SONICWALL

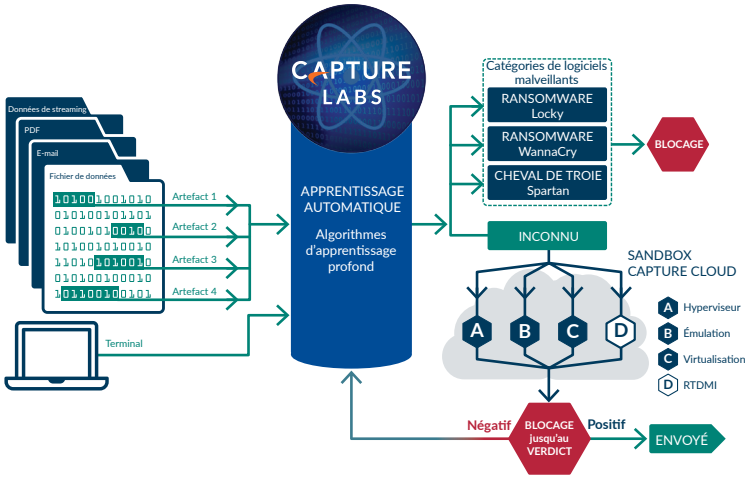
Fiche technique SonicOSX 7.0

L'architecture SonicOSX est au cœur de chaque pare-feu d'entreprise physique et virtuel de SonicWall, notamment les pare-feu des séries NSa, NSv et NSsp. SonicOSX utilise notre technologie brevetée, à faible latence en un seul passage, Reassembly-Free Deep Packet Inspection® (RFDPI) et notre technologie en instance de brevet Real-Time Deep Memory Inspection™ (RTDMI) pour assurer une haute efficacité de sécurité validée par l'industrie, un SD-WAN sécurisé, une visualisation en temps réel, un réseau privé virtuel (VPN) haut débit et d'autres solides fonctionnalités de sécurité.

Notre vision de la sécurisation des réseaux dans le paysage en constante mutation de la cybercriminalité implique une détection et une prévention automatisées et en temps réel des menaces. L'association de technologies intégrées et cloud permet à nos pare-feu d'assurer une sécurité dont l'extrême efficacité a été validée lors de tests par des 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 RTDMI™. En procédant à une inspection directement dans la mémoire, le moteur RTDMI détecte et bloque les logiciels malveillants et les menaces de type zero-day. La technologie RTDMI est précise, elle réduit à un minimum les faux positifs, identifie et neutralise les attaques sophistiquées, dès que les armes du logiciel malveillant sont exposées en moins de 100 nanosecondes.

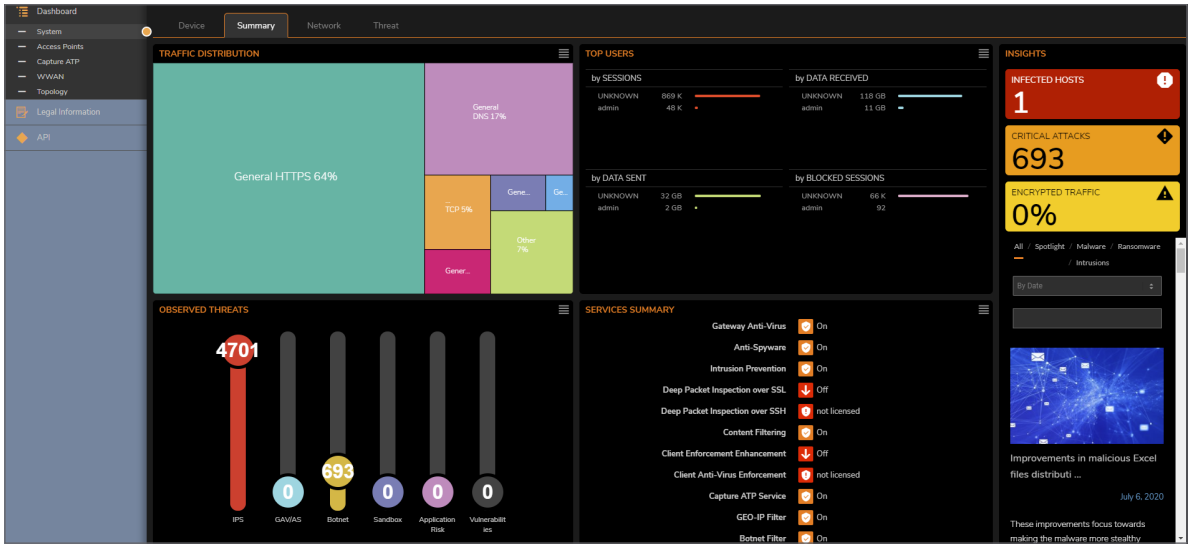
En parallèle, notre moteur RFDPI examine chaque octet de chaque paquet, inspectant simultanément le trafic entrant et sortant directement sur le pare-feu. Tirant parti du service Capture ATP et de la technologie RTDMI sur la plateforme Capture Cloud SonicWall en plus de fonctionnalités intégrées (prévention des intrusions, anti-malware et filtrage des URL/Web notamment), nos pare-feu de nouvelle génération bloquent les logiciels malveillants, les ransomwares et autres menaces à la passerelle.

