Appliances de sécurité réseau SonicWALL : la série NSA

SÉCURITÉ RÉSEAU

Solutions de protection UTM nouvelle génération

- **Sécurité nouvelle génération par SonicWALL**
- **Architecture multi-processeur évolutive et filtrage applicatif avant réassemblage**
- **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 des pare-feu à filtrage dynamique de paquets en exploitant des niveaux supérieurs du réseau. 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. La série d'appliances de sécurité réseau (NSA) SonicWALL® révolutionne la sécurité réseau. Fondée sur une conception multiprocesseur novatrice et la technologie brevetée* de filtrage applicatif « Reassembly-Free Deep Packet Inspection™ », elle assure une protection de bout en bout sans freiner les performances du réseau. Dévoilée sur la série NSA E-Class de SonicWALL, cette plate-forme est désormais disponible pour les entreprises de moyenne taille.

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. Basés sur une plate-forme de traitement multiprocesseur ultrarapide, les boîtiers NSA opèrent un filtrage applicatif sans répercussion sur les performances du réseau ou des applications.

La série NSA applique la technologie de gestion unifiée des menaces (UTM) nouvelle génération contre un éventail complet d'attaques, associant les services de prévention des intrusions, d'anti-virus et d'anti-spyware au contrôle approfondi du pare-feu applicatif SonicWALL. Grâce aux technologies de routage avancé, de haute disponibilité dynamique, et de IPSec et VPN SSL ultra-rapides, 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, NSA 4500 et NSA 5000**, 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

Sécurité nouvelle génération par SonicWALL. Intégrant la prévention des intrusions ainsi qu'un antivirus et anti-spyware au niveau de la passerelle, la nouvelle protection UTM propose également la suite d'outils configurables du pare-feu applicatif conçus pour empêcher les fuites de données et assurer un contrôle granulaire des applications.

Architecture multiprocesseur évolutive et filtrage applicatif avant réassemblage. Ils analysent et éliminent les menaces de fichiers sans limite de taille et traitent un nombre pratiquement illimité de connexions simultanées, sans compromis sur la vitesse. La série NSA 240 peut être configurée en utilisant un modem primaire, secondaire, ou des interfaces sans fil 3G pour une extensibilité durable.

Fonctionnalités de haute disponibilité dynamique et d'équilibrage de charge. Disponibles sur SonicOS 5.0 Enhanced, 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. Les technologies modernes de mise en réseau et de sécurité offertes comprennent notamment les VLAN 802.1q, le basculement automatique WAN/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.

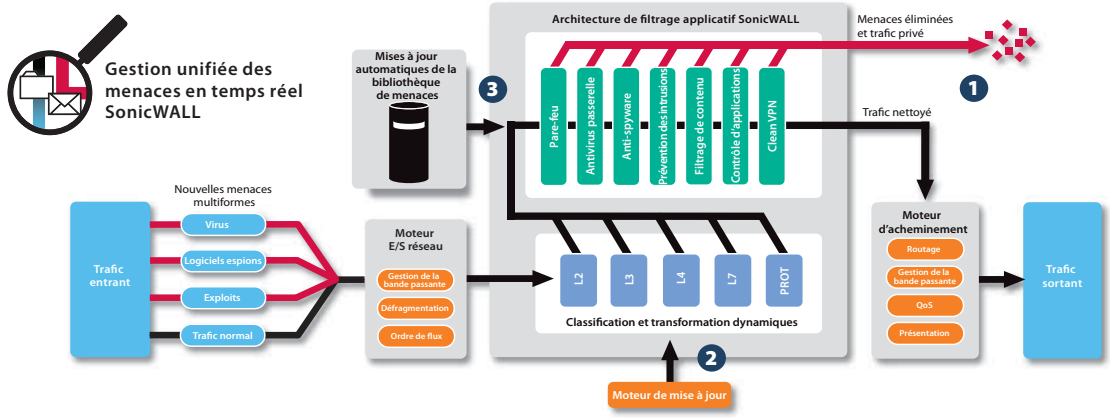
Services WLAN sécurisés. Ils permettent à l'appliance de fonctionner comme un commutateur et contrôleur sans fil sécurisé qui détecte et configure automatiquement les points d'accès sans fil SonicWALL, les SonicPoints™, garantissant ainsi la sécurité des accès distants dans les environnements réseau distribués.

