Serie SonicWall Gen 7 NS*sp*

La serie SonicWall Network Security services platform™ (NS*sp*) ofrece firewalls de nueva generación con alta densidad de puertos e interfaces de velocidad multi-gigabit capaces de procesar varios millones de conexiones en busca de amenazas de día cero y avanzadas. Diseñada para empresas de gran tamaño, colegios y universidades, organismos gubernamentales y MSSPs, detecta ataques en tiempo real sin ralentizar el rendimiento. Está diseñada para ser altamente fiable y suministrar un servicio sin interrupción a las organizaciones.

Avance de las especificaciones de NS*sp*
Ver todas las especificaciones »

100 GbE	Hasta 100 Gbps	80 millones
Puertos	Rendimiento de inspección del firewall	Conexiones máximas (NS*sp* 15700)

FICHA TÉCNICA

PRESTACIONES DESTACADAS

Serie SonicWall NS*sp*

- Alta densidad de puertos
- Puertos 100 GbE
- Se integra con sandboxing local y en la nube
- Interfaz de usuario intuitiva con gestión centralizada
- Seguridad DNS
- Servicio de filtrado de contenido basado en reputación (CFS 5.0)
- Gestión de firewalls mediante Wi-Fi 6
- Integración del control de acceso de red con Aruba ClearPass
- Rendimiento de prevención de amenazas de más de 80 Gbps
- Fuente de alimentación redundante
- Rendimiento de inspección del firewall de hasta 100 Gbps
- Soporte para TLS 1.3
- Soporta millones de conexiones TLS simultáneas
- TCO reducido
- Respaldada por el equipo de investigación de amenazas SonicWall Capture Labs

Obtenga más información sobre la Serie SonicWall Gen 7 NS*sp*:

sonicwall.com/NS*sp*

Firewalls de clase empresarial

Mientras evolucionan las empresas, también aumentan los dispositivos gestionados y no gestionados, las aplicaciones SaaS, las conexiones cifradas, los usuarios, las redes, las cargas de trabajo en la nube y las velocidades de Internet. Ante este panorama, un firewall que no sea capaz de soportar este desarrollo se convierte rápidamente en un cuello de botella. No obstante, un firewall debería destacar por su solidez y no por ser un punto débil.

Con sus interfaces múltiples 100G/40G/25G/10G el firewall de SonicWall NS*sp* permite procesar simultáneamente varios millones de conexiones cifradas y no cifradas con una tecnología de prevención de amenazas sin parangón. Dado que hoy en día más del 70 % de las sesiones están cifradas, es extremadamente importante para la productividad y la seguridad de la información contar con un cortafuegos que pueda procesar y examinar este tráfico sin comprometer la experiencia del usuario.

Las políticas unificadas de NS*sp* 15700 permiten a las organizaciones crear de forma fácil e intuitiva políticas de acceso y seguridad desde una única interfaz.

Gestión e informes simplificados

SonicWall Network Security Manager se encarga de las tareas de gestión y monitorización y de generar informes sobre las actividades de red. Gracias a un panel de control intuitivo, el usuario puede gestionar el cortafuegos y generar informes históricos de forma centralizada. Fácil de implantar, configurar y gestionar, las organizaciones pueden reducir su coste total de propiedad y beneficiarse de un rápido retorno de la inversión.

Implementación

Firewall de nueva generación (NGFW)

- Gestionado a través de una consola única.
- La serie NS*sp* se integra estrechamente con el resto del ecosistema de soluciones de SonicWall.
- Obtenga una visibilidad completa de su red para ver lo que las aplicaciones, los dispositivos y los usuarios hacen. De esta forma podrá aplicar las políticas adecuadas y eliminar las amenazas y los cuellos de botella en el rendimiento.
- Integre con Capture ATP con la tecnología patentada RTDMI para sandboxing basado en la nube o Capture Security Appliance para la detección de malware local.