L'introduction du tout nouveau système d'exploitation (OS) SonicOSX 7.0 catapulte davantage les fonctions et les fonctionnalités de pare-feu de nouvelle génération au niveau supérieur. Construite à partir de rien, l'architecture SonicOSX 7.0 est dotée d'une politique unifiée qui offre une gestion intégrée des différentes politiques de sécurité pour les pare-feu de qualité professionnelle.



La politique unifiée assure des contrôles de couche 3 à couche 7 dans une base de règles unique sur chaque pare-feu, fournissant aux administrateurs un emplacement centralisé pour la configuration des politiques. SonicOSX 7.0 est doté d'une nouvelle interface Web née d'une approche radicalement différente où l'accent est mis sur le design pour l'utilisateur. L'interface Web de SonicOSX offre des visualisations pertinentes des informations sur les menaces et affiche des alertes exploitables vous incitant à configurer des politiques de sécurité contextuelles avec une simplicité « pointer et cliquer ».

En plus d'être plus conviviale pour l'utilisateur, la nouvelle interface est également plus attrayante que la version classique. Avec l'affichage du pare-feu sur un seul écran, l'interface présente à l'utilisateur des informations sur l'efficacité des différentes règles de sécurité. L'utilisateur est ensuite en mesure de modifier en toute simplicité les règles prédéfinies pour les logiciels antivirus et antispyware, le filtrage du contenu, la prévention des intrusions, le filtrage géo-IP et l'inspection approfondie des paquets du trafic chiffré. Grâce à une politique unifiée, SonicWall offre une expérience simplifiée qui permet de réduire les erreurs de configuration et le temps de déploiement pour une meilleure stratégie globale en matière de sécurité.



La politique unifiée donne aux organisations la possibilité de contrôler le trafic dynamique passant par un pare-feu et offre de la visibilité et un aperçu des différentes politiques qui affectent l'antivirus de la passerelle, les antispyware, le filtrage de contenu, la prévention des intrusions, le filtrage géo-IP, l'inspection approfondie des paquets du trafic chiffré et plus encore. Cette solution permet de simplifier les tâches de gestion, de réduire les erreurs de configuration et d'accélérer le temps de déploiement, ce qui contribue à une meilleure posture de sécurité générale.

Cette mise à niveau du système d'exploitation offre aussi une prise en charge multi-instances sur les pare-feu de la série NSsp. La multi-instance est la prochaine génération de mutualisation, où chaque locataire est isolé avec des ressources informatiques dédiées pour éviter le manque de ressources.

Offres groupées de services de sécurité

Les services de sécurité de SonicWall transforment un pare-feu en une solution de sécurité complète. Les services de sécurité sont proposés en trois offres d'abonnement : Essential, Advanced et Premier.

- **SonicWall Essential Protection Service Suite** fournit tous les services de sécurité essentiels nécessaires pour se protéger contre les menaces connues et inconnues.
- **SonicWall Advanced Protection Service Suite** offre une sécurité avancée pour étendre la sécurité de votre réseau avec des services de sécurité essentiels supplémentaires dans le cloud.
- **SonicWall Premier Protection Service Suite*** offre une sécurité totale avec des services de sécurité supplémentaires, une visibilité dans le cloud, des services d'analyse et de terminaux pour une protection ultime.

