

Pare-feux SonicWALL TZ Series

Une sécurité exceptionnelle et des performances de pointe à un coût total de possession extrêmement bas

Les pare-feux nouvelle génération Dell SonicWALL TZ Series constituent la solution idéale pour les entreprises à la recherche d'une protection réseau haut de gamme.

Les pare-feux SonicWALL TZ Series offrent une protection contre une large gamme de risques. Leurs services de sécurité avancés, intégrés ou basés sur le cloud, incluent la protection contre les logiciels malveillants et les logiciels espions, un système de prévention des intrusions (IPS), le contrôle des applications et le filtrage d'URL. Face aux attaques chiffrées qui apparaissent, les pare-feux SonicWALL TZ Series possèdent la puissance de traitement requise pour inspecter les connexions SSL chiffrées et détecter les menaces les plus récentes. Associés aux commutateurs Dell X Series, les pare-feux TZ Series peuvent directement gérer la sécurité de ces ports supplémentaires.

Couverts par le réseau Dell SonicWALL Global Response Intelligent Defense (GRID), les pare-feux SonicWALL TZ Series fournissent des mises à jour continues pour maintenir une protection réseau efficace contre les cybercriminels. Les pare-feux SonicWALL TZ Series sont capables d'analyser chaque octet de chaque paquet sur tous les ports et protocoles avec une latence proche de zéro et aucune restriction quant à la taille des fichiers.

Les pare-feux SonicWALL TZ Series incluent ports Gigabit Ethernet, connectivité sans fil 802.11ac intégrée en option*, réseau VPN IPSec et SSL, basculement via prise en charge 3G/4G intégrée, équilibrage de charge et segmentation du réseau. Les pare-feux UTM SonicWALL TZ Series offrent

également un accès mobile rapide et sécurisé sur les plateformes Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS et Linux.

Le système Dell SonicWALL GMS (Global Management System) permet de centraliser le déploiement et la gestion des pare-feux SonicWALL TZ Series, à partir d'un seul système.

Sécurité gérée pour les environnements distribués

Les écoles, points de vente au détail, sites distants, succursales et entreprises distribuées ont besoin d'une solution qui s'intègre avec leur pare-feu. Les pare-feux SonicWALL TZ Series partagent la même base de code et la même protection que nos pare-feux nouvelle génération SuperMassive. Cela simplifie la gestion des sites distants, car tous les administrateurs voient la même interface utilisateur. Le système GMS permet aux administrateurs réseau de configurer, surveiller et gérer des pare-feux SonicWALL distants à partir d'un seul écran. Si l'on ajoute à cela le haut débit et la connectivité sans fil sécurisée, les pare-feux SonicWALL TZ Series étendent le périmètre de protection aux clients et invités des points de vente au détail ou des bureaux distants.



Avantages :

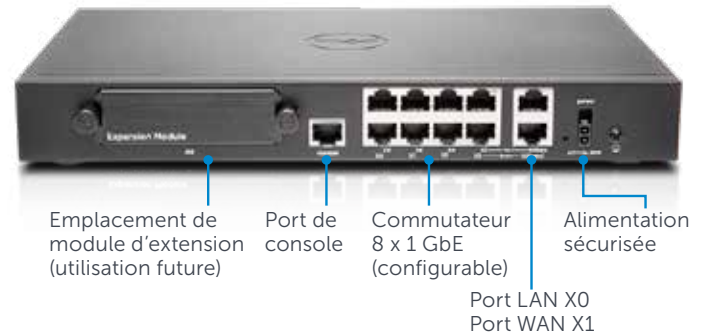
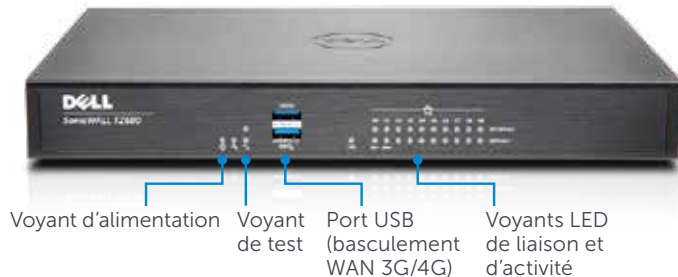
- Protection réseau haut de gamme
- Inspection approfondie des paquets pour l'ensemble du trafic sans limites de taille de fichiers ou de protocole
- Connectivité sans fil 802.11ac sécurisée à l'aide d'un contrôleur sans fil intégré ou via des points d'accès sans fil Dell SonicPoint externes
- Accès mobile VPN SSL pour appareils Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS et Linux
- Plus de 100 ports supplémentaires peuvent être gérés en toute sécurité par la console TZ lorsqu'ils sont déployés en association avec les commutateurs Dell X Series.

* 802.11ac non disponible actuellement sur les modèles SOHO (ces modèles prennent en charge la connectivité 802.11a/b/g/n)

SonicWALL TZ600 Series

Le pare-feu nouvelle génération Dell SonicWALL TZ600 a été conçu pour les entreprises naissantes, les points de vente au détail et les succursales qui recherchent une solution de sécurité offrant un excellent rapport performances/prix. Il sécurise les réseaux avec des fonctionnalités de niveau professionnel et des performances sans compromis.

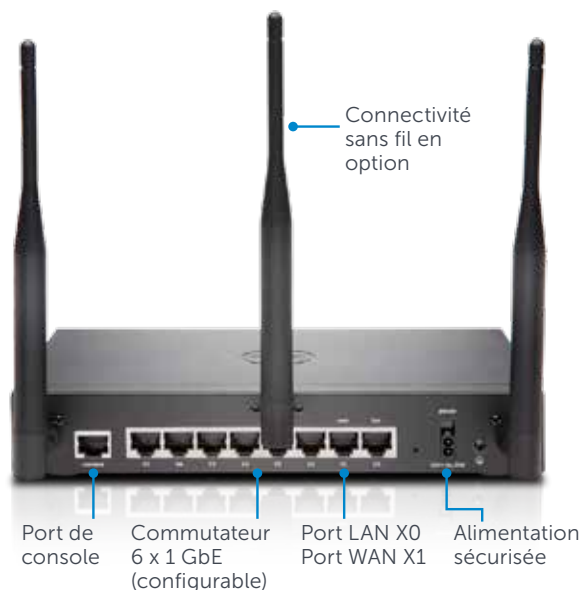
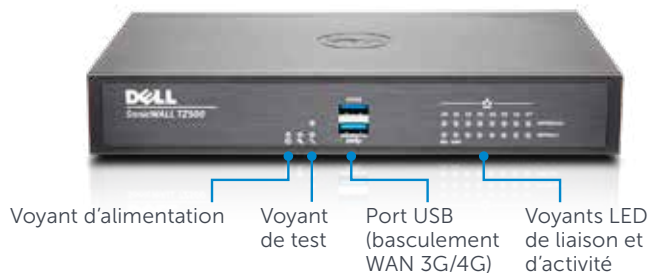
Caractéristiques	TZ600 Series
Débit du pare-feu	1,5 Gbit/s
Débit DPI complet	500 Mbit/s
Débit d'inspection des logiciels malveillants	500 Mbit/s
Débit IPS	1,1 Gbit/s
Débit IMIX	900 Mbit/s
Connexions DPI max.	125 000
Nouvelles connexions/s	12 000



SonicWALL TZ500 Series

Conçu pour les succursales et les PME en pleine croissance, le pare-feu Dell SonicWALL TZ500 Series associe une protection extrêmement efficace et sans compromis avec une productivité réseau et une connectivité sans fil double bande 802.11ac intégrée en option.

