



La serie SonicWALL Network Security Appliance

CORTAFUEGOS

Cortafuegos de próxima generación

- Cortafuegos de próxima generación
- Hardware multinúcleo escalable e inspección profunda de paquetes sin reensamblado
- Inteligencia, control y visualización de aplicaciones
- Alta disponibilidad dinámica y equilibrio de carga
- Alto rendimiento y coste total de propiedad reducido
- Productividad de la red
- Servicios de enrutamiento avanzados y prestaciones de red
- Prestaciones de Voz sobre IP (VoIP) basadas en estándares
- SonicWALL Clean Wireless
- Prestaciones incorporadas de Calidad de Servicio (QoS)
- Soporte para módulos integrados

Las organizaciones de todos los tamaños dependen de sus redes para acceder a las aplicaciones críticas tanto internas como externas. Si bien las empresas continúan beneficiándose enormemente de los avances en la tecnología de red, al mismo tiempo están cada vez más expuestas a los ataques sofisticados y económicamente motivados que interrumpen las comunicaciones, reducen el rendimiento y comprometen la seguridad de los datos. Estos ataques maliciosos superan los cortafuegos de inspección dinámica de paquetes anticuados mediante exploits avanzados de capa de aplicación. Los productos puntuales, aunque incrementan el nivel de seguridad, son caros, difíciles de gestionar, limitados a la hora de controlar el uso inapropiado de la red e inefectivos contra los más recientes ataques mixtos.

La serie de cortafuegos de próxima generación SonicWALL® Network Security Appliance (NSA) utiliza un diseño multinúcleo exclusivo y la tecnología patentada Reassembly-Free Deep Packet Inspection® (RFDPI)* para ofrecer una protección completa sin comprometer el rendimiento de la red. Al realizar un escaneado completo en tiempo real de cada paquete en busca de amenazas tanto internas como externas, la serie NSA de baja latencia supera las limitaciones de las soluciones de seguridad existentes. Los productos de la serie NSA ofrecen asimismo prevención de intrusiones, protección antimalware e inteligencia, control y visualización de aplicaciones, garantizando en todo momento un rendimiento excepcional. Al incluir enrutamiento avanzado, alta disponibilidad dinámica y tecnología IPsec y SSL VPN de alta velocidad, no sólo aumentan el nivel de seguridad, fiabilidad, funcionalidad y productividad de las sucursales, oficinas centrales y redes distribuidas de empresas medianas, sino que además minimizan el coste y la complejidad.

Compuesta por los dispositivos SonicWALL NSA 220, NSA 220 Wireless-N, NSA 250M, NSA 250M Wireless-N, NSA 2400, NSA 3500 y NSA 4500, la serie NSA ofrece una línea de soluciones escalables diseñadas para cumplir las necesidades de seguridad de cualquier organización.

Prestaciones y ventajas

Prestaciones de cortafuegos de próxima generación. Incluyen prevención de intrusiones, antivirus en pasarela, antispam y filtrado URL con inteligencia y control de aplicaciones y descifrado SSL para bloquear las amenazas antes de que entren en la red y controlar las aplicaciones de forma granular sin comprometer el rendimiento.

Hardware multinúcleo escalable e inspección profunda de paquetes sin reensamblado. Escanea miles de conexiones a velocidad de cable y elimina amenazas en archivos de tamaño ilimitado con una latencia prácticamente nula.

Inteligencia, control y visualización de aplicaciones. Ofrece control granular y visualización en tiempo real de las aplicaciones para garantizar la priorización del ancho de banda así como la máxima seguridad y productividad de la red.

Alta disponibilidad dinámica y equilibrio de carga. Estas prestaciones maximizan el ancho de banda total y garantizan el funcionamiento continuado de la red. De esta forma, proporcionan un acceso ininterrumpido a los recursos críticos y garantizan la continuidad de los túneles VPN así como del resto del tráfico de la red en casos de reconexión.

