SonicWALL série TZ

ACCÈS DISTANT SÉCURISÉ

Gestion unifiée des menaces

- Fondée sur l'architecture de sécurité éprouvée de SonicOS, la série TZ assure des services **hautement efficaces de protection anti-malware et de prévention des intrusions** pour maintenir les réseaux à l'abri des menaces sophistiquées modernes.
- **L'accès distant VPN SSL hautement sécurisé** est disponible en natif sur les appareils équipés d'Apple iOS, Google Android, Windows, Mac OS et Linux, permettant d'exploiter pleinement tout le potentiel du personnel mobile.
- Le filtrage de contenu et d'URL SonicWALL **bloque diverses catégories de contenu Web indésirable,** permettant de garantir un niveau élevé de productivité tout en réduisant les risques d'engagement de la responsabilité.
- Facile à comprendre et rapidement installée, l'interface utilisateur de la série TZ **ne donne plus à choisir entre convivialité et puissance,** réduisant ainsi le coût total de possession.

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

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

La série TZ inclut des fonctionnalités évoluées de mise en réseau : VPN IPSec et VPN SSL, basculement multi-FAI, équilibrage de charge, sans-fil 802.11n intégré en option et segmentation du réseau, ainsi que la conformité PCI. Les pare-feu UTM de la série TZ sont les seuls à fournir un client natif d'accès distant VPN pour Apple® iOS, Google® Android™, Windows, Mac OS et Linux. Unique en son genre, ce client prend également en charge la fonctionnalité Clean VPN™ conçue pour décontaminer le trafic VPN de toute menace. Garant de la meilleure sécurité pour les plates-formes mobiles, SonicWALL est le seul à fournir une analyse anti-malware complète du trafic chiffré en SSL et le contrôle des applications pour les appareils équipés d'Android ou d'iOS.

La nouvelle série TZ associe élégamment divers produits individuels au sein d'une même solution, ce qui à la fois crée de la valeur et réduit la complexité.

A propos de SonicWALL

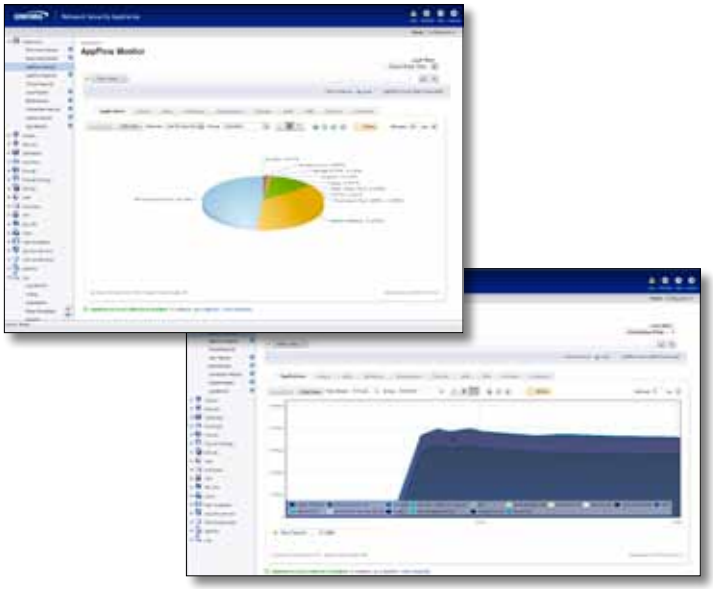
Guidée par sa vision d'une sécurité dynamique pour le réseau global, SonicWALL développe des solutions de sécurité réseau et de protection des données évoluées et intelligentes, sachant s'adapter à l'évolution des entreprises et des menaces. SonicWALL conçoit des solutions matérielles, logicielles et virtuelles primées permettant de détecter et de contrôler les applications et de protéger les réseaux contre les intrusions et les attaques de programmes malveillants. De nombreuses entreprises de par le monde, PME et grands comptes, font confiance à SonicWALL. Depuis 1991, SonicWALL a vendu plus de deux millions d'appliances par l'intermédiaire de son réseau mondial de partenaires. Des appliances qui permettent à des dizaines de millions d'utilisateurs professionnels de protéger leurs ordinateurs et de garder le contrôle de leurs données.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

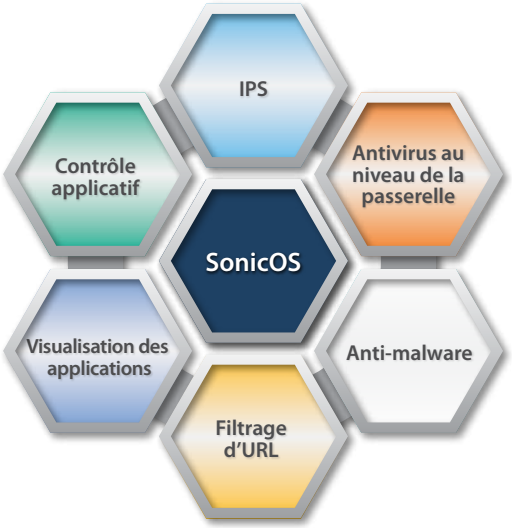
Architecture SonicWALL

Les TZ 205 et TZ 215 de SonicWALL sont dotés de processeurs Cavium double cœur, qui traitent simultanément des flux de données parallèles, améliorant ainsi la protection et les performances d'ensemble. La technologie double cœur est synonyme de performances supérieures, d'évolutivité et économies d'énergie. Elle se différencie en ce sens des plates-formes de sécurité réseau reposant sur des processeurs universels, avec des coprocesseurs de sécurité séparés ou des ASIC (Application-Specific Integrated Circuits), incapables de suivre en temps réel l'évolution d'attaques complexes à l'intérieur ou en dehors du périmètre réseau. Forte de cette architecture double cœur évoluée et performante, la série TZ est la solution la plus rapide de sa catégorie. Elle atteint des débits de filtrage dynamique de 500 Mbit/s, de 110 Mbit/s pour le filtrage applicatif ainsi que de 130 Mbit/s pour le VPN 3DES ou AES.



