Plateforme SonicOS

L'architecture SonicOS est au cœur de tous les pare-feux physiques et virtuels SonicWall, notamment TZ, NS*a*, NS*v* et SuperMassive Series. SonicOS repose sur notre technologie RFDPI (Reassembly-Free Deep Packet Inspection®) « single pass » brevetée* à faible latence ainsi que notre technologie RTDMI (Real-Time Deep Memory Inspection™) en instance de brevet, qui lui permettent d'assurer une sécurité haute efficacité reconnue par le secteur, le SD-WAN, une visualisation en temps réel, des réseaux privés virtuels (VPN) haut débit et autres puissantes fonctionnalités de sécurité.

Fonctionnalités des pare-feux

Moteur RFDPI (Reassembly-Free Deep Packet Inspection)	
Fonctionnalité	Description
Filtrage RFDPI (Reassembly-Free Deep Packet Inspection)	Ce moteur d'inspection hautes performances, propriétaire et breveté effectue des analyses bidirectionnelles des flux de trafic, sans proxy ni mise en mémoire tampon, pour détecter les tentatives d'intrusion, les logiciels malveillants et le trafic des applications indépendamment du port.
Inspection bidirectionnelle	Le trafic entrant et sortant est analysé simultanément pour garantir que le réseau n'est pas utilisé pour distribuer des logiciels malveillants ou lancer des attaques en cas d'intrusion d'une machine infectée.
Inspection basée sur les flux	Cette technologie d'inspection sans proxy et sans mise en mémoire tampon offre des performances à ultra faible latence pour l'inspection DPI de millions de flux réseau simultanés, sans limite de taille des flux et des fichiers. Elle peut en outre être appliquée à des protocoles courants, ainsi qu'aux flux TCP bruts.
Hautement parallèle et extensible	La conception unique du moteur RFDPI fonctionne de concert avec l'architecture multicœurs pour fournir un haut débit DPI et des taux d'établissement de nouvelles sessions extrêmement élevés afin de gérer les pics de trafic sur les réseaux exigeants.
Inspection en un seul passage	L'architecture DPI en un seul passage analyse simultanément le trafic pour identifier les logiciels malveillants, les intrusions et les applications, ce qui réduit considérablement la latence DPI et garantit que toutes les informations sur les menaces sont corrélées au sein d'une architecture unique.
Pare-feu et gestion de réseau	
Fonctionnalité	Description
SD-WAN sécurisé	Plus économique que les technologies telles que MPLS, le SD-WAN sécurisé permet aux entreprises distribuées de mettre en place, de gérer et d'exploiter en toute sécurité des réseaux hautes performances sur des sites distants, et de partager ainsi des données, des applications et des services par le biais de services Internet publics à faible coût et facilement accessibles.
API REST	Permet au pare-feu de recevoir tout type de flux de renseignements propriétaires, d'OEM ou de fournisseurs tiers et de les exploiter pour combattre les menaces évoluées : zero-day, initié malveillant, identifiants compromis, ransomwares et menaces persistantes avancées.
Inspection stateful des paquets	Tout le trafic réseau est inspecté, analysé et mis en conformité avec les règles d'accès du pare-feu.
Mise en cluster/haute disponibilité	Prise en charge des modes hautes disponibilité actif/passif (A/P) avec synchronisation de l'état, DPI[2] actif/actif (A/A) et mise en cluster active/active.[2] Le mode DPI actif/actif permet de décharger la charge DPI vers une appliance passive pour optimiser le débit.
Protection contre les attaques DDoS/DoS	La protection contre les inondations SYN permet de contrer les attaques DOS à l'aide des technologies de liste noire SYN de couche 2 et de proxy SYN de couche 3. Par ailleurs, elle offre la possibilité de se prémunir contre les attaques DOS/DDoS via la protection contre les inondations UDP/ICMP et la limitation du débit de connexion.
Options de déploiement flexibles	Le pare-feu peut être déployé en mode filaire, TAP réseau, NAT ou pont couche 2[2].
Équilibrage de charge WAN	Équilibre la charge de plusieurs interfaces WAN à l'aide des méthodes Round Robin, Spillover ou Percentage. Le routage à base de règles crée des routes basées sur des protocoles pour diriger le trafic vers une connexion WAN préférée avec la possibilité de basculer vers un WAN secondaire en cas de panne.
Qualité de service avancée (QoS)	Protège les communications critiques avec le marquage 802.1p et DSCP, ainsi que le remappage du trafic VoIP sur le réseau.
Prise en charge des proxys SIP et des contrôleurs d'accès H.323	Bloque les appels indésirables en exigeant que tous les appels entrants soient autorisés et authentifiés par un contrôleur d'accès H.323 ou un proxy SIP.

