Pare-feux SonicWall TZ Series

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

Les pare-feux UTM (Unified Threat Management) SonicWall TZ Series constituent une solution optimale pour les structures nécessitant une protection haut de gamme de leur réseau.

Ils protègent contre une large gamme de risques. Leurs services de sécurité avancés incluent la protection contre les logiciels malveillants et les logiciels espions, le contrôle applicatif, un système de prévention des intrusions (IPS, Intrusion Prevention System) et le filtrage d'URL intégrés et basés sur le Cloud. Afin de lutter contre la tendance des attaques chiffrées, les pare-feux TZ Series possèdent la puissance de traitement requise pour inspecter les connexions SSL/TLS chiffrées et rechercher les dernières menaces. Associés aux commutateurs Dell série X, certains pare-feux TZ Series peuvent gérer directement la sécurité de ces ports supplémentaires.

Couverts par le réseau SonicWall Capture Threat Network, 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 des ports Gigabit Ethernet, une connectivité sans fil 802.11ac* intégrée en option, un réseau VPN IPSec et SSL, un basculement par le biais de la prise en charge 3G/4G intégrée, un équilibrage de charge et une segmentation réseau. Les pare-feux UTM SonicWall TZ Series fournissent également un accès mobile rapide et sécurisé sur les plateformes Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS X et Linux.

Le système SonicWall Global Management System (GMS) permet un déploiement et une gestion centralisés 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 de nouvelle génération phares 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 :

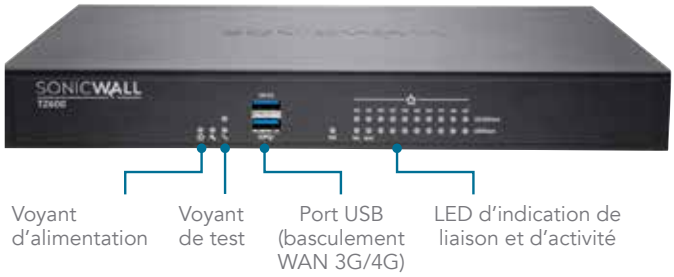
- Protection réseau haut de gamme
- Inspection approfondie des paquets sur l'ensemble du trafic, sans restriction quant à la taille des fichiers ou au protocole
- Connectivité sans fil 802.11ac sécurisée à l'aide d'un contrôleur sans fil intégré ou via des points d'accès sans fil SonicPoint externes
- Accès mobile VPN SSL pour les 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'elle est déployée conjointement avec des commutateurs Dell série X.

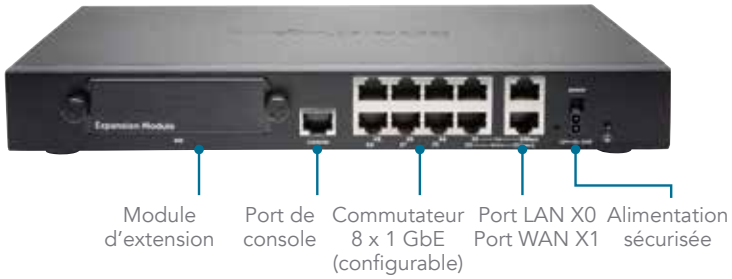
** 802.11ac non disponible actuellement sur les modèles SOHO ; les modèles SOHO prennent en charge 802.11a/b/g/n.*

SonicWall TZ600 Series

Le pare-feu de nouvelle génération 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

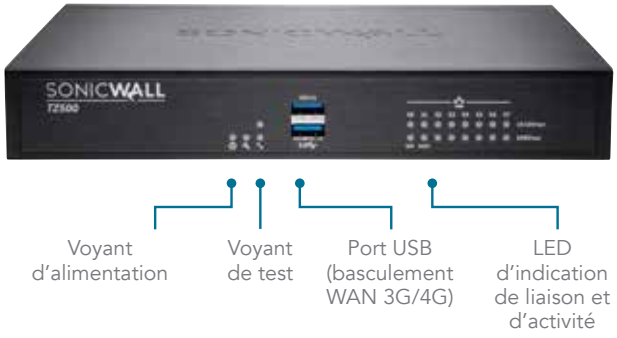


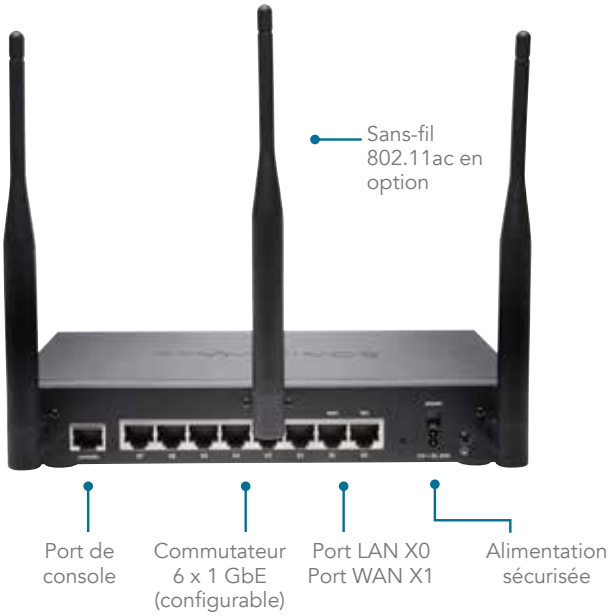


SonicWall TZ500 Series

Conçu pour les succursales et les PME en pleine croissance, le pare-feu SonicWall TZ500 Series associe une protection extrêmement efficace et sans compromis à 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	1,0 Gbit/s
Débit IMIX	700 Mbit/s
Connexions DPI max.	100 000
Nouvelles connexions/s	8 000

