



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**
- **Cookie tampering protection**
- **Secure session management**
- **Anti-evasion measures**
- **HTTPS inspection**
- **Acceleration features**
- **Web site cloaking**
- **Custom rule chains**
- **Application profiling**

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.

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.

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

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.

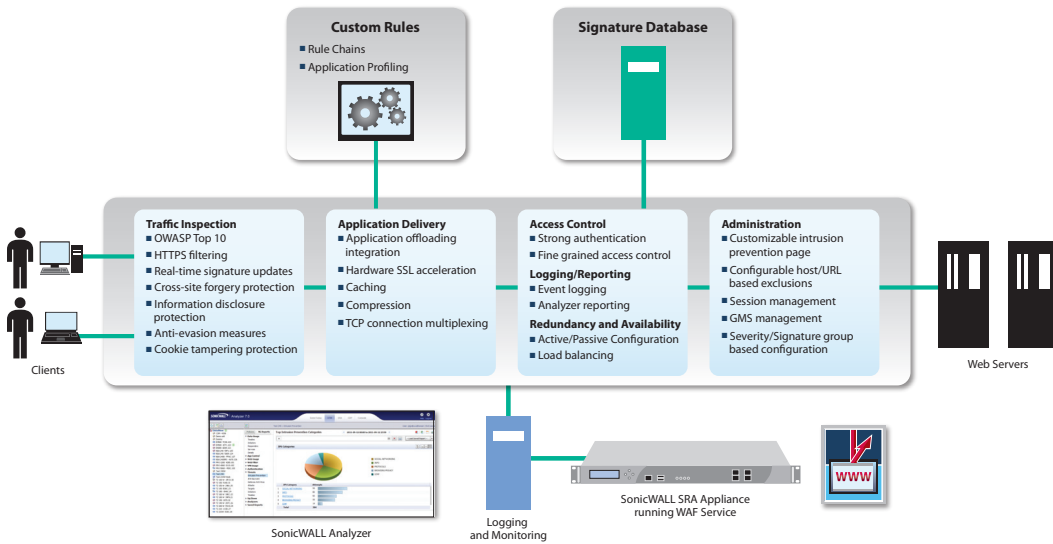
Custom rule chains allows the administrator to create custom rules/signatures in addition to the rules developed by SonicWALL. It also allows the administrator to employ both positive and negative security models.

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.



Specifications

SonicWALL Web Application Firewall Architecture



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
 - Secure Remote Access Virtual Appliance
- 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*
- SRA Virtual Appliance Throughput: 250 Mbps
- SRA Virtual Appliance Back-end Servers Supported: 5-20*

*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
- 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
- Web site cloaking
- Response control
 - Block client
 - Redirect
 - Custom response
- Outbound data theft protection
 - Data Leak Protection (DLP) of Credit Cards, SSN
- Automatic signature updates
- Protocol limit checks
- File upload control

Application Delivery And Acceleration

- High Availability (SRA 4200)
- SSL offloading
- Load balancing with failover
- Hardware SSL acceleration (SRA 4200)
- Caching
- Compression
- TCP connection multiplexing

Logging, Monitoring And Reporting

- System log
- Web Application Firewall log
- Access log
- Audit log
- Syslog support
- PCI Compliance report
- Global statistics dashboard
 - Threats detected and prevented across the world
- Advanced WAF statistics and reports
- Analyzer 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™