

Array Networks: Embraced by Large Enterprises

Introduction¹

What do two of the largest enterprise software and financial services companies in the world have in common? Information exchange is fundamental to each. Furthermore, without the means to reliably and securely connect users to business applications and information repositories, the opportunity to move their respective businesses forward is severely hampered.

In this brief, we will describe how the latest in VPN technology, SSL VPN, can serve business needs and, of equal importance, reduce IT involvement and expense. Recognizing that choice in SSL VPN solutions exist, we will highlight the reasons supporting these companies' selection of Array Networks as their SSL VPN vendor.

What's wrong with existing VPN technologies?

Nothing is wrong with existing VPN technologies, principally IPsec VPNs, "IF" the objective is to create a persistent network-to-network connection between trusted parties. For some, this "IF" may seem insignificant. However, in the new open networking environment in which technical barriers associated with connecting a wide range and growing number of users to critical resources from basically any device and any location (customer or business partner site, homes, and at Internet kiosks) must be eliminated, this "IF" is a very significant. In addition, operating from a mindset of network openness does not in anyway relieve businesses of their responsibility to protect their network infrastructure and control the flow of information. In fact, this responsibility intensifies.

There are several reasons why the network-to-network connection design of IPsec VPN is no longer the right tool for the job. Those reasons include:

1. Network-to-network connections are administratively intensive and require common networking technology to operate at each end of the VPN tunnel. This requirement becomes impractical with access devices that are outside the network administrator's control. Moreover, administrative support expense grows proportionately with the user base.
2. Network-to-network connections default to access permissions that include all resources on the network and require additional procedures and network segmentation to pare access permissions to only specific resources.
3. Network-to-network connections, unless other protective mechanisms are established and maintained, create an unrestrained highway for worms and viruses in which one network can be the unexpected enemy of the other and vice versa.
4. Network-to-network connections are not firewall-friendly. Firewalls and other network perimeter defenses work very well in restraining passage to known and approved activities. When the unplanned occurs, firewall policy controls must be amended; something administrators do not allow without strong justification. Furthermore, helpdesk calls on

¹ The following analysis represents a combination of Stratecast Partners' multi-year study of the evolving SSL VPN market, products, and vendors, and recent interviews with two of Array Networks' large enterprise customers.

connectivity issues are involved and can easily consume 30 minutes of the help desk and user time with the real potential of no positive resolution.

In consideration of these IPsec VPN limitations, the underlying commonality is trust. IPsec VPNs work extremely well where trust exists among communicating parties or can be established and maintained with limited administrative effort. If a trust relationship is not pre-existing or expensive to maintain, IPsec VPNs come up short.

SSL VPNs Overcome IPsec VPN Limitations

For each of the four IPsec VPN limitations, SSL VPNs has a remedy. As a direct and positive outcome, SSL VPNs can reliably establish secure and controlled connections between communicating parties where bi-lateral trust does not exist.

1. **SSL VPNs do not require a vendor-proprietary VPN software client to be installed on remote accessing devices.** For accessing Web applications, just the ubiquitous Web browser serves as the client. This eliminates administrative effort to install and maintain additional software on what can be a highly diverse community of access devices and configurations. To serve a broader range of applications, SSL VPN vendors have developed lightweight application adaptors (e.g., a JAVA applet) that are automatically downloaded and activated on the end-users' device without end-user involvement.
2. **SSL VPNs operate as an application gateway not a facilitator of network-to-network connectivity.** This attribute permits SSL VPNs to be very granular and dynamic in assignment of access privileges. Privileges can be based on several variables such as end-user identity, his/her role, access means (home broadband connection versus Wi-Fi hotspot), authentication strength, and security state of the end-point device. Also noteworthy is that SSL VPN's granular access control occurs without reconfiguration of the enterprise network or application infrastructure. With the minor effort of plugging into enterprise's existing authentication schemes, SSL VPNs granular access control is an independent and unobtrusive operation.
3. **SSL VPNs have a three-prong approach to controlling threat exposure.** First, SSL VPN access for Web and client/server applications passes through a proxy and this proxy creates a virtual barrier between end-users and the application infrastructure. Second, the aforementioned granular access control limits the range of resources and sensitive information accessible by authenticated end-users; they cannot venture beyond their defined access privileges. Third, most SSL VPNs include end-point security policy checks as part of the application access decision. If the end-point is out-of-compliance (e.g., old anti-virus definitions or missing OS patches), the end-user's access can be blocked or limited to fewer resources.
4. **SSL VPNs are firewall-friendly.** Because SSL VPNs form a SSL tunnel between end-users and the SSL VPN appliance, contention with perimeter firewall settings either at the access origination network or the terminating network rarely occur since the SSL tunnel uses the same firewall ports as HTTP and HTTPS traffic; ports that are generally set as open.

