Serie SonicWall TZ

Seguridad excepcional y rendimiento estelar con un coste total de propiedad increíblemente bajo

Los firewalls de Gestión unificada de amenazas (UTM) de SonicWall son ideales para cualquier organización que necesite protección de red de clase empresarial.

Los firewalls de la serie SonicWall TZ ofrecen una amplia protección mediante servicios de seguridad avanzada que incluyen funciones integradas y basadas en la nube de antimalware, antispyware, control de aplicaciones, IPS (Sistema de prevención de intrusiones) y filtrado de URL. Con el fin de contrarrestar la tendencia de los ataques cifrados, la potencia de procesamiento de los firewalls de la serie TZ les permite inspeccionar conexiones SSL/TLS cifradas para hacer frente a las últimas amenazas. En combinación con los switches de la serie X de Dell, algunos firewalls de la serie TZ pueden gestionar directamente la seguridad de estos puertos adicionales.

Con el respaldo de la red Capture Threat Network de SonicWall, la serie SonicWall TZ proporciona actualizaciones continuas a fin de mantener una sólida defensa de la red frente a los ciberdelincuentes. La serie SonicWall TZ es capaz de analizar cada byte de cada paquete en todos los puertos y protocolos casi sin latencia y sin limitaciones en el tamaño de los archivos.

La serie SonicWall TZ incluye puertos Gigabit Ethernet, conectividad inalámbrica 802.11ac integrada opcional,* IPSec y SSL VPN, reconexión mediante soporte integrado para 3G/4G, equilibrio de carga y segmentación de red. Los firewalls UTM de la serie SonicWall TZ también proporcionan un acceso móvil rápido y seguro utilizando las plataformas Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS X y Linux.

El Sistema de gestión global (GMS) de SonicWall permite implementar y gestionar los firewalls de la serie SonicWall TZ de forma centralizada desde un único sistema.

Servicios de seguridad administrados para entornos distribuidos

Los centros escolares, los establecimientos minoristas, los sitios remotos, las sucursales y las empresas distribuidas necesitan una solución que se integre con su firewall corporativo. Los firewalls de la serie SonicWall TZ comparten la misma base de código —y la misma protección— que nuestros firewalls estrella de próxima generación SuperMassive, lo que simplifica la gestión de sitios remotos, ya que todos los administradores ven la misma interfaz de usuario. Con GMS, los administradores de red pueden configurar, supervisar y gestionar los firewalls SonicWall de forma remota desde una única consola. Mediante la incorporación de la conectividad inalámbrica segura y de la alta velocidad, los productos de la serie SonicWall TZ amplían el perímetro de protección para abarcar a los clientes y usuarios invitados que frecuentan un determinado establecimiento minorista o una oficina remota.

Ventajas:

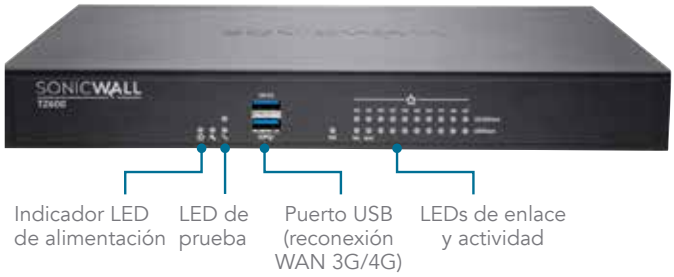
- Protección de red de clase empresarial
- Inspección profunda de paquetes de todo el tráfico sin restricciones de tamaño de archivo ni protocolo
- Conectividad inalámbrica segura 802.11ac mediante un controlador inalámbrico integrado o por medio de puntos de acceso inalámbricos SonicWall SonicPoint externos
- Acceso móvil a VPN SSL para dispositivos de Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS y Linux
- Implementados en combinación con switches de la serie X de Dell, los firewalls TZ permiten gestionar de forma segura más de 100 puertos adicionales a través de su consola.

** 802.11ac no está disponible actualmente en los modelos SOHO; los modelos SOHO soportan 802.11a/b/g/n*

Serie SonicWall TZ600

Para las empresas emergentes, minoristas y sucursales que busquen un rendimiento de seguridad con una buena relación calidad-precio, el firewall de próxima generación SonicWall TZ600 protege las redes con funciones de clase empresarial y un rendimiento sin compromisos.

Especificaciones	Serie TZ600
Rendimiento del firewall	1,5 Gbps
Rendimiento de DPI completo	500 Mbps
Rendimiento de antimalware	500 Mbps
Rendimiento IPS	1,1 Gbps
Rendimiento de IMIX	900 Mbps
Conexiones DPI máximas	125.000
Nuevas conexiones/s	12.000



Serie SonicWall TZ500

Para las pymes y sucursales en crecimiento, la serie SonicWall TZ500 proporciona una protección altamente eficaz sin compromisos con productividad de la red y una conexión inalámbrica integrada y de doble banda 802.11ac opcional.

Especificaciones	Serie TZ500
Rendimiento del firewall	1,4 Gbps
Rendimiento de DPI completo	400 Mbps
Rendimiento de antimalware	400 Mbps
Rendimiento IPS	1,0 Gbps
Rendimiento de IMIX	700 Mbps
Conexiones DPI máximas	100.000
Nuevas conexiones/s	8.000

Serie SonicWall TZ400

La serie SonicWall TZ400 proporciona protección de clase empresarial para pequeñas empresas, comercios minoristas y sucursales. Disponible implementación inalámbrica flexible con conectividad inalámbrica 802.11ac de banda dual opcional integrada en el firewall.

Especificaciones	Serie TZ400
Rendimiento del firewall	1,3 Gbps
Rendimiento de DPI completo	300 Mbps
Rendimiento de antimalware	300 Mbps
Rendimiento IPS	900 Mbps
Rendimiento de IMIX	500 Mbps
Conexiones DPI máximas	90.000
Nuevas conexiones/s	6.000

Serie SonicWall TZ300

La serie SonicWall TZ300 proporciona una solución integral que protege las redes frente a los ataques. A diferencia de los productos para consumidores, el firewall de la serie SonicWall TZ300 combina funciones eficaces de prevención de intrusiones, antimalware y filtrado de contenido/URL con una conexión inalámbrica 802.11ac integrada de carácter opcional y la más amplia compatibilidad con plataformas móviles seguras de portátiles, teléfonos inteligentes y tablets.

Especificaciones	Serie TZ300
Rendimiento del firewall	750 Mbps
Rendimiento de DPI completo	100 Mbps
Rendimiento de antimalware	100 Mbps
Rendimiento IPS	300 Mbps
Rendimiento de IMIX	200 Mbps
Conexiones DPI máximas	50.000
Nuevas conexiones/s	5.000

