporations whose employees are often "on the go."

### **IPSec vs. SSL**

The best way to determine which technology is appropriate for your company is to examine the use case scenarios. The following outlines when the respective types of VPNs should be used.

	<b>IPSec</b>	<b>SSL</b>
My users need access to email, files, and a few applications when operating remotely	Recommended	Recommended
My users need to be able to do everything remotely that they could do from within the office	Recommended	Not Recommended
My users travel frequently, and find themselves connecting from different locations	Not Recommended	Recommended
My users work in a branch office and need access to corporate applications.	Recommended	Not Recommended

### **Are Passwords Enough?**

One of the biggest questions that arises is what degree of access control on the client end is needed. Demand for security that is better than passwords has been minimal with traditional remote access solutions, but with more applications moving to the Web and SSL VPN solutions that enable anywhere access with only a browser start to take off, the interest is renewing. Preventing exploitation of web server vulnerabilities, hacker prevention, and simply reducing password theft are all major drivers to investigate technology better than passwords. The form of client side security, whether it be passwords or not, is your option but should be considered for more sensitive data that is being accessed and protected with an SSL

VPN. Three interesting facts that support the use of technology that is better than passwords are:

- In one survey, carried out by PentaSafe Security, two-thirds of commuters at London's Victoria Station were happy to reveal their computer password in return for a ballpoint pen. Another survey found that nearly half of British office workers used their own name, the name of a family member or that of a pet as their password.
- According to Meta Group, the most common way for intruders to gain access to company systems is not technically related, but simply involves finding out the full name and username of an employee (easily deduced from an e-mail message), calling the help desk posing as that employee, and pretending to have forgotten the password.
- There is well-known software on the market that can guess your passwords in a matter of seconds. Even the most complicated passwords can be broken by brute force in mere minutes.

Tight hardware token integration should be viewed as a key security feature. Password-based credentials are not constantly checked and re-checked on many authentication systems to ensure that the user is authorized to gain access. Tokens should be integrated with solutions such that when a user leaves the workstation with the token then the secure connection to the content is closed. Access control is the key to an effective SSL VPN solution and password alternatives such as random number tokens, USB keys, and digital certificates all exist. For companies concerned about password management, specific solutions replace passwords with tokens and offer a “reduced sign-on” capability, providing users with a single private Web access.

Password-based authentication (single factor) presents a number of problems:

- The compromise of a password often goes undetected. When a hacker guesses a password, the legitimate user is often unaware that his credentials have been stolen—that, in effect, his or her identity has been stolen.
- Password sharing amongst users is a related form of the above problem.
- Passwords that are hard to guess are also hard to remember, resulting in additional administration costs to support users that have forgotten their passwords.
- Since passwords are hard to remember, the typical user often uses the same password in many locations: guess it once, and the hacker has them all. Worse yet, users often write them down.

When deploying a secure remote access solution such as an SSL VPN or other VPN, evaluate the value of your data against your password policies and use scenarios. More organizations are turning to USB tokens, smart cards and other technology to ensure their data is secure.

## Applications

The applications and use case scenarios for an SSL VPN are limitless, but here are the most important ones that apply to almost every organization.

**Email** is the crux of every company's communication and there are always times when you can't get access or have problems. IPSec VPNs allowed you to protect email but with a client installed you were limited on access. With an SSL VPN, the best of both worlds is finally here. Secure access can be granted from any Web

browser to access your Web email, and now you can take advantage of accessing your client server email from your own computer with a high-speed line. Both Web and client server applications are securely protecting via SSL and sent over the Internet where the SSL appliance manages the connections centrally. In the old days, you would need to dial-up to use your local email client and using a high-speed connection at home or on the road was not possible. There were always problems with access and the firewalls. Imagine consultants that are working on site that need access to email. Dial-up is not possible, with an Internet connection; they can either access web or local client server (MS Exchange for example) without interfering with the client's network or firewall settings. Several SSL VPNs allow users to access applications via a portal page and hide the back-end domain of the email or other servers for security reasons.