Logiciel SonicOS

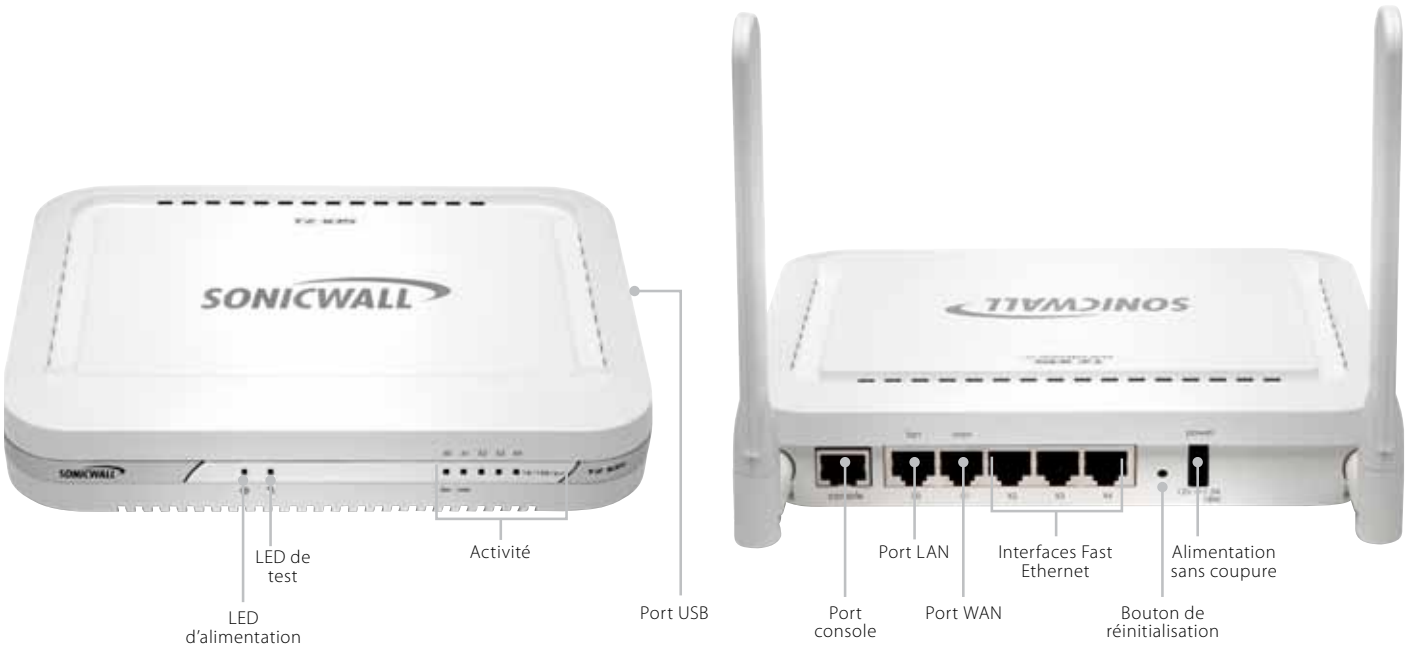
La technologie RFDPI (Reassembly-Free Deep Packet Inspection®) brevetée de SonicWALL permet un filtrage simultané des diverses menaces et des applications ainsi que l'analyse de fichiers de taille illimitée et de connexions à des vitesses extrêmement élevées. Cette base de code unique est au cœur de chaque pare-feu SonicWALL, du TZ 105 à l'appliance SuperMassive E10800. L'appliance SuperMassive E10800 avec SonicOS offre la meilleure protection d'ensemble parmi les pare-feu nouvelle génération recommandés par NSS Labs. Etroitement intégrée à la plate-forme des pare-feu, la technologie RFDPI optimise la gestion de règles granulaires, directement sur l'interface des pare-feu ou via SonicWALL GMS (Global Management System). Les entreprises ont le choix parmi une gamme complète de pare-feu SonicWALL éprouvés, équipés de SonicOS et conçus pour s'adapter aux besoins des réseaux les plus performants.



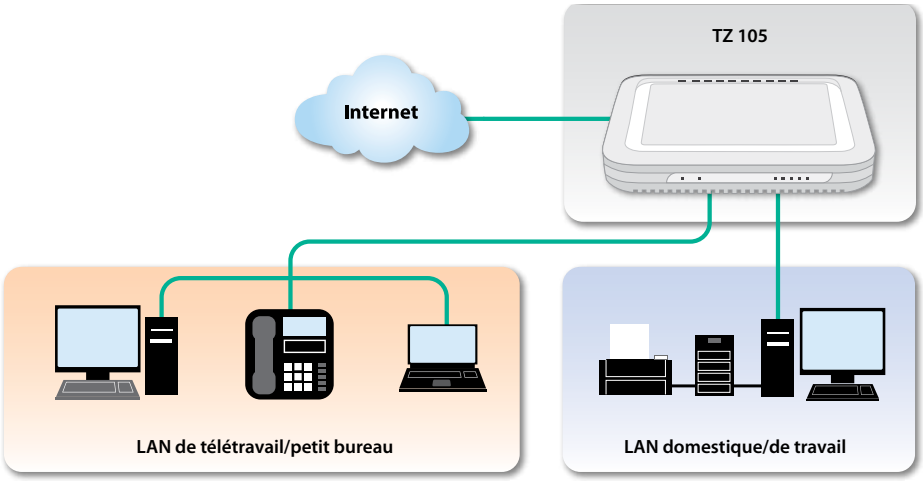
	Série TZ 105	Série TZ 205	Série TZ 215
Vue d'ensemble des pare-feu			
Débit de filtrage dynamique de paquets	200 Mbit/s	500 Mbit/s	500 Mbit/s
Débit IPS	60 Mbit/s	80 Mbit/s	110 Mbit/s
Débit GAV	40 Mbit/s	60 Mbit/s	70 Mbit/s
Débit VPN	75 Mbit/s	100 Mbit/s	110 Mbit/s
Débit Full DPI (UTM)	25 Mbit/s	40 Mbit/s	60 Mbit/s
Connexions UTM/DPI (max.)	8 000	12 000	32 000
Protection de fichiers de taille illimitée	✔	✔	✔
Matériel			
Processeur double cœur		✔	✔
Gigabit Ethernet		✔	✔
Prise en charge 802.11n	✔	✔	✔
Prise en charge 802.11a/b/g/n bibande		✔	✔
Services de sécurité			
Prévention des intrusions*	✔	✔	✔
Gateway Anti-Virus, Anti-Spyware and Cloud AV*	✔	✔	✔
Filtrage de contenu et d'URL (CFS)*	✔	✔	✔
Enforced Client Anti-Virus and Anti-Spyware*	✔	✔	✔
Application Intelligence and Control*			✔

