

Array Purpose-Built SSL VPN

White Paper



Delivering Fast, Secure, and Scalable Universal Access

Executive Summary

As more organizations turn to virtual private networks (VPNs) based on Secure Sockets Layer (SSL) technology to meet their remote access needs, it's becoming clear that SSL VPN solutions based on a general purpose computing platform are not equipped to meet the demanding requirements of medium to large enterprises and service providers.

Such customers have stringent demands for security, user experience, response time, throughput, and scalability. At the same time, they want to become more efficient by consolidating a plethora of access control lists (ACLs)—from firewalls, LAN switches, wireless LAN devices and application security proxies—onto a single VPN system.

Only a purpose-built SSL VPN platform can satisfy these demands.

This paper will discuss the attributes of such a purpose-built SSL VPN platform—the Array Networks SPX— and how it cost-effectively delivers real-world benefits to enterprises and service providers including:

- **Improved security, flexibility and control**
- **Improved performance, productivity and user experience**
- **Reduced total cost of ownership (TCO)**

Introduction

More and more organizations these days are turning to virtual private networks (VPNs) based on Secure Sockets Layer (SSL) technology for solving their remote access needs. According to Gartner research:

"By 2008, SSL VPNs will be the primary remote access method for more than two-thirds of business teleworking employees, more than three-quarters of contractors and for more than 90 percent of casual employee access (0.7 probability)."

"SSL VPNs also will eventually replace millions of simpler SSL sessions in B2C portals."

"Growth potential is sufficient to attract every major network player as well as to sustain a sizeable population of smaller incumbents, startups and investors."

Attribution: Gartner, "Magic Quadrant for SSL VPN, North America, 3Q05" by John Girard. December 8, 2005.

In response to the increasingly mobile and diverse nature of users—including non-employees who typically utilize their own laptop computers with varying levels of security—enterprises and carriers are looking to make secure application and network access an integral part of the resources they provide to end users.

General-purpose SSL VPNs enable users to securely access data and applications from multiple locations and computing devices, offering granular, identity-based access controls. But most SSL VPNs pay almost no attention to the performance required for a positive end-user experience as well as the scalability that large-scale universal deployments demand.

A General-Purpose SSL VPN is Not Sufficient

SSL VPN solutions leverage the ubiquitous SSL encryption of any browser to encrypt traffic, provide data confidentiality and data integrity. As Gartner notes, corporations have generally accepted SSL VPNs as a better remote access alternative to those based on the Internet Security (IPsec) protocol or leased line VPNs.

To date, however, SSL VPN vendors have focused almost exclusively on the flexibility and security benefits of SSL VPNs in providing clientless and client/server application access control. They have done little to ensure that the overall scalability and performance of their SSL VPN solutions match or exceed those of IPsec VPNs.

The problem is that most SSL VPN solutions are packaged as software on a general-purpose Linux platform and thus cannot meet enterprise customer demands in areas including:

- **Performance and user experience** – The ability to nearly match the latency and throughput performance of IPsec VPNs, and improve the end user application performance experience without having to deploy and manage expensive third party solutions.
- **Scalability** – The ability to scale to a large number of concurrent users on a single hardware platform without performance degradation.
- **Security** – The ability to provide not only encryption, but also deep packet inspection and application-level filtering without adversely affecting overall system performance.
- **Universal access** – The ability to consolidate remote users, branch office users, wired and wireless LAN (WLAN) users onto a single SSL VPN platform, without hardware changes.

Performance

SSL VPN solutions delivered on general-purpose platforms have design and architecture limitations that can result in processing bottlenecks that negatively impact latency and throughput. As an example, consider SSL bulk encryption. Most general-purpose SSL VPN solutions perform SSL key exchanges in hardware, using an SSL VPN co-processor, but rely on the main CPU for bulk encryption. Bulk encryption is a CPU-intensive process that puts a heavy toll on system throughput and introduces significant latency.

Application-level throughput is another important factor. As SSL VPNs become more popular, they are being called upon to handle loads that most general-purpose platforms simply weren't designed for. Many SSL VPN platforms are thus being pushed to their practical limit, which may be far below the vendor's stated limit in terms of number of concurrent users supported. The result is they either cease to function properly or function so poorly that it hampers end user productivity.

