La serie SonicWALL Network Security Appliance

CORTAFUEGOS

Cortafuegos de gestión unificada de amenazas

- **Gestión unificada de amenazas**
- **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**
- **Servicios de enrutamiento avanzados y prestaciones de red**
- **Prestaciones de Voz sobre IP (VoIP) basadas en estándares**
- **Servicios de seguridad para WLAN distribuida**
- **Prestaciones incorporadas de Calidad de Servicio (QoS)**

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 SonicWALL® Network Security Appliance (NSA) de cortafuegos de gestión unificada de amenazas (UTM) utiliza la exclusiva y patentada tecnología multinúcleo Reassembly-Free Deep Packet Inspection™ (RFDPI) para ofrecer protección completa sin comprometer el rendimiento de la red. Al escanear cada paquete en tiempo real en busca de amenazas tanto internas como externas, la serie NSA supera las limitaciones de las soluciones de seguridad existentes.

La serie NSA utiliza la tecnología de Gestión unificada de amenazas (UTM) para ofrecer protección contra una amplia variedad de ataques. Combina prestaciones de prevención de intrusiones, antivirus y anti-spyware, anti-spam y filtrado de contenido con inteligencia, control y visualización de aplicaciones. Con enrutamiento avanzado, alta disponibilidad dinámica y tecnología IPSec y SSL VPN de alta velocidad, la serie NSA aumenta la seguridad, la fiabilidad, la funcionalidad y la productividad de las oficinas centrales y sucursales, así como de las redes distribuidas de empresas medianas, minimizando al mismo tiempo los costes y la complejidad.

Compuesta por los dispositivos SonicWALL NSA 240, 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

Gestión unificada de amenazas. Incluye prevención de intrusiones, antivirus en pasarela, antispyware, inteligencia y control de aplicaciones, filtrado de contenido y antispam. De esta forma bloquea el malware y el spam, garantiza el control granular de las aplicaciones y previene la fuga de datos.

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.

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.

Servicios de seguridad para WLAN distribuida. Permiten que el dispositivo adopte las funciones de switch y controlador inalámbrico para detectar y configurar automáticamente los puntos de acceso inalámbricos SonicPoint.

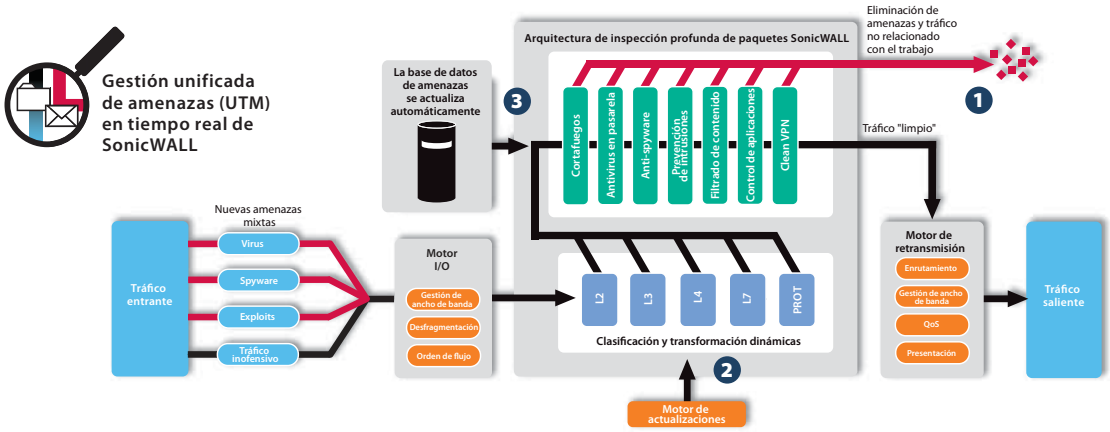
Prestaciones incorporadas de Calidad de Servicio (QoS). Utilizan el estándar 802.1p y la designación de Puntos de código Diffserv (DSCP) de Clase de Servicio (CoS) con el fin de proporcionar una gestión del ancho de banda potente y flexible para Voz sobre IP (VoIP), contenido multimedia o aplicaciones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

*Patente U.S. 7,310,815–A method and apparatus for data stream analysis and blocking (Método y equipo para el análisis y bloqueo de flujos de datos).

