SONICWALL

Pare-feux SonicWall SuperMassive Series

Un pare-feu de nouvelle génération extrêmement performant et offrant une protection intransigeante, conçu pour le réseau de votre entreprise.

Le pare-feu SonicWall SuperMassive Series est le pare-feu de nouvelle génération de SonicWall, conçu pour les vastes réseaux et offrant une évolutivité, une fiabilité et une sécurité approfondie à des vitesses de plusieurs gigaoctets, avec une latence quasi nulle.

Conçu pour répondre aux besoins des entreprises, du service public, de l'éducation, du commerce de détail, des soins médicaux et des prestataires de services, le pare-feu SuperMassive Series est la solution idéale pour sécuriser des réseaux d'entreprise répartis, des centres de données et des prestataires de services.

Grâce à l'association du système d'exploitation SonicOS de SonicWall, de la technologie brevetée* Reassembly-Free Deep Packet Inspection® (RFDPI) et d'une architecture matérielle multi-cœur et hautement évolutive, la SuperMassive 9000 Series offre un contrôle des applications à la fine pointe du secteur, une prévention des intrusions, une protection contre les logiciels malveillants, un déchiffrement TLS/SSL et une inspection à des vitesses de plusieurs gigaoctets. Le pare-feu SuperMassive Series a été judicieusement conçu en tenant compte de la consommation électrique, de l'espace occupé et du refroidissement, offrant ainsi le meilleur pare-feu de nouvelle génération en termes de Gbit/s/watt du secteur pour le traitement haute performance des paquets et des données, le contrôle des applications et la prévention des menaces.

Le moteur RFDPI de SonicWall analyse chaque octet de chaque paquet de données à travers tous les ports, pour une inspection complète du contenu de tout le flux tout en fournissant des performances élevées et une latence limitée. Cette technologie est supérieure aux conceptions par proxy qui reconstituent le contenu à l'aide de connecteurs logiciels intégrés aux programmes anti-logiciels malveillants, qui manquent cruellement d'efficacité et souffrent d'un écroulement de la mémoire des connecteurs logiciels, ce qui entraîne une latence élevée, de piètres performances et des limites liées à la taille des fichiers. Le moteur RFDPI fournit une inspection complète du contenu pour éliminer les différentes formes de programmes malveillants avant qu'ils ne s'immiscent dans le réseau et offre une protection contre les menaces qui évoluent sans cesse, et ce sans limite de taille de fichier, de performance ou de latence.

Le moteur RFDPI réalise également un déchiffrement complet et une inspection du trafic crypté TLS/SSL et SSH, ainsi que des applications ne pouvant pas faire l'objet d'une conception par proxy, ce qui offre une protection totale quel que soit le mode de transport ou le protocole utilisé. Il examine avec minutie chaque paquet (tant au niveau de l'en-tête que des données) à la recherche d'un défaut de conformité du protocole, de menaces (notamment « zero-day ») et d'intrusions. Il utilise également des critères définis pour détecter et empêcher les attaques dissimulées au sein du trafic chiffré, interrompt la propagation des infections et déjoue les communications de commande et de contrôle ainsi que l'exfiltration des données. Les règles d'inclusion et d'exclusion permettent un contrôle total pour définir quel trafic est soumis au déchiffrement et à l'inspection en fonction d'exigences légales et/ou de conformité spécifiques à l'entreprise.

Les outils d'analyse du trafic applicatif permettent d'identifier le trafic applicatif productif et non productif en temps réel. Le trafic peut être contrôlé grâce à des règles puissantes au niveau des applications. Le contrôle des applications peut être réalisé au niveau de chaque utilisateur ou d'un groupe, sur la base de programmes définis et de listes d'exceptions. Toutes les signatures d'applications, de prévention des intrusions et de programmes malveillants sont en permanence mises à jour par l'équipe de recherche SonicWall Capture Labs spécialisée dans les menaces. En outre, SonicOS, un système d'exploitation sophistiqué et conçu sur mesure, offre des outils intégrés qui permettent d'identifier des applications personnalisées et de les contrôler.

SuperMassive 9000 Series

Avantages :

- Bénéficiez d'une prévention complète des failles, avec une prévention des intrusions extrêmement performante, une protection contre les logiciels malveillants à faible latence et une technologie de sandboxing basée sur le cloud
- Profitez d'une identification, d'un contrôle et d'une visualisation extrêmement précis des applications
- Dévoilez et bloquez les menaces cachées grâce au déchiffrement et à l'inspection du trafic chiffré TLS/SSL et SSH, sans problèmes de performances
- Faites évoluer vos performances de sécurité pour des centres de données 10/40 Gbit/s
- Adaptez-vous à l'augmentation du niveau de service et garantissez la disponibilité et la protection des services et des ressources réseau

Partenaire de services

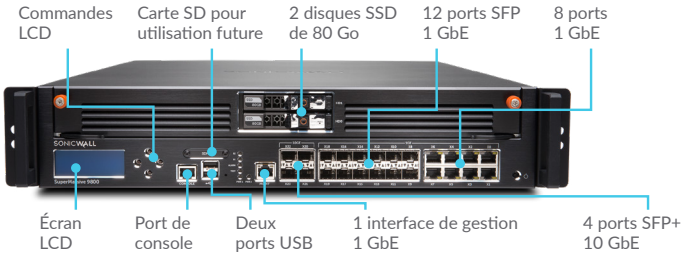
Besoin d'aide pour planifier, déployer ou optimiser votre solution SonicWall ? Le programme avancé Partenaire de services SonicWall a pour objectif de vous fournir des services professionnels de classe mondiale. Pour en savoir plus, rendez-vous sur www.sonicwall.com/PES.

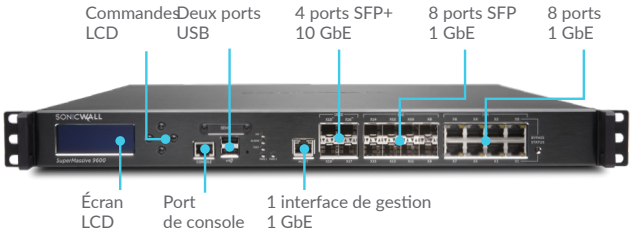
* Brevets américains 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361.

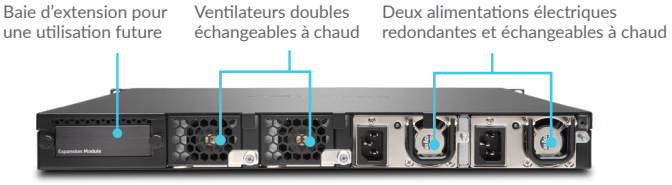
Gamme complète

La SuperMassive 9000 Series de SonicWall se compose des éléments suivants : 4 ports SFP+ 10 GbE, jusqu'à 12 ports SFP 1 GbE, 8 interfaces cuivre 1 GbE et de gestion 1 GbE, avec un port d'extension pour 2 interfaces SFP+ 10 GbE supplémentaires (version future). La série 9000 présente des modules de ventilation et des alimentations électriques échangeables à chaud.

SuperMassive 9000 Series





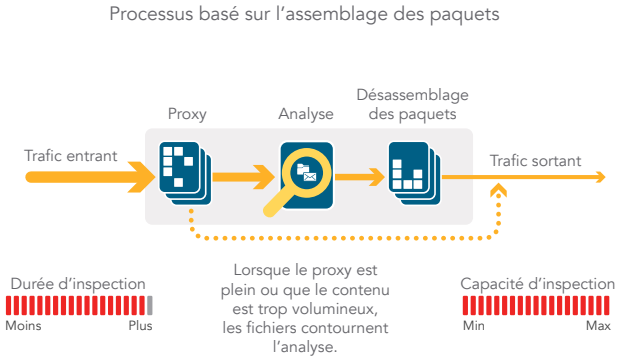


CAPACITÉS	9200	9400	9600	9800
Cœurs de traitement	24	32	32	64
Débit du pare-feu	15 Gbit/s	20 Gbit/s	20 Gbit/s	31,8 Gbit/s
Débit d'inspection des applications	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	23 Gbit/s
Débit du système de prévention des intrusions (IPS)	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	21,3 Gbit/s
Débit d'inspection des logiciels malveillants	3,5 Gbit/s	4,5 Gbit/s	5 Gbit/s	11 Gbit/s
Connexions DPI maximales	1,5 M	1,5 M	2,0 M	8,0 M
MODES DE DÉPLOIEMENT	**9200**	**9400**	**9600**	**9800**
Mode pont de couche 2	Oui	Oui	Oui	Oui
Mode filaire	Oui	Oui	Oui	Oui
Mode passerelle / NAT	Oui	Oui	Oui	Oui
Mode TAP	Oui	Oui	Oui	Oui
Mode transparent	Oui	Oui	Oui	Oui

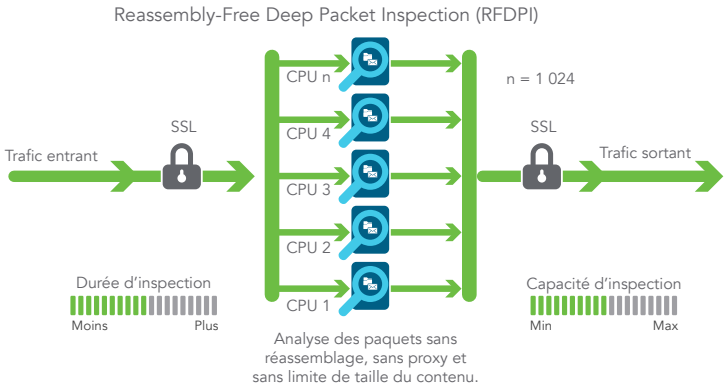
Moteur Reassembly-Free Deep Packet Inspection

La technologie RFDPI est un système d'inspection à faible latence en un seul passage qui effectue des analyses bidirectionnelles à grande vitesse des flux de trafic sans proxy ni mise en mémoire tampon pour détecter efficacement les tentatives d'intrusion et les logiciels malveillants et identifier le trafic applicatif, quel que soit le port ou le protocole utilisé. Ce moteur breveté s'appuie sur une inspection de la charge utile des flux de trafic pour détecter les menaces sur les couches 3 à 7. Il soumet les flux de données réseau à des opérations répétées et étendues de normalisation et de déchiffrement afin de neutraliser les techniques évoluées de brouillage et d'évasion visant à tromper les moteurs de détection pour introduire du code malveillant sur le réseau.

Une fois son traitement préalable (déchiffrement TLS/SSL compris) terminé, chaque paquet est analysé par rapport à une mémoire propriétaire unique rassemblant plusieurs bases de données de signatures : attaques par intrusion, logiciels malveillants, réseaux de zombies et applications. L'état de la connexion affiche la position des flux par rapport à ces bases de données jusqu'à identifier un état d'attaque ou tout autre événement pertinent, ce qui déclenche une action prédéfinie. Dans la plupart des cas, la connexion est interrompue et des événements de journalisation et de notification sont créés. Le moteur peut également être configuré pour l'inspection seulement ou, dans le cadre de la détection d'applications, pour fournir des services de gestion de la bande passante de couche 7 au reste du flux applicatif une fois l'application identifiée.