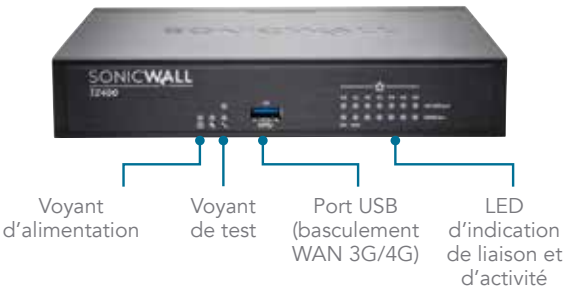


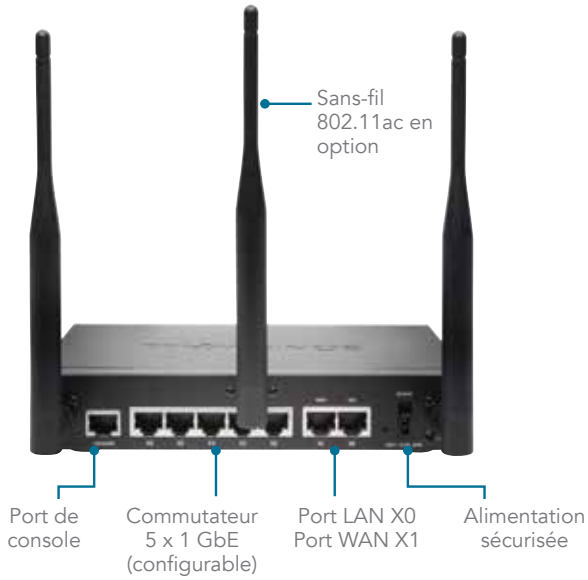


SonicWall TZ400 Series

Conçu pour les petites entreprises, les points de vente au détail et les succursales, le pare-feu SonicWall TZ400 Series assure une protection de niveau professionnel. Des options flexibles de déploiement sans fil sont disponibles avec la connectivité sans fil 802.11ac double bande 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

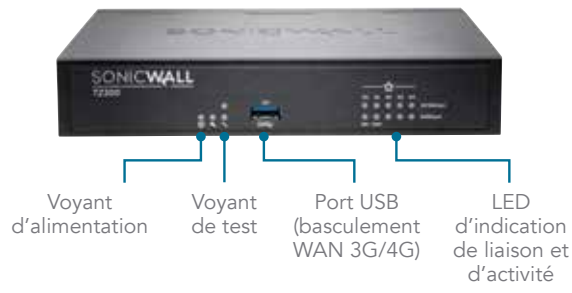


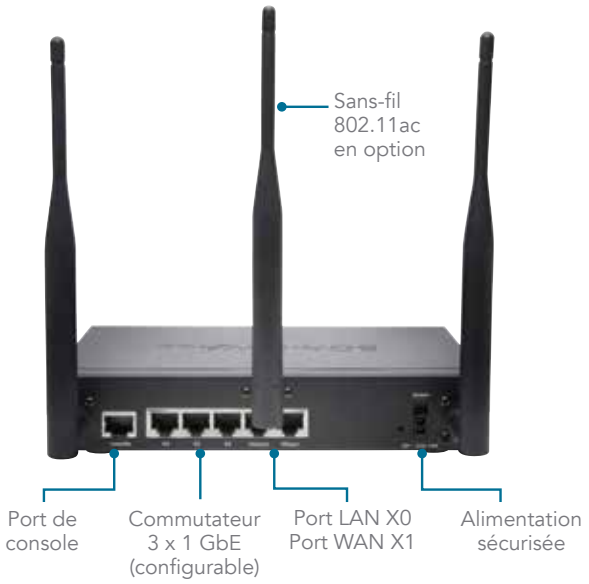


SonicWall TZ300 Series

Le pare-feu SonicWall TZ300 Series 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 à 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

