Serie Network Security Appliance

Firewalls de próxima generación

Hoy en día, las organizaciones se enfrentan a una serie de retos de seguridad sin precedentes. El aumento exponencial del grado de sofisticación y del volumen de los ataques a menudo resulta en la pérdida de datos corporativos, personales y de clientes, el robo de propiedad intelectual, reputaciones dañadas y pérdidas de productividad. Al mismo tiempo, la seguridad se ha vuelto más compleja. Las organizaciones tienen que adaptarse a la revolución BYOD y a la explosión de dispositivos personales que se conectan a la red. Los teléfonos inteligentes y tablets personales ralentizan el rendimiento de la red y la productividad, mientras que las aplicaciones móviles, como los medios sociales y la transmisión por secuencias de vídeo, consumen una enorme cantidad de ancho de banda. Con el fin de superar estos retos, algunas organizaciones optan por comprometer la seguridad desactivando determinadas prestaciones para mantener el nivel de rendimiento de la red.

Ahora, puede garantizar la seguridad y productividad de su organización sin necesidad de comprometer el rendimiento de la red. Los firewalls de próxima generación de la serie Dell™ SonicWALL™ Network Security Appliance (NSA) ofrecen un sistema de seguridad de red que no compromete el rendimiento. Basados en la misma arquitectura que nuestra línea estrella de firewalls de próxima generación Supermassive, estos dispositivos proporcionan un excelente nivel de seguridad y rendimiento sin compromisos. Además, la serie NSA ofrece la facilidad de uso y la rentabilidad que caracterizan a los productos Dell SonicWALL.

Tras años de investigación y desarrollo, la serie NSA ha sido diseñada desde cero para empresas distribuidas, empresas pequeñas y medianas, sucursales, campus escolares y agencias gubernamentales. Combina una arquitectura multinúcleo revolucionaria con el motor patentado* de prevención de amenazas de paso único Reassembly-Free Deep Packet Inspection® (RFDPI) en un diseño altamente escalable. Gracias a ello, proporciona a las organizaciones una protección, un rendimiento y una escalabilidad líderes en la industria, una latencia baja y un elevado número de conexiones simultáneas sin limitaciones del tamaño de los archivos. Algunas prestigiosas empresas de pruebas independientes han evaluado y/o certificado la tecnología de los firewalls de la serie NSA.

A diferencia de las tecnologías de firewall y prevención de intrusiones antiguas de los competidores, la serie NSA inspecciona todo el tráfico, independientemente del puerto y el protocolo. La serie NSA bloquea los ataques de malware avanzados con las mayores tasas de descifrado SSL sobre la marcha de la industria. El servidor de autenticación integrado refuerza de forma eficaz las políticas de uso aceptable mediante controles granulares de las aplicaciones para permitir la gestión del ancho de banda e incrementar la productividad. A diferencia de las soluciones anticuadas compuestas por varios dispositivos, que no comparten la información sobre las amenazas, la serie NSA integra firewall e IPS. Esta inteligencia conectada refuerza las decisiones sobre políticas para intensificar la eficacia de la seguridad, reduciendo al mismo tiempo los esfuerzos de gestión y los riesgos de la organización.

Ventajas:

- La mejor protección de su categoría
- Arquitectura multinúcleo
- Altísimo rendimiento
- Prevención de intrusiones
- Antimalware basado en la red
- Acceso remoto seguro
- Conexión inalámbrica segura
- Filtrado URL
- Antispam en pasarela
- Control de aplicaciones
- Gestión centralizada

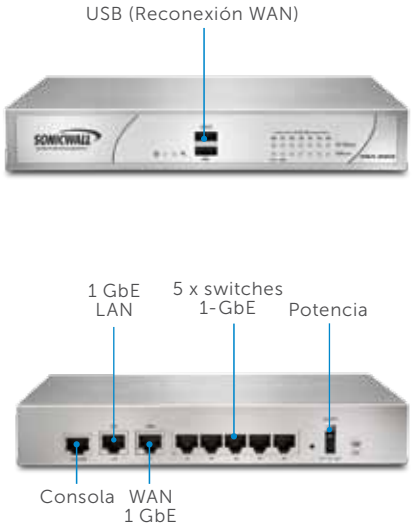
Por otra parte, los firewalls de la serie NSA ofrecen protección antimalware basada en la red con Cloud Assist, proporcionando a las organizaciones una primera capa de defensa esencial contra millones de variantes de malware.

Además, los firewalls de la serie NSA son económicos y fáciles de administrar gracias a la galardonada plataforma Global Management System (GMS) de Dell, capaz de gestionar cientos, o incluso miles, de firewalls Dell SonicWALL desde una única consola. Las funciones completas de visualización en tiempo real muestran lo que ocurre en la red a través de informes detallados tanto integrados como externos.

**Patentes en EE UU 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723*

Los firewalls de próxima generación (NGFW) de la serie Dell SonicWALL NSA se basan en la más moderna arquitectura multinúcleo y en la tecnología de inspección profunda de paquetes sin reensamblado para proteger la red contra ataques internos y externos sin comprometer el rendimiento. La serie NSA combina prevención de intrusiones, inspección de contenido y URL, inteligencia y control de aplicaciones, alta disponibilidad y otras prestaciones avanzadas de red.

Network Security Appliance 220 y 220 Wireless-N



Dell SonicWALL NSA 220 proporciona a pymes y sucursales la más amplia protección de primera línea, un control eficaz de aplicaciones y usuarios y potentes funciones de productividad de red, así como conectividad inalámbrica 802.11n de banda dual opcional.

Firewall	NSA 220 y 220 W
Rendimiento de firewall	600 Mbps
Rendimiento IPS	195 Mbps
Rendimiento antimalware	115 Mbps
Rendimiento DPI pleno	110 Mbps
Rendimiento IMIX	180 Mbps
Conexiones DPI máximas	85.000
Conexiones nuevas/seg.	32.000/seg.

Descripción	NSA 220 y 220 W
NSA 220, solo firewall	01-SSC-9750
NSA 220 Wireless-N, solo firewall	01-SSC-9752
NSA 220 TotalSecure (1 año)	01-SSC-9744
NSA 220 Wireless-N TotalSecure (1 año)	01-SSC-9746
Comprehensive Gateway Security Suite (1 año)	01-SSC-4648
Gateway Anti-Malware/IPS (1 año)	01-SSC-4612
Soporte dinámico 24x7 (1 año)	01-SSC-4630

Network Security Appliance 250M y 250M Wireless-N

Dell SonicWALL NSA 250M proporciona a sucursales y empresas distribuidas la más amplia protección de primera línea, un control eficaz de aplicaciones y usuarios y potentes funciones de productividad de red, así como conectividad inalámbrica 802.11 de banda dual opcional.

Firewall	NSA 250M y 250M W
Rendimiento de firewall	750 Mbps
Rendimiento IPS	250 Mbps
Rendimiento antimalware	140 Mbps
Rendimiento DPI pleno	130 Mbps
Rendimiento IMIX	210 Mbps
Conexiones DPI máximas	110.000
Conexiones nuevas/seg.	64.000/seg.

Descripción	NSA 250M y 250M W
NSA 250M, solo firewall	01-SSC-9755
NSA 250M Wireless-N, solo firewall	01-SSC-9757
NSA 250M TotalSecure (1 año)	01-SSC-9747
NSA 250M Wireless-N TotalSecure (1-año)	01-SSC-9749
Comprehensive Gateway Security Suite (1 año)	01-SSC-4606
Gateway Anti-Malware/IPS (1 año)	01-SSC-4570
Soporte dinámico 24x7 (1 año)	01-SSC-4588

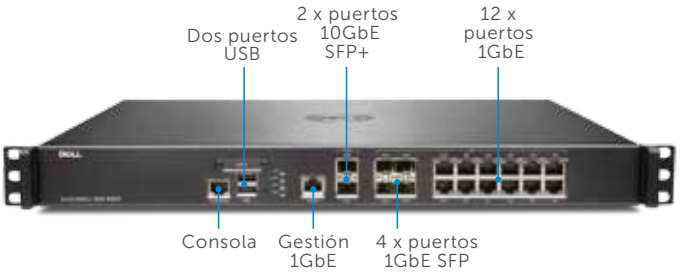
Network Security Appliance 2600

El Dell SonicWALL NSA 2600 ha sido diseñado para responder a las necesidades de las organizaciones pequeñas en crecimiento, las sucursales y los campus escolares.

Firewall	NSA 2600
Rendimiento de firewall	1,9 Gbps
Rendimiento IPS	700 Mbps
Rendimiento antimalware	400 Mbps
Rendimiento DPI pleno	300 Mbps
Rendimiento IMIX	600 Mbps
Conexiones DPI máximas	125.000
Conexiones nuevas/seg.	15.000/seg.

Descripción	Nº producto
NSA 2600, solo firewall	01-SSC-3860
NSA 2600 TotalSecure (1 año)	01-SSC-3863
Comprehensive Gateway Security Suite (1 año)	01-SSC-4453
Gateway Anti-Malware/IPS (1 año)	01-SSC-4459
Soporte Silver 24x7 (1 año)	01-SSC-4314

Network Security Appliance 3600/4600

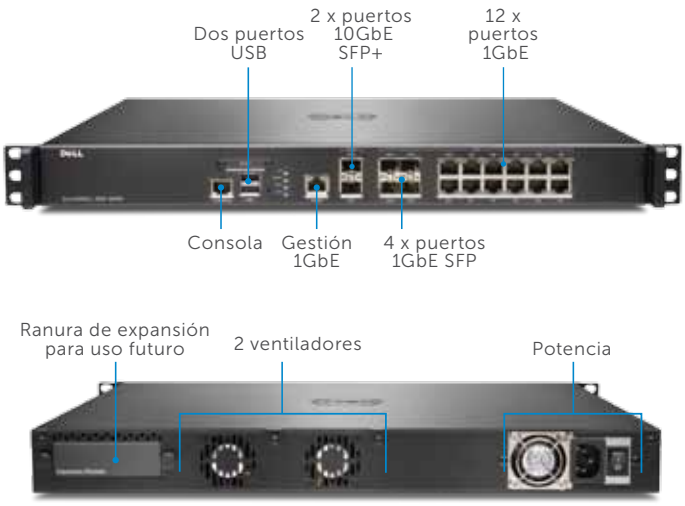


El Dell SonicWALL NSA 3600/4600 es ideal para entornos de redes de empresas pequeñas y medianas y sucursales que se preocupan por su capacidad de transferencia de datos y por su nivel de rendimiento.

Firewall	NSA 3600	NSA 4600
Rendimiento de firewall	3,4 Gbps	6,0 Gbps
Rendimiento IPS	1,1 Gbps	2,0 Gbps
Rendimiento antimalware	600 Mbps	1,1 Gbps
Rendimiento DPI pleno	500 Mbps	800 Mbps
Rendimiento IMIX	900 Mbps	1,6 Gbps
Conexiones DPI máximas	175.000	200.000
Conexiones nuevas/seg.	20.000/seg.	40.000/seg.

Descripción	NSA 3600	NSA 4600
Solo firewall	01-SSC-3850	01-SSC-3840
TotalSecure (1 año)	01-SSC-3853	01-SSC-3843
Comprehensive Gateway Security Suite (1 año)	01-SSC-4429	01-SSC-4405
Gateway Anti-Malware/IPS (1 año)	01-SSC-4435	01-SSC-4411
Soporte Silver 24x7 (1 año)	01-SSC-4302	01-SSC-4290

Network Security Appliance 5600

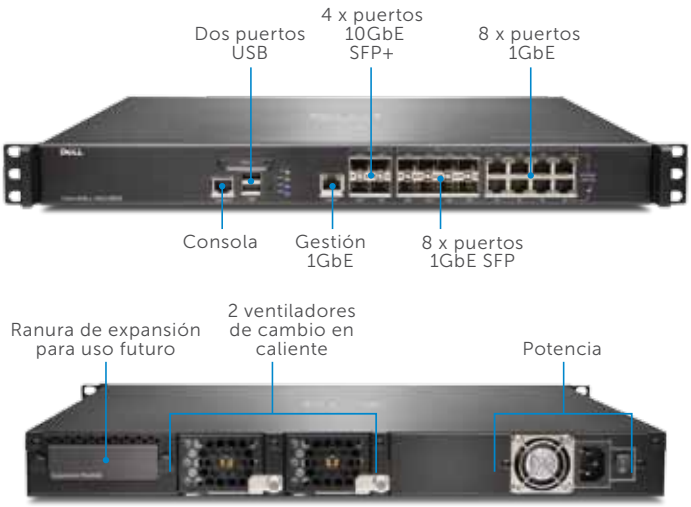


Dell SonicWALL NSA 5600 es ideal para entornos corporativos, redes distribuidas y oficinas sucursales que requieren una capacidad de transferencia de datos considerable.

