Serie de la plataforma de servicios SonicWall Network Security (NS*sp*) 12000

Seguridad innovadora escalable que aprovecha las ventajas de la inteligencia en la nube.

La serie de la plataforma de servicios SonicWall Network Security (NS*sp*) 12000 adopta un enfoque moderno de detección y prevención de amenazas mediante la combinación de inteligencia en la nube con protección basada en dispositivos en una plataforma escalable de alta velocidad. Diseñada para empresas distribuidas de gran tamaño, centros de datos y proveedores de servicios, los firewalls de próxima generación (NGFWs) de la serie NS*sp* utilizan las innovadoras tecnologías de seguridad de aprendizaje profundo de la plataforma Capture Cloud para proporcionar protección probada contra las más avanzadas amenazas sin ranlentizar el rendimiento.

Seguridad para empresas grandes

El volumen y la sofisticación de los ataques contra las redes de hoy en día continúan en aumento. Para identificar y detener las amenazas e intrusiones de día cero desconocidas se requiere un enfoque que amplíe la protección integrada con inteligencia de seguridad en la nube. Sin esa inteligencia en la nube, las soluciones de seguridad en la pasarela de clase empresarial no son capaces de hacer frente a las amenazas complejas actuales.

La serie SonicWall NS*sp* toma la inteligencia de amenazas recopilada por nuestro equipo dedicado de investigación de amenazas Capture Labs y la combina con soluciones de seguridad integrada para ofrecer una protección continuamente actualizada. El servicio Capture Advanced Threat Protection (ATP) de SonicWall basado en la nube utiliza la tecnología pendiente de patente de Inspección de memoria profunda en tiempo real (RTDMI™) para detectar y bloquear de forma proactiva las amenazas de día cero del mercado de masas y el malware desconocido inspeccionando directamente en la memoria. Gracias a su arquitectura en tiempo real, la tecnología RTDMI de SonicWall es precisa, minimiza los falsos positivos e identifica y mitiga los ataques sofisticados en los que los mecanismos dañinos del malware se exponen durante menos de 100 nanosegundos. Con el fin de aumentar la seguridad basada en la nube, el motor patentado* de Inspección profunda de paquetes sin reensamblado (RFDPI®) de paso único de SonicWall inspecciona el trafico entrante y saliente de la red en el firewall. Al utilizar la plataforma SonicWall Capture Cloud junto con prestaciones integradas, como prevención de intrusiones, antimalware y filtrado Web/URL, la serie NS*sp* es capaz de proporcionar la prevención de brechas en tiempo real automatizada que las organizaciones necesitan.

Con el aumento del número de conexiones Web cifradas, resulta esencial que los NGFWs sean capaces de inspeccionar el tráfico cifrado en busca de amenazas ocultas. Los firewalls de SonicWall proporcionan una protección completa al descifrar e inspeccionar cientos de miles de conexiones cifradas mediante TLS/SSL y SSH, independientemente del puerto y el protocolo. El firewall examina cada paquete en profundidad en busca de anomalías de protocolo, amenazas, ataques de día cero, intrusiones e incluso criterios definidos. El motor de inspección profunda de paquetes detecta y previene ataques ocultos que utilizan criptografía, bloquea descargas de malware cifrado, detiene la propagación de infecciones y frustra comunicaciones de comando y control y la exfiltración de datos. Las normas de inclusión y exclusión proporcionan un control total que permite personalizar qué tráfico debe ser sometido al descifrado y a la inspección en base a requisitos legales y/o corporativos específicos.

A medida que las organizaciones crecen, la necesidad de una solución de seguridad escalable cobra más importancia. SonicWall soporta redes empresariales

Ventajas:

Prevención de amenazas y rendimiento superiores

- Tecnología de Inspección de memoria profunda en tiempo real pendiente de patente
- Tecnología patentada de inspección profunda de paquetes sin reensamblado
- Prevención de amenazas basada en la nube e integrada
- Descifrado e inspección TLS/SSL
- Efectividad de la seguridad validada por la industria
- Múltiples interfaces 40-GbE y 10-GbE
- Equipo dedicado de investigación de amenazas Capture Labs

Control y flexibilidad de la red

- Potente sistema operativo SonicOS
- Inteligencia y control de aplicaciones
- Segmentación de la red y creación de zonas
- Implementación en el borde de la red o en el núcleo del centro de datos

Escalabildiad y fiabilidad

- Número elevado de conexiones SPI-SSL
- Múltiples opciones de configuración
- Módulo de almacenamiento integrado
- Fuentes de alimentación y ventiladores redundantes

en crecimiento con una solución que elimina las preocupaciones en torno a la necesidad de añadir más potencia de procesamiento. NS*sp* 12400 incluye cuatro módulos de procesador, que pueden ampliarse a ocho, mientras que NS*sp* 12800 viene de fábrica con ocho módulos de procesador.

Al activar funciones de inspección profunda de paquetes, como IPS, antivirus, antispyware y descifrado e inspección TLS/SSL en el firewall, el rendimiento de la red a menudo se ralentiza, en ocasiones de forma drástica. Los NGFWs de la serie NS*sp*, sin embargo, incluyen interfaces 40-GbE de alta velocidad y una arquitectura de hardware multinúcleo que utiliza procesadores de seguridad especializados. En combinación con nuestros motores RTDMI y RFDPI, este diseño único elimina la pérdida de rendimiento que sufren las redes con otros firewalls.