* Disponible dans le cadre d'un service d'abonnement

SonicWALL TZ 105 — Poste de télétravail/petit bureau

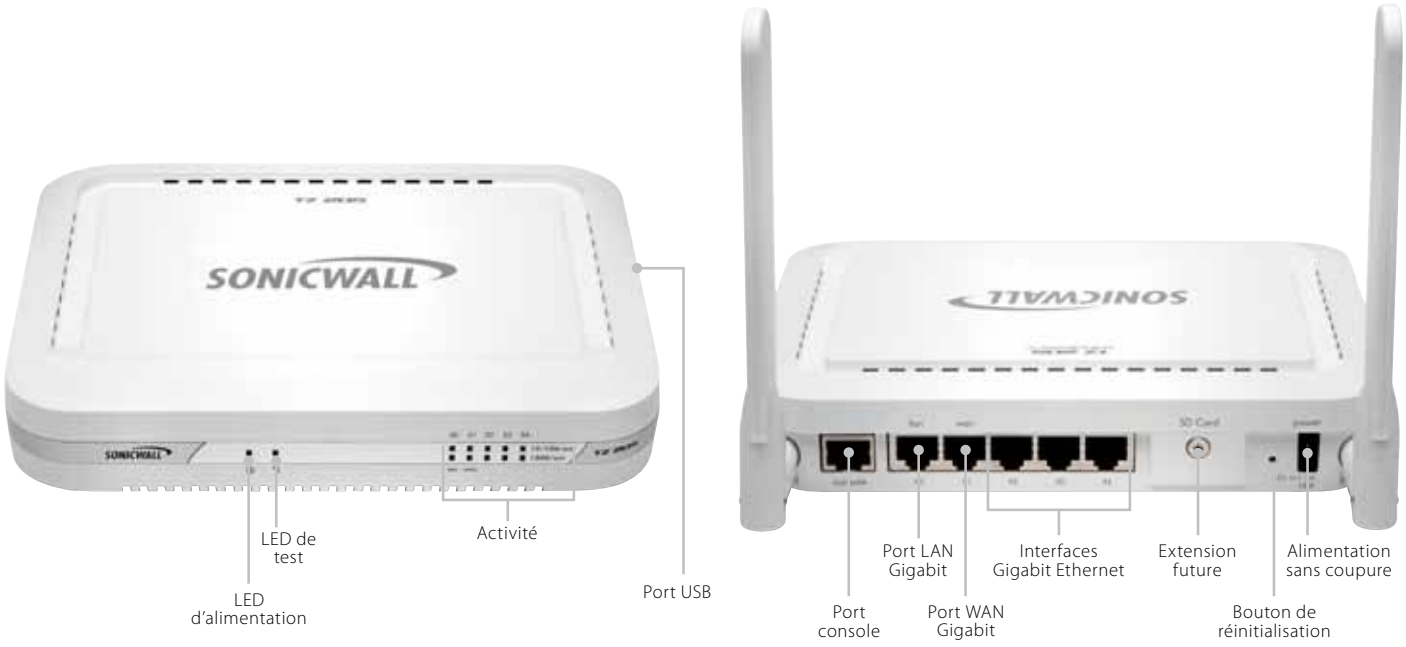


Le nouveau TZ 105 de SonicWALL est le pare-feu UTM (Unified Threat Management) le plus sécurisé à la disposition des petits bureaux, postes de télétravail et petits déploiements de points de vente. A la différence des produits grand public, le TZ 105 assure avec un maximum d'efficacité les services éprouvés de prévention des intrusions, de protection anti-malware et de filtrage de contenu/URL, ainsi que la prise en charge étendue de plates-formes mobiles pour les ordinateurs portables, smartphones et tablettes. Garant d'un filtrage applicatif exhaustif à très hautes performances, il ne crée aucun encombrement sur le réseau, optimisant par là-même la productivité des entreprises sans augmenter les coûts.

