

Securing Wireless LAN Campus

Array Networks SSL VPN Solution Brief



Benefits of Array Industry-leading Security:

- WLAN security breach incidents are cut dramatically within a global 500 company's WLAN campuses.
- 17,000 employees, partners and guests can access the applications that they are authorized to.
- No security holes are left no matter who the users are and what devices they use.
- Zero vulnerability within port 443 traffic, which would otherwise go right through the company's firewalls unprotected.

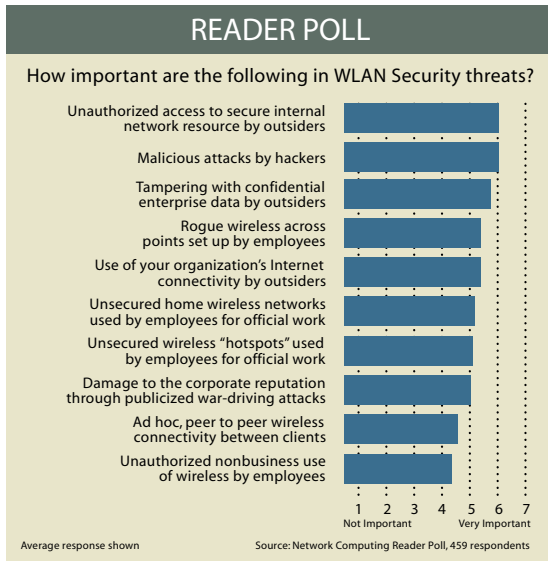
Benefits of Array Industry-leading Performance:

- Array requires 80% less equipment than the nearest competitor to support 17,000 users in high availability configuration, with still plenty of headroom to grow.
- Annual Cost Savings: \$8.5 Million due to Array's virtualization architecture that consolidates and simplifies IT infrastructure.

Security Threats Within A Global 500 Company’s WLAN Campus

More and more enterprises are recognizing the value of Wireless LAN (WLAN) technology. Improved productivity and mobility can have a very positive impact on overall business profitability.

While this mobile and convenient access has driven immense benefits, it has also introduced corresponding risks. According to Network Computing most recent survey of 459 IT managers, 70% of them cited WLAN security as insufficient:



As a practical example, a global 500 company has deployed 10 large WLAN-enabled campuses that provide employee, partner and guest access to its network and the Internet. After seeing tremendous user adoption within less than 3 months, a number of security breaches and Internet attacks have caused significant IT infrastructure damage and loss of productivity within the company.

The Challenge

To support a large user community of 17,000, the company has found no shortage of challenges:

- **WLAN Security Risks:** Even the latest 802.11xi WLAN equipment is not secure enough and has been compromised multiple times.
- **No Enforced End Point Security:** Because partners and guests’ laptop computers are not company’s assets, this makes it impossible to enforce security policies on end user devices. Installing software on every laptop is always an option, but an extremely expensive one that requires ongoing support and maintenance. Still, many partners and guests simply do not follow the company’s IT and security guidelines.
- **No Granular Access Control of Applications:** Existing IPsec solutions provide full network access, leaving file sharing and CRM applications vulnerable to partners and guests.
- **Expensive Distribution, Training & Support of IPsec Client Software:** This cost item alone amounts to \$6M a year.
- **A Plethora of End User Portals:** The Company is using many separate web servers to provide a number of end user portals - some for employees, some for the intranet, some others for the extranet, yet some others for guests. This creates management and security enforcement headaches when supporting 17,000 users.
- **No Room to Grow:** The current IPsec VPN solution cannot scale beyond 8,000 users. Yet the user community of 17,000 will continue to grow. Providing network access to a large contractor/partner community is mission critical to the company’s business operations. Having a solution with industry leading security, performance and scalability becomes imperative.

Array SSL VPN Solution

After a thorough evaluation of many solutions, the Array SSL VPN is selected for its industry leading security, performance and scalability features. As shown in the diagram below, the Array SSL VPN is deployed behind WLAN access points and a router to secure WLAN and provide granular access control based on user identity.

