

Comparing Secure Remote Access Options: IPSec VPNs vs. SSL VPNs

Introduction

Connecting remote users to corporate resources—securely—is not a new problem for IT. But today's end users—with changing work styles, new computing and communication devices and ever-increasing expectations—are driving demand for expanded remote access.

Companies today support full-time remote workers, “day extenders” who supplement office hours by working from a home PC, business partners working from their offices behind their own firewalls, and ad-hoc remote access users who want clientless, broadband, and wi-fi access from anywhere on the road. They all expect easy, clientless access to the network resources they need, from anywhere, at any time, using any device.

Users now access corporate resources from environments that IT can't possibly control—such as home PCs or airport kiosks. Users are also taking advantage of wireless technology, both through the increasing number of public wi-fi hotspots, and also through company-sanctioned wireless LANs and “rogue access points” they've set up on corporate networks. In addition, many companies extend their networks not only to mobile employees but also to trading partners, consultants, and customers around the globe. Both these situations bring security concerns to the forefront.

There are economic factors to consider, too. As companies continue to look for ways to save money, they want to take advantage of the Internet to save over the cost of private leased lines. They want to be able to let home users pay for their own cable modems for connecting to work instead of paying for separate dial-up charges.

Once, traditional Internet Protocol Security (IPSec) Virtual

Private Networks (VPNs) were the only option. Now, a new kind of VPN—SSL VPNs, based on the Secure Sockets Layer (SSL) protocol that secures the world of e-commerce—has emerged as the leading solution for remote access and extranet VPNs. And increasingly, for reasons that are explained in this paper, SSL VPNs are replacing IPSec VPNs for remote access, leaving IPSec VPNs for their original purpose—site-to-site VPNs.

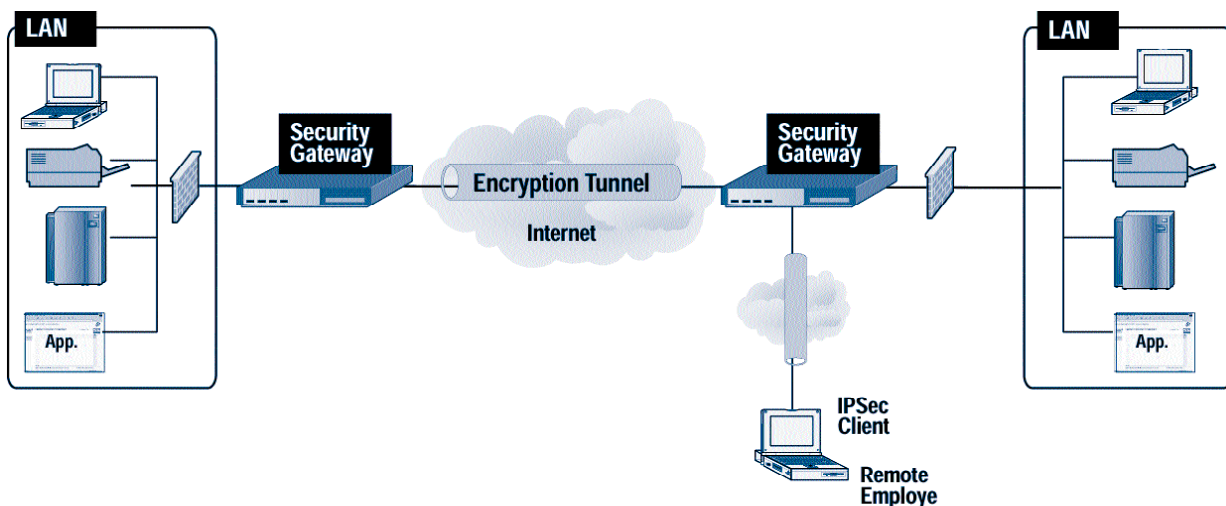
This paper provides an overview of the differences between SSL VPNs and IPSec VPNs, and explains why SSL VPNs are ultimately a better choice for secure remote access and extranets.

IPSec VPNs: Best suited for site-to-site, not remote access and extranets

VPNs, conventionally based on the IPSec protocol and offered by network equipment companies such as Cisco and Nortel, originated to facilitate site-to-site communications between branch offices. As companies broadened their uses to include other remote access needs, proprietary extensions had to be added to the IPSec standard or to vendor implementations of the protocol to address the complexity of adding end-users to the equation.