Control y flexibilidad de la red

La serie NS*sp* utiliza SonicOS, el sistema operativo de SonicWall equipado con gran cantidad de funciones avanzadas. SonicOS proporciona a las organizaciones el control y la flexibilidad de la red que requieren a través de funciones de inteligencia y control de aplicaciones, visualización en tiempo real, un sistema de prevención de intrusiones (IPS) con una sofisticada tecnología antievasión, redes privadas virtuales (VPN) de alta velocidad y prestaciones de seguridad adicionales.

Gracias a las funciones de inteligencia y control de aplicaciones, los administradores de las redes pueden identificar las aplicaciones productivas y distinguirlas de las que son improductivas o potencialmente peligrosas, así como controlar el tráfico mediante potentes políticas a nivel de aplicación tanto por usuarios como por grupos (junto con funciones de planificación y listas de excepciones).

Se puede dar prioridad a las aplicaciones críticas de negocio, asignándoles un mayor volumen de ancho de banda, y limitar el ancho de banda para las aplicaciones que no resulten esenciales. Las funciones de supervisión y visualización en tiempo real ofrecen una representación gráfica de las aplicaciones, los usuarios y el uso del ancho de banda que proporciona una visión granular del tráfico de toda la red.

Para las empresas que busquen una flexibilidad avanzada en el diseño de su red, SonicOS ofrece las herramientas necesarias para segmentar la red en zonas mediante el uso de LANs virtuales (VLANs). Esto permite a los administradores de red crear una interfaz LAN virtual que permita la separación de la red en uno o más grupos lógicos.

Simplificación de las tareas de gestión y creación de informes

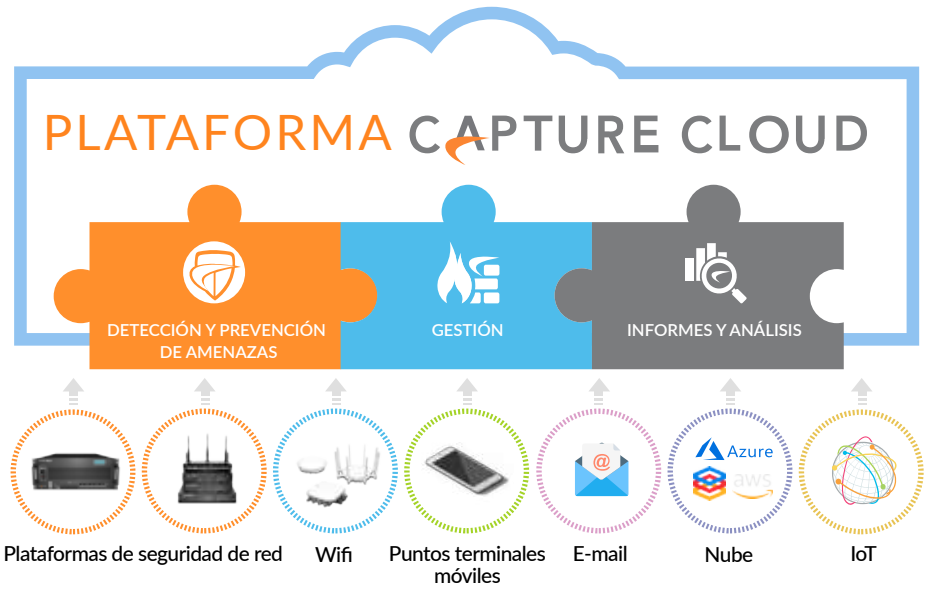
La administración, la monitorización y los informes de actividad de la red se controlan de forma centralizada desde el Sistema de gestión global (GMS). De esta forma, los administradores disponen de una única pantalla de dashboard intuitiva para gestionar todos los aspectos de la red en tiempo real. La implementación y la configuración simplificadas, junto con la facilidad de gestión, permiten a las organizaciones reducir el coste total de propiedad y obtener un elevado rendimiento de la inversión.

Partner Enabled Services

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

Plataforma Capture Cloud

La plataforma Capture Cloud de SonicWall proporciona funciones de prevención de amenazas y gestión de red basadas en la nube, así como informes y análisis, para organizaciones de cualquier tamaño. La plataforma consolida la inteligencia de amenazas recopilada de diversas fuentes, incluidos nuestro galardonado servicio de sandboxing de red multimotor, Capture Advanced Threat Protection, así como más de 1 millón de sensores de SonicWall situados en todo el mundo.



