Top 10 Myths About SSL VPNs

1. SSL VPNs are for Web-based applications only.

Reality: The ability to secure Web applications is just the starting point for an SSL VPN. All vendors claiming to provide "clientless VPNs" or SSL VPNs must, at a minimum, provide secure remote access to Web-based applications. But most SSL VPNs do more, and leading vendors do much more.

Aventail's SSL VPNs secure the broadest range of enterprise applications in the market. With three complementary access technologies, Aventail customers secure complex client/server applications such as Peoplesoft and SAP, office productivity applications such as Microsoft Outlook and Lotus Notes, and even client applications on Pocket PCs. That's in addition to supporting Web-based applications such as Outlook Web Access and iNotes, access to network file shares, and employee and business partner Web portals.

2. SSL VPNs are brand new and immature.

Reality: SSL VPNs have quickly become one of the hottest topics in networking and security, drawing attention to a slew of "pure play" start-ups and a number of established network technology vendors. This recent attention gives the market the appearance of immaturity.

Aventail has been delivering SSL VPN solutions to enterprise customers since 1997, and over half a million people at thousands of companies use our solution. We were winning awards years before most of the other "pure play" SSL VPN start-ups were even founded. Aventail's core SSL VPN technology platform, the Aventail® ASAP™ Platform, is on its seventh major release.

3. SSL VPNs are not proven in enterprise-scale deployments.

Reality: Large SSL VPN deployments do exist. Companies currently use SSL VPNs to enroll tens of thousands of employees in employee benefits programs. Some of the largest health care provider networks in North America use SSL VPNs to provide secure, HIPAA-compliant remote access for doctors. The largest consulting companies in the world use SSL VPNs for secure access to project tracking and financial systems.

Aventail has the largest and most extensive enterprise deployments of any SSL VPN vendor. The above examples are all Aventail customers, with some deployments up to 70,000 users from a single enterprise. Aetna, Cerner Corporation, DuPont, FMC, IBM Global Services, and Mount Sinai NYU all use Aventail's SSL VPNs to secure their remote access.

4. SSL VPNs are less secure than IPSec VPNs.

Reality: SSL is a well established, proven Internet security standard, as is IPSec. Properly implemented, an SSL VPN can actually reduce security risks for remote access, since SSL VPNs are typically used to provide access at the application level, whereas IPSec VPNs create a network-level connection between the remote computer (or network) and the enterprise network.

Aventail considers security to be the most important attribute of an enterprise-class remote access solution. Aventail solutions provide four layers of protection that go beyond IPSec VPNs and other SSL VPNs:

Aventail™

- Aventail provides the richest, most granular access control. This enables administrators to precisely map their security policy so it permits access only to specific applications when accessed remotely under specific conditions.
- Aventail's proxy technology ensures that there is no direct network connection between the remote computer (or network) and the enterprise network.
- Aventail provides the flexibility to vary access by the strength of the cryptography used in the connection, and has implemented all leading cryptography standards, including triple DES.
- Aventail's unique aliasing model masks internal URLs from being displayed to untrusted users, and even to trusted users if they are in less trusted remote access sessions. The administrator defines a Web name (an "alias") for remote access users that is mapped automatically and transparently to the actual name (or IP address) of the internal Web resource.

5. SSL VPNs are slower than IPsec VPNs.

Reality: IPSec VPNs operate at a very low level in the OSI stack (layer 3), securing individual packets regardless of their content. The basic steps are well known and invariant, so IPSec can be implemented in hardware for superior speed, particularly in site-to-site installations. SSL VPNs have more work —and more complex work—to do, since they operate at the ever-changing and ever-expanding application layers of the network. SSL VPNs today are all software (or software appliance) solutions, which tend to be optimized for flexibility and not for raw throughput.

Aventail evaluates performance of its SSL VPNs based on how it impacts the user. With highly tuned software for both Aventail's appliances and client-side agent technology, end users enjoy secure remote access with imperceptible performance differences between their remote use and use on the internal network. And since Aventail solutions provide fast and efficient Web-based "clientless" access that IPSec VPNs can't, no direct performance comparison is possible.

6. SSL is only good for e-commerce, not for remote access.

Reality: SSL was designed to secure application-layer traffic over IP networks. Popularized by the e-commerce boom of the late 90's, SSL is also used to protect many other kinds of application traffic, including e-mail and file-transfer services.