Array Networks Delivers on the Promise of SSL VPN and More

The previous sections provided a top-level review on the reasons for enterprises increasing migration to SSL VPN technology as their preferred remote access solution. All of these reasons contributed to the interviewed companies' decision to examine several SSL VPN products. In the end, Array Networks' SPX Enterprise SSL VPN Remote Access solution scored higher in capabilities that matter the most to these two companies. Those features are described below. Before doing so, it is important to note that large enterprises have very stringent product requirements and evaluation

procedures. Correspondingly, the product selection process is highly competitive encompassing multiple stages: RFP preparation, filtering vendors based on feature match, and the final decision based on lab tests. It is not uncommon for large enterprises to extend RFP participation to six or more potential vendors.

Interviewed companies' reasons for selecting Array over other competitive SSL VPN solutions included the following:

- **Performance** – The Array SPX ranks at the top end of available SSL VPN products on several performance characteristics – scalability, throughput, and latency. For the financial services company, where immediate “click to eyeballs” user response times was critical, latency (the time for packets to be processed through the appliance) for its customized business application could not exceed five milliseconds (0.005 seconds). At levels above five milliseconds, user productivity and business objectives would be impacted. In the company's deployment, latency through the Array SPX averaged 1.5 ms and never exceeded 5 ms.

Scalability is also an important performance attribute as peaks in usage and growth in the number of concurrent end-users are anticipated. The ample headroom of the Array SPX (up to 64,000 concurrent end-users supported with the top model) assures enterprises that the solution can grow with them without becoming a traffic bottleneck. Currently, the enterprise software company supports 7,000 concurrent users with the Array solution and the company plans to materially expand the number of users in the near future.

Also noteworthy, product scalability improves ROI (Return on Investment) and supports network simplification. Higher scalability in a SSL VPN gateway results in fewer SSL VPN gateways necessary to support the same number of users and fewer network devices (e.g., firewalls, load balancers, and switches) are needed to protect network segments and ensure reliability.

- **Feature bonuses** – two were highlighted:
 1. **IPsec tunneling over SSL** – Most large enterprise have IPsec VPNs already deployed for remote access. As previously stated, firewall conflicts reduce IPsec effectiveness particularly for users that connect as network guests (e.g., consultants) on another company's network. An Array feature to transparently encapsulate IPsec within a SSL VPN tunnel allows existing IPsec users to maintain current procedures and avoid productivity robbing firewall blocking. This was an important feature for the enterprise software company as it has several existing communities of users that operate as network guests and need to tunnel back to the home network.
 2. **Layer 3 VPN API** – Many large enterprises also have existing software applications tied to remote access, for example, an ISP local number dialer. Integration of the Array solution with existing applications, enabled through an API, has a direct bearing on end-user convenience. The financial services company is using this feature to automatically and transparently create a VPN tunnel as users click on the company's application icon.
- **Virtualization** – Typically with large enterprises, multiple organizations have similar technical needs but require independent administration and policies. One means to serve these similar yet independent needs is to deploy a SSL VPN gateway or gateways (for high availability) for each organization. The cost of this can mount up quickly and the enterprise software company recognized this upfront in its product evaluations. Array's SPX provides complete segmentation of users, administration, and traffic among multiple communities of users from a single device. This “virtualization” feature allowed the company to save on its SSL VPN expenditures versus solutions lacking comprehensive virtualization while fully serving the needs of multiple user communities.

- **Customer support** – For both companies, Array Networks’ customer support and product customization was highly appreciated. The list of “wants” by enterprise IT staff is never-ending. The enterprise software company was particularly impressed with Array’s responsiveness to their custom feature requests and Array’s flexible platform architecture which, in turn, led to new features delivered in a matter of weeks, not months. The financial services company was also impressed with the overall deployment ease of the Array SPX, as well as the responsiveness of the Array staff when more sophisticated technical assistance was needed.

Conclusion

SSL VPNs are quickly being recognized throughout the industry as a highly viable and economical solution for remote access. The limitations of legacy remote access solutions, such as IPsec VPNs, are solved through SSL VPNs. Even so, SSL VPN products are not created equal. Enterprise-class performance and adaptability are feature attributes of the Array Networks’ SPX Enterprise SSL VPN Remote Access solution that made Array the right choice for the two referenced companies.

Michael Suby

Senior Research Analyst, Communications Services Strategies and Opportunities

msuby@strategcast.com