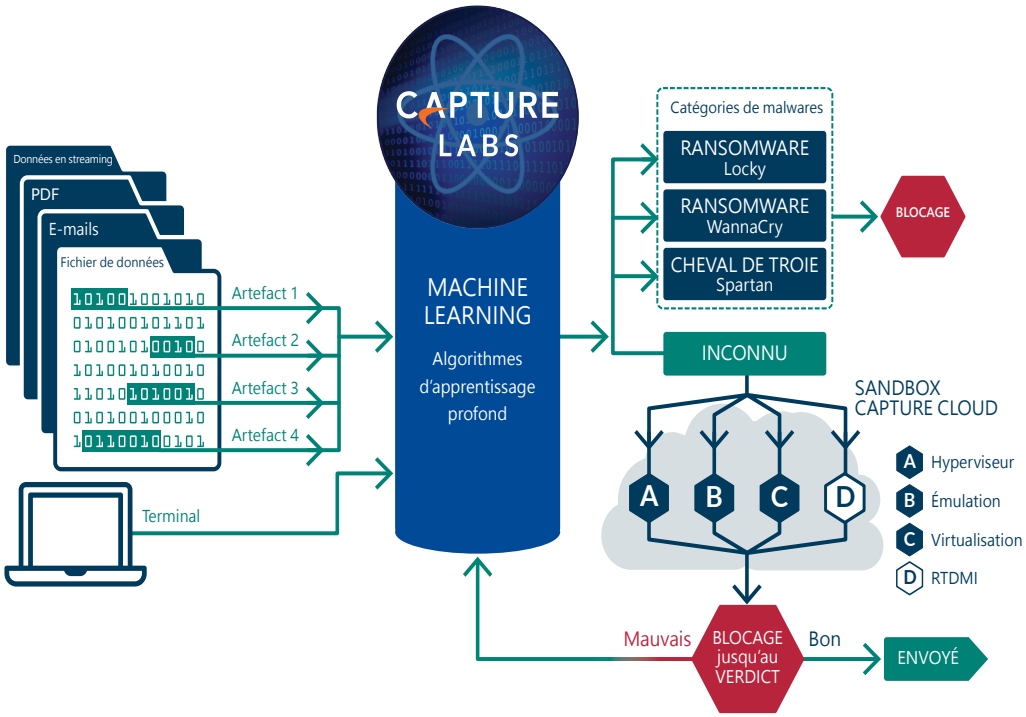
SonicOS 7 et services

L'architecture SonicOS est au cœur des pare-feux physiques et virtuels SonicWall, notamment TZ, NS*a*, NS*v* et NS*sp* Series. SonicOS repose sur nos technologies brevetées RFDPI® (Reassembly-Free Deep Packet Inspection) « single pass » à faible latence et RTDMI™ (Real-Time Deep Memory Inspection), 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 d'autres puissantes fonctionnalités de sécurité.

Notre vision pour la sécurisation des réseaux dans le paysage actuel des cybermenaces en constante mutation est la détection et la prévention automatisées et en temps réel des menaces. Grâce à une combinaison de technologies basées sur le cloud et intégrées, nos pare-feux sont dotés d'une sécurité haute efficacité validée par des tests tiers indépendants. Les menaces inconnues sont envoyées à la sandbox multimoteur cloud de SonicWall, Capture Advanced Threat Protection (ATP), pour y être analysées. Le service Capture ATP est optimisé par notre technologie brevetée RTDMI™. En procédant à une inspection directement dans la mémoire, le moteur RTDMI détecte et bloque les menaces zero-day et les logiciels malveillants inconnus. La technologie RTDMI est précise, réduit le nombre de faux positifs et identifie et limite les attaques sophistiquées dans lesquelles l'arsenal d'armes des malwares est exposé pendant moins de 100 nanosecondes.



FICHE TECHNIQUE

En parallèle, notre moteur RFDPI examine chaque octet de chaque paquet, inspectant directement le trafic entrant et sortant sur le pare-feu. En tirant parti de Capture ATP avec la technologie RTDMI dans la plateforme SonicWall Capture Cloud en plus des fonctionnalités intégrées, notamment la prévention des intrusions, la protection anti-malware et le filtrage des URL/Web, nos pare-feux de nouvelle génération bloquent les malwares, ransomwares et autres menaces au niveau de la passerelle.

