Challenging the Myth of IPSec Security

How SSL VPNs deliver more secure remote access than IPSec VPNs

Aventail

Executive summary

Your users are asking for remote access—and not just the mobile users and telecommuters in your own company, but also your trading partners and customers. Enabling more users to connect from more locations, using a variety of devices can increase productivity; it can also increase the risk of exposing your network to malicious attack.

Both IPSec VPNs and SSL VPNs can deliver secure remote access. But before buying one of these technologies for remote access, you need to make sure you're using criteria that reflect the challenges posed by these new users, devices, and locations.

These new criteria include:

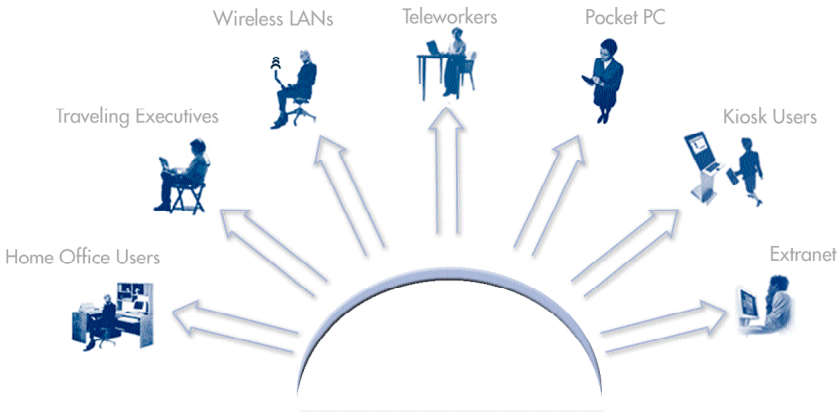
- **Environment detection:** the ability to determine how secure the user's environment is before granting access to corporate resources.
- **Ongoing protection:** monitoring the session to ensure that it remains secure and removing sensitive data from the remote device when the session ends.
- **Authorization:** allowing or denying access to resources based not only on the user's identity but also based on the security of their current environment.

This paper compares IPSec and SSL VPN capabilities in these three areas. Among the findings are these key points:

- Leading SSL VPNs like Aventail's offer strong host integrity checking and application detection, to ensure that virus protection and firewalls are running—and that malicious programs are not—before determining what access to provide.
- Leading SSL VPNs like Aventail's keep sensitive information that may be stored on the remote device safe by encrypting it during the session and permanently destroying it when the session ends, making SSL VPN access safer than IPSec VPN access.
- IPSec tunnels expose too much information about your network, even if user authorization is required to access resources. SSL VPNs never allow a direct connection to resources, and redirect all unauthorized traffic.
- Application awareness and the ability to detect the user's environment allow SSL VPNs to provide superior authorization control—based not only on the user's identity, but also on the user's environment. And, SSL VPNs offer the added benefit of low management and support costs.
- Leading SSL VPNs like Aventail's deliver functionality for environment detection, ongoing protection, and authorization, which are required for secure remote access. IPSec VPNs offer this functionality in limited fashion or not at all.

In summary, for remote access, SSL VPNs deliver the flexibility to meet a greater variety of business needs while providing stronger security than IPSec. And they do so while reducing administration and support costs compared to IPSec. Aventail, the pioneer in SSL VPNs, provides the strongest functionality in areas critical to secure remote access today. Industry experts and customers have recognized Aventail for its leading SSL VPN technology.

More users are demanding secure remote access from more locations than ever before.



The challenge: access vs. security

Providing secure remote access to network resources and corporate information continues to be a challenge. Two opposing forces are creating this challenge: the expanding need for remote access and the necessity of improving control over the network.

Users demand access to networked resources

With broadband available to many homes and hotels, and Wi-Fi offered in more coffee shops and airports, employees want the convenience of connecting any time, from whatever device is at hand. When you make information easily accessible, employees use it to win more business, provide customers with superior service, and extend productivity.

You need to protect your network

Worms, viruses, and a host of other inventive and invasive programs have exponentially increased the need to identify, evaluate, and inoculate every device that connects to the network. To complicate matters, users increasingly request remote access from devices that your corporate IT department doesn't control—such as home PCs, kiosks, PDAs, and trading partner PCs.

Responding to the challenge

One possible response to this challenge is to lock down the network and allow no access. If there is no access from external devices, the network is far easier to secure. But this position denies the advantages of improved employee productivity and streamlined customer and partner interactions. Besides, this "no access" stance is unrealistic, considering how people work today. Users with laptops and other devices expect to move freely, gaining wired and wireless access both inside and outside the corporate network.

