SONICWALL

Gartner peerinsights customers' choice 2018

Serie SonicWall TZ

Plataforma integrada de prevención de amenazas y SD-WAN para organizaciones pequeñas/medianas 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. Al combinar funciones de prevención de amenazas de alta velocidad, tecnología de redes de área amplia definidas por software (SD-WAN), una amplia variedad de prestaciones de redes y de conectividad inlámbrica, una implementación simplificada y gestión centralizada, la serie TZ proporciona una solución de seguridad unificada por 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. SonicOS incluye 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 y el soporte para el estándar IEEE 802.11ac, así como la posibilidad de añadir nuestros puntos de acceso 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 puntos de acceso inalámbricos de alta velocidad y otros dispositivos con tecnología de Alimentación por Ethernet (PoE), como cámaras IP, teléfonos e impresoras, los firewalls TZ300P y TZ600P ofrecen alimentación PoE/PoE+.

Las empresas minoristas distribuidas y los entornos de campus pueden utilizar las numerosas herramientas de SonicOS y obtener ventajas todavía mayores. Las sucursales pueden intercambiar información con la oficina central de forma segura utilizando redes privadas virtuales (VPN). La creación de LANs 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 constantes de las aplicaciones. La implementación sin necesidad de intervención, 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 en pruebas independientes y distinguida 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) para su análisis. Además, la tecnología pendiente de patente de Inspección de memoria profunda en tiempo rea (RTDMI™) aumenta la eficacia de Capture ATP. El motor RTDMI detecta y bloquea el malware y las amenazas de día cero inspeccionando directamente 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 Inspección profunda de paquetes sin reensamblado (RFDPI) examina cada byte de cada paquete, inspeccionando el tráfico entrante y saliente directamente en el firewall. Al utilizar Capture ATP con

Ventajas:

Solución de seguridad flexible e integrada

- Secure SD-WAN
- Potente sistema operativo SonicOS
- Conectividad inalámbrica 802.11ac de alta velocidad
- Alimentación por Ethernet (PoE/ PoE+)
- Segmentación de la red con VLANs

Prevención de amenazas y rendimiento superiores

- Tecnología de Inspección profunda de memoria en tiempo real pendiente de patente
- Tecnología patentada de inspección profunda de paquetes sin reensamblado
- Prevención de amenazas integrada y basada en la nube
- Descifrado e inspección TLS/SSL
- Efectividad de la seguridad validada por la industria
- Equipo dedicado de investigación de amenazas Capture Labs
- Seguridad de puntos terminales con Capture Client

Funciones sencillas de implementación, configuración y gestión continua

- Implementación sin necesidad de intervención
- Gestión centralizada, basada en la nube y local
- Línea de firewalls escalables
- Coste total de propiedad reducido

la tecnología RTDMI en la plataforma SonicWall Capture Cloud junto con 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 pasarela. 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 fiables.

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 y el protocolo. El firewall examina cada paquete de forma exhaustiva en busca de incumplimientos de protocolo, amenazas, ataques de día cero, intrusiones e incluso criterios definidos. 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 en base a requisitos legales y/o corporativos específicos.