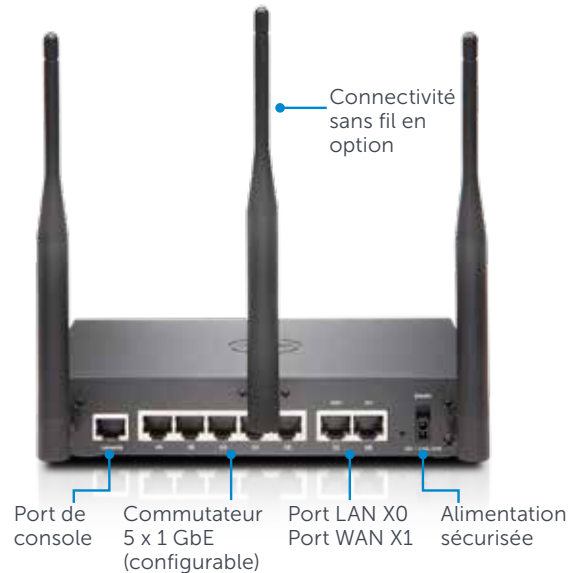
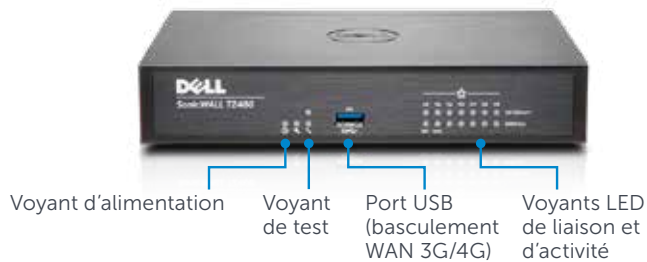
Caractéristiques	TZ500 Series
Débit du pare-feu	1,4 Gbit/s
Débit DPI complet	400 Mbit/s
Débit d'inspection des logiciels malveillants	400 Mbit/s
Débit IPS	1 Gbit/s
Débit IMIX	700 Mbit/s
Connexions DPI max.	100 000
Nouvelles connexions/s	8 000



SonicWALL TZ400 Series

Conçu pour les petites entreprises, les points de vente au détail et les succursales, le pare-feu Dell SonicWALL TZ400 assure une protection de niveau professionnel. Des options flexibles de déploiement sans fil sont disponibles avec des points d'accès SonicPoint externes ou la connectivité sans fil 802.11ac intégrée dans l'unité.

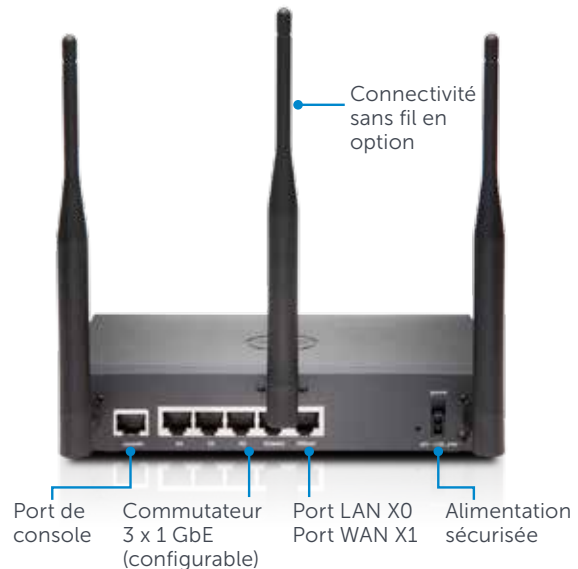
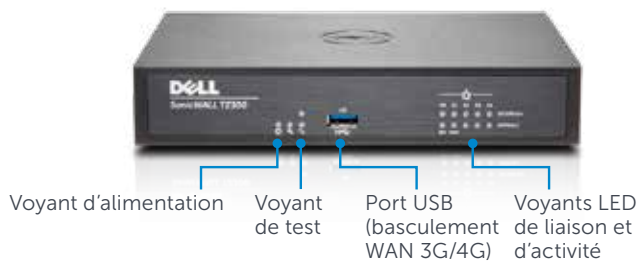
Caractéristiques	TZ400 Series
Débit du pare-feu	1,3 Gbit/s
Débit DPI complet	300 Mbit/s
Débit d'inspection des logiciels malveillants	300 Mbit/s
Débit IPS	900 Mbit/s
Débit IMIX	500 Mbit/s
Connexions DPI max.	90 000
Nouvelles connexions/s	6 000



SonicWALL TZ300 Series

Le pare-feu Dell SonicWALL TZ300 offre une solution tout-en-un qui protège les réseaux contre les attaques. Contrairement aux produits grand public, le pare-feu SonicWALL TZ300 Series associe des fonctionnalités de prévention des intrusions, de protection contre les logiciels malveillants et de filtrage de contenu/d'URL avec une connectivité sans fil intégrée 802.11ac en option et la prise en charge la plus large des plateformes mobiles sécurisées pour les ordinateurs portables, les smartphones et les tablettes.

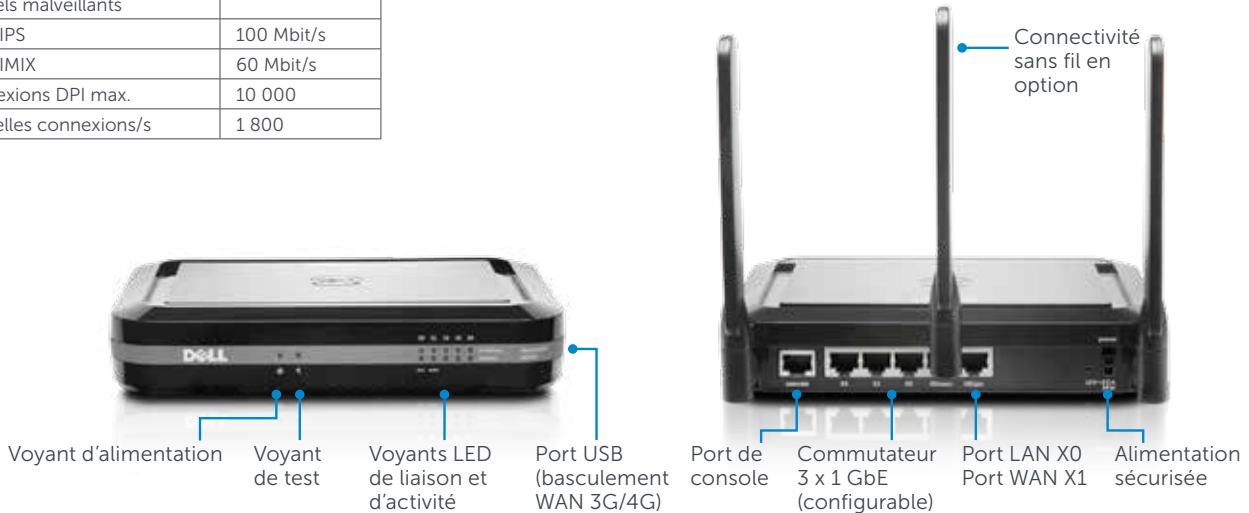
Caractéristiques	TZ300 Series
Débit du pare-feu	750 Mbit/s
Débit DPI complet	100 Mbit/s
Débit d'inspection des logiciels malveillants	100 Mbit/s
Débit IPS	300 Mbit/s
Débit IMIX	200 Mbit/s
Connexions DPI max.	50 000
Nouvelles connexions/s	5 000



SonicWALL SOHO Series

Conçu pour les environnements filaires et sans fil de petits bureaux et de bureaux à domicile, le pare-feu Dell SonicWALL SOHO Series offre la protection de niveau professionnel qu'exigent les grandes entreprises à un tarif plus avantageux.

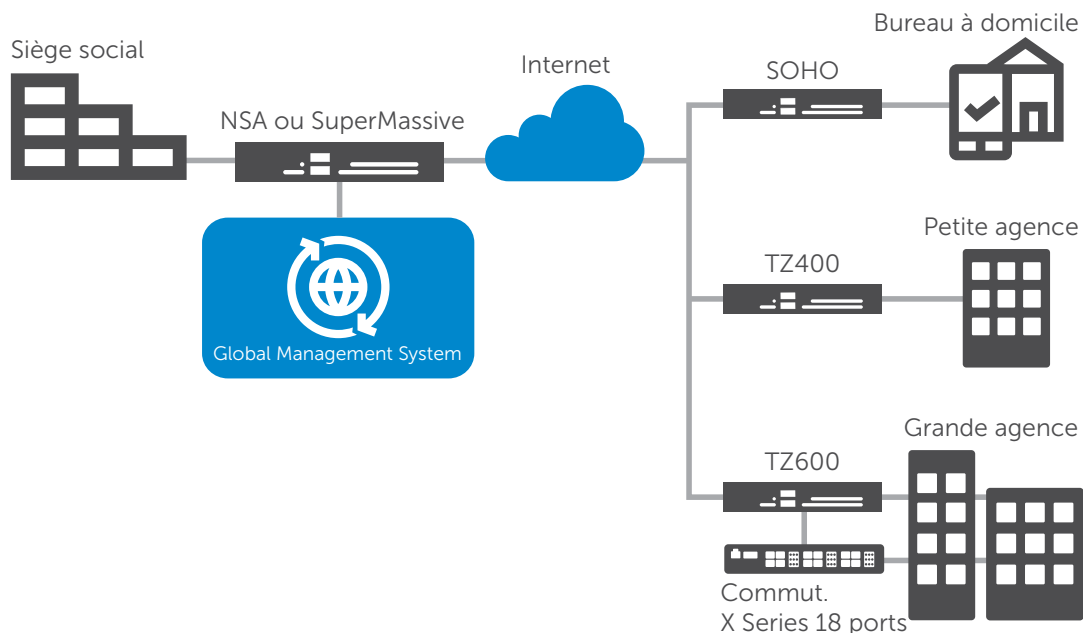
Caractéristiques	SOHO Series
Débit du pare-feu	300 Mbit/s
Débit DPI complet	50 Mbit/s
Débit d'inspection des logiciels malveillants	50 Mbit/s
Débit IPS	100 Mbit/s
Débit IMIX	60 Mbit/s
Connexions DPI max.	10 000
Nouvelles connexions/s	1 800



