



- **Gestion centralisée de la sécurité et du réseau**
- **Configuration et déploiement VPN efficaces**
- **Système de surveillance active et d'alerte**
- **Journalisation centralisée**
- **Logiciel, matériel ou appliance virtuelle**
- **Outils intelligents de reporting et de visualisation des activités**
- **Gestion hors ligne**
- **Gestionnaire de licences simplifié**
- **Support SNMP**
- **Options d'intégration évoluées**

Le Système de Gestion globale de SonicWALL (SonicWALL GMS) fournit aux structures de toute taille, entreprises distribuées et fournisseurs de services, une solution flexible, puissante et intuitive pour gérer de manière centralisée et déployer rapidement les appliances SonicWALL, ainsi que les configurations des règles de sécurité. SonicWALL GMS™ assure également une surveillance centralisée en temps réel des réseaux et fournit des rapports exhaustifs sur les règles de sécurité et normes de conformité.

L'interface utilisateur Web intuitive de SonicWALL GMS permet de contrôler facilement le cycle de vie de milliers d'appliances et services SonicWALL de pare-feu, anti-spam, accès distant sécurisé, sauvegarde et récupération – de la configuration initiale aux modifications de règles complexes, en passant par les mises à jour à distance. Et grâce à une interface de gestion unique, GMS simplifie la tâche des administrateurs de réseaux distribués et diminue le coût total de possession (TCO). Les fournisseurs de services profitent des fonctions de gestion multi-entreprise qui permettent de rassembler, de grouper et de classer des milliers d'appliances gérées de différents clients et leurs règles de sécurité correspondantes. Grâce à une architecture de reporting intégrée, les administrateurs peuvent personnaliser et programmer les rapports selon les besoins des clients gérés, des directions d'entreprises ou des audits de conformité. SonicWALL GMS peut être déployé de manière flexible comme logiciel sur un serveur Windows® tiers, comme appliance de gestion universelle UMA E-Class SonicWALL, ou comme appliance SonicWALL GMS virtuelle dans un environnement VMware®.

Caractéristiques et avantages

La **gestion centralisée de la sécurité et du réseau** est assurée par un outil flexible, puissant et intuitif qui permet de déployer, de gérer et de surveiller un environnement réseau distribué et de définir des règles de manière centralisée. Les administrateurs peuvent désormais définir, distribuer et faire appliquer un ensemble de règles de services et de sécurité pour des milliers d'appliances SonicWALL de pare-feu, anti-spam, accès distant sécurisé, sauvegarde et récupération.

Les fonctions de **configuration et de déploiement VPN efficaces** permettent de réduire la charge des administrateurs de réseaux distribués, les coûts et la complexité associés à l'établissement et au maintien des règles de sécurité, de la connectivité VPN et des configurations réseau. Les fournisseurs de services peuvent rassembler et unifier l'ensemble des règles de sécurité de milliers de clients, permettant en outre de respecter plus efficacement les contrats de niveau de service.

Le **système de surveillance active et d'alerte** émet des alertes en temps réel et comprend des options de surveillance intégrées qui permettent aux administrateurs de prendre des mesures préventives et de remédier immédiatement aux problèmes.

La **journalisation centralisée** rassemble en un endroit les événements de sécurité et les journaux de milliers d'appliances, permettant ainsi de réaliser des analyses forensiques du réseau à partir d'un seul et même point.

Il existe plusieurs options de déploiement flexibles : comme **logiciel** (au sein de l'infrastructure existante), comme **matériel** (sur un boîtier hautes performances) ou comme **appliance virtuelle** (dans le cas de ressources informatiques partagées pour en optimiser l'utilisation, faciliter la migration et réduire les coûts).

Les **outils intelligents de reporting et de visualisation des activités** permettent l'établissement de rapports graphiques et de gestion complets sur les

pare-feu SonicWALL, l'accès distant sécurisé et les appareils de sauvegarde et récupération, offrant ainsi un meilleur aperçu des tendances d'utilisation des applications et du réseau ainsi que des événements de sécurité. Les rapports peuvent être personnalisés et porter les logos et les couleurs des entreprises de manière à transmettre aux utilisateurs et clients un message cohérent de la marque.