FONCTIONNALITÉ	ESSENTIAL	ADVANCED	PREMIER*
Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	√	√	√
Service de filtrage de contenu	√	√	√
Anti-spam	√	√	√
Support 24 h/24, 7 j/7	√	√	√
Visibilité réseau	√	√	√
Sandboxing du service Capture ATP (multimoteur)	√	√	√
Technologie RTDMI	√	√	√
Sécurité DNS de base	√	√	√
Gestion du cloud	!	√	√
Rapports basés sur le cloud – 7 jours	!	√	√
Analyses avancées dans le cloud – Rapports virtuels sur 365 jours	!	!	√
Sécurité DNS avancée	!	!	√
Outil de vérification du système de pare-feu	X	X	√
Pack de démarrage Cloud App Security	X	X	√
Pack de démarrage Capture Client	X	X	√
Assistance Premier Support	X	!	!

√ *Fait partie de l'offre*
! *Non disponible avec l'offre, mais peut être acheté séparément*
X *Non pris en charge par l'offre*
* *Disponibilité en attente*

Fonctionnalités et services de pare-feu

TABLEAU DE BORD AMÉLIORÉ	
Fonctionnalité	**Description**
Tableau de bord amélioré	Tableau de bord avec alertes activables.
Vue améliorée des dispositifs avec affichage de la vue de face, de la vue arrière et des statistiques de stockage du matériel	L'utilisateur peut désormais se renseigner depuis l'onglet d'accueil de l'interface utilisateur sur le statut en temps réel du panneau avant, du panneau arrière et des statistiques d'utilisation du module de stockage. Donne une expérience similaire comme si vous étiez physiquement devant le matériel.
Utilisation du système en temps réel et utilisation de la bande passante	L'utilisateur peut désormais visualiser l'utilisation du système en temps réel du processeur et de la bande passante dans le réseau.
Répartition résumée du trafic	Utilisation de la distribution 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 en fonction des sessions autorisées ou bloquées ; par 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 de type « 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 comme IPS, GAV, antispyware, Capture ATP ou DPI-SSL.
Informations sur les hôtes infectés	Affichage en temps réel du nombre total de machines hôtes infectées sur le réseau.
Informations sur les attaques critiques	Affichage en temps réel du nombre total d'attaques critiques sur le réseau.
Informations sur le trafic chiffré	Affichage en temps réel du volume total de trafic chiffré sur le réseau.
Résumé des principales applications	Affichage des principales applications utilisées sur le réseau avec des options supplémentaires de tri par sessions, octets, blocs de règles d'accès, virus, logiciels espions et intrusions.
Résumé des principales adresses	Affichage des principales adresses utilisées sur le réseau avec des options supplémentaires de tri par sessions, octets, blocs de règles d'accès, virus, logiciels espions et intrusions.
Résumé des principaux utilisateurs	Affichage des principaux utilisateurs sur le réseau avec des options supplémentaires de tri par sessions, octets, blocs de règles d'accès, virus, logiciels espions et intrusions.
Résumé des meilleures évaluations du site Web	Affiche les meilleures évaluations du site par session.
Résumé des statistiques des principaux pays	Affiche les statistiques nationales par session, trafic en baisse, octets envoyés ou reçus.
Résumé des menaces en temps réel	Affichage des menaces principales avec des statistiques séparées pour les virus, intrusions, logiciels espions et botnets par session.
Informations sur les verdicts de Capture ATP	Affiche les verdicts donnés pour l'analyse de fichiers par Capture ATP.
Informations sur les types de fichiers	Affiche le type de fichiers basé sur le rapport Capture-ATP.
Informations sur l'adresse de destination	Affiche les principales destinations utilisées par les fichiers malveillants.
Statistiques de l'analyse des logiciels malveillants	Affiche des statistiques en profondeur sur l'analyse dynamique vs statique des logiciels malveillants par fichier.
Analyse de l'origine des attaques « zero-day » basée sur l'emplacement	Affiche l'origine des attaques par pays.
Statistiques Capture ATP	Analyse des données du total des fichiers soumis, des fichiers analysés dynamiquement, des fichiers malveillants et du temps de traitement moyen par Capture ATP.
Gestion pilotée par les API	La gestion du pare-feu est pilotée par les API.
Assistant SD-WAN	Assistant pour configurer automatiquement la politique SD-WAN sur le pare-feu
Centre de notifications	Nouveau centre de notifications avec résumé des menaces, journaux des événements et alertes du système.
Aide en ligne améliorée	Aide en ligne avec des liens vers la documentation technique sur chaque modèle.
Surveillance SD-WAN	Affiche les sondes de performance SD-WAN et les connexions supérieures.
Utilitaire de surveillance des paquets amélioré	Surveillance améliorée des paquets pour inclure la politique de sécurité, la politique de déchiffrement, la politique d'acheminement, les informations de signature d'application et de sécurité.
Capture Threat Assessment (CTA) 2.0	Le nouveau rapport CTA 2.0 prend en charge le nouveau modèle de rapport avec des options de personnalisation comme le logo, le nom et les sections. Assistance pour l'analyse de fichiers et l'analyse de logiciels malveillants. Statistiques d'entreprise avec secteur d'activité et moyenne mondiale pour chaque section. Modèle de cadre distinct avec recommandations.
Téléchargements de journaux système	Les journaux système incluent les journaux de la console qui peuvent être téléchargés à partir de la section Diagnostics sans que l'utilisateur ait besoin de connecter la machine au port de la console pour enregistrer les journaux de la console. Cela simplifie les méthodes de débogage et le temps de dépannage.
Terminal SSH sur interface utilisateur	Le terminal SSH est accessible à partir de l'interface Web.
Outils de l'utilitaire de diagnostic système	Prise en charge d'autres outils de diagnostic comme GDB, HTOP et Linux Perf Tool.