Architecture évolutive pour des performances et une extensibilité extrêmes

Dès la conception du moteur RFDPI (Reassembly-Free Deep Packet Inspection), l'accent a été mis sur une analyse de sécurité haute performance, afin de couvrir la nature fondamentalement parallèle et en constante augmentation du trafic réseau. Associée à des systèmes dotés de processeurs multicœurs, cette architecture logicielle centrée sur le parallélisme est facilement extensible pour s'adapter aux demandes d'inspection approfondie des paquets (DPI,

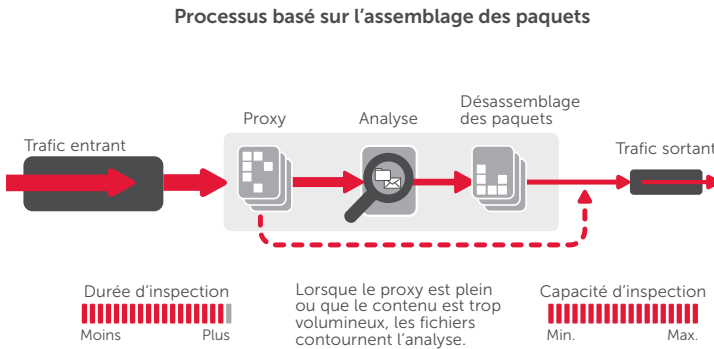
Deep Packet Inspection) lorsque les charges de trafic sont élevées. La plateforme SonicWALL TZ Series repose sur des processeurs qui, contrairement aux systèmes x86, sont optimisés pour le traitement des paquets, du chiffrement et du réseau tout offrant flexibilité et programmabilité sur le terrain, un point faible des systèmes ASIC. Cette flexibilité est essentielle lorsque de nouvelles mises à jour de code et de comportement sont nécessaires pour lutter contre les nouvelles attaques exigeant des techniques de détection actualisées et plus sophistiquées.



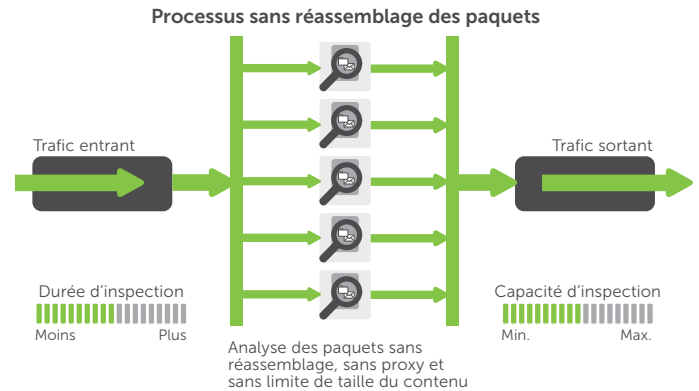
Moteur RFDPI (Reassembly-Free Deep Packet Inspection)

Le moteur RFDPI offre un contrôle des applications et une protection contre les menaces hors pair, sans compromettre les performances. Ce moteur breveté inspecte le flux du trafic pour détecter les menaces au niveau des couches 3 à 7. Il soumet les flux réseau à des opérations répétées et étendues de normalisation et de déchiffrement afin de neutraliser les techniques d'évasion évoluées visant à tromper les moteurs de détection pour introduire du code malveillant sur le réseau. Une fois son prétraitement (déchiffrement SSL compris) terminé, chaque paquet est analysé par rapport à une mémoire propriétaire unique rassemblant trois bases de

données de signatures : attaques par intrusion, logiciels malveillants et applications. L'état de la connexion affiche la position des flux par rapport à ces bases de données jusqu'à identifier un état d'attaque ou tout autre événement pertinent, ce qui déclenche une action prédéfinie. Lorsqu'un logiciel malveillant est identifié, le pare-feu SonicWALL rompt la connexion avant qu'une infiltration puisse se produire et journalise correctement l'événement. Le moteur est également configurable pour l'inspection seulement ou, dans le cadre de la détection d'applications, pour fournir des services de gestion de la bande passante de couche 7 au reste du flux applicatif une fois l'application identifiée.



Architecture concurrente

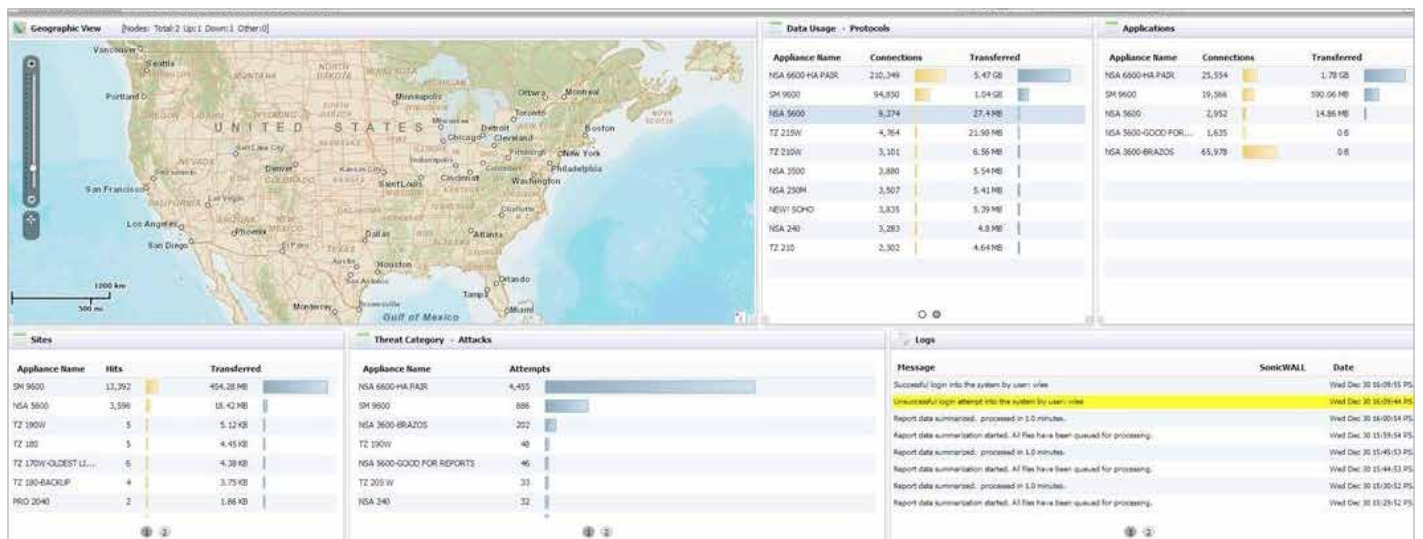


Architecture Dell SonicWALL

Système de gestion et création de rapports

Conçue pour les grands déploiements dans des entreprises distribuées, la solution Dell SonicWALL GMS (Global Management System) offre aux administrateurs une plateforme de gestion unifiée, sécurisée et extensible pour les appliances de sécurité Dell SonicWALL et les commutateurs X Series. La solution GSM permet aux entreprises de consolider aisément la gestion des appliances de sécurité, de réduire les complexités administratives et de dépannage et de contrôler tous les aspects opérationnels de l'infrastructure de sécurité, notamment la centralisation de la gestion et de l'application

des stratégies, la surveillance des événements en temps réel, l'analyse et la création de rapports, et plus encore. La solution GMS répond également aux besoins des entreprises en matière de gestion des modifications de pare-feu via une fonctionnalité d'automatisation des flux de travail. Au lieu d'adopter une approche au cas par cas, la solution GMS optimise la gestion de la sécurité réseau via des processus métiers et des niveaux de service qui simplifient considérablement la gestion du cycle de vie des environnements de sécurité globaux.