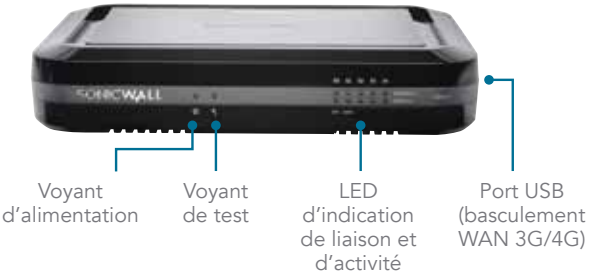


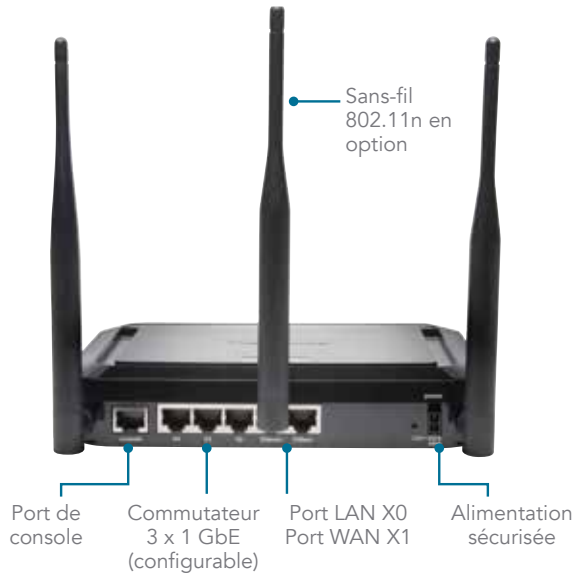


SonicWall SOHO Series

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

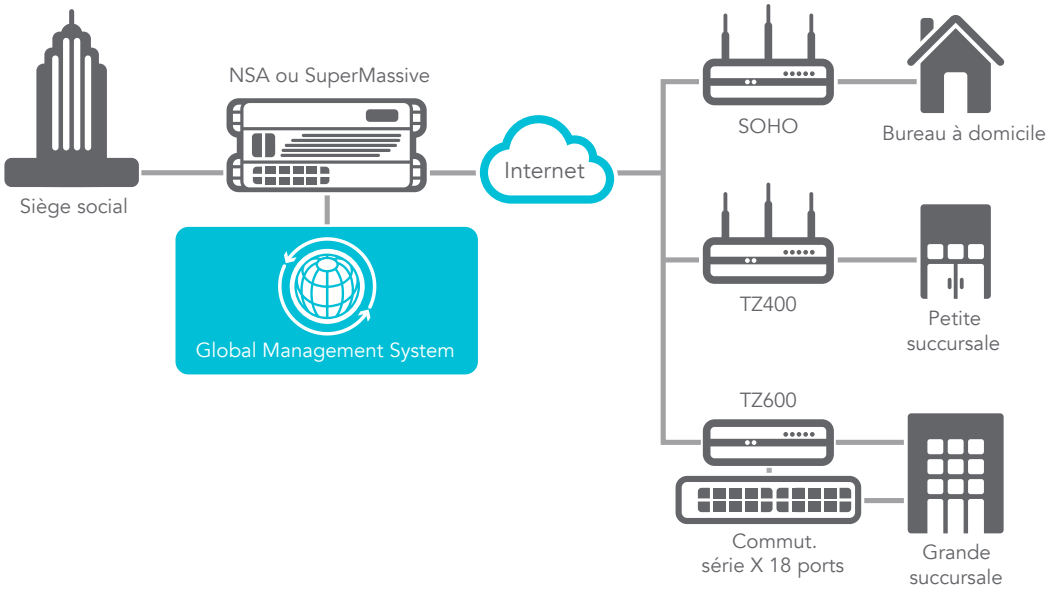
Caractéristiques	SOHO Series
Débit du pare-feu	300 Mbit/s
Débit DPI complet	50 Mbit/s
Débit d'inspection des logiciels malveillants	50 Mbit/s
Débit IPS	100 Mbit/s
Débit IMIX	60 Mbit/s
Connexions DPI max.	10 000
Nouvelles connexions/s	1 800





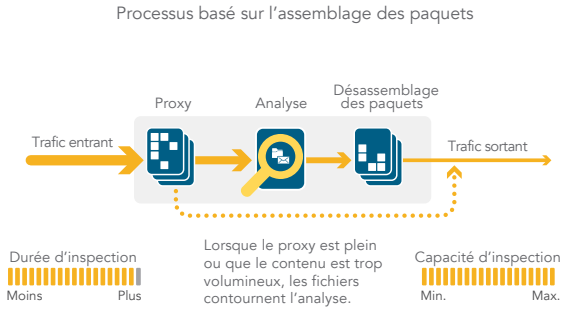
Architecture extensible pour une évolutivité et des performances maximum

Le moteur RFDPI (Reassembly-Free Deep Packet Inspection) est conçu de A à Z pour fournir des analyses de sécurité ultraperformantes afin de répondre à la nature à la fois parallèle et croissante 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 en offrant flexibilité et programmabilité sur le terrain, un point faible des systèmes ASIC. Cette flexibilité est essentielle lorsque du nouveau code et des mises à jour de comportement sont nécessaires pour lutter contre les nouvelles attaques exigeant des techniques de détection actualisées et plus sophistiquées.

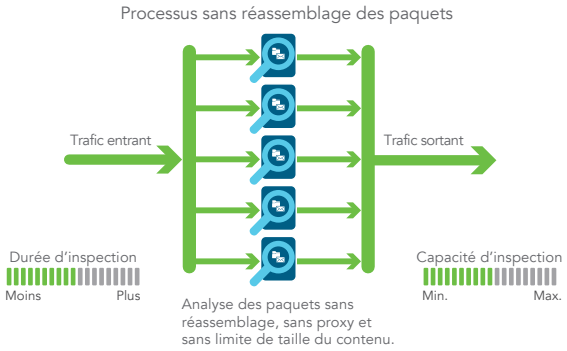


Moteur RFDPI (Reassembly-Free Deep Packet Inspection)

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 peut également être configuré 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.