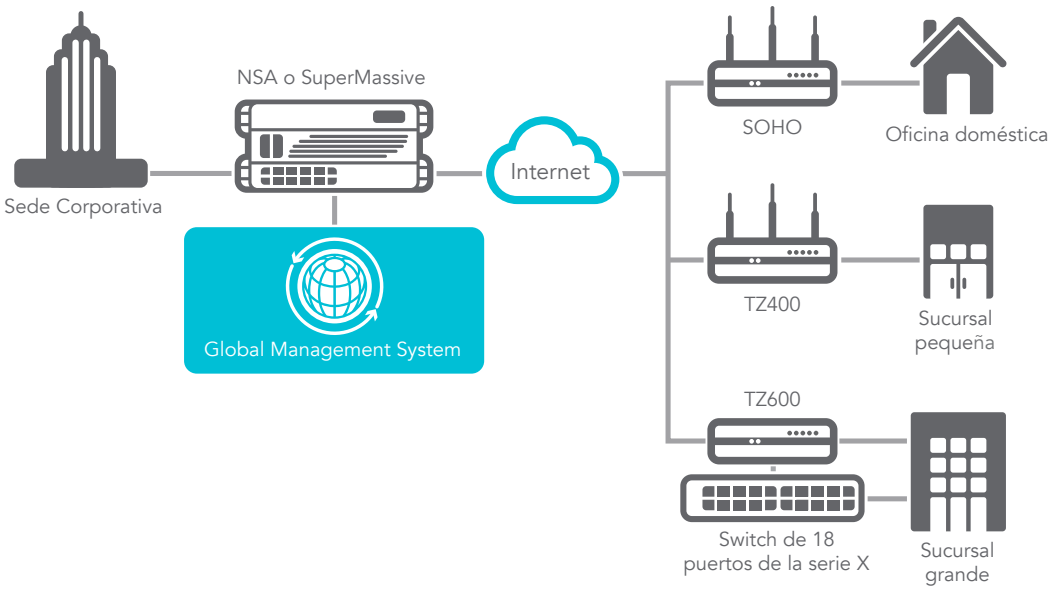
Serie SonicWall SOHO

Para entornos por cable e inalámbricos de pequeñas oficinas u oficinas domésticas, la serie SonicWall SOHO proporciona la misma protección de clase empresarial que precisan las grandes empresas a un precio mucho más asequible.

Especificaciones	Serie SOHO
Rendimiento del firewall	300 Mbps
Rendimiento de DPI completo	50 Mbps
Rendimiento de antimalware	50 Mbps
Rendimiento IPS	100 Mbps
Rendimiento de IMIX	60 Mbps
Conexiones DPI máximas	10.000
Nuevas conexiones/s	1.800

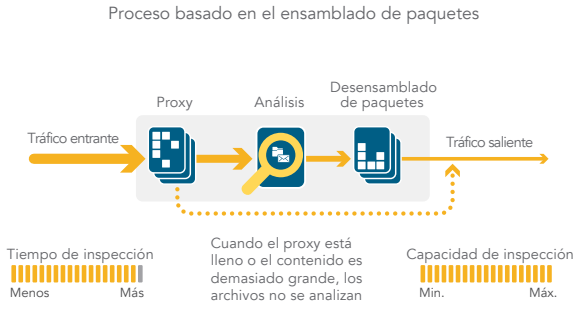
Arquitectura ampliable para máximo nivel de rendimiento y escalabilidad

El motor de Inspección profunda de paquetes sin reensamblado (RFDPI) está diseñado desde cero con el objetivo de proporcionar un escaneado de seguridad de alto rendimiento para adaptarse a la naturaleza paralela y creciente del tráfico de red. Cuando se combina con sistemas de procesador multinúcleo, esta arquitectura de software centrada en el procesamiento paralelo se amplía perfectamente para satisfacer los requisitos de la inspección profunda de paquetes con altas cargas de tráfico. La plataforma SonicWall TZ se basa en procesadores que, a diferencia de los x86, están optimizados para el procesamiento de paquetes, cifrados y red, a la vez que preservan la flexibilidad y la programación in situ, un punto débil de los sistemas ASIC. Esta flexibilidad es esencial cuando se requieren nuevas actualizaciones de código y de comportamiento para ofrecer protección contra nuevos ataques que requieren técnicas de detección actualizadas y más sofisticadas.

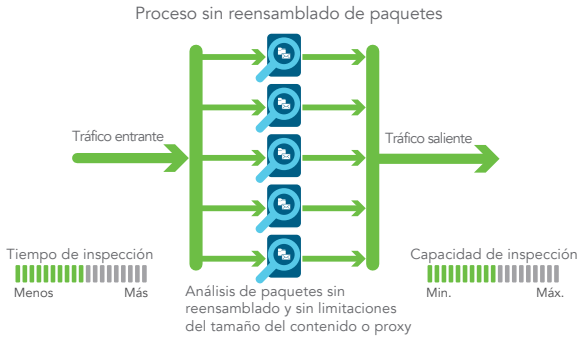


Motor de inspección profunda de paquetes sin reensamblado (Reassembly-Free Deep Packet Inspection, RFDPI)

El motor RFDPI ofrece una protección contra amenazas y un control de aplicaciones excepcionales sin sacrificar el rendimiento. Este motor patentado inspecciona el flujo de tráfico para detectar amenazas en los niveles del 3 al 7. El motor RFDPI somete los flujos de red a amplios y repetidos procesos de normalización y descifrado con el fin de neutralizar las técnicas avanzadas de evasión que pretenden burlar los motores de detección e introducir código malicioso en la red. Una vez aplicado el procesamiento previo necesario a un paquete, incluido el descifrado SSL, éste se analiza en relación con una única representación en memoria propietaria de tres bases de datos de definiciones: ataques de intrusión, malware y aplicaciones. A continuación, se actualiza el estado de conexión para representar la posición del flujo en relación con esas bases de datos hasta que se encuentra un estado de ataque u otro evento que se reconozca como una amenaza. En ese momento, se lleva a cabo una acción predefinida. Cuando se identifica malware, el firewall de SonicWall pone fin a la conexión antes de que se produzcan daños y registra adecuadamente el evento. No obstante, el motor también puede configurarse solo para la inspección o, en el caso de la detección de aplicaciones, para ofrecer servicios de gestión de ancho de banda de capa 7 para el resto del flujo de aplicaciones en cuanto se haya identificado la aplicación.



