SONICWALL

Série SonicWall TZ

Prévention intégrée des menaces et plateforme SD-Branch pour les petites/moyennes organisations et entreprises décentralisées

La série SonicWall TZ permet aux PME et entreprises distribuées de bénéficier de tous les avantages d'une solution de sécurité intégrée qui ne laisse rien au hasard. La série TZ allie la prévention des menaces haut débit et la technologie SD-WAN (Software-Defined Wide Area Network) à un vaste éventail de fonctionnalités réseau et sans fil, sans oublier le déploiement simplifié et la gestion centralisée. Il en résulte une solution de sécurité unifiée à un faible coût total de possession.

Solution de sécurité intégrée, flexible

SonicOS, le système d'exploitation riche en fonctionnalités de SonicWall, est au cœur des pare-feu de la série TZ. Les pare-feu prenant en charge le dernier système d'exploitation SonicOS 7.0 ont une nouvelle interface/expérience utilisateur avec une apparence moderne, une sécurité avancée, des fonctionnalités réseau et une gestion simplifiée des politiques.

SonicOS comporte en plus tout un arsenal de fonctionnalités permettant aux entreprises d'ajuster ces pare-feu UTM (Unified Threat Management) aux exigences spécifiques de leur réseau. Par exemple, la création d'un réseau sans fil haut débit sécurisé est facilitée par l'intégration d'un contrôleur sans fil qui prend en charge la norme IEEE 802.11 ou l'ajout de nos points d'accès SonicWave 802.11ac Wave 2. Afin de réduire le coût et la complexité liés à la connexion de points d'accès sans fil haut débit et d'autres appareils compatibles PoE (Power over Ethernet), tels que les caméras, les téléphones, les imprimantes IP, etc., les pare-feu TZ300P, TZ600P et TZ570P offrent l'alimentation PoE/PoE+.

Les commerces distribués et les environnements de type campus peuvent bénéficier de bien d'autres avantages procurés par les nombreux outils intégrés à SonicOS. Les succursales peuvent échanger des informations avec le siège en toute sécurité grâce au réseau privé virtuel (VPN). Les LAN virtuels, ou VLAN, permettent de segmenter le réseau en différents groupes de collaborateurs ou de clients et d'y associer des règles déterminant le niveau de communication avec des appareils situés sur d'autres VLAN. Le SD-WAN constitue une alternative sûre aux circuits MPLS, coûteux, tout en garantissant la fiabilité de la disponibilité et des performances applicatives. Le déploiement des pare-feu TZ sur les sites distants est un jeu d'enfant. Grâce au déploiement zéro intervention, les pare-feu sont configurés à distance via le cloud.

Prévention des menaces et performances haut de gamme

Notre vision de la sécurisation des réseaux dans le paysage en constante mutation de la cybercriminalité implique une détection et une prévention automatisées et en temps réel des menaces. L'association de technologies intégrées et cloud permet à nos pare-feu d'assurer une sécurité dont l'extrême efficacité a été validée par les tests de tiers indépendants. Les menaces inconnues sont envoyées à la sandbox multimoteur cloud de SonicWall, Capture Advanced Threat Protection (ATP), pour y être analysées. Le service Capture ATP est optimisé par notre technologie Real-Time Deep Memory Inspection (RTDMI™) en instance de brevet. En procédant à une inspection directement dans la mémoire, le moteur RTDMI détecte et bloque les logiciels malveillants et les menaces de type zero-day. La technologie RTDMI est précise, elle réduit à un minimum les faux positifs, identifie et neutralise les attaques sophistiquées, dès que les armes du logiciel malveillant sont exposées en moins de 100 nanosecondes. En parallèle, notre moteur RFDPI (Reassembly-Free

Avantages :

Solution de sécurité intégrée, flexible

- Interfaces multi-gigabits dans un format de bureau
- SD-Branch sécurisé avec SD-WAN
- Puissant système d'exploitation SonicOS 7.0
- Fonctionnalité sans fil haut débit 802.11ac Wave 2
- Power over Ethernet (PoE/PoE+)
- Prise en charge 5G/4G/LTE
- Stockage intégré et extensible
- Alimentation redondante

Prévention des menaces et performances haut de gamme

- Technologie d'inspection approfondie de la mémoire en temps réel, en instance de brevet
- Technologie RFDPI (Reassembly-Free Deep Packet Inspection) brevetée
- Prise en charge de TLS 1.3
- Efficacité de la sécurité reconnue par le secteur

Facilité de déploiement, de configuration et de gestion continue

- Déploiement sans intervention
- Gestion centralisée dans le cloud et sur site
- Intégration de l'application SonicExpress

Deep Packet Inspection) single-pass breveté examine chaque octet de chaque paquet, inspectant simultanément le trafic entrant et sortant directement sur le pare-feu. Tirant parti du service Capture ATP et de la technologie RTDMI sur la plateforme Capture Cloud SonicWall en plus de fonctionnalités intégrées (prévention des intrusions, anti-malware et filtrage des URL/Web notamment), la série TZ bloque les logiciels malveillants, les ransomwares et autres menaces à la passerelle. Pour les appareils mobiles utilisés en dehors du périmètre du pare-feu, SonicWall Capture Client ajoute une couche de protection en appliquant des techniques de protection avancées comme l'apprentissage machine ou le rollback du système. Capture Client tire également parti de l'inspection approfondie du trafic TLS chiffré (DPI-SSL) sur les pare-feu de la série TZ en installant et en gérant des certificats TLS de confiance.

Le chiffrement ayant tendance à se généraliser pour sécuriser les sessions Web, les pare-feu doivent impérativement être en mesure de traquer les menaces dans le trafic chiffré. Les pare-feu de la série SonicWall TZ offrent une protection complète, quel que soit le port ou le protocole, en déchiffrant et inspectant entièrement les connexions TLS/SSL et SSH chiffrées. Le pare-feu procède à une inspection approfondie de chaque paquet pour y déceler toute non-conformité aux protocoles, les menaces, les attaques zero-day, les intrusions et même des critères définis. Le moteur d'inspection approfondie des paquets détecte et prévient les attaques cachées qui exploitent le chiffrement. Il bloque également les téléchargements de logiciels malveillants chiffrés, interrompt la propagation des infections et contre les communications C&C et l'exfiltration de données. Les règles d'inclusion et d'exclusion permettent un contrôle total pour définir quel trafic est soumis au déchiffrement et à l'inspection en fonction d'exigences légales et/ou de conformité spécifiques à l'entreprise.

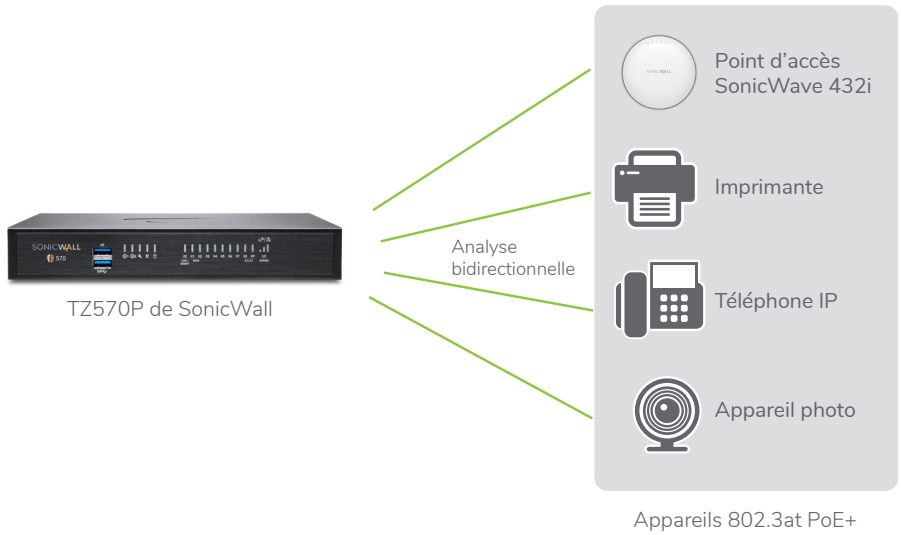
Les pare-feu TZ670 et TZ570 prennent en charge TLS 1.3, qui a subi plusieurs modifications pour améliorer les performances et la sécurité tout en éliminant les complexités.

Facilité de déploiement, de configuration et de gestion continue

La configuration et la gestion des pare-feu de la série TZ et des points d'accès SonicWave 802.11ac Wave 2 est on ne peut plus simple, quel que soit l'endroit où vous souhaitez les déployer. La gestion, le reporting, les licences et l'analyse centralisés sont assurés par notre Capture Security Center dans le cloud. Celui-ci constitue la solution optimale en termes de visibilité, d'agilité et de capacité à contrôler l'écosystème de sécurité SonicWall dans son intégralité, sur un seul et même écran.

L'un des éléments clés du Capture Security Center est le déploiement zéro intervention. Cette fonctionnalité cloud simplifie et accélère le déploiement et la configuration des pare-feu SonicWall sur les sites distants et les succursales. Ce processus ne demande qu'un minimum d'intervention de la part des utilisateurs et est entièrement automatisé de manière à rendre les pare-feu opérationnels à grande échelle en quelques étapes de déploiement simples. D'où une réduction significative du temps, des coûts et de la complexité liés à l'installation et la configuration, tandis que la sécurité et la connectivité sont assurées instantanément et automatiquement. La simplicité de déploiement et de configuration et la facilité de gestion permettent aux entreprises d'abaisser leur coût total de possession et de réaliser un bon retour sur investissement.