Aventail pioneered the use of SSL for remote access in 1997, and since then, has based all of its SSL VPN solutions on SSL combined with proxy technology. SSL has proven to be a robust, flexible, and highly secure technology for securing the complete range of remote access traffic.

7. SSL VPNs are OK for casual remote access users, but I still need to give full IPSec clients to my power users on corporate laptops.

Reality: Since there is no need for client-side software, SSL VPNs do provide quick and easy access for the casual or infrequent remote access user —a benefit that IPSec VPNs cannot provide. Some SSL VPNs even enable some Java- or ActiveX-based "lightweight client" or "clientless" access to client/server applications. But when that's as far as they go, so-called power users may still demand the performance and breadth of access that a full, network-level IPSec client provides.

Aventail delivers a complete "no compromises" VPN solution through the combination of the Aventail® EX-1500™ appliance and the full-featured Aventail® Connect™ Windows agent. Even the most demanding

power user will find the Aventail Connect agent superior in function and security to their IPSec clients. At the same time, Aventail Connect provides the network transparency and ease of setup benefits of SSL VPNs that IPSec can't offer. Aventail Connect integrates with the Windows Graphical Identification and Authentication (GINA) to provide network-level capabilities such as mapped network drives and password notifications. Aventail Connect provides split-tunneling control for added security, integrates with desktop security products such as personal firewalls and anti-virus software, and still provides application-by-application access control to the administrator. With Aventail Connect, there is simply no need for an IPsec client—and its configuration and operational challenges—in your remote access solution portfolio.

8. SSL VPNs don't support as many authentication methods as IPSec VPNs do.

Reality: Because SSL delivers integrated support for digital certificates, it's possible to get the impression that vendors stop there. Digital certificate support is actually much more flexible when used with SSL. For example, unlike with IPSec, SSL allows server authentication with or without client certificates. The leading SSL VPN vendors have invested in supporting the major remote access authentication methods, like two-factor tokens, and directories, like LDAP.

Aventail, over the last seven years, has put an enormous effort into deep enterprise integration with both the user authentication methods and back-end directories. Aventail integrates seamlessly with all leading directories, including Active Directory, LDAP, RADIUS, ACE, to provide a real-time link so that administrators can manage their users and their group associations in one central repository.

9. If you use SSL VPNs, you don't have to worry about split tunneling or personal firewalls.

Reality: SSL provides a significant architectural security advantage over IPSec and other traditional network-level VPNs. That's because with SSL VPNs, user machines aren't nodes on the corporate network, so they can't be turned into routers for attack on that network. It's true, however, that some of the same remote access risks apply in the SSL world, though less severely. For example, control over split tunneling and integration with personal firewalls have become standard features of IPSec clients because of the potential vulnerabilities that remote clients may expose when connecting to the enterprise network via home networks, public Internet sites, or wireless hotspots. Split tunneling matters in the SSL VPN world as well: even if hackers can't exploit network-level attacks, they can misuse privileges. Split tunneling and personal firewalls help prevent that potential for misuse. If an SSL VPN agent can't provide these controls, that vendor isn't taking client-side security seriously.

Aventail provides robust client-side security with its Aventail Connect agent, including split-tunneling control and integration with personal firewalls.

10. It's easy to be successful in the SSL VPN business.

Reality: With increasing demand for SSL VPN products, a lot of new vendors have entered the market. It's easy to announce an entry into the SSL VPN market. It's hard to create a successful product and delivery channel. Just knowing SSL, as many companies from the traditional networking or SSL

acceleration backgrounds do, is not enough. Building an SSL VPN product that defies the myths requires extensive knowledge of networks, applications, security, and remote access issues.

Aventail has been building SSL VPNs and SSL VPNs only for its entire 7-year history. Aventail has conquered many difficult software problems in SSL VPN-specific areas, including application compatibility, policy management, authorization, and end-user security, and the company has extensive experience with remote access. Aventail's SSL VPN products and services have been tested, expanded, and refined in real-world deployments in every size enterprise, across numerous industries. They have built a successful global channel, as well as an impressive list of service provider partners who offer Aventail's SSL VPN solutions as part of their world-class service and product offerings. In addition, Aventail partners with an impressive list of best-of-breed technology providers to give customers an end-to-end secure remote access solution.

DS-4021-1202/1

Aventail™

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

Aventail Europe Ltd: St Martins House • 16 St Martins Le Grand
London EC1A 4NA • Tel +44 (0) 870.240.4499