SonicWall Network Security services platform (NS*sp*) 12000 Series

La sécurité évolutive de pointe qui s'appuie sur la puissance des renseignements Cloud.

Les solutions SonicWall Network Security services platform (NS*sp*) 12000 Series adoptent une approche moderne de la détection et de la prévention des menaces en combinant les renseignements dans le Cloud avec une protection basée sur les appliances dans une plateforme haut débit évolutive. Conçues pour les grandes entreprises distribuées, les centres de données et les fournisseurs de services, les pare-feux de nouvelle génération NS*sp* Series s'appuient sur les technologies d'apprentissage profond novatrices utilisées pour la plateforme Capture Cloud pour assurer une protection fiable contre les menaces les plus évoluées, sans ralentissement des performances.

Sécurité pour l'entreprise

Le volume et la sophistication des attaques réseau actuelles continuent d'augmenter. L'identification et le blocage des menaces zero-day inconnues et des intrusions nécessitent une approche qui étend la protection intégrée avec des renseignements sur la sécurité dans le Cloud. Sans ces renseignements, les solutions de sécurité de passerelle des entreprises ne peuvent pas anticiper les menaces complexes actuelles.

Les pare-feux SonicWall NS*sp* Series utilisent les renseignements sur les menaces recueillis par notre équipe de recherche Capture Labs dédiée et les combinent avec des outils de sécurité intégrés pour assurer une protection mise à jour en continu. Le service SonicWall Capture Advanced Threat Protection (ATP) basé sur le Cloud utilise la technologie Real-Time Deep Memory Inspection (RTDMI™) en instance de brevet pour détecter et bloquer de manière proactive les menaces zero-day grand public et les logiciels malveillants inconnus en inspectant directement la mémoire. Grâce à l'architecture en temps réel, la technologie RTDMI de SonicWall est précise, réduit le nombre de faux positifs et identifie et limite les attaques sophistiquées dans lesquelles l'arsenal d'armes des logiciels malveillants est exposé pendant moins de 100 nanosecondes. Renforcer la sécurité Cloud, c'est ce que fait le moteur single-pass RFDPI® (Reassembly-Free Deep Packet Inspection) breveté de SonicWall qui inspecte le trafic réseau entrant et sortant sur le pare-feu. En utilisant la plateforme SonicWall Capture Cloud ainsi que des fonctionnalités intégrées, notamment prévention des intrusions, anti-logiciels espions et filtrage Web/d'URL, les pare-feux NS*sp* Series peuvent assurer en temps réel la prévention automatisée des failles dont les entreprises ont besoin.

Avec l'augmentation du nombre de connexions Web chiffrées, il est essentiel que les pare-feux de nouvelle génération puissent inspecter le trafic chiffré afin de détecter les menaces cachées. Les pare-feux SonicWall offrent une protection complète, quels que soient le port ou le protocole, puisqu'ils déchiffrent et inspectent entièrement les centaines de milliers de connexions TLS/SSL et SSH chiffrées. Le pare-feu procède à une inspection approfondie de chaque paquet afin de détecter les anomalies de protocole, les menaces, les attaques zero-day, les intrusions et même certains critères définis. Le moteur d'inspection approfondie des paquets détecte et empêche les attaques qui exploitent le chiffrement, bloque les téléchargements de logiciels malveillants chiffrés, 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.

