SONICWALL

SonicWall Network Security appliance (NSa) Series

Une efficacité et des performances de sécurité reconnues par le secteur pour les réseaux de moyenne taille, les entreprises distribuées et les centres de données

Les appliances de sécurité réseau SonicWall NSa Series sont conçues pour les structures allant des réseaux de taille moyenne aux entreprises distribuées, en passant par les centres de données, auxquels elles offrent un système perfectionné de prévention des menaces sur une plateforme de sécurité hautes performances. Grâce aux technologies innovantes d'apprentissage profond intégrées à la plateforme SonicWall Capture Cloud, la série NSa assure la détection et la prévention automatisées des failles en temps réel dont les entreprises ont besoin.

Prévention des menaces à la pointe de la technologie et performance hors pair

Les menaces réseau actuelles sont extrêmement évasives et de plus en plus difficiles à identifier par les méthodes de détection classiques. Pour garder une longueur d'avance sur ces menaces sophistiquées, il faut une approche moderne reposant largement sur les renseignements de sécurité offerts par le cloud. Sans cela, les solutions de sécurité au niveau de la passerelle ne peuvent tenir tête aux menaces complexes que l'on rencontre aujourd'hui. Les pare-feux de nouvelle génération NSa Series intègrent deux technologies de sécurité évoluées pour fournir une prévention de pointe des menaces, permettant à votre réseau de conserver une avance nécessaire. Le service multimoteur Capture Advanced Threat Protection (ATP) de SonicWall est complété par la technologie RTDMI™ (Real-Time Deep Memory Inspection) en instance de brevet. Le moteur RTDMI détecte et bloque proactivement les logiciels malveillants de masse, les attaques zero-day et autres logiciels malveillants inconnus en inspectant directement dans la mémoire. Grâce à son architecture en temps réel, la technologie SonicWall RTDMI est précise, minimise les faux positifs et identifie et atténue les attaques sophistiquées au cours desquelles les armes sont exposées pendant moins de 100 nanosecondes. En parallèle, le moteur RFDPI (Reassembly-Free Deep Packet Inspection) single-pass breveté* de SonicWall examine chaque octet de chaque paquet, inspectant simultanément le trafic entrant et sortant sur le pare-feu. Tirant parti de la plateforme Capture Cloud SonicWall en plus de fonctionnalités intégrées (prévention des intrusions, anti-malware et filtrage des URL/Web notamment), la série NSa bloque même les menaces les plus insidieuses à la passerelle.

De plus, les pare-feux de SonicWall offrent une protection complète, quel que soit le port ou le protocole, en déchiffrant et inspectant entièrement les connexions TLS/SSL et SSH chiffrées. Le pare-feu regarde en profondeur à l'intérieur de chaque paquet (en-tête et données), à la recherche de non-conformité de protocole, de menaces, d'attaques zero-day, d'intrusions et même de critères définis. Le moteur d'inspection approfondie des paquets détecte et empêche les attaques chiffrées évoluées qui exploitent la cryptographie, bloque les téléchargements de logiciels malveillants chiffrés, interrompt la propagation des infections et contre les communications C&C 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.

Lorsque les entreprises activent des fonctions d'inspection approfondie des paquets telles que l'IPS, l'antivirus, l'anti-logiciels espions, le déchiffrement

Avantages :

- Prévention des menaces et performances haut de gamme
- Technologie d'inspection approfondie de la mémoire en temps réel, en instance de brevet
- Technologie RFDPI (Reassembly-Free Deep Packet Inspection) brevetée
- Prévention des intrusions intégrée et basée sur le cloud
- Déchiffrement et inspection TLS/SSL
- Efficacité de la sécurité reconnue par le secteur
- Architecture matérielle multicœur
- Équipe de recherche sur les menaces Capture Labs dédiée

Contrôle du réseau et flexibilité

- SD-WAN sécurisé
- Puissant système d'exploitation SonicOS
- Surveillance et contrôle des applications
- Segmentation du réseau à l'aide de VLAN
- Sécurité sans fil haut débit

Facilité de déploiement, de configuration et de gestion continue

- Déploiement sans intervention
- Gestion centralisée dans le cloud et sur site
- Gamme évolutive de pare-feux
- Faible coût total de possession

** Brevets américains 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723*

et l'inspection TLS/SSL et autres sur leur pare-feu, celles-ci ralentissent souvent les performances du réseau, parfois radicalement. Les pare-feux NSa Series présentent toutefois une architecture matérielle multicœur qui utilise des microprocesseurs de sécurité spécialisés. Associée à nos moteurs RTDMI et RFDPI, cette conception unique élimine toute perte de performances subie par les réseaux avec d'autres pare-feu.

Contrôle du réseau et flexibilité

SonicOS, le système d'exploitation riche en fonctionnalités de SonicWall, est au cœur des pare-feux NSa Series. SonicOS offre aux entreprises le contrôle réseau et la flexibilité dont elles ont besoin, via la surveillance et le contrôle des applications, la visualisation en temps réel, un système de prévention des intrusions (IPS) doté d'une technologie anti-évasion sophistiquée, des réseaux privés virtuels (VPN) haut débit et autres puissantes fonctionnalités de sécurité.

Avec la surveillance et le contrôle des applications, les administrateurs réseau sont à même d'identifier et de distinguer les applications productives de celles qui ne le sont pas, voire qui sont potentiellement dangereuses, et de contrôler ce trafic par le biais de puissantes règles au niveau applicatif, que ce soit pour des utilisateurs uniques ou des groupes (en s'appuyant sur des calendriers et des listes d'exceptions). Les applications vitales peuvent ainsi avoir la priorité et disposer de plus de bande passante, tandis que celle-ci sera limitée pour les applications non essentielles. La surveillance et la visualisation en temps réel offrent une représentation graphique des applications, des utilisateurs et de l'usage qui est fait de la bande passante, permettant d'obtenir une vue d'ensemble précise du trafic réseau.

Pour les entreprises distribuées nécessitant une flexibilité avancée pour la conception de leur réseau, la technologie SD-WAN de SonicOS vient parfaitement compléter les pare-feux NSa déployés en leur siège ou sur les sites distants. Au lieu de s'en remettre aux anciennes technologies, plus coûteuses, telles que MPLS ou T1, les entreprises qui utilisent le SD-WAN peuvent choisir les services moins chers de l'Internet public tout en conservant un niveau élevé de disponibilité des applications et des performances prévisibles.

De série sur chaque pare-feu NSa Series, un contrôleur d'accès sans fil permet d'élargir le périmètre réseau en toute sécurité grâce à la technologie sans fil. Ensemble, les pare-feux SonicWall et les points d'accès sans fil SonicWave 802.11ac Wave 2 constituent une solution de sécurité robuste, associant la technologie leader des pare-feux de nouvelle génération au sans-fil haut débit, pour une sécurité et des performances haut de gamme sur le réseau sans fil.