Pare-feu et gestion de réseau (suite)	
Fonctionnalité	Description
Gestion des commutateurs Dell série N et série X uniques et en cascade[2]	Gérez les paramètres de sécurité de ports supplémentaires, notamment les ports Portshield, HA, PoE et PoE+, sur un seul écran, via le tableau de bord de gestion des pare-feux pour les commutateurs réseau Dell série N ou série X.
Authentification biométrique	Prend en charge les modes d'authentification d'appareils mobiles, comme la reconnaissance d'empreinte digitale, difficiles à dupliquer ou à partager, en vue de déterminer en toute sécurité l'identité de l'utilisateur pour l'accès au réseau.
Authentification ouverte et social login	Permet aux utilisateurs invités d'utiliser leur identifiant des services de réseaux sociaux comme Facebook, Twitter ou Google+ pour se connecter et accéder à Internet et à d'autres services invités par le biais de zones sans fil, LAN ou DMZ d'un hôte en utilisant l'authentification directe.
Authentification multi-domaines	Constitue un moyen simple et rapide d'administrer les règles de sécurité sur tous les domaines du réseau. Gère une règle individuelle pour un seul domaine ou un groupe de domaines.
Gestion et création de rapports	
Fonctionnalité	Description
Gestion dans le cloud et sur site	La configuration et la gestion des appliances SonicWall peut se faire dans le cloud via le SonicWall Capture Security Center ou sur site avec SonicWall Global Management System (GMS).
Gestion puissante avec un seul appareil	L'interface Web intuitive offre une interface de ligne de commande complète, prend en charge le protocole SNMPv2/3 et permet une configuration rapide et pratique.
Rapports sur les flux applicatifs IPFIX/NetFlow	Exporte des analyses du trafic applicatif et des données d'utilisation via les protocoles IPFIX ou NetFlow pour offrir une surveillance et des rapports historiques et en temps réel sur SonicWall Analytics ou d'autres outils prenant en charge IPFIX et NetFlow via des extensions.
Réseau privé virtuel (VPN)	
Fonctionnalité	Description
Configuration automatique du VPN	Simplifie sensiblement le déploiement de pare-feux distribués en automatisant la configuration initiale de la passerelle VPN site à site entre les pare-feux SonicWall. Sécurité et connectivité se mettent en place instantanément et automatiquement.
VPN IPSec pour la connectivité site à site	Le VPN IPSec hautes performances permet au pare-feu de servir de concentrateur VPN pour des milliers d'autres bureaux à domicile, succursales ou sites de grande taille.
Accès client à distance IPSec ou VPN SSL	Utilise la technologie VPN SSL sans client ou un client IPSec facile à gérer pour accéder simplement à la messagerie électronique, aux fichiers, ordinateurs, pages intranet et applications depuis un vaste éventail de plateformes.
Passerelle VPN redondante	Si plusieurs WAN sont utilisés, un VPN principal et un VPN secondaire peuvent être configurés pour permettre un basculement automatique fluide et la restauration de toutes les sessions VPN.
VPN basé sur le routage	La possibilité d'effectuer un routage dynamique sur des liens VPN garantit une disponibilité continue en cas de panne temporaire d'un tunnel VPN via la redirection fluide du trafic entre les points de terminaison sur des routes alternatives.
Indicateur de contexte/contenu	
Fonctionnalité	Description
Suivi de l'activité des utilisateurs	Fournit les données d'identification et d'activité des utilisateurs grâce à l'intégration transparente des services SSO AD/LDAP/Citrix/Terminal Services associée aux nombreuses informations obtenues par l'inspection approfondie des paquets.
Identification du trafic par pays GeoIP	Identifie et contrôle le trafic réseau en direction ou provenant de pays spécifiques pour contrer les attaques liées à une activité d'origine suspecte ou connue ou pour faire des recherches sur le trafic suspect provenant du réseau. Permet de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP. Supprime le filtrage indésirable des adresses IP dû à une classification erronée.
Détection des expressions régulières et filtrage	Empêche les fuites de données en identifiant et en contrôlant les contenus qui transitent sur le réseau via l'identification des expressions régulières.

Services d'abonnement de prévention des intrusions

Capture Advanced Threat Protection[1]	
Fonctionnalité	Description
Service de sandbox multimoteur	La plateforme sandbox multimoteur, qui inclut le sandboxing virtualisé, l'émulation complète du système et une technologie d'analyse au niveau de l'hyperviseur, exécute le code suspect et analyse son comportement, offrant ainsi une visibilité complète sur l'activité malveillante.
Blocage jusqu'au verdict	Pour empêcher les fichiers potentiellement malveillants de pénétrer sur le réseau, les fichiers envoyés dans le cloud pour y être analysés peuvent être retenus à la passerelle jusqu'à ce qu'un verdict soit rendu.
Analyse de nombreux types de fichiers	Ce service assure l'analyse d'un vaste éventail de fichiers, notamment les programmes exécutables (PE), DLL, PDF, documents MS Office, archives, JAR et APK, ainsi que de divers systèmes d'exploitation comme Windows, Android ou Mac OS et des environnements multi-navigateurs.
Déploiement rapide des signatures	Lorsqu'un fichier est identifié comme étant malveillant, une signature est immédiatement mise à la disposition des pare-feux ayant un abonnement à SonicWall Capture, avant d'être envoyée sous 48 heures aux bases de données de signatures Gateway Anti-Virus et IPS ainsi qu'aux bases de données d'URL, d'IP et de réputation de domaine.
Capture Client	Capture Client utilise un moteur statique d'intelligence artificielle (IA) pour identifier des menaces avant qu'elles ne puissent s'exécuter et pour revenir à un état précédant l'infection.
Protection contre les menaces chiffrées	
Fonctionnalité	Description
Déchiffrement et inspection TLS/SSL	Déchiffre et inspecte le trafic chiffré TLS/SSL à la volée, sans proxy, pour détecter les logiciels malveillants, les intrusions et les fuites de données, et applique les règles de contrôle du contenu, des URL et des applications afin de contrer les menaces dissimulées au sein du trafic chiffré. Inclus avec les abonnements de sécurité pour tous les modèles, à l'exception de SOHO. Vendu comme une licence séparée sur les modèles SOHO.
Inspection SSH	L'inspection approfondie des paquets SSH (DPI-SSH) déchiffre et inspecte les données traversant les tunnels SSH en vue de prévenir les attaques qui exploitent ce protocole.
Prévention des intrusions[1]	
Fonctionnalité	Description
Protection basée sur des contre-mesures	Le système de prévention des intrusions (Intrusion Prevention System, IPS) étroitement intégré s'appuie sur les signatures et autres contre-mesures pour détecter les vulnérabilités et les attaques, dont il couvre une large palette, au sein de la charge utile.
Mise à jour automatique des signatures	L'équipe de recherche des menaces SonicWall recherche et déploie en continu des mises à jour pour une longue liste de contre-mesures IPS couvrant plus de 50 catégories d'attaque. Les nouvelles mises à jour prennent effet immédiatement, sans redémarrage ni interruption de service.
Protection IPS intrazone	Renforce la sécurité interne en segmentant le réseau en plusieurs zones de sécurité avec prévention des intrusions, empêchant les menaces de se propager entre ces zones.
Détection et blocage de la commande et du contrôle (Command and Control, CnC) des réseaux de zombies	Identifie et bloque le trafic CnC provenant de robots sur le réseau local vers des IP et des domaines identifiés comme propageant des logiciels malveillants ou comme des points CnC connus.
Abus/anomalies de protocoles	Identifie et bloque les attaques exploitant les protocoles dans le but de contourner le système IPS.
Protection de type « zero-day »	Protège le réseau contre les attaques de type « zero-day » avec des mises à jour constantes répondant aux dernières méthodes et techniques d'attaque et couvrant des milliers de failles.
Technologie anti-évasion	La normalisation intensive des flux, le décodage et d'autres techniques empêchent les menaces d'entrer sur le réseau sans se faire détecter via des techniques d'évasion sur les couches 2 à 7.
Prévention des intrusions[1]	
Fonctionnalité	Description
Anti-logiciels malveillants de passerelle	Le moteur RFDPI analyse tout le trafic entrant, sortant et intrazone pour détecter les virus, chevaux de Troie, enregistreurs de frappes et autres logiciels malveillants dans les fichiers, quelles que soient leur taille et leur longueur, sur tous les ports et les flux TCP.
Protection anti-malware Capture Cloud	Les serveurs cloud SonicWall hébergent une base de données contenant des dizaines de millions de signatures de menaces, mise à jour en continu. Cette dernière est utilisée pour augmenter les capacités de la base de données de signatures locale, offrant au moteur RFDPI une couverture étendue des menaces.
Mises à jour de sécurité en continu	Les nouvelles mises à jour sont automatiquement appliquées aux pare-feux sur le terrain dotés de services de sécurité actifs et prennent effet immédiatement, sans redémarrage ni interruption.
Inspection TCP brute bidirectionnelle	Le moteur RFDPI analyse des flux TCP bruts sur tous les ports, de manière bidirectionnelle, pour détecter et empêcher les menaces entrantes et sortantes.
Prise en charge étendue des protocoles	Identifie les protocoles courants (HTTP/S, FTP, SMTP, SMBv1/v2, etc.) qui n'envoient pas de données sous forme de flux TCP bruts. Décode les charges utiles en vue d'un filtrage anti-malware, même si elles ne transitent pas par les ports standard habituels.

