SONICWALL

Serie SonicWall TZ

Prevención de amenazas integrada y plataforma SD-Branch para pequeñas y medianas empresas y empresas distribuidas

Con la serie SonicWall TZ, las organizaciones pequeñas y medianas y las empresas distribuidas disfrutan de las ventajas de una solución de seguridad integrada que satisface todas sus necesidades. Gracias a la combinación de unas funciones de prevención de amenazas de alta velocidad y la tecnología de red de área amplia definida por software (SD-WAN) con una amplia variedad de prestaciones de redes y de conectividad inalámbrica de implementación más simplificada y gestión centralizada, la serie TZ proporciona una solución de seguridad unificada a un coste total de propiedad reducido.

Solución de seguridad flexible e integrada

La serie TZ se basa en SonicOS, el sistema operativo de SonicWall, que ofrece gran cantidad de prestaciones. Los firewalls compatibles con el último sistema operativo SonicOS 7.0 incorporan una nueva UI/UX de aspecto moderno, funciones avanzadas de seguridad, conexión de red y gestión simplificada de políticas.

SonicOS incluye además un potente conjunto de prestaciones que proporcionan a las organizaciones la flexibilidad necesaria para ajustar estos firewalls de Gestión unificada de amenazas (UTM) a sus requisitos de red específicos. Por ejemplo, el controlador inalámbrico integrado, compatible con las normas IEEE 802.11, así como la posibilidad de añadir nuestros access points SonicWave 802.11ac Wave 2, simplifican la creación de una red inalámbrica de alta velocidad. Con el fin de reducir el coste y la complejidad de la conexión de access points inalámbricos de alta velocidad y otros dispositivos con tecnología de Alimentación por Ethernet (PoE), como cámaras IP, teléfonos e impresoras, los firewalls TZ300P, TZ600P y TZ570P ofrecen alimentación PoE/PoE+.

Las empresas minoristas distribuidas y los entornos de campus pueden utilizar las numerosas herramientas de SonicOS para obtener mayores ventajas. Las sucursales pueden intercambiar información con la oficina central de forma segura utilizando redes privadas virtuales (VPN). La creación de redes LAN virtuales (VLANs) permite segmentar la red en grupos corporativos y de clientes con normas que determinan el nivel de comunicación con dispositivos de otras VLANs. SD-WAN ofrece una alternativa segura a los costosos circuitos MPLS al tiempo que proporciona un rendimiento y una disponibilidad constante de las aplicaciones. La implementación Zero-Touch, que permite aprovisionar el firewall de forma remota a través de la nube, simplifica la instalación de los firewalls TZ en ubicaciones remotas.

Prevención de amenazas y rendimiento superiores

Nuestra visión para la protección de las redes en el actual panorama de las amenazas cibernéticas, en continua evolución, consiste en la detección y la prevención de amenazas en tiempo real y automatizadas. Gracias a la combinación de tecnologías basadas en la nube e integradas, nuestros firewalls cuentan con una sólida protección validada por las pruebas realizadas por terceros independientes y se caracterizan por ofrecer un nivel extremadamente alto de efectividad de la seguridad. Las amenazas desconocidas se envían al sandbox multimotor basado en la nube Capture Advanced Threat Protection (ATP) de SonicWall para su análisis. Además, la tecnología pendiente de patente de Inspección de memoria

Ventajas:

Solución de seguridad flexible e integrada

- Interfaces multigigabit con un factor de forma de sobremesa
- SD-Branch segura con SD-WAN
- Potente sistema operativo SonicOS 7.0
- Conectividad inalámbrica 802.11ac Wave 2 de alta velocidad
- Alimentación por Ethernet (PoE/ PoE+)
- Compatibilidad con 5G/4G/LTE
- Almacenamiento integrado y ampliable
- Alimentación redundante

Prevención de amenazas y rendimiento de calidad superior

- Tecnología de Inspección profunda de memoria en tiempo real pendiente de patente
- Tecnología patentada de inspección profunda de paquetes sin reensamblado
- Compatibilidad con TLS 1.3
- Efectividad de la seguridad validada por la industria

Funciones sencillas de implementación, configuración y gestión continua

- Implementación Zero-Touch
- Gestión centralizada, basada en la nube y local
- Incorporación de la aplicación SonicExpress

profunda en tiempo real (RTDMI™) aumenta la eficacia de Capture ATP. El motor RTDMI detecta y bloquea el malware y las amenazas de día cero mediante una inspección directa en la memoria. La tecnología RTDMI es precisa, minimiza los falsos positivos e identifica y mitiga los ataques sofisticados en los que las armas del malware se exponen durante menos de 100 nanosegundos. En combinación con ella, nuestro motor patentado de un solo paso* de Inspección profunda de paquetes sin reensamblado (RFDPI) examina cada byte de cada paquete e inspecciona el tráfico entrante y saliente directamente en el firewall. Al utilizar Capture ATP con la tecnología RTDMI en la plataforma SonicWall Capture Cloud junto con las prestaciones integradas, como prevención de intrusiones, antimalware y filtrado Web/ URL, los firewalls de la serie TZ detienen el malware, el ransomware y otras amenazas en la gateway. Para los dispositivos móviles utilizados fuera del perímetro del firewall, SonicWall Capture Client proporciona una capa de protección añadida mediante la aplicación de técnicas de protección contra amenazas avanzadas, como el aprendizaje automático y la reversión de sistemas. Capture Client también utiliza la inspección profunda del tráfico cifrado mediante TLS (DPI-SSL) de los firewalls de la serie TZ gracias a la instalación y gestión de certificados TLS de confianza.

Puesto que cada vez se utilizan más las tecnologías de cifrado para proteger las sesiones Web, los firewalls deben ser capaces de escanear el tráfico cifrado para detectar amenazas. Los firewalls de la serie TZ proporcionan una protección completa al descifrar e inspeccionar las conexiones cifradas mediante TLS/ SSL y SSH, independientemente del puerto o del protocolo. El firewall busca incumplimientos de protocolos, amenazas, ataques de día cero, intrusiones e incluso criterios definidos analizando en profundidad cada paquete. Este motor de inspección profunda de paquetes detecta y previene los ataques ocultos que utilizan criptografía. Asimismo, bloquea las descargas de malware cifrado, detiene la propagación de infecciones y frustra las comunicaciones de comando y control y la exfiltración de datos. Las normas de inclusión y exclusión proporcionan un control total que permite personalizar qué tráfico debe ser sometido al descifrado y a la inspección con arreglo a los requisitos legales y/o corporativos específicos.

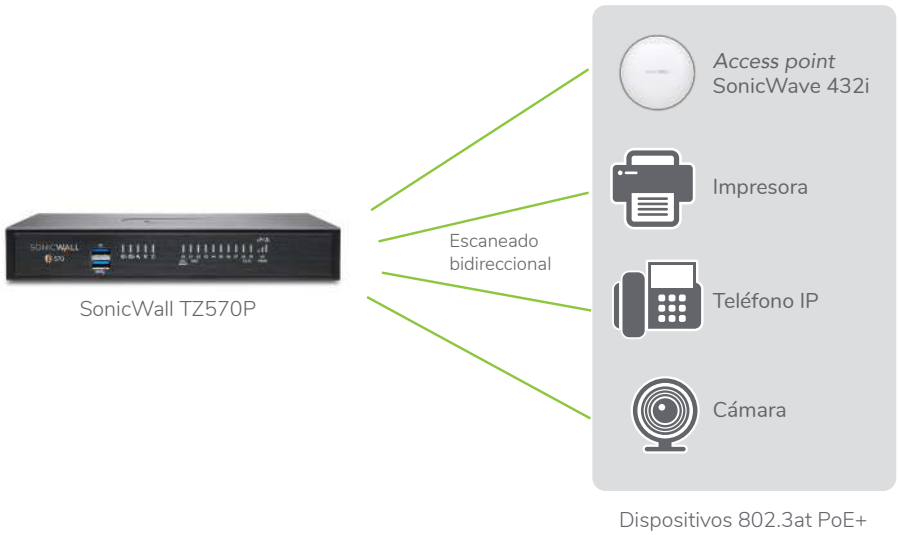
Los firewalls TZ670 y TZ570 son compatibles con TLS 1.3, que ofrece varios cambios que mejoran el rendimiento y la seguridad, a la vez que elimina complejidades.

Funciones sencillas de implementación, configuración y gestión continua

SonicWall simplifica la configuración y la gestión de los firewalls de la serie TZ y los *access points* SonicWave 802.11ac Wave 2, independientemente de dónde se implementen. La gestión, los informes, las licencias y los análisis se centralizan en nuestro Capture Security Center basado en la nube, que ofrece el máximo nivel de visibilidad, agilidad y capacidad de controlar todo el ecosistema de seguridad de SonicWall de forma centralizada desde una única consola.