Sécurité et protection

Notre équipe Dell SonicWALL dédiée à la recherche des menaces met au point des contre-mesures qui seront déployées sur les pare-feux actifs pour une protection actualisée. L'équipe utilise plus d'un million de détecteurs dans le monde entier pour obtenir des échantillons de logiciels malveillants et des informations télémétriques sur les dernières menaces, qui à leur tour alimentent les fonctions de prévention des intrusions et de détection des applications et logiciels malveillants. Les clients des pare-feux Dell SonicWALL ayant des abonnements actifs bénéficient d'une protection actualisée en continu contre les menaces. Les nouvelles mises à jour prennent effet instantanément, sans redémarrage ni interruption. Les signatures sur les appliances offrent une protection contre un grand nombre d'attaques. Chaque signature peut couvrir jusqu'à plusieurs dizaines de milliers de menaces. Outre les contre-mesures déployées sur l'appliance, les pare-feux Dell SonicWALL ont également accès au service Dell SonicWALL CloudAV, qui complète la base de données intégrée de signatures avec plus de 17 millions de signatures, un chiffre en constante expansion. Le pare-feu accède à cette base de données CloudAV via un protocole léger propriétaire pour optimiser l'inspection réalisée sur l'appliance. Avec les fonctionnalités Geo-IP et de filtrage des réseaux de zombies, les pare-feux nouvelle génération Dell SonicWALL sont capables de bloquer le trafic provenant de domaines dangereux ou de zones géographiques entières afin de réduire le profil de risque du réseau.

Surveillance et contrôle des applications

La surveillance des applications renseigne les administrateurs sur le trafic applicatif circulant sur le réseau. Ils peuvent ainsi planifier le contrôle des applications en fonction des priorités de l'entreprise, limiter les applications non productives et bloquer les applications potentiellement dangereuses. La visualisation en temps réel identifie les anomalies du trafic dès qu'elles surviennent, permettant de prendre des contre-mesures immédiates contre les attaques entrantes ou sortantes potentielles ou les goulets d'étranglement des performances. L'analyse Dell SonicWALL fournit des informations granulaires sur le trafic applicatif, l'utilisation de la bande passante et les menaces de sécurité, ainsi

* 802.11ac non disponible actuellement sur les modèles SOHO (ces modèles prennent en charge la connectivité 802.11a/b/g/n)

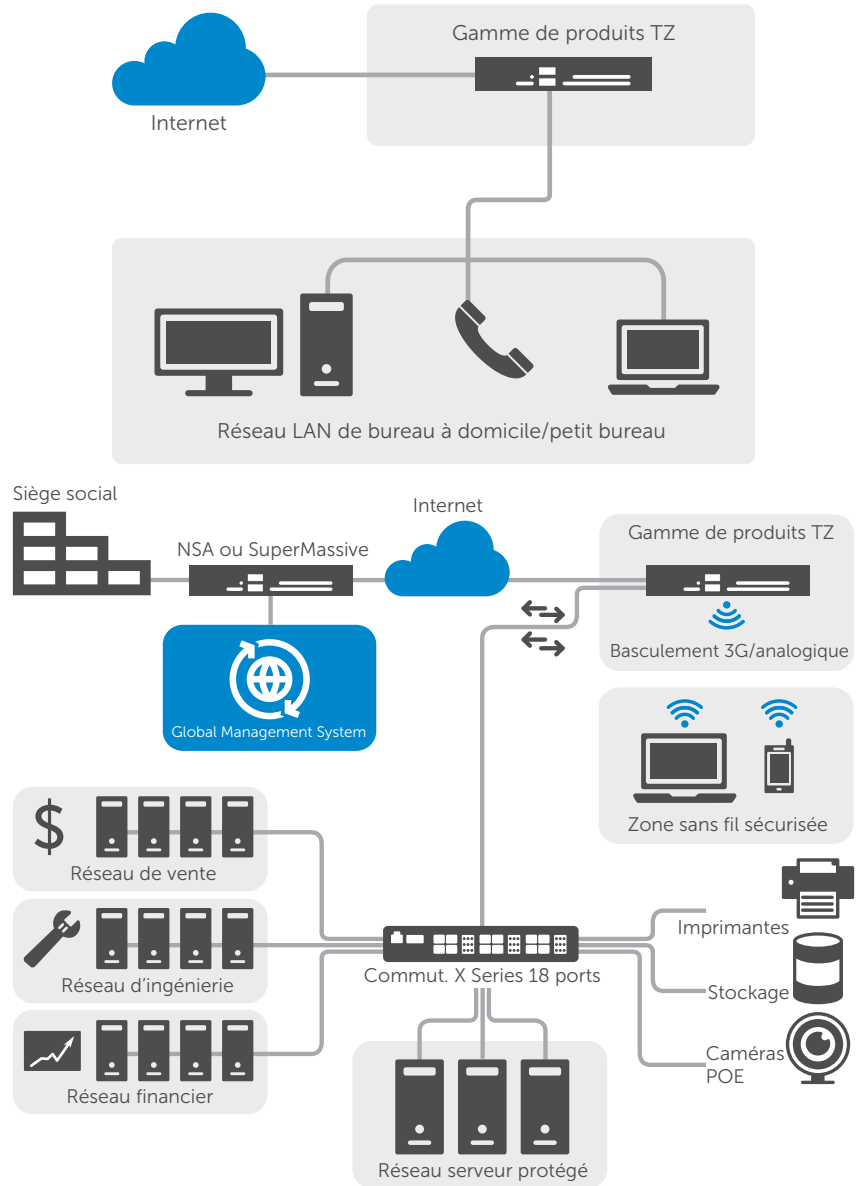
que de puissantes fonctionnalités de dépannage et d'analyse forensique. En outre, les fonctions d'authentification unique (SSO, Single Sign-On) améliorent l'expérience utilisateur, augmentent la productivité et réduisent les appels passés à l'équipe de support. La gestion de la surveillance et du contrôle des applications est facilitée par l'utilisation d'une interface Web intuitive.

Connectivité sans fil flexible et sécurisée

Disponible en option, la connectivité sans fil 802.11ac haut débit* associée à la technologie de pare-feu nouvelle

génération Dell SonicWALL constitue une solution de sécurité réseau sans fil offrant une protection complète pour les réseaux filaires et sans fil.

Ces performances sans fil de niveau professionnel permettent aux appareils compatibles WiFi de se connecter sur de plus grandes distances et d'utiliser des applications mobiles exigeantes en termes de bande passante (applications vidéo et vocales, par exemple), dans des environnements à plus forte densité sans subir de dégradation du signal.



