IPSec vs. SSL VPNs for Secure Remote Access

Executive summary

Changing work styles, new computing and communication devices, and the ever-increasing expectations of today's end users are driving the demand for expanded remote access. Many companies today support full-time remote workers, or "day extenders," who supplement office hours by working from a home PC. Business partners work from their offices behind their own firewalls, and remote users want clientless, broadband, and Wi-Fi access from anywhere their travel takes them. They all expect easy, secure access to the network resources they need, from anywhere, at any time, using any device.

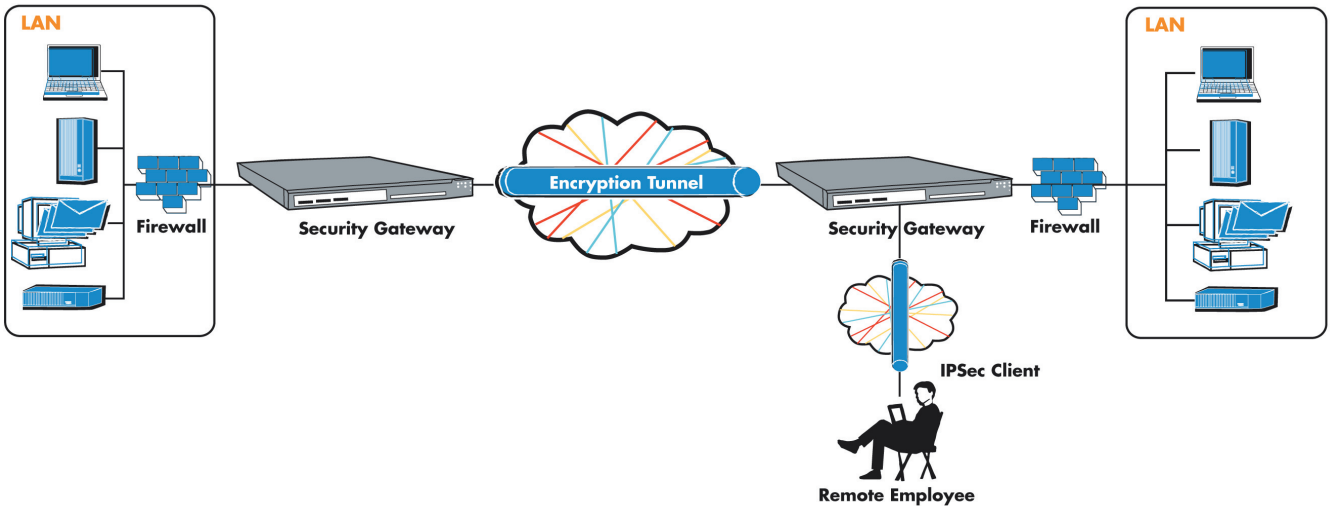
And, today, a greater number of users need access to corporate resources from environments that IT organizations can't possibly control—such as home PCs or airport kiosks. Many users are also taking advantage of wireless technology, both through the increasing number of public Wi-Fi hotspots and through company-sanctioned wireless local area networks (LANs) as well as access points that 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. These new and varied access situations bring security concerns to the forefront.

There are economic factors to consider, too. As companies continue to look for ways to save money, many see advantages in using new technologies such as Voice over Internet Protocol (VoIP) to streamline costs. The rapid expansion and increased availability of broadband access also means that most users are now accessing the corporate network over the Internet from fast broadband connections with near local response times.

At one time, traditional Internet Protocol Security (IPSec) virtual private networks (VPNs) were the only options for secure remote access. However, because IPSec solutions were designed for site-to-site connectivity and not with a highly mobile workforce in mind, these solutions provided limited remote access and often proved both difficult and costly to maintain. In response to increasing user demands for remote access, a new kind of VPN emerged—SSL VPNs. These new VPNs, based on the Secure Sockets Layer (SSL) protocol that safeguards the world of e-commerce, quickly became the leading option for remote access.

