Série TZ de SonicWall

Prévention des menaces intégrée et plateforme SD-WAN pour les PME et les entreprises distribuées

La série TZ de SonicWall 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. SonicOS comporte 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 et la prise en charge de la norme IEEE ac 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) – caméras IP, téléphones, imprimantes...–, les TZ300P et TZ600P 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 moins de 100 nanosecondes. En parallèle, notre moteur RFDPI (Reassembly-Free 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

Avantages :

Solution de sécurité intégrée, flexible

- SD-WAN sécurisé
- Puissant système d'exploitation SonicOS
- Fonctionnalité sans fil 802.11ac haut débit
- Power over Ethernet (PoE/PoE+)
- Segmentation du réseau à l'aide de VLAN

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
- Prévention des intrusions intégrée et basée sur le cloud
- Déchiffrement et inspection TLS/SSL
- Efficacité de la sécurité reconnue par le secteur
- Équipe de recherche sur les menaces Capture Labs dédiée
- Sécurité des terminaux avec Capture Client

Facilité de déploiement, de configuration et de gestion continue

- Déploiement sans intervention
- Gestion centralisée dans le cloud et sur site
- Gamme évolutive de pare-feu
- Faible coût total de possession

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.

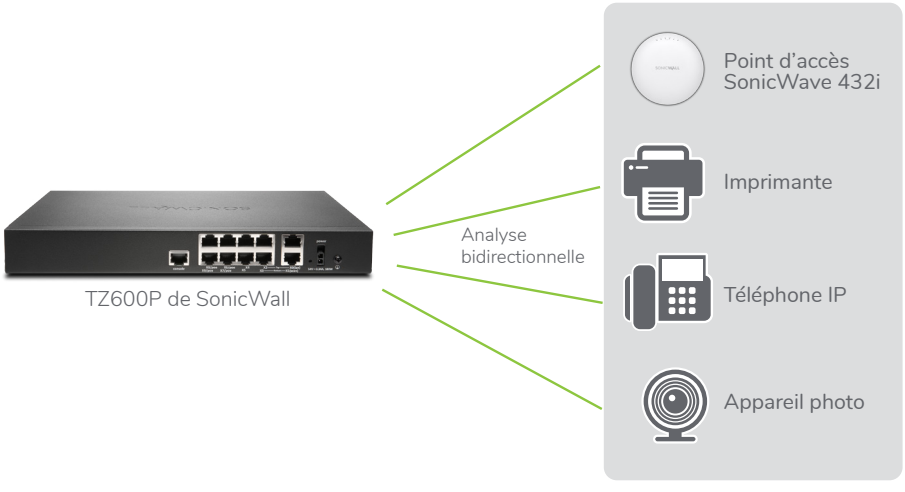
Le chiffrement ayant tendance à se généraliser pour sécuriser les sessions Web, les pare-feu doivent impérativement être en mesure de traquer les menaces dans le trafic chiffré. Les pare-feu de la série TZ de SonicWall offrent une protection complète, quel que soit le port ou le protocole, en déchiffrant 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.

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*



Alimentation et sécurité intégrées pour vos appareils compatibles PoE

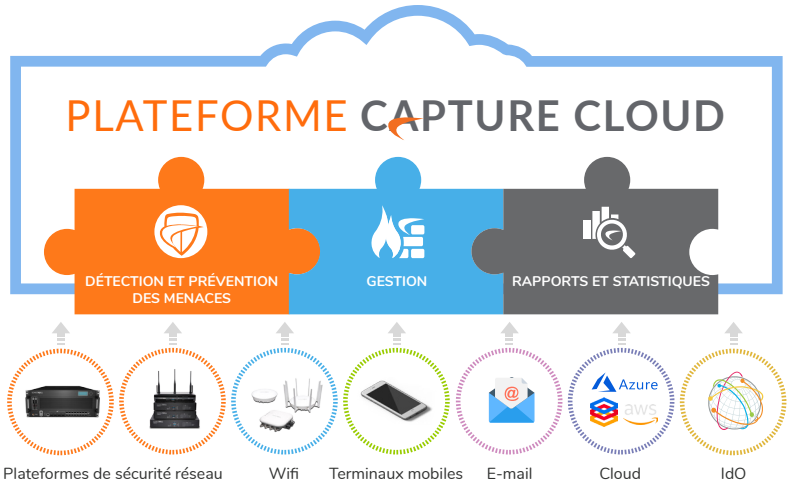
Alimentez vos appareils compatibles PoE sans avoir à payer ni vous encombrer d'un connecteur ou d'un injecteur PoE (Power over Ethernet). Les pare-feu TZ300P et TZ600P intègrent la technologie IEEE 802.3at permettant d'alimenter les appareils PoE et PoE+ : points d'accès sans fil, caméras, téléphones 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 nouvelles mises à jour prennent effet immédiatement, sans redémarrage ni interruption de service. Les signatures présentes sur l'appliance 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'appliance 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.

