



# Gammes de produits Dell SonicWALL



## Table des matières

<b>Présentation</b>	4
<b>Solutions de sécurité réseau/pare-feu</b>	
Les solutions de sécurité réseau en bref	6
Solutions SuperMassive	7
Accessoires pour solutions sans fil	14
Services d'abonnement, licences et firmware	17
<b>Solutions d'accélération WAN</b>	
Solutions d'accélération WAN	19
<b>Solutions d'accès distant sécurisé</b>	
Les solutions d'accès distant sécurisé en bref	21
Solutions E-Class	21
Caractéristiques complémentaires	22
Solutions pour PME et agences	24
Caractéristiques complémentaires	26
<b>Solutions anti-spam/de sécurisation de messagerie</b>	
Les solutions de sécurisation de messagerie en bref	28
Solutions de sécurisation de messagerie	28
Services d'abonnement	30
<b>Solutions de reporting et de gestion des règles</b>	
Global Management System	31
Scrutinizer	31
Analyzer	31
<b>Services de support global</b>	
Support Platinum pour la série SuperMassive E10000	32
Support Gold	32
Support Silver	32
Support E-Class	33
Support dynamique	33
Support Comprehensive Global Management System	33
Assistance technique spécifique	33
Service de démarrage et de configuration à distance	33

## Présentation

### Gestion des menaces

Si elles ne représentaient autrefois qu'un simple désagrément, les menaces Internet sont aujourd'hui plus que jamais malveillantes et sophistiquées et peuvent avoir un impact considérable sur l'entreprise. Les solutions Dell™ SonicWALL™ offrent une protection intelligente contre ces menaces complexes en permanente mutation grâce à un éventail complet de fonctionnalités de sécurité réseau et de sécurisation Web et de messagerie. En matière de sécurité réseau, Dell SonicWALL offre une protection approfondie contre les virus, vers, chevaux de Troie, logiciels espions et intrusions tout en assurant des performances haut de gamme, quelle que soit la charge du réseau. La sécurisation Web de Dell SonicWALL permet de bloquer les sites Web indésirables, voire illégaux, et de contrôler l'utilisation d'applications de messagerie instantanée et poste à poste. Le contrôle de Dell SonicWALL Application Intelligence, Control and Visualization s'étend aux applications non productives comme la bourse en ligne, les chats et messageries instantanées, le partage poste à poste et les sites de streaming vidéo. Enfin, les solutions de sécurisation de messagerie Dell SonicWALL assurent une protection efficace contre les spams et les attaques de phishing pour que les employés ne lisent que des messages authentiques sans être exposés aux e-mails frauduleux. Les solutions intelligentes Dell SonicWALL simplifient considérablement la gestion centralisée des services réseau sur place, à distance ou sans fil, tout en protégeant de manière économique les ressources de communication et les informations vitales.

### Mobilité

Face à une technologie sans fil omniprésente, des employés de plus en plus dispersés, la multiplication des accès par smartphones et tablettes au réseau des entreprises et des exigences élevées en matière de continuité des activités, la mobilité est devenue un impératif commercial. Pour y répondre, Dell SonicWALL fournit aux entreprises de toutes tailles des solutions intelligentes par connexions haut débit et mobiles. Les solutions de sécurité réseau Dell SonicWALL, qui intègrent toutes la protection des pare-feu nouvelle génération de Dell SonicWALL, garantissent des connexions site à site ou d'accès distant sécurisées par VPN IPSec ou VPN SSL. Associées aux SonicPoint à configuration automatique, ces appliances permettent de créer instantanément des réseaux provisoires au moyen de points d'accès sans fil sécurisés. Les pare-feu Dell SonicWALL permettent de disposer en un rien de temps d'une connectivité réseau haut débit sans fil 4G/3G sécurisée, de quasi n'importe où, même sans liaison fixe à Internet. De plus, les VPN SSL spécialisés de Dell SonicWALL étendent l'accès mobile sécurisé à pratiquement tout emplacement distant via des navigateurs Web standard ou des terminaux sans fil de type smartphones et tablettes. Les solutions VPN SSL Dell SonicWALL offrent en outre un niveau de contrôle inégalé des accès.

### Contrôle applicatif

Dell 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. Étroitement intégrée aux pare-feu nouvelle génération Dell SonicWALL, cette fonctionnalité s'appuie sur la technologie RFDPI (Reassembly-Free Deep Packet Inspection®) de Dell SonicWALL pour identifier et contrôler les applications, quels que soient le port ou le protocole. Grâce à une bibliothèque de signatures constamment enrichie et capable de reconnaître actuellement plus de 4 600 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'Application Flow Monitor de Dell 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.

## Conformité

Les menaces existent aussi à l'intérieur du réseau. Que ce soit intentionnellement ou par accident, les employés peuvent transmettre des contenus indésirables, des documents relevant de la propriété intellectuelle ou des données confidentielles, entraînant des dommages significatifs, voire une violation des réglementations industrielles ou gouvernementales telles que les lois Sarbanes-Oxley et HIPAA. La non-conformité peut se traduire par des amendes, l'engagement de la responsabilité de l'entreprise et une perte dommageable de crédibilité. Pour aider les entreprises à se conformer aux obligations réglementaires, Dell SonicWALL propose une technologie de chiffrement leader et un service de filtrage applicatif garants de connexions VPN « propres ». Les solutions VPN SSL de Dell SonicWALL offrent le chiffrement et l'authentification des données, un contrôle d'accès granulaire, la gestion des règles, une fonctionnalité de journalisation et une architecture d'authentification flexible. Dell SonicWALL Email Security simplifie la création de règles pour le courrier sortant, identifie intelligemment les e-mails non conformes et fournit des outils puissants de surveillance et de reporting ainsi qu'une gamme complète d'options de correction. Dell SonicWALL Content Filtering Service, pour sa part, protège votre réseau des contenus illicites ou non productifs. Enfin, le Système de Gestion globale primé de Dell SonicWALL (GMS®) fournit des pistes d'audit avec surveillance centralisée en temps réel, ainsi qu'un ensemble d'options de reporting des règles et de la conformité.

## Continuité des activités

Qu'elle soit causée par une catastrophe naturelle, une vague de grippe ou une coupure de courant localisée, toute interruption des activités normales de l'entreprise peut vous faire perdre des opportunités, de l'argent et même votre réputation. Dell SonicWALL propose des solutions de continuité des activités et de récupération aux entreprises de toutes tailles. Grâce aux VPN SSL Dell SonicWALL, les employés isolés sont aussi productifs de chez eux ou de tout autre lieu occasionnel que s'ils étaient au bureau.

## Analyse du trafic applicatif

Les solutions d'analyse du trafic applicatif Dell SonicWALL livrent des informations précieuses sur la consommation de bande passante, le trafic applicatif et les atteintes à la sécurité, tout en fournissant des services performants de dépannage et d'analyse forensique. Les outils Dell SonicWALL Global Management System et Analyzer exploitent les données d'analyse du trafic applicatif fournies par les pare-feu Dell SonicWALL pour donner un aperçu parlant du réseau. Dell SonicWALL Scrutinizer assure la compatibilité avec les routeurs et commutateurs de fournisseurs tiers.

## Pare-feu/sécurité réseau Dell SonicWALL

Dell SonicWALL fait partie des plus grands fournisseurs de pare-feu nouvelle génération. Déployés comme solution nouvelle génération, les pare-feu Dell SonicWALL intègrent étroitement le filtrage RFDPI fournissant les services haut de gamme de prévention des intrusions, de protection anti-malware, d'intelligence, de contrôle et de visualisation en temps réel au niveau applicatif, ainsi que de filtrage des sessions chiffrées en SSL. Essentiels dans un système de sécurité intelligent et hautement flexible, les pare-feu nouvelle génération de Dell SonicWALL analysent chaque octet de chaque paquet, garantissant ainsi le niveau de protection le plus approfondi. Contrairement aux produits concurrents, le moteur RFDPI « single-pass » assure un filtrage simultané des diverses menaces et des applications ainsi que l'analyse de fichiers de taille illimitée et de connexions, sans réassemblage des paquets. Cela permet aux pare-feu Dell SonicWALL d'être extrêmement évolutifs et aux réseaux d'entreprises de bénéficier d'une sécurité de pointe tout au long de leur croissance. Les appliances de sécurité réseau Dell SonicWALL peuvent également être déployées en tant que pare-feu UTM (Unified Threat Management) pour fournir une sécurité de bout en bout associant les services de filtrage de contenu, d'anti-spam, d'antivirus, d'anti-spyware et de prévention des intrusions au niveau de la passerelle, ainsi que d'intelligence et de contrôle applicatifs.

La technologie RFDPI (Reassembly-Free Deep Packet Inspection) de Dell SonicWALL permet un filtrage simultané des diverses menaces et des applications ainsi que l'analyse de fichiers de taille illimitée et de connexions à des vitesses extrêmement élevées. Allant bien plus loin que le simple filtrage dynamique des paquets, le moteur RFDPI analyse différents types d'applications et de protocoles, garantissant la protection du réseau face aux menaces internes et externes. Cette base de code unique est au cœur de chaque pare-feu Dell SonicWALL, du TZ 105 aux appliances des séries SuperMassive E10000 et 9000. L'appliance SuperMassive E10800 avec SonicOS a obtenu la mention « Recommandé » de NSS Labs pour la deuxième année consécutive. Étroitement intégrée à la plate-forme des pare-feu, la technologie RFDPI optimise la gestion de règles granulaires, directement sur l'interface des pare-feu ou via Dell SonicWALL GMS (Global Management System). Les entreprises ont le choix parmi une gamme complète de pare-feu Dell SonicWALL éprouvés conçus pour s'adapter aux besoins des réseaux les plus performants. De plus, s'appuyant sur le réseau mondial, unique en son genre, d'identification et de surveillance des attaques appelé Dell SonicWALL Global Response Intelligent Defense (GRID), les pare-feu Dell SonicWALL sont à même d'offrir un excellent niveau de sécurité aujourd'hui, tout en étant prêt à stopper les nouvelles attaques de demain.

Sécurité approfondie, hautes performances et faible latence : des pare-feu nouvelle génération pour les centres de données et grands comptes



## La série SuperMassive de Dell SonicWALL en un coup d'œil

La série SuperMassive (E10000 et 9000) constitue la plate-forme de pare-feu nouvelle génération Dell SonicWALL conçus pour fournir aux vastes réseaux une évolutivité, une fiabilité et une sécurité maximum à des débits multi-gigabits. Développée pour répondre aux besoins des grands comptes, des services publics, des universités et des fournisseurs de services, la série SuperMassive est idéale pour sécuriser les réseaux d'entreprises, les centres de données et les fournisseurs de services. Une conception multiprocesseur extrêmement évolutive associée à la technologie RFDPI brevetée\* permet à la série SuperMassive d'opérer les services leaders de contrôle applicatif, de prévention des intrusions, de protection anti-malware et de filtrage SSL.