** 802.11ac non disponible actuellement sur les modèles SOHO/SOHO 250 ; les modèles SOHO/SOHO 250 prennent en charge 802.11a/b/g/n*



TZ570P de SonicWall

Appareils 802.3at PoE+

Alimentation et sécurité intégrées pour vous appareils compatibles PoE

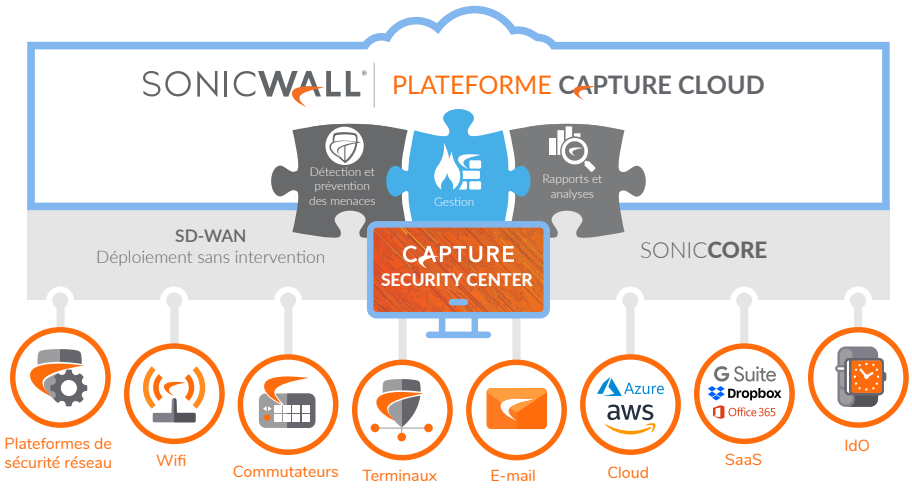
Alimentez vos appareils compatibles PoE sans avoir à payer ni vous encombrer d'un connecteur ou d'un injecteur PoE (Power over Ethernet). Les pare-feu TZ300P, TZ600P et TZ570P intègrent la technologie IEEE 802.3at permettant d'alimenter les appareils PoE et PoE+ : points d'accès sans fil, caméras, téléphones IP, etc. Le pare-feu analyse l'ensemble du trafic sans fil entrant et sortant du réseau à l'aide de la technologie d'inspection approfondie des paquets, puis élimine les menaces dangereuses comme les logiciels malveillants et les intrusions, même pour les connexions chiffrées.

Plateforme Capture Cloud

La plateforme Capture Cloud de SonicWall assure la prévention des menaces et la gestion du réseau dans le cloud, à quoi s'ajoutent des fonctionnalités de reporting et d'analyse pour les entreprises de toute taille. Cette plateforme consolide les renseignements sur les menaces à partir de plusieurs sources dont notre service de sandboxing réseau multi-moteur primé, Capture Advanced Threat Protection, ainsi que plus de 1 million de capteurs SonicWall répartis dans le monde entier.

Si les données entrant sur le réseau s'avèrent contenir du code malveillant jusqu'ici inconnu, l'équipe de recherche interne Capture Labs de SonicWall dédiée aux menaces développe des signatures stockées dans la base de données de la plateforme Capture Cloud et déployées sur le pare-feu du client pour une protection actualisée. Les mises à jour sont actives immédiatement, sans redémarrage ni interruption. Les signatures présentes sur l'application protègent contre de vastes catégories d'attaques, couvrant des dizaines de milliers de menaces individuelles. Outre les moyens de lutte intégrés, les pare-feu TZ ont accès à la base de données de la plateforme Capture Cloud, qui vient compléter les défenses sur l'application par des dizaines de millions de signatures.

En plus de la protection contre les menaces, la plateforme Capture Cloud permet une gestion sur un seul écran. Les administrateurs peuvent facilement créer des rapports en temps réel et historiques de l'activité réseau.



Protection contre les menaces évoluées

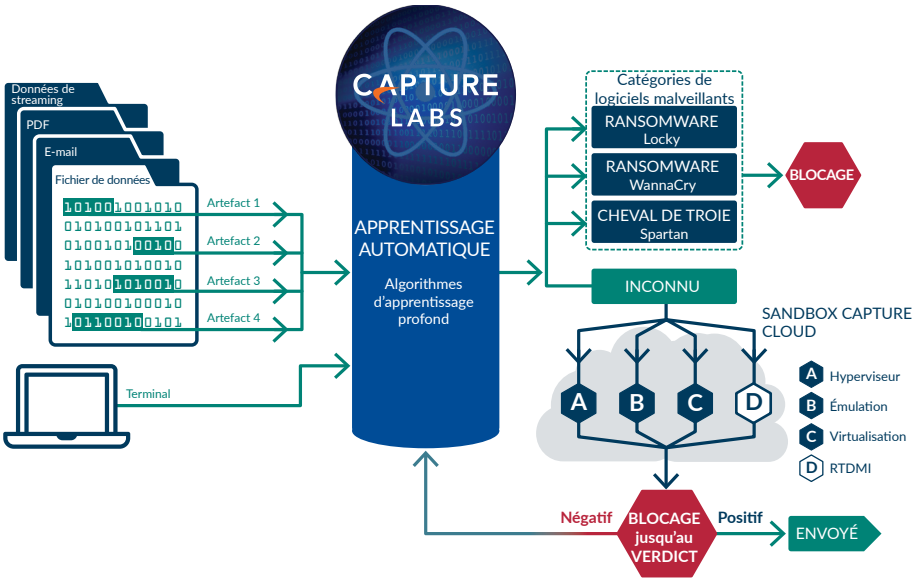
Deux technologies de détection avancée des programmes malveillants sont au cœur de la prévention des failles automatisée et en temps réel de SonicWall : Capture Advanced Threat Protection™ (Capture ATP) et Capture Security appliance™ (CSa).

Capture ATP est une plateforme basée sur le cloud et multimoteur de sandboxing qui comprend Real-Time Deep Memory Inspection™ (RTDMI), un service virtualisé de sandboxing, une émulation complète du système et une technologie d'analyse au niveau de l'hyperviseur. CSa est un dispositif local doté de RTDMI, qui emploie des techniques statiques et dynamiques basées sur la mémoire pour rendre des verdicts rapidement et précisément. Les deux solutions étendent la protection contre les menaces avancées afin de détecter et d'empêcher les menaces de type « zero-day » dans différentes solutions SonicWall, comme les pare-feu de nouvelle génération.

Les fichiers suspects sont envoyés dans l'une des solutions pour y être analysés à l'aide d'algorithmes d'apprentissage profond, avec possibilité de les retenir au niveau de la passerelle jusqu'à ce qu'un verdict soit rendu. Dans le cas de Capture ATP, lorsque les fichiers sont identifiés comme étant malveillants, ils sont bloqués et un hachage est immédiatement créé au sein de la base de données de Capture ATP pour permettre aux clients de bloquer toutes les attaques qui s'ensuivent. Ces signatures finissent par être transmises aux pare-feu pour créer des défenses statiques. Les résultats générés par CSa ne sont pas partagés en dehors de votre entreprise pour des raisons de conformité et de respect de la vie privée.

Ces services analysent un vaste éventail de systèmes d'exploitation et de types de fichiers (notamment programmes exécutables, DLL, PDF, documents MS Office, archives, JAR et APK).

Pour une protection complète des terminaux, SonicWall Capture Client allie une technologie antivirus de nouvelle génération à un service de sandboxing multimoteur basé sur le cloud, avec la possibilité d'intégrer en sus les pare-feu de SonicWall.

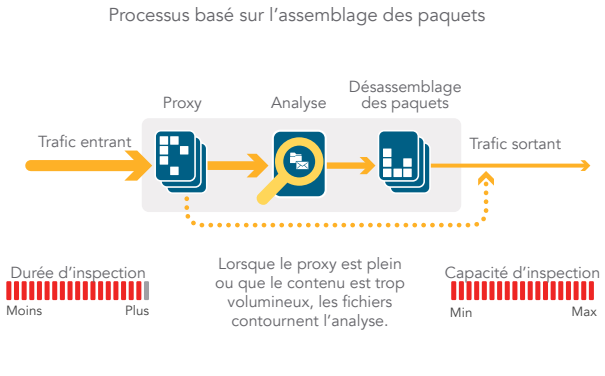


Moteur Reassembly-Free Deep Packet Inspection

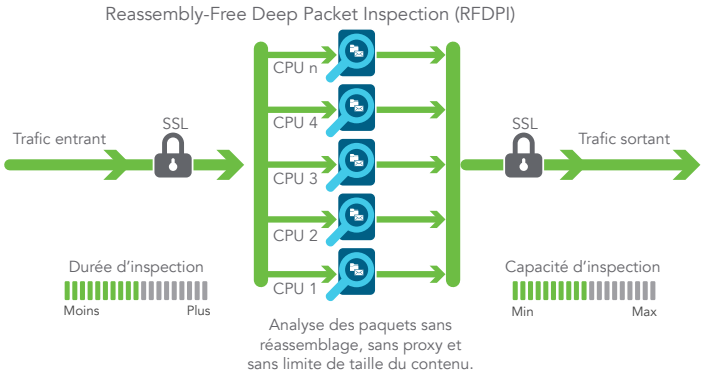
La technologie RFDPI (Reassembly-Free Deep Packet Inspection) est un système d'inspection à faible latence en un seul passage qui effectue des analyses bidirectionnelles à grande vitesse des flux de trafic sans proxy ni mise en mémoire tampon pour détecter efficacement les tentatives d'intrusion et les téléchargements de logiciels malveillants tout en identifiant le trafic applicatif, quels que soient le port ou le protocole. Ce moteur breveté s'appuie sur une inspection de la charge utile des flux de trafic pour détecter les menaces sur les couches 3 à 7 et 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 TLS/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.