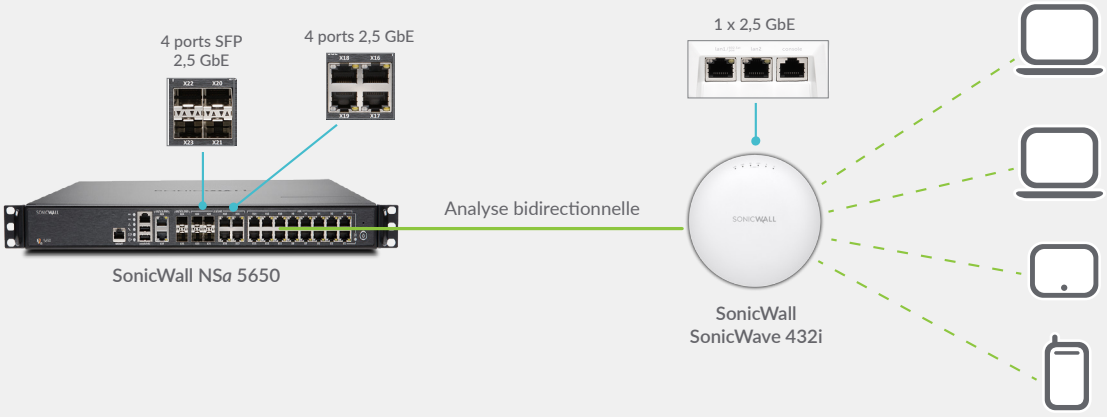
Facilité de déploiement, de configuration et de gestion continue

Comme tous les pare-feux SonicWall, la série NSa intègre étroitement des technologies clés de sécurité, de connectivité et de flexibilité en une seule et même solution complète. En font partie les points d'accès sans fil SonicWave ainsi que les appliances d'accélération WAN SonicWall WXA Series, tous étant automatiquement détectés et configurés par le pare-feu de gestion NSa. Le regroupement de plusieurs fonctionnalités évite l'achat et l'installation de différents produits qui, de plus, ne fonctionnent pas toujours bien ensemble. Cela demande également moins d'efforts pour déployer et configurer la solution sur le réseau, ce qui à son tour se traduit par des économies de temps et d'argent.

Les services de gestion, de reporting, de licence et d'analyse centralisés dans le cloud sont gérés via le SonicWall Capture Security Center. L'un des éléments clés du Capture Security Center est le déploiement zéro intervention. Cette fonctionnalité cloud simplifie et accélère le déploiement et la configuration des pare-feux SonicWall sur les sites distants et les succursales. La simplicité de déploiement et de configuration et la facilité de gestion permettent aux entreprises d'abaisser leur coût total de possession et de réaliser un bon retour sur investissement.

Sans-fil haut débit sécurisé

Combinez un pare-feu de nouvelle génération NSa Series et un point d'accès sans fil SonicWall SonicWave 802.11ac Wave 2 pour créer une solution de sécurité réseau sans fil haut débit. Les pare-feux NSa Series comme les points d'accès SonicWave proposent des ports 2,5 GbE permettant de bénéficier du débit multi-gigabits offert par la technologie sans fil Wave 2. Le pare-feu analyse l'ensemble du trafic sans fil entrant et sortant du réseau à l'aide de la technologie d'inspection approfondie des paquets, puis élimine les menaces comme les logiciels malveillants et les intrusions, même pour les connexions chiffrées. D'autres fonctionnalités de sécurité et de contrôle, par exemple filtrage de contenu, contrôle des applications, Application Intelligence et Capture Advanced Threat Protection, peuvent être exécutées sur le réseau sans fil afin de fournir des couches de protection supplémentaires.

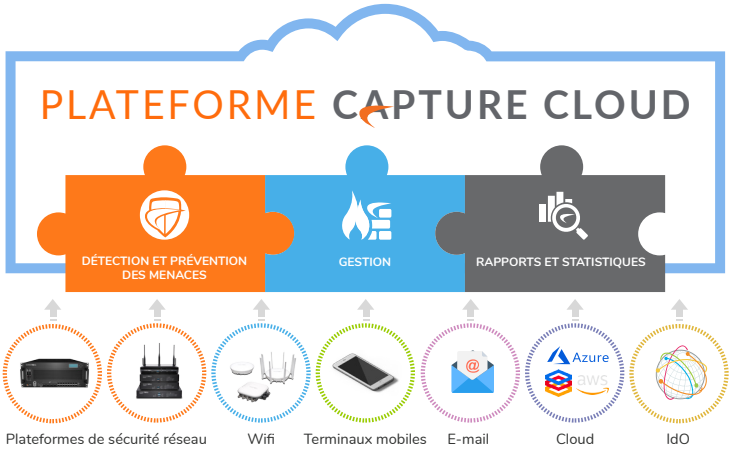


Plateforme Capture Cloud

La plateforme Capture Cloud de SonicWall assure la prévention des menaces et la gestion du réseau dans le cloud, à quoi s'ajoutent des fonctionnalités de reporting et d'analyse pour les entreprises de toute taille. Cette plateforme consolide les renseignements sur les menaces à partir de plusieurs sources dont notre service de sandboxing réseau multi-moteur primé, Capture Advanced Threat Protection, ainsi que plus de 1 million de capteurs SonicWall répartis dans le monde entier.

Si les données entrant sur le réseau s'avèrent contenir du code malveillant jusqu'ici inconnu, l'équipe de recherche interne Capture Labs de SonicWall dédiée aux menaces développe des signatures stockées dans la base de données de la plateforme Capture Cloud et déployées sur le pare-feu du client pour une protection actualisée. Les mises à jour sont actives immédiatement, sans redémarrage ni interruption. Les signatures présentes sur l'appliance protègent contre de vastes catégories d'attaques, couvrant des dizaines de milliers de menaces individuelles. Outre les moyens de lutte intégrés, les pare-feux NSa ont accès à la base de données de la plateforme Capture Cloud, qui vient compléter les défenses sur l'appliance par des dizaines de millions de signatures.

En plus de la protection contre les menaces, la plateforme Capture Cloud permet une gestion sur un seul écran. Les administrateurs peuvent facilement créer des rapports en temps réel et historiques de l'activité réseau.



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).

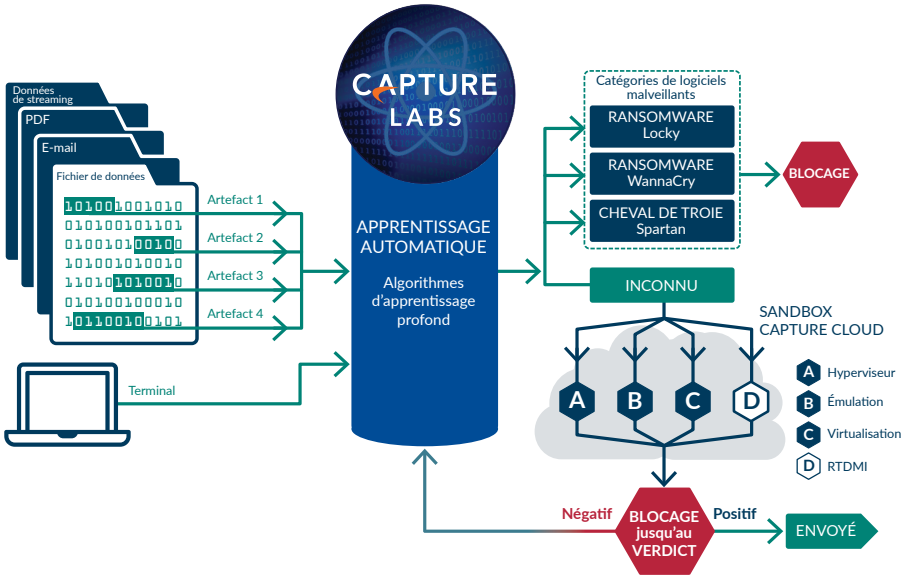
Capture ATP est une plateforme basée sur le cloud et multimoteur de sandboxing qui comprend Real-Time Deep Memory Inspection™ (RTDMI), un service virtualisé de sandboxing, une émulation complète du système et une technologie d'analyse au niveau de l'hyperviseur. CSa est un dispositif local doté de RTDMI, 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.