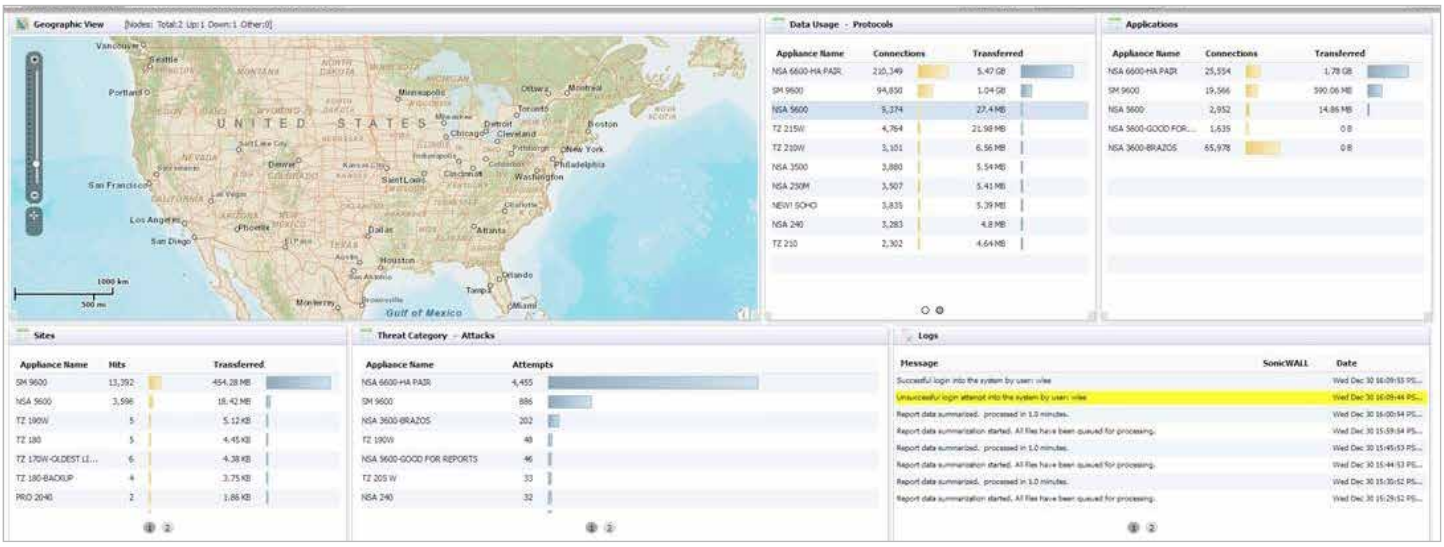
Architecture concurrente



Architecture SonicWall

Gestion globale et reporting

Conçue pour les déploiements dans des entreprises distribuées de plus grande taille, la solution SonicWall Global Management System (GMS) en option offre aux administrateurs une plateforme de gestion des appliances de sécurité SonicWall et des commutateurs Dell série X unifiée, sécurisée et extensible. La solution GMS 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 règles, la surveillance des événements en temps réel, l'analyse, 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 du workflow. Au lieu d'adopter une approche au cas par cas, la solution GMS optimise la gestion de la sécurité réseau via des processus métier et des niveaux de service qui simplifient considérablement la gestion du cycle de vie des environnements de sécurité dans leur ensemble.