Un componente clave del Capture Security Center es la implementación Zero-Touch. Esta prestación basada en la nube simplifica y acelera la implementación y el aprovisionamiento de los firewalls SonicWall en ubicaciones remotas y sucursales. El proceso requiere una intervención mínima por parte del usuario y pone en funcionamiento de forma completamente automatizada los firewalls a escala en tan solo unos pasos. Esto reduce considerablemente el tiempo, el coste y la complejidad asociados a la instalación y la configuración, mientras que la seguridad y la conectividad se producen de forma instantánea y automática. La implementación y la configuración simplificadas, junto con la facilidad de gestión, permiten a las organizaciones reducir el coste total de propiedad y obtener un elevado rendimiento de la inversión.

** 802.11ac no está disponible actualmente en los modelos SOHO/SOHO 250; los modelos SOHO/SOHO 250 admiten 802.11a/b/g/n*



Dispositivos 802.3at PoE+

Seguridad integrada y alimentación para sus dispositivos con tecnología PoE

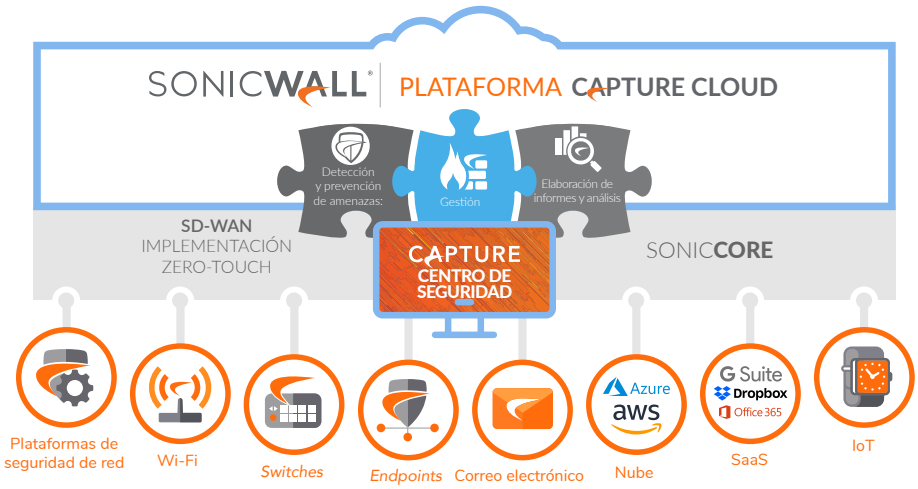
Proporcione alimentación a sus dispositivos con tecnología PoE sin el coste ni la complejidad de un switch o un inyector de Alimentación por Ethernet. Los firewalls TZ300P, TZ600P y TZ570P integran tecnología IEEE 802.3at para alimentar los dispositivos PoE y PoE+, como access points inalámbricos, cámaras, teléfonos IP, etc. El firewall escanea todo el tráfico procedente de y destinado a cada dispositivo utilizando tecnología de inspección profunda de paquetes y a continuación elimina las amenazas dañinas, como el malware y las intrusiones, incluso en las conexiones cifradas.

Plataforma Capture Cloud

La plataforma Capture Cloud de SonicWall proporciona funciones de prevención de amenazas y gestión de red basadas en la nube, así como informes y análisis, para organizaciones de cualquier tamaño. La plataforma consolida la inteligencia de amenazas recopilada de diversas fuentes, incluido nuestro galardonado servicio de sandboxing de red multimotor, Capture Advanced Threat Protection, así como más de un millón de sensores de SonicWall situados en todo el mundo.

Si se detecta que los datos que acceden a la red contienen un código malicioso nunca visto hasta ahora, el equipo de investigación de amenazas interno y especializado de SonicWall Capture Labs, desarrolla definiciones que se almacenan en la base de datos de la plataforma Capture Cloud y se implementan en los firewalls de los clientes para ofrecer una protección actualizada. Las nuevas actualizaciones tienen efecto inmediato sin necesidad de reiniciar ni interrumpir el sistema. Las definiciones residentes en el dispositivo ofrecen protección contra una amplia variedad de tipos de ataques, cubriendo decenas de miles de amenazas individuales. Además de las contramedidas integradas en el dispositivo, los firewalls TZ también tienen acceso continuo a la base de datos de la plataforma Capture Cloud, que incluye decenas de millones de definiciones.

Junto con la prevención de amenazas, la plataforma Capture Cloud ofrece también una consola de gestión única y permite a los administradores crear fácilmente informes tanto históricos como en tiempo real sobre la actividad de la red.



Protección contra amenazas avanzadas

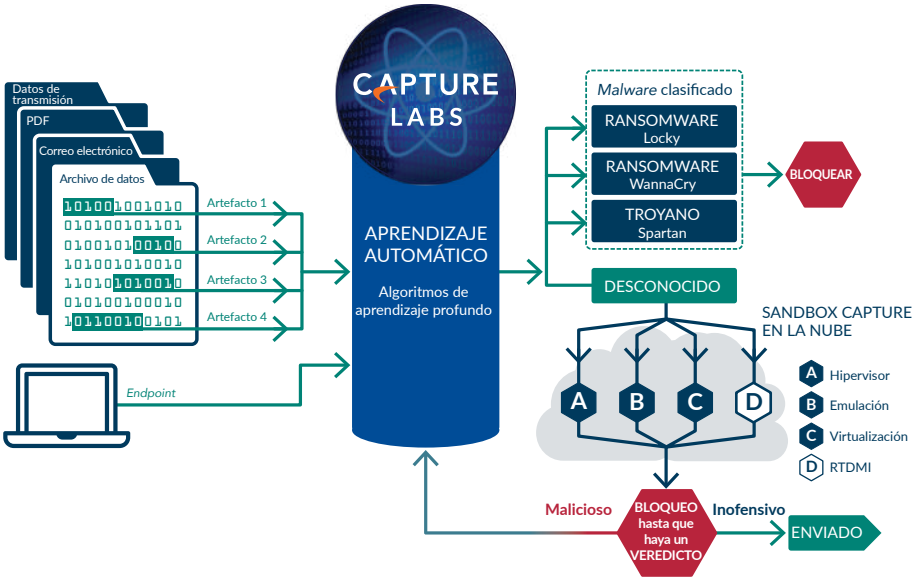
La prevención de infracciones automatizada y en tiempo real de SonicWall se basa en dos tecnologías avanzadas de detección de malware: Capture Advanced Threat Protection™ (Capture ATP) y Capture Security appliance™ (CSa).

Capture ATP es una plataforma de *sandbox* multimotor en la nube, que incluye Real-Time Deep Memory Inspection™ (RTDMI), *sandboxing* virtualizado, emulación completa de sistema y tecnología de análisis a nivel hipervisor. CSa es un dispositivo local equipado con RTDMI, que utiliza técnicas estáticas y dinámicas basadas en la memoria para obtener veredictos rápidos y precisos. Ambas soluciones amplían la protección avanzada contra amenazas para detectar y prevenir los ataques de día cero en distintas soluciones SonicWall, como los firewalls de nueva generación.

Los archivos sospechosos se envían a una de estas soluciones, donde se analizan utilizando algoritmos de aprendizaje profundo, con la posibilidad de retenerlos en la gateway hasta que se emita un veredicto. En el caso de Capture ATP, se bloquean los archivos identificados como maliciosos y se crea inmediatamente un *hash* dentro de la base de datos de Capture ATP para que todos los clientes puedan aprovecharlo para bloquear los posteriores ataques. Estas definiciones se envían después a los firewalls para crear defensas estáticas. Por razones legales y de privacidad, los resultados generados por CSa no se comparten fuera de su organización.

Estos servicios analizan una amplia variedad de sistemas operativos y tipos de archivos, incluidos programas ejecutables, DLL, archivos PDF, documentos MS Office, archivos, JAR y APK.

Con el fin de ofrecer una protección de *endpoints* completa, SonicWall Capture Client combina tecnología antivirus de última generación con el *sandbox* multimotor basado en la nube de SonicWall con integración opcional en firewalls SonicWall.

