

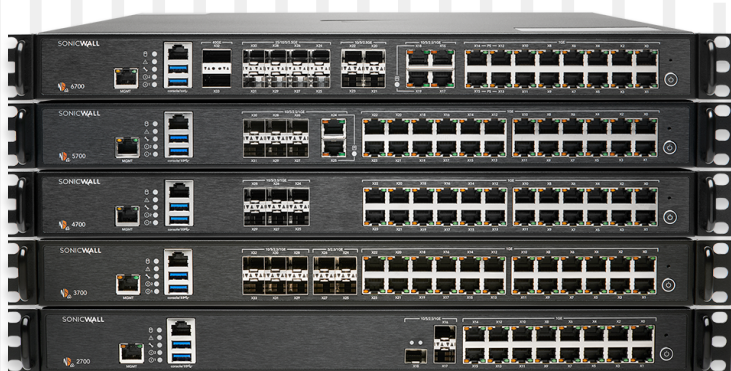
Serie SonicWall Gen 7 NSa

Los firewalls de nueva generación (NGFWs) de 7ª generación (Gen 7) Network Security Appliance (NSa) de SonicWall ofrecen a las empresas medianas y grandes un rendimiento líder en la industria al menor coste total de propiedad de su categoría.

Con prestaciones de seguridad completas, como prevención de intrusiones, VPN, control de aplicaciones, análisis de malware, filtrado URL, Seguridad DNS, Geo-IP y servicios Botnet, protege el perímetro contra amenazas avanzadas sin formar cuellos de botella.

PRESTACIONES DESTACADAS

- Factor de forma – 1 RU
- Soporte para puertos 40G/25G/10G/5G/2,5G/1G
- Rendimiento de análisis de amenazas y malware multigigabit
- Rendimiento de TLS superior (sesiones y capacidad de procesamiento)
- Almacenamiento ampliable
- Seguridad DNS
- Servicio de filtrado de contenido basado en la reputación (CFS 5.0)
- Gestión de firewalls mediante Wi-Fi 6
- Integración del control de acceso a la red con Aruba ClearPass
- Solución de clase empresarial habilitada para el borde de Internet
- Soporte para SonicOS de la más reciente generación 7
- Secure SD-WAN
- Interfaz de usuario intuitiva con gestión centralizada
- Soporte para TLS 1.3
- Mejor relación precio/rendimiento
- Basada en datos del equipo de investigación de amenazas de SonicWall Capture Labs
- Alta densidad de puertos para redes sencillas
- Integración de SonicWall Switch, puntos de acceso SonicWave y Capture Client
- Fuente de alimentación redundante



Avance de las especificaciones de la serie Gen 7 NSa

[Ver todas las especificaciones »](#)

**Hasta
19 Gbps**

Rendimiento de
prevención
de amenazas

**Hasta
8 millones**

Conexiones

**40G/25G/10G/
5G/2,5G/1G**

Puertos

Con una alta densidad de puertos, incluidos múltiples puertos 40 GbE y 10 GbE, la solución soporta redundancia de red y de hardware con alta disponibilidad, y dos fuentes de alimentación.

Los firewalls de nueva generación (NGFWs) de 7ª generación (Gen 7) Network Security Appliance (NSa) de SonicWall ofrecen a las empresas medianas y grandes un rendimiento líder en la industria al menor coste total de propiedad de su categoría.

Con prestaciones de seguridad completas, como prevención de intrusiones, VPN, control de aplicaciones, análisis de malware, filtrado URL, Seguridad DNS, Geo-IP y servicios Botnet, protege el perímetro contra amenazas avanzadas sin formar cuellos de botella.

La serie Gen 7 NSa ha sido creada desde cero con los últimos componentes de hardware, todos ellos diseñados para proporcionar un rendimiento multi-gigabit de prevención de amenazas, incluso para el tráfico cifrado. Con una alta densidad de puertos, incluidos múltiples puertos 40 GbE y 10 GbE, la solución soporta la redundancia de red y de hardware con alta disponibilidad y dos fuentes de alimentación.

Generación 7 – SonicOS 7 y Servicios de seguridad

La serie Gen 7 NSa utiliza SonicOS 7.0, un nuevo sistema operativo creado desde cero con el objetivo de proporcionar una interfaz de usuario moderna, flujos de trabajo intuitivos y un diseño centrado en el usuario. SonicOS 7 ofrece múltiples prestaciones diseñadas para facilitar los flujos de trabajo de nivel empresarial. Ofrece una configuración de políticas sencilla, implementación sin necesidad de intervención y una gestión flexible, todo lo cual permite a las empresas mejorar tanto su seguridad como la eficiencia de sus operaciones.

La serie Gen 7 NSa soporta prestaciones avanzadas de red, como SD-WAN, enrutamiento dinámico, alta disponibilidad de capa 4-7 y funcionalidad VPN de alta velocidad. Además de integrar prestaciones de firewall y de switch, el dispositivo proporciona una única interfaz para gestionar tanto los switches como los puntos de acceso.



Creada para mitigar los ciberataques avanzados de hoy y de mañana, la serie Gen 7 NSa ofrece acceso a los servicios de seguridad de firewall avanzados de SonicWall, permitiéndole proteger toda su infraestructura de TI. Las soluciones y los servicios como Cloud Application Security, el sandboxing basado en la nube Capture Advanced Threat Protection (ATP), la tecnología patentada Real-Time Deep Memory Inspection (RTDMI™) y Reassembly-Free Deep Packet Inspection (RFDPI)—para todo el tráfico, incluido el TLS 1.3—ofrecen protección completa de gateway contra la mayoría del malware sigiloso y peligroso, incluidas las amenazas de día cero y cifradas.

