

An SSL VPN Selection Framework:
One Size Does Not Fit All



INTRODUCTION ¹

Ubiquity in broadband connections to the Internet and the increasing pervasiveness of mobile devices (laptops, PDAs, and Smartphones) plus the accompanying evolution in how, when, and where “business gets done,” businesses are experiencing unending growth in remote access. Whether access originates from employees, business partners, or customers, the facts are clear that there are more remote access users and sessions than ever before. Plus, the diversity of resources being accessed (e.g., file shares, intranet websites, and email and other business-critical application servers) is expanding.

An additional pair of inescapable facts are remote access occurs: (1) through shared network environments such as the Internet and from public and office-deployed wireless access points, and (2) from end-user devices where the security state of those devices is uncertain and far from uniform. As shared network environments, they are open to all and consequently polluted with users and activities that are unwanted, disreputable, and dangerous. From the perspective of end-user devices, “getting business done” has irrevocably changed the population of devices from predominantly owned and managed by the business IT organization to include several categories of devices that IT cannot proactively control the security health of (e.g., patched software). Categories of uncontrolled, unmanageable, and, by default, untrusted devices include: employee home PCs, partner and customer-owned PCs and laptops, user-owned handheld devices, and shared Internet kiosks.

As untrusted, these networks, devices, and even the users themselves, if confirmation of their true identities is weak, contribute to a rising tide of business and security risk for firms that are increasingly dependent on remote access in their business operations. Certainly the level of risk will vary across businesses as the risk profile and risk tolerance for each firm is as unique as fingerprints – no two firms are the same. Nevertheless, the fact remains that risk is present and indifference to that risk has consequences.

The maturing of SSL VPN as a remote access gateway and the escalating adoption of SSL VPN by businesses big and small in our view are testaments that this risk management and business supporting solution should be on the “must list” for evaluation by all businesses with remote access needs. The challenge, like the uniqueness in risk profiles and tolerances, is that there is no one-size-fits-all SSL VPN gateway. Therefore, aligning the SSL VPN gateway with the best mix of capabilities for the business firm is prudent but challenging.

In this bulletin, we will tackle this challenge head-on by introducing an SSL VPN selection framework. With this framework, we believe businesses’ SSL VPN shopping and evaluation time will be reduced and their confidence in reaching the best SSL VPN selection will strengthen. In addition, to take this framework from conceptual to practical, we will use SonicWALL as a representative example of a leading security vendor with a broad SSL VPN product portfolio.

SSL VPN 101

Despite a market presence of more than a half decade, what an SSL VPN is may still not be thoroughly known among businesses with remote access needs. At the most basic level, an SSL VPN is a security gateway logically situated between communities of remote users and business software applications and other information technology resources hosted in a business’ network.

An SSL VPN is typically purchased as a hardware appliance with a software license and physically deployed in the demarcation between a trusted network (e.g., LANs, datacenters, and server farms) and untrusted network environments (e.g., the Internet and wireless access points).

1. Please note that the insights and opinions expressed in this assessment are those of Stratecast and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

Two of the prominent functions an SSL VPN performs are:

1. **Access Control** – SSL VPNs have excelled in controlling access privileges of remote users (i.e., what resources each remote user can access) at a highly granular level based on several variables (i.e., defined as policies) without requiring reconfiguration of the business' trusted network, installation of heavy software client software on end-users devices, and, in many circumstances, without modification of the software code of the applications remote users are accessing.
2. **VPN** – VPN stands for Virtual Private Network. A VPN creates private communication connections over a public network through a combination of security procedures and protocols such as SSL (Secure Sockets Layer). Encryption algorithms, such as DES, Triple DES, and AES, ensure the connection is private and tamper resistant. A key point of differentiation for both users and IT administrators between SSL VPN and, an older VPN approach, IPsec (Internet Protocol security) VPNs is that several categories of applications and IT resources are immediately accessible through the users' existing web browser with SSL VPN. This structural attribute has contributed to the rapid "out-of-the-box" deployment and end-user registration, IT simplicity, and end-user friendliness of SSL VPNs.

