

- Pare-feu nouvelle génération
- Connectivité 10 GbE
- Service performant de prévention des intrusions
- Application Intelligence, Control and Visualization
- Technologie de filtrage RFDPI (Reassembly-Free Deep Packet Inspection)
- Déploiement flexible
- Filtrage applicatif du trafic chiffré en SSL (DPI SSL)
- Réseau GRID (Global Response Intelligent Defense) SonicWALL
- Accélération WAN

Les applications d'entreprise résident de nos jours tant sur le réseau que dans le cloud. Il peut s'agir de solutions professionnelles génératrices de productivité tout comme de sources de divertissement contre-productives – et souvent dangereuses. En termes de bande passante, la priorité doit être accordée aux applications vitales, tandis que les médias sociaux et autres jeux en ligne doivent pouvoir être limités, voire totalement bloqués. Les pare-feu classiques à filtrage dynamique de paquets analysent uniquement les ports et les protocoles, pas les applications. Ils ne peuvent donc pas distinguer les bonnes applications des mauvaises.

Les appliances de la série NSA (Network Security Appliance) E-Class de SonicWALL® sont des solutions hautes performances qui intègrent étroitement la prévention des intrusions, la protection anti-malware et le puissant service d'Application Intelligence, Control and Visualization. Associant la technologie SonicWALL brevetée RFDPI (Reassembly-Free Deep Packet Inspection™)* à une puissante plate-forme matérielle multi-processeur, les solutions de la série NSA E-Class sont capables d'analyser et de contrôler des milliers d'applications individuelles, même chiffrées en SSL. La série NSA E-Class peut être déployée comme pare-feu nouvelle génération ou comme pare-feu UTM (Unified Threat Management).

Constituée des appliances E8510, E8500, E7500, E6500 et E5500, la série NSA E-Class de SonicWALL offre une vaste gamme de solutions évolutives pour les déploiements les plus exigeants dans les environnements de type centres de données, campus et réseaux distribués. En tant que solution intégrée, la série NSA E-Class s'appuie sur l'infrastructure existante tout en ajoutant une couche supplémentaire de sécurité et de visibilité sur le réseau. Déployée en tant que passerelle de sécurité, elle fournit aux entreprises d'importantes fonctionnalités telles que la sécurisation de l'accès distant, la haute disponibilité et autres.

La série NSA E-Class occupe une place particulière dans l'offre SonicWALL de produits et de services professionnels pour la sécurité réseau, la sécurisation de messagerie et l'accès distant sécurisé.

Caractéristiques et avantages

Pare-feu nouvelle génération SonicWALL avec filtrage RFDPI (Reassembly-Free Deep Packet Inspection). Il intègre étroitement les services de prévention des intrusions, de protection anti-malware et d'Application Intelligence and Control optimisés, avec visualisation en temps réel.

Connectivité 10 GbE. Présente sur la NSA E8510, elle permet un déploiement dans les environnements dotés d'une infrastructure 10 GbE.

Puissante fonctionnalité de prévention des intrusions. Elle protège contre un vaste éventail de menaces au niveau de la couche applicative en recherchant directement dans le contenu des paquets de données les éventuels vers, chevaux de Troie, vulnérabilités logicielles, exploits et autres programmes malveillants.

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.

Technologie de filtrage RFDPI (Reassembly-Free Deep Packet Inspection). Elle permet de contrôler des milliers d'applications et détecte des millions d'éléments malveillants, afin de protéger le réseau de manière automatique et transparente, tout en inspectant

simultanément des centaines de milliers de connexions à travers tous les ports, sans limites dans la taille des flux ni pratiquement aucun délai.

Déploiement flexible. Soit comme passerelle classique, soit comme solution intégrée pour permettre aux administrateurs de conserver leur infrastructure tout en ajoutant le service d'Application Intelligence and Control, et de bénéficier ainsi d'une couche supplémentaire de sécurité et de visibilité sur leur réseau.

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.

Réseau GRID (Global Response Intelligent Defense) SonicWALL. Il assure la mise à jour en continu des services de protection, de détection, de prévention des intrusions et d'Application Control, 24 h/24, 7 j/7, pour une sécurité maximum. La suite complète de services de prévention des intrusions protège contre plus d'un million d'attaques de programmes malveillants.

Accélération WAN. Elle réduit la latence et augmente les vitesses de transfert entre les sites distants, optimisant l'efficacité du réseau.

