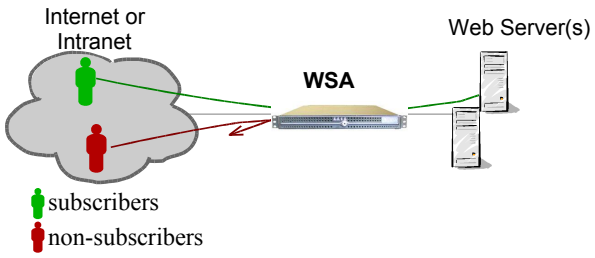
Security Benefits of the Sevan WSA
A Sevan White Paper

The focus of Sevan's WSA, is to provide web access control that is convenient for the users and have the lowest cost of ownership for the service providers. Adding the WSA to a Web site also improves the security of the site. This paper presents the security benefits of the WSA.

Only Subscribers Can Access the Site

Without a device like the WSA protecting your Web Servers, anyone with access to the internet can send packets to your servers. Any person that can reach your servers can also attack them.

The WSA can be configured to require access control for the entire Web site. This means that any user attempting to access your servers will be subjected to Sevan's Identity Authentication. Subscribers to your Web site will be allowed to access your servers, but non-subscribers are blocked. This means that non-subscribers cannot attack your Web Servers.



If you assume that your subscribers form a more trustworthy community than the Internet at large (e.g. your subscribers are your employees), then the WSA is exposing your servers to a safer community. Even if your subscribers are not trustworthy, the WSA is protecting you from most of the potential hackers on the Internet.

User Protection

Password schemes have the nasty property that if anyone on the Internet discovers your password they can become you. As a matter of fact if your password is posted on the Internet, an unlimited numbers of thieves can steal your information or services. Password thieves can operate anywhere in the world, which makes them difficult to track down. Some jurisdictions might not even prosecute password thieves.

The WSA authenticates the subscriber based on the subscriber's secret key. This key is usually safely stored in the browser. For even greater security it can be stored on a smart card or smart token. In order for a thief to steal your identify he must steal your secret key. This requires that the thief gains access to your browser or smart card. If your computer, browser, or smart card is protected by a password or PIN, the thief must know that as well.

In any case, your secret key is vastly more secure than passwords. There are numerous examples of passwords being hacked off the service provider's web site. Since your secret key is never at your service providers, this sort of attack is impossible with the WSA. In the likely attacks an identify thief must actually be sitting in front of your computer or possess your smart card and PIN.

WSA's Network Security Features

The WSA examines every packet destined for the Web servers and applies Web Filter Rules to ensure the packet is safe to pass to the server. Since the WSA is dedicated to Web servers, it is not a full-featured firewall and is therefore far easier to configure and monitor. Unlike general purpose firewalls the WSA Web Filter Rules are simple to understand and do not require extensive network expertise. The administrator simply enables or disabled predefined rules. These rules do not involve networking details like IP addresses or port numbers.

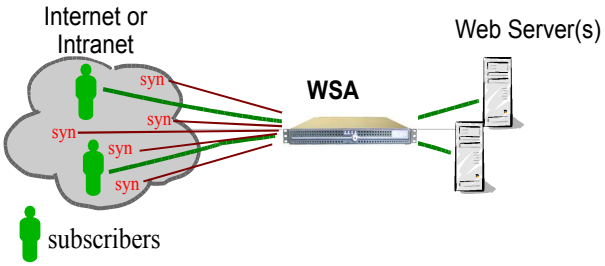
Experience has shown that strong security must be simple to configure. Configuration complexity leads to misconfigurations, which are a major source of vulnerabilities. Because the WSA is dedicated to protecting Web servers, its simple configuration actually makes it stronger than a general-purpose firewall.

TCP Termination

One of the most disruptive denial of service attacks is a SYN flood attack. The attacker simply overloads the Web server with thousands of TCP SYN packets each second. Even the most hardened server will be crippled under such an attack.

The WSA terminates all TCP connections between the browsers and the Web servers. As such the Web server will never see a SYN flood attack, because the WSA will deal with it.

The WSA uses Sevan's Secure Stack, which is especially designed to tolerate extreme SYN flood attacks. Rather than rely on heuristics to detect SYN flood attacks, the Secure Stack is designed to tolerate them. The packets corresponding to the SYN flood are handled by the WSA, and the legitimate traffic is allowed through to the Web servers.



Access Control: WSA or Server Software?

There are significant security considerations when deciding how and where to host access control. A wide variety of software products offer access control on the server. These products come in two flavors: agents on the Web servers interacting with special purpose "AAA" servers at the site (e.g. Netegrity) or integrated solutions where all of the functions are hosted on the Web servers (e.g. IIS). In either case, all users are allowed to send packets to the server before the access control mechanisms allow or disallow further access. This means that the server's stack and operating system are open to attackers before the access control decisions are made.

The WSA enforces access control before the users' packets reach the Web servers. Therefore, only authorized users can even reach the servers. Of course, unauthorized attackers can still attack the WSA, but the WSA proves to be a much more rugged opponent. This is because the WSA is not a general-purpose computing environment. On the contrary, the WSA uses a hardened real-time kernel, a specially designed secure stack, and it does not support the miscellaneous services that are found on most servers. The WSA is designed to be attacked and to repulse the attack.

Management and Administration

Simplicity is the key to strong security. With this in mind, the WSA is simple to install, simple to configure, and simple to manage. The intuitive web-based interface directs the administrators through most administrative functions. It's delegated administration means that administrators see only what is absolutely necessary to do their jobs. The administration is so easy, that most administrators should find the WSA's manual unnecessary.

Freedom to use SSL

The WSA is a simple and efficient means of providing SSL security for the information flowing between the browsers and the server. Because the WSA can terminate the SSL connection, there is no SSL performance penalty. Even when the situation requires an SSL connection all the way to the server, the WSA can reduce the SSL load on the server by efficient reuse of SSL keying material. Because the WSA enforces the SSL

policies, a misconfiguration of a web application cannot inadvertently cause sensitive information to be sent in the clear. The WSA makes it possible to place an SSL security umbrella over specific applications, servers or the entire site.

Summary

Strong, yet convenient security benefits are an important side effect of Sevan's Identity Authentication. The WSA provides a level of security that would be impossible with separate products.

sevan networks

Sevan Networks, Inc
1310 Hollenbeck Ave, Ste F
Sunnyvale, CA 94087
Tel: 408.830.1000
Fax: 408.830.1001
www.sevannetworks.com