SONICWALL

Serie SuperMassive de SonicWall

Firewall de nueva generación de altas prestaciones y seguridad para grandes redes empresariales

La serie SuperMassive de SonicWall es la plataforma de firewall de nueva generación de SonicWall diseñada para que las grandes redes ofrezcan escalabilidad, fiabilidad y seguridad profunda a velocidades de varios gigabits con una latencia casi nula.

Creada para satisfacer las necesidades de las empresas, los gobiernos, los centros educativos, los minoristas, las instituciones sanitarias y los proveedores de servicios, la serie SuperMassive es ideal para asegurar las redes empresariales distribuidas, los centros de datos y los proveedores de servicios.

La serie SuperMassive 9000, que combina el sistema operativo SonicOS de SonicWall, la tecnología patentada* Reassembly-Free Deep Packet Inspection® (RFDPI) y una arquitectura de hardware masivamente multinúcleo y altamente escalable, ofrece control de aplicaciones, prevención de intrusiones, protección contra *malware* y un sistema de descifrado e inspección TLS/SSL líderes en el sector a velocidades de varios gigabits. La serie SuperMassive se ha diseñado con esmero teniendo en cuenta la potencia, el espacio y la refrigeración (PSC), proporcionando el firewall de nueva generación de Gbps/vatio líder del sector para el procesamiento de paquetes y datos de alto rendimiento, el control de aplicaciones y la prevención de amenazas.

El motor RFDPI de SonicWall escanea cada byte de cada paquete en todos los puertos, por lo que ofrece una inspección completa del contenido de todo el flujo, al tiempo que proporciona un alto rendimiento y una baja latencia. Esta tecnología es superior a los proxies que reensamblan el contenido utilizando sockets vinculados a programas *antimalware*, que están llenos de ineficacias y con sobrecarga de la memoria de los sockets, lo que conlleva a una alta latencia, bajo rendimiento y limitaciones en el tamaño de los archivos. El motor RFDPI inspecciona a fondo el contenido para eliminar las diversas formas de *malware* antes de que entren en la red y protege contra las amenazas más avanzadas, sin limitaciones de tamaño de archivo, rendimiento o latencia.

El motor RFDPI también realiza el descifrado y la inspección completos del tráfico cifrado TLS/SSL y SSH, así como de las aplicaciones no proxy, permitiendo una protección completa independientemente del transporte o el protocolo. Busca dentro de cada paquete (en la cabecera y los datos) vulneraciones de protocolos, amenazas, ataques de día cero, intrusiones e incluso criterios definidos para detectar y prevenir los ataques ocultos en el tráfico cifrado, detener la propagación de las infecciones y frustrar la exfiltración de las comunicaciones y de los datos de comando y control. Las normas de inclusión y exclusión proporcionan un control total que permite personalizar qué tráfico debe ser sometido al descifrado y a la inspección en función de requisitos legales y/o corporativos específicos.

El análisis del tráfico de las aplicaciones permite diferenciar en tiempo real el tráfico productivo del improductivo de aplicaciones y controlarlo a través de potentes políticas a nivel de aplicación. El control de aplicaciones se puede hacer tanto por usuarios como por grupos, junto con los calendarios y las listas de excepciones. El equipo de detección de amenazas de SonicWall Capture Labs actualiza continuamente todas las definiciones de aplicaciones, prevención de intrusiones y *malware*. Además, SonicOS, un avanzado sistema operativo concebido expresamente, incorpora herramientas que permiten la identificación y el control de aplicaciones personalizadas.

Serie SuperMassive 9000

Ventajas:

- Disfrute de una prevención de problemas de seguridad completa que incluye prevención de intrusiones de alto rendimiento, protección contra *malware* de baja latencia y *sandboxing* basado en la nube
- Obtenga identificación, control y visualización de aplicaciones exhaustivos
- Detecte y bloquee amenazas ocultas gracias al descifrado y la inspección del tráfico cifrado TLS/SSL y SSH, sin problemas de rendimiento.
- Aumente el rendimiento de la seguridad para centros de datos de 10/40 Gbps
- Adáptese a las mejoras de nivel de servicio y asegúrese de que los servicios y recursos de red estén disponibles y protegidos

Servicios habilitados por partners

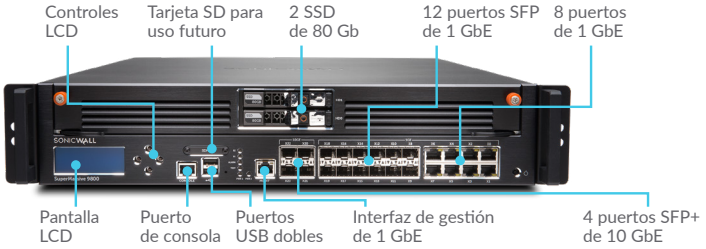
¿Necesita ayuda para planificar, desplegar u optimizar su solución de SonicWall? Los **partners** de servicios avanzados de SonicWall están formados para prestarle servicios profesionales de primera clase. Obtenga más información en www.sonicwall.com/PES.

