



SonicWALL Web Application Firewall Service

SECURE REMOTE ACCESS

Web Application Threat Management

- 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
- Comprehensive audit log
- Secure session management
- Anti-evasion measures
- HTTP inspection
- Acceleration features
- Web site cloaking
- Custom rule chains

As Web 2.0 applications emerge as the platform of choice for businesses and consumers, they increasingly become a target for criminal attacks such as SQL injection, parameter manipulation, cross-site scripting and Denial-of-Service (DoS). While small- to medium-sized businesses (SMBs) are increasingly 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.

A complete, affordable, out-of-box compliance solution, SonicWALL® Web Application Firewall (WAF) Service leverages your existing infrastructure as a licensable add-on module to the SonicWALL Secure Remote Access Series. Utilizing a dynamically updated signature database to detect sophisticated Web-based attacks and protect Web applications including SSL VPN portals, SonicWALL Web Application Firewall Service applies reverse proxy analysis of Layer 7 traffic against known signatures, denies access upon detecting Web application malware, and redirects users to an explanatory error page.

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 blocks this sophisticated type of Web site attack.

Automatic signature updates ensure up-to-date protection by enabling administrators to schedule automatic updates for Web application malware signatures.

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.

Information disclosure protection can block access to Web sites containing administrator-defined keywords or phrases, preventing leakage of sensitive information.

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.

Comprehensive audit log makes logging and reporting available for auditing, compliance and reporting purposes.

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 its vulnerabilities.

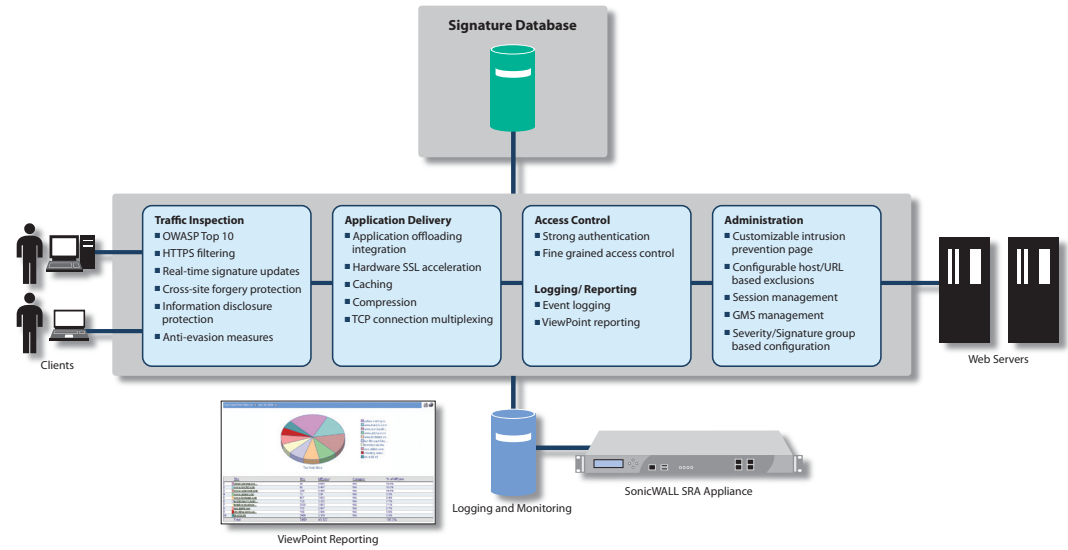
Custom rule chains allows the administrator to create custom rules/signatures in addition to the rules developed by SonicWALL. It also allows the administrator to employ both positive and negative security models.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Specifications

SonicWALL Web Application Firewall Architecture



SonicWALL SRA 1200
5 users
01-SSC-6063



SonicWALL SRA 4200
25 users
01-SSC-5998



Subscription Service

SonicWALL Web Application Firewall Service for SRA 1200 (1-year)
01-SSC-8877

SonicWALL Web Application Firewall Service for SRA 1200 (2-year)
01-SSC-8878

SonicWALL Web Application Firewall Service for SRA 1200 (3-year)
01-SSC-8879

SonicWALL Web Application Firewall Service for SRA 4200 (1-year)
01-SSC-6055

SonicWALL Web Application Firewall Service for SRA 4200 (2-year)
01-SSC-6056

SonicWALL Web Application Firewall Service for SRA 4200 (3-year)
01-SSC-6057

To access SKUs for the complete line of SonicWALL Secure Remote Access appliances, please visit www.sonicwall.com.

Appliances

- Secure Remote Access 1200
- Secure Remote Access 4200

Web Application Firewall Service Subscription Required

Capacity

- SRA 1200 Throughput: 25 Mbps
- SRA 1200 Back-end Servers Supported: Unrestricted, recommend 1-5*
- SRA 4200 Throughput: 50 Mbps
- SRA 4200 Back-end Servers Supported: Unrestricted, recommend 5-10*

** Actual number of Web servers will depend on your network environment, policy configuration and Web server configuration.*

Web Application Security

- 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
- Web site cloaking
- Response control
 - Block client
 - Redirect
 - Custom response
- Outbound data theft protection
- Automatic signature updates
- Protocol limit checks
- File upload control

Application Delivery And Acceleration

- High Availability (SRA 4200)
- SSL offloading
- Load balancing
- Hardware SSL acceleration (SRA 4200)
- Caching
- Compression

Logging, Monitoring And Reporting

- System log
- Web firewall log
- Access log
- Audit log
- Syslog support
- Viewpoint integration

Authentication And Authorization

- LDAP/Radius/Local user database
- Client certificates
- Single sign-on
- Two-Factor Authentication
 - RSA Securid
 - VASCO
 - One-time password

SonicWALL's line-up of dynamic security solutions



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB AND E-MAIL SECURITY



BACKUP AND RECOVERY



POLICY AND MANAGEMENT

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™