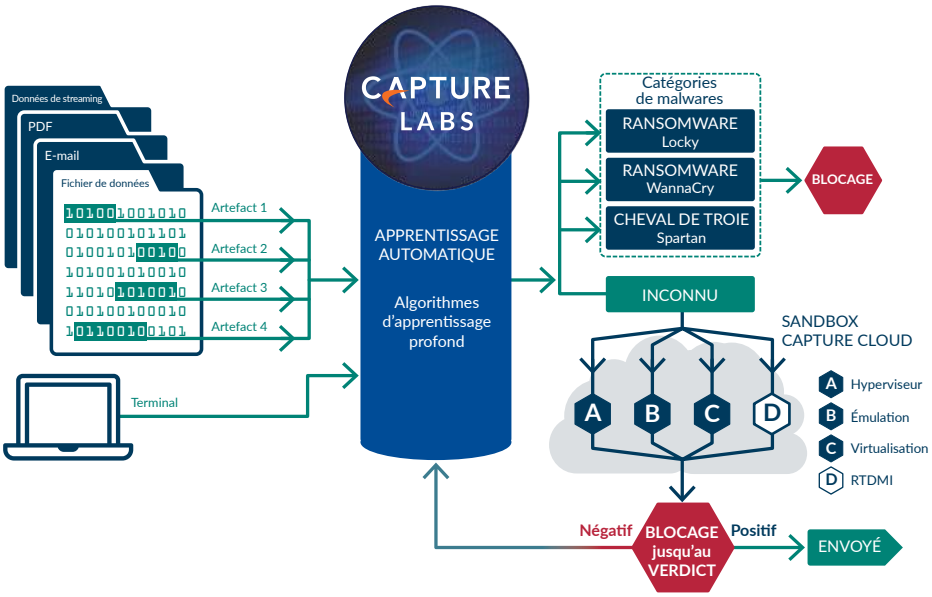


Protection contre les menaces évoluées

Au centre de la solution de prévention automatisée des failles en temps réel SonicWall, le service SonicWall Capture Advanced Threat Protection est une sandbox multimoteur cloud qui complète le travail de protection du pare-feu en détectant et en évitant les attaques zero-day. Les fichiers suspects sont envoyés dans le Cloud pour y être analysés à l'aide d'algorithmes d'apprentissage profond, avec possibilité de les retenir à la passerelle jusqu'à ce qu'un verdict soit rendu. La plateforme sandbox multimoteur, qui inclut l'inspection approfondie de la mémoire en temps réel, 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. Lorsqu'un fichier est identifié comme étant malveillant, il est bloqué et un hachage est immédiatement créé dans Capture ATP. Peu après, une signature est envoyée aux pare-feu afin d'empêcher toute infiltration plus poussée.

Le service analyse 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 une sandbox multimoteur cloud.



