



# SonicWALL Web Application Firewall Service

ACCÈS DISTANT SÉCURISÉ

## Gestion des menaces visant les applications Web

- **Protection contre les 10 principales vulnérabilités OWASP**
- **Protection CSRF**
- **Mises à jour automatiques des signatures**
- **Authentification et autorisation fortes**
- **Protection contre la divulgation d'informations**
- **Puissant tableau de bord**
- **Flexibilité de définition des règles**
- **Journal d'audit complet**
- **Protection contre la falsification de cookies**
- **Gestion de sessions sécurisée**
- **Mesures anti-évasion**
- **Filtrage HTTPS**
- **Fonctionnalités d'accélération**
- **Cloaking de pages Web**
- **Chaînes de règles personnalisées**

En devenant la plate-forme favorite des utilisateurs, en particulier des entreprises, les applications Web 2.0 se trouvent également davantage exposées aux attaques criminelles de type injection SQL, manipulation des paramètres, XSS (cross-site scripting) et déni de service (DoS). Les petites et moyennes entreprises (PME), de plus en plus présentes sur le Web, manquent toutefois souvent des capacités internes nécessaires pour suivre le rythme effréné de l'évolution des risques en matière de sécurité Web. En raison des exigences de conformité, les attaques dirigées contre les applications Web coûtent particulièrement cher aux fournisseurs de services financiers, applicatifs et de santé, ainsi qu'aux entreprises d'e-commerce.

Le SonicWALL® Web Application Firewall (WAF) Service est une solution complète, abordable et prête à l'emploi à l'attention des entreprises, chargée de contrôler la conformité des applications Web. Facile à déployer et à gérer, elle reconnaît les dix principales menaces OWASP et assure la conformité avec la norme PCI DSS, pour une protection contre les attaques par injection et XSS (cross-site scripting), le vol de numéros de cartes de crédit et de sécurité sociale, la falsification de cookies et les attaques CSRF (cross-site request forgery). Des mises à jour dynamiques des signatures et des règles personnalisées protègent contre les vulnérabilités connues et inconnues. Capable de détecter les attaques Web sophistiquées, WAF protège les applications Web (y compris les portails VPN SSL), refuse l'accès en cas de détection d'un programme malveillant dans une application et redirige les utilisateurs vers une page d'erreur explicative. Il comprend une gamme facile à déployer d'options de statistiques et de reporting avancées relatives à la conformité. Le profilage d'applications permet aux administrateurs d'analyser simplement la nature du trafic Web auquel sont confrontés leurs serveurs et de créer des règles automatiquement.

### Caractéristiques et avantages

#### La **protection contre les 10 principales vulnérabilités OWASP (Open Web Application Security Project)**

permet de répondre aux principaux risques sécuritaires en fonction de la prévalence et de la gravité des attaques (norme PCI DSS 6.6 et autres normes industrielles).

La **protection CSRF (Cross-Site Request Forgery)** vient compléter la protection contre les attaques par injection et XSS (cross-site scripting).

Les **mises à jour automatiques des signatures** et le profilage adaptatif d'applications protègent contre les menaces connues et émergentes.

**Authentification et autorisation fortes** pour tout site Web interne ou externe (par ex. les sites Web d'e-commerce). Cela permet de prendre en charge les initiatives de conformité en empêchant tout accès non autorisé à vos sites Web internes et externes. Il s'agit d'une authentification à deux facteurs à jetons, d'une authentification par certificat client et de mots de passe uniques sans jeton. Des règles d'accès granulaires autorisent l'accès à divers serveurs Web selon le nom d'hôte, le sous-réseau, l'adresse IP, le port et le chemin URL.

La **protection contre la divulgation d'informations** permet de bloquer l'accès aux sites Web contenant des mots ou expressions clés définis par l'administrateur, afin d'empêcher la fuite d'informations sensibles. Elle comprend également la prévention des pertes (DLP) de numéros de cartes de crédit et de sécurité sociale.

