



Deploy IPsec and SSL Together for a Complete Remote Access Solution

A Fiberlink White Paper

Derek Finch, Product Marketing Manager

I. Introduction	2
II. Which One is Better?	2
III. About IPsec	3
IPsec's Pain Points	4
IPsec Security Issues	4
IV. About SSL	4
Why the Market is Interested in SSL	5
Challenges of SSL	5
SSL Security Concerns	6
What to Look for in an SSL Solution	6
V. A Time and a Place	7
Integrate for Easier Management	7
VII. Conclusion	8

I. Introduction

Virtual Private Networks (VPNs) allow corporations to provide employees, partners, customers, and others with policy-enforced, secure access to the corporate LAN over the Internet. The primary technologies used in providing VPNs are Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL). Many IT managers are caught in the quandary of deciding which technology is best suited for their enterprise. As a result, organizations are often hesitant to deploy or enhance their VPN at the risk of spending money in the "wrong" direction.

Rarely is one of these technologies a perfect fit for the needs of the enterprise's entire population of remote access users. In most cases, the best solution is the deployment of both technologies to meet corporate policies and the varying needs of the end user community.

Juggling both technologies can be an IT manager's nightmare - but doesn't need to be. This white paper looks at how IPsec and SSL can complement each other in the extended enterprise.

II. Which One is Better?

IPsec VPNs encrypt and secure data exchanged between clients or remote networks and an IPsec gateway located at the edge of an organization's enterprise network. SSL VPNs utilize a gateway to protect application-specific tunnels between remote users and resources behind the corporate firewall. In other words, IPsec provides a connection to the entire private network, while SSL VPNs connect users to specific services and applications inside those networks.

The hottest question in the VPN industry for 2003 was "Which one is better - SSL or IPsec?" It went unanswered for a very simple reason - neither is "better" than the other. Perhaps the answer to the question is "It depends". It depends on the user, their reason for access, the device they're using, the breadth of the access you want to give them and other factors. The typical enterprise includes a population of end users with varying needs best met by a complete VPN solution, that is to say, the availability of both IPsec and SSL based access.

IT professionals have implemented countless IPsec VPNs over the past ten years and have watched the SSL VPN market develop for the last three. There's no question that SSL-based VPNs are gaining popularity and being implemented at a higher rate than IPsec. According to Frost & Sullivan, SSL moved from the introductory to growth phase in 2003. The market is driven primarily by organizations with web-enabled applications, as well as the quest for a simpler solution with less client overhead.

META Group predicts that by 2005/06, SSL-based solutions will be the dominant method for remote access, with 80 percent of users utilizing SSL. John Girard, Vice President and Research Director at Gartner projects that in 2004, 60% of corporate users "will use SSL for remote access at least some of the time."

The key is to implement secure, policy-driven management techniques that allow your organization to provide SSL and IPsec based access to the enterprise harmoniously, and in the most efficient manner possible.

In their September 2003 report, Frost & Sullivan ranked Fiberlink partner Neoteris (since acquired by Netscreen) as the industry leader with a 36% market share as of October 2003. Aventail was Neoteris' closest competitor with 10% market share. Gartner ranks these two firms as leaders in their SSL Magic Quadrant, with about twelve other SSL companies following far behind.

Fiberlink's position on "SSL vs. IPSec" is that neither technology is "better" than the other - and that they both have characteristics that provide great advantages to the enterprise. The key is to implement secure, policy-driven management techniques that allow your organization to provide SSL and IPSec based access to the enterprise harmoniously, and in the most efficient manner possible.

Before we go any further, let's first paint a basic picture of the functional differences between IPSec and SSL - and their primary applications.

III. About IPSec

IPSec is a set of VPN protocols that operate at the IP layer and create a private tunnel that makes an enterprise's entire network neighborhood available to the remote user. In an IPSec scenario, a VPN client is required to be installed on the remote user's access device; typically a laptop. Handheld devices are also evolving and becoming more commonplace as VPN remote access devices as they take on greater sophistication and functionality. IPSec provides an end user experience almost identical to that of sitting at a desk in the corporate office with a connection to the LAN.

Some of the reasons that IT administrators and end users prefer IPSec include:

Use of native applications. Users tend to be more comfortable, and often more productive, when applications look, feel, and perform like the original. When applications don't need to be "proxied", performance and ease of use remain at the level to which the user is accustomed. The longer the end user is connected, the more important this becomes.

Some tasks require full network access. In organizations that require a large amount of client and server administration, the IT staff typically prefers the ease of use provided by IPSec. Configuring devices remotely, Telnet access and other functions are better served through IPSec. Note, however, leading SSL appliance vendors provide terminal access features to help meet this requirement.

