

- Cortafuegos de próxima generación
- Conectividad 10 GbE
- Potente prevención de intrusiones
- Application intelligence, control and visualization
- Tecnología de inspección profunda de paquetes sin reensamblado
- Implementación flexible
- Inspección profunda de paquetes para tráfico cifrado mediante SSL (DPI SSL)
- Red SonicWALL Global Response Intelligent Defense (GRID)
- Aceleración WAN

Hoy en día, las aplicaciones empresariales residen en la red corporativa y en la nube. Estas aplicaciones pueden ser o bien soluciones de negocio productivas o bien software contraproducente, que a menudo encierra peligros. Priorizar el ancho de banda para las aplicaciones críticas es imprescindible, al igual que lo es frenar o incluso bloquear por completo el consumo de ancho de banda de las aplicaciones de medios sociales o juegos. Los cortafuegos de inspección dinámica de paquetes tradicionales solamente escanean los puertos y protocolos, pero no las aplicaciones. Por ello, no son capaces de distinguir entre las aplicaciones “buenas” y las aplicaciones “malas”.

Las soluciones de la serie SonicWALL® E-Class Network Security Appliance (NSA) ofrecen un rendimiento de clase empresarial con funciones estrechamente integradas de prevención de intrusiones, protección contra malware e Inteligencia, control y visualización de aplicaciones. Al basarse en una potente plataforma de hardware multinúcleo y la tecnología patentada de SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI)*, las soluciones de la serie E-Class NSA pueden analizar y controlar miles de aplicaciones diferentes, incluso si están cifradas mediante SSL. La serie E-Class NSA puede implementarse o bien como cortafuegos de próxima generación o como cortafuegos UTM.

Compuesta por los modelos SonicWALL E-Class NSA E8510, E8500, E7500, E6500 y E5500, la serie E-Class NSA ofrece un amplio conjunto de soluciones escalables para las implementaciones de clase empresarial más exigentes en centros de datos, redes de campus y entornos distribuidos. Al desplegarse como solución inline, la serie E-Class NSA permite aprovechar la infraestructura existente, añadiendo una capa adicional de seguridad y visibilidad de red. En implementaciones de pasarela de seguridad, la serie E-Class NSA proporciona acceso remoto seguro, alta disponibilidad y otras prestaciones de clase empresarial.

La serie E-Class NSA constituye una parte esencial de la cartera de productos y servicios de SonicWALL de clase empresarial para la seguridad de red, el acceso remoto seguro y la seguridad del correo electrónico.

Prestaciones y ventajas

Cortafuegos de próxima generación. El cortafuegos SonicWALL de próxima generación con Reassembly-Free Deep Packet Inspection integra prevención de intrusiones, protección contra malware, así como inteligencia y control de aplicaciones con visualización en tiempo real.

La **conectividad 10 GbE** del dispositivo NSA E8510 permite implementar la solución en entornos con infraestructura 10 GbE.

Potente prevención de intrusiones. Esta prestación ofrece protección contra un amplio abanico de amenazas de capa de aplicación basadas en la red. Para ello, escanea los paquetes de datos en busca de gusanos, troyanos, vulnerabilidades de software, exploits de aplicaciones y otros tipos de código malicioso.

Application intelligence, control and visualization. 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.

Tecnología de inspección profunda de paquetes sin reensamblado. Permite controlar miles de aplicaciones y detectar millones de ataques de malware para proteger la red de forma automática. Asimismo, inspecciona cientos de miles de conexiones simultáneas a través de todos los puertos con una latencia prácticamente nula y sin poner límite al tamaño del flujo.

Implementación flexible. Puede implementarse o bien como solución convencional de pasarela o como solución inline, permitiendo mantener la infraestructura de red existente. Añade prestaciones de inteligencia y control de aplicaciones como nivel adicional de seguridad y visibilidad.

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.

Red SonicWALL Global Response Intelligent Defense (GRID). Actualiza constantemente en régimen 24x7 los servicios de protección de amenazas, de detección y prevención de intrusiones y de control de aplicaciones para garantizar la máxima seguridad. La suite completa de servicios de prevención de intrusiones puede proteger la red contra más de 1.000.000 de ataques diferentes de software malicioso.

La aceleración WAN disminuye la latencia y aumenta las velocidades de transmisión entre los emplazamientos remotos, contribuyendo a incrementar todavía más el rendimiento de la red.