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).

SONICWALL®

Architecture et gestion dynamiques de la sécurité

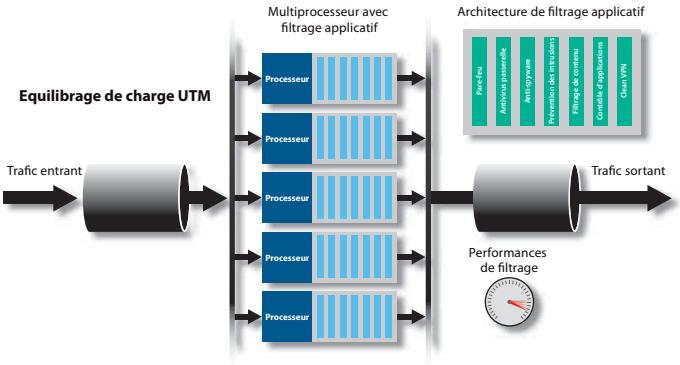


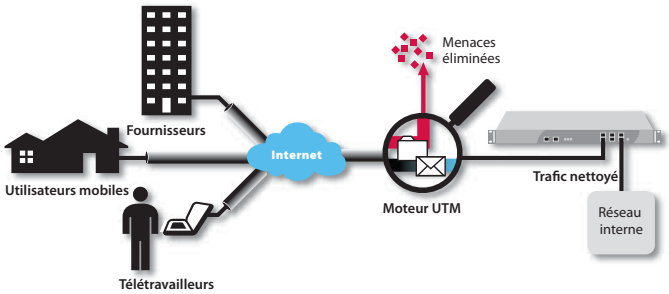
Protection haut de gamme

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 pare-feu applicatif 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 assure une protection réseau dynamique contre les menaces émergentes et en permanente mutation, sans aucune intervention administrative.

Equilibrage de charge UTM

Les dispositifs qui mettent en œuvre plusieurs technologies de protection sont particulièrement limités s'ils se contentent d'un seul processeur centralisé. L'équilibrage de charge UTM de SonicWALL associe un moteur de filtrage applicatif et de classification du trafic ultrarapide à plusieurs processeurs de sécurité qui filtrent les applications, les fichiers et le trafic de contenus en temps réel sans influencer significativement les performances ou l'évolutivité. Cette architecture permet d'analyser et de contrôler les menaces concernant les réseaux qui gèrent des applications à forte consommation de bande passante et sensibles aux délais.





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.

