SonicWall Gen 7 NS*a* Series

Los firewalls de próxima generación (NGFWs) de 7ª generación (Gen 7) Network Security Appliance (NS*a*) 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 y servicios de reputación de IP, protege el perímetro contra amenazas avanzadas sin formar cuellos de botella.

PRESTACIONES DESTACADAS

- Factor de forma – 1 RU
- Múltiples interfaces 1 GbE y 10 GbE
- Rendimiento de análisis de amenazas y malware multigigabit
- Solución de clase empresarial habilitada para el borde de Internet
- Soporte para SonicOS de la más reciente generación 7
- Secure SD-WAN
- Gestión intuitiva desde una única consola
- Soporte para TLS 1.3
- Mejor relación precio/rendimiento
- Rendimiento de DPI rápido
- TCO más bajo en su categoría
- 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 NS*a*. Ver todas las especificaciones »

Rendimiento de prevención de amenazas	Conexiones	Puertos
3,5 Gbps	2 millones	Múltiples puertos 10 GbE

Encuentre la solución de SonicWall adecuada para su empresa:

sonicwall.com/products

DATASHEET

Con una alta densidad de puertos, incluidos múltiples puertos 1 GbE y 10 GbE, la solución soporta la redundancia de red y de hardware con alta disponibilidad, la agrupación y dos fuentes de alimentación.

Los firewalls de próxima generación (NGFWs) de 7ª generación (Gen 7) Network Security Appliance (NS*a*) 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 y servicios de reputación de IP, protege el perímetro contra amenazas avanzadas sin formar cuellos de botella.

La serie Gen 7 NS*a* 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 1 GbE y 10 GbE, la solución soporta la redundancia de red y de hardware con alta disponibilidad, la agrupación y dos fuentes de alimentación.

Generación 7 – SonicOS 7.0 y Servicios de seguridad

La Serie Gen 7 NS*a* 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 7.0 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 NS*a* soporta prestaciones avanzadas de red, como SD-WAN, enrutamiento dinámico, agrupación 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, permiténdole 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), 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.

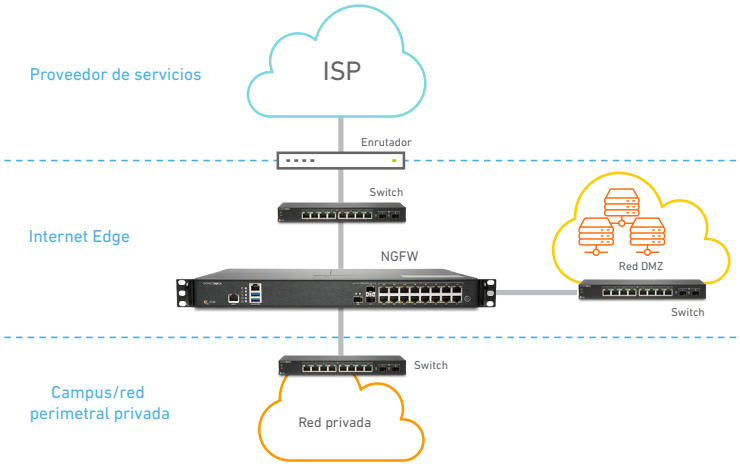
Implementaciones

La Serie Gen 7 NS*a* 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 NS*a* protege las redes privadas del tráfico malicioso procedente de Internet, lo cual le permite:

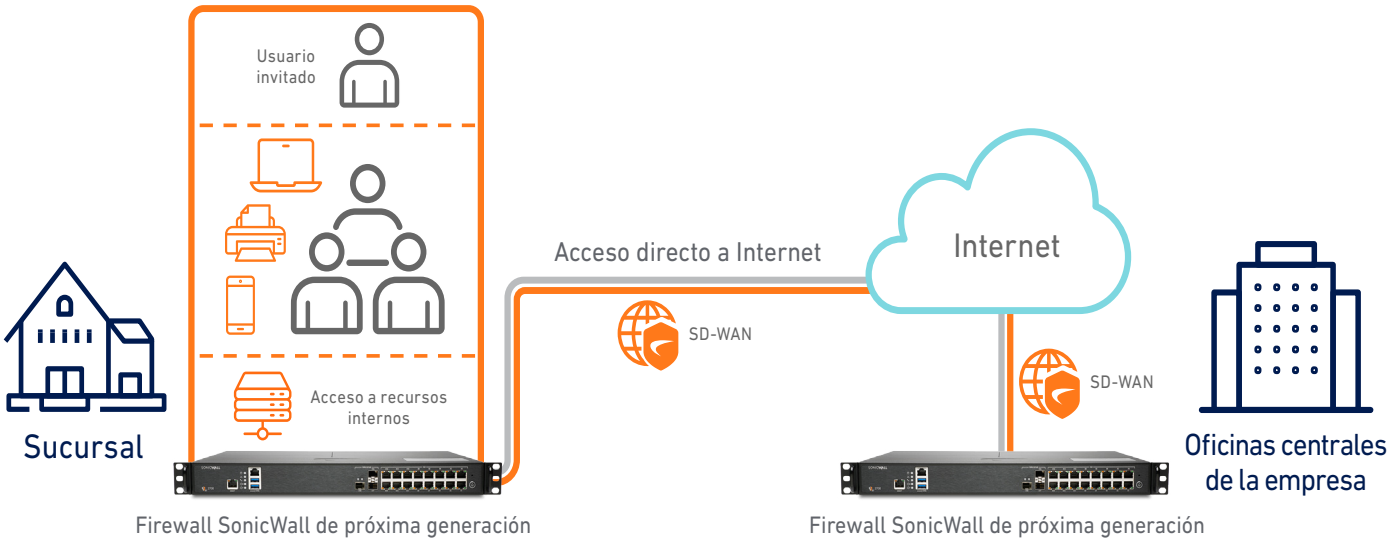
- Implementar una solución NGFW probada con el mayor rendimiento y la mayor densidad de puertos (incluida conectividad 10 GbE) de su categoría
- Obtener visibilidad e inspeccionar el tráfico cifrado, incluido el TLS 1.3, para bloquear las amenazas evasivas procedentes de Internet — todo ello sin comprometer 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

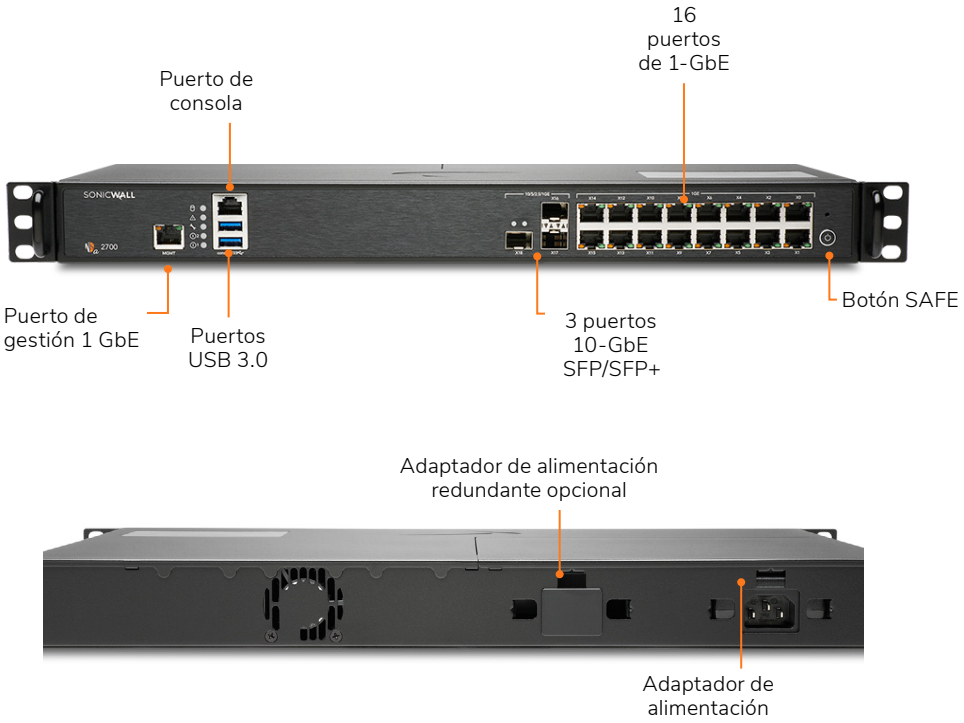
La Serie SonicWall Gen 7 NS*a* soporta SD-WAN y puede gestionarse de forma centralizada, lo cual hace que sea ideal para las empresas medianas y distribuidas. Esta implementación permite a las organizaciones:

- Garantizar su seguridad en el futuro ante un panorama de 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 10 GbE, para soportar una empresa distribuida y redes de área amplia

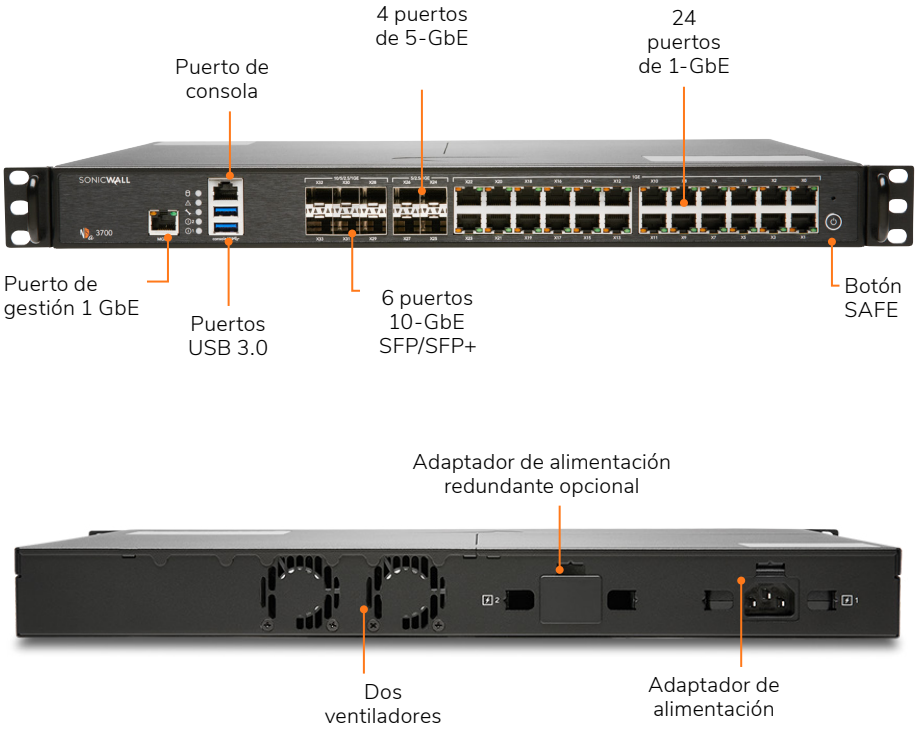


Serie SonicWall Gen 7 NS*a*

NS*a* 2700



NS*a* 3700



Especificaciones del sistema de la Serie Gen 7 NS*a*

Firewall	NS*a* 2700	NS*a* 3700
Sistema operativo	SonicOS 7.0	SonicOS 7.0.1
Interfaces	16x1GbE, 3x10GbE SFP+, 2 USB 3.0, 1 consola, 1 puerto de gestión	24x1GbE, 6x10GbE SFP+, 4x5GbE SFP+, 2 USB 3.0, 1 consola, 1 puerto de gestión
Almacenamiento	64GB M.2	128GB M.2
Expansión	Ranura de expansión de almacenamiento (hasta 256GB)	Ranura de expansión de almacenamiento (hasta 256GB)
Interfaces VLAN	256	256
Puntos de acceso soportados (máximo)	32	32
Rendimiento de firewall/VPN		
Rendimiento de inspección del firewall[1]	5,2 Gbps	5,5 Gbps
Rendimiento de prevención de amenazas[2]	3,0 Gbps	3,5 Gbps
Rendimiento de inspección de aplicaciones[2]	3,6 Gbps	4,2 Gbps
Rendimiento de IPS[2]	3,4 Gbps	3,8 Gbps
Rendimiento de inspección antimalware[2]	2,9 Gbps	3,5 Gbps
Rendimiento de inspección y descifrado TLS/SSL (DPI SSL)[2]	800 Mbps	850 Mbps
Rendimiento de VPN IPSec[3]	2,10 Gbps	2,2 Gbps
Conexiones por segundo	21.500	22.500
Conexiones máximas (SPI)	1.500.000	2.000.000
Conexiones DPI-SSL máximas	125.000	150.000
Número máximo de conexiones (DPI)	500.000	750.000
VPN		
Túneles VPN entre emplazamientos	2.000	3.000
Clientes VPN IPSec (máx.)	50 (1000)	50 (1000)
Licencias de VPN SSL (máximo)	2 (500)	2 (500)
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 VPN, 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 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	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)	
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	
Interconexión		
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	