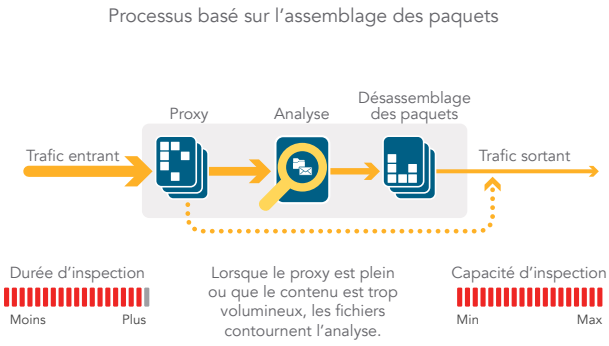
SONICWALL®

Moteur Reassembly-Free Deep Packet Inspection

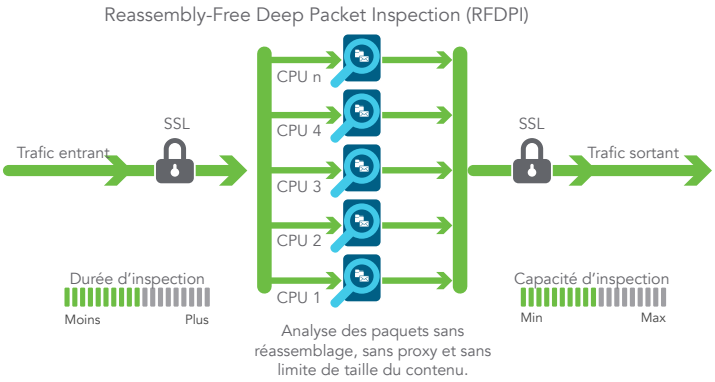
La technologie RFDPI (Reassembly-Free Deep Packet Inspection) est un système d'inspection à faible latence en un seul passage qui effectue des analyses bidirectionnelles à grande vitesse des flux de trafic sans proxy ni mise en mémoire tampon pour détecter efficacement les tentatives d'intrusion et les téléchargements de logiciels malveillants tout en identifiant le trafic applicatif, quels que soient le port ou le protocole. 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 et soumet les flux réseau à des opérations répétées et étendues de normalisation et de déchiffrement afin de neutraliser les techniques 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 trois bases de données de signatures : attaques par intrusion, logiciels malveillants 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



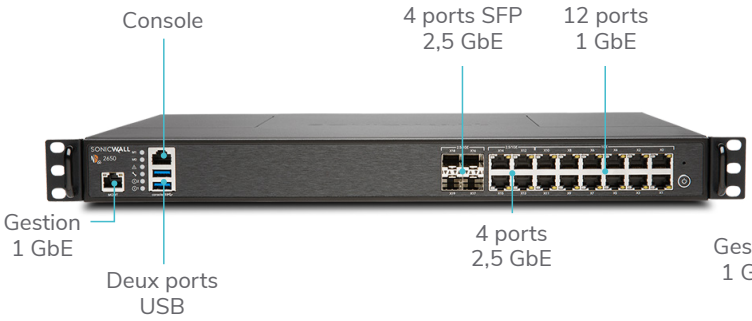
Architecture basée sur les flux SonicWall

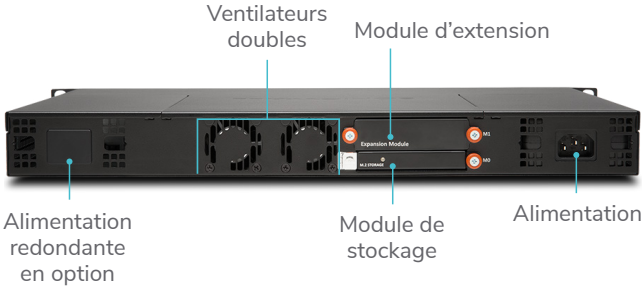
Gestion et reporting centralisés

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 offre aux administrateurs une plateforme unifiée, sécurisée et extensible de gestion des pare-feux, points d'accès sans fil et commutateurs Dell série N et série X par le biais d'un workstream corrélé et vérifiable. Les entreprises peuvent aisément consolider la gestion des appliances de sécurité, réduire les complexités administratives et de dépannage et 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. En outre, les entreprises répondent aux exigences des pare-feux en matière de gestion des modifications via une fonctionnalité d'automatisation du workflow qui offre l'agilité et la confiance nécessaires pour déployer les règles de pare-feu appropriées, au bon moment et conformément aux réglementations de conformité. Disponibles en local avec SonicWall Global Management System et dans le cloud avec le Capture Security Center, les solutions de gestion et de reporting SonicWall offrent, plutôt qu'une approche au cas par cas, 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.

NSa 2650

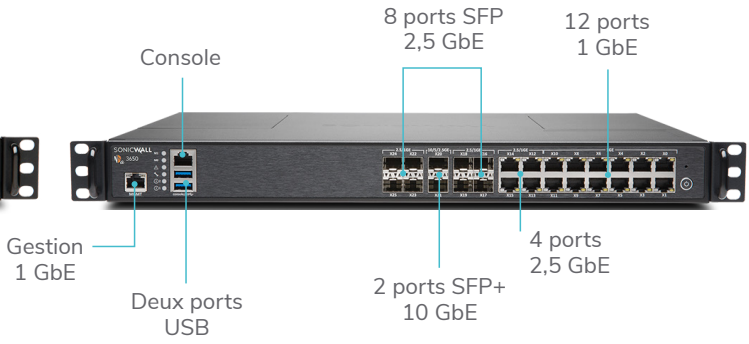
Le NSa 2650 assure une prévention des menaces haut débit sur des milliers de connexions chiffrées et encore davantage de connexions non chiffrées pour les PME et les entreprises distribuées.

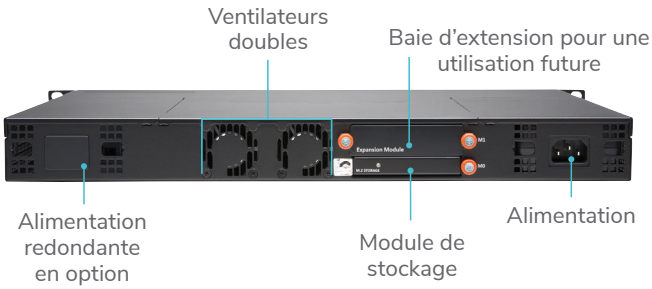




NSa 3650

Le NSa 3650 SonicWall convient idéalement aux environnements de PME et de succursales soucieuses d'optimiser leurs performances et capacités de débit.