	SuperMassive E10800	SuperMassive E10400	SuperMassive E10200
Cœurs de processeurs	96	48	24
Débit IPS	30 Gbit/s	15 Gbit/s	7,5 Gbit/s
Débit de pare-feu	40 Gbit/s	20 Gbit/s	10 Gbit/s
Débit de filtrage applicatif	30 Gbit/s	15 Gbit/s	7,5 Gbit/s
Débit prévention des menaces	12 Gbit/s	6,0 Gbit/s	3,0 Gbit/s
Nb max. de connexions	12,0 M	6,0 M	3,0 M
Possibilités de mise à niveau	—	vers E10800	vers E10400, E10800

	SuperMassive 9600	SuperMassive 9400	SuperMassive 9200
Cœurs de processeurs	32		24
Débit IPS	12 Gbit/s	10 Gbit/s	7,5 Gbit/s
Débit de pare-feu	20 Gbit/s	20 Gbit/s	15 Gbit/s
Débit de filtrage applicatif	12 Gbit/s	10 Gbit/s	7,5 Gbit/s
Débit prévention des menaces	5 Gbit/s	4,5 Gbit/s	3,5 Gbit/s
Nb max. de connexions	1,5 M	1,25 M	

\* Brevets U.S. n° 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723

## Série SuperMassive E10000

	E10200	E10400	E10800
Système d'exploitation	SonicOS		
Cœurs de processeurs	24	48	96
Interfaces 10 GbE	6 x SFP+ 10 GbE		
Interfaces 1 GbE	16 x SFP 1 GbE		
Interfaces de gestion	1 GbE, 1 console		
Mémoire vive	16 Go	32 Go	64 Go
Stockage	SSD 80 Go, Flash		
Débit de filtrage pare-feu	10 Gbit/s	20 Gbit/s	40 Gbit/s
Débit de filtrage applicatif	7,5 Gbit/s	15 Gbit/s	30 Gbit/s
Débit IPS	7,5 Gbit/s	15 Gbit/s	30 Gbit/s
Débit de filtrage anti-malware	3,0 Gbit/s	6,0 Gbit/s	12 Gbit/s
Débit VPN	5,0 Gbit/s	10 Gbit/s	20 Gbit/s
Connexions/s	160 000/s	320 000/s	640 000/s
Nb max. de connexions (SPI)	3,0 M	6,0 M	12,0 M
Nb max. de connexions (DPI)	2,5 M	5,0 M	10,0 M
<b>VPN</b>	<b>E10200</b>	<b>E10400</b>	<b>E10800</b>
Tunnels site à site	10 000		
Clients VPN IPsec	2 000		
Licences VPN SSL	50		
Chiffrement	DES, 3DES, AES (128, 192, 256 bits)		
Authentification	MD5, SHA-1		
Echange de clés	Diffie Hellman Groups 1, 2, 5, 14		
VPN à base de routes	RIP, OSPF		
<b>Mise en réseau</b>	<b>E10200</b>	<b>E10400</b>	<b>E10800</b>
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		
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage à base de règles, multidiffusion		
QoS	Priorité, bande passante max., garantie, marquage DSCP, 802.1p		
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix		
VoIP	H323-v1-5 intégral, SIP		
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Certifications (en instance)	FIPS 140-2, Critères Communs EAL4+, NEBS, ICSA Firewall		
Certifications	Pare-feu nouvelle génération recommandé par NSS et IPS recommandé par NSS		
Prise en charge de la carte CAC (Common Access Card)	En instance		
<b>Matériel</b>	<b>E10200</b>	<b>E10400</b>	<b>E10800</b>
Alimentation	Double, redondante, remplaçable à chaud, 850 W		
Ventilateurs	Doubles, redondants, remplaçables à chaud		
Affichage	Ecran frontal LED		
Alimentation d'entrée	100-240 VCA, 60-50 Hz		
Consommation max. (W)	400	550	750
Facteur de forme	4U rackable		
Dimensions	43x43,5x17,8 cm (17x18x7 in)		
Poids	26,3 kg (58 lb)	27,7 kg (61 lb)	30,3 kg (67 lb)
Poids DEEE	26,8 kg (59 lb)	28,1 kg (62 lb)	30,8 kg (68 lb)
Poids de transport	35,8 kg (79 lb)	37,2 kg (82 lb)	39,9 kg (88 lb)
Conformité aux normes suivantes	FCC classe A, CE, C-Tick, VCCI, MIC, UL, cUL, TÜV/GS, CB, RoHS, DEEE		
Environnement	5-40 °C, 40-105 °F		
Humidité	10-90 % non condensée		

Sous réserve de modification des spécifications, des fonctionnalités et de la disponibilité.



## Série SuperMassive 9000

	9200	9400	9600
Système d'exploitation	SonicOS		
Cœurs de processeurs	24	32	
Interfaces 10 GbE	4 x SFP+ 10 GbE		
Interfaces 1 GbE	8 x SFP 1 GbE, 8 x 1 GbE (1 paire LAN Bypass)		
Interfaces de gestion	1 GbE, 1 console		
Mémoire vive	8 Go	16 Go	32 Go
Extension	1 emplacement (dos)*, carte SD*		
Débit de filtrage pare-feu	15 Gbit/s	20 Gbit/s	
Débit de filtrage applicatif	7,5 Gbit/s	10 Gbit/s	12 Gbit/s
Débit IPS	7,5 Gbit/s	10 Gbit/s	12 Gbit/s
Débit de filtrage anti-malware	3,5 Gbit/s	4,5 Gbit/s	5 Gbit/s
Performances IMIX (Gbit/s)	4,0 Gbit/s	6,2 Gbit/s	
Débit VPN	5,0 Gbit/s	10 Gbit/s	12 Gbit/s
Connexions/s	110 000/s	150 000/s	
Nb max. de connexions (SPI)	1,25 M		1,5 M
Nb max. de connexions (DPI)	1,0 M		1,25 M
SonicPoint pris en charge (max.)	96	128	
<b>VPN</b>	<b>9200</b>	<b>9400</b>	<b>9600</b>
Tunnels site à site	6 000	10 000	
Clients VPN IPSec (max.)	2 000 (4 000)	2 000 (6 000)	2 000 (10 000)
Licences VPN SSL (max.)	2 (50)		50 (50)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1		
Echange de clés	Diffie Hellman Groups 1, 2, 5, 14		
VPN à base de routes	RIP, OSPF		
<b>Mise en réseau</b>	<b>9200</b>	<b>9400</b>	<b>9600</b>
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		
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage à base de règles, multidiffusion		
QoS	Priorité, bande passante max., garantie, marquage DSCP, 802.1p		
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix		
VoIP	H323-v1-5 intégral, SIP		
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Certifications (en instance)	FIPS 140-2, Critères Communs EAL4+, NEBS, ICSA Firewall		
Carte CAC (Common Access Card)	En instance		
<b>Matériel</b>	<b>9200</b>	<b>9400</b>	<b>9600</b>
Alimentation	Double, redondante, remplaçable à chaud, 300 W		
Ventilateurs	Doubles, redondants, remplaçables à chaud		
Affichage	Ecran frontal LED		
Alimentation d'entrée	100-240 VCA, 60-50 Hz		
Consommation max. (W)	300		
Facteur de forme	1U rackable		
Dimensions	43,3x48,5x4,5 cm (17x19,1x1,75 in)		
Poids	8,2 kg (18,1 lb)		
Poids DEEE	10,4 kg (23 lb)		
Poids de transport	13,3 kg (29,3 lb)		
Conformité aux normes suivantes	FCC classe A, CE, C-Tick, VCCI, KCC, UL, cUL, TÜV/GS, CB, RoHS, DEEE, ANATEL, BSMI		
Environnement	0-40 °C, 32-105 °F		
Humidité	10-90 % non condensée		

\* Utilisation future. Sous réserve de modification des spécifications, des fonctionnalités et de la disponibilité.

## La série NSA de Dell SonicWALL en un coup d'œil

La série d'appiances de sécurité réseau (NSA) de Dell™ SonicWALL™ est l'une des plus sécurisées et des plus performantes gammes de pare-feu nouvelle génération. Gage d'une sécurité haut de gamme et de performances sans compromis, elle repose sur la même architecture que les pare-feu nouvelle génération de la série phare SuperMassive, conçue à l'origine pour les réseaux d'opérateurs et de grands comptes les plus exigeants. Mais elle n'en perd pas pour autant la convivialité et le bon rapport qualité/prix caractéristiques de Dell SonicWALL. Fruit de plusieurs années de recherche et de développement, la série NSA a été conçue dès le départ pour les entreprises distribuées, les petites et moyennes structures, les agences, les établissements scolaires et les organismes publics. La série NSA allie une architecture multiprocesseur révolutionnaire au moteur « single-pass » de prévention des menaces breveté\* RFDPI (Reassembly-Free Deep Packet Inspection®) dans une conception extrêmement évolutive. Cette association garantit une protection, des performances et une évolutivité haut de gamme, avec un maximum de connexions simultanées, une latence minimum, pas de limite dans la taille des fichiers et un nombre de connexions par seconde parmi les meilleurs de sa catégorie. Des entreprises de test indépendantes très réputées ont évalué et/ou certifié la technologie pour la fiabilité et la garantie offertes.



### Appiance de sécurité réseau NSA 6600 Dell SonicWALL

Le pare-feu nouvelle génération NSA 6600 de Dell SonicWALL est idéal pour les sièges d'entreprises et grands réseaux distribués nécessitant une protection et des performances élevées.



### Appiance de sécurité réseau NSA 5600 Dell SonicWALL

Le pare-feu nouvelle génération NSA 5600 de Dell SonicWALL est idéal pour les environnements d'entreprises, d'agences ou distribués aux besoins importants en matière de protection et de performance.



### Appiance de sécurité réseau NSA 4600 Dell SonicWALL

Le pare-feu nouvelle génération NSA 4600 de Dell SonicWALL convient idéalement aux environnements de PME et d'agences soucieuses d'optimiser leurs performances et leur débit en matière de protection du réseau.



### Appiance de sécurité réseau NSA 3600 Dell SonicWALL

Le pare-feu nouvelle génération NSA 3600 de Dell SonicWALL est idéal pour les sites d'agences dans les entreprises distribuées, les PME et environnements de vente.



### Appiance de sécurité réseau NSA 2600 Dell SonicWALL

Le pare-feu nouvelle génération NSA 2600 de Dell SonicWALL est conçu pour répondre aux besoins des petites entreprises en développement, agences et établissements scolaires.

\* Brevets U.S. n° 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723



#### **Appliances de sécurité réseau série 250M Dell SonicWALL**

Les pare-feu nouvelle génération de la série NSA 250M de Dell SonicWALL offrent aux agences et petites et moyennes entreprises une sécurité approfondie, doublée, en option, d'une connectivité sans fil bande 802.11n. La NSA 250M peut être étendue par tout un éventail de modules, notamment T1/E1, DSL et SFP, pour bénéficier d'une plus grande flexibilité de déploiement et de fonctionnalités de basculement supplémentaires ainsi que pour réduire les coûts d'achat et de maintenance.



#### **Appliances de sécurité réseau série 220 Dell SonicWALL**

Les pare-feu nouvelle génération série NSA 220 de Dell SonicWALL offrent aux agences et petites et moyennes entreprises une sécurité approfondie facile à gérer, doublée, en option, d'une connectivité sans fil bande 802.11.

## Série NSA

Caractéristique	NSA 220/W-N	NSA 250M/W-N	NSA 2400
Version SonicOS prise en charge	SonicOS 5.8.1.1		SonicOS Enhanced 5.6 (ou supérieure)
Nb d'utilisateurs et de nœuds	Illimité		
Interfaces réseau	7 ports Gigabit 10/100/1000, 2 USB, 1 interface console	5 ports Gigabit 10/100/1000, 2 USB, 1 interface console, emplacement pour module	6 ports cuivre Gigabit 10/100/1000, 1 interface console, 2 USB (utilisation future)
Alimentation électrique	Externe 36 W		1 ATX 180 W
Système de refroidissement (ventilateurs)	Pas de ventilateur/1 ventilateur	2 ventilateurs	
Interfaces VLAN	25	35	25
Haute disponibilité	Active/passive avec synchronisation d'état en option		
Débit dynamique <sup>1</sup>	600 MBit/s	750 MBit/s	775 MBit/s
Débit 3DES/AES <sup>2</sup>	150 MBit/s	200 MBit/s	300 MBit/s
Débit antivirus passerelle <sup>3</sup>	115 MBit/s	140 MBit/s	160 MBit/s
Débit prévention des intrusions <sup>3</sup>	195 MBit/s	250 MBit/s	275 MBit/s
Performances Full DPI <sup>3</sup>	110 MBit/s	130 MBit/s	150 MBit/s
Performances IMIX <sup>3</sup>	180 MBit/s	210 MBit/s	235 MBit/s
Nouvelles connexions/s	2 200	3 000	4 000
Nb max. de connexions	85 000	110 000	225 000
Connexions DPI (max.)	32 000	64 000	125 000
VPN site à site	25	50	75
Sécurité par zones	Oui		
Gestion orientée objet	Oui		
NAT à base de règles	Oui		
Basculement multi-FAI	Oui		
Équilibrage de charge	Oui		
Commutateur et contrôleur sans fil intégré	Oui		
Basculement sans fil 3G	Oui		—
Routage à base de règles	Oui		
Comprehensive Anti-Spam Service	En option		
Voix sur IP (VoIP)	Oui		
VPN IKEv2	Oui		
Télégestion sécurisée (prise en charge SSHv2)	Oui		
Clients d'accès distant VPN SSL et VPN IPSec	Oui		
Techniciens Secure Virtual Assist	Essai de 30 jours		Oui
VPN à base de routes	Oui		
Authentification util. TSA	Oui		
Objets d'adresse dynamiqués	Oui		
Mode pont couche 2	Oui		
Pont sans fil couche 2	Oui		
Commutateur et contrôleur sans fil	Oui		
VLAN 802.1q	Oui		
Routage RIPv2 et OSPF	Oui		
Signature unique (SSO)	Oui		
Intelligence et contrôle applicatifs	En option		
Filtrage applicatif SSL	En option		
Contrôle SSL	Oui		
IPv6 <sup>4</sup>	Non		Oui
Visualisation applicative	Oui		
NetFlow/IPFIX	Oui		

<sup>1</sup> 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. <sup>2</sup> Débit VPN basé sur le trafic UDP par paquets de 1280 octets selon RFC 2544. <sup>3</sup> Débit Full DPI/Gateway AV/Anti-Spyware/IPS basé sur le test de performances HTTP standard Spirent WebAvalanche et les outils de test Ixia. Tests effectués avec différents flux, via plusieurs paires de ports.