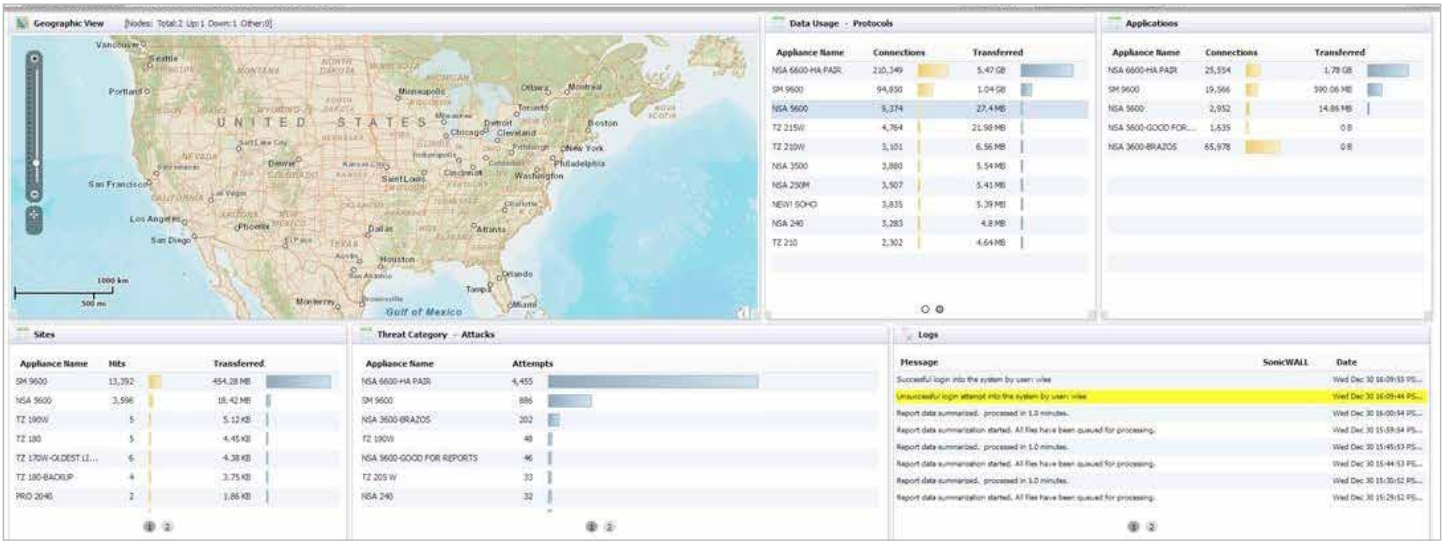
Arquitectura de la competencia



Arquitectura SonicWall

Gestión e informes globales

Para las implementaciones de mayor envergadura en empresas distribuidas, el Sistema de gestión global de SonicWall (GMS) proporciona a los administradores una plataforma unificada, segura y ampliable para gestionar los dispositivos de seguridad de SonicWall y los switches de la serie X de Dell. Este sistema permite a las empresas consolidar fácilmente la gestión de dispositivos de seguridad, reducir las complejidades administrativas y de solución de problemas, y controlar todos los aspectos operativos de la infraestructura de seguridad, como la gestión y la aplicación centralizadas de políticas, la supervisión de eventos en tiempo real, los análisis y la elaboración de informes, entre otras funciones. GMS también cumple los requisitos de gestión de cambios del firewall de las empresas gracias a una prestación de automatización del flujo de trabajo. GMS proporciona una forma mejor de gestionar la seguridad de la red mediante procesos de negocio y niveles de servicio que simplifican drásticamente la gestión del ciclo de vida de sus entornos de seguridad en general, en lugar de hacerlo dispositivo por dispositivo.

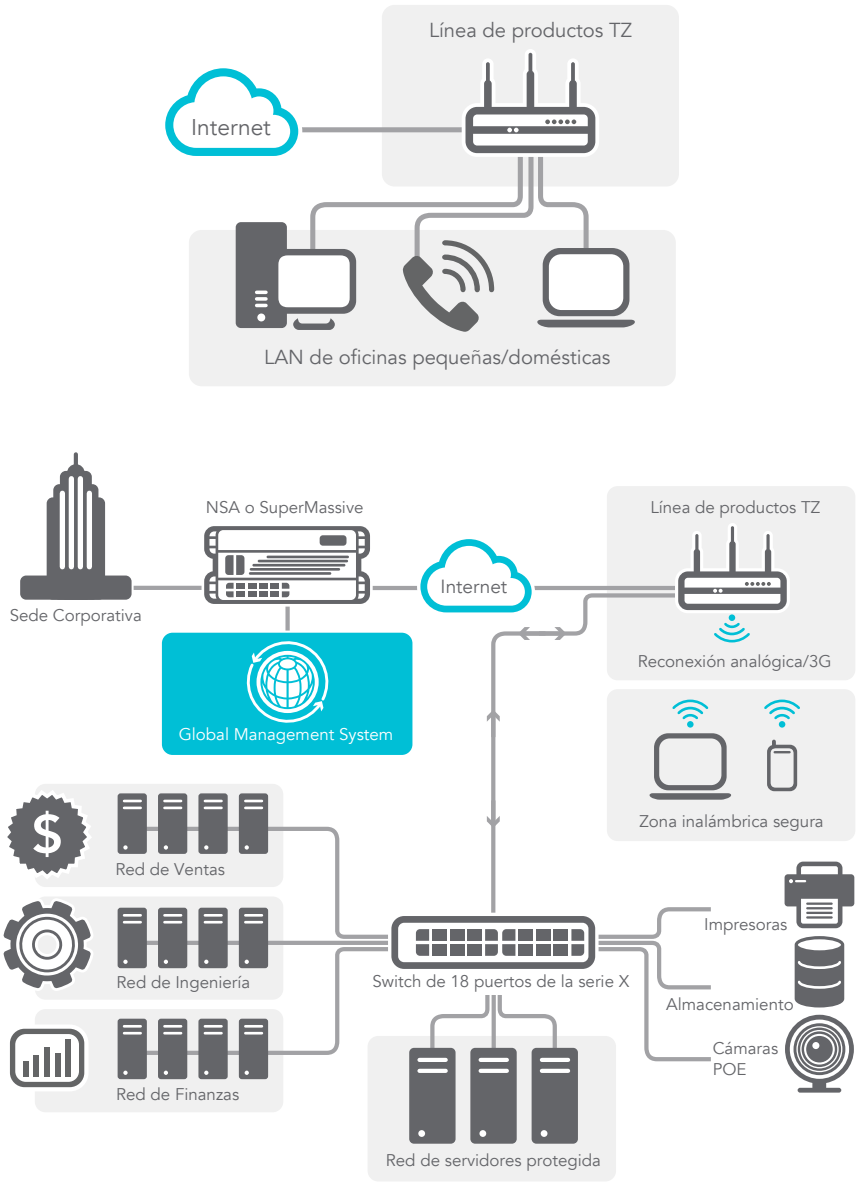


Seguridad y protección

El equipo de investigación de amenazas interno y dedicado de SonicWall Capture Labs estudia y desarrolla contramedidas para aplicarlas a los firewalls in situ a fin de lograr una protección actualizada. Con la ayuda de más de un millón de sensores distribuidos por todo el mundo, obtienen muestras de malware e información telemétrica sobre las últimas amenazas, que a su vez es transmitida a los firewalls para soportar las funciones de prevención de intrusiones, antimalware y detección de aplicaciones. Los clientes de firewalls de SonicWall con suscripciones vigentes disfrutan de una protección contra amenazas que se actualiza de forma continua e ininterrumpida. Además, dichas actualizaciones se aplican de inmediato sin necesidad de reinicios ni interrupciones. Las definiciones disponibles en los dispositivos protegen contra un amplio abanico de ataques. De hecho, cada una de ellas cubre decenas de miles de amenazas individuales. Además de las contramedidas disponibles en el dispositivo, todos los firewalls de SonicWall cuentan con acceso a SonicWall CloudAV, que amplía los datos sobre definiciones integrados con más de 20 millones de definiciones, un número en continuo aumento. El firewall accede a la base de datos CloudAV mediante un protocolo ligero propietario con el fin de reforzar la inspección realizada en el dispositivo. Con las capacidades de filtrado de botnets e IP según los datos geográficos, los firewalls de próxima generación de SonicWall pueden bloquear el tráfico procedente de dominios peligrosos o de regiones geográficas enteras a fin de reducir el perfil de riesgo para la red.

Inteligencia y control de aplicaciones

La inteligencia de aplicaciones informa a los administradores del tráfico de aplicaciones que atraviesa la red para que puedan programar controles de aplicaciones basados en las prioridades de negocio, restringir las aplicaciones improductivas y bloquear las que puedan resultar peligrosas. La visualización en tiempo real identifica anomalías en el tráfico en el momento en que se producen, permitiendo tomar contramedidas inmediatas contra posibles ataques entrantes o salientes o cuellos de botella en el rendimiento. Los análisis de tráfico de aplicaciones de SonicWall ofrecen información detallada sobre el tráfico de aplicaciones, el uso del ancho de banda y las amenazas para la seguridad, así como potentes funciones de solución de problemas y análisis forense. Además, el inicio de sesión único (SSO) seguro mejora la experiencia del usuario, aumenta la productividad y reduce las llamadas al servicio de asistencia. El uso de una intuitiva interfaz basada en Web simplifica la gestión del control y la inteligencia de aplicaciones.



Conexión inalámbrica flexible y segura

La conectividad inalámbrica 802.11ac de alta velocidad, disponible como prestación opcional, se combina con la tecnología del firewall de próxima generación de SonicWall para crear una solución de seguridad de red inalámbrica que proporciona una protección integral para las redes por cable e inalámbricas.

Gracias a este rendimiento inalámbrico de nivel empresarial, los dispositivos preparados para Wi-Fi pueden conectarse a mayor distancia y utilizar aplicaciones móviles que consumen un gran volumen de ancho de banda, como las de vídeo y voz, en entornos de mayor densidad sin que la calidad de la señal se reduzca.

