SonicWall Protection Service Suites

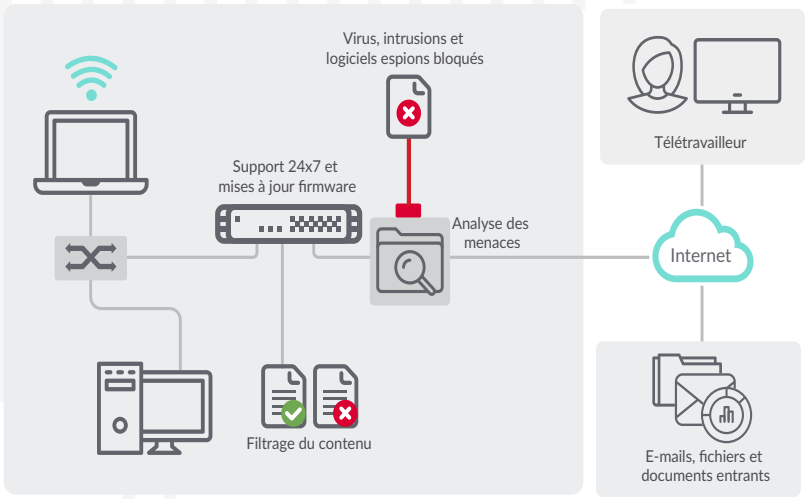
Gestion complète de la sécurité réseau et des pare-feux en une seule offre intégrée

Comprendre et gérer efficacement la sécurité réseau est difficile et complexe. Heureusement, il existe une solution simple pour bloquer les attaques évoluées, évaluer et éliminer les risques et faciliter la gestion des pare-feux.

SonicWall intègre une vaste gamme de services de sécurité réseau au sein de différentes offres pratiques et économiques : Threat Protection Service Suite, Essential Protection Service Suite et Advanced Protection Service Suite.

AVANTAGES

- Solution complète de sécurité réseau
- Protection antivirus et anti-logiciels espions certifiée ICSA
- Gestionnaire de la sécurité réseau cloud
- Service anti-spam complet
- Technologie IPS d'avant-garde
- Surveillance et contrôle des applications
- Sécurité DNS
- Filtrage du contenu
- Support 24h/24, 7j/7 avec mises à jour du firmware et remplacement du matériel
- Sandbox réseau multimoteur avec la technologie brevetée RTDMI™ (Real-Time Deep Memory Inspection)



ICSA labs CERTIFIED ENTERPRISE FIREWALL

ICSA labs CERTIFIED ANTI-VIRUS

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

ICSA labs CERTIFIED ANTI-MALWARE

FICHE TECHNIQUE

Caractéristiques et avantages

Les services de protection contre les menaces gardent votre réseau à l'abri des virus, intrusions, zombies, logiciels espions, chevaux de Troie, vers et autres attaques malveillantes. Dès que de nouvelles menaces sont identifiées et souvent avant que les éditeurs de logiciels aient pu fournir des correctifs, les pare-feux SonicWall et la base de données Capture Cloud sont automatiquement mis à jour avec des signatures qui protègent contre ces menaces. Ces pare-feux SonicWall renferment un moteur breveté RTDMI™ qui analyse différents types d'applications et de protocoles dans le trafic, garantissant la protection permanente de votre réseau face aux attaques internes et externes et autres vulnérabilités applicatives.

Network Security Manager (NSM), une solution cloud de gestion centralisée de pare-feux multi-locataires, vous permet de gérer de manière centralisée et sans erreur l'ensemble des opérations de pare-feu en adoptant des flux pouvant être contrôlés. Les **fonctionnalités de reporting et d'analyse** vous offrent une visibilité sur une interface unique afin de surveiller et d'identifier les menaces grâce à l'unification et à la mise en corrélation des journaux de tous les pare-feux.

Le service **Capture ATP** révolutionne la détection de menaces évoluées et le sandboxing via une solution cloud multimoteur permettant de stopper les attaques inconnues et zero-day au niveau de la passerelle. Capture ATP bloque les attaques zero-day avant qu'elles ne pénètrent sur le réseau. Il vous permet d'établir une protection avancée contre le paysage changeant des menaces et d'analyser un vaste éventail de types de fichiers.