<sup>4</sup> La fonctionnalité IPv6 requiert un firmware séparé. \* Avec Stateful HA et Expansion Upgrade.

## Série NSA

Caractéristique	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Version SonicOS prise en charge	SonicOS 6.1.2	SonicOS 6.1.1			
Nb d'utilisateurs et de nœuds	Illimité				
Interfaces réseau	8 x 1 GbE	2 SFP+ 10 GbE, 4 SFP 1 GbE, 12 ports cuivre Gigabit 10/100/1000, 1 interface console, 2 USB			4 SFP+ 10 GbE, 8 SFP 1 GbE, 8 ports cuivre Gigabit 10/100/1000, 1 interface console, 2 USB
Alimentation électrique	Simple, fixe 200 W		Simple, fixe 250 W		
Système de refroidissement (ventilateurs)	2 ventilateurs				
Interfaces VLAN	50		200	400	500
Haute disponibilité	Active/passive avec synchronisation d'état en option*		Active/passive avec synchronisation d'état en option		
Débit dynamique <sup>1</sup>	1,9 Gbit/s	3,4 Gbit/s	6,0 Gbit/s	9,0 Gbit/s	12,0 Gbit/s
Débit 3DES/AES <sup>2</sup>	1,1 Gbit/s	1,5 Gbit/s	3,0 Gbit/s	4,5 Gbit/s	5,0 Gbit/s
Débit antivirus passerelle <sup>3</sup>	300 MBit/s	600 MBit/s	1,1 Gbit/s	1,7 Gbit/s	3,0 Gbit/s
Débit prévention des intrusions <sup>3</sup>	700 MBit/s	1,1 Gbit/s	2,0 Gbit/s	3,0 Gbit/s	4,5 Gbit/s
Performances Full DPI <sup>3</sup>	300 MBit/s	500 MBit/s	800 MBit/s	1,6 Gbit/s	3,0 Gbit/s
Performances IMIX <sup>3</sup>	600 MBit/s	900 MBit/s	1,6 Gbit/s	2,4 Gbit/s	3,5 Gbit/s
Nouvelles connexions/s	15 000	20 000	40 000	60 000	90 000
Nb max. de connexions	225 000	325 000	400 000	750 000	
Connexions DPI (max.)	125 000	175 000	200 000	500 000	
VPN site à site	75	800	1 500	5 000	6 000
Sécurité par zones	Oui				
Gestion orientée objet	Oui				
NAT à base de règles	Oui				
Basculement multi-FAI	Oui				
Équilibrage de charge	Oui				
Commutateur et contrôleur sans fil intégré	Oui				
Basculement sans fil 3G	—	Oui		—	Oui
Routage à base de règles	Oui				
Comprehensive Anti-Spam Service	En option				
Voix sur IP (VoIP)	Oui				
VPN IKEv2	Oui				
Télégestion sécurisée (prise en charge SSHv2)	Oui				
Clients d'accès distant VPN SSL et VPN IPSec	Oui				
Techniciens Secure Virtual Assist	Oui				
VPN à base de routes	Oui				
Authentification util. TSA	Oui				
Objets d'adresse dynamiques	Oui				
Mode pont couche 2	Oui				
Pont sans fil couche 2	Oui			Non	
Commutateur et contrôleur sans fil	Oui			Non	
VLAN 802.1q	Oui				
Routage RIPv2 et OSPF	Oui				
Signature unique (SSO)	Oui				
Intelligence et contrôle applicatifs	En option				
Filtrage applicatif SSL	En option				
Contrôle SSL	Oui				
IPv6 <sup>4</sup>	Version future				
Visualisation applicative	Oui				
NetFlow/IPFIX	Oui				
Agrégation de liens	Oui <sup>5</sup>				
Redondance de ports	Yes				

<sup>1</sup> 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. <sup>2</sup> Débit VPN basé sur le trafic UDP par paquets de 1280 octets selon RFC 2544. <sup>3</sup> Débit Full DPI/Gateway AV/Anti-Spyware/IPS basé sur le test de performances HTTP standard Spirent WebAvalanche et les outils de test Ixia. Tests effectués avec différents flux, via plusieurs paires de ports. <sup>4</sup> La fonctionnalité IPv6 requiert un firmware séparé. <sup>5</sup> Agrégation de liens statique. \* Avec Stateful HA et Expansion Upgrade.

La série TZ offre la plate-forme de sécurité idéale pour les PME et les déploiements de points de vente.

## Solutions Dell SonicWALL pour PME : la série TZ en un coup d'œil

La série TZ de Dell SonicWALL compte parmi les pare-feu UTM (Unified Threat Management) les plus sécurisés à l'attention des petites entreprises, points de vente, services publics, sites distants et agences. A la différence des produits grand public, la série TZ assure des services extrêmement efficaces de protection anti-malware, de prévention des intrusions, de filtrage de contenu/URL et de contrôle applicatif, ainsi qu'une prise en charge étendue de plates-formes mobiles pour les ordinateurs portables, smartphones et tablettes. Garante d'un filtrage applicatif exhaustif à très hautes performances, elle ne crée aucun encombrement sur le réseau, optimisant par là même la productivité des entreprises. La série TZ est actuellement l'une des plates-formes de sécurité les plus fiables, les plus sophistiquées et les plus déployées du marché.

De plus, la fonctionnalité Application Intelligence and Control de Dell SonicWALL sur le TZ 215 garantit la disponibilité de la bande passante pour les applications vitales, tout en restreignant ou bloquant les applications qui freinent la productivité. Le TZ 215 permet également une analyse avancée du trafic applicatif et l'établissement de rapports fournissant des informations précises sur la consommation de la bande passante et sur les atteintes à la sécurité.

La série TZ inclut des fonctionnalités évoluées de mise en réseau : VPN IPSec et VPN SSL, basculement multi-FAI, équilibrage de charge, sans-fil 802.11n intégré en option et segmentation du réseau, ainsi que la conformité PCI. A la différence d'autres pare-feu UTM, la série TZ fournit un client natif d'accès distant VPN pour iOS, Android, Windows, Windows 8.1/RT, Mac OS et Linux. Unique en son genre, ce client prend également en charge la fonctionnalité Clean VPN™ conçue pour décontaminer le trafic VPN de toute menace. La nouvelle série TZ associe avec élégance et simplicité divers produits individuels au sein d'une même solution, ce qui à la fois crée de la valeur et réduit la complexité.



### Série TZ 215 Dell SonicWALL

Le TZ 215 de Dell SonicWALL est le pare-feu UTM (Unified Threat Management) le plus sécurisé et le plus performant à la disposition des petites entreprises et agences. Conçu pour les petites structures, les entreprises distribuées, les agences et les points de vente, le TZ 215 intègre les services d'anti-malware, de prévention des intrusions, de contrôle applicatif et de filtrage d'URL en une solution simple et économique. Le contrôle applicatif du TZ 215 permet en outre de garantir la disponibilité de la bande passante pour les applications vitales, tout en freinant les applications non productives.



### Série TZ 205 Dell SonicWALL

Petites entreprises, points de vente, services publics, sites distants et agences peuvent profiter des puissantes fonctionnalités de sécurité et des performances haut de gamme du TZ 205 de Dell SonicWALL. A la différence des produits grand public, ce puissant pare-feu UTM (Unified Threat Management) allie les services les plus efficaces de prévention des intrusions, d'anti-malware et de filtrage de contenu/URL à la prise en charge la plus étendue et la plus sûre de plates-formes mobiles pour les ordinateurs portables, smartphones et tablettes.



### Série TZ 105 Dell SonicWALL

Le TZ 105 de Dell SonicWALL assure des services éprouvés de prévention des intrusions, de protection anti-malware et de filtrage de contenu/URL, ainsi qu'une prise en charge étendue de plates-formes mobiles pour les ordinateurs portables, smartphones et tablettes. Il assure un filtrage applicatif exhaustif à très hautes performances, éliminant tout encombrement sur le réseau et optimisant par là même la productivité des entreprises sans augmenter les coûts.

Caractéristique	Série TZ 105	Série TZ 205	Série TZ 215
Nb de nœuds	Illimité		
Interfaces réseau	5 10/100 Fast Ethernet, 1 USB, 1 console	5 Gigabit cuivre 10/100/1000, 1 USB, 1 console	7 Gigabit cuivre 10/100/1000, 2 USB, 1 console
Débit de filtrage dynamique de paquets <sup>1</sup>	200 Mbit/s	500 Mbit/s	
Débit UTM <sup>3</sup>	25 Mbit/s	40 Mbit/s	60 Mbit/s
Débit 3DES/AES <sup>2</sup>	75 Mbit/s	100 Mbit/s	130 Mbit/s
Nb max. de connexions	8 000	12 000	48 000
Connexions UTM (max.)	8 000	12 000	32 000
Tunnels VPN site à site	5	10	20
Tunnels VPN IPSec d'accès distant (max.)	5	10	25
Tunnels VPN IPSec d'accès distant (inclus)	Mise à niveau optionnelle	2	
Tunnels VPN SSL d'accès distant (max.)	5	10	
Tunnels VPN SSL d'accès distant (inclus)		1	2
Techniciens Secure Virtual Assist (max.)	N/A	1	2
Techniciens Secure Virtual Assist (inclus)	N/A	0	Essai de 30 jours
Interfaces VLAN	5, PortShield	10, PortShield	20, PortShield
Sécurité par zones	Oui		
Gestion orientée objet	Oui		
NAT à base de règles	Oui		
Basculement multi-FAI	Oui		
Basculement FAI	Oui		
Basculement matériel	Non	Actif/passif	
Équilibrage de charge WAN	Oui		
Pont sans fil couche 2	Oui		
Commutateur et contrôleur sans fil	Oui		
Points d'accès virtuels (VAP)	Oui <sup>4</sup>		
Point d'accès intégré	802.11n en option		
Comprehensive Anti-Spam Service	En option		
Dual band wireless-N	Oui	Oui (2x2)	Oui (3x3)
Voix sur IP (VoIP)	Oui		
Sécurité PortShield	Oui		
VPN à base de routes	Oui		
Basculement sans fil 3G	Oui		
Gestion de la bande passante	Non	Oui	
Intelligence et contrôle applicatifs	Non	Oui	
Visualisation applicative	Non	Oui	
NetFlow/IPFIX	Non	Oui <sup>5</sup>	Oui

<sup>1</sup> 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. <sup>2</sup> Débit VPN basé sur le trafic UDP par paquets de 1280 octets selon RFC 2544. <sup>3</sup> Débit UTM/Gateway AV/Anti-Spyware/IPS basé sur le test de performances HTTP standard Spirent WebAvalanche et les outils de test Ixia. Tests effectués avec différents flux, via plusieurs paires de ports. <sup>4</sup> Points d'accès virtuels (VAP) pris en charge uniquement sur la radio sans fil intégrée. <sup>5</sup> Pour connaître la disponibilité de cette fonctionnalité, veuillez consulter les dernières notes de mise à jour.