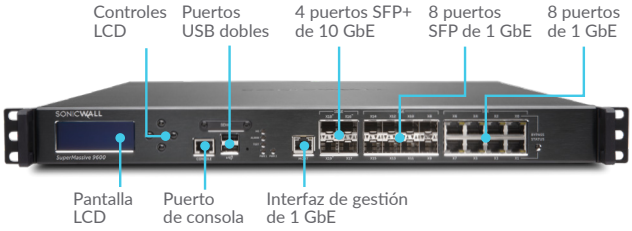
* Patentes Patentes 7.310.815; 7.600.257; 7.738.380; 7.835.361

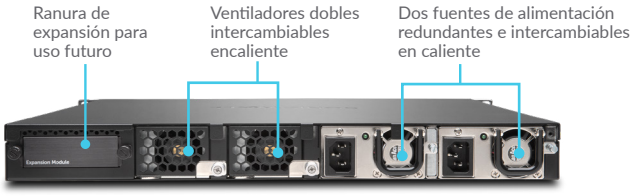
Características de la serie

La serie SuperMassive 9000 de SonicWall cuenta con cuatro SFP+ de 10 GbE, hasta 12 SFP de 1 GbE, 8 puertos de cobre de 1 GbE y de gestión de 1 GbE, con un puerto de expansión para disponer de otros dos SFP+ de 10 GbE (próximamente). La Serie 9000 cuenta con módulos de ventilador intercambiables en caliente y fuentes de alimentación.

Serie SuperMassive 9000





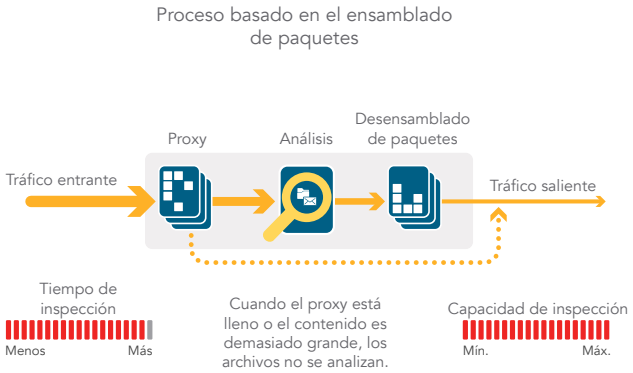


CAPACIDAD	9200	9400	9600	9800
Núcleos de procesamiento	24	32	32	64
Rendimiento del firewall	15 Gbps	20 Gbps	20 Gbps	31,8 Gbps
Rendimiento de inspección de aplicaciones	5 Gbps	10 Gbps	11,5 Gbps	23 Gbps
Rendimiento del sistema de prevención de intrusiones (IPS)	5 Gbps	10 Gbps	11,5 Gbps	21,3 Gbps
Rendimiento de inspección *antimalware*	3,5 Gbps	4,5 Gbps	5 Gbps	11 Gbps
Máximo de conexiones DPI	1,5 M	1,5 M	2,0 M	8,0 M
MODOS DE IMPLEMENTACIÓN	**9200**	**9400**	**9600**	**9800**
Modo puente L2	Sí	Sí	Sí	Sí
Modo cable	Sí	Sí	Sí	Sí
Modo Gateway/NAT	Sí	Sí	Sí	Sí
Modo Tap	Sí	Sí	Sí	Sí
Modo Transparente	Sí	Sí	Sí	Sí

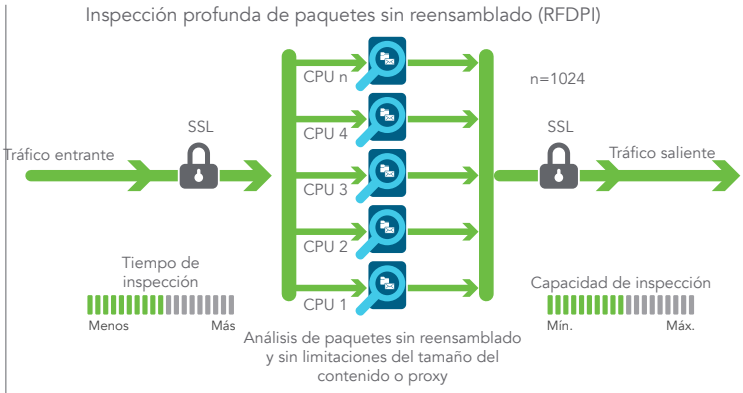
Motor de inspección profunda de paquetes sin reensamblado

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 descargas de *malware* y de identificar el tráfico de aplicaciones independientemente del puerto y el protocolo. Este motor propietario detecta las amenazas en las Capas 3-7 analizando las cargas útiles del tráfico. El motor de RFDPI somete los flujos de red a amplios y repetidos procesos de normalización y descifrado con el fin de neutralizar las técnicas avanzadas de evasión y confusión que pretenden burlar los motores de detección e introducir código malicioso en la red.

Una vez que un paquete pasa el preprocesamiento necesario, incluido el descifrado TLS/SSL, es analizado con la ayuda de una única representación en memoria propietaria de 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 para realizar únicamente la inspección o, en caso de detección de aplicaciones, para proporcionar servicios de gestión de ancho de banda de capa 7 para el resto del flujo de aplicaciones tan pronto como se identifique una aplicación.