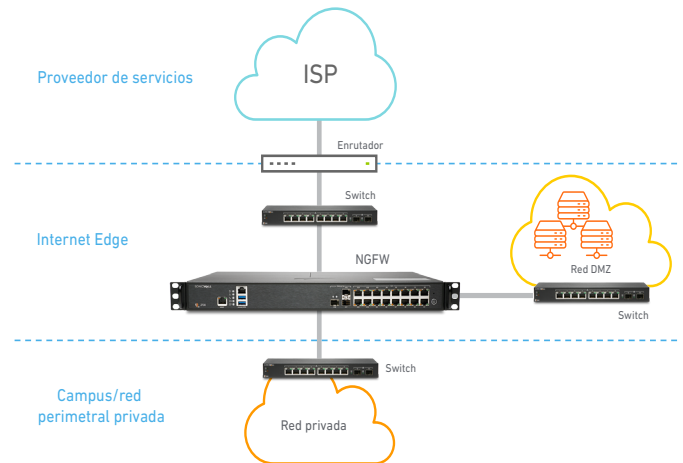
Implementaciones

La serie Gen 7 NSa tiene dos opciones de implementación principales para empresas medianas y distribuidas:

Implementación en el borde de Internet

En esta opción de implementación estándar, el NGFW de la serie Gen 7 NSa protege las redes privadas del tráfico malicioso procedente de Internet, lo cual le permite:

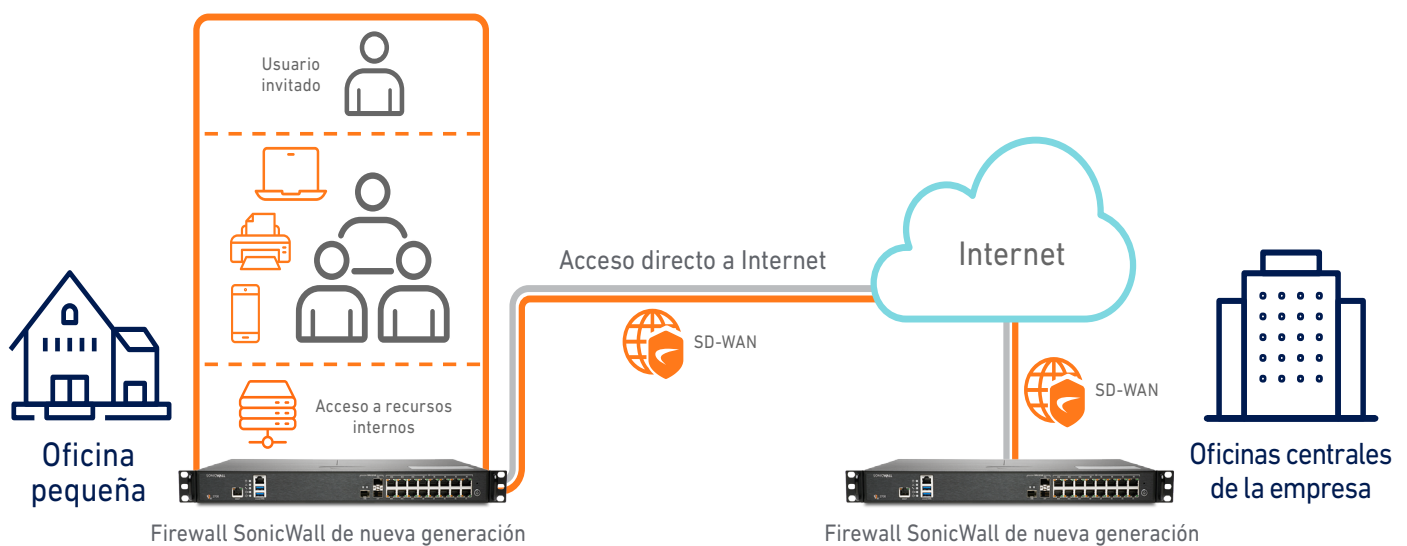
- Implementar una solución NGFW probada con el mayor rendimiento y la mayor densidad de puertos (incluida conectividad 40 GbE y 10 GbE) de su categoría
- Obtener visibilidad e inspeccionar el tráfico cifrado, incluido el TLS 1.3, para bloquear las amenazas evasivas procedentes de Internet, todo ello sin comprometer el rendimiento
- Proteger su empresa con seguridad integrada, incluidos análisis de malware, seguridad de aplicaciones en la nube, filtrado URL y servicios de reputación
- Ahorrar espacio y dinero con una solución NGFW integrada que incluye prestaciones avanzadas de seguridad y de red
- Reducir la complejidad y maximizar la eficiencia utilizando un sistema de gestión central proporcionado a través de una única interfaz de usuario intuitiva