Inspección profunda de paquetes de SSL/TLS (DPI-SSL) para la detección de amenazas ocultas

- NS*sp* inspecciona millones de conexiones cifradas TLS/SSL y SSH simultáneas, independientemente del puerto o protocolo.
- Las reglas de inclusión y exclusión permiten una personalización basada en ciertos requisitos de cumplimiento específicos de la empresa y/o requisitos legales.
- Soporte de para suites de cifrado TLS hasta TLS 1.3.

Segmentación y redes

- Opere a través de múltiples redes segmentadas, nubes o definiciones de servicios con plantillas, grupos de dispositivos y políticas únicas para múltiples dispositivos y tenants.
- Los MSSP también pueden soportar varios clientes con una *clean pipe* y políticas únicas.

Firewall multi-instancia (solo en NS*sp* 15700)

- La multi-instancia es la nueva generación de multiempresa.
- Cada tenant está aislado y tiene recursos informáticos dedicados para evitar la falta de recursos.
- Incluye puertos/usuarios físicos y lógicos.
- Soporta políticas y gestión de la configuración independientes para tenants.
- Soporte independencia de versiones y alta disponibilidad (HA) para tenants.

Funcionalidad de modo Wire

- Modo Bypass para la introducción rápida y relativamente libre de interrupciones de hardware de firewall en una red.
- Modo Inspect para ampliar el Modo Bypass sin alterar funcionalmente la ruta de paquetes de bajo riesgo y latencia cero.
- Modo Secure para interponer activamente los procesadores multinúcleo del firewall en la ruta de procesamiento de paquetes.
- Modo Tap para recibir un flujo de paquetes duplicado a través de un solo puerto de switches en el firewall, eliminando la necesidad de realizar una inserción física intermedia.

Protección contra amenazas avanzadas

- SonicWall Capture Advanced Threat Protection™ (ATP) es utilizada por más de 150.000 clientes en todo el mundo a través en una gran variedad de soluciones para detectar y detener cada día más de 1.200 formas nuevas de malware.
- La serie NS*sp* se integra con Capture Security Appliance para detectar y bloquear amenazas desconocidas con un sandboxing local basado en la Inspección profunda de memoria en tiempo real (Real-Time Deep Memory Inspection™, RTDMI).

Plataforma Capture Cloud

- La plataforma Capture Cloud de SonicWall proporciona a las pequeñas y grandes organizaciones funciones de prevención de amenazas y gestión de red basadas en la nube, así como prestaciones de informes y análisis.

Content Filtering Services (Servicios de filtrado de contenido)

- Compare los sitios web solicitados con una enorme base de datos en la nube que contiene millones de URLs, direcciones de IP y sitios web clasificados.
- Cree y aplique políticas que permitan o denieguen el acceso a los sitios web en función de la identidad del individuo o grupo, o de la hora del día.
- El Servicio de Filtrado de contenido basado en la reputación (CFS 5.0) le permite reforzar las políticas de uso de Internet y controlar el acceso interno a contenido Web inapropiado, improductivo y potencialmente ilegal con un exhaustivo filtrado del contenido que cubre 93 categorías Web. El filtrado de contenido basado en la reputación proporciona una puntuación sobre el riesgo de seguridad de una URL.

