GAMME DES PRODUITS SONICWALL : APERÇU

Pare-feu de nouvelle génération

Haut de gamme : NS*sp* 12000
Série NS*sp* 12800/12400
Une sécurité évolutive et de pointe pour les grandes entreprises décentralisées, les centres de données et les prestataires de services qui exploitent la puissance de l'intelligence du cloud

Moyen de gamme : Série NS*a*
NS*a* 9650/9450/9250/ 6650/5650/4650/3650/2650
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
TZ600/TZ500/TZ400/TZ350/ TZ300/ SOHO 250/SOHO
Prévention intégrée des menaces et plateforme SD-WAN pour les petites/ moyennes organisations et entreprises décentralisées

Virtuel : Série NS*v*
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
SonicWave 432e/432i/432o/ 231c/224w/231o
Sécurité et performances intégrées pour la prochaine vague d'appareils sans fil, gérés par le cloud ou le pare-feu

Accès mobile sécurisé

Série SMA SMA
EX9000/8200v/7200/ 6200/500v/400/200
Accès simple et sécurisé sur la base de règles aux ressources réseau et cloud

Sécurisation de messagerie

ESA 9000/7000/5000/
Logiciel MV/Service dans le Cloud
Solution de protection multicouche contre les menaces évoluées véhiculées par e-mail

Gestion et analyse

Capture Security Center
Global Management System (GMS)
Analytics
Le pouvoir entre vos mains grâce au contrôle et à la connaissance de votre réseau

Série Accélération WAN

WXA 6000 (logiciel)
WXA 5000 (machine virtuelle)/ 500 (logiciel)
Amélioration sensible des performances de transfert de vos applications et productivité accrue de vos employés

Capture Client

Plateforme client unifiée fournissant diverses fonctionnalités de protection des terminaux, dont une protection anti-malware avancée, la technologie sandbox, le contrôle des appareils et la restauration en cas d'infection

Web Application Firewall (WAF)

Sécurité des applications Web, prévention des fuites de données et conformité réglementaire, en local ou dans le cloud

Cloud App Security

Une solution CASB 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

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

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.

Pour en savoir plus, rendez-vous sur : www.sonicwall.com/fr-fr/products

Questions d'évaluation

Pare-feu de nouvelle génération

- Comment mesurez-vous l'efficacité de vos contrôles de sécurité ?
- Quel est votre plan de correction en cas d'identification de brèches de sécurité ?
- Comment réduisez-vous le risque d'applications Web vulnérables auxquelles vos utilisateurs peuvent accéder ?
- De quel type de connexion Internet disposez-vous ? Quelle en est la vitesse ?
- Devez-vous sacrifier les performances pour bénéficier d'une meilleure sécurité sur votre réseau ?
- Que faites-vous pour vous protéger contre les nouvelles menaces telles que les attaques « zero day » ?
- Dans quelle mesure votre équipe est-elle capable de corriger des vulnérabilités dans les 12 heures suivant la publication d'un patch ?
- 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 que la plupart des sessions Internet sont chiffrées, et si votre pare-feu est en mesure de les déchiffrer pour les examiner ?
- 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 ?
- Votre pare-feu actuel intègre-t-il le PoE/PoE+ ou avez-vous besoin d'un commutateur pour alimenter les appareils compatibles PoE ?
- Cela vous intéresse-t-il de réduire vos coûts en remplaçant le MPLS par le SD-WAN pour sécuriser votre réseau privé ?
- Souhaitez-vous avoir un modèle de licence par abonnement pour vos pare-feu virtuels ?

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 à visualiser les terminaux et à gérer votre stratégie de sécurité ?
- Votre solution de sécurité des terminaux se connecte-t-elle à un environnement de sandbox ?
- 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 ?
- Avez-vous la possibilité de bloquer la connexion des appareils inconnus et potentiellement infectés aux terminaux ?

Web Application Firewall

- Protégez-vous actuellement vos ressources et serveurs Web stratégiques ?
- Quelles mesures avez-vous prises pour être en conformité avec les exigences de sécurité PCI ?

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)

Sécurité sans fil

- Vos employés/partenaires/clients se plaignent-ils de la lenteur des performances WiFi ?
- 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 ?

Accès mobile sécurisé

- Votre entreprise est-elle en train de migrer ses applications métiers et ses ressources vers le cloud ou envisage-t-elle de le faire ?
- Fournissez-vous une authentification unique unifiée pour les applications sur site et dans le cloud à vos utilisateurs ?
- Vos employés utilisent-ils Dropbox ou leur messagerie personnelle pour partager des fichiers ?
- Vos employés sont-ils obligés de gérer plusieurs URL et mots de passe ?
- Quelle est votre stratégie actuelle en matière de mobilité/BYOD ?
- Avez-vous une bonne visibilité de chaque appareil qui accède à votre réseau ?

Sécurisation de messagerie

- Êtes-vous préoccupé par les menaces évoluées véhiculées par le courrier électronique : ransomwares, spear-phishing ou encore les menaces du 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 du 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 ?
- À quels défis économiques et opérationnels êtes-vous confronté lors de la gestion de votre infrastructure de sécurité ?
- Dans quelle mesure êtes-vous sûr de pouvoir prouver votre conformité avec les exigences de cybersécurité du 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 ?

Accélération WAN

- Votre entreprise compte-t-elle plusieurs bureaux distants ? Combien ?
- Ces bureaux sont-ils connectés au réseau par VPN ou par un circuit WAN propre (MPLS) ?
- Vos employés utilisent-ils des applications de type Microsoft Windows File Sharing, SharePoint, Office ou FTP ?
- Souhaitez-vous réduire les coûts et la consommation de bande passante sans avoir à payer pour augmenter la capacité ?

Pour en savoir plus, rendez-vous sur : www.sonicwall.com/fr-fr/products

Datasheet-SonicWallProductLineAtAGlance-US-VG-MKTG5159

SONICWALL®