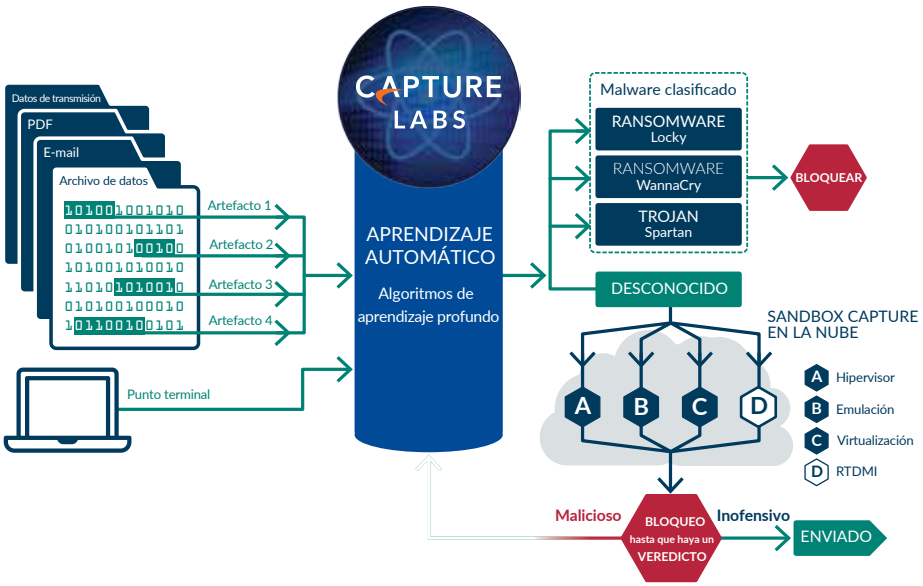
Si el sistema detecta que los datos que acceden a la red contienen código malicioso desconocido hasta el momento, el equipo de investigación de amenazas interno y dedicado de SonicWall Capture Labs, elabora definiciones que se almacenan en la base de datos de la plataforma Capture Cloud y se implementan en los firewalls de los clientes para ofrecer una protección actualizada. Las nuevas actualizaciones tienen efecto inmediato sin necesidad de reiniciar ni interrumpir el sistema. Las definiciones residentes en el dispositivo ofrecen protección contra una amplia variedad de tipos de ataques: cada una de ellas puede cubrir decenas de miles de amenazas individuales. Además de las contramedidas integradas en el dispositivo, los firewalls NS*sp* también tienen acceso continuo a la base de datos de la plataforma Capture Cloud, que incluye decenas de millones de definiciones.

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

Protección contra amenazas avanzadas

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

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



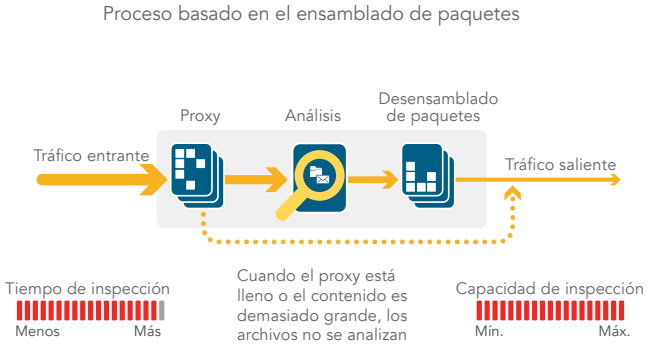
SONICWALL

Motor de inspección profunda de paquetes sin reensamblado

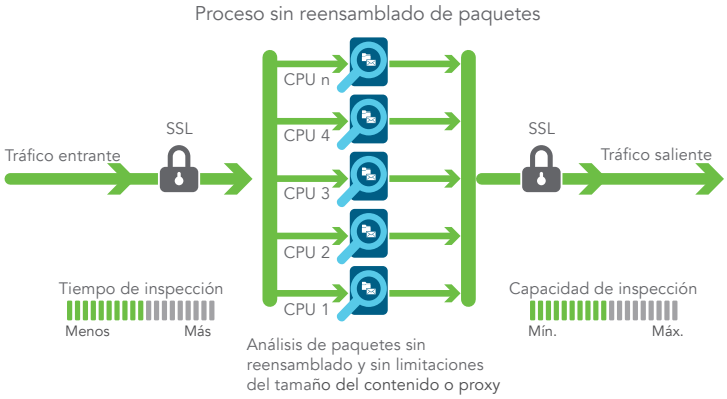
La Inspección profunda de paquetes sin reensamblado (RFDPI) de SonicWall es un sistema de inspección de paso único y baja latencia que realiza análisis bidireccionales del tráfico basados en flujos a alta velocidad sin almacenamiento en búfer ni proxies a fin de descubrir posibles intentos de intrusión o descargas de malware y de identificar el tráfico de aplicaciones independientemente del puerto y el protocolo. Este motor propietario se basa en la inspección de los datos útiles del tráfico de datos para detectar amenazas en las capas 3-7 y somete los flujos de red a amplios y repetidos procesos de normalización y descifrado con el fin de neutralizar las técnicas avanzadas de evasión que pretenden burlar los motores de detección e introducir código malicioso en la red.

Una vez que un paquete pasa el preprocesamiento necesario, incluido el descifrado TLS/SSL, es analizado con la ayuda de una única representación en memoria propietaria de tres bases de datos de definiciones: ataques de intrusión, malware y aplicaciones. El estado de conexión se actualiza constantemente en el firewall y se coteja con estas bases de datos hasta que se identifica un ataque u otro evento de seguridad, en cuyo caso se lleva a cabo una acción preestablecida.

