



SonicWALL Web Application Firewall Service

ACCESSO REMOTO SICURO

Gestione delle minacce alle applicazioni Web

- **Protezione dalle 10 vulnerabilità più critiche secondo OWASP**
- **Protezione CSRF (cross-site request forgery)**
- **Aggiornamenti automatici delle signature**
- **Solido sistema di autenticazione e autorizzazione**
- **Protezione contro la divulgazione di informazioni riservate**
- **Potente dashboard**
- **Impostazione flessibile delle policy**
- **Log di controllo completo**
- **Protezione contro la manipolazione dei cookie**
- **Gestione sicura delle sessioni**
- **Misure anti-evasione**
- **Ispezione HTTPS**
- **Funzionalità di accelerazione**
- **Cloaking dei siti Web**
- **Catene di regole personalizzabili**

Le applicazioni Web 2.0 si stanno affermando come la piattaforma preferita di aziende e consumatori e, inevitabilmente, diventano sempre più spesso oggetto di attacchi criminali quali iniezione SQL, manipolazione dei parametri, cross-site scripting e attacchi DoS (Denial of Service). Anche le piccole e medie imprese (PMI) optano sempre più spesso per una presenza sul web, ma nella maggior parte dei casi non dispongono delle capacità interne per contrastare le minacce in rapida evoluzione associate al Web. Le normative di conformità vigenti rendono gli attacchi alle applicazioni Web un danno particolarmente oneroso per i fornitori di servizi finanziari, sanitari e applicativi nonché per le aziende di e-commerce.

SonicWALL® Web Application Firewall (WAF) Service è una soluzione di conformità completa, conveniente e facile da gestire e implementare per applicazioni basate sul Web. Grazie alla protezione dalle 10 minacce più critiche secondo OWASP e alla conformità PCI DSS, offre una solida protezione da attacchi con iniezione di codice e cross-site scripting, furto di numeri di carte di credito e dati identificativi fiscali, manipolazione dei cookie e cross-site request forgery. L'aggiornamento dinamico delle signature e regole personalizzate offrono protezione da vulnerabilità note e sconosciute. Web Application Firewall Service è in grado di rilevare le più sofisticate minacce basate sul Web per proteggere le applicazioni Web (inclusi i portali SSL VPN), rifiutare l'accesso in caso di rilevamento di malware diretto alle applicazioni Web e reindirizzare gli utenti a una pagina di errore esplicativa. Facile da implementare, offre funzioni statistiche e di reporting avanzate per garantire la conformità alle normative. Il profiling delle applicazioni permette agli amministratori di capire con facilità la natura del traffico Web che attraversa i loro server, con la possibilità di creare automaticamente delle regole.

Caratteristiche e vantaggi

La **protezione dalle 10 vulnerabilità più critiche secondo OWASP (Open Web Application Security Project)** classifica i principali rischi alla sicurezza in base alla prevalenza e alla gravità degli attacchi, come prescritto dal requisito PCI DSS 6.6 e da altri standard industriali.

La **protezione CSRF (Cross-site request forgery)** integra e completa la protezione da attacchi con iniezione di codice e attacchi cross-site scripting (XSS).

Gli **aggiornamenti automatici delle signature** e il profiling adattivo delle applicazioni proteggono da minacce sia note che emergenti.

Solido sistema di autenticazione e autorizzazione per qualsiasi sito Web interno o esterno (ad es. siti di e-commerce). Supporto delle iniziative di conformità mediante la prevenzione di accessi non autorizzati ai siti Web interni o esterni del cliente. Il supporto dell'autenticazione include l'autenticazione a due fattori basata su token, l'autenticazione del certificato del client e password monouso (senza token). Mediante le policy di accesso granulari è possibile autorizzare l'accesso a vari server Web in base a nome host, subnet, indirizzo IP, porta e percorso URL.