** 802.11ac no está disponible actualmente en los modelos SOHO; los modelos SOHO soportan 802.11a/b/g/n*

SONICWALL®

Prestaciones

Motor RFDPI	
Prestación	Descripción
Inspección profunda de paquetes sin reensamblado	Este motor de inspección de alto rendimiento, propietario y patentado lleva a cabo análisis de tráfico bidireccionales basados en flujos, sin proxy ni almacenamiento en búfer, para descubrir intentos de intrusión y malware e identificar el tráfico de aplicaciones independientemente del puerto.
Inspección bidireccional	Escanea el tráfico entrante y saliente de forma simultánea en busca de amenazas con el fin de evitar que la red se utilice para la distribución de malware o se convierta en una plataforma de lanzamiento de ataques en el caso de que se introduzca un equipo infectado.
Inspección de paso único	La arquitectura DPI de paso único escanea el tráfico simultáneamente para la detección de malware y de intrusiones y para la identificación de aplicaciones, reduciendo drásticamente la latencia de la DPI y garantizando la correlación de toda la información sobre las amenazas en una única arquitectura.
Inspección basada en flujos	La tecnología de inspección sin proxy ni almacenamiento en búfer proporciona un rendimiento de muy baja latencia para la inspección profunda de paquetes de flujos de red simultáneos sin introducir limitaciones sobre el tamaño del flujo y los archivos. Además, puede aplicarse a protocolos comunes, así como a flujos de TCP sin procesar.
Inspección profunda de paquetes de Secure Socket Shell (DPI-SSH)	Detecta y previene ataques cifrados avanzados que utilizan SSH, bloquea descargas de malware cifrado, detiene la propagación de infecciones y frustra comunicaciones de comando y control y la exfiltración de datos.
Capture Advanced Threat Protection	
Prestación	Descripción
Sandboxing multimotor	La plataforma de sandbox multimotor, que incluye sandboxing virtualizado, emulación de sistema completo y tecnología de análisis de nivel de hipervisor, ejecuta el código sospechoso y analiza su comportamiento, proporcionando una visibilidad completa de la actividad maliciosa.
Análisis de gran variedad de tipos de archivos	Soporta análisis de una amplia variedad de tipos de archivos, como los programas ejecutables (PE), DLL, PDFs, documentos MS Office, archivos, JAR y APK, así como múltiples sistemas operativos, como Windows, Android, Mac OS X y entornos multinavegador.
Rápida implementación de definiciones	Cuando se detecta un archivo malicioso, inmediatamente se pone una definición a disposición de los firewalls con suscripción a SonicWall Capture y se envía a las bases de datos de definiciones de Gateway Anti-Virus e IPS y a las bases de datos de reputación de URL, IP y dominios en el transcurso de 48 horas.
Bloqueo hasta que haya un veredicto	A fin de evitar el acceso a la red de archivos potencialmente peligrosos, los archivos enviados a la nube para su análisis pueden retenerse en la pasarela hasta que se emita un veredicto.
Prevención de amenazas cifradas	
Prestación	Descripción
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico SSL sobre la marcha, sin necesidad de proxies, en busca de malware, intrusiones y filtraciones de datos, y aplica políticas de control de aplicaciones, URL y contenido para ofrecer protección contra las amenazas ocultas en el tráfico cifrado mediante TLS/SSL. Incluido con las suscripciones de seguridad para todos los modelos excepto SOHO. Para los modelos SOHO, se vende como una licencia independiente.
Inspección SSH	La inspección profunda de paquetes de SSH (DPI-SSH) descifra e inspecciona los datos que atraviesan los túneles SSH para prevenir ataques que utilicen SSH.
Prevención de intrusiones	
Prestación	Descripción
Protección basada en contramedidas	El sistema de prevención de intrusiones (IPS) estrechamente integrado utiliza definiciones y otras contramedidas para escanear los datos útiles de los paquetes en busca de vulnerabilidades y exploits, cubriendo de este modo un amplio abanico de ataques y vulnerabilidades.
Actualizaciones automáticas de las definiciones	El equipo de investigación de amenazas de SonicWall Capture Labs investiga e implementa contramedidas IPS, actualizando continuamente una larga lista que cubre más de 50 categorías de ataques. Las nuevas actualizaciones se hacen efectivas en el acto, sin que sea necesario reiniciar los sistemas ni interrumpir su servicio.
Protección IPS entre zonas	Refuerza la seguridad interna al segmentar la red en múltiples zonas de seguridad con prevención de intrusiones para evitar la propagación de las amenazas de unas zonas a otras.
Detección y bloqueo de actividades de comando y control (CnC) procedente de ataques botnets	Identifica y bloquea el tráfico de comando y control originado en bots de la red local y dirigido a IPs y dominios identificados como propagadores de malware o conocidos como puntos de CnC.
Abuso/anomalía de protocolo	Identifica y bloquea ataques que abusan de los protocolos para intentar eludir el IPS.
Protección de día cero	Protege la red ante los ataques de día cero con actualizaciones constantes contra los últimos métodos y técnicas de exploits, que cubren miles de exploits individuales.
Tecnología antievasión	La amplia normalización de flujos, la descodificación y otras técnicas impiden que las amenazas puedan penetrar la red sin ser detectadas utilizando técnicas de evasión en las capas 2-7.
Prevención de amenazas	
Prestación	Descripción
Antimalware en pasarela	El motor RFDPI analiza todo el tráfico entrante, saliente y dentro de una misma zona en busca de virus, troyanos, registradores de pulsaciones de teclas y otros tipos de malware en archivos de una longitud y un tamaño ilimitados en todos los puertos y flujos de TCP.
Protección antimalware CloudAV	Los servidores de la nube de SonicWall disponen de una base de datos de más de 20 millones de definiciones de amenazas que se actualiza continuamente y se utiliza para aumentar las capacidades de la base de datos de definiciones integrada, lo que ofrece a la tecnología RFDPI una amplia cobertura de amenazas.
Actualizaciones de seguridad las 24 horas	Las nuevas actualizaciones de amenazas se transfieren automáticamente a los firewalls con servicios de seguridad activos, donde se hacen efectivas inmediatamente sin necesidad de reiniciar el sistema ni interrumpir el servicio.