## Solution Clean Wireless de Dell SonicWALL : les points d'accès SonicPoint en un coup d'œil

Soucieux de rendre le sans-fil simple, sûr et abordable, Dell SonicWALL présente sa solution novatrice Clean Wireless, la première solution de sécurité totale à intégrer la gestion sans fil 802.11n et 802.11a/b/g doublée de la sécurité d'un pare-feu nouvelle génération haut de gamme et des services d'intelligence, de contrôle et de visualisation applicatifs pour un contrôle des applications sur la base de règles. La solution Clean Wireless de Dell SonicWALL va au-delà des solutions sans fil sécurisées de base grâce au filtrage applicatif et à la double protection du réseau sans fil : le trafic véhiculé sans fil est chiffré et décontaminé des menaces réseau, tandis que les attaques sans fil sont éliminées. Dell SonicWALL réduit le coût total de possession (TCO) dans la mesure où les administrateurs n'ont pas à installer ni à gérer séparément une solution sans fil spéciale coûteuse parallèlement au réseau câblé.



### Dell SonicPoint-N Dual-Radio

Les SonicPoint-N Dual-Radio de Dell SonicWALL assurent une mise en réseau sans fil sécurisée 802.11a/g/b/n sur les bandes de 2,4 GHz et de 5 GHz grâce à leurs deux radios distinctes. La technologie Clean Wireless de Dell SonicWALL avec les SonicPoint allie la gestion des points d'accès à la sécurité fournie par le moteur RFDPI\* breveté Dell SonicWALL du pare-feu pour éliminer les menaces sur le trafic sans fil. Les SonicPoint-N Dual-Radio fournissent un débit combiné allant jusqu'à 600 Mbit/s, pour une sécurité et une productivité optimisées.



### SonicPoint-Ne Dual-Band

Les points d'accès SonicPoint-Ne Dual-Band de Dell SonicWALL intègrent les fonctionnalités de gestion et d'exécution 802.11a/b/g/n à la technologie RFDPI\* brevetée de Dell SonicWALL, pour un déploiement flexible sur les réseaux Clean Wireless. Ce déploiement peut se faire sous forme d'alimentation 802.3af par câble Ethernet (PoE) dans les endroits dépourvus de prise électrique ou par alimentation directe avec un adaptateur CA. L'idéal pour les hôpitaux ou cliniques, les bureaux professionnels et autres scénarios requérant un déploiement discret des équipements sans fil avec des caches pour les voyants et logos, un fonctionnement silencieux et des LED contrôlables (sauf alimentation).



### SonicPoint-Ni Dual-Band

Les points d'accès SonicPoint-Ni Dual-Band de Dell SonicWALL intègrent les fonctionnalités de gestion et d'exécution 802.11a/b/g/n à la technologie RFDPI\* brevetée de Dell SonicWALL pour sécuriser en toute discrétion les environnements réseau Clean Wireless. L'idéal pour les hôpitaux ou cliniques, les bureaux professionnels et autres scénarios requérant un déploiement discret des équipements sans fil avec des antennes internes, des caches pour les voyants et logos, un fonctionnement silencieux et des LED contrôlables (sauf alimentation).



### Injecteur PoE

Le PoE Injector de Dell SonicWALL est un injecteur d'alimentation conforme IEEE 802.3af ou IEEE 802.3at (SonicPoint-N Dual-Radio) utilisant un algorithme d'auto-détection avancé qui détecte automatiquement la présence de dispositifs compatibles PoE et leur « injecte » le courant nécessaire par le câble de données. Prêt à l'emploi, l'injecteur PoE s'intègre aisément aux infrastructures Ethernet sans fil et ne requiert aucune configuration ni gestion.

\* Brevets U.S. n° 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723





## Services avancés pour les appliances de sécurité réseau

### Dell SonicWALL Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control Service

Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control Service assure une protection intelligente des réseaux, en temps réel, contre un large éventail de menaces dynamiques : virus, logiciels espions, vers, chevaux de Troie et vulnérabilités logicielles telles que dépassements de la mémoire tampon, ou encore les intrusions par porte dérobée et autres programmes malveillants. A cela s'ajoute une protection renforcée contre les attaques au niveau de la couche applicative, que celles-ci soient d'origine interne ou externe. Dell SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service ferme les portes dérobées potentielles en examinant une multitude de protocoles de flux, de messagerie, Web et de transfert de fichiers ainsi que les applications poste à poste (P2P) et de messagerie instantanée (IM). Dell SonicWALL Application Intelligence and Control 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.



### Dell SonicWALL Content Filtering Service

Content Filtering Service (CFS) est une solution puissante de protection et de productivité qui assure un filtrage de contenu hors pair pour les établissements scolaires, les entreprises, les bibliothèques et les organismes publics. Grâce à Dell SonicWALL CFS, ceux-ci peuvent contrôler l'accès aux sites Internet contenant des informations ou des images inappropriées, non productives, voire illégales. Les contrôles granulaires fournissent aux administrateurs les outils pour créer et appliquer les règles qui autorisent ou refusent l'accès aux sites selon l'identité d'un individu ou d'un groupe ou l'heure de la journée pour plus de 56 catégories prédéfinies. CFS met en cache dynamiquement les classifications des sites localement sur le pare-feu Dell SonicWALL pour des délais de réponse quasi instantanés.



### Dell SonicWALL Enforced Client Anti-Virus and Anti-Spyware

Fonctionnant de pair avec les pare-feu Dell SonicWALL, Enforced Client Anti-Virus and Anti-Spyware assure dès la passerelle une protection totale des PC et ordinateurs portables contre les virus et logiciels espions. Les pare-feu Dell SonicWALL confirment que la version la plus récente du logiciel antivirus et anti-spyware est installée et activée sur tous les terminaux avant d'autoriser leur accès au réseau. Grâce aux mises à jour automatiques des signatures de virus et logiciels espions, plus besoin de procéder à l'actualisation fastidieuse ordinateur par ordinateur. Le logiciel Enforced Client Anti-Virus and Anti-Spyware de Dell SonicWALL peut être acheté avec le moteur antivirus de McAfee®.



### Dell SonicWALL Comprehensive Anti-Spam Service

Comprehensive Anti-Spam Service (CASS) s'installe instantanément sur les appliances de sécurité réseau Dell 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.

### Déchiffrement et analyse SSL de Dell SonicWALL

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 de Dell SonicWALL. Le trafic est ensuite rechiffré et envoyé à sa destination d'origine en l'absence de menace ou de vulnérabilité.

\* Brevets U.S. n° 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723



### **Dell SonicWALL Secure Virtual Assist**

Secure Virtual Assist est un outil de support distant sans client qui permet au technicien de prendre le contrôle de l'ordinateur de bureau ou portable d'un utilisateur afin de lui fournir une assistance technique. 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. Le portail Web client est simple d'utilisation et présente une apparence familière aux utilisateurs de Windows comme de Mac. De plus, le portail Web technicien et le client autonome facilitent la gestion et la programmation de la file d'attente du support. Enfin, Dell SonicWALL Virtual Assist garantit une intégration étroite aux infrastructures de réseau et d'authentification existantes.



## **Logiciels pour les appliances de sécurité réseau**

### **Clients VPN Dell SonicWALL**

Pour l'accès sécurisé client/hôte, Dell SonicWALL offre des options de connexion à la fois VPN SSL et VPN IPSec. Concernant le VPN SSL, la technologie NetExtender de Dell SonicWALL fournit un accès distant sans client à tous les systèmes Windows, Mac et Linux via un portail Web assurant connectivité et accès. Pour ce qui est du VPN IPSec, l'utilisateur peut télécharger le client VPN grâce au Global VPN Client de Dell SonicWALL, mettant ainsi en place une structure plus classique de VPN sur client.



### **SonicWALL Mobile Connect™**

Mobile Connect est une application client unifié pour iOS, Android et Windows 8.1/RT qui fournit aux utilisateurs de smartphones et tablettes un accès haut de gamme aux ressources des réseaux d'entreprises et d'établissements scolaires, via des connexions VPN SSL chiffrées. Elle permet également de créer un environnement Clean VPN afin d'éliminer les programmes malveillants des communications relayées par des terminaux mobiles.



### **Logiciel de reporting Dell SonicWALL Analyzer**

Analyzer est un outil Web convivial d'analyse du trafic applicatif et de reporting qui offre un aperçu en temps réel et historique de la santé, des performances et de la sécurité d'un réseau. Analyzer prend en charge les pare-feu et les équipements d'accès distant sécurisé Dell SonicWALL et exploite les données d'analyse du trafic applicatif pour établir des rapports sur les événements de sécurité.



### **Dell SonicWALL Global Management System**

Le Système de Gestion globale (GMS) offre aux entreprises, environnements distribués et fournisseurs de services une solution flexible, puissante et intuitive permettant une gestion centralisée et un déploiement rapide des pare-feu, anti-spam et solutions d'accès distant sécurisé Dell SonicWALL. La flexibilité de déploiement se décline sous forme de logiciel ainsi que d'appliance matérielle ou virtuelle. Dell SonicWALL assure également une surveillance centralisée en temps réel et fournit des rapports exhaustifs sur les règles de sécurité et normes de conformité.

## Solutions Dell SonicWALL d'accélération WAN : la série WXA en un coup d'œil

La série WXA (WAN Acceleration Appliance) de Dell SonicWALL réduit la latence au niveau des applications et économise la bande passante, ce qui améliore sensiblement les performances applicatives et l'expérience des utilisateurs du WAN dans les PME dotées de bureaux distants et d'agences. Après un transfert de données initial, la série WXA réduit radicalement tout le trafic ultérieur en ne transmettant que les données nouvelles ou modifiées. La WXA déduplique les données traversant le WAN, se souvient des données transférées précédemment et remplace les séquences d'octets répétées par un identifiant, ce qui se traduit par une réduction de la latence applicative et par des économies de bande passante. Autres fonctionnalités d'accélération : la mise en cache de données et de métadonnées, la déduplication de fichiers, la mise en cache (Web) HTTP ou encore la compression des données en circulation.

Contrairement aux produits d'accélération WAN indépendants, les solutions WXA sont des compléments intégrés aux appliances de sécurité réseau NSA E-Class, NSA et TZ de Dell SonicWALL déployées en tant que pare-feu nouvelle génération. Cela économise de la place, simplifie l'installation et la configuration et améliore le routage, la gestion ainsi que l'intégration de la WXA avec d'autres éléments, par exemple des VPN. Déployées avec un pare-feu nouvelle génération Dell SonicWALL exécutant Application Intelligence and Control Service, les solutions WXA présentent un double avantage inédit, à savoir la hiérarchisation du trafic applicatif et la réduction à un minimum du trafic entre les sites, garantissant ainsi des performances réseau optimales.

Dell SonicWALL vous permet d'ajouter facilement une solution WXA à votre réseau grâce à toute une gamme d'options de plates-formes, incluant des appliances matérielles et virtuelles ainsi qu'un logiciel Live CD.



### WXA 500 Live CD Dell SonicWALL

Le WXA 500 Live CD assure un déploiement flexible via un live-CD de démarrage.



### WXA 2000 Dell SonicWALL

La WXA 2000 accélère les performances réseau pour un maximum de 120 utilisateurs et 600 connexions d'accélération WAN.



### WXA 4000 Dell SonicWALL

La WXA 4000 accélère les performances réseau pour un maximum de 240 utilisateurs et 1 200 connexions d'accélération WAN.

### Appliance virtuelle WXA 5000 Dell SonicWALL

La WXA 5000 permet des déploiements virtuels flexibles dans les environnements VMware®.