Avantages :

Prévention des menaces et performances haut de gamme

- Technologie RTDMI (Real-Time Deep Memory Inspection) en instance de brevet
- Technologie RFDPI (Reassembly-Free Deep Packet Inspection) brevetée
- Prévention des menaces basée sur le Cloud et intégrée
- Déchiffrement et inspection TLS/SSL
- Efficacité de la sécurité reconnue par le secteur
- Interfaces multiples 40 GbE et 10 GbE
- Équipe de recherche sur les menaces Capture Labs dédiée

Contrôle du réseau et flexibilité

- Puissant système d'exploitation SonicOS
- Surveillance et contrôle des applications
- Segmentation du réseau
- Déploiement à la périphérie du réseau ou au cœur du centre de données

Évolutivité et fiabilité

- Nombre élevé de connexions DPI-SSL
- Options de configuration multiples
- Module de stockage intégré
- Alimentations et ventilateurs redondants

Face à la croissance des entreprises, il est de plus en plus important d'offrir des possibilités de sécurité évolutives. SonicWall prend en charge les réseaux d'entreprise en pleine croissance grâce à une solution qui élimine les problématiques d'ajout de puissance de traitement supplémentaire. Les solutions NS*sp* 12400 incluent quatre modules processeur avec possibilité d'aller jusqu'à huit, tandis que les solutions NS*sp* 12800 intègrent déjà huit modules.

L'activation de l'inspection approfondie des paquets notamment IPS, antivirus, anti-logiciels espions et déchiffrement/inspection TLS/SSL sur le pare-feu ralentit souvent les performances du réseau, parfois radicalement. Les pare-feux de nouvelle génération NS*sp* Series possèdent toutefois des interfaces haut débit 40 GbE et 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-feux.

Contrôle du réseau et flexibilité

SonicOS, le système d'exploitation riche en fonctionnalités de SonicWall, est au cœur des pare-feux NS*sp* Series. SonicOS offre aux entreprises le contrôle du 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 d'autres 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 qui recherchent un maximum de flexibilité en matière de conception réseau, SonicOS propose des outils permettant de segmenter le réseau en zones à l'aide de LAN virtuels (VLAN). Ainsi, les administrateurs réseau peuvent créer une interface VLAN permettant la séparation du réseau en différents groupes logiques.

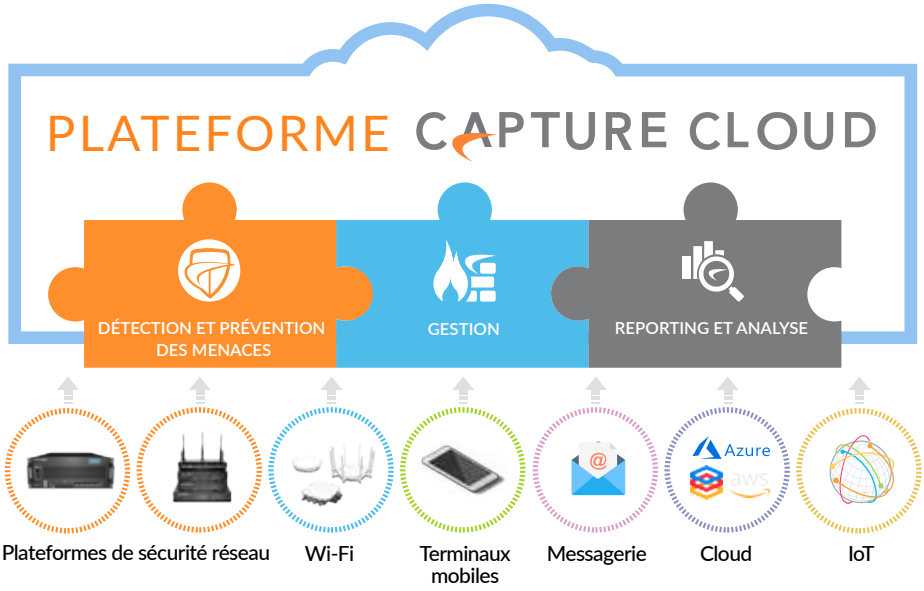
Gestion et reporting simplifiés

Les opérations de gestion continue, de surveillance et de création de rapports sur l'activité réseau sont effectuées via SonicWall GMS (Global Management System), ce qui permet aux administrateurs, depuis un tableau de bord unique, de gérer tous les aspects du réseau en temps réel. 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.