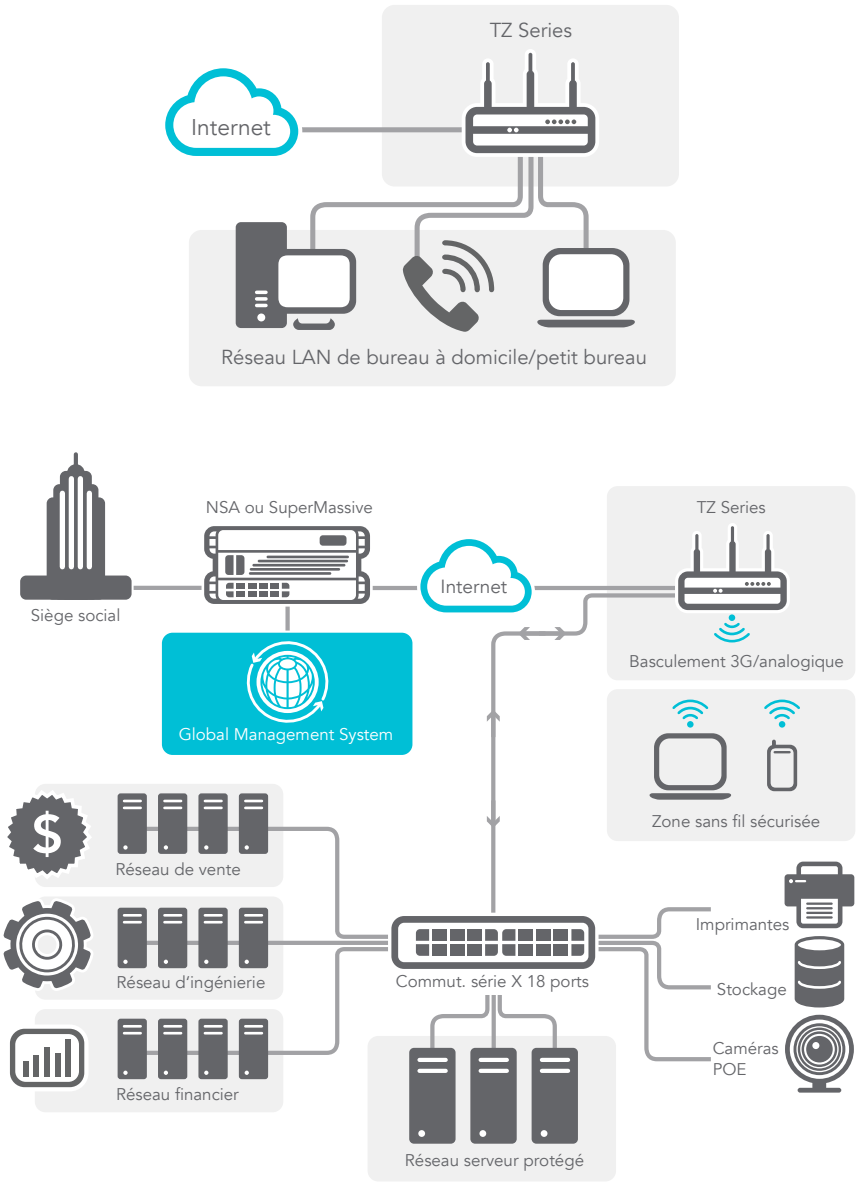
SONICWALL®

Sécurité et protection

L'équipe dédiée de recherche des menaces SonicWall Capture Labs recherche et développe en interne des contre-mesures qui seront déployées sur les pare-feux sur le terrain pour une protection actualisée. L'équipe utilise plus d'un million de capteurs 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 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 SonicWall ont également accès à SonicWall CloudAV, qui complète la base de données intégrée de signatures avec plus de 20 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 de nouvelle génération 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 SonicWall fournit des informations granulaires sur le trafic applicatif, l'utilisation de la bande passante et les menaces de sécurité, ainsi 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 de nouvelle génération SonicWall crée 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.

** 802.11ac non disponible actuellement sur les modèles SOHO ; les modèles SOHO prennent en charge 802.11a/b/g/n.*

SONICWALL®

Fonctionnalités

Moteur RFDPI	
Fonctionnalité	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.
DPI-SSH (Deep Packet Inspection of Secure Socket Shell)	Détecte et empêche les attaques chiffrées évoluées qui exploitent le protocole SSH, bloque les téléchargements de logiciels malveillants chiffrés, interrompt la propagation des infections et contre les communications C&C et l'exfiltration de données.
Capture Advanced Threat Protection	
Fonctionnalité	Description
Service de sandbox multi-moteur	La plateforme sandbox multi-moteur, qui inclut le sandboxing virtualisé, l'émulation complète du système et une technologie d'analyse au niveau de l'hyperviseur, exécute le code suspect et analyse son comportement, offrant ainsi une visibilité complète sur l'activité malveillante.
Analyse de nombreux types de fichiers	Ce service assure l'analyse d'un vaste éventail de fichiers, notamment les programmes exécutables (PE), DLL, PDF, documents MS Office, archives, JAR et APK, ainsi que de divers systèmes d'exploitation comme Windows, Android ou Mac OSX et des environnements multi-navigateurs.
Déploiement rapide des signatures	Lorsqu'un fichier est identifié comme étant malveillant, une signature est immédiatement mise à la disposition des pare-feux ayant un abonnement à SonicWall Capture, avant d'être envoyée sous 48 heures aux bases de données de signatures Gateway Anti-Virus et IPS ainsi qu'aux bases de données d'URL, d'IP et de réputation de domaine.
Blocage jusqu'au verdict	Pour empêcher les fichiers potentiellement malveillants de pénétrer sur le réseau, les fichiers envoyés dans le Cloud pour y être analysés peuvent être retenus à la passerelle jusqu'à ce qu'un verdict soit rendu.
Protection contre les menaces chiffrées	
Fonctionnalité	Description
Déchiffrement et inspection TLS/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 met en application les règles de contrôle du contenu, des URL et des applications afin de contrer les menaces dissimulées au sein du trafic TLS/SSL chiffré. Inclus avec les abonnements de sécurité pour tous les modèles, à l'exception de SOHO. Vendu comme une licence séparée sur les modèles SOHO.
Inspection SSH	L'inspection approfondie des paquets SSH (DPI-SSH) déchiffre et inspecte les données traversant les tunnels SSH en vue de prévenir les attaques qui exploitent ce protocole.
Prévention des intrusions	
Fonctionnalité	Description
Protection basée sur des contre-mesures	Le système de prévention des intrusions (Intrusion Prevention System, IPS) étroitement intégré s'appuie sur 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 SonicWall Capture Labs 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 (Command and Control, CnC) 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.
Abus/anomalies de protocoles	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.
Prévention des menaces	
Fonctionnalité	Description
Anti-logiciels malveillants de passerelle	Le moteur RFDPI analyse tout le trafic entrant, sortant et intrazone pour détecter les virus, chevaux de Troie, enregistreurs de frappes et autres logiciels malveillants dans les fichiers, quelles que soient leur taille et leur longueur, sur tous les ports et les flux TCP.
Protection contre les logiciels malveillants CloudAV	Les serveurs Cloud SonicWall hébergent une base de données de plus de 20 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 dotés de services de sécurité actifs et prennent effet immédiatement, sans redémarrage ni interruption.

