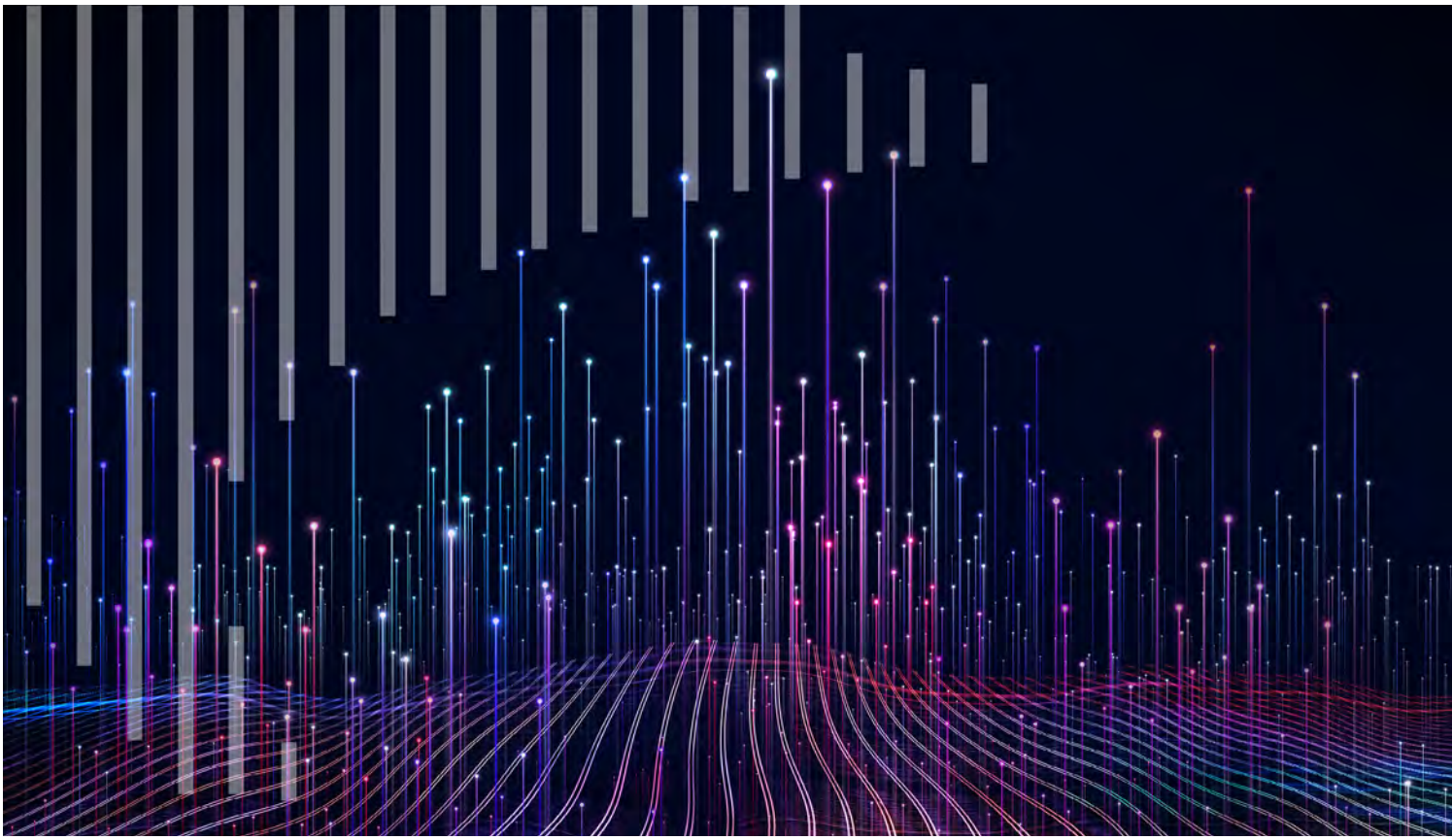
# Les gammes de produits SonicWall

Juin 2022



## Présentation

Sécurisez le cloud public/privé, les applications, les utilisateurs et les données de votre entreprise grâce à une protection en profondeur des réseaux sans en compromettre les performances. La plateforme SonicWall Capture Cloud intègre étroitement des services de sécurité, de gestion, d'analyse et de renseignements sur les menaces en temps réel dans notre gamme de produits sans fil, mobiles, Web et cloud de sécurité réseau et de sécurisation de messagerie. Cette approche permet aux entreprises petites, moyennes ou grandes, aux organismes publics, points de vente au détail, établissements d'enseignement, de santé et fournisseurs de services de bénéficier de tout notre écosystème de sécurité et de maîtriser la puissance, l'agilité et l'évolutivité du cloud.

La stratégie et la vision de la plateforme Capture Cloud reposent sur l'innovation et le développement continus des applications de sécurité conteneurisées as-a-service, qui sont facilement programmables et disponibles à la demande. Elles se composent des éléments et fonctionnalités clés suivants :

- Sécurité réseau
- Sécurité câblée
- Sécurité sans fil
- Sécurité des terminaux
- Accélération WAN
- Services de sécurité avancés
- Cloud App Security
- Cloud Edge Secure Access
- Accès mobile sécurisé
- Sécurisation de messagerie
- Gestion, rapports et analyse
- Services et support professionnels

La combinaison de ces éléments permet de fournir une cyberprotection stratégique à plusieurs niveaux, des renseignements sur les menaces, des possibilités d'analyse et de collaboration, ainsi que des tâches courantes et synchronisées de gestion, de reporting et d'analyse.

## Sécurité réseau

SonicWall fait partie des plus grands fournisseurs de pare-feux de nouvelle génération. Le firmware, SonicOS ou SonicOSX, est au cœur de tous les pare-feux SonicWall. SonicOS s'appuie sur notre architecture matérielle évolutive ainsi que sur nos moteurs RTDMI™ (Real-Time Deep Memory Inspection) en instance de brevet et RFDPI (Reassembly-Free Deep Packet Inspection®) breveté*, « single-pass » et à faible latence, qui analysent l'ensemble du trafic, quels que soient le port ou le protocole.

Nos pare-feux de nouvelle génération analysent chaque octet de chaque paquet, sans pour autant altérer les performances élevées et la faible latence dont ont besoin les réseaux d'aujourd'hui. Contrairement aux produits concurrents, le moteur RFDPI « single-pass » assure un filtrage simultané des diverses menaces et des applications ainsi que l'analyse de fichiers de toute taille, sans réassemblage des paquets. Cela permet aux pare-feux SonicWall d'être extrêmement évolutifs et aux réseaux d'entreprises et centres de données de bénéficier d'une sécurité de pointe tout au long de leur croissance.

Les pare-feux SonicWall abritent de puissantes fonctionnalités, notamment :

- Sandboxing cloud multimoteur Capture ATP
- SD-WAN
- API REST
- Déchiffrement et inspection du trafic chiffré
- Service de prévention des intrusions (IPS)
- Protection anti-malware
- Surveillance, contrôle et visualisation en temps réel des applications
- Filtrage de sites Web/URL (filtrage de contenu)
- Réseau privé virtuel (VPN) par SSL ou IPSec
- Sécurité sans fil
- Sécurité hybride et multi-cloud
- Basculement/reprise dynamiques

Par ailleurs, les pare-feux SonicWall assurent une protection en continu et très réactive contre les menaces zero-day grâce à l'équipe de recherche sur les menaces Capture Labs. Cette équipe collecte, analyse et vérifie des informations sur les menaces multi-vecteur à partir de nombreuses sources, notamment plus d'un million de capteurs placés dans le monde entier, au sein de son réseau Capture Threat Network.

### SonicWall Network Security services platform (NS*sp*) Series

La plateforme de pare-feux de nouvelle génération SonicWall NS*sp* Series est conçue pour fournir aux vastes réseaux une évolutivité, une fiabilité et une sécurité maximum à des débits multi-gigabits.

ICSA Labs a testé les pare-feux SonicWall et constaté l'excellente efficacité de leur sécurité, avec un taux de détection de 100 % sans aucune fausse alerte sur les cinq derniers trimestres consécutifs. Les pare-feux SonicWall sont devenus une référence en matière de contrôle des applications et de prévention des menaces hautes performances, quel que soit le type de déploiement, de la plus petite entreprise au centre de données, en passant par les opérateurs et les fournisseurs de services.

Notre pare-feu multi-instances haut de gamme NS*sp*, par exemple, garantit une qualité de service élevée grâce à la disponibilité et à la connectivité continues du réseau aujourd'hui exigées par les entreprises, administrations publiques, universités et fournisseurs de services, pour des infrastructures de 100/40/10 Gbits/s. Grâce aux technologies d'apprentissage profond utilisées dans la plateforme SonicWall Capture Cloud, la série NS*sp* offre une protection éprouvée contre la majorité des menaces évoluées, sans ralentissement des performances.

### Unified Policy avec SonicOSX 7

La fonctionnalité de gestion unifiée des règles dans SonicOSX 7 assure une gestion intégrée des règles d'accès et de sécurité sur certains pare-feux haut de gamme NS*sp* et virtuels NS*v* SonicWall.

Elle présente une nouvelle interface Web conçue selon une approche radicalement différente. L'accent a été mis sur un design orienté utilisateur, qui se traduit par une configuration plus intuitive de règles de sécurité contextuelles via des alertes actionnables, ainsi que par la simplicité du pointer-cliquer.

Visuellement, elle est également plus attrayante que l'interface classique. Dans l'écran unique d'un pare-feu, l'interface présente des informations sur l'efficacité de diverses règles de sécurité. Elle permet à l'utilisateur de modifier les règles prédéfinies pour l'antivirus au niveau de la passerelle, l'anti-logiciels espions, le filtrage de contenu, la prévention des intrusions, le filtrage Geo-IP et l'inspection approfondie des paquets du trafic chiffré, le tout de manière transparente.

À travers cette nouvelle interface de règles unifiée, SonicWall offre une expérience optimisée permettant de contrôler les modifications du trafic dynamique en moins de temps et assurant une meilleure posture de sécurité globale.

* Brevets (États-Unis) 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723



SONICWALL®

### SonicWall Network Security appliance (NS*a*) Series

Les pare-feux de nouvelle génération SonicWall Network Security appliance (NS*a*) comptent parmi les plus sécurisés et les plus performants de leur classe. Gage d'une sécurité haut de gamme sans compromettre les performances, cette série repose sur la même architecture que les pare-feux de nouvelle génération de la série phare NS*sp*, conçue à l'origine pour les réseaux d'opérateurs et de grands comptes les plus exigeants.

Fruit de plusieurs années de recherche et de développement, la série NS*a* a été conçue dès le départ pour les entreprises distribuées et moyennes structures, les agences, les établissements scolaires et les organismes publics. La série NS*a* allie une architecture multiprocesseur révolutionnaire à la technologie RTDMI (Real-Time Deep Memory Inspection) basée sur le cloud, un moteur breveté de prévention des menaces, dans une conception extrêmement évolutive. Cette association garantit une protection, des performances et une évolutivité haut de gamme, avec un nombre élevé de connexions simultanées, une faible latence, pas de limite dans la taille des fichiers et un nombre de connexions par seconde supérieur à celui d'autres fournisseurs de pare-feux leaders.

### Pare-feux SonicWall TZ Series

La série TZ de SonicWall se compose de pare-feux UTM (Unified Threat Management) haute fiabilité et haute sécurité, conçus pour les petites et moyennes entreprises (PME), les points de vente, les services publics et les entreprises distribuées comprenant sites distants et succursales. À la différence des produits grand public, la série TZ regroupe des services extrêmement efficaces de protection anti-malware, de prévention des intrusions, de filtrage de contenu/URL et de contrôle applicatif sur les réseaux câblés et sans fil, ainsi qu'une prise en charge étendue de plateformes mobiles pour les ordinateurs portables, smartphones et tablettes. Garante d'une inspection approfondie des paquets (DPI) à très hautes performances, elle ne crée aucun encombrement sur le réseau, optimisant par là même la productivité des entreprises.

Comme avec tous les pare-feux SonicWall, la série TZ inspecte l'ensemble du fichier, y compris les fichiers chiffrés TLS/SSL, pour assurer une protection complète. La série TZ intègre en outre les fonctionnalités suivantes : surveillance et contrôle des applications, analyse avancée du trafic applicatif et reporting, VPN IPSec et SSL, basculement multi-FAI, équilibrage de charge et SD-WAN. Intégrées en option, les fonctionnalités PoE (Power over Ethernet) et sans fil 802.11ac haut débit permettent de repousser les limites du réseau simplement et en toute sécurité. Associés aux commutateurs SonicWall, les pare-feux TZ Series permettent d'étendre l'activité de manière simple, sûre et flexible grâce au déploiement zéro intervention.

Cette toute dernière génération réunit les premiers pare-feux au format bureau équipés d'interfaces gigabit ou multi-gigabits (2,5/5/10G), avec le SD-WAN sécurisé, un stockage intégré et extensible, la prise en charge TLS 1.3 et la compatibilité 5G, le tout associé à des performances révolutionnaires. Des alimentations redondantes et la prise en charge 802.11ac Wave 2 améliorent encore les fonctionnalités de ces appareils. Conçue pour les moyennes structures et les entreprises distribuées avec sites SD-Branch, la nouvelle génération de pare-feux TZ Series allie une efficacité de la sécurité reconnue par le secteur et un rapport prix/performances haut de gamme.

### SonicWall Network Security virtual (NS*v*) Series

Les pare-feux SonicWall Network Security virtual (NS*v*) permettent d'étendre la détection et la prévention automatisées des failles aux environnements hybrides et multi-cloud via des versions virtualisées des pare-feux de nouvelle génération SonicWall. Avec des outils et des services de sécurité complets équivalents à un pare-feu SonicWall, la série NS*v* protège avec efficacité vos environnements virtuels et cloud contre les utilisations abusives des ressources, les attaques croisées de machines virtuelles, les attaques par canal auxiliaire ainsi que toutes les menaces et tous les exploits courants sur le réseau.

La série NS*v* offre un déploiement et une configuration simplifiés dans un environnement virtuel mutualisé, généralement entre réseaux virtuels. Elle établit des mesures de contrôle d'accès permettant de préserver la sécurité des données/VM tout en capturant le trafic virtuel entre les machines virtuelles et les réseaux, pour une prévention automatisée des failles.

Grâce à une infrastructure autorisant la haute disponibilité (HA), la série NS*v* répond aux exigences d'évolutivité et de disponibilité définies par le SDDC (Software Defined Data Center). Facile à déployer en tant qu'appliance virtuelle sur les plateformes cloud privées telles que VMWare ESXi, Linux KVM, Nutanix ou Microsoft Hyper-V, ou dans les environnements de cloud public AWS ou Microsoft Azure. Les entreprises peuvent profiter de modèles de licence flexibles BYOL et PAYG avec NS*v* et bénéficier de tous les avantages sécurité d'un pare-feu physique, doublés des avantages opérationnels et économiques de la virtualisation.

Certains modèles de pare-feux NS*v* intègrent SonicOSX avec Unified Policy, qui offre une expérience optimisée permettant de contrôler les modifications du trafic dynamique en moins de temps et assurant une meilleure posture de sécurité globale.

**Pour en savoir plus** sur les pare-feux SonicWall, consultez la page : www.sonicwall.com/fr-fr/products/firewalls/

## Capture Security appliance 1000 (CSa 1000)

Pour être en conformité avec les réglementations et les normes de confidentialité, il vous faut une plateforme d'analyse des menaces respectueuse du budget et qui soit indétectable et incontournable par les codes malveillants. SonicWall Capture Security appliance (CS*a*) est une solution d'analyse de fichiers et de détection des malwares sur site dotée de la technologie SonicWall RTDMI (Real-Time Deep Memory Inspection). RTDMI permet à CS*a* d'intercepter davantage de malwares, plus vite et avec plus d'efficacité. Son faible taux de fausses alertes améliore la sécurité et l'expérience des utilisateurs finaux.

CS*a* permet d'analyser les logiciels malveillants cachés dans un vaste éventail de types de fichiers, tailles de fichiers et environnements d'exploitation afin de pouvoir assurer la meilleure détection possible des menaces zero-day. Les attaques par canal auxiliaire sont détectées et bloquées grâce à une inspection en temps réel basée sur la mémoire. En forçant les malwares à révéler leurs armes dans la mémoire, CS*a* bloque proactivement les menaces de masse, celles qui sont encore inconnues et les zero-day. CS*a* est compatible avec les réseaux fermés et s'utilise avec les tout derniers pare-feux de nouvelle génération SonicWall.

Le déploiement de SonicWall CS*a* est simple et rapide. Pour démarrer, il n'y a que les configurations de base à faire pour le réseau, le reporting et l'accès des appareils autorisés. Conçue de manière à être adressable par IP, la solution CS*a* peut être déployée n'importe où, dès lors qu'elle est joignable par des appareils qui lui soumettront des fichiers pour analyse. Elle peut également être déployée dans des réseaux fermés ou en air gap.

## Sécurité câblée

Les commutateurs SonicWall assurent une commutation réseau haut débit, doublée de performances et d'une gérabilité inégalées. Ils affichent une grande densité de ports, une option PoE (Power over Ethernet) et un débit 1 ou 10 gigabits. Parfaits pour les PME et les réseaux SD-Branch, ils permettent aux entreprises de toute taille d'effectuer leur transformation numérique et de suivre l'évolution du paysage réseau et de la sécurité.

Les commutateurs SonicWall peuvent être gérés via les pare-feux SonicWall ou par Wireless Network Manager (WNM). WNM s'intègre de manière transparente aux solutions de sécurité câblées et sans fil, de bout en bout, assurant une posture de sécurité unifiée. Cela simplifie le déploiement, la gestion et le dépannage et comble les lacunes pouvant survenir avec des commutateurs tiers. Les commutateurs SonicWall s'installent rapidement dans les succursales distribuées grâce au déploiement zéro intervention.

## Sécurité sans fil

Soucieux de rendre le sans-fil simple, sûr et abordable, SonicWall présente sa solution novatrice Wireless Network Security. Les points d'accès sans fil hautes performances SonicWave Series 802.11ax se gèrent facilement via Wireless Network Manager.

Outre les points d'accès sans fil haut débit et le tableau de bord géré dans le cloud, la solution de sécurité sans fil SonicWall comprend Wi-Fi Planner, un outil évolué d'étude de site conçu pour aider les administrateurs à planifier et déployer efficacement des réseaux wi-fi. La solution comporte également l'application mobile SonicExpress pour une intégration et une surveillance aisées des points d'accès, fournissant aux administrateurs des informations en temps réel sur l'état du réseau et de la sécurité.

Notre solution va au-delà de la simple sécurité sans fil en faisant intervenir les technologies RTDMI et RFDPI et en offrant des fonctionnalités de sécurité avancées telles que le sandboxing multimoteur, le filtrage de contenu, l'antivirus cloud directement sur le point d'accès, sans nécessiter de pare-feu. Elle améliore encore la sécurité et les performances de votre réseau grâce à une série de fonctionnalités, dont la prévention des intrusions, le déchiffrement et l'inspection TLS/SSL et le contrôle des applications.

Les points d'accès SonicWave prennent en charge le fast roaming qui permet aux utilisateurs de se déplacer d'un lieu à un autre sans discontinuité de service. Son portefeuille inclut un vaste éventail de fonctionnalités, notamment le portail captif, la sélection de canal automatique, l'analyse du spectre, l'équité du temps d'utilisation du réseau, l'orientation de bande ainsi que des outils d'analyse du signal pour la surveillance et le dépannage.

SonicWall réduit le coût total de possession (TCO) dans la mesure où les administrateurs n'ont pas à installer ni à gérer séparément une solution sans fil spéciale coûteuse parallèlement au réseau câblé.

## Sécurité des terminaux

La gestion et la sécurité des terminaux sont essentielles dans l'environnement actuel des entreprises. Lorsque les utilisateurs finaux entrent et sortent du réseau avec leurs appareils et que des menaces chiffrées atteignent des terminaux sans contrôle, il convient d'intervenir pour protéger ces appareils. Avec l'augmentation des ransomwares et des vulnérabilités applicatives, les terminaux sont un champ de bataille dans le paysage actuel des menaces.

Les administrateurs doivent également faire face à des problèmes de visibilité et de gestion de leur stratégie de sécurité. Ils sont aussi confrontés à l'obligation de garantir en permanence la sécurité des clients et de leur fournir des connaissances et des rapports faciles à utiliser et actionnables.

Si les produits de sécurité des terminaux existent depuis des années, les administrateurs sont toutefois confrontés aux problématiques suivantes :

- Maintenir les produits de sécurité à jour
- Appliquer les règles à l'échelle globale
- Obtenir des rapports et consulter la santé des utilisateurs
- Menaces empruntant ou créant des canaux chiffrés
- Comprendre les alertes et les mesures correctives
- Cataloguer les applications et leurs vulnérabilités
- Bloquer des menaces du type ransomwares
- Attaques sans fichier et périphériques USB infectés contournant les défenses du périmètre

SonicWall Capture Client est une plateforme client unifiée comportant de multiples fonctionnalités de protection des terminaux. Cette solution inclut une console de gestion basée sur le cloud et l'intégration complète en option aux pare-feux de nouvelle génération SonicWall, afin de proposer aux clients SonicWall une expérience de sécurité unifiée. En association avec des fonctionnalités d'exécution automatique, SonicWall Capture Client permet de garantir que les terminaux exécutent des logiciels de sécurité et/ou possèdent un certificat SSL intégré pour l'inspection du trafic chiffré. Par ailleurs, afin de faciliter l'inspection du trafic SSL (DPI-SSL) et d'améliorer l'expérience utilisateur, Capture Client simplifie pour les administrateurs la fourniture des certificats SSL aux terminaux.

En outre, la plateforme propose un moteur antivirus avancé conçu pour bloquer les logiciels malveillants les plus ingénieux, avec une option de restauration permettant de revenir à une version précédente non infectée. Capture Client Advanced intègre également la fonction ATP (SonicWall Capture Advanced Threat Protection) qui examine les fichiers suspects pour mieux bloquer les attaques avant qu'elles ne soient activées.

Les administrateurs peuvent désormais cataloguer toutes les applications sur chaque terminal protégé par Capture Client et établir des rapports sur les vulnérabilités connues au sein de l'écosystème.

Le tableau de bord global a été conçu pour permettre aux MSSP de visualiser le nombre d'infections, quelles vulnérabilités sont présentes et quelle version de Capture Client est installée par chaque utilisateur. Ils peuvent voir

ce qui est le plus souvent bloqué par le filtrage de contenu et chez qui, ainsi que les appareils qui sont en ligne et actifs. Les règles globales permettent aux administrateurs d'appliquer une seule et même base de règles à tous les utilisateurs, ce qui facilite la mise en place de nouveaux et crée rapidement une protection pour les nouvelles menaces, valable pour tous les utilisateurs selon cette base de règles.

Fonctionnalités SonicWall Capture Client :

- Application des mesures de sécurité
- Gestion des certificats DPI-SSL
- Surveillance comportementale en continu
- Déterminations très précises grâce à l'apprentissage automatique
- Diverses techniques heuristiques sur plusieurs niveaux
- Renseignements sur les vulnérabilités applicatives
- Fonctionnalités uniques de rollback
- Intégration de la sandbox réseau Capture Advanced Threat Protection
- Tableau de bord global et règles globales avec héritage
- Recherche en un clic des fichiers suspects dans la base de données Capture ATP de renseignements sur les menaces pour acceptation ou rejet
- Filtrage de contenu pour appliquer les règles Web et bloquer les adresses IP, URL et domaines malveillants sur les appareils en dehors du réseau
- Contrôle des appareils à base de règles afin de bloquer les périphériques de stockage potentiellement infectés

## Services de sécurité avancés

Les services de sécurité réseau des pare-feux SonicWall fournissent une protection de pointe extrêmement efficace à l'intention des entreprises de toute taille, pour les aider à se défendre face aux menaces, à mieux contrôler la sécurité, à améliorer la productivité et à réduire les coûts.

SonicWall propose trois bouquets d'abonnement sur les séries de pare-feux de septième génération : Threat Protection Services Suite, Essential Protection Services Suite et Advanced Protection Services Suite. La Threat Protection Services Suite comprend les services de sécurité de base nécessaires pour garantir la protection du réseau face aux menaces, au sein d'une offre économique. L'ajout de l'offre SonicWall Essential vous permet de bénéficier de services de sécurité essentiels pour vous protéger contre les menaces connues et inconnues. Le niveau Advanced, pour sa part, offre une sécurité évoluée qui complètera la sécurité de votre réseau par des services essentiels pour le cloud.

La **Threat Protection Services Suite**, disponible uniquement sur les séries TZ270/370/470, comprend l'antivirus au niveau de la passerelle, la prévention des intrusions et le contrôle des applications, le service de filtrage du contenu, l'inspection approfondie des paquets du trafic chiffré TLS/SSL (DPI-SSL) et un support 24h/24, 7j/7.

L'**Essential Protection Services Suite** comprend la sandbox Capture Advanced Threat Protection avec RTDMI, l'antivirus au niveau de la passerelle, la prévention des intrusions et le contrôle des applications, le service de filtrage du contenu, le service antispam complet, l'inspection approfondie des paquets du trafic chiffré TLS/SSL (DPI-SSL) et un support 24h/24, 7j/7.

L'**Advanced Protection Services Suite** comprend la sandbox Capture Advanced Threat Protection avec RTDMI, l'antivirus au niveau de la passerelle, la prévention des intrusions et le contrôle des applications, le service de filtrage du contenu, le service antispam complet, l'inspection approfondie des paquets du trafic chiffré TLS/SSL (DPI-SSL), un support 24h/24, 7j/7, la gestion cloud, le reporting cloud pour 7 jours et un support Premier en option.

## Inspection approfondie de la mémoire

Technologie en instance de brevet, le moteur RTDMI (Real-Time Deep Memory Inspection) de SonicWall détecte et bloque de manière proactive les logiciels malveillants grand public inconnus via une inspection approfondie de la mémoire en temps réel. Disponible dès aujourd'hui avec le service de sandboxing cloud SonicWall Capture Advanced Threat Protection (ATP), le moteur identifie et maîtrise même les menaces modernes les plus insidieuses, notamment les futurs exploits Meltdown.

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

## Cloud App Security

La solution SonicWall Cloud App Security protège les applications SaaS courantes de messagerie, de collaboration et de productivité telles qu'Office 365 email, SharePoint, OneDrive, G-Suite, Dropbox et Box. Elle couvre notamment les éléments suivants :

- Business Email Compromise (BEC)
- Prévention contre la perte de données (DLP)
- Piratage de compte (ATO)
- Malwares évolués et menaces zero-day dans les pièces jointes et fichiers stockés malveillants
- Phishing ciblé
- Tentatives de fraude

Cloud App Security utilise des techniques avancées de profilage des utilisateurs et d'analyse comportementale comptant plus de 300 indicateurs de menaces, afin de déterminer si des comptes légitimes sont en prise à des cybercriminels. Grâce au machine learning (ML) et à l'intelligence artificielle (IA), la solution empêche les usurpations d'identité, y compris le scannage rétroactif d'activités.

Pour les applications SaaS et de partage de fichiers du type OneDrive, Cloud App Security fait appel à la sandbox multimoteur de SonicWall Capture ATP pour détecter les malwares inédits. Elle effectue des scans à la fois historiques et en temps réel de fichiers et de données, que ce soit au repos ou lors du passage dans un environnement SaaS, en interne ou d'un cloud à un autre. De plus, le service DLP de la solution protège les données au repos en limitant l'accès aux seules applications autorisées et en empêchant les chargements de données non autorisés.

En tant que service SaaS, Cloud App Security peut être activée et prête à l'emploi en quelques minutes. Évolutive à l'infini, la solution aide les organisations de toute taille à installer une protection immédiate pour leurs utilisateurs d'applications SaaS, qu'ils soient des centaines ou des centaines de milliers dispersés dans le monde entier. Chaque application SaaS a son moteur de règles, avec des règles et des fonctionnalités d'exécution propres. Vous pouvez ainsi définir une politique spécifique à chaque application SaaS en fonction des exigences de sécurité.

Ne requérant ni installation ni gestion de matériel ou de logiciel, Cloud App Security élimine l'investissement initial, l'installation complexe et les coûts réguliers de maintenance associés au déploiement d'une solution sur site.

**Pour en savoir plus** sur SonicWall Cloud App Security, consultez la page https://www.sonicwall.com/fr-fr/products/cloud-security/

## Cloud Edge Secure Access

### Du VPN traditionnel à la sécurité zéro confiance

Aujourd'hui, les collaborateurs souhaitent pouvoir travailler de n'importe où et les entreprises veulent profiter des économies et de l'efficacité opérationnelle offertes par le cloud.

Mais les solutions de VPN traditionnelles n'ont pas été conçues pour cette nouvelle réalité. Aussi, leur déploiement peut durer des jours voire des semaines. Au vu des problèmes de disponibilité en stock, elles peuvent ou pas être livrables, et une fois que vous en avez installé une, il peut être difficile de programmer l'interruption de service.

Pire, elles peuvent ouvrir une porte dérobée dans votre réseau, dans la mesure où toute connexion réussie donne largement accès au réseau et permet les mouvements latéraux dans le sous-réseau.

Comme le trafic utilisateurs transite par le concentrateur VPN local au lieu d'aller directement au cloud, le VPN crée une latence qui amoindrit l'efficacité et dégrade l'expérience cloud des utilisateurs.

Selon les prévisions de Gartner, 60 % des entreprises délaisseront d'ici 2023 leur accès distant par VPN au profit de l'accès réseau zéro confiance (ZTNA).

### Protéger les précieuses ressources grâce à la sécurité du réseau zéro confiance

Avec Cloud Edge Secure Access, SonicWall propose une solution ZTNA qui non seulement résout ces problèmes, mais qui offre en plus une multitude d'autres avantages. SonicWall Cloud Edge Secure Access renferme trois fonctionnalités essentielles :

- Droit d'accès minimal pour protéger les actifs de l'entreprise
- Déploiement rapide en libre-service
- Accès direct et fiable au cloud de n'importe où

En tant que service cloud natif, la solution fournit un réseau en tant que service (NaaS) simple pour la connectivité site à site et cloud hybride intégrant la sécurité zéro confiance et le droit d'accès minimal.

- Le service Device Posture Check (DPC) octroie l'accès au réseau uniquement aux appareils authentifiés et conformes
- Les règles de micro-segmentation à définition logicielle empêchent efficacement les infractions de se propager
- Network Traffic Control (NTC) est un pare-feu en tant que service (FwaaS) dynamique qui assure une protection à base de règles en définissant qui peut accéder à quelle ressource et de quel endroit

Les entreprises peuvent désormais donner à leurs collaborateurs tout ce dont ils ont besoin pour travailler à distance, tout en protégeant leurs actifs stratégiques.

### Un service cloud natif mondial déployé en quelques minutes

SonicWall Cloud Edge est pris en charge par plus de 30 points de présence mondiaux (PoP).

Ce service permet aux responsables informatiques de connecter une succursale et d'effectuer le déploiement en 15 minutes. Les utilisateurs finaux, eux, peuvent installer le client SonicWall Cloud Edge et être productifs en 5 minutes.

L'infrastructure repose sur l'architecture SDP (Software-Defined Perimeter), qui sépare le contrôleur centralisé des passerelles qui font office d'agents de confiance.

La distribution de passerelles SDP permet à Cloud Edge Secure Access d'évoluer rapidement, tout en maintenant de hautes performances, et d'offrir la meilleure expérience cloud possible.

De plus, la séparation des fonctions rend Cloud Edge Secure Access imperméable aux cybermenaces communes telles que DDoS, exploits Log4j, hijacking de wi-fi public, inondations SYN ou encore Slowloris.

### Avantages supplémentaires :

- Solution de sécurité pour entreprises distribuées et collaborateurs distants
- Accès sécurisé instantané aux sites physiques et ressources sur clouds hybrides
- De 10 à plusieurs milliers d'utilisateurs
- Accès Web sans client avec tout appareil public
- Chiffrement WireGuard hautes performances
- Fournisseur d'identité cloud et intégrations SIEM
- Intégration MFA et SSO moderne
- Intégration SIEM
- Mutualisation pour MSSP
- Network Traffic Control (NTC) assure une protection de niveau pare-feu en définissant qui peut accéder à des services réseau spécifiques et de quel endroit
- Le service Device Posture Check (DPC) octroie l'accès au réseau uniquement aux appareils authentifiés et conformes.
- Disponible aux États-Unis, en Europe, au Moyen-Orient et en Asie

**Pour en savoir plus** sur SonicWall Cloud Edge Secure Access, consultez la page https://www.sonicwall.com/fr-fr/products/cloud-edge-secure-access/

## Accès mobile sécurisé

La série SonicWall Secure Mobile Access (SMA) est une passerelle d'accès sécurisé unifiée, destinée aux entreprises confrontées aux thématiques de la mobilité, du télétravail, du BYOD et de la migration vers le cloud. Cette solution leur permet de fournir un accès aux ressources vitales, quels que soient le lieu, le moment ou l'appareil. Le moteur de règles de contrôle granulaire des accès des SMA, l'autorisation contextuelle d'appareils, le VPN au niveau applicatif et l'authentification avancée par SSO donnent aux entreprises les moyens nécessaires pour adopter le BYOD et la mobilité dans les environnements informatiques hybrides.

SMA réduit en outre la surface disponible aux menaces grâce à des fonctionnalités telles que le filtrage GeoIP, la détection de réseaux de zombies, le service WAF (Web Application Firewall) ou encore l'intégration d'une sandbox avec Capture ATP.

### Mobilité et BYOD

Dès lors que les entreprises envisagent d'adopter le BYOD, des méthodes de travail flexibles ou encore un développement à l'étranger, la série SMA devient un outil incontournable. La solution SMA de SonicWall fournit une sécurité de pointe permettant de réduire à un minimum les menaces en surface. La prise en charge des tout derniers algorithmes et méthodes de chiffrement assure, elle, une protection en profondeur. La technologie SMA de SonicWall permet aux administrateurs de configurer en toute simplicité un accès mobile sécurisé et des privilèges en fonction de rôles, de manière à ce que les utilisateurs finaux puissent accéder rapidement et facilement aux applications, données et ressources dont ils ont besoin. Parallèlement, les entreprises peuvent établir des règles de sécurisation BYOD pour protéger leur réseau et leurs données des accès indésirables et des logiciels malveillants.

### Passage au cloud

Les entreprises qui optent pour la migration vers le Cloud disposent avec SMA d'une infrastructure SSO (Single Sign-on) basée sur un portail Web unique pour l'authentification des utilisateurs dans un environnement informatique hybride. Que les ressources de l'entreprise se trouvent sur site, sur le Web ou dans un cloud hébergé, l'expérience d'accès est cohérente et transparente. Les utilisateurs n'ont pas besoin de se souvenir des URL de chaque application ni de constituer des listes de signets. Grâce à Workplace, un portail d'accès centralisé, vos utilisateurs disposent d'une seule et même URL pour accéder à toutes les applications vitales, par un simple navigateur Web. La solution SMA fournit le SSO fédéré, tant pour les applications SaaS hébergées dans le cloud qui utilisent SAML 2.0, que pour les applications hébergées en campus qui reposent sur RADIUS ou Kerberos. SMA est compatible avec différents serveurs d'authentification, d'autorisation et de comptes ainsi qu'avec les principales technologies d'authentification multifacteur (MFA), pour davantage de sécurité. Le SSO sécurisé n'est attribué qu'aux terminaux autorisés, à l'issue de contrôles concernant leur état de santé et de conformité.

### Fournisseurs de services gérés

Aux entreprises disposant de centres de données ou aux fournisseurs de services gérés, SMA fournit une solution clés en main garantissant un niveau élevé de continuité des activités et d'évolutivité. La technologie SMA de SonicWall permet de prendre en charge jusqu'à 20 000 connexions simultanées sur une seule appliance, avec possibilité d'évolution jusqu'à un million d'utilisateurs grâce au clustering intelligent. Réduisez les coûts des centres de données grâce au clustering HA actif/actif (Global High Availability) et à un équilibreur de charge dynamique intégré (Global Traffic Optimizer), qui réalloue le trafic global au centre de données le plus adéquat et ce, en temps réel, à la demande de l'utilisateur. SMA met à la disposition des détenteurs de services toute une gamme d'outils nécessaires à la fourniture d'un service sans la moindre interruption et permettant de respecter des accords SLA très stricts.

### Appliances SMA

La solution SonicWall SMA peut être déployée sous la forme d'une appliance hautes performances renforcée ou d'une appliance virtuelle s'appuyant sur les ressources informatiques partagées pour optimiser l'utilisation, faciliter la migration et réduire les coûts d'investissement. Les appliances matérielles reposent sur une architecture multiprocesseur qui allie accélération SSL et débit VPN hautes performances à de puissants proxys pour fournir un accès sécurisé fiable. Pour les entreprises appartenant à des secteurs réglementés et les organismes publics, la solution SMA est disponible avec la certification FIPS 140-2 niveau 2. Les appliances virtuelles SMA assurent la même robustesse fonctionnelle de l'accès sécurisé sur les principales plateformes virtuelles et cloud, comme Hyper-V, VMWare ESX/ESXi, KVM, AWS et Azure. Que vous optiez pour le matériel ou le virtuel, ou une combinaison des deux, les appliances SMA s'intégreront en toute fluidité à votre infrastructure informatique existante.

### SMA Web Application Firewall

La solution SonicWall SMA100 Series Web Application Firewall (WAF) permet d'établir une stratégie de défense en profondeur en augmentant le périmètre de sécurité, afin de protéger vos applications Web dans les environnements cloud privés, publics ou hybrides. La série SMA100 WAF assure la protection des applications Web et contre la divulgation d'informations, tout en accélérant les fonctionnalités de mise à disposition des applications Web qui permettent d'opérer un équilibrage de charge sensible aux applications, le déchargement SSL pour la résilience,

une résistance accrue aux pannes et une expérience numérique améliorée.

Avantages supplémentaires :

- Protection contre les vulnérabilités connues et zero-day grâce aux règles personnalisées et de correction virtuelle
- Défense contre les vulnérabilités et menaces les plus récentes définies par l'OWASP, notamment l'injection SQL et le cross-site scripting (XSS)
- Prise en charge de l'accès zéro confiance sans client via un navigateur Web pour une utilisation pratique avec tout appareil public
- Exigences de gestion de session et d'authentification fortes telles que OTP, 2FA et SSO
- Garantie d'une protection haute disponibilité des serveurs contre les attaques DoS/ DDOS

### Gestion et reporting

La plateforme Web de gestion intuitive fournie par SonicWall permet de rationaliser la gestion des appliances et propose des fonctionnalités de reporting étendues. L'interface utilisateur conviviale met de la clarté dans la gestion de plusieurs équipements. La gestion unifiée des règles vous permet de créer et de surveiller des règles et configurations d'accès. Une seule configuration de règle peut gérer vos utilisateurs, appareils, applications, données et réseaux. Les tâches routinières et les activités planifiées sont automatisées. Ainsi, au lieu de perdre du temps à des travaux répétitifs, vos équipes de sécurité peuvent se concentrer sur les tâches stratégiques, comme la réponse aux incidents.

Donnez à votre département informatique les moyens d'offrir la meilleure expérience et l'accès le plus sécurisé , selon le scénario d'utilisation. Vous avez le choix entre diverses possibilités d'accès sécurisé entièrement sans client, via le Web, pour les fournisseurs et entreprises tierces, ou un accès plus classique sur client par tunnel VPN pour les dirigeants. Qu'il s'agisse de fournir un accès sécurisé fiable à cinq utilisateurs d'un centre de données ou à des milliers d'utilisateurs répartis dans le monde entier, SonicWall SMA a la solution.

**Pour en savoir plus** sur les produits de sécurité mobile SonicWall, consultez la page : www.sonicwall.com/fr-fr/products/remote-access/

## Sécurisation de messagerie

La messagerie est un composant essentiel de la communication de l'entreprise, mais elle est aussi le vecteur d'attaque n°1 pour les menaces telles que ransomwares, phishing, BEC (Business Email Compromise), spoofing, spam et virus. Qui plus est, d'après les réglementations gouvernementales, votre entreprise peut désormais avoir des comptes à rendre concernant la protection des données confidentielles, les mesures prises pour éviter les fuites et enfin la sécurisation des échanges d'e-mails contenant des informations sensibles ou personnelles de clients. Que votre organisation soit une PME en expansion, une grande entreprise distribuée ou un fournisseur de services gérés (MSP), vous avez besoin d'une solution économique de sécurisation de messagerie et de chiffrement. Évolutive, elle doit vous permettre d'augmenter facilement les capacités pour les unités et les domaines organisationnels et de déléguer la gestion.