Alto rendimiento y coste total de propiedad reducido. Aprovecha la potencia de múltiples núcleos de procesamiento que funcionan al unísono para mejorar el rendimiento y ofrecer funciones de inspección simultánea, reduciendo al mismo tiempo el consumo eléctrico.

Aumento de la **productividad de la red** gracias a que el departamento de TI puede identificar y restringir o bloquear las aplicaciones y páginas Web improductivas, no autorizadas o no relacionadas con el trabajo, como Facebook® o YouTube®. Asimismo, en combinación con

un dispositivo de aceleración WAN (WXA) de SonicWALL, las soluciones de la serie NSA permiten optimizar el tráfico WAN.

Servicios de enrutamiento avanzados y prestaciones de red. Incorporan VLANs 802.1q, reconexión multi-WAN, gestión basada en zonas y objetos, equilibrio de carga y modos NAT avanzados, etc. De esta forma queda asegurada una configuración granular y flexible, así como una sólida protección de la red.

Prestaciones de Voz sobre IP (VoIP) basadas en estándares. Ofrecen máxima seguridad para todos los elementos de la infraestructura VoIP, desde equipos de comunicación a dispositivos VoIP, como SIP Proxies, Gatekeepers H.323 o servidores de llamadas.

SonicWALL Clean Wireless se puede integrar de forma opcional en los modelos dual-band wireless o a través de puntos de acceso inalámbricos SonicWALL SonicPoint. Proporciona conectividad inalámbrica 802.11a/b/g/n 3x3 MIMO y permite realizar escaneados en busca de puntos de acceso inalámbricos no autorizados de acuerdo con el estándar PCI DSS.

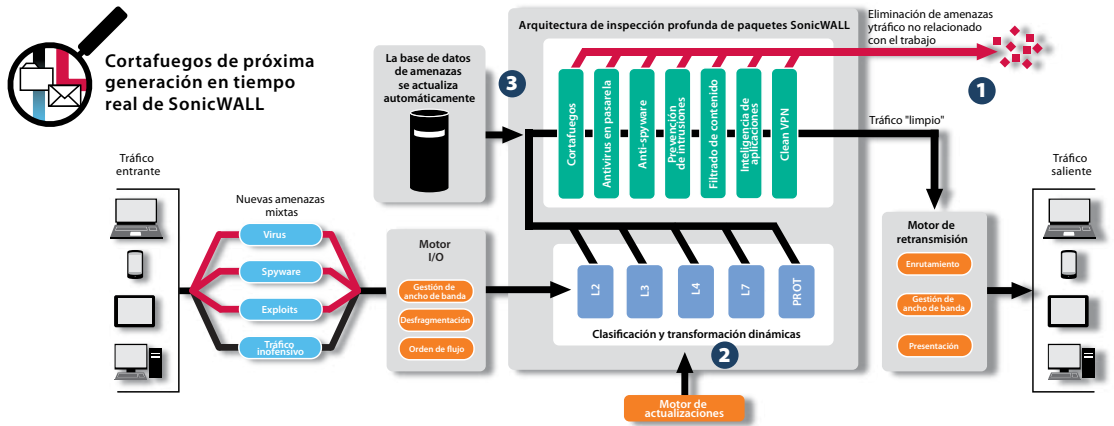
Prestaciones incorporadas de Calidad de Servicio (QoS). Utilizan el estándar 802.1p y la designación de Puntos de código Diffserv (DSCP) de Clase de Servicio (CoS) con el fin de proporcionar una gestión del ancho de banda potente y flexible para Voz sobre IP (VoIP), contenido multimedia o aplicaciones críticas de negocio.

Soporte para módulos integrados. Incluido en los dispositivos NSA 250M y NSA 250M Wireless-N, ofrece una mayor flexibilidad de implementación y reduce los costes de adquisición y mantenimiento ya que contribuye a la consolidación de los equipos.