Firewall	NSA 5600
Rendimiento de firewall	9,0 Gbps
Rendimiento IPS	3,0 Gbps
Rendimiento antimalware	1,7 Gbps
Rendimiento DPI pleno	1,6 Gbps
Rendimiento IMIX	2,4 Gbps
Conexiones DPI máximas	500.000
Conexiones nuevas/seg.	60.000/seg.

Descripción	Nº producto
NSA 5600, solo firewall	01-SSC-3830
NSA 5600 TotalSecure (1 año)	01-SSC-3833
Comprehensive Gateway Security Suite (1 año)	01-SSC-4234
Gateway Anti-Malware/IPS (1 año)	01-SSC-4240
Soporte Gold 24x7 (1 año)	01-SSC-4284

Network Security Appliance 6600



Dell SonicWALL NSA 6600 es ideal para entornos de oficinas centrales y redes distribuidas de gran tamaño que requieren una elevada capacidad de transferencia de datos y un alto nivel de rendimiento.

Firewall	NSA 6600
Rendimiento de firewall	12,0 Gbps
Rendimiento IPS	4,5 Gbps
Rendimiento antimalware	3,0 Gbps
Rendimiento DPI pleno	3,0 Gbps
Rendimiento IMIX	3,5 Gbps
Conexiones DPI máximas	500.000
Conexiones nuevas/seg.	90.000/seg.

Descripción	Nº producto
NSA 6600, solo firewall	01-SSC-3820
NSA 6600 TotalSecure (1 año)	01-SSC-3823
Comprehensive Gateway Security Suite (1 año)	01-SSC-4210
Gateway Anti-Malware/IPS (1 año)	01-SSC-4216
Soporte Gold 24x7 (1 año)	01-SSC-4278

Disfrute de una seguridad de red más profunda

Los firewalls de la serie Dell SonicWALL NSA son capaces de proporcionar a organizaciones de todos los tamaños un nivel de seguridad de red más profundo gracias a su arquitectura de hardware multinúcleo escalable y a su motor patentado de Inspección profunda de paquetes sin reensamblado (RFDPI) de paso único y latencia baja, capaz de escanear todos los bytes de cada paquete manteniendo un alto nivel de rendimiento. La seguridad de red de la serie Dell SonicWALL NSA va más allá que la de otros firewalls, ya que combina funciones de descifrado e inspección SSL en tiempo real, un sistema de prevención de intrusiones (IPS) equipado con una sofisticada tecnología antievasión y un sistema de protección antimalware basado en la red que aprovecha las ventajas de la nube. Ahora, las organizaciones pueden bloquear amenazas nuevas todos los días a medida que aparecen.

Se estima que las organizaciones pasan por alto aproximadamente un tercio de su tráfico de red a causa del cifrado SSL. Con el fin de eliminar ese ángulo muerto, la tecnología de descifrado e inspección SSL de la serie Dell SonicWALL NSA permite al motor RFDPI descifrar e inspeccionar todo el tráfico de red de todos los puertos.

Cada hora se desarrollan nuevas variantes de malware. La serie Dell SonicWALL NSA le mantiene al corriente de estas amenazas con un sistema de protección antimalware basado en la red y conectado a una base de datos en la nube continuamente actualizada que abarca más de 13 millones de variantes de malware.

El Servicio de prevención de intrusiones (IPS) de Dell SonicWALL ofrece protección contra una amplia variedad de vulnerabilidades y exploits de aplicaciones basados en la red. Puesto que todos los días se descubren nuevas vulnerabilidades de aplicaciones, la actualización continua del sistema IPS es fundamental para disfrutar de una protección eficaz contra las amenazas emergentes. Dell SonicWALL va un paso más allá que las soluciones tradicionales: su sistema de prevención de intrusiones incluye una sofisticada tecnología antievasión que escanea todo el tráfico de la red en busca de gusanos, troyanos, vulnerabilidades de software, exploits de puerta trasera y otros tipos de ataques maliciosos. Los ciberdelincuentes a menudo intentan eludir el IPS utilizando algoritmos complejos para evitar ser detectados. Los NGFW de Dell utilizan un avanzado sistema de protección contra amenazas para descodificar los ataques ocultos antes de que puedan dañar su organización. Al concentrarse en el tráfico malicioso conocido, Dell SonicWALL IPS elimina los falsos positivos y aumenta la fiabilidad y el rendimiento de la red. Diseñado para ofrecer protección contra las amenazas tanto internas como externas, Dell SonicWALL IPS monitoriza el tráfico de red en busca de comportamientos maliciosos o anómalos, y a continuación bloquea o protocoliza el tráfico basándose en políticas predefinidas.

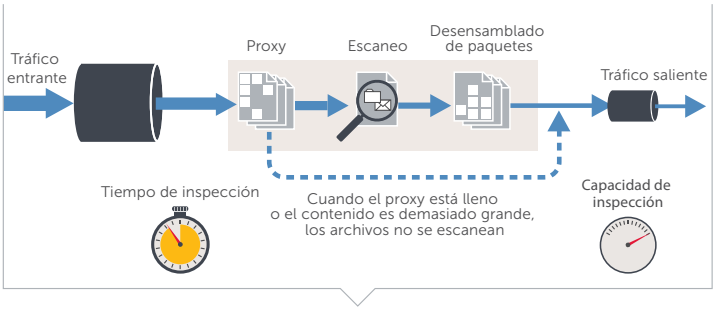
Motor de inspección profunda de paquetes sin reensamblado

El motor de inspección profunda de paquetes sin reensamblado de Dell SonicWALL (RFDPI) proporciona el mejor control de aplicaciones y la mejor protección contra las amenazas sin comprometer el rendimiento. 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 ha sido sometido al preprocesamiento necesario, incluido el descifrado 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.