Arquitectura competitiva basada en proxy (competencia)

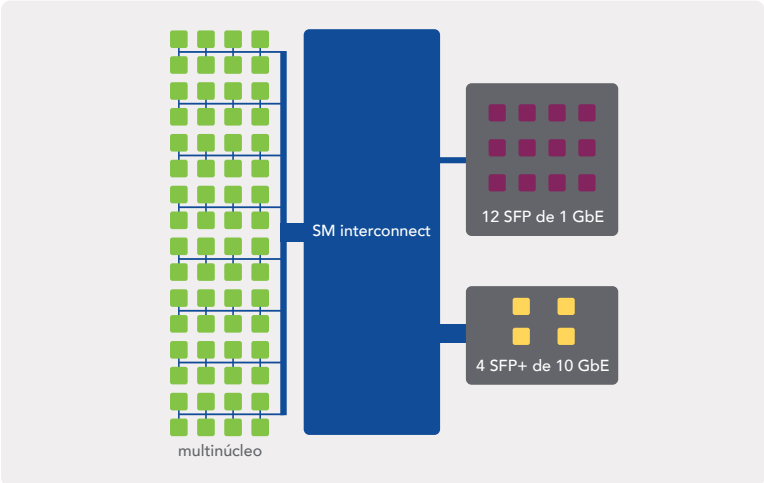


Arquitectura basada en flujos de SonicWall

Arquitectura extensible para una escalabilidad y un rendimiento extremos

El motor RFDPI está específicamente diseñado para proporcionar un análisis de seguridad de alto rendimiento, adaptándose así a la naturaleza inherentemente paralela y el siempre creciente del tráfico de la red. Cuando se combina con sistemas de procesadores multinúcleo, esta arquitectura de software centrada en el paralelismo se amplía para hacer frente a las demandas de la Inspección Profunda de Paquetes (DPI) en grandes cargas de tráfico. La plataforma SuperMassive utiliza procesadores que, a diferencia de x86, están optimizados para el procesamiento de paquetes, la criptografía y las redes, con lo que mantienen la flexibilidad y la programabilidad en el terreno, un punto flaco de los sistemas ASIC.

Esta flexibilidad es esencial cuando se necesita actualizar los códigos y comportamientos para protegerse de los nuevos ataques que exigen técnicas de detección modernas y más sofisticadas. Otro aspecto que destaca de la plataforma es su capacidad única de establecer nuevas conexiones en cualquier núcleo del sistema, lo que proporciona una escalabilidad insuperable y la capacidad de afrontar los picos de tráfico. Esta característica ofrece velocidades de establecimiento de nuevas sesiones (nueva conexión/segundo) extremadamente altas mientras que se habilita la Inspección Profunda de Paquetes, un indicador clave que a menudo supone un cuello de botella para las implementaciones de centros de datos.

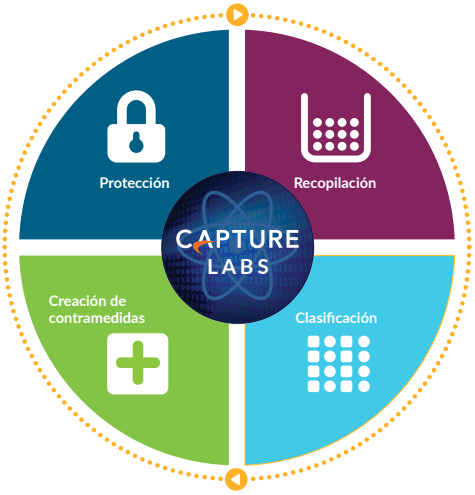


Capture Labs

El equipo de detección de amenazas de SonicWall Capture Labs investiga y desarrolla medidas para instaurar en los firewalls de los clientes la protección más moderna. El equipo recopila datos de amenazas potenciales de diversas fuentes, como 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 nuevas amenazas. El análisis se realiza mediante *machine learning* (aprendizaje automático) con ayuda de los algoritmos de aprendizaje profundo de SonicWall, que extraen el ADN del código para ver si está relacionado con algún tipo de código malicioso.

Los clientes de los firewalls de nueva generación de SonicWall con las prestaciones de seguridad más modernas se benefician de una protección contra amenazas siempre actualizada las 24 horas del día. Las nuevas actualizaciones tienen efecto inmediato sin necesidad de reiniciar ni interrumpir el sistema. Las definiciones de los dispositivos ofrecen protección contra una amplia variedad de tipos de ataques, cubriendo decenas de miles de amenazas individuales con una sola definición.

Además de las contramedidas integradas en el dispositivo, los firewalls SuperMassive también tienen acceso a SonicWall CloudAV[1], que incluye decenas de millones de definiciones y aumenta varios millones cada año. El firewall accede a esta base de datos CloudAV a través de un protocolo propietario y ligero para profundizar la inspección realizada en el dispositivo. Con Capture Advanced Threat Protection[1], un *sandbox* multi-motor en la nube, las organizaciones pueden analizar archivos y código sospechosos en un entorno aislado para neutralizar amenazas avanzadas como los ataques de día cero.



[1] *Requiere suscripción adicional*

Protección contra amenazas avanzadas

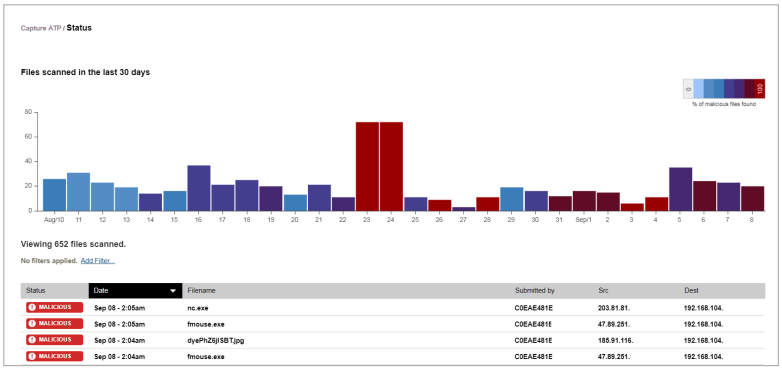
La prevención de infracciones automatizada y en tiempo real de SonicWall se basa en dos tecnologías avanzadas de detección de malware: Capture Advanced Threat Protection™ (Capture ATP) y Capture Security appliance™ (CSa).

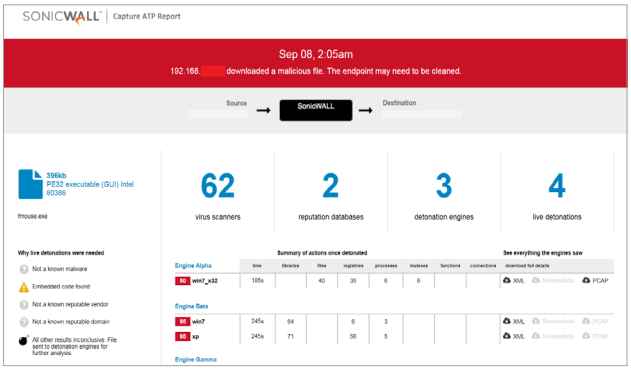
Capture ATP es una plataforma de *sandbox* multi-motor en la nube, que incluye Real-Time Deep Memory Inspection™ (RTDMI), *sandboxing* virtualizado, emulación completa de sistema y tecnología de análisis a nivel hipervisor. CSa es un dispositivo local equipado con RTDMI, que utiliza técnicas estáticas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

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

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

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

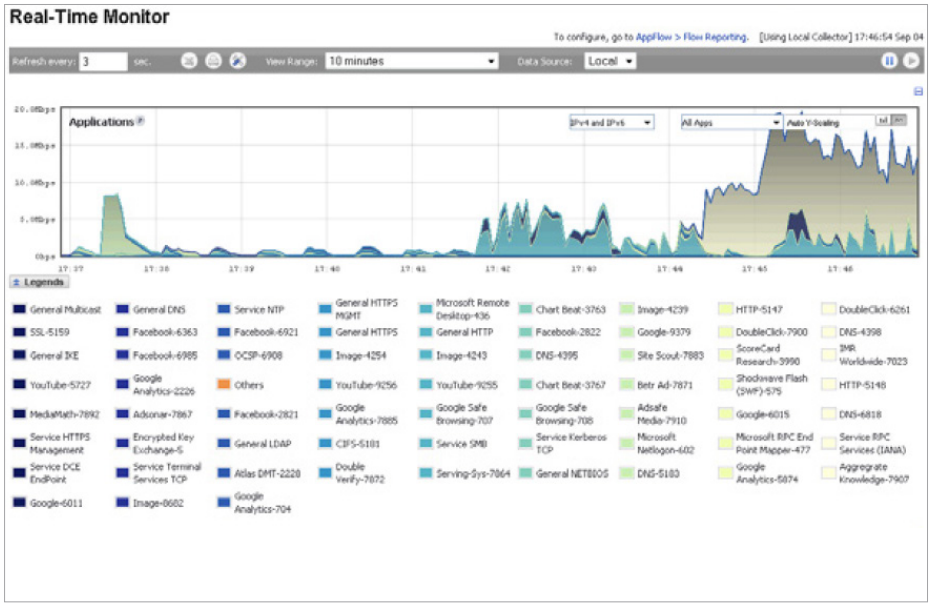




Inteligencia y control de aplicaciones

La Inteligencia de Aplicaciones informa a los administradores del tráfico de aplicaciones que atraviesa la red para que puedan programar los controles necesarios según la prioridad de la empresa, neutralizar las aplicaciones improductivas y bloquear las potencialmente peligrosas. La Visualización en Tiempo Real identifica las anomalías del tráfico justo cuando se producen, lo que permite contrarrestar inmediatamente los ataques entrantes o salientes o los cuellos de botella que frenan el rendimiento.

SonicWall Application Traffic Analytics1 ofrece una visión transparente del tráfico de aplicaciones, del uso del ancho de banda y de las amenazas de seguridad, así como potentes prestaciones de análisis forenses y resolución de problemas. Además, el Inicio de Sesión Único seguro (SSO) facilita la experiencia del usuario, aumenta la productividad y reduce las llamadas al servicio técnico. La gestión de la inteligencia y el control de aplicaciones es más fácil gracias a una intuitiva interfaz web.



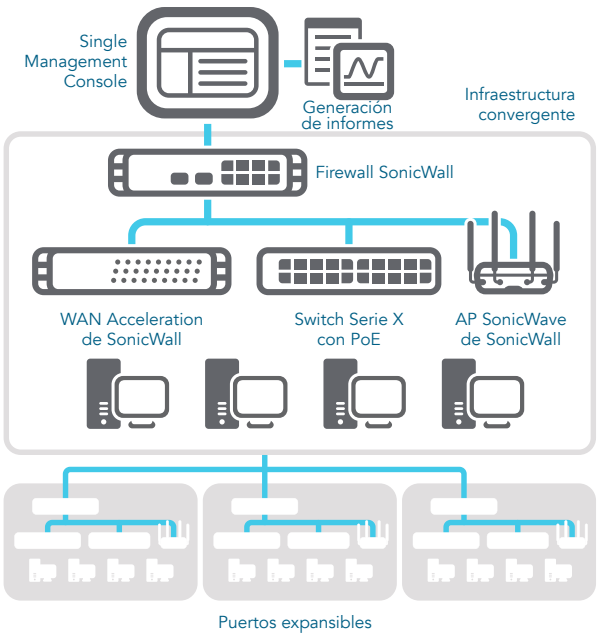
Elaboración de informes y gestión global