Caractéristiques	WXA 500 Live CD	WXA 2000	WXA 4000	WXA 5000 Virtual Appliance
Plate-forme	Logiciel/CD	Appliance matérielle		Appliance virtuelle (VMware)
Nb max. d'utilisateurs <sup>1</sup>	20	120	240	360
Nb max. de connexions	100	600	1 200	1 800 <sup>3</sup>
Nb de licences client WXA simultanées incluses/max. <sup>4</sup>	2/20	2/50	2/125	2/125
Mise en cache d'octets	Oui			
Mise en cache Web (HTTP)	Oui			
Compression	Oui			
Prise en charge de la signature SMB	Oui			
Gestion	Requiert SonicOS 5.8.1 ou version supérieure			
Accélération CIFS/SMB	Oui <sup>2</sup>	Oui		
Visualisation TCP/WFS	Oui			
SNMP	Oui			
Syslog	Oui			
Système d'exploitation	SE Linux Dell SonicWALL renforcé			
Châssis rackable	–	1 U		–
Unité centrale	–	Intel 2,0 GHz	Intel Dual Core 2,0 GHz	–
Mémoire vive	–	2 Go	4 Go	–
Disque dur	–	250 Go	2x250 Go	–
Matrice de disques redondante (RAID)	–	–	RAID 1	–
Dimensions	43,2 x 41,6 x 4,4 cm/17,0 x 16,4 x 1,7 in			
Poids	–	7,26 kg/16 lbs		–
Poids DEEE	–	7,37 kg/16 lbs		–
Consommation (watts)	–	86	101	–
BTU	–	293	344	–
MTBF (années)	14,27			

	WXA 500 Live CD uniquement
Matériel Dell	Dell OptiPlex 3010 Dell Inspiron 660s Dell Vostro 270s

	Appliance virtuelle WXA 5000 uniquement
Hyperviseur	ESX et ESXi (version 4.0, 5.0 ou plus récente)
Système d'exploitation installé	SonicLinux renforcé
CPU minimum	2 x 1,6 GHz
Mémoire allouée	4 Go
Taille de disque appliquée	250 Go
Guide de compatibilité matérielle VMware	<a href="http://vmware.com/resources/compatibility/search.php">http://vmware.com/resources/compatibility/search.php</a>

<sup>1</sup> Le nombre maximum d'utilisateurs peut varier en fonction du nombre de connexions générées par utilisateur. <sup>2</sup> L'accélération CIFS/SMB est disponible uniquement lorsque l'image du Live CD est installée sur le matériel fourni. <sup>3</sup> Le nombre maximum de flux dépend des spécifications matérielles et peut varier suivant la configuration. Les spécifications fournies sont les conditions minimum requises pour pouvoir exécuter l'appliance virtuelle WXA. <sup>4</sup> NetExtender est nécessaire pour utiliser le logiciel client WXA. Pour connaître les systèmes d'exploitation pris en charge, veuillez consulter les notes de mise à jour WXA.

Faciles à utiliser  
et à gérer, les  
solutions d'accès  
distant sécurisé  
Dell SonicWALL  
assurent un  
contrôle granulaire  
des accès.

## Solutions d'accès distant sécurisé Dell SonicWALL

La prolifération des appareils mobiles accroît le besoin d'accès sécurisé aux applications, données et ressources stratégiques. En parallèle, la progression des malwares mobiles fait de la protection des appareils mobiles un impératif commercial. Comme les anciens VPN sur client peuvent être lourds à utiliser et à gérer pour les employés mobiles, les professionnels informatiques cherchent des solutions d'accès mobile sécurisé qui soient conviviales et économiques et répondent aux besoins de leur personnel toujours plus mobile. Dell SonicWALL propose des solutions d'accès mobile sécurisé évolutives qui s'adaptent à toutes les entreprises, des PME aux multinationales. Les séries SRA (Secure Remote Access) E-Class Dell SonicWALL Aventail™ et SRA Dell SonicWALL pour les PME représentent des solutions VPN SSL flexibles pour l'accès distant sécurisé, la récupération après sinistre, la mise en réseau sans fil et la sécurisation des extranets. Elles peuvent être déployées sous forme d'appliances matérielles ou virtuelles. Contrairement aux autres solutions de gestion d'appareils, les solutions Dell peuvent facilement aménager un accès mobile sécurisé et des privilèges basés sur les rôles afin que les utilisateurs finaux bénéficient d'un accès simple et rapide aux applications, données et ressources de l'entreprise dont ils ont besoin. Parallèlement, les entreprises peuvent établir des règles BYOD pour protéger leurs réseaux contre les accès non autorisés et les programmes malveillants.

### La série SRA E-Class de Dell SonicWALL Aventail en un coup d'œil

L'appliance SRA (Secure Remote Access) E-Class de Dell SonicWALL offre aux télétravailleurs des grandes entreprises utilisateurs de smartphones, tablettes ou ordinateurs portables, gérés ou non, un accès facile à base de règles aux applications, données et ressources stratégiques sans compromettre la sécurité. Les appliances SRA de Dell SonicWALL constituent des solutions efficaces offrant les fonctionnalités suivantes :

- Accès distant sécurisé aux ressources et aux applications vitales à partir d'une grande variété de plates-formes, notamment Windows, Windows 8.1/RT, Apple Mac OS, iOS, Linux® et Android
- Accès sans client via un navigateur ou par client Web léger créant un environnement de type « au bureau »
- Continuité des activités et reprise après sinistre lors d'interruptions inattendues
- Contrôle d'accès sécurisé et centralisé pour les réseaux sans fil avec prise en charge de différentes plates-formes de terminaux
- Accès sécurisé aux extranets des partenaires commerciaux pour accroître la productivité collaborative
- Application des règles en différents points d'entrée, permettant un contrôle d'accès granulaire
- Contrôle optimisé de l'accès au portail, du contenu et de la conception grâce au portail WorkPlace de Dell SonicWALL
- Sécurité renforcée qui détecte les risques inhérents à un terminal avant l'authentification, protège les ressources à l'aide de règles granulaires basées sur l'utilisateur et le terminal et ne connecte l'utilisateur qu'aux ressources autorisées
- Analyse des terminaux par l'EPC (End Point Control) récurrent, au moment de la connexion des utilisateurs et à intervalles définis par l'administrateur, afin d'assurer l'intégrité permanente de chaque terminal
- Niveau inégalé de contrôle granulaire qui octroie l'accès en fonction de la confiance accordée à l'utilisateur et à l'appareil utilisé, ainsi que suivant les applications dont l'utilisateur a besoin
- Base solide et durable pour le contrôle d'accès réseau (NAC)



### Solutions d'accès distant sécurisé : la série SRA E-Class de Dell SonicWALL Aventail

#### SRA E-Class EX9000 Dell SonicWALL Aventail

La série SRA (Secure Remote Access) E-Class de Dell SonicWALL Aventail réunit des appliances complètes et faciles à gérer, assurant à elles seules une connectivité de type « au bureau » sans client ou avec un client léger pour un maximum de 20 000 utilisateurs mobiles simultanés. Permettant d'accéder à distance, sur la base de règles, aux ressources du réseau à partir d'appareils Windows, Windows 8.1/RT, Apple Mac OS, iOS, Linux et Android, la solution SRA E-Class améliore la productivité et la continuité des activités.



#### SRA E-Class EX7000 Dell SonicWALL Aventail

La SRA EX7000 de Dell SonicWALL Aventail est une appliance complète et facile à gérer, assurant à elle seule une connectivité de type « au bureau » sans client ou avec un client léger pour un maximum de 5 000 utilisateurs mobiles simultanés. Permettant d'accéder à distance, sur la base de règles, aux ressources du réseau à partir d'appareils Windows, Windows 8.1/RT, Apple Mac OS, iOS, Linux et Android, la solution SRA E-Class améliore la productivité et la continuité des activités.



#### SRA E-Class EX6000 Dell SonicWALL Aventail

La SRA EX6000 de Dell SonicWALL Aventail est une appliance complète et facile à gérer, assurant à elle seule une connectivité de type « au bureau » sans client ou avec un client léger pour un maximum de 250 utilisateurs mobiles simultanés. Permettant d'accéder à distance, sur la base de règles, aux ressources du réseau à partir d'appareils Windows, Windows 8.1/RT, Apple Mac OS, iOS, Linux et Android, la solution SRA E-Class améliore la productivité et la continuité des activités.

#### Appliance virtuelle SRA E-Class Dell SonicWALL Aventail

L'appliance virtuelle SRA E-Class de Dell SonicWALL Aventail est un serveur virtuel renforcé et optimisé en termes de performances, fournissant un accès distant sécurisé sans client, complet et facile à gérer pour les entreprises axées sur la mobilité. Jusqu'à 5 000 utilisateurs simultanés peuvent être pris en charge par une seule appliance virtuelle. Permettant d'accéder à distance, sur la base de règles, aux ressources du réseau à partir d'appareils Windows, Windows 8.1/RT, Apple Mac OS, iOS, Linux et Android, l'appliance virtuelle SRA E-Class améliore la productivité et la continuité des activités.

## Caractéristiques complémentaires E-Class Dell SonicWALL Aventail (en option)



#### Dell SonicWALL Aventail Advanced End Point Control (EPC)<sup>™</sup>

Advanced EPC allie la détection des points d'accès la plus évoluée à la protection des données la plus évoluée. Advanced EPC simplifie la protection des points d'accès avec une liste de contrôle complète d'antivirus, pare-feu personnel et produits anti-spyware qui vérifient même les versions et les mises à jour des fichiers de signature. Advanced EPC ajoute la fonctionnalité de bureau virtuel chiffré de Secure Desktop afin d'offrir le contrôle d'accès distant sécurisé le plus puissant du marché.



#### Dell SonicWALL Aventail Advanced Reporting

Dell SonicWALL Aventail Advanced Reporting <sup>™</sup> offre une analyse puissante de l'accès distant à vos ressources. Advanced Reporting est un solide outil d'analyse hiérarchique de journaux qui peut suivre et évaluer tous les accès d'utilisateurs distants aux ressources de l'entreprise par le biais de l'appliance SRA E-Class.



#### SonicWALL Mobile Connect

Mobile Connect est une application client unifié pour iOS, Android et Windows 8.1/RT qui fournit aux utilisateurs de smartphones et tablettes un accès haut de gamme aux ressources des réseaux d'entreprises et d'établissements scolaires, via des connexions VPN SSL chiffrées.



### Dell SonicWALL Aventail Native Access Modules

L'option Native Access Modules™ de Dell SonicWALL Aventail® permet d'accéder via des protocoles natifs à Citrix®, Windows® Terminal Services et VMWare® View via une appliance sécurisée RSA E-Class Dell SonicWALL Aventail. Elle donne aussi accès aux sessions serveur sans configuration supplémentaire. Grâce à un seul lien de portail, les utilisateurs distants accèdent facilement et en toute transparence à toutes les applications Citrix en bénéficiant de la prise en charge des fermes Citrix avec répartition de charge.



### Dell SonicWALL Aventail Spike License

Spike License est une « police d'assurance » de récupération après sinistre permettant d'augmenter le nombre d'utilisateurs distants. Flexible, le pack Spike License est un complément de licence temporaire qui permet d'augmenter immédiatement le nombre d'utilisateurs distants en cas de sinistre ou autre interruption d'activité. Il s'agit d'une solution idéale dans le cadre d'un plan global de récupération après sinistre ainsi que pour les entreprises qui connaissent des pics d'activité saisonniers.



### Dell SonicWALL Secure Virtual Assist

Outil de support permettant de fournir une assistance technique à distance.



### Dell SonicWALL Analyzer

Outil Web convivial d'analyse du trafic applicatif et de reporting qui offre un aperçu en temps réel et historique des performances et de la sécurité d'un réseau. Pour les appliances SRA E-Class de Dell SonicWALL Aventail, Analyzer établit des rapports sur les connexions à distance des utilisateurs. Analyzer fournit également des rapports sur les pare-feu Dell SonicWALL.

Caractéristique	Appliance virtuelle	EX6000	EX7000	EX9000
Nb de licences utilisateurs simultanés	jusqu'à 5 000	jusqu'à 250	jusqu'à 5 000	jusqu'à 20 000
Interrogation EPC de base	Inclus			
EPC avancé (antivirus, pare-feu personnel, anti-spyware)	Complément		Inclus	
Aventail Secure Desktop/ Cache Cleaner	Complément		Inclus	
Zones d'autorisation, de refus et de mise en quarantaine basés sur l'interrogation EPC	Inclus			
Contrôle d'accès granulaire (utilisateur et groupe, IP source, service/port, URL de destination, nom d'hôte/adresse IP, plage IP, sous-réseau, domaine)	Inclus			
Advanced Reporting	Complément			
Analyzer	Complément			
Portail WorkPlace	Inclus			
WorkPlace Mobile (portail optimisé pour les navigateurs de téléphones portables)	Inclus			
Native Access Modules (Citrix, Windows Terminal Services et VMware View)	Complément		Inclus	
Connect Tunnel (Windows, Mac OS et Linux)	Inclus			
Mobile Connect (iOS)	Inclus			
Mobile Connect (Android)	Inclus			
Mobile Connect (Windows 8.1/RT)	Inclus			
Prise en charge IPv6 côté client	Inclus			
Prise en charge ADA 508	Inclus			
Tableau de bord de statut visible en un coup d'œil	Inclus			



Les VPN SSL de Dell SonicWALL offrent un accès distant sécurisé abordable, facile à utiliser et à gérer.

