



Appliances de sécurité réseau SonicWALL : la série NSA

PARE-FEU

Pare-feu de gestion unifiée des menaces

- **Gestion unifiée des menaces (UTM)**
- **Architecture multiprocesseur évolutive et filtrage RFDPI**
- **Application Intelligence, Control and Visualization**
- **Fonctionnalités de haute disponibilité dynamique et d'équilibrage de charge**
- **Hautes performances et TCO optimisé**
- **Services de routage et fonctionnalités réseau avancés**
- **Fonctionnalités de voix sur IP (VoIP) normalisées**
- **Services WLAN sécurisés**
- **Qualité de service intégrée**

En matière d'accès aux applications vitales internes et externes, les entreprises petites comme grandes sont entièrement dépendantes de leur réseau. Or, si les avancées dans le domaine de la réseautique procurent chaque jour de nouveaux avantages, elles sont aussi de plus en plus contrées par des méthodes évoluées de fraude financière, de nature à perturber les communications, à détériorer les performances et à mettre en péril les données. Les programmes malveillants déjouent les pare-feu à filtrage dynamique de paquets par des exploits sophistiqués visant la couche applicative. Certes, la sécurité peut être renforcée par des produits individuels, mais ces derniers sont chers, difficiles à gérer, limités dans leurs capacités à contrôler les utilisations abusives du réseau et inefficaces face aux attaques multi-fronts les plus récentes.

Fondée sur une conception multiprocesseur novatrice et sur la technologie brevetée de filtrage applicatif RFDPI (Reassembly-Free Deep Packet Inspection™)*, la série NSA SonicWALL de pare-feu UTM (Unified Threat Management) assure une protection de bout en bout dans freiner les performances du réseau. La série NSA va bien plus loin que les solutions de sécurité actuelles dans la mesure où elle analyse l'intégralité de chaque paquet en temps réel à la recherche de menaces internes ou externes.

La série NSA applique la protection UTM contre un vaste éventail d'attaques en alliant les services de prévention des intrusions, d'antivirus, d'anti-spyware, d'anti-spam et de filtrage de contenu aux fonctionnalités d'Application Intelligence, Control and Visualization. Grâce aux technologies de routage avancé, de haute disponibilité dynamique, ainsi que de VPN IPSec et SSL ultrarapides, la série NSA offre sécurité, fiabilité, fonctionnalité et productivité aux sièges, succursales et réseaux distribués de moyennes entreprises, tout en réduisant les coûts et la complexité.

Composée des NSA 240, NSA 2400, NSA 3500 et NSA 4500, la série NSA de SonicWALL propose une gamme évolutive de solutions conçues pour répondre aux besoins de n'importe quelle entreprise en matière de sécurité.

Caractéristiques et avantages

Gestion unifiée des menaces (UTM). Elle intègre les services de prévention des intrusions, d'antivirus et anti-spyware au niveau de la passerelle, d'Application Intelligence and Control, de filtrage de contenu et d'anti-spam pour bloquer les programmes malveillants et le courrier indésirable, assurer un contrôle granulaire des applications et prévenir la fuite de données.

Architecture multiprocesseur évolutive et filtrage RFDPI. Ils analysent et éliminent les menaces de fichiers de taille illimitée sans pratiquement aucun délai, sur des milliers de connexions et à vitesse de ligne.

Application Intelligence, Control and Visualization. Ce service assure un contrôle granulaire et une visualisation en temps réel des applications, permettant de garantir la hiérarchisation de la bande passante, ainsi qu'une sécurité réseau et une productivité maximales.

Fonctionnalités de haute disponibilité dynamique et d'équilibrage de charge. Elles assurent une utilisation optimale de la bande passante et la disponibilité permanente du réseau, afin de garantir un accès ininterrompu aux ressources vitales et le maintien de l'activité des tunnels VPN et autre trafic réseau en cas de basculement.

Hautes performances et TCO optimisé. La puissance de traitement de plusieurs processeurs à l'unisson accroît sensiblement le débit et offre des capacités de filtrage simultané tout en réduisant la consommation.

Services de routage et fonctionnalités réseau avancés. Ils intègrent notamment les VLAN 802.1q, le basculement multi-WAN, la gestion par zones et orientée objet, l'équilibrage de charge et les modes NAT avancés, pour une configuration flexible et granulaire, ainsi qu'un maximum de protection à la discrétion des administrateurs.

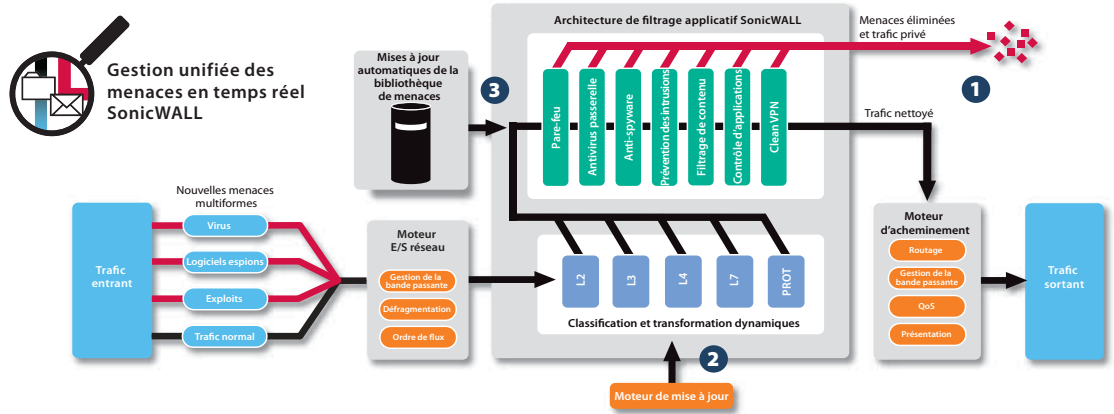
Fonctionnalités de voix sur IP (VoIP) normalisées. Chaque élément de l'infrastructure VoIP est sécurisé au plus haut niveau, des équipements de communication aux appareils VoIP tels que serveurs proxy SIP, portiers H.323 ou commutateurs logiciels.

Services WLAN sécurisés. Ils permettent à l'appliance de fonctionner comme un commutateur et contrôleur sans fil qui détecte et configure automatiquement les points d'accès sans fil SonicPoint.

Qualité de service intégrée. Les fonctionnalités QoS intégrées utilisent la norme industrielle 802.1p et les indicateurs CoS (Class of Service) DSCP (Differentiated Services Code Points) pour assurer une gestion efficace et flexible de la bande passante, indispensable notamment pour la voix sur IP, les contenus multimédias et les applications vitales.

*Brevet U.S. n° 7310815 – A method and apparatus for data stream analysis and blocking (méthode et appareil d'analyse et de blocage du flux de données).





Protection haut de gamme

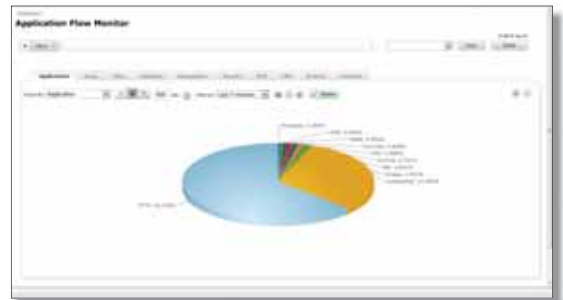
- 1 Le filtrage applicatif SonicWALL élimine les risques associés aux virus, vers, chevaux de Troie, logiciels espions, attaques de phishing, menaces émergentes ou toute utilisation abusive d'Internet. Le service d'Application Intelligence and Control offre des fonctions de contrôle hautement configurables destinées à prévenir toute fuite de données et à gérer la bande passante au niveau des applications.
- 2 La technologie RFDPI de SonicWALL (Reassembly-Free Deep Packet Inspection) s'appuie sur l'architecture multiprocesseur de SonicWALL pour analyser les paquets en temps réel sans

bloquer le trafic en mémoire. Cette fonctionnalité permet d'identifier et d'éliminer les menaces dans les fichiers sans limite de taille et sur un nombre illimité de connexions simultanées, sans interruption.

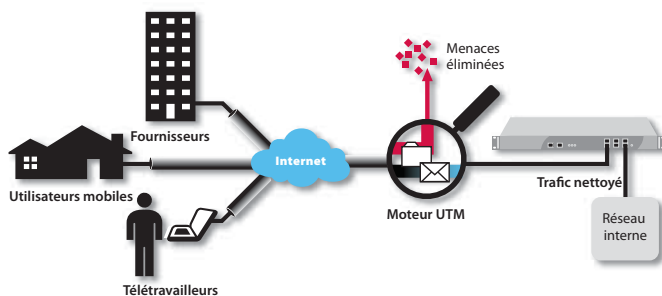
- 3 Par des mises à jour automatiques et en continu de la sécurité, la série NSA SonicWALL assure une protection réseau dynamique contre les menaces émergentes et en permanente mutation, sans aucune intervention administrative.

Application Intelligence and Control

SonicWALL Application Intelligence and Control assure un contrôle granulaire et une visualisation en temps réel des applications, permettant de garantir la hiérarchisation de la bande passante, ainsi qu'une sécurité réseau et une productivité maximales. Intégrée aux pare-feu nouvelle génération SonicWALL, cette fonctionnalité s'appuie sur la technologie RFDPI (Reassembly-Free Deep Packet Inspection™) de SonicWALL pour identifier et contrôler les applications utilisées, selon des catégories prédéfinies et faciles d'utilisation (par ex. médias sociaux ou jeux), quels que soient le port ou le protocole. L'Application Flow Monitor de SonicWALL fournit des graphiques en



temps réel des applications, de la bande passante en entrée et en sortie, des connexions actives à des sites Internet et de l'activité des utilisateurs.



SonicWALL Clean VPN

La série NSA intègre la technologie novatrice SonicWALL Clean VPN™ qui neutralise vulnérabilités et programmes malveillants sur le trafic provenant des terminaux mobiles distants et des succursales avant qu'il n'arrive sur le réseau de l'entreprise, sans intervention des utilisateurs.



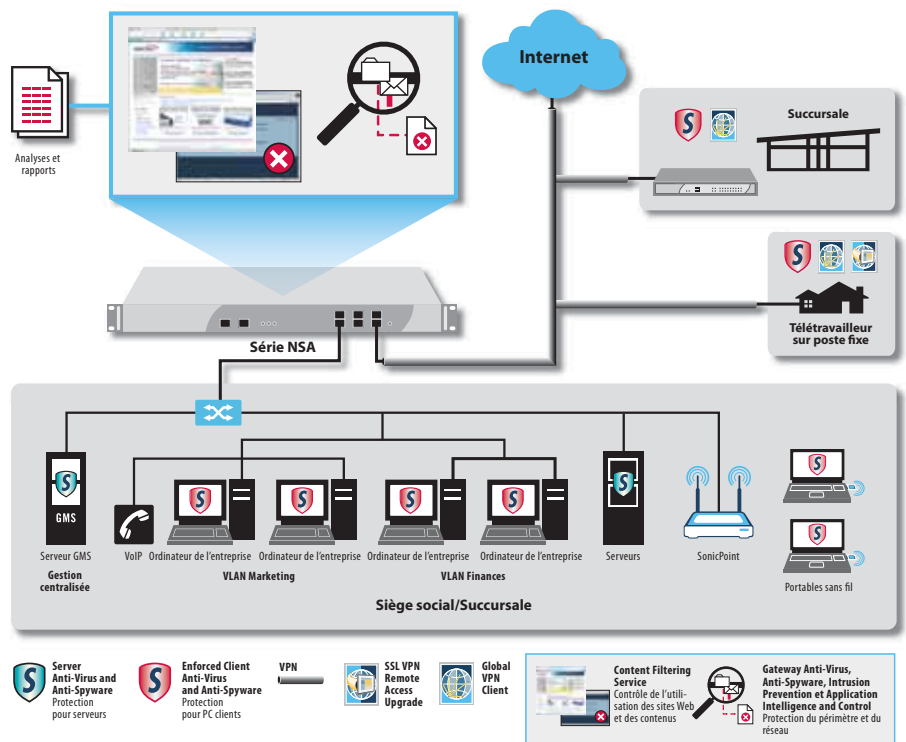
Gestion centralisée des règles

La gestion de la série NSA peut être prise en charge par le système de gestion globale SonicWALL GMS®, qui propose des outils flexibles, puissants et intuitifs permettant de gérer les configurations, de visualiser les données de surveillance en temps réel et d'intégrer le reporting de règles et de conformité, le tout de manière centralisée.