Para organizaciones altamente reguladas que deseen coordinar la seguridad, el control, el cumplimiento normativo y su estrategia de gestión de riesgos, la solución opcional SonicWall Global Management System[1] (GMS®) proporciona a los administradores una plataforma unificada, segura y ampliable para gestionar los firewalls, puntos de acceso inalámbricos y switches 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 solución de problemas, y controlar todos los aspectos operativos de la infraestructura de seguridad, como la gestión y la aplicación centralizadas de políticas, la supervisión de eventos en tiempo real, las actividades de los usuarios, la identificación de aplicaciones, los análisis de flujos y forenses, los informes de cumplimiento y de auditorías, entre otras funciones. GMS también cumple los requisitos de gestión de cambios del firewall de las empresas mediante una función de automatización del flujo de trabajo. Con la automatización de flujos de trabajo de GMS, todas las empresas ganan agilidad y confianza a la hora de aplicar políticas de firewalls correctas, en el momento adecuado y de conformidad con las leyes. GMS ofrece una forma coherente de gestionar la seguridad de la red por procesos empresariales y niveles de servicio. Simplifica enormemente la gestión del ciclo de vida de sus entornos de seguridad en comparación con gestionar cada dispositivo de forma individual.

SonicWall GMS Secure Compliance Enforcement

Ventajas

- Gestión centralizada
- Gestión de políticas sin errores
- Control de acceso sólido
- Pistas de auditoría exhaustivas
- Plantillas de informes PCI, HIPAA, SOX
- Menos costes de funcionamiento



[1] *Requiere suscripción adicional*

Prestaciones

MOTOR RFDPI

Función	Descripción
Inspección profunda de paquetes sin reensamblado (RFDPI)	Este motor de inspección de alto rendimiento patentado y propietario realiza análisis bidireccionales del tráfico basados en flujos sin almacenamiento en búfer ni proxies a fin de descubrir posibles intentos de intrusión o ataques de *malware* y de identificar el tráfico de aplicaciones independientemente del puerto.
Inspección bidireccional	Escanea el tráfico entrante y saliente de forma simultánea en busca de amenazas con el fin de evitar que la red se utilice para la distribución de *malware* o se convierta en una plataforma de lanzamiento de ataques en el caso de que se introduzca un equipo infectado.
Inspección basada en flujos	La tecnología de inspección sin proxy ni búfer proporciona un rendimiento DPI de latencia ultrabaja para millones de flujos de red simultáneos sin limitaciones de tamaño de archivos ni flujos, y puede aplicarse a protocolos comunes y a flujos de TCP sin procesar.
Altamente paralelo y escalable	El diseño único del motor RFDPI, en combinación con la arquitectura multinúcleo, proporciona un rendimiento DPI elevado y tasas de establecimiento de sesiones nuevas extremadamente altas para hacer frente a los picos de tráfico de las redes más exigentes.
Inspección de paso único	La arquitectura DPI de paso único escanea el tráfico simultáneamente para la detección de *malware* y de intrusiones y para la identificación de aplicaciones, reduciendo drásticamente la latencia de la DPI y garantizando la correlación de toda la información sobre las amenazas en una única arquitectura.

FIREWALLS Y REDES

Función	Descripción
API 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 admite los modos de alta disponibilidad Activa/Pasiva (A/P) con sincronización de estado, DPI Activa/Activa (A/A) y agrupación (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 DOS mediante el uso de tecnologías de creación 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 IPv6	La versión 6 del protocolo de Internet (IPv6) se encuentra en las primeras fases para sustituir a IPv4. Con el último SonicOS 6.2, 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. Enrutamiento basado en políticas crea rutas basadas en un protocolo para dirigir el tráfico a la conexión WAN preferida con posibilidad de relevar a una WAN secundaria en caso de interrupción.
Calidad de Servicio (QoS) avanzada	Garantiza las comunicaciones críticas con etiquetado 802.1p y DSCP y reasignación 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 las series X de Dell.	Gestione los ajustes de seguridad de los puertos adicionales, incluidos Portshield, HA, POE y POE+, desde una única consola utilizando el panel de gestión del firewall para el *switch* de red de la serie X de Dell.
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 simple y rápida de administrar las políticas de seguridad en todos los dominios de la red. Administre la política individual a un solo dominio o grupo de dominios.

GESTIÓN E INFORMES

Función	Descripción
Global Management System[1] (GMS)	SonicWall GMS monitoriza, configura e informa sobre múltiples dispositivos SonicWall a través de una única consola de gestión con una interfaz intuitiva, por lo que reduce los costes y la complejidad de la gestión.
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)

Función	Descripción
VPN con aprovisionamiento automático	Simplifica y reduce al máximo la complejidad de las implementaciones de firewalls 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 correos electrónicos, archivos, ordenadores, sitios Intranet y aplicaciones desde una variedad de plataformas.
Pasarela VPN redundante	Al utilizarse múltiples WAN, 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 *endpoints* puede redireccionarse fácilmente a través de rutas alternativas.

