

# Understanding WebWall™

Array Networks Application Firewall Technology

---

## White Paper

### Overview

Network managers are often placed at odds by two chief requirements of their Web-based applications and networks: speed and security. WebWall affords the peace of mind associated with a secure network, without the tradeoff of reduced download speeds caused by third party firewall compatibility and latency issues. Learn about:

- ➔ Causes & Effects of the Typical Tradeoff Between Speed and Security
- ➔ How Array WebWall™ Bridges the Gap Between Speed and Security
- ➔ WebWall Security Features

## Array Networks Application Firewall Technology

### → Having it Both Ways: Speed and Security

Website administrators are often placed at odds with two chief goals of their Internet based operations. The first goal is the speedy response and delivery of end-user queries made to their websites and web-enabled applications. The speed of the content being delivered is crucial to a user's repeated use of any given site or application at any given time. It has become a vicious reality that if content loads slowly, for whatever reason, end-users or customers will grow ever more impatient and ultimately leave. When they leave, business suffers. The second goal for web site administrators is security. Administrators need to protect their sites as well as their customers. If a rogue connection were to successfully enter the backend servers, a web site could be shut down and loads of proprietary data could be compromised. If either of these goals, speed or security, are not met by administrators the results would be catastrophic for business.

Protecting websites, applications, and customers in the past has presented a tenuous "give and take" balance. Administrators had to deploy security devices and protocols that would direct user requests through multiple *firewalls* for protection. These additional processes would require the request to travel through more devices, whether these be hardware mechanisms or software routines, which would add latency and ultimately slow the delivery time between user and website. Of course the risk of not checking each and every request made of an external network is not one any web site administrator would want to take. But what alternative exists that would reduce latency while still providing the heightened level of security required by businesses and customers alike?

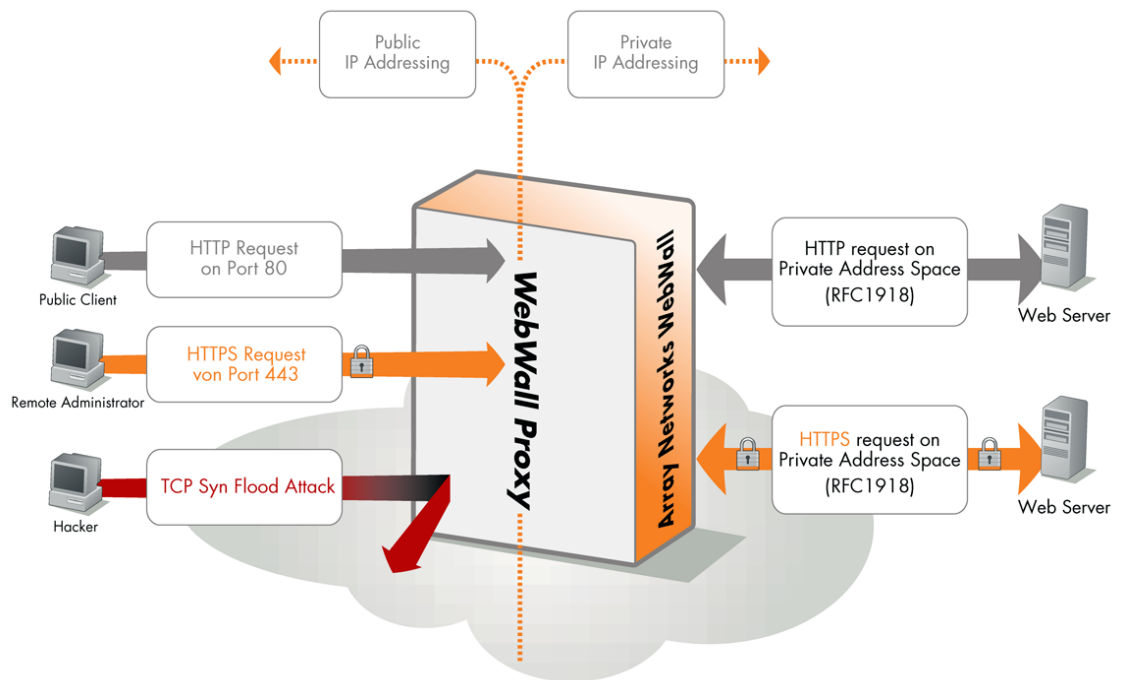
Now administrators can have security and increase delivery speed at the same time. Array Networks' Application Front End appliances offer the WebWall security protocol built into a single platform that also serves as a proxy cache, server load balancer, SSL accelerator, global server load balancer and redundancy fail over master.

The Array appliance contains several built-in security mechanisms to protect Web servers from attack, including:

- Access Control Lists
- Protection against Syn-Flood, Fragmentation, and DoS attacks
- Stateful packet inspection
- Single packet attack prevention

Access control lists provide tight control over who may and may not enter the network, and utilizing Array's ultra-fast rules engine, the access control list mechanism is able to perform as well with 1000 rules as it does with a single rule. Under full load, WebWall uses only 1% of the CPU thereby enabling the other key features of the Application Front End to sustain their performance as well.

## Array Networks Application Firewall Technology



Administration of the Array appliance takes web site security a step further by utilizing only cryptographically secure methods for communication with the network administrator. By using these methods the administrator is able to efficiently manage their system using either the ArrayOS™ CLI or WebUI. In other words, the Array appliance itself is as secure as the network it is protecting.

Array Application Front Ends are full proxies, thus you are guaranteed clean connections to your web servers. For example, once a connection is established, a less than honorable user may try to send a packet that is technically correct but aimed to expose a bug in your web server TCP/IP stack (e.g. a FIN/ACK/PSH/URG). Because WebWall will absorb this packet and properly handle it, administrators need not concern themselves with the internal web server seeing such tainted packets. Handling DoS attacks is also a strong point of WebWall; from SYN-FLOODS, to Frag attacks, to Smurf packets, WebWall fends them off with its focused security protocols.

With Array Networks appliances housing and integrating the WebWall feature into a single device, along with as many of the other features as an administrator could desire, user requests no longer need to travel to and through additional devices - thus reducing latency.

WebWall affords the peace of mind associated with a secure network, without the tradeoff of reduced download speeds because of third party firewall compatibility and latency issues. Now user requests can be verified, processed, and returned achieving both chief goals: speed and security.

## Array Networks Application Firewall Technology

### *About Array Networks*

Array Networks is a world leader in secure application acceleration and deployment appliances for global enterprises. Built upon the Array SpeedStack(TM) technology, Array's unified secure content access solutions enable industry-leading performance, integration, scalability and ease of implementation and management. Headquartered in Campbell, California with sales offices in the U.S., Europe, Asia Pacific and Latin America, Array engineers and manufactures its products in the Silicon Valley and sells them through direct and indirect channels across the globe.

#### **Array Networks, Inc.**

254 East Hacienda Avenue

Campbell, CA 95008

Phone: (408) 378-6800

Toll Free: 1-866-MY-ARRAY

Fax: (408) 874-2753

Email: [info@arraynetworks.net](mailto:info@arraynetworks.net)

[www.arraynetworks.net](http://www.arraynetworks.net)

Distribution:

