SONICWALL GLOBAL MANAGEMENT SYSTEM

Solution complète de gestion de la sécurité, de surveillance, de création de rapports et d'analyse

Une stratégie de gestion de la sécurité réussie exige une très bonne compréhension de l'environnement de sécurité afin de pouvoir favoriser et améliorer la collaboration et la prise de décision en matière de règles. Si les entreprises ne disposent pas d'une vue globale sur l'ensemble du système de sécurité, elles risquent de subir des cyberattaques et des violations des règles de conformité pourtant faciles à éviter. Lorsque de nombreux outils sont exécutés sur différentes plateformes et que des données de rapports sont utilisées dans différents formats, les analyses et les rapports de sécurité deviennent inefficaces sur le plan opérationnel. Ceci affecte encore les capacités de l'entreprise à pouvoir rapidement identifier les risques liés à la sécurité et y réagir. Afin de relever ces défis, les entreprises doivent définir une approche systématique en termes de gouvernance de l'environnement de sécurité du réseau.

SonicWall Global Management System (GMS) permet d'apporter une réponse à ces défis. La solution GMS intègre gestion et surveillance, analyses, rapports d'audit et analyse forensique. Cela constitue la base d'une stratégie de gouvernance de la sécurité, de mise en conformité et de gestion des risques. La richesse fonctionnelle de la plateforme GMS permet aux entreprises distribuées, aux fournisseurs de services et autres entreprises de bénéficier d'une approche fluide et globale pour unifier tous les aspects opérationnels de leur environnement de sécurité. Avec la solution GMS, les équipes de sécurité peuvent aisément gérer les solutions SonicWall de pare-feu, point d'accès sans fil, sécurisation de messagerie et accès mobile sécurisé, ainsi que des solutions tierces de commutateurs réseau. Tout ceci est possible via un workstream contrôlé et vérifiable capable d'assurer un fonctionnement solide, sécurisé et conforme des réseaux. La solution GMS inclut gestion et application centralisée des règles, surveillance d'événements en temps réel, analyse granulaire de données et création de rapports, pistes d'audit, etc., dans une plateforme de gestion unifiée.

Avantages :

- Établit un programme de sécurité unifié en matière de gouvernance, de mise en conformité et de gestion des risques
- Adopte une approche cohérente et vérifiable pour l'orchestration des questions de sécurité, analyse forensique, rapports et analyses
- Réduit le risque et fournit une réponse rapide aux événements de sécurité
- Fournit une vue de l'écosystème de sécurité à l'échelle de l'entreprise
- Automatise les workflows et assure la conformité des opérations de sécurité
- Opérationnalise les pare-feux sur les sites distants et dans les agences en quatre étapes simples grâce au déploiement sans intervention
- Configure, surveille et gère de manière centralisée le déploiement, la connectivité et la performance SDWAN
- Fournit des rapports sur les règlementations HIPAA, SOX et PCI pour les auditeurs internes et externes
- Permet un déploiement facile et rapide avec options logiciel, appliance virtuelle ou Cloud, à faible coût

GOUVERNANCE CENTRALE

- Faciliter la mise en place d'une solution complète de gestion de la sécurité, d'analyse, de création de rapports et de mise en conformité afin d'unifier votre programme de protection de la sécurité réseau
- Automatiser et mettre en corrélation les workflows pour coordonner parfaitement la stratégie de gouvernance de la sécurité, de mise en conformité et de gestion des risques

CONFORMITÉ

- Satisfaire aux exigences des instances de règlementation et des auditeurs via des rapports automatiques de sécurité PCI, HIPAA et SOX
- Personnaliser toute combinaison de données de sécurité vérifiables pour faciliter la mise en conformité avec des exigences spécifiques

GESTION DES RISQUES

- Évoluer rapidement et favoriser la collaboration, la communication et les connaissances sur toute la structure de sécurité partagée
- Prendre des décisions avisées en matière de règles de sécurité, sur la base d'informations sur les menaces consolidées et prioritaires, pour un niveau supérieur de sécurité et d'efficacité

La plateforme GMS fournit une approche globale en matière de gouvernance de la sécurité, de mise en conformité et de gestion des risques.