Funciones sencillas de implementación, configuración y gestión continua

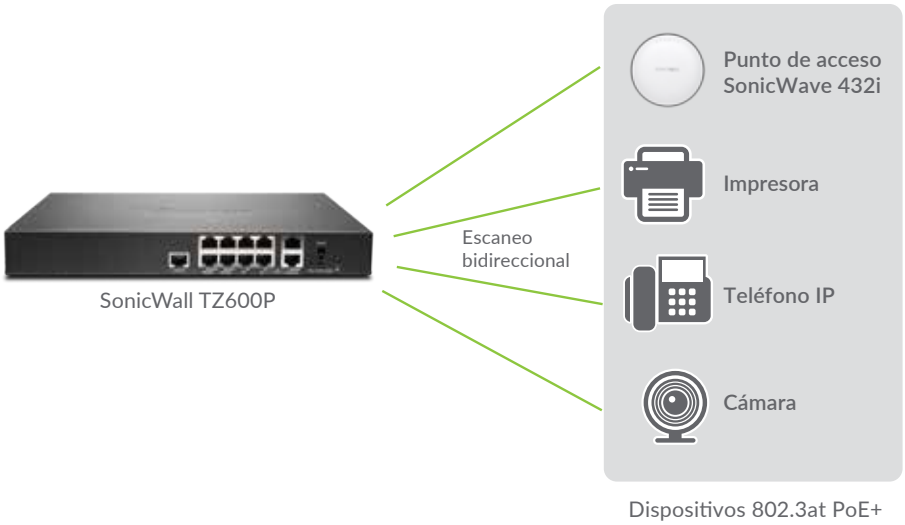
SonicWall simplifica la configuración y la gestión de los firewalls de la serie TZ y los puntos de acceso SonicWave 802.11ac Wave 2 independientemente de dónde se implementen. La gestión, los informes, las licencias y los análisis se centralizan en nuestro Capture Security Center basado en la nube, que 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 sin necesidad de intervención. 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 operacionaliza 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.

Partner Enabled Services

¿Necesita ayuda para planificar, implementar u optimizar su solución SonicWall? Los Partners de servicios avanzados de SonicWall están cualificados para proporcionarle servicios profesionales de clase mundial. Si desea obtener más información, visite www.sonicwall.com/PES.

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



Dispositivos 802.3at PoE+

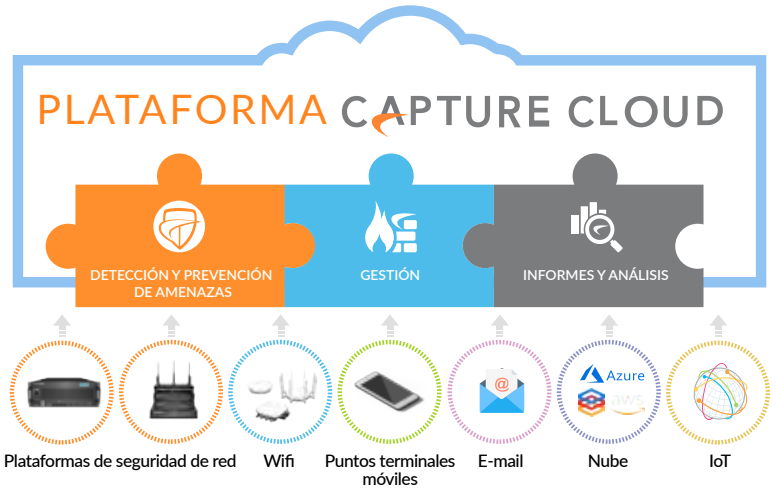
Seguridad integrada y alimentación para sus dispositivos con tecnología PoE

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 y TZ600P integran tecnología IEEE 802.3at para alimentar los dispositivos PoE y PoE+, como puntos de acceso inalámbricos, cámaras, teléfonos IP, etc. El firewall escanea todo el tráfico procedente de y dirigido hacia cada dispositivo utilizando tecnología de inspección profunda de paquetes y a continuación elimina las amenazas dañinas, como el malware y las intrusiones, incluso a través de 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, incluidos nuestro galardonado servicio de sandboxing de red multimotor, Capture Advanced Threat Protection, así como más de 1 millón de sensores de SonicWall situados en todo el mundo.

Si el sistema detecta que los datos que acceden a la red contienen código malicioso desconocido hasta el momento, el equipo de investigación de amenazas interno y dedicado de SonicWall Capture Labs elabora 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.