To achieve an acceptable performance level, customers often find they have to purchase multiple general-purpose SSL VPN boxes and operate them at far below their claimed performance in terms of throughput and concurrent users. This, of course, leads to increased costs – in terms of both initial capital expense and ongoing management – and decreased reliability, due to multiple points of failure.

Some organizations suffer such poor performance that they have to purchase and maintain separate third-party application acceleration solutions. This again leads to higher costs and decreased reliability.

Scalability

Avoiding such costs means finding an SSL VPN solution that is highly scalable. Scalability is measured largely by two factors: maximum number of concurrent users and maximum number of concurrent SSL connections.

While general purpose SSL VPN solutions may claim to scale up to 2,500 concurrent users, their practical limit is likely far less, as noted above. Yet even the 2,500 concurrent user number is far too few for many enterprises and, certainly, service providers.

For a service provider that provides SSL VPN managed services, the ability to scale beyond 10,000 users and hundreds of customers on a single system is essential. The same is true for many large enterprises, given that most Global 2000 companies employ more than 100,000 people. While not all employees need secure remote access, and those that do won't all be logging in at the same time, it's important to remember that SSL VPN use is not limited to employees. In many cases, numerous contractors, partners, suppliers and customers must be given secure access. Given their simple, client-less nature, most IT professionals would prefer to use SSL VPNs to meet the secure access needs of these various groups and individuals. But unless the SLL VPN solution can scale beyond the typical limit of 500 to 1,000 users per system, it is not architecturally or economically feasible for it to support such heavy demands.

In addition, every user community, whether it be different business units, partners, suppliers or customers, have different levels of access privileges. General-purpose SSL VPN solutions can support granular role-based policies for diverse user groups, but they require a separate SSL VPN system to secure each group's user portal. As a result, total cost of ownership (TCO) can skyrocket when more diverse users are added.

Security

The performance and scalability shortcomings of general-purpose SSL VPN platforms also play a part in limiting their security capabilities. Providing proper security requires processing power. On a general-purpose SSL VPN solution, security may be set at the desired level when only 50 users are on the system, but as more and more users are added, performance declines. As a result, the IT manager may be tempted to scale back the level of security until performance is restored to an acceptable level. Clearly, this is not an optimum strategy.

Another problem with general-purpose SSL VPNs is that they are built on off-the-shelf operating systems, and therefore are subject to all the vulnerabilities and security holes associated with those operating systems. Most general-purpose SSL VPNs also lack any advanced security features, such as an integrated firewall and deep packet inspection, which mean customers must add another device to handle such functions – adding complexity, cost and latency. Additionally, general-purpose SSL VPN solutions typically provide transport security only between the client and the SSL VPN appliance, not between the appliance and any attached servers. This leaves the user organization at risk from an internal attack, which account for a significant percentage of all security threats.

In fact, 56% of respondents to the 2005 CSI/FBI Computer Crime and Security Survey reported at least one attack from inside their organization in the previous 12 months.

Universal Access

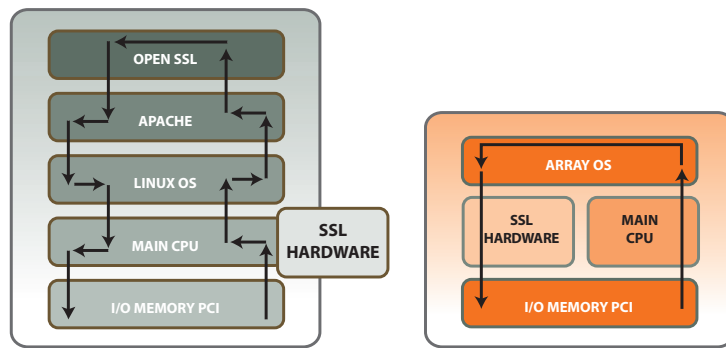
While general-purpose SSL VPN solutions enable access to corporate resources for remote users, they typically do not address access requirements for other enterprise users, such as those attaching to the network from the corporate LAN or wireless LAN. That means the SSL VPN platform becomes yet another area where IT must administer access control lists (ACLs), joining existing ACLs on their LAN and WLAN switches, firewalls and corporate directories. Keeping all these ACLs in sync, with up-to-date information, is a real challenge, and can create security holes if not properly addressed.