Fonctionnalités

Moteur RFDPI	
Fonctionnalités	Description
Reassembly-Free Deep Packet Inspection	Ce moteur d'inspection hautes performances, propriétaire et breveté effectue des analyses bidirectionnelles des flux de trafic, sans proxy ni mise en mémoire tampon, pour détecter les tentatives d'intrusion, les logiciels malveillants et le trafic des applications indépendamment du port.
Inspection bidirectionnelle	Le trafic entrant et sortant est analysé simultanément pour garantir que le réseau n'est pas utilisé pour distribuer des logiciels malveillants ou lancer des attaques en cas d'intrusion d'une machine infectée.
Inspection en un seul passage	L'architecture DPI en un seul passage analyse simultanément le trafic pour identifier les logiciels malveillants, les intrusions et les applications, ce qui réduit considérablement la latence DPI et garantit que toutes les informations sur les menaces sont corrélées au sein d'une architecture unique.
Inspection basée sur les flux	Cette technologie d'inspection sans proxy et sans mise en mémoire tampon offre des performances à ultrafaible latence pour l'inspection DPI de flux réseau simultanés, sans limites de taille des flux et des fichiers. Elle peut en outre être appliquée à des protocoles courants, ainsi qu'aux flux TCP bruts.
Prévention des intrusions	
Fonctionnalités	Description
Protection basée sur des contre-mesures	Le système de prévention des intrusions (IPS, Intrusion Prevention System) étroitement intégré exploite les signatures et autres contre-mesures pour détecter les vulnérabilités et les attaques, dont il couvre une large palette, au sein de la charge utile.
Mise à jour automatique des signatures	L'équipe de recherche des menaces Dell SonicWALL recherche et déploie en continu des mises à jour pour une longue liste de contre-mesures IPS couvrant plus de 50 catégories d'attaque. Les nouvelles mises à jour prennent effet immédiatement, sans redémarrage ni interruption de service.
Protection IPS intrazone	Renforce la sécurité interne en segmentant le réseau en plusieurs zones de sécurité avec prévention des intrusions, empêchant les menaces de se propager entre ces zones.
Détection et blocage de la commande et du contrôle (CnC, Command and Control) des réseaux de zombies	Identifie et bloque le trafic CnC provenant de robots sur le réseau local vers des IP et des domaines identifiés comme propageant des logiciels malveillants ou comme des points CnC connus.
Anomalies/abus de protocole	Identifie et bloque les attaques exploitant les protocoles dans le but de contourner le système IPS.
Protection de type « zero-day »	Protège le réseau contre les attaques de type « zero-day » avec des mises à jour constantes répondant aux dernières méthodes et techniques d'attaque et couvrant des milliers de failles.
Technologie anti-évasion	La normalisation intensive des flux, le décodage et d'autres techniques empêchent les menaces d'entrer sur le réseau sans se faire détecter via des techniques d'évasion sur les couches 2 à 7.
Détection des menaces	
Fonctionnalités	Description
Anti-logiciels malveillants de passerelle	Le moteur RFDPI analyse l'intégralité du trafic entrant, sortant et intrazone pour détecter les virus, chevaux de Troie, enregistreurs de frappe et autres logiciels malveillants dans les fichiers, quelles que soient leur taille et leur longueur, sur tous les ports et les flux TCP.
Protection CloudAV contre les logiciels malveillants	Les serveurs Cloud Dell SonicWALL hébergent une base de données de plus de 17 millions de signatures de menaces mise à jour en continu. Cette dernière est utilisée pour augmenter les capacités de la base de données de signatures locale, offrant au moteur RFDPI une couverture étendue des menaces.
Mises à jour de sécurité en continu	Les nouvelles mises à jour sont automatiquement appliquées aux pare-feux sur le terrain avec des services de sécurité actifs et prennent effet immédiatement, sans redémarrage ni interruption.
Inspection et déchiffrement SSL	Déchiffre et inspecte le trafic SSL à la volée, sans proxy, pour détecter les logiciels malveillants, les intrusions et les fuites de données, et applique les stratégies de contrôle du contenu, des URL et des applications afin de contrer les menaces dissimulées au sein du trafic SSL chiffré. Inclus avec les abonnements de sécurité pour tous les modèles, à l'exception de SOHO. Vendu comme une licence séparée sur le modèle SOHO.
Inspection TCP brute bidirectionnelle	Le moteur RFDPI est capable d'analyser les flux TCP bruts sur tous les ports de manière bidirectionnelle, empêchant ainsi les attaques visant à contourner les systèmes de sécurité obsolètes qui sécurisent uniquement quelques ports connus.
Prise en charge étendue des protocoles	Identifie les protocoles courants (HTTP/S, FTP, SMTP, SMBv1/v2, etc.) qui n'envoient pas de données sous forme de flux TCP bruts, et décode les charges utiles, qu'elles soient ou non exécutées sur des ports standard connus, pour identifier les logiciels malveillants.
Surveillance et contrôle des applications	
Fonctionnalités	Description
Contrôle des applications	Compare les applications, ou les fonctionnalités des applications, identifiées par le moteur RFDPI à une base de données en constante expansion de plus de 3 500 signatures pour renforcer la sécurité et la productivité réseau.
Identification des applications personnalisées	Contrôle les applications personnalisées en créant des signatures basées sur leurs paramètres ou schémas spécifiques dans leurs communications réseau afin de mieux contrôler le réseau.
Gestion de la bande passante applicative	Alloue et régule la bande passante disponible de manière granulaire selon l'importance ou la catégorie des applications tout en limitant le trafic vers les applications non essentielles.
Contrôle granulaire	Contrôle les applications, ou des composants spécifiques d'une application, en fonction de calendriers, de groupes d'utilisateurs, de listes d'exclusion et de plusieurs actions en effectuant une identification SSO complète des utilisateurs via l'intégration LDAP/AD/services Terminal Server/Citrix.
Filtrage du contenu	
Fonctionnalités	Description
Filtrage du contenu interne/externe	Applique des stratégies d'utilisation acceptables et bloque l'accès aux sites Web contenant des informations ou des images répréhensibles ou non productives via le service de filtrage de contenu. Étend l'application des stratégies pour bloquer les contenus Internet des appareils situés hors du périmètre du pare-feu via le service client de filtrage de contenu.
Filtrage du contenu	

Fonctionnalités	Description
Contrôles granulaires	Bloque les contenus à l'aide de catégories prédéfinies ou d'associations de catégories. Le filtrage peut être planifié à certains moments de la journée, pendant les heures de bureau ou d'école par exemple, et appliqué à des groupes ou utilisateurs spécifiques.
YouTube pour les écoles	Permet aux enseignants de choisir parmi des centaines de milliers de vidéos éducatives gratuites YouTube EDU classées par sujet/niveau et conformes aux standards d'enseignement courants.
Mise en cache Web	Les évaluations d'URL sont mises en cache localement sur le pare-feu Dell SonicWALL pour accélérer l'accès ultérieur aux sites les plus fréquentés.
Application des antivirus et anti-logiciels espions	
Fonctionnalités	Description
Protection multicouche	Utilise les fonctionnalités du pare-feu comme première couche de défense au niveau du périmètre et les associe avec la protection des postes clients pour bloquer les virus qui entrent sur le réseau par le biais des ordinateurs portables, des clés USB ou d'autres systèmes non protégés.
Option d'application automatisée	S'assure que chaque ordinateur qui accède au réseau utilise la version la plus récente des signatures de virus et de logiciels espions, éliminant ainsi les coûts couramment liés à la gestion des logiciels antivirus et anti-logiciels espions installés sur les ordinateurs de bureau.
Option de déploiement et d'installation automatisés	Le déploiement et l'installation, ordinateur par ordinateur, des clients antivirus et anti-logiciels espions sont automatiques sur le réseau, ce qui limite la charge d'administration.
Protection antivirus automatique continue	Des mises à jour fréquentes des logiciels antivirus et anti-logiciels espions sont appliquées de manière transparente à tous les ordinateurs de bureau et serveurs de fichiers pour améliorer la productivité des utilisateurs et alléger la gestion de la sécurité.
Protection contre les logiciels espions	Une protection puissante contre les logiciels espions analyse et bloque l'installation d'un large éventail de logiciels espions sur les ordinateurs portables et de bureau avant qu'ils ne transmettent des données confidentielles, renforçant ainsi les performances et la sécurité des postes de travail.
Pare-feu et gestion de réseau	
Fonctionnalités	Description
Inspection des paquets avec état	L'intégralité du trafic réseau est inspectée, analysée et mise en conformité avec les stratégies d'accès du pare-feu.
Protection contre les attaques DDoS/DoS	La protection contre les inondations SYN permet de contrer les attaques DOS à l'aide des technologies de liste noire SYN de couche 2 et de proxy SYN de couche 3. Elle permet également de se prémunir contre les attaques DOS/DDoS via la protection contre les inondations UDP/ICMP et la limitation du débit de connexion.
Options de déploiement flexibles	Les pare-feux SonicWALL TZ Series peuvent être déployés en mode NAT traditionnel, pont de couche 2, filaire et TAP réseau.
Prise en charge du protocole IPv6	Le protocole IPv6 (Internet Protocol version 6) commence à remplacer le protocole IPv4. Avec le dernier système d'exploitation SonicOS, le matériel prendra en charge les implémentations de filtrage.
Intégration des commutateurs Dell X Series	Gère les paramètres de sécurité des ports supplémentaires, notamment POE et POE+, depuis un seul et même écran, via le tableau de bord TZ Series avec commutateur Dell X Series (non disponible pour le modèle SOHO)
Haute disponibilité	Les modèles SonicWALL TZ500 et SonicWALL TZ600 prennent en charge la haute disponibilité et la configuration Active/Standby avec synchronisation d'état. Les modèles SonicWALL TZ300 et SonicWALL TZ400 prennent en charge la haute disponibilité et la configuration Active/Standby sans synchronisation. Les modèles SonicWALL SOHO n'offrent pas la haute disponibilité.
Sécurité du réseau sans fil	La technologie sans fil IEEE 802.11ac peut offrir un débit sans fil atteignant 1,3 Gbit/s avec une portée et une fiabilité supérieures. Disponible sur les modèles SonicWALL TZ600 à SonicWALL TZ300. La technologie 802.11 a/b/g/n en option est disponible sur les modèles SonicWALL SOHO.
Gestion et création de rapports	
Fonctionnalités	Description
Système de gestion global (Global Management System)	Dell SonicWALL GMS surveille, configure et établit des rapports sur diverses appliances Dell SonicWALL et commutateurs Dell X Series via une seule et même console de gestion dotée d'une interface intuitive, ce qui réduit les coûts et la complexité de la gestion.
Gestion puissante avec un seul appareil	L'interface Web intuitive permet une configuration rapide et pratique. Elle offre également une interface en ligne de commande complète et prend en charge le protocole SNMPv2/3.
Rapports sur les flux applicatifs IPFIX/NetFlow	Exporte des analyses du trafic applicatif et des données d'utilisation via les protocoles IPFIX ou NetFlow pour offrir une surveillance et des rapports historiques et en temps réel sur Dell SonicWALL Scrutinizer ou d'autres outils prenant en charge IPFIX et NetFlow via des extensions.
Réseau privé virtuel	
Fonctionnalités	Description
VPN IPSec pour la connectivité intersite	Le VPN IPSec hautes performances permet aux pare-feux SonicWALL TZ Series de servir de concentrateurs VPN pour des milliers d'autres bureaux à domicile, succursales ou sites de grande taille.
Accès client à distance IPSec ou VPN SSL	Utilise la technologie VPN SSL sans client ou un client IPSec facile à gérer pour fournir un accès simple aux courriers électroniques, fichiers, ordinateurs, sites intranet et applications depuis de nombreuses plateformes.
Passerelle VPN redondante	Si plusieurs réseaux WAN sont utilisés, un VPN principal et un WAN secondaire peuvent être configurés pour permettre un basculement automatique fluide et la restauration de toutes les sessions VPN.
VPN basé sur le routage	La possibilité d'effectuer un routage dynamique sur des liens VPN garantit une disponibilité continue en cas de panne temporaire d'un tunnel VPN via la redirection fluide du trafic entre les postes clients sur des routes alternatives.
Reconnaissance du contexte/contenu	
Fonctionnalités	Description
Suivi de l'activité des utilisateurs	L'activité et l'identification des utilisateurs sont disponibles via une intégration SSO AD/LDAP/Citrix1/Services Terminal Server fluide et des informations étendues obtenues via l'inspection DPI.
Identification du trafic par pays GeoIP	Identifie et contrôle le trafic réseau en direction ou provenant de pays spécifiques pour contrer les attaques liées à une activité d'origine suspecte ou connue ou pour faire des recherches sur le trafic suspect provenant du réseau.
Filtrage DPI des expressions régulières	Empêche les fuites de données en identifiant et en contrôlant les contenus qui transitent sur le réseau via l'identification des expressions régulières.