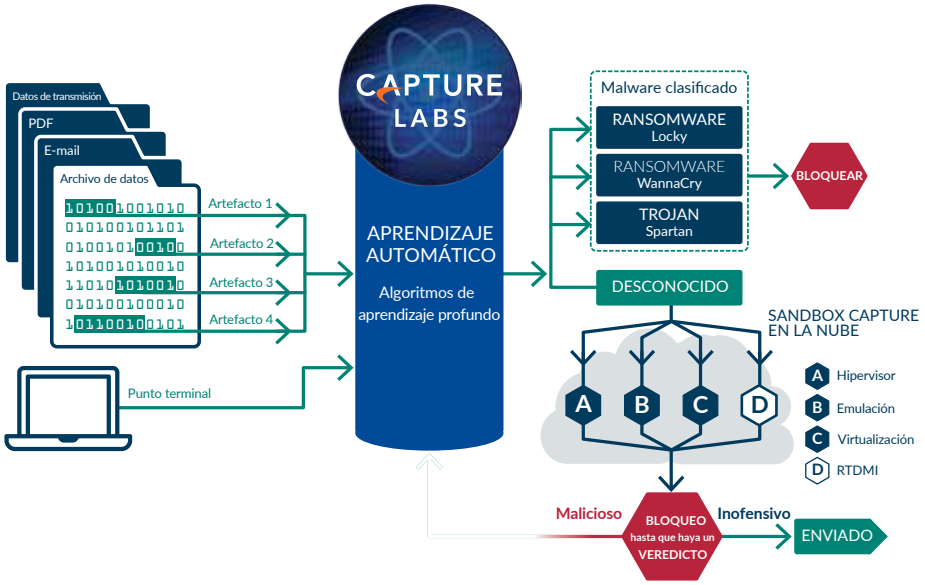


Protección contra amenazas avanzadas

La prevención de brechas en tiempo real automatizada de SonicWall se basa en el servicio Capture Advanced Threat Protection, un sandbox multimotor basado en la nube que amplía la protección del firewall contra las amenazas para detectar y prevenir las amenazas de día cero. Los archivos sospechosos se envían a la nube, donde se analizan utilizando algoritmos de aprendizaje profundo, con la opción de retenerlos en la pasarela hasta que se emita un veredicto. La plataforma de sandbox multimotor, que incluye Inspección profunda de memoria en tiempo real, sandboxing virtualizado, emulación de sistema completo y tecnología de análisis de nivel de hipervisor, ejecuta el código sospechoso y analiza su comportamiento. Cuando se detecta un archivo malicioso, inmediatamente se bloquea y se crea un hash dentro de Capture ATP. A continuación, se envía una definición a los firewalls para prevenir posibles ataques derivados.

El servicio analiza una amplia variedad de sistemas operativos y tipos de archivos, incluidos programas ejecutables, DLL, PDFs, documentos MS Office, archivos, JAR y APK.

Con el fin de ofrecer una protección de puntos terminales completa, SonicWall Capture Client combina tecnología antivirus de próxima generación con el sandbox multimotor basado en la nube de SonicWall.



