



# SonicWALL serie TZ

Seguridad excepcional y rendimiento excelente a un TCO perturbadoramente bajo

Los *firewalls* Dell SonicWALL serie TZ son soluciones de seguridad de red de alto rendimiento de grado empresarial que se adaptan al presupuesto y a los recursos limitados de pequeñas y medianas empresas (SMB), oficinas remotas, sucursales y puntos de venta minoristas.

Los *firewalls* serie TZ de SonicWALL proporcionan una amplia protección a través de servicios avanzados de seguridad que consisten en *antimalware*, *antispyware*, sistema de prevención de intrusiones (IPS) y filtrado de contenido URL. Para contrarrestar la tendencia de ataques cifrados, los nuevos *firewalls* SonicWALL serie TZ tienen el poder de procesamiento necesario para inspeccionar las conexiones SSL cifradas basándose en las amenazas más recientes.

Apoyado por la red de Defensa Inteligente de Respuesta Global (GRID) de Dell SonicWALL, los *firewalls* de la serie TZ de SonicWALL ofrecen actualizaciones continuas para mantener una defensa de red potente contra delincuentes informáticos. Los *firewalls* SonicWALL serie TZ son capaces de analizar cada byte de cada paquete en todos los puertos y protocolos casi sin latencia y sin límite de tamaño de archivo.

Los *firewalls* SonicWALL serie TZ ofrecen puertos Ethernet de gigabit, conexión inalámbrica de 802.11ac integrada opcional, IPSec y VPN SSL, conmutación por error a través de soporte 3G/4G integrado, equilibrio de carga y segmentación de red que reconoce la necesidad de funciones de red avanzadas, así como también de una seguridad avanzada. Los *firewalls* UTM SonicWALL serie TZ también proporcionan un amplio soporte para clientes de acceso remoto VPN nativo en las plataformas Apple iOS,

Google Android, Amazon Kindle, Windows, MacOS y Linux, para obtener un acceso móvil rápido y seguro. Dell SonicWALL Global Management System (GMS) permite la implementación y la administración de *firewalls* SonicWALL de la serie TZ desde un único sistema en la oficina central.

## Protección óptima para su empresa

Para que una SMB crezca, debe adoptar nuevas tecnologías como la movilidad y la nube. Sin embargo, estas nuevas tecnologías pueden exponer a las SMB a ataques maliciosos. Todas las empresas, independientemente de su tamaño, necesitan protección total. Para lograrlo, los SonicWALL serie TZ proporcionan una solución integrada que inspecciona todo el tráfico de la red, incluidas las conexiones SSL cifradas.

## Seguridad administrada para entornos distribuidos

Las escuelas, las tiendas minoristas, los sitios remotos, las sucursales y las empresas distribuidas necesitan una solución que se integra en su *firewall* corporativo. Los *firewalls* SonicWALL serie TZ comparten la misma base de código, y la misma protección, que nuestros *firewalls* emblema de próxima generación SuperMassive. Esto simplifica la administración de sitio remoto, ya que todos los administradores ven la misma interfaz de usuario (UI). GMS permite a los administradores de red configurar, controlar y administrar los *firewalls* SonicWALL remotos a través de un simple panel de vidrio. Al agregar capacidades inalámbricas seguras y de alta velocidad, los *firewalls* SonicWALL serie TZ también extienden el perímetro de protección para incluir a los clientes e invitados que frecuentan el sitio minorista o la oficina remota.



Beneficios:

- Protección de red de grado empresarial que incluye *antimalware*, prevención de intrusiones, control de aplicación y filtrado de contenido/URL
- Inspección profunda de paquete en todo el tráfico: Sin restricciones de tamaño de archivo ni protocolo, incluidas las conexiones SSL cifradas
- Conectividad inalámbrica de 802.11ac segura por medio de controlador inalámbrico integrado o vía *wireless access points* Dell SonicPoint externos
- Acceso remoto VPN SSL para dispositivos Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS y Linux

## SonicWALL serie TZ600

Para empresas emergentes, oficinas minoristas y sucursales que buscan un rendimiento seguro a un precio conveniente, el firewall Dell SonicWALL serie TZ600 de próxima generación brinda seguridad a las redes con características de clase empresarial y rendimiento óptimo.

Especificación	Serie TZ600
Rendimiento del <i>firewall</i>	1,5 Gbps
Rendimiento de DPI completa	500 Mbps
Rendimiento de <i>antimalware</i>	500 Mbps
Rendimiento de IPS	1,1 Gbps
Rendimiento de IMIX	900 Mbps
Conexiones DPI máx.	125.000
Nuevas conexiones/seg	12.000



## SonicWALL serie TZ500

Para las sucursales en crecimiento y las SMB, Dell SonicWALL serie TZ500 aprobó el pdf adjunto de socio para revisión. Ofrece una protección óptima altamente eficaz con productividad de red y conexión inalámbrica integrada de doble banda de 802.11ac opcional.

Especificación	Serie TZ500
Rendimiento del <i>firewall</i>	1,4 Gbps
Rendimiento de DPI completa	400 Mbps
Rendimiento de <i>antimalware</i>	400 Mbps
Rendimiento de IPS	1 Gbps
Rendimiento de IMIX	700 Mbps
Conexiones DPI máx.	100.000
Nuevas conexiones/seg	8000



## SonicWALL serie TZ400

Para pequeñas y medianas empresas, comercios minoristas y sucursales, Dell SonicWALL serie TZ400 ofrece protección de grado empresarial. La implementación inalámbrica flexible está disponible con *access points* SonicPoint externos o conexión inalámbrica de 802.11ac integrada en la unidad.