Surveillance et contrôle des applications	
Fonctionnalité	Description
Contrôle des applications	Compare les applications, ou les fonctionnalités des applications, identifiées par le moteur RFDPI à une base de données en constante expansion de plusieurs milliers de signatures. Cela renforce la sécurité et la productivité réseau.
Identification des applications personnalisées	Contrôle les applications personnalisées en créant des signatures basées sur leurs paramètres ou schémas spécifiques dans leurs communications réseau. Cela permet de mieux contrôler le réseau.
Gestion de la bande passante applicative	Alloue et régule la bande passante disponible de manière granulaire selon l'importance (ou la catégorie) des applications tout en limitant le trafic vers les applications non essentielles.
Contrôle granulaire	Contrôle les applications (ou des composants spécifiques d'une application), en fonction de calendriers, de groupes d'utilisateurs, de listes d'exclusion et de plusieurs actions en effectuant une identification SSO complète des utilisateurs via l'intégration LDAP/AD/Terminal Services/Citrix.
Filtrage du contenu[1]	
Fonctionnalité	Description
Filtrage du contenu interne/externe	Applique des règles d'utilisation acceptables et bloque l'accès aux sites Web HTTP/HTTPS contenant des informations ou des images répréhensibles ou non productives via Content Filtering Service et Content Filtering Client.
Client de filtrage de contenu appliqué	Étend l'application des règles pour bloquer les contenus Internet des appareils Windows, Mac OS, Android et Chrome situés hors du périmètre du pare-feu.
Contrôles granulaires	Bloque des contenus à l'aide d'une combinaison de catégories. Le filtrage peut être planifié à certains moments de la journée, pendant les heures de bureau ou d'école par exemple, et appliqué à des groupes ou utilisateurs spécifiques.
Mise en cache Web	Les évaluations d'URL sont mises en cache localement sur le pare-feu SonicWall pour accélérer l'accès ultérieur aux sites les plus fréquentés.
Local CFS Responder	Le service Local CFS Responder peut être déployé en tant qu'appliance virtuelle dans des clouds privés sur la base de VMWare ou Microsoft Hyper-V. Il offre une flexibilité de déploiement supplémentaire (Light weight VM) de la base d'évaluations CFS sur divers types de réseaux clients nécessitant une solution locale dédiée pour accélérer les délais de requête et de réponse des évaluations CFS, supporter une liste de nombreuses URL autorisées/bloquées (plus de 100 000) et ajouter jusqu'à 1000 pare-feux SonicWall aux recherches d'évaluations CFS.
Antivirus et anti-logiciels espions appliqués[1]	
Fonctionnalité	Description
Protection multicouche	Utilise les fonctionnalités du pare-feu comme première couche de défense au niveau du périmètre et les associe à la protection des terminaux pour bloquer les virus qui entrent sur le réseau par le biais des ordinateurs portables, des clés USB ou d'autres systèmes non protégés.
Option d'application automatisée	S'assure que chaque ordinateur qui accède au réseau utilise le bon logiciel antivirus et/ou un certificat DPI-SSL installé et actif, éliminant ainsi les coûts couramment liés à la gestion des antivirus installés sur les ordinateurs de bureau.
Option de déploiement et d'installation automatisés	Le déploiement et l'installation, ordinateur par ordinateur, des clients antivirus et anti-logiciels espions sont automatiques sur le réseau, ce qui limite la charge d'administration.
Antivirus de nouvelle génération	Capture Client utilise un moteur statique d'intelligence artificielle (IA) pour identifier des menaces avant qu'elles ne puissent s'exécuter et pour revenir à un état précédant l'infection.
Protection contre les logiciels espions	Une protection puissante contre les logiciels espions analyse et bloque l'installation d'un large éventail de logiciels espions sur les ordinateurs portables et de bureau avant qu'ils ne transmettent des données confidentielles, renforçant ainsi les performances et la sécurité des postes de travail.

