Les gammes de produits SonicWall

Vue d'ensemble

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 service 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 de 9 éléments et fonctionnalités clés :

- Sécurité réseau
- Sécurité du réseau sans fil
- Sécurité des applications Web
- Sécurité des terminaux
- Sécurité des applications du Cloud
- Services de sécurité avancés
- Accès à distance
- Sécurisation de messagerie
- Gestion de la sécurité et analyses

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.

Produits de sécurité réseau

SonicWall est l'un des premiers fournisseurs de pare-feu nouvelle génération (NGFW). SonicOS, le micrologiciel éprouvé de SonicWall, est au cœur de chaque pare-feu nouvelle génération (NGFW). SonicOS s'appuie sur notre architecture matérielle évolutive et multicœur, ainsi que sur nos moteurs RTDMI™ (Real-Time Deep Memory Inspection), inspection approfondie de la mémoire en temps réel en instance de brevet, et RFDPI (Reassembly – Free Deep Packet Inspection®, inspection approfondie des paquets sans réassemblage) brevetés*, à passage unique et faible latence, qui analysent tout le trafic indépendamment du port ou du protocole.

Nos NGFW s'assurent que chaque octet de chaque paquet est inspecté, tout en maintenant les performances élevées et la faible latence nécessaires aux réseaux très chargés. Contrairement à ce qu'offre la concurrence, le moteur RFDPI à un seul passage permet une analyse des applications, simultanée et multimenace, ainsi qu'une analyse de fichiers de toutes tailles, sans réassemblage de paquets. Cela permet aux NGFW de SonicWall d'étendre massivement ce qui se fait de mieux en matière de sécurité des réseaux d'entreprises et centres de données évolutifs et distribués.

Les NGFW de SonicWall offrent une gamme de capacités robustes, notamment :

- Sandbox Capture ATP multimoteur basé sur le Cloud
- SD-WAN
- API REST
- Déchiffrement et inspection du trafic chiffré
- Service de prévention des intrusions (IPS)
- Protection contre les programmes malveillants (malwares)
- Surveillance des applications, contrôle et visualisation en temps réel
- Filtrage des sites Web/URL (filtrage des contenus)
- Réseau privé virtuel (RPV) sur SSL ou IPSec
- Sécurisation du réseau sans fil
- Sécurité des environnements hybrides et multi-cloud
- Relais/basculement dynamique

Par ailleurs, les pare-feu SonicWall assurent une protection en continu et très réactive contre les menaces zeroday grâce à l'équipe de recherche sur les menaces Capture Labs. Cette équipe recueille, analyse et étudie les informations relatives aux menaces croisées provenant de diverses sources de détection des menaces, dont plus d'un million de capteurs implantés partout dans le monde au sein de son réseau Capture Threat Network.

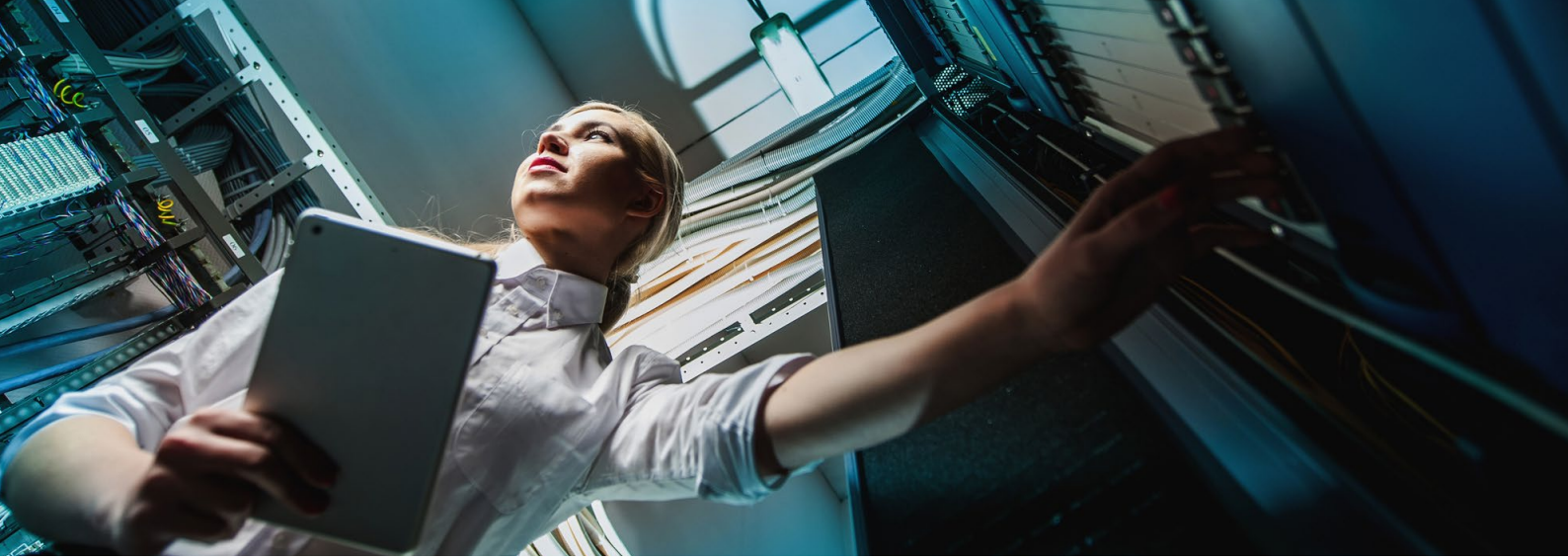
SonicWall Network Security services platform (NS*sp*) Series