* Patentes U.S. 7,310,815; 7,600,257; 7,738,380; 7,835,361

Tecnología de inteligencia y control de aplicaciones

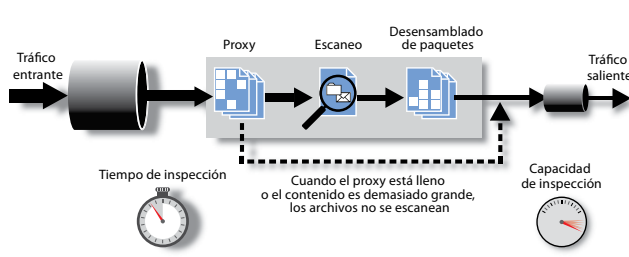
El servicio Application Intelligence and Control de SonicWALL ofrece control granular y visualización en tiempo real de las aplicaciones para garantizar la priorización del ancho de banda así como la máxima seguridad y productividad de la red. Se trata de una prestación integrada en los cortafuegos de 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. Con una base de datos de definiciones de amenazas en continua expansión que actualmente reconoce más de 3.500 aplicaciones y millones de amenazas de malware, Application Intelligence and Control permite mantener un control granular sobre las aplicaciones, priorizar o denegar el ancho de banda y prohibir el acceso a sitios Web. App 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, pudiendo enviar continuamente datos a herramientas de análisis como NetFlow o IPFIX.



Motor de inspección profunda de paquetes sin reensamblado

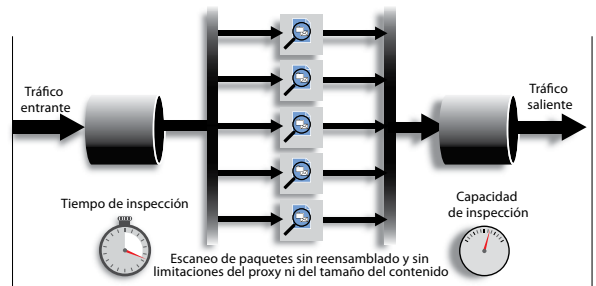
El motor de inspección profunda de paquetes sin reensamblado de SonicWALL es un motor escalable de inspección de aplicaciones capaz de analizar archivos y contenidos de cualquier tamaño en tiempo real, sin reensamblar los paquetes ni el contenido de las aplicaciones. Especialmente diseñado para aplicaciones en tiempo real y tráfico sensible a la latencia, este método de inspección ofrece un control y una inspección completos sin necesidad de recurrir a conexiones Proxy. Gracias a su diseño, este motor permite inspeccionar el tráfico de red de alta velocidad de forma más eficaz y segura, al tiempo que ofrece una mejor experiencia al usuario.

Proceso con ensamblado de paquetes



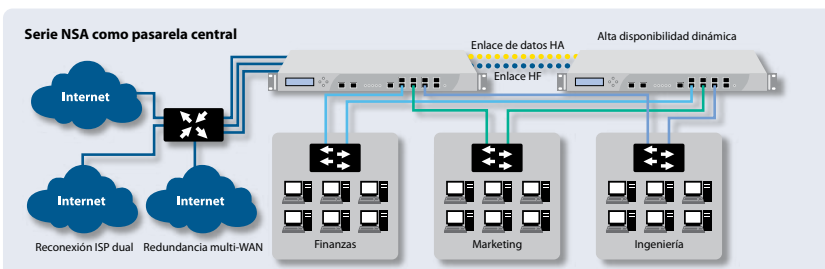
Arquitectura de otros proveedores

Proceso sin reensamblado de paquetes



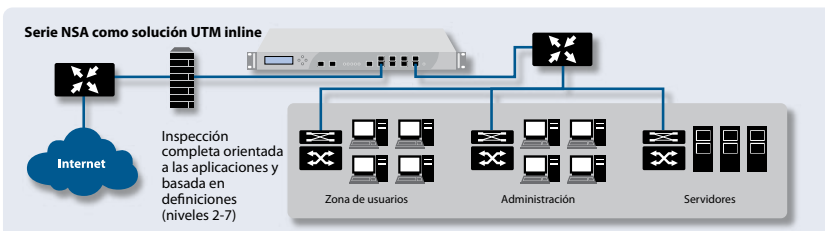
Arquitectura SonicWALL

Opciones de implementación flexibles y personalizables



Pasarela central

Implementada como pasarela central, la serie E-Class NSA constituye una plataforma escalable de alta velocidad que proporciona segmentación y protección utilizando para ello VLANs y zonas de seguridad. También incluye prestaciones de redundancia, como p.ej. equilibrio de carga WAN, reconexión ISP y DPI activa/activa.