RECONOCIMIENTO DE CONTENIDO/CONTEXTUAL

Función	Descripción
Seguimiento de la actividad de los usuarios	Gracias a la integración fluida de las funciones de SSO con AD/LDAP/Citrix1/Terminal Services1, en combinación con la amplia información proporcionada por la DPI, es posible identificar a los usuarios y sus actividades.
GeoIP – Identificación del tráfico en base al país	Identifica y controla el tráfico de red dirigido a, o procedente de, países determinados para ofrecer protección contra ataques de amenazas de origen conocido o sospechoso, o para investigar el tráfico sospechoso originado en la red. Permite crear listas personalizadas de países y *botnets* para anular etiquetas de país o *botnet* erróneas asociadas con una dirección IP.
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]

Función	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 a 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, PDF, documentos MS Office, archivos, JAR y APK, así como múltiples sistemas operativos, como Windows, Android, Mac OS X y entornos multinavegador.
Rápida implementación de definiciones	Cuando se detecta un archivo malicioso, inmediatamente se pone una definición a disposición de los firewalls con suscripciones 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 *endpoints*, 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 *endpoints*.

CAPTURE SECURITY APPLIANCE (CSa)

Función	Descripción
Detección de *malware* centrada en las normas	Analice los archivos sospechosos en su propio entorno sin enviar archivos ni resultados a una nube de terceros.
Integraciones incorporadas	CSa se puede integrar de inmediato con otras soluciones de seguridad (firewalls y seguridad de correo electrónico) de SonicWall.
Protección en tiempo casi real	La tecnología RTDMI patentada de SonicWall detecta rápidamente el *malware*, incluso el desconocido hasta el momento, para que CSa lo bloquee hasta el momento en que los firewalls de próxima generación de SonicWall emitan su veredicto.
Implementación	CSa puede configurarse en una red privada conectada directamente a un firewall de vértice singular o ser accesible directamente a través de Internet o mediante VPN por medio de firewalls de oficina.

PREVENCIÓN DE AMENAZAS CIFRADAS[1]

Función	Descripción
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico cifrado mediante 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 lasamenazas 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]

Función	Descripción
Protección basada encontramedidas	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 delas 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 surten efecto en el acto, sin que sea necesario reiniciar los sistemas ni interrumpir su servicio.
Protección IPS entre zonas	Refuerza la seguridad interna al segmentar la red en múltiples zonas de seguridad con prevención de intrusiones para evitar lapropagación de las amenazas de unas zonas a otras.

Prestaciones

PREVENCIÓN DE INTRUSIONES[1] (CONT.)	
Detección y bloqueo de actividades de comando y control (CnC) procedente deataques *botnets*	Identifica y bloquea el tráfico de comando y control originado en *bots* de la red local y dirigido a IP y dominios identificados como propagadores de *malware* o conocidos como puntos de CnC.
Detección y prevención de infracción de protocolos yanomalías	Identifica y bloquea ataques que abusan de los protocolos para intentar eludir el IPS.
Protección de día cero	Protege la red ante los ataques de día cero con actualizaciones constantes contra los últimos métodos y técnicas de *exploits*, que cubren miles de *exploits* individuales.
Tecnología antievasión	La amplia normalización de flujos, la descodificación y otras técnicas impiden que las amenazas puedan penetrar la red sin ser detectadas utilizando técnicas de evasión en las capas 2-7.

PREVENCIÓN DE AMENAZAS[1]	
Función	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 contra el *malware* 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]	
Función	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]	
Función	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]	
Función	Descripción
Protección en varios niveles	Utilice las funciones del firewall, como la primera capa de defensa en el perímetro, junto con la protección de *endpoints*, 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 instaladas y activas las definiciones de antivirus y antiespía más recientes. De este modo, eliminará los costes asociados habitualmente a la gestión de soluciones antivirus para equipos de escritorio.
Opción de instalación e implementación automatizadas	La implementación y la instalación máquina a máquina de clientes antivirus y antispyware se realiza de forma automática en toda la red, con lo que se minimiza la sobrecarga administrativa.
Protección contra virus: automática y siempre activa	Las frecuentes actualizaciones de antivirus y antiespía se instalan de forma transparente en todos los ordenadores de sobremesa y servidores de archivos para mejorar la productividad del usuario final y reducir la gestión de seguridad.
Antivirus de próxima generación	Capture Client utiliza un motor de inteligencia artificial estático para determinar las amenazas antes de que puedan ejecutarse y regresar a un estado previo a la infección.
Protección *antispyware*	La potente función de protección *antispyware* analiza y bloquea la instalación de un completo conjunto de programas de *spyware* en equipos de escritorio y portátiles antes de que éstos transmitan datos confidenciales, lo que contribuye a aumentar la seguridad y el rendimiento de los equipos de escritorio.