L'introduction du système d'exploitation SonicOS 7.1.1 propulse les caractéristiques et les fonctionnalités du pare-feu de 7e génération à un niveau supérieur. En plus d'offrir une sécurité avancée, une gestion simplifiée des règles et des fonctionnalités de gestion et de réseau essentielles pour les entreprises distribuées avec succursales SD-Branch de nouvelle génération et les PME, SonicOS 7.1.1 ajoute des fonctionnalités nouvelles ou améliorées pour la prise en charge du Wi-Fi 6, la sécurité DNS, le filtrage de contenu basé sur la réputation et l'intégration du contrôle d'accès réseau (NAC).

Offres groupées de services de sécurité

Les services de sécurité SonicWall transforment le pare-feu en véritable solution de sécurité. Trois offres d'abonnement sont disponibles : Threat Protection, Essential Protection et Advanced Protection.

(i) SonicWall Threat Protection Service Suite est une offre groupée rentable qui comprend les services de sécurité de base nécessaires pour garantir la protection du réseau contre les menaces.

(ii) SonicWall Essential Protection Service Suite fournit tous les services de sécurité essentiels nécessaires à la protection contre les menaces connues et inconnues.

(iii) SonicWall Advanced Protection Service Suite offre une sécurité avancée pour étendre la sécurité de votre réseau avec des services de sécurité essentiels dans le cloud.

Fonctionnalité	Threat Protection	Essential Protection	Advanced Protection
Antivirus de passerelle, prévention des intrusions, contrôle des applications	✓	✓	✓
Service de filtrage du contenu	✓	✓	✓
Anti-spam	!	✓	✓
Support 24h/24, 7j/7	✓	✓	✓
Visibilité du réseau	✓	✓	✓
Sandboxing multimoteur Capture ATP	!	✓	✓
Technologie RTDMI	!	✓	✓
Sécurité DNS	✓	✓	✓
Gestion cloud	!	!	✓
Reporting basé sur le cloud : 7 jours	!	!	✓

✓ Fait partie de l'offre groupée ! Non disponible avec l'offre groupée, mais possibilité d'achat séparé