POLITIQUE UNIFIÉE

Fonctionnalité	Description
Présentation de la politique	Vue graphique des statistiques utilisées, inutilisées, autorisées ou refusées concernant la sécurité, le NAT, l'itinéraire, le déchiffrement ou la politique DoS.
Aperçu des objets	Vue graphique des objets personnalisés, adresse par défaut, zone, service, horaires, correspondance personnalisée, application, pays, URL, site Web ou objet de catégorie Web.
Aperçu des groupes	Vue graphique des objets personnalisés, adresse par défaut, zone, service, correspondance personnalisée, application, pays, URL, site Web ou groupes de catégorie Web.
Présentation des profils et signatures	Vue graphique des profils personnalisés par défaut comme IPS, sécurité, DoS ou bloc de page, et présentation des signatures GAV ou antispyware.
Consultation des politiques	Affiche la politique de sécurité correspondante en saisissant les paramètres de flux requis tels que l'adresse IP, le port, l'application et le site Web.
Profil d'action de sécurité	Le profil d'action de sécurité désigne les actions supplémentaires que l'utilisateur peut entreprendre après avoir autorisé ou refusé un paquet, comme l'application de la gestion de la bande passante et des services de sécurité.
Profil d'action DoS	Le profil d'action DoS désigne les actions supplémentaires que l'utilisateur peut entreprendre pour protéger ou contourner un paquet, comme l'application d'un seuil d'attaque et la limitation de connexions.
Objet de signature antivirus	Signatures antivirus avec plus de détails sur chaque signature.
Objet de signature antispyware	Signatures antispyware avec plus de détails sur chaque signature.
Groupe d'applications intuitives	Le groupe d'applications doit inclure plusieurs signatures d'applications avec une expérience utilisateur améliorée.
Compteur en direct sur la politique de sécurité	Permet de saisir des statistiques en direct sur la politique de sécurité.
Correspondance des applications basée sur les politiques	Identification des applications et des correspondances personnalisées basée sur la politique individuelle.
Clonage	Clone la règle de sécurité existante à une nouvelle règle.
Édition sélective des cellules	Possibilité d'effectuer une édition sélective des cellules sur la règle de sécurité sans ouvrir la règle. Réduit le nombre de clics pour l'utilisateur.
Copie shadow	Affiche les règles de doublon et de copie shadow au sein de chaque politique.
Regroupement des politiques par sections	Le regroupement des politiques par sections aide les utilisateurs métier ayant des milliers de règles de sécurité.
Regroupement personnalisé des politiques	Le regroupement des politiques par options personnalisées comme la zone, la balise, etc. aide les utilisateurs métier ayant des milliers de règles de sécurité.
Politique de déchiffrement	Politique d'inspection du trafic SSL/TLS.
Politique DoS	Politique de protection contre les attaques DoS/DDoD telles que la saturation ou de type Smurf