SSL VPN: AN ESSENTIAL TOOL FOR MANAGING SECURITY AND BUSINESS RISKS

With any security appliance, businesses should ask, "What are the risks this security appliance will manage to lower levels?" In the case of SSL VPNs, these appliances either independently or in combination with other security appliances, address a wide range of security and business risks. A summary of these manageable risks are listed below. It should be noted that the degree each of these risks is reduced through the SSL VPN is not uniform across vendors and SSL VPN models. Rather this list is meant to represent the manageable risks addressed by SSL VPN products collectively.

- **Unauthorized access** – Functioning as a gateway between the business' trusted network and untrusted networks, an SSL VPN narrows the entry points into the business network. This represents a first line defense in unauthorized access. The second line of defense is user authentication; accept only users that pass authentication tests. In support of authentication, most SSL VPNs will seamlessly mediate user's credentials with the business' existing directories (e.g., Active Directory) and multi-factor authentication deployments (e.g., RSA SecurID). Some SSL VPN products also can host directories and offer multi-factor authentication within the appliance itself. The third but no less important line of defense to unauthorized access is granular access control. As previously outlined, a distinguishing attribute of SSL VPNs is controlling user access based on several variables without requiring re-engineering of the business network. Examples of variables used in reaching an access decision include: user's identity, group affiliations, and role; type of user authentication passed (single versus two-factor); device type and ownership (business-owned laptop, smartphone, PDA, home PC, or Internet kiosk); access network (e.g., home broadband, hotel room, or public hotspot); and security state of end-user's device. Depending on the SSL VPN, the limiting factor in the level of sophistication in access policies is the business' ability to define its access policies and governance practices.
- **Data leakage** – Ensuring that sensitive information is insulated from unauthorized use is a growing need of businesses for several reasons such as regulatory compliance, brand protection, and safeguarding intellectual property. SSL VPNs can be an integral element of a business' data protection strategy. The aforementioned granular access control of SSL VPNs reduces the potential of data leakage by validating the conditions that must be present before business applications, file servers, and databases where sensitive information exists can be accessed. In addition, most SSL VPNs offer several means at the end-user's device to protect sensitive information accessed during the VPN session. A sample of those means include creating a virtual desktop, post-session wiping, USB port blocking, and controlling network printing.
- **Compliance violations** – Fines and notifying affected individuals of a data breach are two of the most public displays of compliance violations. With several means to control and protect the flow of information, SSL VPNs have been deployed by firms in intensely regulated industries such as health care and financial services as part of their regulatory compliance practices. Logging and reporting the details of denied and allowed access is another critical element of compliance. Without a reliable and systematic

means to substantiate that regulated controls exist and functioning properly, businesses are handicapped in their means to prove that they are compliant. Reporting depth and customization in support of compliance has been a prominent feature for several SSL VPNs.

- **Viruses and malware infections** – Viruses and malware infections are costly. They interfere with user productivity, compete for network capacity, potentially lead to data leakage, and cause the business to spend precious time on identifying and cleaning infected systems. Although there is no approach that can completely eliminate all instances of infection, SSL VPNs have been instrumental in reducing the potential. First, the granular access control of SSL VPNs narrows the footprint of systems that could become infected from connecting remote devices. Second, when operating in reverse proxy mode, SSL VPNs insulate back-end systems from attacks that are based on knowledge of the business network. Third, with end-point security health checking as a variable in access decisions, businesses can reject access by devices that are deemed risky (e.g., unpatched operating system vulnerabilities, aged virus definitions, and lenient firewall settings). Combined with automated remediation, risky devices owned by the business can be brought back into an acceptable security state and users of these devices can be granted wider access privileges without undue exposure to the business network.