Prévention des menaces (suite)	
Fonctionnalité	Description
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 règles 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 les modèles 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	
Fonctionnalité	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/Terminal Services/Citrix.
Filtrage du contenu	
Fonctionnalité	Description
Filtrage du contenu interne/externe	Applique des règles 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 règles pour bloquer les contenus Internet des appareils situés hors du périmètre du pare-feu via le service client de filtrage de contenu.
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 SonicWall pour accélérer l'accès ultérieur aux sites les plus fréquentés.
Antivirus et anti-logiciels espions appliqués	
Fonctionnalité	Description
Protection multicouche	Utilise les fonctionnalités du pare-feu comme première couche de défense au niveau du périmètre et les associe à la protection des terminaux 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	
Fonctionnalité	Description
Inspection stateful des paquets	Tout le trafic réseau est inspecté, analysé et mis en conformité avec les règles 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 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.
Authentification biométrique pour l'accès distant	Prend en charge les modes d'authentification d'appareils mobiles, comme la reconnaissance d'empreinte digitale, difficiles à dupliquer ou à partager, en vue de déterminer en toute sécurité l'identité de l'utilisateur pour l'accès au réseau.
Intégration des commutateurs Dell série X	Gérez les paramètres de sécurité de ports supplémentaires, notamment les ports POE et POE+, à partir d'un seul écran, en combinant le tableau de bord TZ Series avec les commutateurs série X (non disponible avec les modèles SOHO).

Pare-feu et gestion de réseau (suite)	
Fonctionnalité	Description
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.
API de menaces	Permet au pare-feu de recevoir tout type de flux de renseignements propriétaires, d'OEM ou de fournisseurs tiers, pour combattre les menaces évoluées : zero-day, initié malveillant, identifiants compromis, ransomwares, menaces persistantes avancées...
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 reporting	
Fonctionnalité	Description
Global Management System	La solution SonicWall GMS surveille, configure et génère des rapports sur plusieurs appliances SonicWall et connecteurs Dell série X via une console de gestion unique dotée d'une interface intuitive pour réduire les coûts et la complexité de gestion.
Gestion puissante avec un seul appareil	L'interface Web intuitive permet une configuration rapide et pratique. Elle offre également une interface de 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 SonicWall GMSFlow Server ou d'autres outils prenant en charge IPFIX et NetFlow via des extensions.
Réseau privé virtuel	
Fonctionnalité	Description
Configuration automatique du VPN	Simplifie sensiblement le déploiement de pare-feux distribués en automatisant la configuration initiale de la passerelle VPN site à site entre les pare-feux SonicWall. Sécurité et connectivité se mettent en place instantanément et automatiquement.
VPN IPSec pour la connectivité site à site	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 WAN sont utilisés, un VPN principal et un VPN 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 points de terminaison sur des routes alternatives.
Indicateur de contexte/contenu	
Fonctionnalité	Description
Suivi de l'activité des utilisateurs	L'activité et l'identification des utilisateurs sont disponibles via une intégration SSO AD/LDAP/Citrix1/Terminal Services 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.

Récapitulatif des fonctionnalités de SonicOS

Pare-feu

- Inspection stateful des paquets
- Reassembly-Free Deep Packet Inspection
- Protection contre les attaques DDoS (UDP/ICMP/SYN flood)
- Prise en charge IPv4/IPv6
- Authentification biométrique pour l'accès distant
- Proxy DNS
- API de menaces

Déchiffrement et inspection SSL/SSH[1]

- Inspection approfondie des paquets pour TLS/SSL/SSH
- Inclusion/exclusion d'objets, de groupes ou de noms d'hôtes
- Contrôle SSL

Capture Advanced Threat Protection[1]

- Analyse multi-moteur Cloud
- Sandboxing virtualisé
- Analyse au niveau de l'hyperviseur
- Émulation complète du système
- Examen de nombreux types de fichiers
- Soumission automatique et manuelle
- Mises à jour en temps réel des renseignements sur les menaces
- Fonctionnalité de blocage automatique

Prévention des intrusions[1]

- Analyse basée sur des signatures
- Mise à jour automatique des signatures
- Inspection bidirectionnelle
- Fonctionnalité de règles IPS granulaires
- Filtrage GeoIP/de réseaux de zombies[2]
- Détection des expressions régulières

Protection contre les logiciels malveillants[1]

- 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

Identification des applications[1]

- Contrôle des applications
- Visualisation des applications[2]
- 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[1]

- Filtrage des URL
- Technologie anti-proxy
- Blocage par mots-clés
- Catégories d'évaluation CFS pour la gestion de la bande passante
- Modèle unifié de règles avec contrôle des applications
- Content Filtering Client

