

Network Security Appliance (NSa) Datasheet

Seguridad para redes medianas, empresas distribuidas y centros de datos con altos niveles de rendimiento y efectividad validados por la industria

La serie SonicWall Network Security appliance (NSa) proporciona a organizaciones que abarcan desde redes medianas hasta empresas distribuidas y centros de datos funciones de prevención de amenazas avanzadas en una plataforma de seguridad de alto rendimiento. Utilizando innovadoras tecnologías de aprendizaje profundo en la plataforma SonicWall Capture Cloud, la serie NSa proporciona las funciones de detección y prevención de violaciones de seguridad en tiempo real y automatizadas que las organizaciones necesitan.

Prevención de amenazas innovadora con un rendimiento superior

Las amenazas de red de hoy en día son altamente evasivas y cada vez más difíciles de identificar utilizando métodos de detección tradicionales. Para mantenerse un paso por delante de los ataques sofisticados es necesario adoptar un enfoque más moderno que utilice ampliamente inteligencia de seguridad en la nube. Sin esa inteligencia en la nube, las soluciones de seguridad en la pasarela no pueden seguir el ritmo de las amenazas complejas de hoy en día. Los firewalls de próxima generación (NGFWs) de la serie NSa integran dos tecnologías de seguridad avanzadas para proporcionar funciones innovadoras de prevención de amenazas que mantienen su red un paso por delante. El servicio multimotor Capture Advanced Threat Protection (ATP) de SonicWall se ve mejorado por nuestra tecnología pendiente de patente de Inspección de memoria profunda en tiempo real (RTDMI™). El motor RTDMI detecta y bloquea de forma proactiva las amenazas de día cero y el malware desconocido del mercado de masas inspeccionando directamente la memoria. Debido a la arquitectura en tiempo real, la

tecnología SonicWall RTDMI es precisa, minimiza los falsos positivos e identifica y reduce los ataques sofisticados en los que el armamento del malware queda expuesto durante menos de 100 nanosegundos. En combinación con ella, el motor patentado* de Inspección profunda de paquetes sin reensamblado (RFDPI) de SonicWall examina cada byte de cada paquete, inspeccionando el tráfico entrante y saliente 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 NSa bloquea incluso las amenazas más peligrosas en la pasarela.

Además, los firewalls de SonicWall proporcionan una protección completa al descifrar e inspeccionar las conexiones cifradas mediante TLS/SSL y SSH, independientemente del puerto o protocolo. El firewall examina cada paquete en profundidad (encabezado y datos) en busca de incumplimientos 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 (C y C) 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.

Cuando las organizaciones activan funciones de inspección profunda de paquetes, como IPS, antivirus, antispysware, descifrado/inspección TLS/SSL, etc., en sus firewalls, el rendimiento de la red a menudo se ralentiza, en ocasiones de forma drástica. Los



Ventajas:

- Prevención de amenazas y rendimiento superiores
- Tecnología de Inspección profunda de memoria en tiempo real pendiente de patente
- Tecnología patentada de inspección profunda de paquetes sin reensamblado
- Prevención de amenazas integrada y basada en la nube
- Descifrado e inspección TLS/SSL
- Efectividad de la seguridad validada por la industria
- Arquitectura de hardware multinúcleo
- Equipo dedicado de investigación de amenazas Capture Labs

Control y flexibilidad de la red

- Secure SD-WAN
- Potente sistema operativo SonicOS
- Inteligencia y control de aplicaciones
- Segmentación de la red con VLANs
- Seguridad inalámbrica de alta velocidad

Funciones sencillas de implementación, configuración y gestión continua

- Implementación Zero-Touch
- Gestión centralizada, basada en la nube y local
- Línea de cortafuegos escalables
- TCO reducido

firewalls de la serie NSa, sin embargo, ofrecen una arquitectura de hardware multinúcleo con microprocesadores 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 NSa utiliza como base SonicOS, el sistema operativo de SonicWall, que ofrece gran cantidad de prestaciones. 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 anti evasión, redes privadas virtuales (VPN) de alta velocidad y otras prestaciones de seguridad robustas.

Gracias a las funciones de inteligencia y control de aplicaciones, los administradores de las redes pueden identificar las aplicaciones productivas y distinguir las 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 ofrece una visión granular del tráfico de toda la red.

Para las organizaciones distribuidas que requieran flexibilidad avanzada en el diseño de su red, la tecnología SD-WAN en SonicOS es un complemento perfecto de los firewalls NSa instalados en oficinas centrales o en ubicaciones remotas y sucursales. En lugar de confiar en tecnologías existentes más caras, como MPLS y T1, las organizaciones que utilizan SD-WAN pueden elegir servicios de Internet públicos más económicos sin dejar de disfrutar de un alto nivel de disponibilidad de las aplicaciones, así como de un rendimiento predecible.

Cada firewall NSa tiene integrado un controlador de acceso inalámbrico que permite a las organizaciones ampliar el perímetro de la red de forma segura mediante el uso de tecnología inalámbrica. Los firewalls de SonicWall, junto con los access points inalámbricos SonicWave 802.11ac Wave 2, crean una solución de seguridad de red inalámbrica que combina tecnología de firewall de próxima generación líder en la industria con conectividad inalámbrica de alta velocidad para ofrecer una seguridad de red y un rendimiento inalámbricos de alta velocidad y clase empresarial en toda la red inalámbrica.

Funciones sencillas de implementación, configuración y gestión continua

Como todos los firewalls de SonicWall, la serie NSa integra estrechamente tecnologías clave de seguridad, conectividad y flexibilidad en una única solución completa. Ello incluye access points inalámbricos SonicWave y la serie SonicWall WAN Acceleration (WXA), todos ellos detectados y puestos a disposición de forma automática por el firewall NSa de gestión. La consolidación de múltiples prestaciones elimina la necesidad de comprar e instalar productos puntuales que no siempre funcionan bien juntos. De este modo, se reduce el esfuerzo que implican la implementación de la solución en la red y su configuración, ahorrando así tiempo y dinero.

Las funciones de gestión, informes, licencias y análisis en la nube se centralizan en el SonicWall Capture Security Center. Un componente clave del Capture Security Center es la implementación sin necesidad de intervención. Esta prestación basada en la nube simplifica y acelera la implementación y el aprovisionamiento de los cortafuegos SonicWall en ubicaciones remotas y sucursales. 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.

Tecnología inalámbrica segura de alta velocidad

Combine un firewall de próxima generación de la serie NSa con un access point inalámbrico SonicWall SonicWave 802.11ac Wave 2 para crear una solución de seguridad de red inalámbrica de alta velocidad. Los firewalls de la serie NSa y los access points SonicWave incluyen puertos de 2,5 GbE que permiten el rendimiento inalámbrico multigigabit que ofrece la tecnología inalámbrica Wave 2. El firewall escanea todo el tráfico inalámbrico que entra y sale de la red utilizando tecnología de inspección profunda de paquetes y, a continuación, elimina las amenazas dañinas, como el malware y las intrusiones, incluso a través de conexiones cifradas. Se pueden utilizar prestaciones de seguridad y control adicionales en la red inalámbrica, como el filtrado de contenido, control e inteligencia de aplicaciones y Capture Advanced Threat Protection, para proporcionar capas adicionales de protección.