## La série SRA de Dell SonicWALL pour PME en un coup d'œil

La série SRA de Dell SonicWALL allie simplicité et sécurité à petit prix pour permettre d'accéder à distance et sans client au réseau et aux applications des entreprises de toutes tailles. L'installation préalable d'un logiciel n'est plus nécessaire. Un navigateur Web standard suffit aux utilisateurs pour accéder facilement et en toute sécurité, où qu'ils soient, aux e-mails, fichiers, pages intranet, applications, ordinateurs distants, serveurs et autres ressources disponibles sur le LAN de l'entreprise. Les solutions VPN SSL de Dell SonicWALL s'intègrent parfaitement à pratiquement tous les types de réseaux, avec ou sans fil, pour fournir un accès distant puissant, évolutif et abordable aux ressources de l'entreprise. La série SRA de Dell SonicWALL est disponible sous forme d'appliance matérielle ou virtuelle dans un environnement VMware.

- L'intégration parfaite avec la majorité des pare-feu permet de conserver l'infrastructure réseau existante.
- L'authentification à deux facteurs sans jeton assure une protection optimale contre les enregistreurs de frappes en associant un mot de passe à usage unique (généralisé par l'appliance VPN SSL et envoyé à l'équipement mobile d'un utilisateur distant ou à son adresse e-mail) aux nom et mot de passe réseau de l'utilisateur.
- La prise en charge des appareils mobiles iOS, Android et Windows 8.1/RT permet d'accéder à l'intégralité d'un intranet ainsi qu'aux applications Web, ce qui accroît la flexibilité du personnel à distance.
- Le contrôle granulaire de la configuration des règles permet aux administrateurs de limiter l'accès des utilisateurs à certaines applications/ressources et d'en empêcher la visualisation ou l'utilisation sans autorisation.
- Le téléchargement d'applications permet aux utilisateurs d'accéder aux applications Web de manière sécurisée sur la base d'une authentification forte et de règles d'accès granulaires.
- Le Web Application Firewall Service de Dell SonicWALL détecte les attaques basées sur Internet et protège les applications Web (y compris l'appliance VPN SSL elle-même), ce qui réduit les pertes potentielles et permet de respecter les prescriptions de conformité relatives à la protection des données telles que la norme PCI DSS.
- End Point Control (EPC) pour la série SRA permet d'identifier de manière unique les appareils Windows®, Mac OS® ou Linux® afin de les associer à l'utilisateur autorisé et d'évaluer l'état de sécurité de l'appareil en contrôlant des éléments tels que les logiciels antivirus et anti-spyware.
- Le support distant avec Dell SonicWALL Secure Virtual Assist permet aux employés d'obtenir facilement l'assistance nécessaire en permettant aux techniciens de prendre le contrôle d'un appareil Windows, Mac OS ou Linux à distance afin de diagnostiquer et régler les problèmes.
- Secure Virtual Access garantit des flux de travail transparents en permettant aux employés d'accéder facilement à leurs ordinateurs Windows®, de n'importe où et en toute sécurité.
- Intégrant toutes les fonctionnalités de sécurité de la série SRA pour PME, Secure Virtual Meeting assure une protection d'ensemble des communications sensibles et confidentielles, tout en permettant de collaborer de manière économique.
- Les licences Spike permettent à l'administrateur de préparer un plan antispionnage en vue de prendre en charge une pointe dans les effectifs d'utilisateurs.
- Lorsqu'une appliance série SRA est déployée avec un pare-feu nouvelle génération Dell SonicWALL, Clean VPN utilise la puissante technologie de filtrage applicatif pour analyser le trafic et éliminer les programmes malveillants avant qu'ils n'infiltrerent le réseau.





### SRA 4600 Dell SonicWALL

L'appliance SRA 4600 de Dell SonicWALL s'adresse aux entreprises de taille moyenne souhaitant disposer d'une solution d'accès distant sécurisé à la fois puissante, conviviale et économique, sans installation préalable d'un logiciel. Un navigateur Web standard suffit aux utilisateurs pour accéder facilement et en toute sécurité aux e-mails, fichiers, pages intranet, applications, ordinateurs distants, serveurs et autres ressources disponibles sur le LAN de l'entreprise depuis un vaste éventail d'appareils et systèmes d'exploitation, notamment Windows, Windows 8.1/RT, Mac OS, Linux, Apple iOS et Android. Des services supplémentaires à valeur ajoutée permettent d'assurer le support des PC à distance, l'accès à distance aux PC et la collaboration, tandis que le service WAF (Web Application Firewall) renforce la sécurité des applications Web. La haute disponibilité (HA) sur la SRA 4600 offre une configuration active/passive permettant aux entreprises de disposer d'une fiabilité accrue en cas de panne.



### SRA 1600 Dell SonicWALL

Pour les PME, l'appliance SRA 1600 de Dell SonicWALL offre une solution d'accès distant sécurisé à la fois puissante, conviviale et économique, sans installation préalable d'un logiciel. Un navigateur Web standard suffit aux utilisateurs pour accéder facilement et en toute sécurité aux e-mails, fichiers, pages intranet, applications, ordinateurs distants, serveurs et autres ressources disponibles sur le LAN de l'entreprise depuis un vaste éventail d'appareils et systèmes d'exploitation, notamment Windows, Windows 8.1/RT, Mac OS, Linux, Apple iOS et Android. Des services supplémentaires à valeur ajoutée permettent d'assurer le support des PC à distance et l'accès à distance aux PC, tandis que le service WAF (Web Application Firewall) renforce la sécurité des applications Web.

### Appliance virtuelle SRA

L'appliance virtuelle SRA de Dell SonicWALL fournit un accès sans client par tunnel pour Windows, Windows 8.1/RT, Apple Mac OS, iOS, Linux et Android. Des services supplémentaires à valeur ajoutée permettent d'assurer le support des PC à distance, l'accès à distance aux PC et la collaboration, tandis que le service WAF (Web Application Firewall) renforce la sécurité des applications Web. L'appliance virtuelle SRA peut être rapidement déployée dans un environnement virtualisé. Elle constitue une solution économique permettant de réduire le coût total de possession (TCO).

## Caractéristiques complémentaires pour les VPN SSL de Dell SonicWALL (en option)



### Dell SonicWALL Web Application Firewall Service

Solution primée de conformité complète, abordable et prête à l'emploi, le service Web Application Firewall (WAF) de Dell SonicWALL s'appuie sur l'infrastructure existante pour ajouter à la plate-forme d'accès distant sécurisé Dell SonicWALL un module complémentaire sur licence. Grâce à une bibliothèque de signatures actualisée dynamiquement qui permet de détecter les attaques Web sophistiquées et de protéger les applications Web – notamment les portails VPN SSL –, le service WAF applique au trafic de la couche 7 une analyse de proxy inverse pour les signatures connues, refuse l'accès en cas de détection d'un programme malveillant dans une application Web et redirige les utilisateurs vers une page d'erreur explicative. Dell SonicWALL WAF permet également d'ajouter des chaînes de règles et d'utiliser le profilage automatique des applications pour procéder à des « corrections virtuelles » en vue de protéger contre les menaces zero-day véhiculées par les applications Web. Les administrateurs peuvent par ailleurs utiliser la géolocalisation et le filtrage de botnets pour créer et exécuter des règles bloquant les connexions en provenance de certaines régions ou de systèmes connus pour être infectés. Dell SonicWALL WAF est un élément essentiel en matière de conformité PCI. Il est en outre doté de fonctionnalités Web de protection contre la fuite de données destinées à empêcher que des informations sensibles telles que les numéros de cartes de crédit et de sécurité sociale tombent en de mauvaises mains.

## Caractéristiques complémentaires pour les SRA de Dell SonicWALL pour PME (en option)



### SonicWALL Mobile Connect

Mobile Connect est une application client unifié pour iOS, Android et Windows 8.1/RT qui fournit aux utilisateurs de smartphones et tablettes un accès haut de gamme aux ressources des réseaux d'entreprises et d'établissements scolaires, via des connexions VPN SSL chiffrées. Déployée avec un pare-feu Dell SonicWALL nouvelle génération, elle permet à la technologie Clean VPN d'éliminer les programmes malveillants des communications relayées par des terminaux mobiles.



### Dell SonicWALL Secure Virtual Assist

Secure Virtual Assist est un outil de support distant qui permet au technicien de prendre le contrôle de l'ordinateur de bureau ou portable Windows, Mac OS ou Linux d'un utilisateur afin de lui fournir une assistance technique à distance. Avec l'autorisation de l'utilisateur, le technicien peut instantanément accéder à un ordinateur par le biais d'un navigateur Web, puis aisément diagnostiquer et réparer les problèmes à distance sans devoir envoyer quelqu'un sur place pour régler le problème.



### Dell SonicWALL Secure Virtual Access

Secure Virtual Access est un outil de contrôle de PC à distance qui permet aux utilisateurs finaux autorisés d'accéder de n'importe où et en toute sécurité à leurs ordinateurs Windows non surveillés. L'utilisateur n'a qu'à installer l'agent Virtual Access sur un ordinateur Windows disposant d'un accès à Internet. Dès lors, du moment que cet ordinateur est relié au VPN SSL de Dell SonicWALL, l'utilisateur peut accéder au PC distant via le portail Web SRA. Cela est particulièrement utile pour les employés distants devant se connecter à l'ordinateur de leur domicile ou à un PC d'agence qui n'est normalement pas connecté au LAN.



### Dell SonicWALL Secure Virtual Meeting

Secure Virtual Meeting permet de collaborer de manière sécurisée et économique, éliminant les frais de déplacement inutiles. Contrairement aux autres solutions de réunion virtuelle, Dell SonicWALL Secure Virtual Meeting intègre toutes les fonctionnalités de sécurité de la série SRA pour PME, offrant une protection d'ensemble des communications sensibles et confidentielles. Secure Virtual Meeting s'intègre aux systèmes de planification de calendriers tels que Microsoft Outlook™.



### Dell SonicWALL End Point Control pour la série SRA

End Point Control (EPC) pour la série SRA offre des fonctionnalités haut de gamme d'identification et d'interrogation des terminaux à l'attention des petites et moyennes entreprises. EPC pour la série SRA identifie de manière unique les terminaux Windows, Mac OS et Linux et les associe à des utilisateurs autorisés. Elle contrôle aussi rigoureusement leur état de sécurité en vérifiant la présence des composants de sécurité essentiels, tels que les logiciels d'antivirus, d'anti-spyware et de pare-feu personnel, afin de garantir l'intégrité des appareils avant de les autoriser à se connecter au réseau. La liste d'interrogation des appareils comprend les solutions d'antivirus, d'anti-spyware et de pare-feu personnel prises en charge d'éditeurs leaders tels que McAfee, Kaspersky Lab, Symantec®, Computer Associates®, Sophos® et beaucoup d'autres. Cela réduit considérablement les risques d'infiltration sur le réseau de programmes malveillants par les appareils non gérés par les services informatiques.

## Caractéristiques complémentaires pour les SRA de Dell SonicWALL pour PME (en option)



### Dell SonicWALL Spike License

Spike License permet d'accroître immédiatement le nombre d'utilisateurs distants pour une période limitée suite à un sinistre ou à toute autre interruption d'activité.



### Dell SonicWALL Analyzer

Analyzer est un outil convivial d'analyse du trafic applicatif et de reporting qui offre un aperçu en temps réel et historique des performances et de la sécurité d'un réseau. Pour les dispositifs SRA, Analyzer établit des rapports sur les connexions des utilisateurs distants et l'activité du service WAF. Analyzer fournit également des rapports sur les pare-feu Dell SonicWALL.