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

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™



La mejor protección contra amenazas

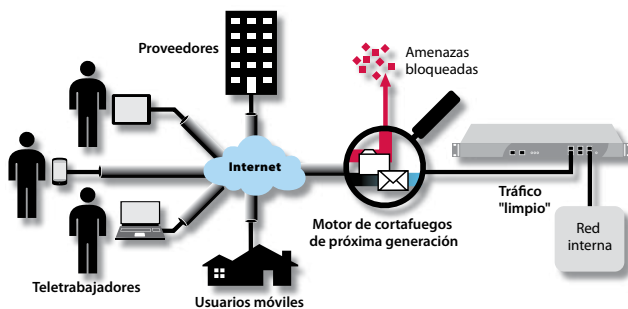
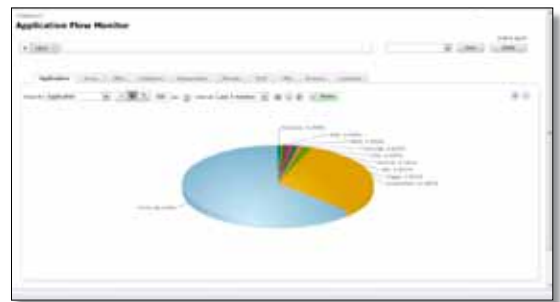
- 1 La inspección profunda de paquetes de SonicWALL protege la red contra riesgos como virus, gusanos, troyanos, spyware, ataques phishing, amenazas emergentes y el uso inapropiado de Internet. Application Intelligence and Control, además, ofrece funciones de control altamente configurables para prevenir la filtración de información y gestionar el ancho de banda a nivel de aplicación.
- 2 La tecnología Reassembly-Free Deep Packet Inspection (RFDPI) de SonicWALL utiliza la arquitectura multinúcleo de SonicWALL para escanear paquetes en tiempo real sin

retener el tráfico en la memoria. Gracias a este sistema, las amenazas pueden ser identificadas y eliminadas independientemente del tamaño de los archivos y del número de conexiones simultáneas, sin que el funcionamiento se vea interrumpido.

- 3 La serie SonicWALL NSA ofrece protección de red dinámica mediante la actualización continua y automática del sistema de seguridad. De esta forma, ya no es necesaria la intervención del administrador para garantizar la protección contra las amenazas nuevas y en constante evolución.

Application Intelligence and Control

Application Intelligence and Control de SonicWALL ofrece control granular y visualización en tiempo real de las aplicaciones para garantizar la priorización del ancho de banda así como la máxima seguridad y productividad de la red. Se trata de una prestación integrada en los cortafuegos de próxima generación de SonicWALL que utiliza la tecnología RFDPI de SonicWALL para identificar y controlar las aplicaciones en uso, independientemente del puerto o del protocolo. Para ello, utiliza categorías de aplicaciones predefinidas fáciles de usar (como por ejemplo, medios sociales, juegos). SonicWALL Application Traffic Analytics proporciona análisis detallados históricos y en tiempo real de los datos transmitidos a través del cortafuegos, incluidas las actividades que los usuarios realizan con las aplicaciones.



SonicWALL Clean VPN

SonicWALL Clean VPN™ garantiza la integridad del acceso VPN desde dispositivos remotos, incluidos los basados en iOS. Para ello comprueba la fiabilidad de los usuarios remotos y los dispositivos terminales y aplica servicios de seguridad antimalware y prestaciones de inteligencia y control de aplicaciones que permiten eliminar las amenazas maliciosas antes de que invadan la red corporativa.