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.

Plateforme Capture Cloud

La plateforme SonicWall Capture Cloud assure gestion du réseau et prévention des intrusions basée sur le Cloud ainsi que le reporting et l'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.



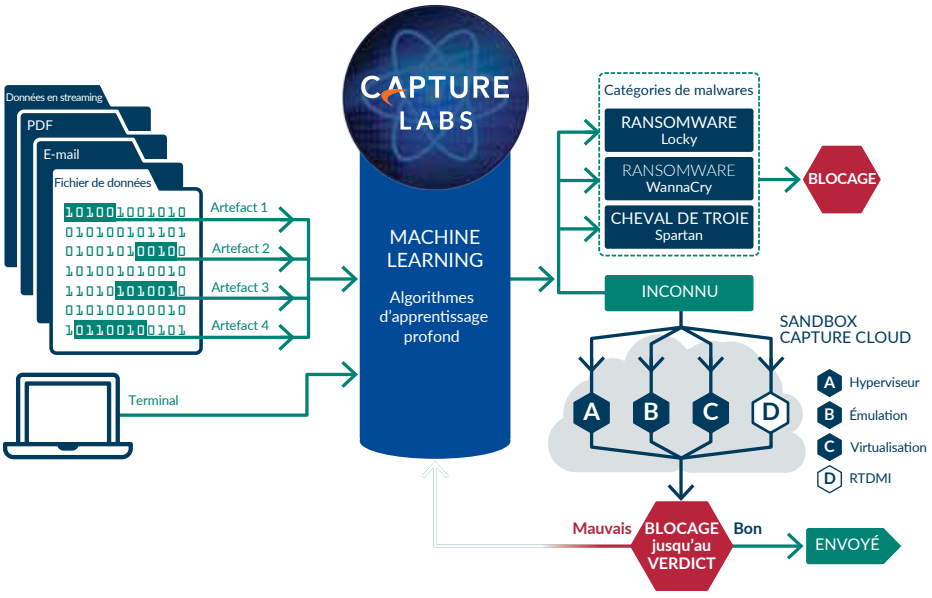
Si les données entrant sur le réseau s'avèrent contenir du code malveillant jusqu'ici inconnu, l'équipe de recherche interne Capture Labs de SonicWall dédiée aux menaces développe des signatures stockées dans la base de données de la plateforme Capture Cloud et déployées sur le pare-feu du client pour une protection actualisée. Les nouvelles mises à jour prennent effet immédiatement, sans redémarrage ni interruption. Les signatures présentes sur l'appliance offrent une protection contre un grand nombre d'attaques. Chaque signature peut couvrir des dizaines de milliers de menaces individuelles. Outre les moyens de lutte intégrés sur l'appliance, les pare-feux NS*sp* disposent d'un accès continu 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 outre, la plateforme Capture Cloud offre un écran unique de gestion et les administrateurs peuvent aisément créer des rapports en temps réel et historiques sur l'activité réseau.

Protection contre les menaces évoluées

Au centre de la prévention automatisée des failles en temps réel de SonicWall se trouve le service Capture Advanced Threat Protection, une sandbox multi-moteur 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 à l'aide d'algorithmes d'apprentissage profond, avec possibilité de les retenir à la passerelle jusqu'à ce qu'un verdict soit rendu. La plateforme sandbox multi-moteur, qui inclut l'inspection RTDMI (Real-Time Deep Memory Inspection), 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, il est bloqué et un hachage est immédiatement créé dans Capture ATP. Peu après, une signature est 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.