Options de déploiement flexibles et personnalisables – la série NSA en un coup d’œil

Chaque solution de la série NSA assure la protection UTM (Unified Threat Management) SonicWALL : une conception matérielle multiprocesseur inédite et la technologie de filtrage RFDPI (Reassembly-Free Deep Packet Inspection) protègent le réseau en interne comme en externe sans empiéter sur les performances. Chacun des produits de la série NSA offre les services haut débit de prévention des intrusions, de filtrage de fichiers et de contenus ainsi que d'Application Intelligence and Control performants, auxquels s'ajoute une gamme complète de fonctionnalités de mise en réseau avancées et d'outils de configuration flexibles. La série NSA constitue une plate-forme peu coûteuse, facile à installer et à gérer sur les réseaux d'entreprises, de succursales ou distribués les plus divers.

- La **NSA 4500** SonicWALL est idéale pour les sièges d'entreprises et grands réseaux distribués nécessitant des capacités et des performances élevées en matière de débit.
- La **NSA 3500** SonicWALL est idéale pour les environnements d'entreprises, de succursales ou distribués nécessitant des performances et des capacités importantes en matière de débit.
- La **NSA 2400** SonicWALL convient idéalement aux environnements de PME et de succursales soucieuses d'optimiser leurs performances et capacités de débit.
- La **NSA 240** SonicWALL convient idéalement aux PME et succursales.



Services de sécurité et mises à niveau



Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention Service et Application Intelligence and Control Service assurent une protection intelligente des réseaux, en temps réel, contre les attaques sophistiquées au niveau de la couche applicative ou basées sur le contenu : virus, logiciels espions, vers, chevaux de Troie et vulnérabilités logicielles telles que dépassements de la mémoire tampon. Le service d'Application Intelligence and Control est doté de divers outils configurables destinés à empêcher les fuites de données et à assurer un contrôle granulaire des applications, le tout complété par des outils de visualisation du trafic réseau.



Enforced Client Anti-Virus and Anti-Spyware fournit une protection antivirus et anti-spyware complète pour les ordinateurs de bureau, les portables et les serveurs, en un seul client intégré. Il assure l'exécution automatique des règles antivirus et anti-spyware, des définitions et des mises à jour logicielles à l'échelle du réseau.



Content Filtering Service exécute les règles de protection et de productivité à l'aide d'une architecture de classification novatrice fondée sur une base de données dynamique qui permet de bloquer jusqu'à 56 catégories de contenus Web indésirables.



ViewPoint Reporting présente des fonctionnalités Web conviviales qui donnent aux administrateurs un aperçu instantané des performances et de la sécurité du réseau. Grâce à une série de rapports historiques présentés sous forme de tableaux de bord et de résumés détaillés, ViewPoint aide les entreprises de toute taille à observer l'utilisation d'Internet, satisfaire aux exigences de conformité réglementaire et surveiller l'état de sécurité de leur réseau.



Virtual Assist est un outil de support distant qui permet au technicien de prendre le contrôle d'un ordinateur de bureau ou d'un portable afin de lui fournir une assistance technique à distance. Avec l'autorisation de l'utilisateur, le technicien peut instantanément accéder à son ordinateur par le biais d'un navigateur Web, puis aisément diagnostiquer et réparer les problèmes à distance sans devoir recourir à un client « lourd » préinstallé.



Les **services de support dynamique** sont disponibles en formules 8x5 ou 24x7, suivant les besoins des clients. Ils proposent un support technique de premier ordre, des mises à jour et mises à niveau firmware spécifiques, l'accès à un large éventail d'outils électroniques, ainsi qu'un remplacement matériel immédiat, pour permettre aux entreprises de retirer le maximum de leur investissement SonicWALL.