Dans un souci de gestion des coûts et des ressources, les entreprises adoptent également Microsoft Office 365 et Google G Suite. Ces produits offrent certes des fonctionnalités de sécurité intégrées, mais les entreprises qui souhaitent

lutter contre les menaces véhiculées par la messagerie ont besoin d'une solution de sécurisation de nouvelle génération qui intègre de façon transparente Office 365 et G Suite, afin de les protéger des menaces évoluées actuelles.

### Appliances SonicWall Email Security

Facile à configurer et à administrer, la solution SonicWall Email Security est conçue pour passer à peu de frais de 10 à 100 000 messageries. Elle peut être déployée sous forme matérielle, comme appliance virtuelle s'appuyant sur des ressources informatiques partagées, ou comme logiciel, y compris le logiciel optimisé pour Microsoft Windows Server ou Small Business Server. Les appliances physiques SonicWall Email Security sont idéales pour les entreprises qui ont besoin d'une solution dédiée sur site. Notre solution multicouche assure une protection entrante et sortante complète. Elle est disponible en une série d'appliances matérielles allant jusqu'à 10 000 utilisateurs par appliance. SonicWall Email Security existe aussi sous forme virtuelle ou logicielle. L'idéal pour les entreprises en quête de la flexibilité et de l'agilité de la virtualisation. La solution peut être configurée en mode divisé à des fins de haute disponibilité, pour gérer de manière centralisée et fiable des déploiements à grande échelle.

La solution de sécurisation de messagerie SonicWall utilise des technologies comme l'apprentissage automatique, l'analyse heuristique, l'analyse de réputation et de contenu, la protection time-of-click des URL et le sandboxing pour les pièces jointes et les URL afin d'assurer une protection complète des messages entrants et sortants.

Cette solution inclut également de puissantes normes d'authentification des e-mails permettant de bloquer les attaques de spoofing et les messages frauduleux, notamment : SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) et DMARC (Domain-based Message Authentication, Reporting et Conformance).

- Bloquez les menaces évoluées avant qu'elles n'atteignent votre boîte de réception
- Protégez-vous des messages frauduleux et des attaques de phishing ciblées
- Bénéficiez de mesures de sécurité actualisées grâce aux renseignements sur les menaces en temps réel
- Sécurisez votre service de messagerie cloud (Office 365, G-Suite)
- Assurez prévention contre la perte de données de messagerie et conformité
- Gestion et reporting simplifiés
- Options de déploiement flexibles

L'administration de la solution Email Security est intuitive, rapide et simple. Vous pouvez déléguer en toute sécurité la gestion des spams aux utilisateurs finaux, tout en conservant le contrôle nécessaire sur les règles de sécurité appliquées. Vous pouvez aussi gérer en toute simplicité les comptes d'utilisateurs et de groupes grâce à une synchronisation multi-LDAP transparente.

La solution assure également une intégration facile pour Office 365 et G-Suite pour une protection contre les menaces de messagerie évoluées.

Dans les grands environnements distribués, la prise en charge de la mutualisation vous permet de charger des sous-administrateurs de gérer les paramètres au niveau de différentes unités organisationnelles (divisions de l'entreprise ou clients MSP, par ex.) au sein d'un seul et même déploiement Email Security.

### SonicWall Hosted Email Security Service

Faites confiance à des services hébergés rapidement déployés et faciles à administrer pour protéger votre structure contre les menaces qui exploitent les messageries : ransomwares, menaces zero-day, spear-phishing ou encore Business Email Compromise (BEC), tout en respectant les exigences réglementaires en matière de conformité des e-mails. Bénéficiez du même niveau de protection des messageries avec notre solution hébergée qu'avec nos appliances matérielles et virtuelles, car les fonctionnalités sont identiques. La solution offre également la continuité de messagerie afin de garantir la remise des e-mails et l'absence d'impact sur la productivité lors de pannes planifiées ou non des serveurs de messagerie sur site ou d'un fournisseur cloud, tel que Office 365 et G Suite.

SonicWall Hosted Email Security assure une protection supérieure, basée sur

le cloud, contre les menaces entrantes et sortantes, à un tarif d'abonnement mensuel ou annuel flexible, prévisible et économique. Elle vous permet de limiter le temps et les coûts de déploiement initiaux, de même que les dépenses d'administration régulières, sans faire aucun compromis sur la sécurité.

SonicWall permet aux revendeurs à valeur ajoutée (VAR) et aux fournisseurs de services gérés (MSP) de gagner en compétitivité et d'accroître leurs revenus, tout en réduisant à un minimum leurs risques, leurs charges administratives et leurs coûts réguliers. SonicWall Hosted Email Security inclut des caractéristiques adaptées aux MSP, telles qu'une puissante mutualisation, la gestion centralisée de plusieurs abonnés, l'intégration avec Office 365, des options d'achat flexibles et la configuration automatisée.

**Pour en savoir plus** sur les produits de sécurisation de messagerie SonicWall, consultez la page www.sonicwall.com/fr-fr/products/secure-email/cloud-email-security/

## Gestion, rapports et analyse

Pour SonicWall, une approche connectée de la gestion de la sécurité est fondamentale dans un cadre préventif. Mais elle constitue également le socle d'une stratégie unifiée de gouvernance de la sécurité, de conformité et de gestion des risques. Avec les solutions SonicWall de gestion, de reporting et d'analyse, les entreprises disposent d'une plateforme intégrée, sécurisée et extensible leur permettant d'établir une ligne de défense robuste et uniforme et une stratégie de réponse sur leurs réseaux câblés, sans fil et multi-cloud. De plus, l'adoption totale de cette plateforme commune confère aux entreprises une vision approfondie de la sécurité, qui leur permet de prendre des décisions avisées en la matière et d'aller plus vite, au profit de la collaboration, de la communication et de la connaissance à travers ce cadre de sécurité partagé.

### SonicWall Network Security Management

SonicWall Network Security Manager (NSM) renferme tout ce dont votre organisation a besoin pour bénéficier d'un système de gestion unifiée des pare-feux. Il assure une visibilité au niveau client, un contrôle des appareils sur la base de groupes et une évolutivité illimitée pour configurer et gérer de manière centralisée vos opérations de sécurité réseau SonicWall, notamment : le déploiement et la gestion de tous les pare-feux, groupes d'appareils et clients, l'orchestration et l'application de configurations et de règles de sécurité cohérentes dans les environnements SD-Branch et SD-WAN, et la surveillance de l'ensemble sur un seul tableau de bord dynamique compilant rapports détaillés et analyses. NSM vous permet de faire tout cela depuis une seule et même console cloud native conviviale, accessible de n'importe où, via tout appareil doté d'un navigateur.