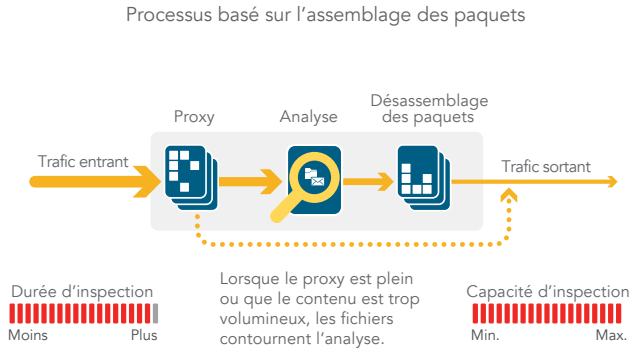
SONICWALL

Moteur RFDPI (Reassembly-Free Deep Packet Inspection)

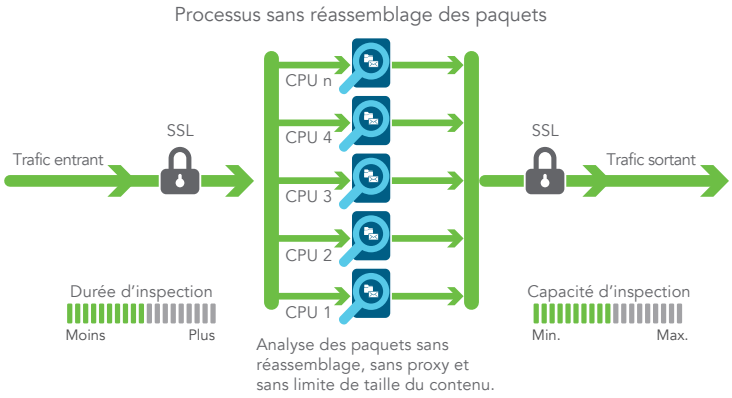
La technologie RFDPI (Reassembly-Free Deep Packet Inspection) est un système d'inspection à faible latence en un seul passage qui effectue des analyses bidirectionnelles à grande vitesse des flux de trafic sans proxy ni mise en mémoire tampon pour détecter efficacement les tentatives d'intrusion et les 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 correspondants sont créés. Mais le moteur peut aussi être configuré uniquement pour le filtrage ou, si la détection des applications est activée, de manière à fournir les services de gestion de la bande passante au niveau de la couche 7 pour le reste du flux dès lors qu'une application a été identifiée.