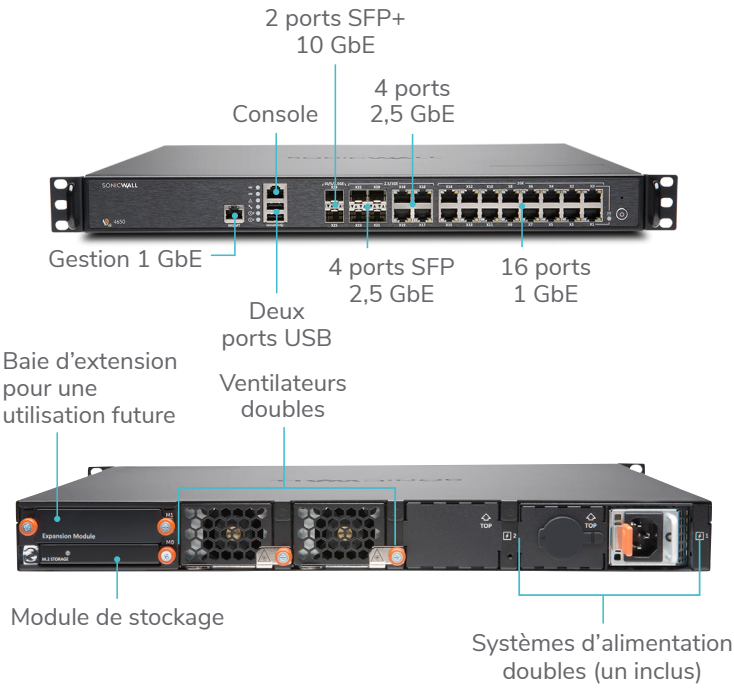


De nouvelle génération	NSa 2650
Débit du pare-feu	3,0 Gbit/s
Débit IPS	1,4 Gbit/s
Débit d'inspection des logiciels malveillants	1,3 Gbit/s
Débit prévention des menaces	1,5 Gbit/s
Connexions maximales	1 000 000
Nouvelles connexions/s	14 000/s
Module de stockage	16 Go
Description	**Référence**
Pare-feu NSa 2650 uniquement	01-SSC-1936
NSa 2650 TotalSecure Advanced (1 an)	01-SSC-1988

De nouvelle génération	NSa 3650
Débit du pare-feu	3,75 Gbit/s
Débit IPS	1,8 Gbit/s
Débit d'inspection des logiciels malveillants	1,5 Gbit/s
Débit prévention des menaces	1,75 Gbit/s
Connexions maximales	2 000 000
Nouvelles connexions/s	14 000/s
Module de stockage	32 Go
Description	**Référence**
Pare-feu NSa 3650 uniquement	01-SSC-1937
NSa 3650 TotalSecure Advanced (1 an)	01-SSC-4081

NSa 4650

Le SonicWall NSa 4650 protège les entreprises de taille moyenne en pleine croissance et leurs succursales grâce à des fonctionnalités professionnelles aux performances sans compromis.

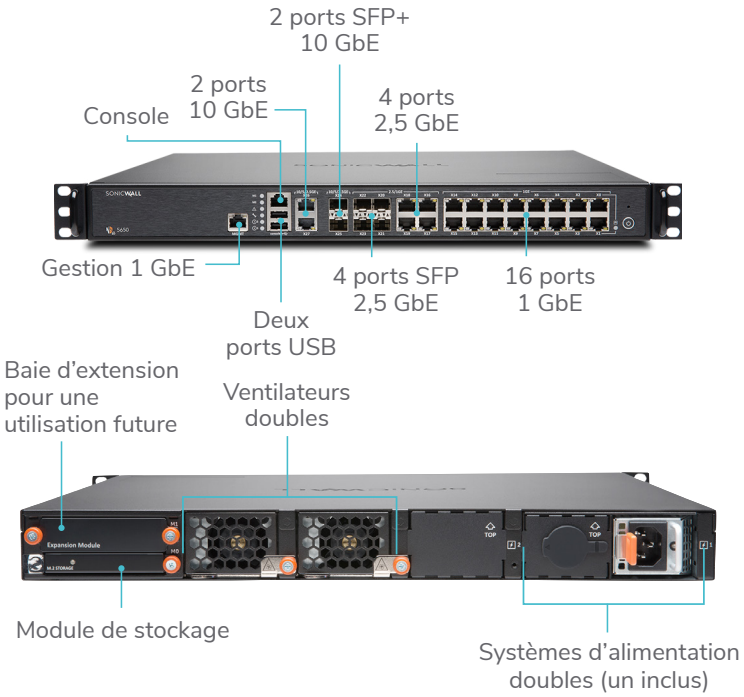


De nouvelle génération	NSa 4650
Débit du pare-feu	6,0 Gbit/s
Débit IPS	2,3 Gbit/s
Débit d'inspection des logiciels malveillants	2,45 Gbit/s
Débit prévention des menaces	2,5 Gbit/s
Connexions maximales	3 000 000
Nouvelles connexions/s	40 000/s
Module de stockage	32 Go

Description	Référence
Pare-feu NSa 4650 uniquement	01-SSC-1938
NSa 4650 TotalSecure Advanced (1 an)	01-SSC-4094

NSa 5650

Le SonicWall NSa 5650 est idéal pour les environnements d'entreprises, de succursales ou distribués aux besoins importants en matière de débit et de densité de ports.

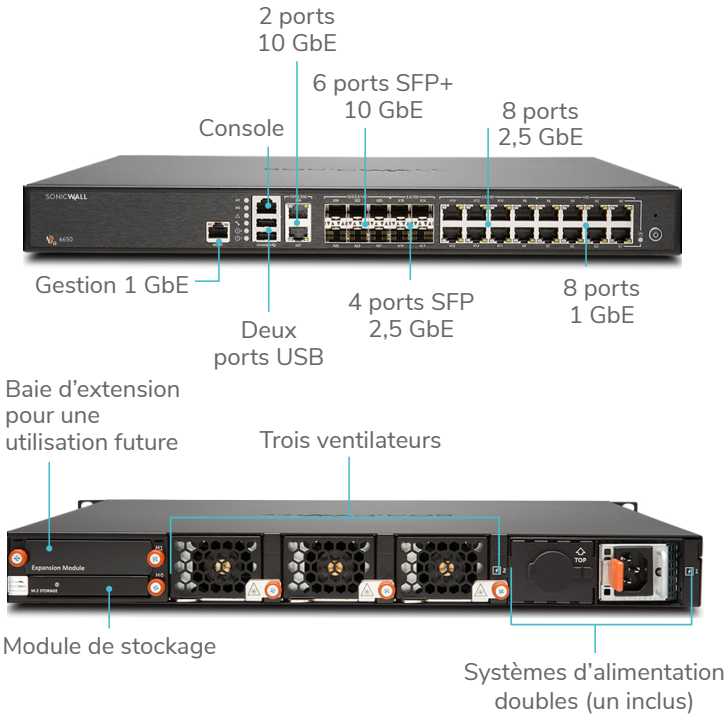


De nouvelle génération	NSa 5650
Débit du pare-feu	6,25 Gbit/s
Débit IPS	3,4 Gbit/s
Débit d'inspection des logiciels malveillants	2,8 Gbit/s
Débit prévention des menaces	3,4 Gbit/s
Connexions maximales	4 000 000
Nouvelles connexions/s	40 000/s
Module de stockage	64 Go

Description	Référence
Pare-feu NSa 5650 uniquement	01-SSC-1939
NSa 5650 TotalSecure Advanced (1 an)	01-SSC-4342

NSa 6650

Le SonicWall NSa 6650 est idéal pour les sièges d'entreprises et grands réseaux distribués nécessitant des capacités de débit et des performances élevées.



NSa 9250/9450/9650

Les pare-feux SonicWall NSa 9250/9450/9650 assurent une sécurité approfondie et évolutive à des débits multi-gigabits aux entreprises distribuées et centres de données.