La plateforme de pare-feu de nouvelle génération SonicWall NS*sp* 12000 Series est conçue pour fournir aux vastes réseaux une évolutivité, une fiabilité et une sécurité maximum à des débits multi-gigabits.

NSS Labs a soumis les pare-feu de nouvelle génération SonicWall à l'un des tests de performances réelles les plus rigoureux. Résultat : SonicWall excelle en termes d'efficacité de la sécurité, de performances, d'évolutivité, de fiabilité et de coût total de possession. Pour la cinquième fois, les pare-feu SonicWall sont exemplaires 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.

La série NS*sp* 12000 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 40/10 Gbits/s. Grâce aux technologies d'apprentissage profond utilisées pour la plateforme SonicWall Capture Cloud, la série NS*sp* 12000 offre une protection dont l'efficacité a été prouvée pour la majorité des menaces évoluées, sans ralentissement des performances.

**É.-U. Brevets 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723*



SonicWall Network Security appliance (NSa) Series

Les pare-feu de nouvelle génération SonicWall Network Security appliance (NS*a*) comptent parmi les plus sécurisés et les plus performants. Gage d'une sécurité haut de gamme et de performances sans compromis, cette gamme repose sur la même architecture que les pare-feu de nouvelle génération de la série phare NS*sp* 12000, conçue à l'origine pour les réseaux d'opérateurs et de grands comptes les plus exigeants. Mais elle n'en perd pas pour autant la convivialité et le bon rapport qualité/prix caractéristiques de SonicWall.

Fruit de plusieurs années de recherche et de développement, la série NS*a* a été conçue dès le départ pour les entreprises distribuées, les petites et moyennes structures, les agences, les établissements scolaires et les organismes publics. La série NS*a* allie une architecture multiprocesseur révolutionnaire avec technologie RTDMI (Real-Time Deep Memory Inspection) basée sur le Cloud au moteur breveté RFDPI « single-pass » de prévention des menaces, dans une conception extrêmement évolutive. Cette association garantit une protection, des performances et une évolutivité haut de gamme, avec un maximum de connexions simultanées, une latence minimum, pas de limite dans la taille des fichiers et un nombre de connexions par seconde parmi les meilleurs de sa catégorie.

SonicWall TZ Series

La série TZ de SonicWall se compose de pare-feu 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 réunit 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-feu SonicWall, la série TZ inspecte l'ensemble du fichier, notamment 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 du trafic applicatif et reporting, VPN IPSec et SSL, basculement multi-FAI, équilibrage de charge et SD-WAN. PoE (Power over Ethernet) et connectivité sans fil haut débit 802.11ac intégrés en option permettent aux entreprises de repousser les limites de leur réseau de manière simple et fiable. Associés aux commutateurs Dell série N et série X, les pare-feu TZ Series permettent d'étendre l'activité de manière simple et flexible.

SonicWall Network Security virtual (NSv) Series

Les pare-feu 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-feu de nouvelle génération SonicWall. Avec des outils et des services de sécurité complets équivalents à un pare-feu SonicWall NS*a*, la série NS*v* protège avec efficacité vos environnements virtuels et Cloud des utilisations abusives des ressources, des attaques croisées de machines virtuelles, des attaques par canal auxiliaire et de 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). Elle peut être facilement déployée en tant qu'appliance virtuelle sur des plateformes Cloud privées comme VMWare ou Microsoft Hyper-V, ou dans des environnements Cloud publics AWS ou Microsoft Azure. Avec NS*v*, le modèle de licence est flexible et les entreprises bénéficient de tous les avantages de sécurité d'un pare-feu physique avec les avantages opérationnels et économiques de la virtualisation.