Dans la plupart des cas, la connexion est interrompue et des événements de journalisation et de notification sont créés. 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 basée sur les proxys



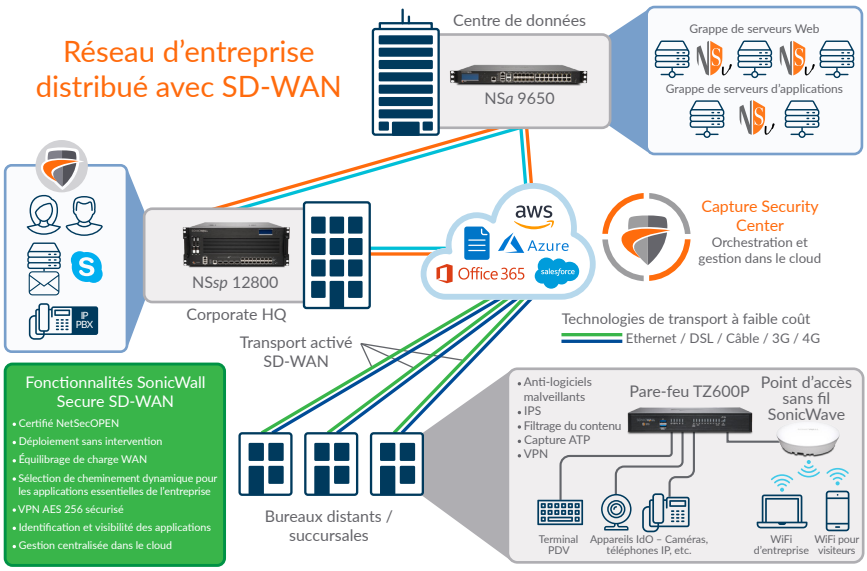
Architecture basée sur les flux SonicWall

Gestion et reporting centralisés

Pour les entreprises appartenant à des secteurs très réglementés et désireuses de coordonner parfaitement la gouvernance, la sécurité, la conformité et la stratégie de gestion des risques, SonicWall offre aux administrateurs une plateforme unifiée, sécurisée et extensible de gestion des pare-feu, points d'accès sans fil et commutateurs Dell série N et série X par le biais d'un workstream corrélé et vérifiable. Les entreprises peuvent aisément consolider la gestion des applications de sécurité, réduire les complexités administratives et de dépannage et 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, les activités des utilisateurs, l'identification des applications, l'analyse, y compris forensique, des flux, la création de rapports d'audit et de conformité et plus encore. En outre, les entreprises répondent aux exigences des pare-feu en matière de gestion des modifications via une fonctionnalité d'automatisation du workflow qui offre l'agilité et la confiance nécessaires pour déployer les règles de pare-feu appropriées, au bon moment et conformément aux réglementations de conformité. Disponibles en local avec SonicWall Global Management System et dans le cloud avec le Capture Security Center, les solutions de gestion et de reporting SonicWall offrent, plutôt qu'une approche au cas par cas, une stratégie cohérente pour 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 globaux.

Réseaux distribués

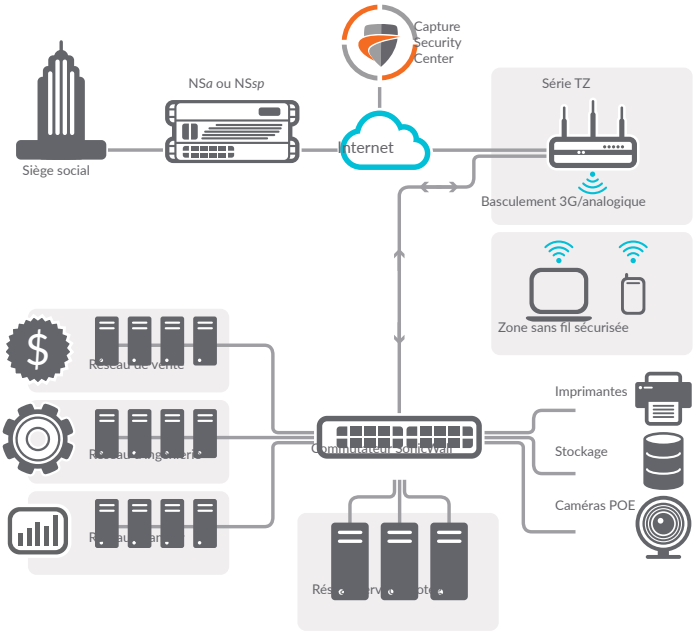
Extrêmement flexibles, les pare-feu de la série TZ conviennent parfaitement tant aux entreprises distribuées qu'aux déploiements monosites. Dans les réseaux distribués, des chaînes commerciales par exemple, chaque site dispose de son propre pare-feu TZ, qui se connecte à Internet, généralement via un fournisseur local, par DSL, câble ou liaison 3G/4G. Outre l'accès à Internet, chaque pare-feu utilise une connexion Ethernet pour transporter des paquets entre les sites distants et le siège. Les services Web et les applications SaaS telles qu'Office 365, Salesforce et autres sont servis depuis le centre de données. Via la technologie de VPN maillé, les administrateurs informatiques peuvent créer une configuration en étoile pour le transport sécurisé de données entre tous les sites.



La technologie SD-WAN de SonicOS complète à merveille les pare-feu TZ déployés sur des sites distants et dans des succursales. Au lieu de s'en remettre aux anciennes technologies, plus coûteuses, telles que MPLS ou T1, les entreprises qui utilisent le SD-WAN peuvent choisir les services moins chers de l'Internet public tout en conservant un niveau élevé de disponibilité des applications et des performances prévisibles.

Capture Security Center

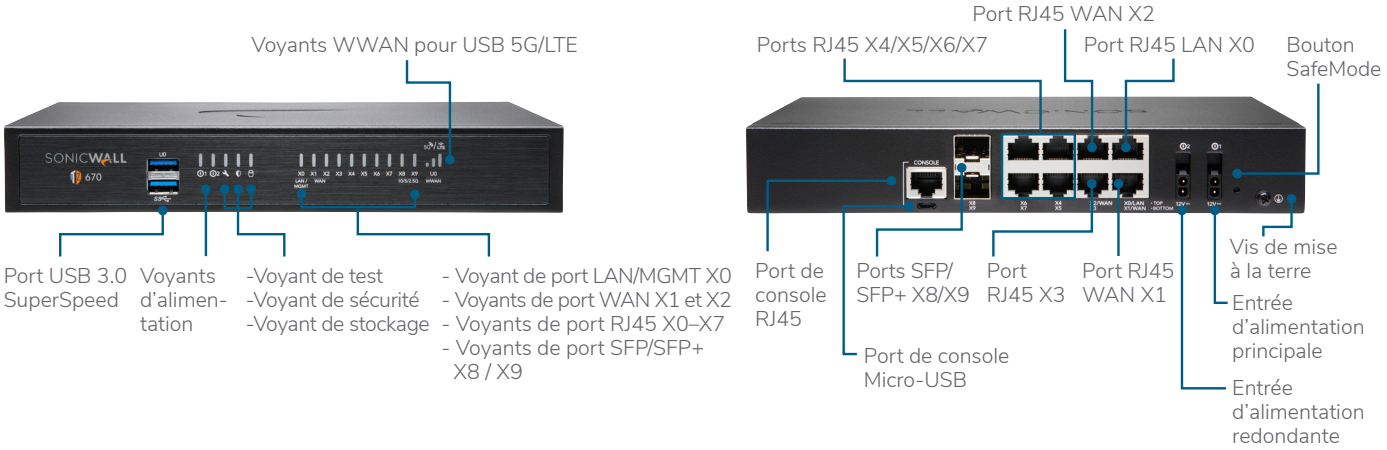
Le Capture Security Center (CSC) de SonicWall, dans le cloud, relie l'ensemble du réseau distribué, ce qui permet de centraliser le déploiement, la gestion courante et l'analyse en temps réel des pare-feu TZ. Le déploiement zéro intervention est l'une des principales fonctionnalités du CSC. La configuration et le déploiement de pare-feu sur différents sites prennent beaucoup de temps et nécessitent du personnel sur place. Le déploiement zéro intervention élimine ces problèmes, dans la mesure où les pare-feu SonicWall sont déployés et configurés à distance, dans le cloud. C'est plus simple et plus rapide. De la même manière, le CSC simplifie la gestion en continu, tous les dispositifs SonicWall du réseau étant gérés dans le cloud via un seul écran. SonicWall Analytics offre une visibilité totale, en situation, de l'environnement de sécurité réseau, un seul écran permettant de visualiser toutes les activités qui se déroulent au sein du réseau. Les entreprises comprennent mieux l'utilisation des applications et les performances, tout en limitant les risques liés à l'informatique de l'ombre, ou Shadow IT.