Le **puissant tableau de bord** avec statistiques avancées présente une interface de gestion Web conviviale qui permet de surveiller l'état du serveur web. La page d'état peut également fournir un aperçu de toutes les activités de surveillance et de blocage des menaces, notamment des informations sur l'état des bibliothèques de signatures et sur les menaces détectées et éliminées, y compris les 10 principales menaces OWASP.

La **flexibilité de définition des règles** permet aux administrateurs d'appliquer des paramètres de signatures adaptés à la gravité des menaces, ainsi que de créer une liste d'exclusion par signature.

Le **journal d'audit complet** permet de répondre aux besoins de journalisation à des fins d'audit, de conformité et de reporting.

La **protection contre la falsification de cookies** limite les risques de faille dus à la modification des cookies.

Grâce à la **gestion de sessions sécurisée**, les administrateurs peuvent définir des temporisations globales selon l'inactivité de l'utilisateur.

Des **mesures anti-évasion** permettent de normaliser les requêtes (par ex. standardisation des jeux de caractères ou des noms de chemins codés ou suspects) avant l'analyse.

Le **filtrage HTTPS** permet de bloquer les attaques intégrées aux paquets chiffrés en SSL.

Les **fonctionnalités d'accélération** incluent la mise en cache, la compression et le multiplexage de connexion et permettent d'améliorer la performance des sites Web protégés, réduisant ainsi considérablement les coûts transactionnels.

Le **cloaking de pages Web** empêche les pirates de deviner l'implémentation du serveur Web et d'exploiter ses vulnérabilités.

Les **chaînes de règles personnalisées** permettent à l'administrateur de créer des règles/signatures personnalisées en plus des règles développées par SonicWALL. Celui-ci peut également employer des modèles de sécurité positifs et négatifs.



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

# Spécifications

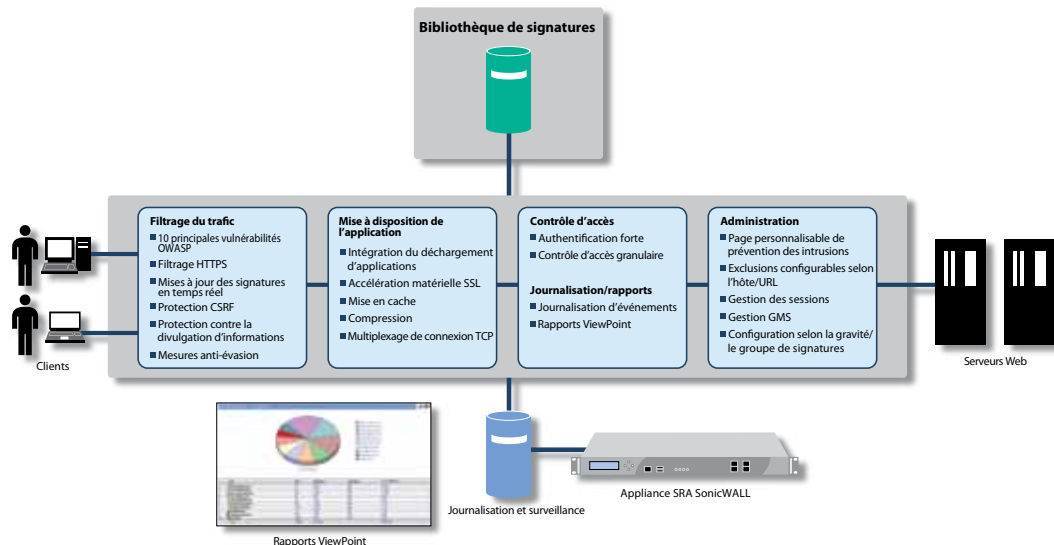


## Service d'abonnement

- SonicWALL Web Application Firewall Service pour SRA 1200 (1 an)  
01-SSC-8877
- SonicWALL Web Application Firewall Service pour SRA 1200 (2 ans)  
01-SSC-8878
- SonicWALL Web Application Firewall Service pour SRA 1200 (3 ans)  
01-SSC-8879
- SonicWALL Web Application Firewall Service pour SRA 4200 (1 an)  
01-SSC-6055
- SonicWALL Web Application Firewall Service pour SRA 4200 (2 ans)  
01-SSC-6056
- SonicWALL Web Application Firewall Service pour SRA 4200 (3 ans)  
01-SSC-6057