Les **mises à niveau Global VPN Client** utilisent un logiciel client installé sur les ordinateurs fonctionnant avec Windows. Elles optimisent la productivité du personnel en garantissant aux utilisateurs distants l'accès sécurisé aux e-mails, fichiers, intranets, et applications. Les licences de mises à niveau sont disponibles pour un large éventail de packs utilisateurs, ce qui permet d'adapter cette solution à mesure que l'entreprise se développe.



Les **mises à niveau de l'accès distant VPN SSL** fournissent un accès distant sans client au niveau du réseau pour les systèmes PC, Mac et Linux. Dotées de la technologie intégrée VPN SSL, les appliances UTM de SonicWALL assurent un accès distant sécurisé et fluide aux e-mails, fichiers, intranets et applications à partir d'une variété de plates-formes clientes via NetExtender, un client léger introduit dans l'ordinateur de l'utilisateur. NetExtender est automatiquement installé et configuré sans qu'aucune intervention de l'utilisateur ne soit nécessaire.



Comprehensive Anti-Spam Service (CASS) s'installe en un instant sur les pare-feu SonicWALL pour offrir aux PME une protection exhaustive contre spam et virus. Par la réunion de plusieurs solutions et la fourniture en un clic de services anti-spam, CASS accélère le déploiement, simplifie l'administration et réduit les frais généraux. Sa configuration avancée ne prend que dix minutes.

Filtrage applicatif du trafic chiffré en SSL (DPI SSL). Le trafic HTTPS entrant et sortant est déchiffré et analysé en toute transparence par le moteur RFDPI SonicWALL, avant d'être rechiffré et envoyé à sa destination d'origine en l'absence de menace ou de vulnérabilité.

Spécifications



Network Security Appliance 4500
01-SSC-7012
NSA 4500 TotalSecure* (1 an)
01-SC-7032



Network Security Appliance 3500
01-SSC-7016
NSA 3500 TotalSecure* (1 an)
01-SC-7033



Network Security Appliance 2400
01-SSC-7020
NSA 2400 TotalSecure* (1 an)
01-SC-7035



Network Security Appliance 240
TotalSecure* (1 an)
01-SSC-8760



Carte SonicWALL PC –
ExpressCard
(pour NSA 240)
01-SSC-2887

Pour plus d'informations sur les solutions de sécurité réseau SonicWALL, consultez notre site à l'adresse suivante : www.sonicwall.com.

* Inclut un an d'abonnement à Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence Service, à Content Filtering Service, à support dynamique 24x7 et à l'outil de reporting ViewPoint.