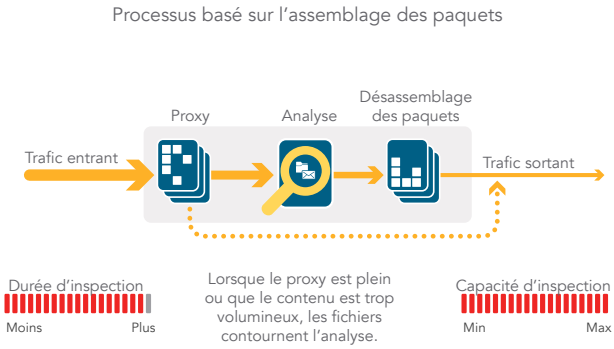
SONICWALL®

Moteur Reassembly-Free Deep Packet Inspection

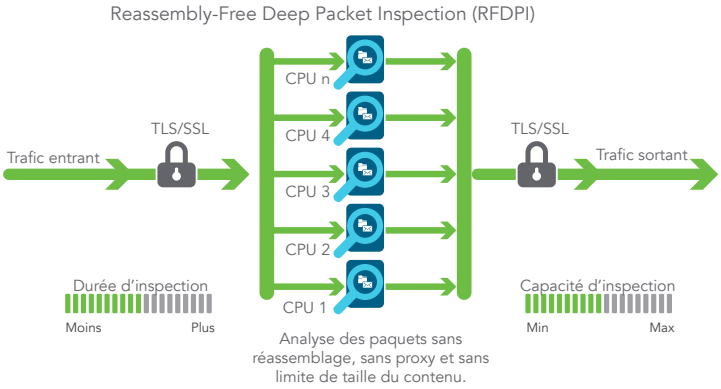
La technologie RFDPI (Reassembly-Free Deep Packet Inspection) est un système d'inspection à faible latence en un seul passage qui effectue des analyses bidirectionnelles à grande vitesse des flux de trafic sans proxy ni mise en mémoire tampon pour détecter efficacement les tentatives d'intrusion et les téléchargements de logiciels malveillants tout en identifiant le trafic applicatif, quel que soit 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



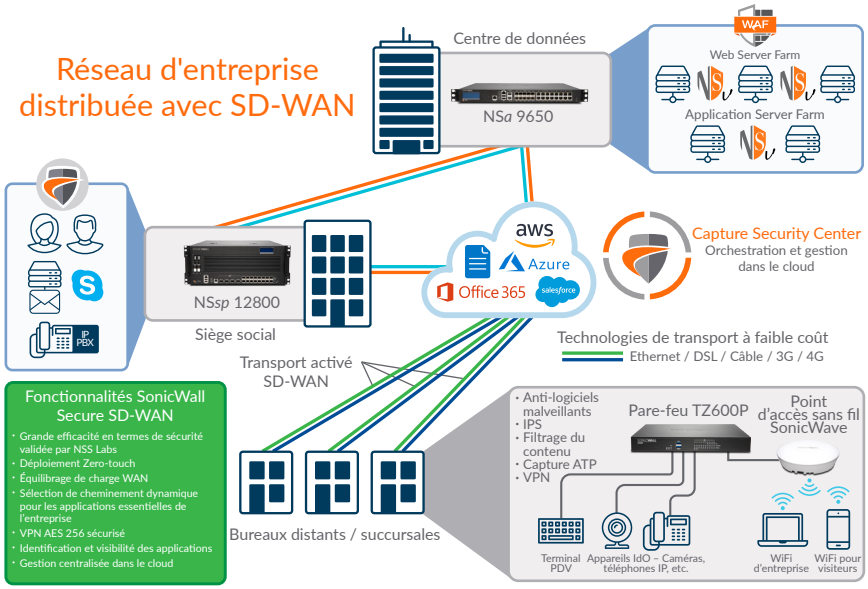
Architecture basée sur les flux SonicWall

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 appliances 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