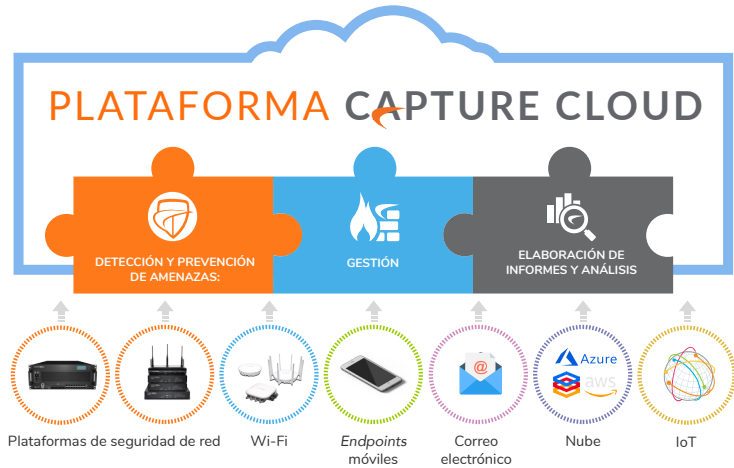
Plataforma Capture Cloud

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 se detecta que los datos que acceden a la red contienen código malicioso nunca visto hasta el momento, el equipo de investigación de amenazas interno y dedicado de SonicWall Capture Labs, desarrolla 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, cubriendo decenas de miles de amenazas individuales. Además de las contramedidas integradas en el dispositivo, los firewalls NSa también tienen acceso continuo a la base de datos de la plataforma Capture Cloud, que incluye decenas de millones de definiciones.

Junto con la prevención de amenazas, la plataforma Capture Cloud ofrece también 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 infracciones automatizada y en tiempo real de SonicWall se basa en dos tecnologías avanzadas de detección de malware: Capture Advanced Threat Protection™ (Capture ATP) y Capture Security appliance™ (CSa).

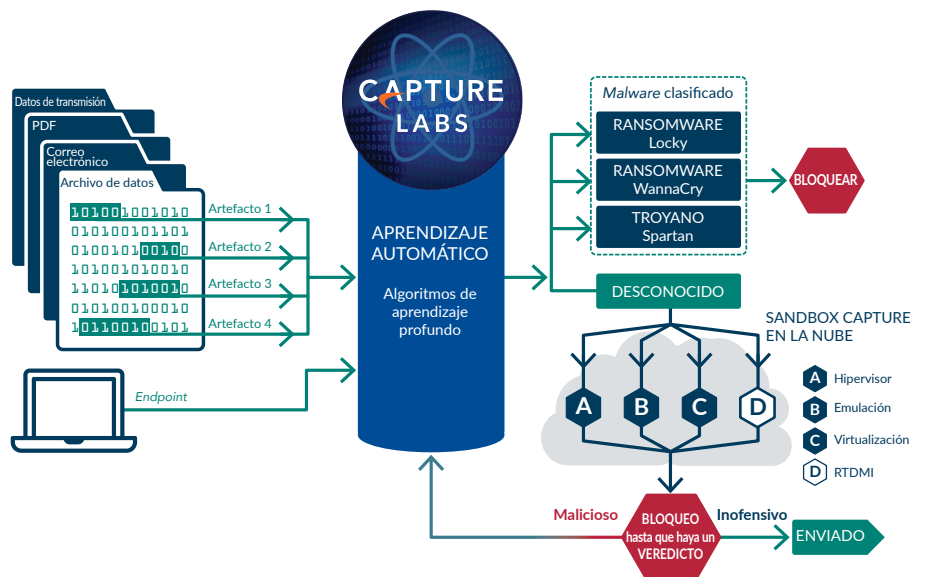
Capture ATP es una plataforma de sandbox multi-motor en la nube, que incluye Real-Time Deep Memory Inspection™ (RTDMI), sandboxing virtualizado, emulación completa de sistema y tecnología de análisis a nivel hipervisor. CSa es un dispositivo local equipado con RTDMI, que utiliza técnicas estáticas y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

Los archivos sospechosos se envían a una de estas soluciones, donde se analizan utilizando algoritmos de aprendizaje profundo, con la opción de retenerlos en la gateway hasta que se emita un veredicto.

En el caso de Capture ATP, se bloquean los archivos identificados como maliciosos y se crea inmediatamente un hash dentro de la base de datos de Capture ATP para que todos los clientes puedan aprovecharlo para bloquear los posteriores ataques. Estas definiciones se envían después a los firewalls para crear defensas estáticas. Por razones legales y de privacidad, los resultados generados por CSa no se comparten fuera de su organización.

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

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



Motor de inspección profunda de paquetes sin reensamblado

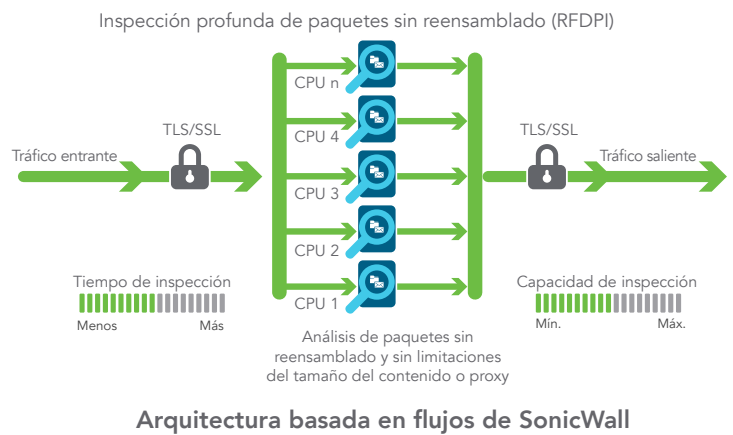
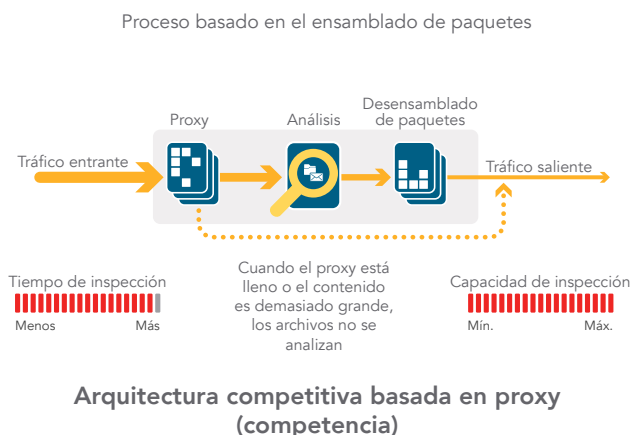
La Inspección profunda de paquetes sin reensamblado (RFDPI) de SonicWall es un sistema de inspección de paso único y baja latencia que realiza análisis bidireccionales del tráfico basados en flujos a alta velocidad sin almacenamiento en búfer ni proxys a fin de descubrir posibles intentos de intrusión 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 cortafuegos 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.