Even if general-purpose SSL VPNs claim to support universal access, their limited capacity make them impractical for service provider or enterprise-wide deployments.

Introducing the Purpose-built SSL VPN

The various shortcomings associated with general-purpose SSL VPNs can all be addressed by using a platform built specifically for SSL VPNs. This is the approach Array Networks has taken with its SPX series of high-performance SSL VPN systems.

Array’s SPX systems are based on a purpose-built platform that runs the custom ArrayOS™ operating system. Its optimized and streamlined operations deliver dramatically higher throughput as compared to general-purpose SSL VPNs platforms and lower latency, while allowing for a much higher number of concurrent users and SSL sessions.



General Purpose SSL VPN

Array Purpose-built SSL VPN

Array Purpose-built SSL VPN Advanced Architecture

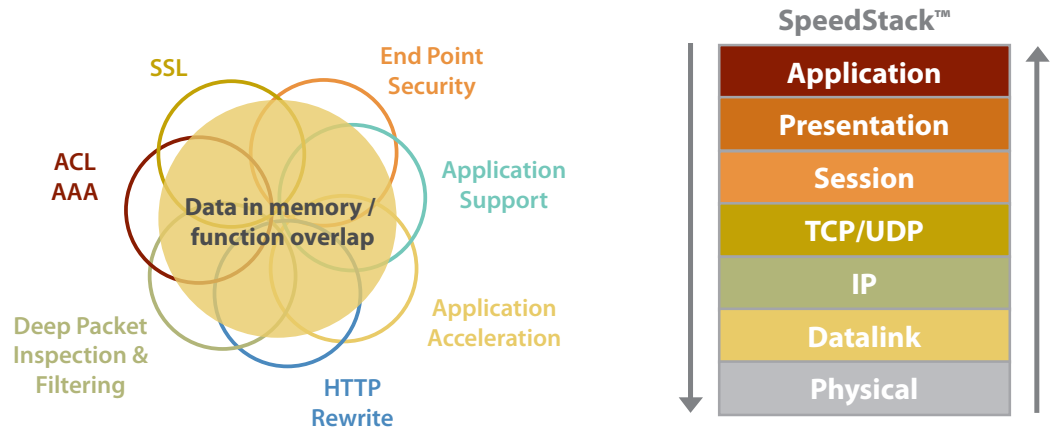
General-purpose SSL VPN	Array Purpose-built Solution
<ul style="list-style-type: none"> • Data must travel through several opensourced interfaces 	<ul style="list-style-type: none"> • Streamlined, linear packet processing
<ul style="list-style-type: none"> • Each interface introduces security holes and vendor implementation dependency 	<ul style="list-style-type: none"> • All data goes through stacks once and are processed in parallel
<ul style="list-style-type: none"> • Processing delay may cause “unpredictable behavior” 	<ul style="list-style-type: none"> • Each processing component is optimized
<ul style="list-style-type: none"> • Difficult to optimize data path 	<ul style="list-style-type: none"> • Custom-made operating system and hardware are built specifically for security processing and performance.

A general-purpose computing platform introduces significant bottlenecks and latency as processes wind their way through multiple layers of processing. Array's custom ArrayOS™ operating system streamlines processing, and ensures CPU-intensive operations such as key exchanges and bulk encryption are performed in hardware.

Superior Performance and User Experience

In fact, its purpose-built platform enables Array to deliver performance, throughput and capacity that's 8 times faster than the nearest SSL VPN platform can offer.

Much of the performance story is owed to both ArrayOS™ and SpeedStack™, which is an Array processing engine that enables TCP overhead functions to be performed just once on behalf of multiple integrated data flows. The diagram below illustrates the integrated features that are able to access data within memory without having to move the data around. If you think of features as being composed of functions, there is a large amount of function overlap. This means, at any given time, a function request may be servicing more than one feature, resulting in more efficient resource utilization and improved performance.



