



# Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service

GESTION UNIFIÉE DES MENACES

Service intelligent de protection en temps réel

SonicWALL® Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service est à la fois un antivirus, un anti-logiciels espions et un service de prévention des intrusions au niveau de la passerelle, réunis pour fournir une protection en temps réel intelligente du réseau contre les attaques sophistiquées ciblant la couche d'application et basées sur le contenu. Chaque jour naissent de nouvelles menaces qu'il est généralement impossible de prévoir. Pour y faire face et offrir une protection maximum, SonicWALL dispose d'un moteur de filtrage applicatif qui les guette directement au niveau de la passerelle de sécurité. Les fichiers téléchargés, envoyés et comprimés sont ainsi comparés à une bibliothèque de signatures très complète et constamment actualisée, établie par l'équipe SonicAlert de SonicWALL en collaboration avec des fournisseurs tiers.

La solution de SonicWALL est la seule à pouvoir traiter des fichiers de taille pratiquement illimitée et jusqu'à des centaines de milliers de téléchargements simultanés, offrant ainsi le meilleur de l'évolutivité et de la performance pour les réseaux destinés à croître. Et pour aller encore plus loin dans la sécurité, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service protège contre les attaques au niveau de la couche d'application, qu'elles soient d'origine externe ou interne. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service est proposé sous forme d'abonnements d'un, de deux ou trois an(s), destinés aux appliances de sécurité réseau SonicWALL séries TZ, NSA et NSA E-Class.

## Caractéristiques et avantages

**Le filtrage de fichiers, sans limite de taille, circulant par tous les types de ports** et dans les deux directions, permet une protection maximale contre les menaces utilisant des ports atypiques.

**L'analyse antivirus en temps réel au niveau de la passerelle** offre une protection efficace au niveau fichier grâce à un moteur haute performance qui procède à un scannage en temps réel pour détecter les virus, vers, chevaux de Troie et autres menaces provenant d'Internet.

**La protection dynamique contre les logiciels espions** bloque l'installation de logiciels espions au niveau de la passerelle et interrompt la communication en arrière-plan de programmes espions existants transmettant des données confidentielles.

**Le service puissant de prévention des intrusions** protège contre un large éventail de menaces au niveau de la couche d'application en analysant la charge utile des paquets à la recherche de vers, chevaux de Troie, vulnérabilités logicielles (telles que dépassements de la mémoire tampon, applications de messagerie instantanée et poste à poste, intrusions par porte dérobée) et autres codes malicieux.

Le **pare-feu applicatif** est un ensemble de règles granulaires spécifiques aux applications qui opère la classification des applications et l'exécution des règles, de façon à aider les administrateurs à contrôler et à gérer les applications, professionnelles ou non.

**Une bibliothèque de signatures actualisée dynamiquement** et contenant des milliers de signatures fournies par l'architecture d'exécution distribuée de SonicWALL détecte et protège contre les virus, logiciels espions, vers et chevaux de Troie, ainsi que contre le transfert de fichiers de messagerie instantanée et poste à poste.

Première sur le marché à utiliser un moteur de scannage par paquet, la solution SonicWALL est la seule à être capable de traiter des fichiers de taille pratiquement illimitée et jusqu'à des centaines de milliers de téléchargements simultanés, offrant par là même **une évolutivité et une performance maximum** pour les environnements de réseaux d'aujourd'hui.

**Une protection contre les attaques dites du « jour zéro »** est offerte par l'équipe SonicAlert de SonicWALL et des fournisseurs tiers, garantissant le blocage de vulnérabilités avant même que celles-ci puissent être exploitées.

**L'analyse inter-zones** offre une protection supplémentaire contre les menaces en permettant aux administrateurs d'exécuter la prévention des intrusions et le scannage antivirus non seulement entre chaque zone du réseau et Internet, mais aussi entre les différentes zones du réseau.

**Le contrôle d'applications** permet d'empêcher les programmes de partage de fichiers poste à poste et de messagerie instantanée d'opérer à travers le pare-feu, fermant ainsi une porte dérobée potentielle susceptible d'être empruntée pour mettre le réseau en danger. Cela améliore la productivité des employés tout en économisant la bande passante Internet.

**La journalisation** exhaustive de toutes les tentatives d'intrusion avec la possibilité de filtrer les fichiers journalisés suivant le niveau de priorité permet aux administrateurs de mettre en évidence les attaques prioritaires et d'établir **des rapports** précis basés sur la source, la destination et le type des attaques grâce à SonicWALL ViewPoint® et au Système de Gestion globale (GMS).