Elaboración de informes y gestión centralizadas

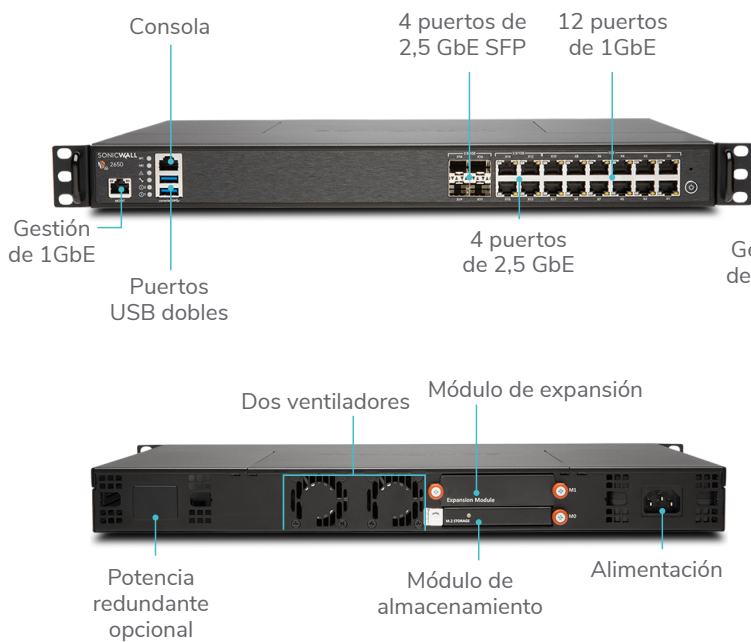
Para organizaciones altamente reguladas que deseen coordinar la seguridad, el control, el cumplimiento normativo y su estrategia de gestión de riesgos, SonicWall proporciona a los administradores una plataforma unificada, segura y ampliable para gestionar los cortafuegos, puntos

de acceso inalámbricos y switches de la serie N y la serie X de Dell 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 cortafuegos mediante la automatización del flujo de trabajo, que proporciona la agilidad y la confianza necesarias para implementar las políticas de cortafuegos apropiadas en el momento oportuno y de conformidad con la normativa vigente. Disponible de forma local como Sistema de gestión global de SonicWall y en la nube como Centro de seguridad de Capture, las soluciones de gestión e informes de SonicWall proporcionan una forma coherente de gestionar la seguridad de la red mediante procesos de negocio y niveles de servicio. De esta forma simplifican drásticamente la gestión del ciclo de vida de sus entornos de seguridad, en comparación con la gestión dispositivo por dispositivo.

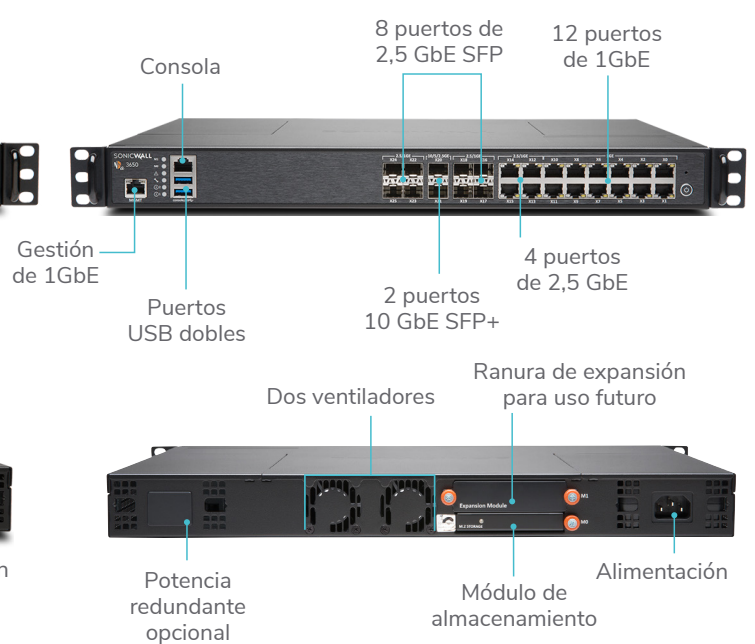
NSa 2650

El firewall NSa 2650 proporciona a organizaciones medianas y empresas distribuidas funciones de prevención de amenazas de alta velocidad a través de miles de conexiones cifradas y aún más si no son cifradas.



NSa 3650

El firewall NSa 3650 de SonicWall 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.

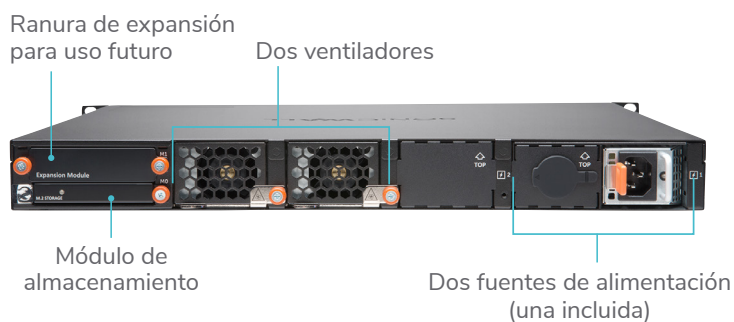
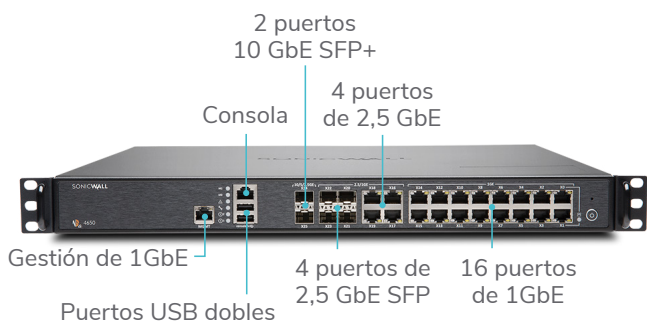


Firewall	NSa 2650
Rendimiento del firewall	3,0 Gbps
Rendimiento IPS	1,4 Gbps
Rendimiento de antimalware	1,3 Gbps
Rendimiento de prevención de amenazas	1,5 Gbps
Máximo de conexiones	1.000.000
Nuevas conexiones/s	14.000/s
Módulo de almacenamiento	16 GB
Descripción	SKU
Solo firewall NSa 2650	01-SSC-1936
NSa 2650 TotalSecure Advanced (1 año)	01-SSC-1988

Firewall	NSa 3650
Rendimiento del firewall	3,75 Gbps
Rendimiento IPS	1,8 Gbps
Rendimiento de antimalware	1,5 Gbps
Rendimiento de prevención de amenazas	1,75 Gbps
Máximo de conexiones	2.000.000
Nuevas conexiones/s	14.000/s
Módulo de almacenamiento	32 GB
Descripción	SKU
Solo firewall NSa 3650	01-SSC-1937
NSa 3650 TotalSecure Advanced (1 año)	01-SSC-4081

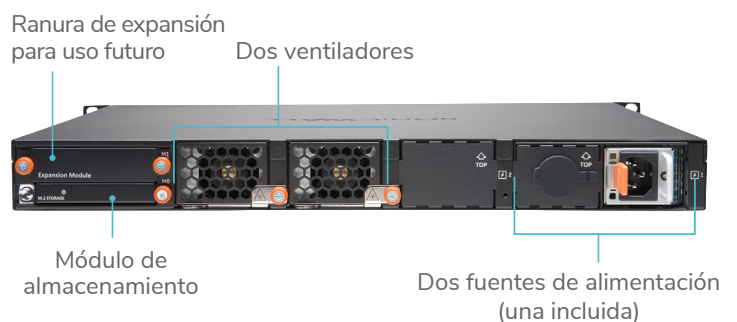
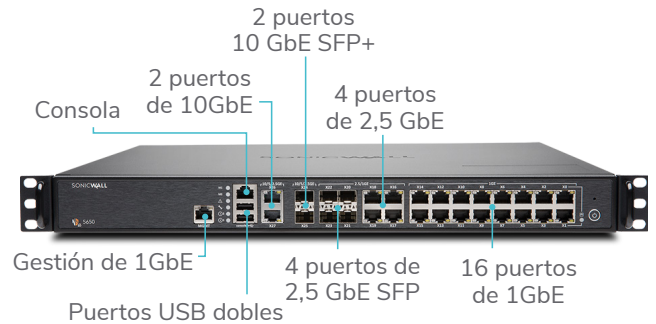
NSa 4650

SonicWall NSa 4650 protege las organizaciones medianas en crecimiento y las sucursales con funciones de clase empresarial y un rendimiento absoluto.