Résumé des fonctionnalités SonicOS

Pare-feu

- Reassembly-Free Deep Packet Inspection
- Inspection approfondie des paquets pour SSL
- Inspection des paquets avec état
- Mode furtif
- Prise en charge Common Access Card (CAC)
- Protection contre les attaques DOS
- Protection contre les attaques par saturation UDP/ICMP/SYN
- Déchiffrement SSL
- Sécurité IPv6

Prévention des intrusions

- Analyse basée sur des signatures
- Mise à jour automatique des signatures
- Moteur d'inspection bidirectionnelle
- Fonctionnalité de règles IPS granulaires
- Filtrage GeolP et basé sur la réputation
- Détection des expressions régulières

Logiciel de protection contre les programmes malveillants

- Analyse des logiciels malveillants basée sur les flux
- Antivirus de passerelle
- Anti-logiciels espions de passerelle
- Inspection bidirectionnelle
- Pas de limitation de la taille des fichiers
- Base de données Cloud de logiciels malveillants

Contrôle des applications

- Contrôle des applications
- Blocage des composants applicatifs
- Gestion de la bande passante applicative
- Création de signatures d'applications personnalisées
- Prévention des fuites de données
- Création de rapports sur les applications via NetFlow/IPFIX
- Suivi de l'activité des utilisateurs (SSO)

- Base de données complète des signatures d'applications

Filtrage du contenu Web

- Filtrage des URL
- Technologie anti-proxy
- Blocage par mot-clé
- Catégories d'évaluation CFS pour la gestion de la bande passante
- Modèle de stratégie unifié avec contrôle des applications
- 57 catégories de filtrage du contenu
- Service client de filtrage de contenu

Réseau privé virtuel

- VPN IPSec pour la connectivité intersite
- Accès client à distance IPSec et VPN SSL
- Passerelle VPN redondante
- Mobile Connect pour iOS et Android™
- VPN basé sur le routage (OSPF, RIP)

Gestion de réseau

- PortShield
- Découverte réseau de couche 2
- IPv6
- Journalisation améliorée
- Mise en miroir des ports
- Qualité de service de couche 2
- Sécurité des ports
- Routage dynamique
- Routage basé sur des stratégies
- Routage asymétrique
- Serveur DHCP
- Gestion de la bande passante
- Haute disponibilité Active/Standby avec synchronisation d'état*
- Équilibrage de la charge entrante/sortante
- DDNS mode pont de couche 2, mode NAT
- Basculement WAN 3G/4G

VoIP

- Contrôle QoS granulaire
- Gestion de la bande passante

- DPI du trafic VoIP
- Prise en charge des proxys SIP et des contrôleurs d'accès H.323

Gestion et surveillance

- Interface utilisateur graphique Web
- Interface en ligne de commande
- SNMPv2/v3
- Création de rapports hors pare-feu (Scrutinizer)
- Gestion centralisée et génération de rapports
- Journalisation
- Exportation NetFlow/IPFix
- Visualisation du trafic applicatif (non disponible sur le modèle SOHO)
- Gestion centralisée des stratégies
- Authentification unique (SSO)
- Prise en charge des services Terminal Server/Citrix
- Visualisation de bande passante et d'applications
- Gestion IPv4 et IPv6

IPv6

- Filtrage IPv6
- 6rd (déploiement rapide)
- Délégation de préfixe DHCP
- Protocole BGP

Connectivité sans fil

- Double bande (2,4 GHz et 5 GHz)
- Normes connectivité sans fil 802.11 a/b/g/n/ac**
- Détection et prévention sans fil des intrusions
- Services sans fil pour les invités
- Messagerie légère à point d'accès
- Segmentation des points d'accès virtuels
- Portail captif
- Cloud ACL

* Haute disponibilité avec synchronisation d'état uniquement disponible sur les modèles SonicWALL TZ500 et SonicWALL TZ600