Prevención de amenazas (cont.)	
Prestación	Descripción
Descifrado e inspección SSL	Descifra e inspecciona el tráfico SSL sobre la marcha sin necesidad de proxy en busca de malware, intrusiones y filtraciones de datos. Además, aplica políticas de control de aplicaciones, URL y contenido a fin de proporcionar protección contra las amenazas ocultas en el tráfico cifrado mediante SSL. Esta prestación se incluye con suscripciones de seguridad para todos los modelos excepto SOHO. Para los modelos SOHO, se vende como una licencia independiente.
Inspección TCP bidireccional (sin procesar)	El motor RFDPI puede analizar flujos de TCP sin procesar en cualquier puerto y en ambas direcciones, con lo que se previenen los ataques que intentan infiltrarse por sistemas de seguridad desactualizados que se centran en proteger solo algunos puertos más conocidos.
Amplio soporte de protocolos	Identifica protocolos comunes, como HTTP/S, FTP, SMTP, SMBv1/v2 y otros tipos, que no envían datos en TCP sin procesar, y descodifica cargas útiles para la inspección de malware, incluso si no se ejecutan en puertos estándares y bien conocidos.
Inteligencia y control de aplicaciones	
Prestación	Descripción
Control de aplicaciones	Controle aplicaciones, o funciones de aplicaciones individuales, identificadas por el motor RFDPI mediante su cotejo con una base de datos en continuo crecimiento de más de 3.500 definiciones de aplicaciones, con el objetivo de aumentar la seguridad y la productividad de la red.
Identificación personalizada de aplicaciones	Controle las aplicaciones personalizadas creando definiciones basadas en parámetros específicos o patrones exclusivos de una aplicación en sus comunicaciones de red para conseguir un mayor control de la red.
Gestión del ancho de banda de las aplicaciones	Asigne y regule de forma detallada el ancho de banda disponible para aplicaciones o categorías de aplicaciones críticas, a la vez que limita el tráfico de aplicaciones no esenciales.
Control granular	Controle aplicaciones (o componentes específicos de una aplicación) basándose en programaciones, grupos de usuarios, listas de exclusión y una gama de acciones con una completa identificación de usuario mediante SSO a través de la integración de LDAP/AD/Terminal Services/Citrix.
Filtrado de contenido	
Prestación	Descripción
Filtrado de contenido dentro y fuera	Aplique políticas de usos aceptables y bloquee el acceso a sitios Web que contengan información o imágenes inaceptables o improductivas con Content Filtering Service. Amplíe la aplicación de políticas para bloquear contenido de Internet en dispositivos situados fuera del perímetro del firewall con Content Filtering Client.
Controles granulares	Bloquee contenido utilizando las categorías predefinidas o cualquier combinación de categorías. El filtrado puede programarse por hora del día, por ejemplo, durante el horario laboral o escolar, y aplicarse a usuarios individuales o grupos.
YouTube para centros educativos	Permita a los profesores elegir entre cientos de miles de vídeos educativos gratuitos de YouTube EDU, organizados por asignaturas y cursos, y adaptados a los estándares educativos comunes.
Almacenamiento en caché Web	Las clasificaciones de URL se almacenan en caché en el firewall de SonicWall, con lo que se reduce el tiempo de respuesta para el posterior acceso a sitios que se visitan con frecuencia a solo una fracción de segundo.
Enforced Anti-Virus and Anti-Spyware	
Prestación	Descripción
Protección en varios niveles	Utilice las funciones del firewall, como la primera capa de defensa en el perímetro, junto con la protección de puntos terminales, a fin de bloquear los virus que penetran en la red por medio de portátiles, unidades de memoria flash y otros sistemas no protegidos.
Opción de aplicación automatizada	Asegúrese de que todos los equipos que accedan a la red tengan instalada y activa la versión más reciente de las definiciones antivirus y antispyware. De este modo, eliminará los costes asociados habitualmente a la gestión de soluciones antivirus y antispyware para equipos de escritorio.
Opción de instalación e implementación automatizadas	La implementación y la instalación máquina a máquina de clientes antivirus y antispyware se realiza de forma automática en toda la red, con lo que se minimiza la sobrecarga administrativa.
Protección antivirus automática e ininterrumpida	Las actualizaciones frecuentes de antivirus y antispyware se envían de forma transparente a todos los equipos de escritorio y servidores de archivos para mejorar la productividad de los usuarios finales y reducir las tareas de gestión de la seguridad.
Protección antispyware	La potente función de protección antispyware analiza y bloquea la instalación de un completo conjunto de programas de spyware en equipos de escritorio y portátiles antes de que éstos transmitan datos confidenciales, lo que contribuye a aumentar la seguridad y el rendimiento de los equipos de escritorio.
Firewall e interconexión	
Prestación	Descripción
Inspección dinámica de paquetes	Todo el tráfico de la red se inspecciona, se analiza y se somete a las políticas de acceso del firewall.
Protección contra ataques DDoS/DOS	La protección contra inundaciones SYN proporciona una defensa contra los ataques de DOS mediante el uso de tecnologías de listas negras de nivel 3 (SYN proxy) y nivel 2 (SYN). Asimismo, ofrece protección contra ataques DOS/DDoS mediante funciones de protección contra inundaciones UDP/ICMP y de limitación de la tasa de conexión.
Opciones de implementación flexibles	Los productos de la serie SonicWall TZ pueden implementarse en el modo tradicional NAT y en los modos Layer 2 Bridge, Wire Mode y Network Tap.
Soporte para IPv6	La versión 6 del protocolo de Internet (IPv6) se encuentra en las primeras fases para sustituir a IPv4. Con el sistema operativo SonicOS más reciente, el hardware será compatible con las implementaciones de filtrado.
Autenticación biométrica para el acceso remoto	Soporta la autenticación de dispositivos móviles, como el reconocimiento de huellas dactilares, que no pueden ser fácilmente duplicadas ni compartidas, con el fin de autenticar la identidad del usuario de forma segura para que pueda acceder a la red.
Integración de los switches de la serie X de Dell	Gestión de los ajustes de seguridad de los puertos adicionales, incluidos POE y POE+, desde una única consola utilizando un dashboard de la serie TZ con un switch de la serie X (no disponible con el modelo SOHO)

Firewall y interconexión (cont.)	
Prestación	Descripción
Alta disponibilidad	Los modelos SonicWall TZ500 y SonicWall TZ600 ofrecen compatibilidad con las configuraciones de alta disponibilidad activa/en espera con sincronización de estado. Los modelos SonicWall TZ300 y SonicWall TZ400 ofrecen compatibilidad con las configuraciones de alta disponibilidad sin sincronización activa/en espera. Los modelos SonicWall SOHO no cuentan con alta disponibilidad.
API contra amenazas	Permite al firewall recibir cualquier información de inteligencia propietaria, de fabricantes de equipos originales o de terceros para combatir las amenazas avanzadas, como los ataques de día cero, usuarios internos maliciosos, credenciales comprometidas, ransomware y amenazas persistentes avanzadas.
Seguridad de las redes inalámbricas	La tecnología inalámbrica IEEE 802.11ac es capaz de ofrecer hasta 1,3 Gb/s de rendimiento inalámbrico con mayor alcance y fiabilidad. Disponible en los modelos SonicWall de la serie TZ300 a la TZ600. La conectividad 802.11 a/b/g/n está disponible de forma opcional en los modelos SonicWall SOHO.
Gestión e informes	
Prestación	Descripción
Sistema de gestión global	SonicWall GMS supervisa y configura múltiples dispositivos SonicWall y switches de la serie X de Dell y elabora informes sobre ellos a través de una única consola de gestión con una interfaz intuitiva para reducir los costes de gestión y la complejidad.
Potente gestión de dispositivos individuales	Una interfaz basada en Web intuitiva permite llevar a cabo una configuración rápida y sencilla. Además, ofrece una interfaz de línea de comandos integral y compatibilidad con SNMPv2/3.
Informes IPFIX/Netflow de flujos de aplicaciones	Exporta análisis del tráfico de aplicaciones y datos de uso mediante protocolos IPFIX o NetFlow para supervisar y elaborar informes en tiempo real y de datos antiguos con herramientas como SonicWall GMSFlow Server u otras compatibles con IPFIX y NetFlow con extensiones.
Redes privadas virtuales	
Prestación	Descripción
VPN con aprovisionamiento automático	Simplifica y reduce al máximo la complejidad de las implementaciones de firewall distribuidas automatizando el aprovisionamiento inicial de la pasarela VPN de extremo a extremo entre los firewalls de SonicWall, mientras que los sistemas de seguridad y conectividad funcionan de forma instantánea y automática.
VPN IPSec para conectividad entre emplazamientos	La VPN IPSec de alto rendimiento permite que la serie SonicWall TZ actúe como un concentrador VPN para miles de otros emplazamientos grandes, sucursales u oficinas domésticas.
Acceso remoto mediante SSL VPN o cliente IPSec	Permite utilizar la tecnología SSL VPN sin clientes o un cliente IPSec de fácil gestión para el acceso sencillo a e-mails, archivos, ordenadores, sitios Intranet y aplicaciones desde una variedad de plataformas.
Pasarela VPN redundante	Al utilizarse múltiples WANs, pueden configurarse una VPN primaria y otra secundaria para permitir la reconexión y la recuperación automáticas de todas las sesiones VPN.
VPN basada en enrutamiento	El enrutamiento dinámico a través de enlaces VPN garantiza un servicio sin interrupciones en caso de fallo temporal del túnel VPN, ya que el tráfico entre los puntos terminales puede reenrutarse fácilmente a través de rutas alternativas.
Reconocimiento de contenido/contextual	
Prestación	Descripción
Seguimiento de la actividad de los usuarios	Gracias a la integración sin complicaciones de las funciones de SSO con AD/LDAP/Citrix1/Terminal Services, en combinación con la amplia información proporcionada por la DPI, es posible identificar a los usuarios y sus actividades.
GeoIP – Identificación del tráfico en base al país	Identifica y controla el tráfico de red dirigido a, o procedente de, países determinados para ofrecer protección contra ataques de amenazas de origen conocido o sospechoso, o para investigar el tráfico sospechoso originado en la red.
Filtrado DPI de expresiones regulares	Previene la filtración de datos gracias a que identifica y controla el contenido que atraviesa la red mediante la coincidencia de expresiones regulares.