**Intranets** are the most basic access points, but always the most complicated to manage. It's always that one file on the network you need when traveling, but can't get to it. Organizations have been reticent to allow full file sharing remotely for security concerns and many don't have a method of pushing out access via a browser. SSL VPNs enable secure file and intranet access now to increase productivity of employees.

**Partner Extranets** are becoming critical as companies move to increase operating efficiencies and improve relationships. SSL VPNs are positioned well to take advantage of this business driver because traditional IPsec VPNs were not ideal to deploy to a business partner. Because organizations are concerned about security and ensuring that business partners can only see what they are allowed to, most organizations have only allowed limited access for partners. Most sensitive pricing, inventory, and other critical business data is still emailed or faxed instead of being able to be downloaded directly from a vendor Extranet. The ability to upload information from partners is also unheard of because of security concerns. SSL VPNs can address all these concerns by providing granular access to allow partner's access not only to specific applications, but limiting users and user group's access even to the file level.

## Summary

SSL VPNs offer a low cost, easy to deploy technology that is ideal for traveling employees or business partners that need access to a limited application set. SSL VPN technology harnesses the flexibility and ubiquity that the Internet offers us with advanced Web security. This gives us the perfect balance between security and ease of use. SSL VPNs will help your organization meet its business, security and information technology goals of securely opening up systems to remote users at an attractive level of investment. Meta Group, a Stamford, Conn.-based research firm, predicts that SSL VPNs will be installed in one out of three major companies by 2004, and in 80 percent by 2006. SafeNet's SafeEnterprise™ SSL iGate is a leading SSL VPN in the space because of SafeNet's extensive SSL background and authentication leadership. For more information the SafeEnterprise™ SSL iGate, go to : <http://www.safenet-inc.com/products/igate/igate.asp>

## SafeNet Overview

SafeNet (NASDAQ:SFNT) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit [www.safenet-inc.com](http://www.safenet-inc.com).



[www.safenet-inc.com](http://www.safenet-inc.com)

**Corporate Headquarters:** 4690 Millennium Drive, Belcamp, Maryland 21017 USA  
Tel: **+1 410.931.7500** or **800.533.3958** eMail: [info@safenet-inc.com](mailto:info@safenet-inc.com)

Phone USA and Canada (800) 533-3958  
Phone Other Countries (410) 931-7500  
Fax (410) 931-7524  
E-mail [info@safenet-inc.com](mailto:info@safenet-inc.com)  
Website [www.safenet-inc.com](http://www.safenet-inc.com)

© 2004 SafeNet, Inc. This document contains information that is proprietary to SafeNet, Inc.  
No part of this document may be reproduced in any form without prior written approval by SafeNet.  
SafeNet shall have no liability for errors, omissions or inadequacies in the information contained herein  
or for interpretation thereof. The opinions expressed herein are subject to change without notice.

**Australia** +61 3 9882 8322  
**Brazil** +55 11 6121 6455  
**China** +86 10 8266 3936  
**Finland** +358 20 500 7800  
**France** +33 1 41 43 29 00  
**Germany** +49 18 03 72 46 26 9  
**Hong Kong** +852 3157 7111  
**India** +91 11 26917538  
**Japan** +81 3 5719 2731  
**Japan(Tokyo)** +81 3 5719 2731  
**Korea** +82 31 705 8212  
**Mexico** +52 55 5575 1441  
**Netherlands** +31 73 658 1900  
**Singapore (1)** +65 6274 2794  
**Singapore (2)** +65 6297 6196  
**Taiwan** +886 2 6630 9388  
**UK** +44 1932 579200  
**UK (Basingstoke)** +44 1256 345900  
**U.S. (Massachusetts)** +1 978.539.4800  
**U.S. (New Jersey)** +1 201.333.3400  
**U.S. (Virginia)** +1 703.279.4500  
**U.S. (Irvine, California)** +1 949.450.7300  
**U.S. (Santa Clara, California)** +1  
408.855.6000  
**U.S. (Torrance, California)** +1 310.533.8100

Distributors and resellers  
located worldwide.