Empresas medianas y distribuidas

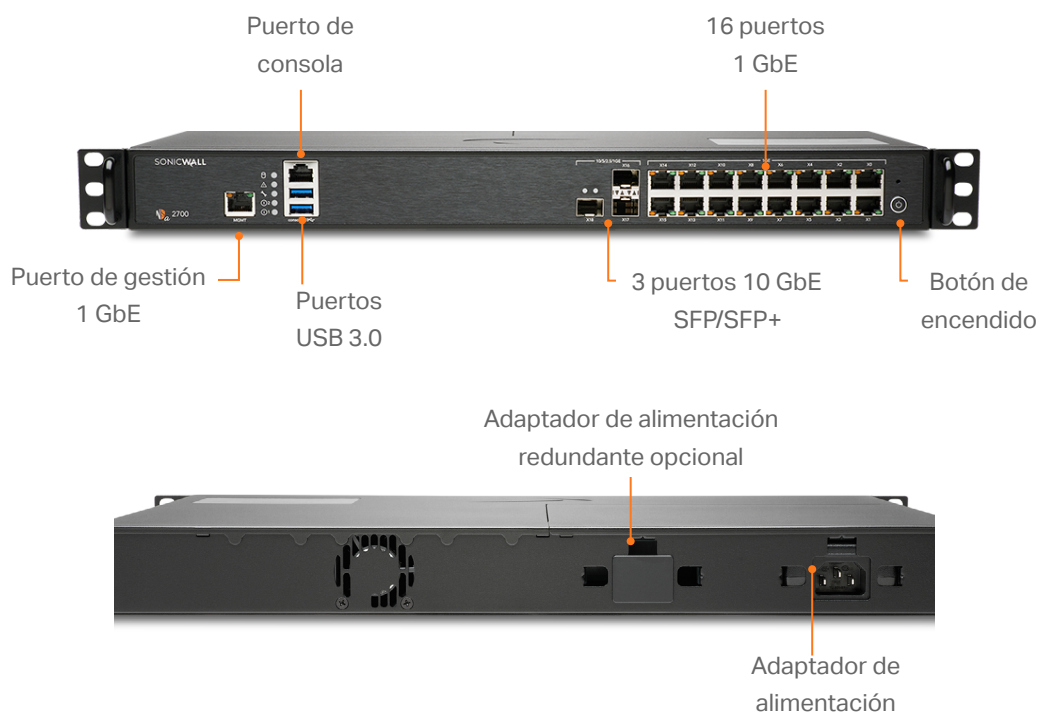
La serie SonicWall Gen 7 NSa soporta SD-WAN y puede gestionarse de forma centralizada, lo cual hace que sea ideal para las empresas medianas y distribuidas. Esta implementación permite a las organizaciones:

- Garantizar su seguridad en el futuro ante un panorama de las amenazas que cambia constantemente, invirtiendo en un NGFW con rendimiento de análisis de amenazas multigigabit.
- Proporcionar acceso a Internet directo y seguro para sucursales distribuidas, en lugar de recurrir al backhauling a través de la sede corporativa.
- Permitir a las sucursales distribuidas acceder de forma segura a los recursos de Internet que se encuentran en la sede corporativa o en una nube pública, mejorando considerablemente la latencia de las aplicaciones.
- Bloquear automáticamente las amenazas que utilizan protocolos cifrados, como TLS 1.3, protegiendo las redes contra los ataques más avanzados.
- Reducir la complejidad y maximizar la eficiencia, utilizando un sistema de gestión central proporcionado a través de una única interfaz intuitiva.
- Aprovechar la alta densidad de puertos, que incluye conectividad 40 GbE y 10 GbE, para soportar una empresa distribuida y redes de área amplia.