Especificaciones del sistema de la Serie Gen 7 NS*a*

Firewall	**NS*a* 2700**	**NS*a* 3700**
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, SSO, Novell, base de datos de usuarios interna, Terminal Services, Citrix, Common Access Card (CAC)	
Base de datos de usuarios local	250	
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	
Certificaciones (pendientes)	FIPS 140-2 (con Suite B) nivel 2, UC APL, VPNC, IPv6 (fase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall e IPS)	
Tarjetas Common Access Card (CAC)	Soportado	
Alta disponibilidad	Activa/pasiva con sincronización de estado	
Hardware		
Factor de forma	Preparado para montaje en bastidor 1U	Preparado para montaje en bastidor 1U
Fuente de alimentación	60W	90W
Consumo máximo de energía (W)	21,5	36,3
Potencia de entrada	100-240 V CA, 50-60 Hz	100-240 V CA, 50-60 Hz
Disipación de calor total	73,32 BTU	123,78 BTU
Dimensiones	16,9 x 12,8 x 43 cm (43 x 32,5 x 4,5 pulgadas)	16,9 x 12,8 x 43 cm (43 x 32,5 x 4,5 pulgadas)
Peso	4,0 kg/8,8 libras	4,6 kg/10,2 libras
Peso WEEE	4,2 kg/9,3 libras	4,8 kg/10,6 libras
Peso de envío	6,4 kg/14,1 libras	7 kg/15,4 libras
Entorno (Operativo/Almacenamiento)	0°-40° C (32°-105° F)/-40° a 70° C (-40° a 158° F)	
Humedad	5-95%, sin condensación	
Normativas		
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	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/GatewayAV/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. Rendimiento de Prevención de amenazas medido con Gateway AV, Anti-Spyware, IPS and Application Control activado.
3. Rendimiento VPN medido sobre la base de tráfico UDP y paquetes de 1.280 bytes según RFC 2544. 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 de SonicWall Switch
- Escalabilidad de SD-WAN
- Asistente de usabilidad de SD-WAN[1]
- Contenedorización de SonicCoreX y SonicOS[1]
- Escalabilidad de conexiones (SPI, DPI, DPI SSL)
- Dashboard mejorado[1]
- 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 mejorada[1]
- 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 Protection[2]
- 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
- Capture Client

Prevención de intrusiones[2]

- Análisis basado en definiciones
- 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[2]

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

Identificación de aplicaciones[2]

- 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 Web[2]

- Filtrado de URL
- Puenteo de proxys
- Bloqueo según palabras clave
- 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)

Interconexión

- PortShield
- Jumbo frames
- Descubrimiento de rutas MTU
- Protocolización mejorada
- VLAN trunking
- Duplicación de puertos (NS*a* 2650 y superior)
- 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 (CS*a*)
- Capture Threat Assessment (CTA) v2.0
- Nuevo diseño o plantilla
- Comparación con la media global y de la industria
- Nuevo layout intuitivo de prestaciones de IU/UX[1]
- Dashboard
- Información sobre dispositivos, aplicación, amenazas
- Vista de topología
- Creación y gestión simplificadas de políticas
- Estadísticas de uso de políticas/objetos[1]
- Usado vs. no usado
- Activo vs. inactivo
- Búsqueda global de datos estadísticos

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

- Soporte de almacenamiento[1]
- Gestión de almacenamiento interno y externo[1]
- 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 sencillos[1]
- Soporte de aplicaciones móviles SonicExpress
- SNMPv2/v3
- Gestión e informes centralizados con SonicWall Global Management System (GMS)[2]
- 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
- 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 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 sin límites, sin perímetro, para la era hiperdistribuida y una realidad laboral caracterizada por la movilidad, el trabajo remoto 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 o síganos en Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com