In addition to performing both SSL key exchange and bulk encryption in hardware, Array also integrates compression and connection multiplexing, to improve response time and reduce server workloads by offloading network connection chores. As a result, Array can maintain an average Web page response time of just 2ms with 500 concurrent SSL users, and remain in single digits with tens of thousands of concurrent users.

For those environments where application servers are too expensive to perform low-level TCP network operations, and WAN bandwidths are precious for remote users, Array SPX offers integrated application acceleration including industry-leading TCP connection multiplexing and hardware-based HTTP compression. This level of integrated feature and performance improves server response time and end user experience while reducing costs.

Enhanced Security

Array's strong performance capabilities also mean users don't have to sacrifice security for performance, as is often the case with general-purpose SSL VPN solutions. Array can simultaneously maintain both maximum security and instantaneous user response time.

Like all SSL VPN solutions, Array supports authentication, authorization and auditing (AAA), and end point security with cache cleaning. But Array has also built in numerous security features not found in typical general-purpose SSL VPN solutions.

The security story starts with the proprietary ArrayOS operating system. As a purpose-built OS, ArrayOS has none of the extraneous features and functions inherent in a general-purpose OS like Windows or Linux, and their concomitant security vulnerabilities. ArrayOS is a security hardened OS, with a greatly reduced potential attack surface.

ArrayOS also employs a full reverse proxy architecture, meaning it fully terminates all connections, and establishes new connections to back-end servers. That serves multiple purposes. For one, it helps protect those back end servers from attack; since all connections stop at the Array device, downstream devices can't "see" those back end servers. Array also uses a delayed binding technique that requires the connection to be fully terminated on the Array box before it is passed to the application server. That prevents spoofed IP addresses from connecting to servers, since they will not terminate correctly.

Array SPX also employs a wire-speed stateful firewall and Layer 7 packet inspection, to immediately detect—and drop—anomalous packets. For particularly sensitive applications that require end-to-end security, Array can also re-encrypt sessions between the Array device and back-end servers.

Scalable and Virtualized Universal Access

As explained earlier, large enterprises and service providers require the highest scalability, lowest TCO, and universal access control to support large number of diverse users. Array SPX meets these stringent demands with its industry leading scalability, virtualization and universal access control capabilities.

A single Array system can support up to:

- 64,000 concurrent users
- 100,000 concurrent SSL sessions
- 10,000 SSL transactions per second
- 850M bps throughput
- 256 virtual portals

These 256 virtual portals can each have unique access policies, as well as their own look, feel and security configuration. That means from a single system, an enterprise can give its customers access to its public Web-based ordering system, enable employees to access e-mail, ERP and CRM systems, and give suppliers access to their extranet. And service providers can support up to 256 distinct customers from a single Array system, dramatically cutting their provisioning and operations costs as compared to a general-purpose SSL VPN solution.

With respect to providing universal access control, Array has made a quantum leap as compared to general purpose SSL VPNs. Array SSL VPN can eliminate the need to set up and maintain ACLs on multiple LAN switches, SSL VPN appliances, and separate wireless LAN switches. With Array SSL VPN, a user's access method is supported whether they happen to be accessing the network remotely, from the wireless LAN, or when directly connected to the LAN. Array's comprehensive security policies can be enforced for all users accessing the network, not just for remote users.