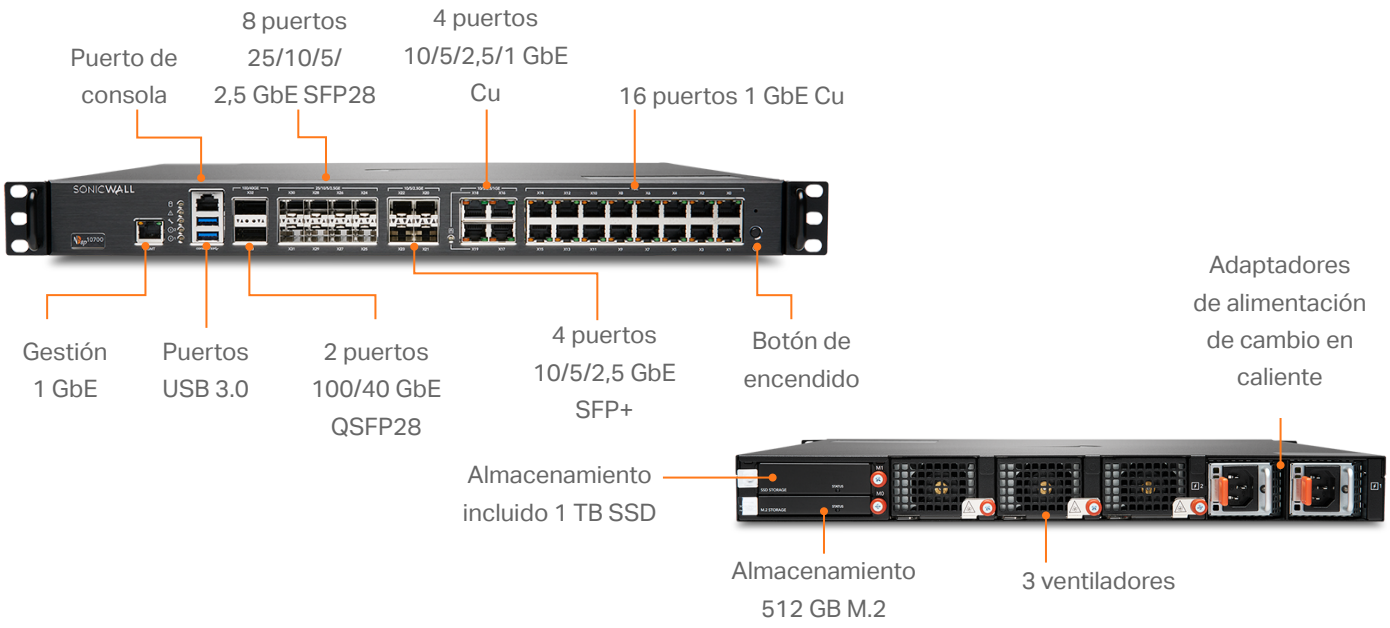
Intrusion Prevention System (Sistema de prevención de intrusiones, IPS)

- Proporciona un motor de inspección profunda de paquetes (Deep Packet Inspection, DPI) configurable y de alto rendimiento para ofrecer una protección ampliada de los servicios de red más importantes, como los servicios Web, el correo electrónico, la transferencia de archivos, los servicios Windows y DNS.
- Está diseñado para ofrecer protección contra las vulnerabilidades de las aplicaciones, así como contra gusanos, troyanos, spyware y exploits de puerta trasera.
- La base de datos de definiciones extensible ofrece una defensa proactiva contra vulnerabilidades de aplicaciones y de protocolos recién descubiertas.
- SonicWall IPS elimina la costosa y pesada tarea de mantener y actualizar definiciones para nuevos ataques, a través de la arquitectura de refuerzo distribuida (DEA) de SonicWall, líder en el sector.