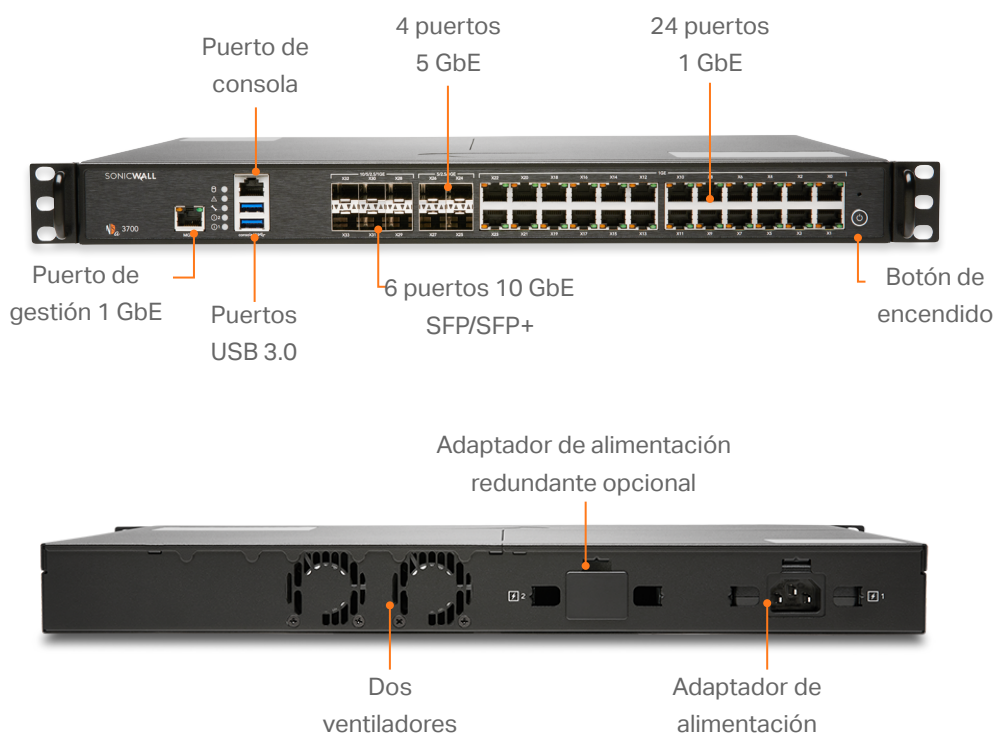


Serie SonicWall Gen 7 NSa

NSa 2700

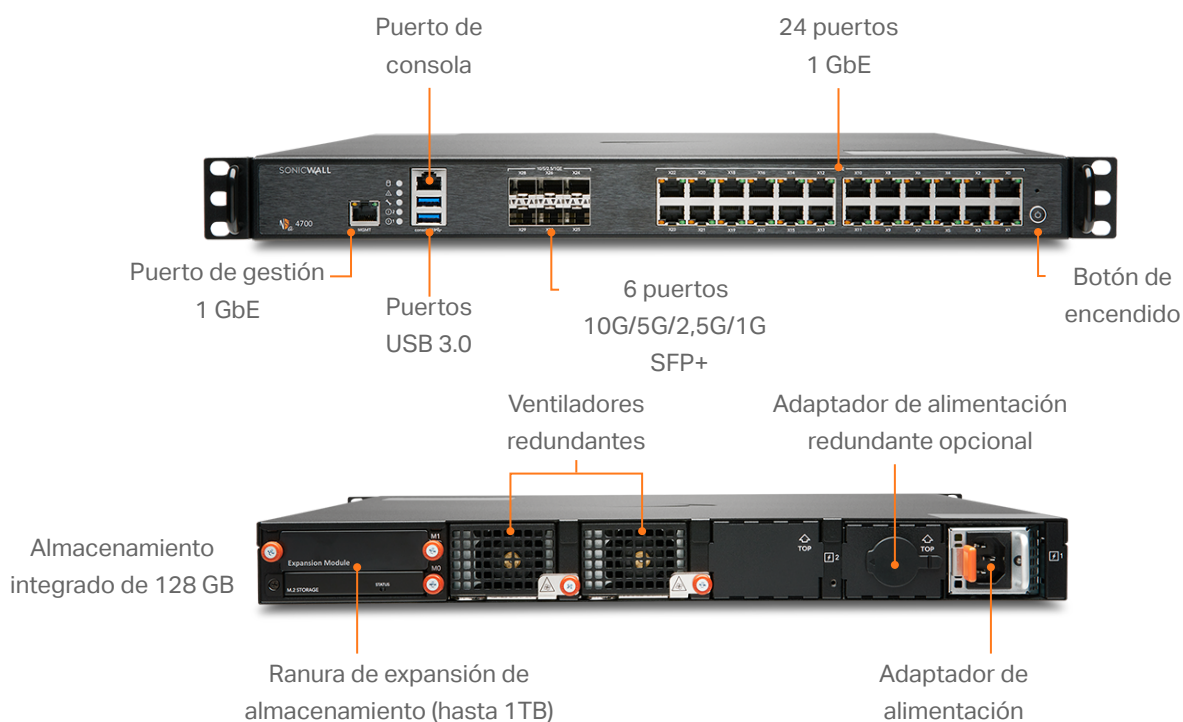


NSa 3700

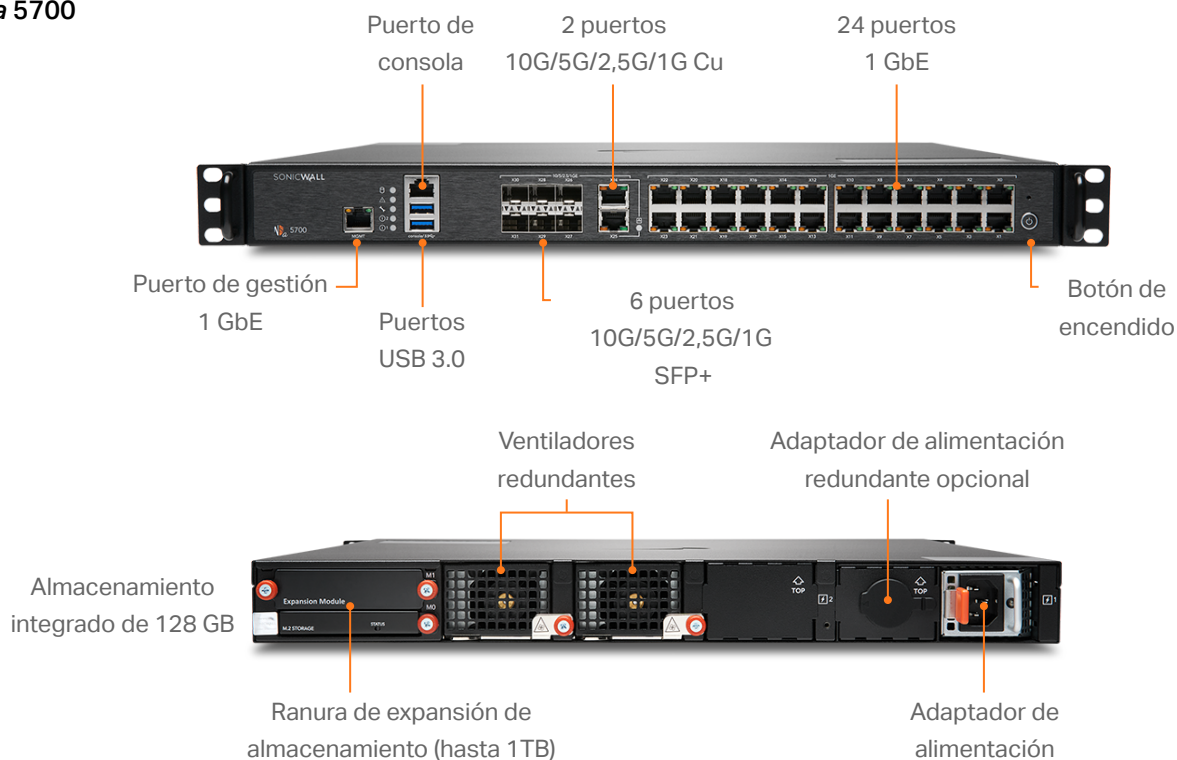


