

Making the Right Move to a Managed Service
Provider for SSL VPN



Executive Summary

Managed Services Providers (MSPs) with proven SSL VPN expertise bring strategically minded enterprises reduced costs, strengthened security, and improved productivity. This paper will illustrate the benefits of MSPs with SSL VPN offerings and why Stratecast Partners believes this is the right decision for an enterprise's remote access needs.

"...we [Stratecast Partners] believe that strategically minded enterprises will reach the logical conclusion that the capabilities of a Managed Services Provider (MSP) with proven SSL VPN expertise is imperative to gain the full strategic benefits that a SSL VPN can bring to their organizations."

Introduction

Adoption of SSL VPNs is growing rapidly. In a recent report by Frost & Sullivan, worldwide unit sales of SSL VPN appliances grew 97% from 2004 to 2005.¹ This growth and the number of high-quality SSL VPN vendors underscore the robust value SSL VPNs deliver to businesses that are confronted with several overlapping and challenging business objectives, each related in some manner to creating and establishing secure and controlled access between end-users and networked resources. A sample of these business objectives includes:

- *Serving More User Communities* - Extending network access to a broader community of users (e.g., stationary and mobile remote workers, suppliers, business partners, consultants, and customers).
- *Supporting More Access Environments* - Ensuring a dependable connection experience through a widening array of endpoint platforms and access environments.
- *Providing Access Without Application and Network Changes* - Providing remote access to all networked resources without re-writing application code, reconfiguring the enterprise network, or causing end-user inconvenience.
- *Enforcing Compliance* - Consistently meeting a mosaic of information use and protection compliance mandates.
- *Protecting the Network* - Protecting the enterprise network from threats introduced through remote-connecting devices regardless of whether the devices are owned or not.
- *Quickly Modifying Access Policies* - Efficiently and comprehensively responding to access policy changes and the dynamic composition of user communities.
- *Ensuring Business Continuity* - Being prepared for rapid response scenarios when traditional in-office connections cannot be supported (e.g., debilitating storms, natural disasters, public health emergencies, and network or power failures).

When considered as a whole, these business objectives underscore three strategic initiatives being pursued by enterprises. These initiatives include:

- 1. Reducing Costs,**
- 2. Strengthening Security, and**
- 3. Improving Productivity.**

In our opinion, enterprises are selecting and using SSL VPNs not only to establish secure and controlled access between end-users and network resources, but more strategically in direct support of these three initiatives.



However, merely utilizing the baseline functionality of SSL VPNs is insufficient to gain all of the potential strategic benefits. Through our several years of research on the SSL VPN market, vendors, and products, we have chronicled the non-stop rise in SSL VPN capabilities. Long gone are the days that SSL VPN vendors would promote and enterprises would evaluate SSL VPNs solely on their ability to establish a private connection between an end-user's Web browser and the SSL VPN gateway for simple Web-enabled applications. Instead, the reality is that SSL VPNs now encompass such a wide and deep range of features and functionality that only the most SSL VPN-astute enterprises are adequately positioned to leverage the full strategic benefits and to do so in a cost effective manner.

Consequently, we believe that strategically minded enterprises will reach the logical conclusion that the capabilities of a Managed Services Provider (MSP) with proven SSL VPN expertise is imperative to gain the full strategic benefits that a SSL VPN can bring to their organizations. It is the purpose of this paper to outline why an enterprise would choose a MSP with SSL VPN expertise and, in greater detail, describe how this type of MSP can directly support the enterprise in all three of these strategic initiatives.

Why Outsource Management Functions

Just as enterprise circumstances differ, so too are their reasons for outsourcing the management of critical functions. Nevertheless, we believe that for most enterprises the reasons to outsource are captured by one or more of the following:

- *A lack of expertise* - The expertise may not exist within the enterprise or cannot be developed to perform the management functions at the level of proficiency required.
- *Time is in short supply* - Business needs may dictate that specific management functions be performed faster than can be completed with internal staff. This need for speed pertains not only to the time consumed in initial deployment but also extends to the time required for routine and change management.
- *Resource Prioritization* - Whether conscious or not, enterprises are defined by their prioritization decisions, that is, decisions on allocating scarce resources. In choosing to outsource, the enterprise has made a conscious decision that: (1) resources that would otherwise be available to conduct the management functions are better employed in other areas of the business, and (2) the managed service provider is better equipped to deliver the services needed.

How does a Managed SSL VPN Service Provider Support Strategic Initiatives

As previously stated, a SSL VPN can be instrumental in supporting enterprise strategic initiatives of reducing costs, strengthening security, and improving productivity. Furthermore, we believe an engagement with a MSP with proven expertise in SSL VPN is essential for this to occur. In the following tables, we will describe how a MSP with SSL VPN expertise resolves the challenges enterprises encounter in each of these strategic initiatives.