Modo puente de capa 2

Este modo proporciona un sistema de detección y prevención de intrusiones inline así como un nivel adicional de seguridad basado en zonas para segmentos de red o unidades de negocio. Al mismo tiempo, simplifica el sistema de seguridad multicapa y permite a los administradores limitar el acceso a la información sensible para determinados servidores de bases de datos o unidades de negocio.

Protección multicapa

Protección para ubicaciones remotas

La serie E-Class NSA incorpora redes privadas virtuales (VPNs) escalables de altísimo rendimiento que pueden escalarse con facilidad para soportar miles de puntos terminales y sucursales. La innovadora tecnología Clean VPN™ de SonicWALL descontamina el tráfico en tiempo real antes de que llegue a la red corporativa y sin necesidad de que intervenga el usuario. De este modo se neutralizan a tiempo las vulnerabilidades y el código malicioso.

Protección a nivel de pasarela

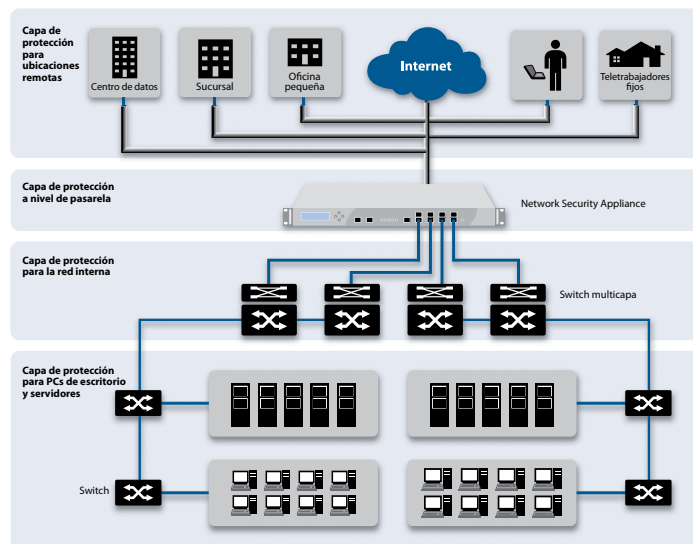
Fácilmente integrables en entornos existentes, las soluciones E-Class NSA ofrecen protección centralizada a nivel de pasarela para todos los archivos y aplicaciones entrantes y salientes así como para el tráfico basado en contenido. Al mismo tiempo, controlan el ancho de banda y las aplicaciones sin repercutir apenas en el rendimiento ni en la escalabilidad del sistema.

Protección interna

Las soluciones altamente configurables de la serie E-Class NSA inspeccionan el tráfico que pasa por las VLANs y las interfaces LAN, extendiendo así la protección hasta la red interna. Especialmente diseñadas para hacer frente a las amenazas de la LAN, las soluciones de la serie E-Class NSA detectan y combaten todo tipo de irregularidades de la red interna, como p.ej., código malicioso, ataques por denegación de servicio, vulnerabilidades de software explotadas, documentos confidenciales, incumplimientos de políticas y casos de uso indebido de la red.

Protección para PCs de escritorio y servidores

Además de ofrecer protección basada en la red y en la pasarela, la serie E-Class NSA proporciona protección adicional para puntos terminales (estaciones de trabajo y servidores) a través de un cliente antivirus y antispyware con heurística avanzada. Esta solución de cliente reforzado permite controlar el acceso a la red restringiendo el acceso a Internet de los puntos terminales cuyos motores o definiciones no estén completamente actualizados. Cuando se activa la función de refuerzo en el dispositivo, cada punto terminal recibe la orden de descargar el cliente antivirus y antispyware



reforzado sin necesidad de que intervengan los administradores. De esta forma se automatiza la implementación de las funciones de seguridad para los puntos terminales.

Gestión centralizada de políticas

Global Management System (GMS®) de SonicWALL ofrece herramientas potentes, flexibles e intuitivas para gestionar de forma centralizada las configuraciones de E-Class NSA en empresas distribuidas, visualizar los parámetros de supervisión en tiempo real y realizar informes sobre políticas y cumplimiento.



Servicios de suscripción

Todos los dispositivos E-Class de seguridad de red soportan una cantidad cada vez mayor de servicios de suscripción dinámicos y de software que se integran a la perfección en cualquier red.



Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service. Proporciona 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. Ofrece visualización en tiempo real del tráfico de la red, políticas personalizables y un control altamente granular sobre las aplicaciones y los usuarios.