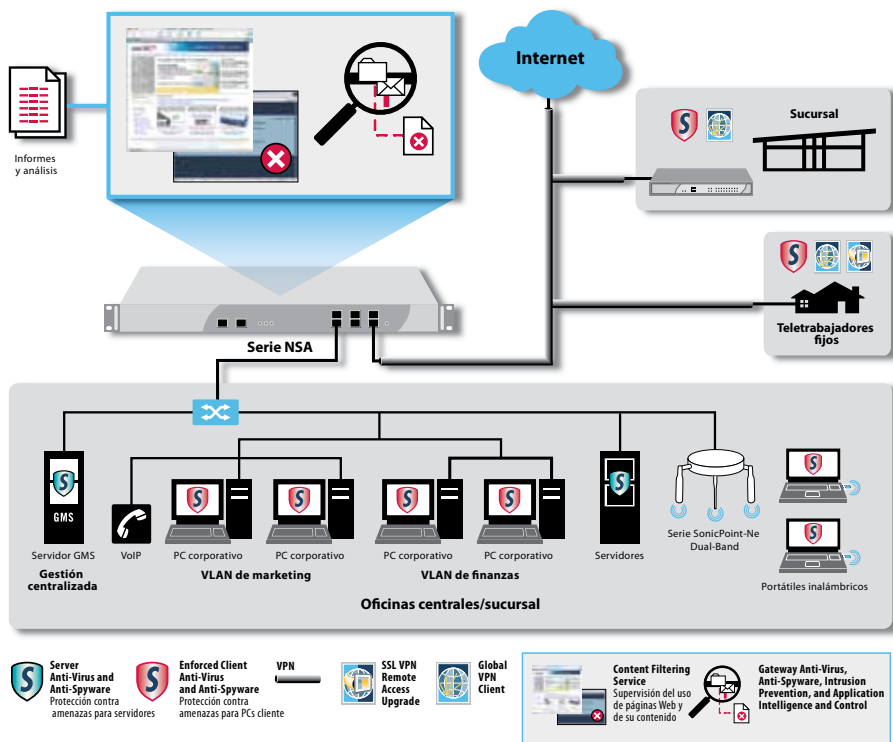
Gestión centralizada de políticas

Los dispositivos de la serie Network Security Appliance se pueden gestionar mediante SonicWALL GMS. El sistema de gestión global de SonicWALL ofrece herramientas potentes, flexibles e intuitivas que permiten gestionar las configuraciones, visualizar los parámetros de supervisión en tiempo real e integrar informes sobre políticas y cumplimiento y análisis del tráfico de aplicaciones, todo ello de forma centralizada.

Opciones de implementación flexibles y personalizables: la serie NSA

Gracias a su revolucionario diseño de hardware multinúcleo y a la tecnología Reassembly-Free Deep Packet Inspection, las soluciones SonicWALL Network Security Appliance ofrecen protección de gestión unificada de amenazas tanto interna como externa sin comprometer el rendimiento de la red. Los dispositivos 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 accesible y asequible que puede implementarse y gestionarse con gran facilidad en una gran diversidad de entornos – ya sean redes corporativas o distribuidas o redes de sucursales.

- SonicWALL NSA 4500 es ideal para entornos de oficinas centrales y redes distribuidas de gran tamaño que requieren una elevada capacidad de transferencia de datos y un elevado rendimiento.
- SonicWALL NSA 3500 es ideal para entornos distribuidos, de sucursales y corporativos que requieren una capacidad de transferencia de datos y un rendimiento considerables.
- SonicWALL NSA 2400 es ideal para entornos de pymes y sucursales que se preocupan por su capacidad de transferencia de datos y por su nivel de rendimiento.
- SonicWALL NSA 220, NSA 220 Wireless-N, NSA 250M y NSA 250M Wireless-N son ideales para sucursales de empresas distribuidas o entornos de pymes y empresas minoristas.



Servicios de seguridad y actualizaciones



Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Service. Proporcionan seguridad de red inteligente en tiempo real contra sofisticados ataques a nivel de aplicación y basados en contenido, como virus, spyware, gusanos, troyanos y vulnerabilidades de software (como desbordamientos de buffer). Application Intelligence and Control incluye una serie de herramientas configurables pensadas para prevenir la filtración de información, proporcionar un control granular de las aplicaciones y visualizar el tráfico de la red.