Pour les fournisseurs de services, NSM propose une gestion mutualisée complète et un contrôle indépendant des règles sur l'ensemble des clients gérés. Cette séparation englobe toutes les fonctionnalités de gestion de la solution NSM qui dictent le fonctionnement du pare-feu pour chaque client. Ainsi, vous pouvez configurer chaque client de manière à ce qu'il dispose de son propre ensemble d'utilisateurs, de groupes et de rôles pour effectuer la gestion des groupes d'appareils, l'orchestration des règles et toutes les autres tâches administratives dans les limites

### SonicWall Analytics

SonicWall Analytics transforme les données en décisions et les décisions en actions qui résolvent les problèmes de sécurité et empêchent leur réapparition.

Il s'agit d'un puissant service de surveillance et d'analyse du trafic, qui fournit une vue plongeante sur tout ce qui survient au sein de l'environnement de sécurité réseau. Le moteur d'analyse décisionnelle agrège, normalise et contextualise les données de sécurité, notamment le trafic réseau et les activités des utilisateurs qui transitent par le pare-feu et les points d'accès sans fil, permettant aux administrateurs d'avoir une connaissance directe des informations sur les menaces de leur réseau et de leurs utilisateurs en temps quasi réel.

Fortes d'analyses et de rapports pertinents, les organisations ont

*[1] NSM SaaS inclut des fonctionnalités de reporting et d'analyse.*
*[2] NSM sur site nécessite une installation et une licence SonicWall Analytics sur site séparée pour les fonctionnalités de reporting et d'analyse.*

les renseignements et la capacité nécessaires pour trouver et affronter plus efficacement les problèmes de sécurité et opérationnels. Les fonctionnalités de zoom permettent aux équipes de sécurité d'enquêter, d'analyser et de prendre des mesures sur la base de preuves contre les activités et comportements suspects ou risqués des utilisateurs, le tout avec davantage de visibilité, de précision et de rapidité. Elles peuvent ainsi concentrer leur temps et leurs efforts à orchestrer des réponses et des actions correctives face aux risques importants au lieu de réagir à chaque événement.

En outre, l'intégration d'Analytics dans le processus métier permet d'opérationnaliser l'analyse en automatisant des alertes actionnables en temps réel, d'orchestrer les règles et les contrôles de sécurité de manière proactive et automatisée ainsi que de surveiller les résultats afin de garantir la sécurité requise.

### SonicWall Wireless Network Manager

SonicWall Wireless Network Manager (WNM) intègre de manière globale la gestion des points d'accès SonicWave et des commutateurs SonicWall. Faisant partie intégrante de l'écosystème SonicWall Capture Security Center, il assure une visibilité et une gestion unifiées à travers les réseaux câblés et sans fil.

WNM est un service cloud convivial qui simplifie l'accès, le contrôle et le dépannage sur un tableau de bord en un seul écran. Grâce à WNM, les administrateurs peuvent créer des règles individuelles au niveau client et les envoyer vers les différents sites et zones, ou zoomer sur les appareils gérés pour bénéficier de données granulaires. WNM est hautement évolutif, capable de gérer un site unique ou des réseaux d'entreprise mondiaux avec des dizaines de milliers d'appareils gérés.

Avant le déploiement des points d'accès, une enquête du site sans fil peut aider à garantir les performances et la productivité. L'outil Wi-Fi Planner intégré à WNM aide à déployer les points d'accès de manière stratégique afin d'optimiser l'expérience wi-fi des utilisateurs et d'éviter les erreurs coûteuses.

Les points d'accès SonicWave et les commutateurs SonicWall utilisent le déploiement zéro intervention pour une intégration automatique en l'espace de quelques minutes, grâce à l'application mobile SonicExpress. La configuration est simple et peut se faire à distance, ce qui permet de gagner du temps et de l'argent.

Les mises à jour automatiques du firmware et de la sécurité assurent l'actualisation des appareils gérés. En cas de panne d'Internet, les points d'accès et les commutateurs peuvent continuer à fonctionner sans WNM, garantissant la continuité des activités.

**Pour en savoir plus** sur les produits de gestion et de reporting SonicWall, consultez la page : www.sonicwall.com/fr-fr/products/management-and-reporting.

## Services et support professionnels

Tirez davantage de votre solution de sécurité réseau SonicWall et bénéficiez du support dont vous avez besoin, quand vous en avez besoin. Le support SonicWall pour les grandes entreprises et les services professionnels vous permettront de mieux rentabiliser votre solution sur le long terme.

### Services de support global

Choisissez une solution de support à votre convenance pour garantir la bonne marche de votre activité :

#### Support technique

- **8x5** : du lundi au vendredi, de 08h00 à 17h00 pour les environnements non critiques.
- **7x24** : support 24 h/24, y compris les week-ends et jours fériés, pour les environnements vitaux.

#### Support à valeur ajoutée

- **Support Premier** : attribue aux environnements de grandes entreprises un responsable de compte technique, ou TAM (Technical Account Manager), dédié. Le TAM est votre conseiller de confiance. Il collabore avec votre équipe afin de limiter autant que possible les interruptions de service imprévues, optimiser les processus informatiques, fournir des rapports opérationnels pour gagner en efficacité. Il est votre point de contact unique, garantissant la fluidité du support.
- Le **technicien de support dédié, ou DSE (Dedicated Support Engineer),** est une ressource désignée à la disposition de votre compte entreprise. Votre DSE connaît et comprend votre environnement, vos règles et vos objectifs informatiques, de sorte qu'il peut vous apporter des solutions techniques rapides lorsque vous avez besoin d'assistance.

### Services professionnels globaux

Vous avez besoin d'aide pour savoir quelle solution de sécurité est la meilleure pour vous, et pour l'installer au sein de votre infrastructure ? Laissez-nous nous en occuper. Avec les Services professionnels globaux, vous disposez d'un point de contact unique pour tous vos besoins de déploiement et d'intégration. Vous recevez des services sur mesure, parfaitement adaptés à votre environnement, ainsi qu'une assistance en matière de :

- **Planification :** délimiter et comprendre les exigences de votre pare-feu.
- **Implémentation / déploiement :** évaluer et déployer votre solution.
- **Transfert de connaissances :** utiliser, gérer et entretenir votre équipement.
- **Migration :** limiter les interruptions et garantir la continuité des activités.

Les services aux entreprises de SonicWall sont disponibles avec les gammes NS*sp*/NS*a*/TZ Series/SMA/ Email Security/GMS.

Pour en savoir plus : www.sonicwall.com/fr-fr/support

## Conclusion

### Découvrez les produits de sécurité SonicWall

Intégrez vos matériels, logiciels et services pour une sécurité optimale. Plus d'infos sur www.sonicwall.com. Pour connaître les options d'achat et de mise à jour, consultez www.sonicwall.com/how-to-buy. Et essayez vous-même les solutions SonicWall sur www.sonicwall.com/trials.

## À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution, dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com