MOTEUR RFDPI (REASSEMBLY-FREE DEEP PACKET INSPECTION)

Fonctionnalité	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	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 GESTION DE RÉSEAU

Fonctionnalité	Description
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 du SD-WAN	Interfaces de tunnel évolutives pour les entreprises distribuées.
Mutualisation[2]	Activer la prise en charge multi-instances sur le pare-feu NSsp.
Vue du locataire en mutualisation[2]	Afficher l'utilisation de chaque instance et d'autres statistiques associées.

PARE-FEU ET RÉSEAU (SUITE)	
Micrologiciel séparé côté locataire[2]	Possibilité d'exécuter un micrologiciel séparé sur chaque instance et instance racine.
Licences de locataire à partir de la racine[2]	Licencier des instances enfant à partir de la racine. Affiche la clé pour chaque instance.
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 d'état 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 les modes haute disponibilité actif/actif (A/A) avec synchronisation de l'état, DPI actif/actif (A/A)[2]et mise en cluster actif/actif[2]. Le mode DPI actif/actif permet de décharger la charge d'inspection approfondie des paquets sur l'application 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 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 acheminements basés sur le protocole pour orienter le trafic vers une connexion WAN préférée, avec la capacité de revenir à 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.
Intégration Switch SonicWall	Les premiers commutateurs de SonicWall offrent une intégration transparente avec les pare-feu pour une gestion sur un seul et même écran et une visibilité de votre réseau
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-feu 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 leurs identifiants des 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	Propose une manière simple et rapide de gérer les règles de sécurité à travers tous les domaines réseau. Permet de gérer les règles individuelles pour un domaine unique ou un groupe de domaines.

GESTION, REPORTING ET ASSISTANCE	
Fonctionnalité	**Description**
Gestion dans le cloud et sur site	La configuration et la gestion des applications SonicWall peuvent 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 avec des outils comme SonicWall Scrutinizer ou d'autres outils prenant en charge IPFIX et NetFlow via des extensions.
Détection des programmes malveillants axée sur la conformité	Analyse les fichiers suspects au sein de votre propre environnement sans envoyer les fichiers ou les résultats vers un cloud tiers.
Objet de correspondance amélioré	L'objet de correspondance prend en charge l'ajout d'applications avec une expérience utilisateur améliorée.
Objets basés sur les profils	Objets de profil pour la sécurité des terminaux, la gestion de la bande passante, le marquage QoS, le filtre de contenu, l'option DHCP et le VPN AWS.
Règles de sécurité améliorées	Affichage amélioré des règles pour une expérience utilisateur intuitive.
Paramètres de grille personnalisables	Colonnes personnalisables et mobiles dans les politiques de sécurité, politique NAT, politique d'acheminement, politique de déchiffrement et politique DoS.
Affichage des règles actives et inactives	Affiche les règles activées ou désactivées.

GESTION, REPORTING ET SUPPORT	
Affichage des règles utilisées et non utilisées	Affiche les règles activement utilisées ou non utilisées.
Exporter les règles d'accès	Exporte toutes les règles d'accès dans un fichier CSV.
Compteur en direct sur la politique de sécurité	Permet de saisir des statistiques en direct sur la politique de sécurité.
Diagramme des règles	Vue schématique d'une politique particulière de sécurité, d'un NAT et d'une règle d'acheminement qui aident à trouver des statistiques en temps réel.
Règles de sécurité des terminaux	Possibilité d'ajouter des règles de sécurité pour la sécurité des terminaux à l'aide de Capture Client.