Enforced Client Anti-Virus and Anti-Spyware. Ofrece protección completa contra virus y spyware para ordenadores portátiles, PCs de escritorio y servidores, a través de un solo cliente integrado. Además, proporciona un refuerzo automático para la aplicación de las políticas de antivirus y anti-spyware, así como de las definiciones y actualizaciones de software en toda la red.



Content Filtering Service. Refuerza las políticas de protección y productividad mediante una arquitectura innovadora de clasificación. Gracias a una base de datos dinámica pueden bloquearse más de 56 categorías de contenido Web cuestionable.



Analyzer es una herramienta de informes y de análisis del tráfico de aplicaciones basada en Web, flexible y fácil de usar, que proporciona una visión detallada y completa, tanto histórica como en tiempo real, del estado, el rendimiento y la seguridad de la red.



Virtual Assist es una herramienta de soporte remoto sin clientes que permite al técnico tomar el control de un PC o portátil con el fin de prestar la asistencia técnica remota requerida. Una vez obtenido el permiso, el técnico accede instantáneamente al ordenador a través de un explorador Web. De este modo, puede realizar un diagnóstico y solucionar el problema de forma remota y sencilla sin necesidad de preinstalar un cliente "pesado".



Servicios de soporte dinámico. Ofrecen soporte 8x5 ó 24x7 dependiendo de las necesidades del cliente. La gama de servicios incluye actualizaciones y ampliaciones cruciales, el más sofisticado soporte técnico, acceso a una serie de herramientas electrónicas y la sustitución inmediata de hardware. Gracias a estos servicios, las organizaciones pueden sacar el máximo partido a sus dispositivos SonicWALL.



Ampliaciones a Global VPN Client. Utilizan un cliente de software que se instala en PCs basados en Windows y mejora la productividad de la plantilla proporcionando a los usuarios remotos un acceso seguro a correos electrónicos, archivos, Intranets y aplicaciones.



Ampliaciones de acceso remoto SSL VPN. Ofrecen un acceso remoto sin clientes a nivel de red para PC, Mac y sistemas basados en Linux. Gracias a la tecnología SSL VPN integrada, los dispositivos de cortafuegos de SonicWALL permiten un acceso remoto seguro y sin fisuras a correos electrónicos, archivos, Intranets y aplicaciones desde una variedad de plataformas cliente a través de NetExtender (un cliente ligero que se instala en el PC del usuario).



La aplicación cliente unificado **SonicWALL Mobile Connect™** para iOS ofrece a los usuarios de Apple® iPad®, iPhone® y iPod touch® pleno acceso de nivel de red a los recursos corporativos y académicos mediante conexiones SSL VPN cifradas.



Comprehensive Anti-Spam Service CASS ofrece protección completa antispam y antivirus para pymes y puede implementarse de forma instantánea en cualquier cortafuegos SonicWALL. CASS agiliza la implementación, simplifica la administración y reduce la complejidad de la infraestructura informática al consolidar soluciones y ofrecer un servicio antispam de un solo clic y una configuración avanzada que requiere tan solo 10 minutos.

Inspección profunda de paquetes para tráfico cifrado mediante SSL (DPI SSL). Descifra y escanea de forma transparente el tráfico HTTPS entrante y saliente en busca de amenazas utilizando SonicWALL RFDPI. En caso de no detectar amenazas o vulnerabilidades, vuelve a cifrar el tráfico y lo envía a su destino original.