Automatisation du workflow

Grâce à l'automatisation native du workflow, GMS facilite la conformité des opérations de sécurité aux exigences de gestion et d'audit des modifications des règles de pare-feu de diverses lois de nature réglementaire, telles que PCI, HIPPA et le RGPD. La modification des règles est rendue possible par une série de procédures rigoureuses de configuration, comparaison, validation, vérification et approbation des règles de pare-feu avant tout déploiement. Les groupes d'approbation sont flexibles, ce qui permet de se conformer aux diverses procédures d'autorisation et d'audit des différents types d'entreprises. L'automatisation du workflow programme le déploiement des règles de sécurité sanctionnées afin d'améliorer l'efficacité opérationnelle, de réduire les risques et d'éliminer les erreurs.

La plateforme GMS fournit une approche globale en matière de gouvernance de la sécurité, de mise en conformité et de gestion des risques.

1. CONFIGURATION ET COMPARAISON

GMS configure les **ordres de modification** des règles et les différences de **code couleur** pour des comparaisons claires.

2. VALIDATION

GMS effectue une **validation d'intégrité de la logique des règles.**

3. RÉVISION ET APPROBATION

GMS envoie un e-mail aux réviseurs et consigne une **piste d'audit d'approbation (ou de désapprobation)** de la règle.

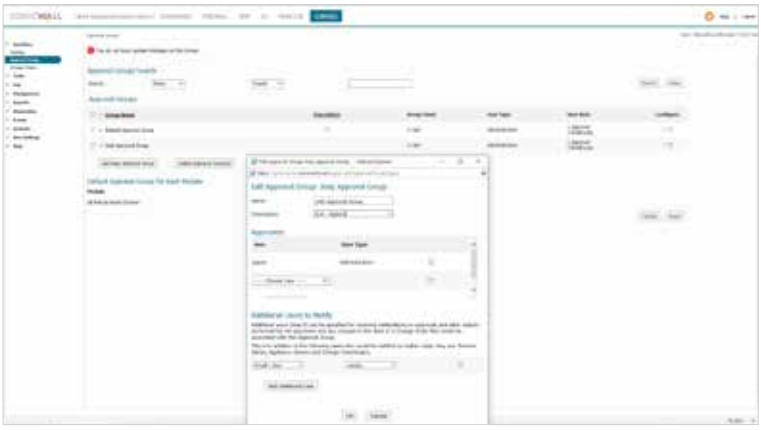
4. DÉPLOIEMENT

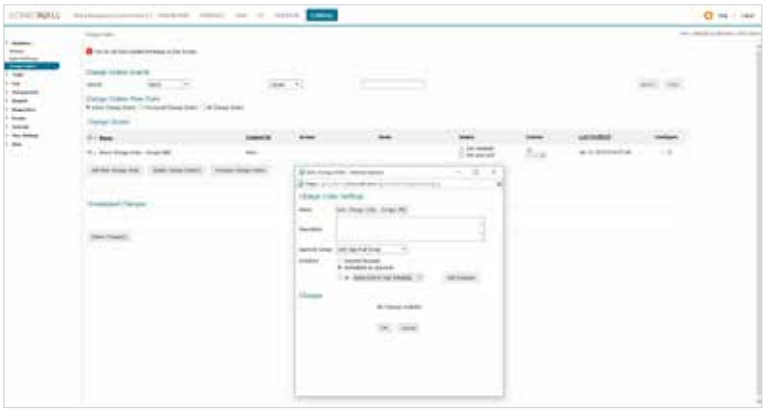
GMS déploie les modifications des règles instantanément ou **selon un calendrier.**

5. AUDIT

Les journaux de modifications permettent d'obtenir des **audits** exacts des règles et des données précises de **conformité.**

Automatisation du workflow GMS : cinq étapes pour une gestion des règles sans erreur





Partner Enabled Services

Vous avez besoin d'aide pour planifier, déployer et optimiser votre solution SonicWall ? Les partenaires SonicWall Advanced Services sont spécialement formés pour vous offrir des services professionnels de premier ordre. Pour en savoir plus, rendez-vous sur www.sonicwall.com/PES.

Déploiement sans intervention

Intégré au système GMS, le service Zero-Touch Deployment simplifie et accélère le processus de configuration des pare-feux SonicWall sur les sites distants et dans les agences. Ce processus, qui nécessite une intervention minimale de l'utilisateur, est entièrement automatisé pour opérationnaliser les pare-feux à l'échelle requise, en quatre étapes simples de déploiement. Cela permet de considérablement réduire le temps, le coût et la complexité associés à l'installation et à la configuration, tandis que sécurité et connectivité sont assurées de manière instantanée et automatique.