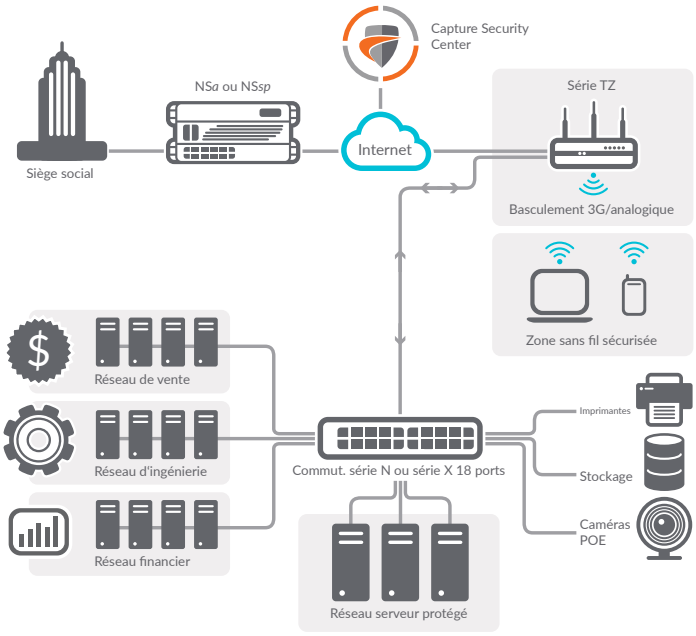
Extrêmement flexibles, les pare-feu de la série TZ conviennent parfaitement tant aux entreprises distribuées qu'aux déploiements monosites. Dans les réseaux distribués, des chaînes commerciales par exemple, chaque site dispose de son propre pare-feu TZ, qui se connecte à Internet, généralement via un 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.



Sites uniques

Pour les déploiements monosites, une solution de sécurité réseau intégrée présente de grands avantages. Les pare-feu de la série TZ allient une sécurité haute efficacité à des options telles que le sans-fil 802.11ac intégré et, dans le cas des TZ300P et TZ600P, la prise en charge PoE/PoE+. Ils reposent sur le même moteur de sécurité présent dans nos produits de milieu de gamme de la série NSa et haut de gamme de la série NSsp, et bénéficient du riche éventail de fonctionnalités de SonicOS. L'interface utilisateur intuitive de SonicOS assure une configuration et une gestion simples. Le design compact permet en outre aux entreprises d'économiser une place précieuse.

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.

Caractéristiques	Série TZ600
Débit du pare-feu	1,9 Gbit/s
Débit prévention des menaces	800 Mbit/s
Débit d'inspection des logiciels malveillants	800 Mbit/s
Débit IPS	1,2 Gbit/s
Connexions maximales	150 000
Nouvelles connexions/s	12 000

TZ600P

Ports PoE/PoE+ (4 PoE/PoE+)

Voyant d'alimentation

Voyant de test

Port USB (basculement WAN 3G/4G)

LED d'indication de liaison et d'activité

Module d'extension

Port de console

Commutateur 8 x 1 GbE (configurable)

Port LAN X0
Port WAN X1

Puissance 12 V DC 2 A

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.

Caractéristiques	Série TZ500
Débit du pare-feu	1,4 Gbit/s
Débit prévention des menaces	700 Mbit/s
Débit d'inspection des logiciels malveillants	700 Mbit/s
Débit IPS	1,0 Gbit/s
Connexions maximales	150 000
Nouvelles connexions/s	8 000

Voyant d'alimentation

Voyant de test

Port USB (basculement WAN 3G/4G)

LED d'indication de liaison et d'activité

Sans-fil 802.11ac en option

Port de console

Commutateur 6 x 1 GbE (configurable)

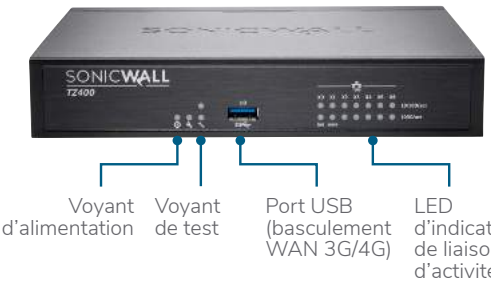
Port LAN X0
Port WAN X1

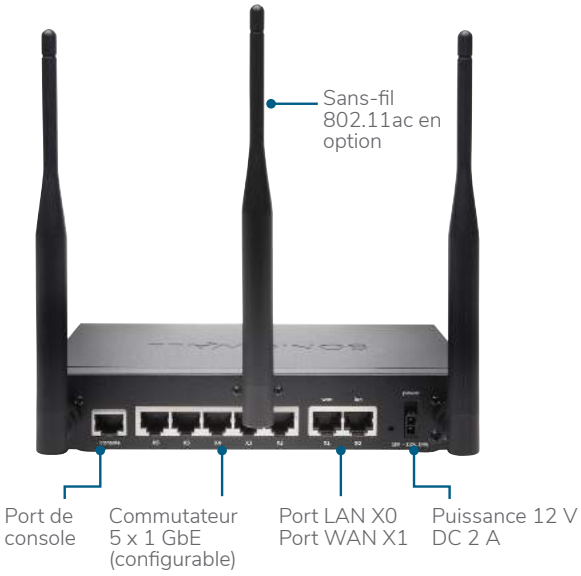
Puissance 12 V DC 2 A

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.