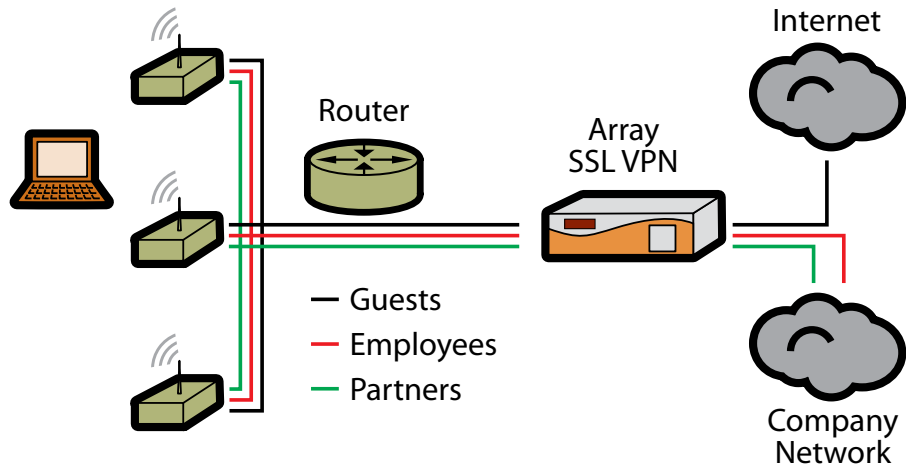


Figure 1 Array SSL VPN Augments WLAN Security

Specifically, the following features are deployed to meet the company’s challenges:

Features	
Integrated SSL VPN Firewall	Protects against generic network attacks that are hidden in SSL encrypted traffic.
End Point Security	Secure non-company laptops without needing client software. Leaves no security holes on user laptops.
Granular Access Control	Granting application access privileges based on user identity
Layer 3 VPN	Full network access is available for those who need it, but without requiring a client software like IPsec does.
Virtual Portal	Consolidates multiple web portals and improves security.
Performance & Scalability	64,000 concurrent SSL VPN users on a single appliance, easily satisfies the current 17,000 users need with plenty of headroom to grow.

Integrated SSL VPN Firewall & Content Filtering

Like any conventional firewall, the company's existing network-based firewall passes SSL or IPsec encrypted traffic through without providing any deep packet inspection or DOS protection.

Array SSL VPN is integrated with a high performance stateful reverse proxy firewall and content filter that:

- Sustains wire-speed packet inspection without performance degradation (see diagram below);
- Protects against DDoS prevention (SYNattack, Smurf, Xmas tree, etc);
- Performs content inspection (NIMDA, forceful browsing, profile)
- Denies by default (SQL Worm, scans);
- Provides a full audit log in WELF format for reporting

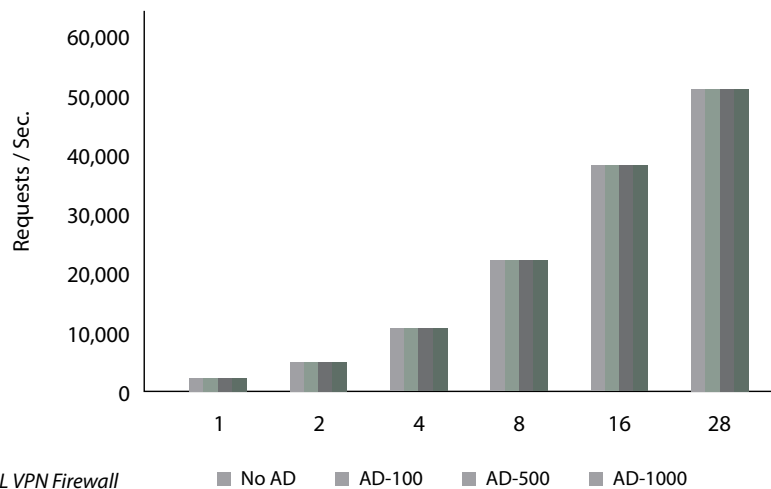


Figure 2 Array SSL VPN Firewall

End Point Security

Array SSL VPN supports several end point security features:

- **Host Checking:** Verifies Antivirus, Firewall, OS version, and service packs and other conditions on user laptops, provides a 3 dimensional authorization capabilities, and does not require administrative rights. This is very easy to manage as shown in the diagram below.
- **Cache Cleaning:** Ensures that web browser information is erased or removed including cookies, history, auto-complete, stored passwords, temporary and downloaded files. This feature can be automatically triggered based on session termination, browser closure, or Per-session with idle timeout. It supports Windows 2K, Windows XP, Windows 98, Windows ME, Windows NT 4, RedHat Linux 9 and Mac OS X
- **Virtual Desktop:** Limits users' ability to store confidential information on unauthorized laptops by wiping all stored information when the session is over. Stores information in an encrypted vault. Controls local resources and can download session data into a local drive. The diagram below shows that a fully secure laptop leaves no traces of usage after the session is over. This feature is particularly useful for those laptops that are used by company visitors such as partners and guests.
- **2-Factor Authentication:** Array SSL VPN seamlessly works with the company's existing authentication mechanism including SecurID, Smart Card and ActivCard.

Granular Access Control

One of the advantages offered by the Array SSL VPN to secure WLAN is the ability to provide both network access (to the corporate network) and Internet access using the same APs. Regular employee access usually requires access to the corporate network, and from there employees may access the Internet.

On the other hand guest access should not be allowed under any circumstances for access to the corporate network, and should be only allowed to the Internet directly.

The Array SSL VPN provides such access control by using the same set of APs so the company can protect their existing investment. On the front-end different virtual portals are configured for guest and employee access. On the backend virtual routing is used to assure that guests access the Internet directly without passing through the corporate network. The following diagram shows the actual deployment scenario within the WLAN campus.