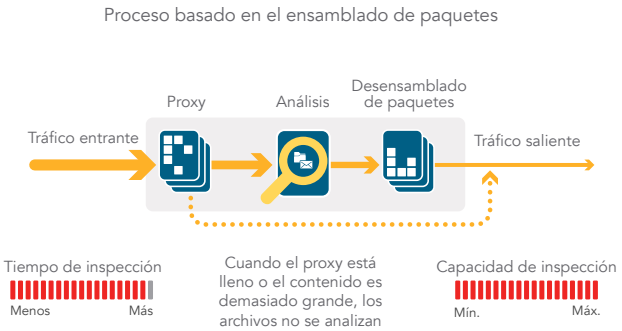


Motor de inspección profunda de paquetes sin reensamblado

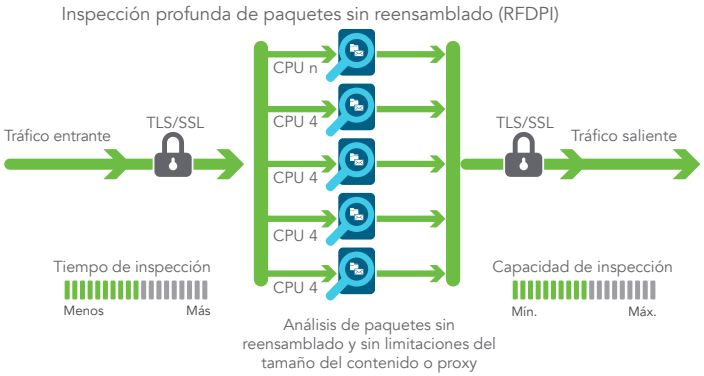
La Inspección profunda de paquetes sin reensamblado (RFDPI) de SonicWall es un sistema de inspección de un solo paso y baja latencia que realiza análisis bidireccionales del tráfico basados en flujos a alta velocidad sin almacenamiento en búfer ni proxys a fin de descubrir posibles intentos de intrusión o descargas de *malware* y de identificar el tráfico de aplicaciones independientemente del puerto y del protocolo. Este motor patentado se basa en la inspección de los datos útiles del tráfico de datos para detectar amenazas en las capas 3-7 y 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 que un paquete se somete al preprocesamiento necesario, incluido el descifrado TLS/SSL, es analizado con la ayuda de una única representación en memoria patentada de tres bases de datos de definiciones: ataques de intrusión, *malware* y aplicaciones. El estado de conexión se actualiza constantemente en el firewall y se coteja con estas bases de datos hasta que se identifica un ataque u otro evento de seguridad, en cuyo caso se lleva a cabo una acción preestablecida.

En la mayoría de los casos, el sistema finaliza la conexión y crea eventos de protocolización y notificación. No obstante, el motor también puede configurarse para realizar únicamente la inspección o, en caso de detección de aplicaciones, para proporcionar servicios de gestión de ancho de banda de capa 7 para el resto del flujo de aplicaciones tan pronto como se identifique una aplicación.



Arquitectura competitiva basada en proxy (competencia)



Arquitectura basada en flujos de SonicWall

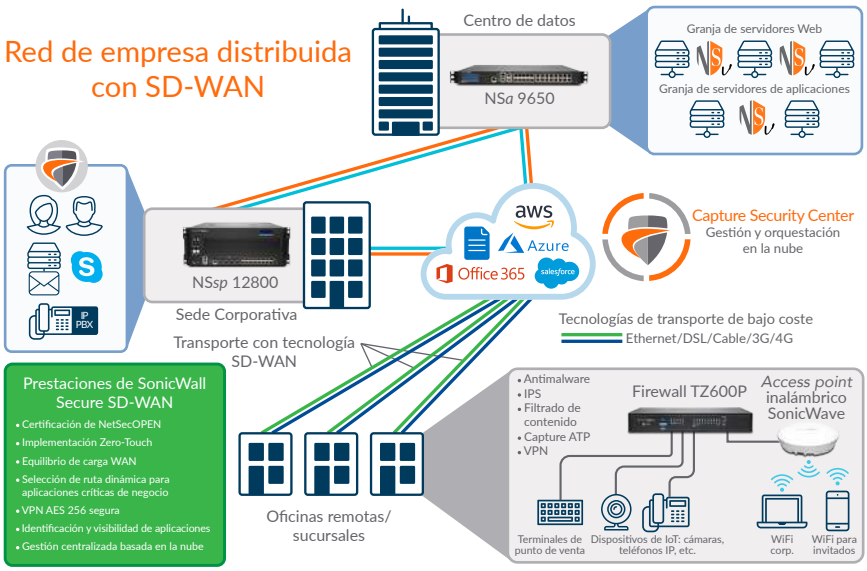
Elaboración de informes y gestión centralizadas

Para organizaciones altamente reguladas que deseen coordinar la seguridad, el control, el cumplimiento normativo y su estrategia de gestión de riesgos, SonicWall proporciona a los administradores una plataforma unificada, segura y ampliable para gestionar los firewalls, *access points* inalámbricos y switches de la serie N y de la serie X de Dell mediante un proceso de flujo de trabajo correlacionado y auditable. Las empresas pueden consolidar fácilmente la gestión de los 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, las actividades de los usuarios, la identificación de aplicaciones, los análisis de flujos y forenses, los informes de cumplimiento y de auditorías, entre otras funciones. Además, las empresas consiguen cumplir los requisitos de gestión de cambios del firewall mediante la automatización del flujo de trabajo, que proporciona la agilidad y la confianza necesarias para implementar las políticas de firewalls apropiadas en el momento oportuno y de conformidad con la normativa vigente. Disponibles de forma local como Sistema de gestión global de SonicWall y en la nube como Centro de seguridad de Capture, las soluciones de gestión e informes de SonicWall proporcionan una forma coherente de gestionar la seguridad de la red mediante procesos de negocio y niveles de servicio. De esta forma simplifican drásticamente la gestión del ciclo de vida de sus entornos de seguridad, en comparación con la gestión dispositivo por dispositivo.

Redes distribuidas

Por su flexibilidad, los firewalls de la serie TZ son ideales tanto para empresas distribuidas como para implementaciones de un solo emplazamiento. En las redes distribuidas, como las de las organizaciones minoristas, cada emplazamiento tiene su propio firewall TZ, que a menudo se conecta a Internet a través de un proveedor local utilizando una conexión DSL, por cable o 3G/4G. Además del acceso a Internet, cada firewall utiliza una conexión Ethernet para transportar los paquetes entre los emplazamientos remotos y la sede central. Desde el centro de datos, se ponen a disposición servicios Web y aplicaciones SaaS, como Office 365, Salesforce, etc. Utilizando tecnología de VPN en malla, los administradores de TI pueden crear una configuración "hub and spoke" para el transporte seguro de datos entre todas las ubicaciones.

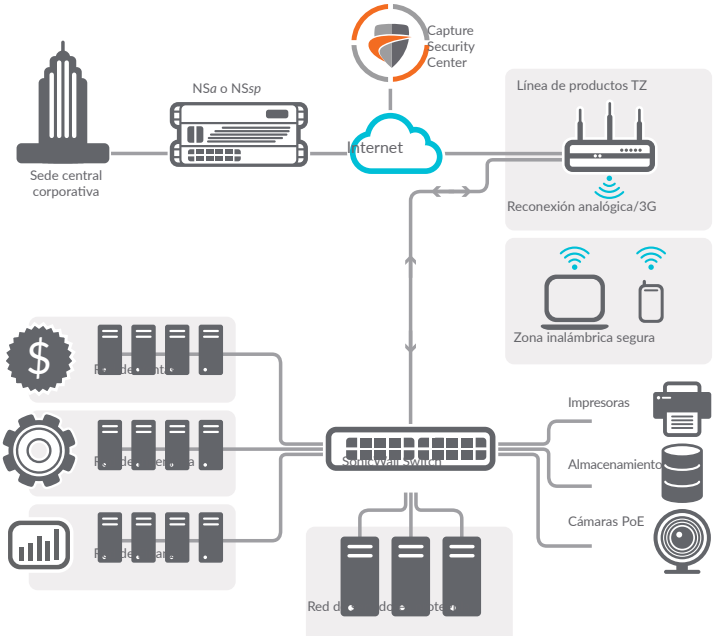
La tecnología SD-WAN de SonicOS es un complemento perfecto para



los firewalls TZ implementados en emplazamientos remotos y sucursales. En lugar de confiar en tecnologías existentes más caras, como MPLS y T1, las organizaciones que utilizan SD-WAN pueden elegir servicios de Internet públicos más económicos sin dejar de disfrutar de un alto nivel de disponibilidad de las aplicaciones, así como de un rendimiento predecible.