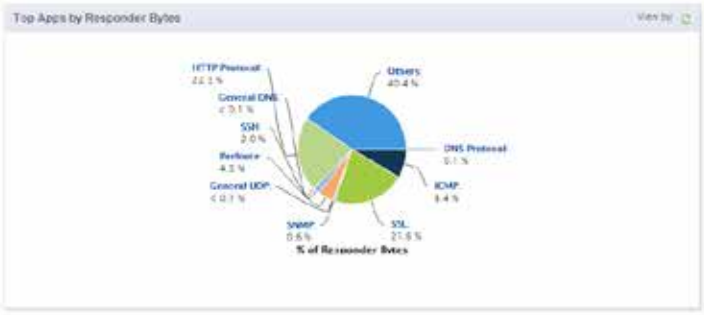
ÉTAPE 1	**ENREGISTRER LE PARE-FEU** Enregistrez le nouveau pare-feu dans MySonicWall à l'aide de son numéro de série et de son code d'authentification.
ÉTAPE 2	**CONNECTER LE PARE-FEU** Connectez le pare-feu au réseau via le câble Ethernet fourni.
ÉTAPE 3	**BRANCHER LE PARE-FEU** Mettez le pare-feu sous tension après y avoir connecté le câble d'alimentation, lui-même branché sur une prise murale standard. Une IP WAN est automatiquement attribuée aux appareils via un serveur DHCP. Une fois la connectivité établie, l'appareil est automatiquement détecté, authentifié et ajouté au Capture Security Center. Toutes les licences et les configurations sont synchronisées avec MySonicWall et le gestionnaire de licences.
ÉTAPE 4	**GÉRER LE PARE-FEU** L'appareil est alors opérationnel. Il est géré via la console centrale Cloud Capture Security Center pour les mises à jour de firmware, les correctifs de sécurité et les modifications de la configuration au niveau groupe.

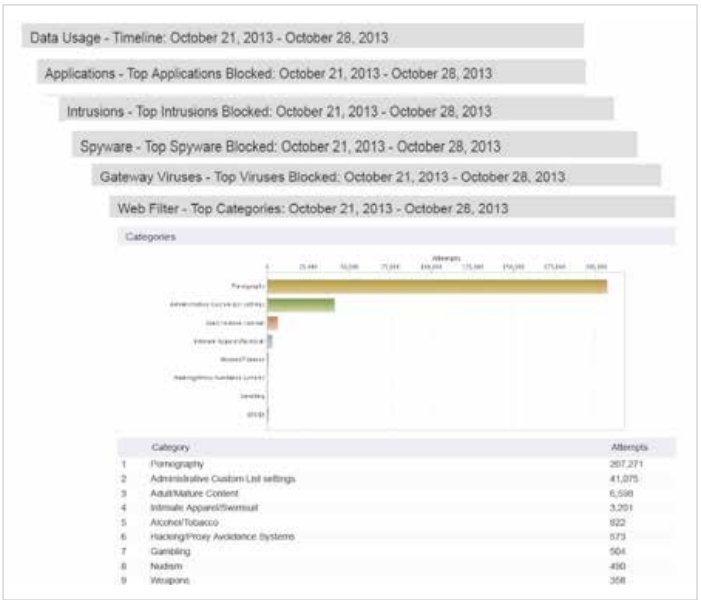
Déploiement sans intervention : Un pare-feu opérationnel en quatre étapes simples