[1] Requiert un abonnement supplémentaire
[2] Non pris en charge sur les pare-feux NSv Series

À propos de nous

SonicWall s'engage depuis plus de 27 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution automatisée de détection et de prévention des failles en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 215 pays et territoires, leur permettant de se concentrer sans crainte sur leur cœur de métier. Pour plus d'informations, consultez notre site à l'adresse : www.sonicwall.com ou suivez-nous sur Twitter, LinkedIn, Facebook et Instagram.

Partner Enabled Services

Vous avez besoin d'aide pour planifier, déployer ou optimiser votre solution SonicWall ? Les partenaires SonicWall Advanced Services sont spécialement formés pour vous fournir des services professionnels de premier ordre. Plus d'infos sur www.sonicwall.com/PES.

Récapitulatif des fonctionnalités de SonicOS

Pare-feu

- Inspection stateful des paquets
- Reassembly-Free Deep Packet Inspection
- Protection contre les attaques DDoS (UDP/ICMP/SYN flood)
- Prise en charge IPv4/IPv6
- Authentification biométrique pour l'accès distant
- Proxy DNS
- API REST

Déchiffrement et inspection TLS/SSL/SSH[2]

- Inspection approfondie des paquets pour TLS/SSL/SSH
- Inclusion/exclusion d'objets, de groupes ou de noms d'hôtes
- Contrôle SSL
- Contrôles DPI SSL granulaires par zone ou par règle

Capture Advanced Threat Protection[2]

- Real-Time Deep Memory Inspection
- Analyse multimoteur cloud
- Sandboxing virtualisé
- Analyse au niveau de l'hyperviseur
- Émulation complète du système
- Examen de nombreux types de fichiers
- Soumission automatique et manuelle
- Mises à jour en temps réel des renseignements sur les menaces
- Blocage jusqu'au verdict
- Capture Client

Prévention des intrusions[2]

- Analyse basée sur des signatures
- Mise à jour automatique des signatures
- Moteur d'inspection bidirectionnelle
- Fonctionnalité de règles IPS granulaires
- Localisation GeoIP
- Filtrage de réseaux de zombies avec liste dynamique
- Détection des expressions régulières

Protection contre les logiciels malveillants[2]