FRAMEWORK FOR SELECTING AN SSL VPN

Our recommended framework for selecting an SSL VPN is for the business to plot its remote access requirements along three outward pointing lines. Each of these lines represents a different set of SSL VPN capabilities or dimensions. The further the business plots its remote access requirements away from the central point of origination of these three dimensions, the more complex, comprehensive, and/or stringent are its requirements. An illustration of this framework follows the description of the dimensions.

As the degree of complexity, comprehensiveness, or stringency varies across the three dimensions, the business gains a visual perspective of its priorities. For example, it is conceivable that some businesses would assess their requirements across the three dimensions as equally complex while other business would assess their requirements associated with one dimension as significantly more complex relative to the other dimensions.

Benchmarking SSL VPN solutions to this plot of business requirements will yield an SSL VPN selection optimally aligned with the needs of the business. The SSL VPN dimensions associated with these lines are:

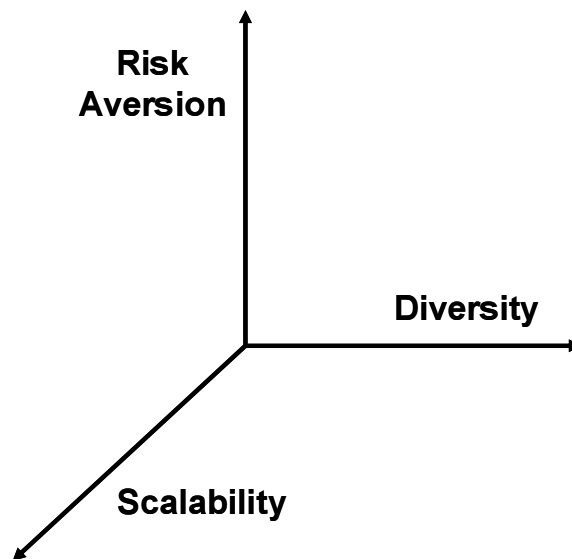
- **Risk aversion** – Businesses are not equal in terms of their risk aversion. Each will balance their assessment on the probability that a damaging event will occur and an estimation of the consequences to the costs of reducing risk. Differences notwithstanding, governmental regulations (e.g., Sarbanes-Oxley Act, HIPAA, and Gramm-Leach-Bliley Act) and industry compliance initiatives (e.g., PCI) effectively push standardization in risk aversion among companies mandated to conform. With forced compliance, businesses will gravitate toward solutions that are highly effective in supporting compliance but also cost efficient as the business benefits (e.g., improved market competitiveness) of forced compliance can be zero.

Outside the realm of forced compliance, risk aversion is higher for businesses with a need to protect their (1) public image, (2) intellectual property, and/or (3) private business information. For firms in which their public images are based on nurtured trust relationships with their customers and business partners, occurrences that damage their public images (e.g., unauthorized access or a data breach) can have both near-term (e.g., costly notifications) and long-term (e.g., lost customers) impacts. Similarly, intellectual property (e.g., new software code for an electronic gaming company) and various forms of private business information (e.g., marketing plans, account lists, and pricing) have material business value. If accessed and used by unauthorized parties, there can be significant business impacts.

- **Diversity** – If all remote accessing devices were business-owned laptops used exclusively by employees in the same department or work group, from the same laptop vendor, have the same OS version, have the same client security applications, only connect through Ethernet within hotel rooms when remote, and there is just one application accessed and that applications has no customization, the complexity involved

in ensuring secure and reliable remote access would be relatively straightforward. This is not reality for many businesses. Any or all of these parameters can be significantly diverse. And with diversity, a higher level of technological sophistication in the SSL VPN solution is a necessity. In addition, easing that technological sophistication for administrators and masking complexity from end-users is not to be assumed; smart design and product development is required by the SSL VPN vendor. From our engagements with numerous SSL VPN vendors, the SSL VPNs that can address higher tiers of diversity are from vendors that have targeted their SSL VPN gateways and directed their product development to serve enterprises with large remote user communities consisting of mobile employees and business partners (e.g., extranets).