1. Reducing Costs: How MSPs Lower Total Cost of Ownership

Effective and Efficient Operations	<p>Challenge: SSL VPN is a new breed of remote access technology. Although there are attributes of SSL VPNs that structurally reduce enterprise’s VPN administration effort (e.g., does not require endpoint configurations), SSL VPNs do require an enterprise’s IT staff to enter a new learning curve. Simultaneously, the enterprise may also be extending remote access to larger and more diverse user communities and be encountering more stringent regulatory compliance requirements. All of this leads to additional demands on the enterprise’s in-house VPN and security administrators.</p>
<p>Solution: In comparison to an in-house management approach, a MSP supplies a level of expertise to SSL VPNs that, in our view, few enterprises can duplicate. A contributing source to the MSP’s differentiated expertise is its exclusive focus on SSL VPN management honed and broadened through experience in serving many enterprise customers, in diverse network and application scenarios, and over time. The MSP applies and demonstrates its expertise horizontally across all SSL VPN functions with a high degree of operational effectiveness (completing each task accurately and completely) and time efficiency (no wasted effort). The collective result is a material reduction in the use of human resources versus what would be required in an in-house approach. For example, the time to deploy an average SSL VPN implementation can be reduced from four months to less than thirty days when using an MSP.</p>	

Scalability Without Capital Investment	<p>Challenge: For enterprises that choose to manage their own SSL VPN, they own the responsibility to scale their deployments as business needs evolve. Either they purchase excess capacity upfront or they add capacity as their needs dictate. Regardless of approach, extra capacity must exist at all times to adequately address untimely and unpredictable spikes in user demand. This extra capacity carries with it real costs in hardware, software, and management.</p>
<p>Solution: In a MSP engagement, the MSP owns the responsibility to seamlessly accommodate temporary and permanent increases in SSL VPN activity. As the owner of the SSL VPN appliances and software licenses, a proficient MSP will have sized the SSL VPN deployment appropriately for current usage levels and reasonable spikes in activity. The cost to the customer does not entail any capital investments but purely reflects the actually level of SSL VPN activity.</p>	

Shared Costs	<p>Challenge: Several important SSL VPN tasks are not enterprise-specific. Subsequently, completing these tasks has a high degree of uniformity across enterprises. Nevertheless, these tasks are non-trivial and require investment in personnel to complete them proficiently.</p>
<p>Solution: For these common SSL VPN tasks, costs savings are realized when the task is learned by one and applied to many. In servicing multiple enterprise customers, the MSP is well positioned to identify and complete these common tasks and distribute the costs across all of its customers at a fraction of the cost an individual enterprise would incur. Examples of this include SSL VPN software upgrade, new feature, and application testing. It is also relevant to recognize that the MSP has the purchasing clout of its many customers and will receive higher discounts from the SSL VPN vendor than possible by an individual enterprise. These savings can be passed on to the enterprise by the MSP.</p>	

Remote Access VPN Consolidation	<p>Challenge: Most enterprises currently have a remote access VPN in place, most likely an IPsec VPN. With the full application connectivity supported in most SSL VPNs and the differentiated attributes of SSL VPNs versus IPsec VPNs, the rationale for maintaining two remote access VPNs types has diminished. In addition, maintaining two types of remote access VPNs adds to enterprise operating expenses in IPsec gateway oversight, periodic updates to IPsec VPN software clients, and end-user helpdesk support.</p>
<p>Solution: Consolidating all remote access VPN functionality into a single technology eliminates the redundant and excessive expense of maintaining multiple technologies. In addition, personnel previously devoted to service the old technology can be re-assigned. A MSP, through its SSL VPN expertise and multi-customer experience, will assist the enterprise in accelerating its transition to a SSL VPN for all of its remote access needs and, in the process, eliminate the additional operating expenses of maintaining dual remote access VPNs.</p>	

2. Strengthening Security: How MSPs Ensure Premium Grade Security

<i>Error-free and Robust Access Policies</i>	<p>Challenge: One of the distinctive attributes of SSL VPNs is granular access control, that is, explicitly defining the networked resources end-users are authorized to access. In leading SSL VPN appliances, several variables are dynamically assessed to determine the appropriate level of access rights and privileges for each user in each session. Underlying granular access control are access policies that define the rules and conditions corresponding to end-user access privileges. Policies are, by nature, a human input and therefore subject to error and conflict (e.g., one policy negates the intent of another policy). Moreover, the potential for error and conflict rises as the number of policy administrators increases and the policies become more complex.</p>
<p>Solution: An important role provided by the MSP is access policy review and design. Through review, the MSP will leverage its knowledge and experience in policy use to assist enterprises in detecting potential errors and conflicts before and after policies are placed into production. In addition, the MSP's best practices experience will assist the enterprise in defining access policies that balance regulatory compliance, industry standards, and business objectives.</p>	