Capture Security Center

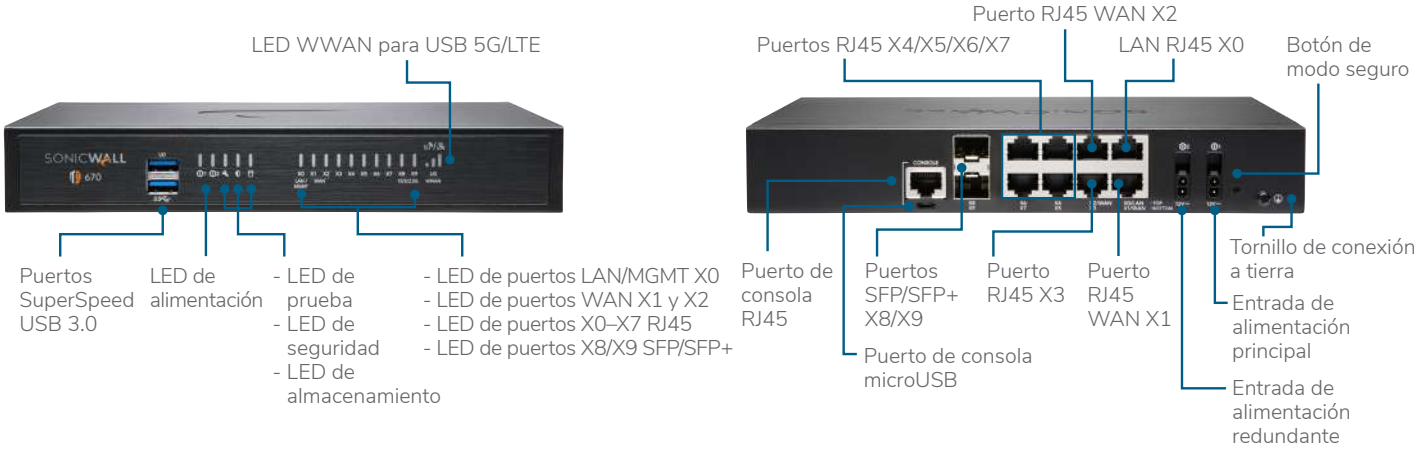
El centro de seguridad basado en la nube Capture Security Center (CSC) de SonicWall actúa como nexo de unión de la red distribuida, en el que se centralizan la implementación, la gestión continuada y los análisis en tiempo real de los firewalls TZ. Una prestación clave del CSC es la Implementación Zero-Touch. La configuración y la implementación de firewalls en múltiples emplazamientos lleva tiempo y requiere la intervención del personal *in situ*. La Implementación Zero-Touch, sin embargo, elimina estos inconvenientes, ya que simplifica y acelera la instalación y el aprovisionamiento de los firewalls de SonicWall de forma remota a través de la nube. De forma similar, el CSC simplifica la gestión continua gracias a que permite gestionar los dispositivos SonicWall de la red a través de la nube y desde una única consola. Para que pueda disfrutar de un completo conocimiento de la situación del entorno de seguridad de la red, SonicWall Analytics le ofrece una visión centralizada de toda la actividad que se desarrolla en la red. De esta forma, las organizaciones adquieren un conocimiento más profundo del uso de las aplicaciones y del rendimiento, al tiempo que frenan la informática en la sombra.



SonicWall Network Security Manager (NSM), que forma parte de CSC, es un gestor de firewalls multiclientes centralizado que le permite administrar de manera centralizada todas las operaciones de firewall sin errores siguiendo flujos de trabajo auditables. Su motor analítico nativo proporciona visibilidad en un solo panel y le permite monitorizar y detectar amenazas unificando y correlacionando registros en todos los firewalls. NSM también le ayuda a cumplir en todo momento con la legislación, ya que proporciona una pista de auditoría completa de cada cambio de configuración e informes detallados. NSM se adapta a las redes de gestión de organizaciones de todos los tamaños con hasta miles de dispositivos de firewall desplegados en muchas ubicaciones.

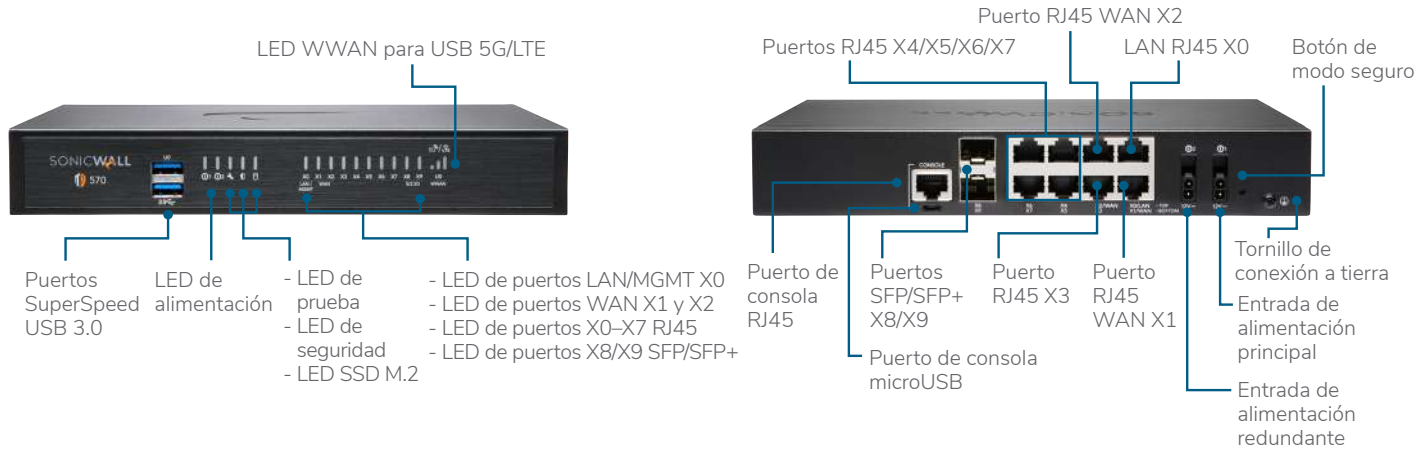
Serie SonicWall TZ670

Concebida para organizaciones de tamaño medio y empresas distribuidas con sitios SD-Branch, la serie TZ670 proporciona una robusta seguridad validada para la industria con la mejor relación precio-rendimiento de su clase.



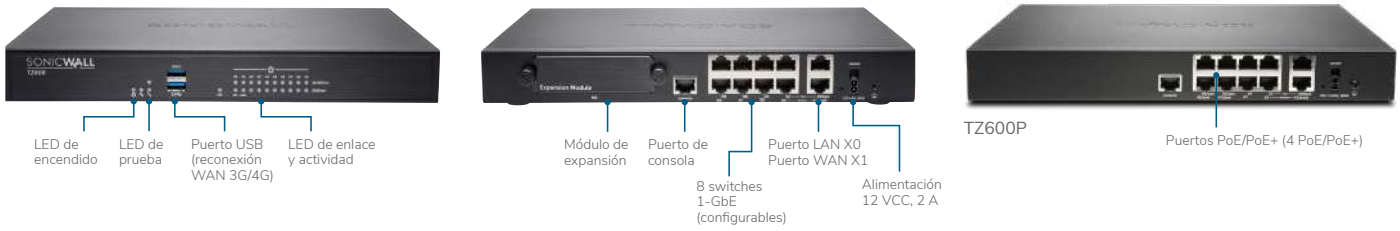
Serie SonicWall TZ570

Concebida para organizaciones pequeñas y medianas y empresas distribuidas con sitios SD-Branch, la serie TZ570 proporciona una robusta seguridad validada para la industria con la mejor relación precio-rendimiento de su clase.



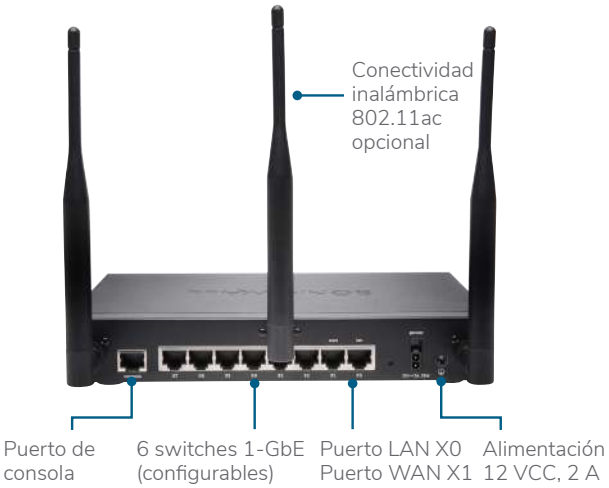
Serie SonicWall TZ600

Para las empresas emergentes, los comercios minoristas y las sucursales que necesitan seguridad, rendimiento y opciones como PoE+ 802.3at con una buena relación calidad-precio, SonicWall TZ600 protege las redes con funciones de clase empresarial y un rendimiento indiscutible.



Serie SonicWall TZ500

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

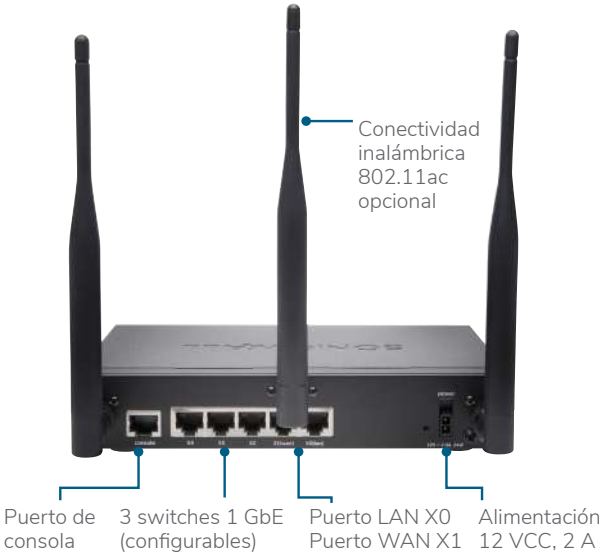


Serie SonicWall TZ400

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

Series SonicWall TZ350/TZ300

Las series TZ300 y TZ350 de SonicWall proporcionan una solución integral que protege las redes frente a ataques avanzados. A diferencia de los productos de consumo, estos firewalls UTM combinan la prevención de intrusiones de alta velocidad, el antimalware y el filtrado de contenidos/URL, además de una amplia compatibilidad de acceso móvil seguro para portátiles, smartphones y tabletas, junto con la tecnología inalámbrica integrada opcional 802.11ac. Además, la serie TZ300 ofrece la opción de 802.3at PoE+ para alimentar dispositivos con PoE.