Architecture concurrente basée sur les proxys

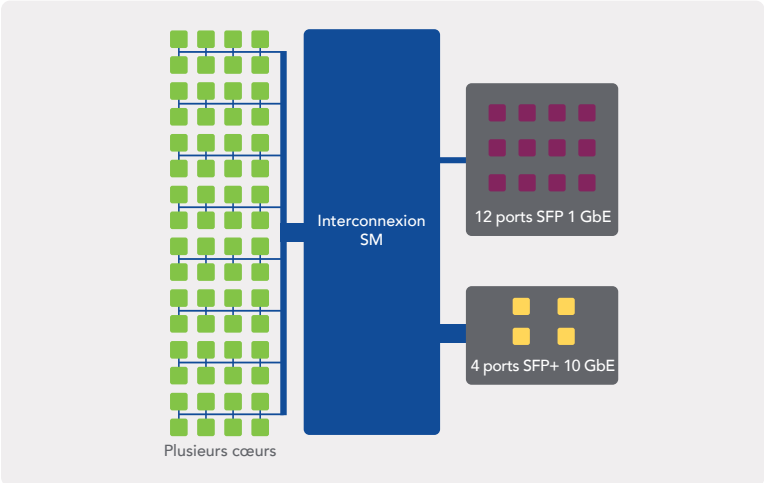


Architecture basée sur les flux SonicWall

Une architecture extensible offrant une évolutivité et des performances extrêmes

Le moteur RFDPI a été spécialement mis au point pour fournir une analyse de sécurité à un niveau élevé de performance, afin de tenir compte de la conception parallèle inhérente et de la nature en constante évolution du trafic réseau. Lorsqu'elle est associée à des systèmes de traitement dotés de plusieurs cœurs, cette architecture logicielle centrée sur le parallélisme évolue parfaitement pour répondre aux demandes d'inspection approfondie des paquets (DPI) à des charges de trafic élevées. La plateforme SuperMassive repose sur des processeurs qui, à la différence des processeurs x86, sont optimisés pour le traitement des paquets, du chiffrement et du réseau, tout en préservant la souplesse et la capacité de programmation sur le terrain, véritable point faible des systèmes ASIC.

Cette souplesse est cruciale lorsque de nouvelles mises à jour du code et des comportements s'avèrent nécessaires pour se prémunir de nouvelles attaques qui exigent des techniques de détection mises à jour et plus élaborées. La conception de la plateforme se différencie également par sa capacité unique à établir de nouvelles connexions sur n'importe quel cœur dans le système, offrant le nec plus ultra en matière d'évolutivité et la possibilité de gérer des pics de trafic. Cette approche génère des taux d'établissement de nouvelles sessions extrêmement élevés (en termes de nouvelles connexions par seconde) pendant que l'inspection approfondie des paquets est activée, considérés comme un indicateur majeur pour connaître l'encombrement lié aux déploiements des centres de données.

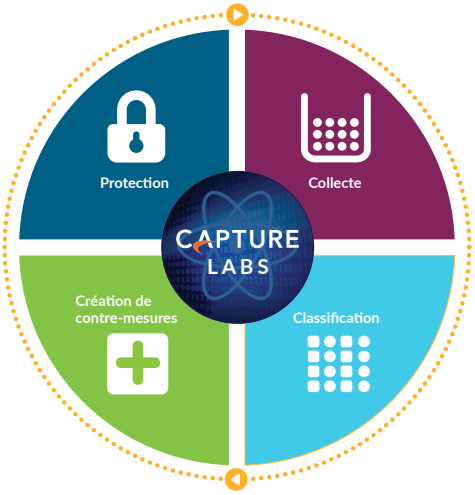


Capture Labs

L'équipe interne de recherche Capture Labs de SonicWall, qui a fait des menaces sa grande spécialité, étudie et élabore des contre-mesures pour déployer des pare-feux pour les clients afin qu'ils bénéficient d'une protection à jour. L'équipe recueille des données sur les menaces potentielles à partir de plusieurs sources, notamment notre service de sandboxing réseau primé, Capture Advanced Threat Protection, et via plus d'un million de capteurs SonicWall répartis dans le monde entier qui surveillent le trafic à la recherche de menaces émergentes. Les données sont analysées par apprentissage automatique grâce aux algorithmes d'apprentissage profond de SonicWall afin d'extraire l'ADN du code et ainsi déterminer s'il est associé à des formes connues de code malveillant.

Les clients dotés d'un pare-feu SonicWall de nouvelle génération avec les capacités de sécurité les plus récentes bénéficient d'une protection contre les menaces mise à jour en permanence. Les mises à jour sont actives immédiatement, sans redémarrage ni interruption. Les signatures sur les appareils offrent une protection contre de vastes catégories d'attaques, une seule signature suffisant à couvrir jusqu'à des dizaines de milliers de menaces individuelles.

Outre les moyens de lutte intégrés, les pare-feux SuperMassive ont accès à SonicWall CloudAV[1], qui vient compléter les défenses sur l'appareil par des dizaines de millions de signatures (des millions de signatures sont ajoutées chaque année). La base de données de CloudAV est accessible par le pare-feu via un protocole privé et léger afin de renforcer l'inspection réalisée sur l'appareil. Grâce à Capture Advanced Threat Protection[1], un service de sandboxing basé sur le cloud et multimoteur, les organisations peuvent examiner des fichiers et du code suspects dans un environnement isolé pour neutraliser les menaces avancées comme les attaques de type « zero-day ».



[1] *Nécessite un abonnement supplémentaire*

Protection contre les menaces évoluées

Deux technologies de détection avancée des programmes malveillants sont au cœur de la prévention des failles automatisée et en temps réel de SonicWall : Capture Advanced Threat Protection™ (Capture ATP) et Capture Security appliance™ (CSa).