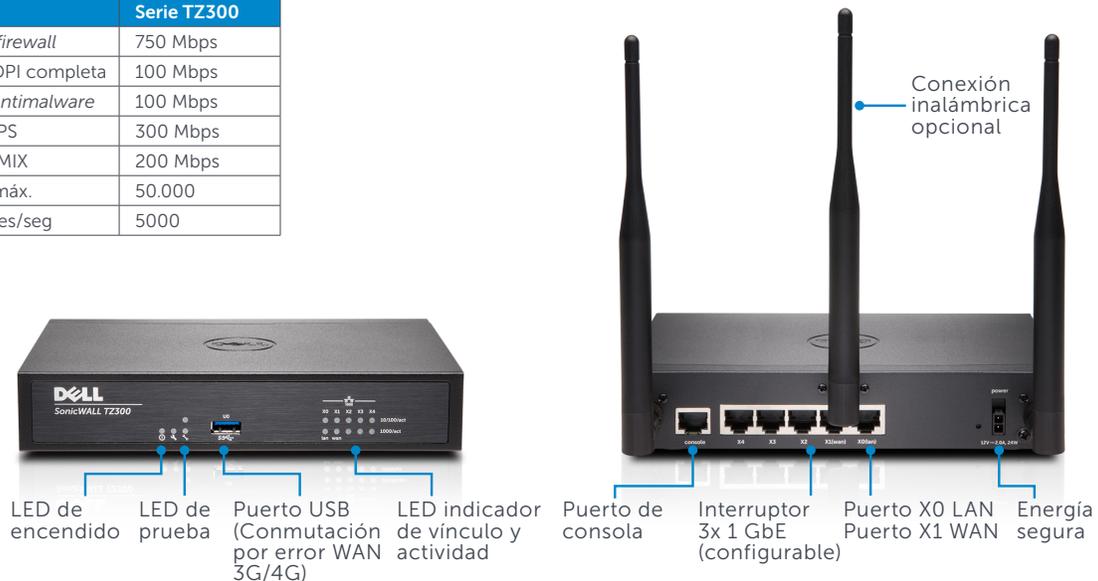
Especificación	Serie TZ400
Rendimiento del <i>firewall</i>	1,3 Gbps
Rendimiento de DPI completa	300 Mbps
Rendimiento de <i>antimalware</i>	300 Mbps
Rendimiento de IPS	900 Mbps
Rendimiento de IMIX	500 Mbps
Conexiones DPI máx.	90.000
Nuevas conexiones/seg	6000



## SonicWALL serie TZ300

Dell SonicWALL serie TZ300 ofrece una solución todo en uno que protege las redes contra ataques. A diferencia de los productos de grado de consumidor, el *firewall* SonicWALL serie TZ300 combina una eficaz prevención de intrusión, *antimalware* y filtrado de contenido/URL con conexión inalámbrica de 802.11ac integrada opcional y soporte amplio y seguro para plataformas móviles para equipos portátiles, teléfonos inteligentes y tabletas.

Especificación	Serie TZ300
Rendimiento del <i>firewall</i>	750 Mbps
Rendimiento de DPI completa	100 Mbps
Rendimiento de <i>antimalware</i>	100 Mbps
Rendimiento de IPS	300 Mbps
Rendimiento de IMIX	200 Mbps
Conexiones DPI máx.	50.000
Nuevas conexiones/seg	5000



## SonicWALL serie SOHO

Para entornos de oficinas pequeñas y del hogar con conexión por cable e inalámbrica, Dell SonicWALL serie SOHO proporciona la misma protección de clase empresarial que requieren las grandes empresas a un precio más accesible.

Especificación	Serie SOHO
Rendimiento del <i>firewall</i>	300 Mbps
Rendimiento de DPI completa	50 Mbps
Rendimiento de <i>antimalware</i>	50 Mbps
Rendimiento de IPS	100 Mbps
Rendimiento de IMIX	60 Mbps
Conexiones DPI máx.	10.000
Nuevas conexiones/seg	1800

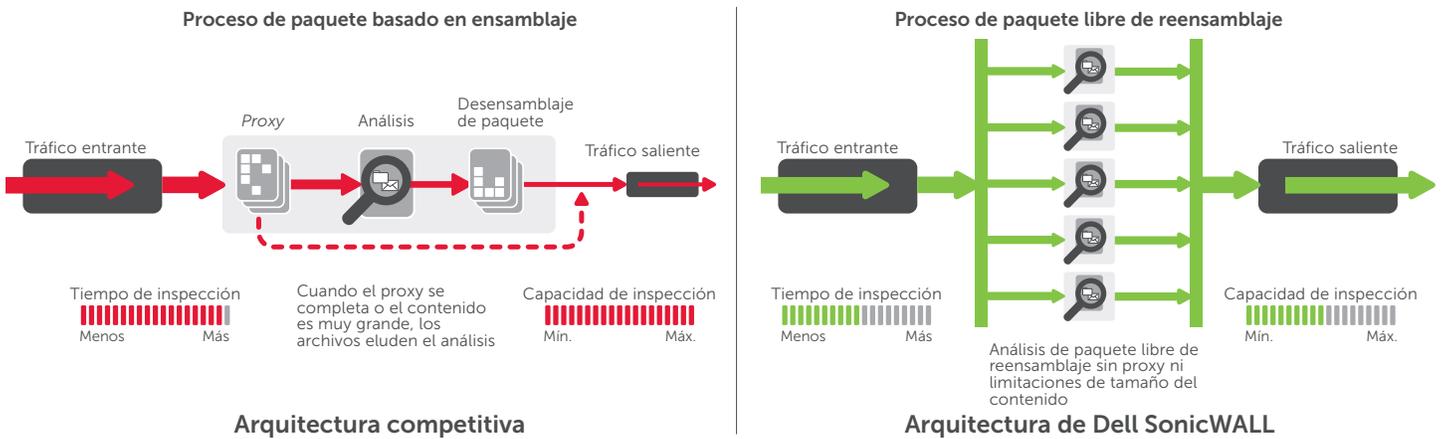


## Administración e informes globales

En el caso de las implementaciones en empresas más grandes y distribuidas, el sistema opcional Dell SonicWALL Global Management System (GMS) proporciona a los administradores una plataforma unificada, segura y extensible, para administrar los dispositivos de seguridad de Dell SonicWALL. Permite a las empresas consolidar fácilmente la administración de los dispositivos de seguridad, reducir las complejidades administrativas y de resolución de problemas, y también se encarga de todos los aspectos operativos de la infraestructura de seguridad, incluidos administración y cumplimiento de políticas centralizados, supervisión de eventos en tiempo real, análisis e informes, y mucho más. GMS también cumple con los requisitos de administración de *firewalls* de las empresas gracias a una función de automatización de flujos de trabajo. GMS proporciona un mejor modo de administrar la seguridad de la red a través de procesos comerciales y niveles de servicio que simplifican significativamente la administración del ciclo de vida de sus entornos de seguridad en general, en lugar de encargarse de un dispositivo por vez.