SonicWall Network Security Manager (NSM), un gestionnaire de pare-feu centralisé multi-locataires faisant partie de CSC, vous permet de gérer de manière centralisée toutes les opérations de pare-feu sans erreur en respectant des flux de travail vérifiables. Son moteur analytique natif offre une visibilité sur une interface unique et vous permet de surveiller et de détecter les menaces en unifiant et en mettant en corrélation les journaux de tous les pare-feu. La solution NSM vous aide également à rester en conformité grâce à une piste d'audit complète de chaque changement de configuration et à un reporting granulaire. La solution NSM s'adapte à toutes les tailles d'organisation gérant des réseaux avec des milliers de pare-feu déployés sur de nombreux sites.

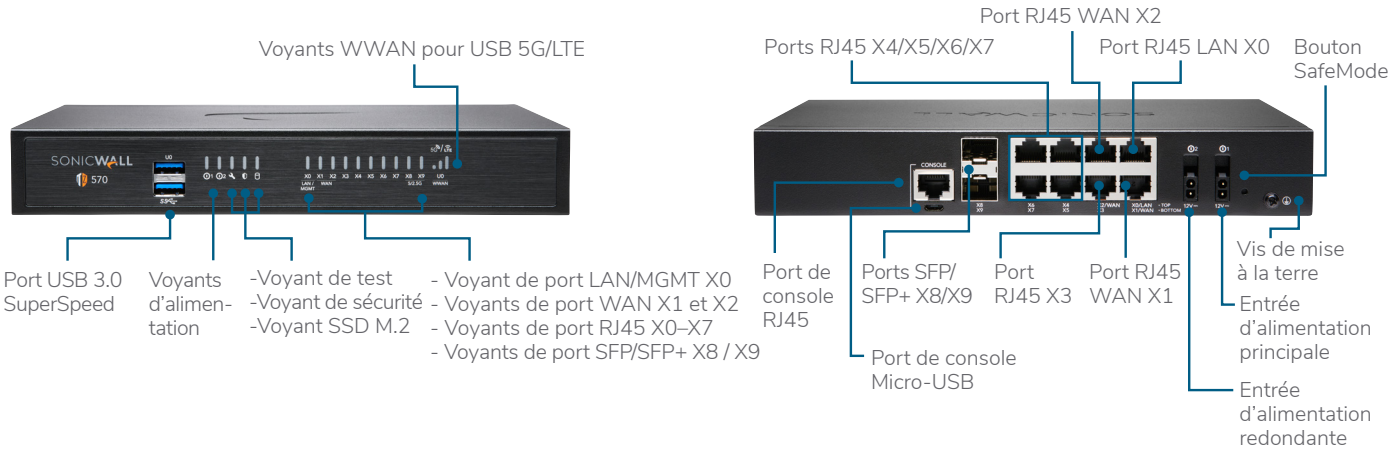
Série TZ670 de SonicWall

Conçu pour les entreprises de taille moyenne et les entreprises distribuées disposant de succursales SD-Branch, le pare-feu TZ670 combine l'efficacité de la sécurité reconnue par le secteur avec le meilleur rapport qualité-prix de sa catégorie.



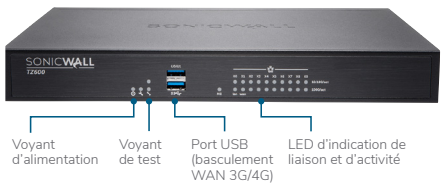
Série TZ570 de SonicWall

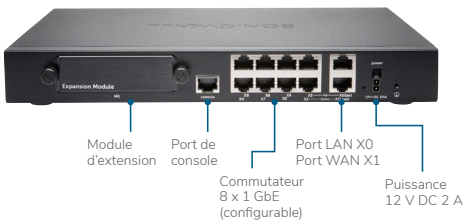
Conçu pour les PME et les entreprises distribuées disposant de succursales SD-Branch, le pare-feu TZ570 combine l'efficacité de la sécurité reconnue par le secteur avec le meilleur rapport qualité-prix de sa catégorie.

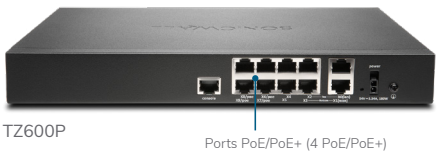


Série TZ600 de SonicWall

Le pare-feu TZ600 de SonicWall a été conçu pour les entreprises naissantes, les points de vente et les succursales recherchant la sécurité, les performances et des options telles que la prise en charge PoE+ 802.3at, le tout à un excellent rapport qualité/prix. Il sécurise les réseaux avec des fonctionnalités de niveau professionnel et des performances sans concession.

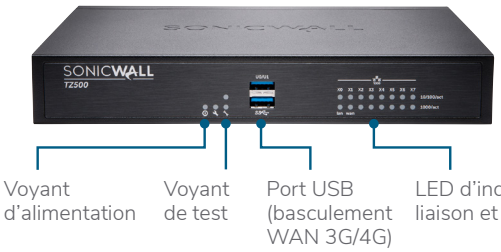


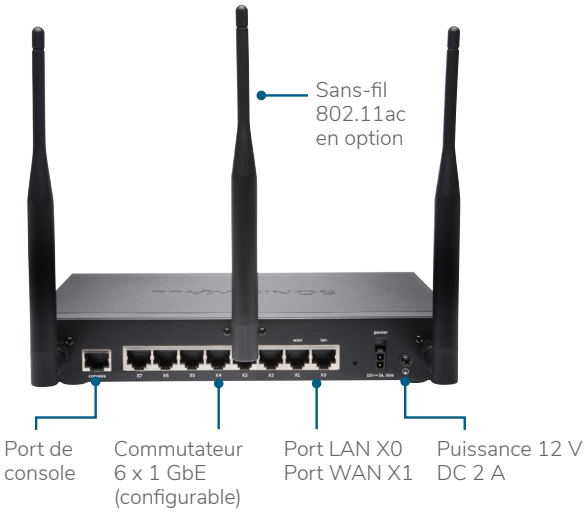




Série TZ500 de SonicWall

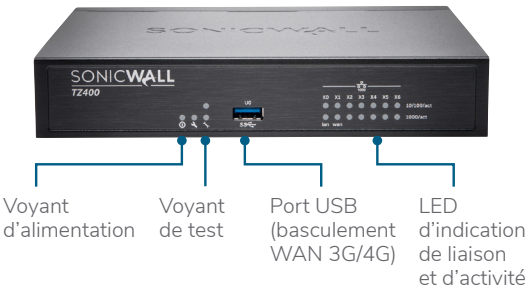
Conçu pour les succursales et les PME en pleine croissance, le pare-feu de la série TZ500 de SonicWall associe une protection extrêmement efficace et sans compromis à une productivité réseau et une connectivité sans fil double bande 802.11ac intégrée en option.

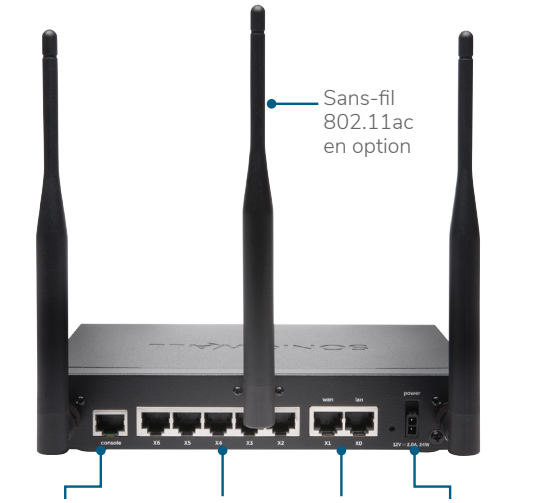




Série TZ400 de SonicWall

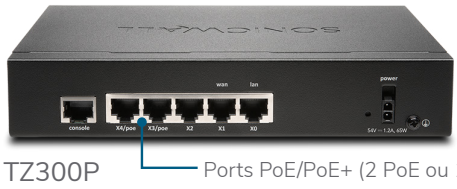
Conçu pour les petites entreprises, les points de vente au détail et les succursales, le pare-feu de la série TZ400 de SonicWall assure une protection de niveau professionnel. Des options flexibles de déploiement sans fil sont disponibles avec la connectivité sans fil 802.11ac double bande intégrée dans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