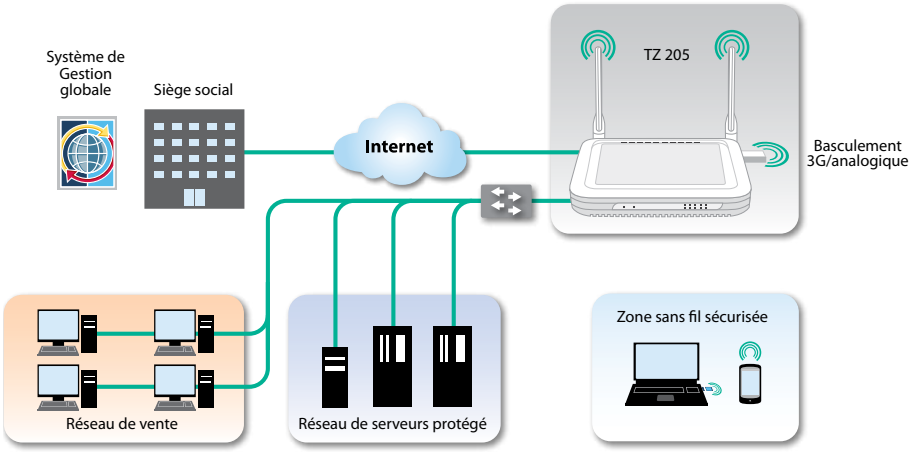


Description du matériel	Référence
TZ 105 TotalSecure 1 an	01-SSC-4906
TZ 105 Wireless-N TotalSecure 1 an	01-SSC-4908
TZ 105 Wireless-N TotalSecure International 1 an	01-SSC-4910

Description des services	Référence
Comprehensive Gateway Security Suite 1 an	01-SSC-4877
Gateway Anti-Virus and Intrusion Prevention Service 1 an	01-SSC-4844
Filtrage de contenu/d'URL 1 an	01-SSC-4850
Comprehensive Anti-Spam Service 1 an	01-SSC-4871
Support 8x5 1 an	01-SSC-4856
Support 24x7 1 an	01-SSC-4862



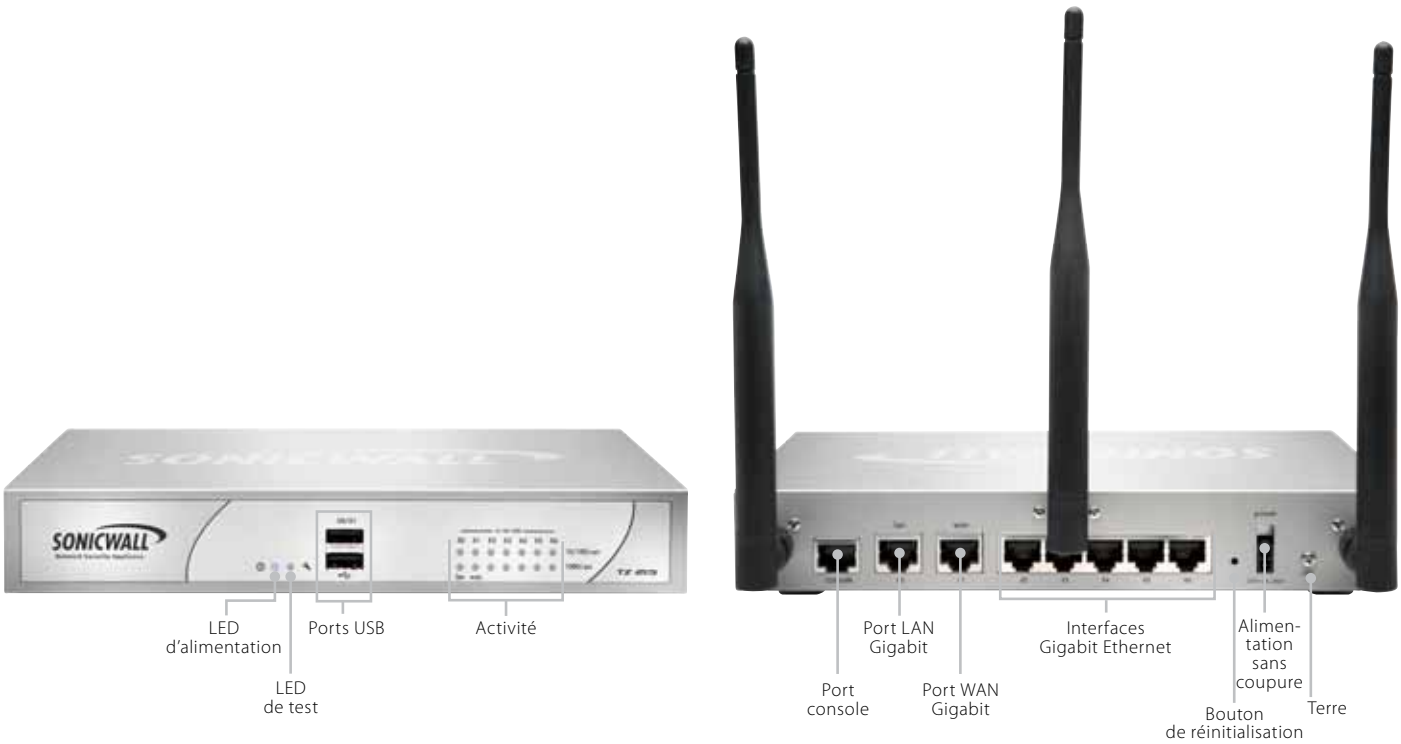
Petites entreprises, points de vente, services publics, sites distants et agences peuvent profiter des puissantes fonctionnalités de sécurité et des performances haut de gamme du nouveau TZ 205 de SonicWALL. A la différence des produits grand public, ce puissant pare-feu UTM (Unified Threat Management)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