VPN

- Configuration automatique du VPN
- VPN IPSec pour la connectivité site à site
- Accès client à distance IPSec et VPN SSL
- Passerelle VPN redondante
- Mobile Connect pour iOS, Mac OS X, Windows, Chrome, Android et Kindle Fire
- VPN basé sur le routage (OSPF, RIP, BGP)

Gestion de réseau

- PortShield
- Journalisation améliorée
- Qualité de service de couche 2
- Sécurité des ports
- Routage dynamique (RIP/OSPF/BGP)
- Contrôleur sans fil SonicWall
- Routage à base de règles (ToS/métrique et ECMP)
- Routage asymétrique
- Serveur DHCP
- NAT
- Gestion de la bande passante
- Haute disponibilité – active/passive avec synchronisation d'état[3]
- Équilibrage de la charge entrante/sortante
- Mode pont de couche 2, mode NAT
- Basculement WAN 3G/4G
- Prise en charge Common Access Card (CAC)

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 de ligne de commande
- SNMPv2/v3
- Gestion et reporting centralisés avec SonicWall GMS
- Journalisation
- Exportation NetFlow/IPFix
- Sauvegarde Cloud de la configuration
- Visualisation de la bande passante et des applications
- Gestion IPv4 et IPv6
- Gestion des commutateurs Dell série X notamment en cascade

Technologie sans fil intégrée

- Double bande (2,4 GHz et 5 GHz)
- Normes sans fil 802.11 a/b/g/n/ac[2]
- 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

[1] *Requiert un abonnement supplémentaire*
[2] *Non disponible sur les pare-feux SOHO Series*
[3] *Haute disponibilité avec synchronisation d'état disponible uniquement sur les modèles SonicWall TZ500 et SonicWall TZ600*

SONICWALL®

Caractéristiques des pare-feux SonicWall TZ Series

Aperçu du matériel	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Système d'exploitation	SonicOS				
Cœurs de processeur de sécurité	2	2	4	4	4
Interfaces	5 x 1 GbE, 1 USB, 1 console	5 x 1 GbE, 1 USB, 1 console	7 x 1 GbE, 1 USB, 1 console	8 x 1 GbE, 2 USB, 1 console	10 x 1 GbE, 2 USB, 1 console, 1 connecteur d'extension
Extension	USB	USB	USB	2 USB	Connecteur d'extension (à l'arrière)*, 2 USB
Utilisateurs de l'authentification unique (SSO)	250	500	500	500	500
Interfaces VLAN	25	25	50	50	50
Points d'accès pris en charge (max.)	2	8	16	16	24
Modèles de commutateurs Dell série X pris en charge	Non disponible	X1008/P, X1018/P, X1026/P, X1052/P, X4012			
Performances pare-feu/VPN	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
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	60 Mbit/s	200 Mbit/s	500 Mbit/s	700 Mbit/s	900 Mbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[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
Connexions maximales (DPI-SSL)	100	500	500	750	750
VPN	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Tunnels VPN 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	Verisign, Thawte, Cybertrust, RSA Keon, Entrust et Microsoft CA pour VPN SonicWall à SonicWall, SCEP				
Fonctionnalités VPN	Dead Peer Detection, DHCP sur VPN, traversée du NAT IPSec, passerelle VPN redondante, VPN basé sur le routage				
Plateformes Global VPN Client 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, Windows 10				
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, Chrome, Windows 8.1 (intégré)				
Services de sécurité	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Services d'inspection approfondie des paquets	Antivirus de passerelle, anti-logiciels espions, prévention des intrusions, DPI-SSL				
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 comme ActiveX, Java, cookies de confidentialité, listes blanches/noires				
Antivirus et anti-logiciels espions client appliqués	McAfee® et Kaspersky™				
Comprehensive Anti-Spam Service	Pris en charge				
Visualisation des applications	Non	Oui	Oui	Oui	Oui
Contrôle des applications	Oui	Oui	Oui	Oui	Oui
Capture Advanced Threat Protection	Non	Oui	Oui	Oui	Oui

SONICWALL®

Caractéristiques des pare-feux SonicWall TZ Series (suite)