Especificaciones técnicas

Cortafuegos	NSA 220/W	NSA 250M/W	NSA 2400	NSA 3500	NSA 4500
Versión de SonicOS	SonicOS 5.8.1.1		SonicOS Enhanced 5.6 (o superior)		
Rendimiento dinámico ¹	600 Mbps	750 Mbps	775 Mbps	1,5 Gbps	2,75 Gbps
Rendimiento de GAV ²	115 Mbps	140 Mbps	160 Mbps	350 Mbps	690 Mbps
Rendimiento de IPS ³	195 Mbps	250 Mbps	275 Mbps	750 Mbps	1,4 Gbps
Pleno rendimiento DPI ⁴	110 Mbps	130 Mbps	150 Mbps	240 Mbps	600 Mbps
Rendimiento IMIX ⁵	180 Mbps	210 Mbps	235 Mbps	580 Mbps	700 Mbps
Nº máxima de conexiones ⁶	85.000	110.000	125.000	325.000	500.000
Conexiones DPI máximas	32.000	64.000	125.000	175.000	250.000
Conexiones nuevas/segundo	2.200	3.000	4.000	7.000	10.000
Nodos soportados	Ilimitados				
Prevención de ataques por denegación de servicio	22 clases de ataques DoS, DDoS y de escaneo				
SonicPoints soportados (máximo)	16	24	32	48	64
VPN					
Rendimiento 3DES/AES ⁷	150 Mbps	200 Mbps	300 Mbps	625 Mbps	1,0 Gbps
Túneles VPN entre emplazamientos	25	50	75	800	1.500
Licencias Global VPN Client en paquete (máx.)	2 (25)	2 (25)	10 (250)	50 (1.000)	500 (3.000)
Licencias SSL VPN en paquete (máx.)	2 (15)	2 (15)	2 (25)	2 (30)	2 (10)
Virtual Assist en paquete (máx.)	1 Versión de prueba de 30 días (5)				
Cifrado/autenticación/grupo DH	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1/grupos DH 1, 2, 5, 14				
Intercambio de claves	Intercambio de claves IKE, IKEv2, clave manual, PKI (X.509), L2TP a través de IPSec				
VPN basada en enrutamiento	Sí (OSPF, RIP)				
Compatible con	Verisign, Thawte, Cybertrust, RSA Keon, Entrust, y Microsoft CA para VPN SonicWALL-SonicWALL VPN, SCEP				
Dead Peer Detection	Sí				
DHCP a través de VPN	Sí				
IPSec NAT Traversal	Sí				
Pasarela VPN redundante	Sí				
Plataformas Global VPN Client soportadas	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32 bits/64 bits, Windows 7 32/64 bits				
Plataformas SSL VPN soportadas	Microsoft® Windows 2000 / XP / Vista 32/64 bits / Windows 7, Mac 10.4+, Linux FC 3+/ Ubuntu 7+ / OpenSUSE				
Plataforma Mobile Connect soportada	iOS 4.2 y superior				
Servicios de seguridad					
Servicio de inspección profunda de paquetes	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control				
Content Filtering Service Premium Edition	Rastreo por HTTP URL, HTTPS IP, palabra clave y contenido, bloqueo de ActiveX, Java Applet, y cookies gestión de ancho de banda según categorías de filtrado, listas de admitidos/bloqueados				
Gateway-enforced Client Anti-Virus and Anti-Spyware	SonicWALL Enforced Client Anti-Virus and Anti-Spyware – McAfee				
Comprehensive Anti-Spam Service ⁸	Soportado				
Application Intelligence and Control	Gestión y control del ancho de banda de aplicaciones, priorización o bloqueo de aplicaciones según definiciones, control de las transferencias de archivos, escaneo según palabras o frases clave				
DPI SSL ⁹	Permite descifrar el tráfico HTTPS de forma transparente, escanearlo en busca de amenazas mediante la tecnología de inspección profunda de paquetes de SonicWALL (GAVAS/PS/ Application Intelligence/CFS), volver a cifrarlo y enviarlo a su destino, siempre que no se hayan encontrado amenazas o vulnerabilidades. Esta prestación puede utilizarse tanto para clientes como para servidores				
Conexión a red					
Asignación de direcciones IP	Estática, (cliente DHCP, PPPoE, L2TP y PPTP), servidor DHCP interno, relé DHCP				
Modos NAT	1:1, 1:muchos, muchos:1, muchos:muchos, NAT flexible (IPs solapadas), PAT, modo transparente				
Interfases VLAN (802.1q)	25	35	25	50	200
Enrutamiento	OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas, Multicast				