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Arquitectura y gestión de seguridad dinámicas



La mejor protección contra amenazas

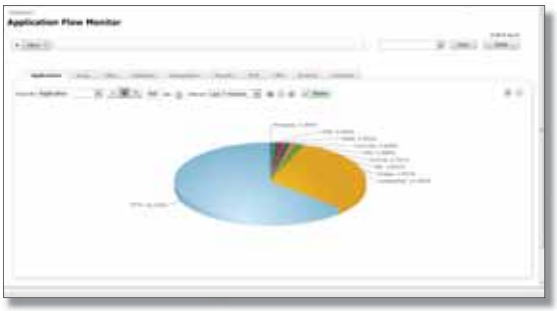
1. La inspección profunda de paquetes de SonicWALL protege la red contra riesgos como virus, gusanos, troyanos, spyware, ataques phishing, amenazas emergentes y el uso inapropiado de Internet. Application Intelligence and Control, además, ofrece funciones de control altamente configurables para prevenir 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.

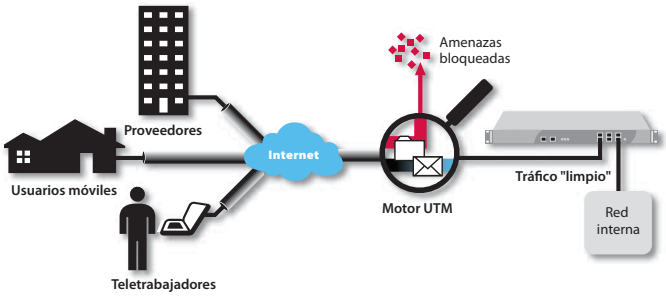
3. La serie SonicWALL NSA ofrece protección de red dinámica mediante la actualización continua y automática del sistema de seguridad. De esta forma, ya no es necesaria la intervención del administrador para garantizar la protección contra las amenazas nuevas y en constante evolución.

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 SonicWALL Reassembly-Free Deep Packet Inspection™ 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). Application Flow Monitor de SonicWALL



proporciona gráficos en tiempo real de las aplicaciones, del ancho de banda entrante y saliente, de las conexiones activas a sitios Web y de la actividad de los usuarios.



SonicWALL Clean VPN

Gracias a la innovadora tecnología Clean VPN™ de SonicWALL, la serie Network Security Appliance "descontamina" las conexiones de los usuarios móviles y el tráfico procedente de las sucursales antes de que acceda a la red corporativa, bloqueando así las vulnerabilidades y el código malicioso sin que sea necesaria la intervención del usuario.

