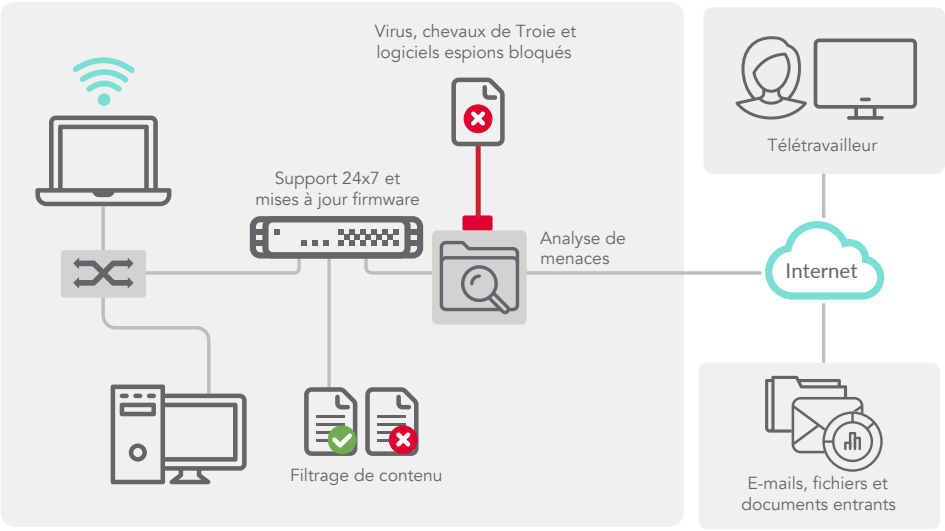
Advanced Gateway Security Suite

Toute la protection réseau en une seule offre intégrée

Comprendre la sécurité des réseaux peut parfois être difficile. Garantir l'immunité de votre réseau face aux menaces connues et inconnues ne doit pas l'être. Vous n'aurez plus à choisir entre différents services de sécurité complémentaires. La suite AGSS (SonicWall Advanced Gateway Security Suite) intègre tout ce qu'exigent les services de sécurité pour une protection de bout en bout, en une seule offre pratique et économique.

Disponible sur tous les pare-feux physiques et virtuels, notamment NSsp, NSa, TZ et NSv Series, SonicWall AGSS garde votre réseau à l'abri des virus, intrusions, zombies, logiciels espions, chevaux de Troie, vers et autres attaques malveillantes. Examinez les fichiers suspects au niveau de la passerelle, grâce à l'inspection d'une sandbox Cloud multicouche, afin de protéger votre réseau des menaces inconnues. 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. Chaque pare-feu SonicWall renferme un moteur breveté RFDPI (Reassembly-Free Deep Packet Inspection®) 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. Votre solution SonicWall fournit également les outils permettant 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. Enfin, cet ensemble puissant de services comprend également un support technique joignable 24 h/24, d'importantes mises à jour firmware et des fonctions de remplacement matériel.



Avantages :

- Solution complète de sécurité réseau
- Protection antivirus et anti-logiciels espions de passerelle certifiée ICSA
- Technologie IPS d'avant-garde
- Surveillance et contrôle des applications
- Filtrage de contenu
- Support 24h/24, 7j/7 avec mises à jour du firmware et remplacement du matériel
- Sandbox réseau multi-moteur avec technologie RTDMI de SonicWall
- Écran unique de gestion dans le Cloud

Advanced Gateway Security Suite
NS*sp* 12800 (1 an) 01-SSC-6591
NS*sp* 12400 (1 an) 01-SSC-6588
NS*a* 9650 (1 an) 01-SSC-2036
NS*a* 9450 (1 an) 01-SSC-0414
NS*a* 9250 (1 an) 01-SSC-0038
NS*a* 6650 (1 an) 01-SSC-8761
NS*a* 5650 (1 an) 01-SSC-3674
NS*a* 4650 (1 an) 01-SSC-3493
NS*a* 3650 (1 an) 01-SSC-3451
NS*a* 2650 (1 an) 01-SSC-1783
TZ600 Series (1 an) 01-SSC-1460
TZ500 Series (1 an) 01-SSC-1450
TZ400 Series (1 an) 01-SSC-1440
TZ300 Series (1 an) 01-SSC-1430
NS*v* 1600 (1 an 01-SSC-5787
NS*v* 800 (1 an) 01-SSC-5737
NS*v* 400(1 an) 01-SSC-5681
NS*v* 300 (1 an) 01-SSC-5584
NS*v* 200 (1 an) 01-SSC-5306
NS*v* 100 (1 an) 01-SSC-5219
NS*v* 50 (1 an) 01-SSC-5194
NS*v* 25 (1 an) 01-SSC-5165
NS*v* 10 (1 an) 01-SSC-5008
Références pluriannuelles disponibles.
Pour connaître les références de la gamme complète de pare-feux SonicWall, rendez-vous sur www.sonicwall.com.

SonicWall Advanced Gateway Security Suite comprend :

- un abonnement à Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control* Service
- l'abonnement à Content Filtering Service
- l'abonnement au support 24x7
- l'abonnement à Capture Advanced Threat Protection (ATP) Service
- l'abonnement à Capture Security Center Lite

Fonctionnalités et avantages

La solution complète de sécurité réseau intègre tout ce dont vous avez besoin pour garantir une protection de bout en bout face aux ransomewares, virus, logiciels espions, vers, chevaux de Troie, logiciels publicitaires, enregistreurs de frappes, MMC (Malicious Mobile Code) et autres applications dangereuses, ainsi que contenus Web.

