White Paper

Array Purpose-Built SSL VPN

Fast, Secure and Scalable Secure Access

AG Series Secure Access Gateways (SSL VPNs)

Introduction

Over the years, organizations have turned to virtual private networks (VPNs) based on Secure Sockets Layer (SSL, a.k.a. TLS) technology to solve their remote and access needs. The rise of personal and corporate-owned smart mobile devices has reemphasized the need for secure mobile access to corporate data and resources. According to industry analysts:

"The consumerization of smartphones and the proliferation of smartphones, iPads, netbooks, and other mobile devices connected 24/7 to the Internet are driving companies to reassess how critical infrastructure in HQ, branch offices, remote offices, and data centers is protected from malware." Infonetics Research[1]

"The changing nature of enterprises and the increasing number of mobile devices that connect to enterprise networks, as well as "consumerization of the enterprise," are imposing new demands on the way organizations approach network security." ABI Research[2]

In response to the increasingly mobile and diverse nature of users – including non-employees such as contractors and guests, who typically utilize their own laptops with varying levels of security – enterprises and service providers are looking to make secure application and network access an integral part of the resources they provide to end users.

In general, SSL VPNs enable users to securely access data and applications from multiple locations and computing devices, offering granular, identity-based access controls. However, in recent years SSL VPNs have increasingly come to be offered as a function that is tacked onto firewalls or next-generation firewalls. Integration with another security appliance that relies upon SSL processing resources can adversely impact the performance required for a positive end-user experience as well as the scalability that large-scale deployments demand.

An Integrated SSL VPN is not Sufficient

SSL VPN solutions leverage the same SSL encryption used by browsers to encrypt traffic and provide data confidentiality and data integrity. Over the past five or more years, corporations have generally accepted SSL VPNs as a better remote access alternative to those based on Internet Security protocol (IPsec) or leased line VPNs.

Many SSL VPN vendors, however, 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 the needs of their customers.

[1] http://www.businesswire.com/news/home/20120308006173/en/Infonetics-Research-Network-Security-Market-Set-Stronger

[2] https://www.abiresearch.com/market-research/product/1006059-world-enterprise-network-and-data-security/

Further, many SSL VPN solutions are offered as a module or option on firewalls and NGFWs, and thus cannot meet enterprise customer demands in areas including:

- **Performance and user experience** – The ability to achieve latency and throughput performance, and improve the end-user experience thus protecting end-user productivity.
- **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.

Performance

Beginning a few years ago, the cyber-security industry moved to 2048-bit encryption, which, while vastly more secure than the previous 1024-bit standard, consumes 5 times more processing power. Incorporating SSL VPN into another compute-intensive product like a firewall or NGFW can create resource contention that inevitably impacts performance of the SSL VPN, and thus the user experience and worker productivity.

For example, consider SSL bulk encryption. Most add-on 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, especially with 2048-bit keys.

Application-level throughput is another important factor. SSL VPNs are being called upon to handle loads that most integrated platforms simply weren't designed for. Many integrated 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, throughput, or both. 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 integrated SSL VPN appliances and operate them at far below their claimed performance in terms of throughput and concurrent users. This, of course, leads to increased costs – 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. In addition, highly complex SSL VPN configurations with more layers of security, rules, virtual portals for different communities of interest, etc. can also impact scalability

While add-on SSL VPN solutions may claim to scale up to 25,000 concurrent users, their practical limit is likely far less, as noted above. Yet even the 25,000 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 25,000 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 use of an SSL VPN is not limited to employees. In many cases, numerous contractors, partners, suppliers and customers must be given secure access. Given their simple, clientless 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 SSL VPN solution can scale beyond the typical limit on 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, will require different levels of access privileges. Integrated firewall/SSL VPN solutions can support granular role-based policies for diverse user groups, but they may require a separate appliance to secure each group's user portal. As a result, total cost of ownership (TCO) can skyrocket when more diverse user populations are added.