Serie SonicWall Gen 7 NSa (cont.)

NSa 4700

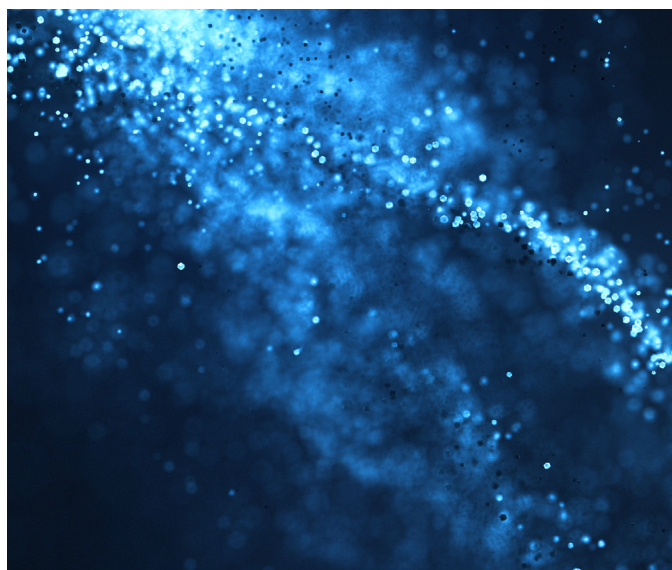
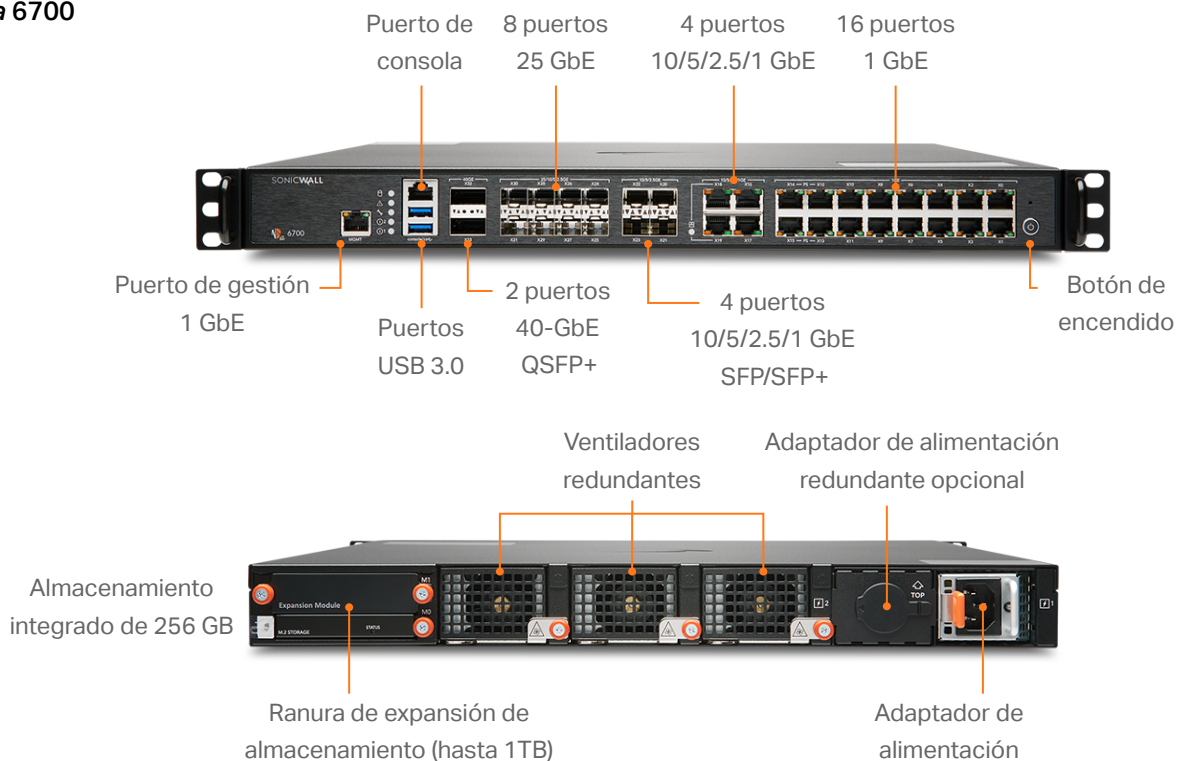


NSa 5700



Serie SonicWall Gen 7 NSa (cont.)