NSa 5650

SonicWall NSa 5650 es ideal para entornos corporativos, redes distribuidas y sucursales que requieren una capacidad de transferencia de datos considerable y una alta densidad de puertos.

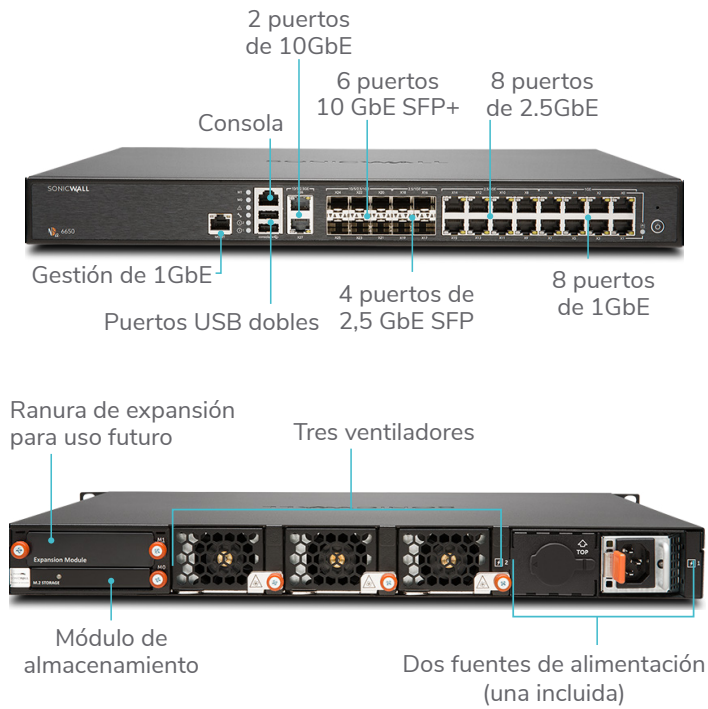


Firewall	NSa 4650
Rendimiento del firewall	6,0 Gbps
Rendimiento IPS	2,3 Gbps
Rendimiento de antimalware	2,45 Gbps
Rendimiento de prevención de amenazas	2,5 Gbps
Máximo de conexiones	3.000.000
Nuevas conexiones/s	40.000/s
Módulo de almacenamiento	32 GB
Descripción	SKU
Solo firewall NSa 4650	01-SSC-1938
NSa 4650 TotalSecure Advanced (1 año)	01-SSC-4094

Firewall	NSa 5650
Rendimiento del firewall	6,25 Gbps
Rendimiento IPS	3,4 Gbps
Rendimiento de antimalware	2,8 Gbps
Rendimiento de prevención de amenazas	3,4 Gbps
Máximo de conexiones	4.000.000
Nuevas conexiones/s	40.000/s
Módulo de almacenamiento	64 GB
Descripción	SKU
Solo firewall NSa 5650	01-SSC-1939
NSa 5650 TotalSecure Advanced (1 año)	01-SSC-4342

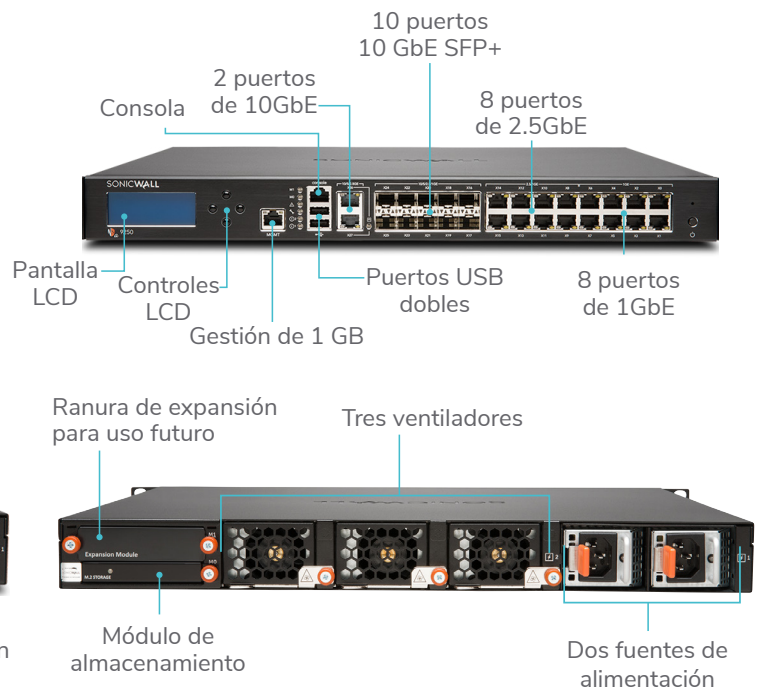
NSa 6650

SonicWall NSa 6650 es ideal para emplazamientos distribuidos y sedes corporativas de gran tamaño que requieren una elevada capacidad de transferencia de datos y un alto nivel de rendimiento.



NSa 9250/9450/9650

SonicWall NSa 9250/9450/9650 proporcionan a las empresas distribuidas y los centros de datos una seguridad profunda escalable a velocidades multigigabit.



Firewall	NSa 6650
Rendimiento del firewall	12,0 Gbps
Rendimiento IPS	6,0 Gbps
Rendimiento de antimalware	5,4 Gbps
Rendimiento de prevención de amenazas	5,5 Gbps
Máximo de conexiones	5.000.000
Nuevas conexiones/s	90.000/s
Módulo de almacenamiento	64 GB

Descripción	SKU
Solo firewall NSa 6650	01-SSC-1940
NSa 6650 TotalSecure Advanced (1 año)	01-SSC-2209

Firewall	NSa 9250	NSa 9450	NSa 9650
Rendimiento del firewall	12,0 Gbps	17,1 Gbps	17,1 Gbps
Rendimiento IPS	7,2 Gbps	10,2 Gbps	10,3 Gbps
Rendimiento de antimalware	6,5 Gbps	8,0 Gbps	8,5 Gbps
Rendimiento de prevención de amenazas	6,5 Gbps	9,0 Gbps	9,4 Gbps
Máximo de conexiones	7.500.000	10.000.000	12.500.000
Nuevas conexiones/s	90.000/s	130.000/s	130.000/s
Módulos de almacenamiento	1 TB, 128 GB	1 TB, 128 GB	1 TB, 256 GB

Descripción	SKU	SKU	SKU
Solo firewalls NSa	01-SSC-1941	01-SSC-1942	01-SSC-1943
NSa TotalSecure Advanced (1 año)	01-SSC-2854	01-SSC-4358	01-SSC-3475