Series SonicWall SOHO 250/SOHO

Para entornos por cable e inalámbricos de pequeños entornos ofimáticos domésticos, las series SOHO 250 y SOHO proporcionan la misma protección de calidad empresarial que precisan las grandes empresas a un precio mucho más asequible. Añada conectividad inalámbrica 802.11n opcional para proporcionar a empleados, clientes e invitados una conectividad inalámbrica segura.

Servicios habilitados por *partners*

¿Necesita ayuda para planificar, desplegar u optimizar su solución de SonicWall? Los *partners* de servicios avanzados de SonicWall están formados para prestarle servicios profesionales de primera clase. Obtenga más información en www.sonicwall.com/PES.

Visión de conjunto de las prestaciones de SonicOS 7.0

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
- Compatibilidad total con API
- Integración de *switch* de SonicWall
- Escalabilidad SD-WAN
- Asistente de usabilidad de SD-WAN[1]
- Contenedorización de SonicCoreX y SonicOS[1]
- Escalabilidad de conexiones (SPI, DPI, DPI SSL)

Panel mejorado[1]
- Vista mejorada de dispositivos
- Resumen de tráfico y usuarios principales
- Información sobre amenazas
- Centro de notificaciones

Descifrado e inspección TLS/SSL/SSH
- TLS 1.3 con seguridad mejorada[1]
- Inspección profunda de paquetes para TLS/SSL/SSH
- Inclusión/exclusión de objetos, grupos o nombres de host
- Control SSL
- Mejoras para DPI-SSL con CFS
- Controles DPI SSL granulares por zona o norma

Capture Advanced Threat Protection[2]
- Inspección profunda de memoria en tiempo real
- 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 automático y manual
- Actualizaciones de inteligencia de amenazas en tiempo real
- Bloqueo hasta que haya un veredicto
- Capture Client

Prevención de intrusiones[2]
- Análisis basado en definiciones
- Actualizaciones automáticas de las definiciones
- Inspección bidireccional
- Capacidad para reglas de IPS detalladas
- Aplicación de políticas GeoIP
- Filtrado de botnets con lista dinámica
- Coincidencia de expresiones regulares

Antimalware[2]
- Análisis de *malware* basado en flujos
- Gateway antivirus
- Gateway antispyware
- Inspección bidireccional
- Tamaño de archivo ilimitado
- Base de datos de *malware* en la nube

Identificación de aplicaciones[2]
- Control 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
- Exhaustiva base de datos de definiciones de aplicaciones

Visualización y análisis del tráfico
- Actividad de los usuarios
- Aplicaciones/ancho de banda/amenazas
- Análisis basados en la nube

Filtrado de contenido web HTTP/HTTPS[2]
- Filtrado de URL
- Puenteo de proxys
- Bloqueo de palabras clave
- Filtrado basado en políticas (exclusión/inclusión)
- Inserción de encabezado HTTP
- Gestión del ancho de banda según categorías de clasificación CFS
- Modelo de políticas unificadas con control de aplicaciones
- Content Filtering Client

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

Redes
- PortShield
- Estructuras Jumbo
- Descubrimiento de rutas MTU
- Protocolización mejorada
- Enlace troncal VLAN
- Duplicación de puertos (NSa 2650 y superiores)
- QoS de nivel 2
- Seguridad de puertos
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Controlador inalámbrico de SonicWall
- Enrutamiento basado en políticas (ToS/métrica y ECMP)
- NAT
- Servidor DHCP
- Gestión del ancho de banda
- Alta disponibilidad A/P con sincronización de estado
- Equilibrio de carga entrante/saliente
- Alta disponibilidad - Activa/En espera con sincronización de estado
- Puente L2, modo Wire/Virtual Wire, modo TAP, modo NAT
- Enrutamiento asimétrico
- 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, monitorización y compatibilidad
- Compatibilidad con Capture Security Appliance (CSa)
- Capture Threat Assessment (CTA) v2.0
  - Nuevo diseño o plantilla
  - Comparación de media global y sectorial
- Nueva UI/UX, disposición intuitiva de funciones[1]
  - Panel de control
  - Información de dispositivos, aplicación, amenazas
  - Vista de topología
  - Creación y gestión simplificadas de políticas
- Estadísticas de uso de políticas/objetos[1]
  - Usado frente a No usado
  - Activo frente a Inactivo
- Búsqueda global de datos estadísticos
- Asistencia de almacenamiento[1]
- Gestión de almacenamiento externo y externo[1]
- Compatible con tarjetas USB WWAN (5G/LTE/4G/3G)
- Compatible con Network Security Manager (NSM)
- GUI Web
- Interfaz de línea de comandos (CLI)
- Registro y aprovisionamiento *Zero-Touch*
- Elaboración sencilla de informes CSC[1]
- Compatible con la aplicación móvil SonicExpress
- SNMPv2/v3
- Gestión e informes centralizados con Global Management System (GMS) de SonicWall[2]
- Protocolización
- Exportaciones NetFlow/IPFIX
- Backup de configuración basado en la nube
- Plataforma de análisis de seguridad de BlueCoat
- Visualización de aplicaciones y ancho de banda
- Gestión de IPv4 e IPv6
- Pantalla de gestión de CD
- Gestión de switches de las series Dell N y Dell X incluidos switches en cascada

Depuración y diagnóstico
- Supervisión de paquetes mejorada
- Terminal SSH en la interfaz de usuario

Conexión inalámbrica
- Gestión en la Nube de AP SonicWave
- WIDS/WIPS
- Prevención de *access points* no autorizados
- Itinerancia rápida (802.11k/r/v)
- Redes de malla 802.11s
- Selección automática de canales
- Análisis del espectro RF
- Vista de planta
- Vista de topología
- *Band steering* (direccionamiento de banda)
- *Beamforming* (conformación de haces)
- AirTime Fairness (equidad de conexión)
- Bluetooth de baja energía
- MiFi Extender
- Mejoras de RF
- Acceso temporal para usuarios invitados

Modelos inalámbricos integrados
- Conectividad inalámbrica 802.11ac Wave 2 (TZ570W)
- Doble banda (2,4 GHz y 5,0 GHz)
- Normas inalámbricas 802.11 a/b/g/n/ac
- Detección y prevención de intrusiones inalámbricas
- Servicios inalámbricos para usuarios invitados
- Mensajería ligera en puntos de conexión
- Segmentación mediante *access points* virtuales
- Portal cautivo
- ACL para la nube

[1] *Nueva función disponible en SonicOS 7.0*
[2] *Requiere suscripción adicional*

Especificaciones del sistema de la serie SonicWall TZ: SOHO, SOHO 250, TZ300 y TZ350

FIREWALL GENERAL	SERIE SOHO	SERIE SOHO 250	SERIE TZ300	SERIE TZ350
Sistema operativo	SonicOS			
Interfaces	5x1GbE, 1 USB, 1 Consola		5x1GbE, 1 USB, 1 Consola	5x1GbE, 1 USB, 1 Consola
Admite alimentación por Ethernet (PoE)	—	—	TZ300P - 2 puertos (2 PoE o 1 PoE+)	—
Expansión	USB			
Gestión	CLI, SSH, IU Web, Centro de seguridad de Capture, GMS, APIs REST			
Usuarios con inicio de sesión único (SSO)	250	350	500	500
Interfaces VLAN	25			
Access points admitidos (máximo)	2	4	8	8
RENDIMIENTO DE FIREWALL/VPN	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Rendimiento de inspección del firewall[1]	300 Mbps	600 Mbps	750 Mbps	1,0 Gbps
Rendimiento de prevención de amenazas[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
Rendimiento de inspección de aplicaciones[2]	—	275 Mbps	375 Mbps	600 Mbps
Rendimiento de IPS[2]	200 Mbps	250 Mbps	300 Mbps	400 Mbps
Rendimiento de inspección de antimalware[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL)[2]	30 Mbps	50 Mbps	60 Mbps	65 Mbps
Rendimiento de IPSec VPN[3]	150 Mbps	200 Mbps	300 Mbps	430 Mbps
Conexiones por segundo	1.800	3.000	5.000	6.000
Número máximo de conexiones (SPI)	10.000	50.000	100.000	100.000
Número máximo de conexiones (DPI)	10.000	50.000	90.000	90.000
Número máximo de conexiones (DPI SSL)	250	25.000	25.000	25.000
VPN	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Túneles VPN entre emplazamientos	10	10	10	15
Clientes VPN IPSec (máximo)	1 (5)	1 (5)	1 (10)	2 (10)
Licencias de VPN SSL (máximo)	1 (10)	1 (25)	1 (50)	1 (75)
Virtual Assist incluido (máximo)	—	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, 14v			
VPN basada en enrutamiento	RIP, OSPF, BGP[4]			
Prestaciones VPN	Dead Peer Detection, DHCP a través de VPN, IPSec NAT Traversal, Gateway VPN redundante, VPN basada en enrutamiento			
Plataformas de cliente VPN globales admitidas	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 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 (Embedded)			
SERVICIOS DE SEGURIDAD	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
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 exhaustivo basado en tipos de archivo como ActiveX, Java, cookies para la privacidad, listas de permitidos/denegados			
Servicio antispam integral	Compatible			
Visualización de aplicaciones	No	Sí	Sí	Sí
Control de aplicaciones	Sí	Sí	Sí	Sí
Capture Advanced Threat Protection	No	Sí	Sí	Sí
REDES	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
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)			