SonicWave Wireless Network Security Series

Soucieux de rendre le sans-fil simple, sûr et abordable, SonicWall présente sa solution novatrice Wireless Network Security. Cette solution associe les points d'accès sans fil hautes performances SonicWave Series 802.11ac Wave 2 à la solution SonicWall WiFi Cloud Manager (WCM) ou aux pare-feu SonicWall leaders du marché pour offrir sur un réseau sans fil les performances et la sécurité d'un réseau de nouvelle génération. WCM est un système de gestion de réseau WiFi basé dans le Cloud, intuitif, évolutif et centralisé, adapté aux réseaux de toutes tailles. Il est accessible via le SonicWall Capture Security Center. La solution WiFi Planner, disponible via WCM, vous permet de concevoir et de déployer de manière optimale un réseau sans fil. Lors du déploiement de points d'accès, l'application mobile SonicWiFi vous permet de configurer, gérer et suivre les réseaux sans fil. Ensemble, ces solutions sans fil garantissent une expérience utilisateur WiFi sécurisée.

Notre solution va au-delà des solutions sans fil sécurisées de base grâce à la sécurisation des réseaux sans fil avec les technologies RTDMI et RFDPI et à la double protection du réseau sans fil : le trafic véhiculé sans fil est chiffré et décontaminé des menaces réseau, tandis que les attaques sans fil sont éliminées. De plus, les points d'accès SonicWave exécutent des services de sécurité avancés, comme Capture et CFS, directement dans le point d'accès.

Grâce à l'itinérance rapide, les utilisateurs peuvent se déplacer d'un endroit à un autre en toute fluidité. Le portefeuille inclut un vaste éventail de fonctionnalités, notamment la sélection automatique des canaux, l'analyse de 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.

SonicWall Web Application Firewall (WAF) Series

La série SonicWall Web Application Firewall (WAF) protège les applications Web exécutées dans un environnement privé, public ou Cloud hybride. Elle propose des outils et des services de sécurité Web avancés permettant d'éviter l'exposition des données de conformité, de protéger les présences Web, d'éviter toute interruption d'activité et d'assurer leurs performances optimales. Les pare-feu WAF appliquent des fonctionnalités de fourniture d'applications de couche 7 qui permettent un équilibrage de charge sensible aux applications, le déchargement SSL et l'accélération en vue d'une résilience ainsi qu'un engagement et une expérience numériques améliorés.

La fonctionnalité WAF associe des moteurs d'inspection approfondie des paquets basés sur les signatures et le profilage d'applications afin de protéger des attaques types visant les applications Web comme celles présentées par le projet OWASP (Open Web Application Security Project), ainsi que des menaces plus avancées comme les attaques par déni de service (DoS) et les exploits contextuels. Outre la protection des applications Web, la fonctionnalité WAF évite également la perte de données grâce à des techniques de masquage et de blocage de pages pour des schémas spécifiques de données sensibles comme les informations de cartes de paiement (PCI) et les documents d'identité émis par le gouvernement.

Pour une protection optimale contre les téléchargements malveillants, les injections de code ou les menaces avancées, WAF s'appuie sur le travail de recherche des menaces de SonicWall Capture Labs. Les services SonicWall Capture ATP et RTDMI™ sont également disponibles en option pour compléter la suite de services de sécurisation Web. À cela s'ajoute la fourniture d'API qui permettent aux administrateurs de surveiller et d'orchestrer l'exécution de la fonctionnalité WAF de manière programmée, améliorant ainsi l'automatisation et l'efficacité de la sécurisation Web.

Cette fonctionnalité fournit des avantages d'échelle en matière de virtualisation et peut être déployée en tant qu'appliance virtuelle dans des Clouds privés basés sur VMWare ou ESXi ou Microsoft Hyper-V, ou dans des environnements Cloud publics AWS ou Microsoft Azure.

Capture Client

La gestion et la sécurité des terminaux sont essentielles au contexte économique actuel. Avec des utilisateurs finaux qui se connectent et se déconnectent du réseau avec leurs propres appareils, et en raison des menaces chiffrées qui s'immiscent dans les terminaux non vérifiés, quelque chose doit être fait pour protéger ces appareils. Avec la croissance des ransomwares et le problème persistant du vol d'informations d'identification, les terminaux représentent le point névralgique du paysage des menaces à l'heure actuelle.