De nouvelle génération	NSa 6650
Débit du pare-feu	12,0 Gbit/s
Débit IPS	6,0 Gbit/s
Débit d'inspection des logiciels malveillants	5,4 Gbit/s
Débit prévention des menaces	5,5 Gbit/s
Connexions maximales	5 000 000
Nouvelles connexions/s	90 000/s
Module de stockage	64 Go
Description	**Référence**
Pare-feu NSa 6650 uniquement	01-SSC-1940
NSa 6650 TotalSecure Advanced (1 an)	01-SSC-2209

De nouvelle génération	NSa 9250	NSa 9450	NSa 9650
Débit du pare-feu	12,0 Gbit/s	17,1 Gbit/s	17,1 Gbit/s
Débit IPS	7,2 Gbit/s	10,2 Gbit/s	10,3 Gbit/s
Débit d'inspection des logiciels malveillants	6,5 Gbit/s	8,0 Gbit/s	8,5 Gbit/s
Débit prévention des menaces	6,5 Gbit/s	9,0 Gbit/s	9,4 Gbit/s
Connexions maximales	7 500 000	10 000 000	12 500 000
Nouvelles connexions/s	90 000/s	130 000/s	130 000/s
Modules de stockage	1 To, 128 Go	1 To, 128 Go	1 To, 256 Go
Description	**Référence**	**SKU**	**SKU**
Pare-feu NSa uniquement	01-SSC-1941	01-SSC-1942	01-SSC-1943
NSa TotalSecure Advanced (1 an)	01-SSC-2854	01-SSC-4358	01-SSC-3475

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 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.

Fonctionnalité	Description
SD-WAN sécurisé	Plus économique que les technologies telles que MPLS, le SD-WAN sécurisé permet aux entreprises distribuées de mettre en place, de gérer et d'exploiter en toute sécurité des réseaux hautes performances sur des sites distants, et de partager ainsi des données, des applications et des services par le biais de services Internet publics à faible coût et facilement accessibles.
API REST	Permet au pare-feu de recevoir tout type de flux de renseignements propriétaires, d'OEM ou de fournisseurs tiers et de les exploiter pour combattre les menaces évoluées : zero-day, initié malveillant, identifiants compromis, ransomwares et menaces persistantes avancées.
Inspection 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 série NSa prend en charge les modes hautes 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 24 h/24, 7 j/7	Le protocole IPv6 (Internet Protocol version 6) commence à remplacer le protocole IPv4. Avec le système d'exploitation SonicOS, le matériel prendra en charge les implémentations en mode filaire et filtrage.
Options de déploiement flexibles	Le pare-feu NSa Series peut être déployé 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.
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 Dell série N et série X uniques et en cascade	Gérez les paramètres de sécurité de ports supplémentaires, notamment les ports Portshield, HA, PoE et PoE+, sur un seul écran, via le tableau de bord de gestion des pare-feux pour les commutateurs réseau Dell série N ou série X.
Authentification biométrique	Prend en charge les modes d'authentification d'appareils mobiles, comme la reconnaissance d'empreinte digitale, difficiles à dupliquer ou à partager, en vue de déterminer en toute sécurité l'identité de l'utilisateur pour l'accès au réseau.
Authentification ouverte et social login	Permet aux utilisateurs invités d'utiliser leurs identifiants sur les 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.

GESTION ET ÉLABORATION DE RAPPORTS

Fonctionnalité	Description
Gestion dans le cloud et sur site	La configuration et la gestion des appliances SonicWall peuvent se faire dans le cloud via le SonicWall Capture Security Center ou sur site avec SonicWall Global Management System (GMS).
Gestion puissante avec un seul appareil	L'interface Web intuitive offre une interface de ligne de commande complète, prend en charge le protocole SNMPv2/3 et permet une configuration rapide et pratique.
Rapports sur les flux applicatifs IPFIX/NetFlow	Exporte des analyses du trafic applicatif et des données d'utilisation via les protocoles IPFIX ou NetFlow pour offrir une surveillance et des rapports historiques et en temps réel avec des outils comme SonicWall Scrutinizer ou d'autres outils prenant en charge IPFIX et NetFlow via des extensions.

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 IPSec pour la connectivité site à site	Le VPN IPSec hautes performances permet à la série NSa 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/Citrix/Terminal Services associée aux nombreuses informations obtenues par l'inspection approfondie des paquets.
Identification du trafic par pays GeoIP	Identifie et contrôle le trafic réseau en direction ou provenant de pays spécifiques pour contrer les attaques liées à une activité d'origine suspecte ou connue ou pour faire des recherches sur le trafic suspect provenant du réseau. Possibilité de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP. Supprime le filtrage indésirable des adresses IP dû à une classification erronée.
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. Permet de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP.

Services d'abonnement de prévention des intrusions

CAPTURE ADVANCED THREAT PROTECTION

Fonctionnalité	Description
Service de sandbox multimoteur	La plateforme sandbox multimoteur, qui inclut le sandboxing virtualisé, l'émulation complète du système et une technologie d'analyse au niveau de l'hyperviseur, exécute le code suspect et analyse son comportement, offrant ainsi une visibilité complète sur l'activité malveillante.
Inspection approfondie de la mémoire en temps réel (RTDMI)	Cette technologie basée dans le cloud, en attente de brevet, détecte et bloque les logiciels malveillants qui ne manifestent aucun comportement malveillant et dissimulent leur armement au moyen d'un cryptage personnalisé. En forçant les logiciels malveillants à révéler leur armement dans la mémoire, le moteur RTDMI détecte et bloque de façon proactive les menaces « Zero Day » et les logiciels malveillants inconnus mais de grande diffusion.
Blocage jusqu'au verdict	Pour empêcher les fichiers potentiellement malveillants de pénétrer sur le réseau, les fichiers envoyés dans le cloud pour y être analysés peuvent être retenus à la passerelle jusqu'à ce qu'un verdict soit rendu.
Analyse de nombreux types de fichiers de toute taille	Ce service assure l'analyse d'un vaste éventail de fichiers, individuellement ou en groupe, 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 X 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 ATP, avant d'être envoyée sous 48 heures aux bases de données de signatures Gateway Anti-Virus et IPS ainsi qu'aux bases de données d'URL, d'IP et de réputation de domaine.
Capture Client	Capture Client 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

Fonctionnalité	Description
Déchiffrement et inspection TLS/SSL	Déchiffre et inspecte le trafic chiffré TLS/SSL à la volée, sans proxy, pour détecter les logiciels malveillants, les intrusions et les fuites de données, et applique les règles de contrôle du contenu, des URL et des applications afin de contrer les menaces dissimulées dans le trafic chiffré. Inclus avec les abonnements de sécurité pour tous les modèles de la série NSa Series.
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

Fonctionnalité	Description
Protection basée sur des contre-mesures	Le système de prévention des intrusions (Intrusion Prevention System, IPS) étroitement intégré s'appuie sur les signatures et autres contre-mesures pour détecter les vulnérabilités et les attaques, dont il couvre une large palette, au sein de la charge utile.
Mise à jour automatique des signatures	L'équipe de recherche des menaces SonicWall recherche et déploie en continu des mises à jour pour une longue liste de contre-mesures IPS couvrant plus de 50 catégories d'attaque. Les nouvelles mises à jour prennent effet immédiatement, sans redémarrage ni interruption de service.
Protection IPS intrazone	Renforce la sécurité interne en segmentant le réseau en plusieurs zones de sécurité avec prévention des intrusions, empêchant les menaces de se propager entre ces zones.

Détection et blocage de la commande et du contrôle (Command and Control, CnC) des réseaux de zombies	Identifie et bloque le trafic CnC provenant de robots sur le réseau local vers des IP et des domaines identifiés comme propageant des logiciels malveillants ou comme des points CnC connus.
Abus/anomalies de protocoles	Identifie et bloque les attaques exploitant les protocoles dans le but de contourner le système IPS.
Protection de type « zero-day »	Protège le réseau contre les attaques de type « zero-day » avec des mises à jour constantes répondant aux dernières méthodes et techniques d'attaque et couvrant des milliers de failles.
Technologie anti-évasion	La normalisation intensive des flux, le décodage et d'autres techniques empêchent les menaces d'entrer sur le réseau sans se faire détecter via des techniques d'évasion sur les couches 2 à 7.