La **gestion hors ligne** permet de réaliser les configurations et/ou les mises à jour firmware programmées des appliances gérées, sans être connecté, afin de réduire les interruptions de service pour les utilisateurs et les clients.

Le **gestionnaire de licences simplifié** présente une console unique pour la sauvegarde, l'application, la localisation et la mise à jour des informations de licences pour l'ensemble des appliances de sécurité SonicWALL gérées, ce qui simplifie la gestion des abonnements aux licences de sécurité et de support.

Le **support SNMP** fournit un mécanisme d'alerte en temps réel puissant pour l'ensemble des dispositifs et applications TCP/IP et SNMP, qui optimise l'identification des événements réseau critiques et la capacité à y répondre.

Des **options d'intégration évoluées** incluent une interface de programmation d'applications (API) pour les services Web, la prise en charge de CLI pour la majorité des fonctions, et la prise en charge de l'interruption SNMP. Les fournisseurs de services comme les entreprises peuvent utiliser ces options pour intégrer le GMS à leurs fonctions d'automatisation, de gestion et de contrôle des services professionnels, ainsi qu'aux autres applications de la société.

Spécifications



SonicWALL Global Management System

Une solution de gestion de la sécurité complète pour les entreprises et les fournisseurs de services.

SonicWALL GMS Standard Edition

Licence logiciel SonicWALL GMS pour 10 nœuds
01-SSC-3363

Licence logiciel SonicWALL GMS pour 25 nœuds
01-SSC-3311

Mise à niveau du logiciel SonicWALL GMS pour 1 nœud
01-SSC-7662

Mise à niveau du logiciel SonicWALL GMS pour 5 nœuds
01-SSC-3350

Mise à niveau du logiciel SonicWALL GMS pour 10 nœuds
01-SSC-7664

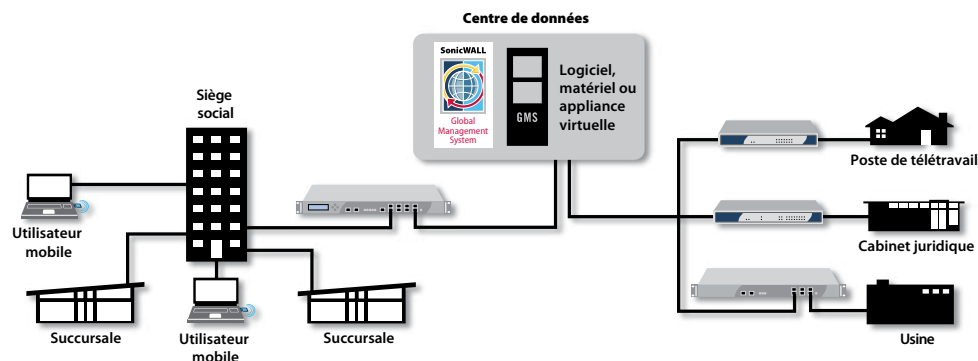
Mise à niveau du logiciel SonicWALL GMS pour 25 nœuds
01-SSC-3301

Mise à niveau du logiciel SonicWALL GMS pour 100 nœuds
01-SSC-3303

Mise à niveau du logiciel SonicWALL GMS pour 250 nœuds
01-SSC-3304

Mise à niveau du logiciel SonicWALL GMS pour 1 000 nœuds
01-SSC-3306

Visitez www.sonicwall.com/us/products/6030.html pour obtenir l'aperçu des références de support.



SonicWALL GMS permet aux administrateurs de créer facilement des règles de sécurité pour les appliances SonicWALL, et de les appliquer au niveau d'un, de plusieurs ou de tous les dispositifs.



SonicWALL GMS permet aux administrateurs de générer un large éventail de rapports informatifs et historiques offrant un aperçu des habitudes d'utilisation (type des sites Web consultés et personnes qui y ont accédé) et des atteintes à la sécurité des appliances SonicWALL gérées.



GMS Mobile est une application iPhone gratuite utilisée par les administrateurs GMS pour se connecter à distance à leur système GMS et leur permettant de voir tous les appareils gérés, de vérifier l'état des appareils et de traiter les alertes émises par le système GMS.