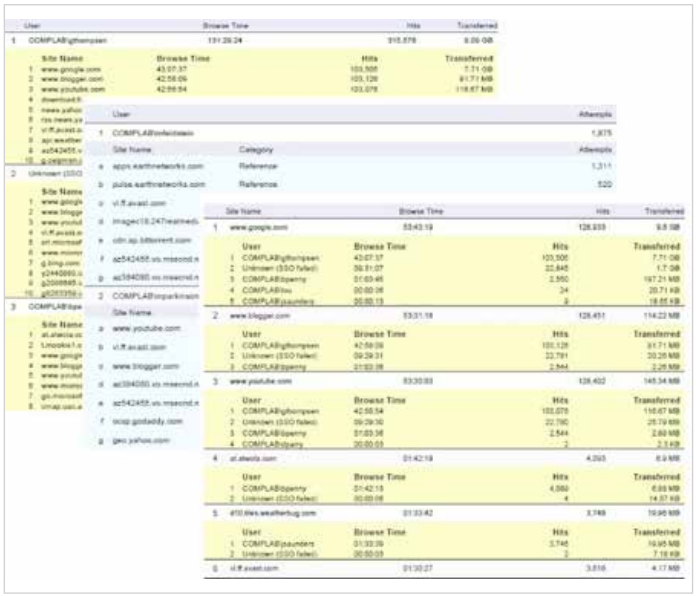
Création de rapports

Capture Security Center propose plus de 140 rapports prédéfinis et offre la possibilité de créer des rapports personnalisés en combinant des données vérifiables dans le but d'obtenir plusieurs résultats de cas d'utilisation. Ceux-ci intègrent une vision générale et détaillée des événements du réseau, des activités des utilisateurs, des menaces, des problèmes de fonctionnement et de performances, de l'efficacité de la sécurité, des risques et des failles de sécurité, de la préparation à la conformité, et même de l'analyse post-mortem. Chaque rapport est élaboré grâce à la contribution collective des clients et partenaires SonicWall. Cette longue collaboration permet d'obtenir une granularité, une portée et une connaissance approfondies des données syslog et IPFIX/NetFlow nécessaires pour suivre, mesurer et exécuter efficacement des opérations de réseau et de sécurité.

Des rapports graphiques intuitifs simplifient la surveillance des appliances gérées. Les administrateurs sont en mesure d'identifier facilement les anomalies de trafic à partir des données d'utilisation pour un horaire, initiateur, répondant ou service spécifiques. Ils peuvent aussi exporter des rapports vers une feuille de calcul Microsoft® Excel®, un fichier au format PDF ou directement vers une imprimante pour diagnostic.