Being on line is not a requirement for getting work done. When applications are only available during a remote access session, as with an SSL connection, it can cut down on productivity and increase connection costs. For example, personal management applications like Lotus Notes and Microsoft Outlook allow a user to synchronize their in-box, out-box, calendar, etc., when on line - and continue to work when disconnected. A prime example is the road warrior that replicates his or her in-box, takes advantage of time on an airplane to respond to email, and subsequently delivers those messages during the next connection.

IPSec provides an end user experience almost identical to that of sitting at a desk in the corporate office with a connection to the LAN.

IPSec's Pain Points

There's no doubt that IPsec has delivered on its promise to help organizations save money, increase worker mobility, and improve the productivity of remote workers. Just ask anyone that previously used RAS and 800 numbers to deploy remote access before the emergence of virtual private networks.

However, no technology is without its challenges. IPsec can require a high level of client administration - especially when users need to be classified into different groups. Typical IT tasks include policy implementation, application distribution, client software and phonebook updates.

Hardware and software costs can also accumulate quickly. Maintaining client security software and providing corporate access devices (e.g., laptop PCs) are obvious examples.

IPSec Security Issues

While the underlying protocols of IPsec are based on ensuring maximum security, the client basically represents an enterprise network node, which can result in problems if the end point is compromised by a virus, intrusion, or other security threat. Finding a way to easily update client machines with the absolute latest virus protection and personal firewall software - while ensuring that users meet corporate security policies can be difficult to manage.

The objective is to implement an IPsec solution that keeps client management and overhead to a minimum. The updating of security applications and policies must be automated without infringing on end user productivity. Additionally, easily managed policy administration and enforcement is critical to ensuring that corporate mandates are enforced.

IV. About SSL

SSL is a standard Internet protocol for transmitting information via the Internet. SSL allows enterprises to implement application-specific Internet access to network resources from outside the firewall. Special client (or dialer) software is not required. Due to its clientless (or thin client) architecture, it's very easy to offer large groups of users controlled, secure access to the enterprise. End users need only a browser and a web connection to initiate an SSL session. As a result, SSL is often termed the "anywhere/anytime" VPN solution.

Encryption is performed at the application layer and the entire network is not exposed to the end user. In many solutions, access policies can be set at user and group levels, allowing, for example, "Group A" to gain entry to web-based email, while "Group B" has permission rights that allow them to see much of the network.

In the typical scenario, an SSL server acts as a secure, application-layer gateway intermediating requests between the public Internet and internal corporate resources. All requests that enter the server have already been encrypted by the end user's browser via HTTPS 128-bit encryption. Unencrypted

requests are dropped. Each request is subject to administratively defined access control and authorization policies, including dual-factor authentication or client-side digital certificates, before the request is forwarded to internal resources.

As a result, through any Internet-connected Web browser, users can access rich Web-based enterprise applications, Java applications, file shares and access to terminal hosts. And those users with corporate laptops and client/server applications, like Microsoft Outlook and Lotus Notes, can gain application access by enabling proxy through this same, secure Web session.

Why the Market is Interested in SSL

Some of the key drivers behind the significant increase in SSL deployments in 2003 include:

- Deployment of a remote access client is not required - significantly decreasing deployment and maintenance overhead.
- Enterprise access can be delivered to large groups quickly and easily.
- SSL provides a secure solution for granting partners, contractors, telecommuters, etc., access to specific applications and resources without opening up the entire network. Users can be segmented and given access to only the resources you want to give them.
- Enables easy deployment of web-based applications.
- Increases mobility - users have access from virtually anywhere there's an Internet connection, including access from behind other enterprise firewalls and proxy servers.

Challenges of SSL

Many of the challenges of SSL-based VPNs are the mirror opposite of the advantages of IPsec. For example:

- Internet Connection Required. The enterprise's SSL server provides the interface to web-enabled applications. Therefore, an Internet connection is required in order for the end user to be productive.
- Working in an SSL Connection Can Be Confusing. "Webified" applications often do not have the same look and feel as the native version. Performing common tasks, such as working with email attachments can be confusing.

SSL provides a secure solution for granting partners, contractors, telecommuters, etc., access to specific applications and resources without opening up the entire network.

SSL Security Concerns

SSL has been criticized because it enables access through such a wide variety of devices, including those with no corporate management. IT managers are reluctant to allow mobile employees to access network resources from, for example, public Internet kiosks. The fear is that sensitive corporate information may be left behind for others to view. As a result, the leading SSL device vendors have introduced features that tighten endpoint security and erase all activity from un-trusted devices related to the session. If you're evaluating an SSL solution, key security-related feature requirements include:

- Encryption of traffic between the SSL gateway and application servers.
- Decryption of traffic and screening for attacks.
- “Cleansing” of the client machine of any files or other secure data that may be downloaded to the machine during a remote access session.
- Screening of sensitive data, such as cookies and file headers to the SSL gateway.
- Checking the security configuration of the remote machine to ensure it meets corporate policies.
- Masking of the hostname in the URL that is displayed in the browser’s address bar.