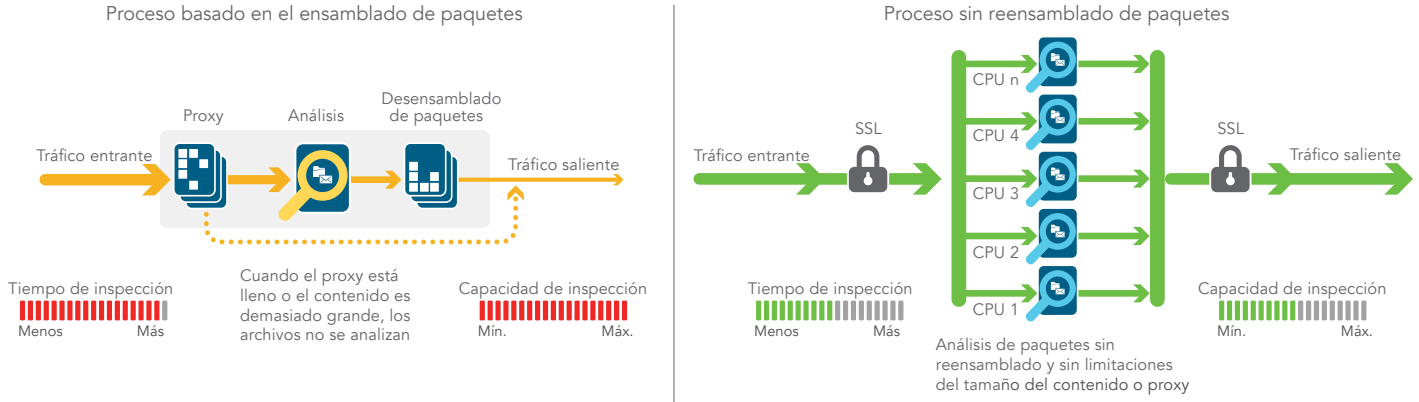
SONICWALL

Motor de inspección profunda de paquetes sin reensamblado

La Inspección profunda de paquetes sin reensamblado (RFDPI) de SonicWall es un sistema de inspección de paso único y baja latencia que realiza análisis bidireccionales del tráfico basados en flujos a alta velocidad sin almacenamiento en búfer ni proxies a fin de descubrir posibles intentos de intrusión o descargas de malware y de identificar el tráfico de aplicaciones independientemente del puerto y el protocolo. Este motor propietario 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 pasa el preprocesamiento necesario, incluido el descifrado TLS/SSL, es analizado con la ayuda de una única representación en memoria propietaria 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.



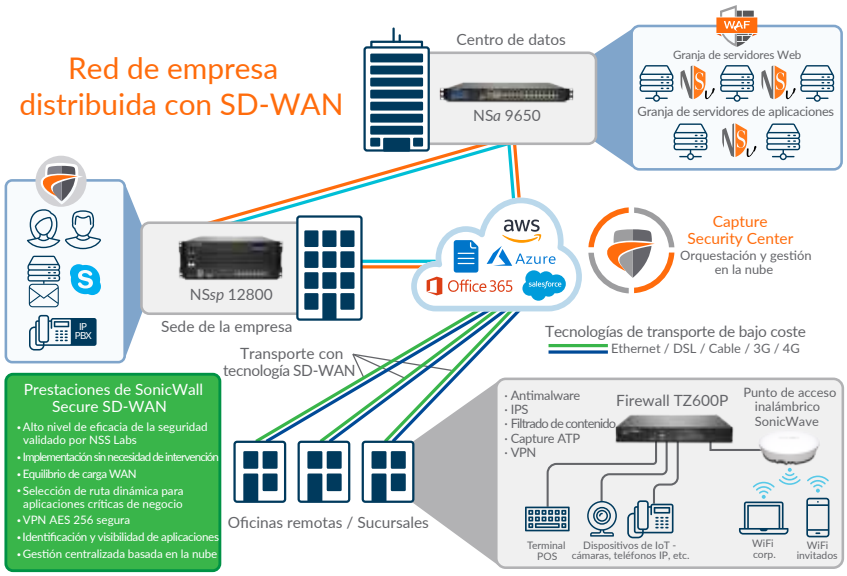
Elaboración de informes y gestión centralizadas

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, puntos de acceso inalámbricos y switches de la serie N y 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 firewall apropiadas en el momento oportuno y de conformidad con la normativa vigente. Disponible 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 las diferentes ubicaciones.

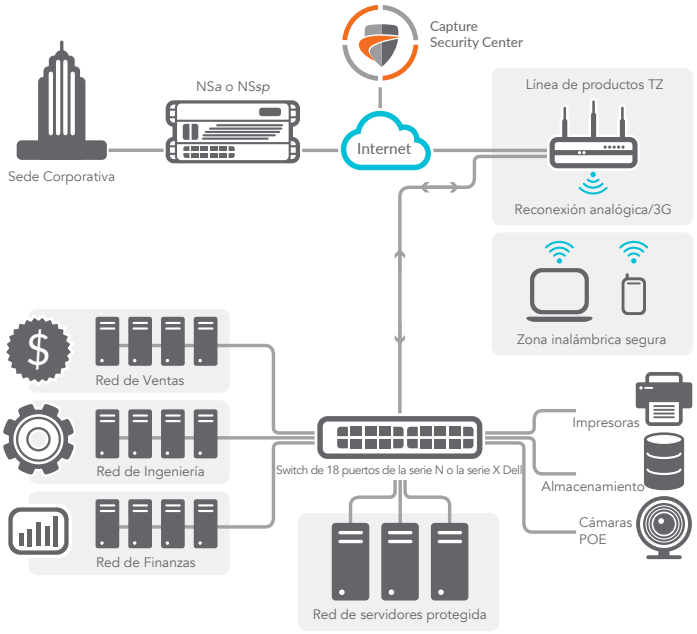
La tecnología SD-WAN de SonicOS es un complemento perfecto para los firewalls



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 sin necesidad de intervención. La configuración y la implementación de firewalls en múltiples emplazamientos lleva tiempo y requiere la intervención del personal in situ. La Implementación sin necesidad de intervención, 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 situacional del entorno de seguridad de 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.



