Pare-feux SonicWall SuperMassive Series

Des pare-feux de nouvelle génération hautes performances pour une protection sans concession de votre réseau d'entreprise.

La série SonicWall SuperMassive constitue la plateforme de pare-feux de nouvelle génération de SonicWall conçus pour fournir aux vastes réseaux une évolutivité, une fiabilité et une sécurité maximum à des débits multi-gigabits, sans pratiquement aucune latence.

Construits pour répondre aux besoins des entreprises, administrations, établissements scolaires ou de santé, commerces de détail et fournisseurs de services, les pare-feux SuperMassive Series se prêtent idéalement à la sécurisation des réseaux distribués, des centres de données et des fournisseurs de services.

Alliant le système d'exploitation SonicOS, la technologie brevetée* RFDPI (Reassembly-Free Deep Packet Inspection®) et une architecture matérielle multicœur extrêmement évolutive, les pare-feux SuperMassive 9000 Series assurent des fonctionnalités de pointe en matière de contrôle des applications, de prévention des intrusions, de protection anti-malware et de déchiffrement et inspection TLS/SSL à des débits multi-gigabits. Bien pensée, la gamme SuperMassive Series tient compte des contraintes d'alimentation, d'espace et de refroidissement, ce qui garantit le meilleur rapport Gbit/s par watt du secteur en matière de traitement hautes performances des paquets et des données, de contrôle des applications et de prévention des menaces.

Le moteur RFDPI SonicWall analyse chaque octet de chaque paquet sur tous les ports. Il permet ainsi d'inspecter les contenus de l'ensemble du flux de données tout en offrant de hautes performances et une faible latence. Cette technologie est plus efficace que les configurations de proxy qui réassemblent le contenu à l'aide de sockets liés à des programmes de protection contre les logiciels malveillants inefficaces et surchargés par le vidage de la mémoire des sockets. Ces solutions obsolètes engendrent une forte latence, de faibles performances et une limite de la taille des fichiers. Le moteur RFDPI assure un filtrage complet des contenus en vue d'éliminer les logiciels malveillants de toute sorte avant qu'ils n'atteignent le réseau et protège contre des menaces en constante mutation, sans aucune restriction que ce soit en termes de taille des fichiers, de performances ou de délais.

Il opère également le déchiffrement et l'inspection du trafic chiffré TLS/SSL et SSH et des applications pour lesquelles il est impossible d'installer un proxy, assurant ainsi une protection complète, quel que soit le transport ou le protocole. Il procède à une inspection approfondie de chaque paquet (l'en-tête et la partie données) pour déceler la non-conformité aux protocoles, les menaces, les attaques zero-day, les intrusions et même des critères définis pour détecter et prévenir les attaques dissimulées dans le trafic chiffré. Il interrompt la propagation des infections et contre les communications C&C (commande et contrôle) et l'exfiltration de 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.

L'analyse du trafic des applications permet d'identifier le trafic productif et non productif des applications en temps réel, qui peut ensuite être contrôlé par de puissantes règles au niveau des applications. Le contrôle des applications peut être exercé par utilisateur et par groupe, avec possibilité de planifier ou d'ajouter des listes d'exception. Toutes les signatures de logiciels malveillants, d'applications et de prévention des intrusions sont constamment mises à jour par l'équipe de recherche SonicWall Capture Labs. De plus, le système d'exploitation avancé SonicOS dédié fournit des outils intégrés qui permettent de contrôler et d'identifier les applications personnalisées.

SuperMassive 9000 Series

Avantages :

- Profitez d'une défense complète alliant prévention hautes performances des intrusions, protection contre les logiciels malveillants à faible latence et sandboxing cloud
- Bénéficiez de l'exhaustivité et de la précision d'identification, de contrôle et de visualisation des applications
- Trouvez et bloquez les menaces dissimulées grâce au déchiffrement et à l'inspection du trafic chiffré TLS/SSL et SSH, sans impact sur les performances
- Adaptez les performances de sécurité aux centres de données 10/40 Gbit/s
- Suivez les augmentations de niveau de service et garantissez la disponibilité et la protection des services et des ressources

Partner Enabled Services

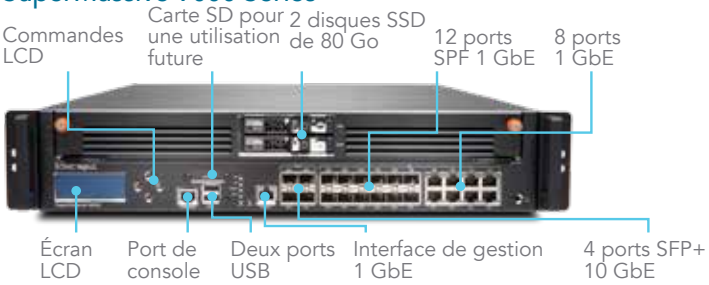
Vous avez besoin d'aide pour planifier, déployer et optimiser votre solution SonicWall ? Les partenaires SonicWall Advanced Services sont spécialement formés pour vous offrir des services professionnels de premier ordre. Pour en savoir plus, rendez-vous sur www.sonicwall.com/PES.