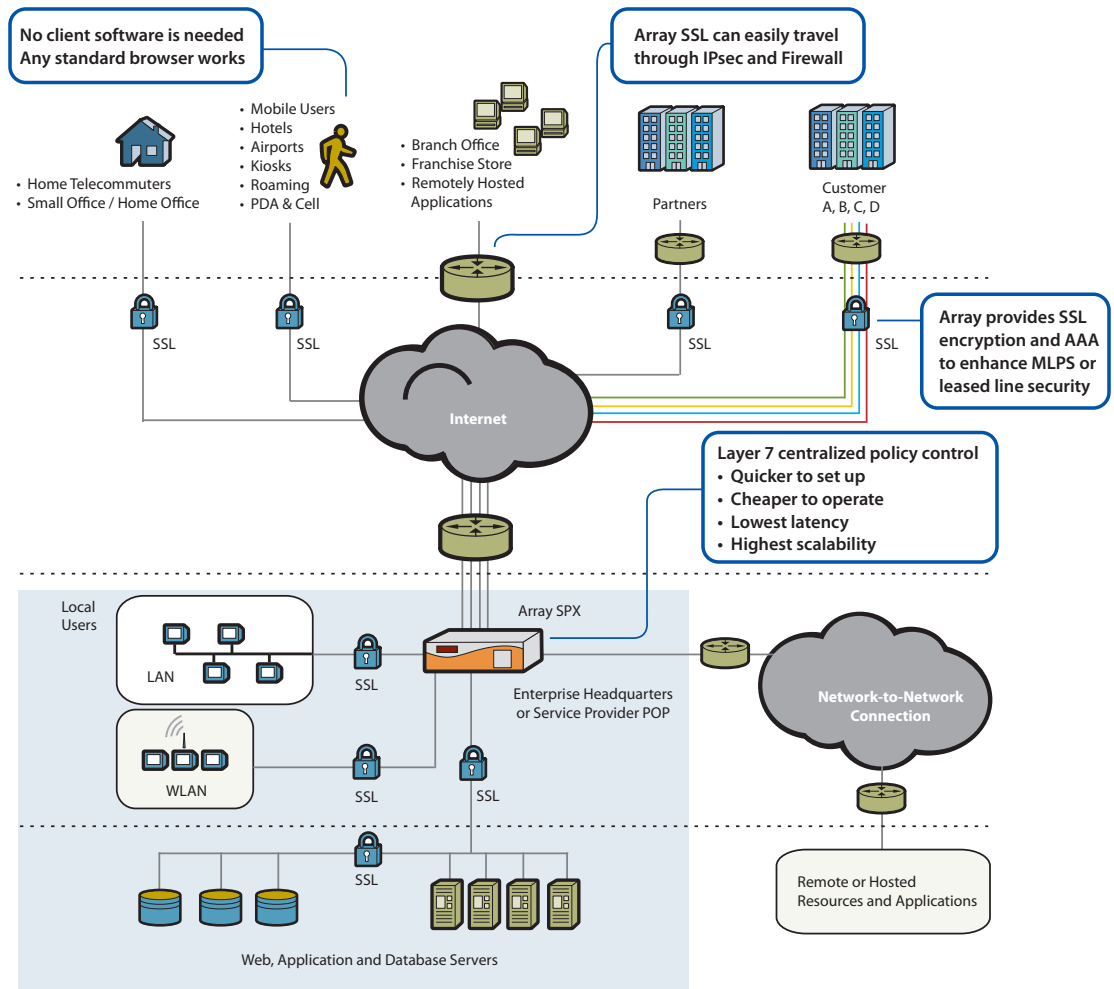
Secure universal access depends on a number of key attributes of the Array SSL VPN system, including:

- Highest number of concurrent users and sessions; without the ability to support a large number of users, it's simply not possible to add users for universal access control.
- Low response time, high throughput, enabling Array to add users for universal access control without slowing down productivity.
- Integrated high performance network and application firewall, enabling an organization to replace its current firewall ACL.
- Up to 256 virtual portals for diverse user groups, making it simpler to support and administer multiple portals for a large number of users, whether they are remote or access the network via the WLAN or LAN.
- Advanced role-based administration, which allows security and network policy responsibilities to be delegated throughout the IT department.

Array is defining the market by enabling an organization to control end-users' access policies and endpoint security in just one place: on the Array SSL VPN. This reduces the costs of administration by eliminating the need to set up and maintain ACLs on multiple LAN switches, firewalls, SSL VPN appliances and separate WLAN switches.

Meeting Your Demanding Requirements

The combination of universal and scalable access, enhanced security and superior performance that Array provides means customers realize significant savings in both cost and time. Being able to meet all remote access requirements with a single system means a lower TCO as compared to employing multiple general-purpose SSL VPN systems. Further cost savings can be realized with the advanced security features that Array offers, and from being able to centrally control all access requirements. At the same time, Array gives customers a foundation upon which to build for future VPN requirements, including site-to-site SSL VPNs.