Technologie d'Application Intelligence and Control

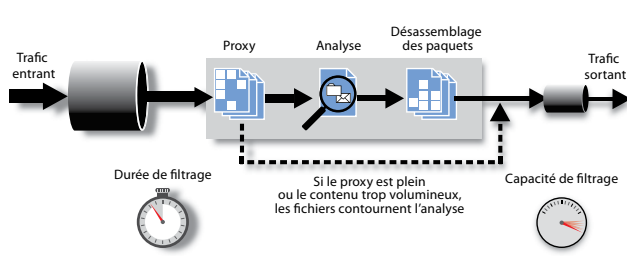
SonicWALL Application Intelligence and Control assure un contrôle granulaire et une visualisation en temps réel des applications, permettant de garantir la hiérarchisation de la bande passante, ainsi qu'une sécurité réseau et une productivité maximales. Intégrée aux pare-feu nouvelle génération SonicWALL, cette fonctionnalité s'appuie sur la technologie RFDPI (Reassembly-Free Deep Packet Inspection) pour identifier et contrôler les applications utilisées, quels que soient le port ou le protocole. Grâce à une bibliothèque de signatures de menaces constamment enrichie et capable de reconnaître actuellement plus de 3 500 applications et des millions de programmes malveillants, elle permet de conserver le contrôle des applications, de hiérarchiser ou de limiter la bande passante et de refuser l'accès à certains sites Internet. L'App 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, et peut envoyer en continu des données à des analyseurs NetFlow/IPFIX.



Moteur de filtrage RFDPI (Reassembly-Free Deep Packet Inspection)

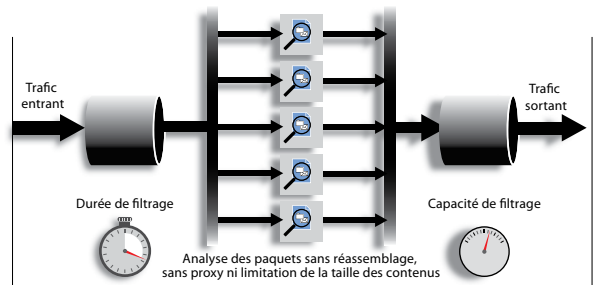
Le moteur RFDPI (Reassembly-Free Deep Packet Inspection) de SonicWALL est un moteur de filtrage évolutif des applications, capable d'analyser des fichiers et des contenus de toute taille en temps réel, sans réassembler les paquets ou le contenu des applications. Ce moyen d'analyse est spécialement conçu pour les applications en temps réel et le trafic sensible aux délais qu'il contrôle sans avoir à recourir à des connexions proxy. Grâce à ce type de moteur, le trafic réseau haut débit est filtré de manière plus efficace et plus fiable, pour un plus grand confort du côté de l'utilisateur final.

Processus basé sur l'assemblage des paquets



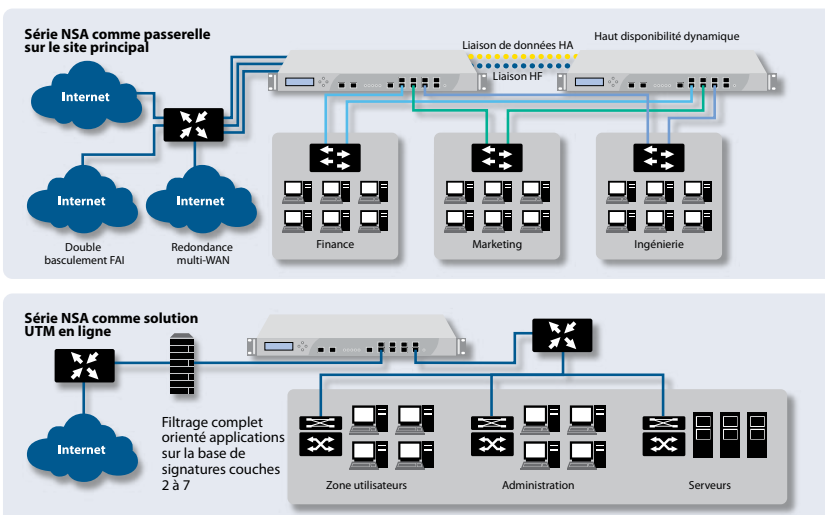
Architecture concurrente

Processus sans réassemblage des paquets



Architecture SonicWALL

Options de déploiement flexibles et personnalisables



Passerelle sur le site principal

Déployée en tant que passerelle sur le site principal, la série NSA E-Class constitue une plate-forme haut débit évolutive qui assure la segmentation du réseau et la sécurité grâce à des VLAN et zones de sécurité. Les fonctionnalités de redondance comprennent l'équilibrage de charge WAN, le basculement vers un autre FAI et le filtrage applicatif (DPI) actif/actif.