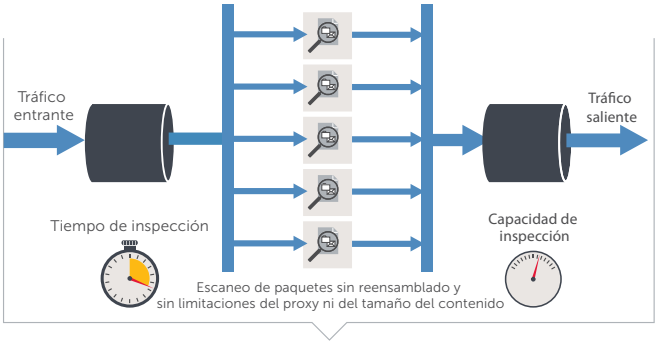
En la mayoría de los casos, el sistema finaliza la conexión y crea eventos de protocolización y notificación. No obstante, el motor también puede configurarse para realizar únicamente la inspección o, en caso de detección de aplicaciones, para proporcionar servicios de gestión de ancho de banda de capa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

Proceso con ensamblado de paquetes



Arquitectura de otros proveedores

Proceso sin ensamblado de paquetes

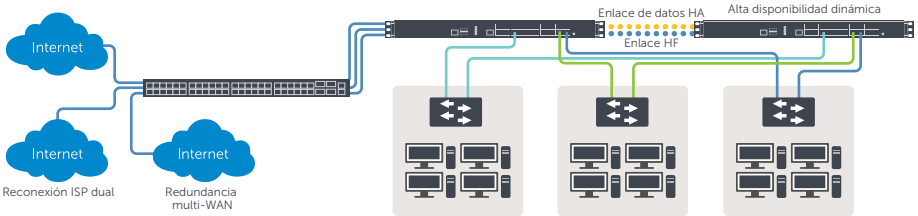


Arquitectura Dell SonicWALL

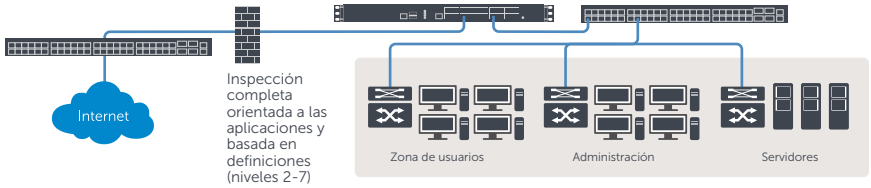
Opciones de implementación flexibles y personalizables–Serie NSA

Gracias a su revolucionario diseño de hardware multinúcleo y a la tecnología Reassembly-Free Deep Packet Inspection, los dispositivos Dell SonicWALL NSA ofrecen protección de red tanto interna como externa sin comprometer el rendimiento de la red. Los NGFW de la serie NSA combinan prevención de intrusiones de alta velocidad, inspección de archivos y de contenido, así como potentes prestaciones de inteligencia y control de aplicaciones, con una extensa variedad de prestaciones avanzadas de red y de flexibilidad de configuración. La serie NSA ofrece una plataforma asequible que puede implementarse y gestionarse con gran facilidad en una gran diversidad de entornos – ya sean redes grandes o distribuidas o redes de sucursales.

Serie NSA como pasarela central



Serie NSA como solución NGFW en línea

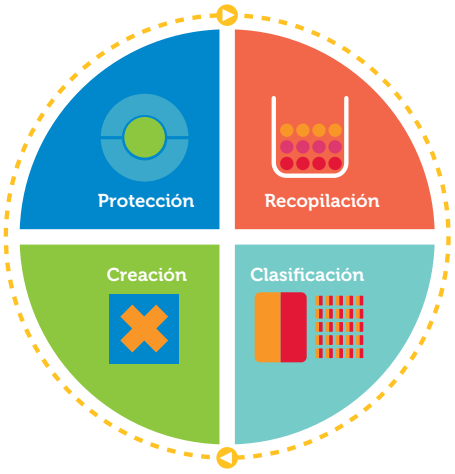


Seguridad y protección

El equipo interno y dedicado de investigación de amenazas de Dell SonicWALL investiga y desarrolla contramedidas para aplicarlas a los firewalls in situ, garantizando así una protección actualizada. Con la ayuda de más de un millón de sensores distribuidos por todo el mundo, obtienen muestras de malware e información telemétrica sobre las últimas amenazas, que a su vez es transmitida a los firewalls para soportar las funciones de prevención de intrusiones, antimalware y detección de aplicaciones.

Los clientes de NGFW de Dell SonicWALL gozan, las 24 horas del día, de una protección contra las amenazas continuamente actualizada. Las nuevas actualizaciones se hacen efectivas inmediatamente sin necesidad de reiniciar el sistema ni interrumpir el servicio. Las definiciones residentes en los dispositivos están diseñadas para ofrecer 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 dispositivos NSA también tienen acceso al servicio de antivirus en la nube (CloudAV) de Dell SonicWALL, que incluye más de doce millones de definiciones. El firewall accede a la base de datos CloudAV mediante un protocolo ligero propietario con el fin de reforzar la inspección realizada en el dispositivo. Gracias a Geo-IP y a las funciones de filtrado botnet, los NGFWs de Dell SonicWALL son capaces de bloquear el tráfico de dominios peligrosos o geografías completas para reducir el perfil de riesgo de la red.



Inteligencia y control de aplicaciones

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

Los análisis del tráfico de aplicaciones de Dell SonicWALL no solo proporcionan una visión granular del tráfico de aplicaciones, del uso del ancho de banda y de las amenazas de seguridad, sino que también ofrecen potentes funciones forenses y de resolución de problemas. Además, el inicio de sesión único (SSO) seguro simplifica la experiencia del usuario, incrementa la productividad y reduce las llamadas al servicio de soporte.

El Sistema de gestión global de Dell SonicWALL (GMS®) simplifica la gestión de la inteligencia y el control de aplicaciones mediante una interfaz intuitiva basada en Web.