QoS	Prioridad de ancho de banda, ancho de banda máximo, ancho de banda garantizado, marcado DSCP, 802.1p				
IPv6	Sí				
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP, base de datos interna de Novell, servicios de terminal, Citrix				
Base de datos interna/usuarios de inicio de sesión único	100/100 usuarios	150/150 usuarios	250/250 usuarios	300/500 usuarios	1.000/1.000 usuarios
VoIP	Total compatibilidad con H.323v1-5, SIP, Gatekeeper, gestión de ancho de banda saliente, VoIP sobre WLAN, seguridad de inspección profunda, total interoperabilidad con la mayoría de los dispositivos VoIP de pasarela y comunicaciones				
Sistema					
Seguridad de zona	Sí				
Programaciones	Una vez, recurrentes				
Gestión basada en objetos/grupos	Sí				
DDNS	Sí				
Gestión y supervisión	Interfaz gráfica Web (HTTP, HTTPS), líneas de comandos (SSH, consola), SNMP v2, gestión global con SonicWALL GMS				
Protocolización e informes	Analyses, Local Log, Syslog, Solera Networks, NetFlow v5/v9, IPFIX con extensiones, visualización en tiempo real				
Alta disponibilidad	Activa/Pasiva con State Sync (opcional)				
Equilibrio de carga	Sí (saliente, porcentual, round-robin y spill-over)				
Normas	(entrante, round robin, distribución aleatoria, sticky IP, reasignación de bloques y reasignación simétrica)				
Normas de conexión inalámbrica	IEEE 802.11a/b/g/n, IEEE 802.11n, IEEE 802.11ac				
Soporte de aceleración WAN ¹⁰	Sí				
LAN inalámbrica integrada					
Estándares	802.11a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, PSK, 02.1x, EAP-PEAP, EAP-TLS)		—		
Puntos de acceso virtuales (VAPs)-Antenas (Diversity de 5 dB)	3 antenas externas extraíbles		—		
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 (2,4GHz)/802.11n (5,0GHz)	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 6Mbps, -74 dBm a 54 Mbps	—			
Sensibilidad de recepción radioeléctrica-802.11n (2,4GHz)/802.11n (5,0GHz)	-89 dBm MCS 0, -70 dBm MCS 15/-95 dBm MCS 0, -76 dBm MCS 15	—			
Hardware					
Interfases	(7) puertos Gigabit 10/100/1000 de cobre, 2 USB, 1 interfaz de consola	(5) puertos Gigabit 10/100/1000 de cobre, 2 USB, 1 interfaz de consola, ranura para módulo	(6) puertos Gigabit 10/100/1000 de cobre, 1 interfaz de consola, 2 USB		
Módulo	No	Sí	No	No	No
Memoria (RAM)	—		512 MB	—	
Memoria Flash	32 MB Compact Flash		512 MB Compact Flash		
3G inalámbrico/módem ¹¹	Con adaptador USB 3G/4G o módem		Con adaptador USB 3G/4G o módem		
Alimentación	36 W (ext.)		1 fuente de alimentación ATX 180 W		
Ventiladores	0 ventiladores/1 ventilador interno	2 ventiladores internos	2 ventiladores		
Potencia de entrada	11 W/15 W		12 W/16 W	42 W	64 W
Consumo eléctrico máximo	37 BTU/50 BTU		41 BTU/55 BTU	144 BTU	219 BTU
Calor disipado total	—		—	—	—
Certificaciones	VPNC, ICSA Firewall 4.1		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2		
Certificaciones pendientes	EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1, IPv6 Phase 2		—		
Factor de forma y dimensiones	Preparada para montaje en bastidor 1U/ 18,1 x 3,8 x 26,7 cm / 7,1 x 1,5 x 10,5 pulgadas		Preparada para montaje en bastidor 1U/ 43,2 x 26 x 4,4 cm / 17 x 10,3 x 1,8 pulgadas		Preparada para montaje en bastidor 1U/ 43,2 x 33,7 x 4,4 cm / 17 x 13,3 x 1,8 pulgadas
Peso	0,88 kg/1,95 libras	1,38 kg/3,05 libras	1,43 kg/3,15 libras	3,65 kg/8,05 libras	5,14 kg/11,30 libras
Peso DEEE	1,38 kg/3,05 libras	2,0 kg/4,4 libras	2,11 kg/4,65 libras	3,65 kg/8,05 libras	5,14 kg/11,30 libras
Conformidad con normas	FCC Class A, CES Class A, CE, CE-Tick, VCCI, Compliance MIC, UL, cUL, TÜVGS, CB, NOM, RoHS, WEEE				
Entorno	0-40°C, 40-105°F				
MTBF	28 años/15 años	23 años/14 años	14,3 años	14,1 años	14,1 años
Humedad	5-95 %, sin condensación				