La **protezione contro la divulgazione di informazioni riservate** può bloccare l'accesso a siti Web che contengono parole chiave o frasi definite dall'amministratore, prevenendo il furto o la divulgazione di informazioni sensibili. È inoltre disponibile la prevenzione della perdita di dati per carte di credito e informazioni identificative fiscali.

Il **potente dashboard** con funzioni statistiche avanzate include un'intuitiva interfaccia di gestione basata sul Web, che può essere utilizzata per monitorare lo stato del server Web. La pagina di stato può anche fornire un riepilogo di tutte le attività di monitoraggio e

bloccaggio, con informazioni sullo stato del database di signature e sulle minacce rilevate e bloccate, incluse le 10 minacce più critiche secondo OWASP.

L'**impostazione flessibile delle policy** consente agli amministratori di applicare le impostazioni delle signature in funzione della gravità delle minacce e di impostare una lista di esclusione tramite signature.

Il **log di controllo completo** rende disponibili funzioni di logging e reporting per operazioni di controllo, conformità e reporting.

La **protezione contro la manipolazione dei cookie** riduce la possibilità di violazioni mediante la modifica dei cookie.

La **gestione delle sessioni** consente agli amministratori di impostare timeout globali in base all'inattività degli utenti.

Le **misure anti-evasione** normalizzano le richieste (ad es. standardizzando i set di caratteri o i nomi di percorso codificati o sospetti) prima dell'analisi.

L'**ispezione HTTPS** è in grado di bloccare gli attacchi incorporati nei pacchetti crittografati con SSL.

Le **funzionalità di accelerazione**, che includono caching dei contenuti, compressione e moltiplicazione delle connessioni, migliorano le prestazioni dei siti Web protetti riducendo sensibilmente i costi di transazione.

Il **cloaking dei siti Web** impedisce agli hacker di scoprire l'implementazione dei server Web e sfruttarne eventuali vulnerabilità.

Le **catene di regole personalizzabili** consentono agli amministratori di creare regole/signature personalizzate, oltre a quelle standard proposte da SonicWALL, e di utilizzare modelli di sicurezza sia positivi che negativi.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Specifiche tecniche