Gestion de réseau	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Attribution d'adresses 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 à base de règles				
Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1e (WMM)				
Authentification	LDAP (domaines multiples), XAUTH/RADIUS, SSO, Novell, base de données utilisateurs interne	LDAP (domaines multiples), XAUTH/RADIUS, SSO, Novell, base de données utilisateurs interne, Terminal Services, Citrix			
Base de données utilisateurs 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	FIPS 140-2 (avec Suite B) niveau 2, APL UC, VPNC, IPv6 (Phase 2), pare-feu réseau ICSA, antivirus ICSA				
Certifications en attente	Critères Communs NDPP				
Carte CAC (Common Access Card)	Pris 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
Format	Bureau				
Bloc d'alimentation (W)	24 W externe	24 W externe	24 W externe	36W externe	60W externe
Consommation électrique maximale (W)	6,4/11,3	6,9/12,0	9,2/13,8	13,4/17,7	16,1
Puissance d'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	3,6x14,1x19 cm	3,5x13,4x19 cm	3,5x13,4x19 cm	3,5x15x22,5 cm	3,5x18x28 cm
Poids	0,34 kg/0,75 lb 0,48 kg/1,06 lb	0,73 kg/1,61 lb 0,84 kg/1,85 lb	0,73 kg/1,61 lb 0,84 kg/1,85 lb	0,92 kg/2,03 lb 1,05 kg/2,31 lb	1,47 kg/3,24 lb
Poids DEEE	0,80 kg/1,76 lb 0,94 kg/2,07 lb	1,15 kg/2,53 lb 1,26 kg/2,78 lb	1,15 kg/2,53 lb 1,26 kg/2,78 lb	1,34 kg/2,95 lb 1,48 kg/3,26 lb	1,89 kg/4,16 lb
Poids avec emballage	1,20 kg/2,64 lb 1,34 kg/2,95 lb	1,37 kg/3,02 lb 1,48 kg/3,26 lb	1,37 kg/3,02 lb 1,48 kg/3,26 lb	1,93 kg/4,25 lb 2,07 kg/4,56 lb	2,48 kg/5,47 lb
Temps de fonctionnement entre deux pannes (en années)	58,9/56,1 (Wireless)	56,1	54,0	40,8	18,4
Environnement (en fonctionnement/stockage)	0 à 40 °C (32 à 105 °F)/-40 à 70 °C (-40 à 158 °F)				
Taux d'humidité	5 à 95 % sans condensation				

Réglementation	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Modèle de réglementation (modèles filaires)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Conformité aux réglementations majeures (modèles filaires)	FCC classe B, ICES classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI classe B, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH, KCC/MSIP	FCC classe B, ICES classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI classe B, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH, KCC/MSIP	FCC classe B, ICES classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI classe B, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH, KCC/MSIP	FCC classe B, ICES classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI classe B, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH, BSMI, KCC/MSIP	FCC classe A, ICES classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI classe A, UL, cUL, TÜV/GS, CB, Mexico CoC 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 (R&TTE, EMC, LVD, RoHS), RCM, VCCI classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH	FCC classe B, FCC RF ICES classe B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH	FCC classe B, FCC RF ICES classe B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH	FCC classe B, FCC RF ICES classe B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH	-

Caractéristiques des pare-feux SonicWall TZ Series (suite)

Technologie sans fil intégrée	SOHO Series	TZ300, TZ400, TZ500 Series	TZ600
Normes	802.11 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[5]	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, Taïwan 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, Taïwan 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 ; 802.11ac : 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] Méthodes de test : performances maximales basées sur RFC 2544 (pour 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 uniquement disponible sur les modèles SonicWall TZ400, TZ500 et TZ600.

[5] Tous les modèles sans fil intégrés TZ prennent en charge les bandes 2,4 GHz ou 5 GHz. Pour une prise en charge double bande, utilisez les points d'accès sans fil SonicWall (SonicPoint).

Informations de commande des pare-feux SonicWall TZ Series

Produit	Référence
Pare-feu SonicWall SOHO avec 1 an d'abonnement au service TotalSecure	01-SSC-0651
Pare-feu SonicWall SOHO Wireless-N avec 1 an d'abonnement au service TotalSecure	01-SSC-0653
Pare-feu SonicWall TZ300 avec 1 an d'abonnement au service TotalSecure	01-SSC-0581
Pare-feu SonicWall TZ300 Wireless-AC avec 1 an d'abonnement au service TotalSecure	01-SSC-0583
Pare-feu SonicWall TZ400 avec 1 an d'abonnement au service TotalSecure	01-SSC-0514
Pare-feu SonicWall TZ400 Wireless-AC avec 1 an d'abonnement au service TotalSecure	01-SSC-0516
Pare-feu SonicWall TZ500 avec 1 an d'abonnement au service TotalSecure	01-SSC-0445
Pare-feu SonicWall TZ500 Wireless-AC avec 1 an d'abonnement au service TotalSecure	01-SSC-0446
Pare-feu 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 SonicWall TZ500 haute disponibilité	01-SSC-0439
Pare-feu SonicWall TZ600 haute disponibilité	01-SSC-0220

Informations de commande des pare-feux SonicWall TZ Series (suite)

Services	Référence
Pour SonicWall SOHO Series	
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 SonicWall TZ300 Series	
Advanced Gateway Security Suite – Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour le pare-feu TZ300 (1 an)	01-SSC-1430
Capture Advanced Threat Protection pour le pare-feu TZ300 (1 an)	01-SSC-1435
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 SonicWall TZ400 Series	
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour le pare-feu TZ400 (1 an)	01-SSC-1440
Capture Advanced Threat Protection pour le pare-feu TZ400 (1 an)	01-SSC-1445
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 SonicWall TZ500 Series	
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour le pare-feu TZ500 (1 an)	01-SSC-1450
Capture Advanced Threat Protection pour le pare-feu TZ500 (1 an)	01-SSC-1455
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 SonicWall TZ600	
Advanced Gateway Security Suite : Capture ATP, prévention des menaces, filtrage du contenu et support 24h/24, 7j/7 pour le pare-feu TZ600 (1 an)	01-SSC-1460
Capture Advanced Threat Protection pour le pare-feu TZ600 (1 an)	01-SSC-1465
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 nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com

Datasheet-TZ Series-US-VG-MKTG658