



SonicWALL Web Application Firewall Service

SECURE REMOTE ACCESS

Schutz vor Bedrohungen durch webbasierte Anwendungen

- Schutz vor den OWASP-Top 10-Schwachstellen
- Schutz vor Cross-Site Request Forgery
- Automatische Signaturen-Updates
- Robuste Authentifizierung und Autorisierung
- Schutz vor Informationslecks
- Leistungsstarkes Dashboard
- Flexible Regeleinstellungen
- Umfassendes Audit-Protokoll
- Sicheres Sitzungsmanagement
- Umgehungsschutz
- HTTP-Prüfung
- Beschleunigungsfunktionen
- Website Cloaking
- Individuell erstellbare Regelketten

Web 2.0-Anwendungen werden immer häufiger von Unternehmen und Privatanwendern genutzt. Mit zunehmender Verbreitung werden sie jedoch immer mehr zur Zielscheibe für kriminelle Angriffe wie SQL-Injection, Parametermanipulation, Cross-Site Scripting und Denial-of-Service (DOS). Selbst kleine und mittlere Unternehmen (KMUs) können heute kaum mehr auf eine Webpräsenz verzichten, doch häufig fehlt es ihnen an internen Kapazitäten, um mit den ständig neuen Herausforderungen in puncto Websicherheit Schritt zu halten. Für Finanz- und Gesundheitsdienstleister sowie für Application Service Provider und E-Commerce-Unternehmen sind Angriffe über Webanwendungen aufgrund gesetzlicher Compliance-Vorgaben besonders problematisch.

Der SonicWALL® Web Application Firewall (WAF)-Service bietet eine komplette und kostengünstige Out-of-the-Box-Compliance-Lösung und kann in die bestehende Infrastruktur als lizensierbares Zusatzmodul zur SonicWALL Secure Remote Access-Serie eingebunden werden. Mittels einer dynamisch aktualisierten Signaturrendatenbank, die komplexe webbasierte Angriffe erkennt und Webanwendungen wie SSL VPN-Portale schützt, prüft der Web Application Firewall Service von SonicWALL Layer 7-Verkehr mittels Reverse Proxy-Analyse auf bekannte Signaturen und sperrt den Zugriff, falls Malware in Webanwendungen identifiziert wird. Anschließend wird der Benutzer auf eine Seite mit Informationen zum aufgetretenen Fehler weitergeleitet.

Funktionen und Vorteile

Schutz vor den OWASP (Open Web Application Security Project)-Top 10-Schwachstellen. Deckt die verbreitetsten und schwerwiegendsten Angriffe gemäß PCI DSS 6.6 und anderen Industriestandards ab.

Schutz vor Cross-Site Request Forgery. Sorgt dafür, dass komplexe CSRF-Website-Angriffe blockiert werden.

Automatische Signaturen-Updates. Gewährleisten laufend aktualisierten Schutz, da Administratoren automatisierte Malware-Signatureupdates für Webanwendungen zeitlich planen können.

Robuste Authentifizierung und Autorisierung für interne und externe Websites (z. B. E-Commerce-Websites). Verhindert den unerlaubten Zugriff auf interne und externe Websites und gewährleistet damit die Einhaltung von Compliance-Vorgaben. Die Authentifizierung kann per tokenbasierter Zwei-Faktor-Authentifizierung, per Client-Zertifikat-Authentifizierung und anhand von Einmalpasswörtern ohne Token erfolgen. Mit granularen Zugriffsregeln lässt sich der Zugriff auf verschiedene Webserver nach Hostname, Subnetz, IP-Adresse, Port und URL-Pfad steuern.

Schutz vor Informationslecks. Der Zugriff auf Websites, die vom Administrator definierte Schlüsselwörter oder Wortgruppen enthalten, kann gesperrt werden. Auf diese Weise wird verhindert, dass sensible Informationen nach außen dringen.

Leistungsstarkes Dashboard mit erweiterten Statistiken bietet eine benutzerfreundliche webbasierte Verwaltungsoberfläche zur Überwachung des Webserver-Status. Daneben liefert die Statusseite einen Überblick zu sämtlichen Überwachungs- und Sperraktivitäten, u. a. mit Statusinformationen zur Signaturen-Datenbank oder zu den erkannten und eliminierten Bedrohungen, darunter die OWASP Top 10.

Flexible Regeleinstellungen. Administratoren können entsprechend dem Schweregrad der Bedrohung Signatureinstellungen vornehmen und eine Ausschlussliste über die Signatur erstellen.

Umfassendes Audit-Protokoll. Bietet Logging- und Reporting-Funktionen für Audits, Compliance-Vorgaben und Berichte.

Sitzungsmanagement. Administratoren können globale Timeouts einrichten, die bei Inaktivität der Benutzer greifen.

Umgehungsschutz. Normalisierung von Anfragen (z. B. durch Standardisierung verschlüsselter oder verdächtiger Zeichensätze oder Pfadnamen) vor der Analyse.

HTTPS-Prüfung. Angriffe, die in SSL-verschlüsselten Paketen eingebettet sind, können blockiert werden.

Beschleunigungsfunktionen wie Content Caching, Komprimierung und Verbindungsmultiplexing verbessern die Performance geschützter Websites und sorgen für erheblich niedrigere Transaktionskosten.