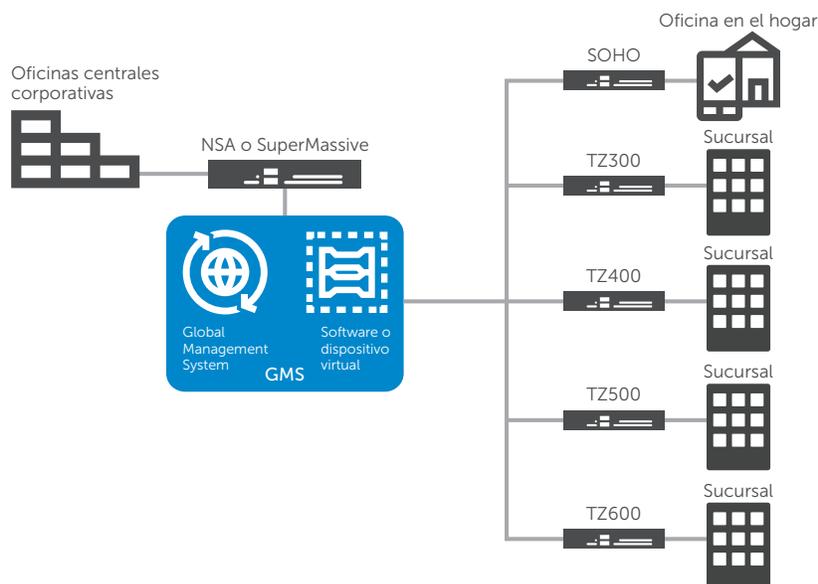
## Motor de inspección profunda de paquetes libre de reensamblaje (RFDPI)

El motor de RFDPI proporciona protección frente a amenazas y control de aplicaciones superiores sin afectar el rendimiento. Este motor patentado inspecciona la transmisión de tráfico para detectar amenazas en los niveles 3 a 7. El motor de RFDPI somete las transmisiones de red a procesos de normalización y cifrado extendidos y reiterados, con el fin de neutralizar las técnicas de evasión avanzadas que intentan confundir a los motores de detección e introducir códigos maliciosos en la red. Después de que se realizan los procedimientos previos necesarios en el paquete, incluido el cifrado SSL, se analiza mediante una representación de memoria propietaria única de tres bases de datos de firmas: Ataques de intrusiones, *malware* y aplicaciones. Luego, se avanza con el estado de la conexión para representar la posición de la transmisión en relación con estas bases de datos hasta que se encuentra un estado de ataque, u otro evento "equivalente", y se lleva a cabo una acción preestablecida. Cuando se identifica *malware*, el *firewall* SonicWALL finaliza la conexión antes de que se vulnere y registra el evento de manera adecuada. No obstante, el motor también puede configurarse como solo inspección o, si se detecta una aplicación, para proporcionar servicios de administración del ancho de banda en el nivel 7 durante el resto de la transmisión de la aplicación tan pronto como se identifica la aplicación.



## Arquitectura extensible para una escalabilidad y un rendimiento extremos

El motor de RFDPI está diseñado desde el comienzo para proporcionar análisis de seguridad a un alto nivel de rendimiento, a fin de adaptarse a la naturaleza inherentemente paralela y en constante crecimiento del tráfico de red. Cuando se combina con sistemas de procesadores de múltiples núcleos, esta arquitectura de software centrada en paralelismos escala perfectamente para abordar las demandas de inspección profunda de paquetes en las cargas de tráfico más altas. La plataforma SonicWALL de la serie TZ utiliza procesadores que, a diferencia de x86, están optimizados para el procesamiento de paquetes, cifrado y redes, al tiempo que se mantiene la flexibilidad y la capacidad de programación en el campo, que es un punto débil de los sistemas ASIC. Esta flexibilidad es esencial cuando se necesitan nuevas actualizaciones de codos y conductas para prevenir nuevos ataques que requieren actualizaciones y técnicas de detección más sofisticadas.