Emplazamientos individuales

Para las implementaciones de emplazamientos individuales, tener una solución de seguridad de red integrada es altamente beneficioso. Los firewalls de la serie TZ combinan una seguridad altamente efectiva con opciones como la conectividad inalámbrica 802.11ac integrada y, en el caso de TZ300P y TZ600P, el soporte de PoE/PoE+. Los firewalls de la serie TZ cuentan con el mismo motor de seguridad que nuestras series de gama media NSa y de gama alta NSsp, así como con la amplia variedad de prestaciones de SonicOS. La configuración y la gestión son tareas sencillas gracias a la IU intuitiva de SonicOS. Las organizaciones ahorran gran cantidad de espacio de bastidor debido al factor de forma compacto.

SONICWALL

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 sin compromisos.

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

TZ600P

Puertos PoE/PoE+ (4 PoE/PoE+)

Indicador LED de alimentación

LED de prueba

Puerto USB (reconexión WAN 3G/4G)

LEDs de enlace y actividad

Módulo de expansión

Puerto de consola

8 switches 1-GbE (configurables)

Puerto LAN X0 Puerto WAN X1

Alimentación segura

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 prevención de amenazas	400 Mbps
Rendimiento de antimalware	400 Mbps
Rendimiento de IPS	1,0 Gbps
Rendimiento de IMIX	700 Mbps
Conexiones DPI máximas	100.000
Nuevas conexiones/s	8.000

Indicador LED de alimentación

LED de prueba

Puerto USB (reconexión WAN 3G/4G)

LEDs de enlace y actividad

Conectividad inalámbrica 802.11ac opcional

Puerto de consola

6 switches 1-GbE (configurables)

Puerto LAN X0 Puerto WAN X1

Alimentación segura

Serie SonicWall TZ400

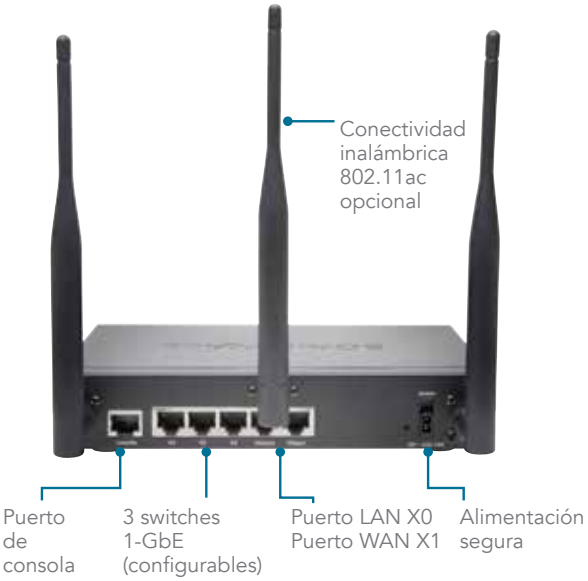
La serie SonicWall TZ400 proporciona protección de clase empresarial para pequeñas empresas, comercios minoristas y sucursales. Disponible implementación inalámbrica flexible con conectividad inalámbrica 802.11ac de banda dual opcional integrada en el firewall.

Especificaciones	Serie TZ400
Rendimiento del firewall	1,3 Gbps
Rendimiento de prevención de amenazas	300 Mbps
Rendimiento de antimalware	300 Mbps
Rendimiento de 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 o alimentación PoE+ 802.3at y el más amplio soporte de acceso móvil seguro para ordenadores portátiles, teléfonos inteligentes y tablets.