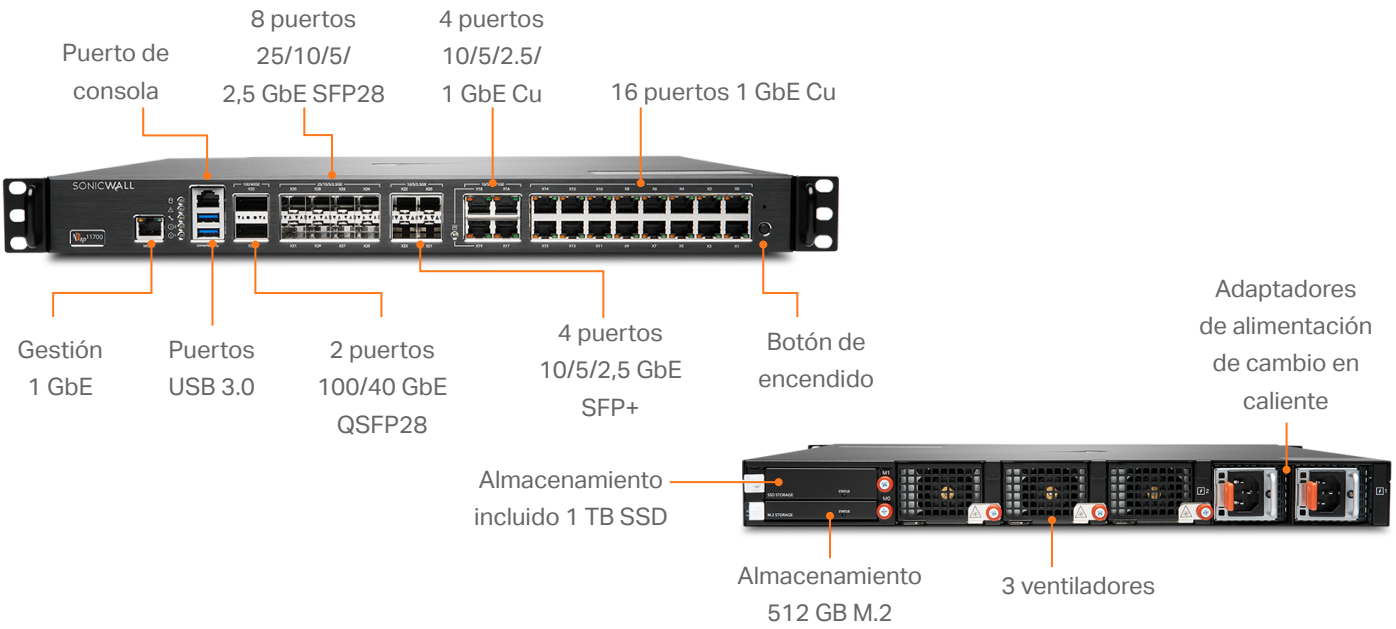
IoT y control de aplicaciones

- La serie NS*sp* cataloga miles de aplicaciones a través de App Control y monitoriza su tráfico para detectar cualquier comportamiento anómalo.

