SONICWALL®

Web Application Firewall Service

Web application threat management

Web 2.0 applications have emerged as the platform of choice for businesses and consumers. As a result, they have increasingly become a target for criminal attacks such as SQL injection, parameter manipulation, cross-site scripting and Denial-of-Service (DoS). While more small- to medium-sized businesses (SMBs) are adopting a web presence, they often lack the in-house capabilities to keep up with the rapidly evolving challenges of web security. Regulatory compliance mandates make web application attacks particularly onerous for financial, healthcare, and application service providers, as well as e-commerce businesses.

The award-winning SonicWall™ Web Application Firewall (WAF) Service offers businesses a complete, affordable, out-of-box compliance solution for web-based applications that is easy to manage and deploy. It supports OWASP Top Ten and PCI DSS compliance, providing protection against injection and cross-site scripting attacks, credit card and Social Security Number theft, cookie tampering and cross-site request forgery. Dynamic signature updates and custom rules protect against known and unknown vulnerabilities. Web Application Firewall Service can detect sophisticated web-based attacks and protect web applications (including SSL VPN portals), deny access upon detecting web application malware, and redirect users to an explanatory error page. It provides an easy-to-deploy offering with advanced statistics and reporting options for compliance. Application profiling makes it easy for administrators to understand the nature of web traffic hitting their servers and to be able to create rules automatically.

Features and benefits

Open Web Application Security Project (OWASP) Top 10 Vulnerability Protection addresses leading security risks based on prevalence and severity of attacks, as included in PCI DSS 6.6 and other industry standards.

Cross-site request forgery protection is delivered in addition to protection against injection and cross-site scripting (XSS) attacks.

Automatic signature updates and adaptive Application Profiling protect against known as well as emerging threats.

Strong authentication and authorization to any internal or external web site (e.g. e-commerce web sites). This supports compliance initiatives by preventing unauthorized access to your internal and external web sites. Authentication support includes token-based two-factor authentication, client certificate authentication and tokenless one-time passwords. Granular access policies can authorize access to various web servers based on hostname, subnet, IP address, port and URL path.

Benefits:

- OWASP Top 10 Vulnerability Protection
- Cross-site request forgery protection
- Automatic signature updates
- Strong authentication and authorization
- Information disclosure protection
- Robust dashboard
- Flexible policy settings
- Cookie tampering protection
- Secure session management
- Anti-evasion measures
- HTTPS inspection
- Acceleration features
- Web site cloaking
- Custom rule chains
- Application profiling
- Geolocation-based policies
- Botnet filtering

Information disclosure protection blocks access to web sites containing administrator-defined keywords or phrases, preventing leakage of sensitive information. Data Loss Prevention (DLP) of credit card and Social Security Number is also offered.

Robust dashboard with advanced statistics provides an easy-to-use web-based management interface. This can be used to monitor web server status. The status page can also provide an overview of all threat monitoring and blocking activities such as signature database status information and threats detected and prevented, including the OWASP Top 10 threats.

Flexible policy settings enable administrators to apply signature settings based on threat severity as well as set exclusion list per signature.

Cookie tampering protection minimizes the chances of a breach by modifying the cookies.

Session management allows administrators to set global timeouts based on user inactivity.

Anti-evasion measures normalize requests (e.g., standardizing encoded or suspect character sets or path names) prior to analysis.

HTTPS inspection can block attacks embedded into SSL-encrypted packets.

Acceleration features include content caching, compression and connection multiplexing, and improve the performance of protected web sites, significantly reducing transactional costs.

Web site cloaking prevents hackers from guessing the web server implementation and exploiting any potential vulnerabilities.

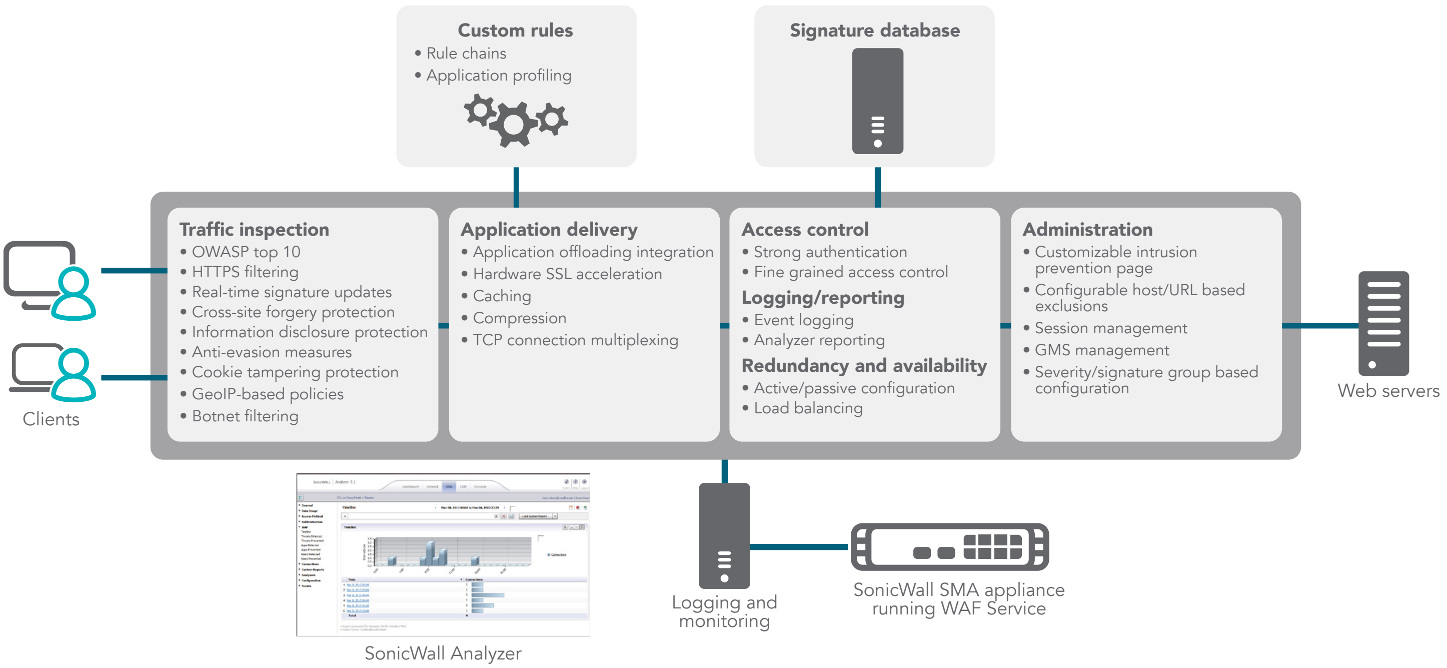
Custom rule chains allows the administrator to create custom rules/signatures in addition to the rules developed by SonicWall. It also allows the administrator to employ both positive and negative security models.