Especificaciones	Serie TZ300
Rendimiento del firewall	750 Mbps
Rendimiento de prevención de amenazas	100 Mbps
Rendimiento de antimalware	100 Mbps
Rendimiento de 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 prevención de amenazas	50 Mbps
Rendimiento de antimalware	50 Mbps
Rendimiento de IPS	100 Mbps
Rendimiento de IMIX	60 Mbps
Conexiones DPI máximas	10.000
Nuevas conexiones/s	1.800

Prestaciones

Motor RFDPI	
Prestación	Descripción
Inspección profunda de paquetes sin reensamblado (RFDPI)	Este motor de inspección de alto rendimiento patentado y propietario realiza análisis bidireccionales del tráfico basados en flujos sin almacenamiento en búfer ni proxies a fin de descubrir posibles intentos de intrusión o ataques de malware y de 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 basada en flujos	La tecnología de inspección sin proxy ni búfer proporciona un rendimiento DPI de latencia ultrabaja para millones de flujos de red simultáneos sin limitaciones de tamaño de archivos ni flujos, y puede aplicarse a protocolos comunes y a flujos de TCP sin procesar.
Altamente paralelo y escalable	El diseño único del motor RFDPI, en combinación con la arquitectura multinúcleo, proporciona un rendimiento DPI elevado y tasas de establecimiento de sesiones nuevas extremadamente altas para hacer frente a los picos de tráfico de las redes más exigentes.
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.
Firewall y redes	
Prestación	Descripción
Secure SD-WAN	Una alternativa a las tecnologías más caras, como MPLS, Secure SD-WAN permite a las empresas distribuidas crear, operar y gestionar redes seguras de alto rendimiento en emplazamientos remotos con el fin de compartir datos, aplicaciones y servicios utilizando servicios de Internet públicos, de bajo coste y fácilmente disponibles.
APIs REST	Permiten al firewall recibir y utilizar 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.
Inspección dinámica de paquetes	Todo el tráfico de la red se inspecciona, se analiza y se somete a las políticas de acceso del firewall.
Alta disponibilidad/agrupación (clústeres)	Los modelos SonicWall TZ500 y TZ600 ofrecen compatibilidad con las configuraciones de alta disponibilidad Activa/En espera con sincronización de estado. Los modelos SonicWall TZ300 y TZ400 ofrecen compatibilidad con las configuraciones de alta disponibilidad sin sincronización Activa/En espera. Los modelos SonicWall SOHO no cuentan con alta disponibilidad.
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.
Soporte para IPv6	La versión 6 del protocolo de Internet (IPv6) se encuentra en las primeras fases para sustituir a IPv4. Con SonicOS, el hardware será compatible con las implementaciones de filtrado y de modo Wire.
Opciones de implementación flexibles	La serie TZ puede implementarse en el modo tradicional NAT, en el modo puente de capa 2, en el modo Wire y en el modo de TAP de red.
Equilibrio de carga WAN	Equilibra la carga de múltiples interfaces WAN mediante Round Robin o Spillover o utilizando métodos basados en porcentajes.
Calidad de Servicio (QoS) avanzada	Garantiza las comunicaciones críticas con etiquetado 802.1p y DSCP y remapeo del tráfico VoIP en la red.
Soporte de Gatekeeper H.323 y proxy SIP	Bloquea las llamadas spam: todas las llamadas entrantes han de ser autorizadas y autenticadas mediante Gatekeeper H.323 o proxy SIP.
Gestión de switches individuales y en cascada de las series N y X de Dell.	Gestione los ajustes de seguridad de los puertos adicionales, incluidos Portshield, HA, PoE y PoE+, desde una única consola utilizando el dashboard de gestión del firewall para el switch de red de las series Dell N y Dell X (prestación no disponible con el modelo SOHO).
Autenticación biométrica	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.
Autenticación abierta e inicio de sesión social	Permite a los usuarios invitados utilizar sus credenciales de servicios de redes sociales, como Facebook, Twitter o Google+, para iniciar sesión y acceder a Internet y a otros servicios para usuarios invitados mediante una conexión inalámbrica de un host, una LAN o zonas DMZ, utilizando una autenticación de paso a través.