Architecture concurrente

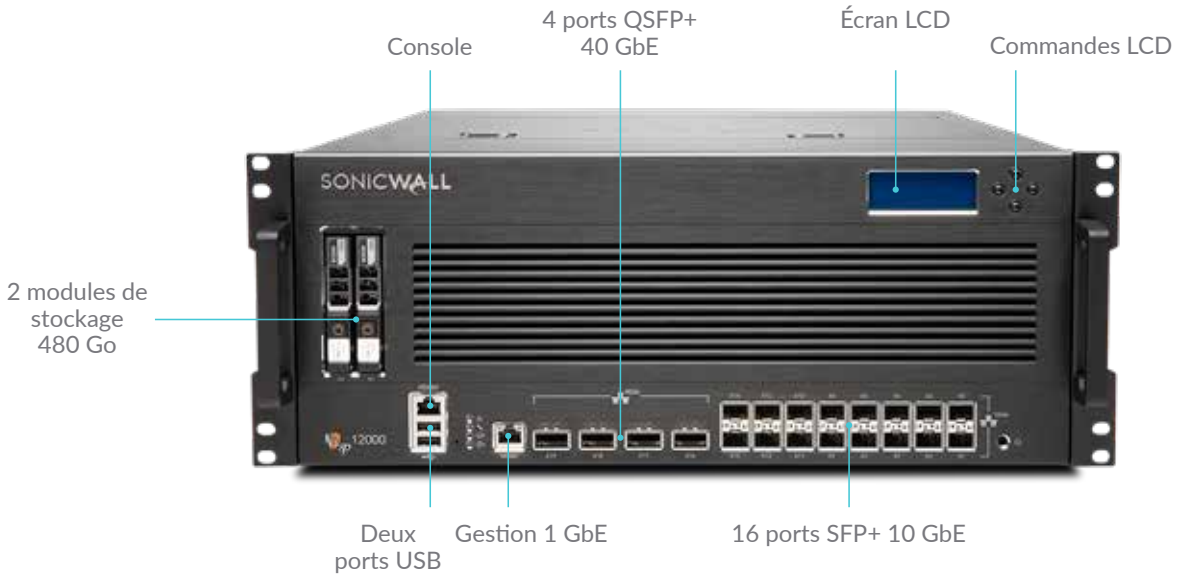


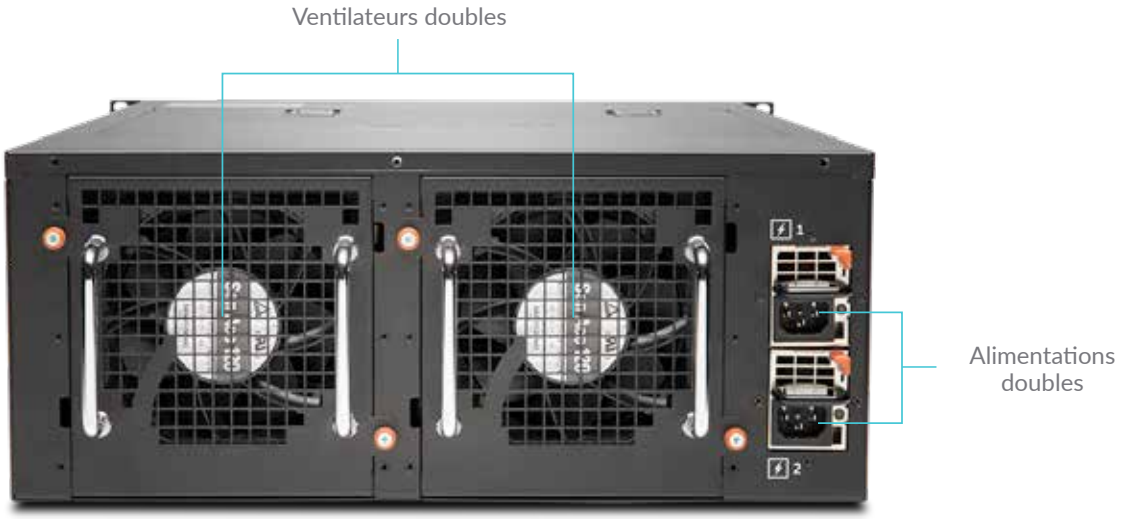
Architecture SonicWall

Gestion globale et reporting

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 solutions d'accélération WAN de SonicWall 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 règlementations de conformité. SonicWall Global Management System (GMS), la solution de gestion et de reporting sur site de SonicWall, offre, 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.

NS*sp* 12000 Series





Pare-feu	NS*sp* 12400	NS*sp* 12800
Débit du pare-feu	58,4 Gbit/s	120,3 Gbit/s
Débit IPS	36,8 Gbit/s	73,0 Gbit/s
Débit d'inspection des logiciels malveillants	33,5 Gbit/s	67,5 Gbit/s
Débit prévention des menaces	33,5 Gbit/s	67,5 Gbit/s
Débit IMIX	14,8 Gbit/s	29,0 Gbit/s
Nb max. de connexions (DPI)	16 000 000	32 000 000
Nouvelles connexions/s	430 000/s	860 000/s
Module de stockage	2 x 480 Go	2 x 480 Go
Description	**Référence**	**Référence**
Pare-feu NS*sp* uniquement	01-SSC-1206	01-SSC-1207
NS*sp* TotalSecure Advanced (1 an)	01-SSC-7883	01-SSC-9139

Résumé des fonctionnalités SonicOS

Pare-feu

- Inspection stateful 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 multi-moteur 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[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

Protection contre les 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 du trafic et analyse

- Activité des utilisateurs
- Utilisation des applications/bande passante/menaces