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



Arquitectura de la competencia

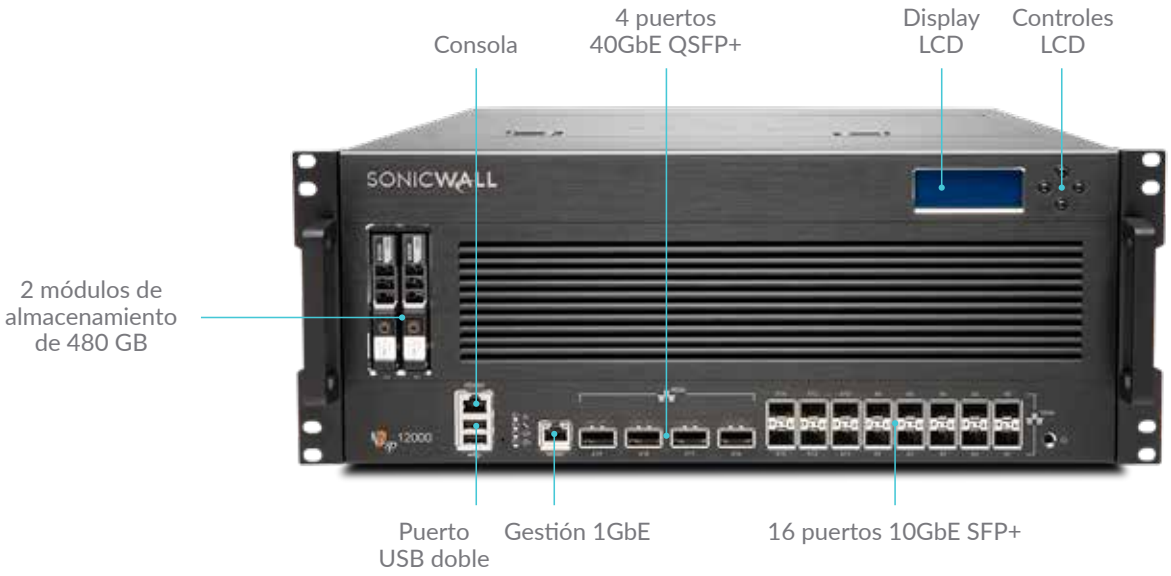


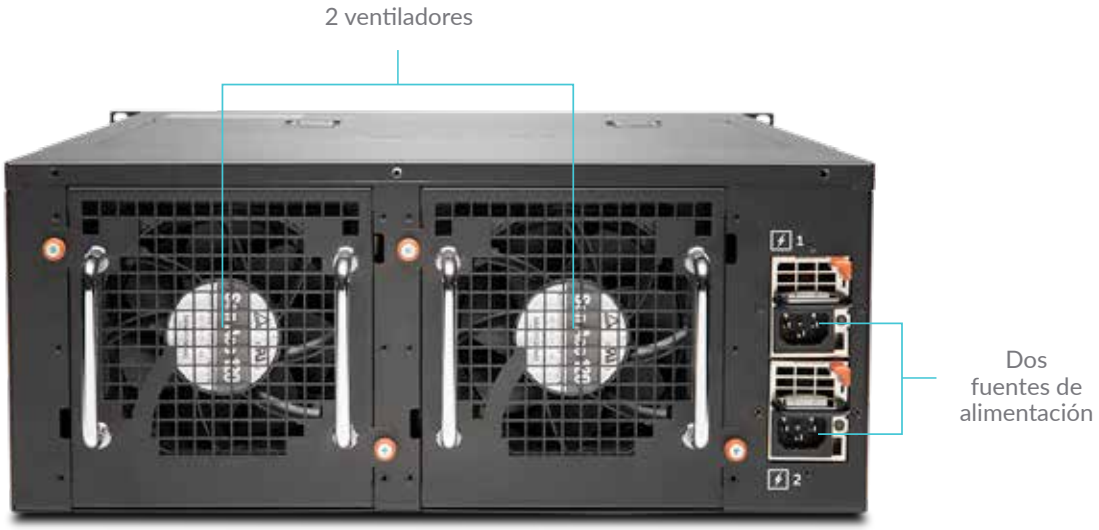
Arquitectura SonicWall

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, SonicWall proporciona a los administradores una plataforma unificada, segura y ampliable para gestionar los firewalls, puntos de acceso inalámbricos y soluciones de aceleración WAN mediante un proceso de flujo de trabajo correlacionado y auditable. Las empresas pueden consolidar fácilmente la gestión de los dispositivos de seguridad, reducir las complejidades administrativas y de solución de problemas, y controlar todos los aspectos operativos de la infraestructura de seguridad, como la gestión y la aplicación centralizadas de políticas, la supervisión de eventos en tiempo real, las actividades de los usuarios, la identificación de aplicaciones, los análisis de flujos y forenses, los informes de cumplimiento y de auditorías, entre otras funciones. Además, las empresas consiguen cumplir los requisitos de gestión de cambios del firewall mediante la automatización del flujo de trabajo, que proporciona la agilidad y la confianza necesarias para implementar las políticas de firewall apropiadas en el momento oportuno y de conformidad con la normativa vigente. El Sistema de gestión global (GMS) de SonicWall, la solución local de gestión de informes de SonicWall, proporciona una forma coherente de adaptar la seguridad de la red a los procesos de negocio y los niveles de servicio. De esta forma, simplificamos drásticamente la gestión del ciclo de vida de sus entornos de seguridad en comparación con la gestión dispositivo por dispositivo.