Website Cloaking. Verhindert, dass Hacker die Webserver-Implementierung erraten und Schwachstellen darin ausnutzen.

Individuell erstellbare Regelketten. Administratoren können zusätzlich zu den von SonicWALL entwickelten Regeln eigene Regeln bzw. Signaturen erstellen. Hierbei lassen sich positive und negative Sicherheitsmodelle (Whitelist/Blacklist) anwenden.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Technische Daten

SonicWALL Web Application Firewall-Architektur



SonicWALL SRA 1200
5 Benutzer
01-SSC-6063



SonicWALL SRA 4200
25 Benutzer
01-SSC-5998



Abo-Services

SonicWALL Web Application Firewall Service für SRA 1200 (1Jahr)
01-SSC-8877

SonicWALL Web Application Firewall Service für SRA 1200 (2 Jahre)
01-SSC-8878

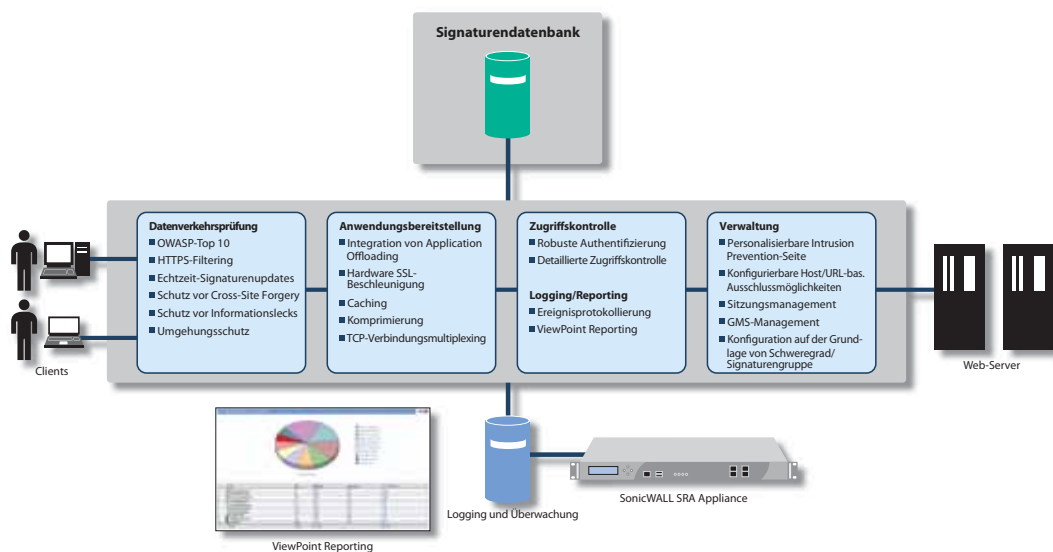
SonicWALL Web Application Firewall Service für SRA 1200 (3 Jahre)
01-SSC-8879

SonicWALL Web Application Firewall Service für SRA 4200 (1 Jahr)
01-SSC-6055

SonicWALL Web Application Firewall Service für SRA 4200 (2 Jahre)
01-SSC-6056

SonicWALL Web Application Firewall Service für SRA 4200 (3 Jahre)
01-SSC-6057

Die Artikelnummern zu allen Secure Remote Access Appliances von SonicWALL finden Sie unter www.sonicwall.com/de.



Appliances

- Secure Remote Access 1200
- Secure Remote Access 4200

Web Application Firewall Service-Abo erforderlich

Kapazität

- SRA 1200
Durchsatz: 25 MBit/s
- SRA 1200
Unterstützte Back-End-Server: Unlimitiert, 1-5* empfohlen
- SRA 4200
Durchsatz: 50 MBit/s
- SRA 4200
Unterstützte Back-End-Server: Unlimitiert, 5-10* empfohlen

*Die tatsächliche Anzahl der Webserver hängt von Ihrer Netzwerkumgebung sowie von der Regel- und Webserver-Konfiguration ab.

Sicherheitsfunktionen für Webanwendungen

- HTTP-Protokollprüfung
- Schutz vor verbreiteten Angriffsarten
 - SQL-Injection
 - OS Command Injection
 - Cross-Site Scripting
 - Cross-Site Request Forgery
- Adaptive Sicherheitsfunktionen mit individuell erstellbaren Regelketten
- Website Cloaking
- Steuerbare Reaktion
 - Sperren des Clients
 - Umleitung
 - Individuell einstellbare Reaktion
- Schutz vor Diebstahl ausgehender Daten
- Automatische Signatureupdates
- Protokoll-Limitprüfungen
- Dateiuploadkontrolle

Anwendungsbereitstellung und Beschleunigung

- Hochverfügbarkeitsoptionen (SRA 4200)
- SSL-Offloading
- Lastverteilung
- Hardware SSL-Beschleunigung (SRA 4200)
- Caching
- Komprimierung

Logging, Überwachung und Reporting

- Systemprotokoll
- Web-Firewallprotokoll
- Zugangsprotokoll
- Audit-Protokoll
- Syslog-Unterstützung
- Viewpoint-Integration

Authentifizierung und Autorisierung

- LDAP/RADIUS/LOKALE BENUTZERDATENBANK
- Client-Zertifikate
- Single Sign-On
- Zwei-Faktor-Authentifizierung
 - RSA SecurID
 - VASCO
 - Einmalpasswort

SonicWALL-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™