

Web Application Security Solutions

With more advancement in internet applications and technology, websites have diversified with various business applications. They have also faced variety of attacks targeting their businesses specifically. The traditional security solutions, such as firewall and IPS, have failed to provide effective and comprehensive protection for those web-based businesses.

Vulnerable Web applications are the No. 1 attack vector today.--- Forrester 2010.2

*"82 percent of websites have had at least one security issue of high, critical or urgent severity."
--WhiteHat Security*

This daunting circumstance generates the need for a special Web application security solution that is capable of protecting Web application traffic and all application resources from attacks, which take advantage of web protocols or exploit application specific vulnerabilities. And the voice calling for Web application firewalls is becoming increasingly prominent.

" WAF is a very different technology, and it protects against vulnerabilities you inadvertently create yourself." --- Gartner analyzer Greg Young

Anchiva WAF provides proactive Web application defenses:

- Anti-SQL injection
- Anti-XSS attacks
- Anti-OS command injection
- Protect webpage against Trojan infection exploiting the existing backdoor in the server.
- Anti-webpage tampering
- Anti-weak password attacks
- Anti-overflow check
- Anti-cookie tampering
- Anti-cookie hijacking
- Cookie encryption
- Detect and monitor servers against Trojan infection
- Virus scanning on uploaded files
- Virus scanning on submitted content
- Anti-directory traversal attack
- Prevent browsing website directory
- Prevent certain file type download
- Prevent certain file type upload
- URL keyword filtering
- URL inquiry parameter keyword filtering
- Sensitive information upload filtering
- Set authorized IP for website administration
- Block server version information
- Block server error response
- Block database error messages
- Prevent server program code leak



Anchiva WAF Differences

Defense to Dynamic Webpage

Anchiva WAF provides real-time inspection on the dynamic webpage that utilize Web2.0 technology to prevent attacks exploiting the breaches in the dynamic webpage programming, including SQL injection, XSS attacks, buffer overflow attacks and the like. Anchiva WAF protects the security and liability of website content and services by preventing those attacks that exploit user ID authentication, gain administrator's password, obtain data in unauthorized methods, tamper data, produce unauthorized contents, and execute unauthorized commands and other malicious behaviors to tamper and destroy website's database, directory and code.

Defense to Static Webpage

Based on the static webpage content, such as HTML, image files, and multi-media files, Anchiva WAF's cache inspection mechanism is purposely designed to check the webpage before them being delivered to the users. Only authorized webpage will be delivered to the clients, whereas the unauthorized and tampered pages are blocked from reaching users, and the administrator is notified in time for the recovery.

Trojan Infection Monitoring and Alert on Website

Anchiva WAF not only prevents websites from Trojan infection, but also inspects and filters webpage that may have already been infected before the WAF being deployed. In addition, customizable replacement pages are available to users until the compromised page is reverted to the normal state.

Unique Malicious File Upload Filtering

Anchiva WAF provides virus scanning and signature matching to file-upload during HTTP/HTTPS application interaction. The powerful built-in virus signature library helps prevent infected files being uploaded to the web server, in order to prevent wider circulation of the Trojan that results in server crashes, and even network disconnection.

Fine Performance and Stability

Anchiva WAF benefits from years of research and technical innovation. AnchivaOS, that supports multi-kernel balanced distribution and optimized TCP protocol stack, is the core technology to assure a fine performance and stability of Anchiva WAF.

Easy Deployment and Management

Anchiva WAF interoperates with existing firewalls, routers, and switches in the Plug-and-Play, layer 2 transparent mode without the need of changing the network and web server topology.

High Return on Investment

- Single appliance provides defense policy configuration and management for multiple website administrators. Provides individual attack incident alert, analysis logs and reports.
- Single appliance provides simultaneous protection to multiple connections.
- Deployed in front of web servers in IDC to provide centralized and customizable defense for multiple hosted Web service systems.