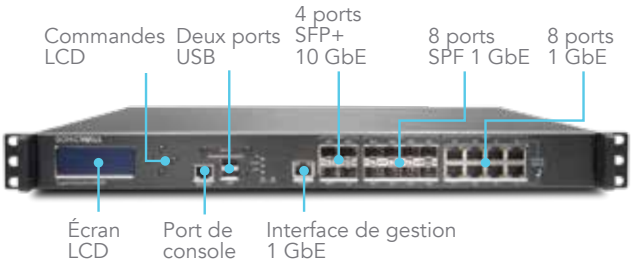
** Brevets U.S. n° 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361*

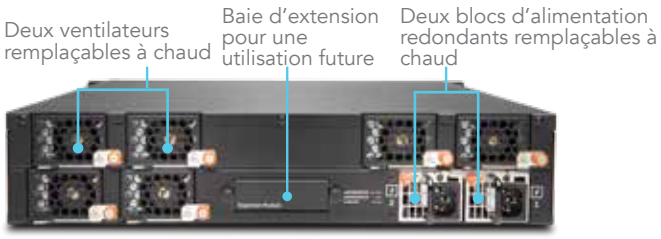
La série en bref

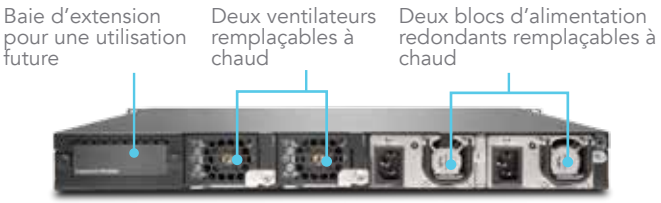
Le modèle SonicWall SuperMassive 9000 Series possède 4 ports SFP+ 10 GbE, jusqu'à 12 ports SFP 1 GbE, 8 ports cuivre 1 GbE et une interface de gestion 1 GbE, ainsi qu'un port d'extension pour 2 interfaces SFP+ 10 GbE supplémentaires (version ultérieure). Le pare-feu SuperMassive 9000 Series comprend des blocs d'alimentation et des modules de ventilation remplaçables à chaud.

SuperMassive 9000 Series







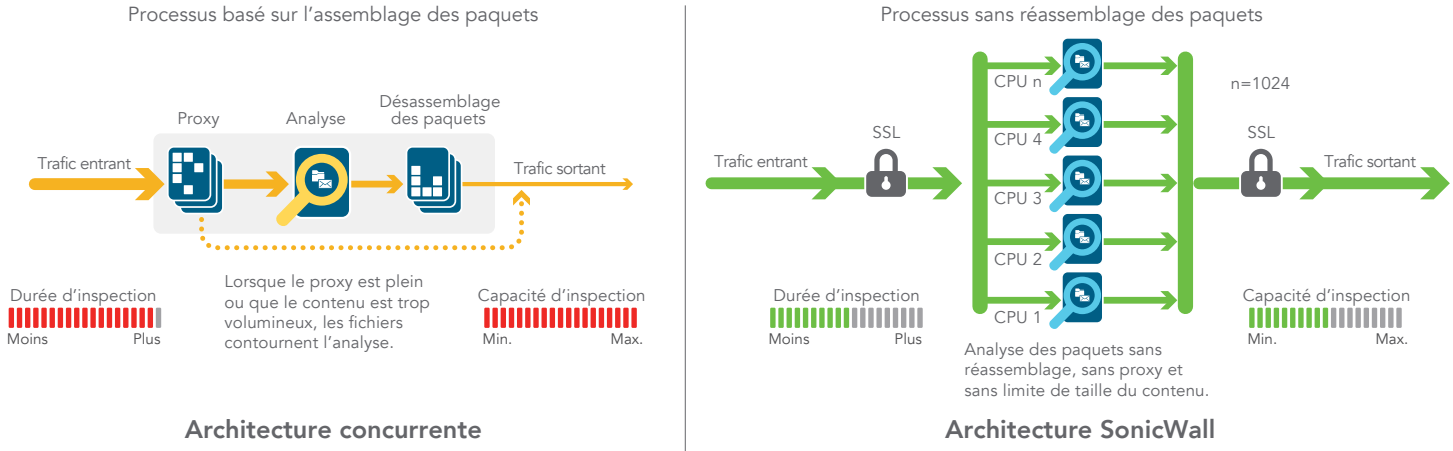


Fonctionnalité	9200	9400	9600	9800
Cœurs de processeur	24	32	32	64
Débit du pare-feu	15 Gbit/s	20 Gbit/s	20 Gbit/s	31,8 Gbit/s
Débit d'inspection approfondie des paquets	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	23 Gbit/s
Débit du système de prévention des intrusions (IPS)	5 Gbit/s	10 Gbit/s	11,5 Gbit/s	21,3 Gbit/s
Débit d'inspection anti-malware	3,5 Gbit/s	4,5 Gbit/s	5 Gbit/s	11 Gbit/s
Connexions DPI (max.)	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, quels que soient le port ou le protocole. Ce moteur propriétaire 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 réseau à des opérations répétées et étendues de normalisation et de déchiffrement afin de neutraliser les techniques d'obscurcissement et d'évasion évoluées visant à tromper les moteurs de détection pour introduire du code malveillant sur le réseau.