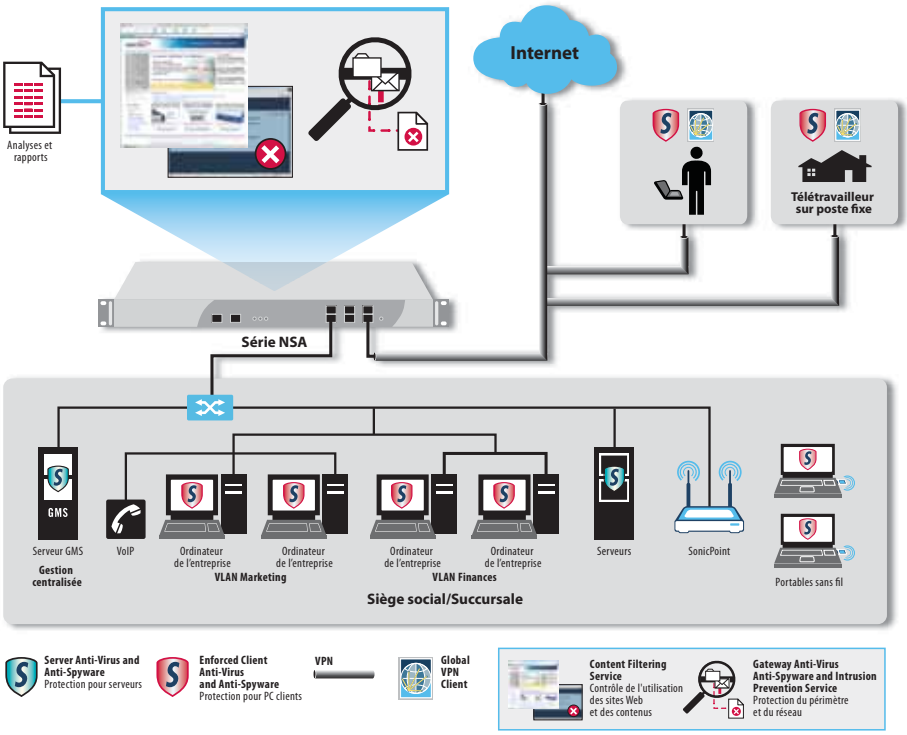
Gestion centralisée des règles

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 SonicWALL assure une protection UTM (Unified Threat Management) de nouvelle génération. Une conception matérielle multi-processeur inédite et la technologie de filtrage applicatif avant réassemblage 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, le filtrage de fichiers et de contenus et les options de contrôle efficaces du pare-feu applicatif, 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.

- Modèle haut de gamme, le SonicWALL **NSA 5000** répond aux besoins des environnements réseau les plus exigeants, de type campus ou distribués.
- Le SonicWALL **NSA 4500** est idéal pour les sièges d'entreprises et grands réseaux distribués nécessitant des capacités et des performances élevées en matière de débit.
- Le SonicWALL **NSA 3500** est idéal pour les environnements d'entreprises, de succursales ou distribués nécessitant des performances et des capacités importantes en matière de débit.
- Le SonicWALL **NSA 2400** convient idéalement aux environnements de PME et de succursales soucieuses d'optimiser leurs performances et capacités de débit.
- Le SonicWALL **NSA 240** convient idéalement aux PME et succursales.



Caractéristiques principales

Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention Service et le pare-feu applicatif 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 pare-feu applicatif est doté de divers outils configurables destinés à empêcher les fuites de données et à assurer un contrôle granulaire des applications.

Enforced Client and Server 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 conviviales basées sur le Web 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.

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.