Prestaciones

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

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 Dell 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 prevenir la propagación de las amenazas de unas zonas a otras.
Detección y bloqueo de actividades de comando y control (CnC) procedente de ataques botnets	Identifica y bloquea el tráfico de comando y control originado en bots de la red local y dirigido a IPs y dominios identificados como propagadores de malware o conocidos como puntos de CnC.
Detección y prevención de abusos/anomalías de los protocolos	Identifica y bloquea ataques que abusan de los protocolos para intentar eludir el IPS.
Protección de día cero	Protege la red ante los ataques de día cero con actualizaciones constantes contra los últimos métodos y técnicas de exploits, que cubren miles de exploits individuales.
Tecnología antievasión	La amplia normalización de flujos, la descodificación y otras técnicas impiden que las amenazas puedan penetrar la red sin ser detectadas utilizando técnicas de evasión en las capas 2-7.

Prestaciones

Prevención de amenazas	
Prestación	Descripción
Protección antimalware basada en la red	El motor RFDPI de Dell SonicWALL escanea todo el tráfico entrante, saliente y entre zonas en busca de virus, troyanos, key loggers y otros tipos de malware, inspeccionando archivos de tamaño ilimitado y todos los puertos y flujos TCP.
Protección antimalware con CloudAssist	Los servidores de la nube de Dell SonicWALL albergan una base de datos continuamente actualizada de más de 13 millones de definiciones de amenazas que refuerza la base de datos de definiciones integrada en los firewalls y amplía significativamente la cobertura de la RFDPI.
Actualizaciones de seguridad las 24 horas	El equipo de investigación de amenazas de Dell SonicWALL analiza las amenazas nuevas y lanza contramedidas las 24 horas del día, los 7 días de la semana. 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.
Descifrado e inspección SSL	Descifra e inspecciona el tráfico SSL sobre la marcha, sin necesidad de proxies, en busca de malware, intrusiones y filtraciones de datos, y aplica políticas de control de aplicaciones, URL y contenido para ofrecer protección contra las amenazas ocultas en el tráfico cifrado mediante SSL.
Inspección TCP bidireccional (sin procesar)	El motor RFDPI es capaz de escanear flujos TCP sin procesar en cualquier puerto y bidireccionalmente para prevenir ataques que intentan burlar los sistemas de seguridad anticuados, centrados en la protección de algunos puertos conocidos.
Amplio soporte de protocolos	Identifica protocolos comunes, como HTTP/S, FTP, SMTP, SMBv1/v2, entre otros, que no envían datos en TCP sin procesar y descodifica los datos útiles para la inspección antimalware, incluso si no se ejecutan en puertos estándar conocidos.

Inteligencia y control de aplicaciones	
Prestación	Descripción
Control de aplicaciones	Controla las aplicaciones, o prestaciones individuales de las aplicaciones, identificadas por el motor RFDPI gracias a una base de datos en continuo crecimiento de más de 4.300 definiciones de aplicaciones, con el fin de aumentar la seguridad y la productividad de la red.
Identificación personalizada de aplicaciones	Controla las aplicaciones personalizadas creando definiciones basadas en parámetros o patrones específicos únicos de una aplicación en sus comunicaciones de red, con el fin de aumentar el control sobre la red.
Gestión de ancho de banda de aplicaciones	Restringe o prioriza aplicaciones o categorías de aplicaciones con el fin de maximizar la disponibilidad de ancho de banda para las aplicaciones críticas y al mismo tiempo eliminar o reducir el tráfico de aplicaciones no deseadas.
Visualización integrada/ externa del tráfico	Identifica el uso del ancho de banda y analiza el comportamiento de la red con funciones integradas de visualización en tiempo real del tráfico de aplicaciones y funciones externas de informes del tráfico de aplicaciones mediante NetFlow/IPFix.
Control granular	Controla las aplicaciones, o determinados componentes de una aplicación, basándose en programaciones, grupos de usuarios, listas de exclusión y una variedad de acciones con plena identificación de usuarios mediante SSO basado en la integración de LDAP/AD/Terminal Services/Citrix.

Prestaciones

Firewall e interconexión	
Prestación	Descripción
Inspección dinámica de paquetes	Todo el tráfico de la red se inspecciona, se analiza y se somete a las políticas de acceso del firewall.
Protección contra ataques DDoS/DOS	La protección SYN Flood proporciona defensas contra ataques DOS mediante tecnologías de lista negra de capa 3 (SYN proxy) y de capa 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.
Opciones de implementación flexibles	La serie NSA 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.
Alta disponibilidad/ agrupación (clústeres)	La serie NSA soporta los modos de alta disponibilidad Activa/Pasiva con State Synchronization, DPI Activa/Activa y agrupada (clústeres). 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.
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 enrutamientos basados en protocolos para direccionar el tráfico a una determinada conexión WAN, con posibilidad de reconexión a una WAN secundaria en caso de fallo de la alimentación.
QoS avanzada	Garantiza las comunicaciones críticas con etiquetado 802.1p y DSCP y remapeo del tráfico VoIP en la red.
Soporte de Gatekeeper H.323 y proxy SIP	Bloquea las llamadas spam: todas las llamadas entrantes han de ser autorizadas y autenticadas mediante Gatekeeper H.323 o proxy SIP.

Gestión e informes	
Prestación	Descripción
Sistema de gestión global	Dell SonicWALL GMS monitoriza, configura y elabora informes sobre múltiples dispositivos Dell SonicWALL a través de una única consola de gestión con una interfaz intuitiva para reducir la complejidad y los costes de gestión.
Potente gestión de dispositivos individuales	Ofrece una interfaz intuitiva basada en Web que puede configurarse de forma rápida y sencilla, una CLI completa y soporte para SNMPv2/3.
Informes IPFIX/Netflow de flujos de aplicaciones	Exporta los análisis del tráfico de aplicaciones y los datos de uso mediante protocolos IPFIX o NetFlow para la monitorización y la creación de informes en tiempo real e históricos con herramientas como Scrutinizer u otras que ofrezcan soporte para IPFIX y NetFlow con extensiones.

Redes privadas virtuales	
Prestación	Descripción
VPN IPSec para conectividad entre emplazamientos	La VPN IPSec de alto rendimiento permite a la serie NSA 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.

Prestaciones

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.
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.