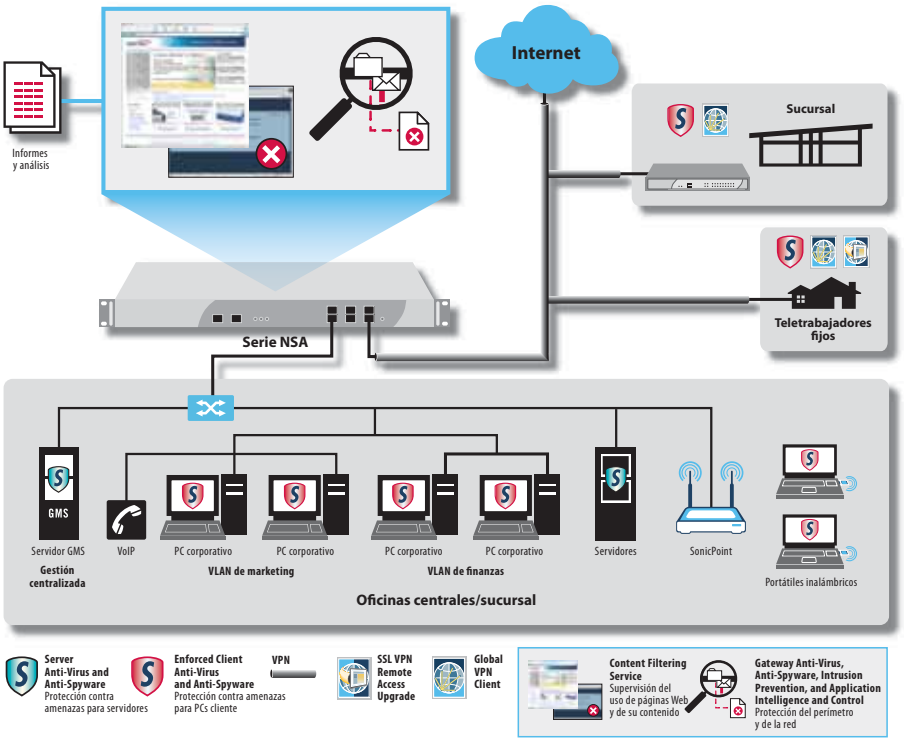
Gestión centralizada de políticas

Los dispositivos de la serie Network Security Appliance se pueden gestionar mediante Global Management System (GMS®) de SonicWALL, que ofrece herramientas potentes, flexibles e intuitivas para gestionar las configuraciones, visualizar los parámetros de supervisión en tiempo real y realizar informes sobre políticas y cumplimiento, 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 oficinas centrales y para entornos de 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 de redes de empresas, de sucursales y distribuidas que requieren una capacidad de transferencia de datos y un rendimiento considerables.
- **SonicWALL NSA 2400** 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.
- **SonicWALL NSA 240** es ideal para empresas pequeñas y medianas y sucursales.



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.

ViewPoint. Es una cómoda herramienta de informes basada en Web que proporciona a los administradores una visión completa e inmediata del rendimiento y la seguridad de la red. Gracias a la gran variedad de informes históricos basados en resúmenes y datos detallados, ViewPoint ayuda a organizaciones de todos los tamaños a supervisar el uso de Internet y el estado de seguridad de la red y a cumplir las leyes vigentes.

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. Las licencias de ampliación están disponibles para un número de usuarios variable, de modo que esta solución puede ampliarse según crece la organización.

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 SonicWALL UTM 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 y configura automáticamente en el PC del usuario sin que éste tenga que intervenir).

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 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

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 240
TotalSecure* (1 año)
01-SSC-8760

Adaptador SonicWALL de tarjeta PC a ExpressCard (para NSA 240)
01-SSC-2887

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, soporte dinámico 24x7 e informes ViewPoint.

