Serie SonicWall SuperMassive

Protección de firewall de próxima generación de alto rendimiento y sin compromisos para su red corporativa.

La serie SonicWall SuperMassive es la plataforma de firewall de próxima generación (NGFW) de SonicWall, diseñada para ofrecer a las redes grandes escalabilidad, fiabilidad y el más alto nivel de seguridad a velocidades multi-gigabit y con una latencia prácticamente nula.

La serie SuperMassive es ideal para proteger las redes empresariales distribuidas, los centros de datos y los proveedores de servicios en entornos corporativos, gubernamentales, educativos, minoristas, sanitarios y de proveedores de servicios.

Al combinar el sistema operativo SonicOS de SonicWall, la tecnología patentada de Inspección profunda de paquetes sin reensamblado (RFDPI) y la arquitectura de hardware mutinúcleo altamente escalable, la serie SuperMassive 9000 ofrece las prestaciones más avanzadas de la industria de control de aplicaciones, prevención de intrusiones, protección antimalware y descifrado e inspección TLS/SSL a velocidades multi-gigabit. Los ingenieros de la serie SuperMassive se han centrado sobre todo en el rendimiento, el espacio y la refrigeración, creando el NGFW con el mejor valor de Gbps/vatio de la industria para ofrecer procesamiento de paquetes y datos de alto rendimiento, control de aplicaciones y prevención de intrusiones.

El motor RFDPI de SonicWall escanea todos los bytes de cada paquete en todos los puertos, garantizando no solo una inspección completa del flujo de datos entero, sino también un alto rendimiento y una latencia mínima. Esta tecnología es superior a los diseños proxy que reensamblan el contenido utilizando sockets ligados a programas antimalware que presentan notables ineficiencias y una hiperpaginación excesiva de la memoria del socket, lo cual provoca una elevada latencia, un bajo rendimiento y limitaciones en el tamaño de los archivos. El motor RFDPI inspecciona por completo el contenido para eliminar varias formas de malware antes de que accedan a la red. De esta forma, proporciona protección contra las amenazas en constante evolución — sin limitación alguna del tamaño de archivo, del rendimiento ni de la latencia.

El motor RFDPI ofrece también descifrado e inspección completos del tráfico cifrado mediante TLS/SSL y SSH y de las aplicaciones que no pasan por el proxy, garantizando una protección integral, independiente de la vía de transporte o del protocolo. Analiza en profundidad cada paquete (el encabezado y los datos) en busca de incumplimientos de protocolo, amenazas, ataques de día cero, intrusiones e incluso criterios definidos para detectar y prevenir ataques ocultos en el tráfico cifrado, detener la propagación de infecciones y frustrar las comunicaciones de comando y control (C&C) y la exfiltración de datos. Las normas de inclusión y exclusión proporcionan un control total que permite especificar el tráfico que debe ser sometido al descifrado y a la inspección en base a requisitos legales y/o corporativos específicos.

El análisis del tráfico de aplicaciones permite identificar en tiempo real el tráfico de aplicaciones productivo y no productivo y controlarlo mediante potentes políticas a nivel de aplicaciones. El control de las aplicaciones puede realizarse según usuarios individuales o según grupos y puede combinarse con funciones de planificación y listas de excepciones. Las definiciones de aplicaciones, de prevención de intrusiones y de malware son constantemente actualizadas por el equipo de investigación de amenazas de SonicWall Capture Labs. Además, el avanzado sistema operativo de SonicWall, SonicOS, proporciona herramientas integradas que permiten personalizar el método de identificación y control de las aplicaciones.

**Patentes en EEEUU 7,310,815; 7,600,257; 7,738,380; 7,835,361*

Serie SuperMassive 9000

Ventajas:

- Disfrute de una prevención de brechas completa, con funciones de prevención de intrusiones de alto rendimiento, protección contra malware de baja latencia y sandboxing basado en la nube
- Obtenga funciones completas y granulares de identificación, control y visualización de aplicaciones
- Detecte y bloquee amenazas ocultas con funciones de descifrado e inspección del tráfico cifrado mediante TLS/SSL y SSH, sin problemas de rendimiento
- Escale el rendimiento de la seguridad para centros de datos de 10/40 Gbps
- Adáptese a aumentos de los niveles de servicios y asegúrese de que los servicios y recursos de la red están disponibles y protegidos