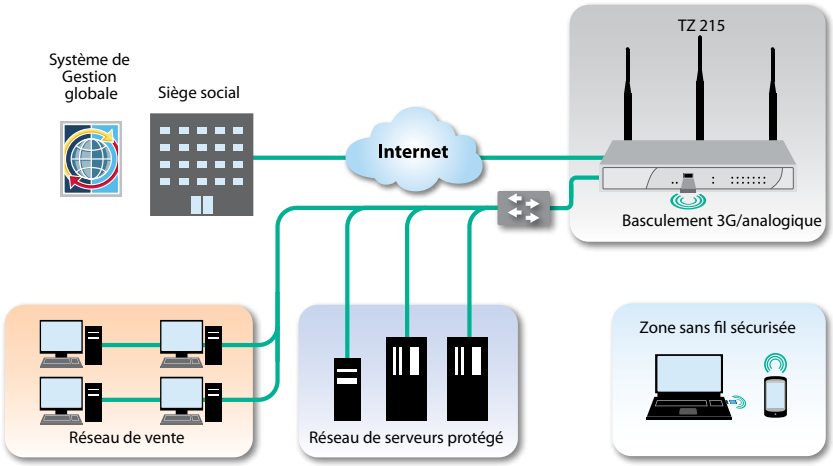
Description du matériel	Référence
Matériel TZ 205 : câblé	01-SSC-6945
Matériel TZ 205 : Wireless-N	01-SSC-6947
Matériel TZ 205 : Wireless-N International	01-SSC-4883
TZ 205 TotalSecure 1 an	01-SSC-4906
TZ 205 Wireless-N TotalSecure 1 an	01-SSC-4908
TZ 205 Wireless-N TotalSecure International 1 an	01-SSC-4910

Description des services	Référence
Comprehensive Gateway Security Suite 1 an	01-SSC-4838
Gateway Anti-Virus and Intrusion Prevention Service 1 an	01-SSC-4799
Filtrage de contenu/d'URL 1 an	01-SSC-4805
Comprehensive Anti-Spam Service 1 an	01-SSC-4832
Support 8x5 1 an	01-SSC-4811
Support 24x7 1 an	01-SSC-4817

SonicWALL TZ 215 — Point de vente/agence



Le nouveau TZ 215 de SonicWALL est le pare-feu UTM (Unified Threat Management) le plus sécurisé et le plus performant à la disposition des petites entreprises et agences. Conçu pour les petites structures, les entreprises distribuées, les agences et les points de vente, le TZ 215 intègre les services d'anti-malware, de prévention des intrusions, de contrôle applicatif et de filtrage d'URL en une solution simple et économique. Doté d'une architecture double cœur garante d'un filtrage applicatif exhaustif sans diminuer les performances, il ne crée aucun encombrement sur le réseau, optimisant par là-même la productivité des entreprises. Le contrôle applicatif du TZ 215 permet en outre de garantir la disponibilité de la bande passante pour les applications vitales, tout en freinant les applications non productives. Diverses fonctionnalités réseau avancées sont proposées : basculement vers plusieurs autres FAI et équilibrage de charge, connectivité sans fil sécurisée bibande en option, prise en charge des VPN IPSec, segmentation du réseau ou encore conformité PCI.



Description du matériel	Référence
Matériel TZ 215 : câblé	01-SSC-4976
Matériel TZ 215 : Wireless-N	01-SSC-4977
Matériel TZ 215 : Wireless-N International	01-SSC-4969
TZ 215 TotalSecure 1 an	01-SSC-4982
TZ 215 Wireless-N TotalSecure 1 an	01-SSC-4984
TZ 215 Wireless-N TotalSecure International 1 an	01-SSC-4986

Description des services	Référence
Comprehensive Gateway Security Suite 1 an	01-SSC-4793
Gateway Anti-Virus and Intrusion Prevention Service 1 an	01-SSC-4757
Filtrage de contenu/d'URL 1 an	01-SSC-4763
Comprehensive Anti-Spam Service 1 an	01-SSC-4787
Support 8x5 1 an	01-SSC-4769
Support 24x7 1 an	01-SSC-4775

Caractéristiques

Prévention des intrusions	
Analyse à base de signatures	Le service étroitement intégré de prévention des intrusions sur la base de signatures analyse la charge utile des paquets à la recherche de vulnérabilités et d'exploits visant les systèmes internes vitaux.
Mises à jour automatiques des signatures	L'équipe de recherche SonicWALL met à disposition une liste exhaustive et constamment mise à jour de plus de 5 400 signatures IPS couvrant 52 catégories d'attaques. Ces signatures prennent effet immédiatement, sans redémarrage ni interruption de service.
Prévention des menaces en sortie	La possibilité d'inspecter le trafic entrant et sortant garantit que le réseau ne sera pas impliqué involontairement dans des attaques par déni de service distribué (DDoS) et empêche toute communication C&C (commande et contrôle) de botnets.
Protection IPS inter-zone	La prévention des intrusions peut être déployée entre les zones de sécurité interne afin de protéger les serveurs sensibles et prévenir les attaques internes.
VPN	
VPN IPSec pour la connectivité site à site	Le VPN IPSec hautes performances permet au pare-feu de connecter des agences à distance avec le site central.
Accès distant par VPN SSL ou client IPSec	Vous pouvez utiliser 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 plates-formes.
Passerelle VPN redondante	En présence de plusieurs WAN, il est possible de configurer un VPN primaire et un VPN secondaire afin de permettre un basculement et une reprise automatiques de toutes les sessions VPN, en toute transparence.
VPN à base de routes	La capacité à réaliser un routage dynamique via les liaisons VPN garantit une disponibilité permanente en cas de panne temporaire d'un tunnel VPN : le trafic est réacheminé de manière transparente entre les terminaux par d'autres routes.
Clean VPN	SonicWALL Clean VPN™ garantit l'intégrité de l'accès VPN et élimine les menaces avant qu'elles n'infiltrent le réseau de l'entreprise.
Prévention des menaces au niveau de la passerelle	
Anti-malware au niveau de la passerelle	Le moteur RFDPI breveté de SonicWALL analyse tous les ports et protocoles à la recherche de virus, sans limitation dans la taille des fichiers ou la longueur des flux. Les chercheurs du laboratoire SonicLabs actualisent en permanence la protection, garantissant des délais de réponse brefs et une prévention plus rapide des intrusions.
Filtrage RFDPI (Reassembly-Free Deep Packet Inspection)	Le filtrage RFDPI (Reassembly-Free Deep Packet Inspection) suit la trace des programmes malveillants indépendamment de l'ordre ou du moment d'arrivée des paquets, ce qui permet de garantir une latence extrêmement faible, de supprimer les limites de taille des fichiers et des flux et de fournir des performances et une sécurité supérieures à celle des systèmes de proxys dépassés. Ceux-ci réassemblent le contenu à l'aide de sockets associés aux programmes antivirus traditionnels qui s'avèrent souvent inefficaces et surchargent la mémoire, entraînant une forte latence, des performances réduites et des restrictions en termes de taille.
Cloud Anti-Virus (AV)	Grâce au moteur RFDPI intégré, SonicWALL exploite la puissance du cloud pour offrir l'ensemble le plus complet de signatures anti-malware, tout en réduisant à un minimum la latence ou les retards. SonicWALL Cloud Anti-Virus Service fournit des millions de signatures supplémentaires de programmes malveillants pour le filtrage de fichiers exécutables avec les informations les plus actuelles qui soient.
Filtrage bidirectionnel	Le filtrage RFDPI peut être opéré à la fois sur les connexions entrantes et sortantes, garantissant la protection du réseau dans toutes les directions du trafic.
Mises à jour des signatures 24h/24, 7j/7	L'équipe de recherche du laboratoire SonicLabs crée et met à jour des bibliothèques de signatures transmises automatiquement aux pare-feu en service. Ces signatures prennent effet immédiatement, sans redémarrage ni interruption de service.
Pare-feu et réseau	
Filtrage dynamique de paquets	Tout le trafic réseau est inspecté, analysé et mis en conformité avec les règles d'accès du pare-feu.
Protection contre les attaques DOS	La protection contre les attaques de type SYN Flood prévient les dénis de service à l'aide des technologies SYN proxy (couche 3) et SYN blacklisting (couche 2).
Déploiement flexible	Le déploiement peut se faire en mode NAT traditionnel ou en mode pont couche 2.
Routage à base de règles	Crée des routes sur la base de protocoles pour diriger le trafic vers une connexion WAN privilégiée avec possibilité de basculer vers un WAN secondaire en cas de panne.
Haute disponibilité	Prise en charge du basculement actif/passif en vue de garantir une fiabilité accrue en protégeant contre les erreurs matérielles et logicielles.
Equilibrage de charge WAN	Jusqu'à quatre interfaces WAN sont utilisées pour équilibrer la charge selon les méthodes cyclique (Round Robin), par débordement (Spillover) ou suivant le pourcentage (Percentage based).
Accélération WAN	L'accélération WAN réduit la latence et augmente les vitesses de transfert entre les sites distants, optimisant l'efficacité du réseau.