Caractéristiques	Série TZ400
Débit du pare-feu	1,3 Gbit/s
Débit prévention des menaces	600 Mbit/s
Débit d'inspection des logiciels malveillants	600 Mbit/s
Débit IPS	900 Mbit/s
Connexions maximales	150 000
Nouvelles connexions/s	6 000

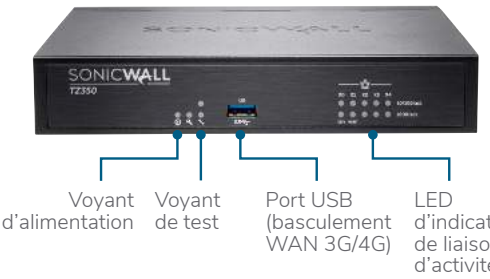


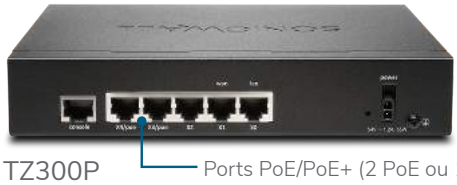


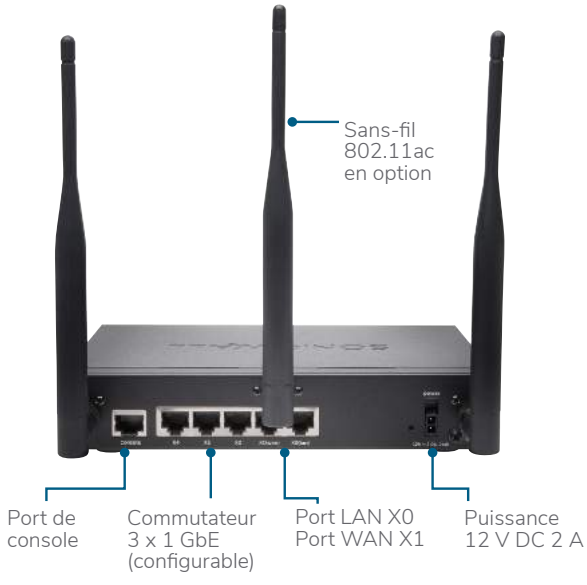
Série TZ350/TZ300 de SonicWall

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.

Caractéristiques	Série TZ350	Série TZ300
Débit du pare-feu	1,0 Gbit/s	750 Mbit/s
Débit prévention des menaces	335 Mbit/s	235 Mbit/s
Débit d'inspection des logiciels malveillants	300 Mbit/s	200 Mbit/s
Débit IPS	400 Mbit/s	300 Mbit/s
Connexions maximales	100 000	100 000
Nouvelles connexions/s	6 000	5 000







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.

Caractéristiques	Série SOHO 250	Série SOHO
Débit du pare-feu	600 Mbit/s	300 Mbit/s
Débit prévention des menaces	200 Mbit/s	150 Mbit/s
Débit d'inspection des logiciels malveillants	100 Mbit/s	50 Mbit/s
Débit IPS	250 Mbit/s	100 Mbit/s
Connexions maximales	50 000	10 000
Nouvelles connexions/s	3 000	1 800

Voyant d'alimentation
Voyant de test
LED d'indication de liaison et d'activité
Port USB (basculement WAN 3G/4G)

Sans-fil 802.11n en option

Port de console
Commutateur 3 x 1 GbE (configurable)
Port LAN X0
Port WAN X1
Puissance 12 V DC 2 A

Partner Enabled Services

Besoin d'aide pour planifier, déployer ou optimiser votre solution SonicWall ? Les partenaires SonicWall Advanced Services sont spécialement formés pour vous offrir des services professionnels de premier ordre. Pour en savoir plus, rendez-vous sur www.sonicwall.com/PES.