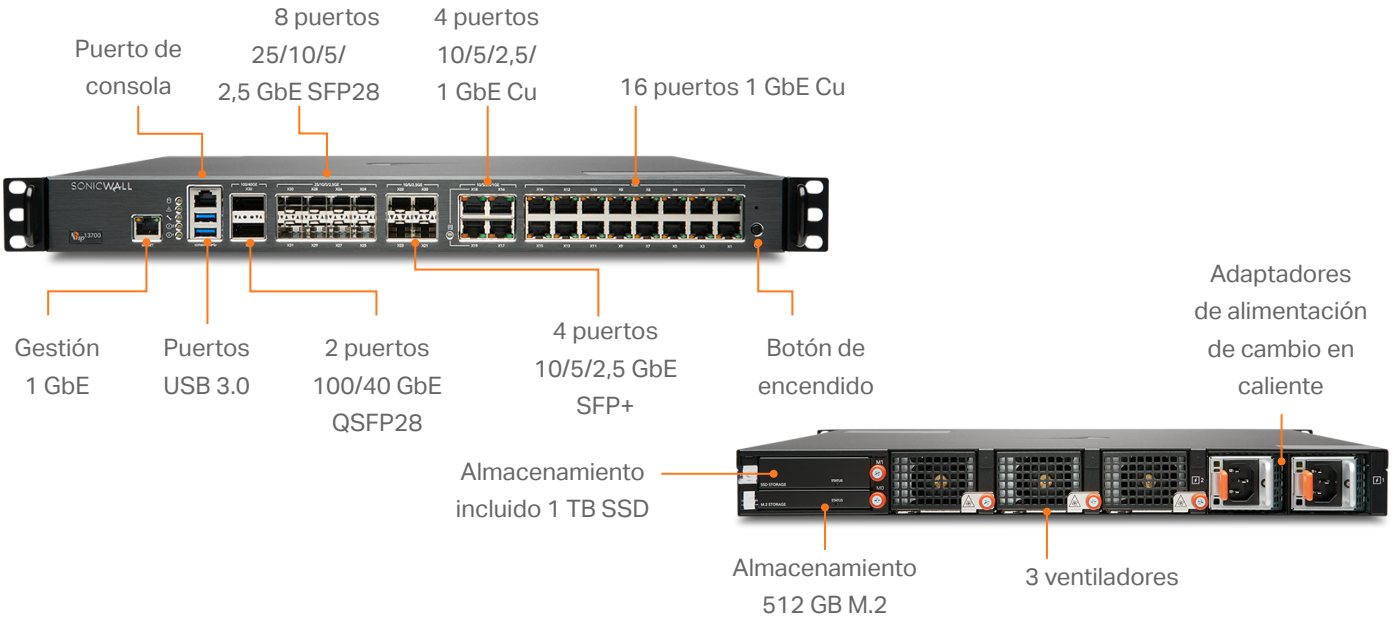
NS*sp* 10700



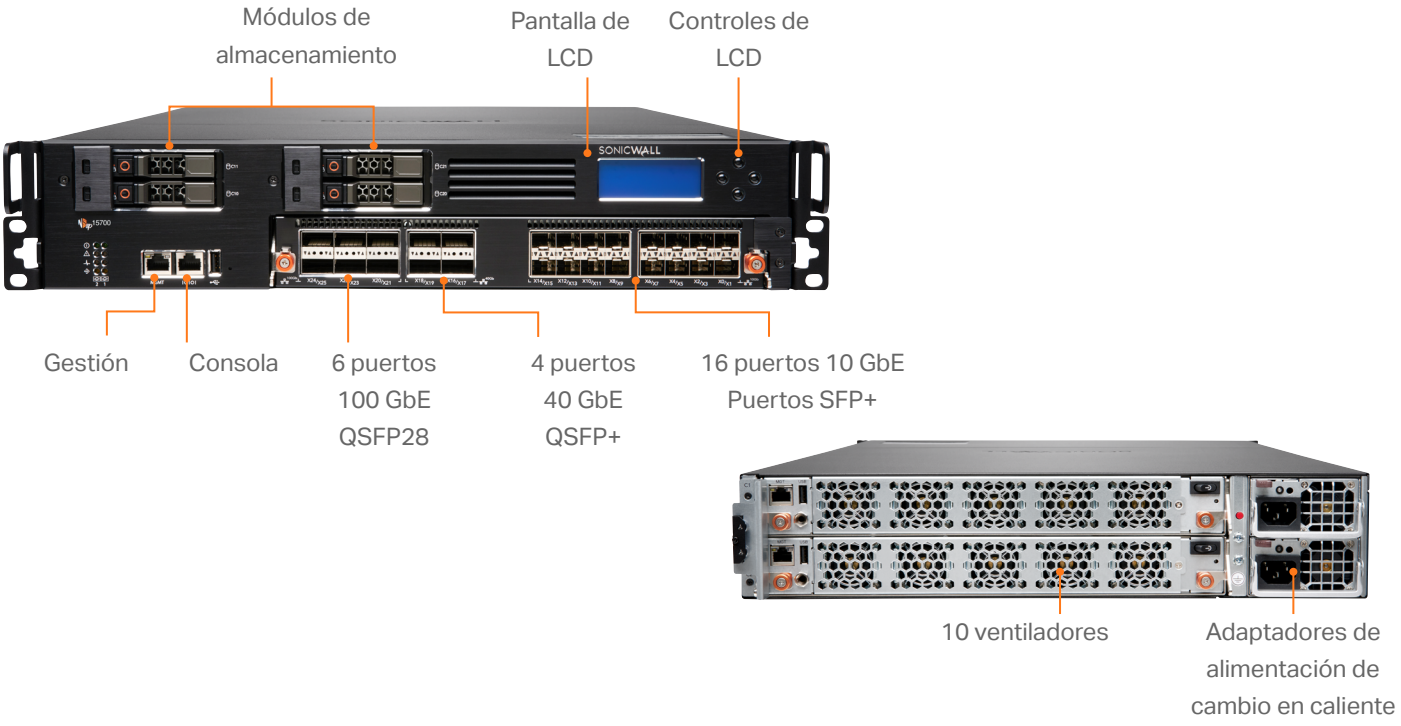
NS*sp* 11700



NS*sp* 13700



NS*sp* 15700



Especificaciones de la serie NS*sp*

Firewall general	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Sistema operativo	SonicOS 7.0.1	SonicOS 7.0.1	SonicOS 7.0.1	SonicOSX 7.0.1
Interfaces	2x100/40 GbE QSFP28, 8x25/10/5/2,5-GbE SFP28 4x10G/5G/2,5G/1G (SFP+), 4 x 10G/5G/2,5G/1G (Cu); 16 x 1 GbE (Cu) 2 USB 3.0, 1 consola, 1 puerto de gestión	2x100/40 GbE QSFP28, 8x25/10/5/2,5-GbE SFP28 4x10G/5G/2,5G/1G (SFP+), 4 x10G/5G/2,5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 consola, 1 puerto de gestión	2x100/40 GbE QSFP28, 8x25/10/5/2,5 GbE SFP28, 4x10/5/2,5 GbE SFP+, 4x10/5/2,5/1 GbE Cu, 16x1 GbE, 2 USB 3.0, 1 consola, 1 puerto de gestión	6 x 100 GbE QSFP28, 4 x 40 GbE QSFP+, 16 x 10 GbE SFP+ 3 USB 3.0, 1 consola, 1 puerto de gestión
Almacenamiento total	1,5 TB	1,5 TB	1,5 TB	2 SSD de 480 GB
Gestión	CLI, SSH, Web UI, APIs REST			
Usuarios de SSO	100.000			
Puntos de acceso soportados (máximo)	512	512	512	512
Protocolización	Analytics, Local Log, Syslog, IPFIX, NetFlow			

Rendimiento de firewall/VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Rendimiento de inspección del firewall[1]	42 Gbps	47 Gbps	60 Gbps	105 Gbps