Serie NS*sp* 12000





Firewall	NS*sp* 12400	NS*sp* 12800
Rendimiento de inspección del firewall	58,4 Gbps	120,3 Gbps
Rendimiento IPS	36,8 Gbps	73,0 Gbps
Rendimiento de inspección antimalware	33,5 Gbps	67,5 Gbps
Rendimiento de prevención de amenazas	33,5 Gbps	67,5 Gbps
Rendimiento de IMIX	14,8 Gbps	29,0 Gbps
Número máximo de conexiones (DPI)	16.000.000	32.000.000
Nuevas conexiones/s	430.000/seg.	860.000/seg.
Módulo de almacenamiento	2 x 480 GB	2 x 480 GB
Descripción	**SKU**	**SKU**
Solo firewall NS*sp*	01-SSC-1206	01-SSC-1207
NS*sp* TotalSecure Advanced (1 año)	01-SSC-7883	01-SSC-9139

Visión de conjunto de las prestaciones de SonicOS

Firewall

- Inspección dinámica de paquetes
- Inspección profunda de paquetes sin reensamblado
- Protección contra ataques DDoS (inundaciones UDP/ICMP/SYN)
- IPv4/IPv6
- Autenticación biométrica para el acceso remoto
- Proxy DNS
- APIs REST

Descifrado e inspección TLS/SSL/SSH[1]

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

Capture advanced threat protection[1]

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

Prevención de intrusiones[1]

- Análisis basado en definiciones
- Actualizaciones automáticas de las definiciones
- Inspección bidireccional
- Capacidad para reglas de IPS detalladas
- Refuerzo de GeoIP
- Filtrado de botnets con lista dinámica
- Coincidencia de expresiones regulares

Antimalware[1]

- Análisis de malware basado en flujos
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Inspección bidireccional
- Tamaño de archivo ilimitado
- Base de datos de malware en la nube

Identificación de aplicaciones[1]

- Control de aplicaciones
- Gestión del ancho de banda de las aplicaciones
- Creación de definiciones de aplicaciones personalizadas
- Prevención de filtración de datos
- Informes de aplicaciones mediante NetFlow/IPFIX
- Completa base de datos de definiciones de aplicaciones

Visualización y análisis del tráfico

- Actividad de los usuarios
- Aplicaciones/ancho de banda/amenazas

Filtrado de contenido Web[1]

- Filtrado de URL
- Puenteo de proxys
- Bloqueo según palabras clave
- Inserción de encabezado HTTP
- Gestión del ancho de banda según categorías de clasificación CFS
- Modelo de políticas unificadas con control de aplicaciones
- Content Filtering Client

VPN

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

Redes

- PortShield
- Jumbo frames
- Protocolización mejorada
- VLAN trunking
- RSTP (protocolo de árbol de expansión rápida)
- Duplicación de puertos
- Seguridad de puertos
- QoS de nivel 2
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Enrutamiento basado en políticas
- NAT
- DNS/Proxy DNS
- 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
- 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
- Cuota cíclica de usuarios invitados
- Portal para invitados LHM

VoIP

- Control QoS granular
- Gestión del ancho de banda
- Transformaciones SIP y H.323 por norma de acceso
- 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

Almacenamiento

- Registros
- Informes
- Backups de firmware

[1] *Requiere suscripción adicional*

SONICWALL®

Prestaciones

Motor RFDPI	
Prestación	Descripción
Inspección profunda de paquetes sin reensamblado (RFDPI)	Este motor de inspección de alto rendimiento patentado y propietario realiza análisis bidireccionales del tráfico basados en flujos sin almacenamiento en búfer ni proxies a fin de descubrir posibles intentos de intrusión o ataques de malware y de identificar el tráfico de aplicaciones independientemente del puerto.
Inspección bidireccional	Escanea el tráfico entrante y saliente de forma simultánea en busca de amenazas con el fin de evitar que la red se utilice para la distribución de malware o se convierta en una plataforma de lanzamiento de ataques en el caso de que se introduzca un equipo infectado.
Inspección basada en flujos	La tecnología de inspección sin proxy ni búfer proporciona un rendimiento DPI de latencia ultrabaja para millones de flujos de red simultáneos sin limitaciones de tamaño de archivos ni flujos, y puede aplicarse a protocolos comunes y a flujos de TCP sin procesar.
Altamente paralelo y escalable	El diseño único del motor RFDPI, en combinación con la arquitectura multinúcleo, proporciona un rendimiento DPI elevado y tasas de establecimiento de sesiones nuevas extremadamente altas para hacer frente a los picos de tráfico de las redes más exigentes.
Inspección de paso único	La arquitectura DPI de paso único escanea el tráfico simultáneamente para la detección de malware y de intrusiones y para la identificación de aplicaciones, reduciendo drásticamente la latencia de la DPI y garantizando la correlación de toda la información sobre las amenazas en una única arquitectura.
Firewall y redes	
Prestación	Descripción
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 NS*sp* 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 SonicOS, el hardware será compatible con las implementaciones de filtrado y de modo Wire.
Opciones de implementación flexibles	La serie NS*sp* puede implementarse en el modo tradicional NAT, en el modo puente de capa 2, en el modo Wire y en el modo de TAP de red.
Equilibrio de carga WAN	Equilibra la carga de múltiples interfaces WAN mediante Round Robin o Spillover o utilizando métodos basados en porcentajes.
Calidad de Servicio (QoS) avanzada	Garantiza las comunicaciones críticas con etiquetado 802.1p y DSCP y remapeo del tráfico VoIP en la red.
Soporte de Gatekeeper H.323 y proxy SIP	Bloquea las llamadas spam: todas las llamadas entrantes han de ser autorizadas y autenticadas mediante Gatekeeper H.323 o proxy SIP.
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.
Gestión e informes	
Prestación	Descripción
Sistema de gestión global (GMS)	Con SonicWall Global Management System (GMS), pueden configurarse y gestionarse los dispositivos SonicWall de forma local.
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 Analytics u otras compatibles con IPFIX y NetFlow con extensiones.
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 IPSec para conectividad entre emplazamientos	La VPN IPSec de alto rendimiento permite a la serie NS*sp* 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/Terminal Services, en combinación con la amplia información proporcionada por la DPI, es posible identificar a los usuarios y sus actividades.
GeoIP – Identificación del tráfico en base al país	Identifica y controla el tráfico de red dirigido a, o procedente de, países determinados para ofrecer protección contra ataques de amenazas de origen conocido o sospechoso, o para investigar el tráfico sospechoso originado en la red. Permite crear listas personalizadas de países y Botnets para anular etiquetas de país o Botnet erróneas asociadas con una dirección IP. Elimina el filtrado de direcciones IP no deseado debido a errores de clasificación.
Filtrado DPI de expresiones regulares	Previene la filtración de datos gracias a que identifica y controla el contenido que atraviesa la red mediante la coincidencia de expresiones regulares. Permite crear listas personalizadas de países y Botnets para anular etiquetas de país o Botnet erróneas asociadas con una dirección IP.