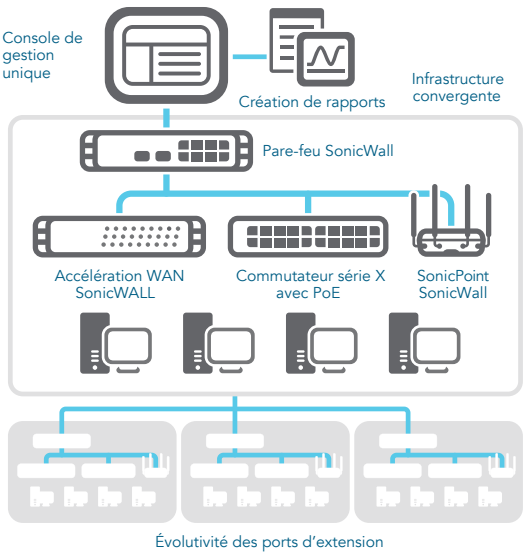
SONICWALL®

Fonctionnalités de gestion de la sécurité et de surveillance	
Fonctionnalité	Description
Gestion centralisée de la sécurité et du réseau	Aide les administrateurs à déployer, gérer et surveiller un environnement de sécurité réseau distribué.
Configuration des règles fédérée	Permet de définir aisément des règles pour des milliers de pare-feux, points d'accès sans fil, commutateurs et équipements de sécurisation de messagerie et d'accès distant sécurisé, depuis un seul et même emplacement.
Gestion des ordres de modification et workflow	Assure exactitude et conformité des modifications des règles en appliquant un processus de configuration, comparaison, validation, révision et approbation des règles avant le déploiement. Les groupes d'approbation peuvent être personnalisés afin de respecter les règles de sécurité de l'entreprise. Toutes les modifications des règles sont consignées sous un format vérifiable qui garantit la conformité du pare-feu avec les contraintes règlementaires. Tous les détails des modifications effectuées sont conservés dans un historique afin de faciliter la mise en conformité, les pistes d'audit et le dépannage.
Déploiement sans intervention	Simplifie et accélère le déploiement et la configuration des pare-feux SonicWall avec utilisation du Cloud à distance. Déploie automatiquement les règles, effectue les mises à jour de firmware et synchronise les licences.
Configuration SD-WAN	Configure, surveille et gère le déploiement et la connectivité SD-WAN, en toute simplicité, dans un environnement d'entreprise distribué.
Configuration et déploiement VPN efficaces	Simplifie l'activation de la connectivité VPN et consolide des milliers de règles de sécurité.
Gestion hors ligne	Permet de planifier les configurations et les mises à jour sur les appliances gérées afin de réduire à un minimum les interruptions de service.
Gestion rationalisée des licences	Simplifie la gestion des appliances via une console unifiée, ainsi que la gestion de la sécurité et des souscriptions de licence de support.
Tableau de bord universel	Réunit des widgets personnalisables, des cartes géographiques et des options de reporting relatives aux utilisateurs.
Système de surveillance active et d'alerte	Émet des alertes en temps réel avec options de surveillance intégrées, simplifie le dépannage en permettant aux administrateurs de prendre des mesures préventives et de remédier immédiatement aux problèmes.
Prise en charge SNMP	Fournit de puissants traps (interruptions) en temps réel pour l'ensemble des applications et dispositifs TCP/IP et SNMP, ce qui simplifie le dépannage et permet d'identifier les événements réseau critiques et d'y répondre.
Visualisation et contrôle des applications	Affiche des rapports historiques et temps réel indiquant quelles applications sont en cours d'utilisation et qui sont les utilisateurs. Les rapports sont entièrement personnalisables à l'aide de fonctionnalités intuitives de filtrage et de zoom.
Nombreuses options d'intégration	Fournit une interface de programmation applicative pour les services Web, la prise en charge CLI (interface en ligne de commande) pour la majorité des fonctions et la prise en charge de traps SNMP tant pour les fournisseurs de services que pour les entreprises.
Gestion des commutateurs réseau Dell série X	Les commutateurs réseau Dell série X peuvent désormais être facilement gérés au sein des pare-feux TZ, NSA et SuperMassive pour offrir une gestion centralisée sur l'ensemble de l'infrastructure de sécurité du réseau.
Prise en charge de réseaux fermés	Déploie le système GMS dans des environnements fermés, comme les réseaux hautement protégés des instances gouvernementales. Toutes les clés de licence et les fichiers de signatures des services backend de SonicWall sont groupés, chiffrés et transférés de manière sécurisée vers le système de fichiers local, auquel le système GMS peut accéder et dans lequel il peut charger puis déployer les mises à jour requises pour toutes les appliances de sécurité gérées.
Rapports et analyses de sécurité	
Fonctionnalité	Description
Rapport sur les botnets	Il existe quatre types de rapports : Tentatives, Cibles, Initiateurs et Chronologie, contenant le contexte du vecteur de l'attaque, par ex. identifiant du botnet, adresses IP, pays, hôtes, ports, interfaces, initiateur/cible, source/destination et utilisateur.
Rapport Geo IP	Contient des informations sur le trafic bloqué en fonction de son pays d'origine ou de sa destination. Il existe quatre types de rapports : Tentatives, Cibles, Initiateurs et Chronologie, contenant le contexte du vecteur de l'attaque, par ex. identifiant du botnet, adresses IP, pays, hôtes, ports, interfaces, initiateur/cible, source/destination et utilisateur.