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 :

- Veiller à la mise à jour des produits de sécurité
- Faire appliquer les politiques et garantir la conformité
- Obtenir des rapports
- Traiter les menaces cachées empruntant des canaux chiffrés
- Comprendre les alertes et les mesures correctives
- Gérer les licences
- Mettre un coup d'arrêt aux menaces comme les ransomwares
- Gérer les attaques sans fichiers et les appareils 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 aux pare-feu 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 vers les 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.

Fonctionnalités SonicWall Capture Client :

- Application des mesures de sécurité
- Gestion des certificats DPI-SSL
- Surveillance continue des comportements
- Déterminations très précises grâce à l'apprentissage automatique
- Multiples techniques heuristiques sur plusieurs niveaux
- Fonctionnalités uniques de restauration (Capture Client Advanced uniquement)
- Intégration de la sandbox réseau Capture Advanced Threat Protection (Capture Client Advanced uniquement)
- Recherche en un clic des fichiers suspects dans la base de données Capture ATP de renseignements sur les menaces pour acceptation ou rejet
- Protection contre les menaces sur le Web pour bloquer les sites et les adresses IP malveillants connus
- Contrôle des appareils basé sur des règles pour bloquer les appareils de stockage potentiellement infectés

SonicWall WAN Acceleration (WXA) Series

Les solutions SonicWall WAN Acceleration (WXA) Series réduisent la latence au niveau des applications et économisent la bande passante, ce qui améliore sensiblement les performances applicatives et l'expérience des utilisateurs du WAN dans les PME dotées de bureaux distants et succursales. Après un transfert de données initial, la série WXA réduit radicalement tout le trafic ultérieur en ne transmettant que les données nouvelles ou modifiées. La WXA déduplique les données traversant le WAN, se souvient des données transférées précédemment et remplace les séquences d'octets répétées par un identifiant, ce qui se traduit par une réduction de la latence applicative et par des économies de bande passante.

Autres fonctionnalités d'accélération : la mise en cache de données et de métadonnées, la déduplication de fichiers, la mise en cache (Web) HTTP ou encore la compression des données en circulation.

Contrairement aux produits d'accélération WAN indépendants, les solutions WXA sont des compléments intégrés aux pare-feu SonicWall NS*a* et TZ. Cela économise de la place, simplifie l'installation et la configuration et améliore le routage, la gestion ainsi que l'intégration de la WXA avec d'autres éléments, par exemple des VPN. Déployées avec un pare-feu de nouvelle génération SonicWall exécutant le service de surveillance et de contrôle des applications, les solutions WXA présentent un double avantage inédit, à savoir la hiérarchisation du trafic applicatif et la réduction à un minimum du trafic entre les sites, garantissant ainsi des performances réseau optimales.

Pour en savoir plus sur les produits de sécurité réseau SonicWall, rendez-vous sur : www.sonicwall.com/en-us/products.

Services de sécurité réseau et produits complémentaires

Les services et compléments de sécurité réseau des pare-feu 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.

Services et compléments disponibles :

- Offre TotalSecure Advanced : pare-feu plus l'offre Advanced Gateway Security Suite (sandbox multi-moteur, antivirus, anti-logiciels espions, prévention des intrusions, contrôle des applications, filtrage de contenu/Web et support 24x7)
- Offre Advanced Gateway Security Suite : Capture Advanced Threat Protection, Gateway Anti-Virus, antilogiciels espions, prévention des intrusions, filtrage de contenu/Web et support 24x7
- Gateway Security Services : Gateway Anti-Virus, anti-logiciels espions, prévention des intrusions et contrôle des applications
- Capture Advanced Threat Protection (ATP)
- Services de filtrage de contenu
- Antivirus et anti-logiciels espions client appliqués
- Service anti-spam complet
- Inspection approfondie des paquets du trafic chiffré TLS/SSL (DPI-SSL)
- Surveillance et contrôle des applications
- Système de prévention des intrusions (IPS)

Pour en **savoir plus** sur les services et compléments de sécurité réseau, consultez la page : www.sonicwall.com/en-us/products/firewalls/security-services.

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.