IPSec works by establishing a “tunnel” over the Internet to connect users outside a corporate firewall or gateway to internal corporate resources. It requires compatible hardware or software, almost always from a single vendor, on both ends of the tunnel. With IPSec, the corporate IT department dictates the technology used on both ends of the tunnel. Few companies are willing or able to mandate the technology their business partners or customers use, and this limits the extranet capabilities of an IPSec VPN.

A typical IPSec VPN provides site-to-site remote access via an encryption tunnel.



As for the remote access market, IPSec satisfies the basic requirements when there are a limited number of tunnels to create. However, when there are thousands of remote users at different locations, distributing and managing the required client software can be cumbersome and costly. These are just some of the many factors that make IPSec VPNs less than ideal for remote access and extranet implementations.

IPSec clients are costly to manage and they add hidden costs

With an IPSec VPN, IT must install and maintain individual VPN clients on each PC from which a user needs access, and changes to the desktop may be required. As a result, support costs will be high.

End-users are mobile, unlike the remote offices for which IPSec VPNs were designed. Users today want to move around freely on different desktops and networks. With IPSec solutions, a client has to be provisioned to each desktop. These clients must be configured differently depending on the environment and networks used. Users who access corporate networks from different places require multiple configurations, generating costly support calls.

With IPSec, if a user doesn't have a pre-provisioned client on her computer, she will be unable to gain access to the resources she needs. That means that today's highly mobile employee who wants remote access from a home computer, an airport kiosk, or any other computer than their own, will either be out of luck entirely, or will need to call the corporate Help Desk to get connected.

For telecommuters or day extenders using their home computers, IPSec VPNs require that corporations provide each employee with a home machine that has the appropriate client software installed, or equip each one with an expensive laptop to take home. If they do neither, the company is stuck with the support costs of helping the user install corporate software on his home computer. In addition, if a user is using DSL or cable modem at home, he may have non-static IP addresses that require configuration changes. Should the user have a firewall set up at home—which is widely viewed as the right thing for broadband users to do—it raises additional barriers to IPSec VPNs. Some IPSec products have difficulty tunneling traffic through a firewall without opening up the correct ports—yet another configuration and security issue on a machine that IT doesn't control.

Security risks for remote access and extranet use

IPSec VPNs can increase security risks because they create a tunnel between two points, providing direct (non-proxied)

access and full visibility to the entire network. Once the tunnel is created, it is as if the user's PC is physically on the corporate LAN and the user can directly access corporate applications. A user may not have access to each server, but he or she will see all that is available, greatly magnifying the security risks. Users working from personal computers at home or through wireless LANs face additional threats from malicious hackers, threats that must be countered by extra security precautions. These personal risks become corporate hacking risks with IPSec VPNs; companies run the risk that hackers can use the remote IPSec VPN network tunnel to gain unauthorized access to the corporate network.

No easy solutions to NAT and firewall traversal

IPSec VPN products and services don't always offer easy solutions to complex remote access situations involving network address translation (NAT), firewall traversal, or broadband access. For example, if a user has an IPSec client on his or her computer, yet is gaining Internet access through another company's network (for example, consultants working at clients' sites), the IPSec will be stopped at that network's firewall, unless the user negotiates opening up another port in the firewall with that company's network administrator. This is a tedious and time-consuming process that also creates a security risk that many companies do not want to take.

The same problem occurs at wireless hotspots. Because many public hotspots use NAT, non-technical users of IPSec solutions are often unable to figure out how to get connected without a call to their support desk and the need for some configuration changes.