[1] *Requiere suscripción adicional*

Resumen de características

Firewall

- Inspección dinámica de paquetes
- Inspección profunda de paquetes sin reensamblado
- Protección contra ataques DDoS (inundaciones UDP/ICMP/SYN)
- Soporte para IPv4/IPv6
- Autenticación biométrica para el acceso remoto
- Proxy DNS
- API 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
- Aplicación de políticas GeoIP
- Filtrado de botnets con lista dinámica
- Coincidencia de expresiones regulares

Antimalware[2]

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

Identificación de aplicaciones[2]

- Control de aplicaciones
- Visualización del tráfico de las 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 mediante NetFlow/IPFIX
- Seguimiento de la actividad de los usuarios(SSO)
- Completa base de datos de definiciones deaplicaciones

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 categoríasCFS
- 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

- Dynamic LAG usando LACP
- PortShield
- Estructuras Jumbo
- Descubrimiento de ruta MTU
- Protocolización mejorada
- Enlace troncal VLAN
- Duplicación de puertos
- QoS de nivel 2
- Seguridad de puertos
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Controlador inalámbrico de SonicWall
- Enrutamiento basado en políticas (ToS/métrica y ECMP)
- NAT
- Servidor DHCP
- Gestión del ancho de banda
- Agregación de enlaces (estáticos y dinámicos)
- Redundancia de puertos
- Alta disponibilidad A/P con sincronización de estado
- Agrupación A/A
- Equilibrio de carga entrante/saliente
- Puente L2, modo cable/cable virtual, modo detoma de corriente, modo NAT
- Reconexión WAN 3G/4G (no en SuperMassive 9800)
- Enrutamiento asimétrico
- Compatibilidad con tarjetas Common Access Card (CAC)

Conexión inalámbrica

- WIDS/WIPS
- Análisis del espectro RF
- Prevención de access *points* no autorizados
- Itinerancia rápida (802.11k/r/v)
- Vista de planta/vista de topología
- *Band steering* (direccionamiento de banda)
- *Beamforming* (conformación de haces)
- AirTime Fairness (equidad de conexión)
- 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, UI, CLI, API REST, SNMPv2/v3
- Protocolización
- Exportaciones NetFlow/IPFIX
- Backup de configuración basado en la nube
- Plataforma de análisis de seguridad de BlueCoat
- Gestión de access *points* de SonicWall
- Gestión de *switches* de la serie N y la serie X de Dell[1]

[1] *No admitido en SuperMassive 9800*
[2] *Requiere suscripción adicional*

Especificaciones del sistema de la serie SuperMassive 9000

FIREWALL GENERAL	9200	9400	9600	9800
Sistema operativo	SonicOS			
Núcleos de procesamiento de seguridad	24	32		64
Interfaces	4 SFP+ de 10 GbE , 8 SFP de 1 GbE, 8 de 1 GbE, Gestión 1 GbE, 1 Consola			4 SFP+ de 10 GbE , 12 SFP de 1 GbE, 8 de 1 GbE, Gestión 1 GbE, 1 Consola
Memoria (RAM)	8 GB	16 GB	32 GB	64 GB
Almacenamiento	Flash			2 SSD de 80 GB, Flash
Expansión	1 ranura de expansión (trasera)*, tarjeta SD*			
Gestión	CLI, SSH, GUI, GMS			
Usuarios de SSO	80.000	90.000	100.000	110.000
Máximo de access points admitidos	128			-
Protocolización	Analizador, Registro local, Registro del sistema			
Alta disponibilidad	DPI Activo/Pasivo con sincronización de estado/DPI Activo/Activo con sincronización de estado			
RENDIMIENTO DE FIREWALL/VPN	**9200**	**9400**	**9600**	**9800**
Velocidad de inspección del firewall[1]	15 Gbps	20 Gbps	20 Gbps	31,8 Gbps
Rendimiento de prevención de amenazas[2]	3 Gbps	4,4 Gbps	4,5 Gbps	10,5 Gbps
Velocidad 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
Velocidad de inspección de antimalware[1]	3,5 Gbps	4,5 Gbps	5,0 Gbps	11 Gbps
Rendimiento IMIX	4,4 Gbps	5,5 Gbps	5,5 Gbps	7,3 Gbps
Velocidad 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/s	130.000/s	130.000/s	229.000/s
Número máximo de conexiones (SPI)	5.0M	7.5M	10.0M	20.0M
Número máximo de conexiones (DPI)	1,5 M	1,5 M	2.0M	8.0M
Conexiones DPI SSL[6] (máximo)	8.000 (15.500[6])	10.000 (17.500[6])	12.000 (22.500[6])	650.000
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 (máximo)	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 (IP solapadas), PAT, modo transparente			
Interfaces VLAN	512			
Protocolos de enrutamiento	BGP, OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas, multicast			
QoS	Prioridad de ancho de banda, ancho de banda máximo, ancho de banda garantizado, marcado DSCP, 802.1p			
Autenticación	LDAP (múltiples dominios), XAUTH/RADIUS, SSO, Novell, base de datos de usuarios interna, Terminal Services[5], Citrix[5]			
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], Firewall empresarial ICSA, IPV6 Fase 2, VPNC, VPAT, FIPS 140-2[4], Common Criteria NDPP[4] , Antivirus ICSA[4]			
HARDWARE	**9200**	**9400**	**9600**	**9800**
Fuente de alimentación	Doble, redundante, intercambiables en caliente, 300 W			Doble, redundante, intercambiables en caliente, 500 W
Ventiladores	Doble, redundante, intercambiables en caliente			
Pantalla	Pantalla LED frontales			
Potencia de entrada	100-240 VCA, 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	Montable en 1U rack			Montable en 2U rack
Dimensiones	17x19.1x1.75 in (43,3 x 48,5 x 4,5 cm)			17x24x3.5 in (9 x 60 x 43 cm)
Peso	8,2 kg (18,1 lb)			18,38 kg (40,5 lb)
Peso WEEE	10,4 kg (23 lb)			22,4 kg (49,5 lb)
Peso de envío	13,3 kg (29,3 lb)			29,64 kg (65 lb)
Normativa principal	FCC Clase A, ICES Clase A, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase A, UL, cUL, TUV/ GS, CB, Certificado de cumplimiento para México por UL, RAEE, REACH, BSMI, KCC/MSIP, ANATEL			
Medio ambiente	15-40 grados 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 activado. [3] Medición del rendimiento de VPN basada en el tráfico UDP con paquetes de 1280 bytes. [4] Se aplica a SuperMassive 9200, 9400 y 9600. La certificación SuperMassive 9800 UC APL está pendiente. [5] Admitido 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.