Rapports et analyses de sécurité (suite)	
Fonctionnalité	Description
Rapport adresse Mac	Indique l'adresse MAC (Media Access Control) sur la page du rapport. Inclut des informations spécifiques à l'équipement (Initiateur MAC et Répondant MAC) dans cinq types de rapports : • Utilisation des données > Initiateurs • Utilisation des données > Répondants • Utilisation des données > Détails • Activité des utilisateurs > Détails • Activité Web > Initiateurs
Rapport Capture ATP	Affiche des informations détaillées sur le comportement de menaces, en réponse à une menace ou une infection.
Rapports HIPPA, PCI et SOX	Inclut des modèles prédéfinis de rapports PCI, HIPAA et SOX conformes aux exigences de sécurité des audits.
Rapports sur les points d'accès sans fil sauvages	Affiche tous les appareils sans fil en cours d'utilisation ainsi que le comportement sauvage lié à une mise en réseau ad-hoc ou poste à poste entre les hôtes et les associations accidentelles pour les utilisateurs qui se connectent aux réseaux sauvages voisins.
Analyse et reporting sur les flux	Fournit un agent de création de rapports sur les flux pour l'analyse du trafic applicatif et sur les données d'utilisation via les protocoles IPFIX ou NetFlow, pour une surveillance en temps réel et historique. Offre aux administrateurs une interface efficace pour surveiller visuellement leur réseau en temps réel. Ils peuvent ainsi identifier les applications et sites Web très consommateurs en bande passante, voir l'utilisation que fait chaque utilisateur des applications et anticiper les attaques et menaces rencontrées sur le réseau. • Un visualiseur en temps réel avec personnalisation par glisser-déposer • Un écran de rapport en temps réel avec filtrage en un clic • Un tableau de bord des principaux flux avec boutons d'affichage en un clic • Un écran de rapport sur les flux avec cinq onglets d'attributs de flux supplémentaires • Un écran d'analyse des flux avec puissantes fonctionnalités de corrélation et de rotation • Un visualiseur de sessions pour les zooms avant détaillés de sessions et de paquets
Rapports intelligents et visualisation des activités	Fournit des rapports graphiques et de gestion complets sur les pare-feux SonicWall, les équipements de sécurisation de messagerie et d'accès mobile sécurisé. Permet de mieux connaître les tendances d'utilisation et les événements de sécurité tout en fournissant une identité de marque cohérente pour les fournisseurs de services.
Journalisation centralisée	Offre un emplacement central pour consolider les événements de sécurité et les journaux de milliers d'appliances, ce qui permet de réaliser des analyses forensiques du réseau à partir d'un point unique.
Rapports syslog de nouvelle génération en temps réel et historique	Simplifie, grâce à des améliorations révolutionnaires, le processus fastidieux de synthèse des données, permettant la génération en temps quasi réel de rapports sur les messages syslog entrants. Offre en outre la possibilité de zoomer sur les données ainsi que de nombreuses options de personnalisation des rapports.
Rapports universels planifiés	Planifie des rapports qui sont automatiquement créés et envoyés vers les destinataires autorisés pour plusieurs appliances de divers types.
Analyse du trafic applicatif	Fournit des informations précieuses sur le trafic applicatif, la consommation de bande passante et les atteintes à la sécurité, tout en fournissant des services performants de dépannage et d'analyse forensique.
Sécurité de l'authentification	
Fonctionnalité	Description
Verrouillage des comptes	La politique de verrouillage des comptes désactive le compte d'un utilisateur GMS en cas de saisie de mots de passe incorrects, après un nombre donné de tentatives autorisées, sur une période définie. Cela permet d'empêcher les pirates de deviner les mots de passe des utilisateurs et de réduire les attaques qui réussissent à accéder aux ressources et aux données protégées sur le réseau.
Complexité des mots de passe	La politique de complexité des mots de passe définit les règles minimales qu'il est important d'appliquer pour qu'un mot de passe soit suffisamment fiable lors de l'identification et de l'accès au système GMS.
Accès de l'administrateur à une plage d'adresses spécifique	Les clients peuvent contrôler l'accès de l'administrateur à des plages d'adresses spécifiques.

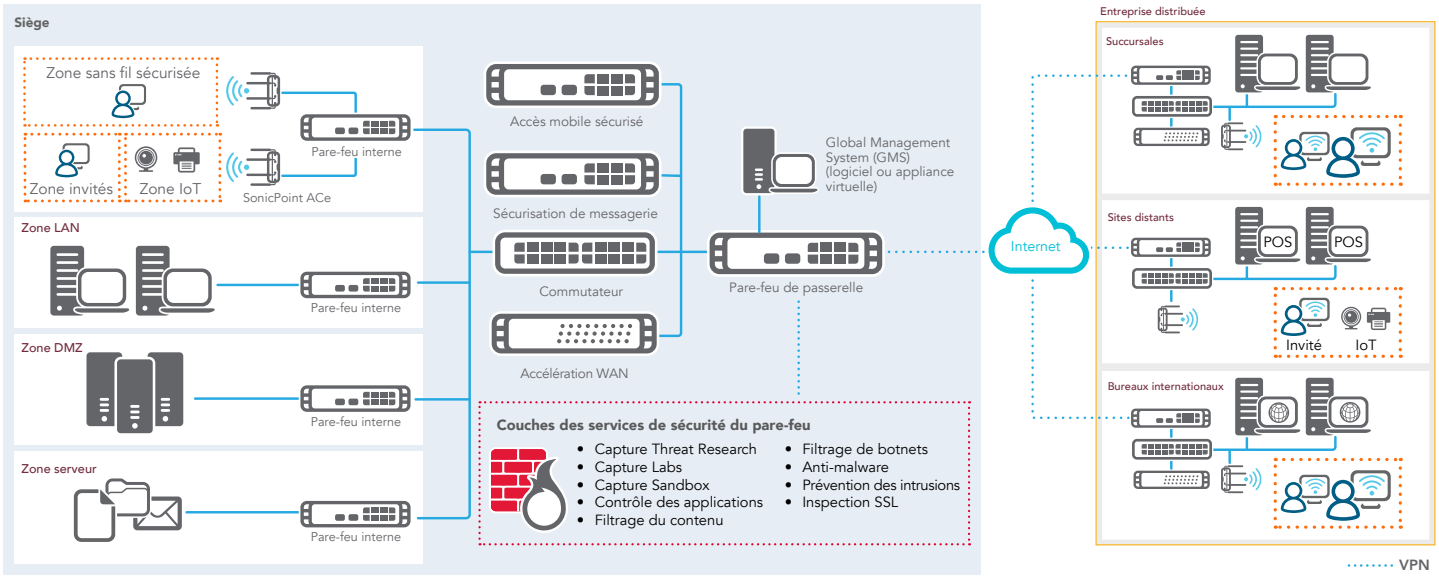
Architecture évolutive en mode distribué