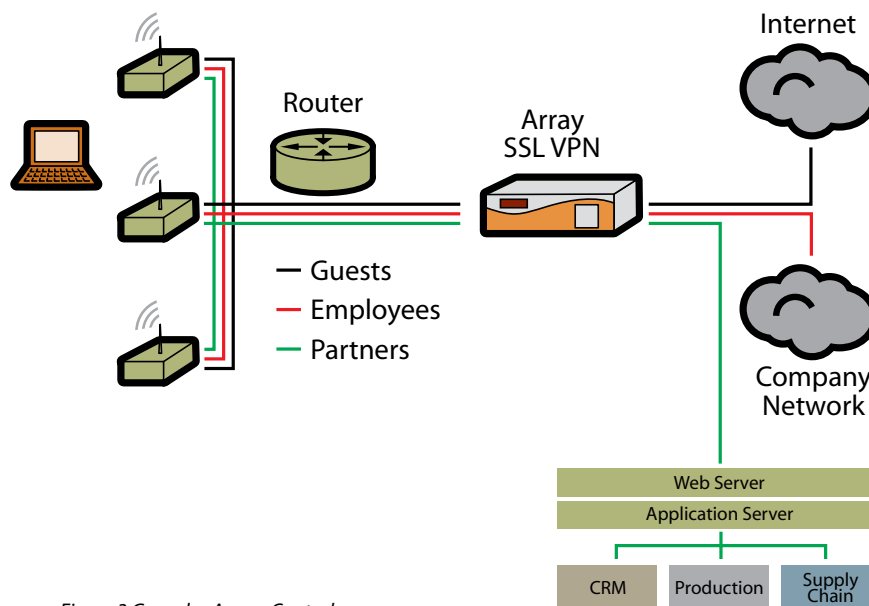


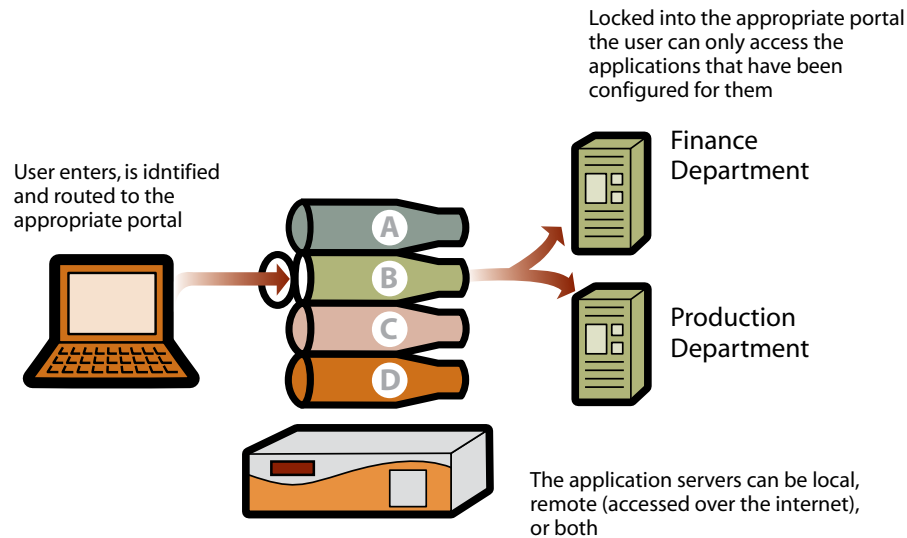
Figure 3 Granular Access Control

Layer-3 VPN

Normally users do not require full network access; they can simply access any web-based applications through their web browsers. However some special users require full layer-3 access. The advantage of using Array layer 3 VPN is that it does not need client software like existing IPsec VPNs do. Those users can simply click a button (see below) and a layer-3 VPN client will be downloaded immediately. And the layer-3 VPN client will be automatically updated in the future, requiring zero maintenance and support on user laptops.

Virtual Portals

The Array SSL VPN is configured into multiple virtual portals, each for a different community - employees, partners and guests who will access the WLAN campus. Multiple virtual portals are also configured for different departments for employees-finance, production, or sales & marketing.



Performance & Scalability

The Array SSL VPN is a true enterprise-class solution. In fact, it is the only solution that can support the following performance on a single piece of hardware:

- 64,000 concurrent user sessions (not TCP connections)
- 10,000 SSL transactions per second
- 850Mbps near wire-rate throughput
- 100,000 SSL sessions

After deploying Array SSL VPN, the company's most recent performance tests (using OWA as a metric) demonstrates the following results:

- Handling 800 Mbps with 1,000 concurrent users
- Average response time of 19ms
- Average 15 transactions/sec per user, at 10,000 concurrent user level

Conclusion

Widespread adoption of WLAN increases a global 500 company's mobility, flexibility and productivity. However, this also introduces significant security risks since WLAN security does not sufficiently protect company resources against user abuses.

Protecting WLAN campus by treating it as a remote access point, and using SSL VPN to improve security and provide granular access control has been a proven solution with significant benefits.

Array SSL VPN not only provides uncompromised security that goes beyond WLAN encryption, it is also the highest performing and scalable solution available on the market.

About Array Networks

Founded in 2000, Array Networks is a leading provider of high-performance, secure universal access solutions. Array delivers product lines that address the rapidly growing SSL VPN market as well as the application acceleration market. More than 500 customers including enterprises, service providers, government and vertical organizations in healthcare, finance and education rely on Array to provide anytime, anywhere secure and optimized access. Array provides the world's fastest and most scalable SSL VPN products on the market today. Array's technology performs 8 times faster and scales 12 times higher than its nearest competitor. As a result, no other company can deliver high-performance SSL VPN solutions at a comparable cost. Array has been recognized by industry leaders including Deloitte, Red Herring, and Synergy 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**.