Application profiling automatically suggests custom rules by intelligently learning from multiple offloaded web applications while also providing the ability to manage the generated custom rules on a per-portal basis.

Geolocation-based policies enable administrators to monitor and enforce policies based on the geographic location of the remote user.

Botnet filtering leverages a dynamically updated database that the SMA uses to identity and block rogue activity from compromised endpoints.

SonicWall Web Application Firewall architecture



Custom rules
- Rule chains
- Application profiling

Signature database

Traffic inspection
- OWASP top 10
- HTTPS filtering
- Real-time signature updates
- Cross-site forgery protection
- Information disclosure protection
- Anti-evasion measures
- Cookie tampering protection
- GeoIP-based policies
- Botnet filtering

Application delivery
- Application offloading integration
- Hardware SSL acceleration
- Caching
- Compression
- TCP connection multiplexing

Access control
- Strong authentication
- Fine grained access control

Logging/reporting
- Event logging
- Analyzer reporting

Redundancy and availability
- Active/passive configuration
- Load balancing

Administration
- Customizable intrusion prevention page
- Configurable host/URL based exclusions
- Session management
- GMS management
- Severity/signature group based configuration

Features

Appliances

- Secure Mobile Access 200
- Secure Mobile Access 400
- Secure Mobile Access 500v Virtual Appliance

Web Application Firewall Service Subscription Required

Capacity

- SMA 200 throughput 25 Mbps
- SMA 200 back-end servers supported: Unrestricted, recommend 1-5*
- SMA 400 throughput: 50 Mbps
- SMA 400 back-end servers supported: Unrestricted, recommend 5-10*
- SMA 500v Virtual Appliance throughput: 50 Mbps
- SMA 500v Virtual Appliance back-end servers supported: 5-1*

*Actual number of web servers will depend on your network environment, policy configuration, web server configuration and underlining physical hardware for virtual appliances

Web application security

- HTTP DoS Attack protection
  - Protection against Slowloris attacks
  - Botnet filter protection using IP reputation*
- HTTP protocol validation
- Protection against common attacks
  - SQL injection
  - OS command injection
  - Cross-site scripting
  - Cross-site request forgery
- Adaptive security with custom rule chains
  - Rate limiting support
- Cookie tampering protection
- Application Profiling to auto-generate rules
  - Simultaneous profiling of multiple applications
  - Manage custom rules filtered by application
- Website cloaking
- Response control
  - Block client
  - Redirect
  - Custom response
- Outbound data theft protection
  - Data Leakage Protection (DLP) of Credit Cards, SSN
- Automatic signature updates
- Protocol limit checks
- File upload control
- Geolocation-based policies*

Application delivery and acceleration

- High Availability (SMA 400)
- SSL offloading
- Load balancing with failover
- Caching
- Compression
- TCP connection multiplexing

Logging, monitoring and reporting

- System log
- Web Application Firewall log
- Access log
- Syslog support
- PCI Compliance report
- Global statistics dashboard
  - Threats detected and prevented across the world
- Advanced WAF statistics and reports
- Analyzer integration
- Geolocation-based monitoring and reporting

Authentication and authorization

- LDAP/Radius/Local user database
- Client certificates
- Single sign-on
- Two-factor authentication
  - Quest Defender
  - One-time password
  - Other technology partners

*Geolocation and Botnet filtering protection require a valid support contract on the SMA appliance.

SonicWall Web Application Firewall Subscription Service

01-SSC-2241 SMA 200 WEB APPLICATION FIREWALL (1 YR)

01-SSC-2409 SMA 200 WEB APPLICATION FIREWALL (2 YR)

01-SSC-2410 SMA 200 WEB APPLICATION FIREWALL (3 YR)

01-SSC-2254 SMA 400 WEB APPLICATION FIREWALL (1 YR)

01-SSC-2407 SMA 400 WEB APPLICATION FIREWALL (2 YR)

01-SSC-2408 SMA 400 WEB APPLICATION FIREWALL (3 YR)

01-SSC-9185 SONICWALL SMA 500v WEB APPLICATION FIREWALL (1 YR)

01-SSC-9186 SONICWALL SMA 500v WEB APPLICATION FIREWALL (2 YR)

01-SSC-9187 SONICWALL SMA 500v WEB APPLICATION FIREWALL (3 YR)

To access SKUs for the complete line of SonicWall Secure Mobile Access appliances, please visit www.SonicWall.com.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®