Fonctionnalités

MOTEUR RFDPI	
Fonctionnalité	**Description**
Reassembly-Free Deep Packet Inspection (RFDPI)	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 basée sur les flux	Cette technologie d'inspection sans proxy et sans mise en mémoire tampon offre des performances à ultra faible latence pour l'inspection DPI de millions de flux réseau simultanés, sans limite de taille des flux et des fichiers. Elle peut en outre être appliquée à des protocoles courants, ainsi qu'aux flux TCP bruts.
Hautement parallèle et extensible	La conception unique du moteur RFDPI fonctionne de concert avec l'architecture multicœurs pour fournir un haut débit DPI et des taux d'établissement de nouvelles sessions extrêmement élevés afin de gérer les pics de trafic sur les réseaux exigeants.
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.

PARE-FEU ET GESTION DE RÉSEAU	
Fonctionnalité	**Description**
SD-WAN sécurisé	Plus économique que les technologies telles que MPLS, le SD-WAN sécurisé permet aux entreprises distribuées de mettre en place, de gérer et d'exploiter en toute sécurité des réseaux hautes performances sur des sites distants, et de partager ainsi des données, des applications et des services par le biais de services Internet publics à faible coût et facilement accessibles.
API REST	Permet au pare-feu de recevoir tout type de flux de renseignements propriétaires, d'OEM ou de fournisseurs tiers et de les exploiter pour combattre les menaces évoluées : zero-day, initié malveillant, identifiants compromis, ransomwares et menaces persistantes avancées.
Inspection stateful des paquets	Tout le trafic réseau est inspecté, analysé et mis en conformité avec les règles d'accès du pare-feu.
Mise en cluster/haute disponibilité	Les modèles TZ500 et TZ600 de SonicWall prennent en charge la haute disponibilité et la configuration Active/Standby avec synchronisation d'état. Les modèles TZ300 et TZ400 SonicWall prennent en charge la haute disponibilité sans synchronisation Active/Standby. Les modèles SonicWall SOHO n'offrent pas la haute disponibilité.
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. Par ailleurs, elle offre la possibilité de se prémunir contre les attaques DoS/DDoS via la protection contre les inondations UDP/ICMP et la limitation du débit de connexion.
Prise en charge IPv6	Le protocole IPv6 (Internet Protocol version 6) commence à remplacer le protocole IPv4. Avec le système d'exploitation SonicOS, le matériel prendra en charge les implémentations en mode filaire et filtrage.
Options de déploiement flexibles	La série TZ peut être déployée en mode NAT traditionnel, pont de couche 2, filaire et TAP réseau.
Équilibrage de charge WAN	Équilibre la charge de plusieurs interfaces WAN à l'aide des méthodes Round Robin, Spillover ou Percentage.
Qualité de service avancée (QoS)	Protège les communications critiques avec le marquage 802.1p et DSCP, ainsi que le remappage du trafic VoIP sur le réseau.
Prise en charge des proxys SIP et des contrôleurs d'accès H.323	Bloque les appels indésirables en exigeant que tous les appels entrants soient autorisés et authentifiés par un contrôleur d'accès H.323 ou un proxy SIP.
Gestion des commutateurs Dell série N et série X uniques et en cascade	Gérez les paramètres de sécurité de ports supplémentaires, notamment les ports Portshield, HA, PoE et PoE+, sur un seul écran, via le tableau de bord de gestion des pare-feu pour les commutateurs réseau Dell série N ou série X (non disponible sur le modèle SOHO).
Authentification biométrique	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.
Authentification ouverte et social login	Permet aux utilisateurs invités d'utiliser leurs identifiants sur les services de réseaux sociaux comme Facebook, Twitter ou Google+ pour se connecter et accéder à Internet et à d'autres services invités par le biais de zones sans fil, LAN ou DMZ d'un hôte en utilisant l'authentification directe.
Sécurité du réseau sans fil	Disponible en option intégrée sur les pare-feu TZ300 à TZ500 SonicWall, 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. La technologie 802.11 a/b/g/n en option est disponible sur les modèles SonicWall SOHO.