TABLEAU DE BORD AMÉLIORÉ

Tableau de bord amélioré	
Fonctionnalité	**Description**
Sécurité DNS	Utilise le DNS pour bloquer les sites Web ou applications malveillants et pour filtrer les contenus nuisibles ou inappropriés.
Intégration du contrôle d'accès réseau (NAC)	Fournit un contrôle d'accès réseau aux clients SonicWall en s'intégrant à Aruba ClearPass. Cette architecture transformera la sécurité statique en sécurité contextuelle afin de fournir une protection plus souple et plus avancée.
Prise en charge du Wi-Fi 6	Intégration et gestion des points d'accès Wi-Fi 6 SonicWave.
Amélioration du stockage secondaire	Prise en charge de la capture de paquets, des fichiers TSR et des données de corrélation des menaces dans le stockage. Enregistrement des journaux suivants : journaux des menaces, journaux d'audit, flux d'applications, pcap.
Enregistrements par jeton	Une chaîne qui remplacera le nom d'utilisateur et le mot de passe MySonicWall dans le fichier bootstrap utilisé pour le processus de bootstrap NSv afin d'automatiser les déploiements de masse avec la configuration de base et les informations de licence.
Bootstrap NS*v*	Simplification des déploiements NSv de masse ; prise en charge sur VMware, Hyper-V, AWS et Azure ; simplification des enregistrements de produits grâce à des licences basées sur des jetons ; le fichier INIT inclut une configuration de base pour que l'instance soit prête avec une configuration minimale.
Tableau de bord amélioré	Tableau de bord avec alertes actionnables.
« Vue améliorée de l'appareil avec affichage de la vue avant, de la vue arrière et des statistiques de stockage du matériel »	L'utilisateur peut désormais connaître, depuis l'onglet d'accueil de l'interface utilisateur, l'état en temps réel des statistiques d'utilisation du panneau avant, du panneau arrière et du module de stockage. Vous bénéficiez d'une expérience similaire à celle que vous auriez si vous vous trouviez physiquement devant le matériel.
Utilisation du système et de la bande passante en temps réel	L'utilisateur peut désormais visualiser l'utilisation en temps réel du système au niveau du cœur et de la bande passante du réseau.
Résumé de la répartition du trafic	Utilisation de la répartition du trafic sur le pare-feu de l'utilisateur avec mise à jour en temps réel de l'application la plus utilisée.
Résumé des principaux utilisateurs	Résumé des principaux utilisateurs sur la base des sessions autorisées ou bloquées, en fonction des données envoyées et reçues.
Résumé des menaces observées	Résumé en temps réel des menaces observées sur le réseau du client, comme les virus, les logiciels malveillants zero-day, les logiciels espions, les vulnérabilités et les applications à risque.
Résumé des services	Statut en temps réel des services de sécurité activés ou désactivés (IPS, GAV, Anti-Spyware, Capture ATP ou DPI-SSL).
Aperçu des hôtes infectés	Affiche en temps réel le nombre total de machines hôtes infectées dans le réseau.
Aperçu des attaques critiques	Affiche en temps réel le nombre total d'attaques critiques dans le réseau.
Aperçu du trafic chiffré	Affiche en temps réel la totalité du trafic chiffré dans le réseau.
Résumé des principales applications	Affiche les principales applications utilisées dans le réseau avec des options supplémentaires de tri par sessions, octets, blocages de règles d'accès, virus, logiciels espions et intrusions.
Résumé des principales adresses	Affiche les principales adresses utilisées dans le réseau avec des options supplémentaires de tri par sessions, octets, blocages de règles d'accès, virus, logiciels espions et intrusions.
Résumé des principaux utilisateurs	Affiche les principaux utilisateurs dans le réseau avec des options supplémentaires de tri par sessions, octets, blocages de règles d'accès, virus, logiciels espions et intrusions.
Résumé des meilleures classifications de sites Web	Affiche les meilleures classifications de sites Web par session.
Résumé des meilleures statistiques par pays	Affiche les meilleures statistiques nationales par session, trafic abandonné, octets envoyés ou reçus.
Résumé des menaces en temps réel	Affiche les principales menaces avec des statistiques distinctes pour les virus, les intrusions, les logiciels espions et les botnets par session.
Instantané du point d'accès amélioré	Affiche les statistiques sur le statut du point d'accès dans le réseau et les statistiques en temps réel sur les associations de clients.
Taux de trafic du point d'accès	Fournit l'utilisation de la bande passante en temps réel par point d'accès.
Rapport sur le client Wi-Fi	Fournit un rapport en temps réel sur le client Wi-Fi en fonction du type de système d'exploitation, de la fréquence et du tableau des principaux clients.
Surveillance du client Wi-Fi en temps réel	Détermine la machine hôte, le type de système d'exploitation, la fréquence, les informations sur le point d'accès et le transfert de données.
Aperçu des verdicts Capture ATP	Affiche les verdicts donnés pour l'analyse de fichiers par Capture ATP.
Aperçu des types de fichiers	Affiche le type de fichiers basé sur le rapport Capture ATP.
Aperçu de l'adresse de destination	Affiche les principales destinations utilisées par les fichiers malveillants.
Statistiques d'analyse des malwares	Affiche des statistiques approfondies sur l'analyse dynamique ou statique des logiciels malveillants par fichier.
Analyse de l'origine des attaques zero-day selon la localisation	Affiche l'origine des attaques par pays.
Statistiques Capture ATP	Affiche des informations sur le nombre total de fichiers soumis, les fichiers analysés dynamiquement, les fichiers malveillants et le temps de traitement moyen avec Capture ATP.
Vue topologique du réseau	Vue topologique affichant les hôtes et les points d'accès connectés au réseau de l'utilisateur selon le nom de l'appareil, l'adresse MAC et l'adresse IP.
Gestion pilotée par l'API	La gestion du pare-feu est pilotée par l'API.

Assistant SDWAN	Assistant de configuration automatique de la règle SDWAN sur le pare-feu.
Centre de notification	Nouveau centre de notification avec résumé des menaces, journaux d'événements et alertes système.
Aide en ligne améliorée	Aide en ligne avec des liens vers la documentation technique de chaque modèle.
Surveillance SDWAN	Affiche les sondes de performance SD-WAN et les principales connexions.
Utilitaire de surveillance des paquets améliorée	La surveillance des paquets a été améliorée pour inclure les règles d'accès, les règles NAT et les informations sur l'acheminement.
Configuration des périphériques de stockage	Prise en charge de la configuration des modules de stockage, y compris les modules étendus. Statistiques d'utilisation du module.
Capture Threat Assessment (CTA) 2.0	Le nouveau rapport CTA 2.0 prend en charge un modèle de rapport inédit avec des options de personnalisation comme le logo, le nom et les sections. Prise en charge de l'analyse des fichiers et des logiciels malveillants. Statistiques de l'entreprise avec moyenne mondiale et par secteur d'activité pour chaque section. Modèle exécutif séparé avec recommandations.
Téléchargement des journaux système	Les journaux système, y compris les journaux de la console, peuvent être téléchargés depuis la section de diagnostic sans que l'utilisateur ait besoin de connecter la machine au port console pour capturer les journaux de la console. Cela simplifie les méthodes de débogage et la durée du dépannage.
Terminal SSH sur l'interface utilisateur	Le terminal SSH est accessible depuis l'interface Web.
Utilitaire de vérification du GRID	Cet utilitaire permet de vérifier l'adresse IP du GRID à des fins de diagnostic.
Utilitaire de débogage	L'utilisateur peut activer le mode de débogage dans le même firmware et exécuter des commandes de débogage depuis le terminal SSH dans l'interface utilisateur.
Outils de l'utilitaire de diagnostic système	Prise en charge d'autres outils de diagnostic comme GDB, HTOP et Linux Perf Tool.
Vue d'ensemble du réseau de switchs	Vue du switch SonicWall comme la vue physique, la vue sous forme de liste et la vue VLAN.
Utilisation de la bande passante par SwitchPort	SonicWall Switch Info affiche l'utilisation de la bande passante par port.
Statut WWAN	Affichage du statut du modem WWAN et du réseau.