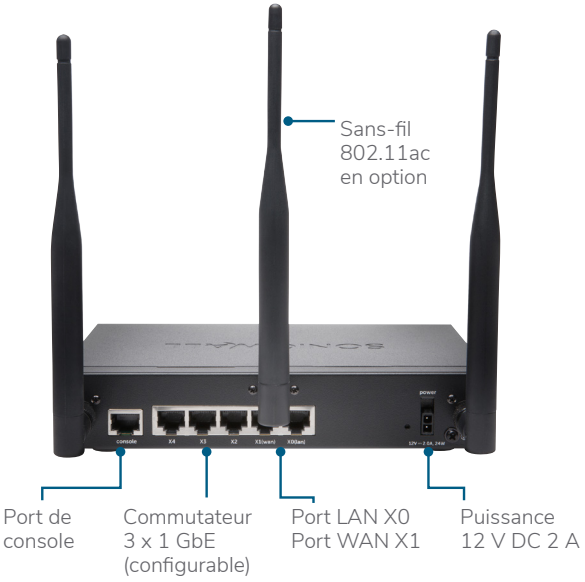




Série TZ350/TZ300 de SonicWall

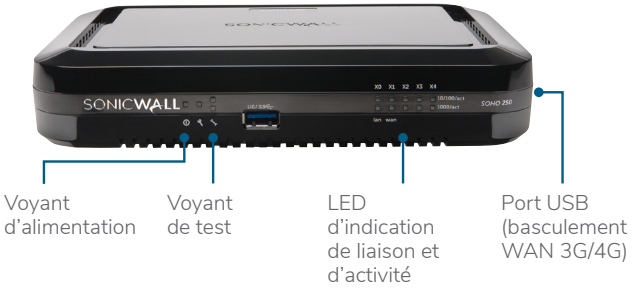
Les produits de la série TZ300 et TZ350 de SonicWall offrent une solution tout-en-un qui protège les réseaux contre les attaques avancées. Contrairement aux produits de qualité grand public, ces pare-feu UTM associent des fonctionnalités haut débit de prévention des intrusions, de protection contre les logiciels malveillants et de filtrage de contenu/d'URL, ainsi qu'une prise en charge étendue de l'accès mobile sécurisé pour les ordinateurs portables, les smartphones et les tablettes et une connectivité sans-fil 802.11ac intégrée en option. De plus, la série TZ300 propose en option une connectivité 802.3at PoE+ pour alimenter des appareils compatibles PoE.

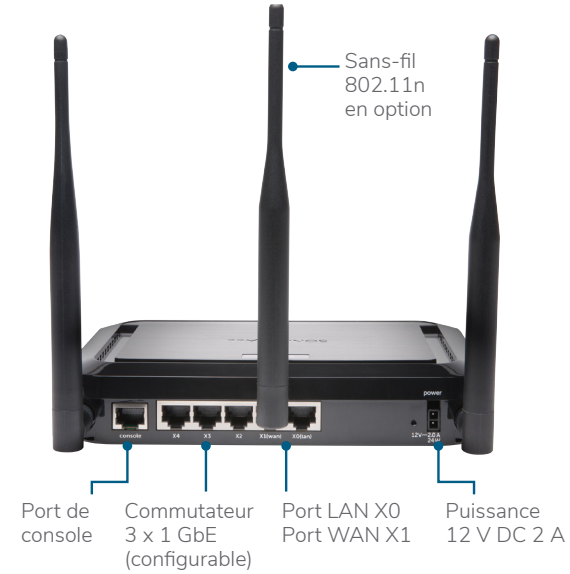




Série SOHO 250/SOHO de SonicWall

Conçus pour les environnements filaires et sans fil de petits bureaux et de bureaux à domicile, les pare-feu de la série SOHO 250 et SOHO de SonicWall offrent la protection de niveau professionnel qu'exigent les grandes entreprises à un tarif plus avantageux. Ajoutez la connectivité sans fil 802.11n en option pour fournir aux employés et clients une connectivité sans fil sécurisée.





Partenaire de services

Besoin d'aide pour planifier, déployer ou optimiser votre solution SonicWall ? Le programme avancé Partenaire de services SonicWall a pour objectif de vous fournir des services professionnels de classe mondiale. Pour en savoir plus, rendez-vous sur www.sonicwall.com/PES.

Récapitulatif des fonctionnalités de SonicOS 7.0

Pare-feu
- Inspection d'état des paquets
- Moteur RFDPI (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
- Prise en charge complète de l'API
- Intégration Switch SonicWall
- Évolutivité du SD-WAN
- Assistant d'utilisation SD-WAN[1]
- Conteneurisation SonicCoreX et SonicOS[1]
- Évolutivité des connexions (SPI, DPI, DPI SSL)

Tableau de bord amélioré[1]
- Affichage amélioré des appareils
- Résumé du trafic et des utilisateurs principaux
- Renseignements sur les menaces
- Centre de notifications

Déchiffrement et inspection TLS/SSL/SSH
- TLS 1.3 avec sécurité améliorée[1]
- Inspection approfondie des paquets pour TLS/SSL/SSH
- Inclusion/exclusion d'objets, de groupes ou de noms d'hôtes
- Contrôle SSL
- Améliorations de DPI-SSL avec CFS
- Contrôles DPI SSL granulaires par zone ou règle

Capture Advanced Threat Protection[2]
- Real-Time Deep Memory Inspection
- Analyse multimoteur 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
- Blocage jusqu'au verdict
- Capture Client

Prévention contre les intrusions[2]
- Analyse basée sur des signatures
- Mise à jour automatique des signatures
- Inspection bidirectionnelle
- Fonctionnalité de règles IPS granulaires
- Localisation GeoIP
- Filtrage de réseaux de zombies avec liste dynamique
- Détection des expressions régulières

Anti-logiciels malveillants[2]
- 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[2]
- Contrôle des applications
- 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
- Base de données complète des signatures d'applications

Visualisation et analyse du trafic
- Activité des utilisateurs
- Utilisation par les applications/bande passante/menaces
- Analyse dans le cloud

Filtrage du contenu Web HTTP/HTTPS[2]
- Filtrage des URL
- Évitement de proxy
- Blocage par mots-clés
- Filtrage à base de règles (exclusion/inclusion)
- Insertion d'en-tête HTTP
- Catégories d'évaluation CFS pour la gestion de la bande passante
- Modèle unifié de règles avec contrôle des applications
- Content Filtering Client

VPN
- SD-WAN sécurisé
- 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
- Trames Jumbo
- Découverte de cheminement MTU
- Journalisation améliorée
- Jonction VLAN
- Mise en miroir des ports (NSa 2650 et versions ultérieures)
- 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)
- NAT
- Serveur DHCP
- Gestion de la bande passante
- Haute disponibilité A/P avec synchro. d'état
- Équilibrage de la charge entrante/sortante
- Haute disponibilité – active/passive avec synchronisation d'état
- Mode pont de couche 2, mode filaire/filaire virtuel, mode TAP, mode NAT
- Routage asymétrique
- 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, surveillance et assistance
- Prise en charge de Capture Security Appliance (CSa)
- Capture Threat Assessment (CTA) v2.0
  - Nouveau design ou modèle
  - Comparaison entre la moyenne du secteur et la moyenne mondiale
- Nouvelle interface/expérience utilisateur avec fonctionnalités intuitives[1]
  - Tableau de bord
  - Informations sur les appareils, applications, menaces
  - Vue topologique
  - Création et gestion simplifiées des politiques
- Statistiques d'utilisation des politiques/objets[1]
  - Utilisation vs non-utilisation
  - Actif vs Inactif
- Recherche globale des données statiques
- Prise en charge du stockage[1]
- Gestion du stockage internet et externe[1]
- Prise en charge des cartes USB WWAN (5G/LTE/4G/3G)
- Prise en charge de Network Security Manager (NSM)
- Interface utilisateur Web
- Interface de ligne de commande
- Inscription et configuration sans intervention
- Rapports CSC simples[1]
- Prise en charge de l'application mobile SonicExpress
- SNMPv2/v3
- Gestion et reporting centralisés avec SonicWall Global Management System (GMS)[2]
- Journalisation
- Exportation NetFlow/IPFix
- Sauvegarde cloud de la configuration
- Plateforme d'analyse de sécurité BlueCoat
- Visualisation de la bande passante et des applications
- Gestion IPv4 et IPv6
- Écran de gestion CD
- Gestion des commutateurs Dell série N et série X notamment en cascade

Débogage et diagnostic
- Surveillance améliorée des paquets
- Terminal SSH sur interface utilisateur

Sans fil
- Gestion du cloud SonicWave AP
- WIDS/WIPS
- Prévention des points d'accès sauvages
- Itinérance rapide (802.11k/r/v)
- Mise en réseau maillé 802.11s
- Sélection automatique des canaux
- Analyse du spectre RF
- Vue plan de sol
- Vue topologique
- Orientation de bande
- Formation de faisceaux
- Équité du temps d'utilisation du réseau
- Bluetooth à basse consommation
- Extendeur MiFi
- Améliorations RF
- Quota cyclique invités

Modèles sans fil intégrés
- Sans fil 802.11ac Wave 2 (TZ570W)
- Double bande (2,4 GHz et 5 GHz)
- Normes sans fil 802.11 a/b/g/n/ac
- Détection et prévention sans fil des intrusions
- Services sans fil pour les invites
- Messagerie légère à point d'accès
- Segmentation des points d'accès virtuels
- Portail captif
- Cloud ACL