Prestaciones

MOTOR RFDPI	
Función	Descripción
Inspección profunda de paquetes sin reensamblado (RFDPI)	Este motor de inspección de alto rendimiento patentado y propietario realiza análisis bidireccionales del tráfico basados en flujos sin almacenamiento en búfer ni proxys 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.
Función	Descripción
Secure SD-WAN	Secure SD-WAN ofrece una alternativa a las tecnologías más caras, como MPLS, y permite a las organizaciones empresariales distribuidas crear, operar y gestionar redes seguras de alto rendimiento en emplazamientos remotos con el fin de compartir datos, aplicaciones y servicios utilizando servicios de Internet públicos, de bajo coste y fácilmente disponibles.
API REST	Permiten al firewall recibir y utilizar cualquier información de inteligencia propietaria, de fabricantes de equipos originales o de terceros para combatir las amenazas avanzadas como los ataques de día cero, usuarios internos maliciosos, credenciales comprometidas, ransomware y amenazas persistentes avanzadas.
Inspección dinámica de paquetes	Todo el tráfico de la red se inspecciona, se analiza y se somete a las políticas de acceso del firewall.
Alta disponibilidad/agrupación (clústeres)	La serie NSa soporta los modos de alta disponibilidad Activa/Pasiva (A/P) con sincronización de estado, DPI Activa/Activa (A/A) y agrupación (clústeres) Activa/Activa. La DPI Activa/Activa desvía la carga de la inspección profunda de paquetes a los núcleos del dispositivo pasivo con el fin de mejorar el rendimiento.
Protección contra ataques DDoS/DOS	La protección contra inundaciones SYN proporciona una defensa contra los ataques 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 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 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.
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 reasignación del tráfico VoIP en la red.
Soporte de Gatekeeper H.323 y proxy SIP	Bloquea las llamadas spam: todas las llamadas entrantes han de ser autorizadas y autenticadas mediante Gatekeeper H.323 o proxy SIP.
Gestión de switches individuales y en cascada de las series N y X de Dell.	Gestione los ajustes de seguridad de los puertos adicionales, incluidos Portshield, HA, PoE y PoE+, desde una única consola utilizando el panel de gestión del firewall para el switch de red de las series Dell N y Dell X.
Autenticación biométrica	Soporta la autenticación de dispositivos móviles, como el reconocimiento de huellas dactilares, que no pueden ser fácilmente duplicadas ni compartidas, con el fin de autenticar la identidad del usuario de forma segura para que pueda acceder a la red.
Autenticación abierta e inicio de sesión social	Permite a los usuarios invitados utilizar sus credenciales de servicios de redes sociales, como Facebook, Twitter o Google+, para iniciar sesión y acceder a Internet y a otros servicios para usuarios invitados mediante una conexión inalámbrica de un host, una LAN o zonas DMZ, utilizando una autenticación de paso a través.
GESTIÓN E INFORMES	
Función	Descripción
Gestión basada en la nube y local	Funciones de configuración y gestión de los dispositivos SonicWall disponibles en la nube a través del SonicWall Capture Security Center y localmente utilizando el Sistema de gestión global (GMS) de SonicWall.
Potente gestión de dispositivos individuales	Ofrece una interfaz intuitiva basada en Web que puede configurarse de forma rápida y sencilla, una interfaz de línea de comandos completa y soporte para SNMPv2/3.
Informes IPFIX/Netflow de flujos de aplicaciones	Exporta análisis del tráfico de aplicaciones y datos de uso mediante protocolos IPFIX o NetFlow para supervisar y elaborar informes en tiempo real y de datos antiguos con herramientas como SonicWall Scrutinizer u otras compatibles con IPFIX y NetFlow con extensiones.
REDES PRIVADAS VIRTUALES (VPN)	
Función	Descripción
VPN con aprovisionamiento automático	Simplifica y reduce al máximo la complejidad de las implementaciones de firewalls distribuidas automatizando el aprovisionamiento inicial de la pasarela VPN de extremo a extremo entre los firewalls de SonicWall, mientras que los sistemas de seguridad y conectividad funcionan de forma instantánea y automática.
VPN 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 correos electrónicos, 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 endpoints puede redirigirse fácilmente a través de rutas alternativas.

RECONOCIMIENTO DE CONTENIDO/CONTEXTUAL

Función	Descripción
Seguimiento de la actividad de los usuarios	La identificación de usuario y la actividad están disponibles a través de la integración fluida de AD/LDAP/Citrix/Terminal Services SSO en combinación con una amplia información obtenida a través de DPI.
GeolP – 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 violaciones de seguridad

CAPTURE ADVANCED THREAT PROTECTION

Función	Descripción
Sandbox multimotor	La plataforma de sandbox multimotor, que incluye sandboxing virtualizado, emulación de sistema completo y tecnología de análisis de nivel de hipervisor, ejecuta el código sospechoso y analiza su comportamiento, proporcionando una visibilidad completa de la actividad maliciosa.
Inspección de memoria profunda en tiempo real (RTDMI)	Esta tecnología basada en la nube, pendiente de patente, detecta y bloquea el malware que no presenta ningún comportamiento malicioso y oculta su armamento mediante cifrado. Al obligar al malware a revelar su armamento a la memoria, el motor RTDMI detecta y bloquea de forma proactiva las amenazas de mercado masivo, de día cero y el malware desconocido.
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, ya sea de forma individual o en grupo, como los programas ejecutables (PE), DLL, PDF, documentos MS Office, archivos, JAR y APK, así como múltiples sistemas operativos, como Windows, Android, Mac OS X y entornos multinavegador.
Rápida implementación de definiciones	Cuando se detecta un archivo malicioso, inmediatamente se pone una definición a disposición de los firewalls con suscripción a SonicWall Capture ATP y se envía a las bases de datos de definiciones de Gateway Anti-Virus e IPS ya las bases de datos de reputación de URL, IP y dominios en el transcurso de 48 horas.
Capture Client	Capture Client es una plataforma de cliente unificada que proporciona múltiples prestaciones de protección de endpoints, como protección de malware avanzada y soporte para la visibilidad del tráfico cifrado. Utiliza tecnologías de protección multicapa, funciones completas de informes y prestaciones de refuerzo de protección de endpoints.

CAPTURE SECURITY APPLIANCE (CSa)

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

PREVENCIÓN DE AMENAZAS CIFRADAS

Función	Descripción
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico cifrado mediante TLS/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. Incluido con las suscripciones de seguridad para todos los modelos de la serie NSa.
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

Función	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 IP 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

Función	Descripción
Antimalware en pasarela	El motor RFDPI analiza todo el tráfico entrante, saliente y dentro de una misma zona en busca de virus, troyanos, registradores de pulsaciones de teclas y otros tipos de malware en archivos de una longitud y un tamaño ilimitados en todos los puertos y flujos de TCP.
Protección 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 amenazas se transfieren automáticamente a los firewalls con servicios de seguridad activos, donde se hacen efectivas inmediatamente sin necesidad de reiniciar el sistema ni interrumpir el servicio.
Inspección TCP bidireccional (sin procesar)	El motor RFDPI puede analizar flujos de TCP sin procesar en cualquier puerto y en ambas direcciones, con lo que se previenen los ataques que intentan infiltrarse por sistemas de seguridad desactualizados que se centran en proteger solo algunos puertos más conocidos.
Amplio soporte de protocolos	Identifica protocolos comunes, como HTTP/S, FTP, SMTP, SMBv1/v2 y otros tipos, que no envían datos en TCP sin procesar, y descodifica cargas útiles para la inspección de malware, incluso si no se ejecutan en puertos estándares y bien conocidos.

INTELIGENCIA Y CONTROL DE APLICACIONES

Función	Descripción
Control de aplicaciones	Controle aplicaciones, o funciones de aplicaciones individuales, identificadas por el motor RFDPI mediante su cotejo con una base de datos en continuo crecimiento de miles de definiciones de aplicaciones, con el objetivo de aumentar la seguridad y la productividad de la red.
Identificación personalizada de aplicaciones	Controle las aplicaciones personalizadas creando definiciones basadas en parámetros específicos o patrones exclusivos de una aplicación en sus comunicaciones de red para conseguir un mayor control de la red.
Gestión del ancho de banda de las aplicaciones	Asigne y regule de forma detallada el ancho de banda disponible para aplicaciones o categorías de aplicaciones críticas, a la vez que limita el tráfico de aplicaciones no esenciales.
Control granular	Controle aplicaciones (o componentes específicos de una aplicación) basándose en programaciones, grupos de usuarios, listas de exclusión y una gama de acciones con una completa identificación de usuario mediante SSO a través de la integración de LDAP/AD/Terminal Services/Citrix.