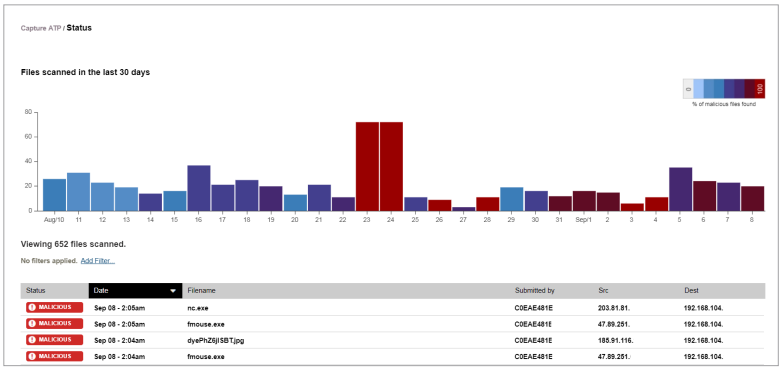
Capture ATP est une plateforme basée sur le cloud et multimoteur de sandboxing qui comprend Real-Time Deep Memory Inspection™ (RTDMI), un service virtualisé de sandboxing, une émulation complète du système et une technologie d'analyse au niveau de l'hyperviseur. CSa est un dispositif local doté de RTDMI, qui emploie des techniques statiques et dynamiques basées sur la mémoire pour rendre des verdicts rapidement et précisément. Les deux solutions étendent la protection contre les menaces avancées afin de détecter et d'empêcher les menaces de type « zero-day » dans différentes solutions SonicWall, comme les pare-feux de nouvelle génération.

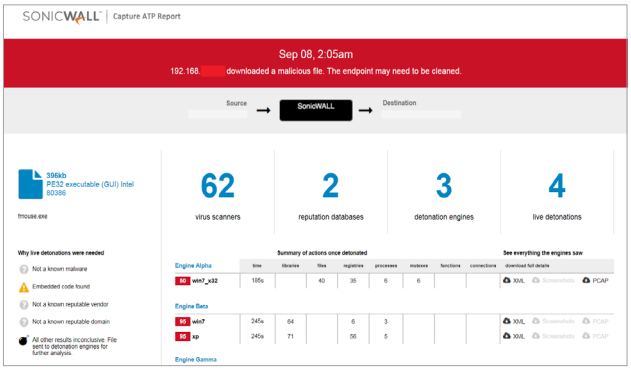
Les fichiers suspects sont envoyés dans l'une des solutions pour y être analysés à l'aide d'algorithmes d'apprentissage profond, avec possibilité de les retenir au niveau de la passerelle jusqu'à ce qu'un verdict soit rendu. Dans le cas de Capture ATP, lorsque les fichiers sont identifiés comme étant malveillants, ils sont bloqués et un hachage est immédiatement créé au sein de la base de données de Capture ATP pour permettre aux clients de bloquer toutes les attaques qui s'ensuivent.

Ces signatures finissent par être transmises aux pare-feux pour créer des défenses statiques. Les résultats générés par CSa ne sont pas partagés en dehors de votre entreprise pour des raisons de conformité et de respect de la vie privée.

Ces services analysent un vaste éventail de systèmes d'exploitation et de types de fichiers (notamment programmes exécutables, DLL, PDF, documents MS Office, archives, JAR et APK).

Pour une protection complète des terminaux, SonicWall Capture Client allie une technologie antivirus de nouvelle génération à un service de sandboxing multimoteur basé sur le cloud, avec la possibilité d'intégrer en sus les pare-feux de SonicWall.

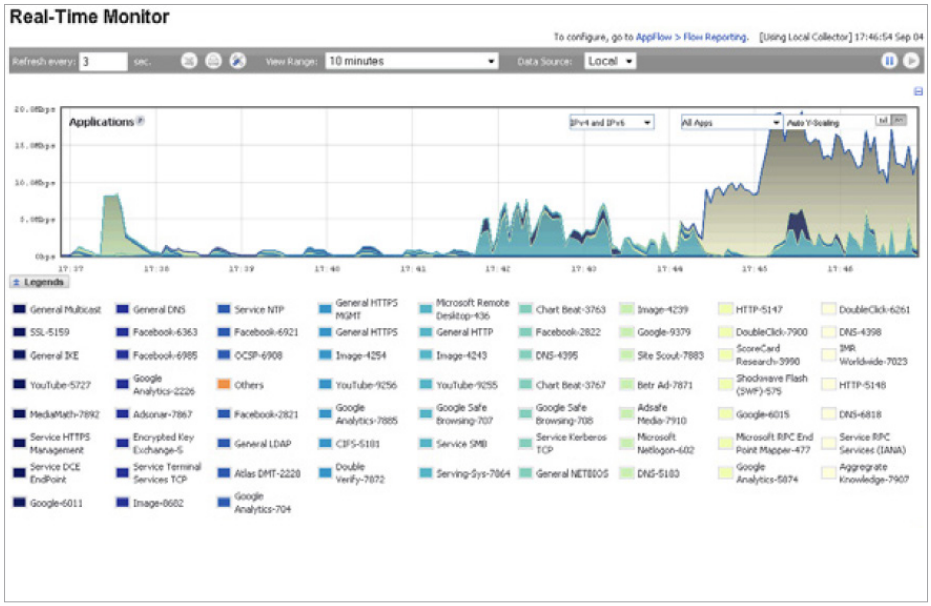




Surveillance et contrôle des applications

La surveillance des applications informe les administrateurs du trafic applicatif qui transite par leur réseau, de manière à ce qu'ils puissent programmer des contrôles des applications selon la priorité opérationnelle, limiter les applications non productives et bloquer les applications potentiellement dangereuses. La visualisation en temps réel identifie les anomalies de trafic au fur et à mesure qu'elles surviennent, ce qui permet d'élaborer immédiatement des mesures correctives contre les attaques potentielles entrantes ou sortantes ou contre les problèmes de performances.

SonicWall Application Traffic Analytics[1] confère une vision approfondie du trafic applicatif, de l'utilisation de la bande passante et des menaces pour la sécurité, tout en fournissant des capacités robustes de dépannage et d'investigation scientifique. En outre, les capacités sécurisées d'authentification unique (SSO) facilitent l'expérience des utilisateurs, augmentent la productivité et réduisent le nombre d'appels



de soutien technique. La gestion de la surveillance et du contrôle des applications est simplifiée par l'interface Web intuitive.