Network Security Appliance 4500 01-SSC-7012
NSA 4500 TotalSecure* (1 año) 01-SC-7032



Network Security Appliance 3500 01-SSC-7016
NSA 3500 TotalSecure* (1 año) 01-SC-7033



Network Security Appliance 2400 01-SSC-7020
NSA 2400 TotalSecure* (1 año) 01-SC-7035



Network Security Appliance 250M 01-SSC-9755
Network Security Appliance 250M Wireless-N 01-SSC-9758 (Internacional)
Network Security Appliance 250M TotalSecure* 01-SSC-9747
Network Security Appliance 250M Wireless-N TotalSecure* 01-SSC-9749 (Internacional)



Network Security Appliance 220 01-SSC-9750
Network Security Appliance 220 Wireless-N 01-SSC-9753 (Internacional)
Network Security Appliance 220 TotalSecure* 01-SSC-9744
Network Security Appliance 220 Wireless-N TotalSecure* 01-SSC-9746 (Internacional)

Si desea obtener más información sobre las soluciones de seguridad de red de SonicWALL, visítenos en www.sonicwall.com.

*Incluye un año de Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence Service, Content Filtering Service y soporte dinámico 24x7.

Certificaciones



SonicWALL Iberia
T + 34 935 041 694
Spain@sonicwall.com
Contactos de soporte SonicWALL
www.sonicwall.com/emea/4724.html

¹ Métodos de prueba: Rendimiento máximo basado en RFC 2544 (para cortafuegos). El rendimiento real puede variar dependiendo de las condiciones de la red y de los servicios activados. ² Pleno rendimiento DPI/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 La cantidad máxima de conexiones real es inferior cuando se activan los servicios de cortafuegos de próxima generación. ⁴ Rendimiento VPN medido sobre la base de tráfico UDP y paquetes de 1.280 bytes según RFC 2544. ⁵ Soportado para NSA 3500 o superior. ⁶ No está disponible para NSA 2400. ⁷ La tarjeta 3G y el módem no están incluidos. Visite <http://www.sonicwall.com/us/products/cardsupport.html> para obtener información sobre los equipos USB soportados. ⁸ Comprehensive Anti-Spam Service soporta un número de usuarios ilimitado. No obstante, se recomienda utilizarlo para 250 usuarios o menos. ⁹ Con los dispositivos de la serie SonicWALL WXA.

Gama de soluciones de seguridad dinámica de SonicWALL

SEGURIDAD DE RED

ACCESO REMOTO SEGURO

SEGURIDAD DE WEB Y EMAIL

BACKUP Y RECUPERACIÓN

POLÍTICAS Y GESTIÓN

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™