Security

The performance and scalability shortcomings of integrated firewall/SSL VPN platforms also play a part in limiting their security capabilities. Providing proper security requires processing power. On an integrated 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 will decline. 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 integrated SSL VPNs is that they may be built on off-the-shelf or open-source operating systems like OpenSSL, and therefore are subject to all the vulnerabilities and security holes associated with those operating systems. Most integrated SSL VPNs also lack advanced security features, which means customers must add another device to handle such functions – adding complexity, cost and latency. Additionally, integrated firewall/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 accounts for a significant percentage of all security threats. (According to IBM's 2016 Cyber Security Intelligence Index[3], 60% of all attacks are attributable to insiders, either maliciously or inadvertently.)

Introducing the Purpose-built SSL VPN

The various shortcomings associated with integrated firewalls/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 AG Series high-performance SSL VPN appliances.

Array's AG Series dedicated appliances are based on a purpose-built platform that runs the custom ArrayOS™ operating system. Its optimized and streamlined operations deliver dramatically higher throughput and lower latency as compared to add-on SSL VPN platforms, while allowing for a much higher number of concurrent users and SSL sessions.

A multi-purpose, integrated 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.

[3] http://www-03.ibm.com/security/data-breach/cyber-security-index.html

SSL VPN Architecture Comparison

	SSL VPN Integrated with Firewall	Array Purpose-built Solution
2048-bit SSL encryption and bulk encryption require more processor horsepower	Processor resources shared with firewall functions	Dedicated processor resources assure high performance
Number of concurrent users increases due to employees, partners, contractors and others	Typically limited in number of concurrent users; additional hardware required to secure other users	Supports up to 130,000 concurrent users on a single appliance, reducing management overhead & TCO
Strong security requires processing resources in order to maintain performance levels	Resources shared with firewall may require scaleback of security settings to achieve performance	Dedicated processing resources allow highly customized security without degrading performance
Open-source or off-the-shelf OS may lack advanced security and be subject to vulnerabilities	Additional hardware may be required for advanced security; servers may be at risk	Custom-made operating system and hardware are built specifically for security processing and performance

Superior Performance and User Experience

In fact, its purpose-built platform enables Array to deliver performance, throughput and capacity that's eight times faster than the nearest competing SSL VPN platform (integrated or standalone) can offer.

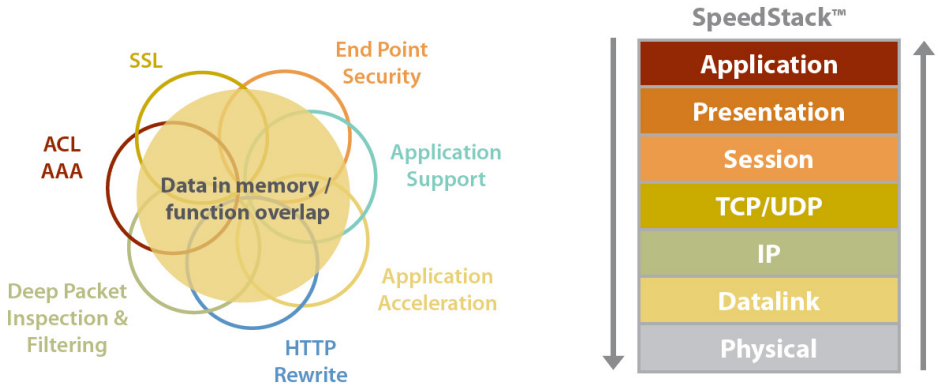
Much of the performance story is owed to both ArrayOS and SpeedStack®, which is an Array processing engine that enables TCP overhead functions to be performed just once on behalf of multiple integrated data flows. The diagram below illustrates the integrated features that are able to access data within 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.[4]

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

From a quality-of-experience perspective, in the absence of a high-performance SSL VPN solution, office workers who are accustomed to LAN speeds could get frustrated and give up while attempting to work remotely over the WAN. Additionally, these workers' lack of experience with VPN solutions would require significant training and support to overcome inevitable login and navigation problems. Both problems can be mitigated through the AG Series.

[4] See Appendix A for performance testing results on all AG Series models.



Enhanced Security

Array's strong performance capabilities also mean users don't have to sacrifice security for performance, as is often the case with integrated 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 integrated 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 security hardened, with a greatly reduced potential attack surface. In addition, the AG Series includes a proprietary SSL stack that has proved immune to the vast majority of vulnerabilities reported for OpenSSL – the foundation for almost all competing SSL VPN products.