Visión de conjunto de las prestaciones de SonicOS

Firewall
- Inspección profunda de paquetes sin reensamblado
- Inspección profunda de paquetes para SSL
- Inspección dinámica de paquetes
- Reensamblado TCP
- Modo stealth
- Soporte CAC (Common Access Card)
- Protección contra ataques DOS
- Protección contra ataques UDP/ICMP/SYN Flood

Prevención de intrusiones
- Escaneo basado en definiciones
- Actualizaciones automáticas de las definiciones
- Prevención de amenazas salientes
- Lista de exclusiones IPS
- GeoIP y filtrado basado en la reputación
- Coincidencia de expresiones regulares

Antimalware
- Escaneo antimalware basado en flujos
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Descifrado SSL
- Inspección bidireccional
- Tamaño de archivo ilimitado
- Base de datos de amenazas CloudAV

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

• Filtrado de contenido Web
- Filtrado URL
- Tecnología antiproxy
- Bloqueo en base a palabras clave
- Gestión del ancho de banda según categorías de clasificación CFS
- Modelo de políticas unificadas con control de aplicaciones
- 56 categorías de filtrado de contenido

VPN
- VPN IPSec para conectividad entre emplazamientos
- Acceso remoto mediante SSL VPN o cliente IPSec
- Pasarela VPN redundante
- Mobile Connect para iOS y Android™
- VPN basada en enrutamiento (OSPF, RIP)

Interconexión
- Enrutamiento dinámico
- Controlador inalámbrico SonicPoint
- Enrutamiento basado en políticas
- NAT avanzado
- Servidor DHCP
- Gestión del ancho de banda
- Agregación de enlaces
- 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, Modo Tap, Modo NAT

VoIP
- QoS avanzada
- Gestión del ancho de banda

DPI del tráfico VoIP
- Soporte de Gatekeeper H.323 y proxy SIP

• Gestión y supervisión
- GUI Web
- Interfaz de línea de comandos (CLI)
- SNMPv2/v3
- Informes externos (Scrutinizer)
- Gestión e informes centralizados
- Protocolización
- Exportación IPFix/Netflow
- Visualización del tráfico de aplicaciones
- Gestión centralizada de políticas
- Inicio de sesión único (SSO)
- Soporte de servicios de terminal/Citrix
- Integración de funciones de análisis forense de Solera Networks

Especificaciones del sistema de la serie NSA

	NSA 220/W	NSA 250M/W
Sistema operativo	SonicOS 5.9	
Núcleos de seguridad	2	
Interfaces 1 GbE	7 x 1GbE	5 x 1GbE
Interfaces de gestión	CLI, SSH, GUI, GMS	
Memoria (RAM)	512 MB	512 MB
Expansión	2 USB, tarjeta SD	1 Interfaz modular, 2 USB, tarjeta SD
Rendimiento de inspección de firewall[1]	600 Mbps	750 Mbps
Rendimiento DPI pleno[2]	110 Mbps	130 Mbps
Rendimiento de inspección de aplicaciones[2]	195 Mbps	250 Mbps
Rendimiento IPS[2]	195 Mbps	250 Mbps
Rendimiento de inspección de antimalware[2]	115 Mbps	140 Mbps
Rendimiento IMIX[3]	180 Mbps	210 Mbps
Rendimiento VPN[3]	150 Mbps	200 Mbps
Conexiones por segundo	2.200/seg.	3.000/seg.
Conexiones máximas (SPI)	85.000	110.000
Conexiones máximas (DPI)	32.000	64.000
SonicPoints soportados (máximo)	16	16
Usuarios Inicio de sesión único (SSO)	250	250[4]
VPN	**NSA 220/W**	**NSA 250M/W**
Túneles entre emplazamientos	25	50
Clientes VPN IPSec (máximo)	2 (25)	2 (25)
Licencias SSL VPN (máximo)	2 (15)	2 (15)
Cifrado/Autenticación	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1	
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14	
VPN basada en enrutamiento	RIP, OSPF	
Funciones de red	**NSA 220/W**	**NSA 250M/W**
Asignación de direcciones IP	Estática (DHCP PPPoE, L2TP y cliente PPTP), servidor DHCP interno, DHCP Relay	
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT, modo transparente	
Interfaces VLAN	25	35
Protocolos de enrutamiento	BGP, OSPF, RIPv1/v2, enrutamiento estático, enrutamiento basado en políticas, multicast	
QoS	Prioridad de ancho de banda, ancho de banda máx., ancho de banda garantizado, marcado DSCP, 802.1p	
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos de usuarios interna, Terminal Services, Citrix	
VoIP	H323-v1-5 completo, SIP	
Estándares	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3	
Certificaciones	VPNC, ICSA Firwall, ICSA Anti-Virus	
Certificaciones pendientes	FIPS 140-2, Common Criteria EAL1+	
CAC (Common Access Card)	Soportada	
Wireless	**NSA 220/W**	**NSA 250M/W**
Estándares	802.11a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS	
Puntos de acceso virtuales (VAPs)5–antenas (Diversity de 5 dBi)	Externa triple, extraíble	
Potencia radioeléctrica–802.11a/802.11b/802.11g	15,5 dBm máx./18 dBm máx./17 dBm a 6 Mbps, 13 dBm a 54 Mbps	
Potencia radioeléctrica–802.11n (2,4 GHz)/802.11n (5,0 GHz)	19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15	
Sensibilidad de recepción radioeléctrica–802.11a/802.11b/802.11g	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm a 11Mbps/-91 dBm a 6 Mbps, -74 dBm a 54 Mbps	
Sensibilidad de recepción radioeléctrica–802.11n (2,4 GHz)/802.11n (5,0 GHz)	-89 dBm MCS 0, -70 dBm MCS 15/-95 dBm MCS 0, -76 dBm MCS 15	
Hardware	**NSA 220/W**	**NSA 250M/W**
Fuente de alimentación	36W externa	
Ventiladores	Sin ventiladores/1 ventilador interno	2 ventiladores internos
Potencia de entrada	100-240 V CA, 60-50 Hz	
Consumo máximo de energía (W)	11W/15W	12W/16W
Factor de forma	Escritorio / Disponible kit de montaje en bastidor 1U	
Dimensiones	18,10 x 3,81 x 26,67 cm 7,125 x 1,5 x 10,5 pulgadas	
Peso	0,88 kg/1,95 libras/0,97 kg/2,15 libras	1,38 kg/3,05 libras/1,43 kg/3,15 libras
Peso WEEE	1,38 kg/3,05 libras/1,56 kg/3,45 libras	2,0 kg/4,4 libras/2,11 kg/4,65 libras
Peso de envío	1,97 kg/4,35 libras/2,13 kg/4,7 libras	2,54 kg/5,6 libras/2,68 kg/5,9 libras
Cumplimiento de 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, GOST-R (NSA 220), CU (NSA 250M)	
Entorno	40-105° F, 0-40° C	
Humedad	5-95%, sin condensación	

[1] Métodos de prueba: Rendimiento máximo basado en RFC 2544 (para firewalls). 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. [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. [4] Consulte la última versión de SonicOS 5.9 para el último número de usuarios de SSO. *Uso futuro.