Rendimiento de prevención de amenazas[2]	28 Gbps	37 Gbps	45,5 Gbps	82 Gbps
Rendimiento de inspección de aplicaciones[2]	30 Gbps	44 Gbps	57 Gbps	86 Gbps
Rendimiento de IPS[2]	28 Gbps	37 Gbps	48 Gbps	76,5 Gbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL)[2]	10 Gbps	11,5 Gbps	16,5 Gbps	21 Gbps
Rendimiento de VPN[3]	22,5 Gbps	26,7 Gbps	29 Gbps	32 Gbps
Conexiones por segundo	280.000	280.000	280.000	800.000
Conexiones máximas (SPI)	15.000.000	20.000.000	25.000.000	40.000.000
Número máximo de conexiones (DPI)	12.000.000	17.000.000	22.000.000	40.000.000
Número máximo de conexiones (DPI SSL)	1.500.000	1.750.000	2.000.000	4.000.000

VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Túneles VPN entre emplazamientos	6.000	12.000	12.000	25.000
Clientes VPN IPSec (máx.)	2000 (6000)	2000 (6000)	2.000 (6.000)	2.000 (10.000)
Licencias de VPN SSL (máximo)	100 (3000)	100 (3000)	100 (3000)	256 (3000)
Cifrado/autenticación	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA (1,256,384,512), criptografía Suite B		DES, 3DES, AES (128, 192, 256-bit)/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	Microsoft® Windows 11, Windows 10 (64 y 32 bits)			
NetExtender	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, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (integrado)			