- **Scalability** – Without the requirements to pre-configure end-users’ devices for remote access and to provide on-going oversight of VPN client software, the incremental costs for expanding remote user communities is materially less with SSL VPN versus IPsec VPN. Driven by this economic value proposition, enterprises are using SSL VPNs to support larger remote user populations and a larger number of concurrent VPN tunnels. In addition, SSL VPNs are being used to support predictable spikes in remote access (e.g., in-session periods at colleges and universities) and random spikes (e.g., an integral element of business continuity plans). In all of these SSL VPN use circumstances, rapid scalability and reliability are essential attributes of the SSL VPN platform. Similarly to the diversity dimension, not all SSL VPNs are equally equipped to support larger user populations (e.g., into the hundreds and even thousands registered users) either on a continuous or an event-driven basis. Consistent throughput as concurrent tunnels increase in number, system pooling of multiple gateways, uninterrupted user sessions if a failover occurs, and centralized and remote management are a sample of the attributes that should be examined when evaluating the scalability dimension.



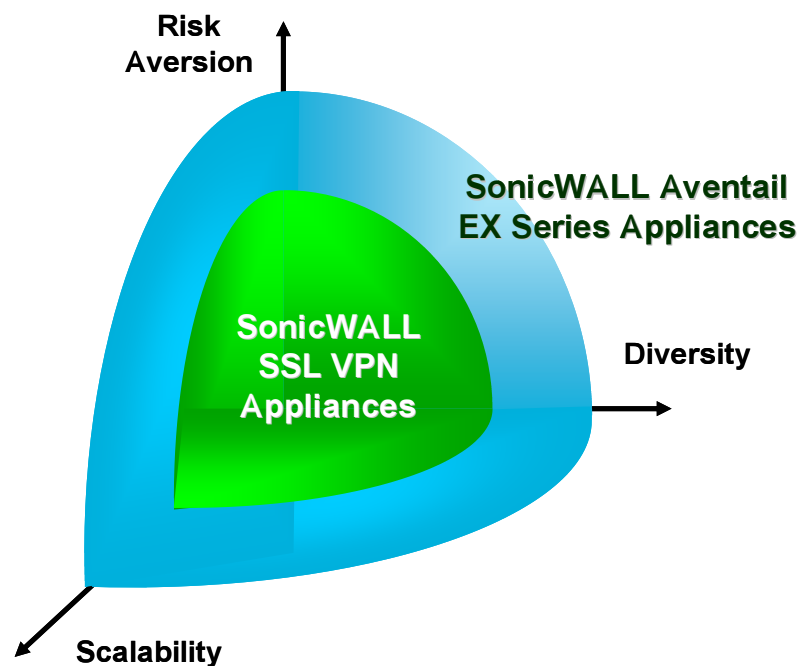
There is a fourth important dimension, an overlay dimension to the other three, reflecting ease of use. In this selection framework context, we will define ease of use as the capacity of the SSL VPN to meet the business’ requirements with the least amount of IT engagement and/or the greatest level of end-user transparency and convenience. For example, if there are two SSL VPN solutions that are equally capable in meeting the business requirements as described in the other three dimensions, the SSL VPN solution that consumes the least IT resources without trading off effectiveness is more appealing, particularly with businesses that are constrained in their in-house IT personnel. Similarly with user transparency, SSL VPN solutions that can meet more of the remote access requirements without interfering with end-user routines is a more compelling SSL VPN to one that does not score as high in this dimension.

SonicWALL AND THE SSL VPN SELECTION FRAMEWORK

SonicWALL is an established provider of network and content security appliances. Historically, SonicWALL has specialized in sturdy security appliances that are easy to deploy and simple to configure and manage. The company's products have appealed to small and mid-sized businesses (SMBs) where the range of requirements and need for customization does not reach the level of larger enterprises and the availability of in-house security and IT personnel is limited.

