

Array's Multi-Layer Approach to Security

White Paper



Learn about Array SSL VPN multi-layer security:

- Physical, logical, network & application layer defenses
- End-point security
- Authentication, authorization & auditing
- Deep packet inspection & request processing
- Web resource mapping
- Encryption & authentication
- Third-party audits

Introduction

Array employs a defense in-depth approach to security with a multi-layer SSL firewall built on Array's proprietary SpeedStack™ which is a networking architecture where every single flow (associated stream of packets) is inspected in both directions. Inspection of packets is done at multiple layers of the OSI stack. However, the beauty of the architecture lies in the underlying implementation where no data is ever copied or otherwise moved around, and all duplication of work is eliminated. If a certain piece of work has already been done at a certain layer and the information is required for a subsequent piece of work at a different layer, the information is made available without the second layer needing to repeat the same work.

The fundamental principle that Array operates on is a “default deny” architecture where nothing goes through the box unless the administrator configures it. This ensures protection against a variety of attacks such as SQL worms and scans because typically the only open port is SSL. The data is encrypted/decrypted using a hardware based SSL accelerator that does bulk encryption and key exchange handling in its hardware ensuring that there is no deterioration in performance even at rates exceeding 10,000 SSL transactions per second delivering throughputs over 850 Mbps.

The following section describes the various defenses that Array employs at different layers of the TCP/IP stack.

Physical Layer — Array supports up to four physical interfaces (Gigabit copper or fiber), which allows customers to have extranet, intranet, DMZ and management networks with physical separation between them.

Logical Layer — ArrayOS supports 256 VLANs and multi-nets, which provide a logical layer separation between different networks. Array's virtualization technology allows up to 256 instant DMZs to be deployed on the same architecture. Each virtual portal is designed such that data belonging to one customer is completely separated from another customer on a different network. Array's virtualization management toolset allows service providers to manage these as a customer unit and make available SSL VPN services to a much larger base of users at a more affordable cost point of \$20/month per user. Array's massive scalability gives the service providers instant ROI within a period as short as 3 months.

Network Layer Defenses — Array employs a wirespeed ACL layer that is able to provide firewall functionality of allow/deny rules based on source/destination port/IP/network combinations, without performance degradation regardless of whether there is a single rule configured or 1000 rules configured. Built on top of it is a full reverse proxy that cleanly separates all external packets from internal packets.

As part of the WebWall® feature, several important mechanisms are embedded in the ArrayOS Speed-Stack to prevent DoS attacks:

1. Connections between the client and the proxy are never the same as connections between the proxy and the server. The server is guaranteed a clean connection.
2. ArrayOS TCP/IP stack imposes strict rules as to what types of packets and connections are accepted. Rogue (anomalous) packets are immediately dropped.
3. Syn-Floods and like attacks have little or no impact. The Array architecture has been tested to sustain over 80,000 SYN/sec. By comparison, the Cisco PIX firewall fails to perform at 3,000 SYN/sec levels.

4. Rather than rely on vendor updates for protection against the latest worms, viruses, or attacks, the ArrayOS captures all rogue packets and drops them. There is no need to wait for a vendor fix.
5. IP Spoofing is protected by use of "delayed binding". This technique requires the connection to be fully terminated on the Array box before it is passed to the inside server. Spoofed IP addresses cannot correctly terminate a connection and thus will never access the servers.

Any abnormal events detected by WebWall are audited through the logging system.

Application Layer Defenses — includes a suite of Client Side Security applications, authentication, authorization and deep packet inspection for non-conforming content.

End-Point Security

Prior to even presenting the login screen to the user, a variety of client security related checks are conducted. These include scans for ensuring that appropriate personal firewalls, anti-virus software, browsers, operating systems with required service packs, patches etc. are deployed. Multiple remediation options are available to the administrator including limiting access to a secure desktop, directing to a healing server to download the required fixes, providing access to certain applications or environments etc.

The Array SPX's host integrity checking tool is downloaded automatically to the remote machine prior to the user being allowed to login. The tool is configured by the administrator to check status/acceptability of virus scanning tools, appropriate personal firewall, suitable versions of browser with the up-to-date service pack, OS (version and service pack), and other controls such as presence or absence of registry/file parameters. If the remote machine doesn't have the required privileges, a virtual secure desktop with limited access to the file system is created to give an encrypted vault like environment to allow limited access to the network. These tools as well as Layer 3 VPN tool prohibit end user modification.

Array Networks supports the following personal firewalls:

- Norton Personal Firewall,
- ISS RealSecure Desktop Protector,
- Sygate Personal Firewall/SSA,
- ZoneAlarm Personal Firewall,
- Internet Connection Firewall (ICF), and

The following anti-virus solutions are supported:

- Norton Antivirus (Corporate, 2000, 2003/2004),
- ETrust Anti-Virus,
- McAfee Virus Scan (4.0-7.0),
- Panda AntiVirus (4.0-7.2),
- PC-Cillin (2002, 2003).

User Authentication, Authorization and Auditing

One of the critical features offered by Array's SSL VPN is that it presents data only to authenticated users if and only if they are authorized to access a particular piece of content. Array is not only able to authenticate but is also able to authorize users based on information retrieved from client certificates using flexible rules configured by the administrator. Array can authenticate users with an external LDAP, Microsoft Active Directory, RADIUS, RSA SecurID server, or with local authentication database.