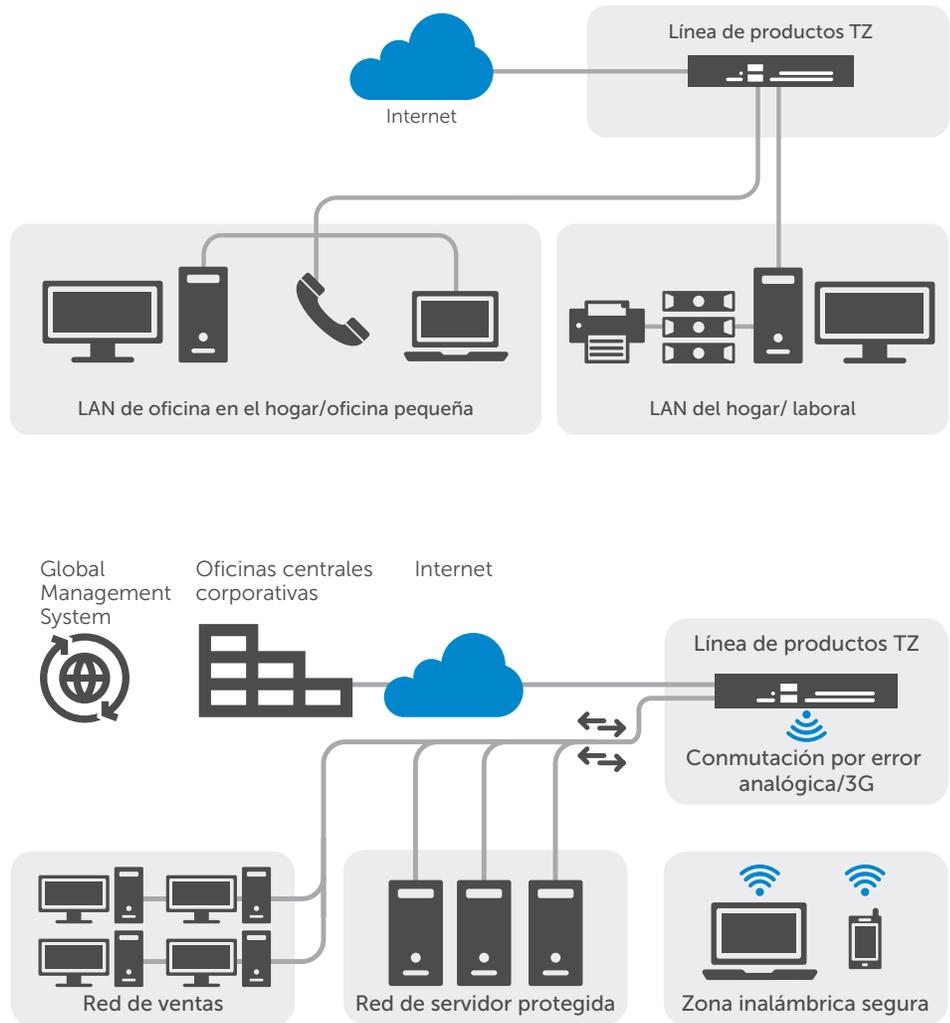


## Seguridad y protección

El equipo de investigación de amenazas interno y especializado de Dell SonicWALL trabaja en la investigación y el desarrollo de tácticas defensivas para implementar los *firewalls* en el campo, a fin de ofrecer una protección actualizada. El equipo utiliza más de un millón de sensores en todo el mundo para tomar muestras de *malware* y obtener datos de telemetría sobre la información de amenazas más reciente, que luego se incluyen en las capacidades de prevención de intrusiones, *antimalware* y detección de aplicación. Los clientes de Dell SonicWALL con suscripciones actuales obtienen protección contra amenazas constantemente actualizada durante todo el día, con nuevas actualizaciones que se aplican inmediatamente sin reinicios ni interrupciones. Las firmas que residen en los dispositivos están diseñadas para proteger contra una amplia gama de ataques y abarcan hasta miles de amenazas individuales con una única firma. Además de las medidas correctivas en el dispositivo, todos los *firewalls* Dell SonicWALL también tienen acceso al servicio Dell SonicWALL CloudAV, que extiende la inteligencia de la firma integrada en más de 17 millones de firmas, y continúa creciendo. El *firewall* obtiene acceso a esta base de datos de CloudAV a través de un protocolo ligero del propietario para profundizar la inspección realizada en el dispositivo. Con las capacidades de filtrado de Geo-IP y *botnet*, los *firewalls* de próxima generación Dell SonicWALL pueden bloquear el tráfico de dominios peligrosos o de geografías enteras, a fin de reducir el perfil de riesgo de la red.

## Inteligencia y control de aplicaciones

La inteligencia de aplicaciones informa a los administradores acerca del tráfico en la red de modo que puedan programar controles de las aplicaciones según la prioridad comercial, acelerar las aplicaciones no productivas y bloquear las aplicaciones potencialmente peligrosas. La visualización en tiempo real permite identificar anomalías en el tráfico a medida que se van produciendo, lo que posibilita la toma de medidas correctivas



inmediatas contra potenciales ataques entrantes o salientes o cuellos de botella en el rendimiento. Con el análisis de tráfico de aplicaciones de Dell SonicWALL se proporciona visibilidad granular del tráfico, el uso de ancho de banda y las amenazas de seguridad de la aplicación, además de potentes capacidades de solución de problemas e investigación forense. Asimismo, con las capacidades seguras de Inicio de sesión único (SSO) se simplifica la experiencia del usuario, se aumenta la productividad y se reduce la cantidad de llamadas al soporte. La administración de la inteligencia y el control de las aplicaciones se simplifica con el uso de una interfaz web intuitiva.

## Conexión inalámbrica flexible y segura

Disponible como característica opcional, la conexión inalámbrica de 802.11ac de alta velocidad se combina con la tecnología del *firewall* Dell SonicWALL de próxima generación para crear una solución de seguridad de red WLAN que proporciona protección integral para redes por cable y WLAN.

Con este rendimiento de clase empresarial los dispositivos compatibles con wifi pueden conectarse desde mayores distancias y utilizar aplicaciones móviles con un gran consumo de ancho de banda, como video y voz, en entornos de mayor densidad sin que la señal se degrade.

## Características

Motor de RFDPI	
Característica	Descripción
Inspección profunda de paquetes libre de reensamblaje	Este motor de inspección propio, patentado y de alto rendimiento realiza análisis de tráfico bidireccional basado en transferencias, sin <i>proxy</i> ni almacenamiento en búfer, con el fin de detectar intentos de intrusión y <i>malware</i> e identificar el tráfico de aplicación sin importar el puerto.
Inspección bidireccional	Analiza el tráfico entrante y saliente de manera simultánea en busca de amenazas, a fin de garantizar que la red no se utilice para distribuir <i>malware</i> y no se convierta en una plataforma de lanzamiento de ataques en el caso de que haya un equipo infectado.
Inspección de un solo paso	La arquitectura de DPI de un solo paso realiza análisis simultáneos para detectar <i>malware</i> e intrusiones y también identificar aplicaciones, lo que reduce significativamente la latencia de DPI y garantiza que toda la información sobre amenazas se correlacione en una única arquitectura.
Inspección basada en transferencias	La tecnología de inspección sin <i>proxy</i> ni almacenamiento en búfer ofrece un rendimiento de latencia ultrabaja para la inspección profunda de paquetes de millones de transferencias simultáneas de la red sin la necesidad de utilizar límites de tamaño de archivo y transferencia, y puede utilizarse en protocolos comunes y en transferencias TCP sin procesar.
Prevención de intrusiones	
Característica	Descripción
Protección basada en medidas correctivas	El sistema de prevención de intrusiones (IPS) perfectamente integrado utiliza las firmas y las demás medidas correctivas para analizar las cargas de paquete en busca de vulnerabilidades y ataques, lo que permite abarcar un amplio espectro de ataques y vulnerabilidades.
Actualizaciones automáticas de firmas	El equipo de investigación de amenazas de Dell SonicWALL analiza e implementa de manera continua actualizaciones en una extensa lista de medidas correctivas del IPS, que abarca más de 50 categorías de ataques. Las nuevas actualizaciones se implementan de inmediato sin la necesidad de reiniciar o interrumpir el servicio.
Protección IPS entre zonas	Mejora la seguridad interna al segmentar la red en varias zonas de seguridad con la prevención de intrusiones, lo que permite evitar que las amenazas se propaguen en los límites de cada zona.
Detección y bloqueo de comando y control (CnC) de Botnet	Identifica y bloquea el tráfico de comando y control que se origina en los <i>bots</i> de la red local y se dirigen a las direcciones IP y los dominios, y se identifica como <i>malware</i> o puntos conocidos de CnC.
Abuso/anomalía de protocolo	Identifica y bloquea ataques que se abusan de los protocolos para intentar eludir el IPS.
Protección de día cero	Protege la red frente a ataques de día cero con actualizaciones constantes contra los métodos y las técnicas de ataques más recientes, lo que cubre miles de ataques individuales.
Tecnología antievasión	La normalización extensa de transferencia, la decodificación y las demás técnicas garantizan que ninguna amenaza ingrese en la red sin ser detectada, mediante el uso de las técnicas de evasión entre las capas 2-7.
Prevención de amenazas	
Característica	Descripción
<i>Antimalware</i> de puertas de enlace	El motor de RFDPI analiza todo el tráfico entrante, saliente y entre zonas en busca de virus, troyanos, registradores de pulsaciones de teclas y demás <i>malware</i> en archivos de longitud y tamaño ilimitados en todos los puertos, y todas las transferencias de TCP.
Protección contra <i>malware</i> CloudAV	Una base de datos continuamente actualizada de más de 17 millones de firmas de amenazas reside en los servidores de nube de Dell SonicWALL y se recurre a esta para aumentar las capacidades de la base de datos de firmas integrada, lo que proporciona una RFDPI con una amplia cobertura de amenazas.
Actualizaciones de seguridad constantes	Las actualizaciones de nuevas amenazas se implementan en los <i>firewalls in situ</i> mediante servicios activos de seguridad y no es necesario reiniciar ni interrumpir el trabajo.
Descifrado e inspección de SSL	Descifra e inspecciona el tráfico SSL sobre la marcha, sin <i>proxy</i> , en busca de <i>malware</i> , intrusiones y fuga de datos, y aplica políticas de aplicación, URL y control de contenido a fin de proteger la red contra amenazas ocultas en el tráfico SSL cifrado incluido en las suscripciones de seguridad de todos los modelos, excepto SOHO. En SOHO se vende como licencia separada.
Inspección bidireccional de TCP sin procesar	El motor de RFDPI puede analizar bidireccionalmente transferencias de TCP sin procesar en cualquier puerto, lo que permite evitar ataques que intentan eludir sistemas de seguridad obsoletos que se enfocan en unos pocos puertos conocidos.
Amplia compatibilidad de protocolos	Identifica protocolos comunes como HTTP/S, FTP, SMTP, SMBv1/v2 y otros, que no envían datos en TCP sin procesar, y decodifica las cargas para realizar una inspección de <i>malware</i> , incluso si no se transfieren en puertos estándares y conocidos.
Inteligencia y control de aplicaciones	
Característica	Descripción
Control de aplicaciones	Controla aplicaciones o funciones de aplicaciones individuales, que el motor de RFDPI identifica utilizando una base de datos en constante expansión de más de 3500 firmas de aplicaciones, con el fin de aumentar la seguridad de la red y mejorar la productividad de la red.
Identificación de aplicación personalizada	Controla las aplicaciones personalizadas mediante la creación de firmas basadas en patrones o parámetros específicos que son exclusivos de una aplicación en las comunicaciones de red, con el fin de obtener un mayor control de la red.
Administración de ancho de banda de aplicación	Asigna y regula granularmente el ancho de banda disponible para aplicaciones o categorías de aplicaciones críticas al tiempo que inhibe el tráfico de aplicaciones no esenciales.
Control granular	Controla las aplicaciones o los componentes específicos de una aplicación, basándose en programas, grupos de usuarios, listas de exclusión y un rango de acciones con una identificación SSO de usuario completa mediante la integración en LDAP/AD/Terminal Services/Citrix.
Filtrado de contenido	
Característica	Descripción
Filtrado de contenido interno/externo	Refuerza las políticas aceptables de uso y bloquea el acceso a los sitios web que contienen información o imágenes inapropiadas o improductivas con Content Filtering Service. Extiende el cumplimiento de políticas para el bloqueo de contenido de Internet en dispositivos ubicados fuera del perímetro del <i>firewall</i> mediante Content Filtering Client.