Interoperability issues between different IPSec vendors

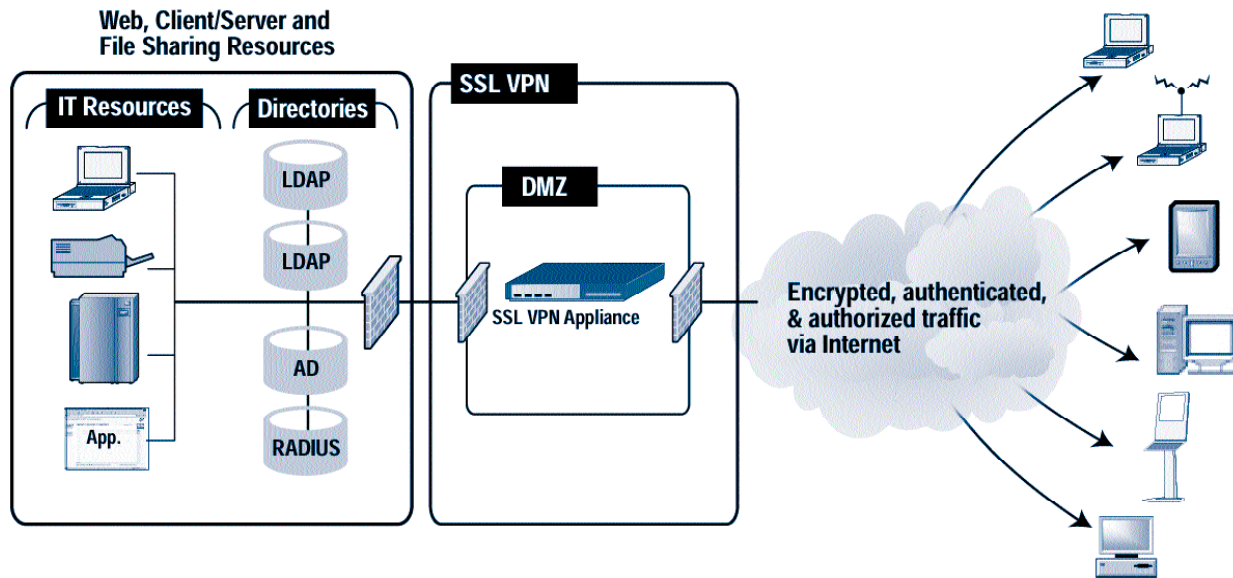
The lack of a standard between different IPSec vendors can create problems for the IT department tasked with setting up a VPN that involves integrating different vendors. An example of this is when the IT department must provide business partner or customer access. Often, complex interoperability and integration hassles delay the process of getting new partners on board quickly.

SSL VPNs: Benefits you can't afford to ignore

Secure Sockets Layer (SSL) has emerged as the leader in the remote access VPN space. Analysts and the press are giving more attention to SSL VPNs than ever before and usage is on the rise.

In fact, John Girard, vice president and research director at

An SSL VPN solution provides secure remote access to corporate resources.



Gartner predicts that, "By year-end 2004, sixty percent of corporate users will regularly use a thin-client VPN, instead of a full, fat-client VPN for access to business data. Compared to IPSec VPNs, thin-client VPNs built on SSL are easier to deploy and support, better for non-managed equipment such as kiosks or home PCs, and are easily portable across emerging mobile and wireless platforms."

In addition, analyst firm Frost & Sullivan estimates that by 2008, SSL VPN sales will exceed USD \$1 billion. The same report directly addresses the cost-savings of an SSL VPN solution, by stating that the average cost per user drops to between \$60 and \$220 when using an SSL remote access VPN versus \$150 to \$300 per user when using an IPSec VPN.

The increasing attention on SSL VPNs does not eliminate the value of traditional IPSec VPN solutions. IPSec is established as the de-facto standard for site-to-site VPNs. If that's all your company requires, IPSec will do the job. If, on the other hand, you need to implement a secure remote access or extranet solution, you should consider an SSL VPN solution, either in addition to, or as a replacement for your IPSec VPN.

What is an SSL VPN?

SSL is a commonly used protocol for managing the security of a message transmission on the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL is a higher-layer security protocol, sitting closer to the application. This close connection to application layers means that, compared to IPSec, SSL can more easily provide the granular access control that remote access and extranet VPNs require.

An SSL VPN uses SSL and proxies to provide authorized and

secure access for end-users to HTTP, client/server, and file sharing resources. Adding proxy technology to SSL offers companies greater security, because it prevents users from making a direct connection into a secured network. SSL VPNs deliver user-level authentication, ensuring that only authorized users have access to the specific resources as allowed by the company's security policy.

A key benefit of choosing an SSL VPN solution is its ability to provide clientless access. Because SSL is included in standard browsers like Microsoft Internet Explorer and Netscape, SSL VPNs such as Aventail's offer a clientless solution—saving the IT departments the headache of installing and managing complex IPSec clients.

One downside of most SSL VPN solutions is that they provide access only to Web applications, while failing to address the needs of companies whose users require access to client/server applications. Many companies rely on legacy or client/server applications by vendors such as SAP or Oracle, so they rule out SSL VPNs or determine that they will only

"By 2005/06, SSL-based solutions will be the dominant method for remote access, with 80% of users utilizing SSL, though IPSec will still be used for specialized applications and user requirements."