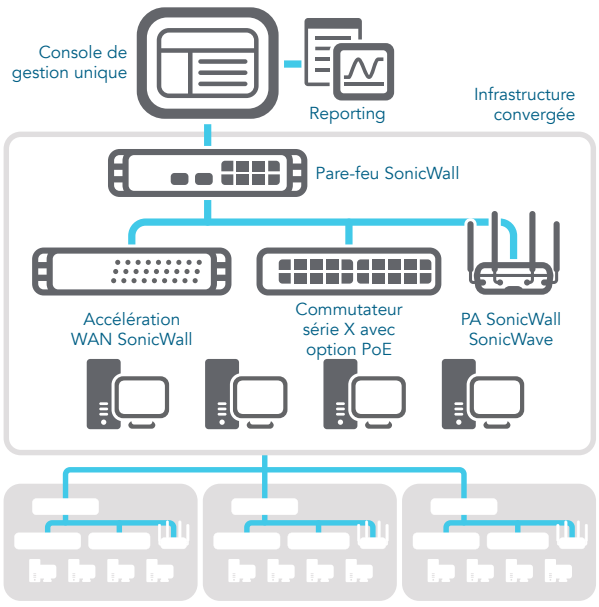
Gestion globale et élaboration de rapports

Pour les entreprises appartenant à des secteurs très réglementés et désireuses de coordonner parfaitement la gouvernance, la sécurité, la conformité et la stratégie de gestion des risques, SonicWall propose en option aux administrateurs une plateforme unifiée, sécurisée et extensible de gestion des pare-feux, points d'accès sans fil et commutateurs par le biais d'un flux de travail corrélé et vérifiable, et baptisée Global Management System[1] (GMS®). GMS permet aux entreprises de consolider facilement la gestion des appareils de sécurité, de réduire les complexités administratives et de dépannage et de contrôler tous les aspects opérationnels de l'infrastructure de sécurité, notamment la centralisation de la gestion et de l'application des règles, la surveillance des événements en temps réel, les activités des utilisateurs, l'identification des applications, l'analyse (y compris scientifique) des flux, l'élaboration de rapports d'audit et de conformité et bien plus encore. La solution GMS répond également aux besoins des entreprises en matière de gestion des modifications de pare-feu via une fonction d'automatisation du flux de travail. Grâce à cette fonction, toutes les entreprises bénéficieront d'une souplesse et d'une confiance dans le déploiement des règles de pare-feu adéquates, au moment opportun et dans le respect des réglementations sur la conformité. La solution GMS offre une manière cohérente de gérer la sécurité des réseaux par processus opérationnels et niveaux de service, ce qui simplifie grandement la gestion du cycle de vie de vos environnements de sécurité généraux par rapport à une gestion individuelle des appareils.

Conformité sécurisée aux exigences grâce à la solution GMS de SonicWall

Avantages

- Gestion centralisée
- Gestion des règles sans erreur
- Contrôle d'accès strict
- Pistes de vérification complètes
- Modèles de rapports PCI, HIPAA et SOX
- Coûts d'exploitation réduits



Évolutivité grâce à l'extension des ports

[1] *Nécessite un abonnement supplémentaire*

Fonctionnalités

MOTEUR RFDPI

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 de données 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
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	La SuperMassive Series prend en charge les modes haute disponibilité actif/passif (A/P) avec synchronisation de l'état, DPI actif/actif (A/A) et mise en cluster active/active. Le mode DPI actif/actif permet de décharger la charge DPI vers les cœurs sur 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.
Support IPv6	Le protocole IPv6 (Internet Protocol version 6) commence à remplacer le protocole IPv4. Avec la version la plus récente du système d'exploitation SonicOS (version 6.2), le matériel prendra en charge les implémentations en mode filaire et filtrage.
Options de déploiement flexibles	La SuperMassive Series peut être déployée en mode NAT traditionnel, pont de couche 2, filaire et TAP réseau.
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.
Gestion des commutateurs réseau Dell 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 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 identifiants de réseaux sociaux	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	Offre 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 ET ÉLABORATION DE RAPPORTS

Fonctionnalité	Description
Global Management System[1] (GMS)	La solution GMS de SonicWall surveille, configure et élabore des rapports sur plusieurs appareils SonicWall via une console de gestion unique dotée d'une interface intuitive, ce qui limite les coûts et la complexité en matière de gestion.
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.

Fonctionnalités

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-feux SonicWall. Sécurité et connectivité se mettent en place instantanément et automatiquement.
VPN pour la connectivité site à site	Le VPN IPSec hautes performances permet à la SuperMassive Series 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/ Citrix1/Terminal Services1 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.
Filtrage DPI 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.

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	Permet de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP.
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-feux 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 est une plateforme client unifiée fournissant diverses fonctionnalités de protection des terminaux, dont une protection anti-logiciels malveillants avancée et la visibilité sur le trafic chiffré. Elle repose sur des technologies de protection multicouche, un reporting complet et l'exécution automatique de la protection des terminaux.

CAPTURE SECURITY APPLIANCE (CSa)

Fonctionnalité	Description
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.
Intégrations préconçues	La solution CSa prend en charge des intégrations prêtes à l'emploi avec d'autres solutions de sécurité de SonicWall (pare-feux et systèmes de sécurisation de la messagerie électronique).
Protection quasiment en temps réel	La technologie brevetée RTDMI de SonicWall aide à détecter les logiciels malveillants rapidement, même ceux qui étaient préalablement inconnus, et la solution CSa peut les bloquer jusqu'à ce qu'un verdict soit rendu sur les pare-feux SonicWall de nouvelle génération.
Déploiement	La solution CSa peut être configurée sur un réseau privé directement relié à un pare-feu périphérique particulier ou être accessible via Internet directement ou en utilisant un VPN par les pare-feux de succursales.