Higher performance, lower TCO

Array's capacity of 64,000 concurrent users per system, and 100,000 concurrent SSL sessions, makes for a powerful TCO story when you consider cost per user. Array is cost-effective even below 1,000 users, but at higher numbers the cost dramatically decreases. The cost of competing solutions, meanwhile, increases dramatically above 1,000 users because they require more boxes, with the accompanying management complexity. And by offloading tasks from back end servers, Array's connection multiplexing technology reduces server hardware and software costs, further lowering TCO.

When a \$13 billion healthcare company needed to add 5,000 people to its network within two months, it considered numerous VPN and thin client alternatives. It opted for an Array system because it provided significantly higher performance, with higher reliability and greater security than competing solutions. It could also scale to as many as 100,000 users without a hardware upgrade and proved simpler to manage.

The Array system cost the company just \$40 per user to implement, vs. \$200 or more for competing solutions. It also required far less help desk support and was simpler to manage, bringing the total savings from the Array system to more than \$1 million as compared to the alternatives.

Another healthcare organization, Presbyterian Healthcare, deployed the Array SPX to enable doctors and other support staff to securely access patient information. It realized a 100% increase in the number of concurrent users it could handle as compared to its previous solution, along with a 50% improvement in end user response times. Additionally, the organization saw a 400% increase in server capacity, with its Microsoft IIS Web servers handling about 4,000 users per server, up from the previous 800. The organization also realized a 50% reduction in the number of back-end servers it needed.

Similarly, one of the world's largest communications service providers, which provides mobile telecommunications services to more than 100 million customers, was spending \$3.1 million per year on help desk personnel to help its vendor clients manage their IPsec-based VPN access solution. That solution couldn't scale beyond 2,000 users, yet the provider already had a community of 5,000 vendors, which was continuing to grow. Switching to an Array SPX system enabled the company to dramatically reduce its support costs, since client side support and training were no longer required. And the Array system can easily support the company's 5,000 users, with plenty of room to grow.

Array's virtualization features also lead to significant cost savings vs. general-purpose SSL VPNs. Consider the cost savings of supporting all your diverse user groups—employees, partners, suppliers and customers—from the same platform, as opposed to buying and managing separate SSL VPN boxes for each group. For service providers, in addition to supporting up to 256 customers on a single platform, deploying an Array SPX means no longer having to place appliances at the customer premise, a significant cost savings in both the initial expense and ongoing management.

All the while, the Array system doesn't require customers to skimp on security for the sake of performance. Its purpose-built architecture, with the ability to handle many CPU-intensive tasks in hardware, enables the SPX to deliver performance that far surpasses competing solutions. And its integrated Web firewall and deep packet inspection technology means customers don't have to buy additional security products to handle those functions, further reducing TCO.

Security everywhere: Universal access control

Another aspect of TCO has to do with the way organizations handle user access policies, a process that is often riddled with inefficiency, redundancy and complexity. Most organizations are forced to define user access policies at numerous points within the network for the same users, including:

- SSL VPN devices, for remote access
- WLAN switches, for wireless access
- LAN switches, for wired access
- Firewalls
- Proxy servers, such as for E-mail and other applications

Besides being costly to administer, defining policies numerous times in this manner makes it difficult to ensure all policies are in sync, leading to the unintentional creation of security holes.

Array SSL VPN systems enable IT managers to define end-users access policies in just one place, eliminating the need to set up and maintain ACLs on multiple switches and appliances.

The idea of universal access control is especially important now that network access has become ubiquitous, with users logging on to the corporate network from wherever they may be, using myriad devices that may or may not be configured according to corporate security policies. Enterprise users, business partners or guests may become unknowingly infected when surfing the Internet or working remotely, then bring those infected devices directly into the network. Similarly, without proper access controls, internal users on the corporate LAN could open the network to a host of threats when they access the Internet.

These kinds of threats are unacceptable to any organization, but especially those that must meet stringent regulatory requirements to protect corporate data.

Enterprises need a centralized universal access solution that ties together all aspects of the user's identity, device and network permissions, and can uniformly enforce policies, even for groups they do not control.

Array provides just such a solution. Array SSL VPN systems provide user access control no matter whether the user is accessing the network remotely, from the wireless LAN or directly from the wired LAN. And Array's comprehensive security policies can be enforced for all users accessing the network, not just remote users.