— David Thompson,
Senior Research Analyst,
Meta Group

be part of the complete VPN solution they need. But this doesn't have to be the case. Proxy technology enables access to a broader range of application types than SSL alone would provide.

Aventail offers a unique solution that provides secure, anywhere access to any application—including Web, legacy, client/server, file transfer, terminal servers, and mainframe.

Aventail's SSL VPN solution: Setting the standard

Only the leading, most technically advanced SSL VPN providers can deliver full access to client/server and Web applications, as well as file sharing. Aventail's SSL VPN appliances provide this and more. Users get secure, hassle free, but controlled access to a broad range of critical applications and resources including:

- E-mail programs such as Microsoft Exchange and Lotus Notes
- Customer relationship management (CRM) tools such as Siebel
- Business management software such as SAP
- Intranet resources, including custom applications
- Enterprise file servers

Our access agents provide secure access across a wide range of environments, whether the IT organization is managing the desktop or not. For example, for convenient access from desktops that IT does not manage, such as a kiosk, Aventail offers clientless, browser-based access to Web applications and file shares. In addition, Aventail offers the Aventail® OnDemand™ agent, which uses Java to provide seamless secure access to Citrix, Windows Terminal Services, Lotus Notes, and other common client/server or thin-client applications without deploying a traditional VPN client. Finally, Aventail offers our award-winning Aventail® Connect™ client, which sits transparently on the user's desktop to provide an additional means of connecting for situations where IT controls the desktop and broad access to client/server applications is required. Aventail's unique technology makes using non-HTTP applications as easy for users to access as Web applications are.

Aventail sets the standard for SSL VPN solutions by providing clientless “anywhere” access and increased security, making administration easier for IT and simplifying the end users experience when compared to IPSec VPNs.

Clientless access

Without the burden of configuring, managing and supporting complex IPSec clients for each user, SSL VPNs are easier, less expensive to support, and faster to deploy than IPSec VPNs.

And with Aventail technology, clientless access means easy access to more than just Web-based applications. Aventail's clientless solution enables doctors to securely access patient records from any convenient computer, not just their own PC. Sales people and executives can access e-mail and corporate knowledge bases from wireless hotspots or tradeshow kiosks. Users can access Web applications, client/server applications, and enterprise file shares. Without a traditional IPSec client, users gain true freedom and anywhere access to the resources they need. And administrators get secure, controllable access—and fewer support calls.

Anywhere access

SSL VPNs like Aventail's offer users the benefit of “anywhere access.” Users can access their applications from anywhere they have Internet access—from an airport kiosk, from another person's computer, or even using a wireless device. And SSL VPNs work over broadband networks, too. In addition, SSL VPNs can successfully traverse firewalls and can handle network address translation (NAT) issues, which can be problematic with IPSec-based VPNs.

Increased security

Aventail technology provides a secure, proxied connection to resources that the user is authorized to access. As a result, users never have a direct network connection to the resource they are trying to access. In addition, our proxies hide the internal domain name system (DNS) namespace, providing an additional level of protection for your network.

By combining our proxy servers with SSL, Aventail can provide other types of authentication beyond the exchange of digital certificates that SSL allows. Our solution can support Username/Password and two-factor authentication, such as RSA SecurID tokens or digital certificates.

A combined SSL/proxy solution such as Aventail's does a more complete job of securing and managing the connection than either technology could do alone. Aventail's SSL VPN provides data encryption and authentication, granular access control, a single point of management, logging capability, cache control, and a flexible authentication architecture.

Beyond all that, Aventail's End Point Control (EPC) initiative helps organizations control remote access policy not just based on a user's identity, but also on the level of risk in the user's environment. To deliver EPC, Aventail integrates its leading SSL VPN appliances with best-of-breed enforcement partners' firewalls, intrusion detection, virus protection, and other client-side security offerings.