Especificaciones del sistema de la serie SonicWall TZ: SOHO, SOHO 250, TZ300 y TZ350 (continuación)

REDES, CONTINUACIÓN	SERIE SOHO	SERIE SOHO 250	SERIE TZ300	SERIE TZ350
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, Common Access Card (CAC)	
Base de datos de usuarios local	150			
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[5]	FIPS 140-2 (con Suite B) nivel 2, UC APL, VPNC, IPv6 (fase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (firewall e IPS)			
Tarjeta Common Access Card (CAC)	Compatible			
Alta disponibilidad	No		Activa/En espera	
HARDWARE	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
Factor de forma	Sobremesa			
Fuente de alimentación	24 W (externa)		24 W (externa) 65 W (externa, solo TZ300P)	24 W (externa)
Consumo máximo de energía (W)	6,4/11,3	6,9/11,3	6,9/12,0	6,9/12,0
Potencia de entrada	De 100 a 240 V CA, 50-60 Hz, 1 A			
Disipación de calor total	21,8/38,7 BTU	23,5/38,7 BTU	23,5/40,9 BTU	23,5/40,9 BTU
Dimensiones	3,6 x 14,1 x 19 cm 1,42 x 5,55 x 7,48 pulgadas		3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 pulgadas	3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 pulgadas
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
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
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
MTBF (en años)	58,9/56,1 (inalámbrico)	56,1	56,1	56,1
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 SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
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, ANATEL		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, ANATEL	
Cumplimiento de las principales 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, WEEE, 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, WEEE, REACH	
CONEXIÓN INALÁMBRICA INTEGRADA	**SERIE SOHO**	**SERIE SOHO 250**	**SERIE TZ300**	**SERIE TZ350**
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[6]	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	

Especificaciones del sistema de la serie SonicWall TZ: SOHO, SOHO 250, TZ300 y TZ350 (continuación)

CONEXIÓN INALÁMBRICA INTEGRADA	SERIE SOHO	SERIE SOHO 250	SERIE TZ300	SERIE TZ350
Canales operativos	802.11a: EE. UU. y Canadá 12, Europa 11, Japón 4, Singapur 4, Taiwán 4; 802.11b/g: EE. UU. y Canadá 1-11, Europa 1-13, Japón 1-14 (solo 14-802.11b); 802.11n (2,4 GHz): EE. UU. y Canadá 1-11, Europa 1-13, Japón 1-13; 802.11n (5 GHz): EE. UU. y Canadá 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64;		802.11a: EE. UU. y Canadá 12, Europa 11, Japón 4, Singapur 4, Taiwán 4; 802.11b/g: EE. UU. y Canadá 1-11, Europa 1-13, Japón 1-14 (solo 14-802.11b); 802.11n (2,4 GHz): EE. UU. y Canadá 1-11, Europa 1-13, Japón 1-13; 802.11n (5 GHz): EE. UU. y Canadá 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64; 802.11ac: EE. UU. y Canadá 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64	
Potencia de salida de transmisión	Se basa en el ámbito normativo especificado por el administrador del sistema			
Control de la potencia de transmisión	Compatible			
Velocidades de transferencia admitidas	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11b: 1, 2, 5,5, 11 Mbps por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 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 Mbps por canal		802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11b: 1, 2, 5,5, 11 Mbps por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 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 Mbps 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 Mbps 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 de Prevención de amenazas/GatewayAV/Anti-Spyware/IPS medido con el uso de 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. Rendimiento de Prevención de amenazas medido con Gateway AV, Anti-Spyware, IPS and Application Control activado.*

[3] *Medición del rendimiento de VPN utilizando 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 TZ350, TZ400, TZ500 y TZ600.*

[5] *Pendiente de aprobación FIPS e ICSA en SOHO 250 y TZ350*

[6] *Todos los modelos TZ inalámbricos integrados pueden soportar bandas de 2,4GHz o 5GHz. Para soporte de banda dual, utilice los productos de* access points *inalámbricos de SonicWall*

Especificaciones del sistema de la serie SonicWall TZ: TZ400, TZ500 y TZ600

FIREWALL GENERAL	SERIE TZ400	SERIE TZ500	SERIE TZ600
Sistema operativo		SonicOS	
Interfaces	7x1GbE, 1 USB, 1 Consola	8x1GbE, 2 USB, 1 Consola	10x1GbE, 2 USB, 1 Consola, 1 ranura de expansión
Admite alimentación por Ethernet (PoE)	—	—	TZ600P - 4 puertos (4 PoE o 4 PoE+)
Expansión	USB	2 USB	Ranura de expansión (posterior),* 2 USB
Gestión	CLI, SSH, IU Web, Centro de seguridad de Capture, GMS, APIs REST		
Usuarios con inicio de sesión único (SSO)	500	500	500
Interfaces VLAN	50	50	50
Access points admitidos (máximo)	16	16	24
RENDIMIENTO DE FIREWALL/VPN	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
Rendimiento de inspección del firewall[1]	1,3 Gbps	1,4 Gbps	1,9 Gbps
Rendimiento de prevención de amenazas[2]	600 Mbps	700 Mbps	800 Mbps
Rendimiento de inspección de aplicaciones[2]	1,2 Gbps	1,3 Gbps	1,8 Gbps
Rendimiento de IPS[2]	900 Mbps	1,0 Gbps	1,2 Gbps
Rendimiento de inspección de antimalware[2]	600 Mbps	700 Mbps	800 Mbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL)[2]	180 Mbps	225 Mbps	300 Mbps
Rendimiento de IPSec VPN[3]	900 Mbps	1,0 Gbps	1,1 Gbps
Conexiones por segundo	6.000	8.000	12.000
Número máximo de conexiones (SPI)	150.000	150.000	150.000
Número máximo de conexiones (DPI)	125.000	125.000	125.000
Número máximo de conexiones (DPI SSL)	25.000	25.000	25.000
VPN	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
Túneles VPN entre emplazamientos	20	25	50
Clientes VPN IPSec (máximo)	2 (25)	2 (25)	2 (25)
Licencias de VPN SSL (máximo)	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)
Cifrado/autenticación	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, criptografía Suite B		
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14v		
VPN basada en enrutamiento	RIP, OSPF, BGP		
Prestaciones VPN	Dead Peer Detection, DHCP a través de VPN, IPSec NAT Traversal, Gateway VPN redundante, VPN basada en enrutamiento		
Plataformas de cliente VPN globales admitidas	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 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 (Embedded)		
SERVICIOS DE SEGURIDAD	**SERIE TZ400**	**SERIE TZ500**	**SERIE 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 exhaustivo basado en tipos de archivo como ActiveX, Java, cookies para la privacidad, listas de permitidos/denegados		
Servicio antispam integral	Compatible		
Visualización de aplicaciones	Sí	Sí	Sí
Control de aplicaciones	Sí	Sí	Sí
Capture Advanced Threat Protection	Sí	Sí	Sí
REDES	**SERIE TZ400**	**SERIE TZ500**	**SERIE 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)		

Especificaciones del sistema de la serie SonicWall TZ: TZ400, TZ500 y TZ600 (continuación)

REDES	SERIE TZ400	SERIE TZ500	SERIE TZ600
Autenticación	LDAP (múltiples dominios), XAUTH/RADIUS, SSO, Novell, base de datos de usuarios interna, Terminal Services, Citrix, Common Access Card (CAC)		
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, Common Criteria NDPP (firewall e IPS)		
Tarjeta Common Access Card (CAC)	Compatible		
Alta disponibilidad	Activa/En espera	Activa/En espera con sincronización de estado	
HARDWARE	**SERIE TZ400**	**SERIE TZ500**	**SERIE TZ600**
Factor de forma	Sobremesa		
Fuente de alimentación	24 W (externa)	36W (externa)	60W (externa) 180W (externa) (TZ600P únicamente)
Consumo máximo de energía (W)	9,2/13,8	13,4/17,7	16,1
Potencia de entrada	100-240 VCA, 50-60 Hz, 1 A		
Disipación de calor total	31,3/47,1 BTU	45,9/60,5 BTU	55,1 BTU
Dimensiones	3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 pulgadas	3,5 x 15 x 22,5 cm 1,38 x 5,91 x 8,86 pulgadas	3,5 x 18 x 28 cm 1,38 x 7,09 x 11,02 pulgadas
Peso	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	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	1,37 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 (en años)	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 TZ400**	**SERIE TZ500**	**SERIE TZ600**
Cumplimiento de las principales normativas (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, ANATEL	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, ANATEL	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
Cumplimiento de las principales 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, WEEE, 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, WEEE, REACH	—