Servicios de suscripción de prevención de brechas

Capture Advanced Threat Protection	
Prestación	Descripción
Sandboxing multimotor	La plataforma de sandbox multimotor, que incluye sandboxing virtualizado, emulación de sistema completo y tecnología de análisis de nivel de hipervisor, ejecuta el código sospechoso y analiza su comportamiento, proporcionando una visibilidad completa de la actividad maliciosa.
Inspección de memoria profunda en tiempo real (RTDMI)	Esta tecnología basada en la nube pendiente de patente detecta y bloquea el malware que no exhibe ningún comportamiento malicioso y oculta sus armas mediante el cifrado. Al forzar al malware a revelar sus armas en la memoria, el motor RTDMI detecta y bloquea de forma proactiva las amenazas de día cero y el malware desconocido del mercado de masas.
Bloqueo hasta que haya un veredicto	A fin de evitar el acceso a la red de archivos potencialmente peligrosos, los archivos enviados a la nube para su análisis pueden retenerse en la pasarela hasta que se emita un veredicto.
Análisis de gran variedad de tipos y tamaños de archivos	Soporta análisis de una amplia variedad de tipos de archivos, como los programas ejecutables (PE), DLL, PDFs, documentos MS Office, archivos, JAR y APK, así como múltiples sistemas operativos, como Windows, Android, Mac OS X y entornos multinavegador.
Rápida implementación de definiciones	Cuando se detecta un archivo malicioso, inmediatamente se pone una definición a disposición de los firewalls con suscripción a SonicWall Capture ATP y se envía a las bases de datos de definiciones de Gateway Anti-Virus e IPS y a las bases de datos de reputación de URL, IP y dominios en el transcurso de 48 horas.
Capture Client	Capture Client es una plataforma de cliente unificada que proporciona múltiples prestaciones de protección de puntos terminales, como protección de malware avanzada y soporte para la visibilidad del tráfico cifrado. Utiliza tecnologías de protección multicapa, funciones completas de informes y prestaciones de refuerzo de protección de puntos terminales.
Prevención de amenazas cifradas	
Prestación	Descripción
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico cifrado mediante TLS/SSL sobre la marcha sin necesidad de proxy en busca de malware, intrusiones y filtraciones de datos. Además, aplica políticas de control de aplicaciones, URL y contenido a fin de proporcionar protección contra las amenazas ocultas en el tráfico cifrado. Esta prestación se incluye con suscripciones de seguridad para todos los modelos de la serie NS*sp*.
Inspección SSH	La inspección profunda de paquetes de SSH (DPI-SSH) descifra e inspecciona los datos que atraviesan los túneles SSH para prevenir ataques que utilicen SSH.
Prevención de intrusiones	
Prestación	Descripción
Protección basada en contramedidas	El sistema de prevención de intrusiones (IPS) estrechamente integrado utiliza definiciones y otras contramedidas para escanear los datos útiles de los paquetes en busca de vulnerabilidades y exploits, cubriendo de este modo un amplio abanico de ataques y vulnerabilidades.
Actualizaciones automáticas de las definiciones	El equipo de investigación de amenazas de SonicWall investiga e implementa contramedidas IPS, actualizando continuamente una larga lista que cubre más de 50 categorías de ataques. Las nuevas actualizaciones se hacen efectivas en el acto, sin que sea necesario reiniciar los sistemas ni interrumpir su servicio.
Protección IPS entre zonas	Refuerza la seguridad interna al segmentar la red en múltiples zonas de seguridad con prevención de intrusiones para evitar la propagación de las amenazas de unas zonas a otras.
Detección y bloqueo de actividades de comando y control (CnC) procedente de ataques botnets	Identifica y bloquea el tráfico de comando y control originado en bots de la red local y dirigido a IPs y dominios identificados como propagadores de malware o conocidos como puntos de CnC.
Abuso/anomalía de protocolo	Identifica y bloquea ataques que abusan de los protocolos para intentar eludir el IPS.
Protección de día cero	Protege la red ante los ataques de día cero con actualizaciones constantes contra los últimos métodos y técnicas de exploits, que cubren miles de exploits individuales.
Tecnología antievasión	La amplia normalización de flujos, la descodificación y otras técnicas impiden que las amenazas puedan penetrar la red sin ser detectadas utilizando técnicas de evasión en las capas 2-7.

