

SSL VPNs: Benefits you can't afford to ignore

Secure Sockets Layer (SSL), the protocol that secures the world of e-commerce, is now emerging as the leader in the 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 Gartner predicts that, "By year-end 2004, 60 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."

And, according to a new Infonetics Research report titled "VPN and Firewall Products," by the end of 2005, sales of SSL VPN products will reach \$871 million.

So does all this hype about SSL mean companies should forget about traditional IPsec VPN solutions? Not necessarily. IPsec is established as the de-facto standard for site-to-site VPNs. If that's what your company

requires, IPsec will do the job well. If, on the other hand, you are looking to implement a secure remote access or extranet solution, you'll want to consider an SSL VPN solution, either in addition to, or as a replacement for your IPsec VPN.

The appeal of anywhere access, proven security, easy deployment, and simpler administration

SSL VPNs offer users the benefit of "anywhere access." Because SSL is included in standard browsers like Microsoft Internet Explorer and Netscape, SSL VPNs offer the possibility of a clientless solution. 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.

SSL, a commonly used protocol for securing messages and transactions over the Internet, includes client and server authentication and data encryption for Web-based applications. It is a higher-layer security protocol, sitting closer to the application, which means that compared to IPsec, it can more easily provide the granular access control that remote access and extranet VPNs require. SSL VPNs

deliver user-level authentication, ensuring that the right people have access only to the right resources.

Ongoing administration is simpler with an SSL VPN than with an IPsec VPN. Because users can securely access Web-based applications from any browser, SSL VPNs eliminate the administrative headache of distributing and managing VPN clients. Also, SSL-based VPNs 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.

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

Two kinds of VPNs

IPSec VPNs

- Connecting
 - branch offices, data center
- Site-to-Site
 - LAN to LAN
- Gives full network access
- Expensive to deploy and support IPsec clients

SSL VPNs

- Connecting
 - mobile users & commuters
 - partners, vendors, & customers
- From anywhere to any resource
- Clientless access
- Granular access control
- Increased security

"By year-end 2004, 60% of corporate users will regularly use a thin-client VPN."

—John Girard, Gartner (Sept. '02)

rely on legacy or client/server applications such as SAP or Oracle applications, so they rule out SSL VPNs or determine that they will only be part of the complete VPN solution they need. But this doesn't have to be the case.

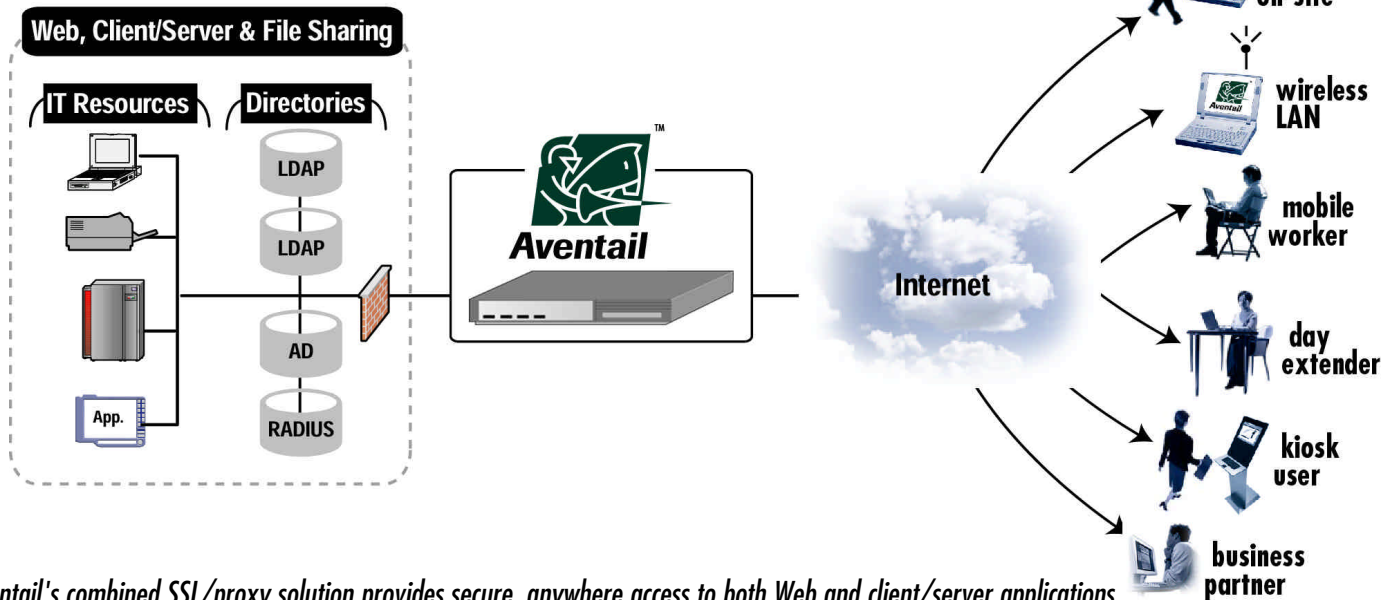
Adding proxy technology improves security