Especificaciones del sistema de la serie SonicWall TZ: TZ400, TZ500 y TZ600 (continuación)

CONEXIÓN INALÁMBRICA INTEGRADA	SERIE TZ400	SERIE TZ500	SERIE TZ600
Estándares	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: 5,180-5,825 GHz; 802.11b/g: 2,412-2,472 GHz; 802.11n: 2,412-2,472 GHz, 5,180-5,825 GHz; 802.11ac: 5,180-5,825 GHz		—
Canales operativos	802.11a: EE. UU. y Canadá 12, Europa 11, Japón 4, Singapur 4, Taiwán 4; 802.11b/g: EE. UU. y Canadá 1-11, Europa 1-13, Japón (solo 14-802.11b); 802.11n (2,4 GHz): EE. UU. y Canadá 1-11, Europa 1-13, Japón 1-13; 802.11n (5 GHz): EE. UU. y Canadá 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64; 802.11ac: EE. UU. y Canadá 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64		—
Potencia de salida de transmisión	Se basa en el ámbito normativo especificado por el administrador del sistema		—
Control de la potencia de transmisión	Compatible		—
Velocidades de transferencia admitidas	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11b: 1, 2, 5,5, 11 Mbps por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 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 Mbps 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 Mbps 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) 802.11ac: Multiplexación por división de frecuencias ortogonales (OFDM)		—

Especificaciones del sistema de la serie SonicWall TZ: TZ500 y TZ670

FIREWALL GENERAL	SERIE TZ570	SERIE TZ670
Sistema operativo	SonicOS 7.0	
Interfaces	8x1GbE, 2x5GbE, 2 USB 3.0, 1 Consola	8x1GbE, 2x10GbE, 2 USB 3.0, 1 Consola
Admite alimentación por Ethernet (PoE)	TZ570P (5 PoE o 3PoE+)	—
Expansión	Ranura de expansión de almacenamiento (hasta 256 GB)	Ranura de expansión de almacenamiento (hasta 256 GB) (32 GB incluidas)
Gestión	Network Security Manager, CLI, SSH, IU Web, GMS, APIs REST	
Usuarios con inicio de sesión único (SSO)	2.500	2.500
Interfaces VLAN	256	256
Access points admitidos (máximo)	32	32
RENDIMIENTO DE FIREWALL/VPN	**SERIE TZ570**	**SERIE TZ670**
Rendimiento de inspección del firewall[1]	4,00 Gbps	5,00 Gbps
Rendimiento de prevención de amenazas[2]	2,00 Gbps	2,50 Gbps
Rendimiento de inspección de aplicaciones[2]	2,5 Gbps	3,0 Gbps
Rendimiento de IPS[2]	2,5 Gbps	3,0 Gbps
Rendimiento de inspección de antimalware[2]	2,00 Gbps	2,50 Gbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL)[2]	750 Mbps	800 Mbps
Rendimiento de IPSec VPN[3]	1,80 Gbps	2,10 Gbps
Conexiones por segundo	16.000	25.000
Número máximo de conexiones (SPI)	1.250.000	1.500.000
Número máximo de conexiones (DPI)	400.000	500.000
Número máximo de conexiones (DPI SSL)	30.000	30.000
VPN	**SERIE TZ570**	**SERIE TZ670**
Túneles VPN entre emplazamientos	200	250
Clientes VPN IPSec (máximo)	10 (500)	10 (500)
Licencias de VPN SSL (máximo)	2 (200)	2 (250)
Cifrado/autenticación	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, criptografía Suite B	
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14v	
VPN basada en enrutamiento	RIP, OSPF, BGP	
Prestaciones VPN	Dead Peer Detection, DHCP a través de VPN, IPSec NAT Traversal, gateway VPN redundante, VPN basada en enrutamiento	
Plataformas de cliente VPN globales admitidas	Microsoft® Windows 10	
NetExtender	Microsoft® Windows 10, Linux	
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome OS, Windows 10	
SERVICIOS DE SEGURIDAD	**SERIE TZ570**	**SERIE TZ670**
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	
Servicio antispam integral	Sí	
Visualización de aplicaciones	Sí	
Control de aplicaciones	Sí	
Capture Advanced Threat Protection	Sí	
Seguridad DNS	Sí	

Especificaciones del sistema de la serie SonicWall TZ: TZ500 y TZ670 (continuación)

REDES	SERIE TZ570	SERIE TZ670
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	BGP4, 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 Terminal Services, Citrix, Common Access Card (CAC)	
Base de datos de usuarios local	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 a802.3	
Certificaciones pendientes	FIPS 140-2 (con Suite B) nivel 2, IPv6 (fase 2), ICSA Network Firewall, ICSA Antivirus, Common Criteria NDPP (firewall e IPS)	

HARDWARE	SERIE TZ570	SERIE TZ670
Factor de forma	Sobremesa[5]	
Fuente de alimentación	60W (externa) 180W (externa) (TZ570P únicamente)	60W (externa)
Consumo máximo de energía (W)	13,1	13,1
Tensión de entrada y frecuencia	100-240 VCA, 50-60 Hz,	100-240 VCA, 50-60 Hz,
Disipación de calor total	45,9/60,5 BTU	55,1 BTU
Dimensiones	3,5 x 15 x 22,5 (cm) 1,38 x 5,91 x 8,85 pulgadas	3,5 x 15 x 22,5 (cm) 1,38 x 5,91 x 8,85 pulgadas
Peso	0,97 kg/2,14 libras	0,97 kg/2,14 libras
Peso WEEE	1,42 kg/3,13 libras	1,42 kg/3,13 libras
Peso de envío	1,93 kg/4,25 libras	1,93 kg/4,25 libras
MTBF a 25 °C en años	26,1	43,9
Entorno (Operativo/Almacenamiento)	0-40 °C (32-105 °F)/-40 a 70 °C (-40 a 158 °F)	
Humedad	5-95 %, sin condensación	

NORMATIVAS	SERIE TZ570	SERIE TZ670
Cumplimiento de las principales normativas (modelos por cable: TZ670, TZ570)	FCC Clase B, FCC, ICES Clase B, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase B, UL/cUL, TUV/GS, CB, notificación de DGN para México por UL, WEEE, REACH, BSMI, KCC/ MSIP, ANATEL	FCC Clase B, FCC, ICES Clase B, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase B, UL/cUL, TUV/GS, CB, notificación de DGN para México por UL, WEEE, REACH, BSMI, KCC/ MSIP, ANATEL
Cumplimiento de las principales normativas (modelos por cable: TZ570W)	FCC Clase B, FCC P15C, FCC P15E, ICES Clase B, ISED/IC, CE (RED, RoHS), C-Tick, VCCI Clase B, Japan Wireless, UL/cUL, TUV/GS, CB, notificación de DGN para México por UL, WEEE, REACH, BSMI, NCC (TW) KCC/ MSIP, SRRC, ANATEL	—
Cumplimiento de las principales normativas (modelos PoE: TZ570P)	FCC Clase A, ICES Clase A, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase A, UL/cUL, TUV/GS, CB, notificación de DGN para México por UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	—

Especificaciones del sistema de la serie SonicWall TZ: TZ500 y TZ670 (continuación)

CONEXIÓN INALÁMBRICA INTEGRADA	SERIE TZ570	SERIE TZ670
Estándares	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: 5,180-5,825 GHz; 802.11b/g: 2,412-2,472 GHz; 802.11n: 2,412-2,472 GHz, 5,180-5,825 GHz; 802.11ac: 5,180-5,825 GHz	—
Canales operativos	802.11a: EE. UU. y Canadá 12, Europa 11, Japón 4, Singapur 4, Taiwán 4; 802.11b/g: EE. UU. y Canadá 1-11, Europa 1-13, Japón (solo 14-802.11b); 802.11n (2,4 GHz): EE. UU. y Canadá 1-11, Europa 1-13, Japón 1-13; 802.11n (5 GHz): EE. UU. y Canadá 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64; 802.11ac: EE. UU. y Canadá 36-48/149-165, Europa 36-48, Japón 36-48, España 36-48/52-64	—
Potencia de salida de transmisión	Se basa en el ámbito normativo especificado por el administrador del sistema	—
Control de la potencia de transmisión	Compatible	—
Velocidades de transferencia admitidas	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11b: 1, 2, 5,5, 11 Mbps por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 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 Mbps 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 Mbps 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) 802.11ac: Multiplexación por división de frecuencias ortogonales (OFDM)	—

[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 de Prevención de amenazas/GatewayAV/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. Rendimiento de Prevención de amenazas medido con Gateway AV, Anti-Spyware, IPS and Application Control activado.*
[3] *Medición del rendimiento de VPN utilizando 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] *Hay disponible un kit de montaje en bastidor aparte.*
[5] *Todos los modelos TZ inalámbricos integrados pueden soportar bandas de 2,4GHz o 5GHz. Para soporte de banda dual, utilice los productos de access points inalámbricos de SonicWall*