Seguridad de las redes inalámbricas	Disponible como opción integrada en SonicWall TZ300 hasta TZ500, la tecnología inalámbrica IEEE 802.11ac es capaz de ofrecer hasta 1,3 Gb/s de rendimiento inalámbrico con mayor alcance y fiabilidad. La conectividad 802.11 a/b/g/n está disponible de forma opcional en los modelos SonicWall SOHO.
Gestión e informes	
Prestación	Descripción
Gestión basada en la nube y local	Funciones de configuración y gestión de los dispositivos SonicWall disponibles en la nube a través del SonicWall Capture Security Center y localmente utilizando el Sistema de gestión global (GMS) de SonicWall.
Potente gestión de dispositivos individuales	Ofrece una interfaz intuitiva basada en Web que puede configurarse de forma rápida y sencilla, una interfaz de línea de comandos completa y soporte para 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 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 a la serie TZ actuar como un concentrador VPN para miles de 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 fluida de las funciones de SSO con AD/LDAP/Citrix1/Terminal Services1, 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. Permite crear listas personalizadas de países y Botnets para anular etiquetas de país o Botnet erróneas asociadas con una dirección IP. Elimina el filtrado de direcciones IP no deseado debido a errores de clasificación.
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. Permite crear listas personalizadas de países y Botnets para anular etiquetas de país o Botnet erróneas asociadas con una dirección IP.
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.
Inspección profunda de memoria en tiempo real (RTDMI)	Esta tecnología basada en la nube pendiente de patente detecta y bloquea el malware que no exhibe ningún comportamiento malicioso y oculta sus armas mediante el cifrado. Al forzar al malware a revelar sus armas en la memoria, el motor RTDMI detecta y bloquea de forma proactiva las amenazas de día cero y el malware desconocido del mercado de masas.
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.
Análisis de gran variedad de tipos y tamaños de archivos	Soporta análisis de una amplia variedad de tipos de archivos, ya sea de forma individual o en grupo, 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 ATP 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.
Capture Client	Capture Client es una plataforma de cliente unificada que proporciona múltiples prestaciones de protección de puntos terminales, como protección de malware avanzada y soporte para la visibilidad del tráfico cifrado. Utiliza tecnologías de protección multicapa, funciones completas de informes y prestaciones de refuerzo de protección de puntos terminales.
Prevención de amenazas cifradas	
Prestación	Descripción
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico cifrado mediante TLS/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 SSL. Incluido con las suscripciones de seguridad para todos los modelos de la serie TZ 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 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 de Capture Cloud	Los servidores de la nube de SonicWall disponen de una base de datos de decenas de 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 proporciona 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.
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 miles de 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 HTTP/HTTPS que contengan información o imágenes inaceptables o improductivas con Content Filtering Service y Content Filtering Client.
Cliente de filtrado de contenido reforzado	Amplíe el refuerzo de políticas para bloquear contenido de Internet para dispositivos Windows, Mac OS, Android y Chrome situados fuera del perímetro del firewall.
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.
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.
Antivirus y antispyware reforzados	
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 instalado y activo el software antivirus y/o certificado DPI-SSL apropiado. De este modo, eliminará los costes asociados habitualmente a la gestión de soluciones antivirus 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.
Antivirus de próxima generación	Capture Client utiliza un motor de inteligencia artificial estático para determinar las amenazas antes de que puedan ejecutarse y regresar a un estado previo a la infección.
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.