Déploiement	SRA 1600	SRA 4600	Appliance virtuelle SRA
Type et taille de l'environnement de déploiement	Petites entreprises de 50 employés max.	Moyennes entreprises de 500 employés max.	Petites entreprises de 50 employés max.
Nb inclus/max. (recommandé) de licences utilisateurs	5/50 (25)	25/500 (100)	5/50
Nb inclus/max. de licences de connexion Virtual Access/Virtual Assist	Essai de 30 jours/10	Essai de 30 jours/25	

Caractéristiques	SRA 1600	SRA 4600	Appliance virtuelle SRA
Secure Virtual Access		Complément	
Secure Virtual Assist		Complément	
Secure Virtual Meeting	—	Complément	
End Point Control pour la série SRA		Complément	
Analyzer		Complément	
Web Application Firewall		Complément	
Licences Spike		Complément	
Règles basées sur la géolocalisation		Complément	
Filtrage de botnets		Complément	
Authentification OTP (mot de passe unique)		Inclus	
Authentification à deux facteurs de Dell Quest Defender		Inclus	
Prise en charge Citrix (ICA)		Inclus	
NetExtender : prise en charge de plusieurs plages d'adresses IP et routes		Inclus	
Prise en charge des certificats client en option		Inclus	
Surveillance graphique de l'utilisation		Inclus	
Option de création d'une sauvegarde système		Inclus	
Proxy inverse : OWA Premium et Lotus Domino Access		Inclus	
Fonction de test RADIUS		Inclus	
Prise en charge des groupes Active Directory		Inclus	
Prise en charge des noms de domaine/hôte virtuel		Inclus	
Applet Java FileShares		Inclus	
Diagnostics : DNS Lookup et Traceroute		Inclus	
SNMPv2		Inclus	
Equilibrage de charge de couche 7		Inclus	
Haute disponibilité (HA)	—	Inclus	—
Déchargement SSL avec assistance matérielle	—	Inclus	Dépend du matériel sous-jacent
Mobile Connect (iOS)		Inclus	
Mobile Connect (Android)		Inclus	
Mobile Connect (Windows 8.1/RT)		Inclus	

Protection efficace  
et conviviale  
contre les menaces  
véhiculées  
par le courrier  
électronique

## Dell SonicWALL Email Security

Protégez votre structure contre les menaces véhiculées par les e-mails, entrants comme sortants, et la violation de règles de conformité avec Dell SonicWALL Email Security. Bénéficiez d'une protection haut de gamme en temps réel contre les attaques de type spam, phishing, virus, zombies, DHA (Directory Harvest Attack), DoS (Denial of Service) et autres grâce aux diverses techniques éprouvées et brevetées<sup>1</sup> de détection des menaces de Dell SonicWALL et son réseau mondial, unique en son genre, d'identification et de surveillance des attaques. De plus, Email Security prévient les fuites de données confidentielles et la violation des règles grâce à une analyse et une gestion avancées de la conformité.

Dell SonicWALL Email Security peut couvrir de manière simple et économique de 10 à 100 000 boîtes aux lettres électroniques. Flexible, cette solution peut être déployée sous forme d'appliance matérielle évolutive, d'appliance virtuelle ou de logiciel, y compris un logiciel optimisé pour Microsoft Windows® Server ou Small Business Server (SBS), pour s'adapter parfaitement à votre budget et à votre infrastructure et vous permettre de rentabiliser au mieux votre investissement sur le long terme. Vous pouvez la configurer en mode divisé à des fins de haute disponibilité et d'évolutivité, et gérer de manière fiable et centralisée, de vastes déploiements. L'administration est simple, rapide et intuitive. Vous pouvez déléguer la gestion des spams aux utilisateurs finaux, tout en conservant le contrôle nécessaire sur les règles de sécurité appliquées. Ou encore gérer en toute simplicité les comptes d'utilisateurs et de groupes grâce à une synchronisation multi-LDAP transparente. Dans les grands environnements distribués, la prise en charge de la mutualisation vous permet désormais de charger des sous-administrateurs de gérer les paramètres au niveau de différentes unités organisationnelles (divisions de l'entreprise ou fournisseurs MSP, par ex.) au sein d'un seul et même déploiement Email Security.

## Série Email Security de Dell SonicWALL

### Appliances Email Security Dell SonicWALL

Les appliances Email Security de Dell SonicWALL offrent une protection complète, efficace et évolutive, spécialement adaptée aux besoins des PME, grands comptes et fournisseurs de services gérés. Puissante et facile à gérer, elle allie les services d'anti-spam, d'antivirus et d'anti-phishing au filtrage de contenu et à la gestion des e-mails sortants, afin d'empêcher toute fuite d'informations confidentielles et d'assurer le respect des lois de conformité en vigueur. Le scannage préventif de l'agent MTA (Mail Transfer Agent) offre une analyse approfondie des messages ainsi que des débits de transmission inégalés, garants de performances hors pair et d'une excellente évolutivité dans l'ensemble de l'entreprise.

### Logiciel Email Security Dell SonicWALL

Pour les entreprises équipées d'un matériel spécifique, qui disposent déjà de systèmes de surveillance et de sauvegarde ou qui souhaitent tout simplement garder un maximum de flexibilité en matière de déploiement, le logiciel Dell SonicWALL E-Class Email Security rassemble toutes les fonctionnalités des appliances E-Class Email Security de Dell SonicWALL sur une plate-forme logicielle pour garantir une protection optimale, un contrôle aisé et des performances hors pair.

### Appliance virtuelle Email Security Dell SonicWALL

L'appliance virtuelle Email Security de Dell SonicWALL présente un serveur virtuel renforcé et optimisé en termes de performances pour Dell SonicWALL Email Security. Jusque-là, fidèles au modèle « un serveur, une application », les administrateurs avaient souvent tendance à sous-exploiter les ressources matérielles et à perdre beaucoup de temps avec la gestion des serveurs. Les appliances virtuelles Dell SonicWALL améliorent sensiblement l'efficacité et la disponibilité des ressources et des applications. Pour répondre à des besoins plus importants en termes de déploiement et d'évolutivité, les administrateurs peuvent faire appel au mode Split-Config leur permettant de déployer plusieurs appliances virtuelles sur un seul ou plusieurs serveurs physiques.



<sup>1</sup>Brevets U.S. n° 7 814 545 ; 7 343 624 ; 7 665 140 ; 7 653 698 ; 7 546 348

### **Dell SonicWALL Hosted Email Security**

Dell SonicWALL Hosted Email Security assure une protection supérieure, basée sur le cloud, contre les menaces entrantes et sortantes, notamment les spams, le phishing, les attaques de zombies et les programmes malveillants, à un tarif d'abonnement mensuel ou annuel flexible, prévisible et économique. Parallèlement, ce service réduit en amont le temps et les coûts de déploiement ainsi que les dépenses administratives régulières. Dell SonicWALL Hosted Email Security est la seule solution hébergée à intégrer plusieurs technologies antivirus, dont Dell SonicWALL GRID (Global Response Intelligent Defense) Anti-Virus, Dell SonicWALL Time Zero et autres technologies haut de gamme, pour une sécurisation maximum des messageries. Le réseau GRID de Dell SonicWALL soumet chaque jour des millions d'e-mails à des évaluations et des tests rigoureux, puis réutilise cette analyse mise à jour en permanence, ce qui lui permet de garantir des résultats exceptionnels en termes de blocage et de protection antivirus et anti-spyware. La protection antivirus « Time Zero » de Dell SonicWALL utilise des technologies prédictives et réactives pour protéger les entreprises de toute infection virale avant même que les mises à jour de signatures antivirus soient disponibles. Les e-mails suspects sont identifiés et immédiatement mis en quarantaine, assurant la sécurité du réseau dans l'intervalle de temps séparant la déclaration d'un virus et la disponibilité de la nouvelle signature. La technologie haut de gamme de partenaires leaders venant s'ajouter comme couche de sécurité supplémentaire, il en résulte une protection supérieure à celle des solutions reposant sur une seule technologie antivirus.

## Services de sécurisation de messagerie Dell SonicWALL



### Abonnement à Dell SonicWALL Email Protection et support dynamique (8x5 ou 24x7)

L'abonnement au service Email Protection et au support dynamique est nécessaire pour les appliances et logiciels Email Security dans la mesure où il complète la solution de sécurisation de messagerie par des mises à jour anti-spam et anti-phishing en temps réel ainsi que des mises à jour logiciel/firmware. L'abonnement comprend un support technique 8x5 ou 24x7 avec retour matériel (RMA) pour l'appliance et une garantie de réparation ou de remplacement de tout produit présentant des défauts de fabrication.



### Abonnement à Dell SonicWALL Email Anti-Virus

Grâce à la technologie « Time Zero » de Dell SonicWALL, l'abonnement à Email Anti-Virus protège de manière instantanée dans l'intervalle de temps séparant la déclaration d'un virus et la disponibilité de la nouvelle signature. Le partenariat de Dell SonicWALL avec McAfee assure en outre la fourniture systématique des signatures virales les plus récentes, pour une protection optimale.



### Abonnement à Dell SonicWALL Email Compliance

L'abonnement à Email Compliance permet aux entreprises de satisfaire aux exigences de conformité réglementaire et de gérer de manière optimale l'utilisation de leur messagerie. Ce service offre notamment les caractéristiques suivantes : analyse détaillée des pièces jointes, dictionnaires de conformité, boîtes de validation, filtrage des ID d'enregistrement, routage et chiffrement, archivage d'e-mails, règles prédéfinies et rapports de conformité. Autant de fonctions qui permettent d'identifier intelligemment les messages non conformes, de surveiller et de signaler les problèmes avant d'appliquer les mesures appropriées... pour que les entreprises aient toujours une longueur d'avance en matière de protection et de conformité.

Appliances Email Security	PME		E-Class
Modèle	3300	4300	ES8300
Châssis rackable	1 U		2 U
Unité centrale	Intel 2,0GHz	Intel Dual Core 2,0GHz	Quad Core Xeon
Mémoire vive	2 Go	4 Go	
Disque dur	250 Go	2 x 250 Go	4 x 750 Go
Matrice de disques redondante (RAID)	Non	Oui	RAID 5
Lecteurs remplaçables à chaud	Non	Oui	
Alimentation redondante	Non		Oui

Logiciel Email Security	
Plates-formes logicielles	Microsoft Windows 2003 Server ou Windows Server 2008

Appliance virtuelle Email Security	
Hyperviseur	ESXi™ et ESX™ (version 4.0 ou plus récente)

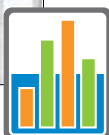
## Solutions de reporting et de gestion des règles Dell SonicWALL

### Dell SonicWALL Global Management System

Global Management System (GMS) fournit aux entreprises, environnements distribués et fournisseurs de services un outil puissant et intuitif permettant une gestion centralisée et un déploiement rapide des solutions de pare-feu, d'anti-spam, de sauvegarde et récupération et d'accès distant sécurisé Dell SonicWALL. GMS offre diverses options de déploiement, sous forme de logiciel ainsi que d'appliance matérielle ou virtuelle ; il assure également une surveillance centralisée en temps réel des réseaux et fournit des rapports exhaustifs sur les règles de sécurité et normes de conformité. Pour les entreprises, Dell SonicWALL GMS optimise la gestion des règles de sécurité et le déploiement des appliances, réduisant par là même la charge administrative. Pour les fournisseurs de services, Dell SonicWALL GMS simplifie la gestion de la sécurité de nombreux clients et crée des sources de revenus supplémentaires. Pour augmenter la redondance et l'évolutivité, le système GMS peut être déployé en cluster.



- Logiciel GMS : Dell SonicWALL GMS peut être déployé de manière flexible comme logiciel sur un serveur Windows tiers, au sein de l'infrastructure existante.
- Appliance virtuelle GMS : cette appliance présente un agent virtuel renforcé et optimisé en termes de performances pour le système de gestion globale Dell SonicWALL GMS. Jusque-là, fidèles au modèle « un serveur, une application », les administrateurs avaient souvent tendance à sous-exploiter les ressources matérielles et à perdre beaucoup de temps avec la gestion des serveurs. Les appliances virtuelles Dell SonicWALL améliorent sensiblement l'efficacité et la disponibilité des ressources et des applications.
- Appliance de gestion universelle EM5000 : cette UMA primée, sur un boîtier hautes performances renforcé, simplifie et automatise la gestion mult niveau des règles, la surveillance et le contrôle de conformité, grâce à des outils flexibles, intuitifs et puissants. Un déploiement en cluster de plusieurs appliances UMA convient parfaitement à la gestion de milliers d'appliances de sécurité Dell SonicWALL.