[1] *Nouvelle fonctionnalité de SonicOS 7.0*
[2] *Requiert un abonnement supplémentaire*

Spécifications système de la série SonicWall TZ — SOHO, SOHO 250, TZ300 et TZ350

GÉNÉRALITÉS DES PARE-FEU	SÉRIE SOHO	SÉRIE SOHO 250	SÉRIE TZ300	SÉRIE TZ350
Système d'exploitation	SonicOS			
Interfaces	5 x 1 GbE, 1 USB, 1 console		5 x 1 GbE, 1 USB, 1 console	5 x 1 GbE, 1 USB, 1 console
Prise en charge Power over Ethernet (PoE)	—	—	TZ300P – 2 ports (2 PoE ou 1 PoE+)	—
Extension	USB			
Gestion	CLI, SSH, IU Web, Capture Security Center, GMS, API REST			
Utilisateurs de l'authentification unique (SSO)	250	350	500	500
Interfaces VLAN	25			
Points d'accès pris en charge (max.)	2	4	8	8
PERFORMANCES PARE-FEU/VPN	**SÉRIE SOHO**	**SÉRIE SOHO 250**	**SÉRIE TZ300**	**SÉRIE TZ350**
Débit d'inspection du pare-feu[1]	300 Mbit/s	600 Mbit/s	750 Mbit/s	1,0 Gbit/s
Débit prévention des menaces[2]	150 Mbit/s	200 Mbit/s	235 Mbit/s	335 Mbit/s
Débit d'inspection des applications[2]	—	275 Mbit/s	375 Mbit/s	600 Mbit/s
Débit IPS[2]	200 Mbit/s	250 Mbit/s	300 Mbit/s	400 Mbit/s
Débit d'inspection des logiciels malveillants[2]	150 Mbit/s	200 Mbit/s	235 Mbit/s	335 Mbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[2]	30 Mbit/s	50 Mbit/s	60 Mbit/s	65 Mbit/s
Débit VPN IPSec[3]	150 Mbit/s	200 Mbit/s	300 Mbit/s	430 Mbit/s
Connexions par seconde	1 800	3 000	5 000	6 000
Connexions maximales (SPI)	10 000	50 000	100 000	100 000
Nombre maximum de connexions (DPI)	10 000	50 000	90 000	90 000
Connexions maximales (DPI-SSL)	250	25 000	25 000	25 000
VPN	**SÉRIE SOHO**	**SÉRIE SOHO 250**	**SÉRIE TZ300**	**SÉRIE TZ350**
Tunnels VPN site à site	10	10	10	15
Clients VPN IPSec (maximum)	1 (5)	1 (5)	1 (10)	2 (10)
Licences VPN SSL (maximum)	1 (10)	1 (25)	1 (50)	1 (75)
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)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B Cryptography			
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v			
VPN basé sur le routage	RIP, OSPF, BGP[4]			
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	**SÉRIE SOHO**	**SÉRIE SOHO 250**	**SÉRIE TZ300**	**SÉRIE TZ350**
Services d'inspection approfondie des paquets	Antivirus de passerelle, anti-logiciels espions, prévention des intrusions, DPI-SSL			
Content Filtering Service (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			
Service antispam complet	Pris en charge			
Visualisation des applications	Non	Oui	Oui	Oui
Contrôle des applications	Oui	Oui	Oui	Oui
Capture Advanced Threat Protection	Non	Oui	Oui	Oui
GESTION DE RÉSEAU	**SÉRIE SOHO**	**SÉRIE SOHO 250**	**SÉRIE TZ300**	**SÉRIE TZ350**
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)			

Spécifications système de la série SonicWall TZ — SOHO, SOHO 250, TZ300 et TZ350 (suite)

GESTION DE RÉSEAU (SUITE)	SÉRIE SOHO	SÉRIE SOHO 250	SÉRIE TZ300	SÉRIE TZ350
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, Common Access Card (CAC)	
Base de données utilisateurs locale	150			
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[5]	FIPS 140-2 (avec Suite B) niveau 2, APL UC, IPv6 (Phase 2), pare-feu réseau ICSA, antivirus ICSA, NDPP Common Criteria (pare-feu et IPS)			
Carte CAC (Common Access Card)	Pris en charge			
Haute disponibilité	Non		Active/Standby	
MATÉRIEL	**SÉRIE SOHO**	**SÉRIE SOHO 250**	**SÉRIE TZ300**	**SÉRIE TZ350**
Format	Bureau			
Alimentation électrique	24 W externe		24 W externe 65 W externe (TZ300P uniquement)	24 W externe
Consommation électrique maximale (W)	6,4/11,3	6,9/11,3	6,9/12,0	6,9/12,0
Puissance d'entrée	100 à 240 V CA, 50-60 Hz, 1 A			
Dissipation thermique totale	21,8/38,7 BTU	23,5/38,7 BTU	23,5/40,9 BTU	23,5/40,9 BTU
Dimensions	3,6 x 14,1 x 19 cm 1,42 x 5,55 x 7,48 po		3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 po	3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 po
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
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
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
Temps de fonctionnement entre deux pannes (en années)	58,9/56,1 (Wireless)	56,1	56,1	56,1
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	**SÉRIE SOHO**	**SÉRIE SOHO 250**	**SÉRIE TZ300**	**SÉRIE TZ350**
Conformité aux réglementations majeures (modèles filaires)	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TUV/GS, CB, Mexico CoC par UL, WEEE, REACH, KCC/MSIP, ANATEL		FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TUV/GS, CB, Mexico CoC par UL, WEEE, REACH, KCC/MSIP, ANATEL	
Conformité aux réglementations majeures (modèles sans fil)	FCC Classe B, FCC RF ICES Classe B, IC RF CE (RED, 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 (RED, RoHS), RCM, VCCI Classe B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH	
TECHNOLOGIE SANS FIL INTÉGRÉE	**SÉRIE SOHO**	**SÉRIE SOHO 250**	**SÉRIE TZ300**	**SÉRIE TZ350**
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[6]	802.11a : 5,180-5,825 GHz ; 802.11b/g : 2,412-2,472 GHz ; 802.11n : 2,412 à 2,472 GHz, 5,180 à 5,825 GHz		802.11a : 5,180-5,825 GHz ; 802.11b/g : 2,412-2,472 GHz ; 802.11n : 2,412-2,472 GHz, 5,180-5,825 GHz ; 802.11ac : 2,412 à 2,472 GHz, 5,180 à 5,825 GHz	

Spécifications système de la série SonicWall TZ — SOHO, SOHO 250, TZ300 et TZ350 (suite)

TECHNOLOGIE SANS FIL INTÉGRÉE	SÉRIE SOHO	SÉRIE SOHO 250	SÉRIE TZ300	SÉRIE TZ350
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			
Contrôle de puissance de transmission	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 de prévention des menaces/antivirus de passerelle/anti-logiciels espions/IPS 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. Débit de prévention des menaces mesuré en ayant activé l'antivirus de passerelle, l'anti-spyware, l'IPS et le contrôle des applications.*

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

[4] *BGP uniquement disponible sur les modèles TZ350, TZ400, TZ500 et TZ600 de SonicWall.*

[5] *FIPS et ICSA en attente d'approbation sur SOHO 250 et TZ350.*

[6] *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*

Spécifications système de la série SonicWall TZ — TZ400, TZ500 et TZ600

GÉNÉRALITÉS DES PARE-FEU	SÉRIE TZ400	SÉRIE TZ500	SÉRIE TZ600
Système d'exploitation		SonicOS	
Interfaces	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
Prise en charge Power over Ethernet (PoE)	—	—	TZ600P - 4 ports (4 PoE ou 4 PoE+)
Extension	USB	2 USB	Connecteur d'extension (à l'arrière)*, 2 USB
Gestion		CLI, SSH, IU Web, Capture Security Center, GMS, API REST	
Utilisateurs de l'authentification unique (SSO)	500	500	500
Interfaces VLAN	50	50	50
Points d'accès pris en charge (max.)	16	16	24
PERFORMANCES PARE-FEU/VPN	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
Débit d'inspection du pare-feu[1]	1,3 Gbit/s	1,4 Gbit/s	1,9 Gbit/s
Débit prévention des menaces[2]	600 Mbit/s	700 Mbit/s	800 Mbit/s
Débit d'inspection des applications[2]	1,2 Gbit/s	1,3 Gbit/s	1,8 Gbit/s
Débit IPS[2]	900 Mbit/s	1,0 Gbit/s	1,2 Gbit/s
Débit d'inspection des logiciels malveillants[2]	600 Mbit/s	700 Mbit/s	800 Mbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[2]	180 Mbit/s	225 Mbit/s	300 Mbit/s
Débit VPN IPSec[3]	900 Mbit/s	1,0 Gbit/s	1,1 Gbit/s
Connexions par seconde	6 000	8 000	12 000
Connexions maximales (SPI)	150 000	150 000	150 000
Nombre maximum de connexions (DPI)	125 000	125 000	125 000
Connexions maximales (DPI-SSL)	25 000	25 000	25 000
VPN	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
Tunnels VPN site à site	20	25	50
Clients VPN IPSec (maximum)	2 (25)	2 (25)	2 (25)
Licences VPN SSL (maximum)	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)
Chiffrement/authentification		DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B Cryptography	
Échange de clés		Groupes Diffie Hellman 1, 2, 5, 14v	
VPN basé sur le routage		RIP, OSPF, BGP	
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	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
Services d'inspection approfondie des paquets		Antivirus de passerelle, anti-logiciels espions, prévention des intrusions, DPI-SSL	
Content Filtering Service (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	
Service antispam complet		Pris en charge	
Visualisation des applications	Oui	Oui	Oui
Contrôle des applications	Oui	Oui	Oui
Capture Advanced Threat Protection	Oui	Oui	Oui
GESTION DE RÉSEAU	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE 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)	