Visión de conjunto de las prestaciones de SonicOS

Firewall

- Inspección dinámica de paquetes
- Inspección profunda de paquetes sin reensamblado
- Protección contra ataques DDoS (inundaciones UDP/ICMP/SYN)
- Soporte para IPv4/IPv6
- Autenticación biométrica para el acceso remoto
- Proxy DNS
- API contra amenazas

Descifrado e inspección SSL/SSH[1]

- Inspección profunda de paquetes para TLS/SSL/SSH
- Inclusión/exclusión de objetos, grupos o nombres de host
- Control SSL

Capture Advanced Threat Protection[1]

- Análisis multimotor basado en la nube
- Sandboxing virtualizado
- Análisis de nivel de hipervisor
- Emulación de sistema completo
- Análisis de gran variedad de tipos de archivos
- Envío automatizado y manual
- Actualizaciones de inteligencia de amenazas en tiempo real
- Función de autobloqueo

Prevención de intrusiones[1]

- Análisis basado en definiciones
- Actualizaciones automáticas de las definiciones
- Inspección bidireccional
- Capacidad para reglas de IPS detalladas
- Filtrado de GeoIP/botnets[2]
- Coincidencia de expresiones regulares

Antimalware[1]

- Análisis de malware basado en flujos
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Inspección bidireccional
- Tamaño de archivo ilimitado
- Base de datos de malware en la nube

Identificación de aplicaciones[1]

- Control de aplicaciones
- Visualización de aplicaciones[2]
- Bloqueo de componentes de aplicaciones
- Gestión del ancho de banda de las aplicaciones
- Creación de definiciones de aplicaciones personalizadas
- Prevención de filtración de datos
- Informes de aplicaciones mediante NetFlow/IPFIX
- Seguimiento de la actividad de los usuarios (SSO)
- Completa base de datos de definiciones de aplicaciones

Filtrado de contenido Web[1]

- Filtrado de URL
- Tecnología antiproxy
- Bloqueo según palabras clave
- Gestión del ancho de banda según categorías de clasificación CFS
- Modelo de políticas unificadas con control de aplicaciones
- Content Filtering Client

VPN

- VPN con aprovisionamiento automático
- VPN IPSec para conectividad entre emplazamientos
- Acceso remoto mediante VPN SSL y cliente IPSec
- Pasarela VPN redundante
- Mobile Connect para iOS, Mac OS X, Windows, Chrome, Android y Kindle Fire
- VPN basada en rutas (OSPF, RIP, BGP)

Interconexión

- PortShield
- Protocolización mejorada
- QoS de nivel 2
- Seguridad de puertos
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Controlador inalámbrico de SonicWall
- Enrutamiento basado en políticas (ToS/metric y ECMP)
- Enrutamiento asimétrico
- Servidor DHCP
- NAT
- Gestión del ancho de banda
- Alta disponibilidad - Activa/en espera con sincronización de estado[3]
- Equilibrio de carga entrante/saliente
- Modo L2 bridge, modo NAT
- Reconexión WAN 3G/4G
- Compatibilidad con tarjetas Common Access Card (CAC)

VoIP

- Control QoS granular
- Gestión del ancho de banda
- DPI para tráfico VoIP
- Soporte de Gatekeeper H.323 y proxy SIP

Gestión y supervisión

- GUI Web
- Interfaz de línea de comandos (CLI)
- SNMPv2/v3
- Gestión e informes centralizados con SonicWall GMS
- Protocolización
- Exportaciones NetFlow/IPFIX
- Backup de configuración basado en la nube
- Visualización de aplicaciones y ancho de banda
- Gestión de IPv4 e IPv6
- Gestión de switches de la serie Dell X, incluidos switches en cascada

Conexión inalámbrica integrada

- Doble banda (2,4 GHz y 5,0 GHz)
- Estándares inalámbricos 802.11 a/b/g/n/ac[2]
- Detección y prevención de intrusiones inalámbricas
- Servicios inalámbricos para usuarios invitados
- Mensajería ligera en puntos de conexión
- Segmentación mediante puntos de acceso virtuales
- Portal cautivo
- ACL para la nube

[1] *Requiere suscripción adicional*
[2] *No disponible en la serie SOHO*
[3] *La alta disponibilidad con sincronización de estado solo está disponible en los modelos SonicWall TZ500 y SonicWall TZ600*