### Dell SonicWALL Analyzer

Analyzer est un outil Web convivial d'analyse du trafic et de reporting qui offre un aperçu en temps réel et historique de la santé, des performances et de la sécurité d'un réseau. Analyzer prend en charge les pare-feu et les équipements d'accès distant sécurisé Dell SonicWALL et exploite les données d'analyse du trafic applicatif pour établir des rapports sur les événements de sécurité. Les entreprises de toute taille bénéficient d'une meilleure productivité de leur personnel, d'une consommation optimisée de la bande passante réseau et d'une sensibilité accrue aux questions de sécurité. Dell SonicWALL est le seul éditeur de pare-feu à proposer une solution complète combinant l'analyse externe du trafic applicatif aux données statistiques granulaires générées par les pare-feu Dell SonicWALL. Dell SonicWALL Analyzer est disponible sous forme d'application Windows et d'appliance virtuelle.



### Dell SonicWALL Scrutinizer

Scrutinizer est un outil multifournisseur d'analyse, de visualisation et de génération de rapports sur le trafic applicatif basé sur les flux, qui permet de mesurer l'utilisation et les performances du réseau et de résoudre les problèmes survenus, tout en améliorant la productivité des entreprises et des fournisseurs de services. Scrutinizer prend en charge une vaste palette de routeurs, commutateurs, pare-feu et protocoles de reporting sur les flux de données, offrant une vision unique de l'analyse du trafic applicatif à partir des données IPFIX/NetFlow exportées par les pare-feu Dell SonicWALL. Scrutinizer permet d'identifier facilement les principaux flux, protocoles, applications, conversations, domaines, pays et sous-réseaux, et émet des alertes lors de comportements suspects. Scrutinizer inclut l'analyse de trafic avec filtrage applicatif, le contrôle proactif de gigue/latence, la génération de rapports automatisée et des tableaux de bord personnalisables. Scrutinizer propose également des options de reporting historique et avancé, d'administration par rôle, d'analyse avancée et d'alertes par seuil, en plus des nombreuses fonctionnalités spécifiques MSP et ISP. Dell SonicWALL Scrutinizer est disponible sous forme d'application Windows et d'appliance virtuelle.





## Services de support global Dell SonicWALL

Dell SonicWALL offre une gamme variée de services de support global conçus non seulement pour garder à jour votre infrastructure de sécurité réseau et de sauvegarde et récupération des données, mais aussi pour résoudre rapidement tout problème éventuel. Cependant, à l'heure actuelle, cela ne suffit plus pour protéger efficacement les réseaux. C'est pourquoi Dell SonicWALL a complété ses services par des mises à jour et des mises à niveau logiciel et firmware spécifiques, une assistance technique efficace, un remplacement matériel immédiat et l'accès à un large éventail d'outils électroniques.



### Support Platinum Dell SonicWALL pour la série SuperMassive E10000

Le support et les services professionnels Platinum allient assistance technique et services personnalisés pour permettre de rentabiliser au maximum votre investissement Dell SonicWALL. Le support Platinum Dell SonicWALL est une offre personnalisée réunissant un ensemble complet de services destinés à garantir l'efficacité et la rentabilité opérationnelles. Il est géré et assuré par une équipe de techniciens chevronnés qui connaissent les contraintes techniques et entrepreneuriales de leurs clients. Axé sur un cycle de vie proactif des services et du support, le support Platinum Dell SonicWALL établit une base opérationnelle solide, anticipe les exigences en matière de sécurité et s'adapte dynamiquement pour assister les entreprises dans la réalisation de leurs objectifs. De plus, les services professionnels Platinum proposent l'installation et la configuration sur site, des cours et formations ainsi que la migration du système à partir d'une solution Dell SonicWALL ou d'un produit d'une autre marque.

- Assistance 24 heures/24, 7 jours/7 d'une équipe de techniciens spécialisés
- Mises à jour et mises à niveau logiciel et firmware
- Remplacement anticipé de matériel (RMA)

### Support Gold

Réservé aux pare-feu nouvelle génération des séries NSA 5600, NSA 6600 et SuperMassive 9000, le support Gold offre des options d'assistance avancées aux grands comptes devant garantir un fonctionnement fiable et sécurisé de leur réseau. Avec le support Gold, vous pouvez contacter 24 heures/24 les techniciens chevronnés d'un centre d'assistance technique (TAC) Dell SonicWALL pour grands comptes, et bénéficier des toutes dernières fonctionnalités firmware ainsi que du remplacement anticipé de matériel. Autant d'atouts conçus pour protéger et rentabiliser au mieux votre investissement Dell SonicWALL.

- Mises à jour et mises à niveau logiciel et firmware
- Accès 24 heures/24, 7 jours/7 à une équipe de techniciens compétents d'un TAC Dell SonicWALL pour grands comptes assurant une assistance téléphonique, par courrier électronique et Web
- Remplacement anticipé de matériel (RMA)

### Support Silver

Plus qu'un simple service de dépannage, le support Silver de Dell SonicWALL est une offre de sécurité multicouche qui vous donne accès aux mises à jour et mises à niveau importantes ainsi qu'à l'assistance technique de spécialistes afin de garantir un fonctionnement optimal de votre solution Dell SonicWALL. Aperçu des prestations :

- Abonnement aux mises à jour et mises à niveau firmware
- Accès à l'assistance téléphonique, par courrier électronique, chat et Web en formule 8x5 ou 24x7
- Remplacement anticipé de matériel le prochain jour ouvré en cas de panne



### Support E-Class

Conçu pour les solutions E-Class de Dell SonicWALL, le support 24x7 E-Class de Dell SonicWALL offre l'assistance et la qualité de service haut de gamme dont les grandes entreprises ont besoin pour assurer un fonctionnement fluide et efficace de leur réseau.

- Accès 24 heures/24, 7 jours/7 à une équipe de techniciens compétents d'un TAC Dell SonicWALL pour grands comptes assurant une assistance téléphonique, par courrier électronique et Web
- Abonnement aux mises à jour et mises à niveau firmware
- Remplacement anticipé de matériel le prochain jour ouvré en cas de panne

### Support dynamique

Destinés aux clients désirant une protection continue via des mises à niveau logiciel et firmware régulières et un support technique avancé, les services de support dynamique Dell SonicWALL sont accessibles aux heures normales d'ouverture, ou 24 heures/24 et 7 jours/7 en fonction de vos besoins. Aperçu des prestations :

- Abonnement aux mises à jour et mises à niveau firmware
- Accès à l'assistance téléphonique, par courrier électronique, chat et Web
- Remplacement anticipé de matériel le prochain jour ouvré en cas de panne

### Support Comprehensive Global Management System (support CGMS)

Le support Comprehensive GMS de Dell SonicWALL s'adresse aux clients qui utilisent le système de gestion globale Dell SonicWALL GMS pour gérer leur réseau distribué. Ce service général englobe tous les avantages d'un contrat de support dynamique 24x7 pour chaque appliance gérée par l'intermédiaire de Dell SonicWALL GMS. Le support Comprehensive GMS comprend :

- Tous les services et avantages d'un contrat de support dynamique 24x7
- Le support et les mises à jour logicielles de l'application GMS elle-même
- Une échéance commune à tous les services, ce qui simplifie la gestion et l'administration

### Assistance technique spécifique

Les clients travaillant avec des applications et systèmes d'importance stratégique doivent pouvoir compter sur un support de premier ordre. C'est ce que propose le « Focused Technical Support » (FTS) de Dell SonicWALL, conçu pour offrir à nos grands comptes le plus haut niveau de service et la meilleure réactivité du secteur. Cette offre de support Premium comprend une gamme complète de services proactifs, tous gérés par un Dell SonicWALL Security Engineer (SSE) qui connaît vos besoins techniques et votre entreprise.

- Service personnalisé pour les entreprises requérant un support haut de gamme offert par un technicien attitré
- Disponible en formules 8x5 (FTS Standard et Lite) ou 24x7 (FTS Ultra)
- Accès immédiat aux experts techniques et soutien rapide concernant les produits Dell SonicWALL, ce qui optimise les processus de signalisation progressive et de traitement de nouvelles fonctionnalités



### Service de démarrage et de configuration à distance Dell SonicWALL

Quelle que soit la taille de l'entreprise, le service Dell SonicWALL de configuration et de démarrage à distance exécute une configuration et un déploiement rapides et sécurisés des appliances Dell SonicWALL dans un réseau nouveau ou existant. La configuration à distance est effectuée par des techniciens certifiés CSSA qui utilisent une méthode Dell SonicWALL éprouvée, garantissant que la solution est correctement configurée et prête au déploiement. Ce service réduit les coûts associés à la configuration et au déploiement de nouvelles appliances et améliore la productivité en libérant le personnel qui peut dès lors se consacrer à d'autres tâches stratégiques. Avec le service de configuration à distance, votre appliance Dell SonicWALL est mise en marche en quelques heures, d'où un retour plus rapide sur votre investissement Dell SonicWALL.

## Dell SonicWALL

Dell SonicWALL fournit des solutions intelligentes de sécurité réseau permettant à ses clients et à ses partenaires de sécuriser, contrôler et élargir leurs réseaux, dynamiquement et globalement. Exploitant les données partagées de millions de capteurs au sein du réseau GRID (Global Response Intelligent Defense) de Dell SonicWALL, le Dell SonicWALL Threat Center fournit en continu des informations et des analyses sur la nature, le comportement et l'évolution des menaces. Le laboratoire de recherches Dell SonicWALL Research Labs traite toutes ces informations, sans interruption, afin de livrer proactivement les armes et les mises à jour dynamiques nécessaires pour contrer les menaces les plus récentes. La technologie RFDPI (Reassembly-Free Deep Packet Inspection) brevetée\* associée à une architecture multiprocesseur en parallèle permet un filtrage et une analyse simultanés des diverses menaces à vitesse de ligne (wire-speed) et crée les conditions techniques nécessaires à la solution pour s'adapter dans son intégralité aux déploiements dans les réseaux haut débit. La gamme de solutions de sécurité réseau Dell SonicWALL, qui s'étend des PME aux grands comptes, couvre les besoins de vastes environnements campus, d'entreprises distribuées, de segments tels que les services publics, le commerce de détail ou la santé, ainsi que des fournisseurs de services.

Dell SonicWALL a reçu les éloges de publications industrielles telles que Network World, InfoWorld, PC Magazine et SC Magazine pour la convivialité, la qualité et les excellentes performances de ses appliances et services. Gartner a placé Dell SonicWALL parmi les visionnaires de son Carré magique 2011 consacré aux VPN SSL et, plus récemment, parmi les leaders de son Carré magique 2013 dédié à la gestion unifiée des menaces (UTM). Selon le Security Value Map™ 2013 de NSS Labs sur les pare-feu nouvelle génération, l'appliance SuperMassive E10800 de Dell SonicWALL équipée de SonicOS a obtenu la mention « Recommandé » pour la deuxième année consécutive. L'architecture éprouvée du système d'exploitation SonicOS est au cœur de tous les pare-feu Dell SonicWALL.

Dell SonicWALL propose une gamme complète de solutions leaders dans les domaines de la sécurité réseau : pare-feu, accès distant sécurisé/VPN SSL, anti-spam/sécurisation de messagerie, auxquels s'ajoutent des services de gestion et de reporting centralisés ainsi que de support technique 24x7.

Fondée en 1991, SonicWALL a été rachetée par Dell en 2012.

\* Brevets U.S. n° 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723



**Pour plus d'informations, contactez :**

Dell SonicWALL  
2001 Logic Drive  
San Jose, CA 95124

[www.sonicwall.com](http://www.sonicwall.com)

T +1 408.745.9600

F +1 408.745.9300

---

**Dell Software**

5 Polaris Way, Aliso Viejo, CA 92656 | [www.dell.com](http://www.dell.com)  
Si vous êtes situé en dehors de l'Amérique du Nord, vous  
trouverez les coordonnées des bureaux locaux sur notre site  
Internet.

DellSW 546-09/13

© 2013 Dell Inc. TOUS DROITS RÉSERVÉS. Dell, Dell, Dell Software ainsi que le logo et les produits de Dell Software, tels qu'identifiés dans ce document, sont des marques déposées de Dell Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales et déposées sont la propriété de leurs sociétés respectives.