** 802.11ac non disponible sur le modèle SOHO



Caractéristiques des pare-feux SonicWALL TZ Series

Performances	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600 Series
Système d'exploitation	SonicOS 5.9x/6.2.x	SonicOS 6.2.x			
Processeur de sécurité	2 x 400 MHz / 2 x 800 MHz	2 x 800 MHz	4 x 800 MHz	4 x 1 GHz	4 x 1,4 GHz
Mémoire (RAM)	512 Mo/1 Go	1 Go	1 Go	1 Go	1 Go
Mémoire (Flash)	32 Mo/64 Mo	64 Mo	64 Mo	64 Mo	64 Mo
Interfaces cuivre 1 GbE	5	5	7	8	10
Extension	USB	USB	USB	2 ports USB	Connecteur d'extension (à l'arrière)*, 2 ports USB
Débit d'inspection du pare-feu ¹	300 Mbit/s	750 Mbit/s	1 300 Mbit/s	1 400 Mbit/s	1 500 Mbit/s
Débit DPI complet ²	50 Mbit/s	100 Mbit/s	300 Mbit/s	400 Mbit/s	500 Mbit/s
Débit d'inspection des applications ²	-	300 Mbit/s	900 Mbit/s	1 000 Mbit/s	1 100 Mbit/s
Débit IPS ²	100 Mbit/s	300 Mbit/s	900 Mbit/s	1 000 Mbit/s	1 100 Mbit/s
Débit d'inspection des logiciels malveillants ²	50 Mbit/s	100 Mbit/s	300 Mbit/s	400 Mbit/s	500 Mbit/s
Débit IMIX ³	60 Mbit/s	200 Mbit/s	500 Mbit/s	700 Mbit/s	900 Mbit/s
Débit d'inspection et de déchiffrement SSL (SSL DPI) ²	15 Mbit/s	45 Mbit/s	100 Mbit/s	150 Mbit/s	200 Mbit/s
Débit VPN IPSec ³	100 Mbit/s	300 Mbit/s	900 Mbit/s	1 000 Mbit/s	1 100 Mbit/s
Connexions par seconde	1 800	5 000	6 000	8 000	12 000
Connexions maximales (SPI)	10 000	50 000	100 000	125 000	150 000
Connexions maximales (DPI)	10 000	50 000	90 000	100 000	125 000
Utilisateurs de l'authentification unique (SSO, Single Sign-On)	250	500	500	500	500
Interfaces de réseau VLAN	25	25	50	50	50
Points d'accès SonicPoint pris en charge (maximum)	2	8	16	16	24
Prise en charge des modèles Dell X Series	Non disponible	X1008/P, X1018/P, X1026/P, X1052/P, X4012			
Réseau privé virtuel (VPN)	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600 Series
Tunnels VPN de site à site	10	10	20	25	50
Clients VPN IPSec (maximum)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
Licences VPN SSL (maximum)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Virtual Assist groupé (maximum)	-	1 (version d'essai de 30 jours)	1 (version d'essai de 30 jours)	1 (version d'essai de 30 jours)	1 (version d'essai de 30 jours)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B Cryptography				
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14				
VPN basé sur le routage	RIP, OSPF				
Prise en charge des certificats	Autorité de certification Microsoft, Verisign, Thawte, Cybertrust, RSA Keon et Entrust pour le VPN Dell SonicWALL vers Dell SonicWALL, SCEP				
Fonctionnalités VPN	Dead Peer Detection, DHCP sur VPN, traversée du NAT IPSec, passerelle VPN redondante, VPN basé sur le routage				
Plateformes clientes VPN globales prises en charge	Microsoft® Windows Vista 32/64 bits, Windows 7 32/64 bits, Windows 8.0 32/64 bits, Windows 8.1 32/64 bits				
NetExtender	Microsoft Windows Vista 32/64 bits, Windows 7, Windows 8.0 32/64 bits, Windows 8.1 32/64 bits, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Windows 8.1 (intégré)				
Services de sécurité	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600 Series
Services d'inspection approfondie des paquets	Antivirus de passerelle, anti-logiciels espions, prévention des intrusions, SSL DPI				
Service de filtrage de contenu (CFS)	Analyse des URL HTTP, des IP HTTPS, du contenu et des mots-clés, filtrage complet basé sur le type de fichiers tel que ActiveX, Java, cookies de confidentialité, listes vertes/noires				
Antivirus et anti-logiciels espions client appliqués	McAfee®				
Service antispam complet	Pris en charge				
Virtualisation des applications	Non	Oui	Oui	Oui	Oui
Contrôle des applications	Oui	Oui	Oui	Oui	Oui

Caractéristiques des pare-feux SonicWALL TZ Series suite

Gestion de réseau	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600 Series
Attribution d'adresse IP	Statique, (DHCP, PPPoE, L2TP et client PPTP), serveur DHCP interne, relais DHCP				
Modes NAT	1 à 1, 1 à plusieurs, plusieurs à 1, NAT flexible (adresses IP superposées), PAT, mode transparent				
Protocoles de routage ⁴	BGP ⁴ , OSPF, RIPv1/v2, routes statiques, routage basé sur des règles, multidiffusion				
Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1e (WMM)				
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix			
Base de données utilisateur locale	150			250	
VoIP	H.323v1-5 complet, SIP				
Normes	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certifications	VPNC, IPv6 (Phase 2), pare-feu réseau ICESA, anti-virus ICESA				
Certifications en attente	Critères communs NDPP, FIPS 140-2 (avec Suite B) Level 2, UC APL				
Carte CAC (Common Access Card)	Prise en charge				
Haute disponibilité	Non	Active/Standby	Active/Standby	Active/Standby avec synchronisation d'état	Active/Standby avec synchronisation d'état
Matériel	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600 Series
Format	Bureau				
Bloc d'alimentation (W)	24 W externe	24 W externe	24 W externe	36 W externe	60 W externe
Consommation électrique maximale (W)	6,4/11,3	6,9/12	9,2/13,8	13,4/17,7	16,1
Puissance en entrée	100 à 240 V CA, 50-60 Hz, 1 A				
Dissipation thermique totale	21,8/38,7 BTU	23,5/40,9 BTU	31,3/47,1 BTU	45,9/60,5 BTU	55,1 BTU
Dimensions	3,6 x 14,1 x 19 cm	3,5 x 13,4 x 19 cm	3,5 x 13,4 x 19 cm	3,5 x 15 x 22,5 cm	3,5 x 18 x 28 cm
Poids	0,34 kg/0,75 livre 0,48 kg/1,06 livre	0,73 kg/1,61 livre 0,84 kg/1,85 livre	0,73 kg/1,61 livre 0,84 kg/1,85 livre	0,92 kg/2,03 livres 1,05 kg/2,31 livres	1,47 kg/3,24 livres
Poids DEEE	0,80 kg/1,76 livre 0,94 kg/2,07 livres	1,15 kg/2,53 livres 1,26 kg/2,78 livres	1,15 kg/2,53 livres 1,26 kg/2,78 livres	1,34 kg/2,95 livres 1,48 kg/3,26 livres	1,89 kg/4,16 livres
Poids d'expédition	1,20 kg/2,64 livres 1,34 kg/2,95 livres	1,37 kg/3,02 livres 1,48 kg/3,26 livres	1,37 kg/3,02 livres 1,48 kg/3,26 livres	1,93 kg/4,25 livres 2,07 kg/4,56 livres	2,48 kg/5,47 livres
Temps de fonctionnement entre deux pannes (en années)	30/15	28/14	27/13	20/12	18
Environnement	40 à 105°F, 0 à 40°C				
Taux d'humidité	5 à 95 % sans condensation				
Réglementation	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600 Series
Modèle de réglementation (modèles filaires)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Conformité aux réglementations majeures (modèles filaires)	BFCC classe B, ICES classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI classe B, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH, KCC/MSIP	BFCC classe B, ICES classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI classe B, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH, KCC/MSIP	BFCC classe B, ICES classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI classe B, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH, KCC/MSIP	BFCC classe B, ICES classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI classe B, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH, BSMI, KCC/MSIP	FCC classe A, ICES classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI classe A, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH, KCC/MSIP
Modèle de réglementation (modèles sans fil)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Conformité aux réglementations majeures (modèles sans fil)	FCC classe B, FCC RF ICES classe B, IC RF CE (EMC, LVD, RoHS), RCM, VCCI classe B, MIC/TELEC, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH	FCC classe B, FCC RF ICES classe B, IC RF CE (EMC, LVD, RoHS), RCM, VCCI classe B, MIC/TELEC, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH	FCC classe B, FCC RF ICES classe B, IC RF CE (EMC, LVD, RoHS), RCM, VCCI classe B, MIC/TELEC, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH	FCC classe B, FCC RF ICES classe B, IC RF CE (EMC, LVD, RoHS), RCM, VCCI classe B, MIC/TELEC, UL, cUL, TUV/GS, CB, centre de compétence du Mexique par UL, DEEE, REACH	-