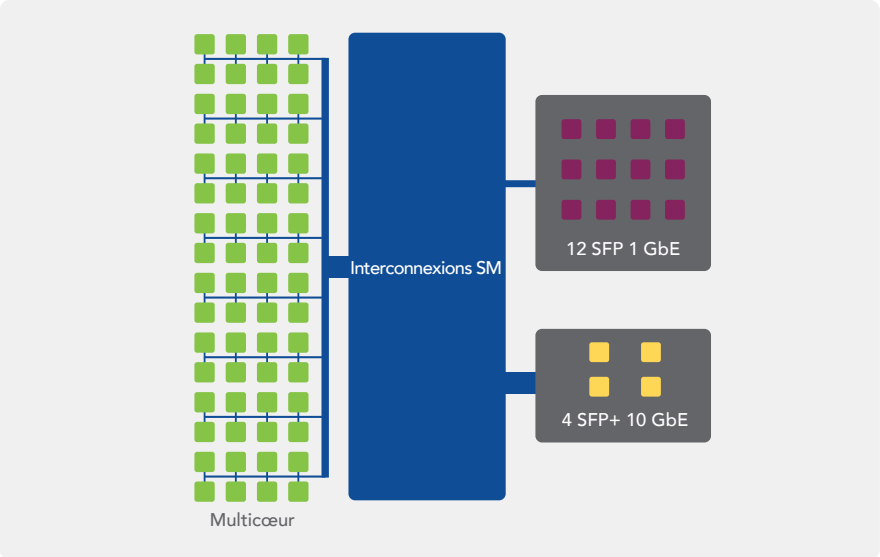
Une fois son prétraitement (déchiffrement TLS/SSL compris) terminé, chaque paquet est analysé par rapport à une mémoire propriétaire unique rassemblant plusieurs bases de données de signatures : attaques par intrusion, logiciels malveillants, botnets et applications. L'état de la connexion affiche la 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 extensible pour une évolutivité et des performances maximum

Le moteur RFDPI est conçu spécifiquement pour fournir des analyses de sécurité ultraperformantes afin de répondre à la nature à la fois parallèle et croissante du trafic réseau. Associée à des systèmes dotés de processeurs multicœurs, cette architecture logicielle centrée sur le parallélisme est facilement extensible pour s'adapter aux demandes d'inspection approfondie des paquets (DPI, Deep Packet Inspection) lorsque les charges de trafic sont élevées. La plateforme SuperMassive repose sur des processeurs qui, contrairement aux systèmes x86, sont optimisés pour le traitement des paquets, du chiffrement et du réseau tout en offrant flexibilité et programmabilité sur le terrain, un point faible pour les systèmes ASIC.

Cette flexibilité est essentielle lorsque du nouveau code et des mises à jour de comportement sont nécessaires pour lutter contre les nouvelles attaques exigeant des techniques de détection actualisées et plus sophistiquées. Un autre aspect de la conception de la plateforme est sa capacité unique à établir de nouvelles connexions sur tout cœur du système, ce qui lui permet d'offrir une extensibilité inégalée et de gérer les pics de trafic. Outre la capacité à exécuter la technologie DPI, cette approche permet d'obtenir des taux d'établissement de nouvelles sessions extrêmement élevés (nouvelles connexions par seconde), un indicateur clé qui représente souvent un goulet d'étranglement pour les déploiements au sein des centres de données.



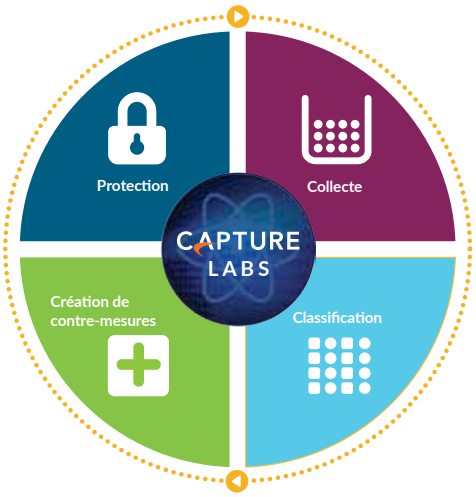
SONICWALL®

Capture Labs

L'équipe spécialisée de recherche sur les menaces SonicWall Capture Labs étudie et développe des contre-mesures qui seront déployées sur les pare-feux client pour une protection actualisée. Cette équipe collecte des données sur les menaces potentielles à partir de plusieurs sources dont notre service de sandboxing réseau primé, Capture Advanced Threat Protection, ainsi que plus de 1 million de capteurs SonicWall répartis dans le monde entier pour surveiller le trafic et y détecter les menaces émergentes. Les données sont analysées automatiquement via les algorithmes d'apprentissage SonicWall afin d'extraire l'ADN du code et savoir s'il est lié à une forme connue de code malveillant.