Anchiva WAF Defense Mechanism

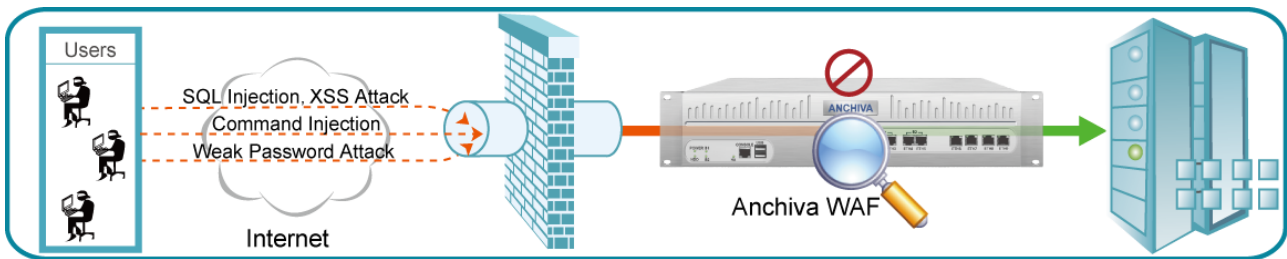
Beforehand Prevention

Anchiva WAF detects and blocks various types of sensitive information in the Web application infrastructure from attackers before the attack happens. For example, it detects and blocks server version information, Web application source code, website directory, database message, and HTTP error message and prevents them being used to launch next round of attacks.



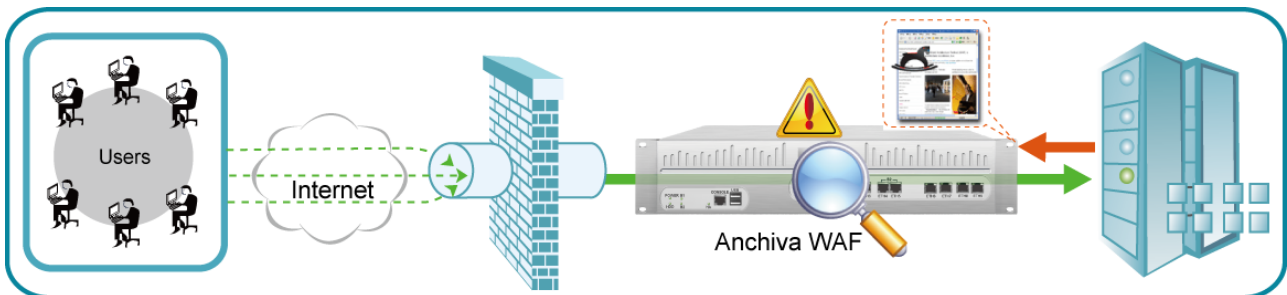
Continuous Block

Anchiva WAF inspects web applications' interactive sessions for SQL injection, XSS attack, command injection, weak password attack, and provides in-time blocking to secure the web services.



Post-event Monitor

Anchiva offers a post-event monitoring and diagnose on Trojan infection on webpage as well as an in-time alert.



Product Specifications

Model	S100	S300	S600	S900
Performance				
Throughput	400Mbps	600Mbps	1Gbps	2Gbps
HTTP Max Concurrent	150000	200000	300000	400000
HTTP New Sessions /Second	5300	7000	9000	11000
Specifications				
Network Interfaces	6C	6C+4F	6C+4F	6C+4F
RAID		√	√	√
Redundant Power		Optional	√	√
Chassis	IU	2U	2U	2U
Management				
WebUI	√	√	√	√
CLI (SSH/Console)	√	√	√	√
Report System	√	√	√	√
Alarm Notify (SNMP & E-mail)	√	√	√	√
High Availability				
OS on Flash	√	√	√	√
HA	√	√	√	√
Hardware Bypass	2 pairs	2 pairs	2 pairs	2 pairs
Deployment				
In-line Transparent Deployment	√	√	√	√
Off-line Recon Deployment	√	√	√	√
VLAN	√	√	√	√



Anchiva System Ltd.

2033 Gateway Place 5th Floor, San Jose, CA 95110

Phone: +1-408-392-2300, Email: info@anchiva.com

B 601A, SP Tower, Tsinghua Science Park, Beijing, P. R. China

Phone: +86-10-51266678, Email: info_cn@anchiva.com

For more information, visit www.anchiva.com.

Product Quality Control and Services

Anchiva Services provides a wide range of service available for purchasing. We strongly recommend you purchase the service to assure the latest software version and user experience. In addition, Anchiva provides professional consulting services, installation services and configuration support as well as corresponding training courses.

All information referred in this document may be updated at any time, and Anchiva will not notify especially.

Copyright ©2011 Anchiva System Ltd. All rights reserved. AnchivaOS and Anchiva are registered trademarks. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.