There is a way to meet the challenge. Traditionally, companies have used VPNs based on IPSec (Internet Protocol Security) to extend the network. Today, Secure Sockets Layer (SSL) VPNs provide a strong alternative. Both enable strong authentication and encryption. But when you apply these two security technologies to remote access use cases, SSL VPNs stand out as more secure, more flexible, easier to use, less expensive, and more scalable for enterprise environments.

Let's examine each technology.

IPSec VPNs

IPSec refers to a set of protocols that provide encryption and authentication at the IP layer. The Internet Engineering Task Force (IETF) designed IPSec as a solution for site-to-site secure communications. Applying both encryption and authentication, IPSec creates a "tunnel" between the two sites, transmitting all packets without regard to their purpose or content. All resource names are visible on both ends of the tunnel. This provides visibility into your entire network, and access to all the networked resources and applications the user normally has access to, regardless of the user's location or environment.

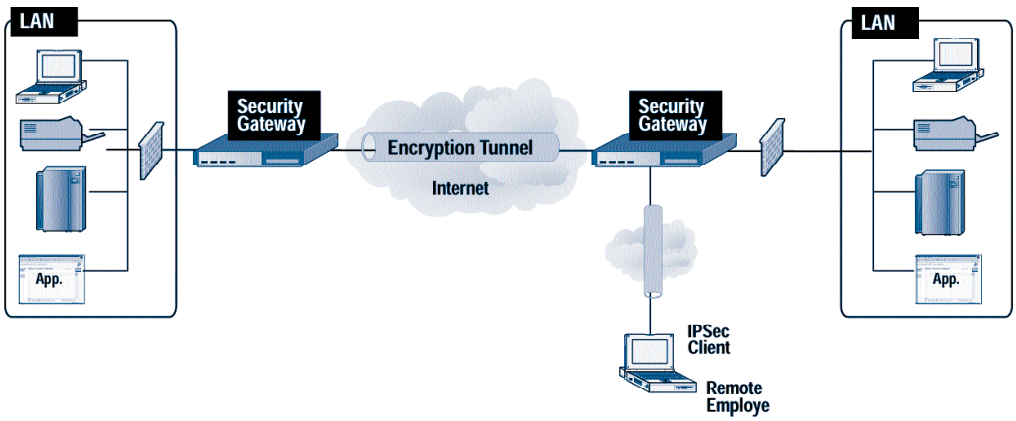
IPSec enables high-speed communication, well suited for site-to-site communications where high throughput without restriction is critical and IP addresses are static. With IPSec, both sites must be under IT control so that compatible software can be installed, configured, and maintained at each end of the VPN tunnel.

IPSec VPNs require an IT-installed and configured client on the remote device. Having the remote device under IT control before it connects makes sense for securing site-to-site connections. For remote access, however, the assumption of IT control is often not true—which opens the network to attack and compromises data security.

Limitations of IPSec for employee remote access

As an example, consider the home PC. Home PCs are generally not company-owned, and are not under your control. That makes it difficult to determine the integrity of the PC and its contents, as well as its IP address. And even for company-owned laptops control is not totally assured. Employees may disable personal firewalls or antivirus software because as those programs do their job, they cause interruptions in other tasks.

A typical IPSec VPN provides remote access via an encryption tunnel that transmits all traffic.



IPSec for extranet access: You don't control both ends of the VPN tunnel

For non-employee access by trading partners or customers via an extranet, you would need to coordinate IPSec clients and configurations across organizational boundaries. With every trading partner serving multiple customers, finding a single VPN client to use as a standard becomes impossible. IPSec clients are often incompatible with each other, making it impractical to install multiple clients on a single PC. And if you could install two IPSec clients successfully, whose help desk would support it?

Design considerations necessary for going beyond a site-to-site use case

When customers, trading partners, consultants working onsite at a customer, or even some home users need to connect from behind a firewall, IPSec VPNs require that ports be opened in the firewall to allow traffic through. In addition, Network Address Translation (NAT) can be problematic with an IPSec VPN.

The creators of IPSec did not have remote access use cases in the scope of their original design. IETF has not yet finalized all the standards necessary for IPSec protocols to meet Public Key Infrastructure (PKI) and other remote access needs, forcing IPSec VPN vendors to create proprietary extensions to the basic protocols, resulting in products that don't interoperate.

SSL VPNs

SSL is a protocol originally developed to enable secure message transmission over the Internet. It creates an authenticated, encrypted end-to-end link between a Web browser and a Web server over which HTTP or any other application protocol (such as SMTP, LDAP, POP, IMAP, or TELNET) operates. Working at the transport layer, SSL is more application-aware than IPSec, so it can establish secure connections for specific applications rather than just passing all packets through the VPN tunnel.