Información para pedidos de la serie SonicWall TZ

Producto	SKU
SOHO 250 con 1 año de TotalSecure Advanced Edition	02-SSC-1815
SOHO 250 Wireless-AC con 1 año de TotalSecure Advanced Edition	02-SSC-1824
TZ300 con 1 año de TotalSecure Advanced Edition	01-SSC-1702
TZ300 Wireless-AC con 1 año de TotalSecure Advanced Edition	01-SSC-1703
TZ300P con 1 año de TotalSecure Advanced Edition	02-SSC-0602
TZ350 con 1 año de TotalSecure Advanced Edition	02-SSC-1843
TZ350 Wireless-AC con 1 año de TotalSecure Advanced Edition	02-SSC-1851
TZ400 con 1 año de TotalSecure Advanced Edition	01-SSC-1705
TZ400 Wireless-AC con 1 año de TotalSecure Advanced Edition	01-SSC-1706
TZ500 con 1 año de TotalSecure Advanced Edition	01-SSC-1708
TZ500 Wireless-AC con 1 año de TotalSecure Advanced Edition	01-SSC-1709
TZ570 con 1 año de TotalSecure Essential Edition	02-SSC-5651
TZ570W con 1 año de TotalSecure Essential Edition	02-SSC-5649
TZ570P con 1 año de TotalSecure Essential Edition	02-SSC-5653
TZ600 con 1 año de TotalSecure Advanced Edition	01-SSC-1711
TZ600P con 1 año de TotalSecure Advanced Edition	02-SSC-0600
TZ670 con 1 año de TotalSecure Essential Edition	02-SSC-5640
Opciones de alta disponibilidad (todas las unidades deben ser del mismo modelo)	
TZ500 con alta disponibilidad	01-SSC-0439
TZ570 con alta disponibilidad	02-SSC-5694
TZ570P con alta disponibilidad	02-SSC-5655
TZ600 con alta disponibilidad	01-SSC-0220
TZ670 con alta disponibilidad	02-SSC-5654

Servicios	SKU
Para la serie SonicWall SOHO 250	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas y soporte 24x7 (1 año)	02-SSC-1726
Capture Advanced Threat Protection para SOHO 250 (1 año)	02-SSC-1732
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	02-SSC-1750
Servicio de filtrado de contenido (1 año)	02-SSC-1744
Servicio antispam integral (1 año)	02-SSC-1823
Soporte 24x7 (1 año)	02-SSC-1720
Para la serie SonicWall TZ300	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas y soporte 24x7 (1 año)	01-SSC-1430
Capture Advanced Threat Protection para TZ300 (1 año)	01-SSC-1435
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	01-SSC-0602
Servicio de filtrado de contenido (1 año)	01-SSC-0608
Servicio antispam integral (1 año)	01-SSC-0632
Soporte 24x7 (1 año)	01-SSC-0620
Para la serie SonicWall TZ350	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas y soporte 24x7 (1 año)	02-SSC-1773
Capture Advanced Threat Protection para TZ350 (1 año)	02-SSC-1779
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	02-SSC-1797
Servicio de filtrado de contenido (1 año)	02-SSC-1791
Servicio antispam integral (1 año)	02-SSC-1809
Soporte 24x7 (1 año)	02-SSC-1767

Información para pedidos de la serie SonicWall TZ

Para la serie SonicWall TZ400	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas y soporte 24x7 (1 año)	01-SSC-1440
Capture Advanced Threat Protection para TZ400 (1 año)	01-SSC-1445
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	01-SSC-0534
Servicio de filtrado de contenido (1 año)	01-SSC-0540
Servicio antispam integral (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 y soporte 24x7 (1 año)	01-SSC-1450
Capture Advanced Threat Protection para TZ500 (1 año)	01-SSC-1455
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	01-SSC-0458
Servicio de filtrado de contenido (1 año)	01-SSC-0464
Servicio antispam integral (1 año)	01-SSC-0482
Soporte 24x7 (1 año)	01-SSC-0476
Para la serie SonicWall TZ600	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas y soporte 24x7 (1 año)	01-SSC-1460
Capture Advanced Threat Protection para TZ600 (1 año)	01-SSC-1465
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	01-SSC-0228
Servicio de filtrado de contenido (1 año)	01-SSC-0234
Servicio antispam integral (1 año)	01-SSC-0252
Soporte 24x7 (1 año)	01-SSC-0246
Para la serie SonicWall TZ670	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas, filtrado de contenido, antispam y soporte 24x7 (1 año)	02-SSC-5053
Capture Advanced Threat Protection para TZ670 (1 año)	02-SSC-5035
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	02-SSC-5059
Servicio de filtrado de contenido (1 año)	02-SSC-5047
Servicio antispam integral (1 año)	02-SSC-5041
Soporte 24x7 (1 año)	02-SSC-5029
Para la serie SonicWall TZ570 (TZ570)	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas, filtrado de contenido, antispam y soporte 24x7 (1 año)	02-SSC-5137
Capture Advanced Threat Protection para TZ570 (1 año)	02-SSC-5083
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	02-SSC-5155
Servicio de filtrado de contenido (1 año)	02-SSC-5119
Servicio antispam integral (1 año)	02-SSC-5101
Soporte 24x7 (1 año)	02-SSC-5065
Para la serie SonicWall TZ570 (TZ570W)	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas, filtrado de contenido, antispam y soporte 24x7 (1 año)	02-SSC-5149
Capture Advanced Threat Protection para TZ570W (1 año)	02-SSC-5095
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	02-SSC-5167
Servicio de filtrado de contenido (1 año)	02-SSC-5131
Servicio antispam integral (1 año)	02-SSC-5113
Soporte 24x7 (1 año)	02-SSC-5077
Para la serie SonicWall TZ570 (TZ570P)	
Advanced Gateway Security Suite: Capture ATP, prevención de amenazas, filtrado de contenido, antispam y soporte 24x7 (1 año)	02-SSC-5143
Capture Advanced Threat Protection para TZ570P (1 año)	02-SSC-5089
Gateway Anti-Virus, prevención de intrusiones y control de aplicaciones (1 año)	02-SSC-5161
Servicio de filtrado de contenido (1 año)	02-SSC-5125
Servicio antispam integral (1 año)	02-SSC-5107
Soporte 24x7 (1 año)	02-SSC-5071

Accesorios	SKU
Series TZ670/570	
Fuente de alimentación para series SonicWall TZ670/570, FRU	02-SSC-3078
Kit de montaje en bastidor para series SonicWall TZ670/570	02-SSC-3112
Módulo de almacenamiento de 32 GB SonicWall para las series TZ670/570	02-SSC-3114
Módulo de almacenamiento de 64 GB SonicWall para las series TZ670/570	02-SSC-3115
Módulo de almacenamiento de 128 GB SonicWall para las series TZ670/570	02-SSC-3116
Módulo de almacenamiento de 256 GB SonicWall para las series TZ670/570	02-SSC-3117
Cable de consola microUSB SonicWall para las series TZ670/570	02-SSC-5173
Series TZ600/500/400/350/300, SOHO 250	
Kit de montaje en bastidor para SonicWall TZ600	01-SSC-0225
Fuente de alimentación para las serie SonicWall TZ600, FRU	01-SSC-0280
Kit de montaje en bastidor para la serie SonicWall TZ500	01-SSC-0438
Fuente de alimentación para la serie SonicWall TZ500, FRU	01-SSC-0437
Kit de montaje en bastidor para la serie SonicWall TZ400	01-SSC-0525
Kit de montaje en bastidor para las series SonicWall TZ350, TZ300	01-SSC-0742
Fuente de alimentación para las series SonicWall TZ400, TZ350, TZ300, SOHO 250, SOHO, FRU	01-SSC-0709
Fuente de alimentación PoE para SonicWall TZ300, FRU	02-SSC-0613
Módulos SonicWall SFP/SFP+	
Módulo de fibra de corto alcance 10GB-SR SFP+ multimodo sin cable	01-SSC-9785
Módulo de fibra de largo alcance 10GB-LR SFP+ de modo único sin cable	01-SSC-9786
Cable Twinax 10GB SFP+ de cobre de 1 m	01-SSC-9787
Cable Twinax 10GB SFP+ de cobre de 3 m	01-SSC-9788
Módulo de fibra de corto recorrido 1GB-SX SFP+ multimodo sin cable	01-SSC-9789
Módulo de fibra de largo recorrido 1GB-LX SFP+ de modo único sin cable	01-SSC-9790
Módulo de cobre 1GB-RJ45 SFP sin cable	01-SSC-9791
Transceptor de cobre SFP+ 10GBASE-T de sonicwall con módulo RJ45	02-SSC-1874

Números de modelo oficiales:

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

Acerca de SonicWall

SonicWall ofrece Ciberseguridad Ilimitada para la época de la informática hiperdistribuida y una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia e insegura. Gracias al conocimiento de lo desconocido, así como al hecho de proporcionar visibilidad en tiempo real y de facilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Para obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
(Estados Unidos)
Encontrará más información en nuestro sitio web.
www.sonicwall.com

Datasheet-TZSeries-US-KJ-2126