Caractéristiques

VoIP

Qualité de service (QoS) avancée	Protection des communications vitales grâce au marquage 802.1p et DSCP, ainsi qu'au remappage du trafic VoIP sur le réseau.
Filtrage applicatif du trafic VoIP	Des signatures prédéfinies détectent et bloquent les menaces VoIP spécifiques.
Prise en charge des portiers H.323 et des proxys SIP	Bloque les appels indésirables en exigeant que tous les appels entrants soient autorisés et authentifiés par le portier H.323 ou le proxy SIP.

Gestion et surveillance

Interface utilisateur Web	Une interface Web intuitive assure une configuration rapide et pratique, en plus de la gestion via SonicWALL GMS® (Global Management System) ou l'interface CLI.
SNMP	SNMP permet de surveiller et de répondre aux menaces et aux alertes.
NetFlow/IPFIX	Permet d'exporter un vaste ensemble de données par les protocoles IPFIX ou Netflow pour bénéficier d'informations précises sur la consommation de bande passante, le trafic applicatif et les atteintes à la sécurité, tout en fournissant des services performants de dépannage et d'analyse forensique. Compatible avec SonicWALL Scrutinizer et les applications de surveillance et de reporting de tiers (TZ 215 uniquement).
Gestion centralisée des règles	SonicWALL GMS permet de surveiller, de configurer et d'établir des rapports sur diverses appliances SonicWALL, à partir d'une seule et même interface intuitive, et de personnaliser votre environnement de sécurité en fonction de vos propres règles.

Intelligence et contrôle applicatifs

Contrôle applicatif	Identification et contrôle d'applications ou d'éléments d'une application sur la base de la technologie RFDPI et non des ports et protocoles connus.
Gestion de la bande passante applicative	Allocation de bande passante aux applications vitales et restriction du trafic d'applications non productives afin d'améliorer l'efficacité et la productivité du réseau.
Identification personnalisée des applications	Création et configuration d'une identification personnalisée des applications sur la base de paramètres du trafic ou de modes de communication propres à une application sur le réseau.
Analyse du trafic applicatif	Livre des informations précises sur la consommation de bande passante, le trafic applicatif et la sécurité, tout en fournissant des services performants de dépannage et d'analyse forensique (TZ 215 uniquement).
Bibliothèque de signatures d'applications	Bibliothèque constamment enrichie de plus de 3 500 signatures d'applications garantissant que les administrateurs puissent contrôler l'utilisation des toutes dernières applications sur leur réseau au niveau d'une catégorie ou individuel.
Suivi des activités des utilisateurs	L'identification des utilisateurs est intégrée de manière transparente aux systèmes d'authentification Microsoft® Active Directory et autres, permettant un suivi et l'établissement de rapports sur l'identification d'utilisateurs individuels.
Identification du trafic par pays GeoIP	Identification et contrôle du trafic réseau acheminé ou provenant de certains pays (TZ 215 uniquement).