And increasingly, SSL VPNs are replacing IPSec VPNs for remote access as they offer everywhere access with complete control and security. In addition, recent advances in SSL VPN technology offer many benefits for both users and companies. When compared to IPSec VPNs, SSL VPNs are less costly to manage, eliminate security risks of open-by-default tunnels, and offer a simpler, easier experience for employees and business partners who need access to a wide range of applications and resources from remote locations.

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.



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

Traditional IPSec VPNs: Designed for site-to-site connectivity

VPNs, initially based on the IPSec protocol and offered by network equipment companies, were originally developed for site-to-site communications between branch offices. These site-to-site VPNs were an economical way to extend the corporate network to remote offices over the public Internet, avoiding the high cost of private wide area network (WAN) connections. The resulting secure connection between trusted private networks offered access similar to that of the corporate network. As companies broadened their use of VPNs to meet 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 individual end users to the remote access equation.

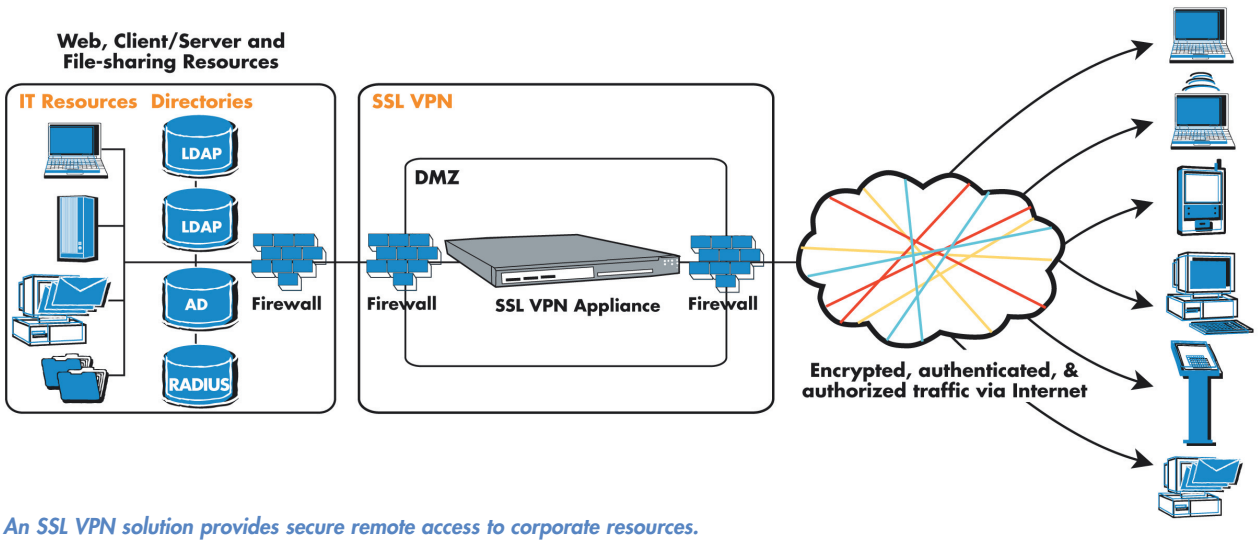
An IPSec VPN works by establishing a tunnel over the Internet to connect users outside a corporate firewall or gateway to internal corporate resources. It requires compatible hardware or software—almost always from a single vendor—on both ends of the tunnel. With IPSec, the corporate IT department dictates the technology used on both ends of the tunnel. Although this may work for systems managed by the IT department, few companies are willing or able to determine and mandate what technology their business partners or customers use. The fact that IPSec VPNs are not suited for access from unmanaged end points and devices limits their ability to connect users to the applications and resources they need.

As for the remote access market, IPSec solutions satisfy user requirements when there are a limited number of tunnels to create and the access scenarios are limited to corporate-managed systems. However, when there are thousands of remote users at different locations, distributing and managing the required client software quickly becomes cumbersome and costly. These are just some of the many factors that make IPSec VPNs less than ideal for remote access.