Especificaciones del sistema de la serie SonicWall TZ

Hardware - Visión general	Serie SOHO	Serie TZ300	Serie TZ400	Serie TZ500	TZ600
Sistema operativo	SonicOS				
Núcleos de procesamiento de seguridad	2	2	4	4	4
Interfaces	5x1GbE, 1 USB, 1 Consola	5x1GbE, 1 USB, 1 Consola	7x1GbE, 1 USB, 1 Consola	8x1GbE, 2 USB, 1 Consola	10x1GbE, 2 USB, 1 Consola, 1 ranura de expansión
Expansión	USB	USB	USB	2 USB	Ranura de expansión (posterior),* 2 USB
Usuarios con inicio de sesión único (SSO)	250	500	500	500	500
Interfaces VLAN	25	25	50	50	50
Puntos de acceso soportados (máximo)	2	8	16	16	24
Modelos de switches de la serie X de Dell soportados	No disponible	X1008/P, X1018/P, X1026/P, X1052/P, X4012			
Rendimiento de firewall/VPN	**Serie SOHO**	**Serie TZ300**	**Serie TZ400**	**Serie TZ500**	**TZ600**
Rendimiento de inspección del firewall[1]	300 Mbps	750 Mbps	1.300 Mbps	1.400 Mbps	1.500 Mbps
Rendimiento de DPI completo[2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Rendimiento de inspección de aplicaciones[2]	-	300 Mbps	900 Mbps	1.000 Mbps	1.100 Mbps
Rendimiento de IPS[2]	100 Mbps	300 Mbps	900 Mbps	1.000 Mbps	1.100 Mbps
Rendimiento de inspección antimalware[2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Rendimiento de IMIX	60 Mbps	200 Mbps	500 Mbps	700 Mbps	900 Mbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL)[2]	15 Mbps	45 Mbps	100 Mbps	150 Mbps	200 Mbps
Rendimiento de VPN IPSec[3]	100 Mbps	300 Mbps	900 Mbps	1.000 Mbps	1.100 Mbps
Conexiones por segundo	1.800	5.000	6.000	8.000	12.000
Conexiones máximas (SPI)	10.000	50.000	100.000	125.000	150.000
Número máximo de conexiones (DPI)	10.000	50.000	90.000	100.000	125.000
Número máximo de conexiones (DPI SSL)	100	500	500	750	750
VPN	**Serie SOHO**	**Serie TZ300**	**Serie TZ400**	**Serie TZ500**	**TZ600**
Túneles VPN entre emplazamientos	10	10	20	25	50
Clientes VPN IPSec (máximo)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
Licencias de VPN SSL (máximo)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Virtual Assist incluido (máximo)	-	1 (prueba de 30 días)	1 (prueba de 30 días)	1 (prueba de 30 días)	1 (prueba de 30 días)
Cifrado/autenticación	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, criptografía Suite B				
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14				
VPN basada en enrutamiento	RIP, OSPF				
Soporte de certificados	Verisign, Thawte, Cybertrust, RSA Keon, Entrust, y Microsoft CA para VPN SonicWall-SonicWall VPN, SCEP				
Prestaciones VPN	Dead Peer Detection, DHCP a través de VPN, IPSec NAT Traversal, pasarela VPN redundante, VPN basada en enrutamiento				
Plataformas de cliente VPN globales admitidas	Microsoft® Windows Vista de 32/64 bits, Windows 7 de 32/64 bits, Windows 8.0 de 32/64 bits, Windows 8.1 de 32/64 bits, Windows 10				
NetExtender	Microsoft Windows Vista de 32/64 bits, Windows 7, Windows 8.0 de 32/64 bits, Windows 8.1 de 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 (integrado)				
Servicios de seguridad	**Serie SOHO**	**Serie TZ300**	**Serie TZ400**	**Serie TZ500**	**TZ600**
Servicios Deep Packet Inspection	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL				
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, análisis de contenidos y palabras clave, filtrado completo basado en tipos de archivo como ActiveX, Java, cookies para la privacidad, listas de permitidos/denegados				
Enforced Client Anti-Virus and Anti-Spyware	McAfee® y Kaspersky™				
Comprehensive Anti-Spam Service	Soportado				
Visualización de aplicaciones	No	Sí	Sí	Sí	Sí
Control de aplicaciones	Sí	Sí	Sí	Sí	Sí
Capture Advanced Threat Protection	No	Sí	Sí	Sí	Sí

SONICWALL®

Especificaciones del sistema de la serie SonicWall TZ (cont.)

Interconexión	Serie SOHO	Serie TZ300	Serie TZ400	Serie TZ500	TZ600
Asignación de direcciones IP	Estática, (cliente DHCP, PPPoE, L2TP y PPTP), servidor DHCP interno, relé DHCP				
Modos NAT	1:1, 1:muchos, muchos:1, muchos:muchos, NAT flexible (IPs solapadas), PAT, modo transparente				
Protocolos de enrutamiento[4]	BGP[4], OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas				
QoS	Prioridad de ancho de banda, ancho de banda máximo, ancho de banda garantizado, marcado DSCP, 802.1e (WMM)				
Autenticación	LDAP (múltiples dominios), XAUTH/ RADIUS, SSO, Novell, base de datos de usuarios interna	LDAP (múltiples dominios), XAUTH/RADIUS, SSO, Novell, base de datos de usuarios interna, Terminal Services, Citrix			
Base de datos de usuarios local	150			250	
VoIP	H.323 v1-5 completo, SIP				
Estándares	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certificaciones	FIPS 140-2 (con Suite B) nivel 2, UC APL, VPNC, IPv6 (fase 2), ICSA Network Firewall, ICSA Anti-virus				
Certificaciones pendientes	Common Criteria NDPP				
Tarjetas Common Access Card (CAC)	Soportado				
Alta disponibilidad	No	Activo/en espera	Activo/en espera	Activo/en espera con sincronización de estado	Activo/en espera con sincronización de estado
Hardware	**Serie SOHO**	**Serie TZ300**	**Serie TZ400**	**Serie TZ500**	**TZ600**
Factor de forma	PC de escritorio				
Fuente de alimentación (W)	24 W (externa)	24 W (externa)	24 W (externa)	36 W (externa)	60W (externa)
Consumo máximo de energía (W)	6,4/11,3	6,9/12,0	9,2/13,8	13,4/17,7	16,1
Potencia de entrada	De 100 a 240 V CA, 50-60 Hz, 1 A				
Disipación de calor total	21,8/38,7 BTU	23,5/40,9 BTU	31,3/47,1 BTU	45,9/60,5 BTU	55,1 BTU
Dimensiones	3,6 x 14,1 x 19 cm	3,5 x 13,4 x 19 cm	3,5 x 13,4 x 19 cm	3,5 x 15 x 22,5 cm	3,5 x 18 x 28 cm
Peso	0,34 kg/0,75 libras 0,48 kg/1,06 libras	0,73 kg/1,61 libras 0,84 kg/1,85 libras	0,73 kg/1,61 libras 0,84 kg/1,85 libras	0,92 kg/2,03 libras 1,05 kg/2,31 libras	1,47 kg/3,24 libras
Peso WEEE	0,80 kg/1,76 libras 0,94 kg/2,07 libras	1,15 kg/2,53 libras 1,26 kg/2,78 libras	1,15 kg/2,53 libras 1,26 kg/2,78 libras	1,34 kg/2,95 libras 1,48 kg/3,26 libras	1,89 kg/4,16 libras
Peso de envío	1,20 kg/2,64 libras 1,34 kg/2,95 libras	1,37 kg/3,02 libras 1,48 kg/3,26 libras	1,37 kg/3,02 libras 1,48 kg/3,26 libras	1,93 kg/4,25 libras 2,07 kg/4,56 libras	2,48 kg/5,47 libras
MTBF (años)	58,9/56,1 (inalámbrico)	56,1	54,0	40,8	18,4
Entorno (Operativo/Almacenamiento)	0°-40° C (32°-105° F)/-40° a 70° C (-40° a 158° F)				
Humedad	5-95%, sin condensación				
Normativas	**Serie SOHO**	**Serie TZ300**	**Serie TZ400**	**Serie TZ500**	**TZ600**
Modelo normativo (por cable)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Cumplimiento de normas (modelos por cable)	FCC Clase B, ICES Clase B, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase B, UL, cUL, TUV/GS, CB, Certificado de cumplimiento para México por UL, WEEE , REACH, KCC/MSIP	FCC Clase B, ICES Clase B, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase B, UL, cUL, TUV/GS, CB, Certificado de cumplimiento para México por UL, WEEE , REACH, KCC/MSIP	FCC Clase B, ICES Clase B, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase B, UL, cUL, TUV/GS, CB, Certificado de cumplimiento para México por UL, WEEE , REACH, KCC/MSIP	FCC Clase B, ICES Clase B, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase B, UL, cUL, TUV/GS, CB, Certificado de cumplimiento para México por UL, WEEE , REACH, BSMI, KCC/MSIP	FCC Clase A, ICES Clase A, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase A, UL, cUL, TUV/ GS, CB, Certificado de cumplimiento para México por UL, WEEE , REACH, KCC/MSIP
Modelo normativo (por cable)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Cumplimiento de las principales reglas normativas (modelos inalámbricos)	FCC Clase B, FCC RF ICES Clase B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Clase B, MIC/TELEC, UL, cUL, TUV/GS, CB, certificado de cumplimiento para México por UL, RAEE, REACH	FCC Clase B, FCC RF ICES Clase B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Clase B, MIC/TELEC, UL, cUL, TUV/GS, CB, certificado de cumplimiento para México por UL, RAEE, REACH	FCC Clase B, FCC RF ICES Clase B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Clase B, MIC/TELEC, UL, cUL, TUV/GS, CB, certificado de cumplimiento para México por UL, RAEE, REACH	FCC Clase B, FCC RF ICES Clase B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Clase B, MIC/TELEC, UL, cUL, TUV/GS, CB, certificado de cumplimiento para México por UL, RAEE, REACH	-

Especificaciones del sistema de la serie SonicWall TZ (cont.)