## Características

Filtrado de contenido	
Característica	Descripción
Controles granulares	Bloquea contenido utilizando categorías predefinidas o cualquier combinación de categorías. El filtrado puede programarse por momentos del día, como, por ejemplo, durante el horario de oficina o clases, y aplicarse a usuarios y grupos individuales.
YouTube para escuelas	Permite que los profesores elijan cientos de miles de videos educativos gratuitos de YouTube EDU, que se organizan por asignatura y año, y se alinean con estándares educativos comunes.
Almacenamiento en caché de web	Las clasificaciones de URL se almacenan en caché de manera local en el <i>firewall</i> de Dell SonicWALL para que el tiempo de respuesta del acceso subsiguiente a los sitios con más visitas sea de solo una fracción de segundo.
Antivirus y <i>antispyware</i> reforzados	
Característica	Descripción
Protección multicapa	Utiliza las capacidades del <i>firewall</i> como la primera capa de defensa del perímetro, en combinación con protección de extremo para bloquear los virus que ingresan en la red a través de equipos portátiles, unidades de almacenamiento en miniatura y otros sistemas no protegidos.
Opción de cumplimiento automatizado	Garantiza que cada equipo que obtiene acceso a la red cuente con la versión más reciente de las firmas antivirus y <i>antispyware</i> instaladas y activas, lo que elimina los gastos comúnmente asociados con la administración antivirus y <i>antispyware</i> de los equipos de escritorio.
Opción de implementación e instalación automatizadas	La implementación y la instalación equipo por equipo de los clientes antivirus y <i>antispyware</i> se automatizan en la red, lo que minimiza los gastos administrativos.
Protección antivirus automática siempre habilitada	Se entregan actualizaciones frecuentes de antivirus y <i>antispyware</i> para todos los equipos de escritorio y los servidores de archivos, a fin de mejorar la productividad del usuario final y reducir la administración de seguridad.
Protección contra <i>spyware</i>	La sólida protección <i>antispyware</i> analiza y bloquea la instalación de un conjunto integral de programas <i>spyware</i> en equipos de escritorio y portátiles antes de que transmitan datos confidenciales, lo que proporciona mejor rendimiento y mayor seguridad en el equipo de escritorio.
Firewalls y redes	
Característica	Descripción
Inspección de paquetes con estado	Todo el tráfico de red se inspecciona y se analiza, y cumple con las políticas de acceso del <i>firewall</i> .
Protección contra ataques DDoS/DoS	La protección frente a la inundación SYN proporciona una defensa contra ataques DOS mediante el uso del proxy de SYN nivel 3 y las tecnologías de lista negra de SYN nivel 2. Asimismo, proporciona protección frente a DOS/DDoS mediante la protección de inundación UDP/ICMP y los límites de tasas de conexión.
Opciones de implementación flexibles	Los dispositivos SonicWALL serie TZ pueden implementarse en los modos tradicionales NAT, puente nivel 2, modo cableado y conexión de red.
Compatibilidad con IPv6	El Protocolo de Internet versión 6 (IPv6) aún se encuentra en una etapa temprana para sustituir a IPv4. Con el SonicOS más reciente, el hardware admitirá las implementaciones de filtrado.
Alta disponibilidad	Los modelos SonicWALL TZ500 y TZ600 admiten alta disponibilidad con activa/en espera con sincronización de estado. Los modelos SonicWALL TZ300 y TZ400 admiten alta disponibilidad sin sincronización activa/en espera. No hay alta disponibilidad en los modelos SonicWALL SOHO.
Seguridad de la red WLAN	La tecnología IEEE 802.11ac inalámbrica puede proporcionar hasta 1,3 Gbps de rendimiento de conexión inalámbrica con mayor alcance y confiabilidad. Disponible en modelos desde el SonicWALL TZ600 hasta el SonicWALL TZ300. 802.11 a/b/g/n opcional disponible en los modelos SonicWALL SOHO.
Administración y generación de informes	
Característica	Descripción
Global Management System	Dell SonicWALL GMS monitorea, configura y genera informes de varios dispositivos Dell SonicWALL a través de una única consola de administración con una interfaz intuitiva, a fin de reducir los costos y la complejidad de la administración.
Administración sólida con un único dispositivo	Una interfaz web intuitiva que permite una configuración veloz y cómoda. Además, una interfaz de línea de comandos completa y compatibilidad con SNMPv2/3.
Informes de flujo de aplicación de IPFIX/NetFlow	Exporta el análisis de tráfico de aplicaciones y los datos de uso mediante protocolos IPFIX o NetFlow para el monitoreo histórico y en tiempo real, y la generación de informes con herramientas como Dell SonicWALL Scrutinizer u otras herramientas que admiten IPFIX y NetFlow a través de extensiones.
Red privada virtual	
Característica	Descripción
VPN IPSec para conectividad sitio a sitio	La VPN IPSec de alto rendimiento permite que SonicWALL de la serie TZ actúe como un concentrador de VPN para miles de sitios amplios, sucursales u hogares.
Acceso remoto de VPN SSL o cliente IPSec	Utiliza una tecnología VPN SSL sin cliente o un cliente IPSec fácil de administrar para obtener acceso fácilmente a los correos electrónicos, los archivos, los equipos, los sitios de intranet y las aplicaciones de las diversas plataformas.
Puerta de enlace redundante de VPN	Cuando se utilizan varias WAN, se puede configurar una VPN primaria y una secundaria para permitir una conmutación por error y una conmutación por recuperación automática y perfecta de todas las sesiones de VPN.
VPN basada en ruta	La capacidad de realizar enrutamiento dinámico en vínculos de VPN garantiza una actividad continua en el caso de que haya un error temporal de túnel de VPN, ya que vuelve a enrutar sin problemas el tráfico entre los extremos mediante rutas alternativas.
Comprensión de contenido/contexto	
Característica	Descripción
Seguimiento de las actividades de los usuarios	Se proporciona la identificación y la actividad de usuario a través de la integración SSO perfecta en AD/LDAP/Citrix1/Terminal Services junto con la extensa información obtenida a través de la DPI.
Identificación GeolP del tráfico de país	Identifica y controla el tráfico de la red entrante o saliente de países específicos para proporcionar protección contra ataques conocidos u orígenes sospechosos de amenazas, o bien investigar el tráfico sospechoso que se origina en la red.
Filtrado DPI de expresión regular	Evita la fuga de datos al identificar y controlar el contenido que se transmite por la red mediante las coincidencias de expresión regular.