Some vendors combine SSL with proxies to help overcome some of the shortcomings of using SSL alone. Aventail, for example, offers a combined SSL/proxy approach. One of the key benefits of this approach is the ability to provide secure access to both Web and client/server applications. To do so, Aventail uses two different types of proxy technology. For Web-based applications, Aventail creates a secure Web gateway integrating HTTP reverse proxies. For any non-Web traffic, Aventail uses the SOCKS v5 protocol to encapsulate and secure the application traffic.

In addition to enabling access to a broader range of application types, adding proxy technology to SSL offers companies greater 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, by combining our proxy servers with SSL, Aventail can provide other types of authentication beyond the exchange of digital certificates SSL allows. Our solution can support Username/Password and two-factor authentication, such as RSA SecurID tokens.

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

Aventail's SSL VPN Approach



Aventail's combined SSL/proxy solution provides secure, anywhere access to both Web and client/server applications.

SSL VPNs: Straightforward solution for remote access and extranets

Whether an SSL VPN is right for you really depends on your company's needs. While SSL VPNs aren't designed to replace traditional IPSec-based site-to-site VPN, they do solve the remote access and extranet VPN issues in a simpler, more straightforward way. They offer easier deployment, fewer ongoing administrative hassles, and greater security for remote access and extranet VPNs.

Please visit our Web site at www.aventail.com to learn more about Aventail and how our combined SSL VPN and proxy solution can improve your remote access.

Aventail 

Secure access for the real world.

***Before You Buy:* Top 10 Criteria for Evaluating a Remote Access & VPN Provider**

1. Look for a financially stable provider with a proven track record.

In this market, solid fundamentals, a proven track record, and a healthy list of customers are key to ensuring that you find a partner who can serve your long term needs.

2. Find a solution that will meet your corporation's security policies.

Security concerns will continue to increase, so it's important that you implement a solution that gives only the right people access to the right resources. In addition, look for a service or product that not only provides control, but clear visibility on who is authorized to access which resources and information.

3. Purchase a solution that provides true, anywhere access and is network independent.

Your users are everywhere—behind a firewall on another company's network, at home or at a hotel using a broadband connection, on wireless LANs, or at a public kiosk. Be sure to find a solution that seamlessly works in every scenario and works over any telecommunication provider's network. This will not only make your users happy but it will reduce the number of expensive end-user support calls. In addition, having a network independent solution will save you money by eliminating expensive "switching costs."

4. Seek providers who offer solutions that make it easy to manage your VPN users.

Small-scale VPNs are relatively easy to manage. But, once a VPN goes beyond 200 users, the management of those users can be a headache for IT administrators. Find a solution that either eliminates or minimizes the need to distribute and manage hard-to-configure VPN clients. Also look for sophisticated management tools and services that will help you enroll, provision, and support your users.

5. Look for a provider that can scale with your needs.

Companies that offer a variety of products and services will offer you greater flexibility as your business requirements change and user communities grow. Don't get stuck with a solution that can only support a limited number of users.

6. Find a company who has proven experience in working with multiple types of Web and client/server applications.

As many IT professionals know, not all applications behave in a similar way. By providing your users with secure access to applications, there are multiple integration and compatibility problems that can arise with your out-of-the box and custom applications. Find a vendor who understands the intricate details of what it takes to support various types of applications.

7. Seek providers that have a predictable and quick implementation process.

The key here is to keep your users up and running, so you need a provider who can quickly transition your users to the new system. But don't be fooled by the vendors who promise "instant" activation of your remote access and/or extranet VPN. Anyone who understands enterprise networking and security knows that it takes more than a mere installation of a box to get your VPN up and running.

8. Challenge your provider to prove ROI on your remote access and extranet initiatives.

Economic pressures are driving an increased need for customers to see value from their IT expenditures. Ask your vendor for specific details on how they can provide a lower TCO or what return you can expect on your investment.

9. Find a company that puts customer service first.

Understand how they will serve your needs and what they will do to continue to add value above and beyond your existing service level agreement (SLA).

10. Most importantly, be sure to check customer references!

Ask for references that have similar technical and business requirements to your own. This allows you to get a candid, honest perspective from your peers and it will validate the vendor's claim to broad marketing statements such as "highly scalable," "very secure," "excellent customer service," and "easy to manage."