NSa 6700



SERVICIOS HABILITADOS POR PARTNERS

¿Necesita ayuda para planificar, implementar u optimizar su solución de SonicWall? Los **SonicWall Advanced Services Partners** están formados para proporcionarle servicios profesionales de clase mundial. Obtenga más información en:

www.sonicwall.com/PES

Especificaciones del sistema de la serie Gen 7 NSa

Firewall	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700
Sistema operativo	SonicOS 7				
Interfaces	16x1 GbE, 3x10G SFP+, 2 USB 3.0, 1 consola, 1 puerto de gestión	24x1 GbE, 6x10G SFP+, 4x5G SFP+, 2 USB 3.0, 1 consola, 1 puerto de gestión	6 x 10G/5G/2,5G/1G (SFP+); 24 x 1 GbE Cu 2 USB 3.0, 1 consola, 1 puerto de gestión	6 x 10G/5G/2,5G/1G (SFP+); 2x 10G/5G/2,5G/1G (Cu); 24 x 1 GbE Cu 2 USB 3.0, 1 consola, 1 puerto de gestión	2x40G; 8x25G, 4 x10G/5G/2.5/1G SFP+, 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 consola, 1 puerto de gestión
Almacenamiento	64GB M.2	128GB M.2	128 GB	128 GB	256GB M.2
Expansión	Ranura de expansión de almacenamiento (hasta 256GB)	Ranura de expansión de almacenamiento (hasta 256GB)	Ranura de expansión de almacenamiento (hasta 1TB)	Ranura de expansión de almacenamiento (hasta 1TB)	Ranura de expansión de almacenamiento (hasta 1TB)
Interfaces VLAN y de túnel lógicas (máximo)	256	256	512	512	512
Usuarios de SSO	40000	40000	50000	50000	70000
Puntos de acceso soportados (máximo)	512	512	512	512	512
Rendimiento de firewall/VPN					
Rendimiento de inspección del firewall ¹	5,2 Gbps	5,5 Gbps	18 Gbps	28 Gbps	36 Gbps
Rendimiento de prevención de amenazas ²	3,0 Gbps	3,5 Gbps	9,5 Gbps	15 Gbps	19 Gbps
Rendimiento de inspección de aplicaciones ²	3,6 Gbps	4,2 Gbps	11 Gbps	18 Gbps	20 Gbps
Rendimiento de IPS ²	3,4 Gbps	3,8 Gbps	10 Gbps	17 Gbps	20 Gbps
Rendimiento de inspección antimalware ²	2,9 Gbps	3,5 Gbps	9,5 Gbps	16 Gbps	18,5 Gbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL) ²	800 Mbps	850 Mbps	5 Gbps	7 Gbps	9 Gbps
Rendimiento de VPN IPsec ³	2,10 Gbps	2,2 Gbps	11 Gbps	15 Gbps	19 Gbps
Conexiones por segundo	21000	22000	115000	228000	228000
Conexiones máximas (SPI)	1500000	2000000	4000000	5000000	8000000
Conexiones DPI-SSL máximas	125000	150000	350000	350000	750000
Número máximo de conexiones (DPI)	500000	750000	2000000	3500000	6000000
VPN					
Túneles VPN entre emplazamientos	2000	3000	4000	6000	6000
Clientes VPN IPsec (máx.)	50 (1000)	50 (1000)	500 (3000)	2.000 (4000)	2.000 (6.000)
Licencias de VPN SSL (máximo)	2 (500)	2 (500)	2 (1000)	2 (1500)	2 (1500)
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				
Soporte de certificados	Verisign, Thawte, Cybertrust, RSA Keon, Entrust, y Microsoft CA para VPN SonicWall-SonicWall, SCEP				
Prestaciones VPN	Dead Peer Detection, DHCP a través de VPN, IPsec NAT Traversal, pasarela VPN redundante, VPN basada en enrutamiento				
Plataformas de cliente VPN globales admitidas	Windows 10		Microsoft® Windows Vista de 32/64 bits, Windows 7 de 32/64 bits, Windows 8.0 de 32/64 bits, Windows 8.1 de 32/64 bits, Windows 10		
NetExtender	Windows 10 y Linux		Microsoft Windows Vista de 32/64 bits, Windows 7, Windows 8.0 de 32/64 bits, Windows 8.1 de 32/64 bits, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE		
Mobile Connect	Apple® iOS, Mac OS X, Android, Kindle Fire, Chrome OS, Windows 10		Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (integrado)		