GESTION ET CRÉATION DE RAPPORTS	
Fonctionnalité	**Description**
Gestion dans le cloud et sur site	La configuration et la gestion des appliances SonicWall peuvent se faire dans le cloud via le SonicWall Capture Security Center ou sur site avec SonicWall Global Management System (GMS).
Gestion puissante avec un seul appareil	L'interface Web intuitive offre une interface de ligne de commande complète, prend en charge le protocole SNMPv2/3 et permet une configuration rapide et pratique.
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 des 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-feu distribués en automatisant la configuration initiale de la passerelle VPN site à site entre les pare-feu 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 à la série TZ de servir de concentrateur 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 accéder simplement à la messagerie électronique, aux fichiers, ordinateurs, pages intranet et applications depuis un vaste éventail de 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	Fournit les données d'identification et d'activité des utilisateurs grâce à l'intégration transparente des services SSO AD/LDAP/Citrix1/Terminal Services1 associée aux nombreuses informations obtenues par l'inspection approfondie des paquets.
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. Permet de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP. Supprime le filtrage indésirable des adresses IP dû à une classification erronée.
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. Permet de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP.
CAPTURE ADVANCED THREAT PROTECTION	
Fonctionnalité	Description
Service de sandbox multimoteur	La plateforme sandbox multimoteur, 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.
Real-Time Deep Memory Inspection (RTDMI)	Cette technologie Cloud en instance de brevet détecte et bloque les logiciels malveillants qui n'affichent aucun comportement malveillant mais masquent leur arsenal via le chiffrement. En obligeant les logiciels malveillants à révéler leur arsenal en mémoire, le moteur RTDMI détecte et bloque de manière proactive les menaces zero-day grand public et les malwares inconnus.
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.
Analyse de nombreux types de fichiers de toute taille	Ce service assure l'analyse d'un vaste éventail de fichiers, individuellement ou en groupe, 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 OS X 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-feu ayant un abonnement à SonicWall Capture ATP, 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.
Capture Client	Capture Client est une plateforme client unifiée fournissant diverses fonctionnalités de protection des terminaux, dont une protection anti-malware avancée et la visibilité sur le trafic chiffré. Elle repose sur des technologies de protection multicouche, un reporting complet et l'exécution automatique de la protection des terminaux.
PROTECTION CONTRE LES MENACES CHIFFRÉES	
Fonctionnalité	Description
Déchiffrement et inspection TLS/SSL	Déchiffre et inspecte le trafic chiffré TLS/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 dans le trafic chiffré. Inclus avec les abonnements de sécurité pour tous les modèles de la série TZ, 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 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.

PRÉVENTION CONTRE LES INTRUSIONS (SUITE)	
Fonctionnalité	Description
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 anti-malware Capture Cloud	Les serveurs cloud SonicWall hébergent une base de données contenant des dizaines de 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-feu sur le terrain dotés de services de sécurité actifs et prennent effet immédiatement, sans redémarrage ni interruption.
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 plusieurs milliers de 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 HTTP/HTTPS contenant des informations ou des images répréhensibles ou non productives via Content Filtering Service et Content Filtering Client.
Client de filtrage de contenu renforcé	Étend l'application des règles pour bloquer les contenus Internet des appareils Windows, Mac OS, Android et Chrome situés hors du périmètre du pare-feu.
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.
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 le bon logiciel antivirus et/ou un certificat DPI-SSL installé et actif, éliminant ainsi les coûts couramment liés à la gestion des antivirus 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.
Antivirus de nouvelle génération	Capture Client utilise un moteur statique d'intelligence artificielle (IA) pour identifier des menaces avant qu'elles ne puissent s'exécuter et pour revenir à un état précédant l'infection.
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.