FILTRADO DE CONTENIDO

Función	Descripción
Filtrado de contenido dentro y fuera	Aplique políticas de usos aceptables y bloquee el acceso a sitios Web HTTP/HTTPS que contengan información o imágenes inaceptables o improductivas con Content Filtering Service y Content Filtering Client.
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 IMPUESTOS

Función	Descripción
Protección en varios niveles	Utilice las funciones del firewall, como la primera capa de defensa en el perímetro, junto con la protección de endpoints, a fin de bloquear los virus que penetran en la red por medio de portátiles, unidades de memoria flash y otros sistemas no protegidos.
Opción de aplicación automatizada	Asegúrese de que todos los equipos que accedan a la red tengan 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 antispymware 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 antispymware	La potente función de protección antispymware 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.

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
- API REST

Descifrado e inspección TLS/SSL/SSH¹

- 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 Protection¹

- Inspección profunda de memoria 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 intrusiones¹

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

Antimalware¹

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

Identificación de aplicaciones¹

- 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
- Análisis basados en la nube

Filtrado de contenido web HTTP/HTTPS¹

- Filtrado de URL
- Punteo de proxys
- Bloqueo según palabras clave
- Filtrado basado en políticas (exclusión/inclusión)
- 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

- Secure SD-WAN
- PortShield
- Estructuras Jumbo
- Protocolización mejorada
- Enlace troncal VLAN
- RSTP (Protocolo de árbol de expansión rápida)
- Duplicación de puertos
- QoS de nivel 2
- Seguridad de puertos
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Controlador inalámbrico de SonicWall
- Enrutamiento basado en políticas (ToS/métrica y ECMP)
- NAT

- Seguridad DNS
- Servidor DHCP
- Gestión del ancho de banda
- Agregación de enlaces (estáticos y dinámicos)
- Redundancia de puertos
- Alta disponibilidad A/P con sincronización de estado
- Agrupación A/A
- Equilibrio de carga entrante/saliente
- Modo L2 Bridge, modo Wire/Virtual Wire, modo Tap
- Reconexión WAN 3G/4G
- Enrutamiento asimétrico
- Compatibilidad con tarjetas Common Access Card (CAC)

Conexión inalámbrica

- WIDS/WIPS
- Análisis del espectro RF
- Prevención de access points no autorizados
- Itinerancia rápida (802.11k/r/v)
- Selección automática de canales
- Vista de planta/vista de topología
- Band steering (direccionamiento de banda)
- Beamforming (conformación de haces)
- AirTime Fairness (equidad de conexión)
- MiFi Extender
- Acceso temporal para usuarios invitados
- Portal para invitados LHM

VoIP

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

Gestión y supervisión

- Capture Security Center, GMS, Web UI, 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 access points de SonicWall
- Gestión de switches de las series Dell N y Dell X incluidos switches en cascada

Almacenamiento local

- Registros
- Informes
- Copias de seguridad de firmware

¹ Requiere suscripción adicional

Especificaciones del sistema de la serie NSa

Firewall general	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Sistema operativo	SonicOS 6.5.4			
Interfaces	4 x 2,5-GbE SFP, 4 x 2,5-GbE, 12 x 1-GbE, Gestión de 1 GbE, 1 Consola	2 x 10 GbE SFP+, 8 x 2,5-GbE SFP, 4 x 2,5-GbE, 12 x 1-GbE, Gestión de 1 GbE, 1 Consola	2 x 10 GbE SFP+, 4 x 2,5-GbE SFP, 4 x 2,5-GbE, 16 x 1-GbE, Gestión de 1 GbE, 1 Consola	2 x 10 GbE SFP+, 2 x 10-GbE, 4 x 2,5-GbE SFP, 4 x 2,5-GbE, 16 x 1-GbE, Gestión de 1 GbE, 1 Consola
Expansión	1 ranura de expansión (trasera)*			
Almacenamiento integrado (SSD)	16 GB	32 GB	32 GB	64 GB
Gestión	CLI, SSH, IU Web, Centro de seguridad de Capture, GMS, APIs REST			
Usuarios de SSO	40.000	50.000	60.000	70.000
Máximo de access points admitidos	48	96	128	192
Protocolización	Analizador, Registro local, Registro del sistema			
Rendimiento de firewall/VPN	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Rendimiento de inspección del cortafuegos ¹	3,0 Gbps	3,75 Gbps	6,0 Gbps	6,25 Gbps
Rendimiento de prevención de amenazas ²	1,5 Gbps	1,75 Gbps	2,5 Gbps	3,4 Gbps
Rendimiento de inspección de aplicaciones ²	1,85 Gbps	2,1 Gbps	3,0 Gbps	4,25 Gbps
Rendimiento de IPS ²	1,4 Gbps	1,8 Gbps	2,3 Gbps	3,4 Gbps
Rendimiento de inspección de antimalware ²	1,3 Gbps	1,5 Gbps	2,45 Gbps	2,8 Gbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL) ²	300 Mbps	320 Mbps	675 Mbps	800 Mbps
Rendimiento de VPN ³	1,45 Gbps	1,5 Gbps	3,0 Gbps	3,5 Gbps
Conexiones por segundo	14.000/s	14.000/s	40.000/s	40.000/s
Número máximo de conexiones (SPI)	1.000.000	2.000.000	3.000.000	4.000.000
Número máximo de conexiones (DPI)	500.000	750.000	1.000.000	1.500.000
Número máximo/predeterminado de conexiones (DPI SSL)	100.000/60.000	100.000/40.000	175.000/145.000	175.000/125.000
VPN	NSa 2650	NSa 3650	NSa 4650	NSa 4650
Túneles entre emplazamientos	1.000	3.000	4.000	6.000
Clientes VPN IPSec (máximo)	50 (1.000)	500 (3.000)	2.000 (4.000)	2.000 (6.000)
Clientes SSL VPN NetExtender (máx.)	2 (350)	2 (500)	2 (1.000)	2 (1.500)
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	NSa 2650	NSa 4650	NSa 4650	NSa 4650
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 (IP solapadas), PAT, modo transparente			
Interfaces VLAN	256	256	400	500
Protocolos de enrutamiento	BGP4, 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 (múltiples dominios), XAUTH/RADIUS, SSO, Novell, base de datos de usuarios interna, Terminal Services, Citrix, 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 curso)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall e IPS), UC APL, USGv6, CsFC			
Alta disponibilidad ⁵	Activa/Pasiva con State Sync	Activa/Pasiva con State Sync	Agrupación Activa/Activa	DPI Activo/Pasivo con sincronización de estado/ DPI Activo/Activo con sincronización de estado, Agrupación (clústeres) Activa/Activa
Hardware	NSa 2650	NSa 3650	NSa 4650	NSa 4650
Fuente de alimentación	Doble, redundante 120 W (una incluida)		Doble, redundante 350W (una incluida)	
Ventiladores	Doble, fijo			
Potencia de entrada	100-240 VCA, 50-60 Hz,			
Consumo máximo de energía (W)	37,2	46	93,6	103,6
MTBF a 25 °C en horas	162.231	156.681	154.529	153.243
MTBF a 25 °C en años	18,5	17,9	17,6	17,5
Factor de forma	Montaje en bastidor 1U			
Dimensiones	43 x 32,5 x 4,5 cm (16,9 x 12,8 x 1,8 pulg.)		43 x 41,5 x 4,5 cm (16,9 x 16,3 x 1,8 pulg.)	
Peso	5,2 kg (11,5 lb)	5,3 kg (11,7 lb)	6,9 kg (15,2 lb)	6,9 kg (15,2 lb)
Peso WEEE	5,5 kg (12,1 lb)	5,6 kg (12,3 lb)	8,9 kg (19,6 lb)	8,9 kg (19,6 lb)
Peso de envío	7,7 kg (17,0 lb)	7,8 kg (17,2 lb)	11,3 kg (24,9 lb)	11,3 kg (24,9 lb)
Normativa principal	FCC Clase A, ICES Clase A, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase A, UL, cUL, TUV/ GS, CB, Certificado de cumplimiento para México por UL, RAEE, REACH, BSMI, KCC/MSIP, ANATEL			
Entorno (Operativo/Almacenamiento)	0°-40 °C (32-105 °F)/-40 a 70 °C (-40 a 158 °F)			
Humedad	10-90%, sin condensación			