Prevención de amenazas	
Prestación	Descripción
Antimalware en pasarela	El motor RFDPI analiza todo el tráfico entrante, saliente y dentro de una misma zona en busca de virus, troyanos, registradores de pulsaciones de teclas y otros tipos de malware en archivos de una longitud y un tamaño ilimitados en todos los puertos y flujos de TCP.
Protección antimalware de Capture Cloud	Los servidores de la nube de SonicWall disponen de una base de datos de decenas de millones de definiciones de amenazas que se actualiza continuamente y se utiliza para aumentar las capacidades de la base de datos de definiciones integrada, lo que proporciona a la tecnología RFDPI una amplia cobertura de amenazas.
Actualizaciones de seguridad las 24 horas	Las nuevas actualizaciones de las amenazas se transfieren automáticamente a los firewalls con servicios de seguridad activos, donde se hacen efectivas inmediatamente sin necesidad de reiniciar el sistema ni de interrumpir el servicio.
Inspección TCP bidireccional (sin procesar)	El motor RFDPI puede analizar flujos de TCP sin procesar en cualquier puerto y en ambas direcciones, con lo que se previenen los ataques que intentan infiltrarse por sistemas de seguridad desactualizados que se centran en proteger solo algunos puertos más conocidos.
Amplio soporte de protocolos	Identifica protocolos comunes, como HTTP/S, FTP, SMTP, SMBv1/v2 y otros tipos, que no envían datos en TCP sin procesar, y descodifica cargas útiles para la inspección de malware, incluso si no se ejecutan en puertos estándares y bien conocidos.

Inteligencia y control de aplicaciones	
Prestación	Descripción
Control de aplicaciones	Controle aplicaciones, o funciones de aplicaciones individuales, identificadas por el motor RFDPI mediante su cotejo con una base de datos en continuo crecimiento de miles de definiciones de aplicaciones, con el objetivo de aumentar la seguridad y la productividad de la red.
Identificación personalizada de aplicaciones	Controle las aplicaciones personalizadas creando definiciones basadas en parámetros específicos o patrones exclusivos de una aplicación en sus comunicaciones de red para conseguir un mayor control de la red.
Gestión del ancho de banda de las aplicaciones	Asigne y regule de forma detallada el ancho de banda disponible para aplicaciones o categorías de aplicaciones críticas, a la vez que limita el tráfico de aplicaciones no esenciales.
Control granular	Controle aplicaciones (o componentes específicos de una aplicación) basándose en programaciones, grupos de usuarios, listas de exclusión y una gama de acciones con una completa identificación de usuario mediante SSO a través de la integración de LDAP/AD/Terminal Services/Citrix.
Filtrado de contenido	
Prestación	Descripción
Filtrado de contenido dentro y fuera	Aplique políticas de usos aceptables y bloquee el acceso a sitios Web 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	
Prestación	Descripción
Protección en varios niveles	Utilice las funciones del firewall, como la primera capa de defensa en el perímetro, junto con la protección de puntos terminales, a fin de bloquear los virus que penetran en la red por medio de portátiles, unidades de memoria flash y otros sistemas no protegidos.
Opción de aplicación automatizada	Asegúrese de que todos los equipos que accedan a la red tengan instalado y activo el software antivirus y/o certificado DPI-SSL apropiado. De este modo, eliminará los costes asociados habitualmente a la gestión de soluciones antivirus para equipos de escritorio.
Opción de instalación e implementación automatizadas	La implementación y la instalación máquina a máquina de clientes antivirus y antispyware se realiza de forma automática en toda la red, con lo que se minimiza la sobrecarga administrativa.
Antivirus de próxima generación	Capture Client utiliza un motor de inteligencia artificial estático para determinar las amenazas antes de que puedan ejecutarse y regresar a un estado previo a la infección.
Protección antispyware	La potente función de protección antispyware analiza y bloquea la instalación de un completo conjunto de programas de spyware en equipos de escritorio y portátiles antes de que éstos transmitan datos confidenciales, lo que contribuye a aumentar la seguridad y el rendimiento de los equipos de escritorio.