GMS est une solution sur site qu'il est possible de déployer en tant que logiciel ou appliance virtuelle. Au cœur de la solution GMS se trouve une architecture distribuée qui favorise la disponibilité et l'évolutivité d'un système sans limites. Une seule instance GMS peut ajouter visibilité et contrôle pour des milliers d'appareils de sécurité réseau placés sous sa gestion, quel qu'en soit l'emplacement. Côté client, ses tableaux de bord universels hautement interactifs, chargés de données de surveillance, de création de rapport et d'analyse en temps réel, permettent de prendre des décisions éclairées et favorisent la collaboration, la communication et les connaissances sur toute la structure de sécurité partagée. Cette vue de l'environnement de sécurité à l'échelle de l'entreprise et une surveillance de la sécurité en temps réel qui atteint les bonnes personnes permettent d'établir des règles de sécurité précises et de prendre des mesures de contrôle avisées, pour une sécurité adaptative renforcée.



SonicWall Global Management System (GMS)

La solution GMS sur site est une plateforme complète et évolutive de gestion de la sécurité, d'analyse et de création de rapports pour les entreprises distribuées et les centres de données.



SonicWall Global Management System – environnements sur site

Récapitulatif des fonctionnalités

Création de rapports

- Éventail complet de rapports graphiques
- Rapports de conformité
- Rapports personnalisables avec fonctionnalités de zoom
- Journalisation centralisée
- Rapports multi-menaces
- Rapports axés sur les utilisateurs
- Rapports d'utilisation des applications
- Rapports granulaires de services
- Fonctions intelligentes d'analyse des attaques
- Bande passante et rapport de services par interface
- Rapports pour pare-feu SonicWall
- Rapports pour appliances SRA SSL VPN SonicWall
- Rapports universels planifiés
- Rapports syslog et IPFIX de nouvelle génération
- Rapports flexibles et granulaires en temps quasi réel
- Rapports sur la bande passante par utilisateur
- Rapports sur l'activité Client VPN
- Récapitulatif détaillé des services via rapport VPN
- Rapports sur les points d'accès sans fil sauvages
- Rapports WAF (Web Application Firewall) SRA SMB

Gestion

- Accès universel
- Alertes et notifications
- Outils de diagnostic
- Sessions utilisateur multiples et simultanées
- Gestion et planification hors ligne
- Gestion des règles de sécurité des pare-feux
- Gestion des règles de sécurité VPN
- Gestion des règles de sécurité de messagerie
- Gestion des règles d'accès distant sécurisé/SSL VPN
- Gestion des services de sécurité à valeur ajoutée
- Définition des modèles de règles au niveau groupe
- Réplication des règles appareil vers groupe d'appareils
- Réplication des règles niveau groupe vers appareil unique
- Redondance et haute disponibilité
- Gestion du provisioning
- Architecture évolutive et distribuée
- Vues dynamiques de gestion
- Gestionnaire de licences unifié
- Interface de ligne de commande
- Interface de programmation applicative (API) de services Web
- Gestion basée sur les rôles (utilisateurs, groupes)
- Tableau de bord universel
- Sauvegarde des fichiers de préférences pour les pare-feux
- SD-WAN
- Déploiement sans intervention
- Prise en charge de réseaux fermés
- Prise en charge de pare-feux sandwich