Spécifications

Network Security Appliance 5000
01-SSC-7042

NSA 5000 TotalSecure (1 an)
01-SC-7031

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

Certifications

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

	NSA 240	NSA 2400	NSA 3500	NSA 4500	NSA 5000
Pare-feu					
Version SonicOS	SonicOS Enhanced 5.0 (ou supérieur)				
Débit dynamique[1]	600 Mbit/s	775 Mbit/s	1,5 Gbit/s	2,75 Gbit/s	3,5 Gbit/s
Performances GAV[1]	115 Mbit/s	160 Mbit/s	350 Mbit/s	690 Mbit/s	800 Mbit/s
Performances IPS[1]	195 Mbit/s	275 Mbit/s	750 Mbit/s	1,4 Gbit/s	1,7 Gbit/s
Performances UTM[1]	110 Mbit/s	150 Mbit/s	240 Mbit/s	600 Mbit/s	800 Mbit/s
Performances IMIX	195 Mbit/s	235 Mbit/s	580 Mbit/s	700 Mbit/s	950 Mbit/s
Maximum de connexions[3]	25 000/35 000[2]	48 000	128 000	450 000	600 000
Nouvelles connexions/s	2 000	4 000	7 000	10 000	12 000
Nb de nœuds supportés	Illimité				
Prévention d'attaques par déni de service	22 classes d'attaques DoS, DDoS et scans				
SonicPoints supportés (maximum)	16	32	32	64	64
VPN					
Débit 3DES/AES[1]	150 Mbit/s	300 Mbit/s	625 Mbit/s	1,0 Gbit/s	1,5 Gbit/s
Tunnels VPN site à site	25/50[2]	75	800	1 500	2 500
Licences Global VPN Client offertes (max.)	2 (25)	10 (250)	50 (1 000)	500 (3 000)	1 000 (3 500)
Licences VPN SSL incluses (max.)	2 (15)	2 (25)	2 (30)	2 (30)	2 (30)
Chiffrement / Authentification	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1				
Echange de clés	Echange de clés IKE, IKEv2, clé manuelle, PKI (X.509)				
L2TP/IPSec	Oui				
Certificats pris en charge	Verisign, Thawte, Cybertrust, RSA Keon, Entrust et Microsoft CA pour VPN SonicWALL à SonicWALL				
DPD (Dead Peer Detection)	Oui				
DHCP Over VPN	Oui				
IPSec NAT Traversal	Oui, NAT_Tv00 et v03				
Passerelle VPN redondante	Oui				
Plates-formes Global VPN Client prises en charge	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32 bits				
Plates-formes VPN SSL prises en charge	Microsoft® Windows 2000 / XP / Vista 32/64 bits, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE				
Services de filtrage applicatif					
Filtrage applicatif Service de signature	Bibliothèque de signatures exhaustive. Contrôle des applications poste à poste et de messagerie instantanée, mise à jour des signatures par une architecture d'exécution distribuée				
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				
Gateway-enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP et FTP, clients McAfee™ activés, blocage de pièces jointes				
Pare-feu applicatif	Exécution au niveau des applications et contrôle de la bande passante, régulation du trafic Web, des e-mails, des pièces jointes et des transferts de fichiers, analyse et blocage de documents et fichiers sur la base de mots et expressions clés				
Mise en réseau					
Attribution d'adresses IP	Statique (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP				
Modes NAT	1:1, 1:plusieurs, plusieurs:1, plusieurs:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent				
Interfaces VLAN (802.1q)	10/25[2]	25	50	200	256
Routage	OSPF, RIPv1/v2, routes statiques, routage à base de règles, multidiffusion				
QoS	Priorité, bande passante maximum, garantie, marquage DSCP, 802.1p				
IPv6	Compatible IPv6				
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, base de données utilisateurs interne				
Base de données utilisateurs	100 utilisateurs	250 utilisateurs	500 utilisateurs	1 000 utilisateurs	1 500 utilisateurs
VoIP	H.323v1-5 intégral, SIP, gatekeeper support, gestion de la bande passante en sortie, VoIP sur le WLAN, sécurité par filtrage applicatif, compatibilité totale avec la plupart des dispositifs de passerelles et de communication VoIP				
Système					
Sécurité par zones	Oui				
Horaires	Oui				
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				
Haute disponibilité	Active/passive en option avec synchronisation d'état[2]	Active/passive en option avec synchronisation d'état		Active/passive avec synchronisation d'état	
Equilibrage 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				
Normes sans fil	802.11 a/b/g, WP, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS				
Matériel					
Interfaces	(3) Ports Gigabit Ethernet+ (6) 10/100, 2 USB (utilisation future), emplacement de carte PC (en option modem analogique/3G), 1 interface console	(6) ports cuivre Gigabit 10/100/1000, 1 interface console, 2 USB (utilisation future)			
Mémoire vive	256 Mo	512 Mo	512 Mo	512 Mo	1 Go
Mémoire flash	Compact Flash 32 Mo	Compact Flash 512 Mo			
Alimentation	36 W (externe)	1 ATX 180 W			
Ventilateurs	Pas de ventilateur	2 ventilateurs			
Alimentation d'entrée	10-240 V, 50-60 Hz	100-240 Vac, 60-50 Hz			
Consommation max.	15 W	42 W	64 W	66 W	66 W
Dissipation thermique totale	51,1 BTU	144 BTU	219 BTU	225 BTU	225 BTU
Certifications	VPNC		EAL4+, FIPS 140-2 Level 2, VPNC		
Certifications (en instance)	ICSA Firewall 4.1, EAL-4+, FIPS 140-2		ICSA Firewall 4.1		
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, TÜV/GS, CB, NOM, RoHS, DEEE				
Environnement	0-40 °C, 32-105 °F	5-40 °C, 40-105 °F			
MTBF	À définir	16,0 ans	14,3 ans	14,1 ans	14,1 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. Débit VPN basé sur le trafic UDP par paquets de 1418 octets selon RFC 2544. Performances UTM basées sur des tests HTTP opérés sur Spirent Avalanche/Reflector. Tests effectués avec différents flux, via de multiples paires de ports.

[2] Seulement avec mise à niveau HA dynamique et mise à niveau Expansion de la série NSA 240

[3] Le nombre maximum effectif de connexions est inférieur quand les services UTM sont activés.

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

Support France
Appel gratuit : 0800.970.019
Tél. : +31 (0) 411.617.812
E-mail : sales_support-europe@sonicwall.com

Bureau France
Tél. : +33.0.1.49.33.73.09
Inside sales : +32 (0)15.293.001
E-mail : france@sonicwall.com

SONICWALL®