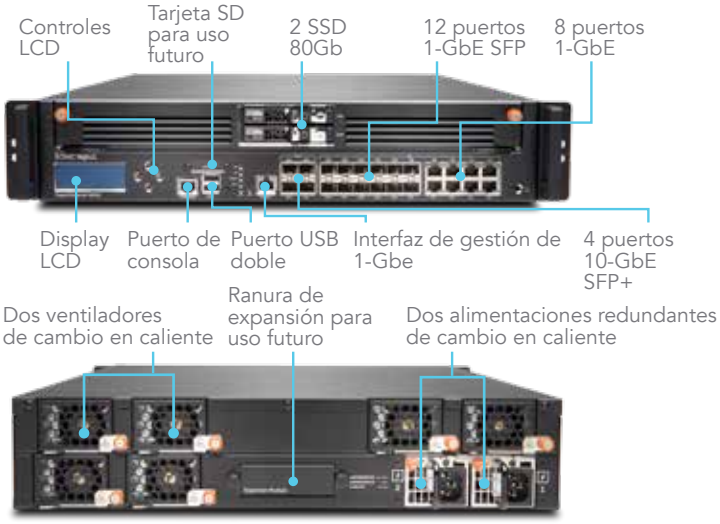
Partner Enabled Services

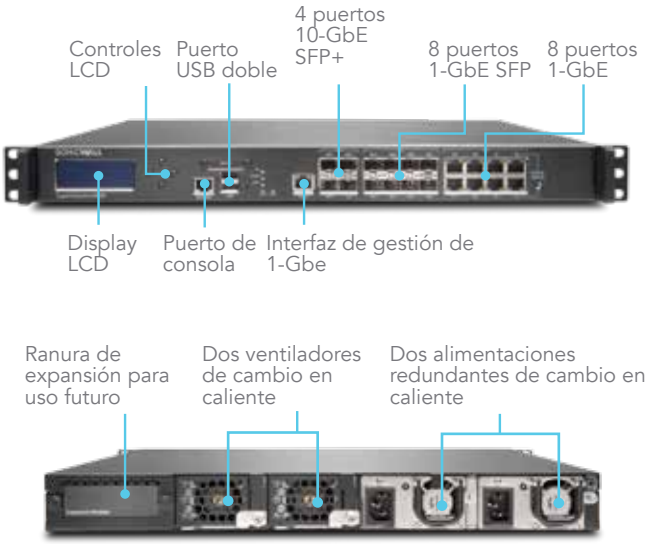
¿Necesita ayuda para planificar, implementar u optimizar su solución SonicWall? Los Partners de servicios avanzados de SonicWall están cualificados para proporcionarle servicios profesionales de clase mundial. Si desea obtener más información, visite www.sonicwall.com/PES.

Visión de conjunto de la serie

La serie SonicWall SuperMassive 9000 incluye 4 puertos 10-GbE SFP+, 12 puertos 1-GbE SFP, 8 puertos 1-GbE de cobre e interfaces de gestión de 1 GbE, con un puerto de expansión para dos interfaces 10-GbE SFP+ adicionales (versión futura). La serie 9000 incluye módulos de ventilador y dos fuentes de alimentación de cambio en caliente.

Serie SuperMassive 9000



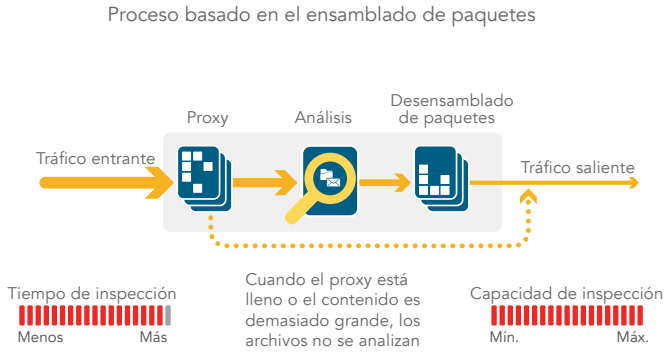


Prestación	9200	9400	9600	9800
Núcleos de procesamiento	24	32	32	64
Rendimiento del firewall	15 Gbps	20 Gbps	20 Gbps	31,8 Gbps
Rendimiento de inspección de aplicaciones	5 Gbps	10 Gbps	11,5 Gbps	23 Gbps
Rendimiento del sistema de prevención de intrusiones (IPS)	5 Gbps	10 Gbps	11,5 Gbps	21,3 Gbps
Rendimiento de inspección antimalware	3,5 Gbps	4,5 Gbps	5 Gbps	11 Gbps
Conexiones DPI máximas	1,5 millones	1,5 millones	2,0 millones	8,0 millones
Modos de implementación	**9200**	**9400**	**9600**	**9800**
Modo L2 bridge	Sí	Sí	Sí	Sí
Modo Wire	Sí	Sí	Sí	Sí
Modo pasarela/NAT	Sí	Sí	Sí	Sí
Modo Tap	Sí	Sí	Sí	Sí
Modo transparente	Sí	Sí	Sí	Sí

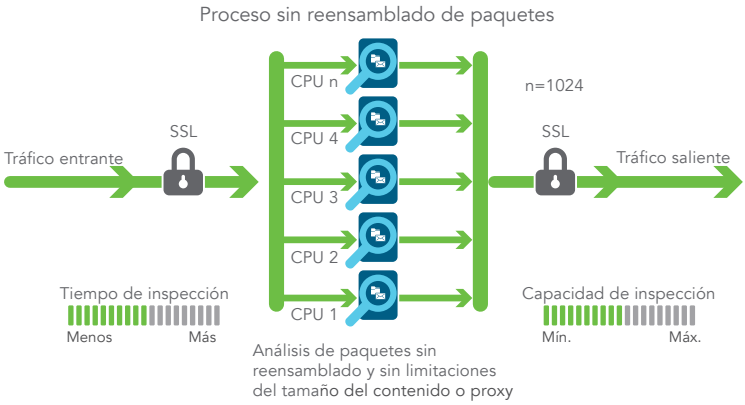
Motor de inspección profunda de paquetes sin reensamblado