IPSec clients are costly to manage and have hidden costs

With an IPSec VPN, IT departments must install and maintain individual VPN clients on each PC from which a user needs access; an IPSec VPN may also require changes to the desktop. These factors result in high support costs.

Unlike the workers at branch offices for whom IPSec VPNs were designed, today's end users are mobile. To be productive wherever they are, users need to be able to move freely between different devices such as portable computers, desktop computers, personal digital assistants (PDAs), kiosks, and between multiple networks including ISP broadband, WiFi, customer intranets, and others. With IPSec solutions, a VPN client must be provisioned to each supported system. Because IPSec clients don't support all access points, users cannot get the everywhere access they expect and need. Also, IT departments must configure IPSec clients differently, depending on the environment and



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

networks used. Individuals who access corporate networks from different places require multiple configurations, often increasing the complexity and cost of support.

With IPSec, if a user doesn't have a preprovisioned client on his or her computer, the user will not be able to access the resources needed. That means that today's highly mobile employee who wants remote access from a home computer, an airport kiosk, or any other remote location 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 computer that has the appropriate client software installed or equip each employee with an expensive portable computer to take home. If corporations don't do this, then they must pay the support costs of helping users install corporate software on their home computers. In addition, if using a DSL or cable modem at home, a user may have nonstatic IP addresses that require configuration changes. If the user has a firewall set up at home—which is widely viewed as a necessary safeguard for broadband users—this raises additional barriers to IPSec VPN access. Some IPSec products have difficulty tunneling traffic through a firewall without opening up the correct ports—yet another computer configuration and security issue over which IT departments have no control.

Security risks for remote access

IPSec VPNs can increase security risks. Because they create a tunnel between two points, IPSec VPNs provide direct (nonproxied) access and full visibility to the entire network. After a tunnel is created, it is as if the user's PC is physically on the corporate LAN: The user can directly access corporate applications and resources from his or her remote location. Although the user may not have access to each server, he or she will see all of the applications available, which greatly magnifies the security risks for corporations. Users working from PCs at home or through wireless LANs face additional threats from malicious hackers, viruses, worms, and malware—threats that must be countered by extra security precautions. With IPSec VPNs, these personal risks become corporate security risks; companies face the possibility that hackers will 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 offer no 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 and is accessing the Internet through another company's network (for example, a consultant working at a customer site), the IPSec connection will be stopped at that network's firewall unless the user negotiates the opening of another port in the firewall with that company's

network administrator. Not only is this a tedious and time-consuming process, but it also creates a security risk that many companies may not want to take.

The same problem occurs at wireless hotspots. Because many public hotspots use NAT, nontechnical users of IPSec solutions are often unable to figure out how to get connected and must contact their support staff for help in making configuration changes.

Interoperability issues between different IPSec vendors

The lack of standard technology between different IPSec vendors can create problems for the IT department tasked with setting up a VPN that involves integrating different vendors. For example, if an IT department must provide business partner or customer access, complex interoperability and integration hassles often delay the process.

SSL VPNs: Benefits that you can't afford to ignore

SSL technology has emerged as the technology of choice for remote access. Because of their superior ease of use, high degree of granular control, and proven clientless, secure access to applications, SSL VPNs surpass IPSec VPNs for remote access. Analysts and the press are giving more attention to SSL VPNs than ever before, and SSL VPN usage is on the rise.

John Girard, a vice president and research director at Gartner, says, "Compared to IPSec VPNs, thin-client VPNs built on SSL are easier to deploy and support, better for nonmanaged equipment such as kiosks or home PCs, and are easily portable across emerging mobile and wireless platforms." For that reason, Girard estimates that from 2005 on 60 percent or more of all corporate users will regularly use a thin-client VPN, instead of a full, fat-client VPN for access to business data.