Especificaciones del sistema de la serie NSa, continuación

Firewall general	NSa 6650	NSa 9250	NSa 4650	NSa 4650
Sistema operativo	SonicOS 6.5.4			
Interfaces	6 x 10 GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 8 x 2.5-GbE, 8 x 1-GbE, Gestión de 1 GbE, 1 Consola	10 x 10 GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, Gestión de 1 GbE, 1 Consola	10 x 10 GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, Gestión de 1 GbE, 1 Consola	10 x 10 GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, Gestión de 1 GbE, 1 Consola
Expansión	1 ranura de expansión (trasera)*			
Almacenamiento integrado (SSD)	64 GB	1TB, 128 GB	1TB, 128 GB	1TB, 256 GB
Gestión	CLI, SSH, IU Web, Centro de seguridad de Capture, GMS, APIs REST		CLI, SSH, IU Web, GMS, APIs REST	
Usuarios de SSO	70.000	80.000	90.000	100.000
Máximo de access points admitidos	192	192	192	192
Protocolización	Analizador, registro local, Syslog, IPFIX, NetFlow			
Rendimiento de firewall/VPN	NSa 6650	NSa 9250	NSa 4650	NSa 9650
Rendimiento de inspección del cortafuegos ¹	12,0 Gbps	12,0 Gbps	17,1 Gbps	17,1 Gbps
Rendimiento de prevención de amenazas ²	5,5 Gbps	6,5 Gbps	9,0 Gbps	9,4 Gbps
Rendimiento de inspección de aplicaciones ²	6,0 Gbps	7,8 Gbps	10,8 Gbps	11,5 Gbps
Rendimiento de IPS ²	6,0 Gbps	7,2 Gbps	10,2 Gbps	10,3 Gbps
Rendimiento de inspección de antimalware ²	5,4 Gbps	6,5 Gbps	8,0 Gbps	8,5 Gbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL) ²	1,45 Gbps	1,5 Gbps	2,1 Gbps	2,25 Gbps
Rendimiento de VPN ³	6,0 Gbps	6,75 Gbps	10,0 Gbps	10,0 Gbps
Conexiones por segundo	90.000/s	90.000/s	130.000/s	130.000/s
Número máximo de conexiones (SPI)	5.000.000	7.500.000	10.000.000	12.500.000
Número máximo de conexiones (DPI)	2.000.000	3.000.000	4.000.000	5.000.000
Número máximo/predeterminado de conexiones (DPI SSL)	250.000/170.000	250.000/170.000	450.000/290.000	550.000/320.000
VPN	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Túneles entre emplazamientos	8.000	12.000	12.000	12.000
Clientes VPN IPSec (máximo)	2.000 (6.000)	2.000 (6.000)	2.000 (6.000)	2.000 (6.000)
Clientes SSL VPN NetExtender (máx.)	2 (2.000)	2 (3.000)	2 (3.000)	50 (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	NSa 6650	NSa 9250	NSa 9450	NSa 9650
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 (IP solapadas), PAT, modo transparente			
Interfaces VLAN	512			
Protocolos de enrutamiento	BGP4, 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 (múltiples dominios), 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 curso)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall e IPS), UC APL, USGv6, CsFC			
Alta disponibilidad ⁵	DPI Activo/Pasivo con sincronización de estado/DPI Activo/Activo con sincronización de estado, Agrupación (clústeres) Activa/Activa			
Hardware	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Fuente de alimentación	Doble, redundante 350W (una incluida)		Doble, redundante, 350 W	
Ventiladores	Triple, desmontable			
Potencia de entrada	100-240 VCA, 50-60 Hz,			
Consumo máximo de energía (W)	144,3	86,7	90,9	113,1
MTBF a 25 °C en horas	157.193	139.783	134.900	116.477
MTBF a 25 °C en años	17,9	15,96	15,4	13,3
Factor de forma	Montaje en bastidor 1U			
Dimensiones	43 x 41,5 x 4,5 cm (16,9 x 16,3 x 1,8 pulg.)			
Peso	8,1 kg (17,9 lb)		8,1 kg (17,9 lb)	
Peso WEEE	10,2 kg (22,5 lb)		10,2 kg (22,5 lb)	
Peso de envío	12,6 kg (27,8 lb)		12,6 kg (27,8 lb)	
Normativa principal	FCC Clase A, CE (EMC, LVD, RoHS), C-Tick, VCCI Clase A, MSIP/KCC Clase A, UL, cUL, TUV/ GS, CB, Certificado de cumplimiento para México por UL, RAEE, REACH, ANATEL, BSMI			
Entorno (Operativo/Almacenamiento)	0°-40 °C (32-105 °F)/-40 a 70 °C (-40 a 158 °F)			
Humedad	10-90%, sin condensación			

¹ Métodos de prueba: Rendimiento máximo basado en RFC 2544 (para firewall). El rendimiento real puede variar dependiendo de las condiciones de la red y de los servicios activados.

² Rendimiento de Prevención de amenazas/Gateway AV/Anti-Spyware/IPS medido mediante la prueba de rendimiento HTTP estándar Spirent WebAvalanche y herramientas de prueba Ixia. Para las pruebas se han utilizado múltiples flujos a través de múltiples pares de puertos. Rendimiento de Prevención de amenazas medido con Gateway AV, Anti-Spyware, IPS and Application Control activado. Rendimiento SSL DPI medido en tráfico HTTPS con IPS habilitado.

³ Medición del rendimiento de VPN basada en el tráfico UDP con paquetes de 1280 bytes de conformidad con RFC 2544. Las especificaciones, las prestaciones y la disponibilidad están sujetas a modificaciones.

⁴ Por cada 125.000 conexiones DPI reducidas, la cantidad de conexiones DPI SSL disponibles aumenta en 3.000, excepto en NSa 9250 y superiores.

⁵ La agrupación (clústeres) Activa/Activa y la DPI Activa/Activa con State Sync requieren la compra de licencias ampliadas, excepto para NSa 9250 y superiores.

*Uso futuro. Las especificaciones, las prestaciones y la disponibilidad están sujetas a modificaciones.