Surveillance

Flux de données IPFIX en temps réel

Prise en charge SNMP

Système de surveillance active et d'alerte

Gestion des relais SNMP

Surveillance de l'état des VPN et pare-feux

Surveillance Syslog dynamique et alertes

Sécurité de l'authentification

Verrouillage des comptes

Complexité des mots de passe

Accès de l'administrateur à une plage d'adresses spécifique

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 2016
- Windows Server 2012 Standard 64 bits
- Windows Server 2012 R2 Standard 64 bits (anglais et japonais)
- Windows Server 2012 R2 Datacenter

Configuration matérielle requise

- Utilisez GMS Capacity Calculator pour déterminer la configuration matérielle requise pour votre déploiement.

Configuration requise pour les appliances virtuelles

- Hyperviseur : ESXi 6.5, 6.0 ou 5.5
- Utilisez GMS Capacity Calculator pour déterminer la configuration matérielle requise pour votre déploiement.

Guide de compatibilité matérielle VMware :

www.vmware.com/resources/compatibility/search.php

Bases de données prises en charge

- Bases de données externes : Microsoft SQL Server 2012 et 2014
- Inclus dans l'application GMS : MySQL

Navigateurs Internet

- Microsoft® Internet Explorer 11.0 ou version supérieure (ne pas utiliser le mode de compatibilité)
- Mozilla Firefox 37.0 ou version supérieure
- Google Chrome 42.0 ou version supérieure
- Safari (version la plus récente)

Appliances SonicWall prises en charge avec GMS

- Appliances de sécurité réseau SonicWall : SuperMassive E10000 et 9000 Series, E-Class NSA, NSa Series et TZ Series
- Appliances virtuelles de sécurité réseau SonicWall : NSv 10 Series
- SonicWall Secure Mobile Access (SMA) : SMA Series et E-Class SRA
- Appliances SonicWall Email Security
- Tous les appareils et applications compatibles TCP/IP et SNMP pour la surveillance active

Informations de commande Global Management System (GMS)	
Produit	Référence
LICENCE LOGICIEL 5 NŒUDS SONICWALL GMS	01-SSC-3311
LICENCE LOGICIEL 10 NŒUDS SONICWALL GMS	01-SSC-7662
LICENCE LOGICIEL 25 NŒUDS SONICWALL GMS	01-SSC-3350
MISE À NIVEAU LOGICIEL 1 NŒUD SONICWALL GMS	01-SSC-7664
MISE À NIVEAU LOGICIEL 5 NŒUD SONICWALL GMS	01-SSC-3301
MISE À NIVEAU LOGICIEL 10 NŒUDS SONICWALL GMS	01-SSC-3303
MISE À NIVEAU LOGICIEL 25 NŒUDS SONICWALL GMS	01-SSC-3304
MISE À NIVEAU LOGICIEL 100 NŒUDS SONICWALL GMS	01-SSC-3306
MISE À NIVEAU LOGICIEL 250 NŒUDS SONICWALL GMS	01-SSC-0424
MISE À NIVEAU LOGICIEL 1000 NŒUDS SONICWALL GMS	01-SSC-7675
SONICWALL GMS CHANGE MANAGEMENT AND WORKFLOW	01-SSC-6524
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 1 NOEUD (1 AN)	01-SSC-6514
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 5 NOEUDS (1 AN)	01-SSC-3334
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 10 NOEUDS (1 AN)	01-SSC-3336
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 25 NOEUDS (1 AN)	01-SSC-3337
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 100 NOEUDS (1 AN)	01-SSC-3338
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 250 NOEUDS (1 AN)	01-SSC-6524
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 1000 NOEUDS (1 AN)	01-SSC-6514
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 25 NOEUDS (1 AN)	01-SSC-3334
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 100 NOEUDS (1 AN)	01-SSC-3336
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 250 NOEUDS (1 AN)	01-SSC-3337
SUPPORT LOGICIEL SONICWALL GMS E-CLASS (24h/24, 7j/7) POUR 1000 NOEUDS (1 AN)	01-SSC-3338

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 plus d'informations, consultez notre site à l'adresse : **www.sonicwall.com** ou suivez-nous sur Twitter, LinkedIn, Facebook et Instagram.

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

DataSheet-SonicWallGlobalManagementSystem-US-VG-MKTG4042