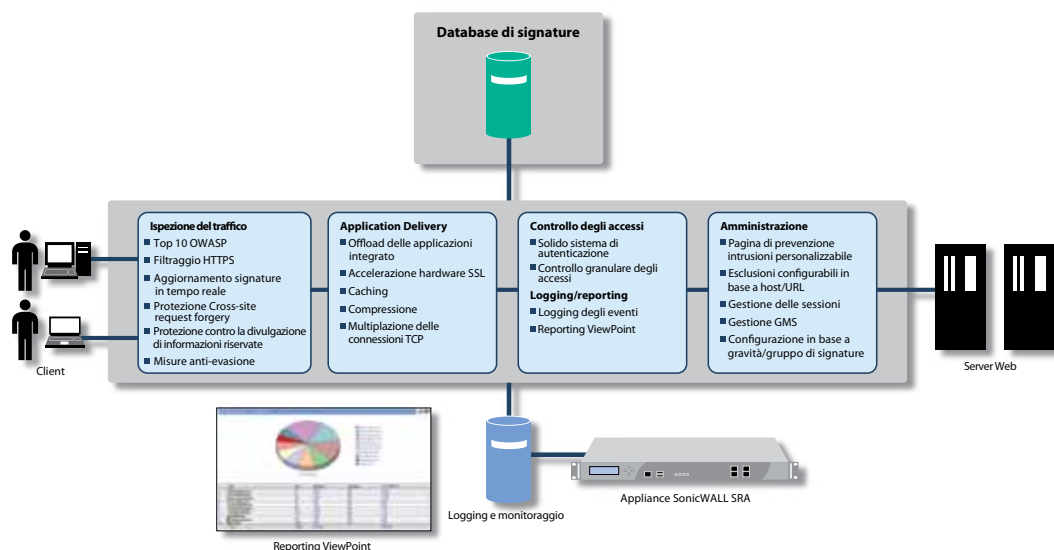


Servizio in abbonamento

- SonicWALL Web Application Firewall Service per SRA 1200 (1 anno)
01-SSC-8877
- SonicWALL Web Application Firewall Service per SRA 1200 (2 anni)
01-SSC-8878
- SonicWALL Web Application Firewall Service per SRA 1200 (3 anni)
01-SSC-8879
- SonicWALL Web Application Firewall Service per SRA 4200 (1 anno)
01-SSC-6055
- SonicWALL Web Application Firewall Service per SRA 4200 (2 anni)
01-SSC-6056
- SonicWALL Web Application Firewall Service per SRA 4200 (3 anni)
01-SSC-6057

Per consultare i codici della linea completa di appliance SonicWALL Secure Remote Access (SRA), visitare il sito www.sonicwall.com.

Architettura SonicWALL Web Application Firewall



Appliance

- Secure Remote Access 1200
- Secure Remote Access 4200
- Secure Remote Access (appliance virtuale)

È richiesto l'abbonamento a Web Application Firewall Service

Capacità

- Throughput SRA 1200: 25 Mbps
- Server back-end supportati (SRA 1200): illimitati (consigliati: 1-5)*
- Throughput SRA 4200: 50 Mbps
- Server back-end supportati (SRA 4200): illimitati (consigliati: 5-10)*
- Throughput SRA Virtual Appliance: 250 Mbps*
- Server back-end supportati (SRA Virtual Appliance): 5-20

* Il numero effettivo di server Web dipende dall'ambiente di rete specifico, dalla configurazione delle policy e del server Web e dai dispositivi hardware sui quali sono installate le appliance virtuali.

Protezione delle applicazioni Web

- Convalida del protocollo HTTP
- Protezione dagli attacchi comuni
 - Iniezione SQL
 - Iniezione da comandi del sistema operativo
 - Cross-site scripting
 - Cross-site request forgery
- Protezione adattativa con catene di regole personalizzabili
 - Supporto limitazione velocità
- Protezione contro la manipolazione dei cookie
- Profiling delle applicazioni per la generazione automatica di regole (solo SRA 4200)
- Cloaking dei siti Web
- Controllo delle reazioni
 - Blocco del client
 - Reindirizzamento
 - Reazione personalizzabile
- Protezione da fughe di dati verso l'esterno
 - Prevenzione di fughe di dati (DLP) per carte di credito, SSN
- Aggiornamenti automatici delle signature
- Controlli del limite del protocollo
- Controllo upload dei file

Application delivery e accelerazione

- Elevata disponibilità (SRA 4200)
- Offload SSL
- Bilanciamento del carico con failover
- Accelerazione hardware SSL (SRA 4200)
- Caching
- Compressione
- Multiplazione delle connessioni TCP

Logging, monitoraggio e reporting

- Log di sistema
- Log del Web Application Firewall
- Log firewall Web
- Log degli accessi
- Log di controllo
- Supporto Syslog
- Report di conformità allo standard PCI
- Dashboard con statistiche globali
 - Minacce rilevate e bloccate nel mondo
- Statistiche e report WAF avanzati
- Integrazione di Viewpoint

Autenticazione e autorizzazione

- LDAP/RADIUS/DATABASE UTENTI LOCALE
- Certificati client
- Single sign-on
- Autenticazione a due fattori
 - RSA SecurID
 - VASCO
 - Password monouso

Linea di soluzioni di sicurezza dinamica SonicWALL



SICUREZZA DI RETE



ACCESSO REMOTO SICURO



SICUREZZA WEB / E-MAIL



BACKUP E RECOVERY



GESTIONE BASATA SU POLICY



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SonicWALL Italy
T + 39.010.7407851
Italy@sonicwall.com

Contatti Supporto SonicWALL
www.sonicwall.com/emea/4724.html