RÉSEAU PRIVÉ VIRTUEL (VPN)	
Fonctionnalité	**Description**
Configuration automatique du VPN	Simplifie sensiblement le déploiement de pare-feu distribués en automatisant la configuration initiale de la passerelle VPN site à site entre les pare-feu 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 à la série TZ 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. Possibilité 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 et filtrage des expressions régulières	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.
Inspection approfondie de la mémoire en temps réel (RTDMI™)	La technologie en instance de brevet RTDMI de SonicWall est utilisée par le Capture Cloud pour identifier et parer aux menaces modernes les plus insidieuses, y compris les attaques futures exploitant la vulnérabilité à Meltdown. Elle détecte et bloque les logiciels malveillants qui ne manifestent aucun comportement malveillant et dissimulent leur armement au moyen d'un chiffrement personnalisé.
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	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 et Android, 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-feu ayant un abonnement à SonicWall Capture, avant d'être envoyée sous 48 heures aux bases de données de signatures Gateway Anti-Virus GRID et IPS ainsi qu'aux bases de données d'URL, d'adresses 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
Prise en charge de TLS 1.3	Prise en charge du TLS 1.3 pour améliorer la sécurité globale du pare-feu. Ceci est implémenté dans Firewall Management, SSL VPN et DPI.
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 dans le 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 CONTRE LES 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 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-logiciels malveillants 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-feu 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 les flux TCP bruts sur n'importe quel port et de manière bidirectionnelle pour détecter et prévenir les menaces entrantes et sortantes.
Prise en charge étendue des protocoles	Identifie les protocoles courants tels que HTTP/S, FTP, SMTP, SMBv1/v2 et autres, qui n'envoient pas de données en flux TCP bruts. Décode les charges utiles pour l'inspection des logiciels malveillants, même s'ils ne fonctionnent pas sur des ports standard bien connus.

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 augmente la sécurité du réseau et améliore la productivité du réseau.
Identification des applications personnalisées	Elle contrôle les applications personnalisées en créant des signatures basées sur des paramètres spécifiques ou des schémas particuliers à une application dans ses communications réseau, ce qui offre un contrôle supplémentaire sur le réseau.
Gestion de la bande passante applicative	Cette fonctionnalité 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 renforcé	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 le contenu en utilisant toute 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.
Serveur CFS local	Un serveur CFS local peut être déployé en tant qu'application virtuelle dans des clouds privés basés sur VMWare ou Microsoft Hyper-V. Cela offre une option de déploiement flexible (VM légère) de la base de données d'évaluation du CFS dans divers cas d'utilisation du réseau client qui nécessitent une solution sur site dédiée qui accélère les demandes d'évaluation du CFS (service de filtrage du contenu) et les temps de réponse, prend en charge un grand nombre d'URL autorisées/bloquées (+100K), et ajoute jusqu'à 1000 pare-feu SonicWall pour les recherches d'évaluation du CFS.

ANTIVIRUS ET ANTISPYWARE 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 antispyware sont automatiques sur le réseau, ce qui limite les frais administratifs.
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.

SÉCURITÉ AVANCÉE

Fonctionnalité	Description
Sécurité DNS avancée	La sécurité DNS fournit un meilleur temps de détection et améliore le coût total de possession. La sécurité DNS inspecte les champs DNS pour identifier les domaines malveillants et ainsi bloquer la connexion à un stade très précoce de l'établissement de la connexion. SonicWall dispose de pétaoctets de données de menace qui aident à classer les domaines comme malveillants, réduisant ainsi les faux positifs.
Outil de vérification du système de pare-feu	Identifier les risques et renforcer la conformité et la sécurité. Disponible sur l'interface utilisateur du pare-feu, l'outil de vérification de bon fonctionnement surveille en permanence en temps réel l'infrastructure de sécurité, les passerelles, les technologies, les politiques et les paramètres de configuration.
Visibilité réseau	Elle offre une visibilité granulaire de la topologie du réseau et des informations sur l'hôte
Gestion du cloud	Gérer les pare-feu via le cloud grâce à Network Security Manager du Capture Security Center
Analyse basée sur le cloud	Comprend un reporting sur le cloud de sept jours

[1] *Requiert un abonnement supplémentaire*
[2] *Disponible uniquement sur NSsp*

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites 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 commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour en savoir plus, rendez-vous sur www.sonicwall.com.

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

Fiche technique SonicOSX-COG-2758