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 REST

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 TLS/SSL
- Contrôles DPI SSL granulaires par zone ou règle

Capture Advanced Threat Protection[1,2]
- 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[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

Anti-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
- 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[1]
- Filtrage des URL
- Technologie anti-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
- 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
- SD-WAN sécurisé
- 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 Web
- Interface de ligne de commande
- SNMPv2/v3
- Gestion et reporting centralisés avec SonicWall GMS et Capture Security Center
- 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 N et série X notamment en cascade[2]

Technologie sans fil intégrée
- Double bande (2,4 GHz et 5 GHz)
- Normes sans fil 802.11 a/b/g/n/ac[2]
- WIDS/WIPS
- 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 modèles SOHO/SOHO Wireless*
[3] *Haute disponibilité avec synchronisation d'état disponible uniquement sur les modèles TZ500 et TZ600 de SonicWall*

Spécifications système des pare-feu de la série TZ de SonicWall

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]	100 Mbit/s	250 Mbit/s	300 Mbit/s	400 Mbit/s
Débit d'inspection des logiciels malveillants[2]	50 Mbit/s	100 Mbit/s	200 Mbit/s	300 Mbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[2]	30 Mbit/s	40 Mbit/s	50 Mbit/s	65 Mbit/s
Débit VPN IPSec[3]	100 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
Nb max. 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)	1 (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			
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	**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			
Comprehensive Anti-Spam Service	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)			

Caractéristiques des pare-feu de la série TZ de SonicWall (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	FIPS 140-2 (avec Suite B) niveau 2, APL UC, VPNC, IPv6 (Phase 2), pare-feu réseau ICSA, antivirus ICSA			
Certifications en attente	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			
Bloc d'alimentation	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 by UL, WEEE, REACH, KCC/MSIP		FCC Classe B, ICES Classe B, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP	
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	
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[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		802.11a : 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 : 2,412-2,472 GHz, 5,180-5,825 GHz	

Spécifications système des pare-feu de la série TZ de SonicWall (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 TZ400, TZ500 et TZ600 de SonicWall.*

[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*

Spécifications système des pare-feu de la série TZ de SonicWall (suite)

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]	150 Mbit/s	200 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
Nb max. 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		
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	**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		
Comprehensive Anti-Spam Service	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		

Spécifications système des pare-feu de la série TZ de SonicWall (suite)

Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1e (WMM)		
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, VPNC, IPv6 (Phase 2), pare-feu réseau ICSA, antivirus ICSA		
Certifications en attente	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		
Bloc d'alimentation	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 by UL, WEEE, 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
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	—

Spécifications système des pare-feu de la série TZ de SonicWall (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 : 2,412-2,472 GHz, 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 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 ; 802.11ac : 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)		—

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

Produit	Référence
SOHO avec 1 an d'abonnement à TotalSecure	01-SSC-0651
SOHO Wireless-N avec 1 an d'abonnement à TotalSecure	01-SSC-0653
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
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
Options de haute disponibilité (chaque unité doit correspondre au même modèle)	
TZ500 haute disponibilité	01-SSC-0439
TZ600 haute disponibilité	01-SSC-0220

Services	Référence
Pour la série SOHO de SonicWall	
Comprehensive Gateway Security Suite - Prévention des menaces, filtrage du contenu et support 24 h/24, 7 j/7 (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 24 h/24, 7 j/7 (1 an)	01-SSC-0700
Pour la série SOHO 250 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces, filtrage du contenu 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, filtrage du contenu 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

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

Pour la série TZ350 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces, filtrage du contenu 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
Pour la série TZ400 de SonicWall	
Advanced Gateway Security Suite - Capture ATP, prévention des menaces, filtrage du contenu 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, filtrage du contenu 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, filtrage du contenu 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

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

À propos de SonicWall

Depuis plus de 27 ans, SonicWall lutte contre la cybercriminalité pour défendre les PME, les grandes entreprises et les agences gouvernementales du monde entier. S'appuyant sur les travaux de recherche des Capture Labs de SonicWall, nos solutions primées de détection et de prévention des intrusions en temps réel sécurisent plus d'un million de réseaux et leurs e-mails, applications et données dans plus de 215 pays et territoires. Ces entreprises peuvent ainsi fonctionner plus efficacement sans crainte pour leur sécurité. Pour en savoir plus, rendez-vous sur www.sonicwall.com ou suivez-nous sur Twitter, LinkedIn, Facebook et Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
États-Unis
Veuillez consulter notre site Web pour obtenir des informations complémentaires.
www.sonicwall.com

Datasheet-TZ Series-US-VG-MKTG5144