

AppWall

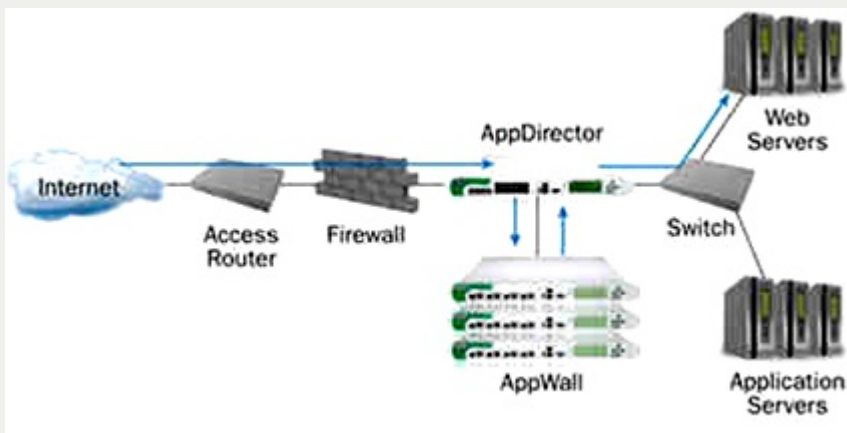
AppWall firmy Radware jest zaawansowanym urządzeniem typu WAF (z ang. Web Application Firewall), które chroni Web Aplikacje, portale i serwery internetowe przed zagrożeniami pochodzącymi z wewnątrz i zewnątrz sieci. AppWall opiera się m.in. o klasyfikacje zagrożeń i standardy organizacji tj. OWASP, WASC (Web Application Security Consortium), FBI i instytutu SANS (SysAdmin Audit, Network, Security).

AppWall chroni:

- Web aplikacje;
- Portale/ strony internetowe.

Funkcjonalność AppWalla:

- Wykrywa, rejestruje i blokuje ataki;
- Blokuje ataki typu Zero-day;
- Walidacja XML – kontroluje wykorzystywanie XML;
- Walidacja protokołu - powstrzymuje exploity, które korzystają z podatności protokołu HTTP;
- Wykrywa i blokuje exploity wykorzystujące podatności aplikacji internetowych.



AppWall chroni Web aplikacje przed zagrożeniami sklasyfikowanymi przez:

OWASP (top ten):

- A1-Injection
- A2-Cross Site Scripting (XSS)
- A3-Broken Authentication and Session Management
- A4-Insecure Direct Object References
- A5-Cross Site Request Forgery (CSRF)
- A6-Security Misconfiguration
- A7-Insecure Cryptographic Storage
- A8-Failure to Restrict URL Access
- A9-Insufficient Transport Layer Protection
- A10-Unvalidated Redirects and Forwards

Organizacje WASC:

Authentication:

- Brute Force Attacks
- Insufficient Authentication
- Weak Password Recovery Validation

Authorization:

- Credential/Session Prediction
- Insufficient Authorization
- Insufficient Session Expiration
- Session Fixation

Information Disclosure

- Directory Indexing
- Path Traversal
- Predictable Resource Location

Logical Attacks

- Abuse of Functionality
- Denial of Service (DOS)
- Insufficient Anti-Automation
- Insufficient Process Validation

Inne zagrożenia:

- From field manipulation
- Session hijacking
- Access to predictable resource locations Unauthorized navigation
- Web server reconnaissance
- Directory\path traversal
- Forceful browsing
- HotLink
- Exploit Web application
- Gateway circumvention
- Web server reconnaissance
- SOAP and Web services manipulation
- HTTP response splitting
- Evasion and illegal encoding
- XML validation
- Web services method restrictions and validation
- HTTP RFC violations
- HTTP request format and limitation violations (size, unknown method, etc.)
- Use of revoked or expired client certificate

Client-Side Attacks:

- Content Spoofing
- Cross-site scripting

Command Execution:

- Buffer Overflow
- Format String Attack
- LDAP Injection
- OS Commanding
- SQL Injection
- SSI Injection
- XPath Injection

Unclassified Application Layer Attack Types

- Parameters Tampering
- Cookie Poisoning
- Database Sabotage
- Web Services Manipulation
- Stealth Commanding
- Debug Options
- Backdoor
- Manipulation of IT Infrastructure Vulnerabilities
- 3rd Party Misconfiguration
- Data Encoding
- Protocol Piggyback
- Malicious file upload

AppWall składa się z następujących komponentów:

AppWall Management Application- Java GUI - panel zarządzający, który pozwala na:

- zarządzanie i konfigurację ustawień AppWalla
- zarządzanie politykami bezpieczeństwa
- rejestrowanie zdarzeń i analizę incydentów
- generowanie raportów
- administrację dostępnymi komponentami i usługami

zarządzanie klastrem AppWalli

AppWall Gateway - przechwytuje ruch (warstwa aplikacji) i chroni przed atakami

AppWall Cluster Manager- umożliwia stworzenie klastra AppWalli.

AppWall Publisher - umożliwia przesyłanie zarejestrowanych zdarzeń do określonych użytkowników lub wyspecjalizowanych programów.

Watchdog - utrzymuje poprawne działanie AppWalla i zapobiega przed jego postojom i niepoprawnym działaniem.

Command Line Interface Manager - umożliwia konfigurację podstawowych ustawień, dostępny za pomocą portu szeregowego RS232 lub połączenia SSH.

Zdjęcia produktu

Inne rozwiązania producenta

- [AppDirector](#)

Podobne produkty

- [Metasploit](#)
- [QRadar SIEM](#)
- [Safend Data Protection Suite](#)
- [CA SiteMinder](#)
- [AppDirector](#)
- [SourceFire 3D IPS](#)
- [Nexpose](#)