Pare-feu	NSA 240	NSA 2400	NSA 3500	NSA 4500
Version SonicOS	SonicOS Enhanced 5.6 (ou version supérieure)			
Débit dynamique ¹	600 Mbit/s	775 Mbit/s	1,5 Gbit/s	2,75 Gbit/s
Performances GAV ²	115 Mbit/s	160 Mbit/s	350 Mbit/s	690 Mbit/s
Performances IPS ³	195 Mbit/s	275 Mbit/s	750 Mbit/s	1,4 Gbit/s
Performances UTM ⁴	110 Mbit/s	150 Mbit/s	240 Mbit/s	600 Mbit/s
Performances IMIX ⁵	195 Mbit/s	235 Mbit/s	580 Mbit/s	700 Mbit/s
Connexions (max.) ⁶	85 000/110 000*	225 000	325 000	500 000
Connexions DPI (max.)	32 000/50 000*	125 000	175 000	250 000
Nouvelles connexions/s	2 000	4 000	7 000	10 000
Nb de nœuds supportés	Illimité			
Prévention d'attaques par déni de service	22 classes d'attaques DoS, DDoS et scans			
Nb de SonicPoint pris en charge (max.)	16	32	32	64
VPN	NSA 240	NSA 2400	NSA 3500	NSA 4500
Débit 3DES/AES ⁷	150 Mbit/s	300 Mbit/s	625 Mbit/s	1,0 Gbit/s
Tunnels VPN site à site	25/50 ⁸	75	800	1 500
Licences Global VPN Client incluses (max.)	2 (25)	10 (250)	50 (1 000)	500 (3 000)
Licences VPN SSL incluses (max.)	2 (15)	2 (25)	2 (30)	2 (30)
Virtual Assist inclus (max.)	1 essai de 30 jours (5)	1 (5)	2 (10)	2 (10)
Chiffrement/authentification/groupes DH	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1/groupes DH 1, 2, 5, 14			
Echange de clés	IKE, IKEv2, clé manuelle, PKI (X.509), L2TP sur IPSec			
VPN à base de routes	Oui (OSPF, RIP)			
Certificats pris en charge	Verisign, Thawte, Cybertrust, RSA Keon, Entrust et Microsoft CA pour VPN SonicWALL à SonicWALL, SCEP			
DPD (Dead Peer Detection)	Oui			
DHCP Over VPN	Oui			
IPSec NAT Traversal	Oui			
Passerelle VPN redondante	Oui			
Plates-formes Global VPN Client prises en charge	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32/64 bits, Windows 7 32/64 bits			
Plates-formes VPN SSL prises en charge	Microsoft® Windows 2000/XP/Vista 32 bits/64 bits/Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE			
Services de sécurité	NSA 240	NSA 2400	NSA 3500	NSA 4500
Service de filtrage applicatif	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention et Application Intelligence and Control			
Content Filtering Service (CFS) Premium Edition	Analyse d'URL HTTP, d'IP HTTPS, de mots-clés et de contenus, blocage ActiveX, d'applets Java et de cookies gestion de la bande passante sur les catégories de filtrage, listes d'autorisation/interdiction			
Enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP et FTP, blocage automatique de pièces jointes par le client McAfee™			
Comprehensive Anti-Spam Service ⁹	Pris en charge			
Application Intelligence and Control	Gestion et contrôle de la bande passante applicative, applications prioritaires ou bloquées en fonction de signatures, contrôle des transferts de fichiers, analyse sur la base de mots et expressions clés			
DPI-SSL ¹⁰	Procède au déchiffrement transparent du trafic HTTPS, analyse ce trafic à la recherche de menaces en utilisant la technologie SonicWALL de filtrage applicatif (GAV/AS/IPS/Application Intelligence/CFS), puis rechiffre le trafic avant de l'envoyer vers sa destination si aucune menace ou vulnérabilité n'a été détectée. Cette fonctionnalité s'applique aux clients comme aux serveurs.			
Mise en réseau	NSA 240	NSA 2400	NSA 3500	NSA 4500
Attribution d'adresses IP	Statique (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP			
Modes NAT	1:1, 1:plusieurs, plusieurs:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent			
Interfaces VLAN (802.1q)	10/25 ⁴	25	50	200
Routeage	OSPF, RIPv1/v2, routes statiques, routeage à base de règles, multidiffusion			
QoS	Priorité, bande passante maximum, garantie, marquage DSCP, 802.1p			
IPv6	Oui			
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix			
Base de données interne/utilisateurs SSO	100/100 utilisateurs	250/250 utilisateurs	300/500 utilisateurs	1 000/1 000 utilisateurs
VoIP	H.323v1-5 intégral, SIP, gatekeeper support, gestion de la bande passante en sortie, VoIP sur le WLAN, sécurisé par filtrage applicatif, compatibilité totale avec la plupart des dispositifs de passerelles et de communication VoIP			
Système	NSA 240	NSA 2400	NSA 3500	NSA 4500
Sécurité par zones	Oui			
Horaires	Unique, périodique			
Gestion orientée objet/groupe	Oui			
DDNS	Oui			
Gestion et surveillance	Interface utilisateur Web (HTTP, HTTPS), ligne de commande (SSH, console) SNMP v2 : gestion globale avec SonicWALL GMS			
Journalisation et reporting	ViewPoint™, Local Log, Syslog, Solera Networks, NetFlow v5/v9, IPFIX avec extensions, visualisation en temps réel			
Haute disponibilité	Active/passive en option avec synchronisation d'état ¹¹	Active/passive en option avec synchronisation d'état	Active/passive en option avec synchronisation d'état	Active/passive avec synchronisation d'état
Équilibrage de charge	Oui, (sortant, cyclique, suivant le pourcentage du trafic et par débordement) ; (entrant, cyclique, répartition aléatoire, sticky IP, remappage de blocs et symétrique)			
Normes	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Normes sans fil	802.11 a/b/g/n, WPA2, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS			
Matériel	NSA 240	NSA 2400	NSA 3500	NSA 4500
Interfaces	(3) ports Gigabit Ethernet+ (6) 10/100, 2 USB, emplacement de carte PC (en option modem analogique/3G), 1 interface console	(6) ports cuivre Gigabit 10/100/1000, 1 interface console, 2 USB		
Mémoire vive	256 Mo	512 Mo	512 Mo	512 Mo
Mémoire flash	Compact Flash 32 Mo	Compact Flash 512 Mo		
Sans-fil 3G/Modem*	Avec modem adaptateur USB 3G			
Alimentation	36 W (externe)	1 ATX 180 W		
Ventilateurs	Pas de ventilateur	2 ventilateurs		
Consommation max.	10-240 V, 50-60 Hz	100-240 VCA, 60-50 Hz		
Alimentation d'entrée	15 W	42 W	64 W	66 W
Dissipation thermique totale	51,1 BTU	144 BTU	219 BTU	225 BTU
Certifications	EAL4+, VPNC, ICSA Firewall 4.1		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1	
Certifications (en instance)	FIPS 140-2		-	
Facteur de forme et dimensions	18,1 x 3,8 x 26,7 cm 7,1 x 1,5 x 10,5 in	1U rackable/ 43,2 x 26 x 4,4 cm 17 x 10,3 x 1,8 in		1U rackable/ 43,2 x 33,7 x 4,4 cm 17 x 13,3 x 1,8 in
Poids	1,16 kg/2,55 lbs	3,65 kg/8,05 lbs		5,14 kg/11,30 lbs
Poids DEEE	1,43 kg/3,15 lbs	3,65 kg/8,05 lbs		5,14 kg/11,30 lbs
Conformité aux normes suivantes	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUV/GS, CB, NOM, RoHS, DEEE			
Environnement	32-105 °F, 0-40 °C		5-40 °C, 40-105 °F	
MTBF	9,5 ans		14,3 ans	
Humidité	0-95 % non condensée		10-90 % non condensée	

