Gamme des produits SonicWall : Aperçu

Pare-feu de nouvelle génération

Haut de gamme : Série NS*sp*

Pare-feu multi-instances conçu pour les grandes entreprises distribuées, les centres de données et les fournisseurs de services gérés (MSSP), offrant une protection haute vitesse, une densité de ports élevée et une véritable isolation des locataires grâce à une politique unifiée

Milieu de gamme : Série NS*a*

Efficacité et performance de sécurité validées par l'industrie pour les réseaux, les succursales et les entreprises décentralisées de taille moyenne.

Entrée de gamme : Série TZ

Prévention intégrée des menaces et plateforme SD-WAN pour les déploiements dans les maisons, les petites/moyennes organisations et SD-Branch

Virtuel : Série NSv

Pare-feu virtuels avec modèles de licences flexibles pour protéger tous les composants stratégiques de votre infrastructure cloud publique et privée.

Sécurité sans fil

Série SonicWave

Sécurité et performances intégrées pour la prochaine vague d'appareils sans fil, gérés par le cloud ou le pare-feu.

Série SMA

Accès simple et sécurisé sur la base de règles aux ressources réseau et cloud.

SonicWall Switch

Fournit une commutation intelligente pour la connectivité sécurisée de nouvelle génération des déploiements PME et SD-Branch.

Sécurisation de messagerie

Série ESA

Solution de protection multicouche contre les menaces évoluées véhiculées par e- mail ; proposée sous forme d'appliance, de MV et de SaaS cloud.

Capture Security appliance (CS*a*)

Test de fichiers et prévention des logiciels malveillants sur site.

Gestion et analyse

Capture Security Center
Global Management System (GMS)
Network Security Manager
WIreless Network Manager

Le pouvoir entre vos mains grâce au contrôle et à la connaissance de votre réseau.

Capture Client

Plateforme client unifiée avec un tableau de bord global fournissant diverses fonctionnalités de protection des terminaux, dont une protection anti-logiciels malveillants avancée, la technologie sandbox, les informations sur la vulnérabilité des applications et la restauration en cas d'infection.

Cloud Edge Secure Access

Une application SaaS puissante qui fournit un network-as-a-service simple pour une connectivité de site à site et hybride vers AWS, Azure et Google Cloud. Dans ce processus, elle combine des approches de sécurité Zero-Trust et Least-Privilege dans une offre intégrée.

Cloud App Security

Une solution native dans le cloud qui fournit une sécurité de nouvelle génération pour les applications SaaS, comme Office 365 et G Suite, afin de protéger les e-mails, données et identifiants de connexion des utilisateurs contre les menaces avancées, tout en garantissant la conformité dans le Cloud.

Services d'abonnement aux pare-feu de nouvelle génération

La suite Threat Protection Service inclut des services de sécurité de base afin de garantir que le réseau est protégé contre les menaces dans une offre économique. Disponible uniquement sur les séries TZ270/370/470, cette offre inclut l'antivirus Gateway, la prévention des intrusions et le contrôle des applications, le service de filtre des contenus, la visibilité du réseau et une assistance 24 heures sur 24, 7 jours sur 7.

La suite de services de protection essentiels fournit tous les services de sécurité essentiels nécessaires pour se protéger contre les menaces connues et inconnues. Elle comprend Capture Advanced Threat Protection avec la technologie RTDMI, Gateway Anti-Virus, la prévention des intrusions et le contrôle des applications, Content Filtering Service, le service antispam complet, la visibilité du réseau et une assistance 24 h/24 et 7 j/7.

Advanced Protection Services Suite fournit une sécurité avancée au réseau. Cette offre inclut les services de l'offre de services essentiels avec la gestion du cloud et le reporting sur le cloud pendant 7 jours.

Advanced Gateway Security Suite (AGSS) est disponible en tant que service complémentaire pour tous les pare-feu physiques et virtuels de SonicWall, afin d'assurer une protection contre les menaces les plus avancées et les menaces inconnues.