Especificaciones del sistema de la serie NS*sp*

Firewall general	NS*sp* 12400	NS*sp* 12800
Sistema operativo	SonicOS 6,5.1.8	
Núcleos de procesamiento de seguridad	128	256
Interfaces	4 x 40-GbE QSFP+, 16 x 10-GbE SFP+, 1 GbE gestión, 1 consola	4 x 40-GbE QSFP+, 16 x 10-GbE SFP+, 1 GbE gestión, 1 consola
Almacenamiento integrado	2 x 480 GB	
Gestión	CLI, SSH, IU Web, GMS, APIs REST	
Usuarios con SSO	110.000	110.000
Número máximo de puntos de acceso soportados	128	128
Protocolización	Analyzer, Local Log, Syslog, IPFIX, NetFlow	
Rendimiento de firewall/VPN	**NS*sp* 12400**	**NS*sp* 12800**
Rendimiento de inspección del firewall[1]	58,4 Gbps	120,3 Gbps
Rendimiento de prevención de amenazas[2]	33,5 Gbps	67,5 Gbps
Rendimiento de inspección de aplicaciones[2]	45,5 Gbps	91,0 Gbps
Rendimiento de IPS[2]	36,8 Gbps	73,0 Gbps
Rendimiento de inspección antimalware[2]	33,5 Gbps	67,5 Gbps
Rendimiento de IMIX	14,8 Gbps	29,0 Gbps
Rendimiento de descifrado e inspección TLS/SSL (DPI SSL)[2]	8,1 Gbps	17,6 Gbps
Rendimiento de VPN[3]	24,5 Gbps	47,0 Gbps
Conexiones por segundo	430.000/seg.	860.000/seg.
Conexiones máximas (SPI)	40.000.000	80.000.000
Número máximo de conexiones (DPI)	16.000.000	32.000.000
Número máximo de conexiones (DPI SSL)	800.000	1.600.000
VPN	**NS*sp* 12400**	**NS*sp* 12800**
Túneles VPN entre emplazamientos	25.000	25.000
Clientes VPN IPSec (máx.)	2.000 (10.000)	2.000 (10.000)
Clientes SSL VPN NetExtender (máx)	2 (3.000)	2 (3.000)
Cifrado/Autenticación	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, criptografía Suite B	
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14v	
VPN basada en enrutamiento	RIP, OSPF, BGP	
Redes	**NS*sp* 12400**	**NS*sp* 12800**
Asignación de direcciones IP	Estática, (cliente DHCP, PPPoE, L2TP y PPTP), servidor DHCP interno, relé DHCP	
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT, modo transparente	
Interfaces VLAN	512	512
Protocolos de enrutamiento	BGP, OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas	
QoS	Prioridad de ancho de banda, ancho de banda máximo, ancho de banda garantizado, marcado DSCP, 802.1p	
Autenticación	LDAP, XAUTH/RADIUS, SSO, Novell, base de datos de usuarios interna, Terminal Services, Citrix, Tarjeta Common Access Card (CAC)	
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 (en progreso)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall e PS), UC APL, USGv6, CsFC	
Alta disponibilidad	Activa/Pasiva con State Sync, DPI activa/activa con State Sync, Agrupación (clústeres) activa/activa	
Hardware	**NS*sp* 12400**	**NS*sp* 12800**
Fuente de alimentación	Dual, redundante, 1,200W	
Ventiladores	Dual, extraíble	
Potencia de entrada	100-240 V CA, 50-60 Hz	
Consumo máximo de energía (W)	679	965
MTBF a 25°C en horas	113.114	91.118
MTBF a 25°C en años	12,9	10,4
Factor de forma	Preparado para montaje en bastidor 4U	
Dimensiones	61 x 43 x 18 cm (24,0 x 16,9 x 3,4 pulgadas)	
Peso	26,9 kg (59,3 lb)	30,5 kg (67,2 lb)
Peso WEEE	30,7 kg (67,7 lb)	34,3 kg (75,6 lb)
Peso de envío	37,7 kg (83,1 lb)	41,3 kg (91,1 lb)
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	
Entorno (Operativo/Almacenamiento)	0°-40° C (32°-105° F)/-40° a 70° C (-40° a 158° F)	
Humedad	10-95%, 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 DPI pleno/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. Rendimiento DPI SSL medido sobre la base de tráfico HTTPS con IPS activado.
[3] Rendimiento VPN medido sobre la base de tráfico UDP y paquetes de 1.280 bytes según RFC 2544. Las especificaciones, las prestaciones y la disponibilidad están sujetas a modificaciones.
Uso futuro. Las especificaciones, las prestaciones y la disponibilidad están sujetas a modificaciones.

Información de pedido de la serie NS*sp* 12000

NS*sp* 12400	SKU
NS*sp* 12400 TotalSecure Advanced Edition (1 año)	01-SSC-7883
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para NS*sp* 12400 (1 año)	01-SSC-6588
Capture Advanced Threat Protection para NS*sp* 12400 (1 año)	01-SSC-6598
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NS*sp* 12400 (1 año)	01-SSC-7853
Soporte 24x7 para NS*sp* 12400 (1 año)	01-SSC-6384
Content Filtering Service para NS*sp* 12400 (1 año)	01-SSC-7698
NS*sp* 12800	**SKU**
NS*sp* 12800 TotalSecure Advanced Edition (1 año)	01-SSC-9139
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas, filtrado de contenido y soporte 24x7 para NS*sp* 12800 (1 año)	01-SSC-6591
Capture Advanced Threat Protection para NS*sp* 12800 (1 año)	01-SSC-7178
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NS*sp* 12800 (1 año)	01-SSC-7879
Soporte 24x7 para NS*sp* 12800 (1 año)	01-SSC-6498
Content Filtering Service para NS*sp* 12800 (1 año)	01-SSC-7850
Módulos y accesorios*	**SKU**
Módulo de procesadores serie NS*sp* 12000	01-SSC-1211
Módulo SSD serie NS*sp* 12000	01-SSC-1212
Ventilador de sistema serie NS*sp* 12000	01-SSC-1213
Alimentación CA serie NS*sp* 12000	01-SSC-1215

**Si desea obtener una lista completa de los módulos SFP y SFP+ soportados, consulte a su revendedor local de SonicWall*

Números de modelo oficiales:

NS*sp* 12400/12800 – 4RK02-0C0

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
Para más información, consulte nuestra página Web.
www.sonicwall.com

Datasheet-NSsp-US-KJ-MKTG4029