Analyst firm Frost & Sullivan estimates that by 2008, SSL VPN sales will exceed $1 billion (USD). In a Frost & Sullivan report, the firm 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 the $150 to $300 cost per user of using an IPSec VPN.

This increasing recognition of the benefits of SSL VPNs, though, 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 solution to serve an increasingly diverse and mobile user population, 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 the standard protocol for managing the security of message transmission on the Internet. At a high level, it starts with a handshake process initiated by the client. The server responds with a digital certificate, which the client can validate against a trusted Certificate Authority (CA). If successful, the client will use the server's public key in the process of creating a secret key to encrypt and decrypt the rest of the conversation. SSL is a higher-layer security protocol than IPSec, working at the application layer rather than at the network layer. By operating at the application layer, SSL can provide the highly granular policy and access control required for secure remote access. And because SSL is included in all modern browsers, SSL VPNs such as Aventail's offer clientless remote access—saving IT departments the headache of installing and managing complex IPSec clients.

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

Not all SSL VPNs are created equal

One disadvantage of the less functional SSL VPN solutions is that they provide access only to Web applications, failing to address the needs of users who require access to client/server applications. Because many companies rely on legacy or client/server applications by vendors such as SAP or Oracle, they rule out the use of SSL VPNs or determine that they need to use both SSL and IPSec VPNs to meet their remote access needs. This doesn't have

Three critical, integrated components of Aventail® Smart SSL VPNs make secure everywhere application access possible:

- **Aventail® Smart Tunneling™**—is a revolutionary tunneling architecture that provides unparalleled application reach, including support for UDP, TCP, and IP protocols, as well as back-connect applications such as those using voice over Internet protocol (VoIP). Aventail Smart Tunneling offers a Layer 3 tunnel with Layers 4-7 control.
- **Aventail® Smart Access™**—automatically determines and deploys the appropriate access method behind the scenes, providing a seamless experience for end users from any device or end point.
- **Aventail® Smart Policy™**—incorporates cross-platform Aventail® End Point Control™ and a unified policy management model that ensure the highest level of security for managed and unmanaged devices, while also simplifying set up and administration.

to be the case—adding tunneling and port-forwarding capabilities to an SSL VPN enables access to a broader range of application types than SSL alone provides. However, when adding these additional capabilities, many SSL VPN providers ignore one of the true strengths of SSL VPNs—granular access control.

Another shortcoming of most SSL VPN solutions is a segmented, difficult-to-manage policy model that does not scale well. A complex policy model not only requires unnecessary work to manage, but it also opens the door to shortcuts and mistakes that may compromise security. In addition, it can throw off the balance between mitigation of risk and business requirements, because the technology imposes artificial constraints that either limit access options and usability for the sake of strict security, or that compromise security to accommodate a wider range of access methods, locations, and devices.

Aventail offers a unique solution—the Aventail® Smart SSL VPN—which provides secure, everywhere access to any application or resource, including Web, legacy, client/server, back-connect, and file transfer applications, as well as terminal servers and mainframe computers. For IT departments and end users, the Smart SSL VPN provides granular control and ease of use for the highest level of security, manageability, and productivity available in any VPN solution.

The Aventail Smart SSL VPN solution: Setting the standard

Only the leading, most technically advanced SSL VPN providers can deliver full access to client/server applications, Web applications, and file shares. Aventail Smart SSL VPN appliances provide this and more. Pioneering new technologies that extend the capabilities of SSL VPNs, Aventail SSL VPNs rely on three critical, integrated components to deliver on the promise of secure everywhere access—Aventail® Smart Access™, Aventail® Smart Policy™, and Aventail® Smart Tunneling™. The result is a cost-effective, next-generation VPN that gives administrators the most secure, easy-to-deploy and -manage VPN available. Users get hassle-free yet controlled access to the broadest range of advanced 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.
- Internet telephony applications that require a back connection such as VoIP.
- Streaming and conferencing applications.
- Remote management and control applications.
- Enterprise file servers.