Redes	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Firewall multi-instancia	No disponible	No disponible	No disponible	Tenants máximos por hardware: 12
Asignación de direcciones IP	Estática (cliente DHCP, PPPoE, L2TP y PPTP), servidor DHCP interno, relé DHCP			

Especificaciones de la serie NS*sp*

Redes	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IP solapada), PAT, modo transparente			
Interfaces lógicas VLAN y de túnel (máximo)	1024			
Modo Wire	–	–	–	Sí
Protocolos de enrutamiento	BGP4, OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas	BGP4, OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas	BGP4, OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas	BGP, 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, Radius accounting NTLM, base de datos de usuarios interna, 2FA, Terminal Services, Citrix, Common Access Card (CAC)		LDAP (múltiples dominios), XAUTH/RADIUS, SSO, Novell, base de datos de usuarios interna, Terminal Services, Citrix, Common Access Card (CAC)	
Base de datos de usuarios local	4.000	4.000	4.000	5.000
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			
Compatible con FIPS 140-2	Pendiente	Pendiente	Pendiente	Sí
Certificaciones	ICSA Enterprise Firewall, ICSA Antivirus, IPv6/USGv6			
Certificaciones (en proceso)	Common Criteria NDPP Firewall con VPN e IPS			
Alta disponibilidad	Activa/pasiva con sincronización de estado			

Hardware	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Fuente de alimentación	2 x 350 W	2 x 350 W	2 x 350 W	Doble, redundante, 1.200 W
Ventiladores	3 (extraíble)	3 (extraíble)	3 (extraíble)	10
Fuente de alimentación redundante	100-240 V CA, 50-60 Hz			
Consumo máximo de energía (W)	155,3	155,3	181,2	1135,0
Disipación de calor total	529,57 BTU	529,57 BTU	617,89 BTU	3870,35 BTU
Factor de forma	Preparado para montaje en bastidor 1U	Preparado para montaje en bastidor 1U	Preparado para montaje en bastidor 1U	Preparado para montaje en bastidor 2U
Dimensiones	43 x 46 x 4,5 (cm) 16,9 x 18,1 x 1,8 pulgadas	43 x 46 x 4,5 (cm) 16,9 x 18,1 x 1,8 pulgadas	43 x 46 x 4,5 (cm) 16,9 x 18,1 x 1,8 pulgadas	68,6 x 43,8 x 8,8 (cm)
Peso	9,1 kg	9,1 kg	9,1 kg	26 kg
Peso WEEE	11 kg	11 kg	11 kg	30,1 kg
Peso de envío	14,9 kg	14,9 kg	14,9 kg	37,3 kg
Entorno (Operativo/ Almacenamiento)	0°-40° C (32°-105° F)/-40° a 70° C (-40° a 158° F)			
Humedad	0-90 % de HR, sin condensación	0-90 % de HR, sin condensación	0-90 % de HR, sin condensación	10–95 %, sin condensación
Normativas	**NS*sp* 10700**	**NS*sp* 11700**	**NS*sp* 13700**	**NS*sp* 15700**
Números de modelo oficiales	1RK54-118	1RK54-119	1RK54-118	2RK05-0FE
Conformidad con 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	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	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	FCC Class A, ICES Class A, CE (EMC Class A, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/GS, CB, Mexico UL DGN notification, 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/GatewayAV/ 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.