Compris dans la suite AGSS (Advanced Gateway Security Suite) ; associés au pare-feu de nouvelle génération dans TotalSecure Advanced Edition

- Capture Advanced Threat Protection (ATP), service de sandboxing cloud multimoteur
- Antivirus et anti-logiciels espions de passerelle
- Intrusion Prevention Service
- Contrôle des applications
- Service de filtrage de contenu/Web
- Support 24 h/24, 7 j/7

Security-as-a-Service (SECaaS)

Externalisez la sécurité de votre réseau avec notre solution clés en main.

Pour en savoir plus, rendez-vous sur sonicwall.com

Questions d'évaluation

Pare-feu de nouvelle génération

- Pouvez-vous suivre le rythme de l'augmentation de la bande passante entraînant des besoins de performance en gigabits ou en multi-gigabits ?
- Votre pare-feu actuel est-il capable d'inspecter les menaces à mesure qu'elles entrent dans le système ?
- Quels sont vos critères en matière d'exigences de performance ?
- Nombre total d'utilisateurs/réseaux derrière le pare-feu ?
- Nombre total de sessions/connexions aux heures de pointe ?
- Combien de sites et d'utilisateurs distants se connecteront au pare-feu ?
- Comment mesurez-vous l'efficacité de vos contrôles de sécurité ?
- De quel type de connexion Internet disposez-vous ? Quelle en est la vitesse ?
- Que faites-vous pour vous protéger contre les nouvelles menaces telles que les attaques « zero day » ?
- Votre sandbox peut-elle détecter et bloquer des menaces cachées dans la mémoire profonde ?
- Combien de moteurs se trouvent dans votre sandbox ?
- Votre sandbox peut-elle retenir les fichiers à la passerelle, avant de les laisser passer ?
- Savez-vous si le pare-feu de votre entreprise inspecte le trafic HTTPS ?
- Avez-vous subi des perturbations des services réseau ou une interruption de service due à l'inspection du trafic HTTPS ?
- Votre pare-feu virtuel est-il aussi robuste que votre pare-feu physique ?
- Comment sécurisez-vous vos environnements cloud publics ou privés ?
- Êtes-vous en mesure de mettre en place des zones de sécurité adéquates et une microsegmentation sur votre réseau virtuel ?
- Disposez-vous d'une visibilité et d'un contrôle complets de votre trafic virtuel ?
- Cela vous intéresse-t-il de réduire vos coûts en remplaçant le MPLS par le SD-WAN pour sécuriser votre réseau privé ?

Capture Client

- Vos terminaux ont-ils besoin d'une protection évoluée et uniforme contre les ransomwares et les menaces chiffrées ?
- Avec quel degré de facilité parvenez-vous à établir la conformité aux règles et la gestion des licences sur l'ensemble des terminaux ?
- Avez-vous des problèmes pour visualiser les terminaux et pour gérer votre stratégie de sécurité ?
- Votre solution de sécurité des terminaux se connecte-t-elle à un environnement de sandbox ?
- Pouvez-vous cataloguer les applications installées sur les terminaux et savoir combien de vulnérabilités elles contiennent ?
- Votre solution actuelle surveille-t-elle en continu l'intégrité de votre système ?
- Pouvez-vous annuler les dommages causés par un ransomware en restaurant l'appareil au dernier état sain connu ?
- À quelle vitesse pouvez-vous ajouter ou modifier des politiques pour les locataires ?

Cloud App Security

- Utilisez-vous O365 ou G Suite ?
- Utilisez-vous Proofpoint ou Mimecast pour sécuriser la suite O365/G Suite ?
- Analysez-vous les e-mails internes O365 ?
- Combien d'applications SaaS autorisées votre organisation utilise-t-elle ?
- Avez-vous des difficultés à garantir la conformité des données stockées dans les applications SaaS ?
- Comment saurez-vous si les identifiants de connexion de vos utilisateurs sont compromis ?
- Avez-vous une visibilité sur les informations suivantes : qui accède aux données, d'où et quand ? (BYOD – utilisation de votre propre équipement)

Inspecter la mémoire en profondeur

Le moteur SonicWall Real-Time Deep Memory Inspection (RTDMI™), une technologie en instance de brevet, détecte et bloque proactivement les logiciels malveillants de masse encore inconnus via une inspection approfondie de la mémoire en temps réel. Désormais disponible avec le service de sandbox cloud SonicWall Capture Advanced Threat Protection (ATP), ce moteur identifie et élimine les menaces modernes les plus insidieuses, y compris les futurs exploits de type Meltdown.