The Array SPX can also authenticate users using SSL client certificates. Array Networks relies on cryptographically valid certificates issued by approved certificate authorities specified by the administrator. In addition, client certificates can be validated against the local authentication database or an external LDAP server.

An added security feature when logging into a virtual site, the Array SPX supports a client certificate based two-factor authentication solution by requiring users to provide a client certificate, as well as username and password.

A unique area of strength Array Networks provides is with the integration of different Certificate Authorities, intermediate CA, two-factor authentication via certificate and LDAP or local database. Integration is enhanced with automatic group lookup and mapping capabilities, schema extensions and local configuration. Extending client certificates to provide authorization based on flexible information retrieved from client certificates is unique. Client side certificates can be used as a first stage in a multi-staged authentication or serve as a single form of authentication (by disabling all other authentication methods). When enabled, a user will not be able to access the login page without a valid certificate. All of these elements are bound by a uniform Access Control mechanism that allows an administrator to control access to internal servers and applications. Only authorized users are provided access to the appropriate resources, and all access is always logged along with attempts at penetration with enough information to provide an audit trail and to ensure compliance with regulations such as HIPAA, GLBA, Sarbanes-Oxley and others.

Deep Packet Inspection – Request Processing

Array employs deep packet inspection techniques to inspect the entire payload of the request and response in order to have full control over the bi-directional flow of traffic. Array's filtering rules can be configured to pass through only those requests that meet the profile of the sites that are supported behind the Array SPX. For example, if the maximum length of URLs expected at the site is 2000 bytes and the maximum request length including cookies and various headers is 4000 bytes, there is no reason to accept requests that are bigger than that. For example, if a 10,000 byte request is received, it is likely because the remote side is trying to create a buffer overflow on some poor defenseless server. If a request is received with patterns such as "cmd.exe", "root.exe", "command center", "." etc., it is likely because the remote user is trying to forcefully browse past what they are allowed to do, and get access to resources they should not be allowed to get to or, it is a worm such as NIMDA that is trying to get through. These and more such exploits are promptly dropped at the border. Every request and associated response is always inspected for correctness and conformance with underlying protocols such as HTTP/1.0, HTTP/1.1. Array inspects every single packet associated with the request up to a default limit of 140 Kbytes, subject to rules configured by the administrator. Array's open architecture and its associated APIs can be used to provide integration with specialized security logic providers or to create custom rules that provide very specialized and focused security if the needs exceed those that are provided as standard out-of-box deployment.

Web Resource Mapping

Array's Web Resource Mapping is a unique technique for hiding the internal namespace of web servers from the external world and bringing them back through the same portal interface. For this purpose, Array modifies packets on the fly as they are being sent back to the client whether it is HTML, Javascript or other content. To be able to effectively and correctly do this, even in the presence of non-compliant code, Array performs syntactic and semantic inspection of the payload before reassembly back in to the required format to provide the function of HTTP NATing. This processing is typically set to unlimited size so that Array is able to understand the logic behind the application to make the appropriate decision. XML and other markup languages can be supported using Array's open architecture API, which is an extensible mechanism for providing additional deep packet inspection.

Encryption and Authentication

The following SSL cipher suites are supported:

- 128 bit RC4 with MD5 or SHA
- 40 bit RC4 with MD5
- 56 bit DES with SHA
- 168 bit triple-DES with SHA

Administrators can assign each virtual site with different minimum cipher strength. Users who do not meet the minimum requirement will be redirected to a URL configured by the administrator.

Third-Party Audits

The Array SPX has been certified as compatible with RSA BSAFE® security software, including RSA Security's industry-standard SSL and PKI implementations. The Array SPX also met Internet Security Systems, Inc. (ISS) X-Force's "best practices" criteria for application security. ISS X-Force Penetration Team is well known for its attack simulation and analysis services. Their application security testing addressed 60 tests, including intense penetration evaluation. The Array SPX application development and maintenance procedures were also audited

The Array Networks SPX withstood all attempts to breach the device's security. The tests included buffer overflow, PROTOS remote SNMP, denial of service (DoS), SynFlood, script, and also included validation of security against a variety of unconventional hacking methods. Light Reading's review of SSL VPN products conducted a series of penetration tests in which the Array SPX was deemed the only product without vulnerability. Array SPX is currently undergoing ICSA and FIPS certifications to add to the current list of hardware certifications such as FCC part A, CSA and TUV.

Conclusion

As can be seen with the brief description on Array's defense-in-depth approach to security, most administrators will find that Array offers much more than a typical SSL VPN in terms of security and does not need a traditional firewall or specialized application firewall for most deployments. Array offers 70-80% of the functionality offered by application firewalls with respect to deep packet inspection, but offers a lot more functionality that is not offered by application firewalls providing much more than 100% of the security requirements for most environments. In those environments where additional out of the box deep packet inspection functionality is required, Array can load balance or provide scalability to specialized application firewalls thereby improving the level of application security which is usually needed because of poor coding practices on the part of application developers.

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**.