

# Comprehensive Gateway Security Suite

Une offre intégrée pour stopper les menaces connues et les attaques

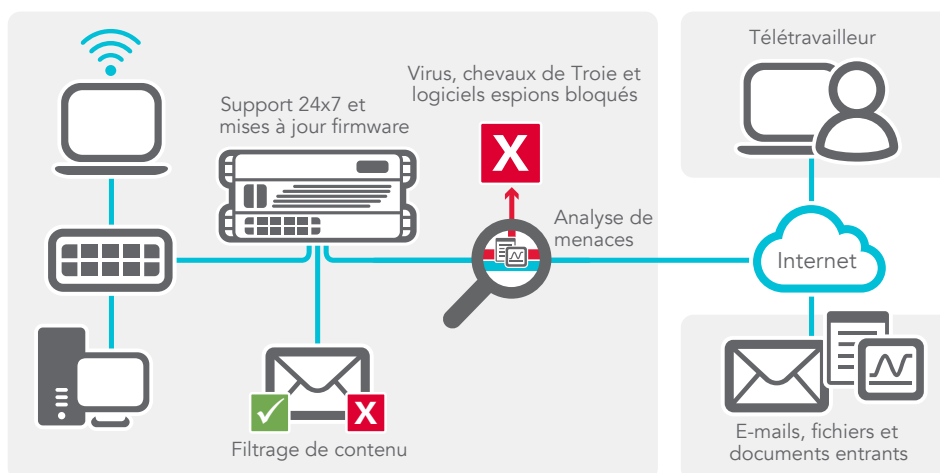
Chaque jour voit naître des centaines de milliers de logiciels malveillants personnalisés. Le paysage des menaces évolue à une telle vitesse qu'il est impossible d'y faire face seul. Au moment de choisir les technologies de sécurité propres à assurer la protection de votre réseau, vous ne devez pas être confronté aux incertitudes et à la complexité associées aux malwares que vous voulez combattre. SonicWall™ Comprehensive Gateway Security Suite (CGSS) simplifie et accélère la sélection de vos services de sécurité en intégrant tout ce qu'il faut pour protéger votre réseau contre les menaces connues au sein d'une offre pratique et abordable.

Disponible sur les pare-feux SonicWall TZ, NSA (Network Security Appliance) et SuperMassive, SonicWall CGSS

garde 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 Cloud AV 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

## Avantages :

- Solution de sécurité complète contre les menaces connues
- Protection antivirus et anti-logiciels espions certifiée ICSA
- Technologie IPS d'avant-garde
- Surveillance et contrôle des applications
- Filtrage du contenu
- Support 24h/24, 7j/7 avec mises à jour du firmware et remplacement du matériel
- Mise à niveau aisée vers AGSS pour bénéficier d'une sandbox multi-moteur



Réseau sécurisé SonicWall

## Comprehensive Gateway Security Suite

SuperMassive E10800 (1 an)  
01-SSC-9569

SuperMassive E10400 (1 an)  
01-SSC-9551

SuperMassive E10200 (1 an)  
01-SSC-9533

SuperMassive 9800 (1 an)  
01-SSC-0809

SuperMassive 9600 (1 an)  
01-SSC-4100

SuperMassive 9400 (1 an)  
01-SSC-4136

SuperMassive 9200 (1 an)  
01-SSC-4172

NSA 6600 (1 an)  
01-SSC-4210

NSA 5600 (1 an)  
01-SSC-4234

NSA 4600 (1 an)  
01-SSC-4405

NSA 3600 (1 an)  
01-SSC-4429

NSA 2650 (1 an)  
01-SSC-1964

TZ600 (1 an)  
01-SSC-0258

TZ500 Series (1 an)  
01-SSC-0488

TZ400 Series (1 an)  
01-SSC-0567

TZ300 Series (1 an)  
01-SSC-0638

SOHO Series (1 an)  
01-SSC-0688

Références pluriannuelles disponibles.

Pour connaître les références de la gamme complète de pare-feux SonicWall, rendez-vous sur [sonicwall.com](http://sonicwall.com).

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 de services performants comprend également un support technique joignable 24 heures/24, d'importantes mises à jour firmware et le remplacement de matériel.

SonicWall Comprehensive Gateway Security Suite comprend les abonnements suivants :

- Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Service
- Content Filtering Service
- Support 24h/24, 7j/7

### Caractéristiques et avantages

La **solution de sécurité réseau** intègre tout ce dont vous avez besoin pour garantir votre protection face aux menaces connues : virus, logiciels espions, vers, chevaux de Troie, logiciels publicitaires, enregistreurs de frappes, MMC et autres applications et contenus Web dangereux.

La **protection antivirus et anti-logiciels espions certifiée ICSA** associe un anti-malware niveau réseau à une base de données Cloud croissante, comptant plus de 20 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 classer ces dernières et

aident les administrateurs à contrôler et à gérer toutes les applications, qu'elles soient à caractère professionnel ou privé.

À des fins de sécurité et de productivité, le **filtrage de contenu** offre les contrôles permettant d'appliquer des règles d'utilisation d'Internet et de bloquer l'accès aux contenus Web nuisibles et non productifs.

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.

### Les services CGSS en un coup d'œil Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and 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 dynamique contre les logiciels espions 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 programmes malveillants.
- La surveillance et le contrôle des applications permettent de classer les applications et d'appliquer des règles.
- La base de données de signatures avec mise à jour dynamique garantit une protection en continu.

## Service de filtrage de contenu (CFS)

- Le filtrage de contenu complet assure le contrôle 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.
- Une architecture de classification à actualisation dynamique examine toutes les pages Web demandées par rapport à une base de données Cloud répertoriant des millions d'URL, d'adresses IP et de domaines, puis compare chaque classification aux règles paramétrées localement.

## Content Filtering Client

- 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. Disponible en abonnement indépendant pour les terminaux Windows, Mac OS et Chrome.

## Support 24h/24, 7j/7

- Les mises à jour et mises à niveau logiciel et firmware maintiennent la sécurité du réseau et votre solution reste aussi efficace qu'au premier jour.
- Un accès 24 heures/24 à l'assistance téléphonique, par chat ou courrier électronique et Web est disponible pour la configuration de base et le dépannage.
- Remplacement anticipé 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.

## Mise à niveau aisée vers AGSS

Advanced Gateway Security Suite (AGSS) inclut toutes les fonctionnalités offertes par CGSS, à quoi s'ajoute Capture Advanced Threat Protection (ATP), une plateforme de sandbox multi-moteur, destinée à protéger contre les menaces inconnues telles que les attaques zero-day. [Pour en savoir plus, cliquez ici.](#)

[Pour plus d'informations sur SonicWall Comprehensive Gateway Security Suite, rendez-vous sur \[www.sonicwall.com\]\(http://www.sonicwall.com\).](#)

## À propos de nous

SonicWall s'engage depuis plus de 25 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 de cybersécurité en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.