SONICWALL®

Cloud App Security

Cloud App Security

La solution SonicWall Cloud App Security fournit une sécurité de nouvelle génération pour les applications SaaS, comme Office 365 et G Suite, en protégeant les e-mails, données et identifiants de connexion des utilisateurs des menaces avancées, tout en garantissant la conformité dans le Cloud. Si vous migrez dans le Cloud, SonicWall fournit la meilleure sécurité basée sur les API de sa catégorie avec un faible coût total de possession, des dépenses minimes pour le déploiement et une expérience utilisateur fluide.

Une sécurité de nouvelle génération pour la messagerie électronique dans le Cloud

En plus des couches de sécurité traditionnelles des messageries électroniques des vérifications SPF, DKIM et DMARC, ainsi que du filtrage des URL en exploitant trois principales sources de données pour les listes noires des URL, l'architecture unique de la solution Cloud App Security fournit une protection qui est impossible pour une solution passerelle externe :

1. **Ajoute une couche de protection contre les menaces avancées :** la solution Cloud App Security bloque les messages d'hameçonnage ayant réussi à passer malgré Office 365 et G Suite. La solution exploite l'apprentissage automatique, l'intelligence artificielle et l'analyse du Big Data pour fournir une capacité puissante anti-hameçonnage, une technologie sandbox des pièces jointes et une analyse des URL au moment du clic, ainsi qu'une protection contre l'usurpation de l'identité.
2. **Surveille les messages électroniques entrants, sortants et internes :** l'intégration SaaS de la solution Cloud App Security peut scanner et mettre en quarantaine chaque e-mail avant qu'il n'atteigne la boîte de réception d'un utilisateur, qu'il provienne de l'extérieur de l'entreprise ou d'un compte interne compromis.
3. **Scanne l'historique des messages pour détecter d'éventuelles menaces :** dès la première connexion, la solution Cloud App Security scanne l'historique des messages (même les comptes fermés) pour détecter d'éventuelles intrusions ou des comptes compromis.
4. Suppression globale d'e-mails : des messages malveillants peuvent être modifiés ou supprimés à tout moment, qu'ils soient malveillants, qu'ils contiennent des informations confidentielles ou après qu'un employé a répondu à tous par inadvertance.

Comme la protection de la messagerie électronique de la solution Cloud App Security est appliquée avant la boîte de la réception, mais après les filtres Microsoft ou Google natifs (ainsi que n'importe quelle passerelle MTA externe pouvant être déployée), ses algorithmes d'apprentissage automatique sont adaptés de manière unique pour identifier les menaces qui ont pu être ratées. Cloud App Security est également capable d'intégrer les résultats des scans natifs dans ses propres algorithmes de détection.

Sécurité nouvelle génération pour la suite complète de productivité

Cloud App Security offre une sécurité complète de défense en profondeur pour Office 365 ou G Suite. Que vous utilisiez une messagerie électronique, des lecteurs partagés, des messageries instantanées ou l'environnement de pleine collaboration, la solution vous aide à réaliser les actions de sécurité suivantes :

1. Éviter la propagation du hameçonnage et des logiciels malveillants au sein de votre organisation ou jusqu'à vos clients et partenaires.
2. Vérifier chaque fichier pour détecter un éventuel contenu malveillant en utilisant la technologie sandbox de Capture ATP et une analyse de contenu actif pour mettre en quarantaine les menaces avant qu'elles ne soient téléchargées par vos utilisateurs.
3. Identifier les informations confidentielles et appliquer les règles compatibles au Cloud qui les contiennent au sein de l'organisation ou d'un groupe de travail. Vos utilisateurs peuvent exploiter tout le potentiel de la suite de productivité basée dans le Cloud, tandis que les flux de travail automatisés garantissent la conformité réglementaire, s'assurant que les données PCI, HIPAA, DCP ou les autres données confidentielles ne sont pas partagées en externe.

Sécurité informatique autorisée

La solution SonicWall Cloud App Security analyse tout le trafic (par ex., événements des journaux de bord, activités des utilisateurs, fichiers et objets de données, état de configuration, etc.) et applique les politiques de sécurité nécessaires via des intégrations directes avec des API natives du service dans le Cloud. Comme la solution exploite les API natives, la solution n'utilise pas de proxy et ne se trouve pas entre l'utilisateur et le Cloud. Cela permet à la solution de fournir une protection pour les applications autorisées, quel que soit le dispositif ou le réseau de l'utilisateur. De plus, l'approche basée sur les API permet un déploiement facile et un contrôle granulaire, sans aucun impact sur l'expérience utilisateur.