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 UTM/Gateway AV/Anti-Spyware/IPS basé sur le test de performances HTTP standard Spirent WebValanche et les outils de test Ixia. Tests effectués avec différents flux, via plusieurs paires de ports. ³ Le nombre maximal effectif de connexions est inférieur quand les services UTM sont activés. ⁴ Seulement avec NSA 240 Stateful HA & Expansion Upgrade. ⁵ Débit VPN basé sur le trafic UDP par paquets de 1280 octets selon RFC 2544. ⁶ Pris en charge sur l'appliance NSA 3500 ou supérieure. ⁷ Non disponible sur l'appliance NSA 2400. ⁸ Comprehensive Anti-Spam Service prend en charge un nombre illimité d'utilisateurs, mais est recommandé pour 250 utilisateurs ou moins. ⁹ Carte USB 3G et modem non fournis. Pour savoir quels appareils USB sont pris en charge, consultez <http://www.sonicwall.com/us/products/cardsupport.html>. ¹⁰ Comprehensive Anti-Spam Service prend en charge un nombre illimité d'utilisateurs, mais est recommandé pour 250 utilisateurs ou moins.

Certifications



SonicWALL France
T +33 1 49 33 73 19 France@sonicwall.com
SonicWALL BeNeLux
T +32 (0) 15 280 985 Benelux@sonicwall.com
Contacts du support SonicWALL
www.sonicwall.com/emea/4724.html

La gamme SonicWALL de solutions de sécurité dynamique



SÉCURITÉ
RÉSEAU



ACCÈS DISTANT
SÉCURISÉ



SÉCURISATION WEB
ET DE MESSAGERIE



SAUVEGARDE ET
RÉCUPÉRATION



GESTION
ET RÈGLES



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™