La protection **antivirus de passerelle** certifiée ICSA associe un anti-malware réseau à une base de données cloud mise à jour de manière dynamique, comportant des dizaines de millions de signatures de logiciels malveillants. La protection anti-logiciels espions dynamique bloque l'installation de logiciels malveillants et perturbe les communications établies par les logiciels espions déjà installés.

La **technologie IPS d'avant-garde** protège contre les vers, chevaux de Troie, vulnérabilités logicielles et autres intrusions en scannant l'ensemble du trafic à la recherche de comportements malveillants ou anormaux, ce qui augmente la fiabilité et les performances du réseau.

Application Intelligence and Control réunit un ensemble de règles granulaires, spécifiques aux applications, qui permettent de classifier ces dernières et aident les administrateurs à contrôler et à gérer toutes les applications, qu'elles soient à caractère professionnel ou privé.

SonicWall **Comprehensive Anti-Spam Service** offre aux PME une efficacité supérieure à 99 % contre le spam : plus de 80 % des spams sont bloqués au niveau de la passerelle, tandis que des techniques anti-spam évoluées telles que le filtrage Adversarial Bayesian™ et l'apprentissage machine analysent le reste du courrier.

Content Filtering Services (CFS) vous permet d'appliquer des règles d'utilisation d'Internet et de contrôler l'accès en interne à des contenus Web indésirables, non productifs voire illégaux grâce au filtrage de contenu complet. Le service de filtrage de contenu **CFS 5.0** basé sur la réputation fournit un score de réputation qui prévoit le risque de sécurité d'une URL selon 93 catégories Web.

Le **filtrage DNS** bloque les applications ou sites malveillants au niveau de la couche DNS afin de filtrer tout contenu nuisible ou inapproprié sans activer le déchiffrement TLS ni affecter les performances.

Les **points d'accès** hautement sécurisés de SonicWall peuvent être gérés via le cloud grâce à SonicWall Wireless Network Manager (WNM) ou par l'intermédiaire des pare-feux SonicWall, alliant facilité de gestion et une intégration transparente avec les produits sans fil SonicWall.

L'intégration du **contrôle d'accès réseau** permet aux clients SonicWall de contrôler les accès à leur réseau via l'intégration avec Aruba ClearPass, qui offre un profilage, une authentification et une autorisation complets et précis des systèmes et des appareils tentant d'accéder aux ressources informatiques. SonicOS présente une API RESTful qui prendra en charge Aruba ClearPass en tant que solution NAC pour l'intégration aux pare-feux de nouvelle génération SonicWall. Cette architecture transformera la sécurité statique en sécurité contextuelle afin d'assurer une protection plus flexible et plus évoluée.

Le **support 24h/24, 7j/7** avec mises à jour du firmware et remplacement du matériel protège votre activité et votre investissement SonicWall. Il comprend un accès 24 h/24 à l'assistance téléphonique et Web pour la configuration de base et le dépannage, ainsi que le remplacement de matériel en cas de panne.

FONCTIONNALITÉ	THREAT PROTECTION SECURITY SUITE*	ESSENTIAL PROTECTION SECURITY SUITE	ADVANCED PROTECTION SECURITY SUITE
Support 24h/24, 7j/7	O	O	O
IPS	O	O	O
Contrôle des applications	O	O	O
Service de filtrage du contenu	O	O	O
Antivirus de passerelle	O	O	O
Sécurité DNS – de base	O	O	O
Filtrage DNS	N	N	O
Intégration du contrôle d'accès réseau (NAC) avec Aruba ClearPass	O	O	O
Intégration Wi-Fi 6	O	O	O
Inspection approfondie des paquets pour SSL	O	O	O
Mises à jour GeoIP	O	O	O
Service de botnet	O	O	O
Service anti-spam complet	N	O	O
Capture ATP – sandboxing (statique, RTDMI, mémoire, hyperviseur, émulation)	N	O	O
Gestion NSM (cloud)	N	N	O
Reporting NSM (cloud) – conservation pendant 7 jours	N	N	O

* Disponible uniquement sur TZ 270, 370 et 470

À propos de SonicWall

SonicWall offre une solution de cybersécurité stable, évolutive et transparente pour l'ère de l'hyper-distribution, dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com

Datasheet-ProtectionServiceSuites-A4-JK-9964