Visibilité et contrôle du « shadow IT »

Les pare-feu de nouvelle génération SonicWall analysent et consignent l'ensemble du trafic qui entre et sort du réseau. Les journaux générés pour les données du trafic sortant ne distinguent pas clairement les applications Cloud utilisées et ne proposent pas de score de risque pour chaque application utilisée par les employés. Pour les employés nomades redirigés via un pare-feu de nouvelle génération avec VPN, la solution recueille à partir de ces journaux des détails supplémentaires sur les mesures que prennent les utilisateurs dans les services Cloud. Cloud App Security traite les fichiers journaux des pare-feu de nouvelle génération SonicWall et révèle les services Cloud en cours d'utilisation, identifient leurs utilisateurs, les volumes de données téléchargées depuis et vers le Cloud ainsi que le risque et la catégorie de chaque service Cloud. Avec Cloud App Security, l'infrastructure existante devient compatible Cloud. Tandis que les employés utilisent de plus en plus les applications Cloud dans un cadre professionnel, Cloud App Security permet aux administrateurs de détecter les lacunes dans la stratégie de sécurité, de classer les applications Cloud dans les catégories autorisées/interdites et d'appliquer des règles d'accès pour bloquer les applications à risque. Cloud App Security constitue une part essentielle de la vision de SonicWall consistant à fournir des capacités de détection et de prévention automatisées en temps réel des intrusions pour les clients lorsqu'ils adoptent les technologies dans le Cloud.

Pour **en savoir plus** sur SonicWall Cloud App Security, rendez-vous sur : www.sonicwall.com/casb.

Produits de sécurité pour l'accès à distance

SonicWall SMA est une passerelle d'accès sécurisé unifiée, destinée aux entreprises confrontées aux thématiques de la mobilité, du BYOD et de la migration vers le Cloud. Cette solution leur permet de fournir un accès aux ressources vitales, quel que soit 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. SMA fournit une sécurité optimale pour réduire les menaces de surface, tout en rendant les organisations plus sécurisées en prenant en charge les derniers algorithmes et codes de chiffrement. La solution SMA de SonicWall fournit une sécurité de pointe permettant de réduire à un minimum les menaces en surface. 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 multifacteurs (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 des centaines de milliers 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

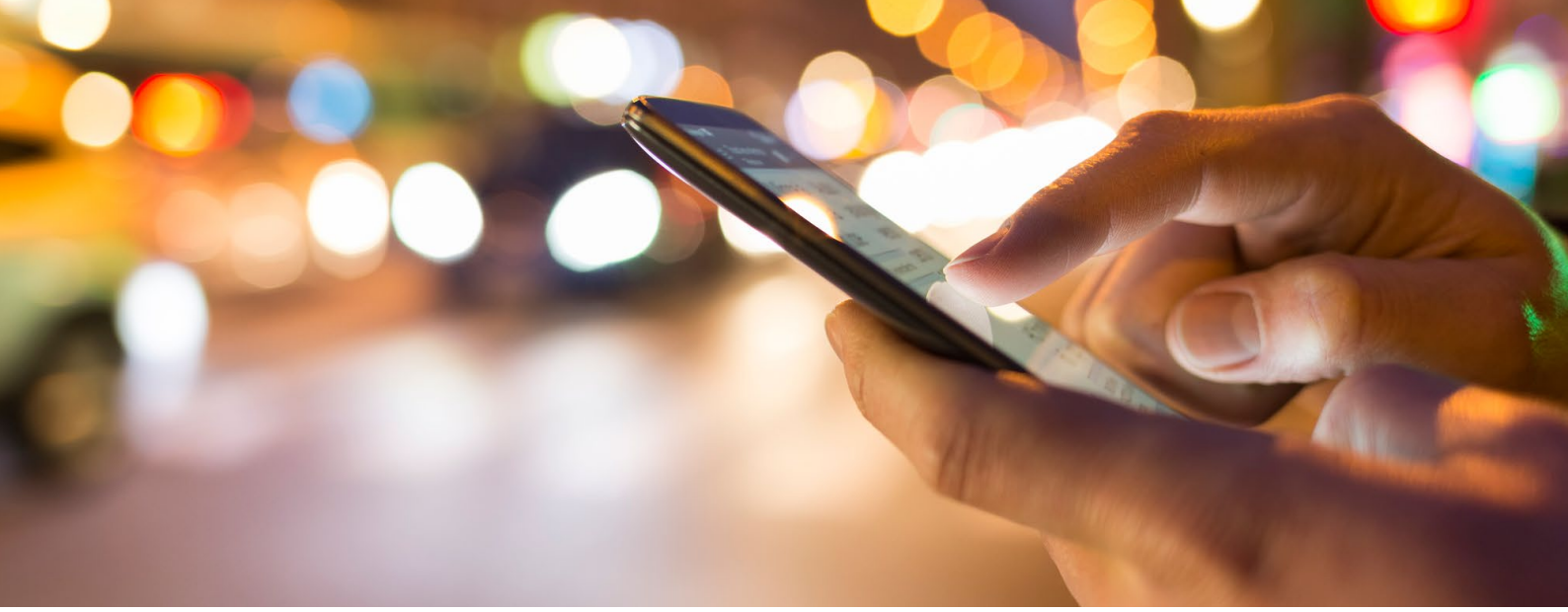
La solution SonicWall SMA peut être déployée sous la forme d'une appliance hautes performances renforcée ou d'une appliance virtuelle s'appuyant sur les ressources informatiques partagées pour optimiser l'utilisation, faciliter la migration et réduire les coûts d'investissement. Les appliances matérielles 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, comme Hyper-V et VMware. 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.