La RFDPI 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 ataques de malware y de identificar el tráfico de aplicaciones independientemente del puerto y el protocolo. Este motor propietario se basa en la inspección de la carga útil del tráfico de streaming para detectar amenazas en las capas 3-7. El motor RFDPI somete los flujos de red a amplios y repetidos procesos de normalización y descifrado con el fin de neutralizar las técnicas avanzadas de ofuscación y evasión que pretenden burlar los motores de detección e introducir código malicioso en la red.

Una vez que un paquete ha sido sometido al preprocesamiento necesario, incluido el descifrado TLS/SSL, es analizado con la ayuda de una única representación en memoria propietaria de múltiples bases de datos de definiciones (ataques de intrusión, malware, botnets 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 solo para la inspección o, en el caso de la detección de aplicaciones, para ofrecer servicios de gestión de ancho de banda de capa 7 para el resto del flujo de aplicaciones en cuanto se haya identificado la aplicación.



Arquitectura de la competencia

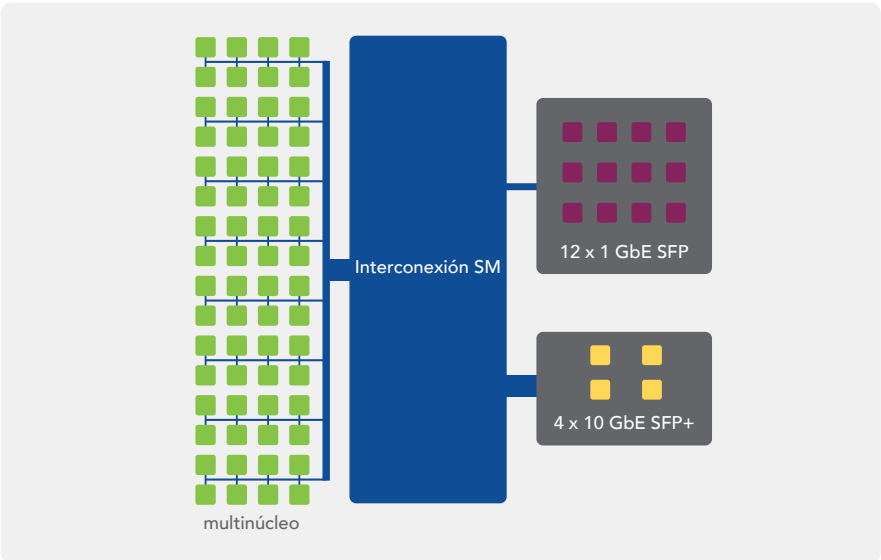


Arquitectura SonicWall

Arquitectura ampliable para máximo rendimiento y escalabilidad

El motor RFDPI está diseñado específicamente con el objetivo de proporcionar un escaneado de seguridad de alto rendimiento para adaptarse a la naturaleza paralela y creciente del tráfico de red. Cuando se combina con sistemas de procesador multinúcleo, esta arquitectura de software centrada en el paralelismo se amplía perfectamente para satisfacer los requisitos de la inspección profunda de paquetes con altas cargas de tráfico. La plataforma SuperMassive se basa en procesadores que, a diferencia de los x86, están optimizados para el procesamiento de paquetes, cifrados y red, a la vez que preservan la flexibilidad y la programación in situ, un punto débil de los sistemas ASIC.

Esta flexibilidad es esencial cuando se requieren nuevas actualizaciones de código y de comportamiento para ofrecer protección contra nuevos ataques que requieren técnicas de detección actualizadas y más sofisticadas. Otro aspecto importante del diseño de esta plataforma es su capacidad exclusiva de establecer nuevas conexiones en cualquier núcleo del sistema, proporcionando el máximo nivel de escalabilidad y permitiendo hacer frente a picos de tráfico. Este enfoque proporciona tasas muy elevadas de establecimiento de sesiones nuevas (conexiones nuevas/seg.) con la inspección profunda de paquetes activada —un parámetro clave que a menudo provoca cuellos de botella en las implementaciones de centros de datos.



SONICWALL®

Capture Labs

El equipo de investigación de amenazas interno y dedicado de SonicWall Capture Labs estudia y desarrolla contramedidas para aplicarlas a los firewalls de los clientes a fin de que éstos gocen de una protección actualizada. El equipo recopila datos sobre amenazas potenciales de diversas fuentes, incluidos nuestro galardonado servicio de sandboxing de red, Capture Advanced Threat Protection, así como más de 1 millón de sensores de SonicWall situados en todo el mundo que monitorizan el tráfico en busca de amenazas emergentes. Los datos se analizan mediante aprendizaje automático utilizando los Algoritmos de aprendizaje profundo de SonicWall para extraer el ADN del código a fin de comprobar si está relacionado con alguna forma conocida de código malicioso.