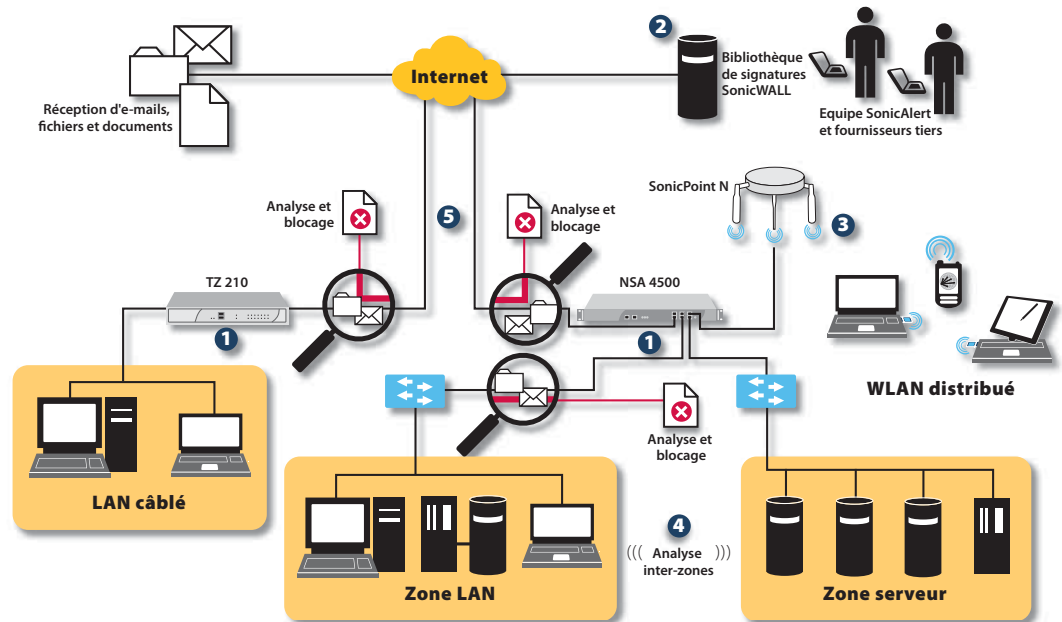
- Filtrage de fichiers, sans limite de taille, circulant par tous les types de ports
- Analyse anti-virus en temps réel au niveau de la passerelle
- Protection dynamique contre les logiciels espions
- Service puissant de prévention des intrusions
- Pare-feu applicatif
- Bibliothèque de signatures actualisée dynamiquement
- Evolutivité et performance maximum
- Protection contre les attaques « jour zéro »
- Analyse inter-zones
- Contrôle d'applications
- Journalisation et rapports

**SONICWALL**®

# Spécifications

## Architecture de filtrage applicatif SonicWALL

### Déploiement de SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service sur les séries TZ et NSA



- 1 Moteur haute performance permettant de détecter en temps réel les virus, logiciels espions, vers, chevaux de Troie et autres menaces provenant d'Internet
- 2 Bibliothèque contenant des milliers de signatures actualisée en permanence
- 3 Protection élargie aux réseaux câblés et sans fil
- 4 Analyse inter-zones pour une protection non seulement entre chaque zone du réseau et Internet, mais aussi entre les différentes zones internes du réseau
- 5 Protection pour les communications d'affaires, comprenant la navigation sur le Web, l'utilisation de messageries électroniques et le transfert de fichiers

## Liste de caractéristiques

<b>Fonctions d'analyse antivirus</b>	<ul style="list-style-type: none"><li>■ Protocoles communs tels que SMTP, POP3, IMAP, HTTP, FTP, NetBIOS et bien d'autres</li><li>■ Tous les protocoles non chiffrés à travers tous types de ports</li><li>■ Des dizaines de protocoles de flux</li><li>■ Messagerie instantanée et transferts de fichiers poste à poste</li></ul>
<b>Protection contre les menaces</b>	<ul style="list-style-type: none"><li>■ Protection contre les virus, logiciels espions, vers, chevaux de Troie, vulnérabilités logicielles (telles que dépassements de la mémoire tampon, applications de messagerie instantanée et poste à poste, intrusions par porte dérobée) et autres codes malicieux</li></ul>
<b>Evolutivité</b>	<ul style="list-style-type: none"><li>■ Capacité de scanner un nombre infini de téléchargements simultanés, quelle que soit la taille de fichier</li></ul>
<b>Bibliothèque de signatures</b>	<ul style="list-style-type: none"><li>■ Bibliothèque de signatures actualisée dynamiquement, comprenant des milliers de signatures d'attaques, de vulnérabilités et de virus hautement dangereux</li></ul>
<b>Journalisation et rapports</b>	<ul style="list-style-type: none"><li>■ Journalisation et alertes en temps réel</li><li>■ Rapports précis grâce à SonicWALL ViewPoint et le Système de Gestion globale (GMS)</li></ul>
<b>Formats de compression supportés</b>	<ul style="list-style-type: none"><li>■ ZIP, Deflate et GZIP</li></ul>

Pour plus d'informations sur la gamme SonicWALL de services de sécurité à valeur ajoutée, dont Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Enforced Client Anti-Virus and Anti-Spyware, et le service de filtrage de contenu, consultez notre site Internet à l'adresse suivante : <http://www.sonicwall.com>.

### Support France

Appel gratuit : 0800.970.019  
Tél. : +31 (0) 411.617.812  
E-mail : [sales\\_support-europe@sonicwall.com](mailto:sales_support-europe@sonicwall.com)

### Bureau France

Tél. : +33.01.49.33.73.09  
Inside sales : +32 (0)15.293.001  
E-mail : [france@sonicwall.com](mailto:france@sonicwall.com)



### Service d'abonnement d'1 an :

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour NSA E6500  
01-SSC-6130

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour NSA E7500  
01-SSC-6131

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour NSA E5500  
01-SSC-6132

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour NSA 5000  
01-SSC-6159

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour NSA 4500  
01-SSC-6133

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour NSA 3500  
01-SSC-6134

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour NSA 2400  
01-SSC-6135

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour série NSA 240  
01-SSC-6162

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour série TZ 210  
01-SSC-6165

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour série TZ 200  
01-SSC-6168

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour série TZ 100  
01-SSC-6171

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour série TZ 190  
01-SSC-5751

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour TZ 180  
10 et 25 nœuds  
01-SSC-6912

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service pour TZ 180 Series  
Nombre de nœuds illimité  
01-SSC-6915

Services d'abonnements pluriannuels également disponibles.

Vous trouverez les références de la gamme complète des appliances de sécurité réseau SonicWALL sur [www.sonicwall.com](http://www.sonicwall.com)