PRÉVENTION DES MENACES

Fonctionnalité	Description
Anti-logiciels malveillants de passerelle	Le moteur RFDPI analyse tout le trafic entrant, sortant et intrazone pour détecter les virus, chevaux de Troie, enregistreurs de frappes et autres logiciels malveillants dans les fichiers, quelles que soient leur taille et leur longueur, sur tous les ports et les flux TCP.
Protection anti-logiciels malveillants Capture Cloud	Les serveurs cloud SonicWall hébergent une base de données contenant des dizaines de millions de signatures de menaces, mise à jour en continu. Cette dernière est utilisée pour augmenter les capacités de la base de données de signatures locale, offrant au moteur RFDPI une couverture étendue des menaces.
Mises à jour de sécurité en continu	Les nouvelles mises à jour sont automatiquement appliquées aux pare-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

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

Fonctionnalité	Description
Filtrage du contenu interne/externe	Applique des règles d'utilisation acceptables et bloque l'accès aux sites Web HTTP/HTTPS contenant des informations ou des images répréhensibles ou non productives via Content Filtering Service et Content Filtering Client.
Client de filtrage de contenu renforcé	Étend l'application des règles pour bloquer les contenus Internet des appareils Windows, Mac OS, Android et Chrome situés hors du périmètre du pare-feu.
Contrôles granulaires	Bloque 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

Fonctionnalité	Description
Protection multicouche	Utilise les fonctionnalités du pare-feu comme première couche de défense au niveau du périmètre et les associe à la protection des terminaux pour bloquer les virus qui entrent sur le réseau par le biais des ordinateurs portables, des clés USB ou d'autres systèmes non protégés.
Option d'application automatisée	S'assure que chaque ordinateur qui accède au réseau utilise le bon logiciel antivirus et/ou un certificat DPI-SSL installé et actif, éliminant ainsi les coûts couramment liés à la gestion des antivirus installés sur les ordinateurs de bureau.
Option de déploiement et d'installation automatisés	Le déploiement et l'installation, ordinateur par ordinateur, des clients antivirus et anti-logiciels espions sont automatiques sur le réseau, ce qui limite la charge d'administration.
Antivirus de nouvelle génération	Capture Client utilise un moteur statique d'intelligence artificielle (IA) pour identifier des menaces avant qu'elles ne puissent s'exécuter et pour revenir à un état précédant l'infection.
Protection contre les logiciels espions	Une protection puissante contre les logiciels espions analyse et bloque l'installation d'un large éventail de logiciels espions sur les ordinateurs portables et de bureau avant qu'ils ne transmettent des données confidentielles, renforçant ainsi les performances et la sécurité des postes de travail.

Récapitulatif des fonctionnalités de SonicOS

De nouvelle génération

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

Déchiffrement et inspection TLS/SSL/SSH[1]

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

Capture Advanced Threat Protection[1]

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

Prévention contre les intrusions[1]

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

Anti-logiciels malveillants[1]

- 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[1]

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

Visualisation et analyse du trafic

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

Filtrage du contenu Web HTTP/HTTPS[1]

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

VPN

- 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

- SD-WAN sécurisé
- PortShield
- Trames Jumbo
- Journalisation améliorée
- Jonction VLAN
- RSTP (Rapid Spanning Tree Protocol)
- 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
- Sécurité DNS
- 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, filaire/filaire virtuel, mode TAP
- Basculement WAN 3G/4G
- 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)
- Sélection automatique des canaux
- 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
- Transformations SIP et H.323 par règle d'accès
- Prise en charge des proxys SIP et des contrôleurs d'accès H.323

Gestion et surveillance

- Capture Security Center, GMS, interface utilisateur Web, 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 notamment en cascade

Stockage local

- Journaux
- Rapports
- Sauvegardes firmware

[1] *Nécessite un abonnement supplémentaire*

Spécifications système des pare-feux NSa Series

Généralités des pare-feu	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Système d'exploitation	SonicOS 6.5.4			
Interfaces	4 ports SFP 2,5 GbE, 4 ports 2,5 GbE 12 ports 1 GbE 1 gestion GbE, 1 console	2 ports SFP+ 10 GbE, 8 ports SFP 2,5 GbE, 4 ports 2,5 GbE 12 ports 1 GbE 1 gestion GbE, 1 console	2 ports SFP+ 10 GbE, 4 ports SFP 2,5 GbE, 4 ports 2,5 GbE 16 ports 1 GbE 1 gestion GbE, 1 console	2 ports SFP+ 10 GbE, 2 ports 10 GbE 4 ports SFP 2,5 GbE, 4 ports 2,5 GbE 16 ports 1 GbE 1 gestion GbE, 1 console
Extension	1 connecteur d'extension (à l'arrière)*			
Stockage intégré (SSD)	16 Go	32 Go	32 Go	64 Go
Gestion	CLI, SSH, IU Web, Capture Security Center, GMS, API REST			
Utilisateurs de l'authentification unique (SSO)	40 000	50 000	60 000	70 000
Max. de points d'accès pris en charge	48	96	128	192
Journalisation	Analyzer, Local Log, Syslog			
Performances pare-feu/VPN	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Débit d'inspection du pare-feu[1]	3,0 Gbit/s	3,75 Gbit/s	6,0 Gbit/s	6,25 Gbit/s
Débit prévention des menaces[2]	1,5 Gbit/s	1,75 Gbit/s	2,5 Gbit/s	3,4 Gbit/s
Débit d'inspection des applications[2]	1,85 Gbit/s	2,1 Gbit/s	3,0 Gbit/s	4,25 Gbit/s
Débit IPS[2]	1,4 Gbit/s	1,8 Gbit/s	2,3 Gbit/s	3,4 Gbit/s
Débit d'inspection des logiciels malveillants[2]	1,3 Gbit/s	1,5 Gbit/s	2,45 Gbit/s	2,8 Gbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[2]	300 Mbit/s	320 Mbit/s	675 Mbit/s	800 Mbit/s
Débit VPN[3]	1,45 Gbit/s	1,5 Gbit/s	3,0 Gbit/s	3,5 Gbit/s
Connexions par seconde	14 000/s	14 000/s	40 000/s	40 000/s
Nombre maximum de connexions (SPI)	1 000 000	2 000 000	3 000 000	4 000 000
Nombre maximum de connexions (DPI)	500 000	750 000	1 000 000	1 500 000
Connexions maximales/par défaut (DPI-SSL)	100 000/60 000	100 000/40 000	175 000/145 000	175 000/125 000
VPN	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Tunnels site à site	1 000	3 000	4 000	6 000
Clients VPN IPSec (max)	50 (1 000)	500 (3 000)	2 000 (4 000)	2 000 (6 000)
Clients VPN SSL NetExtender (max)	2 (350)	2 (500)	2 (1 000)	2 (1 500)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B Cryptography			
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v			
VPN basé sur le routage	RIP, OSPF, BGP			
Gestion de réseau	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Attribution d'adresses IP	Statique, (DHCP, PPPoE, L2TP et client PPTP), serveur DHCP interne, relais DHCP			
Modes NAT	1 à 1, plusieurs à 1, 1 à plusieurs, NAT flexible (adresses IP superposées), PAT, mode transparent			
Interfaces VLAN	256	256	400	500
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage à base de règles			
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, Citrix, Common Access Card (CAC)			
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 (en cours)	Pare-feu ICSA, antivirus ICSA, FIPS 140-2, NDPP Common Criteria (pare-feu et IPS), APL UC, USGv6, CsFC			
Haute disponibilité[5]	Active/passive avec synchronisation d'état	Active/passive avec synchronisation d'état Clustering actif/actif		Active/passive avec synchro. d'état, DPI actif/actif avec synchro. d'état, clustering actif/actif
Matériel	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Alimentation électrique	Double, redondant 120 W (un inclus)		Double, redondant 350W (un inclus)	
Ventilateurs	Doubles, fixes		Doubles, amovibles	
Puissance d'entrée	100 à 240 V CA, 50-60 Hz			
Consommation électrique maximale (W)	37,2	46	93,6	103,6
MTBF @25°C en heures	162 231	156 681	154 529	153 243
MTBF @25°C en années	18,5	17,9	17,6	17,5
Format	1U rackable			
Dimensions	43 x 32,5 x 4,5 cm (16,9 x 12,8 x 1,8 in)		43 x 41,5 x 4,5 cm (16,9 x 16,3 x 1,8 in)	
Poids	5,2 kg (11,5 lb)	5,3 kg (11,7 lb)	6,9 kg (15,2 lb)	6,9 kg (15,2 lb)
Poids DEEE	5,5 kg (12,1 lb)	5,6 kg (12,3 lb)	8,9 kg (19,6 lb)	8,9 kg (19,6 lb)
Poids avec emballage	7,7 kg (17,0 lb)	7,8 kg (17,2 lb)	11,3 kg (24,9 lb)	11,3 kg (24,9 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 (en fonctionnement/stockage)	0 à 40 °C (32 à 105 °F)/-40 à 70 °C (-40 à 158 °F)			
Taux d'humidité	10 à 90 % sans condensation			