Mode pont couche 2

Le mode pont couche 2 assure une détection et une prévention en ligne des intrusions, offre un niveau supplémentaire de sécurité pour les segments de réseau ou les unités commerciales sur la base de zones et simplifie la mise en place d'une sécurité multicouche. Cela permet en outre aux administrateurs de limiter l'accès aux données sensibles suivant les unités commerciales ou les serveurs de bases de données.

Protection multicouche

Protection des sites distants

La série NSA E-Class met en œuvre des réseaux privés virtuels (VPN) ultra-haute performance qui accueillent facilement des milliers de terminaux et de succursales. La technologie novatrice Clean VPN™ de SonicWALL neutralise les vulnérabilités et les programmes malveillants en décontaminant le trafic avant qu'il entre sur le réseau de l'entreprise, en temps réel et sans intervention des utilisateurs.

Protection au niveau de la passerelle

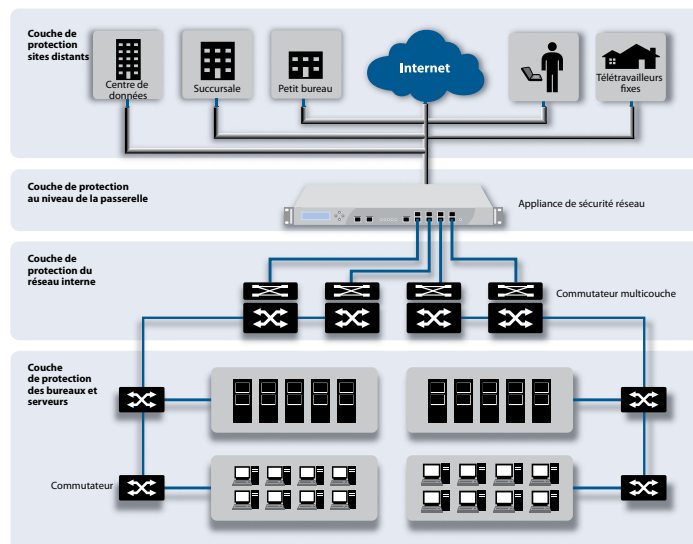
Faciles à intégrer dans les environnements existants, les NSA E-Class centralisent la protection au niveau de la passerelle et l'appliquent à l'ensemble des applications, fichiers et trafics de contenus entrants et sortants. Parallèlement, elles contrôlent la bande passante et les applications sans entraver les performances ou l'évolutivité.

Protection interne

Les NSA E-Class sont des boîtiers hautement configurables qui assurent une protection globale du réseau interne en filtrant le trafic via les interfaces LAN et les VLAN. Spécialement conçue pour lutter contre les menaces ciblant les réseaux LAN, la série NSA E-Class surveille et empêche la propagation interne de programmes malveillants et d'attaques par déni de service, l'exploitation de vulnérabilités logicielles, la transmission de documents confidentiels, les violations de règles ou l'utilisation abusive du réseau.

Protection des bureaux et serveurs

Outre la protection au niveau du réseau et de la passerelle, la série NSA E-Class offre une protection supplémentaire au niveau des points d'accès pour les postes de travail et les serveurs grâce à un client antivirus et anti-spyware offrant une technologie heuristique avancée. Ce client automatique permet de contrôler les accès au réseau en restreignant l'accès Internet aux terminaux qui ne sont pas à jour au niveau des signatures ou du moteur. Lorsque l'exécution est activée sur le boîtier, chaque point d'accès reçoit l'ordre de télécharger le client antivirus et anti-spyware. L'administrateur n'a pas à intervenir. Le déploiement de la sécurité est automatique.



Gestion centralisée des règles

Le système de gestion globale (GMS®) de SonicWALL propose des outils flexibles, puissants et intuitifs permettant de gérer de manière centralisée les configurations des NSA E-Class à travers les réseaux distribués, de visualiser les données de surveillance en temps réel et d'intégrer le reporting de règles et de conformité.



Services d'abonnement

Chaque appliance de sécurité réseau E-Class prend en charge un éventail croissant de services et de logiciels dynamiques sur abonnement compatibles avec tous les types de réseau.



Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service assure 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.



Application Intelligence and Control offre une visualisation en temps réel du trafic réseau, des règles personnalisables et un contrôle granulaire des applications et utilisateurs.



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 plus de 56 catégories de contenus Web indésirables.



ViewPoint est un outil de reporting convivial basé sur le Web qui offre 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 confor-

mité réglementaire et surveiller l'état de sécurité de leur réseau.