The standard for Internet security

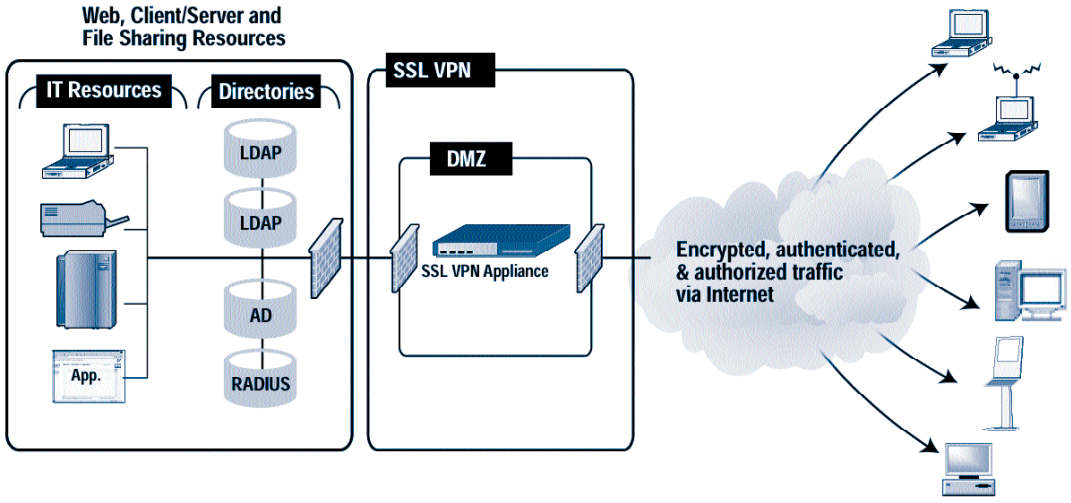
The security standard for the Internet, SSL protects over $50B in e-commerce transactions a year, and is supported by all of the most widely used browsers, Web servers, and Open Source software. Because it was developed for Internet use, it was designed with firewalls, gateways, NAT, and PKI in mind.

By design, SSL VPNs make it simple for users to connect securely to appropriate resources; for example, by automatically navigating firewalls and NAT, SSL VPNs significantly reduce help desk costs. SSL VPNs also lower support and maintenance costs because they are clientless—meaning that you avoid installation, updating, and configuration issues.

Some security administrators may view SSL VPNs as less secure than IPSec VPNs, since remote devices do not need to be under IT control with an SSL VPN. That works for site-to-site, when you control both ends of the network.

But when you need to extend remote access to devices beyond your network and beyond your control, which technology delivers the strongest security?

An SSL VPN solution provides authorized remote access to specific corporate resources.



New criteria for evaluating remote access technologies

The clash of expanded remote access requirements and the growing list of security issues that result, demands new criteria for evaluating VPN solutions. It's no longer sufficient to compare checklists of authentication and encryption methods supported by each VPN solution. Both typically support DES, 3DES, RC4, MD5, and SHA encryption methods. They both support server- and client-side digital certificates, hard and soft tokens, two-factor authentication, Username/Password, RADIUS, LDAP, and Active Directory. While important, this information is no longer enough to base a remote access technology decision on.

Three new ways to look at secure remote access

For remote access, we need to look at three additional criteria in order to find out which technology best addresses the needs:

- **Environment detection:** Before allowing remote access to corporate resources, the technology needs to determine how secure the user's environment (or "end point") is. Detecting the user's environment allows you to make intelligent decisions about allowing or denying access, and about what resources to enable access to from a given device and location.
- **Ongoing protection:** Once a session is established, the connection and the end point need continuous monitoring to ensure that the session remains secure. And at the end of the session, all sensitive data must be removed from the device so that other users can't steal it or use it to gain entry to your network.
- **Authorization:** The technology needs to provide fine-grained authorization for users at different times and locations. Users should be granted access only to specific applications, based on their current environment. The "one size fits all" access granted by IPSec is inadequate for the variety of remote access situations that companies face.

Let's compare IPSec and SSL VPNs in each of the three areas.

Environment detection

Some IPSec VPN clients now include the ability to detect some aspects of the user's environment, including the presence of virus detection and personal firewall software. This capability is dependent upon the vendor's proprietary software being installed, appropriately configured, and operating. If the client isn't installed or the user can't get it to work, perhaps because

Attribute	*IPSec VPNs*	*Leading SSL VPNs*
Environment Detection		
Detects user's environment to determine access rights	No	Yes
Host integrity checking	Some	Yes
Application detection with digital certificate support	Some	Yes
Dynamically traverses firewalls, NAT, proxy services	No	Yes
Ongoing Protection		
Cleans cache, cookies, passwords, and URLs, browser history, and downloaded files automatically when session ends	No	Yes
Controls connections by time of day	Some	Yes
Integrated proxy to hide internal DNS names and IP addresses	No	Yes
Monitors end point for continued virus, firewall protection; disconnects if problems	Some	Yes
Split tunneling control	Some	Yes
Automatic client updates for policy or access changes	Some	Yes
Authorization		
Provides specific access privileges based on user environment	No	Yes
Access by user, group, resource, application, protocol, time of day, source IP	No	Yes

of a firewall configuration issue, no access is possible. This is great for security, but impractical for mobile access, home users, and extranet users.

Controlled clientless access

SSL VPNs provide a secure clientless connection to specific corporate applications and resources, such as extranets and e-mail, ideal for kiosk, home, or non-employee users. Because the access provided with SSL VPNs is so granular in nature, it is often even safer than connecting with a corporate laptop that has an IPSec client.

Securing the remote device

Leading SSL VPNs, designed for mobile use on a variety of devices you don't control, offer:

- Host integrity checking to ensure that no spyware or other malicious programs are running on the user's machine.
- Application detection to ensure that virus protection and personal firewalls are installed and running.
- Digital certificates to ensure that applications on both sides are from trusted sources.
- Microsoft Authenticode to eliminate risk of application spoofing.

Easy connections and lower costs

SSL VPNs make it easier for users to establish connections compared to IPSec VPNs, since SSL deals with proxy configuration changes, firewalls, and NAT automatically. This greatly reduces support costs for remote access.

Ongoing protection

Your corporate data and network infrastructure needs to be protected from unauthorized use during and after the session. Kiosks and home PCs are a major concern because they're shared, and even corporate laptops are sometimes used in environments outside of IT control.

Continuous monitoring

The best VPN technology for remote access monitors the end point continuously and disconnects if the status changes in a way that no longer complies with your security policy. Examples include monitoring the end point to ensure that the virus checker or personal firewall is still running, and that no spyware or other intrusive applications have been started.

Split tunneling control

Another aspect of ongoing protection, split tunneling control ensures that no other connections to unauthorized networks are opened during the VPN session. An IPSec VPN without split tunneling control lets users open non-secured Internet sessions while using a wide-open IPSec tunnel to your network, providing a superhighway for hackers and malicious programs to attack.

SSL VPNs also employ split tunneling control. In addition, SSL VPNs establish a secure connection to a specific application, redirecting unauthorized traffic and keeping the session secure.

No direct connections

By design, IPSec VPNs expose all resource names and provides a direct connection them, revealing all your network resources to everyone, friend or foe. But combining proxy services with SSL VPNs eliminates dangerous direct connections to network resources. The proxy hides DNS namespace using aliasing, providing an additional level of protection.

Removal of sensitive data

The degree of IT control assumed with IPSec VPNs also leads to the conclusion that sensitive data on the remote device is safe. In reality, with users today accessing from places IT can't possibly control such as public kiosks, you need a way to ensure that corporate data is safe. Many clientless SSL VPNs address this through some sort of cache cleaning support.

Aventail® Cache Control™ goes farther, cleaning the cache, cookies, auto-completed or stored passwords, URLs, browser history, viewed e-mail attachments, and downloaded files from the remote device automatically at session end. And if the user forgets to log out or close the browser, it automatically ends a session. Aventail® Secure Desktop™ delivers an even higher level of protection, by creating an "encrypted vault" to safely store all data downloaded in a Web session and permanently destroy it at the end of the session.

Ease of maintenance and upgrades

When hardware, software, or policy updates are needed to close gaps or improve security, your network may be vulnerable or inaccessible to remote users until you make the changes across all devices. IPSec client software often requires manual intervention to get updates installed and working correctly in spite of automated software update tools. Meanwhile, the user has no access to needed resources.

Clientless SSL VPNs are built to accommodate mobile workforces and trading partners. With no client to upgrade or configure, SSL VPNs allow business to continue, safely, regardless of infrastructure changes.

Authorization

For remote access, the ability to grant access only to specific applications, based on a user's current environment becomes critical. SSL VPNs and IPSec VPNs differ in the amount of control they offer in this area.

IPSec VPNs, working at the network layer, establish a tunnel through which all resources on the network are exposed to all users, with their real identifiers. This level of access is inappropriate for partners, customers, or anyone using a shared PC. While you may have additional authorizations applied to specific resources, exposing this information certainly removes a big obstacle for hackers.