Les détenteurs de pare-feux de nouvelle génération SonicWall bénéficient des toutes dernières fonctionnalités de sécurité et d'une mise à jour en continu de leur protection, 24 heures/24. Les nouvelles mises à jour prennent effet immédiatement, sans redémarrage ni interruption. Les signatures sur les appliances offrent une protection contre un grand nombre d'attaques. Chaque signature peut couvrir jusqu'à plusieurs dizaines de milliers de menaces.

Outre les contre-mesures déployées sur l'appliance, les pare-feux SuperMassive ont également accès au SonicWall CloudAV[1], qui complète la base de données de signatures intégrée par des dizaines de millions d'autres signatures, un chiffre qui augmente lui-même de plusieurs millions chaque année. Le pare-feu accède à cette base de données CloudAV via un protocole léger propriétaire pour optimiser l'inspection réalisée sur l'appliance. Avec Capture Advanced Threat Protection[1], une sandbox multimoteur cloud, les entreprises peuvent examiner les fichiers et le code suspects dans un environnement isolé afin de stopper les menaces évoluées telles que les attaques zero-day.



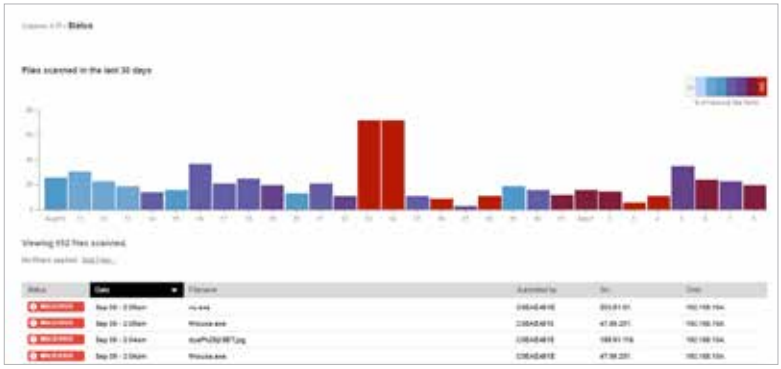
[1] *Requiert un abonnement supplémentaire*

Protection contre les menaces évoluées

Le service SonicWall Capture Advanced Threat Protection[1] est une sandbox multimoteur cloud qui complète le travail de protection du pare-feu en détectant et en évitant les attaques zero-day. Les fichiers suspects sont envoyés dans le cloud pour y être analysés, avec possibilité de les retenir à la passerelle jusqu'à ce qu'un verdict soit rendu. 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. Lorsqu'un fichier est identifié comme étant malveillant, un hachage est immédiatement créé dans Capture et une signature est ensuite envoyée aux pare-feux pour empêcher toute infiltration plus poussée.

Le service analyse un vaste éventail de systèmes d'exploitation et de types de fichiers, notamment programmes exécutables, DLL, PDF, documents MS Office, archives, JAR et APK.

Capture fournit un tableau de bord concis de l'analyse des menaces, ainsi que des rapports détaillant les résultats d'analyse des fichiers envoyés au service, à savoir source, destination et récapitulatif ainsi que les détails relatifs à l'action des programmes malveillants une fois déclenchés.



SONICWALL

Surveillance et contrôle des applications

La surveillance des applications informe les administrateurs du trafic applicatif circulant sur leur réseau. Ils peuvent ainsi planifier le contrôle des applications en fonction des priorités de l'entreprise, limiter les applications non productives et bloquer les applications potentiellement dangereuses. La visualisation en temps réel identifie les anomalies du trafic dès qu'elles surviennent, permettant de prendre des contre-mesures immédiates contre les attaques entrantes ou sortantes potentielles ou les goulets d'étranglement des performances.

SonicWall Application Traffic Analytics[1] fournit des informations granulaires sur le trafic applicatif, l'utilisation de la bande passante et les menaces de sécurité, ainsi que de puissantes fonctionnalités de dépannage et d'analyse forensique. En outre, les fonctions d'authentification unique (Single Sign-On, SSO) simplifient l'expérience utilisateur, augmentent la productivité et réduisent les appels de support. La gestion de la surveillance et du contrôle des applications est facilitée par l'utilisation d'une interface Web intuitive.