Conexión inalámbrica integrada	Serie SOHO	Serie TZ300, TZ400 y TZ500	TZ600
Estándares	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)	-
Bandas de frecuencia[5]	802.11a: 5180-5825 GHz; 802.11b/g: 2412-2472 GHz; 802.11n: 2412-2472 GHz, 5180-5825 GHz;	802.11a: 5180-5825 GHz; 802.11b/g: 2412-2472 GHz; 802.11n: 2412-2472 GHz, 5180-5825 GHz; 802.11ac: 2,412-2,472 GHz, 5,180-5,825 GHz	-
Canales operativos	802.11a: Canadá y EE. UU. 12, Europa 11, Japón 4, Singapur 4, Taiwán 4; 802.11b/g: 1-11, Europa 1-13, Japón 1-14 (14 solo 802.11b); 802.11n (2,4 GHz): Canadá y EE. UU. 1-11, Europa 1-13, Japón 1-13; 802.11n (5 GHz): Canadá y EE. UU. 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64;	802.11a: Canadá y EE. UU. 12, Europa 11, Japón 4, Singapur 4, Taiwán 4; 802.11b/g: 1-11, Europa 1-13, Japón 1-14 (14 solo 802.11b); 802.11n (2,4 GHz): Canadá y EE. UU. 1-11, Europa 1-13, Japón 1-13; 802.11n (5 GHz): Canadá y EE. UU. 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64; 802.11ac: Canadá y EE. UU. 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64	-
Potencia de salida de transmisión	Se basa en el dominio normativo especificado por el administrador del sistema	Se basa en el dominio normativo especificado por el administrador del sistema	-
Control de la potencia de transmisión	Soportado	Soportado	-
Velocidades de transferencia admitidas	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s por canal; 802.11b: 1, 2, 5,5, 11 Mb/s por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s por 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 Mb/s por canal;	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s por canal; 802.11b: 1, 2, 5,5, 11 Mb/s por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s por 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 Mb/s por 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 Mb/s por canal	-
Espectro de la tecnología de modulación	802.11a: Multiplexación por división de frecuencias ortogonales (OFDM); 802.11b: Espectro expandido de secuencia directa (DSSS); 802.11g: Multiplexación por división de frecuencias ortogonales (OFDM)/Espectro expandido de secuencia directa (DSSS); 802.11n: Multiplexación por división de frecuencias ortogonales (OFDM)	802.11a: Multiplexación por división de frecuencias ortogonales (OFDM); 802.11b: Espectro expandido de secuencia directa (DSSS); 802.11g: Multiplexación por división de frecuencias ortogonales (OFDM)/Espectro expandido de secuencia directa (DSSS); 802.11n: Multiplexación por división de frecuencias ortogonales (OFDM); 802.11ac: Multiplexación por división de frecuencias ortogonales (OFDM)	-

**Uso futuro.*

[1] *Métodos de prueba: Rendimiento máximo basado en RFC 2544 (para firewall). El rendimiento real puede variar dependiendo de las condiciones de la red y de los servicios activados.*

[2] *Rendimiento DPI pleno/Gateway AV/Anti-Spyware/IPS medido mediante la prueba de rendimiento HTTP estándar Spirent WebAvalanche y herramientas de prueba Ixia. Para las pruebas se han utilizado múltiples flujos a través de múltiples pares de puertos.*

[3] *Medición del rendimiento de VPN basada en el tráfico UDP con paquetes de 1280 bytes de conformidad con RFC 2544. Las especificaciones, las prestaciones y la disponibilidad están sujetas a modificaciones.*

[4] *BGP solo está disponible en SonicWall TZ400, TZ500 y TZ600.*

[5] *Todos los modelos TZ inalámbricos integrados pueden soportar bandas de 2,4GHz ó 5GHz. Para soporte de banda dual, utilice los productos de puntos de acceso inalámbricos de SonicWall (SonicPoints)*

Información para pedidos de la serie SonicWall TZ

Producto	SKU
SonicWall SOHO con 1 año de TotalSecure	01-SSC-0651
SonicWall SOHO Wireless-N con 1 año de TotalSecure	01-SSC-0653
SonicWall TZ300 con 1 año de TotalSecure	01-SSC-0581
SonicWall TZ300 Wireless-AC con 1 año de TotalSecure	01-SSC-0583
SonicWall TZ400 con 1 año de TotalSecure	01-SSC-0514
SonicWall TZ400 Wireless-AC con 1 año de TotalSecure	01-SSC-0516
SonicWall TZ500 con 1 año de TotalSecure	01-SSC-0445
SonicWall TZ500 Wireless-AC con 1 año de TotalSecure	01-SSC-0446
SonicWall TZ600 con 1 año de TotalSecure	01-SSC-0219
Opciones de alta disponibilidad (todas las unidades deben ser del mismo modelo)	
SonicWall TZ500 con alta disponibilidad	01-SSC-0439
SonicWall TZ600 con alta disponibilidad	01-SSC-0220

Información para pedidos de la serie SonicWall TZ

Servicios	SKU
Para la serie SonicWall SOHO	
Comprehensive Gateway Security Suite (1 año)	01-SSC-0688
Gateway Anti-Virus, Intrusion Prevention y Application Control (1 año)	01-SSC-0670
Content Filtering Service (1 año)	01-SSC-0676
Comprehensive Anti-Spam Service (1 año)	01-SSC-0682
Soporte 24x7 (1 año)	01-SSC-0700
Para la serie SonicWall TZ300	
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para TZ300 (1 año)	01-SSC-1430
Capture Advanced Threat Protection para TZ300 (1 año)	01-SSC-1435
Gateway Anti-Virus, Intrusion Prevention y Application Control (1 año)	01-SSC-0602
Content Filtering Service (1 año)	01-SSC-0608
Comprehensive Anti-Spam Service (1 año)	01-SSC-0632
Soporte 24x7 (1 año)	01-SSC-0620
Para la serie SonicWall TZ400	
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para TZ400 (1 año)	01-SSC-1440
Capture Advanced Threat Protection para TZ400 (1 año)	01-SSC-1445
Gateway Anti-Virus, Intrusion Prevention y Application Control (1 año)	01-SSC-0534
Content Filtering Service (1 año)	01-SSC-0540
Comprehensive Anti-Spam Service (1 año)	01-SSC-0561
Soporte 24x7 (1 año)	01-SSC-0552
Para la serie SonicWall TZ500	
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para TZ500 (1 año)	01-SSC-1450
Capture Advanced Threat Protection para TZ500 (1 año)	01-SSC-1455
Gateway Anti-Virus, Intrusion Prevention y Application Control (1 año)	01-SSC-0458
Content Filtering Service (1 año)	01-SSC-0464
Comprehensive Anti-Spam Service (1 año)	01-SSC-0482
Soporte 24x7 (1 año)	01-SSC-0476
Para SonicWall TZ600	
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para TZ600 (1 año)	01-SSC-1460
Capture Advanced Threat Protection para TZ600 (1 año)	01-SSC-1465
Gateway Anti-Virus, Intrusion Prevention y Application Control (1 año)	01-SSC-0228
Content Filtering Service (1 año)	01-SSC-0234
Comprehensive Anti-Spam Service (1 año)	01-SSC-0252
Soporte 24x7 (1 año)	01-SSC-0246

Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios globales en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com

Datasheet-TZ Series-US-VG-MKTG658