- Analyse des logiciels malveillants basée sur les flux
- Antivirus de passerelle
- Anti-logiciels espions de passerelle
- Inspection bidirectionnelle
- Pas de limitation de la taille des fichiers
- Base de données cloud de logiciels malveillants

Identification des applications[2]

- Contrôle des applications
- Gestion de la bande passante applicative
- Création de signatures d'applications personnalisées
- Prévention des fuites de données
- Création de rapports sur les applications via NetFlow/IPFIX
- Base de données complète des signatures d'applications

Visualisation et analyse du trafic

- Activité des utilisateurs
- Utilisation par les applications/bande passante/menaces
- Analyse dans le cloud

Filtrage du contenu Web HTTP/HTTPS[2]

- Filtrage des URL
- Évitement de proxy
- Blocage par mots-clés
- Filtrage à base de règles (exclusion/inclusion)
- Insertion d'en-tête HTTP
- Catégories d'évaluation CFS pour la gestion de la bande passante
- Modèle unifié de règles avec contrôle des applications
- Content Filtering Client

VPN

- SD-WAN sécurisé
- Configuration automatique du VPN
- VPN IPSec pour la connectivité site à site
- Accès client à distance IPSec et VPN SSL
- Passerelle VPN redondante
- Mobile Connect pour iOS, Mac OS X, Windows, Chrome, Android et Kindle Fire
- VPN basé sur le routage (RIP/OSPF/BGP)

Gestion de réseau

- PortShield
- Trames Jumbo
- Découverte MTU de chemin
- Journalisation améliorée
- Jonction VLAN
- Mise en miroir des ports (NS*a* 2650 et plus récentes)
- Qualité de service de couche 2
- Sécurité des ports
- Routage dynamique (RIP/OSPF/BGP)
- Contrôleur sans fil SonicWall[1]
- Routage à base de règles (ToS/métrique et ECMP)
- NAT
- Serveur DHCP
- Gestion de la bande passante
- Agrégation de liens[1] (statique et dynamique)
- Redondance de ports[1]
- Haute disponibilité A/P avec synchro. d'état
- Clustering A/A[1]
- Équilibrage de la charge entrante/sortante
- Mode NAT, mode TAP, mode filaire/filaire virtuel, mode pont de couche 2[1]
- Basculement WAN 3G/4G[1]
- Routage asymétrique
- Prise en charge Common Access Card (CAC)

VoIP

- Contrôle QoS granulaire
- Gestion de la bande passante
- DPI du trafic VoIP
- Prise en charge des proxys SIP et des contrôleurs d'accès H.323

Gestion et surveillance

- Interface utilisateur Web
- Interface de ligne de commande (CLI)
- SNMPv2/v3
- Création de rapports et gestion centralisés avec SonicWall Global Management System (GMS)[2]
- Journalisation
- Exportation NetFlow/IPFix
- Sauvegarde cloud de la configuration
- Plateforme d'analyse de sécurité BlueCoat
- Visualiseur de bande passante et d'applications
- Gestion IPv4 et IPv6
- Création de rapports hors pare-feu (Scrutinizer)
- Écran de gestion LCD[1]
- Gestion des commutateurs Dell série N et série X, notamment en cascade[1]

Sans-fil[1]

- WIDS/WIPS
- Prévention des points d'accès sauvages
- Itinérance rapide (802.11k/r/v)
- Sélection de canal automatique
- Analyse du spectre RF
- Vue plan de sol
- Vue topologique
- Orientation de bande
- Formation de faisceaux
- Équité du temps d'utilisation du réseau
- Extendeur MiFi
- Quota cyclique invités
- Portail invités LHM

Sans-fil intégré (TZ Series uniquement)

- Double bande (2,4 GHz et 5,0 GHz)
- Normes 802.11 a/b/g/n/ac
- Détection et prévention sans fil des intrusions
- Services sans fil pour les invités
- Messagerie légère à point d'accès
- Segmentation des points d'accès virtuels
- Portail captif
- Cloud ACL

[1] Non pris en charge sur les pare-feux NSv Series
[2] Requiert un abonnement supplémentaire.

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

Datasheet-SonicOSplatform-US-VG-MKTG4136