Filtrage du contenu Web[1]

- Filtrage des URL
- Anonymiseurs
- Blocage par mots-clés
- Insertion d'en-têtes 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

- PortShield
- Trames Jumbo
- Journalisation améliorée
- Jonction VLAN
- RSTP (Rapid Spanning Tree Protocol)
- Mise en miroir des ports
- Sécurité des ports
- Qualité de service de couche 2
- Routage dynamique (RIP/OSPF/BGP)
- Routage à base de règles
- NAT
- Proxy DNS/DNS
- Serveur DHCP
- Gestion de la bande passante
- Agrégation de liens (statique et dynamique)
- Redondance de ports
- Haute disponibilité A/P avec synchronisation d'état
- Clustering A/A
- Équilibrage de la charge entrante/sortante
- Mode pont de couche 2, filaire/filaire virtuel, mode TAP
- Routage asymétrique
- Prise en charge Common Access Card (CAC)

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
- 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

- 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

Stockage

- Journaux
- Rapports
- Sauvegardes firmware

[1]Requiert un abonnement supplémentaire

SONICWALL

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.
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	La série NS*sp* prend en charge les modes haute disponibilité actif/passif (A/P) avec synchronisation de l'état, DPI actif/actif (A/A) et mise en cluster active/active. Le mode DPI actif/actif permet de décharger la charge DPI vers les cœurs sur l'appliance passive pour optimiser le débit.
Protection contre les attaques DDoS/DoS	La protection contre les inondations SYN permet de contrer les attaques DoS à l'aide des technologies de liste noire SYN de couche 2 et de proxy SYN de couche 3. Par ailleurs, elle offre la possibilité de se prémunir contre les attaques DoS/DDoS via la protection contre les inondations UDP/ICMP et la limitation du débit de connexion.
Prise en charge IPv6	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	Les pare-feux NS*sp* 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.
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.
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 création de rapports	
Fonctionnalité	Description
Global Management System (GMS)	La configuration et la gestion des appliances SonicWall sont disponibles sur site via SonicWall Global Management System (GMS).
Gestion puissante avec un seul appareil	L'interface Web intuitive offre une interface de ligne de commande complète, prend en charge le protocole SNMPv2/3 et permet une configuration rapide et pratique.
Rapports sur les flux applicatifs IPFIX/ NetFlow	Exporte des analyses du trafic applicatif et des données d'utilisation via les protocoles IPFIX ou NetFlow pour offrir une surveillance et des rapports historiques et en temps réel sur SonicWall Analytics ou d'autres outils prenant en charge IPFIX et NetFlow via des extensions.
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 à la série NS*sp* de faire office de concentrateur VPN pour des milliers d'autres sites importants, agences ou postes de télétravail.
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 à base de routes	La possibilité d'effectuer un routage dynamique sur des liens VPN garantit une disponibilité continue en cas de panne temporaire d'un tunnel VPN via la redirection fluide du trafic entre les points de terminaison sur des routes alternatives.