Los clientes que tienen NGFWs de SonicWall con las últimas prestaciones de seguridad disfrutan de protección contra las amenazas actualizada las 24 horas. Las nuevas actualizaciones tienen efecto inmediato sin necesidad de reiniciar ni interrumpir el sistema. Las definiciones disponibles en los dispositivos protegen contra un amplio abanico de ataques. De hecho, cada una de ellas cubre decenas de miles de amenazas individuales.

Además de las contramedidas residentes en el dispositivo, los firewalls SuperMassive también tienen acceso al servicio de antivirus en la nube (CloudAV[1]) de SonicWall, que amplía la inteligencia de definiciones integrada con decenas de millones de definiciones, cantidad que aumenta en millones todos los años. El firewall accede a la base de datos de CloudAV mediante un protocolo ligero propietario con el fin de reforzar la inspección realizada en el dispositivo.

Con Capture Advanced Threat Protection[1], un sandbox multimotor basado en la nube, las organizaciones pueden examinar archivos y código sospechosos en un entorno aislado para detener las amenazas avanzadas, como los ataques de día cero.

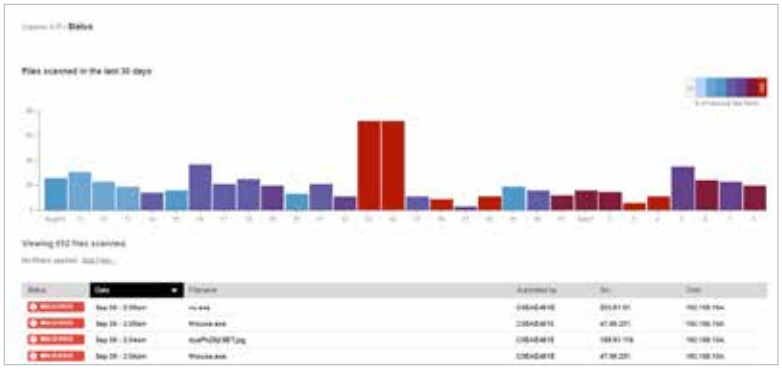
[1] *Requiere suscripción adicional*

Protección contra amenazas avanzadas

SonicWall Capture Advanced Threat Protection Service[1] es 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 para su análisis, con la opción de retenerlos en la pasarela hasta que se emita un veredicto. 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. Cuando se identifica un archivo malicioso, inmediatamente se crea un hash dentro de Capture y más adelante se envía una definición a los firewalls para prevenir 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.

Capture proporciona informes y un cuadro de mando de análisis de amenazas de un solo vistazo con información detallada sobre los resultados del análisis de los archivos enviados al servicio (origen, destino y un resumen con detalles de la acción del malware tras su detonación).



SONICWALL

Inteligencia y control de aplicaciones

La inteligencia de aplicaciones informa a los administradores del tráfico de aplicaciones que atraviesa su red. De esta forma, pueden programar controles basados en las prioridades de negocio, restringir las aplicaciones no productivas y bloquear aquellas que puedan ser potencialmente peligrosas. La visualización en tiempo real identifica anomalías en el tráfico en el momento en que se producen, permitiendo tomar contramedidas inmediatas contra posibles ataques entrantes o salientes o cuellos de botella en el rendimiento.

Los análisis de tráfico de aplicaciones[1] de SonicWall ofrecen información detallada sobre el tráfico de aplicaciones, el uso del ancho de banda y las amenazas para la seguridad, así como potentes funciones de resolución de problemas y análisis forense. Además, el inicio de sesión único (SSO) seguro simplifica la experiencia del usuario, incrementa la productividad y reduce las llamadas al servicio de soporte. El uso de una intuitiva interfaz basada en Web simplifica la gestión del control y la inteligencia de aplicaciones.