Aventail sets the standard for SSL VPN solutions by providing clientless everywhere access with complete policy control, increased security, and seamless traversal of complex network environments. And Aventail solutions make administration easier for IT departments and simplify the end user experience when compared to traditional IPSec and other SSL VPNs.

Flexible access meets diverse needs

Aventail's Smart Access methods automatically deliver the right level of access across a wide range of access environments to provide easy, secure access—whether the

IT organization manages the end device used or not. For example, for convenient access from desktops that an IT organization does not manage, such as a kiosk, Aventail offers Aventail® WorkPlace for clientless, browser-based access to Web applications and file shares. For additional access through WorkPlace, Aventail offers Aventail® OnDemand™, which provides seamless secure access to Citrix, Microsoft Windows Terminal Services, Lotus Notes, and other common client/server or thin-client applications, without requiring a traditional VPN client. Finally, for situations where IT departments control the desktop, Aventail offers its award-winning Aventail® Connect™ client, which sits transparently on the user's desktop and provides complete access to all network applications and resources. Aventail's unique technology gives users an "in office" experience while also offering companies a high level of centralized access control.

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

And with Aventail's SSL VPN technology, clientless access means easy access to the applications that users need to be productive. For example, Aventail's clientless solution allows doctors to securely access patient records from any convenient computer—not just from their own PCs. Salespeople and executives can access e-mail and corporate knowledge bases from wireless hotspots or tradeshow kiosks. Road warriors can take advantage of VoIP. Without a traditional IPSec client, users gain true freedom and everywhere access to all the resources they need. And administrators get secure, controllable access—and fewer support calls.

Everywhere access

With an Aventail Smart SSL VPN, users can access their applications from wherever they have Internet access—from an airport kiosk, from another person's computer, or even by using a wireless device. SSL VPNs work over broadband networks, too. In addition, SSL VPNs can successfully traverse firewalls and can handle NAT issues, which are problematic with IPSec VPNs.

By dynamically adapting to the access environment, Aventail SSL VPNs go further than other VPN solutions to deliver the promise of everywhere access. Aventail's patent-pending Smart Tunneling technology implements a full IP tunnel over SSL, transparently extending universal access to all applications, including back-connect applications and those requiring bidirectional control. This unique ability to extend application reach over SSL allows support for such applications as VoIP; various streaming, conferencing, and collaboration applications; and remote management and control applications.

Increased security

Aventail technology provides a secure, proxied connection to all 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. Aventail proxies also hide the internal domain name system (DNS) namespace, providing an additional level of protection for your network.

In addition to a proxied connection, Aventail provides multiple options for authentication, including support for Username/Password and two-factor authentication, such as RSA SecurID tokens and client-based digital certificates.

A key component of the Aventail SSL VPN is Aventail's End Point Control (EPC) initiative, which helps organizations control remote access policy based not only on a user's identity, but also on the level of risk in the user's environment. Aventail's cross-platform EPC supports the widest range of systems, enabling access from Windows, Macintosh, and Linux devices. Aventail appliances also integrate with best-of-breed technology partners' firewalls, intrusion detection, virus protection, and other client-side security offerings, thereby ensuring complete end-to-end security.

By extending its SSL VPN with Smart Tunneling technology, Aventail goes beyond combining SSL technology and the option of a proxy, like other SSL VPNs do. As a result, Aventail SSL VPNs do a more complete job of securing and managing the connection than other technologies. Along with Smart Tunneling, Aventail Smart Policy and Smart Access make the Aventail SSL VPN the most complete solution available for secure remote access. Aventail VPN technology provides secure everywhere access by using data encryption and authentication, granular access control, a single point of management, logging capability, cache control, a flexible authentication architecture, and more—delivering remote users the

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 a friend's PC	Not without client	Yes
Public kiosk or PC	No	Yes
Standard PC on a wireless LAN	Yes	Yes
Wireless PDA	Yes	Yes, varies with 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 with 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

appropriate access to resources from any location or access environment.