Série SonicWave

- Vos employés/partenaires/clients se plaignent-ils de la lenteur des performances Wi-Fi ?
- Quel pourrait être le nombre maximum de vos utilisateurs sans fil à un moment donné ?
- Vous préoccupez-vous de ce que coûterait l'ajout d'une solution de sécurité sans fil à votre réseau ?
- Que savez-vous de la norme sans fil 802.11ac Wave 2 ?
- Avez-vous besoin de flexibilité pour gérer les points d'accès : gestion cloud vs gestion pare-feu ?
- Avez-vous planifié efficacement votre réseau WiFi ?
- Auriez-vous besoin que les PA se déconnectent des pare-feu ?
- Vous souciez-vous de fournir des fonctionnalités de sécurité avancées sur votre réseau WiFi ?
- Les services pour les invités sont-ils importants pour vous ?
- Aurez-vous besoin d'un portail de connexion personnalisé des invités pour leur intégration ?

SonicWall Switch

- Avez-vous besoin de switches d'accès gigabits pour alimenter des appareils compatibles PoE ?
- Une stratégie de sécurité unifiée avec une visibilité et une gestion unifiées est-elle importante pour vous ?
- Êtes-vous confronté à des problèmes de solution avec les switches tiers qui fonctionnent avec l'écosystème SonicWall ?

Accès mobile sécurisé

- Quelle est votre stratégie actuelle d'accès à distance des employés ?
- Que pensez-vous de l'utilisation d'une approche d'accès au réseau zero-trust ?
- Comment fournissez-vous aux utilisateurs un accès sécurisé aux ressources et applications de l'entreprise hébergées sur site et dans le cloud ?
- Avez-vous une bonne visibilité de chaque utilisateur et appareil accédant à votre réseau ?
- Protégez-vous actuellement vos ressources et serveurs Web stratégiques ?

Sécurité de la messagerie

- Êtes-vous préoccupé par les menaces évoluées véhiculées par le courrier électronique : ransomwares, spear-phishing ou encore les menaces de type BEC (Business Email Compromise) ?
- Votre solution de sécurisation de messagerie actuelle offre-t-elle des fonctionnalités de protection avancée contre les menaces ?
- Êtes-vous préoccupé par la fuite éventuelle d'informations confidentielles dans les messages électroniques ?
- Comment faites-vous pour être en conformité avec les réglementations de type RGPD, Sarbanes-Oxley, GLBA ou HIPAA ?
- Envisagez-vous de proposer des services de sécurisation de messagerie gérés à vos clients ? (MSSP)

Gestion et analyse

- Quels problèmes pourriez-vous résoudre en unifiant vos solutions de sécurité sur une même plateforme de gestion commune avec écran unique ?
- Quels avantages opérationnels obtiendrez-vous si vous pouvez gérer de manière centralisée tous vos pare-feu, points d'accès et switches depuis n'importe quel emplacement à l'aide d'une console cloud unique ?
- Dans quelle mesure êtes-vous sûr de pouvoir prouver votre conformité avec les exigences de cybersécurité de type PCI, HIPAA et le RGPD ?
- Dans quelle mesure vos conditions de sécurité changeraient-elles si vous pouviez mieux détecter les menaces et les risques et y répondre rapidement et précisément ?
- Que gagneriez-vous et votre équipe dirigeante à disposer d'une visibilité totale des cybermenaces et des risques encourus par votre entreprise ?

Cloud Edge Secure Access

- Avez-vous beaucoup de données sensibles ? Êtes-vous préoccupé par les utilisateurs ayant des privilèges excessifs ?
- Êtes-vous préoccupé par les réglementations croissantes en matière de protection des données et de sécurité des informations ?
- Avez-vous besoin de contrôler les interactions entre les employés, les partenaires commerciaux externes et les ressources sensibles ?
- Combien de succursales avez-vous ? Avec quelle efficacité pouvez-vous intégrer une nouvelle succursale ?
- Combien de temps vous faut-il pour intégrer en toute sécurité un utilisateur à distance ?

Datasheet-SonicWallProductLineAtAGlance-A4-VG-4116

SONICWALL®