PROTECTION CONTRE LES MENACES CHIFFRÉES[1]

Fonctionnalité	Description
Déchiffrement et inspection TLS/SSL	Déchiffre et inspecte le trafic chiffré SSL/TLS 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 adresses URL et des applications afin de contrer les menaces dissimulées dans le trafic chiffré TLS/SSL. Inclus avec les abonnements de sécurité pour tous les modèles.
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.

Fonctionnalités

PRÉVENTION CONTRE LES INTRUSIONS[1] (SUITE)	
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.
Détection et prévention des 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.

PROTECTION CONTRE LES 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 contre les programmes malveillants CloudAV	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 est capable d'analyser les flux TCP bruts sur tous les ports de manière bidirectionnelle, empêchant ainsi les attaques visant à contourner les systèmes de sécurité obsolètes qui sécurisent uniquement quelques ports connus.
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, et décode les charges utiles, qu'elles soient ou non exécutées sur des ports standard connus, pour identifier les logiciels malveillants.

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 pour renforcer 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 afin 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 contenant des informations ou des images répréhensibles ou non productives via le Service de filtrage du contenu.
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 les contenus à l'aide de catégories prédéfinies ou d'associations 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.

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 dispose de la version la plus récente des signatures antivirus et anti-logiciels espions installées et actives, ce qui élimine les coûts habituellement associés à la gestion des antivirus et des anti-logiciels espions 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 les frais administratifs.
Protection contre les virus automatique et toujours active	Des mises à jour fréquentes des antivirus et anti-logiciels espions sont fournies en toute transparence sur l'ensemble des ordinateurs de bureau et les serveurs de fichiers pour accroître la productivité des utilisateurs finaux et limite la gestion en matière de sécurité.
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] *Nécessite un abonnement supplémentaire*

Résumé des fonctionnalités

Pare-feu

- Inspection d'état 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[2]

- Inspection approfondie des paquets pour TLS/SSL/SSH
- Inclusion/exclusion d'objets, de groupes ou de noms d'hôtes
- Contrôle SSL

Capture Advanced Threat Protection[2]

- 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 contre les intrusions[2]

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

Anti-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
- Visualisation du trafic applicatif
- Blocage des composants applicatifs
- 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
- Suivi de l'activité des utilisateurs (SSO)
- Base de données complète des signatures d'applications

Filtrage du contenu Web[2]

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

VPN

- 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 (OSPF, RIP, BGP)

Gestion de réseau

- Agrégation de liens dynamique avec LACP
- PortShield
- Trames Jumbo
- Détection MTU
- Journalisation améliorée
- Jonction VLAN
- Mise en miroir des ports
- Qualité de service de couche 2
- Sécurité des ports
- Routage dynamique (RIP/OSPF/BGP)
- Contrôleur sans fil SonicWall
- Routage à base de règles (ToS/métrique et ECMP)
- NAT
- Serveur DHCP
- Gestion de la bande passante
- Agrégation de liens (statique et dynamique)
- Redondance de ports
- Haute disponibilité A/P avec synchro. d'état
- Clustering A/A
- Équilibrage de la charge entrante/ sortante
- Mode pont de couche 2, mode filaire/filaire virtuel, mode TAP, mode NAT
- Basculement WAN 3G/4G (hormis SuperMassive 9800)
- Routage asymétrique
- Prise en charge Common Access Card (CAC)

Sans fil

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

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

- GMS, Web, interface utilisateur, interface de ligne de commande, API REST, SNMPv2/v3
- Journalisation
- Exportation NetFlow/IPFix
- Sauvegarde cloud de la configuration
- Plateforme d'analyse de sécurité BlueCoat
- Gestion des points d'accès SonicWall
- Gestion des commutateurs Dell série N et série X[1]

[1] *Fonction non prise en charge sur les pare-feux SuperMassive 9800*
[2] *Requiert un abonnement supplémentaire*