Especificaciones del sistema de la serie NSA

	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Sistema operativo	SonicOS 6.1				
Núcleos de seguridad	4	6	8	10	24
Interfaces 10 GbE	—	2 x 10-GbE SFP+			4 x 10-GbE SFP+
Interfaces 1 GbE	8 x 1 GbE	4 x 1-GbE SFP, 12 x 1 GbE			8 x 1-GbE SFP, 8 x 1 GbE (1 par Bypass de LAN)
Interfaces de gestión	1 GbE, 1 consola				
Memoria (RAM)	2,0 GB			4,0 GB	
Expansión	1 ranura de expansión (trasera)*, tarjeta SD*				
Rendimiento de inspección de firewall[1]	1,9 Gbps	3,4 Gbps	6,0 Gbps	9,0 Gbps	12,0 Gbps
Rendimiento DPI pleno[2]	300 Mbps	500 Mbps	800 Mbps	1,6 Gbps	3,0 Gbps
Rendimiento de inspección de aplicaciones[2]	700 Mbps	1,1 Gbps	2,0 Gbps	3,0 Gbps	4,5 Gbps
Rendimiento IPS[2]	700 Mbps	1,1 Gbps	2,0 Gbps	3,0 Gbps	4,5 Gbps
Rendimiento de inspección de antimalware[2]	400 Mbps	600 Mbps	1,1 Gbps	1,7 Gbps	3,0 Gbps
Rendimiento IMIX[3]	600 Mbps	900 Mbps	1,6 Gbps	2,4 Gbps	3,5 Gbps
Inspección y descifrado SSL (DPI SSL)[2]	200 Mbps	300 Mbps	500 Mbps	800 Mbps	1,3 Gbps
Rendimiento VPN[3]	1,1 Gbps	1,5 Gbps	3,0 Gbps	4,5 Gbps	5,0 Gbps
Conexiones por segundo	15.000/seg.	20.000/seg.	40.000/seg.	60.000/seg.	90.000/seg.
Conexiones máximas (SPI)	225.000	325.000	400.000	750.000	750.000
Conexiones máximas (DPI)	125.000	175.000	200.000	500.000	500.000
SonicPoints soportados (máximo)	32	48	64	96	96
Usuarios Inicio de sesión único (SSO)	250	500	1.000	2.500	4.000
VPN	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Túneles entre emplazamientos	75	800	1.500	4.000	6.000
Clientes VPN IPSec (máximo)	10 (250)	50 (1.000)	500 (3.000)	2.000 (4.000)	2.000 (6.000)
Licencias SSL VPN (máximo)	2 (25)	2 (30)	2 (30)	2 (50)	2 (50)
Cifrado/Autenticación	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1				
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14				
VPN basada en enrutamiento	RIP, OSPF				
Funciones de red	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Asignación de direcciones IP	Estática (DHCP PPPoE, L2TP y cliente PPTP), servidor DHCP interno, DHCP Relay				
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT, modo transparente				
Interfaces VLAN	50	50	200	400	500
Protocolos de enrutamiento	BGP, OSPF, RIPv1/v2, enrutamiento estático, enrutamiento basado en políticas, multicast				
QoS	Prioridad de ancho de banda, ancho de banda máx., ancho de banda garantizado, marcado DSCP, 802.1p				
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos de usuarios interna, Terminal Services, Citrix				
VoIP	H323-v1-5 completo, SIP				
Estándares	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certificaciones	VPNC, ICSA Firwall, ICSA Anti-Virus				
Certificaciones pendientes	FIPS 140-2, Common Criteria EAL1+				
Common Access Card (CAC)	Pendiente				
Hardware	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Fuente de alimentación	200W	Una, fija 250W			
Ventiladores	Dos, fijos				Dos, redundantes, de cambio en caliente
Potencia de entrada	100-240 V CA, 60-50 Hz				
Consumo máximo de energía (W)	49,4	74,3	86,7	90,9	113,1
Factor de forma	Preparado para montaje en bastidor 1U				
Dimensiones	(4,5 x 26 x 43 cm) 1,75 x 10,25 x 17 pulgadas	(4,5 x 48,5 x 43 cm) 1,75 x 19,1 x 17 pulgadas			
Peso	4,6 kg (10,1 libras)	6,15 Kg (13,56 libras)			6,77 Kg (14,93 libras)
Peso WEEE	5,0 kg (11,0 libras)	6,46 Kg (14,24 libras)			8,97 Kg (19,78 libras)
Peso de envío	6,5 kg (14,3 libras)	9,43 Kg (20,79 libras)			11,85 Kg (26,12 libras)
Cumplimiento de normas	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/GS, CB, Mexico CoC by UL, WEEE, REACH, ANATEL, BSMI, CU				
Entorno	0-40° C, 32-105° F				
Humedad	10–90%, sin condensación.				
MTBF (años)	20,2	16,8	16,0	15,4	13,3

[1] Métodos de prueba: Rendimiento máximo basado en RFC 2544 (para firewalls). 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. [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.