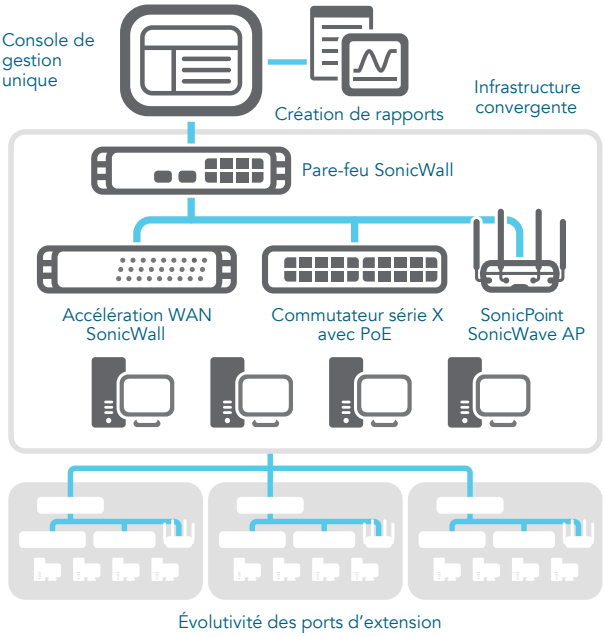
Gestion globale et reporting

Pour les entreprises appartenant à des secteurs très réglementés désireuses de coordonner parfaitement la gouvernance, la sécurité, la conformité et la stratégie de gestion des risques, la solution SonicWall Global Management System[1] (GMS®) en option offre aux administrateurs une plateforme de gestion des pare-feux, points d'accès sans fil et commutateurs SonicWall par le biais d'un workstream corrélé et vérifiable. La solution GMS permet aux entreprises de consolider aisément la gestion des appliances 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 forensique des flux, la création de rapports d'audit et de conformité et plus encore. La solution GMS répond également aux besoins des entreprises en matière de gestion des modifications de pare-feu via une fonctionnalité d'automatisation du workflow. Cette fonctionnalité permet à toutes les entreprises de bénéficier de l'agilité et de la confiance nécessaires pour déployer les bonnes règles de pare-feu, au bon moment et conformément aux réglementations de conformité. Au lieu d'adopter une approche au cas par cas, la solution GMS offre une stratégie cohérente pour la gestion de la sécurité réseau via des processus métier et des niveaux de service qui simplifient considérablement la gestion du cycle de vie des environnements de sécurité globaux.

Application des normes de sécurité avec SonicWall GMS

Avantages

- Gestion centralisée
- Gestion des règles sans erreur
- Contrôle des accès optimal
- Pistes d'audit complètes
- Modèles de rapports PCI, HIPAA, SOX
- Baisse des coûts d'exploitation



[1] *Requiert un abonnement supplémentaire*

SONICWALL®

Caractéristiques

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 ultrafaible 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
API REST	Permet au pare-feu de recevoir tout type de flux de renseignements propriétaires, d'OEM ou de fournisseurs tiers et de les exploiter pour combattre les menaces évoluées : zero-day, initié malveillant, identifiants compromis, ransomwares et menaces persistantes avancées.
Inspection stateful des paquets	Tout le trafic réseau est inspecté, analysé et mis en conformité avec les règles d'accès du pare-feu.
Mise en cluster/haute disponibilité	Les pare-feux SuperMassive Series prennent 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.
Prise en charge IPv6	Le protocole IPv6 (Internet Protocol version 6) commence à remplacer le protocole IPv4. Avec le dernier système d'exploitation SonicOS 6.2, le matériel prendra en charge les implémentations en mode filaire et filtrage.
Options de déploiement flexibles	Les pare-feux SuperMassive Series peuvent être déployés 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 routes basées sur des protocoles pour diriger le trafic vers une connexion WAN préférée avec la possibilité de basculer vers un WAN secondaire en cas de panne.
Qualité de service avancée (QoS)	Protège les communications critiques avec le marquage 802.1p et DSCP, ainsi que le remappage du trafic VoIP sur le réseau.
Prise en charge des proxys SIP et des contrôleurs d'accès H.323	Bloque les appels indésirables en exigeant que tous les appels entrants soient autorisés et authentifiés par un contrôleur d'accès H.323 ou un proxy SIP.
Gestion des commutateurs réseau Dell série X uniques et en cascade	Gère les paramètres de sécurité de ports supplémentaires, notamment les ports Portshield, HA, POE et POE+, à partir d'un seul écran, via le tableau de bord de gestion des pare-feux pour le commutateur 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 social login	Permet aux utilisateurs invités d'utiliser leur identifiant des services de réseaux sociaux comme Facebook, Twitter ou Google+ pour se connecter et accéder à Internet et à d'autres services invités par le biais de zones sans fil, LAN ou DMZ d'un hôte en utilisant l'authentification directe.
Authentification multi-domaines	Constitue un moyen simple et rapide d'administrer les règles de sécurité sur tous les domaines du réseau. Gère une règle individuelle pour un seul domaine ou un groupe de domaines.