Spécifications système des pare-feux de la SuperMassive 9000 Series

GÉNÉRALITÉS DES PARE-FEUX	9200	9400	9600	9800
Système d'exploitation	SonicOS			
Cœurs de traitement de la sécurité	24	32		64
Interfaces	4 ports SFP+ 10 GbE, 8 ports SFP 1 GbE, 8 ports 1 GbE, port de gestion 1 GbE, 1 console			4 ports SFP+ 10 GbE, 12 ports SFP 1 GbE, 8 ports 1 GbE, port de gestion 1 GbE, 1 console
Mémoire (RAM)	8 Go	16 Go	32 Go	64 Go
Stockage	Mémoire flash			2 disques SSD de 80 Go, Flash
Extension	1 connecteur d'extension (à l'arrière)*, logement pour carte SD*			
Gestion	CLI, SSH, GUI, GMS			
Utilisateurs de l'authentification unique (SSO)	80 000	90 000	100 000	110 000
Max. de points d'accès pris en charge	128			-
Journalisation	Analyzer, Local Log, Syslog			
Haute disponibilité	Active/passive avec synchro. d'état, DPI actif/actif avec synchro. d'état			
PERFORMANCES PARE-FEU/VPN	**9200**	**9400**	**9600**	**9800**
Débit d'inspection du pare-feu[1]	15 Gbit/s	20 Gbit/s	20 Gbit/s	31,8 Gbit/s
Débit prévention des menaces[2]	3 Gbit/s	4,4 Gbit/s	4,5 Gbit/s	10,5 Gbit/s
Débit d'inspection des applications[2]	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	23 Gbit/s
Débit IPS[2]	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	21,3 Gbit/s
Débit d'inspection des logiciels malveillants[1]	3,5 Gbit/s	4,5 Gbit/s	5,0 Gbit/s	11 Gbit/s
Débit IMIX	4,4 Gbit/s	5,5 Gbit/s	5,5 Gbit/s	7,3 Gbit/s
Débit d'inspection et de déchiffrement SSL (DPI-SSL)[2]	1,0 Gbit/s	2,0 Gbit/s	2,0 Gbit/s	3,5 Gbit/s
Débit VPN[3]	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	14,3 Gbit/s
Connexions par seconde	100 000/s	130 000/s	130 000/s	229 000/s
Nombre maximum de connexions (SPI)	5.0M	7.5M	10.0M	20.0M
Nombre maximum de connexions (DPI)	1,5 million	1,5 million	2.0M	8.0M
Connexions DPI SSL[6] (nombre maximal)	8 000 (15 500[6])	10 000 (17 500[6])	12 000 (22 500[6])	650 000
VPN	**9200**	**9400**	**9600**	**9800**
Tunnels VPN site à site	10 000			25 000
Clients VPN IPSec (maximum)	2 000 (4 000)	2 000 (6 000)		2 000 (10 000)
Clients VPN SSL NetExtender (nombre maximal)	2 (3 000)	2 (3 000)	50 (3 000)	50 (3 000)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B, carte CAC (Common Access Card)			
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v			
VPN basé sur le routage	RIP, OSPF			
GESTION DE RÉSEAU	**9200**	**9400**	**9600**	**9800**
Attribution d'adresses IP	Statique, DHCP, PPPoE, L2TP et client PPTP, serveur DHCP interne, relais DHCP[4]			
Modes NAT	1 à 1, plusieurs à 1, 1 à plusieurs, NAT flexible (adresses IP superposées), PAT, mode transparent			
Interfaces VLAN	512			
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage à base de règles, multidiffusion			
Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1p			
Authentification	LDAP (domaines multiples), XAUTH/RADIUS, SSO, Novell, base de données utilisateurs interne, Terminal Services[5], Citrix[5]			
VoIP	H323/v1-5 complet, SIP			
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications	UC APL[4], pare-feu d'entreprise ICSA, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2[4], NDPP Common Criteria[4], antivirus ICSA[4]			
MATÉRIEL	**9200**	**9400**	**9600**	**9800**
Alimentation électrique	Double, redondante et échangeable à chaud, 300 W			Double, redondante et échangeable à chaud, 500 W
Ventilateurs	Doubles, redondants et échangeables à chaud			
Écran	Écran LED à l'avant			
Puissance d'entrée	100 à 240 V CA, 50-60 Hz			
Consommation électrique maximale (W)	200			350
MTBF @25°C en heures	188 719	187 702	186 451	126 144
MTBF @25°C en années	21,53	21,43	21,28	14,40
Format	1U pouvant être monté sur châssis			2U pouvant être monté sur châssis
Dimensions	43,3 x 48,5 x 4,5 cm			9 x 60 x 43 cm
Poids	8,2 kg (18,1 lb)			18,38 kg (40,5 lb)
Poids DEEE	10,4 kg (23 lb)			22,4 kg (49,5 lb)
Poids avec emballage	13,3 kg (29,3 lb)			29,64 kg (65 lb)
Réglementations majeures	FCC classe A, ICES classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI classe A, UL/cUL, TÜV/ GS, CB, Mexico CoC par UL, DEEE, REACH, BSMI, KCC/MSIP, ANATEL			
Environnement	15 à 40 °C			
Taux d'humidité	10 à 90 % sans condensation			

[1] Méthodes de test : performances maximales basées sur RFC 2544 (pour pare-feu). Les performances réelles peuvent varier en fonction des conditions réseau et des services activés. [2] Débit de prévention des menaces/antivirus de passerelle/anti-logiciels espions/IPS mesuré en utilisant les tests de performance HTTP Spirent WebAvalanche et les outils de test Ixia conformes aux standards actuels. Tests réalisés avec plusieurs flux sur plusieurs paires de ports. Débit de prévention des menaces mesuré en ayant activé l'antivirus de passerelle, l'anti-spyware, l'IPS et le contrôle des applications. [3] Débit VPN mesuré à l'aide du trafic UDP avec une taille de paquet de 1 280 octets [4] S'applique aux pare-feux de la série SuperMassive 9200, 9400 et 9600. La certification UC APL pour les pare-feux SuperMassive 9800 est en cours d'obtention. [5] Fonction prise en charge sur SonicOS 6.1 et 6.2. [6] Pour 125 000 connexions DPI réduites, le nombre de connexions DPI SSL disponibles augmente de 750. * Utilisation future. Sous réserve de modification des spécifications, des fonctionnalités et de la disponibilité.