Especificaciones del sistema de la serie Gen 7 NSa

Firewall	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700
Servicios de seguridad					
Servicios Deep Packet Inspection	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL				
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, análisis de contenidos y palabras clave, filtrado completo basado en tipos de archivo como ActiveX, Java, cookies para la privacidad, listas de permitidos/denegados				
Comprehensive Anti-Spam Service	Soportado				
Visualización de aplicaciones	Sí				
Control de aplicaciones	Sí				
Capture Advanced Threat Protection	Sí				
Redes					
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				
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, 802.1e (WMM)				
Autenticación	LDAP (múltiples dominios), XAUTH/RADIUS, TACACS+, SSO, administración de cuentas Radius NTLM, base de datos de usuarios interna, 2FA, Terminal Services, Citrix, Common Access Card (CAC)				
Base de datos de usuarios local	1000	1000	2500	2500	3200
VoIP	H323-v1-5 completo, SIP				
Estándares	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Conforme con FIPS 140-2	Sí	Sí	Pendiente	Pendiente	Pendiente
Certificaciones	ICSA Enterprise Firewall, ICSA Antivirus, IPv6/USGv6				
Certificaciones (en proceso)	Common Criteria NDPP (Firewall con VPN e IPS)				
Common Access Card (CAC)	Soportado				
Alta disponibilidad	Activa/pasiva con sincronización de estado				
Hardware					
Factor de forma	Preparado para montaje en bastidor 1U				
Ventiladores	1	2	2 (extraíbles)	2 (extraíbles)	3 (extraíbles)
Fuente de alimentación	60 W	90 W	350 W	350 W	350 W
Consumo máximo de energía (W)	21,5	36,3	108,1	128,1	139,2
Fuente de alimentación redundante	100-240 V CA, 50-60 Hz				
Disipación de calor total	73,32 BTU	123,78 BTU	368,62 BTU	436,82 BTU	474,67 BTU
Dimensiones	43 x 32,5 x 4,5 (cm) 16,9 x 12,8 x 1,8 pulgadas	43 x 32,5 x 4,5 (cm) 16,9 x 12,8 x 1,8 pulgadas	43 x 46,5 x 4,5 (cm) 16,9 x 18,1 x 1,8 pulgadas	43 x 46,5 x 4,5 (cm) 16,9 x 18,1 x 1,8 pulgadas	43 x 46,5 x 4,5 (cm) 16,9 x 18,1 x 1,8 pulgadas
Peso	4,0 kg/8,8 libras	4,6 kg/10,2 libras	7,8 Kg	7,8 Kg	8,1 Kg
Peso WEEE	4,2 kg/9,3 libras	4,8 kg/10,6 libras	9,6 kg	9,6 kg	9,9 kg
Peso de envío	6,4 kg/14,1 libras	7 kg/15,4 libras	13,5 kg	13,5 kg	13,8 kg
Entorno (Operativo/Almacenamiento)	0°-40° C (32°-105° F)/-40° a 70° C (-40° a 158° F)				
Humedad	5-95%, sin condensación	5-95%, sin condensación	0-90% de HR, sin condensación	0-90% de HR, sin condensación	0-90% de HR, sin condensación
Normativas					
Números de modelo oficiales	1RK51-109	1RK52-110	1RK53-115	1RK53-116	1RK54-118
Cumplimiento de normas	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/GS, CB, Mexico CoC by UL, WEEE, REACH, ANATEL, BSMI				

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 herramientas de prueba de rendimiento de HTTP estándar Keysight. 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.

³ Rendimiento de VPN medido con tráfico de UDP utilizando un tamaño de paquetes de 1418 bytes, Codificación AESGMAC16-256 en conformidad con RFC 2544. Todas las especificaciones, las prestaciones y la disponibilidad están sujetas a modificaciones.

Visión de conjunto de las prestaciones de SonicOS 7.0

Firewall

- Inspección dinámica de paquetes
- Inspección profunda de paquetes sin reensamblado
- Protección contra ataques DDoS (inundaciones UDP/ICMP/SYN)
- Soporte para IPv4/IPv6
- Autenticación biométrica para el acceso remoto
- Proxy DNS
- Soporte completo de APIs
- Integración con SonicWall Switch
- Integración de puntos de acceso SonicWall Wi-Fi 6
- Escalabilidad de SD-WAN
- Asistente de usabilidad de SD-WAN¹
- Escalabilidad de conexiones (SPI, DPI, DPI SSL)
- Dashboard mejorado¹
- Vista de dispositivos mejorada
- Resumen de tráfico y usuarios principales
- Información valiosa sobre las amenazas
- Centro de notificaciones

Descifrado e inspección TLS/SSL/SSH

- TLS 1.3 con seguridad mejorada¹
- Inspección profunda de paquetes para TLS/SSL/SSH
- Inclusión/exclusión de objetos, grupos o nombres de host
- Control SSL
- Mejoras para DPI-SSL con CFS
- Controles DPI SSL granulares por zona o norma
- Capture Advanced Threat Protection²
- Inspección profunda de memoria en tiempo real
- Análisis multimotor basado en la nube²
- 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 real²
- Bloqueo hasta que haya un veredicto
- Capture Client²

Prevención de intrusiones²

- Análisis basado en definiciones
- Integración del control de acceso a la red con Aruba ClearPass
- Actualizaciones automáticas de las definiciones

- Inspección bidireccional
- Capacidad para reglas de IPS detalladas
- Refuerzo de GeolIP
- Filtrado de botnets con lista dinámica
- Coincidencia de expresiones regulares

Antimalware²

- Análisis de malware basado en flujos
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Inspección bidireccional
- Tamaño de archivo ilimitado
- Malware en la nube

Identificación de aplicaciones²

- 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 HTTP/HTTPS Web²

- Filtrado de URL
- Punteo de proxys
- Bloqueo según palabras clave
- Servicio de filtrado de contenido basado en la reputación (CFS 5.0)
- Filtrado de DNS
- 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