ArrayOS 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 appliance before it is passed to the application server. That prevents spoofed IP addresses from connecting to servers, since they will not terminate correctly.

Array's AG Series 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, sessions between the Array device and back-end servers can also be re-encrypted.

Scalable and Virtualized Universal Access

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

A single Array system can support up to:

- 130,000 concurrent users
- 3 Gbps 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 an add-on SSL VPN solution.

With respect to providing access control, Array has made a quantum leap as compared to general-purpose SSL VPNs. Array's 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's SSL VPN, a user's access method is supported whether they happen to be accessing the network remotely or from the wireless LAN, on a corporate-issued device or personal mobile device (if allowed).

Secure access depends upon a number of key attributes of the Array SSL VPN solution, including:

- Highest number of concurrent users and sessions, coupled with low response time and high throughput, enable Array to support large numbers of users without slowing down productivity.
- Integrated high-performance network and application firewall, enabling an organization to replace its current firewall ACLs.
- 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 they access the network via smart mobile device, etc.
- Advanced role-based administration, which allows security and network policy responsibilities to be delegated to the appropriate personnel throughout the IT department.

Array has defined 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 scalable access, enhanced security and superior performance that the AG Series 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 integrated SSL VPN systems. Further cost savings can be realized with the advanced security features that Array offers, and from being able to centrally control access requirements. At the same time, Array gives customers a foundation upon which to build for future VPN requirements.

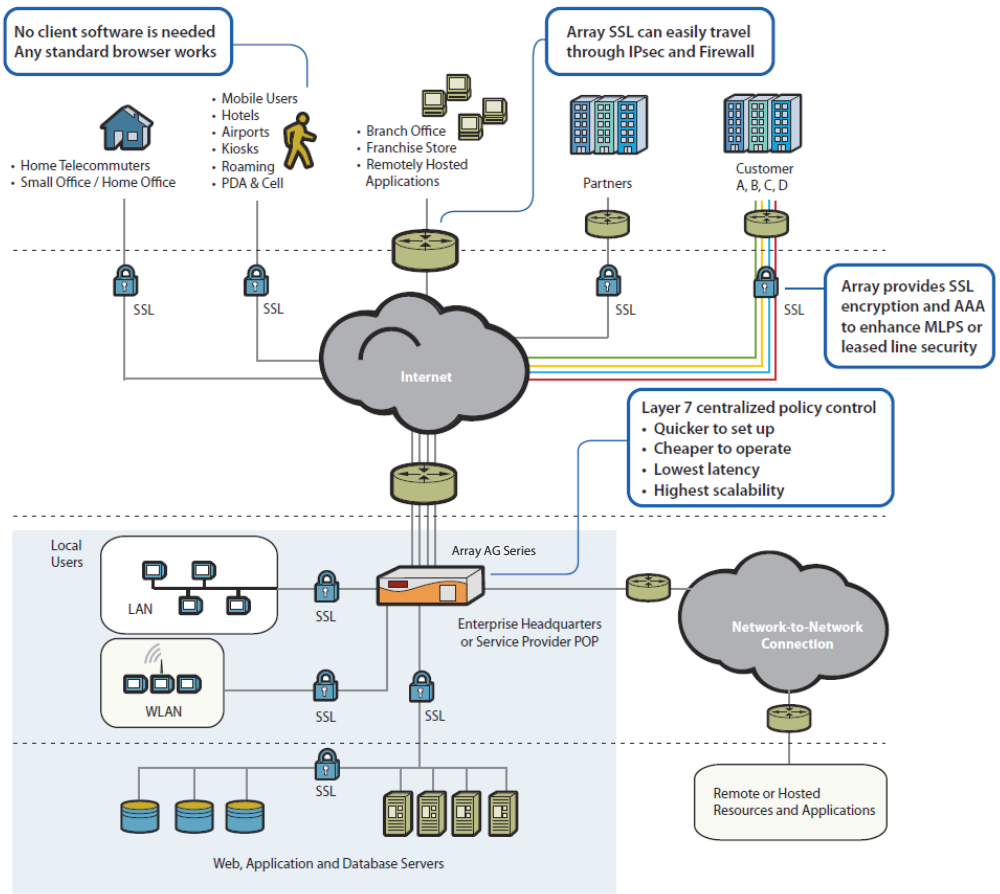
Higher performance, Lower TCO

Array's capacity of 130,000 concurrent users per system makes for a powerful TCO story when you consider cost per user. The AG Series 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 usually require more appliances, 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.