Spécifications système de la série SonicWall TZ — TZ400, TZ500 et TZ600 (suite)

GESTION DE RÉSEAU	SÉRIE TZ400	SÉRIE TZ500	SÉRIE TZ600
Authentification	LDAP (domaines multiples), XAUTH/RADIUS, SSO, Novell, base de données utilisateurs interne, Terminal Services, Citrix, Common Access Card (CAC)		
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, IPv6 (Phase 2), pare-feu réseau ICSA, antivirus ICSA, NDPP Common Criteria (pare-feu et IPS)		
Carte CAC (Common Access Card)	Pris en charge		
Haute disponibilité	Active/Standby	Active/Standby avec synchronisation d'état	
MATÉRIEL	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
Format	Bureau		
Alimentation électrique	24 W externe	36 W externe	60 W externe 180 W externe (TZ600P uniquement)
Consommation électrique maximale (W)	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	31,3/47,1 BTU	45,9/60,5 BTU	55,1 BTU
Dimensions	3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 po	3,5 x 15 x 22,5 cm 1,38 x 5,91 x 8,86 po	3,5 x 18 x 28 cm 1,38 x 7,09 x 11,02 po
Poids	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	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	1,37 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)	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	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
Conformité aux réglementations majeures (modèles filaires)	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TUV/ GS, CB, Mexico CoC par UL, WEEE, REACH, KCC/MSIP, ANATEL	FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TÜV/ GS, CB, Mexico CoC par UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, UL, cUL, TÜV/ GS, CB, Mexico CoC par UL, WEEE, REACH, KCC/MSIP, ANATEL
Conformité aux réglementations majeures (modèles sans fil)	FCC Classe B, FCC RF ICES Classe B, IC RF CE (RED, 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 (RED, RoHS), RCM, VCCI Classe B, MIC/TELEC, UL, cUL, TÜV/ GS, CB, Mexico CoC par UL, DEEE, REACH	—

Spécifications système de la série SonicWall TZ — TZ400, TZ500 et TZ600 (suite)

TECHNOLOGIE SANS FIL INTÉGRÉE	SÉRIE TZ400	SÉRIE TZ500	SÉRIE TZ600
Normes	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 : 5,180-5,825 GHz ; 802.11b/g : 2,412-2,472 GHz ; 802.11n : 2,412-2,472 GHz, 5,180-5,825 GHz ; 802.11ac : 5,180-5,825 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 (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		—
Contrôle de puissance de transmission	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 ; 802,11ac : 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) ; 802.11ac : multiplexage par répartition orthogonale de la fréquence (OFDM)		—

Spécifications système de la série SonicWall TZ — TZ570 et TZ670

GÉNÉRALITÉS DES PARE-FEU	SÉRIE TZ570	SÉRIE TZ670
Système d'exploitation	SonicOS 7.0	
Interfaces	8 x 1 GbE, 2 x 5 GbE, 2 USB 3.0, 1 console	8 x 1 GbE, 2 x 10 GbE, 2 USB 3.0, 1 console
Prise en charge Power over Ethernet (PoE)	TZ570P (5 PoE ou 3 PoE+)	—
Extension	Connecteur d'extension de stockage (jusqu'à 256 Go)	Connecteur d'extension de stockage (jusqu'à 256 Go) (32 Go inclus)
Gestion	Network Security Manager, CLI, SSH, IU Web, GMS, API REST	
Utilisateurs de l'authentification unique (SSO)	2 500	2 500
Interfaces VLAN	256	256
Points d'accès pris en charge (max.)	32	32
PERFORMANCES PARE-FEU/VPN	**SÉRIE TZ570**	**SÉRIE TZ670**
Débit d'inspection du pare-feu[1]	4,00 Gbit/s	5,00 Gbit/s
Débit prévention des menaces[2]	2,00 Gbit/s	2,50 Gbit/s
Débit d'inspection des applications[2]	2,5 Gbit/s	3,0 Gbit/s
Débit IPS[2]	2,5 Gbit/s	3,0 Gbit/s
Débit d'inspection des logiciels malveillants[2]	2,00 Gbit/s	2,50 Gbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[2]	750 Mbit/s	800 Mbit/s
Débit VPN IPSec[3]	1,80 Gbit/s	2,10 Gbit/s
Connexions par seconde	16 000	25 000
Connexions maximales (SPI)	1 250 000	1 500 000
Nombre maximum de connexions (DPI)	400 000	500 000
Connexions maximales (DPI-SSL)	30 000	30 000
VPN	**SÉRIE TZ570**	**SÉRIE TZ670**
Tunnels VPN site à site	200	250
Clients VPN IPSec (maximum)	10 (500)	10 (500)
Licences VPN SSL (maximum)	2 (200)	2 (250)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B Cryptography	
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v	
VPN basé sur le routage	RIP, OSPF, BGP	
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 10	
NetExtender	Microsoft® Windows 10, Linux	
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome OS, Windows 10	
SERVICES DE SÉCURITÉ	**SÉRIE TZ570**	**SÉRIE TZ670**
Services d'inspection approfondie des paquets	Antivirus de passerelle, anti-logiciels espions, prévention des intrusions, DPI-SSL	
Content Filtering Service (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	
Service antispam complet	Oui	
Visualisation des applications	Oui	
Contrôle des applications	Oui	
Capture Advanced Threat Protection	Oui	
Sécurité DNS	Oui	

Spécifications système de la série SonicWall TZ — TZ570 et TZ670 (suite)

GESTION DE RÉSEAU	SÉRIE TZ570	SÉRIE TZ670
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	BGP, 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, Terminal Services, Citrix, Common Access Card (CAC)	
Base de données utilisateurs locale	250	
VoIP	H.323v1-5 complet, SIP	
Normes	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE a802.3	
Certifications en attente	FIPS 140-2 (avec Suite B) Niveau 2, IPv6 (Phase 2), pare-feu réseau ICSA, antivirus ICSA, NDPP Common Criteria (pare-feu et IPS)	

MATÉRIEL	SÉRIE TZ570	SÉRIE TZ670
Format	Bureau[5]	
Alimentation électrique	60 W externe 180 W externe (TZ570P uniquement)	60 W externe
Consommation électrique maximale (W)	13,1	13,1
Tension d'entrée et fréquence	100 à 240 V CA, 50-60 Hz	100 à 240 V CA, 50-60 Hz
Dissipation thermique totale	45,9/60,5 BTU	55,1 BTU
Dimensions	3,5 x 15 x 22,5 po 1,38 x 5,91 x 8,85 po	3,5 x 15 x 22,5 po 1,38 x 5,91 x 8,85 po
Poids	0,97 kg/2,14 lb	0,97 kg/2,14 lb
Poids DEEE	1,42 kg/3,13 lb	1,42 kg/3,13 lb
Poids avec emballage	1,93 kg/4,25 lb	1,93 kg/4,25 lb
MTBF à 25°C en années	26,1	43,9
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	SÉRIE TZ570	SÉRIE TZ670
Conformité aux réglementations majeures (modèles câblés - TZ670, TZ570)	FCC Classe B, FCC, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL/cUL, TUV/GS, CB, avis Mexico DGN par UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Classe B, FCC, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL/cUL, TUV/GS, CB, avis Mexico DGN par UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL
Conformité aux réglementations majeures (modèles sans fil - TZ570W)	FCC Classe B, FCC P15C, FCC P15E, ICES Classe B, ISED/IC, CE (RED, RoHS), C-Tick, VCCI Classe B, Japan Wireless, UL/cUL, TUV/GS, CB, avis Mexico DGN par UL, WEEE, REACH, BSMI, NCC (TW) KCC/MSIP, SRRC, ANATEL	—
Conformité aux réglementations majeures (modèles PoE - TZ570P)	FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, UL/cUL, TUV/GS, CB, avis Mexico DGN par UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	—

Spécifications système de la série SonicWall TZ — TZ570 et TZ670 (suite)

TECHNOLOGIE SANS FIL INTÉGRÉE	SÉRIE TZ570	SÉRIE TZ670
Normes	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 : 5,180-5,825 GHz ; 802.11b/g : 2,412-2,472 GHz ; 802.11n : 2,412-2,472 GHz, 5,180-5,825 GHz ; 802.11ac : 5,180-5,825 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 (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	—
Contrôle de puissance de transmission	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 ; 802,11ac : 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) ; 802.11ac : multiplexage par répartition orthogonale de la fréquence (OFDM)	—