Spécifications système des pare-feux NSa Series (suite)

Généralités des pare-feu	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Système d'exploitation	SonicOS 6.5.4			
Interfaces	6 ports SFP+ 10 GbE, 2 ports 10 GbE 4 ports SFP 2,5 GbE, 8 ports 2,5 GbE 8 ports 1 GbE 1 gestion GbE, 1 console	10 ports SFP+ 10 GbE, 2 ports 10 GbE 8 ports 2,5 GbE 8 ports 1 GbE 1 gestion GbE, 1 console	10 ports SFP+ 10 GbE, 2 ports 10 GbE 8 ports 2,5 GbE 8 ports 1 GbE 1 gestion GbE, 1 console	10 ports SFP+ 10 GbE, 2 ports 10 GbE 8 ports 2,5 GbE 8 ports 1 GbE 1 gestion GbE, 1 console
Extension	1 connecteur d'extension (à l'arrière)*			
Stockage intégré (SSD)	64 Go	1 To, 128 Go	1 To, 128 Go	1 To, 256 Go
Gestion	CLI, SSH, IU Web, Capture Security Center, GMS, API REST	CLI, SSH, IU Web, GMS, API REST		
Utilisateurs de l'authentification unique (SSO)	70 000	80 000	90 000	100 000
Max. de points d'accès pris en charge	192	192	192	192
Journalisation	Analyzer, Local Log, Syslog, IPFIX, NetFlow			
Performances pare-feu/VPN	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Débit d'inspection du pare-feu[1]	12,0 Gbit/s	12,0 Gbit/s	17,1 Gbit/s	17,1 Gbit/s
Débit prévention des menaces[2]	5,5 Gbit/s	6,5 Gbit/s	9,0 Gbit/s	9,4 Gbit/s
Débit d'inspection des applications[2]	6,0 Gbit/s	7,8 Gbit/s	10,8 Gbit/s	11,5 Gbit/s
Débit IPS[2]	6,0 Gbit/s	7,2 Gbit/s	10,2 Gbit/s	10,3 Gbit/s
Débit d'inspection des logiciels malveillants[2]	5,4 Gbit/s	6,5 Gbit/s	8,0 Gbit/s	8,5 Gbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[2]	1,45 Gbit/s	1,5 Gbit/s	2,1 Gbit/s	2,25 Gbit/s
Débit VPN[3]	6,0 Gbit/s	6,75 Gbit/s	10,0 Gbit/s	10,0 Gbit/s
Connexions par seconde	90 000/s	90 000/s	130 000/s	130 000/s
Nombre maximum de connexions (SPI)	5 000 000	7 500 000	10 000 000	12 500 000
Nombre maximum de connexions (DPI)	2 000 000	3 000 000	4 000 000	5 000 000
Connexions maximales/par défaut (DPI-SSL)	250 000/170 000	250 000/170 000	450 000/290 000	550 000/320 000
VPN	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Tunnels site à site	8 000	12 000	12 000	12 000
Clients VPN IPSec (max)	2 000 (6 000)	2 000 (6 000)	2 000 (6 000)	2 000 (6 000)
Clients VPN SSL NetExtender (max)	2 (2 000)	2 (3 000)	2 (3 000)	50 (3 000)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B Cryptography			
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v			
VPN basé sur le routage	RIP, OSPF, BGP			
Gestion de réseau	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Attribution d'adresses IP	Statique, (DHCP, PPPoE, L2TP et client PPTP), serveur DHCP interne, relais DHCP			
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			
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, Citrix, Carte CAC (Common Access Card)			
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 (en cours)	Pare-feu ICSA, antivirus ICSA, FIPS 140-2, NDPP Common Criteria (pare-feu et IPS), APL UC, USGv6, CsFC			
Haute disponibilité[5]	Active/passive avec synchro. d'état, DPI actif/actif avec synchro. d'état, clustering actif/actif			
Matériel	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Alimentation électrique	Double, redondant 350W (un inclus)	Double, redondant, 350 W		
Ventilateurs	Trois, amovibles			
Puissance d'entrée	100 à 240 V CA, 50-60 Hz			
Consommation électrique maximale (W)	144,3	86,7	90,9	113,1
MTBF @25°C en heures	157 193	139 783	134 900	116 477
MTBF @25°C en années	17,9	15,96	15,4	13,3
Format	1U rackable			
Dimensions	43 x 41,5 x 4,5 cm (16,9 x 16,3 x 1,8 in)			
Poids	8,1 kg (17,9 lb)	8,1 kg (17,9 lb)		
Poids DEEE	10,2 kg (22,5 lb)	10,2 kg (22,5 lb)		
Poids avec emballage	12,6 kg (27,8 lb)	12,6 kg (27,8 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, WEEE , REACH, ANATEL, BSMI			
Environnement (en fonctionnement/stockage)	0 à 40 °C (32 à 105 °F)/-40 à 70 °C (-40 à 158 °F)			
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. Performance DPI SSL mesurée sur le trafic HTTPS avec IPS activé.
[3] Débit VPN mesuré à l'aide du trafic UDP avec une taille de paquet de 1 280 octets et conformément à la norme RFC 2544. Sous réserve de modification des spécifications, des fonctionnalités et de la disponibilité.
[4] Pour 125 000 connexions DPI réduites, le nombre de connexions DPI SSL disponibles augmente de 3 000, hormis pour les pare-feux NSa 9250 et supérieurs.
[5] Clustering actif/actif et DPI actif/actif avec synchronisation d'état nécessitent l'achat d'une licence étendue, sauf pour NSa 9250 et versions supérieures.
** Utilisation future. Sous réserve de modification des spécifications, des fonctionnalités et de la disponibilité.*