Pour consulter les références de la gamme complète d'appiances SonicWALL d'accès distant sécurisé, rendez-vous sur [www.sonicwall.com](http://www.sonicwall.com).

## Architecture de SonicWALL Web Application Firewall



### Appiances

- SRA 1200
- SRA 4200
- Appliance virtuelle SRA

Abonnement à SonicWALL Web Application Firewall Service requis

### Capacité

- Débit SRA 1200 : 25 Mbit/s
- Serveurs d'arrière-plan SRA 1200 pris en charge : sans restriction, 1-5 recommandés\*
- Débit SRA 4200 : 50 Mbit/s
- Serveurs d'arrière-plan SRA 4200 pris en charge : sans restriction, 5-10 recommandés\*
- Débit de l'appliance virtuelle SRA : 250 Mbit/s\*
- Serveurs d'arrière-plan de l'appliance virtuelle SRA pris en charge : 5-20

\* Le nombre réel de serveurs Web dépendra de votre environnement réseau, des règles définies et de la configuration du serveur Web, ainsi que du matériel sous-jacent pour les appliances virtuelles

### Sécurité des applications Web

- Validation du protocole HTTP
- Protection contre les attaques courantes
  - Injection SQL
  - Injection de commande OS
  - Cross-site scripting
  - Attaques CSRF (Cross-Site Request Forgery)
- Sécurité adaptative avec chaînes de règles personnalisées
  - Prise en charge de la limitation de débit
- Protection contre la falsification de cookies
- Profilage d'applications pour la génération automatique de règles (SRA 4200 uniquement)
- Cloaking de pages Web
- Contrôle de réponse
  - Blocage de client
  - Redirection
  - Réponse personnalisée
- Protection contre le vol de données sortantes
  - Protection contre la fuite (DLP) de numéros de cartes de crédit ou de sécurité sociale
- Mises à jour automatiques des signatures
- Vérification des limites de protocole
- Contrôle du chargement de fichiers

### Fourniture et accélération d'applications

- Haute disponibilité (SRA 4200)
- Déchargement SSL
- Equilibrage de charge avec basculement
- Accélération SSL matérielle (SRA 4200)
- Mise en cache
- Compression
- Multiplexage de connexions TCP

### Journalisation, surveillance et reporting

- Journal système
- Journal de Web Application Firewall
- Journal des accès
- Journal d'audit
- Prise en charge Syslog
- Rapports sur la conformité PCI
- Tableau de bord des statistiques globales
  - Menaces détectées et bloquées dans le monde
- Statistiques et rapports WAF avancés
- Intégration de ViewPoint

### Authentification et autorisation

- Base de données utilisateurs LDAP/Radius/locale
- Certificats clients
- Signature unique (SSO)
- Authentification à deux facteurs
  - RSA Securid
  - VASCO
  - Mot de passe unique

## La gamme SonicWALL de solutions de sécurité dynamique



SÉCURITÉ  
RÉSEAU



ACCÈS DISTANT  
SÉCURISÉ



SÉCURISATION WEB  
ET DE MESSAGERIE



SAUVEGARDE ET  
RÉCUPÉRATION



GESTION  
ET RÈGLES



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SonicWALL France  
T +33 1 49 33 73 19 France@sonicwall.com

SonicWALL BeNeLux  
T +32 (0) 15 280 985 Benelux@sonicwall.com

Contacts du support SonicWALL  
[www.sonicwall.com/emea/4724.html](http://www.sonicwall.com/emea/4724.html)