## Resumen de características de SonicOS

### Firewall

- Inspección profunda de paquetes libre de reensamblaje
- Inspección profunda de paquetes de SSL
- Inspección de paquetes con estado
- Modo discreto
- Compatibilidad con tarjetas de acceso común (CAC)
- Protección contra ataques DOS
- Protección contra ataques UDP/ICMP/SYN
- Descifrado SSL
- Seguridad IPv6

### Prevención de intrusiones

- Análisis basado en firmas
- Actualizaciones automáticas de firmas
- Motor de inspección bidireccional
- Capacidad de reglas granulares de IPS
- Filtrado basado en reputación y GeolP
- Coincidencias de expresión regular

### Antimalware

- Análisis de *malware* basado en la transmisión
- Antivirus para puerta de enlace
- *Antispyware* de puerta de enlace
- Inspección bidireccional
- Sin límite de tamaño de archivo
- Base de datos de *malware* en la nube

### Control de aplicaciones

- Control de aplicaciones
- Bloqueo de componente de aplicación
- Administración de ancho de banda de aplicación
- Creación de firma personalizada de aplicación
- Prevención de fuga de datos
- Generación de informes de aplicación mediante NetFlow/IPFIX
- Seguimiento de la actividad del usuario (SSO)
- Base de datos integral de firmas de aplicación

### Filtrado de contenido web

- Filtrado URL
- Tecnología *antiproxy*
- Bloqueo de palabras clave
- Categorías de clasificación de CFS para la administración del ancho de banda
- Modelo de políticas unificado con control de aplicación
- 57 categorías de filtrado de contenido
- Content Filtering Service Client

### VPN

- VPN IPSec para conectividad sitio a sitio
- Acceso remoto de VPN SSL y cliente IPSEC
- Puerta de enlace redundante de VPN
- Conexión móvil para iOS y Android™
- VPN basada en ruta (OSPF, RIP)

### Redes

- PortShield
- Detección de redes en nivel 2
- IPv6
- Registros mejorados
- Replicación de puertos
- QoS de nivel 2
- Seguridad del puerto
- Enrutamiento dinámico
- Enrutamiento basado en políticas
- Enrutamiento asimétrico
- Servidor DHCP
- Administración del ancho de banda
- Alta disponibilidad activa/en espera con sincronización de estado\*
- Equilibrio de la carga entrante/saliente
- Puente L2, modo NAT, DDNS
- Conmutación por error WAN 3G/4G

### Voz sobre protocolo de Internet (VoIP)

- Control granular de calidad de servicio
- Administración del ancho de banda
- DPI para el tráfico VoIP
- Equipo selector H.323 y compatibilidad con *proxy* SIP

### Administración y monitoreo

- GUI web
- Interfaz de línea de comandos (CLI)
- SNMPv2/v3
- Informes externos (Scrutinizer)
- Administración y generación de informes centralizados
- Registros
- Exportación de Netflow/IPFix
- Visualización del tráfico de aplicación
- Administración de políticas centralizada
- Inicio de sesión único (SSO)
- Compatibilidad con servicio de terminal/Citrix
- Visualización de aplicación y ancho de banda
- Administración de IPv4 e IPv6

### IPv6

- Filtrado IPv6
- 6rd (implementación veloz)
- Delegación de prefijo DHCP
- BGP

### Inalámbrico

- Doble banda (2,4 GHz y 5,0 GHz)
- Estándares inalámbricos 802.11 a/b/g/n/ac
- Detección y prevención de intrusiones inalámbricas
- Servicios de invitados inalámbricos
- Mensajería ligera de zonas activas
- Segmentación de punto de acceso virtual
- Portal cautivo
- ACL en la nube

\*Alta disponibilidad de sincronización de estado solo en los modelos SonicWALL TZ500 y TZ600