Gestion et reporting

SonicWall propose une plateforme de gestion Web intuitive qui simplifie la gestion des appliances tout en fournissant un vaste éventail de fonctionnalités de reporting. 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 règle gère 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, rendez-vous sur : https://www.sonicwall.com/fr-fr/products/remote-access/.



Produits de 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.

Par ailleurs, dans un souci de gestion des coûts et des ressources, les entreprises adoptent Microsoft Office 365 et Google G Suite. Les produits Office 365 et G Suite 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 boîtes aux lettres de messagerie. 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 multi-couche assure une protection complète en entrée et en sortie, et se décline en diverses appliances matérielles pouvant accueillir jusqu'à 10 000 utilisateurs par appliance. SonicWall Email Security existe aussi sous forme virtuelle ou logicielle, idéales pour les entreprises en quête de flexibilité et d'agilité. La solution peut être configurée en mode divisé à des fins de haute disponibilité et gérée de manière centralisée et fiable pour 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 des URL au moment du clic 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 comme SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) et DMARC (Domain-based Message Authentication, Reporting & Conformance) permettant de bloquer les attaques de spoofing et les messages frauduleux.

- 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
- Simplifiez la gestion et le reporting
- Flexibilisez les options de déploiement

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.

Service SonicWall Hosted Email Security

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, rendez-vous sur : https://www.sonicwall.com/fr-fr/products/secure-email/cloud-email-security/.

Gestion, reporting et analyse

Pour SonicWall, une approche connectée de la gestion de la sécurité est non seulement 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 forte et uniforme et une stratégie de réponse sur leurs réseaux câblés, sans fil, terminaux, mobiles et multi-cloud. La pleine adoption 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 Global Management System

Déployable sur site en tant que logiciel ou appliance virtuelle, la solution GMS (Global Management System) de SonicWall permet de gérer la sécurité réseau de manière cohérente via des processus métier et des niveaux de service, plutôt que d'adopter une approche cloisonnée, au cas par cas, moins efficace. La solution GMS permet aux structures de toute taille et de tout type de consolider aisément la gestion des appliances de sécurité, de réduire du dépannage et de fédérer tous les aspects opérationnels de l'infrastructure de sécurité. Cela inclut également la centralisation de la gestion et de l'application des règles, la surveillance des événements en temps réel, une analyse des données et un reporting granulaires, des pistes d'audit, le déploiement sans intervention, la configuration SD-WAN, etc., dans une plateforme de gestion unifiée.

La solution GMS répond également aux besoins des entreprises en matière de gestion des modifications de pare-feu via l'automatisation du flux de travail. Ce processus intrinsèque automatisé garantit l'exactitude et la conformité des modifications de règles en appliquant une méthode rigoureuse de configuration, comparaison, validation, vérification et approbation des règles de gestion de la sécurité avant tout déploiement. Les groupes d'approbation sont flexibles, ce qui permet d'adhérer aux règles de sécurité de chaque entreprise et de garantir que les bonnes règles de pare-feu sont déployées au bon moment, conformément aux exigences de conformité.

SonicWall Capture Security Center

Inclus dans la plateforme SonicWall Capture Cloud, Capture Security Center est une plateforme ouverte et évolutive de gestion de la sécurité Cloud, de surveillance, de création de rapports et d'analyse, fournie en tant que solution SaaS (Software-as-a-Service). Elle est conçue pour différentes tailles de structures et différents cas d'utilisation, qu'il s'agisse d'entreprises distribuées ou de fournisseurs de services qui adoptent le Cloud computing pour des raisons de rentabilité. Capture Security Center est une plateforme idéale de gestion de la sécurité Cloud qui permet d'établir une sécurité durable et parfaitement coordonnée sur les réseaux.