What to Look for in an SSL Solution

As mentioned previously, IPSec has been deployed so extensively over the last decade, that most IT managers know what to look for when developing their shortlist of vendors. But due to the relative youth of SSL, the industry has only recently begun to identify the primary benchmarks of a complete SSL solution. In addition to the [security features noted above](#), general features and qualifiers to look for include:

- How extensive is the list of applications supported by the device without needing to push a Java or Active X module to the client?
- Does the platform include options for redundancy and fail-over?
- Does the solution have a successful track record when deployed in a network the size of yours – and can it grow as you grow?
- How much set-up is required - is it easy to administer?
- How much usage data or reporting is available?

V. A Time and a Place

You may be getting a sense by now that neither VPN type is the perfect sole solution. Each has its pros and cons and, in their own way, provides a better fit for different VPN configurations and user types. So what are those times and places? Based on each technology's fundamental characteristics,

IPSec is excellent for organizations that:

- need to support a broad range of applications and provide easy access to the network neighborhood, not just Intranet or email access.
- prefer to provide applications in their native form.
- require administrative control over the end user's PC.
- have corporate guidelines that prohibit the use of non-corporate devices for remotely accessing the network.
- have the resources to administer end users.

SSL is a great fit when:

- Email is the primary resource accessed by mobile workers.
- access from non-corporate devices is often required.
- access is provided to partners, contractors and others who do not need the issuance of a corporate device.
- users frequently need to access the network from behind another firm's firewall.
- maintenance of client software is logistically difficult.

Integrate for Easier Management

If both have their place in satisfying the needs of remote users, how do you offer the two VPN types without doubling IT administrative overhead? The key is to implement an administration framework that takes every opportunity to tie the two solutions together and manage them as one. Fiberlink's next generation remote access platform, Dynamic Network Architecture™ (DNA), allows organizations to utilize a single platform to manage multiple groups of users, regardless of the VPN type. For example, based on your company's "DNA", you can

- Ensure that users authenticate to the enterprise per your corporate security policies.
- Determine the mode of transport that's available to the user (dial, premium broadband, Wi-Fi or all of the above)
- Dictate which VPN type is used for the connection – or let the user choose.

Authentication to the enterprise should be handled through integration with a single external user database, such as RADIUS or LDAP. This is also the case when including two-factor authentication systems, such as RSA SecureID®. Maintaining a separate database for tie-in to each type of VPN gateway is unnecessary and counterproductive.

Should there be a remote access client, such as Fiberlink’s Extend360™, in front of the VPN login, that client should be configured to pass login credentials to the VPN, providing a single logon experience.

End-point security can also be strengthened through tighter integration between the client and the VPN. Two primary examples include:

- The VPN tunnel should instantly be shut down when remote access policies are not met. To ensure as high a level of security as possible, the remote access client should automatically log the user out of the VPN as soon as an infraction is detected – and not wait for the gateway to check the client for adherence to policies. This is especially critical in the case of “always on” broadband connections.
- Ensure that policy enforcement is active and running. In both SSL and IPsec connections, the VPN device should check to ensure that the client is actively enforcing policies, and shut down the session immediately if enforcement is not detected.

Policies and points of integration should be manageable through a web interface to some sort of administrative console provided by your enterprise remote access service provider.

VI. Conclusion

Although some organizations have found themselves in situations where deploying solely SSL or IPsec is satisfactory, chances are that you'll need to support users that want access from trusted and untrusted environments. As a result, neither VPN type may be a perfect fit for your entire population of remote enterprise access users. And while IPsec is a great match for "Group A" and SSL is perfect for "Group B", there's always "Group C", which needs both types in order to be most productive.

The following table outlines several remote access scenarios, and identifies the VPN that provides the best fit for each situation.

Type of Application	Type of PC	Security Level	Type of Connection	Type of VPN
Mobile Employee	Corporate	Managed, Trusted	Mobile	IPsec / SSL*
Mobile Employee	Non-Corporate (home PC/public kiosk)	Unknown, Untrusted	Mobile	SSL
Fixed Telecommuter	Corporate	Managed, Trusted	Fixed	IPsec
Contractor/Partner/ Customer Extranet	Non- Corporate	Unknown, Untrusted	Fixed/Mobile	SSL
RemoteOffice/ Branch Office	Corporate	Managed, Trusted	Fixed	IPsec
Fixed Partner Site to Site	Corporate	Managed, Trusted	Fixed	IPsec

*Consider the account executive, armed with a corporate laptop, who often connects during on-site customer meetings. While utilizing IPsec a majority of the time, SSL helps the user get out from behind another organization's firewall.

Choosing the right solution that enables employees, partners and others to access the enterprise network securely without inhibiting productivity is critical. Luckily, you don't have to choose between SSL and IPsec to get the job done. The objective is to make it easy - easy for IT staff to deploy and manage an integrated VPN solution in unison, and easy for users to connect regardless of who they are, where they are, the device they're using, or the resources they're after.