[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 de prévention des menaces/antivirus de passerelle/anti-logiciels espions/IPS 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. Débit de prévention des menaces mesuré en ayant activé l'antivirus de passerelle, l'anti-spyware, l'IPS et le contrôle des applications.*

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

[4] *Un kit de montage sur châssis est disponible séparément.*

[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.*

Informations de commande des pare-feu de la série SonicWall TZ

Produit	Référence
SOHO 250 avec 1 an d'abonnement à TotalSecure Advanced Edition	02-SSC-1815
SOHO 250 Wireless-AC avec 1 an d'abonnement à TotalSecure Advanced Edition	02-SSC-1824
TZ300 avec 1 an d'abonnement à TotalSecure Advanced Edition	01-SSC-1702
TZ300 Wireless-AC avec 1 an d'abonnement à TotalSecure Advanced Edition	01-SSC-1703
TZ300P avec 1 an d'abonnement à TotalSecure Advanced Edition	02-SSC-0602
TZ350 avec 1 an d'abonnement à TotalSecure Advanced Edition	02-SSC-1843
TZ350 Wireless-AC avec 1 an d'abonnement à TotalSecure Advanced Edition	02-SSC-1851
TZ400 avec 1 an d'abonnement à TotalSecure Advanced Edition	01-SSC-1705
TZ400 Wireless-AC avec 1 an d'abonnement à TotalSecure Advanced Edition	01-SSC-1706
TZ500 avec 1 an d'abonnement à TotalSecure Advanced Edition	01-SSC-1708
TZ500 Wireless-AC avec 1 an d'abonnement à TotalSecure Advanced Edition	01-SSC-1709
TZ570 avec 1 an d'abonnement à TotalSecure Essential Edition	02-SSC-5651
TZ570W avec 1 an d'abonnement à TotalSecure Essential Edition	02-SSC-5649
TZ570P avec 1 an d'abonnement à TotalSecure Essential Edition	02-SSC-5653
TZ600 avec 1 an d'abonnement à TotalSecure Advanced Edition	01-SSC-1711
TZ600P avec 1 an d'abonnement à TotalSecure Advanced Edition	02-SSC-0600
TZ670 avec 1 an d'abonnement à TotalSecure Essential Edition	02-SSC-5640
Options de haute disponibilité (chaque unité doit correspondre au même modèle)	
TZ500 haute disponibilité	01-SSC-0439
TZ570 haute disponibilité	02-SSC-5694
TZ570P haute disponibilité	02-SSC-5655
TZ600 haute disponibilité	01-SSC-0220
TZ670 haute disponibilité	02-SSC-5654

Services	Référence
Pour la série SOHO 250 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 (1 an)	02-SSC-1726
Capture Advanced Threat Protection pour le pare-feu SOHO 250 (1 an)	02-SSC-1732
Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	02-SSC-1750
Service de filtrage de contenu (1 an)	02-SSC-1744
Service antispam complet (1 an)	02-SSC-1823
Support 24 h/24, 7 j/7 (1 an)	02-SSC-1720
Pour la série TZ300 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 (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 24 h/24, 7 j/7 (1 an)	01-SSC-0620
Pour la série TZ350 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 (1 an)	02-SSC-1773
Capture Advanced Threat Protection pour le pare-feu TZ350 (1 an)	02-SSC-1779
Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	02-SSC-1797
Service de filtrage de contenu (1 an)	02-SSC-1791
Service antispam complet (1 an)	02-SSC-1809
Support 24 h/24, 7 j/7 (1 an)	02-SSC-1767

Informations de commande des pare-feu de la série SonicWall TZ

Pour la série TZ400 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 (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 24 h/24, 7 j/7 (1 an)	01-SSC-0552
Pour la série TZ500 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 (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 24 h/24, 7 j/7 (1 an)	01-SSC-0476
Pour la série TZ600 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces et support 24 h/24, 7 j/7 (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 24 h/24, 7 j/7 (1 an)	01-SSC-0246
Pour la série TZ670 de SonicWall	
Essential Protection Service Suite - Capture ATP, prévention des menaces, filtrage du contenu, anti-spam et support 24 h/24, 7 j/7 (1 an)	02-SSC-5053
Capture Advanced Threat Protection pour le pare-feu TZ670 (1 an)	02-SSC-5035
Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	02-SSC-5059
Service de filtrage de contenu (1 an)	02-SSC-5047
Service antispam complet (1 an)	02-SSC-5041
Support 24 h/24, 7 j/7 (1 an)	02-SSC-5029
Pour la série TZ570 de SonicWall (TZ570)	
Essential Protection Service Suite - Capture ATP, prévention des menaces, filtrage du contenu, anti-spam et support 24 h/24, 7 j/7 (1 an)	02-SSC-5137
Capture Advanced Threat Protection pour le pare-feu TZ570 (1 an)	02-SSC-5083
Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	02-SSC-5155
Service de filtrage de contenu (1 an)	02-SSC-5119
Service antispam complet (1 an)	02-SSC-5101
Support 24 h/24, 7 j/7 (1 an)	02-SSC-5065
Pour la série TZ570 de SonicWall (TZ570W)	
Essential Protection Service Suite - Capture ATP, prévention des menaces, filtrage du contenu, anti-spam et support 24 h/24, 7 j/7 (1 an)	02-SSC-5149
Capture Advanced Threat Protection pour le pare-feu TZ570W (1 an)	02-SSC-5095
Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	02-SSC-5167
Service de filtrage de contenu (1 an)	02-SSC-5131
Service antispam complet (1 an)	02-SSC-5113
Support 24 h/24, 7 j/7 (1 an)	02-SSC-5077
Pour la série TZ570 de SonicWall (TZ570P)	
Essential Protection Service Suite - Capture ATP, prévention des menaces, filtrage du contenu, anti-spam et support 24 h/24, 7 j/7 (1 an)	02-SSC-5143
Capture Advanced Threat Protection pour le pare-feu TZ570P (1 an)	02-SSC-5089
Antivirus de passerelle, prévention des intrusions et contrôle des applications (1 an)	02-SSC-5161
Service de filtrage de contenu (1 an)	02-SSC-5125
Service antispam complet (1 an)	02-SSC-5107
Support 24 h/24, 7 j/7 (1 an)	02-SSC-5071

Accessoires	Référence
Série TZ670/570	
Alimentation FRU SonicWall série TZ670/570	02-SSC-3078
Kit de montage sur châssis SonicWall série TZ670/570	02-SSC-3112
Module de stockage SonicWall 32 Go pour la série TZ670/570	02-SSC-3114
Module de stockage SonicWall 64 Go pour la série TZ670/570	02-SSC-3115
Module de stockage SonicWall 128 Go pour la série TZ670/570	02-SSC-3116
Module de stockage SonicWall 256 Go pour la série TZ670/570	02-SSC-3117
Câble de console Micro-USB SonicWall pour la série TZ670/570	02-SSC-5173
Série TZ600/500/400/350/300, SOHO 250	
Kit de montage sur châssis SonicWall TZ600	01-SSC-0225
Alimentation FRU SonicWall série TZ600	01-SSC-0280
Kit de montage sur châssis SonicWall série TZ500	01-SSC-0438
Alimentation FRU SonicWall série TZ500	01-SSC-0437
Kit de montage sur châssis SonicWall série TZ400	01-SSC-0525
Kit de montage sur châssis SonicWall série TZ350, TZ300	01-SSC-0742
Alimentation FRU SonicWall série TZ400, TZ350, TZ300, SOHO 250, SOHO	01-SSC-0709
Alimentation FRU SonicWall TZ300 PoE	02-SSC-0613
Modules SonicWall SFP/SFP+	
10 GB-SR SFP+, module de fibre à courte portée multi-mode, sans câble	01-SSC-9785
10 GB-LR SFP+, module de fibre à longue portée mode unique, sans câble	01-SSC-9786
10 GB SFP+, cuivre avec 1 m de câble Twinax	01-SSC-9787
10 GB SFP+, cuivre avec 3 m de câble Twinax	01-SSC-9788
10 GB-SX SFP, module de fibre à courte portée multi-mode, sans câble	01-SSC-9789
10 GB-LX SFP, module de fibre à longue portée mode unique, sans câble	01-SSC-9790
1GB-RJ45 SFP, module cuivre, sans câble	01-SSC-9791
SonicWall SFP+ 10GBASE-T, transmetteur cuivre, module RJ45	02-SSC-1874

Numéros de modèles réglementaires

SOHO/SOHO Wireless	APL31-0B9/APL41-0BA
SOHO 250/SOHO 250 Wireless	APL41-0D6/APL41-0BA
TZ300/TZ300 Wireless/TZ300P	APL28-0B4/APL28-0B5/APL47-0D2
TZ350/TZ350 Wireless	APL28-0B4/APL28-0B5
TZ400/TZ400 Wireless	APL28-0B4/APL28-0B5
TZ500/TZ500 Wireless	APL29-0B6/APL29-0B7
TZ600/TZ600P	APL30-0B8/APL48-0D3
TZ670	APL62-0F7
TZ570/ TZ570W/ TZ570P	APL62-0F7/APL62-0F8/APL63-0F9

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour en savoir plus, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

Datasheet-TZSeries-US-KJ-2126