Array offers a host of security features, including:

- Client-side integrity checking, to ensure client machines adhere to company security policies. Multiple remediation options are available, including limiting access, directing offending machines to a patch server and restricting access to certain applications or environments.
- Secure access to Web applications, with role-based secure access to intranets and extranets and URL masking, to protect Web applications.
- Secure access to file servers and client/server applications
- Role-based administration, with the ability to delegate administration for different groups to appropriate IT staff.
- Strong authentication, including support for two-factor authentication and integration with Microsoft Active Directory, RADIUS, UNIX NIS or a local authentication database.
- Integrated network and application-layer firewall.

The Array SPX platform itself is also crucial to the notion of providing universal access. Only a platform that is capable of supporting a large number of concurrent users and sessions, with high throughput and low response time, is suitable for handling universal access in a large environment.

Security for thin client applications

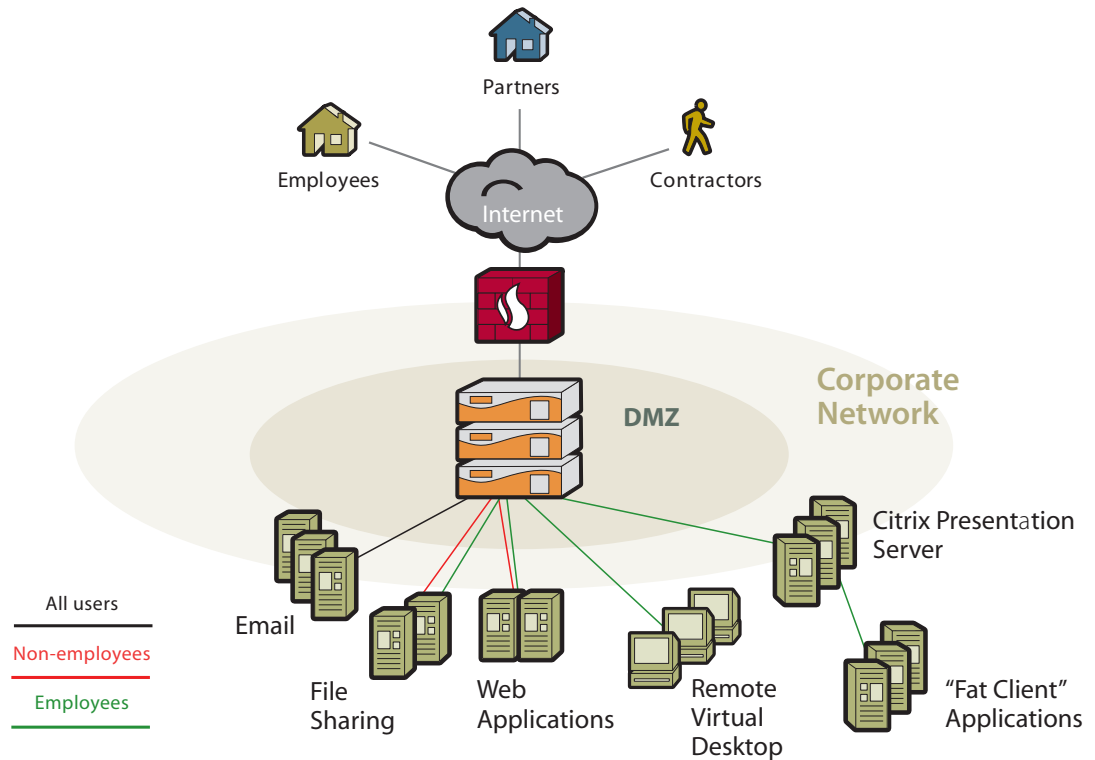
In addition to providing secure access to Web applications, e-mail, file servers and the like, Array SPX also provides a crucial security layer for thin client applications, including Citrix and Windows Terminal Server.

Placing an Array system in front of a Citrix server, for example, reduces an organization's network exposure. Traditionally, remote clients are connected directly to the Citrix server, which is typically resident on the corporate network. That means an intruder who gains access to the Citrix server

could likewise gain access to the rest of the network.