Since SSL VPNs work at the transport layer, they discriminate between different types of applications and resources. When combined with the ability to detect the user's environment, you now have unprecedented control over which applications and resources are accessible, based on the user's situation. You can provide different levels of authorization if the user is currently at home, using a public kiosk, or using a corporate laptop with VPN client software. This distinction is *critical*. Further, SSL VPNs like Aventail's let you authorize access by source network, application, time of day, and other granular variables.

Using IPSec VPNs, security policy definition can provide some level of access control, but only SSL VPNs deliver the power to secure your network at a highly granular level and the flexibility to give users the access they demand.

Aventail delivers superior security and flexibility

There are many SSL VPN vendors out there to choose from. On the surface they look similar, but significant differences exist.

Aventail's award-winning SSL VPNs result from both its pioneering efforts and its ongoing investment in SSL VPN technology. Aventail developed the first SSL VPN in 1997. Today, Aventail is advancing the technology with more resources focused on SSL VPN research and development than any other company.

Aventail delivers environment detection and ongoing protection through its End Point Control and proxy capabilities. Aventail End Point Control and advanced policy management provide superior authorization control. These capabilities are deployed to meet the expanding demands for remote access via Aventail's comprehensive access options.

Aventail® End Point Control™

To detect and secure environments that are not under IT control, Aventail integrates its leading SSL VPN appliances with best-of-breed enforcement partners' firewall, intrusion detection, virus protection, host integrity checking, and other client-side security offerings. Aventail's application detection, split tunneling control, and advanced data protection features—Aventail Cache Control and Aventail Secure Desktop—make every environment more secure. Aventail solutions provide the power to enforce policy based upon the level of trust for the user's environment, not just the level of trust for the user.

Policy management

With Aventail technology, access to applications and resources can be authorized by any combination of source or destination network, application, time of day, protocol (including UDP), resource (file shares, network drives, and printers), and service or port (such as FTP, HTTP, Telnet). Users see only what is appropriate based on a combination of identity, environment, and time, to provide the strongest security in any setting.

Aventail's unique object-based policy model is scalable, easy to set up and maintain, and cost-effective to administer. Using the Aventail® ASAP™ Management Console (AMC), it's simple to create and maintain fine-grained access controls that keep security strong while allowing optimum access for remote users.

Comprehensive access options

Aventail provides three options to securely address the broadest range of business requirements:

- Browser-based access, for Web application and file share access.
- Aventail® OnDemand™, a Web-delivered Java SSL VPN agent for secure client/server application access, including access to Citrix, Windows Terminal Services, and Lotus Notes.
- Aventail® Connect™, a Web-deployed Windows SSL VPN client for full secure access to network resources from corporate laptops.

These options work seamlessly together to enable users to access important information, while providing security administrators the control they need to protect their networks. And by improving usability and significantly easing deployment issues, you reduce support and maintenance costs.

Proven performance

Aventail delivers secure SSL VPN solutions that serve nearly a million users globally. Aventail is the preferred partner for companies where secure remote access to information provides a key competitive edge.

Conclusion: Aventail's SSL VPNs meet the challenge

SSL delivers stronger security for remote access VPNs by directly addressing the assumptions and limitations inherent in IPSec. IPSec simply exposes too much of your network. Its requirement for client software leads to dangerous assumptions and is impractical for trading partners, customers, and today's highly mobile workforce.

Designed for remote access, Aventail's SSL VPNs give you more granular access control and more confidence in securing remote environments, allowing you to safely expand remote access to new users and new locations to satisfy business needs.

Industry analysts and Aventail customers agree: Aventail's superior combination of multiple access options, granular policy management, and End Point Control deliver the best secure access for your organization's needs, and lets you expand remote access without increasing costs. And Aventail's expertise and vision make it the ideal partner to help you meet tomorrow's secure access challenges.

Aventail: the leading SSL VPN product company

Aventail is the leading SSL VPN product company and the authority on clientless anywhere secure access. Aventail's appliances and managed services deliver secure, seamless access from anywhere, to any application, on any device. With the most widely deployed SSL VPN on the market, Aventail is positioned in the Leader quadrant in Gartner's 2004 SSL VPN Magic Quadrant and was recently awarded "Best VPN" by *SC Magazine*. Major service providers such as AT&T, IBM Global Services, MCI, Sprint, SITA SC, and Bell Canada have built their SSL VPN managed service businesses on Aventail's technology. To find out what Aventail customers like Aetna, DuPont, Office Depot, Sanyo, and TNT already know about Aventail's SSL VPN, go to www.aventail.com.

Aventail

WP-4088-0804/1

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