Gestión e informes globales

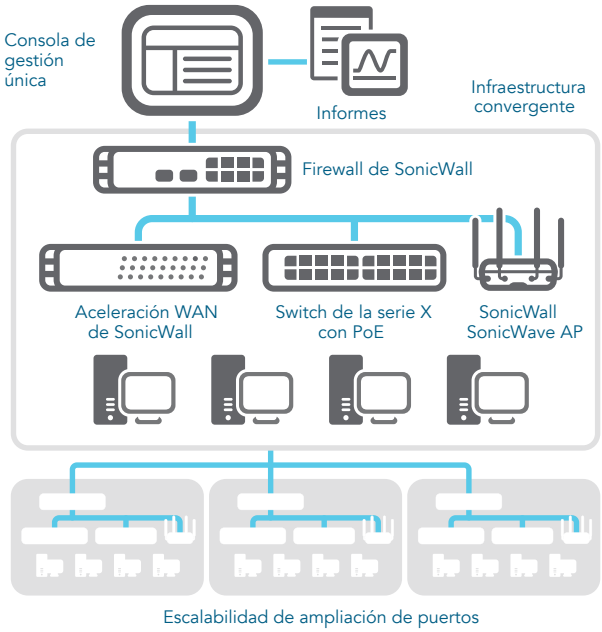
Para organizaciones altamente reguladas que deseen coordinar la seguridad, el control, el cumplimiento normativo y su estrategia de gestión de riesgos, el Sistema de gestión global[1] (GMS®) opcional de SonicWall proporciona a los administradores una plataforma unificada, segura y ampliable para gestionar los firewalls, puntos de acceso inalámbricos y switches de SonicWall mediante un proceso de flujo de trabajo correlacionado y auditable. GMS permite a las empresas consolidar fácilmente la gestión de los dispositivos de seguridad, reducir las complejidades administrativas y de resolución 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. GMS también cumple los requisitos de gestión de cambios del firewall de las empresas gracias a una prestación de automatización del flujo de trabajo. Con la automatización del flujo de trabajo de GMS, todas las empresas ganarán en agilidad y confianza a la hora de implementar las políticas de firewall adecuadas, en el momento oportuno y de conformidad con la normativa vigente.

GMS proporciona una forma coherente de gestionar la seguridad de la red mediante procesos de negocio y niveles de servicio, simplificando drásticamente la gestión del ciclo de vida de sus entornos de seguridad en general, en comparación con la gestión dispositivo por dispositivo.

SonicWall GMS Secure Compliance Enforcement

Ventajas

- Gestión centralizada
- Gestión de políticas sin errores
- Estricto control del acceso
- Seguimiento completo
- Plantillas de informes sobre PCI, HIPAA, SOX
- Menores costes operativos



[1] *Requiere suscripción adicional*

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 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
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)	La serie SuperMassive soporta los modos de alta disponibilidad Activa/Pasiva (A/P) con State Synchronization, DPI Activa/Activa (A/A) y agrupada (clústeres) Activa/Activa. La DPI Activa/Activa desvía la carga de la inspección profunda de paquetes a los núcleos del dispositivo pasivo con el fin de mejorar el rendimiento.
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 el sistema operativo SonicOS 6.2 más reciente, el hardware será compatible con las implementaciones de filtrado y de modo Wire.
Opciones de implementación flexibles	La serie SuperMassive 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. El enrutamiento basado en políticas crea enrutamientos basados en protocolos para direccionar el tráfico a una determinada conexión WAN, con posibilidad de reconexión a una WAN secundaria en caso de fallo de la alimentación.
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 de red individuales y en cascada de la serie Dell X.	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 la serie Dell X.
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.
Autenticación multidominio	Ofrece una forma rápida y sencilla de administrar las políticas de seguridad en todos los dominios de la red. Gestione una política individual para un dominio individual o un grupo de dominios.

Gestión e informes	
Prestación	Descripción
Sistema de gestión global[1] (GMS)	SonicWall GMS supervisa y configura múltiples dispositivos SonicWall, y elabora informes sobre ellos, a través de una única consola de administración con una interfaz intuitiva a fin de reducir los costes de gestión y la complejidad.
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 como SonicWall Scrutinizer u otras compatibles con IPFIX y NetFlow con extensiones.

Prestaciones

Redes privadas virtuales (VPN)	
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 para conectividad entre emplazamientos	La VPN IPSec de alto rendimiento permite a la serie SuperMassive 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/Citrix[1]/Terminal Services[1], 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.
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.

Capture Advanced Threat Protection[1]	
Prestación	Descripción
Sandbox 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.
Bloqueo hasta que haya un veredicto	Permite crear listas personalizadas de países y Botnets para anular etiquetas de país o Botnet erróneas asociadas con una dirección IP.
Análisis de gran variedad de tipos de archivos	Soporta análisis de una amplia variedad de tipos de archivos, como los programas ejecutables (PE), DLL, PDFs, documentos MS Office, archivos, JAR y APK, así como múltiples sistemas operativos, como Windows, Android, Mac OS y entornos multinavegador.
Rápida implementación de definiciones	Cuando se detecta un archivo malicioso, inmediatamente se pone una definición a disposición de los firewalls con suscripción a SonicWall Capture y se envía a las bases de datos de definiciones de GRID 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[1]	
Prestación	Descripción
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico SSL/TLS sobre la marcha, sin necesidad de proxies, en busca de malware, intrusiones y filtraciones de datos, y aplica políticas de control de aplicaciones, URL y contenido para ofrecer protección contra las amenazas ocultas en el tráfico cifrado mediante TLS/SSL. Incluido con las suscripciones de seguridad para todos los modelos.
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[1]	
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 aplican de inmediato sin necesidad de reiniciar ni interrumpir el 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.
Detección y prevención de abusos/anomalías de los protocolos	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.