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 una visión 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, a monitorear la seguridad

de la red y a cumplir las leyes vigentes.



Soporte SonicWALL E-Class 24x7. Concebido específicamente para los clientes con productos E-Class, el soporte técnico E-Class 24x7 proporciona soporte de clase empresarial y prestaciones de calidad de servicio. El soporte E-Class 24x7 incluye asistencia telefónica y a través de la Web las 24 horas del día y los 365 días del año con acceso directo a un equipo de técnicos expertos altamente cualificados, así como actualizaciones y ampliaciones de software y firmware, sustitución avanzada de hardware, acceso a herramientas electrónicas de soporte técnico y a grupos de discusión moderados, y mucho más.



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.

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 antispyware, así como de las definiciones y actualizaciones de software en toda la red.

Números de producto de la serie E-Class NSA



SonicWALL NSA E8510
01-SSC-9770



SonicWALL NSA E8500
01-SSC-8866



SonicWALL NSA E8500 High Availability
01-SSC-8867



SonicWALL NSA E7500
01-SSC-7000

SonicWALL NSA E7500 TotalSecure* (1 año)
01-SSC-7027



SonicWALL NSA E6500
01-SSC-7004

SonicWALL NSA E6500 TotalSecure* (1 año)
01-SSC-7028



SonicWALL NSA E5500
01-SSC-7008

SonicWALL NSA E5500 TotalSecure* (1 año)
01-SSC-7029

SonicWALL NSA E7500

Servicios de seguridad

SonicWALL GAV / IPS / Application Intelligence para NSA E7500 (1 año)
01-SSC-6130

SonicWALL Comprehensive Gateway Security Suite para NSA E7500 (1 año)
01-SSC-9220

Soporte 24x7 SonicWALL E-Class para NSA E7500 (1 año)
01-SSC-7254

SonicWALL NSA E6500

Servicios de seguridad

SonicWALL GAV / IPS / Application Intelligence para NSA E6500 (1 año)
01-SSC-6131

SonicWALL Comprehensive Gateway Security Suite para NSA E6500 (1 año)
01-SSC-9221

Soporte SonicWALL E-Class 24x7 para NSA E6500 (1 año)
01-SSC-7257

SonicWALL NSA E5500

Servicios de seguridad

SonicWALL GAV / IPS / Application Intelligence para NSA E5500 (1 año)
01-SSC-6132

SonicWALL Comprehensive Gateway Security Suite para NSA E5500 (1 año)
01-SSC-9222

Soporte SonicWALL E-Class 24x7 para NSA E5500 (1 año)
01-SSC-7260

También se ofrecen números de producto válidos por varios años, visite www.sonicwall.com.

*Incluye un año de Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence Service, Content Filtering Service, soporte E-Class 24x7 e informes ViewPoint.