Indicateur de contexte/contenu	
Fonctionnalité	Description
Suivi de l'activité des utilisateurs	Fournit les données d'identification et d'activité des utilisateurs grâce à l'intégration transparente des services SSO AD/LDAP/ Citrix/Terminal Services associée aux nombreuses informations obtenues par l'inspection approfondie des paquets.
Identification du trafic par pays GeoIP	Identifie et contrôle le trafic réseau en direction ou provenant de pays spécifiques pour contrer les attaques liées à une activité d'origine suspecte ou connue ou pour faire des recherches sur le trafic suspect provenant du réseau. Permet de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP. Supprime le filtrage indésirable des adresses IP dû à une classification erronée.
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 multi-moteur	La plateforme sandbox multi-moteur, 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.
Real-Time Deep Memory Inspection (RTDMI)	Cette technologie Cloud en instance de brevet détecte et bloque les logiciels malveillants qui n'affichent aucun comportement malveillant mais masquent leur arsenal via le chiffrement. En obligeant les logiciels malveillants à révéler leur arsenal en mémoire, le moteur RTDMI détecte et bloque de manière proactive les menaces zero-day grand public et les malwares inconnus.
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, 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 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	
Fonctionnalité	Description
Déchiffrement et inspection TLS/SSL	Déchiffre et inspecte le trafic TLS/SSL chiffré à la volée, sans proxy, pour détecter les logiciels malveillants, les intrusions et les fuites de données, et applique les règles de contrôle du contenu, des URL et des applications afin de contrer les menaces dissimulées au sein du trafic SSL chiffré. Inclus avec les abonnements de sécurité pour tous les modèles NS*sp* 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 sur les 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-malware Capture Cloud	Les serveurs Cloud SonicWall hébergent une base de données de dix 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 avec des 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 de contenu	
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.
Enforced Content Filtering Client	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 possède un logiciel antivirus et/ou un certificat DPI-SSL appropriés, installés et actifs, éliminant ainsi les coûts couramment liés à la gestion des logiciels 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 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.

Spécifications système NS*sp* Series

Pare-feu – Général	NS*sp* 12400	NS*sp* 12800
Système d'exploitation	SonicOS 6.5.1.8	
Cœurs de processeur de sécurité	128	256
Interfaces	4 ports QSFP+ 40 GbE, 16 ports SFP+ 10 GbE Gestion 1 GbE, 1 console	4 ports QSFP+ 40 GbE, 16 ports SFP+ 10 GbE Gestion 1 GbE, 1 console
Stockage intégré	2 x 480 Go	
Gestion	CLI, SSH, Web UI, GMS, API REST	
Utilisateurs de l'authentification unique (SSO)	110 000	110 000
Nb. max. de points d'accès pris en charge	128	128
Journalisation	Analyzer, Local Log, Syslog, IPFIX, NetFlow	
Performances pare-feu/VPN	**NS*sp* 12400**	**NS*sp* 12800**
Débit d'inspection du pare-feu[1]	58,4 Gbit/s	120,3 Gbit/s
Débit prévention des menaces[2]	33,5 Gbit/s	67,5 Gbit/s
Débit d'inspection des applications[2]	45,5 Gbit/s	91,0 Gbit/s
Débit IPS[2]	36,8 Gbit/s	73,0 Gbit/s
Débit d'inspection des logiciels malveillants[2]	33,5 Gbit/s	67,5 Gbit/s
Débit IMIX	14,8 Gbit/s	29,0 Gbit/s
Débit d'inspection et de déchiffrement TLS/SSL (DPI SSL)[2]	8,1 Gbit/s	17,6 Gbit/s
Débit VPN[3]	24,5 Gbit/s	47,0 Gbit/s
Connexions/s	430 000/s	860 000/s
Nb. de connexions max. (SPI)	40 000 000	80 000 000
Nb. de connexions max. (DPI)	16 000 000	32 000 000
Nb de connexions max. (DPI SSL)	800 000	1 600 000
VPN	**NS*sp* 12400**	**NS*sp* 12800**
Tunnels VPN site à site	25 000	25 000
Clients VPN IPSec (max.)	2 000 (10 000)	2 000 (10 000)
Clients VPN SSL NetExtender (max)	2 (3 000)	2 (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	**NS*sp* 12400**	**NS*sp* 12800**
Attribution d'adresses IP	Statique (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP	
Modes NAT	1:1, plusieurs:1, 1:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent	
Interfaces VLAN	512	512
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage basé sur des règles	
QoS	Priorité, bande passante max., garantie, marquage DSCP, 802.1p	
Authentification	LDAP, 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	Actif/passif avec synchro. d'état, DPI actif/actif avec synchro. d'état, mise en cluster active/active	
Matériel	**NS*sp* 12400**	**NS*sp* 12800**
Alimentation	Double, redondante, 1200 W	
Ventilateurs	Doubles, amovibles	
Puissance d'entrée	100-240 VCA, 50-60 Hz	
Consommation max. (W)	679	965
Temps de fonctionnement entre deux pannes à 25 °C (heures)	113 114	91 118
Temps de fonctionnement entre deux pannes à 25 °C (années)	12,9	10,4
Format	Montable en rack 4U	
Dimensions	61 x 43 x 18 cm/24,0 x 16,9 x 7,1 in	
Poids	26,9 kg (59,3 lb)	30,5 kg (67,2 lb)
Poids DEEE	30,7 kg (67,7 lb)	34,3 kg (75,6 lb)
Poids de transport	37,7 kg (83,1 lb)	41,3 kg (91,1 lb)
Principales règlementations	FCC classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI classe A, MSIP/KCC classe A, UL, cUL, TUV/GS, CB, Mexico CoC par UL, WEEE , REACH, ANATEL, BSMI	
Environnement (fonctionnement/stockage)	0°-40°C (32°-105°F) / -40° à 70°C (-40° à 158°F)	
Taux d'humidité	10 à 95 % sans condensation	