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 an Array SSL VPN 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 response times for end users. 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 concurrent users, yet the provider already had a community of 5,000 vendors, which was continuing to grow. Switching to an Array SSL VPN 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 vendors, with plenty of room to grow.

Array's virtualization features also lead to significant cost savings vs. integrated 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 AG Series 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 AG Series to deliver performance that far surpasses competing solutions. And its integrated Web firewall technology means customers don't have to buy an additional security product to handle those functions, further reducing TCO.

Security Everywhere: 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 email 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 solutions 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.

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.

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

Enterprises need a centralized 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 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 built-in one-time password, third-party multifactor authentication suport, and integration with Microsoft Active Directory, RADIUS or a local authentication database
- Integrated network and application-layer firewall

The Array AG Series platform itself is also crucial to the notion of providing secure 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 secure access in a large environment.

Security for Thin Client Applications

In addition to providing secure access to Web applications, email, file servers and the like, Array AG Series 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 AG Series.

The Array AG Series 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 out.

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 external 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 an integrated SSL VPN solution is unlikely to be able to provide the kind of response time – typically less that 5ms – that trading applications require, especially for a large user base.

Always-on, Site-to-Site Connectivity

While SSL VPNs have clearly displaced 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.

Array's AG Series supports Site2Site, a hub-and-spoke SSL VPN tunneling solution to support site-to-site VPN connectivity, and, with its ability to support up to 130,000 concurrent users 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 long since won the battle with IPsec for remote access requirements, with Gartner predicting back in 2008 that SSL VPNs would be the primary remote access method for most business use. But as SSL VPN use has increased, and mobile devices have entered the picture, demands for access, security and performance have increased as well.

Integrated firewall/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.

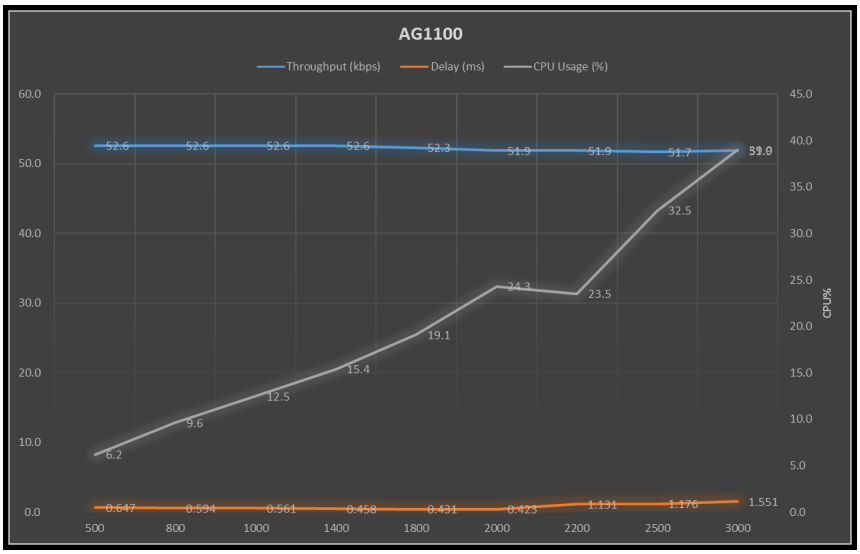
Only a platform built from the ground up to meet SSL VPN requirements can meet the demands of enterprises and service providers. Array's AG Series secure access gateway, with its proprietary ArrayOS operating system, has the horsepower to meet even the most demanding needs, with support for as many as 130,000 concurrent users. And its support for 256 distinct portals is 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.