Gestion et reporting	
Fonctionnalité	Description
Global Management System[1] (GMS)	La solution SonicWall GMS surveille, configure et génère des rapports sur plusieurs appliances SonicWall via une console de gestion unique dotée d'une interface intuitive pour réduire les coûts et la complexité de gestion.
Puissant outil de gestion en un seul appareil	L'interface Web intuitive offre une interface de ligne de commande complète, prend en charge le protocole SNMPv2/3 et permet une configuration rapide et pratique.
Rapports sur les flux applicatifs IPFIX/NetFlow	Exporte des analyses du trafic applicatif et des données d'utilisation via les protocoles IPFIX ou NetFlow pour offrir une surveillance et des rapports historiques et en temps réel sur SonicWall Scrutinizer ou d'autres outils prenant en charge IPFIX et NetFlow via des extensions.

Caractéristiques

Réseau privé virtuel (VPN)	
Fonctionnalité	Description
Configuration automatique du VPN	Simplifie sensiblement le déploiement de pare-feux distribués en automatisant la configuration initiale de la passerelle VPN site à site entre les pare-feux SonicWall. Sécurité et connectivité se mettent en place instantanément et automatiquement.
VPN IPSec pour la connectivité site à site	Le VPN IPSec hautes performances permet aux pare-feux SuperMassive Series de servir de concentrateurs 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 fournir un accès simple aux courriers électroniques, fichiers, ordinateurs, sites intranet et applications depuis de nombreuses 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[1]/ Terminal Services[1] associée aux nombreuses informations obtenues par l'inspection approfondie des paquets.
Identification du trafic par pays GeoIP	Identifie et contrôle le trafic réseau en direction ou provenant de pays spécifiques pour contrer les attaques liées à une activité d'origine suspecte ou connue ou pour faire des recherches sur le trafic suspect provenant du réseau. Permet de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP.
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	Ce service assure l'analyse d'un vaste éventail de fichiers, notamment les programmes exécutables (PE), DLL, PDF, documents MS Office, archives, JAR, et APK, ainsi que de divers systèmes d'exploitation comme Windows, Android ou Mac OS et des environnements multi-navigateurs.
Déploiement rapide des signatures	Lorsqu'un fichier est identifié comme étant malveillant, une signature est immédiatement mise à la disposition des pare-feux ayant un abonnement à SonicWall Capture, avant d'être envoyée sous 48 heures aux bases de données de signatures GRID Gateway Anti-Virus et IPS ainsi qu'aux bases de données d'URL, d'IP et de réputation de domaine.
Capture Client	Capture Client est une plateforme client unifiée comportant de multiples fonctionnalités de protection des terminaux, notamment protection avancée contre les programmes malveillants et visibilité sur le trafic chiffré. Elle s'appuie sur des technologies de protection sur plusieurs couches, sur un reporting complet et sur la protection des terminaux.

Protection contre les menaces chiffrées[1]	
Fonctionnalité	Description
Déchiffrement et inspection TLS/ SSL	Déchiffre et inspecte le trafic SSL/TLS à la volée, sans proxy, pour détecter les logiciels malveillants, les intrusions et les fuites de données, et met en application les règles de contrôle du contenu, des URL et des applications afin de contrer les menaces dissimulées au sein du trafic TLS/SSL chiffré. 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 des intrusions[1]	
Fonctionnalité	Description
Protection basée sur des contre-mesures	Le système de prévention des intrusions (Intrusion Prevention System, IPS) étroitement intégré s'appuie sur les signatures et autres contre-mesures pour détecter les vulnérabilités et les attaques, dont il couvre une large palette, au sein de la charge utile.
Mise à jour automatique des signatures	L'équipe de recherche des menaces SonicWall recherche et déploie en continu des mises à jour pour une longue liste de contre-mesures IPS couvrant plus de 50 catégories d'attaque. Les nouvelles mises à jour prennent effet immédiatement, sans redémarrage ni interruption de service.
Protection IPS intrazone	Renforce la sécurité interne en segmentant le réseau en plusieurs zones de sécurité avec prévention des intrusions, empêchant les menaces de se propager entre ces zones.
Détection et blocage de la commande et du contrôle (Command and Control, CnC) des réseaux de zombies	Identifie et bloque le trafic CnC provenant de robots sur le réseau local vers des IP et des domaines identifiés comme propageant des logiciels malveillants ou comme des points CnC connus.
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.