Prestaciones

Prevención de amenazas[1]	
Prestación	Descripción
Antimalware en pasarela	El motor RFDPI analiza todo el tráfico entrante, saliente y dentro de una misma zona en busca de virus, troyanos, registradores de pulsaciones de teclas y otros tipos de malware en archivos de una longitud y un tamaño ilimitados en todos los puertos y flujos de TCP.
Protección antimalware CloudAV	Los servidores de la nube de SonicWall disponen de una base de datos de 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[1]	
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[1]	
Prestación	Descripción
Filtrado de contenido dentro y fuera	Aplique políticas de usos aceptables y bloquee el acceso a sitios Web que contengan información o imágenes inaceptables o improductivas con Content Filtering Service.
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[1]	
Prestación	Descripción
Protección en varios niveles	Utilice las funciones del firewall, como la primera capa de defensa en el perímetro, junto con la protección de puntos terminales, a fin de bloquear los virus que penetran en la red por medio de portátiles, unidades de memoria flash y otros sistemas no protegidos.
Opción de aplicación automatizada	Asegúrese de que todos los equipos que accedan a la red tengan instalada y activa la versión más reciente de las definiciones antivirus y antispyware. De este modo, eliminará los costes asociados habitualmente a la gestión de soluciones antivirus y antispyware para equipos de escritorio.
Opción de instalación e implementación automatizadas	La implementación y la instalación máquina a máquina de clientes antivirus y antispyware se realiza de forma automática en toda la red, con lo que se minimiza la sobrecarga administrativa.
Protección antivirus automática e ininterrumpida	Las actualizaciones frecuentes de antivirus y antispyware se envían de forma transparente a todos los equipos de escritorio y servidores de archivos para mejorar la productividad de los usuarios finales y reducir las tareas de gestión de la seguridad.
Antivirus de próxima generación	Capture Client utiliza un motor de inteligencia artificial (IA) 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.

[1] *Requiere suscripción adicional*

Visión de conjunto de las prestaciones

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[2]

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

Capture Advanced Threat Protection[2]

- Análisis multimotor basado en la nube
- Sandboxing virtualizado
- Análisis de nivel de hipervisor
- Emulación de sistema completo
- Análisis de gran variedad de tipos de archivos
- Envío automático y manual
- Actualizaciones de inteligencia de amenazas en tiempo real
- Bloqueo hasta que haya un veredicto
- Capture Client

Prevención de intrusiones[2]

- Análisis basado en definiciones
- Actualizaciones automáticas de las definiciones
- Motor de inspección bidireccional
- Conjunto de reglas de IPS detalladas
- Refuerzo de políticas GeoIP
- Filtrado de botnets con lista dinámica
- Coincidencia de expresiones regulares

Anti-malware[2]

- 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[2]

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

Filtrado de contenido Web[2]

- Filtrado de URL
- Puenteo de proxys
- Bloqueo según palabras clave
- Inserción de encabezado HTTP
- Gestión del ancho de banda según categorías 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

- LAG dinámico utilizando LACP
- PortShield
- Jumbo frames
- Descubrimiento de rutas MTU
- Protocolización mejorada
- VLAN trunking
- Duplicación de puertos
- QoS de nivel 2
- Seguridad de puertos
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Controlador inalámbrico SonicWall[1]
- Enrutamiento basado en políticas (ToS/metric y ECMP)
- NAT
- Servidor DHCP
- Gestión del ancho de banda
- Agregación de enlaces (estática y dinámica)
- Redundancia de puertos
- Alta disponibilidad A/P con State Sync
- Agrupación (clústeres) A/A
- Equilibrio de carga entrante/saliente
- Modo puente de capa 2, modo wire/virtual wire, modo tap, modo NAT
- Reconexión WAN 3G/4G (no en SuperMassive 9800)
- Enrutamiento asimétrico
- Compatibilidad con tarjetas Common Access Card (CAC)

Conexión inalámbrica

- WIDS/WIPS
- Análisis de espectro de radiofrecuencia
- Prevención de puntos de acceso no autorizados
- Itinerancia rápida (802.11k/r/v)
- Vista del plano de planta/vista de topología
- Band steering
- Beamforming
- AirTime fairness
- MiFi extender
- Acceso temporal para usuarios invitados
- Portal para invitados LHM

VoIP

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

Gestión y supervisión

- GMS, Web, IU, CLI, APIs REST, SNMPv2/v3
- Protocolización
- Exportaciones NetFlow/IPFIX
- Backup de configuración basado en la nube
- Plataforma de análisis de seguridad de BlueCoat
- Gestión de puntos de acceso de SonicWall
- Gestión de switches de las series Dell N y Dell X[1]

[1] *Prestación no soportada en SuperMassive 9800*
[2] *Requiere suscripción adicional*