Spécialement conçu pour les grandes entreprises, le **support 24x7 SonicWALL E-Class** offre une assistance et une qualité de service haut de gamme. Il comprend l'accès direct à une équipe de techniciens compétents et expérimentés assurant une assistance téléphonique et Web 24 heures/24, 7 jours/7, 365 jours/an. A cela s'ajoutent les mises à jour et mises à niveau logiciel et firmware, le remplacement anticipé de matériel, l'accès aux outils de support électronique et aux groupes de discussion dirigés, et bien plus encore.



Le **filtrage applicatif du trafic chiffré en SSL (DPI SSL)** déchiffre et analyse le trafic HTTPS entrant et sortant, en toute transparence, grâce au moteur RFDPI SonicWALL. Le trafic est ensuite rechiffré et envoyé à sa destination d'origine en l'absence de menace ou de vulnérabilité.

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, et assure l'exécution automatique des règles antivirus et anti-spyware, des définitions et des mises à jour logicielles à l'échelle du réseau.

Série NSA E-Class – références



SonicWALL NSA E8510
01-SSC-9770



SonicWALL NSA E8500
01-SSC-8866



SonicWALL NSA E8500 High Availability
01-SSC-8867



SonicWALL NSA E7500
01-SSC-7000

SonicWALL NSA E7500 TotalSecure* (1 an)
01-SSC-7027



SonicWALL NSA E6500
01-SSC-7004

SonicWALL NSA E6500 TotalSecure* (1 an)
01-SSC-7028



SonicWALL NSA E5500
01-SSC-7008

SonicWALL NSA E5500 TotalSecure* (1 an)
01-SSC-7029

Services de sécurité NSA E7500 SonicWALL

SonicWALL GAV / IPS / Application Intelligence pour NSA E7500 (1 an)
01-SSC-6130

SonicWALL Comprehensive Gateway Security Suite pour NSA E7500 (1 an)
01-SSC-9220

Support 24x7 SonicWALL E-Class pour NSA E7500 (1 an)
01-SSC-7254

Services de sécurité NSA E6500 SonicWALL

SonicWALL GAV / IPS / Application Intelligence pour NSA E6500 (1 an)
01-SSC-6131

SonicWALL Comprehensive Gateway Security Suite pour NSA E6500 (1 an)
01-SSC-9221

Support 24x7 SonicWALL E-Class pour NSA E6500 (1 an)
01-SSC-7257

Services de sécurité NSA E5500 SonicWALL

SonicWALL GAV / IPS / Application Intelligence pour NSA E5500 (1 an)
01-SSC-6132

SonicWALL Comprehensive Gateway Security Suite pour NSA E5500 (1 an)
01-SSC-9222

Support 24x7 SonicWALL E-Class pour NSA E5500 (1 an)
01-SSC-7260

Les références des offres pluriannuelles sont disponibles sur www.sonicwall.com.