Resumen de las funciones de SonicOSX

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
- APIs REST
- Integración de SonicWall Switch
- Integración de puntos de acceso SonicWall Wi-Fi 6

Política de seguridad unificada

- Las políticas unificadas combinan normas de capa 4 a capa 7:
  - Fuente/IP de destino/Puerto/Servicio
  - Control de aplicaciones
  - CFS/Filtrado Web
  - Refuerzo de servicios de seguridad de paso único
  - IPS/GAV/AS/Capture ATP
- Gestión de normas:
  - Clonado
  - Análisis *shadow rule*
  - Edición en celdas
  - Edición de grupos
- Gestión de vistas
  - Normas utilizadas/no utilizadas
  - Normas activas/inactivas
  - Secciones

Descifrado e inspección TLS/SSL/SSH

- TLS 1.3
- Inspección profunda de paquetes para TLS/SSL/SSH
- Inclusión/exclusión de objetos, grupos o nombres de host
- Control SSL
- Controles DPI-SSL granulares por zona o norma
- Políticas de descifrado para SSL/TLS y SSH

Capture Advanced Threat Protection[1]

- Inspección profunda de memoria en tiempo real
- Análisis multimotor basado en la nube
- Sandboxing virtualizado
- Análisis de nivel de hipervisor
- Emulación de sistema completo
- Análisis de gran variedad de tipos de archivos
- Envío automático y manual
- Actualizaciones de inteligencia de amenazas en tiempo real
- Bloqueo hasta que haya un veredicto
- Integración de Capture Client

Prevención de intrusiones[1]

- Análisis basado en definiciones
- Integración del control de acceso de red con Aruba ClearPass
- Actualizaciones automáticas de las definiciones
- Inspección bidireccional
- Capacidad para reglas de IPS detalladas
- Refuerzo de GeoIP
- Filtrado de botnets con lista dinámica
- Coincidencia de expresiones regulares

Antimalware[1]

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

Identificación de aplicaciones[1]

- 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
- Uso de aplicaciones/ancho de banda/ amenazas
- Análisis basados en la nube

Filtrado de contenido HTTP/HTTPS Web[1]

- Filtrado de URL
- Puenteo 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
- Content Filtering Client

VPN

- VPN con aprovisionamiento automático
- VPN IPSec para conectividad entre emplazamientos
- Acceso remoto mediante VPN SSL y cliente IPSec
- Pasarela VPN redundante
- Mobile Connect para iOS, Mac OS X, Windows, Chrome, Android y Kindle Fire
- VPN basada en rutas (OSPF, RIP, BGP)

Redes

- Firewall multi-instancia (solo en NS*sp* 15700)
- PortShield
- Jumbo frames
- Descubrimiento de rutas MTU
- Protocolización mejorada
- VLAN trunking
- Duplicación de puertos
- QoS de nivel 2
- Seguridad de puertos
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Enrutamiento basado en políticas (ToS/ métrico y ECMP)
- NAT
- Servidor DHCP
- Gestión del ancho de banda
- Agregación de enlaces (estática y dinámica)
- Redundancia de puertos
- Alta disponibilidad A/P con sincronización de estado
- Equilibrio de carga entrante/saliente
- Alta disponibilidad - Activa/en espera con sincronización de estado
- Modo wire/virtual wire, modo tap, modo NAT
- Enrutamiento asimétrico

VoIP

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

Gestión y supervisión

- GUI Web
- Interfaz de línea de comandos (CLI)
- Registro y aprovisionamiento sin necesidad de intervención
- API Rest
- Soporte de aplicaciones móviles SonicExpress
- SNMPv2/v3
- Gestión e informes centralizados con SonicWall Network Security Manager (NSM)[1]
- Protocolización
- Exportaciones NetFlow/IPFIX
- Backup de configuración basado en la nube
- Visualización de aplicaciones y ancho de banda
- Gestión de IPv4 e IPv6

[1] Requiere suscripción adicional.

Encuentre el firewall adecuado de SonicWall para su empresa

www.sonicwall.com/firewalls

Acerca de SonicWall

SonicWall proporciona una ciberseguridad estable, escalable y fluida para la era hiperdistribuida, así como para 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 seguridad cibernética 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

Datasheet-NSsp-A4-JK-9962