<i>SSL VPN Appliance Protection</i>	<p>Challenge: An SSL VPN appliance operates as a gateway between end-users and enterprise resources and the dependability of that gateway is imperative. In addition, the SSL VPN appliance is typically situated between uncontrolled networks (e.g., the Internet and wireless access points) and a controlled network, the enterprise LAN and/or data center. As a result, the SSL VPN appliance itself can be the target of an attack.</p>
<p>Solution: Recognizing that security vulnerabilities are possible with SSL VPN appliances is an essential first step in managing security risk. Categorizing potential threats aimed at SSL VPN vulnerabilities and taking action to reduce and/or eliminate vulnerabilities is a second essential step. A MSP with SSL VPN expertise has the dedicated perspective and broad insight gained from serving multiple customers to be more effective in each of these steps than most enterprises. In addition, the MSP will work with the SSL VPN vendor as new software releases are being developed to discover and eliminate new vulnerabilities. In the event that a new vulnerability is introduced following a software upgrade, the MSP can take protective action on behalf of all of its customers.</p>	

<i>Business Continuity</i>	<p>Challenge: Despite a future that holds uncertainty, enterprises demand confidence that their employees can access data resources. If access to data is limited to in-office connections, business continuity is at risk. Seasonal storms, natural disasters, public health emergencies, and network or power failures can disrupt the routine flow of business activity.</p>
<p>Solution: The clientless nature of SSL VPNs can be an effective means to quickly put in-office employees back online when they are unexpectedly locked out from the office environment. However, as SSL VPN is an enabling technology, it is not the full solution. Expertise is essential. A MSP with SSL VPN expertise can assist the enterprise in using SSL VPN technology to its advantage for business continuity. Unlike in-house remote access VPN solutions where the enterprise is limited to a set number of concurrent connections, the MSP can provide a burstable SSL VPN service that is ready when the organization needs it. MSPs also provide the assurance that an audited staff of specialists is continuously available when unforeseen disruptions occur.</p>	

3. Improving Productivity: How MSPs Drive Productivity Gains

Application Assurance	Challenge: Enterprise investments in business applications (e.g., collaboration, communication, sales force automation, and customer resource management) are significant. The return on investment in terms of improvements in end-user productivity and business enablement is incomplete if end-users cannot effectively reach those resources when they need to, wherever they are located, and through the access devices they are presently using.
Solution: MSPs with SSL VPN expertise operate to ensure that authorized end-users can access and reliably interact with business applications when remote. However, end-user devices, operating systems, access environments, and business applications represent a highly diverse and sophisticated mix. Assuring application access is a multi-faceted and complex undertaking. If unsuccessful, undesired consequences that affect end-user productivity and business enablement will occur, such as: slower end-user adoption of remotely accessible business applications, dissatisfied end-users, and increases in helpdesk calls. Through continuous monitoring and interacting with a diverse enterprise customer base, MSPs are uniquely positioned to recognize and resolve potential remote access application issues before they become widespread. Furthermore, an enterprise who engages the MSP prior to a new application introduction or application updates gains a valuable stamp of approval and confidence in rolling out new applications and updates to their remote accessing end-users.	
SSL VPN Appliance Reliability	Challenge: An SSL VPN appliance is the primary gateway between remote accessing end-users and business resources. If this gateway fails, end-user connections are severed and productivity suffers. As a result, the IT organization faced with a fire drill to reprioritize its IT resources, analyze the problem, develop an action plan, and then execute – hopefully correctly the first time.
Solution: A primary objective of the MSP is gateway reliability, that is, ensuring a steady state. Quickly responding and rectifying outages with a high degree of precision and speed are important. Of equal importance is preventing disruptions before they become business impacting. Proactive testing and installation of SSL VPN software patches, modifying security settings for changing conditions, and continuously monitoring device health and usage are examples of critical preventive duties performed by the MSP. Enterprises should expect explicit SLAs (Service Level Agreements) from a MSP on device reliability.	
Security Compliance	Challenge: The upward trend in security compliance is non-reversing. Two aspects of compliance exist in tandem: (1) establishing the required security technologies and procedures, and (2) proving substantiation that the established technologies and procedures were operational. Both are important and both can consume significant time and organizational resources.
Solution: A MSP with SSL VPN expertise is effective in supporting the enterprise in both of these compliance aspects. By design, a SSL VPN solution delivers several elements of security that are relevant in today's compliance environment. Those elements include: private communication via encryption, granular access control, and protecting networked resources from infected remote-connecting devices. The additional functions MSPs deliver that support enterprise compliance effort are ensuring these security elements are continuously operating and compliance substantiation is available through audits, status reports, and alerts. In addition, MSP attention to and active involvement in designing and following best practices plays a key role in conserving an enterprise's compliance efforts.	

Conclusion

As the preceding tables show, tangible strategic benefits flow from an engagement with a MSP with SSL VPN experience. A MSP's focused SSL VPN expertise, multiple customer engagements, and continuous availability directly contribute to reduced costs, strengthened security, and improved productivity for the enterprise. Moreover, a MSP with SSL VPN expertise will deliver a substantially faster and more comprehensive SSL VPN deployment to enterprises with moderate to highly complex remote access requirements at a total cost that is lower than if attempted with in-house staff.

Michael Suby
Business Market Strategies Program Manager
Stratecast Partners (a Division of Frost & Sullivan)
msuby@stratecast.com

About Stratecast Partners

Stratecast Partners 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 Partners' 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 Partners 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.