## Especificaciones del sistema de SonicWALL serie TZ

Descripción general del rendimiento	Serie SOHO	Serie TZ300	Serie TZ400	Serie TZ500	Serie TZ600
Sistema operativo	SonicOS 5.9x/6.2.x	SonicOS 6.2.x			
Procesador de seguridad	2 x 400 MHz/ 2 x 800 MHz	2 x 800 MHz	4 x 800 MHz	4 x 1 GHz	4 x 1,4 GHz
Memoria (RAM)	512 MB/1 GB	1 GB	1 GB	1 GB	1 GB
Memoria (flash)	32 MB/64 MB	64 MB	64 MB	64 MB	64 MB
Interfaces de cobre de 1 GbE	5	5	7	8	10
Expansión	USB	USB	USB	2 USB	Ranura de expansión (trasera)*, 2 USB
Rendimiento de inspección de <i>firewall</i> <sup>1</sup>	300 Mbps	750 Mbps	1300 Mbps	1400 Mbps	1500 Mbps
Rendimiento de DPI completa <sup>2</sup>	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Rendimiento de inspección de aplicación <sup>2</sup>	-	300 Mbps	900 Mbps	1000 Mbps	1100 Mbps
Rendimiento de IPS <sup>2</sup>	100 Mbps	300 Mbps	900 Mbps	1000 Mbps	1100 Mbps
Rendimiento de inspección <i>antimalware</i> <sup>2</sup>	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Rendimiento de IMIX <sup>3</sup>	60 Mbps	200 Mbps	500 Mbps	700 Mbps	900 Mbps
Rendimiento de inspección y descifrado SSL (DPI SSL) <sup>2</sup>	15 Mbps	45 Mbps	100 Mbps	150 Mbps	200 Mbps
Rendimiento de VPN IPSec <sup>3</sup>	100 Mbps	300 Mbps	900 Mbps	1000 Mbps	1100 Mbps
Conexiones por segundo	1800	5000	6000	8000	12.000
Cantidad máxima de conexiones (SPI)	10.000	50.000	100.000	125.000	150.000
Cantidad máxima de conexiones (DPI)	10.000	50.000	90.000	100.000	125.000
Usuarios con inicio de sesión único (SSO)	250	500	500	500	500
Interfaces de Red de área local virtual (VLAN)	25	25	50	50	50
SonicPoints admitidos (máximo)	2	8	16	16	24
<b>VPN</b>	<b>Serie SOHO</b>	<b>Serie TZ300</b>	<b>Serie TZ400</b>	<b>Serie TZ500</b>	<b>Serie TZ600</b>
Túneles VPN de sitio a sitio	10	10	20	25	50
Clientes de 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 en paquete (máximo)	-	1 (prueba de 30 días)			
Autenticación/cifrado	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, Criptografía Suite B				
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14				
VPN basada en ruta	Protocolo de información de enrutamiento (RIP), Protocolo de Primero la ruta más corta (OSPF)				
Compatibilidad con certificados	Verisign, Thawte, Cybertrust, RSA Keon, Entrust y Microsoft CA para VPN de Dell SonicWALL a Dell SonicWALL, SCEP				
Características de VPN	Detección de extremo muerto, DHCP sobre VPN, cruce seguro de NAT IPsec, puerta de enlace VPN redundante, VPN basada en rutas				
Plataformas de clientes 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				
NetExtender	Microsoft Windows Vista 32/64 bits, Windows 7, Windows 8.0 32/64 bits, Windows 8.1 32/64 bits, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE				
Conexión móvil	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Windows 8.1 (integrada)				
<b>Servicios de seguridad</b>	<b>Serie SOHO</b>	<b>Serie TZ300</b>	<b>Serie TZ400</b>	<b>Serie TZ500</b>	<b>Serie TZ600</b>
Servicios de inspección profunda de paquetes	Antivirus de puerta de enlace, <i>antispyware</i> , prevención de intrusiones, DPI SSL				
Content Filtering Service (CFS)	URL HTTP, HTTPS IP, análisis de contenido y palabras clave, filtrado integral según tipos de archivos como ActiveX, Java, cookies para privacidad, permitir/prohibir listas				
Enforced Client Anti-Virus and Anti-Spyware	McAfee®				
Comprehensive Anti-Spam Service	Admitido				
Visualización de la aplicación	No	Sí	Sí	Sí	Sí
Control de aplicaciones	Sí	Sí	Sí	Sí	Sí

## Especificaciones del sistema de SonicWALL serie TZ

Redes	Serie SOHO	Serie TZ300	Serie TZ400	Serie TZ500	Serie TZ600
Asignación de direcciones IP	Estática, (cliente PPTP, DHCP, PPPoE, L2TP), servidor DHCP interno, retransmisión DHCP				
Modos de Traducción de dirección de red (NAT)	1 a 1, 1 a muchos, muchos a 1, muchos a muchos, NAT flexible (IP superpuestas), PAT, modo transparente				
Protocolos de enrutamiento	Protocolo de pasarela externa (BGP), OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en las políticas, multidifusión				
QoS (Calidad del servicio)	Prioridad de ancho de banda, máximo de ancho de banda, ancho de banda garantizado, marcado con (DSCP), 802.1e (WMM)				
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos de usuarios interna, Terminal Services, Citrix				
Base de datos de usuarios locales	150			250	
Voz sobre protocolo de Internet (VoIP)	Full H.323v1-5, SIP				
Estándares	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certificaciones	VPNC, IPv6 (Fase 2)				
Certificaciones pendientes	Common Criteria NDPP, FIPS 140-2 (con Suite B) Nivel 2, ICSA Firewall, ICSA Anti-virus, UC APL				
Capacidad para tarjetas de acceso común (CAC)	Admitido				
Alta disponibilidad	No	Activo/en espera	Activo/en espera	Activo/en espera con sincronización de estado completo	Activo/en espera con sincronización de estado completo
Hardware	Serie SOHO	Serie TZ300	Serie TZ400	Serie TZ500	Serie TZ600
Factor de forma	Equipo de escritorio				
Fuente de alimentación (W)	24 W externa	24 W externa	24 W externa	36 W externa	60 W externa
Consumo máximo de energía (W)	6,4/11,3	6,9/12,0	9,2/13,8	13,4/17,7	16,1
Alimentación de entrada	100 a 240 V CA, 50 a 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 lb 0,048 kg/0,106 lb	0,73 kg/1,61 lb 0,84 kg/1,85 lb	0,73 kg/1,61 lb 0,84 kg/1,85 lb	0,92 kg/2,03 lb 1,05 kg/2,31 lb	1,47 kg/3,24 lb
Peso de la WEEE	0,80 kg/1,76 lb 0,94 kg/2,07 lb	1,15 kg/2,53 lb 1,26 kg/2,78 lb	1,15 kg/2,53 lb 1,26 kg/2,78 lb	1,34 kg/2,95 lb 1,48 kg/3,26 lb	1,89 kg/4,16 lb
Peso de envío	1,20 kg/2,64 lb 1,34 kg/2,95 lb	1,37 kg/3,02 lb 1,48 kg/3,26 lb	1,37 kg/3,02 lb 1,48 kg/3,26 lb	1,93 kg/4,25 lb 2,07 kg/4,56 lb	2,48 kg/5,47 lb
Tiempo medio entre fallas (MTBF) (años)	30/15	28/14	27/13	20/12	18
Entorno	40-105 °F, 0-40 °C				
Humedad	5-95 % sin condensación				
Regulaciones	Serie SOHO	Serie TZ300	Serie TZ400	Serie TZ500	Serie TZ600
Modelo reglamentario (por cable)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Cumplimiento de la normativa principal (modelos por cable)	FCC Clase B, ICES Clase B, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase B, UL, cUL, TUV/GS, CB, México CoC 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, México CoC 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, México CoC 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, México CoC 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, México CoC por UL, WEEE, REACH, KCC/MSIP
Modelos reglamentarios (inalámbricos)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Cumplimiento de la normativa principal (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, México CoC 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, México CoC 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, México CoC 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, México CoC por UL, WEEE, REACH	-