Array’s reverse proxy architecture eliminates that threat. All remote sessions are terminated on the Array system, which then re-establishes a connection with the Citrix server, thus preventing remote users from gaining access to any other network resources. The Citrix server, then, becomes just one more application protected by the Array SPX (see Figure x).

Protection for Your Citrix Servers



The Array SPX also gives administrators granular control of user access rights, right down to the URL, directory or application level. Array also provides enhanced auditing features, covering all user actions from the time they log in to when they log .

A solution for real-time transactions

Many organizations are facing increasingly stringent requirements for fast response time. Whether it’s customers demanding better performance from your customer-facing Web site or internal users pounding on the ERP system, nobody wants to wait to get what they’re after.

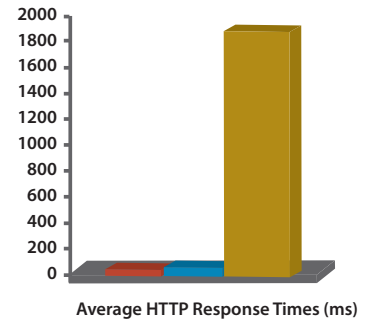
In many instances, time is indeed money. In the financial services arena, for example, fast response time is essential, because huge sums of money are dependent on timely access and trades. Stock prices change literally every second, and can fluctuate greatly from one minute to the next. The problem is compounded by the fact that many traders are not in a traditional office. Rather, they’re on the road, visiting clients, yet they still need fast, secure access to trading applications.

In such a case, an SSL VPN solution is likely to be the preferred option, because it's far simpler than installing and maintaining IPsec software on each client machine. But a general-purpose SSL VPN solution is unlikely to be able to provide the kind of response time – typically less than 5ms – that trading applications require, especially for a large user base.

Array SPX, however, is up to the task, with a response time of less than 2ms for as many as 500 concurrent users.

Banks Key Requirements	Array Purpose-built Solution	Other SSL VPN
100% clientless remote access to web-based applications	Yes	Partially
No more than 5ms Lowest latency	1.7ms	10 times slower
Integrated Symantec End Point Security	Yes	Yes
High Scalability	Yes	No
High Performance	Yes	No

Web Application Response Time



- Array SPX
- Competitor J
- Competitor F

Orders of Magnitude Lower Latency

A foundation for the future

While SSL VPNs are clearly displacing IPsec VPNs for remote access, IPsec is still widely used for site-to-site VPN connectivity. In a site-to-site configuration, more users are likely to be connected at the same time to a single VPN device than in a remote access configuration, which means the system has to be highly scalable.

With its ability to support 64,000 concurrent users today, and 256 virtual portals, Array is well-positioned to take this next step in the evolution of SSL VPN technology.

Summary

SSL VPN technology has won the battle with IPsec for remote access requirements, with Gartner predicting that by 2008, SSL VPNs will be the primary remote access method for most business use. But as SSL VPN use increases, so do the demands for access, security and performance.

General-purpose VPN solutions are simply not equipped to meet these growing demands, falling short in terms of performance, scalability, security, end user experience and the ability to provide universal access.

Only a platform built from the ground up to meet SSL VPN requirements can meet the demands of enterprises and service providers. Array's SPX system, with its proprietary ArrayOS operating system, has the horsepower to meet even the most demanding needs, with support for as many as 64,000 concurrent users and 100,000 SSL sessions. And its virtualization capabilities, with support for 256 distinct portals, are unmatched in the industry.

Such features position Array not only as a sound choice to meet today's requirements, but as the only platform that can grow with you to meet the VPN requirements of tomorrow.

About Array Networks

Array Networks Inc. is a global leader in enterprise secure application delivery and universal access solutions for the rapidly growing SSL VPN and application delivery controller (ADC) markets. More than 3,500 customers worldwide – including enterprises, service providers, government and vertical organizations in healthcare, finance, insurance and education – rely on Array to provide anytime, anywhere secure and optimized application access. Industry leaders including Deloitte, Red Herring, Gartner, and Frost and Sullivan have recognized Array as a market and technology leader.

Array is headquartered in Milpitas, California with sales offices around the world. The company has approximately 60 resellers and VARs worldwide.

For more information, please visit www.arraynetworks.net or call **1-866-MY-ARRAY**.