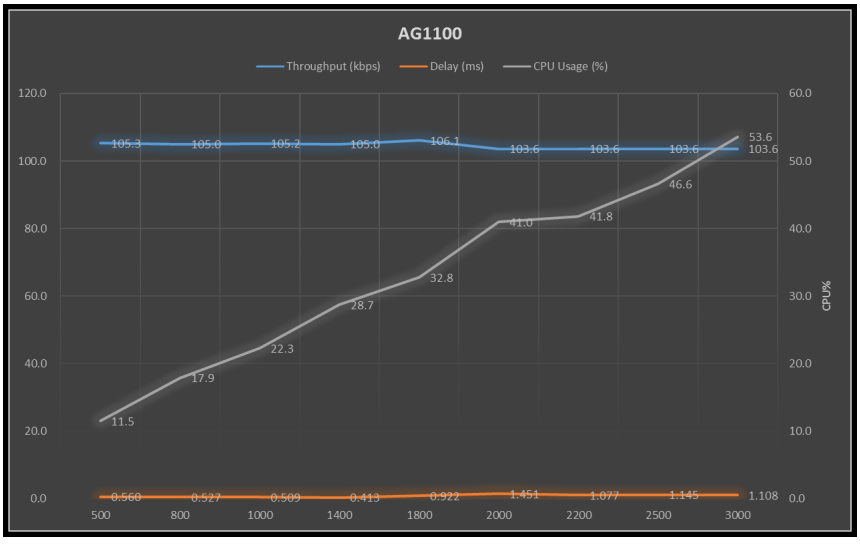
Appendix A

In-house testing proves the robust performance and throughput of Array AG Series SSL VPN appliances. Following are graphical test results for a range of AG Series models.

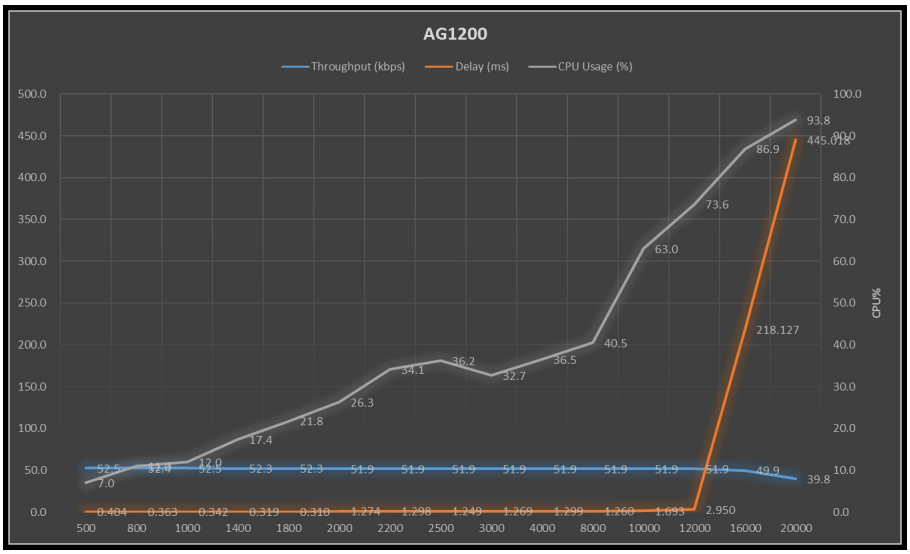
AG1100 at 50kbps throughput per user:



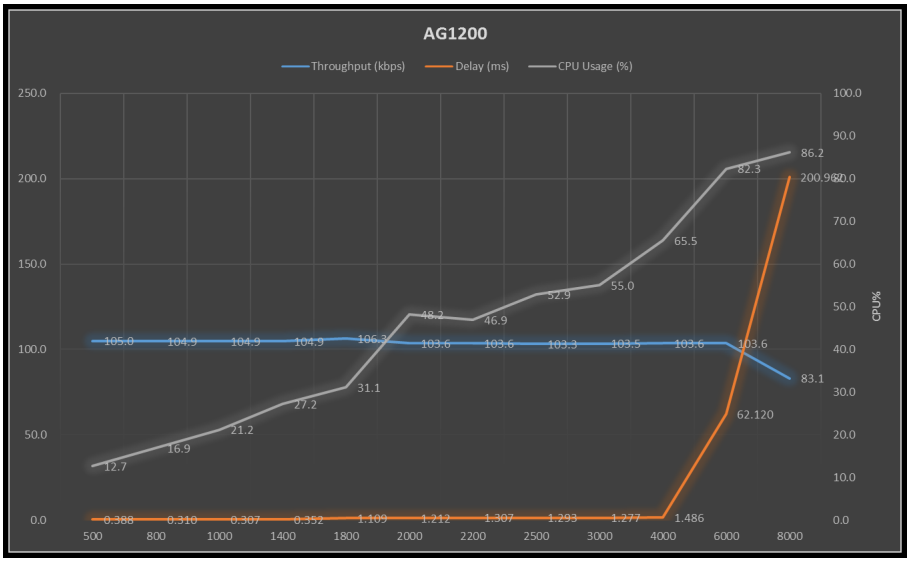
AG1100 at 100kbps throughput per user:



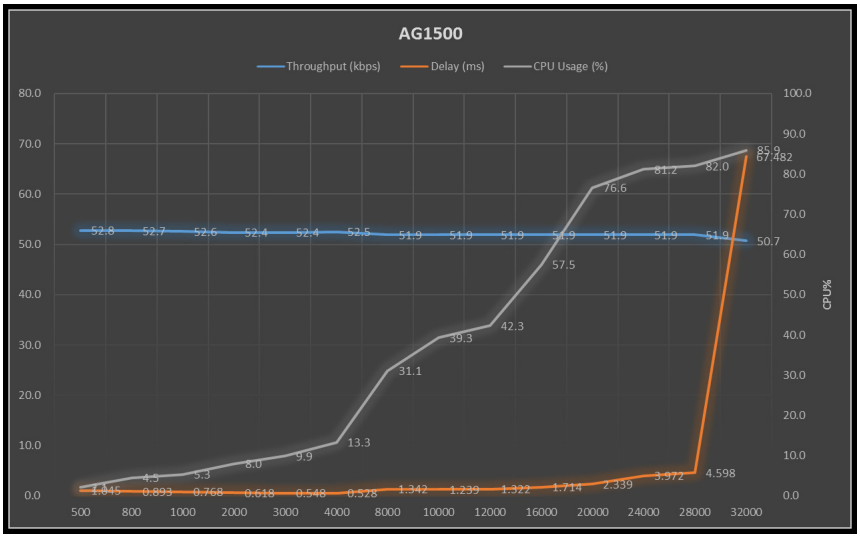
AG1200 at 50kbps throughput per user:



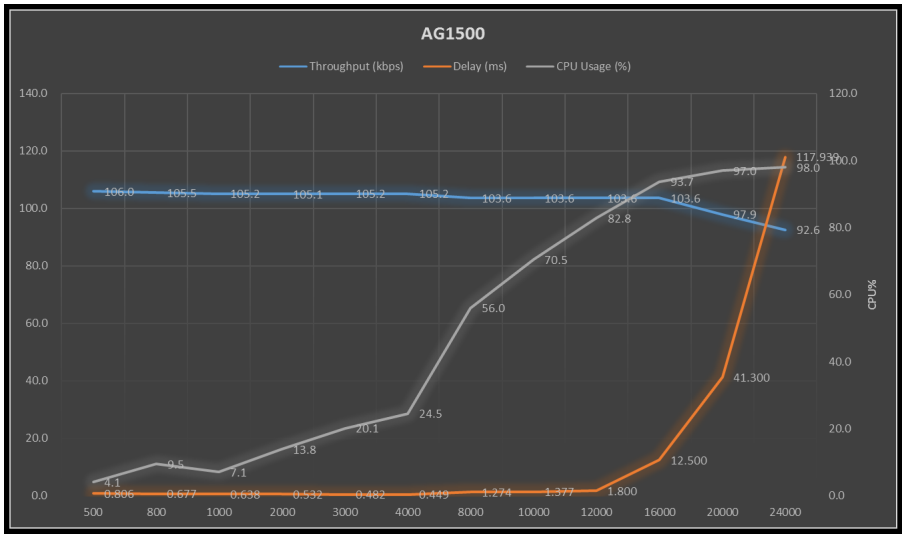
AG1200 at 100kbps throughput per user:



AG1500 at 50kbps throughput per user:



AG1500 at 100kbps throughput per user:



About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 250 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

Feb-2017-rev. a