SONICWALL®

Especificaciones del sistema de la serie SuperMassive E9000

Firewall general	9200	9400	9600	9800
Sistema operativo	SonicOS			
Núcleos de procesamiento de seguridad	24	32		64
Interfaces	4x10GbE SFP+, 8x1GbE SFP, 8x1GbE, 1GbE gestión, 1 consola			4x10GbE SFP+, 12x1GbE SFP, 8x1GbE, 1GbE gestión, 1 consola
Memoria (RAM)	8 GB	16 GB	32 GB	64 GB
Almacenamiento	Flash			2x 80GB SSD, Flash
Expansión	1 ranura de ampliación (trasera)*, tarjeta SD*			
Gestión	CLI, SSH, GUI, GMS			
Usuarios con SSO	80.000	90.000	100.000	110.000
Número máximo de puntos de acceso soportados	128			-
Protocolización	Analyzer, Local Log, Syslog			
Alta disponibilidad	Activa/Pasiva con State Sync, DPI Activa/Activa con State Sync			
Rendimiento de firewall/VPN	**9200**	**9400**	**9600**	**9800**
Rendimiento de inspección del firewall[1]	15 Gbps	20 Gbps	20 Gbps	31,8 Gbps
Rendimiento de la prevención de amenazas[2]	3 Gbps	4,4 Gbps	4,5 Gbps	10,5 Gbps
Rendimiento de inspección de aplicaciones[2]	5 Gbps	10 Gbps	11,5 Gbps	23 Gbps
Rendimiento de IPS[2]	5 Gbps	10 Gbps	11,5 Gbps	21,3 Gbps
Rendimiento de inspección antimalware[1]	3,5 Gbps	4,5 Gbps	5,0 Gbps	11 Gbps
Rendimiento de IMIX	4,4 Gbps	5,5 Gbps	5,5 Gbps	7,3 Gbps
Rendimiento de inspección y descifrado SSL (DPI SSL)[2]	1,0 Gbps	2,0 Gbps	2,0 Gbps	3,5 Gbps
Rendimiento de VPN[3]	5 Gbps	10 Gbps	11,5 Gbps	14,3 Gbps
Conexiones por segundo	100.000/seg.	130.000/seg.	130.000/seg.	229.000/seg.
Conexiones máximas (SPI)	5,0 millones	7,5 millones	10,0 millones	20,0 millones
Número máximo de conexiones (DPI)	1,5 millones	1,5 millones	2,0 millones	8,0 millones
Conexiones DPI SSL[6] (máximas)	8.000 (15.500[6])	10.000 (17.500[6])	12.000 (22.500[6])	400.000
VPN	**9200**	**9400**	**9600**	**9800**
Túneles VPN entre emplazamientos		10.000		25.000
Clientes VPN IPSec (máximo)	2.000(4.000)	2.000(6.000)	2.000(10.000)	
Clientes SSL VPN NetExtender (máximos)	2 (3.000)	2 (3.000)	50 (3.000)	50 (3.000)
Cifrado/autenticación	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, Suite B, Common Access Card (CAC)			
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14v			
VPN basada en enrutamiento	RIP, OSPF			
Redes	**9200**	**9400**	**9600**	**9800**
Asignación de direcciones IP	Estática, (cliente DHCP, PPPoE, L2TP y PPTP, servidor DHCP interno, relé DHCP[4]			
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT, modo transparente			
Interfaces VLAN	512			
Protocolos de enrutamiento	BGP, OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas, multidifusión			
QoS	Prioridad de ancho de banda, ancho de banda máximo, ancho de banda garantizado, marcado DSCP, 802.1p			
Autenticación	LDAP (multidominios), XAUTH/RADIUS, SSO, Novell, base de datos de usuarios interna, Terminal Services, Citrix,			
VoIP	H323-v1-5 completo, SIP			
Estándares	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certificaciones	UC APL[4], ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2[4], Common Criteria NDPP[4], ICSA Anti-Virus[4]			
Hardware	**9200**	**9400**	**9600**	**9800**
Fuente de alimentación	Dos, redundantes, de cambio en caliente, 300W			Dos, redundantes, de cambio en caliente, 500W
Ventiladores	Dos, redundantes, de cambio en caliente			
Display	Display LED frontal			
Potencia de entrada	100-240 V CA, 50-60 Hz			
Consumo máximo de energía (W)	200			350
MTBF a 25°C en horas	188.719	187.702	186.451	126.144
MTBF a 25°C en años	21,53	21,43	21,28	14,40
Factor de forma	Preparada para montaje en bastidor 1U			Preparada para montaje en bastidor 2U
Dimensiones	43,3x48,5x4,5 cm (17x19,1x1,75 pulgadas)			9x60x43 cm (17x24x3,5 pulgadas)
Peso	8,2 kg (18,1 libras)			18,38 kg (40,5 libras)
Peso WEEE	10,4 kg (23 libras)			22,4 kg (49,5 libras)
Peso de envío	13,3 kg (29,3 libras)			29,64 kg (65 libras)
Conformidad con normas	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/GS, CB, Mexico CoC by UL, WEEE, REACH, ANATEL, BSMI, CU			
Entorno	15-40 ° C			
Humedad	10–90%, sin condensación			