Informations de commande des pare-feux SuperMassive 9000 Series

PRODUIT	RÉFÉRENCE
SuperMassive 9800 Total Secure Advanced Edition (1 an)	01-SSC-0312
SuperMassive 9600 Total Secure Advanced Edition (3 ans)	02-SSC-0410
SuperMassive 9400 Total Secure Advanced Edition (3 ans)	02-SSC-0409
SuperMassive 9200 Total Secure Advanced Edition (3 ans)	02-SSC-0408
ABONNEMENTS D'ASSISTANCE ET DE SÉCURITÉ POUR LE PARE-FEU SUPERMASSIVE 9200	**RÉFÉRENCE**
Advanced Gateway Security Suite – Capture ATP, prévention des menaces, gestion et reporting des pare-feux, visibilité du « shadow IT » et assistance 24 h/24, 7 j/7 pour le pare-feu SuperMassive 9200 (1 an)	01-SSC-1570
Capture Advanced Threat Protection pour le pare-feu SuperMassive 9200 (1 an)	01-SSC-1575
Comprehensive Gateway Security Suite : Surveillance des applications, Prévention des menaces, Filtrage du contenu avec assistance pour le pare-feu SuperMassive 9200 (1 an)	01-SSC-4172
Prévention des intrusions, Anti-logiciels malveillants, CloudAV, Surveillance des applications, Contrôle et visualisation pour le pare-feu SuperMassive 9200 (1 an)	01-SSC-4202
Content Filtering Premium Business Edition pour le pare-feu SuperMassive 9200 (1 an)	01-SSC-4184
Assistance Platine pour le pare-feu SuperMassive 9200 (1 an)	01-SSC-4178
ABONNEMENTS D'ASSISTANCE ET DE SÉCURITÉ POUR LE PARE-FEU SUPERMASSIVE 9400	**RÉFÉRENCE**
Advanced Gateway Security Suite – Capture ATP, prévention des menaces, gestion et reporting des pare-feux, visibilité du « shadow IT » et assistance 24 h/24, 7 j/7 pour le pare-feu SuperMassive 9400 (1 an) feux	01-SSC-1580
Capture Advanced Threat Protection pour le pare-feu SuperMassive 9400 (1 an)	01-SSC-1585
Comprehensive Gateway Security Suite : Surveillance des applications, Prévention des menaces, Filtrage du contenu avec assistance pour le pare-feu SuperMassive 9400 (1 an)	01-SSC-4136
Prévention des intrusions, Anti-logiciels malveillants, CloudAV, Surveillance des applications, Contrôle et visualisation pour le pare-feu SuperMassive 9400 (1 an)	01-SSC-4166
Content Filtering Premium Business Edition pour le pare-feu SuperMassive 9400 (1 an)	01-SSC-4148
Assistance Platine pour le pare-feu SuperMassive 9400 (1 an)	01-SSC-4142
ABONNEMENTS D'ASSISTANCE ET DE SÉCURITÉ POUR LE PARE-FEU SUPERMASSIVE 9600	**RÉFÉRENCE**
Advanced Gateway Security Suite – Capture ATP, prévention des menaces, gestion et reporting des pare-feux, visibilité du « shadow IT » et assistance 24 h/24, 7 j/7 pour le pare-feu SuperMassive 9600 (1 an)	01-SSC-1590
Capture Advanced Threat Protection pour le pare-feu SuperMassive 9600 (1 an)	01-SSC-1595
Comprehensive Gateway Security Suite : Surveillance des applications, Prévention des menaces, Filtrage du contenu avec assistance pour le pare-feu SuperMassive 9600 (1 an)	01-SSC-4100
Prévention des intrusions, Anti-logiciels malveillants, CloudAV, Surveillance des applications, Contrôle et visualisation pour le pare-feu SuperMassive 9600 (1 an)	01-SSC-4130
Content Filtering Premium Business Edition pour le pare-feu SuperMassive 9600 (1 an)	01-SSC-4112
Assistance Platine pour le pare-feu SuperMassive 9600 (1 an)	01-SSC-4106
ABONNEMENTS D'ASSISTANCE ET DE SÉCURITÉ POUR LE PARE-FEU SUPERMASSIVE 9800	**RÉFÉRENCE**
Advanced Gateway Security Suite – Capture ATP, prévention des menaces, gestion et reporting des pare-feux, visibilité du « shadow IT » et assistance 24 h/24, 7 j/7 pour le pare-feu SuperMassive 9800 (1 an)	01-SSC-1183
Capture Advanced Threat Protection pour le pare-feu SuperMassive 9800 (1 an)	01-SSC-1188
Comprehensive Gateway Security Suite : Surveillance des applications, Prévention des menaces, Filtrage du contenu avec assistance pour le pare-feu SuperMassive 9800 (1 an)	01-SSC-0809
Prévention des intrusions, Anti-logiciels malveillants, CloudAV, Surveillance des applications, Contrôle et visualisation pour le pare-feu SuperMassive 9800 (1 an)	01-SSC-0827
Content Filtering Premium Business Edition pour le pare-feu SuperMassive 9800 (1 an)	01-SSC-0821
Assistance Or 24 h/24, 7 j/7 pour le pare-feu SuperMassive 9800 (1 an)	01-SSC-0815
MODULES ET ACCESSOIRES*	**RÉFÉRENCE**
FRU ventilateur système pour le pare-feu SuperMassive 9800 Series de SonicWall	01-SSC-0204
FRU alimentation électrique CA pour le pare-feu SuperMassive 9800 Series de SonicWall	01-SSC-0203
FRU ventilateur système pour le pare-feu SuperMassive 9000 Series de SonicWall	01-SSC-3876
FRU alimentation électrique CA pour le pare-feu SuperMassive 9000 Series de SonicWall	01-SSC-3874
Module à courte portée 10GBASE-SR SFP+	01-SSC-9785
Module à longue portée 10GBASE-LR SFP+	01-SSC-9786
Module à courte portée 1000BASE-SX SFP	01-SSC-9789
Module à longue portée 1000BASE-LX SFP	01-SSC-9790
Module cuivre 1000BASE-T SFP	01-SSC-9791
GESTION ET CRÉATION DE RAPPORTS	**RÉFÉRENCE**
Licence logicielle GMS SonicWall pour 10 nœuds	01-SSC-3363
Assistance logicielle 24 h/24 et 7 j/7 pour la classe E de GMS SonicWall pour 10 nœuds (1 an)	01-SSC-6514
Appareil virtuel SonicWall Scrutinizer avec licence logicielle Flow Analytics Module pour un maximum de 5 nœuds (comprend une assistance logicielle 24 h/24 et 7 j/7 d'un an)	01-SSC-3443
SonicWall Scrutinizer avec licence logicielle Flow Analytics Module pour un maximum de 5 nœuds (comprend une assistance logicielle 24 h/24 et 7 j/7 d'un an)	01-SSC-4002
Licence logicielle Advanced Reporting Module pour SonicWall Scrutinizer pour un maximum de 5 nœuds (comprend une assistance logicielle 24 h/24 et 7 j/7 d'un an)	01-SSC-3773

** Veuillez contacter un représentant de SonicWall pour obtenir la liste complète des modules SFP et SFP+ pris en charge.*

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

Datasheet-SuperMassive-US-COG-2465