Certificaciones



Especificaciones técnicas

	NSA E5500	NSA E6500	NSA E7500	NSA 8500	NSA 8510
Cortafuegos					
Versión de SonicOS	SonicOS Enhanced 5.6 (o superior)				SonicOS Enhanced 5.8.0.6 (o superior)
Rendimiento dinámico¹	3,9 Gbps	5 Gbps	5,6 Gbps	8,0 Gbps	
Rendimiento de GAV²	1,0 Gbps	1,69 Gbps	1,84 Gbps	2,25 Gbps	
Rendimiento de IPS³	2,0 Gbps	2,3 Gbps	2,58 Gbps	3,7 Gbps	
Pleno rendimiento DPI (inspección profunda de paquetes)²	850 Mbps	1,59 Gbps	1,7 Gbps	2,2 Gbps	
Rendimiento IMIX²	1,1 Gbps	1,4 Gbps	1,6 Gbps	2,0 Gbps	
Nº máximo de conexiones²	750.000	1.000.000	1.500.000	1.500.000	
Cantidad máxima de conexiones DPI plenas	500.000	600.000	1.000.000	1.250.000	
Conexiones nuevas/segundo	30.000	60.000	64.000	85.000	
Nodos soportados	Ilimitados				
Prevención de ataques por denegación de servicio	22 clases de ataques DoS, DDoS y de escaneo				
SonicPoints soportados (máximo)	96				128
VPN					
Rendimiento 3DES/AES⁴	1,7 Gbps	2,7 Gbps	3,0 Gbps	4,0 Gbps	
Túneles VPN entre emplazamientos	4.000	6.000			10.000
Licencias Global VPN Client en paquete (máx.)	2.000 (4.000)	2.000 (6.000)			2.000 (10.000)
Licencias SSL VPN en paquete (máx.)	2 (50)	2 (50)			2 (50)
Virtual Assist en paquete (máx.)	1 (25)	1 (25)			1 (25)
Cifrado/autenticación/grupos DH	DES, 3DES, AES (128, 192, 256 bits)/MDS, SHA-1/grupos DH 1, 2, 5, 14				
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				
Pasarela VPN redundante	Sí				
Plataformas Global VPN Client soportadas	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32 bits/64 bits, Windows 7				
Plataformas SSL VPN Client soportadas	Microsoft® Windows 2000 / XP / Vista 32/64 bits / Windows 7 32/64 bits, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE				
Servicios de seguridad					
Servicio de inspección profunda de paquetes	Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware and Application Intelligence				
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 clasificación, listas de admitidos/bloqueados personalizadas				
Enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP y FTP, clientes McAfee™ reforzados, bloqueo de archivos adjuntos de correo electrónico				
Comprehensive Anti-Spam Service⁵	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	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					
Asignación de direcciones IP	Estática, (cliente DHCP, PPPoE, L2TP y PPTP), Interna, servidor DHCP, relé DHCP				
Modos NAT	1:1, 1:muchos, muchos:1, muchos:muchos, NAT flexible (IPs solapadas), PAT, modo transparente				
Interfaces VLAN (802.1q)	400	500			512
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				
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP; base de datos interna de Novell, servicios de terminal, Citrix				
IPv6	Sí				
Base de datos interna/usuarios de inicio de sesión único	1.500/2.500 usuarios	2.500/4.000 usuarios			2.500/7.000 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				
Agregación de enlaces	Sí				
Redundancia de puertos	Sí				
Sistema					
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, DPI activa/activa				
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, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TTLS				
Soporte de aceleración WAN	Sí				
Hardware					
Interfaces	(8) puertos gigabit 10/100/1000 de cobre, interfaz HA 1 Gbe, 1 interfaz de consola, 2 USB		(4) SFP (SX, LX o TX), (4) 10/100/1000 Gbe, interfaz HA 1 Gbe, 2 USB, 1 interfaz de consola		(2) SFP+ 10Gbe, (4) 10/100/1000 interfaz HA 1 Gbe, 2 USB, 1 interfaz de consola
Memoria (RAM)	1 GB	1 GB	2 GB	4 GB	
Memoria Flash	Compact Flash 512 MB				
3G inalámbrico/módem*	Con un adaptador 3G o módem analógico soportados				
Alimentación	1 fuente de alimentación ATX 250W			2 fuentes de alimentación ATX 250 W de cambio en caliente	
Ventiladores	2 ventiladores de cambio en caliente				
Display	Display LCD frontal				
Potencia de entrada	100-240 V CA, 60-50 Hz				
Consumo eléctrico máximo	81 W	90 W			150 W
Calor disipado total	276 BTU	307 BTU			511,5 BTU
MTBF	11,9	11,9			12,4
Certificaciones	EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 fase 1, IPv6 fase 2		ICSA Firewall 4.1		—
Certificaciones pendientes	—		EAL4+, FIPS 140-2 Level 2, VPNC, IPv6 fases 1 y 2		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 fases 1 y 2
Factor de forma	Preparada para montaje en bastidor 1U				
Dimensiones	43, 2 x 42,5 x 4,4 cm/17 x 16,8 x 1,8 pulgadas				
Peso	6,80 kg/15,00 libras	6,85 kg/15,10 libras			7,9 kg/17,30 libras
Peso DEEE	6,80 kg/15,00 libras	6,85 kg/15,10 libras			7,9 kg/17,30 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	5-40° C, 40-105° F				
Humedad	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 DPI pleno/Gateway AV/Anti-Spyware/IPS medido mediante la prueba de rendimiento HTTP estándar Spirent WebValanche 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 reales es inferior cuando se activan los servicios UTM. ⁴ Rendimiento VPN medido sobre la base de tráfico UDP y paquetes de 1.280 bytes según RFC 2544. ⁵ 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. ⁶ Comprehensive Anti-Spam Service soporta un número de usuarios ilimitado. No obstante, se recomienda utilizarlo para 250 usuarios o menos. ⁷ 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

SonicWALL Iberia

T + 34 935 041 694
Spain@sonicwall.com

Contactos de soporte SonicWALL

www.sonicwall.com/emea/4724.html



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™