Caractéristiques des pare-feu SonicWALL TZ Series suite

Technologie sans fil intégrée	SOHO Series	TZ300, TZ400, TZ500 Series	TZ600 Series
Normes	802.11 ac/a/b/g/n	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK, 02.1x, EAP-PEAP, EAP-TTLS)	-
Bandes de fréquence	802.11a : 5,180 à 5,825 GHz ; 802.11b/g : 2,412 à 2,472 GHz ; 802.11n : 2,412 à 2,472 GHz, 5,180 à 5,825 GHz ;	802.11a : 5,180 à 5,825 GHz ; 802.11b/g : 2,412 à 2,472 GHz ; 802.11n : 2,412 à 2,472 GHz, 5,180 à 5,825 GHz ; 802.11ac : 2,412 à 2,472 GHz, 5,180 à 5,825 GHz	-
Canaux de fonctionnement	802.11a : États-Unis et Canada 12, Europe 11, Japon 4, Singapour 4, Taiwan 4 ; 802.11b/g : États-Unis et Canada 1-11, Europe 1-13, Japon 1-14 (14-802.11b uniquement) ; 802.11n (2,4 GHz) : États-Unis et Canada 1-11, Europe 1-13, Japon 1-13 ; 802.11n (5 GHz) : États-Unis et Canada 36-48/149-165, Europe 36-48, Japon 36-48, Espagne 36-48/52-64 ;	802.11a : États-Unis et Canada 12, Europe 11, Japon 4, Singapour 4, Taiwan 4 ; 802.11b/g : États-Unis et Canada 1-11, Europe 1-13, Japon 1-14 (14-802.11b uniquement) ; 802.11n (2,4 GHz) : États-Unis et Canada 1-11, Europe 1-13, Japon 1-13 ; 802.11n (5 GHz) : États-Unis et Canada 36-48/149-165, Europe 36-48, Japon 36-48, Espagne 36-48/52-64 ;	-
Puissance de transmission en sortie	Selon le domaine réglementaire spécifié par l'administrateur système	Selon le domaine réglementaire spécifié par l'administrateur système	-
Contrôle de puissance de transmission	Pris en charge	Pris en charge	-
Débits pris en charge	802.11a : 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s par canal ; 802.11b : 1, 2, 5, 5, 11 Mbit/s par canal ; 802.11g : 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s par canal ; 802.11n : 7, 2, 14, 4, 21, 7, 28, 9, 43, 3, 57, 8, 65, 72, 2, 15, 30, 45, 60, 90, 120, 135, 150 Mbit/s par canal ;	802.11a : 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s par canal ; 802.11b : 1, 2, 5, 5, 11 Mbit/s par canal ; 802.11g : 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s par canal ; 802.11n : 7, 2, 14, 4, 21, 7, 28, 9, 43, 3, 57, 8, 65, 72, 2, 15, 30, 45, 60, 90, 120, 135, 150 Mbit/s par canal ; 802.11ac : 7, 2, 14, 4, 21, 7, 28, 9, 43, 3, 57, 8, 65, 72, 2, 86, 7, 96, 3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32, 5, 65, 97, 5, 130, 195, 260, 292, 5, 325, 390, 433, 3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866, 7 Mbit/s par canal	-
Spectre de technologie de modulation	802.11a : Multiplexage par répartition orthogonale de la fréquence (OFDM) ; 802.11b : Étalement de spectre à séquence directe (DSSS) ; 802.11g : Multiplexage par répartition orthogonale de la fréquence (OFDM)/Étalement de spectre à séquence directe (DSSS) ; 802.11n : Multiplexage par répartition orthogonale de la fréquence (OFDM)	802.11a : Multiplexage par répartition orthogonale de la fréquence (OFDM) ; 802.11b : Étalement de spectre à séquence directe (DSSS) ; 802.11g : Multiplexage par répartition orthogonale de la fréquence (OFDM)/Étalement de spectre à séquence directe (DSSS) ; 802.11n : Multiplexage par répartition orthogonale de la fréquence (OFDM) ; 802.11ac : Multiplexage par répartition orthogonale de la fréquence (OFDM)	-

*Utilisation future.

¹ Méthodologies de test : performances maximales d'après la norme RFC 2544 (pour le pare-feu). Les performances réelles peuvent varier en fonction des conditions réseau et des services activés.

² Débit DPI/antivirus de passerelle/anti-logiciels espions/IPS complet mesuré en utilisant les tests de performance HTTP Spirent WebAvalanche et les outils de test Ixia conformes aux standards actuels. Tests réalisés avec plusieurs flux sur plusieurs paires de ports.

³ Débit VPN mesuré à l'aide du trafic UDP avec une taille de paquet de 1 280 octets et conformément à la norme RFC 2544. Toutes les caractéristiques, fonctionnalités et disponibilités peuvent faire l'objet de modifications.

⁴ BGP disponible uniquement sur SonicWALL TZ400, TZ500 et TZ600.

Informations de commande des pare-feux SonicWALL TZ Series

Produit	Référence SKU
Pare-feu Dell SonicWALL SOHO avec 1 an d'abonnement au service TotalSecure	01-SSC-0651
Pare-feu Dell SonicWALL SOHO Wireless-N avec 1 an d'abonnement au service TotalSecure	01-SSC-0653
Pare-feu Dell SonicWALL TZ300 avec 1 an d'abonnement au service TotalSecure	01-SSC-0581
Pare-feu Dell SonicWALL TZ300 Wireless-AC avec 1 an d'abonnement au service TotalSecure	01-SSC-0583
Pare-feu Dell SonicWALL TZ400 avec 1 an d'abonnement au service TotalSecure	01-SSC-0514
Pare-feu Dell SonicWALL TZ400 Wireless-AC avec 1 an d'abonnement au service TotalSecure	01-SSC-0516
Pare-feu Dell SonicWALL TZ500 avec 1 an d'abonnement au service TotalSecure	01-SSC-0445
Pare-feu Dell SonicWALL TZ500 Wireless-AC avec 1 an d'abonnement au service TotalSecure	01-SSC-0446
Pare-feu Dell SonicWALL TZ600 avec 1 an d'abonnement au service TotalSecure	01-SSC-0219
Options de haute disponibilité (chaque unité doit correspondre au même modèle)	
Pare-feu Dell SonicWALL TZ500 haute disponibilité	01-SSC-0439
Pare-feu Dell SonicWALL TZ600 haute disponibilité	01-SSC-0220

Services	Référence SKU
Pour le pare-feu Dell SonicWALL SOHO	
• Comprehensive Gateway Security Suite (1 an)	01-SSC-0688
• Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	01-SSC-0670
• Service de filtrage de contenu (1 an)	01-SSC-0676
• Service antispam complet (1 an)	01-SSC-0682
• Support 24h/24, 7j/7 (1 an)	01-SSC-0700
Pour le pare-feu Dell SonicWALL TZ300	
• Comprehensive Gateway Security Suite (1 an)	01-SSC-0638
• Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	01-SSC-0602
• Service de filtrage de contenu (1 an)	01-SSC-0608
• Service antispam complet (1 an)	01-SSC-0632
• Support 24h/24, 7j/7 (1 an)	01-SSC-0620
Pour le pare-feu Dell SonicWALL TZ400	
• Comprehensive Gateway Security Suite (1 an)	01-SSC-0567
• Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	01-SSC-0534
• Service de filtrage de contenu (1 an)	01-SSC-0540
• Service antispam complet (1 an)	01-SSC-0561
• Support 24h/24, 7j/7 (1 an)	01-SSC-0552
Pour le pare-feu Dell SonicWALL TZ500	
• Comprehensive Gateway Security Suite (1 an)	01-SSC-0488
• Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	01-SSC-0458
• Service de filtrage de contenu (1 an)	01-SSC-0464
• Service antispam complet (1 an)	01-SSC-0482
• Support 24h/24, 7j/7 (1 an)	01-SSC-0476
Pour le pare-feu Dell SonicWALL TZ600	
• Comprehensive Gateway Security Suite (1 an)	01-SSC-0258
• Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	01-SSC-0228
• Service de filtrage de contenu (1 an)	01-SSC-0234
• Service antispam complet (1 an)	01-SSC-0252
• Support 24h/24, 7j/7 (1 an)	01-SSC-0246

À propos de Dell Security

Les solutions Dell Security vous aident à créer et à maintenir une base solide de sécurité, avec des solutions interconnectées à l'échelle de l'entreprise. Des terminaux aux réseaux en passant par les utilisateurs, les données et les identités, les solutions Dell Security réduisent les risques et la complexité pour favoriser la croissance de votre entreprise. www.dell.com/security

Dell

5455 Great America Parkway, Santa Clara, CA 95054
www.dell.com/security

Si vous n'êtes pas situé en Amérique du Nord, vous trouverez les coordonnées de notre bureau local sur notre site Internet.

© 2016 Dell, Inc. TOUS DROITS RÉSERVÉS. Le logo et les produits Dell et Dell Security, tels qu'identifiés dans ce document, sont des marques commerciales ou 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.
 Datashheet-SonicWALL-TZ Series-US-VG-27853