Easy for IT and end users

Ongoing administration is simpler with an SSL VPN than with an IPSec VPN. Because users can securely access

Comparing IPSec VPNs and Leading SSL VPNs

Attributes	Secure Access Option	
	IPSec VPNs	Aventail's SSL VPN
Applications supported:		
Broad client/server support	Yes	Yes
Legacy applications	Yes	Yes
HTTP applications	Yes	Yes
File sharing	Yes	Yes
Mainframe applications	Yes	Yes
Terminal servers	Yes	Yes
Desktop environment:		
Clientless access	No	Yes
Support for wireless devices	Yes	Yes
Java applets activated by session and then turned off	No	Yes
Environments supported:		
Corporate PC	Yes	Yes
From home or hotel with broadband	Varies	Yes
Business partner access	Varies	Yes
From behind another company's firewall	Varies	Yes
From home or friend's PC	Not w/out client	Yes
Public Kiosk or PC	No	Yes
Standard PC on Wireless LAN	Yes	Yes
Wireless PDA	Yes	Yes, varies w/ device type
Security model:		
Proxy protection	No	Yes
Strong user authentication	Proprietary	Yes
Strong central authorization	Limited	Yes
Web single sign-on	No	Yes
Granular access control to URL level	No	Yes
Protection of DNS names and IP addresses	Anyone w/ access to tunnel can see	Yes
Other Key Attributes:		
Cost-effective deployment, configuration, and support	No	Yes
Easy to use and support in any network without reconfiguring	No	Yes
Easy NAT and firewall traversal	No	Yes
Best Fit:		
Site-to-site VPNs: Sharing all network resources with trusted branch offices.	Yes	No
Sharing Web, legacy, and custom applications with users who are mobile and require varying degrees of access, including remote employees, business partners, suppliers, and customers.	No	Yes

applications from any browser, SSL VPNs like Aventail eliminate the administrative headache of distributing and managing VPN clients.

Aventail's SSL VPN solutions require no network changes, no firewall modifications, and no end user configurations. That adds up to a lower TCO than an IPSec solution can deliver.

In addition, Aventail's flexible, object-based policy model is easier on administrators, because—no matter how complex the organizational structure—resources and people only have to be defined one time, and access control rules can describe the desired access policy in one centralized location.

Also, Aventail's solutions work well for business partner and customer access. They provide companies with a high level of security, yet because partners aren't required to add any equipment to their network, SSL VPNs are easier and less intrusive than traditional VPNs in partner environments.

Different from other SSL VPNs: Proven in the enterprise

Aventail, the leading SSL VPN product company, is transforming secure remote access with our broad range of clientless and client-based solutions. Aventail's powerful technology platform accommodates rapidly changing user communities of any scale, giving them the broadest range of application access available. Only Aventail has proven deployments of over 70,000 users. You can purchase Aventail products from leading Value Added Resellers and distributors in 75 countries. Or, you can buy our technology as a fully managed service through any of our global service providers, including top-tier global service providers such as AT&T, IBM Global Services, and Sprint. Only Aventail gives you this choice.

Since the company's inception in 1996, Aventail has focused exclusively on SSL VPNs and providing end-to-end secure access solutions. It has provided SSL-based products and services to more than three-quarters of a million end users and helped more than 600 corporations, including many of the Fortune 500, build and manage their remote access and extranet VPNs. Much of its success has come from tackling the complexities that hinder traditional VPN solutions, such as scalability, end-user simplicity, and strong security.

SSL VPNs: Straightforward solution for remote access and extranets

Whether an SSL VPN is the right choice for a company really depends on the enterprise's needs. Traditional IPSec VPN technology is designed for site-to-site VPNs and does the job quite well. SSL VPN technology, on the other hand, works much better for secure remote access and extranet implementations—offering clientless access, simpler deployment, greater ability to gain access from anywhere, greater security, and easier ongoing administration.

As the SSL VPN market grows, a number of traditional IPSec VPN vendors are blurring the lines by integrating SSL VPN technology in the same appliance as IPSec technology. However, the fact remains that SSL VPNs and IPSec VPNs solve different problems for different users. Therefore, putting SSL VPN technology into an IPSec appliance adds no value as there are no overlapping technologies or components that can be leveraged between the two. Besides, with Aventail's full range of clientless access solutions plus Aventail Connect for full application access, your users already get the best of both worlds: the convenience of our SSL solution and the robust application access comparable to IPSec solutions.

Aventail helps enterprises deliver anywhere access to any application from the broadest range of devices. Our proven security and the breadth of our application support deliver lower costs and increase the productivity of both end-users and IT professionals. Aventail's deep application experience and mature vision for SSL VPN technology make Aventail the market leader.

According to Dave Kosiur, a senior analyst at Burton Group, "SSL VPNs are gaining momentum in the secure access market because of their clientless access, proven security, and ease of management benefits. Aventail has a strong record of success in this market. They continue to lead the way in solving customers' remote access and extranet VPN problems by adding new capabilities that incorporate their field experience in large, complex environments."