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

Certifications



Spécifications

	NSA E5500	NSA E6500	NSA E7500	NSA 8500	NSA 8510
Pare-feu					
Version SonicOS	SonicOS Enhanced 5.6 (ou supérieure)				SonicOS Enhanced 5.8.1 (ou supérieure)
Débit dynamique¹	3,9 Gbit/s	5 Gbit/s	5,6 Gbit/s	8,0 Gbit/s	
Débit GAV²	1,0 Gbit/s	1,69 Gbit/s	1,84 Gbit/s	2,25 Gbit/s	
Débit ISP²	2,0 Gbit/s	2,3 Gbit/s	2,58 Gbit/s	3,7 Gbit/s	
Performances Full DPI³	850 Mbit/s	1,59 Gbit/s	1,7 Gbit/s	2,2 Gbit/s	
Performances IMIX³	1,1 Gbit/s	1,4 Gbit/s	1,6 Gbit/s	2,0 Gbit/s	
Connexions (max.)³	750 000	1 000 000	1 500 000	1 500 000	
Connexions Full DPI (max.)	500 000	600 000	1 000 000	1 250 000	
Nouvelles connexions/s	30 000	60 000	64 000	85 000	
Nb de nœuds pris en charge	Illimité				
Prévention d'attaques par déni de service	22 classes d'attaques DoS, DDoS et scans				
Nb de SonicPoint pris en charge (max.)	96				128
VPN					
Débit 3DES/AES⁴	1,7 Gbit/s	2,7 Gbit/s	3,0 Gbit/s	4,0 Gbit/s	
Tunnels VPN site à site	4 000	6 000			10 000
Licences Global VPN Client incluses (max.)	2 000 (4 000)	2 000 (6 000)			2 000 (10 000)
Licences VPN SSL incluses (max.)	2 (50)	2 (50)			2 (50)
Virtual Assist inclus (max.)	1 (25)	1 (25)			1 (25)
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				
Passerelle VPN redondante	Oui				
Plates-formes Global VPN Client prises en charge	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32 bits/64 bits, Windows 7				
Plates-formes VPN SSL prises en charge	Microsoft® Windows 2000/XP/Vista 32 bits/64 bits/Windows 7 32 bits/64 bits, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE				
Services de sécurité					
Service de filtrage applicatif	Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware et Application Intelligence				
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 classification, listes d'autorisation/interdiction personnalisées				
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 Service⁵	Pris en charge				
Application Intelligence and Control	Gestion et contrôle de la bande passante applicative, applications priorisées ou bloquées en fonction de signatures, contrôle des transferts de fichiers, analyse sur la base de mots et expressions clés				
DPI-SSL	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					
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)	400	500			512
Routing	OSPF, RIPv1/v2, routes statiques, routage à base de règles, multidiffusion				
QoS	Priorité, bande passante maximum, garantie, marquage DSCP, 802.1p				
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix				
IPv6	Oui				
Base de données interne/utilisateurs SSO	1 500/2 500 utilisateurs	2 500/4 000 utilisateurs			2 500/7 000 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				
Agrégation de liens	Oui				
Redondance de ports	Oui				
Système					
Gestion et surveillance	Interface utilisateur Web (HTTP, HTTPS), ligne de commande (SSH, console) SNMP v2 ; gestion globale avec SonicWALL GMS				
Journalisation et rapports	ViewPoint*, Local Log, Syslog, Solera Networks, NetFlow v5/v9, IPFIX avec extensions, visualisation en temps réel				
Haute disponibilité	Active/passive avec synchronisation d'état, DPI actif/actif				
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, IEEE 802.3				
Normes sans fil	802.11 a/b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TLS				
Prise en charge de l'accélération WAN	Oui				
Matériel					
Interfaces	(8) ports cuivre Gigabit 10/100/1000, interface HA 1Gbe, 1 interface console, 2 USB	1 Go	(4) SFP (SX, LX ou TX), (4) 10/100/1000 GbE, interface HA 1 GbE, 2 USB, 1 interface console	2 Go	(2) SFP+ 10GbE, (4) 10/100/1000 GbE, interface HA 1 GbE, 2 USB, 1 interface console
Mémoire vive	1 Go	1 Go	2 Go	4 Go	
Mémoire flash	Compact Flash 512 Mo				
Sans-fil 3G/Modem*	Avec un adaptateur 3G ou modem analogique pris en charge				
Alimentation	1 ATX 250 W			2 ATX 250 W, remplaçables à chaud	
Ventilateurs	Ventilateurs doubles, remplaçables à chaud				
Affichage	Ecran LCD				
Alimentation d'entrée	100-240 VCA, 60-50 Hz				
Consommation max.	81 W	90 W			150 W
Dissipation thermique totale	276 BTU	307 BTU			511,5 BTU
MTBF	11,9	11,9			12,4
Certifications	EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2		ICSA Firewall 4.1		—
Certifications (en instance)	—		EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1 et 2		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1 et 2
Facteur de forme	1U rackable				
Dimensions	43,2 x 42,5 x 4,4 cm/17 x 16,8 x 1,8 in				
Poids	6,80 kg/15,00 lbs	6,85 kg/15,10 lbs			7,9 kg/17,30 lbs
Poids DEEE	6,80 kg/15,00 lbs	6,85 kg/15,10 lbs			7,9 kg/17,30 lbs
Conformité aux normes suivantes	FCC class A, CE class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, DEEE				
Environnement	5-40 °C, 40-105 °F				
Humidité	10-90 % non condensée				

¹Méthodes 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. ²Débit Full DPI/ 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. ³Le nombre maximal effectif de connexions est inférieur quand les services UTM sont activés. ⁴Débit VPN basé sur le trafic UDP par paquets de 1280 octets selon RFC 2544. ⁵Carte USB 3G et modem non fournis. Pour savoir quels appareils USB sont pris en charge, consultez <http://www.sonicwall.com/us/products/cardsupport.html>. ⁶Comprehensive Anti-Spam Service prend en charge un nombre illimité d'utilisateurs, mais est recommandé pour 250 utilisateurs ou moins. ⁷Avec les appliances SonicWALL série WXA.

La gamme SonicWALL de solutions de sécurité dynamique



SonicWALL France

T +33 1 49 33 73 19 France@sonicwall.com

SonicWALL BeNeLux

T +32 (0) 15 280 985 Belux@sonicwall.com

Contacts du support SonicWALL

www.sonicwall.com/emea/4724.html



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™