Informations de commande des pare-feux NSa Series

NSa 2650	Référence
NSa 2650 TotalSecure Advanced Edition (1 an)	01-SSC-1988
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 pour NSa 2650 (1 an)	01-SSC-1783
Capture Advanced Threat Protection pour NSa 2650 (1 an)	01-SSC-1935
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus cloud pour le pare-feu NSa 2650 (1 an)	01-SSC-1976
Support 24h/24, 7j/7 pour le pare-feu NSa 2650 (1 an)	01-SSC-1541
Service de filtrage du contenu pour NSa 2650 (1 an)	01-SSC-1970
Capture Client	Selon le nombre d'utilisateurs
Service antispam complet pour NSa 2650 (1 an)	01-SSC-2001

NSa 3650	Référence
NSa 3650 TotalSecure Advanced Edition (1 an)	01-SSC-4081
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 pour NSa 3650 (1 an)	01-SSC-3451
Capture Advanced Threat Protection pour NSa 3650 (1 an)	01-SSC-3457
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus cloud pour le pare-feu NSa 3650 (1 an)	01-SSC-3632
Support 24h/24, 7j/7 pour le pare-feu NSa 3650 (1 an)	01-SSC-3439
Service de filtrage du contenu pour NSa 3650 (1 an)	01-SSC-3469
Capture Client	Selon le nombre d'utilisateurs
Service antispam complet pour NSa 3650 (1 an)	01-SSC-4030

NSa 4650	Référence
NSa 4650 TotalSecure Advanced Edition (1 an)	01-SSC-4094
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 pour NSa 4650 (1 an)	01-SSC-3493
Capture Advanced Threat Protection pour NSa 4650 (1 an)	01-SSC-3499
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus cloud pour le pare-feu NSa 4650 (1 an)	01-SSC-3589
Support 24h/24, 7j/7 pour le pare-feu NSa 4650 (1 an)	01-SSC-3487
Service de filtrage du contenu pour NSa 4650 (1 an)	01-SSC-3583
Capture Client	Selon le nombre d'utilisateurs
Service antispam complet pour NSa 4650 (1 an)	01-SSC-4062

NSa 5650	Référence
NSa 5650 TotalSecure Advanced Edition (1 an)	01-SSC-4342
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 pour NSa 5650 (1 an)	01-SSC-3674
Capture Advanced Threat Protection pour NSa 5650 (1 an)	01-SSC-3680
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus cloud pour le pare-feu NSa 5650 (1 an)	01-SSC-3698
Support 24h/24, 7j/7 pour le pare-feu NSa 5650 (1 an)	01-SSC-3660
Service de filtrage du contenu pour NSa 5650 (1 an)	01-SSC-3692
Capture Client	Selon le nombre d'utilisateurs
Service antispam complet pour NSa 5650 (1 an)	01-SSC-4068

NSa 6650	Référence
NSa 6650 TotalSecure Advanced Edition (1 an)	01-SSC-2209
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 pour NSa 6650 (1 an)	01-SSC-8761
Capture Advanced Threat Protection pour NSa 6650 (1 an)	01-SSC-8930
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus cloud pour le pare-feu NSa 6650 (1 an)	01-SSC-8979
Support 24h/24, 7j/7 pour le pare-feu NSa 6650 (1 an)	01-SSC-8663
Service de filtrage du contenu pour NSa 6650 (1 an)	01-SSC-8972
Capture Client	Selon le nombre d'utilisateurs
Service antispam complet pour NSa 6650 (1 an)	01-SSC-9131

NSa 9250	Référence
NSa 9250 TotalSecure Advanced Edition (1 an)	01-SSC-2854
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 pour NSa 9250 (1 an)	01-SSC-0038
Capture Advanced Threat Protection pour NSa 9250 (1 an)	01-SSC-0121
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus cloud pour le pare-feu NSa 9250 (1 an)	01-SSC-0343
Support 24h/24, 7j/7 pour le pare-feu NSa 9250 (1 an)	01-SSC-0032
Service de filtrage du contenu pour NSa 9250 (1 an)	01-SSC-0331
Capture Client	Selon le nombre d'utilisateurs

Informations de commande des pare-feux NSa Series (suite)

NSa 9450	Référence
NSa 9450 TotalSecure Advanced Edition (1 an)	01-SSC-4358
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 pour NSa 9450 (1 an)	01-SSC-0414
Capture Advanced Threat Protection pour NSa 9450 (1 an)	01-SSC-0855
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus cloud pour le pare-feu NSa 9450 (1 an)	01-SSC-1196
Support 24 h/24, 7 j/7 pour le pare-feu NSa 9450 0 (1 an)	01-SSC-0407
Service de filtrage du contenu pour NSa 9450 (1 an)	01-SSC-1158
Capture Client	Selon le nombre d'utilisateurs

NSa 9650	Référence
NSa 9650 TotalSecure Advanced Edition (1 an)	01-SSC-3475
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 pour NSa 9650 (1 an)	01-SSC-2036
Capture Advanced Threat Protection pour NSa 9650 (1 an)	01-SSC-2042
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus cloud pour le pare-feu NSa 9650 (1 an)	01-SSC-2142
Support 24 h/24, 7 j/7 pour le pare-feu NSa 9650 0 (1 an)	01-SSC-1989
Service de filtrage du contenu pour NSa 9650 (1 an)	01-SSC-2136
Capture Client	Selon le nombre d'utilisateurs

Modules et accessoires*	Référence
Module à courte portée 10GBASE-SR SFP+	01-SSC-9785
Module à longue portée 10GBASE-LR SFP+	01-SSC-9786
Câble TwinAx 10GBASE SFP+, 1M	01-SSC-9787
Câble TwinAx 10GBASE SFP+, 3M	01-SSC-9788
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

**Veuillez contacter votre revendeur SonicWall pour obtenir la liste complète des modules SFP et SFP+ pris en charge.*

Offre groupée sur les pare-feux SonicWall NSa/NSv

Les pare-feux NSa Series suivants sont éligibles à l'obtention d'une licence d'un an sur l'abonnement TotalSecure* à l'appliance virtuelle NSv correspondante sans frais supplémentaires.

Pare-feu NSa éligible	Pare-feu NSv correspondant
NSa 5650	NSv 200
NSa 6650	NSv 200
NSa 9250	NSv 400
NSa 9450	NSv 400
NSa 9650	NSv 400

** L'abonnement TotalSecure à l'appliance virtuelle NSv inclut le pare-feu virtuel NSv, une passerelle antivirus, une solution anti-logiciel espion, un service de pare-feu des applications et de prévention des intrusions, ainsi que le service de filtrage de contenu et une assistance 24 h sur 24, 7 jours sur 7.*

Numéros de modèles réglementaires :

NSa 2650 - 1RK38-0C8
NSa 3650 - 1RK38-0C7
NSa 4650 - 1RK39-0C9
NSa 5650 - 1RK39-0CA
NSa 6650 - 1RK39-0CB
NSa 9250 - 1RK39-0CC
NSa 9450 - 1RK39-0CD
NSa 9650 - 1RK39-0CE

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.

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

Le logo Gartner Peer Insights Customers' Choice est une marque commerciale et une marque de service de Gartner, Inc., et/ou de ses filiales, et est utilisé avec sa permission. Tous droits réservés. Les récompenses Gartner Peer Insights Customers' Choice sont attribuées d'après les opinions subjectives d'utilisateurs finaux sur la base de leur expérience personnelle, le nombre d'avis publiés sur Gartner Peer Insights et les notes données à un fournisseur sur le marché, comme décrit plus amplement ici, et ne représentent en aucun cas le point de vue de Gartner ou de ses filiales.

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

Datasheet-NetworkSecurityAppliance-COG-2464