Cortafuegos	NSA 240	NSA 2400	NSA 3500	NSA 4500
Versión de SonicOS	SonicOS Enhanced 5.6 (o superior)			
Rendimiento dinámico[1]	600 Mbps	775 Mbps	1,5 Gbps	2,75 Gbps
Rendimiento de GAV[2]	115 Mbps	160 Mbps	350 Mbps	690 MBps
Rendimiento de IPS[2]	195 Mbps	275 Mbps	750 Mbps	1,4 Gbps
Rendimiento de UTM[2]	110 Mbps	150 Mbps	240 Mbps	600 Mbps
Rendimiento IMIX[2]	195 Mbps	235 Mbps	580 Mbps	700 Mbps
Nº máximo de conexiones[3]	85.000/110.000[4]	225.000	325.000	500.000
Conexiones DPI máximas	32.000/50.000[4]	125.000	175.000	250.000
Conexiones nuevas/segundo	2.000	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	32	32	64
VPN	**NSA 240**	**NSA 2400**	**NSA 3500**	**NSA 4500**
Rendimiento 3DES/AES[5]	150 Mbps	300 Mbps	625 Mbps	1,0 Gbps
Túneles VPN entre emplazamientos	25/50[4]	75	800	1.500
Licencias Global VPN Client en paquete (máx.)	2 (25)	10 (250)	50 (1.000)	500 (3.000)
Licencias SSL VPN en paquete (máx.)	2 (15)	2 (25)	2 (30)	2 (30)
Virtual Assist en paquete (máx.)	1 Versión de prueba de 30 días (5)	1 (5)	2 (10)	2 (10)
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)			
Compatibe 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-bit/64 bit, Windows 7 32/64 bits			
Plataformas SSL VPN soportadas	Microsoft® Windows 2000 / XP / Vista 32/64-bit / Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE			
Servicios de seguridad	**NSA 240**	**NSA 2400**	**NSA 3500**	**NSA 4500**
Servicio de inspección profunda de paquetes	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention y Application Intelligence and Control			
Content Filtering Service (CFS) Premium Edition	Rastreo por HTTP URL, HTTPS IP, palabra clave y contenido, bloqueo de ActiveX, Java Applet, y cookies gestión del ancho de banda según categorías de filtrado, listas de admitidos/bloqueados			
Enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP y FTP, bloqueo de archivos adjuntos de correo electrónico mediante cliente McAfee™ reforzado			
Comprehensive Anti-Spam Service[7]	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[6]	Permite descifrar el tráfico HTTPS de forma transparente, escanearlo en busca de amenazas mediante la tecnología de inspección profunda de paquetes de SonicWALL (GAV/AS/IPS/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	**NSA 240**	**NSA 2400**	**NSA 3500**	**NSA 4500**
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			
Interfaces VLAN (802.1q)	10/25[4]	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 única	100/100 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	**NSA 240**	**NSA 2400**	**NSA 3500**	**NSA 4500**
Seguridad de zona	Sí			
Programaciones	Una vez, recurrentes			
Gestión basada en objetos/grupos	Sí			
DDNS	Sí			
Gestión y supervisión	Interfaz gráfica Web (HTTP, HTTPS), línea de comandos (SSH, consola), SNMP v2, gestión global con SonicWALL GMS			
Protocolización e informes	ViewPoint, Local Log, Syslog, Solera Networks, NetFlow v5/v9, IPFIX con extensiones, visualización en tiempo real			
Alta disponibilidad	Activa/Pasiva con State Sync (opcional)[4]	Activa/Pasiva con State Sync (opcional)		Activa/Pasiva con State Sync
Equilibrio de carga	Sí, (saliente, porcentual, round-robin y spill-over) (entrante, round robin, distribución aleatoria, sticky IP, reasignación de bloques y reasignación simétrica)			
Normas	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Normas de conexión inalámbrica	802.11 a/b/g/n, WPA2, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS			
Hardware	**NSA 240**	**NSA 2400**	**NSA 3500**	**NSA 4500**
Interfaces	(3) puertos GE + (6) 10/100, 2 USB, ranura de tarjeta PC (Módem 3G/análogo opcional), 1 interfaz de consola	(6) puertos Gigabit 10/100/1000 de cobre, 1 interfaz de consola, 2 USB		
Memoria (RAM)	256 MB	512 MB	512 MB	512 MB
Memoria Flash	32 MB Compact Flash	512 MB Compact Flash		
3G inalámbrico/módem[7]*	Con adaptador USB 3G/módem			
Alimentación	36 W (ext.)	1 fuente de alimentación ATX 180W		
Ventiladores	0 ventiladores	2 ventiladores		
Potencia de entrada	10-240 V, 50-60 Hz	100-240 Vac, 60-50 Hz		
Consumo eléctrico máximo	15 W	42 W	64 W	66 W
Calor disipado total	51,1 BTU	144 BTU	219 BTU	225 BTU
Certificaciones	EAL4+, VPNC, ICSA Firewall 4.1		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1	
Certificaciones pendientes	FIPS 140-2		–	–
Factor de forma y dimensiones	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	1,16 kg/2,55 libras	3,65 kg/ 8,05 libras		5,14 kg/11,30 libras
Peso DEEE	1,43 kg/3,15 libras	3,65 kg/ 8,05 libras		5,14 kg/11,30 libras
Conformidad con normas	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, DEEE			
Entorno	32-105° F, 0-40° C	5-40 °C, 40-105 °F		
MTBF	9,5 años	16,0 años	14,3 años	14,1 años
Humedad	0-95 %, sin condensación		10-90 %, sin condensación	

[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] Rendimiento de UTM/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 UTM. [4] Solo con las ampliaciones Stateful HA y Expansion de la serie NSA 240. [5] Rendimiento VPN medido sobre la base de tráfico UDP y paquetes de 1.280 bytes según RFC 2544. [6] Soportado para NSA 3500 o superior. [7] No está disponible para NSA 2400. * 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. [7] Comprehensive Anti-Spam Service soporta un número de usuarios ilimitado. No obstante, se recomienda utilizarlo para 250 usuarios o menos.

Certificaciones

SonicWALL Iberia
T + 34 653 948 287
Spain@sonicwall.com
Contactos de soporte SonicWALL
www.sonicwall.com/emea/4724.html

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™

©2010 SonicWALL y el logo de SonicWALL son marcas registradas de SonicWALL, Inc. Dynamic Security For The Global Network es una marca de SonicWALL, Inc. Los demás nombres de productos aquí mencionados pueden ser marcas registradas y/o marcas comerciales registradas de sus respectivos propietarios. Las especificaciones y las descripciones están sujetas a modificación sin previo aviso. 10/10 SW 1042