## Especificaciones del sistema de SonicWALL serie TZ

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	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	-
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 transmisión de salida	Basada en el dominio regulatorio especificado por el administrador del sistema	Basada en el dominio regulatorio especificado por el administrador del sistema	-
Control de potencia de transmisión	Admitido	Admitido	-
Velocidades de datos 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, 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 tecnología de modulación	802.11a: multiplexación por división de frecuencias ortogonales (OFDM); 802.11b: espectro ensanchado por secuencia directa (DSSS); 802.11g: multiplexación por división de frecuencias ortogonales (OFDM)/espectro ensanchado por secuencia directa (DSSS); 802.11n: multiplexación por división de frecuencias ortogonales (OFDM)	802.11a: multiplexación por división de frecuencias ortogonales (OFDM); 802.11b: espectro ensanchado por secuencia directa (DSSS); 802.11g: multiplexación por división de frecuencias ortogonales (OFDM)/espectro ensanchado por secuencia directa (DSSS); 802.11n: multiplexación por división de frecuencias ortogonales (OFDM);802.11ac: multiplexación por división de frecuencias ortogonales (OFDM)	-

\*Uso futuro.

<sup>1</sup> Metodologías de prueba: Máximo rendimiento según RFC 2544 (para *firewall*). El rendimiento real puede variar según las condiciones de red y los servicios que se activan.

<sup>2</sup> El rendimiento de DPI completa/antivirus de puerta de enlace/*antispysware*/IPS se mide con la prueba de rendimiento estándar de la industria de Spirent WebAvalanche HTTP y las herramientas de prueba de Ixia. Pruebas realizadas con distintos flujos a través de distintos pares de puertos.

<sup>3</sup> El rendimiento de VPN se mide al utilizar el tráfico de UDP en un paquete de 1280 bytes según RFC 2544. Todas las especificaciones, las características y la disponibilidad pueden variar.

<sup>4</sup> Solo disponible para SonicWALL series TZ300, TZ400, TZ500 y TZ600

## Información de pedido de SonicWALL TZ Series

Producto	SKU
Dell SonicWALL SOHO con 1 año de TotalSecure	01-SSC-0651
Dell SonicWALL SOHO Wireless-N con 1 año de TotalSecure	01-SSC-0655
Dell SonicWALL TZ300 con 1 año de TotalSecure	01-SSC-0581
Dell SonicWALL TZ300 Wireless-AC con 1 año de TotalSecure	01-SSC-0585
Dell SonicWALL TZ400 con 1 año de TotalSecure	01-SSC-0514
Dell SonicWALL TZ400 Wireless-AC con 1 año de TotalSecure	01-SSC-0518
Dell SonicWALL TZ500 con 1 año de TotalSecure	01-SSC-0445
Dell SonicWALL TZ500 Wireless-AC con 1 año de TotalSecure	01-SSC-0447
Dell SonicWALL TZ600 con 1 año de TotalSecure	01-SSC-0219
<b>Opciones de alta disponibilidad (cada unidad debe ser del mismo modelo)</b>	
Dell SonicWALL TZ500 High Availability	01-SSC-0439
Dell SonicWALL TZ600 High Availability	01-SSC-0220

Servicios	SKU
<b>Para Dell SonicWALL SOHO</b>	
• Comprehensive Gateway Security Suite, 1 año	01-SSC-0688
• Gateway Anti-Virus, Intrusion Prevention and 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 las 24 horas del día, los siete días de la semana, 1 año	01-SSC-0700
<b>Para Dell SonicWALL TZ300</b>	
• Comprehensive Gateway Security Suite, 1 año	01-SSC-0638
• Gateway Anti-Virus, Intrusion Prevention and 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 las 24 horas del día, los siete días de la semana, 1 año	01-SSC-0620
<b>Para Dell SonicWALL TZ400</b>	
• Comprehensive Gateway Security Suite, 1 año	01-SSC-0567
• Gateway Anti-Virus, Intrusion Prevention and 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 las 24 horas del día, los siete días de la semana, 1 año	01-SSC-0552
<b>Para Dell SonicWALL TZ500</b>	
• Comprehensive Gateway Security Suite, 1 año	01-SSC-0488
• Gateway Anti-Virus, Intrusion Prevention and 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 las 24 horas del día, los siete días de la semana, 1 año	01-SSC-0476
<b>Para Dell SonicWALL TZ600</b>	
• Comprehensive Gateway Security Suite, 1 año	01-SSC-0258
• Gateway Anti-Virus, Intrusion Prevention and 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 las 24 horas del día, los siete días de la semana, 1 año	01-SSC-0246

### Dell Software

www.dell.com

Si se encuentra fuera de América del Norte, puede encontrar información sobre su oficina local en nuestro sitio web.

© 2015 Dell Inc. TODOS LOS DERECHOS RESERVADOS. Dell, Dell Software, el logotipo del software de Dell y los productos, como se identifican en este documento, son marcas registradas de Dell, Inc. en los Estados Unidos y en otros países. Todas las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos dueños.

Datasheet-SonicWALL-TZ Series-US-KS-26675