Información de pedido de la serie NSA

Producto	Nº producto
NSA 220 TotalSecure (1 año)	01-SSC-9744
NSA 220 Wireless-N TotalSecure (1 año)	01-SSC-9746
NSA 250M TotalSecure (1 año)	01-SSC-9747
NSA 250M Wireless-N TotalSecure (1 año)	01-SSC-9749
NSA 2600 TotalSecure (1 año)	01-SSC-3863
NSA 3600 TotalSecure (1 año)	01-SSC-3853
NSA 4600 TotalSecure (1 año)	01-SSC-3843
NSA 5600 TotalSecure (1 año)	01-SSC-3833
NSA 6600 TotalSecure (1 año)	01-SSC-3823
NSA 220W y 220 Wireless-N: suscripciones de soporte y seguridad	**Nº producto**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention, Content Filtering con soporte para NSA 220 (1 año)	01-SSC-4648
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSA 220 (1 año)	01-SSC-4612
Soporte dinámico para NSA 220 (1 año)	01-SSC-4630
Content Filtering Premium Business Edition para NSA 220 (1 año)	01-SSC-4618
Comprehensive Anti-Spam Service para NSA 220 (1 año)	01-SSC-4642
NSA 250M y 250M Wireless-N: suscripciones de soporte y seguridad	**Nº producto**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention, Content Filtering con soporte para NSA 250M (1 año)	01-SSC-4606
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSA 250M (1 año)	01-SSC-4570
Soporte dinámico para NSA 250M (1 año)	01-SSC-4588
Content Filtering Premium Business Edition para NSA 250M (1 año)	01-SSC-4576
Comprehensive Anti-Spam Service para NSA 250M (1 año)	01-SSC-4600
NSA 2600: suscripciones de soporte y seguridad	**Nº producto**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention, Content Filtering con soporte para NSA 2600 (1 año)	01-SSC-4453
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSA 2600 (1 año)	01-SSC-4459
Soporte Silver 24x7 para NSA 2600 (1 año)	01-SSC-4314
Content Filtering Premium Business Edition para NSA 2600 (1 año)	01-SSC-4465
Comprehensive Anti-Spam Service para NSA 2600 (1 año)	01-SSC-4471
NSA 3600: suscripciones de soporte y seguridad	**Nº producto**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention, Content Filtering con soporte para NSA 3600 (1 año)	01-SSC-4429
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSA 3600 (1 año)	01-SSC-4435
Soporte Silver 24x7 para NSA 3600 (1 año)	01-SSC-4302
Content Filtering Premium Business Edition para NSA 3600 (1 año)	01-SSC-4441
Comprehensive Anti-Spam Service para NSA 3600 (1 año)	01-SSC-4447
NSA4600: suscripciones de soporte y seguridad	**Nº producto**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention, Content Filtering con soporte para NSA 4600 (1 año)	01-SSC-4405
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSA 4600 (1 año)	01-SSC-4411
Soporte Silver 24x7 para NSA 4600 (1 año)	01-SSC-4290
Content Filtering Premium Business Edition para NSA 4600 (1 año)	01-SSC-4417
Comprehensive Anti-Spam Service para NSA 4600 (1 año)	01-SSC-4423

Información de pedido de la serie NSA

NSA 5600: suscripciones de soporte y seguridad	Nº producto
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention, Content Filtering con soporte para NSA 5600 (1 año)	01-SSC-4234
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSA 5600 (1 año)	01-SSC-4240
Soporte Gold 24x7 para NSA 5600 (1 año)	01-SSC-4284
Content Filtering Premium Business Edition para NSA 5600 (1 año)	01-SSC-4246
Comprehensive Anti-Spam Service para NSA 5600 (1 año)	01-SSC-4252
NSA 6600: suscripciones de soporte y seguridad	**Nº producto**
Comprehensive Gateway Security Suite – Application Intelligence, Threat Prevention, Content Filtering con soporte para NSA 6600 (1 año)	01-SSC-4210
Prevención de amenazas – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSA 6600 (1 año)	01-SSC-4216
Soporte Gold 24x7 para NSA 6600 (1 año)	01-SSC-4278
Content Filtering Premium Business Edition para NSA 6600 (1 año)	01-SSC-4222
Comprehensive Anti-Spam Service para NSA 6600 (1 año)	01-SSC-4228
Módulos y accesorios*	**Nº producto**
Módulo de corto alcance 10GBASE-SR SFP+	01-SSC-9785
Módulo de largo alcance 10GBASE-LR SFP+	01-SSC-9786
Cable Twinax (1M) 10GBASE SFP+	01-SSC-9787
Cable Twinax (3M) 10GBASE SFP+	01-SSC-9788
Módulo de corta distancia 1000BASE-SX SFP	01-SSC-9789
Módulo de larga distancia 1000BASE-LX SFP	01-SSC-9790
Módulo de cobre 1000BASE-T SFP	01-SSC-9791
Kit de montaje en bastidor para NSA 220/250M	**Nº producto**
Kit de montaje en bastidor para NSA 220	01-SSC-9212
Kit de montaje en bastidor para NSA 250M	01-SSC-9211
Módulos de expansión para NSA 250M	**Nº producto**
Módulo de expansión GbE de 4 puertos para la serie NSA 250M	01-SSC-8619
Módulo SFP de 2 puertos	01-SSC-8826
Módulo M1 T1/E1 de 1 puerto	01-SSC-8829
Módulo ADSL de 1 puerto Annex A M1	01-SSC-8827
Módulo ADSL de 1 puerto Annex B M1	01-SSC-8828
Módulo GbE M1 de 2 puertos con bypass LAN	01-SSC-8830
Gestión e informes	**Nº producto**
Licencia de software Dell SonicWALL GMS de 10 nodos	01-SSC-3363
Soporte de software E-Class 24x7 de 10 nodos para Dell SonicWALL GMS (1 año)	01-SSC-6514
Dell SonicWALL Scrutinizer Virtual Appliance con licencia de software para módulo Flow Analytics, hasta 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-3443
Dell SonicWALL Scrutinizer con licencia de software para el módulo Flow Analytics, hasta 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-4002
Dell SonicWALL Scrutinizer con licencia de software para el módulo Advanced Reporting, hasta 5 nodos (incluye un año de soporte de software 24x7)	01-SSC-3773

*Si desea obtener una lista completa de los módulos SFP y SFP+ soportados, consulte a un ingeniero de productos de seguridad de Dell

Números de modelo:

NSA 220–APL24-08E
NSA 220 W–APL24-08F
NSA 250M–APL25-090
NSA 250M W–APL25-091
NSA 2600–1RK29-0A9
NSA 3600–1RK26-0A2
NSA 4600–1RK26-0A3
NSA 5600–1RK26-0A4
NSA 6600–1RK27-0A5

Si desea obtener más información:

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300