Caractéristiques

Prévention des intrusions[1]	
Fonctionnalité	Description
Anti-logiciels malveillants de passerelle	Le moteur RFDPI analyse tout le trafic entrant, sortant et intrazone pour détecter les virus, chevaux de Troie, enregistreurs de frappes et autres logiciels malveillants dans les fichiers, quelles que soient leur taille et leur longueur, sur tous les ports et les flux TCP.
Protection contre les logiciels 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 de contenu.
Client de filtrage de contenu appliqué	Étend l'application des règles pour bloquer les contenus Internet des appareils Windows, Mac OS, Android et Chrome situés hors du périmètre du pare-feu.
Contrôles granulaires	Bloque 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 utilise la version la plus récente des signatures de virus et de logiciels espions, éliminant ainsi les coûts couramment liés à la gestion des logiciels antivirus et 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 la charge d'administration.
Protection antivirus automatique continue	Des mises à jour fréquentes des logiciels antivirus et anti-logiciels espions sont appliquées de manière transparente à tous les ordinateurs de bureau et serveurs de fichiers pour améliorer la productivité des utilisateurs et alléger la gestion de la sécurité.
Antivirus de nouvelle génération	Capture Client utilise un moteur statique d'intelligence artificielle (IA) pour détecter les menaces avant leur exécution et pour restaurer une version précédente non infectée.
Protection contre les logiciels espions	Une protection puissante contre les logiciels espions analyse et bloque l'installation d'un large éventail de logiciels espions sur les ordinateurs portables et de bureau avant qu'ils ne transmettent des données confidentielles, renforçant ainsi les performances et la sécurité des postes de travail.

[1] *Requiert un abonnement supplémentaire*

Récapitulatif des fonctionnalités

Pare-feu

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

Déchiffrement et inspection SSL/SSH[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 des 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

Protection contre les logiciels malveillants[2]

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

Identification des applications[2]

- Contrôle des applications
- 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
- Anonymiseurs
- Blocage par mots-clés
- Insertion d'en-têtes 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

- LAG dynamique à l'aide de LACP
- PortShield
- Trames Jumbo
- Découverte MTU de chemin
- 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 SonicPoint[1]
- 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 NAT, mode TAP, mode filaire virtuel/filaire, mode pont de couche 2
- Basculement WAN 3G/4G (sauf sur SuperMassive 9800)
- Routage asymétrique
- Prise en charge Common Access Card (CAC)

Connectivité sans fil

- WIDS/WIPS
- Analyse de spectre RF
- Prévention AP malveillants
- Itinérance rapide (802.11k/r/v)
- Vue plan/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, UI, CLI, 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 N-Series et X-Series[1]

[1] *Non pris en charge sur SuperMassive 9800*
[2] *Requiert un abonnement supplémentaire*

SONICWALL®

Spécifications système des pare-feux SuperMassive 9000 Series

Pare-feu – Général	9200	9400	9600	9800
Système d'exploitation	SonicOS			
Cœurs de processeur de sécurité	24	32		64
Interfaces	4 SFP+ 10GbE, 8 SFP 1GbE, 8 1GbE, gestion 1GbE, 1 console			4 SFP+ 10GbE, 12 SFP 1GbE, 8 1GbE, gestion 1GbE, 1 console
Mémoire (RAM)	8 Go	16 Go	32 Go	64 Go
Stockage	Flash			2 disques SSD Flash de 80 Go
Extension	1 connecteur d'extension (à l'arrière)*, carte SD*			
Gestion	CLI, SSH, interface utilisateur graphique, 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 de 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
Nb max. de connexions (SPI)	5,0 M	7,5 M	10,0 M	20,0 M
Nb max. de connexions (DPI)	1,5 M	1,5 M	2,0 M	8,0 M
Connexions DPI SSL[6] (max.)	8 000 (15 500[6])	10 000 (17 500[6])	12 000 (22 500[6])	400 000
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 (max.)	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, Common Access Card (CAC)			
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	1:1, plusieurs:1, 1:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent			
Interfaces VLAN	512			
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage basé sur des règles, multidiffusion			
Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1p			
Authentification	LDAP (multi-domaines), 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	APL UC[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**
Bloc d'alimentation	Deux blocs redondants remplaçables à chaud de 300 W			Deux blocs redondants remplaçables à chaud de 500 W
Ventilateurs	Deux ventilateurs redondants remplaçables à chaud			
Affichage	Écran LED avant			
Puissance d'entrée	100-240 V CA, 50-60 Hz			
Consommation électrique maximale (W)	200			350
Temps de fonctionnement entre deux pannes à 25 °C (heures)	188 719	187 702	186 451	126 144
Temps de fonctionnement entre deux pannes à 25 °C (années)	21,53	21,43	21,28	14,40
Format	Montable en rack 1U			Montable en rack 2U
Dimensions	43,3 x 48,5 x 4,5 cm (17 x 19,1 x 1,75 in)			9 x 60 x 43 cm (17 x 24 x 3,5 in)
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 de transport	13,3 kg (29,3 lb)			29,64 kg (65 lb)
Conformité aux réglementations majeures	FCC classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI classe A, MSIP/KCC classe A, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH, ANATEL, BSMI, CU			
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 des paquets de 1 280 octets. [4] Valable pour les pare-feux SuperMassive 9200, 9400 et 9600. Certification APL UC en attente pour le pare-feu SuperMassive 9800. [5] Pris en charge sur SonicOS 6.1 et 6.2. [6] Pour chaque réduction de 125 000 connexions DPI, le nombre de connexions DPI SSL disponibles augmente de 750. * Utilisation future. Toutes les caractéristiques, fonctionnalités et disponibilités peuvent faire l'objet de modifications.*