[1] Méthodes de test : performances maximales basées sur RFC 2544 (pour pare-feu). Les performances réelles peuvent varier suivant les conditions de réseau et les services activés.
[2] Débit DPI/antivirus de passerelle/anti-logiciels espions/IPS complet mesuré en utilisant les tests de performance HTTP Spirent WebAvalanche et les outils de test Ixia conformes aux standards actuels. Tests effectués avec différents flux, via plusieurs paires de ports. Débit pour la prévention des menaces mesuré avec Gateway AV, Anti-Spyware, IPS et Application Control activés. 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 1280 octets et conformément à la norme RFC 2544. Sous réserve de modification des spécifications, des fonctionnalités et de la disponibilité.
˙Utilisation future. Toutes les caractéristiques, fonctionnalités et disponibilités peuvent faire l'objet de modifications.

Informations de commande des pare-feux NS*sp* 12000 Series

NS*sp* 12400	Référence
NS*sp* 12400 TotalSecure Advanced Edition (1 an)	01-SSC-7883
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour NS*sp* 12400 (1 an)	01-SSC-6588
Capture Advanced Threat Protection pour NS*sp* 12400 (1 an)	01-SSC-6598
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus Cloud pour NS*sp* 12400 (1 an)	01-SSC-7853
Support 24h/24, 7j/7 pour NS*sp* 12400 (1 an)	01-SSC-6384
Content Filtering Service pour NSsp 12400 (1 an)	01-SSC-7698
NS*sp* 12800	**Référence**
NS*sp* 12800 TotalSecure Advanced Edition (1 an)	01-SSC-9139
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour NS*sp* 12800 (1 an)	01-SSC-6591
Capture Advanced Threat Protection pour NS*sp* 12800 (1 an)	01-SSC-7178
Prévention des menaces : prévention des intrusions, antivirus de passerelle, anti-logiciels espions de passerelle, antivirus Cloud pour NS*sp* 12800 (1 an)	01-SSC-7879
Support 24h/24, 7j/7 pour NS*sp* 12800 (1 an)	01-SSC-6498
Content Filtering Service pour NSsp 12800 (1 an)	01-SSC-7850
Modules et accessoires*	**Référence**
Module processeur NS*sp* 12000 Series	01-SSC-1211
Module SSD NS*sp* 12000 Series	01-SSC-1212
Ventilateur système NS*sp* 12000 Series	01-SSC-1213
Alimentation CA NS*sp* 12000 Series	01-SSC-1215

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

Numéros de modèles réglementaires :

NS*sp* 12400/12800 – 4RK02-0C0

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 plus d'informations.
www.sonicwall.com

Datasheet-NSsp-US-KJ-MKTG4029