Pare-feu et réseau

Pare-feu
- Filtrage RFDPI (Reassembly-Free Deep Packet Inspection)
- Filtrage dynamique de paquets
- Protection contre les attaques DOS
- Réassemblage TCP
- Mode furtif

Contrôle applicatif
- Contrôle applicatif
- Blocage d'éléments d'applications
- Gestion de la bande passante applicative
- Création de signatures d'applications personnalisées
- Visualisation du flux applicatif
- Prévention des fuites de données
- IPFIX avec rapports sur les extensions
- Suivi des activités des utilisateurs
- Identification du trafic par pays GeoIP
- Bibliothèque exhaustive de signatures d'applications

Prévention des intrusions
- Analyse à base de signatures
- Mises à jour automatiques des signatures
- Prévention des menaces en sortie
- Liste d'exclusions IPS
- Messages de journalisation avec hyperliens
- Filtrage de contenu unifié et contrôle applicatif avec restriction de bande passante

Anti-malware
- Analyse anti-malware au niveau du flux
- Antivirus au niveau de la passerelle
- Anti-spyware au niveau de la passerelle
- Service d'antivirus cloud

VoIP
- Qualité de service (QoS) avancée
- Gestion de la bande passante
- Filtrage applicatif du trafic VoIP
- Interopérabilité totale
- Prise en charge des portiers H.323 et des proxys SIP

Mise en réseau
- Routage dynamique
- Routage à base de règles
- NAT avancé
- Serveur DHCP
- Gestion de la bande passante
- Agrégation de liens
- Redondance de ports
- Haute disponibilité
- Compatible IPv6
- Equilibrage de charge

Gestion et surveillance
- Interface utilisateur Web
- Interface en ligne de commande (CLI)
- SNMP
- Reporting via Analyzer
- Reporting via Scrutinizer
- Gestion et reporting via GMS
- Journalisation
- NetFlow/IPFIX
- Visualisation applicative
- Gestion centralisée des règles
- Signature unique (SSO)
- Prise en charge Terminal Services/Citrix

Services de sécurité
- Intrusion Prevention Service
- Gateway Anti-Malware Service
- Content Filtering Service
- Enforced Client Anti-Virus and Anti-Spyware Service – options McAfee® ou Kaspersky®
- Application Intelligence, Control and Visualization Service