With email security and firewalls already in use by large enterprises, SonicWALL further underscored its expansion into and dedication to serve the enterprise market, the company recently acquired Aventail. Aventail was among the original developers of SSL VPN appliances and has earned high marks from its customer base for its breadth and depth of SSL VPN features. And, like SonicWALL, Aventail has diligently refined its feature capabilities to be easy to use without compromising effectiveness.

With the combined suite of SonicWALL and Aventail SSL VPN appliances, the company's coverage of the selection framework is greatly expanded. Depicted in the illustration that follows, we view the SonicWALL SSL-VPN, which includes the SSL-VPN 200, SSL-VPN 2000, and SSL-VPN 4000, as occupying the center area of this framework and moving outward along all three of the product dimensions of risk aversion, diversity, and scalability. Highly complementary to SonicWALL SSL-VPN line, the SonicWALL Aventail appliances, which include the EX-750, EX-1600, and EX-2500 models, occupy the outer shell of this multi-dimensional framework for enterprises with more demanding requirements and move inward to serve businesses with moderate requirements.



Favorably for buyers of SSL VPN appliances, SonicWALL has a product range that captures the current secure remote access requirements of small businesses up to large enterprises. Moving forward into the future, we anticipate that the company will cede existing features and capabilities between its two SSL VPN product lines and continue the long-standing practice at SonicWALL and Aventail of incorporating new features into their SSL VPN appliances to meet the constant evolution in businesses' remote access requirements.

CONCLUSION

Remote access is a fact of life for many businesses. It is essential to getting business done but also must be approached with caution to avoid offsetting levels of risk, IT management, and end-user inconvenience. SSL VPN is a remote access solution category explicitly designed to serve this burgeoning need for secure, easily customizable, highly adaptable, and end-user friendly remote access. But with the remote access requirements of businesses so varied, the process of selecting the SSL VPN solution that is optimally aligned with a business' unique set of requirements can be quite challenging. The SSL VPN selection framework introduced in this bulletin is intended to assist in this selection process.

SonicWALL is poised to further assist in this selection process. Rather than examining SSL VPN solutions from several vendors, SonicWALL with its recent acquisition of the Aventail SSL VPN product line offers a wide range of SSL VPN appliances that can satisfy the standard to sophisticated requirements and budgets of small businesses up to large enterprises.

Realizing that an SSL VPN represents an important but not the only layer of network and information protection businesses need, integrating SSL VPN with threat management technologies (e.g., intrusion detection and preventing, email scanning, and URL filtering) is a wise path to follow. Tight integration of SSL VPN with threat management from a single security vendor is a step in the right direction of fully coordinated risk management and can save the business time and money. With a successful business in threat management appliances, we expect that SonicWALL customers will see integrated SSL VPN and threat management solutions in the future.

Michael Suby
Research Program Director
Stratecast (a Division of Frost & Sullivan)
msuby@stratecast.com

About Stratecast

Stratecast directly assists clients in achieving their objectives by providing critical, objective and accurate strategic insight, in a variety of forms, via an access-and-industry-expertise-based strategic intelligence solution. Stratecast provides communications industry insight superior to a management consultancy, yet priced like a market research firm. Stratecast's product line includes: Monthly Analysis Services [Convergence Strategies & Network Architectures (CSNA), OSS Competitive Strategies (OSSCS), Network Professional Services Strategies (NPSS), Consumer Market Strategies (CMS), and Business Market Strategies (BMS)]. Weekly Analysis Service [Stratecast Perspectives and Insight for Executives (SPIE)], Standalone Research, and Business Strategy Consulting.

About Frost & Sullivan

Frost & Sullivan, a global growth consulting company founded in 1961, partners with clients to create value through innovative growth strategies. The foundation of this partnership approach is our Growth Partnership Services platform, whereby we provide industry research, marketing strategies, consulting and training to our clients to help grow their business. A key benefit that Frost & Sullivan brings to its clients is a global perspective on a broad range of industries, markets, technologies, econometrics, and demographics. With a client list that includes Global 1000 companies, emerging companies, as well as the investment community, Frost & Sullivan has evolved into one of the premier growth consulting companies in the world.