Easy for IT departments and end users

Ongoing administration is simpler with an SSL VPN than with an IPSec VPN. Because users can securely access applications from any browser, SSL VPNs like those from Aventail eliminate the administrative headache of distributing and managing VPN clients. Aventail Smart Access expands this ease-of-use advantage by seamlessly delivering the right method of access according to policy and the end-user environment.

Users needing Web access from unmanaged systems can use the customized Aventail WorkPlace portal to gain everywhere access to Web applications, client/server applications, or other resources. Smart Access determines what resources the user is allowed to access from his or her current environment and displays the available options. Users running managed Windows systems can use the Aventail Connect Tunnel for full network access with the greatest ease of use. The lightweight Aventail Connect client is deployed through the Aventail WorkPlace portal. After it is installed, the client automatically updates itself without intervention and can either be run manually or set to run at startup or at application launch. With Aventail Smart Access, IT administrators set the policy, and Smart Access takes care of the rest.

Aventail SSL VPN solutions use the advanced capabilities of Smart Tunneling to streamline remote access, automatically adapting to network conditions in complex and diverse environments. Adaptive routing and adaptive addressing dynamically and transparently negotiate network obstacles that limit remote access in other VPNs. Aventail Smart SSL VPNs require no network changes, no firewall modifications, and no end-user configurations. That adds up to a lower total cost of ownership than an IPSec solution can deliver.

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

Aventail's solutions are also ideally suited for business partner and customer access. These solutions provide companies with the granular policy control they need to tailor access according to the varying business requirements of those relationships with a high level of security. Yet because partners aren't required to add any equipment to their network, install software, or make special configuration changes, Aventail Smart SSL VPNs are easier and less intrusive than other 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 the company's integrated clientless and client-based solutions. Aventail's powerful Smart SSL VPN technology accommodates rapidly changing user communities of any scale, giving them the broadest range of application access available. Only Aventail has proven deployments of more than 70,000 users. To provide the widest range of purchasing options, Aventail offers its full product family through leading value added resellers and distributors in 75 countries. Customers also have the option of purchasing an Aventail SSL VPN as a fully managed service through any of Aventail's global service provider partners.

Since the company's inception in 1996, Aventail has focused exclusively on SSL VPN technology and providing end-to-end secure access solutions. It has provided SSL-based products and services to over1 million end users and helped hundreds of corporations, including many of the Fortune 500, build and manage their remote access VPNs. Much of Aventail's success has come from tackling the complexities that hinder traditional VPN solutions, such as scalability, manageability, end-user simplicity, and strong security.

Aventail Smart SSL VPNs: The most complete solutions for remote access

Whether an SSL VPN is the right choice for a company really depends on the company's needs. Traditional IPSec VPN technology is designed for site-to-site VPNs and does the job quite well, if that is the primary need of a company. SSL VPN technology, on the other hand, works much better for secure remote access—offering clientless access, simpler deployment, and the opportunity to deliver everywhere access with greater security and easier ongoing administration.

With Aventail's clientless access options and the Aventail Connect client for full application reach, your users can get the best of both worlds: the unparalleled convenience of Aventail's Smart SSL VPN solution and robust application access that is comparable to, and exceeds, IPSec solutions. For remote access, the Aventail Smart SSL VPN is an ideal replacement for other incomplete SSL VPNs and IPSec VPNs, extending SSL VPN technology to provide a single solution for access to all network applications and resources with complete control, complete security, and unmatched ease of use.

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

Dave Kosiur, a senior analyst at Burton Group, sums up the Aventail advantage: "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."

Aventail
More secure. More access. It's that simple.

WP 4010 0605/4

Corporate Headquarters
808 Howell Street
Seattle, WA 98101
Tel 206.215.1111
Fax 206.215.1120
www.aventail.com

Aventail Europe Ltd
Tel +44 (0) 870.240.4499
emea@aventail.com

Aventail Asia-Pacific
Tel +65 6832.5947
asiapac@aventail.com