FONCTIONNALITÉS ET SERVICES DES PARE-FEUX

Moteur RFDPI (Reassembly-Free Deep Packet Inspection)

Fonctionnalité	Description
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 multicœur 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 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	Prend en charge des modes hautes disponibilité actif/passif (A/P) avec synchronisation de l'état, DPI2 actif/actif (A/A) et mise en cluster active/active. Le mode DPI actif/actif permet de décharger la charge DPI vers l'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 de 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 (QoS) avancée	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.
Intégration de SonicWall Switch	Le tout premier switch de SonicWall permet une intégration transparente avec les pare-feux pour une gestion et une visibilité de votre réseau depuis un écran unique.
Gestion des commutateurs Dell série N et série X uniques et en cascade	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.
Prise en charge complète de l'API	Prise en charge complète de l'API pour chaque section de l'interface utilisateur du pare-feu.
Évolutivité SD-WAN	Interfaces de tunnel évolutives pour les entreprises distribuées.

Gestion, reporting et support

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.
Détection des logiciels malveillants centrée sur la conformité	Analyse des fichiers suspects dans votre environnement sans envoyer les fichiers ou les résultats à un cloud tiers.

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.
RTDMI™ (Real-Time Deep Memory Inspection)	Technologie et processus brevetés, SonicWall RTDMI est utilisé par le cloud SonicWall Capture pour identifier et atténuer les menaces modernes les plus insidieuses, y compris les exploits futurs de Meltdown. Elle détecte et bloque même les logiciels malveillants qui n'affichent aucun comportement malveillant ou qui masquent leur arsenal via le chiffrement.
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 malveillant, une signature est immédiatement déployée sur les pare-feux ayant un abonnement à SonicWall Capture, avant d'être envoyée 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.

Sécurité des terminaux

Fonctionnalité	Description
Protection des terminaux	Capture Client applique une protection contre les menaces évoluées basée sur le comportement et alimentée par l'EDR de nouvelle génération SentinelOne. Intégration de Capture ATP pour une sécurité encore plus efficace, des délais de réponse plus brefs et un coût total de possession réduit.
Exécution DPI-SSL	Déploiement des certificats DPI SSL et exécution de l'inspection approfondie des paquets du trafic chiffré (DPI SSL) sur les terminaux.
Exécution des terminaux	Dirige les utilisateurs non protégés vers une page de téléchargement de Capture Client avant tout accès à Internet lorsqu'ils sont derrière un pare-feu.
Connexion SSO	Permet d'utiliser les informations sur les utilisateurs provenant des terminaux pour les règles SSO.

Prévention des 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.
Prise en charge de TLS 1.3	Prise en charge de TLS 1.3 pour améliorer la sécurité globale du pare-feu. Elle est mise en œuvre dans la gestion des pare-feux, le VPN SSL et le DPI.

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 contre les attaques zero-day	Protège le réseau contre les attaques 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 menaces[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[1]

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 basé sur la réputation	Restreint et contrôle le contenu Web auquel un internaute peut accéder. Le filtrage de contenu basé sur la réputation fournit un score de réputation qui prévoit le risque de sécurité d'une URL.
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 1 000 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.
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.

Sécurité avancée

Fonctionnalité	Description
Visibilité du réseau	Fournit une visibilité granulaire de la topologie du réseau ainsi que des informations sur les hôtes.
Gestion cloud	Gère les pare-feux via le cloud par le biais de la vignette Network Security Manager de Capture Security Center.
Reporting dans le cloud	Inclut un reporting dans le cloud sur sept jours.

[1] Requiert un abonnement supplémentaire

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**

À propos de SonicWall

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

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

SONICWALL