- Secure SD-WAN
- 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

- PortShield
- Jumbo frames
- Descubrimiento de rutas MTU
- Protocolización mejorada
- VLAN trunking
- Duplicación de puertos (SonicWall Switch)
- QoS de nivel 2
- Seguridad de puertos
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Controlador inalámbrico de SonicWall
- Enrutamiento basado en políticas (ToS/métrico y ECMP)
- NAT
- Servidor DHCP
- Gestión del ancho de banda
- Alta disponibilidad A/P con sincronización de estado
- Equilibrio de carga entrante/saliente
- Alta disponibilidad - Activa/en espera con sincronización de estado
- Modo puente de capa 2, modo wire/virtual wire, modo tap, modo NAT
- Enrutamiento asimétrico
- Compatibilidad con tarjetas Common Access Card (CAC)

VoIP

- Control QoS granular
- Gestión del ancho de banda
- DPI para tráfico VoIP
- Soporte de Gatekeeper H.323 y proxy SIP

Gestión, monitorización y soporte

- Soporte para Capture Security Appliance (CSa)
- Capture Threat Assessment (CTA) v2.0
- Nuevo diseño o plantilla
- Comparación entre la industria y la media global
- Nuevo layout intuitivo de prestaciones de IU/UX¹
- Dashboard
- Información sobre dispositivos, aplicación, amenazas
- Vista de topología
- Creación y gestión simplificadas de políticas

Visión de conjunto de las prestaciones de SonicOS 7.0 (cont.)

Gestión, monitorización y soporte (cont.)

- Estadísticas de uso de políticas/objetos¹
- Usado vs. no usado
- Activo vs. inactivo
- Búsqueda global de datos estadísticos
- Soporte de almacenamiento¹
- Gestión de almacenamiento interno y externo¹
- Soporte de tarjeta USB WWAN (5G/LTE/4G/3G)
- Soporte de Network Security Manager (NSM)
- GUI Web
- Interfaz de línea de comandos (CLI)
- Registro y aprovisionamiento sin necesidad de intervención
- Informes de CSC sencillos¹
- Soporte de aplicaciones móviles SonicExpress
- SNMPv2/v3

- Gestión e informes centralizados con SonicWall Global Management System (GMS)²
- API para informes y análisis
- Protocolización
- Exportaciones NetFlow/IPFIX
- Backup de configuración basado en la nube
- Plataforma de análisis de seguridad de BlueCoat
- Visualización de aplicaciones y ancho de banda
- Gestión de IPv4 e IPv6
- Pantalla de gestión CD
- Gestión de switches de las series Dell N y Dell X, incluidos switches en cascada

Depuración y diagnósticos

- Monitorización de paquetes mejorada
- Terminal SSH en IU

Conexión inalámbrica

- Gestión en la nube de los puntos de acceso SonicWave y gestión de firewalls
- WIDS/WIPS
- Prevención de puntos de acceso no autorizados
- Itinerancia rápida (802.11k/r/v)
- Redes en malla 802.11s
- Selección de autocanal
- Análisis de espectro de radiofrecuencia
- Vista del plano de planta
- Vista de topología
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth de baja energía
- MiFi extender
- Mejoras de radiofrecuencia
- Acceso limitado para usuarios invitados

¹ Nueva prestación, disponible en SonicOS 7.0

² Requiere suscripción adicional

Obtenga más información sobre la serie SonicWall Gen 7 NSa

www.sonicwall.com/products/firewalls

Acerca de SonicWall

SonicWall proporciona una ciberseguridad estable, escalable y fluida para la era hiperdistribuida, así como una realidad laboral caracterizada por la movilidad, el teletrabajo y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la ciberseguridad para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.



SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035

Si desea obtener más información, consulte nuestra página Web.

www.sonicwall.com

SONICWALL®

© 2023 SonicWall Inc. TODOS LOS DERECHOS RESERVADOS.

SonicWall es una marca comercial o marca comercial registrada de SonicWall Inc. y/o sus filiales en EEUU y/u otros países. Las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos propietarios. La información incluida en este documento se proporciona en relación con los productos de SonicWall Inc. y/o sus filiales. No se otorga mediante este documento, ni en relación con la venta de productos SonicWall, ninguna licencia, expresa ni implícita, por doctrina de los propios actos ni de ningún otro modo, sobre ningún derecho de propiedad intelectual. A excepción de lo establecido en los términos y condiciones tal y como se especifican en el contrato de licencia de este producto, SonicWall y/o sus filiales no asumen ninguna responsabilidad y rechazan cualquier garantía expresa, implícita o legal en relación con sus productos, incluidas, entre otras, las garantías implícitas de comercialización, adecuación para un determinado propósito o no violación de derechos de terceros. SonicWall y/o sus filiales no se harán responsables en ningún caso de daños directos, indirectos, consecuentes, punitivos, especiales ni incidentales (incluidos, sin limitación, los daños relacionados con la pérdida de beneficios, la interrupción del negocio o la pérdida de información) derivados del uso o de la incapacidad de utilizar el presente documento, incluso si se ha advertido a SonicWall y/o sus filiales de la posibilidad de que se produzcan tales daños. SonicWall y/o sus filiales no ofrecen declaración ni garantía alguna con respecto a la precisión ni a la integridad de la información contenida en el presente documento y se reservan el derecho de modificar las especificaciones y las descripciones de productos en cualquier momento y sin previo aviso. SonicWall Inc. y/o sus filiales no se comprometen a actualizar la información contenida en el presente documento.