*[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/Gateway AV/Anti-Spyware/IPS medido mediante la prueba de rendimiento HTTP estándar Spirent WebAvalanche y herramientas de prueba Ixia. Para las pruebas se han utilizado múltiples flujos a través de múltiples pares de puertos. Rendimiento de Prevención de amenazas medido con Gateway AV, Anti-Spyware, IPS and Application Control activados. [3] Medición del rendimiento de VPN basada en el tráfico UDP con paquetes de 1280 bytes. [4] Aplicable a SuperMassive 9200, 9400 y 9600. Certificación SuperMassive 9800 UC APL pendiente. [5] Soportado en SonicOS 6.1 y 6.2. [6] Por cada 125.000 conexiones DPI reducidas, la cantidad de conexiones DPI SSL disponibles aumenta en 750. *Uso futuro. Las especificaciones, las prestaciones y la disponibilidad están sujetas a modificaciones.*

SONICWALL®

Información de pedido de la serie SuperMassive 9000

Producto	SKU
SuperMassive 9800 Total Secure Advanced Edition (1 año)	01-SSC-0312
SuperMassive 9600 Total Secure Advanced Edition (3 años)	02-SSC-0410
SuperMassive 9400 Total Secure Advanced Edition (3 años)	02-SSC-0409
SuperMassive 9200 Total Secure Advanced Edition (3 años)	02-SSC-0408
Suscripciones de soporte y seguridad para SuperMassive 9200	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para SuperMassive 9200 (1 año)	01-SSC-1570
Capture Advanced Threat Protection para SuperMassive 9200 (1 año)	01-SSC-1575
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering con soporte para 9200 (1 año)	01-SSC-4172
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization para SuperMassive 9200 (1 año)	01-SSC-4202
Content Filtering Premium Business Edition para 9200 (1 año)	01-SSC-4184
Soporte Platinum para SuperMassive 9200 (1 año)	01-SSC-4178
Suscripciones de soporte y seguridad para SuperMassive 9400	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para SuperMassive 9400 (1 año)	01-SSC-1580
Capture Advanced Threat Protection para SuperMassive 9400 (1 año)	01-SSC-1585
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering con soporte para 9400 (1 año)	01-SSC-4136
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization para SuperMassive 9400 (1 año)	01-SSC-4166
Content Filtering Premium Business Edition para 9400 (1 año)	01-SSC-4148
Soporte Platinum para SuperMassive 9400 (1 año)	01-SSC-4142
Suscripciones de soporte y seguridad para SuperMassive 9600	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para SuperMassive 9600 (1 año)	01-SSC-1590
Capture Advanced Threat Protection para SuperMassive 9600 (1 año)	01-SSC-1595
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering con soporte para 9600 (1 año)	01-SSC-4100
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization para SuperMassive 9600 (1 año)	01-SSC-4130
Content Filtering Premium Business Edition para 9600 (1 año)	01-SSC-4112
Soporte Platinum para SuperMassive 9600 (1 año)	01-SSC-4106
Suscripciones de soporte y seguridad para SuperMassive 9800	**SKU**
Advanced Gateway Security Suite Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para SuperMassive 9800 (1 año)	01-SSC-1183
Capture Advanced Threat Protection para SuperMassive 9800 (1 año)	01-SSC-1188
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering con soporte para 9800 (1 año)	01-SSC-0809
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization para SuperMassive 9800 (1 año)	01-SSC-0827
Content Filtering Premium Business Edition para 9800 (1 año)	01-SSC-0821
Soporte Gold 24x7 para SuperMassive 9800 (1 año)	01-SSC-0815
Módulos y accesorios*	**SKU**
Ventilador de sistema FRU para la serie SonicWall SuperMassive 9800	01-SSC-0204
Alimentación CA FRU para la serie SonicWall SuperMassive 9800	01-SSC-0203
Ventilador de sistema FRU para la serie SonicWall SuperMassive 9000	01-SSC-3876
Alimentación CA FRU para la serie SonicWall SuperMassive 9000	01-SSC-3874
Módulo de corto alcance 10GBASE-SR SFP+	01-SSC-9785
Módulo de largo alcance 10GBASE-LR SFP+	01-SSC-9786
Módulo de corta distancia 1000BASE-SX SFP	01-SSC-9789
Módulo de larga distancia 1000BASE-LX SFP	01-SSC-9790
Módulo de cobre 1000BASE-T SFP	01-SSC-9791
Gestión e informes	**SKU**
Licencia de software para SonicWALL GMS de 10 nodos	01-SSC-3363
Soporte de software E-Class 24x7 de 10 nodos para SonicWall GMS (1 año)	01-SSC-6514
Dispositivo virtual SonicWall Scrutinizer con licencia de software para el módulo Flow Analytics, hasta 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-3443
SonicWall Scrutinizer con licencia de software para el módulo Flow Analytics, hasta 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-4002
SonicWall Scrutinizer con licencia de software para el módulo Advanced Reporting, hasta 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-3773

**Si desea obtener una lista completa de los módulos SFP y SFP+ soportados, consulte a un ingeniero de ventas de SonicWall.*

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.

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

Datasheet-SuperMassive-US-VG-MKTG4043