Le service ATP (Capture Advanced Threat Protection) révolutionne la détection de menaces évoluées et le sandboxing via une solution Cloud multi-moteur permettant de stopper les attaques inconnues et zero-day au niveau de la passerelle, et de déclencher des corrections automatiques.

Capture ATP inclut la technologie RTDMI (Real-Time Deep Memory Inspection) de SonicWall qui détecte et bloque les logiciels malveillants ne présentant pas de comportement suspect ou dissimulant son arsenal d'armes par le chiffrement. En les forçant à révéler leurs armes dans la mémoire, le moteur RTDMI peut détecter et bloquer proactivement des menaces très répandues et de type zero-day ainsi que des logiciels malveillants inconnus, en utilisant avec précision des techniques d'inspection en temps réel, basées sur la mémoire.

La protection antivirus et anti-logiciels espions de passerelle certifiée ICSA associe un anti-malware niveau réseau à une base de données Cloud comptant des dizaines de millions de signatures de logiciels malveillants, pour une sécurité approfondie contre les menaces évoluées modernes.

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.

Le filtrage de contenu répond aux problématiques de sécurité et de productivité grâce à des contrôles permettant d'appliquer les règles d'utilisation d'Internet et de bloquer l'accès au contenu Web nuisible et non productif.

Le support dynamique 24h/24, 7j/7 avec mises à jour du firmware et remplacement du matériel protège et complète votre investissement SonicWall par la fourniture de mises à jour et mises à niveau firmware indispensables, une assistance technique efficace, un remplacement matériel immédiat et l'accès à des outils d'auto-assistance en ligne.

Capture Security Center Lite vous permet de gérer votre déploiement SonicWall et d'exécuter des sauvegardes/restaurations des préférences de votre pare-feu, le tout via un écran unique dans le Cloud.

Les services AGSS en un coup d'œil

Sandbox multi-moteur, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention et Application Intelligence and Control* Service

- Le moteur antivirus en temps réel au niveau de la passerelle traque en temps réel les virus, vers, chevaux de Troie et autres menaces Internet.
- La protection anti-logiciels espions dynamique bloque l'installation de logiciels malveillants et perturbe les communications établies par les logiciels espions déjà installés.
- Le puissant service de prévention des intrusions protège contre un vaste éventail de menaces réseau telles que vers, chevaux de Troie et autres logiciels malveillants.
- La surveillance et le contrôle des applications permet de classifier les applications et d'appliquer des règles.

- La bibliothèque de signatures avec mise à jour dynamique garantit une protection en continu.
- La sandbox multi-moteur avec technologie RTDMI permet d'éviter les menaces inconnues telles que les attaques zero-day et les ransomwares.

Capture Advanced Threat Protection (Capture ATP)

- Blocage des attaques zero-day avant qu'elles ne pénètrent sur le réseau.
- Déploiement rapide des signatures correctives sur d'autres appliances de sécurité réseau.
- Protection avancée pour combattre l'ensemble protéiforme des menaces.
- Analyse d'un vaste éventail de types de fichiers.

Content Filtering Service (CFS)

- Le filtrage de contenu complet assure le contrôle personnalisé de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux.
- Les classifications de pages Web avec mise en cache locale sur les pare-feux SonicWall assurent une réponse quasi instantanée des sites fréquemment consultés.
- L'architecture de classification à actualisation dynamique examine tous les sites Web demandés par rapport à une base de données Cloud qui contient des millions d'URL, d'adresses IP et de domaines, puis compare chaque classification aux règles paramétrées localement.

Content Filtering Client

- Blocage rapide et précis des logiciels malveillants grâce à la technologie RTDMI (Real-Time Deep Memory Inspection).
- SonicWall Content Filtering Client étend la sécurité et la productivité par l'application de règles d'utilisation d'Internet sur les terminaux situés en dehors du périmètre du pare-feu. Existe en tant que service d'abonnement séparé pour terminaux Windows, Mac OS et Chrome.

Support 24h/24, 7j/7

- Les mises à jour et mises à niveau logiciel et firmware maintiennent le réseau en sécurité et votre solution reste aussi efficace qu'au premier jour.
- Un accès 24 heures/24 à l'assistance téléphonique et Web est disponible pour la configuration de base et le dépannage.
- Remplacement de matériel en cas de panne.
- Abonnement annuel aux bulletins de service SonicWall et accès aux outils d'assistance électroniques et aux groupes de discussion dirigés.

Capture Security Center Lite

- Portail Cloud
- Écran unique de gestion
- Sauvegarde et restauration des préférences de pare-feu

Pour plus d'informations sur SonicWall Advanced Gateway Security Suite, rendez-vous sur www.sonicwall.com.

À propos de nous

SonicWall s'engage depuis plus de 27 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution automatisée de détection et de prévention des failles en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 215 pays et territoires, leur permettant de se concentrer sans crainte sur leur cœur de métier.

*Pour SuperMassive 9000, NS*a* 9250/9450/9650 et NS*sp* 12000 Series, CSC Management est automatiquement disponible sur activation de l'abonnement AGSS correspondant.

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

Datasheet-AdvancedGatewaySecuritySuite-US-VG-MKTG4091