Referencias disponibles de la serie NSa

NSa 2650	SKU
NSa 2650 TotalSecure Advanced Edition (1 año)	01-SSC-1988
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas y soporte 24x7 para NSa 2650 (1 año)	01-SSC-1783
Capture Advanced Threat Protection para NSa 2650 (1 año)	01-SSC-1935
Prevención de amenazas - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSa 2650 (1 año)	01-SSC-1976
Soporte 24x7 para NSa 2650 (1 año)	01-SSC-1541
Servicio de filtrado de contenidos para NSa 2650 (1 año)	01-SSC-1970
Capture Client	Basado en el recuento de usuarios
Servicio antispam integral para NSa 2650 (1 año)	01-SSC-2001
NSa 3650	SKU
NSa 3650 TotalSecure Advanced Edition (1 año)	01-SSC-4081
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas y soporte 24x7 para NSa 3650 (1 año)	01-SSC-3451
Capture Advanced Threat Protection para NSa 3650 (1 año)	01-SSC-3457
Prevención de amenazas - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSa 3650 (1 año)	01-SSC-3632
Soporte 24x7 para NSa 3650 (1 año)	01-SSC-3439
Servicio de filtrado de contenidos para NSa 3650 (1 año)	01-SSC-3469
Capture Client	Basado en el recuento de usuarios
Servicio integral antispam para NSa 3650 (1 año)	01-SSC-4030
NSa 4650	SKU
NSa 4650 TotalSecure Advanced Edition (1 año)	01-SSC-4094
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas y soporte 24x7 para NSa 4650 (1 año)	01-SSC-3493
Capture Advanced Threat Protection para NSa 4650 (1 año)	01-SSC-3499
Prevención de amenazas - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSa 4650 (1 año)	01-SSC-3589
Soporte 24x7 para NSa 4650 (1 año)	01-SSC-3487
Servicio de filtrado de contenidos para NSa 4650 (1 año)	01-SSC-3583
Capture Client	Basado en el recuento de usuarios
Servicio antispam integral para NSa 4650 (1 año)	01-SSC-4062
NSa 5650	SKU
NSa 5650 TotalSecure Advanced Edition (1 año)	01-SSC-4342
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas y soporte 24x7 para NSa 5650 (1 año)	01-SSC-3674
Capture Advanced Threat Protection para NSa 5650 (1 año)	01-SSC-3680
Prevención de amenazas - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSa 5650 (1 año)	01-SSC-3698
Soporte 24x7 para NSa 5650 (1 año)	01-SSC-3660
Servicio de filtrado de contenidos para NSa 5650 (1 año)	01-SSC-3692
Capture Client	Basado en el recuento de usuarios
Servicio antispam integral para NSa 5650 (1 año)	01-SSC-4068
NSa 6650	SKU
NSa 6650 TotalSecure Advanced Edition (1 año)	01-SSC-2209
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas y soporte 24x7 para NSa 6650 (1 año)	01-SSC-8761
Capture Advanced Threat Protection para NSa 6650 (1 año)	01-SSC-8930
Prevención de amenazas - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSa 6650 (1 año)	01-SSC-8979
Soporte 24x7 para NSa 6650 (1 año)	01-SSC-8663
Servicio de filtrado de contenidos para NSa 6650 (1 año)	01-SSC-8972
Capture Client	Basado en el recuento de usuarios
Servicio antispam integral para NSa 6650 (1 año)	01-SSC-9131
NSa 9250	SKU
NSa 9250 TotalSecure Advanced Edition (1 año)	01-SSC-2854
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas y soporte 24x7 para NSa 9250 (1 año)	01-SSC-0038
Capture Advanced Threat Protection para NSa 9250 (1 año)	01-SSC-0121
Prevención de amenazas - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSa 9250 (1 año)	01-SSC-0343
Soporte 24x7 para NSa 9250 (1 año)	01-SSC-0032
Servicio de filtrado de contenidos para NSa 9250 (1 año)	01-SSC-0331
Capture Client	Basado en el recuento de usuarios

Referencias disponibles de la serie NSa (Continuación)

NSa 9450	SKU
NSa 9450 TotalSecure Advanced Edition (1 año)	01-SSC-4358
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas y soporte 24x7 para NSa 9450 (1 año)	01-SSC-0414
Capture Advanced Threat Protection para NSa 9450 (1 año)	01-SSC-0855
Prevención de amenazas - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSa 9450 (1 año)	01-SSC-1196
Soporte 24x7 para NSa 9450 0 (1 año)	01-SSC-0407
Servicio de filtrado de contenidos para NSa 9450 (1 año)	01-SSC-1158
Capture Client	Basado en el recuento de usuarios
NSa 9650	SKU
NSa 9650 TotalSecure Advanced Edition (1 año)	01-SSC-3475
Advanced Gateway Security Suite – Capture ATP, prevención de amenazas soporte 24x7 para NSa 9650 (1 año)	01-SSC-2036
Capture Advanced Threat Protection para NSa 9650 (1 año)	01-SSC-2042
Prevención de amenazas - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus para NSa 9650 (1 año)	01-SSC-2142
Soporte 24x7 para NSa 9650 0 (1 año)	01-SSC-1989
Servicio de filtrado de contenidos para NSa 9650 (1 año)	01-SSC-2136
Capture Client	Basado en el recuento de usuarios
Módulos y accesorios*	SKU
Módulo de corto alcance 10GBASE-SR SFP+	01-SSC-9785
Módulo de largo alcance 10GBASE-LR SFP+	01-SSC-9786
Cable Twinax 10GBASE SFP+ 1 m	01-SSC-9787
Cable Twinax de 10GBASE SFP+ 3 m	01-SSC-9788
Módulo de corto recorrido 1000BASE-SX SFP	01-SSC-9789
Módulo de largo recorrido 1000BASE-LX SFP	01-SSC-9790
Módulo de cobre 1000BASE-T SFP	01-SSC-9791

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

Paquete de firewalls NSa/NSv de SonicWall

Los siguientes firewalls de la serie NSa pueden recibir una licencia de un año de la suscripción correspondiente NSv Virtual Appliance TotalSecure correspondiente* sin coste adicional.

Firewall NSa elegible	Firewall NSv correspondiente
NSa 5650	NSv 200
NSa 6650	NSv 200
NSa 9250	NSv 400
NSa 9450	NSv 400
NSa 9650	NSv 400

* La suscripción a NSv Virtual Appliance TotalSecure incluye firewall virtual NSv, antivirus para puertas de enlaces, antispyware, prevención de intrusiones y servicio de puertas de enlace de aplicaciones, servicio de filtrado de contenido y soporte 24x7.

Números de modelo oficiales:

NSa 2650 - 1RK38-0C8
 NSa 3650 - 1RK38-0C7
 NSa 4650 - 1RK39-0C9
 NSa 5650 - 1RK39-0CA
 NSa 6650 - 1RK39-0CB
 NSa 9250 - 1RK39-0CC
 NSa 9450 - 1RK39-0CD
 NSa 9650 - 1RK39-0CE

Servicios habilitados por partners

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

Acerca de SonicWall

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

El logo de Gartner Peer Insights Customers' Choice es una marca comercial y marca de servicio de Gartner, Inc., y/o sus filiales, y se utiliza en el presente documento con el correspondiente consentimiento. Todos los derechos reservados. Las distinciones Peer Insights Customers' Choice de Gartner vienen determinadas por las opiniones subjetivas de clientes finales individuales en base a sus experiencias, por la cantidad de críticas publicadas en los Peer Insights de Gartner y por las clasificaciones globales de un determinado proveedor en el mercado, tal y como se describe con mayor detalle en el presente documento, y no están pensadas en modo alguno para representar las visiones de Gartner ni de sus filiales.