Pour les clients, Capture Security Center offre une visibilité, une agilité et une capacité optimales permettant de contrôler l'ensemble de l'écosystème de sécurité réseau SonicWall, avec davantage de clarté, de précision et de rapidité, le tout de manière centralisée, quel que soit l'emplacement concerné. Grâce à une vision de l'environnement de sécurité à l'échelle de l'entreprise et une surveillance de la sécurité ciblée, en temps réel, il est possible d'établir des règles de sécurité précises et de prendre des décisions adéquates en termes de contrôle, pour une sécurité renforcée.

Pour les fournisseurs de services, Capture Security Center simplifie la gestion discrète des opérations de sécurité de nombreux clients. Les MSP/MSSP peuvent ainsi proposer des services de sécurité plus flexibles, tout en réduisant les dépenses d'exploitation et les difficultés liées à la maintenance d'une infrastructure dont ils seraient les seuls propriétaires.

SonicWall Analytics

Au-delà des questions de gestion de la sécurité et de reporting, SonicWall Analytics fournit une vue plongeante sur tout ce qui survient au sein de l'environnement de sécurité réseau. Son puissant moteur d'analyse décisionnel orienté automatise l'agrégation, la normalisation et la contextualisation des données de sécurité qui transitent par tous les pare-feu SonicWall. Le tableau de bord offre une visibilité centralisée, le contrôle et la flexibilité nécessaires pour effectuer des analyses approfondies pour investigation et forensique.

L'analyse présente les données de sécurité sous une forme pertinente, actionnable et facilement consommable que les acteurs concernés peuvent interpréter, classer par priorités, utiliser comme base pour prendre leurs décisions et les mesures de défense appropriées. Cette connaissance et cette compréhension approfondies de l'environnement de sécurité permettent de disposer d'une visibilité complète et de toutes les capacités nécessaires pour identifier mais aussi orchestrer les mesures de correction adaptées aux risques de sécurité, ainsi que de surveiller et suivre les résultats avec davantage de clarté, de certitude et de rapidité. 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.

Analytics est optimisée à la fois pour les cas d'utilisation de déploiement dans le Cloud et sur site. La solution peut donner lieu à l'octroi d'une licence d'un logiciel en tant que service (SaaS) économique via le Capture Security Center, en tant qu'appliance virtuelle dans des environnements de Cloud privés basés sur VMWare ou sur Microsoft Hyper-V ou dans des environnements de Cloud publics basés sur AWS ou Microsoft Azure. Même si cela donne aux organisations les avantages opérationnels et économiques de la virtualisation et de l'informatique dans le Cloud, cela permet également une amélioration dynamique du stockage pour répondre aux exigences croissantes de conservation des données depuis un nombre virtuellement illimité de nœuds de pare-feu.

Pour **en savoir plus** sur les produits de gestion et de reporting SonicWall, rendez-vous sur : [www.sonicwall.com/en-us/products/firewalls/management-and-reporting.](www.sonicwall.com/en-us/products/firewalls/management-and-reporting)

SONICWALL®

Services SonicWall pour les grandes entreprises

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 8 h à 17 h 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.
- **Mise en œuvre / 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/SRA/SMA/Email Security/GMS.

Pour en savoir plus : https://support.software.com/essentials/support-offerings.

Conclusion

Découvrez les produits de sécurité SonicWall

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

RSA SECURED

Connect+Wise CERTIFIED Partner

À propos de SonicWall

Depuis plus de 27 ans, SonicWall lutte contre la cybercriminalité pour défendre les PME, les grandes entreprises et les agences gouvernementales du monde entier. S'appuyant sur les travaux de recherche des Capture Labs de SonicWall, nos solutions primées de détection et de prévention des intrusions en temps réel sécurisent plus d'un million de réseaux et leurs e-mails, applications et données dans plus de 215 pays et territoires. Ces entreprises peuvent ainsi fonctionner plus efficacement sans crainte pour leur sécurité. Pour en savoir plus, rendez-vous sur www.sonicwall.com ou suivez-nous sur Twitter, LinkedIn, Facebook et Instagram.

Si vous avez la moindre question concernant votre utilisation potentielle du présent contenu, merci de contacter :

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Veuillez consulter notre site Web pour obtenir des informations complémentaires.
www.sonicwall.com