Configuration minimum requise :

Les configurations minimum requises pour SonicWALL GMS en ce qui concerne les systèmes d'exploitation, les bases de données, les pilotes, le matériel et les appliances SonicWALL prises en charge sont décrites ci-dessous :

Système d'exploitation

Windows Server 2003 32 bits et 64 bits (SP2), Windows Server 2008 SBS 64 bits (R2), Windows Server 2008 Standard 32 bits (SP2) et 64 bits (R2).

Dans tous les cas, SonicWALL GMS fonctionne comme une application 32 bits.

Appliance virtuelle

Hyperviseur : VMware ESX et ESXi
Système d'exploitation installé : SonicLinux renforcé
Taille de l'appliance : de 250 Go à 950 Go
Mémoire allouée : 3 Go
Guide de compatibilité matérielle VMware : <http://www.vmware.com/resources/compatibility/search.php>

Matériel pour un déploiement simple

Environnement x86 : serveur avec processeur Intel double cœur 3 GHz minimum, 4 Go de mémoire vive et 300 Go d'espace disque

Matériel pour un déploiement de serveurs distribués

Serveur GMS	Environnement x86 : processeur Intel simple 3 GHz minimum, 2 Go de mémoire vive et 300 Go d'espace disque
Serveur de base de données	Environnement x86 : processeur Intel double cœur 3 GHz minimum, 2 Go de mémoire vive et 300 Go d'espace disque

Passerelle GMS

Appliance de sécurité réseau SonicWALL des séries NSA E-Class, NSA ou PRO avec version minimum du firmware et appliances de sécurité réseau SonicWALL basées sur VPN¹

Bases de données prises en charge

Bases de données externes : Microsoft SQL 2000 (SP4), Microsoft SQL 2005 32 bits et 64 bits (SP2), Microsoft SQL 2008 64 bits (R2)

Associées à l'application GMS : MySQL

Java

Plug-in Java version 1.6 ou supérieure

Appliances SonicWALL prises en charge pour la gestion avec GMS

Appliances de sécurité réseau SonicWALL : NSA E-Class, NSA, série PRO, série TZ

Appliances de protection continue des données CDP SonicWALL, appliances Content Security Manager (CSM) SonicWALL, appliances d'accès distant sécurisé SonicWALL : SRA pour PME et SRA E-Class, appliances SonicWALL Email Security

Tous les appareils et applications compatibles TCP/IP et SNMP pour la surveillance active

Navigateurs Internet

Microsoft® Internet Explorer 6.0 ou version supérieure

Mozilla Firefox 2.0 ou version supérieure

Prise en charge uniquement sur les plates-formes Microsoft Windows

Firmware pris en charge

Appliances de sécurité réseau SonicWALL NSA E-Class et NSA : SonicOS Enhanced 5.0 ou version supérieure

SonicWALL série PRO : SonicOS Enhanced 3.2 ou version supérieure

SonicWALL série TZ : SonicOS Standard 3.1 ou version supérieure et SonicOS Enhanced 3.2 ou version supérieure

Appliances SonicWALL CDP : SonicWALL CDP 2.3 ou version supérieure

Appliances SonicWALL CSM : SonicWALL 2.0 ou version supérieure

Appliances SonicWALL SSL-VPN : firmware SRA SonicWALL pour PME 2.0 ou version supérieure et firmware SRA E-Class SonicWALL Avenail 9.0 ou version supérieure

Appliances SonicWALL Email Security : firmware SonicWALL Email Security 7.0 ou version supérieure

¹ Une passerelle GMS est nécessaire pour l'utilisation de l'option de tunnel VPN de gestion qui garantit une communication sécurisée entre le serveur GMS SonicWALL et les appliances gérées utilisant les tunnels VPN. La passerelle GMS doit au moins être une solution NSA de SonicWALL dotée au minimum du firmware SonicOS Enhanced 5.0, ou une appliance SonicWALL PRO 2040 dotée au minimum du firmware SonicOS Enhanced 3.2. La passerelle GMS n'est pas nécessaire pour l'utilisation des tunnels VPN existants ou de HTTPS comme méthode de gestion.



La gamme complète de solutions de sécurité dynamique SonicWALL



SÉCURITÉ RÉSEAU



ACCÈS DISTANT SÉCURISÉ



SÉCURISATION WEB ET DE MESSAGERIE



SAUVEGARDE ET RÉCUPÉRATION



GESTION ET RÈGLES

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 DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