Spécifications

Pare-feu	Série TZ 105	Série TZ 205	Série TZ 215
Version SonicOS		SonicOS 5.8.1 ou plus récente	
Débit dynamique[1]	200 Mbit/s	500 Mbit/s	500 Mbit/s
Débit IPS[2]	60 Mbit/s	80 Mbit/s	110 Mbit/s
Débit GAV[2]	40 Mbit/s	60 Mbit/s	70 Mbit/s
Débit UTM[2]	25 Mbit/s	40 Mbit/s	60 Mbit/s
Nb max. de connexions[3]	8 000	12 000	48 000
Connexions UTM/DPI (max.)	8 000	12 000	32 000
Nouvelles connexions/s	1 000	1 500	1 800
Nb de nœuds pris en charge		Illimité	
Protection contre les attaques par déni de service		22 classes d'attaques DoS, DDoS et scans	
Nb de SonicPoint pris en charge	1	2	16
VPN			
Débit 3DES/AES[4]	75 Mbit/s	100 Mbit/s	130 Mbit/s
Tunnels VPN site à site	5	10	15
Licences GVC incluses (max.)	0 (5)	2 (10)	2 (25)
Licences VPN SSL incluses (max.)	1 (5)	1 (10)	2 (10)
Chiffrement/authentification/groupes DH		DES, 3DES, AES (128, 142, 256 bits), MD5, SHA-1/groupes DH 1, 2, 5, 14	
Virtual Assist inclus (max.)	—	1 (essai de 30 jours)	2 (essai de 30 jours)
Echange de clés		IKE, clé manuelle, certificats (X.509), L2TP sur IPSec	
Certificats pris en charge		Verisign, Thawte, Cybertrust, RSA Keon, Entrust et Microsoft CA pour VPN SonicWALL à SonicWALL, SCEP	
Caractéristiques VPN		DPD (Dead Peer Detection), DHCP Over VPN, IPSec NAT Traversal, passerelle VPN redondante, VPN à base de routes	
Plates-formes Global VPN Client prises en charge		Microsoft® Windows XP, Vista 32/64 bits, Windows 7 32/64 bits	
Plates-formes VPN SSL		Microsoft Windows XP/Vista 32/64 bits/Windows 7, Mac OSX 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE	
Plate-forme Mobile Connect prise en charge		Apple® iOS 4.2 ou supérieure, Google® Android™ 4.0 ou supérieure	
Services de sécurité			
Services de filtrage applicatif		Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control (TZ 215 uniquement)	
Content Filtering Service (CFS)		Analyse d'URL HTTP, d'IP HTTPS, de mots-clés et de contenus, blocage ActiveX, d'applets Java et de cookies, gestion de la bande passante sur les catégories de filtrage, listes d'autorisation/interdiction	
Enforced Client Anti-Virus and Anti-Spyware		McAfee® ou Kaspersky®	
Comprehensive Anti-Spam Service[6]		Pris en charge	
Application Intelligence and Control		Contrôle applicatif	Visualisation du trafic applicatif et gestion de la bande passante
Mise en réseau			
Attribution d'adresses IP		Statique (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP	
Modes NAT		1:1, 1:plusieurs, plusieurs:1, plusieurs:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent	
VLAN	5, PortShield	10, PortShield	20, PortShield
DHCP		Serveur interne, relais	
Routage		OSPF, RIPv1/v2, routes statiques, routage à base de règles, multidiffusion	
Authentification		XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix	
Base de données utilisateurs locale		150 utilisateurs	
VoIP		H.323v1-5 intégral, SIP, gatekeeper support, gestion de la bande passante en sortie, VoIP sur le WLAN, sécurité par filtrage applicatif, interopérabilité totale avec la plupart des dispositifs de passerelles et de communication VoIP	
Système			
Sécurité par zones		Oui	
Horaires		Oui	
Gestion orientée objet/groupe		Oui	
DDNS		Fournisseurs de DNS dynamiques : dyndns.org, yi.org, no-ip.com et changeip.com	
Gestion et surveillance		CLI locale, interface utilisateur Web (HTTP, HTTPS), SNMP v2 ; gestion globale avec SonicWALL GMS	
Journalisation et rapports		Analyzer, Scrutinizer, GMS, Local Log, Syslog, Solera Networks, NetFlow v5/v9, IPFIX avec extensions, visualisation en temps réel	
Basculement matériel automatique	—	Actif/passif	Actif/passif
Anti-spam		Prise en charge RBL, listes d'autorisation/blocage, SonicWALL Comprehensive Anti-Spam Service en option[6]	
Equilibrage de charge		Oui, des trafics entrant et sortant	
Normes		TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3	
Prise en charge de l'accélération WAN[7]		Oui, avec les appliances SonicWALL série WXA.	
LAN sans fil intégré			
Normes	802.11b/g/n	802.11a/b/g/n (2x2)	802.11a/b/g/n (3x3)
Normes de sécurité sans fil		(WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS)	
Points d'accès virtuels (VAP)		Jusqu'à 8	
Antennes	Doubles, amovibles, externes	Doubles, amovibles, externes	Triples, amovibles, externes
Puissance radio – 802.11b/802.11g/802.11n	18 dBm max./18 dBm à 6 Mbit/s, 15 dBm à 54 Mbit/s	15,5 dBm max./18 dBm max./17 dBm à 6 Mbit/s, 13 dBm à 54 Mbit/s	
Puissance radio – 802.11a/802.11b/802.11g/802.11n	—	15,5 dBm max./18 dBm max./17 dBm à 6 Mbit/s, 13 dBm à 54 Mbit/s	
Puissance radio – 802.11n (2.4 GHz)/802.11n (5,0 GHz)	19 dBm MCS 0, 12 dBm MCS 15	19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15	
Sensibilité de réception radio – 802.11a/802.11b/802.11g	-90 dBm à 11 Mbit/s, -91 dBm à 6 Mbit/s, -74 dBm à 54 Mbit/s	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm à 11 Mbit/s / -91 dBm à 6 Mbit/s, -74 dBm à 54 Mbit/s	
Sensibilité de réception radio – 802.11n (2.4 GHz)/802.11n (5,0 GHz)	-89 dBm MCS 0, -70 dBm MCS 15	-89 dBm MCS 0, -70 dBm MCS 15/ -95 dBm MCS 0, -76 dBm MCS 15	
Matériel LAN sans fil intégré			
Interfaces	(5) 10/100 Fast Ethernet, 1 USB, 1 console	(5) Gigabit cuivre 10/100/1000 , 1 USB, 1 console	(7) Gigabit cuivre 10/100/1000, 2 USB, 1 console
Processeur	Monocœur	Double cœur	Double cœur
Mémoire flash/vive	32 Mo/256 Mo	32 Mo/256 Mo	32 Mo/512 Mo
Sans-fil 3G/modem[5]		Avec les adaptateurs homologués[5]	
Ports USB	1	1	2
Alimentation d'entrée		100-240 VCA, 50-60 Hz, 1 A	
Consommation max.	5,2 W/7,0 W	6,4 W/10,5 W	9,0 W/12,0 W
Dissipation thermique totale	17,8 BTU/23,7 BTU	21,9 BTU/35,8 BTU	30,6 BTU/41,4 BTU
Certifications		VPNC, ICSA Firewall 4.1	
Certifications (en instance)		EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1, IPv6 Phase 2	
Facteur de forme et dimensions	14,1 x 3,6 x 19 cm (5,6 x 1,4 x 7,5 in)	14,1 x 3,6 x 19 cm (5,6 x 1,4 x 7,5 in)	18,1 x 3,8 x 26,7 cm (7,1 x 1,5 x 10,5 in)
Poids	0,34 kg/0,75 lbs 0,38 kg/0,84 lbs	0,34 kg/0,75 lbs 0,38 kg/0,84 lbs	0,97 kg/1,95 lbs 0,97 kg/2,15 lbs
Conformité aux normes suivantes		FCC classe A, CES classe A, CE, C-Tick, VCCI, MIC, UL, cUL, TÜV/GS, CB, NOM, DEEE, RoHS	
Environnement/humidité		0-40 °C, 40-105 °F/5-95 % non condensée	
MTBF		28 ans/15 ans	

[1] Méthodes de test : performances maximales basées sur RFC 2544 (pour pare-feu). Les performances réelles peuvent varier suivant les conditions de réseau et les services activés. [2] Débit UTM/Gateway AV/Anti-Spyware/IPS basé sur le test de performances HTTP standard Spirent WebAvalanche et les outils de test Ixia. Tests effectués avec différents flux, via plusieurs paires de ports. [3] Le nombre maximal effectif de connexions est inférieur quand les services UTM sont activés. [4] Débit VPN basé sur le trafic UDP par paquets de 1280 octets selon RFC 2544. [5] Carte 3G et modem non fournis. Pour savoir quels appareils USB sont pris en charge, consultez http://www.sonicwall.com/us/products/cardsupport.html [6] Comprehensive Anti-Spam Service prend en charge un nombre illimité d'utilisateurs, mais est recommandé pour 250 utilisateurs ou moins. [7] Avec les appliances SonicWALL série WXA.

ICSA labs CERTIFIED FIREWALL - CORPORATE

VPNC CERTIFIED

Available on the App Store

ANDROID APP ON Google play

La gamme SonicWALL de solutions de sécurité dynamique

SÉCURITÉ RÉSEAU | ACCÈS DISTANT SÉCURISÉ | SÉCURISATION WEB ET DE MESSAGERIE | SAUVEGARDE ET RÉCUPÉRATION | GESTION ET RÈGLES

SonicWALL France
T +33 1 49 33 73 19 France@sonicwall.com

SonicWALL BeNeLux
T +32 (0) 15 280 985 Benelux@sonicwall.com

Contacts du support SonicWALL
www.sonicwall.com/emea/4724.html

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™