SONICWALL®

Informations de commande du pare-feu 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 de support et de sécurité du pare-feu SuperMassive 9200	**Référence**
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour SuperMassive 9200 (1 an)	01-SSC-1570
Capture Advanced Threat Protection pour SuperMassive 9200 (1 an)	01-SSC-1575
Comprehensive Gateway Security Suite : surveillance des applications, prévention des menaces, filtrage du contenu avec support technique pour SuperMassive 9200 (1 an)	01-SSC-4172
Prévention des intrusions, protection contre les logiciels malveillants, CloudAV, surveillance, contrôle et visualisation des applications pour SuperMassive 9200 (1 an)	01-SSC-4202
Content Filtering Service Premium Business Edition pour SuperMassive 9200 (1 an)	01-SSC-4184
Support Platinum pour SuperMassive 9200 (1 an)	01-SSC-4178
Abonnements de support et de sécurité du pare-feu SuperMassive 9400	**Référence**
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour SuperMassive 9400 (1 an)	01-SSC-1580
Capture Advanced Threat Protection pour SuperMassive 9400 (1 an)	01-SSC-1585
Comprehensive Gateway Security Suite : surveillance des applications, prévention des menaces, filtrage du contenu avec support technique pour SuperMassive 9400 (1 an)	01-SSC-4136
Prévention des intrusions, protection contre les logiciels malveillants, CloudAV, surveillance, contrôle et visualisation des applications pour SuperMassive 9400 (1 an)	01-SSC-4166
Content Filtering Service Premium Business Edition pour SuperMassive 9400 (1 an)	01-SSC-4148
Support Platinum pour SuperMassive 9400 (1 an)	01-SSC-4142
Abonnements de support et de sécurité du pare-feu SuperMassive 9600	**Référence**
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour SuperMassive 9600 (1 an)	01-SSC-1590
Capture Advanced Threat Protection pour SuperMassive 9600 (1 an)	01-SSC-1595
Comprehensive Gateway Security Suite : surveillance des applications, prévention des menaces, filtrage du contenu avec support technique pour SuperMassive 9600 (1 an)	01-SSC-4100
Prévention des intrusions, protection contre les logiciels malveillants, CloudAV, surveillance, contrôle et visualisation des applications pour SuperMassive 9600 (1 an)	01-SSC-4130
Content Filtering Service Premium Business Edition pour SuperMassive 9600 (1 an)	01-SSC-4112
Support Platinum pour SuperMassive 9600 (1 an)	01-SSC-4106
Abonnements de support et de sécurité du pare-feu SuperMassive 9800	**Référence**
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour SuperMassive 9800 (1 an)	01-SSC-1183
Capture Advanced Threat Protection pour SuperMassive 9800 (1 an)	01-SSC-1188
Comprehensive Gateway Security Suite : surveillance des applications, prévention des menaces, filtrage du contenu avec support technique pour SuperMassive 9800 (1 an)	01-SSC-0809
Prévention des intrusions, protection contre les logiciels malveillants, CloudAV, surveillance, contrôle et visualisation des applications pour SuperMassive 9800 (1 an)	01-SSC-0827
Content Filtering Service Premium Business Edition pour SuperMassive 9800 (1 an)	01-SSC-0821
Support Gold 24h/24, 7j/7 pour SuperMassive 9800 (1 an)	01-SSC-0815
Modules et accessoires*	**Référence**
Ventilateur SonicWall SuperMassive 9800 Series (unité remplaçable sur site)	01-SSC-0204
Bloc d'alimentation CA SonicWall SuperMassive 9800 Series (unité remplaçable sur site)	01-SSC-0203
Ventilateur SonicWall SuperMassive 9000 Series (unité remplaçable sur site)	01-SSC-3876
Bloc d'alimentation CA SonicWall SuperMassive 9000 Series (unité remplaçable sur site)	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 reporting	**Référence**
Licence logiciel 10 nœuds SonicWall GMS	01-SSC-3363
Support logiciel SonicWall GMS E-Class (24h/24, 7j/7) pour 10 nœuds (1 an)	01-SSC-6514
Licence logicielle pour l'appliance virtuelle SonicWall Scrutinizer avec module Flow Analytics pour jusqu'à 5 nœuds (inclut un an de support logiciel 24h/24, 7j/7)	01-SSC-3443
Licence logicielle SonicWall Scrutinizer avec module Flow Analytics pour jusqu'à 5 nœuds (inclut un an de support logiciel 24h/24, 7j/7)	01-SSC-4002
Licence logicielle SonicWall Scrutinizer avec module Advanced Reporting pour jusqu'à 5 nœuds (inclut un an de support logiciel 24h/24, 7j/7)	01-SSC-3773

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

À propos de nous

SonicWall s'engage depuis plus de 27 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution automatisée de détection et de prévention des failles en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 215 pays et territoires, leur permettant de se concentrer sans crainte sur leur cœur de métier.

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

Datasheet-SuperMassive-US-VG-MKTG4043