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
- APIs REST

Descifrado e inspección SSL/SSH[1]

- Inspección profunda de paquetes para TLS/SSL/SSH
- Inclusión/exclusión de objetos, grupos o nombres de host
- Control TLS/SSL
- Controles DPI SSL granulares por zona o norma

Capture Advanced Threat Protection[1,2]

- 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[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
- 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
- Completa 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 HTTP/HTTPS Web[1]

- Filtrado de URL
- Tecnología antiproxy
- Bloqueo según 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

- 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)

Redes

- Secure SD-WAN
- 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 N y la serie X de Dell, incluidos switches en cascada[2]

Conexión inalámbrica integrada

- Doble banda (2,4 GHz y 5,0 GHz)
- Estándares inalámbricos 802.11 a/b/g/n/ac[2]
- WIDS/WIPS
- Servicios inalámbricos para usuarios invitados
- Mensajería ligera en puntos de conexión
- Segmentación mediante puntos de acceso virtuales
- Portal cautivo
- ACL para la nube
- Vista del plano de planta/vista de topología
- Band steering

[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 SonicWall TZ

Hardware - Visión general	Serie SOHO	Serie TZ300	Serie TZ400	Serie TZ500	Serie 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
Soporte de alimentación por Ethernet (PoE)	–	TZ300P - 2 puertos (2 PoE o 1 PoE+)	–	–	TZ600P - 4 puertos (4 PoE o 4 PoE+)
Expansión	USB	USB	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)	250	500	500	500	500
Interfaces VLAN	25	25	50	50	50
Puntos de acceso soportados (máximo)	2	8	16	16	24
Rendimiento de firewall/VPN	**Serie SOHO**	**Serie TZ300**	**Serie TZ400**	**Serie TZ500**	**Serie TZ600**
Rendimiento de inspección del firewall[1]	300 Mbps	750 Mbps	1,3 Gbps	1,4 Gbps	1,5 Gbps
Rendimiento de prevención de amenazas[2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Rendimiento de inspección de aplicaciones[2]	-	300 Mbps	900 Mbps	1,0 Gbps	1,1 Gbps
Rendimiento de IPS[2]	100 Mbps	300 Mbps	900 Mbps	1,0 Gbps	1,1 Gbps
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	1,0 Gbps	1,1 Gbps
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**	**Serie 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, 14v				
VPN basada en enrutamiento	RIP, OSPF, BGP				
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**	**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 completo basado en tipos de archivo como ActiveX, Java, cookies para la privacidad, listas de permitidos/denegados				
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

Especificaciones de la serie SonicWall TZ (cont.)

Redes	Serie SOHO	Serie TZ300	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)				
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			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 (Firewall e IPS)				
Tarjetas Common Access Card (CAC)	Soportado				
Alta disponibilidad	No	Activa/En espera	Activa/En espera	Activa/En espera con sincronización de estado	Activa/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	24 W (externa)	24 W (externa) 65 W (externa) (solo TZ300P)	24 W (externa)	36 W (externa)	60 W (externa) 180 W (externa) (solo TZ600P)
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 (en 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	Serie 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 de la serie SonicWall TZ (cont.)

Conexión inalámbrica integrada	Serie SOHO	Series TZ300, TZ400 y TZ500	Serie 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: 2412-2472 GHz, 5180-5825 GHz	-
Canales operativos	802.11a: Canadá y EE.UU. 12, Europa 11, Japón 4, Singapur 4, Taiwán 4; 802.11b/g: Canadá y EE.UU. 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: Canadá y EE.UU. 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 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 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
SOHO con 1 año de TotalSecure	01-SSC-0651
SOHO Wireless-N con 1 año de TotalSecure	01-SSC-0653
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
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
TZ600 con 1 año de TotalSecure Advanced Edition	01-SSC-1711
TZ600P con 1 año de TotalSecure Advanced Edition	02-SSC-0600
Opciones de alta disponibilidad (todas las unidades deben ser del mismo modelo)	
TZ500 con alta disponibilidad	01-SSC-0439
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 la serie 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

Números de modelo oficiales:

SOHO/SOHO Wireless - APL31-0B9/APL41-0BA

TZ300/TZ300 Wireless/TZ300P - APL28-0B4/APL28-0B5/APL47-0D2

TZ400/TZ400 Wireless - APL28-0B4/APL28-0B5

TZ500/TZ500 Wireless - APL29-0B6/APL29-0B7

TZ600/TZ600P - APL30-0B8/APL48-0D3

Acerca de nosotros

SonicWall lleva más de 27 años combatiendo la industria del crimen cibernético y defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución automatizada de detección y prevención de brechas en tiempo real adaptada a las necesidades específicas de más de 500.000 organizaciones en más de 215 países y territorios, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas. Para más información, visite www.sonicwall.com o síganos en Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com

Datasheet-TZ Series-US-VG-MKTG4140

SONICWALL