Información para pedidos de la serie SuperMassive 9000

PRODUCTO	SKU
SuperMassive 9800 Total Secure Advance Edition (1 año)	01-SSC-0312
SuperMassive 9600 Total Secure Advance Edition (3 años)	02-SSC-0410
SuperMassive 9400 Total Secure Advance Edition (3 años)	02-SSC-0409
SuperMassive 9200 Total Secure Advance Edition (3 años)	02-SSC-0408
COMPATIBILIDAD Y SUSCRIPCIONES DE SEGURIDAD SUPERMASSIVE 9200	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, gestión e informes de firewall, visibilidad de IT en la sombra, 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: Inteligencia de Aplicaciones, prevención de amenazas, filtrado de contenidos con compatibilidad con 9200 (1 año)	01-SSC-4172
Prevención de intrusiones, Antimalware, CloudAV, Inteligencia de Aplicaciones, Control y Visualización para SuperMassive 9200 (1 año)	01-SSC-4202
Filtrado de contenido Premium Business Edition para 9200 (1 año)	01-SSC-4184
Soporte Platinum para SuperMassive 9200 (1 año)	01-SSC-4178
COMPATIBILIDAD Y SUSCRIPCIONES DE SEGURIDAD SUPERMASSIVE 9400	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, gestión e informes de firewall, visibilidad de TI en la sombra, 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: Inteligencia de Aplicaciones, prevención de amenazas, filtrado de contenidos con compatibilidad con 9400 (1 año)	01-SSC-4136
Prevención de intrusiones, Antimalware, CloudAV, Inteligencia de Aplicaciones, Control y Visualización para SuperMassive 9400 (1 año)	01-SSC-4166
Filtrado de contenido Premium Business Edition para 9400 (1 año)	01-SSC-4148
Soporte Platinum para SuperMassive 9400 (1 año)	01-SSC-4142
COMPATIBILIDAD Y SUSCRIPCIONES DE SEGURIDAD SUPERMASSIVE 9600	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, gestión e informes de firewall, visibilidad de TI en la sombra, 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: Inteligencia de Aplicaciones, prevención de amenazas, filtrado de contenidos con compatibilidad con 9600 (1 año)	01-SSC-4100
Prevención de intrusiones, Antimalware, CloudAV, Inteligencia de Aplicaciones, Control y Visualización para SuperMassive 9600 (1 año)	01-SSC-4130
Filtrado de contenido Premium Business Edition para 9600 (1 año)	01-SSC-4112
Soporte Platinum para SuperMassive 9600 (1 año)	01-SSC-4106
COMPATIBILIDAD Y SUSCRIPCIONES DE SEGURIDAD SUPERMASSIVE 9800	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, gestión e informes de firewall, visibilidad de IT en la sombra, 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: Inteligencia de Aplicaciones, prevención de amenazas, filtrado de contenidos con compatibilidad con 9800 (1 año)	01-SSC-0809
Prevención de intrusiones, Antimalware, CloudAV, Inteligencia de Aplicaciones, Control y Visualización para SuperMassive 9800 (1 año)	01-SSC-0827
Filtrado de contenido 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 SonicWall serie SuperMassive 9800, FRU	01-SSC-0204
Fuente de alimentación CA SonicWall serie SuperMassive 9800, FRU	01-SSC-0203
Ventilador de sistema SonicWall serie SuperMassive 9000, FRU	01-SSC-3876
Fuente de alimentación CA SonicWall serie SuperMassive 9000, FRU	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 corto recorrido 1000BASE-SX SFP	01-SSC-9789
Módulo de largo recorrido 1000BASE-LX SFP	01-SSC-9790
Módulo de cobre 1000BASE-T SFP	01-SSC-9791
GESTIÓN E INFORMES	**SKU**
Licencia de software de 10 nodos de SonicWall GMS	01-SSC-3363
Soporte de software para 10 nodos SonicWall GMS E-Class 24x7 (1 año)	01-SSC-6514
Dispositivo virtual SonicWall Scrutinizer con licencia del software Flow Analytics Module para un máximo de 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-3443
SonicWall Scrutinizer con licencia del software Flow Analytics Module para un máximo de 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-4002
Licencia del software SonicWall Scrutinizer Advanced Reporting Module para un máximo de 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-3773

**Consulte con un distribuidor de SonicWall para obtener una lista completa de los módulos SFP y SFP+ compatibles*

Acerca de SonicWall

SonicWall ofrece Ciberseguridad sin límites, sin perímetro para la era hiperdistribuida y una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia y poco segura. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y posibilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Para más información, visite www.sonicwall.com.

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

Datasheet-SuperMassive-US-COG-2465